Sécurité de la plate-forme Washington DC

Dernière mise à jour: 17/12/2025

Traduction automatique

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.

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

servicenow

Sommaire

Traduction automatique

Traduction automatique

Traduction automatique

Traduction automatique

Traduction automatique

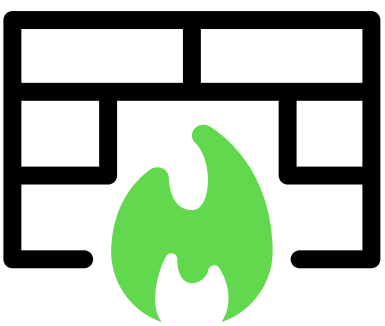
Sécuriser votre instance

Now Platform® Security vous permet de sécuriser votre instance, de chiffrer vos données, de vérifier l'identité, d'authentifier les utilisateurs et de consulter vos niveaux de conformité actuels en fonction des normes de sécurité des applications.

Security est intégré à tous les niveaux de la Now Platform. Implémentez les fonctionnalités de sécurité adaptées à votre organisation, de la gestion des connexions ayant échoué à la protection chiffrée des mots de passe, en passant par les règles de contrôle et les journaux d'audit.

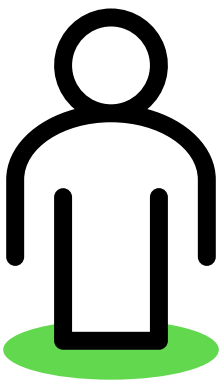
Choisissez l'une des vignettes suivantes pour commencer.

Sécurité de la plateforme



ServiceNow® L'application Platform Security de dispose d'un ensemble de fonctionnalités qui protègent votre instance contre les intrusions de sécurité et assurent la sécurité de vos données.

Confidentialité de la plateforme



L'application Confidentialité de la plateforme vous permet de classer les données sensibles et de supprimer les informations à caractère personnel (PII) des données utilisateur dans une instance de production et d'anonymiser les données dans les instances de non-production. Une fois anonymisées, les données utilisateur ne sont plus considérées comme des informations privées réglementées.

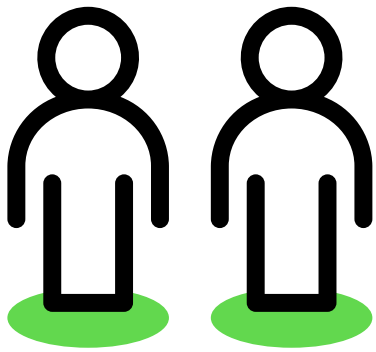
Identité

ServiceNow® L'application Platform Identity de dispose d'un ensemble de fonctionnalités pour connaître les identités dans l'ensemble de l'instance.

Traduction automatique

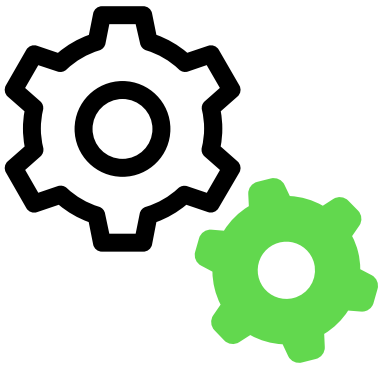
servicenow

Gestion des accès



ServiceNow® permet d’authentifier un utilisateur qui accède à une instance, puis autorise l’utilisateur à accéder aux fonctionnalités correspondant au rôle ou à la fonction de l’utilisateur.

Paramètres généraux de sécurité de la plateforme



En savoir plus sur les paramètres généraux de l'application Sécurité de la plateforme.

Traduction automatique

Sécuriser votre instance

Security est intégré à tous les niveaux de la Now Platform. Implémentez les fonctionnalités de sécurité adaptées à votre organisation, de la gestion des connexions ayant échoué à la protection chiffrée des mots de passe, en passant par les règles de contrôle et les journaux d'audit.

ServiceNow Vault

Utilisez les outils de sécurité des données du produit ServiceNow Vault pour protéger les informations sensibles contre tout accès non autorisé, endommagement ou vol tout au long de leur cycle de vie. Appliquez des protections telles que le chiffrement, la gestion des secrets et la confidentialité des données pour la rédaction et l'audit des informations sensibles. La page d'accueil de ServiceNow Vault constitue un emplacement unique pour rechercher des produits de sécurité des données ServiceNow Vault et y accéder.

Traduction automatique

Réduire les risques liés aux données sensibles

Chiffrez les données de la plateforme à l'aide de Key Management Framework et Entreprise de Chiffrement au niveau des colonnes, qui assurent la protection des clés et la gestion du cycle de vie des clés pour le chiffrement des champs au niveau de l'application.

Chiffrer les données en cours

Chiffrez les données à l'aide d'un serveur de votre réseau capable de chiffrer et de déchiffrer les données sensibles qui transitent entre votre centre de données et le cloud ServiceNow.

Sécuriser l'accès à votre instance

Validez l’identité d’un utilisateur qui accède à une instance et autorisez l’utilisateur à accéder aux fonctionnalités qui correspondent au rôle ou à la fonction de l’utilisateur.

Anonymiser les informations à caractère personnel (PII)

Déterminez s'il convient d'anonymiser toutes les informations de tous les utilisateurs ou d'un sous-ensemble d'utilisateurs. Une fois anonymisées, les données des enregistrements utilisateur sélectionnés sont remplacées par des valeurs aléatoires 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. 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.

Répondre rapidement aux risques

Augmentez la visibilité de la sécurité grâce à un tableau de bord en temps réel, à des recommandations personnalisées et à des étapes guidées pour une résolution rapide des failles de sécurité.

Réduire les risques liés aux données sensibles à l'aide de Column Level Encryption

Entreprise de Chiffrement au niveau des colonnes utilise Key Management Framework et permet la gestion adéquate du cycle de vie des clés en vue de personnaliser et de gérer les spécifications granulaires à chiffrer et à déchiffrer sur votre instance. Vous devez acheter un abonnement à Entreprise de Chiffrement au niveau des colonnes, mais Key Management Framework est disponible par défaut pour toutes les instances.

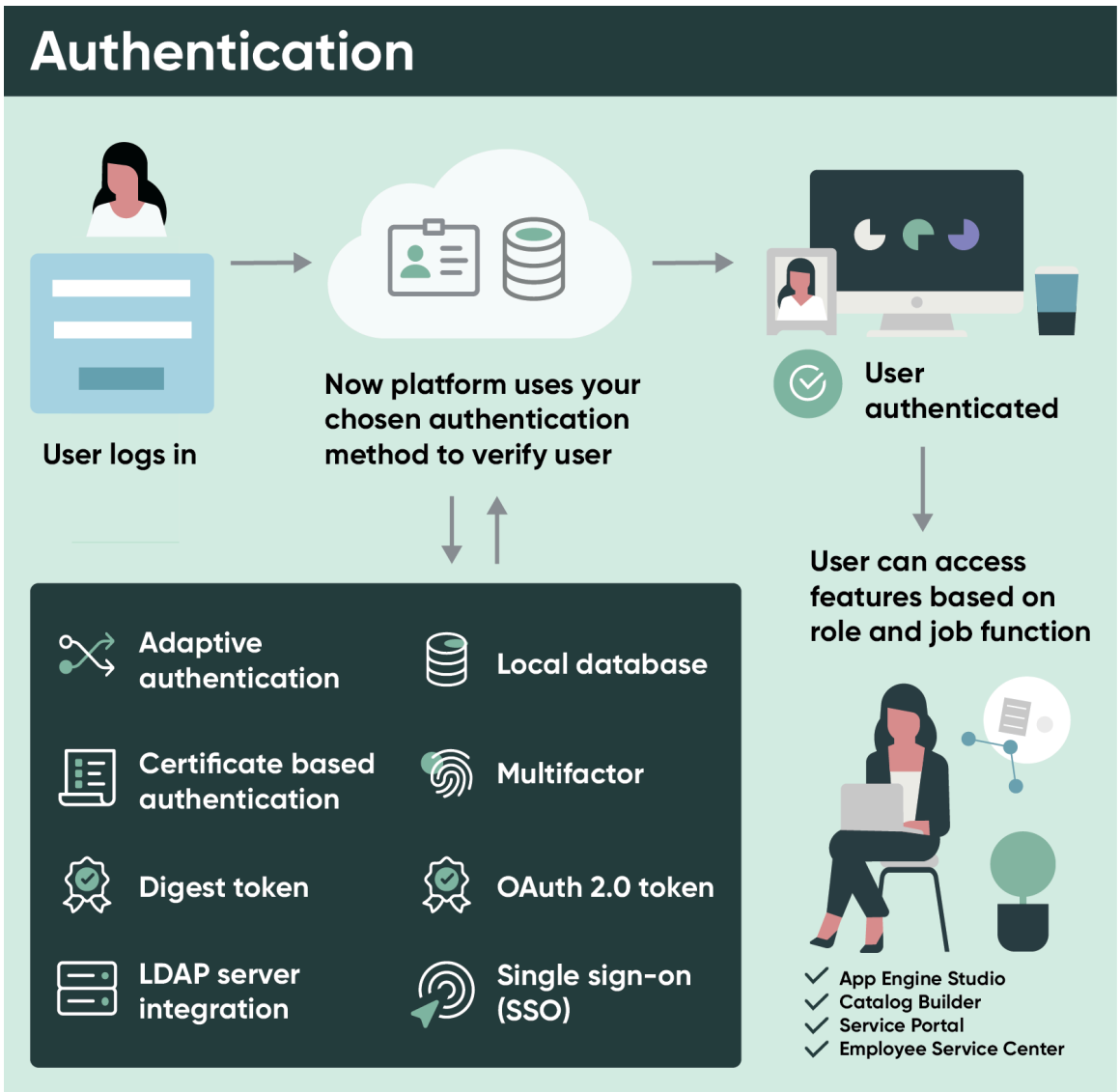
Chiffrer les données en cours à l'aide d'Edge Encryption

Chiffrement Edge chiffre les données sensibles dans les locaux de votre entreprise avant de les envoyer par Internet à votre instance (chiffrement en vol), où elles resteront chiffrées au repos. Edge utilise une technologie nommée « chiffrement côté client ». Elle exige que tout le trafic utilisateur bidirectionnel transite par des proxys gérés sur votre infrastructure.

Traduction automatique

Vous avez le contrôle total sur la gestion de vos clés, car les clés sont stockées dans votre proxy sur votre infrastructure.

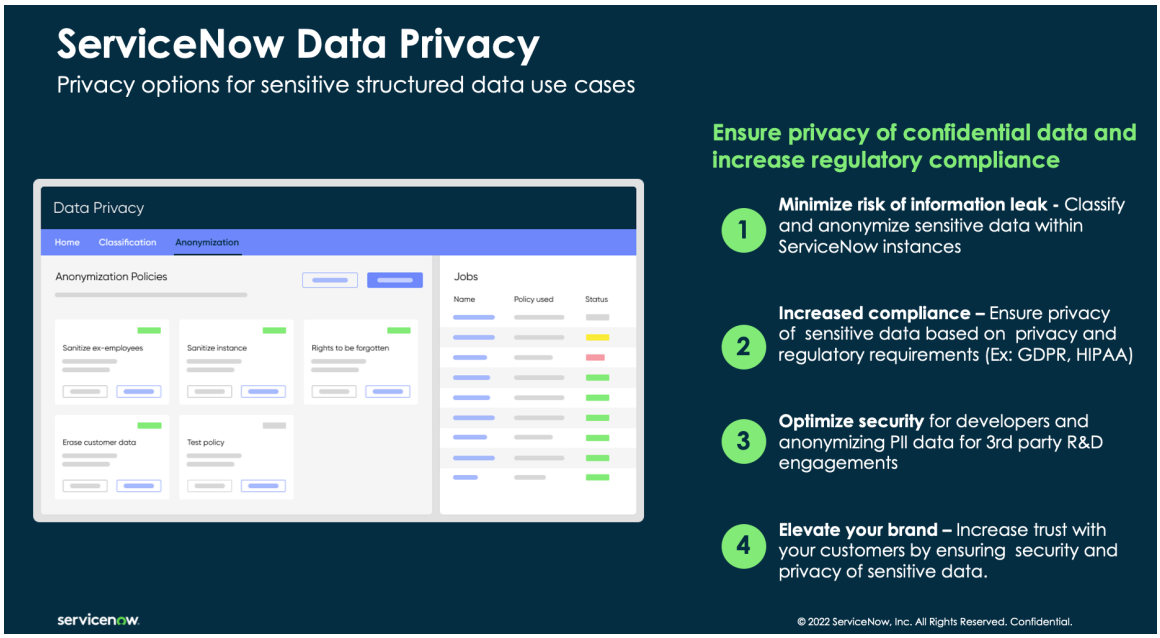
Sécuriser l'accès à votre instance



Choisissez le type d'authentification qui répond aux besoins de votre entreprise. Vous pouvez authentifier les utilisateurs, activer l'authentification unique, autoriser les clients Web à accéder à votre instance, etc.

Traduction automatique

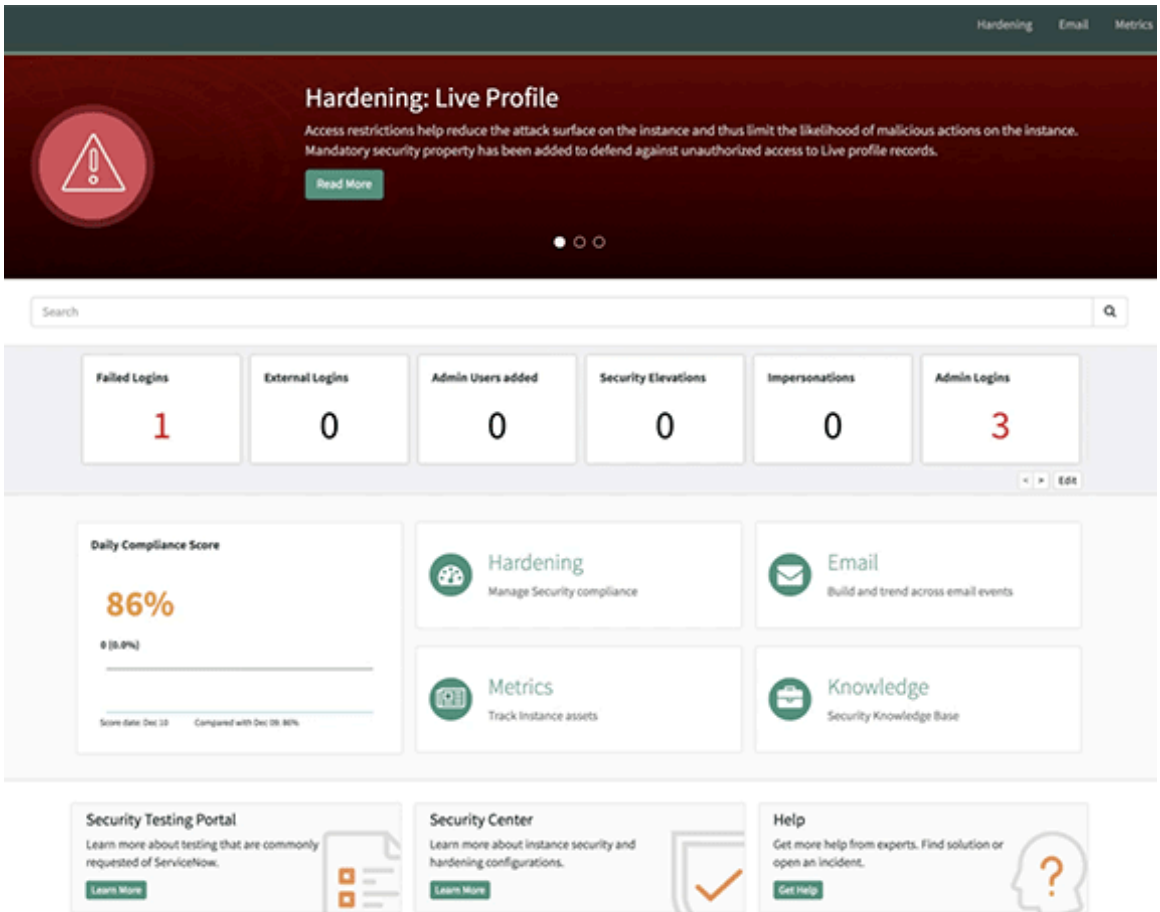
Anonymiser les informations à caractère personnel (PII)



Utilisez Data Privacy pour 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. Vérifiez que vos données utilisateur ne sont plus considérées comme informations privées réglementées.

Traduction automatique

Répondre rapidement aux risques



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 depuis Instance Security Center. Instance Security Center consolide divers composants de sécurité clés en une console de contrôle unique pour vous aider à détecter, protéger et répondre aux événements de sécurité basés sur l'instance.

Produits

- Règles des listes de contrôles d'accès
- Antivirus Scanning
- Audit
- Authentification
- Certificats
- Connexions et informations d'identification
- Classification des données
- Filtration des données
- Confidentialité des données
- Domain Separation pour les fournisseurs de services
- Gestion et chiffrement des clés

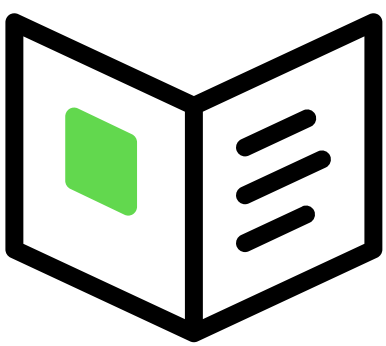
- Rôles explicites
- Identité
- Centre de sécurité de l'instance
- Paramètres de la sécurisation pour la sécurité de l'instance
- Vault
- VPN (Virtual Private Network)

Traduction automatique

Sécurité de la plateforme

Platform Security fournit des options pour sécuriser l'instance.

Certificats



Utilisez des certificats pour établir des connexions sécurisées et valider les signatures.

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.

Rôles de sécurité

Les rôles de sécurité fournissent une sécurité supplémentaire, chaque utilisateur doit avoir au moins un rôle afin que l'instance puisse faire la distinction entre les utilisateurs internes et externes.

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.

ServiceNow Vault

Centre de sécurité

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

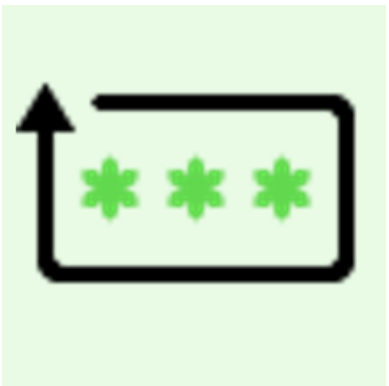
Traduction automatique

Utilisez les outils de sécurité des données du produit ServiceNow Vault pour protéger les informations sensibles contre tout accès non autorisé, endommagement ou vol tout au long de leur cycle de vie.

Gestion et chiffrement des clés

Le chiffrement est une procédure cryptographique qui convertit le texte brut en texte chiffré pour contrôler la divulgation d'informations.

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.

Certificats

Les certificats sont utilisés pour des fonctionnalités telles que LDAPS, l'authentification réciproque des services Web sortants, le service de sécurité Web et MID Server afin d'établir des connexions sécurisées et de valider les signatures.

Signature de code

La signature de code permet d'améliorer la sécurité en validant les scripts et les données de configuration d'application sensibles 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. La signature de code est un module sous licence de ServiceNow Vault.

Rôles de sécurité

Les rôles de sécurité fournissent une sécurité supplémentaire, chaque utilisateur doit avoir au moins un rôle afin que l'instance puisse faire la distinction entre les utilisateurs internes et externes.

Gestion et chiffrement des clés

Le chiffrement est une procédure cryptographique qui convertit le texte brut en texte chiffré pour contrôler la divulgation d'informations.

Centre de sécurité

Security Center permet aux administrateurs de maintenir en permanence le niveau de posture de sécurité le plus élevé et de surveiller facilement les événements et les comportements non sécurisés.

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

ServiceNow Secrets Management fournit une gestion granulaire de l'accès à vos mots de passe pour répondre aux besoins de votre entreprise.

ServiceNow Vault

ServiceNow Vault Le produit permet de définir des outils de sécurité des données qui protègent les informations sensibles contre tout accès non autorisé, corruption ou vol tout au long de leur cycle de vie. Appliquez des protections telles que le chiffrement, la gestion des secrets et la confidentialité des données pour la rédaction et l'audit des informations sensibles.

Certificats

Votre instance a besoin de certificats pour établir des connexions sécurisées et valider les signatures.

Explorer

Configurer

Traduction automatique

Découvrez les principales fonctionnalités et la valeur commerciale des certificats.	Planifiez vos configurations principales.
Charger  Planifiez et configurez l’application.	

Exploration des certificats

Votre instance a besoin de certificats pour établir des connexions sécurisées et valider les signatures.

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 ou le client sécurisé et le charger dans 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	N’importe quel type pris en charge	Toutes les configurations LDAP

Certificat	Type	Requis pour
Certificat client LDAP	Type de magasin de clés 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 exige que le client présente un certificat en plus du serveur. Si votre serveur LDAP nécessite une authentification réciproque, vous devez également fournir le certificat client de votre serveur LDAP dans un certificat de type keystore Java.

Critères de certification

Un certificat valide doit répondre aux critères suivants :

- Le certificat peut avoir une taille de clé allant jusqu'à 2 048 bits.
- Le certificat doit avoir l'une des extensions de fichier suivantes :

Extension	Description
DER	Le format *Distinguished Encoding Rules* est une syntaxe de transfert de messages binaires. Ce format prend également en charge le fichier . CER et . Extensions de fichiers CRT.
CER	Extensions de fichier de certificat pour les certificats utilisant le format Distinguished Encoding Rules.
CRT	Extensions de fichier de certificat pour les certificats utilisant le format Distinguished Encoding Rules.
PEM	Le format *Privacy Enhanced Mail* est un certificat DER codé en base 64 placé entre des chaînes de texte « -----BEGIN CERTIFICATE----- » et « -----END CERTIFICATE----- ».

Certificat de confiance

Par défaut, votre instance fait confiance uniquement aux certificats issus d'une autorité de certification (CA) reconnue dans la machine virtuelle Java (JVM). Les certificats autosignés ou signés par l'entreprise ne sont pas fiables.

Remarque :
Pour en savoir plus sur les propriétés qui affectent l'utilisation des certificats, consultez Communications sécurisées les 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. Le résultat final 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 autosigné.

   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. Convertissez 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
   ```

4. Chargez le certificat dans le fichier du magasin de clés (`test1.jks`) vers 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 un message d'erreur indiquant « Aucun certificat valide trouvé pour traiter le chargement 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

Pour plus d'informations sur la génération de clés et de CSR, consultez la documentation de l'outil de clé Java .

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* (CA) racine ou intermédiaire 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 signataire de 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.

   ```
   keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
   ```

5. Chargez le certificat dans le fichier keystore (my.keystore) vers 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

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 sur l'instance.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Certificats**.
2. Cliquez sur **Nouveau**.
3. Sur le formulaire, renseignez les champs.

4. Cliquez sur **Envoyer**.

   Pendant le 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. Cliquez sur **Valider les magasins/certificats** pour vérifier si le certificat est correct.
   Si l'instance rencontre des erreurs avec le certificat ou le magasin de clés, un message d'erreur s'affiche.

Chargement d'un certificat de serveur de confiance

En téléchargeant le certificat de serveur approuvé du fournisseur de services, 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.

Procédure

1. Créez un enregistrement de certificat de type **Certificat de magasin de confiance**.
2. Effectuez l'une des actions suivantes :
   - Joignez le certificat au format DER du fournisseur de service.
   - Copiez et collez le certificat au format PEM du fournisseur de services dans le champ **Certificat PEM** .

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 de ServiceNow Vault.

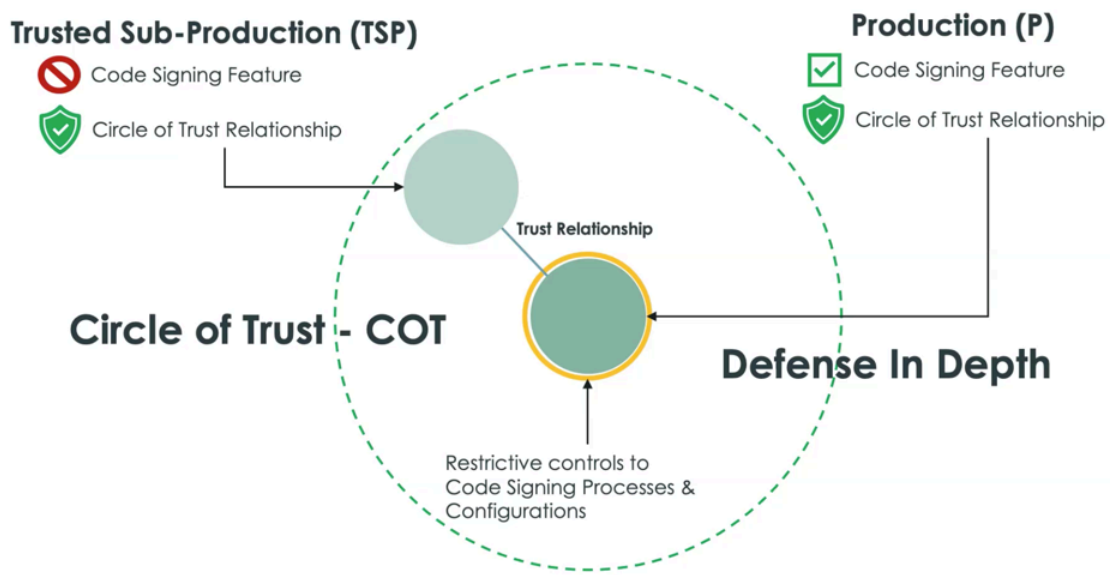
Signature de code et cercle de confiance

Le Circle of Trust (COT) est un prérequis pour la signature de code qui crée une communication sécurisée entre vos instances de confiance et vos instances de production afin de s'assurer que seuls les utilisateurs autorisés peuvent accéder à la fonctionnalité de signature de code.

De multiples mesures de sécurité permettent d'empêcher les acteurs malveillants de désactiver ou d'utiliser à mauvais escient la signature de code dans le cas où une instance de production serait compromise. Dans le cadre de la stratégie de défense en profondeur, le utilise COT les éléments suivants :

- Des contrôles qui restreignent même les comptes administrateur les plus puissants sont établis dans l'instance de production pour aider à protéger les processus et la configuration de signature de code.
- Les instances approuvées (TSP) doivent collaborer avec les instances de production afin d'établir la Circle of Trust relation. Au moins une instance de confiance est requise, mais plusieurs instances TSP peuvent être configurées pour collaborer avec l'instance de production.

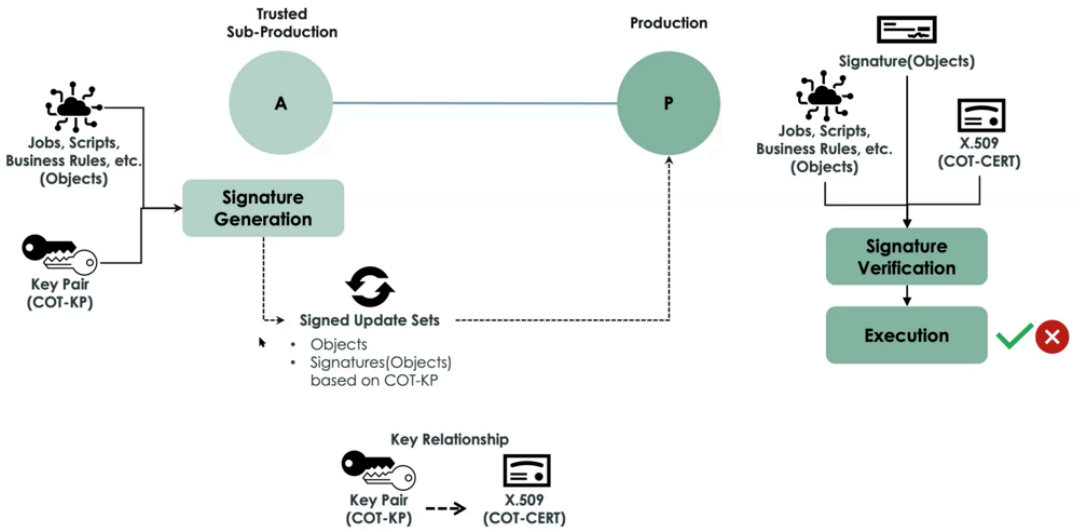
Vue d'ensemble du cercle de confiance



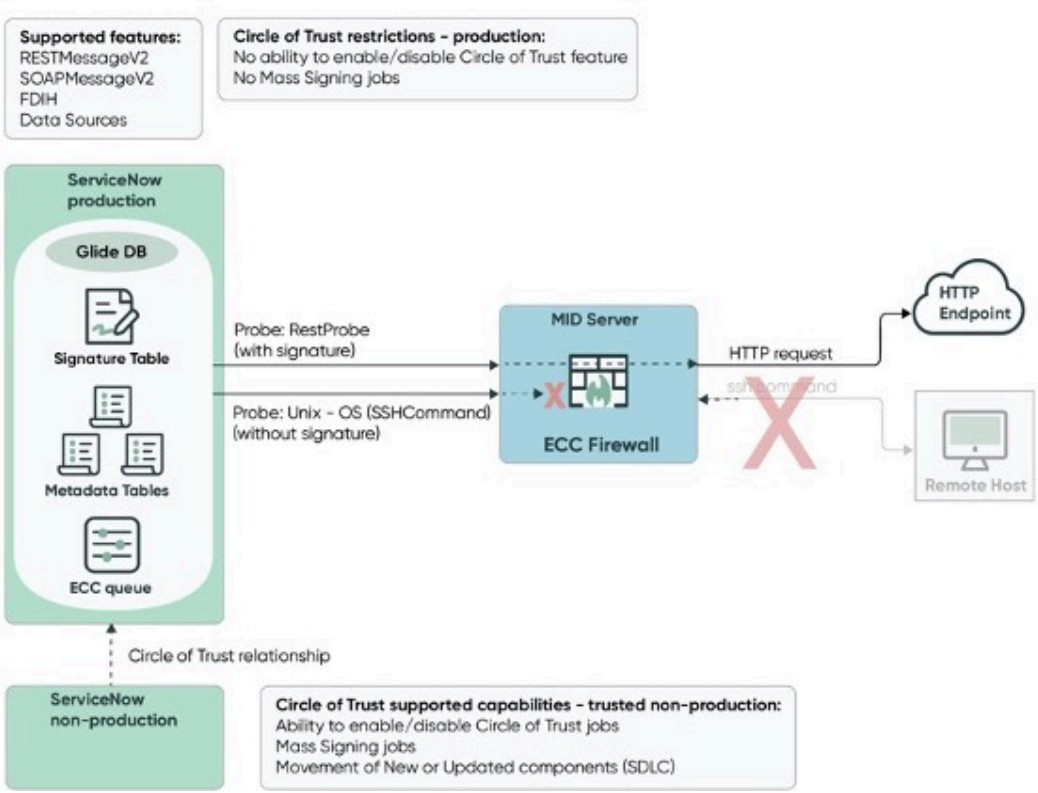
Le recours utilise Circle of Trust des tâches, des scripts et des règles métier, ainsi qu'une paire de clés, pour générer des signatures et signer des ensembles de mises à jour vers l'instance de production. Lorsque la tâche est appelée, la signature et le certificat approuvé sont vérifiés pour exécuter les mises à jour de l'instance de production.

Traduction automatique

Processus d'ensembles de mises à jour approuvés



Flux de signature de code

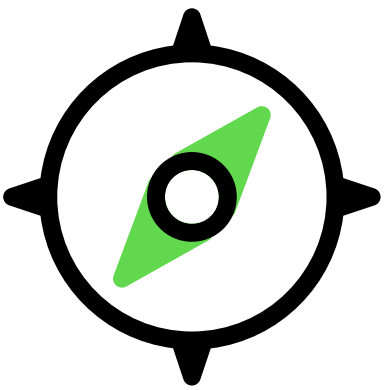


Cela Circle of Trust nécessite une relation de confiance initiale entre les instances approuvées et les instances de production qui empêche tout utilisateur non autorisé, quel que soit son niveau d'autorisation, d'accéder à des activités non approuvées.

Traduction automatique

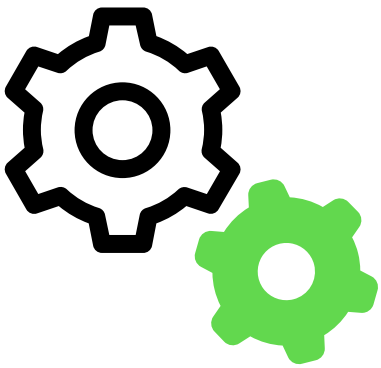
Premiers pas

Explorer



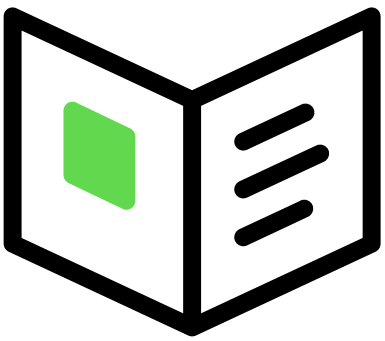
Découvrez les principales fonctionnalités et la valeur commerciale de la signature de code.

Configurer



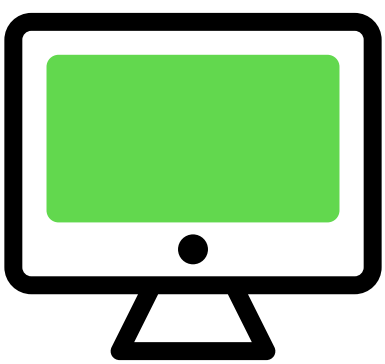
Activez et configurez la signature de code.

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 et assistance client

Traduction automatique

Explorer la signature de code

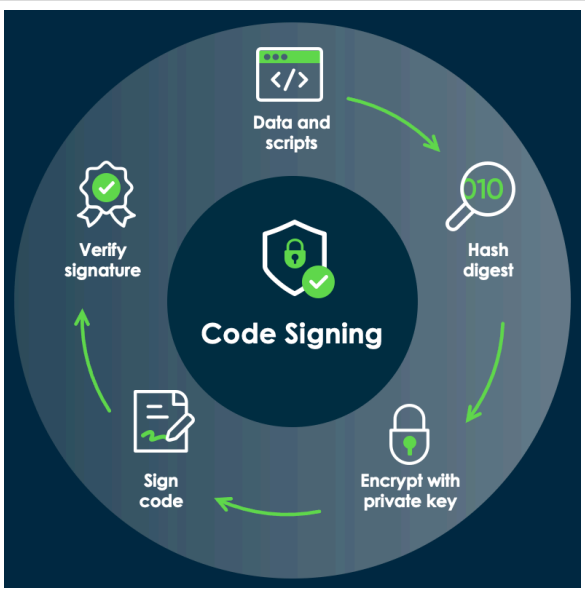
La signature de code peut contribuer à améliorer la sécurité en validant les données et les scripts de configuration d'application sensibles avant leur utilisation.

La signature de code crée des signatures numériques pour les données, qui sont vérifiées ultérieurement pour confirmer l'authenticité et l'intégrité des données. La signature de code est un module sous licence de ServiceNow Vault.

Remarque :
L'équipe Service et assistance client 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 Key Management Framework (KMF) utilise des certificats numériques et un 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 (COT) sécurisé Circle of Trust entre vos instances de confiance et de production pour s'assurer que seules les instances autorisées et sécurisées peuvent accéder à la fonctionnalité de signature de code.

Cas d'utilisation

La signature de code peut être utilisée pour les opérations avec le et Hub d'intégration.Serveur MID La notarisation est l'utilisation de la signature de code pour créer des signatures numériques pour les enregistrements de file d'attente ECC utilisés dans les opérations de Serveur MID et les opérations du concentrateur d'intégration.

Par exemple, un script include écrit par ServiceNow pour créer des enregistrements de file d'attente ECC lors de l'exécution est signé comme « contenu du système de base ». Il est signé comme « correctement émis par l'instance ServiceNow », par opposition à une insertion dans la file d'attente ECC à partir d'un script d'arrière-plan ou d'une autre origine qui n'est pas validée et signée.

Hub d'intégration peut utiliser la signature de code pour signer du contenu dynamique généré sur la plateforme et valider les parties critiques des données de l'application.

Traduction automatique

Conseil :

Les horodatages garantissent que les enregistrements signés n'expirent pas lorsque le certificat expire, à condition que l'enregistrement ait été signé avant l'expiration du certificat. Une période de grâce de 4 heures autour de la fenêtre de validité du certificat existe pour garantir que les différences de temps entre les serveurs n'invalident pas intentionnellement les certificats.

Validation et tâches de signature de code

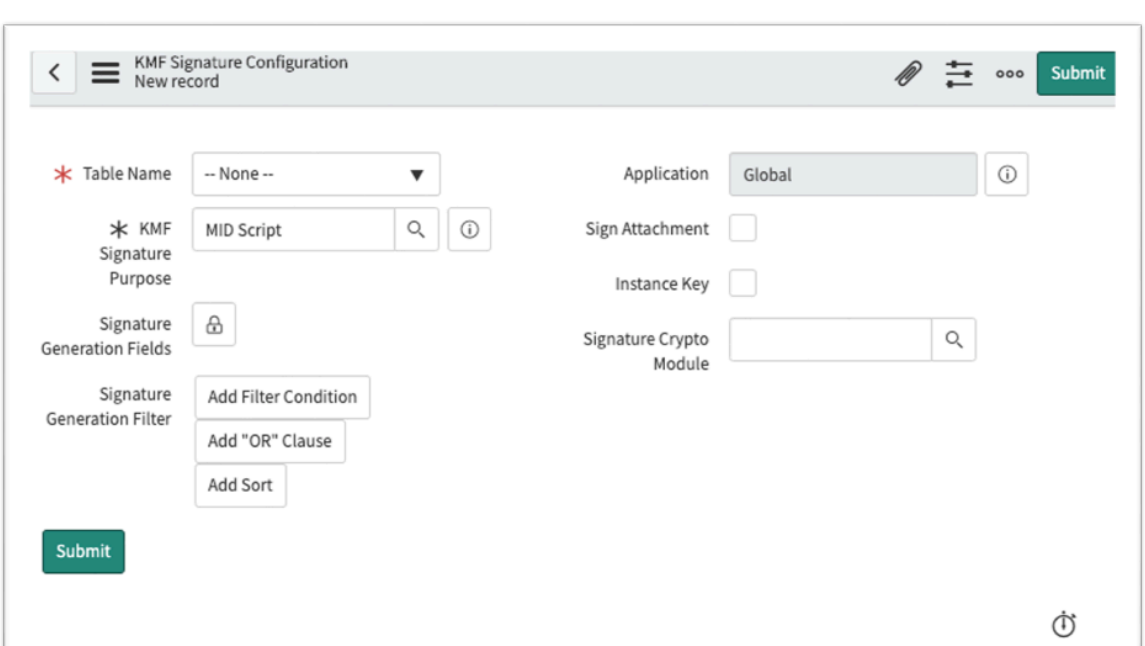
Toutes les tables de métadonnées avec des configurations valides sont signées au moment de la génération à l'aide du module d'extension de métadonnées de signature de code (`com.glide.code_signing`). Si vous choisissez de signer des tables, les utilisateurs administrateurs ayant le rôle d'administrateur de sécurité ont accès aux tâches de chiffrement de signature de code :

- Signez les ensembles de mises à jour.
- Enregistrements de signes en masse.
- Signez en masse les 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 signature et les certificats de vérification à l'ensemble de mises à jour.

Enregistrement de signature KMF pour l'ensemble de mises à jour



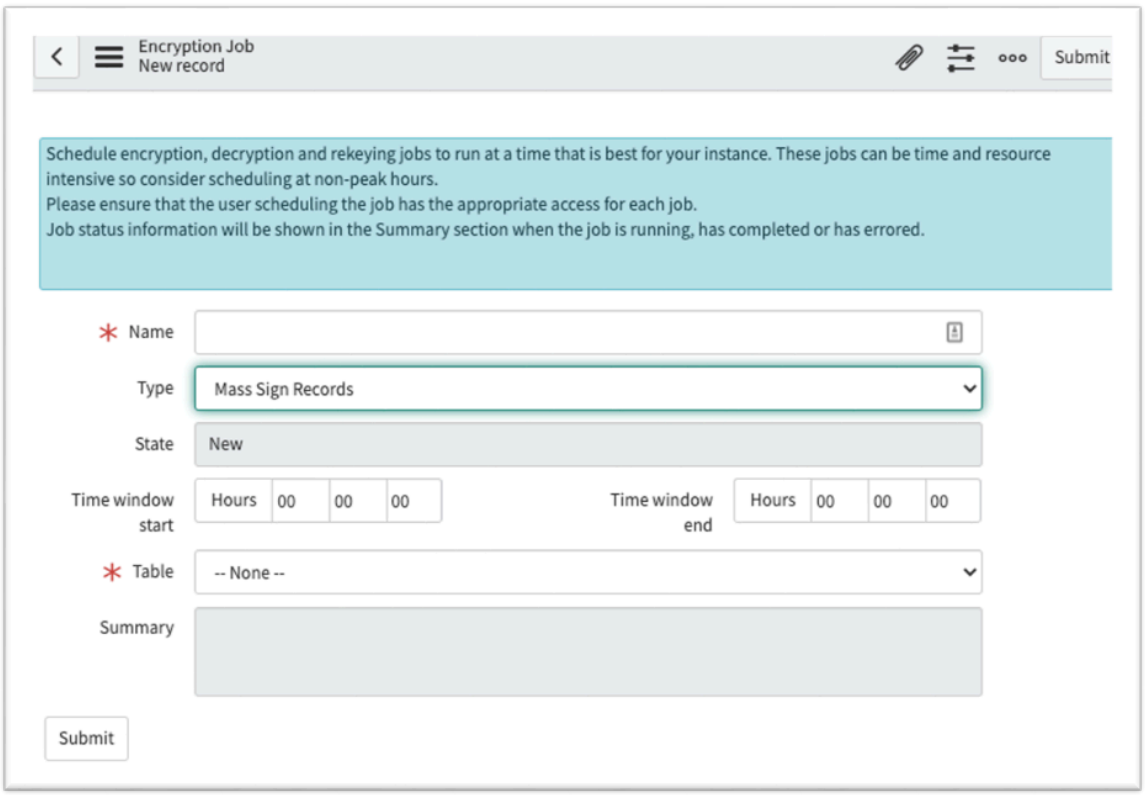
Enregistrements de signature en masse

Cette tâche signe tous les enregistrements qui correspondent à la configuration de signature appliquée sur une table de métadonnées spécifique.

Pièces jointes de signature en masse

Cette tâche signe tous les enregistrements de pièces jointes qui sont joints à une table qui correspond à une configuration de signature spécifiée.

Tâche de chiffrement pour signer en masse les enregistrements



Configuration de la signature de code

Activez et configurez la signature de code pour garantir l'authenticité et l'intégrité de vos données.

Vue d'ensemble de la configuration

La signature de code exige une relation de confiance initiale entre les instances de confiance et les instances de production qui empêche tout utilisateur non autorisé, quel que soit son niveau d'autorisation, d'accéder à des activités non approuvées.

Reportez-vous à chaque rubrique pour terminer les étapes de configuration afin d'établir l'environnement avec la Circle of Trust signature de code :

Activer la signature de code

Activez la signature de code sur votre instance approuvée pour identifier les instances approuvées qui se connectent à votre instance de production.

Créer des paires de clés et des certificats de signature de code

Créez deux paires de clés pour les certificats signés afin d'établir la confiance entre vos instances de production et les instances approuvées.

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 Circle of Trust signature de code. Cette première étape charge une clé de chiffrement dans l'environnement de non-production afin d'établir une source fiable pour les mises à jour de l'instance de production.

Préparer les certificats du cercle de confiance

Créez un ensemble de mises à jour dans l'instance approuvée pour exporter le certificat approuvé vers l'environnement de production.

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 après l'exportation de l'ensemble de mises à jour depuis l'environnement approuvé. Les certificats qui ont été créés pour représenter la confiance dans l'instance approuvée doivent être acceptés dans l'instance de production.

Spécifier des règles personnalisées dans le pare-feu ECC

Configurez le pare-feu ECC (External Communication Channel) dans votre Serveur MID pour créer des règles personnalisées qui autorisent ou rejettent les messages entrants de manière sélective et remplacent la configuration de signature de code.

Charger les paires de clés et les certificats requis pour la signature de code

Établissez la relation dans une instance de non-production désignée à l'aide de la signature de code. Cette première étape charge deux clés de chiffrement dans l'environnement de non-production afin d'établir une source fiable pour les mises à jour de l'instance de production.

Avant de commencer

Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

La première étape de l'établissement de la relation consiste à établir la fondation de confiance dans une instance de non-production désignée à l'aide de la signature de code. Pour effectuer cette tâche, vous aurez besoin des éléments suivants.

- 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 cryptographique cm_code_signing
  - Une paire pour le module cryptographique 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 signé automatiquement.

- Un fichier Public Key Cryptography Standard #12 (.p12) contenant votre certificat de distribution.

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 de chiffrement** , sélectionnez le nom de la spécification de chiffrement 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 cryptographique nommé `cm_code_attest`.
3. Dans le champ **Saisir le mot de passe du magasin de clés** , saisissez le mot de passe de demande que vous avez créé lors de la génération de votre certificat RSA.

Remarque :
Le mot de passe de demande que vous avez créé est appelé ici **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'exportation**. Dans tous les cas, ce mot de passe est le même que celui que vous avez créé lors des étapes précédentes.

4. Sélectionnez le bouton **Parcourir** en regard de **Importer un magasin de clés/certificat**.
5. Sélectionnez votre fichier p12 (mentionné dans la section Avant de commencer en haut de ce document), puis sélectionnez **Télécharger tout**.
6. Sélectionnez **OK**.

Important :
Si vous utilisez votre propre autorité de certification interne, vous devez charger les certificats intermédiaires de l'autorité de certification interne à l'aide du processus des étapes 5 et 6.

Si votre clé et vos certificats sont importés avec succès, 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].

Que faire ensuite
Exportez le certificat vers la production. Voir pour plus de détails.

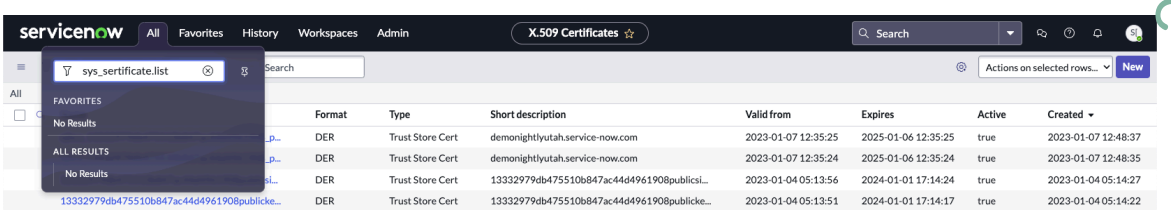
Préparer les certificats du cercle de confiance

Créez un ensemble de mises à jour dans l'environnement approuvé pour exporter le certificat approuvé vers l'environnement de production.

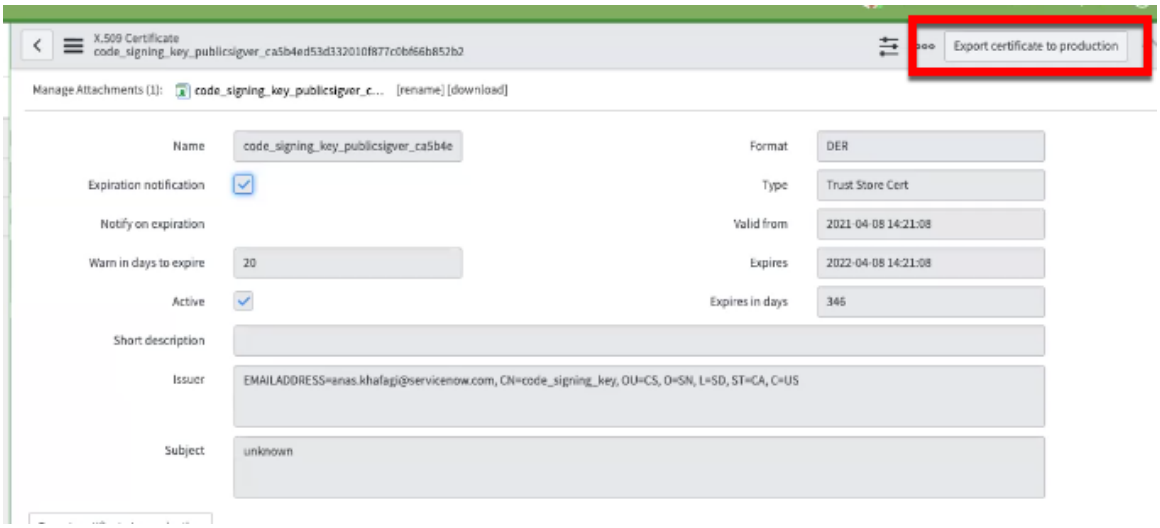
Avant de commencer
Rôles requis : admin, security_admin

Procédure

1. Dans l'environnement approuvé, accédez à **sys_certificate.list**.



2. Ouvrez le certificat X.509 le plus récemment créé et 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. Reportez-vous à la section Listes personnelles .
3. Sélectionnez **Exporter le certificat vers la production**.



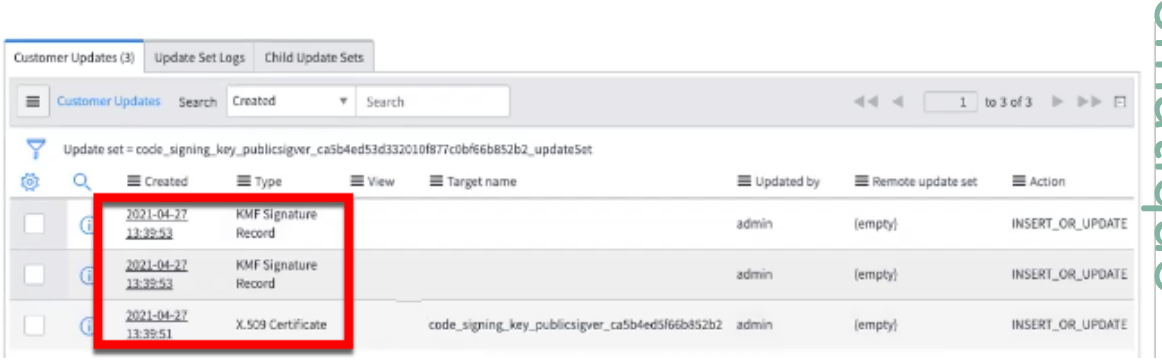
Une signature est créée en même temps que le certificat.

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.

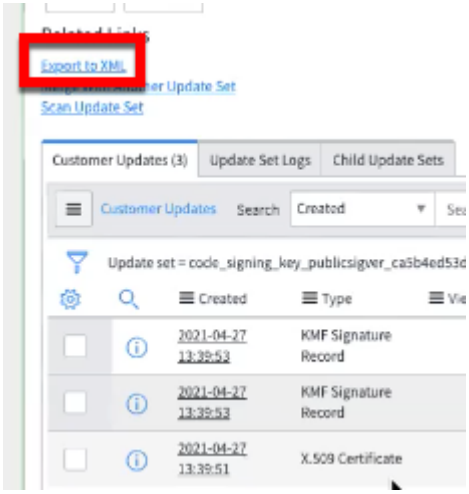
   Cette mise à jour commence par le texte `code_signing_key_publicsigver`.

   Un nouvel enregistrement d'ensemble de mises à jour de signature de code a été créé lors des 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 inclut 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 cryptographiques cm_code_attest et cm_code_signing.

Importer et installer des certificats pour le cercle de confiance

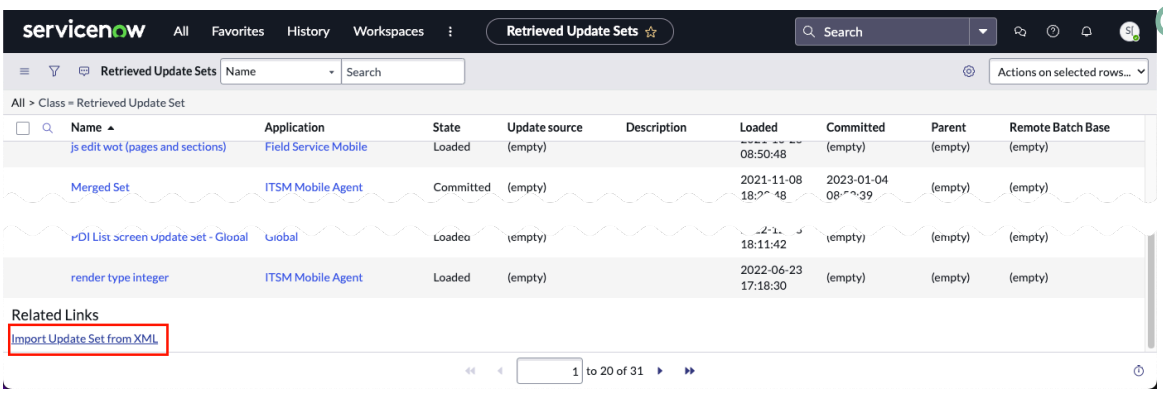
Récupérez l'ensemble de mises à jour en production pour établir la relation de confiance entre les deux instances. Les certificats qui ont été créés pour représenter la confiance dans l'instance approuvée doivent être acceptés dans l'instance de production.

Avant de commencer

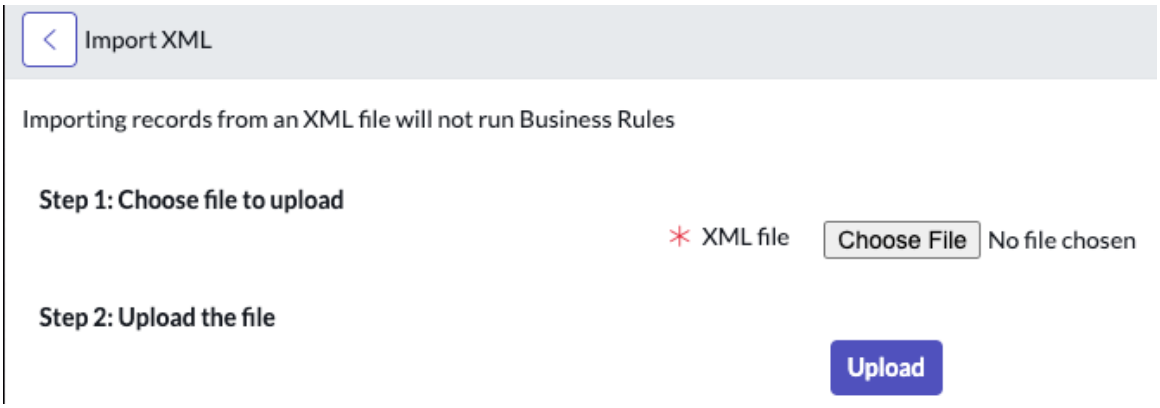
Rôles requis : admin, security_admin

Procédure

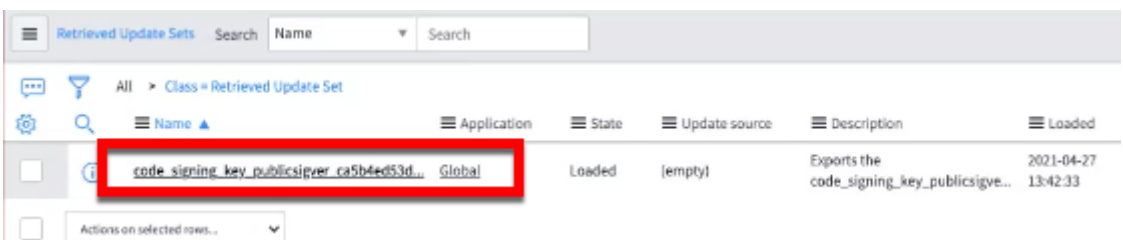
1. Dans l'instance de production, accédez à **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
2. Sélectionnez le bouton **Importer l'ensemble de mises à jour à partir d'un fichier XML** dans le coin inférieur gauche de l'écran.



3. Sélectionnez **Choisir un fichier** , puis recherchez le fichier XML que vous avez exporté au format Préparer les certificats du cercle de confiance.

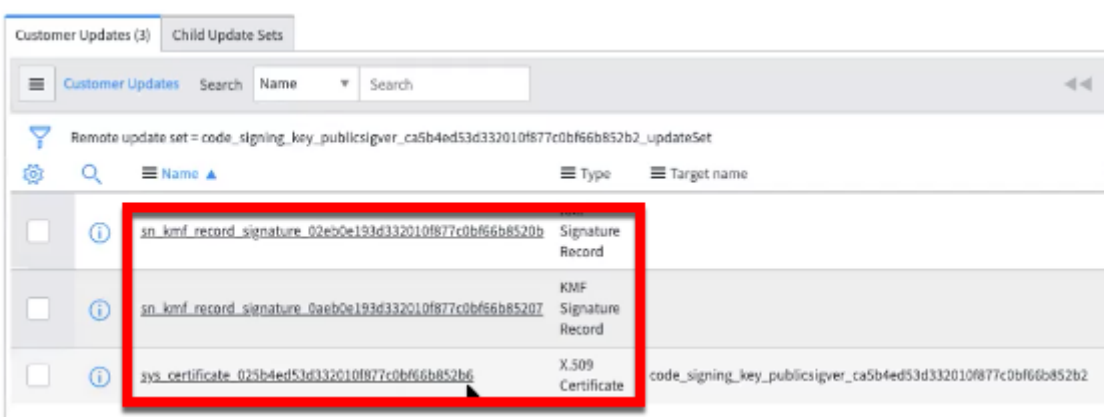


4. Sélectionnez **Charger**.
   L'ensemble de mises à jour de signature de code est ajouté à la table Ensembles de mises à jour récupérés.

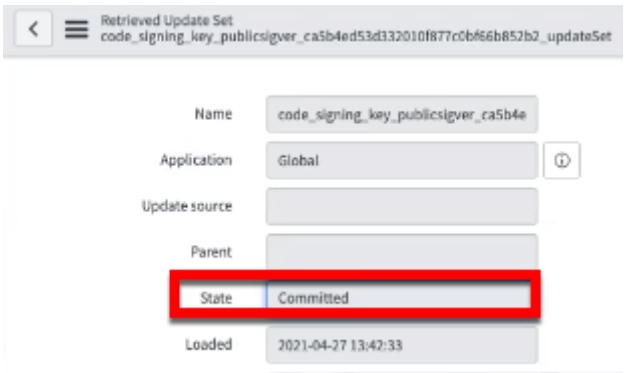


Remarque :
Si vous ne voyez pas votre ensemble de mises à jour, filtrez votre liste pour les enregistrements à l'état Chargé, puis triez la liste en fonction du champ **Chargé** .

5. Ouvrez l'enregistrement de l'ensemble de mises à jour pour vérifier que la table Mises à jour du client contient les trois enregistrements suivants :
   - Deux KMF enregistrements de signatures
   - Certificat X.509

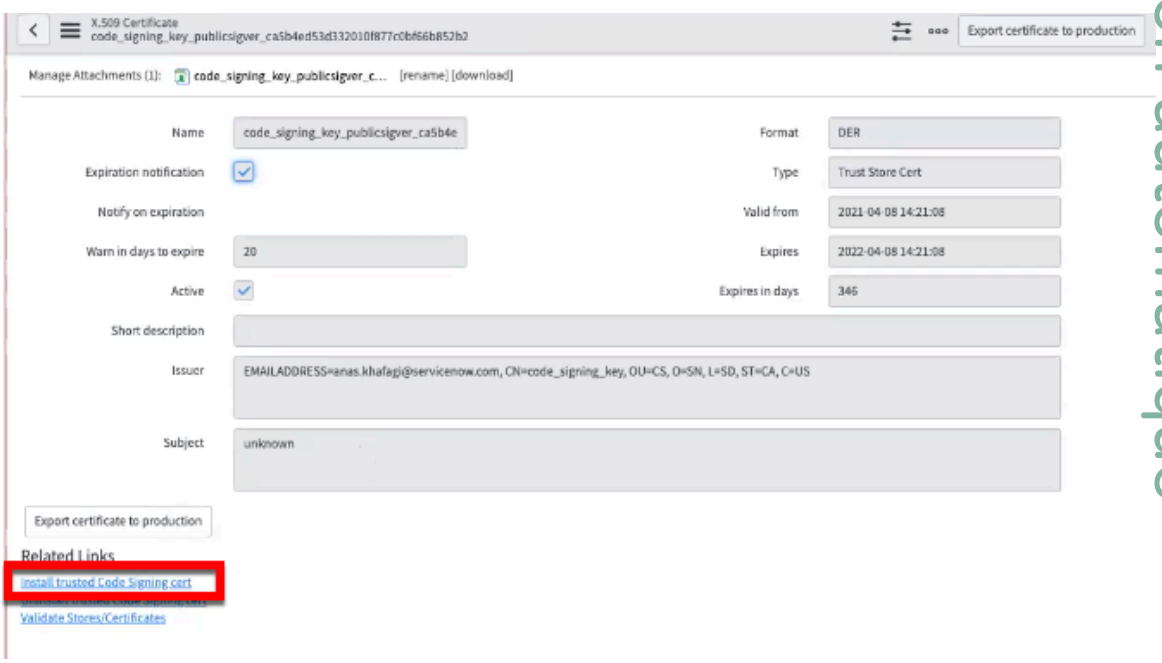


6. Sélectionnez **Aperçu de l'ensemble de mises à jour**.
7. Sélectionnez **Valider l'ensemble de mises à jour.**



L'état de l'ensemble de mises à jour récupéré passe à Validé.

8. Dans le navigateur, saisissez `sn_kmf_record_signature.list` pour ouvrir la liste des **enregistrements de signatures KMF** .
9. Localisez les deux KMF enregistrements de signature.
   Ces enregistrements sont les enregistrements les plus récemment créés où le champ **Objectif de signature KMF** a la valeur `Cercle de confiance`. Vous devrez peut-être ajouter le champ **Créé** à votre liste ou filtrer pour les enregistrements créés à la date actuelle.
10. Dans le navigateur, entrez `sys_certificate.list` et ouvrez l'enregistrement avec une valeur **Brève description** de `code_signing_key` et une valeur **Type** de Certificat de `magasin de confiance`.
11. Sélectionnez **Installer le certificat de signature de code approuvé**.



Le type de certificat est mis à jour et `devient Certificat CodeSigning approuvé`.

> **Important :**
> Répétez ces étapes pour votre deuxième certificat. N'oubliez pas qu'il existe un certificat pour les modules cryptographiques cm_code_attest et cm_code_signing.

Résultats

La relation de confiance est établie entre les instances de production et approuvées. Vous êtes prêt à activer la signature de code. Consultez Activer la signature de code 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 qui sont liées à votre instance de production.

Avant de commencer

Rôles requis : security_admin et sn_kmf.crypto_manager ou sn_kmf.admin

Avant d'activer la signature de code, vous devez contacter l'équipe Service et assistance client pour activer le module d'extension Cadre de travail de signature de code [com.glide.code_signing].

Pourquoi et quand exécuter cette tâche

Les tâches de signature de code avec des ensembles de mises à jour signés sont utilisées pour activer ou désactiver la fonctionnalité de signature de code. Il n'existe aucune autre méthode pour cette fonctionnalité. Ce processus comprend les éléments suivants :

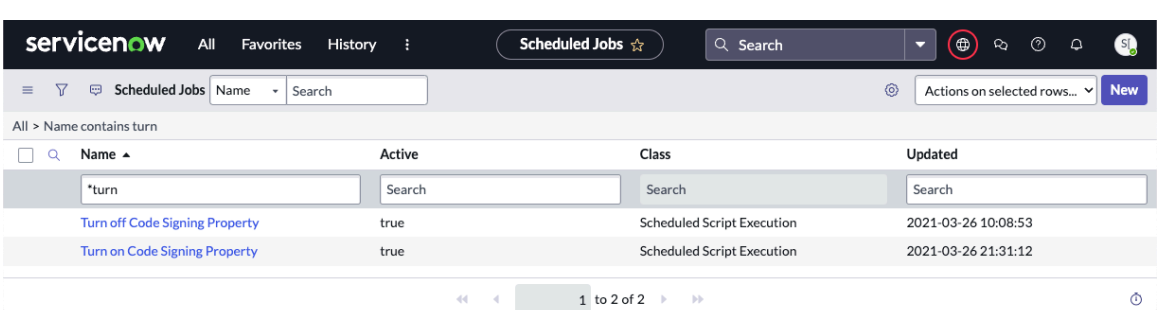
- Créez deux tâches de signature de code dans Trusted, l'une pour activer la signature de code et l'autre pour désactiver la signature de code.
  - La tâche planifiée **Activer** démarre le processus de validation du code signé par le MID Server.
  - La tâche planifiée **Désactiver** arrête la validation du code signé par le MID Server.

> **Remarque :**
> Lorsque vous désactivez la signature de code, la propriété système est marquée comme **fausse**, mais la liste d'amis de confiance de la signature de code est toujours disponible.

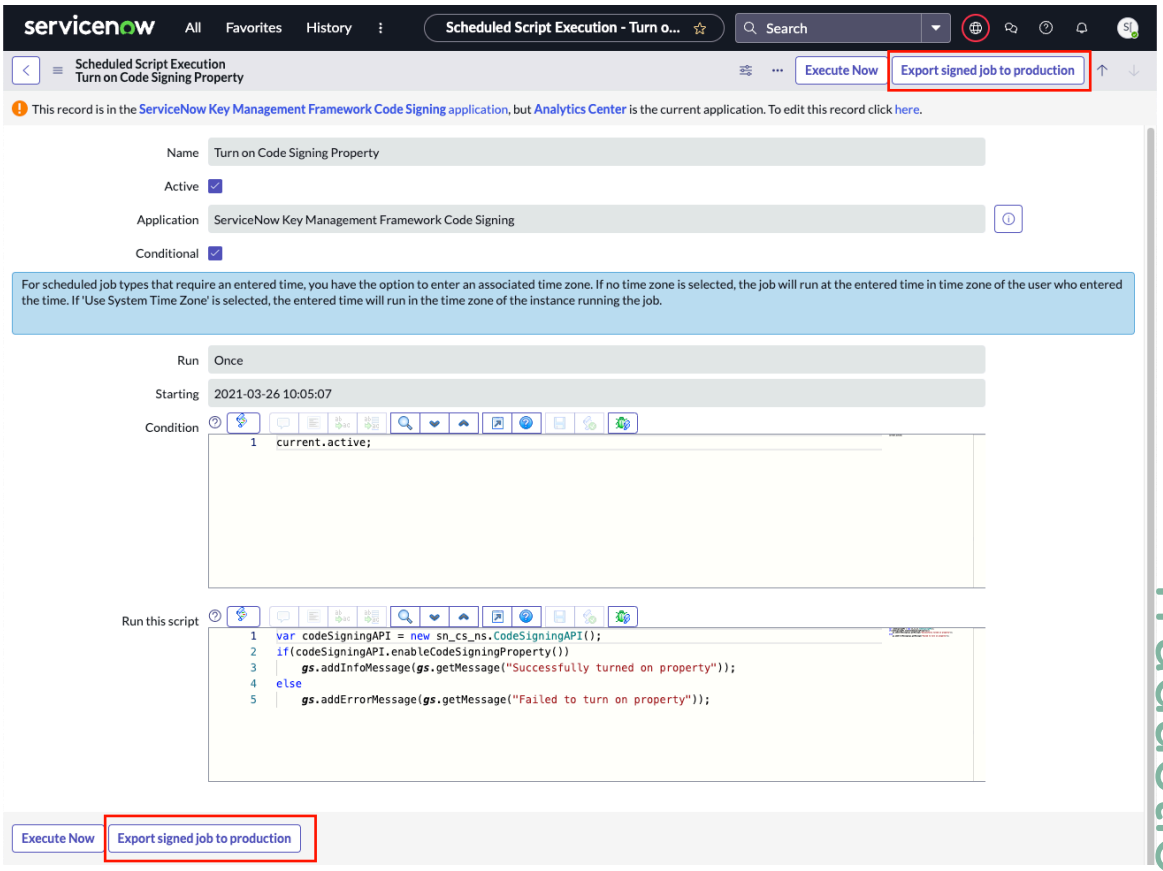
- Placer la tâche **Activer la propriété de signature de code** dans un ensemble de mises à jour.
- Mettez le travail en production.
- Utilisez la tâche **Activer la propriété de signature de code** en production si après vérification la signature provient d'une instance approuvée.

Procédure

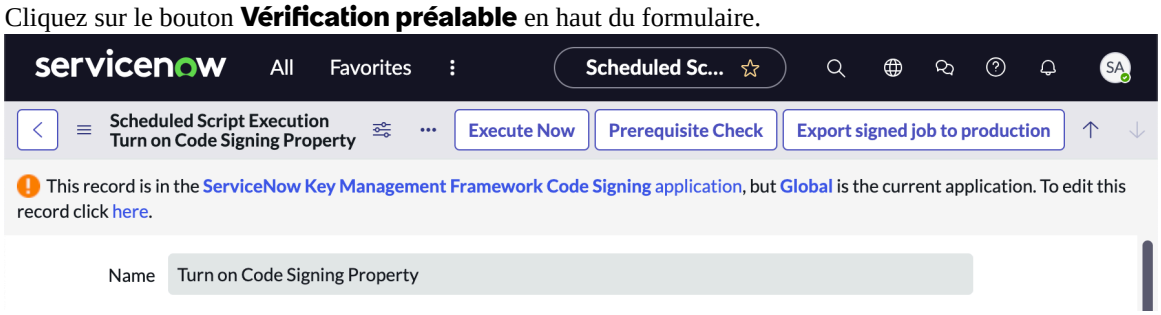
1. Dans votre instance approuvée, accédez à **Tous** > **Définition du système** > **Travaux planifiés**.
2. Recherchez « *Turn » dans le champ de nom.
3. Sélectionnez **Activer la propriété de signature de code**.



Chargement **du formulaire Exécution de script planifiée** . Ce formulaire contient des informations permettant d'activer la propriété de 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.



4. Pour exécuter immédiatement le script, signez le certificat, créez l'ensemble de mises à jour, puis sélectionnez **Exporter la tâche signée vers la production**.
   Vous pouvez également configurer le script pour qu'il s'exécute selon un calendrier désigné.
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 de signature de code et sélectionnez **Exporter vers 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 fichier XML** , puis sélectionnez l'ensemble de mises à jour de la propriété de signature de code.
10. Sélectionnez **Choisir un fichier** , puis chargez et validez les ensembles de mises à jour.
11. Revenez à la liste des tâches planifiées en accédant à **Tous** > **Définition du système** > **Travaux planifiés**.
12. Ouvrez l'enregistrement de tâche **Activer la propriété de signature de code** .
13. Cliquez sur le bouton **Vérification préalable** en haut du formulaire.



14. Cliquez sur le bouton **Exécuter maintenant** une fois la vérification des conditions préalables terminée. La tâche planifiée **Activer la propriété de signature de code** démarre le processus de validation du code signé par le MID Server.
15. Dans le navigateur, entrez `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 `Cercle de confiance`.
    La relation de confiance a déplacé les tâches et, lorsque les tâches sont utilisées, le processus de vérification de la signature s'exécute. Si les tâches, les signatures et les certificats font tous partie du , vous pouvez activer la Circle of Trustsignature de code avec Circle of Trust .
16. Dans le navigateur, saisissez `sys_properties.list` pour ouvrir la liste des propriétés système.
17. *`com_snc_kmf_signature.validation.flag`* Recherchez et 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 `Circle of Trust` tâche en production pour vérifier la relation de confiance. Aucune tâche directe qui tente de signer le code ne peut être exécutée en production. Consultez pour en savoir plus sur les options de configuration.

Créer des paires de clés et des certificats de signature de code

Créez deux paires de clés pour les certificats signés afin d'établir la confiance entre vos instances de production et les instances approuvées.

Pour établir la confiance entre vos instances, vous devez créer une paire de clés et un certificat pour chacun des modules de chiffrement `cm_code_attest` et `cm_code_signing` .

La création de paires de clés et de certificats s'effectue 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 https://www.openssl.org . Si votre organisation utilise d'autres outils cryptographiques, tels que LibreSSL ou GnuTLS, reportez-vous à la documentation de ces produits pour connaître des 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.

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 façon 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 de l'emplacement : agent/boot-config.yaml.

Ces balises sont spécifiques à un protocole. La configuration spécifiée pour la balise parent 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
SYSLOG	
WINDOWS	• CIM • POWERSHELL • WMI • WINRM
JAVASCRIPT	
GROOVY	
VCS	GIT
BASES	JDBC
DATA_SOURCES	
INTEGRATION_HUB	
ITOM	• CLOUD_PROVISIONING_GOVERNANCE • DISCOVERY • EVENT_MANAGEMENT

Balise parente	Balise enfant
	• HEALTH_LOG_ANALYTICS • SERVICE_MAPPING
ORCHESTRATION	

Pour configurer les règles personnalisées :

1. Dans le Serveur MID, identifiez le fichier boot-config-sample.yaml.
2. Renommez le fichier YAML en boot-config.yaml et déplacez le fichier à l'emplacement : agent/boot-config.yaml.
3. Dans le fichier YAML, spécifiez les règles personnalisées et enregistrez les modifications. Exemple du fichier YAML :

```
security:
  eccFirewall:
    mode: enforcing
    rules:
      - tags: [rest]
        action: accept
      - tags: [soap]
        action: accept
      - tags: [jdbc]
        action: reject
```

4. Redémarrez le Serveur MIDfichier .

Changer la configuration de votre racine de confiance

Faites confiance à vos propres certificats et utilisez-les au lieu de vous appuyer sur ServiceNow des certificats de version (par défaut) en changeant pour utiliser votre racine de confiance (ROT). ServiceNow Les composants tels que les script includes, les règles métier, entre autres, sont signés au moment de la version à l'aide d'une ServiceNow clé au moment de la version (le certificat de vérification correspond au certificat de ServiceNow version).

Changer la racine de confiance

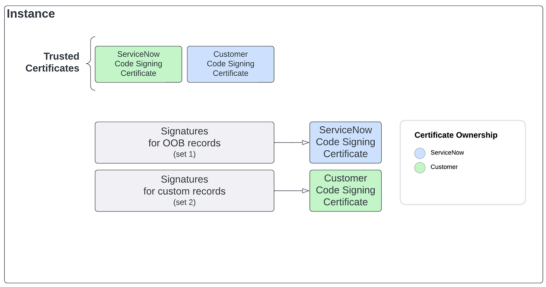
Pour modifier la racine de confiance pour ces signatures d'enregistrements, vous devez suivre le processus de changement de racine de confiance.

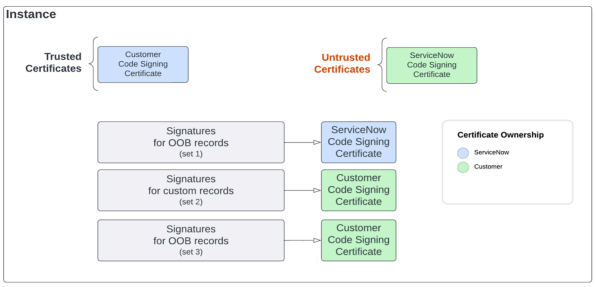
- Générez et migrez un nouvel ensemble de signatures pour tous les composants fournis, à l'aide de votre certificat fourni.
- Désactivez la propriété racine de confiance à l'aide d'une tâche planifiée.

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 vérification et de génération de signature

Par défaut, les certificats de version de signature de code sont approuvés pendant le processus de vérification de la signature. Une fois cette modification effectuée, votre instance accepte uniquement les signatures provenant de votre propre certificat de signature de code.





Propriété ROT définie sur faux (par défaut)	Propriété ROT définie sur vrai
• Lors de la vérification, les signatures avec les 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 les certificats de version de signature de code ainsi que d'autres certificats présents sur l'instance.	• Lors de la vérification, les signatures avec les certificats de construction ne sont pas fiables. • Lors de la signature, si vous ne fournissez pas les clés, la signature n'est pas effectuée. • Le point *api/sn_kmf/signature/certificates* de terminaison REST de signature exclut les ServiceNow certificats de build (San Diego, Vancouver PKI, W PKI).

Impact sur votre MID Server

Lorsque la propriété ROT est définie sur false

Si vous choisissez de conserver la valeur par défaut de votre propriété ROT (faux), cela n'a aucun impact sur votre MID Server.

Lorsque la signature de code est activée et que la propriété ROT est définie sur true

- L'API *isTrusted()* renvoie la valeur false pour les signatures avec un certificat de build.
- L'API *isTrusted()* renvoie la valeur true pour les signatures accompagnant votre certificat.
- L'appel d'API REST pour les certificats exclut les certificats de version.
- Des problèmes de MID Server tels que des messages d'échec de validation de signature peuvent s'afficher 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 de production et approuvées. Pour le vérifier, assurez-vous que la propriété système **com.snc.kmf.signature.validation.flag** est définie sur vrai.

Cette procédure fait partie d'une série de procédures visant à modifier une racine de confiance client (ROT) sur vos instances. Pour obtenir une vue d'ensemble de ce processus, reportez-vous à la section Changer la configuration de votre racine de confiance.

Procédure

1. Connectez-vous à votre instance de production.
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 des signatures à l'aide d'un certificat client** .
4. Au bas du formulaire, sélectionnez **Exécuter maintenant**.
5. Accédez à la **Tous** > **Sécurité de système** > **Tâches de Security** > **Créer**.
6. À l'invite, sélectionnez **Tâche de signature**.
7. Dans le formulaire **de tâche de signature** , renseignez les champs comme il convient.

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. L'ensemble de mises à jour a un nom qui commence par change_root_of_trust_updateSet.

8. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer** pour sauvegarder l'enregistrement.
9. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis 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 Security** > **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 lors des étapes précédentes.
14. Sélectionnez **Charger**.
15. Dans 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 de production.

> **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.

19. Sélectionnez **Exporter XML** pour exporter votre ensemble de mises à jour sous forme de fichier XML.
20. Connectez-vous à votre instance de production.
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 d'un fichier XML**.
23. Dans le formulaire **Importer XML** , sélectionnez **Choisir un fichier** et sélectionnez le fichier XML que vous avez téléchargé lors des 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 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 Security** > **Tous**.
29. Ouvrez la tâche de sécurité importée.
30. Sélectionnez **Démarrer** pour exécuter la tâche de sécurité.

    Une fois la tâche de sécurité terminée, des informations relatives à l'état de la tâche apparaissent 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 dans la table Enregistrements de signatures KMF [sn_kmf_record_signature].

Que faire ensuite

Pour poursuivre le processus de configuration de la racine de confiance, reportez-vous à Désactiver la racine de confiance ServiceNow.

Désactiver la racine de confiance ServiceNow

Exécutez une tâche planifiée sur votre instance de non-production approuvée 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 de production et approuvées. Pour le vérifier, assurez-vous que la propriété système **com.snc.kmf.signature.validation.flag** est définie sur vrai.

Cette procédure fait partie d'une série de procédures pour passer à une racine de confiance client (ROT) sur vos instances. Pour obtenir une vue d'ensemble de ce processus, reportez-vous à la section Changer la configuration de votre 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**.

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 de production.
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 d'un fichier XML**.
11. Dans le formulaire **Importer XML** , sélectionnez **Choisir un fichier** et sélectionnez le fichier XML que vous avez téléchargé lors des 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 de la tâche planifiée définit la propriété ROT sur true. Votre instance est configurée pour utiliser la racine de confiance du client.

Désactiver la signature de code

Désactivez la signature de code dans votre instance approuvée de non-production pour identifier les instances approuvées qui sont liées à votre instance de production.

Avant de commencer

Rôles requis : security_admin et sn_kmf.crypto_manager ou sn_kmf.admin

Pourquoi et quand exécuter cette tâche

Les tâches de signature de code avec des ensembles de mises à jour signés sont utilisées pour activer et désactiver la fonctionnalité de signature de code. Il n'existe aucune autre méthode pour cette fonctionnalité. Ce processus comprend les éléments suivants :

- Créez deux tâches de signature de code dans votre instance de confiance : l'une pour activer la signature de code et l'autre pour désactiver la signature de code.

  Remarque :
  Lorsque vous désactivez la signature de code, la propriété système est définie sur **faux**, mais la liste d'amis de confiance pour la signature de code est toujours disponible.

- Placez la tâche **Désactiver la propriété de signature de code** dans un ensemble de mises à jour.
- Mettez le travail en production.
- Utilisez la tâche en production si après vérification la signature provient d'une instance approuvée.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Travaux planifiés**.
2. Recherchez « *Turn » dans le champ de nom.

> **Important :**
> Deux tâches sont répertoriées dans la table **Activer la propriété de signature de code** et **Désactiver la propriété de signature de code**. Effectuez cette procédure sur chacune de ces tâches.

3. Sélectionnez **Désactiver la propriété de signature de code**.
   Le formulaire Exécution de script planifiée se charge et contient des informations permettant de désactiver la propriété de 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.
4. Pour exécuter immédiatement le script, signez le certificat, créez l'ensemble de mises à jour, puis sélectionnez **Exporter la tâche signée vers la production**.
   Vous pouvez également configurer le script pour qu'il s'exécute selon un calendrier désigné.
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 de signature de code et sélectionnez **Exporter vers 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 **Importer l'ensemble de mises à jour à partir d'un fichier XML** et sélectionnez l'ensemble de mises à jour de la propriété de signature de code.
10. Sélectionnez **Choisir un fichier** , puis chargez et validez les ensembles de mises à jour.
11. Sélectionnez chacun des ensembles de mises à jour, puis sélectionnez **Exécuter maintenant**.
12. Accédez à la **Enregistrements de signatures KMF** > **Tous** et recherchez l'objectif KMF de signature de Circle of Trust.
    La relation de confiance a déplacé les tâches et, lorsque les tâches sont utilisées, le processus de vérification de la signature s'exécute. Si les tâches, les signatures et les certificats font tous partie du , vous pouvez désactiver la Circle of Trustsignature de code avec Circle of Trust .
13. Accédez à la **Propriétés système** > **Tous.**
14. `com_snc_kmf_signature.validation.flag` Recherchez et assurez-vous que la valeur est définie sur **vrai**.
15. Vérifiez qu'une nouvelle propriété `com_snc_kmf_signature.validation.certificate` est répertoriée dans la table.

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 de production

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 de production et approuvées.

Signez 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 de production et approuvées.

Signer les flux, les flux secondaires et les actions dans l'instance de production

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 de production et approuvées.

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

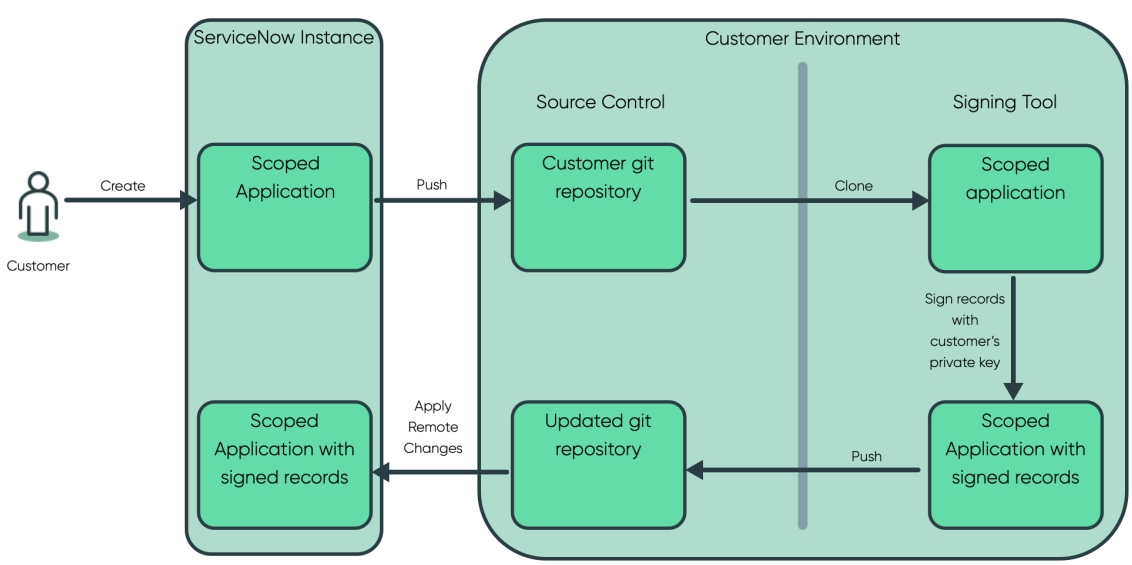
Utilisez l'outil de signature autonome pour signer les enregistrements pris en charge dans ServiceNow les applications à l'aide de votre propre clé privée.

Outil de signature autonome

Utilisez l'outil de signature autonome pour signer les enregistrements pris en charge dans ServiceNow les applications à l'aide de votre propre clé privée.

Utilisez l'outil de signature pour signer des enregistrements dans ServiceNow des 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 script includes.
2. Transmettez l'application par push dans votre référentiel Git, qui réside 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 Source Control integration .

3. Clonez l'application dans votre environnement local.
4. Utilisez l'outil de signature (également disponible 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 signature

Traduction automatique

et des enregistrements de certificat X.509 [sys_certificate]. Pour en savoir plus sur l'utilisation de l'outil de signature, reportez-vous à la section Utilisation de l'outil de signature.

5. Transférez l'application mise à jour vers votre référentiel Git.
6. Dans votre instance, importez l'application mise à jour en appliquant des modifications distantes.

Utilisation de l'outil de signature

Découvrez comment utiliser l'outil de signature pour signer les enregistrements pris en charge dans ServiceNow les applications.

Avant de commencer
Rôle requis : admin

Pour effectuer ces étapes, vous devez disposer des éléments suivants :

- Une ServiceNow application qui comporte des enregistrements à signer.
- Une clé privée pour les enregistrements de signature.
- Le `script signRecords.sh` dans votre environnement local, avec l'autorisation d'exécution.

> **Important :**
> Le script `signRecords.sh` est inclus dans le fichier jar de l'outil de signature, que vous devez demander à partir de ServiceNow Soutien à la 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, entrez 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 une signature réussie.

```
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 enregistrement pris en charge `65e811327702111057416efe7c5a994f` et l'a signé.
- Dans le répertoire ServiceNow-App-1, deux enregistrements ont été créés : sys_certificate.xml et sn_kmf_record_signature.xml.

5. Importez à nouveau l'application mise à jour dans votre instance en appliquant les modifications distantes dans Studio.
   Pour plus d'informations, consultez Apply remote changes .

Arguments de l'outil de signature

Découvrez les arguments disponibles pour l'outil de signature.

Arguments de ligne de commande

Argument	Obligatoire	Description
-d	Oui	Répertoire racine du projet à signer. Doit contenir le répertoire de projet (aléatoire 32 alphanumériques), le fichier sn_source_control.properties et un fichier <project_name>.iml
-f	Oui	Chemin d'accès au fichier du 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 en un seul fichier.
-K	Non	Mot de passe permettant d'accéder à la clé stockée dans le magasin de clés. Vous pouvez également entrer ce mot de passe lorsque vous y êtes invité plutôt qu'à l'intérieur de l'argument.
-O	Non	Signez avec un nouveau certificat à la place de tout fichier sys_cert existant.
-p	Non	Mot de passe permettant d'accéder au magasin de clés s'il possède un mot de passe. Vous pouvez également entrer ce mot de passe lorsque vous y êtes invité plutôt qu'à l'intérieur de l'argument.
-W	Non	Effacez 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 de production

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 de production et de non-production approuvées.

- Établissez Circle of Trust un lien entre les instances de production et les instances approuvées.
- Rôle requis : security_admin

Remarque :

- Serveur MID ne gère pas les sources de données de fichier et, par conséquent, ces sources de données ne sont pas codées.
- Les sources de données LDAP ne peuvent pas être signées par code.

Signer les sources de données existantes du type JDBC

Utilisez des ensembles de mises à jour pour apporter des tâches de signature en masse à l'instance de production.

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 Security** > **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 **Enregistrements de signature en masse**.
Table	Table à partir de laquelle les enregistrements doivent être signés. Sélectionnez **la source de données**.

   d. Cliquez sur **Exporter la tâche de signature de code vers la production**.
   Un message de confirmation indiquant que l’ensemble de mises à jour est signé.

   e. Exportez l’ensemble de mises à jour généré vers un fichier XML.

2. Dans l’instance de production, importez et validez l’ensemble de mises à jour pour récupérer les tâches signées en masse à partir de l’instance de confiance.

   a. Accédez à la **Sécurité de système** > **Tâches de Security** > **Tous**.

   b. Ouvrez l’ensemble de mises à jour exporté à partir de l’instance approuvée.

   c. Cliquez sur **Démarrer**.
   Un message de confirmation s’affiche indiquant que les enregistrements sont signés.

Signer les nouvelles sources de données du type JDBC

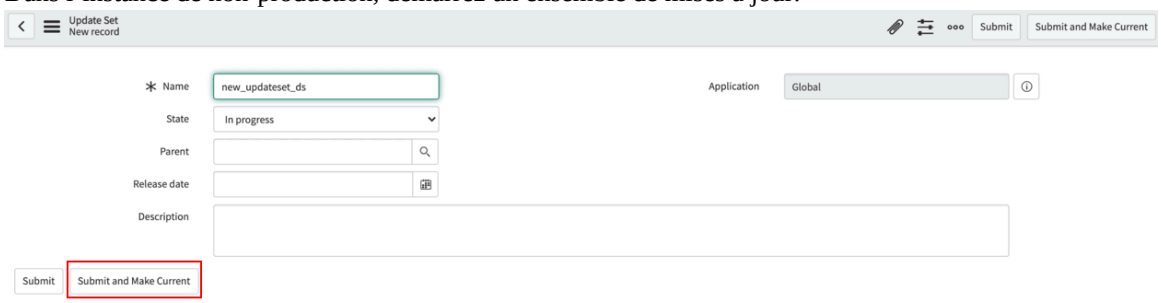
Utilisez des ensembles de mises à jour pour apporter l’ensemble de mises à jour signé à l’instance de production.

Avant de commencer

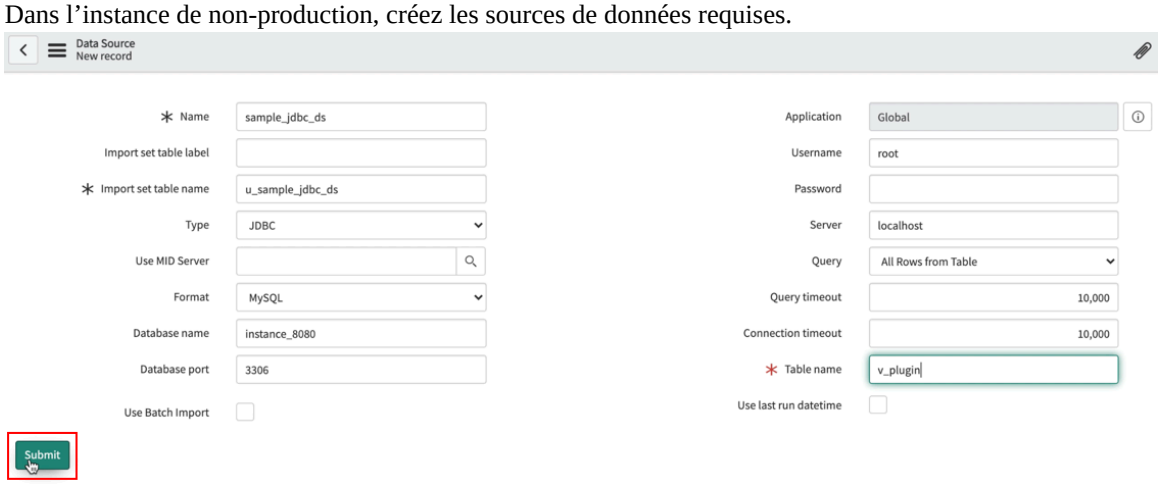
Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Dans l'instance de non-production, démarrez un ensemble de mises à jour.

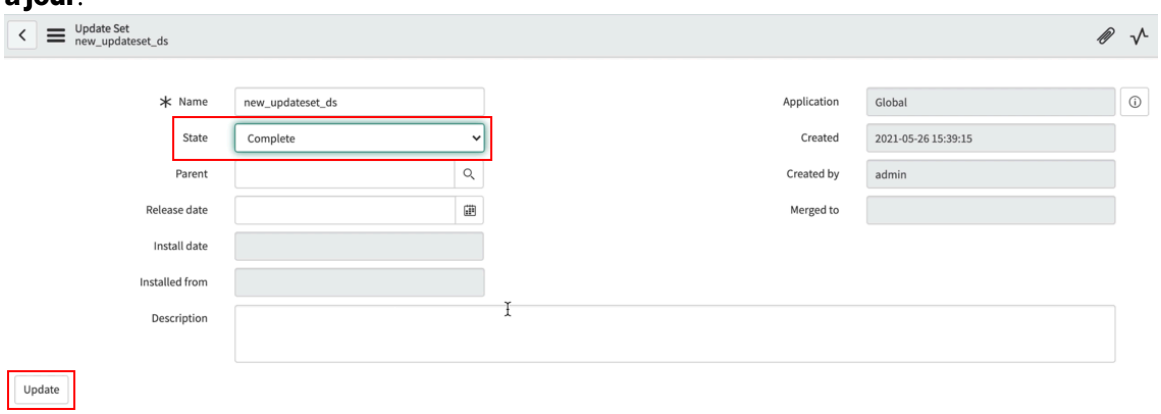


2. Dans l'instance de non-production, créez les sources de données requises.



Les sources de données sont ajoutées à l'ensemble de mises à jour.

3. Dans l'instance de non-production, modifiez l'état du jeu de mises à jour sur **Terminé** et cliquez sur **Mettre à jour**.



4. Dans l'instance de non-production, signez l'ensemble de mises à jour en créant une tâche de chiffrement.

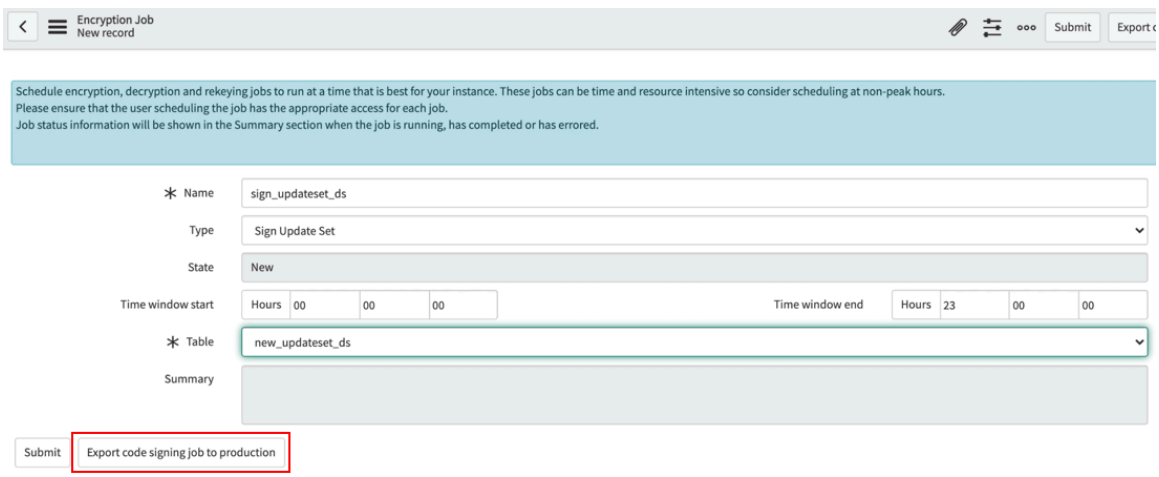
   a. Accédez à la **Sécurité de système** > **Tâches de Security** > **Tous**.

   b. Cliquez sur **Nouveau**.

   c. Renseignez ces valeurs sur le formulaire.

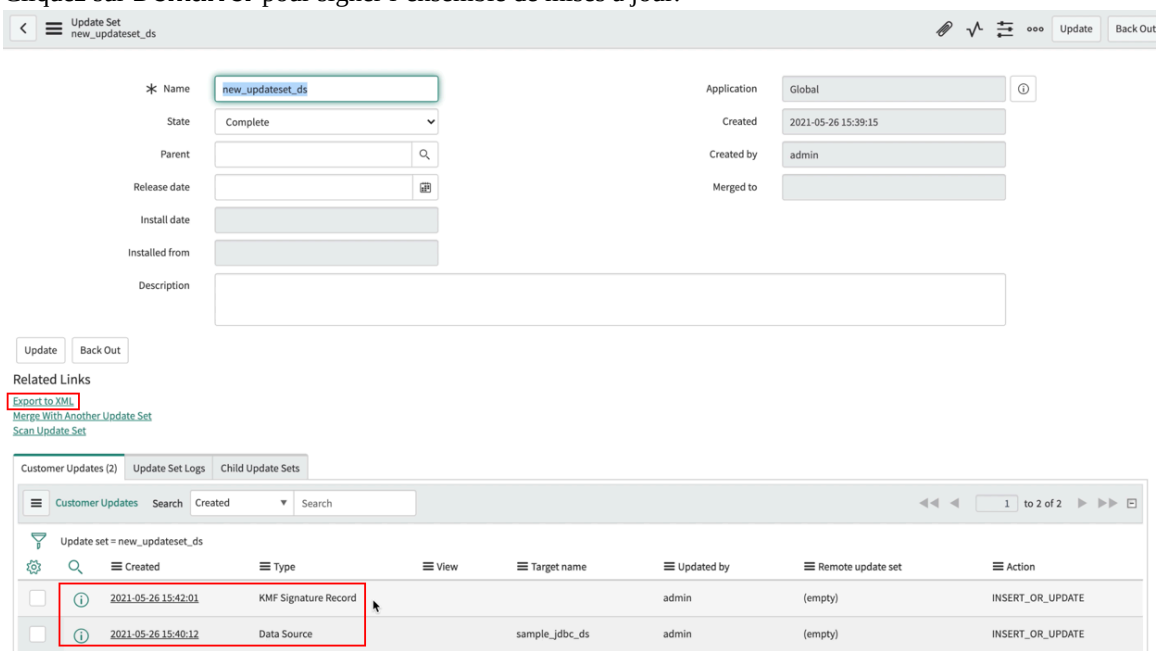
Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.

Champ	Description
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.



- **Le résumé** est mis à jour lorsque les enregistrements sont signés.
- L'ensemble de mises à jour est mis à jour et inclut la signature.

5. Dans l'instance de non-production, ouvrez l'enregistrement d'ensemble de mises à jour signé et exportez-le au format XML.

6. Dans l'instance de production, 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 de 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.

Signez 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 de production et de non-production.

- Établissez Circle of Trust un lien entre les instances de production et de non-production.
- Rôle requis : security_admin

Signer les messages REST et SOAP existants

Signez et validez les messages REST et SOAP existants en activant la signature de code dans les instances de production et de non-production approuvées.

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 table Glide. Par exemple, sélectionnez **Actions d'interface utilisateur [sys_ui_action].**
Objectif de signature KMF	Objectif de la signature des enregistrements. Sélectionnez **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 de 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 respectés pour signer les enregistrements.
Signer la pièce jointe	Option permettant de signer la pièce jointe dans l'enregistrement Glide.

Champ	Description
Clé d'instance	Option pour 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 de confiance, signez les enregistrements requis.

a. Accédez à la **Sécurité de système** > **Tâches de Security** > **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 **Enregistrements de signature en masse**.
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 de production, 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 de 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 de production, exécutez la tâche de chiffrement que vous avez précédemment créée dans l’instance approuvée en **sélectionnant Démarrer**.
Un message de confirmation s’affiche indiquant que les enregistrements sont signés.

Signer les nouveaux messages REST et SOAP

Signez et validez les nouveaux messages REST et SOAP à partir de l'instance approuvée en activant la signature de code dans les instances de production et approuvées.

Procédure

1. Dans l'instance de non-production, démarrez un ensemble de mises à jour.
2. Dans l'instance de non-production, créez les messages REST ou SOAP requis.
   Les messages sont ajoutés à l'ensemble de mises à jour.
3. Dans l'instance de non-production, modifiez l'état du jeu de mises à jour sur **Terminé** et cliquez sur **Mettre à jour**.
4. Dans l'instance de non-production, signez l'ensemble de mises à jour en créant une tâche de chiffrement.

   a. Accédez à la **Sécurité de système** > **Tâches de Security** > **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 un 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 lorsque les enregistrements sont signés.
      - L'ensemble de mises à jour est mis à jour et inclut la signature.

5. Dans l'instance de non-production, ouvrez l'enregistrement d'ensemble de mises à jour signé et exportez-le au format XML.
6. Dans l'instance de production, importez l'ensemble 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 de 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 les flux, les flux secondaires et les actions dans l'instance de production

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 de production et approuvées.

Avant de commencer

- Établissez Circle of Trust un lien entre les instances de production et les instances 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 non-production approuvées.

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 Security** > **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 **Enregistrements de signature en masse**.
Table	Table à partir de laquelle les enregistrements doivent être signés. Sélectionnez **l'instance d'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 de production, importez le fichier XML.

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 de 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 de production, exécutez la tâche de chiffrement que vous avez précédemment créée dans l'instance approuvée.

a. Accédez à la **Sécurité de système** > **Tâches de Security** > **Tous**.

b. Ouvrez la tâche de chiffrement que vous avez précédemment créée dans l'instance approuvée.

c. Cliquez sur **Démarrer** pour démarrer la tâche.
Un message de confirmation s'affiche indiquant que les enregistrements sont signés.

Signer un nouveau flux, des flux secondaires et des actions

Signez et validez les nouveaux flux, flux secondaires et actions en activant la signature de code dans les instances de production et de non-production approuvées.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Dans l'instance de confiance, 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 approuvée, 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 Security** > **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.

- **Le résumé** est mis à jour lorsque 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 d'ensemble de mises à jour signé et exportez-le au format XML.
6. Dans l'instance de production, 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 l'ensemble de mises à jour à partir du fichier 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.

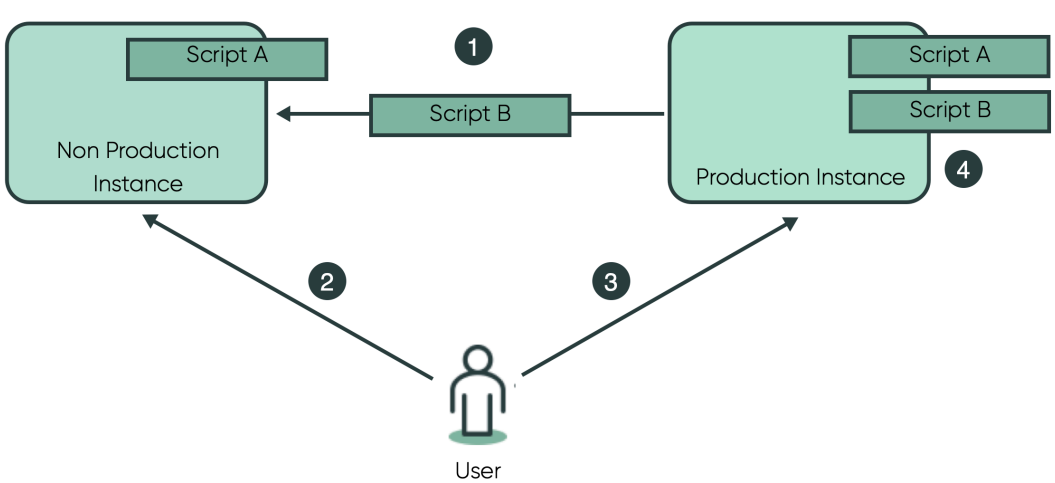
Signer des enregistrements ou des pièces jointes spécifiques

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 compter de cette Vancouver version, les administrateurs de sécurité peuvent utiliser des tâches de sécurité pour signer des enregistrements spécifiques sur une table plutôt que tous les enregistrements d'une table. Signez des enregistrements spécifiques pour éviter de signer accidentellement du 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 de la façon dont vous pouvez utiliser le processus de signature. Dans cet exemple, un script, intitulé Script B , n'existe que sur l'instance de production et doit être importé dans une instance approuvée pour être signé. Le script A existe déjà sur les deux instances, il n'a pas besoin d'être signé. Soit il a déjà été examiné et signé, soit il n'a pas encore été examiné et ne devrait pas être signé.

Traduction automatique

1. Importez l'enregistrement dans votre environnement de confiance.
2. Dans l'instance de confiance, 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 de production à l'aide d'un ensemble de mises à jour.
4. Dans l'instance de production, 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 non-production approuvée.

Avant de commencer

Rôle requis : security_admin ou sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Tâches de Security** > **Créer**.
2. À **l'invite Quel type de tâche de sécurité voulez-vous créer ?** , sélectionnez **Tâche de signature**. Un nouvel enregistrement **de tâche de signature** s'affiche.
3. Renseignez les champs du formulaire comme il convient :

Champs de tâche de signature

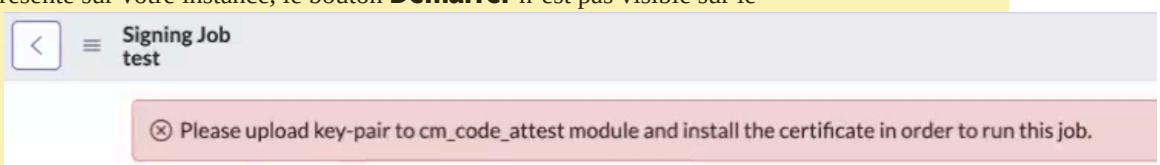
Champ	Description
Nom	Nom descriptif pour cette tâche.
Type	Type de tâche de sécurité. Pour signer des enregistrements spécifiques, sélectionnez l'option **Signer des enregistrements spécifiques** . Pour signer des pièces jointes spécifiques, sélectionnez **Signer des pièces jointes spécifiques**.
État	État de cette tâche. Ce champ commence par la valeur **Nouveau**. Ce champ est en lecture seule.
Table	Table contenant les enregistrements ou les pièces jointes que vous souhaitez signer. Si vous signez des pièces jointes, sélectionnez la table avec les enregistrements auxquels les pièces jointes sont associées, et non la table Pièce jointe [sys_attachment]. **Conseil :** Vérifiez la table d'enregistrement de signature [sn_kmf_record_signature] de Key Management Framework (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 s'affichent dans la table **Sélectionner les enregistrements à signer** .

Champ	Description
Sélectionner les enregistrements à signer	Liste des enregistrements de la table sélectionnés dans le champ **Table** , limitée par le filtre créé dans le champ **Filtrer les enregistrements** . 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 exprimée en heure universelle coordonnée, selon une notation temporelle de 24 heures.
Fin de la fenêtre de temps	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 prochain début de la fenêtre horaire. L'heure de fin doit être postérieure à l'heure de début. Une valeur de temps valide est exprimée en heure universelle coordonnée, selon une notation temporelle de 24 heures.
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 à être exportée.
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 correspondant à 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 vers 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 d'un fichier 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 le bouton **Valider l'ensemble de mises à jour** apparaître.
15. Sélectionnez **Valider l'ensemble de mises à jour.**

16. **Tous** > **Sécurité de système** > **Tâches de Security** > **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 chargée dans 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 à effectuer et une liste de sys_ids pour chaque enregistrement signé.

Signer des enregistrements ou des pièces jointes spécifiques sur une instance de production

Signez un enregistrement spécifique ou un groupe d'enregistrements que vous définissez sur une instance de production.

Avant de commencer

Rôle requis : security_admin ou sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Si aucune relation de confiance n'est établie entre vos instances de production et les instances approuvées, vous pouvez signer vos enregistrements ou pièces jointes directement sur votre instance de production en suivant ces étapes. Pour créer cette relation entre vos instances, reportez-vous à Charger les paires de clés et les certificats requis pour la signature de code.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Tâches de Security** > **Créer**.
2. À **l'invite Quel type de tâche de sécurité voulez-vous créer ?,** sélectionnez **Tâche de signature**. Un nouvel enregistrement **de tâche de signature** s'affiche.
3. Renseignez les champs du formulaire comme il convient :

Champs de tâche de signature

Champ	Description
Nom	Nom descriptif pour 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.

Champ	Description
Table	Table contenant les enregistrements ou les pièces jointes que vous souhaitez signer. Si vous signez des pièces jointes, sélectionnez la table avec les enregistrements auxquels les pièces jointes sont associées, et non la table Pièce jointe [sys_attachment]. **Conseil :** Vérifiez la table d'enregistrement de signature [sn_kmf_record_signature] de Key Management Framework (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 s'affichent dans la table **Sélectionner les enregistrements à signer** .
Sélectionner les enregistrements à signer	Liste des enregistrements de la table sélectionnés dans le champ **Table** , limitée par le filtre créé dans le champ **Filtrer les enregistrements** . 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 exprimée en heure universelle coordonnée, selon une notation temporelle de 24 heures.
Fin de la fenêtre de temps	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 prochain début de la fenêtre horaire. L'heure de fin doit être postérieure à l'heure de début. Une valeur de temps valide est exprimée en heure universelle coordonnée, selon une notation temporelle de 24 heures.
Résumé	Résumé de l'exécution de cette tâche. Ce champ est en lecture seule.

4. Sélectionnez **Envoyer**.

Que faire ensuite

La tâche de sécurité s'exécute entre les heures spécifiées dans les champs Début de la **fenêtre** de temps et Fin de la **fenêtre de temps** , ou lorsque vous sélectionnez le bouton **Exécuter** . 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 à effectuer et une liste de sys_ids pour chaque enregistrement signé.

Référence de signature de code

Les rubriques de référence fournissent des informations supplémentaires sur la gestion et le dépannage de 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 divers 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 vrai, la longueur de validation de la pile meta 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 effectuer lorsque la signature de code est activée. La valeur par défaut est de 3. **Important :** Une sécurité élevée est nécessaire pour modifier cette propriété.
liste com.glide.codesigning.expanded_tracking.rubrique.liste	Chaîne	Liste des rubriques séparées par des virgules qui doivent faire l'objet d'un suivi de la méta-pile augmentée. **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 de débogage pour le suivi de signature de code est activée.
com.glide.codesigning.tracking.enabled	true|false	Si la valeur est vrai, active le suivi de l'appelant par signature de code.

Propriété	Type	Description
		Important : Une sécurité élevée est nécessaire pour modifier cette propriété.
com.glide.codesigning.tracking.logging.enabled	true|false	Si vrai, active la journalisation pour le suivi de la signature de code.
com.glide.codesigning.tracking.unsupported_script_tracking.enabled	true|false	Si la valeur est vrai, ecc_queue enregistrements 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 la valeur est vraie, la vérification de la signature du 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. **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.servicenow_root_of_trust.désactivé	true|false	Si la fonctionnalité de racine de confiance est active. La valeur par défaut est false, ce qui signifie que ServiceNow les certificats de build sont approuvés.

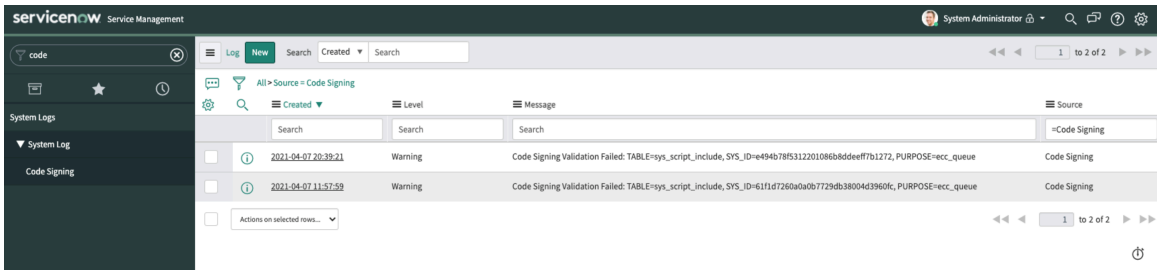
Propriété	Type	Description
		Important : Cette propriété ne peut être modifiée qu'à l'aide d'une tâche planifiée signée par un utilisateur ayant les rôles administrateur, administrateur de sécurité et gestionnaire KMF. Pour en savoir plus sur la modification de votre racine de confiance, reportez-vous à la section Changer la configuration de votre 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 qu'en envoyant une requête à Service et assistance client. Pour plus d'informations, voir KB1205749
glide.jdbcprobeloader.tracking	true|false	Active/désactive la signature de code pour les sources de données JDBC. **Important :** Une sécurité élevée est nécessaire pour modifier cette propriété.
glide.rest.codesigning.tracking	true|false	Si la valeur est vrai, active le suivi de la signature de code RESTMessageV2. **Important :** Une sécurité élevée est nécessaire pour modifier cette propriété.

Dépannage et accès aux journaux

Accédez à divers 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 Code Signing Tracker, 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 obtenir des 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

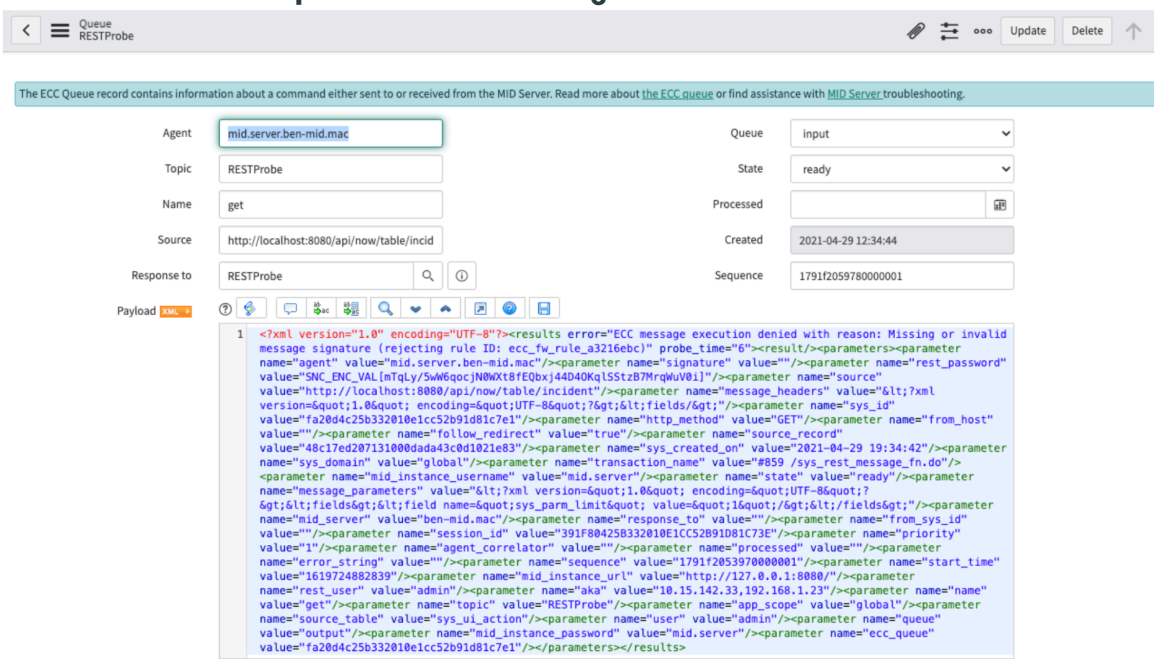
Accédez au message d'erreur relatif à l'échec de validation de la signature en accédant à **Services web du système** > **Sortant** > **Message REST** et l'ouverture de l'enregistrement de message REST requis.

Échec de la validation de la signature sur Serveur MID

Remarque :
Les messages d'erreur liés aux rejets de pare-feu ECC commencent par `Exécution du message ECC refusée`.

Traduction automatique

File d'attente ECC lorsque la validation de la signature échoue le Serveur MID



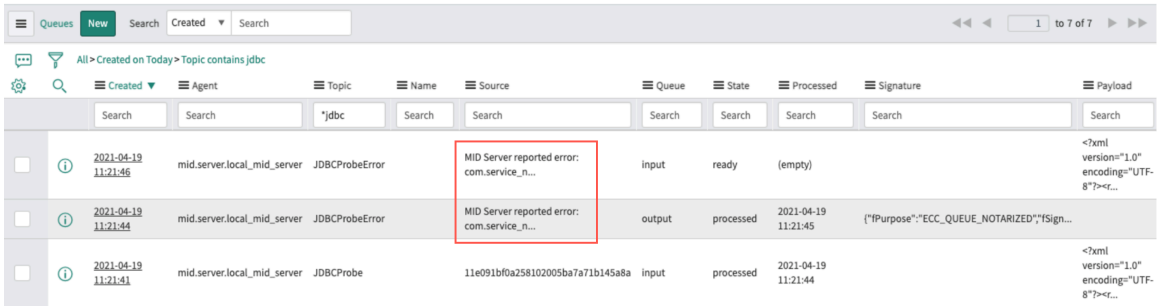
Message d'erreur lorsque le message ECC est bloqué par la règle utilisateur

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.

Traduction automatique



Serveur MID Journaux

Pour activer la journalisation détaillée du pare-feu ECC, augmentez le niveau de journal en définissant la valeur du paramètre de configuration du MID Server, `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 raison de laquelle un message ECC doit être accepté ou rejeté.

Remarque :
Si boot-config.xml n'est pas valide, les Serveur MID échecs de démarrage et les détails de l'échec sont consignés dans les journaux des agents MID.

Rôles de sécurité

Les rôles de sécurité fournissent une sécurité supplémentaire, chaque utilisateur doit avoir au moins un rôle afin que l'instance puisse faire la distinction entre les utilisateurs internes et externes.

Explorer les rôles explicites

Découvrez les principales fonctionnalités et la valeur commerciale d'Explicit Roles.

Explorez Elevated Privilege

Découvrez comment le rôle de privilège élevé active les privilèges basés sur la session.

Traduction automatique

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. Now Platform abandonne toute opération qui créerait un tel scénario.

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 :

- Ressources Scripted REST API qui ne sont pas marquées comme étant externes.
- 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 accorder l’accès au rôle snc_external ou à un rôle qui hérite du rôle snc_external.
- Tableaux de bord Now Intelligence.

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 avoir le rôle snc_internal pour accéder aux ressources internes ou le 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.

  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.

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.

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

Now Platform empêche les utilisateurs d'avoir le rôle snc_external et le rôle snc_internal à la fois. L'application Now Platform applique cette exclusion mutuelle partout dans le système et saisit des messages d'erreur dans les journaux pour chaque conflit.

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 utilisateur a le rôle snc_internal.	Ajoutez le rôle snc_external.	L'action est abandonnée.
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.

Rôle	Tentative d'action	Résultat
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.
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 Now 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 Explicit Roles en demandant le module d'extension Explicit Roles (com.glide.explicit_roles) via Service Now Support Catalog.

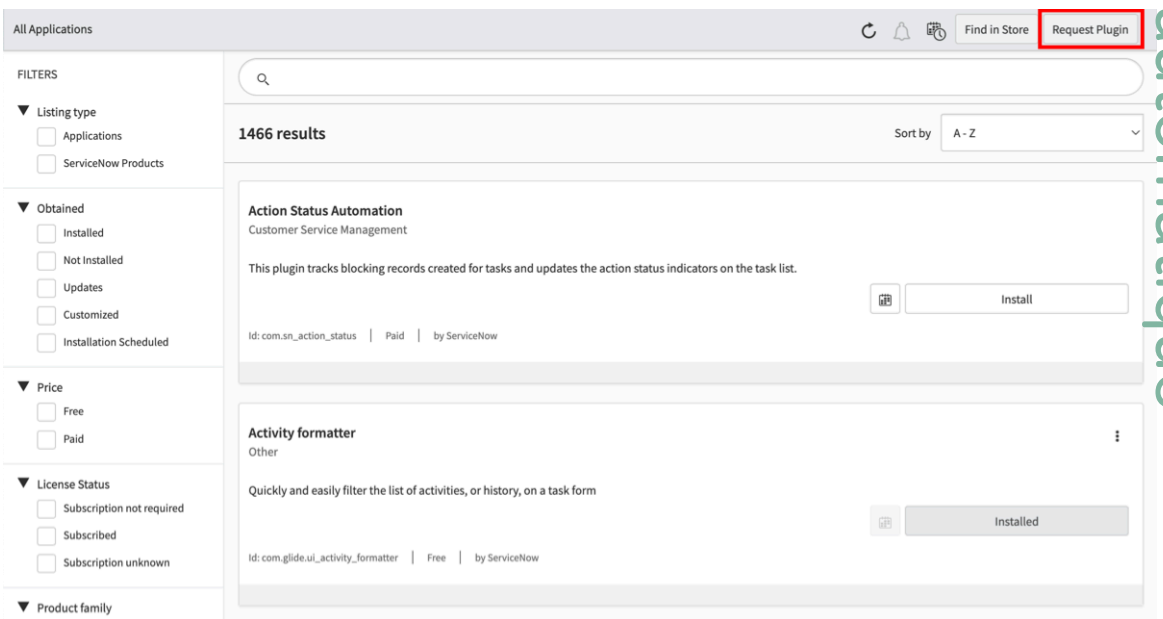
Avant de commencer

Rôle requis : admin

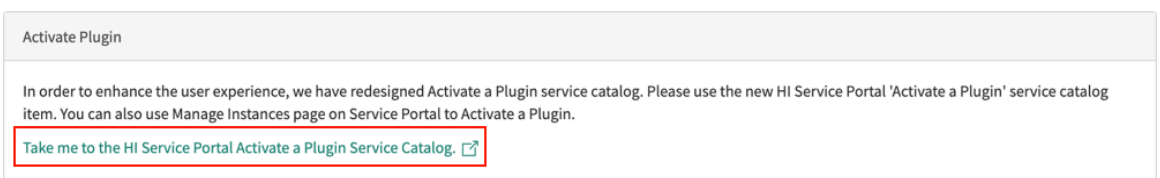
Important :
Activez ce module d'extension pendant une fenêtre de maintenance ou lorsque peu d'utilisateurs sont connectés. Les utilisateurs actuellement connectés lorsque le module d'extension est activé ne se verront pas attribuer dynamiquement le rôle snc_internal. Les utilisateurs doivent plutôt se 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.

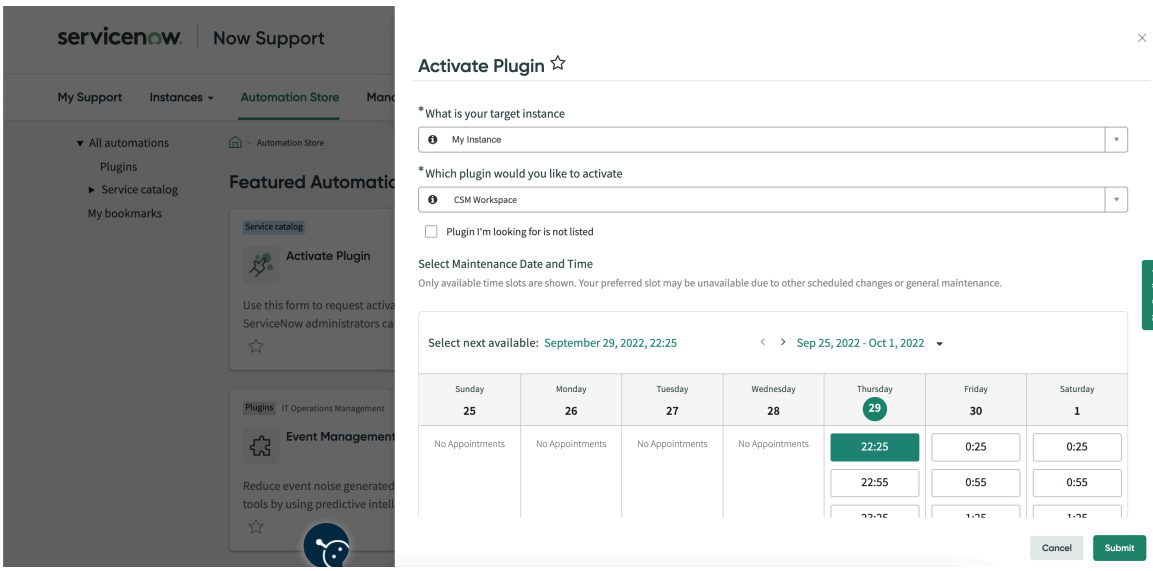
Formulaire Activer le module d'extension

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



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 Service Catalog [KB0751715] de la Now Support Base de connaissances.

Rôles de privilège élevé

Les rôles de privilège élevé vous obligent à accepter manuellement la responsabilité d'utilisation du rôle avant de pouvoir accéder aux fonctionnalités du rôle.

Par défaut, vous ne disposez pas de rôles de privilège élevé lors de la connexion. Vous devez manuellement élever le rôle au privilège. Un rôle de privilège élevé ne dure que le temps de votre session utilisateur. L'expiration de la session ou la déconnexion entraîne la suppression du rôle.

Vous pouvez désigner n'importe quel rôle comme rôle de privilège élevé, puis affecter ce rôle à un ou plusieurs utilisateurs. Faites cela lorsque vous souhaitez empêcher les utilisateurs d'accéder aux droits que le rôle fournit 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 l'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 le rôle élevé A contient le rôle B élevé, même si vous l'élevez au rôle A, vous devez quand même l'élever au rôle B pour obtenir ses privilèges.

Le rôle admin

Pour accorder le rôle administrateur à un utilisateur, l'utilisateur qui accorde le rôle doit également avoir le rôle administrateur. Par exemple, un utilisateur disposant uniquement du rôle user_admin ne peut pas accorder le rôle administrateur à d'autres utilisateurs.

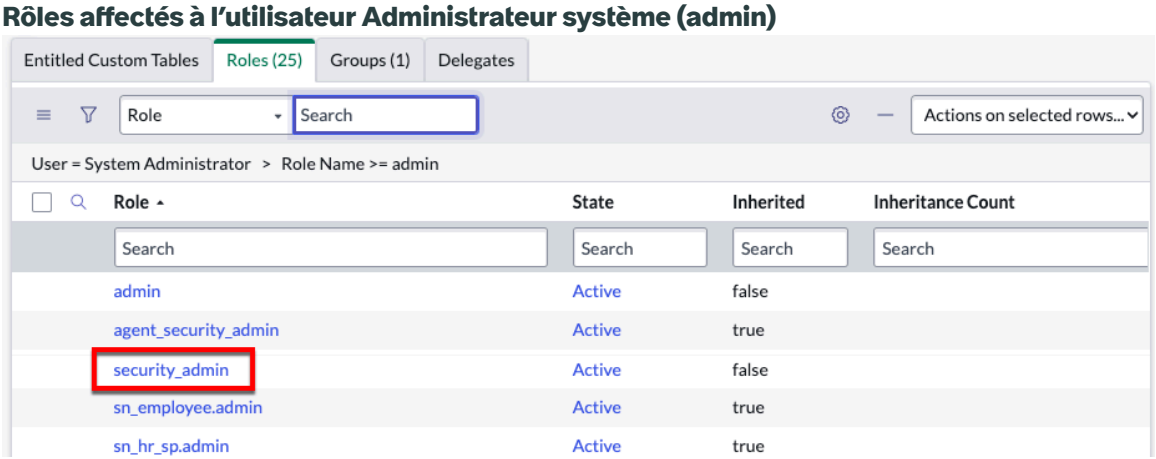
- Les utilisateurs non administrateurs ne peuvent pas ajouter un utilisateur à un groupe qui contient le rôle administrateur.
- Pour accorder le rôle security_admin à un utilisateur, l'utilisateur qui accorde le rôle doit également avoir le rôle administrateur et doit s'élever au rôle security_admin avant d'accorder le rôle security_admin à d'autres utilisateurs. Un utilisateur ayant uniquement le 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 le rôle administrateur n'est pas prise en charge et peut provoquer un comportement inattendu. Pour exiger des administrateurs qu'ils élèvent manuellement, reportez-vous à la section 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'administrateur système (admin) par défaut. Il permet d'accéder aux ACL et aux paramètres de sécurité élevée.

Rôles affectés à l'utilisateur Administrateur système (admin)



Remarque :
Pour voir ce rôle, vous devez d'abord vous élever au rôle security_admin. Si vous êtes connecté uniquement en tant qu'administrateur système (admin), vous ne pouvez pas voir l'enregistrement security_admin dans la liste des rôles.

Security_admin rôle

Le rôle security_admin est un rôle de privilège élevé fourni avec des paramètres de sécurité élevée qui permet aux utilisateurs de créer et de modifier des contrôles d'accès et de modifier les paramètres de sécurité élevée.

Dans le système de base, seul l'administrateur système par défaut (admin) dispose du rôle security_admin. Étant donné que cela nécessite des privilèges élevés, l'utilisateur administrateur ne dispose pas de ce rôle lors de la connexion. Après avoir élevé les privilèges, l'utilisateur administrateur dispose du rôle security_admin pour la durée de la session utilisateur. Consultez Élever à un rôle privilégié pour plus d'informations.

Pour maintenir une sécurité élevée, le rôle security_admin nécessite d'élever les privilèges. Limitez les utilisateurs et les groupes auxquels vous affectez ce rôle.

Élever à un rôle privilégié

L’administrateur système de base peut accéder à un rôle privilégié afin d’accéder aux fonctionnalités des paramètres de sécurité élevée.

Avant de commencer

Rôle requis : admin

Remarque :
Si vous accordez à d’autres utilisateurs le rôle administrateur, ils ne peuvent pas accéder à un rôle privilégié. Seul l’administrateur du système de base peut élever le niveau.

Procédure

1. Dans la bannière, cliquez sur votre image ou cliquez sur vos initiales si aucune image n’a été chargée.
2. Sélectionnez **Élever les privilèges des rôles**.
   Une boîte de dialogue contenant les rôles disponibles pour l’élévation s’affiche.
3. Sélectionnez les rôles élevés à affecter, puis cliquez sur **OK**.
   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 lors de la connexion suivante.
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 disposant du rôle administrateur à sélectionner manuellement le rôle auquel ils souhaitent accéder.

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 fenêtre de dialogue s’affiche pour sélectionner le rôle auquel il peut s’adresser.

Security Center

ServiceNow Security Center est une application qui se compose d’un ensemble d’outils conçus pour aider votre organisation à maintenir la sécurité de vos déploiements ServiceNow. Security Center vous permet d’améliorer la posture de sécurité et de renforcer les niveaux de conformité grâce à une expérience utilisateur transparente.

Security Center est une application gratuite que les administrateurs système peuvent télécharger à partir du ServiceNow Store. Elle est installée par défaut à partir de la version Vancouver.

Remarque :
Instance Security Center (ISC) atteindra la fin des ventes d'ici septembre 2024. SPC est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Migration d'Instance Security Center vers ServiceNow Security Center.

Page d'accueil

Affichez votre score de conformité à la sécurisation renforcée en pourcentage, analysez les principaux paramètres de sécurisation renforcée non conformes à corriger et consultez les résultats de vos analyses de sécurité.

Sécurisation renforcée

Découvrez comment les configurations de sécurisation renforcée sont conformes aux recommandations de sécurité de ServiceNow

Analyseur de sécurité

Analysez un ensemble de contrôles de sécurité pour identifier les erreurs de configuration et les comportements non sécurisés

Mesures de sécurité

Surveillez plus de 50 indicateurs différents qui permettent d'identifier les menaces de sécurité potentielles.

Antivirus

Affiche la tendance à laquelle les événements se produisent sur les fichiers potentiellement infectés.

Apprentissage de la sécurité

Référentiel central de ressources de sécurité permettant d'accéder aux documents de sécurité et de conformité de ServiceNow.

Traduction automatique

Rôles d'utilisateur

Pour utiliser Security Center, vous devez avoir le rôle administrateur ou security_dashboard_user.

Rôle requis	Utilisateur	Avantages
administrateur	Personnel de sécurité de votre organisation qui surveille les informations liées à la sécurité d'une instance et a l'autorisation de modifier les paramètres de renforcement de la sécurité. Ils doivent pouvoir revenir au centre de sécurité à tout moment pour ajuster les paramètres et gérer l'intégrité globale de la sécurité d'une instance.	Surveillez et gérez en permanence la conformité de la sécurité de l'instance.
sn_vsc.security_center_viewer	Personnel de sécurité de votre organisation qui surveille les informations liées à la sécurité d'une instance, mais qui n'est pas autorisé à modifier les paramètres de renforcement de la sécurité. Par exemple, un analyste de sécurité disposant de ce rôle peut consulter les informations de sécurité de l'instance. Toutefois, un autre utilisateur doté d'un rôle d'administrateur devra effectuer les mises à jour des paramètres de sécurité proprement dites.	Surveillez en permanence la conformité de la sécurité de l'instance pour détecter les menaces de sécurité et y répondre.

Premiers pas

- Security Center est inclus dans toutes les versions de la famille à partir de Vancouver.
- Lisez la documentation du produit, en commençant par Page d'accueil.

Page d'accueil

Obtenez un résumé rapide de la posture de sécurité de votre instance sur la page d'accueil. Affichez votre score de conformité à la sécurisation renforcée en pourcentage, découvrez les tendances graphiques de votre score de conformité, analysez les principaux paramètres de sécurisation renforcée non conformes à corriger et consultez les résultats de vos analyses de sécurité.

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. Le résumé du score de conformité à la sécurisation renforcée affiche ce pourcentage et les données associées aux changements récents du score. Utilisez le graphique de tendance

du score de conformité à la sécurisation renforcée pour voir comment votre score de conformité a changé au fil du temps.

Améliorez votre score de conformité en utilisant les principaux paramètres de sécurisation renforcée non conforme. Cette liste affiche les 10 paramètres de sécurisation renforcée qui ont le plus d'impact négatif sur votre score de conformité à la sécurisation renforcée. Cette visibilité vous aide à classer par ordre de priorité les paramètres de sécurisation renforcée à corriger.

La section de résumé de l'analyse de sécurité affiche des histogrammes, qui reflètent le nombre de résultats au fil du temps pour chacune de vos analyses de sécurité.

1. Accédez au graphique de tendance du score de conformité à la sécurisation renforcée via la page d'accueil ou en naviguant vers **Sécurisation renforcée** > **Tendance des scores**.
2. Sélectionnez **Examiner la tendance du score** pour personnaliser la période et sélectionner des points sur la ligne de tendance à analyser.
3. Dans la section Résumé de l'analyse de sécurité, sélectionnez une barre pour accéder à la page des résultats de l'analyse correspondant à cette suite d'analyse.

Sécurisation renforcée

Utilisez l'outil de renforcement du Centre de sécurité pour afficher votre score de conformité au renforcement optimal, le comparer aux scores précédents et modifier les paramètres afin d'améliorer votre score de conformité et votre posture de sécurité.

Spécifiez Paramètres de sécurisation renforcée les valeurs recommandées pour les propriétés et modules d'extension liés à la sécurité dans la Now Platform. L'outil de sécurisation renforcée calcule le score de conformité du paramètre de sécurisation renforcée en pourcentage. Ce nombre indique le niveau de conformité de votre instance avec les paramètres de sécurisation renforcée du Centre de sécurité.

La formule pour calculer le score de conformité à la sécurisation renforcée :

- Chaque paramètre de sécurisation renforcée a un score de risque compris entre 0 et 10.
- Le score est égal à la somme de tous les scores de risque de conformité divisée par la somme de tous les scores de risque.

Par exemple, si la somme de tous les scores de risque de conformité est de 25,4 et que le total de tous les scores de risque est de 34,9, le score de conformité sera 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.

Comparaison des scores de sécurisation renforcée

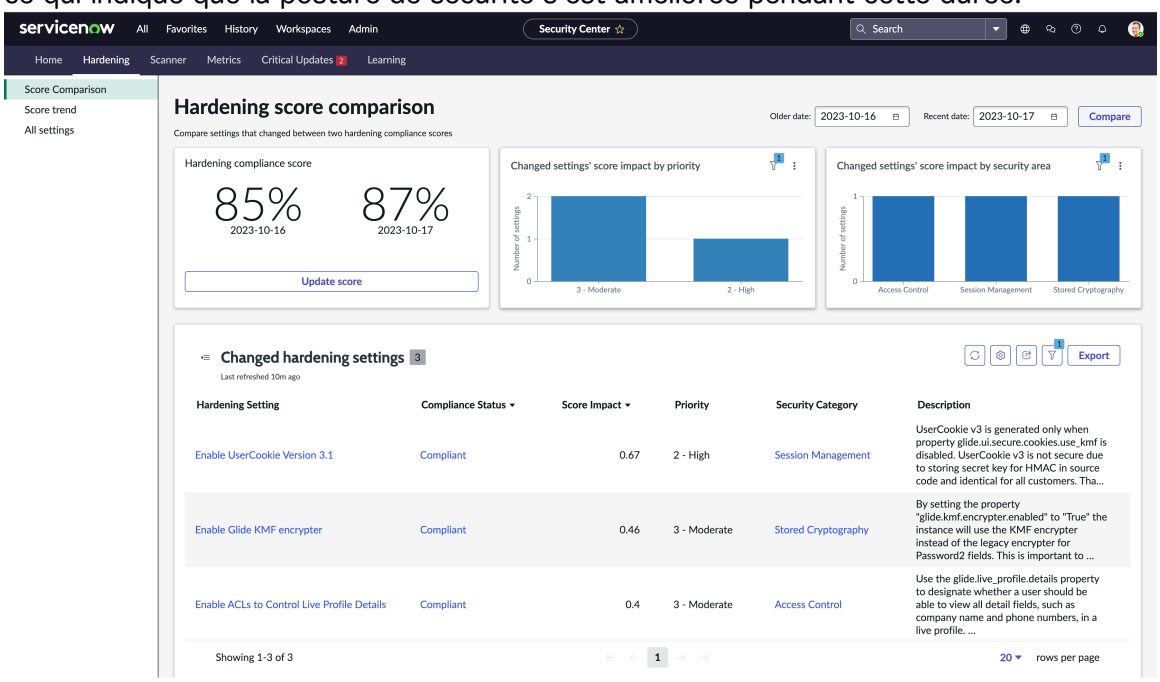
Obtenez une visibilité sur l'intégrité de vos paramètres de sécurisation renforcée et utilisez ces données pour améliorer la posture de sécurité de votre instance.

La page de comparaison des scores de sécurisation renforcée affiche tous les paramètres de sécurisation renforcée dont l'état de conformité a été modifié entre la première et la deuxième date, ainsi que leur impact sur le score de conformité à la sécurisation renforcée. Par exemple, si un paramètre passait de conforme à non conforme, le score aurait diminué.

Pour afficher les résultats de ces changements, entrez une date antérieure et une date récente dans le sélecteur de date en haut à droite de la page, puis sélectionnez Comparer. Voici une explication de chaque carte :

- Score de conformité à la sécurisation renforcée : affiche le score de conformité de votre instance sous forme de pourcentage pour la première et la deuxième date que vous avez sélectionnées.
- Impact du score des paramètres modifiés par priorité : affiche le nombre de paramètres de sécurisation renforcée dont l'état de conformité a été modifié entre les deux dates, organisé par valeur de priorité.
- Impact du score des paramètres modifiés par domaine de sécurité : affiche le nombre de paramètres de sécurisation renforcée qui ont modifié l'état de conformité entre les deux dates, organisé par domaine de sécurité.
- Paramètres de sécurisation renforcée modifiés : affiche la liste des paramètres de sécurisation renforcée qui ont modifié les statuts de conformité entre les deux dates. Vous pouvez passer en revue les paramètres qui sont devenus non conformes et qui ont diminué votre score de comparaison de sécurisation renforcée afin de trouver des opportunités de les rendre conformes afin d'augmenter votre score. Consultez Augmenter le score de conformité à la sécurisation renforcée.

Par exemple, dans la capture d'écran suivante, le score de conformité a augmenté, ce qui indique que la posture de sécurité s'est améliorée pendant cette durée.

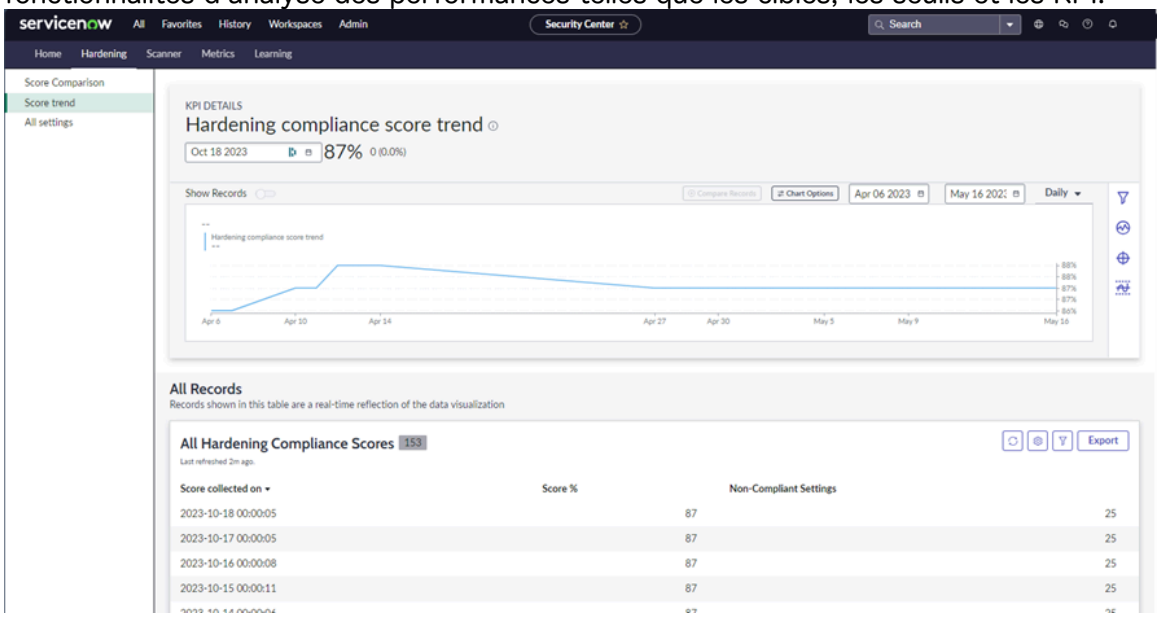


Tendance du score de conformité à la sécurisation renforcée

Affichez les tendances du score de conformité à la sécurisation renforcée sur une période donnée dans un graphique ou un tableau.

Consultez les tendances de votre score de conformité sur une période donnée. Utilisez le sélecteur de date pour sélectionner une période à analyser, puis obtenez des informations plus approfondies sur les données en appliquant des

fonctionnalités d'analyse des performances telles que les cibles, les seuils et les KPI.



Options de graphique : sélectionnez **les options de graphique** pour effectuer une analyse, afficher les séries chronologiques et afficher les données dans plusieurs types de graphiques.

Analyse

- Cible : objectifs que votre organisation souhaite atteindre. Consultez Performance Analytics targets .
- Seuil : définit une plage normale de scores pour un indicateur et vous alerte lorsque certains événements se produisent. Consultez Performance Analytics thresholds .
- Prévision : décrit la capacité à prévoir les scores futurs en fonction du comportement passé. Consultez Performance Analytics scores forecasts .
- Tendance : indique la façon dont 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 associés aux visualisations.
- Statistiques : affiche les statistiques relatives à votre score de conformité.

Séries chronologiques

- Score : score du KPI.
- Changement : changement de score pour cet indicateur.
- Pourcentage de changement : pourcentage de changement des scores.

Types de graphiques : reportez-vous à la section Time series visualization type use cases .

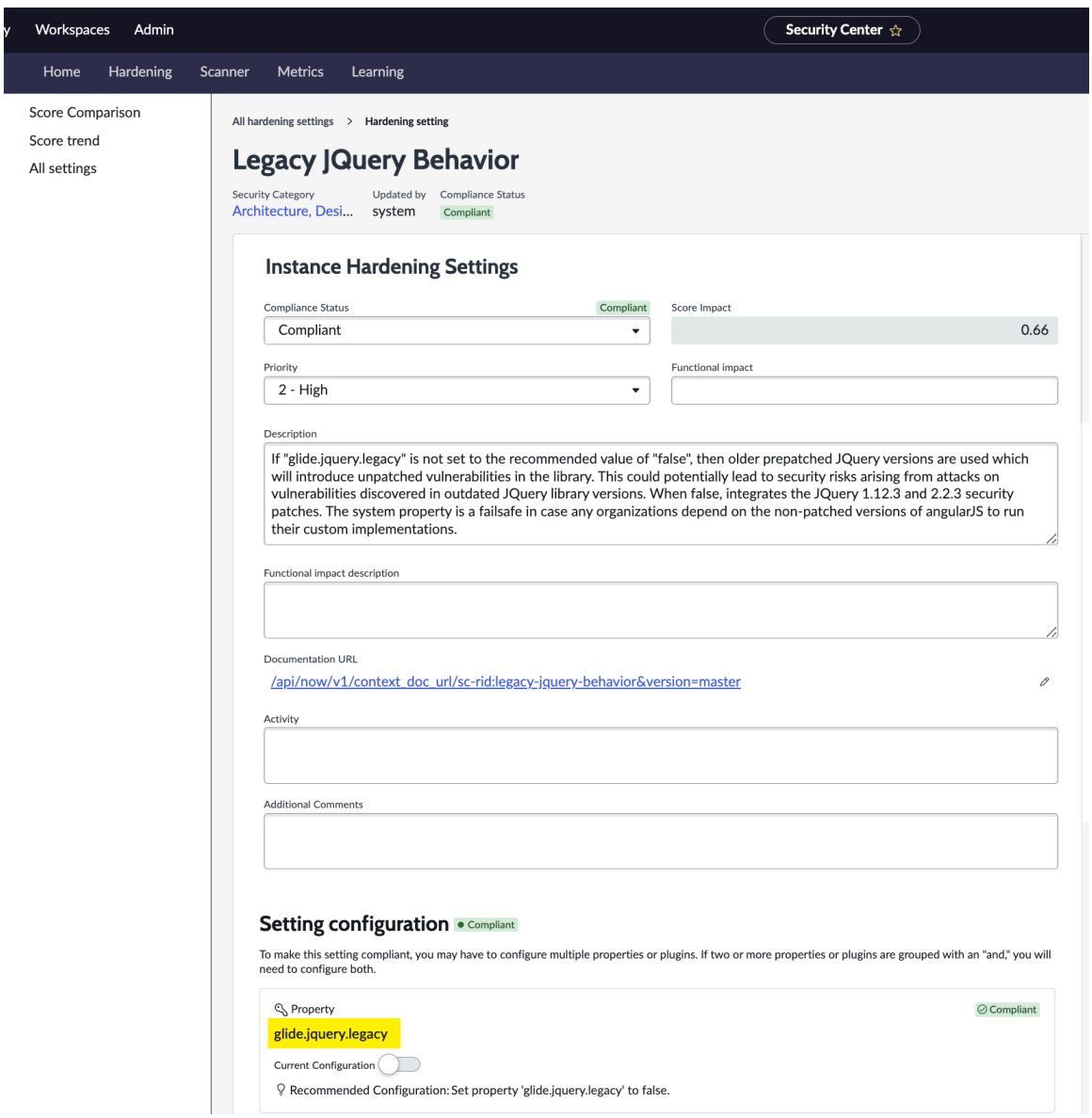
Table Tous les enregistrements

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.

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 à rediriger vers une page de l'outil de sécurisation renforcée qui affiche ses informations relatives à la sécurité.



Détails de la configuration des paramètres de sécurisation renforcée

Attribut de configuration	Description
Statut 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 la force de l'impact de

Traduction automatique

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

Attribut de configuration	Description
	ce paramètre de renforcement sur votre posture de sécurité.
Impact fonctionnel	L'impact de ce paramètre de sécurisation renforcée sur le fonctionnement de votre instance.
Description	Aperçu général du paramètre de sécurisation renforcée.
Documentation Url	Lien vers la documentation du paramètre de sécurisation renforcée.
Activité	Notifications de mises à jour liées au paramètre de sécurisation renforcée.
Configuration des paramètres	Détails liés 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 vous obliger à configurer plusieurs propriétés et modules d'extension pour les rendre conformes.

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.

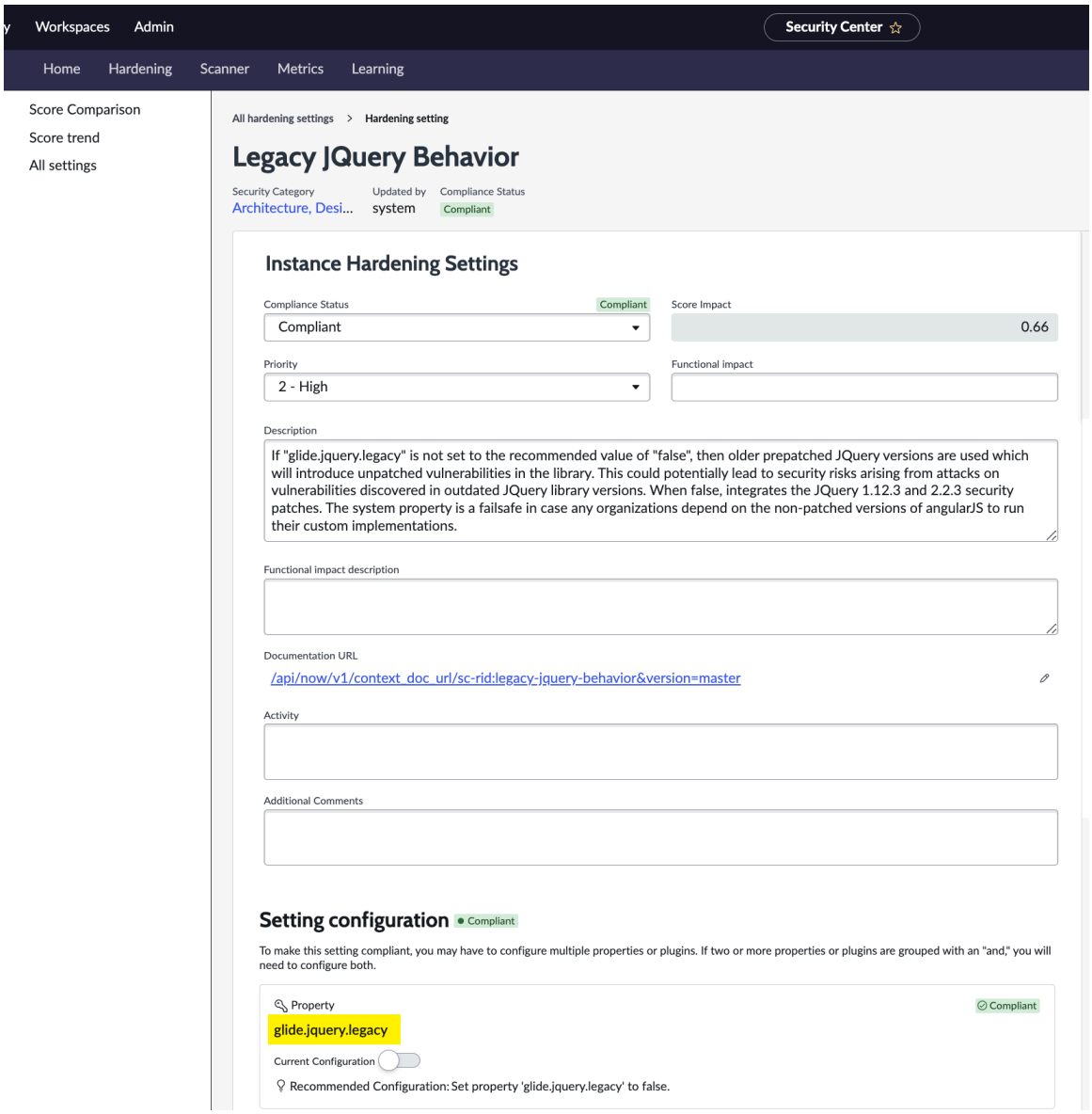
Avant de commencer

Rôle requis : admin

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

Procédure

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



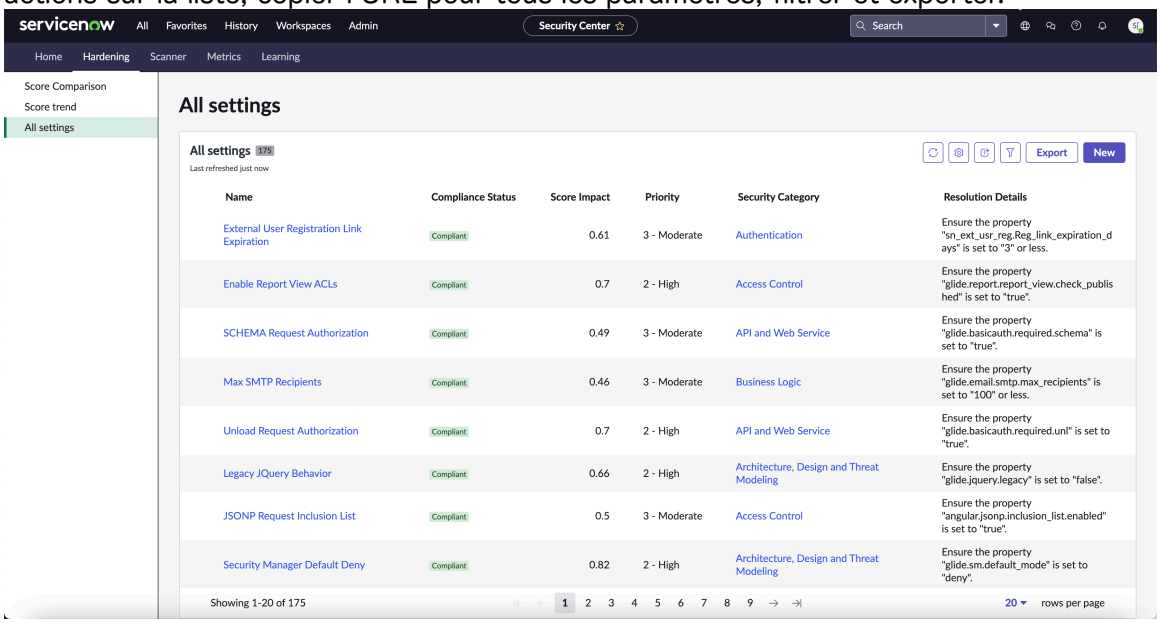
5. Assurez-vous que le paramètre de durcissement est conforme.
6. Si vous mettez à jour un score de sécurisation renforcée non conforme pour le rendre conforme, accédez à la page d'accueil et sélectionnez **Mettre à jour le score** pour afficher le score le plus à jour.
   Le score de sécurisation renforcée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

Tous les paramètres

Affichez tous les paramètres de sécurisation renforcée disponibles dans votre instance à partir d'une seule page.

Table qui affiche tous les paramètres de sécurisation renforcée disponibles dans votre instance. Vous pouvez appliquer les opérations courantes pour une table en sélectionnant les icônes en haut à droite de la table : actualiser la liste,

actions sur la liste, copier l'URL pour tous les paramètres, filtrer et exporter.



- **Nom** : nom du paramètre de sécurisation renforcée de la propriété.
- **Statut de conformité** : **conforme** indique que le paramètre de sécurisation renforcée est correctement configuré ; **Non conforme** indique que le paramètre de sécurisation renforcée de la propriété n'est pas configuré conformément à la recommandation du système.
- **Impact du score** : une valeur en pourcentage de l'impact de ce paramètre de sécurisation renforcée sur votre posture de sécurité. La somme de tous les impacts de score est égale à 100 %.
- **Priorité** : valeur qui représente le niveau de criticité du paramètre : critique, élevée, modérée et faible. La relation entre l'impact du score et la priorité est la suivante : un impact de score plus élevé indique une criticité plus élevée.
- **Catégorie de sécurité** : catégorie de sécurité de la propriété.
- **Détails** de la résolution : étapes à suivre pour corriger la vulnérabilité de sécurité du paramètre de sécurisation renforcée.

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

Base de référence des paramètres de sécurisation renforcée

Découvrez comment des versions de base de référence distinctes pour les paramètres de sécurisation renforcée s'alignent sur les différentes versions de famille et de stockage.

Security Center 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 référence pour les propriétés système qui sont ingérées avec chaque version de l'application Security Center.

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 soutenues	Date de sortie de la boutique	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 (en anglais seulement)	Base de référence v2.0	Vancouver, Washington	nov. 2023	Famille Washington
SSC v1.4 (en anglais seulement)	Base de référence v4.0	Washington, Xanadu	mai 2024	Xanadu

Scanner de sécurité

Utilisez l'outil de scanner pour analyser votre instance par rapport à un ensemble de contrôles de sécurité afin d'identifier les erreurs de configuration. L'outil 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.

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

Lorsque vous accédez 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 créer vos propres vérifications et suites personnalisées.

Comparaison des scores de sécurisation renforcée

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

La page de comparaison des scores de sécurisation renforcée affiche les changements de sécurité dans vos paramètres de sécurisation renforcée entre la première et la deuxième date. Pour afficher des visualisations de ces changements, entrez une **date antérieure** et une **date récente** dans le sélecteur de date en haut à droite de la page, puis cliquez sur **Comparer**. Vous trouverez ci-dessous une explication de chaque carte :

- **Score de conformité à la sécurisation renforcée** : affiche le score de conformité de votre instance sous forme de pourcentage aux première et deuxième dates.
- **Impact du score des paramètres modifiés par priorité** : affiche le nombre de paramètres qui ont changé de priorité.
- **Impact du score des paramètres modifiés par domaine de sécurité** : affiche le nombre de paramètres qui ont changé de catégories. Par exemple, passer du **contrôle d'accès** à **la protection des données**.

- **Paramètres de sécurisation renforcée modifiés** : affiche une vue consolidée des paramètres qui ont été modifiés ainsi que leurs données de sécurité associées dans la liste. En outre, peut appliquer des fonctionnalités communes associées aux listes telles que l'actualisation, la liste des actions d'interface utilisateur, la copie d'URL, les filtres et l'exportation.

Par exemple, dans la capture d'écran suivante, le score de conformité est passé de 71 % à 73 %, ce qui indique que la posture de sécurité a été renforcée au cours de cette période.

Le nombre total de paramètres dont la priorité a changé est de quatre : deux élevés et deux modérés. En outre, le nombre de paramètres qui ont modifié la sécurité est de quatre au total : deux contrôles d'accès, une authentification et une logique métier. Les détails de sécurité de ces quatre paramètres sont également affichés dans la liste Paramètres de sécurisation renforcée modifiés. Vous pouvez afficher les paramètres non conformes et les corriger, ce qui recalculera le score de conformité à la sécurisation renforcée.

Vérifications d'analyse

Les vérifications sont des règles qui spécifient des configurations ou des activités qui ne sont pas conformes aux pratiques de sécurité. Les vérifications peuvent porter sur des tables, des enregistrements ou des métadonnées.

Les types de vérifications que vous pouvez créer sont les suivants :

- Vérification de la table
- Vérification par type de colonne
- Vérification du script uniquement
- Vérification Linter

Pour en savoir plus sur les vérifications, reportez-vous à Getting started with checks .

Lorsque vous êtes prêt à créer une vérification, cliquez sur **Nouveau**.

Créer une suite

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

Avant de commencer

Rôle requis : admin

Une suite est un ensemble de vérifications qui peuvent être utilisées pour une analyse. Affichez une liste des suites d'analyse disponibles dans votre instance, organisées dans une table, en accédant à **Scanner** > **Suites**. Vous avez la possibilité de créer vos propres suites ou d'utiliser la suite par défaut, Auditor : il s'agit d'une suite prête à l'emploi par défaut qui contient des vérifications des bonnes pratiques de sécurité. Ces vérifications concernent des propriétés système, des modules d'extension et des tables qui peuvent affecter la posture de sécurité de votre instance. Les étapes suivantes indiquent comment créer une suite, ainsi que les différentes options disponibles pour les configurer.

Procédure

1. Accédez à la **Suites** > **Nouveau**.
2. Entrez un **nom** et une **description** de suite, puis sélectionnez **Enregistrer**.
3. **Vérifications**

C’est ici que vous ajoutez des vérifications à votre suite.

a. Sélectionnez **Modifier**.

b. Sélectionnez les vérifications que vous souhaitez ajouter, puis sélectionnez Ajouter (**>**) pour les placer dans votre suite.

c. Sauvegarder.

4. **Suites enfants**
   Il s’agit de l’endroit où vous ajoutez des suites enfants ou les suites placées sous les suites parentes.

   a. Sélectionnez **Modifier**.

   b. Sélectionnez les suites enfants que vous souhaitez ajouter, puis sélectionnez Ajouter (**>**) pour la placer dans votre suite enfant.

   c. Sauvegarder.

5. **Suites parentes**
   C’est ici que vous ajoutez des suites parentes. Toutes les suites enfants sont exécutées lorsqu’une suite parente est utilisée dans une analyse.

   a. Sélectionnez **Modifier**.

   b. Sélectionnez les suites enfants que vous souhaitez ajouter, puis sélectionnez Ajouter (**>**) pour la placer dans votre suite parente.

   c. Sauvegarder.

6. **Calendrier**
   Définissez une heure d’exécution de votre suite.

   a. Sélectionnez **Nouveau**.

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

   c. Sauvegarder.

Résultats d'analyse

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

Accédez à **Conclusions** pour afficher une liste des conclusions de l’analyse sur votre instance. Sélectionnez un lien sous la colonne **Créé** pour explorer et afficher les détails granulaires associés à un résultat :

- **Vérification** : liste des vérifications associées à l’analyse.
- **Catégorie** : catégorie de sécurité associée à l’analyse. Par exemple, contrôle d’accès ou 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** : état et type de l’analyse.
- **Version** de la vérification : version modifiée de la vérification.

- **Table source** : enregistrement qui a violé une règle de la vérification.
- **Motif de désactivation** : motif de désactivation du résultat.
- **Source** : date à laquelle le résultat a été créé.
- **Tâche** : permet de faciliter les affectations de tâches à partir de la recherche d'un enregistrement.
- **Domaine** : définit ce à quoi vous pouvez et ne pouvez pas accéder.
- **Brève description** : une brève explication de l'analyse.
- **Détails de résolution** : instructions sur la façon de résoudre les problèmes d'analyse.

Mesures de sécurité

Utilisez l'outil Mesures pour surveiller plus de 50 mesures de sécurité différentes afin d'identifier les menaces de sécurité potentielles ou les comportements non sécurisés. Vous pouvez définir des seuils pour les notifications par e-mail, visualiser et analyser les données de plusieurs façons, exporter les données ou créer des tableaux de bord avec les mesures les plus importantes pour votre organisation.

Les mesures sont implémentées sous forme de visualisations du centre d'analyse qui offrent un ensemble riche de fonctionnalités, notamment l'envoi d'alertes par e-mail lorsque des seuils sont dépassés, la visualisation des cibles, ainsi que l'affichage et le filtrage des événements sous-jacents.

Tableau de bord de mes mesures de sécurité

Affichez les mesures de sécurité de votre instance à partir d'un tableau de bord unique.

Pour accéder à la page **Mesures, sélectionnez Mes mesures**. Cette page affiche le tableau de bord par défaut, mais vous pouvez également créer votre propre tableau de bord en sélectionnant **Modifier**.

Vous pouvez personnaliser votre propre 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 section Platform Analytics dashboards .

Toutes les mesures de sécurité

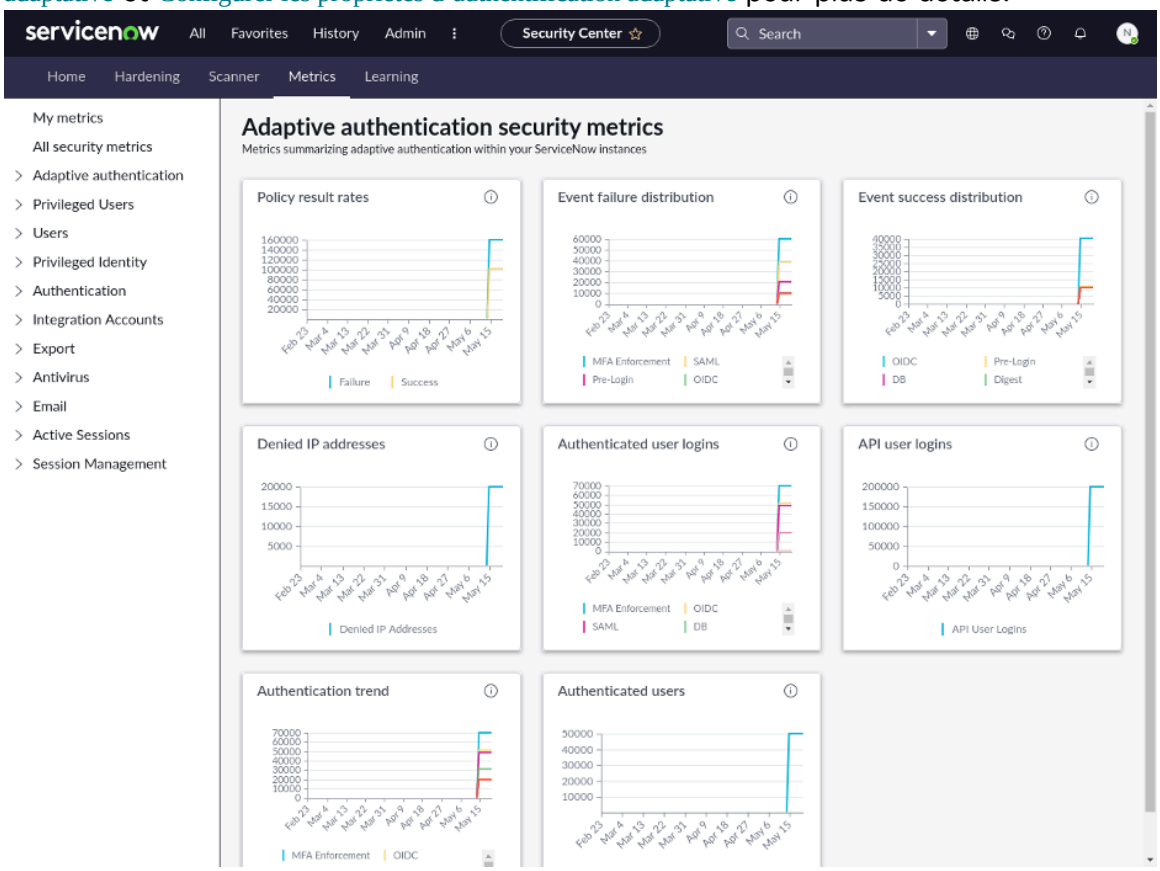
Accédez à **Toutes les mesures de sécurité** pour afficher une table contenant les données associées aux mesures de sécurité de votre instance.

Mesures de sécurité pour l'authentification adaptative

Utilisez les 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.

Les mesures d'authentification adaptative vous permettent de surveiller la façon dont l'authentification adaptative est utilisée sur votre instance. Vous pouvez afficher un résumé de toutes vos mesures sur l'authentification adaptative, ou explorer et afficher des mesures individuelles telles que les taux de résultats de politique ou les adresses IP refusées. Cette page nécessite que le module d'extension Authentification adaptative (`com.snc.adaptive_authentication`) pour l'authentification adaptative soit disponible dans votre instance. Vous devez également 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 politique : tous les événements d'authentification adaptative ayant réussi et échoué.
- Distribution des échecs d'événements : tous les événements ayant échoué pour chaque type d'événement.
- Distribution de réussite d'événement : événements réussis associés à chaque type d'événement.
- Adresses IP refusées : nombre d'adresses IP bloquées par l'instance, ainsi que leurs données associées.
- Connexions de l'utilisateur authentifiés : nombre d'événements comptabilisés 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 de l'API pour chaque type d'événement.
- Tendance d'authentification : nombre total d'événements enregistrés.
- Utilisateurs authentifiés : nombre d'utilisateurs comptabilisés pour chaque type d'événement, à l'exclusion de l'événement de préconnexion.

Utilisateurs privilégiés

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

La section Vue d'ensemble des utilisateurs privilégiés affiche la ligne de tendance des utilisateurs privilégiés (actifs et inactifs) et leur activité sur le Now 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 connectés récemment, mais qui ont toujours accès à leur compte.
- Utilisateurs verrouillés : 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 : échecs de tentatives de connexion.
- 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 réinitialisation de mot de passe pour les utilisateurs : nombre d'échecs de mot de passe par utilisateur.

Utilisateurs

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

La section Vue d'ensemble des utilisateurs affiche la ligne de tendance du nombre total d'utilisateurs (actifs et inactifs) et de leur activité sur le Now 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 connectés récemment, 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 : échecs de tentatives de connexion.
- Connexions externes : authentifications qui utilisent un tiers.
- Connexions locales non protégées par MFA : connexions qui n'utilisent pas 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 réinitialisation de mot de passe pour les utilisateurs : nombre d'échecs de mot de passe par utilisateur.

Identité privilégiée

Analyser les données relatives aux mesures pour les utilisateurs disposant d'une identité privilégiée.

Ce tableau de bord affiche les données relatives aux utilisateurs d'identité privilégiés et à leur activité sur votre instance.

- Connexions d'administration : nombre total de connexions avec des utilisateurs ayant le rôle administrateur.
- Emprunt d'identité : nombre total d'emprunts d'identité effectués par les utilisateurs disposant du rôle emprunteur d'identité.
- Altitude : nombre total d'élévations de sécurité effectuées par les utilisateurs ayant le rôle security_admin.
- Connexions ServiceNow : nombre total de connexions par les employés de ServiceNow.
- Utilisateurs administrateurs ajoutés : nombre total d'utilisateurs ayant reçu le rôle administrateur.

Mesures d'authentification

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

Affiche les données pour les mesures liées aux schémas d'authentification telles que l'utilisation de la MFA, les comptes de services Web et l'utilisation des scanners biométriques.

- Utilisateurs inscrits pour MFA : nombre total d'utilisateurs inscrits pour utiliser MFA.
- Utilisateurs utilisant le contournement de la 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 l'authentification MFA.
- Utilisateurs de MFA actifs : nombre total d'utilisateurs de MFA actifs sur votre instance.
- Utilisateurs de MFA bloqués : nombre total d'utilisateurs de MFA qui sont verrouillés sur votre instance.
- Utilisateur du 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 qui arrivent à expiration dans les 30 prochains jours.

Comptes d'intégration

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

Le tableau de bord des comptes d'intégration affiche les tendances relatives aux comptes d'intégration créés sur le Now Platform.

Vous trouverez ci-dessous des explications sur les métriques des comptes d'intégration :

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

Exporter

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

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

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.

- Fichiers mis en quarantaine : nombre de fichiers susceptibles de contenir des programmes malveillants.
- Fichiers téléchargés : nombre de fichiers téléchargés.
- Fichiers restaurés : nombre de fichiers qui ont été restaurés.
- Fichiers supprimés : nombre de fichiers supprimés.

E-mail

Affiche les données relatives aux courriers indésirables reçus en externe.

Les spams représentent le nombre de courriers indésirables reçus par jour.

Sessions actives

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

La ligne de tendance peut être affichée pour les mesures suivantes :

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

Gestion des sessions

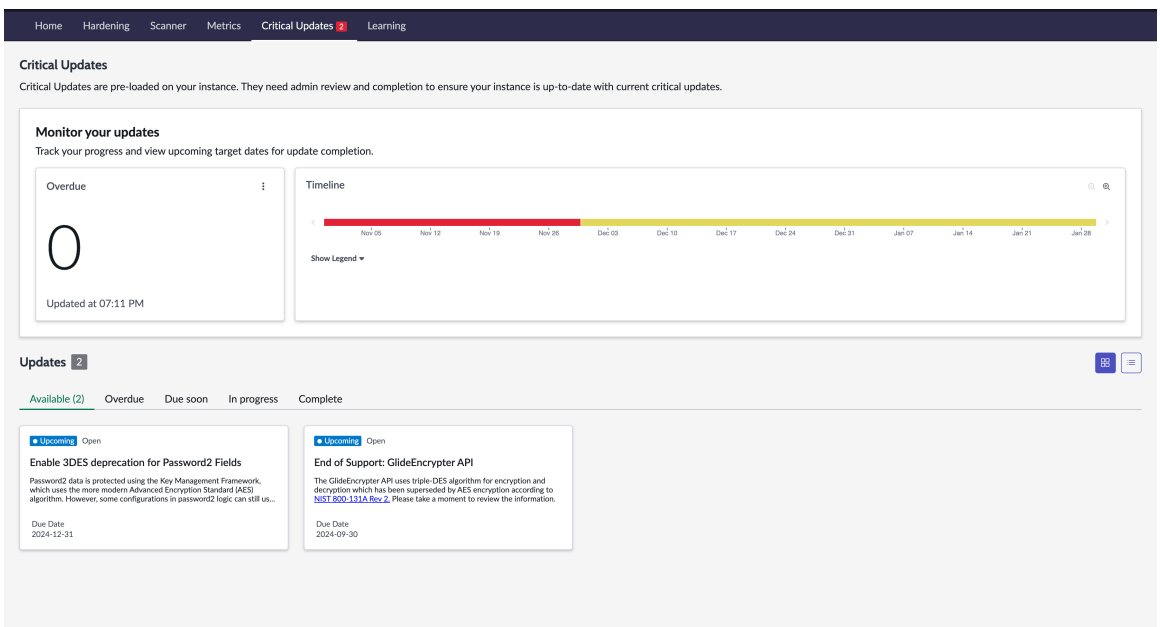
Affichez les mesures associées aux sessions utilisateur et à la fréquence des verrouillages des sessions.

Mises à jour essentielles

Renforcez la posture de sécurité de votre instance en vous assurant que les mises à jour critiques recommandées par le système sont implémentées à temps.

Critical Updates est un outil qui aide les administrateurs à implémenter des mises à jour de sécurité importantes en fonction de leur instance et de la configuration des modules d'extension. Une mise à jour critique est un changement recommandé sur une instance qui vise à vous aider à comprendre l'importance des changements liés à la sécurité. Les mises à jour critiques vous aident à mettre en œuvre les étapes pour analyser, mettre à jour et tester les mises à jour de sécurité sur votre instance. Implémentez une mise à jour critique pour éviter d'interférer avec la personnalisation de votre instance. Les mises à jour critiques implémentées manuellement sont différentes des mises à jour automatiques rendues sur votre instance au code ou aux fonctionnalités ServiceNow avec des versions de famille ou des correctifs.

Sur la page d'accueil des mises à jour critiques, vous pouvez voir la chronologie des mises à jour critiques afin que vous puissiez classer par ordre de priorité le moment de l'implémentation des étapes. La chronologie de la capture d'écran affiche les mises à jour critiques en retard et celles à échéance prochainement. En outre, vous pouvez suivre la progression de vos mises à jour critiques sous l'étiquette Mises à jour. Sélectionnez les onglets pour afficher les mises à jour critiques disponibles, en retard, à échéance prochainement, en cours ou terminées.



Traduction automatique

Premiers pas :

- Accédez à cet outil en accédant aux **mises à jour critiques** dans Security Center.
- Les mises à jour critiques sont incluses dans l'application Security Center à partir de Washington DC.

Implémenter des étapes pour les mises à jour critiques

Découvrez comment implémenter des mises à jour critiques sur votre instance afin d'améliorer sa posture de sécurité.

Avant de commencer

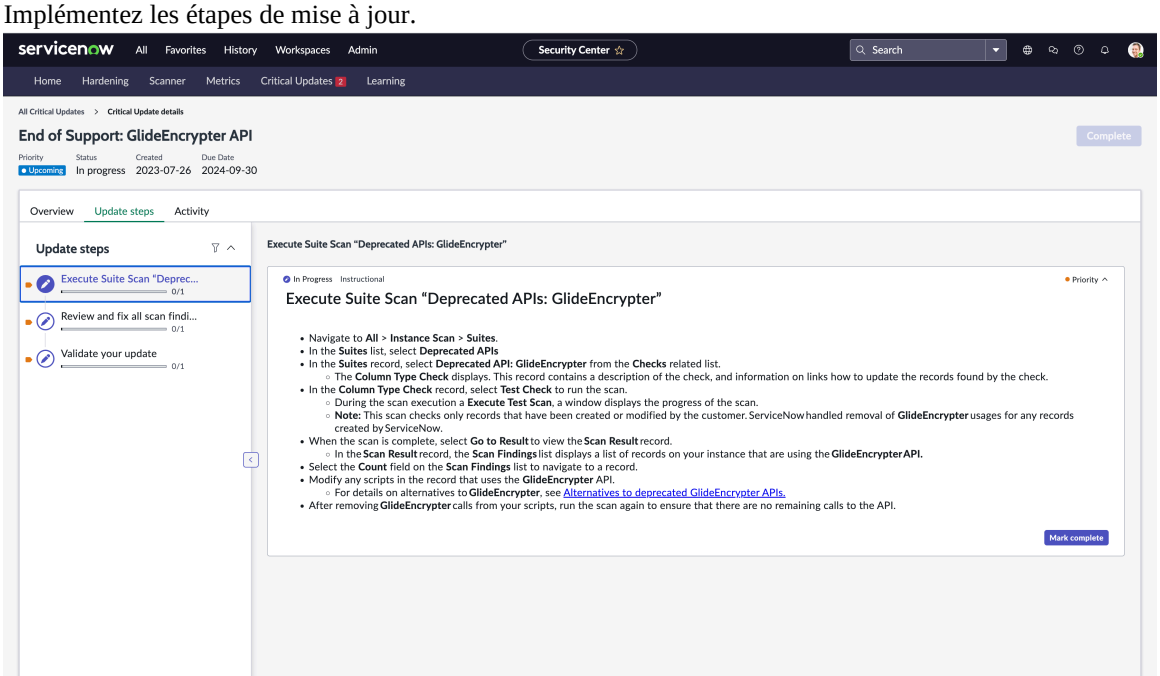
Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les mises à jour critiques (CU) vous fournissent des instructions étape par étape sur la façon d'implémenter les changements sur votre instance afin d'améliorer votre posture de sécurité. CU extrait le contenu pertinent de la documentation du produit pour vous guider à chaque étape du processus d'implémentation. Suivez les étapes ci-dessous pour savoir comment implémenter une mise à jour critique.

Procédure

1. Accédez à l'application Critical Updates (**Mises à jour essentielles**).
2. Cliquez sur une mise à jour critique pour l'implémenter.
   Dans la section **Mises à jour** , l'onglet Disponible répertorie toutes les mises à jour critiques sur votre instance. Cliquez sur une mise à jour critique sous cet onglet pour afficher les instructions.
3. Lisez la présentation pour découvrir pourquoi la mise à jour critique est nécessaire et pour vous préparer à son implémentation.
   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.

Traduction automatique

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**.
La mise à jour critique ne doit plus être disponible dans la section Mises à jour de la page d'accueil des mises à jour critiques.

Afficher l'activité des mises à jour critiques

Consultez les détails de toutes les activités liées à vos mises à jour critiques.

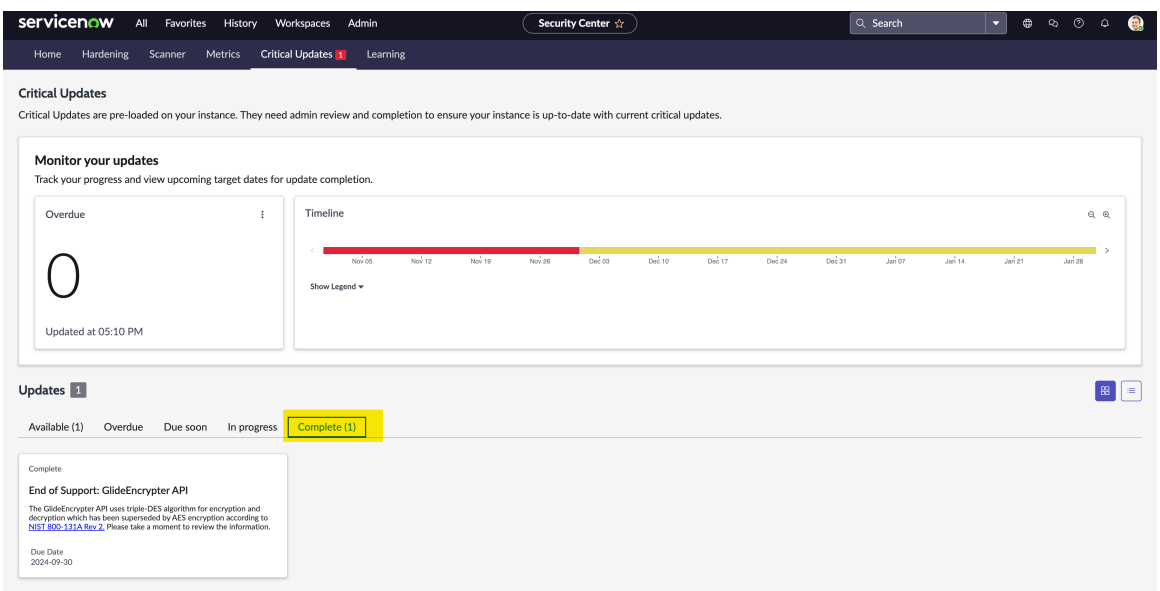
Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Les activités sont répertoriées de la plus récente à la plus ancienne afin que vous puissiez analyser l'activité la plus récente en premier. Chaque mise à jour d'une activité est horodatée, et vous pouvez utiliser la recherche et le filtre pour interroger des informations spécifiques.

Procédure

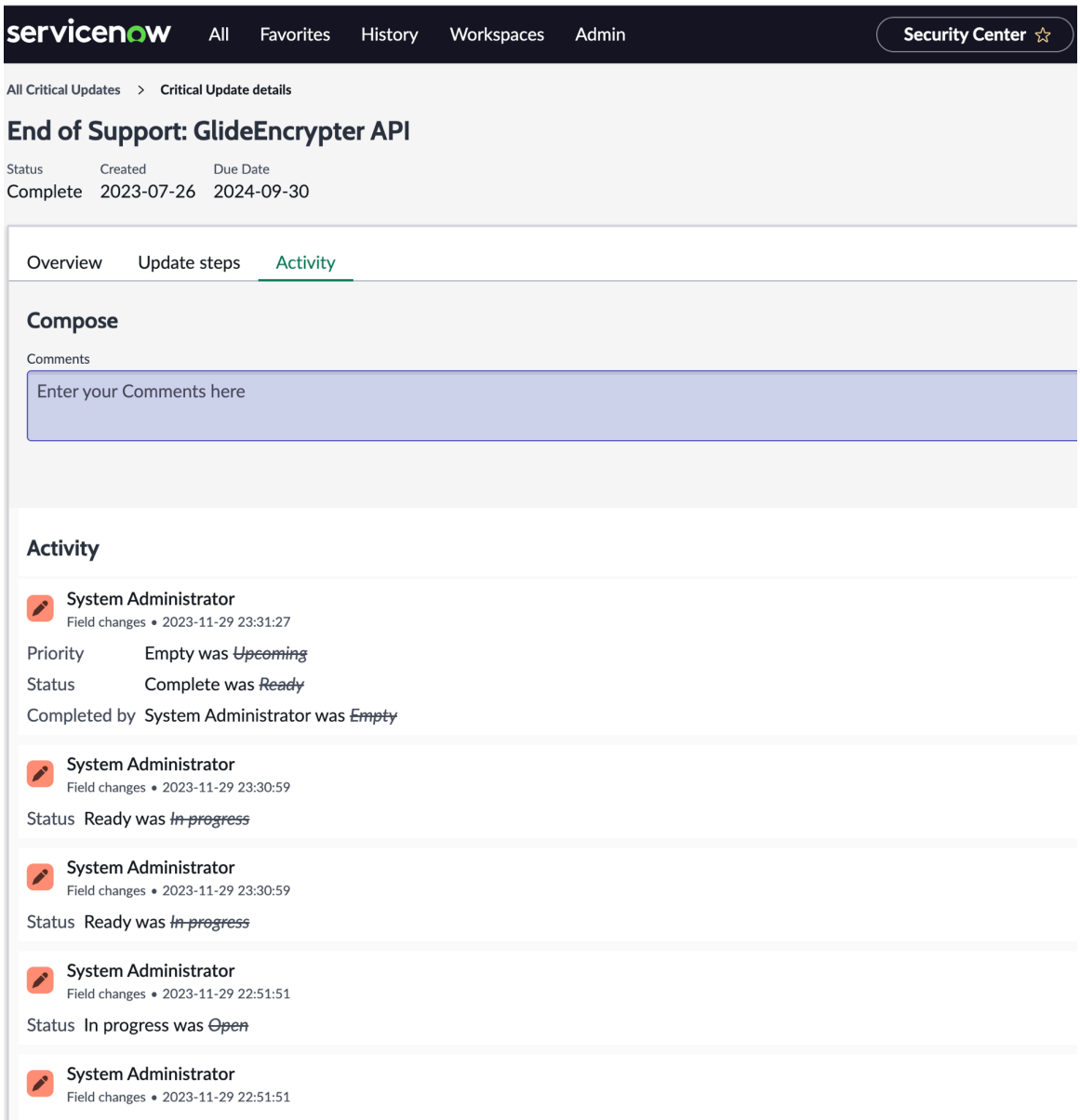
1. Accédez à l'application **Mises à jour critiques** dans Security Center.
2. Accédez à l'étiquette**Mises à jour** des mises à jour critiques.
3. Cliquez sur un état, puis sélectionnez une mise à jour critique à partir de cet état.

   Dans l'exemple ci-dessous, l'état **Terminé** est sélectionné, puis la mise à jour critique pour **Fin de prise en charge : API GlideEncrypter** est sélectionnée.



4. Affichez l'activité de votre mise à jour critique.

Traduction automatique



Toutes les activités liées à une mise à jour critique sont automatiquement enregistrées. De plus, vous avez la possibilité d'ajouter des commentaires supplémentaires aux activités.

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 la base de connaissances, de la documentation produit et des discussions Community à partir d'une vue consolidée en accédant à **Learning**. Le contenu est organisé par en-têtes et cartes d'interface utilisateur descriptives pour vous permettre d'identifier rapidement la ressource appropriée.

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 depuis Instance

Security Center. Instance Security Center consolide plusieurs composants de sécurité clés en une console de contrôle unique qui vous aide à détecter, protéger et répondre aux événements de sécurité basés sur l'instance.

Vue d'ensemble du Centre de sécurité de l'instance

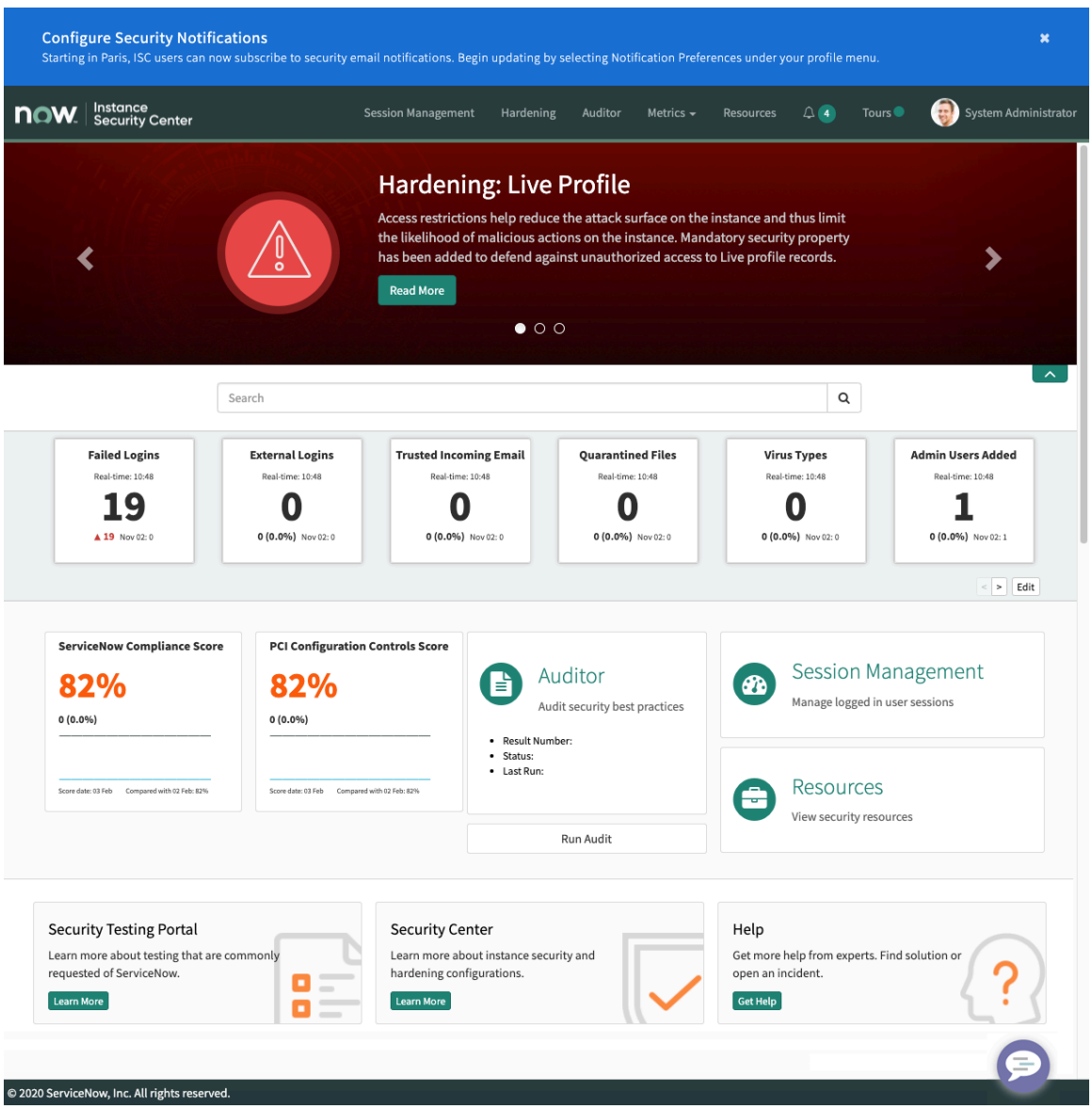
Remarque :

Le Centre de sécurité de l'instance sera prochainement obsolète. Ce module d'extension sera masqué et ne sera plus activé sur les nouvelles instances, mais continuera d'être pris en charge. ServiceNow Security Center fournit la dernière expérience pour cette fonctionnalité.

Pour en savoir plus, consultez l'article Processus de retrait dans la base de connaissances Now Support.

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 de l'administration système.



Traduction automatique

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 sécurité
- Centre de sécurité
- Aide
- Accès à Virtual Agent

Depuis la page d'accueil d'Instance Security Center, vous pouvez afficher le score de conformité de sécurité pour 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 :
Instance Security Center ne prend pas en charge Domain Separation.

Rôles d'utilisateur

Pour utiliser Instance Security Center, 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 rôle.	Utilisez des Security Center outils pour améliorer la posture de sécurité de l'instance et surveiller les comportements liés à la sécurité.

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 Security Center les outils, mais pas de les modifier ou de modifier les Security Center configurations d'instance en exploitant les Security Center outils. Par exemple, les propriétaires de plateformes, les analystes des opérations de sécurité ou les parties prenantes de la conformité peuvent souhaiter ou avoir besoin de consulter certains des KPI de sécurité, des informations de sécurité et du matériel d'apprentissage sur la sécurité disponibles dans Security Center.	Gagnez en visibilité sur Security Center les outils permettant de surveiller la posture de sécurité des instances et de surveiller les comportements de sécurité.

Avertissement :
Pour vous assurer que 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

Les messages et rappels, destinés principalement aux administrateurs, s'affichent au-dessus de la bannière de sécurité rotative.

Par exemple, un message Configurer les notifications de sécurité apparaît pour rappeler aux administrateurs de configurer les préférences pour les notifications de sécurité s'ils ne l'ont pas déjà fait. Il les dirige également vers la page appropriée pour le faire.

Remarque :
La bannière de messages de l'administrateur ne s'affiche pas pour les utilisateurs non administrateurs, ou s'il n'y a pas d'éléments actionnables pour les utilisateurs administrateurs.

Bannière de sécurité rotative

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

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

Les couleurs d'arrière-plan de la bannière indiquent la sévérité 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'informations générales.

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

- Lorsque vous utilisez à nouveau Instance Security Center, le contenu textuel apparaît comme réduit ou développé, selon l'utilisation que vous en avez faite au cours de votre session précédente.
- Si le contenu du texte lui-même change, il apparaît comme agrandi pour tous les utilisateurs.

Rechercher

Utilisez la barre de recherche pour rechercher dans l'ensemble d'Instance Security Center 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 Actualités
- 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 parcourir 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, consultez Surveiller les événements de sécurité et Configurer le ruban des événements de sécurité.

Score de conformité quotidien

La section Score de conformité quotidien contient les vignettes **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. Il est basé sur la conformité des paramètres actuels des propriétés de sécurité de votre instance avec les valeurs de conformité publiées dans le Paramètres de la sécurisation pour la sécurité de l'instance.

- Pour en savoir plus sur les calculs du score de conformité quotidien et sur l'impact des paramètres de sécurisation renforcée sur celui-ci, reportez-vous à Vérifier le score de conformité quotidien et configurer les paramètres de propriété de sécurité.
- Le bouton **Actualiser** permet à un administrateur de recalculer instantanément le score de conformité quotidien. Pour en savoir plus, consultez Mode d'actualisation des données quotidiennes de score, de tendance et de graphique de conformité.

Sécurisation renforcée

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

1. Pour accéder à la page Configurations de la conformité à la sécurisation renforcée et effectuer le renforcement de la sécurité de l'instance, sélectionnez la vignette **Score de conformité quotidien** ou le lien **de sécurisation renforcée** .
2. Spécifiez si vous souhaitez afficher tous les contrôles de sécurité recommandés ou uniquement ceux recommandés. Ensuite, sélectionnez 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 les informations détaillées d'une propriété.

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

Pour en savoir plus sur la façon dont les données de tendance et de graphique sont actualisées, reportez-vous à Mode d'actualisation des données quotidiennes de score, de tendance et de graphique de conformité.

Auditeur

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

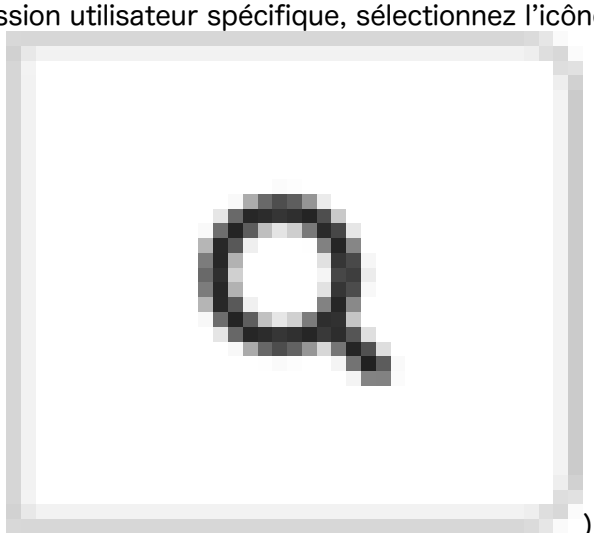
Pour accéder à la page Auditeur, sélectionnez la vignette **Auditeur** ou le lien **Auditeur** . Pour en savoir plus, consultez Rechercher les définitions de sécurité incorrectes.

Gestion des sessions

Utilisez Gestion des sessions pour :

- Afficher et gérer les sessions de connexion de l'utilisateur.
- Affichez la session de connexion de l'utilisateur du nœud actuel auquel vous êtes connecté.
- Consultez des informations détaillées sur chaque session, telles que le nom d'utilisateur et l'adresse IP.
- Isolez et verrouillez les 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, mot clé de l'agent utilisateur ou adresse IP. Par exemple, si vous souhaitez trouver toutes les connexions actuelles à partir d'un type de navigateur spécifique, 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 de 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	Case à cocher indiquant si l'authentification multifacteur (MFA) est activée pour l'utilisateur connecté. Pour en savoir plus sur l'authentification multifacteur, consultez Authentification multifacteur (MFA).
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.

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 accéder à la page Mesures utilisateur, cliquez sur le lien **Mesures** , puis sélectionnez **Mesures utilisateur**.
Exporter	Mesures de sécurité associées aux données exportées à partir de l'instance. Pour accéder à la page Exporter les mesures, sélectionnez le lien **Mesures** , puis sélectionnez **Exporter les mesures**.
Authentification	Mesures de sécurité associées à l'authentification, telles que les adresses IP peu utilisées, les échecs de connexion et les types de schémas d'authentification utilisés par vos utilisateurs. Pour accéder à la page Exporter les mesures, cliquez sur le lien **Mesures** , puis sélectionnez **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 le lien **Métriques** , puis sélectionnez **Antivirus**.

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

Ressources

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

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

Catégorie	Description
Directives recommandées	Accès aux directives de sécurité recommandées, y compris les articles du Paramètres de la sécurisation pour la sécurité de l'instanceGuide de codage sécurisé [KB0623354].
Ressources de sécurité	Accès aux ressources liées à la sécurité dans , notamment Base de connaissances: ○ 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 cloche de notifications ( ) apparaît dans Instance Security Center, avec un décompte total de notifications de sécurité non lues. Les notifications sont conservées et incluses dans ce nombre 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 de connexion d'administrateur, d'administrateurdéverrouillé**, **d'échec de connexion**, de **rôle de privilège élevé**, d'emprunt **d'identité**, **d'élévation de la sécurité** et **de synthèse hebdomadaire** ont lieu dans votre instance. Pour en savoir plus sur ces événements de sécurité, reportez-vous à 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). Utilisez cette table pour voir quels utilisateurs ont été affectés à des rôles privilégiés au cours d'un jour de calendrier. Cet historique vous aide à déterminer si les rôles ont été affectés correctement.

3. S'il y a 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'événement de sécurité.

Visites guidées

Cliquez sur le lien **Visites guidées** pour afficher une visite visuelle guidée d'Instance Security Center.

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

Portail de test de sécurité, centre de sécurité et aide

Il Now Support Portail de services s'agit 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 **Obtenir de l'aide** dans les vignettes suivantes :

Mosaïque	Description
Portail de test de la sécurité	Accès au tableau de bord de sécurité dans le portail de test de Now Support 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 sécurité Now Support : • Demandez à un expert de trouver des réponses aux questions les plus fréquentes. • Signalez un problème ou une panne à l'assistance ServiceNow technique globale en ouvrant un ticket. • Ressources d'assistance en libre-service, y compris : ◦ 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 Virtual Agent

Il Agent virtuel s'agit d'une plate-forme permettant de fournir une assistance utilisateur 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 Virtual Agent :

Il vous permet d'effectuer les tâches suivantes :

- Posez des questions liées à la sécurité, puis obtenez rapidement des réponses récapitulatives et des liens de référence pour en savoir plus.
- Obtenez des réponses relatives 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 Now Support rubriques du portail de sécurité.

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

- Agent virtuel
- Activer l'interface ISC Agent virtuel

Migration d'Instance Security Center vers ServiceNow Security Center

Découvrez les principales différences lors de la migration d'Instance Security Center (ISC) vers ServiceNow Security Center (SSC).

ServiceNow Security Center (SSC) est une nouvelle application de sécurité qui se compose d'un ensemble d'outils spécialement conçus pour aider les organisations à maintenir la sécurité de leurs déploiements ServiceNow. À l'aide de Security Center, les entreprises peuvent améliorer leur posture de sécurité et renforcer leurs niveaux de conformité à l'aide d'une expérience utilisateur transparente. Centre de sécurité de l'instance (ISC) est le produit hérité ; ServiceNow mettra fin à la prise en charge d'ISC avec la sortie de Now Platform Xanadu, prévue pour septembre 2024. Par conséquent, SPC est la solution recommandée à adopter à l'avenir.

Mises à jour des paramètres de sécurisation renforcée pour SPC

Découvrez les mises à jour apportées aux paramètres de sécurisation renforcée dans ServiceNow Security Center (SSC).

Améliorations des fonctionnalités	ISC par rapport à SPC
Paramètres de sécurisation renforcée étendus	La SSC contient un nombre beaucoup plus important de paramètres de sécurisation renforcée que les versions précédentes d'ISC. Les futures versions de SPC continueront d'augmenter le nombre de paramètres.
Notation simplifiée des paramètres de sécurisation renforcée	• ISC utilise une formule qui garantit un pourcentage d'impact spécifique pour les paramètres élevé, moyen et faible. • SPC utilise une formule différente :

Traduction automatique

Améliorations des fonctionnalités	ISC par rapport à SPC
	○ Chaque paramètre a son propre poids de score. ○ Le score de conformité à la sécurisation renforcée est calculé en divisant le numérateur (somme de tous les paramètres conformes) par le dénominateur (somme des poids d'impact pour tous les paramètres).
Expérience utilisateur améliorée pour l'évaluation des données	• Comparez les scores de conformité sur deux dates différentes. • Visualisez les scores de conformité sur un graphique linéaire et analysez les données à l'aide du Centre d'analyse.

Effectuer des tâches courantes de renforcement de la sécurité dans SPC

Voici des instructions pour effectuer des tâches courantes de renforcement de la sécurité dans SPC.

Passer en revue le dernier score	Accédez à l'un des modules suivants : • **Accueil** Consultez Page d'accueil. • **Score de > de sécurisation renforcée** Consultez Tendance du score de conformité à la sécurisation renforcée.
Mettre à jour le dernier score	Sur la page d'accueil de SSC, sélectionnez **Mettre à jour le score**.
Modifier la configuration du paramètre	Sélectionnez un nom de paramètre sur l'une des pages suivantes pour afficher les pages de détails des paramètres, où vous pouvez modifier la configuration, afficher les activités précédentes et ajouter des notes : • Accueil • Sécurisation renforcée > Tous les paramètres • Comparaison des scores de > de sécurisation renforcée Reportez-vous à la rubrique Augmenter le score de conformité à la sécurisation renforcée.
Définir un calendrier pour le recalcul de votre score de conformité	Pour planifier le moment où le système déclenche une actualisation de votre score de conformité :

Traduction automatique

- Dans la table sysauto_script , filtrez par SC - Calculer la conformité mensuellement.
- Modifiez l'enregistrement pour refléter le calendrier préféré.

Mises à jour des KPI et des mesures de sécurité pour SPC

Découvrez les mises à jour apportées aux KPI et mesures de sécurité dans ServiceNow Security Center (SSC).

Améliorations des fonctionnalités	ISC par rapport à SPC
Améliorations apportées aux KPI	Dans SPC, vous pouvez : • Voir la tendance du score dans le temps. • Surveillez tous les KPI et mesures à l'aide de la même interface et des mêmes capacités d'analyse.
Améliorations apportées aux mesures	À SPC, les améliorations suivantes ont été apportées : • Plus de 50 nouvelles mesures ont été ajoutées. • Vous pouvez surveiller et analyser les KPI et les mesures à partir de la même interface utilisateur. • Vous pouvez créer des cibles et des seuils pour les mesures.

Accéder aux KPI et aux mesures de sécurité dans SPC

Effectuez l'une des actions suivantes :

- Accédez à la **Accueil** > **Mesures**, puis sélectionnez **Mesures** dans le menu de navigation de gauche.
- Accédez à la **Accueil** > **Toutes les mesures**, puis sélectionnez Mesures dans la table.

Mises à jour des analyseurs de sécurité dans SPC

Découvrez les mises à jour apportées au scanner de sécurité dans ServiceNow Security Center (SSC).

Améliorations des fonctionnalités	ISC par rapport à SPC
Nouvelle fonctionnalité	SPC comprend les nouvelles fonctionnalités suivantes : • Exécutez manuellement les analyses ou planifiez-les pour qu'elles s'exécutent à des moments spécifiques. • Créez vos propres vérifications d'analyse.

Améliorations des fonctionnalités	ISC par rapport à SPC
	• Créez votre propre suite d'analyse. • Comparez les résultats de deux analyses.
Amélioration de la fonctionnalité de messagerie	Configurez des notifications par e-mail afin d'être alerté des nouveaux événements de sécurité sur votre instance.

Effectuer des tâches courantes d'analyse de sécurité dans SPC

Voici des instructions pour l'exécution des tâches courantes de l'analyseur de sécurité dans SPC.

Exécuter l'analyse de la suite Auditor	**1.** Accédez à la **Scanner** > **Suites**. **2.** Sélectionnez la suite Auditor dans la liste. **3.** Sélectionnez **Exécuter l'analyse de sécurité**.
Afficher les résultats de l'analyse de la suite	Accédez à la **Scanner** > **Résultats**.

Nouvelles fonctions de sécurité dans SPC

Découvrez les nouvelles fonctionnalités de sécurité introduites dans ServiceNow Security Center (SSC).

Les nouvelles fonctionnalités suivantes ont été ajoutées à ServiceNow Security Center.

- Surveiller les sessions : vous pouvez visualiser les activités de session dans le temps à l'aide du nouvel outil Mesures.
- Trouver des ressources : toutes les ressources d'apprentissage sur la sécurité sont désormais regroupées sur une seule page.

Utiliser les nouvelles fonctions de sécurité de SPC

Surveiller l'activité de la session	**1.** Accédez à **Mesures**. **2.** Dans le volet de navigation de gauche, sous Gestion des sessions, sélectionnez **Session active**.
Accéder à des ressources d'apprentissage	Accédez à **Apprentissage**.

Surveiller les événements de sécurité

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

Dans le ruban de l'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 nombre de scores uniques en temps réel s'affiche, indiquant le nombre de fois où 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 graphiques et de tendance de conformité sur une plage de dates. Ces informations sont mises à jour quotidiennement lorsque vous exécutez la tâche Performance Analytics. Pour en savoir plus, consultez la section **Analyse des détails de 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 de l'événement pour les faire défiler. Pour apprendre à configurer le ruban d'événement, reportez-vous à la section Configurer le ruban des événements de sécurité.

Préférence de notification	Description
Connexions des administrateurs	Nombre de tentatives de connexion dans cette instance, au cours du jour du calendrier, par les utilisateurs auxquels un rôle administrateur a été affecté.
Utilisateurs administrateurs ajoutés	Nombre d'utilisateurs avec un rôle administrateur qui ont été ajoutés dans cette instance au cours du jour du calendrier. 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 d'administrateur affecté.
E-mail entrant externe	Pour en savoir plus, consultez Mesures d'e-mail.
Connexions externes	Nombre d'utilisateurs à qui un rôle de snc_external affecté se sont connectés à cette instance au cours de la journée du calendrier. Ces connexions sont généralement effectuées à des fins de maintenance, d'assistance, de conseil ou d'audit. La surveillance de cette mesure vous permet de vérifier que les tentatives de connexion externe sont légitimes et ne posent pas de problèmes de sécurité potentiels. Pour en savoir plus sur l'affectation de rôles d'utilisateur externe, reportez-vous à Explicit Roles.
Échecs de connexion	Nombre de tentatives de connexion ayant échoué dans cette instance au cours de la journée du calendrier. Cette mesure peut indiquer que des tentatives de connexion sont effectuées et compromettre la sécurité de votre instance.
Emprunts d'identité	Nombre de connexions d'emprunt d'identité dans cette instance au cours d'un jour calendaire. Pour en savoir plus sur l'emprunt d'identité d'utilisateurs, voir Emprunter l'identité d'un utilisateur .

Préférence de notification	Description
Fichiers en quarantaine	Nombre de fichiers qui ont été mis en quarantaine lors de votre exécution Analyse anti-virus dans cette instance au cours de la journée civile. Pour en savoir plus sur les fichiers mis en quarantaine et Analyse anti-virus, consultez Mesures antivirus et Analyse anti-virus.
Élévations de la sécurité	Nombre de fois où un administrateur de sécurité a élevé la sécurité des utilisateurs standard en remplaçant le rôle d'utilisateur qui lui est affecté par un rôle de sécurité avec des privilèges élevés au cours d'un jour civil. Ces rôles de sécurité à privilège élevé comprennent oauth_admin, admin, security_admin et emprunteur d'identité. • Cette mesure indique que quelqu'un a peut-être essayé d'améliorer la sécurité d'un utilisateur non autorisé. N'utilisez pas cette mesure seule pour détecter une compromission de sécurité spécifique. Au lieu de cela, traitez 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 Élever à un rôle privilégié et Rôles de privilège élevé.
Connexions SNC	Nombre de membres du Service et assistance client personnel qui se sont connectés à cette instance à l'aide de la technique de saut hi-hop au cours de la journée civile. Ces connexions sont généralement effectuées à des fins de maintenance, d'assistance, de conseil ou d'audit. Pour plus d'informations sur la façon de contrôler ServiceNow l'accès 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 différents types d'événements antivirus qui se sont produits dans cette instance au cours de la journée civile. Pour en savoir plus sur les types d'événements antivirus, consultez Mesures antivirus.

Analyse des détails de tendance d'un événement

Pour afficher les détails de la tendance d'une mesure d'événement, cliquez sur le nombre d'événements pour accéder à la page 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 échouée 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 échouées.
- Le détail inclut 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 Centre d'analyse afin de 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 infructueuses ou plus se produisent au cours de la journée, une alerte est envoyée au personnel de sécurité spécifique. Vous pouvez également définir une cible similaire qui fournit un point culminant visuel lorsque Centre d'analyse 10 connexions échouées se produisent au cours d'une journée.

Les données et les graphiques de tendance qui s'affichent dans la vignette du ruban d'événement Centre d'analyse et qui sont mis à jour après l'exécution de la tâche d'analyse des performances à 02h00, heure locale. Pour en savoir plus, consultez Mode d'actualisation des données quotidiennes de score, de tendance et de graphique de conformité.

Information associée

Centre de sécurité de l'instance

Now Intelligence

Centre d'analyse

Cibles et seuils Performance Analytics

Configurer le ruban des événements de sécurité

Configurez le ruban des événements de sécurité sur la page d'accueil d'Instance Security Center pour inclure uniquement les événements pertinents pour le suivi de la sécurité de l'instance dans vos opérations. Vous pouvez également modifier l'ordre dans lequel les vignettes d'événements de sécurité s'affichent sur le ruban.

Avant de commencer

Rôle requis : security_dashboard_user ou admin

Pourquoi et quand exécuter cette tâche

Le ruban des événements de sécurité est initialement renseigné avec un ensemble complet d'événements de sécurité standard. Vous pouvez le 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 administrateur, Utilisateurs administrateurs ajoutés et Élévations de sécurité.
- Ces indicateurs surveillent le nombre de fois où les utilisateurs disposant du rôle administrateur ont tenté de se connecter et, si des utilisateurs administrateurs ont été ajoutés, les tentatives effectuées pour élever les rôles de sécurité.

Remarque :
Pour en savoir plus sur les types d'événements de sécurité qui s'affichent 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'affichage 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'événements du Centre de sécurité de l'instance.
   - Les événements que vous placez en haut de la colonne **Disponible** s'affichent par séquence, en commençant par le côté gauche du ruban des événements du Centre de sécurité de l'instance. Les événements placés vers le bas de la colonne s'affichent à droite sur le ruban de l'événement.
4. Pour supprimer des événements de sécurité du ruban d'événement :
   - Dans la colonne **Sélectionné** , sélectionnez les événements de sécurité que vous souhaitez supprimer du ruban d'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'événement 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 Mobileou 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). Chaque utilisateur doit configurer ses propres paramètres. Pour plus d'informations, consultez Notifications dans les applications de messagerie .

Rôle requis : admin.

Procédure

1. Sur la page d'accueil d'Instance Security Center, 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 de notification sélectionné chaque fois que d'autres utilisateurs ayant des rôles d'administrateur affectés se connectent à cette instance à partir d'une adresse IP différente.
Déverrouillage administrateur	Envoyer le type de notification sélectionné chaque fois qu'un compte d'utilisateur avec privilèges élevés a été déverrouillé.
Échec de la connexion	Envoyez le type de notification sélectionné 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 Spécifier le verrouillage en cas d'échec de tentative de connexion.
Rôle HP ajouté	Envoyez le type de notification sélectionné chaque fois qu'un rôle de sécurité à privilège élevé (y 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 Élever à un rôle privilégié et Rôles de privilège élevé.
Emprunt d'identité	Envoyez le type de notification sélectionné chaque fois qu'un autre utilisateur emprunte votre identité. Pour en savoir plus sur l'emprunt d'identité d'utilisateurs, voir Emprunter l'identité d'un utilisateur .
Élévation de la sécurité	Envoyez le type de notification sélectionné chaque fois que d'autres utilisateurs sont élevés à un rôle d'administrateur de sécurité dans cette instance.
Résumé hebdomadaire	Envoyer une synthèse hebdomadaire sur le type de notification sélectionné. Il comprend :

Préférence de notification	Description
	○ Un résumé de toutes les activités de sécurité qui ont eu lieu dans cette instance tout au long de la semaine. ○ Le score de conformité quotidien actuel pour l'instance.

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

3. Cliquez sur **Enregistrer**.

Vérifier le score de conformité quotidien et configurer les paramètres de propriété de sécurité

Passez en revue 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.

Le score de conformité quotidien est un score en pourcentage. Il est basé sur la conformité des paramètres actuels des propriétés de sécurité de votre instance avec les valeurs de conformité publiées dans le Paramètres de la sécurisation pour la sécurité de l'instance.

Examinez régulièrement le score de conformité quotidien de votre instance. Suivez ces directives 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.
- Un taux inférieur à 50 % indique un faible niveau de conformité en matière de 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 respectant les exigences de sécurité de votre entreprise.

Avant de commencer

Rôle requis : security_dashboard_user ou admin.

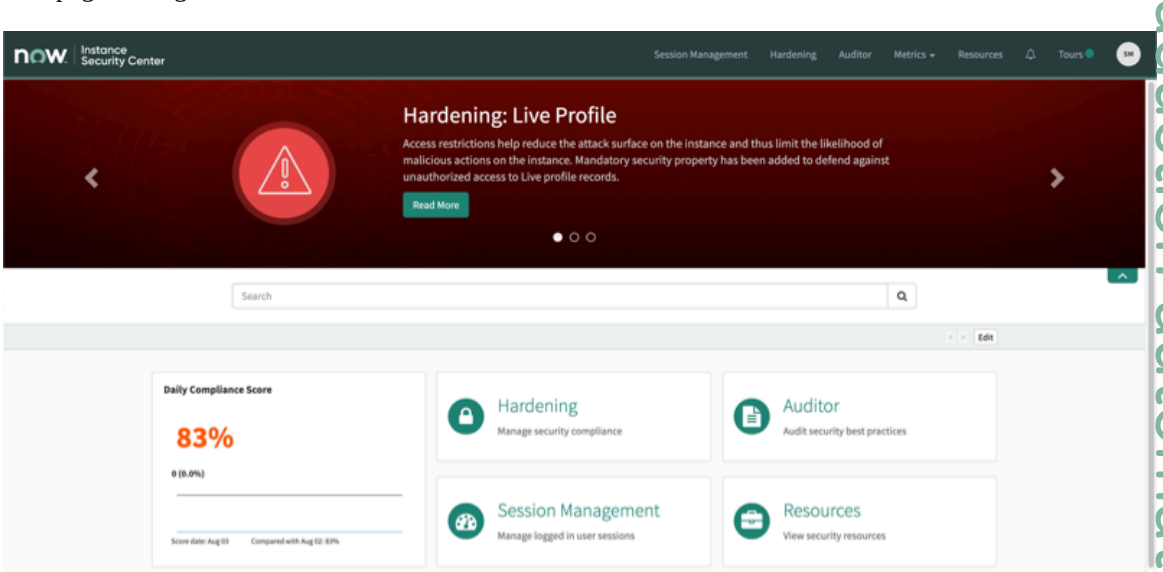
Consultez le Paramètres de la sécurisation pour la sécurité de l'instance contenu pour obtenir des descriptions détaillées et les valeurs de conformité des propriétés système et des modules d'extension liés à la sécurité dans le Now Platform.

- 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 de 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

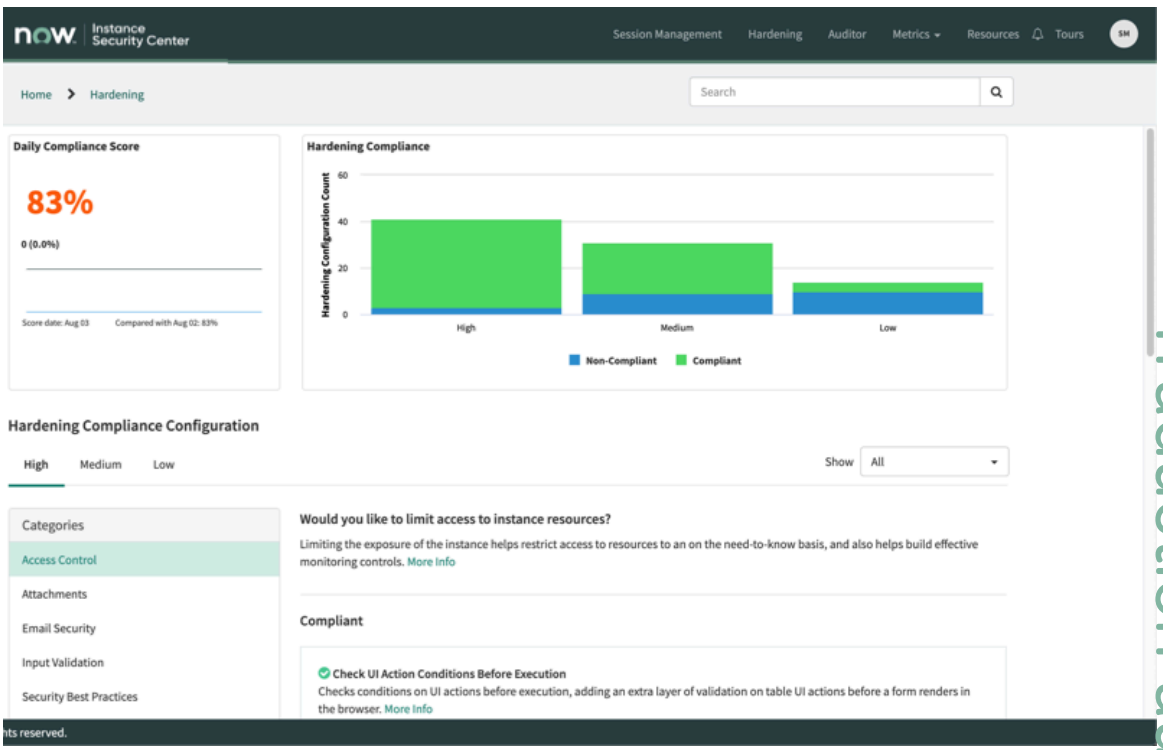
1. Accédez à la **Tous** > **Sécurité de système** > **Centre de sécurité de l'instance**.
2. Cliquez sur la vignette **Score de conformité quotidien** ou sur le lien **de sécurisation renforcée** pour accéder à la page Configuration de la conformité à la sécurisation renforcée.



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

Option	Description
Conforme	Nombre de propriétés de configuration de sécurité conformes aux valeurs de conformité 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. Pour ce faire, vous devez les mettre à jour dans les propriétés système. Pour en savoir plus, reportez-vous à la rubrique Ajouter une propriété système .

Option	Description
Non conforme	Nombre de propriétés de configuration de sécurité qui ne respectent pas les 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.

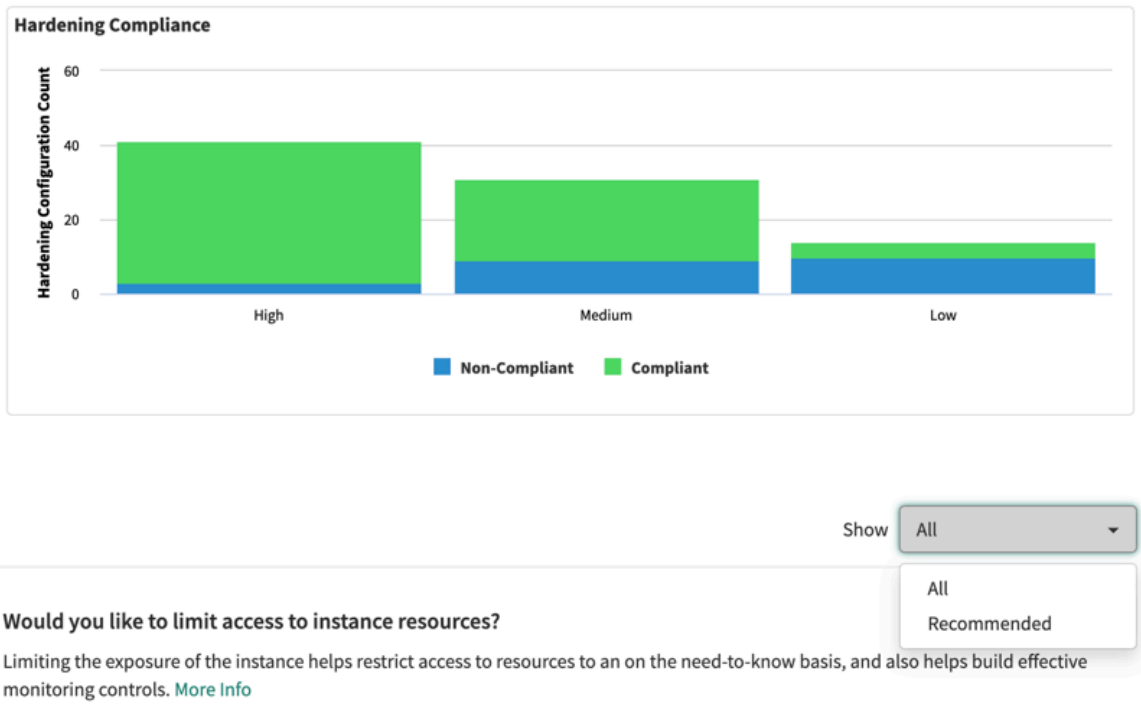


Remarque :
Pour afficher le nombre de scores de sécurité conformes ou non conformes sur une plage de dates, déplacez le point bleu sur le curseur sous le score de conformité quotidien.

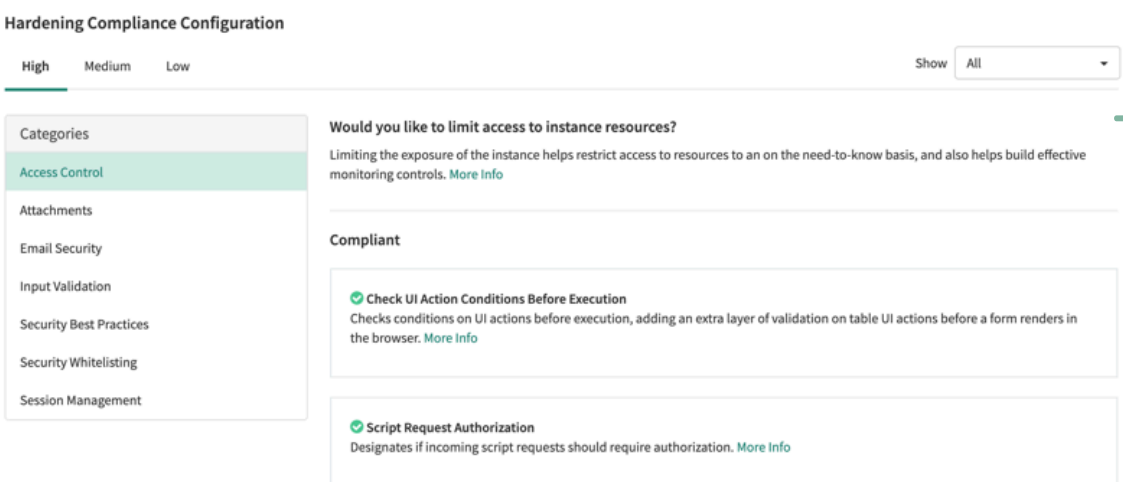
4. Dans la liste **Afficher** sous le graphique, spécifiez si vous souhaitez accéder à toutes les propriétés de configuration de sécurité ou uniquement aux propriétés recommandées.

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 Now Platformfichier . Considérez ces propriétés de configuration de sécurité comme le nombre minimal de paramètres que vous devez définir pour sécuriser le Now Platformfichier .

Option	Description
	Remarque : Pour sécuriser entièrement votre instance, utilisez l'option **Tout** . Il inclut également toutes les propriétés de configuration de sécurité recommandées.



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

Option	Description
	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 Pièces jointes les paramètres de renforcement de la sécurité de l’instance.
Sécurité de la messagerie	La sécurité des e-mails 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 Sécurité des e-mails (renforcement de la sécurité de l’instance) les paramètres de renforcement de la sécurité de l’instance.
Validation de l'entrée	La validation d’entrée inclut des propriétés liées à la sécurité qu’un administrateur peut configurer pour minimiser la saisie de données mal formées, quelle qu’en soit la source. Pour en savoir plus, consultez Validation de l'entrée 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 sécurisées les paramètres de renforcement de la sécurité de l’instance.
Meilleures pratiques de sécurité	Les meilleures pratiques de sécurité englobent les tâches de sécurité qu’un administrateur doit effectuer périodiquement, dans un certain intervalle de temps, et incluent les propriétés de configuration associées. Pour en savoir plus, consultez Bonnes pratiques en matière 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. Pour en savoir plus, consultez Liste d’inclusion de sécurité les paramètres de renforcement de la sécurité de l’instance
Gestion des sessions	Session Management inclut des propriétés liées à la sécurité qu’un administrateur peut configurer pour garantir une gestion de session sécurisée dans .Now 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 l'interrupteur définit une propriété de sécurité sur son paramètre recommandé. Par exemple, vous définissez la plupart des contrôles sur true ou false, 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 dédiée Paramètres de renforcement de la sécurité de l'instance pour le contrôle de sécurité et en savoir plus à ce sujet, cliquez sur **Plus d'informations**.

Résultats
Le score de conformité quotidien augmente ou diminue en fonction des modifications apportées aux paramètres de contrôle de sécurité non conformes.

Information associée

Centre de sécurité de l'instance

Mode d'actualisation des données quotidiennes de score, de tendance et de graphique de conformité

Les données de tendance et de graphique dans Instance Security Center sont mises à jour après l'exécution de la tâche d'analyse des performances à 02h00, heure locale. Il apparaît dans la mosaïque Score de conformité quotidien, dans les mosaïques du ruban Événement et dans les détails de la Centre d'analyse page lorsque vous cliquez sur l'une des vignettes d'événement.

La tâche de gestion quotidienne des données [AppSec] est une tâche planifiée régulièrement qui s'exécute tous les soirs et effectue les tâches suivantes :

1. Vérifie si des utilisateurs valides ont été affectés aux tâches de gestion quotidienne des données [AppSec] et de collecte de données quotidienne [PA AppSec] lors de leur première planification.
   - 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 auquel un rôle administrateur est affecté.
   - Si vous avez saisi un utilisateur non valide, un message d'erreur s'affiche au-dessus de la bannière de sécurité rotative dans Instance Security Center.

   Remarque :
   Pour en savoir plus sur la mise à jour de l'utilisateur affecté lors de l'exécution de tâches planifiées, consultez Créer ou planifier une tâche 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 de propriété de sécurité.
3. Exécute la tâche d'analyse des performances de collecte de données quotidienne [PA AppSec] pour collecter des données de conformité et mettre à jour le score de conformité quotidien.

Actualisation manuelle du score de conformité quotidien

Si un rôle administrateur vous est affecté, vous pouvez également actualiser et recalculer le score de conformité quotidien à tout moment en cliquant sur **Actualiser**.

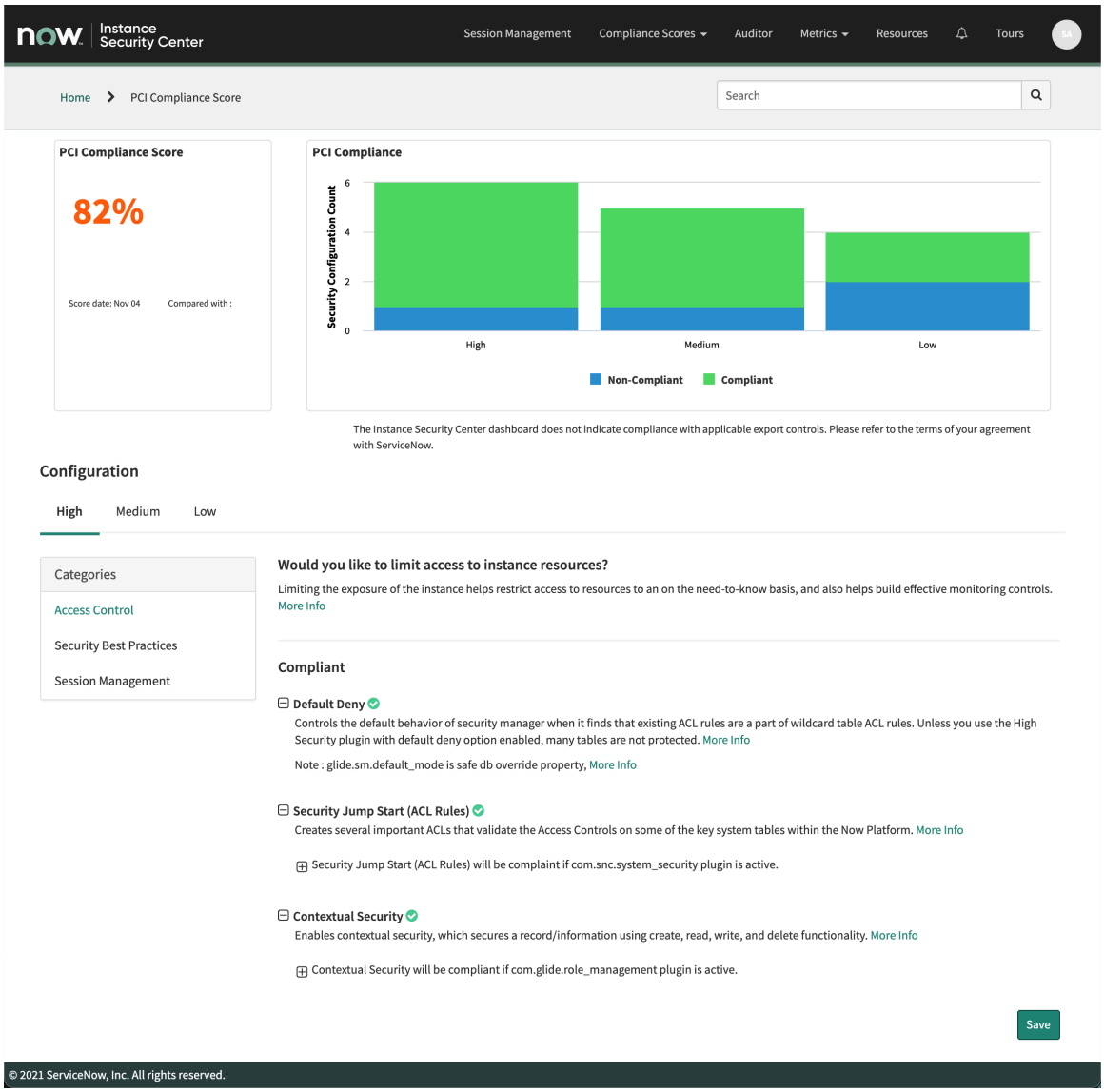
Remarque :
Le bouton **Actualiser** n'apparaît pas pour les utilisateurs auxquels un rôle de security_dashboard_user est affecté.

- La fonction d'actualisation effectue les mêmes tâches que la tâche d'analyse des performances de collecte de données quotidienne, 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 afficher immédiatement l'impact des activités de sécurité de l'instance.
- Il peut y avoir un léger délai avant l'affichage du score mis à jour.

Remarque :
Lorsque vous effectuez une mise à niveau (par exemple, de vers Washington DC), le module d'extension London ISC (Instance Security Center) est automatiquement activé. Un script correctif fourni affecte automatiquement un utilisateur personnalisé sans 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 modifier votre configuration pour améliorer la sécurité.



Rôles Now Platform requis

security_dashboard_user ou admin, 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 de l'instance.

Utilisateur	Utilisation du tableau de bord
Administrateur (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 de votre instance qui répondent aux normes de conformité. L'indicateur affiche également la date à laquelle le score de conformité a été calculé, ainsi qu'une comparaison avec le score calculé précédemment.

Visualisation des données

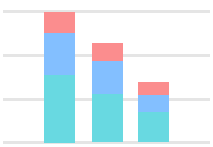
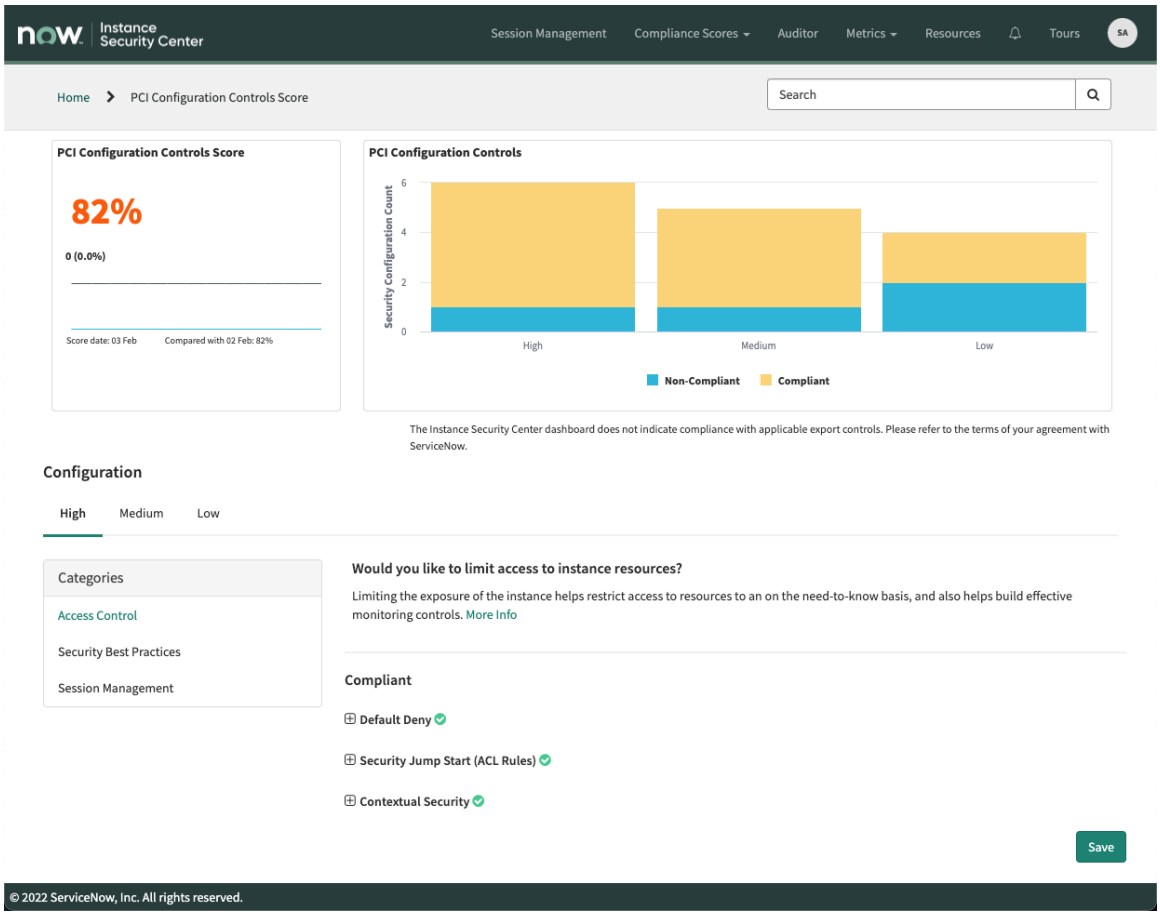
Titre	Type	Table source	Description
Conformité PCI	 Graphique à barres empilées	Configurations de Security [isc_security_configurations]	Affiche les configurations de sécurité conformes et non conformes dans les catégories haute, moyenne et faible. Cliquez sur une zone du rapport pour afficher les configurations de sécurité correspondantes.

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 d'Instance Security Center.



Rôles Now 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 des configurations 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 de configuration 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.

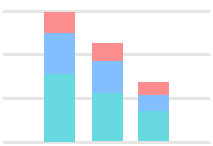
Utilisateur	Utilisation du tableau de bord
Utilisateur du tableau de bord de sécurité (security_dashboard_user)	Surveillez et gérez en permanence la conformité des contrôles de configuration PCI sur votre instance. Modifiez la configuration PCI pour assurer la conformité et améliorer la sécurité de l'instance.
Administrateur (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, ainsi qu'une comparaison avec le score calculé précédemment.

Visualisation des données

Titre	Type	Table source	Description
Contrôles des configurations PCI	 Graphique à barres empilées	Configurations de Security [isc_security_configurations]	Affiche les configurations de contrôle PCI conformes et non conformes dans les catégories haute, moyenne et faible. Cliquez sur une zone du rapport pour afficher les configurations de sécurité correspondantes.

Rechercher les définitions de sécurité incorrectes

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

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, ainsi qu'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 ce que vous pouvez améliorer. Ces informations et recommandations vous aident à répondre aux questions suivantes :

- Les propriétés appropriées liées à la sécurité sont-elles définies ?
- Le module d'extension de haute sécurité est-il activé ?
- Existe-t-il les bonnes règles de contrôle d'accès ?

Exécuter l'auditeur et analyser les résultats de l'analyse

1. Pour exécuter l'auditeur, cliquez sur **Audit** sur la page d'accueil d'Instance Security Center.
2. À l'issue de l'opération, ouvrez 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 incluent son état, le type d'analyse, le temps d'exécution et les messages d'erreur.
4. Chacune des conclusions de l'auditeur contient des détails de résolution et une URL vers le contenu produit expliquant comment les traiter. Suivez les directives documentées pour résoudre les problèmes associés à chacune des conclusions.

Information associée

Paramètres de la sécurisation pour la sécurité de l'instance

Module d'extension de haute sécurité

Règles des listes de contrôles d'accès

Surveiller les mesures d'instance

Surveillez les mesures d'utilisateur, d'exportation, d'authentification, d'e-mail et antivirus pour votre instance. Par exemple, vous pouvez surveiller la sécurité de votre messagerie en vérifiant les mesures pour détecter les spams, les e-mails externes et les e-mails entrants provenant de domaines non approuvés et approuvés pour votre instance. Analysez ces mesures pour rechercher les comportements de sécurité anormaux liés aux activités qui ont lieu dans votre instance.

Mesures des utilisateurs

Analysez les mesures utilisateur pour rechercher les 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 :

- Cliquez sur la mesure pour afficher une liste des utilisateurs qui ne se sont pas connectés à l'instance au cours de 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 qui a accès à l'ensemble des fonctionnalités, fonctions et données système, indépendamment des contraintes de sécurité.
ais_high_security_admin	Rôle de 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 de mot de passe, d'identifier les menaces de sécurité potentielles 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 de changement de mot de passe .

Rôle d'utilisateur	Description
script_include_admin	Rôle d'administrateur qui a également accès aux scripts includes.
security_admin	Rôle de privilège élevé qui permet à un utilisateur de créer et de modifier les contrôles d'accès et les paramètres de sécurité élevée. Pour en savoir plus, reportez-vous à la rubrique Security_admin rôle.
user_admin	Rôle d'administrateur qui peut également 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 de rôle du nombre d'utilisateurs pour afficher une liste des utilisateurs ayant ce type de rôle à 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 des informations sur le nombre d'informations de tendance 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.

Pour afficher les détails de l'utilisateur pour un nombre d'utilisateurs spécifique (par exemple, les 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 en lock-out et remédier à la situation.

Tendance des événements

Affiche les informations de tendance du nombre pour des types d'événements spécifiques, sur une période :

Type d'événement	Description
Connexion de l'administrateur	Nombre d'utilisateurs disposant de rôles d'utilisateur administrateur aux privilèges élevés qui se sont connectés un jour spécifique.
Connexion externe	Nombre d'utilisateurs à qui un rôle de snc_external affecté se sont connectés à cette instance au cours de la journée du calendrier. Ces connexions sont généralement effectuées à des fins de maintenance, d'assistance, de conseil

Type d'événement	Description
	ou d'audit. La surveillance de cette mesure vous permet de vérifier que les tentatives de connexion externe sont légitimes et ne posent pas de problèmes de sécurité potentiels.
Échec de la connexion	Nombre de tentatives de connexion infructueuses un jour donné.
Emprunt d'identité	Nombre d'utilisateurs connectés un jour spécifique qui empruntent l'identité d'autres utilisateurs.
Élévation de la sécurité	Nombre de fois où un administrateur de sécurité a élevé la sécurité des utilisateurs standard en remplaçant le rôle d'utilisateur qui lui est affecté par un rôle de sécurité avec des privilèges élevés au cours d'un jour civil. Ces rôles de sécurité à privilège élevé comprennent oauth_admin, admin, security_admin et emprunteur d'identité.
Connexion SNC	Nombre de Service et assistance client personnes qui se sont connectées à cette instance à l'aide de la technique Hi-hopping au cours d'une journée spécifique.

Pour afficher les détails de l'utilisateur pour un nombre d'événements spécifique (par exemple, Emprunt d'identité) :

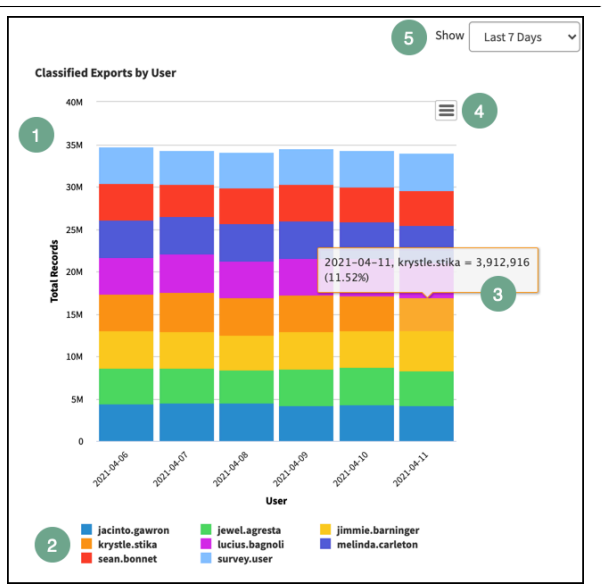
- Cliquez sur la mesure du nombre d'utilisateurs. La page Journal des événements du tableau de bord de sécurité répertorie les journaux d'événements pour ce type d'événement.
- Cliquez sur un nom d'utilisateur pour afficher plus de détails sur cet événement.

Information associée

Centre d'analyse

Mesures d'exportation

Analysez les mesures d'exportation pour identifier les données les plus couramment exportées et les utilisateurs qui exportent le plus de données.



1. **Exporter le graphique**

   Chaque rapport affiche le nombre d'événements d'exportation par date, à l'aide d'une clé à 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. **Clé du rapport**

   La clé en bas du rapport indique quelles couleurs identifient quels utilisateurs ou tables.

3. **Fenêtre contextuelle d'aperçu**

   Pointez sur une entrée du 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 sous forme d'image. Vous pouvez enregistrer le rapport au format PNG ou JPEG.

5. **Plage de dates du rapport**

   Utilisez la liste **Afficher** pour afficher les exportations au cours des dernières 24 heures ou des 7 derniers jours.

Exporter les rapports de mesures

La page des 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 lesquels de vos utilisateurs exportent le plus de données correspondant à des classifications telles que des informations confidentielles, restreintes ou personnelles. Les administrateurs peuvent définir les classifications utilisées par ce rapport dans l'onglet **Paramètres** .

Exportations par table

Utilisez le rapport **Exportations par table** pour voir à partir de quelles tables les exportations sont les plus fréquentes.

Exportations classées par table

Utilisez le rapport **Exportations classées par table** pour voir les tables exportées le plus fréquemment qui correspondent à des classifications telles que les informations confidentielles, restreintes ou personnelles. Les administrateurs peuvent définir les classifications utilisées par ce rapport dans l'onglet **Paramètres** .

Remarque :
Les rapports de mesures d'exportation suivent uniquement les événements d'exportation. Les exportations provenant d'autres sources, telles que les API REST ou les workflows, ne sont pas suivies dans le cadre de cette fonctionnalité.

Exporter les paramètres de mesures

Utilisez les options de configuration de l'onglet Paramètres pour affiner les résultats de génération de rapports.

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 dans 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 dans 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 plus de détails sur ces alertes, consultez 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 le déclenchement et l'alerte de votre instance.
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** .

Utilisez le bouton **Enregistrer** (⌘ **+ s)** pour enregistrer vos paramètres.

Mesures d'authentification

Analysez les mesures d'authentification pour afficher les 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 sont affichés dans cet onglet.

Remarque :
La page des mesures d'authentification nécessite le **module d'extension REST API Access Policy** (com.glide.rest.policy). Pour plus d'informations sur cette fonctionnalité, consultez Politiques d'accès des REST APIs.

API sans politique d’authentification

Affiche un nombre en temps réel de toutes les API sans politique d’accès

Sécurisation renforcée : flux de récupération de compte

Sécurisation renforcée : paramètre lié à la fonctionnalité MFA basée sur le rôle

Comptes d’accès au service Web uniquement

Affiche le nombre d’enregistrements utilisateur pour lesquels l’option d’accès au service Web est 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 arrivent à expiration dans 30 jours.

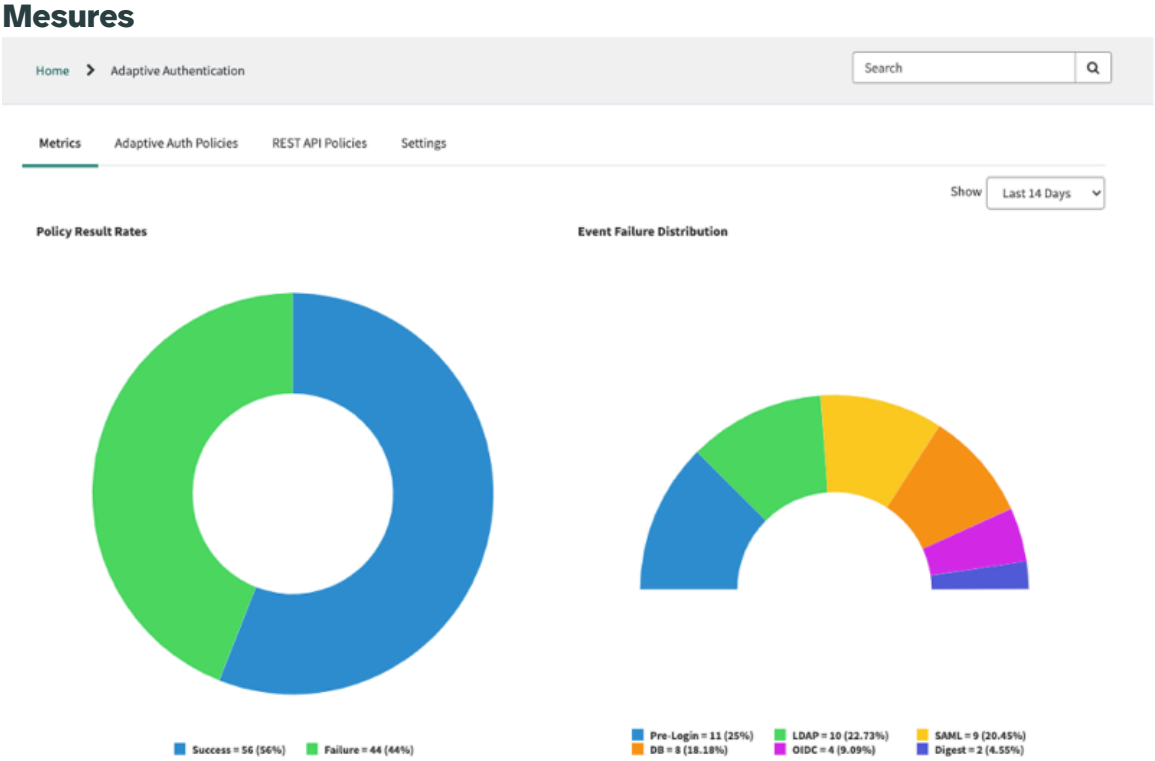
Mesures d'authentification adaptative

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 dans Sur place à l’aide de la page Mesures d’authentification adaptative. Les administrateurs de sécurité peuvent utiliser les 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 **Adaptive Authentication** (com.snc.adaptive_authentication). Pour plus d’informations sur cette fonctionnalité, consultez Authentification adaptative.

Mesures



Utilisez l’onglet Mesures pour afficher **les** rapports relatifs à votre configuration d’authentification adaptative. Les rapports suivants sont affichés dans cet onglet.

Traduction automatique

- Taux des résultats de la politique
- Distribution d'échecs d'événements
- Distribution de la réussite d'événement
- Adresses IP refusées
- Connexions des utilisateurs pour l’authentification
- Connexions des utilisateurs de l'API
- Tendance en matière d'authentification

Utilisez la liste **Afficher** pour sélectionner une période pour les rapports affichés

Politiques d’authentification adaptative

Utilisez l’onglet **Politiques d’authentification adaptative** pour afficher les politiques d’authentification adaptative et les contextes de politique sur votre instance. Cliquez sur n’importe quelle entrée de ces listes pour afficher l’enregistrement associé. Pour plus de détails sur ces enregistrements, consultez Authentification adaptative

Paramètres

Utilisez l’onglet Paramètres pour afficher et configurer les propriétés système d’authentification adaptative. Pour plus d’informations sur ces propriétés, consultez Configurer les propriétés d’authentification adaptative

Mesures d’e-mail

Analysez vos mesures d’e-mail pour rechercher les comportements anormaux liés aux e-mails entrants vers votre instance. Par exemple, si les mesures indiquent un pic de courriers indésirables provenant de domaines spécifiques, vous pouvez définir des actions entrantes qui empêchent leur remise 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 d’un jour calendaire.

Préférence de notification	Description
E-mail entrant externe	Nombre d’e-mails entrants du jour du calendrier qui ont été remis à l’instance à partir de domaines de messagerie externes. **Remarque :** Les domaines d’e-mail externe sont les domaines qui ne sont pas répertoriés dans la propriété système, car cette propriété suit uniquement vos domaines d’e-mail internes. Pour en savoir plus sur cette propriété, reportez-vous à la rubrique Propriétés système disponibles .
Courrier indésirable	Nombre d’e-mails entrants du jour du calendrier qui ont été remis à l’instance et marqués comme courrier indésirable. Un nombre qui ne correspond pas aux

Préférence de notification	Description
	tendances historiques peut indiquer que des tentatives de compromission de la sécurité de votre instance sont effectuées.
E-mail entrant approuvé	Nombre d'e-mails entrants vers l'instance pour le jour du calendrier à partir de domaines de messagerie désignés comme approuvés.
E-mail entrant non approuvé	Nombre d'e-mails entrants vers l'instance pour un jour civil à partir de domaines de messagerie désignés comme non approuvés. Vous pouvez désigner des domaines de messagerie non approuvés ou approuvés dans le formulaire Domaine non approuvé et approuvé afin de pouvoir suivre vos e-mails entrants qui sont envoyés à partir de ces domaines. Pour savoir comment désigner des domaines de messagerie non approuvés ou approuvés, consultez Désigner des domaines d'e-mail comme non approuvés ou approuvés.

Après avoir cliqué sur une mesure d'e-mail, vous pouvez en apprendre davantage sur les problèmes de sécurité des e-mails possibles dans votre instance en cliquant sur l'un des éléments suivants :

Commande	Description
Graphique	Nombre d'e-mails entrants et tendances dans le temps pour le type d'e-mail sélectionné (courrier indésirable, externe entrant, non approuvé ou approuvé).
Enregistrements	Enregistrements d'e-mail individuels qui compromettent le décompte 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 à vos e-mails entrants vers l'instance. Les mesures ne s'appliquent pas au trafic normal qui est traité via vos serveurs de messagerie à l'échelle de l'entreprise. Pour en savoir plus sur la définition des actions entrantes et leur impact sur le traitement de vos e-mails entrants, consultez la section Actions sur e-mail entrant .

Désigner des domaines d'e-mail comme non approuvés ou approuvés

Désignez des domaines d'e-mail spécifiques comme non approuvés ou approuvés afin de pouvoir surveiller les mesures des e-mails entrants provenant de ces sources dans votre instance.

Avant de commencer
Rôle requis : security_dashboard_user ou admin

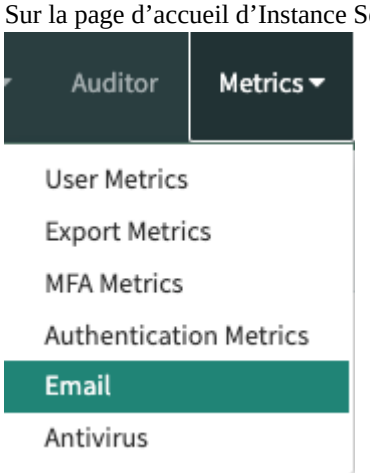
Pourquoi et quand exécuter cette tâche
Lorsque des domaines non approuvés ou approuvés envoient des e-mails à votre instance, leurs nombres quotidiens s'affichent dans les mesures **E-mail entrant non approuvé** ou **E-mail entrant approuvé** sur la page E-mail. Vous pouvez ensuite suivre l'activité des e-mails issus 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, à notifier 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 afin de bloquer leur remise, voir Filtres d’adresse système .

Procédure

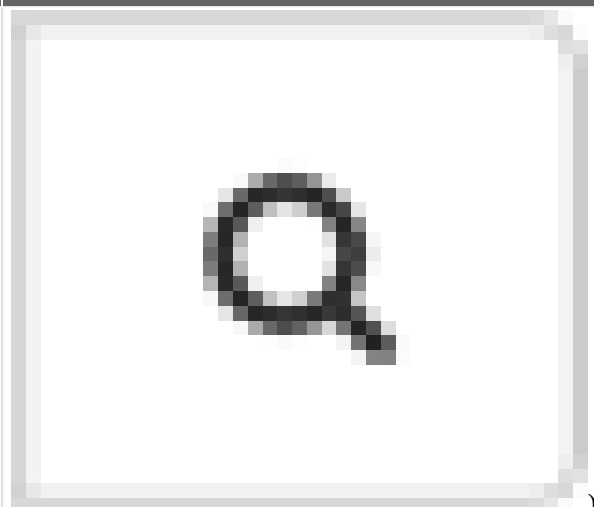
1. Accédez à la **Tous** > **Sécurité de système** > **Centre de sécurité de l'instance**.
2. Sur la page d’accueil d’Instance Security Center, sélectionnez **E-mail** dans le menu **Mesures** .



3. Sur la page E-mail, dans la section Domaines non approuvés et approuvés, cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire.

Formulaire Domaine non approuvé ou approuvé

Champ	Description
Domaine	Nom du domaine de messagerie que vous désignez comme non approuvé ou approuvé. Par exemple, saisissez servicenow.com pour désigner que ServiceNow les employés peuvent envoyer des e-mails fiables à l’instance.
Catégorie	Catégorie qui indique si le domaine d’e-mail n’est pas approuvé ou s’il est approuvé : **Non approuvé** Indique que le domaine de messagerie n’est pas approuvé. Vous l’utilisez pour identifier les domaines qui envoient des e-mails suspects ou qui constituent une menace potentielle pour la sécurité de l’instance. **Approuvé** Indique que le domaine de messagerie est approuvé. Vous l’utilisez pour identifier les domaines lorsque vos mesures indiquent que les e-mails entrants ne présentent aucune menace pour la sécurité. Désigner le domaine comme approuvé vous permet de suivre son activité d’e-mails entrants au fil du temps.
Actifs	Cochez la case pour activer ou désactiver l’état désigné comme 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 (

Champ	Description
	) pour rechercher le nom de l’utilisateur. Si vous ne souhaitez pas que des notifications vous soient envoyées, laissez le champ **Notifier** vide.

5. Sélectionnez **Enregistrer**.

Résultats

Les informations sur les domaines de messagerie 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 anti-virus il Analyse anti-virus s’exécute dans votre instance pour aider à le protéger contre les virus provenant de pièces jointes.

Les mesures suivantes s’affichent pour les 60 derniers jours d’activité et vous permettent d’évaluer l’efficacité Analyse anti-virus des 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 Analyse anti-virus en quarantaine dans cette instance pour la date indiquée.
Vert	Nombre de fichiers infectés téléchargés sur l’instance, puis mis en quarantaine jusqu’à la date indiquée. Il s’agit principalement de pièces jointes d’e-mails contenant un code de virus ou un code rouge.
Jaune	Nombre de fichiers mis en quarantaine dans l’instance qui ont été supprimés pour la date indiquée.

Couleur	Description
Orange	Nombre de fichiers mis en quarantaine dans l'instance qui ont été restaurés pour la date indiquée. **Remarque :** Après Analyse anti-virus l'exécution et la détection de faux positifs, vous pouvez restaurer un fichier mis 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 l'icône Centre d'analyse, puis cliquez sur :

Répartition	Description
AppSec : source de l'événement antivirus	Source de l'événement antivirus. ○ **Lors du téléchargement :** S'est produit en raison du chargement d'un fichier infecté, généralement une pièce jointe. ○ **De la quarantaine :** S'est produit en raison de la mise en quarantaine d'un fichier infecté, généralement une pièce jointe. ○ **En 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 à la suite du téléchargement d'un fichier, généralement une pièce jointe. ○ **Restauré:** S'est produite en raison de la restauration d'un fichier mis en quarantaine. ○ **Supprimé:** S'est produit en raison de la suppression d'un fichier mis en quarantaine.
AppSec : outil de téléchargement d'antivirus	Nom de l'utilisateur connecté qui a téléchargé les fichiers qui étaient à l'origine des infections virales détectées par l'application Analyse anti-virus .

Fichiers en quarantaine

Répertorie les fichiers infectés dans l'instance mise en quarantaine par Analyse anti-virus:

Champ	Description
Nom de fichier	Nom du fichier infecté.
Type de contenu	Type de contenu qui a été infecté dans le fichier. Par exemple, **application/x-dosexec** est un fichier exécutable d'application ou DOS infecté, tandis que **text/plain** est un fichier .txt infecté.
Table	Nom de la table qui contient le fichier infecté. Par exemple, **incident** apparaît pour un enregistrement de fichier d'incident.
Virus	Nom du fichier mis en quarantaine par Analyse anti-virus.
Détectée	Date et heure auxquelles le fichier infecté a été détecté.
Créé par	Nom de l'utilisateur qui a mis en quarantaine le fichier infecté.
Créé	Date et heure de création de l'enregistrement du fichier de quarantaine.
ID système de table	Identificateur système de table affecté à l'enregistrement de fichier de quarantaine.

Remarque :
Vous pouvez également ajouter des **vignettes Fichiers en quarantaine** et **Types de virus** au ruban Événement. Pour en savoir plus, consultez Surveiller les événements de sécurité et Configurer le ruban des événements de sécurité.

Information associée

- Analyse anti-virus
- Configurer Analyse anti-virus
- Examen des fichiers mis en quarantaine
- Examen de l'activité antivirus
- Centre d'analyse
- Répartitions de Performance Analytics
- 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 Now Platform requis

security_dashboard_user ou admin, 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 Instance Security Center, cliquez sur **Mesures dans l'en-tête** , puis sélectionnez **Mesures MFA**.

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 de l'instance.
Administrateur (admin)	Surveillez en permanence la conformité de la sécurité de l'instance pour détecter les menaces de sécurité et y répondre.

Indicateurs

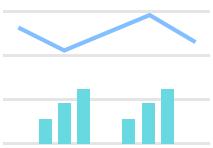
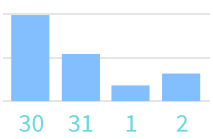
Utilisateurs inscrits pour MFA

Affiche le nombre total d'utilisateurs sur l'instance inscrits à MFA . Cliquez pour ouvrir le centre d'analyse et obtenir plus de détails.

Utilisateurs utilisant le contournement MFA

Affiche le nombre total d'utilisateurs utilisant le contournement MFA. Cliquez pour ouvrir le centre d'analyse et obtenir plus de détails.

Visualisations de 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 admin, 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 contenu and Compréhension du langage naturel (NLU, fournissant Agent virtuel un Agent virtuel accès à partir d'Instance Security Center.

Avant de commencer

L'interface Agent virtuel dans Instance Security Center est uniquement disponible pour les utilisateurs ayant des abonnements payants Agent virtuel et qui ont activé le module d'extension Glide Virtual Agent (com.glide.cs.chatbot). Pour en savoir plus, consultez Activer Virtual Agent .

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 rapidement des réponses récapitulatives 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, aux risques et à d'autres processus.
- Recherchez des ressources liées à la sécurité, telles que les 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 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 l com.glide.isc_virtualagent activer manuellement.

Procédure

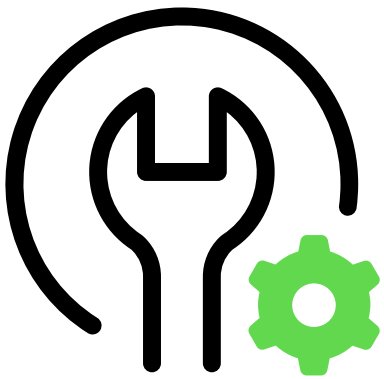
1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Trouvez le module d'extension à l'aide des critères de filtre et de la barre de recherche.

   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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

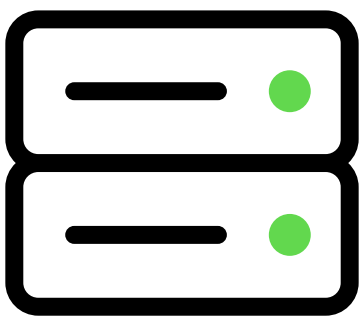
Autres paramètres et ressources de sécurité

Cette section contient les propriétés de sécurité que vous définissez en dehors d'Instance Security Center, ainsi que d'autres ressources liées à la sécurité.



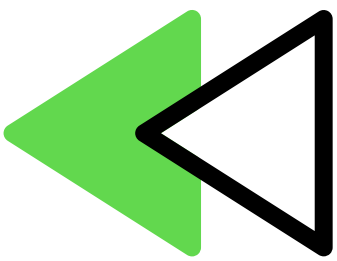
Propriétés système de sécurité

Les paramètres de sécurité fournissent plusieurs propriétés pour contrôler le niveau de sécurité de votre instance.



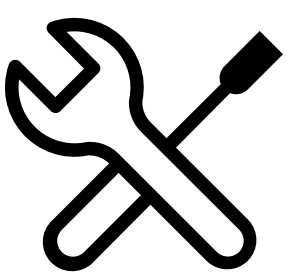
Guide de déploiement du MID Server

ServiceNow Management, Integration, and Discovery (MID) Server 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.



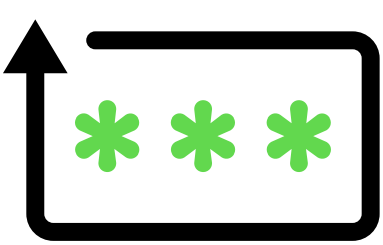
Comportement réversible

Certaines propriétés système sont classées comme « safe_overrides » ou « no_db_override ».



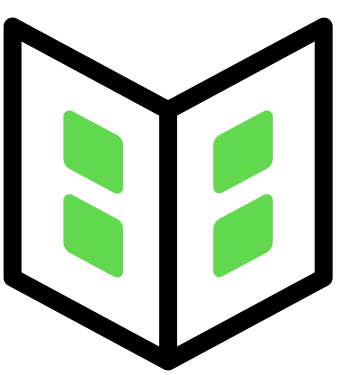
Propriétés de sécurité obsolètes

Ces propriétés de sécurité ont été déconseillées dans les versions antérieures.



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 dans votre instance.



Autres ressources sur la sécurisation renforcée

Sources supplémentaires d'informations sur le renforcement des contrôles de sécurité, en lien avec Now Platform.

Traduction automatique

Journalisation, audit et erreurs (renforcement de la sécurité de l'instance)

Appliquez une stratégie de journalisation et d'audit afin de pouvoir identifier les activités suspectes et intervenir en temps utile.

Pour en savoir plus sur ce qui peut être journalisé dans l'instance, reportez-vous à Journaux système. Assurez-vous qu'il existe un calendrier pour la surveillance des événements système tels que les connexions et les échecs de connexion à l'aide de **Journaux système** > **Events**.

Désactivation des messages d'erreur SQL (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour désactiver le `glide.db.loguser` rendu 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 cadre d'un message d'erreur sur une page Web.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Autres ressources sur la sécurisation renforcée

Vous trouverez ci-dessous d'autres sources d'information sur le renforcement des contrôles de sécurité en ce qui concerne le Now Platform.

Ressources	Description
Portail de test de sécurité	Portefeuille de services de sécurité sur HI
KB0538598	Test d'intrusion de l'application client | Politique et procédure
KB0546756	Désactivation de l'accès public au système de gestion de contenu (CMS)
KB0550071	ServiceNow, Inc. Révision du contrôle d'accès à l'instance
KB0550613	Identification et activation des restrictions d'adresse IP
KB0550828	Auditer et examiner les transactions GlideAjax

Ressources	Description
KB0550837	Correction 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. Monitoring - Vue d’ensemble et aperçu
KB0564232	Utilisation de ServiceNow, Inc. l’application Mobile avec authentification externe
Sécurité et risque	ServiceNow, Inc. Communauté

Paramètres de la sécurisation pour la sécurité de l'instance

Les paramètres de renforcement de la sécurité de l'instance contiennent des descriptions détaillées et des valeurs de conformité pour les propriétés système et les modules d'extension liés à la sécurité dans la Now Platform. Vous pouvez définir la plupart de ces propriétés dans la page Configuration de la conformité à la sécurisation renforcée d'Instance Security Center.

Vue d'ensemble et objectif

Instance Security Center calcule un score de conformité quotidien, exprimé en pourcentage. Il est basé sur la conformité de vos paramètres de sécurité d'instance actuels avec les valeurs de conformité définies dans les paramètres de renforcement de la sécurité de l'instance.

Dans sa page Configuration de la conformité à la sécurisation renforcée, vous pouvez gérer les paramètres de configuration de sécurité spécifiques qui peuvent affecter le score de votre instance. Pour en savoir plus sur l'assurance que vos instances répondent aux exigences de sécurisation renforcée, consultez :

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

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 de sécurité.

Autres ressources

Pour la référence utilisateur, la Now 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
- Paramètres de sécurité élevée

Tables de sécurisation renforcée de l'instance

Tables Configurations de Security

Les enregistrements de la table Configurations de Security [isc_security_configurations] contiennent les détails d'une configuration de sécurité. Dans un enregistrement, vous trouvez la description d'une configuration, son état de conformité et d'autres détails importants.

Utilisez l'enregistrement des configurations de sécurité pour afficher toutes les propriétés et dépendances que vous devez configurer pour rendre votre configuration conforme en un seul endroit.

Dans l'enregistrement des configurations de sécurité, vous pouvez voir les enregistrements de groupes de dépendance de sécurité et de dépendance associés à cette configuration.

Table Dépendances de Security

Les enregistrements de la table des dépendances de sécurité [isc_security_dependencies] définissent les critères entrants et sortants, ainsi qu'un type recommandé. Ce type définit le mode d'affichage de la dépendance dans Instance Security Center.

Table des groupes de dépendances

Utilisez les enregistrements de la table des groupes de dépendances [isc_dependency_groups] pour regrouper plusieurs dépendances. Toutes les dépendances d'un groupe doivent être conformes pour que le groupe soit considéré comme tel.

Contrôle d’accès (renforcement de la sécurité de l’instance)

Les contrôles d’accès déterminent si l’accès à une ressource particulière doit être accordé ou refusé. L’accès aux ressources n’est autorisé qu’aux utilisateurs autorisés à les utiliser.

L’autorisation n’est pas équivalente à l’authentification, car ces termes et leurs définitions sont souvent confondus.

- L’authentification consiste à fournir et à valider une identité.
- L’autorisation comprend des règles d’exécution qui déterminent les fonctionnalités et les données auxquelles l’utilisateur (ou le principal) peut accéder, garantissant ainsi l’allocation correcte des droits d’accès une fois l’authentification réussie.

L’autorisation est un processus qui survient après une authentification réussie. Vous pouvez configurer des propriétés de sécurité qui désignent si, après avoir déterminé qu’un utilisateur détient des informations d’identification valides associées à un ensemble bien défini de rôles et de privilèges, l’autorisation de ressource se produit.

Voici quelques-uns des contrôles de sécurité qu’un administrateur peut configurer pour restreindre l’accès non autorisé à des entités sensibles dans le Now Platform.

- Règles des listes de contrôles d’accès
- Configurer une règle ACL
- Contrôle d'accès ServiceNow

Accès à l'API de script GlideSystemUserSession

L’API scriptable GlideSystemUserSessionSandbox pouvant être appelée par le client expose les méthodes GlideSystemUserSession’s addErrorMessageNoSanitization et addInfoMessageNoSanitization au bac à sable JavaScript. Cela permet à tous les utilisateurs d’appeler cette méthode via le script.

Lorsqu'elle est définie sur **vrai**, une session utilisateur bac à sable (sandbox) est autorisée à appeler des informations ou des messages d'erreur sans nettoyage. Un avertissement sera consigné lors de l'appel du message. Lorsqu'elle est définie sur **faux**, l'appel n'est pas autorisé.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sandbox.usersession.allow_unsanitized_messages`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurable dans le centre de sécurité de l'instance	Oui
Objectif	Cette propriété empêche l'appel de messages d'information ou d'erreur non désinfectés dans une session utilisateur bac à sable.
Type	vrai | faux booléen
Valeur recommandée	faux
Dépendances de Security	La valeur de cette propriété est un remplacement sécurisé et ne peut pas être modifiée une fois modifiée.
Impact fonctionnel	(Élevé) Définir la propriété avec la valeur false n'entraînera aucune création ou journalisation de message si ces fonctions sont appelées.
Risque de sécurité	(Élevé) En l'absence d'assainissement approprié, il est possible d'accéder à du contenu potentiellement dangereux et de mettre la fonction d'erreur non désinfectée à la disposition du script.
Références	Contrôle d'accès Remplacement sécurisé

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Autorisation pour l'exécution du script

Utilisez cette `glide.script_processor.authorized_script_module_role` propriété pour restreindre l'utilisation des scripts `d'exécution d'sys_app_module` table au rôle défini au sein de la propriété.

Cette propriété empêchera tous les utilisateurs système d'exécuter un script à partir de la sys_app_module à moins qu'ils n'aient le rôle spécifié dans la propriété. Utilisez la propriété glide.script_processor.authorized_script_module_role pour spécifier le rôle qui peut exécuter des scripts.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.script_processor.authorized_script_module_role`
Type de configuration	Propriétés système (/sys_properties_list.do)

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour exiger un rôle désigné afin d'exécuter un script à partir de la `sys_app_module`.
Valeur recommandée	Zone de texte avec une liste de rôles séparés par des virgules.
Impact fonctionnel	(Moyen) Cette correction applique l'authentification sous la forme d'une autorisation par rôle défini. • 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, les utilisateurs non autorisés peuvent accéder au contenu/aux données sensibles sur l'instance.
Références	Contrôle d'accès

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Authentification de base : demandes JSONv2 (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.jsonv2` demandes JSONv2 entrantes doivent obtenir une autorisation de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.jsonv2
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'autorisation des demandes JSONv2.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) 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.

Attribut	Description
	• Il effectue cette authentification tout en récupérant les données des tables/pages sous la 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 a besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, consultez JSONv2 Web Service Web JSONv2 .
Risque de sécurité	(Élevé) Sans 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 Exiger une authentification de base pour les demandes JSONv2 entrantes

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Authentification de base : demandes SOAP (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.soap` demandes SOAP entrantes doivent obtenir une autorisation de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.soap
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour faire respecter l'autorisation des demandes SOAP.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) 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.

Attribut	Description
	• Il effectue cette authentification tout en récupérant les données des tables/pages sous la 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 a besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, consultez Informations d'identification d'authentification SOAP Web Service et MID Server et demandes SOAP.
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les demandes SOAP de source de données, un utilisateur non autorisé peut accéder à du contenu/des 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 Add a system property .

Bloquer l'accès pour le développeur délégué

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 n'est pas en mesure de mettre à jour ou d'insérer des enregistrements dans le `sys_user_has_role` de table sans 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)
Configurer dans le centre de sécurité de l'instance	Oui
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 recommandée	VRAI
Dépendances de Security	aucun

Attribut	Description
Impact fonctionnel	(Élevé) Lorsqu'un utilisateur disposant du rôle delegated_developer tente de modifier un enregistrement dans `sys_user_has_role`, cette propriété active des contrôles de sécurité supplémentaires par rapport à l'opération. Les vérifications de sécurité supplémentaires valident que l'utilisateur a reçu le rôle `user_admin` s'il essaie de créer ou de mettre à jour `sys_user_has_role`. S'il ne dispose pas du rôle `user_admin` , l'accès lui sera refusé. Lorsque la propriété est définie sur false, ces vérifications supplémentaires ne sont pas validées.
Risque de sécurité	(Élevé) Sans autorisation appropriée, les utilisateurs non autorisés peuvent accéder au contenu/aux données sensibles sur l'instance.
Références	Contrôle d'accès

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Vérifier les conditions de l'action d'interface utilisateur avant son exécution (renforcement de la sécurité de l'instance)

Utilisez cette 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 des 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)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour garantir une validation supplémentaire sur la table, les actions d'interface utilisateur avant qu'elles ne soient exécutées.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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	(Moyen) La demande d'accès est toujours vérifiée lorsque des transactions ont lieu entre deux zones. Cette opération valide toutes les actions d'interface utilisateur avant que le formulaire ne soit rendu à 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 Add a system property .

Module d'extension Contextual Security : Role Management (renforcement de la sécurité de l'instance)

Activez le module d'extension Contextual Security : Role Management (*com.glide.role_management*) pour activer la sécurité contextuelle, qui sécurise un enregistrement/des informations utilisant des fonctionnalités de création, de lecture, d'écriture et de suppression.

Une fois installé et activé, les rôles du dictionnaire (créés par Simple Security Manager) ne sont plus testés. Au lieu de cela, la recherche des Now Platform 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 implémentées 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 dans les 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
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Contrairement au gestionnaire de sécurité simple, le gestionnaire de sécurité contextuelle connaît la hiérarchie des tables système. Vous pouvez potentiellement avoir différentes règles de sécurité pour un champ en fonction de l'endroit où il apparaît dans la hiérarchie.
Valeur recommandée	Actif (module d'extension activé par défaut)
Impact fonctionnel	(Moyen) 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 côté serveur avant d'exécuter les opérations CRUD, afin de garantir le niveau d'accès approprié pour les utilisateurs de l'instance.
Références	Gestionnaire de sécurité contextuelle

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à Activate a plugin .

Autorisation de demande CSV (renforcement de la sécurité de l'instance)

Utilisez cette *glide.basicauth.required.csv* propriété pour indiquer si les demandes CSV (valeurs séparées par des virgules) entrantes doivent faire l'objet d'une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.csv
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base sur les demandes CSV.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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, reportez-vous à la section Récupération de données à partir d'un fichier au format CSV .
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les demandes CSV entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Sécurité des services Web

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Refus par défaut (renforcement de la sécurité de l'instance)

Utilisez cette *glide.sm.default_mode* propriété pour contrôler le comportement par défaut du gestionnaire de sécurité lorsqu'il détecte que des règles ACL font partie des règles ACL d'une table à caractère générique.

Lorsque le module d'extension Paramètres de sécurité élevée (*com.glide.high_security*) est activé lors de l'installation initiale de l'instance, il crée cette propriété, et des règles ACL génériques sont créées. Pour fournir un accès basé sur les rôles aux tables système, ces règles contrôlent un nombre important d'ACL et les opérations basées sur les enregistrements les plus courantes :

- Lecture
- Écriture
- Créer
- Supprimer

À moins que vous n'utilisiez le module d'extension High Security avec l'option de refus par défaut activée, de nombreuses tables ne sont pas protégées. Le utilise Now Platform un modèle de sécurité de refus par défaut qui empêche les utilisateurs non administrateurs d'accéder aux objets à moins qu'ils ne répondent à une règle ACL correspondante. À l'aide de ce modèle, il supprime de nombreux vecteurs d'attaque, tels que les scripts non sécurisés.

En savoir plus

Attribut	Description
Nom de la propriété	glide.sm.default_mode
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	La meilleure pratique en matière de sécurité consiste à restreindre l'accès aux tables par un utilisateur non autorisé. • Si aucune règle d'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 toutes les tables, sauf si l'utilisateur dispose du rôle d'administrateur ou répond aux exigences d'une autre règle ACL de table.
Valeur recommandée	refuser
Impact fonctionnel	(Élevé) Si vous définissez cette propriété sur **Autoriser**, les règles ACL de 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 sécurisé aux tables déjà utilisées dans un environnement de production.
Risque de sécurité	(Élevé) Les utilisateurs non administrateurs peuvent accéder aux objets qui correspondent aux règles ACL de la table de caractères génériques.
Références	Propriété de refus par défaut

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Double vérification des transactions entrantes (renforcement de la sécurité de l'instance)

La *glide.security.strict.updates* propriété permet d'activer la sécurité à deux facteurs sur les transactions entrantes lors de la soumission d'un formulaire et ajoute une

couche supplémentaire de validation de table avant qu'un formulaire ne s'affiche dans le navigateur. Cette propriété est définie sur **true** par défaut

En savoir plus

Remarque :
Cette propriété est définie sur **true** par défaut dans Vancouver la version et les 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 client.

Attribut	Description
Nom de la propriété	glide.security.strict.updates
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour assurer une couche supplémentaire de vérification des autorisations utilisateur avant de présenter le formulaire dans le navigateur.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette correction ajoute une couche supplémentaire de validation pour vérifier les autorisations utilisateur sur la table/page cible sur l'instance. Tant que les contrôles d'accès sont définis de manière appropriée sur l'instance client, il ne devrait y avoir aucun impact.
Risque de sécurité	(Élevé) Vous devez toujours vérifier la demande d'accès lorsque des transactions ont lieu entre deux zones. Cette opération vérifie les autorisations lorsque le formulaire est demandé et avant que le rendu du formulaire ne se produise.
Références	Propriétés des paramètres de sécurité

Activer les ACL pour contrôler les détails du profil en direct (renforcement de la sécurité de l'instance)

Utilisez cette `glide.live_profile.details` propriété pour indiquer si un utilisateur doit être en mesure d'afficher tous les champs de détail, tels que le nom de l'entreprise et les numéros de téléphone, sur un profil actif.

Selon le paramètre de la `glide.live_profile.details` propriété, les éléments suivants se produisent :

- Si la valeur est définie sur **Afficher**, l'accès aux informations de profil actif est accordé, quelles que soient les ACL créées pour le profil d'utilisateur.
- Si la valeur est définie sur **ACL,** l'accès aux informations du 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, quelles que soient les ACL créées pour le profil d'utilisateur.

En savoir plus

Attribut	Description
Nom de la propriété	glide.live_profile.détails
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
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)
Valeur recommandée	ACL
Impact fonctionnel	(Moyen) 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	(Moyen) Les demandes d'API doivent toujours respecter 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 Add a system property .

Activation de la vérification de l'ACL de AJAXGlideRecord (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour effectuer la `glide.script.secure.ajaxgliderecord` validation de la règle de contrôle d'accès (ACL, Access Control Rule) 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.

À partir de scripts clients, il est possible d'interroger des données arbitraires du serveur à l'aide de l'attribut AJAXGlideRecord (GlideAjax -Client), à l'aide d'une syntaxe telle qu'un enregistrement Glide côté serveur. C'est 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 pouvez interroger uniquement 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 le est en cours d'exécution sans vérification de l'appel Now Platform GlideAjax ACL, une API peut renvoyer des informations auxquelles l'utilisateur actuellement connecté ne pourrait pas accéder autrement.

En savoir plus

Attribut	Description
Nom de la propriété	glide.script.secure.ajaxgliderecord
Type de configuration	Propriétés système (/sys_properties_list.do)

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Assurez-vous que les ACL de sécurité sont vérifiées et validées même lorsque les enregistrements sont consultés via des API côté client.
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) 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 d'informations sur son impact et sur la façon de l'identifier, consultez Reportez-vous à l'article Auditer et examiner les transactions GlideRecord côté client [KB0550828] dans le 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, de sorte que l'utilisation de la validation ACL aide 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 script includes, les processeurs et les autres entités utilisées par une API GlideAjax (AJAXGlideRecord) afin qu'elle s'exécute avec l'autorisation appropriée. Implémentez des méthodes telles que `canRead ()`,`canWrite()`,`canCreate ()` et `canDelete ()` pour effectuer l'autorisation de l'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 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 des scripts provenant du client : • *`glide.script.use.sandbox`*: voir Bac à sable pour les scripts générés par le client. • *`glide.script.allow.ajaxevaluate`*: voir Activer AJAXEvaluate.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Autorisation des demandes Excel (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.excel` demandes Excel entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.excel
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base sur les demandes Excel.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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	(Moyen) 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 Add a system property .

Module d'extension Explicit Role (renforcement de la sécurité de l'instance)

Activez le module d'extension Explicit Role (`com.glide.explicit_roles`) pour fournir à l'instance les nouveaux rôles snc_internal et snc_external pour les applications B2B et B2C, empêchant ainsi les utilisateurs externes d'accéder aux données internes. Les utilisateurs d'entreprise (employés) doivent avoir le rôle interne, tandis que les utilisateurs externes (non-employés) doivent avoir le rôle externe.

Lorsque vous installez le module d'extension de rôle explicite :

- Elle affecte le nouveau rôle de snc_internal à tous les utilisateurs existants. Il affecte également toutes les tables sans aucun rôle au rôle snc_internal.
- Lorsque vous créez un utilisateur ou une table après l'activation du module d'extension Explicit Role, la fonction affecte Now Platform le rôle snc_internal à l'utilisateur ou à la table.
- Cela Now Platform empêche les utilisateurs ayant le rôle snc_external d'accéder à une table qui n'est pas explicitement affectée au rôle snc_external.

- Toutes les tables disposant du rôle public sont accessibles à la fois par les utilisateurs internes et externes.
- Certains widgets du portail de services nécessitent une connexion, mais pas de rôle d'utilisateur spécifique. Après l'installation du module d'extension de rôles explicites, ces portails deviennent inaccessibles aux utilisateurs externes.

- ○ Pour autoriser l'accès aux utilisateurs externes, modifiez votre widget pour modifier les rôles **requis de vide** à **snc_internal, snc_external**.
  - Par exemple, les clients qui utilisent l'application de gestion des tickets ont besoin que des utilisateurs externes puissent joindre des fichiers à leurs enregistrements de tickets. Modifier la configuration du widget **encryption-context-picker** comme décrit permet aux utilisateurs externes de s'attacher comme prévu.
  - Pour plus d'informations sur la configuration des widgets, consultez Configurer les options d'instance de widget

Remarque :
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 .

Résumé du rôle

snc_internal

Ce rôle est affecté à tous les utilisateurs internes (employés ou internes à une organisation). Tout nouvel utilisateur ajouté obtient également ce rôle lors de sa première connexion/emprunt d'identité, à condition que l'utilisateur n'ait pas le rôle snc_external déjà affecté. Toutes les règles de contrôle d'accès (ACL) existantes sans rôle sont corrigées avec le rôle « snc_internal ». Pour les nouvelles ACL, le Now Platform ajoute automatiquement ce rôle si l'ACL est enregistrée sans aucun rôle.

snc_external

Ce rôle indique que l'utilisateur est externe à votre organisation et qu'il ne doit pas avoir accès aux ressources, sauf si :

- Vous autorisez explicitement l'accès par le biais des ACL pour le rôle snc_external, ou
- Vous leur accordez explicitement des rôles supplémentaires.

Par défaut, les utilisateurs disposant du rôle snc_external ne peuvent pas accéder aux ressources qui ne sont pas de type Enregistrement, telles que les processeurs et les pages de l'interface utilisateur.

publique

Toutes les entités auxquelles un rôle public est affecté sont accessibles aux utilisateurs snc_internal et snc_external.

Lors de l'utilisation du module d'extension Explicit Role :

1. Vérifiez et validez qu'une table ayant le rôle public ne contient aucun enregistrement sensible pour les utilisateurs externes, y compris les utilisateurs publics non authentifiés.
2. Si la table ayant le rôle public contient des données sensibles et que vous souhaitez restreindre les enregistrements sensibles des utilisateurs externes, procédez comme suit :

- Supprimer le rôle public de la table ou
- Ajoutez des ACL scriptées supplémentaires à la table.

3. Vérifiez et validez que tous les points de terminaison, tels que les API REST scriptées, utilisent les rôles ou vérifiez explicitement à l'aide de `GlideRecordSecure`canRead(),canWrite(),canUpdate() et canDelete().

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.explicit_roles
Type de configuration	Module d'extension > de définition du système
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Pour empêcher les utilisateurs externes d'accéder aux données internes.
Valeur recommandée	Actif
Impact fonctionnel	(Faible) Aucun impact significatif, car le module d'extension affecte automatiquement le rôle snc_internal à la table de sorte que les utilisateurs internes existants disposent toujours de l'accès nécessaire.
Risque de sécurité	(Élevé) Les utilisateurs externes (non-employés) peuvent accéder à de nombreuses tables sensibles dans la table à Now Platform laquelle aucun rôle n'est affecté. Ils sont destinés à être accessibles uniquement par les utilisateurs internes (employés).
Références	Explicit Roles

Étapes de configuration

Lors de la création d'une fonctionnalité ou d'une application avec les rôles explicites :

1. Créez un rôle qui hérite du rôle snc_external pour votre nouvelle fonctionnalité ou application.
2. Lors de la création d'un utilisateur externe, supprimez le rôle snc_internal et ajoutez le rôle nouvellement créé qui hérite du rôle snc_external.
3. Lors de l'ajout du nouveau rôle qui hérite du rôle snc_external à la table existante, vérifiez et validez que la table ne contient aucun enregistrement sensible.
4. Lors de la création d'une table, validez le fait que la table n'est accessible que par les rôles d'utilisateur internes et externes autorisés.
5. Lors de la création de points de terminaison tels que l'API REST scriptée, utilisez GlideRecordSecure ou vérifiez explicitement les rôles à l'aide de canRead(),canWrite(), canUpdate() et canDelete().

Lors de la création d'une table avec le rôle public, assurez-vous que la table ne contient aucun enregistrement sensible pour les utilisateurs externes, y compris les utilisateurs publics non authentifiés.

Autorisation des demandes d'importation (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.importprocessor` demandes d'importation entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.importprocessor
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base sur les demandes d'importation.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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 d'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, reportez-vous à la section Récupération de données à partir d'un fichier au format CSV .
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les demandes d'importation de sources 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 Service SOAP

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Autorisation de demande de PDF (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.pdf` demandes PDF entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.pdf

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base sur les demandes PDF.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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	(Moyen) Sans autorisation appropriée 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 Add a system property .

Surveillance des performances (ACL) (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour contrôler l'accès `glide.security.diag_txns_acl` stats.do, threads.do, thread_pool_stats et replication.do à partir d'une connexion non authentifiée.

Lorsque vous définissez cette propriété sur **true**, elle `glide.security.diag_txns_acl` autorise uniquement l'accès aux éléments suivants pour le compte administrateur :

- https://<nominstance>.servicenow.com/stats.do
- https://<nominstance>.servicenow.com/threads.do
- https://<nominstance>.servicenow.com/replication.do
- https://<nominstance>.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)

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Restreindre l'accès aux pages de configuration au compte administrateur uniquement
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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	(Faible) 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 Add a system property .

Surveillance des performances Restriction IP (renforcement de la sécurité de l'instance)

Utilisez cette `glide.custom.ip.authenticate.allow` propriété pour permettre uniquement l'accès à une liste spécifiée séparée par des virgules ou à une plage d'adresses IP aux pages stats.do, threads.do et replication.do. Si cette propriété n'est pas activée, il est possible d'accéder à ces types de pages à partir de n'importe quelle adresse IP.

Remarque :
Sur la base de modifications récentes, le contrôle d'accès à l'adresse IP doit être utilisé pour toutes les restrictions IP. Reportez-vous à la section Étapes de configuration dans Restreindre l'accès à des plages IP spécifiques.

En savoir plus

Attribut	Description
Nom de la propriété	glide.custom.ip.authenticate.allow
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Limitez l'accès aux pages de configuration aux adresses IP de la liste d'inclusion.
Valeur recommandée	Liste d'adresses IP séparées par des virgules.
Impact fonctionnel	(Faible) Les pages d'informations sensibles sont accessibles même à partir d'une adresse IP non fiable.
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.
Référence	Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Protection de la vie privée sur includes de script pouvant être appelés par le client (renforcement de la sécurité de l'instance)

Par défaut, les script includes pouvant être appelés par le client qui ne définissent pas explicitement la visibilité sont publics. Si nécessaire, ajoutez la propriété pour activer le contrôle de la `glide.script.ccsi.ispublic` confidentialité sur tous les includes de script appelables par les clients accessibles via des pages publiques.

Lorsque vous ajoutez cette propriété, vous devez définir sa valeur sur **false**, ce qui signifie que tous les script includes 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 une valeur **vrai**, ni 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 script include particulier pouvant être appelé par un client en ajoutant la fonction `isPublic( )`.

- Le paramètre `isPublic()` a priorité sur la `glide.script.ccsi.ispublic` propriété.
- Par exemple, si vous définissez `isPublic()` sur **true** dans un script individuel, cela le rend public, ce qui remplace la propriété qui rend privées toutes les autres inclusions de script pouvant être appelées par un `glide.script.ccsi.ispublic` client.

En savoir plus

Attribut	Description
Nom de la propriété	glide.script.ccsi.ispublic
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Rendre privé les includes de script appelables par le client signifie que les invités qui accèdent aux pages publiques ne peuvent pas accéder à l'include de script pouvant être appelé par le client. Un utilisateur non connecté ne peut pas exécuter de script privé.
Valeur recommandée	faux
Impact fonctionnel	(Élevé) 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, les includes de script côté client contournent les ACL, ce qui peut entraîner une fonctionnalité publique non prévue. Si le script client fournit des informations confidentielles, il peut présenter un risque de sécurité potentiel défavorable.
Solution de contournement	Si vous définissez la `glide.script.ccsi.ispublic` propriété sur **false** , tous les script includes pouvant être appelés par le client sont privés.

Attribut	Description
	Vous pouvez modifier le paramètre de confidentialité pour un script include client pouvant être appelé individuel en ajoutant la fonction isPublic(). La fonction isPublic a priorité sur la *glide.script.ccsi.ispublic* propriété. Ajoutez la syntaxe suivante au script include : isPublic :function(){return[vrai/faux] ;},

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Accès public aux favoris

Utilisez le *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 sera conforme si *glide.ui.magellan.favorites.allow_public* défini 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
Objectif	Contrôlez si les utilisateurs non authentifiés sont autorisés à voir **les favoris** dans le navigateur.
Type	vrai/faux
Valeur recommandée	*false*
Dépendances de Security	Définir 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 aux données sensibles.
Références	Créer ou afficher des favoris

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Restreindre l'accès à des plages IP spécifiques (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour restreindre l'accès *com.snc.ipauthenticator* à des plages IP spécifiques. À moins que l'accès public ne soit prévu pour l'instance, les administrateurs doivent limiter l'accès aux blocs réseau IP qui leur sont affectés.

Prérequis

Avant de définir cette propriété, vous devez activer le module d'extension IP Range Based Authentication `com.snc.ipauthenticator` . Pour en savoir plus, consultez Authentification basée sur la plage IP la section Étapes de configuration (ci-dessous).

En savoir plus

Attribut	Description
Nom du module d'extension	com.snc.ipauthenticator
Type de configuration	Sécurité du système > contrôle d'accès à l'adresse IP
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour ajouter la plage d'adresses IP qui peut ou ne peut pas accéder à l'instance aux listes des domaines approuvés et non approuvés.
Valeur recommandée	Actif
Impact fonctionnel	(Faible) Les plages IP refusées par le client sont utilisées pour cet élément de rattrapage. 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**.
3. Cliquez sur **Nouveau** pour créer une liste d'exclusion (refuser) ou une liste d'inclusion (Autoriser) d'adresses IP.
4. Cliquez sur **Envoyer**.

Autorisation de demande de RSS (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.rss` demandes RSS entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.rss
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base sur les demandes RSS.
Valeur recommandée	VRAI

Attribut	Description
Impact fonctionnel	(Faible) 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 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, consultez Générateur de flux RSS.
Risque de sécurité	(Moyen) Sans autorisation appropriée 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

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property.

Profil SSO du navigateur Web SAML 2.0 (renforcement de la sécurité de l'instance)

Le `com.snc.integration.sso.saml20.update1` module d'extension garantit que l'état du module d'extension SAML 2.0 Single Sign-On est actif.

SAML (Security Assertion Markup Language) est une norme basée sur 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).

Le `com.snc.integration.sso.saml20.update1` module d'extension est requis, mais vous n'avez pas besoin de l'activer manuellement. Le site `sso.multi.installer` installe tous les modules d'extension requis liés à SAML et contient également des scripts d'implémentation saml2 qui fournissent des options pour la validation des réponses. Pour en savoir plus, consultez les rubriques de la section Références de la section En savoir plus.

En savoir plus

Attribut	Description
Nom du module d'extension	com.snc.integration.sso.saml20.update1 (nouveau)
Type de configuration	Définition du système > Modules d'extension
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour se prémunir contre les attaques de script de site à site.
Valeur recommandée	Actif

Attribut	Description
Rôle requis	Votre administrateur ne peut pas activer le module d'extension. Demandez à la personne ayant des privilèges de sécurité élevés de l'activer sur l'instance.
Références	Authentification avec intégration SAML SAML Authentification Mettre à jour votre intégration SAML 2.0 existante

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à Activate a plugin .

Autorisation de demande de script (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.scriptedprocessor` demandes de script entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.scriptedprocessor
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base sur les demandes de scripts.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Ce rattrapage applique 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 Add a system property .

Démarrage rapide de la sécurité (règles ACL) (renforcement de la sécurité de l'instance)

Activez le module d'extension Security Jump Start (ACL Rules) (`com.snc.system_security`) pour créer plusieurs ACL importantes qui valident les contrôles d'accès sur certaines des tables clés du système dans .Now Platform

Ces règles permettent de démarrer rapidement la sécurisation de nombreuses tables système, simplifiant ainsi 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
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Activez le module d'extension de démarrage rapide de la sécurité (règles ACL) pour obtenir une conformité de sécurité appropriée. Il fournit des ACL de base qui sécurisent les tables système au lieu de les créer manuellement pour chaque table système fournie avec la mise en service par défaut d'une instance. Ces ACL sont utiles lorsque l'instance nouvellement créée doit passer rapidement en production.
Valeur recommandée	Actif
Impact fonctionnel	(Moyen) L'installation de ce module d'extension sans audit des ACL existantes sur l'instance a un impact fonctionnel important. La sensibilisation et les définitions des clients sont requises avant que le rattrapage 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 pour sécuriser de nombreuses tables système afin de faciliter la mise en production rapide d'une organisation.
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 d'ACL fournies par le module d'extension, vous pouvez créer manuellement une ou plusieurs d'entre elles dans une instance existante si nécessaire. Cette liste d'ACL peut être utilisée à titre indicatif dans ce cas.

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à Activate a plugin .

Module d'extension SNC Access Control (renforcement de la sécurité de l'instance)

Activez le module d'extension SNC Access Control (*com.snc.snc_access_control*) pour contrôler l'accès du personnel à vos instances Service et assistance client .

La configuration par défaut de permet Now Platform au service client et au support d'accéder aux instances via un processus interne qui crée des informations d'identification de support à court terme. Bien que tous les accès soient audités, certains clients préfèrent contrôler cet accès.

Ce module d'extension permet à l'administrateur client Service et assistance client d'interdire aux employés d'accéder à l'instance. Cette décision a un impact sur les SLA de support, car vous devez activer Now Platform l'accès avant que les activités de support puissent commencer. Pour en savoir plus, consultez Contrôle d'accès ServiceNow.

En savoir plus

Attribut	Description
Nom du module d'extension	com.snc.snc_access_control
Type de configuration	Définition du système > Modules d'extension
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Interdit Service et assistance client aux employés d'accéder à l'instance
Valeur recommandée	Actif
Rôle requis	L'administrateur client ne peut pas activer ce module d'extension. Elle doit faire l'objet d'une demande explicite, car l'activation du module d'extension nécessite des privilèges élevés.
Impact fonctionnel	(Faible) Si ce module d'extension est inactif, tous les Service et assistance client employés peuvent accéder à l'instance du client. L'activation du module d'extension permet au client de restreindre l'accès aux employés autorisés Service et assistance client uniquement.
Risque de sécurité	(Faible) 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 ce module d'extension, suivez les étapes décrites dans Activation du contrôle d'accès ServiceNow. Les clients doivent demander le module d'extension SNC Access Control (com.snc.snc_access_control) auprès de HI.
2. Pour activer le contrôle d'accès SNC, procédez comme suit dans Configuration ServiceNow du contrôle d'accès. Configurez un enregistrement de contrôle d'accès pour spécifier un ou plusieurs Service et assistance client employés qui ont l'autorisation de se connecter à votre instance.

Vérification du type de contenu SOAP (renforcement de la sécurité de l'instance)

Utilisez cette 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.

- Lorsqu'elle est définie sur **vrai**, elle Now Platform valide le type de contenu comme texte/xml et protège contre les demandes SOAP invalides.
- Si la valeur est définie sur **false**, toutes les valeurs de type de contenu sont autorisées.

En savoir plus

Attribut	Description
Nom de la propriété	glide.soap.require_content_type_xml
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Protégez-vous contre les demandes SOAP invalides
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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	(Élevé) Lors de l'acceptation des demandes SOAP entrantes, la validation appropriée est effectuée pour s'assurer que le type de contenu pertinent est défini dans le cadre de la demande. Elle restreint les réponses SOAP invalides qui peuvent être considérées comme un risque pour la sécurité.
Référence	Types de contenus

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Restriction IP stricte (renforcement de la sécurité de l'instance)

Utilisez cette `glide.ip.authenticate.strict` propriété pour permettre à un ensemble strict d'adresses IP, tel que DC et VPN sécurisé, d'accéder à cette instance.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ip.authentifier.strict
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Permet aux employés de ServiceNow d'accéder à l'instance uniquement par le biais d'un ensemble sécurisé de plages IP
Valeur recommandée	VRAI
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).

Attribut	Description
	Remarque : Si vous définissez cette propriété sur vrai, une propriété plus restrictive `glide.ip.authenticate.allow.secured` est utilisée Now Platform au lieu de 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

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Remarque :
Une règle de refus de tout doit être ajoutée au contrôle d'accès IP pour restreindre l'accès à partir de n'importe quelle adresse IP qui n'est pas ajoutée au contrôle d'accès IP. Toutes les adresses IP autorisées requises doivent ensuite être ajoutées au contrôle d'accès IP.

Autorisation de la demande de déchargement (renforcement de la sécurité de l'instance)

Utilisez la propriété (useUnloadFormat) pour indiquer si les `glide.basicauth.required.unl` demandes de déchargement entrantes doivent requérir 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)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base sur les demandes de déchargement.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) 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.
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.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Autorisation de demande WSDL (renforcement de la sécurité de l'instance)

Utilisez cette `glide.basicauth.required.wsdl` propriété pour indiquer si les demandes WSDL (Web Services Description Language) entrantes doivent requérir une authentification de base.

Remarque :
Si vous choisissez de ne pas exiger l'authentification de base pour les demandes WSDL entrantes, vous devez modifier les règles Access Control (ACL) pour permettre aux utilisateurs invités d'accéder au contenu WSDL.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.wsdl
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base sur les demandes WSDL.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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 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 au contenu/aux données WSDL sensibles sur l'instance cible.
Références	Sécurité des services Web

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Autorisation de demande XML (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.xml` demandes XML entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.xml
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base sur les demandes XML.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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 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, reportez-vous à la section Étape de l'analyseur XML .
Risque de sécurité	(Moyen) 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

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Autorisation de demande XSD (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.xsd` demandes XSD (XML Schema Definition) entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.xsd
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base sur les demandes XSD.
Valeur recommandée	VRAI

Attribut	Description
Impact fonctionnel	(Faible) 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 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, reportez-vous à la section Sessions non interactives .
Risque de sécurité	(Moyen) 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

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Pièces jointes (renforcement de la sécurité de l'instance)

De nombreux Now Platform processus d'affaires permettent le téléchargement de données/informations. Il vérifie régulièrement la validité et la sécurité du texte, mais l'acceptation de ces fichiers peut introduire encore plus de risques.

Pour réduire le risque, vous devez valider les fichiers malveillants afin qu'ils Now Platform puissent se protéger correctement contre les attaquants qui envoient ces fichiers. Vous gérez ces fichiers en incluant une logique métier qui analyse les fichiers pendant le processus de chargement et rejette les fichiers perçus comme malveillants.

Références internes

- Administration des pièces jointes
- Configurer les propriétés système des pièces jointes

Types MIME téléchargeables (renforcement de la sécurité de l'instance)

Utilisez cette `glide.ui.attachment.download_mime_types` propriété pour spécifier une liste de types MIME de pièces jointes séparés par des virgules qui doivent être téléchargés, mais qui ne doivent pas être affichés dans le navigateur.

Pour afficher une liste des types MIME existants, tapez `/sys_attachment_icon_rule_list.do`. Vous pouvez activer l'un de ces types MIME pour satisfaire aux exigences de conformité de sécurité dans le Now Platform.

Remarque :
Si vous définissez la propriété **Forcer le téléchargement des types MIME** sur **true**, elle remplace la propriété **Types MIME téléchargeables** , qui est une liste de types MIME téléchargeables séparés par des virgules. Pour en savoir plus, consultez Forcer le téléchargement des types MIME.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.attachment.download_mime_types
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour empêcher l'affichage des types de fichiers dans le navigateur afin d'éviter toute exécution de script malveillante cachée.
Valeur recommandée	Certains types de fichiers définis, par exemple, text/html, text/csv.
Impact fonctionnel	(Faible) Cette correction impose l'exécution de contrôles de validation avant d'effectuer une action lorsque vous cliquez sur une pièce jointe dans une Now Platform application. Il n'y a pas d'impact potentiel, mais l'expérience utilisateur est altérée.
Risque de sécurité	(Moyen) Les vecteurs d'attaque de scripting côté client se déclinent en différents types et l'abus de pièce jointe de type MIME ne fait pas exception. Les attaquants peuvent abuser des types MIME et placer du contenu de script involontaire dans la pièce jointe du côté de la victime pour capturer des informations sensibles. Dans le contexte actuel, renseignez la propriété avec une liste de types MIME de pièces jointes séparés par des virgules qui ne doivent pas être affichés en ligne dans le navigateur. Exemple : texte/html

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Activer la liste de refus pour les pièces jointes (renforcement de la sécurité de l'instance)

Utilisez la `glide.security.attachment_type.use_blacklist` propriété pour indiquer si le Now Platform doit valider la pièce jointe par rapport à une liste d'exclusion spécifiée.

Remarque :
Ne définissez pas la `glide.security.attachment_type.use_blacklist` propriété sur `vrai` tant que vous n'avez pas configuré les `glide.attachment.blacklisted.extensions` propriétés and `glide.attachment.blacklisted.types` . Pour en savoir plus, consultez Spécifier les extensions refusées et Spécifier les types de fichiers refusés.

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.attachment_type.use_blacklist
Type de configuration	Propriétés système (/sys_properties_list.do)

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Limitez l'opération de chargement (Insérer/Écrire/Mettre à jour) des pièces jointes dont les extensions et les types de fichiers douteux sont douteux, tels que exe, dll, jar, text/html.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Aucun impact sur les fonctionnalités, sauf en cas de tentative de chargement d'extensions ou de types de fichiers spécifiés dans les propriétés répertoriées pour l'exclusion (`glide.attachment.blacklisted.extensions` et `glide.attachment.blacklisted.types`)
Risque de sécurité	(Moyen) Un utilisateur malveillant peut télécharger une pièce jointe infectée par un logiciel malveillant avec des extensions et/ou des types de fichiers exécutables courants.
Solution de contournement	Des propriétés qui résolvent le même problème avec des listes d'inclusion et non des listes d'exclusion sont disponibles. Pour en savoir plus, consultez : • Restreindre les extensions de fichiers • Restriction de type MIME de téléchargement

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Activer les restrictions de téléchargement de fichiers (renforcement de la sécurité de l'instance)

Utilisez cette 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, qui crée une liste délimitée par des virgules des types de fichiers téléchargeables restreints. Pour en savoir plus, reportez-vous à la section Types de fichiers téléchargeables.

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)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Permet de s'assurer que les types de fichiers sûrs peuvent être téléchargés à partir de l'application.
Valeur recommandée	VRAI

Attribut	Description
Impact fonctionnel	(Faible) Cette correction applique la restriction des téléchargements de fichiers en fonction des valeurs spécifiées dans la `glide.ui.strict_customer_uploaded_content_types` propriété. Pour en savoir plus, reportez-vous à la section Types de fichiers téléchargeables.
Risque de sécurité	(Moyen) Les restrictions de téléchargement de fichiers doivent être appliquées à toutes les sources d'entrée utilisateur non approuvées.

Appliquer un chargement d'image utilisateur strict (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer le `glide.security.strict.user_image_upload` contrôle d'accès pour le téléchargement ou la mise à jour d'une photo de profil lorsqu'il est effectué sur un enregistrement utilisateur.

Ce paramètre ouvre la possibilité pour un utilisateur non autorisé de télécharger 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 lors des 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)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour restreindre le téléchargement de l'image de l'utilisateur aux utilisateurs autorisés.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Aucun impact sur les fonctionnalités, car les utilisateurs autorisés peuvent toujours télécharger des images sur leur profil d'utilisateur.
Risque de sécurité	(Moyen) Lorsque vous définissez cette propriété sur **faux**, 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 Add a system property .

Forcer les types MIME de téléchargement (renforcement de la sécurité de l'instance)

Utilisez cette `glide.ui.attachment.force_download_all_mime_types` propriété pour forcer le téléchargement de toutes les pièces jointes de type MIME.

Remarque :
Si vous définissez la propriété **Forcer le téléchargement des types MIME** sur **true**, elle remplace la propriété **Types MIME téléchargeables** , qui est une liste de types MIME téléchargeables séparés par des virgules. Pour en savoir plus, consultez Types MIME téléchargeables.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.attachment.force_download_all_mime_types
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Pour forcer le téléchargement de toutes les pièces jointes, au lieu de s'exécuter dans le navigateur.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction impose le téléchargement de toutes les pièces jointes. Aucun impact sur les fonctionnalités, mais il en résulte une altération de l'expérience utilisateur.
Risque de sécurité	(Élevé) Pour réduire les attaques de scripting côté client, les pièces jointes de fichier doivent être téléchargées de force plutôt que d'être rendues dans le contexte du navigateur.
Références	Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Restreindre les extensions de fichiers (renforcement de la sécurité de l'instance)

Définissez les types de fichiers qui peuvent être téléchargés sur votre instance à l'aide de la `glide.attachment.extensions` propriété système. Cette propriété utilise une liste de types d'extensions de fichier autorisés séparés par des virgules. Seuls les types d'extensions de fichier spécifiés peuvent être chargés en tant que pièces jointes.

Utilisez la `glide.attachment.extensions` propriété sur votre instance pour fournir les avantages suivants :

Amélioration de la sécurité

Utilisez cette propriété pour améliorer la sécurité en empêchant les utilisateurs de télécharger des fichiers nuisibles, tels que des virus, en tant que pièces jointes. Sécurisez votre instance en bloquant les types généralement utilisés par les programmes exécutables ou les scripts.

Éviter les types de fichiers incompatibles

Utilisez cette propriété pour empêcher les utilisateurs de charger des fichiers incompatibles. Par exemple, certains navigateurs ne prennent pas en charge les icônes au format PNG. En n'incluant pas l'extension de fichier `png` , vous pouvez empêcher les utilisateurs de télécharger des fichiers PNG.

Important :
Cette propriété ne restreint pas les fichiers en fonction du type de fichier réel (type MIME), mais uniquement en fonction de l'extension. Pour restreindre les chargements basés sur le type MIME, configurez la propriété une fois que vous avez terminé la `glide.security.file.mime_type.validation`glide.attachment.extensions configuration. Pour obtenir des détails sur la configuration `glide.security.file.mime_type.validation`de , consultez Restriction de type MIME de téléchargement.

Étapes de configuration

1. Dans le navigateur de filtre de votre instance, saisissez sys_properties.list, puis appuyez sur Entrée.
2. Recherchez et ouvrez la `glide.attachment.extensions` propriété.
3. Dans le champ **Valeur** , saisissez les extensions de fichier dont vous souhaitez autoriser le chargement en tant que pièces jointes. Séparez les entrées du champ par des virgules. Voici un exemple de valeur pour plusieurs entrées `doc,docx,xls,xlxs,pdf,jpeg,jpg,png,ico`.

   Remarque :
   Si aucun type de fichier n'est spécifié dans le champ **Valeur** , n'importe quel type de fichier peut être chargé en tant que pièce jointe.

4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

En savoir plus

Attribut	Description
Nom de la propriété	glide.attachment.extensions
Type de configuration	Propriété système (/sys_properties_list.do)
Configurable dans Centre de sécurité de l'instance	Non
Objectif	Pour n'activer que les extensions de fichier acceptables à télécharger pendant la pièce jointe. Il bloque toute tentative de téléchargement d'extensions potentiellement malveillantes.
Valeur recommandée	Certaines extensions de fichiers définies, telles que doc, docx, pdf, xls, xlsx
Impact fonctionnel	(Moyen) Cette correction restreint toutes les extensions de fichiers, à l'exception de celles qui figurent dans la liste d'inclusion. Aucun impact sur les fonctionnalités, sauf en cas de tentative de chargement d'un fichier autre que les extensions acceptables par l'organisation.
Risque de sécurité	(Moyen) Comme la vérification du type MIME dépend de cette propriété, il est recommandé d'atténuer les vulnérabilités liées au chargement de fichiers malveillants.

Restreindre l'accès non authentifié aux pièces jointes (renforcement de la sécurité de l'instance)

Utilisez cette `glide.image_provider.security_enabled` propriété pour contrôler les paramètres de sécurité des images. Si la valeur est définie sur **true**, les images ne sont

visibles que par les utilisateurs authentifiés et autorisés. Si la valeur est définie sur **false**, les images sont visibles par toutes les personnes qui possèdent l'URL de la pièce jointe.

En savoir plus

Attribut	Description
Nom de la propriété	glide.image_provider.security_enabled
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour empêcher l'accès non authentifié à la pièce jointe lorsqu'elle est rendue au format .iix.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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	(Élevé) Une 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 Add a system property .

Spécifier les extensions de pièce jointe exclues (renforcement de la sécurité de l'instance)

Lorsque vous activez la validation de la liste d'exclusion dans le Now Platform, utilisez la `glide.attachment.blacklisted.extensions` propriété pour créer une liste délimitée par des virgules des types d'extensions de fichiers téléchargeables restreints. Le téléchargement des types d'extensions de fichiers spécifiés est limité.

Prérequis

Définissez cette propriété avant de définir la `glide.security.attachment_type.use_blacklist` propriété sur vrai. Pour en savoir plus, consultez Activer la liste noire pour les pièces jointes.

En savoir plus

Attribut	Description
Nom de la propriété	glide.attachment.blacklisted.extensions
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui

Attribut	Description
Objectif	Limitez l'opération de téléchargement (Insérer/Écrire/Mettre à jour) des pièces jointes dont l'extension de fichier est douteuse.
Type	Chaîne
Valeur recommandée	Extensions de fichiers spécifiées par l'utilisateur. Les exemples courants incluent ex, dll, xslx.
Impact fonctionnel	(Faible) Aucun impact sur la fonctionnalité, sauf en cas de tentative de chargement d'une extension de fichier spécifiée sous cette propriété.
Risque de sécurité	(Moyen) Un utilisateur malveillant peut télécharger une pièce jointe infectée par un logiciel malveillant avec des extensions de fichiers exécutables courantes.
Solution de contournement	Les propriétés sont disponibles dans les fonctionnalités du système de base qui résolvent le même problème, avec une liste d'inclusion au lieu d'une liste d'exclusion. Pour en savoir plus, consultez : • Restreindre les extensions de fichiers • Restriction de type MIME de téléchargement

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Spécifier les types de fichiers de pièces jointes exclus (renforcement de la sécurité de l'instance)

Lorsque la validation de la liste d'exclusion est activée dans le Now Platform, utilisez la `glide.attachment.blacklisted.types` propriété pour créer une liste de types de fichiers téléchargeables restreints délimitée par des virgules. Le chargement des types de fichiers spécifiés est limité.

Prérequis

Définissez cette propriété avant de définir la `glide.security.attachment_type.use_blacklist` propriété sur vrai. Pour en savoir plus, consultez Activer la liste noire pour les pièces jointes.

En savoir plus

Attribut	Description
Nom de la propriété	glide.attachment.blacklisted.types
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Limitez l'opération de chargement (Insérer/Écrire/Mettre à jour) des pièces jointes dont le type de fichier est douteux. Exemple : text/html.
Valeur recommandée	Quelques types de fichiers définis (par exemple : text/html,text/csv).

Attribut	Description
Impact fonctionnel	(Faible) Aucun impact sur la fonctionnalité, sauf en cas de tentative de chargement d'un type de fichier spécifié sous cette propriété.
Risque de sécurité	(Moyen) Un utilisateur malveillant peut télécharger une pièce jointe infectée par un programme malveillant avec des types de fichiers exécutables courants.
Solution de contournement	Les propriétés sont disponibles dans les fonctionnalités du système de base qui résolvent le même problème avec la liste d'inclusion plutôt qu'avec la liste d'exclusion. Pour en savoir plus, consultez : • Restreindre les extensions de fichiers • Restriction de type MIME de téléchargement

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Types de fichiers téléchargeables (renforcement de la sécurité de l'instance)

Utilisez cette `glide.ui.strict_customer_uploaded_content_types` propriété pour créer une liste délimitée par des virgules des types de fichiers téléchargeables restreints. Les types de fichiers spécifiés sont les seuls qui peuvent être téléchargés en tant que contenu statique à partir d'une instance.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.strict_customer_uploaded_content_types
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Permet de s'assurer que seuls les types de fichiers figurant dans les listes d'inclusion sont autorisés à être téléchargés.
Valeur recommandée	Spécifié par l'utilisateur (commun : doc, docx, xls, xlsx, pdf, etc.)
Impact fonctionnel	(Moyen) Seuls les fichiers figurant sur des listes d'inclusion peuvent être téléchargés, ce qui peut affecter la politique de l'organisation. La liste d'inclusion, séparée par des virgules, doit être modifiée pour se conformer à la politique de l'organisation en matière de types de fichiers téléchargeables acceptables.
Risque de sécurité	(Faible) Les restrictions de téléchargement de fichiers doivent être appliquées à toutes les sources d'entrée utilisateur non approuvées.
Références	Propriétés des paramètres de sécurité Types de contenus

Étapes de configuration

1. Accédez à la **/sys_properties_list.do**.
2. Recherchez la propriété `glide.ui.strict_customer_uploaded_content_types`.
3. Spécifiez les types de fichiers téléchargeables acceptables dans une liste séparée par des virgules comme indiqué, puis cliquez sur **Mettre à jour**. Voici un exemple de valeur correctement formatée pour la liste `ico,gif,png,jpg,jpeg,bmp,ogg,mp3,doc,docx,xls,pdf`.

Restriction de type MIME de téléchargement (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour activer la `glide.security.file.mime_type.validation` vérification du type MIME pour les chargements. Vous pouvez activer (propriété sur **true**) ou désactiver (définir la propriété sur **false**) pour les fichiers en pièces jointes.

Prérequis

Avant de définir cette propriété, définissez-la `glide.attachment.extensions` . Le type MIME est vérifié uniquement pour les extensions spécifiées dans `glide.attachment.extensions` lors du chargement. Pour en savoir plus, reportez-vous à la section Restreindre les extensions de fichiers.

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.file.mime_type.validation
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer la vérification du type MIME / des octets magiques pendant les chargements de fichiers.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction permet la vérification du 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 téléchargements de fichiers malveillants, la vérification du type MIME doit être activée.
Références	Administration des pièces jointes

Consultez Paramètres de la sécurisation pour la sécurité de l'instance pour plus d'informations 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 Add a system property .

Sécurité des e-mails (renforcement de la sécurité de l'instance)

Cette section contient des contrôles 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.

Convertir les e-mails entrants en HTML (renforcement de la sécurité de l'instance)

Utilisez cette `glide.email.inbound.convert_html_inline_attachment_references` propriété pour spécifier si le code HTML de l'e-mail entrant doit être converti afin que les images de l'e-mail apparaissent dans l'aperçu HTML du corps de l'e-mail.

Les actions suivantes se produisent lorsque la `glide.email.inbound.convert_html_inline_attachment_reference` propriété système est définie sur false :

- Dans le , des Now Platformliens cid (content ID) rompus apparaissent à la place des images reçues. Le format dans lequel l'image de l'e-mail apparaît dépend du paramètre de propriété au moment de la réception de l'e-mail, et non du paramètre de propriété actuel.
- Le contenu « malveillant » reçu dans la pièce jointe n'est pas référencé dans le code HTML de l'e-mail. La pièce jointe elle-même est stockée dans la table sys_attachment.
- Le traitement des e-mails entrants ne mettra pas à jour les données HTML de l'e-mail pour refléter l'emplacement stocké de la pièce jointe dans la table sys_attachment. Il en résulte ce qui suit :
  - Les images en ligne n'apparaissent pas dans l'affichage d'e-mail du formateur d'activité.

    Remarque :
    Pour résoudre ce problème avec le formateur d'activité, vérifiez d'abord s'il n'existe aucun problème de sécurité. Définissez ensuite la `glide.email.inbound.convert_html_inline_attachment_reference` propriété système sur**vrai** pour permettre aux futurs e-mails reçus de contenir l'URL HTML nécessaire pour référencer l'image. La modification de la propriété ne met pas à jour les e-mails déjà reçus. La nouvelle valeur affecte uniquement les e-mails entrants reçus après la modification de la propriété.

  - Les images en ligne n'apparaissent pas lorsque l'e-mail est affiché dans l'aperçu HTML de l'e-mail.
  - Lors de l'ajout d'email.body_htm dans des actions entrantes entre des balises de code, les images sont manquantes.

Prérequis

Avant de définir cette propriété, définissez-la `glide.email.read.active` sur vrai. Pour en savoir plus, consultez Activer l'utilisation de votre propre serveur POP3 .

En savoir plus

Attribut	Description
Nom de la propriété	glide.email.inbound.convert_html_inline_attachment_references
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui

Attribut	Description
Objectif	Pour restreindre le rendu de l'image dans l'aperçu du corps HTML.
Valeur recommandée	faux
Impact fonctionnel	(Moyen) Une fois cette propriété configurée, l'utilisateur ne peut pas voir l'aperçu de l'image dans le corps de l'e-mail.
Risque de sécurité	(Moyen) Si la propriété n'est pas activée, un attaquant peut envoyer une image malveillante contenant des logiciels malveillants.
Références	Propriétés d'e-mail Configuration des messages entrants

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Filtrage et notation des e-mails indésirables (renforcement de la sécurité de l'instance)

Installez le module d'extension Email Filter (`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.

Chaque message envoyé via Now Platform des serveurs de messagerie est évalué pour la probabilité d'être un spam.

Remarque :
Si une instance utilise un serveur de messagerie privé, cette rubrique ne s'applique pas. Pour plus d'informations, reportez-vous à la section Notation et filtrage des courriers indésirables.

Prérequis

Avant de définir cette propriété :

- Définissez la propriété `glide.email.read.active` sur true. Pour en savoir plus, consultez Activer l'utilisation de votre propre serveur POP3 .
- Ce filtre remplace la `glide.pop3.ignore_headers` propriété. Pour en savoir plus, reportez-vous à la section Propriétés système disponibles .

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.email_filter
Type de configuration	Définition du système > Modules d'extension
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer un filtrage afin d'éviter le spamming d'e-mails.
Valeur recommandée	Actif
Impact fonctionnel	(Faible) Les e-mails ne sont jamais filtrés, bloqués ou mis en quarantaine de l'instance dans le cadre du score de courrier

Attribut	Description
	indésirable. Elles sont seulement notées, puis envoyées à l'instance. Tout le filtrage est effectué dans l'instance avec le module d'extension Email Filters.
Risque de sécurité	(Moyen) Les filtres d'e-mail permettent aux administrateurs d'utiliser un créateur de condition ou un script conditionnel pour spécifier quand ignorer les e-mails entrants malveillants provenant d'expéditeurs connus/inconnus.
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 Activate a plugin .

Restreindre l'accès aux e-mails dont la table cible est vide (renforcement de la sécurité de l'instance)

Activez la propriété pour restreindre l'accès `glide.email.email_with_no_target_visible_to_all` de l'utilisateur aux e-mails, sauf s'il en est l'expéditeur ou qu'il possède le rôle administrateur.

Les utilisateurs non autorisés peuvent accéder aux e-mails de la table E-mails [sys_email] qui n'ont pas d'enregistrement cible. Au lieu d'appliquer des ACL aux entrées d'e-mail, cette propriété restreint l'accès uniquement à l'expéditeur de l'e-mail et aux utilisateurs disposant du rôle administrateur.

Remarque :
Les e-mails envoyés et reçus par l'instance apparaissent dans la table E-mails [sys_email]. Toutefois, seuls les e-mails reçus qui ont été marqués avec un état Erreur et Ignoré devraient 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]
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour empêcher le client de messagerie d'afficher les e-mails lorsque l'utilisateur n'autorise pas l'accès.
Valeur recommandée	faux
Impact fonctionnel	(Faible) 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	(Moyen) Si la propriété n'est pas activée, les utilisateurs non autorisés peuvent accéder à n'importe quel e-mail dont le champ target_table est vide.

Attribut	Description
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 Add a system property .

Restreindre les e-mails par domaine pour la création d'utilisateurs (renforcement de la sécurité de l'instance)

Utilisez cette `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.

Par défaut, un astérisque (*) est utilisé pour approuver tous les domaines. Des domaines spécifiques doivent être fournis s'il n'est pas nécessaire d'autoriser les e-mails provenant de tous les domaines. L'instance ignore les e-mails entrants provenant d'autres domaines, sauf s'ils proviennent de l'adresse d'un utilisateur existant. L'instance ne crée pas d'utilisateurs invités à partir d'e-mails provenant de domaines non approuvés.

Prérequis

Avant de définir cette propriété :

- Définissez la propriété `glide.email.read.active` sur true. Pour en savoir plus, consultez Activer l'utilisation de votre propre serveur POP3 .
- Définissez la propriété `glide.pop3readerjob.create_caller` sur true. Pour en savoir plus, reportez-vous à la section Activer la création automatique d'utilisateurs .

> **Remarque :**
> Ignorez la `glide.user.default_password` propriété si elle `glide.pop3readerjob.create_caller` est définie sur **faux**.

En savoir plus

Attribut	Description
Nom de la propriété	glide.user.trusted_domain
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Valeur recommandée	Liste des domaines de confiance séparés par des virgules [par exemple, servicenow.com (un nom de domaine spécifique)].
Impact fonctionnel	(Moyen) 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	(Moyen) Si la propriété n'est pas activée, un attaquant peut utiliser une campagne d'usurpation d'adresse e-mail/spamming

Attribut	Description
	pour envoyer plusieurs e-mails, ce qui entraîne la création d'utilisateurs invités plus inutiles.
Références	Propriétés d'e-mail Configuration des messages entrants

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Validation de l'entrée (renforcement de la sécurité de l'instance)

Le Now Platform effectue la validation de l'entrée pour éviter les problèmes résultant de la saisie de données mal formées.

Cette section décrit les Now Platform contrôles de sécurité qu'un administrateur peut configurer pour minimiser la saisie de données mal formées, quelle qu'en soit la source. Ces sources incluent la saisie manuelle de l'utilisateur, ou provenant d'une infrastructure, d'entités externes ou de systèmes de base de données.

Autoriser le code HTML intégré (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour désactiver la `glide.ui.security.allow_codetag` prise en charge de l'incorporation du code HTML créé à l'aide de la balise [code].

Il Now 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 des entrées au format HTML pour les champs de journal. Toutefois, les champs journal peuvent afficher du texte encadré par des balises de code au format HTML.

- Cependant, il existe un risque de sécurité associé. Si `la valeur est définie sur vrai`, les utilisateurs malveillants peuvent écrire du code HTML JS nuisible qui peut être exécuté sur un autre navigateur client après le rendu des champs de journal.
- Définissez cette propriété sur `false` afin que les administrateurs puissent empêcher les champs 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)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Protégez-vous contre le script site à site et l'exécution de scripts malveillants
Valeur recommandée	faux
Impact fonctionnel	(Moyen) Cette correction applique le codage HTML sur l'interface utilisateur et renvoie les résultats codés à l'utilisateur.

Attribut	Description
	Cette propriété est définie sur `true` par défaut. Dans cet état, votre instance affiche le rendu HTML dans les champs et formulaires de journal. Si cette propriété est définie sur `false`, le HTML n'est pas restitué correctement et des balises HTML peuvent apparaître dans les champs 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 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.
Références	Restreindre la balise CODE dans les champs journal Afficher les entrées de 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 Add a system property .

Autoriser les balises JavaScript dans le HTML intégré (renforcement de la sécurité de l'instance)

La *`glide.ui.security.codetag.allow_script`* propriété désactive la prise en charge de l'incorporation du code JavaScript HTML créé à l'aide de la balise [code].

Remarque :
Cette propriété est définie sur **true** par défaut dans Vancouver la version et les 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 client.

Il Now 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 de journal. Toutefois, les champs journal peuvent restituer le texte compris entre des balises de code au format HTML.

- 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 autre navigateur client après le rendu des champs de journal.
- Définissez cette propriété sur **false** afin que les administrateurs puissent empêcher les champs journal de rendre le code JavaScript HTML en désactivant la prise en charge de la balise `[code]`.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.security.codetag.allow_script
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Protège contre le script intersite et l'exécution de scripts malveillants
Valeur recommandée	faux
Impact fonctionnel	(Moyen) Cette correction applique l'échappement JavaScript sur l'interface utilisateur et renvoie les résultats codés à l'utilisateur. Elle peut avoir un impact sur les fonctionnalités 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 de l'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 journal Afficher les entrées de 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 Add a system property .

Vérifier le HTML non désinfecté (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour appliquer le *com.glide.security.check_unsanitized_html* comportement de nettoyage de translated_html champs à un niveau global pour les affectations de champs.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ fournit la fonctionnalité de mise en forme du contenu à l'aide de balises HTML (par exemple, <p>, , <a href>, <b><font><img>,). Pour empêcher toute activité malveillante, certaines balises HTML peuvent être interdites à l'aide d'une liste de blocage. Cette propriété empêchera l'utilisation de balises non autorisées 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 les balises HTML bloquées sur translated_html champs.

En savoir plus

Attribut	Description
Nom de la propriété	com.glide.security.check_unsanitized_html
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
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`*
Impact fonctionnel	(Moyen) 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 la mise en forme.
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 des utilisateurs dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Assainisseur HTML

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Bac à sable pour les scripts générés par le client (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour activer le *`glide.script.use.sandbox`* sandboxing des scripts.

Il existe deux cas dans le Now Platform qui permettent au client d'envoyer des scripts au serveur pour évaluation :

Filtres ou requêtes

Il est légal d'envoyer un filtre au serveur tel que `assigned_to=JavaScript :getMyGroups()`.

API système

L'appel d'API permet au client d'exécuter des scripts arbitraires sur le serveur et de recevoir une réponse.

Si vous activez le sandboxing des scripts, le script évalué à l'un de ces deux points d'entrée s'exécute dans un bac à sable avec des droits réduits, avec les caractéristiques suivantes :

- Seules les règles métier marquées Client pouvant être appelé sont disponibles dans le bac à sable.
- Seules les includes de script marquées Client pouvant être appelé sont disponibles dans le bac à sable.
- Certains appels d'API (en grande partie, mais pas entièrement, limités à ceux traitant d'un accès direct à la base de données ne sont pas autorisés.

- Vous ne pouvez pas insérer, mettre à jour ou supprimer des données depuis le bac à sable. Par exemple, tous les appels à current.update() sont ignorés. Si vous exécutez le sans activer le sandboxing des Now Platform scripts, aucune de ces restrictions ne s'applique.

En savoir plus

Attribut	Description
Nom de la propriété	glide.script.use.sandbox
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Applique la validation pour les requêtes JavaScript côté client qui sont lancées sur la plateforme
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) Cette correction applique la validation des requêtes JavaScript côté client lancées sur le Now Platformfichier . Il y a un impact potentiel si le client a des personnalisations qui incluent des requêtes JavaScript codées en dur pour effectuer des opérations CRUD.
Risque de sécurité	(Élevé) Le Now Platform fournit une grande variété de fonctions et de fonctionnalités via des requêtes JavaScript. Cependant, en l'absence d'autorisation et de validation appropriées, il est possible qu'un attaquant effectue des opérations non autorisées contre la plateforme.
Références	Configuration de la propriété de bac à sable de script *glide.script.use.sandbox* appartient à la même famille de propriétés qui sécurisent et restreignent l'exécution des scripts provenant du client : • *glide.script.allow.ajaxevaluate*: voir Activer AJAXEvaluate. • *glide.script.secure.ajaxgliderecord*: voir Activation de la vérification de l'ACL de AJAXGlideRecord.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Activer AJAXEvaluate (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour restreindre l'exécution *glide.script.allow.ajaxevaluate* arbitraire du script client à l'aide de l'API système côté serveur.

Il existe deux cas dans le Now Platform qui permettent au client d'envoyer des scripts au serveur pour évaluation :

Filtres et/ou requêtes

Il est légal d'envoyer un filtre au serveur tel que : assigned_to=javascript :getMyGroups()

API système

L’appel d’API AJAXEvaluate permet au client d’exécuter des scripts arbitraires sur le serveur et de recevoir une réponse.

Lorsque vous définissez cette propriété sur **false**, cela Now Platform n’active pas l’utilisation de l’appel d’API AJAXEvaluate à partir du script client.

En savoir plus

Attribut	Description
Nom de la propriété	glide.script.allow.ajaxevaluate
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l’instance	Oui
Objectif	Restreindre l’exécution arbitraire du script client à l’aide de l’API système côté serveur
Valeur recommandée	faux
Impact fonctionnel	(Moyen) Cette correction force la désactivation du processeur AJAEvaluate. Cela peut avoir un impact sur les fonctionnalités si vous utilisez explicitement le processeur d’évaluation AJAX dans le cadre de scripts personnalisés. Pour plus d’informations, consultez GlideAjax .
Risque de sécurité	(Élevé) AJAXEvaluate peut permettre à du code JavaScript arbitraire de s’exécuter sur le navigateur du client en appliquant les objets côté serveur.
Références	Configuration de la propriété de bac à sable de script GlideAjax `glide.script.allow.ajaxevaluate` appartient à la même famille de propriétés qui sécurisent et restreignent l’exécution des scripts provenant du client : • `glide.script.use.sandbox`: voir Bac à sable pour les scripts générés par le client. • `glide.script.secure.ajaxgliderecord`: Reportez-vous à la section Activation de la vérification de l’ACL de AJAXGlideRecord.

Pour en savoir plus sur l’ajout ou la création d’une propriété système, reportez-vous à Add a system property .

Échapper à une formule Excel (renforcement de la sécurité de l’instance)

Utilisez la propriété pour empêcher l’injection Excel, également connue sous le `glide.export.escape_formulas` nom d’injection de formule.

L’injection Excel se produit lorsque des sites Web intègrent des entrées non fiables dans des fichiers Excel. Lorsque vous utilisez un tableur tel que Microsoft Excel ou LibreOffice Call pour ouvrir un fichier, toutes les cellules commençant par +, -, = ou @ sont interprétées comme une formule. Lorsque vous définissez la propriété sur **true**, les

glide.export.escape_formulas valeurs de chaîne commençant par +, -, = ou @ sont précédées d'une apostrophe unique lorsque vous exportez vers des fichiers CSV, XLS ou XLSX.

En savoir plus

Attribut	Description
Nom de la propriété	glide.export.escape_formulas
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour empêcher l'application par rapport à l'injection d'Excel ou de formule.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Des formules malveillantes peuvent être utilisées pour détourner l'ordinateur de l'utilisateur en exploitant les vulnérabilités du tableur.
Risque de sécurité	(Moyen) Les formules malveillantes présentent un risque même lorsque la feuille de calcul d'intégration ne contient pas d'informations sensibles, car elles peuvent être utilisées pour compromettre l'ordinateur de l'utilisateur.
Solution de contournement	Comme alternative, envisagez de supprimer tous les espaces blancs 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 Add a system property .

HTML d'échappement (renforcement de la sécurité de l'instance)

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.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ fournit la fonctionnalité de mise en forme du contenu à l'aide de codes HTML (par exemple, <p>, , <a href>, <b><font><img>,). Un utilisateur malveillant peut injecter du code HTML dans le champ de formulaire pour exécuter des scripts indésirables sur différentes sessions client/utilisateur.

- Définissez cette propriété sur **true** pour effectuer un échappement HTML avant que les enregistrements/champs ne soient restitués dans le navigateur lorsque la table s'affiche en tant que vue de liste.
- S'ils sont définis sur **faux** et que vous sélectionnez cette colonne dans une vue de liste lors de l'affichage d'une liste de tables ou d'enregistrements, ces champs au format HTML peuvent apparaître.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.escape_html_list_field
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour prévenir les attaques de script de site à site contre les applications
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction applique l'encodage HTML à se produire sur l'interface utilisateur au niveau de l'analyseur HTML et renvoie ainsi les résultats codés à l'utilisateur. Elle peut avoir un impact sur les fonctionnalités 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 les sessions des utilisateurs 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 Add a system property .

Échapper à JavaScript (renforcement de la sécurité de l'instance)

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.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ permet à l'utilisateur de mettre en forme le contenu à l'aide de codes HTML (par exemple, <p>, , <a href>, <b><font><img> ,). Si vous définissez la propriété sur *glide.html.escape_script***false**, les balises (<script></script>) peuvent apparaître lorsque vous sélectionnez cette colonne dans une vue de liste tout en consultant une liste de tables ou d'enregistrements.

Un attaquant malveillant peut insérer du code JavaScript en l'intégrant dans les balises (<script></script>). L'attaquant peut en tirer parti en injectant un vecteur JS sophistiqué qui peut s'exécuter lorsqu'un utilisateur ouvre l'enregistrement de table.

En savoir plus

Attribut	Description
Nom de la propriété	glide.html.escape_script
Type de configuration	Propriétés système (/sys_properties_list.do)

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour éviter les attaques de script de site à site contre une application.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction applique l'échappement JavaScript sur l'interface utilisateur et renvoie les résultats codés 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 de l'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 Add a system property .

Échapper à Jelly (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour forcer l'échappement `glide.ui.escape_all_script` de tous les scripts injectés dans Jelly.

Il 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 empêche plusieurs problèmes XSS de se produire.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.escape_all_script
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Si la propriété n'est pas définie sur **true**, 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 le rendu sur les pages Web et l'exécution de l'échappement sur chacune des balises suivantes : `$â {JS :expression}`

Attribut	Description
	$â {HTML :expression} OU $â {JS,HTML :expression}
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction applique l'échappement de Jelly au niveau de l'analyseur. Cela peut avoir un impact fonctionnel sur l'interaction de l'utilisateur avec les données résultantes.
Risque de sécurité	(Élevé) La validation d'entrée doit avoir lieu sur toutes les entrées utilisateur saisies dans l'application. Ce faisant, les attaques par injection contre la plateforme peuvent être défendues et protégées.
Solution de contournement	L'interface utilisateur peut être affectée, car certains des scripts et balises HTML conçus pour le rendu sur une page Web peuvent sembler défectueux. Cette correction envoie la page codée de sortie au navigateur pour qu'il effectue le rendu. Par exemple, au lieu de « ma chaîne ici », il peut afficher « <u>ma chaîne ici</u> » car la <u> balise a été correctement échappée. Dans ce cas, pour éviter les échappements, ajoutez le préfixe NOESC à l'expression Jelly pour empêcher l'échappement JS. Par exemple : • Avant : ($[jvar_context_menus]) ; • Après : ($[NOESC :jvar_context_menus]) ; • Avant : $[jvar_ui_policy_scripts] • Après : $[NOESC :jvar_ui_policy_scripts]
Références	Paramètres de sécurité élevée Balises Jelly

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

XML d'échappement (renforcement de la sécurité de l'instance)

La *glide.ui.escape_text* propriété force l'échappement des valeurs XML au niveau de l'analyseur avant de les transmettre au navigateur du client.

Remarque :
Cette propriété est définie sur **true** par défaut dans Vancouver la version et les 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 client.

Le cross-site scripting se produit lorsqu'un attaquant injecte du code 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, échapper signifie ce qui suit :

- **&** --> &
- **<** --> <
- **>** --> >
- **«** --> »
- **'** --> '
- **/** --> /

Exemple : <![CDATA[<script>alert('Attaque XSS') ;]] >

Échappement : <script>alert('XSS Attack') ; </script>

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.escape_text
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	L'échappement XML empêche les navigateurs d'analyser le code JavaScript malveillant incorporé dans des données non approuvées et de l'exécuter 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. • Le contient du code pour sécuriser les Now Platform cookies, mais pour l'échapper, cette propriété doit être définie sur **true**.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) 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 de l'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 que vous avez défini cette propriété sur **vrai**, le rendu s'arrête sur les balises HTML dans la description de l'élément de catalogue ou dans le texte d'aide de la variable d'élément de catalogue. Il se

Attribut	Description
	peut que vous ne puissiez pas utiliser le formatage HTML pour certains champs. Toutefois, si la *glide.ui.escape_text* propriété est désactivée, toutes les expressions JEXL sont préfixées d'un encodeur de sortie : ${JS :expression} ${HTML :expression} ou ${JS,HTML :expression}
Références	Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Assainisseur HTML (renforcement de la sécurité de l'instance)

Utilisez cette *glide.html.sanitize_all_fields* propriété pour activer l'include de script HTMLSanitizer, qui nettoie l'entrée HTML selon les attributs mis sur liste d'exclusion et d'inclusion configurés dans un script.

Les types de champs disponibles avec le dictionnaire/les champs incluent HTML et HTML traduit. Ces champs d'entrée HTML permettent aux utilisateurs d'écrire une entrée au format HTML, par exemple :

<h1>Test</h1>), à l'aide des 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)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Empêche l'application contre les attaques de script de site à site et d'injection HTML
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) 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

Attribut	Description
	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 grâce à l'encodage de sortie des données.
Solution de contournement	Cette propriété nettoie tous les champs HTML du système. Si vous devez activer l'assainissement HTML sur des champs individuels, voir Activer l'assainissement sur des champs individuels. Vous pouvez également configurer la liste d'inclusion ou la liste d'exclusion pour assainir les balises et attributs 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 Add a system property .

Interpolation Jelly/JS (renforcement de la sécurité de l'instance)

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 de Jelly.

Lorsque vous définissez la propriété sur **true**, une application passe par une arborescence de script Jelly (imbriquée). Il enveloppe les expressions Jelly potentiellement dangereuses avec un filtre qui :

- Échappe à ses 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.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.jelly.js_interpolation.protect
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour atténuer les attaques d'exécution de code malveillant qui peuvent se produire à l'aide de Jelly Injection.
Valeur recommandée	Vrai
Impact fonctionnel	(Élevé) Cette propriété permet de deviner si une expression est entre guillemets. Il peut citer à tort une expression légitime. Dans

Attribut	Description
	ce cas, il peut être nécessaire de marquer manuellement une expression comme sûre.
Risque de sécurité	(Moyen) L'injection JEXL est une forme d'injection d'entrée unique qui Now Platform peut conduire à la fois à la falsification de requête intersite et à l'exécution 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 le préfixe SAFE à l'expression Jelly : `${SAFE :sysparm_input} ;` L'ajout aveugle de SAFE à chaque expression n'est pas la bonne façon d'aborder le problème, car cela peut ouvrir une faille de sécurité. • Ajoutez SAFE à une expression uniquement 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 l'évaluation du JavaScript privilégié.
Références	Balises Jelly Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Sécurité stricte des requêtes SOAP (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour appliquer la *glide.soap.strict_security* sécurité du service 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 module d'extension Contextual Security : Role Management.

Si vous définissez cette propriété sur **true**, elle effectue les actions suivantes :

- Si l'utilisateur dispose du rôle approprié pour effectuer l'opération, il vérifie l'autorisation de rôle de la demande SOAP entrante à valider. Cela se produit lors des appels/requêtes SOAP Web Service effectués sur Now Platform des tables lors de l'exécution des opérations CRÉER, LIRE, METTRE À JOUR ou SUPPRIMER.
- Vérifie les ACL au niveau du système tout en récupérant les 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 la table.

En savoir plus

Attribut	Description
Nom de la propriété	glide.soap.strict_security
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Assurez-vous que les ACL de sécurité sont vérifiées et validées même lorsque les enregistrements sont accessibles via des appels SOAP
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) 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 ayant accès aux données SOAP, consultez Rôles SOAP .
Risque de sécurité	(Élevé) 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	Appliquer une sécurité stricte pour le SOAP entrant SOAP Web Service

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Communications sécurisées (renforcement de la sécurité de l'instance)

Les propriétés de communication sécurisées se rapportent à la sécurité du transport du trafic HTTP.

Certificat de confiance (renforcement de la sécurité de l'instance)

Par défaut, cette *`com.glide.communications.trustmanager_trust_all`* propriété est définie sur **false**. La Now Platform seule approuve les certificats qu'elle peut vérifier par rapport au magasin de certificats JVM. Les certificats autosignés ou signés par l'entreprise ne sont pas approuvés.

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 et assistance client.

En savoir plus

Attribut	Description
Nom de la propriété	com.glide.communications.trustmanager_trust_all
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer la validation de certificat pour les demandes sortantes.
Valeur recommandée	faux
Impact fonctionnel	(Moyen) Cette correction applique une validation stricte sur le champ CA (autorité de certification) de certificat. 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 Vérification du nom d'hôte du client HTTP

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Désactivation de SSLv2/SSLv3 (renforcement de la sécurité de l'instance)

Utilisez cette `glide.outbound.sslv3.disabled` propriété pour forcer le MID Server à utiliser TLS en cas 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)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'utilisation du TLS if lors de toutes les connexions sortantes de l'instance ServiceNow.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) 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.

Attribut	Description
Risque de sécurité	(Moyen) Il a été prouvé que les versions héritées de SSL n'étaient pas sécurisées lorsqu'elles étaient utilisées pour l'implémentation de HTTP Secure Shell, en raison d'attaques côté client, notamment BEAST et SSL.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Vérification du nom d'hôte du client HTTP

Utilisez la pour vérifier le nom d'hôte et la chaîne de `com.glide.communications.httpclient.verify_hostname` certification présentés par les hôtes SSL distants.

Défini sur `com.glide.communications.httpclient.verify_hostname`**true** pour vous protéger contre les attaques de l'homme du milieu (MitM) dans lesquelles les communications entre deux parties sont interceptées. La définition de cette propriété remplace la `com.glide.communications.trustmanager_trust_all` propriété.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.communications.httpclient.verify_hostname`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Désactivez le processus de vérification de certification, qui évalue toutes les certifications de la chaîne de certification en vérifiant l'état de révocation.
Type	vrai | faux
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Permet à un certificat non validé de se connecter en tant qu'hôte non sécurisé.
Risque de sécurité	(Moyen) Permet ou empêche le client HTTP de se connecter à un nom d'hôte potentiellement dangereux sans exception.
Références	Certificats Certificat de confiance

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Vérification du certificat révoqué

Utilisez cette propriété pour désactiver le processus de vérification de certification qui évalue toutes les certifications de la chaîne de certification en vérifiant l'état de révocation.

Les appels d'API qui utilisent le module d'extension de haute sécurité peuvent vouloir configurer cette propriété. Si la chaîne de certification complète n'est pas définie dans le

magasin de confiance de l'instance ou si les certificats utilisés ne sont pas compatibles avec une vérification de révocation OCSP (Online Certificate Status Protocol), des erreurs peuvent être renvoyées aux appels d'API.

La vérification de révocation du certificat peut être désactivée en définissant la propriété `com.glide.communications.httpclient.verify_revoked_certificate` sur **faux**.

Les erreurs associées à une incapacité à effectuer la vérification sont NPE, SSLPeerUnverifiedException, CertPathValidatorException. Ces erreurs peuvent être encapsulées dans une HttpException. Plusieurs facteurs peuvent affecter la capacité à effectuer un contrôle réussi :

- L'URI doit être accessible à l'instance. Notez que l'implémentation OCSP d'origine peut ne pas avoir accès à une connexion proxy.
- Le service OCSP référent doit être en ligne au moment de la vérification.

Remarque :
Les valeurs de ces propriétés sont Remplacement sécurisé et ne peuvent pas être modifiées une fois modifiées (elles ne sont pas réversibles). Si vous avez d'autres questions, contactez Service et assistance client.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.communications.httpclient.verify_revoked_certif`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Désactivez le processus de vérification des certificats, qui évalue tous les certificats de la chaîne de certificats en vérifiant l'état de révocation. Seul un certificat de serveur autosigné doit être chargé dans le magasin de confiance d'instance.
Type	vrai | faux
Valeur par défaut	VRAI
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen)
Risque de sécurité	(Moyen) Les appels d'API utilisant le module d'extension de haute sécurité ne seront pas vérifiés à l'aide d'une vérification de révocation OCSP dans le magasin de confiance d'instance.
Références	Certificats

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Bonnes pratiques de sécurité (renforcement de la sécurité de l'instance)

En plus des configurations de sécurité, un effort manuel supplémentaire est nécessaire pour sécuriser Now Platform davantage les applications au quotidien. Cette section contient

les tâches de sécurité qu'un administrateur doit effectuer périodiquement, dans un certain intervalle de temps.

Options de type de contenu définies automatiquement

L'en-tête HTTP de réponse X-Content-Type-Options est utilisé par le serveur pour indiquer que les types MIME (Multipurpose Internet Mail Extensions) annoncés dans les en-têtes Content-Type doivent être suivis.

La définition de cet en-tête empêchera le navigateur d'interpréter les fichiers comme un autre élément déclaré par le type de contenu dans les en-têtes HTTP. Cet en-tête peut aider à atténuer les attaques de confusion MIME.

Les options de définition automatique du type de contenu seront conformes si `glide.security.header.auto_set_x_content_type_options` la valeur est définie sur **vrai**.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.header.auto_set_x_content_type_options`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Empêche le navigateur d'interpréter les fichiers comme autre chose que ce qui est déclaré par le type de contenu dans les en-têtes HTTP.
Type	vrai | faux
Valeur recommandée	**true**
Impact fonctionnel	(Élevé) Cet en-tête peut aider à atténuer les attaques de confusion MIME.
Risque de sécurité	(Élevé) Si cette propriété n'est pas activée, le navigateur peut mal interpréter le type de contenu dans les en-têtes HTTP.
Références	Types MIME téléchargeables

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

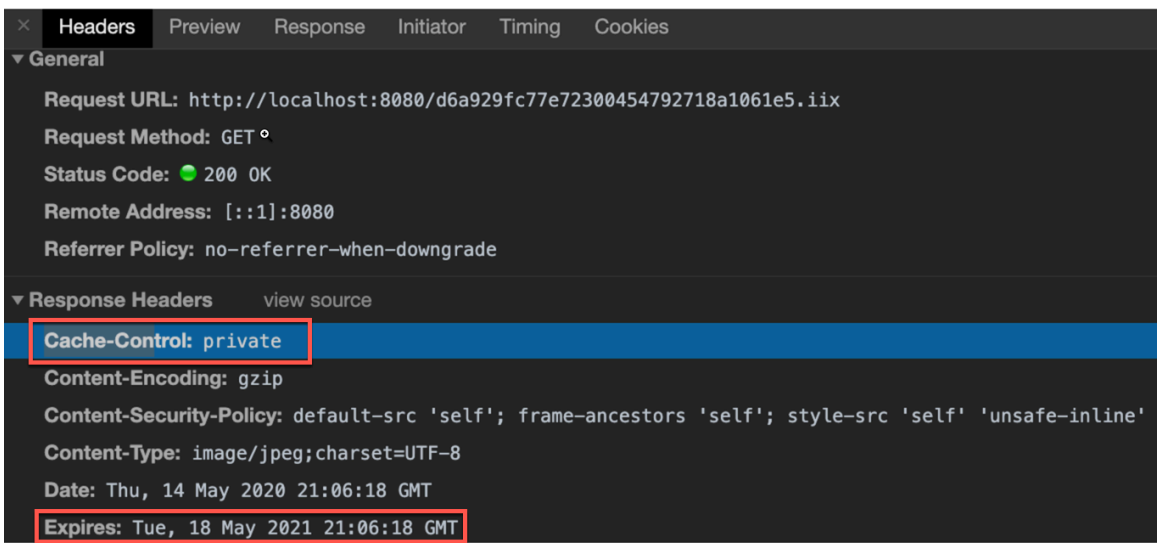
Valeur de l'en-tête HTTP du contrôle de cache (renforcement de la sécurité de l'instance)

Utilisez cette `glide.http.cache_control` propriété pour définir la valeur de contrôle de cache par défaut dans les en-têtes de réponse HTTP qu'envoie lors de Now Platform la demande de données de contenu statique pour une page. Les images, le CSS et le JavaScript rendus de l'intérieur d'une page sont des exemples de contenu statique.

La `glide.http.cache_control` propriété définit la valeur Cache-Control par défaut dans les en-têtes de réponse HTTP sur **privé** ou **public**. La valeur par défaut est **privé**.

Valeur	Description
privé	Le contenu statique peut être mis en cache au niveau du navigateur (client), mais pas au niveau du serveur proxy.
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 `glide.http.cache` propriété désigner s'il faut activer ou désactiver la définition 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 Cache-Control 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)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour configurer la valeur de l'en-tête de réponse HTTP Cache-Control pour le contenu statique.
Valeur recommandée	privé
Impact fonctionnel	(Moyen) Définit la valeur Cache-Control par défaut dans un en-tête de réponse HTTP.

Attribut	Description
Risque de sécurité	(Élevé) Si vous définissez cette propriété sur **public**, les instances avec CDN/proxys peuvent mettre en cache du contenu statique et s'afficher sans authentification. • **privé** est un paramètre plus approprié pour les instances avec la 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 Add a system property .

Appliquer la sécurité aux rapports

Désactivez cette propriété pour empêcher l'utilisateur de publier des rapports ou d'y accéder. Cette propriété désactive la fonctionnalité des rapports publiés dans la génération de rapports.

Activez la publication des rapports en définissant la `glide.report.published_reports.enabled` sur **vrai**.

Appliquer la sécurité sur les rapports est conforme si `glide.report.published_reports.enabled` est défini sur **faux**.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.report.published_reports.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Désactive la fonctionnalité des rapports publiés dans la génération de rapports.
Type	vrai | faux
Valeur recommandée	**false**
Impact fonctionnel	(Moyen) L'utilisateur ne peut pas publier de rapports.
Risque de sécurité	(Moyen) Si cette propriété n'est pas activée, les utilisateurs peuvent être en mesure d'accéder ou de publier des rapports exposant des données sensibles. La publication d'un rapport crée une URL que tout le monde, y compris les personnes qui ne sont pas des utilisateurs, peut utiliser pour y accéder. Lorsque quelqu'un accède à 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 Add a system property .

Module d’extension de haute sécurité (renforcement de la sécurité de l’instance)

Lorsque vous activez le module d’extension High Security, celui-ci 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 permettant un contrôle d’accès strict, la validation d’entrée et l’encodage de sortie.

Ces configurations comprennent :

- Contrôle d'accès
- Règles métier
- Propriétés système
- Action de politique d’interface utilisateur
- Actions des scripts
- Script includes

Exemple

Consultez les exemples pour les propriétés suivantes :

Propriété	Sujet
glide.ui.escape_all_script	Échapper à Jelly
glide.security.strict.actions	Vérifier l’action d’interface utilisateur avant son exécution
glide.security.csrf_previous.autoriser	Jeton anti-CSRF
glide.security.csrf.strict.validation.mode	Validation stricte du CSRF

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.high_security
Type de configuration	Définition du système > Modules d’extension : Développement
Objectif	L’activation de ce module d’extension est obligatoire. Il augmente le niveau de sécurité d’une instance, ce qui réduit la surface d’attaque en atténuant les 10 principales attaques owasp, y compris CSRF, XSS, sécurisation des cookies de session et chargements de fichiers.
Valeur recommandée	Actif
Impact fonctionnel	(Élevé) Ce module d’extension active plusieurs configurations de sécurité 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 des vulnérabilités critiques.
Références	Activation des paramètres de sécurité élevée

Attribut	Description
	Paramètres de sécurité élevée

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à Activate a plugin .

ID de connexion individuels (renforcement de la sécurité de l'instance)

Assurez-vous que tous les utilisateurs ont des ID d'utilisateur individuels, ce qui permet l'audit de toutes les activités utilisateur.

Remarque :
Le marqueur **Actif** des comptes d'utilisateurs locaux qui ne sont pas utilisés doit être défini sur faux.

- Si vous définissez le marqueur **Actif** sur **faux** , le marqueur **Verrouillé** devient **automatiquement vrai**. Si le marqueur **Verrouillé** est défini sur **vrai**, ce compte d'utilisateur ne peut pas s'authentifier auprès de l'instance.
- Définir le marqueur **Actif** sur **faux** ne supprime pas un utilisateur de l' Now Platform, mais supprime la visibilité des comptes non administrateurs.
- Si **le marqueur Actif** est défini sur **faux** et que **le marqueur Verrouillé** est également défini sur **faux**, un utilisateur peut toujours se connecter à ce compte.

Pour en savoir plus sur les comptes d'utilisateurs, consultez Administration des utilisateurs .

Obfuscation de l'interface utilisateur Mobile (renforcement de la sécurité de l'instance)

Utilisez cette `glide.ui.m.blur_ui_when_backgrounded` propriété pour brouiller tous les champs de la capture instantanée lors de l'enregistrement de l'image pendant le processus d'arrière-plan. pour brouiller.

Sur les appareils Android, le système d'exploitation Android effectue 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 effectuer des captures d'écran manuelles de l'application, qui sont stockées publiquement sur l'appareil.

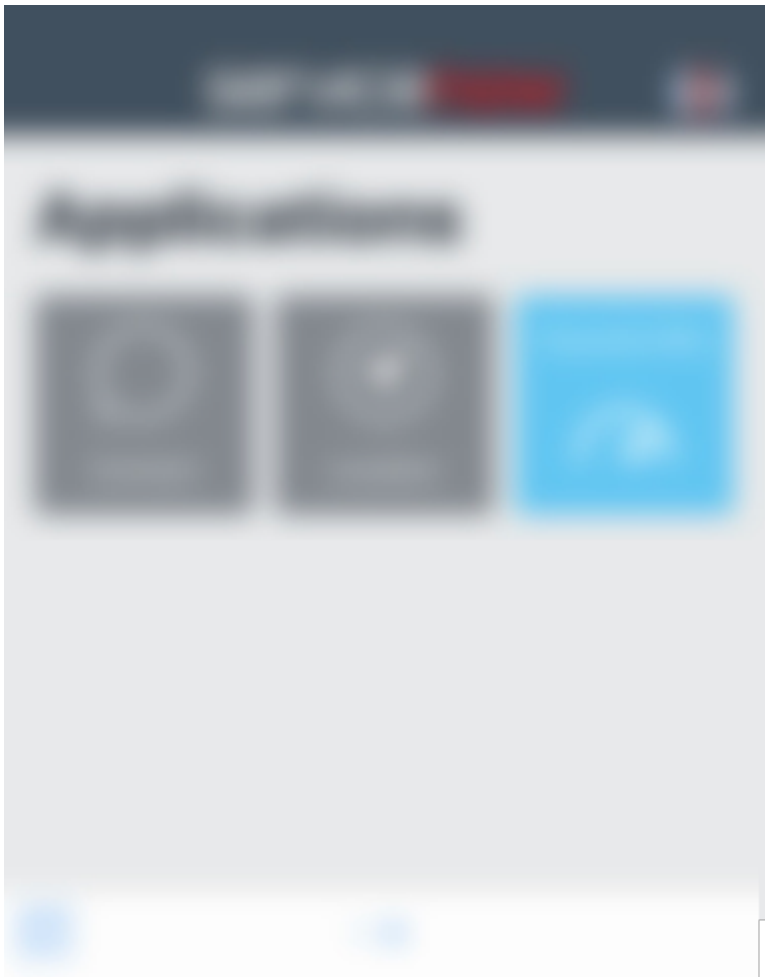
Sur les appareils iOS, le système d'exploitation iOS permet également aux applications d'enregistrer un fichier image. Ce fichier représente le dernier écran vu par l'utilisateur lorsque l'application est envoyée en arrière-plan. Bien que l'objectif soit de fournir une meilleure expérience utilisateur, cela crée également un risque de sécurité, car les images sont enregistrées en tant que fichiers image PNG.

Remarque :
Ce paramètre ou cette configuration est basé sur chaque instance, l'utilisateur doit donc se connecter à l'instance avec la propriété configurée.

Pour brouiller tous les champs de l'instantané dans l'application ServiceNow Classic, consultez Configurer l'option de floutage de l'application pour améliorer la sécurité .

Exemple

Lorsque vous définissez cette propriété sur **vrai**. L'application en arrière-plan est brouillée pour les appareils iOS et noircie pour les appareils iOS Android.



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)
Configurable dans le centre de sécurité de l’instance	Non
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
Impact fonctionnel	(Faible) Si la *`glide.ui.m.blur_ui_when_backgrounded`* propriété est définie sur **vrai**, les applications natives utilisent le paramètre défini sur le serveur pour flouter l’écran lorsque l’application passe en arrière-plan.

Attribut	Description
	• Il floute 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 serait 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 un 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 Add a system property .

Correctifs et mises à jour (renforcement de la sécurité de l'instance)

Assurez-vous que l'instance exécute le niveau de correctif le plus récent. Des correctifs de sécurité sont régulièrement publiés pour la plupart des correctifs et correctifs d'urgence qui accompagnent les Now Platform mises à jour des fonctionnalités du produit. La mise à niveau lorsque de nouveaux correctifs et correctifs logiciels sont disponibles réduit le risque de vulnérabilités potentielles.

Il Now Platform subit en moyenne deux tests d'intrusion par semaine.

- Bien que la plupart de ces tests n'aboutissent pas à des vulnérabilités significatives, des vulnérabilités sont détectées et corrigées régulièrement.
- Vous trouverez des informations sur Now Platform les versions, les correctifs et les correctifs d'urgence dans la section Notes de version de la documentation du produit. Pour plus d'informations, consultez les notes de version des mises à niveau .

Supprimer les données de démonstration (renforcement de la sécurité de l'instance)

Les données de démonstration, en particulier les comptes de démonstration, sont généralement incluses lors de la création d'une instance. Si tel est le cas, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production.

Ouvrez une demande dans HI. Assurez-vous de créer un compte administratif avant de soumettre la demande.

Il est fortement recommandé de vérifier la suppression des données de démonstration en production sur une instance de sous-production qui est un clone récent de l'instance de production.

Ressources internes

https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107

https://community.servicenow.com/community?id=community_blog&sys_id=786eaeaddbd0dbc01dcaf3231f961959

Suppression des données de démonstration à l'aide de Catalogue de services

Au lieu de soumettre la demande en tant qu'incident, certains utilisateurs peuvent demander la suppression des données de démonstration sur une instance à l'aide de

Service Catalog. Ces utilisateurs comprennent les utilisateurs internes et les utilisateurs qui ont les rôles customer_admin ou partner_admin.

1. Accédez à https://support.servicenow.com/now .
2. Spécifiez l'instance à partir de laquelle supprimer les données de démonstration.

   Si vous ne parvenez pas à trouver votre instance, ajoutez * au nom de l'instance pour lancer une requête contient.
3. Cliquer sur **Libre-service** > **Supprimer les données de démonstration** > **.**
4. Spécifiez la date et l'heure de suppression des données de démonstration de l'instance sélectionnée.

   La date et l'heure doivent être postérieures d'au moins quatre heures à l'heure actuelle.
5. Cliquez sur **Envoyer**.

Une nouvelle demande de changement est créée et apparaît automatiquement. La **date de fin planifiée** est automatiquement calculée en fonction de la **date de début planifiée** augmentée de cinq heures, ce qui correspond à la durée du processus. Dans la demande de changement. Utilisez la liste de surveillance pour ajouter tous les autres membres de votre équipe qui doivent être au courant de l'état de la demande de changement.

Liste d'inclusion de la sécurité (renforcement de la sécurité de l'instance)

Un modèle de sécurité « positif » (également connu sous le nom de « liste d'inclusion ») est un modèle qui définit ce qui est autorisé et rejette tout le reste. Cette section contient des contrôles de sécurité qu'un administrateur peut configurer pour restreindre le comportement aux listes d'inclusion connues.

Remarque :
Les propriétés de la liste d'inclusion de sécurité doivent être configurées manuellement dans chaque instance, car les ensembles de mises à jour ne favoriseront pas la configuration et renverront une erreur.

Vérifier les appels des membres de la liste d'autorisation (renforcement de la sécurité de l'instance)

Examinez et supprimez les entrées d'appel des membres de la liste d'inclusion si besoin à partir de la table sys_whitelist_member.

Les entrées d'appel de membres ont accès aux ressources Java du côté serveur afin de réaliser des opérations basées sur les applications sans la validation appropriée. Étant donné qu'il peut entraîner la divulgation ou l'altération non autorisée des données des clients, il s'agit d'un grave problème de sécurité.

En savoir plus

Attribut	Description
Nom de la table	sys_whitelist_member **Remarque :** Dans les versions récentes, seuls les employés ServiceNow peuvent accéder à cette table. Même les administrateurs ne sont pas en mesure de le faire.

Attribut	Description
Type de configuration	Table
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour examiner et supprimer des entrées de cette table.
Valeur recommandée	Aucun enregistrement ne doit exister dans la table (la liste doit être vide).
Impact fonctionnel	(Faible) Il ne devrait y avoir aucun impact tant que vous examinez et approuvez les résultats générés lors de l'exécution de l'outil de suppression des appels de packages. 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. Pour en savoir plus, reportez-vous à la section Outil de suppression des appels de packages.
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 ces éléments pour l'autorisation et la restriction de l'accès aux objets sensibles.

Étapes de configuration

Remarque :
Les étapes suivantes sont similaires aux étapes décrites dans les sections Étapes de configuration dans :

- Outil de suppression d'appel de packages
- Vérifier les appels de package sur la liste d'autorisation

Si vous les avez déjà terminées, vous pouvez ignorer ces étapes.

1. Activez le module d'extension Packages Call Removal Tool. Pour en savoir plus, reportez-vous à la section Outil de suppression des appels de packages.
2. À l'aide du navigateur de filtre, accédez à **l'utilitaire de suppression des appels de packages**.
3. Cliquez sur chaque script en commençant par (1) à (4). Attendez la sortie, puis passez à la suivante.
4. Une fois que vous avez exécuté le script (4), une liste des champs concernés s'affiche sur la page Éléments d'appels de packages.
5. Résolvez tous les éléments des sections Proposé et Erreur.

Remarque :
Cet outil peut signaler certains appels de packages utilisés dans `sa_mapping_ext_commands` et `sa_custom_operation`. Ces appels de package appartiennent au MID Server. Comme il n'existe aucune classe, le code s'exécute dans MID Server. Si vous trouvez les appels de membre suivants dans la section Erreurs, marquez-les comme **Rejeté** (Ignoré). L'outil ne signale plus cet appel de membre.

- `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`

6. Contactez ServiceNow l'assistance pour d'autres corrections.

Vérifier les appels de package sur la liste d'autorisation (renforcement de la sécurité de l'instance)

Examinez et supprimez les entrées d'appels de package sur liste d'inclusion si besoin à partir de la table sys_whitelist_package.

Les entrées d'appel en paquet ont accès aux ressources Java du côté serveur afin de réaliser des opérations basées sur les applications sans la validation appropriée. Étant donné qu'il peut entraîner la divulgation ou l'altération non autorisée des données des clients, il s'agit d'un grave problème de sécurité.

En savoir plus

Attribut	Description
Nom de la table	sys_whitelist_package **Remarque :** Dans les versions récentes, seul Service et assistance client l'accès à cette table ; même les administrateurs ne sont pas en mesure de le faire.
Type de configuration	Table
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour examiner et supprimer des entrées de cette table.
Valeur recommandée	Aucun enregistrement ne doit exister dans la table (la liste doit être vide).
Impact fonctionnel	(Faible) Il ne devrait y avoir aucun impact tant que les résultats de l'exécution de l'outil de suppression des appels de packages 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. Pour en savoir plus, consultez Outil de suppression d'appel de packages.

Attribut	Description
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 ces éléments pour l'autorisation et la restriction de l'accès aux objets sensibles.
Solution de contournement	Contactez ServiceNow l'assistance pour obtenir de l'aide.

Étapes de configuration

1. Activez le module d'extension Packages Call Removal Tool. Pour en savoir plus, reportez-vous à la section Outil de suppression des appels de packages.
2. À l'aide du navigateur de filtre, accédez à **l'utilitaire de suppression des appels de packages**.
3. Cliquez sur chaque script en commençant par (1) à (4). Attendez la sortie, puis passez à la suivante.
4. Une fois que vous avez exécuté le script (4), une liste des champs concernés s'affiche sur la page Éléments d'appels de packages.
5. Résolvez tous les éléments des sections Proposé et Erreur.

   Remarque :
   Cet outil peut signaler certains appels de packages utilisés dans `sa_mapping_ext_commands` et `sa_custom_operation`. Ces appels de package appartiennent au MID Server. Comme il n'existe aucune classe, le code s'exécute dans MID Server. Si vous trouvez les appels de packages suivants dans la section Erreurs, marquez-les 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`

6. Contactez ServiceNow l'assistance pour d'autres corrections.

Activer la liste d'autorisation d'URL pour la communication cross-origin entre iframes (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour activer la *`glide.ui.concourse.onmessage_enforce_same_origin`* communication cross-origin entre iframes.

OpenFrame ne peut traiter que les messages provenant des domaines de confiance spécifiés dans la *`glide.ui.concourse.onmessage_enforce_same_origin_whitelist`* propriété. Pour en savoir plus, consultez Spécifier la liste d'autorisation UTL pour la communication cross-origin 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)

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour activer l'inclusion de domaines de confiance, afin qu'ils puissent communiquer entre iframes pour OpenFrame.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Si vous n'incluez pas les domaines prévus, la possibilité d'intégrer d'autres pages dans Now Platform les instances peut être limitée.
Risque de sécurité	(Élevé) Si une page Web contient des gestionnaires d'événements qui n'effectuent pas une validation d'origine appropriée, une page Web, ou un script, quelle que soit son origine, peut communiquer avec elle. Il peut également lancer n'importe quelle 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 Add a system property .

Renforcer les liens relatifs (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour appliquer des *glide.cms.catalog_uri_relative* liens relatifs à partir du paramètre URI sur /ess/catalog.do.

- Lorsqu'elle est définie sur **vrai**, seules les URL relatives sont autorisées via la page /ess/catalog.do à l'aide du *uri* paramètre.
- Lorsqu'elle est définie sur **faux**, toutes les URL sont autorisées, ce qui peut permettre la liaison à du contenu externe non autorisé.

En savoir plus

Attribut	Description
Nom de la propriété	glide.cms.catalog_uri_relative
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour limiter les tentatives de lier du contenu externe non autorisé.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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 Add a system property .

Outil de suppression d'appel de packages (renforcement de la sécurité de l'instance)

Activez et exécutez le module d'extension Packages Call Removal Tool (`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 plugin qui :

- Analyse les scripts à la recherche d'appels de packages aux Now Platform classes Java.
- Propose des changements pour les remplacer par des 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. Il est possible que ce script ne prenne pas en charge d'autres mises à jour à l'avenir. Dans les versions ultérieures, les tables sys_whtelist_xxx sont censées être vides. Cependant, il peut toujours être utile d'utiliser cet outil car il signale les appels Packages,xxx.

L'outil de suppression d'appels de packages peut signaler certains appels de packages utilisés dans sa_mapping_ext_commands et sa_custom_operation. Ces appels de package appartiennent au MID Server. Comme il n'y a pas de classes, le code s'exécute dans MID Server. Si vous trouvez l'un des appels de package répertoriés suivants dans la section Erreurs, marquez-les 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`

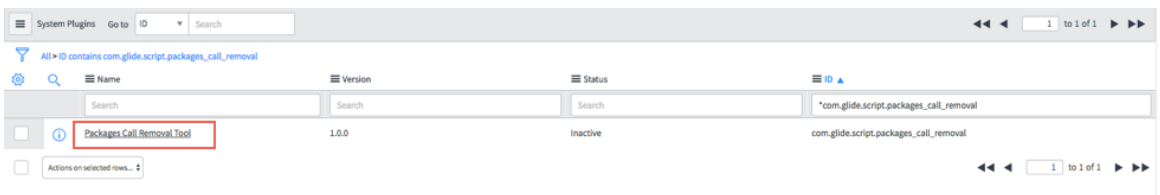
En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.script.packages_call_removal
Type de configuration	Définition du système > Modules d'extension
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour supprimer/remplacer les appels de packages/membres non autorisés par des noms Glide acceptables (GlideScriptable) qui n'autorisent qu'un accès autorisé aux données.
Valeur recommandée	Actif
Impact fonctionnel	(Faible) 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 alors décider d'accepter ou de rejeter le changement proposé.

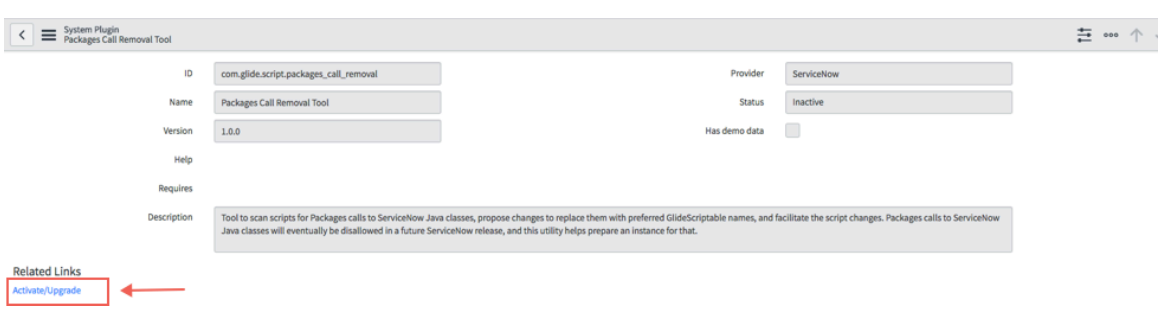
Attribut	Description
Risque de sécurité	(Moyen) Les appels d'API côté client qui entraînent la récupération de données ou l'accès à des objets sur le serveur sont considérés comme dangereux du point de vue de la sécurité. Ils doivent être validés pour l'autorisation et la restriction de l'accès aux objets sensibles.

Étapes de configuration

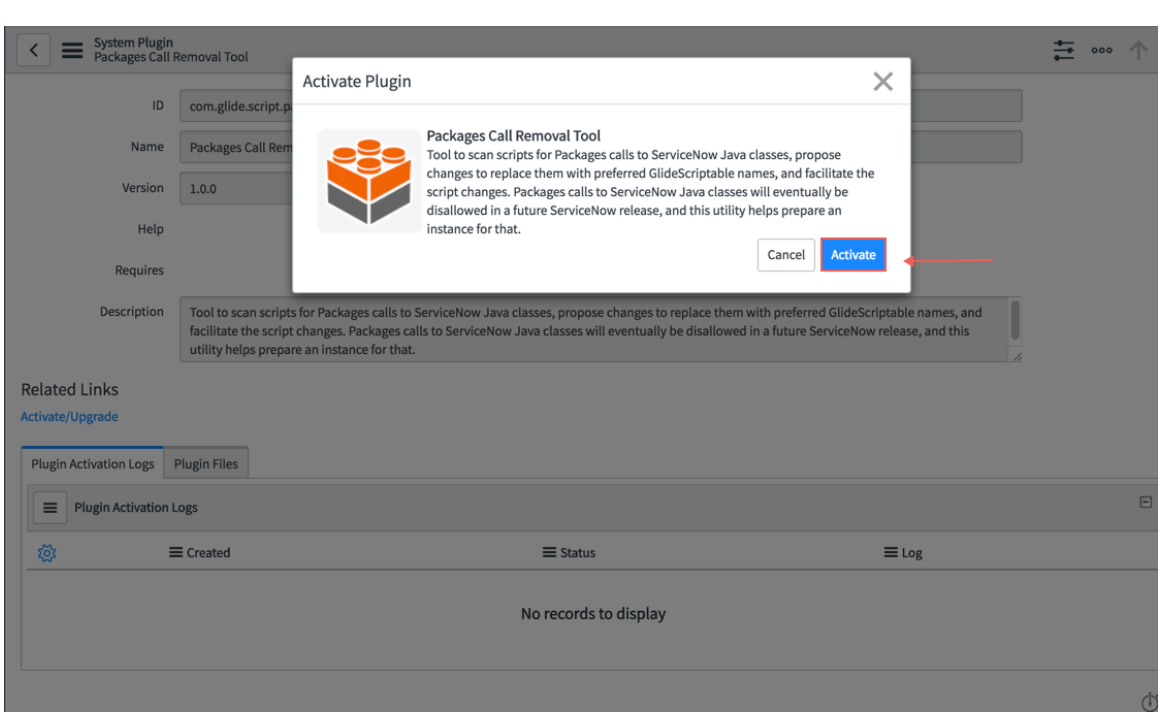
1. Accédez à la **Définition du système** > **Modules d'extension**



2. Recherchez 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.



4. Pour vérifier les appels de package sur liste d'inclusion et les appels de membres sur liste d'inclusion, effectuez les actions décrites dans les sections Étapes de configuration des rubriques suivantes :

Traduction automatique

- Vérifier les appels des membres de la liste d'autorisation
- Vérifier les appels de package sur la liste d'autorisation

Spécifier la liste d'autorisation d'URL pour la communication iframe interorigine (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour activer la `glide.ui.concourse.onmessage_enforce_same_origin_whitelist` communication cross-origin entre les iframes à partir des domaines de confiance que vous spécifiez dans une liste d'inclusion.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.concourse.onmessage_enforce_same_origin_whitelist
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Pour activer la liste d'inclusion des domaines de confiance, afin qu'ils puissent communiquer entre iframes pour OpenFrame.
Besoin	Obligatoire
Impact fonctionnel	(Moyen) Si vous n'incluez pas les domaines prévus, la possibilité d'intégrer d'autres pages dans les Now Platform instances peut être limitée.
Risque de sécurité	(Élevé) Si une page Web contient des gestionnaires d'événements qui n'effectuent pas une validation d'origine appropriée, une page Web, ou un script, quelle que soit son origine, peut communiquer avec elle. Il peut également lancer n'importe quelle fonctionnalité exécutée par le gestionnaire d'événements. La communication avec des iframes d'autres domaines constitue un risque pour la sécurité.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Liste d'URL autorisées pour les redirections de déconnexion (renforcement de la sécurité de l'instance)

Utilisez cette `glide.security.url.whitelist` propriété pour ajouter une validation supplémentaire afin de garantir que toute URL externe introduite doit faire partie des URL sur liste d'inclusion.

La redirection ouverte se produit lorsqu'une page Web vulnérable est redirigée vers une page non fiable et malveillante susceptible de compromettre l'utilisateur. Les attaques de redirection ouverte s'accompagnent d'une attaque de phishing, car le lien vulnérable modifié est identique au site d'origine, ce qui augmente les chances de succès de l'attaque de phishing.

Cette propriété est applicable dans les cas suivants :

- /logout.do ?sysparm_goto_url={URL externe}
- /cms_login_redirect.do ?sysparm_goto_url={URL externe}

Les utilisateurs sont dirigés vers un site de confiance externe après s'être déconnectés de l'instance :

- /logout_redirect.do ?sysparm_url={URL externe}
- /saml_redirector.do ?sysparm_uri={URL externe}

Lorsque SAML est activé, il appelle une URL de déconnexion du fournisseur d'identité (IDP).

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.url.whitelist
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour implémenter la redirection d'URL sécurisée lors de la connexion, de la déconnexion ou d'autres redirections. Cette propriété atténue l'une des 10 principales attaques OWASP appelées Redirections et transferts invalidés.
Type	Chaîne séparée par des virgules et des espaces. Exemple : https://example.com, https://wiki.example.com.
Valeur	URL approuvées de votre organisation [certains FQDN (nom de domaine complet) définis, par ex. http://www.servicenow.com]
Impact fonctionnel	(Moyen) 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 pour la sécurité.
Références	Erreurs et correctifs de Multi-SSO (SAML 2.0)

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Politique de sécurité du contenu client incorporé de Virtual Agent (renforcement de la sécurité de l'instance)

Utilisez cette *com.glide.cs.embed.csp_frame_ancestors* propriété pour activer la configuration de la politique frame-ancestors uniquement pour la page https://<votre-instance>.service-now.com/sn_va_web_client_app_embed.do .

Le module d'extension Virtual Agent permet d'incorporer un client dans une page Web externe. Pour permettre l'intégration de la page client dans la page Web, la politique de sécurité du contenu doit autoriser la page externe en tant qu'image parente.

Remarque :
Évitez d'utiliser uniquement « * » comme politique de sécurité du contenu, car cela activerait tous les domaines et rendrait l'application potentiellement vulnérable au détournement de clic.

En savoir plus

Attribut	Description
Nom de la propriété	com.glide.cs.embed.csp_frame_ancestors
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Pour activer la création d'une politique de sécurité du contenu personnalisée pour la page Agent virtuel pouvant être incorporée.
Valeur recommandée	Définir sur les domaines approuvés
Impact fonctionnel	(Élevé) Le client intégrable d'Agent virtuel ne s'autorise pas à être incorporé dans des sites externes à moins que la politique de sécurité du contenu ne soit configurée correctement.
Risque de sécurité	(Moyen) Si elle n'est pas configurée correctement (en autorisant tous les cadres parents), elle peut rendre la page client intégrable vulnérable au détournement de clic.
Références	Incorporer le client Web de l'Agent virtuel dans une page Web externe Pour en savoir plus sur la création d'une politique de sécurité du contenu frame-ancestors, cliquez ici.

Étapes de configuration

1. Accédez à la **/sys_properties_list.do**.
2. Recherchez la propriété *com.glide.cs.embed.csp_frame_ancestors*.
3. Attribuez une politique de sécurité de contenu acceptable (n'autorisez que l'entreprise ou d'autres domaines acceptés), puis cliquez sur **Mettre à jour**.

X-Frame-Options du client incorporé de Virtual Agent (renforcement de la sécurité de l'instance)

Utilisez cette *com.glide.cs.embed.xframe_options* propriété pour activer la configuration de l'en-tête X-Frame uniquement pour la page https://<votre-instance>.service-now.com/sn_va_web_client_app_embed.do .

Le module d'extension Virtual Agent permet d'incorporer un client dans une page Web externe. Pour permettre l'intégration de la page client dans la page Web, l'en-tête X-Frame-Options doit permettre d'inclure l'iframe dans le cadre parent.

Remarque :
Évitez d'utiliser allow-from * comme valeur d'en-tête X-Frame-Options, car cela activerait tous les domaines et rendrait l'application potentiellement vulnérable au détournement de clic.

En savoir plus

Attribut	Description
Nom de la propriété	com.glide.cs.embed.xframe_options
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Pour activer la spécification de la directive pour l'en-tête X-Frame-Options pour la page Agent virtuel intégrable.
Valeur recommandée	Origine identique
Impact fonctionnel	(Élevé) Le client incorporable d'Agent virtuel ne peut pas être incorporé dans des sites externes à moins que l'en-tête X-Frame-Options ne soit configuré correctement.
Risque de sécurité	(Moyen) Si elle n'est pas configurée correctement (en autorisant tous les cadres parents), elle peut rendre la page client intégrable vulnérable au détournement de clic.
Références	Incorporer le client Web de l'Agent virtuel dans une page Web externe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

X-Frame-Options : SAMEORIGIN (renforcement de la sécurité de l'instance)

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.

Utilisez l'en-tête de réponse HTTP X-Frame-Options pour indiquer si le navigateur doit être autorisé à rendre une page dans un <frame> ou <iframe>. Les sites peuvent utiliser cette fonction pour éviter les attaques de détournement de clic en s'assurant que leur contenu n'est pas intégré dans 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 uniquement 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)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour atténuer les attaques de ClickJacking.
Valeur recommandée	VRAI

Attribut	Description
Impact fonctionnel	(Faible) Cette correction applique la restriction pour le rendu d'une Now 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 politique 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 stratégie de même origine qui permet d'accéder aux ressources/scripts à partir d'un autre domaine lorsqu'il est explicitement indiqué dans le cadre d'une valeur d'en-tête. • Dans ce cas, l'en-tête **X-Frame-Options** contrôle si l'application Now Platform peut être rendue sur le site Web tiers. • Cela réduit l'exposition sensible, car la valeur de propriété, lorsqu'elle est définie sur **SAMEORIGIN** , n'active pas le rendu.
Références	Propriétés système disponibles Configurer les iFrames

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Validation du traitement d'entité externe XML

Ces propriétés permettent l'expansion de l'entité et restreignent toute entité externe (par exemple, l'URL) lorsqu'elles sont incluses dans le cadre de la référence DOCTYPE XML. DTD est essentiellement un schéma XML. Si vous recherchez une solution pour les déclarations d'entité qui pourraient avoir un potentiel pour XXE (entité externe), activez une défense avec liste d'inclusion contre XXE à l'aide des propriétés système.

Pour l'analyse XMLDocument et XMLUtil

Si vos personnalisations utilisent `XMLDocument` ou `XMLUtil`, définissez les propriétés système suivantes. Ils contrôlent l'expansion des entités et permettent la validation des entités externes, qui permettent le traitement uniquement de celles figurant sur les listes d'inclusion.

Définition du seuil d'expansion de l'entité (renforcement de la sécurité de l'instance)

Utilisez cette *`glide.xmlutil.max_entity_expansion`* propriété pour réduire la limite maximale d'expansion de l'entité.

Le Now Platform ne traite pas les expansions d'entité ultérieures supérieures à la limite autorisée spécifiée dans cette propriété.

Remarque :
3000 est le minimum par défaut imposé par le Now Platform, qui est considéré comme un seuil de sécurité. Par conséquent, la plateforme considère cette valeur minimale par défaut si la valeur entière que vous saisissez est inférieure à 3 000.

En savoir plus

Attribut	Description
Nom de la propriété	glide.xmlutil.max_expansion_entité
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre les attaques XML Entity Expansion/Billion Laugh.
Valeur recommandée	3000
Impact fonctionnel	(Faible) Si la personnalisation utilise l'extension d'entités volumineuses, le peut bloquer le Now Platform traitement ultérieur.
Risque de sécurité	(Élevé) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources du système.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Validation d'entité XMLdoc/XMLUtil avec liste d'autorisation (renforcement de la sécurité de l'instance)

Utilisez la `glide.xml.entity.whitelist.enabled` propriété pour activer la validation des entités externes et n'autorise que le traitement des entités sur liste d'inclusion.

- Si vous définissez cette propriété sur **vrai**, elle autorise uniquement le traitement des entités sur liste d'inclusion (paramètre recommandé).
- Si vous définissez cette propriété sur **false**, elle autorise le traitement de toutes les entités externes.

Prérequis

Avant de définir cette propriété, définissez une liste de noms de domaine complets délimités par des virgules dans la `glide.xml.entity.whitelist` propriété, qui sont les seules URL atteignables à l'aide du processus XML Entity. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.xml.entity.whitelist.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Ce contrôle de correction doit être activé pour assurer la défense contre les attaques XXE.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Si la personnalisation utilise une entité externe, non répertoriée comme inclusion dans la propriété, le traitement ultérieur peut bloquer le `glide.xml.entity.whitelist`Now Platform traitement ultérieur. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.
Risque de sécurité	(Élevé) 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.
Solution de contournement	Si vous n'utilisez pas l'extension d'entité externe, désactivez-la. Pour en savoir plus, reportez-vous à la rubrique Désactiver l'expansion des entités.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Pour les analyseurs XMLDocument2

Si vos personnalisations utilisent un analyseur XMLDocument2, utilisez les propriétés système suivantes pour activer la validation d'entité externe.

Désactiver l'expansion de l'entité (renforcement de la sécurité de l'instance)

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 XML termine l'analyse, mais n'inclut aucune entité interne ou externe.

- Si vous définissez cette propriété sur **vrai**, toutes les entités externes tentent de résoudre ou de développer les entités sujets, sous réserve de la définition de la `glide.stax.whitelist_enabled` propriété.
- Si vous définissez cette propriété sur **faux**, toute la résolution et l'expansion de l'entité sont bloquées. Pour en savoir plus, consultez Validation d'entité XMLdoc2 avec liste d'autorisation.

Prérequis

Avant de définir cette propriété :

- Définissez les `glide.xml.entity.whitelist.enabled` propriétés and `glide.stax.whitelist_enabled` sur true. Pour en savoir plus, consultez Validation d'entité XMLdoc/XMLUtil avec liste d'autorisation et Validation d'entité XMLdoc2 avec liste d'autorisation.
- Définissez une liste de noms de domaine complets délimités par des virgules dans la `glide.xml.entity.whitelist` propriété, qui sont les seules URL atteignables à l'aide du processus XML Entity. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.

En savoir plus

Attribut	Description
Nom de la propriété	glide.stax.allow_entity_resolution
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre une attaque d'expansion d'entité XML/d'un milliard de rires.
Valeur recommandée	faux
Impact fonctionnel	(Faible) Si la personnalisation utilise l'expansion de l'entité, la peut bloquer le Now Platform traitement ultérieur.
Risque de sécurité	(Élevé) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources du système.
Solution de contournement	Si la personnalisation nécessite une expansion de l'entité, définissez cette propriété sur true et suivez les étapes documentées à la section Validation d'entité XMLdoc2 avec liste d'autorisation.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Pour plus d'informations sur les ressources OWASp, consultez OWASp .

Validation d'entité XMLdoc2 avec liste d'autorisation (renforcement de la sécurité de l'instance)

Utilisez une propriété pour activer le traitement, à l'aide de XMLDocument2, des entités externes apparaissant dans une liste d'inclusion.

Prérequis

Avant de définir cette propriété :

- Définissez la propriété `glide.xml.entity.whitelist.enabled` sur true. Pour en savoir plus, consultez Validation d'entité XMLdoc/XMLUtil avec liste d'autorisation.
- Définissez une liste de noms de domaine complets délimités par des virgules dans la `glide.xml.entity.whitelist` propriété, qui sont les seules URL atteignables à l'aide du processus XML Entity. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.

En savoir plus

Attribut	Description
Nom de la propriété	glide.stax.whitelist_enabled
Type de configuration	Propriétés système (/sys_properties_list.do)

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre les attaques d'entité externe XML.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Si la personnalisation utilise une entité externe qui n'est pas sur liste d'inclusion, le traitement ultérieur peut bloquer le Now Platform traitement. Pour en savoir plus, consultez Traitement d'entité externe XML - Liste d'autorisation.
Risque de sécurité	(Élevé) Un attaquant peut utiliser la DTD peut inclure des requêtes HTTP arbitraires que le serveur peut exécuter. En utilisant la relation de confiance du serveur avec d'autres entités, cela pourrait conduire à d'autres attaques.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Traitement d'entité externe XML : liste d'autorisation (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour activer l'accès `glide.xml.entity.whitelist` à une liste de noms de domaine complets délimités par des virgules, si nécessaire. Ces URL sont les seules qui peuvent être atteintes à l'aide du traitement XML Entity.

Prérequis

Avant de définir cette propriété, définissez la `glide.xml.entity.whitelist.enabled` propriété qui active la validation d'une entité externe et autorise uniquement le traitement de la liste d'inclusion que vous spécifiez dans la `glide.xml.entity.whitelist` propriété. Pour en savoir plus, consultez Validation d'entités XMLdoc/XMLUtil avec mise sur liste blanche.

En savoir plus

Attribut	Description
Nom de la propriété	glide.xml.entité.liste blanche
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour créer une liste d'inclusion des URL auxquelles le traitement d'entité XML peut accéder.
Valeur recommandée	Spécifié par l'utilisateur (par exemple, https://google.com)
Impact fonctionnel	(Faible) Le traitement de l'entité externe peut être bloqué si elle n'est pas mentionnée dans la liste d'inclusion. Lorsque la liste d'inclusion est activée, elle nécessite le formulaire PUBLIC d'une définition d'entité externe.
Risque de sécurité	(Élevé) Un attaquant peut utiliser la DTD peut inclure des requêtes HTTP arbitraires que le serveur peut exécuter. Cela

Attribut	Description
	pourrait conduire à d'autres attaques utilisant la relation de confiance du serveur avec d'autres entités

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Gestion des sessions (renforcement de la sécurité de l'instance)

La gestion des sessions permet d'identifier correctement le trafic qui appartient à un utilisateur spécifique. Prenez des précautions pour vous assurer qu'il n'y a pas d'abus de la relation de confiance.

Les applications Web peuvent créer des sessions pour suivre les utilisateurs anonymes après la première demande de l'utilisateur. Par exemple, le maintien de la préférence de langue de l'utilisateur, en veillant à ce que :

- Identification de l'utilisateur sur toutes les demandes ultérieures.
- Application de contrôles d'accès de sécurité.
- Autorisation d'accès aux données privées de l'utilisateur.
- Augmentation de l'ergonomie de l'application.

Par conséquent, les applications Web actuelles peuvent fournir des options de session avant et après l'authentification.

Authentification et gestion des sessions

L'authentification est le processus qui consiste à vérifier qu'une personne, une entité ou un site Web est bien celui qu'elle prétend être.

L'authentification tente de vérifier l'identité numérique de l'expéditeur d'une communication. Tester le schéma d'authentification implique de comprendre le fonctionnement du processus d'authentification et d'utiliser ces informations pour contourner le mécanisme d'authentification. Un exemple courant est le processus de connexion. L'authentification a lieu après l'envoi d'un nom d'utilisateur, d'un ID d'utilisateur et d'une ou plusieurs informations privées que seul l'utilisateur connaît.

La gestion des sessions inclut des propriétés liées à la sécurité qu'un administrateur peut configurer pour garantir que des mécanismes de gestion des sessions sécurisées sont établis dans le Now Platform.

Délai absolu de session (renforcement de la sécurité de l'instance)

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 forcés de s'authentifier à nouveau dans l'instance.

Il permet au cookie utilisateur d'être valide pendant la durée de jours spécifiés, à compter de la date à laquelle le cookie a été émis pour la première fois. La valeur par défaut est de 30 jours et la limite maximale est de 365 jours.

Remarque :
Pour imposer une durée de session maximale pour toutes les sessions utilisateur actives, reportez-vous à la section Configure a maximum active time for 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)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour forcer les utilisateurs qui ont coché la case **Se souvenir de moi** à s'authentifier à nouveau après des jours spécifiques.
Impact fonctionnel	(Moyen) Cette propriété applique la reconnexion obligatoire en évitant toute sorte de rotation des cookies après une période donnée.
Risque de sécurité	(Moyen) Le fait que les cookies utilisateur soient actifs pour une durée indéterminée constitue un risque pour la sécurité et doit expirer selon une configuration basée sur le temps.
Références	Propriétés système disponibles Modifier les paramètres de la case à cocher Mémoriser mon nom et du cookie

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Jeton anti-CSRF (renforcement de la sécurité de l'instance)

Utilisez cette `glide.security.use_csrf_token` propriété pour garantir l'utilisation d'un jeton de sécurité pour identifier et valide les demandes entrantes, qui sont ensuite utilisées pour prévenir ces attaques.

Le Cross-Site Request Forgery (CSRF) est une attaque qui oblige un utilisateur final à exécuter des actions indésirables sur une application Web dans laquelle il est actuellement authentifié. Les attaques CSRF ciblent spécifiquement les demandes de changement d'état, et non le vol de données, car l'attaquant n'a aucun moyen de voir la réponse à la requête falsifiée.

Les propriétés suivantes peuvent être activées pour des contrôles supplémentaires sur le jeton CSRF :

- `glide.security.csrf_previous.time_limit`
- `glide.security.csrf_previous.allow`
- `glide.security.csrf.strict.validation.mode`

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.use_csrf_token
Type de configuration	Propriétés système (/sys_properties_list.do)

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour protéger l'application contre une attaque CSRF potentielle.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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 falsification des requêtes intersites constitue un risque de sécurité important qui compromet l'intégrité des données de l'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 requête 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 Add a system property .

Changer les informations d'identification par défaut (renforcement de la sécurité de l'instance)

Utilisez la case à cocher **Mot de passe à réinitialiser** dans Utilisateurs et groupes pour vous assurer qu'un utilisateur illégitime ne peut pas tirer parti des données par défaut.

Cela Now Platform inclut certaines données par défaut lorsque l'instance est zbooted, ou lorsque vous mettez en service une nouvelle instance. Il peut contenir les comptes d'utilisateur de démonstration tels que l'administrateur par défaut, ITIL et l'employé. La définition de la propriété rend nécessaire la modification des informations d'identification par défaut de l'administrateur, de l'ITIL et de l'employé lors de la connexion à l'application.

Étapes de configuration

1. Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe **admin**.
2. Accédez à la **Sécurité de système** > **Utilisateurs** > **Utilisateurs et groupes.**
3. Recherchez l'utilisateur sous ID d'utilisateur **admin** et Nom **administrateur**. Cliquez sur l'ID d'utilisateur **administrateur** pour modifier les paramètres de l'utilisateur.
4. Modifiez le champ **E-mail** pour indiquer une adresse e-mail valide pour cet utilisateur.
5. Cochez la case **Mot de passe à réinitialiser** .
6. Cliquez sur **Mettre à jour**.
7. Déconnectez-vous.
8. Connectez-vous à nouveau pour être invité à définir un nouveau mot de passe.
9. Répétez les étapes 3 à 7 pour les comptes ITIL et d'employés.

Cookies HTTP uniquement (renforcement de la sécurité de l'instance)

Utilisez cette `glide.cookies.http_only` propriété pour activer l'attribut HTTPOnly pour les cookies confidentiels.

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 intersite mais élimine certains vecteurs d'exploitation.

En savoir plus

Attribut	Description
Nom de la propriété	glide.cookies.http_only
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour atténuer le risque que le script côté client accède au cookie protégé.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette correction ajoute un marqueur HTTPOnly supplémentaire sur les cookies de session, les protégeant ainsi contre le vol. • Si vous disposez d'une fonctionnalité personnalisée qui nécessite JavaScript pour accéder au cookie de l'utilisateur, cela interrompt cette fonctionnalité. Cela ne devrait pas être le cas dans des circonstances normales. • Il Now Platform gère la gestion des sessions et il ne devrait pas y avoir de raison pour qu'un script personnalisé accède aux cookies de l'utilisateur.
Risque de sécurité	(Moyen) Les cookies de session dans l'application authentifient un utilisateur final et fournissent des autorisations d'accès implicites à l'application. Cela signifie qu'il est nécessaire de les protéger contre le vol ou l'exportation. Les indicateurs 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 Add a system property .

Validation stricte CSRF (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour activer la `glide.security.csrf.strict.validation.mode` validation stricte du jeton CSRF. Si le jeton CSRF ne correspond pas, une nouvelle soumission de la demande est impossible.

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.csrf.strict.validation.mode

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer une validation stricte du jeton CSRF et empêcher sa réutilisation.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction active une étape de validation supplémentaire avant que l'utilisateur d'instance n'envoie une demande d'écriture à l'instance. 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 falsification 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 de l'instance en abusant de la confiance de l'utilisateur de l'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.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Désactiver l'authentification sans mot de passe (renforcement de la sécurité de l'instance)

Utilisez cette `glide.login.no_blank_password` propriété pour empêcher les utilisateurs de se connecter à la avec des Now Platform mots de passe vierges 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 car les noms d'utilisateur sont parfois faciles à deviner au sein d'une organisation.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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.

Attribut	Description
Risque de sécurité	(Élevé) Un attaquant peut se connecter à l'instance avec les noms d'utilisateur par défaut, ou par personne/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.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Activer l'authentification multifacteur (MFA) (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour activer l'authentification `glide.authenticate.multifactor` à plusieurs facteurs (MFA) dans l'instance. L'authentification MFA est une exigence de sécurité qui demande à l'utilisateur de saisir plus d'un ensemble d'informations d'identification pour s'authentifier sur une instance.

En savoir plus

Attribut	Description
Nom de la propriété	glide.authenticate.multifactor
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Renforcez la sécurité des instances en introduisant l'authentification multifacteur pour les connexions interactives des utilisateurs.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) 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	(Moyen) Si cette propriété n'est pas activée, il existe un risque d'accès non autorisé aux données sensibles.
Références	Propriétés système de l'authentification multifacteur

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Définir des critères d'authentification multifacteur basés sur les rôles

Utilisez cette propriété pour appliquer l'authentification multifacteur basée sur les `glide.authenticate.multifactor` rôles (MFA) à tous les utilisateurs affectés à des rôles spécifiques.

appliquer l'authentification multifacteur en fonction des rôles affectés à l'utilisateur. Si les rôles « administrateur », « security_admin » ou « user_admin » de la liste des rôles multifacteur ont été affectés à un utilisateur, 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.
- Définissez cette propriété sur **faux** pour désactiver l'authentification multifacteur basée sur les rôles 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)
Configurer dans le centre de sécurité de l'instance	Oui
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 Security	**Activez l'authentification multifacteur basée sur les rôles** dans la **table Critères multifacteur**.
Impact fonctionnel	(Moyen) 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	(Moyen) Si cette propriété n'est pas activée, il existe un risque d'accès non autorisé aux données sensibles.
Références	Configurer des critères multifacteur basés sur les rôles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Activer les contrôles de la politique de Réinitialisation du mot de passe (renforcement de la sécurité de l'instance)

Utilisez la propriété **glide.enable.password_policy** pour activer les vérifications de la politique de mot de passe chaque fois qu'un utilisateur change 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.

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.

En savoir plus

Attribut	Description
Nom de la propriété	glide.enable.password_policy

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Type de configuration	Propriétés système (/sys_properties_list.do)
Objectif	Pour appliquer la politique de mot de passe au moment du changement de mot de passe.
Valeur recommandée	true (pour les mots de passe de niveau de sécurité élevé)
Impact fonctionnel	(Moyen) définir la propriété sur true active les vérifications de la politique de mot de passe lorsqu'un utilisateur réinitialise son mot de passe.
Risque de sécurité	(Moyen) 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 d'Instance Security Center :

1. Sous **Moyen**, sélectionnez **Gestion des sessions**.
2. Dans le paramètre **Activer la vérification de la stratégie de réinitialisation du mot de passe** , sélectionnez **Moyen** pour les mots de passe de complexité moyenne ou **Fort** pour les mots de passe plus robustes et plus forts. Si vous sélectionnez l'une de ces options, la propriété **glide.enable.password_policy** est définie sur true et démarre 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.

Gestion des échecs de tentatives de connexion (renforcement de la sécurité de l'instance)

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 Now 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
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer une stratégie stricte pour les tentatives de connexion échouées, afin d'éviter l'attaque par force brute des informations d'identification.
Valeur recommandée	Actif

Attribut	Description
Impact fonctionnel	(Faible) 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	(Moyen) Appliquez une stratégie de journalisation et d'audit définie afin de pouvoir identifier les activités suspectes et intervenir en temps opportun.
Références	

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, faites passer l'état Actif de l'action `SNC User Lockout Check with Auto Unlock` ou `SNC User Lockout Check` des scripts 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.

Saisie semi-automatique du champ de mot de passe (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour permettre aux navigateurs d'utiliser la saisie semi-automatique sur les champs de mot de passe dans les `glide.login.autocomplete` formulaires de connexion.

En savoir plus

Attribut	Description
Nom de la propriété	glide.login.autocomplete
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour désactiver le navigateur afin de tenter de saisie semi-automatique pour un champ de mot de passe.
Valeur recommandée	faux
Impact fonctionnel	(Faible) Cette correction entraîne la désactivation du marqueur de **saisie semi-automatique du champ Mot de passe** , de sorte que le cache de l'historique des mots de passe par le navigateur n'est pas affiché dans le champ. Il ne devrait pas y avoir d'impact sur les fonctionnalités.
Risque de sécurité	(Faible) Les champs d'authentification utilisateur doivent être validés et ne doivent jamais laisser la mise en cache côté client se produire.
Références	https://support.servicenow.com/kb_view.do?sysparm_article=KB0563953

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Supprimer les informations d'identification de la page d'accueil (renforcement de la sécurité de l'instance)

Modifiez le contenu par défaut de la page d'accueil pour supprimer les informations d'identification par défaut.

Remarque :
Deux enregistrements Comment se connecter font partie des données de démonstration du module d'extension CMS. 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 sécurité conformément aux pratiques de sécurité recommandées. Pour en savoir plus, consultez Bonnes pratiques en matière de sécurité.

Étapes de configuration

1. Accédez à la **Interface utilisateur du système** > **Contenu de page d'accueil** > **.**
2. Trouvez les deux sections avec une brève description de **Comment se connecter**.
3. Faites passer l'état Actif de **chacun** d'eux de vrai à **faux**.

Supprimer Se souvenir de moi (renforcement de la sécurité de l'instance)

Utilisez cette `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)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour s'assurer qu'aucune information d'authentification n'est mise en cache.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette correction modifierait 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 Gérer les sessions utilisateur .
Risque de sécurité	(Moyen) 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. • Cela pose un risque de sécurité car il permet à la session utilisateur d'être active jusqu'à ce qu'il se déconnecte délibérément. La probabilité

Attribut	Description
	d'une attaque pour ce scénario augmente lorsque l'utilisateur final a laissé le navigateur sans surveillance ou s'il est compromis par une autre attaque.
Références	Décochez la case Se souvenir de moi

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Rotation des identificateurs de session HTTP (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour activer la rotation des identificateurs de session HTTP afin de réduire les `glide.ui.rotate_sessions` failles 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 désormais cette session authentifiée.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.rotate_sessions
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour obtenir une authentification de session plus sécurisée.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction a modifié l'ID de session lorsque l'utilisateur navigue d'une page non authentifiée vers des pages authentifiées. • Si vous utilisez un proxy ou codez en dur l'ID de session 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 Single Sign-on, 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 false.
Risque de sécurité	(Tardif) SessionID est utilisé pour traiter et authentifier l'utilisateur de l'instance en maintenant l'état de la session sur le navigateur. Par conséquent, les SessionID sont considérés comme des données sensibles et doivent être sécurisés par défaut. La rotation de session est un contrôle de sécurité qui applique la modification de l'ID de session chaque fois que l'utilisateur

Attribut	Description
	navigue à partir de pages non authentifiées pour authentifier des pages.
Références	Authentification avec SAML

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Cookies de session sécurisés (renforcement de la sécurité de l'instance)

Utilisez la propriété pour exiger des `glide.ui.secure_cookies` 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.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.secure_cookies
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour obtenir une authentification de session plus sécurisée.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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 Add a system property .

Politique de référence en matière de sécurité (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour contrôler les `com.glide.security.referrerpolicy` données de référent qui doivent être envoyées dans les en-têtes de réponse HTTP lorsque Now Platform pages envoie des demandes de données. La valeur Referrer-Policy d'un en-tête HTTP contrôle les informations de référent qui doivent être incluses dans les demandes de données.

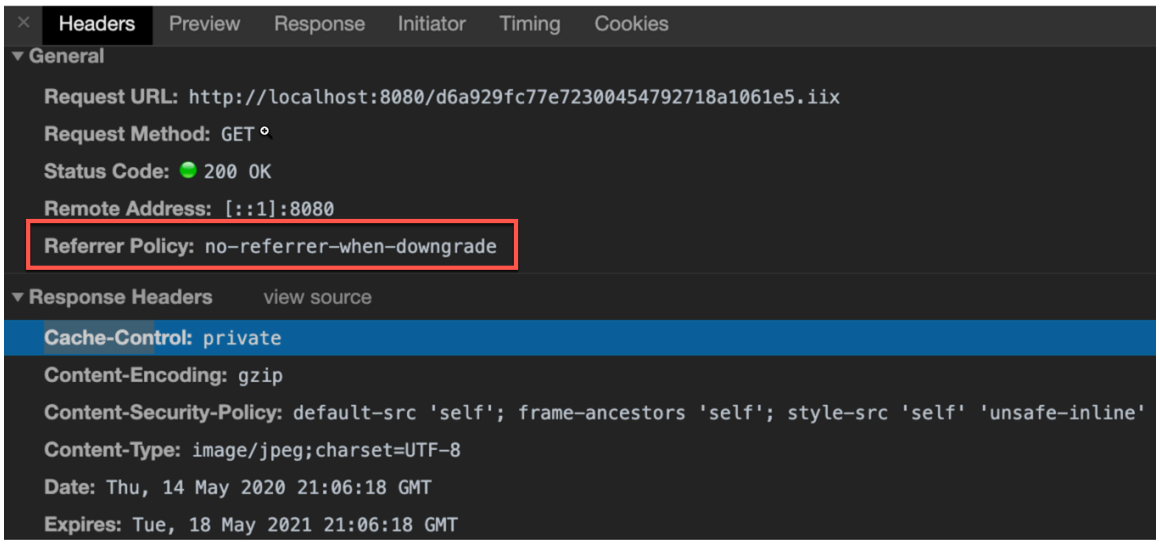
Valeurs de la politique de recommandation de sécurité

Définissez la `com.glide.security.referrerpolicy` propriété sur l'une des valeurs suivantes.

Valeur	Description
Par défaut	Now Platform L'instance gère le niveau d'informations envoyées dans les en-têtes de référent

Valeur	Description
	qui est approprié pour la demande de page spécifique Now Platform .
d'origine identique	Now Platform Les pages envoient une URL de référent complète au sein de l'instance et du même domaine, et aucun en-tête de référent vers une origine extérieure. Ce paramètre garantit un bon niveau de sécurité de l'instance.
origine	Now Platform Les pages envoient l'URL de base dans l'en-tête de référent au sein de l'instance et du même domaine, ainsi qu'en externe. Ce paramètre garantit un bon niveau de sécurité de l'instance.
origine-quand-origine-croisée	Now Platform Les pages envoient l'URL entière dans l'en-tête de référent au sein de l'instance et du même domaine, et envoient uniquement l'URL de base en externe. Ce paramètre garantit un bon niveau de sécurité de l'instance.
no-referrer-when-downgrade	Now Platform Les pages envoient l'origine, le chemin d'accès et la chaîne de requête dans l'URL, tant qu'il n'y a pas de rétrogradation dans un protocole de sécurité. **Remarque :** Ce paramètre ne garantit pas un bon niveau de sécurité de l'instance dans et Now Platform ne doit pas être utilisé.

Exemple de politique de référent et résumé des valeurs



En savoir plus

Attribut	Description
Nom de la propriété	com.glide.security.referrerpolicy
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Contrôle la quantité de données entrantes envoyées via l'en-tête « référent » lorsqu'une Now Platform page envoie une demande de données.
Valeur recommandée	Par défaut
Impact fonctionnel	(Faible) Si la valeur est définie sur « par défaut », l'instance Now Platform gère le niveau d'informations envoyées dans les en-têtes de référent.
Risque de sécurité	(Élevé) Définir cette valeur de propriété sur « no-referrer-when-downgrade » ne garantit pas un bon niveau de sécurité pour votre instance.
Référence	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy https://developer.mozilla.org/en-US/docs/Glossary/origin

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Délai d'activité de la session (renforcement de la sécurité de l'instance)

Utilisez cette 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 session spécifié est long, plus la quantité de mémoire utilisée au cours d'une session de traitement est importante. Le système de base utilise un délai d'expiration Apache Tomcat par défaut de 30 minutes.
- L'utilisateur Now Platform se déconnecte toujours avec Se souvenir de moi. Après 30 minutes d'inactivité dans l'application, la plateforme déconnecte automatiquement l'utilisateur, sauf si la case **à cocher Se souvenir de moi** dans la page de connexion est sélectionnée. Ce qui est différent, c'est qu'ils ne se reconnectent pas pour continuer.
- S'il existe des jauges ou du contenu sur les pages d'accueil des utilisateurs qui s'actualisent automatiquement, ce délai d'expiration risque de 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)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer le délai d'expiration de la session.
Valeur recommandée	Délai d'expiration spécifié par l'utilisateur, en minutes. 30 minutes est la valeur recommandée, mais cette valeur peut varier en fonction des exigences de fonctionnalité et de sécurité. Ne définissez pas cette valeur sur plus d'un jour.
Impact fonctionnel	(Moyen) 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	(Moyen) Le fait que les sessions utilisateur soient actives pendant une durée indéterminée constitue un risque de sécurité et doit expirer selon la configuration temporelle.
Références	Gérer les sessions utilisateur

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Délai d'expiration de la fenêtre de session (renforcement de la sécurité de l'instance)

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 le délai maximum est de 30 jours.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.user_cookie.life_span_in_days

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour activer l'expiration par défaut du cookie « Se souvenir de moi ».
Valeur recommandée	Valeur entière définie par l'utilisateur (# de jours) [Exemple : 15]
Impact fonctionnel	(Moyen) Cette propriété est activée par l'utilisateur final lorsque celui-ci coche la case **Mémoriser** mon nom dans la page de connexion et se connecte au Now Platform.
Risque de sécurité	(Moyen) Le fait que les cookies utilisateur soient actifs pour une durée indéterminée constitue un risque pour la sécurité et doit expirer selon une configuration basée sur le temps.
Références	Propriétés système disponibles Modifier les paramètres de la case à cocher Mémoriser mon nom et du cookie

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Configurer les mots de passe pour les comptes d'utilisateurs créés automatiquement

Utilisez les propriétés système et `glide.user.default_password` pour définir comment `glide.email.inbound.use_default_password` créer des mots de passe pour les nouveaux utilisateurs créés à partir d'e-mails entrants.

Les propriétés système décrites dans ce document définissent la manière dont l'instance gère les mots de passe des comptes utilisateur générés à partir d'e-mails entrants. Votre instance doit être configurée avec la possibilité de recevoir des e-mails et d'activer la création automatique d'utilisateurs. Consultez la section ci-dessous pour plus de détails sur ces configurations.

Une fois que votre instance est configurée pour créer automatiquement des comptes, vous pouvez utiliser les propriétés pour déterminer s'il faut utiliser un mot de passe par défaut et définir ce mot de passe, si nécessaire.

Prérequis

Pour utiliser ces propriétés, votre instance doit être configurée pour créer automatiquement de nouveaux comptes d'utilisateur.

- Vous devez configurer votre propre serveur POP3 pour stocker et recevoir des e-mails pour votre instance. Ensuite, vous devez définir la `glide.email.read.active` propriété système sur vrai. Pour en savoir plus sur la configuration d'un serveur POP3 sur votre instance, consultez Activer l'utilisation de votre propre serveur POP3 .
- Définissez la propriété `glide.pop3readerjob.create_caller` sur true. Avec ce changement de propriété, votre instance peut créer automatiquement des utilisateurs

à partir de l'e-mail entrant. Pour en savoir plus, reportez-vous à la section Activer la création automatique d'utilisateurs .

Remarque :
Ignorez la `glide.user.default_password` propriété si elle `glide.pop3readerjob.create_caller` est définie sur **faux**.

Comment votre instance définit les mots de passe

Dans Quebec et les versions antérieures de ServiceNow, votre instance crée des comptes d'utilisateurs à partir d'e-mails entrants à l'aide d'un mot de passe complexe défini dans la `glide.user.default_password` propriété système. Les utilisateurs utilisent ce mot de passe la première fois qu'ils se connectent, puis l'instance invite l'utilisateur à saisir un nouveau mot de passe. Si vous avez mis à niveau votre instance vers ou des Rome versions ultérieures, ce processus reste inchangé. En tant qu'administrateur, vous pouvez mettre à jour votre instance pour utiliser la nouvelle méthode décrite ci-dessous.

Dans les nouvelles instances à partir de la version, les Rome comptes d'utilisateurs créés à partir d'e-mails entrants n'ont pas de mot de passe. Lorsqu'un utilisateur accède pour la première fois à l'instance avec son nouveau compte, il doit saisir son nom d'utilisateur et cliquer sur le bouton **Mot de passe oublié ? pour** créer un mot de passe initial.

Dans Rome les versions et ultérieures, vous pouvez choisir le processus que votre instance suit en définissant une valeur dans la `glide.email.inbound.use_default_password` propriété système. Pour modifier le comportement par défaut décrit ci-dessus, créez cette propriété système à l'aide des informations suivantes :

Champ de propriété système	Valeur
Nom	glide.email.inbound.use_default_password
Type	true|false
Valeur	Sélectionnez une valeur en fonction du comportement souhaité : **VRAI** Les nouveaux comptes utilisent un mot de passe par défaut défini dans la `glide.user.default_password` propriété système. **faux** Les nouveaux comptes n'ont pas de mot de passe par défaut. Les utilisateurs doivent définir un mot de passe, comme décrit précédemment dans cette section.

Pour plus de détails sur la création de propriétés système, consultez Ajouter une propriété système .

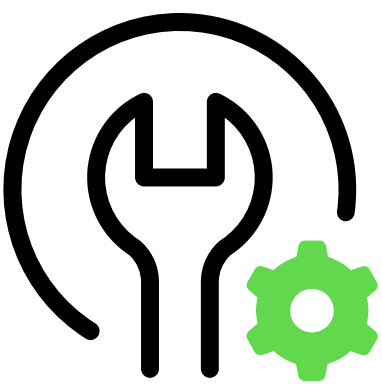
Définir un mot de passe par défaut

Si votre instance est configurée pour utiliser un mot de passe par défaut, vous devez définir ce mot de passe à l'aide de la `glide.user.default_password` propriété système. Créez cette propriété à l'aide des informations suivantes :

Champ de propriété système	Valeur
Nom	glide.user.default_password
Type	mot_de_passe2
Valeur	Saisissez un mot de passe unique à utiliser par défaut. Utilisez une complexité de mot de passe forte pour assurer la sécurité de votre instance.

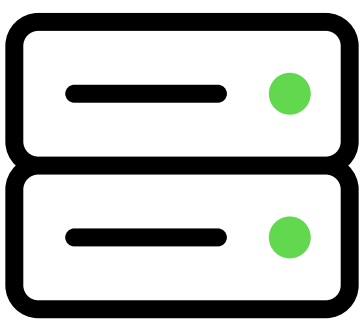
Autres paramètres et ressources de sécurité

Cette section contient les propriétés de sécurité que vous définissez en dehors d'Instance Security Center, ainsi que d'autres ressources liées à la sécurité.



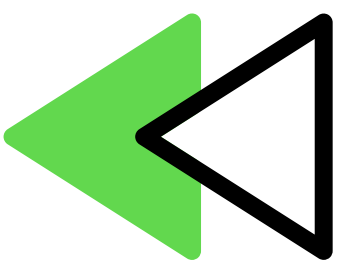
Propriétés système de sécurité

Les paramètres de sécurité fournissent plusieurs propriétés pour contrôler le niveau de sécurité de votre instance.



Guide de déploiement du MID Server

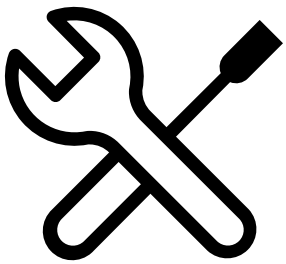
ServiceNow Management, Integration, and Discovery (MID) Server est une application Java légère qui s'exécute en tant que service Windows ou démon UNIX sur du matériel standard, y compris des ordinateurs virtuels.



Comportement réversible

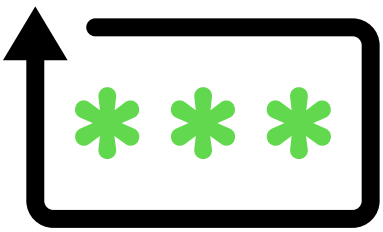
Certaines propriétés système sont classées comme « safe_overrides » ou « no_db_override ».

Traduction automatique



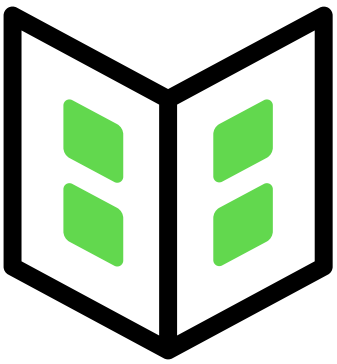
Propriétés de sécurité obsolètes

Ces propriétés de sécurité ont été déconseillées dans les versions antérieures.



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 dans votre instance.



Autres ressources sur la sécurisation renforcée

Sources supplémentaires d'informations sur le renforcement des contrôles de sécurité, en lien avec Now Platform.

Journalisation, audit et erreurs (renforcement de la sécurité de l'instance)

Appliquez une stratégie de journalisation et d'audit afin de pouvoir identifier les activités suspectes et intervenir en temps utile.

Pour en savoir plus sur ce qui peut être journalisé dans l'instance, reportez-vous à Journaux système. Assurez-vous qu'il existe un calendrier pour la surveillance des événements système tels que les connexions et les échecs de connexion à l'aide de **Journaux système** > **Events**.

Désactivation des messages d'erreur SQL (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour désactiver le `glide.db.loguser` rendu des messages d'erreur SQL dans un navigateur.

En savoir plus

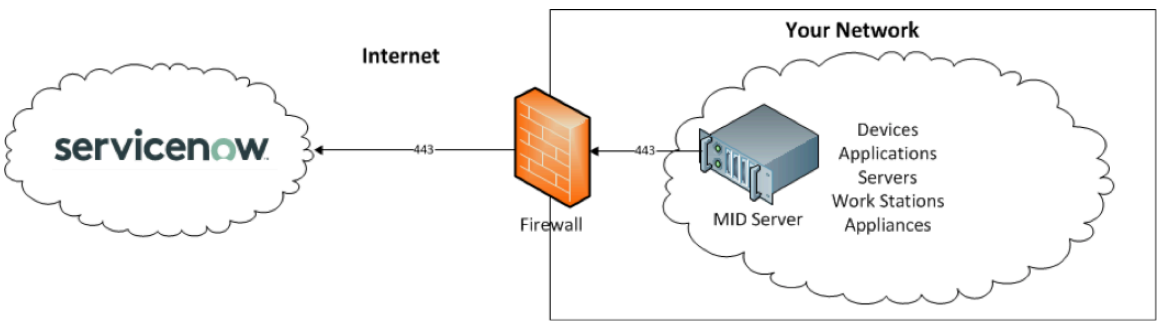
Attribut	Description
Nom de la propriété	glide.db.loguser
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurable dans le centre de sécurité de l'instance	Non
Objectif	Pour désactiver l'affichage des messages d'erreur SQL dans le navigateur.
Type	true|false
Valeur recommandée	faux
Impact fonctionnel	(Faible) Cette correction désactive le rendu des messages d'erreur SQL. Il n'y a aucun impact sur les fonctionnalités.

Attribut	Description
Risque de sécurité	(Moyen) Aucune information SQL sensible susceptible d'aider un attaquant ne doit apparaître dans le cadre d'un message d'erreur sur une page Web.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Guide de déploiement sécurisé du MID Server (renforcement de la sécurité de l'instance)

Le ServiceNow Management, Integration, and Discovery (MID) Server est une application Java légère qui s'exécute comme un service Windows ou un démon UNIX sur du matériel standard, y compris des ordinateurs virtuels.



Il s'authentifie en toute sécurité auprès de votre instance dans le ServiceNow Cloud à l'aide de ses propres identifiants de connexion et facilite la transmission des données avec vos applications, sources de données et services. Plusieurs MID Servers peuvent être déployés dans différents segments de réseau pour offrir une évolutivité supplémentaire.

Tenez compte des facteurs suivants concernant la sécurité de votre MID Server :

Sécurité physique

Sécurisez le matériel physique qui héberge le MID Server ou l'hyperviseur pour les MID Servers virtualisés.

- Placez le matériel dans un endroit sécurisé qui le protège contre tout accès non autorisé.
- Protégez l'accès à cet emplacement à l'aide d'un lecteur de carte électronique et d'une surveillance CCTV.
- Placez le matériel physique dans une cage verrouillée ou un rack avec un contrôle d'accès par clé physique.

Sécurité de l'infrastructure virtuelle

Utilisez la virtualisationavec la possibilité d'installer plusieurs MID Servers 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 MID Server 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 de confiance interne pour la console de gestion, tel que ESX Server et VirtualCenter.

- Utilisez les VLAN pour vous prémunir contre les attaques réseau.
- Suivez les consignes de sécurité publiées dans les guides de sécurisation renforcée des fournisseurs.

Sécurité du système d'exploitation

Découvrez comment le MID Server stocke son nom d'utilisateur et son Now Platform mot de passe dans son fichier de configuration, nommé config.xml, pour une authentification sécurisée à l'instance.

Le MID Server doit être déployé dans un système d'exploitation sécurisé et renforcé pour assurer la protection contre tout accès non autorisé aux informations d'identification :

- 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 MID Server.
- Installez régulièrement les correctifs de sécurité du système d'exploitation avec les logiciels antivirus les plus récents et mettez régulièrement à jour les définitions antivirus.
- Le MID Server nécessite un cadre de travail Java actuel pour s'exécuter. Maintenez Java à jour régulièrement.
- Supprimez ou désactivez les services et applications inutiles.
- Installez un pare-feu du système d'exploitation pour limiter l'accès aux ports non autorisés.
- Suivez les consignes de sécurité publiées dans les guides de sécurisation renforcée du système d'exploitation des fournisseurs.

Sécurité réseau

Le MID Server communique sur le port 443 à l'aide du protocole SSL vers l'instance et ne nécessite aucune connexion entrante.

Pour sécuriser correctement votre MID Server dans un réseau, procédez comme suit :

- Installez le MID Server 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 le MID Server pour qu'il n'accepte aucune connexion entrante autre que celles requises pour la gestion d'entreprise du système d'exploitation et du matériel.
- Le système qui héberge le MID Server doit être en mesure d'accéder au ServiceNow site de téléchargement à **install.servicenow.com**.

> **Remarque :**
> Cette URL renvoie vers le site de téléchargement, qui n'est ServiceNow pas accessible à partir de cette rubrique.

L'ordinateur hôte MID Serve doit être en mesure d'accéder à ce site pour télécharger le package d'installation. Il contacte **install.servicenow.com** 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 du MID Server a également lieu lorsque vous mettez à niveau une instance.

Pare-feu

Configurez votre pare-feu pour autoriser le trafic réseau sortant du MID Server vers votre instance et mettre à niveau automatiquement le serveur.

Pour configurer votre pare-feu, utilisez les exemples de syntaxe suivants :

- `<source IP> VERS &lt;instance_name>.service-now.com SUR LE PORT 443`
- `<source IP> VERS install.service-now.com SUR LE PORT 443`

Administrer et gérer

Cette section décrit les pratiques de sécurité et les directives pour l'administration et la gestion du MID Server 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 les instructions suivantes :

- N'utilisez pas de compte administratif dans l'instance pour le MID Server.
- Utilisez une longueur et une complexité de mot de passe suffisantes pour le compte de MID Server.
- Le mot de passe doit comporter au moins 12 caractères avec des majuscules, des minuscules, des chiffres et des caractères spéciaux.
- Utilisez différents comptes MID Server avec des mots de passe uniques pour différents MID Servers dans une instance.
- Utilisez la fonctionnalité de sécurité SOAP stricte pour protéger toutes les tables avec des listes de contrôle d'accès (ACL) en l'activant *`Enforce strict security on incoming SOAP requests`* dans **Propriétés système** > **Services web**.
- Changez les mots de passe du MID Server à la fréquence qui respecte la politique de mot de passe de votre organisation.

Remarque :
Pour en savoir plus, consultez Créer l'utilisateur du MID Server et lui accorder le rôle .

Configurer un MID Server sur un hôte Windows

Lorsque vous installez le MID Server sur un hôte Windows, il crée un service Windows. 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 MID Server sur l'hôte Windows.

1. Accédez à la **Gestion des ordinateurs** > **Services et applications** > **Services**.
2. Cliquez avec le bouton droit sur **ServiceNow MID Server**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Se connecter** 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 **ServiceNow MID Server**, puis cliquez sur **Redémarrer**.
8. Assurez-vous que le MID Server a pu redémarrer et se connecter à l'instance.

Informations d'identification Windows Discovery and Orchestration

Configurez un compte Windows ou Active Directory local sur les systèmes cibles avec le moins de privilèges nécessaires. Il n'est peut-être pas nécessaire d'utiliser les informations d'identification de l'administrateur du domaine.

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 pour la détection Linux et l'orchestration

Utilisez un compte non racine avec des privilèges sudo limités sur les systèmes Linux cibles lors de la détection et de l'orchestration.

Appliquez les consignes 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 majuscules, des minuscules, des chiffres et des caractères spéciaux.
- Lors de la configuration des autorisations sudo, les chemins d'accès locaux aux fichiers exécutables binaires peuvent différer en fonction de la distribution Linux que vous exécutez, consultez Commandes privilégiées du MID Server .

Chiffrer les informations d'identification de connexion au MID Server

Par défaut, les informations d'identification de connexion au MID Server 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, en utilisant la syntaxe suivante :

```
&lt;parameter name=&amp;quot;MID.instance.username » value=&amp;quot;MIDsrvadmin » />
```

```
&lt;parameter name=&amp;quot;MID.instance.password » encrypt=&amp;quot;true » value=&amp;quot;
$ECUREpassw 0rd&amp;quot;/>
```

Remarque :
Le chiffrement des informations d'identification de connexion au MID Server ne remplace pas un hôte de serveur non sécurisé avec une sécurité physique et réseau médiocre. Le mot de passe stocké dans le fichier config.xml est chiffré au premier démarrage du MID Server ou, s'il s'agit d'un MID Server 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 MID Server pour lequel vous souhaitez désactiver cette fonctionnalité.
3. Dans la configuration du MID Server, cliquez sur le bouton **Nouveau** en regard de Paramètres de configuration.
4. Dans Paramètre de configuration du MID Server, configurez les paramètres suivants :
   - **Nom de paramètre** mid.ssh.dh_group_length_min
   - **Valeur** 2048

Désactiver le SSL sortant

Vous pouvez désactiver SSLv2 et SSLv3 dans le Now Platform. La définition de cette propriété force le MID Server à utiliser TLS, profitant de sa sécurité accrue, lors des connexions sortantes, telles que les 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** : vrai

Désactiver les algorithmes faibles

Vous pouvez désactiver les algorithmes les plus faibles afin que les requêtes adressées 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, en utilisant 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 devez donc avoir un processus en place pour remettre à jour ce fichier après chaque mise à niveau.

Les utilisateurs de Powershell doivent consulter leur administrateur pour obtenir de l'aide Windows afin de désactiver les versions inférieures de TLS. Pour savoir quelles versions de TLS sont 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 de remplacement sécurisé.

Attribut	Catégorie
Refus par défaut	Contrôle d'accès
Activation de la vérification de l'ACL de AJAXGlideRecord	Contrôle d'accès
La protection de la vie privée sur les includes de script pouvant être appelés par le client comprend	Contrôle d'accès
Bac à sable pour les scripts générés par le client	Validation de l'entrée
Remplacement du mode de collecte (obsolète)	Liste d'inclusion de sécurité

Aucun remplacement de base de données

Les valeurs existantes de ces propriétés ne peuvent pas être modifiées ou remplacées.

Attribut	Catégorie
Activer les restrictions de téléchargement de fichiers	Pièces jointes

Propriétés de sécurité déconseillées

Ces propriétés de sécurité ont été déconseillées dans les versions antérieures.

Remplacement du mode de collecte (obsolète)

La `glide.whitelist.manager.collection_mode.override` propriété a été conçue pour fournir une rétrocompatibilité pour des 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 package 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.

Attribut	Description
	Validez-les pour l'autorisation et la restriction d'accès aux objets sensibles.
Références	https://support.servicenow.com/kb_view.do?sysparm_article=KB0621483

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 remis 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 jusqu'à ce que vous définissiez la propriété et fournissiez 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 du contrôle d'accès au contenu JavaScript

Si vous êtes un client ayant effectué une mise 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 ayant effectué une mise 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 ServiceNow® l'assistance pour obtenir de l'aide.

Rôle requis : admin

Procédure

1. Dans Application Navigator, recherchez sys_js_content_provider_rule.list.
2. Cliquez sur **Nouveau**.

3. Renseignez les champs du formulaire.

Règle du fournisseur de contenu JavaScript

Champ	Description
Actif	Option qui, lorsqu'elle est sélectionnée, active la règle. Lorsque cette option est désactivée, si aucune autre règle ne correspond, l'URL **du chemin d'accès** est admise.
Chemin d'accès	URL absolue vers 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 Not Found** 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. ○ **Rediriger** : le serveur renvoie le contenu d'un autre fichier 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 périmètre/de l'application ou du domaine.
Chemin de redirection	Champ qui clarifie le chemin vers lequel la redirection s'effectue. Lorsque **l'option Action** est définie sur **Rediriger**, le contenu de cette URL est

Champ	Description
	proposé à une demande pour l'URL du **chemin d'accès** .

4. Cliquez sur **Envoyer**.

Autres ressources sur la sécurisation renforcée

Vous trouverez ci-dessous d'autres sources d'information sur le renforcement des contrôles de sécurité en ce qui concerne le Now Platform.

Ressources	Description
Portail de test de sécurité	Portefeuille de services de sécurité sur HI
KB0538598	Test d'intrusion de l'application client | Politique et procédure
KB0546756	Désactivation de l'accès public au système de gestion de contenu (CMS)
KB0550071	ServiceNow, Inc. Révision du contrôle d'accès à l'instance
KB0550613	Identification et activation des restrictions d'adresse IP
KB0550828	Auditer et examiner les transactions GlideAjax
KB0550837	Correction 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. Monitoring - Vue d'ensemble et aperçu
KB0564232	Utilisation de ServiceNow, Inc. l'application Mobile avec authentification externe
Sécurité et risque	ServiceNow, Inc. Communauté

Paramètres de sécurisation renforcée

Le ServiceNow, Inc. contenu des paramètres de renforcement du Centre de sécurité contient des descriptions détaillées et des valeurs de conformité pour les propriétés système et les modules d'extension liés à la sécurité dans .Now Platform Vous pouvez définir ces propriétés à l'aide de l'application Paramètres de sécurisation renforcée dans Security Center.

Vue d'ensemble et objectif

Security Center calcule un score de conformité quotidien, exprimé en pourcentage, basé sur la conformité des paramètres de sécurité de votre instance actuels avec les valeurs de conformité définies dans les paramètres de renforcement de Security Center.

Vous pouvez gérer les paramètres de configuration de sécurité spécifiques qui peuvent affecter le score de votre instance directement à partir du Centre de sécurité.

Les configurations des paramètres de sécurisation renforcée sont expliquées avec 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	Nom de la propriété ou du module d'extension.
Type de configuration	Décrit l'endroit 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. Par exemple, booléen vrai/faux, installation, module d'extension, chaîne, etc.
Valeur recommandée	Valeur recommandée par le Centre de sécurité pour améliorer la conformité de la sécurité dans votre instance.
Valeur par défaut	La valeur définie pour la configuration dans le système de base.
Catégorie	Le nom et le lien vers la catégorie pour le 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 que la vulnérabilité soit exploitée. La faille de sécurité est prise en compte et notée individuellement à l'aide du score CVSS (Common Vulnerability 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 la gravité par score CVSS : • Critique : 9,0-10,0 • Haute : 7.0-8.9 • Moyenne : 4,0 à 6,9 • Faible : 0,01-3,9 • Aucun : 0,0
	Détails du risque de sécurité : décrit l'importance de la configuration du paramètre 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	L'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 et assistance client et seront indiquées comme telles.

Pour en savoir plus sur l'assurance que vos instances répondent aux exigences de sécurisation renforcée, consultez Sécurisation renforcée.

Autres ressources

Pour la référence utilisateur, la Now 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

Base de référence des paramètres de sécurisation renforcée

Découvrez comment des versions de base de référence distinctes pour les paramètres de sécurisation renforcée s'alignent sur les différentes versions de famille et de stockage.

Security Center 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 référence pour les propriétés système qui sont ingérées avec chaque version de l'application Security Center.

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 soutenues	Date de sortie de la boutique	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 (en anglais seulement)	Base de référence v2.0	Vancouver, Washington	nov. 2023	Famille Washington
SSC v1.4 (en anglais seulement)	Base de référence v4.0	Washington, Xanadu	mai 2024	Xanadu

Nouveaux paramètres de sécurisation renforcée

Voici une liste de tous les nouveaux paramètres de sécurisation renforcée publiés avec la base de référence de la Security Center version 2.0.

- Appliquer l'utilisation d'alias d'informations d'identification [Mise à jour dans Security Center 1.5]
- Appliquer la vérification OCSP en cas d'erreur réseau [Nouveau dans Security Center 1.3]
- Vérifier la chaîne de certificats et le nom d'hôte [Nouveau dans Security Center 1.3]
- Vérifier la révocation du certificat [Nouveau dans Security Center 1.3]
- Définir une politique de sécurité du contenu sécurisé pour les fichiers SVG [Nouveau dans Security Center 1.3]
- Utilisation de l'opération multiple d'insertion sécurisée dans l'API de jeu d'importation

- Activer le module d’extension des tables protégées [Nouveau dans Security Center 1.3]
- Appliquer la stratégie de référent sécurisé [Nouveau dans Security Center 1.3]
- Définir les rôles d’exception de délai d’expiration de session active [Nouveau dans Security Center 1.3]
- Invalider de manière proactive les sessions inactives [Nouveau dans Security Center 1.3]
- Valider le type MIME de fichier dans le service Web SOAP AttachmentCreator [Nouveau dans Security Center 1.3]
- Authentification basée sur certificat non mise en application
- Consigner les événements d’audit de session [Nouveau dans Security Center 1.3]
- Exiger l’authentification sur le processeur HTTP Event Management [nouveau dans Security Center 1.3]
- Appliquer des règles de sécurité au partage de tableaux de bord Nouveau dans Security Center 1.3]
- Interdire le clonage cible [Nouveau dans Security Center 1.3]
- Appliquer la sécurité du champ d’application pour les services numériques du secteur public [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]
- Limiter la durée de vie de la session active de l’invité [Nouveau dans Security Center 1.3]
- Limiter la taille du corps de la réponse HTTP [Mise à jour dans Security Center 1.5]
- Limiter la durée de vie de la session active des intégrations [Nouveau dans Security Center 1.3]
- Restreindre l’accès aux bases de connaissances [Nouveau dans Security Center 1.3]
- Masquer les commentaires des utilisateurs sur les articles [Nouveau dans Security Center 1.3]
- Restreindre les paramètres OAuth au corps de la publication [Nouveau dans Security Center 1.3]
- Limiter la taille des pièces jointes dans les flux de formation et de prédiction [Mise à jour dans Security Center 1.5]
- S’assurer que la création/la suppression des tableaux de bord nécessite une vérification d’accès [Nouveau dans Security Center 1.3]
- Activer le comportement hérité de clôture du champ d’application GlideRecord [Nouveau dans Security Center 1.3]
- Appliquer les restrictions de périmètre de l’application [supprimé dans Security Center 1.5]
- Exiger un accès en écriture pour accéder à la page d’ajout d’élément du catalogue de services [Nouveau dans Security Center 1.3]
- Durée de validation du jeton anti-CSRF [Nouveau dans Security Center 1.3]
- S’assurer que les ACL de table d’archivage sont vérifiées [Nouveau dans Security Center 1.3]
- Activer le gestionnaire de sécurité Java renforcé [Nouveau dans Security Center 1.3]
- Appliquer le privilège d’élévation stricte [Nouveau dans Security Center 1.3]
- Exiger l’effacement du presse-papiers lors de l’affichage en arrière-plan d’une application mobile [Nouveau dans Security Center 1.3]
- Appliquer les exigences en matière de chiffrement des appareils et de code d’accès [Nouveau dans Security Center 1.3]
- Limiter la durée de vie de la session active de l’interface utilisateur [Nouveau dans Security Center 1.3]

- Activer le journal d’audit MID [mis à jour dans Security Center 1.5]
- Instanciateurs de connexions JMS requis [Mise à jour dans Security Center 1.5]
- Exiger un captcha pour l’expérience de visite d’un invité dans l’application Customer Service [Mise à jour dans Security Center 1.5]
- Vérifier l’emprunt d’identité dans l’évaluation ACL de l’application RH [Mise à jour dans Security Center 1.5]
- Restreindre les mises à jour des tickets RH à partir d’e-mails personnels [Mise à jour dans Security Center 1.5]

Paramètres de sécurisation renforcée mis à jour

Cette liste contient les paramètres de sécurisation renforcée qui ont été mis à jour dans Security Center la version de base de référence 2.0.

Documentation	Mises à jour
Restreindre les demandes JSONP aux URL approuvées	• Nouvelle brève description : Restreindre les demandes JSONP aux URL approuvées • Ancienne brève description : Liste d’inclusion des demandes JSONP
Minimiser la taille autorisée des pièces jointes	• Nouvelle brève description : Minimiser la taille autorisée des pièces jointes • Ancienne description brève : Taille maximale autorisée des pièces jointes
Appliquer le certificat de confiance [supprimé dans Security Center 1.5]	• Nouvelle brève description : Appliquer le certificat de confiance • Ancienne brève description : Certificat de confiance
Définir des options Xframe pour empêcher l’intégration de sites Web tiers [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Définir des options XFrame pour empêcher l’intégration de sites Web tiers • Ancienne description courte : Options XFrame
Activer l'assainisseur HTML dans Agent virtuel	• Nouvelle brève description : Activer l’assainisseur HTML dans Agent virtuel • Ancienne description courte : Activer l’assainisseur HTML

Documentation	Mises à jour
Restreindre l’accès en lecture des développeurs délégués [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Restreindre l’accès en lecture des développeurs délégués • Ancienne brève description : Liste d’autorisations d’accès en lecture des développeurs délégués
Activer la notation et le filtrage d’e-mail indésirable [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Activer la notation et le filtrage d’e-mail indésirable • Ancienne brève description : Filtrage et notation d’e-mail indésirable
Module d’extension de haute sécurité [mis à jour dans Security Center 1.3]	• Nouvelle brève description : Activer le module d’extension de haute sécurité • Ancienne brève description : Module d’extension de haute sécurité
Activer le module d’extension de sécurité contextuelle [mis à jour dans Security Center 1.3]	• Nouvelle brève description : Activer le module d’extension de sécurité contextuelle • Ancienne brève description : Module d’extension de sécurité contextuelle
Appliquer l’assainissement HTML [mis à jour dans Security Center 1.3]	• Nouvelle brève description : Appliquer l’assainissement HTML • Ancienne description brève : Vérifier le HTML non désinfecté
Définir l’utilisateur invité pour les demandes SOAP [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Définir l’utilisateur invité pour les demandes SOAP • Ancienne description courte : utilisateur invité pour les demandes SOAP
Activer le module d’extension du contrôle d’accès SNC	• Nouvelle brève description : Activer le module d’extension du contrôle d’accès SNC • Ancienne brève description : Module d’extension du contrôle d’accès SNC

Documentation	Mises à jour
Activer le module d’extension de démarrage rapide de la sécurité (règles ACL) [mis à jour dans Security Center 1.3]	• Nouvelle brève description : Activer le module d’extension de démarrage rapide de la sécurité • Ancienne brève description : Module d’extension de démarrage rapide de la sécurité (règles ACL)
Désactiver le comportement AngularJS hérité [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Désactiver le comportement AngularJS hérité • Ancienne brève description : Comportement AngularJS hérité
Limiter les sessions interactives simultanées	• Nouvelle brève description : Limiter les sessions interactives simultanées • Ancienne brève description : Sessions interactives simultanées de limite d’authentification Glide
Limiter les sessions simultanées sur tous les nœuds [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Limite de sessions simultanées dans tous les nœuds • Ancienne description courte : limite de sessions simultanées dans tous les nœuds : limite d’authentification Glide
Minimiser le nombre de sessions interactives simultanées [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Minimiser le nombre de sessions interactives simultanées • Ancienne brève description : Sessions interactives simultanées max. authentification Glide
Activer l’authentification multifacteur basée sur les rôles [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Activer l’authentification multifacteur basée sur les rôles • Ancienne brève description : Authentification multifacteur basée sur les rôles

Documentation	Mises à jour
Activer la version mise à jour du module d'extension Multi SSO [Mise à jour dans Security Center 1.5]	• Nouvelle brève description : Activer la version actualisée du module d'extension Multi SSO • Ancienne description courte : La version mise à jour du module d'extension Multi SSO est activée
Minimiser la durée de contrainte SAML notBefore ou notOnOrAfter [Mise à jour dans Security Center 1.5]	• Nouvelle brève description : Minimiser la durée de contrainte SAML « notBefore » ou « notOnOrAfter » • Ancienne description courte : contrainte SAML « notBefore » ou « notOnOrAfter »
Exiger une autorisation pour les demandes d'API [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger une autorisation pour les demandes d'API • Ancienne brève description : Autorisation des demandes d'API
Exiger une autorisation pour les demandes CSV [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger une autorisation pour les demandes CSV • Ancienne brève description : Autorisation des demandes de CSV
Exiger une autorisation pour l'API REST du courtier en données [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger une autorisation pour l'API REST du courtier en données • Ancienne brève description : Autorisation de l'API REST du courtier en données
Exiger une autorisation pour les demandes Excel [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger une autorisation pour les demandes Excel • Ancienne brève description : Autorisation des demandes Excel
Exiger une autorisation pour les demandes d'importation [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger une autorisation pour les demandes d'importation • Ancienne brève description : Autorisation des demandes d'importation

Documentation	Mises à jour
Exiger une autorisation pour la demande JSONv2 [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger une autorisation pour la demande JSONv2 • Ancienne brève description : Autorisation de demande de JSONv2
Exiger une autorisation pour les demandes PDF [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger une autorisation pour les demandes PDF • Ancienne brève description : Autorisation de demande de PDF
Exiger une autorisation pour les demandes RSS [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger une autorisation pour les demandes RSS • Ancienne description courte : Autorisation de demande de RSS
Exiger une autorisation pour les demandes SCHEMA [mis à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger une autorisation pour les demandes SCHEMA • Ancienne brève description : Autorisation de demande de SCHEMA
Exiger une autorisation pour les demandes SOAP [mis à jour dans Security Center 1.5]	• Nouvelle brève description : Exiger une autorisation pour les demandes SOAP • Ancienne brève description : Autorisation de demande SOAP
Exiger une autorisation pour les demandes de déchargement	• Nouvelle brève description : Exiger une autorisation pour les demandes de déchargement • Ancienne description courte : Autorisation de la demande de déchargement
Exiger une autorisation pour la demande WSDL [mis à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger une autorisation pour la demande WSDL • Ancienne brève description : Autorisation de demande de WSDL
Exiger une autorisation pour les demandes XML	• Nouvelle brève description : Exiger une autorisation pour les demandes XML • Ancienne brève description : Autorisation de demande XML

Documentation	Mises à jour
Exiger une autorisation pour les demandes de sortie XML	• Nouvelle brève description : Exiger une autorisation pour les demandes de sortie XML • Ancienne brève description : Autorisation de sortie XML
Activer le marqueur de cookie HTTP uniquement [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Activer le marqueur de cookie HTTP uniquement • Ancienne description courte : Marqueur de cookie HTTP uniquement
Désactiver l'exécution de la requête de base de données brute	• Nouvelle brève description : Désactiver l'exécution de la requête de base de données brute • Ancienne brève description : Exigences de contrôle d'accès au niveau opérationnel
Désactiver les messages d'erreur SQL [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Désactiver les messages d'erreur SQL • Ancienne description courte : Désactivation des messages d'erreur SQL
Convertir les images des e-mails entrants en pièces jointes [supprimé dans Security Center 1.5]	• Nouvelle brève description : convertir les images des e-mails entrants en pièces jointes • Ancienne description courte : Convertir les e-mails entrants en HTML
Minimiser la quantité de destinataires SMTP [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Minimiser la quantité de destinataires SMTP • Ancienne description courte : Nombre maximal de destinataires SMTP
Formules Excel d'échappement [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : formules Excel d'échappement • Ancienne description courte : Échapper à une formule Excel
Activer l'assainisseur HTML [Mise à jour dans Security Center 1.5]	• Nouvelle brève description : Activer l'assainisseur HTML • Ancienne brève description : Assainisseur HTML

Documentation	Mises à jour
Valeur de l'en-tête HTTP du contrôle de cache [supprimé dans Security Center 1.5]	• Nouvelle brève description : Valeur de l'en-tête HTTP du contrôle de cache • Ancienne description courte : Valeur de l'en-tête HTTP du contrôle de cache
Appliquer le comportement de l'instance de production [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Appliquer le comportement de l'instance de production • Ancienne brève description : Comportement de l'instance de production
Définir les adresses IP internes autorisées ServiceNow [Mise à jour dans Security Center 1.5]	• Nouvelle brève description : Définir les adresses IP internes ServiceNow autorisées • Ancienne brève description : Liste d'autorisations d'accès pour les adresses IP
Désactiver le comportement JQuery hérité [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Désactiver le comportement JQuery hérité • Ancienne brève description : Comportement JQuery hérité
Annuler le nom distinctif initial LDAP [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Annuler le nom distinctif initial LDAP • Ancienne description courte : Nom distinctif initial LDAP
Restreindre l'accès aux écritures de journal personnalisées [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Restreindre l'accès aux écritures de journal personnalisées • Ancienne brève description : Sécurisation des écritures de journal personnalisées
Minimiser la durée de vie unique du vérificateur hors bande [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Minimiser la durée de vie unique du vérificateur hors bande • Ancienne brève description : Durée de vie courte et unique du vérificateur hors bande

Traduction automatique

Documentation	Mises à jour
Désactiver les connexions SSLv2/SSLv3 sortantes [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Désactiver les connexions SSLv2/SSLv3 sortantes • Ancienne brève description : Désactivation de SSLv2/SSLv3
Désactiver la création d'utilisateurs à partir d'e-mails entrants [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Désactiver la création d'utilisateurs à partir d'e-mails entrants • Ancienne brève description : Restreindre les e-mails par domaine
Restreindre l'accès à l'API de script GlideSystemUserSession [mis à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger l'authentification par défaut pour les includes de script pouvant être appelés par le client • Ancienne brève description : Protection de la vie privée sur les includes de script pouvant être appelés par le client
Exiger l'authentification par défaut pour les includes de script pouvant être appelés par le client [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger l'authentification par défaut pour les includes de script pouvant être appelés par le client • Ancienne brève description : Protection de la vie privée sur les includes de script pouvant être appelés par le client
Exiger la vérification de l'ACL AJAXGlideRecord [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Exiger la vérification de l'ACL AJAXGlideRecord • Ancienne description courte : Activation de la vérification de l'ACL de AJAXGlideRecord
Appliquer le bac à sable pour les scripts générés par le client [Mise à jour dans Security Center 1.3]	• Nouvelle brève description : Appliquer le bac à sable pour les scripts générés par le client • Ancienne brève description : Bac à sable pour les scripts générés par le client
Appliquer la validation stricte du jeton CSRF [Mise à jour dans Security Center 1.5]	• Nouvelle brève description : Appliquer la validation stricte du jeton CSRF • Ancienne brève description : Validation stricte du CSRF

Traduction automatique

Documentation	Mises à jour
Restreindre les types MIME chargés [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Restreindre les types MIME chargés* Description brève • Ancienne description courte : Restriction de type MIME de chargement, LA VALEUR PAR DÉFAUT EST PASSÉE DE TRUE À FALSE
Activer les ACL d'application administrateur incluses dans le périmètre	• Nouvelle brève description : Activer les ACL d'application administrateur incluses dans le champ d'application • Ancienne brève description : Administrer les ACL d'application d'administration incluses dans le champ d'application
Activer le jeton anti-CSRF [supprimé dans Security Center 1.5]	• Nouvelle brève description : Activer le jeton anti-CSRF • Ancienne description courte : Jeton anti-CSRF
Implémenter x-frame-options : en-tête de sécurité SAMEORIGIN	• Nouvelle brève description : Implémenter X-Frame-Options : en-tête de sécurité SAMEORIGIN • Ancienne description courte : X-Frame-Options : SAMEORIGIN
Exiger le brouillage de l'interface utilisateur de l'application mobile	• Nouvelle brève description : nécessite le brouillage de l'interface utilisateur de l'application mobile • Ancienne brève description : Obfuscation de l'interface utilisateur d'une application mobile
Refuser par défaut en cas d'ACL vides	• Nouvelle brève description : Refuser par défaut en cas d'ACL vides • Ancienne description courte : Refus par défaut du gestionnaire de sécurité
Valider le type de contenu SOAP	• Nouvelle brève description : Valider le type de contenu SOAP • Ancienne description courte : Vérification du type de contenu SOAP

Documentation	Mises à jour
Appliquer la sécurité stricte des requêtes SOAP	• Nouvelle brève description : Appliquer la sécurité stricte des requêtes SOAP • Ancienne brève description : sécurité stricte des requêtes SOAP
Activer la récupération de compte [Mise à jour dans Security Center 1.5]	• Nouvelle brève description : Activer la récupération de compte • Ancienne brève description : Récupération de compte
Exiger la validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable	• Nouvelle brève description : Exiger la validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable • Ancienne brève description : validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable
Appliquer Domain Separation sur les champs de type « remontée pas à pas » [Mise à jour dans Security Center 1.5]	• Nouvelle brève description : appliquer Séparation de domaine sur les champs de type « remontée pas à pas » • Ancienne brève description : Appliquer Séparation de domaine
Restreindre les types MIME téléchargeables	• Nouvelle brève description : Restreindre les types MIME téléchargeables • Ancienne description courte : Liste de refus des types de Mime téléchargeables
Définir les types MIME téléchargeables restreints [supprimé dans Security Center 1.5]	• Nouvelle brève description : Définir les types MIME téléchargeables restreints • Ancienne brève description : Types Mime téléchargeables
Script Jelly d'échappement	• Nouvelle brève description : Script Jelly d'échappement • Ancienne description courte : Escape Jelly
HTML d'échappement dans les vues de listes	• Nouvelle brève description : HTML d'échappement dans les vues de listes • Ancienne brève description : HTML d'échappement

Traduction automatique

Documentation	Mises à jour
Scripts d’échappement dans le bloc-notes	• Nouvelle brève description : Scripts d’échappement dans le bloc-notes • Ancienne brève description : Bloc-notes d’évasion
Balisage XML d’échappement	• Nouvelle brève description : Balisage XML d’échappement • Ancienne brève description : XML d’échappement
Exiger le brouillage de l’interface utilisateur de l’application mobile classique	• Nouvelle brève description : nécessite le brouillage de l’interface utilisateur de l’application mobile classique • Ancienne brève description : Obfuscation classique de l’interface utilisateur d’une application mobile
Accès public aux favoris	• Nouvelle brève description : Désactiver l’accès public aux favoris • Ancienne brève description : Accès public aux favoris
Appliquer la sécurité stricte des cookies de session	• Nouvelle brève description : Appliquer la sécurité stricte des cookies de session • Ancienne brève description : Cookies de session sécurisés
Désactiver le code HTML intégré	• Nouvelle brève description : Désactiver le code HTML intégré • Ancienne brève description : Code HTML intégré
Désactiver les balises JavaScript dans le HTML intégré	• Nouvelle brève description : Désactiver les balises JavaScript dans le HTML intégré • Ancienne brève description : Autoriser les balises Javascript dans le HTML intégré

Documentation	Mises à jour
Minimiser la durée du délai d'expiration d'activité de la session	• Nouvelle brève description : Minimiser la durée du délai d'expiration d'activité de la session • Ancienne brève description : Délai d'activité de la session
Restreindre les types de fichiers téléchargeables dans le contenu statique	• Nouvelle brève description : Restreindre les types de fichiers téléchargeables dans le contenu statique • Ancienne brève description : Restrictions de téléchargement des types de fichiers provenant d'un contenu statique
Minimiser la durée du délai d'expiration de la fenêtre de session	• Nouvelle brève description : Minimiser la durée du délai d'expiration de la fenêtre de session • Ancienne brève description : Délai d'expiration de la fenêtre de session
Minimiser la durée du délai absolu d'expiration de la session	• Nouvelle brève description : Minimiser la durée du délai absolu d'expiration de la session • Ancienne brève description : Délai absolu de session
Maximiser la durée du délai d'expiration de déverrouillage en cas d'échec de la connexion	• Nouvelle brève description : Maximiser la durée du délai d'expiration de déverrouillage en cas d'échec de la connexion • Ancienne brève description : Gestion du délai de déverrouillage en cas d'échec de la connexion
Restreindre les entités externes XML	• Nouvelle brève description : Restreindre les entités externes XML • Ancienne brève description : Liste d'autorisations d'URL pour validation d'entités XML
Minimiser le seuil d'expansion des entités [Mise à jour dans Security Center 1.5]	• Nouvelle brève description : Minimiser le seuil d'expansion des entités • Ancienne brève description : Définition du seuil d'expansion des entités

Documentation	Mises à jour
Minimiser la durée d’expiration de la demande de réinitialisation du mot de passe	• Nouvelle brève description : Minimiser la durée d’expiration de la demande de réinitialisation du mot de passe • Ancienne brève description : Expiration de la demande de réinitialisation du mot de passe
Minimiser le nombre maximal autorisé de tentatives de demande de réinitialisation du mot de passe	• Nouvelle brève description : Minimiser le nombre maximal autorisé de tentatives de demande de réinitialisation du mot de passe • Ancienne brève description : Tentatives maximales de demande de réinitialisation du mot de passe
Minimiser la durée de la fenêtre de tentatives maximales de demande de réinitialisation du mot de passe	• Nouvelle brève description : Minimiser la durée de la fenêtre de tentatives maximales de demande de réinitialisation du mot de passe • Ancienne brève description : Fenêtre Tentatives max. de demande de réinitialisation du mot de passe
Maximiser la durée de la fenêtre de nouvelle tentative de demande de réinitialisation du mot de passe	• Nouvelle brève description : Maximiser la durée de la fenêtre de nouvelle tentative de demande de réinitialisation du mot de passe • Ancienne brève description : Fenêtre de nouvelle tentative de demande de réinitialisation du mot de passe
Minimiser la durée de la fenêtre de succès des demandes de réinitialisation du mot de passe	• Nouvelle brève description : Minimiser la durée de la fenêtre de succès de demande de réinitialisation du mot de passe • Ancienne brève description : Fenêtre de réussite de la demande de réinitialisation du mot de passe

Documentation	Mises à jour
Maximiser la durée de la fenêtre de déverrouillage de demande de réinitialisation du mot de passe	• Nouvelle brève description : Maximiser la durée de la fenêtre de déverrouillage de demande de réinitialisation du mot de passe • Ancienne brève description : Fenêtre de déverrouillage de la demande de réinitialisation du mot de passe
Maximiser la complexité du SMS de réinitialisation du mot de passe	• Nouvelle brève description : Maximiser la complexité du SMS de réinitialisation du mot de passe • Ancienne brève description : Complexité du SMS de réinitialisation du mot de passe
Minimiser la durée d'expiration du SMS de réinitialisation du mot de passe	• Nouvelle brève description : Minimiser la durée d'expiration de SMS de réinitialisation du mot de passe • Ancienne description courte : Expiration du SMS de réinitialisation du mot de passe
Minimiser le nombre maximal de SMS de réinitialisation du mot de passe par jour	• Nouvelle brève description : Minimiser le nombre maximal de SMS de réinitialisation du mot de passe par jour • Ancienne description courte : Réinitialisation du mot de passe Nombre maximal de SMS par jour
Maximiser la durée de la fenêtre de pause du SMS de réinitialisation du mot de passe	• Nouvelle brève description : Maximiser la durée de la fenêtre de pause du SMS de réinitialisation du mot de passe • Ancienne brève description : Fenêtre de pause du SMS de réinitialisation du mot de passe
Activer la notification du code SMS pour l'inscription et la vérification	• Nouvelle brève description : Activer la notification du code SMS pour l'inscription et la vérification • Ancienne description courte : Notification du code SMS pour l'inscription et la vérification

Documentation	Mises à jour
Maximiser la durée du délai de vérification de la réinitialisation du mot de passe	• Nouvelle brève description : Maximiser la durée du délai de vérification de la réinitialisation du mot de passe • Ancienne brève description : Délai de vérification de la réinitialisation du mot de passe
Notifier les utilisateurs pendant le processus de réinitialisation/changement de mot de passe [supprimé dans Security Center 1.5]	• Nouvelle brève description : Notifier les utilisateurs pendant le processus de réinitialisation/changement de mot de passe • Ancienne brève description : Processus de réinitialisation du mot de passe/ notification de changement
Restreindre les domaines d'e-mail pour l'inscription des utilisateurs externes [Mise à jour dans Security Center 1.5]	• Nouvelle brève description : Restreindre les domaines d'e-mail pour l'inscription des utilisateurs externes • Ancienne description courte : Liste d'autorisation de domaines d'e-mails d'inscription d'utilisateur externe
Minimiser la durée d'expiration du lien d'inscription de l'utilisateur externe [Mise à jour dans Security Center 1.5]	• Nouvelle brève description : Minimiser la durée d'expiration du lien d'Inscription de l'utilisateur externe • Ancienne description courte : Expiration du lien d'Inscription de l'utilisateur externe
Restreindre les packages Java autorisés	• Nouvelle brève description : Restreindre les packages Java autorisés • Ancienne brève description : Liste d'autorisation des packages Java

Paramètres de sécurisation renforcée supprimés

Cette liste contient les paramètres de sécurisation renforcée qui ont été supprimés dans Security Center la version de base de référence 2.0.

- Activer la signature de code pour les données de configuration de l'application et les scripts
- Activer l'encrypteur Glide KMF
- Désactiver l'utilisation du chiffrement au niveau de l'instance
- Enregistrer tous les champs des requêtes HTTP sortantes

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. L’accès aux ressources n’est autorisé 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 en secondes d’expiration d’un jeton de sécurité.

Lorsqu’une session utilisateur expire, le jeton de sécurité expire avec elle, sauf si la propriété **Autoriser la réutilisation des jetons expirés est autorisée** est activée et si elle est comprise dans la période décrite par 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
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 : Si vous ne définissez pas cette propriété sur la valeur recommandée, la validation du jeton utilisée pour éviter les attaques de contrefaçon de requête intersite est désactivée.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété détermine la durée en secondes de validité d’un jeton de sécurité. Le jeton de sécurité expire à l’expiration de la session utilisateur, sauf si **l’option permettant la réutilisation des jetons expirés** est activée et si le jeton est compris dans la période spécifiée dans cette propriété. Ce jeton empêche les attaques de contrefaçon de requête intersite. La valeur par défaut est de 86 400 secondes ou 1 jour.

Appliquer Domain Separation sur les champs de type « remontée pas à pas » [Mise à jour dans Security Center 1.5]

La *glide.sys.domain.include_domain_condition_on_join* propriété contrôle si des conditions distinctes par domaine sont attribuées ou non à des requêtes de jointure afin de s'assurer qu'elles appliquent la fonctionnalité de séparation de domaine pour les champs de remontée pas à pas.

Cette *glide.sys.domain.include_domain_condition_on_join* propriété contrôle si des conditions distinctes par domaine sont attribuées ou non à des requêtes de jointure 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* ce paramètre n'est pas défini sur la valeur recommandée vrai sur une instance utilisant Domain Separation, des informations sensibles qui ne doivent pas être partagées avec un domaine spécifique peuvent alors être divulguées.

Remarque :
Lorsque le module d'extension Domain Separation est installé, un enregistrement sys_properties de cette propriété est installé avec sa valeur définie sur **vrai**, qui n'est pas sa valeur par défaut. Dans le cas contraire, dans le système de base où Domain Separation n'est pas installée, l'enregistrement de propriété n'existera pas et sa valeur autre que celle par défaut lui sera attribuée.

Avertissement :
Il s'agit d'une propriété d'exonération, 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	true, lorsque Domain Separation est installé, sinon la propriété n'existera pas.
Valeur par défaut	faux
Catégorie	Contrôle d'accès
Objectif	Contrôle si des conditions distinctes par domaine sont attribuées ou non à des requêtes de jointure afin de s'assurer qu'elles appliquent la fonctionnalité de Domain Separation pour les champs de 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* ce paramètre n'est pas défini sur la valeur recommandée vrai, des informations sensibles qui ne doivent pas être partagées avec un domaine spécifique peuvent être divulguées.
Références	Domain Separation pour les fournisseurs de services

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Activer les ACL d'application administrateur incluses dans le périmètre

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 champ d'application n'est définie pour le champ d'application de l'enregistrement.

Définissez la valeur `glide.security.scoped_administration.honor_global_acl` sur true pour empêcher un utilisateur ayant peu de privilèges et ayant des autorisations sur 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 champ d'application n'est définie pour le champ d'application de l'enregistrement, les ACL globales sont honorées. Si la valeur est définie sur false et qu'aucune ACL d'application administrateur incluse dans le champ d'application n'est définie pour le champ d'application de l'enregistrement, les vérifications ACL sont 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

Bloquer l'accès pour le développeur délégué

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 n'est pas en mesure de mettre à jour ou d'insérer des enregistrements dans la table de sys_user_has_role sans disposer également du 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 recommandée	VRAI
Dépendances de Security	aucun
Cote de risque de sécurité	6.7
Impact fonctionnel	(Élevé) Lorsqu'un utilisateur disposant du rôle delegated_developer tente de modifier un enregistrement dans la table de 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 a été 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 false, 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 sur l'instance.
Références	Contrôle d'accès

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Bloquer les jetons CSRF expirés [Mise à jour dans Security Center 1.5]

Bloquez les jetons CSRF expirés pour éviter les attaques de contrefaçon de requête intersite.

Vue d'ensemble

Les falsifications de requêtes intersites sont un type d'exploitation malveillante par lequel des commandes non autorisées sont exécutées pour le compte 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 expiré précédemment 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 la gravité par score CVSS : moyenne
	Détails du risque de sécurité : applique un mécanisme anti-CSRF fort pour protéger les fonctionnalités authentifiées, et un mécanisme anti-automatisation ou anti-CSRF efficace protège les fonctionnalités non authentifiées.
Dépendances et prérequis	Aucun
Références	Activer le jeton anti-CSRF [supprimé dans Security Center 1.5], falsification de requête intersites .

Vérifier les conditions de l'action d'interface utilisateur avant son exécution

Utilisez cette 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 des 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
Objectif	Pour garantir une validation supplémentaire sur la table, les actions d'interface utilisateur avant qu'elles ne soient exécutées.

Attribut	Description
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	3.3
Impact fonctionnel	(Faible) 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 d'interface utilisateur avant que le formulaire ne soit rendu à 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 Add a system property .

Configurer les rôles d'administrateur du groupe d'affectation Event Management [Nouveau dans Security Center 1.5]

Utilisez cette propriété pour définir les `evt_mgmt.connector_assignment_group_admin_roles` 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 la `evt_mgmt.connector_assignment_group_admin_roles` 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
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : faible

Attribut	Description
	• Détails du risque de sécurité : modifier les 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

Refuser l'accès interne aux rôles externes explicites [Mise à jour dans Security Center 1.5]

Plusieurs propriétés constituent la configuration du paramètre de sécurisation renforcée **de la liste de refus interne pour activer les rôles explicites** . La *glide.security.explicit_roles.enable_internal_user_blacklist* propriété empêche d'affecter le rôle de snc_internal à des utilisateurs externes et permet à la *glide.security.explicit_roles.internal_user_blacklist* propriété d'affecter le rôle de snc_external.

Glide.security.explicit_roles.enable_internal_user_blacklist

Vous pouvez donner l'accès à votre instance à la fois aux utilisateurs internes et aux utilisateurs externes. 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.

Définissez la *glide.security.explicit_roles.enable_internal_user_blacklist* propriété sur la valeur recommandée, **c'est-à-dire vrai** , pour pouvoir affecter le rôle snc_external.

Définissez la valeur sur **faux** pour désactiver la possibilité d'affecter le rôle snc_external. Le rôle snc_internal par défaut sera attribué à tous les utilisateurs

Remarque :
Les instances sans rôles explicites installés ne sont pas affectées. À partir de la version Paris, les nouvelles installations de rôles explicites obtiennent la propriété avec la valeur par défaut true.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.security.explicit_roles.enable_internal_user_blackl*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Permet l'affectation de classes d'utilisateurs spécifiées au rôle snc_external au lieu du rôle snc_internal.
Valeur recommandée	Vrai (valeur par défaut).
Type de configuration	Booléen.
Risque de sécurité	(Modéré) La désactivation de la propriété peut entraîner une affectation de rôle par défaut inappropriée.

Attribut	Description
Cote de risque de sécurité	5.4
Références	rôles explicites dans CSM ,

Glide.security.explicit_roles.internal_user_blacklist

La `glide.security.explicit_roles.internal_user_blacklist` valeur détermine les classes d'utilisateurs (tables qui étendent sys_user) à affecter au rôle snc_external au lieu du rôle snc_internal. La valeur par défaut csm_consumer_user customer_contact est définie pour s'aligner sur les cas d'utilisation dans les modules d'extension de Customer Service Management.

La valeur de la propriété ne doit être modifiée que s'il existe des classes d'utilisateurs supplémentaires ou différentes qui doivent être affectées au rôle snc_external par défaut, au lieu du rôle snc_internal. Contactez l'assistance pour modifier ces valeurs.

Attribut	Description
Nom de la propriété	`glide.security.explicit_roles.internal_user_blacklist`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Permet l'affectation du rôle snc_external affecté par défaut, au lieu du rôle snc_internal.
Valeur recommandée	`csm_consumer_user`, `customer_contact`
Type de configuration	Chaîne
Impact fonctionnel	
Risque de sécurité	(Modéré) La désactivation de la propriété peut entraîner une affectation de rôle par défaut inappropriée.
Cote de risque de sécurité	5.4
Références	Explicit Roles, Corriger les affectations de rôles d'utilisateur externe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Empêcher les utilisateurs inactifs de se connecter [Nouveau dans Security Center 1.5]

Configurez cette propriété pour contrôler si les utilisateurs inactifs peuvent s'authentifier sur votre instance.

Si le `glide.authenticate.only.allow.active.user.login` paramètre n'est pas défini sur la valeur recommandée vrai, les utilisateurs de la table sys_user marquée comme inactive peuvent toujours se connecter à l'instance. Les utilisateurs peuvent être marqués comme inactifs s'ils n'ont plus l'autorisation de se connecter, par exemple lorsqu'ils sont révoqués d'une entreprise. Si le paramètre est configuré sur false, les utilisateurs peuvent toujours accéder à l'instance et aux données auxquelles ils avaient accès précédemment.

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
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 : Si vous ne définissez pas cette propriété sur la valeur recommandée, vrai, des utilisateurs inactifs, tels qu'un employé licencié, peuvent continuer d'accéder à l'instance et à toutes les données.
Dépendances et prérequis	Aucun

Refuser l'accès non autorisé aux éléments demandés

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 pas de valeurs. Si `glide.sc.req_for.roles` a des valeurs, cette propriété n'a aucune signification et les utilisateurs ayant uniquement des rôles définis ont accès à l'API.

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, le script Client pouvant être appelé `Script Include 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 afin qu'elle puisse être exposée à des utilisateurs non privilégiés.
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` elle n'est pas définie sur la valeur recommandée de **refus** (autoriser) et que la valeur `glide.sc.req_for.roles` est vide, tout utilisateur peut demander des éléments pour d'autres utilisateurs, ce qui permet 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 Add a system property .

Activer le jeton anti-CSRF [supprimé dans Security Center 1.5]

Utilisez cette `glide.security.use_csrf_token` propriété pour garantir l'utilisation d'un jeton de sécurité pour identifier et valide les demandes entrantes, qui sont ensuite utilisées pour prévenir ces attaques.

Le Cross-Site Request Forgery (CSRF) est une attaque qui oblige un utilisateur final à exécuter des actions indésirables sur une application Web dans laquelle il est actuellement authentifié. Les attaques CSRF ciblent spécifiquement les demandes de changement d'état, et non le vol de données, car l'attaquant n'a aucun moyen de voir la réponse à la requête falsifiée.

Les propriétés suivantes peuvent être activées pour des contrôles supplémentaires sur le jeton CSRF :

- `glide.security.csrf_previous.time_limit`
- `glide.security.csrf_previous.allow`
- `glide.security.csrf.strict.validation.mode`

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	(Faible) 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 falsification des requêtes intersites constitue un risque de sécurité important qui compromet l'intégrité des données de l'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 requête 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 Add a system property .

S'assurer que les ACL de table d'archivage sont vérifiées [Nouveau dans Security Center 1.3]

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 false.

La `glide.security.enable_archive_table_acls` propriété ne doit pas être définie sur false, car les ACL de la table d'origine seront évaluées, quelle que soit sa valeur. Vous pouvez éviter d'ajouter 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 ajoutés aux tables archivées seront ignorées, une action contre-intuitive qui 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 en lecture actives sur les 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 à partir de laquelle les données ont été archivées) s'appliquera à la table d'archivage.

Attribut	Description
	Remarque : Seules les ACL de lecture sont prises en charge sur les tables d'archivage. D'autres opérations sur les tables d'archivage sont pilotées en interne par un gestionnaire d'accès.

Activer le module d'extension de sécurité contextuelle [mis à jour dans Security Center 1.3]

Activez le module d'extension Contextual Security (`com.glide.role_management`) pour activer la sécurité contextuelle, qui sécurise un enregistrement/des informations utilisant la création, la lecture, l'écriture et la suppression d'une fonctionnalité.

Une fois installé et activé, les rôles du dictionnaire (créés par Simple Security Manager) ne sont plus testés. Au lieu de cela, la recherche des Now Platform 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 implémentées 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 dans les 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
Objectif	Contrairement au gestionnaire de sécurité simple, le gestionnaire de sécurité contextuelle connaît la hiérarchie des tables système. Vous pouvez potentiellement avoir différentes règles de sécurité pour un champ en fonction de l'endroit où il apparaît dans la hiérarchie.
Valeur recommandée	Actif (module d'extension activé par défaut)
Cote de risque de sécurité	8.1
Impact fonctionnel	(Moyen) 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 côté serveur avant d'exécuter les opérations CRUD, afin de garantir le niveau d'accès approprié pour les utilisateurs de l'instance.
Références	Gestionnaire de sécurité contextuelle

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à Activate a plugin .

Activation de la vérification de l'ACL de AJAXGlideRecord (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour effectuer la `glide.script.secure.ajaxgliderecord` validation de la règle de contrôle d'accès (ACL, Access Control Rule) 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.

À partir de scripts clients, il est possible d'interroger des données arbitraires du serveur à l'aide de l'attribut AJAXGlideRecord (GlideAjax -Client), à l'aide d'une syntaxe telle qu'un enregistrement Glide côté serveur. C'est 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 pouvez interroger uniquement 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 le est en cours d'exécution sans vérification de l'appel Now Platform GlideAjax ACL, une API peut renvoyer des informations auxquelles l'utilisateur actuellement connecté ne pourrait pas accéder autrement.

En savoir plus

Attribut	Description
Nom de la propriété	glide.script.secure.ajaxgliderecord
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Assurez-vous que les ACL de sécurité sont vérifiées et validées même lorsque les enregistrements sont consultés via des API côté client.
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) 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 d'informations sur son impact et sur la façon de l'identifier, consultez Reportez-vous à l'article Auditer et examiner les transactions GlideRecord côté client [KB0550828] dans le 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, de sorte que l'utilisation de la validation ACL aide 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 script includes, les processeurs et les autres entités utilisées par une API GlideAjax

Attribut	Description
	(AJAXGlideRecord) afin qu'elle s'exécute avec l'autorisation appropriée. Implémentez des méthodes telles que `canRead ()`,`canWrite()`,`canCreate ()` et `canDelete ()` pour effectuer l'autorisation de l'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 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 des scripts provenant du client : • *`glide.script.use.sandbox`*: voir Bac à sable pour les scripts générés par le client. • *`glide.script.allow.ajaxevaluate`*: voir Activer AJAXEvaluate.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Appliquer la validation stricte du jeton CSRF [Mise à jour dans Security Center 1.5]

Utilisez cette propriété pour activer la *`glide.security.csrf.strict.validation.mode`* validation stricte du jeton CSRF. Si le jeton CSRF ne correspond pas, une nouvelle soumission de la demande est impossible.

La *`glide.security.csrf.strict.validation.mode`* propriété active la validation stricte du jeton CSRF qui empêche la réutilisation des jetons CSRF. Si cette propriété n'est pas définie sur la valeur recommandée, vrai, les jetons CSRF peuvent être réutilisés, ce qui ouvre la porte aux attaques CSRF.

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.
Valeur recommandée	VRAI
Valeur par défaut	VRAI

Attribut	Description
Cote de risque de sécurité	(Moyen) La falsification 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 de l'instance en abusant de la confiance de l'utilisateur de l'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.
Impact fonctionnel	(Moyen) Cette correction active une étape de validation supplémentaire avant que l'utilisateur d'instance n'envoie une demande d'écriture à l'instance. 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 falsification 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 de l'instance en abusant de la confiance de l'utilisateur de l'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.

Revenez à Configurer et charger votre clé fournie par le client pour charger votre clé emballée.

Restreindre l'accès en lecture des développeurs délégués [Mise à jour dans Security Center 1.3]

Si *com.glide.dd_allow_global_access_tables* elle 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 pourrait 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 qu'il `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.

Désactiver les e-mails entrants pour les utilisateurs bloqués

Utilisez cette propriété pour contrôler Inbound `glide.pop3.process_locked_out` Email Actions pour les utilisateurs actifs et bloqués.

Définissez cette propriété sur **faux** pour désactiver les e-mails entrants pour les utilisateurs bloqués.

Remarque :
Réfléchissez aux implications en matière de sécurité de l'autorisation pour les utilisateurs de domaines non approuvés, et aux raisons pour lesquelles ils ont été bloqués, avant d'autoriser les e-mails de leur part à déclencher des actions sur e-mail entrant.

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 Inbound Email Actions pour les utilisateurs bloqués.
Valeur recommandée	faux
Valeur par défaut	faux
Type de configuration	Booléen
Risque de sécurité	(Élevé) Lorsque vous définissez cette propriété sur **vrai**, il peut y avoir une divulgation d'informations, car les e-mails entrants seraient 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 Add a system property .

Double vérification des transactions entrantes

Utilisez cette propriété pour activer la double vérification de la sécurité sur les transactions entrantes lors de la `glide.security.strict.updates` soumission du 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.

En savoir plus

Avertissement :
Il s'agit d'une propriété d'exonération, 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.
Valeur recommandée	VRAI
Cote de risque de sécurité	8.1
Impact fonctionnel	(Faible) Cette correction ajoute une couche supplémentaire de validation pour vérifier les autorisations utilisateur sur la table/page cible sur l'instance. Tant que les contrôles d'accès sont définis de manière appropriée sur l'instance client, il ne devrait y avoir aucun impact.
Risque de sécurité	(Élevé) Vous devez toujours vérifier la demande d'accès lorsque des transactions ont lieu entre deux zones. Cette opération vérifie 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 Add a system property .

Activer les ACL pour contrôler les détails du profil en direct

Utilisez cette `glide.live_profile.details` propriété pour indiquer si un utilisateur doit être en mesure d'afficher tous les champs de détail, tels que le nom de l'entreprise et les numéros de téléphone, sur un profil actif.

Selon le paramètre de la `glide.live_profile.details` propriété, les éléments suivants se produisent :

- Si la valeur est définie sur Afficher, l'accès aux informations de profil actif est accordé, quelles 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, selon les ACL créées pour le profil d'utilisateur.
- Si la valeur est définie sur Masquer, l'accès aux informations de profil actif est restreint, quelles 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)

Attribut	Description
Valeur recommandée	ACL
Cote de risque de sécurité	4.3
Impact fonctionnel	(Moyen) 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 respecter 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 Add a system property .

Activer les ACL de la vue du rapport

Gérez une vérification des ACL report_view des rapports publiés.

Utilisez cette`glide.report.report_view.check_published` propriété pour gérer une vérification des ACL report_view pour les rapports publiés. Si la propriété n'est pas définie sur la valeur recommandée, **vrai**, la vérification des ACL report_view pour les rapports publiés est désactivée.

Avertissement :
Il s'agit d'une propriété d'exonération, 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.report.report_view.check_published`
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 : élevé • Score CVSS : 7,5 • Détails du risque de sécurité : si la propriété est définie sur **vrai**, la vérification des ACL pour report_view rapports publiés est désactivée.
Dépendances et prérequis	Aucun

Activer la liste d'autorisation d'URL pour la communication cross-origin entre iFrame

Utilisez cette propriété pour activer la `glide.ui.concourse.onmessage_enforce_same_origin` communication cross-origin entre iframes.

OpenFrame ne peut traiter que les messages provenant des domaines de confiance spécifiés dans la `glide.ui.concourse.onmessage_enforce_same_origin_whitelist` propriété. Pour en savoir plus, consultez Spécifier la liste d'autorisation UTL pour la communication cross-origin 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)
Catégorie	Contrôle d'accès
Objectif	Pour activer la liste d'inclusion des domaines de confiance, afin qu'ils puissent communiquer entre iframes pour OpenFrame.
Valeur recommandée	VRAI
Cote de risque de sécurité	4.2
Impact fonctionnel	(Moyen) Si vous n'incluez pas les domaines prévus, la possibilité d'intégrer d'autres pages dans Now Platform les instances peut être limitée.
Risque de sécurité	(Élevé) Si une page Web contient des gestionnaires d'événements qui n'effectuent pas une validation d'origine appropriée, une page Web, ou un script, quelle que soit son origine, peut communiquer avec elle. Il peut également lancer n'importe quelle 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 Add a system property .

Appliquer l'authentification pour l'ACL sans rôle

Utilisez cette `glide.security.enforce_auth_roleless_acl` propriété pour vous assurer que seuls les utilisateurs authentifiés passeront les vérifications des ACL vides.

Lorsque la `glide.security.enforce_auth_roleless_acl` propriété n'est pas définie sur vrai, GlideRecordSecure accorde l'accès aux utilisateurs non authentifiés lorsqu'un rôle ou des conditions sont manquants dans une liste de contrôle d'accès sous-jacente (ACL) protégeant les données.

Les ACL sont souvent laissées vides par les développeurs qui ont l'intention d'accorder l'accès à tous les utilisateurs authentifiés sur une instance. Cela signifie que n'importe quel utilisateur passera une vérification pour toute ACL vide. Cette propriété garantit que seuls les utilisateurs authentifiés passeront avec succès les vérifications des ACL vides. Le rôle public devra être explicitement utilisé pour accorder l'accès aux utilisateurs non authentifiés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.enforce_auth_roleless_acl`
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 : 7,5 • Score CVSS : élevé • Détails du risque de sécurité : lorsque cette propriété n'est pas définie sur vrai, une fuite de données non authentifiées peut avoir un impact sur la confidentialité.
Dépendances et prérequis	Aucun

Appliquer les restrictions de périmètre de l'application [supprimé dans Security Center 1.5]

Utilisez cette 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	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 : si cette propriété n'est pas définie sur la valeur recommandée,

Attribut	Description
	les applications incluses dans le périmètre et les développeurs délégués pour ces applications peuvent créer et mettre à jour des enregistrements dans des tables globales telles que Incident.
Dépendances et prérequis	Aucun

Appliquer des règles de sécurité au partage de tableaux de bord Nouveau dans Security Center 1.3]

Utilisez cette `glide.cms.dashboards.sharing_with_secure_search` propriété pour contrôler si les utilisateurs peuvent partager des tableaux de bord.

Lorsque la propriété n'est `glide.cms.dashboards.sharing_with_secure_search` pas définie sur **vrai**, les utilisateurs peuvent partager les groupes de tableaux de bord et les rôles auxquels ils n'ont pas accès. L'activation de cette propriété applique les listes de contrôle d'accès (ACL) lors de la recherche des tables sys_user, sys_user_role et sys_user_group pendant le processus de partage du 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 `glide.cms.dashboards.sharing_with_secure_search` la valeur sur true afin que les tableaux de bord ne soient partagés qu'avec les utilisateurs disposant 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 : Si vous ne définissez pas cette propriété sur la valeur recommandée vrai, les listes de contrôle d'accès ne sont pas appliquées lors de la recherche dans les tables sys_user, sys_user_role et sys_user_group. Cela peut entraîner le partage de tableaux de bord avec des utilisateurs non autorisés, exposant ainsi des informations sensibles.
Dépendances et prérequis	Aucun

Attribut	Description
Références	Access control
Impact fonctionnel	Cette propriété applique des règles de sécurité à la liste des utilisateurs, des groupes d'utilisateurs et des rôles qui sont visibles lors du partage de tableaux de bord.

Appliquer la sécurité du champ d'application pour les services numériques du secteur public [Nouveau dans Security Center 1.3]

Utilisez cette propriété pour contrôler la façon dont les données d'application de l'application Public Sector Digital Services sont accessibles.

`glide.enforce_security_scope.sn_gsm`

L'application ServiceNow Public Sector Digital Services vous permet de développer des applications pour le secteur public qui fournissent des services numériques aux citoyens, aux entreprises et aux agences.

Lorsqu'elle `glide.enforce_security_scope.sn_gsm` est définie sur faux, l'accès aux données d'application dans les tables globales de l'application Public Sector Digital Services peut être accessible en fonction des listes de contrôle d'accès (ACL) 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 par des 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	

Appliquer l'accès ACL inclus dans le champ d'application pour les playbooks de demande d'informations Nouveau dans Security Center 1.3]

Utilisez la propriété pour contrôler l'accès `glide.enforce_security_scope.sn_gsm_info_req` aux données du playbook pour la fonctionnalité Information Request Playbook.

L'application Information Request Playbook permet aux utilisateurs finaux du secteur public de soumettre et de suivre les demandes d'enregistrement public 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 true 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`
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 false, 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 cette propriété pour contrôler si les `glide.security.strict_elevate_privilege` rôles marqués comme privilégiés doivent être élevés manuellement pour que les options du rôle soient attribuées à l'utilisateur.

Définissez cette propriété sur true 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 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 dotés du rôle administrateur élèvent les privilèges si nécessaire.

Exiger la vérification de l'ACL AJAXGlideRecord [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour effectuer la `glide.script.secure.ajaxgliderecord` validation de la règle de contrôle d'accès (ACL, Access Control Rule) 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.

À partir de scripts clients, il est possible d'interroger des données arbitraires du serveur à l'aide de l'attribut AJAXGlideRecord (GlideAjax -Client), à l'aide d'une syntaxe telle qu'un enregistrement Glide côté serveur. C'est 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 pouvez interroger uniquement 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 le est en cours d'exécution sans vérification de l'appel Now Platform GlideAjax ACL, une API peut renvoyer des informations auxquelles l'utilisateur actuellement connecté ne pourrait pas accéder autrement.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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 consultés via des API côté client.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	8.1
Impact fonctionnel	(Élevé) 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 d'informations sur son impact et sur la façon de l'identifier, consultez Reportez-vous à l'article Auditer et examiner les transactions GlideRecord côté client [KB0550828] dans le 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, de sorte que l'utilisation de la validation ACL aide 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 script includes, les processeurs et les autres entités utilisées par une API GlideAjax (AJAXGlideRecord) afin qu'elle s'exécute avec l'autorisation appropriée. Implémentez des méthodes telles que `canRead ()`,`canWrite()`,`canCreate ()` et `canDelete ()` pour effectuer l'autorisation de l'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 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 des scripts provenant du client :

Attribut	Description
	• *glide.script.use.sandbox*: voir Bac à sable pour les scripts générés par le client. • *glide.script.allow.ajaxevaluate*: voir Activer AJAXEvaluate.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Appliquer les ACL au niveau des champs dans GlideRecordSandbox

Gérez les ACL au niveau des champs dans GlideRecordSandbox sur votre instance.

Utilisez lapropriété pour *glide.sandbox.fields.check_acl* appliquer les ACL de niveau champ 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 d'ACL peuvent être contournées, ce qui permet de compromettre les données sensibles, par exemple celles *sys_user.user_password* provenant d'un utilisateur non autorisé.

⚠ Avertissement :
La valeur de cette propriété est aucun remplacement de 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 [Mise à jour dans Security Center 1.5]

Découvrez comment sécuriser vos informations d'identification contre toute utilisation non autorisée en configurant la propriété MID Server.

Le Management, Instrumentation, and Discovery (MID) Server est une application Java qui s'exécute comme un service Windows ou un démon UNIX sur votre réseau local. Les propriétés du MID Server 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 fournissent un contrôle plus granulaire sur les informations d'identification qu'une table Discovery est autorisée à utiliser. Pour remédier à cette faille de sécurité, définissez `alias_filtering_behavior` l'option sur strict pour empêcher l'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 système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	Stricte
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, quels que soient leurs alias, pour les tables Discovery, ce qui augmente les risques d'accès non autorisé.
Dépendances et prérequis	Aucun
Références	• MID Server • Alias d'informations d'identification pour la détection

Appliquer les ACL de type GroupBy

Configurez votre instance pour effectuer des vérifications d'ACL sur les colonnes groupby.

Utilisez cette propriété pour configurer votre instance afin d'effectuer des vérifications d'ACL sur les colonnes groupby. Si cette propriété est définie sur la valeur **recommandée vrai,** l'attribut d'une `groupby_acl_check` table est défini pour honorer les ACL groupby. Si la propriété est définie sur **faux**, il n'y a alors aucune vérification d'ACL sur les colonnes groupby d'une table pouvant entraîner une fuite d'informations.

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 qui pourrait entraîner une fuite d'informations.
Dépendances et prérequis	Aucun

S'assurer que la création/la suppression des tableaux de bord nécessite une vérification d'accès [Nouveau dans Security Center 1.3]

La `glide.processors.check_access_before_process` propriété permet 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. Cette propriété doit toujours être définie sur true.

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	faux
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 un contournement de l'ACL sur les tableaux de bord.

Attribut	Description
	Cela permet à tous les utilisateurs authentifiés avec des privilèges faibles 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 false, les utilisateurs ayant des rôles inappropriés peuvent ajouter et supprimer sys_dashboard entrées (bien que la couche GlideRecord doive revérifier les ACL existantes). Une valeur définie sur true limite les opérations d'ajout et de suppression pour les utilisateurs ne disposant pas des droits d'accès requis.

Appliquer la validation des paramètres de l'état OAuth

Configurez cette *glide.oauth.state.parameter.required*propriété pour empêcher votre instance contre les attaques de contrefaçon de requête de site à site (CSRF).

Cette *glide.oauth.state.parameter.required* propriété permet d'exiger le paramètre State 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
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 d'empêcher les attaques CSRF.
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 téléchargement ou la mise à jour d'une photo de profil lorsqu'il est effectué sur un enregistrement utilisateur.

Ce paramètre ouvre la possibilité pour un utilisateur non autorisé de télécharger 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 lors des 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 restreindre le téléchargement de l'image de l'utilisateur aux utilisateurs autorisés.
Valeur recommandée	VRAI
Cote de risque de sécurité	3.7
Impact fonctionnel	(Faible) 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 **faux**, 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 Add a system property .

Restreindre les domaines d'e-mail pour l'inscription des utilisateurs externes [Mise à jour dans Security Center 1.5]

Utilisez cette propriété pour répertorier les *sn_ext_usr_reg.allowed_email_domains* domaines de messagerie externes acceptables.

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

Attribut	Description
Objectif	Répertoriez les domaines d'e-mail pour autoriser l'e-mail de l'utilisateur à s'inscrire.
Valeur recommandée	Définir comme 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 provenant de domaines indésirables. Assurez-vous que `sn_ext_usr_reg.allowed_email_domains` cette valeur n'est pas 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 Add a system property .

Masquer les commentaires des utilisateurs sur les articles [Nouveau dans Security Center 1.3]

Utilisez cette propriété pour contrôler si les `glide.knowman.show_user_feedback` commentaires sont visibles ou non.

Lorsque `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.knowman.show_user_feedback.roles`Glide sont visibles sur les articles de la base de connaissances (KB). Comme les commentaires peuvent contenir des informations sensibles, vous ne souhaitez peut-être 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
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails du risque de sécurité : si vous ne définissez pas cette propriété sur « jamais », des informations sensibles seront divulguées dans les commentaires de commentaires.

Attribut	Description
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.

Module d'extension de haute sécurité [mis à jour dans Security Center 1.3]

Lorsque vous activez le module d'extension High Security, celui-ci 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 permettant un contrôle d'accès strict, la validation d'entrée et l'encodage de sortie.

Ces configurations comprennent :

- Contrôle d'accès
- Règles métier
- Propriétés système
- Action de politique d'interface utilisateur
- Actions des scripts
- Script includes

Exemple

Consultez les exemples pour les propriétés suivantes :

Propriété	Sujet
glide.ui.escape_all_script	Échapper à Jelly
glide.security.strict.actions	Vérifier l'action d'interface utilisateur avant son exécution
glide.security.csrf_previous.autoriser	Jeton anti-CSRF
glide.security.csrf.strict.validation.mode	Validation stricte du CSRF

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	L'activation de ce module d'extension est obligatoire. Il augmente le niveau de sécurité d'une instance, ce qui réduit la surface d'attaque en atténuant les 10 principales attaques owasp, y compris CSRF, XSS, sécurisation des cookies de session et chargements de fichiers.
Valeur recommandée	Actif
Cote de risque de sécurité	9.8

Attribut	Description
Impact fonctionnel	(Élevé) Ce module d'extension active plusieurs configurations de sécurité 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 des 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

Respecter les ACL de remplacement de l'administrateur

Cette `glide.security.admin.override.accessterm` propriété empêche les administrateurs de remplacer l'évaluation de l'ACL, même lorsque le remplacement doit être appliqué.

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 les administrateurs dans l'impossibilité de remplacer l'évaluation de l'ACL.
Valeur recommandée	Vrai (par défaut)
Type de configuration	Booléen
Risque de sécurité	(Faible) Les ACL sont évaluées de façon cumulative. S'il existe un nombre d'ACL sur un champ donné et que l'option Remplacements administrateur est définie sur faux (non sélectionné) sur l'une d'elles, les remplacements administrateur effectifs pour toutes les ACL sont considérés comme faux.
Cote de risque de sécurité	3.8
Références	Règles des listes de contrôles d'accès

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Restreindre les demandes JSONP aux URL approuvées

Spécifiez des URL fiables pour le service $http AngularJS afin d'autoriser ou de rejeter les demandes JSONP.

La `angular.jsonp.inclusion_list.enabled` propriété indique des URL fiables pour le service $http angularJS afin d'autoriser ou de rejeter les demandes JSONP. Cette propriété est nécessaire, car il s'agit d'un changement qui peut avoir des conséquences importantes

pour les clients, ils ont donc besoin d'une solution pour ajouter leurs URL fiables. Si cette propriété n'est pas définie sur la valeur recommandée, vrai, les demandes JSONP sont alors autorisées pour n'importe quelle URL.

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 : moyen • Score CVSS : 5,4 • Détails du risque de sécurité : définir cette propriété sur **faux** active les demandes JSONP vers n'importe quelle URL.
Dépendances et prérequis	Aucun

Désactiver l'exécution de la requête de base de données brute

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 , `false`cela permet l'appel d'un `dbi.executeStatement()` scriptable Glide, ce qui peut entraîner l'exécution d'instructions SQL malveillantes.

⚠ Avertissement :
Cette propriété est à la fois sécurisée et sans remplacement de base de données.

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

Attribut	Description
Risque de sécurité	• Score de gravité : 7,2 • Score CVSS : élevé • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur **faux,** l'appel de à `dbi.executeStatement()` partir d'un scriptable Glide.
Dépendances et prérequis	Aucun
Références	Règles des listes de contrôles d'accès

Définir l'utilisateur invité pour les demandes SOAP [Mise à jour dans Security Center 1.3]

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. Si elle n'est pas définie sur la valeur conseillée, ou `soap.guest`si elle est définie sur un utilisateur avec des privilèges limités, les demandes SOAP s'exécutent alors 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	savon.invité
Valeur par défaut	savon.invité
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 8,1 • Score CVSS : élevé • Détails du risque de sécurité : si vous laissez cette propriété vide, vous pouvez accéder aux opérations de niveau administrateur ou de maintenance sans authentification.
Dépendances et prérequis	Aucun

Exiger l'authentification par défaut pour les includes de script pouvant être appelés par le client [Mise à jour dans Security Center 1.3]

Par défaut, les script includes pouvant être appelés par le client qui ne définissent pas explicitement la visibilité sont publics. Si nécessaire, ajoutez la propriété pour activer le contrôle de la `glide.script.ccsi.ispublic` confidentialité sur tous les includes de script appelables par les clients accessibles via des pages publiques.

Lorsque vous ajoutez cette propriété, vous devez définir sa valeur sur **false**, ce qui signifie que tous les script includes 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 une valeur **vrai**, ni 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 script include particulier pouvant être appelé par un client en ajoutant la fonction `isPublic( )`.

- Le paramètre `isPublic()` a priorité sur la `glide.script.ccsi.ispublic` propriété.
- Par exemple, si vous définissez `isPublic()` sur **true** dans un script individuel, cela le rend public, ce qui remplace la propriété qui rend privées toutes les autres inclusions de script pouvant être appelées par un `glide.script.ccsi.ispublic` client.

Avertissement :
Il s'agit d'une propriété d'exonération, 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	Rendre privé les includes de script appelables par le client signifie que les invités qui accèdent aux pages publiques ne peuvent pas accéder à l'include de script pouvant être appelé par le client. Un utilisateur non connecté ne peut pas exécuter de script privé.
Valeur recommandée	faux
Cote de risque de sécurité	7.5
Impact fonctionnel	(Élevé) 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, les includes de script côté client contournent les ACL, ce qui peut entraîner une fonctionnalité publique non prévue. Si le script client fournit des informations confidentielles, il peut présenter un risque de sécurité potentiel défavorable.

Attribut	Description
Solution de contournement	Si vous définissez la *glide.script.ccsi.ispublic* propriété sur **false** , tous les script includes pouvant être appelés par le client sont privés. Vous pouvez modifier le paramètre de confidentialité pour un script include client pouvant être appelé individuel en ajoutant la fonction isPublic(). La fonction isPublic a priorité sur la *glide.script.ccsi.ispublic* propriété. Ajoutez la syntaxe suivante au script include : isPublic :function(){return[vrai/faux] ;},

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Appliquer le comportement de l'instance de production [Mise à jour dans Security Center 1.3]

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 vrai,** 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
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 : la définition de cette valeur de propriété sur **faux** traite l'instance 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 en lecture au contexte de flux [Nouveau dans Security Center 1.5]

Utilisez cette propriété pour appliquer si *com.snc.process_flow.reporting.require_flow_access* 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 d'informations mineures 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 : définir cette propriété sur faux conserve son comportement existant. Définir cette propriété sur true applique la couche de sécurité supplémentaire de l'accès en lecture.
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque cette propriété est activée, la sécurité de lecture des enregistrements de contexte de flux est augmentée. L'instance impose que l'utilisateur qui tente de lire le contexte de flux dispose également d'un accès en lecture au flux parent.

Limiter l'accès au script en arrière-plan

Configurez la *glide.script_processor.admin*propriété pour définir le rôle requis pour accéder au module Arrière-plan de script.

La *glide.script_processor.admin* propriété dispose du rôle requis pour accéder au module Arrière-plan de script. Si cette propriété n'est pas définie sur la valeur **recommandée admin,** n'importe quel utilisateur, quel que soit son rôle, est en mesure d'exécuter des scripts en arrière-plan sur l'instance. Cela permet aux acteurs malveillants de contourner le système d'ACL, en leur accordant un accès complet aux tables.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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 admin 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 `glide.email.email_with_no_target_visible_to_all` de l'utilisateur aux e-mails, sauf s'il en est l'expéditeur ou qu'il possède le rôle administrateur.

Les utilisateurs non autorisés peuvent accéder aux e-mails de la table sys_email_list qui n'ont pas d'enregistrement cible. Au lieu d'appliquer des ACL aux entrées d'e-mail, cette propriété restreint l'accès uniquement à l'expéditeur de l'e-mail et aux utilisateurs disposant du rôle administrateur.

Remarque :
Les e-mails envoyés et reçus par l'instance apparaissent dans la table sys_email_list. Toutefois, seuls les e-mails reçus qui ont été marqués avec un état Erreur et Ignoré devraient 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 le client de messagerie d'afficher les e-mails lorsque l'utilisateur n'autorise pas l'accès.
Valeur recommandée	faux
Cote de risque de sécurité	5.4

Attribut	Description
Impact fonctionnel	(Faible) 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 n'importe quel e-mail 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 Add a system property .

Restreindre l'accès au module d'extension des plages d'adresses IP spécifiques

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 prévu pour l'instance, les administrateurs doivent limiter l'accès aux blocs réseau IP qui leur sont affectés.

Prérequis

Avant de définir cette propriété, vous devez activer le module d'extension IP Range Based Authentication (com.snc.ipauthenticator).`com.snc.ipauthenticator` Pour en savoir plus, consultez Authentification basée sur la plage IP la section Étapes de configuration (ci-dessous).

En savoir plus

Attribut	Description
Nom du module d'extension	`com.snc.ipauthenticator`
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 peut ou ne peut pas accéder à l'instance aux listes des domaines approuvés et non approuvés.
Valeur recommandée	Actif
Cote de risque de sécurité	5.3
Impact fonctionnel	(Faible) Les plages IP refusées par le client sont utilisées pour cet élément de rattrapage. 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**.
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 KB.
Dépendances et prérequis	Aucun
Impact fonctionnel	Refuse l'accès à une base de connaissances lorsque l'option Peut lire ou Peut contribuer n'est pas spécifiée.

Restreindre les autorisations pour le modèle CMDB

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 pour 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 Modèles de consommables [cmdb_consumable_product_model]
- 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 cmdb_model sont masquées par défaut.

Définissez la propriété sur **false** pour ne pas prendre en compte la colonne customer_visible/l'élément sur la table cmdb_model et pour vous appuyer sur les bases cmdb_model ACL auxquelles sn_esm_user ont accès.

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	Lorsqu'elle est définie sur**tue true**, le système utilise le paramètre du champ Visible par le client pour déterminer l'accès aux données des modèles de produits sur le Customer Service Portal.
Valeur recommandée	Vrai (la valeur par défaut est 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 disposer des autorisations nécessaires pour le modèle CMDB. **Remarque :** Ce rôle a tendance à être accordé à des utilisateurs externes. Des 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 Add a system property .

Restreindre l'accès non authentifié aux pièces jointes

Utilisez cette *glide.image_provider.security_enabled* propriété pour contrôler les paramètres de sécurité des images. Si la valeur est définie sur **true**, les images ne sont visibles que par les utilisateurs authentifiés et autorisés. Si la valeur est définie sur **false**, les images sont visibles par toutes les personnes qui possèdent l'URL de la pièce jointe.

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 rendue au format `.iix` .
Valeur recommandée	True (valeur par défaut)
Impact fonctionnel	(Faible) 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	(Élevé) Une 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 Add a system property .

Restreindre l'accès aux écritures de journal personnalisées [Mise à jour dans Security Center 1.3]

Utilisez cette `glide.live_feed.custom_journal.acl_check_enabled` propriété pour respecter les ACL sur les champs journal personnalisés.

Si `glide.live_feed.custom_journal.acl_check_enabled` cette option n'est pas définie sur la valeur recommandée, vrai, tous les utilisateurs peuvent alors voir toutes les entrées de journal dans la fonctionnalité de flux en direct. Définir la propriété sur vrai respecte les ACL sur les champs de journal personnalisé, ce qui est une bonne fonctionnalité.

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 écritures de journal en fonction des ACL.
Valeur recommandée	Vrai
Type de configuration	Booléen.
Risque de sécurité	(Modéré) Lorsque cette valeur est définie sur true, seules les écritures de journal personnalisées qui passent l'ACL sont

Attribut	Description
	affichées dans Flux en direct. Dans le cas contraire, 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 Add a system property .

Examiner les conditions de contrôle d'accès aux rôles explicites superflus [Nouveau dans Security Center 1.5]

Le module d'extension Explicit Roles est recommandé pour exiger que tous les utilisateurs disposent du rôle snc_internal pour accéder aux ressources internes, ou 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 renseignées avec les conditions de rôle. En raison d'une logique d'automatisation ou d'une 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 disposant d'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 sur la même liste de contrôle d'accès au sein d'une table. L'ACL est destinée à accorder l'accès aux administrateurs, auquel cas le rôle snc_internal est une erreur. Sinon, l'ACL est 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 sont en mesure de fonctionner pour un cas d'utilisation spécifique, le résultat doit être revu périodiquement.

Exécutez le script en arrière-plan suivant pour capturer une liste des ACL auxquelles ont snc_internal ou snc_external ajoutées à une ACL déjà mappée à un autre rôle. Validez si les ACL doivent accorder l'accès aux utilisateurs ayant les rôles snc_internal ou snc_external. Si les utilisateurs ayant des privilèges faibles ne doivent pas avoir accès via l'ACL, supprimez les rôles snc_internal ou snc_external. La suppression de ces rôles peut empêcher les utilisateurs d'accéder à la ressource protégée par l'ACL s'ils ne disposent pas d'un rôle restant.

```
var ExplicitRolesEnabled = new GlidePluginManager().isActive('com.glide.explicit_roles');

// Only check if Explicit Roles is enabled
if (ExplicitRolesEnabled) {

   var counterBadInternalACLs = 0;
   var counterBadExternalACLs = 0;
   var sysIdSncInternal = '7fcaa702933002009c8579b4f47ffbde';
   var sysIdSncExternal = '940ba702933002009c8579b4f47ffbe2';
   var api = new SNC.RoleManagementAPI();

   var gr = new GlideRecord('sys_security_acl_role');
   gr.addQuery('sys_user_role', sysIdSncInternal);
   gr.query();
   while (gr.next()) {
      var aclSysId = gr.sys_security_acl;
```

```
    var gr2 = new GlideRecord('sys_security_acl_role');
    gr2.addQuery('sys_security_acl', aclSysId);
    gr2.addQuery('sys_user_role', '!=', sysIdSncInternal);
    gr2.addQuery('sys_user_role', '!=', sysIdSncExternal);
    gr2.query();

    while (gr2.next()) {
      // exclude the roles if that contain snc_external
      var role = gr2.sys_user_role;
      var containedRoles = api.findAllContainedRolesForRole(role);
      if (containedRoles.contains(sysIdSncExternal))
        continue;
      gs.print('Found an ACL with snc_internal and yet another role=' + role + '; ACL sys_id='
+ aclSysId);
      counterBadInternalACLs++;
      break;
    }
  }

  var gr = new GlideRecord('sys_security_acl_role');
  gr.addQuery('sys_user_role', sysIdSncExternal);
  gr.query();
  while (gr.next()) {
    var aclSysId = gr.sys_security_acl;
    var gr2 = new GlideRecord('sys_security_acl_role');
    gr2.addQuery('sys_security_acl', aclSysId);
    gr2.addQuery('sys_user_role', '!=', sysIdSncInternal);
    gr2.addQuery('sys_user_role', '!=', sysIdSncExternal);
    gr2.query();

    while (gr2.next()) {
      // exclude the roles if that contain snc_internal
      var role = gr2.sys_user_role;
      var containedRoles = api.findAllContainedRolesForRole(role);
      if (containedRoles.contains(sysIdSncInternal))
        continue;
      gs.print('Found an ACL with snc_external and yet another role=' + role + '; ACL sys_id='
+ aclSysId);
      counterBadExternalACLs++;
      break;
    }
  }

  gs.print('Total number of ACLs with snc_internal and other roles: ' +
counterBadInternalACLs);
  gs.print('Total number of ACLs with snc_external and other roles: ' +
counterBadExternalACLs);
}
```

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.explicit_roles*, *sys_security_acl* et *sys_security_acl_role*

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Aucun type de données
Valeur recommandée	Aucune valeur recommandée
Valeur par défaut	Aucune valeur par défaut
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : en raison de l'automatisation ou de l'intervention d'un administrateur d'instance, les rôles src_internal ou src_external peuvent être ajoutés 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 disposant d'un rôle mappé à une ACL, l'ajout de l'un ou l'autre rôle sera trop large pour l'objectif d'une ACL et risque d'entraîner une fuite de données si un utilisateur ayant peu de privilèges se voit accorder l'accès via l'ACL.
Références	Explicit Roles

Activer le module d'extension de démarrage rapide de la sécurité (règles ACL) [mis à jour dans Security Center 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 .Now Platform

Ces règles permettent de démarrer rapidement la sécurisation de nombreuses tables système, simplifiant ainsi 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 obtenir une conformité de sécurité appropriée. Il fournit des ACL de base qui sécurisent les tables système au lieu de les créer manuellement pour chaque table système fournie avec la mise en service

Attribut	Description
	par défaut d'une instance. Ces ACL sont utiles lorsque l'instance nouvellement créée doit passer rapidement en production.
Valeur recommandée	Actif
Cote de risque de sécurité	8.1
Impact fonctionnel	(Moyen) L'installation de ce module d'extension sans audit des ACL existantes sur l'instance a un impact fonctionnel important. La sensibilisation et les définitions des clients sont requises avant que le rattrapage 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 pour sécuriser de nombreuses tables système afin de faciliter la mise en production rapide d'une organisation.
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 d'ACL fournies par le module d'extension, vous pouvez créer manuellement une ou plusieurs d'entre elles dans une instance existante si nécessaire. Cette liste d'ACL peut être utilisée à titre indicatif dans ce cas.

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à Activate a plugin .

Activer les règles de requête de gestion des commandes de travaux pour les organisations de services [Nouveau dans Security Center 1.5]

Utilisez la propriété pour appliquer des `sn_fsm.use_query_rules` règles et des filtres aux tables Field Service Management.

Lorsque la `sn_fsm.use_query_rules` propriété est définie sur vrai, les règles et les filtres de la table sn_query_rule seront utilisés pour déterminer l'accès en lecture aux tables Gestion des services sur site des utilisateurs authentifiés. Pour ce faire, il interroge les règles métier et les ACL en lecture. Lorsque cette propriété est définie sur faux, les enregistrements ne sont pas filtrés en fonction des règles de requête. Les règles métier de requête ajoutent des validations de sécurité supplémentaires lorsqu'elles sont activées sur cette propriété, et elles filtrent les enregistrements pour les agents, les qualificateurs et les répartiteurs en fonction de leur territoire affecté ou de leur appartenance au territoire. Cela met en œuvre le principe du moindre privilège lors de la lecture des documents.

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

Attribut	Description
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 des sn_query_rule seront utilisés pour déterminer l'accès en lecture aux tables de Gestion des services sur site en implémentant le principe du moindre privilège. Si la valeur est définie sur faux, les enregistrements ne sont pas filtrés en fonction des règles métier de requête et peuvent présenter un risque accru d'exposition des données des tables de Gestion des services sur site.
Dépendances et prérequis	Aucun
Impact fonctionnel	Quand 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. Par exemple, la commande de travaux (OF) et la table de commande de travaux (WOT) pour l'utilisateur connecté via les règles métier de requête et les 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	

Utilisation de l'opération multiple d'insertion sécurisée dans l'API de jeu d'importation

Utilisez la *com.glide.import_set_api.insert_multiple_optimize* propriété pour contrôler si *GlideRecordSecure* ou *GlideRecord* est utilisé pour l'opération Insérer plusieurs dans l'API de jeu d'importation.

Si *com.glide.import_set_api.insert_multiple_optimize* cette propriété est définie sur la valeur recommandée faux, *GlideRecordSecure* est utilisé pour insérer les 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 multiple de l'API de jeu d'importation (sys_id : 3101b770ff2211105cf343d0653bf182) est active et que les utilisateurs disposent du 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
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 en utilisant 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

Utilisez cette propriété pour appliquer la `glide.soap.strict_security` sécurité du service 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 Module d'extension Contextual Security : Role Management.

Si vous définissez cette propriété sur **true**, elle effectue les actions suivantes :

- Si l'utilisateur dispose du rôle approprié pour effectuer l'opération, il vérifie l'autorisation de rôle de la demande SOAP entrante à valider. Cela se produit lors des appels/requêtes SOAP Web Service effectués sur Now Platform des tables lors de l'exécution des opérations CRÉER, LIRE, METTRE À JOUR ou SUPPRIMER.

- Vérifie les ACL au niveau du système tout en récupérant les 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 la table.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.soap.strict_security`
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 appels SOAP
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) 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 ayant 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 Add a system property .

Instanciateurs de connexions JMS requis [Mise à jour dans Security Center 1.5]

La `mid.property.jms.command.allowed_factory_names` propriété contrôle les instanciateurs de connexions JMS (Java Messaging Service) que le MID Server peut utiliser.

Il est destiné à quelques usines sélectionnées nécessaires 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 la possibilité d'une 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'usine Java supplémentaires au-delà de la valeur par défaut de 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
Valeur par défaut	`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 MID Server (`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'usine supplémentaires au-delà de la valeur par défaut de connectionFactory, queueConnectionFactory et topicConnectionFactory sont nécessaires.
Dépendances et prérequis	Aucun

Définir l'utilisateur invité pour les demandes SOAP

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. Si elle n'est pas définie sur la valeur conseillée, ou `soap.guest`si elle est définie sur un utilisateur avec des privilèges limités, les demandes SOAP s'exécutent alors 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	savon.invité
Valeur par défaut	savon.invité

Attribut	Description
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 8,1 • Score CVSS : élevé • Détails du risque de sécurité : si vous laissez cette propriété vide, vous pouvez accéder aux opérations de niveau administrateur ou de maintenance sans authentification.
Dépendances et prérequis	Aucun

Activer l'accès à la session basé sur des règles pour Mobile [Nouveau dans Security Center 1.5]

Utilisez le module d'extension Zero Trust - Policy Based Session Access pour contrôler si les utilisateurs s'authentifiant via une application mobile verront leurs rôles réduits.

Le module d'extension Zero Trust - Policy Based Session Access permet aux administrateurs de sécurité de réduire l'accès de l'utilisateur dans une session en fonction de paramètres tels que l'adresse IP, l'emplacement, l'identification des attributs du fournisseur et les attributs de l'utilisateur avec des politiques d'authentification adaptative. Lorsque ce module d'extension est activé ou défini sur vrai, les rôles des utilisateurs s'authentifiant via un équipement mobile sont restreints en fonction des politiques du module d'extension. Les administrateurs d'instance peuvent souhaiter restreindre l'accès aux privilèges élevés lorsque les utilisateurs s'authentifient via un équipement mobile, car cela pourrait indiquer un environnement non sécurisé pour les opérations sensibles.

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 une politique 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 de confiance voient leurs rôles avec des privilèges réduits. True est le paramètre sécurisé. Si ce paramètre est configuré sur false, l'accès à la

Attribut	Description
	session basé sur une stratégie est désactivé et les utilisateurs continuent d'avoir des rôles complets, y compris les rôles hautement privilégiés comme admin 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 viennent pas d'un environnement approuvé ou s'ils n'utilisent pas d'appareil approuvé.
Références	Authentification adaptative

Activer le module d'extension du contrôle d'accès SNC

Activez le module d'extension SNC Access Control (com.snc.snc_access_control*com.snc.snc_access_control*) pour contrôler l'accès du personnel à vos instances Service et assistance client .

La configuration par défaut de permet d'accéder aux instances via un processus interne qui crée des informations d'identification Now PlatformService et assistance client de support à court terme. Bien que tous les accès soient audités, certains clients préfèrent contrôler cet accès.

Ce module d'extension Service et assistance client permet au service client et au support d'empêcher les employés d'accéder à l'instance. Cette décision a un impact sur les SLA de support, car vous devez activer Now Platform l'accès avant que les activités de support puissent commencer. Pour en savoir plus, consultez Contrôle d'accès ServiceNow.

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 et assistance client aux employés d'accéder à l'instance
Valeur recommandée	Actif
Rôle requis	L'administrateur client ne peut pas activer ce module d'extension. Elle doit faire l'objet d'une demande explicite, car l'activation du module d'extension nécessite des privilèges élevés.
Cote de risque de sécurité	8.2
Impact fonctionnel	(Faible) Si ce module d'extension est inactif, tous les Service et assistance client employés peuvent accéder à l'instance du client. L'activation du module d'extension permet au client de restreindre l'accès aux employés autorisés Service et assistance client uniquement.

Attribut	Description
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 ce module d'extension, suivez les étapes décrites dans Activation du contrôle d'accès ServiceNow. Les clients doivent demander le module d'extension SNC Access Control (com.snc.snc_access_control) auprès de HI.
2. Pour activer le contrôle d'accès SNC, procédez comme suit dans Configuration ServiceNow du contrôle d'accès. Configurez un enregistrement de contrôle d'accès pour spécifier un ou plusieurs Service et assistance client employés qui ont l'autorisation de se connecter à votre instance.

Appliquer le périmètre de sécurité pour Agent Workspace for HR Case Management [Nouveau dans Security Center 1.5]

Configurez le module d'extension Agent Workspace for HR Case Management de sorte que les données des tables maître du champ d'application ne soient accessibles qu'aux utilisateurs disposant des autorisations appropriées, conformément au principe du moindre privilège.

Lorsque le module d'extension `glide.enforce_security_scope.sn_hr_agent_ws` est configuré sur la valeur recommandée, vrai, seules les listes de contrôle d'accès (ACL) du module d'extension Agent Workspace for HR Case Management sont utilisées pour déterminer l'accès à une ressource. Lorsque ce paramètre est défini sur false, les données d'Agent Workspace for HR Case Management dans les tables maîtres du champ d'application sont exposées, car les ACL de tous les champs d'application bénéficient d'un accès.Par exemple, un administrateur informatique peut accéder aux données d'Agent Workspace for HR Case Management lorsque ce paramètre est défini sur false. Pour éviter que cela ne se produise, définissez la valeur recommandée, vrai, `glide.enforce_security_scope.sn_hr_agent_ws` qui garantit que le principe de moindre privilège existe, car les utilisateurs ne peuvent accéder qu'aux ressources pour lesquelles ils ont une 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

Attribut	Description
	• Détails du risque de sécurité : Si vous configurez ce paramètre sur false, les données d'Agent Workspace for HR Case Management dans les tables maîtres du champ d'application 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 applique des ACL globales à exécuter pour une table, si des ACL incluses dans le champ d'application n'existent pas pour elle.
Références	• https://owasp.org/www-project-proactive-controls/#div-numbering • Add a component to Agent Workspace

Appliquer le playbook de licence et d'autorisation de périmètre de sécurité [Nouveau dans Security Center 1.5]

Utilisez cette propriété pour déterminer si seules les listes de contrôle d'accès (ACL) du module d'extension License and Allow seront utilisées pour déterminer l'accès au champ d'application, ou si les ACL de tous les périmètres seront prises en compte.

Lorsque la `glide.enforce_security_scope.sn_gsm_lic_prmt` propriété est définie sur la valeur recommandée, vrai, seules les ACL du module d'extension License and Allow sont utilisées pour déterminer l'accès au champ d'application. Lorsque ce paramètre est configuré sur false, les données des playbooks de licence et d'autorisation dans les tables maîtres du champ d'application sont exposées, car l'accès est accordé aux ACL de tous les périmètres. Pour réduire l'exposition des données, définissez la `glide.enforce_security_scope.sn_gsm_lic_prmt` 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 true sécurise les données des playbooks de licence et

Attribut	Description
	d'autorisation dans les tables maîtres du champ d'application en prenant en compte uniquement les ACL du champ d'application pour accorder l'accès `sn_gsm_lic_prmt` . Si vous définissez cette valeur sur false, les données des playbooks de licence et d'autorisation sont exposées dans les tables maîtres du champ d'application en tenant compte des ACL de tous les champs d'application pour accorder l'accès. Par exemple, l'administrateur informatique peut accéder aux données des playbooks de licence et d'autorisation lorsque ce paramètre est défini sur faux.
Dépendances et prérequis	Aucun
Références	• Using License and Permit Playbook • Application scope

Empêcher les utilisateurs inactifs de se connecter [Nouveau dans Security Center 1.5]

Configurez cette propriété pour contrôler si les utilisateurs inactifs peuvent s'authentifier sur votre instance.

Si le `glide.authenticate.only.allow.active.user.login` paramètre n'est pas défini sur la valeur recommandée vrai, les utilisateurs de la table sys_user marquée comme inactive peuvent toujours se connecter à l'instance. Les utilisateurs peuvent être marqués comme inactifs s'ils n'ont plus l'autorisation de se connecter, par exemple lorsqu'ils sont révoqués d'une entreprise. Si le paramètre est configuré sur false, les utilisateurs peuvent toujours accéder à l'instance et aux données auxquelles ils avaient accès précédemment.

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
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 : Si vous ne définissez pas cette propriété sur la valeur recommandée,

Attribut	Description
	vrai, des utilisateurs inactifs, tels qu'un employé licencié, peuvent continuer d'accéder à l'instance et à toutes les données.
Dépendances et prérequis	Aucun

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

Utilisez cette 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.

- Lorsqu'elle est définie sur **vrai**, elle Now Platform valide le type de contenu comme texte/xml et protège contre les demandes SOAP invalides.
- Si la valeur est définie sur **false**, toutes les valeurs de type de contenu sont autorisées.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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
Objectif	Protégez-vous contre les demandes SOAP invalides
Valeur recommandée	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Faible) 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.

Attribut	Description
Risque de sécurité	(Modéré) Lors de l'acceptation des demandes SOAP entrantes, la validation appropriée est effectuée pour s'assurer que le type de contenu pertinent est défini dans le cadre de la demande. Elle restreint les réponses SOAP invalides qui peuvent être considérées comme un risque pour la sécurité.
Référence	Types de contenus

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger une autorisation pour les demandes PDF [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.pdf` demandes PDF entrantes doivent requérir une authentification de base.

En savoir plus

Avertissement :
Il s'agit d'une propriété d'exonération, 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 sur les demandes PDF.
Valeur recommandée	VRAI
Cote de risque de sécurité	7.5
Impact fonctionnel	(Faible) 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 .

Attribut	Description
Risque de sécurité	(Élevé) Sans autorisation appropriée 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 Add a system property .

Exiger l'authentification sur le processeur HTTP Event Management [nouveau dans Security Center 1.3]

Découvrez comment établir une authentification de base sécurisée pour les demandes Amazon Simple Notification Service (SNS) entrantes lorsque le module d'extension Event Management (`com.glideapp.itom.snac`) est activé.

Si la `glide.basicauth.required.evtmgmthttpprocessor` propriété n'est pas définie sur la valeur recommandée **, vrai et** que le module d'extension Event Management (`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 corriger ce risque de sécurité, assurez-vous que `glide.basicauth.required.evtmgmthttpprocessor` cette option est définie sur**true** et active `com.glideapp.itom.snac` .

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
Valeur par défaut	VRAI
Catégorie	API et service web
Risque de sécurité	• Score de gravité : 7 • Score CVSS : élevé • Détails du risque de sécurité : La non-définition`glide.basicauth.required.evtmgmthttpprocessor` de la valeur recommandée, vrai, et la non-activation du module d'extension entraînent la non-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

Attribut	Description
Références	• https://docs.aws.amazon.com/sns/latest/dg/welcome.html • Access control
Impact fonctionnel	Si `glide.basicauth.required.evtmgmthttpprocessor` cette propriété n'est pas définie sur la valeur conseillée, Vrai, et si le module d'extension Event Management (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 Security Center 1.5]

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 d'exonération, 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.soap`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour faire respecter l'autorisation des demandes SOAP.
Valeur recommandée	VRAI
Cote de risque de sécurité	8.1
Impact fonctionnel	(Moyen) 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 SOAP sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. • Créez un compte pour un utilisateur qui a besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, consultez Informations d'identification d'authentification SOAP Web Service et MID Server et demandes SOAP.

Attribut	Description
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les demandes SOAP de source de données, un utilisateur non autorisé peut accéder à du contenu/des 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 Add a system property .

Exiger une autorisation pour les demandes de déchargement [Mise à jour dans Security Center 1.3]

Utilisez la propriété (useUnloadFormat) pour indiquer si les `glide.basicauth.required.unl` demandes de déchargement entrantes doivent requérir 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 sur les demandes de déchargement.
Valeur recommandée	VRAI
Cote de risque de sécurité	7.5
Impact fonctionnel	(Moyen) 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.
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 qu'il existe dans le sys_properties_table et qu'il `glide.basicauth.required.unl` est défini sur vrai.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger une autorisation pour les demandes CSV [Mise à jour dans Security Center 1.3]

Utilisez cette `glide.basicauth.required.csv` propriété pour indiquer si les demandes CSV (valeurs séparées par des virgules) entrantes doivent faire l'objet d'une authentification de base.

En savoir plus

> **⚠ Avertissement :**
> Il s'agit d'une propriété d'exonération, 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 sur les demandes CSV.
Valeur recommandée	VRAI
Cote de risque de sécurité	7.5
Impact fonctionnel	(Faible) 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, reportez-vous à la section Récupération de données à partir 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. 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

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger une autorisation pour les demandes Excel [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.excel` demandes Excel entrantes doivent requérir une authentification de base.

En savoir plus

> **⚠ Avertissement :**
> Il s'agit d'une propriété d'exonération, 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 sur les demandes Excel.
Valeur recommandée	VRAI
Cote de risque de sécurité	7.5
Impact fonctionnel	(Faible) 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 Add a system property .

Exiger une autorisation pour les demandes d'importation [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.importprocessor` demandes d'importation entrantes doivent requérir une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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 sur les demandes d'importation.
Valeur recommandée	VRAI

Attribut	Description
Cote de risque de sécurité	5.3
Impact fonctionnel	(Faible) 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 d'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, reportez-vous à la section Récupération de données à partir d'un fichier au format CSV .
Risque de sécurité	(Modéré) Sans autorisation appropriée configurée sur les demandes d'importation de sources 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 Service SOAP

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger une autorisation pour la demande JSONv2 [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.jsonv2` demandes JSONv2 entrantes doivent obtenir une autorisation de base.

En savoir plus

Avertissement :
Il s'agit d'une propriété d'exonération, 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.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

Traduction automatique

Attribut	Description
Impact fonctionnel	(Moyen) 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 JSON sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. • Créez un compte pour un utilisateur qui a besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, consultez JSONv2 Web Service Web JSONv2 .
Risque de sécurité	(Élevé) Sans 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 Exiger une authentification de base pour les demandes JSONv2 entrantes

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger une autorisation pour la demande WSDL [mis à jour dans Security Center 1.3]

Utilisez cette `glide.basicauth.required.wsdl` propriété pour indiquer si les demandes WSDL (Web Services Description Language) entrantes doivent requérir une authentification de base.

Remarque :
Si vous choisissez de ne pas exiger l'authentification de base pour les demandes WSDL entrantes, vous devez modifier les règles Access Control (ACL) pour permettre aux utilisateurs invités d'accéder au contenu WSDL.

En savoir plus

Avertissement :
Il s'agit d'une propriété d'exonération, 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

Attribut	Description
Objectif	Pour appliquer l'authentification de base sur les demandes WSDL.
Valeur recommandée	VRAI
Cote de risque de sécurité	4.3
Impact fonctionnel	(Faible) 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 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 au contenu/aux données WSDL sensibles sur l'instance cible.
Références	Sécurité des services Web

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger une autorisation pour les demandes XML

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.xml` demandes XML entrantes doivent requérir une authentification de base.

En savoir plus

Avertissement :
Il s'agit d'une propriété d'exonération, 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
Objectif	Pour appliquer l'authentification de base sur les demandes XML.
Cote de risque de sécurité	7.5
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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.

Attribut	Description
	• Il effectue cette authentification tout en récupérant les données des tables/pages sous la 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, reportez-vous à la section 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

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger une autorisation pour les demandes de sortie XML

Configurez cette propriété de sorte 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 recommandée, **vrai**, l'autorisation de base n'est pas requise pour les demandes XMLOutputProcessor entrantes, ce qui pourrait entraîner une divulgation d'informations non authentifiées de l'instance.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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
Catégorie	API et service web
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé

Attribut	Description
	• Détails du risque de sécurité : ne pas définir la propriété sur la valeur recommandée, **vrai** peut entraîner la fuite d'informations sensibles de l'instance.
Dépendances et prérequis	Aucun

Exiger une autorisation pour les demandes XSD

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.xsd` demandes XSD (XML Schema Definition) entrantes doivent requérir une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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 sur les demandes XSD.
Valeur recommandée	VRAI
Cote de risque de sécurité	5.3
Impact fonctionnel	(Faible) 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 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, reportez-vous à la section Sessions non interactives.
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

Utilisez la propriété pour indiquer si les `glide.basicauth.required.scriptedprocessor` demandes de script entrantes doivent requérir une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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 sur les demandes de scripts.
Valeur recommandée	VRAI
Cote de risque de sécurité	7.2
Impact fonctionnel	(Moyen) Ce rattrapage applique 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 Add a system property .

Exiger une autorisation pour les demandes SCHEMA [mis à jour dans Security Center 1.3]

Utilisez cette propriété pour exiger une `glide.basicauth.required.schema` autorisation de base pour toutes les demandes du processeur de schéma de table entrante.

Le processeur Schebma pour la table entrante gère les demandes de schéma entrantes pour la plateforme.

Définissez la valeur recommandée, **vrai**, `glide.basicauth.required.schema` pour exiger une 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 d'exonération, 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 entrantes du processeur de schéma de table.
Valeur recommandée	True (valeur par défaut).
Type de configuration	Booléen
Risque de sécurité	(Modéré) Omettre l'authentification à partir de ce processeur entraîne un accès non authentifié aux données d'instance.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger une autorisation pour les demandes RSS [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.rss` demandes RSS entrantes doivent requérir une authentification de base.

En savoir plus

> **⚠ Avertissement :**
> Il s'agit d'une propriété d'exonération, 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 sur les demandes RSS.
Valeur recommandée	VRAI
Cote de risque de sécurité	7.5
Impact fonctionnel	(Faible) 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.

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, consultez Générateur de flux RSS .
Risque de sécurité	(Élevé) Sans autorisation appropriée 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

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger une autorisation pour les demandes d'API [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour améliorer la `glide.basicauth.required.api` sécurité de l'autorisation de base pour les demandes REST entrantes.

Définissez la propriété sur **true** pour exiger une `glide.basicauth.required.api` 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 d'exonération, 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	Vrai (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

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger une autorisation pour les demandes de déchargement

Utilisez la propriété (useUnloadFormat) pour indiquer si les `glide.basicauth.required.unl` demandes de déchargement entrantes doivent requérir 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 sur les demandes de déchargement.
Valeur recommandée	VRAI
Cote de risque de sécurité	7.5
Impact fonctionnel	(Moyen) 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.
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.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Architecture, conception et modélisation des menaces

Ce contrôle étendu prend en compte les considérations de conception de haut niveau et les éléments clés pour implémenter une application sécurisée. Cela couvre les locataires de la disponibilité, de l'intégrité du traitement de la confidentialité, de la non-répudiation et de la vie privée. De plus, des éléments d'un cycle de vie de développement logiciel sécurisé sont inclus.

Authentification basée sur certificat non mise en application

La `glide.authenticate.mutual.enabled` propriété active l'authentification basée sur certificat, un type d'authentification mutuelle pour les connexions REST entrantes aux API REST et SOAP dans le Now 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 source fiable se connecte au Now

Platformfichier . Si cette instance n'est pas définie sur la valeur recommandée, true, elle peut être vulnérable aux attaques de l'homme du milieu (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 Now Platform, suivez les Configurer l'authentification basée sur certificat instructions. En outre, assurez-vous que la *glide.authenticate.mutual.enabled* propriété est définie sur true 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 avec 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
Références	• https://csrc.nist.gov/glossary/term/man_in_the_middle_attack • Authentification basée sur certificat • Configuration de l'authentification réciproque

Vérifier l'emprunt d'identité dans l'évaluation ACL de l'application RH [Mise à jour dans Security Center 1.5]

Utilisez cette *sn_hr_core.impersonateCheck* propriété pour empêcher un utilisateur d'emprunter l'identité 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 à des données RH telles que les résultats d'enquêtes ou les enregistrements d'audit avec l'accès de l'utilisateur dont l'identité a été usurpée. 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 le courrier électronique, cela n'est pas recommandé. Définir *sn_hr_core.impersonateCheck* la valeur sur vrai n'autorise l'accès aux informations RH que lorsque l'utilisateur n'emprunte pas l'identité d'autrui.

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 à des données RH telles que les résultats d'enquêtes ou les enregistrements d'audit avec l'accès de l'utilisateur dont l'identité a été usurpée.
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque cette propriété est définie sur true, elle empêche un administrateur de voir les informations RH d'un autre utilisateur lorsqu'il utilise l'emprunt d'identité. Lorsqu'elle est définie 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'enquêtes 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 accessibles qu'à l'utilisateur lui-même, comme un e-mail, cela n'est pas recommandé. Définir sn_hr_core.impersonateCheck sur vrai n'autorise l'accès aux informations RH que si l'utilisateur n'emprunte l'identité d'aucune autre personne.

Désactiver les rapports publiés non authentifiés

Désactivez cette propriété pour empêcher l'utilisateur de publier des rapports ou d'y accéder. Cette propriété désactive la fonctionnalité des rapports publiés dans la génération de rapports.

Activez la publication des rapports en définissant la *glide.report.published_reports.enabled* sur **vrai**.

Appliquer la sécurité sur les rapports est conforme si `glide.report.published_reports.enabled` est défini sur **faux**.

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	(Moyen) 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 ou de publier des rapports exposant des données sensibles. La publication d'un rapport crée une URL que tout le monde, y compris les personnes qui ne sont pas des utilisateurs, peut utiliser pour y accéder. Lorsque quelqu'un accède à 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 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 `glide.report.report_view.check_published` propriété pour vérifier la façon dont 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 et 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.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.report.report_view.check_published`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI

Attribut	Description
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, ce qui peut 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 de lecture sont appliquées sur votre instance.

Utilisez cette `glide.report.report_view.read_acl` propriété pour appliquer l'ACL de lecture (niveau de table) aux fonctions de génération de rapports lorsqu'il n'y a pas d'ACL de vue de rapport sur la table ou le champ. Si cette propriété **n'est** pas définie pour être appliquée, les ACL peuvent être contournées, ce qui entraîne 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 : Si vous ne définissez pas cette propriété comme **appliquée** , vous risquez d'éviter le contournement des ACL.
Dépendances et prérequis	Aucun

Définir les adresses IP internes autorisées ServiceNow [Mise à jour dans Security Center 1.5]

Utilisez cette `glide.ip.authenticate.strict` propriété pour spécifier les plages IP qui peuvent établir des connexions entrantes sur une instance.

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 sur une instance. Cette propriété contient une liste de plages IP internes ServiceNow essentielles uniquement (VPN sécurisé, DC).

Si *glide.ip.authenticate.allow.secured* elle n'est pas définie sur la valeur recommandée « 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 », elle peut permettre à des sources non approuvées en dehors du centre de données ServiceNow et du VPN sécurisé d'accéder aux points de terminaison de surveillance sensibles sur les instances.

Avertissement :
La valeur de cette propriété est aucun remplacement de 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 par le biais d'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). **Remarque :** Si vous définissez cette propriété sur vrai, une propriété plus restrictive *glide.ip.authenticate.allow.secured* est utilisée Now Platform au lieu de 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

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Remarque :
Une règle de refus de tout doit être ajoutée au contrôle d'accès IP pour restreindre l'accès à partir de n'importe quelle adresse IP qui n'est pas 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 [Mise à jour dans Security Center 1.3]

L'application est utilisée pour empêcher l'utilisation `glide.jquery.legacy` d'anciennes versions de JQuery prédéfinies, ce qui introduirait des vulnérabilités non corrigées dans la bibliothèque.

Défini sur `glide.jquery.legacy` la valeur **recommandée false pour** empêcher l'utilisation d'anciennes versions JQuery prédéfinies qui introduisent des vulnérabilités non corrigées dans la bibliothèque. Définissez la valeur sur **true** 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 Add a system property .

Activer le comportement hérité de clôture du champ d'application GlideRecord [Nouveau dans Security Center 1.3]

La `glide.record.legacy_cross_scope_access_policy_in_script` propriété désactive la clôture du champ d'application, ce qui permet aux applications incluses dans le périmètre d'accéder aux interfaces de script globales. Il a été créé en tant que correctif pour l'accès entre champs d'application de GlideRecord.

GlideRecord fournit un accès à la création et à la mise à jour entre champs d'application aux 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 a été corrigé, la `glide.record.legacy_cross_scope_access_policy_in_script` propriété a été créée. Lorsque cette propriété est définie sur true, l'accès entre champs d'application revient au comportement hérité, qui n'est pas sécurisé.

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
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 avoir des répercussions sur la confidentialité, la disponibilité et l'intégrité.
Dépendances et prérequis	Aucun

Désactiver le comportement AngularJS hérité [Mise à jour dans Security Center 1.3]

Utilisez cette 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.

Définir `glide.angular.legacy` sur la valeur **recommandée false pour** empêcher l'utilisation d'anciennes versions AngularJS prédéfinies. Définissez la propriété sur **true** 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

Attribut	Description
Risque de sécurité	(Élevé) L'utilisation d'anciennes versions d'AngularJS peut entraîner des risques de sécurité découlant des attaques sur les vulnérabilités détectées dans les versions de bibliothèque AngularJS obsolètes.
Cote de risque de sécurité	7.1

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Accès public aux favoris

Utilisez le `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 sera conforme si `glide.ui.magellan.favorites.allow_public` défini 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
Objectif	Contrôlez si les utilisateurs non authentifiés sont autorisés à voir **les favoris** dans le navigateur.
Type	vrai/faux
Valeur recommandée	`false`
Dépendances de Security	Définir 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 aux données sensibles.
Références	Créer ou afficher des favoris

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger une autorisation pour l'API REST du courtier en données [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour exiger une `glide.basicauth.required.databrokerrestapiprocessor` autorisation de base pour toutes les demandes d'API REST du courtier de données entrantes.

Si cette propriété est définie sur **vrai**, l'autorisation est appliquée. Si elle est définie sur **false**, aucune autorisation n'est utilisée, ce qui peut entraîner la fuite d'informations sensibles à partir de votre instance.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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)
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 à des données sensibles.
Dépendances et prérequis	Aucun

Refuser par défaut en cas d'ACL vides

Utilisez cette `glide.sm.default_mode` propriété pour contrôler le comportement par défaut du gestionnaire de sécurité lorsqu'il détecte que des règles ACL font partie des règles ACL d'une table à caractère générique.

Lorsque le module d'extension Paramètres de sécurité élevée (com.glide.high_security) est activé lors de l'installation initiale de l'instance, il crée cette propriété, et des règles ACL génériques sont créées. Pour fournir un accès basé sur les rôles aux tables système, ces règles contrôlent un nombre important d'ACL et les opérations basées sur les enregistrements les plus courantes :

- Lecture
- Écriture
- Créer
- Supprimer

À moins que vous n'utilisiez le module d'extension High Security avec l'option de refus par défaut activée, de nombreuses tables ne sont pas protégées. Le utilise Now Platform un modèle de sécurité de refus par défaut qui empêche les utilisateurs non administrateurs d'accéder aux objets à moins qu'ils ne répondent à une règle ACL correspondante. À

l'aide de ce modèle, il supprime de nombreux vecteurs d'attaque, tels que les scripts non sécurisés.

Avertissement :
Il s'agit d'une propriété d'exonération, 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 en matière de sécurité consiste à restreindre l'accès aux tables par un utilisateur non autorisé. • Si aucune règle d'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 toutes les tables, sauf si l'utilisateur dispose du rôle d'administrateur ou répond aux exigences d'une autre règle ACL de table.
Valeur recommandée	refuser
Impact fonctionnel	(Élevé) Si vous définissez cette propriété sur **Autoriser**, les règles ACL de 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 sécurisé aux tables déjà utilisées dans un environnement de production.
Risque de sécurité	8.8
Références	Propriété de refus par défaut

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Authentification

La catégorie d'authentification couvre les principaux éléments de l'authentification moderne pour confirmer qu'une entité et ses revendications sont authentiques et correctes, résistent 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, l'implémentation appropriée des authentificateurs et l'implémentation appropriée des vérificateurs hors bande ou à usage unique.

Activer l'authentification multifacteur basée sur les rôles

Utilisez cette propriété pour appliquer l'authentification multifacteur basée sur les `glide.authenticate.multifactor` rôles (MFA) à tous les utilisateurs affectés à des rôles spécifiques.

appliquer l'authentification multifacteur en fonction des rôles affectés à l'utilisateur. Si les rôles « administrateur », « security_admin » ou « user_admin » de la liste des rôles multifacteur ont été affectés à un utilisateur, 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.
- Définissez cette propriété sur **faux** pour désactiver l'authentification multifacteur basée sur les rôles 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	vrai/faux
Valeur recommandée	`true`
Dépendances de Security	**Activez l'authentification multifacteur basée sur les rôles** dans la **table Critères multifacteur**.
Cote de risque de sécurité	7.2
Impact fonctionnel	(Moyen) 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 aux données sensibles.
Références	Configurer des critères multifacteur basés sur les rôles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Activer la récupération de compte [Mise à jour dans Security Center 1.5]

Cette *glide.sso.acr.enabled* propriété contrôle la fonctionnalité de récupération de compte.

Défini sur *glide.sso.acr.enabled* la valeur **recommandée vrai pour** permettre la récupération du compte par ID d'utilisateur possible. Définissez la valeur sur **faux** pour interdire la récupération de compte par ID d'utilisateur.

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 du compte par fonctionnalité d'ID d'utilisateur.
Valeur recommandée	Vrai (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	Pour plus d'informations, consultez Récupération de compte (ACR).

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger le brouillage de l'interface utilisateur de l'application mobile classique

Utilisez cette *glide.ui.m.blur_ui_when_backgrounded* propriété pour masquer tous les champs de la capture instantanée lors de l'enregistrement de l'image pendant le processus d'arrière-plan.

Sur les appareils Android, le système d'exploitation Android effectue 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 effectuer des captures d'écran manuelles de l'application, qui sont stockées publiquement sur l'appareil.

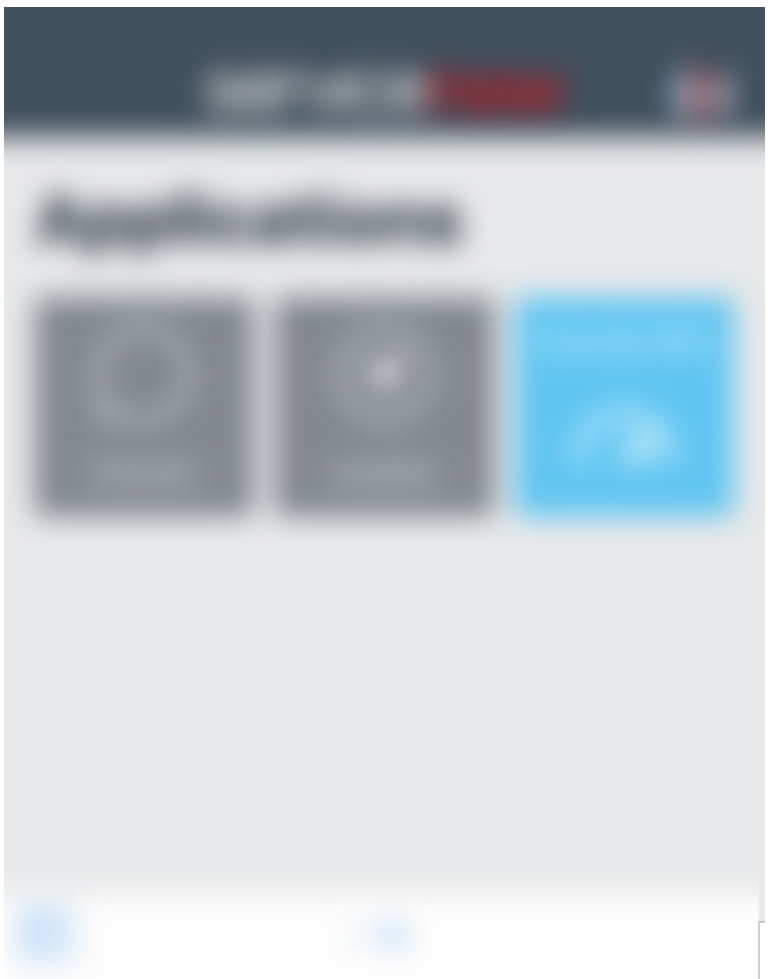
Sur les appareils iOS, le système d'exploitation iOS permet également aux applications d'enregistrer un fichier image. Ce fichier représente le dernier écran vu par l'utilisateur lorsque l'application est envoyée en arrière-plan. Bien que l'objectif soit de fournir une meilleure expérience utilisateur, cela crée également un risque de sécurité, car les images sont enregistrées en tant que fichiers image PNG.

Remarque :
Ce paramètre ou cette configuration est basé sur chaque instance, l'utilisateur doit donc se connecter à l'instance avec la propriété configurée.

Pour brouiller tous les champs de l'instantané dans l'application ServiceNow Classic, consultez Configurer l'option de floutage de l'application pour améliorer la sécurité .

Exemple

Lorsque vous définissez cette propriété sur true, l'application background est masquée pour les appareils iOS et noircie pour les appareils iOS Android.



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	(Faible) Si la *glide.ui.m.blur_ui_when_backgrounded* propriété est définie sur vrai, les applications natives utilisent le paramètre défini sur le serveur pour flouter l'écran lorsque l'application passe en arrière-plan.

Attribut	Description
	• Il floute 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 serait 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 un 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 Add a system property .

Désactiver l'authentification sans mot de passe

Utilisez cette `glide.login.no_blank_password` propriété pour empêcher les utilisateurs de se connecter à la Now Platform avec des mots de passe vierges 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 car les noms d'utilisateur sont parfois faciles à deviner au sein d'une organisation.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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 peut se connecter à l'instance avec les noms d'utilisateur par défaut, ou par personne/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.

Ne pas appliquer la politique de mot de passe lors de la connexion

Gérez la complexité des mots de passe dans votre instance.

Utilisez cette`glide.apply.password_policy.on_login` propriété pour gérer la complexité des mots de passe. Si cette propriété est définie sur **faux**, il n'y a pas d'application de la complexité du mot de passe lors de la connexion. Si la valeur est définie sur **true**, elle applique une complexité de mot de passe susceptible d'entraîner des problèmes de conformité à la politique de l'organisation. Au lieu d'appliquer la complexité du mot de passe, la norme de vérification de la sécurité des applications (ASVS) suggère d'appliquer une longueur minimale de 12 caractères pour la longueur du mot de passe.

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** pourrait appliquer la complexité du mot de passe et entraîner des problèmes de conformité de l'organisation.
Dépendances et prérequis	Aucun

Activer le contrôle de validation des mots de passe sur liste noire

Gérez les mots de passe sur liste noire dans la table Mot de passe exclu.

Utilisez cette propriété pour surveiller les `glide.enable.blacklist_password` mots de passe sur liste noire. Lorsque la propriété est définie sur **Vrai**, le mot de passe de l'utilisateur est vérifié par rapport à une liste de mots de passe sur liste noire, ce qui l'empêche 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

Attribut	Description
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Authentification
Dépendances et prérequis	Aucun
Références	Exclure les mots de passe via des politiques de mot de passe sur votre instance

Activer le captcha pour l'enregistrement des utilisateurs externes [Mise à jour dans Security Center 1.5]

Contrôle *sn_ext_usr_reg.captchaEnabled* si le CAPTCHA sera validé pour l'enregistrement des utilisateurs externes.

Définissez la valeur **recommandée vrai pour** éviter les attaques de création automatique de compte nécessitant un CAPTCHA pour l'enregistrement des utilisateurs externes*sn_ext_usr_reg.captchaEnabled*. Définissez la valeur sur **faux** pour ne pas exiger de CAPTCHA pour l'enregistrement 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'inscription d'utilisateurs externes sur des portails tels que CSP, Community. Il est également utilisé dans les applications de magasin telles que VAM et CSM Guest Walkup pour activer/désactiver le captcha.
Valeur recommandée	Vrai
Type de configuration	Booléen
Risque de sécurité	(Faible) La propriété contrôle l'activation de CAPTCHA dans l'enregistrement des utilisateurs externes. Unideal peut entraîner une vulnérabilité de 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 Add a system property .

Activer CAPTCHA dans la réinitialisation du mot de passe

Utilisez cette propriété pour activer ou désactiver l'exigence *password_reset.captcha.ignore* d'un défi CAPTCHA lorsqu'un utilisateur réinitialise son mot de passe.

Définissez *password_reset.captcha.ignore* la valeur **recommandée faux pour** exiger un défi CAPTCHA pour qu'un utilisateur réinitialise son mot de passe. Définissez la valeur sur **true** 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 pour l'automatisation de la réinitialisation du mot de passe uniquement.

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 est utilisée pour activer ou désactiver la validation CAPTCHA pendant la réinitialisation du mot de passe.
Valeur recommandée	faux
Type de configuration	Booléen
Risque de sécurité	(Modéré) Unideal peut entraîner une vulnérabilité de 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 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 à votre instance.

Utilisez cette*glide.authenticate.multifactor.email.otp.enabled* propriété pour contrôler si un jeton d'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 le MFA. En définissant cette propriété sur **false**, le risque qu'un attaquant contourne l'authentification multifacteur 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

Attribut	Description
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	Authentification multifacteur avec e-mail

Activer les vérifications de la politique de réinitialisation du mot de passe

Utilisez la propriété **glide.enable.password_policy** pour activer les vérifications de la politique de mot de passe chaque fois qu'un utilisateur change 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.

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 d'exonération, 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.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	true (pour les mots de passe de niveau de sécurité élevé)
Cote de risque de sécurité	7.4
Impact fonctionnel	(Moyen) définir la propriété sur true 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 d'Instance Security Center :

1. Sous **Moyen**, sélectionnez **Gestion des sessions**.
2. Dans le paramètre **Activer la vérification de la stratégie de réinitialisation du mot de passe** , sélectionnez **Moyen** pour les mots de passe de complexité moyenne ou **Fort** pour les mots de passe plus robustes et plus forts. Si vous sélectionnez l'une de ces options, la propriété **glide.enable.password_policy** est définie sur true et démarre 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 SSL dans LDAP Authentication

Gérez le chiffrement des demandes d'authentification LDAP sur votre instance.

Utilisez la propriété 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 **recommandée vrai,** LDAP Authentication est susceptible de faire l'objet d'une attaque de l'intercepteur.

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.
Dépendances et prérequis	Aucun
Références	Activer SSL dans LDAP Authentication

Minimiser la durée d'expiration du lien d'inscription de l'utilisateur externe [Mise à jour dans Security Center 1.5]

Gérez le nombre de jours d'accès à un lien d'inscription.

Utilisez cette *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 détecté 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 : moyen • Score CVSS : 6,6 • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur l'entier 3, un utilisateur involontaire peut utiliser le lien d'inscription.
Dépendances et prérequis	Aucun

Gestion des échecs de tentatives de connexion

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 Now 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
Objectif	Pour appliquer une stratégie stricte pour les tentatives de connexion échouées, afin d'éviter l'attaque par force brute des informations d'identification.
Valeur recommandée	Actif
Cote de risque de sécurité	7.3
Impact fonctionnel	(Faible) Cette correction permettrait à l'administrateur de l'instance de surveiller et de signaler tout accès utilisateur

Attribut	Description
	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 intervenir 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, faites passer l'état Actif de l'action `SNC User Lockout Check with Auto Unlock` ou `SNC User Lockout Check` des scripts 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

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 Now 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	`glide.user.unlock_timeout_in_mins`
Type de configuration	Politique système > Actions des scripts
Catégorie	Authentification
Objectif	Pour appliquer une stratégie stricte pour les tentatives de connexion échouées, afin d'éviter l'attaque par force brute des informations d'identification.
Valeur recommandée	Actif
Impact fonctionnel	(Faible) 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 intervenir 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, faites passer l'état Actif de l'action *SNC User Lockout Check with Auto Unlock* ou *SNC User Lockout Check* des scripts 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.

Exiger le brouillage de l'interface utilisateur de l'application mobile

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 **recommandée vrai,** l'interface utilisateur de l'application Mobile est visible lorsqu'elle est affichée à partir du commutateur d'application. L'interface utilisateur est toujours visible même lorsque l'application est en cours d'exécution en arrière-plan, ce qui réduit le niveau de sécurité et de confidentialité pour les 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	Fichier et ressources
Risque de sécurité	• Score de gravité : 2,4 • Score CVSS : faible • Détails du risque de sécurité : la définition de la valeur sur **true** accroît le niveau 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
Références	Obfuscation de l'interface utilisateur mobile

Notifier les utilisateurs pendant le processus de réinitialisation/changement de mot de passe [supprimé dans Security Center 1.5]

Utilisez cette application pour permettre aux utilisateurs finaux de réinitialiser ou de modifier les mots de passe à l'aide d'un processus en libre-service.

Cette application permet à un utilisateur final de réinitialiser ou de modifier un mot de passe à l'aide d'un processus en libre-service. Vous pouvez également implémenter un processus qui nécessite qu'un agent du Service Desk réinitialise les mots de passe des utilisateurs finaux.

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 : si un processus de modification et/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 bloquer l'accès de cet utilisateur à son compte à son 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 informe les utilisateurs en cas de changement ou réinitialisation du mot de passe.
Dépendances et prérequis	Aucun

Supprimer les informations d'identification de la page d'accueil

Modifiez le contenu par défaut de 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 sécurité conformément aux pratiques de sécurité recommandées.

En savoir plus

Attribut	Description
Nom	*How to login*
Type de configuration	Tableau : sys_home
Catégorie	Authentification

Attribut	Description
Objectif	Pour supprimer les informations d'identification par défaut de la page d'accueil qui ont été ajoutées avec des données de démonstration.
Valeur recommandée	Faux ou nul si aucune donnée de démonstration n'a été utilisée.
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 Add a system property .

Minimiser le nombre maximal de SMS de réinitialisation du mot de passe par jour

Gérez le nombre maximal de codes SMS envoyés pour vérification par jour et 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, l'attaque par force brute du code SMS est plus facile.
Dépendances et prérequis	Aucun

Minimiser la durée d'expiration de la demande de réinitialisation du mot de passe

Cela `password_reset.request.expiry` désigne la période en minutes pendant laquelle un utilisateur doit effectuer le processus de réinitialisation du mot de passe.

Remarque :
Le paramètre de la `password_reset.request.expiry` propriété a priorité sur le paramètre de `glide.pwd_reset.onetime.token.validity`la propriété dont la valeur par défaut est 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	Définissez la valeur 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 recommandée 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
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 Add a system property .

Minimiser le nombre maximal autorisé de tentatives de demande de réinitialisation du mot de passe

La est `password_reset.request.max_attempt` utilisée pour contrôler le nombre maximal de tentatives infructueuses de réinitialisation ou de modification du mot de passe d'un utilisateur avant d'être bloqué 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 avoir

Attribut	Description
	lieu avant que le processus de réinitialisation du mot de passe de l'utilisateur ne soit verrouillé. La période de verrouillage est déterminée par la valeur de *password_reset.request.max_attempt_window*.
Valeur recommandée	Défini 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 de nombres entiers positifs
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur recommandée de « **3** » ou sur une autre valeur faible raisonnable, une attaque par force brute contre le processus de réinitialisation du mot de passe peut se produire.
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 Add a system property .

Minimiser la durée de la fenêtre de tentatives maximales de demande de réinitialisation du mot de passe

La *password_reset.request.max_attempt_window* propriété contrôle le nombre de minutes pendant lesquelles un utilisateur doit attendre pour réinitialiser ou changer son mot de passe après avoir dépassé le nombre maximal de tentatives infructueuses défini avec la *password_reset.request.max_attempt* propriété.

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 que le nombre maximal de tentatives infructueuses de réinitialisation du mot de passe a été atteint.
Valeur recommandée	Défini sur une valeur entière positive de **1 440** ou moins. La valeur par défaut est **de 1 440** minutes.
Type de configuration	Valeurs de nombres entiers positifs
Impact fonctionnel	
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 attaque par force brute du compte, car le compte n'est pas verrouillé après un nombre maximum de tentatives d'authentification incorrectes.
Cote de risque de sécurité	7.5

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 Add a system property .

Maximiser la durée de la fenêtre de nouvelle tentative de demande de réinitialisation du mot de passe

Cette *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 le délai en minutes avant que le nombre de tentatives d'utilisation d'un 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 de **1 440** ou plus. La valeur par défaut est **de 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, un processus de réinitialisation du mot de passe par force brute du compte peut se produire.
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 Add a system property .

Minimiser la durée de la fenêtre de succès des demandes de réinitialisation du mot de passe

Cette *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 une réinitialisation réussie du mot de passe. L'utilisateur ne pourra pas réinitialiser 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)

Attribut	Description
Catégorie	Authentification
Objectif	Il désigne la période en minutes pendant laquelle un utilisateur doit patienter après avoir réinitialisé le mot de passe pour le réinitialiser à nouveau.
Valeur recommandée	Défini sur une valeur entière positive de **1 440** ou moins. La valeur par défaut est **de 1 440** minutes.
Type de configuration	Valeurs de nombres entiers positifs
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 de mot de passe pour obtenir un accès non autorisé à un compte d'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 Add a system property .

Maximiser la durée de la fenêtre de déverrouillage de demande de réinitialisation du mot de passe

Cette `password_reset.request.unlock_window` propriété contrôle le nombre de minutes pendant lesquelles un utilisateur doit attendre pour lancer une demande de réinitialisation après la dernière action de déverrouillage de compte réussie.

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
Objectif	Il désigne la période en minutes pendant laquelle un utilisateur doit patienter après avoir réinitialisé le mot de passe pour le réinitialiser à nouveau.
Valeur recommandée	Défini sur une valeur entière positive de **1 440** ou plus. La valeur par défaut est **de 1 440** minutes.
Type de configuration	Valeurs de nombres entiers positifs
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur recommandée de 1 440 ou supérieure, cela augmente la possibilité pour un acteur malveillant d'accéder par force brute au 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 Add a system property .

Maximiser la complexité du SMS de réinitialisation du mot de passe

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	Définissez la valeur sur un nombre entier supérieur ou égal à **4** . La valeur par défaut est 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 du compte.
Cote de risque de sécurité	3.8

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Minimiser la durée d'expiration du SMS de réinitialisation du mot de passe

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.

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

Attribut	Description
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

Maximiser la durée de la fenêtre de pause du SMS de réinitialisation du mot de passe

Gérez la durée en minutes pendant laquelle un utilisateur doit attendre avant de pouvoir demander un nouveau code de réinitialisation de 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 des mots de passe dans un bref laps de temps. Cela augmente les chances qu'un acteur malveillant prédise le code de réinitialisation du 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* cette valeur est de 2 ou plus.
Dépendances et prérequis	Aucun

Maximiser la durée du délai de vérification de la réinitialisation du mot de passe

Configurez le délai, en millisecondes, qu'un utilisateur doit attendre avant de soumettre une nouvelle demande de réinitialisation de mot de passe.

Un acteur malveillant pourrait tenter de forcer les identifiants de connexion en utilisant des outils d'automatisation tels que des bots, contre lesquels la propriété de **délai de vérification du mot de passe de réinitialisation** 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)
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 de contrainte SAML notBefore ou notOnOrAfter [Mise à jour dans Security Center 1.5]

Configurez cette propriété pour ajouter une période de grâce au cours de laquelle les demandes et les réponses SAML sont considérées comme valides.

Cette propriété ajoute une période de grâce au cours de laquelle les demandes et les réponses SAML sont considérées comme valides. La valeur de la propriété représente le nombre de secondes à ajouter aux `NotBefore` contraintes et `NotOnOrAfter` pour tenir compte des différences de temps entre l'horloge du fournisseur d'identité (IdP) et celle du fournisseur de service (SP). Ces contraintes permettent de se défendre contre les attaques par rejeu en refusant les demandes qui ne sont pas effectuées dans les délais spécifiés. Si les horloges IdP et SP sont significativement 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)

Attribut	Description
Type de données	chaîne
Valeur recommandée	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 valeur de la propriété sur 60 ou plus peut empêcher les contraintes de se défendre contre les attaques par rejeu.
Dépendances et prérequis	Aucun

Désactiver la création d'utilisateurs à partir d'e-mails entrants [Mise à jour dans Security Center 1.3]

Utilisez cette `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 des 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.user.trusted_domain`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Valeur recommandée	Liste des domaines de confiance séparés par des virgules [par exemple, servicenow.com (un nom de domaine spécifique)].
Cote de risque de sécurité	7.4
Impact fonctionnel	(Moyen) 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 plus inutiles.

Attribut	Description
Références	Configuration des messages entrants

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Activer l'authentification multifacteur basée sur les rôles [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour appliquer l'authentification multifacteur basée sur les `glide.authenticate.multifactor` rôles (MFA) à tous les utilisateurs affectés à des rôles spécifiques.

appliquer l'authentification multifacteur en fonction des rôles affectés à l'utilisateur. Si les rôles « administrateur », « security_admin » ou « user_admin » de la liste des rôles multifacteur ont été affectés à un utilisateur, 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.
- Définissez cette propriété sur **faux** pour désactiver l'authentification multifacteur basée sur les rôles 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	vrai/faux
Valeur recommandée	`true`
Dépendances de Security	**Activez l'authentification multifacteur basée sur les rôles** dans la **table Critères multifacteur**.
Cote de risque de sécurité	7.2
Impact fonctionnel	(Moyen) 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 aux données sensibles.
Références	Configurer des critères multifacteur basés sur les rôles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Définir la longueur minimale du mot de passe

Définissez la longueur minimale d'un mot de passe utilisateur sur votre instance.

Cette`set.password.length` propriété définit la longueur minimale requise pour un mot de passe et est utilisée pour évaluer la conformité par rapport à la politique de mot de passe actuelle. La valeur de la propriété est un nombre entier avec une valeur minimale recommandée de **12**. L'utilisation d'une longueur plus courte pourrait entraîner un non-respect de la réglementation recommandée.

En savoir plus

Attribut	Description
Nom de la configuration	`set.password.length`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	12
Valeur par défaut	12
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 5,9 • Score CVSS : moyen • Détails du risque de sécurité : définir la propriété sur une valeur inférieure à 12 peut entraîner des problèmes de conformité et augmenter le risque qu'une personne malveillante réussisse à forcer des mots de passe par force brute.
Dépendances et prérequis	Aucun

Définir la durée de vie de l'OTP pour la réinitialisation du mot de passe à 12 heures ou moins

Contrôlez la durée du lien dans l'e-mail de réinitialisation du mot de passe.

Cette propriété fait expirer le lien dans l'e-mail de réinitialisation du mot de passe une fois le nombre d'heures spécifié dans la propriété passé. 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.

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	12

Attribut	Description
Valeur par défaut	12
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 5,6 • Score CVSS : moyen • Détails sur les risques de sécurité : une longue période de validité du jeton de réinitialisation du mot de passe augmente le risque qu'un acteur malveillant prenne le contrôle d'un compte.
Dépendances et prérequis	Aucun

Minimiser la durée de vie unique du vérificateur hors bande [Mise à jour dans Security Center 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, réinitialisation d'un jeton multifacteur. Si cette méthode est activée par les administrateurs dans le module d'extension Authentification multifacteur (MFA) , un code à usage unique est envoyé par e-mail. Définissez les vérificateurs hors bande uniques pour qu'ils expirent après 10 minutes afin de 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 • Détails du risque de sécurité : configurez les vérificateurs hors bande à usage unique 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 mauvais acteur.
Dépendances et prérequis	Authentification multifacteur (MFA)
Références	Activer le module d'extension MFA

Appliquer les exigences en matière de chiffrement des appareils et de code d'accès [Nouveau dans Security Center 1.3]

La *glide.sg.device_encryption_enabled* propriété applique le chiffrement FIPS 140-2 (Federal Information Processing Standard). 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 l'appareil est physiquement en sa possession.

Quand *glide.sg.device_encryption_enabled* défini 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.

Exiger une autorisation pour les demandes de sortie XML [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour indiquer si les *glide.basicauth.required.xml* demandes XML entrantes doivent requérir une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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
Objectif	Pour appliquer l'authentification de base sur les demandes XML.
Cote de risque de sécurité	7.5
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) 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 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, reportez-vous à la section 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 et à des données sensibles sur l'instance cible. Vérifiez qu'il `glide.basicauth.required.xml` existe dans la table sys_properties et qu'il est défini sur vrai.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger un captcha pour l'expérience de visite d'un invité dans l'application Customer Service [Mise à jour dans Security Center 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

Attribut	Description
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 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 true.

Activer la notification du code SMS pour l'inscription et la vérification

Cette`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 réinitialiser son 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)
Type de données	Boénoël
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 : définir cette propriété sur**faux** fait de l'e-mail la méthode par défaut de récupération de mot de passe, qui est moins sécurisée que les SMS.
Dépendances et prérequis	Aucun

Logique métier

Cette catégorie examine la logique et le flux propres à chaque application avec les 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 de privilèges existent.

Voici quelques contrôles de sécurité qu'un administrateur peut configurer pour restreindre l'accès non autorisé à des entités sensibles au sein de Now Platform.

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 qui pourrait 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 : si vous ne définissez pas la valeur recommandée de cette propriété sur 500 ou moins, aucune limite n'est imposée pour les commentaires QA par jour, ce qui pourrait entraîner l'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 en une journée.

Si cette propriété n'est pas définie sur la valeur recommandée de **500** ou moins, il n'y a aucune restriction quant au nombre maximal de questions et réponses auxquelles un utilisateur peut s'abonner par jour. Cette absence de limitation peut 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
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 [Mise à jour dans Security Center 1.3]

La `glide.email.smtp.max_recipients` spécifie le nombre maximal de destinataires que l'instance peut répertorier dans la ligne **À :** pour une notification par e-mail unique.

Définissez cette valeur `glide.email.smtp.max_recipients` sur la valeur conseillée 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 maximal 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	Définir sur un nombre entier inférieur ou égal à 100. La valeur par défaut est 100.
Type de configuration	Entier
Impact fonctionnel	

Attribut	Description
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 Add a system property .

Valider l'hôte distant

Définissez la propriété sur true pour empêcher les personnes malveillantes d'utiliser l'analyse des ports internes dans votre réseau.

Si la `glide.update_set.remote.check_host` propriété n'est pas définie sur la valeur **recommandée vrai,** la fonctionnalité de test d'instance distante autorise l'analyse Team Development interne des ports, une méthode que les personnes malveillantes peuvent utiliser pour détecter 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, ce qui pourrait entraîner une fuite d'informations ou un accès non autorisé aux données.

Avertissement :
Il s'agit d'une propriété d'exonération, 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)
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 : Si vous ne définissez pas la propriété sur la valeur recommandée, **vrai** , des personnes malveillantes peuvent utiliser l'analyse interne des ports pour accéder à des données non autorisées.
Dépendances et prérequis	Aucun
Références	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0755132

Attribut	Description
	Define a remote instance

Communications

Ce contrôle garantit un cryptage 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.

Appliquer le certificat de confiance [supprimé dans Security Center 1.5]

Par défaut, cette *com.glide.communications.trustmanager_trust_all* propriété est définie sur **false**. La Now Platform seule approuve les certificats qu'elle peut vérifier par rapport au magasin de certificats JVM. Les certificats autosignés ou signés par l'entreprise ne sont pas approuvés.

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 et assistance client.

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	6.6
Impact fonctionnel	(Moyen) Cette correction applique une validation stricte sur le champ CA (autorité de certification) de certificat. 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 Vérification du nom d'hôte du client HTTP

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Désactiver les connexions SSLv2/SSLv3 sortantes [Mise à jour dans Security Center 1.3]

Utilisez cette `glide.outbound.sslv3.disabled` propriété pour forcer le MID Server à utiliser TLS en cas 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 du TLS if lors de toutes les connexions sortantes de l'instance ServiceNow.
Valeur recommandée	VRAI
Cote de risque de sécurité	6.5
Impact fonctionnel	(Moyen) 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) Il a été prouvé que les versions héritées de SSL n'étaient pas sécurisées lorsqu'elles étaient utilisées pour l'implémentation de HTTP Secure Shell, en raison d'attaques côté client, notamment BEAST et SSL.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Ne pas utiliser de certificats de démonstration pour les configurations SAML actives [Mise à jour dans Security Center 1.5]

Contrôlez si les 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, l'intégrité des demandes signées avec des certificats partagés n'offre aucune garantie. 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
Risque de sécurité	• Score de gravité : 3,9 • Score CVSS : faible
Dépendances et prérequis	Aucun

Appliquer la vérification OCSP en cas d'erreur réseau [Nouveau dans Security Center 1.3]

Découvrez comment configurer la propriété pour empêcher les `com.glide.communications.httpclient.ocsp_allow_network_error` acteurs malveillants de contourner les vérifications du protocole OCSP (Online Certificate Status Protocol).

Si elle n'est pas définie sur la valeur recommandée, faux, et que `com.glide.communications.httpclient.ocsp_allow_network_error` la vérification du protocole 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 considère qu'elle a réussi. Cela pourrait permettre à un attaquant avec un certificat révoqué de casser l'infrastructure de clé publique (PKI) et la confiance du certificat numérique qui est fondamentale pour le Web. L'utilisation de certificats révoqués est souvent un indicateur d'activité malveillante, sauf si les serveurs ne sont pas synchronisés.

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

Attribut	Description
Risque de sécurité	• Score de gravité : 5,9 • Score CVSS : moyen • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur faux, un acteur malveillant peut contourner le contrôle de sécurité OCSP.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété détermine si une demande relative à l'URI du protocole OCSP (Online Certificate Status Protocol) AIA (Authority Information Access) aboutit à une réussite ou à un échec en cas d'erreur de connexion ou de délai d'expiration. Lorsqu'il est défini 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 de 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.

Vérifier la chaîne de certificats et le nom d'hôte [Nouveau dans Security Center 1.3]

Configurez la propriété pour empêcher les *com.glide.communications.httpclient.verify_hostname* attaques de l'homme du milieu en vous assurant que le processus de vérification de certification est exécuté.

Si *com.glide.communications.httpclient.verify_hostname* la valeur n'est pas **définie sur true**, cela pourrait permettre des attaques de l'homme du milieu, dans lesquelles les communications entre deux parties sont interceptées. Définir cette propriété sur faux désactive le processus de vérification du certificat. Pour remédier à cette menace de sécurité, définissez *com.glide.communications.httpclient.verify_hostname* la valeur **sur true** pour empêcher le client HTTP de se connecter à un nom d'hôte potentiellement dangereux.

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

Attribut	Description
	• Détails du risque de sécurité : si vous ne définissez pas `com.glide.communications.httpclient.verify_hostname` votre instance sur la valeur recommandée, vous risquez de rendre votre instance vulnérable aux attaques de l'intercepteur.
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 true pour assurer la sécurité contre les attaques de l'homme du milieu (MITM). **Remarque :** Cette propriété remplace la `com.glide.communications.trustmanager_trust_al` 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 la liaison TLS (Transport Layer Security) pour s'assurer que les contrôles de sécurité ne sont pas contournés.

Si `com.glide.communications.httpclient.verify_revoked_certificate` ce champ n'est pas défini sur la valeur recommandée, **vrai**, la révocation du certificat n'est pas vérifiée pendant la connexion 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. Contourner l'établissement de liaison TLS présente un risque pour la sécurité, car un attaquant avec un certificat révoqué peut négliger de fournir un certificat valide et rompre l'infrastructure de clé publique (PKI) et la confiance du 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 : La non-définition `com.glide.communications.httpclient.verify_revoked_cert`

Attribut	Description
	de la valeur recommandée, vrai, entraîne la non-vérification de la révocation du certificat pendant la connexion 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 false, le certificat n'est pas vérifié, ce qui peut compromettre la sécurité de l'instance.

Configuration

La catégorie Configuration garantit que les applications disposent d'un environnement de génération sécurisé et de composants de bibliothèque tiers renforcés. Plus précisément, il s'agit de s'assurer qu'un pipeline de version et de déploiement est répétable et inclut des tests automatisés, et empêche le déploiement des problèmes de sécurité connus. Il s'agit notamment de maintenir les dépendances à jour et de les exempter de vulnérabilités connues.

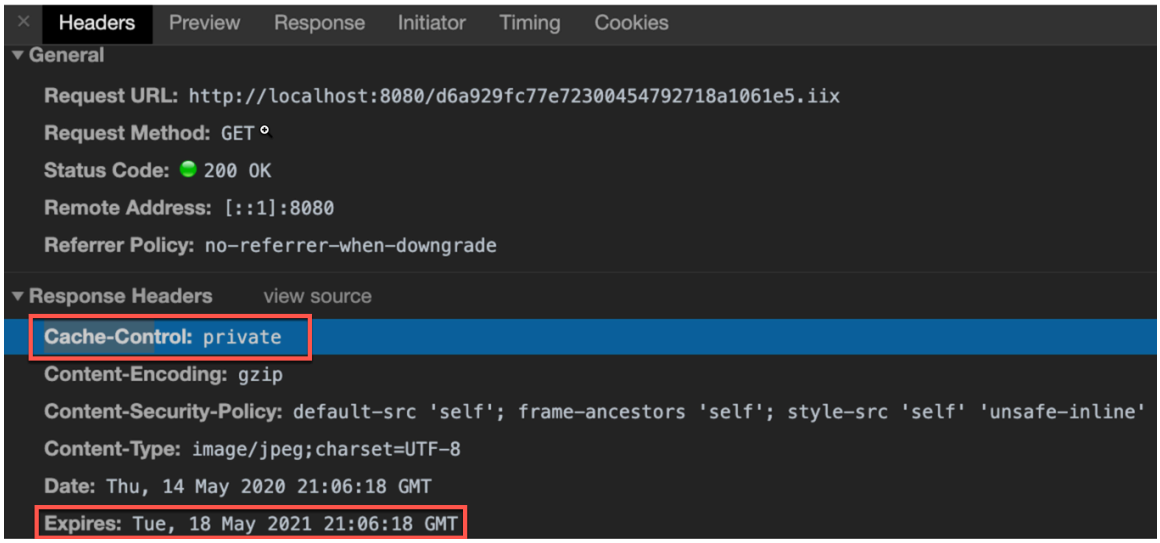
Valeur de l'en-tête HTTP du contrôle de cache [supprimé dans Security Center 1.5]

Utilisez cette `glide.http.cache_control` propriété pour définir la valeur de contrôle de cache par défaut dans les en-têtes de réponse HTTP qu'envoie lors de Now Platform la demande de données de contenu statique pour une page. Les images, le CSS et le JavaScript rendus de l'intérieur d'une page sont des exemples de contenu statique.

La `glide.http.cache_control` propriété définit la valeur Cache-Control par défaut dans les en-têtes de réponse HTTP sur **privé** ou **public**. La valeur par défaut est **privé**.

Valeur	Description
privé	Le contenu statique peut être mis en cache au niveau du navigateur (client), mais pas au niveau du serveur proxy.
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 *glide.http.cache* propriété désigner s'il faut activer ou désactiver la définition 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 Cache-Control 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 de l'en-tête de réponse HTTP Cache-Control pour le contenu statique.
Valeur recommandée	privé
Cote de risque de sécurité	4.3
Impact fonctionnel	(Moyen) Définit la valeur Cache-Control par défaut dans un en-tête de réponse HTTP.
Risque de sécurité	(Élevé) Si vous définissez cette propriété sur **public**, les instances avec CDN/proxys peuvent mettre en cache du contenu statique et s'afficher sans authentification. • **privé** est un paramètre plus approprié pour les instances avec la 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 Add a system property .

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`glide.cs.debug`façon dont votre instance gère les 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 **true**, les journaux système sont activés. Définissez la propriété sur **true** uniquement lorsque vous souhaitez résoudre les problèmes, 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 de 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 avec des messages de journal qui exposent par inadvertance des informations sensibles.
Dépendances et prérequis	Aucun

Désactiver le débogage des éléments de formulaire verrouillés

Voici la description de `glide.security.explain.write.locks`.

Définir sur `glide.security.explain.write.locks` la valeur **recommandée faux pour** empêcher l'affichage de l'explication des éléments de formulaire verrouillés. Définissez la valeur sur **true** 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)

Attribut	Description
Catégorie	Configuration
Objectif	Limite le comportement d'affichage de SecurityDebugger sans dépendance à d'autres propriétés.
Valeur recommandée	Faux
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 Add a system property .

Désactiver le débogage multiSSO [Mise à jour dans Security Center 1.5]

La `glide.authenticate.multisso.debug` propriété contrôle la journalisation du débogage pour l'authentification unique (SSO) multiple.

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 de l'authentification unique (SSO) à fournisseurs multiples.
Valeur recommandée	Faux
Type de configuration	Booléen
Risque de sécurité	(Élevé) Définissez la propriété sur la valeur recommandée « Faux », faute de quoi le débogage MultiSSO est activé, ce qui peut entraîner une fuite d'informations sensibles involontaire.
Cote de risque de sécurité	4
Références	Propriétés, tables et scripts de l'authentification unique (SSO) de plusieurs fournisseurs

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Interdire le clonage cible [Nouveau dans Security Center 1.3]

Configurez la `glide.db.clone.allow_clone_target` propriété pour empêcher votre instance d'être utilisée comme cible de clone.

Si `glide.db.clone.allow_clone_target` elle n'est pas définie sur la valeur recommandée 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. Un clone système se produit 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, ce qui entraîne une perte de données et un manque d'intégrité des données. En tant que correction, assurez-vous que `glide.db.clone.allow_clone_target` est défini sur faux.

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 : 5,9 • Score CVSS : moyen • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur la valeur recommandée faux, l'instance peut être utilisée comme cible de clone. Il s'agit d'un risque de sécurité, car la base de données d'instance peut être remplacée lors du processus de clonage.
Dépendances et prérequis	Aucun
Références	• System clone • Clone Target Registration and Authentication
Impact fonctionnel	Cette propriété fournit une protection supplémentaire qui empêche la clonage d'une instance de production. La valeur par défaut est false pour les instances de production et true pour les instances de sous-production telles que dev ou qa. Pour permettre à une instance d'être utilisée comme cible de clone, définissez cette propriété sur vrai.

Désactiver l'affichage de la trace de la pile d'erreurs SOAP

Gérez le mode d'affichage des traces de la pile dans votre instance.

Utilisez cette propriété pour gérer les `glide.soapfault.display_stack_trace`traces de la pile dans votre instance. Si cette propriété est configurée sur **faux**, des informations sensibles peuvent être divulguées. Si la valeur est définie sur **true**, aucune trace de pile ne s'affiche.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.soapfault.display_stack_trace`
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 : si vous définissez cette propriété sur **faux,** vous risquez d'exposer des informations sensibles de la trace de la pile.
Dépendances et prérequis	Aucun

Restreindre l'accès à la surveillance des performances

Utilisez cette propriété pour contrôler l'accès `glide.security.diag_txns_acl` stats.do, threads.do, thread_pool_stats et replication.do à partir d'une connexion non authentifiée.

Lorsque vous définissez cette propriété sur **true**, elle `glide.security.diag_txns_acl` autorise uniquement l'accès aux éléments suivants pour le compte administrateur :

- https://<nominstance>.servicenow.com/stats.do
- https://<nominstance>.servicenow.com/threads.do
- https://<nominstance>.servicenow.com/replication.do
- https://<nominstance>.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	Restreindre l'accès aux pages de configuration au compte administrateur uniquement
Valeur recommandée	VRAI
Cote de risque de sécurité	5.3

Attribut	Description
Impact fonctionnel	(Faible) 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 Add a system property .

Activer la version mise à jour du module d'extension Multi SSO [Mise à jour dans Security Center 1.5]

Vérifiez que vous utilisez la version 2 du module d'extension Multi SSO et qu'elle est définie sur true pour réduire les failles de sécurité.

Si le module d'extension Multi SSO est activé sur votre instance, la version doit être v2 et la valeur doit être définie sur **vrai**. Les versions antérieures à MultiSSOv2, y compris SAML 1.1 et SAML 2.0, ne respectent pas les normes de sécurité, car elles utilisent des versions de bibliothèque OpenSAML avec des vulnérabilités et des expositions courantes connues (CVE). Si les CVE connus constituaient des menaces de sécurité dans des bibliothèques OpenSAML obsolètes, cela pourrait permettre à un acteur malveillant de falsifier des messages et de contourner l'authentification par le biais d'attaques par encapsulation de signature XML, en empruntant l'identité d'entités ou en permettant à des attaquants de l'homme du milieu d'obtenir un accès non autorisé à une instance.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.multissov2_feature.enabled`
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	• Score de gravité : 5 • Score CVSS : moyen • Détails du risque de sécurité : définir la valeur de la propriété sur **faux** signifie que vous utilisez des versions précédentes de MultiSSOv2 qui utilisent des bibliothèques OpenSAML présentant des failles de sécurité. Cela pourrait permettre à des acteurs malveillants de falsifier des messages.
Dépendances et prérequis	Aucun

Attribut	Description
Références	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0756504

Appliquer la stratégie de référent sécurisé [Nouveau dans Security Center 1.3]

Utilisez cette `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 `com.glide.security.referrerpolicy` propriété est définie sur la valeur par défaut, elle garantit que l'en-tête HTTP Referrer-Policy est géré avec le niveau approprié d'informations envoyées, spécifiquement adapté à la Now 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 de référence
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 : • valeur par défaut : l'instance s'occupera des en-têtes référents • same-origin : envoyer l'URL référente complète au sein de l'instance/du même domaine et aucun référent à l'origine extérieure

Attribut	Description
	• 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 en dehors de l'origine

Implémenter x-frame-options : en-tête de sécurité SAMEORIGIN

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.

Utilisez l'en-tête de réponse HTTP X-Frame-Options pour indiquer si le navigateur doit être autorisé à rendre une page dans un <frame> ou <iframe>. Les sites peuvent utiliser cette fonction pour éviter les attaques de détournement de clic en s'assurant que leur contenu n'est pas intégré dans 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 uniquement 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
Cote de risque de sécurité	7.1
Impact fonctionnel	(Faible) Cette correction applique la restriction pour le rendu d'une Now 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 politique 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 stratégie de même origine qui permet d'accéder aux ressources/scripts à partir d'un autre domaine lorsqu'il est explicitement indiqué dans le cadre d'une valeur d'en-tête.

Attribut	Description
	• Dans ce cas, l'en-tête X-Frame-Options contrôle si l'application Now Platform peut être rendue sur le site Web tiers. • Cela réduit l'exposition sensible, car la valeur de propriété, lorsqu'elle est définie sur **SAMEORIGIN** , n'active pas le rendu.
Références	Propriétés système disponibles Configurer les iFrames

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Exiger un accès en écriture pour accéder à la page d'ajout d'élément du catalogue de services [Nouveau dans Security Center 1.3]

Utilisez cette 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 pourrait 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

Attribut	Description
Impact fonctionnel	Lorsque la propriété est définie sur true, l'utilisateur doit avoir un accès en écriture à l'enregistrement dans le contexte de la page d'interface utilisateur.

Définir des options Xframe pour empêcher l'intégration de sites Web tiers [Mise à jour dans Security Center 1.3]

Configurez cette propriété pour empêcher l'intégration du contenu d'une application Web dans un site tiers.

Si cette propriété n'est pas définie 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** ; Permettre aux sites tiers non approuvés d'activer des attaques telles que le détournement de clic.

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	Origine identique
Valeur par défaut	Origine identique
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, le contenu d'une application Web peut être intégré 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 porte sur les éléments de confidentialité, d'intégrité et de disponibilité (CIA) des données.

Les composants CIA sont les suivants :

- Confidentialité : les données sont protégées contre tout accès non autorisé en transit et au repos.
- Intégrité : Les données sont protégées contre la création, la suppression ou la modification non autorisées.
- Disponibilité : les données sont accessibles en cas de besoin.

Supprimer Se souvenir de moi

Utilisez cette *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
Objectif	Pour s'assurer qu'aucune information d'authentification n'est mise en cache.
Cote de risque de sécurité	3.5
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette correction modifierait 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 indiqué à la section 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. • Cela pose 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 pour ce scénario augmente lorsque l'utilisateur final a laissé le navigateur sans surveillance ou s'il est compromis par une autre attaque.
Références	Décochez la case Se souvenir de moi

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property

Exiger l'effacement du presse-papiers lors de l'affichage en arrière-plan d'une application mobile [Nouveau dans Security Center 1.3]

La *glide.sg.clear_pasteboard_when_backgrounded* propriété contrôle si le texte copié à partir de l'application mobile ServiceNow est conservé dans le clipper et le presse-papiers une fois que l'application est en mode arrière-plan.

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
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 aux autres applications de l'appareil.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété efface le presse-papiers copier-coller lorsque l'application ServiceNow passe en arrière-plan.

Restreindre les mises à jour des tickets RH à partir d'e-mails personnels [Mise à jour dans Security Center 1.5]

Utilisez cette`sn_hr_core.restrict_guest_email` propriété pour contrôler si un utilisateur peut répondre à un ticket RH avec son adresse e-mail personnelle.

Lorsque la propriété n'est `sn_hr_core.restrict_guest_email` 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

Attribut	Description
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails du risque de sécurité : si cette propriété n'est pas définie sur vrai, 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.
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 true, toute réponse provenant d'un e-mail personnel sera ajoutée aux notes du ticket. Si la valeur est définie sur faux, le ticket et les notes ne seront pas mis à jour.

Restreindre les paramètres OAuth au corps de la publication [Nouveau dans Security Center 1.3]

Cette `glide.oauth.allow.parameters.in.post.body.only` propriété contrôle 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 : 7,4 • Score CVSS : élevé • Détails du risque de sécurité : si `glide.oauth.allow.parameters.in.post.body.only` cette propriété n'est pas définie sur la valeur recommandée, vrai, les jetons d'accès peuvent se trouver dans le paramètre de demande GET, ce qui pourrait persister dans les journaux d'infrastructure du client et entraîner la prise de contrôle du compte en cas de fuite de ces journaux.
Dépendances et prérequis	Aucun

Attribut	Description
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'attribution pris en charge.

Gestion et journalisation des erreurs

La catégorie de gestion et de journalisation des erreurs porte sur la qualité et 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, qu'ils protègent correctement les données conformément à la classification et qu'ils ont une durée de vie appropriée. En outre, cette catégorie concerne la gestion appropriée des erreurs et le fait de ne pas révéler d'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

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 **false**, la connexion 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 **true** pour empêcher les utilisateurs ayant 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

Attribut	Description
	• Détails du risque de sécurité : définir cette propriété sur **faux** permet la journalisation des utilisateurs ayant des privilèges inférieurs, ce qui pourrait permettre à un acteur malveillant d'obscurcir une attaque.
Dépendances et prérequis	Aucun

Désactiver le débogage des cookies sécurisés

Gérer les messages de journal liés aux cookies dans votre instance.

Utilisez cette`glide.secure_cookie.debug` propriété pour gérer vos messages de journal liés aux cookies. Si cette propriété est définie sur **false**, aucun message de journal n'est affiché. Si la valeur **est définie sur true**, les messages des classes `SecureUserCookie` et `Cookie` sont enregistrés. Cela pourrait 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 : définir cette propriété sur **vrai** peut entraîner l'exposition d'informations sensibles.
Dépendances et prérequis	Aucun

Désactiver les messages d'erreur SQL [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour désactiver le `glide.db.loguser` rendu des messages d'erreur SQL dans un navigateur.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.db.loguser`

Attribut	Description
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	true|false
Valeur recommandée	faux
Cote de risque de sécurité	3.1
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 cadre d'un message d'erreur sur une page Web.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Activer le journal d'audit MID [mis à jour dans Security Center 1.5]

Le journal d'audit de la commande MID Server 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 naviguant vers **MID Server** > **Journaux d'audit de commande**.

Définissez la valeur *`mid.log.command_audit.enable`* sur vrai dans la table ecc_agent_property pour activer l'audit des commandes exécutées par le MID Server.

En savoir plus

Attribut	Description
Nom de la configuration	*`mid.log.command_audit.enable`*
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 : 2,2 • Score CVSS : faible • Détails du risque de sécurité : en cas d'enquête de sécurité, cette table peut être utilisée par les équipes de réponse aux incidents pour auditer les commandes exécutées sur le MID Server.

Attribut	Description
	Sans ce journal, il se peut que les détails soient insuffisants pour répondre à des situations telles que l'utilisation non autorisée d'un compte.
Dépendances et prérequis	Aucun

Activer le module d'extension des tables protégées [Nouveau dans Security Center 1.3]

Utilisez cette propriété pour empêcher les utilisateurs avec des privilèges plus élevés d'altérer les `com.glide.security.protected_table.enabled` tables de journal.

Lorsque la `com.glide.security.protected_table.enabled` propriété est définie sur **vrai**, le 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 disposent de protections spéciales lorsque cette propriété est définie sur **true** :

- 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 : ne pas définir `com.glide.security.protected_table.enabled`

Attribut	Description
	la valeur recommandée 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

Enregistrer tous les champs des requêtes HTTP sortantes [supprimé dans Security Center v1.3.2]

Configurez la propriété sur `glide.outbound_http.security.log.allow.all.fields` false pour empêcher laconnexion des champs HTTP sortants sensibles 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 consignées en texte brut non chiffré et visibles par des utilisateurs ayant des privilèges inférieurs.

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 : si vous ne définissez pas cette propriété sur **faux,** vous augmentez les chances que des champs sortants sensibles soient consignés en texte brut, ce qui constitue un risque pour la sécurité.
Dépendances et prérequis	Aucun

Assainissement des journaux HTML

Configurez `glide.html_sanitize.discarded_log.enable` la propriété pour déterminer si les événements d'assainissement HTML seront journalisés dans votre instance.

Si cette propriété n'est pas définie sur la valeur recommandée, **vrai**, les événements d'assainissement HTML ne sont pas consignés dans la `sys_log` table. Le manque de journalisation peut avoir un impact négatif sur les capacités de détection et d'investigation de sécurité automatisées 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 options automatisées de détection et d'investigation `sys_log` 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]

Définissez la propriété sur **vrai** pour que des `glide.authenticate.session_access.log_audit_event` événements d'audit de session soient créés dans la `sys_session_access_audit` table.

L'enregistrement des informations sur l'accès à la session vous aidera à analyser les attaques de cybersécurité. Les informations consignées 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.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.session_access.log_audit_event`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI

Attribut	Description
Catégorie	Gestion et journalisation des erreurs
Risque de sécurité	• Score de gravité : 6,3 • Score CVSS : moyen • Détails du risque de sécurité : 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'usurpation d'identité d'un utilisateur

Configurez `glide.sys.log_impersonation` pour contrôler si les événements d'emprunt d'identité de l'utilisateur sont journalisés dans votre instance.

Si cette propriété n'est pas définie sur la valeur conseillée, **vrai**, les événements d'emprunt d'identité de l'utilisateur ne sont plus consignés. L'absence de journalisation peut avoir un impact sur les fonctionnalités automatisées de détection et d'investigation de sécurité de votre instance.

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 consignés, ce qui pourrait avoir un impact sur les capacités de détection et d'enquête de sécurité de votre instance.
Dépendances et prérequis	Aucun
Références	Impersonating users

Désactiver les messages d'erreur SQL détaillés pour le processeur d'importation

Configurez cette propriété pour contrôler l'affichage ou non des messages d'erreur SQL détaillés.

Si la propriété est définie sur **false**, un message d'erreur SQL détaillé s'affiche, susceptible de divulguer des informations sensibles. Pour éviter cela, définissez la propriété sur **true** pour afficher un message générique.

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 détaillés, ce qui peut entraîner une fuite d'informations.
Dépendances et prérequis	Aucun

Fichier et ressources

La catégorie Fichier et 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 d'accès.

Interdire le téléchargement de fichiers infectés [Mise à jour dans Security Center 1.5]

Gérez cette propriété pour contrôler si des traces de pile sont affichées dans votre instance.

Si `com.glide.snap.infected_download_allowed` elle n'est pas définie 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.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.snap.infected_download_allowed`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Catégorie	Fichier et ressources
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, vous risquez d'exposer votre instance au téléchargement de fichiers malveillants.
Dépendances et prérequis	Aucun

Activer la notation et le filtrage d'e-mail indésirable [Mise à jour dans Security Center 1.3]

Installez le module d'extension Email Filter (`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.

Chaque message envoyé via Now Platform des serveurs de messagerie est évalué pour la probabilité d'être un spam.

Remarque :
Si une instance utilise un serveur de messagerie privé, cette rubrique ne s'applique pas. Pour plus d'informations, reportez-vous à la section Notation et filtrage des courriers indésirables.

Prérequis

Avant de définir cette propriété :

Définissez la propriété `glide.email.read.active` sur true. Pour en savoir plus, consultez Activer l'utilisation de votre propre serveur POP3 .

En savoir plus

Attribut	Description
Nom du module d'extension	`com.glide.email_filter`
Type de configuration	Définition du système > Modules d'extension
Catégorie	Fichier et ressources
Objectif	Pour appliquer un filtrage afin d'éviter le spamming d'e-mails.

Attribut	Description
Valeur recommandée	Actif
Cote de risque de sécurité	8.1
Impact fonctionnel	(Faible) Les e-mails ne sont jamais filtrés, bloqués ou mis en quarantaine de l'instance dans le cadre du score de courrier indésirable. Elles sont seulement notées, puis envoyées à l'instance. Tout le filtrage est effectué dans l'instance avec le module d'extension Email Filters.
Risque de sécurité	(Modéré) Les filtres d'e-mail permettent aux administrateurs d'utiliser un créateur de condition ou un script conditionnel pour spécifier quand ignorer les e-mails entrants malveillants provenant d'expéditeurs connus/inconnus.
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 Activate a plugin .

Activer l'analyse antivirus

La `com.glide.snap.enable_scan` propriété active la fonctionnalité d'analyse antivirus.

Définissez sur `com.glide.snap.enable_scan` la valeur **recommandée vrai pour** activer l'analyse antivirus.

Avertissement :
Il s'agit d'une propriété d'exonération, 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	Fichier et ressources
Objectif	Pour activer ou désactiver l'analyse antivirus sur une instance spécifique.
Valeur recommandée	Vrai (par défaut)
Type de configuration	Booléen
Risque de sécurité	(Élevé) L'analyse antivirus permet de protéger votre instance contre les infections de virus qui peuvent être introduites par les pièces jointes de fichiers 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

Utilisez cette 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, qui crée une liste délimitée par des virgules des types de fichiers téléchargeables restreints. Pour en savoir plus, reportez-vous à la section Types de fichiers téléchargeables.

⚠ Avertissement :
La valeur de cette propriété est aucun remplacement de 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	Fichier et ressources
Objectif	Permet de s'assurer que les types de fichiers sûrs peuvent être téléchargés à partir de l'application.
Valeur recommandée	VRAI
Cote de risque de sécurité	3.1
Impact fonctionnel	(Faible) Cette correction applique la restriction des téléchargements de fichiers en fonction des valeurs spécifiées dans la `glide.ui.strict_customer_uploaded_content_types` propriété. Pour en savoir plus, reportez-vous à la section Types de fichiers téléchargeables.
Risque de sécurité	(Faible) Les restrictions de téléchargement de fichiers doivent être appliquées à toutes les sources d'entrée utilisateur non approuvées.

Limiter la taille des pièces jointes dans les flux de formation et de prédiction pour les points de terminaison GraphQL

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)

Attribut	Description
Type de données	entier
Valeur recommandée	5,242,880
Valeur par défaut	5,242,880
Catégorie	Fichier 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 [Mise à jour dans Security Center 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	Fichier et ressources
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : s'il `glide.platform_ml_di.max_attachment_size` n'est pas défini sur la valeur recommandée de 4 000 000 ou moins, le renvoi de fichiers volumineux peut provoquer une attaque par déni de service (DoS).
Dépendances et prérequis	Aucun

Limiter la taille du corps de la réponse HTTP [Mise à jour dans Security Center 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`.

Les `glide.http.response.get_body.limit.enabled` propriétés and `glide.http.response.get_body.limit` ont été introduites pour activer une nouvelle fonctionnalité qui empêche `OutOfMemoryExceptions` d'être levée lorsque la réponse à une requête est trop volumineuse. `OutOfMemoryExceptions` peut entraîner des attaques par déni de service (DoS) ainsi que d'autres problèmes susceptibles d'aider les attaquants à compromettre une instance.

Pour protéger votre instance contre ces failles de sécurité, assurez-vous que `glide.http.response.get_body.limit.enabled` cette valeur est définie sur true et qu'elle `glide.http.response.get_body.limit` ne dépasse pas 524 288 000 mégaoctets (500 Mo).

En savoir plus

Attribut	Description
Nom de la configuration	`glide.http.response.get_body.limit.enabled` Et `glide.http.response.get_body.limit`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Fichier et ressources
Risque de sécurité	• Score de gravité : 6,4 • Score CVSS : moyen • Détails du risque de sécurité : si vous ne définissez pas ces propriétés sur les valeurs recommandées, vous risquez de rendre votre instance vulnérable aux `exceptions OutOfMemoryExceptions` et aux attaques par déni de service.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété réduit les chances d'une `exception OutOfMemoryException` en raison du chargement accidentel par un client d'un fichier volumineux en mémoire.

Limiter le nombre maximum de pièces jointes dans un e-mail

Configurez le nombre de pièces jointes d'e-mails entrants sur votre instance.

Cette`glide.email.inbound.max_attachment_count` propriété contrôle le nombre maximal de pièces jointes d'e-mails entrants 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	Fichier 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 une valeur supérieure à 30 peut entraîner des problèmes de dégradation.
Dépendances et prérequis	Aucun
Références	Email properties

Minimiser la taille autorisée des pièces jointes

Configurez la `com.glide.attachment.max_size` propriété pour contrôler la taille maximale autorisée pour une pièce jointe chargée.

Cette propriété contrôle la taille maximale d'une pièce jointe chargée. Si cette propriété n'est pas définie sur la valeur recommandée de **1 024** ou moins, la plateforme peut accepter des fichiers volumineux susceptibles de remplir le stockage et d'entraîner une attaque par déni de service (DoS).

Remarque :
La taille réelle d'une pièce jointe est calculée en multipliant 1024 x 1024 par la valeur de la propriété. Si la valeur de la propriété est **1024**, la taille maximale autorisée pour une pièce jointe est de 1 Go.

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	1 024
Valeur par défaut	4096
Catégorie	Fichier et ressources

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 **1 024** ou moins, la plateforme peut accepter des fichiers volumineux susceptibles d'entraîner une attaque par déni de service.
Dépendances et prérequis	Aucun
Références	Attachment limit properties

Valider le type MIME de fichier dans le service Web SOAP AttachmentCreator [Nouveau dans Security Center 1.3]

La *glide.attachment.enforce_security_validation* propriété détermine si les fichiers MIME (Multipurpose Internet Mail Extensions) doivent être validés.

Si *glide.attachment.enforce_security_validation* cette propriété n'est pas définie sur la valeur recommandée, **vrai**, les fichiers MIME ne sont pas validés, ce qui permet de charger des fichiers malveillants avec des extensions de fichier incorrectes. Lorsque cette propriété est définie sur **vrai**, les fichiers sont téléchargés 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)
Type de données	Booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Fichier et ressources
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé • 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 de déguiser des fichiers malveillants en modifiant 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 true pour exécuter les validations de type MIME et d'extension de fichier

Attribut	Description
	sur les pièces jointes chargées. Aucune validation n'est exécutée si cette propriété est définie sur faux. Cette propriété est définie sur true par défaut.

Code malveillant

La catégorie Code malveillant garantit que tous les efforts sont déployés pour confirmer que votre code est exempt de vulnérabilités et de fonctionnalités indésirables.

Il s'agit notamment d'assurer une gestion sécurisée et appropriée des activités malveillantes, l'absence d'attaques basées sur le temps, l'absence de communications sortantes 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 provenant de la base de code de l'application.

Bloquer les appareils mobiles racines ou jailbreakés

Sécurisez votre instance en empêchant l'accès non autorisé à partir d'appareils jailbreakés.

Utilisez cette propriété pour sécuriser 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 **false**, il reçoit l'alerte suivante : Ce périphérique paraît débridé et ne peut pas être utilisé pour accéder à cette instance. Veuillez contacter votre administrateur ServiceNow. L'application est figée lorsque le message d'alerte est affiché, et la seule façon d'ignorer ce message consiste à sélectionner **Se déconnecter**. Si cette propriété est définie sur **true** , les utilisateurs s'authentifient dans une instance à l'aide d'un appareil jailbreaké.

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 des risques de sécurité : Le manque de sécurité des appareils jailbreakés en fait une cible de choix pour les acteurs malveillants. 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

Attribut	Description
Références	Contrôle d'accès

Désactiver la racine de confiance ServiceNow [Nouveau dans Security Center 1.5]

Utilisez cette `com.snc.csf.servicenow_root_of_trust.disabled` propriété pour contrôler quels certificats de clé de build sont approuvés sur une instance.

Lorsque la `com.snc.csf.servicenow_root_of_trust.disabled` propriété n'est pas définie sur la valeur recommandée, vrai, les signatures sur la `sn_kmf_record_signature` table avec des certificats de version ServiceNow sont approuvées sur l'instance. Lorsque la propriété est définie sur true, seules les signatures avec les certificats clients sont approuvées. Les administrateurs d'instance ne doivent faire confiance qu'à leurs propres certificats, car cela réduit l'impact sur la sécurité en cas de compromission de la clé de build et des certificats d'un ServiceNow.

En savoir plus

Attribut	Description
Nom de la configuration	`com.snc.csf.servicenow_root_of_trust.disabled`
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 : 4 • Score CVSS : moyen • Détails du risque de sécurité : lorsque cette propriété n'est pas définie sur la valeur recommandée vrai, les signatures sur la `sn_kmf_record_signature` table avec des certificats de version ServiceNow sont approuvées sur l'instance. Cela augmente l'impact sur la sécurité dans le cas où une version ServiceNow est compromise par un acteur malveillant.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété active ou désactive la racine de confiance ServiceNow.

Activer la signature de code pour les données et les scripts de configuration de l'application [supprimé dans Security Center 1.3.2]

Gérez la signature de code pour les données de configuration d'application et les scripts sur votre instance.

La signature de code permet d'améliorer la sécurité en validant les scripts et les données de configuration d'application sensibles 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 données ou de scripts malveillants sur l'instance, qui pourrait entraîner une compromission complète de l'instance.

Utilisez cette propriété pour gérer la signature de code pour les données de configuration d'application`com.snc.kmf.signature.validation.flag` et les scripts. Lorsque cette propriété est définie sur **vrai**, la signature de code est activée pour les données et les scripts de configuration de l'application.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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`
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 scripts et les données 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 à partager, et invalidées après des périodes d'inactivité ou lorsqu'elles ne sont pas requises. Cela inclut des facteurs tels que les attributs de cookie pour les sessions basées sur les cookies, la génération et le stockage de jetons de session, ainsi que les exigences en matière de réauthentification fédérée.

Minimiser la durée du délai absolu d'expiration de la session

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 forcés de s'authentifier à nouveau dans l'instance.

Il permet au cookie utilisateur d'être valide pendant la durée de jours spécifiés, à compter de la date à laquelle le cookie a été émis pour la première fois. La valeur par défaut est de 30 jours et la limite maximale est de 365 jours.

Remarque :
Pour imposer une durée de session maximale pour 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
Objectif	Pour forcer les utilisateurs qui ont coché la case **Se souvenir de moi** à s'authentifier à nouveau après des jours spécifiques.
Valeur recommandée	Inférieur ou égal à 30
Valeur par défaut	30 jours
Impact fonctionnel	(Moyen) Cette propriété applique la reconnexion obligatoire en évitant toute sorte de rotation des cookies après une période donnée.
Cote de risque de sécurité	4.2
Risque de sécurité	(Moyen) Le fait que les cookies utilisateur soient actifs pour une durée indéterminée constitue un risque pour la sécurité et doit expirer selon une configuration basée sur le temps.
Références	Propriétés système disponibles Modifier les paramètres de la case à cocher Mémoriser mon nom et du cookie

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Définir les rôles d'exception de délai d'expiration de session active [Nouveau dans Security Center 1.3]

Cette `glide.active.session.timeout.exception.roles` propriété contrôle les rôles qui sont exemptés d'une limite de délai d'expiration de session active.

Le délai d'expiration de session actif garantit qu'une session détournée ne peut pas être utilisée indéfiniment sans fournir à nouveau d'informations d'authentification. Pour remédier à ce risque de sécurité, assurez-vous que la `glide.active.session.timeout.exception.roles` propriété est définie sur **edge_encryption, mid_server**.

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
Valeur par défaut	edge_encryption, mid_server
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 7,1 • Score CVSS : élevé • Détails du risque de sécurité : Considérez uniquement une exception de limite de délai d'expiration de session active pour les rôles de compte d'intégration interne. Si une exception est accordée à un rôle au délai d'expiration de session et que ce rôle est attribué à un utilisateur victime d'une attaque de détournement de session, un attaquant peut continuer à s'authentifier indéfiniment auprès de cette session. 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

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 `glide.ui.secure.cookies.use_kmf` propriété est désactivée. UserCookie v3 n'est pas sécurisé en raison du stockage de la clé secrète pour les codes d'authentification de message basés sur le hachage (HMAC) dans le code source qui est identique pour tous les clients. Un acteur malveillant peut utiliser une clé secrète pour tenter de détourner les sessions des utilisateurs. Pour remédier à cette menace de sécurité, assurez-vous que la `glide.ui.secure.cookies.use_kmf` propriété est définie sur **vrai** et utilise UserCookie v3.1. La clé secrète est stockée dans un stockage sécurisé 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

Attribut	Description
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 : la définition de cette valeur sur **faux** est une faille de sécurité en raison du stockage de la clé secrète des codes d'authentification de message basés sur le hachage (HMAC) dans le code source.
Dépendances et prérequis	Aucun

Appliquer la réinitialisation du mot de passe aux demandes d'API

Gérez le fonctionnement de la fonctionnalité de réinitialisation de mot de passe sur votre instance.

Lorsqu'un utilisateur est marqué comme **Mot de passe doit 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 **recommandée vrai,** les comptes d'utilisateurs marqués comme **Mot de passe doit être réinitialisé** peuvent toujours effectuer des opérations en interrogeant l'API de table via l'authentification de base. Cette faille de sécurité pourrait entraîner des fuites d'informations si un compte inactif est 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 Security Center 1.3]

Utilisez cette `glide.cookies.http_only` propriété pour activer l'attribut HTTPOnly pour les cookies confidentiels.

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 intersite mais élimine certains vecteurs d'exploitation.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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.cookies.http_only`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion des sessions
Objectif	Pour atténuer le risque que le script côté client accède au cookie protégé.
Valeur recommandée	VRAI
Cote de risque de sécurité	8
Impact fonctionnel	(Faible) Cette correction ajoute un marqueur HTTPOnly supplémentaire sur les cookies de session, les protégeant ainsi contre le vol. • Si vous disposez d'une fonctionnalité personnalisée qui nécessite JavaScript pour accéder au cookie de l'utilisateur, cela interrompt cette fonctionnalité. Cela ne devrait pas être le cas dans des circonstances normales. • Il Now Platform gère la gestion des sessions 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 à l'application. Cela signifie qu'il est nécessaire de les protéger contre le vol ou l'exportation. Les indicateurs 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 Add a system property .

Minimiser le nombre de sessions interactives simultanées [Mise 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 Authentifier le nombre maximal de sessions interactives simultanées** avec le module d'extension **Limite de session simultanée** (`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).

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 une valeur par défaut de la propriété supérieure à 1 augmente les risques de détournement de session.
Dépendances et prérequis	Le module **d'extension Sessions interactives simultanées** (`com.glide.limit.concurrent.sessions`) doit être actif.
Références	Sessions simultanées limites

Limiter les sessions simultanées sur tous les nœuds [Mise à jour dans Security Center 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 (**Limite de sessions simultanées authentifiée par Glide 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 **faux**, 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
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails des risques de sécurité : lors de l'utilisation du module d'extension **Limite de sessions simultanées** , la définition de cette propriété sur **faux** permet l'ouverture de plusieurs sessions sur plusieurs nœuds, ce qui augmente les risques de vulnérabilité de sécurité telle qu'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 les risques 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

Attribut	Description
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : Si ce plugin n'est pas actif, le risque de détournement de session augmente.
Dépendances et prérequis	Aucun

Limiter la durée de vie de la session active de l'invité [Nouveau dans Security Center 1.3]

Utilisez cette *glide.guest.active.session.life_span* propriété pour contrôler la durée des sessions HTTP d'un invité actif.

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 d'inactivité d'un utilisateur 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, ce qui augmenterait 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 corriger cette faille de sécurité, définissez une *glide.guest.active.session.life_span* 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	1-720 (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 : la définition de la durée de vie maximale sur une valeur élevée permet à un acteur malveillant de passer plus de temps au sein d'une instance en cas de vol de session.
Dépendances et prérequis	Aucun

Attribut	Description
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'expiration `glide.guest.session_timeout` inactif (30 minutes par défaut).

Limiter les sessions interactives simultanées

Gérez le nombre de sessions interactives sur votre instance.

Utilisez cette `glide.authenticate.limit.concurrent.interactive.sessions` propriété pour gérer le nombre de sessions interactives sur une instance. Cette propriété est destinée à être utilisée avec le module d'extension Sessions simultanées limites(com.glide.limit.concurrent.sessions). 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 sur une instance. Un plus grand nombre de sessions ouvertes signifie une plus grande possibilité de détournement de session.

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 d'un détournement de session.
Dépendances et prérequis	Aucun
Références	Limiter les sessions interactives simultanées

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
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails sur les risques 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 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.

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.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

Attribut	Description
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails sur les risques de sécurité : une durée de vie maximale plus longue pourrait permettre à un attaquant de rester plus longtemps dans une session volée, ce qui augmenterait 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'expiration inactif glide.ui.session_timeout (30 minutes par défaut).

Invalider de manière proactive les sessions inactives [Nouveau dans Security Center 1.3]

Cette `glide.active.session.timeout.invalidate.session` propriété contrôle si une session de délai d'expiration est invalidée de manière proactive avant le serveur Tomcat.

Si `glide.active.session.timeout.invalidate.session` cette option n'est pas définie sur **true**, 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 piratée, un attaquant peut être en mesure d'utiliser une session pendant cette courte période de temps. 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 : Si vous ne définissez pas cette propriété sur la valeur recommandée,

Attribut	Description
	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 cette propriété pour activer la rotation des identificateurs de session HTTP afin de réduire les `glide.ui.rotate_sessions` failles 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 désormais cette session authentifiée.

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
Cote de risque de sécurité	8.8
Impact fonctionnel	(Moyen) Cette correction a modifié l'ID de session lorsque l'utilisateur navigue d'une page non authentifiée vers des pages authentifiées. • Si vous utilisez un proxy ou codez en dur l'ID de session 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 Single Sign-on, 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 false.
Risque de sécurité	(Modéré) SessionID est utilisé pour traiter et authentifier l'utilisateur de l'instance en maintenant l'état de la session sur le navigateur. Par conséquent, les SessionID sont considérés comme des données sensibles et doivent être sécurisés par défaut. La rotation de session est un contrôle de sécurité qui applique la modification de l'ID de session chaque fois que l'utilisateur navigue à partir de pages non authentifiées pour authentifier des pages.

Attribut	Description
Références	Authentification avec SAML

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Minimiser le nombre de sessions interactives simultanées

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 Authentifier le nombre maximal de sessions interactives simultanées** avec le module d'extension **Limite de session simultanée** (`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).

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 une valeur par défaut de la propriété supérieure à 1 augmente les risques de détournement de session.
Dépendances et prérequis	Le module **d'extension Sessions interactives simultanées** (`com.glide.limit.concurrent.sessions`) doit être actif.
Références	Sessions simultanées limites

Minimiser la durée du délai d'expiration d'activité de la session

Utilisez cette 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 session spécifié est long, plus la quantité de mémoire utilisée au cours d'une session de traitement est importante. Le système de base utilise un délai d'expiration Apache Tomcat par défaut de 30 minutes.
- L'utilisateur Now Platform se déconnecte toujours avec Se souvenir de moi. Après 30 minutes d'inactivité dans l'application, la plateforme déconnecte automatiquement l'utilisateur, sauf si la case **à cocher Se souvenir de moi** dans la page de connexion est sélectionnée. Ce qui est différent, c'est qu'ils ne se reconnectent pas pour continuer.
- S'il existe des jauges ou du contenu sur les pages d'accueil des utilisateurs qui s'actualisent automatiquement, ce délai d'expiration risque de 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 la session.
Valeur recommandée	Délai d'expiration spécifié par l'utilisateur, en minutes. La valeur recommandée est de 60 minutes, mais cette valeur peut varier en fonction des exigences de fonctionnalité et de sécurité. Ne définissez pas cette valeur sur plus d'un jour.
Cote de risque de sécurité	7.5
Impact fonctionnel	(Moyen) 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 indéterminée constitue un risque de sécurité et doit expirer selon la configuration temporelle.
Références	Gérer les sessions utilisateur

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Limiter l'intervalle de jeton d'actualisation mobile d'accès à la session en fonction de règles [Nouveau dans Security Center 1.5]

Utilisez cette `glide.authenticate.session_access.mobile.refresh_token_interval` propriété pour régir le temps qui doit s'écouler avant qu'un utilisateur d'équipement mobile ne soit forcé de s'authentifier une nouvelle fois.

L'utilisateur est invité à s'authentifier à nouveau uniquement si l'administrateur a configuré les attributs du fournisseur d'identité dans la stratégie de session (les attributs peuvent varier d'une connexion à l'autre) 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_ir`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1 800 (secondes)
Valeur par défaut	1 800 (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 éclipse la valeur par défaut de 1 800 secondes (30 minutes). Si une valeur plus élevée est utilisée, les utilisateurs seront forcés d'attendre ce temps écoulé.
Dépendances et prérequis	Zero Trust - Accès à la session basé sur une politique
Impact fonctionnel	Ce paramètre régit le délai, en secondes après la connexion, pendant lequel les utilisateurs seront forcés de se déconnecter des équipements mobiles s'ils utilisent l'authentification unique pour s'authentifier et que l'administrateur a configuré les attributs Identifier le fournisseur dans la politique d'accès à la session.

Minimiser la durée du délai d'expiration de la fenêtre de session

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 le délai maximum 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 activer l'expiration par défaut du cookie **Se souvenir de moi** .
Valeur recommandée	Valeur entière définie par l'utilisateur (# de jours) [Exemple : 15]
Cote de risque de sécurité	4.9

Attribut	Description
Impact fonctionnel	(Moyen) Cette propriété est activée par l'utilisateur final lorsque celui-ci coche la case **Mémoriser** mon nom dans la page de connexion et se connecte au Now Platform.
Risque de sécurité	(Modéré) Le fait que les cookies utilisateur soient actifs pour une durée indéterminée constitue un risque pour la sécurité et doit expirer selon une configuration basée sur le temps.
Références	Propriétés système disponibles Modifier les paramètres de la case à cocher Mémoriser mon nom et du cookie

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Cryptographie stockée

Cette catégorie se concentre sur le chiffrement des données stockées. Il englobe plusieurs aspects clés, tels que l'utilisation d'algorithmes et de modules cryptographiques établis, la garantie de la bonne génération de valeurs pseudo-aléatoires, la mise en œuvre d'un cryptage basé sur la classification des données, ainsi que le stockage et l'isolement sécurisés du matériel clé.

Activer l'encrypteur glide KMF [supprimé dans Security Center 1.3.2]

Gérez les chiffreurs utilisés pour les champs Password2 sur votre instance.

Utilisez lapropriété pour définir l'encrypteur `glide.kmf.encrypter.enabled` KMF comme chiffreur par défaut pour les champs Password2. Cette propriété garantit l'utilisation de normes de chiffrement solides et conformes au lieu d'un chiffreur hérité. Pour vous assurer que l'encrypteur KMF est utilisé au lieu de l'encrypteur 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 l'encrypteur KMF est utilisé au lieu de l'encrypteur hérité.

Attribut	Description
Dépendances et prérequis	Aucun
Références	Chiffrement Password2 avec Key Management Framework (KMF)

Validation, assainissement et encodage

La validation, l'assainissement et l'encodage traitent la validation de l'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, le sandboxing, le cas échéant, et la validation positive via des listes d'autorisation.

Restreindre l'accès à l'API de script GlideSystemUserSession [mis à jour dans Security Center 1.3]

L'API scriptable GlideSystemUserSessionSandbox pouvant être appelée par le client expose les méthodes GlideSystemUserSession's addErrorMessageNoSanitization et addInfoMessageNoSanitization au bac à sable JavaScript. Cela permet à tous les utilisateurs d'appeler cette méthode via le script.

Lorsqu'elle est définie sur **vrai**, une session utilisateur bac à sable (sandbox) est autorisée à appeler des informations ou des messages d'erreur sans nettoyage. Un avertissement sera consigné lors de l'appel du message. Lorsqu'elle est définie sur **faux**, l'appel n'est pas autorisé.

> ⚠ **Avertissement :**
> Il s'agit d'une propriété d'exonération, 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.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 désinfectés dans une session utilisateur bac à sable.
Type	vrai | faux booléen
Valeur recommandée	faux
Cote de risque de sécurité	8.1
Impact fonctionnel	(Élevé) Définir la propriété avec la valeur false n'entraînera aucune création ou journalisation de message si ces fonctions sont appelées.

Attribut	Description
Risque de sécurité	(Élevé) En l'absence d'assainissement approprié, il est possible d'accéder à du contenu potentiellement dangereux et de mettre la fonction d'erreur non désinfectée à la disposition du script.
Références	Contrôle d'accès

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Désactiver les balises JavaScript dans le HTML intégré

Utilisez cette propriété pour désactiver la `glide.ui.security.codetag.allow_script` prise en charge de l'incorporation du code JavaScript HTML créé à l'aide de la balise [code].

Il Now 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 de journal. Toutefois, les champs journal peuvent restituer le texte compris entre des balises de code au format HTML. Assurez-vous que la `glide.ui.security.codetag.allow_script` propriété existe dans la table sys_properties et qu'elle 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 autre navigateur client après le rendu des champs de journal.
- Définissez cette propriété sur **false** afin que les administrateurs puissent empêcher les champs journal de rendre le code JavaScript HTML en désactivant la prise en charge de la balise [code].

Avertissement :
Il s'agit d'une propriété d'exonération, 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.security.codetag.allow_script`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	Protège contre le script intersite et l'exécution de scripts malveillants
Valeur recommandée	faux
Cote de risque de sécurité	8.8
Impact fonctionnel	(Moyen) Cette correction applique l'échappement JavaScript sur l'interface utilisateur et renvoie les résultats codés à l'utilisateur. Elle peut avoir un impact sur les fonctionnalités 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

Attribut	Description
	attaques permettent à des scripts étrangers de s'exécuter sur la session de l'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 journal Afficher les entrées de 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 Add a system property .

Activer le gestionnaire de sécurité Java renforcé [Nouveau dans Security Center 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 d'exonération, 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
Valeur recommandée	`com.glide.sys.security.ContextualSecurityManager`
Valeur par défaut	`com.glide.sys.security.ContextualSecurityManager`
Catégorie	Validation, assainissement et encodage
Risque de sécurité	• Score de gravité : 7,2 • Score CVSS : élevé • Détails du risque de sécurité : s'il `glide.security.manager` n'est pas défini sur la valeur recommandée , `com.glide.sys.security.ContextualSecurityManager`l'instanc utilise peut-être un gestionnaire de sécurité Java obsolète pour lequel 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 l'exécution de code à distance sur l'instance.
Dépendances et prérequis	Aucun

Appliquer l'assainissement HTML [mis à jour dans Security Center 1.3]

Utilisez cette propriété pour appliquer le `com.glide.security.check_unsanitized_html` comportement de nettoyage de translated_html champs à un niveau global pour les affectations de champs.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ fournit la fonctionnalité de mise en forme du contenu à l'aide de balises HTML (par exemple, <p>, , <a href>, <b><font><img>,). Pour empêcher toute activité malveillante, certaines balises HTML peuvent être interdites à l'aide d'une liste de blocage. Cette propriété empêchera l'utilisation de balises non autorisées 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 les balises HTML bloquées sur translated_html champs.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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, assainissement et encodage
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`
Cote de risque de sécurité	7.3
Impact fonctionnel	(Moyen) 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 la mise en forme.
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 des utilisateurs dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Assainisseur HTML

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Appliquer le bac à sable pour les scripts générés par le client [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour activer le *glide.script.use.sandbox* sandboxing des scripts.

Il existe deux cas dans le Now Platform qui permettent au client d'envoyer des scripts au serveur pour évaluation :

Filtres ou requêtes

Il est légal d'envoyer un filtre au serveur tel que `assigned_to=JavaScript :getMyGroups()`.

API système

L'appel d'API permet au client d'exécuter des scripts arbitraires sur le serveur et de recevoir une réponse.

Si vous activez le sandboxing des scripts, le script évalué à l'un de ces deux points d'entrée s'exécute dans un bac à sable avec des droits réduits, avec les caractéristiques suivantes :

- Seules les règles métier marquées Client pouvant être appelé sont disponibles dans le bac à sable.
- Seules les includes de script marquées Client pouvant être appelé sont disponibles dans le bac à sable.
- Certains appels d'API (en grande partie, mais pas entièrement, limités à ceux traitant d'un accès direct à la base de données ne sont pas autorisés.
- Vous ne pouvez pas insérer, mettre à jour ou supprimer des données depuis le bac à sable. Par exemple, tous les appels à `current.update()` sont ignorés. Si vous exécutez le sans activer le sandboxing des Now Platform scripts, aucune de ces restrictions ne s'applique.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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.use.sandbox*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	Applique la validation pour les requêtes JavaScript côté client qui sont lancées sur la plateforme
Valeur recommandée	VRAI
Cote de risque de sécurité	9.8
Impact fonctionnel	(Critique) Cette correction applique la validation des requêtes JavaScript côté client lancées sur le Now Platformfichier . Il y a un impact potentiel si le client a des personnalisations qui incluent des requêtes JavaScript codées en dur pour effectuer des opérations CRUD.
Risque de sécurité	(Critique) Le Now Platform fournit une grande variété de fonctions et de fonctionnalités via des requêtes JavaScript.

Attribut	Description
	Cependant, en l'absence d'autorisation et de validation appropriées, il est possible qu'un attaquant effectue des opérations non autorisées contre la plateforme.
Références	Configuration de la propriété de bac à sable de script `glide.script.use.sandbox` appartient à la même famille de propriétés qui sécurisent et restreignent l'exécution des scripts provenant du client : • `glide.script.allow.ajaxevaluate`: voir Activer AJAXEvaluate. • `glide.script.secure.ajaxgliderecord`: voir Activation de la vérification de l'ACL de AJAXGlideRecord.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Convertir les images des e-mails entrants en pièces jointes [supprimé dans Security Center 1.5]

Utilisez cette `glide.email.inbound.convert_html_inline_attachment_references` propriété pour spécifier si le code HTML de l'e-mail entrant doit être converti afin que les images de l'e-mail apparaissent dans l'aperçu HTML du corps de l'e-mail.

Les actions suivantes se produisent lorsque la `glide.email.inbound.convert_html_inline_attachment_reference` propriété système est définie sur false :

- Dans le , des Now Platformliens cid (content ID) rompus apparaissent à la place des images reçues. Le format dans lequel l'image de l'e-mail apparaît dépend du paramètre de propriété au moment de la réception de l'e-mail, et non du paramètre de propriété actuel.
- Le contenu « malveillant » reçu dans la pièce jointe n'est pas référencé dans le code HTML de l'e-mail. La pièce jointe elle-même est stockée dans la table sys_attachment.
- Le traitement des e-mails entrants ne mettra pas à jour les données HTML de l'e-mail pour refléter l'emplacement stocké de la pièce jointe dans la table sys_attachment. Il en résulte ce qui suit :
  - Les images en ligne n'apparaissent pas dans l'affichage d'e-mail du formateur d'activité.

    Remarque :
    Pour résoudre ce problème avec le formateur d'activité, vérifiez d'abord s'il n'existe aucun problème de sécurité. Définissez ensuite la `glide.email.inbound.convert_html_inline_attachment_reference` propriété système sur **vrai** pour permettre aux futurs e-mails reçus de contenir l'URL HTML nécessaire pour référencer l'image. La modification de la propriété ne met pas à jour les e-mails déjà reçus. La nouvelle valeur affecte uniquement les e-mails entrants reçus après la modification de la propriété.

  - Les images en ligne n'apparaissent pas lorsque l'e-mail est affiché dans l'aperçu HTML de l'e-mail.
  - Lors de l'ajout d'email.body_htm dans des actions entrantes entre des balises de code, les images sont manquantes.

Prérequis

Avant de définir cette propriété, définissez-la `glide.email.read.active` sur vrai. Pour en savoir plus, consultez Enable using your own POP3 server .

En savoir plus

Attribut	Description
Nom de la propriété	`glide.email.inbound.convert_html_inline_attachment_refere`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	Pour restreindre le rendu de l'image dans l'aperçu du corps HTML.
Valeur recommandée	faux
Cote de risque de sécurité	5.4
Impact fonctionnel	(Moyen) Une fois cette propriété configurée, l'utilisateur ne peut pas voir l'aperçu de l'image dans le corps de l'e-mail.
Risque de sécurité	(Moyen) Si la propriété n'est pas activée, un attaquant peut envoyer une image malveillante contenant des logiciels malveillants.
Références	Email properties Inbound mail configuration

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property

Désactiver AJAXEvaluate

Utilisez le `glide.script.allow.ajaxevaluate` pour 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 d'exonération, 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, assainissement et encodage
Objectif	Pour empêcher un utilisateur d'exécuter des scripts avec un privilège d'administrateur.

Attribut	Description
Valeur recommandée	Faux
Type de configuration	Booléen
Impact fonctionnel	(Moyen) Cette correction 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 des scripts clients dans le bac à sable, mais il existe plusieurs propriétés supplémentaires qui peuvent permettre de développer ou de désactiver entièrement 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 des scripts provenant du client : • `glide.script.use.sandbox`: voir Bac à sable pour les scripts générés par le client. • `glide.script.allow.ajaxevaluate`: voir Activer AJAXEvaluate.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Désactiver l'expansion des entités [Mise à jour dans Security Center 1.5]

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 XML termine l'analyse, mais n'inclut aucune entité interne ou externe.

- Si vous définissez cette propriété sur **vrai**, toutes les entités externes tentent de résoudre ou de développer les entités sujets, sous réserve de la définition de la `glide.stax.whitelist_enabled` propriété.
- Si vous définissez cette propriété sur **faux**, toute la résolution et l'expansion de l'entité sont bloquées. Pour plus d'informations, consultez Validation d'entités XMLdoc2 avec liste blanche.

Prérequis

Avant de définir cette propriété :

- Définissez les `glide.xml.entity.whitelist.enabled` propriétés and `glide.stax.whitelist_enabled` sur true. Pour plus d'informations, consultez Validation d'entité XMLdoc/XMLUtil avec liste blanche et Validation d'entité XMLdoc2 avec liste blanche.
- Définissez une liste de noms de domaine complets délimités par des virgules dans la `glide.xml.entity.whitelist` propriété, qui sont les seules URL atteignables à l'aide du processus XML Entity. Pour en savoir plus, consultez Traitement d'entité externe XML - liste blanche.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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	Authentification
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre une attaque d'expansion d'entité XML/d'un milliard de rires.
Valeur recommandée	faux
Impact fonctionnel	(Faible) Si la personnalisation utilise l'expansion de l'entité, la peut bloquer le Now Platform traitement ultérieur.
Risque de sécurité	(Critique) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources du système.
Solution de contournement	Si la personnalisation nécessite une expansion de l'entité, définissez cette propriété sur true et suivez les étapes documentées dans Validation de l'entité XMLdoc2 avec liste blanche.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property.

Pour plus d'informations sur les ressources OWASp, consultez OWASp.

Désactiver l'URL de contenu externe

Gérez la façon dont les métadonnées des liens externes sont utilisées dans votre instance avec la Messagerie instantanée de Connexion.

Utilisez cette 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 rendue. Si la valeur est définie sur **vrai** , Connect Chat les métadonnées de liens externes sont récupérées à partir de sources telles que YouTube ou des articles d'actualités pour afficher des messages plus riches. Cela pourrait conduire à des attaques de falsification de requête côté serveur (SSRF).

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

Attribut	Description
Valeur recommandée	faux
Valeur par défaut	VRAI
Catégorie	Validation, assainissement et encodage
Risque de sécurité	• Score de gravité : 8,1 • 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

La *glide.ui.attachment.download_mime_types* propriété forcera la liste spécifiée des types de fichiers dangereux à être téléchargée sur le client et non affichée dans le navigateur.

Si le type MIME d'un fichier est présent dans le, le *glide.ui.attachment.download_mime_types* téléchargement est forcé. 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.

Pour afficher une liste des types MIME existants, tapez `/sys_attachment_icon_rule_list.do`. Vous pouvez activer l'un de ces types MIME pour satisfaire aux exigences de conformité de sécurité dans le Now Platform.

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*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	En maintenant correctement la liste des types de fichiers dangereux qui ne peuvent pas être affichés dans le navigateur, vous éviterez les attaques de script de site à site (XSS).
Valeur recommandée	Liste des types MIME applicables ou 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.

Attribut	Description
Impact fonctionnel	(Faible) Cette correction impose l'exécution de contrôles de validation avant d'effectuer une action lorsque vous cliquez sur une pièce jointe dans une Now 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 involontaire dans la pièce jointe du côté de la victime pour capturer des informations sensibles. La possibilité d'avoir des XSS peut conduire à une élévation 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 de pièces jointes séparés par des virgules qui ne doivent pas être affichés en ligne dans le navigateur.
Cote de risque de sécurité	6.3
Propriétés connexes	• *glide.ui.attachment.force_download_all_mime_types* • *glide.ui.attachment.tables_ignore_force_download*
Références	Forcer le téléchargement des types MIME.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Définir les types MIME téléchargeables restreints [supprimé dans Security Center 1.5]

Utilisez cette propriété pour télécharger les *glide.ui.attachment.force_download_all_mime_types* types MIME et pour ne pas effectuer le rendu en ligne dans 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.

Pour afficher une liste des types MIME existants, tapez /sys_attachment_icon_rule_list.do. Vous pouvez activer l'un de ces types MIME pour satisfaire aux exigences de conformité de sécurité dans le Now Platform.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.attachment.force_download_all_mime_types*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	Pour empêcher l'affichage des types de fichiers dans le navigateur afin d'éviter toute exécution de script malveillante cachée.

Attribut	Description
Cote CVSS	8
Valeur recommandée	Vrai
Impact fonctionnel	(Faible) Cette correction impose l'exécution de contrôles de validation avant d'effectuer une action lorsque vous cliquez sur une pièce jointe dans une Now Platform application. Il n'y a pas d'impact potentiel, mais l'expérience utilisateur est altérée.
Risque de sécurité	(Élevé) Les vecteurs d'attaque de scripting côté client se déclinent en différents types et l'abus de pièce jointe de type MIME ne fait pas exception. Les attaquants peuvent abuser des types MIME et placer du contenu de script involontaire dans la pièce jointe du côté de la victime pour capturer des informations sensibles. La possibilité d'avoir des XSS peut conduire à une élévation 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 de pièces jointes séparés par des virgules qui ne doivent pas être affichés en ligne dans le navigateur. Exemples : text/html, text/csv
Liens connexes	Forcer le téléchargement des types MIME.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Désactiver le code HTML intégré

Utilisez cette propriété pour désactiver la *glide.ui.security.allow_codetag* prise en charge de l'incorporation du code HTML créé à l'aide de la balise [code].

Il Now 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 des entrées au format HTML pour les champs de journal. Toutefois, les champs journal peuvent afficher du texte encadré par des balises de code au format HTML.

- Cependant, il existe un risque de sécurité associé. Si la valeur est définie sur vrai, les utilisateurs malveillants peuvent écrire du code HTML JS nuisible qui peut être exécuté sur un autre navigateur client après le rendu des champs de journal.
- Définissez cette propriété sur false afin que les administrateurs puissent empêcher les champs 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, assainissement et encodage
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Protégez-vous contre le script site à site et l'exécution de scripts malveillants
Valeur recommandée	faux
Cote de risque de sécurité	4.2
Impact fonctionnel	(Moyen) Cette correction applique le codage HTML sur l'interface utilisateur et renvoie les résultats codés à l'utilisateur. Cette propriété est définie sur `true` par défaut. Dans cet état, votre instance affiche le rendu HTML dans les champs et formulaires de journal. Si cette propriété est définie sur `false`, le HTML n'est pas restitué correctement et des balises HTML peuvent apparaître dans les champs 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 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

Utilisez la *`com.glide.cs.html.sanitizer.enabled`* propriété pour activer HTMLSanitizerService.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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, assainissement et encodage

Attribut	Description
Objectif	Empêche l'application contre les attaques de script de site à site et d'injection HTML.
Valeur recommandée	VRAI
Cote de risque de sécurité	8
Impact fonctionnel	(Élevé) 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 grâce à l'encodage de sortie des données.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à 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 de Jelly.

Lorsque vous définissez la propriété sur **true**, une application passe par une arborescence de script Jelly (imbriquée). Il enveloppe les expressions Jelly potentiellement dangereuses avec un filtre qui :

- Échappe à ses 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 d'exonération, 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, assainissement et encodage
Objectif	Pour atténuer les attaques d'exécution de code malveillant qui peuvent se produire à l'aide de Jelly Injection.
Valeur recommandée	Vrai
Cote de risque de sécurité	9
Impact fonctionnel	(Élevé) Cette propriété permet de deviner si une expression est entre guillemets. Il peut citer à tort une expression légitime. Dans

Attribut	Description
	ce cas, il peut être nécessaire de marquer manuellement une expression comme sûre.
Risque de sécurité	(Modéré) L'injection JEXL est une forme d'injection d'entrée unique qui Now Platform peut conduire à la fois à la falsification de requête intersite et à l'exécution 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 le préfixe SAFE à l'expression Jelly : `${SAFE :sysparm_input} ;` L'ajout aveugle de SAFE à chaque expression n'est pas la bonne façon d'aborder le problème, car cela peut ouvrir une faille de sécurité. • Ajoutez SAFE à une expression uniquement 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 l'évaluation du JavaScript privilégié.
Références	Balises Jelly Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Activer la protection de l'interpolation Jelly JS pour les expressions imbriquées

Gérez la protection contre l'interpolation sur votre instance.

Utilisez la propriété pour gérer la protection contre l'interpolation*`glide.ui.jelly.js_interpolation.protect_nested_expressions`*. La protection contre l'interpolation garantit que lorsque des expressions Jelly sont utilisées en JavaScript, elles doivent être considérées comme sûres soit en relevant de certaines catégories, soit 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 entraîner l'évaluation du 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 **recommandée vrai,** les expressions Jelly malveillantes interpolées dans JavaScript sont autorisées et un utilisateur peut exécuter du code à l'aide d'un modèle Jelly.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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_expressior*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Validation, assainissement et encodage
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

Utilisez cette propriété pour appliquer des *glide.cms.catalog_uri_relative* liens relatifs à partir du paramètre URI sur /ess/catalog.do.

- Lorsqu'elle est définie sur **vrai**, seules les URL relatives sont autorisées via la page /ess/catalog.do à l'aide du *uri* paramètre.
- Lorsqu'elle est définie sur **faux**, toutes les URL sont autorisées, ce qui peut permettre la liaison à du contenu externe non autorisé.

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, assainissement et encodage
Objectif	Pour limiter les tentatives de lier du contenu externe non autorisé.
Valeur recommandée	VRAI
Cote de risque de sécurité	2.6
Impact fonctionnel	(Faible) 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

Attribut	Description
	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 Add a system property .

Appliquer la vérification de la liste d'autorisations d'URL

Utilisez cette `glide.security.url.whitelist` propriété pour ajouter une validation supplémentaire afin de garantir que toute URL externe introduite doit faire partie des URL sur liste d'inclusion.

La redirection ouverte se produit lorsqu'une page Web vulnérable est redirigée vers une page non fiable et malveillante susceptible de compromettre l'utilisateur. Les attaques de redirection ouverte s'accompagnent d'une attaque de phishing, car le lien vulnérable modifié est identique au site d'origine, ce qui augmente les chances de succès de l'attaque de phishing.

Cette propriété est applicable dans les cas suivants :

- `/logout.do ?sysparm_goto_url={URL externe}`
- `/cms_login_redirect.do ?sysparm_goto_url={URL externe}`

Les utilisateurs sont dirigés vers un site de confiance externe après s'être déconnectés de l'instance :

- `/logout_redirect.do ?sysparm_url={URL externe}`
- `/saml_redirector.do ?sysparm_uri={URL externe}`

Lorsque SAML est activé, il appelle une URL de déconnexion du fournisseur d'identité (IDP).

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.url.whitelist`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	Pour implémenter la redirection d'URL sécurisée lors de la connexion, de la déconnexion ou d'autres redirections. Cette propriété atténue l'une des 10 principales attaques OWASP appelées Redirections et transferts invalidés.
Type	Chaîne
Valeur	URL approuvées de votre organisation [certains FQDN (nom de domaine complet) définis, par ex. http://www.servicenow.com]
Cote de risque de sécurité	8.3
Impact fonctionnel	(Moyen) 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.

Attribut	Description
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 pour la sécurité.
Références	Erreurs et correctifs de Multi-SSO (SAML 2.0)

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Formules Excel d'échappement [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour empêcher l'injection Excel, également connue sous le `glide.export.escape_formulas` nom d'injection de formule.

L'injection Excel se produit lorsque des sites Web intègrent des entrées non fiables dans des fichiers Excel. Lorsque vous utilisez un tableur tel que Microsoft Excel ou LibreOffice Call pour ouvrir un fichier, toutes les cellules commençant par +, -, = ou @ sont interprétées comme une formule. Lorsque vous définissez la propriété sur **true**, les `glide.export.escape_formulas` valeurs de chaîne commençant par +, -, = ou @ sont précédées d'une apostrophe unique lorsque vous exportez vers des fichiers CSV, XLS ou XLSX.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.export.escape_formulas`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	Pour empêcher l'application par rapport à l'injection d'Excel ou de formule.
Valeur recommandée	VRAI
Cote de risque de sécurité	6.5
Impact fonctionnel	(Faible) 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 pas d'informations sensibles, car elles peuvent être utilisées pour compromettre l'ordinateur de l'utilisateur.
Solution de contournement	Comme alternative, envisagez de supprimer tous les espaces blancs 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 Add a system property .

HTML d'échappement dans les vues de listes

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.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ fournit la fonctionnalité de mise en forme du contenu à l'aide de codes HTML (par exemple, <p>, , <a href>, <b><font><img>,). Un utilisateur malveillant peut injecter du code HTML dans le champ de formulaire pour exécuter des scripts indésirables sur différentes sessions client/utilisateur.

- Définissez cette propriété sur **faux** pour effectuer un échappement HTML avant que les enregistrements/champs ne soient restitués dans le navigateur lorsque la table apparaît en tant que vue de liste.
- Si la valeur est définie sur **vrai** et que vous sélectionnez cette colonne dans une vue de liste lors de l'affichage d'une liste de tables ou d'enregistrements, ces champs au format HTML peuvent apparaître.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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_html_list_field*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	Pour prévenir les attaques de script de site à site contre les applications
Valeur recommandée	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Moyen) Cette correction applique l'encodage HTML à se produire sur l'interface utilisateur au niveau de l'analyseur HTML et renvoie ainsi les résultats codés à l'utilisateur. Elle peut avoir un impact sur les fonctionnalités 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 les sessions des utilisateurs 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 Add a system property .

Échapper à JavaScript

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.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ permet à l'utilisateur de mettre en forme le contenu à l'aide de codes HTML (par exemple, <p>, , <a href>, <b><font><img> ,). Si vous définissez la propriété sur *glide.html.escape_script***false**, les balises (<script></script>) peuvent apparaître lorsque vous sélectionnez cette colonne dans une vue de liste tout en consultant une liste de tables ou d'enregistrements.

Un attaquant malveillant peut insérer du code JavaScript en l'intégrant dans les balises (<script></script>). L'attaquant peut en tirer parti en injectant un vecteur JS sophistiqué qui peut s'exécuter lorsqu'un utilisateur ouvre l'enregistrement de table.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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.html.escape_script*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	Pour éviter les attaques de script de site à site contre une application.
Valeur recommandée	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Moyen) Cette correction applique l'échappement JavaScript sur l'interface utilisateur et renvoie les résultats codés 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 de l'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 Add a system property .

Script Jelly d'échappement

Utilisez cette propriété pour forcer l'échappement `glide.ui.escape_all_script` de tous les scripts injectés dans Jelly.

Il 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 empêche plusieurs problèmes XSS de se produire.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.escape_all_script`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	Si la propriété n'est pas définie sur **true**, 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 le rendu sur les pages Web et l'exécution de l'échappement sur chacune des balises suivantes : $â {JS :expression} $â {HTML :expression} OU $â {JS,HTML :expression}
Valeur recommandée	VRAI
Cote de risque de sécurité	7.3
Impact fonctionnel	(Moyen) Cette correction applique l'échappement de Jelly au niveau de l'analyseur. Cela peut avoir un impact fonctionnel sur l'interaction de l'utilisateur avec les données résultantes.
Risque de sécurité	(Élevé) La validation d'entrée doit avoir lieu 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 des scripts et balises HTML conçus pour le rendu sur une page Web peuvent sembler défectueux. Cette correction envoie la page codée de sortie au navigateur pour qu'il effectue le rendu. Par exemple, au lieu de « ma chaîne ici », il peut afficher « <u>ma chaîne ici</u> » car la <u> balise a été correctement échappée. Dans ce cas, pour éviter les échappements, ajoutez le préfixe NOESC à

Attribut	Description
	l'expression Jelly pour empêcher l'échappement JS. Par exemple : • Avant : ($[jvar_context_menus]) ; • Après : ($[NOESC :jvar_context_menus]) ; • Avant : $[jvar_ui_policy_scripts] • Après : $[NOESC :jvar_ui_policy_scripts]
Références	Paramètres de sécurité élevée Balises Jelly

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Scripts d'échappement dans le bloc-notes

Découvrez comment le bloc-notes prend en compte 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, **vrai**, 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, assainissement et encodage
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
Références	Workflow administration

Balisage XML d'échappement

Utilisez cette 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 cross-site scripting se produit lorsqu'un attaquant injecte du code 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, échapper signifie ce qui suit :

- **&** --> &
- **<** --> <
- **>** --> >
- **«** --> »
- **'** --> '
- **/** --> /

Exemple : <![CDATA[<script>alert('Attaque XSS') ;]] >

Échappement : <script>alert('XSS Attack') ; </script>

Assurez-vous que la `glide.ui.escape_text` propriété existe dans la table sys_properties et qu'elle est définie sur vrai.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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, assainissement et encodage
Objectif	L'échappement XML empêche les navigateurs d'analyser le code JavaScript malveillant incorporé dans des données non approuvées et de l'exécuter 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, il faut que cette propriété soit définie sur **true**.
Valeur recommandée	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Moyen) Cette correction applique le codage XML au niveau de l'analyseur XML sur l'interface utilisateur. Il restitue les

Attribut	Description
	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 de l'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 que vous avez défini cette propriété sur **vrai**, le rendu s'arrête sur les balises HTML dans la description de l'élément de catalogue ou dans le texte d'aide de la variable d'élément de catalogue. Il se peut que vous ne puissiez pas utiliser le formatage HTML pour certains champs.
	
	Toutefois, si la `glide.ui.escape_text` propriété est désactivée, toutes les expressions JEXL sont préfixées d'un encodeur de sortie :
	
	`${JS :expression}`
	
	`${HTML :expression}`
	
	ou
	
	`${JS,HTML :expression}`

Échapper à la réponse XML

Gérez la façon dont les caractères d'échappement 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 sont 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
Catégorie	Validation, assainissement et encodage
Risque de sécurité	• Score de gravité : 6,4 • Score CVSS : moyen

Attribut	Description
	• Détails du risque de sécurité : définir cette propriété sur **faux** désactive l'échappement XML, ce qui peut entraîner une attaque par injection XML.
Dépendances et prérequis	Aucun

Activer l'assainisseur HTML [Mise à jour dans Security Center 1.5]

Utilisez cette *glide.html.sanitize_all_fields* propriété pour activer l'include de script HTMLSanitizer, qui nettoie l'entrée HTML selon les attributs mis sur liste d'exclusion et d'inclusion configurés dans un script.

Les types de champs disponibles avec le dictionnaire/les champs incluent HTML et HTML traduit. Ces champs d'entrée HTML permettent aux utilisateurs d'écrire une entrée au format HTML, par exemple :

<h1>Test</h1>), à l'aide des 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, assainissement et encodage
Objectif	Empêche l'application contre les attaques de script de site à site et d'injection HTML
Valeur recommandée	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Élevé) 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 grâce à l'encodage de sortie des données.
Solution de contournement	Cette propriété nettoie tous les champs HTML du système. Si vous devez activer l'assainissement

Attribut	Description
	HTML sur des champs individuels, voir Activer l'assainissement sur des champs individuels. Vous pouvez également configurer la liste d'inclusion ou la liste d'exclusion pour assainir les balises et attributs 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 Add a system property .

Restreindre les packages Java autorisés

La configuration de ces propriétés protège contre l'exposition d'API dangereuses au moteur de scripting.

Configurez les tables système et installez le module d'extension recommandé en conséquence.

Si la table et `sys_whitelist_package` ne sont pas des `sys_whitelist_member` valeurs vides, les API dangereuses peuvent être exposées au moteur de script. 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 d'appel de packages. Consultez Outil de suppression d'appel de packages pour en savoir plus.

Contact Service et assistance client pour modifier ces tables.

En savoir plus

Attribut	Description
Table, nom du module d'extension	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, assainissement et encodage
Objectif	Protégez-vous contre l'exposition d'API dangereuses au moteur de scripting.
Valeur recommandée	Vide
Type de configuration	liste de tables, module d'extension
Impact fonctionnel	

Attribut	Description
Risque de sécurité	(Élevé) Des API dangereuses peuvent être exposées au moteur de scripting. Ces API prises en charge risquent de créer une instabilité et une 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 Add a system property .

Outil de suppression d'appel de packages

Activez et exécutez le module d'extension Packages Call Removal Tool (`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 plugin qui :

- Analyse les scripts à la recherche d'appels de packages aux Now Platform classes Java.
- Propose des changements pour les remplacer par des 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 signale les appels Packages,xxx.

L'outil de suppression d'appels de packages peut signaler certains appels de packages utilisés dans sa_mapping_ext_commands et sa_custom_operation. Ces appels de package appartiennent au MID Server. Comme il n'y a pas de classes, le code s'exécute dans MID Server. Si vous trouvez l'un des appels de package répertoriés suivants dans la section Erreurs, marquez-les 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`

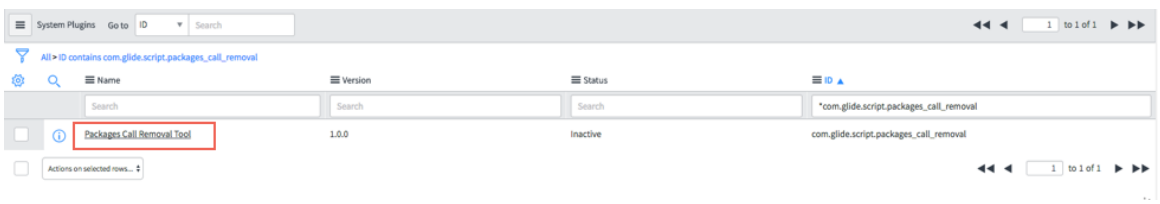
En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.script.packages_call_removal
Type de configuration	Définition du système > Modules d'extension
Objectif	Pour supprimer/remplacer les appels de packages/membres non autorisés par des noms Glide acceptables (GlideScriptable) qui n'autorisent qu'un accès autorisé aux données.
Valeur recommandée	Actif
Impact fonctionnel	(Faible) 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

Attribut	Description
	de cela, il fournit des suggestions qui sont stockées dans la table packages_call_item. Votre administrateur peut alors décider d'accepter ou de rejeter le changement proposé.
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.

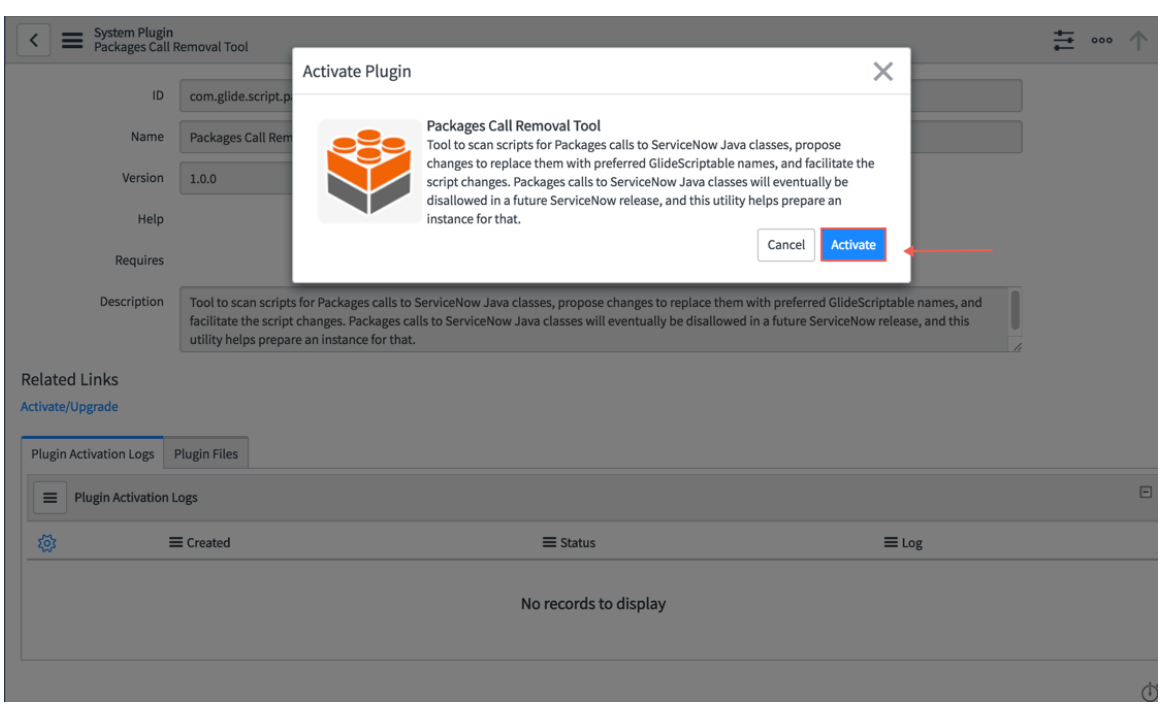
Étapes de configuration

1. Accédez à la **Définition du système** > **Modules d'extension**



2. Recherchez 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

4. Pour vérifier les appels de package sur liste d'inclusion et les appels de membres sur liste d'inclusion, effectuez les actions décrites dans les sections Étapes de configuration des rubriques suivantes :
   - Vérifier les appels des membres de la liste d'autorisation
   - Vérifier les appels de package sur la liste d'autorisation

Annuler le nom distinctif initial LDAP [mis à jour dans Security Center 1.3]

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 correctif prêt à l'emploi (OOB). Si elle est définie sur la valeur recommandée « » ou vide, les données du serveur LDAP peuvent être énumérées par un utilisateur ayant des privilèges inférieurs.

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, assainissement et encodage
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Détails du risque de sécurité : si la définition de la valeur de la propriété sur « » ou sur un champ vide peut rendre les données du serveur LDAP accessibles à un utilisateur ayant des privilèges inférieurs.
Dépendances et prérequis	Aucun

Appliquer la sécurité stricte des cookies de session

Utilisez la propriété pour exiger des `glide.ui.secure_cookies` 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 d'exonération, 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, assainissement et encodage
Objectif	Pour obtenir une authentification de session plus sécurisée.
Valeur recommandée	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Faible) 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 Add a system property .

Minimiser le seuil d'expansion des entités [Mise à jour dans Security Center 1.5]

Utilisez cette `glide.xmlutil.max_entity_expansion` propriété pour réduire la limite maximale d'expansion de l'entité.

Le Now Platform ne traite pas les expansions d'entité ultérieures supérieures à la limite autorisée spécifiée dans cette propriété.

Remarque :
500 est le minimum par défaut imposé par le Now Platform, qui est considéré comme un seuil sécurisé.

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, assainissement et encodage
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre les attaques XML Entity Expansion/Billion Laugh.
Valeur recommandée	3000
Cote de risque de sécurité	5.3
Impact fonctionnel	(Faible) Si la personnalisation utilise l'extension d'entités volumineuses, le peut bloquer le Now Platform traitement ultérieur.
Risque de sécurité	(Modéré) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources du système.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Restreindre les types MIME chargés [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour activer la `glide.security.file.mime_type.validation` vérification du type MIME pour les chargements. Vous pouvez activer (propriété sur **true**) ou désactiver (définir la propriété sur **false**) pour les fichiers en pièces jointes.

Prérequis

Avant de définir cette propriété, définissez-la `glide.attachment.extensions` .
Le type MIME est vérifié uniquement pour les extensions spécifiées dans `glide.attachment.extensions` lors du chargement. Pour en savoir plus, consultez Restrict file extensions .

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, assainissement et encodage
Objectif	Pour appliquer la vérification du type MIME / des octets magiques pendant les chargements de fichiers.
Valeur recommandée	VRAI
Cote de risque de sécurité	5.4
Impact fonctionnel	(Moyen) Cette correction permet la vérification du 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 téléchargements de fichiers malveillants, la vérification du type MIME doit être activée.
Références	Administering attachments

Consultez Paramètres de la sécurisation pour la sécurité de l'instance pour plus d'informations 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 Add a system property .

Restreindre les entités externes XML

Utilisez cette propriété pour activer la `glide.security.file.mime_type.validation` vérification du type MIME pour les chargements. Vous pouvez activer (propriété sur **true**) ou désactiver (définir la propriété sur **false**) pour les fichiers en pièces jointes.

Prérequis

Avant de définir cette propriété, définissez-la `glide.attachment.extensions` .
Le type MIME est vérifié uniquement pour les extensions spécifiées dans `glide.attachment.extensions` lors du chargement.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	Ce contrôle de correction doit être activé pour assurer la défense contre les attaques XXE.
Valeur recommandée	VRAI
Cote de risque de sécurité	5.4
Impact fonctionnel	(Faible) Si la personnalisation utilise une entité externe, et non une inclusion répertoriée dans la propriété, la Now Platform peut bloquer le `glide.xml.entity.whitelist` 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

Si les personnalisations ne nécessitent pas d'expansion d'entité, utilisez la propriété pour désactiver complètement l'expansion d'entité `glide.xmlutil.max_entity_expansion` externe. Le XML termine l'analyse, mais n'inclut aucune entité interne ou externe.

- Si vous définissez cette propriété sur **vrai**, toutes les entités externes tentent de résoudre ou de développer les entités sujets, sous réserve de la définition de la `glide.stax.whitelist_enabled` propriété.
- Si vous définissez cette propriété sur **faux**, toute la résolution et l'expansion de l'entité sont bloquées. Pour en savoir plus, consultez Validation d'entité XMLdoc2 avec liste d'autorisation.

Prérequis

Avant de définir cette propriété :

- Définissez les *glide.xml.entity.whitelist.enabled* propriétés and *glide.stax.whitelist_enabled* sur true. Pour en savoir plus, consultez Validation d'entité XMLdoc/XMLUtil avec liste d'autorisation et Validation d'entité XMLdoc2 avec liste d'autorisation.
- Définissez une liste de noms de domaine complets délimités par des virgules dans la *glide.xml.entity.whitelist* propriété, qui sont les seules URL atteignables à l'aide de la propriété de traitement Entité XML. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.

⚠ Avertissement :
Il s'agit d'une propriété d'exonération, 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.xmlutil.max_entity_expansion*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, assainissement et encodage
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre une attaque d'expansion d'entité XML/d'un milliard de rires.
Valeur recommandée	faux
Cote de risque de sécurité	9.8
Impact fonctionnel	(Faible) Si la personnalisation utilise l'expansion de l'entité, la peut bloquer le Now Platform traitement ultérieur.
Risque de sécurité	(Critique) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources du système.
Solution de contournement	Si la personnalisation nécessite une expansion de l'entité, définissez cette propriété sur true et suivez les étapes documentées à la section Validation d'entité XMLdoc2 avec liste d'autorisation.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

Pour plus d'informations sur les ressources OWASp, consultez OWASp .

Définir une politique de sécurité du contenu sécurisé 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 les SVG (Scalable Vector Graphics) sont accessibles via l'extension de fichier IIX (Translation Memory Index).

Cette propriété empêche les *com.glide.csp.self_script_src_svg* pièces jointes malveillantes qui stockent des attaques de script de site à site (XSS) de s'exécuter dans une instance. Sans cette politique, un acteur malveillant pourrait amener un utilisateur à

exécuter du code JavaScript arbitraire dans son navigateur Web, ce qui pourrait entraîner des failles 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, assainissement et encodage
Risque de sécurité	• Score de gravité : 7,1 • Score CVSS : élevé • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur la valeur recommandée, vrai, un utilisateur peut exécuter du code JavaScript arbitraire provenant 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.

Gestion et chiffrement des clés

Le chiffrement est une procédure cryptographique qui convertit le texte brut en texte chiffré pour contrôler la divulgation d'informations.

Vue d'ensemble

ServiceNow La gestion des clés comprend les activités impliquant la manipulation des clés cryptographiques et des paramètres de sécurité associés pendant le cycle de vie de la clé de bout en bout, et constitue un contrôle efficace basé sur les directives 800-57 du National Institute of Standards and Technology (NIST).

Le chiffrement est utilisé pour convertir des chaînes de caractères en texte brut en texte chiffré, qui reste indéchiffrable sans accès à la clé correcte. Les avantages du chiffrement en matière de sécurité découlent de la combinaison d'algorithmes puissants et d'une gestion des clés de qualité.

Le chiffrement de toutes les informations n'est peut-être pas nécessaire pour toutes les données et augmenterait considérablement le temps de traitement en raison du grand nombre de données prises en charge dans toutes les applications. Lorsque vous déterminez que le chiffrement des données est nécessaire, les options suivantes Now Platform sont disponibles :

servicenow

Premiers pas

Cadre de travail de gestion des clés (KMF)

L'API

[qa: BEGIN review][End]

/UX Key Management Framework (KMF) vous permet de personnaliser et de gérer entièrement la façon dont les opérations de chiffrement sont effectuées sur votre

[qa: BEGIN review][End]

instance ServiceNow.

Chiffrement au niveau des colonnes (CLE)

Application intégrée qui permet le chiffrement des champs de chaîne, de date, de date/heure ou de pièce jointe à l'aide d'AES-128 ou AES-256 dans les modules de chiffrement.

Entreprise de Chiffrement au niveau des colonnes (CLE_Ent)

Offre une solution de chiffrement plus complète pour Column Level Encryption, comme les clés fournies par le client, l'accès aux scripts via des API, des modules cryptographiques et des politiques d'accès aux modules supplémentaires, etc.

Chiffrement dans le cloud

Cloud Encryption vous permet d'utiliser une

[qa: BEGIN review][End]

clé générée par ServiceNow ou de fournir une clé que vous créez et gérez.

Ensemble d'autorisations Chiffrement de la plateforme

Effectuez une mise à niveau vers Column Level Encryption Enterprise, Cloud Encryption et Database Encryption à utilisation illimitée.

Chiffrement intégral du disque (FDE)

Le chiffrement intégral du disque s'applique uniquement à l'ensemble du système de stockage du serveur de base de données. 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 d'envoyer des données sur Internet à votre

[qa: BEGIN review][End]

instance ServiceNow. Les données restent chiffrées au repos sur l'instance.

Traduction automatique

Informations sur l'activation

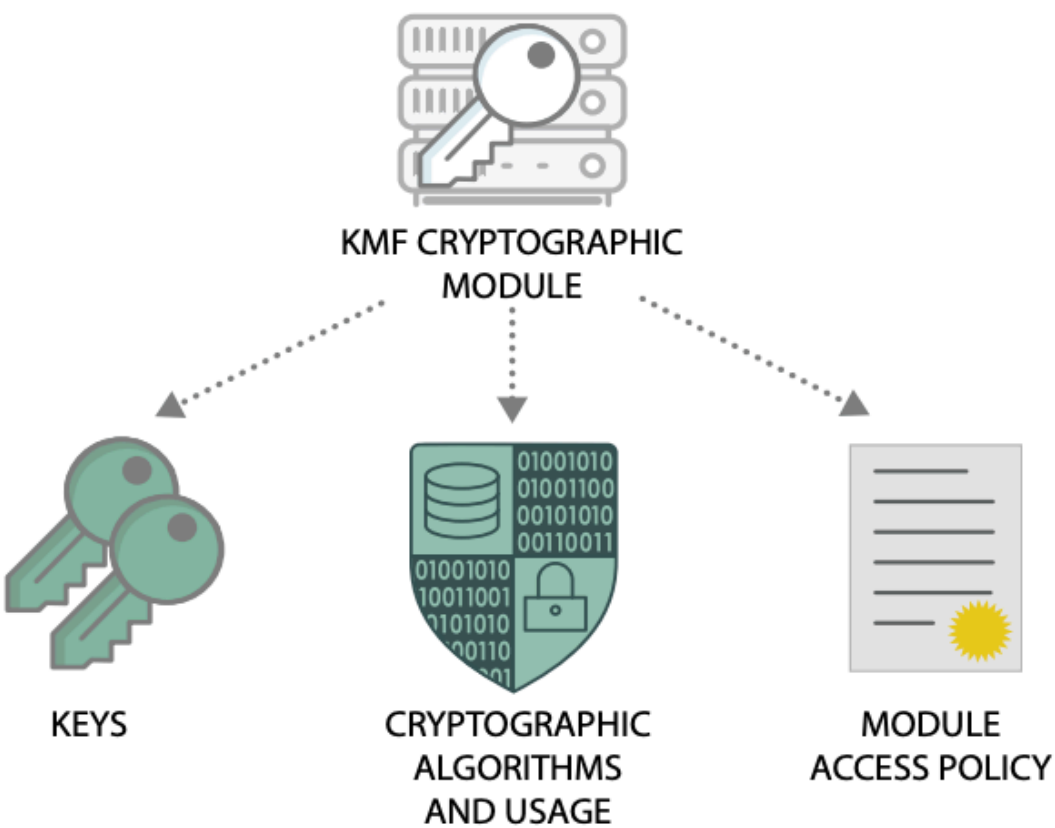
Le ServiceNow lot d'abonnements Chiffrement de la plateforme est une autorisation commerciale de groupe qui inclut Entreprise de Chiffrement au niveau des colonnes, Chiffrement dans le cloudet Chiffrement de base de données.

Entreprise de Chiffrement au niveau des colonnes est la licence illimitée de Chiffrement au niveau des colonnes. Le Chiffrement au niveau des colonnes module d'extension Enterprise est disponible avec l'activation du module d'extension com.glide.now.platform.encryption. Pour plus d'informations, consultez Offre groupée d'abonnements Chiffrement et gestion des clés.

Exploration du cadre de gestion des clés

L'API/UX Key Management Framework (KMF) vous permet de personnaliser et de gérer entièrement la façon dont les opérations de chiffrement sont effectuées sur votre instance. KMF fournit une interface sécurisée et complète pour les services de gestion des clés cryptographiques côté instance.

Vue d'ensemble de Key Management Framework



Ce graphique vous montre les composants qui composent le KMF.

Modules cryptographiques KMF

Les modules cryptographiques sont la pièce maîtresse du KMF. Chaque module de chiffrement sur votre instance définit une méthode de chiffrement pour un cas d'utilisation spécifique. Pour en savoir plus sur ces modules, reportez-vous à la section Vue d'ensemble du module de chiffrement.

Clés

Les clés de chiffrement sont des chaînes de caractères utilisées en cryptographie. Lorsqu'ils sont utilisés avec un algorithme cryptographique, ils peuvent coder ou décoder des données

cryptographiques. Ces clés sont utilisées par vos modules de chiffrement. Vous pouvez choisir d'utiliser une clé générée ou de charger votre propre clé fournie par le client avec Column Level Encryption Enterprise. Pour en savoir plus sur les clés, reportez-vous à la section Clés au niveau de l'instance dans Key Management Framework.

Algorithmes de chiffrement

Les algorithmes cryptographiques sont des procédures de calcul qui utilisent une clé cryptographique pour coder ou décoder vos données. Ces algorithmes sont définis par la configuration de la spécification cryptographique sur votre instance.

Politiques d'accès au module

Les politiques d'accès aux modules sont les mécanismes de contrôle d'accès appliqués aux modules de chiffrement pour définir des contrôles au niveau de l'instance. Ces politiques déterminent les conditions dans lesquelles l'accès est accordé ou refusé aux modules cryptographiques. Pour plus d'informations, consultez Vue d'ensemble de la politique d'accès au module.

Workflow de Key Management Framework

1. Affecter KMF des administrateurs, qui peuvent à leur tour affecter d'autres KMF rôles.
2. Configurez vos paramètres de chiffrement de champ pour sélectionner les ServiceNow clés fournies ou vos propres clés fournies par le client (CSK) pour le chiffrement.
3. Créez des modules cryptographiques pour définir les mécanismes utilisés pour les opérations de chiffrement.
4. Créez une spécification de chiffrement, dans laquelle vous définissez un algorithme de chiffrement et générez une clé.
5. Créez des politiques d'accès au module qui déterminent dans quels contextes vos données peuvent être chiffrées ou déchiffrées.
6. Créez une politique de cycle de vie du module de chiffrement. Ces politiques imposent des limites aux modules de chiffrement au niveau de l'instance, telles que la durée de validité de la clé. Ces stratégies peuvent protéger les modules cryptographiques en limitant leur exposition.

Pour obtenir des détails sur ces processus, reportez-vous à .

Avantages de Key Management Framework

Avantage	Fonctionnalité	Utilisateurs
Protégez vos données sensibles et propriétaires.	Gestion et chiffrement des clés	Tous
Maintenez la conformité aux directives NIST 800-57. Ces directives sont fournies par le National Institute of Standards and Technology pour réduire les risques de cybersécurité pour vos réseaux et vos données.	Gestion et chiffrement des clés	Administrateurs de sécurité
Utilisez Key Management Framework pour générer, charger, afficher et gérer vos clés de chiffrement. Utilisez la rotation des clés pour une rotation manuelle ou programmée de vos clés afin d'accroître la sécurité.	Key Management Framework	Administrateurs de sécurité

Offre groupée d'abonnements Chiffrement et gestion des clés

Grâce à la gestion des clés, Column Level Encryption 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, Platform Encryption, qui inclut Entreprise de Chiffrement au niveau des colonnes et Chiffrement dans le cloud.

Fonctionnalités de Column Level Encryption

Column Level Encryption avec modules de chiffrement est inclus gratuitement dans votre instance et inclut la gestion des clés NIST 800-57 avec les éléments suivants pris en charge :

- ServiceNow Les clés gérées sont prises en charge (les clés fournies par le client ne sont pas prises en charge).
- L'accès aux modules de chiffrement est uniquement basé sur les rôles.
- Rotation manuelle illimitée des touches.
- Un maximum de cinq modules de chiffrement peut exister à un moment donné.
- Un maximum de cinq politiques d'accès aux modules peut exister à un moment donné.
- Les types de champs existants sont pris en charge. (Les nouveaux types de champs créés dans les versions ultérieures ne seront pas pris en charge dans la version hors entreprise.)
- La prise en charge de l'API peut être utilisée en fonction de l'accès aux rôles.
- Audit des actions de chiffrement.
- Visite guidée Chiffrement au niveau des colonnes.

ServiceNow Fonctionnalités du groupe Platform Encryption

Le groupe Chiffrement de la plateforme ajoute les fonctionnalités et offres suivantes :

- Entreprise de Chiffrement au niveau des colonnes :
  - Clés fournies par le client.
  - Rotation automatique des clés.
  - Prise en charge avancée des types de champs et futures mises à jour.

    Remarque :
    La prise en charge des types de champs étendus comprend les types **de champs Journal**, **Liste de journaux**, **Entrée de journal** et **HTML et Traduit (Champ/Texte/HTML).**

  - Prise en charge avancée des pièces jointes.
  - L'accès au module de chiffrement peut être accordé avec une politique d'accès au module basée sur les éléments suivants :
    - Utilisateur système
    - Script
    - Périmètres d'application spécifiques
  - Modules de chiffrement et politiques d'accès aux modules illimités.

Traduction automatique

- Importer une clé à partir d'un service Web.
- Définissez une date de rotation future pour les clés de chiffrement.

- Chiffrement dans le cloud avec Key Management.

Information supplémentaire

Pour en savoir plus sur la gestion des clés, reportez-vous à Comprendre le cadre de gestion des clés.

Comprendre le cadre de gestion des clés

L'API Key Management Framework /UX (KMF) vous permet de personnaliser et de gérer entièrement la façon dont les opérations de chiffrement sont effectuées sur votre ServiceNow instance. Il ServiceNow Key Management Framework fournit une interface sécurisée et complète pour les services de gestion des clés cryptographiques côté instance.

Conformément aux directives NIST 800-57 , KMF fournit les fonctionnalités suivantes :

- Séparation des tâches avec des rôles dédiés à la gestion et aux opérations cryptographiques, à l'audit et à l'intégration
- Les modules de chiffrement permettent de configurer des spécifications de chiffrement à des fins et des types de clé uniques
  - Clé symétrique : chiffrement et déchiffrement, encapsulation et désencapsulation de la clé, et authentification
  - Clé asymétrique : génération et vérification de signature numérique, chiffrement et déchiffrement, encapsulation et désencapsulation de clés
- Gestion du cycle de vie des clés pour générer, faire pivoter, révoquer et suspendre des clés, y compris la prise en charge de plusieurs états de cycle de vie clés
- Mise en application des contrôles d'accès avec des politiques d'accès aux modules, garantissant que l'accès n'est accordé qu'aux modules de chiffrement configurés dans les politiques.
- Protection des clés : racine de confiance (RoT) matérielle FIPS (Federal Information Processing Standard) 140-2-L3, infrastructure à clé publique (PKI), hiérarchie des clés et chiffrement de l'enveloppe
- Audit qui inclut les statistiques d'utilisation clés

Activation de KMF

KMF est actif par défaut.

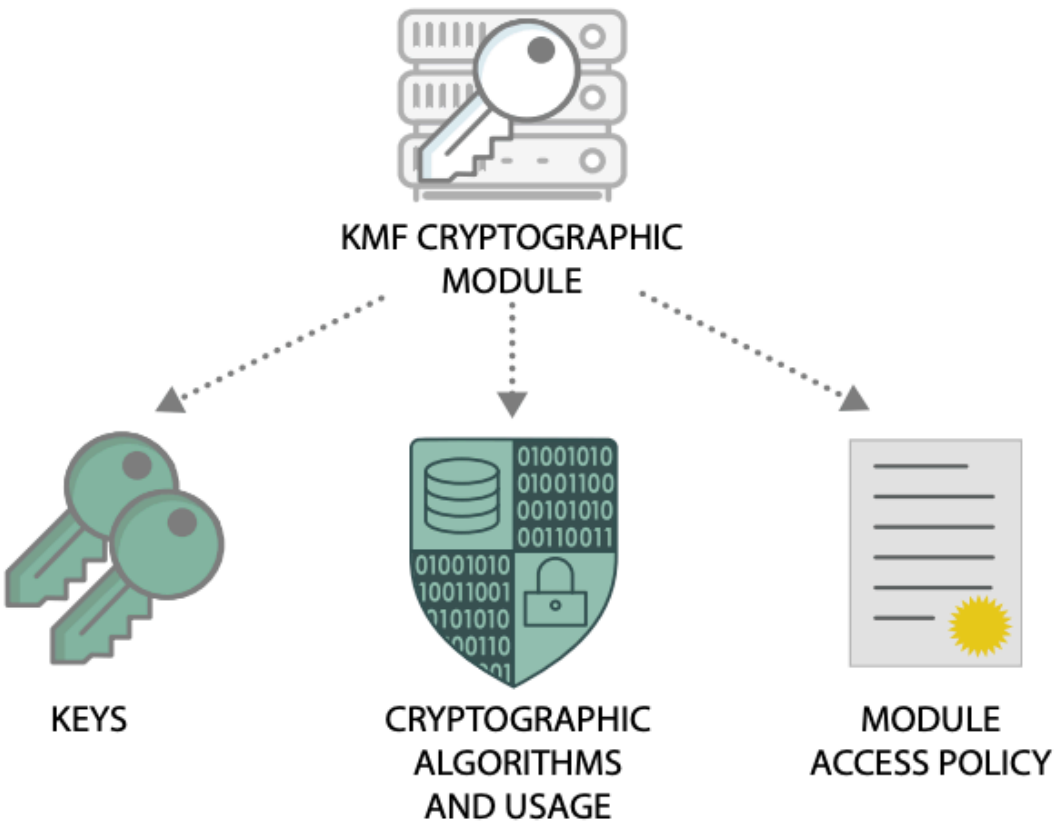
Remarque :
KMF ne prend pas en charge Domain Separation, mais peut être utilisé avec des instances sur site.

Fonctionnement de KMF

Ce graphique vous montre les composants qui composent KMF :

- Les modules cryptographiques sont utilisés pour définir la méthode de chiffrement.
- La spécification cryptographique est une configuration qui définit un algorithme de chiffrement.

- La spécification vous permet également de définir la clé du module, une ServiceNow clé ou votre propre clé fournie par le client.
- Une politique d'accès aux modules est une politique au niveau de l'instance qui régit les conditions dans lesquelles l'accès est accordé ou refusé aux modules de chiffrement.



Pour plus d'informations sur KMF, commencez par Vue d'ensemble du module de chiffrement.

Key Management Framework (KMF) introduit des rôles spécifiques pour les configurations liées au module cryptographique et à la gestion des clés. Seuls les administrateurs KMF peuvent affecter des utilisateurs à d'autres rôles KMF. Consultez Rôles installés avec Key Management Framework pour plus d'informations.

Pour plus d'informations sur l'infrastructure de chiffrement qui succède à CLE, reportez-vous à la section Entreprise de Chiffrement au niveau des colonnes.

Vue d'ensemble du module de chiffrement

Les modules cryptographiques sont la pièce maîtresse de (KMF). Ils définissent les mécanismes de chiffrement spécifiques utilisés pour les opérations de chiffrement pour un cas d'utilisation donné.

Un module de chiffrement applique le mécanisme de chiffrement de votre choix à un cas d'utilisation que vous définissez. Par exemple, si vous souhaitez sécuriser les données de votre application RH 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 de chiffrement, et définir votre méthode de chiffrement. Les modules cryptographiques sont composés des composants suivants :

Spécification cryptographique

Définit les aspects de votre module, y compris son objectif cryptographique et les algorithmes à utiliser.

Clés de chiffrement

Clé que votre module utilise pour coder ou décoder des données de chiffrement. Il peut s'agir d'une clé générée par votre instance ou d'une clé fournie par le client que vous créez et chargez.

Politiques d'accès au module

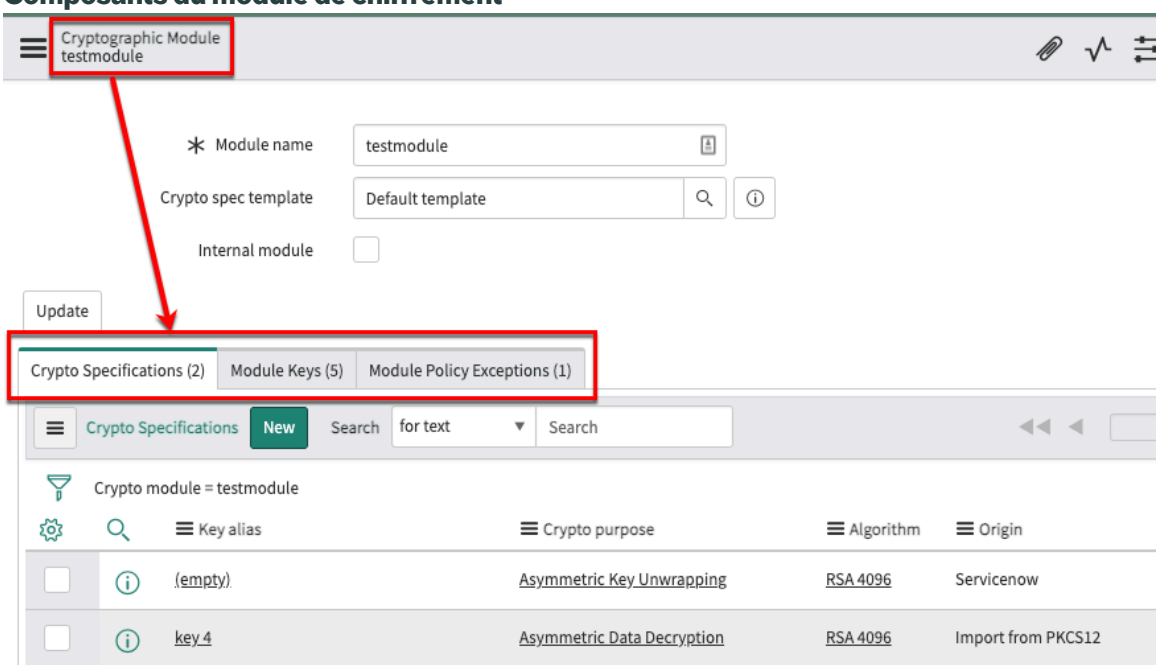
Les politiques d'accès aux modules sont les mécanismes de contrôle d'accès qui limitent le chiffrement ou le déchiffrement des données.

Exceptions de politique de module

Mécanisme de contrôle permettant de définir des exceptions à une politique d'accès au module.

L'écran suivant montre ces composants de haut niveau dans un module de chiffrement :

Composants du module de chiffrement



Pour en savoir plus sur la création de modules de chiffrement, reportez-vous à la section Créer un module cryptographique.

Vue d'ensemble de la politique d'accès au module

Les politiques d'accès aux modules sont les contrôles d'accès que vous appliquez à vos modules de chiffrement pour définir des contrôles au niveau de l'instance.

Politiques d'accès au module

Les politiques d'accès aux modules sont introduites avec le Key Management Framework (KMF) dans le système de base.

Remarque :
Un abonnement est requis pour utiliser la Entreprise de Chiffrement au niveau des colonnes fonctionnalité. Pour en savoir plus, reportez-vous à la section Activer Entreprise de Chiffrement au niveau des colonnesEntreprise de Chiffrement au niveau des colonnes.

Les politiques d'accès aux modules développent les désignations basées sur les rôles fournies avec les modules de chiffrement. Les politiques d'accès au module peuvent être basées sur les éléments suivants :

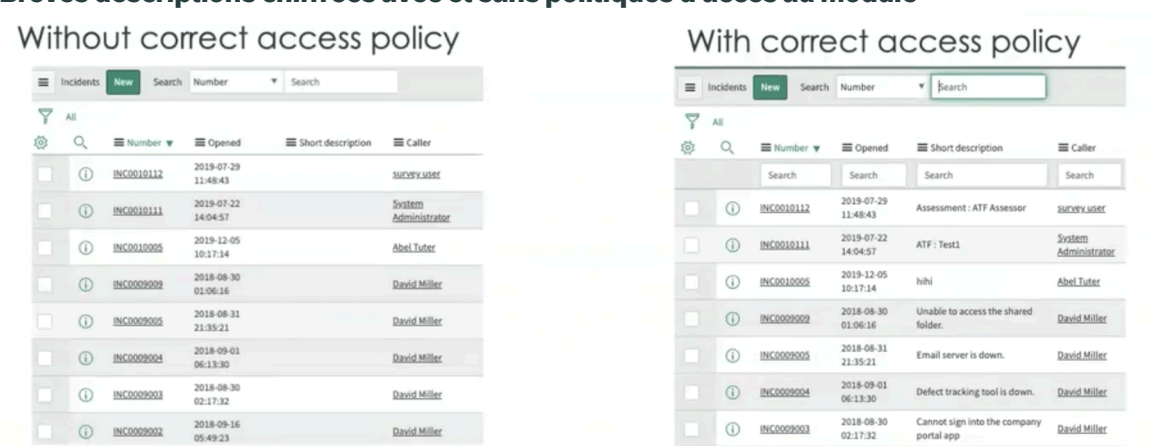
- Basique (périmètre)
- Rôle
- Utilisateur système
- Script
- Resource Exchange

Remarque :
Consultez Échange de ressources du cadre de travail de gestion de clés pour en savoir plus.

Dans un module de chiffrement, vous devez configurer les politiques d'accès au module appropriées pour allouer l'accès aux données chiffrées. Sans une 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 sont vides.

Dans cette image, l'absence de politique d'accès au module sur le champ Brève description chiffré masque le contenu à tous les utilisateurs qui accèdent à la table Incident. Avec une politique d'accès au module en place, les utilisateurs ayant le rôle autorisé sont en mesure de 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 qui ne disposent pas du rôle correct spécifié dans la politique d'accès au module.

Reportez-vous à Créer une politique d'accès au module pour 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. Il s'agit de politiques de niveau global qui sont générées et appliquées si aucune politique de niveau granulaire n'est définie lorsque le système ou le script tente d'accéder au module de chiffrement donné.

Traduction automatique

Important :

Les règles de stratégie de génération automatique ne sont pas appliquées aux types de tâches planifiées ou aux modules de chiffrement de champ (modules où le module parent est Chiffrement au niveau des colonnes).

Clés au niveau de l'instance dans Key Management Framework

L'architecture Key Management Framework (KMF) introduit une structure clé conçue dans un souci de sécurité. L'utilisation d'un module de sécurité matériel (HSM) KMF utilise le 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.

Au niveau de l'instance, KMF définit plusieurs clés qui sont utilisées en interne à des fins de chiffrement variables tout au long du Now Platform.

Le chiffrement d'enveloppe consiste à chiffrer une clé avec une autre clé. La figure suivante fournit un exemple de chiffrement d'enveloppe. Ici, les CDEK sont chiffrés par l'enveloppe par l'IKEK, qui à son tour est l'enveloppe cryptée par l'IRK, qui est finalement l'enveloppe cryptée par le RK. Étant donné que l'IRK n'est accessible que par le HSM, l'IKEK doit être téléchargé pour le déchiffrement.

Ce tableau fournit des exemples d'un sous-ensemble de clés client/d'application 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	Clé propre à votre instance qui est utilisée pour chiffrer 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). L'IHK permet de garantir l'authenticité et l'intégrité des clés de module et est encapsulé dans KeySecure ou 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 soit dans KeySecure, soit 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 Key Exchange ou Réplication de données d'instance l'approbation du consommateur.
Clé de signature d'instance (ISK)	Instance	Clé unique à votre instance qui est utilisée en interne à des fins de signature.

Clé	Emplacement	Description
Password2 (PW2)	Instance	Avec KMF, la clé des PW2 champs est entièrement gérée par KMF.
Clé de chiffrement des données client (CDEK)	Instance	Les clés de chiffrement créées sont KMF chiffrées 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.

Objectif cryptographique, algorithmes et informations clés

Les spécifications cryptographiques peuvent être adaptées à un objectif cryptographique spécifié, 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.

Objectifs cryptographiques, algorithmes et informations clés

Objectif cryptographique	Algorithme	Informations clés
Déchiffrement asymétrique des données	RSA	Asymétrique : clés 2 048 bits, 3 072 bits et 4 096 bits
Chiffrement asymétrique des données	RSA	Asymétrique : clés 2 048 bits, 3 072 bits et 4 096 bits
Désencapsulation de clé asymétrique	RSA	Asymétrique : clés 2 048 bits, 3 072 bits et 4 096 bits
Encapsulation de clé asymétrique	RSA	Asymétrique : clés 2 048 bits, 3 072 bits et 4 096 bits
Génération de signature	RSA	Asymétrique : clés 2 048 bits, 3 072 bits et 4 096 bits
Vérification de signature	RSA	Asymétrique : clés 2 048 bits, 3 072 bits et 4 096 bits
Authenticité symétrique	HMAC	Symétrique : clés 256 bits, 384 bits et 512 bits
Chiffrement/déchiffrement symétrique des données*	AES-CBC *	Symétrique – clé 128 bits, 192 bits, 256 bits
	AES-CFB	
	AES-OFB	
	AES-CTR (en anglais seulement)	
	AES-GCM **	
Encapsulation/désencapsulation de clé symétrique*	AES-CBC *	Symétrique – clé 128 bits, 192 bits, 256 bits
	AES-CFB	
	AES-OFB	
	AES-CTR (en anglais seulement)	

Objectifs cryptographiques, algorithmes et informations clés (suite)

Objectif cryptographique	Algorithme	Informations clés
	AES-GCM **	

* AES-CBC prend en charge les options de préservation de l'égalité. Entreprise de Chiffrement au niveau des colonnes utilise AES-CBC.

** AES-GCM intègre l'intégrité des données.

La configuration de ces paramètres est décrite dans la section Créer un module cryptographique.

États du cycle de vie de la clé Key Management Framework

KMF prend en charge plusieurs états du cycle de vie des clés cryptographiques grâce à l'application d'actions autorisées spécifiques. Par exemple, seules les clés dont l'état est actif peuvent être entièrement utilisées aux fins de chiffrement prévues. Le tableau suivant fournit plus de détails sur les différents états clés du cycle de vie.

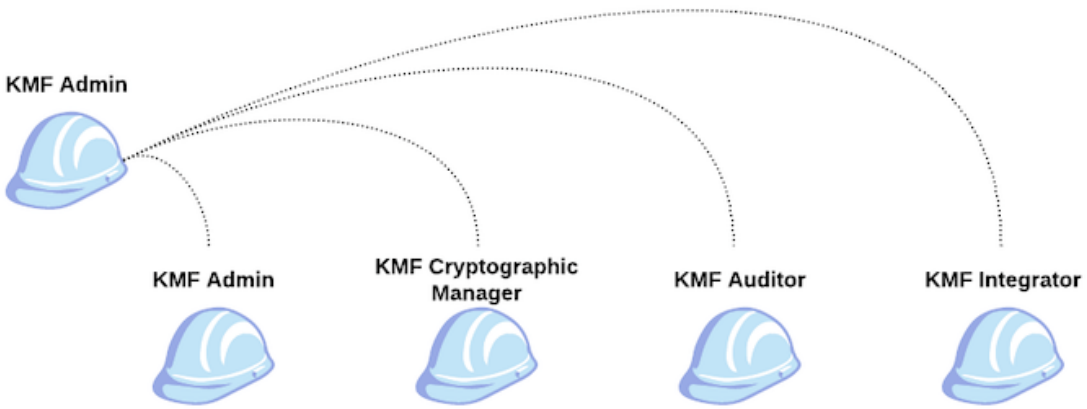
État ou action du cycle de vie de la clé	Description
Actif	Il ne peut y avoir qu'une seule clé active pour une spécification de chiffrement donnée dans un module de chiffrement.
Compromis	Plusieurs clés peuvent exister à l'état compromis pour être révoquées dans une spécification cryptographique donnée dans un module cryptographique. Toute clé active ou suspendue peut être passée à un état compromis. Les clés compromises ne peuvent pas être utilisées pour générer de nouveaux contenus, tels que le chiffrement ou la signature, mais peuvent toujours être utilisées pour identifier l'objectif du contenu existant, tel que le déchiffrement ou la vérification.
Désactivé	Toute clé active peut être désactivée. Il peut y avoir plusieurs clés dans un état désactivé pour une spécification cryptographique donnée dans un module cryptographique. 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, par exemple pour le chiffrement et la signature, mais elles peuvent tout de même être utilisées pour identifier les objectifs du 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 le délai désigné configuré. Il peut y avoir plusieurs clés dans un état détruit pour une spécification cryptographique donnée dans un module cryptographique.

État ou action du cycle de vie de la clé	Description
	⚠ Avertissement : Les données associées à une clé détruite ne sont plus accessibles, il convient donc de faire preuve d'une extrême prudence lors de l'exécution d'une action de destruction de clé.
Généré	Plusieurs clés peuvent exister à l'état généré pour une spécification de chiffrement donnée dans un module de chiffrement. 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 vous choisissez de générer une nouvelle clé, une nouvelle clé est générée et rendue active, même s'il existe des clés dans un état généré pour la spécification de chiffrement donnée.
Renouvelé	Une clé active ayant une date d'expiration peut être renouvelée autant de fois que nécessaire 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 à partir du jour actuel.
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 passer à l'état Révoqué. Les clés révoquées ne peuvent pas être utilisées pour générer de nouveau contenu, à des fins de chiffrement ou de signature, mais elles peuvent tout de même être utilisées pour identifier l'objectif du contenu existant, à des fins de déchiffrement ou de vérification, par exemple. Plusieurs clés à l'état révoqué peuvent exister pour une spécification de chiffrement donnée dans un module de chiffrement.
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 vers une clé importée existante. N'importe quelle touche active peut être pivotée.
Suspendu	Il peut y avoir plusieurs clés à l'état suspendu pour une spécification cryptographique donnée dans un module cryptographique. 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 Key Management Framework (KMF) introduit des rôles spécifiques pour les configurations liées au module cryptographique et à la gestion des clés.

Important :
Pour affecter le rôle administrateur KMF, vous devez avoir les rôles administrateur, security_admin et sn_kmf_admin. Utilisez le rôle administrateur KMF pour affecter d'autres rôles KMF. Pour en savoir plus sur l'affectation des rôles KMF, reportez-vous à la section Affecter KMF des rôles.



Administrateur KMF [sn_kmf.admin]

Affecte des rôles à d'autres utilisateurs pour effectuer des opérations autour de ServiceNow Key Management Framework.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Important :
Évitez d'accorder un rôle d'administrateur lorsque des rôles plus spécialisés sont disponibles.

- Ce rôle est affecté via le processus illustré à la section Affecter KMF des rôles.
- Vous devez disposer de ce rôle pour affecter des rôles KMF et vous pouvez en outre exécuter toutes les options du gestionnaire de chiffrement KMF.

Gestionnaire de chiffrement KMF [sn_kmf.cryptographic_manager]

Créez, lisez et mettez à jour les opérations sur les modules cryptographiques (association de clés à l'utilisation cryptographique et aux configurations d'algorithmes) et les politiques d'accès aux modules. En outre, les gestionnaires de chiffrement KMF peuvent effectuer des opérations de gestion des clés (générer, rotation, révoquer) et 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 particulières

Aucun.

Auditeur cryptographique KMF [sn_kmf.cryptographic_auditor]

Affichez les informations cryptographiques du module, les métadonnées clés et les détails relatifs 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 particulières

Aucun.

Intégrateur cryptographique KMF [sn_kmf.cryptographic_integrator]

Intégrer Key Management Framework à des magasins de clés ou à 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 particulières

Aucun.

Opérateur de chiffrement KMF [sn_kmf.cryptographic_operator]

Accéder à une partie du cycle de vie de la ServiceNow Key Management Framework 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 particulières

Aucun.

Affecter KMF des rôles

Affectez KMF des rôles aux administrateurs, qui peuvent à leur tour affecter d'autres KMF rôles.

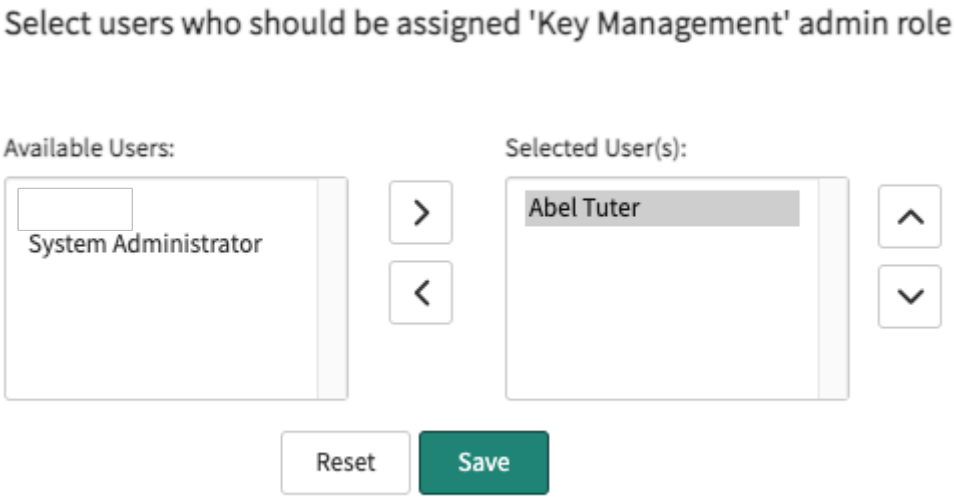
Avant de commencer
Rôle requis : admin et security_admin

Vous devez vous élever au rôle security_admin avant d'affecter le KMF rôle administrateur. Pour obtenir des instructions, consultez Élever à un rôle privilégié

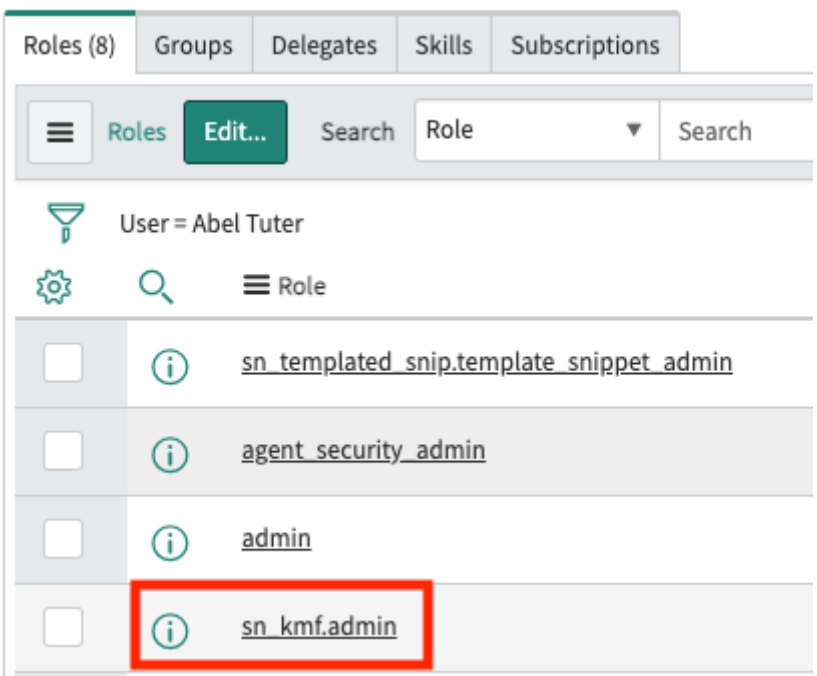
Pour obtenir la liste complète des rôles KMF disponibles et leurs descriptions, consultez Rôles installés avec Key Management Framework.

Procédure

1. Élever au rôle d'administrateur de sécurité.
2. Accédez à la **Administration utilisateurs** > **Utilisateurs** et sélectionnez l'utilisateur que vous souhaitez investiguer en tant qu'administrateur KMF .
3. Vérifiez que l'utilisateur dispose déjà des rôles administrateur et security_admin.
   Si ce n'est pas le cas, sélectionnez **Modifier** sous la liste connexe Rôles et ajoutez des _admin **d'administration** et **de sécurité**.
4. Accédez à la **Sécurité de système** > **Administration de la gestion de clés**.
5. Sélectionnez l'utilisateur que vous souhaitez nommer KMF administrateur dans la colonne **Utilisateurs disponibles** et déplacez-le dans la colonne **Utilisateur(s) sélectionné(s).**



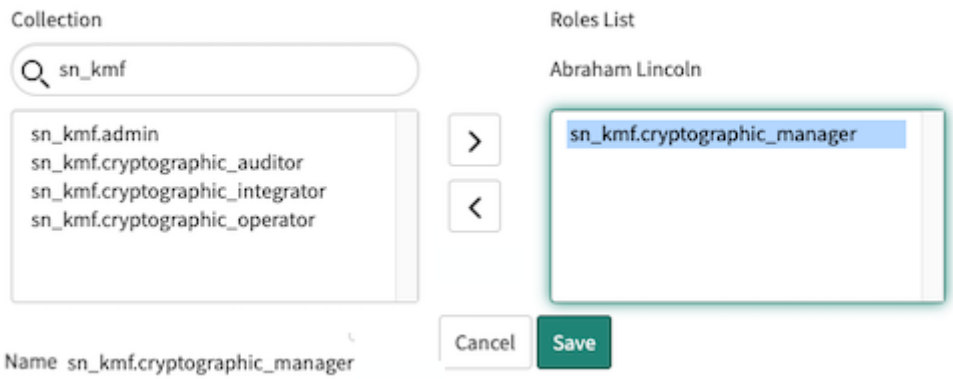
6. Sélectionnez **Enregistrer**.
7. Accédez à la **Administration utilisateurs** > **Utilisateurs** et sélectionnez l'utilisateur auquel vous venez d'attribuer le rôle sn_kmf.admin.
   L'utilisateur dispose du rôle sn_kmf.admin dans la liste connexe **Rôles** et peut affecter d'autres rôles KMF.



Que faire ensuite

Si vous disposez du rôle d'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** , sélectionnez Modifier et sélectionnez les rôles KMF que vous souhaitez affecter aux utilisateurs. Tous les rôles KMF commencent par `sn_kmf`.



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 la Now Platform.

Avant de commencer

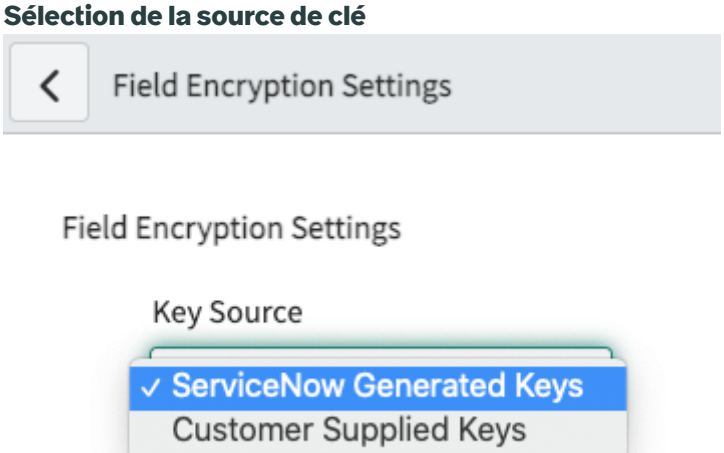
Les clés fournies par le client ne sont prises en charge qu'avec Entreprise de Chiffrement au niveau des colonnes.

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 **soit Clés générées par ServiceNow** , soit **Clés fournies** par le client dans la liste **Source de clé** .

Sélection de la source de clé



Traduction automatique

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 Configurer les propriétés des clés fournies par le client.
- 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 de chiffrement pour définir les mécanismes utilisés pour les opérations de chiffrement. Une fois que vous avez créé le module, vous créez une spécification de chiffrement, dans laquelle vous définissez un algorithme de chiffrement et générez une clé.

Avant de commencer

Si vous fournissez vos propres clés, reportez-vous à Configurer et charger votre clé fournie par le clientla section .

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Cette procédure décrit les options disponibles dans KMF le système de base de la ServiceNow plateforme. Entreprise de Chiffrement au niveau des colonnes La fonctionnalité n'est disponible que lorsque le module d'extension *com.glide.now.platform.encryption* est actif. Pour Activer Entreprise de Chiffrement au niveau des colonnes plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes. Consultez Créer un module de chiffrement pour Column Level Encryption.

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 d'algorithmes pris en charge pour les spécifications de chiffrement.
Valeur de la politique d'accès au module par défaut	○ S'appuyer sur le système par défaut : ○ Refuser ○ Trace

Champ	Description
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 ajouté au nom du périmètre de l'application.
État du cycle de vie du module de chiffrement	Le cycle de vie fait référence à la création, à l'utilisation et à la désactivation d'un module cryptographique. Défini 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 **Envoyer**.

⚠ Avertissement :

Pour les utilisateurs de l'assistance de chiffrement héritée :

Si vous utilisez la version non entreprise de Column Level Encryption, vous êtes limité à cinq modules. Si vous avez dépassé cette limite, vous recevez l'avertissement suivant :

Cette insertion dépasse le nombre de limites de modules publiés de Chiffrement au niveau des colonnes autorisées avec le produit d'abonnement. L'abonnement Entreprise à Column Level Encryption est requis pour les modules supplémentaires. Veuillez contacter l'équipe de votre compte.

Une fois l'envoi réussi, votre module de chiffrement est répertorié dans la table Modules de chiffrement. Le système fait précéder le nom du périmètre pour éviter tout conflit avec d'autres applications incluses dans le périmètre. Par exemple, si vous avez créé un module dont le nom `my_crypto_module` dans le périmètre global de l'application, le nom est enregistré en tant que `global.my_crypto_module`.

Que faire ensuite

Créer une spécification cryptographique

.

Créer une spécification cryptographique

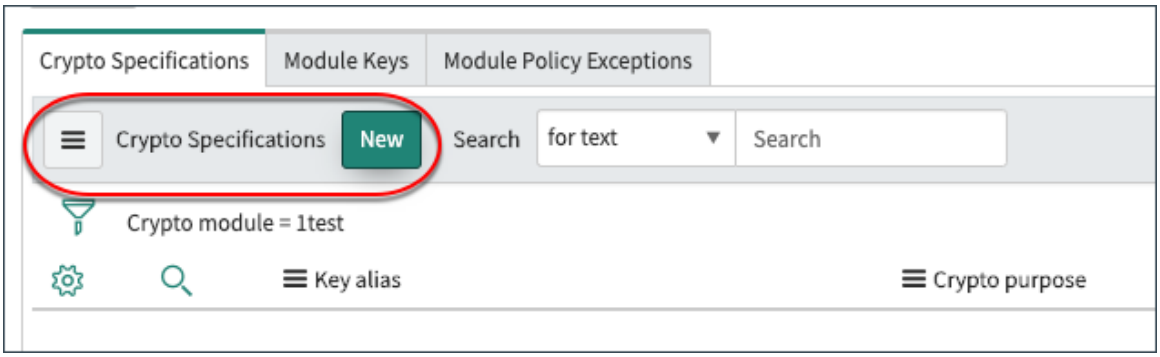
Après avoir créé un module de chiffrement, créez une spécification de chiffrement pour définir les algorithmes du module.

Avant de commencer

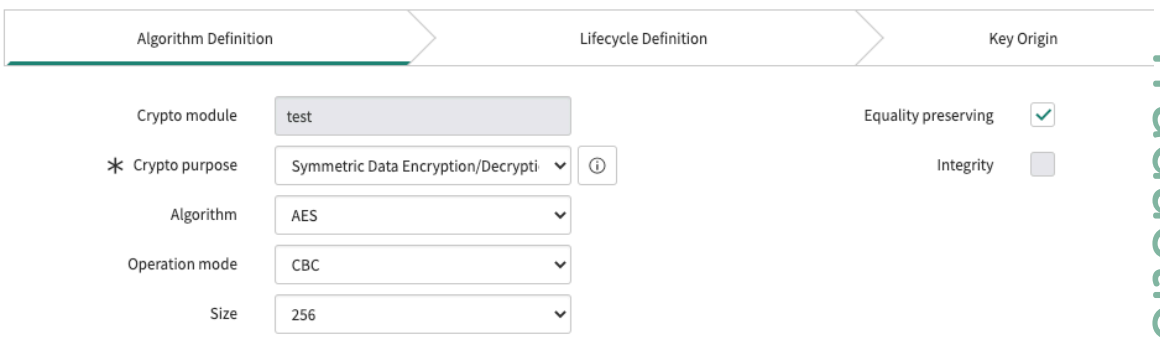
Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tous**.
2. Sélectionnez le module de chiffrement pour la définition afin d'ouvrir les options de configuration.
3. Dans l'onglet **Spécifications de chiffrement** , cliquez sur **Nouveau**.



4. Remplissez le formulaire Définition de l'algorithme.
Consultez Objectif cryptographique, algorithmes et informations clés 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.

Champs 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. Vous pouvez par exemple l'utiliser pour le chiffrement des données, la génération de signature ou l'emballage de clé. Les algorithmes disponibles s'ajustent en fonction de l'objectif de chiffrement sélectionné. Consultez Objectif cryptographique, algorithmes et informations clés pour en savoir plus.
Algorithme	Type d'algorithme utilisé pour atteindre l'objectif de chiffrement. L'algorithme contrôle également l'origine de la clé. S'ajuste automatiquement en fonction de l'objectif de chiffrement sélectionné. Objectif cryptographique, algorithmes et informations clés pour plus de détails.
Mode d'opération	Ce champ peut s'afficher en fonction de l'objectif de chiffrement sélectionné.
Taille	Sélectionnez la taille de bit.

Champ	
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 symétrique des données** avec **AES** et en mode **CBC (Cipher Block Chaining).** La sélection de cette option signifie que si les mêmes données sont chiffrées à nouveau, 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. Cliquez sur **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 :

- Sélectionnez une entrée dans la table Cycle de vie de la clé pour définir le comportement du cycle de vie de la clé. Consultez Configurer les états clés du cycle de vie pour en savoir plus afin de terminer la définition du cycle de vie de la clé.
- Cliquez sur **Suivant** pour créer une clé cryptographique. Consultez l'une des tâches suivantes pour la génération de clés :
  - Générer une ServiceNow clé cryptographique.
  - 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

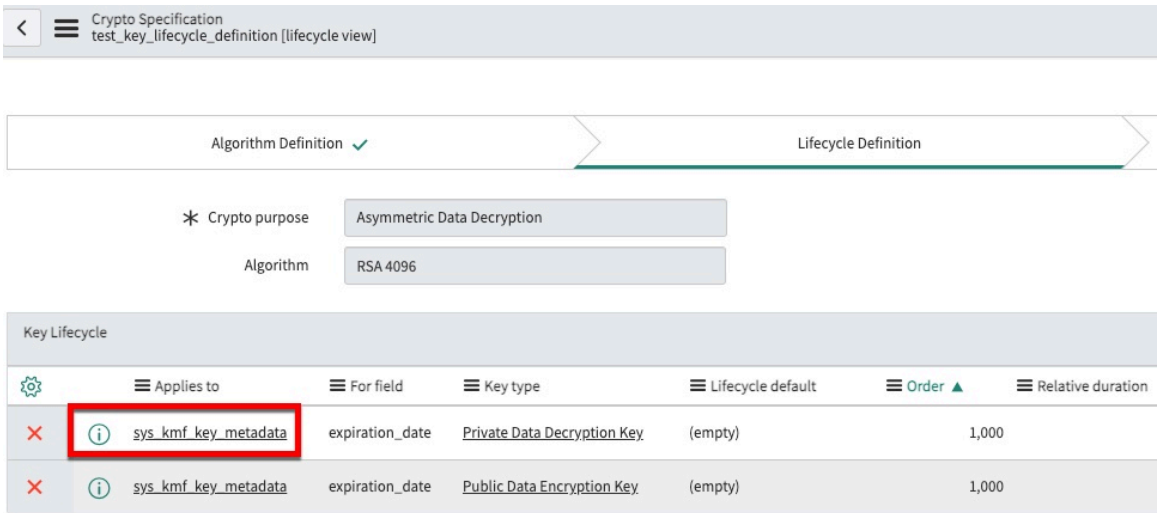
Une fois que vous avez créé une spécification de chiffrement, vous pouvez configurer les actions de cycle de vie pour les clés de votre instance.

Avant de commencer

Rôle requis : sn_kmf.admin

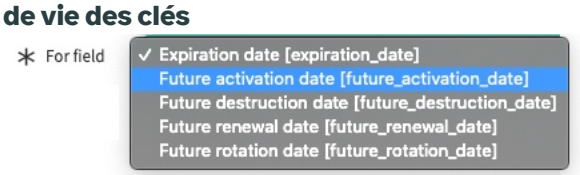
Procédure

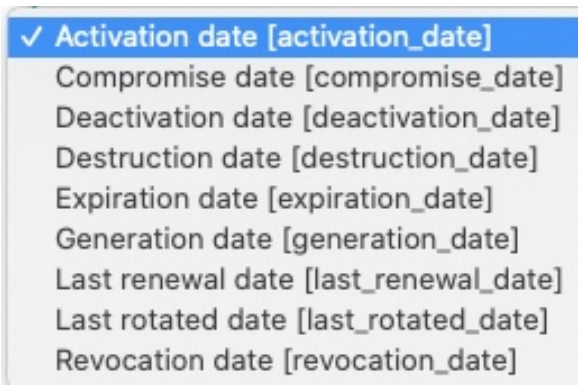
1. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tous**.
2. Sélectionnez le module de chiffrement pour configurer le cycle de vie d'une clé.
3. Cliquez sur un alias de clé dans l'onglet Spécifications de chiffrement.
   Le formulaire Définition de l'algorithme s'ouvre pour la clé sélectionnée.



4. Cliquez sur **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 de chiffrement 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.
Pour le champ	Sélectionnez le type de contrôle pour la clé à laquelle le cycle de vie s'applique. **Valeurs « Pour champ » de la gestion du cycle de vie des clés** 
Type	Sélectionnez si l'évaluation du cycle de vie de la 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 de chiffrement.
Type de durée relative	Durée du cycle de vie : **années**, **mois** ou **jours**.
Durée relative	Nombre d'années, de mois ou de jours de validité de la clé.
Opération relative	**Avant**ou **après**.

Champ	Description
Relatif à	Champ auquel la durée est relative. S'affiche si une durée relative ou une opération est sélectionnée. 

Générer une ServiceNow clé cryptographique

Suivez cette procédure pour charger et configurer une ServiceNow clé cryptographique afin de chiffrer les données sensibles.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

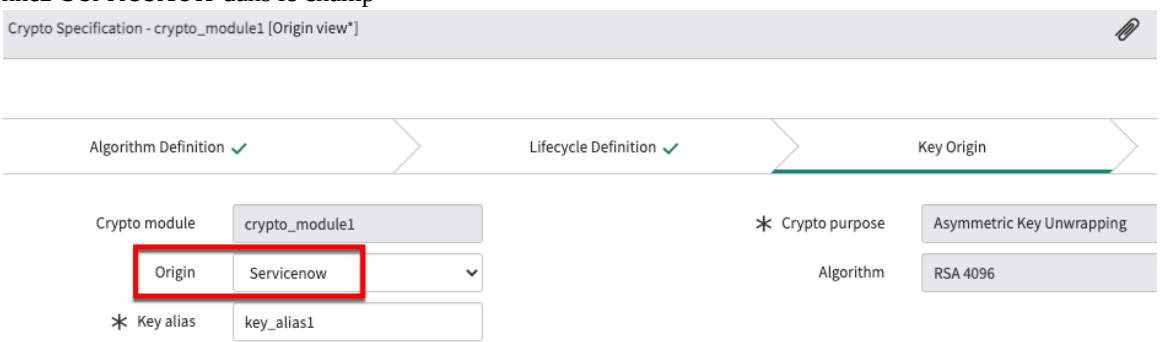
Pourquoi et quand exécuter cette tâche

Les gestionnaires de chiffrement ont le choix d'utiliser ServiceNow les clés fournies ou leurs propres clés fournies par le client (CSK) pour le chiffrement sur le Now Platform .Entreprise de Chiffrement au niveau des colonnes Pour plus d'informations sur CSK, reportez-vous à Configurer les propriétés des clés fournies par le client.

Procédure

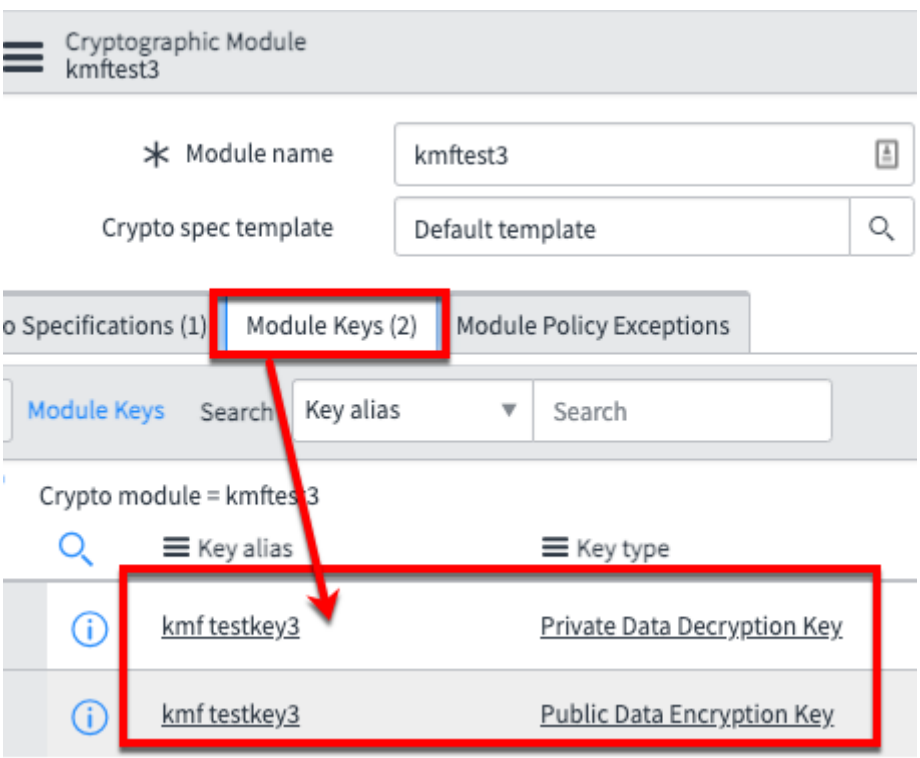
1. Définissez les paramètres de chiffrement de champ pour utiliser ServiceNow les clés générées.
   Consultez Configurer les paramètres de chiffrement de champ pour sélectionner le type de clé pour en savoir plus.
2. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tous**.
3. Sélectionnez le module de chiffrement correspondant pour ouvrir la page des détails du module de chiffrement.
4. Cliquez sur la ligne de l'entrée de l'alias de clé dans l'onglet Spécifications de chiffrement.
   Si aucune clé n'a encore été générée, le champ alias de clé est vide.
5. Cliquez sur **Suivant** pour accéder à l'onglet Key Origin (Origine de la clé) des composants Spécification de chiffrement.
   L'onglet Définition du cycle de vie s'affiche avec la table Cycle de vie de la clé et peut être révisé 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 Importer la paire de clés d'encapsulation/de désencapsulation. Vérifiez Configurer les propriétés des clés fournies par le client si vous utilisez votre propre clé.

7. Entrez un nom convivial pour l'alias de clé.
8. Cliquez sur **Suivant** pour accéder à l'onglet Création de clé.
9. Cliquez sur **Générer la clé**.
   Une fois la clé générée, le formulaire Module de chiffrement se recharge en affichant la spécification de chiffrement.
10. Cliquez sur l'onglet **Clés de module** pour afficher les clés.
    Les informations sécurisées pour la clé seront stockées dans l'onglet Clés de module avec le nombre de clés qui existent pour la spécification de chiffrement.



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 limiter le chiffrement ou le déchiffrement des données.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf.admin

Pourquoi et quand exécuter cette tâche

Column Level Encryption (CLE) 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 politiques 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 par module ou module de chiffrement.
- Associez les versions de script pour lesquelles les modifications apportées au script sont suivies et invalidez la stratégie de script, ce qui permet d’améliorer la sécurité des politiques d’accès au module de type script.

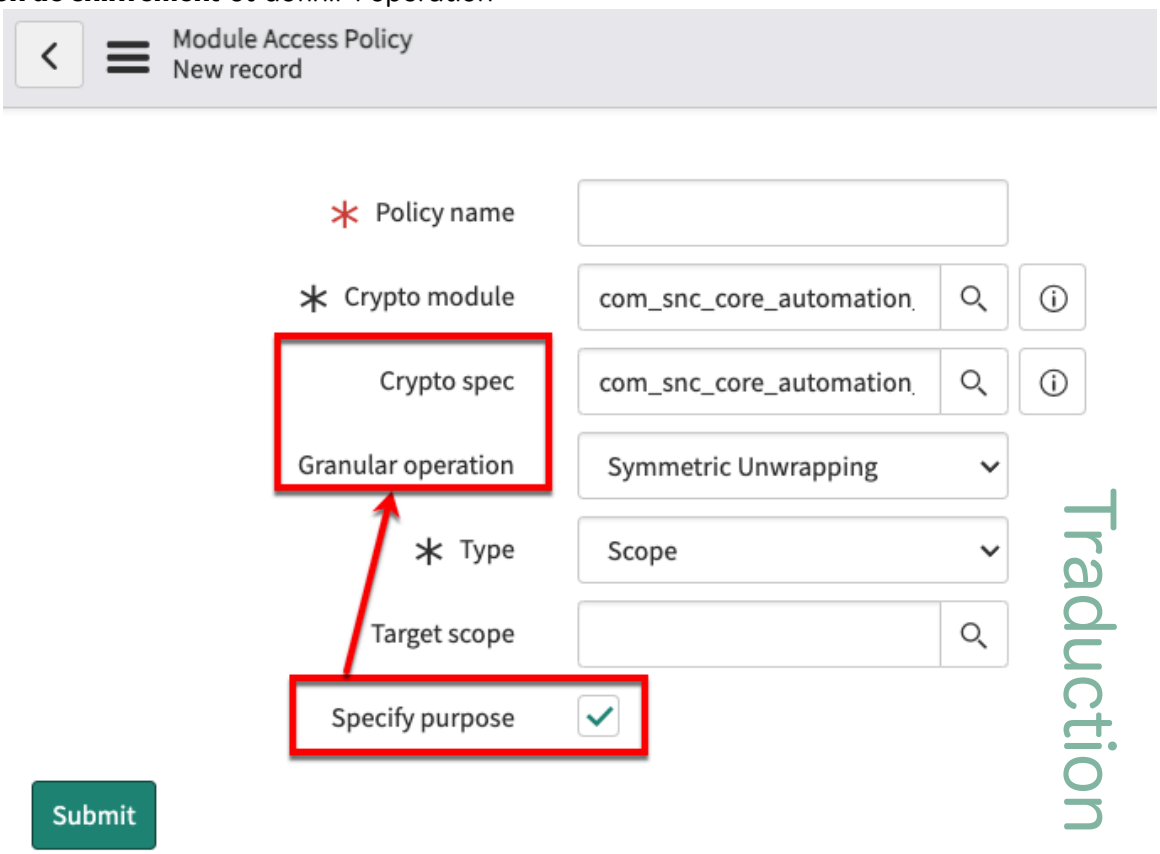
CLE_Ent Cette fonctionnalité est disponible avec un abonnement payant. Consultez les fonctionnalités et options prises en charge disponibles avec chaque offre. Pour plus d'informations, consultez Entreprise de Chiffrement au niveau des colonnes.

Remarque :
Le comportement par défaut des politiques d’accès au module (MAP) est Rejeter pour empêcher tout accès non autorisé, sauf s’il est explicitement déclaré 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 cryptographique configuré pour le chiffrement/déchiffrement symétrique des données, une politique d’accès au module générée automatiquement est créée et répertoriée dans la table.
2. Cliquez sur **Nouveau**.

- Sélectionnez **Spécifier l'objectif** pour choisir une **spécification de chiffrement** et définir l'opération **Granulaire**.



- Avec les spécifications de chiffrement pour le chiffrement/déchiffrement symétrique des données et l'encapsulation/désencapsulation symétrique, le champ **Opération granulaire** est disponible si vous cochez la case **Spécifier l'objectif** .

3. Complétez le formulaire.

Champs des politiques d'accès au module

Champ	Description
Nom de la stratégie	Entrez un nom pour la politique.
Module de chiffrement	Cliquez sur l'icône de recherche ( ) pour sélectionner un module.
Spécification du chiffrement	Sélectionnez ou créez une spécification de chiffrement lors de la génération de la politique d'accès au module. Ce champ devient 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 Objectif cryptographique, algorithmes et informations clés pour plus de détails sur les objectifs de cryptographie.

Champ	Description
Type	○ **Champ d'application** : contrôle l'accès par le périmètre de l'application. ○ **Utilisateur système** : permet aux utilisateurs système d'accéder aux modules de chiffrement. ○ **Script** : contrôler l'accès par script. Voir Configurer l'accès de script aux données chiffrées pour plus d'informations ○ **Rôle** : contrôle l'accès par rôle d'utilisateur. ○ **Échange de ressources** : contrôlez l'accès à l'aide du Resource Exchangefichier . Consultez Échange de ressources du cadre de travail de gestion de clés pour plus d'informations. **Remarque :** Seul le type de rôle est pris en charge avec Column Level Encryption. Tous les autres types sont disponibles avec Entreprise de Chiffrement au niveau des colonnes.
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 Entreprise de Chiffrement au niveau des colonnes
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 de chiffrement, l'accès au module est refusé et le développeur reçoit une erreur. Cela donne au propriétaire du module la possibilité d'accorder ou de refuser l'accès au module.
Échange de ressources : ○ Spécification de chiffrement ○ Type d'approbation ○ Hôte de l'instance cible	Ces options s'affichent lorsque vous sélectionnez Resource Exchange le type. Resource Exchange est pris en charge à la fois par KMF et par Entreprise de Chiffrement au niveau des colonnes lorsque le module parent est **column_level_encryption**.

Champ	Description
	Sélectionnez la spécification de chiffrement, ponctuelle ou récurrente, et l'URL de l'instance cible. Consultez Échange de ressources du cadre de travail de gestion de clés pour plus d'informations.
Emprunt d'identité	Dans les stratégies d'accès au module basées sur les rôles, les utilisateurs peuvent accéder à des 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 activer/désactiver le champ de spécification de chiffrement en tant que champ disponible pour la politique.
Actif	Sélectionnez cette option pour activer la politique.
Résultat	Sélectionnez l'une des options suivantes : ○ **StrictReject** rejette l'accès dans toutes les circonstances. ○ **Rejeter** rejette les utilisateurs ayant le **rôle cible** ou le **champ d'application cible** de l'accès à ce module de chiffrement, à moins qu'une autre politique ne leur accorde l'accès. ○ **Suivre** pour autoriser l'accès et surveiller l'utilisation du module.

4. Sélectionnez **Envoyer**.

⚠ Avertissement :

Pour les utilisateurs de l'assistance de chiffrement héritée :

Si vous utilisez la version non entreprise de Column Level Encryption, vous êtes limité à cinq modules. Si vous avez dépassé cette limite, vous recevez l'avertissement suivant :

Cette insertion dépasse le nombre de limites de modules publiés de Chiffrement au niveau des colonnes autorisées avec le produit d'abonnement. L'abonnement Entreprise à Column Level Encryption est requis pour les modules supplémentaires. Veuillez contacter l'équipe de votre compte.

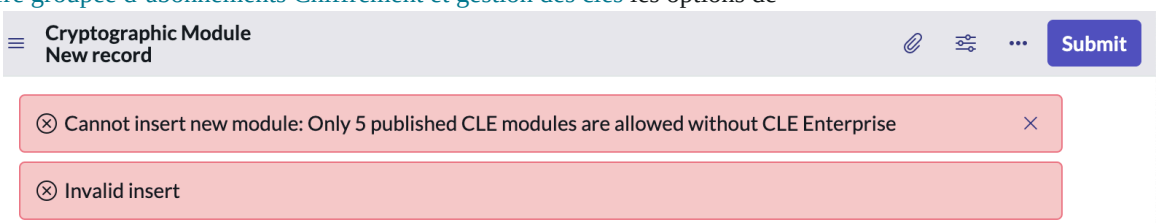
5. Sélectionnez le nom de politique associé au module de chiffrement que vous souhaitez examiner.
À l'aide de la politique d'accès au module de type Script :

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 comme « AutoGen-Module-TestPolicy » dans la colonne Nom de la stratégie.

Le formulaire Politique d'appel de chiffrement répertorie la politique d'appelant que vous avez sélectionnée. Le champ Champ d'application cible spécifie le champ d'application du

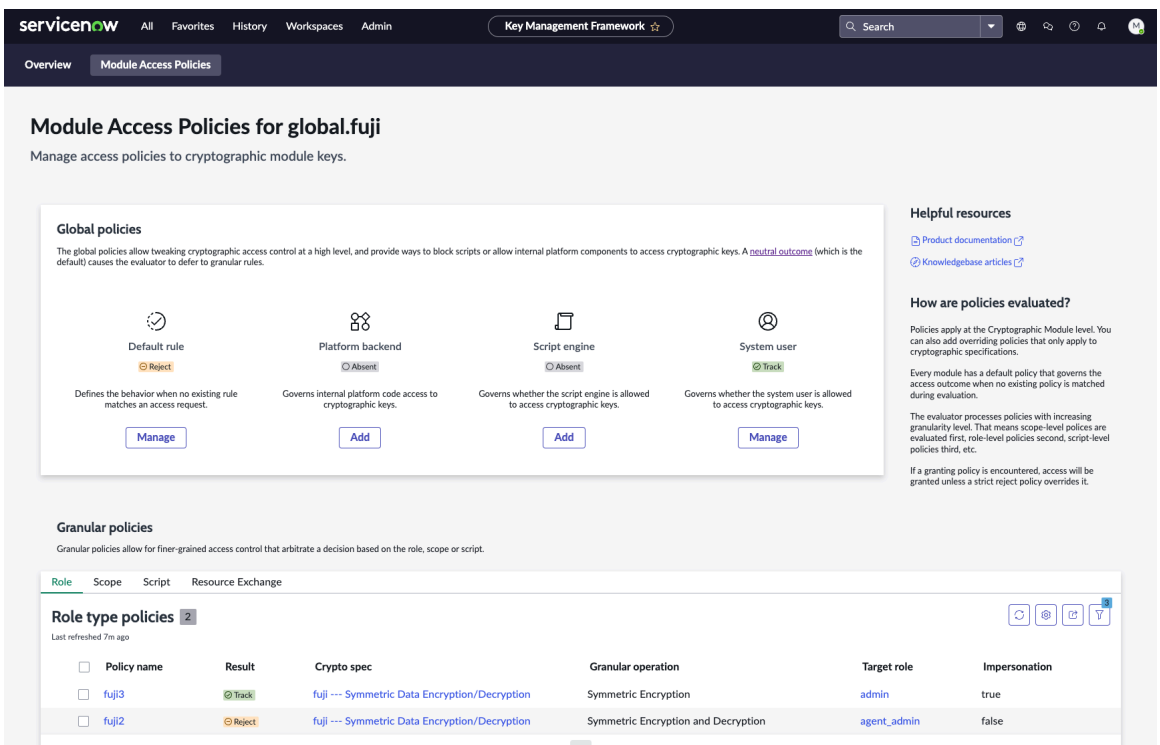
script qui tente d'utiliser le module. Consultez Configurer l'accès de script aux données chiffrées pour plus d'informations.

Remarque :
Un maximum de cinq politiques d'accès aux modules est autorisé avec Column Level Encryption. Consultez Offre groupée d'abonnements Chiffrement et gestion des clés les options de configuration.



Visualisation de la politique d'accès au module

Utilisez la visualisation de la politique d'accès au module pour afficher toutes les informations de module de chiffrement pertinentes sur une seule page d'interface utilisateur.



Les administrateurs et les gestionnaires de chiffrement de Key Management Framework peuvent utiliser la page d'interface utilisateur de politique d'accès au module, afficher tous les mécanismes de contrôle d'accès associés à un module cryptographique unique. Utilisez les informations collectées sur cette page d'interface utilisateur pour déterminer rapidement qui a accès aux informations chiffrées sur votre instance.

Les utilisateurs disposant des `sn_kmf.admin` rôles ou `sn_kmf.cryptographic_manager` peuvent accéder à la page d'interface 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 faut accorder l'accès au module de chiffrement sélectionné. La page d'interface utilisateur

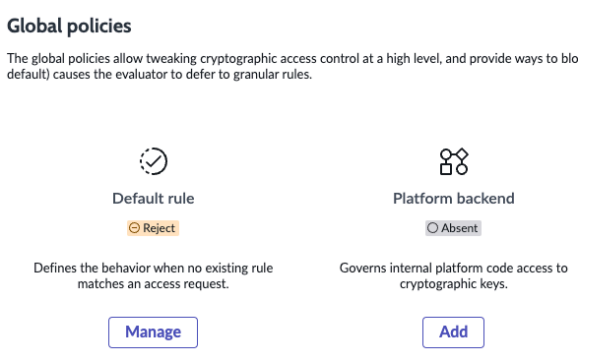
affiche une étiquette sur les éléments de la page d'interface utilisateur en fonction de la valeur de ce champ.

Étiquette de l'interface utilisateur	Valeur du 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 jusqu'à ce qu'une politique d'accès au module de suivi soit trouvée.
StrictReject	*StrictReject*	L'accès est 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 **Stratégies globales** pour passer en revue les politiques d'accès au module qui contrôlent l'accès au niveau de la plateforme.

Sélectionnez le bouton **Gérer** sous l'une des politiques pour accéder à cet enregistrement de politique. 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.

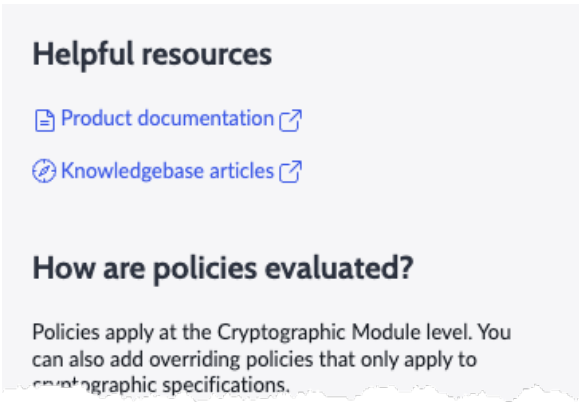


Politique	Définition
Règle par défaut	La politique de règle par défaut définit le comportement lorsqu'aucune règle existante ne correspond à une demande d'accès.
Back-end de la plateforme	La stratégie back-end de la plateforme régit l'accès du code interne de la plateforme aux clés de chiffrement.
Moteur 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.

Traduction automatique

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 stratégies d'accès aux modules sont évaluées, reportez-vous à la section Débogueur de politique d'accès au module.

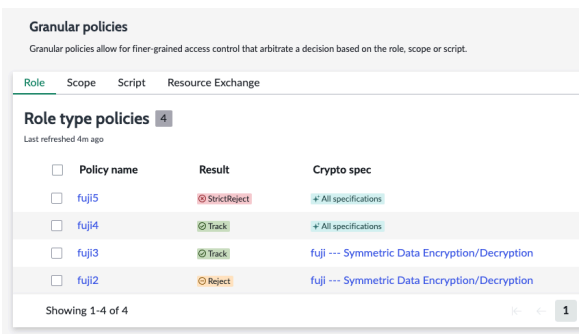


Politiques granulaires

Utilisez la section **Stratégies granulaires** pour afficher les listes des politiques d'accès au module, séparées par type de politique. Utilisez les onglets situés au-dessus de la liste pour sélectionner une catégorie de politique à afficher.

- Rôle
- Périmètre
- Périmètre et domaine (si l'option Séparation de domaine est activée)
- Script
- Échange de ressources (si le module cryptographique est un sous-module Password2 ou Chiffrement au niveau des colonnes)
- Identité (si Secrets Management Enterprise est actif)

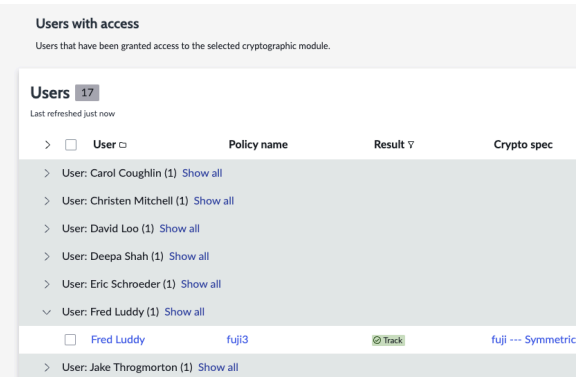
Par défaut, chaque liste affiche uniquement les politiques actives. Utilisez l'icône de filtre pour modifier le filtre par défaut de la liste.



Traduction automatique

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 seul utilisateur peut avoir plusieurs rôles qui accordent l'accès à un module cryptographique.

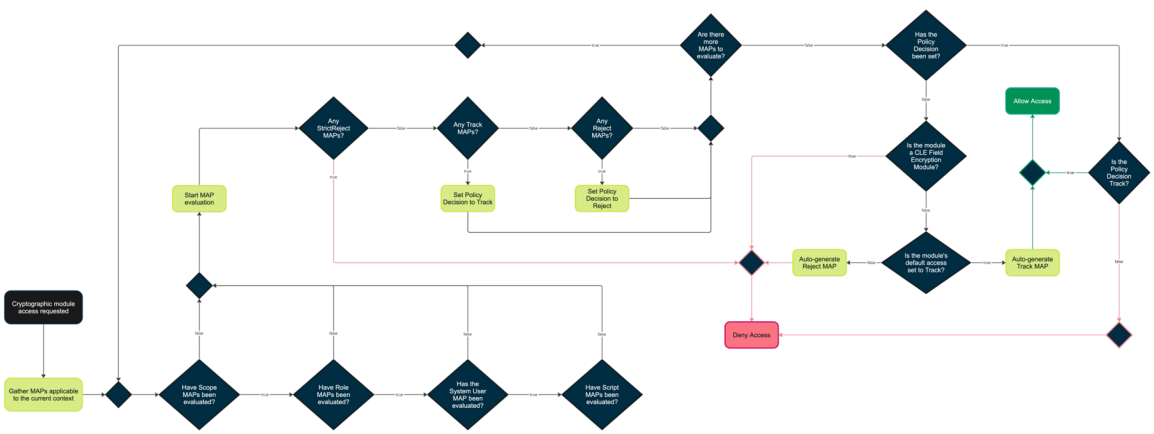


Débogueur de politique d'accès au module

Utilisez le débogueur de politique d'accès au module pour examiner les informations de journalisation et comprendre pourquoi vos utilisateurs ont ou n'ont pas accès à un contexte de chiffrement.

Les politiques d'accès aux modules (MAP) définissent des contrôles au niveau de l'instance pour l'accès aux modules de chiffrement. Les appelants (par exemple, un utilisateur ou un script) ont besoin d'un accès explicite afin d'utiliser un module cryptographique pour le chiffrement et le déchiffrement. Il n'est pas toujours clair quelles MAP sont évaluées lorsque les appelants tentent d'accéder à un module cryptographique. Utilisez le débogueur pour voir quelles politiques sont évaluées lorsqu'un appelant tente d'accéder à un module de chiffrement et savoir pourquoi l'accès est accordé ou non.

Cet organigramme montre comment votre instance évalue les demandes d'accès à un module de chiffrement.



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 toujours accès au débogueur. Accordez l'accès à d'autres rôles à l'aide de la `glide.kmf.module_access_policies.debugger.authorized.roles` propriété système. La valeur de cette propriété est une liste séparée par des virgules des rôles qui accèdent aux journaux de débogage.

Traduction automatique

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** > **.**

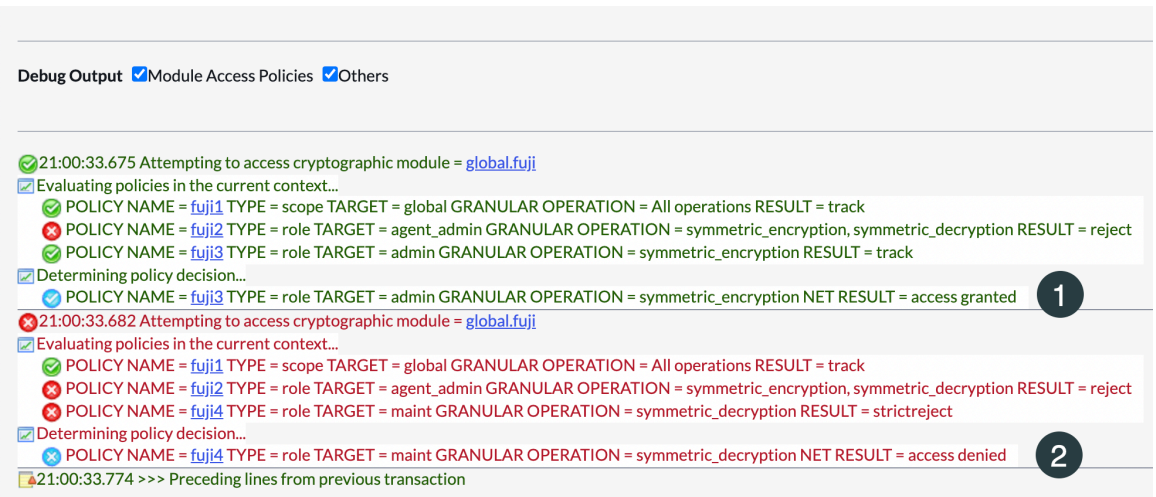
Lorsque vous avez terminé le débogage, vous pouvez désactiver les messages de journalisation en accédant à **Tous** > **Diagnostics** > **Débogage de session** > **Désactiver tout** > **.**

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 Impersonating users . Pour afficher les journaux de débogage du point de vue d'un autre utilisateur, assurez-vous que le champ **Emprunt d'identité** est défini sur **vrai** dans vos politiques d'accès au module avec ce `role` type.



Dans cet exemple, un appelant appelle deux demandes d'accès au module cryptographique `global.fuji` . Un chiffrement symétrique, qui est accordé, et un déchiffrement symétrique, qui a été refusé.

Comprendre les entrées de journal

Les informations de débogage sont structurées à l'aide de ce format.

1. Cette première ligne affiche le module cryptographique recevant 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'appelant bénéficie ou non de l'accès).

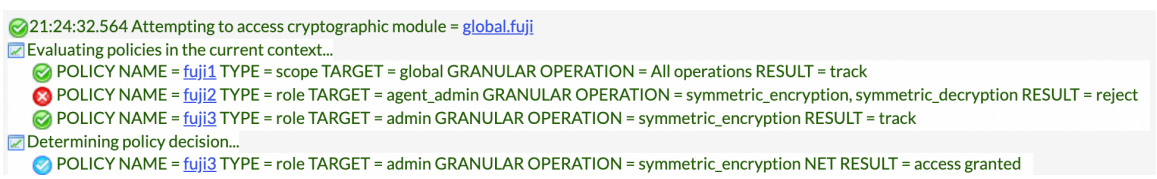
Chaque ligne commence par une icône qui indique son type de message.

Icônes de message

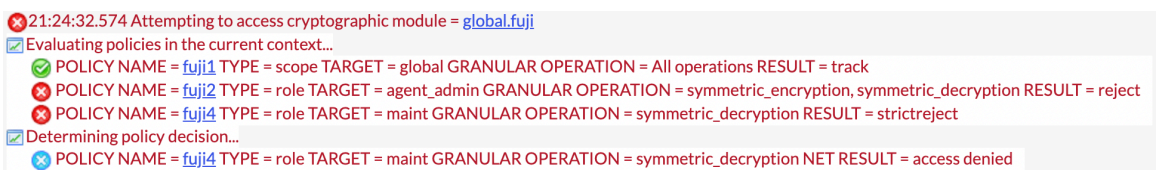
Icône	Type de message
	Message d’information
	La politique d’accès au module accorde l’accès
	La politique d’accès au module refuse l’accès
	L’appelant se voit accorder un accès
	L’accès est refusé à l’appelant
	Aucune politique d’accès au module à évaluer

Exemples de journal de débogage

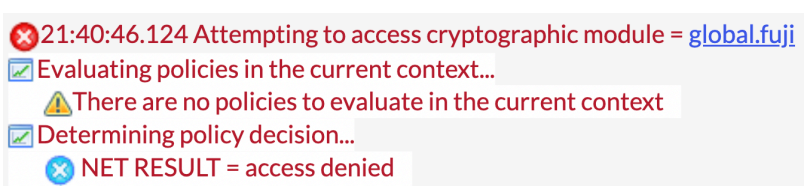
Message d’accès accordé



Message d’accès refusé



Accès refusé (aucune politique d’accès au module à évaluer



Accès refusé (privilèges insuffisants)

Créer une politique de cycle de vie du module de chiffrement

Créez une politique de cycle de vie des modules de chiffrement pour imposer des limites aux modules de chiffrement, telles que la durée de validité de la clé. Créez des politiques pour protéger les modules de chiffrement 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 des modules de chiffrement est une politique au niveau de l’instance. Plus une clé cryptographique est exposée, plus elle est susceptible d’être compromise. Protégez les clés en limitant la durée d’utilisation des clés et les personnes autorisées à les utiliser.

Les fonctionnalités suivantes régissent les modules de chiffrement :

- Les politiques d'instance définissent les limites de l'instance. Par exemple, si vous spécifiez dans une politique d'instance que la date d'expiration ne doit jamais être postérieure de plus de deux ans à 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 de chiffrement 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 postérieure de deux ans à 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. Complétez le formulaire.

   Champs Politiques de cycle de vie de chiffrement

Que faire ensuite

Si vous souhaitez ajouter des exceptions à cette stratégie de cycle de vie au niveau du module, reportez-vous à la section Créer des exceptions de politique de cycle de vie des modules.

Créer des exceptions de politique de cycle de vie des modules

Créez une exception de politique de module pour modifier la politique de cycle de vie d'une clé au niveau du module pour une instance. La ou les exceptions s'appliquent uniquement à ce module et non à l'ensemble de l'instance. Par exemple, si l'administrateur a configuré des clés symétriques pour qu'elles soient limitées à un an au niveau de l'instance, une exception peut être faite au niveau du module pour qu'elle soit de deux ans.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager et sn_kmf.admin

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 **Exceptions de politique du module** Onglet.
4. Cliquer sur **Nouveau**.
5. Complétez le formulaire.

Champs Exceptions de politique de module

Champ	Description
Module de chiffrement	Lecture seule, nom du module sélectionné.
Concerne	La clé spécifiée est renseignée automatiquement.
Type de clé	Sélectionnez le type de clé, car les politiques d'exception sont liées à une clé spécifique. Plusieurs politiques d'exception peuvent être créées par module de chiffrement.
Condition de la politique	Choisissez les conditions de qualification dans la liste déroulante et complétez les critères de contrainte supplémentaires.
Nouveau critère	Sélectionnez des conditions de politique supplémentaires, au besoin.
Résultat	Sélectionnez **Rejeter** pour rejeter l'utilisation de la clé ou **Suivre** pour autoriser son utilisation lorsque les critères sont remplis.

6. Cliquer sur **Envoyer** à renvoyer à la table Module cryptographique.

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 `actif`.
Faire pivoter la clé	Désactive la clé actuelle et en génère une nouvelle. La nouvelle clé de module est définie sur actuelle (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 les 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 décryptage. 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 cryptographique.
Clé de reprise	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 cas suivants :

Action de gestion des clés	Description
	• Le rôle de gestionnaire cryptographique vous est affecté. • L'état du cycle de vie est marqué **comme Actif** ou **Renouvelé**. • Une date d'expiration est définie dans la définition du cycle de vie du module.

Afficher et gérer les clés

Passez en revue l'état de n'importe quelle clé pour déterminer les actions à effectuer sur la clé, telles que le renouvellement, la rotation, la suspension, la désactivation ou 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. Révisez 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 du cycle de vie de la clé.
Prochaine date d'activation	Affiche la date future d'activation de la clé.
Prochaine date de renouvellement	Affiche la date future de renouvellement de la clé.
Prochaine date de rotation	Affiche la date future pour la rotation des clés.
Prochaine date de destruction	Affiche la date future de destruction de la clé.
Date d'expiration	Affiche la date d'expiration de la clé.

5. Pour effectuer une action sur la clé, sélectionnez l'une des options suivantes pour qu'elle prenne 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 augmente de 1. Voir pour plus de détails.
- **Suspendre la clé**: sélectionnez cette option pour désactiver la clé actuelle.
- **Reprendre la clé** : sélectionnez cette option pour marquer une touche suspendue comme clé active. Cette option n'est disponible qu'une fois que la clé active a été suspendue.

Faire pivoter les clés

Pour une sécurité accrue, vous pouvez alterner 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 en générant une nouvelle clé cryptographique.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

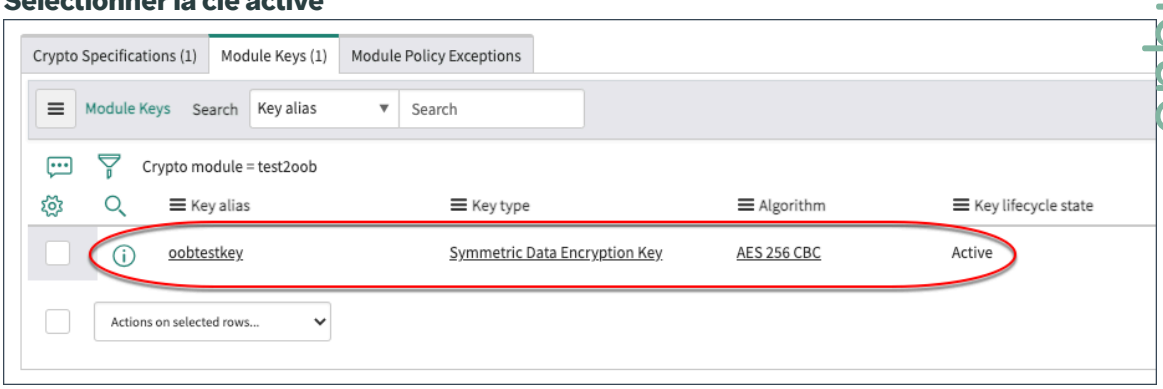
Pourquoi et quand exécuter cette tâche

Contrairement aux contextes de chiffrement, les modules de chiffrement prennent en charge une nouvelle saisie des enregistrements en vue d'un nouveau chiffrement avec une nouvelle clé. L'article suivant montre comment effectuer manuellement une opération de rotation de clés sur un module de chiffrement.

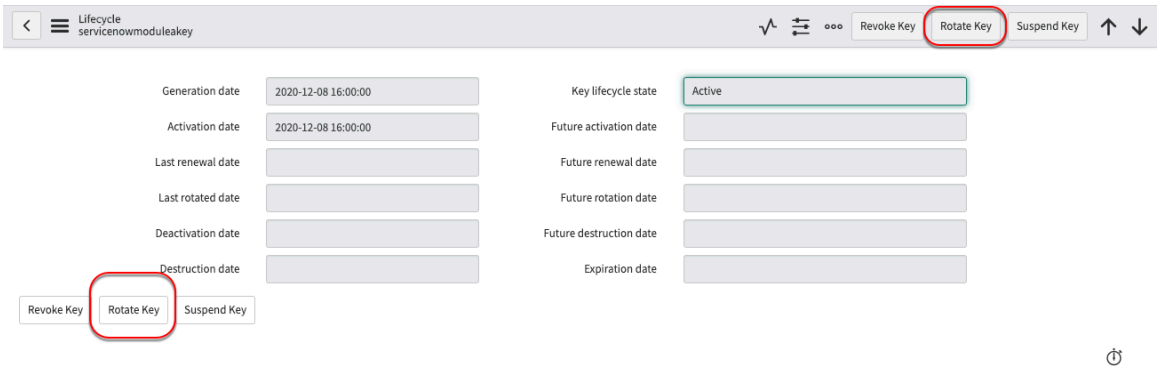
Procédure

1. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tous**.
2. Sélectionnez le module de chiffrement pour la rotation de clé.
3. Dans l'onglet **Clés de module** , sélectionnez la clé Active.

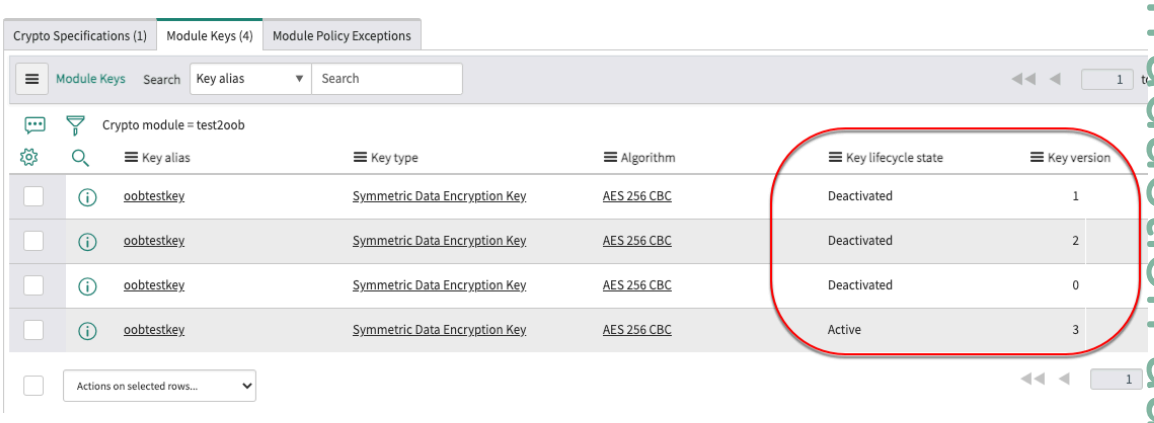
Sélectionner la clé active



Traduction automatique



4. Sélectionnez **Faire pivoter la clé**.
   L'état du cycle de vie de la clé passe à « Désactivé ». Les champs **Dernière date de rotation**, **Date de désactivation** et **Version de clé** sont mis à jour.
5. Retourner à **Module de chiffrement** > **Clés de module**.



Il y a une clé de module supplémentaire répertoriée dans la table. La touche nouvellement tournée devient « Active » 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, l'API REST de clé). 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'encapsulation 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 avant que la clé cible encapsulée puisse être chargée via l'importation à partir des services Web.

Ces deux procédures distinctes (importation de la paire de clés encapsulée 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 cryptographique 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 de l'API Postman pour afficher 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 Key Management Framework 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.

Procédure

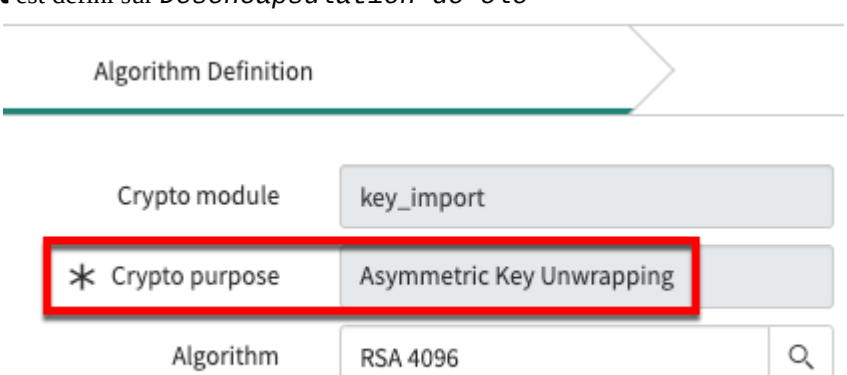
1. Dans votre environnement local, utilisez le terminal pour créer un certificat.
   Par exemple : `openssl req -x509 -sha256 -nodes -days 365 -newkey rsa :4096 -keyout wrapping_private.key -out wrapping_public.crt`

   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 le certificat public (avec la clé d'encapsulation) et la 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 matériau de clé asymétrique pour le magasin de clés importé.
   Consultez Objectif cryptographique, algorithmes et informations clés 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 ») spécifié lors de la génération du certificat ou du magasin de clés à charger. En poursuivant l'exemple ci-dessus, ce serait `wrapping_key_alias`.
10. Sélectionnez **Suivant**.
    La section **Création de clé** comprend un lien **Importer la clé** , qui affiche une boîte de dialogue permettant de charger le magasin de clés. En poursuivant l'exemple, il s'agirait de `wrapping_keystore.p12`.

Importer une clé encapsulée à partir d'un service Web

Chargez votre clé encapsulée dans un module de chiffrement 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 suivies 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)

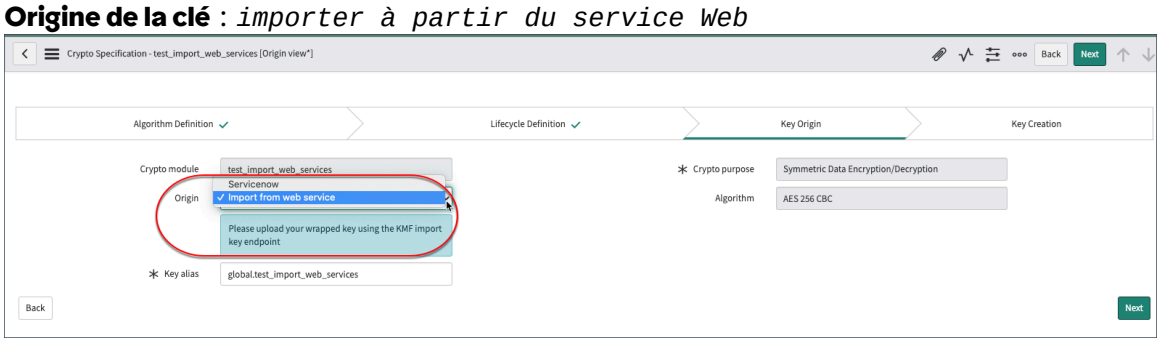
Pourquoi et quand exécuter cette tâche

KMF L'accès au point de terminaison de clé d'importation est requis pour terminer le processus d'importation de clé.

Cet exemple utilise OpenSSL pour générer des clés et des certificats. Vous pouvez substituer d'autres outils comparables en fonction de vos besoins.

Procédure

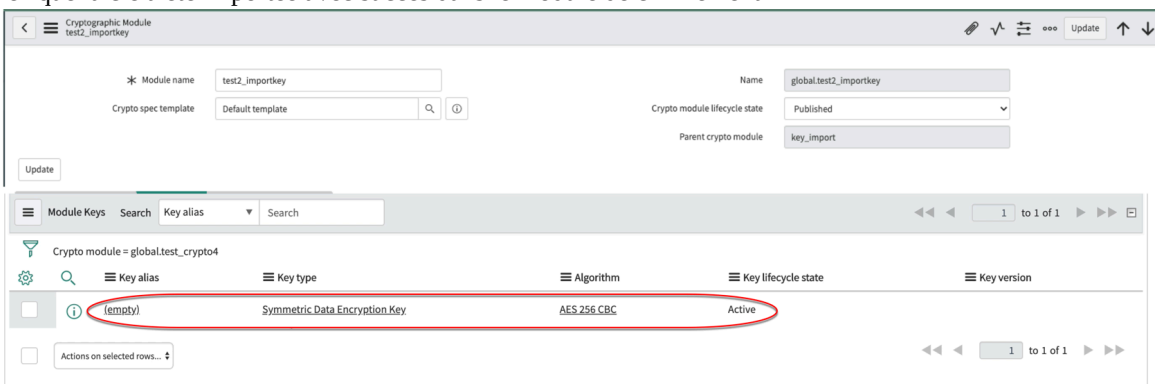
1. À l'aide du terminal de votre périphérique local, encapsulez votre clé symétrique à l'aide de la clé encapsulée de clé publique du module d'importation de clés.
   Par exemple : `openssl pkeyutl -encrypt -pubin -inkey public_wrapping_key.pem -in symmetric_key.bin -pkeyopt rsa_padding_mode :oaep -pkeyopt 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 de chiffrement à lier à l'API.
   Voir ou pour plus d'informations.
3. Ajoutez une spécification cryptographique avec les sélections suivantes.
   - **Objectif de chiffrement** : *`Cryptage/déchiffrement symétrique des données.`*
   - **Origine de la clé** : *`importer à partir du service Web`*



   Voir ou pour plus d'informations.
4. Exécutez une *`demande HTTP POST`* vers l'importation à partir d'un point de terminaison REST de service Web.

L’importation réussie de la clé publique génère 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 aux informations sur l’état de santé sur demande pour le Key Management Framework. Les erreurs d’avertissement et de dysfonctionnement sont accompagnées d’un message détaillé.

Avant de commencer

Rôle requis : auditeur sn_kmf_cryptographic ou sn_kmf_admin ou sn_kmf_cryptographic_manager

Pourquoi et quand exécuter cette tâche

Chaque composant de la Key Management Framework 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 irrécupérable empêche le fonctionnement du composant, 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 sont signalés comme ayant mal fonctionné, le parent signale également un dysfonctionnement.

Pour plus d’informations sur les sous-composants, reportez-vous à la section Clés au niveau de l’instance dans Key Management Framework.

Remarque :
Les vérifications de l’intégrité s’exécutent toutes les 15 secondes. Actualisez la page d’intégrité pour réexécuter le rapport.

Procédure

1. Accédez à la **Tous** > **Gestion des clés** > > **Diagnostics**.
2. Passez en revue les informations suivantes sur l'état de santé :

Informations de diagnostic

Catégorie	Détails
Clé sécurisée	Vérifie si le chiffrement est tenté.
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 (en anglais seulement)	Vérifie si un module cryptographique, une spécification et une clé au niveau de l'instance GlideEncrypter sont présents. **Remarque :** GlideEncrypter est un composant pouvant contenir des scripts qui permet le chiffrement transparent des champs et d'autres utilisations de Password2 chiffrement héritées via le Key Management Frameworkfichier .
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 récupérés à partir du cache et du LDAP.
PKI d'instance	Recherche une clé dans le magasin de clés de fichier et KeySecure et si le certificat est présent et correspond à la clé symétrique. **Remarque :** L'instance PKI n'est disponible que sur les instances d'un centre de ServiceNow données.

Pour obtenir de l'aide sur le dépannage, contactez Service et assistance client.

Préparer votre instance pour la dépréciation de GlideEncrypter

Utilisez un script d'analyse d'instance pour rechercher 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.

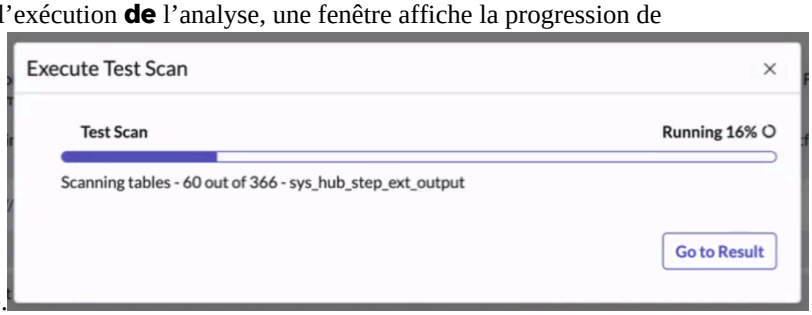
Avant de commencer

Rôle requis : admin

L'API GlideEncrypter devrait être obsolète à compter de la version Xanadu du ServiceNow. La suppression des appels GlideEncrypter de votre script est également une étape nécessaire avant de déconseiller le chiffrement 3DES sur votre instance.

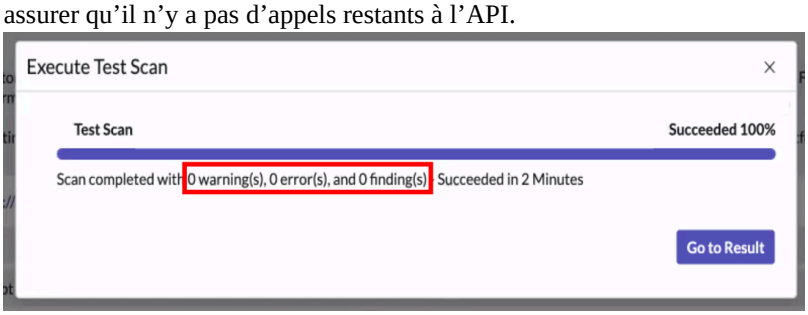
Procédure

1. Accédez à la **Tous** > **Instance Scan** > **Suites**.
2. Dans la liste **Suites** , sélectionnez **API déconseillées**
3. Dans l'enregistrement **Suites** , sélectionnez **API déconseillée : GlideEncrypter** dans la liste connexe **Vérifications** .
   La **vérification du type de colonne** s'affiche. Cet enregistrement contient une description de la vérification, ainsi que des informations et des liens sur la façon de mettre à jour les enregistrements trouvés par la vérification.
4. Dans l'enregistrement **Vérification du type de colonne** , sélectionnez **Tester la vérification** pour exécuter l'analyse.
   Pendant l'exécution **de** l'analyse, 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** .
   Dans l'enregistrement **des résultats de l'analyse**, la liste des conclusions de l'analyse affiche une liste des enregistrements sur votre instance qui utilisent l'API **GlideEncrypter**.
6. Sélectionnez le champ **Nombre** de la liste **Conclusions de l'analyse** pour accéder à un enregistrement.
7. Modifiez tous les scripts de l'enregistrement qui utilisent l'API **GlideEncrypter** .
   Pour plus d'informations sur les alternatives à **GlideEncrypter**, consultez Alternatives aux API GlideEncrypter obsolètes .
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 3DES par GlideEncrypter pour les champs password2

Déconseiller l'utilisation de 3DES par GlideEncrypter pour les champs password2

Déconseiller l'utilisation par GlideEncrypter de la norme de chiffrement 3DES sur votre instance afin de vous assurer que votre instance utilise la norme AES (Advanced Encryption Standard), plus sécurisée, exclusivement pour le chiffrement et le déchiffrement de vos données Password2.

À partir de Rome, les données password2 sont protégées à l'aide de , Key Management Frameworkqui utilise l'algorithme AES (Advanced Encryption Standard) plus moderne. Toutefois, certaines configurations et secours dans la logique password2 peuvent toujours utiliser l'algorithme 3DES pour le chiffrement et le déchiffrement.

Dans cette Vancouver version, les administrateurs peuvent choisir de déconseiller entièrement l'algorithme 3DES. Une fois cette modification terminée, votre instance utilise le chiffrement AES exclusivement pour toutes les tâches de chiffrement et de déchiffrement relatives aux données password2. Cette modification offre une meilleure sécurité de l'instance que le chiffrement 3DES et est nécessaire pour rester conforme au NIST.

Éléments à prendre en considération avant l'obsolescence

Transfert de données password2 entre instances

Lors du transfert de textes chiffrés password2 vers d'autres instances, vous devez vous assurer que cette option KMF Key Exchange est activée entre les instances source et cible. Cette configuration garantit que les clés utilisées pour chiffrer les textes password2 sont disponibles sur les deux instances afin de déchiffrer les textes chiffrés password2. Avant de déconseiller 3DES, prenez en compte les cas d'utilisation suivants qui peuvent avoir un impact sur les données password2 entre les instances.

- Si vous disposez d'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 de niveau 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 de clés.
- Si vous envisagez 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 chiffrer les données password2 sur l'instance source sont disponibles sur les instances cibles pour le déchiffrement. Pour obtenir des détails sur cette configuration, reportez-vous à Échange de clés dans le cadre de travail de gestion de clés.

> **Important :**
> Les exemples ci-dessus sont des scénarios plus courants, mais si vous utilisez d'autres moyens pour transférer du texte chiffré password2 entre des 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 l'obsolescence de 3DES

Ce qui suit s'applique uniquement aux instances dont les champs password2 ont des longueurs d'entrée supérieures à 125 caractères et que vous avez déjà déconseillé le chiffrement 3DES.

Pour passer à une version antérieure Vancouver d'une instance 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 du champ password2.
2. Si c'est le cas, contactez le support technique avant de demander un clone.ServiceNow Dans le champ **Motif** , utilisez « Cloner la version antérieure préalable à la prise en charge de password2 ».

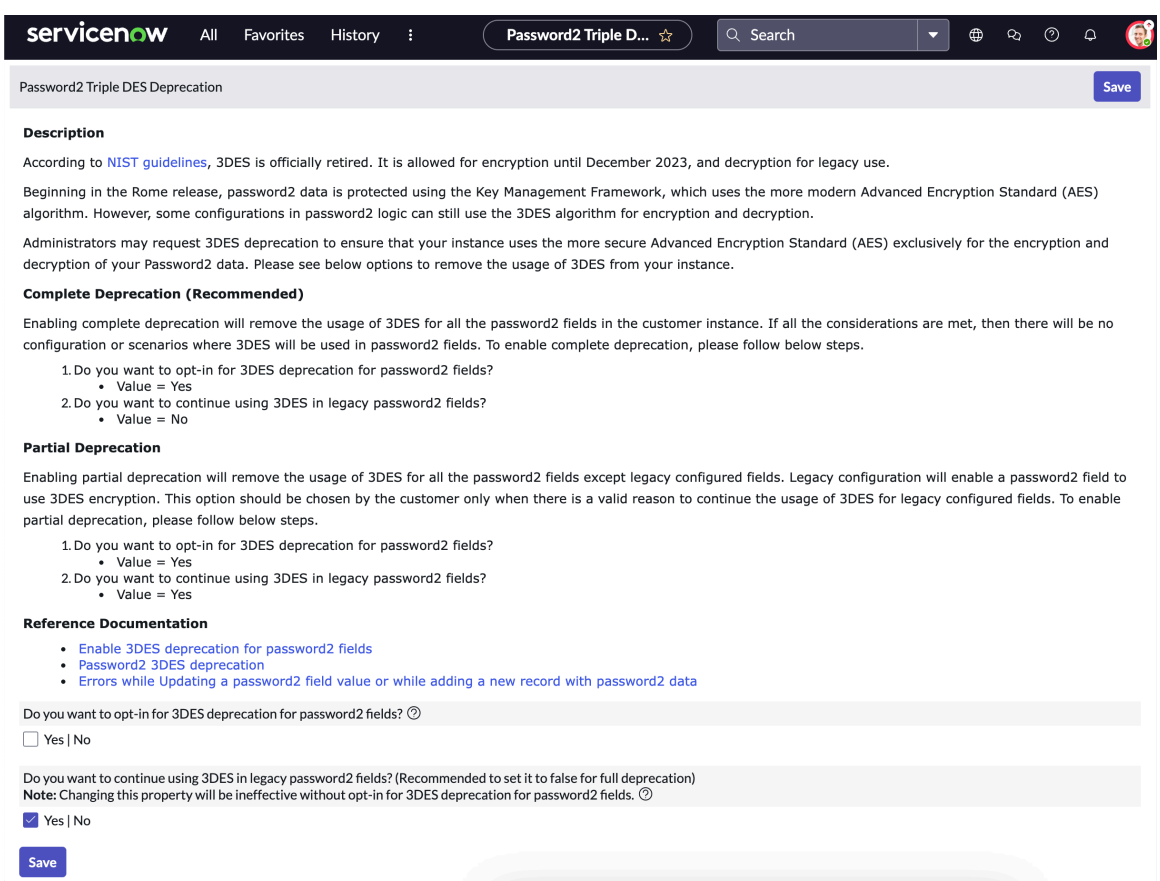
Champs password2 hérités

Votre instance utilise le chiffrement 3DES pour convertir les données password2 en données password2 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 la dépréciation partielle (voir les détails dans la section suivante).

Comment déprécier 3DES

Une fois que vous avez examiné les cas d'utilisation précédents, activez l'obsolescence partielle ou totale en fonction de vos besoins. Pour l'une ou l'autre option, vous pouvez accéder au formulaire pour contrôler l'obsolescence en accédant à **Tous** > **Sécurité de système** > **Conformité de la sécurité** > **Obsolescence de Triple DES Password2**.

Important :
Vous devez vous élever au rang d'administrateur de sécurité pour voir le module **Conformité de la sécurité** et effectuer ces étapes. Pour obtenir plus de détails sur ce processus, voir Élever à un rôle privilégié.



Traduction automatique

Le formulaire **d'obsolescence Triple DES de Password2** contient des informations sur le processus d'obsolescence complète et partielle de 3DES. Sélectionnez les options d'obsolescence totale ou partielle, puis sélectionnez **Enregistrer**.

Dépréciation complète

L'activation de l'obsolescence complète supprime l'utilisation de 3DES pour tous les champs password2 dans votre instance. Si toutes les conditions préalables sont remplies, il n'y a pas de configuration ou de scénarios où 3DES est utilisé dans les champs password2.

Pour activer l'obsolescence complète :

- Sélectionnez **Voulez-vous accepter l'obsolescence 3DES pour les champs password2 ?**
- **Voulez-vous continuer à utiliser 3DES dans les champs password2 hérités ?**

Dépréciation partielle

L'activation de l'obsolescence partielle supprime l'utilisation de 3DES pour tous les champs password2, à l'exception des champs configurés hérités. Les champs password2 de configuration hérités continuent d'utiliser le chiffrement 3DES. Sélectionnez cette option uniquement si vous devez continuer à utiliser 3DES pour les champs configurés hérités.

Pour activer l'obsolescence partielle :

- Sélectionnez **Voulez-vous accepter l'obsolescence 3DES pour les champs password2 ?**
- Sélectionnez **Voulez-vous continuer à utiliser 3DES dans les champs password2 hérités ?**

Après l'indisponibilité de GlideEncrypter

Une fois le processus d'obsolescence terminé, les informations suivantes s'appliquent à votre instance.

- 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 inchangées 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 KMF l'aide d'AES.
- Dans certains cas, 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, reportez-vous aux informations d'assistance dans l'article KB1296997 de la base de connaissances.

Échange de ressources du cadre de travail de gestion de 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, consultez 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 entre les instances.
Instance de source de clé (source de clé)	L'instance qui possède les clés.
Instance cible de clé (cible de clé)	L'instance qui demande les clés.

Vue d'ensemble

Resource Exchange utilise les API cryptographiques pour assurer la confidentialité, l'intégrité, l'authentification et la KMF non-répudiation. Resource Exchange Prend actuellement en charge la Key Exchange fonctionnalité. Consultez Échange de clés dans le cadre de travail de gestion de clés pour plus d'informations.

Échange de clés dans le cadre de travail de gestion de clés

KMF Key Exchange est une fonction sous-ensemble de KMF Resource Exchange. Key Exchange transfère en toute sécurité des données chiffrées sur plusieurs instances.

Vue d'ensemble de Key Exchange

Key Exchange Transfère les clés en toute sécurité entre les instances.

KMF Key Exchange fournit aux clients un moyen sécurisé d'échanger KMF des clés entre les instances. Un cas d'utilisation d'application est le processus de clonage de données. Avec Key Exchange, les clés du module de chiffrement sont copiées lors du clonage de données des KMF composants. Les modules de chiffrement, les spécifications de clé de module et les politiques d'accès aux modules sont inclus dans le processus de clonage. La remise des clés n'est pas incluse.

Utiliser Key Exchange

Les administrateurs qui utilisent KMF pour le chiffrement au niveau des colonnes peuvent Key Exchange cloner les clés entre les instances de production lors du clonage de données. Dans le clonage de données, l'administrateur/ KMF responsable cryptographique peut effectuer les opérations suivantes :

- Échangez toutes les clés vers les autres instances.
- Échangez des clés particulières une fois ou périodiquement à l'autre instance.
- Envoyez des demandes sur demande de l'instance cible à l'instance source clé.
- Échangez des clés de la source vers la cible pour retaper le texte chiffré.
  - Gérez le délai d'expiration de la demande avec la possibilité de supprimer des clés ou de rejeter la demande d'échange de clé si la demande a expiré.
  - Une fois la requête terminée et la clé importée, la clé utilisée sera définie comme expirée et horodatée.
  - Retapez le texte chiffré sur l'instance cible qui a été chiffrée avec les clés de la source.

Modes pris en charge

Key Exchange prend en charge plusieurs modes au niveau de la 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 au courant)	L'administrateur envoie à la source une demande sur demande sur l'instance cible. La demande doit être approuvée par un administrateur sur l'instance de source de clé.
Renouvellement de saisie (demande automatisée)	L'administrateur sélectionne l'option de nouvelle saisie pendant le processus de configuration du clonage.

Configurer l'échange de clés

Key Management Framework (KMF) génère des demandes automatiques d'échange de clés 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 de chiffrement avec une clé doit être créé dans les instances cible et source avant d'utiliser Key Exchange.

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 automatique de clés est actif par défaut lors du clonage d'une instance, où la propriété est clonée vers l'instance cible. KMFAvec , configurez les propriétés système pour gérer la façon dont les clés sont traitées pendant un clone d'instance :

- **Désactivez l'échange automatique de clés :** 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 **false** si vous utilisez la Renouvellement de saisie du texte chiffré avec Key Exchange fonctionnalité d'échange de clés récurrente ou la fonctionnalité Récurrent. Consultez la rubrique Procédure pas à pas récurrente d'échange de clés pour en savoir plus.

Procédure

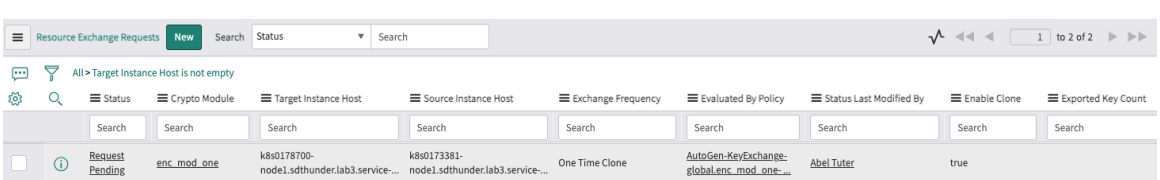
1. Accédez à la **Tous** > **Gestion des clés** > **Demandes d'échange de ressources** > **Nouveau**.
2. Renseignez les champs du formulaire.

Traduction automatique

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 l'sys_id d'instance et les informations d'hôte pour la source. Non pris en charge avec le renouvellement de 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 le sys_id de l'instance source à laquelle demander les clés. ○ **Clone unique**, **clone récurrent** : saisissez le sys_id de l'instance cible qui envoie les demandes. **Conseil :** Saisissez stats.do dans Application Navigator pour localiser l'ID d'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 d'un module de chiffrement définissent les clés à cloner. Pour les demandes de clone uniques et récurrentes, votre instance crée 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 Référencer à l'aide de la liste (pour parcourir les spécifications de chiffrement disponibles.
Activer le renouvellement de saisie après l'importation de la clé	Option permettant d'activer le renouvellement de saisie automatique.

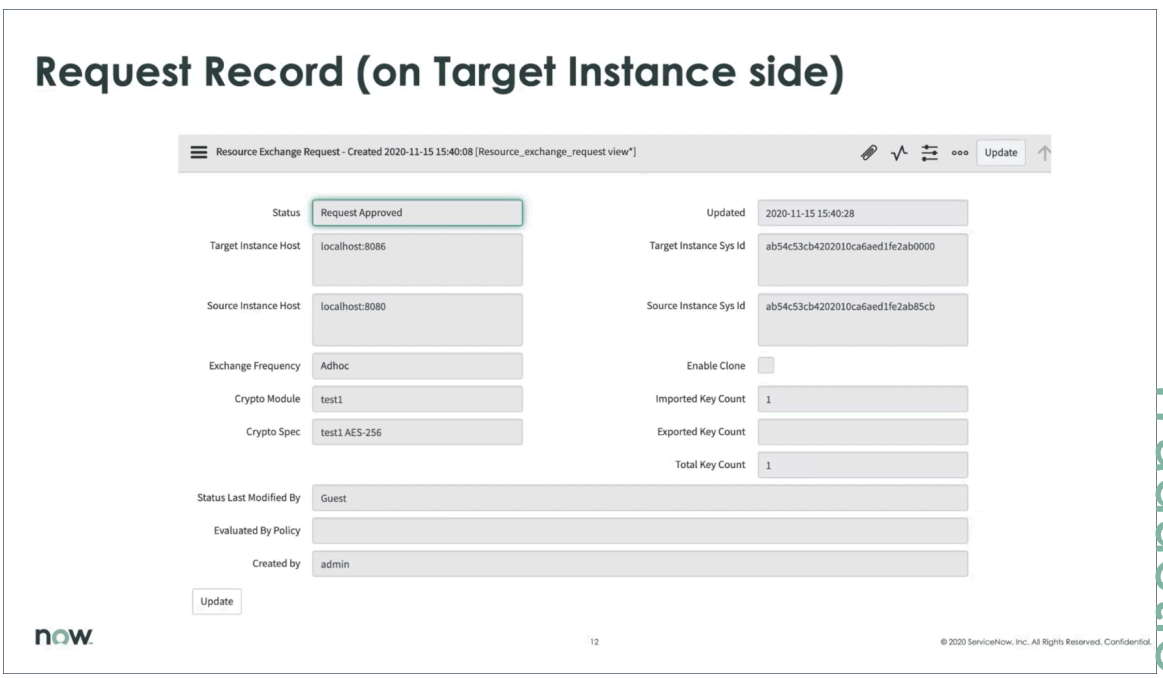
3. Sélectionnez **Envoyer**.
En cas de réussite, une confirmation s'affiche en haut du formulaire. La table Demandes est mise à jour avec une entrée Demande **en attente** dans l'instance source et dans l'instance cible. Ouvrez l'enregistrement de demande pour afficher l'état de la demande, le nombre de clés importées et le nombre total de clés sur l'hôte cible ou source.



Traduction automatique

4. La demande en attente est acceptée dans l'instance source pour terminer l'échange.

   Au moment du clone, la politique d'accès au module sur l'instance source est appelée pour approuver automatiquement la demande et envoyer les clés à la cible nouvellement clonée.



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 **true**. Sinon, la propriété a la valeur **false**. Si la valeur est définie sur faux, l'instance tente de chiffrer à nouveau le lendemain.

Renouvellement de saisie du texte chiffré avec Key Exchange

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 le chiffrement au niveau des colonnes peuvent l'utiliser Key Exchange pour retaper les clés de chiffrement entre les instances de production lors du clonage de données. Une clé active doit d'abord être disponible sur l'instance cible pour une nouvelle saisie, car la nouvelle saisie nécessite une clé active. Une tâche de chiffrement est automatiquement créée et exécutée par le système pour faire pivoter et retaper la clé source, puis chiffrer à nouveau le texte chiffré.

Utilisez l'application Key Exchange pour effectuer les actions suivantes :

- Définissez un délai d'expiration pour la nouvelle saisie.

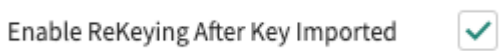
  Si la demande a expiré, elle est rejetée et la clé est supprimée.

- Automatisez la renouvellement de saisie du texte chiffré avec les clés 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 clé est défini pendant le processus de clonage et est automatisé dans le cadre du clone.
- L'activité de renouvellement de saisie est suivie dans l'onglet **Clé de 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 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'activation. Consultez Configurer l'échange de clés pour en savoir plus.



Procédure pas à pas récurrente d'échange de clés

Utilisez cette procédure pas à pas pour configurer un échange de clés récurrent dans votre instance à l'aide de et Resource Exchange.

Avant de commencer

Rôles requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Cet exemple montre comment une instance cible demande des clés à une instance hôte.

- Avant de pouvoir effectuer cette procédure, vous devez cloner une instance. Reportez-vous à la section Clone système pour plus d'informations.
- **Échange de clés automatique** : la propriété `glide_encryption.auto_key_exchange.enabled` système de base est **définie sur 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'option automatique en définissant la propriété sur **faux**.

Procédure

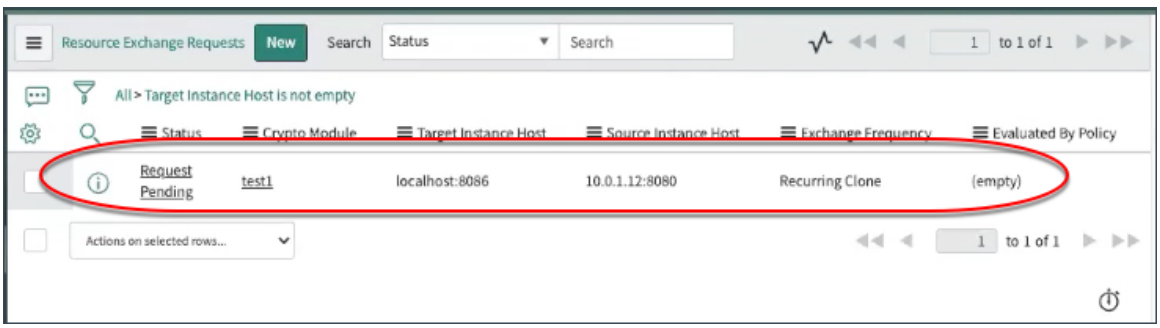
1. Sur l'instance source, créez un module de chiffrement ou accédez à un module de chiffrement existant à l'aide de column_level_encryption et configurez les configurations de champs chiffrés pour le chiffrement du texte chiffré pour Key Exchange.
   Voir et pour plus de détails.

   a. Assurez-vous que les clés ont été générées dans le module de chiffrement.

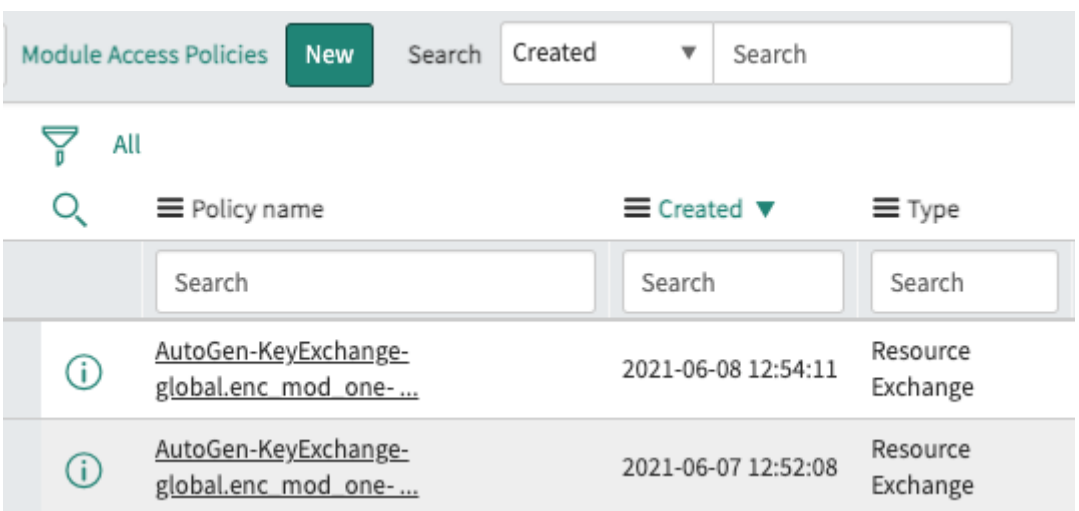
   Remarque :
   Votre instance crée automatiquement une politique d'accès au module lors de l'exécution de la demande de clone.

2. À partir de 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. À partir de l'instance cible du clone, accédez à **Gestion des clés** > **Demandes d'échange de ressources**.
   La demande de l'instance hôte est affichée dans la table.

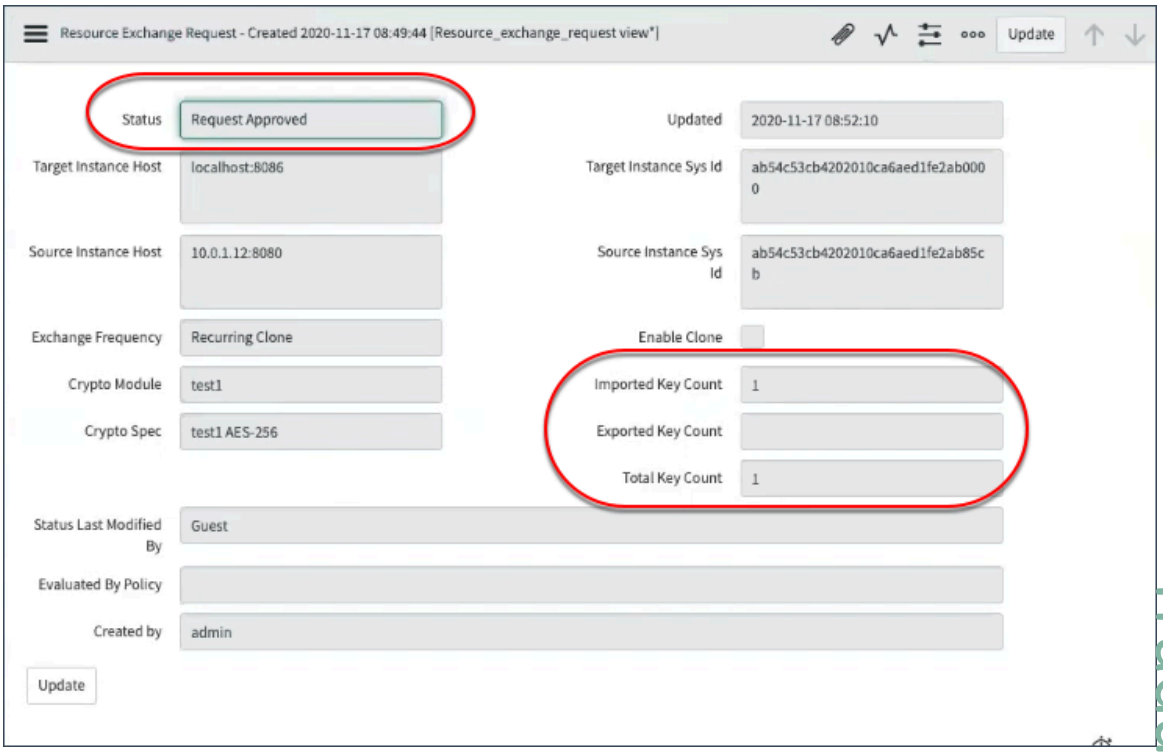


Important :
Pour les demandes de clone ponctuelles et récurrentes, votre instance crée automatiquement une politique d'accès au module. Vous n'avez pas besoin de configurer une politique manuellement. Au moment du clonage, cette politique sur l'instance source est invoquée pour approuver automatiquement la demande et envoyer des clés à la cible nouvellement clonée.

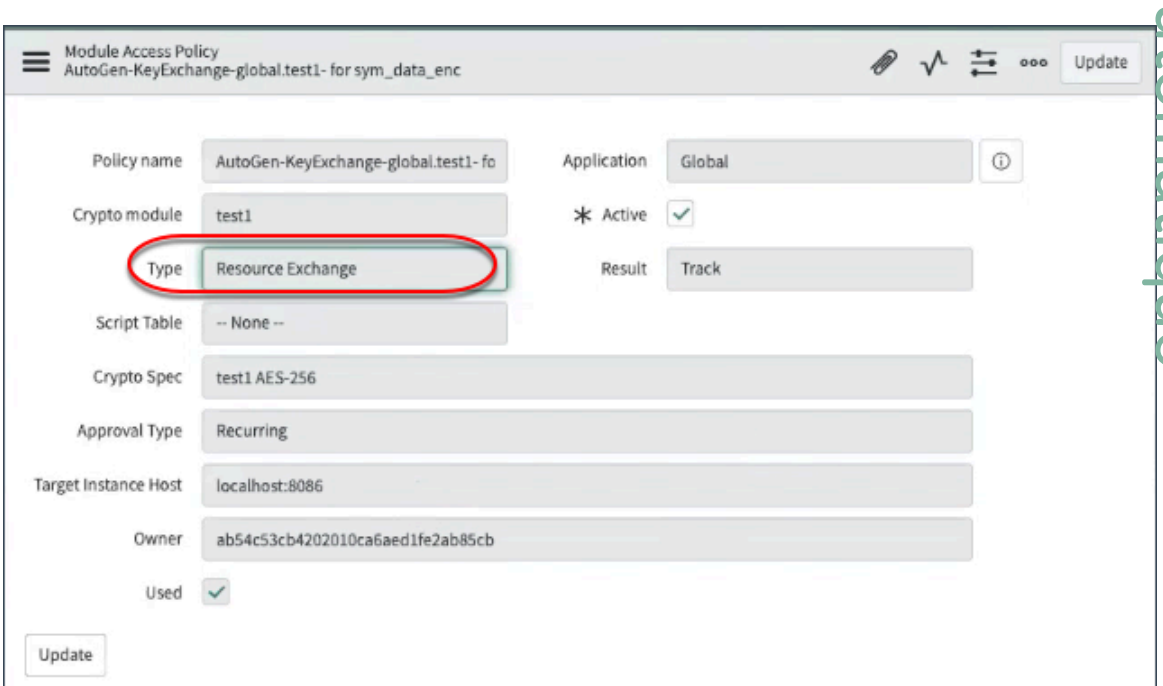


Dans le formulaire Demandes, l'état passe à **Demande approuvée** et le champ **Nombre de clés importées** apparaît dans l'enregistrement.

Traduction automatique



5. Revenez à l'instance hôte.
6. Affichez l'enregistrement de demande pour voir le nombre de clés exportées.
7. Affichez l'enregistrement de la politique d'accès au module pour vérifier que le **type** est Resource Exchange.



Remarque :
Resource Exchange prend également en charge la nouvelle saisie du texte chiffré sur l'instance cible. Voir pour plus de détails.

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 **true**. Sinon, la propriété a la valeur **false**. Si la valeur est définie sur false, votre instance tentera de chiffrer à nouveau le lendemain.

Chiffrement au niveau des colonnes

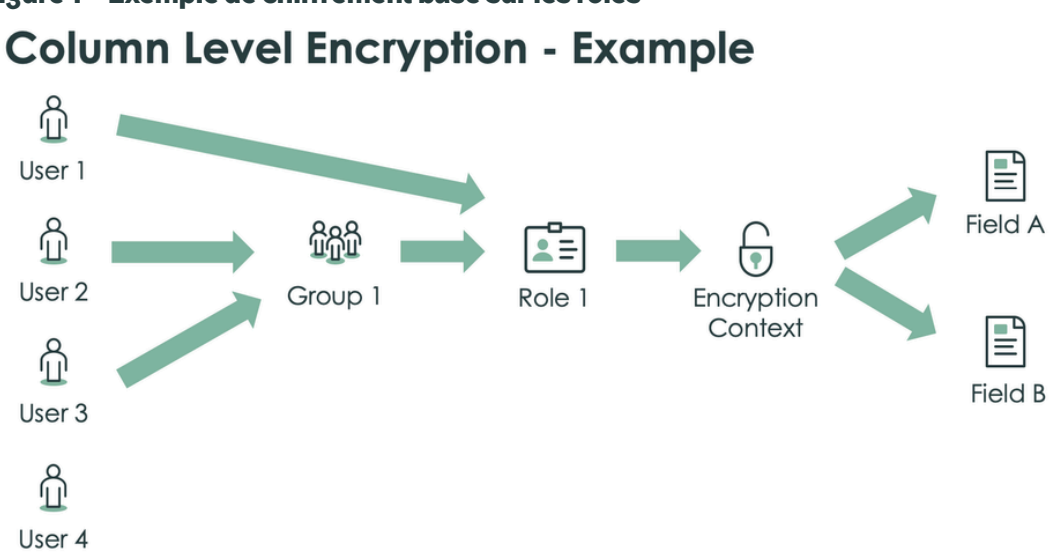
Column Level Encryption (CLE), anciennement Support de chiffrement, autorise et refuse l'accès aux données chiffrées en fonction du rôle de l'utilisateur. Column Level Encryption a été amélioré pour inclure la gestion de base des clés à l'aide de modules de chiffrement sans frais supplémentaires.

À propos de Column Level Encryption

Remarque :
Les contextes de chiffrement précédemment configurés sont automatiquement convertis en modules de chiffrement. Column Level Encryption (CLE) est une amélioration gratuite de la sécurité de la prise en charge du chiffrement. Pour en savoir plus sur les options de chiffrement, reportez-vous à Offre groupée d'abonnements Chiffrement et gestion des clés.

L'implémentation du chiffrement au niveau des colonnes commence par la définition d'un ou de plusieurs modules de chiffrement dans vos instances du Now Platform. Ce processus comprend la sélection d'un algorithme de chiffrement et la fourniture d'une clé secrète appropriée. L'accès aux données chiffrées ultérieurement à l'aide de cette fonctionnalité est basé sur les rôles, les modules étant associés à des rôles. Les utilisateurs sans le rôle approprié ne voient pas du tout le champ. La figure 1 illustre le fonctionnement du chiffrement basé sur les rôles.

Figure 1 – Exemple de chiffrement basé sur les rôles



Voici les résultats des relations de la figure 1 :

- L'utilisateur 1 est un membre du rôle 1, qui donne accès au module de chiffrement 1. L'utilisateur 1 peut voir le contenu des champs A et B.
- L'utilisateur 2 et l'utilisateur 3 sont membres du groupe 1. Le groupe 1 est membre du rôle 1, qui permet à tous les membres du groupe 1 d'accéder au module de chiffrement 1 et permet aux utilisateurs 2 et 3 de voir le contenu des champs A et B.

- L'utilisateur 4 n'est membre d'aucun groupe ou rôle et n'a pas accès au module de chiffrement 1. Non seulement l'utilisateur 4 n'a pas accès aux champs A ou B, mais l'utilisateur 4 ne voit même pas ces champs sur un formulaire. Dans une vue de liste, les valeurs seraient vides.

Vous pouvez également mettre en œuvre un chiffrement basé sur les rôles beaucoup plus complexe.

L'accès basé sur les rôles doit également être implémenté de manière appropriée pour que ce champ soit accessible aux utilisateurs qui sont affectés au module de chiffrement via un rôle.

Toutes les clés de chiffrement client à utiliser avec column-level encryption sont stockées dans la même base de données d'instance unique où sont stockées les données chiffrées. Par mesure de sécurité supplémentaire, ils sont chiffrés à nouveau avec une clé secondaire unique pour cette instance, ce qui limite l'accès direct à la clé de chiffrement pour tout module de chiffrement, soit par un administrateur d'instance, soit ServiceNowpar .

Les données chiffrées au niveau des colonnes ne peuvent pas être filtrées.

Chiffrement au niveau des colonnes :

- L'accès aux données chiffrées est déterminé par le rôle d'utilisateur.
- Vous pouvez choisir la force de l'algorithme de chiffrement : AES-128 ou AES-256.
- Vous pouvez chiffrer le texte de chaîne, les champs Date et Date/heure, les pièces jointes et les URL.
- Les modules de chiffrement fournissent un chiffrement préservant l'égalité.

Entreprise de Chiffrement au niveau des colonnes prend en charge les fonctionnalités supplémentaires suivantes :

- Clés fournies par le client.
- L'accès à la clé permet aux sessions utilisateur d'accéder au module et la clé peut accéder à d'autres processus utilisateur back-end ou système.
- Accès aux scripts Resource Exchangeet aux applications
- Prise en charge avancée des pièces jointes.
- L'accès à l'interface de programmation d'application (API) est disponible.
- Ordre La préservation du chiffrement ou le chiffrement standard non déterministe ne sont pas pris en charge.

Éditions Standard et Enterprise

Column Level Encryption est disponible en versions standard et entreprise. Column Level Encryption Enterprise est un module d'extension payant qui fournit des fonctionnalités supplémentaires ainsi qu'un plus grand nombre de modules et de politiques d'accès aux modules.

Fonctionnalités de Column Level Encryption par version

Chiffrement au niveau des colonnes	Entreprise de Chiffrement au niveau des colonnes
• L'accès aux données chiffrées est déterminé par le rôle d'utilisateur • Prise en charge d'un maximum de 5 modules et politiques d'accès aux modules (MAP) • Algorithmes de chiffrement AES-128 et AES-256 • Chiffrement du texte de chaîne, des champs Date et Date/heure, des pièces jointes et des URL. • Les modules de chiffrement fournissent un chiffrement préservant l'égalité. • Mise à jour des API `getDisplayValue()` et `setDisplayValue()` qui peuvent renvoyer des valeurs en clair et insérer des données chiffrées pour les champs chiffrés	En plus des fonctionnalités répertoriées à gauche, Column Level Encryption Enterprise prend en charge ces fonctionnalités supplémentaires. • Prise en charge de plus de 5 modules et politiques d'accès aux modules (MAP) • Chiffrement pour les types de champs supplémentaires, tels que les champs journal, HTML et traduits. • Rotation automatique des clés configurable. • Clés fournies par le client. Gérez le cycle de vie complet de vos clés de chiffrement de données. Vous pouvez éventuellement échanger en toute sécurité les clés de chiffrement des données générées au sein de votre environnement. • Clés cryptographiques éphémères • Mise à jour des API `getValue()` et `setValue( )`.

Pour plus d'informations sur la version entreprise de ce produit, voir Entreprise de Chiffrement au niveau des colonnes

Méthodes de chiffrement

Les champs qui utilisent Column Level Encryption peuvent inclure :

- Champs de texte chiffré nouveaux ou existants.
- Les champs Chaîne, Date, Date/Heure ou URL inclus dans les enregistrements de configuration de champ ont été chiffrés.

La table Configurations des champs chiffrés [*sys_platform_encryption_configuration*] contient un enregistrement pour chaque champ chiffré avec Column Level Encryption. Cette table permet à un administrateur de sécurité de surveiller tous les champs de l'instance qui utilise Column Level Encryption.

Remarque :
Lors de la mise à niveau, les enregistrements de configuration des champs chiffrés sont créés pour tous les champs de texte chiffrés existants. Lorsqu'un nouveau champ de texte chiffré est ajouté, un enregistrement de configuration de champ chiffré est créé par défaut.

Les configurations de champs chiffrés peuvent chiffrer des champs à l'aide de l'une des méthodes suivantes.

Méthode	Description
Module de chiffrement unique	Le champ est chiffré avec la méthode de chiffrement définie dans le champ du module de chiffrement. Les utilisateurs qui ne disposent pas d'un accès chiffré au module ne peuvent pas afficher ni mettre à jour les valeurs de champ.
Plusieurs modules de chiffrement	Le champ est chiffré avec le module de chiffrement du premier utilisateur à saisir des données dans ce champ. Si l'utilisateur dispose de deux modules de chiffrement ou plus, le module défini dans le sélecteur de module de chiffrement est utilisé. Étant donné que le module de chiffrement est défini pour chaque enregistrement, les champs d'une liste peuvent avoir différents modules de chiffrement. Toutefois, au sein d'un enregistrement unique, le champ ne peut être chiffré que par un seul module. Lorsqu'un champ Texte chiffré est créé, une configuration de champ chiffré est créée avec la méthode des modules de chiffrement multiples. Les champs de texte chiffré et les champs chiffrés avec la méthode de modules de chiffrement multiples se comportent de la même manière. **Remarque :** Le chiffrement en masse n'est pas disponible lors de l'utilisation de la méthode des modules de chiffrement multiples.

Accès aux données chiffrées

Un module de chiffrement détermine l'accès aux données chiffrées. Security_admin utilisateurs peuvent donner une politique d'accès au module de chiffrement à un utilisateur en lui attribuant un rôle associé.

Pour surveiller l'affectation des rôles, le service client ou professionnel peut mettre en place des mesures de sécurité. Par exemple, un e-mail peut être envoyé à un gestionnaire de chiffrement désigné chaque fois qu'un rôle associé à un module de chiffrement est accordé à un utilisateur.

Remarque :
L'emprunt d'identité ne modifie pas le module de chiffrement disponible pour un utilisateur. Même en empruntant une identité, vous n'avez à votre disposition que les modules de chiffrement à l'origine. Cette fonctionnalité est introduite dans Vancouver.

Niveau d'accès	Accès aux données d'un champ à l'aide de la méthode du module de chiffrement unique	Accès aux données d'un champ à l'aide de la méthode des modules de chiffrement multiples
Utilisateur sans modules de chiffrement	Le formulaire masque le champ chiffré. Dans la vue de liste, le champ apparaît vide et ne peut pas être modifié, même si les données du champ sont déchiffrées.	Le formulaire masque le champ chiffré. Dans la vue de liste, le champ apparaît vide et ne peut pas être modifié, même si les données du champ sont déchiffrées.
Utilisateur avec un module de chiffrement	Pour utiliser le champ, l'utilisateur doit avoir accès aux modules de chiffrement définis dans la configuration du champ chiffré. Si l'utilisateur n'a pas accès aux modules de chiffrement, le formulaire masque le champ.	L'utilisateur utilise automatiquement ses modules de chiffrement avec le champ chiffré.

Niveau d'accès	Accès aux données d'un champ à l'aide de la méthode du module de chiffrement unique	Accès aux données d'un champ à l'aide de la méthode des modules de chiffrement multiples
	Dans la vue de liste, le champ apparaît vide et ne peut pas être modifié. • S'il n'y a pas de données dans le champ : ◦ Si l'utilisateur a accès au module de chiffrement, le formulaire affiche le champ (en supposant que la politique d'interface utilisateur ne l'empêche pas). ◦ Les utilisateurs ayant accès au module de chiffrement peuvent afficher et mettre à jour le champ vide. ◦ Les données saisies dans le champ sont chiffrées avec le module de chiffrement défini dans la configuration du champ chiffré. • S'il y a des données dans le champ : si l'utilisateur a accès au module de chiffrement, il peut afficher et modifier les données dans le champ.	• S'il n'y a pas de données dans le champ : ◦ Le formulaire affiche le champ (en supposant qu'il ne soit pas empêché par une politique d'interface utilisateur). ◦ Les utilisateurs disposant de n'importe quel module de chiffrement peuvent afficher et mettre à jour le champ vide. ◦ La saisie de données dans le champ entraîne l'utilisation par le module de chiffrement actuellement sélectionné pour le chiffrement des données. • Si des données sont contenues dans le champ : si l'utilisateur a accès au module de chiffrement utilisé pour chiffrer le champ, il peut afficher et modifier le champ.
Utilisateur avec deux modules de chiffrement ou plus	Pour utiliser le champ, l'utilisateur doit avoir accès au module de chiffrement défini dans la configuration du champ chiffré. Si l'utilisateur n'a pas accès au module de chiffrement, le formulaire masque le champ. Dans la vue de liste, le champ apparaît vide et ne peut pas être modifié. • S'il n'y a pas de données dans le champ : ◦ Si l'utilisateur a accès au module de chiffrement, le formulaire affiche le champ (en supposant que la politique d'interface utilisateur ne l'empêche pas). ◦ Les utilisateurs ayant accès au module de chiffrement peuvent afficher et mettre à jour le champ vide. ◦ Les données saisies dans le champ sont chiffrées avec le module de chiffrement défini dans la configuration du champ chiffré.	L'utilisateur peut sélectionner un module de chiffrement dans le sélecteur de module de chiffrement de la barre d'accueil. • S'il n'y a pas de données dans le champ : ◦ Le formulaire affiche le champ (en supposant que la politique d'interface utilisateur ne l'empêche pas). Les utilisateurs disposant de n'importe quel module de chiffrement peuvent afficher et mettre à jour le champ vide. ◦ La saisie de données dans le champ entraîne l'utilisation par le module de chiffrement actuellement sélectionné pour le chiffrement des données. ◦ Le champ utilise toujours le module de chiffrement d'origine pour chiffrer les modifications apportées au champ. Ce comportement permet d'empêcher les

Niveau d'accès	Accès aux données d'un champ à l'aide de la méthode du module de chiffrement unique	Accès aux données d'un champ à l'aide de la méthode des modules de chiffrement multiples
	• S'il y a des données dans le champ : ◦ Si l'utilisateur a accès au module de chiffrement, il peut afficher et modifier le champ. ◦ Le champ utilise toujours le module de chiffrement d'origine pour chiffrer les modifications apportées au champ. Ce comportement permet d'empêcher les utilisateurs disposant d'au moins deux modules de chiffrement de modifier le module de chiffrement d'un champ.	utilisateurs disposant d'au moins deux modules de chiffrement de modifier le module de chiffrement d'un champ. • S'il y a des données dans le champ : ◦ Si l'utilisateur a accès au module de chiffrement utilisé pour chiffrer le champ, il peut afficher et modifier le champ. ◦ Le champ utilise le module de chiffrement d'origine pour chiffrer les modifications apportées au champ. Ce comportement permet d'empêcher les utilisateurs disposant de plusieurs modules de chiffrement de modifier le module de chiffrement d'un champ.

Informations de configuration prises en charge

- Les types de champs suivants peuvent être chiffrés :
  - Pièces jointes
  - Date
  - Date/Heure
  - Texte de chaîne
  - URL

Remarque :
D'autres types de champs sont disponibles dans Entreprise. Consultez Entreprise de Chiffrement au niveau des colonnes pour en savoir plus.

- Étant donné que les modules sont liés à des rôles et que les rôles sont liés aux utilisateurs, vous n'avez pas accès aux clés des sessions non-utilisateur. Tout élément en cours d'exécution en tant qu'utilisateur système ou tâche planifiée qui n'a pas de session utilisateur ne peut pas accéder à la clé pour chiffrer ou déchiffrer les données.
- Vous pouvez accéder à la « valeur » ou à la « valeur d'affichage » :
  - Lorsque vous choisissez « valeur », le texte chiffré est renvoyé.
  - Lorsque vous choisissez « valeur d'affichage », à condition que vous disposiez du bon rôle, le texte clair est renvoyé.

  De nombreux scripts dans les couches d'application sont scriptés de telle sorte qu'ils ignorent cette distinction et utilisent la valeur. Si vous ne modifiez pas les scripts pour utiliser la valeur d'affichage, les données ne sont pas chiffrées ou déchiffrées.

Chiffrement de la pièce jointe

Chiffrement des pièces jointes par défaut

Les clients qui utilisent Column Level Encryption ont des pièces jointes chiffrées par défaut dans les 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 qu'une pièce jointe doit être chiffrée manuellement lors du chargement de ces tables.

Désactiver 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 l'assistance.

Pour désactiver cette fonctionnalité, créez un ticket de support avec support et incluez cette déclaration dans un commentaire sur l'enregistrement de ticket :

« Je [nom du client] comprends que je demande de désactiver une bonne pratique de sécurité recommandée pour les pièces jointes, et que [l'entreprise cliente] assume tout risque supplémentaire lié à la configuration et à l'utilisation de pièces jointes non chiffrées dans l'application. »

Filtrage et recherche de champs chiffrés

Lorsqu'un champ de texte chiffré ou un champ avec une configuration de champ chiffré est sélectionné comme opérande de gauche dans un filtre, les opérateurs suivants sont disponibles :

- **est**
- **n'est pas**
- **est vide**
- **n'est pas vide**

Pour les champs Date, utilisez le sélecteur de date pour spécifier la date :

Pour les champs Date/heure, utilisez le sélecteur de date et heure pour spécifier la date et l'heure :

Si un utilisateur avec un module de chiffrement filtre pour l'égalité, ou recherche une valeur dans une liste :

- Seules les valeurs chiffrées avec un module de chiffrement disponible pour l'utilisateur sont renvoyées.
- Les opérateurs **sont vides** et **ne sont pas vides** , renvoient tous les enregistrements correspondants. Les champs chiffrés avec un module de chiffrement non disponible pour l'utilisateur actuel apparaissent vides.

Si un utilisateur ne dispose d'aucun module de chiffrement, aucun enregistrement n'est renvoyé.

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 conditions est pris en charge dans des scripts tels que les politiques d'interface utilisateur et les règles métier.

Exporter des données à partir de champs chiffrés

Lors de l'exportation de champs chiffrés dans une liste ou un formulaire vers un format de fichier, seuls les champs chiffrés par un module de chiffrement apparaissent dans le document exporté. Le module de chiffrement utilisé doit être disponible pour l'utilisateur actuel.

Pour désactiver les exportations de données chiffrées à partir d'une vue de liste, ajoutez la `glide.encryption.export_encrypted_data.allowed` propriété système et définissez la valeur sur **faux**.

Chiffrement sur les tables système

Column Level Encryption ne prend actuellement pas en charge le chiffrement des champs et des pièces jointes des tables système (tables commençant par **sys_**).

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 vous élever au rôle security_admin 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, les utilisateurs voient un sélecteur d'interface utilisateur sur les enregistrements qui ont une configuration de champs chiffrés 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 la propriété système et ouvrez-la.
3. Définissez la **valeur** de la propriété sur `faux`.

Visite guidée Chiffrement au niveau des colonnes

La visite guidée donne un bref aperçu de la configuration de Column Level Encryption (CLE) nécessaire pour chiffrer des champs de table ou des pièces jointes. Les étapes de création de modules de chiffrement de champ, de politiques d'accès au module et de configurations de champs chiffrés sont également abordées. La visite guidée comprend des liens vers la documentation détaillée et le cours Vue d'ensemble de ServiceNow University sur Chiffrement au niveau des colonnes.

Avant de commencer

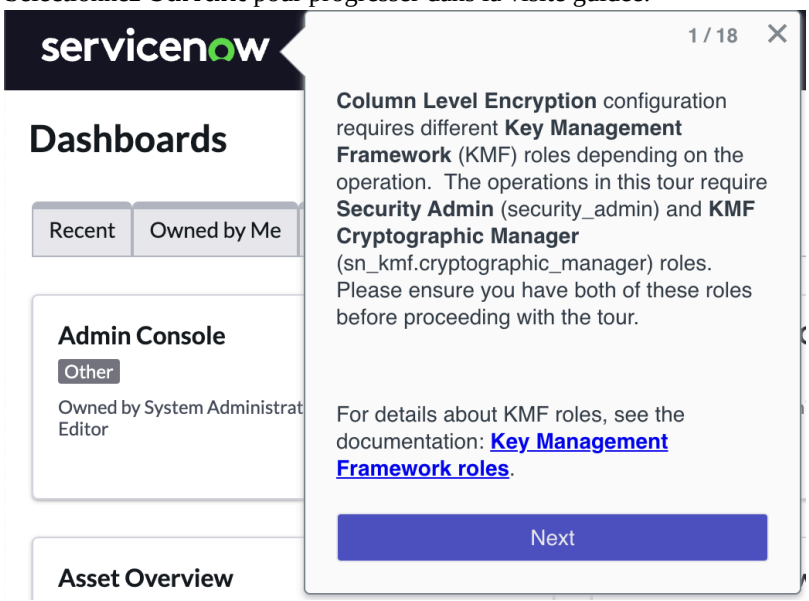
Rôle requis : sn_kmf.crypto_manager ou security_admin

Remarque :
La visite guidée n'est pas encore disponible lorsqu'elle Next Experience est activée.

Procédure

1. Accédez à la page d'interface utilisateur **$pa_dashboards_overview.do** sur votre instance.
   Par exemple : `http://yourcompany.servicenow.com/nav_to.do?uri=%2F$pa_dashboards_overview.do` remplacez `votresociété` par le nom de votre instance.
2. Ouvrez l'icône **Afficher l'aide** ( dans le coin supérieur gauche.
3. Sélectionnez **Effectuer une visite guidée** en bas de la barre latérale.

4. Sélectionnez **Suivant** pour progresser dans la visite guidée.



Entreprise de Chiffrement au niveau des colonnes

Entreprise de Chiffrement au niveau des colonnes (CLE) utilise le Key Management Framework (KMF) pour vous permettre de personnaliser et de gérer entièrement la façon dont les champs et les pièces jointes sont chiffrés et déchiffrés sur votre instance. Un abonnement est requis pour utiliser Entreprise de Chiffrement au niveau des colonnes.

Important :
Cette rubrique couvre la version d'entreprise de Column Level Encryption. Pour en savoir plus sur la version standard de CLE ou pour connaître les différences entre les deux versions, reportez-vous à la section Chiffrement au niveau des colonnes.

Entreprise de Chiffrement au niveau des colonnesest basé sur Column Level Encryption (CLE) et utilise la et sa prise en charge complète des fonctions de gestion des clés. Entreprise de Chiffrement au niveau des colonnes fournit la protection des clés et la gestion du cycle de vie des clés pour le chiffrement des champs au niveau de l'applicationKey Management Framework. Toutes les clés sont protégées par une hiérarchie d'encapsulation de clé enracinée dans les modules de sécurité matériels (HSM) FIPS 140-2-L3.

Entreprise de Chiffrement au niveau des colonnes vous donne la possibilité de gérer la façon dont les champs pris en charge sont chiffrés et déchiffrés conformément aux pratiques NIST 800-57 . Il utilise également la version la plus récente du chiffrement au niveau du champ, y compris l'intégration pour une protection et une gestion appropriées des clés.

Plus précisément, Entreprise de Chiffrement au niveau des colonnes utilise les KMF modules de chiffrement, ce qui vous permet de mieux contrôler le chiffrement côté serveur. KMF Assure une protection adéquate des clés de chiffrement des données à l'aide de la hiérarchie des clés et du chiffrement de l'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 les spécifications de chiffrement et les politiques d'accès et contrôler le contrôle de la gestion du cycle de vie des clés.

Entreprise de Chiffrement au niveau des colonnes prend en charge les politiques d'accès aux modules basées sur :

- Périmètre
- Rôle
- Script
- Échange de ressources
- Utilisateur système

Consultez Créer une politique d’accès au module pour plus d'informations.

Remarque :
Pour en savoir plus sur les fonctionnalités prises en charge par Column Level Encryption et sur la procédure de mise à niveau et d’abonnement à l’autorisation Entreprise de Chiffrement au niveau des colonnes , reportez-vous à Offre groupée d’abonnements Chiffrement et gestion des clés.

Termes de chiffrement

Terme	Description
Gestion des clés 	Prise en charge de la gestion des clés Le Cadre de gestion des clés (KMF) est fondamental Entreprise de Chiffrement au niveau des colonnes . Bénéficiez des options suivantes : • Gestion du cycle de vie des clés. • Rotation des clés. Consultez Faire pivoter les clés pour en savoir plus. • Protection et génération de clés avec les modules matériels de sécurité (HSM) FIPS 140-2-L3. • Séparation des rôles et des tâches. • 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 encapsulation de clé. • Chiffrement non déterministe. • Chiffrement/déchiffrement de masse. • Audit de l’accès et de l’utilisation des clés. Consultez Comprendre le cadre de gestion des clés pour en savoir plus.

Terme	Description
Clé fournie par le client 	Prise en charge des clés fournies par le client L'un des plus grands avantages Entreprise de Chiffrement au niveau des colonnes est que vous pouvez utiliser vos propres clés pour le chiffrement. Les administrateurs ont le choix d'utiliser ServiceNow les clés fournies ou les vôtres (CSK) pour le chiffrement sur le Now Platform® fichier . Vous pouvez également gérer le cycle de vie des clés et décider quand les révoquer, les faire pivoter et les désactiver. Après avoir activé les clés fournies par le client et créé un module de chiffrement, 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 Configurer les propriétés des clés fournies par le client.
Chiffrement au niveau des colonnes 	Prise en charge du chiffrement des champs et du chiffrement des pièces jointes Le chiffrement des champs et le chiffrement des pièces jointes utilisent des modules cryptographiques et des politiques 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 Définir des configurations de champs chiffrés pour en savoir plus et connaître les types de champs pris en charge.
Chiffrement non déterministe 	Prise en charge du chiffrement non déterministe Entreprise de Chiffrement au niveau des colonnes 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 avec Cipher Block Chaining (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, définissez un algorithme de chiffrement et générez la clé. Voir Créer un module cryptographique pour définir les mécanismes utilisés pour les opérations de chiffrement et pour plus d'informations sur l'activation du chiffrement non déterministe.

Terme	Description
Resource Exchange 	Resource Exchange Entreprise de Chiffrement au niveau des colonnes clés d'instance en instance de manière sécurisée à l'aide des API de chiffrement pour garantir la confidentialité, l'intégrité, l'authentification KMF 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 de clés pour en savoir plus.

Remarque :
Si vous choisissez de ne pas activer Entreprise de Chiffrement au niveau des colonnes, vous pouvez toujours utiliser CLE. Les modules Chiffrement au niveau des colonnes autorisent et refusent l'accès aux données chiffrées en fonction du rôle de l'utilisateur. Voir Chiffrement au niveau des colonnes pour plus d'informations.

Entreprise de Chiffrement au niveau des colonnes prend en charge les clients sur site. Domain Separation ne prend pas en charge Domain Separation.

Prise en charge de modules supplémentaires et de politiques d'accès aux modules

La version standard de est limitée à cinq modules et politiques d'accès Chiffrement au niveau des colonnes aux modules (MAP). Entreprise de Chiffrement au niveau des colonnes prend en charge un plus grand nombre de modules et de MAP.

Informations sur les champs pris en charge

Les types de champs suivants peuvent être chiffrés :

- Pièces jointes
- Date
- Date/Heure
- E-mail
- 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 des pièces jointes par défaut

Les clients qui utilisent Column Level Encryption ont des pièces jointes chiffrées par défaut dans les 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 lors du chargement pour ces tables.

Désactiver 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 l'assistance ServiceNow .

Pour désactiver cette fonctionnalité, créez un ticket de support avec ServiceNow support et incluez cette déclaration dans un commentaire sur l'enregistrement de 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 la configuration et à l'utilisation de pièces jointes non chiffrées dans l'application ServiceNow . »

Prise en charge de l'API

Entreprise de Chiffrement au niveau des colonnes 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. Si l'utilisateur n'a pas accès au module cryptographique, `getValue()` renvoie le texte chiffré.

Activer Entreprise de Chiffrement au niveau des colonnes

En s'abonnant à Entreprise de Chiffrement au niveau des colonnes, un administrateur peut activer le module d'extension com.glide.now.platform.encryption.

Avant de commencer

Rôle requis : admin

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 non-production de votre organisation, en général en quelques jours à peine.

Pourquoi et quand exécuter cette tâche

L'activation du module d'extension Entreprise de Chiffrement au niveau des colonnes (com.glide.now.platform.encryption) apporte les modifications suivantes à votre instance :

- Le module d'extension Support de chiffrement (com.glide.encryption) est également activé.

  Remarque :
  Le Key Management Framework module d'extension (com.glide.kmf.global) est déjà actif par défaut.

- La propriété `glide_encryption.set_value_support_cle.disabled` est définie sur **faux**, ce qui active la fonctionnalité SetValue. La prise en charge de SetValue permet aux API `setDisplayValue()` et `setValue()` de prendre en charge les données chiffrées. Il permet également à `getDisplayValue()` et `getValue()` de renvoyer des valeurs en texte clair.
- Deux tâches planifiées sont activées :

  - **autoKeyMigration** : migre les clés de contexte de chiffrement vers Key Management Framework des clés de module cryptographique (KMF).
  - **autoDataMigration** : migre les données que vous avez déjà chiffrées pour utiliser la clé du KMF module de chiffrement.

  Les administrateurs peuvent modifier le moment d'exécution de ces tâches planifiées et les mettre en pause ou les redémarrer à tout moment.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Trouvez le module d'extension *`Platform Encryption - com.glide.now.platform.encryption`* 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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

   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>.

Migrer vers Entreprise Chiffrement au niveau des colonnes

Les tâches planifiées migrent vos clés et données chiffrées du support de chiffrement vers Entreprise de Chiffrement au niveau des colonnes.

Vous pouvez passer en revue les tâches planifiées en accédant à **Sécurité de système** > **Paramètres de sécurité élevée** > **Tâches de Security**:

- **autoKeyMigration** : migre les clés de contexte de chiffrement vers Key Management Framework des clés de module cryptographique (KMF).
- **autoDataMigration** : migre les données que vous avez déjà chiffrées pour utiliser la clé du KMF module de chiffrement.

Vous pouvez modifier le moment d'exécution de ces tâches planifiées 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 **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.

Clones Enterprise et système de Column Level Encryption

Si Chiffrement au niveau des colonnes 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 clone. Ces clés sont générées pour tous les modules auxquels l'utilisateur a accès et qui n'ont pas encore 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 :

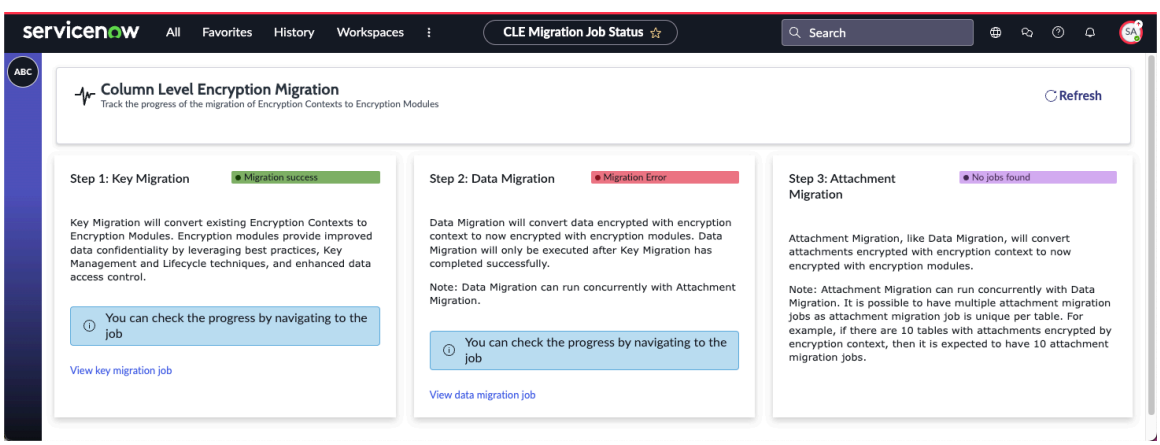
- Clé de chiffrement de module active. Il s'agit de la nouvelle clé générée après clone, tant que le module est accessible à l'utilisateur et qu'il n'a pas de clés préalables.
- Une clé du module de chiffrement désactivé (à partir du transfert automatisé d'échange de clés)

  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.

  Pour utiliser une clé unique afin de 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 modules, consultez Planifier des tâches de chiffrement, de déchiffrement et de nouvelle saisie en masse.

Page État de migration de Column Level Encryption

Utilisez la page État de migration pour suivre la migration des contextes de chiffrement vers les modules de chiffrement.

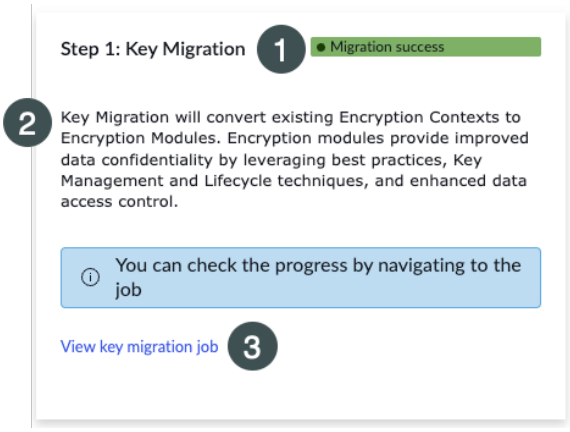


La Chiffrement au niveau des colonnes page Migration affiche l'état des étapes impliquées dans la migration des contextes de chiffrement vers les modules de chiffrement. Chacune des trois sections affiche l'état d'une étape spécifique du processus.

Cartes de sections de page

La page contient trois cartes représentant les étapes de la progression de la migration. Ces cartes affichent :

- (1) L'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 tâche de chiffrement [sys_mass_encryption_job] concerné.



Créer un module de chiffrement pour Column Level Encryption

Créez un module cryptographique Chiffrement au niveau des colonnes pour définir les mécanismes utilisés pour les opérations de chiffrement.

Avant de commencer

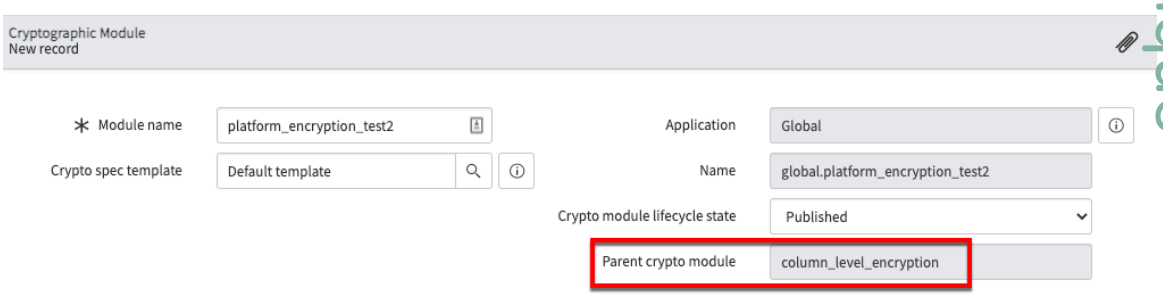
Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf_admin, security_admin, admin

Pourquoi et quand exécuter cette tâche

Cette procédure décrit les options disponibles avec Column Level Encryption (CLE) avec le système de base, ainsi que les options de configuration supplémentaires disponibles avec Entreprise de Chiffrement au niveau des colonnes la fonctionnalité Entreprise de Chiffrement au niveau des colonnes (CLE_Ent). est disponible avec un abonnement payant. Consultez les fonctionnalités et options prises en Offre groupée d'abonnements Chiffrement et gestion des clés charge disponibles avec chaque offre. Pour Activer Entreprise de Chiffrement au niveau des colonnes plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Modules de chiffrement de champ** > **Nouveau**.



2. Renseignez les champs du formulaire.

Formulaire Module de chiffrement

Champ	Description
Nom du module	Chaîne alphanumérique à référencer lors de l'exécution de scripts.

Champ	Description
Modèle de spécification de chiffrement	Modèle par défaut utilisé pour créer le module de chiffrement qui contient des mappages de nombreux objectifs de chiffrement aux spécifications de chiffrement et aux algorithmes recommandés.
Application	Périmètre de l'application sélectionné.
Nom	Le nom du module de chiffrement est ajouté au 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 dont le nom `my_crypto_module` dans le périmètre global de l'application, 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. Défini sur **Brouillon** initialement pendant la configuration. Lorsque vous utilisez le module, définissez l'option **sur Publié**. Le modèle par défaut est automatiquement défini sur **Publié**.
Module de chiffrement parent	Le parent est automatiquement renseigné comme **column_level_encryption**.

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 l'assistance de chiffrement héritée :

Si vous utilisez la version non entreprise de Column Level Encryption, vous êtes limité à cinq modules. Si vous avez dépassé cette limite, vous recevez l'avertissement suivant :

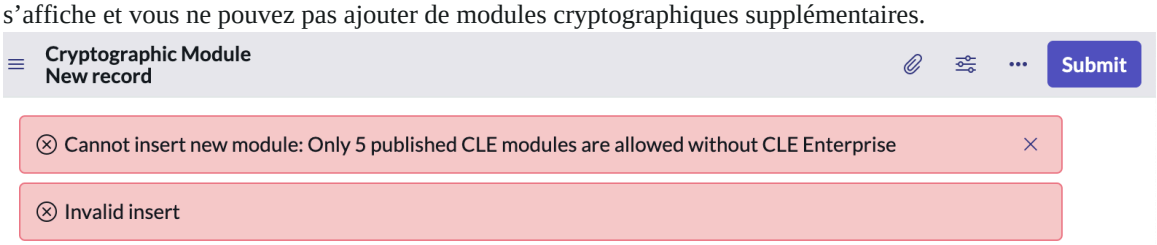
Cette insertion dépasse le nombre de limites de modules publiés de Chiffrement au niveau des colonnes autorisées avec le produit d'abonnement. L'abonnement Entreprise à Column Level Encryption est requis pour les modules supplémentaires. Veuillez contacter l'équipe de votre compte.

Une spécification cryptographique par défaut est créée avec l'objectif de chiffrement défini sur Symmetric Data Encryption/Decryption (Chiffrement symétrique des données) et l'algorithme AES 256 CBC. Sélectionnez l'algorithme pour les mises à jour.

4. Pour ouvrir les options de configuration, cliquez sur le module de chiffrement nouvellement créé.

ℹ Remarque :

Un maximum de cinq modules Column Level Encryption est autorisé avant la mise à niveau vers Entreprise de Chiffrement au niveau des colonnes. Un message d'erreur s'affiche et vous ne pouvez pas ajouter de modules cryptographiques supplémentaires.



Que faire ensuite

Créer une spécification cryptographique pour Column Level Encryption.

Utilisation de plusieurs modules de chiffrement

Plusieurs modules de chiffrement permettent de chiffrer les données avec plusieurs modules de chiffrement. Si chaque module a sa propre politique d'accès basée sur un rôle, par exemple, les utilisateurs ayant des rôles différents peuvent chiffrer des données sur la même table, mais ils peuvent toujours être empêchés de consulter les données chiffrées des autres.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf.admin

Pourquoi et quand exécuter cette tâche

Remarque :
Seul le chiffrement sur les colonnes prend en charge plusieurs modules. Ce n'est pas le cas du chiffrement des pièces jointes. 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 saisir les données. Étant donné que le module de chiffrement est défini pour chaque enregistrement, les champs d'une liste peuvent avoir différents modules de chiffrement. Dans un seul enregistrement, le champ ne peut être chiffré que par un seul module.

Procédure

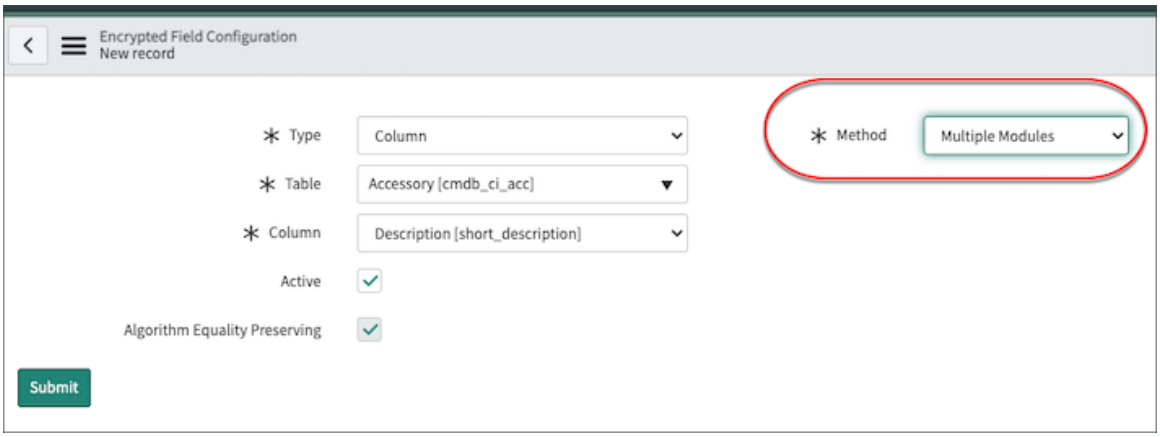
1. Créez plusieurs modules de chiffrement et une politique d'accès pour chacun d'eux.

   Assurez-vous d'accorder différents rôles aux différents modules de chiffrement via les politiques d'accès.

2. Accédez à la **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés**.

   Si vous avez besoin de plus d'informations sur les configurations des 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. Cliquez sur **Envoyer**.

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 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.

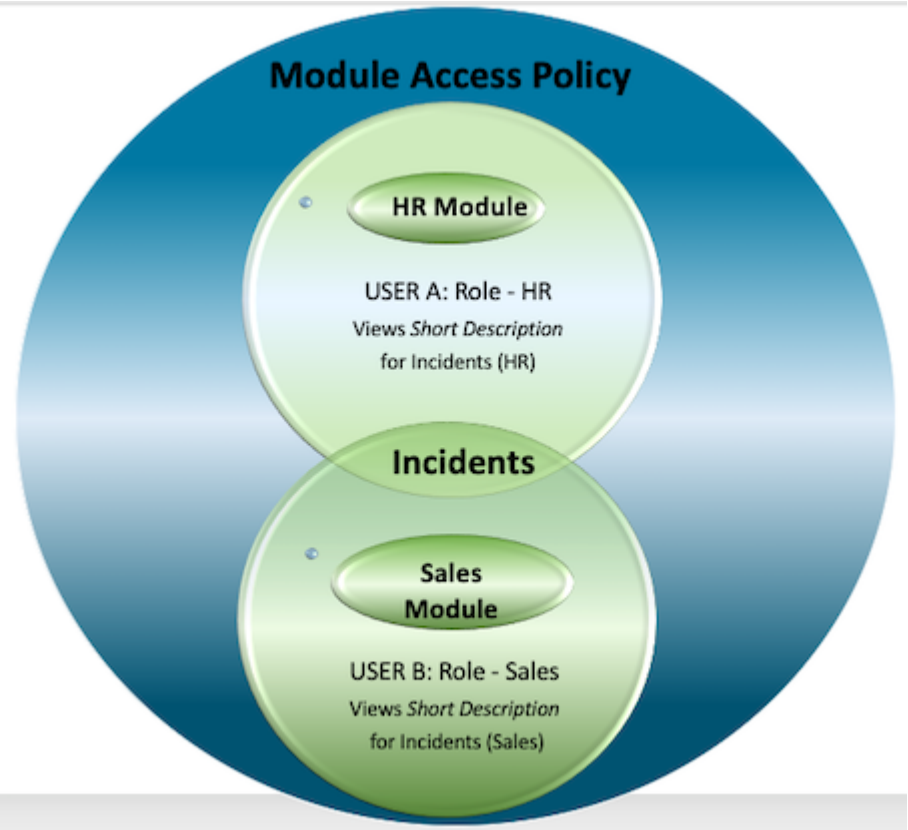
Example:
Pour chiffrer la colonne Brève description de la table Incident. Procédez comme suit :

1. Créez deux modules de chiffrement 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, donnez accès aux utilisateurs ayant un rôle de vente.
3. Créez un enregistrement de configuration de champs chiffrés spécifiant la colonne Brève description sur la table Incident et assurez-vous de sélectionner **plusieurs modules** dans le champ **Méthode** .
4. Demandez à deux utilisateurs, l'un ayant le rôle RH (utilisateur A) et l'autre ayant 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 brève description de l'incident créée par l'utilisateur ayant le rôle RH est chiffrée par la clé du module A. De même, la brève description de l'incident créée par l'utilisateur ayant le rôle Ventes est chiffrée par la clé du module B.

   Bien que tous les utilisateurs disposant des rôles RH et Ventes aient accès aux incidents, seul un utilisateur disposant du rôle RH peut déchiffrer et afficher la brève description de ces incidents créés par l'utilisateur A, qui avait le rôle RH. De même, seuls les utilisateurs disposant du rôle commercial peuvent déchiffrer et afficher les brèves descriptions des incidents créés par l'utilisateur B, qui avait le rôle commercial.



Créer une spécification cryptographique pour Column Level Encryption

Après avoir créé un module de chiffrement, accédez à la spécification de chiffrement 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 avec Column Level Encryption (CLE) avec le système de base et les options de configuration supplémentaires qui deviennent disponibles avec Entreprise de Chiffrement au niveau des colonnes la fonctionnalité Entreprise de Chiffrement au niveau des colonnes (CLE_Ent). Cette fonctionnalité est disponible avec un abonnement payant. Consultez les fonctionnalités et options prises en Offre groupée d'abonnements Chiffrement et gestion des clés charge disponibles avec chaque offre. Pour Activer Entreprise de Chiffrement au niveau des colonnes plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes.

Une spécification cryptographique est créée par le système lorsque vous créez un module de chiffrement pour le chiffrement au niveau des colonnes.

.

Procédure

1. Accédez à la **Sécurité de système** > **Modules de chiffrement de champ** > **Tous**.
2. Sélectionnez le module de chiffrement pour ouvrir les options de configuration.
   Les informations du module de chiffrement sont affichées en haut de l'écran. Une spécification cryptographique de chiffrement/déchiffrement symétrique des données est créée automatiquement à l'aide d'un algorithme AES 256 CBC.
3. Sélectionnez la spécification de chiffrement dans la table pour ouvrir la définition de l'algorithme.

Traduction automatique

Pour Entreprise de Chiffrement au niveau des colonnes voir Configurer des algorithmes avancés pour Column Level Encryption 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. Consultez Configurer les états clés du cycle de vie pour en savoir plus afin de terminer 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 ServiceNow clé cryptographique.

Configurer des algorithmes avancés pour Column Level Encryption Enterprise

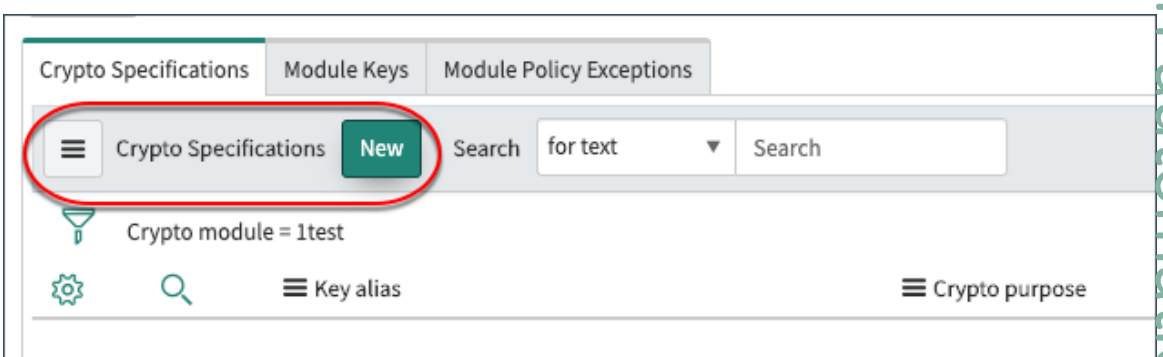
Créez une spécification cryptographique pour définir l'algorithme d'un module de chiffrement. Personnalisez les spécifications de chiffrement avec les options avancées disponibles pour Entreprise de Chiffrement au niveau des colonnes.

Avant de commencer

Rôle requis : admin

Procédure

1. Dans l'onglet **Spécifications de chiffrement (#),** cliquez sur **Nouveau**.



2. Renseignez les champs du formulaire.

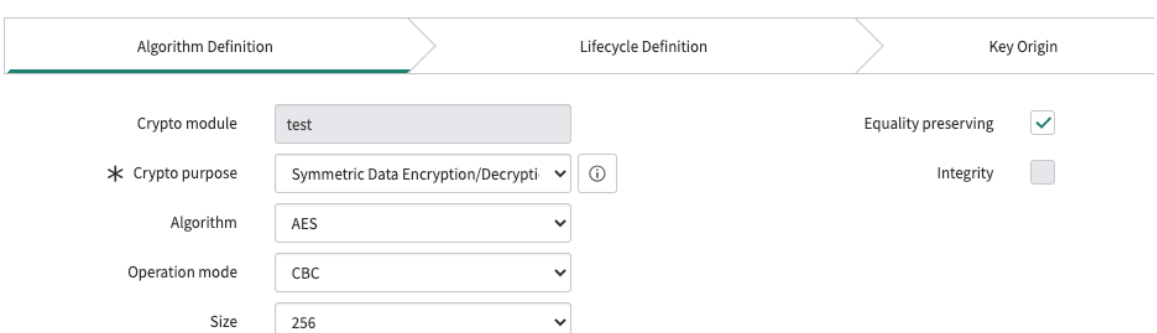
Formulaire Définition d'algorithme

Champ	Description
Module de chiffrement	Le nom du module de chiffrement sélectionné est renseigné.
Objectif de chiffrement	La valeur est **Chiffrement/déchiffrement symétrique des données** pour Entreprise de Chiffrement au niveau des colonnes.
Algorithme	La valeur est **AES** pour Entreprise de Chiffrement au niveau des colonnes.

Champ	Description
Mode d'opération	La valeur est **CBC** pour Entreprise de Chiffrement au niveau des colonnes.
Taille	Les valeurs possibles sont **256** et **128**. **Remarque :** La taille 256 bits est la plus sécurisée pour le chiffrement et est utilisée pour le chiffrement/déchiffrement symétrique des données pour Entreprise de Chiffrement au niveau des colonnes.
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 symétrique des données** avec **AES** en mode **de chaînage de blocs de chiffrement (CBC).**
Intégrité	Option permettant de fournir l'intégrité dans l'opération GCM et ne s'applique pas à Entreprise de Chiffrement au niveau des colonnes la fonctionnalité.

3. Cliquez sur **Envoyer**.

L'exemple suivant montre le chiffrement AES CBC-256. Lorsque Entreprise de Chiffrement au niveau des colonnes cette option est activée et que le module parent est column_level_encryption, seul le chiffrement et le déchiffrement symétrique des données AES CBC-256 s'applique en tant qu'objectif de chiffrement. Consultez Objectif cryptographique, algorithmes et informations clés pour en savoir plus.



Traduction automatique

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. Consultez Configurer les états clés du cycle de vie pour en savoir plus afin de terminer la définition du cycle de vie de la clé.
- Cliquez sur **Suivant** pour créer une clé cryptographique. Consultez l'une des tâches suivantes pour la génération de clés :
  - Générer une ServiceNow clé cryptographique.
  - Configurer les propriétés des clés fournies par le client.
  - Importer la paire de clés d'encapsulation/de désencapsulation.

Configurer les propriétés des clés fournies par le client

Si le module d'extension est activé, vous pouvez utiliser les Entreprise de Chiffrement au niveau des colonnes propriétés système pour définir le remplissage des clés, la taille de la paire de clés éphémères et la période de validité des clés fournies par le client.

Entreprise de Chiffrement au niveau des colonnes avec Key Management vous permet de gérer le cycle de vie complet de vos clés de chiffrement de données. Vous pouvez éventuellement échanger en toute sécurité les clés de chiffrement des données générées au sein de votre environnement.

Remarque :
Les propriétés de cette rubrique s'appliquent uniquement à Entreprise de Chiffrement au niveau des colonnes la fonctionnalité. Entreprise de Chiffrement au niveau des colonnes La fonctionnalité est disponible uniquement lorsque le module d'extension `com.glide.now.platform.encryption` est actif. Pour Activer Entreprise de Chiffrement au niveau des colonnes plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes.

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 encapsulée 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 Clés au niveau de l'instance dans Key Management Framework les types 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 encapsulée :

- `glide.kmf.ephemeral_key.key_padding` Contrôle le schéma de remplissage de 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 la clé de la paire de clés éphémères. La valeur par défaut est de 4 096 bits, mais 2 048 bits sont également pris en charge.
- `glide.kmf.ephemeral_key.key_validity_period` Définit la période de validité de la paire de clés éphémères. La valeur par défaut est de deux heures.

Passez à Encapsuler votre clé fournie par le client.

Encapsuler votre clé fournie par le client

Si vous utilisez des clés fournies 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 Entreprise de Chiffrement au niveau des colonnes la fonctionnalité. Entreprise de Chiffrement au niveau des colonnes La fonctionnalité n'est disponible que lorsque le module d'extension `com.glide.now.platform.encryption` est actif. Pour Activer Entreprise de Chiffrement au niveau des colonnes plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes.

Certaines des étapes décrites dans ce document nécessitent l'utilisation d'un outil cryptographique installé sur votre appareil local. Les exemples de cette tâche utilisent l'outil OpenSSL. Pour plus d'informations 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 des étapes similaires.

- Modifiez les propriétés facultatives qui contrôlent la taille, l'algorithme de remplissage et la période de validité de la clé.
- Vous devez avoir votre clé symétrique (. BIN) pour le chiffrement.
- 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 redirigé vers l'étape **Création de la clé** .
4. Si vous n'avez pas encore téléchargé la clé encapsulée, 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.
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 encapsulée.
8. Modifiez ce script en remplaçant les exemples par les noms de vos fichiers de chiffrement.

```
"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'habillage des touches dans le tableau suivant.

Commandes d'encapsulation de clé

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 affiche `token_publickey_&lt;keynumber>`. La clé sera générée et un fichier *`wrapped_key_material`* sera ajouté au répertoire.
10. Chargez la clé emballée.

Que faire ensuite

Revenez à Configurer et charger votre clé fournie par le client pour charger votre clé emballée.

Configurer et charger votre 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 de chiffrement pour Column Level Encryption.

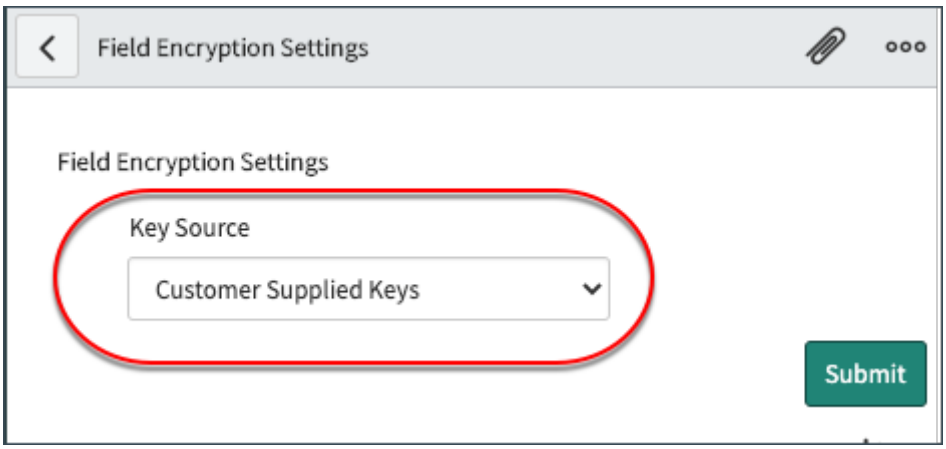
Remarque :
Cette procédure s'applique uniquement aux Entreprise de Chiffrement au niveau des colonnes fonctionnalités. Consultez Activer Entreprise de Chiffrement au niveau des colonnes pour plus d'informations.

Important :
Vous ne pouvez pas révoquer une clé fournie par le client.

Procédure

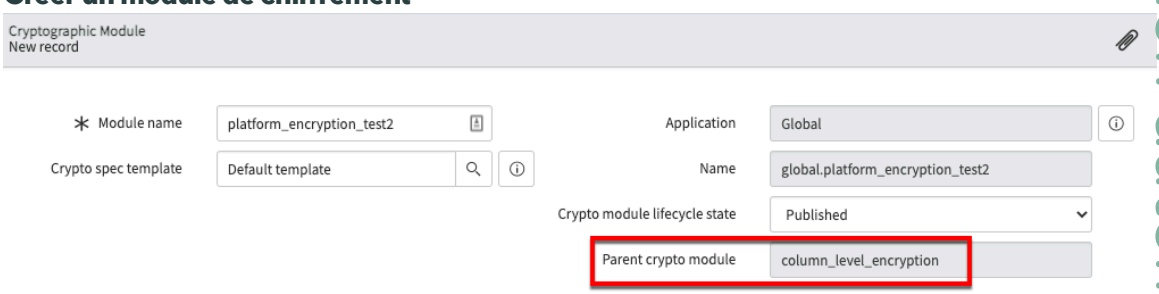
1. Accédez à la **Tous** > **Sécurité de système** > **Paramètres de Chiffrement de champ** et vérifiez que **l'option Clés fournies par le client** est sélectionnée.

Sélection de la source de clé



2. Sélectionnez **Envoyer**.
3. Retourner à **Sécurité de système** > **Modules de chiffrement de champ** > > **Créer**.

Créer un module de chiffrement



4. Remplissez le formulaire Module cryptographique, comme suit :

Champs du module de chiffrement

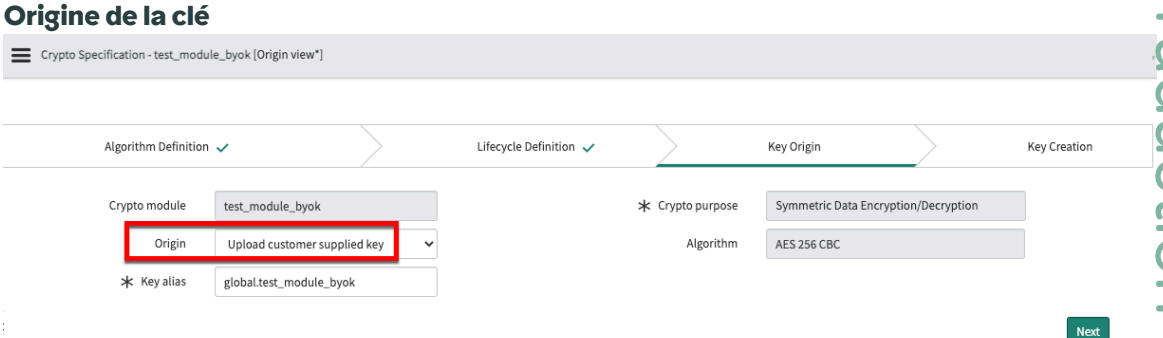
Champ	Description
Nom du module	Entrez un nom pour le module.
Modèle de spécification de chiffrement	Le modèle de chiffrement par défaut est sélectionné.
Nom	Se remplit automatiquement en fonction du nom du module et ajoute le périmètre au nom pour garantir quelle application est appliquée. Dans ce cas, le champ d'application global est appliqué.
État du cycle de vie du module de chiffrement	Sélectionner **Publié** pour activer le module de chiffrement.

Champ	Description
Module de chiffrement parent	La **column_level_encryption** de module parent est sélectionnée automatiquement lors de l'utilisation des clés et modules de chiffrement fournis par le client.

5. Sélectionnez **Envoyer**.
6. Sélectionnez le module de chiffrement nouvellement créé dans la table.
   Dans la liste connexe **Spécifications de chiffrement** , sélectionnez l'alias de clé généré automatiquement avec l'algorithme de base de données de conteneurs AES 256.

   Le système remplit automatiquement l'objectif de chiffrement et l'algorithme pour CLE et passe à l'étape **d'origine** de la clé.
7. Notez que Télécharger la **clé fournie par le client** est l'origine et que **l'alias** de clé est déjà renseigné.

Origine de la clé

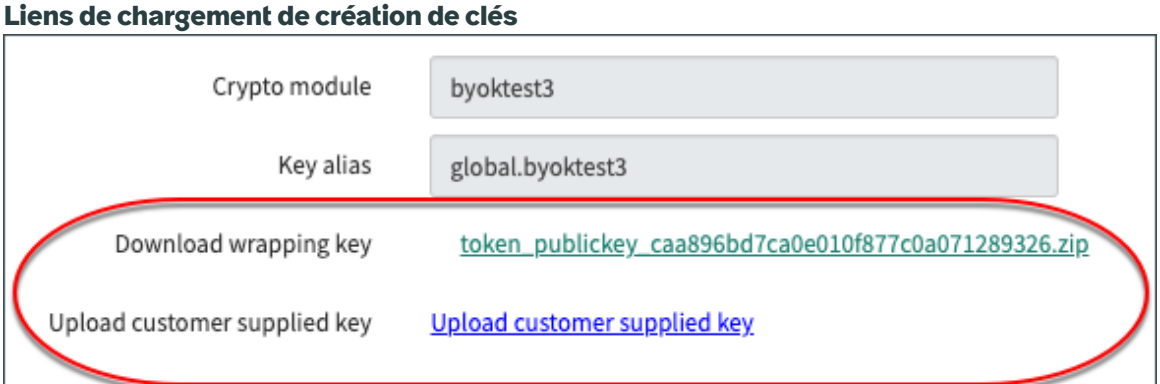


8. Sélectionnez **Suivant** pour passer à l'étape **Création de clé** .

   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'encapsulation de clé est correcte conformément aux spécifications de sécurité de l'instance. Utilisez le certificat de clé publique . PEM pour envelopper votre clé fournie par le client en toute sécurité avant de la charger avec le jeton.
   - **Télécharger la clé fournie par le client** ouvre l'explorateur de fichiers pour sélectionner le jeton et la clé chiffrée que vous avez encapsulés.

Liens de chargement de création de clés



9. Sélectionnez **Télécharger la clé d'encapsulation** pour enregistrer le jeton.

Enregistrez le jeton au même emplacement de destination que celui où la clé est enregistrée sur votre système. Ne renommez pas le jeton téléchargé.

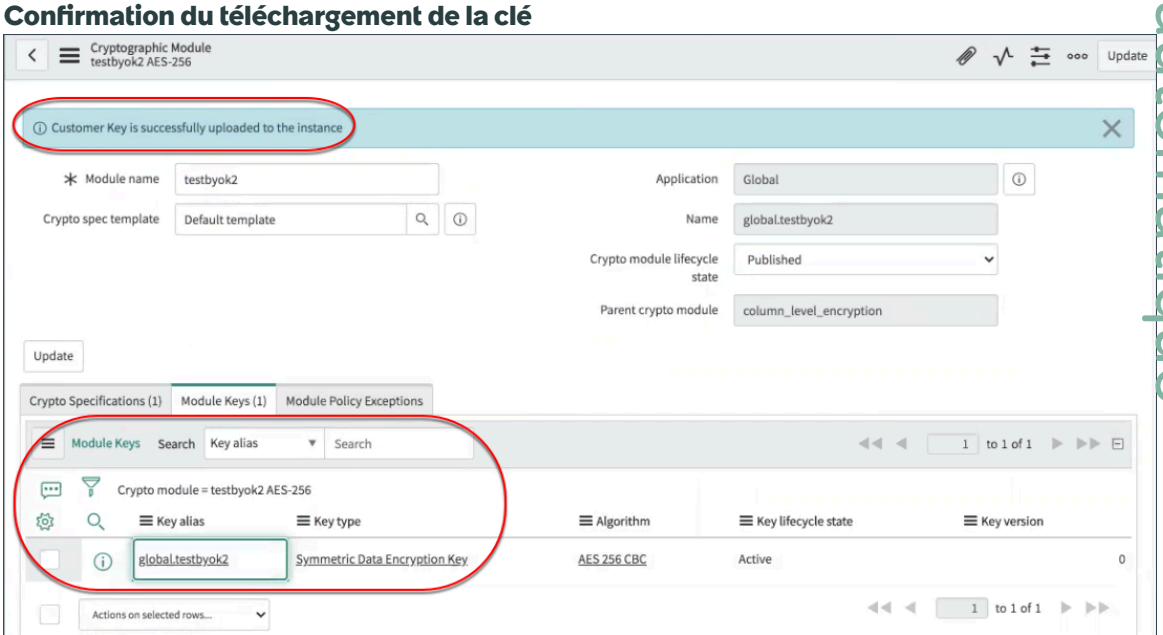
10. Exécutez la commande BYOK sur un terminal pour envelopper la clé.
    Pour plus d'informations, référez-vous à Encapsuler votre clé fournie par le client.
11. Sélectionnez **Télécharger la clé fournie par le client**.
12. Sélectionnez **Parcourir** pour sélectionner les deux fichiers, la clé enveloppée et le fichier de jeton.
    La fenêtre Pièces jointes affiche les deux fichiers.

Chargement des pièces jointes de clé encapsulée

Sélectionnez un fichier à supprimer et à charger à nouveau, si nécessaire.

13. Sélectionnez **OK**.
    Vous êtes renvoyé à l'écran Module cryptographique. Un message de confirmation s'affiche pour un chargement réussi de la clé client. La clé est également répertoriée dans la liste connexe Clés de module.

Confirmation du téléchargement de la clé



Que faire ensuite

Maintenant que vous avez terminé la configuration de votre module de chiffrement avec votre clé fournie par le client, passez à Créer une politique d'accès au module

Chiffrement de champs et de pièces jointes

Après avoir créé vos modules de chiffrement, créez des configurations de champs chiffrés et spécifiez s'il faut chiffrer un champ sur une table ou chiffrer les pièces jointes.

Comment chiffrer des champs

Remarque :
Les champs chiffrés ne sont pas audités de par leur conception. Ce comportement n'est pas configurable.

1. Spécifiez la source de clé : clés générées par le système ou clés fournies par votre client (apporter votre propre clé) dans **Sécurité de système** > **Paramètres de Chiffrement de champ**.
2. Après avoir spécifié la source de clé, créez un module de chiffrement ou utilisez un module de chiffrement existant. Commencez par Créer un module cryptographique pour obtenir des instructions.

   Remarque :
   Si vous utilisez les clés fournies par le client, suivez les instructions dans Créer un module de chiffrement pour Column Level Encryption et Configurer les propriétés des clés fournies par le client.

3. Créez une configuration de champ chiffré, dans laquelle vous spécifiez la table sur laquelle le chiffrement est effectué et la colonne de la table ou les pièces jointes de la table à chiffrer. Voir Définir des configurations de champs chiffrés pour commencer.

Remarque :
Consultez la section Exemples de Column Level Encryption Enterprise qui illustre comment chiffrer des champs et des 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 cryptographique préconfiguré.

Avant de commencer
Rôle requis : sn_kmf.cryptographic_manager et security_admin ou élever le rôle au rôle d'administrateur de sécurité.

Pourquoi et quand exécuter cette tâche
Assurez-vous que vous êtes dans le bon périmètre de l'application afin de pouvoir voir les tables dans ce périmètre.

Seuls les utilisateurs ayant accès au module de chiffrement que vous spécifiez dans cette configuration de champs chiffrés 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 d'un accès en lecture, le champ s'affiche en mode de modification 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 le mode lecture seule des données déchiffrées.
- Si un utilisateur dispose de tous les accès, les fonctionnalités de lecture/d'écriture sont disponibles dans le champ chiffré.

Voir Créer un module cryptographique ou Créer un module de chiffrement pour Column Level Encryption pour commencer.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés** > **Nouveau**.
2. Cliquez sur **Nouveau**.
3. Complétez 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 ○ Pièces jointes ○ Date, Date/Heure : **Remarque :** Vous pouvez créer des configurations de champs chiffrés pour chiffrer les champs Date et Date/Heure existants. Vous pouvez ajouter une nouvelle configuration de chiffrement à une table parente uniquement. Vous ne pouvez pas ajouter une nouvelle configuration de chiffrement à une table enfant. ○ URL ○ Entreprise de Chiffrement au niveau des colonnes prend également en charge les types de champs suivants : ▪ HTML ▪ Journal ▪ Traduit
Table	Table dont les champs ou les pièces jointes doivent être chiffrés.
Colonne	Colonne (champ) à chiffrer si vous avez sélectionné la **colonne** comme type.
Actif	Sélectionnez cette option pour marquer la configuration comme active. Désélectionnez cette option si la configuration n'est pas encore utilisée.
Module de chiffrement	Module de chiffrement auquel la configuration du champ chiffré s'applique.
Méthode	Sélectionnez **Module unique** pour définir la configuration de champ dans un module. Sélectionnez **plusieurs modules** pour un accès basé sur les rôles qui couvre plusieurs modules de chiffrement. **Module unique** Utilisez cette option pour chiffrer toutes les pièces jointes à l'aide d'un seul module. Vos utilisateurs doivent avoir accès à ce module, sinon ils ne sont pas en mesure de télécharger des 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

Champ	Description
	module peuvent sélectionner un module à utiliser pour le chiffrement. Les utilisateurs n'ayant pas accès au module peuvent télécharger des pièces jointes non chiffrées.
Préservation chiffrée par 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 cryptage est différent à chaque fois.

4. Cliquez sur **Envoyer**.

Accès aux scripts pour les modules de chiffrement

Des scripts peuvent être exécutés pour accéder à une politique de module de chiffrement à des fins de chiffrement.

Pour Key Management Framework, les politiques peuvent être basées sur des scripts. Lorsqu'une politique d'accès est déclenchée pour l'accès aux scripts, le script back-end peut exécuter les actions de politique de module à partir du script.

Les modules de chiffrement peuvent prendre en charge un ou plusieurs objectifs de chiffrement, tels que le déchiffrement des données asymétriques et le déchiffrement symétrique des données. Chaque objectif cryptographique nécessite la génération d'une clé de chiffrement et d'un objectif cryptographique défini.

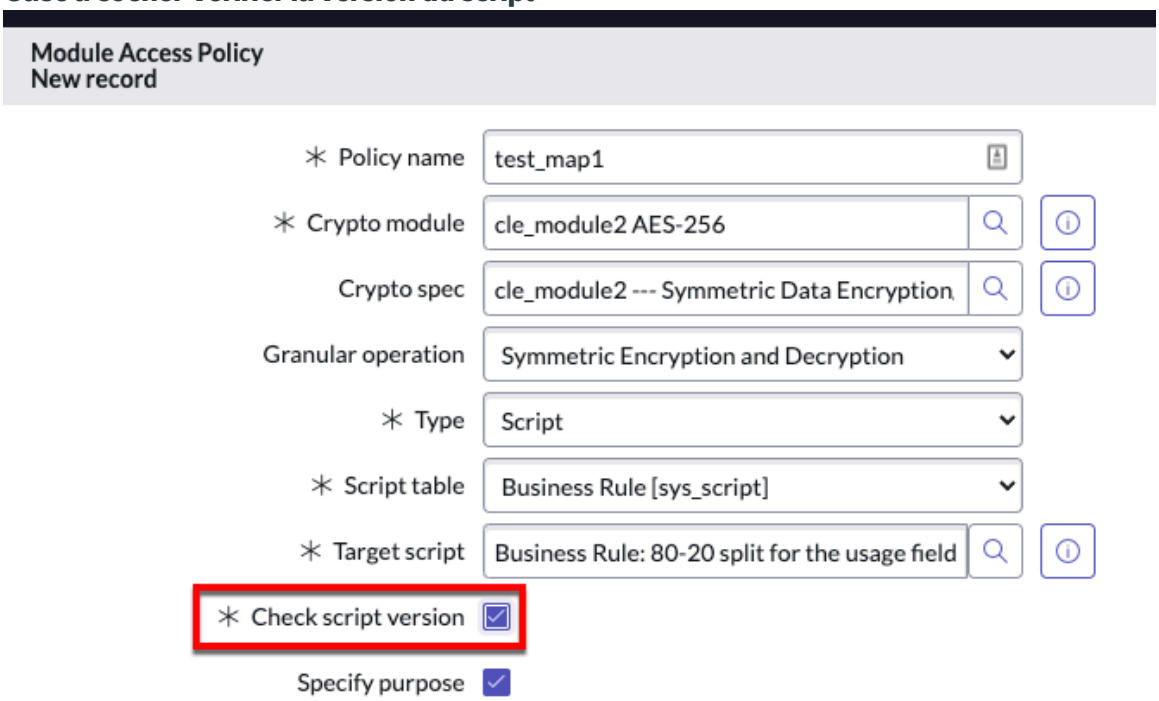
Lors de l'exécution d'une demande de script de chiffrement, prenez en compte les éléments suivants :

- La finalité de chiffrement référencée doit être définie dans le module de chiffrement.
- 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 est disponible pour valider l'intégrité de la version de script à laquelle vous accédez. Seule la version affectée du script est autorisée à accéder aux modules de chiffrement. Lorsque la case à cocher **Vérifier la version du script** est sélectionnée 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.

Case à cocher Vérifier la version du script



Configurer l'accès de script 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 de l'opération de la politique d'accès au module.

Avant de commencer

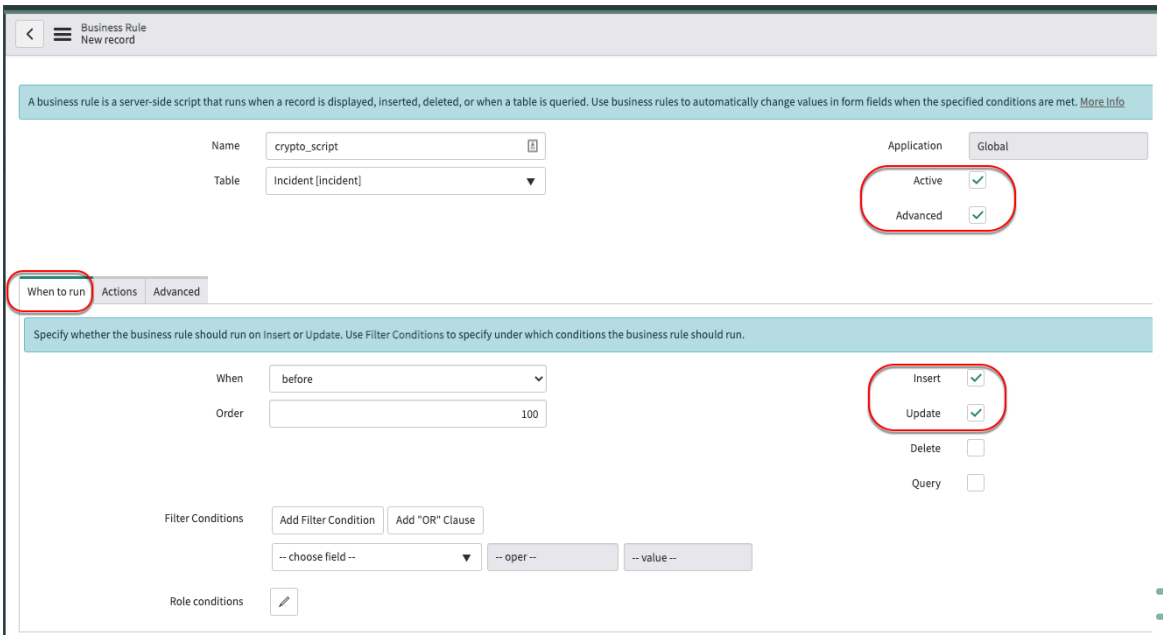
Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Les règles métier et les scripts includes sont des exemples d'utilisation. Cette procédure utilise un script pour les règles métier.

Procédure

1. Créez un module de chiffrement avec l'algorithme de chiffrement/déchiffrement symétrique des données. 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 dont les caractéristiques sont les 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 chiffrées téléchargées ou les pièces jointes, mais ne parvient pas à chiffrer les données ou les pièces jointes.
   - Chiffrement et déchiffrement symétriques : le script est capable à la fois de chiffrer et de déchiffrer des données ou des pièces jointes.
2. Accédez à la **Définition du système** > **Règles métier**.
3. Cliquez sur **Nouveau**.



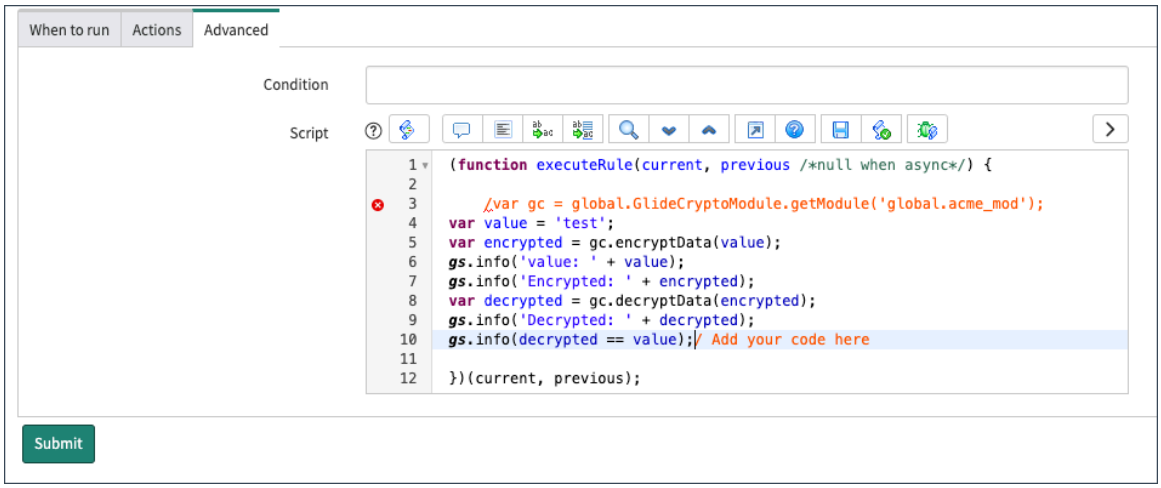
4. Remplissez le formulaire dans l'onglet **Quand exécuter** et entrez le script dans l'onglet **Avancé** :

Champs de 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 en savoir plus.

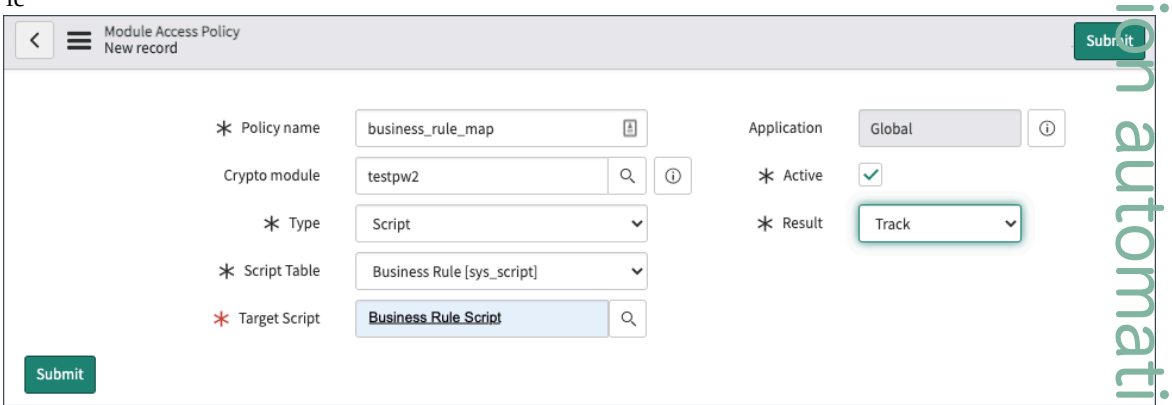
Traduction automatique



5. Cliquez sur **Envoyer**.
6. Accédez à la **Gestion des clés** > **Politiques d'accès au module** > **Tous**.

> **Remarque :**
> Pour en savoir plus, reportez-vous à Créer une politique d'accès au module.

7. Cliquez sur **Nouveau**.
8. Complétez le formulaire.



Champs des politiques d'accès au module

9. Cliquez sur **Envoyer**.
   La politique d'accès au module pour le script est maintenant disponible dans le système.

Afficher les demandes d'utilisation du module cryptographique 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 de chiffrement peuvent prendre en charge un ou plusieurs objectifs de chiffrement, tels que le déchiffrement des données asymétriques et le déchiffrement symétrique des données. Les données chiffrées ne sont accessibles que sur la base de la politique d'accès au module. Si un script tente d'utiliser un module de chiffrement à des fins non définies dans le module, le script ne peut pas accéder aux données chiffrées.

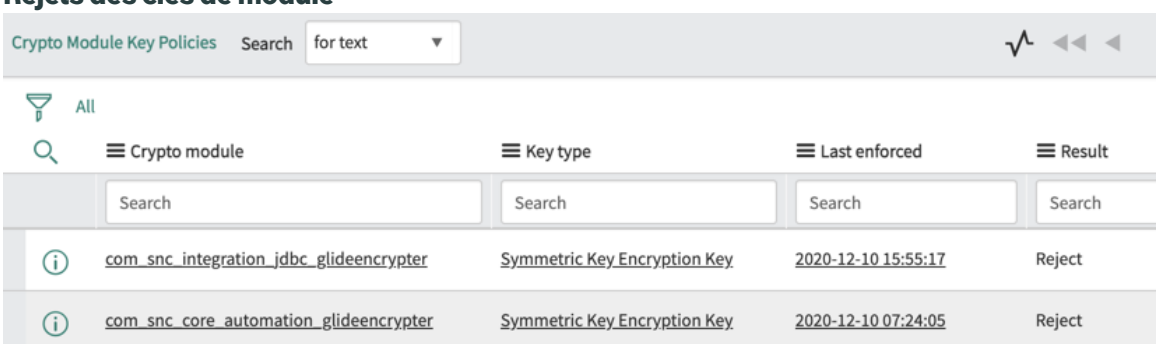
Dans l'exemple suivant, un objectif de chiffrement a été affecté à un module de chiffrement, mais aucune clé n'a jamais été générée pour celui-ci.

Procédure

Accédez à la **Tous** > **Gestion des clés** > **Politiques de clé de module** > **Rejets des clés de module**.

Une liste des modules de chiffrement qui ont rejeté des demandes s'affiche avec 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 de Dernières mises à jour **appliquées** . Aucune autre ligne n'est générée.

Dans cet exemple, à 2020-02-10_15 :55 :17, le premier module a rejeté une demande, car la clé du module1 est compromise. À 2020-02-10_07 :24 :05, le deuxième module a rejeté une demande car la clé du deuxième module est suspendue.

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 des scripts. Pour plus d'informations, référez-vous à Configurer l'accès de script 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 en dehors des heures de pointe. 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 des 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** > **Paramètres de sécurité élevée** > **Tâches de Security**.
2. Cliquez sur **Nouveau**.
3. Complétez 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 des clés vers le 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 ○ **Pièce jointe de déchiffrement en masse** :D chiffre toutes les pièces jointes chiffrées dans les enregistrements pour une table unique que vous définissez dans le champ **Table** . ○ **Pièce jointe de chiffrement en masse** : chiffre toutes les pièces jointes des enregistrements pour une table unique que vous définissez dans le champ **Table** . ○ **Module de 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. ○ **Module multiple de déchiffrement en masse** : déchiffre toute valeur préexistante dans la colonne/le champ défini utilisé dans la configuration de chiffrement de champ avec plusieurs modules. ○ **Renouvellement de saisie du module** : 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 sur la table définie dans la configuration de Chiffrement de champ. Toute pièce jointe précédemment chiffrée avec un contexte est chiffrée à nouveau avec le module.
État	L'état de la tâche initiale est Nouveau. Une fois que la tâche a été exécutée comme prévu, l'état se met à jour en conséquence.
Début de la fenêtre de temps	Heure de début de la tâche au format 24 heures.
Fin de la fenêtre	Heure de fin de la tâche au format 24 heures.

Champ	Description
de temps	
Table	Table à chiffrer ou à déchiffrer.
Champ	Champ à chiffrer ou à déchiffrer.
Résumé	Informations sur l'état de la tâche lorsqu'elle est en cours d'exécution, qu'elle est terminée ou qu'elle présente des erreurs.

Remarque :
En raison de la surcharge du système, vous devez planifier des tâches de chiffrement en masse, de déchiffrement et de nouvelle saisie pour qu'elles s'exécutent en dehors des heures de pointe. Exécute Now Platform la tâche entre le **début** et la fin de la **fenêtre de temps**. Si la tâche n'est pas terminée au cours d'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 actions suivantes.
   - Cliquez sur **Annuler la tâche** pour annuler une tâche en cours d'exécution.
   - Cliquez sur **Démarrer** pour commencer une tâche immédiatement.
   - Cliquez sur **Mettre à jour** pour enregistrer toutes les modifications apportées 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

Pourquoi et quand exécuter cette tâche
Vous pouvez également créer des tâches planifiées 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 cryptographique unique. Le déchiffrement de masse est disponible pour les méthodes de cryptage uniques et multiples.

Remarque :
Vous ne devez exécuter le chiffrement et le déchiffrement en masse que pendant les heures creuses, car les opérations demandent beaucoup de temps et de ressources.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés**.
2. Ouvrez la configuration du champ chiffré 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

Si vous exécutez 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.

Exemples de Column Level Encryption Enterprise

Ces exemples vous guident dans le chiffrement des champs et des pièces jointes à l'aide des clés fournies par le client.

Procédure pas à pas de chiffrement de champ

Cette procédure pas à pas vous montre comment chiffrer un champ dans votre instance à l'aide Entreprise de Chiffrement au niveau des colonnes de (Key Management FrameworkKMF). Il vous montre également comment utiliser votre propre clé.

Avant de commencer

Remarque :
Cette procédure s'applique uniquement aux Entreprise de Chiffrement au niveau des colonnes fonctionnalités. Pour Activer Entreprise de Chiffrement au niveau des colonnes plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes.

Rôle requis : admin ou security_admin

Remarque :
security_admin s'agit d'un rôle privilégié, pour plus d'informations sur l'utilisation des rôles privilégiés, consultez 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 téléchargé votre clé cryptographique personnelle. Vous pouvez utiliser la clé, mais cet exemple utilise une clé fournie par le ServiceNow client.

Une fois que la clé a été stockée dans un module de chiffrement, vous pouvez commencer à configurer les champs de votre instance, tels que les numéros de salaire ou de sécurité sociale dont l'accès est limité pour certains utilisateurs. Dans la configuration du champ chiffré, spécifiez quel personnel autorisé peut accéder aux données sensibles.

Cette tâche illustre deux scénarios. Par exemple, chiffrez le champ **Brève description** dans un incident 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 bénéficient d'un accès, ou sont visibles par tous les utilisateurs qui ne sont pas empêchés de consulter les données. Reportez-vous à la section Procédure pas à pas de chiffrement des pièces jointes pour chiffrer une pièce jointe.

Procédure

1. Assurez-vous que cette option Entreprise de Chiffrement au niveau des colonnes est activée.
2. Créez un module cryptographique pour column_level_encryption.

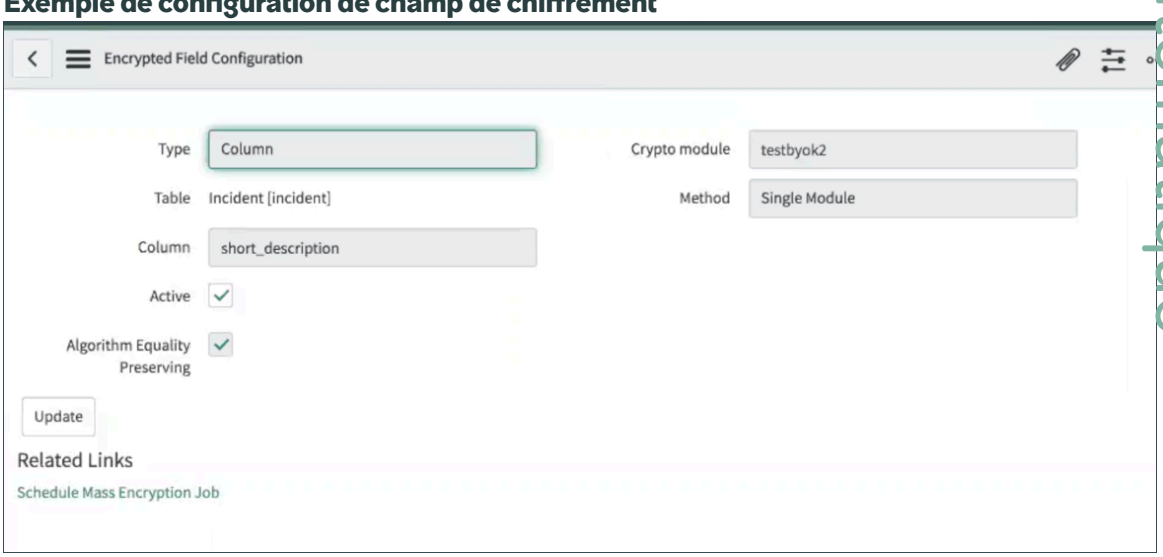
Consultez Créer un module de chiffrement pour Column Level Encryption Créer un module cryptographique pour en savoir plus.

3. Accédez à la **Sécurité de système** > **Configurations des champs chiffrés**.
4. Cliquez sur **Nouveau**.
5. Renseignez 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 représente la date sensible à chiffrer. Pour cet exemple, sélectionnez **short_description**.
Actif	Option permettant de marquer **Actif** pour utiliser la configuration de champ.
Préservation de l'égalité des algorithmes	L'option est automatiquement sélectionnée.
Module de chiffrement	Module que vous avez créé pour être utilisé avec la clé personnelle.
Méthode	L'option **Module unique** est utilisée pour appliquer les politiques d'un module. **L'option Modules multiples** est utilisée pour appliquer les politiques à plusieurs modules.

Exemple de configuration de champ de chiffrement



6. Cliquez sur **Envoyer**.

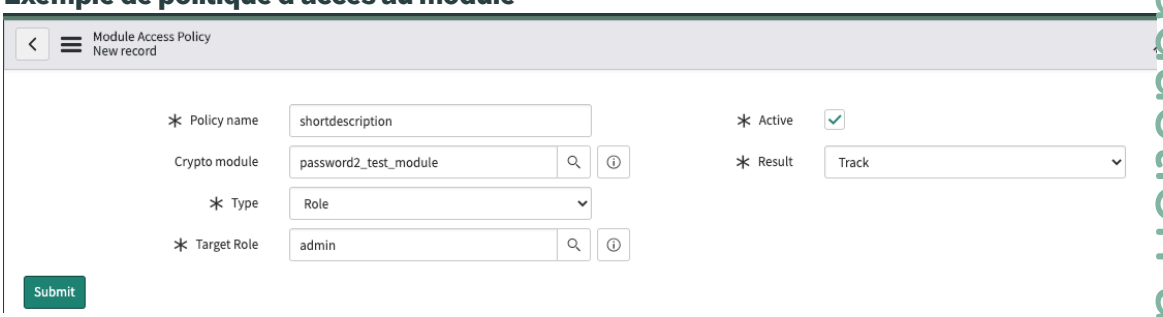
Établissez une politique d'accès au module pour affecter l'accès au module de chiffrement. Consultez Créer une politique d'accès au module pour plus d'informations.

7. Accédez à la **Gestion des clés** > **Politiques d'accès au module** > > **Créer** > **.**
8. Renseignez les champs du formulaire.

Formulaire Politique d'accès au module

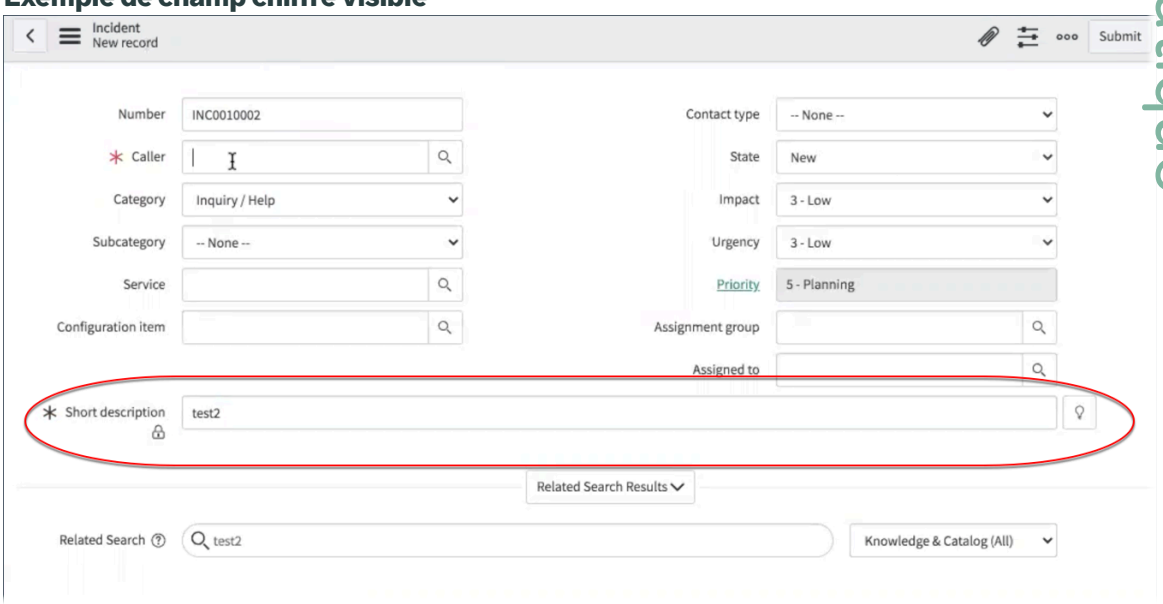
Champ	Description
Nom de la stratégie	Nom de la politique, par exemple, description brève.
Module de chiffrement	Module de chiffrement que vous avez créé pour chiffrer votre clé.
Type	Type de désignation d'accès pour la politique de chiffrement. Utilisez le **rôle** pour accorder l'accès au champ chiffré uniquement aux utilisateurs disposant du 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**permet d'accéder au champ pour le rôle sélectionné. (Pour restreindre l'accès à ce champ pour le rôle sélectionné, sélectionnez **Rejeter** ou**Rejeter strict**.)

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



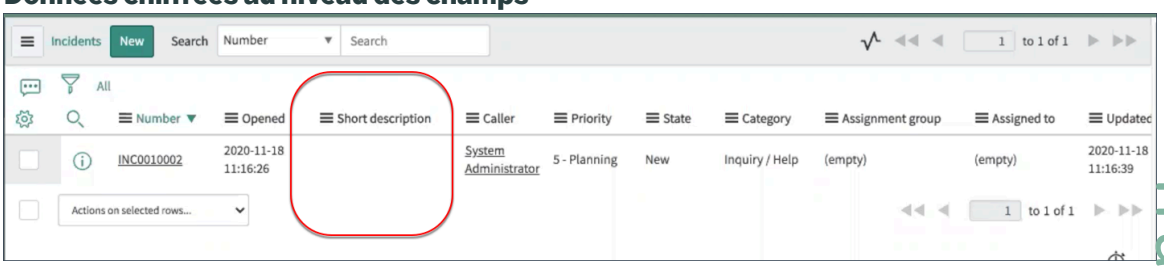
Vous pouvez maintenant afficher le champ Brève description en fonction de la configuration de la politique d'accès au module.

Remarque :
Le rôle sn_kmf.admin a obtenu l'accès utilisateur au champ chiffré, Brève description, en définissant la politique d'accès au module sur **Suivi**. Remarquez l'icône de verrouillage ( ) sous le nom du champ indiquant que le champ est un champ chiffré.

Vous pouvez désormais 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.

Données chiffrées au niveau des champs



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 Entreprise de Chiffrement au niveau des colonnesde .

Procédure pas à pas de chiffrement des pièces jointes

Cette procédure pas à pas vous montre comment chiffrer une pièce jointe dans votre instance à l'aide Entreprise de Chiffrement au niveau des colonnes de (Key Management FrameworkKMF). Il vous montre également comment utiliser votre propre clé.

Avant de commencer

Remarque :
Cette procédure s'applique uniquement aux Entreprise de Chiffrement au niveau des colonnes fonctionnalités. Pour Activer Entreprise de Chiffrement au niveau des colonnes plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes.

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 votre clé cryptographique fournie par le client. Vous pouvez utiliser la clé, mais cet exemple utilise une clé fournie par le ServiceNow® client.

Chargez des pièces jointes confidentielles dans votre instance et limitez l'accès de certains utilisateurs. Utilisez la configuration des champs chiffrés pour spécifier le personnel autorisé qui peut accéder aux données sensibles.

Nous vous montrons comment chiffrer des pièces jointes pour qu'elles ne soient visibles que par les utilisateurs qui bénéficient d'un accès ou pour tous les utilisateurs qui ne sont pas empêchés de consulter les données. Dans cet exemple, nous restreignons l'accès à une pièce jointe dans le module **Incidents** pour un certain rôle.

Remarque :
Bien que vous puissiez utiliser plusieurs modules avec le chiffrement des colonnes, le chiffrement des pièces jointes doit utiliser des modules uniques.

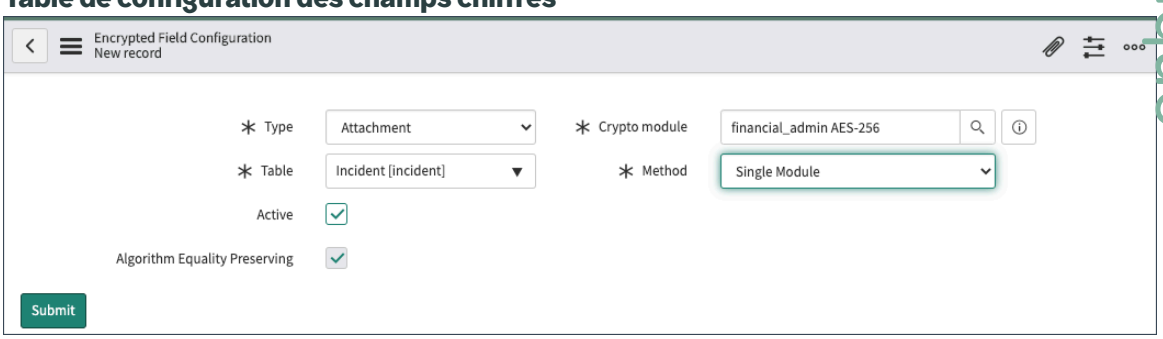
Procédure

1. Assurez-vous que cette option Entreprise de Chiffrement au niveau des colonnes est activée.
2. Créez un module de chiffrement.
   Consultez Créer un module de chiffrement pour Column Level Encryption pour plus d'informations.
3. Accédez à la **Sécurité de système** > **Configurations des champs chiffrés**.
4. Cliquez sur **Nouveau**.
5. Complétez le formulaire :

Champs de configuration des champs chiffrés

Champ	Description
Type	Sélectionnez **Pièce jointe** pour utiliser votre clé personnelle pour chiffrer une pièce jointe à partir 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 **Actif** pour pouvoir utiliser la configuration de champ.
Préservation de l'égalité des algorithmes	Lorsque vous sélectionnez Chiffrement au niveau des colonnes, ce champ est visible en fonction de la table sélectionnée.
Module de chiffrement	Sélectionnez le module que vous avez créé à utiliser avec la clé personnelle.
Méthode	L'option **Module unique** est utilisée pour appliquer les politiques d'un module. **L'option Modules multiples** est utilisée pour appliquer les politiques à plusieurs modules.

Table de configuration des champs chiffrés



6. Cliquez sur **Envoyer**.

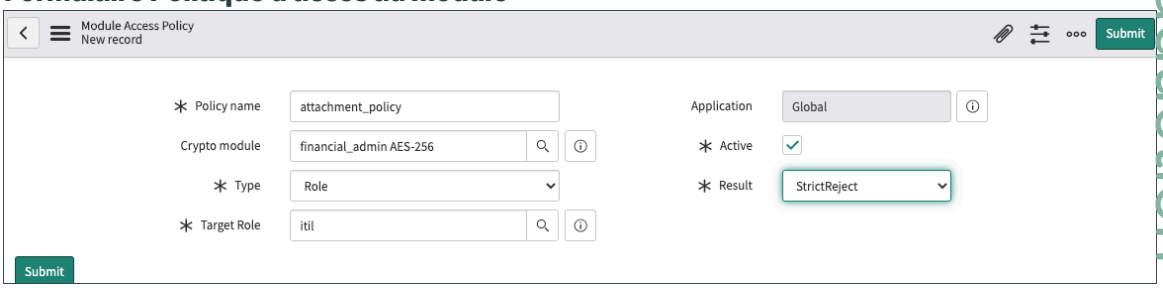
Établissez une politique d'accès au module pour affecter l'accès au module de chiffrement. Reportez-vous à pour plus d'informations Créer une politique d'accès au module .

7. Accédez à la **Gestion des clés** > **Politiques d'accès au module** > **Tous**.
8. Cliquez sur **Nouveau**.
9. Complétez le formulaire :

Champs de la politique d'accès au module

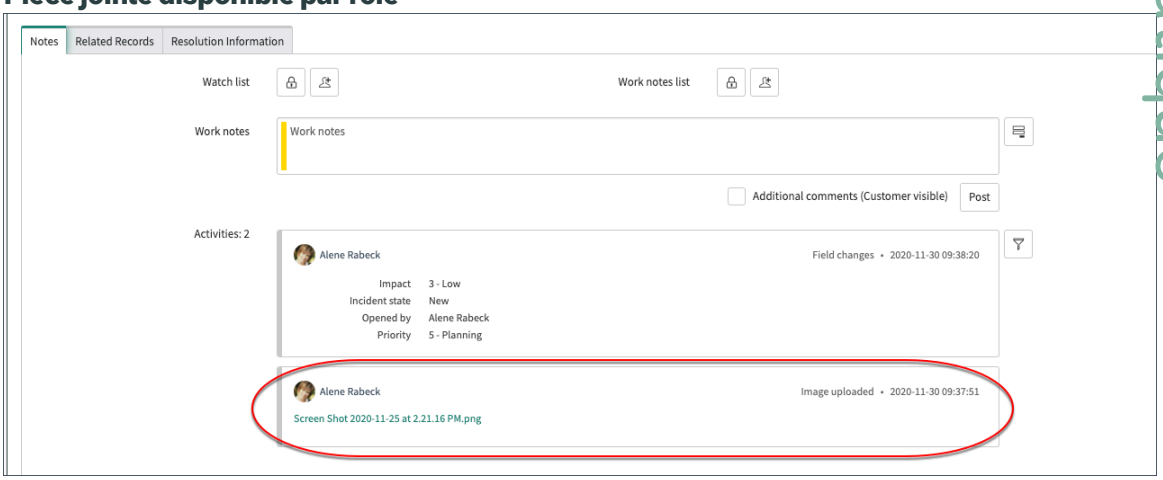
Champ	Description
Nom de la stratégie	Entrez un nom pour la politique, par exemple « Politique relative aux pièces jointes ».
Module de chiffrement	Sélectionnez le module de chiffrement que vous avez créé pour chiffrer votre clé.
Type	Sélectionnez **Rôle** pour restreindre l'accès au champ chiffré aux utilisateurs ayant le rôle affecté.
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 **Rejet strict** pour contrôler l'accès à la pièce jointe à partir du rôle sélectionné. (Pour accorder l'accès au rôle sélectionné, sélectionnez **Piste**.)

Formulaire Politique d'accès au module



10. Cliquez sur **Envoyer**.
11. En tant qu'administrateur ou en tant que 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 faites défiler jusqu'à la section **Activités :** .

Remarque :
Le lien permettant d'ouvrir la pièce jointe n'est pas accessible pour les utilisateurs disposant du rôle restreint.

14. Vous avez maintenant utilisé avec succès votre clé fournie par le client pour contrôler l'accès à une pièce jointe spécifique à l'aide du chiffrement au niveau des colonnes.

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 vers le 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.

Générez et chargez 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.

Installer le module d'extension Infrastructure Security

Installez le module d'extension Paramètres de sécurité de l'infrastructure ServiceNow (com.glide.infrastructure_security) pour commencer à utiliser ces fonctionnalités. Pour obtenir des détails sur l'activation d'un module d'extension, consultez Activer un module d'extension .

Après avoir installé le module d'extension, activez la fonctionnalité Sign Your Own Security (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 l'équilibreur de charge de votre instance.

Avant de commencer
Rôle requis : admin

Pour en savoir plus 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**.

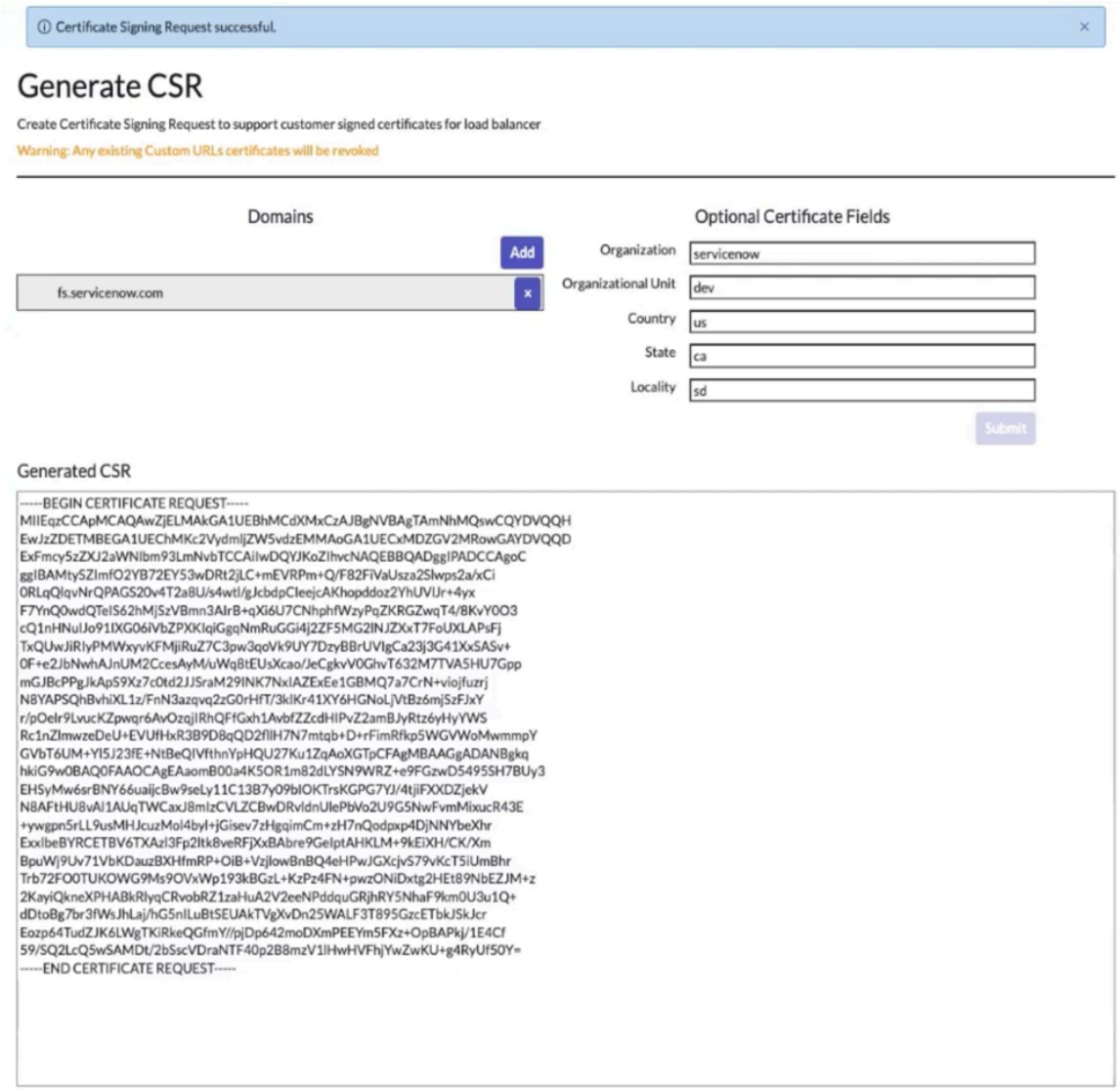
   c. Répétez ces étapes autant de fois que nécessaire pour ajouter d'autres domaines.

   Remarque :
   Les domaines peuvent être supprimés en sélectionnant le bouton X à gauche de chaque entrée de domaine.

3. Saisissez toute information que vous souhaitez inclure dans votre demande dans les **champs de certificat facultatifs**.
4. Sélectionnez **Envoyer**.

Avertissement :
Vous ne pouvez pas soumettre une demande pendant qu'une autre demande est en cours de génération. Si ce problème se produit, l'erreur « Ressource en conflit » s'affiche. Pour traiter, annulez la demande actuelle ou attendez que la demande actuelle soit traitée avant d'en soumettre une autre.

Après avoir sélectionné **Soumettre**, votre instance générera la demande de signature de certificat. La demande apparaît dans le champ **CSR généré** .



5. Copiez le contenu du champ **CSR généré** .

Que faire ensuite

Signez la demande de certificat à l'aide de l'autorité de certification de votre choix. Ce processus est défini par l'autorité de certification que vous sélectionnez. Vous devez consulter la documentation de l'autorité pour ce processus. Une fois que vous avez signé un certificat, chargez-le sur votre instance en suivant les étapes de la section Chargement d'un certificat sur une instance.

Chiffrement Password2 avec Key Management Framework (KMF)

Pris en charge par le Key Management Framework, utilisez le type de Password2 champ (chiffrement bidirectionnel) pour chiffrer et déchiffrer des champs personnalisés avec séparation des tâches, protection des clés et 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 forme de valeur chiffrée sécurisée qui peut être déchiffrée dans l'instance.

Conseil :
À partir de cette Vancouver version, les administrateurs peuvent déconseiller le chiffrement 3DES sur les champs password2 au profit de la nouvelle norme AES (Advanced Encryption Standard). Pour plus de détails, voir Déconseiller l'utilisation de 3DES par GlideEncrypter pour les champs password2.

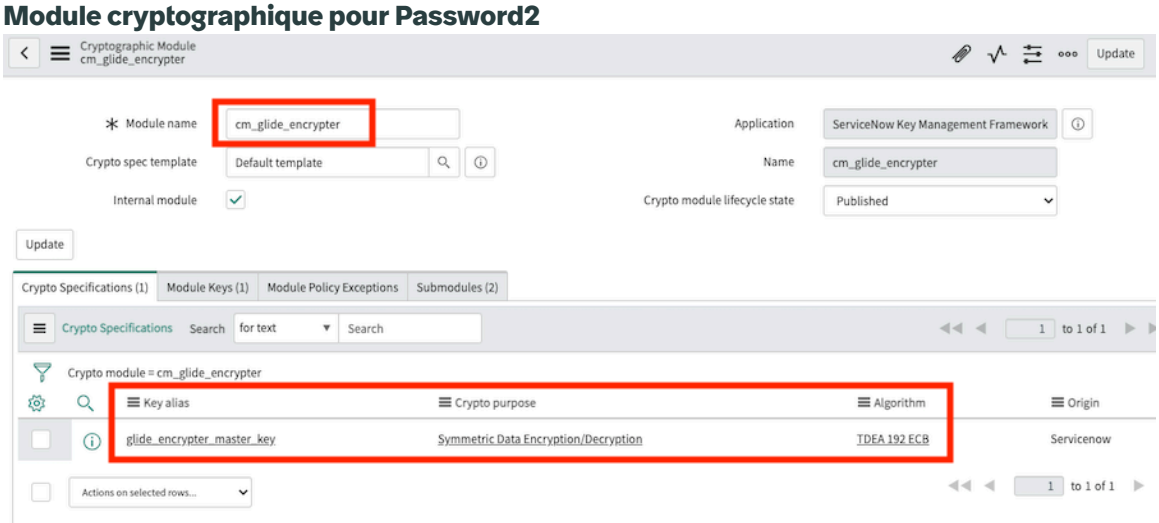
Activation

Password2 La fonctionnalité est active par défaut. Il est contrôlé par la `glide.kmf.encrypter.enabled` propriété, qui est définie sur **true** pour toutes les nouvelles instances et mises à niveau. Vous n'avez pas besoin d'activer Entreprise de Chiffrement au niveau des colonnes pour utiliser Password2.

Mode de fonctionnement de Password2

Le Key Management Framework fournit un module cryptographique parent du système de base **cm_glide_encrypter**. Ce module fournit une spécification cryptographique et une clé qui peut déchiffrer les champs hérités Password2 .

Module cryptographique pour Password2



Ce module cm_glide_encrypter peut avoir des sous-modules, chacun avec sa propre clé de module et sa propre spécification. Si un sous-module est présent avec le même périmètre de l'application que l'application dans laquelle se trouve le Password2 champ, le système utilise le sous-module. Par exemple, si une table de l'application ServiceNow® Service clientèle dispose d'un sous-module et que vous écrivez des informations dans un Password2 champ d'une table du périmètre de l'application Service clientèle , le processus de chiffrement appelle le Service clientèle 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 Washington DC. Des sous-modules sont fournis dans divers modules d'extension d'application sur le Now Platform. Vous pouvez faire pivoter les clés sur les sous-modules, mais pas sur le module de cm_glide_encrypter parent.

Domain Separation et clients sur site

KMF Password2 ne prend pas en charge Domain Separation. Vous pouvez l'utiliser Password2 avec des instances sur site.

L'héritage Password2 et l'actuel Password2

En Washington DC, le champ existant Password2 a été mis à niveau.

La mise en œuvre actuelle de Password2:

- Utilise le conformément aux directives d'encapsulation Key Management Framework de clé 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, fournissant un contrôle via le périmètre de l'application. Chaque sous-module possède sa propre clé de chiffrement AES 256 GCM unique.

Champs Password2 dans les scripts

Lorsque vous accédez à Password2 des champs avec un script, exécutez le script sous 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.setDisplayValue('pwd2column_name', '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 champ d'application. Il est disponible dans le monde entier.

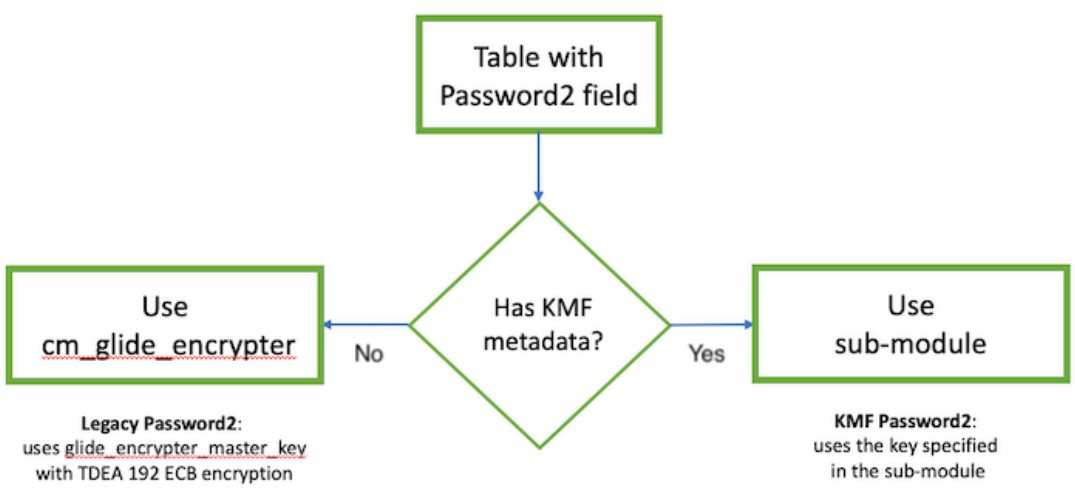
Traduction automatique

1. Lorsque vous chiffrez des données dans un Password2 champ, le système détermine le périmètre de l'application où réside le Password2 champ.
2. Le système recherche ensuite 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 la même portée 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 :

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 les données chiffrées avec un chiffrement hérité Password2 et les chiffre à nouveau avec la clé dans une KMF Password2 clé de sous-module. Le nouveau chiffrement s'applique uniquement aux tables avec Password2 des champs dans les périmètres de l'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) n'est chiffré à nouveau que 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 (chiffrement d'enveloppe) dans la KMF hiérarchie des clés.

Chiffrement dans le cloud avec Key Management

ServiceNow® Chiffrement dans le cloud offre un stockage chiffré pour la base de données à l'aide du chiffrement par blocs, ainsi qu'une gestion améliorée des clés. Chiffrement dans le cloud est disponible avec le ServiceNow® Lot d'abonnements Platform Encryption.

Chiffrement dans le cloud Offre:

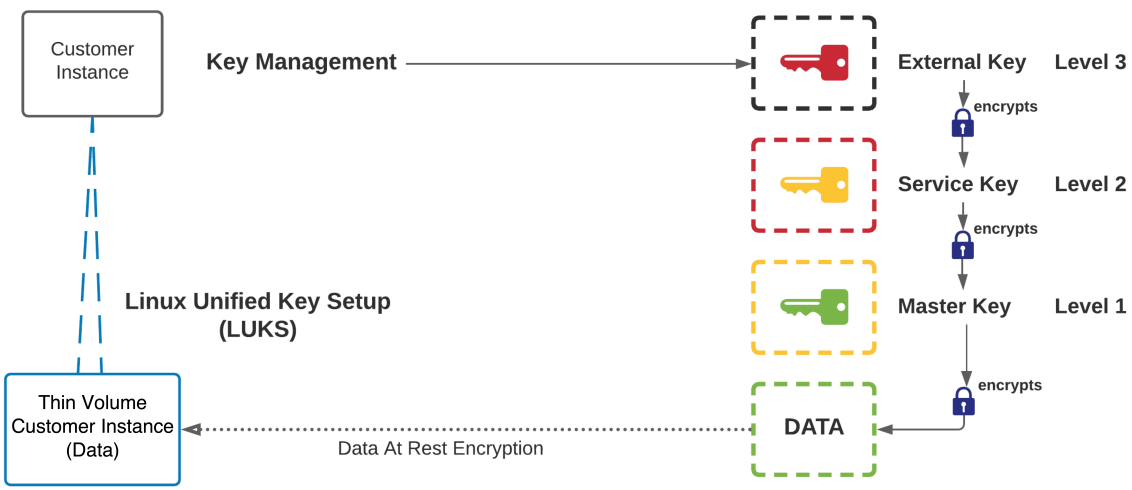
- Séparation des tâches.
- Rotation des ServiceNow clés gérées.

- Option Clés gérées par le client.

Remarque :
Vous pouvez utiliser cette option si votre organisation exige que vous utilisiez du matériel clé généré par vos propres outils ou bibliothèques de chiffrement, votre système de gestion des clés d'entreprise ou votre module de sécurité matériel (HSM). Consultez Opérations de gestion des clés pour en savoir plus.

Le diagramme suivant montre comment Chiffrement dans le cloud cela fonctionne.

Vue d'ensemble de Chiffrement dans le cloud



Le Chiffrement dans le cloud module Key Management se compose des sous-modules suivants :

- Opérations de gestion des clés :
  - Accédez à la liste des clés.
  - Effectuez des opérations de rotation de clés.
  - Retirer la clé gérée par le client.
- Transactions de gestion des clés :

  Référencez toutes les transactions qui ont eu lieu pour les clés qui ont été utilisées.

  Utilisez votre propre clé gérée par le client pour le chiffrement.

Dans certaines circonstances, une demande de retrait de clé peut être choisie lors de l'utilisation de clés gérées par le client. Vous devez d'abord demander la fonctionnalité de retrait de Service et assistance client clé et remplir un addendum légal.

L'option Paramètres de la politique de contrôle du quorum devient disponible lorsque la fonction 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 stratégie permet de configurer les 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 la base de données MariaDB pour les instances de production et de non-production. Postgres avec les extensions Swarm64 est pris en charge pour ServiceNow les bases de données de réplication en lecture.

Pour en savoir plus sur la gestion des licences Chiffrement dans le cloud, reportez-vous à Offre groupée d'abonnements Chiffrement et gestion des clés.

Pour que les clients sous licence puissent demander qu'une instance soit déplacée vers Chiffrement dans le cloud, suivez les instructions de la section KB1117369 . Vous devez avoir le rôle d'administrateur client ou administrateur partenaire pour demander à l'élément de Service Catalog **d'activer Cloud Encryption sur votre instance**. L'activation de cette fonctionnalité nécessite une fenêtre de maintenance d'une heure.

Opérations de gestion des clés

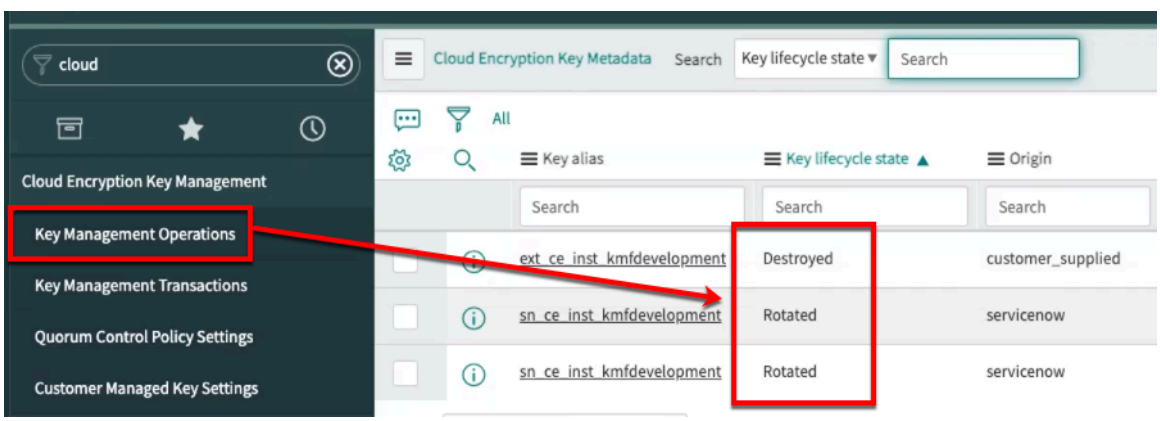
Le sous-module Opérations de gestion des clés permet d'afficher et de gérer toutes les clés de chiffrement utilisées avec ServiceNow Chiffrement dans le cloud.

Prise en main de Cloud Encryption

États du cycle de vie de la clé

Il n'y a qu'une seule clé active dans le système à un moment donné. Lorsque vous sélectionnez une clé, vous accédez à l'activité de la clé sélectionnée, telle que les clés pivotées ou retirées et l'horodatage correspondant.

L'état du cycle de vie de la clé est mis à jour en fonction de l'opération de gestion des clés effectuée.



Voir Rotation d'une clé gérée par ServiceNow ou Rotation d'une clé gérée par le client pour plus de détails.

Remarque :
Le processus de rotation des clés peut prendre jusqu'à 20 minutes.

Rotation d'une clé gérée par ServiceNow

Faites pivoter la clé gérée active Chiffrement dans le cloud ServiceNow .

Avant de commencer
Rôles requis : kmf_admin, kmf_cryptomanager

Important :
Si vous utilisez des clés gérées par le client, reportez-vous à la section Rotation d'une clé gérée par le client.

Traduction automatique

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 Métadonnées clés se charge. Toutes les clés utilisées dans votre instance sont répertoriées. Une seule clé peut être active à la fois.

   Si vous Chiffrement dans le cloud accédez au module pour la première fois, les entrées de clés seront disponibles après une rotation de clés initiale. 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 votre ServiceNow clé générée.
3. Sélectionnez le bouton **Faire pivoter la clé** .
   Une notification s'affiche avec la possibilité de continuer la rotation des 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 de la Chiffrement dans le cloud clé.
   Les entrées sont répertoriées pour la clé active actuelle et la clé qui est générée pour tourner à la place de la clé active actuelle. Consultez États du cycle de vie de la clé Key Management Framework les différents états disponibles.

   La clé active est répertoriée avec la version de clé `0` et la clé générée a la version `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 du 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 en vue de son chargement dans votre instance.

Avant de commencer

Rôles requis : sn_kmf.cryptographic_manager, sn_kmf.admin

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 encapsulée par un certificat d'encapsulation Cloud Encryption 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 Windowsde , vous devez générer la clé encapsulée via les applications de prise en charge du shell Bash telles que Git Bash.

Procédure

1. Générez une valeur aléatoire à utiliser comme clé symétrique AES-256 bits à l'aide d'OpenSSL.

   Pour des raisons de compatibilité, votre clé symétrique doit avoir les attributs suivants :

Attribut	Valeur
Type de clé	Clé symétrique basée sur l'algorithme AES (Advanced Encryption Standard).
Taille de la clé	256 bits (32 octets)
Besoin d'encapsulation de clé	○ Algorithme de chiffrement RSA ○ Remplissage de chiffrement asymétrique optimal (OAEP) ○ Fonction de hachage SHA-256 (RSAES_OAEP_SHA_256) ○ Encodé à l'aide de l'algorithme Base64

2. Enregistrez la clé dans un fichier similaire à « openssl rand 32 > plaintext_key.bin ».

   Important :
   Enregistrez ce fichier en toute sécurité pour référence future. Cette clé est encapsulée avec la clé publique pour le chargement.

3. Extrayez la clé publique du fichier de certificat encapsulé téléchargé de votre instance :

```
openssl x509 -pubkey -noout -in wrapping_cert.pem > public_key.pem
```

   Remarque :
   Reportez-vous à la section pour plus d'informations afin de télécharger le certificat d'encapsulation.

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 sur cette commande contient une clé encapsulée gérée par le client qui peut être fournie à SN pour le processus CMK.

Basculer entre les clés ServiceNow et les clés gérées par le client

Basculez entre une clé gérée par le client ou une clé gérée pour une ServiceNow utilisation dans ServiceNow Chiffrement dans le cloud.

Par défaut, votre instance est configurée pour utiliser ServiceNow des clés gérées, et ServiceNow la génération de la clé 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 une fois que vous avez encapsulé la clé gérée par le client pour Chiffrement dans le cloud.

Avant de commencer

Rôles requis : kmf_admin, kmf_cryptomanager

Procédure

1. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés**.
   La liste **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 **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 du **cycle de vie** de la clé est Actif. Il n'y a 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**.
   La `public_certificate.... Le fichier zip` est téléchargé sur votre ordinateur local et est utilisé pour encapsuler votre clé gérée par le client.

   > **⚠ Avertissement :**
   > Évitez les problèmes potentiels liés aux certificats en téléchargeant le certificat d'encapsulation chaque fois que vous effectuez une rotation ou basculez vers une clé gérée par le client.

   b. Sélectionnez **Parcourir** pour charger votre clé gérée par le client, puis recherchez et sélectionnez votre clé de chiffrement encapsulée.
   Pour choisir un autre fichier, sélectionnez-le, puis 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 s'affiche, 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 et de chargement des clés sont répertoriées. Consultez Transactions de gestion des clés pour plus de détails 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 de votre clé gérée par le client. Cette nouvelle clé a une valeur **d'origine** de **customer_supplied** et est à l'état **Actif** . Votre clé précédente a 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 : kmf_admin ou kmf_cryptomanager

Pour passer à une clé gérée par le client, vous devez disposer d'une clé gérée par le client encapsulée prête à être téléchargée dans le cadre de ces étapes. Pour en savoir plus sur la préparation de cette clé en vue du chargement, 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 **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 du **cycle de vie** de la clé est Actif. Il n'y a 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** , effectuez les étapes répertoriées.

   a. Sélectionnez **Télécharger le certificat d'encapsulation**.

   > **Avertissement :**
   > Évitez les problèmes potentiels liés aux certificats en téléchargeant le certificat d'encapsulation chaque fois que vous effectuez une rotation ou basculez vers une clé gérée par le client.

   b. Sélectionnez **Parcourir**, puis suivez les instructions pour sélectionner et télécharger 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 d'origine est passé à **Tournée**.
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 de votre clé gérée par le client. Cette nouvelle clé a une valeur **d'origine** 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 risque d'être inaccessible.

Basculer vers une clé gérée par ServiceNow

Passer d'une clé gérée par le client à une clé gérée pour ServiceNow Chiffrement dans le cloud.

Avant de commencer
Rôle requis : kmf_admin ou kmf_cryptomanager

Procédure

1. Accédez à la **Tous** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés**.
2. Dans la liste **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 du **cycle de vie** de la clé est Actif. Il n'y a 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 d'origine est passé à **Tournée**.
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. 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 clé cryptographique nouvellement générée. Si vous utilisez une clé gérée par le client, ce calendrier peut vous rappeler de faire pivoter manuellement vos clés personnalisées.

Avant de commencer
Rôle requis : 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.

Champ	Description
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.
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 pour que votre instance envoie des notifications.
Les notifications par e-mail sont envoyées à la liste suivante de vos administrateurs de sécurité approuvés :	Liste des utilisateurs qui reçoivent des notifications pour la rotation des clés. **L'administrateur système** figure sur cette liste par défaut.

4. Sélectionnez **Soumettre**.
   Après avoir sélectionné Soumettre, une notification s'affiche 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. Lors du clonage d'une tâche de rotation de clés planifiée d'une instance source A vers une instance cible B, la tâche planifiée sur l'instance B échouera la validation de la signature. Dans ce cas, vous pouvez recréer la signature en désélectionnant puis en cochant à nouveau la case **Activer la rotation de clés planifiée** . Pour plus d'informations sur ce problème, consultez 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 sur la page Opérations de gestion de clés. Les opérations de retrait de clé et d'approbation du quorum peuvent également être gérées.

Avant de commencer

Rôles requis : kmf_admin, kmf_cryptomanager

Cette section s'applique uniquement si vous disposez d'une licence Cloud Encryption Withdrawal and Resupply, un module complémentaire facultatif à 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 des touches est désormais disponible.
3. Sélectionnez la **clé de retrait** pour déclencher le processus de retrait.

Traduction automatique

Avertissement :

Un message d'avertissement Retirer la clé s'affiche. Le retrait de la clé déclenche l'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 clé, 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 [Standard Operating Procedure] de sauvegarde et de restauration pour plus d'informations), les sauvegardes de votre base de données d'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 êtes renvoyé 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 effectué avec succès pour terminer le retrait de clé. Consultez Gérer le contrôle du quorum pour en savoir plus.

Réapprovisionner une clé gérée par le client

Une fois l'opération de retrait de clé terminée, votre clé gérée par le client doit être de nouveau fournie dans votre instance.

Avant de commencer
Rôle requis : kmf_admin, kmf_cryptomanager

Remarque :
Cette section s'applique uniquement si vous disposez d'une licence Cloud Encryption Retrait et réapprovisionnement.

Procédure

1. Accéder à Now Support et naviguer jusqu'à **Catalogue de services** > **Catalogue** > **Gestion de l'instance** > **Restauration d'instance : réapprovisionner la clé gérée**.
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** .
4. Téléchargez le certificat d'encapsulation en cliquant sur le texte du **certificat d'encapsulation** .

> **⚠ Avertissement :**
> Vous devez télécharger un nouveau certificat d'encapsulation chaque fois que vous effectuez une rotation 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 téléchargée, vous pouvez voir la clé sous **Fichier téléchargé avec succès**. Si vous devez télécharger à nouveau la clé, cliquez sur **Supprimer le fichier** et téléchargez à nouveau votre clé comme décrit dans les étapes précédentes.
7. Cliquez sur **la touche Rotation** pour terminer le réapprovisionnement.

Politique de contrôle du quorum

La politique de contrôle du quorum spécifie le nombre minimal d'approbations requises parmi le nombre total d'approbateurs sélectionnés pour atteindre le quorum pour le retrait de clé géré par le client.

> **⚠ Avertissement :**
> Vous devez signer un addendum juridique pour activer la fonctionnalité de retrait de clé. L'option Paramètres de la politique de contrôle du quorum devient disponible lorsque la fonction 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 fournie de nouveau et qu'elle 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 à partir de Service et assistance client.

La politique de contrôle du quorum spécifie le nombre minimal d'approbations requises parmi le nombre total d'approbateurs sélectionnés pour atteindre le quorum pour le retrait de clé géré 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 minimum d'approbateurs atteint, le quorum est atteint et le retrait de clé se déclenche. Le retrait est effectué et consigné, y compris les noms des utilisateurs qui ont approuvé la demande.

Consultez Configurer les paramètres de la politique de contrôle du quorum les détails de la configuration.

Configurer les paramètres de la politique de contrôle du quorum

Suivez ces étapes pour configurer les paramètres de politique de contrôle du quorum.

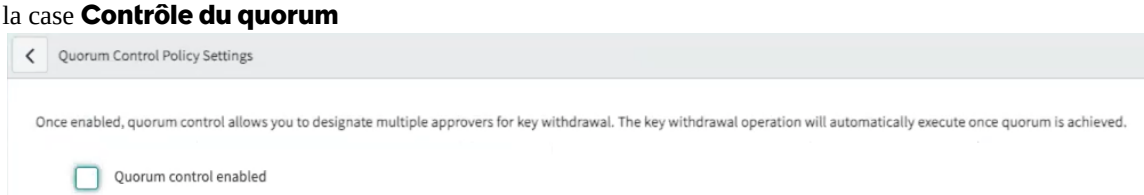
Avant de commencer
Rôles requis : kmf_admin, kmf_cryptomanager

Pourquoi et quand exécuter cette tâche

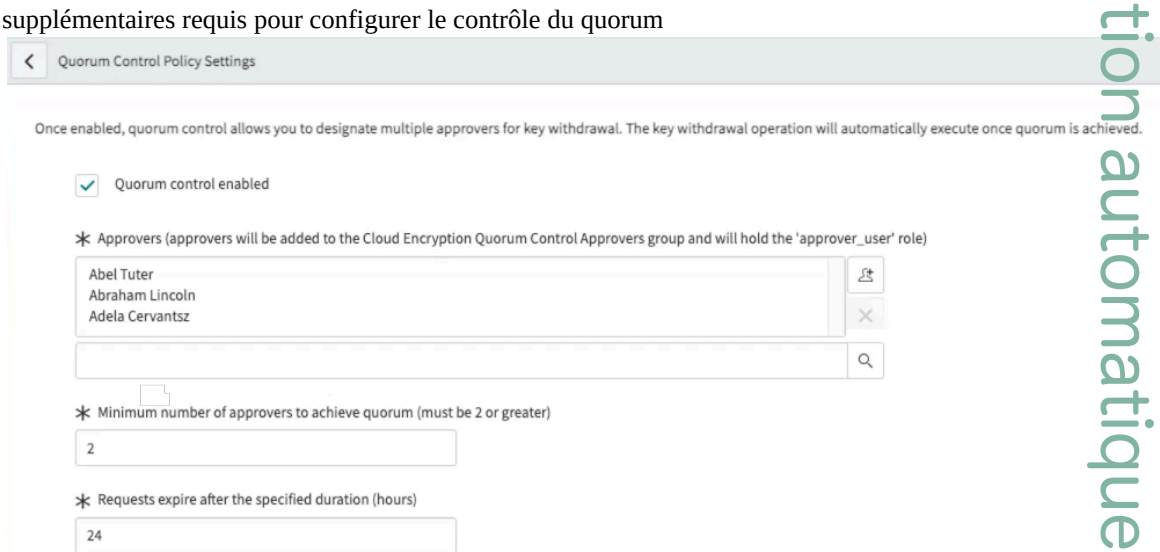
Avertissement :
Vous devez signer un addendum juridique pour activer la fonctionnalité de retrait de clé. L'option Paramètres de la politique de contrôle du quorum devient disponible lorsque la fonction de retrait est activée, sinon le module n'est pas visible dans le menu de l'application. Après le retrait de la clé, votre instance n'est plus disponible tant que la clé de chiffrement n'est pas à nouveau active.

Procédure

1. Demandez la fonctionnalité de retrait de clé à partir de Service et assistance client.
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 .
Les champs supplémentaires requis pour configurer le contrôle du quorum



apparaissent.

4. Renseignez les champs pour remplir le formulaire.
5. Cliquez sur **Envoyer**.
   Un message de confirmation s'affiche.

Que faire ensuite
Les actions de retrait sont disponibles en Opérations de gestion des clés.

Gérer le contrôle du quorum

Une fois qu'un workflow d'opération de retrait est déclenché, 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.

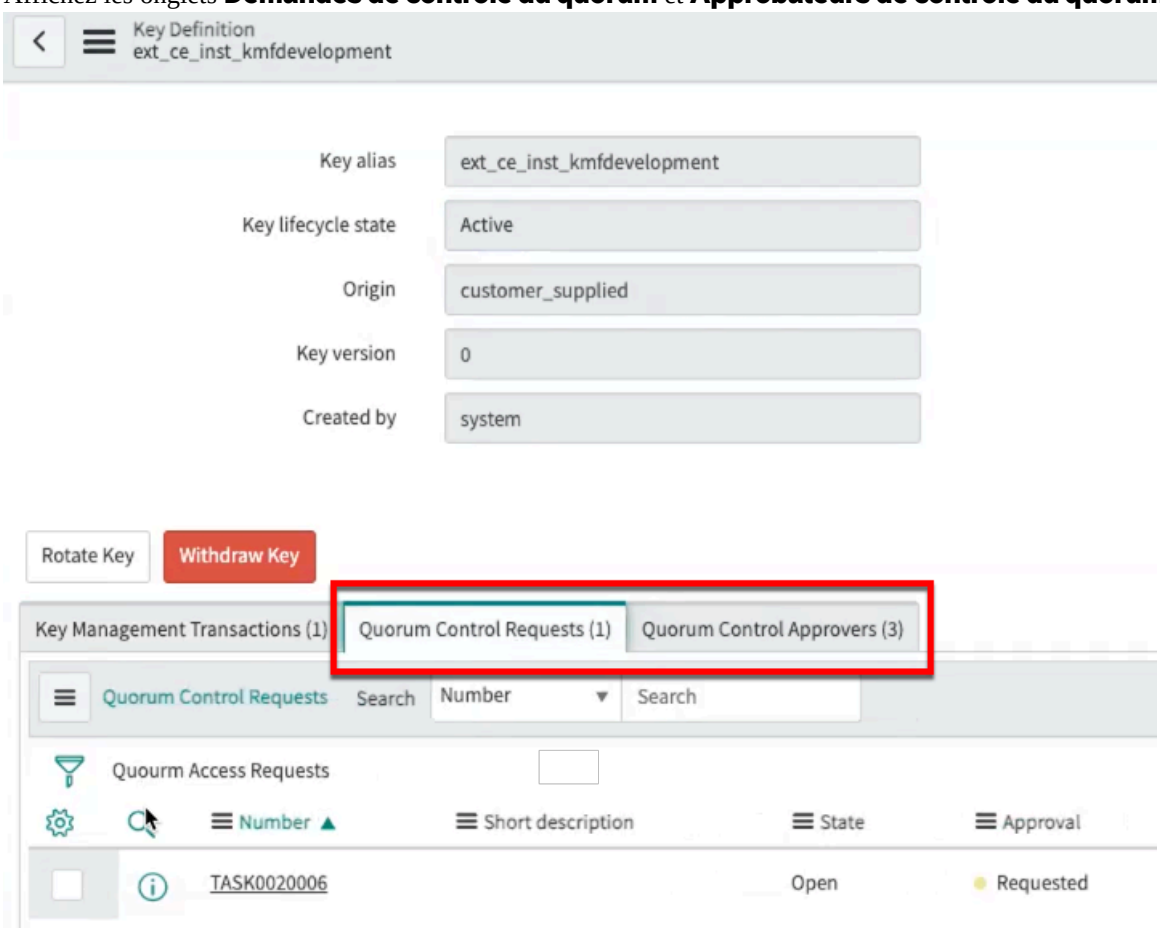
Avant de commencer

Rôle requis : kmf_admin ou kmf_cryptomanager

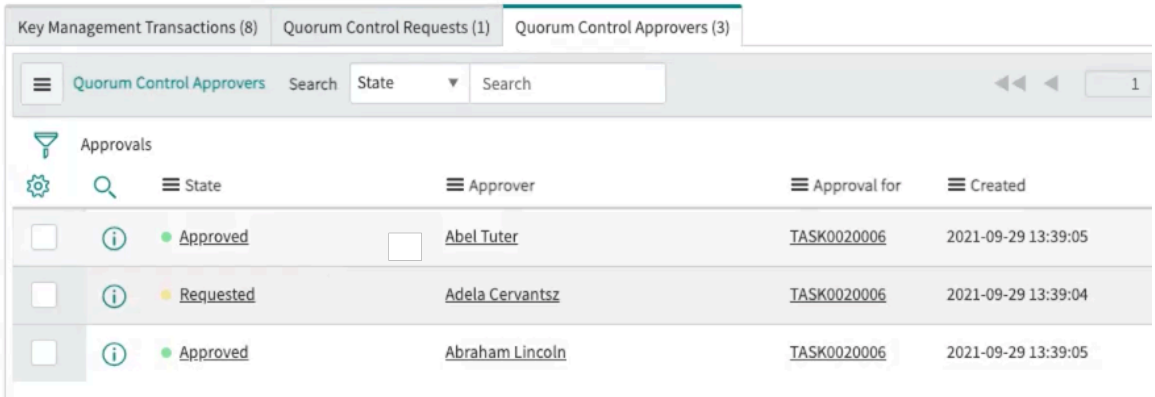
Lorsque le quorum a été approuvé ou rejeté, le demandeur du retrait de clé reçoit un e-mail indiquant si le quorum a été atteint ou refusé.

Procédure

1. Effectuez les étapes pour retirer une clé gérée par le client trouvée dans Opérations de gestion des clés.
2. Affichez les onglets **Demandes de contrôle du quorum** et **Approbateurs de contrôle du quorum** .



3. Ouvrez le **Demandes de contrôles du quorum** pour afficher la demande réelle qui est créée.
   - État :
     - Ouvert : l'action de retrait de clé est en attente que le quorum soit atteint.
     - Fermé terminé : le quorum a été atteint et il ne peut y avoir aucune autre action sur cette demande de quorum particulière.
   - Approbation:
     - 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 effectuée 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 effectué d'action sur la demande d'approbation.
- Approuvée : la demande a été approuvée à partir de l'e-mail ou 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 complétée afin de déclencher les étapes clés de retrait.
   - Étape 1 - Retrait de clé : L'étape de retrait de clé. Il comprend les étapes deux à sept.
   - Étape 2 - Request_preparation : crée une demande de déclenchement, d'emballage et de rotation.
   - Étape 3 - request_integrity_check : Validez 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.

Pourquoi et quand exécuter cette tâche
Lorsqu'une demande de quorum a été créée, le nombre minimal d'approbations est requis par les membres. Une fois qu'un workflow d'opération de retrait est déclenché, 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, 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 : kmf_admin, kmf_cryptomanager

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.

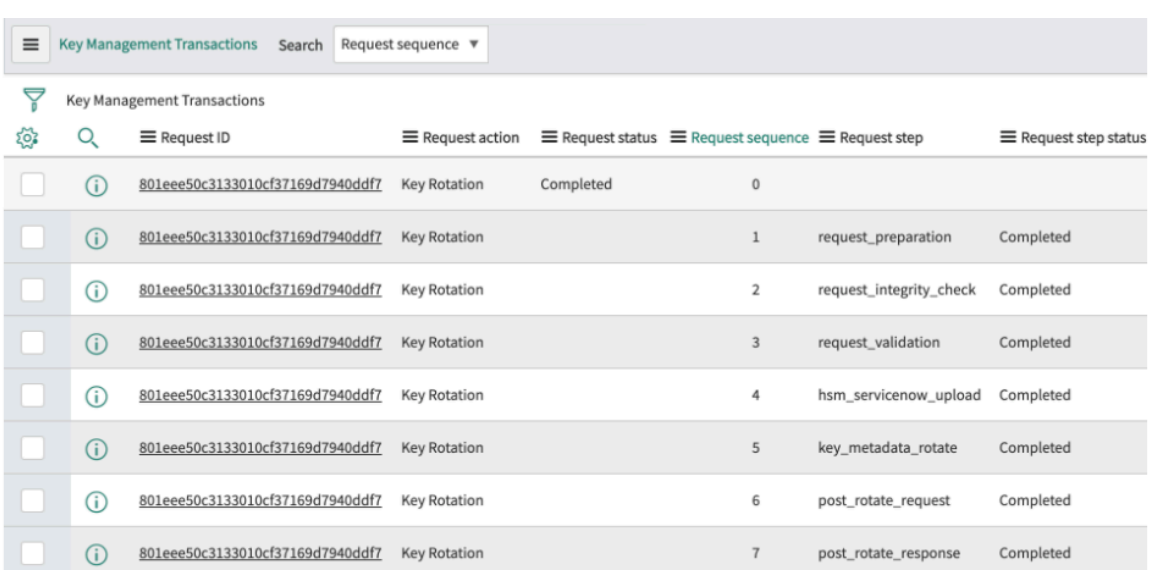
Transactions de gestion des clés

Le sous-module Transactions de gestion des clés affiche toutes les transactions qui ont eu lieu pour les clés dans votre ServiceNow instance.

- Une transaction de clé est définie par les éléments suivants :
  - Composé de plusieurs étapes de demande.
  - Un seul `ID de demande` est partagé pour toutes les étapes de demande.
  - L'étape initiale (séquence de demande 0) d'une transaction fournit l'état actuel de la transaction globale.

    Comme le montre l'image ci-dessous, `l'état` global de la demande de l'étape initiale 0 est 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 a l'état Échoué. Si toutes les étapes sont terminées, l'état de la transaction est également terminé.

L'écran suivant est un exemple du type d'informations qui s'affichent avec une ServiceNow rotation de touches.



Le tableau suivant affiche les informations de champ disponibles sur la page Transactions de gestions de 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 pour toutes les étapes de demande.
Action de demande	Affiche l'action de l'opération clé en cours d'exécution.
État de la demande	• En cours de traitement : une demande a été saisie, mais n'a pas encore été traitée. • Terminée : la demande a été effectuée avec succès. • Échec : un problème s'est produit et le processus n'a pas été terminé. **Remarque :** Contactez Service et assistance client et fournissez le numéro de demande où la panne s'est produite.
Alias de la clé	Entrée alphanumérique.
État du cycle de vie de la clé	Voir États du cycle de vie de la clé Key Management Framework pour les définitions.
Origine	• ServiceNow Clé • Clé gérée par le client
Version de la clé	Lorsqu'une clé pivote, le numéro de version s'incrémente.
Séquence de demande	Affiche l'ordre dans lequel une demande est traitée dans le système.
Étape de demande	Indique 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 clé effectuée. 1. request_preparation : crée une demande de déclenchement, d'emballage et de 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, une seule demande de rotation peut être traitée à la fois. 4. attachment_process : extrait le matériel de clé encapsulée 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 clés. 7. post_rotate_request : envoie une demande pour effectuer la rotation de clés. 8. post_rotate_response : réponse permettant d'effectuer la rotation de clés en fonction de la demande de l'instance client.

Transactions de gestion des clés (suite)

Champ	Description
	Remarque : Fournissez l'étape de demande pour Service et assistance client 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 : échec de la rotation. **Remarque :** Fournissez l'étape de demande pour Service et assistance client analyser la progression de l'état au cas où une étape de demande ne se terminerait pas.

Journalisation de Chiffrement dans le cloud

Découvrez 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 journalisation relatives aux transactions Chiffrement dans le cloud sur votre instance.

Table	Description
Métadonnées de chiffrement dans le cloud [dare_key_metadata]	Les métadonnées Cloud Encryption capturent les métadonnées clés de la gestion du cycle de vie. Dans cette table, vous trouverez des informations clés sur le cycle de vie, l'état et la version. Cette table est mise à jour après chaque opération clé.
Transactions de gestion des clés [dare_key_request]	Transactions de gestion des clés capture les informations sur les transactions de gestion des clés. Dans ce tableau, vous trouverez la journalisation de chaque étape d'une transaction. La table enregistre toute information d'erreur pour une transaction dans le champ de **message d'erreur** .
Audits sys[sys_audit]	La table Audits système capture, insère et met à jour tous les enregistrements audités sur votre instance. Dans cette table, vous pouvez trouver les changements apportés aux enregistrements sur votre instance, la date à laquelle les changements ont été apportés et le compte d'utilisateur à l'origine du changement.

Surveiller les opérations de rotation des clés

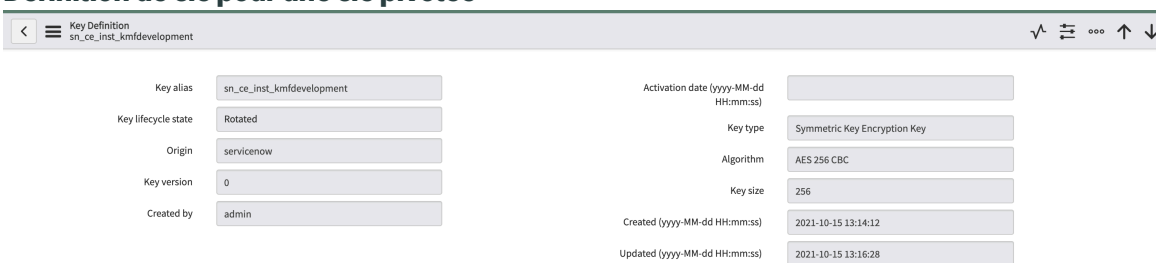
Utilisez la table Métadonnées de clé de chiffrement dans le cloud [dare_key_metadata] pour trouver des informations sur le cycle de vie de votre clé. Dans ce tableau, vous trouverez des informations telles que l'origine, la date d'activation, l'état et la version de vos clés.

Utilisez la table Transactions de gestion des clés [dare_key_request] pour surveiller les transactions des opérations clés. Dans ce tableau, vous trouverez toutes les demandes

relatives à vos clés, y compris l'état, le statut et l'étape du processus dans laquelle se trouve la demande. Les demandes terminées sont conservées dans cette table avec l'état **Terminé** .

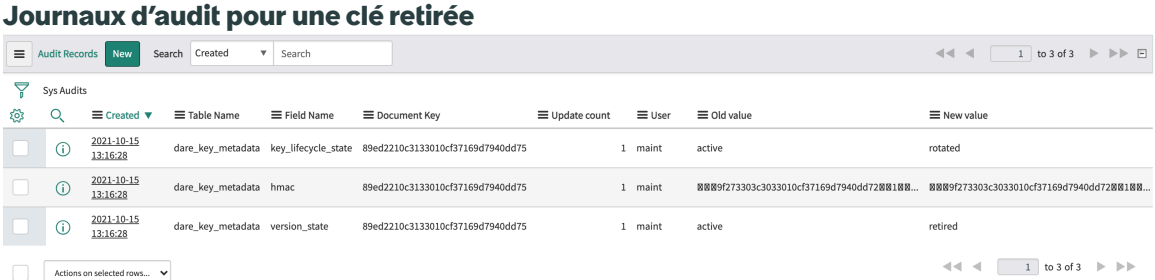
Cet exemple montre une opération de rotation de clés. Au cours de cette opération, l'état de l'ancien cycle de vie de la clé passe d'Actif à Pivoté, et l'état de la version passe d'Actif à Mis hors service.

Définition de clé pour une clé pivotée



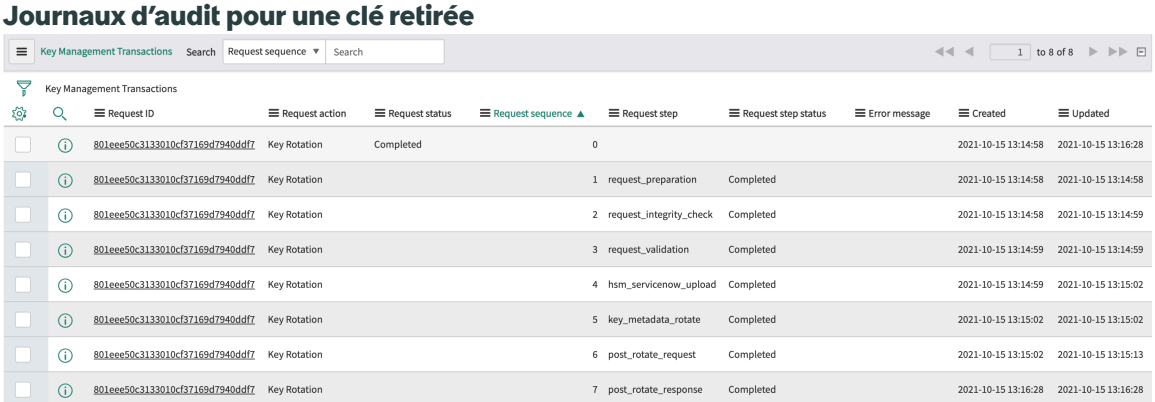
En examinant la table Audits système[sys_audit], les administrateurs peuvent voir les changements apportés aux enregistrements dans la table Métadonnées de clé de chiffrement dans le cloud [dare_key_metadata]. Les administrateurs peuvent voir quels enregistrements ont été mis à jour et quand. Les entrées du journal enregistrent également le champ qui a été modifié, ainsi que les anciennes et nouvelles valeurs.

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 enregistrements d'audit ci-dessous, l'état de la demande est passé de Traitement à Terminée.

Journaux d'audit pour une clé retirée

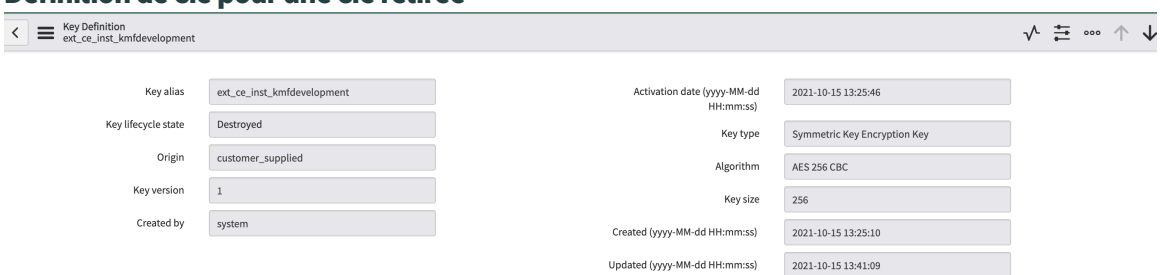


Journalisation des opérations de retrait de clés

Les informations de journalisation sur le retrait de clé sont stockées dans la table Audits [sys_audit]. Ces informations de connexion contiennent des informations sur la personne à l'origine du retrait de clé et sur le moment où le retrait a eu lieu.

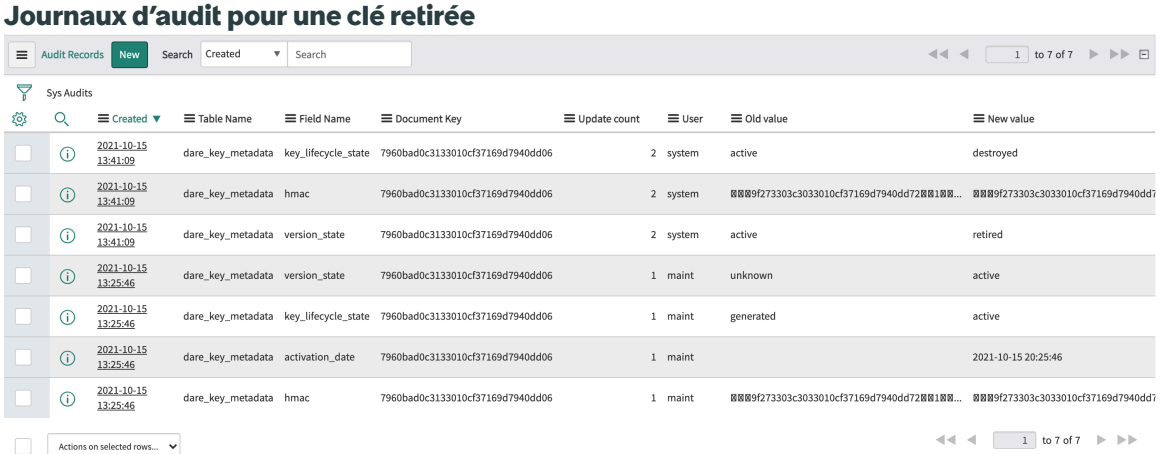
Cet exemple montre une opération de retrait de clé. Au cours de cette opération, l'état du cycle de vie de la clé est mis à jour de généré à actif, puis défini. La version de clé est mise à jour de Inconnue à Active, puis à Mise hors service.

Définition de clé pour une clé retirée



En examinant la table Audits système[sys_audit], les administrateurs peuvent modifier la table Métadonnées de clé de chiffrement dans le cloud [dare_key_metadata].

Journaux d'audit pour une clé retirée



Détection de falsification

Utilisez la détection de falsification pour améliorer la sécurité en détectant les changements non autorisés apportés à vos paramètres de contrôle du quorum.

Processus de détection de falsification

Lorsqu'elle est activée, la détection de sabotage valide vos paramètres de contrôle du quorum en vérifiant toute modification non autorisée (altération). La détection de falsification utilise un code d'authentification de message basé sur le hachage (HMAC).

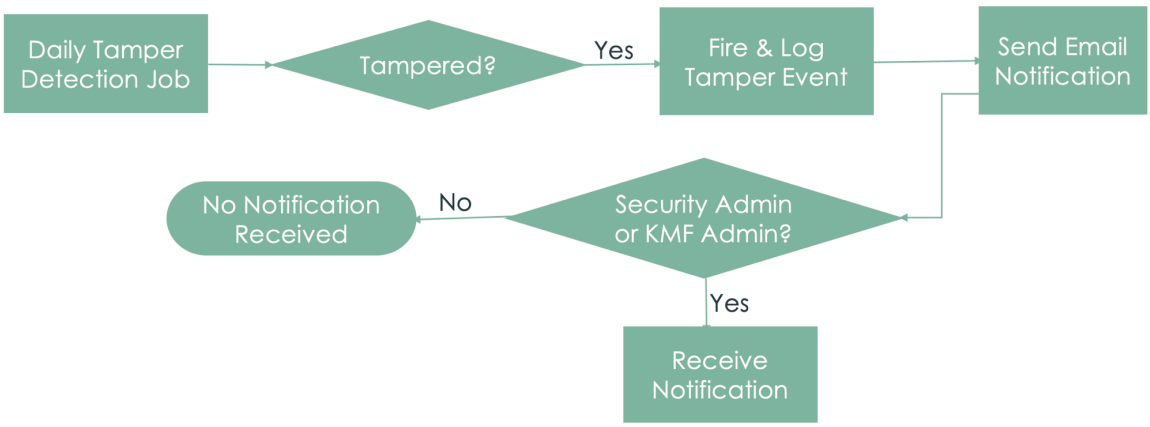
1. Lorsqu'un paramètre est modifié ou créé, votre instance crée un HMAC. Le protocole HMAC est basé sur la valeur de l'enregistrement de paramètre (dare_property).
2. Chaque fois que votre instance utilise ces paramètres, la détection d'altération les valide à l'aide du HMAC.
3. Si le paramètre est validé avec succès, il peut être utilisé par la plateforme, sinon ce n'est pas le cas.

La détection de falsification s'exécute quotidiennement sur votre instance

La détection d'altération vérifie l'altération 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. La détection de falsification envoie une

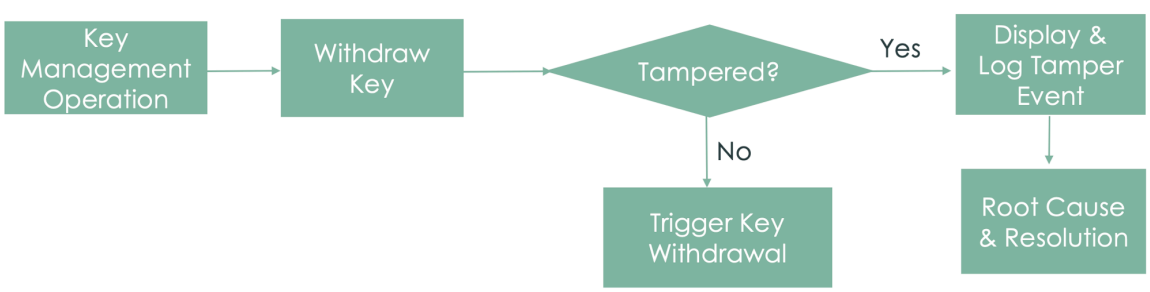
Traduction automatique

notification aux administrateurs de sécurité et KMF en cas d'échec de validation.



La détection de falsification s'exécute avant l'exécution d'un retrait de clé

La détection d'effraction 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 avoir lieu.



Identification de l'altération

La détection de falsification 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.

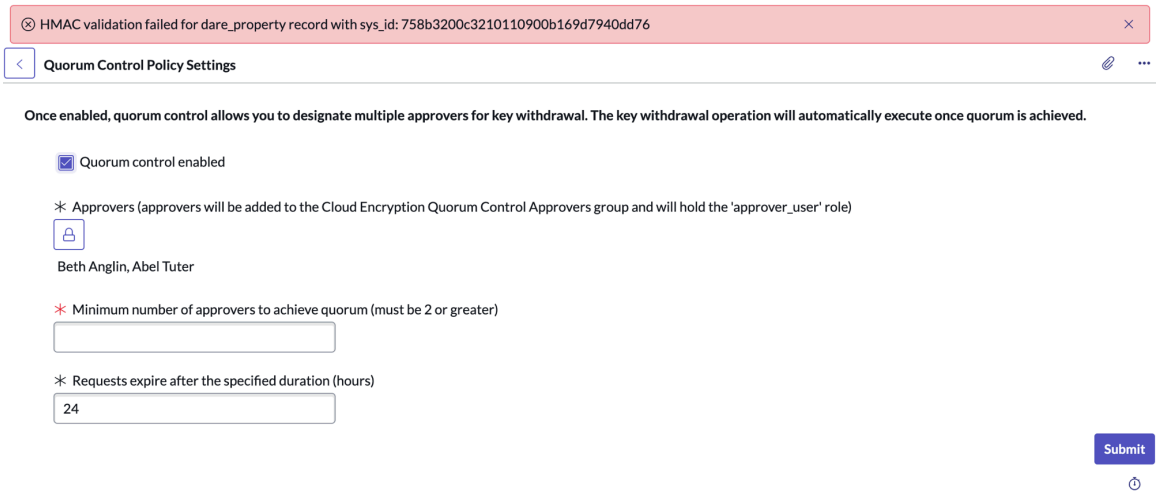
```
2022-06-28 13:45:46 (582) Default-thread-5
 B6FAC1F6C3D01110CF37169D7940DD6E txid=231c4d72c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 776e3200c3210110900b169d7940dd76 failed HMAC validation

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.

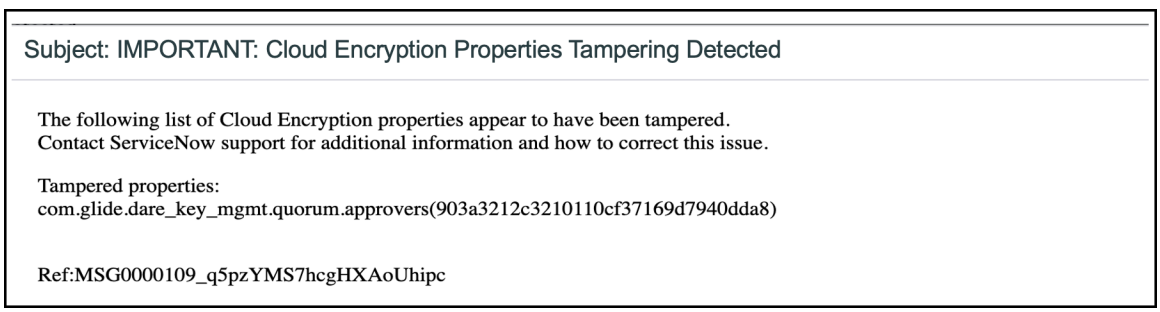
La détection de falsification affiche un message d'avertissement sur la page des paramètres de contrôle du quorum

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 la sys_id de l'enregistrement des paramètres (dare_property) dont la validation a échoué.



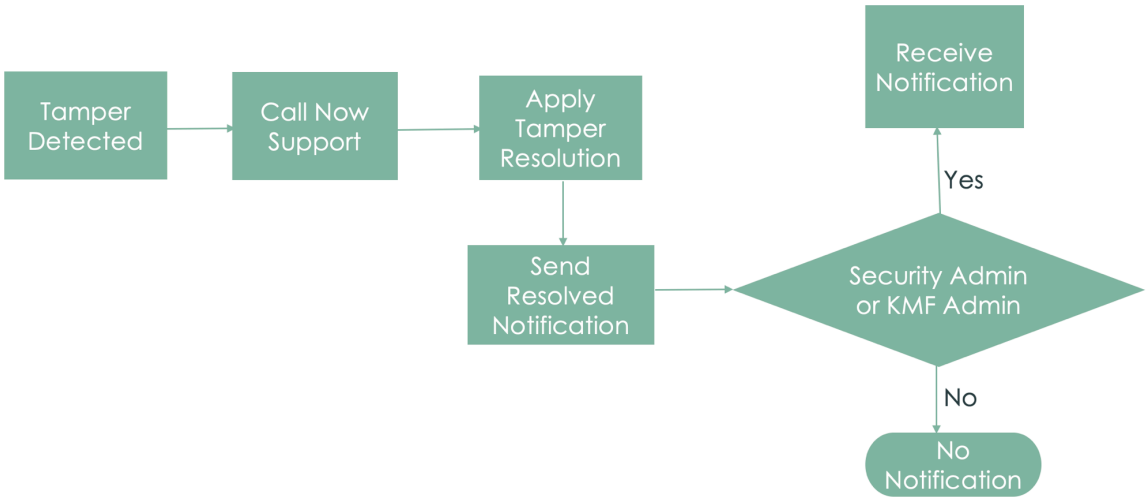
La détection d'altération envoie des notifications aux utilisateurs disposant des `Security Admin` rôles et `KMF Admin`

Si la détection d'altération ne valide aucun de vos paramètres de contrôle du quorum, vos administrateurs de sécurité et vos administrateurs KMF reçoivent une notification semblable à cet exemple.



Résolution des problèmes de falsification grâce à l'assistance ServiceNow

Important :
Les échecs de validation de la détection d'effraction ne peuvent être résolus qu'avec l'aide de l'assistance ServiceNow .



Si la détection de sabotage ne valide aucun 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 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 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.

Important :
À partir de cette Washington DC version, Database Encryption ne sera plus disponible. Cloud Encryption est la solution de remplacement pour le chiffrement des données au repos. Pour en savoir plus, consultez Chiffrement dans le cloud avec Key Management

Explorer

Découvrez les principales fonctionnalités et la valeur commerciale de Database Encryption.

Demande

En savoir plus sur la façon de demander la rotation des clés de base de données.

Référence

En savoir plus sur le chiffrement de base de données.

Traduction automatique

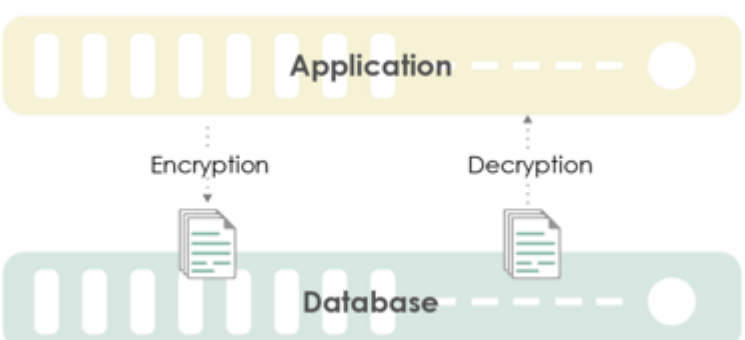
Exploration de Database Encryption

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 cette Washington DC version, Database Encryption ne sera plus disponible. Cloud Encryption est la solution de remplacement pour le chiffrement des données au repos. Pour en savoir plus, consultez Chiffrement dans le cloud avec Key Management

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. De ce point de Now Platform vue, toutes les données sont déchiffrées.

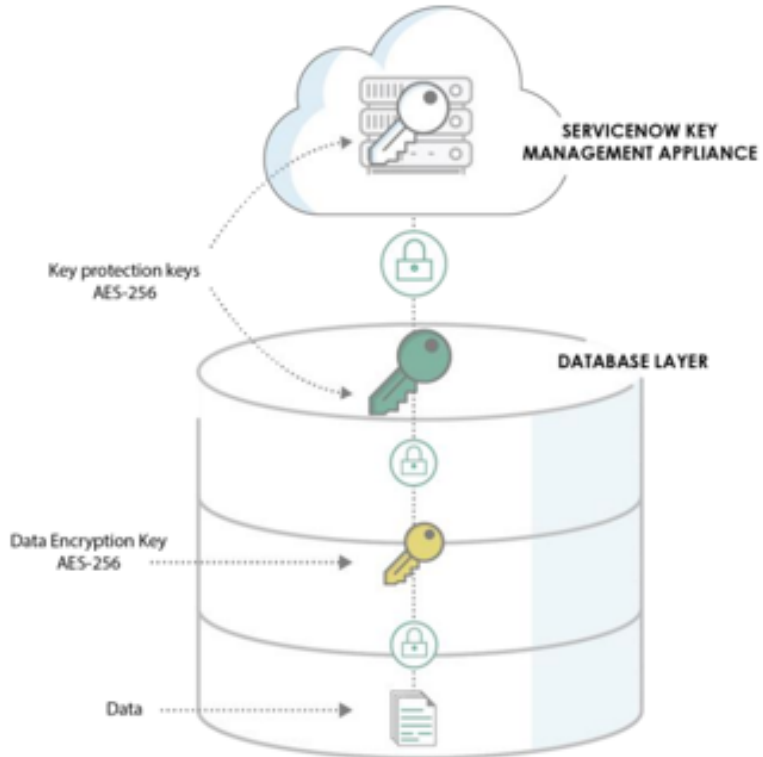
- Le chiffrement de la base de données prend en charge le chiffrement de toutes les données stockées en temps réel, offrant une protection des données en ligne et hors ligne sans perte de fonctionnalité.
- Le chiffrement intégral du disque protège les données hors ligne en cas de perte ou de vol du disque.



Avec le chiffrement de la base de données, toutes les données stockées sont chiffrées et les enregistrements individuels ou les tables 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, rétablissement, annulation et erreur) sont également chiffrés.

Database Encryption 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 allant jusqu'à 5 %. Les instances nouvelles et existantes sur les versions prises en charge de la Now Platform peuvent tirer parti du chiffrement de base de données.

Comme illustré, ServiceNow stocke et gère les clés à l'aide d'une hiérarchie de clés à trois niveaux :



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 des clés validés par FIPS 140 dans les ServiceNow centres de données. Cette clé protège la clé de deuxième niveau et est unique par instance client.

Il Now Platform prend également en charge le chiffrement de la 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 le cryptage AES standard de l'industrie sans impact sur les fonctionnalités. La base de données chiffre les données au fur et à mesure qu'elles sont écrites sur le disque et déchiffre les données au fur et à mesure qu'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 :
Database Encryption 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 de la clé de base de données une fois par an ou selon les besoins en soumettant une demande d'assistance.

Avant de commencer

Rôle requis : admin

Important :
À partir de cette Washington DC version, Database Encryption ne sera plus disponible. Cloud Encryption est la solution de remplacement pour le chiffrement des données au repos. Pour en savoir plus, consultez Chiffrement dans le cloud avec Key Management

Pourquoi et quand exécuter cette tâche

La rotation de clé 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, Government Community Cloud (GCC), France et Singapour.

Procédure

Contact Service et assistance client pour demander l'une des actions de rotation clés suivantes :

- Inscrivez-vous pour effectuer une rotation annuelle de clés sur toutes les instances désignées.
- Obtenez un rapport historique des trois dernières rotations clés contenant les éléments suivants :
  - 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

Database Encryption with Customer-Controlled Switch (DBE with 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 :
À partir de cette Washington DC version, Database Encryption ne sera plus disponible. Cloud Encryption est la solution de remplacement pour le chiffrement des données au repos. Pour en savoir plus, consultez Chiffrement dans le cloud avec Key Management

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 la fonctionnalité. La base de données chiffre les données au fur et à mesure qu'elles sont écrites sur le disque et déchiffrées par la base de données au fur et à mesure de leur lecture. 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 Tablespace Encryption ou Transparent Data Encryption. Pour plus d'informations sur la technologie, reportez-vous au site Web MariaDB sous « Tablespace Encryption ».

DBE-CCS vous demande de configurer un point de terminaison de service REST HTTPS qui fournit périodiquement la clé secrète à 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 à votre disposition pour mettre en œuvre votre point de terminaison client à votre place. Contactez directement le partenaire technologique pour plus de détails sur l'intégration. Pour en savoir plus, consultez Utilisation de Fortanix Data Security Manager avec ServiceNow .

Prise en charge de plusieurs ServiceNow versions

> **Important :**
> Database Encryption est une offre d'infrastructure payante indépendante de la version. Elle peut être appliquée à n'importe quelle version prise en charge et aux instances nouvelles ou existantes.

Autres références

Reportez-vous à ces références pour plus d'informations sur DBE avec CCS :

Référence	Description
KB0993681	Architecture du commutateur contrôlé par le client de chiffrement de base de données
KB0789788	Guide de mise en œuvre de DBE avec CSC

> **Remarque :**
> Pour accéder aux articles de la base de connaissances, vous devez d'abord vous authentifier dans Now Support.

Chiffrement intégral du disque

Le chiffrement complet du disque (FDE) applique le chiffrement à l'ensemble du système de stockage au sein du serveur de base de données uniquement, car il s'agit du seul composant de stockage des données client. FDE protège uniquement contre la perte physique ou le vol des périphériques de stockage. Lorsque des serveurs à disque chiffrés sont alimentés 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 des appareils de stockage peuvent également être un facteur dans son choix.

De ce point de Now Platform vue, toutes les données sont déchiffrées.

Les environnements commerciaux utilisent le chiffrement complet du disque (FDE) avec du matériel ou des périphériques de stockage validés par FIPS 140 qui sont en cours de validation, ainsi qu'une ServiceNow option matérielle dédiée (coût supplémentaire). FDE s'applique au matériel lui-même et fournit donc un chiffrement au repos pour toutes les données stockées dans chaque instance qui vous est attribuée.

Pour plus de détails sur la sélection des options FDE et matérielles dédiées, contactez votre ServiceNow représentant.

Chiffrement Edge

ServiceNow® Chiffrement Edge ™ chiffre les données sensibles dans les locaux de votre entreprise avant de les envoyer sur Internet à votre ServiceNow instance (chiffrées en vol), où elles resteront chiffrées au repos.

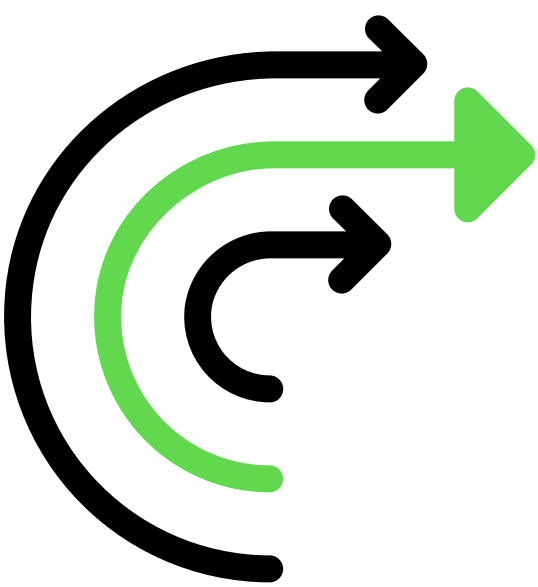
Explorer

Découvrez les fonctionnalités et la valeur commerciale d'Edge Encryption.

Plan

Découvrez comment planifier Edge Encryption.

Installer



Mise à niveau d'Edge Encryption

Référence de mise à niveau

Traduction automatique

Installez Edge Encryption.

Découvrez comment mettre à niveau Edge Encryption.

Configurer

Découvrez comment configurer Edge Encryption.

Traduction automatique

Explorer Chiffrement Edge

Chiffrement Edge est un système de chiffrement 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 utilisateur bidirectionnel passe par des proxys gérés sur votre infrastructure. Vous avez le contrôle total sur la gestion de vos clés, car les clés sont stockées dans votre proxy sur votre infrastructure. Ils Now 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 de vos clés. Chiffrement Edge utilise une application proxy, fournie et ServiceNow installée par vous au sein de votre propre réseau. Cette application proxy tokenise les modèles 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 déchiffre également les mêmes données, encore une fois uniquement au sein de votre propre réseau, à l'aide de clés stockées uniquement au sein de 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 chiffrées à partir du moment où elles quittent votre environnement et ne sont déchiffrées qu'à la récupération. À aucun moment, les données ne sont accessibles en 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 des 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 de 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 d'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 tokenisation

Chiffrement Edge prend en charge à la fois le chiffrement (via des configurations de chiffrement) et la tokenisation (via des modèles de chiffrement) comme moyen de protéger 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.

En plus des 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

Remarque :

Si un champ Journal marqué pour le chiffrement est ajouté au flux d'activité, toutes les entrées de l'utilisateur dans ce 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.

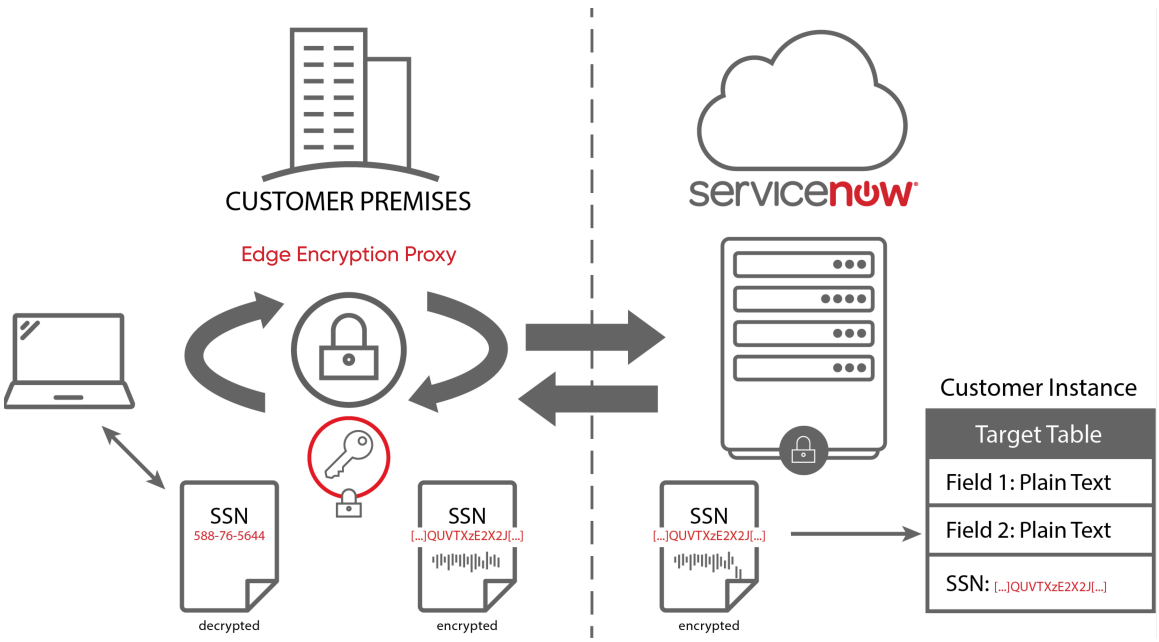
Vous pouvez également chiffrer les types de variables de catalogue de services suivants :

- 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

Modèles de chiffrement

Vous pouvez utiliser des modèles de chiffrement pour tokeniser des chaînes qui correspondent à des modèles réguliers tels que des 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 a besoin d'une base de données MySQL dans votre réseau uniquement si vous utilisez un chiffrement préservant l'ordre ou des modèles de chiffrement. Les valeurs en 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.



Chiffrement Edge on the Now 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 qui sont marquées pour le 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 Entreprise de Chiffrement au niveau des colonnes le chiffrement au niveau des colonnes, Chiffrement Edge impose certaines limitations fonctionnelles au sein d'une instance en raison de la sécurité supplémentaire. Toutefois, le proxy Edge local fournit également des fonctionnalités supplémentaires relatives au tri par rapport au chiffrement au niveau des colonnes.

Avantages:

- Chiffrement Edge fournit 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 chiffrées.
- Les informations sont chiffrées en transit, avant même qu'elles n'atteignent 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 fournit le chiffrement standard, la préservation de l'égalité et la préservation de l'ordre des données au repos au sein de la base de données et de l'instance.
- Les règles de chiffrement vous permettent d'écrire des scripts personnalisés qui indiquent précisément au serveur proxy ce qu'il faut chiffrer et où placer ces informations chiffrées dans l'instance. Ces scripts sont utiles lorsque la structure des données ne correspond pas exactement à l'instance ServiceNow .
- Les modèles de chiffrement vous permettent de tokeniser 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 s'avérer complexe et prendre beaucoup de temps.
- Vous pouvez conserver un maximum de deux clés, sans la 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 plate-forme ne peut pas déchiffrer les données pour effectuer une manipulation des données déchiffrées. Par conséquent, les fonctionnalités et le traitement des données sur le Now Platform peuvent être limités lors du chiffrement des colonnes avec Edge Encryption.

À savoir avant de commencer

Étant donné que le chiffrement et la tokenisation modifient la nature de vos données, ils Chiffrement Edge peuvent affecter d'autres processus d'instance. Avant d'utiliser Chiffrement Edge, examinez attentivement l'impact sur votre instance.

Étant donné que le serveur proxy est installé et maintenu dans votre réseau, Chiffrement Edge il nécessite une administration et une gestion réseau. Passez en revue la configuration réseau requise pour assurer une implémentation sans heurts.

Passez en revue les rubriques suivantes pour comprendre l'impact d'Edge Encryption sur votre instance :

- Planification pour Edge Encryption
- Chiffrement Edge Configuration requise
- Dimensionnement de votre environnement Edge Encryption
- Calculer la taille de la base de données de conservation de l'ordre et de tokenisation
- Chiffrement Edge Limitations
- Gestion des clés pour Edge Encryption

Composants Chiffrement Edge

Chiffrement Edge se compose du serveur proxy qui s'exécute Chiffrement Edge 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.

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 les éléments qui doivent être chiffrés, le cas échéant, et les chiffre avant de transmettre la demande à l'instance. Pour le déchiffrement, le Chiffrement Edge serveur proxy examine les réponses HTTP pour toutes les 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 incluent 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 sur votre réseau. Tous les serveurs proxy de votre réseau doivent utiliser la même base de données.

La base de données proxy contient les tables suivantes.

Tables de bases de données proxy

Nom	Description
db_id	ID unique de la base de données
edge_token_map	Données du 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 toute perte de données, sauvegardez votre base de données proxy conformément aux ServiceNow recommandations.

- Sauvegardez votre base de données toutes les 24 heures.
- Conservez les fichiers journaux binaires de base de données MySQL pendant au moins deux jours. Une fois qu'une sauvegarde a été restaurée, utilisez le journal binaire pour régénérer toutes les données perdues depuis la sauvegarde la plus récente.

Chiffrement Edge Maîtres d'ouvrage

Chiffrement Edge utilise trois clients pour informer l'instance que le proxy est en cours d'exécution, pour synchroniser les demandes entre le proxy et l'instance et pour transmettre toutes les demandes de l'utilisateur final à l'instance après tout chiffrement potentiel.

Client	Description
client heartbeat/keepalive	Chargé d'envoyer une demande à l'instance ServiceNow toutes les 5 secondes pour faire savoir à l'instance que ce proxy est en cours d'exécution. Les demandes pilotent le champ last_response_on de la table proxy Edge et, par conséquent, déterminent l'état du proxy. Si votre système rencontre des problèmes lors de l'envoi des demandes, ou si le traitement de la demande ou de la demande est retardé, l'instance peut marquer le proxy comme ne répondant pas, même si les autres clients (y compris celui du trafic utilisateur) sont opérationnels. Ce client contrôle également l'état en ligne du proxy sur l'instance. La *edgeencryption.proxy.keepalive.interval* propriété contrôle la fréquence d'interrogation pour ce client. La valeur par défaut est 5 (secondes).
Client d'interrogation/de synchronisation	En charge de diverses demandes que le proxy envoie à l'instance pour la synchronisation sur la configuration Edge Encryption (par exemple, la table, la colonne ou la pièce jointe à chiffrer, les clés, les tâches, les règles et les modèles de tokenisation). La *edgeencryption.config.poll.interval* propriété contrôle la fréquence 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 de trafic par défaut/utilisateur	Pour tout le reste, ce client gère toutes les demandes de l'utilisateur final et les transmet à l'instance ServiceNow après tout chiffrement potentiel. Ce client gère également les réponses de l'instance, en les transmettant à l'utilisateur final après tout déchiffrement potentiel.

Gestion des clés pour Edge Encryption

Vous êtes responsable de la fourniture et de la gestion des clés de chiffrement utilisées par Chiffrement Edge.

Cette rubrique se réfère aux clés du Chiffrement Edge produit. Si vous recherchez des informations sur Key Management Framework, qui peut être utilisé avec Column Level Encryption, consultez Key Management Framework.

Lors de l'obtention et de la création de clés de chiffrement pour prendre en charge les types de chiffrement utilisés par Chiffrement Edge, tenez compte des éléments suivants :

- Indique s'il faut utiliser 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.
- Indique s'il faut utiliser le système de fichiers, Java KeyStore ou Enterprise Key Management (EKM).
- Quand alterner les clés de chiffrement.
- Quand et si une tâche de chiffrement en masse doit être utilisée pour chiffrer à nouveau les 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, ajoutez une nouvelle clé de chiffrement et planifiez 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 d'un système de fichiers auquel le Chiffrement Edge proxy a accès. 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 magasin de clés Java est protégé par un mot de passe, il est donc plus sûr que le stockage des clés dans un fichier du magasin de fichiers. Un seul magasin de clés Java 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 à l'aide des systèmes de gestion des clés SafeNet KeySecure ou Unbound Technology.

Le Chiffrement Edge proxy est livré 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 KeyStore Java JCEKS du système de base, vous devez importer la clé publique dans votre magasin de ServiceNow clés. L'alias de clé publique est *`servicenow`*.

En plus des clés de chiffrement, le KeyStore 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.

Gestion des versions des clés SafeNet pour Edge Encryption

Utilisez la gestion des versions de clés SafeNet pour simplifier le changement de clés. Au lieu de créer un alias pour chaque nouvelle clé, la gestion des versions des clés SafeNet conserve le même alias et incrémente la version.

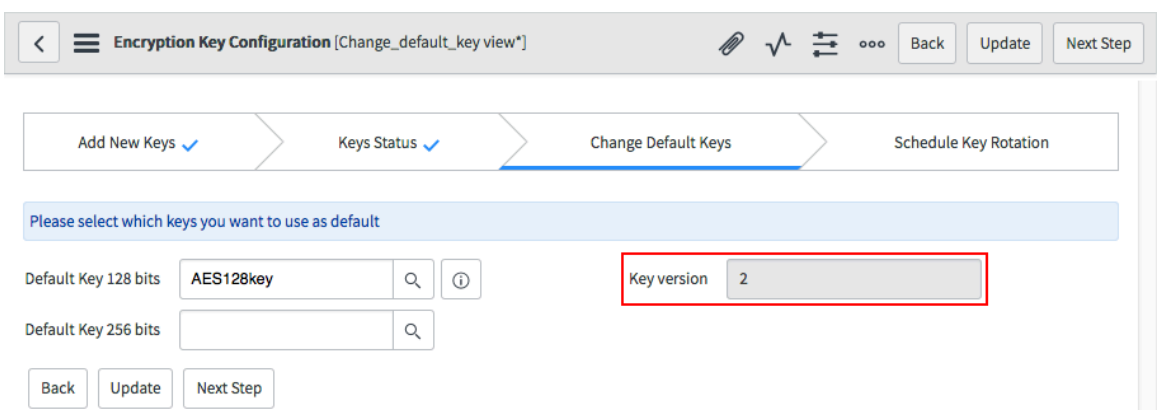
Vous devez configurer la gestion des versions des clés dans SafeNet avant de pouvoir configurer la gestion des versions des clés SafeNet sur le serveur proxy Edge.

Remarque :
Les proxys Edge installés avant la London version prennent en charge les clés SafeNet, mais pas la gestion des versions des clés SafeNet. Si vous utilisez par erreur une clé versionnée sur un proxy ou une Kingston version antérieure, lorsque vous effectuez une mise à niveau vers une version antérieure ou ultérieure, le proxy ou une London version ultérieure détecte ce problème et, pour éviter toute London perte potentielle de données, le proxy ne démarre pas.

Vous devez d'abord planifier une tâche de rotation de clé en masse ou une tâche de rotation de clé unique pour remplacer l'ancienne clé versionnée SafeNet par une clé non versionnée, 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 128 bits et 256 bits par défaut. **Les** champs de version de clé sont grisés et ne peuvent pas être modifiés.

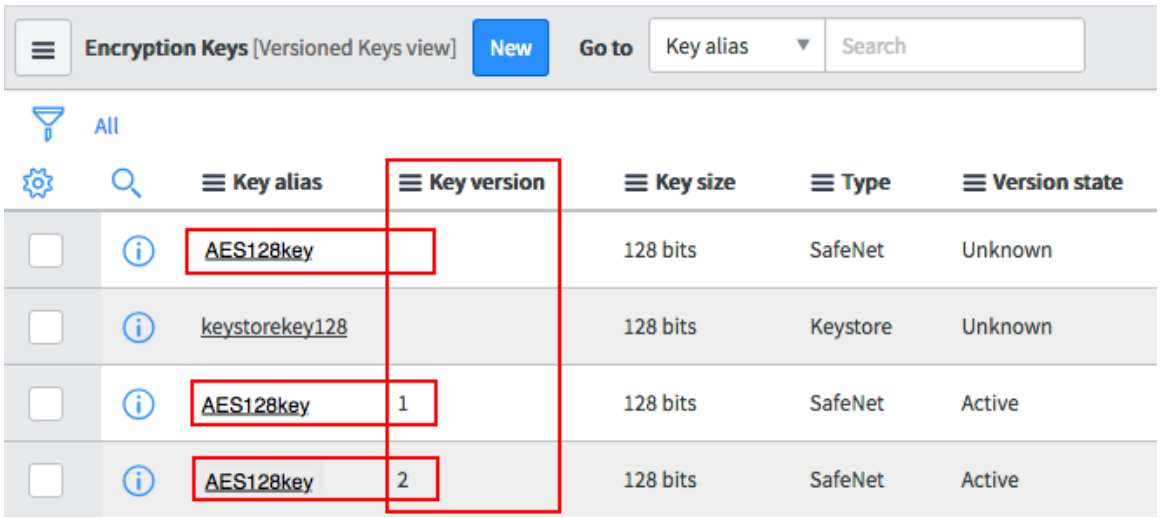


Pour plus d'informations sur les procédures, reportez-vous à la section Configurer les clés de chiffrement sur l'instance.

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



Un numéro de version n'apparaît pas pour les entrées initiales que vous effectuez dans la section Changer 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 la **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 à partir de SafeNet, de nouvelles lignes sont ajoutées pour enregistrer la **version de clé** actuellement utilisée.

Configurations et modèles 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 politique de juridiction de force illimitée 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 suivantes.

Chiffrement standard

La valeur chiffrée d'un champ est différente chaque fois que le champ est chiffré, même lorsque la valeur du champ reste la même. Le chiffrement standard est la forme de chiffrement la plus robuste. Les champs utilisant un 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.

Remarque :
Lorsque le chiffrement préservant l'égalité est sélectionné pour un champ qui contient déjà des données, l'exécution d'une action Regrouper par sur le champ peut ne pas regrouper les champs ayant la même valeur si l'un est chiffré et l'autre non.

Chiffrement 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, le regroupement par opérations et la possibilité de trier les données. Le type de chiffrement préservant l'ordre n'est pris en charge que s'il existe une base de données MySQL configurée pour le Chiffrement Edge serveur proxy.

Remarque :
Lorsque vous utilisez le chiffrement préservant l'ordre et que la base de données proxy est indisponible, des mises à jour peuvent être effectuées sur les 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 sera 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 dans Qualité de sécurité décroissante.

Type de chiffrement	Description
AES 256 standard	Les champs ne peuvent pas être filtrés, triés ou comparés.
AES 128 standard	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.

Modèles 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 en texte clair est stockée dans la base de données proxy et remplacée sur l'instance par un jeton. Utilisez des modèles de chiffrement pour tokeniser les 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.

Remarque :
Le Chiffrement Edge serveur proxy a besoin d'une base de données MySQL dans votre réseau uniquement si vous utilisez un chiffrement préservant l'ordre ou des modèles de chiffrement. Les valeurs en 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 modèles de chiffrement

Installé avec Edge Encryption

Chiffrement Edge installe les tables pour stocker les données relatives au chiffrement, les 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 de 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 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 des tâches 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 tâches planifiées pour le chiffrement, le déchiffrement, la rotation de clés, la réparation des jetons de commande et la récupération de 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 attributs de clé disponibles.

Clé de chiffrement de proxy [sys_encryption_proxy_key]

Répertorie les clés de chiffrement de proxy.

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

Une liste de caractères interdits 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 autorisée du motif. Autoriser des modèles plus petits signifie trouver plus de correspondances, ce qui augmente les frais généraux.

- **Type** : nombre
- **Valeur par défaut** : 5
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.journalisation.destination

Endroit où les messages sont consignés.

- **Type** : chaîne
- **Valeur par défaut** : fichier
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.journalisation.verbosité

Le niveau de journalisation à utiliser.

- **Type** : chaîne
- **Valeur par défaut** : info
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.encryption.proxy.buildtag

La version du proxy enregistrée auprès de votre instance.

- **Type** : chaîne
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.cleartext.allowed

Si la valeur est vrai, autorise l'enregistrement 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 définie sur false, le système empêche l'enregistrement du texte clair dans un champ chiffré.

- **Type** : booléen
- **Valeur par défaut** : faux
- **Emplacement** : table Propriétés système [sys_properties]

Planification pour Edge Encryption

La mise en œuvre réussie de nécessite une Chiffrement Edge planification et une préparation.

Répondez aux questions suivantes au cours de la phase de planification.

- Quels champs doivent être chiffrés ?
- Quels types de chiffrement doivent être utilisés ?
- Combien de Chiffrement Edge proxys sont nécessaires ? Consultez la section Dimensionnement de votre environnement Edge Encryption pour obtenir des recommandations et des éléments à prendre en considération.
- Si un ordre préservant le type de chiffrement ou les modèles de chiffrement doivent être utilisés, 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 la mise en œuvre Chiffrement Edgede .

- Les administrateurs système doivent avoir le rôle d'administrateur de sécurité. L'administrateur système doit :
  - Téléchargez l'application Chiffrement Edge proxy.
  - Configurez un Chiffrement Edge compte d'utilisateur que les proxys doivent utiliser pour se connecter à l'instance. Le rôle 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.
  - Moniteur Chiffrement Edge.
  - Créez et modifiez des règles de chiffrement.
- Votre administrateur réseau doit :
  - Installez l'application Chiffrement Edge proxy.
  - Connaître les adresses réseau des serveurs proxy et la base de données proxy utilisée pour le chiffrement préservant l'ordre et les modèles de chiffrement.
  - 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.
  - Effectuer la gestion des clés 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 pools et les paramètres des équilibreurs de charge.
- Votre administrateur de sécurité doit déterminer les types de chiffrement à affecter à chaque champ.

Chiffrement Edge Configuration requise

Vous pouvez exécuter l'application proxy sur des serveurs ou des ordinateurs virtuels Chiffrement Edge fonctionnant sur les systèmes d'exploitation Microsoft Windows ou Linux. Pour des performances optimales, assurez-vous que votre configuration répond à ces exigences.

Configuration requise pour Java

L'ordinateur hôte qui installe ou exécute le Chiffrement Edge serveur proxy doit disposer d'une version prise en charge de Java. Les versions actuellement prises en charge sont Java 11.0.6 ou ultérieure dans la série de versions 11.x

Remarque :
Java 8 n'est plus pris en charge à compter de cette Utah version. Mettez à niveau votre environnement avec le Chiffrement Edge proxy vers Java 11 avant de tenter d'installer la Utah version du Chiffrement Edge proxy.

Remarque :
Java n'autorise pas automatiquement un nombre illimité de clés de force. Vous devez spécifiquement activer l'utilisation du chiffrement AES 256 bits.

Prise en charge d'OpenJDK

Il prend en charge la version 11 d'OpenJDK Now 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 qu'il utilise 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 cette London version.

- Processeur de 3 GHz ou plus (processeur à 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 pour le basculement. Consultez Dimensionnement de votre environnement Edge Encryption pour plus d'informations.
- Possibilité d'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 :

Système pris en charge	Description
Windows Server 2012, 2012-R2, éditions 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 pour CentOS est `yum install glibc.i686`.

Exigences de 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 à de nouvelles fonctionnalités et à des corrections de bogues importantes.

Besoins de connexion au serveur proxy

Le serveur proxy qui exécute l'application Chiffrement Edge doit être en mesure de communiquer avec les machines de votre réseau. Assurez-vous que le serveur proxy dispose des privilèges réseau suivants :

Privilège réseau	Description
Accès par pare-feu	Configurez tous 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 DMZ, vous devrez peut-être déployer un serveur proxy sur une machine dans la 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 qui peuvent 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 de serveurs proxy pour autoriser le trafic sur le port TCP 443.

Privilège réseau	Description
Compte réseau	Installez le serveur proxy auprès d'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 de configurer 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 les données chiffrées, sans avoir à déchiffrer les données au préalable. 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 la base de données est la suivante :

Base de données MySQL	Besoin
Version	Base 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 du support.
Systèmes d'exploitation	Systèmes 64 bits
Processeur	Processeur de 2 GHz ou plus (processeur à 4 cœurs préféré pour des performances optimales)
RAM	16 Go
Disque	Réseau de zone de stockage (SAN) 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 conservation de l'ordre et de tokenisation.
Configuration	Cluster 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

Choisir le nombre de serveurs proxy pour votre environnement est une tâche importante. Tenez compte du nombre d'utilisateurs, des besoins en redondance et de la latence acceptable.

Redondance

Conservez des serveurs proxy redondants en cas de défaillance matérielle. Les serveurs proxy doivent être situés derrière un équilibreur de charge pour fournir un chemin fonctionnel à tous les utilisateurs si un serveur proxy est inaccessible. Assurez-vous au minimum que deux serveurs proxy sont toujours disponibles.

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 en masse réguliers sont exécutés, ajoutez des serveurs proxy supplémentaires pour gérer la charge ou exécutez les chiffrements en masse lorsque la charge utilisateur est faible. En outre, le matériel sur lequel le serveur proxy s'exécute influence les performances et la latence. Les serveurs proxy s'exécutant sur du matériel doté de processeurs plus rapides, d'un plus grand nombre de processeurs et de plus de RAM ont un débit plus élevé que les systèmes plus lents et limités.

Les directives suivantes supposent que votre serveur proxy s'exécute avec au moins 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 tous les 500 utilisateurs simultanés.
- En fonction de la redondance souhaitée, ajoutez des serveurs proxy supplémentaires pour le basculement.

Par exemple, pour une instance avec 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 placerez 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, répartissez 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 requêtes au serveur proxy avec le moins de connexions actives, empêchant ainsi la surcharge d'un seul proxy.

Utilisation du processeur

Étant donné que le chiffrement et la tokenisation des données sont des opérations gourmandes en ressources processeur, les pics de CPU lors du chiffrement des données sont normaux et attendus. Lorsque l'utilisation du processeur est supérieure à 80 % pendant plusieurs minutes d'affilée, 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 la réduire.

Mémoire

Le serveur proxy doit disposer d'un minimum de 4 Go de RAM (6 Go recommandés). Définissez les limites de mémoire initiales et supérieures du serveur proxy sur les paramètres recommandés.

Calculer la taille de la base de données de conservation de l'ordre et de tokenisation

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 de l'enregistrement.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Utilisez une machine dédiée pour exécuter la base de données de conservation 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 permettre 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 modèles de chiffrement, effectuez les étapes 1 et 2 pour les enregistrements jetonisés et ajoutez le résultat au total.

Résultats
La valeur calculée est la taille recommandée en octets pour votre base de données de conservation des commandes 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 des types de champs

Vous pouvez chiffrer uniquement 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

Vous ne pouvez pas chiffrer les types de champs suivants :

- Champs de choix
- Champs virtuels
- Champs des tables système, à l'exception de certains champs dans sys_user

- Champs système dans les tables
- Champs de numérotation ou champs 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 **Aller à et Filtre d'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, consultez Types de champs .

Restrictions de filtrage et de recherche

Chiffrement standard

Lorsque vous sélectionnez un champ Chaîne, Date, Date/Heure ou URL avec une configuration de champ chiffré standard comme opérande de 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 de gauche dans un filtre, les opérateurs suivants sont disponibles :

- **est**
- **n'est pas**
- **est vide**
- **n'est pas vide**

Chiffrement préservant l'ordre

Lorsque vous sélectionnez un champ de chaîne avec une configuration de champ chiffré préservant l'ordre comme opérande de 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**

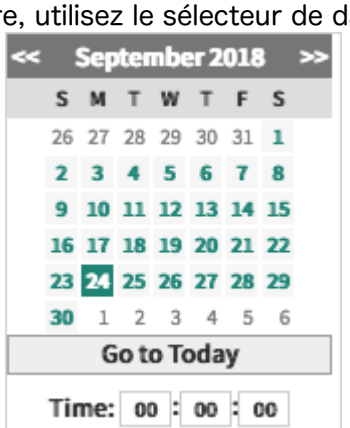
Lorsque vous sélectionnez un champ Date ou Date/Heure avec une configuration de champ chiffré préservant l'ordre comme opérande de gauche dans un filtre, les opérateurs suivants sont disponibles, en plus de **est**, **n'est pas**, **est vide** et **n'est pas vide** :

- **après**
- **avant**
- **après ou le**
- **avant ou sur**

Sélecteurs de date et de date/heure

Pour les champs Date, utilisez le sélecteur de date pour spécifier la date :

Pour les champs 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 conditions est pris en charge dans des scripts tels que les politiques d'interface utilisateur et les règles métier.

Restrictions de configuration

Restrictions et comportement des configurations de chiffrement :

- Après avoir ajouté un champ à la Chiffrement Edge table de configuration, vous ne pouvez pas supprimer l'enregistrement de configuration. Si vous ne souhaitez plus qu'un champ soit chiffré, 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 pour être 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.
- Si un champ hérité d'une table parente est marqué pour être chiffré, le champ de la table parente ne peut pas être chiffré. Par exemple, si la **brève description** de la table Incident est marquée comme étant chiffrée, la **brève description** de la table Tâche ne peut pas être chiffrée. Dans cet exemple, vous pouvez chiffrer la **brève description** 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'elles sont exportées 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 de colonne** , et vous ne pouvez pas créer de configurations de chiffrement de date ou de date/heure pour ces champs.
- Vous pouvez chiffrer un champ Chaîne ou URL uniquement 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 chiffrées avec un chiffrement préservant l'égalité ou l'ordre passent toujours les contrôles d'équivalence lorsqu'elles sont comparées à une valeur chiffrée 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 des données chiffrées et en texte clair, les résultats peuvent différer de ceux attendus.
- Les données chiffrées ne peuvent pas être copiées-collées dans un enregistrement dont 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 regrouper, de trier et de rechercher peut être affectée. En règle générale, plus le chiffrement 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.
- 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, la AL32UTF8 Unicode 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.

Installation d'Edge Encryption

Vous pouvez installer un Chiffrement Edge proxy manuellement ou à l'aide du programme d'installation Chiffrement Edge interactif.

Configuration requise pour Java

L'ordinateur hôte qui installe ou exécute le Chiffrement Edge serveur proxy doit disposer d'une version prise en charge de Java. Les versions actuellement prises en charge sont Java 11.0.6 ou ultérieure dans la série de versions 11.x

Remarque :
Java 8 n'est plus pris en charge à compter de cette Utah version. Mettez à niveau votre environnement avec le Chiffrement Edge proxy vers Java 11 avant de tenter d'installer la Utah version du Chiffrement Edge 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, procurez-vous un certificat de serveur et importez-le dans le Java KeyStore.
- Configurez votre magasin de clés et votre clé de chiffrement.
- Si vous devez utiliser des types de chiffrement ou des modèles de chiffrement préservant l'ordre, configurez une base de données MySQL sur un ordinateur 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 qui Chiffrement Edge peut traiter les demandes provenant de ce serveur proxy.

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'aide de l'adresse suivante : `http://hostname.mycompany.com:8081/`.

Remarque :
Les paramètres DNS et les règles de routage peuvent être utilisés. Les valeurs d'hôte et de port sont déterminées par votre administrateur réseau.

Demander Edge Encryption

Le Chiffrement Edge module d'extension (com.glide.edgeencryption) est disponible sous forme d'abonnement distinct.

Avant de commencer

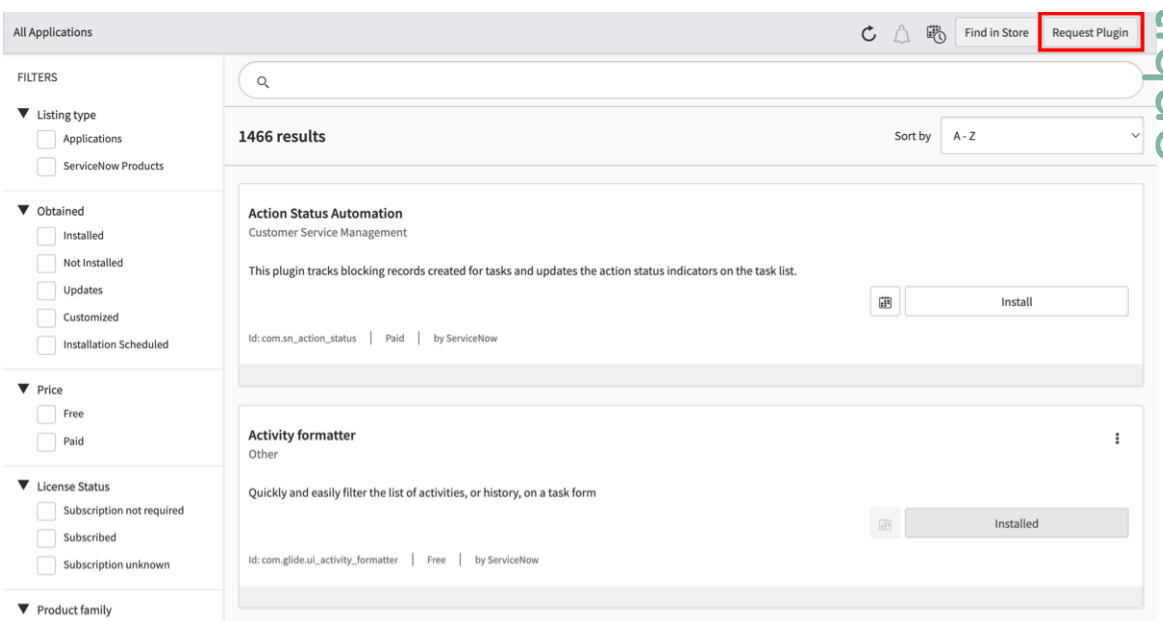
Pour acheter un abonnement, contactez votre chargé de clientèle ServiceNow. Le chargé de clientèle peut faire en sorte que le module d'extension soit activé sur les instances de production et de sous-production de votre organisation, en général en quelques jours à peine.

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.

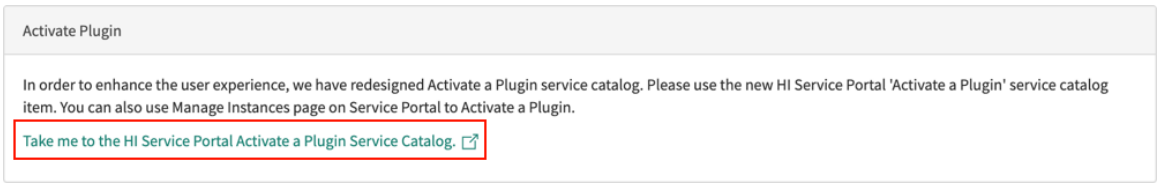
Rôle requis : aucun

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.



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.

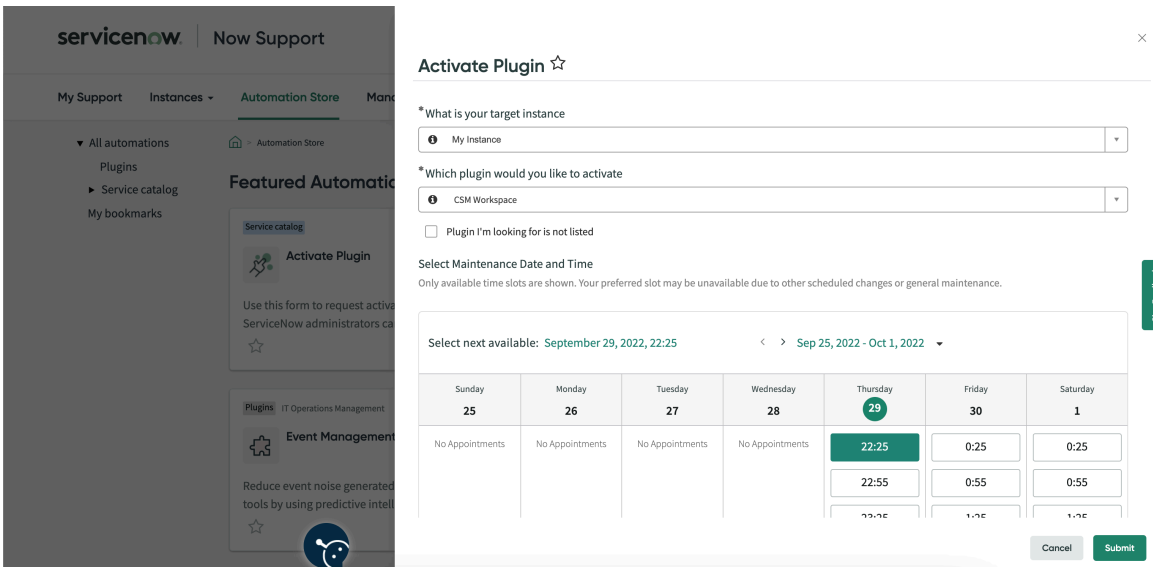
Formulaire Activer le module d'extension

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.

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 Service Catalog [KB0751715] de la Now Support Base de connaissances.

Configurer un compte d'utilisateur Chiffrement Edge

Les Chiffrement Edge proxys se connectent à l'instance en tant qu'utilisateurs pour obtenir et mettre à jour les informations de configuration de chiffrement. Créez un compte d'utilisateur à cet effet et attribuez le rôle de edge_encryption à l'utilisateur.

Avant de commencer

Le Chiffrement Edge module d'extension doit être installé avant que vous puissiez affecter le rôle.

Rôle requis : admin

Procédure

1. Sur votre ServiceNow instance, créez un compte d'utilisateur à utiliser par les Chiffrement Edge applications proxy.
2. Affectez le rôle edge_encryption à l'utilisateur.

Télécharger le serveur proxy Edge Encryption

Téléchargez l'application de serveur Chiffrement Edge 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.

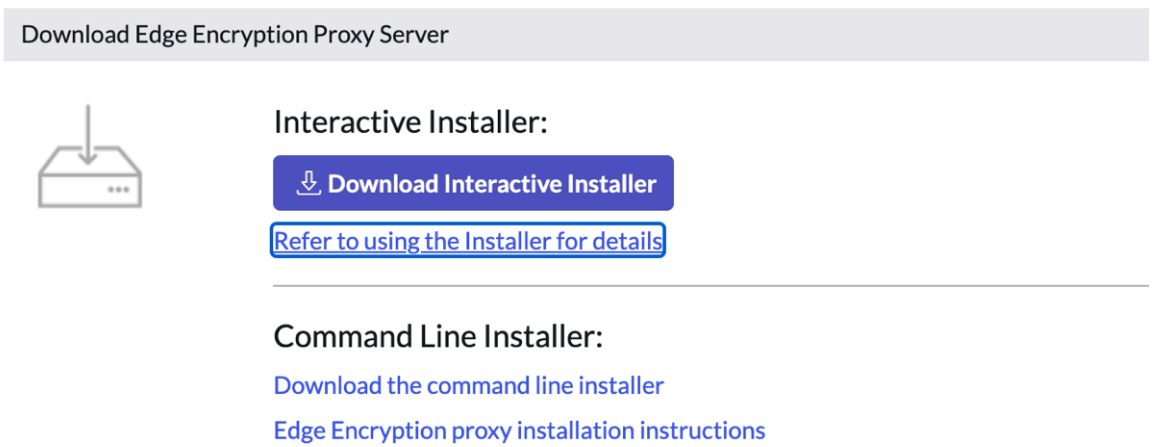
Rôle requis : security_admin

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 l'exécution du serveur proxy nécessite au moins 4 Go de mémoire, les environnements JRE 32 bits et les systèmes d'exploitation 32 bits ne sont plus pris en charge à partir de cette Washington DC version.

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 Edge Encryption à l'aide du programme d'installation interactif. En cas d'installation manuelle, Installez le serveur proxy Edge Encryption à l'aide du programme d'installation de ligne de commande.

Installer le serveur proxy Edge Encryption 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 :
SafeNet KeyLes fichiers du magasin de clés sécurisés ne sont pas pris en charge par le programme d'installation Chiffrement Edge . Pour utiliser un keystore SafeNet KeySecure, Installez le serveur proxy Edge Encryption à l'aide du programme d'installation de ligne de commande.

Le module d'extension Chiffrement Edge doit être installé et activé sur votre instance avant de démarrer cette procédure. Assurez-vous que Java version 11.0.6 ou ultérieure est installé 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 du service avec accès complet au système de fichiers sur un hôte Linux

Pourquoi et quand exécuter cette tâche

Après l'installation d'un nouveau serveur proxy, vous pouvez exécuter à nouveau le programme d'installation pour effectuer des tests afin de détecter les problèmes d'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 root 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 fonctionnalité 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 vous y êtes invité par le programme d'installation, fournissez 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 racine.

Procédure

Utilisez le programme d'installation pour installer plusieurs proxys pour votre instance sur plusieurs machines, en vous assurant que les critères suivants s'appliquent :

- Tous les proxys doivent disposer des mêmes clés de chiffrement et de la même paire de clés RSA utilisée pour signer numériquement les configurations et les règles de chiffrement.
- La clé de chiffrement doit être la clé configurée par défaut 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, consultez Configurer un hôte Windows 64 bits pour utiliser NVDA 32 bits avec des applications Java .

Après l'installation du Chiffrement Edge serveur proxy, définissez la limite de mémoire initiale et la limite supérieure de mémoire du serveur proxy.

Installer le serveur proxy (programme d'installation Chiffrement Edge 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 Edge Encryption.
2. Ouvrez le programme d'installation du Chiffrement Edge proxy.

> **Remarque :**
> En cas d'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`.

Programme d'installation du proxy ServiceNow Edge Encryption

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 entrez 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**.

Paramètre	Description
Hôte proxy	Nom de domaine complet de l'ordinateur sur lequel vous installez le serveur proxy. **Remarque :** Cliquez sur **Détecter le nom de domaine complet** pour rechercher le nom de domaine complet de l'ordinateur et renseigner 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, le proxy n'a que 5 secondes pour être informé des modifications de la configuration de chiffrement. Plus les valeurs sont élevées, plus l'instance met de temps à détecter les proxys mis en ligne.

Paramètre	Description
	Remarque : La modification du paramètre par défaut de l'intervalle d'interrogation du proxy peut entraîner des retards de détection lorsqu'un proxy est mis en ligne.
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.

7. Cliquez sur **Installer**.
   Le Chiffrement Edge serveur proxy s'installe. L'installation peut prendre quelques minutes.

Configurer la protection des propriétés de CyberArk

Vous pouvez également configurer 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 dans le répertoire d'installation du client AIM. Le coffre-fort 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 AIM de CyberArk 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 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 **Passer** d'un écran CyberArk à l'autre.

Procédure

1. Sur la page Connexion CyberArk du programme d'installation Chiffrement Edge , entrez les paramètres de connexion CyberArk.

Paramètres de connexion CyberArk

Paramètre	Description
Chemin d'accès à PasswordSDK.jar	Le chemin d'accès au fichier JavaPasswordSDK.jar installé sur l'ordinateur

Paramètre	Description
	Windows hôte pendant la configuration de CyberArk.
ID d'application	**L'identifiant de l'application** saisi lors de la configuration de CyberArk.
Nom sûr	Le **nom de sécurité** 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'identification pour tous les mots de passe protégés, cochez la case **Appliquer un nom d'identification à tous les identifiants** , saisissez le nom du justificatif et cliquez sur **Appliquer**.
   - Saisissez 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 par CyberArk

Paramètre	Description
Utilisateur Chiffrement Edge	Le nom d'informations d'identification CyberArk d'un utilisateur Edge Encryption.
Magasin de clés de signature	Le nom des informations d'identification CyberArk pour le magasin de clés de signature.
Magasin de clés de certificat HTTPS	Le nom d'informations d'identification CyberArk pour le magasin de clés de certification HTTPS.
Magasin de clés de chiffrement	Le nom d'informations d'identification CyberArk du magasin de clés de chiffrement.
Base de données	Le nom des informations d'identification CyberArk pour le magasin de clés de base de données.
Magasin de clés de certificat HTTPS SafeNet	Le nom des informations d'identification CyberArk pour le magasin de clés de certification HTTPS SafeNet.
Serveur SafeNet	Le nom des informations d'identification CyberArk pour le serveur SafeNet.
Transférer proxy	Le nom des informations d'identification CyberArk du proxy direct.

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, sélectionnez le magasin de Chiffrement Edge clés sur l'ordinateur hôte pour stocker la clé de signature.
   - **Créer un 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 du 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 la clé existante** : utilisez une paire de clés RSA du magasin de clés sélectionné.
   - **Importer une clé existante** : importez une paire de clés RSA à partir d'un magasin de clés différent. Accédez au fichier du magasin de clés, saisissez 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 Chiffrement Edge serveur proxy à l'aide d'une connexion SSL sécurisée, importez le certificat HTTPS dans le serveur proxy.

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 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 du 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, saisissez 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 du 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 toutes les deux utiliser le même magasin de clés.

Si vous mettez à jour un certificat SSL sur un serveur proxy Edge, reportez-vous à la section 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. 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.

Exigences 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 de 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, reportez-vous à la rubrique Mettre à jour le certificat SSL.

Procédure

1. Sélectionnez l'emplacement de la clé de chiffrement.

2. Sélectionnez **Suivant**.

3. Sélectionnez ou créez la clé de chiffrement.

4. Sélectionnez **Suivant**.
5. **Facultatif :** Si vous souhaitez utiliser le chiffrement 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 magasin de clés Java :

   ```
   keytool -list -keystore keystore.jceks -storetype jceks -storepass MY_SUPER_PASSWORD
   ```
2. Supprimez 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 Java KeyStore.

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 base de Chiffrement Edge 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 en cours d'exécution 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.

Remarque :
Si vous utilisez 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 correspond à 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 démarrer le proxy à partir du programme d'installation.

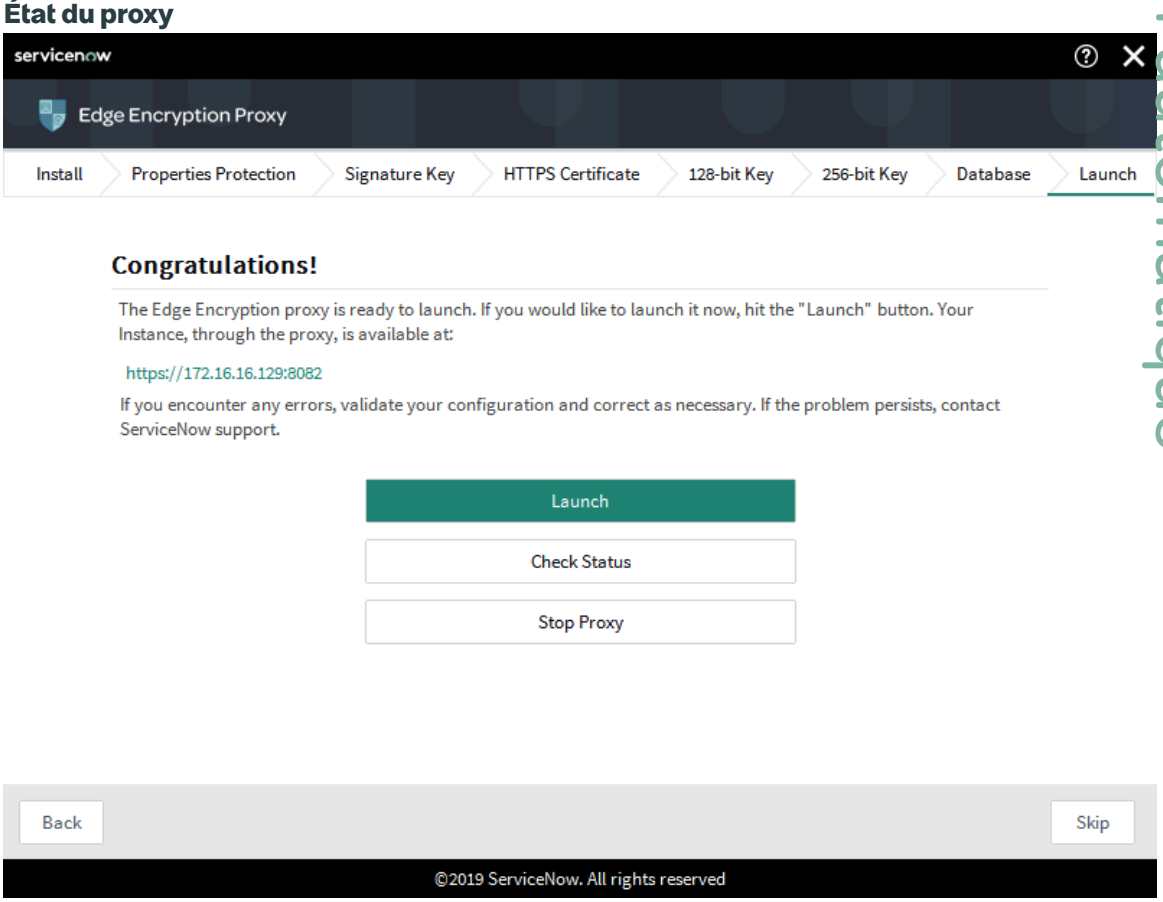
Avant de commencer

Rôle requis : admin

Procédure

1. Après avoir configuré les clés sur l'instance et la base de données proxy, revenez au programme d'installation Chiffrement Edge du proxy, puis 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.
   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 supérieure du serveur proxy.

Vérifiez et dépannez 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.

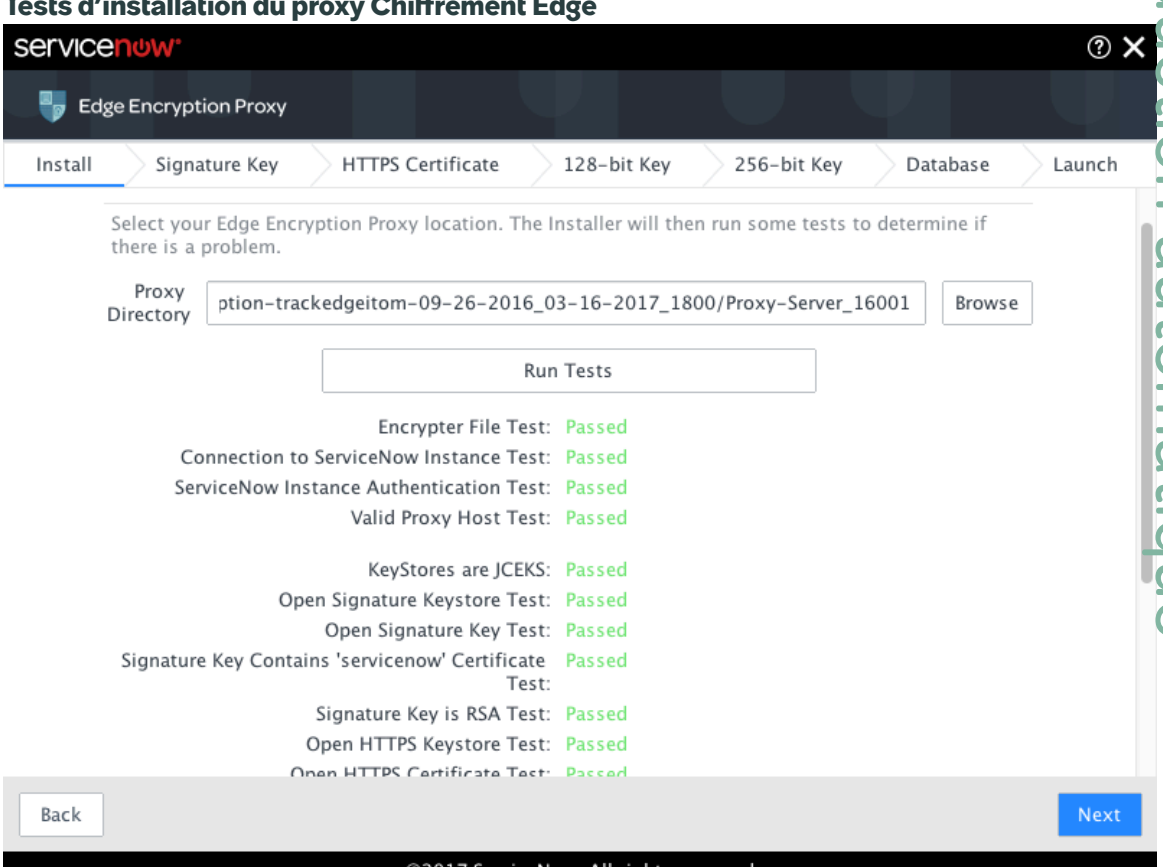
Avant de commencer

Rôle requis : admin

Procédure

1. Ouvrez le programme d'installation du Chiffrement Edge proxy.
2. Sélectionnez **Vérifier l'installation**.
3. Cliquez sur **Proxy Directory (Répertoire proxy**) et sélectionnez le répertoire proxy.
4. Cliquez sur **Exécuter les tests**.
   Les résultats des tests s'affichent.

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 **Lancer** .

Installez le serveur proxy Edge Encryption 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 un ordinateur de votre réseau si ce n'est pas déjà fait.

Remarque :
Si vous utilisez les clés de chiffrement Unbound Technology avec Chiffrement Edge, installez le serveur proxy à l'aide du programme d'installation de ligne de commande sur la machine cliente Unbound. Le Chiffrement Edge serveur proxy doit s'exécuter sur le même ordinateur que le client technologique Unbound.

Procédure

1. Configurez un Chiffrement Edge serveur proxy.
2. Vérifiez que le serveur proxy s'exécute correctement.
3. Ajoutez des serveurs proxy supplémentaires pour une instance.
   Des serveurs supplémentaires permettent d'assurer un environnement optimal. Consultez Dimensionnement de votre environnement Edge Encryption pour vous aider à déterminer le nombre de serveurs proxy supplémentaires nécessaires.

Installez le serveur proxy Edge Encryption (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

Java version 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 Edge Encryption, 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 lors du processus de mise à niveau et stocke les anciennes informations de proxy.

Lorsque vous exécutez une mise à niveau via la ligne de commande, une dist-upgrade.log peut être générée dans le répertoire dans lequel la commande s'exécute. Le dist-upgrade.log contient les journaux du processus de mise à niveau.

En cas d'échec de la mise à niveau, le système crée un répertoire failed-backup.dist-upgrade-<timestamp> . En outre, 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 proxy Chiffrement Edge 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 l'ordinateur cible et modifiez les variables en fonction de votre configuration : `java -jar edgeencryption-<version>-all.jar -m install -n <ProxyName> --instancehost <host> -p <InstancePort> --protocol https`

Option	Variable	Description
aucun	version	Numéro de version Chiffrement Edge du proxy utilisé pour effectuer l'opération en cours.
-M	Mode	Opération ou mode d'exécution (installation ou mise à niveau).
-n	Nom du proxy	Nom de l'instance du proxy de chiffrement. Utilisez un ProxyName unique pour identifier des instances de proxy spécifiques.
--instancehost	hôte	Le nom d'hôte de votre instance ServiceNow (par exemple, mycompany.service-now.com).
-p	Port d'instance	Port de votre instance. Lorsque le protocole est https, le port est normalement 443.
--Protocole	protocol	Protocole utilisé pour accéder à votre instance ServiceNow (généralement https).

Remarque :
Ne copiez pas et ne collez pas les commandes du navigateur. Parfois, les opérations de copier/coller entraînent le collage de caractères inattendus sur l'ordinateur 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.

Pour afficher l'écran d'aide, exécutez cette commande sans arguments : `java -jar edgeencryption-<version>-all.jar`

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 **Edge Encryption**.

b. Enregistrez et fermez le fichier.

c. Ouvrez l'invite de commande Windows et cd pour ServerName_port/bin.

d. Exécutez edgeencryption.bat installation.

Résultats

Le répertoire ProxyName_port est créé dans le répertoire courant. Le fichier edgeencryption.properties est mis à jour avec les valeurs d'hôte, de port et de protocole à partir 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 destinée à la signature des 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 magasin de clés Java JCEKS 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 proxy java-installation. 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.

Procédure

1. Accédez au répertoire KeyStore dans le répertoire de téléchargement du 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 :
   N'entrez 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. Passez au répertoire <installation directory>/conf/ .

   b. Ouvrez le fichier edgeencryption.properties .

   c. Saisissez les propriétés de la signature numérique.

      Ces propriétés doivent être les mêmes pour tous les proxys.

5. Enregistrez et fermez le fichier edgeencryption.properties .

Importer et configurer le certificat pour une 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 de serveur et la clé privée correspondante avant de l'ajouter au magasin de clés Java.

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 qu'elle la fasse 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.

   ```
   keytool -importkeystore -destkeystore keystore.jceks -deststoretype jceks -srckeystore
   MY_SERVER.p12 -srcstoretype pkcs12 -alias MYALIAS
   ```

   L'alias, affiché dans l'exemple sous la forme MYALIA , 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 <installation directory>/conf/ .

5. Arrêtez et redémarrez le proxy Edge.

> **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 d'un système de fichiers auquel le Chiffrement Edge serveur proxy accède 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 magasin de clés Java : ○ Stocke les clés dans un KeyStore Java JCEKS. ○ Est protégé par un mot de passe et plus sécurisé que le stockage des clés dans un fichier du 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 livré 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)	**Clé SafeNetSecure** Les clés sont stockées et récupérées à l'aide de 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 machine hôte de votre réseau avant de configurer le magasin de clés sur le Chiffrement Edge serveur proxy. **Technologie Unbound**

Magasin de clés pris en charge	Description
	La clé de chiffrement encodée 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 technologique Unbound.

Remarque :
Si vous utilisez un magasin de clés autre que le KeyStore Java JCEKS du système de base, vous devez importer la clé publique dans votre magasin de ServiceNow clés. L'alias de clé publique est *servicenow*.

2. Configurez le magasin de clés et les clés de chiffrement dans 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 livré 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. Passez au répertoire <installation directory>/conf/ .
   b. Ouvrez le fichier edgeencryption.properties .
   c. Entrez les propriétés du Java KeyStore.
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 de l'outil clé Java KeyStore.

Créer des clés de chiffrement à l'aide de l'outil clé Java KeyStore

Vous pouvez utiliser l'outil clé fourni avec la distribution du proxy de chiffrement pour créer des clés de chiffrement AES 128 bits et AES 256 bits.

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 KeyStore Java exige que le nom de l'alias (nom de la clé, alias de clé) utilise des lettres minuscules et des chiffres.

Procédure

1. Accédez au répertoire du magasin de clés, <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 keystore, *c'est-à-dire* que vous avez ignoré l'étape précédente, vous devez modifier l'option -keystore pour inclure le chemin d'accès de votre répertoire actuel au répertoire keystore. 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 à l'instance lorsque vous affectez des clés par défaut.

Remarque :
Le mot de passe de la clé doit être le même que celui du magasin de clés.

Configurer un keystore SafeNet KeySecure

Si vous utilisez un magasin de clés SafeNet, copiez un ensemble de bibliothèques dans le répertoire de distribution du proxy.

Avant de commencer
Rôle requis : admin

Vous devez installer et configurer le magasin de clés SafeNet avant d'effectuer cette étape. Obtenir 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`

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/ , puis 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 de l'authentification par certificat client, mais pas d'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 d'un 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) à l'instance lorsque vous affectez des clés par défaut.
4. Enregistrez et fermez le fichier edgeencryption.properties .

Mise à niveau de Kingston ou d'une version antérieure vers London ou une version supérieure

Si vous utilisez un serveur NAE SafeNet pour le stockage des clés avec Edge, avant de mettre à niveau le proxy d'une version antérieure Kingston ou inférieure ou London supérieure, vous devez copier les fichiers JAR ProtectApp du client Gemalto SafeNet et ajouter de nouvelles propriétés.

Avant de commencer
Rôle requis : admin

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 <installation directory>/lib vers le répertoire <installation directory>/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 <installation directory>/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. Poursuivez avec la mise à niveau vers ou une London version supérieure.

Configurer les clés Unbound Technology

Utilisez les clés Unbound Technology (anciennement sécurité dyadique) en Chiffrement Edge stockant la clé de chiffrement encodée en base64 sous forme de fichier texte sur le Chiffrement Edge serveur proxy et en fournissant l'alias de clé encapsulée. 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 encapsulée et la clé encapsulée. Utilisez l'algorithme RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING pour l'emballage et le remplissage. Exportez la clé enveloppée 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 , installez le serveur proxy à Chiffrement Edgel'aide du programme d'installation de ligne de commande sur la machine cliente Unbound. Le Chiffrement Edge serveur proxy doit s'exécuter sur le même ordinateur que le client technologique Unbound.

Procédure

1. Ajoutez la clé de chiffrement encapsulée au format texte codé en base64 dans le 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 .

a. Allez dans le 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 indique 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 Edge Encryption.

d. Annulez le commentaire des propriétés de la configuration du fournisseur Dyadic 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 encapsulée ajoutée au répertoire <proxy-installation-directory>/keys . Par exemple, si le fichier du 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 seule clé de chiffrement.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Cette étape crée à la fois le stockage de clé 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 .

a. Passez au répertoire <installation directory>/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 à l'appareil Java KeyStore ou Enterprise Key Management (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 marquées d'un **X** dans la colonne de gauche peuvent être supprimées. Les clés qui ont été utilisées par défaut ou dont **l'état** est **Disponible** 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 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 encapsulée ajoutée au répertoire <proxy-installation-directory>/keys . Par exemple, si le fichier du répertoire est nommé myunboundkey, ajoutez ce nom au champ Alias de **clé** .

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**, **Magasin de clés**, **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 des proxys ne disposent pas de 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 chargée la clé, ou au moins un proxy a échoué à charger la clé.

5. Dans la section Changer 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 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 sur **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 sont pas les 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.

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 rotation de clé unique, les données existantes restent chiffrées avec l'ancienne clé jusqu'à ce que les données soient à nouveau consultées.

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 <installation directory>/conf/edgeencryption.properties et configurez les propriétés du serveur proxy suivantes Chiffrement Edge :
   - Propriétés de la cible (instance)
   - Propriétés du compte utilisateur
   - Propriétés du proxy
   - Si vous utilisez des types de chiffrement ou des modèles de chiffrement préservant l'ordre, configurez les propriétés de base de données proxy
   - Texte clair et propriétés de l'IV statique
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 qu'il utilise 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. Passez au répertoire <installation directory>/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 du client, ajoutez ce certificat à la JVM utilisée par le Chiffrement Edge serveur proxy pour établir la confiance entre le proxy Web et le Chiffrement Edge serveur proxy.

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 supérieure du serveur proxy

Définissez la limite de mémoire initiale et la limite supérieure de mémoire 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
Par défaut, définissez la limite de mémoire initiale et la limite de mémoire de limite supérieure sur la même valeur. Sur n'importe quel ordinateur, allouez 2 Go de mémoire physique au système d'exploitation. Ensuite, allouez le reste de la mémoire physique au tas à l'aide des propriétés de limite de mémoire initiale et de limite de mémoire de limite supérieure. Par exemple, sur un ordinateur doté de 8 Go de mémoire, allouez 2 Go au système d'exploitation et allouez les 6 Go (6 144 m) restants 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 l'arrêter et le redémarrer après avoir mis à jour ces propriétés.

Procédure

1. Dans le répertoire de votre serveur proxy, ouvrez <install dir>/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>` sur le `<number>` disponible suivant dans la séquence des propriétés `wrapper.java.additional.<number>` définies dans le fichier `wrapper.conf` .

Example
Par exemple, vous disposez de la liste suivante des propriétés `wrapper.java.numéro.supplémentaire<>` :

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

Le `<nombre>` maximal dans la liste ci-dessus est **2**. Lorsque vous ajoutez la ligne `wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m` , définissez `<number>` sur **3**, le numéro disponible suivant.

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 supérieure de mémoire de limite.
Étant donné qu'aucune limite supérieure de mémoire n'est 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 supérieure de la mémoire.

Ajoutez la ligne suivante à la fin du fichier :

wrapper.java.nombre<supplémentaire>=-Xmx<max_memory_in_MB>m

Définissez <number> sur le <number> disponible suivant dans la séquence des propriétés wrapper.java.additional.<number> définies dans le fichier wrapper.conf .

Example
Par exemple, vous disposez de la liste suivante des propriétés wrapper.java.numéro.supplémentaire<> :

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

Le <nombre> maximal dans la liste ci-dessus est **2**. Lorsque vous ajoutez la ligne wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m , définissez <number> sur **3**, le numéro disponible suivant.

Remarque :
Ne laissez pas d'espaces dans la séquence de numérotation.

Définissez <max_memory_in_MB> sur le nombre de mégaoctets de mémoire restant après avoir alloué 2 Go de mémoire au système d'exploitation.

4. Enregistrez et fermez le fichier.

Example: Exemple : définition des limites de mémoire initiales et supérieures 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 démarrer le proxy 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 type de chiffrement ou des modèles de chiffrement préservant l'ordre, la base de données proxy est en cours d'exécution.

Remarque :
La première fois que vous configurez le fichier edgeencryption.properties ou que vous modifiez les propriétés, il se peut que vous ne souhaitiez pas définir la propriété de chiffrement du mot de passe. Une fois que vous avez vérifié que tout fonctionne, vous pouvez définir la propriété de chiffrement 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/bac **b.** Exécuter edgeencryption.bat démarrage

2. Vérifiez le journal sur le serveur proxy pour vérifier que le proxy est en cours d'exécution.

Brouiller 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 les mots de passe en texte clair.

Avant de commencer
Rôle requis : admin

Assurez-vous que le serveur proxy est configuré et s'exécute correctement avant de Chiffrement Edge 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. Passez au répertoire <installation directory>/conf/ .
2. Dans le répertoire conf , créez un fichier texte contenant une chaîne ou une phrase complexe qui peut être utilisée comme phrase secrète que le proxy utilise pour brouiller les mots de passe dans le fichier edgeencryption.properties .
   Cette phrase de passe doit être 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 .

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 la même machine.

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. Consultez Dimensionnement de votre environnement Edge Encryption pour déterminer le nombre de proxys supplémentaires nécessaires.

Remarque :
Assurez-vous que tous les proxys disposent des mêmes clés de chiffrement et de 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 serveur proxy (programme d'installation Chiffrement Edge 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	Le nom du serveur, l'adresse IP ou le 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 de l'ordinateur.
edgeencryption.proxy.https.port	Port sur le proxy pour la communication HTTPS. Doit être unique à tous 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.

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 qui Chiffrement Edge peut traiter les demandes provenant de ce serveur proxy.

Avant de commencer

Si un serveur proxy n'est pas authentifié, le journal de la console comprend 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 n'est pas accessible`.

Pour maintenir le proxy dans un état opérationnel pendant le processus de mise à niveau, l'authentification n'est requise qu'après la réussite de la mise à jour du proxy.

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. Lorsque l'authentification est terminée, l'état passe de **En attente** à **Authentifié,** et vous pouvez accéder au proxy et Chiffrement Edge accepter les demandes du proxy.

Remarque :
Si vous arrêtez et redémarrez le proxy, le proxy 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

Procédure

1. Arrêtez le serveur proxy.

Option	Description
Sur un ordinateur Linux	Exécuter `./shutdown.sh`
Sur un ordinateur Windows	Exécuter `edgeencryption.bat` arrêt Pour supprimer le service Windows, exécutez `edgeencryption.bat supprimez`

2. Consultez le journal sur le serveur proxy pour vérifier que le proxy s'est arrêté.

Désinstaller le proxy Edge Encryption 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 utilisant le proxy.

Le proxy de chiffrement exécuté sous Linux fonctionne comme un processus unique. Vous pouvez mettre fin à 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 Edge Encryption 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.

Avant d'arrêter le Chiffrement Edge proxy, assurez-vous qu'aucun utilisateur n'est connecté à l'instance utilisant le proxy.

Procédure

1. Vous pouvez enregistrer le fichier edgeencryption.properties avant de supprimer le répertoire de distribution.
2. Exécuter `edgeencryption.bat arrêt`
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 Chiffrement Edge serveur proxy ou l'URL d'instance. Si vous implémentez l'authentification unique (SSO) de plusieurs fournisseurs avec Chiffrement Edge l'option activée, certains utilisateurs devront peut-être se connecter à votre instance via le Chiffrement Edge serveur proxy, tandis que d'autres ne le feront pas.

Avant de commencer

- Activez le module d'extension Integration - Multiple Provider Single Sign-On Installer (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 Chiffrement Edge serveur proxy par lequel les utilisateurs se connecteront à l'aide de l'authentification unique de plusieurs fournisseurs. Pour déterminer l'URL d'un Chiffrement Edge serveur proxy, reportez-vous à la section Installation d'Edge Encryption.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

L'utilisateur qui se connecte doit utiliser l'URL appropriée pour se connecter, soit en utilisant le proxy Edge, soit en n'utilisant pas le proxy Edge.

- Si vous acheminez tous les utilisateurs via le Chiffrement Edge serveur proxy, configurez votre enregistrement de fournisseur d'identification et définissez l'URL du serveur proxy dans les champs **Page d'accueil de ServiceNow**, **ID d'entité/Émetteur** et **URI d'audience** .
- Pour acheminer certains utilisateurs via le serveur proxy et d'autres utilisateurs vers l'instance, créez deux enregistrements d'identification du fournisseur. Les deux enregistrements utilisent la même valeur dans le champ **URL du fournisseur d'identité** . Toutefois, l'un des enregistrements passe par le serveur proxy, tandis que l'autre passe par l'instance.
  - Connexion 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 du proxy Edge

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** de 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 à l'aide de 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 d'instance, remplissez le formulaire à l'aide de 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 d'installation MultiSSO.

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 **MultiSSO** .

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 les 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 la connexion d'un utilisateur via le Chiffrement Edge serveur proxy, utilisez la sys_id de l'enregistrement du fournisseur d'identité qui utilise l'URL du Chiffrement Edge serveur proxy.
- Pour configurer la connexion d'un utilisateur à l'instance, utilisez la sys_id de l'enregistrement du fournisseur d'identité qui utilise l'URL de l'instance.

URL de connexion

URL	Destination de connexion
https://<nom d'hôte du 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 d'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 les 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 de l'IV statique

edgeencryption.client.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 en clair et envoie le texte chiffré à l'instance. L'instance ne connaît pas le texte clair, et les clés ne lui sont pas envoyées non plus. Cette propriété doit être la même pour tous les proxys.
edgeencryption.encrypter.static.iv	Static IV (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>. Changez le mot de passe après avoir installé Java KeyStore.
edgeencryption.proxy.signature.keystore.keyalias	Alias de clé indiqué comme argument -alias lors de la génération de la paire de clés RSA.

Propriété du magasin de fichiers

edgeencryption.keyfile.directory	Le répertoire spécifie où les fichiers clés sont stockés. Si vous utilisez le magasin de clés Java ou un magasin

	de clés SafeNet KeySecure, laissez cette propriété en commentaire. Exemple : `edgeencryption.keyfile.directory=keys` Si vous utilisez des clés Unbound Technology, annulez le commentaire de 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 pour que le proxy apprenne les modifications de la configuration de chiffrement. Plus les valeurs sont élevées, plus l'instance met de temps à détecter un proxy hors ligne. **⚠ Avertissement :** Ne modifiez en aucun cas cette propriété. La modification du paramètre par défaut de l'intervalle d'interrogation du proxy peut entraîner des retards de détection lorsqu'un proxy est mis en ligne.
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 tâches HTTP par seconde qui peuvent être envoyées à l'instance par ce proxy.
edgeencryption.attachments.request.timeout.seconds	Délai de la demande de téléchargement 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 en aucun cas cette propriété.
edgeencryption.httpclient.request.buffer.size	Taille de la demande du client. Si la demande du client est supérieure à cette taille, l'excédent est enregistré sur le disque.

	⚠ Avertissement : Ne modifiez en aucun cas cette propriété.
edgeencryption.httpclient.header.size	Taille de l'en-tête de demande/de réponse. • Valeur minimale : 8K • Valeur maximale : 32K **⚠ Avertissement :** Ne modifiez en aucun cas 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 où le proxy envoie un ping à l'instance pour essayer de s'inscrire. Valeur par défaut : 0 (aucune limite)
edgeencryption.tokenization.exclusion.list	Les modèles de chiffrement ne peuvent pas tokeniser les chaînes trouvées dans ces champs.

Propriétés Java KeyStore

edgeencryption.keystore.path	Chemin d'accès au magasin de clés Java. Si vous utilisez un magasin de fichiers ou un magasin de clés SafeNet KeySecure, laissez cette propriété en commentaire. Exemple : `edgeencryption.keystore.path = keystore/keystore.jceks`
edgeencryption.keystore.password	Mot de passe utilisé par le proxy pour se connecter au Java KeyStore. Si vous utilisez un magasin de fichiers ou un magasin de clés SafeNet KeySecure, 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 qu'à des fins de dépannage ou sur demande de l'assistance ServiceNow . Pour plus d'informations, reportez-vous à la rubrique Comment augmenter la journalisation de débogage pour le proxy Edge Encryption .

Propriétés du keystore de périphérique NAE

edgeencryption.nae.retries	Nombre de nouvelles tentatives à effectuer.
edgeencryption.nae.enabled	Le paramètre indique si un périphérique 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.username	Nom d'utilisateur à utiliser pour s'authentifier avec l'appareil NAE.
edgeencryption.nae.password	Mot de passe à utiliser pour s'authentifier avec l'appareil NAE.
edgeencryption.nae.client.certificate	Certificat situé dans le magasin de clés sur le serveur NAE. Définissez cette propriété pour vous 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 brouiller 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 brouiller les mots de passe dans le fichier edgeencryption.properties .

Propriétés du proxy

edgeencryption.proxy.host	Nom du 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.

Propriété verrouillée de configuration du proxy

edgeencryption.proxy.locked	Si la valeur est vrai, le proxy n'accepte pas les changements de configuration de chiffrement ou les modifications de règle de chiffrement de l'instance. Définissez cette propriété sur l'instance de production une fois que toutes les configurations et règles de chiffrement sont finalisées.

Propriétés de la base de données proxy

edgeencryption.db.url	Emplacement de la base de données proxy. Elle doit être la 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. Elle doit être la 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. Elle doit être la même pour tous les proxys de chiffrement qui se connectent à la même instance.
edgeencryption.db.name	Nom de la base de données proxy. Elle doit être la 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.bootstrap.file	Fichier d'amorce pour la base de données proxy. Le fichier est relatif au répertoire `sql/` . Elle doit être la 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 de performances du serveur proxy

Les propriétés de performances du serveur proxy ne sont pas présentes dans le fichier de configuration par défaut. Pour modifier les valeurs par défaut, vous devez ajouter les propriétés et redémarrer le serveur proxy. Pour plus d'informations, consultez Diagnostics et performances d'Edge Encryption.

edgeencryption.stat.collection.enabled	Active la collecte des statistiques utilisées par le Chiffrement Edge tableau de bord des performances du serveur proxy. Valeur par défaut : true Ajoutez cette propriété et définissez sa valeur sur faux pour désactiver la collecte

	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 du certificat 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 du serveur proxy et déterminer comment le proxy répond aux demandes du client.

edgeencryption.proxy.https.cert.alias	Alias du certificat fourni par le serveur proxy aux clients qui se connectent.
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 de la cible (instance)

edgeencryption.target.host	Nom d'hôte de l'instance. Elle doit être la 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. Elle doit être la 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. Elle doit être la 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

Non lié Propriétés du fournisseur de technologie

edgeencryption.ekm.provider.classname	Nom de classe interne pour l'implémentation. **⚠ Avertissement :** Ne modifiez en aucun cas cette propriété.

edgeencryption.thirdparty.vendor.library.path	Chemin d'accès au fichier JAR de l'API Unbound sur l'ordinateur client Unbound.
edgeencryption.ekm.provider.rsa.wrapping.key.alias	Encapsulation de l'alias de clé dans l'implémentation Unbound Technology. Elle doit être la 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 avoir le rôle edge_encryption. Voir Configurer un compte d'utilisateur Chiffrement Edge.
edgeencryption.target.password	Mot de passe utilisé par le proxy pour se connecter à l'instance.

Propriétés du proxy Web

edgeencryption.webproxy.host	Nom ou adresse IP du proxy Web.
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 l'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 l'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. Elle doit être la 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. Elle doit être la 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 de 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.

edgeencryption.encrypter.password

Spécifie le mot de passe pour accéder au magasin de clés.

Intégration de CyberArk avec le serveur proxy Edge

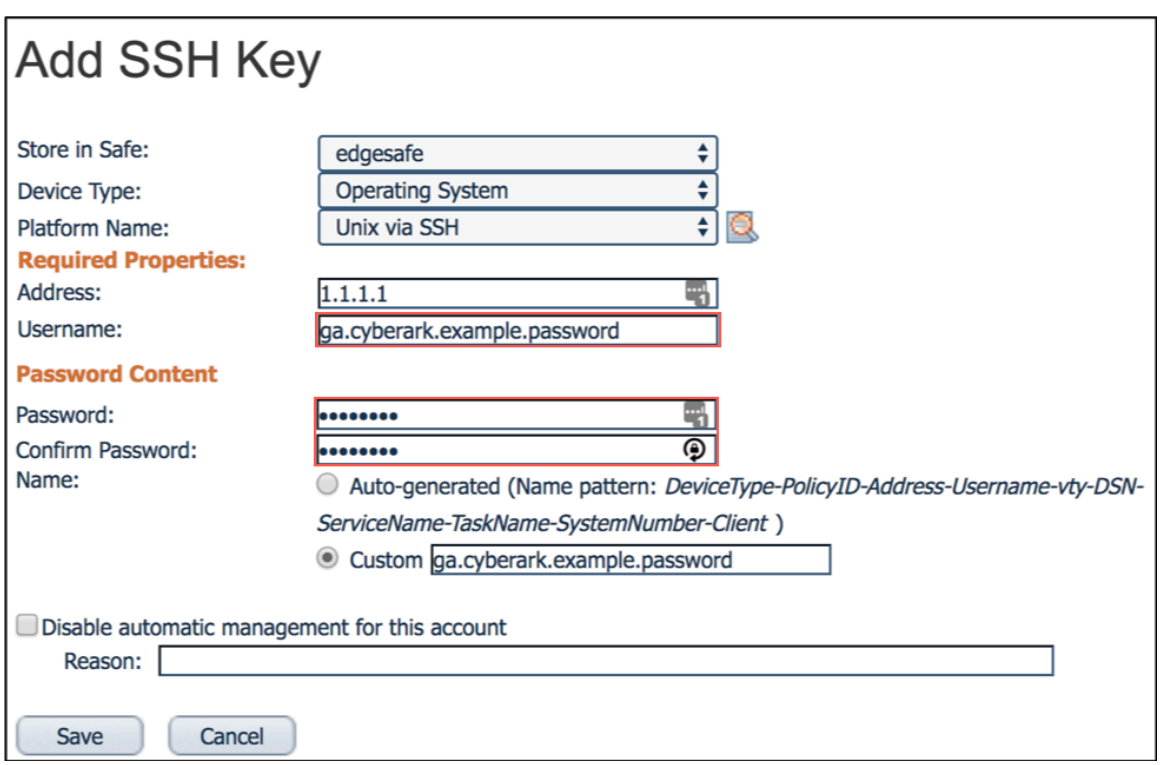
Utilisez CyberArk pour stocker les mots de passe dans un coffre-fort numérique centralisé et sécurisé afin de sécuriser les mots de passe qui étaient auparavant stockés en texte clair et sécurisés par l'accès aux fichiers, ou qui étaient précédemment chiffrés via un deuxième fichier.

CyberArk AIM (Application Identity Management) empêche tout accès non autorisé 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 justificatifs d'identité numériques. Les clients AIM (les serveurs proxy Edge) utilisent les informations d'identification 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 plate-forme** des informations d'identification sur **Unix via SSH** et **assurez-vous** de créer un **nom** d'informations d'identification **personnalisé** ou d'écrire le **nom** des 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.



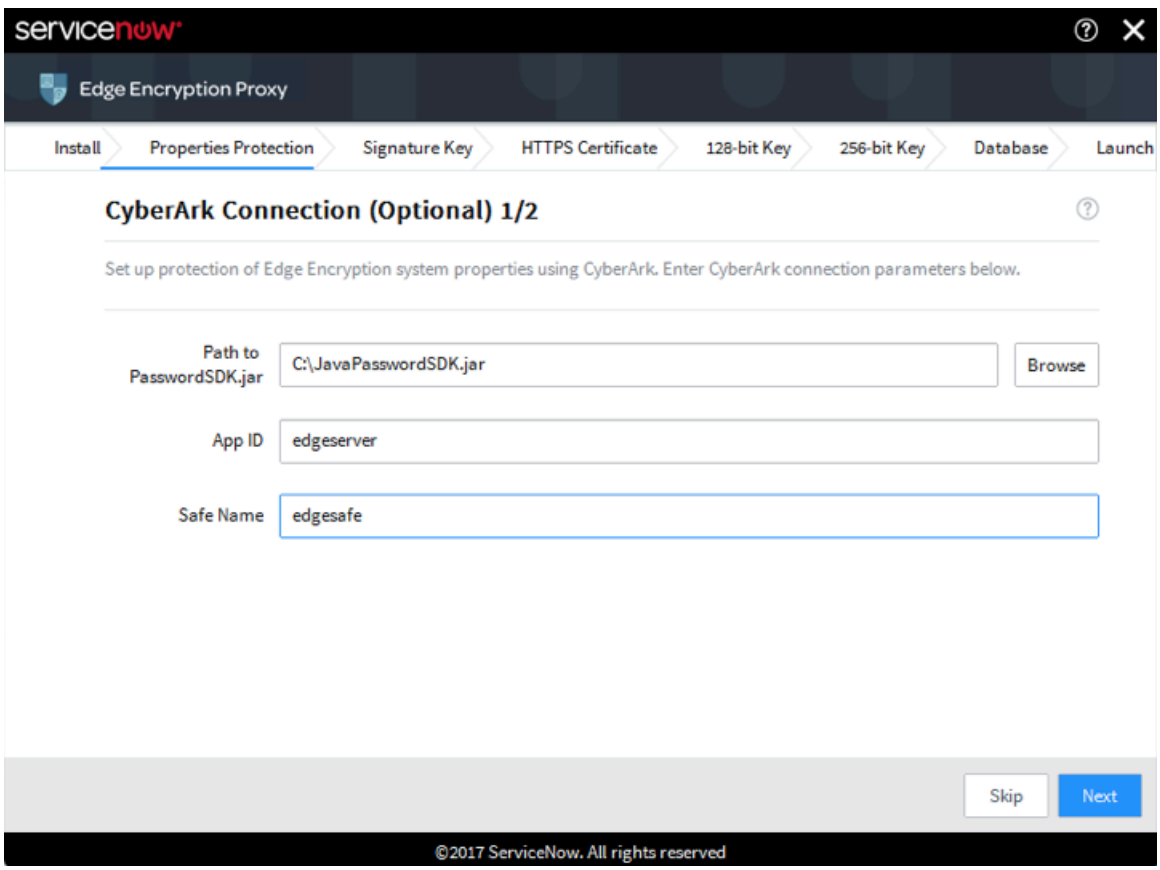
Chaque entrée d'informations d'identification contient un **mot de passe** qui est sécurisé, ainsi qu'un **nom** d'informations d'identification utilisé par une application pour accéder à ce mot de passe.

Traduction automatique

Remarque :
Les informations d'identification CyberArk ne sont pas des clés de chiffrement.

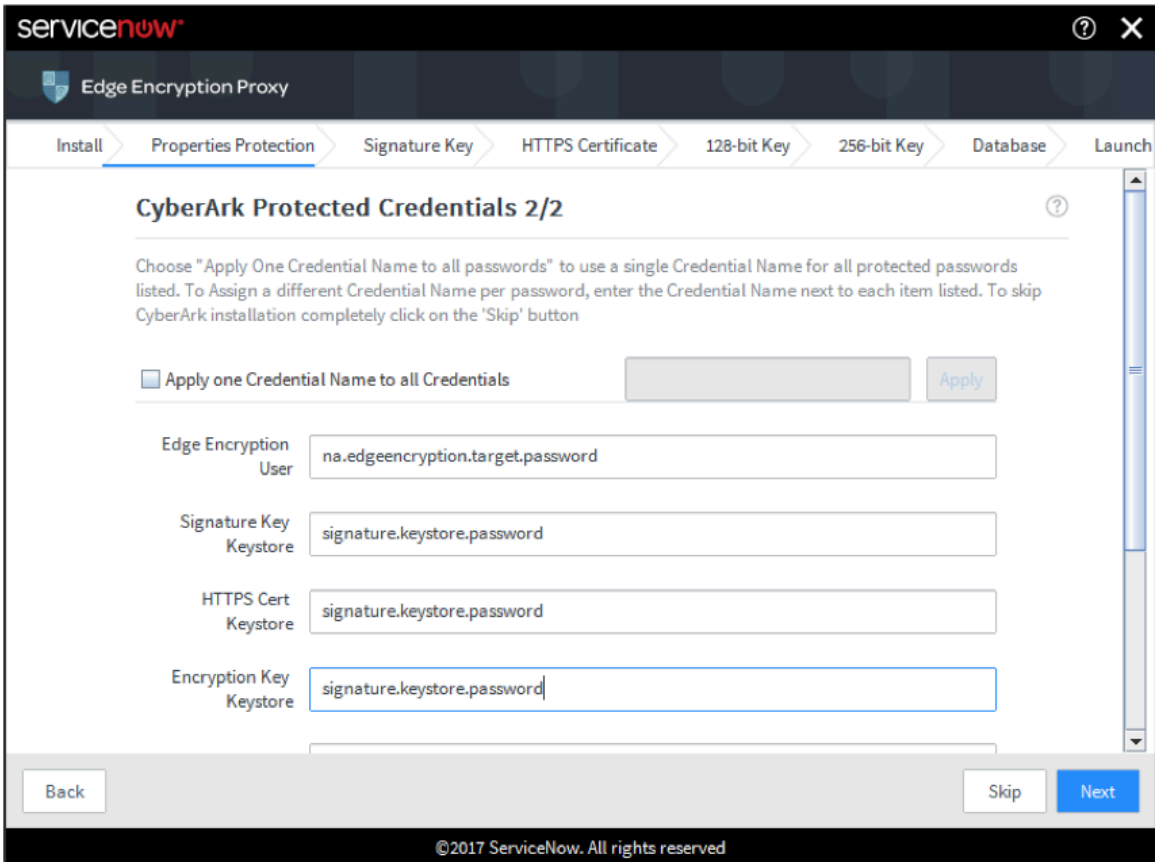
Ajout de CyberArk lors de l'installation d'un proxy Edge

Le programme d'installation du proxy inclut 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 configurer manuellement l'intégration de CyberArk dans le fichier de configuration.



Le programme d'installation du proxy inclut également une nouvelle page pour les informations d'identification protégées par CyberArk. Cette page permet de configurer différentes propriétés à l'aide d'un seul nom d'informations d'identification 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



Protection par mot de passe CyberArk

Tous les champs de mot de passe du programme d'installation du proxy Edge qui disposent d'informations d'identification CyberArk configurées dans le coffre-fort CyberArk et spécifiés sur la page Informations d'identification protégées de CyberArk du programme d'installation sont grisés et contiennent 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 dans la configuration de votre proxy Edge Encryption. 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 Edge Encryption pour la redondance.

Traitement de demande Edge 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 requête 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.
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 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 de demande Edge 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 du serveur proxy.

1. L'utilisateur émet une requête à partir d'un navigateur.
2. Le navigateur envoie la demande à une adresse IP virtuelle (VIP) d'équilibreur de charge, également appelée serveur virtuel.
3. L'adresse IP virtuelle est configurée pour pointer vers le serveur proxy (par exemple, 10.2.200.148 :1025), de sorte que l'équilibreur de charge transfère 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 pour 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 transfère 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 ou non 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 communique uniquement avec l'équilibreur de charge, mais la réponse est 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 réacheminer les messages de réponse vers l'équilibreur de charge si le serveur proxy et l'équilibreur de charge utilisent des ports différents.

- *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 du 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 terminées. ○ S'il existe un équilibreur de charge dans la configuration du proxy, spécifiez le nom d'hôte utilisé pour accéder à ServiceNow via l'équilibreur de charge. ○ Facultatif : s'il n'y a pas d'équilibreur de charge dans la configuration du proxy, 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. ○ S'il existe un équilibreur de charge dans la configuration, spécifiez le port HTTPS utilisé pour accéder à ServiceNow via l'équilibreur de charge. ○ Facultatif : s'il n'y a pas d'équilibreur de charge dans la configuration, vous pouvez définir cette valeur sur le port HTTPS utilisé par le serveur proxy.

4. Enregistrez le fichier.

Résultats

Les demandes peuvent être complétées, car les utilisateurs peuvent maintenant afficher les réponses sur leur navigateur.

Mise à niveau d'Edge Encryption

Les mises à niveau d'instance et 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 Edge Encryption nécessitent une certaine 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 Edge Encryption
- Modèles de tokenisation Chiffrement Edge
- Travaux planifiés Chiffrement Edge
- Configurations des clés de chiffrement Edge
- Mises à niveau planifiées de Chiffrement Edge
- Configurations IP de la liste de refus de Chiffrement Edge

Toute tâche planifiée exécutée pendant la mise à niveau de l'instance ne sera pas terminée. Pour terminer la tâche interrompue, réexécutez la tâche une fois l'instance 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 de fichier et la mise à niveau peut échouer. Pour que la mise à niveau réussisse, aucun fichier ne doit être ouvert dans le répertoire d'installation. De plus, il ne doit pas y avoir de shell 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 dans le 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 des serveurs d'instance et proxy si elles sont conservées dans le même répertoire. Vous pouvez effectuer les actions suivantes pour éviter la perte de bibliothèques tierces lors des mises à niveau :

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 la *edgeencryption.thirdparty.vendor.library.path* bibliothèque 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 d'accès.

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 :
Pendant ServiceNow les mises à niveau d'instance, mettez également à niveau la version de votre serveur proxy pour qu'elle s'aligne sur la version de votre instance et réduise 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 prévue. 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 si une nouvelle version est 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 Edge Encryption pour chaque serveur proxy.

   Remarque :
   Seuls les utilisateurs disposant du rôle security_admin peuvent créer une planification de mise à niveau via le serveur proxy.

4. Une fois la mise à niveau planifiée, le serveur proxy effectue automatiquement la mise à niveau à l'heure prévue. 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. Lors de 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 de votre ancien répertoire proxy sont copiés dans le nouveau répertoire proxy.
   - Répertoire /conf
   - Répertoire /keys
   - Répertoire /keystore
   - fichier java/jre/lib/security/cacerts

Par conséquent, vos clés, magasins de clés, paramètres et certificats sont conservés.

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 Edge Encryption, vérifiez les points suivants :

1. La variable d'environnement *JAVA_HOME* pointe vers une installation Java sur l'ordinateur qui se trouve en dehors de la structure du répertoire du proxy Edge Encryption.
2. La variable d'environnement *JAVA_HOME* pointe vers une installation Java de version 1.8_u144 ou supérieure.
3. Le `-Djava.io.tmpdir` paramètre dans le fichier wrapper.conf du proxy Edge Encryption pointe vers un répertoire qui se trouve en dehors de la structure de répertoire du proxy Edge Encryption, et le proxy dispose d'autorisations de lecture/écriture/exécution sur le répertoire. Si vous le souhaitez, 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 Edge Encryption exécuté sur Linux ou Mettre à niveau manuellement un serveur proxy Edge Encryption exécuté sous Windows.

État de la version du proxy

Vous pouvez facilement identifier si un serveur proxy n'est pas à jour 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

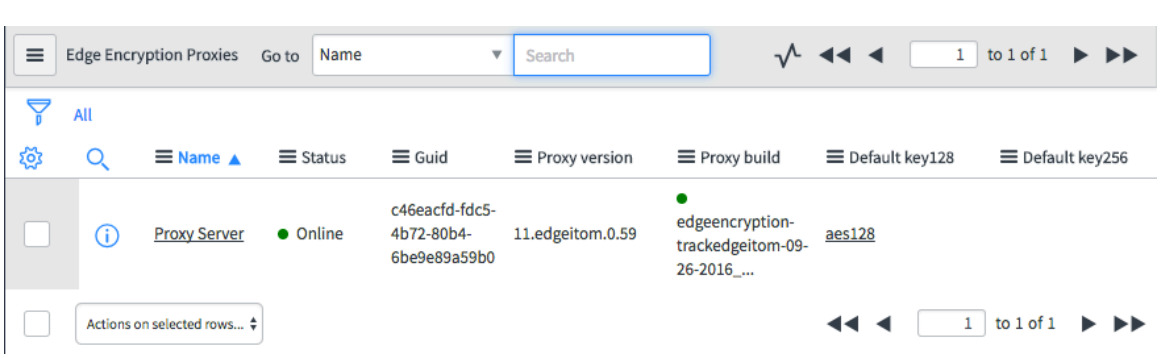
Votre serveur proxy est à jour.

Jaune

Votre serveur proxy n'est pas à jour 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.



Dépanner un 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. Contact Service et assistance client pour garantir la réussite de la mise à niveau.

Pour déterminer la raison de l'échec, vous pouvez vérifier la **raison de l'échec** dans le calendrier de mise à niveau. En outre, le répertoire d'installation de l'échec de la mise à niveau est conservé de sorte que les fichiers journaux sont disponibles pour le dépannage.

Remarque :
Avant de supprimer des répertoires proxy supplémentaires, vérifiez toujours quel répertoire est à jour en examinant les fichiers journaux. Si les fichiers journaux ont une activité récente, le proxy peut être connecté à votre instance.

Si la mise à niveau d'un proxy planifiée échoue à plusieurs reprises, vous pouvez mettre à niveau manuellement votre serveur proxy. Consultez Mettre à niveau manuellement un serveur proxy Edge Encryption exécuté sur Linux et Mettre à niveau manuellement un serveur proxy Edge Encryption exécuté sous Windows.

Configuration minimale requise pour Java

L'ordinateur hôte qui installe ou exécute le Chiffrement Edge serveur proxy doit disposer d'une version prise en charge de Java. Les versions actuellement prises en charge sont Java 11.0.6 ou ultérieure dans la série de versions 11.x

Remarque :
Java 8 n'est plus pris en charge à compter de cette Utah version. Mettez à niveau votre environnement avec le Chiffrement Edge proxy vers Java 11 avant de tenter d'installer la Utah version du Chiffrement Edge proxy.

Si vous utilisez un chiffrement AES 256 bits avec Java 8 mise à jour 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 de 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 stratégie 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 possible de le faire si tous les serveurs proxy se trouvent dans la même famille de versions que votre instance. Par exemple, si vous avez une instance sur la Washington DC version, votre environnement prend en charge les serveurs proxy à partir de n'importe quel Washington DC correctif ou correctif d'urgence. 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 n'est pas à jour, il se peut qu'il n'inclue pas 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

n’est pas à jour. Pour garantir un environnement optimal et sécurisé, ServiceNow il est recommandé 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 un chiffrement AES 256 bits avec Java 8 mise à jour 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 de 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 stratégie 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 effectue automatiquement la mise à niveau à l’heure prévue. 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.

Lors de 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 de votre ancien répertoire proxy sont copiés dans le nouveau répertoire proxy.

- Répertoire /conf
- Répertoire /keys
- Répertoire /keystore
- fichier java/jre/lib/security/cacerts

Par conséquent, vos clés, magasins de clés, paramètres et certificats sont conservés.

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 les mises à niveau vers plusieurs proxys sur la même machine 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 récente disponible pour votre instance.
Heure de début planifiée	Date et heure de démarrage de la mise à niveau.
Actifs	Si la mise à niveau planifiée est active. Si ce champ n'est pas sélectionné, la mise à niveau ne s'effectuera pas aux date et heure prévues.
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 moyenne 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 à son sujet. En cas d'échec de votre mise à niveau, examinez le **motif de l'échec** pour déterminer les étapes suivantes.

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	La 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.
Causes des défaillances	Motif de l'échec de la mise à niveau.

Mettre à niveau manuellement un serveur proxy Edge Encryption exécuté sur Linux

Mettez à jour un proxy fonctionnant sous Linux.

Avant de commencer

Si vous utilisez un chiffrement AES 256 bits avec Java 8 mise à jour 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 de 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 stratégie 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. Modifiez le répertoire d'installation.
3. Exécutez la commande suivante :

   ```
   java -jar edgeencryption-dist-&lt;version>-linux-x86-64.jar -m dist-upgrade -c &lt;répertoire proxy>
   ```

Option	Description
Répertoire proxy	Le répertoire dans le répertoire d'installation où le proxy a été initialement installé. 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 sous la forme 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.
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 Edge Encryption exécuté sous Windows

Mettez à jour un proxy en cours d'exécution sur Windows.

Avant de commencer

Si vous utilisez un chiffrement AES 256 bits avec Java 8 mise à jour 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 de 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 stratégie 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 télechargements** > **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. Modifiez le répertoire d'installation.
4. Exécutez la commande suivante :

   ```
   java -jar edgeencryption-dist-&lt;version>-all.jar -m dist-upgrade -c &lt;répertoire proxy>
   ```

Option	Description
Répertoire proxy	Le répertoire dans le répertoire d'installation où le proxy a été initialement installé. 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 sous la forme 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 qu'il est en cours d'exécution.

Restaurer une mise à niveau du serveur proxy Chiffrement Edge

Si la mise à niveau d'un proxy échoue, vous pouvez revenir à la version antérieure.

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 Washington DC version, le serveur proxy revient automatiquement à l'ancienne version. L'ancien serveur proxy est stocké tel quel dans un répertoire de sauvegarde.

Si vous souhaitez restaurer une mise à niveau manuelle, vous pouvez suivre les étapes suivantes.

Procédure

1. Arrêtez 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. Consultez le journal du proxy et l'instance pour vérifier que le proxy est en ligne.

Configuration d'Edge Encryption

Une fois le serveur proxy installé et en cours d'exécution Chiffrement Edge , effectuez la gestion Chiffrement Edge via le serveur proxy.

Vous devez terminer toutes les étapes avant Installation d'Edge Encryption 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 vous élever 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 uniques.

Avant de définir une clé de chiffrement comme clé par défaut, rendez la clé disponible pour chaque proxy. Cela garantit que les proxys ont 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 clé en masse pour vous assurer qu'aucune donnée sur 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 des clés par défaut, assurez-vous d'effectuer une rotation de clés (en masse ou une seule clé). Sinon, vous risquez de recevoir des résultats inattendus lors du tri et du filtrage des enregistrements. Imaginons par exemple le scénario suivant :

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 nouvel 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 ne fonctionne que 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 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 tâche de rotation de clé unique

Planifiez une tâche pour trouver 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 chiffrées à nouveau 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 d'une seule touche**.
Clé	Entrez la clé à retirer. Vérifiez 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 estimé total d'enregistrements à traiter. Cette option n'est pas disponible lors de l'exécution d'une rotation de clés unique.
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 pour 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. Cette option n'est pas disponible lors de l'exécution d'une rotation de clés unique.
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 de la première exécution de la tâche.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
   L'estimation du nombre d'enregistrements n'est pas prise en charge lors du traitement des champs audités.

Planifier une tâche de rotation de clés en masse

Planifiez une tâche pour trouver 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 chiffrées à nouveau 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 la clé de masse**.
Estimer le nombre d'enregistrements	Nombre estimé total d'enregistrements à traiter. Cette option n'est pas 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 pour 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. Cette option n'est pas 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 de la première exécution de la tâche.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
L'estimation du nombre d'enregistrements n'est pas prise en charge lors du traitement des champs audités.

Planifier une tâche de rotation de clé de pièce jointe

Planifiez une tâche pour trouver des pièces jointes chiffrées à l'aide d'un alias de clé spécifié, puis chiffrez à 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 **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 de la première exécution de la tâche.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
4. Pour afficher une estimation du nombre d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.
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 ne disposent de la clé. Une fois qu'une clé par défaut est définie, vous pouvez créer des configurations de chiffrement.

Affecter des champs et des pièces jointes à chiffrer

Affecter des champs et des pièces jointes à chiffrer signifie affecter un type de chiffrement au champ ou à la pièce jointe. Avant de marquer un champ comme chiffré, évaluez ces problèmes.

- Déterminez quelles fonctionnalités système peuvent être impactées.
- Examinez tous les scripts pour l'utilisation du champ.
- Ajustez la taille du champ selon vos besoins. 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 augmente la taille du champ pour stocker les données chiffrées. Le processus d'agrandissement de la taille du champ peut prendre beaucoup de temps, selon le nombre d'enregistrements dans la table.

Prise en charge de l'API

Column Level Encryption 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. Complétez le formulaire.

Champ	Description
Table	Table contenant le champ à chiffrer.
Type	S'il faut chiffrer une colonne de table ou des pièces jointes pour la table. **Sélectionner une colonne**.
Colonne	Champ à chiffrer. S'affiche uniquement lorsque le **type** est **Colonne**. 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 pouvez ajouter une configuration de chiffrement à une table parente uniquement. 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.

Champ	Description
Type de chiffrement	Le type de chiffrement à utiliser.

Remarque :
Une combinaison spécifique de table et de champ 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 sont modifiées. Pour plus de détails, voir Planifier une tâche de chiffrement.

Créer une configuration de chiffrement de variable

Sélectionnez les variables du 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. Complétez le formulaire.

Champ	Description
Variable	Variable à chiffrer.
Type de chiffrement	Le type de chiffrement à utiliser.

4. 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 sont modifiées. Pour plus de détails, voir Planifier une tâche de chiffrement.

Désactiver une configuration de chiffrement

Après avoir configuré un champ ou des pièces jointes de table à chiffrer, vous pouvez arrêter le chiffrement en désactivant la configuration de chiffrement. Après la désactivation du 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 d'Edge Encryption** s'affiche.
3. Cliquez sur la case **Actif** .
   La case **Actif** est vide.
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 seront déchiffrées la prochaine fois qu'elles seront 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** afin de 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.
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. La partie inférieure 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**.

Champ	Valeur
Table	Selectionner une table.
Colonne	Sélectionnez une colonne.
Estimer le nombre d'enregistrements	Nombre estimé total d'enregistrements à traiter. Se remplit 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 pour 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 Audit.
Estimer le nombre d'enregistrements d'audit maximal	Nombre maximal estimé d'enregistrements audités à traiter. Se remplit après avoir sélectionné **Estimer le nombre d'enregistrements**. Ce champ n'est visible que lorsque l'option **Traiter les enregistrements historiques** 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 de la première exécution de la tâche.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher une estimation du nombre 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 les données dans un champ chiffré, afin de stocker les données effacées dans l'instance.

Avant de commencer

Remarque :
Vous devez marquer l'enregistrement de chiffrement pour le champ comme inactif (décochez la case **Actif**) afin d'exécuter la tâche de déchiffrement.

Rôle requis : security_admin

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Tous** afin de 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. La partie inférieure 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 estimé total d'enregistrements à traiter. Se remplit 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 pour 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 Audit.
Estimer le nombre d'enregistrements d'audit maximal	Nombre maximal estimé d'enregistrements audités à traiter. Se remplit après avoir sélectionné **Estimer le nombre d'enregistrements**. Ce champ n'est visible que lorsque l'option **Traiter les enregistrements historiques** 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 de la première exécution de la tâche.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher une estimation du nombre 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.

Toutes les pièces jointes d'une table utilisent le même type de chiffrement. Les pièces jointes chiffrées ne sont pas recherchées lors d'une recherche textuelle. 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 contournant le Chiffrement Edge proxy :

- Sur un enregistrement où le chiffrement des pièces jointes est activé :
  - L'utilisateur peut voir qu'il existe 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 les pièces jointes existantes.
- L’utilisateur peut ajouter de nouvelles pièces jointes.

Lors d’une session utilisant le proxy de chiffrement, l’utilisateur peut ouvrir et télécharger des pièces jointes existantes et ajouter de nouvelles pièces jointes.

Configurer le chiffrement des pièces jointes

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	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 les 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 aucune tâche de chiffrement des pièces jointes, le système chiffre les nouvelles pièces jointes lorsque vous les joignez.

Remarque :
Si vous marquez *`l’attribut edge_encryption_clear_attachment_allowed`* sur **Vrai** dans l’entrée Dictionnaire de collection de la table, des pièces jointes non chiffrées sont ajoutées à une table à l’aide d’Edge Encryption pour chiffrer les pièces jointes. Si vous activez cet attribut, 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 des pièces jointes

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. La partie inférieure 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 des pièces jointes**.
Table	Selectionner une table.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure de la première exécution de la tâche.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher une estimation du nombre 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 (désactivez la case **Actif**) avant que la tâche de déchiffrement ne s'exécute, sinon rien ne se passe.

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 en pièce jointe**.

   Le formulaire **Tâche de chiffrement planifiée** s'affiche avec tous les champs renseignés. La partie inférieure 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 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 de la première exécution de la tâche.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher une estimation du nombre 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 spécifique de tables et de champs 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 modifier la configuration de chiffrement.
3. Cliquez sur la liste déroulante **Type de chiffrement** et sélectionnez un nouveau type de chiffrement.

   Remarque :
   Pour les pièces jointes, seuls les AES128 standard et AES256 standard sont autorisés.

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 sera 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 modèles 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 que celle 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 du 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 composé uniquement de caractères alphabétiques 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 incorporées 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 racinisation ne sont pas prises en charge.

Lors de l'utilisation de modèles, le texte clair ne quitte jamais votre réseau. Lorsque le serveur proxy correspond à un modèle dans une demande envoyée 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 en 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 en texte clair.

Remarque :
Les modèles de chiffrement des champs chiffrés ne sont pas vérifiés.

Procédure

1. Accédez à la **Tous** > **Configuration de Chiffrement Edge** > **Modèles 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 d'arête**.

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 sur la ligne suivante. Cela vous permet de regrouper des caractères dans un modèle long.

Option	Description
	Cliquez sur **X** pour supprimer le dernier caractère du modèle.
Avancé	Une expression RegEx Java. Si l'option Avancé est sélectionnée, vous ne pouvez pas redéfinir le type d'entrée sur De base. Dans le champ **Exemple de correspondance** , entrez un exemple de modèle pour tester l'expression RegEx. Dans le champ **Modèle** , entrez une expression RegEx Java. Cliquez sur **Valider** pour vérifier que l'expression correspond au modèle d'échantillon.

Le type d'entrée définit la façon dont vous allez entrer le modèle. Cela n'a aucune incidence sur la façon dont le modèle est utilisé.

4. Cliquez sur **Envoyer**.

Réparez ou récupérez des 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 préservant 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 chronophage 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'utilise le système, par exemple à 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.

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 que l'instance était en cours d'exécution, ce qui entraîne la conservation de l'ordre des champs pour lesquels il manque des jetons de commande.

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 **Commander la réparation des jetons**.
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 de la première exécution de la tâche.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
4. Pour afficher une estimation du nombre d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.

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.
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 de la première exécution de cette tâche.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
4. Pour afficher une estimation du nombre d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.

Configurer la liste de refus d'adresses IP

Empêcher une adresse IP de votre réseau d'envoyer des demandes 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 scanner IP ou d'autres demandes d'être transférés à votre ServiceNow instance, vous pouvez ajouter des adresses IP, des plages d'adresses IP ou des masques réseau à une liste de refus. Toute connexion au serveur proxy à partir d'une adresse sur liste de refus 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 dans votre réseau. Si une adresse IP est ajoutée à la liste de refus, tout utilisateur avec 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 listes de refus des adresses IP de proxy de chiffrement [edge_encryption_ip_blacklist] s'ouvre.
2. Cliquez sur **Nouveau**.
3. Complétez le formulaire.

Champ	Description
Serveur proxy	Le Chiffrement Edge serveur proxy qui ne peut pas transférer les demandes à partir d'adresses figurant sur la liste de refus.
Adresse IP, plage d'adresses IP ou masque réseau	Les demandes de cette adresse IP, plage ou masque réseau ne sont pas transmises à votre ServiceNow instance. Exemples de valeurs : ○ Adresse IP : 10.10.10.5 ○ Plage IP : 10.10.10.1-15 ○ Masque réseau : 10.10.10.0/24 **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 ne peuvent pas envoyer de 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 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 Catalogue de services partir du et Portail de services. Si un créateur d'enregistrement tente d'insérer des données dans un champ marqué pour le chiffrement, un message d'insertion non valide s'affiche et les données ne sont pas enregistrées dans le champ.

Le chiffrement de données provenant 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 des pièces jointes à partir d'un créateur d'enregistrement, Configurer le chiffrement des pièces jointes.

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 Edge Encryption**.
   Deux règles de chiffrement inactives sont automatiquement créées pour chiffrer les données envoyées par le créateur d'enregistrement au champ marqué pour le chiffrement.

Règle de chiffrement	Description
<NomProducteurEnregistrement>	Règle créée pour traiter les paramètres POST à partir de la Catalogue de services et mapper les variables sur les champs de l'instance.
<RecordProducerName>JSON	Règle créée pour traiter une charge utile JSON à partir de la Portail de services et 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**.

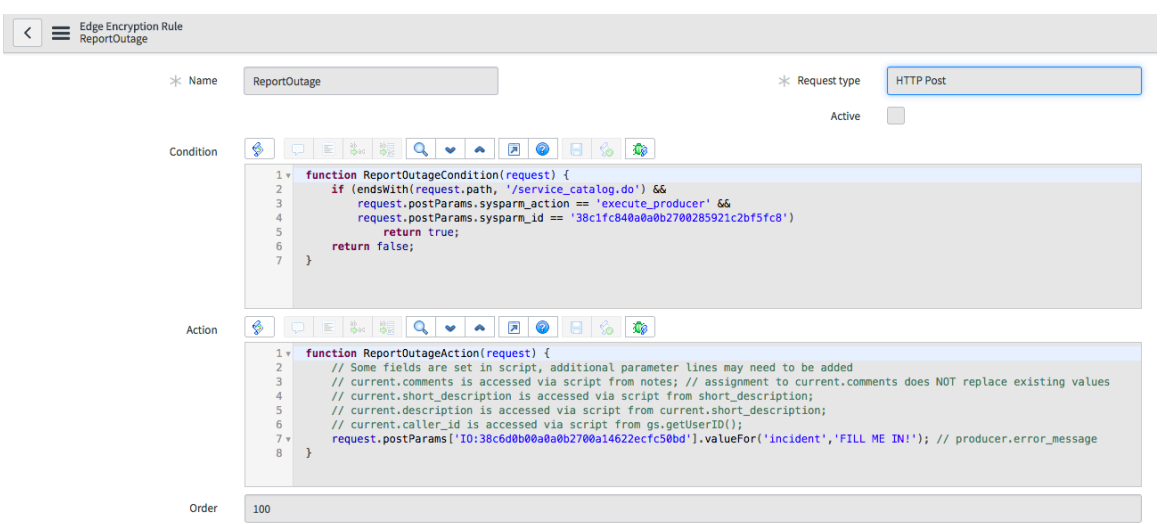
b. Selon l'endroit où le créateur d'enregistrement sera utilisé, ouvrez la règle de chiffrement associée créée par le créateur d'enregistrement et sélectionnez le marqueur **Actif** .
Si le créateur d'enregistrement est utilisé dans le Catalogue de services, activez la règle de chiffrement <RecordProducerName >. Si le créateur d'enregistrement est utilisé dans le Portail de services, activez la règle de chiffrement <RecordProducerName>JSON.

6. **Facultatif :** Examinez **le champ Action** de règle de chiffrement et ajoutez tous 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 via différents scripts sur la plateforme, vous devrez peut-être mettre à jour les règles pour mapper chaque variable au champ approprié.

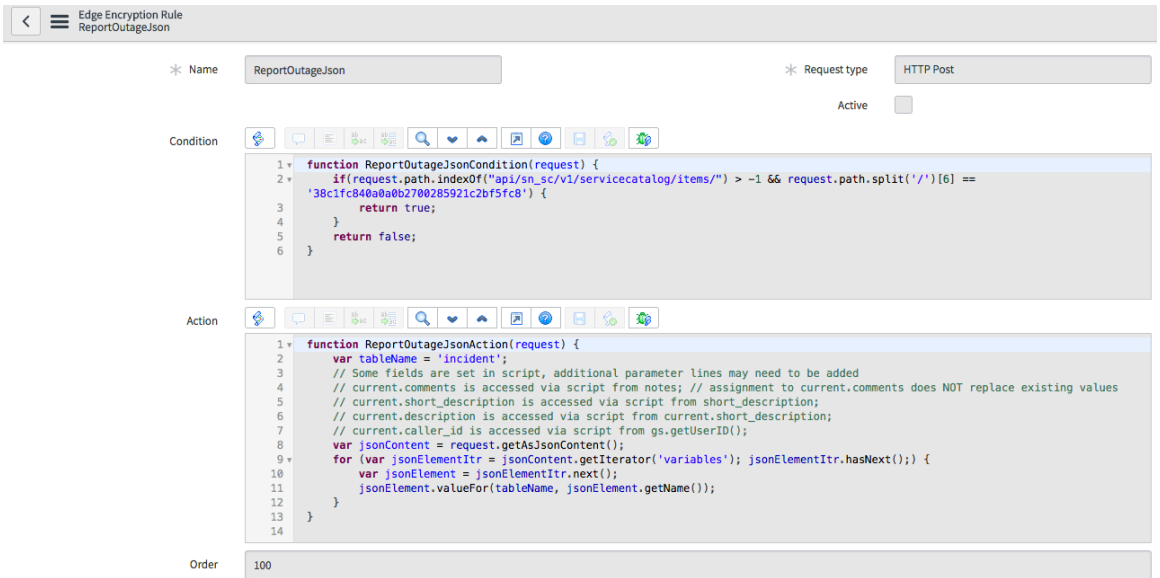
Example

(Optional) La règle de chiffrement ci-dessous a été créée à partir du créateur d'enregistrement Signaler une panne et traite les Catalogue de services paramètres POST du pour mapper les variables aux champs de l'instance. Remplacez 'FILL ME IN' par le champ cible.



La règle de chiffrement ci-dessous a été créée à partir du créateur d'enregistrement de panne de rapport et traite une charge utile JSON à Portail de services partir du pour mapper les variables aux champs de l'instance. Ajoutez des instructions supplémentaires pour mapper toutes les variables de script aux champs cibles.

Traduction automatique



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 de ou Catalogue de servicesPortail de services.

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 vers votre instance. Vous pouvez écrire des règles de chiffrement

pour identifier, interpréter et chiffrer les données dans de telles demandes, en mappant les champs de la demande aux noms de table-champ sur votre instance.

Qu'est-ce qu'une règle de chiffrement ?

Les règles de chiffrement sont des scripts exécutés sur le serveur proxy pour mapper les champs d'une Chiffrement Edge demande aux champs d'une table sur 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 prennent uniquement en charge 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
- Mise à jour d'un enregistrement à partir du formulaire d'enregistrement
- Gestion du service Web direct
- Traitement des données de l'interface de programme 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 table-champ Glide. Par exemple :

- Processeurs scriptés
- Services Web basés sur un script
- API REST basées sur un script, des interfaces utilisateur ou des scripts Ajax

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, chiffrant les valeurs qui sont mappées 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. À l'instar des règles métier, les règles vont 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 règles de chiffrement par ordre de priorité jusqu'à ce que toutes les conditions retournent la valeur faux ou qu'une condition renvoie la valeur vrai. Lorsqu'une condition renvoie la valeur true, 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 des règles 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 pour la validation des scripts.

Règle générale : Lorsque les règles deviennent longues, faites de votre mieux pour minimiser le nombre de blocs et séparez 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 ifs ou switch dans le script d'action.

1. Divisez 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'enregistrement 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 des sous-ensembles plus petits de créateurs d'enregistrements, ou même créer une règle par sys_id.

     Remarque :
     La création de plusieurs règles nécessite plus de maintenance. La contrepartie 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 contenues dans le corps d'une demande. L'API utilise des expressions similaires à xPath pour parcourir le contenu JSON et XML.

Chiffrement Edge Les API traitent la demande au fur et à mesure qu'elle est écrite dans le flux de sortie. L'analyse des flux permet aux règles de chiffrement d'être performantes sur le réseau. Toutefois, l'extraction et l'analyse du contenu à partir 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 script includes, les règles métier ou tout autre paramètre global tel que `actuel`. Étant 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 listes 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 du 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 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 parcourent les demandes du client et déterminent ce qui doit être chiffré, le cas échéant, vous devez comprendre le type de demande pour lequel vous créez une règle. Le format de la demande client détermine la structure de votre règle de chiffrement et les API disponibles pour une utilisation dans la règle.

Procédure

1. Inspectez la demande du client.

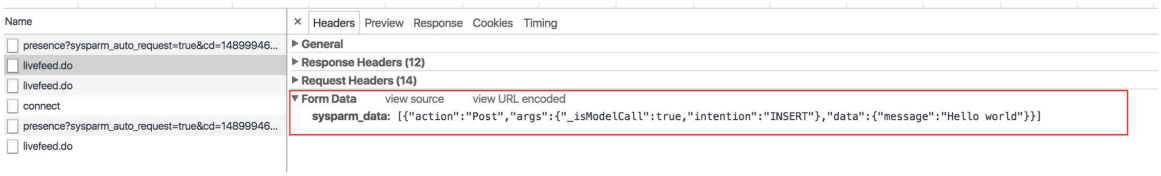
   Selon la source de la demande, les outils suivants sont disponibles pour inspecter la demande et déterminer son format.

Source de la demande	Outils disponibles
Navigateur du client	Utilisez la console développeur dans votre navigateur pour inspecter la demande du client. Les outils utiles sont les suivants : ○ Moniteur réseau Firefox ○ Panneau réseau Chrome
Tiers/source externe	Utilisez un analyseur de protocole HTTP pour inspecter la demande. Les outils utiles sont les suivants : ○ Wireshark ○ HTTP Scoop Vous pouvez également utiliser la documentation de la source externe pour déterminer le format de la demande.

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
- Les paramètres d'auto-test de démarrage (No POST), le cas échéant
- Format du corps de la demande, s'il est inclus

Example



Résultats
L'inspection de la demande vous permet de comprendre les champs que vous devez filtrer et itérer dans votre règle de chiffrement. Pour comprendre les champs de l'objet de *la demande* , reportez-vous à Demande.

Créer une règle de chiffrement

Les règles de chiffrement sont utilisées par le proxy pour trouver le contenu des 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** , saisissez un nom.
3. Dans Type de **demande**, sélectionnez une méthode HTTP.
   - **HTTP Post**
   - **HTTP Get**
   - **Put HTTP**
   - **Correctif HTTP**
   - **HTTP Delete**

   Remarque :
   Les instances préalablesJakarta autorisent uniquement **les méthodes HTTP Get** et **HTTP Post** .
4. Dans la zone **Condition** , entrez une instruction JavaScript définissant quand la règle doit s'exécuter.
5. Dans la zone **Action** , entrez une fonction JavaScript à exécuter lorsque la condition est vraie.
6. Dans la zone **Ordre** , entrez la priorité relative de la règle.
7. Cliquez sur **Envoyer** ou enregistrez le formulaire.

Conditions des règles 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, elle doit retourner la valeur false.

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 de la condition. Des vérifications excessives peuvent coûter cher au serveur proxy et entraîner une latence accrue lors de la gestion de demandes complexes.

La condition peut utiliser le type de méthode, le type de contenu, le chemin d'accès de l'URL ou n'importe quel paramètre de chaîne de requête d'URL pour déterminer si la règle doit gérer 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 d'avoir compris 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 évaluer par une règle. Créez votre condition pour qu'elle retourne d'abord la valeur false pour ces demandes. Cette méthode augmente les performances et achemine rapidement la demande vers la règle appropriée.

Objets de règles 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 d'utilisation de 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;
  }
 return false;
}
```

Actions de règle de chiffrement

Une règle de chiffrement mappe les champs d'une demande client aux champs d'une table sur votre instance et identifie les champs marqués pour le chiffrement.

Une action de règle de chiffrement s'exécute uniquement lorsque la condition de 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 sur le contenu de l'objet de la demande, vous devez comprendre la forme et la structure du corps de votre demande et déterminer les éléments de la demande qui doivent être chiffrés. Les données à chiffrer peuvent se trouver dans :

- Paramètre POST ou URL.
- Contenu JSON ou XML dans un paramètre POST ou URL.
- Charge utile JSON .
- Une charge utile XML .

Avant d'écrire une action de règle de chiffrement, assurez-vous de :

- Inspecter la demande du client.
- Identifiez où se trouvent les données sensibles dans l'objet de la demande .
- Déterminez le nom de champ et de table dans lequel insérer des données, ou découvrez comment les extraire dynamiquement de la demande.

Objets de règles de chiffrement et API sont disponibles pour les actions et conditions de règle de chiffrement.

Objets de règles de chiffrement et API

Utilisez des API de règles de chiffrement pour analyser et chiffrer les valeurs dans les demandes transitant par le Chiffrement Edge serveur proxy vers l'instance.

Les API disponibles pour votre règle de chiffrement dépendent du format de l'objet de la demande. Par exemple, si le paramètre contentType de l'objet de la demande est XML, vous pouvez utiliser le API XML pour analyser et chiffrer les valeurs de 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 d'action et de condition de règle de chiffrement.

Demande

L'objet *de demande* est un objet global disponible dans Chiffrement Edge les scripts d'action et de condition de règle.

L'objet de *la demande* est un objet JavaScript qui représente la demande du client entrant dans le Chiffrement Edge serveur proxy. Vous devez créer votre règle de chiffrement pour analyser l'objet de *demande* , mapper les valeurs de l'objet de *demande* aux champs d'une table de l'instance et chiffrer toutes les données sensibles de l'objet de *demande* .

L'objet de *demande* inclut les attributs et données suivants issus de la demande client :

Champs d'objet de demande

Champ	Description
chemin d'accès	La partie chemin d'accès de l'URL.
requestMethod (Méthode de demande)	OBTENIR, PUBLIER, METTRE, CORRIGER, SUPPRIMER.
Contenttype	Le champ d'en-tête Content-Type.
Urlparams	Paramètres de la chaîne de requête. Cela peut également être évalué à une chaîne de caractères.
PostParams	S'il s'agit d'une publication de formulaire, elle contient les paramètres de publication.

demande : getAsJsonContent()

Renvoie la demande sous la forme d'un 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 dans l'objet de la `demande` .

Une fois que la demande est renvoyée en tant qu'objet `JsonNode` , vous pouvez utiliser la API JSON pour itérer sur l'objet et chiffrer les champs.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Nœud JSON	La demande en tant que `JsonNode` itérable.

requête : getAsXmlContent()

Renvoie le contenu de la demande en tant qu'objet itérable de type `XMLContent`.

Cette méthode n'est disponible que dans une Chiffrement Edge règle 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 dans l'objet de la `demande` .

Une fois que la requête est renvoyée en tant qu'objet `XMLContent` , vous pouvez utiliser la 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*.

request - XMLContains(chemin d'accès de la chaîne)

Renvoie la valeur true si le chemin d'accès donné existe dans le 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 dans l'objet de la *demande* .

Paramètres

Nom	Type	Description
chemin d'accès	Chaîne	XPath que vous recherchez.

Renvoie

Type	Description
Booléen	Indique si le chemin d'accès donné existe dans le DOM XML.

API de paramètres POST et URL

Les paramètres POST et URL sont accessibles en tant que propriétés de l'objet de la *demande* à l'aide de request.postParams et request.urlParams.

Vous pouvez accéder à n'importe quel paramètre unique 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 client, il peut être nécessaire d'accéder aux valeurs de paramètre et de les chiffrer à partir de l'objet de la *demande* . Selon les données contenues dans la demande client, vous pouvez chiffrer des 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 contiendront les données chiffrées, vous pouvez les définir explicitement dans la règle de chiffrement. Par exemple, vous savez peut-être que la demande sera traitée sur l'instance pour créer un incident et que 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 susceptible de 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;
   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 Chiffrement Edge au serveur proxy de chiffrer tout paramètre d'URL dont le nom correspond à un champ marqué pour le chiffrement.
- Recherche un paramètre spécifique appelé `texte` et demande Chiffrement Edge au proxy de chiffrer la valeur en fonction de la configuration de chiffrement pour le champ de description de la table d'incidents.

Dans cet exemple, la méthode valueFor() n'effectue pas de 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 le 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 du paramètre, itérer sur les valeurs et chiffrer les champs requis. Dans cet exemple, **l'attribut tableName** est toujours accessible à partir d'un paramètre POST, mais la valeur du champ correspond aux **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'action de règle de chiffrement qui traite XML dans un paramètre POST.

```
function SampleAction4() {
  var tableName = request.postParams.table;
  var data = request.postParams.data;
  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 de l'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 des champs de la requête ont des configurations de chiffrement.

Dans cet exemple, la règle itère sur les paramètres à la recherche du paramètre **de filtre** , qui est censé 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^number=INC000056^category=Panne`, la requête deviendra `short_description=<Chiffré(Mes informations sensibles)>^number=INC000056^category=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	La valeur du paramètre sous forme de chaîne.

ParameterValue : getAsJsonContent()

Renvoie la demande sous la forme d'un 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 dans l'objet de la *demande* .

Une fois que la demande est renvoyée en tant qu'objet `JsonNode` , vous pouvez utiliser la API JSON pour itérer sur l'objet et chiffrer les champs.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Nœud JSON	La demande en tant que `JsonNode` itérable.

ParameterValue : getAsXmlContent()

Renvoie le contenu de la demande en tant qu'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 requête est renvoyée en tant qu'objet `XMLContent` , vous pouvez utiliser la 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.

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	Le nom du champ.

Renvoie

Type	Description
nul	

API XML

Les API XML peuvent être utilisées après avoir appelé `getAsXmlContent()` sur l'objet de `la demande` ou sur 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 `requête` 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().`
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 vers une table-champ connue 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 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 parcourt 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'itère qu'une seule fois dans la boucle.

Mappage vers un champ de table inconnu sur l'instance

Dans cet exemple, la règle itère sur les balises **d'enregistrement** , mais ne sait pas quelles balises attendre dans la balise **d'enregistrement** . La seule inconnue est que les balises

dans les balises **d'enregistrement** correspondent aux noms des colonnes spécifiées dans le paramètre URL de table.

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>
```

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 vraie, la règle demande au serveur proxy de chiffrer les valeurs de la requête codée. Si la valeur est false, la règle demande au proxy de vérifier si le champ doit être chiffré.

XMLContent

Objet global qui fournit des méthodes d'itération 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.<parameter name>.getAsXmlContent() ou request.urlParams.<parameter name>.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` .

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 où commencer 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 d'itération 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.

Xmlelement

Fournit des méthodes permettant d'itérer à travers des éléments XML et de 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	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 requête.

Paramètres

Nom	Type	Description
tableName	Chaîne	Le nom de la table.
Fieldname	Chaîne	Le nom du champ.

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 de l'attribut.

Renvoie

Type	Description
Chaîne	Valeur d'attribut.

API JSON

Les API JSON peuvent être utilisées après avoir appelé `getAsJsonContent()` sur l'objet de `demande` ou sur 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 requête` . 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 retourner 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 vers une table-champ connue 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 Description remplit 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');
   while (jsonNodeIterator.hasNext()) {
      var jsonNode = jsonNodeIterator.next();
      jsonNode.valueFor('incident', 'short_decription');
   }
}
```

Cette action parcourt 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 la structure xPath et itérateur. Cependant, il n'itère qu'une seule fois dans la boucle.

Mappage vers un champ de table inconnu sur l'instance

Dans cet exemple, la règle itère sur les **enregistrements**, mais ne sait pas trop à quoi s'attendre. La seule chose connue est que pour chaque objet dans les **enregistrements**, les nœuds correspondent aux noms des colonnes spécifiées dans le paramètre URL de 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 du 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 le chiffrement, le proxy chiffre la valeur.

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 d'itération 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.<parameter name>.getAsJsonContent() ou request.urlParms.<parameter name>.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()`.

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 - itérateur()

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	La 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.

Renvoie

Type	Description
Chaîne	La 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 spécifiée.

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 requête.

Paramètres

Nom	Type	Description
tableName	Chaîne	Le nom de la table.
Fieldname	Chaîne	Le 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.

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	Vrai 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 n'est disponible que dans un script d'action Chiffrement Edge de règle.

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 règles 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__
__FICHIER__
__LIGNE__
__Parent__
__Proto__
Erreur
Eval
getClass
getPrototypeOf
Java
JavaScript
Javafx
JavaImporter
Charge
loadWithNewGlobal
nouveau
Packages
Objet

Mots clés interdits (suite)

Mot clé
Prototype
Regexp
setPrototypeOf
ce
Jeter

Attributs du dictionnaire Chiffrement Edge

Ajoutez des attributs de dictionnaire aux tables et aux champs pour contrôler leur fonctionnement avec Edge Encryption.

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, voir Attributs de dictionnaire .

Chiffrement Edge exclu [edge_encryption_excluded]

Détermine si le champ est exclu du chiffrement.

Si la valeur est définie sur `true`, le champ ou la table ne peuvent pas être chiffrés. Lorsqu'il est défini 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.

Lorsqu'il est défini sur `vrai`, le champ est éligible pour le chiffrement. Lorsqu'elle 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 pour l'utilisateur.

Remarque :
Cet attribut n'indique pas qu'un champ est chiffré et ne déclenche aucune logique de chiffrement sur le champ. Au contraire, l'attribut détermine la possibilité que le champ soit chiffré par un utilisateur.

- Valeur : vrai/faux
- Élément cible : champ
- Valeur par défaut : true pour les champs de type chaîne

Chiffrement Edge : effacer le texte 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 des scripts automatisés côté serveur, tels que les tâches planifiées.

Lorsque la valeur est définie sur true, l'ajout de données est autorisé. Lorsqu'elle est définie sur faux, l'ajout de données n'est pas autorisé.

- Valeur : vrai/faux
- Élément cible : champ
- Valeur par défaut : false

Séparation de domaine et Chiffrement Edge

Domain Separation est prise en charge dans des circonstances limitées avec Chiffrement Edge. Chiffrement Edge offre la possibilité de chiffrer des données depuis l'environnement du client à l'aide de configurations, de règles et de clés spécifiques définies sur le Chiffrement Edge proxy. Le proxy ne prend pas en charge le Chiffrement Edge domaine et ne peut pas prendre en charge les paramètres spécifiques au 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.

Comment fonctionne Domain separation dans Edge Encryption

Edge Encryption peut être utilisé lorsque des clés, des configurations et des règles spécifiques au domaine ne sont pas requises.

Information associée

Séparation de domaine pour les fournisseurs de services

Intégration des données avec Chiffrement Edge

Pour intégrer des données tierces à une instance à l'aide Chiffrement Edgede , vous devez acheminer les données via le Chiffrement Edge serveur proxy à l'aide des intégrations 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 les champs marqués pour le chiffrement

Chiffrement Edge ne prend pas en charge l'importation ou l'exportation de données à partir d'un fichier Excel, CSV, XML ou d'autres types de fichiers vers ou depuis des champs dont les configurations de chiffrement sont définies.

ODBC driver

Chiffrez les demandes et interrogez les données via le Chiffrement Edge serveur proxy à l'aide du pilote ODBC.

Pour en savoir plus : Intégration du pilote ODBC de Chiffrement Edge

MID Server

Vous pouvez configurer le pour acheminer les Serveur MID données via un Chiffrement Edge serveur proxy. Cependant, certaines restrictions s'appliquent.

Pour en savoir plus : Intégration du MID Server Chiffrement Edge

Services Web REST/SOAP

Utilisez les services Web REST/SOAP pour mettre à jour ou récupérer des données d'enregistrement via le Chiffrement Edge serveur proxy.

En savoir plus : Services Web

Service Web JSONv2

Utilisez les API de service Web JSONv2 pour mettre à jour ou récupérer des 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 des 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()`.

Pour en savoir plus : JSONv2 Web Service

Pour chiffrer les données provenant d'intégrations tierces personnalisées non répertoriées ci-dessus, créez des règles de chiffrement personnalisées. Voir Définir une règle de chiffrement personnalisée.

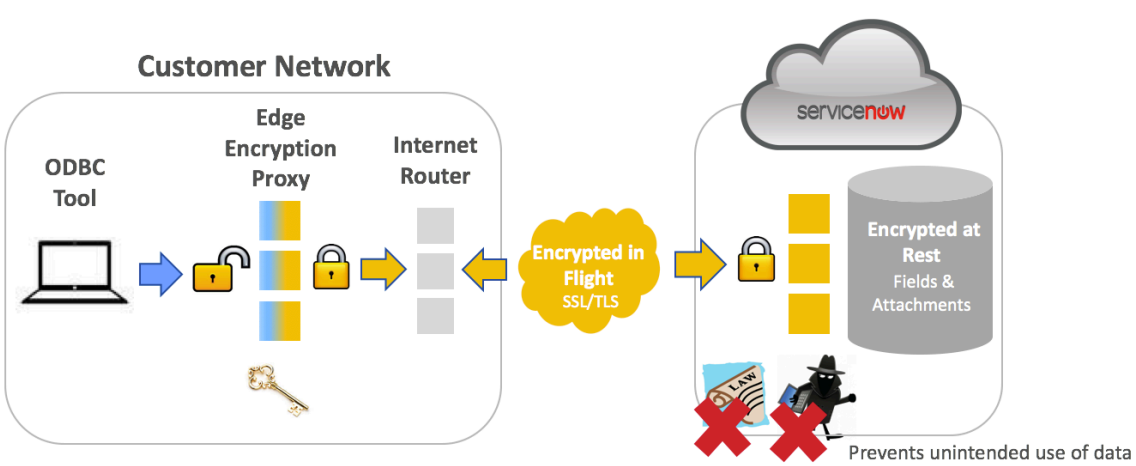
Charger les pièces jointes aux enregistrements marqués pour le chiffrement

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 de Chiffrement Edge

Configurez votre pilote ODBC pour interroger les données chiffrées par Chiffrement Edge. Le Chiffrement Edge serveur proxy chiffre les demandes de pilote ODBC envoyées à l'instance ServiceNow lorsqu'il Chiffrement 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

Pour une intégration réussie, le pilote ODBC doit faire confiance au 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 autosigné dans le magasin de confiance ODBC.

Importer un certificat autosigné dans le magasin 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 autosigné dans le magasin de confiance ODBC. Vous pouvez exporter le certificat à partir du Chiffrement Edge serveur proxy et l'importer dans le magasin 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 d'accueil 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 proxys par l'intermédiaire Chiffrement Edge d'un équilibreur de charge, de sorte que le certificat est 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, reportez-vous à la rubrique Configurer des propriétés supplémentaires dans le fichier de propriétés de Chiffrement Edge

Procédure

1. Modifiez le répertoire du magasin de clés dans le répertoire de base du proxy.
2. Vérifiez le magasin de clés pour le certificat autosigné.
   a. Pour vérifier le magasin de clés du certificat, exécutez 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 des éléments.
3. À l'aide de l'alias de clé, exportez le certificat vers un fichier .cer.

```
keytool -export -alias <key alias> -keystore keystore.jceks -storetype jceks -rfc -file <file name>.cer
```

4. Modifiez votre répertoire de magasin de confiance ODBC : ODBC\ip\Java\jre\lib\security\cacerts.
5. Importez le certificat dans votre magasin 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.

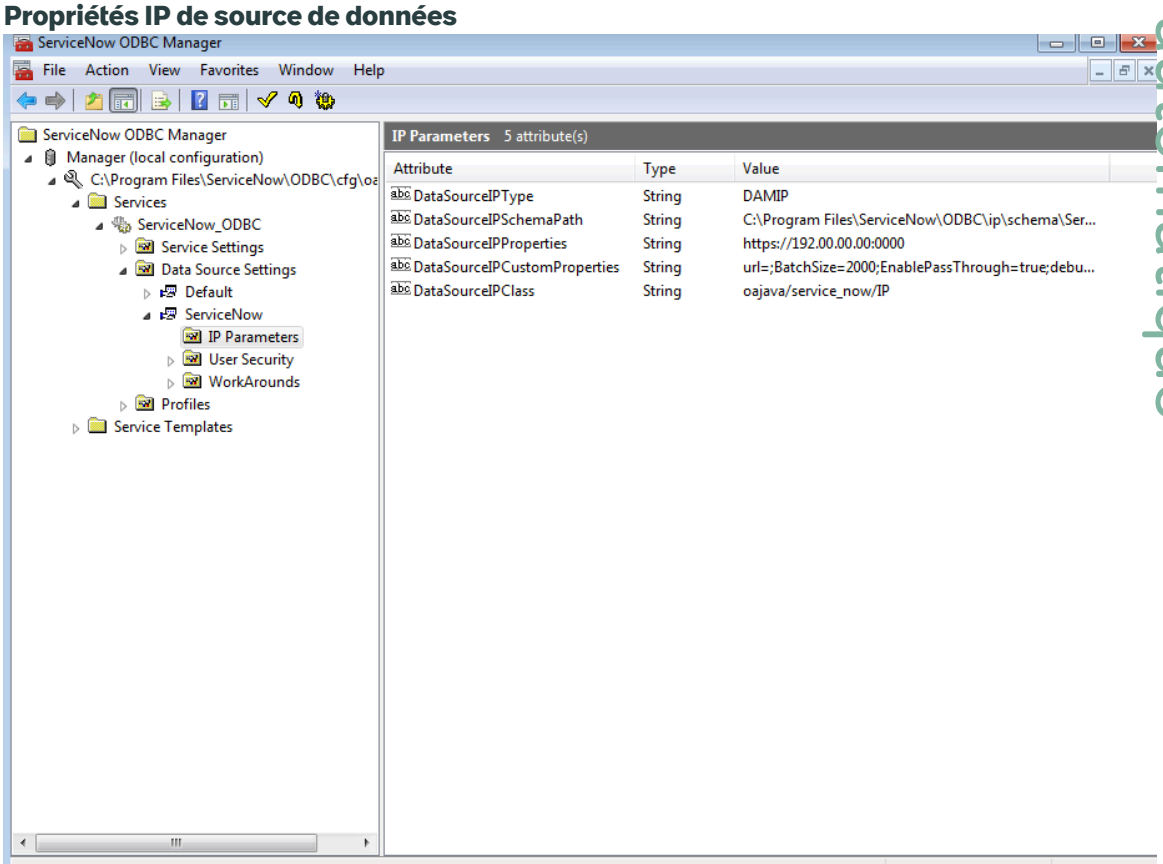
Avant de commencer

Rôle requis : admin

Procédure

1. Dans Windows, accédez à **Début** > **Programmes** > **Console de gestion ODBC ServiceNow**.
2. Développez la racine de l'arborescence de la console comme suit : Gestionnaire ODBC ServiceNow \Gestionnaire\<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>

Propriétés IP de source de données



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 MID Server Chiffrement Edge

Configurez le pour acheminer les Serveur MID données via un Chiffrement Edge serveur proxy.

Lorsqu'il est intégré à , Serveur MIDle Chiffrement Edge serveur proxy fait office de Serveur MIDpoint de terminaison de . Le Chiffrement Edge serveur proxy chiffre et déchiffre ensuite les données transmises entre l'instance et le ServiceNow .Serveur MID

Limitations lors de l'intégration au MID Server

Lorsque Serveur MID les données sont configurées pour transiter 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 Détection ou Mappage des services.

Pointez le MID Server vers le serveur proxy Chiffrement Edge

Pour transmettre les Serveur MID données via le Chiffrement Edge serveur proxy, mettez à jour le Serveur MID fichier de configuration afin de pointer vers Serveur MID le Chiffrement Edge serveur proxy.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Lors de la configuration de la pour qu'elle Serveur MID passe par le Chiffrement Edge serveur proxy, vous ne pouvez pas utiliser les propriétés de 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 Serveur MIDcela, vous devez définir le Chiffrement Edge serveur proxy comme point de 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 dirige le trafic vers le Chiffrement Edge serveur proxy plutôt que Serveur MID vers 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. S'il est en cours d'exécution, redémarrez le Serveur MIDfichier .

Diagnostics et performances d'Edge Encryption

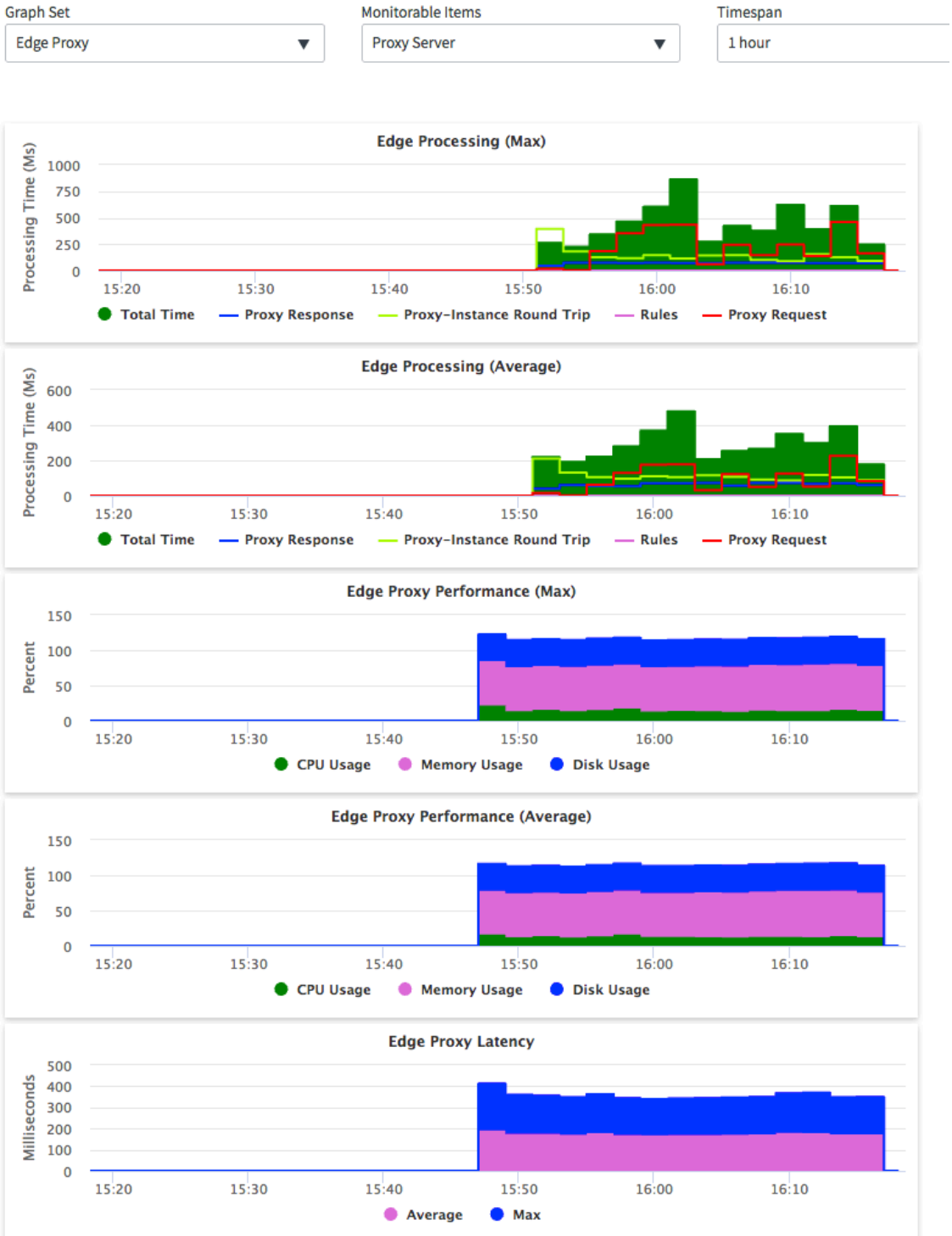
Surveillez les Chiffrement Edge tendances des performances du serveur proxy et analysez les erreurs générées par le Chiffrement Edge serveur proxy.

Performances du proxy Edge

Affichez les tendances clés Chiffrement Edge des performances du serveur proxy à l'aide du graphique Proxy Edge défini sur la page d'accueil ServiceNow Performances. Les tendances surveillées sont les suivantes :

- Délais de réponse maximaux et moyens 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 performances.



Traitement en bordure (max et moyen)

Délai maximal et moyen, en millisecondes, de traitement d'une demande. Ces points de données sont des tendances générales dans le temps.

- **Temps total** : délai accordé 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 du proxy** : délai de traitement par le serveur proxy d'une réponse de l'instance.

- **Aller-retour proxy-instance** : temps pour le serveur proxy d'envoyer une demande à l'instance et de recevoir une réponse. Inclut la latence du réseau entre le serveur proxy et l'instance, ainsi que le temps passé par l'instance à traiter la demande.
- **Règles** : délai pendant lequel le serveur proxy évalue une demande à l'aide de règles de chiffrement définies.
- **Demande proxy** : délai pendant lequel le serveur proxy doit traiter une demande client et la transmettre à l'instance.

Performances du proxy Edge (max. et moyennes)

Pourcentage maximal et moyen de ressources utilisées sur l'ordinateur hôte.

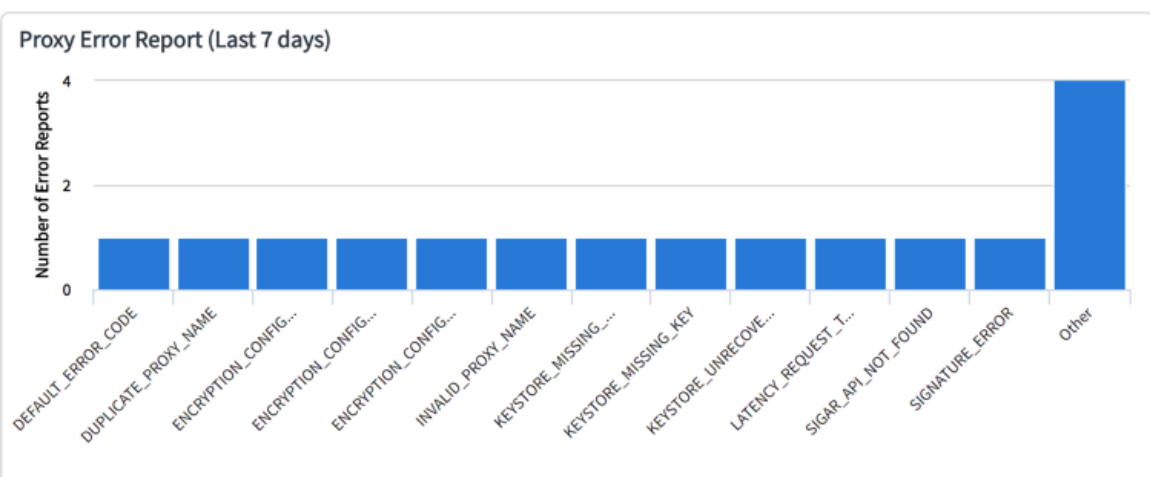
- Utilisation du processeur
- Utilisation de la mémoire
- Utilisation du disque

Latence du proxy Edge

Latence réseau maximale et moyenne en millisecondes à un moment donné. La latence est déterminée par le temps d'aller-retour 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 de DEFAULT_ERROR_CODE est générée plusieurs fois au cours d'une période de rapport d'une minute, la barre de DEFAULT_ERROR_CODE n'atteindra qu'une seule fois sur l'axe **Nombre de rapports d'erreurs** .

Dans cette vue, vous pouvez :

- Cliquez sur chaque barre de code d'erreur de proxy pour afficher le rapport sur une seule erreur pour chaque serveur proxy. Dans cette vue, vous pouvez cliquer à nouveau sur la barre pour afficher le texte d'erreur dans la Chiffrement Edge table Stat. proxy [edge_encryption_stat]. Suivez les liens dans le texte d'erreur pour afficher plus d'informations et les étapes de correction possibles.
- Cliquez sur **Autre** pour afficher la deuxième page du rapport d'erreur.

Remarque :
Si vous avez plusieurs serveurs proxy du même nom, une seule erreur DUPLICATE_PROXY_NAME s'affiche dans le rapport d'erreurs de 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 de surveillance supplémentaires

L'instance suit tous les proxys de chiffrement. Chaque Chiffrement Edge serveur proxy s'enregistre au démarrage. L'instance est notifiée quand :

- Un nouveau Chiffrement Edge serveur proxy démarre.
- Un Chiffrement Edge serveur proxy est intentionnellement arrêté.

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 font l'objet d'un audit 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 et 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 correctement.
Journaux système	L'instance vérifie périodiquement les messages provenant 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 ping à l'instance.

Table	Description
	Si l'instance détermine 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 Chiffrement Edge serveur proxy d'envoyer des statistiques Edge Proxy Graph Set à la page d'accueil ServiceNow Performances 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.
- Modifiez 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 <installation directory>/conf /.
2. Ajoutez l'un des Propriétés du serveur proxy Chiffrement Edgefichiers .
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 de débogage dans le Chiffrement Edge proxy. Augmentez le niveau de journalisation pour déboguer les problèmes, fournissez à l'assistance technique des informations pour examiner le problème avec des instructions de journal plus détaillées.

Selon le problème en cours de débogage, configurez la journalisation de débogage de l'une des trois façons suivantes :

- Problèmes de débogage autres que la connectivité SSL
- Journalisation des mesures de minutage des 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 les vôtres 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 autre que la Chiffrement Edge connectivité SSL

Utilisez cette méthode pour déboguer les problèmes avec l'application Chiffrement Edge , sans arrêter et redémarrer le proxy. Ces étapes augmentent le niveau de journalisation et aident à résoudre la cause première grâce à des instructions de journal plus détaillées.

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 un délai d'environ 60 secondes après que vous ayez effectué 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 la suivante :

```
logger.edge.level=debug
```

3. Enregistrez le changement.
   La prise d'effet de la modification peut prendre jusqu'à 60 secondes, mais cela ne nécessite pas de redémarrage du proxy.
4. Reproduisez votre problème.
5. Vérifiez les instructions du journal de débogage liées 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 . Lorsque vous avez terminé le débogage, annulez la modification apportée au fichier $proxy_installation_location/conf/log4j2.properties .

Journalisation des mesures de minutage des demandes via le proxy

Activez la journalisation des mesures de synchronisation pour ajouter une instruction de mesure pour chaque demande traitée par le Chiffrement Edge proxy. Chacune de ces instructions de journal de mesure de synchronisation 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 prises en charge dynamiquement par le proxy dans un délai d'environ une minute après que les modifications aient été 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
```

```
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 s'affichent dans le fichier journal $proxy_installation_location/logs/edgenetwork.log pour connaître 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 dans les 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
```

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 liés à la connectivité SSL entre le proxy et l'instance Chiffrement Edge

Utilisez cette méthode pour déboguer les problèmes de connectivité SSL entre le proxy et votre instance, tels que les Chiffrement Edge échecs d'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. Dans la 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 la modification et redémarrez le serveur proxy.
4. Reproduisez votre problème de connectivité.

Résultats

Après avoir reproduit le problème, les déclarations du journal de débogage liées 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 déplacer la journalisation supplémentaire à distance en supprimant ou en commentant la ligne créée lors des étapes précédentes.

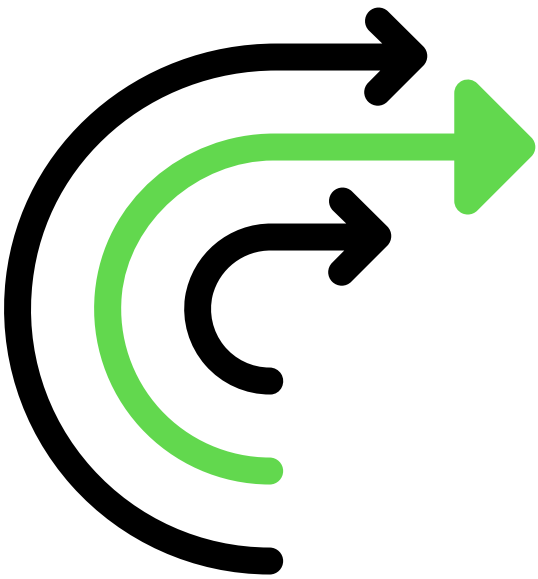
Journaux

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.

servicenow

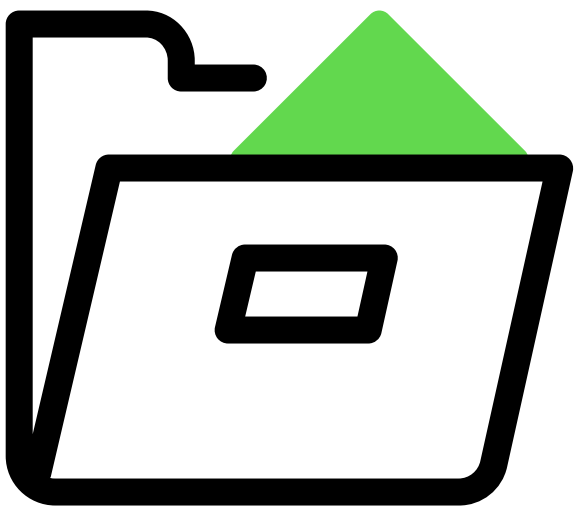
Premiers pas

Journaux système



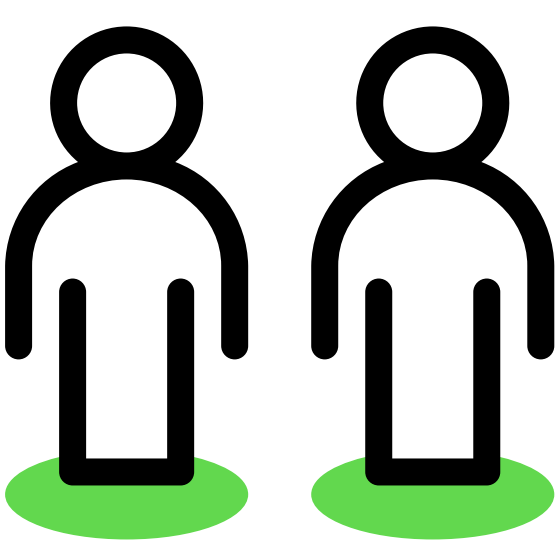
Le module Journaux système fournit une variété de journaux que vous pouvez utiliser pour résoudre et déboguer les transactions et les événements qui se produisent au sein de l'instance.

Service d'exportation de journaux



Log Export Service (LES) vous permet de transférer de manière sélective les journaux de l'instance ServiceNow vers Hermes, puis de consommer les journaux pour les alimenter dans leurs systèmes.

Journalisation, audit et erreurs



Traduction automatique

Appliquez une stratégie de journalisation et d'audit afin de pouvoir identifier les activités suspectes et intervenir en temps utile.

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 notifications push	Toutes les notifications par e-mail et les messages push envoyés depuis toutes les instances du système.
Journaux des événements	Tous les événements système qui se produisent dans le système.
Importer	Activité d'importation de données au sein de la plateforme.
Changements de tables	Changements apportés à toutes les tables du système.
Connexion aux 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 l'ordinateur serveur.

Utilisez l'Explorateur de fichiers journaux 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, la Module Diagnostics du système fournit un historique des mises à niveau et des journaux de requêtes lents, que vous pouvez utiliser pour mieux comprendre comment les requêtes affectent les performances de la plateforme. Ils Table Mises à jour du client enregistrent chaque modification apportée au système.

Journal système

Affichez les avertissements et les erreurs pour les processus d'instance, les enregistrements et les événements non critiques, tels que l'utilisation de la mémoire sur l'ordinateur serveur.

Les informations suivantes sont suivies dans le journal système :

- 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 sur la mise à niveau pour toute activation de module d'extension, ensemble de mises à jour ou mise à niveau système

Les entrées de journal s'affichent uniquement pour le jour en cours. Pour afficher d'autres fichiers journaux, utilisez l'explorateur de fichiers journaux. Ce journal fournit les informations suivantes pour toutes les occurrences :

Journal système

Champ	Description
Créé	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 Déboguer, 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 touchée par l'événement. Par exemple, la source de l'occurrence peut être E-mail ou Mémoire.
Source Package	Nom du package d'application associé à l'occurrence. Cliquez sur le nom pour afficher l'enregistrement Application de stockage [sys_store_app] de 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 ou Erreur
  - Résultat
  - Description du panne, s'il y a eu une erreur
- Historique de transition, y compris :
  - Heure de la transition
  - Activité effectuée à partir de

  - Activité passée à
  - Quelle transition a été déclenchée
- Journal du workflow, y compris toutes les instructions de journal ajoutées au workflow

Informations de 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 dans laquelle le changement a été effectué
- Nom de l'objet en cours de modification
- Type d'objet en cours de modification
- Vue dans laquelle le changement a été effectué, 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 de transactions par périmètre de l'application, en limitant les transactions qui s'affichent aux seules transactions provenant de périmètres spécifiques.

Le journal des transactions fournit les informations suivantes pour toutes les activités.

Champ	Description
Créé	Date et heure de l'action d'application pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Type	Type de transaction enregistrée.
Créé par	Utilisateur qui a créé cette activité.
Application d'origine	Périmètre de l'application à l'origine de la transaction. Global apparaît 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	Délai de latence de la réponse réseau après l'exécution 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.

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 il est connecté par l'application cliente.
ID système	Identificateur généré par le système de l'instance client effectuant la demande. Cet ID est utilisé pour les environnements de cluster dans lesquels plusieurs instances (nœuds) communiquent avec la base de données.
Adresse IP	Adresse IP du client effectuant la demande.
Compressé avec GZIP	Indique si une page Web compressée a été demandée par l'application.
Protocole	Protocole HTTP utilisé par l'application pour cette instance.

Minutages des transactions clientes

Le module d'extension Client Transaction Timings améliore les journaux système en fournissant des informations supplémentaires sur la durée des transactions ayant lieu entre le client et le serveur.

Vous pouvez retrouver les problèmes de performances jusqu'à leur source en affichant où le temps est consommé et comment le temps a été passé au cours d'une transaction.

Ce module d'extension requiert l'activation de l'indicateur de temps de réponse Indicateur de temps 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
Créé	Moment où la transaction a été enregistrée.
Temps de réponse	Nombre de ms passés par le serveur à exécuter la transaction.
Temps de règle métier	Nombre de ms passés par les règles métier déclenchées par la transaction.
Temps SQL	Nombre de ms passés par la base de données SQL.

Informations sur les transactions clientes (suite)

Champ	Description
Temps de réponse client	(Load_completion_time) - (start_time). Il comprend le temps de serveur.
Délai réseau du client	Nombre de ms passés par le réseau via lequel le client se connecte.
Temps navigateur	Nombre de ms passés par le navigateur au cours de la transaction.
Heure du script client	Nombre de ms passés à exécuter des scripts clients.
Heure de politique d'interface utilisateur	Durée en ms consacrée à l'exécution de 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 durées client pour tous les rendus de formulaires (mais pas de listes) est également suivie. Pour afficher les détails, explorez un enregistrement de transaction client particulier et observez la liste connexe à la base 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 des notifications push pour suivre l'état des notifications push qui sont mises en file d'attente pour être envoyées depuis votre système.

Pour afficher le journal push, accédez à **Journaux système** > **Notifications push**. Les utilisateurs doivent avoir le rôle push_admin ou admin pour afficher le journal des pushs.

Champs du journal push

Champ	Description
Réclamation	Numéro d'identification généré par la tâche planifiée qui envoie la notification push. Ce numéro est appliqué au champ **Réclamation** pour assurer la cohérence entre plusieurs tâches planifiées par push.
Charge utile	Contenu de la notification push.
Nombre de files d'attente	Nombre de fois que le système a essayé d'envoyer la notification push. L'état de la notification push dépend de son nombre de files d'attente. • Si le nombre de files d'attente est égal à 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 **typeest 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. Semblable à l'ID de message pour 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 les valeurs suivantes : • **échec** : le message n'a pas pu être envoyé. • **en attente** : le message est mis en file d'attente pour traitement. • **réussite** : le message a été envoyé avec succès, bien qu'il ne soit pas nécessairement reçu par l'équipement mobile.

Information associée

Travaux planifiés

Journal des e-mails système et boîtes aux lettres

Le journal d'e-mails système enregistre tous les e-mails que l'instance crée ou reçoit. Les boîtes aux lettres système sont des vues filtrées de ce journal.

Chaque e-mail de notification que l'instance crée ou reçoit 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 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, consultez Boîtes aux lettres système .

Les champs suivants peuvent être inclus dans la mise en page du journal système et de toutes les boîtes aux lettres système :

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	L'état de l'e-mail. Les choix possibles sont les suivants : • received : 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. Pour plus d'informations, reportez-vous au champ de chaîne d'erreur. • send - failed : le serveur a tenté d'envoyer l'e-mail et a échoué. Pour plus d'informations, reportez-vous au champ de chaîne d'erreur. • send - ignored : 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 sans adresse e-mail du destinataire ou qui est un e-mail en double. Pour plus d'informations, reportez-vous au champ de chaîne d'erreur. • 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. • send - translation - ready : l'e-mail est généré lors de 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 d'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	Le 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	L'ID unique de l'e-mail stocké sur le serveur.
Créé	La date et l'heure de l'activité de messagerie pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Supprimé	Pour les e-mails entrants, indique si l'e-mail a été supprimé du serveur de messagerie.

Journal d'e-mail (suite)

Champ	Description
Poids	Le poids de l'e-mail, qui détermine la priorité d'envoi par rapport aux autres notifications de la même table.
Importance	Une indication que l'e-mail a été envoyé avec un niveau d'importance modifié, tel qu'Urgent.
Événement et notification d'origine	Pour les e-mails générés par les notifications, une liste incorporée qui stocke l'événement et la notification qui ont créé 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	Chaîne d'erreur capturée à partir du serveur de messagerie pour déterminer pourquoi l'e-mail n'a pas été envoyé. Elle n'est consignée que si l'e-mail a échoué à l'état d'envoi.
Destinataires	Adresses e-mail des destinataires.
Corps	Le corps de l'e-mail, affiché dans le balisage HTML brut. Utilisez le lien connexe Afficher un aperçu du corps HTML pour afficher le corps du texte en tant que rendu HTML.
Type de contenu	Le type de contenu de l'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 Now Platform.

Ce journal fournit les informations suivantes pour tous les événements qui se produisent :

Journal des événements

Champ	Description
Créé	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.
Parm1	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 l'événement a été traité Cette heure reflète les paramètres régionaux de l'ordinateur exécutant l'instance.
Délai de traitement	Temps nécessaire pour traiter cet événement, en millisecondes.
File d'attente	Nom de la file d'attente du processeur.

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 obtenir une vue plus détaillée des jeux d'importation qui ont produit un journal particulier, reportez-vous à la rubrique **Ensembles d'importation** > **Historique de transformation**.

Ce journal fournit les informations suivantes pour toutes les importations :

Journal d'importation

Champ	Description
Créé	Date et heure de l'importation des 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 Diagnostics du système

L'application System Diagnostics 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. Reportez-vous à la section Utiliser un journal de requêtes lent .

Table Mises à jour du client

Les modifications apportées dans le système sont enregistrées chronologiquement dans la table Mises à jour du client [sys_update_xml]. Il y a quelques exceptions, comme indiqué ci-dessous.

Pour accéder à cette table, saisissez sys_update_xml.list dans le filtre de navigation. Pour plus d'informations sur les ensembles de mises à jour, consultez Ensembles de mises à jour système .

Les informations suivantes sont stockées sur chaque mise à jour :

Table Mises à jour du client

Champ	Description
Nom	Un nom qui identifie l'enregistrement mis à jour.
Créé	La date et l'heure de création de l'enregistrement Mise à jour du client.
Créé par	Utilisateur qui a effectué le changement.
Type	Type de la mise à jour.
Mis à jour	La date et l'heure de mise à jour de l'enregistrement Mise à jour du client.

Table Mises à jour du client (suite)

Champ	Description
Mis à jour par	Utilisateur qui a effectué la mise à jour.
Mises à jour	Nombre de mises à jour de l'enregistrement.
Nom cible	Nom de l'élément qui a été modifié.
Vue	La 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
- Modifications en cascade des tables et des champs, telles que les changements de nom d'affichage
- Références de métadonnées non résolues provenant d'autres applications (ce qui entraîne l'absence de « valeur d'affichage » sur l'élément)
- sys_id changements pour les fichiers fusionnés
- Changements apportés au flux/aux actions de flux qui peuvent 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, reportez-vous à la section Valider les modifications .

Historique du journal

Le système utilise la rotation 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 des journaux commun

Table	Archiver la planification	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]	Toutes les semaines	8	Rotation

Calendrier d'archivage des journaux commun (suite)

Table	Archiver la planification	Rotations	Type
Journal des transactions [syslog_transaction]	Toutes les semaines	8	Rotation
Courriel [sys_email]	Tous les 30 jours	8	Extension

Utiliser le navigateur de fichier journal

L'instance fournit le navigateur de fichiers journaux des utilitaires et le téléchargement des fichiers journaux.

Utiliser **Journaux système** > **Utilités** > **Navigateur de fichier journal de nœud** pour afficher une entrée du 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 ayant 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'événement générée par le système.
Niveau	Type de message affiché. Les niveaux sont Déboguer, 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 retournés 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 avant 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 journaux 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

qui ont été générées lors de l'exécution de la transaction. Une transaction peut avoir n'importe quel nombre d'entrées syslog. Les entrées syslog multiples 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 corrélation 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 du journal de 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.

Réalisez les actions suivantes à l'aide des nouvelles améliorations :

- Suivre l'origine source de chacune des lignes de journal
- Dans le cas où les informations d'origine ne sont pas disponibles, affichez le nom de classe Java et une attribution
- Au début de chaque ligne de transaction, elle contient l'ID et le type de transaction

Utilisez l'ID de transaction de chaque ligne de journal pour comprendre les informations données à chaque ligne de journal. Une fois que vous avez identifié le type de transaction, vous obtenez les informations d'origine de chaque ligne de journal. Le type de transaction et les informations d'origine de chaque ligne de journal vous donnent les informations de source requises de chaque ligne de journal de nœud.

Remarque :
SYS_UI_MACRO et SERVICE_PORTAL_WIDGET types de script dans l'attribution ne sont pas signalés.

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

- Lot REST
- Instance Scan

Propriétés système

Voici les propriétés système requises pour la fonctionnalité :

- Glide.log.append.attribution : cette propriété est activée par défaut. Il 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 du nom de classe Java

Éviter la falsification des journaux

Configurez les règles de protection des tables de journaux système pour limiter le champ d'application de la modification et de la suppression des enregistrements de journal d'application. Les règles vous permettent de déterminer l'enregistrement des modifications ou tentatives de modification dans ces tables.

Si vous êtes un security_admin, activez le module d'extension Tables protégées (com.glide.protected_tables) qui permet à la plateforme de restreindre les opérations de mise à jour, d'insertion et de suppression sur les tables de journal 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 journal 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.

Consultez 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 journalise 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 journalise la tentative
- Ne pas bloquer ni enregistrer la tentative : ne bloque pas la modification et n'enregistre pas la tentative

La plateforme utilise les niveaux de protection des journaux spécifiés pour chacune des tables de journaux système afin de bloquer et/ou d'enregistrer 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.

S'il y a eu des tentatives de modification des tables de journal système, elles sont consignées dans la table protected_table_log.

Remarque :
Si le niveau de protection n'est pas spécifié pour une table, aucune tentative de modification n'est enregistrée dans la table protected_table_log.

Pour désactiver les opérations du module d'extension sur les tables dans le panneau d'administration, définissez la propriété com.glide.security.protected_table.enabled sur false. Pour plus d'informations, consultez Créer une propriété de protection de journal .

Configuration du module d'extension de protection des journaux

Configurez les règles de protection pour chaque table et opération afin de 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 cette Utah version, 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 changés 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.

Remarque :
Pour la table sysevent, les protections d'insertion ne peuvent pas être définies sur Bloquer.

Si vous aviez activé **l'option Appliquer aux tables enfants** pour syslog dans la version précédente, les tables enfants sont ajoutées à Log Protection avec les mêmes règles de protection que syslog lors de la mise à niveau vers la Utah version. Cela ne se produit que pour syslog, pas pour d'autres tables.

4. Activez la fonctionnalité en sélectionnant le bouton bascule **Activer la protection de 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 de journal

Créez une propriété de protection des journaux pour éviter le risque d'altération des journaux.

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 de propriété système s'affiche.
2. Renseignez les détails du formulaire

Champs	Description
Nom	Nom de la propriété comme com.glide.security.protected_table.enabled
Application	Application qui possède la propriété.
Description	Description de la propriété
Choix	
Type	Type de valeur : vrai | 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.

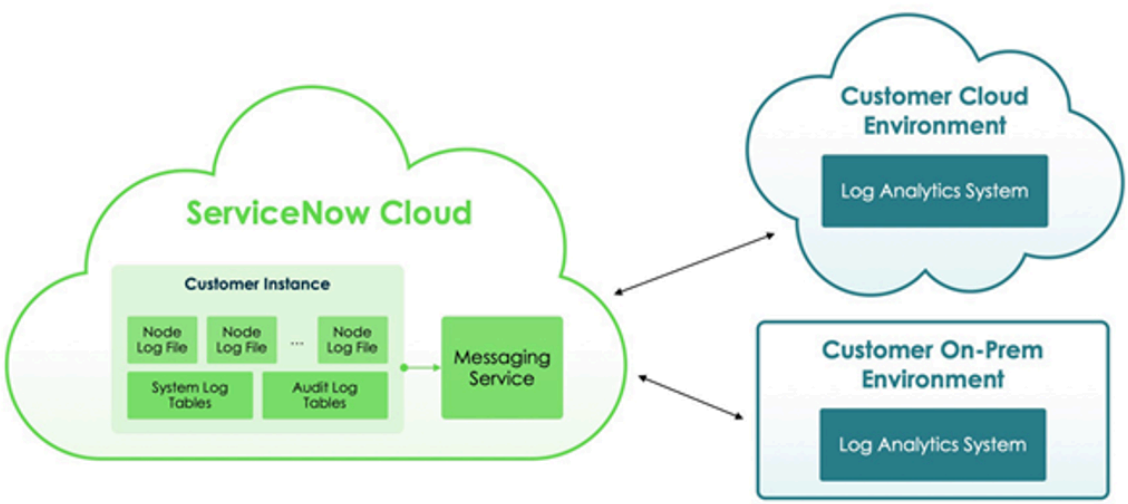
Log Export Service (LES)

Log Export Service (LES) vous permet d'exporter de manière transparente les journaux système et d'application de votre instance vers les outils d'analyse de sécurité de votre

entreprise. Le service fournit une intégration hautement évolutive et presque en temps réel avec vos outils d'analyse, qui est facile à configurer et à gérer.

L'outil d'intégration vous permet de tirer parti de vos solutions analytiques pour effectuer les opérations suivantes :

- Détecter ServiceNow les menaces de sécurité et analyser les incidents de sécurité
- Dépanner et optimiser les ServiceNow performances des applications
- Surveiller et optimiser l'expérience ServiceNow utilisateur



LES transmet une copie des événements de journal au fur et à mesure qu'ils sont générés au Service de messagerie Hermes .

Il Service de messagerie Hermes s'agit d'un service de transport et de mise en file d'attente de données multilocataire et multi-cluster qui Apache Kafka permet à votre instance de produire et d'utiliser de grands volumes d'événements Kafka. il s'agit Service de messagerie Hermes d'une option de la Now Platform disponible dans le cadre de Connexion au flux pour Apache Kafka, Log Export Service (LES) et Réplication de données d'instance (IDR).

Les systèmes d'analyse de journaux externes, dans le cloud ou sur site, peuvent utiliser et consommer les événements de journal du Service de messagerie Hermes . LES fournit trois options de connectivité pour consommer les journaux :

- Dédié Serveur MID: Un dédié Serveur MID est installé sur site ou dans le cloud qui se connecte Service de messagerie Hermes automatiquement, extrait les événements de journal en continu et les pousse ensuite vers des outils d'analyse de journaux via une connexion REST.
- Exploitez le connecteur Kafka à partir de votre solution d'analyse des journaux (par exemple, Splunk) : un connecteur Kafka du produit d'analyse des journaux de votre choix est installé sur site ou dans le cloud. Il s'y connecte Service de messagerie Hermes automatiquement, extrait les événements de journal en continu, puis les transfère vers des outils d'analyse des journaux.
- Directement à partir de votre système Kafka : votre système Kafka se connecte directement au Service de messagerie Hermes et utilise ses commandes et sa connectivité natives du protocole Kafka pour en extraire les événements de journal.

Traduction automatique

Pour configurer et gérer ERP, vous devez l'installer à partir de ServiceNow Store. L'application LES fournit 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.

Log Export Service rôles

Log Export Service est installé avec ces rôles.

Administrateur d'application [sn_logstoanalytics.admin]

Pour en savoir plus sur la gestion des abonnements par utilisateur, consultez et contactez votre représentant de compte.

Ce rôle est installé avec 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 élévation. Pour plus de détails, consultezÉlever à un rôle privilégié.

N°

Considérations particulières

Aucun.

Administrateur système [admin]

Pour en savoir plus sur la gestion des abonnements par utilisateur, consultez et contactez votre représentant de compte.

Le rôle administrateur est requis pour la configuration de l'application de la boutique LES.

Contient des rôles

Liste des rôles contenus dans le rôle.

- 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 élévation. Pour plus de détails, voir Élever à un rôle privilégié.

N°

Considérations particulières

Aucun.

Sources du journal

Log Export Service (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.

- Tables de journaux système
  - table syslog : affichez les avertissements et les erreurs pour les processus d'instance, les enregistrements et les événements non critiques, tels que l'utilisation de la mémoire sur l'ordinateur serveur
  - Table syslog_transaction : afficher toute l'activité du navigateur pour une instance
  - sys_outbound_http_log table : afficher toutes les demandes et réponses pour les services Web sortants tels que REST et SOAP
- Table d'audit : utilisez la vue de table sys_audit enregistrez les modifications apportées aux tables choisies pour être auditées
- Fichiers journaux du nœud d'application : utilisez les fichiers journaux localhost pour afficher les erreurs du nœud de l'application. Votre instance aura plusieurs nœuds, et chaque nœud aura plusieurs fichiers journaux.

Consultez Journaux système pour en savoir plus sur le schéma et le but des sources de journal ci-dessus.

Créer une configuration de source de journal

Régulez et définissez des filtres sur les journaux à transférer 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 nouvelle 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 journaux ○ Journal de nœud ○ Table Consultez Sources du journal pour plus d'informations.
Niveau de journal	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.

Champs	Description
	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 Hermès. Ils peuvent être envoyés au format JSON ou au format texte brut.
Table	Sélection de la table pour les journaux de type table. **Remarque :** Ce champ n’est visible que lorsque vous sélectionnez Table comme type de source.
Type de filtre	Conditions permettant de transférer les journaux de manière sélective. **Remarque :** Ce champ n’est visible que si vous sélectionnez syslog ou sys_audit comme table.

4. Sélectionnez **Soumettre** pour créer une nouvelle configuration source.

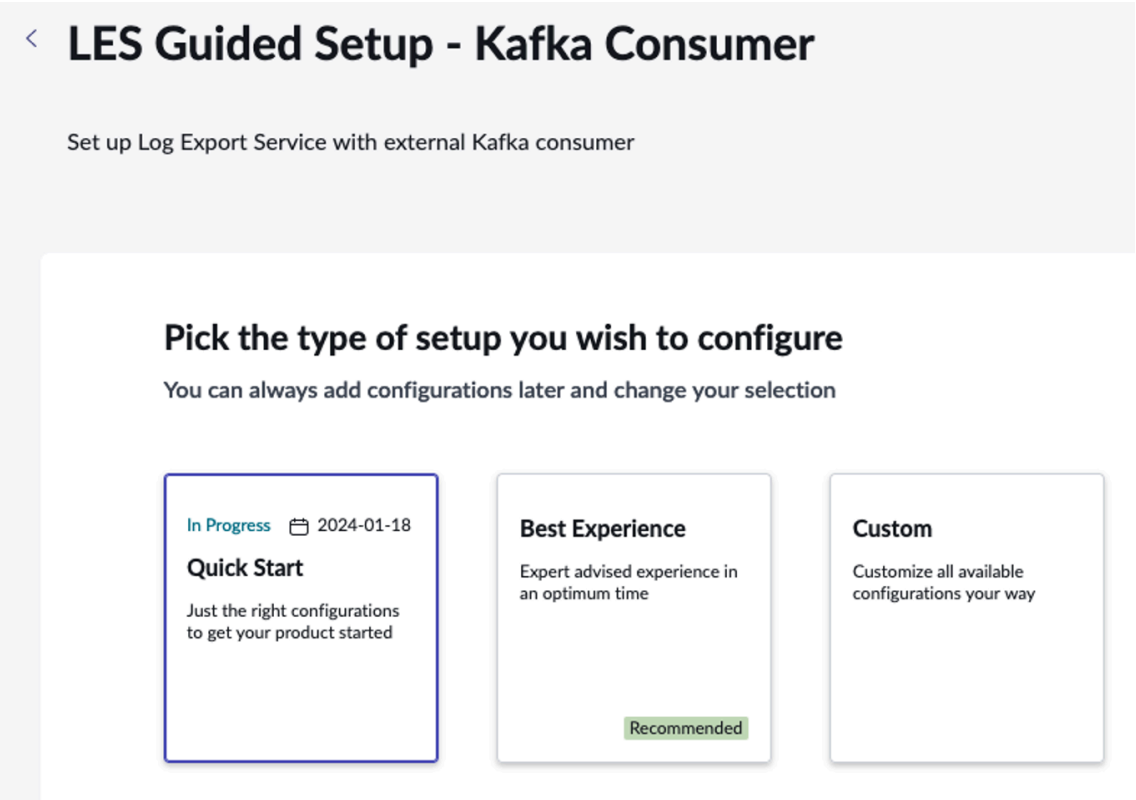
Consommateur Kafka

Utilisez la configuration guidée pour passer par la configuration initiale des LES. La configuration guidée vous aide à planifier le déploiement du produit et à effectuer la configuration de base pour la mise en service.

Guided Setup 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 conserve une trace de ce que vous avez terminé, de sorte que vous pouvez arrêter et recommencer là où vous vous étiez arrêté.

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 et sélectionner **Continuer** pour ouvrir les étapes de configuration guidée et commencer la configuration.

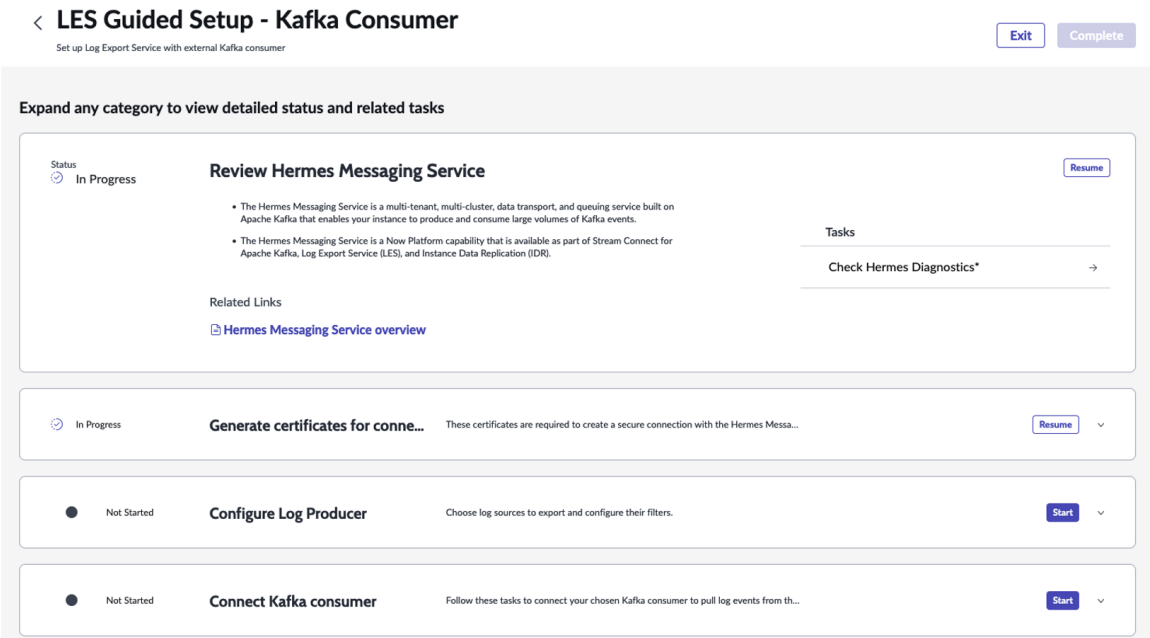


Les trois configurations de cette page, Démarrage rapide/Meilleure expérience/Personnalisé, fournissent les mêmes tâches et fonctionnalités. Il est nécessaire de coordonner l'intégration entre l'instance ServiceNow et l'outil d'analyse des journaux de destination avec l'administrateur respectif. L'administrateur de log analytics 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 log Set up a secure connection to the Hermes Messaging Service analytics à l'avance. Même si vous avez marqué une tâche comme terminée, vous pouvez revenir en arrière et la décocher à nouveau comme étant en cours. Pour ce faire, cliquez d'abord sur la zone **Modifier** dans le coin supérieur droit de la catégorie. Cliquez ensuite sur la zone **Modifier** de la tâche que vous souhaitez décocher. La case **Marquer comme terminée** ne sera plus marquée.

Page des catégories de configuration guidée

La page des catégories contient une vue d'ensemble et une description des catégories et des tâches associées. Vous pouvez cliquer sur la flèche déroulante pour afficher les informations sur la catégorie ou sur le bouton Démarrer pour ouvrir les étapes de configuration guidée et commencer la configuration.

Traduction automatique



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 cliquez sur **Continuer**.

Rôle requis : admin

Procédure

1. Passer en revue le service de messagerie Hermes : vérifiez les informations suivantes pour réussir les diagnostics Hermes.
   - Informations de configuration : les informations d'amorce suivantes sont utilisées pour se connecter à Hermes Messaging Service. Le « Producer Bootstrap » est la connexion utilisée pour envoyer des messages dans Hermes et le « Consumer Bootstrap 1 & 2 » est utilisé pour récupérer des messages dans Hermes.
     - Amorce du créateur
     - Amorce de consommateur 1
     - Amorce du 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 : cliquez sur **Exécuter le test** pour confirmer que le client externe est en mesure de se connecter aux ports d'instance définis (producteur et consommateur).

- Connectivité de l'instance : cliquez sur **Exécuter le test** pour confirmer que l'instance est en mesure d'envoyer et de recevoir des messages.
- Afficher les rubriques : cliquez sur la rubrique répertoriée pour récupérer l'horodatage du dernier message connu.

2. Générez des certificats pour une connexion sécurisée à Hermes Messaging Service et extrayez les événements de journal à partir de celui-ci.

   Vous allez utiliser ces certificats lors de la connexion de votre système externe.

   Établissez une connexion sécurisée à Service de messagerie Hermes. Consultez Set up a secure connection to the Hermes Messaging Service pour plus d'informations. Vous aurez besoin de ces certificats pour l'authentification et l'autorisation dans le client qui extraira les journaux d'Hermès.

   Remarque :
   Les rôles administrateur ou Hermes_admin sont requis pour cette étape.

3. Configurer le générateur de journaux : choisissez des sources de journaux à exporter et configurez leurs filtres.
   Effectuez les tâches suivantes pour configurer le générateur de journaux.

   - Configurer les sources de journal pour l'exportation : 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. Cliquez sur **Nouveau** dans le coin supérieur droit

     b. Sélectionner un type de source

     c. Sélectionnez les filtres appropriés pour le type de source sélectionné

     Remarque :
     Les filtres sont différents selon le type de source sélectionné

     d. Cliquez sur Mettre à jour.
     Une fois créée, elle 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 détermine si cette source de journal va être exportée ou non. Si vous voyez des erreurs, veuillez revenir à la tâche « Vérifier les diagnostics Hermes » et vérifier l'état Hermes.

   - Valider le créateur de journaux : une fois que vous avez créé une source à partir de laquelle produire des journaux, vous pouvez afficher les enregistrements de journaux en direct dans la rubrique à l'aide de **Service de messagerie Hermes** > **Inspecteur de rubrique Hermes**.

     a. Sélectionner des rubriques externes

     b. Cliquer sur Répertorier les rubriques

     c. Sélectionnez la ligne avec votre rubrique de l'étape précédente (répertoriée dans Sources)

d. Ajuster la date de début du message si nécessaire

e. Cliquez sur **Afficher** pour afficher un message de journal qui a été exporté vers la rubrique

4. Connecter le consommateur Kafka : procédez comme suit pour connecter le consommateur Kafka de votre choix afin d'extraire les événements de journal d'Hermes.

- Identifier le consommateur Kafka : deux options s'offrent à vous en fonction de votre architecture d'analyse des journaux.
  - Si vous avez votre propre système Kafka et que vous le choisissez pour l'agrégation de journaux, vous pouvez vous connecter directement à Hermes Messaging Service via le protocole Kafka natif.
  - Si vous choisissez de connecter votre outil d'analyse des journaux directement au service de messagerie Hermes, vous devez déployer un connecteur Kafka pris en charge par votre système d'analyse des journaux (c'est-à-dire Splunk Connect for Kafka).

  Remarque :
  Dans les deux cas, vous devez travailler avec l'administrateur pour que ces systèmes coordonnent la connexion avec le service de messagerie Hermes.

- Importer des certificats Hermes dans le système consommateur Kafka : connectez-vous à votre système grand public Kafka et assurez-vous que vous disposez des autorisations d'administrateur appropriées pour le configurer et le connecter à un système externe. Importez les certificats générés dans la tâche « Configurer une connexion sécurisée à 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'Hermès. Deux processus sont requis, car Hermes utilise une paire de grappes Kafka à des fins de basculement. Si une grappe tombe en panne, des données sont produites pour l'autre grappe Hermes Kafka.

  Dans votre système grand public Kafka, vous devrez créer deux processus consommateurs distincts pour vous connecter aux deux clusters Hermes Kafka. 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, ajoutez « snc.<instance name>. » à la rubrique vers laquelle les journaux sont transférés.
  - Configurez chaque consommateur avec le même ID de groupe de consommateurs Kafka.

- Installez vos fichiers keystore et truststore dans un emplacement auquel vos consommateurs peuvent accéder.
- Si vos consommateurs en ont besoin, 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 pouvez extraire les événements de journal à partir de Hermes Messaging Service.

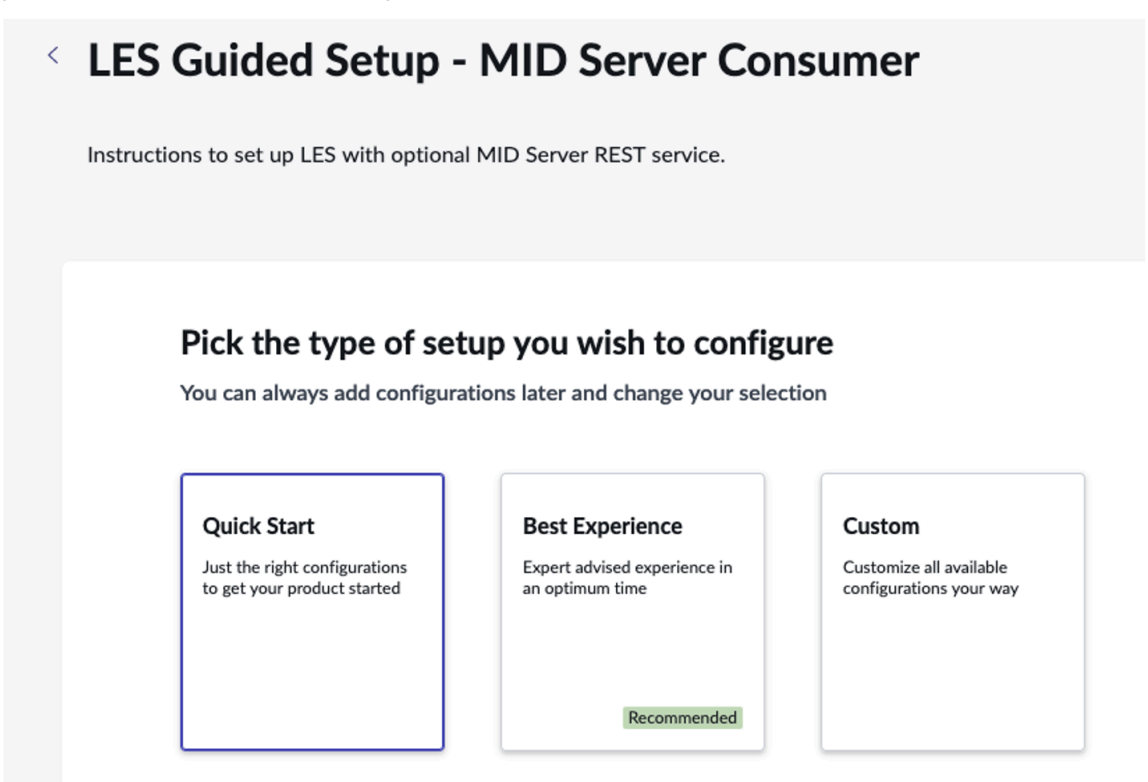
Consommateur de MID Server

Utilisez la configuration guidée pour passer par la configuration initiale des LES. La configuration guidée vous aide à planifier le déploiement du produit et à effectuer la configuration de base pour la mise en service.

Guided Setup 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 conserve une trace de ce que vous avez terminé, de sorte que vous pouvez arrêter et recommencer là où vous vous étiez arrêté.

Page d'accueil de la configuration guidée

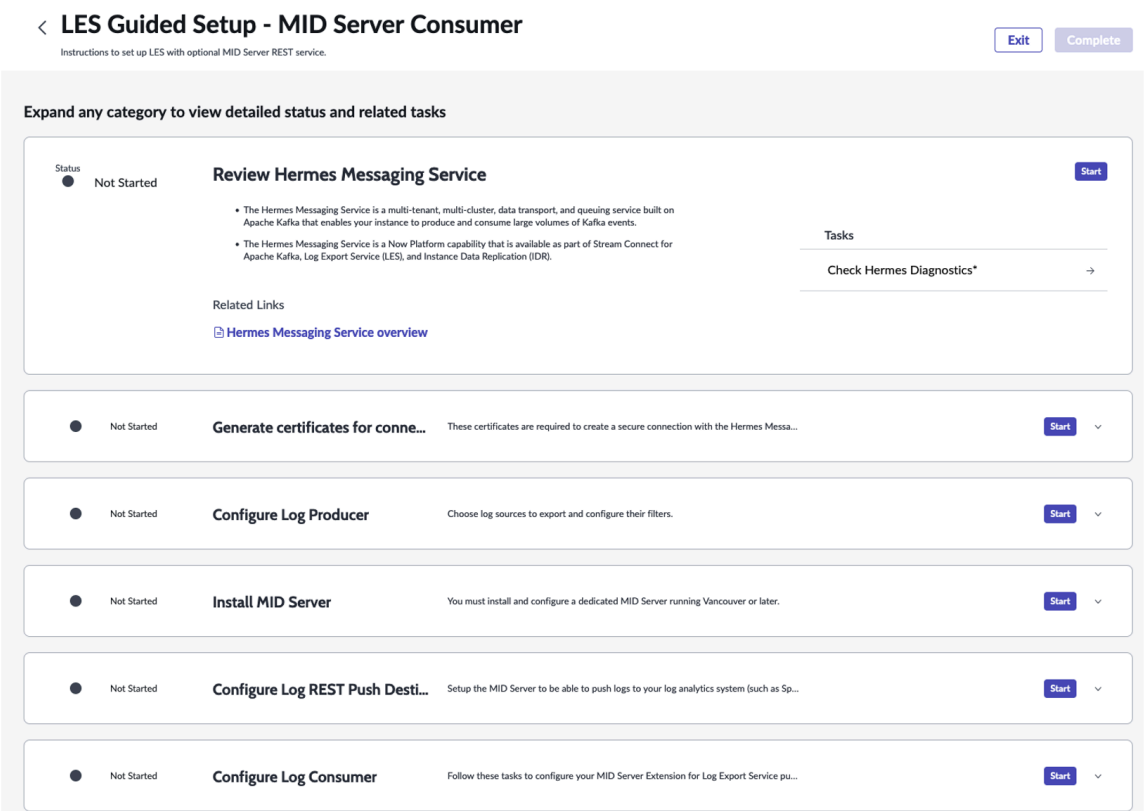
La page d'accueil de la configuration guidée contient une vue d'ensemble des types de configuration pour votre configuration guidée. Vous pouvez sélectionner votre type de configuration guidée et sélectionner **Continuer** pour ouvrir les étapes de configuration guidée et commencer la configuration.



Les trois configurations de cette page, Démarrage rapide/Meilleure expérience/Personnalisé, fournissent les mêmes tâches et fonctionnalités. Un MID Server dédié est nécessaire pour diffuser en continu les journaux de votre instance vers votre système d'analyse des journaux. Le MID Server 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 pour la remettre à l'état en cours. Pour ce faire, cliquez d'abord sur la zone **Modifier** dans le coin supérieur droit de la catégorie. Cliquez ensuite sur la zone **Modifier** de la tâche que vous souhaitez décocher. La case **Marquer comme terminé** ne sera plus marquée.

Page des catégories de configuration guidée

La page des catégories contient une vue d'ensemble et une description des catégories et des tâches associées. Vous pouvez cliquer sur la flèche déroulante pour afficher les informations sur la catégorie ou cliquer sur **Démarrer** pour ouvrir les étapes de configuration guidée et commencer la configuration.



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 cliquez sur **Continuer**.

Rôle requis : admin

Traduction automatique

Procédure

1. Passer en revue le service de messagerie Hermes : vérifiez les informations suivantes pour réussir les diagnostics Hermes.
   - Informations de configuration : les informations d'amorce suivantes sont utilisées pour se connecter à Hermes Messaging Service. Le « Producer Bootstrap » est la connexion utilisée pour envoyer des messages dans Hermes et le « Consumer Bootstrap 1 & 2 » est utilisé pour récupérer des messages dans Hermes.
     - Amorce du créateur
     - Amorce de consommateur 1
     - Amorce du 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 : cliquez sur **Exécuter le test** pour confirmer que le client externe est en mesure de se connecter aux ports d'instance définis (producteur et consommateur).
   - Connectivité de l'instance : cliquez sur **Exécuter le test** pour confirmer que l'instance est en mesure d'envoyer et de recevoir des messages.
   - Afficher les rubriques : cliquez sur la rubrique répertoriée pour récupérer l'horodatage du dernier message connu.
2. Générez des certificats pour une connexion sécurisée à Hermes Messaging Service et extrayez les événements de journal à partir de celui-ci.

   Établissez une connexion sécurisée à Service de messagerie Hermes. Consultez Set up a secure connection to the Hermes Messaging Service pour plus d'informations. Vous aurez besoin de ces certificats pour l'authentification et l'autorisation dans le client qui extraira les journaux d'Hermès.

   Remarque :
   Les rôles administrateur ou Hermes_admin sont requis pour cette étape.

3. Configurer le générateur de journaux : choisissez des sources de journaux à exporter et configurez leurs filtres.
   Effectuez les tâches suivantes pour configurer le générateur de journaux.
   - Configurer les sources de journal pour l'exportation : 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. Cliquez sur **Nouveau** dans le coin supérieur droit

     b. Sélectionner un type de source

     c. Sélectionnez les filtres appropriés pour le type de source sélectionné

     Remarque :
     Les filtres sont différents selon le type de source sélectionné

     d. Cliquez sur Mettre à jour

Une fois créée, elle 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 détermine 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 Hermes.

- Valider le créateur de journaux : une fois que vous avez créé une source à partir de laquelle produire des journaux, vous pouvez afficher les enregistrements de journaux en direct dans la rubrique à l'aide de **Service de messagerie Hermes** > **Inspecteur de rubrique Hermes**.

  a. Sélectionner des rubriques externes

  b. Cliquer sur Répertorier les rubriques

  c. Sélectionnez la ligne avec votre rubrique de l'étape précédente (répertoriée dans Sources)

  d. Ajuster la date de début du message si nécessaire

  e. Cliquez sur **Afficher** pour afficher un message de journal qui a été exporté vers la rubrique

4. Installer un MID Server : vous devez installer et configurer un MID Server dédié exécutant Vancouver ou une version ultérieure.
Effectuez les tâches suivantes pour installer le MID Server.

- Installez un MID Server dédié : le MID Server utilisé par le service d'exportation de journaux ne doit être dédié qu'à cette fin et n'est pas censé exécuter d'autres processus. Ceci est important pour garantir la livraison en temps opportun des messages de journal exportés vers votre point de terminaison REST. Vous pouvez installer le nouveau MID Server à l'aide de la commande 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.
- Valider le MID Server : vous devez valider manuellement le MID Server après son installation pour lui permettre d'exécuter des tâches d'automatisation. Pour valider le MID Server que vous dédiez pour LES, consultez Validate the MID Server

5. Configurer la destination push REST du journal : configurez le MID Server pour qu'il puisse transmettre les journaux par push à votre système d'analyse des journaux (tel que Splunk).
Effectuez les tâches suivantes pour configurer la destination push REST du journal.

- Ajouter des propriétés MID : vous devez ajouter des propriétés MID Server 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.location	<your_path>/<magasin de confiance>.p12
mid.les.kafka.ssl.keystore.location	<your_path>/<magasin de clés>.p12
mid.les.kafka.ssl.truststore.type	PKCS12
mid.les.kafka.ssl.keystore.type	PKCS12

Nom	Valeur
mid.les.kafka.client.id	<instance_name>
mid.les.kafka.group.id	snc.<instance_name>.group1
mid.les.kafka.bootstrap.servers	<instance_name>.<domaine> :4100,<instance_name>.<dom
mid.les.kafka.set2.bootstrap.servers	<instance_name>.<domaine> :4200,<instance_name>.<dom

Suivez ces notes pour savoir comment obtenir certaines des valeurs ci-dessus

- <password> 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 keystore et truststore que vous avez téléchargés. Les certificats doivent se trouver sur le serveur sur lequel vous exécutez le MID
- <instance_name>'agit du 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. Spécifier l'URL de votre point de terminaison souhaité pour les sources de journal exportées

d. Recherchez ou créez de nouvelles informations d'identification pour vous connecter à votre point de terminaison. Lors de la création d'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 livrons avec le script pré-écrit, **SplunkTransform** pour Splunk

6. Configurer le consommateur de journaux : suivez ces tâches pour configurer votre extension de serveur MID à des fins de service d'exportation de journaux.

◦ Configurer le contexte de consommateur LES : dans cette étape, vous allez mettre à jour l'enregistrement de consommateur LES à exécuter sur le MID Server dédié que vous venez d'installer pour le service d'exportation de journaux. Accédez à la **Serveur MID** > **Extensions** > **Contexte de consommateur LES** et mettez à jour l'enregistrement de consommateur LES en définissant les champs suivants :

- Cliquez sur « Consommateur LES » pour ouvrir l'enregistrement de contexte du Serveur MID.
- Sélectionner un MID Server spécifique pour le champ « Exécuter sur »
- Saisissez le nom du MID que vous avez validé à l'étape précédente pour le champ « Serveur MID »

Cliquez sur **Mettre à jour** pour enregistrer.

Remarque :
Nous livrons avec un contexte préconstruit. N'en créez pas un deuxième. Cela peut avoir des conséquences inattendues.

- Configurer le consommateur : créez un nouvel enregistrement de consommateur qui représente le processus qui fait partie de l'extension du 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 en spécifiant la rubrique Hermes à partir de laquelle récupérer les messages de journal et la destination vers laquelle les relayer.

  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

- Vérifier l'intégration du MID Server : accédez à **Service d'exportation de journaux (LES)** > **Consommateurs** et afficher les champs État et Détail de l'état de l'enregistrement défini. Les informations contenues dans ces champs signalent l'état actuel du processus en cours d'exécution sur le MID Server, y compris les erreurs éventuelles qui ont pu se produire lors du relais de messages au point de terminaison REST. #Si l'état du consommateur indique que le processus a démarré, vous devez 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 MID Server pour voir s'il existe des détails supplémentaires sur les erreurs qui peuvent être rencontrées. Vous pouvez également activer la journalisation de débogage sur le MID Server pour obtenir des informations supplémentaires si nécessaire.

Passer en revue l'exportation des journaux quotidiens par rapport source

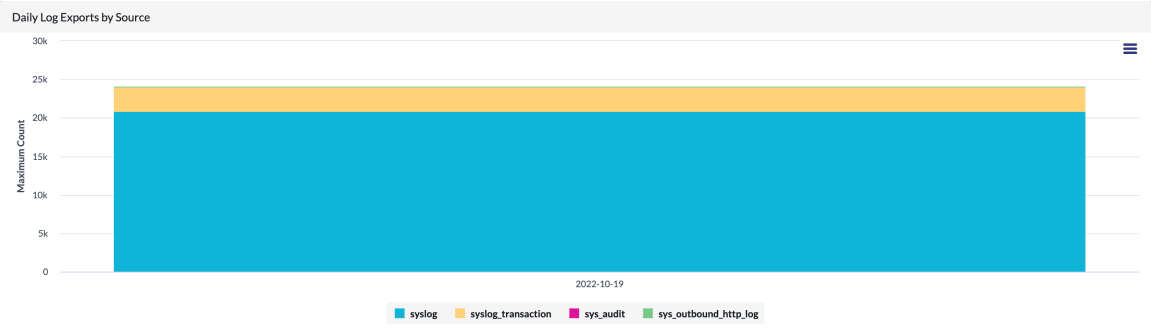
Analysez la taille de chaque source de journal de données en examinant le rapport d'exportation des journaux quotidiens par source. Le rapport indique le nombre d'événements de journal générés par chaque table de journal par jour.

Avant de commencer

Rôle requis : admin ou sn_logstoanalytics.admin

Procédure

1. Accédez à la **Tous** > **Service d'exportation de journaux** > **Exportation des journaux quotidiens par source**.
2. Passez en revue les décomptes quotidiens des journaux produits dans les tables suivantes par jour.
   - syslog
   - syslog_transaction
   - sys_audit
   - sys_outbound_http_log



En fonction de la taille des sources de données, vous pouvez décider de les inclure ou non dans le rapport d'exportation LES.

Remarque :
Vous pouvez sélectionner une barre à code couleur dans le graphique à rediriger vers le rapport d'agrégation quotidienne d'exportation de journaux, dans laquelle vous pouvez modifier les filtres pour analyser les données de manière plus approfondie. Vous pouvez réduire le nombre d'événements de journal à exporter par le service d'exportation de journaux en configurant des filtres de source de journal. Les fichiers journaux du nœud d'application ne sont pas inclus dans ce rapport.

Journalisation, audit et erreurs (renforcement de la sécurité de l'instance)

Appliquez une stratégie de journalisation et d'audit afin de pouvoir identifier les activités suspectes et intervenir en temps utile.

Pour en savoir plus sur ce qui peut être journalisé dans l'instance, reportez-vous à Journaux système. Assurez-vous qu'il existe un calendrier pour la surveillance des événements système tels que les connexions et les échecs de connexion à l'aide de **Journaux système** > **Events**.

Désactivation des messages d'erreur SQL (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour désactiver le *glide.db.loguser* rendu 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.

Attribut	Description
Risque de sécurité	(Moyen) Aucune information SQL sensible susceptible d'aider un attaquant ne doit apparaître dans le cadre d'un message d'erreur sur une page Web.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à 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.

Explorer

Découvrez les principales fonctionnalités et la valeur commerciale de Secrets Management.

Analyser

En savoir plus sur le tableau de bord Gestion des secrets.

Configurer	
	
Planifiez vos configurations principales.	

Exploration de 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.

Important :
Les administrateurs doivent avoir le rôle de voir les modules et les enregistrements associés à la gestion des secrets. Pour plus d'informations sur le rôle de gestion des secrets, reportez-vous à Rôles de gestion des secrets.

Choisissez parmi les versions Core et Enterprise de Gestion des secrets

Choisissez parmi Secrets Management Core et Secrets Management Enterprise en fonction des besoins de votre entreprise.

Gestion des secrets Core	Gestion des secrets Enterprise
Vous pouvez activer Secrets Management Core sur votre instance sans frais supplémentaires. Le module d'extension offre la possibilité d'utiliser des groupes 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.	Secrets Management 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 secrets en fonction de l'un de ces critères. ○ Périmètre ○ Table

Gestion des secrets Core	Gestion des secrets Enterprise
	◦ 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 de secrets configurés sur votre instance et en savoir plus sur les problèmes de sécurité potentiels. **Remarque :** Secrets Management Enterprise est un plug-in payant que ServiceNow le personnel doit activer sur votre instance de production.

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

Ces groupes s'appliquent à tous les secrets d'un champ d'application. Ces secrets sont déchiffrés par un module cryptographique commun et des politiques 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
- Enregistrement du filtre

Les groupes secrets de l'un ou l'autre type peuvent être rendus accessibles aux instances 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 publique et privée pour s'assurer que les secrets ne peuvent être déchiffrés que par le client. Lorsque vous créez un groupe de secrets accessibles au client, vous chargez la clé publique dans l'instance et conservez la clé privée sur votre MID Server. 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 Comprendre le côté client Gestion des secrets.

Utiliser des groupes secrets pour un contrôle plus granulaire

Bien que password2 soit disponible sur la ServiceNow plateforme, Secrets Management fournit ces fonctionnalités supplémentaires.

Contrôles d'accès granulaires	**Mot de passe 2** Avec password2, les administrateurs peuvent contrôler l'accès à un périmètre de l'application, mais ne peuvent pas restreindre l'accès aux éléments dans le périmètre. **Gestion des secrets** Avec Gestion des secrets, les administrateurs peuvent restreindre l'accès en fonction de critères qu'ils définissent. Les types de critères peuvent être basés sur des critères tels que le package, la table ou la colonne.
Stockage sécurisé	Pour les groupes secrets côté client, 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 les politiques d'accès au module à vos groupes

Une fois que vous avez regroupé vos secrets dans un groupe secret, vous pouvez appliquer des politiques qui déterminent comment vous pouvez accéder à ces secrets au niveau d'un groupe. Les politiques d'accès aux modules sont les mécanismes de contrôle d'accès que vous appliquez aux modules de chiffrement pour définir des contrôles au niveau de l'instance, tels qu'un délai de validité de la clé de chiffrement. Pour plus d'informations sur les politiques d'accès au module, consultez Vue d'ensemble de la politique d'accès au module.

Tables installées avec Secrets Management

La gestion des secrets ajoute ou modifie ces tables.

Nouvelles tables	
[sn_sm_secret_group]	Stocke les groupes secrets
[sn_sm_secret_group_criteria]	Stocke les groupes secrets de critères
[sn_sm_secrets]	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 d'un type de module cryptographique. (Module cryptographique d'identité ou module cryptographique de groupe secret)

[sys_kmf_module_key]	• Stocke la clé de chiffrement secrète conceptuelle (sans matériau de clé) • Stocke la clé publique d'identité
[sys_kmf_crypto_caller_policy]	Ajout d'un nouveau type de politique d'accès au module

Comprendre le côté client Gestion des secrets

Découvrez comment gérer l'accès Gestion des secrets aux secrets et aux groupes.

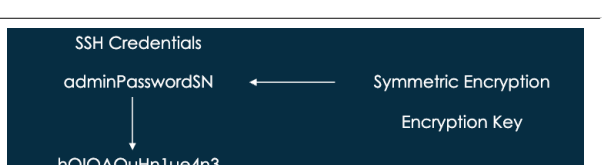
Terminologie

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 utiliser les termes de chiffrement suivants.

Terme	Description
Chiffrement symétrique	Le chiffrement symétrique utilise une seule clé identique 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 un texte chiffré illisible.
Chiffrement asymétrique	Le chiffrement asymétrique utilise deux clés, l'une pour chiffrer et l'autre pour déchiffrer.
Clé publique	La clé publique est la moitié de la paire de clés asymétrique. Cette clé est stockée sur votre instance, qui utilise la clé 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 MID Server. ServiceNow n'a pas accès à cette clé. Combinée à la clé publique, la paire de clés asymétrique est utilisée pour déchiffrer vos secrets.

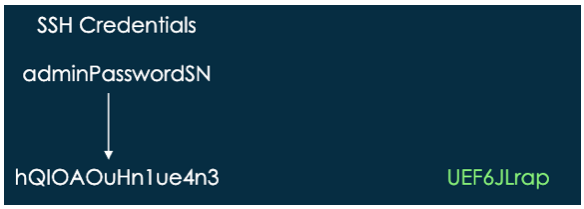
Processus de chiffrement côté client

Une clé symétrique chiffre des informations d'identification (dans ce cas, un mot de passe administrateur), les faisant passer de texte clair lisible à un texte chiffré chiffré.

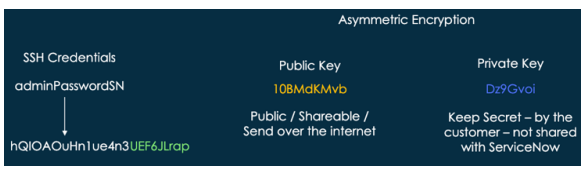


Traduction automatique

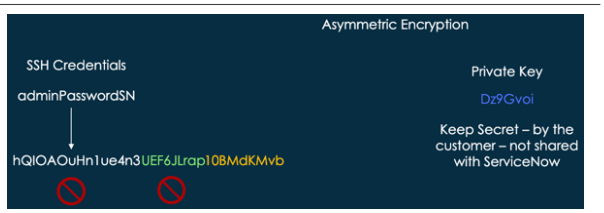
La clé symétrique (représentée en vert) peut être appliquée aux informations d'identification pour les chiffrer ou les déchiffrer.



À ce stade, le chiffrement asymétrique commence à utiliser des clés publiques (jaunes) et privées (bleues).



La clé publique chiffre les informations d'identification avec 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 le déchiffrer.



Après avoir été chiffrée avec la clé publique, la clé privée est nécessaire pour déchiffrer les informations d'identification. Étant donné que seul le client possède cette clé, il est le seul à pouvoir accéder aux informations d'identification chiffrées.

Configurer les 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 proxy, 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 qu'un MID Server est configuré sur votre réseau local. Pour plus d'informations sur ce processus, reportez-vous à 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 de 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 MID Server à ce groupe d'identités.

4. **Créer des informations d'identification et tester le chiffrement des informations d'identification**

Créez des informations d'identification pour vous authentifier dans un système tiers et testez-le qui ServiceNow ne peut pas accéder aux informations d'identification.

5. **Charger la paire de clés publique/privée sur le MID Server**

   Chargez votre paire de clés publique/privée sur votre MID Server. Cette paire de clés permet au MID Server de gérer les demandes d'authentification provenant de votre instance.

6. **Configurer Flow Designer pour gérer l'intégration**

   Sur votre instance, utilisez Concepteur de flux pour gérer une intégration entre votre réseau local et votre instance.

7. **Tester l'intégration des secrets chiffrés côté client de bout en bout**

   Testez votre intégration et passez en revue les détails d'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 de 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 dans lequel vous souhaitez stocker vos clés de chiffrement.
3. À l'aide du terminal, saisissez les informations suivantes :

   ```
   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 substituer d'autres outils comparables en fonction de vos besoins.

   La commande génère une clé privée et un certificat public (avec la clé publique correspondante). Vous trouverez ci-dessous une série d'invites pour obtenir les informations requises, 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 (p. ex., ville)
   - Nom de l'organisation (p. ex., société)
   - Nom de l'unité organisationnelle (p. ex., section)
   - Nom commun (p. ex., nom d'hôte complet)
   - Adresse e-mail

   Collaborez avec votre équipe de sécurité pour vous assurer de saisir les informations de certificat correctes.

```
Country Name (2 letter code) []:US
State or Province Name (full name) []:CO
Locality Name (eg, city) []:Boulder
Organization Name (eg, company) []:ServiceNow
Organizational Unit Name (eg, section) []:Product Management
Common Name (eg, fully qualified host name) []:fake@servicenow.com
Email Address []:fake@servicenow.com
```

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 en un seul fichier à charger dans votre MID Server lors des étapes ultérieures.
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 : aucun

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 pouvoir l'utiliser. Lorsque vous utilisez un certificat provenant d'une autorité de certification, vous n'avez pas besoin d'effectuer cette étape.

Procédure

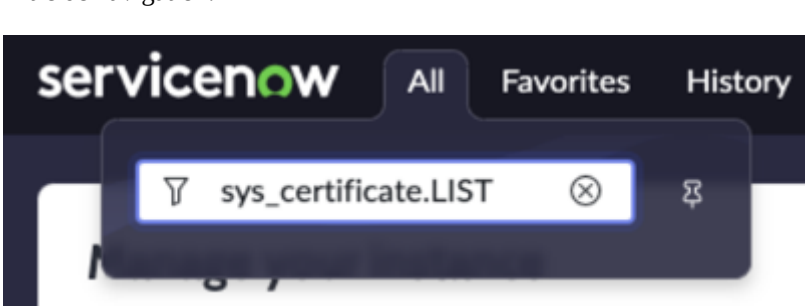
1. Dans votre environnement local, ouvrez Terminal (sur Mac ou Linux) ou Ligne de commande (sous Windows).
2. À l'aide du terminal, utilisez `cd` pour accéder au dossier dans lequel vous avez créé vos clés de chiffrement.

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.

4. Copiez les informations du certificat dans votre presse-papiers.
   Commencez par la ligne `-----BEGIN CERTIFICATE -----` et incluez-la et terminez par la ligne `-----END CERTIFICATE -----` et incluez-la.
5. Sur votre ServiceNow instance, accédez à la liste des **certificats X.509** en entrant `sys_certificate. LIST` dans le filtre de navigation.



6. Sélectionnez **Nouveau** pour créer un enregistrement de **certificat X.509** .
7. Renseignez les champs suivants du formulaire.

Traduction automatique

Champs de certificat X.509

Champ	Valeur
Nom	Nom du certificat. Ce nom peut être n'importe quel nom que vous choisissez.
Format	Sélectionner **PEM** **Remarque :** Les fichiers PEM (Privacy Enhanced Mail) sont un type de fichier PKI (Public Key Infrastructure) 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 du magasin de confiance**
Description courte	Description du certificat. Entrez une valeur qui vous permet de savoir à quoi sert ce certificat.
Certificat PEM	Collez les informations de certificat que vous avez copiées à l'étape 4.

8. Sélectionnez **Envoyer** 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. Ensuite, associez votre groupe de secrets à un groupe d'identités, puis ajoutez votre MID Server à ce groupe d'identités.

Avant de commencer

Rôle requis : admin, KMF_admin

Procédure

1. Accédez à la **Tous** > **Gestion des secrets** > **Groupes secrets avec critères**.
2. Sélectionnez **Nouveau** pour créer un **groupe secret avec enregistrement de critères** .
3. Renseignez les champs suivants du formulaire.

Groupe secret avec champs de critères

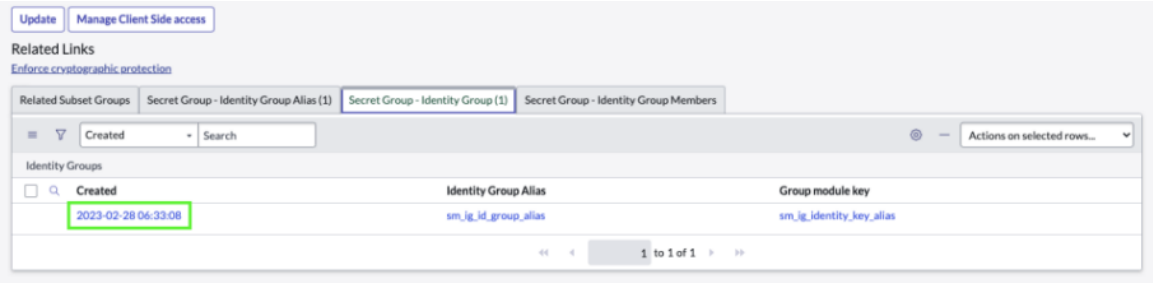
Champ	Valeur
Nom de groupe	Nom du groupe secret. Ce nom peut être n'importe quel nom que vous choisissez.
Type de secret	Sélectionner **Client accessible**
Module de génération automatique	Cochez la case
Description brève	Description du groupe secret. Entrez une valeur qui vous permet de savoir à quoi sert ce groupe.

Champ	Valeur
Type de critère	**Sélectionner une table cible**
Table cible	**Sélectionner les informations d'identification SSH [ssh_credentials]**

4. Cliquez avec le bouton droit sur l'en-tête du formulaire et sélectionnez **Enregistrer** dans le menu contextuel pour sauvegarder 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 **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** , saisissez une valeur.
   Ce nom peut être la valeur de votre choix.
10. Sélectionnez **Envoyer**.
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 tout ce que vous voulez, mais elle doit correspondre exactement à ce que vous insérez dans le MID Server dans les étapes ultérieures.

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 certificats sont importés avec succès dans la bannière de l'instance** , confirmant une importation réussie.
18. Sélectionnez **Envoyer**.
    La liste **des groupes d'identité** s'affiche.
19. Cochez la case située à gauche de votre enregistrement de groupe d'identité dans la liste.
20. Sélectionnez le bouton **Associer un groupe secret** .
    Vous êtes renvoyé à votre **groupe secret avec l'enregistrement de critères** . Les listes connexes **Groupe secret – Alias de groupe d'identité** et **Groupe secret – Groupe d'identité** 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'identité** , sélectionnez le champ **Créé** pour l'enregistrement de cette liste.



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'identité** s'affiche.
23. Dans le champ Table des **membres**, sélectionnez **MID Server [ecc_agent].**
24. Sélectionnez l'icône de référence ( ) en regard du champ **d'enregistrement Membre du groupe d'identité** , puis sélectionnez votre MID Server.

> **Remarque :**
> Si vous activez la case à cocher **Inclure tous les enregistrements** , tous les MID Servers connectés à votre instance sont ajoutés au groupe d'identités.

25. Sélectionnez **OK** pour fermer la fenêtre **Sélectionner le document** .
26. Sélectionnez **Envoyer**.
27. Revenez 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.

Créer des informations d'identification et tester le chiffrement des informations d'identification

Créez des informations d'identification pour vous authentifier dans un système tiers et testez-le qui ServiceNow ne peut pas accéder aux informations d'identification.

Avant de commencer

Rôle requis : admin

Procédure

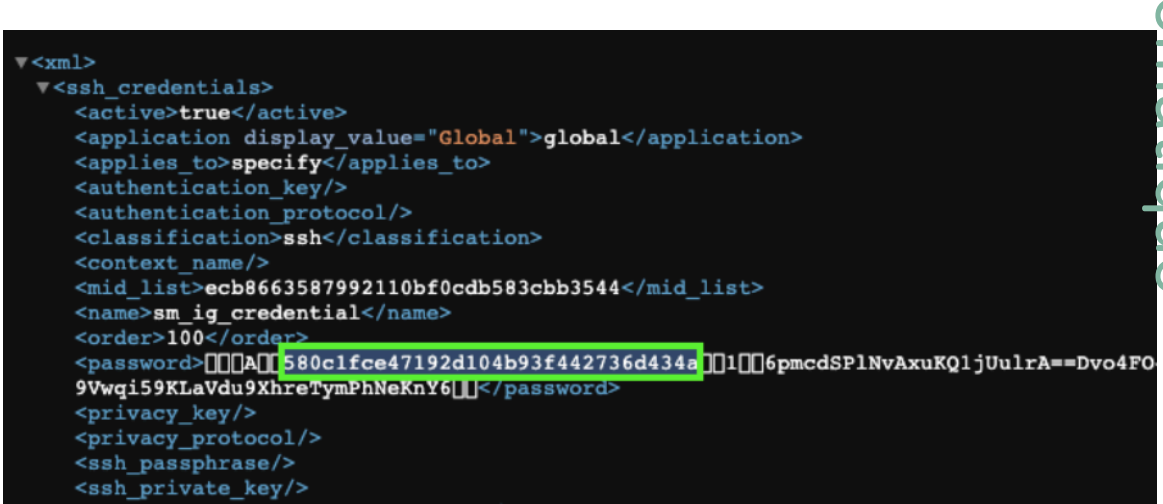
1. Accédez à la liste **des informations d'identification SSH** en saisissant `ssh_credentials.list` dans le filtre de navigation.
2. Sélectionnez **Nouveau** pour créer un enregistrement **d'informations d'identification SSH** .
3. Renseignez les champs suivants du formulaire.

Formulaire Informations d'identification SSH

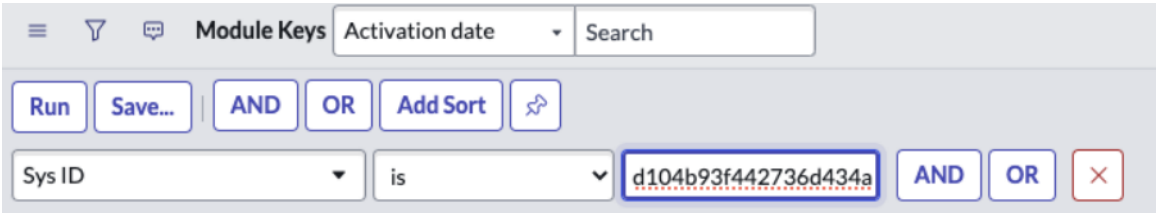
Champ	Valeur
Nom	Saisissez un nom pour votre enregistrement d'informations d'identification. Ce nom peut être la valeur de votre choix.

Champ	Valeur
Concerne	**Sélectionner des MID Servers spécifiques**
Serveurs MID	Sélectionnez votre MID Server.
Nom d'utilisateur	Entrez le nom d'utilisateur.
Mot de passe	Saisissez 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. Saisissez un nom dans le champ **Nom** .
8. Sélectionnez **Informations d'identification** dans le champ **Type** .
9. Sélectionnez **Envoyer**.
   Vous êtes renvoyé à l'enregistrement **des informations d'identification SSH** . Dans les étapes suivantes, vous vérifiez que les informations d'identification sont chiffrées.
10. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Afficher le code XML**.
11. Recherchez la balise XML <password> dans le fichier XML.
12. Copiez le sys_id de cette balise <mot de passe> dans votre presse-papiers.
    Le sys_id est un code de 32 caractères qui représente 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 zones sur cette même ligne.



13. Accédez à la liste **Clés de module** en saisissant sys_kmf_module_key.list dans le filtre de navigation.
14. Filtrez la liste pour les enregistrements où le champ **ID** système correspond au 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 une clé symétrique et que vous l'utilisez.

15. Accédez à la liste **Clés de module encapsulées** en saisissant `sys_kmf_wrapped_module_key.list` dans le filtre de navigation.
16. Filtrez la liste pour les enregistrements où le champ **Module de chiffrement** correspond au module de chiffrement que vous avez créé lors des étapes précédentes, puis sélectionnez **Exécuter**.
    Votre recherche doit renvoyer un seul enregistrement **de clé de module encapsulée** . Dans cette liste, vous pouvez vérifier les éléments suivants :
    - La colonne **Matériau de clé encapsulée** indique que la clé symétrique dans le module de chiffrement (utilisé pour chiffrer les informations d'identification SSH) est chiffrée par la clé publique que vous avez chargée dans le groupe d'identités.
    - Le champ **ID système de clé encapsulée** indique que c'est la clé (la clé symétrique du module de chiffrement) qui est chiffrée par l'ID système de la **clé encapsulée** (la clé publique chargée dans le groupe d'identités).

    Remarque :
    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** ( ).

Charger la paire de clés publique/privée sur le MID Server

Chargez votre paire de clés publique/privée sur votre MID Server. Cette paire de clés permet au MID Server de traiter 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 MID Server tente d'utiliser ces informations d'identification chiffrées, il ne peut pas déchiffrer les informations d'identification pour l'authentification sans accéder à la clé privée.

Au fil de ces étapes, vous allez charger la clé privée sur le MID Server pour compléter le trousseau public/privé. Ce chargement accorde l'accès au MID Server sans donner d'accès ServiceNow .

Pour accorder au MID Server l'accès à la clé privée, vous devez construire une commande à exécuter en tant qu'administrateur dans Powershell. Dans cet exemple, la commande est destinée à l'ordinateur virtuel Windows Azure.

Important :

Assurez-vous que le système sur lequel vous effectuez ces étapes a accès à la fois au MID Server et au fichier de paire de clés.

Procédure

1. Dans votre environnement local, localisez le dossier dans lequel vous avez créé votre paire de clés au Créer des clés de chiffrement et un certificat cours des étapes.
2. Recherchez et copiez le chemin d'accès complet au fichier `manage-certificates.bat` .

   Remarque :
   Ce fichier se trouve dans votre dossier MID Server. Selon l'endroit où vous avez stocké votre dossier MID Server, 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\manage-certificates.bat
   ```

3. Créez un fichier texte et collez le chemin d'accès 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 indiqués 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__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manage-certificates.bat -a your_identity_key_alias
    C:\Users\<your_user_account>\Desktop\sm_keypair_bundle.pem
   ```

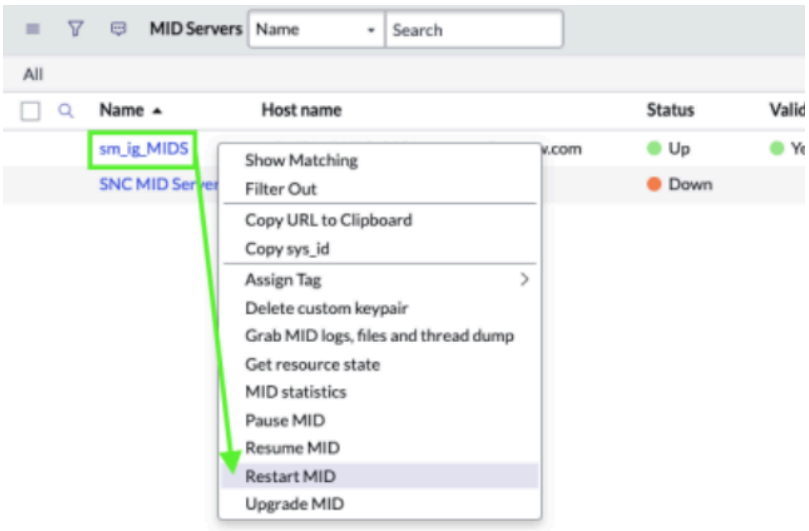
   Remarque :
   Dans cet exemple, le fichier `sm_keypair_bundle.pem` se trouve sur le bureau pour raccourcir le chemin d'accès.

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.
   ```

   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 MID Server en accédant à votre enregistrement de MID Server, cliquez avec le bouton droit sur l'enregistrement et sélectionnez **Redémarrer MID.**



Le redémarrage du MID Server synchronise la paire de clés chargée dans le magasin de clés MID pour l'utiliser avec les opérations. Attendez que le MID Server redémarre avec l'état **Actif** et la valeur validée **Oui** avant de continuer.

Configurer Flow Designer pour gérer l'intégration

Sur votre instance, utilisez Concepteur de flux pour gérer une intégration entre votre réseau local et votre instance.

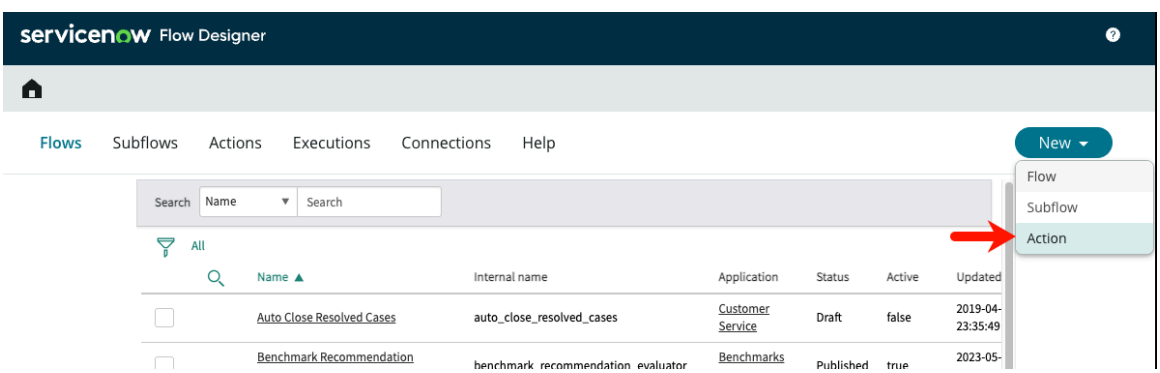
Avant de commencer

Rôle requis : admin

Au fil de ces étapes, vous allez créer un Concepteur de flux workflow pour créer un fichier texte sur votre système local.

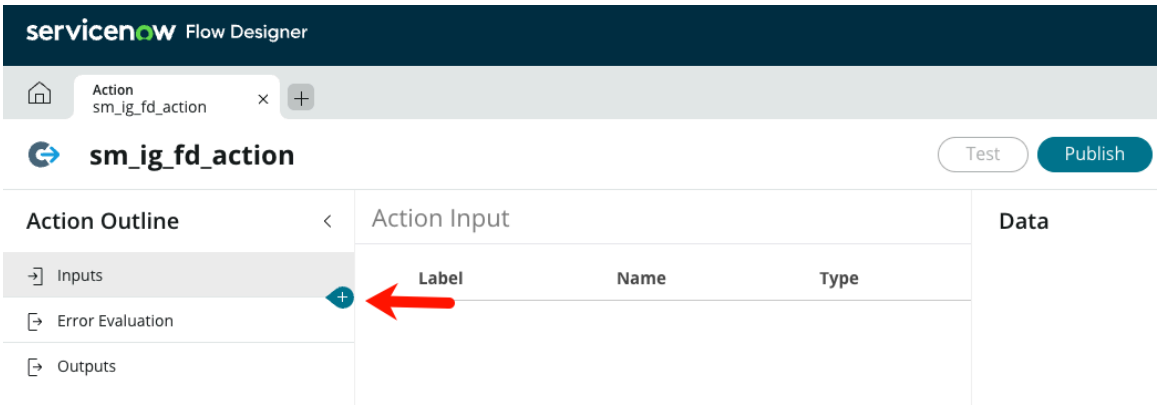
Procédure

1. Sur votre instance, accédez à **Tous** > **Automatisation des processus** > **Concepteur de flux**.
2. Créez une action dans ServiceNow en sélectionnant **Nouveau** , puis **Action**.

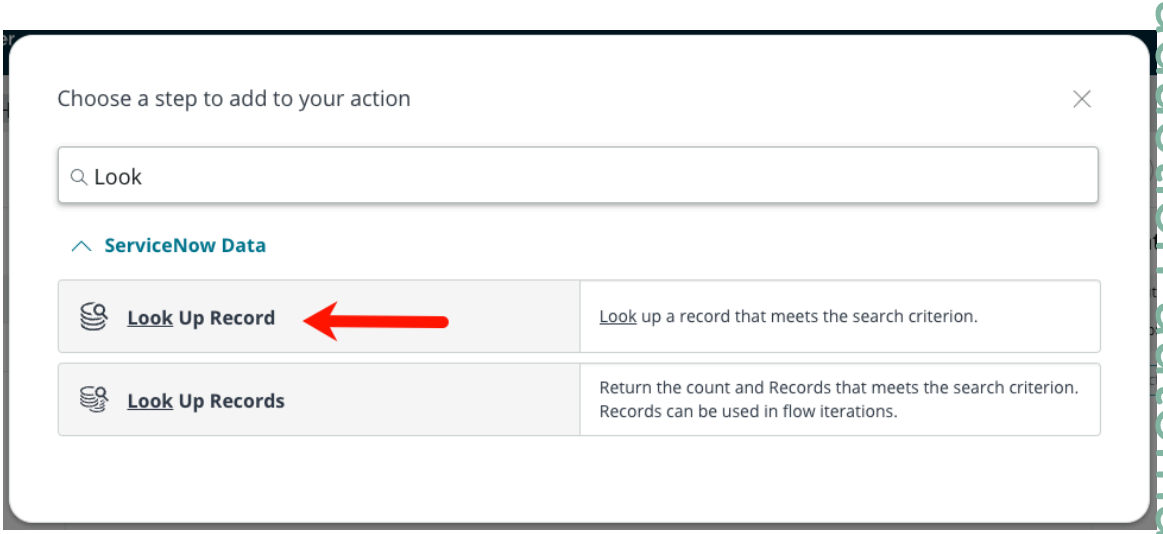


3. Saisissez un nom dans le champ **Nom de l'action** , puis sélectionnez **Soumettre**.

4. Créez une étape en sélectionnant le signe plus entre **Entrées** et **Évaluation de l'erreur** dans Plan **d'action**.



5. Dans la fenêtre **Choisir une étape à ajouter à votre action** , sélectionnez **Rechercher un enregistrement**.



6. Dans la section de **l'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 action** , sélectionnez **SSH**.

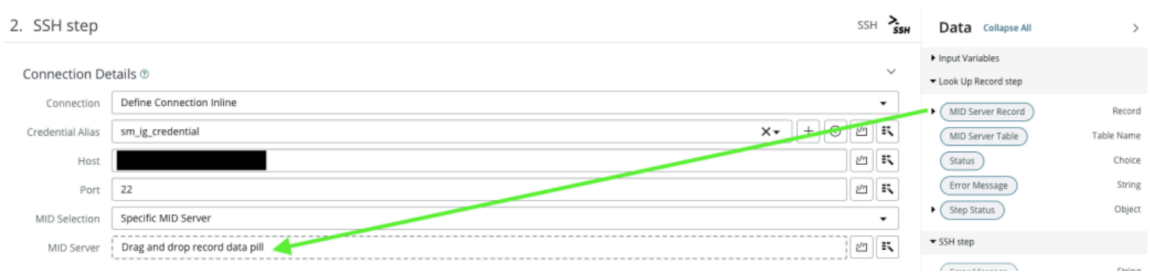
> **Remarque :**
> Si vous ne voyez pas l'option **SSH** , vous devez activer le module d'extension requis.

9. Dans la section **Étape SSH** , entrez 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 pour les informations d'identification SSH qui ont été créées lors des étapes précédentes.

Champ	Valeur
Hôte	Entrez l'adresse IP de l'hôte auquel vous vous connectez via SSH.
Port	Entrez 22.
Sélection de MID	**Sélectionnez un MID Server spécifique**.

10. Pour remplir le champ **MID Server** , faites glisser la pastille **d'enregistrement MID Server** de la section **Données** à droite vers le champ.



Avertissement :
Lorsque vous faites glisser la pilule dans le champ, sélectionnez la pilule et non la flèche noire à gauche de la pilule.

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 MID Server. Le MID Server accorde l'accès à l'instance ServiceNow (via Concepteur de flux) 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 et l'heure de création du fichier texte.

12. Sélectionnez le bouton **Enregistrer** dans le coin supérieur droit de l'écran pour enregistrer le workflow.

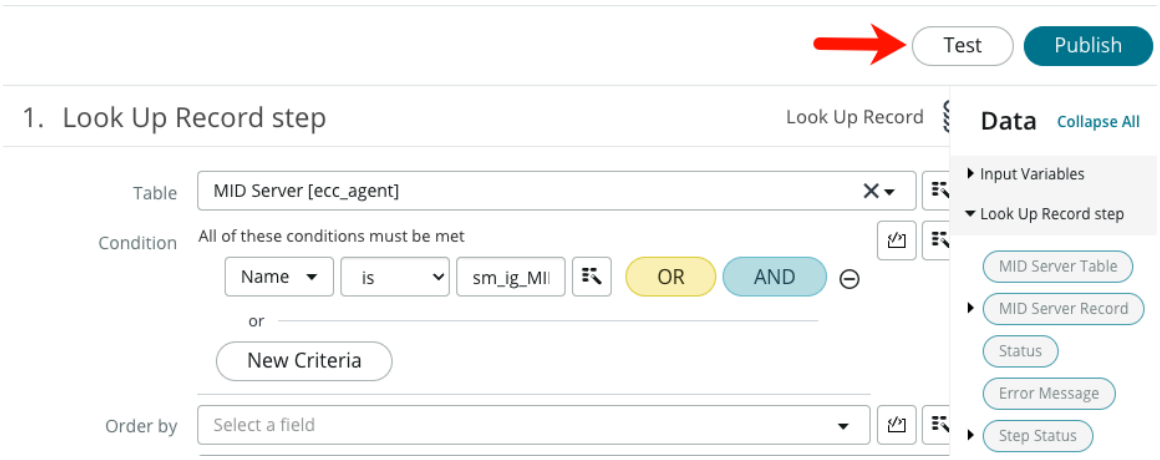
Tester l'intégration des secrets chiffrés côté client de bout en bout

Testez votre intégration et passez en revue les détails d'exécution pour confirmer que votre configuration fonctionne.

Avant de commencer
Rôle requis : admin

Procédure

1. Dans Concepteur de flux sélectionnez le bouton **Test** dans le coin supérieur droit de l'écran.



2. Dans la fenêtre Action du **test** , sélectionnez **Exécuter le test**.
3. Sélectionnez **L'exécution de votre test est terminée. Affichez les détails d'exécution de l'action.**
4. Actualisez votre écran jusqu'à ce que vous **voyiez Exécution du test - Terminé** dans le coin supérieur droit de l'écran.
5. Sélectionnez la flèche **Étapes** en bas à gauche de l'écran.
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 Concepteur de flux, assurez-vous que votre fichier texte a été créé dans votre système local.

Tableau de bord de gestion des secrets

Utilisez le tableau de bord de gestion des secrets pour examiner les groupes de secrets configurés sur votre instance et en savoir plus sur les problèmes de sécurité.

Vue d'ensemble du groupe secret

L'onglet **Vue d'ensemble des groupes secrets** affiche des informations sur vos groupes secrets configurés. Utilisez cet onglet pour afficher des informations sur les groupes secrets configurés sur votre instance.

Groupe secret par type

Affiche un graphique circulaire montrant les groupes secrets installés sur votre instance, regroupés par type de secret (côté instance du côté client).

Groupe secret par type de critère

Affiche un graphique à secteurs montrant les groupes secrets avec des critères configurés sur votre instance selon le type de critères utilisés.

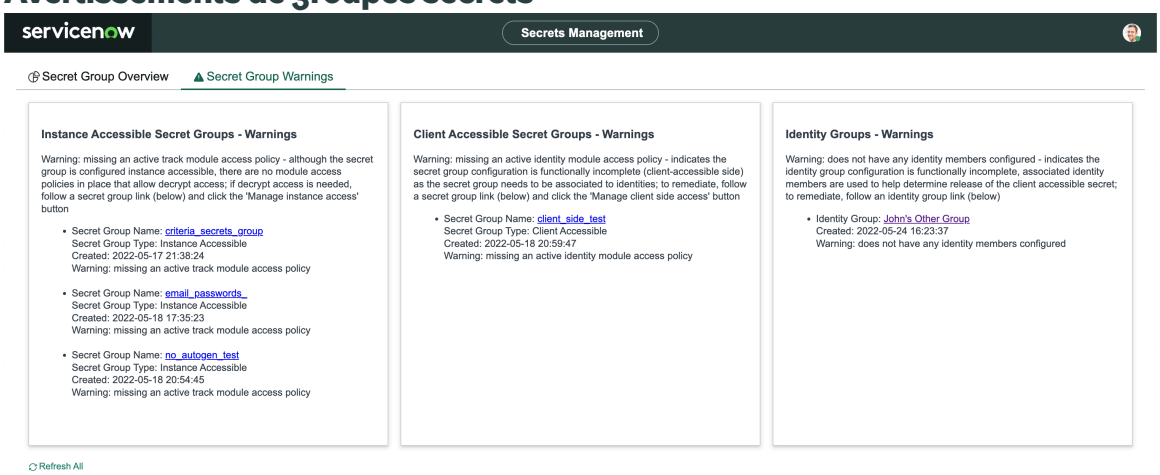
Nombre de groupes secrets inactifs

Affiche un nombre de groupes secrets inactifs configurés sur votre instance.

Nombre de secrets dédiés

Affiche un nombre de secrets dans les groupes secrets de base.

Avertissements de groupes secrets



L'onglet Avertissements de groupe secret affiche les avertissements relatifs à vos groupes secrets et groupes d'identité.

Groupes secrets accessibles aux clients - Avertissements

Cette carte affiche des avertissements s'il existe des groupes secrets pour lesquels aucune politique d'accès active n'est 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 au client qui n'ont pas de politique d'accès au module d'identité (MAP) active. Sélectionnez un nom de groupe secret pour afficher cet enregistrement.

Groupes d'identité - Avertissements

Cette carte affiche des avertissements s'il existe des groupes d'identité qui n'ont pas de membres configurés. Sélectionnez le nom du groupe d'identité pour afficher l'enregistrement.

Remarque :
Le tableau de bord de gestion des secrets fait partie de Secrets Management Enterprise. Secrets Management Enterprise est un plug-in 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 de secrets [sn_secrets.admin]

Affectez des rôles de secrets non-administrateurs à d'autres utilisateurs. Les administrateurs de secrets ont les mêmes privilèges que le gestionnaire et le visionneur de 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 particulières

Important :
Évitez d'accorder un rôle d'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 administrateur lorsque des rôles plus ciblés sont disponibles.

Gestionnaire de secrets [sn_secrets.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 des accès et d'autres informations sur l'activité d'utilisation
- Créer des filtres et des groupes secrets
- Créer des fournisseurs de secrets
- Déplacer les secrets entre les groupes secrets
- Modifier les paramètres de groupe secret et de fournisseur secret

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

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 les enregistrements de groupes secrets et 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 particulières

Aucun.

Créer un module cryptographique de groupe secret

Créez un module de chiffrement de groupe secret pour effectuer le chiffrement et le déchiffrement.

Avant de commencer

Rôle requis :

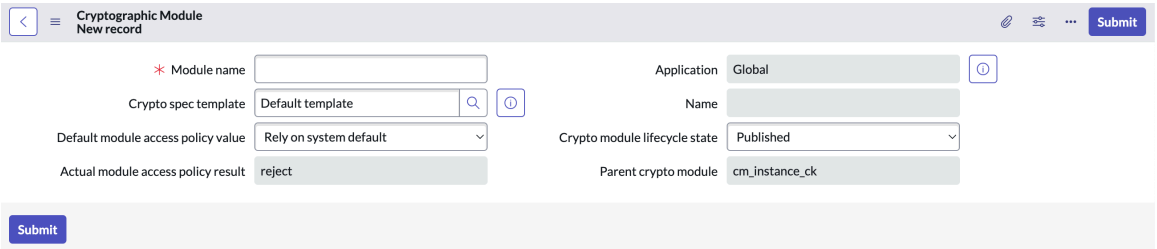
- administrateur
- sn_secrets.admin
- sn_secrets.secret_manager
- sn_kmf.cryptographic_manager
- sn_kmf.admin

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.

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 au client	Créez des secrets clients accessibles qui sont chiffrés à l'aide de votre propre clé, qui ServiceNow ne peut pas accéder.

3. Renseignez les champs du formulaire **Module de chiffrement** .



Champ	Description
Nom du module	Nom descriptif pour votre module
Application	Le périmètre de l'application qui contient votre module. Ce champ est automatiquement rempli 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	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	Le module de chiffrement parent, qui est déterminé par le type de module de chiffrement que vous avez sélectionné à l'étape précédente. Ce champ est en lecture seule.

4. Sélectionnez **Envoyer**.

Créer un groupe secret de base

Créez un groupe secret de base pour regrouper tous les secrets, quels que soient leurs critères.

Avant de commencer

Rôle requis : admin

Les groupes secrets de base peuvent contenir n'importe quel secret que vous y ajoutez, indépendamment de leur table, de leur périmètre ou de leur application. Après l'avoir créé, vous ajoutez manuellement des secrets au groupe. Pour créer un groupe spécifique pour tous les secrets qui partagent un attribut commun tels que ceux-ci, 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. Remplissez les champs du formulaire **Groupe secret** .

Champs de groupe secret

Champ	Description
Nom de groupe	Nom du 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 **au client**.
Module de génération automatique	Génère un nouveau module de chiffrement pour ce groupe secret. Ce module crypte et décrypte 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 courte	Description du groupe
Module de chiffrement	Sélectionnez le module de chiffrement à utiliser avec ce groupe. Ce module crypte et décrypte vos données. Ce champ n'est visible que lorsque **Module de génération automatique** n'est pas sélectionné. Pour plus d'informations sur les politiques d'accès au module, consultez Vue d'ensemble de la politique d'accès au module **Remarque :** Vous pouvez passer en revue les politiques d'accès au module liées à votre groupe secret à l'aide du bouton **Gérer l'accès à l'instance** .

5. Cliquez sur **Envoyer**.

Remarque :
Lorsqu'il est créé, un groupe secret est inactif par défaut. Retournez 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 pour 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

Les secrets de ce type de groupe secret doivent tous partager des critères communs. Pour les groupes ne disposant pas de cette restriction, envisagez de créer un groupe secret de base. Pour en savoir plus sur la création d'un groupe secret de base, reportez-vous à Créer un groupe secret de baselа section .

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. Remplissez les champs du formulaire **Groupe secret** .

Champs de groupe secret

Champ	Description
Nom de groupe	Nom du 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 **au client.**
Module de génération automatique	Génère un nouveau module de chiffrement pour ce groupe secret. Ce module crypte et décrypte 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 courte	Description du groupe
Type de critère	Critères partagés par les secrets de ce groupe. ○ Périmètre ○ Package ○ Table cible ○ Colonne secrète ○ Enregistrement du filtre
Module de chiffrement	Sélectionnez le module de chiffrement à utiliser avec ce groupe. Ce module crypte et décrypte vos données. Ce champ n'est visible que lorsque **Module de génération automatique** n'est pas sélectionné. Pour plus d'informations sur les politiques d'accès au module, consultez Vue d'ensemble de la politique d'accès au module

Champ	Description
	Remarque : Vous pouvez passer en revue les politiques d'accès au module liées à votre groupe secret à l'aide du bouton **Gérer l'accès à l'instance** .

5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.

   Remarque :
   Lorsqu'il est créé, un groupe secret est inactif par défaut.

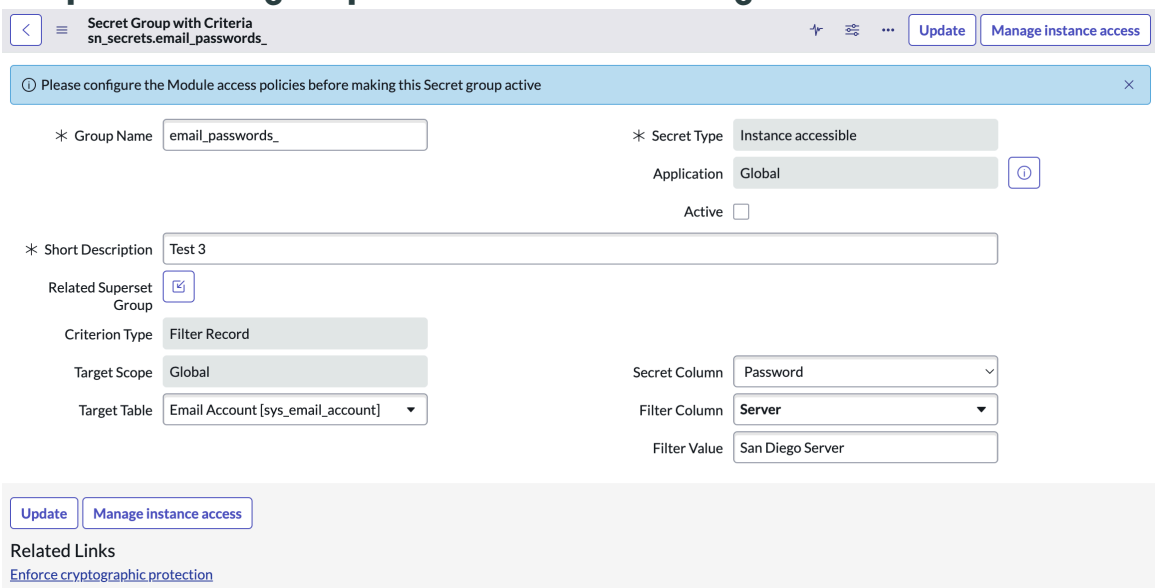
6. Après avoir sauvegardé l'enregistrement, des champs supplémentaires peuvent apparaître en fonction de la façon dont vous avez configuré votre groupe.

Champs de groupe secret supplémentaires

Champ	Description
Périmètre cible	Champ d'application partagé par les secrets à affecter à ce groupe. Ce champ n'est disponible que lorsque vous 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 n'est visible que lorsque vous sélectionnez Table, Colonne de filtre ou Colonne secrète dans le champ Type de **critère** .
Colonne secrète	Colonne de table qui contient les secrets pasword2 que vous inclurez dans ce groupe. Les champs disponibles dans cette liste sont déterminés par la table sélectionnée dans le champ **Table cible** . **Remarque :** Si la table de sélection n'a pas de colonnes contenant des secrets, ce champ s'affiche uniquement en tant que sélection : Aucune .

Champ	Description
Colonne de filtre	Colonne de la table sélectionnée dans **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 au champ sélectionné dans le champ **Colonne de filtre** .

Example: Groupe accessible à l'instance contenant tous les mots de passe d'un compte de messagerie pour 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 les étapes 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

Chargez 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 du 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 **Importer le certificat de clé publique d'identité** s'affiche.

4. Entrez un alias pour votre clé dans le champ **Alias de clé d'identité** .
5. Sélectionnez le bouton **Importer** pour charger la clé à partir de votre environnement local.
6. Sélectionnez le bouton **OK** .
   Le champ **Clé du module Groupe** utilise le nom de l'alias de clé d'identité.
7. Sélectionnez **Soumettre** pour sauvegarder l'enregistrement du groupe d'identité.

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 vous élever au rôle security_admin. Pour plus d'informations sur ce processus, consultez Élever à un rôle privilégié

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Tâches de Security** > **Créer**.
2. À **l'invite Quel type de tâche de sécurité voulez-vous créer ?** , sélectionnez **Tâche de gestion des secrets**.
3. Renseignez les champs du formulaire.

Formulaire Tâche de gestion des secrets

Champ	Description
Nom	Nom de la tâche de sécurité
État	L'état de la tâche initiale est Nouveau. Une fois que la tâche a été exécutée comme prévu, l'état se met à jour en conséquence
Début de la fenêtre de temps	Heure de début de la tâche au format 24 heures. La tâche commence à s'exécuter 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

Champ	Description
	⚠ Avertissement : La sélection de l'option **Toutes les tables** peut affecter les performances de l'instance. Envisagez de planifier 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**
Tables	Les 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 **Niveau d'application** est défini sur **Tables spécifiques**
Champs	Les tables à inclure dans cette tâche. Le chiffrement est appliqué à tous les champs sélectionnés. Cette option s'affiche uniquement lorsque **Niveau d'application** est défini sur **Champs spécifiques**
Mode de tâche	Sélectionnez parmi **Gestion de Password2 vers clés secrètes** Chiffrez tous les champs password2 au sein de vos groupes secrets à l'aide des modules cryptographiques définis par la politique d'accès au module de chaque groupe. **Gestion des clés secrètes 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 aucun changement. Si la requête trouve des données qui ne sont pas encore dans le groupe, la tâche chiffre à nouveau ces

Champ	Description
	données dans le 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 secret.
Groupe secret	Groupe secret contenant les secrets à chiffrer. Ce champ n'est disponible que lorsque **l'option Groupe secret** est sélectionnée dans le champ **Mode de tâche** .
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 **Envoyer**.

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 aucun changement. Si la requête trouve des données qui ne sont pas encore dans le groupe, la tâche chiffre à nouveau ces données dans le groupe secret. (Si l'instance peut le déchiffrer, ce qui peut ne pas être le cas pour les secrets chiffrés côté client).

ServiceNow Vault

Utilisez les outils de sécurité des données du produit ServiceNow Vault pour protéger les informations sensibles contre tout accès non autorisé, endommagement ou vol tout au long de leur cycle de vie. Appliquez des protections telles que le chiffrement, la gestion des secrets et la confidentialité des données pour la rédaction et l'audit des informations sensibles. La page d'accueil de ServiceNow Vault constitue un emplacement unique pour rechercher des produits de sécurité des données ServiceNow Vault et y accéder.

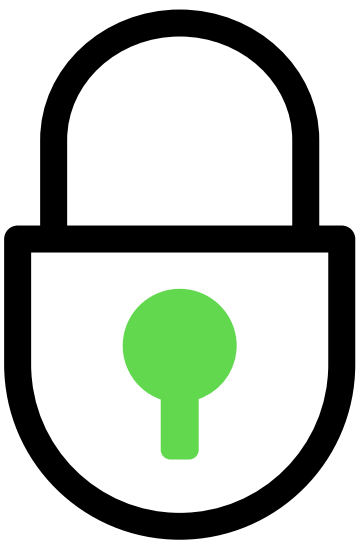
ServiceNow Vault est un module d'extension payant que le personnel ServiceNow doit activer sur votre instance de production. ServiceNow Vault inclut les composants répertoriés ici.

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.

servicenow

Composants ServiceNow Vault

Chiffrement

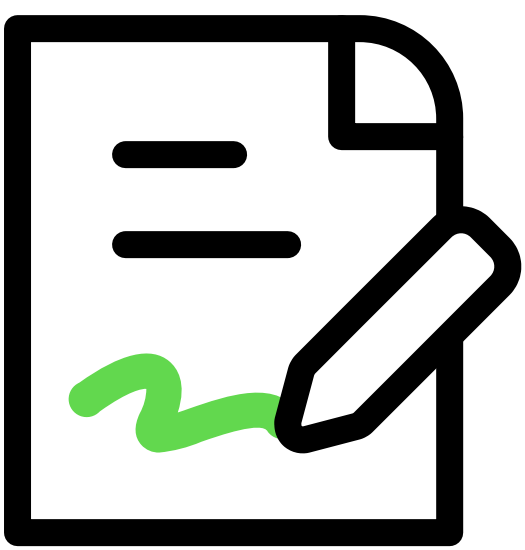


Key Management et Column Level Encryption sont une suite de modules de chiffrement hautement configurables

Gestion des secrets

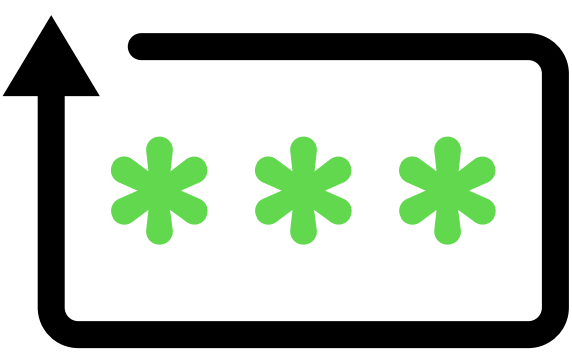
Cette solution permet de remplacer tous les secrets codés en dur sur la plateforme, tels que les mots de passe, les certificats et les clés API, par la garde des secrets par le client.

Signature de code



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

Confidentialité des données



Traduction automatique

Utilisez le module d’extension Data Privacy pour supprimer les informations d’identification personnelle (PII) des données utilisateur lors de leur migration d’une instance de production vers une instance de non-production.

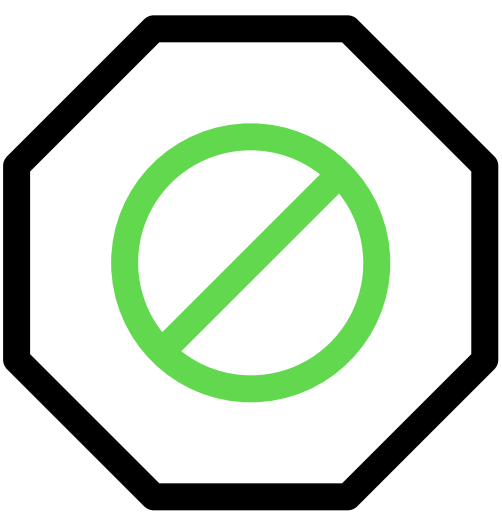
Détection de données

Le module d’extension de détection de données vous permet de trouver des informations d’identification personnelle (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 journal ServiceNow dans l’analyse des [qa: BEGIN review][End]journaux d’entreprise à l’aide du service d’exportation de journaux.

Accès zéro confiance



Traduction automatique

[qa: BEGIN review][End]L’accès à la session ServiceNow permet aux organisations de réduire dynamiquement les privilèges des utilisateurs au sein d’une session Web

Traduction automatique

servicenow

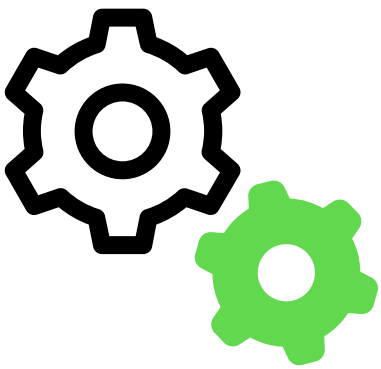
Confidentialité de la plateforme

La confidentialité vous permet de masquer la date sensible sur l'instance.

ACL

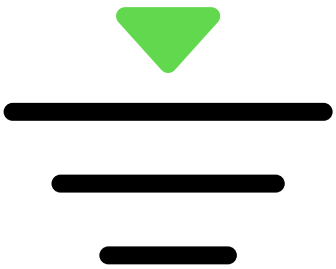
Les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données.

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.

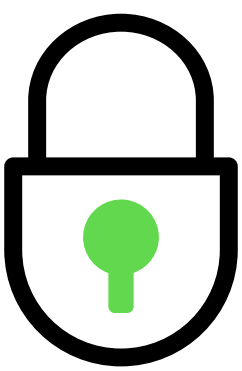
Filtration des données



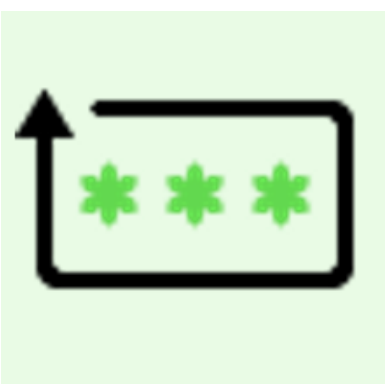
Utilisez la filtration des données pour contrôler l'accès aux tables et aux enregistrements en fonction des attributs d'objet lors de l'exécution de requêtes de lecture.

Séparation de domaine

Confidentialité des données



Détection de données



Traduction automatique

Grâce à la ServiceNow plateforme, 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.

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.

Utilisez la détection de données pour identifier les données sensibles au sein d'une instance afin de classer, protéger ou générer des rapports.

Règles des listes 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

En savoir plus sur ACL.

Configurer

Configurez l’ACL.

Traduction automatique

Référence

Obtenez des détails sur le gestionnaire de sécurité contextuelle.

Avancés

En savoir plus sur l’ACL avancée.

Exploration des listes de contrôle d’accès

Explorez les listes de contrôle d’accès (ACL).

Composants des ACL

Toutes les règles de liste de contrôle d’accès spécifient :

- *Objet* et *opération* sécurisés
- *Autorisations* requises pour accéder à l’objet

L’objet est la cible dont 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.

Par exemple, toutes ces entrées spécifient un objet :

Type	Nom	Objet sécurisé
record	[incident]. [--Aucun--]	La table Incident.
record	[incident]. [actif]	Champ Actif de la table Incident.
REST_Endpoint	user_role_inheritance	L’enregistrement de l’API REST scriptée user_role_inheritance.

Chaque *opération* décrit une *action* valide que le système peut effectuer 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.

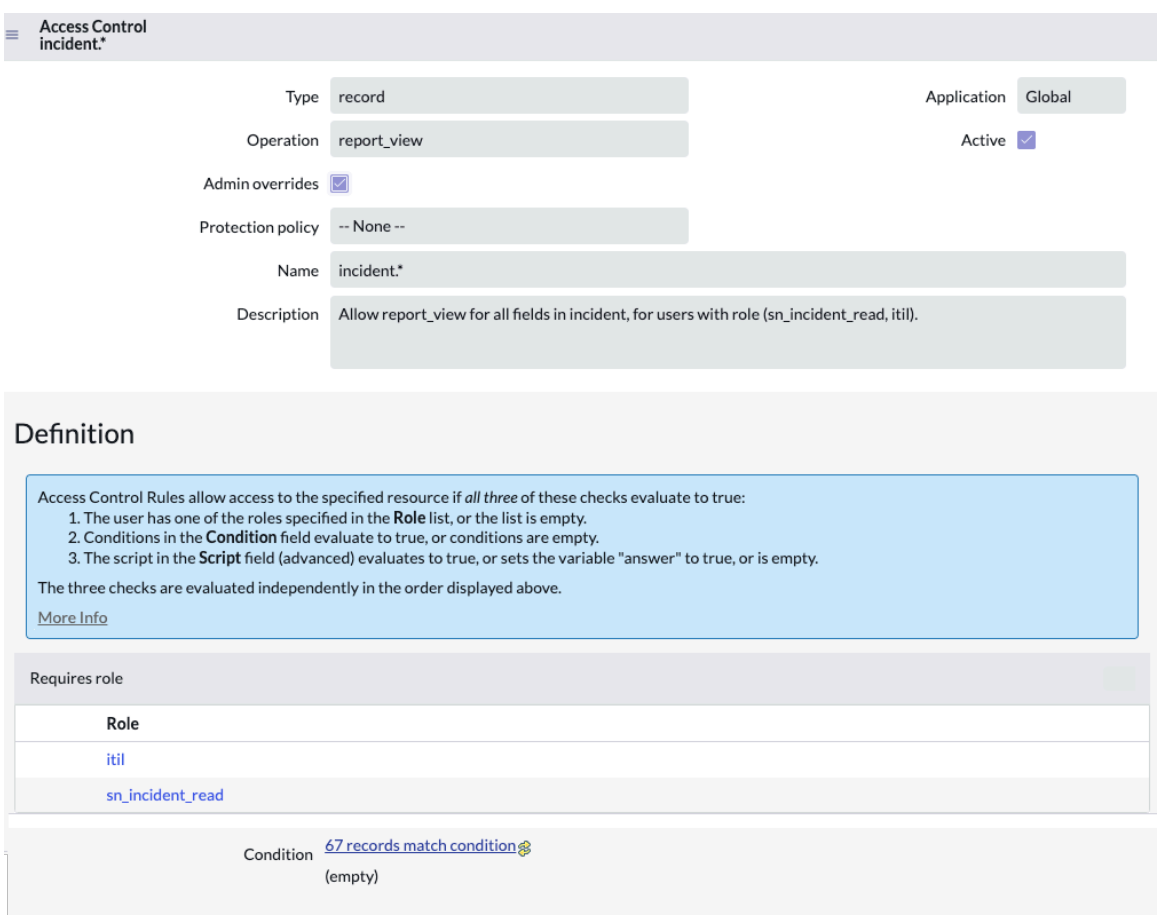
Par exemple, toutes ces entrées spécifient une opération :

Type	Nom	Opération	Opération sécurisée
record	[incident]. [-- Aucun --]	créer	Création d'enregistrements dans la table Incident.
record	[incident]. [actif]	write	Mise à jour du champ Actif dans la table Incident.
REST_Endpoint	user_role_inheritance	execute	Exécution de l'API REST scriptée user_role_inheritance.

Les *autorisations* spécifient quand une personne peut accéder à l'objet et à l'opération nommés. Les administrateurs de sécurité peuvent spécifier les exigences en matière d'autorisation en ajoutant :

- Un ou plusieurs rôles d'utilisateur à la liste **Rôles requis** .
- Une ou plusieurs conditions.
- Script qui évalue sur vrai ou faux ou définit la variable `de réponse` sur vrai ou faux.

Pour accéder à un objet et à une opération, un utilisateur doit passer toutes les autorisations répertoriées dans un contrôle d'accès. Par exemple, ce contrôle d'accès restreint l'accès à l'affichage des opérations sur la table d'incidents.



Traduction automatique

Pour mettre à jour un enregistrement dans la table d'incidents, un utilisateur doit avoir les rôles répertoriés et l'enregistrement doit répondre à la condition.

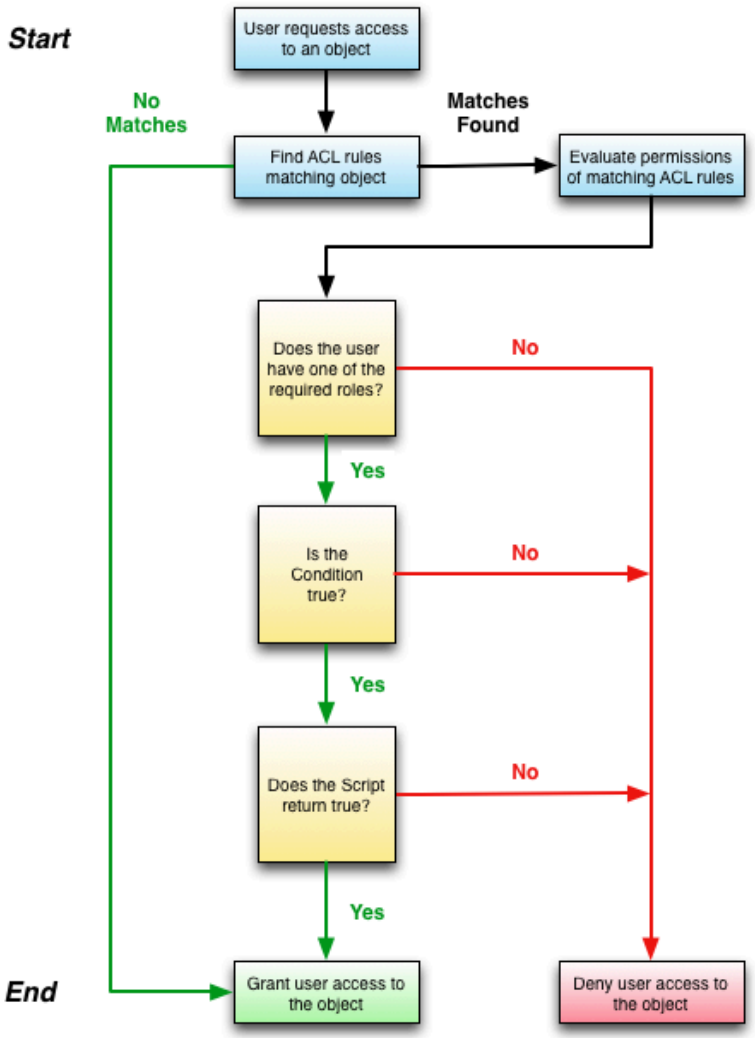
Type d'autorisation	Besoin	Description
Demande un rôle	**Demande role** :itil	Autorisez uniquement les utilisateurs disposant du rôle ITIL à mettre à jour les incidents.
Condition	[État de l'incident] [n'est pas] [Fermé]	Autorisez uniquement les mises à jour des enregistrements d'incidents actifs.

Processus d'évaluation ACL

Une règle ACL accorde à un utilisateur l'accès à un objet uniquement si l'utilisateur répond à toutes les autorisations requises par la règle ACL correspondante.

- La condition doit être *évaluée comme vraie*.
- Le script doit donner la valeur *true* ou renvoyer une variable de réponse avec la valeur *true*.
- L'utilisateur doit avoir 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 les deux avoir la *valeur true*.

ACL évaluer les autorisations



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 dispose des autorisations requises pour accéder à l'objet et à l'opération. Si une règle de contrôle d'accès spécifie plusieurs autorisations, l'utilisateur doit disposer de toutes les autorisations pour accéder à l'objet et à l'opération. L'échec d'une vérification d'autorisation empêche l'utilisateur d'accéder à l'objet et à l'opération correspondants.

Si un utilisateur ne satisfait pas aux autorisations de la première règle de correspondance, le système évalue les autorisations de la règle de contrôle d'accès correspondante suivante, comme spécifié par l'ordre de traitement du contrôle d'accès. Si l'utilisateur ne répond pas aux autorisations 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'y a pas de règles de contrôle d'accès correspondantes pour l'objet et l'opération demandés, le système accorde l'accès à l'utilisateur. Dans la pratique, il est rare que le système ne trouve aucune règle de correspondance, car le système dispose d'un ensemble de règles de contrôle d'accès par défaut qui protègent toutes les opérations d'enregistrement.

Les conséquences d'un refus d'accès à un objet dépendent de la règle ACL selon 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 sur un formulaire, masque des lignes d'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 ait effectué une requête. Étant donné que des informations différentes sont disponibles avant et après une requête, les résultats peuvent être différents.

Vérification de l'ACL avant requête

Avant que votre instance n'exécute une requête de base de données, elle 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 aux 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 ces données en compte. 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 lui est pas présentée.

Vérification de l'ACL après la 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 lui est pas présentée, mais l'utilisateur voit l'étiquette du champ si ses rôles autorisent l'accès au champ.

Opération	Résultats de l'échec d'une règle ACL sur un objet
execute	L'utilisateur ne peut pas exécuter de scripts sur un enregistrement ou une page de l'interface utilisateur.
créer	L'utilisateur ne peut pas voir la **nouvelle** action d'interface utilisateur à partir des 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 est toujours évaluée comme fausse. Les champs des nouveaux enregistrements sont considérés comme vides jusqu'à ce que l'enregistrement soit enregistré.
lu	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.
write	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.

Opération	Résultats de l'échec d'une règle ACL sur un objet
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	Utilisé pour contrôler les champs qui doivent être enregistrés lors de la création d'un modèle.
add_to_list	L'utilisateur ne peut pas afficher ni personnaliser des colonnes spécifiques dans la mécanique 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**.

Besoins 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 disposer des autorisations de deux règles ACL : 1. Toutes les règles ACL génériques pour l'objet (s'il existe une règle ACL 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 pas de règles génériques (*) 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.
Pages de l'interface utilisateur Enregistrement	Les utilisateurs doivent disposer des autorisations de deux règles ACL : 1. Première règle ACL qui correspond au champ de l'enregistrement (s'il existe une règle ACL pour l'opération). 2. Première règle ACL qui correspond à la table de l'enregistrement (s'il existe une règle ACL pour l'opération).	Par défaut, il existe des règles de table génériques (*) pour les opérations de création, de lecture, d'écriture et de suppression et des règles de champs génériques (*.*) 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 du gestionnaire de sécurité (`glide.sm.default_mode`) détermine si les utilisateurs peuvent accéder aux objets qui correspondent uniquement aux règles ACL de table à caractère générique. 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 de champ générique (*.*) pour l'opération de création réutilise les mêmes autorisations que l'opération d'écriture. Cela signifie que les autorisations de création sont les mêmes que les autorisations d'écriture, sauf si vous définissez une règle ACL d'opération de création explicite.

Plusieurs règles ACL au même point dans l'ordre de traitement

Si au moins deux règles correspondent au même point de l'ordre de traitement, l'utilisateur doit transmettre l'une des autorisations de règles ACL pour accéder à l'objet. Par exemple, si vous créez deux règles ACL de champ pour `incident.number`, un utilisateur qui transmet une règle a accès au champ de nombre, que l'utilisateur ait échoué ou non à une autre règle ACL de champ au même point 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 Élever à un rôle privilégié pour obtenir les instructions.

Règles ACL dans les applications incluses dans le périmètre

Vous pouvez créer des règles ACL pour les objets dans le même champ d'application que la règle ACL. Vous pouvez également créer des règles ACL pour les tables ayant au moins un champ qui se trouve dans le même champ d'application que la règle ACL.

Pour les tables qui sont dans un champ d'application différent de l'enregistrement de règle ACL, les types de règles sont limités.

- Vous pouvez créer une règle ACL pour n'importe quelle table, page d'interface utilisateur ou autre objet du même champ d'application que la règle ACL.
- Vous pouvez créer une ACL pour un champ qui est dans le même champ d'application que la règle ACL.
  - Si la table se trouve dans le même champ d'application, vous pouvez utiliser un script pour évaluer les autorisations.
  - Si la table se trouve dans un champ d'application différent, vous ne pouvez pas utiliser de script pour évaluer les autorisations.
- Vous ne pouvez pas créer ni modifier les règles d'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 un ACL dans un périmètre différent.
- Vous pouvez créer des règles de table génériques (*) uniquement dans le champ d'application global.
- Vous pouvez créer des règles de champ générique (*) uniquement pour les tables dans le même champ d'application que la règle ACL.

Types de règles ACL

Créez des règles ACL sur différents composants du système.

Règles ACL d'enregistrement

Les règles ACL d'enregistrement sont constituées 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 :

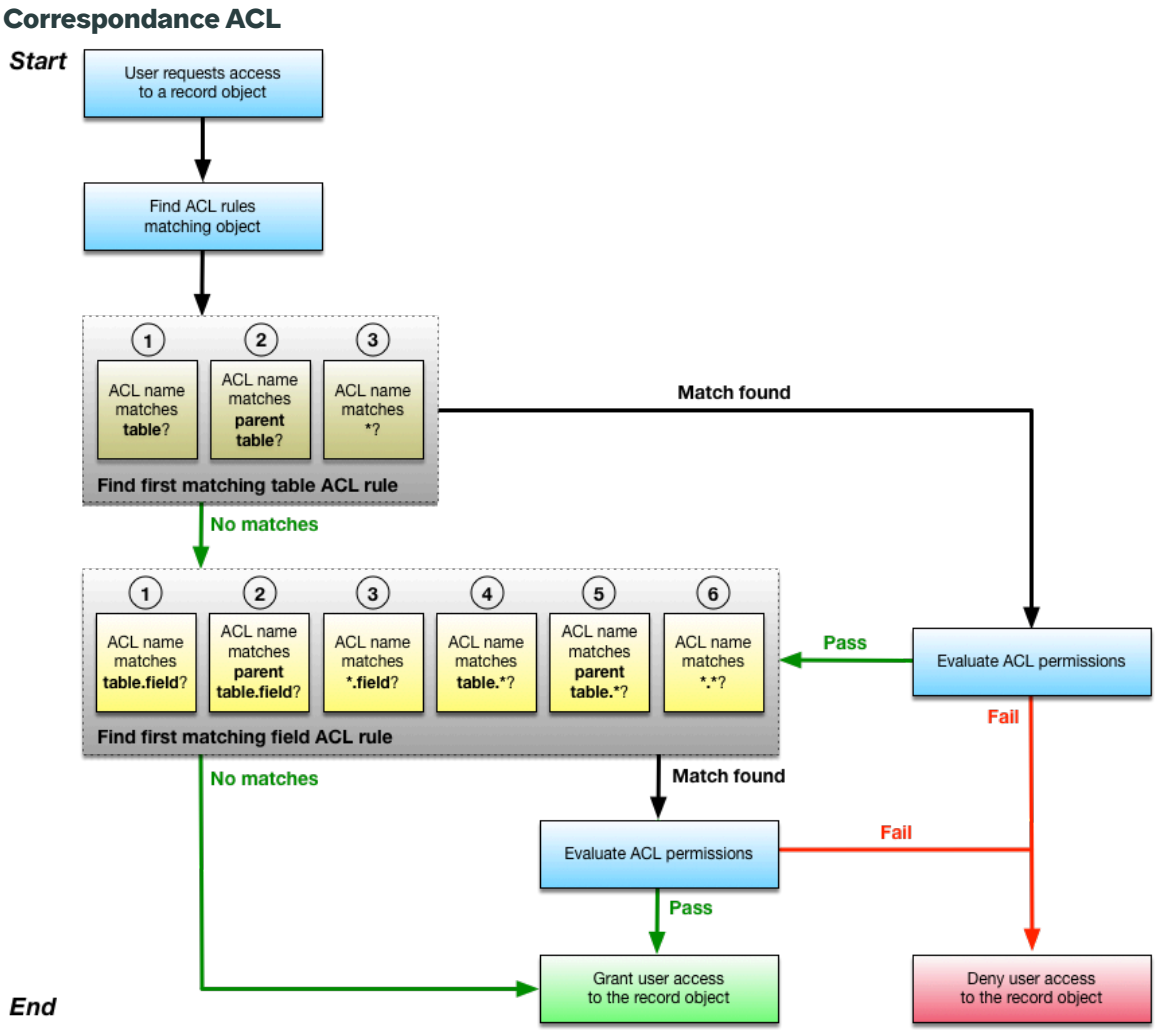
Opération	Description
créer	Permet aux utilisateurs d'insérer de nouveaux enregistrements (lignes) dans une table.
lu	Permet aux utilisateurs d'afficher les enregistrements d'une table.
write	Permet aux utilisateurs de mettre à jour les enregistrements d'une table.
supprimer	Permet aux utilisateurs de supprimer des enregistrements d'une table ou de supprimer une table.
edit_task_relations	Permet aux utilisateurs d'étendre la table Tâche [task].
edit_ci_relations	Permet aux utilisateurs d'étendre la table Élément de configuration [cmdb_ci].
save_as_template	Permet aux utilisateurs de sauvegarder 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 les enregistrements (lignes) à partir d'une liste.
report_on	Permet aux utilisateurs de créer 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.

Les règles ACL d'enregistrement sont traitées dans l'ordre suivant :

- Faites correspondre l'objet aux règles ACL de table.
- Faites correspondre l'objet avec les règles ACL de 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 transmettre 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 réussit 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.



Règles ACL du processeur

Les règles ACL de processeur spécifient le processeur que vous souhaitez sécuriser. Pour obtenir une 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 (*) s'il est impossible de trouver une 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. Faites correspondre le 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, *.

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 d'ACL de table, le système évalue alors les règles d'ACL de champ.

Règles ACL de champ

Une fois qu'un utilisateur a transmis 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 de champ. Par exemple, task.number.
3. Correspond à n'importe quelle table (*) et n'importe quel nom de champ. Par exemple, *.number.
4. Faites correspondre la table et n'importe quel champ (*). Par exemple, incident.*.
5. Faites correspondre la table parente et n'importe quel champ (*). Par exemple, tâche.*.
6. Correspond à n'importe quelle table (*) et à n'importe quel champ (*). Par exemple, *.*.

Un utilisateur doit transmettre la règle ACL de 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 réussie de l'ACL de champ arrête le traitement de la règle d'ACL au niveau du champ. Lorsqu'un utilisateur transmet une règle ACL de champ, le système arrête de rechercher 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 d'interrogation des données déduites est restreint pour les champs protégés, empêchant ainsi le renvoi d'informations prédictives.

Règles ACL de page d'interface utilisateur

Les règles ACL de page d'interface utilisateur spécifient la page d'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 d'interface utilisateur, utilisez le nom de page dans le champ d'application complet. Par exemple, **x_myapp_mypage**.

Remarque :
Vous pouvez utiliser le caractère ÉTOILE (*) dans le champ **Nom** sur les ACL **de type ui_page** pour correspondre à n'importe quelle page de l'interface utilisateur.

Les règles ACL de page d'interface utilisateur respectent la règle STAR (*) si elles ne trouvent pas d'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
lu	Permet aux utilisateurs d'afficher la page d'interface utilisateur.

Règles ACL du script include client-pouvant être appelé

Les règles ACL de script include spécifient l'include de script pouvant être appelé par le client à sécuriser. Pour obtenir une liste des script includes disponibles, accédez à **Définition du système** > **Includes de script**. Vous pouvez personnaliser la liste pour afficher la colonne *Client pouvant être appelé* .

Le système de base n'inclut aucune règle ACL pour les script includes pouvant être appelés par le client.

Les règles ACL de script include pouvant être appelées par le client respectent la règle STAR (*) s'ils ne trouvent pas d'ACL plus spécifique pour ces ressources.

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, consultez Champ de fonction .

À l'intérieur Rome et à l'avant, 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 ou non accès aux champs de contribution.

À partir Washington DC des années suivantes, 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 de champ de contribution refusent l'accès, le champ de fonction refuse également l'accès.

Les seules opérations concernées par la nouvelle exigence sont lues et 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 définies sur vrai : • L'utilisateur dispose d'un accès en lecture au champ de fonction. • L'utilisateur dispose d'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 remplies : • 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 de rôle uniquement sans conditions et sans script, et l'utilisateur dispose de ce rôle. • L'utilisateur dispose d'un accès en lecture aux champs de contribution (rôle uniquement), de sorte que seules les ACL sans condition ou script peuvent les autoriser.

Exemples

Donné:

- Tableau : salaire
- Colonnes : base, bonus, total (tous sont des entiers dans cet exemple)
- Champ de fonction : La colonne de total est marquée comme un 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, de base, bonus : lire et report_view pour le rôle salary_admin, sans conditions ni scripts	Un utilisateur disposant du rôle salary_admin dispose d'un accès en lecture et report_view au total, car il possède le rôle requis.

Exemple 2 : le champ Contribution refuse l'accès en lecture

ACL	Résultat
• Total, base : lecture et report_view pour les salary_admin de rôle, sans conditions ni scripts • Bonus : report_view pour le rôle salary_admin, sans conditions ni scripts • Bonus : lecture pour le rôle bonus_admin, sans conditions ni scripts	Un utilisateur disposant du rôle salary_admin se voit refuser l'accès en lecture et report_view au total, car le bonus refuse l'accès en lecture à son rôle.

Exemple 3 : l'ACL du champ Contribution comporte un script

ACL	Résultat
• Total, base : lecture et report_view pour les salary_admin de rôle, sans conditions ni scripts • Bonus : report_view pour le rôle bonus_admin, 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 soit là)	Un utilisateur disposant du rôle salary_admin dispose d'un accès en lecture à total, car il dispose du rôle requis pour tous les champs. Cependant, l'accès est refusé report_view ce même utilisateur avec le salary_admin, car l'ACL de lecture avec le script refuse l'accès par défaut pour ce cas, même s'il dispose du rôle requis.

Module d'extension Security jump-start - ACL rules

Le module d'extension 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 altérer l'accès sécurisé aux tables déjà utilisées dans un environnement de production. Si un administrateur souhaite vivement installer ce module d'extension sur une instance existante, il est recommandé de le tester d'abord de manière approfondie dans une instance de test. Cela permet d'assurer la compatibilité avec l'implémentation actuelle de l'organisation.

Si un administrateur est intéressé par les nouvelles règles d'ACL fournies par ce module d'extension, il peut en créer une ou plusieurs manuellement dans une instance existante, en utilisant la liste des ACL comme ligne directrice.

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 touche Opération est la suivante :

- R = lire
- W=write
- D=supprimer
- C=créer

Nom	Opération	Description
cmdb_ci	CMS	Rôle d'actif ou ITIL requis pour écrire/créer/supprimer des enregistrements d'éléments de configuration
cmn_department	WD	user_admin rôle requis pour écrire/supprimer des enregistrements de département
cmn_location	WC	user_admin rôle requis pour écrire/créer des enregistrements d'emplacement
core_company	WD	user_admin rôle requis pour écrire/supprimer des enregistrements de société
kb_knowledge	créer	rôle de la base de connaissances requis pour créer des enregistrements de la base de connaissances
ldap_ou_config	RWCD (en anglais seulement)	user_admin rôle requis pour lire/écrire/créer/supprimer des enregistrements de définitions LDAP OU
ldap_server_config	RWCD (en anglais seulement)	user_admin rôle requis pour lire/écrire/créer/supprimer des enregistrements de serveur LDAP
process_guide	CMS	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements du guide de processus
process_step	CMS	Rôle administrateur 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 Service Catalog

Nom	Opération	Description
sc_category	supprimer	catalog_admin rôle requis pour supprimer des enregistrements de catégorie de Catalogue de services
sc_category	write	catalog_admin rôle requis pour écrire dans des enregistrements de catégorie de Catalogue de services
sc_cat_item	write	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	lu	tous les utilisateurs peuvent lire les enregistrements de notification par e-mail (à des fins d'abonnement)
sysevent_register	RWCD (en anglais seulement)	Le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements du registre d'événements
sysevent_script_action	RWCD (en anglais seulement)	Rôle administrateur requis pour lire/écrire/créer/supprimer des enregistrements d'action des scripts
syslog	RWCD (en anglais seulement)	admin tenu de lire/écrire/créer/supprimer des enregistrements d'entrée de journal
règle système	RWCD (en anglais seulement)	administrateur tenu de lire/écrire/créer/supprimer des enregistrements de règles (notifications par e-mail, actions sur e-mail entrant, règles d'approbation, etc.)
règle système	lu	tous les utilisateurs peuvent lire les enregistrements de notification par e-mail pour (notifications basées sur un abonnement)
sys_app_application	CMS	admin tenu d'écrire/créer/supprimer des enregistrements d'application
sys_app_category	CMS	Rôle administrateur requis pour écrire/créer/supprimer des enregistrements de catégorie d'application
sys_app_module	CMS	admin requis pour écrire/créer/supprimer les enregistrements de module
sys_audit	RWCD (en anglais seulement)	administrateur tenu de lire/écrire/créer/supprimer des enregistrements d'audit
sys_dictionary	RWC	personalize_dictionary rôle requis pour lire/écrire/créer des enregistrements de dictionnaire
sys_dictionary.*	lu	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	write	Le Rôle « personalize_dictionary » est requis pour écrire dans des enregistrements d'étiquette de champ.

Nom	Opération	Description
sys_gauge	RWCD (en anglais seulement)	Le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements de jauge
sys_gauge_count	RWCD (en anglais seulement)	Le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements du nombre de jauges
sys_group_has_role	lu	Rôle itil requis pour afficher les enregistrements de rôle de groupe
sys_home	CMS	itil_admin rôle requis pour écrire/créer/supprimer des enregistrements Section de page d'accueil
sys_installation_exit	CMS	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de sortie d'installation
sys_job	CMS	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de tâches système
sys_nav_link	CMS	Rôle administrateur requis pour écrire/créer/supprimer des enregistrements de lien de navigation
sys_perspective	CMS	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de liste de menus
sys_portal	RWCD (en anglais seulement)	Rôle administrateur requis pour lire/écrire/créer/supprimer des enregistrements de portail
sys_portal_page	RWCD (en anglais seulement)	Rôle administrateur requis pour lire/écrire/créer/supprimer des enregistrements de page d'accueil
sys_portal_preferences	RWCD (en anglais seulement)	Le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements de préférences de portail
sys_processor	WC	Le rôle administrateur est requis pour écrire/créer des enregistrements de processeur
sys_properties	WC	Le rôle administrateur est requis pour écrire/créer des enregistrements de propriétés système
sys_properties_category	CMS	Rôle administrateur requis pour écrire/créer/supprimer des enregistrements de catégorie de propriété
sys_report	supprimer	rôles qui peuvent supprimer des enregistrements de rapports (ne limite pas la suppression via l'interface utilisateur de rapport)
sys_report	write	rôles qui peuvent écrire dans les enregistrements de rapports (ne restreint pas la modification via l'interface utilisateur de rapport)
sys_report	lu	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	lu	rôles qui peuvent lire les enregistrements de rapports (ne limite pas l'affichage via l'interface utilisateur de rapport)
sys_reportroles	lu	Le rôle administrateur est requis pour lire les enregistrements des rôles de rapport

Nom	Opération	Description
sys_script	CMS	Rôle administrateur requis pour écrire/créer/supprimer des enregistrements de règle métier
sys_script_ajax	CMS	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de script AJAX
sys_script_client	CMS	Rôle administrateur requis pour écrire/créer/supprimer des enregistrements de script client
sys_script_include	CMS	Rôle administrateur requis pour écrire/créer/supprimer des enregistrements Script Include
sys_security_acl	write	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 les enregistrements des rôles d'accès
sys_security_acl_role	write	rôle administrateur 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	write	Rôle administrateur requis pour écrire dans les enregistrements d'opérations de sécurité
sys_security_type	write	Le rôle administrateur est requis pour écrire dans les enregistrements de type de sécurité
sys_security_type	créer	Rôle administrateur requis pour créer des enregistrements de type de sécurité
sys_security_type	supprimer	Rôle administrateur 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 les enregistrements d'état du système
sys_status	write	Le rôle administrateur est requis pour écrire dans les enregistrements d'état du système
sys_template	write	template_editor rôle requis pour écrire dans des enregistrements de modèles
sys_template	créer	emplate_editor rôle requis pour créer des enregistrements de modèles
sys_template	supprimer	template_editor rôle requis pour supprimer des enregistrements de modèles
sys_template	lu	template_editor rôle requis pour lire les enregistrements des rôles de modèle

Nom	Opération	Description
sys_ui_action	créer	Rôle administrateur requis pour créer des enregistrements d'action d'interface utilisateur
sys_ui_action	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements d'action d'interface utilisateur
sys_ui_action	write	Rôle administrateur requis pour écrire dans les enregistrements d'action d'interface utilisateur
sys_ui_action_view	write	Rôle administrateur requis pour écrire dans les enregistrements de l'action de vue de l'interface utilisateur
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 les enregistrements de l'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	write	Le rôle administrateur est requis pour écrire dans les enregistrements de la politique d'interface utilisateur
sys_ui_policy_action	créer	Le rôle administrateur est requis pour créer des enregistrements d'action de politique d'interface utilisateur
sys_ui_policy_action	supprimer	Le rôle administrateur est requis pour supprimer les enregistrements d'action de politique d'interface utilisateur
sys_ui_policy_action	write	Rôle administrateur requis pour écrire dans les enregistrements d'action de politique d'interface utilisateur
sys_ui_script	write	le rôle administrateur est requis pour écrire dans les enregistrements de script d'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	write	Les utilisateurs sans rôle ne peuvent mettre à jour aucun enregistrement utilisateur autre que le leur
sys_user_grmember	supprimer	user_admin rôle requis pour supprimer les enregistrements de membres du groupe
sys_user_grmember	write	user_admin rôle requis pour écrire dans les enregistrements des membres du groupe
sys_user_group	créer	Seuls les formats ITIL et supérieurs peuvent créer des enregistrements de groupe
sys_user_group	write	Seuls les formats ITIL et versions supérieures peuvent écrire dans des enregistrements de groupe
sys_user_has_role	lu	Rôle ITIL requis pour afficher les enregistrements de rôle d'utilisateur
sys_user_role	créer	Rôle administrateur requis pour créer des enregistrements de rôle

Nom	Opération	Description
sys_user_role	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements de rôle
sys_user_role	write	rôle administrateur requis pour écrire dans les enregistrements de rôle
sys_user_role_contains	lu	Rôle ITIL requis pour afficher les enregistrements de rôles contenus
sys_user_role_contains	write	Rôle administrateur requis pour écrire dans des enregistrements de rôles contenus
sys_user_token	RWCD (en anglais seulement)	Rôle administrateur requis pour lire/écrire/créer/supprimer des enregistrements de jetons d'utilisateur

Remarque :
Pour en savoir plus sur ce module d'extension, consultez Démarrage rapide de la sécurité (règles ACL) (renforcement de la sécurité de l'instance) dans les paramètres de renforcement de la sécurité de l'instance.

Configurer une règle ACL

Configurez une règle 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

Pourquoi et quand exécuter cette tâche
Pour créer des règles d'ACL, vous devez élever les privilèges au rôle security_admin.

Pour les tables qui sont dans un champ d'application différent de l'enregistrement de règle ACL, les types de règles sont limités. Pour que les tables maître de champ d'application dérivent le champ d'application et exécutent les ACLS incluses dans le champ d'application, définissez la *glide.enforce_security_scope.<scope_name>* propriété sur **true**. Cela garantit que les ACL du champ d'application global ne correspondent pas lorsque des ACL spécifiques au champ d'application sont créées sur la table pertinente. Vous pouvez par exemple sécuriser les données dans des tables d'application partagées dans le champ d'application Global, telles que les tables sys_attachment ou sys_question_answer.

Procédure

1. Rôles de privilège élevés au rôle security_admin.
2. Accédez à la **Sécurité de système** > **Contrôle d'accès (ACL)**.
3. Cliquez sur **Nouveau**.
4. Complétez 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 comment l'objet est nommé et quelles opérations sont disponibles. Ce champ passe en lecture seule une fois la règle ACL créée. Si vous souhaitez modifier le type, vous devez supprimer l'ACL et en créer une nouvelle avec le type approprié.

Champ	Description
Opération	Sélectionnez l'opération que cette règle ACL sécurise. Chaque type d'objet possède 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.
Remplacement administrateur	Cochez cette case pour que les utilisateurs dotés 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 ServiceNow le personnel peut affecter, a priorité sur l'option de remplacement administrateur. Si un ACL est affecté au rôle **personne** , les utilisateurs administrateurs ne peuvent pas accéder à la ressource, même lorsque **l'option Remplacements administrateur** est sélectionnée. Reportez-vous à la section Rôles système de base . Décochez cette case si les administrateurs doivent disposer des autorisations définies dans cette règle ACL pour accéder à l'objet sécurisé. Étant donné que les administrateurs réussissent toujours les vérifications de rôle (voir la description du champ **Rôle requis**), utilisez le créateur de condition ou le champ **Script** pour créer une vérification des autorisations que les administrateurs doivent passer.
Actif	Cochez cette case pour appliquer cette règle ACL.
Avancés	Cochez cette case pour afficher le champ **Script** . **Important :** **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.
Nom	Saisissez le nom de l'objet sécurisé, soit le nom de l'enregistrement, soit les noms de table et de champ. Plus le nom est spécifique, plus la règle ACL est spécifique. Vous pouvez utiliser un astérisque générique (*) 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, toutes les tables ou 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 règles 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 sécurisé. 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.
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 *Rôle requis* s'affiche sous la forme d'une liste connexe. **Remarque :** Les utilisateurs disposant du rôle administrateur réussissent toujours cette vérification d'autorisation, car le rôle administrateur accorde automatiquement aux utilisateurs tous les autres rôles.

Champ	Description
Condition	Utilisez ce créateur de condition pour sélectionner les champs et les valeurs qui doivent être vrais pour que les utilisateurs puissent accéder à l'objet.
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 métier ainsi que dans les propriétés système. Le script doit générer une réponse Vrai ou Faux de l'une des deux façons suivantes : ○ Renvoyer une variable de *réponse* définie sur 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 prend la valeur true et que l'utilisateur remplit toutes les conditions de la règle ACL. Les conditions et le script doivent être évalués comme vrais pour qu'un utilisateur puisse accéder à l'objet. **Remarque :** Si l'élément évalué se trouve dans une liste connexe, **la valeur actuelle** pointe sur l'élément sur lequel se trouve la liste connexe, et non sur l'élément actuel auquel l'ACL est destinée. Toutefois, si l'élément pour lequel vous évaluez l'ACL ne se trouve pas dans une liste connexe, **actuel** pointe vers l'élément réel.

5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.

Sécuriser les enregistrements dans une liste incorporée

Pour appliquer la sécurité aux enregistrements dans les listes incorporées, limitez la modification et la suppression des enregistrements dans les 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 **En écriture** ou **Suppression** pour la table appropriée.
3. Dans la section Rôle requis du formulaire, ajoutez les rôles qui ont l'autorisation d'écriture ou de suppression pour cette table.
4. Enregistrez les changements.
   Lorsque les enregistrements de la table associée s'affichent dans une liste incorporée, les options de modification et de suppression ne sont disponibles que pour les utilisateurs ayant les rôles spécifiés.

Gestionnaire de sécurité contextuelle

Contextual Security Manager protège vos données en contrôlant les autorisations de lecture, d'écriture, de création et de suppression.

Avantages clés

Le gestionnaire de sécurité contextuelle connaît la hiérarchie des tables système, ce qui vous permet de créer des règles de sécurité spécifiques pour un champ en fonction

de l'endroit où il apparaît dans la hiérarchie. Les avantages du gestionnaire de sécurité contextuelle sont les suivants :

- **Sécurité contextuelle** : sécurisez un enregistrement en fonction de son contenu.
- **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 pouviez sécuriser les champs et les tables en ajoutant des rôles à l'entrée de dictionnaire appropriée. Avec le gestionnaire de sécurité contextuelle, ces rôles de dictionnaire ne sont plus testés. Au lieu de cela, le système recherche des 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 via les règles ACL. Même si vous configurez la mise en page du formulaire de dictionnaire et ajoutez des rôles à une entrée de dictionnaire, aucune modification des droits ne se produit.

Sécurité contextuelle et rôles

Vous pouvez accorder des rôles à des utilisateurs ou à des groupes. Toutefois, après l'installation du gestionnaire de sécurité contextuelle, le champ **Rôles** de l'enregistrement utilisateur n'est plus vérifié et n'apparaît plus dans 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 de l'utilisateur ou du groupe.

Les applications et modules contiennent des listes des rôles requis pour les afficher. Par exemple, pour afficher l'application Définition du système, 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 y a beaucoup d'entrées en double dans la table Rôles d'utilisateur, vous devrez peut-être effectuer une mise à niveau vers Contextual Security : Role Management 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 Contextual Security : Role Management Enhancements est une version précédente de ce module d'extension. Le module d'extension Role Management Enhancements n'inclut pas le script RoleManagementVerify(). Ce script renvoie une liste des modifications qu'une mise à

niveau effectuera, ce qui vous permet de surveiller les modifications apportées par le module d'extension.

Remarque :
Après l'activation de Role Management 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, consultez :

- Activer l'audit des rôles avec Contextual Security : Role Management V2.
- Module d'extension Contextual Security : Role Management dans les paramètres de renforcement de la sécurité de l'instance.
- Rôles d'utilisateur d'audit

Empêcher les entrées en double avec Contextual Security : Role Management 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 dans un rôle. Contextual Security : Role Management 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 qu'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 apportés à l'activation

Contextual Security : Role Management V2 est automatiquement installé sur les nouvelles instances et peut être activé pour les mises à niveau. Lorsqu'il est activé, Contextual Security : Role Management V2 remplace à la fois Contextual Security et Contextual Security : Role Management Enhancements.

Lorsque Contextual Security : Role Management V2 est activé, 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

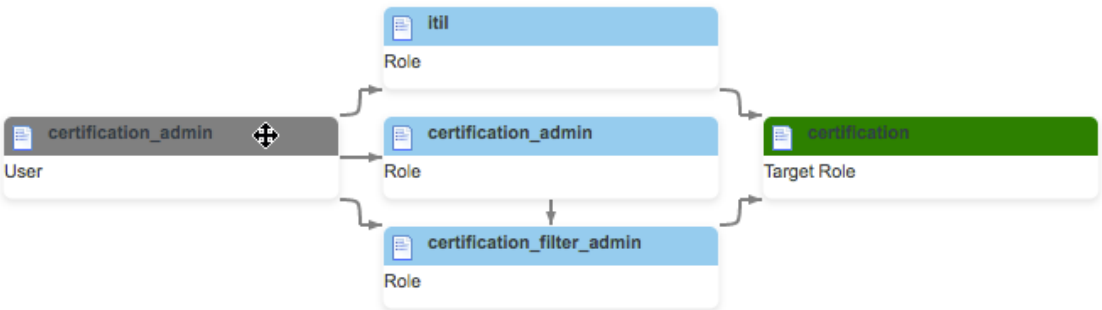
Avertissement :
Si ces colonnes sont utilisées dans des scripts personnalisés sur votre instance, ne mettez pas à niveau vers Gestion des rôles V2.

Visualiser l'héritage de rôle 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] de façon à afficher la colonne Carte d’héritage de rôle.

Carte d'héritage de rôle



Mise à niveau vers Contextual Security : Role Management v2

Contextual Security : Role Management V2 est automatiquement installé sur les nouvelles instances. Vous pouvez effectuer une mise à niveau de Contextual Security : Role Management vers Contextual Security : Role Management V2 pour éliminer les doublons dans la table Rôles d’utilisateur et empêcher les doublons à l’avenir.

Avant de commencer

Rôle requis : admin, security_admin

Vous devez disposer du rôle admin et Élever à un rôle privilégié pour obtenir le rôle security_admin effectif.

Remarque :

Avant de mettre à niveau vers Contextual Security : Role : Management 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 Activer l’audit des rôles avec Contextual Security : Role Management 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 Contextual Security : Role Management 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 disposant de privilèges élevés est requis pour activer le module d’extension, ou contactez Service et assistance client.
Sécurité contextuelle : API REST Gestion des rôles V2 [com.glide.role_management.inh_count.rest_api]	Active la fonctionnalité d’API pour la gestion des rôles.

Avant d'effectuer une mise à niveau de Contextual Security : Role Management vers Contextual Security : Role Management V2, testez les résultats d'une mise à niveau en exécutant le script. Le script renvoie une liste des changements qu'une mise à niveau effectuera. Si les modifications sont acceptables, installez le module d'extension Contextual Security : Role Management V2. Si les modifications ne sont pas acceptables, n'installez pas le module d'extension Contextual Security : Role Management 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 de sys_user_has_role volumineuses, l'exécution peut prendre jusqu'à 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 Contextual Security : Role Management V2.

> **Important :**
> Le rôle security_admin ou un utilisateur disposant de privilèges élevés est requis pour activer le module d'extension, ou contactez Service et assistance client.

a. Accédez à la **Définition du système** > **Modules d'extension**.

b. Recherchez le nom du module d'extension et cliquez dessus.

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. Cliquez sur **Activer**.

Résultats

Après l'activation de Role Management V2, les modifications décrites dans le résultat du script sont appliquées. La colonne Nombre d'héritages (inh_count) de la table Rôles d'utilisateur est en lecture seule et reflète automatiquement le nombre de fois que l'utilisateur hérite d'un rôle.

Activer l'audit des rôles avec Contextual Security : Role Management V2

Définissez une propriété système pour permettre à la table Rôles d'audit de créer des enregistrements d'audit liés aux rôles d'utilisateur.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Lorsqu'elle est activée, la table Rôles d'audit [sys_audit_role] gère les changements apportés aux enregistrements utilisateur. Pour plus d'informations sur les audits de rôles, consultez Auditer les rôles d'utilisateurs. Si le module d'extension Contextual Security : Role Management V2 [com.glide.role_management.inh_count] est installé, vous devez définir une propriété système sur **true** 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 Contextual Security : Role Management V2 [com.glide.role_management.inh_count] est installé, la définition de cette propriété sur **true** 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, le système affiche ce champ en mode lecture seule, c'est pourquoi le champ numérique n'est pas accessible en écriture sur la plupart des incidents.

Si vous configurez le système de façon à ce qu'il vérifie l'écriture des valeurs de tous les champs entrants, 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 deux fois si le champ de numéro peut être rempli par écriture avant de publier des modifications.

Si vous demandez au système de ne pas vérifier les transactions entrantes, le système vous permet d'écrire dans un champ 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 aux sélections de l'utilisateur dans d'autres champs accessibles en écriture.

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 génériques pour les opérations basées sur les enregistrements les plus courantes est disponible : lecture, écriture, création et suppression. Un nombre important d'ACL pour fournir un accès basé sur les rôles aux tables système 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 table à caractère générique restreignent les opérations de lecture, d'écriture, de création et de suppression sur toutes les tables, sauf si l'utilisateur dispose du rôle d'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 ces 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 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 Refus par défaut 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.

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 dans un formulaire ou dans une liste. L'activation de cette option peut avoir un impact sur les performances de votre instance.
Appliquer des ACL à AJAXGlideRecord (enregistrement Glide côté client)	Appliquez les 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 remplacement administrateur au niveau de l'accès	Forcer l'évaluation de l'ACL pour les remplacements administrateur au niveau de l'accès. Par défaut, les utilisateurs dotés du rôle administrateur réussissent automatiquement la vérification des autorisations pour cette règle ACL lorsque l'option Contournements administrateur est sélectionnée dans le formulaire de règles ACL.
Utiliser les 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 de règle d'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. Élevez-vous 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.

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 en savoir plus sur la création de propriétés système, reportez-vous à la section Add a system property .

Propriété système

Propriété	Description
glide.sys_vérification_ligne_de_référence	Contrôle si les conditions de script des règles de contrôle d'accès s'appliquent aux champs de référence d'une table.

Propriété système (suite)

Propriété	Description
	• Type : true | false • Valeur par défaut : **faux** • Emplacement : ajoutez une propriété système à la table Propriétés système [sys_properties]

Remarque :
Si la propriété système n'existe `glide.sys_reference_row_check` pas ou a été définie sur faux, les conditions de script pour les règles de contrôle d'accès ne sont pas appliquées. Cela signifie qu'une ACL contenant des conditions scriptées passera sa vérification tant que les autres critères d'ACL sont respectés (tels que les exigences de rôle).

Appliquer des ACL à AJAXGlideRecord (enregistrement Glide côté client)

Utilisez une propriété système pour effectuer la validation des règles de liste de contrôle d'accès (ACL) lorsque l'accès aux enregistrements côté serveur (par exemple, les tables) se fait via des 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 et qu'il n'a pas le droit de lire la table de `cmn_location` , tout appel d'API `GlideAjax` effectué par l'utilisateur échouera.

Si vous exécutez le système sans vérification d'ACL sur les appels `GlideAjax` , l'API peut renvoyer des informations auxquelles l'utilisateur actuellement connecté ne pourrait pas accéder via l'interface utilisateur.

Remarque :
Définir cette propriété dans **Propriétés système** > **Sécurité**.

Remarque :

Pour en savoir plus sur cette propriété, consultez Activation de la vérification de l'ACL de AJAXGlideRecord Paramètres de renforcement de la sécurité de l'instance.

Évaluer le remplacement administrateur au niveau de l'accès

Si vous souhaitez forcer l'évaluation de l'ACL pour les remplacements 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 nombre d'ACL sur un champ donné et que l'option **Remplacements** administrateur est **définie sur faux** (non sélectionné) sur l'une d'elles, les remplacements administrateur effectifs pour toutes les ACL sont considérés comme **faux**. Dans ce cas, les administrateurs ne peuvent même pas transmettre l'ACL dans laquelle 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 false.

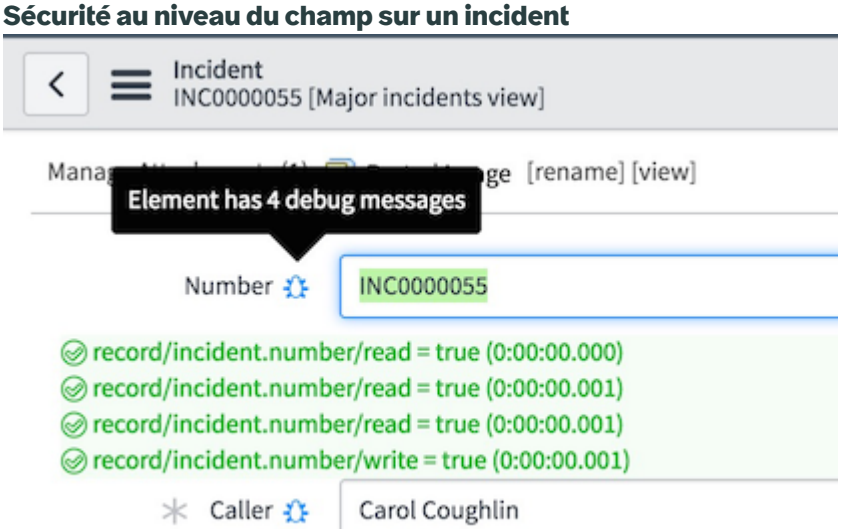
Outils de débogage d'ACL

Des messages de sortie de règle ACL de débogage et d'accès au niveau des champs sont disponibles pour vous aider à dépanner et à déboguer les ACL. L'observateur de configuration des ACL vous permet de savoir quelles ACL connexes existent lorsque vous en modifiez une.

Débogage au niveau des champs

Lorsque le débogage est activé, une petite icône de bogue ( ) apparaît à côté de chaque champ avec une règle ACL. Cliquer sur l'icône répertorie les règles ACL qui s'appliquent au champ et les résultats de l'évaluation. Activez le débogage en accédant à **Sécurité de système** > **Débogage** > **Déboguer les règles de sécurité**.

Sécurité au niveau du champ sur un incident



Traduction automatique

Après avoir activé le débogage d'ACL, vous pouvez emprunter l'identité d'un autre utilisateur pour voir quelles règles ACL l'utilisateur réussit 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 à l'ACL est activé par défaut, même en cas d'emprunt d'identité d'un utilisateur qui ne dispose pas d'un accès en lecture aux tables. Pour modifier cette fonctionnalité, définissez la propriété suivante sur **false**.

Pour activer le débogage de règle ACL, accédez à **Sécurité de système** > **Déboguer les règles de sécurité**.

Propriété système	Description	Paramètre par défaut
glide.security.access_acl_impersonator	Permet d'accorder un 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 empruntant 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 usurpée peut être empêché de lire les données liées à l'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 règle d'ACL au bas de chaque liste et formulaire. Le message de sortie affiche les éléments suivants :

Élément de message	Description
HEURE	Durée totale utilisée 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 la règle ACL>/<Opération>.
CONTEXTE	Objet évalué par la règle ACL.
RC	Code de retour de la règle ACL. Une valeur vraie passe la règle ACL. Une valeur fausse échoue 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 affichent un résultat global de réussite ou d'échec, suivi d'une répartition des résultats pour chaque type de critère ACL : • 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. IAccessHandler 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

Élément de message	Description
	aucun cas modifier les vérifications IAccessHandler. Par exemple, une implémentation IAccessHandler est utilisée pour les contrôles d'accès sur les ressources d'application et cela ne peut pas être modifié. Cette option est disponible à partir de la Istanbul version. • Rôles : vérification que l'utilisateur dispose du rôle correct. • 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 dans la règle ACL (le cas échéant).

Les icônes qui s'affichent montrent comment l'ACL a été évaluée :

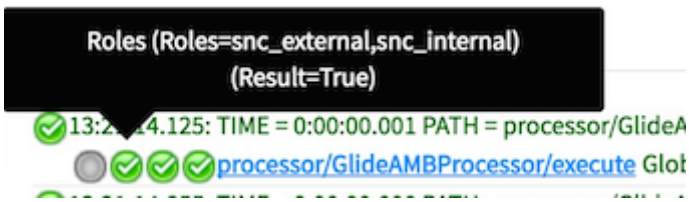
Icône	Description
Une coche verte ( )	Indique que la table ou le champ a satisfait aux critères.
Icône x rouge (icône)	Indique que la table ou le champ n'a pas réussi.
Icône cercle gris vide ( )	Indique que l'évaluation de l'ACL n'a pas eu besoin d'être effectuée.
Une coche bleue, un x ou un cercle vide	Indique que l'ACL a été extraite d'un résultat mis en cache d'une vérification d'ACL précédente. Les icônes signifient la même chose que ci-dessus.

Vous pouvez effectuer les actions suivantes sur la sortie de débogage d'ACL :

- Cochez ou décochez ces cases en haut de la sortie de débogage :
  - **Règles de sécurité** : affichez ou masquez les résultats des contrôles d'ACL.
  - **Autres** : affichez ou masquez d'autres avertissements ou messages.
- Cliquez sur le nom de l'ACL en regard de l'un des messages de sortie pour ouvrir cet enregistrement ACL.

Traduction automatique

- Placez le pointeur de la souris sur l'une des icônes des quatre vérifications d'ACL pour afficher plus d'informations.



Référence de dépannage ACL

Une liste des erreurs courantes de règle ACL et 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. En l'absence d'une règle ACL de table explicite, les utilisateurs doivent transmettre les autorisations dans la règle ACL de caractère générique de table (*) qui, par défaut, restreint l'accès aux administrateurs uniquement. Activez le débogage et déterminez quelles règles ACL 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 les règles ACL évaluées pour le champ. Vérifiez qu'il n'y a pas de règle ACL de table ou de champ ACL en conflit.
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 qui interfère avec la règle ACL de table. Activez le débogage et déterminez les règles ACL évaluées pour la table.
Vous pouvez voir un champ dans une liste, mais pas dans un 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 qu'il adopte le même comportement dans la liste et le formulaire.
Vous recevez un message d'erreur lors de la tentative d'exécution d'un script include de processeur ou de client pouvant être appelé.	Il existe une règle ACL pour le processeur ou l'include de script pouvant être appelé 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 pour le processeur ou le script include. Mettez à jour la règle ACL ou les rôles d'utilisateur selon les besoins pour accéder à l'objet.

Observateur de configuration d'ACL

L'observateur de configuration des 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 résumé des règles de sécurité dans laquelle vous pouvez afficher les ACL associées à celle que vous modifiez. Vous ne pouvez pas modifier les ACL à partir de la fenêtre des règles de sécurité. Pour effectuer des modifications, fermez la fenêtre d'observateur et accédez à ces ACL.

L'observateur de configuration d'ACL n'apparaît pas dans les situations suivantes :

- Si vous enregistrez ou mettez à jour un enregistrement ACL sans réellement y apporter de modifications.
- Si vous effectuez des mises à jour mineures (et non une insertion ou une suppression), telles que la mise à jour des scripts, des conditions et de l'option admin-overrides.
- Si l'enregistrement ACL n'est pas actif.

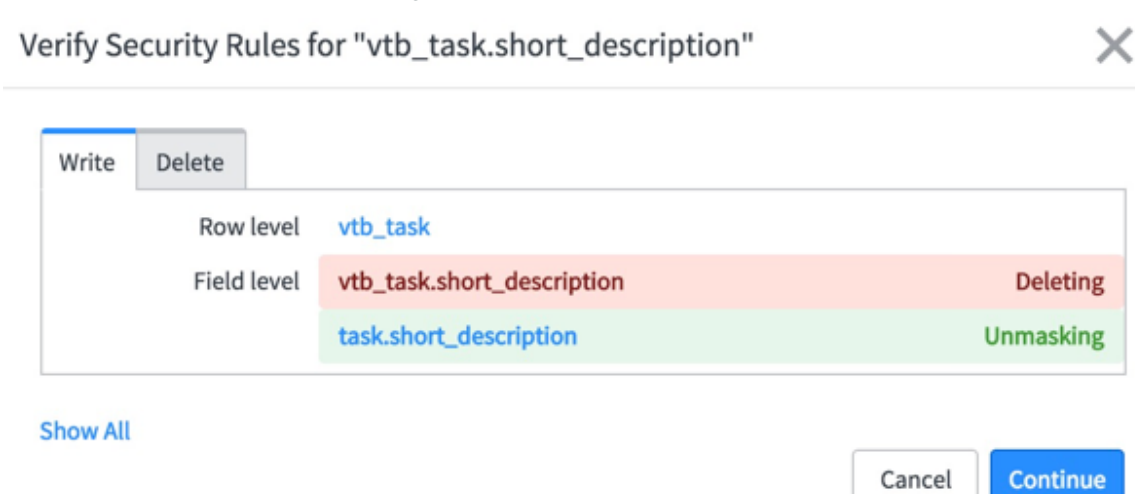
Fenêtre Règles de sécurité ACL

L'observateur de configuration affiche le plan d'exécution de l'ACL. Le plan d'exécution est affiché 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.
surbrillance verte	ACL ajoutée ou active.
Masqué	ACL effective jusqu'à ce que vous apportiez un changement.
Démasqué	ACL qui vient d'être effective lorsque vous avez effectué un changement.

Exemple d'observateur de configuration



Afficher le plan d'exécution ACL

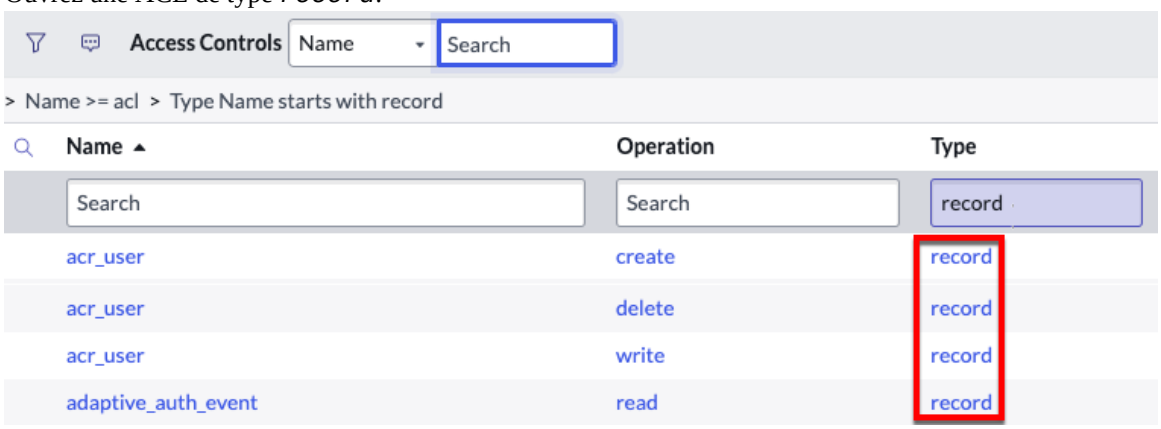
Les administrateurs peuvent voir comment les ACL sont liées les unes aux autres en affichant un plan d'exécution pour n'importe quelle ACL de l'instance.

Avant de commencer

Rôle requis : security_admin

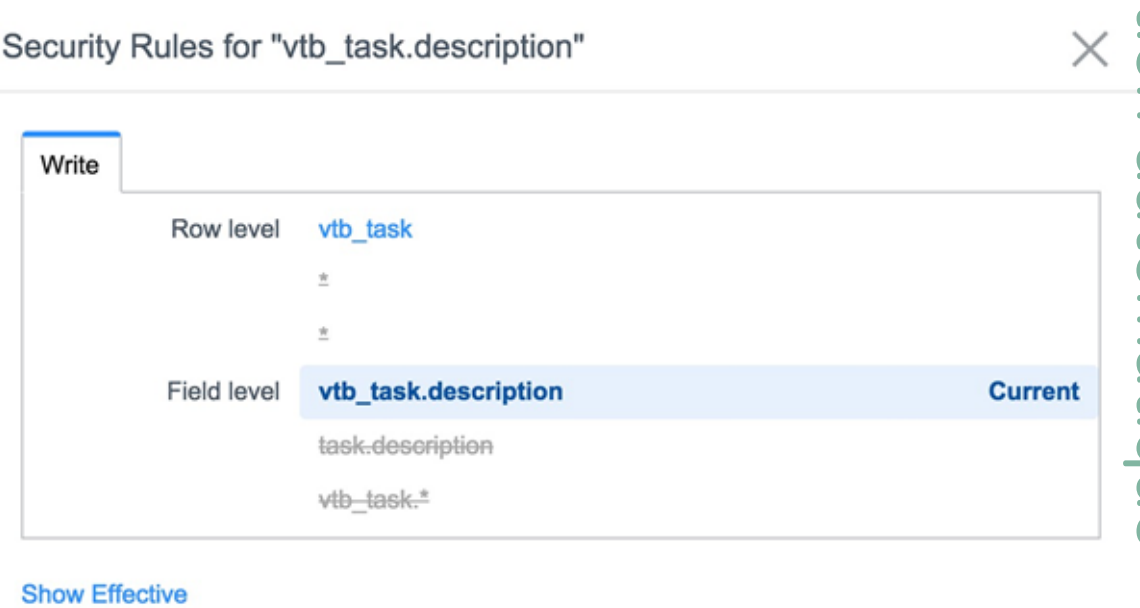
Procédure

1. Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Contrôle d'accès (ACL)**.
3. Ouvrez une ACL de type *record*.



4. Cliquez sur **Afficher le plan d'exécution 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 ».



Fenêtre Plan d'exécution ACL

Élément de l'interface utilisateur	Description
Titre	Nom de l'ACL.
Nom d'onglet	Si l'ACL est créée, en lecture, en écriture ou supprimée.
Niveau de ligne	ACL de niveau ligne 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 **Afficher tout** pour afficher toutes les ACL associées, y compris les ACL remplacées et les ACL génériques qui s'appliquent à tous les enregistrements.
   Les ACL remplacées traversent le nom par une ligne, tandis que les ACL génériques comportent un astérisque générique (*).
6. Affichez uniquement les ACL immédiates associées à celle que vous consultez et masquez les ACL sur les tables à partir desquelles la table ACL est étendue et les ACL génériques génériques (*) en cliquant sur **Afficher effectif**.

Utiliser l'observateur de configuration d'ACL

Utilisez l'observateur de configuration d'ACL après votre élévation au rôle security_admin.

Avant de commencer

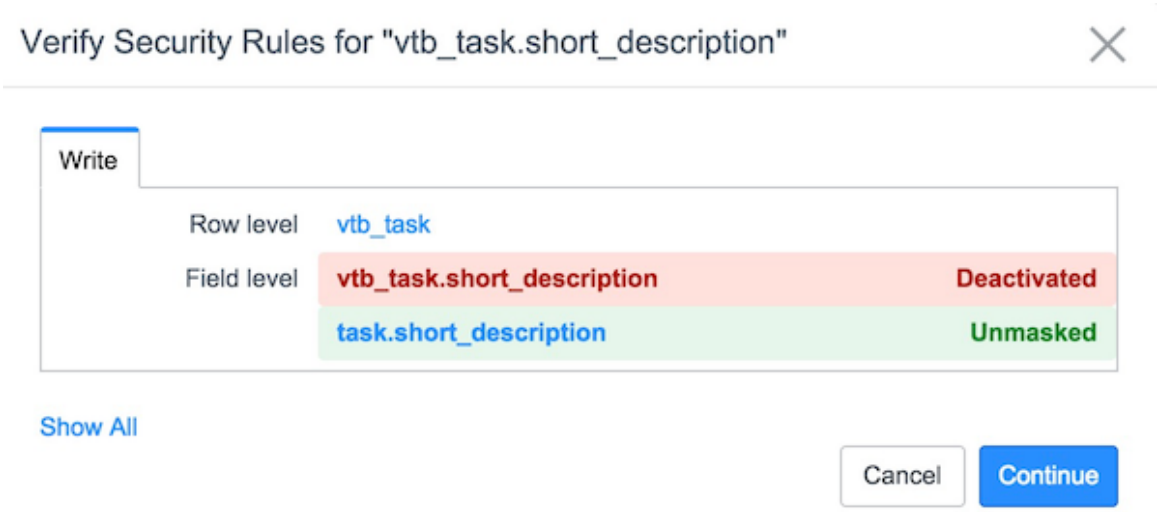
Rôle requis : security_admin
Élever à un rôle privilégié

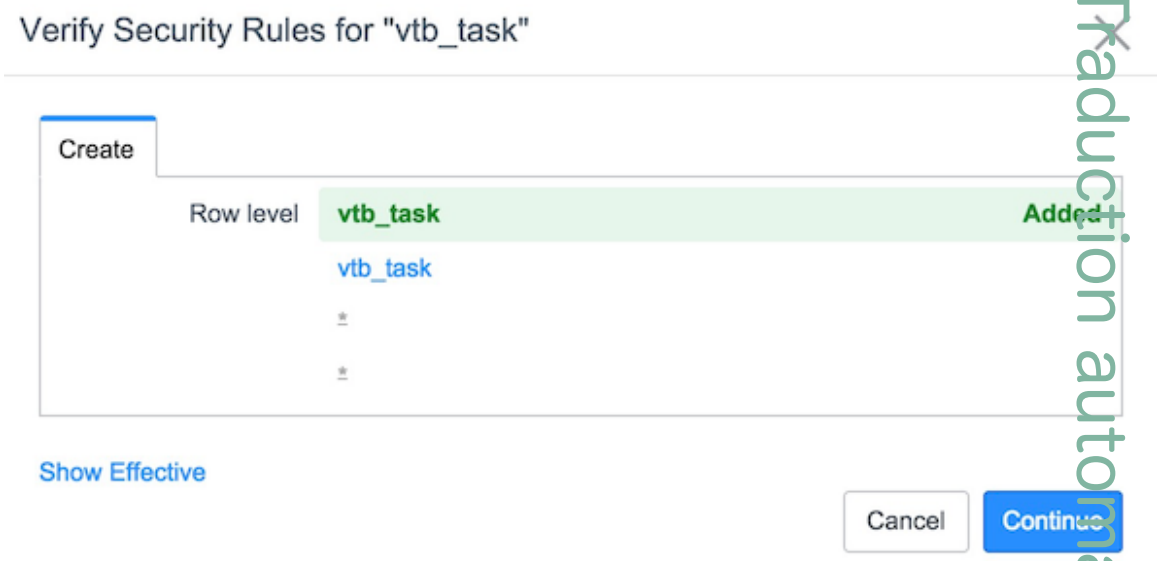
Procédure

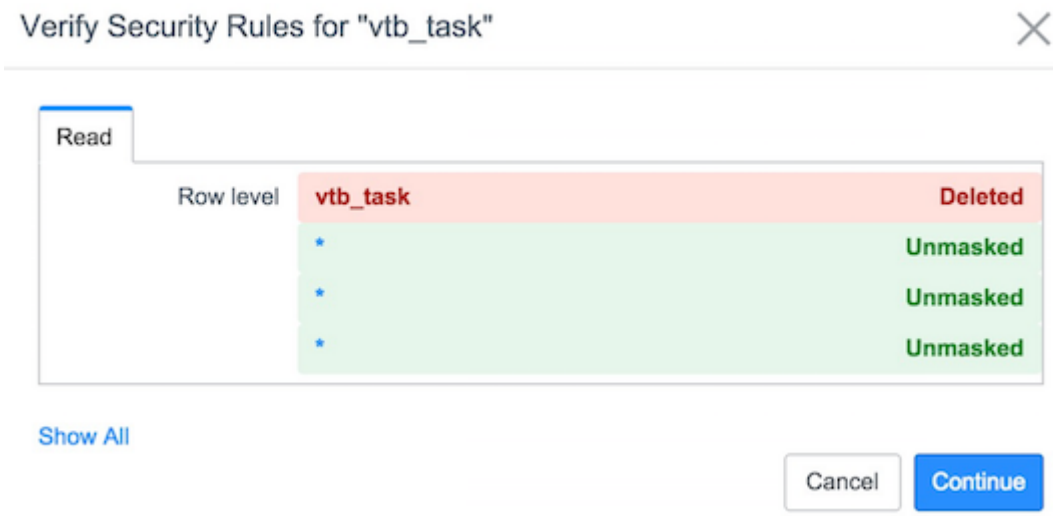
1. Ouvrez une ACL qui est une ACL de type enregistrement.
2. Effectuez une action sur l'ACL, telle que la modifier, ou sélectionner une option dans le menu contextuel comme **Insérer**.
3. Si vous avez modifié des valeurs sur le formulaire Contrôle d'accès, cliquez avec le bouton droit sur l'en-tête et sélectionnez **Enregistrer** ou cliquez sur **Mettre à jour** ou **Supprimer**.

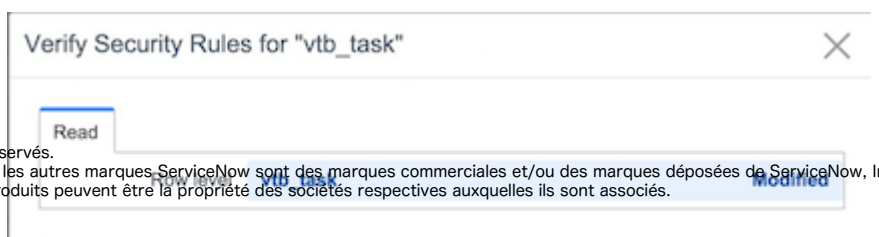
   La fenêtre Règles de sécurité s'affiche. Le système n'a pas encore effectué l'action de base de données sur l'ACL, de sorte que les modifications ne sont pas encore enregistrées.

   Voici des exemples de règles de sécurité sur la table Tâche privée [vtb_task] de l'application Visual Task Board. Voir Observateur de configuration d'ACL pour une description des éléments de cette fenêtre.









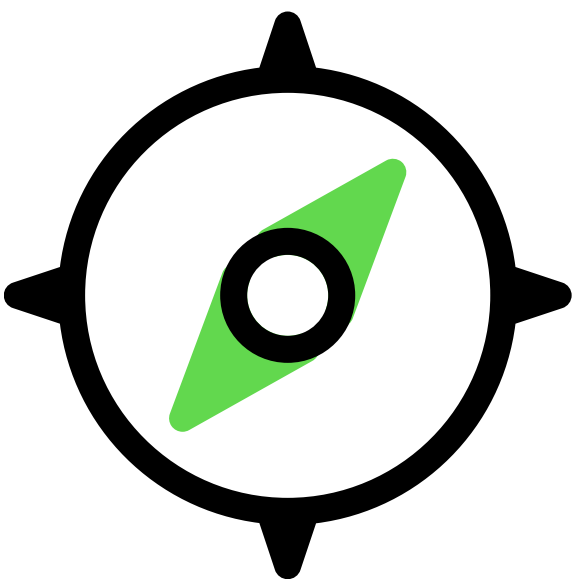
4. Comme pour le plan d’exécution, vous pouvez cliquer sur **Afficher tout** pour afficher toutes les ACL associées, y compris celles qui sont remplacées et les ACL génériques qui s’appliquent à tous les enregistrements, ou cliquer sur **Afficher** effectif pour afficher uniquement les ACL immédiates associées à celle que vous consultez.
5. Passez votre souris sur l’une des ACL pour afficher une description.

Page d’accueil des attributs de sécurité

Les attributs de sécurité offrent une alternative flexible aux listes de contrôle d’accès.

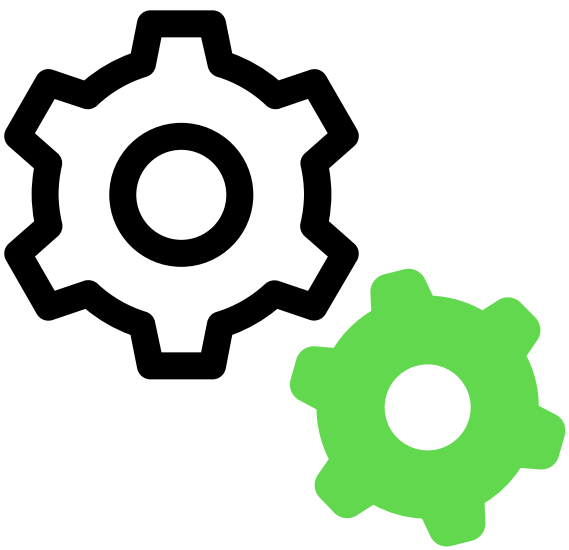
Premiers pas

Explorer les attributs de sécurité



Apprendre les principes de base des attributs de sécurité

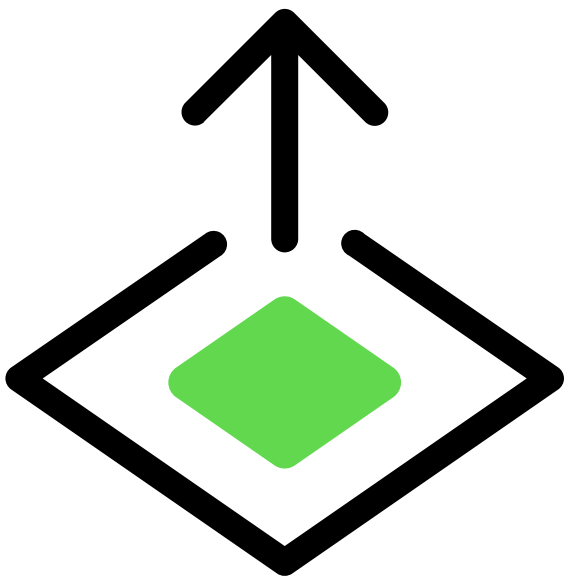
Créer des attributs de sécurité



Créer des attributs de sécurité

Traduction automatique

Attributs de sécurité OOB (prêts à l'emploi)



Expliquer les attributs de sécurité OOB

Journalisation des attributs de sécurité

Examiner la journalisation des attributs de sécurité

Notions fondamentales des attributs de sécurité

Un attribut de sécurité est un élément d'information hautement configurable sur un sujet ou son environnement, lorsqu'il est utilisé dans les contrôles d'accès, permet une configuration de sécurité fine d'une manière non complexe.

Vue d'ensemble

Les attributs de sécurité offrent une méthode alternative de contrôle d'accès via des définitions de rôle à la configuration des listes de contrôle d'accès (ACL) actuellement pratiquée. Les attributs de sécurité offrent plusieurs avantages aux configurations basées sur les ACL :

Meilleure sécurité

L'amélioration du brouillage 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 la sécurité.

Créer des attributs de sécurité

Créez des attributs de sécurité à l'aide d'un guide étape par étape.

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 Champs d'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, consultez 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
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 évaluation.
Colonne de table de recherche	Référencez une colonne de table pour évaluation.
Script	Dérivez une valeur d'un script.

Attributs de sécurité OOB (prêts à l'emploi)

Rôles d'attributs de sécurité généralisés couramment utilisés, prêts à l'emploi.

Vue d'ensemble

Les attributs de sécurité prêts à l'emploi (prêts à l'emploi) constituent un moyen facile de commencer à utiliser et à apprendre les options des attributs de sécurité avec une série de rôles d'attributs 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 OOB, consultez Attributs de sécurité composés

Attributs de sécurité OOB

Attribut	Description
Groupe	L'utilisateur est membre d'un groupe spécifié
Explicite de groupe	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
Séance interactive	Session interactive en cours
Connecté	L'utilisateur est connecté et authentifié
Critères de réseau	Critères de réseau supplémentaires
Rôle	L'utilisateur a un rôle spécifique
Rôle explicite	L'utilisateur a un rôle spécifique explicitement défini

Comportement explicite et non explicite expliqué

Les attributs de sécurité répondent à des besoins d'autorisation nuancés avec une évaluation explicite par rapport à une évaluation non explicite (héritée) des autorisations de rôle.

[qa: BEGIN review]

Example: Séparer l'accès à un profil IT de l'accès au fichier de rôle RH

Nous allons définir un attribut de sécurité qui permet à l'administrateur de voir les fichiers liés aux RH, mais ne permet pas à l'administrateur d'y accéder. Supposons que le rôle administrateur n'est pas défini comme faisant partie du groupe RH, mais qu'il est _____. 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 pour répondre aux besoins de votre entreprise

Vue d'ensemble

Les attributs de sécurité composés sont définis à partir d'un ou de 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 des attributs de sécurité composés

Créez un attribut de sécurité composé pour faciliter sa réutilisation.

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 Champs d'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
Condition	Conditions spécifiques d'attribut de sécurité utilisées pour définir l'évaluation des attributs de sécurité.
Nouveau critère	Ajouter un ensemble supplémentaire de conditions **Or** 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 périmètre des attributs de sécurité

Le comportement dans le champ d'application des attributs de sécurité est cohérent avec les comportements de définition du champ d'application de Platform. Les attributs de sécurité créés dans un champ d'application ne sont disponibles que dans les contrôles d'accès dans le même champ d'application.

Attributs de sécurité locaux et existants

Les attributs de sécurité existants et locaux permettent aux clients de réutiliser les ensembles de conditions d'attributs de sécurité.

Attributs locaux et existants

Le créateur de condition d'attribut de sécurité ACL permet aux clients de spécifier si un attribut de sécurité est existant ou local.

Remarque :
Les conditions d'attributs de sécurité sont définies par défaut sur local.

Un attribut de sécurité défini localement n'est enregistré que dans l'ACL unique dans laquelle il est créé.

L'option existante permet aux utilisateurs de référencer des conditions d'attributs de sécurité existantes au créateur de condition.

Data Classification

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

Référence pour la classification des données

Découvrez comment la classification des données fonctionne avec les données de démonstration.

Analyser les classifications de données

Découvrez comment analyser les classifications de données.

Exploration de la classification des données

En savoir plus sur la classification des données.

Data Classification Active la prise en charge de :

- Visibilité sur les types de données hébergées sur des Now Platform instances.
- Conformité aux lois sur la protection de la vie privée et respect des exigences réglementaires pour des 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 aux entrées de dictionnaire existantes dans n'importe quelle table. Consultez Data dictionary tables pour plus d'informations.

- Vous pouvez classer les données comme bon vous semble pour votre entreprise et 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, consultez Installation

des données de démonstration du module d'extension Data Classification et Composants installés avec Data Classification des données de démonstration.

- Si vous créez vos propres classifications de données, vous pouvez également concevoir un système hiérarchique à plusieurs niveaux 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 la façon dont vos utilisateurs mondiaux, régionaux et internationaux peuvent avoir besoin d'approches différentes de la 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 Vue d'ensemble pour répondre à 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 : REST API
- DCManager : global
- ScopedDCManager - Inclus dans le périmètre

Remarque :
Data Classification prend en charge la 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 donner aux individus le contrôle de 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 à caractère personnel (PII) lorsque cela est nécessaire pour suivre les données soumises à la réglementation des lois locales sur la Now Platformprotection de la vie privée. Lorsque vous installez des données de démonstration, ce code de classification est automatiquement appliqué à certains champs sensibles pour la sécurité dans la table Utilisateur [sys_user]. Pour en savoir plus, consultez :

- Composants installés avec Data Classification des données de démonstration
- Affectation de classifications de données à des entrées de dictionnaire

Vous pouvez appliquer une classification de données restreintes aux colonnes de la table Employé qui stockent des informations sensibles sur les employés, telles que les numéros de sécurité sociale (SSN). Les administrateurs et les auditeurs peuvent ensuite utiliser le tableau de bord Vue d'ensemble pour confirmer que vous avez affecté des classifications de données aux colonnes correctes. Ils peuvent également afficher les détails de classification pour les types d'informations restreints.

Installation des données de démonstration du module d'extension Data Classification

Lorsque vous effectuez une mise à niveau vers ou une installation Washington DC (et versions ultérieures), le module d'extension Data Classification (com.glide.data_classification) est automatiquement activé. Toutefois, vous devez installer manuellement les données de démonstration fournies avec le module d'extension. Il inclut plusieurs classifications de données prédéfinies importantes et affecte également l'une d'entre elles à des colonnes de table Utilisateur [sys_user] spécifiques 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 Data Classification ajoute les rôles d'utilisateur suivants dans votre instance :

- data_classification_admin : peut gérer tous les aspects de l'application, y compris la configuration et l'affectation Data Classification de la classification des données.
- data_classification_auditor : peut auditer Data Classification les affectations de code effectuées aux tables et colonnes de l'utilisateur.

Important :

Avis concernant l'utilisation par les clients :

Toutes les décisions relatives à la mise en œuvre de cette application sont à la seule discrétion du Client. Les clients reconnaissent et acceptent que l'utilisation de l'application n'engage en rien ServiceNow à se conformer à une loi ou à une réglementation, et que toute suggestion de langage, de champ ou de classification fournie prête à l'emploi avec l'application ne constitue pas un avis juridique émis par ServiceNow.

Les clients demeurent seuls responsables du respect de leurs obligations légales en vertu des lois en vigueur, y compris (mais sans s'y limiter) des lois sur la protection des données, les exigences de sécurité et la confidentialité, et sont responsables de la configuration et de la modification nécessaire de cette application, y compris (mais sans s'y limiter) des 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 Data Classification à l'aide des critères de filtre et de la barre de recherche. Un message Installed (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 Data Classification des données de démonstration

Lorsque vous installez les données de démonstration incluses dans le module d'extension Data Classification (com.glide.data_classification), plusieurs types de composants sont installés dans votre instance. Ces composants comprennent des classifications de données prédéfinies et des affectations de code pour des colonnes Utilisateur [sys_user} spécifiques.

Classifications de données installées

Classification des données	Description
Confidentiel	Données sensibles qui, si elles étaient compromises, pourraient avoir un impact négatif sur les opérations.
Interne	Données internes non destinées à être divulguées publiquement.
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	Des données d'entreprise hautement sensibles qui, si elles étaient compromises, pourraient exposer l'organisation à un risque financier ou juridique.

Data Classification 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 Data Classification table [data_classification] que vous pouvez ensuite affecter à des colonnes spécifiques dans des tables spécifiques.

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 une classification de parent à enfant.
Application	Champ d'application de cette classification de données.

4. Si cette classification de données doit être une classification de parent à enfant, cliquez sur **Nouveau**.
   Si vous ne souhaitez pas créer de classifications des 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 une classification de parent à enfant.
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 spécifiques dans la table Dictionnaire [sys_dictionary]. Lorsque vous affectez des classifications de données, il crée des entrées dans la table Dictionnaire-Classe de données [m2m_dictionary_dataclass], que vous pouvez ensuite examiner dans le tableau de bord Vue d'ensemble.

Avant de commencer

Rôle requis : data_classification_admin et admin

Procédure

1. Dans la fenêtre Navigator (Navigateur), saisissez `sys_dictionary.list`.
2. Dans Entrées de 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 **Classifier**.

   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 que vous avez sélectionnés, puis cliquez sur **Classer**.

   Avertissement :
   Cela remplacera toutes les classifications existantes pour les éléments de dictionnaire sélectionnés.

   Vous pouvez sélectionner plusieurs classifications de données selon vos besoins.

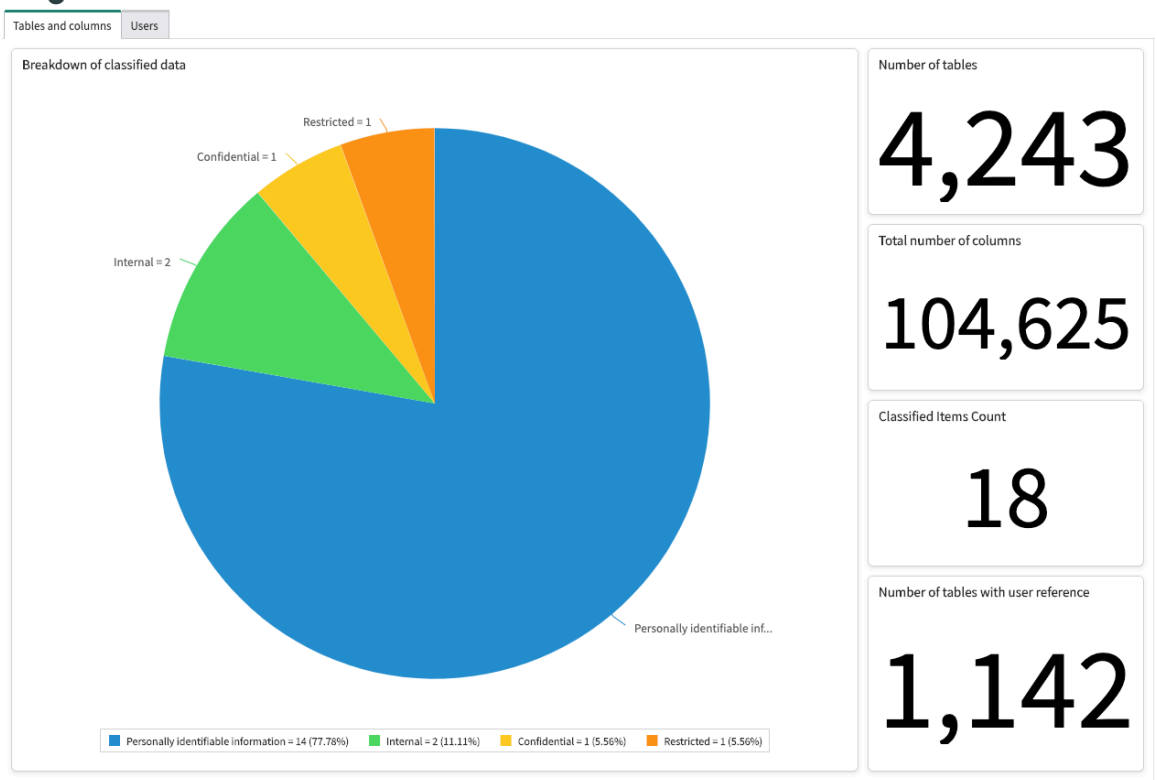
   Pour plus d'informations, reportez-vous à la rubrique Tables du dictionnaire de données .

Analyser les classifications de données à l'aide du tableau de bord Vue d'ensemble

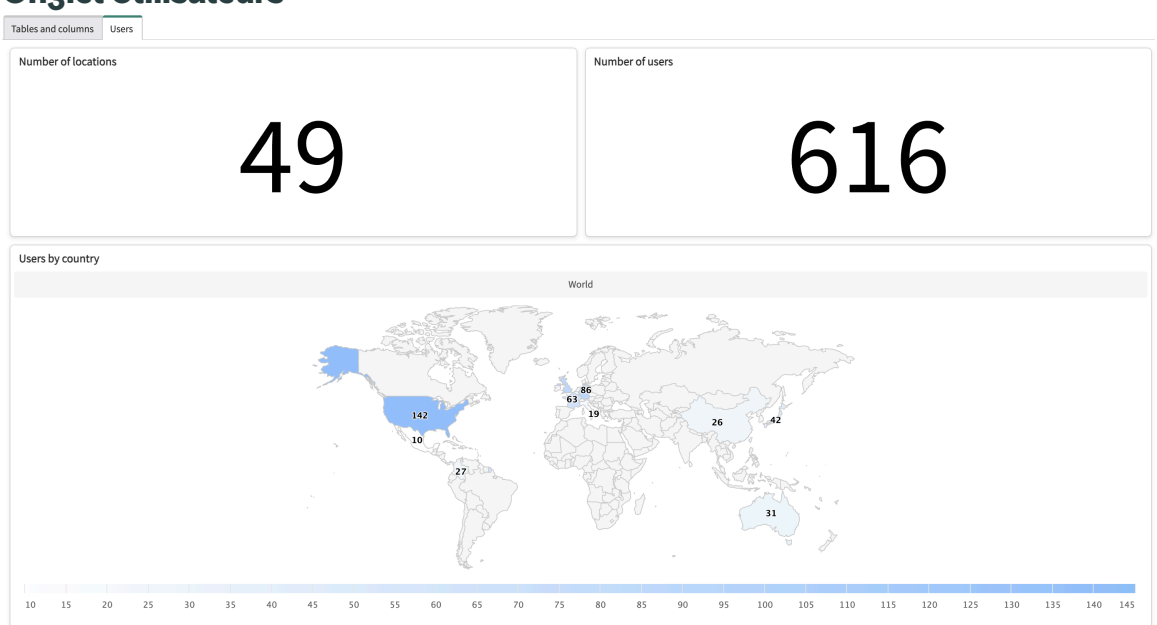
Le tableau de bord Vue d'ensemble indique l'état actuel des classifications de données au sein de votre instance et la façon dont vos utilisateurs sont répartis par emplacement.

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 renforcer la sécurité et la conformité aux lois sur la confidentialité. En utilisant le champ Emplacement dans les enregistrements utilisateur, les administrateurs mappent les utilisateurs dans différentes régions où les réglementations en matière de confidentialité diffèrent.

Onglet Tables et colonnes



Onglet Utilisateurs



Rôles Now Platform requis

- data_classification_admin : administre tous les aspects de l'application, y compris la classification des données, la configuration et l'affectation Data Classification .
- data_classification_auditor : Audite les affectations de Data Classification code.

Traduction automatique

Cas d'utilisation

Pour obtenir d'autres exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez Cas d'utilisation dans Data Classification.

Utilisateur	Utilisation du tableau de bord
data_classification_admin	Confirmez que vous avez affecté des classifications de données aux champs corrects de votre instance.
data_classification_auditor	Auditez la sénilité et la sécurité des données dans votre instance.

Rapports

Titre	Type	Table source	Description
Répartition des données classées	Graphique circulaire	m2m_dictionary_dataclass	Fournit une répartition des classifications des données d'instance, par classe de données.
Nombre total de tables	Score unique	sys_dictionary	Nombre total de tables de données dans votre instance.
Nombre total de colonnes	Score unique	sys_dictionary	Nombre total de colonnes de données classifiées dans votre instance. Ce nombre correspond au nombre de colonnes auxquelles vous avez affecté des classifications de données.
Nombre d'éléments classés	Score unique	m2m_dictionary_dataclass	Nombre total de tables auxquelles des classifications de données ont été affectées.
Nombre de tables avec référence utilisateur	Score unique	sys_dictionary	Nombre total de tables ayant au moins une colonne qui fait référence à la table sys_user.
Nombre d'emplacements	Score unique	sys_dictionary	Nombre total d'emplacements dans votre instance.
Nombre d'utilisateurs	Score unique	sys_user	Nombre total d'utilisateurs dans votre instance.
Utilisateurs par pays	Carte	sys_user	Répartition géographique des utilisateurs par pays.

Séparation de domaine et Data Classification

Domain Separation est pris en charge pour Data Classification . 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 : 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 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 Data Classification

Pour Domain Separation, l’application utilise la séparation de processus pour la Data Classification 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 Explication de Domain Separation.

Information associée

Séparation de domaine pour les fournisseurs de services

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.

Explorez la filtration des données

En savoir plus sur le filtrage de 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

Exploration de la 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.

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 d'objet 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.

Créateur de condition basé sur l'attribut d'objet

Utilisez des attributs d'objet pour évaluer le rôle d'utilisateur, le groupe, les critères d'objet ou l'adresse de réseau IP.

La filtration des données utilise un modèle basé sur le refus

La filtration des données utilise un modèle basé sur le refus pour contrôler l'accès aux enregistrements. Avec le filtrage des données, votre instance refuse l'accès aux enregistrements, sauf si un enregistrement répond aux critères définis par le filtrage des données.

Application de la filtration des données

Les règles de filtration 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 filtration des données est cohérente avec celle des ACL en lecture.
- Le filtrage des données, comme les ACL, fonctionne en conjonction avec les comportements existants `Report_view access control list` . Consultez Report_view contrôle d'accès 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 pour 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'enregistrements suivants :

Enregistrements de filtration des données

Créez un enregistrement Filtration des données [sys_df_data_filtration] pour accorder l'accès aux tables sur votre instance. L'enregistrement de filtration des données contient les conditions **d'attributde filtre de données** et d'objet décrites ci-dessus pour limiter le champ d'application de la règle et les utilisateurs affectés.

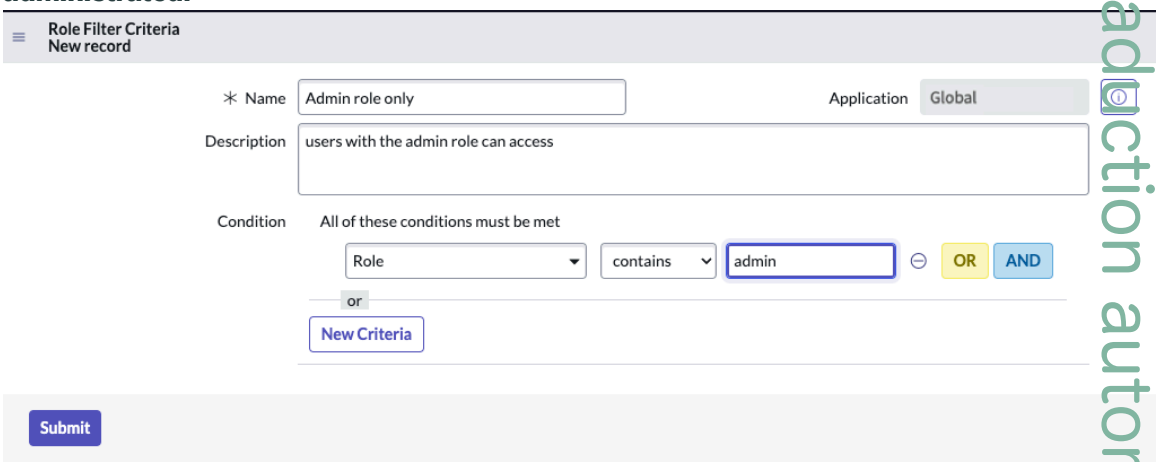
Enregistrements de critères de sujet

Les enregistrements de 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 des 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 Création de critères de sujet.

Après avoir créé des enregistrements de critères de sujet, vous pouvez les appliquer à une règle. Cela se fait dans l'onglet **Condition de l'objet** de votre règle de filtrage des données.

Exemples d'enregistrements d'entrées de critères

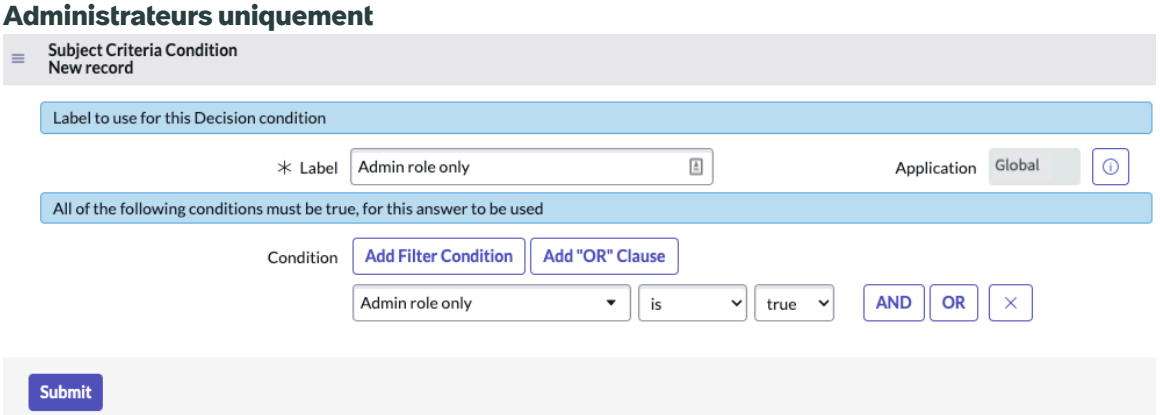
Exemple d'entrée de critères pour tous les rôles contenant un rôle administrateur



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 d'utilisateurs ou de rôles, 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 évaluer les groupes, rôles ou adresses IP d'un utilisateur afin de déterminer l'accès à une table ou à ses enregistrements.

Enregistrements des conditions de critères de sujet

Exemple de condition de critères à l'aide de l'entrée de critères Administrateurs uniquement



Utilisez les enregistrements de condition de critères d'objet [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 condition de critères d'objet unique pour affiner davantage l'accès à vos enregistrements.

Activation de 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.

Création de règles de filtrage des données

Découvrez comment créer des règles de filtrage des données pour permettre à vos utilisateurs d'accéder aux enregistrements dans des tables.

Avant de commencer

Rôle requis : security_admin

Remarque :
Pour créer ou modifier les règles de filtrage des données, vous devez vous élever au rôle privilégié. Pour obtenir des détails sur ce processus, consultez 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 filtrage des données s'affiche.
3. Renseignez les champs du formulaire comme il convient.

Formulaire Filtration des données

Champ	Description
Table	Table à laquelle s'applique cette règle de filtration des données.
Actif	Définit la règle de filtration des données comme active. **Remarque :** Conservez les règles de filtrage des données inactives jusqu'à ce que vous soyez prêt à effectuer le test, afin d'éviter d'empêcher involontairement les utilisateurs d'accéder aux enregistrements.
Description	Description de la règle de filtrage des données.
En cascade	Sélectionnez cette option pour définir la règle de filtration des données à appliquer aux tables étendues.

Champ	Description
	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 plus d'informations sur l'extension de table, consultez Extension de table et classes **Remarque :** Ce champ est activé par défaut.

4. Sélectionnez **Enregistrer** dans le menu de 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. Vous pouvez restreindre le champ d'application de cette règle à des enregistrements spécifiques de la table à l'aide des conditions des onglets **Filtre de données** et **Condition d'objet** .

Ajouter un filtre de données pour votre règle de filtrage des données

Vous pouvez éventuellement utiliser un filtre de données pour affiner le champ d'application de votre règle de filtrage des données afin de ne l'appliquer qu'à des enregistrements spécifiques sur une table.

Avant de commencer

Rôle requis : admin

Procédure

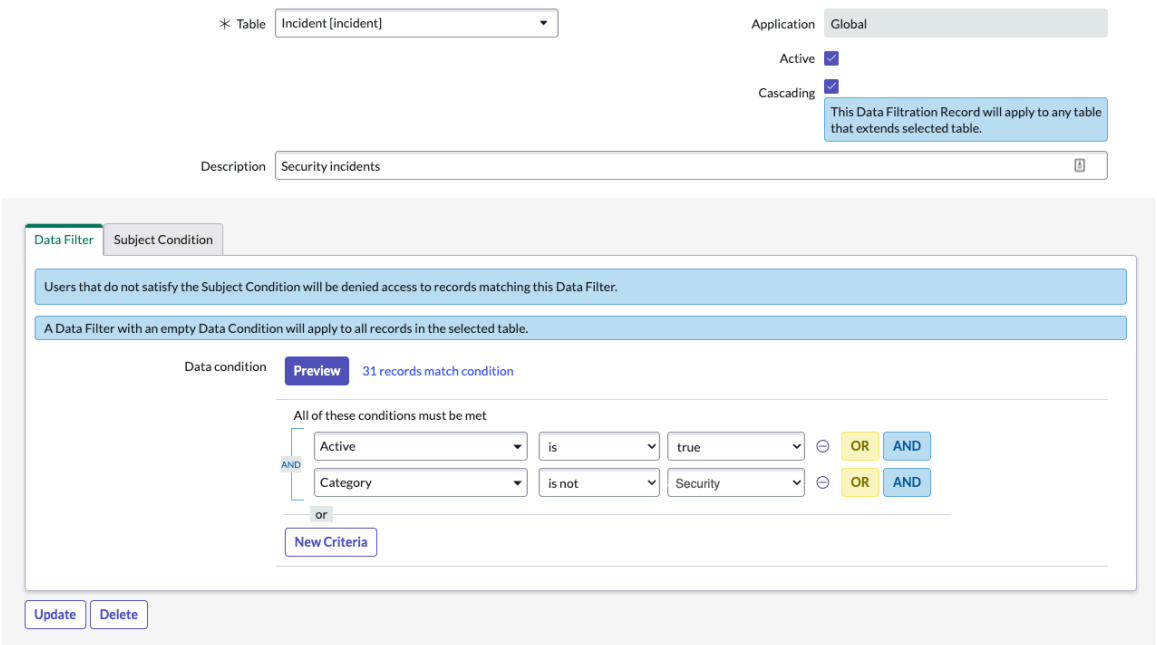
1. Dans votre enregistrement de filtration des données, ouvrez l'onglet **Filtre de données** .
2. Utilisez le créateur de condition pour filtrer les valeurs de champ des enregistrements de table.
   Le filtre de données utilise le même créateur de condition que celui utilisé dans d'autres parties de la plateforme. Pour plus de détails sur l'utilisation de cette interface, consultez Créateur de condition .

   Important :
   L'onglet **Filtre de données** reste vide jusqu'à ce que vous sélectionniez une table dans le champ **Table** .

3. Utilisez le bouton **Aperçu** pour afficher 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 filtration de 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** . Lorsque cette règle est active, les utilisateurs peuvent voir ces enregistrements. Reportez-vous à la section ci-dessous pour utiliser davantage des critères en dehors du contenu de l'enregistrement.



Important :

L'opération not dans vos conditions peut renvoyer des résultats inattendus, selon le type de base de données utilisé par votre instance. Prenons l'exemple de la condition suivante :

Pour cette condition, le résultat attendu serait que l'ensemble de résultats soit tous les enregistrements pour lesquels 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 **de société** vide. Lorsque vous utilisez des requêtes **not** 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 également utiliser des attributs d'objet pour affiner la portée de votre règle de filtrage des données en fonction d'attributs tels que l'adresse de réseau IP, les groupes d'utilisateurs et les rôles, ou les critères d'objet.

Avant de commencer
Rôle requis : admin

Procédure

1. Dans votre enregistrement de filtration des données, ouvrez l'onglet **Critères de sujet** .
2. Utilisez le créateur de condition pour filtrer les enregistrements de table en fonction d'un ou plusieurs des critères suivants.

Options de critères de sujet

Option	Description
Critères réseau	Autorise l'accès aux enregistrements en fonction d'une plage d'adresses IP de réseau ou d'un sous-réseau IP.
Critères de sujet	L'accès aux enregistrements basés sur des critères de sujet. Sélectionnez un enregistrement de critères de sujet pour appliquer ses conditions à votre règle de filtrage des données. Pour en savoir plus sur la création d'enregistrements de critères de sujet, reportez-vous à la section Création de critères de sujet.
Groupe de sujets	Autorisez l'accès si l'utilisateur est membre d'un groupe spécifique. Sélectionnez un groupe à partir de la table **Groupes**[sys_user_group].
Rôle du sujet	Autorisez l'accès si l'utilisateur est membre d'un groupe spécifique. Sélectionnez un groupe à partir de la table **Rôles** [sys_user_role].

Important :
Les conditions de critères de sujet prennent uniquement en charge l'opérateur **is** .

3. Après avoir ajouté vos critères de sujet, cliquez sur **Enregistrer**.

Création de critères de sujet

Créez des enregistrements de critères de sujet à utiliser dans les règles de filtration des données.

Avant de commencer

Rôle requis : security_admin

Important :
Pour créer ou modifier des règles de filtrage de données, vous devez élever à un rôle privilégié. Pour obtenir des détails sur ce processus, consultez Élever à un rôle privilégié.

Procédure

1. Accédez à la **Tous** > **Filtration des données** > **Critères de sujet**.
2. Dans la liste **Critères du sujet** , cliquez sur le bouton **Nouveau** .
   Un nouveau formulaire de critères de sujet s'affiche.
3. Renseignez les champs du formulaire comme il convient.

Champs de critères de sujet

Champ	Description
Nom	Nom des critères de sujet.

Champ	Description
Application	Application incluse dans le périmètre pour les critères de sujet. Ce champ est en lecture seule et se remplit automatiquement avec l'application incluse dans le périmètre actuelle.
Description	Description pour les 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 critère de sujet

Créez une entrée de critères d'objet pour définir les critères par rapport auxquels vos règles de filtrage des données filtrent.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Dans votre enregistrement de 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
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 Critères de filtre d'adresse IP**, **Critères de filtre de rôle** ou **Critères de filtre de groupe** s'affiche, selon votre sélection dans cette étape.
4. Dans le formulaire de critères de filtre, renseignez les champs comme il convient.

Champs de critères de filtres

Champ	Description
Nom	Nom des critères de filtre
Application	Application incluse dans le périmètre pour les critères de sujet. Ce champ est en lecture seule et se remplit automatiquement avec l'application incluse dans le périmètre actuelle.
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.

Champs de critères de filtre pour des types d'entrée spécifiques

Type d'entrée de la politique	Description	Création
Critère de filtre d'adresses IP	Critères de filtre d'adresse 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** ou le **sous-réseau IP (CIDR)** pour définir les 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'IP **de démarrage**. 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 réseau dans le champ **Adresse IP réseau** . 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 données des tâches planifiées déclenchées par un planificateur ne sont pas destinées à être filtrées à l'aide d'un critère de réseau, car elles n'ont pas le contexte de l'adresse IP du client demandeur. Un type de filtration plus approprié peut être la condition de sujet du rôle/groupe.
Critère de filtre de rôle	Utilisez les critères de filtre de rôle 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 créateur de condition dans le **champ Condition** pour sélectionner les rôles de votre entrée.

Type d'entrée de la politique	Description	Création
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 à l'utilisateur par rapport à cette sélection.	Dans la table **Groupes pour les critères** , double-cliquez sur **Insérer une nouvelle ligne**, puis 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 parmi n'importe quelle entrée existante.

Créer une condition de critères de sujet

Créez une condition pour comparer les informations d'un utilisateur avec l'entrée existante de critères de sujet.

Avant de commencer

Rôle requis : security_admin

Les conditions de critères comparent les attributs d'utilisateur aux entrées de critères existantes pour déterminer s'il faut autoriser l'accès aux enregistrements. Pour créer une condition de critères, vous devez avoir créé des critères de sujet. Pour plus d'informations sur ce processus, Créer une entrée de critère de sujetvoir .

Procédure

1. Dans votre enregistrement de critères de sujet, ouvrez l'onglet **Conditions de critères** .
2. Dans la liste **Conditions de critères** , cliquez sur **Nouveau**.
3. Sur le formulaire **Condition de critères de sujet** , renseignez les champs comme il convient.

Formulaire Condition de critères d'objet

Champ	Description
Étiquette	Une étiquette descriptive pour votre condition
Application	Application incluse dans le périmètre pour les critères de sujet. Ce champ est en lecture seule et se remplit automatiquement avec l'application incluse dans le périmètre actuelle.

4. Créez une condition pour votre condition de critères de sujet à l'aide du créateur de condition 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 **or** , toutes les conditions doivent être évaluées sur true pour que la condition de critères de sujet soit évaluée sur true.

6. Cliquez sur **Soumettre** pour enregistrer la condition de critères d'objet.

Que faire ensuite

Utilisez des critères d'objet dans vos règles de filtrage des données pour limiter l'accès aux tables et aux enregistrements. Pour en savoir plus sur l'utilisation des critères d'objet dans les règles de filtrage des données, reportez-vous à Création de 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.

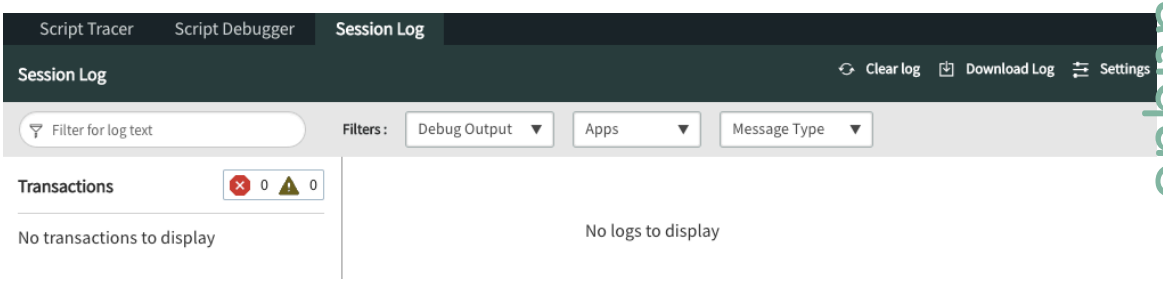
Avant de commencer

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 connexion 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 avez l'intention de voir.

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 fenêtre du navigateur, empruntez l'identité d'un utilisateur pour résoudre les problèmes d'accès de celui-ci.

> **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 d'informations 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 dans lequel vous observez un comportement inattendu.

Il peut s'agir d'un enregistrement que l'utilisateur voit, mais qu'il ne doit pas voir, ou d'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 usurpée, vous devriez commencer à voir la sortie dans le débogueur de session.

5. Recherchez les informations sur la filtration des données dans le débogueur de session.

Cet exemple montre deux messages de journal dans lesquels un filtre de données refusait l'accès aux enregistrements. Les entrées du journal s'affichent en 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 s'affichent en 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 ajuster vos règles de filtrage des données.
Répétez ces étapes pour affiner vos règles et donner aux utilisateurs l'accès dont ils ont besoin.

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.

Explorez la confidentialité des données

En savoir plus sur la confidentialité des données.

Configurer Data Privacy

Découvrez comment configurer Data Privacy.

Rôles dans Data Privacy

Obtenez des détails sur les rôles dans Data Privacy.

Fonctionnalités avancées de Confidentialité des données

Découvrez les fonctionnalités avancées de Data Privacy.

Traduction automatique

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 grâce à la classification et à l'anonymisation. À l'aide de l'application Store Data Privacy, 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 Data Privacy 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 en fonction de critères prédéfinis déterminés par le niveau de sensibilité des types de données dans votre instance. Les niveaux de sensibilité des données aident à déterminer comment chaque type de données classifiées doit être traité. Plusieurs classes prédéfinies sont fournies avec la confidentialité des données au niveau de base. Utilisez la section de classification de Data Privacy pour étiqueter et regrouper les données au sein de votre instance. Ajoutez des classes, affichez la structure des classes 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 les données à l'aide de l'application de stockage Confidentialité des données.

Anonymisation des données utilisateur

En tant qu'administrateur, vous déterminez s'il faut anonymiser toutes les informations de tous les utilisateurs ou d'un sous-ensemble d'utilisateurs. Une fois anonymisées, les données des enregistrements utilisateur sélectionnés sont remplacées par des valeurs aléatoires 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 de stockage Data Privacy.

Options de confidentialité des données

- Confidentialité des données (classique): utilisez d'abord l'application de classification des données pour regrouper vos données par type, à l'aide de classifications de données prédéfinies ou définies par l'utilisateur. Créez ensuite des techniques et des tâches de confidentialité des données pour anonymiser les informations personnelles.
- Confidentialité des données (App Store) : classifiez et anonymisez vos données depuis l'application de confidentialité des données.

Considérations

- Seules les données classifiées peuvent être anonymisées. Pour plus d'informations sur les classes et la classification des données, consultez Classification des données (Classique) ou Classification des données App Store.
- Les informations PII dans les journaux et autres données d'audit ne sont pas anonymisées.

Traduction automatique

- Seules les données structurées peuvent être anonymisées. Les données non structurées, telles que les champs de journal, les commentaires, les pièces jointes et les autres champs où un 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 des systèmes d'authentification unique (SSO) peuvent resynchroniser les informations utilisateur à partir de leurs systèmes sources de vérité. Il n'y a pas de mécanisme en place pour assurer la permanence de l'anonymisation des données sys_user. Pour plus d'informations sur l'administration et la sys_users utilisateurs, consultez la section Administration des utilisateurs .

Domain separation et confidentialité des données

La confidentialité des données n'est pas prise en charge par Domain Separation. 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 classifiés 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, consultez Types de champs .

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
Flotteur	Oui

Type de champ	Disponible par défaut
glide_date	Oui
glide_date_time	Oui
glide_duration	Non
glide_time	Oui
html	Non
icône	Non
entier	Oui
Adr_ip	Non
ip_address	Non
Journal	Non
journal_input	Non
journal_list	Non
Entier long	Oui
name_values	Non
percent_complete	Non
phone_number_e164	Oui
price	Oui
chaîne	Oui
string_full_utf8	Oui
translated_html	Non
translated_text	Non
URL	Non
user_image	Non
Vidéo	Non
wiki_text	Non

Rôles de confidentialité des données

Data Privacy ajoute ces rôles.

Description du rôle

Titre du rôle [name]

Nom du rôle. Le texte entre parenthèses correspond au champ **Nom** dans la table Rôles [sys_user_role].

Description

Description du rôle et de l'utilisation prévue.

Contient des rôles

Liste des rôles contenus dans le rôle.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Abonnement

Indique s'il s'agit d'un rôle d'utilisateur payant qui nécessite l'allocation d'utilisateurs disposant de ce rôle à des abonnements.

Élevé

Indique si le rôle est élevé. Les rôles élevés ne sont pas affectés à des utilisateurs ou à des groupes et doivent être utilisés par élévation. Pour plus d'informations, consultez Élever à un rôle privilégié.

Considérations

Avertissements ou autres considérations à l'intention des administrateurs.

Remarque :

Simplifiez l'administration des utilisateurs en attribuant des rôles à des groupes plutôt qu'à des utilisateurs individuels. Créez des groupes contenant tous les rôles nécessaires pour des profils spécifiques, puis affectez des utilisateurs à ces groupes. Lorsque les utilisateurs changent de rôle, vous pouvez réaffecter les groupes et éviter les cas où les utilisateurs conservent des rôles inattendus.

Pour plus d'informations sur l'administration des utilisateurs, des groupes et des rôles, consultez Administration des utilisateurs .

Administrateur de la confidentialité des données

Les rôles administrateur de confidentialité des données sont un rôle d'administrateur utilisé pour créer des techniques et des politiques de confidentialité des données.

Administrateur de confidentialité des données [data_privacy_admin]

Contient des rôles

Aucun

Affectés à des groupes

Aucun

Abonnement

Non

Élevé

Non

Considérations

Évitez d'affecter ce rôle à vos utilisateurs lorsque des rôles plus ciblés sont disponibles.

Auditeur de la confidentialité des données

L'auditeur de confidentialité des données est un rôle en lecture seule utilisé pour afficher les enregistrements de confidentialité des données.

Auditeur de la confidentialité des données [data_privacy_auditor]

Contient des rôles

Aucun

Affectés à des groupes

Aucun

Abonnement

Non

Élevé

Non

Considérations

Aucun

Processeur de clone Data Privacy

Les utilisateurs disposant du rôle de processeur de clone pour la confidentialité des données peuvent créer et exécuter des tâches de confidentialité des données de classe données.

Processeur de clone Data Privacy [data_privacy_clone_processor]

Contient des rôles

Aucun

Affectés à des groupes

Aucun

Abonnement

Non

Élevé

Oui

Considérations

Aucun

Processeur de confidentialité des données

Les utilisateurs dotés du rôle de processeur de confidentialité des données créent et exécutent des tâches de confidentialité des données sur la table utilisateur [sys_user].

Sous-traitant de la confidentialité des données [data_privacy_processor]

Contient des rôles

Aucun

Affectés à des groupes

Aucun

Abonnement

Non

Élevé

Oui

Considérations

Aucun

Confidentialité des données (classique)

Data Privacy (Classic) est disponible en tant que version familiale. Les dernières mises à jour de la famille ont été publiées lors du lancement de Tokyo.

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 associés ServiceNow® Store , le cas échéant.

Avant de commencer

La confidentialité des données nécessite un abonnement distinct du reste de la Now Platformgamme .

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.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les éléments suivants sont installés avec Data Privacy :

- Modules d'extension
- Rôles
- Tables

Pour plus d'informations, consultez Composants installés avec Data Privacy (Classic).

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Trouvez le module d'extension Confidentialité des données (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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

Composants installés avec Data Privacy (Classic)

Découvrez les composants installés avec le module d'extension de confidentialité des données (com.glide.data_privacy).

Tables installées

Table	Description
Tâche fédérée Confidentialité des données [dp_federated_job]	Tâches fédérées pour la confidentialité des données
Tâche Confidentialité des données [dp_job]	Tâches Confidentialité des données
Tâche Confidentialité des données [dp_job_summary]	Résumés des tâches de confidentialité des données
Technique 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 champs classifiés Confidentialité des données
Configuration de la confidentialité [dp_configuration]	Configurations de Data Privacy
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 de confidentialité des données avec des paramètres

Table	Description
Valeur de paramètre de la technique de confidentialité [dp_technique_with_parameter_value]	Valeurs de paramètre utilisées dans les techniques de confidentialité des données avec des paramètres.

Configuration de Data Privacy (classique)

Découvrez comment créer des techniques et des politiques de confidentialité des données, et comment créer et exécuter des tâches de confidentialité des données.

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. Reportez-vous à la rubrique Créer une configuration technique de confidentialité des données pour associer une technique de confidentialité à une **configuration de technique de confidentialité** associée.

Politiques 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 Confidentialité des données

Les tâches de confidentialité des données utilisent tous ces composants pour anonymiser vos données. Pour en savoir plus sur ces tâches, reportez-vous à Configurer une tâche de confidentialité des données.

Créer une configuration technique de confidentialité des données

Créez une configuration technique de confidentialité des données pour personnaliser la façon dont confidentialité des données anonymise vos données.

Avant de commencer
Rôle requis : data_privacy_admin et admin

Procédure

1. Élevez-vous au **rôle data_privacy_admin** .
   Pour plus d'informations sur l'élévation des rôles, 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. Cette option ne modifie pas les champs lorsqu'ils sont sélectionnés.
Remplacement aléatoire	Cette technique échange les valeurs avec des valeurs générées de manière 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. Si ce champ 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 par le 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, astérisques (*) est utilisé 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 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 (nulles).

Remarque :
La valeur précédemment prise en charge **Remplacer** est déconseillée et renommée **Remplacement-Déconseillé** et ne doit pas être utilisée.

6. Cliquez avec le bouton droit sur l'en-tête, puis cliquez sur **Enregistrer** dans le menu contextuel.
   Une fois l'enregistrement sauvegardé, la liste **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.
   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 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. Si ce champ est laissé vide, le masquage se termine par le dernier caractère.	(Vide)
exclude_char	Caractère pour ignorer le masquage. Un seul caractère peut être utilisé dans cette valeur. Si plus d'un caractère est saisi, 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 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 true** pour préserver la longueur des données. Les données anonymisées 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 true** pour remplacer les données par	faux

Valeur du paramètre Technique de confidentialité	Description	Valeur par défaut
	des valeurs générées de façon aléatoire. Seules les données de chaîne et de numéro peuvent être remplacées par des valeurs 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, sys_user et autres, ainsi que les colonnes à anonymiser, en fonction du cas d'utilisation et spécifie les types paramétrés des techniques à utiliser lors de l'anonymisation des données.

Remarque :
Pour effectuer une configuration de confidentialité, vous devez d'abord configurer une technique de confidentialité des données. Consultez Créer une configuration technique de confidentialité des données pour plus d'informations.

Rôle requis : data_privacy_admin et admin

Procédure

1. Élevez-vous au **rôle data_privacy_admin** .
   Pour plus d'informations sur l'élévation des rôles, 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 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.

- **Appliquer lors du clonage** : cette option devient disponible. Lorsque cette option est sélectionnée, la configuration de confidentialité s'exécute pendant le clonage de confidentialité des données.
- **Ordre de l'application** : une tâche de confidentialité des données pour la configuration Postclone avec un ordre d'application plus élevé peut commencer avant une autre tâche avec un ordre inférieur.

> **Important :**
> Évitez de créer plusieurs politiques de confidentialité des données avec le même ordre d'application, car l'ordre de traitement qui en résultera pour celles ayant le même ordre sera incohérent.

7. **Facultatif :** Sélectionnez **Prise en charge** de 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 classées** pour la confidentialité pour afficher la liste **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 **DoNothing** 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 des tâches de confidentialité des données.

11. Sélectionnez **Soumettre** ou **Enregistrer** pour sauvegarder 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 afin d'utiliser des données anonymisées 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 d'anonymisation :

- 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 d'informations sur l'élévation des rôles, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Tâche Confidentialité des données**.
3. Dans la liste Tâches de confidentialité des données, cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire.

Champs de tâche 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.
Utilisateurs	Sélectionnez les utilisateurs ou le groupe d'utilisateurs à anonymiser dans cette tâche. Il est possible de traiter jusqu'à 1 000 utilisateurs d'un groupe. **Remarque :** Ce champ s'affiche uniquement lorsque la condition de politique de confidentialité sélectionnée nécessite une sélection d'enregistrements utilisateur.
Essai	Exécutez la tâche en tant que 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. **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 :

Champ	Description
	○ **Prêt à planifier** : état par défaut pour les nouvelles tâches. ○ **Restauration en cours** : la tâche a été définie pour restaurer l'anonymisation. ○ **Restauration terminée** : la restauration de la tâche d'anonymisation s'est terminée avec succès. Un champ en lecture seule.
Estimer le nombre d'enregistrements	Nombre estimé d'enregistrements affectés par cette tâche. Un champ en lecture seule.
Résumé	Un 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 en temps universel coordonné basée sur une notation de temps de 24 heures.
Fin de la fenêtre de temps	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 prochain début de la fenêtre horaire. L'heure de fin doit être postérieure à l'heure de début. Une valeur de temps valide est en temps universel coordonné basée sur une notation de temps de 24 heures.

5. Cliquez avec le bouton droit dans l'en-tête du formulaire et sélectionnez **Enregistrer** dans le menu contextuel.
   Après avoir sauvegardé l'enregistrement, les boutons **Planifier la tâche** et **Supprimer la tâche** apparaissent.
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 de temps** et Fin de la **fenêtre de temps** . Si la tâche n'est pas terminée pendant la fenêtre d'heure de début et de fin, elle se poursuivra au début de la fenêtre horaire 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 la même tâche, créez une tâche de confidentialité des données en utilisant les 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'affiche 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.

- **Reprendre** : redémarre une tâche en pause. La restauration n'est pas prise en charge pour les tâches reprises si elle est mise en pause. Annulez la tâche et créez une tâche de confidentialité des données. L'enregistrement utilise un contexte de restauration non expiré.

Restauration des tâches de confidentialité des données

Les modifications apportées à la base de données sont capturées pour des actions telles que des tâches et des scripts afin que les modifications puissent être annulées. 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 un 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 . Reportez-vous à la section Contextes de restauration.

    Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

    pour plus d'informations.
- La restauration est disponible pour les tâches de confidentialité des données dont l'état est Terminé, Annulé ou Erreur.
- Un contexte de restauration est créé pour chaque tâche de désanonymisation sys_user réussie configurée avec une politique de confidentialité des données avec prise en charge de la restauration activée. Il ne peut y avoir qu'un seul 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 antérieur à la désidentification d'une classe de données ou d'une tâche utilisateur.

Avant de commencer

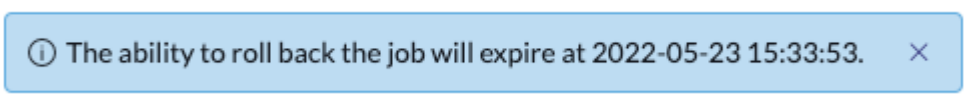
Rôle requis : data_privacy_admin ou data_privacy_processor et admin

Procédure

1. Élevez-vous au **rôle data_privacy_processor** ou **data_privacy_admin** .
   Pour plus d'informations sur l'élévation des rôles, consultez Élever à un rôle privilégié.
2. Accédez à la **Tous** > **Sécurité de système** > **Confidentialité des données** > **Tâche 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 informant du délai d'expiration. Au cours de la période d'expiration, vous avez la possibilité d'annuler 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 Data Privacy

Lorsque les données client sont clonées d'une source vers une instance cible, généralement de la production vers la non-production, les données sensibles sont anonymisées sur l'instance cible.

Un administrateur de confidentialité des données configure les politiques post-clonage. 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 de Data Privacy peuvent configurer des politiques de désidentification à appliquer à l'instance cible lors du clonage afin de s'assurer que l'instance cible ne contiendra pas de données sensibles d'origine. Un ordre est spécifié pour la politique à exécuter par rapport aux autres politiques.

Remarque :
Le clonage Data Privacy est disponible sur les instances auto-hébergées.

Le clone Data Privacy possède les attributs supplémentaires suivants :

- Le module d'extension de confidentialité des données crée le script post-clone à exécuter sur l'instance cible.
- Les tâches de confidentialité des données créées pour la configuration de 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 plus élevé peut commencer avant une autre tâche d'ordre inférieur, si la tâche d'ordre supérieur n'implique aucune table liée à une autre tâche d'ordre inférieur.
- Avec le module d'extension de confidentialité des données, les tables de confidentialité des données se trouvent par défaut dans l'ensemble de tables Conservateurs de données de clone.
- Une tentative d'ajout d'une table de confidentialité des données (dp_[table]) aux tables d'exclusion de clones recevra un avertissement, cette table ne doit pas être exclue.

Configurer la demande de clone de confidentialité des données

L'intégration du 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. Après avoir exécuté le script, 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 (com.glide.data_privacy) sur l'instance source.
   Le module d'extension ne peut être installé que par Service et assistance client.
   Le script PostClone de confidentialité des données est installé.
2. Élevez-vous au **rôle data_privacy_admin** .
   Pour plus d'informations sur l'élévation des rôles, 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 Data Privacy s'exécute sur l'instance cible et le script PostClone crée un enregistrement de tâche fédérée Data Privacy sur l'instance cible. La tâche fédérée crée et exécute une tâche de confidentialité des données pour chaque politique post-clone, dans l'ordre d'application, sur l'instance cible.La source de copie de sauvegarde est clonée dans l'instance cible. Le script PostClone Confidentialité des données crée et exécute des tâches de confidentialité des données pour les politiques configurées sur l'instance cible.

Le processeur de clone de confidentialité des données avec élévation de privilèges peut se connecter à l'instance cible et surveiller l'état de la tâche fédérée post-clonage sur les dp_federated_job.list et dp_job.list.

Confidentialité des données

L'application de stockage de confidentialité des données est une actualisation Next Experience pour la classification et la confidentialité des données avec une apparence, une convivialité et une convivialité modernes. L'application de stockage de confidentialité des données est prise en charge dans Utah et les versions ultérieures.

La confidentialité des données comprend plusieurs composants, la vue d'ensemble, la classification et l'anonymisation.

Vue d'ensemble

Utilisez la section Vue d'ensemble comme point de départ pour gérer vos données et la conformité en matière 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 en vue d'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. Classifier les données à utiliser pour l'anonymisation. Pour plus d'informations sur les classes de données et la classification, reportez-vous à Classification des données.

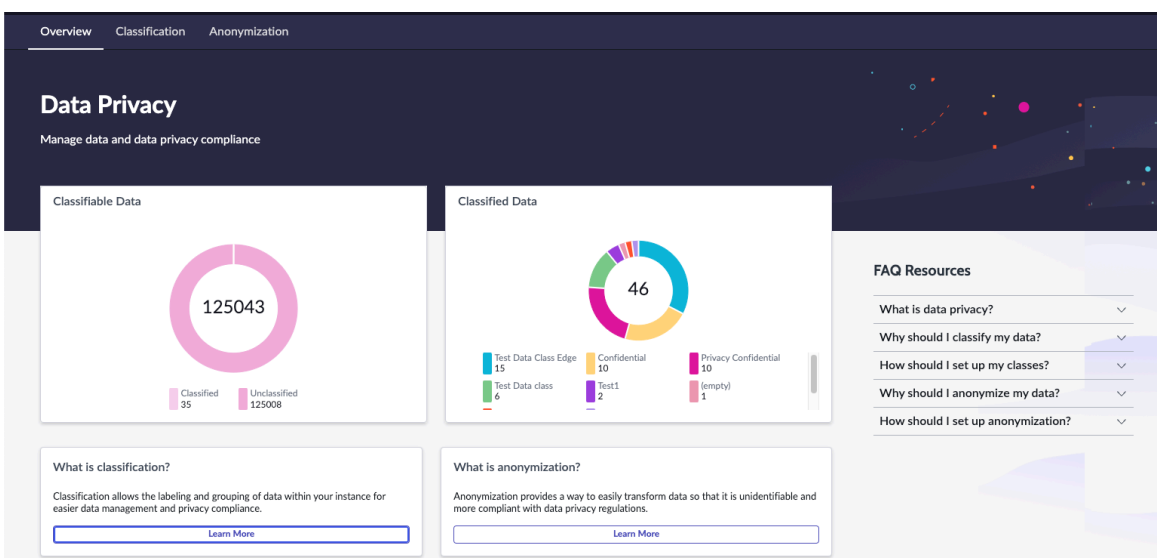
Anonymisation

Anonymisez les informations pour tous les utilisateurs ou pour un sous-ensemble d'utilisateurs et définissez les techniques. Consultez Anonymisation des données pour plus d'informations.

Vue d'ensemble de la confidentialité des données

La page d'accueil Vue d'ensemble est un point de départ pour gérer vos données et la conformité en matière de confidentialité des données.

Le tableau de bord Vue d'ensemble signale 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 classifiées, les classes de données disponibles, la quantité de données dans chaque classe et un état général des tâches d'anonymisation. Les données classées sont réparties 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.



Données classifiables

Affiche le nombre total d'enregistrements de données pouvant être classés dans l'instance. Ce nombre est réparti entre le nombre total de données classifiées et le nombre total de données non classifiées. Cela donne aux administrateurs une vue d'ensemble des possibilités de classification potentielles.

Traduction automatique

Données classifiées

Affiche le nombre total d'enregistrements de données classifiés dans l'instance. Ce nombre est réparti en nombre total de données classifiées pour chaque classe de données affectée. Cela permet de comprendre rapidement la quantité de données qui ont été classifiées dans chaque domaine.

Tâches d'anonymisation

Affiche les tâches de confidentialité des données 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 démarrer le processus.

Ressources de la FAQ

Accédez aux ressources d'apprentissage sur la classification ou l'anonymisation des produits pour obtenir des informations supplémentaires sur la façon de commencer à sécuriser votre instance avec la confidentialité des données.

Activer Confidentialité des données

Data Privacy, qui comprend la classification et l'anonymisation des données, est installé à partir du ServiceNow Store.

Avant de commencer
Pour utiliser l'anonymisation des données, la confidentialité des données (classique) doit d'abord être activée avec l'autorisation ServiceNow Vault . Consultez Activer la confidentialité des données (classique) pour plus d'informations.

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.

   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 Storenotes 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**.

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.

Data Classification Active la prise en charge de :

- Visibilité sur les types de données hébergées sur des Now Platform instances.
- Conformité aux lois sur la protection de la vie privée et respect des exigences réglementaires pour des 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 aux entrées de dictionnaire existantes dans n'importe quelle table. Consultez Data dictionary tables pour plus d'informations.

- Vous pouvez classer les données comme bon vous semble pour votre entreprise et 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 à plusieurs niveaux avec des classifications de données parentes et enfants.

Remarque :
Data Classification prend en charge la séparation de domaine et la table data_classification elle-même est séparée par processus. Consultez Séparation de domaine et Data Classification 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 donner aux individus le contrôle de 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 à caractère personnel (PII) lorsque cela est nécessaire pour suivre les données soumises à la réglementation des lois locales sur la Now Platformprotection de la vie privée.

Vous pouvez appliquer une classification de données restreintes aux colonnes de la table Employé qui stockent des informations sensibles sur les employés, telles que les numéros de sécurité sociale (SSN). Les administrateurs et les auditeurs peuvent ensuite utiliser le tableau de bord Vue d'ensemble pour confirmer que vous avez affecté des classifications de données aux colonnes correctes. Ils peuvent également afficher les détails de classification pour les types d'informations restreints.

Créer des classifications de données

Créez vos propres classifications de données définies par l'utilisateur dans la table [data_classification] que vous pourrez ensuite affecter à des colonnes spécifiques dans des tables spécifiques. Créez de nouvelles classes de données pour démarrer le processus de classification.

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 spécifiques dans la table Dictionnaire [sys_dictionary]. Lorsque vous affectez des classifications de données, il crée des entrées dans la table Dictionnaire-Classe de données [m2m_dictionary_dataclass], que vous pouvez ensuite examiner 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'une table particulière.
4. Sélectionnez **Classifier les données**.
   Les données sont classées sous le nom de classification dans la table Données classifiées.
5. Affichez ou exportez les données au format Excel, CSV, JSON ou PDF.
   Choisissez de télécharger les données au format choisi ou de les recevoir par e-mail.

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. Data Privacy peut être utilisée dans les instances de production pour anonymiser des 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 Data Privacy pour créer et afficher des politiques et des techniques de confidentialité et effectuer une affectation en bloc de la confidentialité. Affichez toutes les tâches, avec la description, la politique de confidentialité utilisée et l'état. Pour accéder à la section d'anonymisation, un administrateur doit d'abord s'élever aux rôles data_privacy_admin et data_privacy_processor.

Techniques d'anonymisation

Les techniques d'anonymisation sont des options que vous sélectionnez pour déterminer comment vos données sont anonymisées. Vous devez créer une technique d'anonymisation à référencer dans la tâche d'anonymisation. Reportez-vous à la rubrique 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. Voir pour Créer des politiques d'anonymisation plus de détails.

Tâches d'anonymisation

Les tâches d'anonymisation utilisent tous ces composants pour anonymiser vos données. Pour en savoir plus sur ces tâches, reportez-vous à Créer une tâche d'anonymisation.

Créer des techniques d'anonymisation

Créez une configuration technique de confidentialité des données pour personnaliser la façon dont confidentialité des données anonymise vos données.

Avant de commencer
Rôle requis : data_privacy_admin et admin

Procédure

1. Élevez-vous au **rôle data_privacy_admin** .
   Pour plus d'informations sur l'élévation des rôles, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Anonymisation**.
3. Sélectionnez **Afficher les techniques**.
   Il existe plusieurs techniques prédéfinies 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. Si ce champ 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 par le 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, astérisques (*) est utilisé 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 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.
Remplacement aléatoire	Cette technique échange les valeurs avec des valeurs générées de manière aléatoire. Les données chaîne et numéro peuvent utiliser cette technique.

Technique	Description
Supprimer	Cette technique supprime les valeurs et les remplace par des valeurs vides (nulles).
Aucune action	Cette technique est un espace réservé. Cette option 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 modèles de données dans Explorer Détection de données.
Anonymisation du modèle de données	Rend anonyme uniquement les modèles de données détectés dans des champs de données non structurés tout en conservant le contexte sous-jacent intact. **Remarque :** Les paramètres de cette technique d'anonymisation du modèle de données de référence sont définis dans Explorer Détection de données.

4. Sélectionnez **Ajouter une technique personnalisée**, si vous n'utilisez pas une technique prédéfinie.
5. Renseignez les champs du formulaire **Personnaliser la technique** .

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 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. Si ce champ est laissé vide, le masquage se termine par le dernier caractère.	(Vide)

Technique de base	Valeur du paramètre Technique de confidentialité	Description	Valeur par défaut
Remplacement sélectif	exclude_char	Caractère pour ignorer le masquage. Un seul caractère peut être utilisé dans cette valeur. Si plus d'un caractère est saisi, 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
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 true** pour préserver la longueur des données. Les données anonymisées 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

Reportez-vous à la rubrique 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

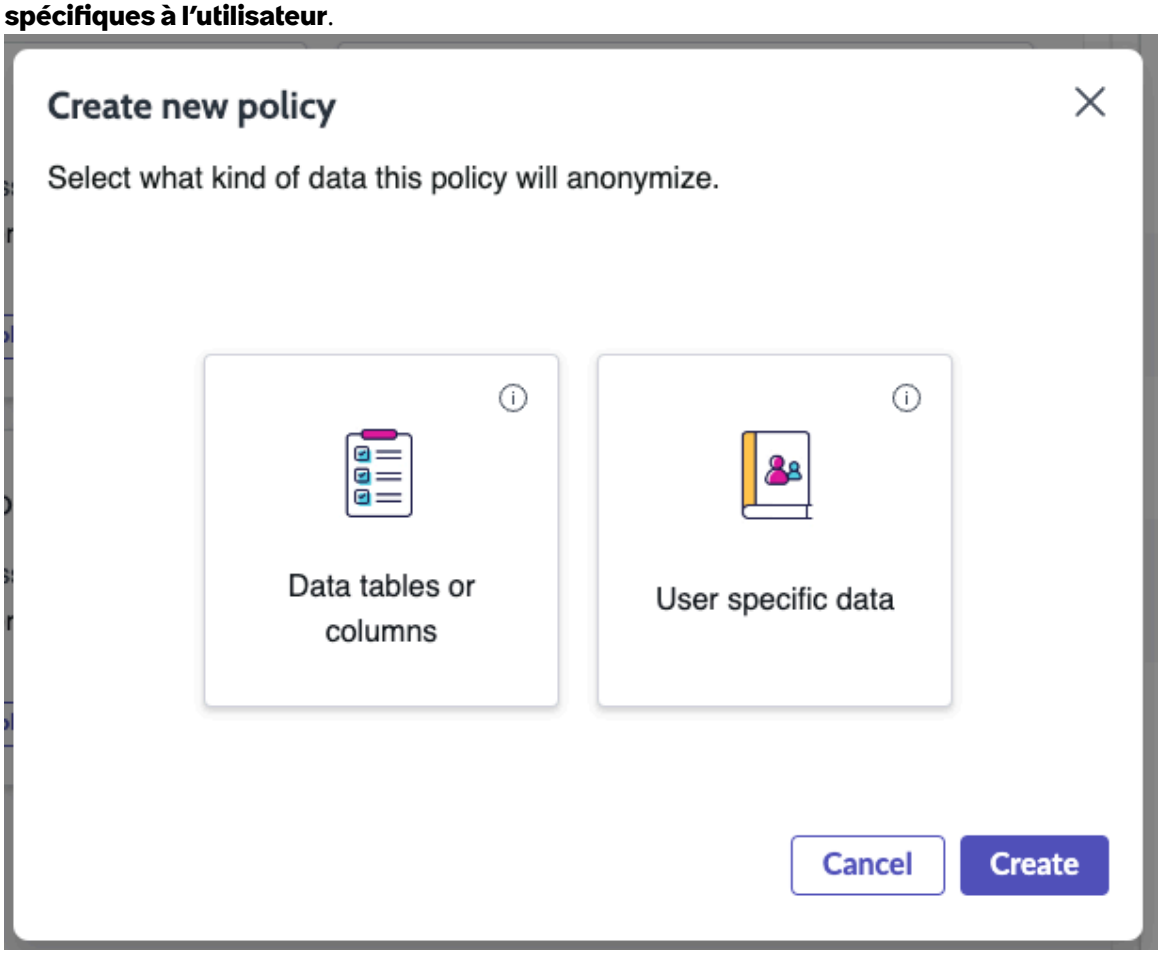
La configuration de confidentialité des données définit les tables, sys_user et autres, ainsi que les colonnes à anonymiser, en fonction du cas d'utilisation et spécifie les types paramétrés des techniques à utiliser lors de l'anonymisation des données.

Remarque :
Pour effectuer une configuration de confidentialité, vous devez d'abord configurer une technique de confidentialité des données. Consultez pour en savoir plus.

Rôle requis : data_privacy_admin et admin

Procédure

1. Élevez-vous au **rôle data_privacy_admin** .
   Pour plus d'informations sur l'élévation des rôles, 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 **les tables ou colonnes de données ou lesdonnées spécifiques à l'utilisateur**.



   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.

5. Sélectionnez **Créer**.

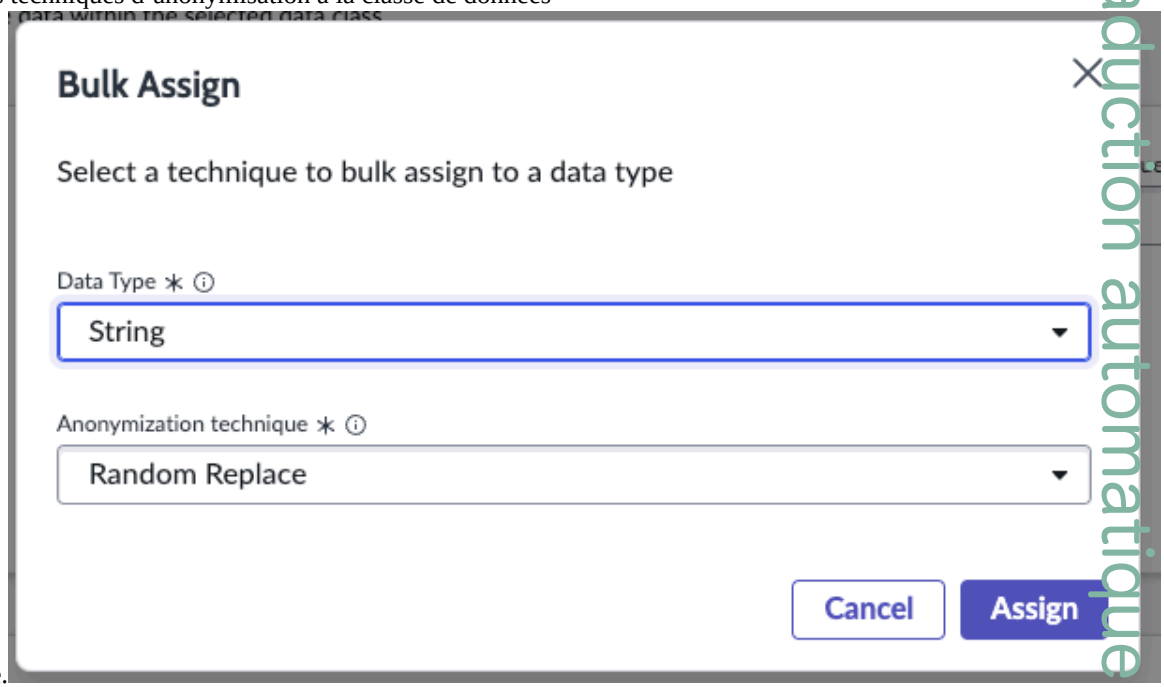
Des étapes séquentielles sont requises pour compléter la politique, **définir les détails**et **affecter des techniques**. **La sélection de la référence utilisateur** est également requise lors de la définition de la politique pour les données spécifiques à l'utilisateur.

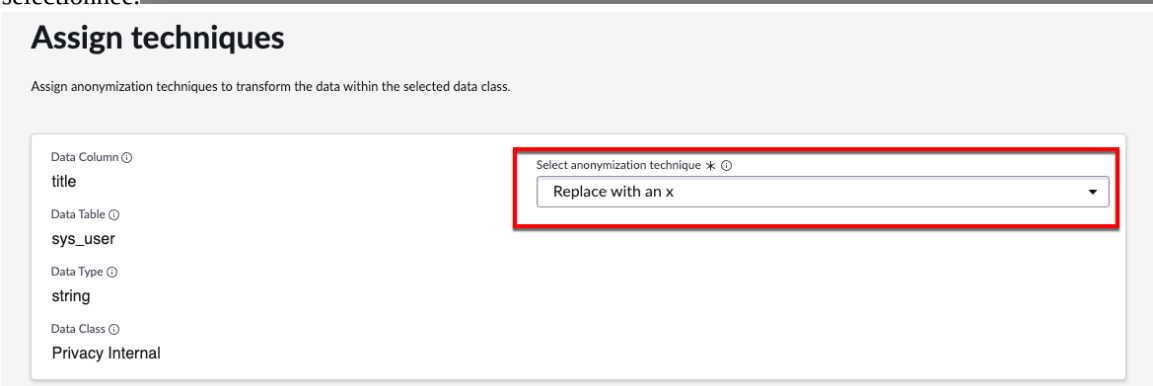
6. Définissez les détails de la nouvelle politique d'anonymisation.
   - Entrez le nom de la politique dans le champ **Nom** et la description de la politique dans le champ **Description** .
   - Dans le champ **Classe de données** , sélectionnez la classe de données à utiliser avec cette stratégie.

   Remarque :
   Si vous n'anonymisez pas une entrée, sélectionnez la technique **Ne rien** faire plutôt que de laisser l'entrée vide. Impossible d'exécuter les politiques avec des valeurs vides dans le champ Configuration de la technique de confidentialité lorsqu'elles sont utilisées dans des tâches de confidentialité des données.

Après avoir sélectionné une classe de données, 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 :** Si l'anonymisation du modèle de données est sélectionnée, sélectionnez la technique d'anonymisation à utiliser.

9. **Facultatif :** Définissez le classement des modèles de données.
10. **Facultatif :** Sélectionnez le bouton **Test** pour tester la stratégie.
11. Sélectionnez **Enregistrer**.
12. Sélectionnez **Publier** pour mettre à jour la politique d'anonymisation pour la planification et être renvoyé 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 du 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. Après avoir exécuté le script, les utilisateurs verront les données anonymisées et n'auront pas accès aux données d'origine.

Avant de commencer

Le script de confidentialité des données PostClone est installé avec l'activation du module d'extension de confidentialité des données (com.glide.data_privacy). Consultez Activer 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 (com.glide.data_privacy) sur l'instance source.
   Le script PostClone de confidentialité des données est installé.
2. Élevez-vous au **rôle data_privacy_admin** .
   Pour plus d'informations sur l'élévation des rôles, 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 **Tables ou colonnes de données**.
6. Sélectionnez **Créer**.
7. Saisissez un nom et sélectionnez une classe de données.
8. Sélectionnez cette option pour **activer la stratégie pendant le clonage**.
9. Sélectionnez l'ordre de la politique à exécuter s'il existe plusieurs politiques de clonage.
   Une tâche de confidentialité des données pour la configuration Postclone avec un ordre d'application plus élevé peut commencer avant une autre tâche d'ordre inférieur, si la tâche d'ordre supérieur n'implique aucune table liée à une autre tâche d'ordre inférieur.
10. Sélectionnez **Continuer**.
11. Terminez la configuration de la politique et publiez la politique.
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 Data Privacy s'exécute sur l'instance cible et le script PostClone crée un enregistrement de tâche fédérée Data Privacy sur l'instance cible. La tâche fédérée crée et exécute une tâche de confidentialité des données pour chaque politique post-clone, dans l'ordre d'application, sur l'instance cible.La source de copie de sauvegarde est clonée dans l'instance cible. Le script PostClone Confidentialité des données crée et exécute des tâches de confidentialité des données pour les politiques configurées sur l'instance cible.

Le processeur de clone de confidentialité des données avec élévation de privilèges peut se connecter à l'instance cible et surveiller l'état de la tâche fédérée post-clonage sur les 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 afin d'utiliser des données anonymisées 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 d'anonymisation :

- 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 d'informations sur l'élévation des rôles, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Anonymisation**.
3. Dans une politique d'anonymisation, sélectionnez **Tâche** planifiée pour la politique à utiliser 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.

Champs de tâche Confidentialité des données

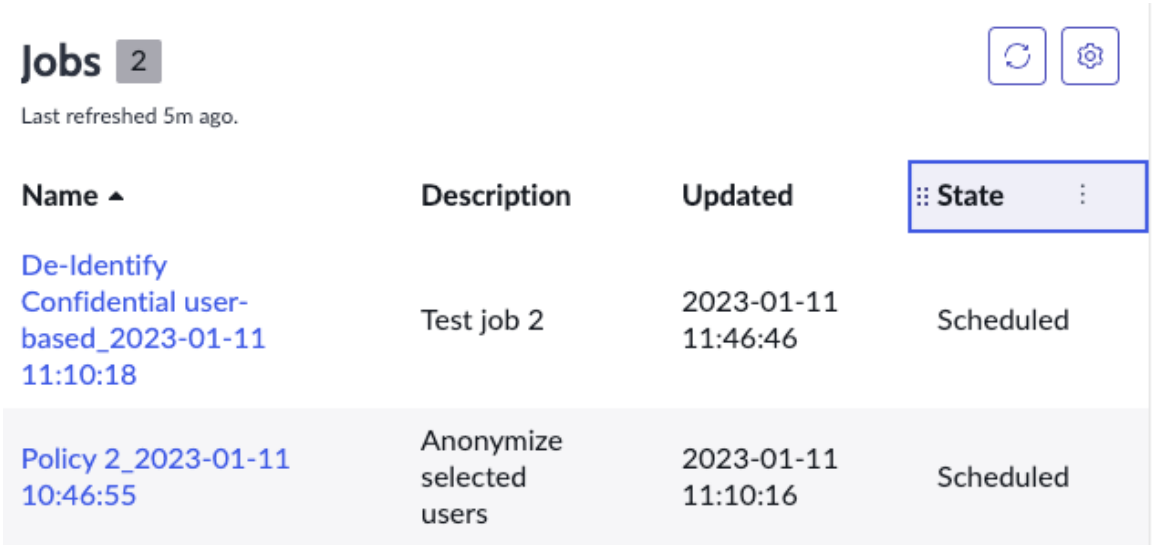
Champ	Description
Politique utilisée	Nom en lecture seule de la configuration de politique de confidentialité sélectionnée à utiliser pour cette tâche. Modifiez la politique pour afficher des informations supplémentaires sur la politique. Pour en savoir plus sur les configurations de la politique de confidentialité, reportez-

Champ	Description
	vous à la section Créer des politiques d'anonymisation.
Description de poste	Description de la tâche.
Heure de début	Début de la période d'exécution de cette tâche dans **HH :MM :SS.**
Heure de fin	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 prochain début de la fenêtre horaire.
Essai	Exécutez la tâche en tant que test. Aucun enregistrement n'est affecté lors de l'exécution de cette tâche. Les résultats sont affichés dans la liste **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 Restaurer une tâche de confidentialité des données pour en savoir plus.
Sélectionner des utilisateurs	Sélectionnez dix utilisateurs au maximum à anonymiser dans cette tâche. **Remarque :** Ce champ obligatoire s'affiche uniquement lorsque la condition de politique de confidentialité sélectionnée nécessite une sélection d'enregistrements utilisateur.

5. Sélectionnez **Planifier la tâche** sur le formulaire pour placer l'anonymisation dans la file d'attente des tâches.
   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, elle se poursuivra au début de la fenêtre horaire 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 une tâche basée sur la même politique, sélectionnez **Planifier la tâche** et remplissez le formulaire en utilisant les mêmes valeurs de champ.

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 pour les nouvelles **tâches**. ○ **Terminé** : la tâche a anonymisé avec succès les données sélectionnées. ○ **Annulée** : la tâche a été annulée manuellement. ○ **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 de configuration si l'erreur persiste. ○ **Restauration en cours** : la tâche a été définie pour restaurer l'anonymisation. ○ **Restauration terminée** : la restauration de la tâche d'anonymisation s'est terminée avec succès. Un 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 **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 affectés par cette exécution d'essai avant son exécution. Un champ en lecture seule

Champ	Description
Nombre total d'enregistrements de données traités	Nombre total d'enregistrements de données individuels affectés par cette tâche. Un champ en lecture seule.
Nombre total de tables de données traitées	Nombre total de tables de données traitées par cette tâche. Un champ en lecture seule.
Temps restant pour la restauration	Le temps restant pendant lequel une tâche d'anonymisation des données terminée peut être restaurée et désanonymiser les données. Un champ en lecture seule.
Nombre total d'utilisateurs traités	Le nombre total d'enregistrements d'utilisateurs individuels affectés par cette tâche. Un 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 passe à *Annulé*.
Mise 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'affiche 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 *En pause*.
Reprendre	Redémarre une tâche en pause. La restauration n'est pas prise en charge pour les tâches reprises si elle est mise en pause. Annulez la tâche et créez une tâche de confidentialité des données. L'enregistrement utilise un contexte de restauration non expiré. Lorsque cette option est sélectionnée, l'état de la tâche passe à *Planifié*.
Exporter	Télécharge un fichier .PDF contenant les détails de la tâche de confidentialité des données.

Restauration des tâches de confidentialité des données

Les modifications apportées à la base de données sont capturées pour des actions telles que des tâches et des scripts afin que les modifications puissent être annulées. 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 un 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 . Reportez-vous à la section Contextes de restauration.

  Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à Add a system property .

  pour plus d'informations.

- La restauration est disponible pour les tâches de confidentialité des données dont l'état est Terminé, Annulé ou Erreur.
- Un contexte de restauration est créé pour chaque tâche de désanonymisation sys_user réussie configurée avec une politique de confidentialité des données avec prise en charge de la restauration activée. Il ne peut y avoir qu'un seul 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 antérieur à 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 admin

Procédure

1. Élevez-vous au **rôle data_privacy_processor** ou **data_privacy_admin** .
   Pour plus d'informations sur l'élévation des rôles, consultez Élever à un rôle privilégié.
2. Accédez à la **Tous** > **Sécurité de système** > **Confidentialité des données** > **Anonymisation**.

   Remarque :
   Au préalable, une configuration de politique de confidentialité des données prenant en charge la restauration doit être créée. Consultez Créer des politiques d'anonymisation pour plus d'informations.

3. Sélectionnez une tâche d'anonymisation dont l'état est **Terminé** .
   - Une fois la tâche exécutée, les données sont anonymisées pour la configuration sélectionnée.
   - Dans le résumé de la tâche, le **champ Temps restant pour la restauration** informe du délai d'expiration. Dans ce délai, vous avez la possibilité de restaurer la tâche.
4. Sélectionnez **Restaurer** pour désanonymiser les données.
   En cas de réussite, la tâche sera mise à jour sur Rollback_Complete.

API Confidentialité des données

Référence pour l'API de confidentialité des données

DataPrivacyAPI : anonymize(entrée de chaîne)

Anonymise la chaîne d'entrée en appliquant la technique d'anonymisation du modèle de données à l'aide de modèles de données actifs configurés dans le Détection de données module d'extension.

Paramètres

Nom	Type	Description
entrée	Chaîne	Entrée de chaîne d'entrée à anonymiser.

Renvoie

Type	Description
Chaîne	Chaîne JSON sérialisée. réussite Renvoie la valeur true si l'anonymisation a réussi entrée modifiée Renvoie la valeur true si la valeur anonymisée est différente de l'entrée. erreur Renvoie le code d'erreur si une erreur s'est produite sortie Si la réussite est vraie, contient une chaîne anonymisée.

Example: Exemple de code

```
var privacyApi = new SNC.DataPrivacyApi();
var input = 'SSN: 123-45-6789';
var jsonString = privacyApi.anonymize(input);  // activate necessary data patterns first in
 discovery plugin
var output = JSON.parse(jsonString);

if (output.success) {
   gs.info('anonymized string: ' + output.output);
} else {
  gs.info('anonymization failed: ' + output.error);
}
```

Configuration

Nom	Configuration Mode	Description
Taille de l'entrée DataPrivacyApi.anonymize	sys_property : data_privacy.api.input.size	Propriété système permettant de définir la taille d'entrée maximale

Configuration (suite)

Nom	Configuration Mode	Description
		prise en charge par les appels DataPrivacyApi.anonymize. , . • La valeur par défaut est 4 000 • La plage est une valeur entière comprise entre 0 et 10 000
Utilisation du cache par l'API de confidentialité des données	sys_property : data_privacy.api.use.cache	Propriété système permettant de définir si DataPrivacyApi doit mettre en cache les configurations. • La valeur par défaut est true • La plage est booléenne
Délai d'expiration de l'API d'anonymisation	DataPrivacyApi.setAnonymizeTimeoutMs(timeoutMillis)	Appel d'API pour définir le temps maximal en millisecondes pour effectuer les appels DataPrivacyAPI.anonymize. • La valeur par défaut est 20 000 (ms) • La plage est une valeur entière comprise entre 0 et 50 000 (ms)

Détection de données

Permet Détection de données d'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 détection de données

En savoir plus sur la détection de données.

Configurer la détection de données

Obtenez de l’aide sur la configuration de la détection de données.

Rôles dans la détection de données

En savoir plus sur les rôles dans la détection de données.

Résultats de détection de données

Examinez les résultats de détection de données.

Traduction automatique

Explorer Détection de données

Permet Détection de données d'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.

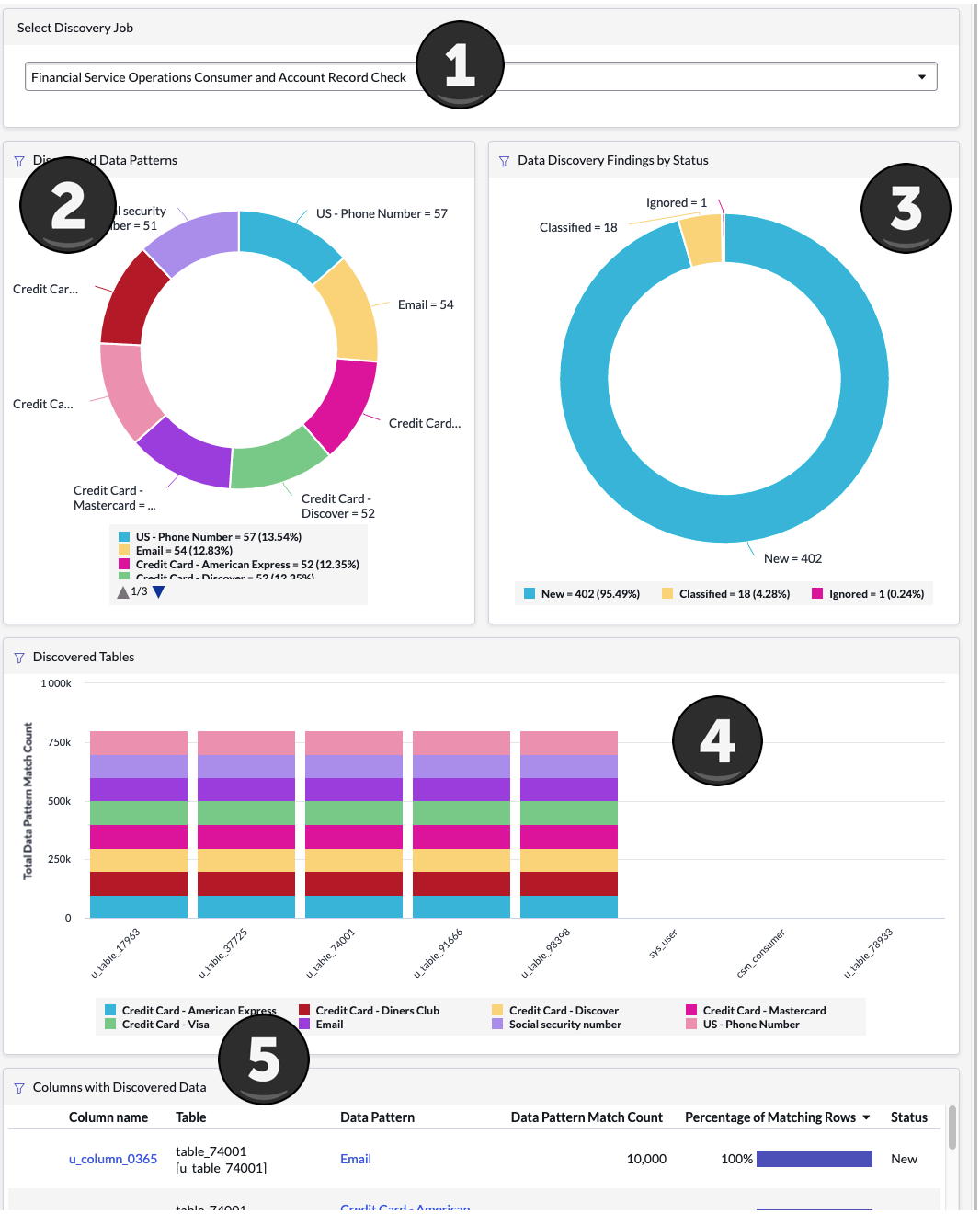
Détection de données Exécute un ensemble de tâches défini par l'utilisateur sur un ensemble de tables. Les tâches recherchent et signalent des informations sensibles en vue de leur examen sur le tableau de Détection de données bord. Une tâche planifiée utilise automatiquement tous les modèles de données actifs et les tables cibles lors de son exécution.

Détection de données inclut 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** > **Détection de données (classique)** > **Tableau de bord** pour afficher le Détection de données tableau de bord et examiner les résultats de votre tâche actuelle.

Tableau de bord de Détection de données



Détection de données Guide du tableau de bord

Numéro	Titre de la section	Détails de section
1	**Sélectionner la tâche de détection**	
2	**Modèles de données détectés**	Affiche le nombre et le pourcentage de modèles de données détectés par type
3	**Résultats de détection de données par état**	Affiche le nombre et le pourcentage de modèles de données détectés par état

Traduction automatique

Détection de données Guide du tableau de bord (suite)

Numéro	Titre de la section	Détails de section
4	**Tables détectées**	Affiche les modèles détectés par graphique
5	**Colonnes avec données détectées**	Affiche des détails sur les colonnes avec des modèles de données détectés

Activer Détection de données

L'application s'installe et les applications et modules d'extension associés Détection de donnéesServiceNow® Store , le cas échéant.

Avant de commencer

La détection de données nécessite un abonnement distinct du reste du Now Platformfichier .

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.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les éléments suivants sont installés avec la détection de données :

- Rôles
- Tables

Pour en savoir plus sur les rôles et les tables installés, reportez-vous aux sections Détection de données rôles et Modèles de données par défaut.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Trouvez le module d'extension Data Discovery (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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

Classer les données dans la Détection de données page Conclusions

Classez les données sensibles trouvées par toutes les tâches réussies par le biais Détection de données des résultats.

Avant de commencer
Rôles requis : data_discovery_admin

Une tâche doit terminer une exécution réussie pour que des données de résultat puissent apparaître comme étant classifiées.

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** > **Détection de données (classique)** > **Résultats de détection 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 modèles de données et de tables cibles définis par l'utilisateur.

Détection de données fonctionne en planifiant d'abord une tâche dans la section **Tâche de détection de données** . Lorsqu'une tâche planifiée s'exécute, tous les modèles de données actifs sont recherchés sur les tables cibles actuelles. Pour en savoir plus sur la création et la configuration d'une Détection de données tâche, reportez-vous à Configurer une Détection de données tâche.

Remarque :
Jusqu'à 10 000 enregistrements sont analysés par table et par modèle.

Détection de données Modèles de données

La section **Modèles de données** affiche tous les modèles 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 et la

configuration des modèles de données, reportez-vous à Configurer Détection de données des modèles.

Remarque :
La section **Modèles de données actifs** affiche uniquement les modèles actifs. Les modèles inactifs n'apparaissent pas.

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 (en anglais)
- v
- sh$
- syslog
- UA
- UsageAnalytics
- Ecc
- cloner
- jrobin
- Pa
- sla_repair_log
- numériser
- 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

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** > **Détection de données (classique)** > **Tâche de détection de données**.
2. Dans la Détection de données liste Tâches, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire Champs de tâche Détection de données .

Détection de données Champs de tâches

Champ	Description
Nom	Nom de la tâche.
Description	Description de la tâche.
Type d'analyse	Nombre d'entrées à scanner. Les états possibles sont les suivants : ○ **Exemple** : analyse 10 000 entrées. ○ **Complet** : analyse toutes les entrées.
Contexte	Détails de la tâche sur les modèles analysés, les entrées de tables cibles touchées et le temps écoulé.
État	État de la Détection de données tâche. Les états possibles sont les suivants : ○ **Prêt à planifier** : état par défaut pour les nouvelles tâches. ○ **Planifié** : la tâche est planifiée pour s'exécuter. ○ **En cours** : la tâche est en cours d'exécution. ○ **Terminé** : l'exécution de 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 après l'avoir exécutée.
Date de démarrage	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 Début de la

Champ	Description
	fenêtre horaire doit se situer avant l'heure saisie dans le champ Fin de la **fenêtre** horaire. **Remarque :** Une valeur de temps valide est exprimée en heure universelle coordonnée, selon une notation temporelle de 24 heures.
Fin de la fenêtre de temps	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, elle s'interrompt et reprend au début de la fenêtre horaire suivante. L'heure saisie dans le champ de fin de la **fenêtre horaire** doit être postérieure à l'heure saisie dans le champ de début de la **fenêtre horaire** . **Remarque :** Une valeur de temps valide est exprimée en heure universelle coordonnée, selon une notation temporelle de 24 heures.

4. Sélectionnez **Envoyer**.
   Les boutons **Planifier la tâche** et **Mettre à jour** s'affichent.
5. Sélectionnez **Planifier la tâche** pour exécuter votre tâche.
   La tâche s'exécute entre les heures sélectionnées dans les champs Début de la **fenêtre de temps** et Fin de la **fenêtre de temps** . Si la tâche ne s'est pas terminée pendant la fenêtre d'heures de début et de fin, elle se poursuivra au début de la fenêtre horaire suivante.
6. **Facultatif :** Choisissez l'une des fonctions suivantes :
   - **Annuler la tâche** : annule la tâche.
   - **Pause** : met la tâche en pause.
   - **Reprendre** : redémarre une tâche en pause.

Configurer Détection de données des modèles

Configurez un Détection de données modèle et examinez les modèles actuels. Un Détection de données modèle définit l'expression régulière utilisée pour mettre en correspondance des données avec une table cible.

Avant de commencer

Rôle requis : data_discovery_admin

Procédure

1. Accédez à la **Sécurité de système** > **Détection de données** > **Tous les modèles de données**.
2. Dans la Détection de données liste Modèle, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire Champs de Détection de données tâche.

Détection de données Champs de tâches

Champ	Description
Périmètre interne	Champ d'application 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 détecter le modèle de données.
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 du mot clé** **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 différencier une date de naissance d'une date d'embauche, étant donné qu'elles ont le même format MM/JJ/AA.
Proximité du mot clé (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

4. Sélectionnez **Envoyer**.
   - 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 des tâches planifiées.

5. Accédez à la **Sécurité de système** > **Détection de données** > **Modèles de données actifs**.
6. Dans la Détection de données liste Modèle actif, sélectionnez **Modifier**.
7. Sélectionnez la liste des modèles dans **Listes disponibles** , puis déplacez-la vers **Listes sélectionnées**.

Modèles de données par défaut

Passez en revue les expressions régulières de modèle de données par défaut incluses dans Détection de données. Ces modèles de données par défaut peuvent être utilisés pour filtrer les entrées de table en vue d'une classification plus poussée.

Voici les modèles par défaut disponibles pour la détection de données.

Nom	Expression régulière
Carte de crédit - Visa	\b4[0-9]{12}(?:[0-9]{3}) ?\b
Carte de crédit – American Express	\b3[47][0-9]{13}\b
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
Carte de crédit - Diners Club	\b3(?:0[0-5]|[68][0-9])[0-9]{11}\b
Carte de crédit : Discover	\b6(?:011|5[0-9]{2})[0-9]{12}\b
Numéro de sécurité sociale	\b(?! 666|000|9\d{2})\d{3}-(?! 00)\d{2}-(?! 0{4})\d{4}\b
E-mail	\b[\w !#$%&'*+/= ?'{\|} ~^-]+(?:\. [\w !#$%&'*+/= ?'{|} ~^-]+)*@(?:[a-zA-Z0-9-]+\.)+[a-zA-Z]{2,6}\b
États-Unis - Numéro de téléphone	\b\(?([0-9] {3}) \)? [-.]? ([0-9]{3}) [-.]? ([0-9]{4})\b

Configurer Détection de données la table cible

Ajoutez des tables cibles à utiliser dans les Détection de données tâches. Seules les tables cibles seront analysées pour les modèles 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 modèles actifs.

Procédure

1. Sélectionner **Sécurité de système** > **Détection de données (classique)** > **Tables cibles**.
2. Sélectionnez **Nouveau**.
3. Sélectionnez votre table cible dans le champ **Nom** de table.
4. Sélectionnez **Envoyer**.

Détection de données rôles

Vous pouvez affecter Détection de données des rôles pour limiter l'accès des utilisateurs à certains types de données.

Administrateur de détection de données [sn_data_discovery.data_discovery_admin]

Affichez, créez et modifiez des modèles de données et les tâches connexes.

- Modèles de données :
  - Créer
  - Lecture

- Mettre à jour
- Supprimer

- Modèles de données actifs :
  - Supprimer
  - Lecture
- Emplois:
  - Créer
  - Lecture
  - Mettre à jour
  - Supprimer
  - Calendrier
  - Mise en pause
  - Reprendre
  - Interrompre
- Tables cibles :
  - Créer
  - Lecture
  - Écriture

Contient des rôles

Liste des rôles contenus dans le rôle.

- data_classification_auditor
- data_classification_admin
- sn_data_discovery.data_discovery_api_processor

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Ce rôle est automatiquement affecté aux administrateurs lors de l'installation du produit.

Remarque :
Évitez d'accorder un rôle d'administrateur lorsque des rôles plus spécialisés sont disponibles.

Auditeur de détection de données [sn_data_discovery.data_discovery_auditor]

Lire des modèles de données et des tables cibles.

- Lire des modèles de données
- Lire les modèles de données actifs
- Lire Détection de données les tâches
- Lire les tables cibles

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Aucun.

Administrateur de classification des données [data_classification_admin]

Lire les modèles de données, les tâches de détection et la table de data_classification lorsqu'un résultat de modèle spécifique activé est classifié.

Contient des rôles

Le rôle 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.

Considérations particulières

Remarque :
Pour plus d'informations sur le rôle administrateur Classification des données, consultez Installation des données de démonstration du module d'extension Data Classification.

Détection de données Résultats des tâches

La Détection de données page Résultats affiche des détails sur les données trouvées par une tâche. Vous pouvez utiliser la page Résultats pour examiner les résultats d'une tâche et commencer à classer les 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 se trouvaient les données

Colonne	Description
Table	Table cible où les données ont été trouvées
Modèle de données	Modèle de données utilisé pour rechercher 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 numérisées pendant la tâche
Pourcentage de lignes correspondantes	Pourcentage de lignes de 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 avoir exécuté une Détection de données tâche, les résultats sont à l'état Nouveau. Si aucune action n'est nécessaire, vous pouvez ne pas toucher aux données, 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 préparer l'anonymisation des données à l'aide de l'outil Data Classification .

Consolider les résultats

Les résultats de la tâche peuvent être consolidés à l'aide du bouton **Consolider les résultats** . Les résultats de la tâche partagée entre deux tâches distinctes seront alors consolidés sous la tâche la plus récemment exécutée.

Remarque :
Seules les tâches d'analyse complète terminées peuvent être consolidées

Classer les données dans la page des résultats de tâches 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 pour que des données de résultat puissent apparaître comme étant classifiées.

Procédure

1. Accéder à **Sécurité de système** > **Détection de données** > **Tâche de détection 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**.

API de détection de données

Référence pour l'API de détection de données

DataPatternValidator : matchs(modèle de chaîne, entrée de chaîne)

Valide si l'entrée correspond au modèle regex (expression régulière).

Paramètres

Nom	Type	Description
modèle	Chaîne	Le modèle regex
entrée	Chaîne	Données d'entrée à mettre en correspondance

Renvoie

Type	Description
Booléen	Renvoie la valeur true si l'entrée correspond au modèle, sinon valeur false.

Example: Exemple de code

```
var datapatternValidatorApi = new sn_data_discovery_api.DataPatternValidator();
var pattern = '\\b[0-3]?[0-9]/[0-3]?[0-9]/(?:[0-9]{2})?[0-9]{2}\\b';
var input = '09/09/2023';
var output = datapatternValidatorApi.matches(pattern, input);
if (output) {
  gs.info('pattern found!');
} else {
  gs.info('pattern not found');
}
```

DataPatternValidator : isValid(modèle de chaîne)

Valide si le modèle donné est une expression régulière valide.

Paramètres

Nom	Type	Description
modèle	Chaîne	Le modèle regex

Renvoie

Type	Description
Booléen	Renvoie la valeur true si l'expression est une expression régulière valide, sinon false.

Example: Exemple de code

```
var datapatternValidatorApi = new sn_data_discovery_api.DataPatternValidator();
var pattern = '\\b[0-3]?[0-9]/[0-3]?[0-9]/(?:[0-9]{2})?[0-9]{2}\\b';
var output = datapatternValidatorApi.isValid(pattern);
if (output) {
 gs.info('pattern is valid!');
} else {
```

```
  gs.info('pattern is not valid');
}
```

DataPatternValidator – keywordMatches(String pattern, String input, String keywords, int keywordProximity)

Validez si les données d'entrée indiquées correspondent au modèle d'expression régulière (regex) ainsi qu'aux mots clés. Consultez Configurer Détection de données des modèles pour plus d'informations sur les mots clés et la proximité des mots clés.

Paramètres

Nom	Type	Description
modèle	Chaîne	Le modèle regex
entrée	Chaîne	Données d'entrée à mettre en correspondance
Mots clés	Chaîne	Valeurs de mots clés séparées par des virgules à faire correspondre
mot-cléProximité	int	Proximité des mots clés du modèle correspondant

Renvoie

Type	Description
Booléen	Renvoie la valeur true si l'expression est une expression régulière valide, sinon valeur false

Example: Exemple de code

```
var datapatternValidatorApi = new sn_data_discovery_api.DataPatternValidator();
var pattern = '\\b[0-3]?[0-9]/[0-3]?[0-9]/(?:[0-9]{2})?[0-9]{2}\\b';
var keywords = 'dob,date of birth';
var keywordProximity = 20;
var matchInput = 'dob: 09/09/2023';
var noMatchInput = '09/09/2023';
var output = datapatternValidatorApi.keywordMatches(pattern, matchInput, keywords,
 keywordProximity);
gs.info('match found for input: ' + matchInput + ' = ' + output);
output = datapatternValidatorApi.keywordMatches(pattern, noMatchInput, keywords,
 keywordProximity);
gs.info('match found for noMatchInput: ' + noMatchInput + ' = ' + output);
```

DataPatternScanner : scan (entrée de chaîne)

Remarque :
Un tableau d'ID système de modèle de données doit être transmis au constructeur DataPatternScanner.

Paramètres

Nom	Type	Description
entrée	Chaîne	Données d'entrée à analyser

Renvoie

Type	Description
Chaîne	Chaîne JSON sérialisée hasMatches (en anglais seulement) Renvoyez la valeur vrai si au moins 1 correspondance de modèle est présente. « finding » : [{ # pour chaque modèle avec correspondance, contient la liste des positions de début et de fin des correspondances. erreur Contient un code d'erreur et un message en cas d'échec de l'API, sinon vide. unprocessedPatterns Renvoie un tableau des ID système de modèle de données qui n'ont pas été traités Trouver Renvoie l'ID de chaque modèle ainsi qu'une liste des positions de début et de fin des correspondances.

Example: Exemple de code

```
var emailSysId = '8e5605bceb0561107977d256385228e6';
var ssnSysId = '4964417ceb0561107977d256385228b8';
var dataPatternSysIds = [emailSysId, ssnSysId] // Email and SSN
var dataDiscoveryApi = new sn_data_discovery_api.DataDiscoveryScanner(dataPatternSysIds);

var input = 'my ssn is 123-45-6789 and email is abcd@company.com'
var jsonString = dataDiscoveryApi.scan(input);
var output = JSON.parse(jsonString);

if (output.hasMatches) {
  gs.info('found matches for patterns in input');
  for (var i=0; i<output.finding.length; i++) {
      curFinding = output.finding[i];
      gs.info('first match for ' + curFinding.pattern + ' is (' + curFinding.matches[0]['start'] + ','
 + + curFinding.matches[0]['end'] + ')');
  }
}
```

Configuration

Nom	Configuration Mode	Description
Longueur maximale de la chaîne de mots clés (csv).	Ne peut pas être configuré	Définit la longueur maximale de chaîne qui peut être configurée dans le champ DataPattern.keyword • La valeur par défaut est 128 • La valeur maximale est 128.
Valeur minimale et maximale pour la proximité des mots clés	Ne peut pas être configuré	Définit les valeurs minimale et maximale qui peuvent être saisies dans DataPattern.keyword_proximity champ. • Minimum de 0 • Maximum de 64
Taille maximale de l'entrée pour les correspondances et l'API keywordMatches	Ne peut pas être configuré	Définit la taille d'entrée maximale prise en charge par les API DataPatternValidator.matches et DataPatternValidator.keywordMatches • La valeur par défaut est 2048 • La valeur maximale est 2 048.
Délai d'expiration de l'API d'analyse	DataDiscoveryScanner.setScanTimeout(long timeoutMillis)	Appel l'API pour définir le temps maximal, en millisecondes, pour terminer les appels DataDiscoveryScanner.scan. • La valeur par défaut est 20 000 (ms) • La plage est une valeur entière comprise entre 0 et 50 000 (ms)

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.

servicenow

Explorer

En savoir plus sur Domain Separation.

Configurer

Configurez Domain Separation.

Référence

Obtenez des détails sur Domain Separation.

Analyser

En savoir plus sur la façon d'analyser Domain Separation

Traduction automatique

Exploration de Domain Separation

Domain separation vous permet de séparer les données, les processus et les tâches administratives en domaines définis logiquement.

Domain Separation est idéal pour les clients qui :

- Nécessité d'appliquer une séparation absolue des données entre les entités business (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.
- présentent des différences de processus mineures ou modérées entre les clients.

Domain Separation par rapport 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 que le système *Mémoriser mon* nom figure 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, la meilleure approche à adopter est l'utilisation d'instances distinctes.

Séparation des données

Les membres d'un domaine ne voient que les données contenues dans leur domaine ou les domaines enfants qui sont inférieurs dans la hiérarchie de 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 sont autorisés à voir. Les locataires peuvent avoir accès à d'autres données de locataire, mais ne peuvent pas interroger les données des locataires s'ils n'y ont pas accès.

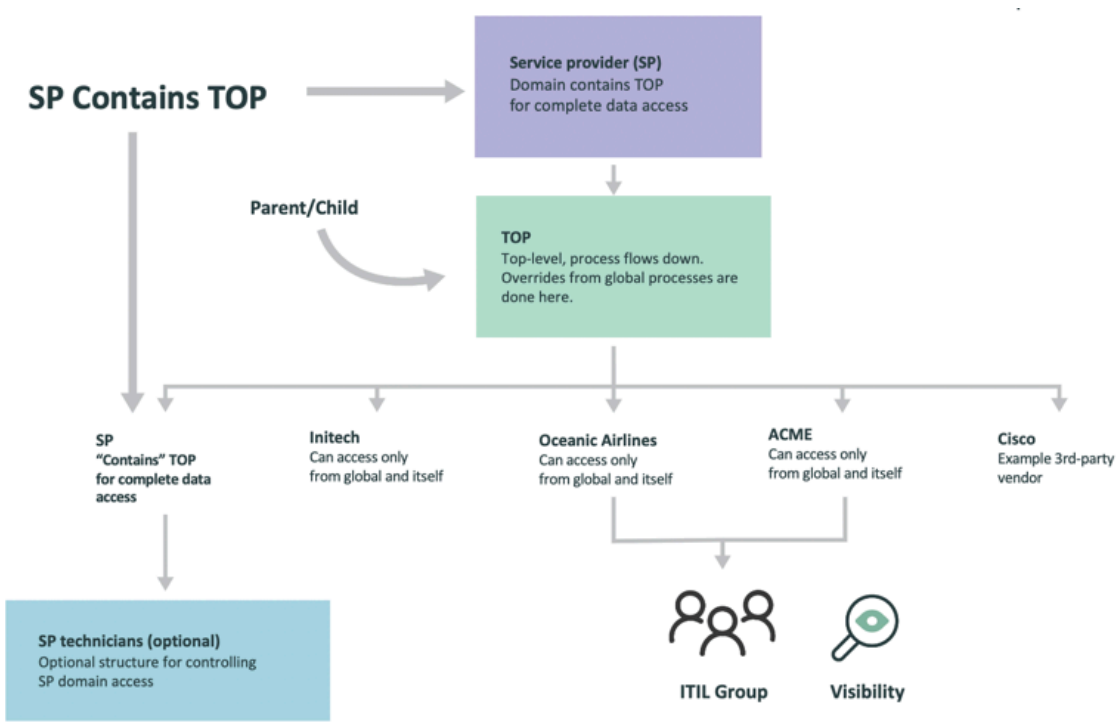
Séparation de l'interface utilisateur : prend en charge une expérience spécifique au locataire pour les éléments d'interface utilisateur tels que les vues, les listes, les étiquettes, etc.

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.

Modélisation hiérarchique : mutualisation 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.

Inter-tenant Intelligence (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 de la hiérarchie des domaines ne sont pas visibles aux niveaux inférieurs de la hiérarchie.

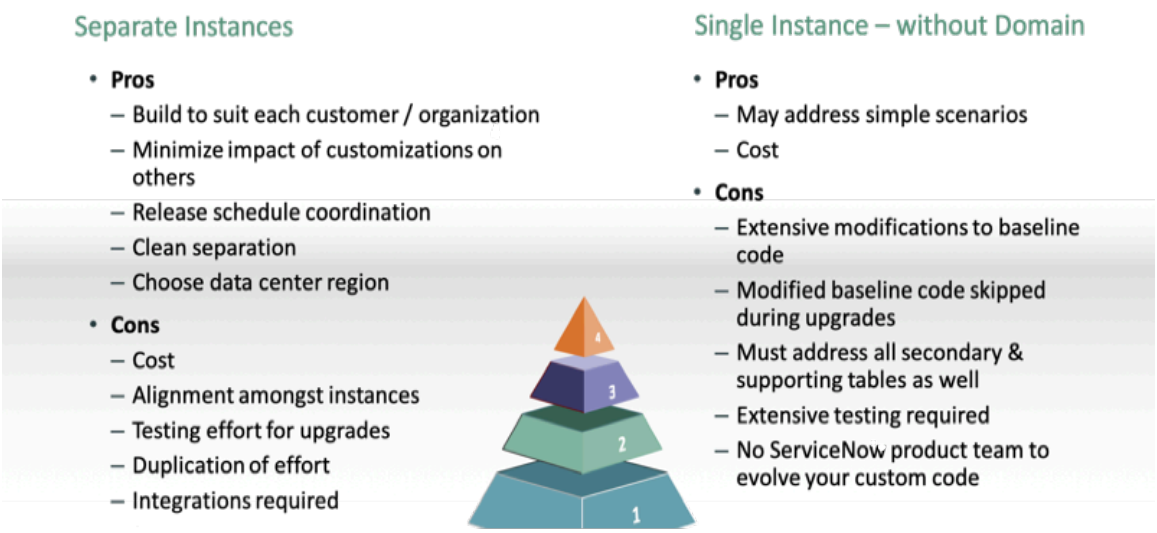


Migration du chemin de domaine

Les chemins de domaine sont utilisés pour tous les clients. La numérotation de domaine n'est pas utilisée. Service et assistance client peut vous aider dans la mise à niveau.

Alternatives à Domain Separation

Les instances distinctes constituent une alternative courante à Domain Separation. 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.



⚠ Avertissement :
Avant d'activer Domain Separation, consultez votre représentant pour vérifier qu'il est adapté à votre environnement. Domain Separation ajoute un niveau de charge d'administration. Bien qu'il puisse être désactivé, il ne peut pas être supprimé 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

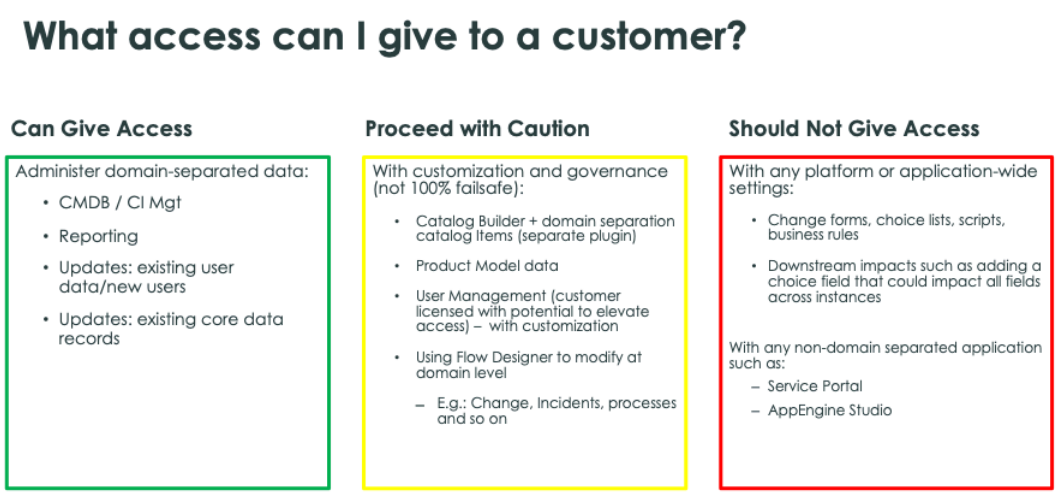
L'application Domain Separation est conçue pour permettre ServiceNow® aux fournisseurs de services de configurer les services qu'ils proposent à leurs clients. Il n'est pas conçu pour permettre à ses clients d'administrer ces services eux-mêmes, à l'exception de quelques domaines détaillés dans cette rubrique.

Vue d'ensemble

Les clients SP peuvent gérer en toute sécurité les données contenues dans leur domaine qui n'ont aucune incidence sur la gestion des licences ou d'autres clients. Par exemple, un client peut créer des rapports ou gérer des éléments de configuration en toute sécurité, mais il ne peut pas le faire en toute sécurité pour personnaliser des champs, des choix, des règles métier et d'autres processus lorsqu'ils peuvent impacter d'autres clients sur la même instance.

Les ServiceNow rôles administratifs 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 créer de nouveaux domaines. Pour toutes les tâches d'administration spécifiques au domaine, les fournisseurs de services doivent créer de nouveaux rôles « administrateur client » et des contrôles d'accès selon les besoins pour accorder un accès spécifique à ses clients.

L'image suivante est une vue d'ensemble des fonctions d'administration courantes dans diverses catégories de ce qu'un client peut faire en toute sécurité.



Autoriser l'accès

Exemples :

- Gestion des données CI dans la CMDB
- Création de rapport
- Mises à jour des données utilisateur existantes ou des nouveaux utilisateurs sans rôles
- Met à jour les enregistrements de données de base existants tels que département, groupe, emplacement, centre de coûts ou les nouveaux groupes sans rôle, ainsi que les nouveaux départements/centres de coûts/emplacements.

Procéder 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 conjointement : Domain separation pour les éléments de catalogue (Domain Separation et Service Catalog) 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 les champs fiables tels que le prix, la description et les images. Le générateur de catalogue (nouveau dans la version Quebec) donne à l'équipe d'administration du 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 : vous pouvez créer en toute sécurité un rôle « administrateur client » qui peut créer et modifier des enregistrements utilisateur, mais l'ajout et la suppression de rôles peuvent affecter la sécurité et la gestion des licences. Le système de base ne permet pas de subdiviser les rôles qu'un client peut accorder en toute sécurité. 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 des rôles doit être contrôlé.
- Flow Designer : ServiceNow Concepteur de flux outil de création utilisé pour créer un processus (workflow) pour les tables. Le rôle flow_designer donne aux clients un accès

sans script aux flux de build. Ils peuvent lire et cloner tous les flux dans les domaines situés au-dessus d'eux dans la hiérarchie. Ils peuvent créer et modifier des flux dans leur domaine. Cependant, cela ne peut pas se faire en vase clos. Toute personne susceptible d'influer sur les processus doit être ajoutée à l'équipe d'administration globale pour la gouvernance afin que les processus ne s'annulent pas les uns les autres ou n'entraînent pas d'autres conflits.

Ne pas donner accès

Il est utile de comprendre le fonctionnement des champs de choix pour comprendre pourquoi seule l'équipe d'administration du SP doit 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 la table, du domaine et de la 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 **d'État** dans toutes les tables, domaines et langues sont considérées comme les valeurs du champ **État** .

- Mode de fonctionnement des modifications apportées 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 tous les ensembles de mises à jour importés ayant une incidence sur ce champ remplaceraient les choix existants. Dans certains cas, les champs de choix peuvent entraîner eux-mêmes des processus, qui ne fonctionneraient pas si un client venait à 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
- Prise en charge de Domain Separation par les applications
- Notes de publication de Domain Separation

Affectation de domaine

Par défaut, Domain Separation ajoute un champ de domaine aux tables et à leurs extensions.

Vous pouvez également étendre Domain Separation 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 les tables de plateforme de séparation de domaine (toutes les tables avec 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 d'un 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 le crée

Le système empêche la séparation de domaine des tables suivantes :

- 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 entreprises

Les administrateurs peuvent affecter rapidement 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, reportez-vous à Pratiques recommandées de séparation de domaine pour les fournisseurs de services.

Utilisation de modules pour affecter des domaines

Les administrateurs peuvent utiliser le paramètre URL **sysparm_domain** 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** de : `sysparm_domain=sys_ID de domaine`.

Utilisation de modèles de formulaire 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, définir le champ **sys_domain** sur **domaine TOP/ACME** affecte automatiquement tous les enregistrements de ce modèle 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.

Attribution automatique de domaines en fonction des domaines d'utilisateurs

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 de contenu

Les domaines de visibilité contrôlent ce qu'un utilisateur ou un groupe d'utilisateurs spécifique peut voir. Les domaines « Contains » 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 Utilisateur [sys_user] et 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 :

- Correspond à une relation utilisateur-domaine et est 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.

Traduction automatique

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 contains pour un contrôle plus robuste.

Contient les domaines

Normalement, les relations parent-enfant définissent la hiérarchie des domaines. Un domaine contient vous permet de relier des domaines selon les besoins, indépendamment des relations parent-enfant. Toutefois, les domaines contenus n'accordent une visibilité qu'aux données de domaine. Les processus ne sont pas affectés par les relations contient.

A contient le domaine :

- Il s'agit d'une relation de domaine à domaine, plusieurs à plusieurs.
- 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.

Exemple de domaine Contains

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 homologues. Cela signifie que l'utilisateur voit les données des domaines A, B et C dans son domaine d'origine 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 C, ils ne voient que les données de ce domaine.

Exemple de domaine de visibilité

En utilisant la visibilité du domaine, si Don Goodliffe est dans le domaine Base de données et Bow Ruggeri est dans le domaine Réseau et qu'aucun incident n'est dans le domaine global, alors Don ne peut pas accéder aux incidents de Bow en raison de la séparation des données.

Hériter de domaines de visibilité en fonction de l'appartenance à un 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.

Information associée

Contient les 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 sur 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 périmètre 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 données et les contraintes 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 des données d'autres domaines. Par exemple, un utilisateur dans le domaine du 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 du 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 **Activer/désactiver le champ d'application de domaine** sur le formulaire. Lorsque le périmètre de l'enregistrement est en vigueur, cliquez sur l'action d'interface utilisateur pour étendre le périmètre de la session et afficher toutes les données disponibles en fonction du domaine de l'utilisateur et des domaines enfant. Lorsque le périmètre de la session est activé, cliquez sur l'action d'interface utilisateur pour le réduire au périmètre 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 de basculer 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.

Enregistrer la sélection de valeur à partir d'autres domaines

Les utilisateurs qui peuvent voir plusieurs domaines ont la possibilité de sélectionner des valeurs d'enregistrement à partir d'un domaine différent du domaine de l'enregistrement.

Par exemple, les agents du Service Desk travaillant pour un fournisseur de service peuvent vouloir s'affecter certains incidents pour résoudre les problèmes au nom de leurs clients. Dans ce cas, le champ **Incident affecté à** 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 à partir 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 provenant de plusieurs domaines, la visibilité du domaine de l'utilisateur détermine ce qu'il voit.

Sélection de 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, voit le nom d'utilisateur dans le champ **Affecté à** . • Affichez l'enregistrement connexe à partir de l'icône de référence. Par exemple, il affiche l'enregistrement de l'utilisateur dans le champ **Affecté à** . • Sélectionnez les valeurs dans n'importe quel domaine visible. Par exemple, peut sélectionner des utilisateurs à partir des 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 Domain separation a été activé dans Madrid ou dans 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, ne peut sélectionner que des utilisateurs du domaine ACME.

Domaines et sociétés associées

Domain Separation vous permet d'appliquer en cascade les modifications que vous apportez à un enregistrement d'entreprise, au domaine et à d'autres enregistrements associés à l'entreprise.

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 vouloir désactiver l'administration déléguée ou mettre en place un processus d'approbation pour vérifier que l'utilisateur a besoin du rôle administrateur.

Lorsque vous modifiez le domaine d'une société, l'instance modifie automatiquement le domaine des enregistrements associés suivants pour qu'il corresponde au nouveau domaine de la société.

- Emplacements
- Départements
- Groupes
- Utilisateurs

Remarque :
L'instance ne modifie pas automatiquement le domaine d'un enregistrement pour lequel vous avez coché la case **Domaine géré** .

Désactivation de domaine et sociétés associées

Lorsque vous désactivez un domaine, l'instance effectue également 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 société inactive tente de se connecter, l'utilisateur reçoit 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 exemples d'utilisateurs sont verrouillés.

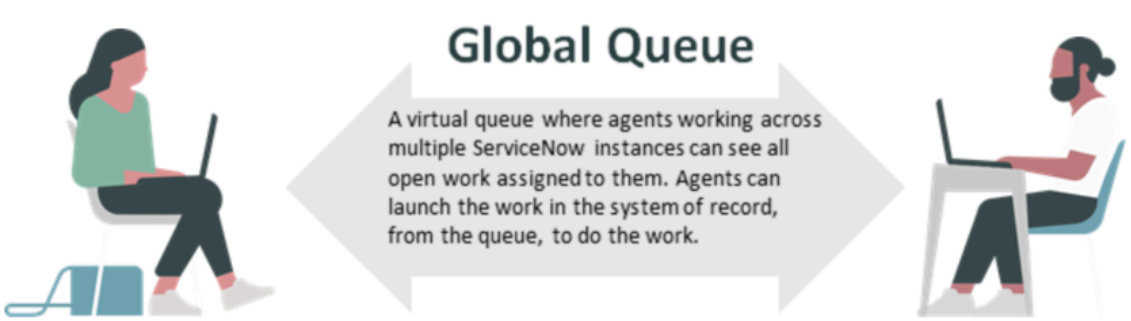
Concepts pour les prestataires de services

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 résidant dans plusieurs instances. Le concept crée une application personnalisée pour fournir une vue de prestataire du travail résidant dans plusieurs instances sans avoir à répliquer des tâches ou des données.

Vue d'ensemble



Les fournisseurs de services dont les agents travaillent sur des tâches provenant de plusieurs systèmes ont tendance à réintégrer les données dans une instance centrale, ou un « siège pivotant » entre les instances. Bien que cette méthode puisse être appropriée dans certains cas, sa création et sa maintenance peuvent être coûteuses et chronophages. Cette méthode expose également le fournisseur à d'éventuelles considérations d'audit et d'exigences en matière de données, telles que le Règlement général sur la protection des données (RGPD) dans tous les cas où les données se trouvent désormais.

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

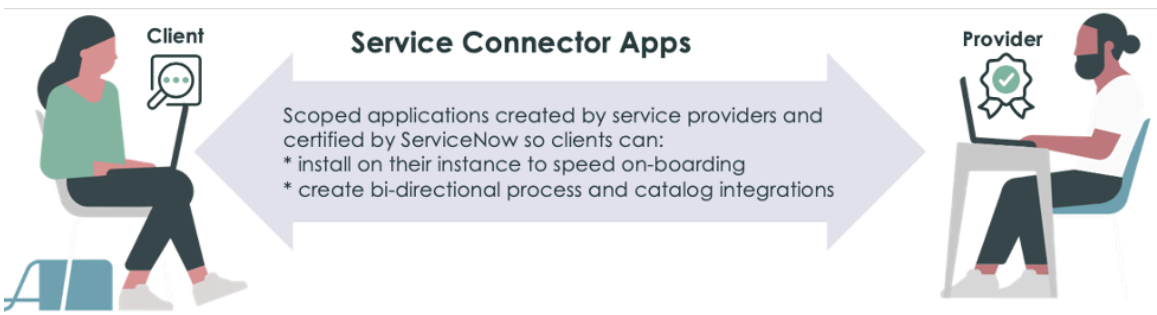
cas où les clients ont des exigences en matière de résidence des données, mais autorisent l'accès à des agents d'autres pays, le fournisseur peut utiliser un service d'assistance « follow-the-sun » à l'aide de la file d'attente mondiale v.2.

Pour en savoir plus sur la preuve de concept de la file d'attente globale v.2 , consultez le ServiceNow site Knowledge.

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 de fournisseur de service

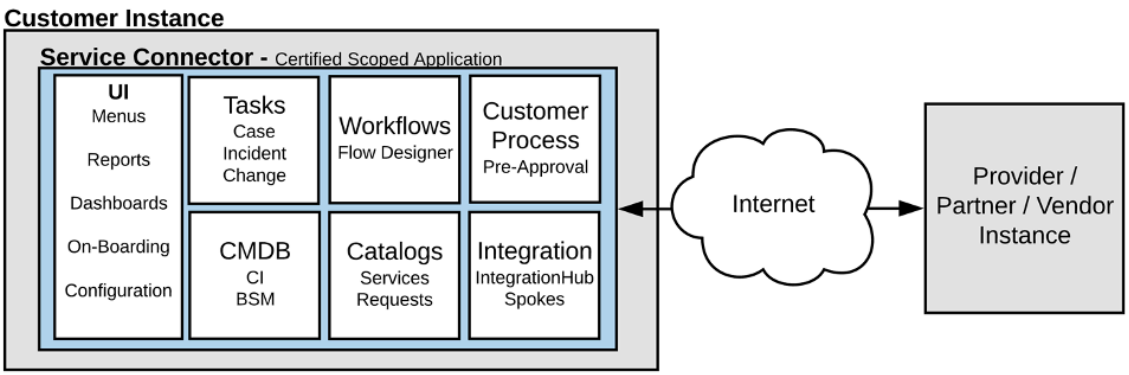
L'application Service Provider Connector est une conception de référence pour la création d'une ServiceNow application Store que vos clients peuvent utiliser pour une intégration à vos systèmes. Les applications des fournisseurs de services vous aident à accélérer l'intégration et à créer des intégrations standardisées.



Avantages des connecteurs de service

Lorsque les fournisseurs de services (vendeurs, 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, augmentent la visibilité dans l'écosystème ServiceNow et offrent les avantages du programme de partenariat. Les avantages spécifiques sont les suivants :

- Élimine les intégrations personnalisées, y compris le coût des services nécessaires pour les fournir et les gérer.
- Les services sont définis par le fournisseur au sein de leurs ServiceNow instances et éliminent la complexité et le coût des intégrations personnalisées.
- Les workflows et les demandes de catalogue peuvent être synchronisés avec les processus et 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 synchronisées dans l'instance du client afin d'en assurer la visibilité et l'utilisation dans les processus.



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 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 menu descriptif du **fournisseur 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 n'est requis pour que le client soit mis en service. (Des services professionnels sont disponibles, mais l'intégration peut être réalisée sans eux). • Configuration – Les points de données doivent être intégrés dans les processus pour tenir compte de la majeure partie de la configuration de processus normale qu'un client doit réaliser. Cela permet d'éliminer autant que possible les services professionnels. • Documentation – Une documentation complète augmente la satisfaction du client et la facilité d'utilisation.

Fonctionnalité	Description
	• Intégration de l’assistance ou informations de contact : le client a besoin d’un moyen facile de rester en contact avec le fournisseur de services pour tout problème, question ou demande.
Tâches	Utilisez l’application pour que les tâches, telles que les incidents, les Service Exchange (legacy) tickets, les changements, les problèmes, etc., doivent être prédéfinies dans le connecteur. Ces intégrations sont conçues à l’aide Concepteur de flux de et Hub d'intégration pour garantir le plus haut niveau de résilience et de performances.
CMDB	La synchronisation des données de base, telles que les CI requis pour les processus ITIL appropriés, doit être synchronisée entre les instances du fournisseur et du client.
Workflows	Tous les workflows doivent être conçus Concepteur de flux pour garantir la résilience et les performances.
Catalogues	Le catalogue du fournisseur à partir duquel le client effectue la demande doit être inclus dans l’application en tant que catalogue produisant des enregistrements. La demande générée par l’élément dans l’instance du client doit être liée aux instances du fournisseur. Les workflows du fournisseur tiennent la demande à jour et la synchronisent avec l’instance du client.
Processus client	Tous les mécanismes de synchronisation des demandes avec l’instance du fournisseur doivent permettre aux processus client 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 à l’aide Concepteur de flux de et Hub d'intégration pour garantir le plus haut niveau de résilience et de performances.

Composants possibles que vous pouvez inclure dans un connecteur de service

Composant	Description
Réplication de données d’instance (IDR)	Lorsque l’objectif est la réplication :

Composant	Description
	• Peut être utilisé pour l'intégration de processus, mais peut être trop rigide en fonction de la logique d'intégration de complexité 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 : • Plus facile à injecter au milieu d'un processus, dans le cadre d'une étape complexe ou conditionnelle au milieu d'un flux • Pour en savoir plus, consultez Centre d'intégration
File d'attente de travail globale (virtuelle)	Lorsque l'objectif est la fédération des 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 tous les travaux ouverts qui leur sont affectés • Les lignes renvoyées doivent être limitées à moins de 1 000 • Pour en savoir plus, consultez File d'attente de travail globale
Tables distantes	Lorsque l'objectif est d'utiliser des 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 regrouper, trier, regrouper et filtrer. • Pour en savoir plus, consultez Récupération de données externes à l'aide de tables et de scripts distants
Concepteur de flux	Quand l'objectif est la conception des processus • Utilisé pour automatiser les processus dans un seul environnement de conception. Les propriétaires de processus peuvent utiliser le langage naturel pour automatiser les approbations, les tâches, les notifications

Composant	Description
	et les opérations d'enregistrement sans codage. • Pour en savoir plus, consultez Flow Designer

Pour en savoir plus sur la preuve de concept de Service Connector , consultez le ServiceNow site Knowledge.

Installé avec Domain Separation

Plusieurs composants de plateforme sont ajoutés ou modifiés avec Domain Separation.

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 de 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
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 associées sont inactives.
Domaine : Cascade Company	core_company	Synchronise le domaine d'une entreprise avec ses utilisateurs, groupes, départements et emplacements.
Domaine : Cascade Domaine : 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 : Cascade Domaine : Base de connaissances	kb_knowledge	Synchronise le domaine d'un article de la base de connaissances avec ses commentaires connexes.
Domaine : Cascade Domaine : 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, ainsi que sysapproval_group et son workflow.
Domaine : Cascade Domaine : 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 : Cascade Domaine : Version	wf_workflow_version	Synchronise les domaines avec les versions de workflow connexes pour wf_activity et wf_transition.

Nom	Table	Description
Domaine : désactiver les sociétés	domain	Désactive les sociétés liées 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 le domaine sur Par défaut à la place.
Domaine : Par défaut : Utilisateur	sys_user	Définit le domaine d'un utilisateur sur Par défaut si le domaine aurait été global autrement.
Domaine : interdire l'enregistrement de domaine global	domain	Empêche la création d'un domaine avec le nom global.
Domaine - Remplacer la copie	sys_app_application	Lorsqu'une application est remplacée pour 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 ses nombres 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 incorporée est remplacé pour un domaine, crée une copie de ses scripts client et serveur pour le nouveau contrôle de liste incorporée.
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 le domaine - Approbations	sysapproval_approver	Définit le domaine en fonction de celui de l'enregistrement en cours d'approbation.
Domaine - Définir le domaine - Pièce jointe	sys_attachment	Définit le domaine en fonction du domaine de l'enregistrement parent.
Domaine - Définir le domaine - CMDB_CI	cmdb_ci	Définit le domaine d'un CI sur celui de sa société.
Domaine - Définir le	cmn_department	Définit le domaine d'un département sur celui de sa société.

Nom	Table	Description
domaine - Département		
Domaine - Définir Domaine - Domaine	domain	Définit le domaine d'un domaine à lui-même.
Domaine - Définir le 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 le domaine - Commentaire	kb_feedback	Définit le domaine d'un commentaire de la base de connaissances sur celui de son article de la base de connaissances.
Domaine - Définir le 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 de 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 sa société.
Domaine - Définir le domaine - SLA de tâche	task_sla	Définit le domaine d'un SLA de tâche sur celui de sa tâche.
Domaine - Définir le domaine - Utilisateur	sys_user	Définit le domaine d'un utilisateur sur celui de sa société.
Domaine - Définir le domaine - Rôle de l'utilisateur	sys_user_has_role	Définit le domaine d'un rôle d'utilisateur sur celui de son utilisateur.
Domaine - Définir le domaine - Historique de l'activité WF	wf_history	Définit le domaine de l'historique de l'activité du workflow en fonction du domaine du contexte du workflow parent.

Nom	Table	Description
Domaine - Définir le domaine - Contexte WF	wf_context	Définit le domaine de contexte du workflow en fonction du domaine de l'enregistrement référencé, le cas échéant.
Domaine - Définir le 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 valeur Tâche du ticket.
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 obtenir la valeur.
Domaine : valider par défaut	domain	Garantit que la case Par défaut est cochée pour un seul domaine.
Domaine : Valider primaire	domain	Garantit que la case Primaire est cochée dans un seul domaine.
Règles métier installées avec le module d'extension Domain Support		
Changer l'ensemble de domaine	sys_dictionary	Définit le domaine défini 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 de domaine).

Scripts clients

Script client	Description
Domaine - Définir la société et l'emplacement (sys_script)	Surveille les changements apportés au champ Appelant de l'incident. Si les champs de société et d'emplacement n'ont pas déjà de valeur, le script ajoute cette information à partir de l'enregistrement de l'appelant. Si les champs de société et d'emplacement ont déjà une valeur, le script conserve les valeurs existantes.
Script désactivé	
(BP) Définir l'emplacement sur 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 de Domain Separation par les applications

De nombreuses ServiceNow applications prennent en charge Domain Separation 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 délimitent les niveaux de prise en charge de Domain Separation 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 Domain Separation peuvent prendre en charge la séparation des données et l'acheminement des données uniquement, disposer d'une séparation de logique métier avancée ou prendre en charge l'administration au niveau du locataire (client) de l'application. ServiceNow Les applications sont définies avec les niveaux de prise en charge incrémentielle suivants.

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 le support 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 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 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 des 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’applications 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.		●	●

Fonctionnalité prise en charge	Élémentaire	Standard	Amélioré
Les propriétés d'application sont sensibles au domaine si nécessaire.		●	●
Les processus et la logique métier peuvent être séparés par domaine par le propriétaire de l'instance.		●	●
Les processus et la logique métier peuvent être administrés par le domaine de locataire.			●

Niveaux de prise en charge par application

Suite de produits	Application	Niveau de prise en charge
Hyperautomation and low-code	App Engine Studio	Aucune prise en charge
	Automation Center	Élémentaire
	Plateforme d'automatisation robotisée des processus (RPA)	Élémentaire
	Table Builder	Élémentaire
	Management Center du moteur de développement d'application	Aucune prise en charge
	Générateur de décision	Standard
	Intégration de la planification des ressources de l'entreprise	Aucune prise en charge
	Exploration de la personnalisation de la planification des ressources de l'entreprise	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	Base*
	Order Management pour Customer Service Management	Élémentaire
	Post-Sales Support	Élémentaire
	Domain separation in Workforce Optimization for Customer Service	Élémentaire
DevOps	DevOps	Aucune prise en charge
	Configuration DevOps	
Gestion des services aux employés	HR Service Delivery	Base*
	Santé et sécurité	Élémentaire
	Legal Service Delivery	Élémentaire

Suite de produits	Application	Niveau de prise en charge
	Gestion des services de procurement (PSM)	Aucune prise en charge
	Safe Workplace Suite	Consultez le site de l'application pour connaître les niveaux de prise en charge de chaque application
	Connecteur de recherche SharePoint Online	Élémentaire
	Demande universelle	Élémentaire
	Tâche universelle	Élémentaire
	Optimisation des effectifs pour les RH	Élémentaire
Gestion environnementale, sociale et de gouvernance	Gestion ESG	Élémentaire
Field Service Management	Field Service Management	Élémentaire
Governance, Risk, and Compliance	Business Continuity Management	Élémentaire
	Gouvernance, risque et conformité (GRC)	Élémentaire
	Operational Resilience	Élémentaire
Produits spécifiques à chaque secteur		
•	Financial Services Card Operations	Élémentaire
	Financial Services Deposit Operations	Élémentaire
	Financial Services Payment Operations	Élémentaire
	Entretien intelligent en cas de fraude	
	Services d'assurance de dommages	
	Gestion des services d'assurance-vie	
	Réclamations d'assurance	
	Financial Services Know Your Customer	
	Services financiers Opération de crédit	
	Processeur de documents pour les services financiers	Élémentaire
• Santé et sciences de la vie	EMR Help	Élémentaire
	Cœur de Service Management pour les soins de santé et les sciences de la vie	Élémentaire
	Gestion des pré-visites	Élémentaire
	Services de soutien aux patients	Élémentaire
	Vaccine Administration Management	Élémentaire

Suite de produits	Application	Niveau de prise en charge
• Production industrielle	Gestionnaire de processus de fabrication	Standard
	Operational Technology Manager	Standard
	Operational Technology Vulnerability Integration Response	Standard
	Operational Technology Service Management	Standard
•Télécommunications	Service Bridge	Élémentaire
	Gestion des commandes pour les télécommunications, les médias et la technologie	Élémentaire
	Workflows des télécommunications et de l'assurance des médias	Standard
IT Asset Management	Cloud Insights	Aucune prise en charge
	Hardware Asset Management	Amélioré
	Gestion des actifs logiciels	Amélioré
	Gestion des évaluations d'entreprise	Standard
Strategic Porfolio Management	Agile Development	Base*
	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	Base*
	Gestion des mises en production	Base*
	Scaled Agile Framework (SAFe)	Base*
	Test Management	Base*
	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
	Analyse de santé du journal	Élémentaire
	Analyse des mesures	Élémentaire

Suite de produits	Application	Niveau de prise en charge
	Service Mapping	Élémentaire
	Évaluation de la migration vers le cloud	Élémentaire
	Bibliothèque d'actions	Aucune prise en charge
	Cloud Configuration Governance	Aucune prise en charge
	Tag Governance	Élémentaire
	Facturation 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 des opérations dans le cloud	Élémentaire
	Détection 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
	Expense Line	Aucune prise en charge
	Gestion des communications d'incident	Standard
	Gestion des incidents	Standard
	Facilities Service Management	Standard
	Gestion des incidents	Standard
	On-Call Scheduling	Standard
	Gestion des actifs	Élémentaire
	Problem Management	Standard
	Procurement	Standard*
	Catalogue de produits	Standard
	Gestion des requêtes	Standard
	Service Catalog	Standard
	Appel du centre de services	Élémentaire
	Service Level Management	Élémentaire
	Gestion des portefeuilles de services	Base*
	Opérations pour la fiabilité des sites	Base*

Suite de produits	Application	Niveau de prise en charge
	Panne de tâche	Élémentaire
	Domain separation and Vendor Management Workspace	Aucune prise en charge
	Expérience de visite	Élémentaire
Configuration et navigation Mobile	Mobile	Élémentaire
Now Intelligence	Dashboards	Élémentaire
	Performance Analytics	Amélioré
	Process Optimization	Élémentaire
	Reporting	Élémentaire
	User Experience Analytics	Élémentaire
La Now Platform	,Administration,Moteur d’application, Options de la Now Platform Interface utilisateur	
	Domain separation and Agent Chat	Standard
	Advanced Work Assignment	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	
	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	Base*
	Classification des données	Amélioré
	Confidentialité des données	Aucune prise en charge
	Gestion des données	Base*
	Développement délégué	Aucune prise en charge
	Dependency Views	Élémentaire
	Services documentaires	Aucune prise en charge
	Dynamic Translation	Élémentaire
	Edge Encryption	Aucune prise en charge

Suite de produits	Application	Niveau de prise en charge
	Chiffrement au niveau des colonnes	Aucune prise en charge
	Entreprise de Chiffrement au niveau des colonnes	Aucune prise en charge
	Chiffrement dans le cloud avec gestion des clés	Support de base
	Normalisation de champ	Aucune prise en charge
	Flow Designer	Standard*
	Configuration guidée	Aucune prise en charge
	Administration de la page d'accueil	Base*
	IntegrationHub	Standard*
	Intégrations avec des applications tierces et des sources de données	Basique + Standard
	Knowledge Management	Standard
	Service de messagerie Hermes	Aucune prise en charge
	Documents gérés	Aucune prise en charge
	MetricBase	Élémentaire
	Compréhension naturelle de la lessification	Basique + Standard
	Notifications	Standard
	Pilote ODBC	Base*
	Orchestration	Standard*
	Password Reset	Standard
	Sécurité de la plateforme	Page de destination de Domain Separation
	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
	Domain separation and Sidebar	Standard
	Flux d'états	Aucune prise en charge
	Subscription Management	Base*
	Gestion des enquêtes	Base*

Suite de produits	Application	Niveau de prise en charge
	Intelligence des tâches	Aucune prise en charge
	Carte de pointage	Base*
	UI Builder	Standard
	Virtual Agent	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
	Trusted Security Circles	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 de la main d'œuvre pour ITSM	Élémentaire
	Vendor Management Workspace	Élémentaire

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Vous pouvez créer, implémenter et gérer Domain Separation pour vos applications et services.

Notions de base sur les domaines

Avec Domain Separation (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 comment Domain separation est configuré et quelles règles affectent la configuration.

Avant de vous lancer dans l'aventure de la séparation de 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.

Explication de Domain Separation

Avec Domain Separation, 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 logiquement prend en charge des hiérarchies spécifiques pour tous les clients qui utilisent vos applications.

Notions de base sur les domaines

Domain Separation, également connue sous le nom d'architecture ServiceNow de plateforme mutualisée, entraîne une surcharge considérable dans la gestion d'une instance. Cependant, si vous utilisez correctement Domain Separation, cela 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 Domain Separation

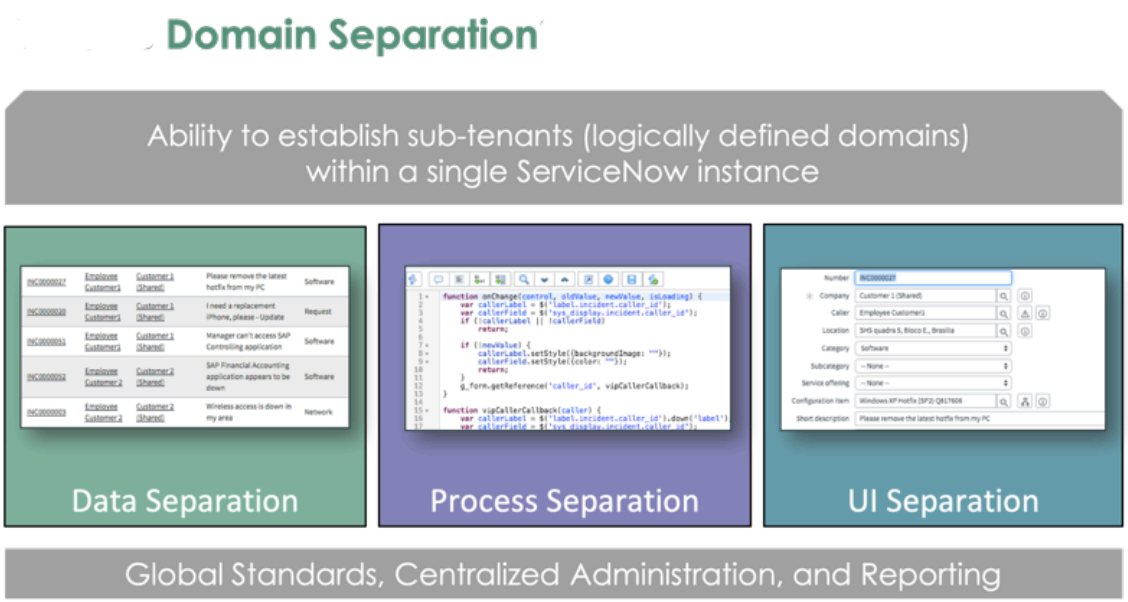
- Séparation des données : permet aux locataires du domaine d'afficher uniquement les données pour lesquelles ils sont autorisés. Les locataires peuvent avoir accès à d'autres données de locataire, mais ne peuvent pas interroger les données des locataires auxquelles ils n'ont pas accès.
  - Lorsque vous 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 dans les domaines auxquels ils sont autorisés à accéder.
  - Les clients, les agents et les prestataires peuvent accéder aux données relatives aux clients et aux organisations qu'ils prennent en charge.
- 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 ou un ensemble de domaines spécifique tout en préservant votre logique de processus de base.
- Les fournisseurs de services peuvent modifier les marques affichées et les éléments d'interface utilisateur pour répondre aux besoins individuels des clients.

- Séparation de la logique métier : crée 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.
- Modélisation hiérarchique : imbrique vos locataires multiples 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 entre locataires : 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.

Domain separation 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.

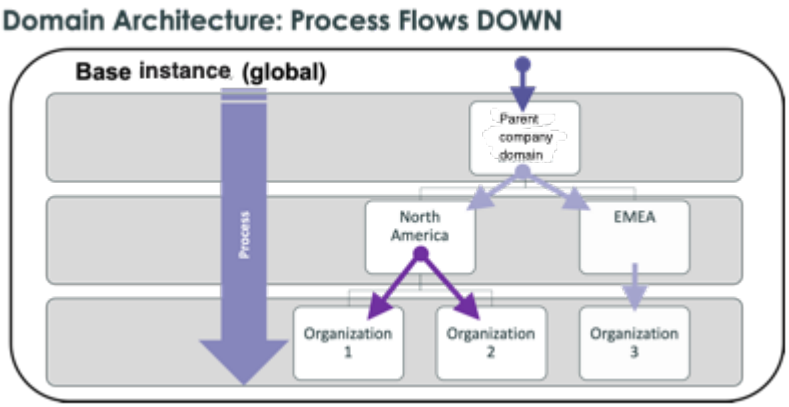


Architecture de domaine

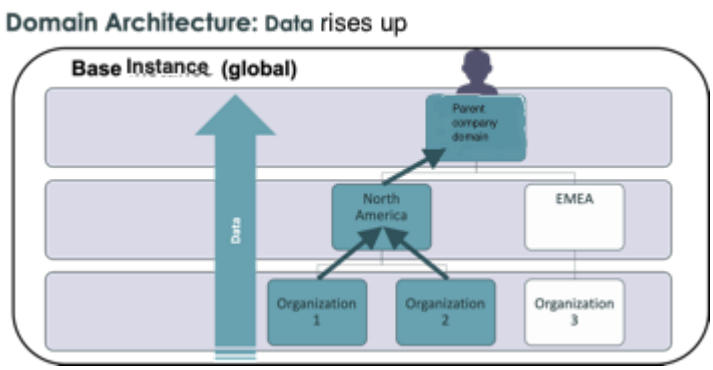
Les enregistrements utilisateur se voient attribuer une valeur de domaine qui représente le domaine d'origine de l'utilisateur. Les utilisateurs n'ont pas accès aux données des domaines parents, des domaines pairs ou des domaines d'autres branches de la hiérarchie.

Consultez Contient les requêtes et l'accès au domaine les options avancées permettant d'accorder une visibilité de domaine supplémentaire.

Le diagramme suivant montre comment le processus d'architecture s'écoule jusqu'aux



domaines enfants.



Proposition de valeur Domain Separation

Avec Domain Separation, les fournisseurs de services peuvent disposer d'une architecture d'instance mutualisée qui fournit des offres efficaces et sécurisées à leurs clients. Des normes de processus universelles rigoureuses, une conception de processus pilotée par les données, une gouvernance stricte et une administration centralisée contribuent à maximiser ces avantages.

Avantages de Domain Separation

Les locataires d'un domaine bénéficient d'un retour sur investissement rapide, d'une réduction des frais administratifs 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 de domaines
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 clients	Une intégration plus rapide
Évolutivité et évolutivité	Tirer parti des dernières versions
Ségrégation des données	Services fournis par le propriétaire de l'instance
Génération de rapports globaux	

Définition de Domain Separation

Avec Domain Separation (également connue sous le nom d'architecture de plateforme mutualisée), vous pouvez séparer les données d'application, l'interface utilisateur et la ServiceNow® logique métier dans une instance client unique qui prend en charge la modélisation hiérarchique avec l'intelligence interlocataire (client).

Propriétés de Domain Separation

Les applications séparées ServiceNow par domaine sont définies avec les propriétés suivantes :

Séparation des données

Permet aux clients d'afficher uniquement les données pour lesquelles ils ont l'autorisation. 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 spécifique au client pour les éléments d'interface utilisateur tels que les vues, les listes, les étiquettes, etc.

Séparation 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 des clients enfants. La logique métier pour les clients parents s'exécute automatiquement pour les clients enfants et peut être remplacée à n'importe quel niveau.

Connaissance 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.

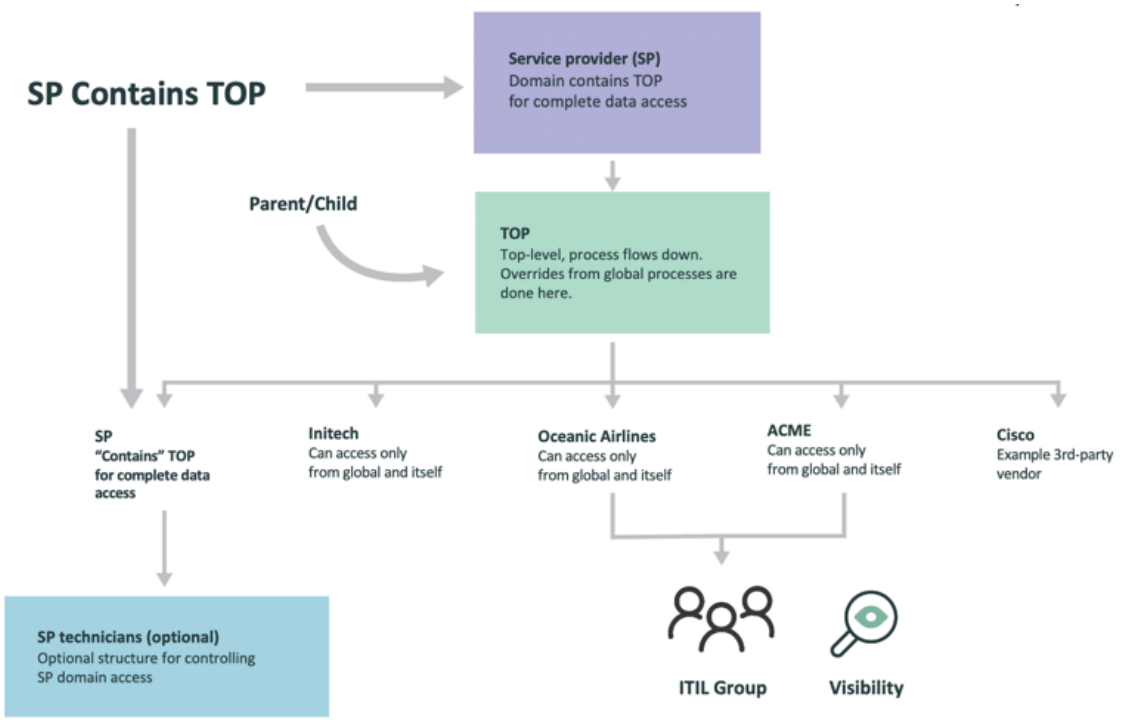
Vous ne voyez pas le mot « Global » dans ce diagramme car il n'y a pas de domaine global. N'oubliez pas que « global » se traduit par l'absence d'un domaine dans un enregistrement.

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.
  - 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

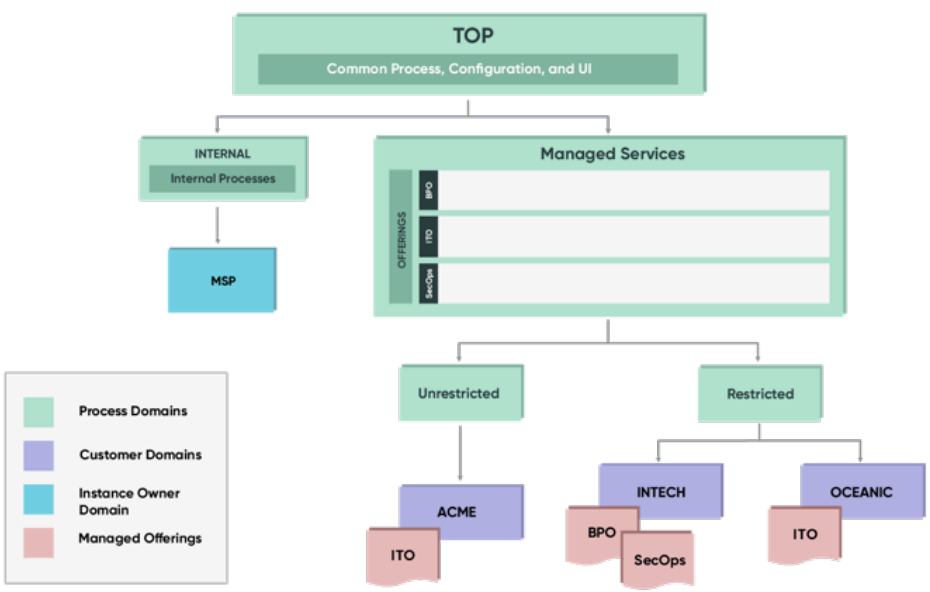
Cas d'utilisation avec et sans restriction pour la séparation de domaines.

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).

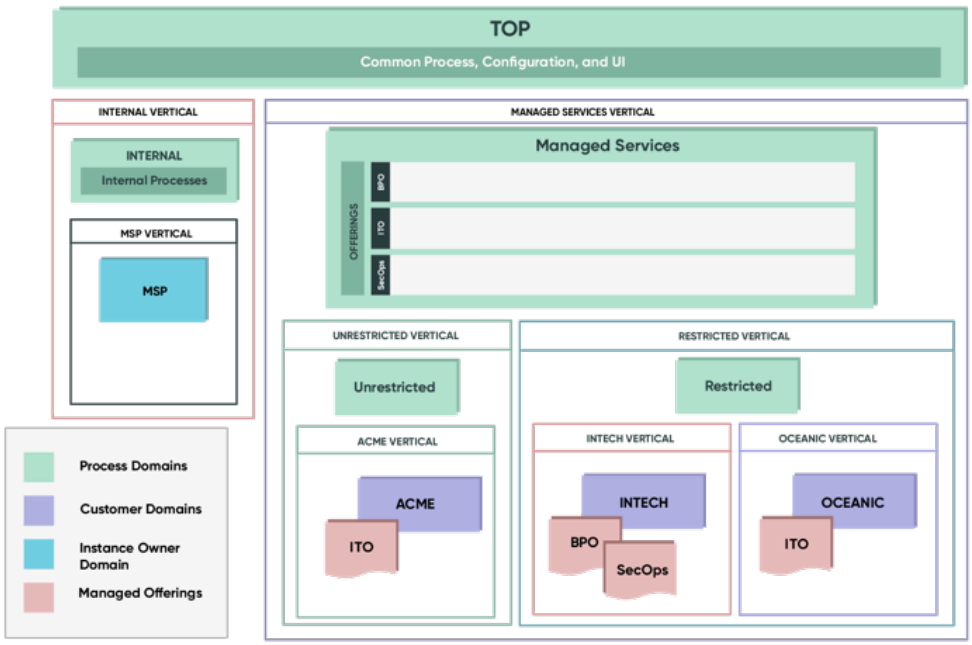
1. Les clients se trouvent dans un « vertical » spécifique de la hiérarchie de séparation de domaines Cela signifie qu'ils n'utilisent que des processus définis dans leur domaine et tous les domaines parent au-dessus du leur dans la hiérarchie. Tous les processus définis dans les domaines qui ne sont 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

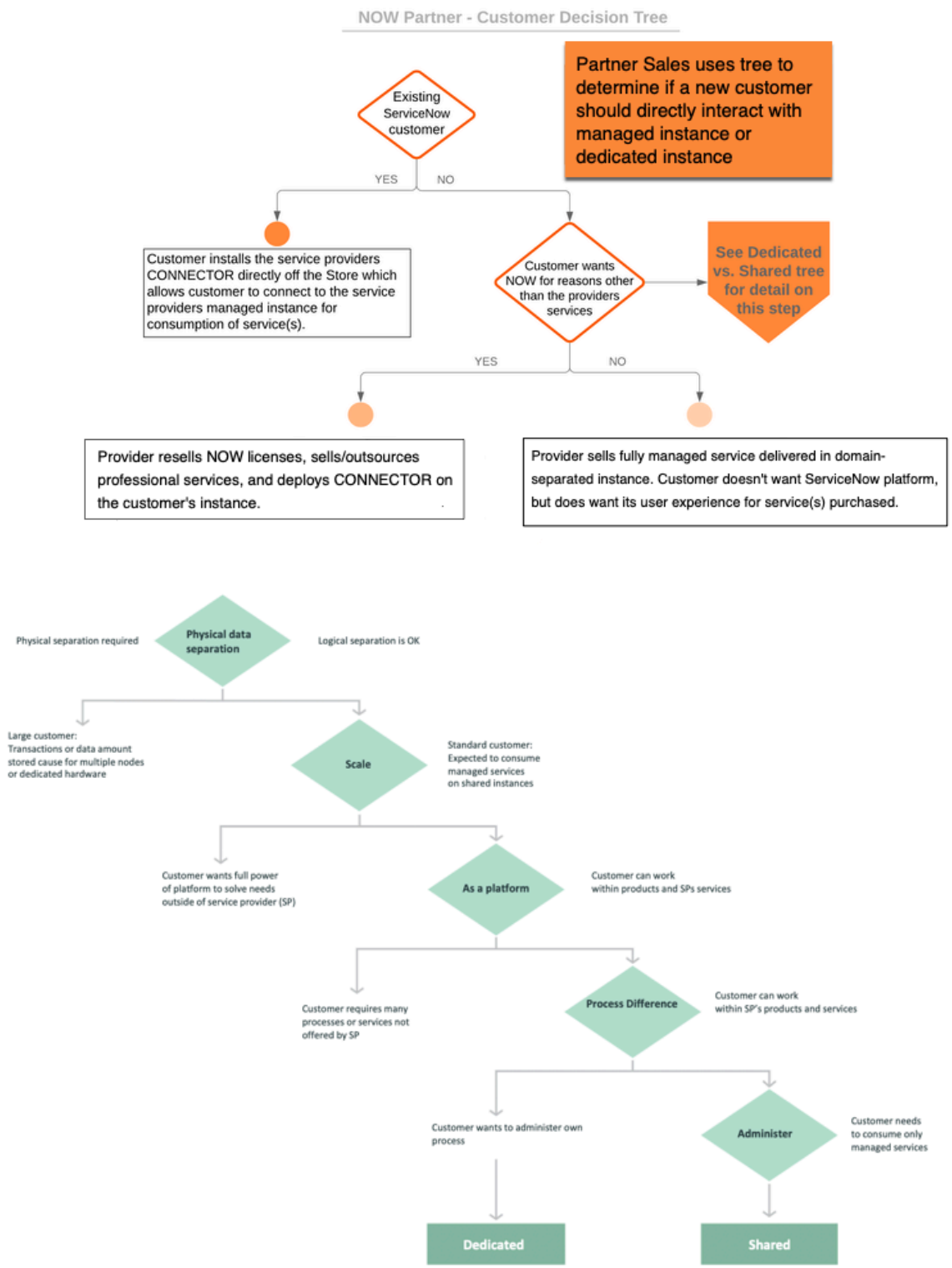


Voici quelques cas d'utilisation :

- 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 ».

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.



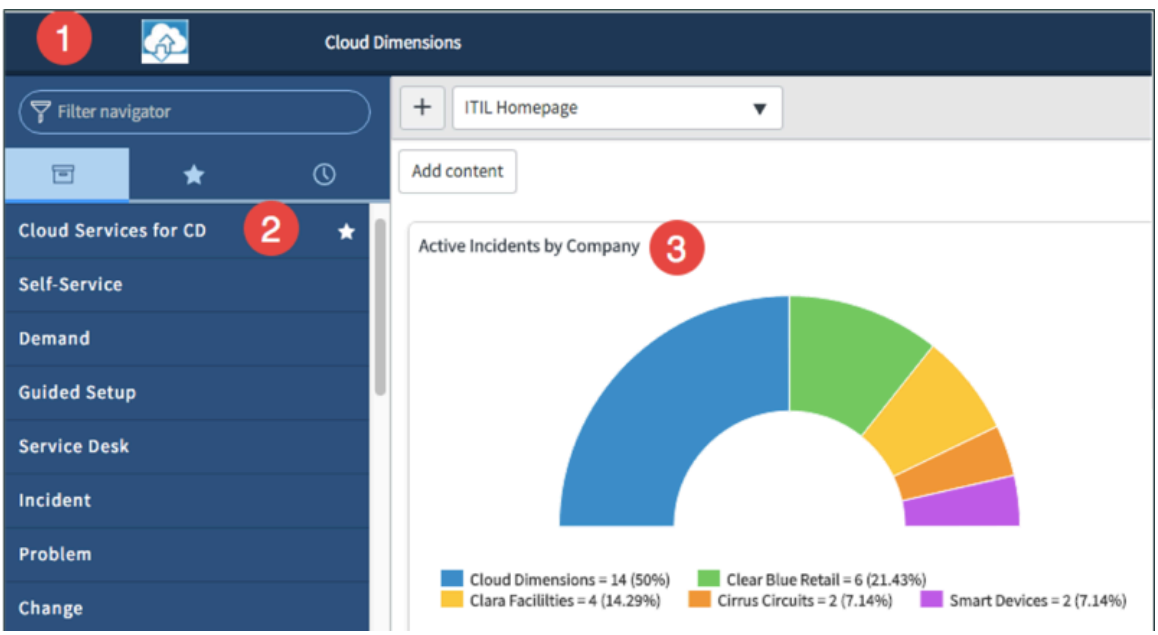
Pour en savoir plus sur l'architecture des hiérarchies, consultez Architecture de référence du fournisseur de services.

Contexte et séparation de domaine

Le contexte de la session d'un utilisateur détermine les processus, les données et l'interface utilisateur lorsque 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 de l'utilisateur

De nombreux facteurs déterminent le contexte d'une session utilisateur, tels que les profils d'utilisateurs, les groupes, les critères d'entreprise, etc. Dans le diagramme suivant, vous voyez que les incidents qu'une entreprise a créés font partie du contexte.

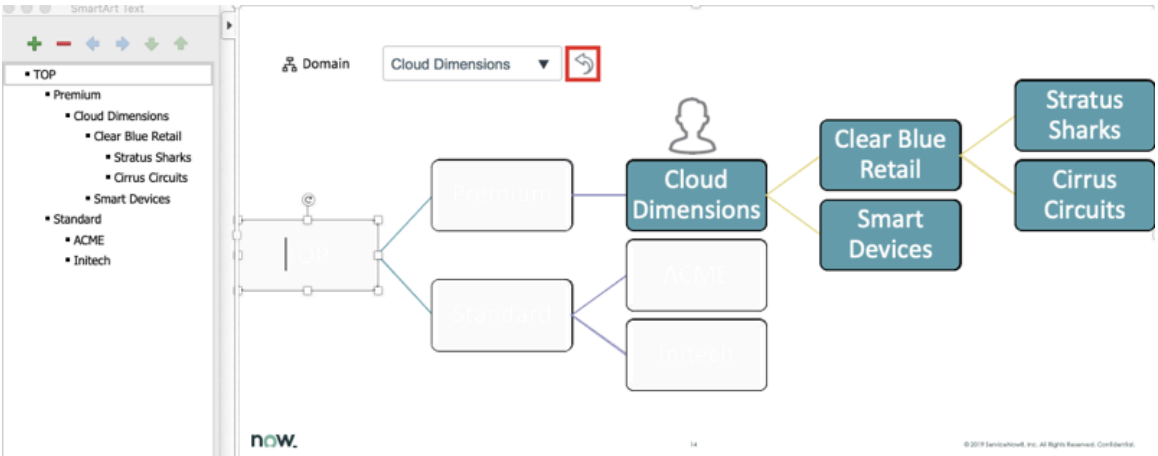


Dans cet exemple, l'utilisateur a un domaine d'accueil Cloud Dimensions.

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 qui sont définis dans le domaine Dimensions cloud.
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 Dimensions du cloud peut voir les données dans les dimensions du cloud, les domaines enfants et le domaine global.

Le contexte de la session utilisateur commence dans le domaine d'origine

Dans le diagramme suivant, vous pouvez voir les éléments du contexte.



L'administrateur système définit les domaines d'origine 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 sa société. Lorsque l'utilisateur se connecte, le sélecteur de domaine se définit automatiquement sur le domaine d'origine de l'utilisateur. Les utilisateurs peuvent revenir à leur domaine d'origine à tout moment en cliquant sur l'icône flèche dans le sélecteur de domaine.

La liste du sélecteur de domaine inclut les domaines dans le contexte de la session de l'utilisateur. Les utilisateurs peuvent limiter davantage le contexte de leur session en sélectionnant des domaines enfants à l'aide du sélecteur.

Le contexte de la session utilisateur inclut le domaine d'origine 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 ont également 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 que le développeur a configurées.

Pour en savoir plus sur d'autres méthodes d'ajout de domaines au contexte de la session d'un utilisateur, reportez-vous à Architecture de référence du fournisseur de serviceslа section .

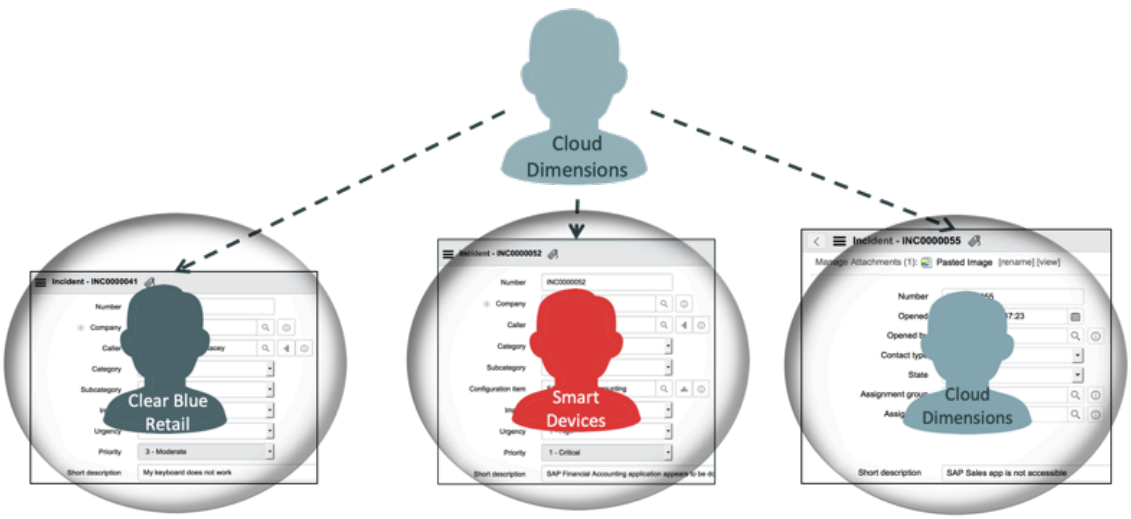
Contexte d'enregistrement

Au fur et à mesure qu'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 détermine le processus, les données et la disponibilité des éléments d'interface utilisateur au sein de l'enregistrement.

Remarque :

- Le contexte d'enregistrement est conservé même si le domaine de l'utilisateur change.
- Les utilisateurs peuvent afficher les enregistrements simultanément dans plusieurs onglets de navigateur, tout en conservant leur propre contexte d'enregistrement.

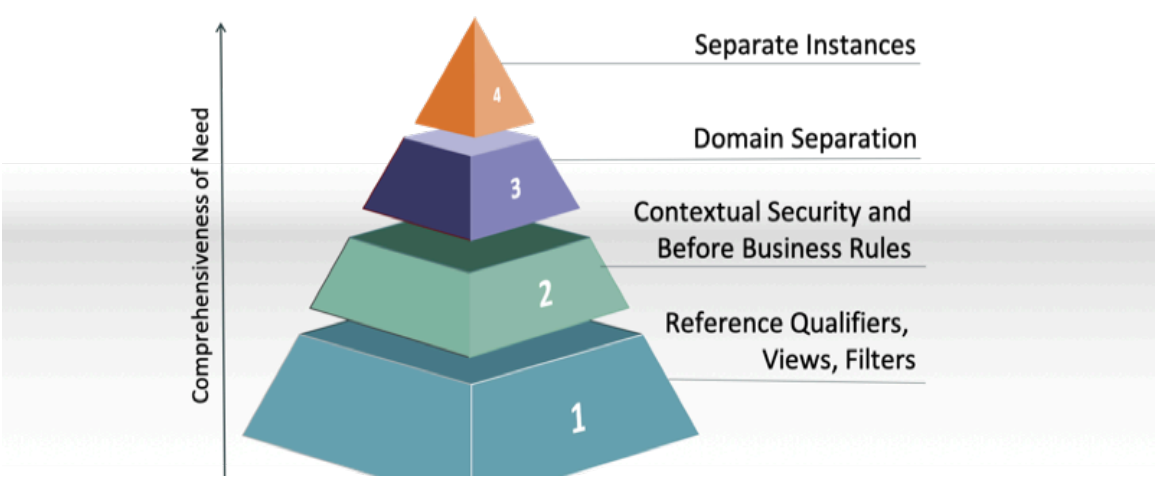


Ségrégation et sécurisation des données avec Domain Separation

Vous pouvez séparer et sécuriser les données sur la ServiceNow plateforme de plusieurs façons, en fonction des besoins de vos clients.

Séparation des données de plusieurs façons

Le diagramme suivant montre quatre façons de séparer les données. Vous pouvez utiliser des instances distinctes, Domain Separation, la sécurité contextuelle et les règles métier, ainsi que l'architecture de référence elle-même pour séparer les données.



Vous pouvez séparer les données de ces quatre façons :

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 de la sécurité contextuelle et des règles métier Avant requête comme couches de sécurité supplémentaires pour se prémunir contre les violations de données. Consultez Contexte et séparation de domaine et Règles métier Avant requête pour en savoir plus sur Domain Separation et les règles métier.

Traduction automatique

3. Ajouter un niveau de sécurité supplémentaire dans une entreprise en utilisant Domain Separation. Les données de chaque requête de base de données sont limitées aux données 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 couche de base de données et de l'application.

Les instances distinctes, la séparation de domaine, la sécurité contextuelle et les règles métier, ainsi que l'architecture de référence sont des méthodes de ségrégation des données. Ces quatre voies 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 Domain Separation.

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 Évaluation de la nécessité d'une séparation de domaine.

Intelligence entre locataires

Une architecture multilocataire est une instance unique desservant plusieurs locataires. Les données, les métadonnées, la logique métier et le contexte de traitement pour les locataires sont automatiquement gérés avec l'accès aux données supplémentaires des locataires.

Locataires uniques ou multiples

Instance à locataire unique

Vous êtes client ServiceNow , vous avez acheté les licences, et c'est à vous de décider quels services vous voulez. Vous pouvez effectuer la mise à niveau quand vous le souhaitez, afficher des aperçus de toutes les nouvelles fonctionnalités et configurer votre instance immédiatement. Le fait d'être un locataire unique présente les avantages et les restrictions suivants :

- Vous avez des coûts initiaux et des frais administratifs plus élevés, mais vous avez plus de liberté pour rénover et agrandir.
- Vous avez des coûts plus élevés pour obtenir et maintenir l'instance et le personnel d'administration des approvisionnements. Bien que vous soyez libre d'aménager l'environnement selon vos besoins, vous devez vous conformer aux ServiceNow pratiques et aux normes recommandées.

Instance à locataires multiples

Quelqu'un d'autre est propriétaire de l'instance, peut-être un fournisseur de services avec plusieurs clients. Ils effectuent une 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 services, vous êtes probablement sur leur instance parce que vous vouliez ce qu'ils offrent. Plusieurs locataires bénéficient des avantages et restrictions suivants :

- Un personnel centralisé administre les configurations, les intégrations et les mises à niveau.
- Le propriétaire de l'instance fournit des services supplémentaires.
- Les locataires de domaines ont des coûts initiaux inférieurs pour utiliser la ServiceNow plate-forme, ont des coûts mensuels inférieurs parce qu'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 Domain Separation

Vous pouvez utiliser une instance distincte comme alternative à Domain Separation 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 des 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 de référence
Choisir la région du CENTRE DE DONNÉES	Code du système de base modifié ignoré pendant les mises à niveau
Contre	Doit également s'adresser à toutes les tables secondaires et de support
Coût	Des tests approfondis requis
Alignement des instances	Pas ServiceNow d'équipe produit pour 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 assurer une coordination importante avec d'autres personnes qui administrent les instances. En configurant une instance avec une sécurité contextuelle, des vues de formulaire, des qualificatifs de référence, des filtres et des conditions robustes, vous n'avez pas besoin d'utiliser Domain Separation dans votre entreprise.

Avec une instance distincte, vous pouvez traiter la séparation des données et des processus, mais vos propriétaires d'instances doivent gérer et suivre les personnalisations étendues requises pour des instances distinctes.

Information associée

Contexte et séparation de domaine

Architecture de référence du fournisseur de services

Évaluation de la nécessité d'une séparation de domaine

Vous constaterez peut-être que Domain Separation ne fonctionne pas toujours pour les organisations de vos clients. Il est préférable que vous basiez votre décision d'opter pour la séparation de domaine en examinant les besoins de vos clients.

Évaluation de la nécessité d'une séparation de domaine

Raisons de Domain separation

Ces facteurs peuvent vous aider à choisir Domain Separation 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 les 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 votre propriétaire d'instance a déterminé que le besoin peut être traité ailleurs dans la configuration.
- Les propriétaires d'instances de votre entreprise ont des entités entières qui fonctionnent comme des organisations physiquement séparées et ne partagent pas de données, mais des rapports complets sont toujours nécessaires. Des domaines distincts permettraient une visibilité des données lorsqu'ils sont configurés correctement.

Raisons pour lesquelles il n'y a pas de séparation de domaine

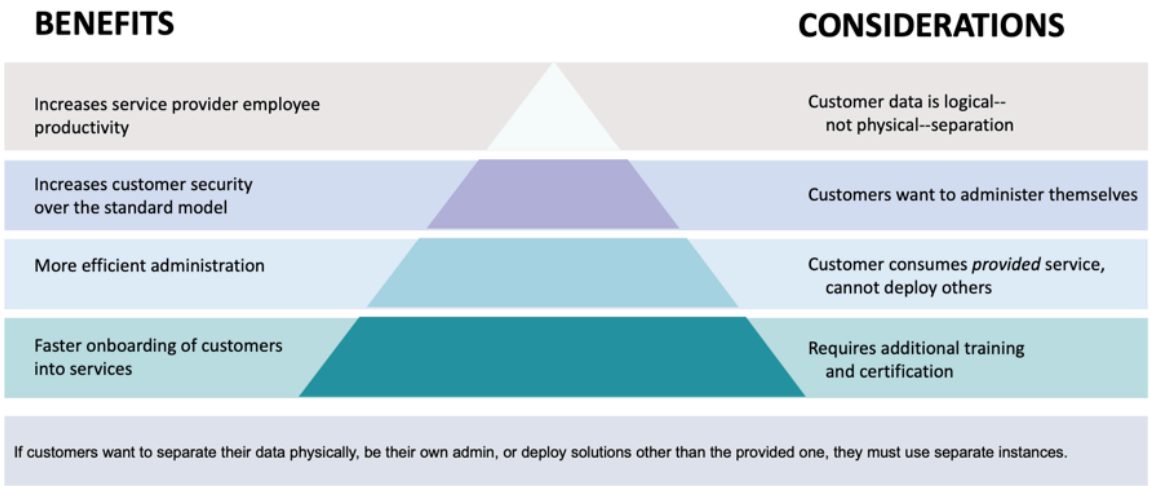
Ces facteurs peuvent indiquer des raisons pour lesquelles les organisations de vos clients ne souhaitent peut-être pas configurer Domain Separation :

- Vos clients veulent administrer leur environnement, se l'approprier intégralement et définir la feuille de route pour l'expansion.
- Vos clients exigent que les données et le 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 réduit l'exigence d'isolement.

- Les départements de l'organisation de vos clients souhaitent isoler les enregistrements. (Des 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 uniquement en tant qu'utilisateurs finaux.

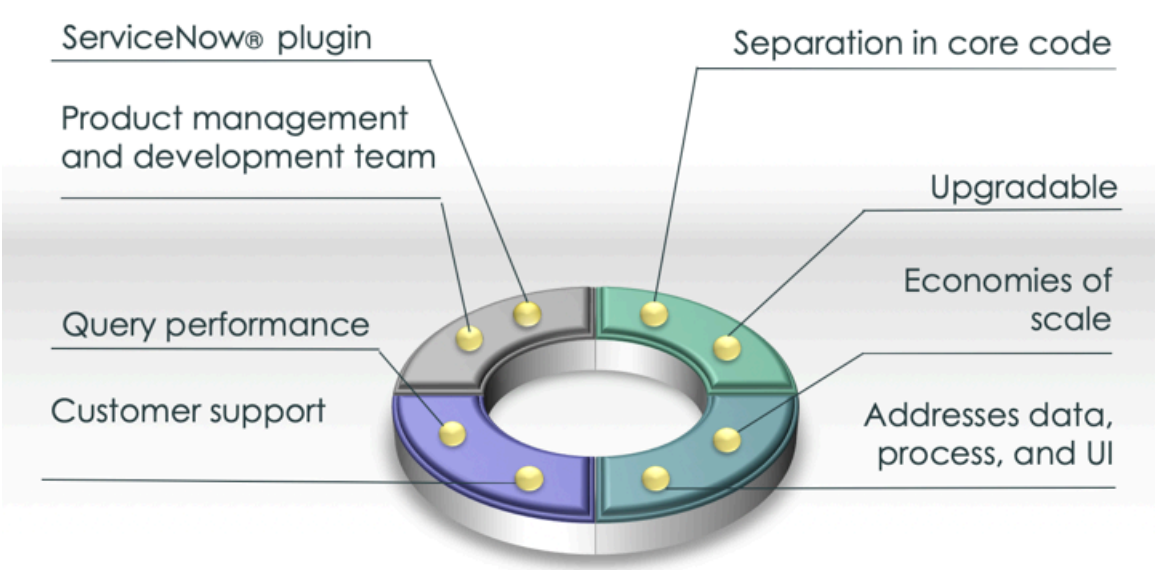


Avantages de Domain Separation

Domain Separation peut être plus efficace pour les organisations de vos clients que toute autre méthode de séparation des données entre les groupes et les départements.

Les avantages de Domain Separation en un coup d'œil

Vous pouvez activer Domain Separation à l'aide d'un module d'extension ServiceNow doté de fonctionnalités intégrées à la plateforme principale. La configuration de domaines distincts est gérée par un chef de produit assisté d'une équipe de développement. Des améliorations et des correctifs pour la fonctionnalité Domain Separation sont inclus dans ServiceNow les versions et sont prêts à être utilisés par les clients. Pour obtenir de l'aide concernant Domain Separation, les propriétaires de votre instance peuvent utiliser Service et assistance client des ressources, telles que le Service Portal .



Fonctionnement d'une requête de base de données avec Domain Separation

L'utilisation de requêtes de base de données avec Domain Separation dans les applications de vos clients les aide à protéger leurs données. Ces requêtes accélèrent ensuite les processus de configuration et de génération.

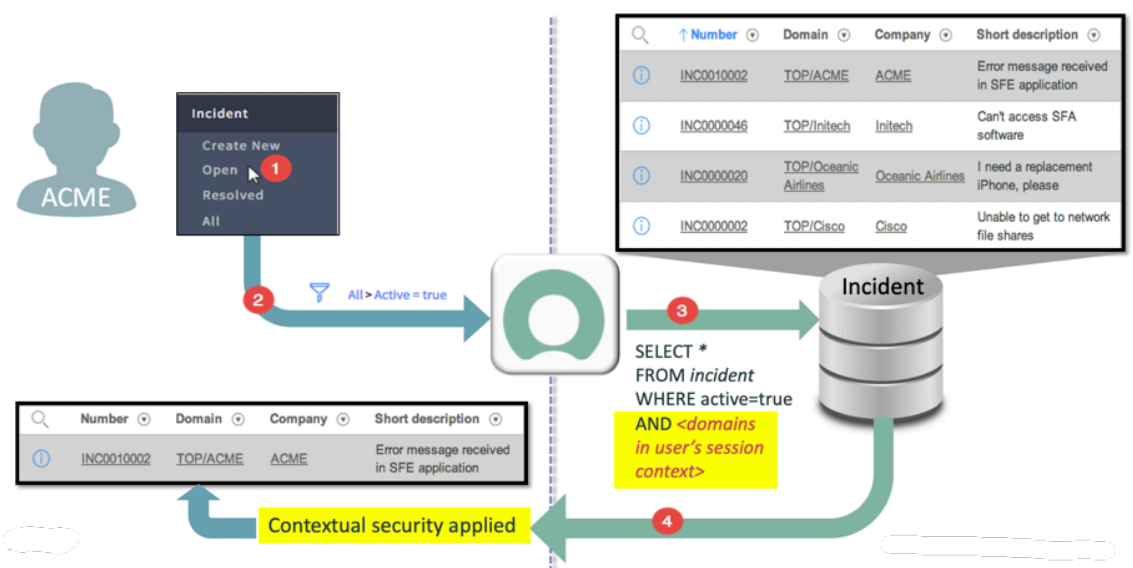
Traduction automatique

Comment Domain Separation protège les données

Dans la figure suivante, la table Incident [incident] possède un champ de domaine 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'origine s'affiche avec l'ensemble des domaines auxquels ils peuvent accéder. C'est ce qu'on appelle le contexte de la session de l'utilisateur. Pour plus d'informations sur les contextes de session, reportez-vous à la section Contexte et séparation 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 active=true.
2. Le filtre active=true 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, ce qui limite davantage les données renvoyées à l'utilisateur. Les enregistrements d'incident apparaissent dans la liste 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 Contexte et séparation de domaine.

Remarque :

Cette logique de traitement s'applique à toutes les requêtes adressées à la base de données, y compris les requêtes déclenchées à l'aide d'intégrations.

Niveaux de prise en charge de Domain Separation

Choisissez parmi trois catégories pour Domain Separation d'une application pour les organisations de vos clients.

Les applications qui prennent en charge Domain Separation peuvent prendre en charge la séparation des données et l'acheminement des données uniquement, 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, la génération de rapports, les déploiements, les agrégations, etc. prennent tous en compte les propriétés du domaine au moment de l'exécution. • Les propriétaires de votre instance doivent être en mesure de configurer l'application pour qu'elle fonctionne normalement sur plusieurs locataires. Cas d'utilisation : lorsqu'un fournisseur de service utilise la messagerie instantanée

Niveau	Type	Résumé
		pour répondre au message d'un client, le client doit pouvoir voir la réponse.
Standard	Gestion des processus clients	• Comprend le niveau de base • Logique métier : les processus peuvent être créés ou modifiés par client par le fournisseur de services. Les cas d'utilisation reflètent la façon dont l'application est utilisée par plusieurs clients fournisseurs de services dans une seule instance. • Les propriétaires de votre instance 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 rendre les commentaires nécessaires lorsqu'un enregistrement se ferme pour un client, mais pas pour un autre.
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 modifications 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 services, même si le cadre de travail de domaine n'est pas utilisé. Les cas d'utilisation doivent être détaillés pour prendre en charge Domain Separation. Un

Niveau	Type	Résumé
		astérisque (*) après le niveau de prise en charge indique ce type de configuration. 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 dans une instance séparée par domaine à l'aide de critères d'utilisateur. Par conséquent, chaque locataire pouvait utiliser Service Catalog à un niveau standard.

Pour afficher toutes les applications répertoriées par niveau de prise en charge, reportez-vous Prise en charge de Domain Separation par les applicationsà .

Résumé

Domain Separation est un cadre de travail que vous devez utiliser pour faire connaître les clients de vos applications.

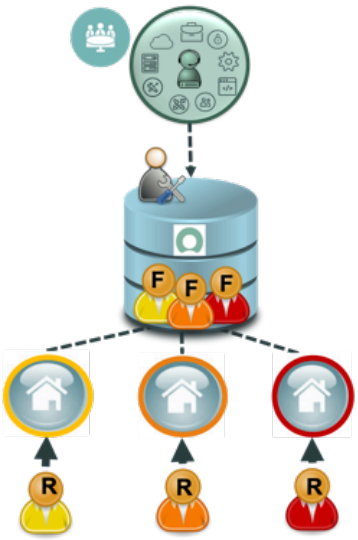
Tenez compte des options du cadre de travail de domaine, des cas d'utilisation métier de vos applications, des profils et de la façon dont ils utilisent l'application avant de pouvoir utiliser le cadre de travail pour rendre votre application possible à prendre en charge.

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 accèdent à leur instance séparée par domaine.

Attributs de base de l'architecture de référence du fournisseur de services

- Vous n'affectez pas de prestataires à un domaine. Au lieu de cela, vous les partagez entre les domaines. Il est donc plus difficile d'auditer le nombre de prestataires que vous avez par domaine.
- Vous pouvez partager et exploiter l'administration du domaine. Cela signifie qu'il n'y a pas de frais généraux 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.



- 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

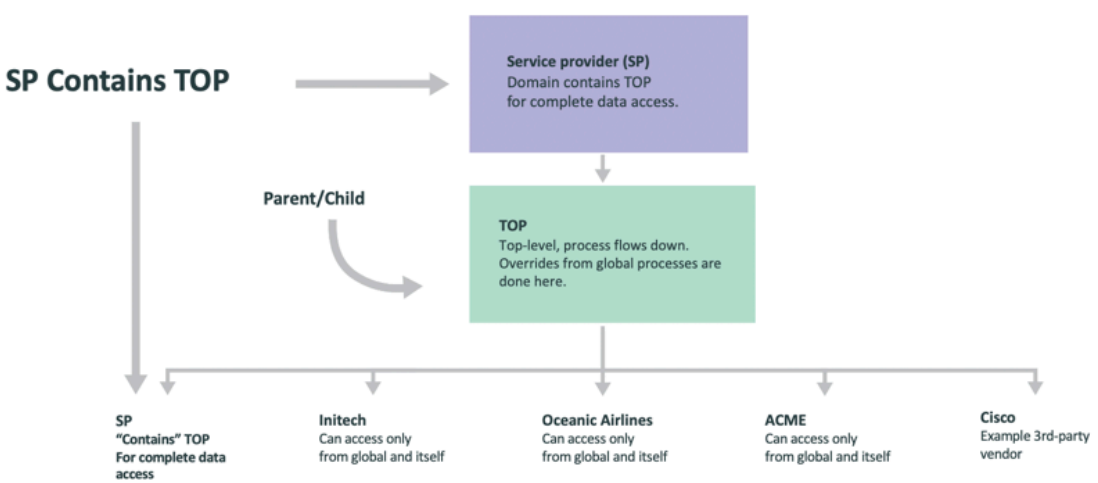
Centralized administration at the SP. Shared business requirements and configurations

Both SP and customer fulfillers on one instance

Customer requesters on each instance

Le portail des services du SP est dédié ou partagé avec l'instance partagée du 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

Comparaison de l'architecture de référence du SP

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.

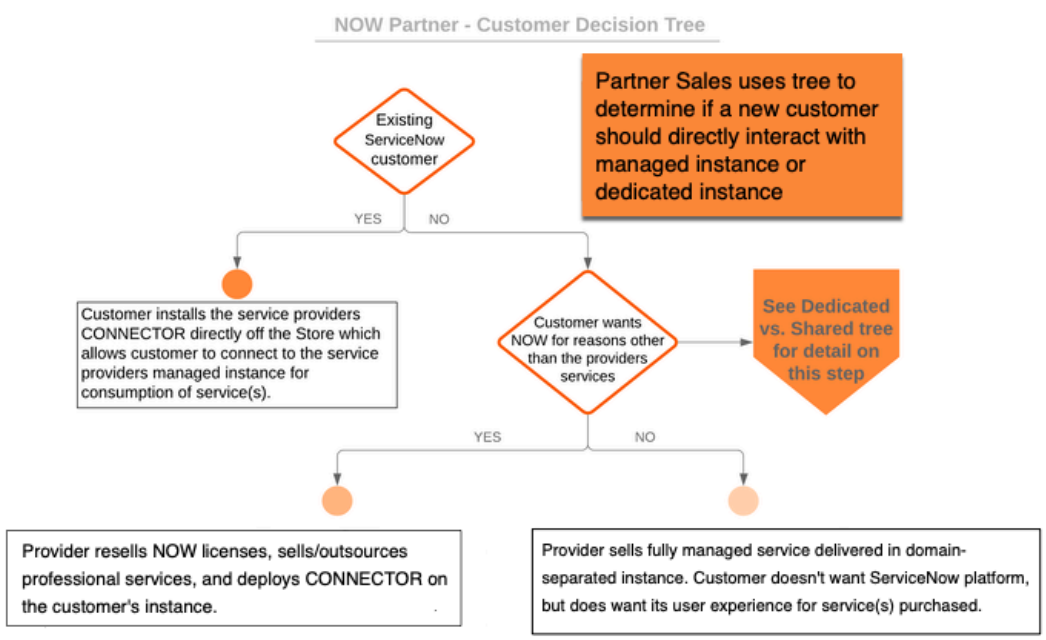
Arborescences de décision relatives à l'architecture de référence du fournisseur de services

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.

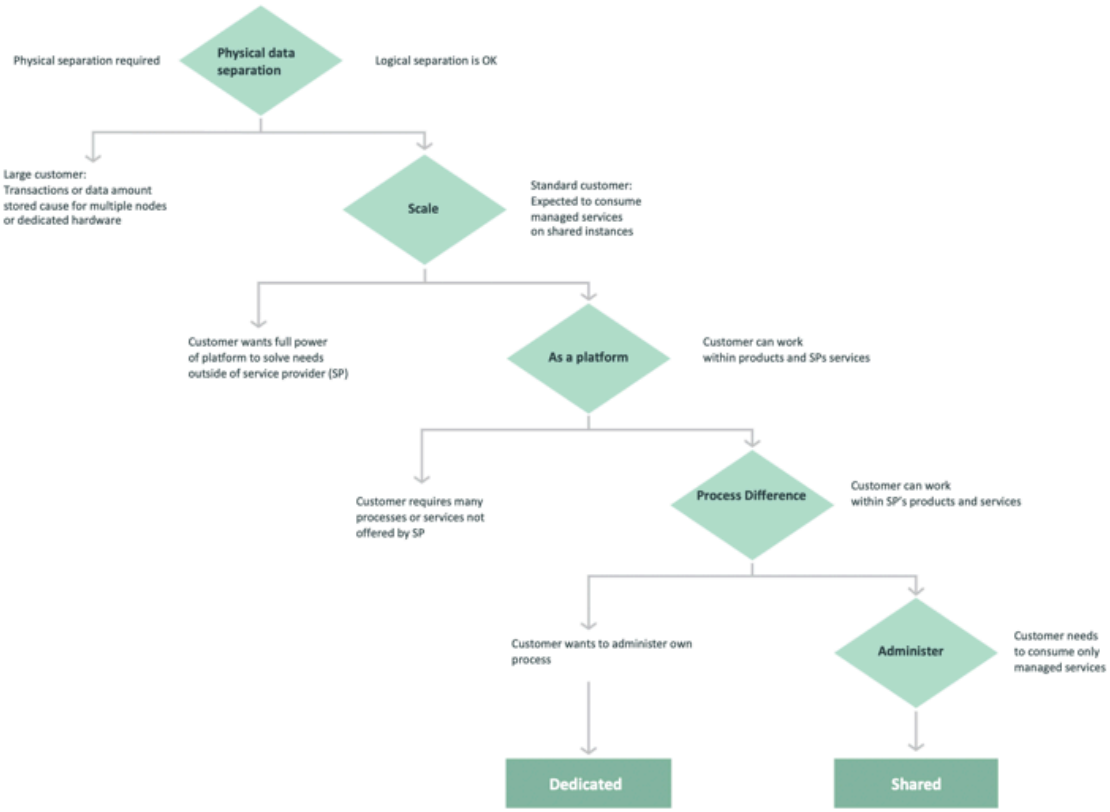
Arborescences de décision

Utilisez ces arborescences de décision pour aider vos clients à décider s'ils doivent utiliser une instance gérée ou dédiée.

Arborescence des décisions client



Traduction automatique



Comparaison de l'architecture de référence du SP

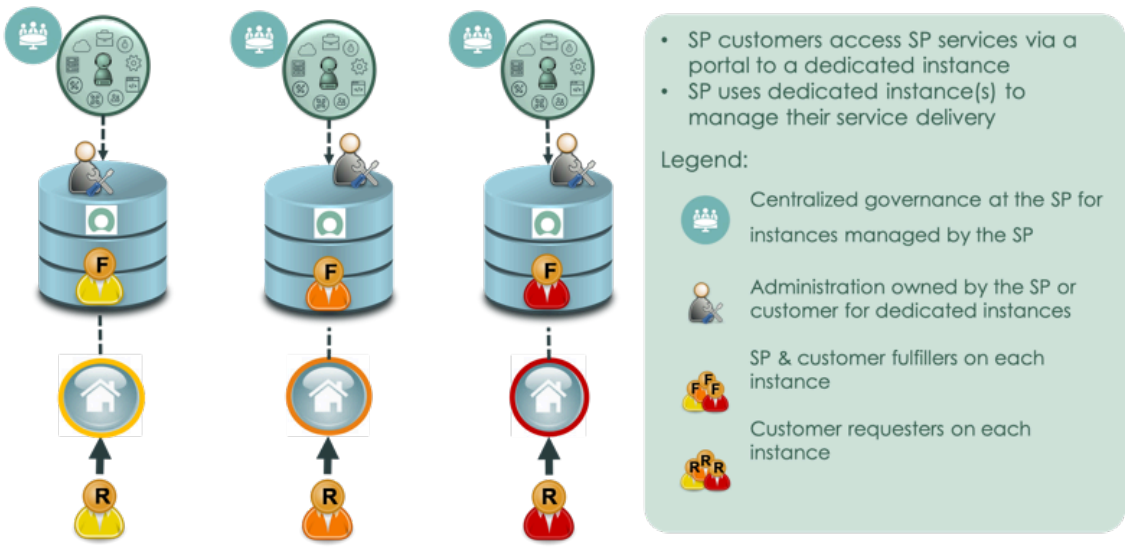
Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside 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 les instances dédiées

Les clients des fournisseurs de services (SP) peuvent accéder aux services SP à l'aide d'un portail vers une instance dédiée. Les fournisseurs de services utilisent ces instances dédiées pour gérer leur prestation de services.

Traduction automatique

Instances dédiées



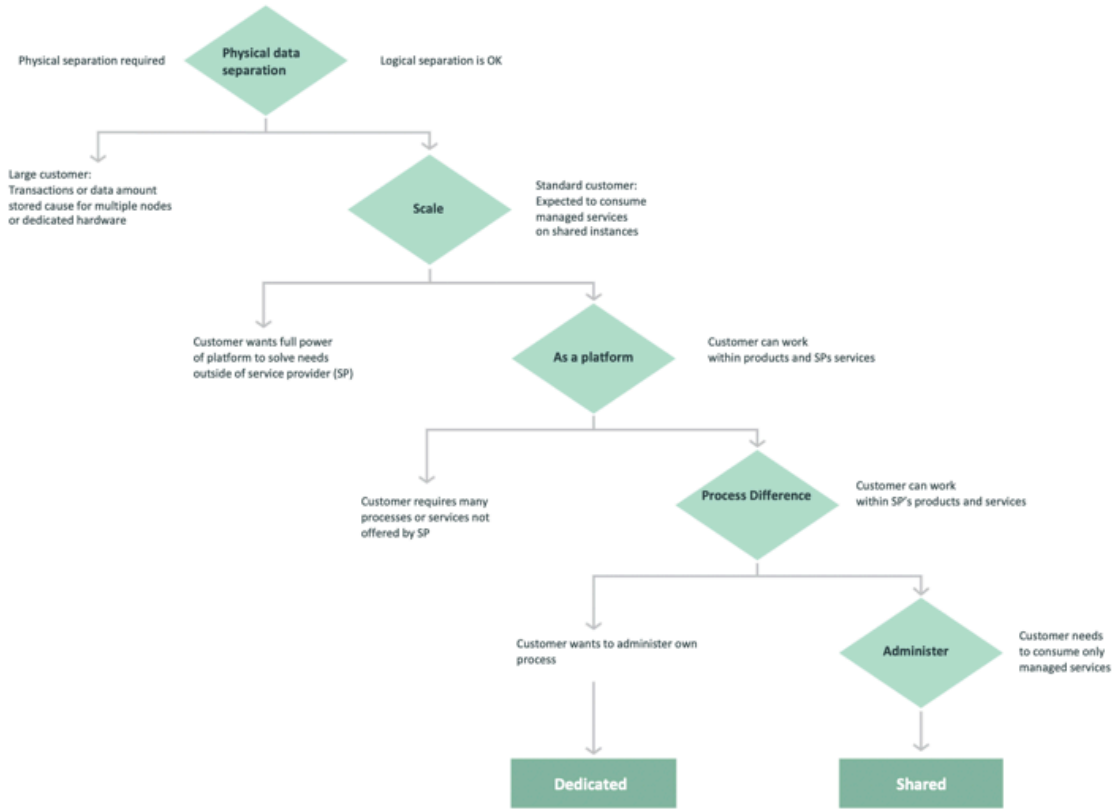
Attributs

- Les instances dédiées nécessitent que vous disposiez d'une administration et d'équipes dédiées distinctes. Vous avez besoin de plusieurs licences pour les administrateurs et les développeurs qui se connectent à plusieurs instances.
- Chaque instance dispose d'un nombre limité de demandeurs et de prestataires. Lorsque vous recevez un nouveau client, vous devez vous procurer une instance basée sur la taille et l'échelle de la société de votre client.

Traduction automatique

Instance partagée

Instance dédiée vs. instance partagée



Comparaison de l'architecture de référence du SP

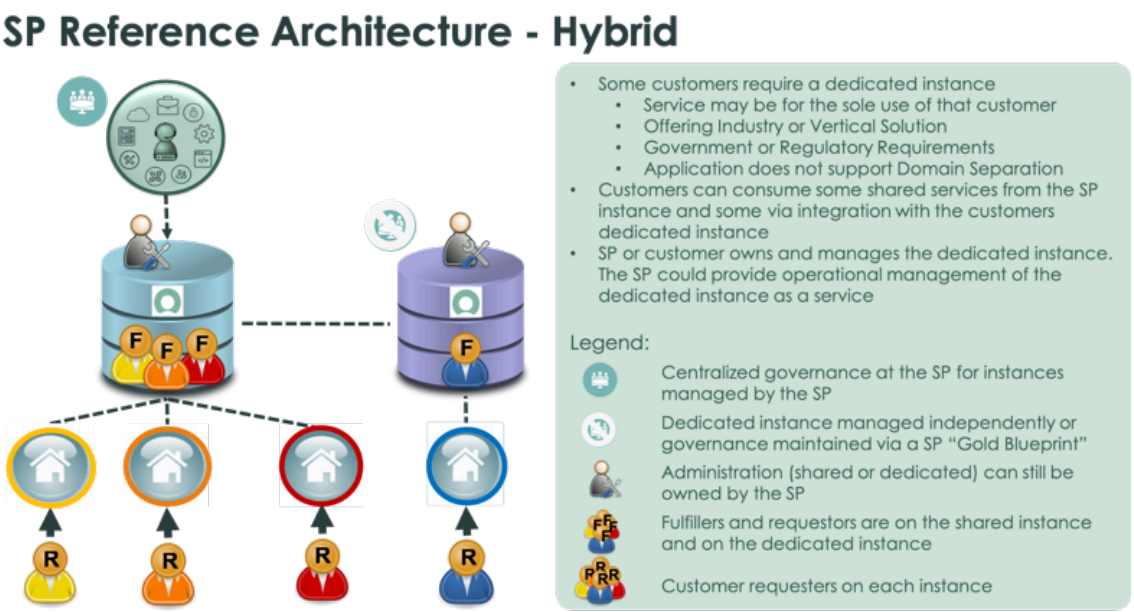
Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside 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 des fournisseurs de services pour l'hybride

Utilisez l'architecture de référence du fournisseur de services (SP) hybride 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 chaque instance requiert une intégration.

Architecture hybride

Votre client peut être responsable de la livraison directe de ce service supplémentaire. Vous devez créer une solution hybride composée 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 les 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 dispose d'un nombre limité de demandeurs et de prestataires. Lorsque vous recevez un nouveau client, vous devez vous procurer une instance basée sur la taille et l'échelle de la société de votre client.

Traduction automatique

servicenow

Comparaison de l'architecture de référence du SP

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.

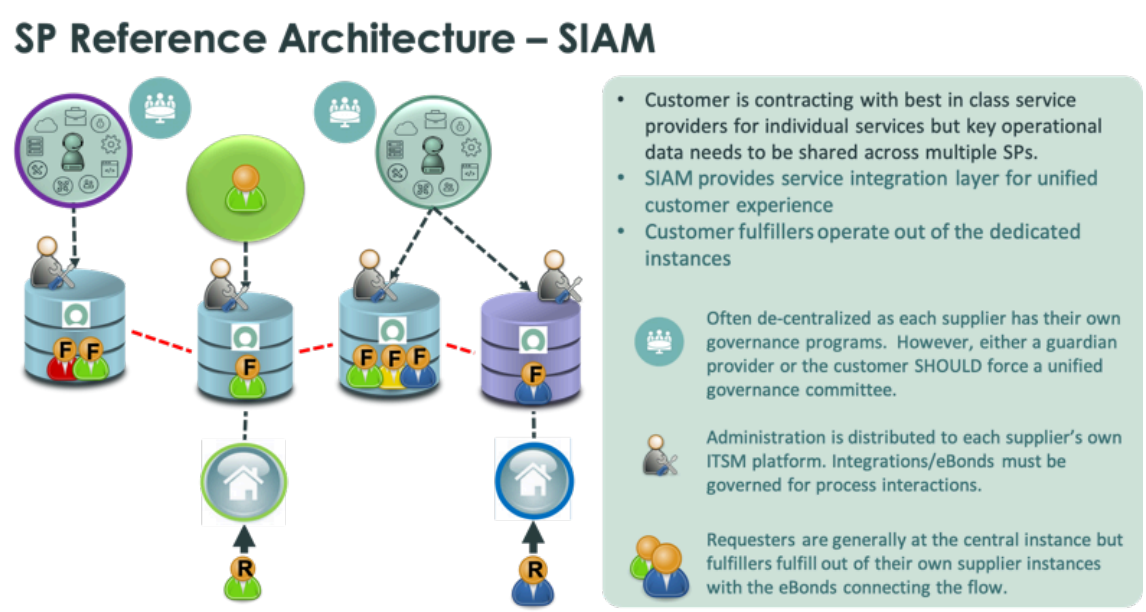
Architecture de référence du fournisseur de services pour Service Integration and Management (SIAM)

L'architecture Service Integration and Management SIAM (Service Integration and Management) pour les fournisseurs de services (SP) intègre les services pour une expérience client unifiée.

Attributs de l'architecture SIAM

- Les clients accèdent aux services SP via un portail dédié ou partagé vers l'instance partagée du SP.
- Les fournisseurs de services utilisent ServiceNow des instances partagées pour gérer leur prestation de services.

L'architecture SIAM en un coup d'œil



Traduction automatique

Comparaison de l'architecture de référence du SP

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.

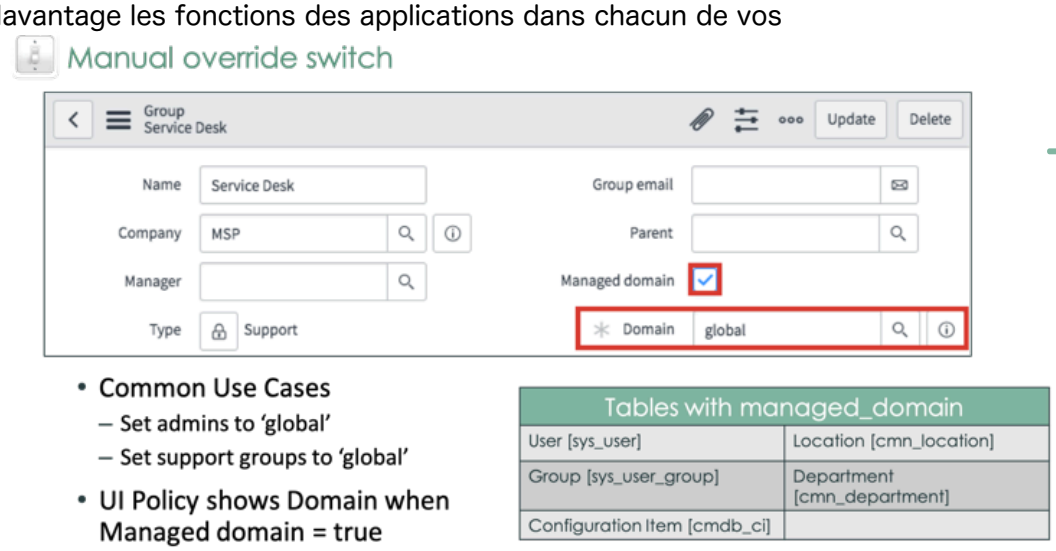
Termes de Domain Separation

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 CI, plutôt que d'utiliser le domaine qui est affecté automatiquement à partir de l'enregistrement de la 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 politiques

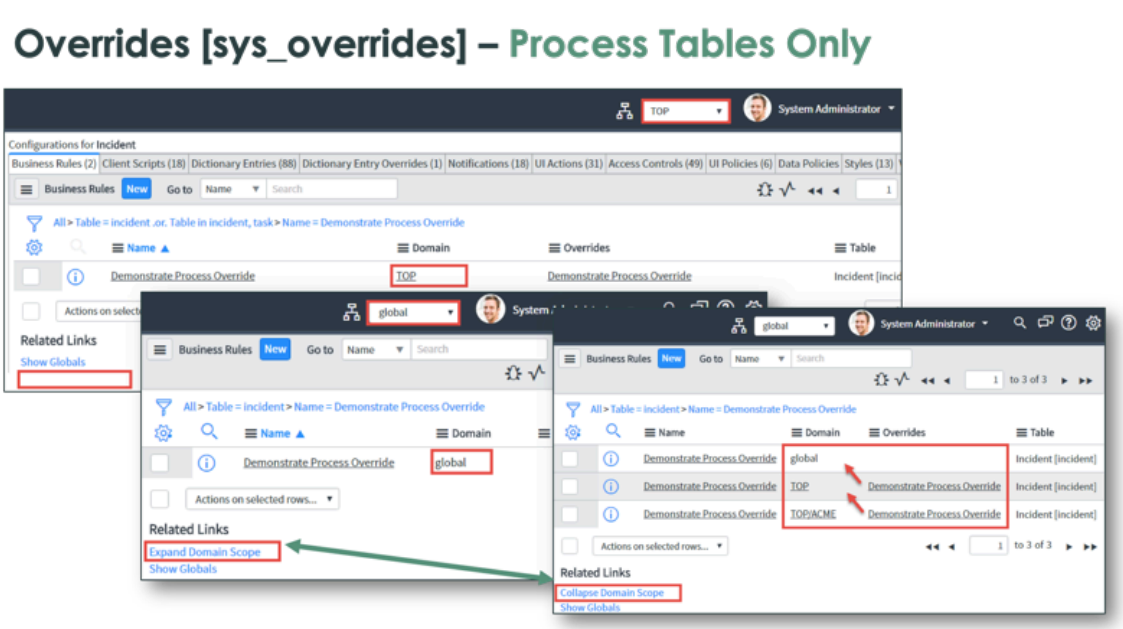
Traduction automatique

spécifiques à un domaine, est en vigueur. Les administrateurs du domaine global peuvent utiliser le lien connexe **Développer/réduire le champ d'application du domaine** pour voir 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 les tables de processus d'un domaine, vous ne voyez que les enregistrements de processus pertinents pour le domaine sélectionné. Lorsque vous affichez une table de processus à partir du domaine global, le lien connexe **Étendre 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 l'application globale, utilisez le lien connexe **Réduire le champ d'application du domaine** .

La fonctionnalité de champ d'application de domaine n'est utilisée que 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 du 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, ainsi que 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 dans l'image suivante est un domaine client.

Domaine du processus

Vous créez des processus définissant la façon dont les données sont utilisées et ce qu'elles font dans le domaine. Ces processus doivent avoir les attributs suivants :

- Processus et paramètres d'interface utilisateur spécifiques pour un ensemble de domaines
- Pas de données 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 de données contient des données pertinentes pour plusieurs clients. Ces données peuvent être partagées sans partager les domaines clients réels. Chaque client dispose de son propre domaine de données et peut y accéder.

Remarque :

Ce type de domaine n'est pas courant et peut entraîner 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 les fournisseurs de services doivent interagir.

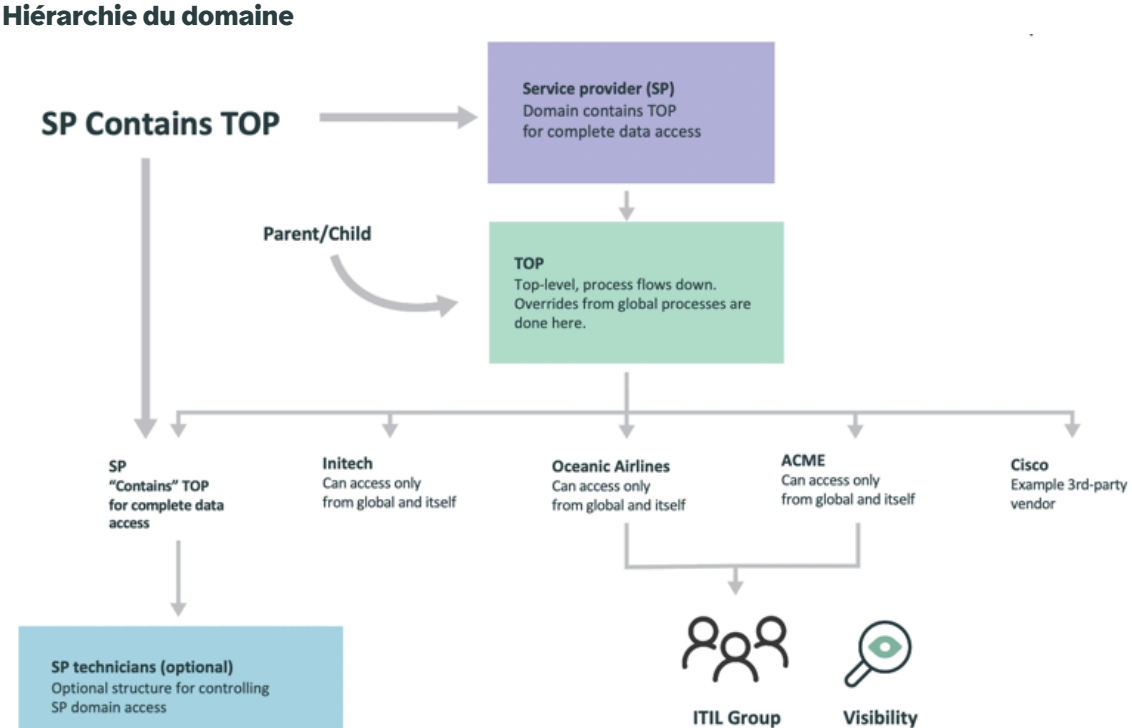
Le domaine par défaut dans l'image suivante est un domaine de données.

Données utilisateur

Les données de l'enregistrement utilisateur n'appartiennent jamais au domaine global ou à l'un des domaines de processus. Les utilisateurs sont principalement créés dans les domaines clients et peuvent parfois être créés dans les domaines de données.

Les comptes d'administrateur sont spéciaux, car ils ne doivent pas être utilisés en tant qu'utilisateurs quotidiens de l'instance et doivent se trouver dans le domaine global pour faciliter les fonctions administratives.

Hiérarchie du domaine



Traduction automatique

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 redirigé vers 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 la création, la modification et la maintenance de tous les 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 domaine gèrent l'administration utilisateur, les appartenances à des groupes de support et les emplacements, ou gèrent les applications conçues avec l'administration des locataires à l'esprit.

Processus/paramètres globaux

Vous pouvez créer et gérer le processus qui affecte 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 et base de données), ACL, sorties d'installation, actions entrantes, pages publiques et intercepteurs.

Séparation de 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 de séparation de 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.

Utilisez ces points comme ligne directrice pour créer un champ sys_domain.

- Créez un nouveau champ en tant que *`domain_id`* type.
  - Nom de colonne : sys_domain
  - Autres attributs : définis automatiquement
- Le Sys_domain_path est créé automatiquement.

La **sys_domain** de nom de colonne est réservée dans le Now Platform, ce qui signifie que le système la reconnaît et applique automatiquement le type de champ et les attributs appropriés pour vous. Cette configuration automatique crée également un champ **sys_domain_path** correspondant.

- Définissez le nom de colonne sur `sys_domain` plutôt que d'utiliser l'étiquette.
- Domain separation 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 laisser celle-ci 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 des règles métier

Le domaine est affecté à l'aide d'une logique scriptée, généralement basée sur le champ Société.

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 affecter 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** modifie le domaine sur tous les enregistrements associés 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 de l'appelant ou du `requested_for` . Cette règle vérifie si vous pouvez définir le domaine de l'enregistrement en fonction du domaine de l'utilisateur. Si ce n'est pas le cas, 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
*/
```

4. Domaine – domaine en cascade – tâche

Les tâches peuvent avoir de nombreuses tables connexes qui fonctionnent ensemble pour atteindre 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 pour les utilisateurs dans le nouveau domaine.

Cette règle de cascade est généralement déclenchée lorsque vous effacez les enregistrements du domaine par défaut.

Les enregistrements connexes pour un domaine en cascade contenu dans le script s'affichent de la même façon que l'exemple ci-dessous :

```
/*
* 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 les thèmes de l'entreprise de vos clients dans les domaines que vous avez configurés. La personnalisation permet à leurs instances de s'adapter à l'apparence générale de leur entreprise.

Personnalisation des thèmes et des logos de l'entreprise

Dans 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 services est installé, les règles métier standard contenues dans les tables de base entraînent la définition du domaine de l'enregistrement sur le domaine de la société qui lui est associée. 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. Vous disposez ainsi de plus d'options de personnalisation.

Gestion de Domain Separation 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, donnant ainsi à vos clients plus de flexibilité.

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 remplacement basé sur le domaine de l'enregistrement joint uniquement, et non sur le domaine entier de l'utilisateur.

Catalogue de services

Le Service Catalog est maintenant séparé par domaine afin que vos clients puissent voir le catalogue et y accéder. Les éléments sont traités en tant que conditions OR lorsque plusieurs éléments sont utilisés. Les fournisseurs de services doivent gérer eux-mêmes les catégories et les éléments afin qu'ils correspondent précisément à leurs propres critères.

Utilisateurs et groupes

Utilisez uniquement des comptes d'administrateur dans le domaine global, car les administrateurs doivent avoir accès à tous les domaines. Effectuez 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 recevoir des comptes d'utilisateur en production s'ils doivent utiliser l'application.

Utilisation des champs

Il y a plusieurs points à prendre en compte lorsque vous travaillez avec des champs. Portez une attention particulière à ces champs, car ils peuvent avoir 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 des processus et qui doivent descendre vers des domaines enfants ont également besoin du champ `sys_domain` .

Configurer Domain Separation 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 laquelle vous pouvez faire un choix.

Si votre session expire et même si vous n'êtes pas déconnecté, votre session revient au domaine de votre enregistrement utilisateur. Vous perdez également tous les rôles élevés en même temps. Dans ce cas, votre sélecteur de domaine peut toujours afficher 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 domaine TOP ou au domaine global

Domain Separation fonctionne mieux lorsque vous fournissez des services à des 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 concerner les propriétés qui fonctionnent automatiquement pour chaque client. Bien que les processus puissent toujours être ajustés selon les besoins, soyez très prudent 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 marge de personnalisation trop importante, et donc des erreurs.

- Approche recommandée pour la configuration :
  - **80 %** ou plus **Standard**
  - **15 %** ou plus **Paramétrique**
  - **Configuration** de moins de **5 %**
- Déterminez si un changement suggéré doit être une propriété globale ou configurable.
- Ne construisez pas trop en ajoutant de plus en plus de personnalisation qui doit être gérée. Procédez plutôt comme suit :
  - Commencez par les fonctionnalités du système de base et vérifiez toutes les lacunes avant d'apporter des modifications.
  - Recherchez des solutions no-code.
  - Utilisez des scripts côté serveur, créez des API modulaires et intégrez des propriétés séparées par domaine.
  - Si vous devez utiliser des scripts clients, utilisez uniquement ServiceNow des API. Limitez les appels « synchrones » (ceux qui vont et viennent du client au serveur, aussi appelés AJAX).
  - Écrivez tous les scripts de manière logique pour qu'ils restent simples et efficaces. Appliquez des examens par les pairs des modifications du code et assurez-vous que tout le monde respecte les instructions Pratiques recommandées de séparation de domaine pour les fournisseurs de services de cette section.

Considérations relatives aux performances de Domain Separation

Lorsque vous configurez Domain Separation dans votre application et vos services, assurez-vous de prendre en compte le nombre et les propriétés des domaines que vous créez. Un trop grand nombre de domaines lourds en propriétés peut avoir un impact sur les performances de votre instance.

Limiter les domaines à propriétés lourdes

Vous pouvez créer autant de domaines que nécessaire, mais assurez-vous de ne pas créer de domaines inutiles sur l'instance. Pondérer un trop grand nombre de domaines sur l'instance avec un grand nombre de propriétés peut avoir un impact sur les performances de votre instance.

Le nombre de domaines n'est pas ce qui a un impact sur les performances, mais plutôt ce qu'ils contiennent. Un trop grand nombre de propriétés peut 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 de la session. Ce processus peut entraîner une panne où vous ne pouvez accéder à aucun élément sur l'instance tant que le sélecteur de domaine n'a 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 Interface utilisateur principale du 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 à la fois, 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 intégrations ou des jeux d'importation sans effectuer d'abord des tests, sinon vous risquez de fermer votre instance.

Configurer 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 des domaines, les utilisateurs ont accès aux données de leur domaine d'origine et de tous les domaines enfants. Le processus s'écoule vers les domaines enfants et les données remontent.

Apportez des modifications à la hiérarchie de domaine existante uniquement si 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 des domaines. Lorsque la hiérarchie des domaines est mise à jour, le système déclenche une mise à jour en cascade sur toutes les tables qui se rapportent aux domaines pour les enregistrements créés sur ce domaine. Par conséquent, un grand nombre de tables de support doivent également être mises 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 indiquent s'il y a des erreurs après la modification de la hiérarchie des domaines.

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 détecter les erreurs et avertissements

Consultez les journaux de domaine pour trouver des erreurs ou des avertissements dans vos processus de chemin de domaine et vos configurations de hiérarchie.

Vous pouvez trouver les journaux de domaine dans la table Journal de domaine [syslog_domain]. Lorsque la hiérarchie des domaines est mise à jour, le système déclenche une tâche planifiée pour recalculer les chemins de domaine. La table Journaux de domaine capture les résultats.

Recherchez les erreurs et avertissements dans cette table. Après avoir examiné cette table, vous devez résoudre ces erreurs et exécuter à nouveau le validateur de chemin de domaine.

Dans cet exemple de journal, le système a détecté dix enregistrements orphelins dans la table sys_ui_list. Les erreurs dans 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 de domaine, reportez-vous à Résoudre les erreurs de Domain Separation.

Importance du domaine par défaut

L'organisation de vos domaines est une étape cruciale du processus de séparation des domaines. Si vous ne définissez pas de domaine par défaut, les nouvelles tâches et les nouveaux enregistrements d'utilisateurs sont transférés vers le domaine global. Tout le monde peut voir les enregistrements dans le domaine global, ce qui signifie que les données peuvent être consultées 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 l'endroit où le système affecte automatiquement les enregistrements de tâche et d'utilisateur qui ne sont pas déjà affectés à un domaine.

Lorsque vous créez un domaine par défaut à partir de l'écran Administration des domaines, ajoutez le nom par défaut dans le champ **Nom** pour le différencier des autres domaines. Cochez la case **Par défaut** pour l'enregistrement.

Conservez 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 chercher la raison. Idéalement, vous devez vous assurer que tous les enregistrements sont créés dans les domaines appropriés (et non dans les domaines globaux ou par défaut).

Contient les 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 les 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 de domaine « contient » ou si vous fournissez un accès large, vous générerez des requêtes avec trop de conditions OR. Les conditions de salle d'opération sont lentes et ont un impact sur les performances de votre instance. Au lieu d'utiliser trop de relations « contains », 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 doivent vraiment y avoir accès. Pesez les avantages et les limites. La requête ci-dessus ne concerne qu'une seule relation 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 OR. Soyez prudent lorsque vous créez une carte de domaine afin de ne pas avoir d'impact sur les performances de votre instance.

Chemins de domaine, méthode de requête

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 SQL et les requêtes lentes peuvent vous aider à résoudre les problèmes de lenteur dans une instance.

Lorsque vous déboguez une instance, vous pouvez activer le débogage SQL pour rechercher les requêtes lentes ou rechercher les requêtes lentes en consultant la table Requêtes lentes [sys_query_pattern] en accédant à **Diagnostics du système > 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 afin de déterminer si des requêtes lentes sont dues au chemin de domaine de 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, consultez Contient les requêtes et l'accès au domaine). Dans la hiérarchie des domaines, placez l'utilisateur ou un domaine à un niveau hiérarchique où le contenu ou la visibilité n'est pas nécessaire.
- La méthode de requête n'est pas la méthode de requête du chemin de domaine (pour plus d'informations, voir Chemins de domaine, méthode de requête) : Si vous n'utilisez pas la méthode de requête du chemin de domaine, contactez Service et assistance client.
- Une requête a besoin d'une base de données pour être indexée afin que vous puissiez voir rapidement ce qui s'y trouve. 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 se passe avec elle.

Règles métier Avant requête

Vous pouvez utiliser une règle métier Avant requête pour aider à prendre en charge la ségrégation des données sur une instance. ServiceNow Les applications qui prennent en charge Domain Separation peuvent prendre en charge la séparation des données et l'acheminement des données uniquement, disposer d'une séparation de logique métier avancée ou prendre en charge l'administration au niveau du locataire (client) de l'application.

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 séparation des données dans les situations suivantes :

- Lorsque Domain Separation n'est prise en charge par aucune ServiceNow application et que vous devez accorder ou restreindre l'accès aux tables ou aux lignes à un ou plusieurs clients non internes en dehors de l'organisation du fournisseur de services.

Remarque :
Avant de commencer le développement, contactez ServiceNow le support client au sujet de la feuille de route de l'application pour ce produit ; des améliorations de la prise en charge du domaine peuvent être prévues pour les versions à venir.

- 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 du domaine X a plusieurs fournisseurs qui prennent 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 parent et enfant 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 être appliquées 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 des domaines, afin que la règle s'exécute uniquement 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 si vous avez désactivé l'option Exécuter les règles métier sur des cartes de transformation, ou si vous avez des scripts dont le workflow est 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 dans un domaine.

Avertissement :
Lors de la conception et du codage de règles métier (en particulier les règles métier Query), limitez les clauses OR et les recherches dans les champs non indexés. Trop de clauses OR 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.

Les règles métier avant requête 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 dans les environnements de fournisseur de services (SP) qui ont accès à plusieurs domaines du système.

Remarque :
Le filtrage des données est transparent (contrairement aux ACL) pour les utilisateurs qui ne voient pas le message « La sécurité des données restreint... » lors de l'interaction avec des données.

Quand ne pas utiliser les règles métier et ACL Avant requête

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'elles ne perturbent pas le système.

Domain Separation assure 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 ServiceNow équipes de la plateforme et de l'application sont responsables de la maintenance du framework, soulageant ainsi le client.

Pour les entreprises comptant de nombreux clients, l'utilisation excessive des requêtes Before et des ACL peut entraîner une dysfonctionnement des requêtes de base de données.

Comment Domain separation est-il activé ?

Vous pouvez activer Domain Separation à l'aide d'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 Domain Separation sont inclus dans ServiceNow les versions. Les propriétaires d'instances peuvent consulter Service et assistance client des ressources, telles que le , à l'adresse pour https://support.servicenow.com obtenir de Portail de servicesl'aide concernant Domain Separation.

Éviter le chemin de domaine dans les scripts

Les chemins de domaine peuvent entraîner la modification, voire l'interruption des valeurs de votre script, par conséquent, ne les utilisez pas dans des scripts.

Votre script ne doit pas dépendre du chemin de domaine, car si vous modifiez la hiérarchie des domaines, le chemin de domaine est recalculé et sa valeur change. Lorsque cela se produit, vos scripts sont inutiles ou peuvent générer des erreurs ou des pannes. 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 des domaines, le chemin de domaine est recalculé et sa valeur change, ce qui peut rendre vos scripts inutiles, générer des erreurs ou s'interrompre. Recherchez les règles métier du système de base, qui utilisent le champ **sys_domain** , pour obtenir des idées 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 de domaines après avoir importé un ensemble de mises à jour pour vous assurer que les valeurs de chemin de domaine de vos enregistrements sont correctes.

Pour en savoir plus sur le chemin de domaine, consultez Demander Domain Separation et Centre Séparation de domaine.

Affectations de domaines

La façon dont vous affectez un domaine influe 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 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

- 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 le crée

Assurez-vous que vos conceptions et stratégies 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 approprié. De cette façon, vous pouvez voir les propriétés de chaque domaine si vous avez besoin de les dupliquer ou de les modifier.

Domain separation et le module d'extension Gestion du service clientèle (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'instances doivent nous contacter Service et assistance client pour activer la *csm_auto_account_domain_generation* propriété.

Remarque :
Cette propriété système de base se trouve dans la table des propriétés système et est disponible une fois que les modules d'extension CSM sont activés.

Fonction de 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'est pas vraie 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.

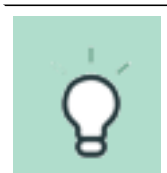
Dans la barre d'en-tête, vous pouvez voir l'état des enregistrements lorsque le module d'extension est activé.

Aide Domain Separation

Assistance supplémentaire avec Domain Separation

Présentation vidéo de Domain separation

Explorer, apprendre, développer



Pratiques recommandées

Trucs et astuces pour créer et développer judicieusement votre structure de domaine

Niveaux de prise en charge par application

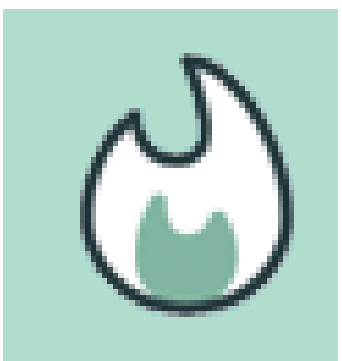
Votre application est-elle prise en charge pour Domain Separation ? Consultez les niveaux de prise en charge et les cas d'utilisation.

Concepts pour les prestataires de services

Concepts qui fonctionnent avec la ServiceNow plateforme pour vous aider à résoudre les cas d'utilisation courants

Classes

- Pour les développeurs : ServiceNow Site développeur Domain Separation
- Pour les fournisseurs de services : Domain Separation pour les fournisseurs de services (connexion ServiceNow University requise)



Safe Workplace Suite et Domain Separation

ServiceNow Les applications Safe Workplace vous aident à rouvrir vos lieux de travail et à prendre en charge la santé et la sécurité de vos employés suite à des crises et à des pandémies telles que la COVID-19. La suite dispose de nombreuses applications pour aider votre organisation à se mobiliser, à récupérer et à se reconstruire.

Configuration et administration

- Mises à niveau
- Demander Domain Separation
- 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 et assistance client
- Poser des questions ou y répondre dans la communauté

Traduction automatique

Administration et configuration de Domain Separation

La configuration de Domain Separation 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.

Pour configurer Domain Separation, procédez comme suit :

1. Demander Domain Separation
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 Administration avancée de Domain Separation la liste des tâches à effectuer après avoir configuré Domain Separation et effectué l'administration de base.

Configuration pouvant être déléguée à des clients internes ou externes

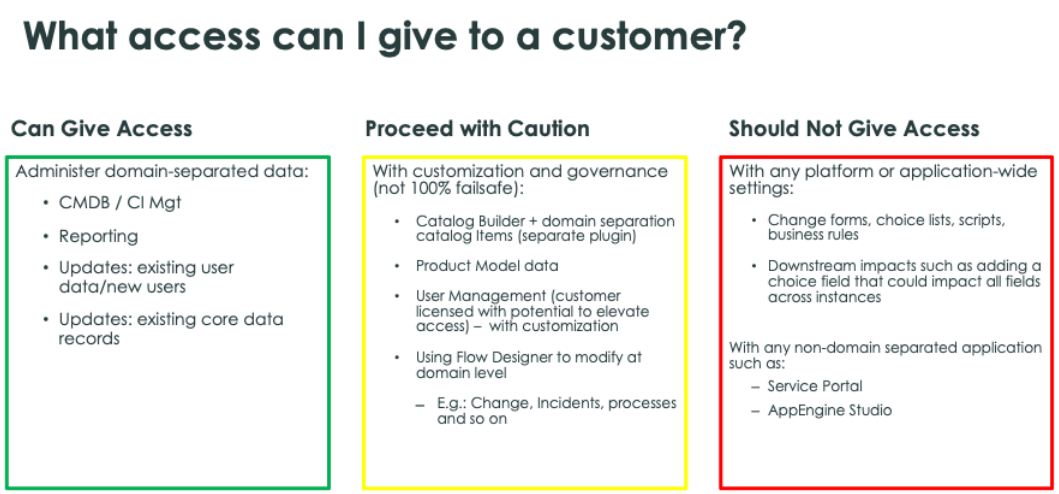
L'application Domain Separation est conçue pour permettre ServiceNow® aux fournisseurs de services de configurer les services qu'ils proposent à leurs clients. Il n'est pas conçu pour permettre à ses clients d'administrer ces services eux-mêmes, à l'exception de quelques domaines détaillés dans cette rubrique.

Vue d'ensemble

Les clients SP peuvent gérer en toute sécurité les données contenues dans leur domaine qui n'ont aucune incidence sur la gestion des licences ou d'autres clients. Par exemple, un client peut créer des rapports ou gérer des éléments de configuration en toute sécurité, mais il ne peut pas le faire en toute sécurité pour personnaliser des champs, des choix, des règles métier et d'autres processus lorsqu'ils peuvent impacter d'autres clients sur la même instance.

Les ServiceNow rôles administratifs 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 créer de nouveaux domaines. Pour toutes les tâches d'administration spécifiques au domaine, les fournisseurs de services doivent créer de nouveaux rôles « administrateur client » et des contrôles d'accès selon les besoins pour accorder un accès spécifique à ses clients.

L'image suivante est une vue d'ensemble des fonctions d'administration courantes dans diverses catégories de ce qu'un client peut faire en toute sécurité.



Autoriser l'accès

Exemples :

- Gestion des données CI dans la CMDB
- Création de rapport
- Mises à jour des données utilisateur existantes ou des nouveaux utilisateurs sans rôles
- Met à jour les enregistrements de données de base existants tels que département, groupe, emplacement, centre de coûts ou les nouveaux groupes sans rôle, ainsi que les nouveaux départements/centres de coûts/emplacements.

Procéder 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 conjointement : Domain separation pour les éléments de catalogue (Domain Separation et Service Catalog) 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 les champs fiables tels que le prix, la description et les images. Le générateur de catalogue (nouveau dans la version Quebec) donne à l'équipe d'administration du 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 : vous pouvez créer en toute sécurité un rôle « administrateur client » qui peut créer et modifier des enregistrements utilisateur, mais l'ajout et la suppression de rôles peuvent affecter la sécurité et la gestion des licences. Le système de base ne permet pas de subdiviser les rôles qu'un client peut accorder en toute sécurité. 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 des rôles doit être contrôlé.
- Flow Designer : ServiceNow Concepteur de flux outil de création utilisé pour créer un processus (workflow) pour les tables. Le rôle flow_designer donne aux clients un accès

sans script aux flux de build. Ils peuvent lire et cloner tous les flux dans les domaines situés au-dessus d'eux dans la hiérarchie. Ils peuvent créer et modifier des flux dans leur domaine. Cependant, cela ne peut pas se faire en vase clos. Toute personne susceptible d'influer sur les processus doit être ajoutée à l'équipe d'administration globale pour la gouvernance afin que les processus ne s'annulent pas les uns les autres ou n'entraînent pas d'autres conflits.

Ne pas donner accès

Il est utile de comprendre le fonctionnement des champs de choix pour comprendre pourquoi seule l'équipe d'administration du SP doit 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 la table, du domaine et de la 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 **d'État** dans toutes les tables, domaines et langues sont considérées comme les valeurs du champ **État** .

- Mode de fonctionnement des modifications apportées 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 tous les ensembles de mises à jour importés ayant une incidence sur ce champ remplaceraient les choix existants. Dans certains cas, les champs de choix peuvent entraîner eux-mêmes des processus, qui ne fonctionneraient pas si un client venait à 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
- Prise en charge de Domain Separation par les applications
- Notes de publication de Domain Separation

Demander Domain Separation

Toutes les fonctionnalités de prise en charge du domaine sont activées à l'aide d'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

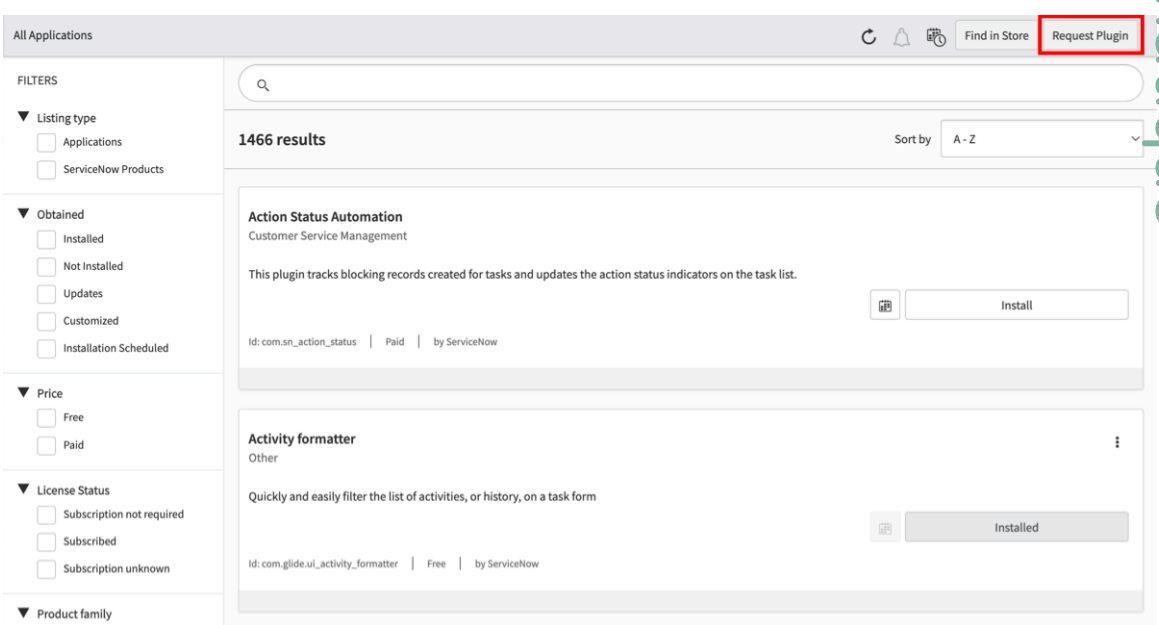
Si le module d'extension Domain Support - Domain Extensions Installer est déjà actif, le contenu du module d'extension Domain Support - Domain Extensions Installer ne sera pas installé pour éviter tout conflit potentiel avec une implémentation existante.

La séparation de domaine remplace la séparation d'entreprise. Le module d'extension Séparation d'entreprise ne peut plus être activé à partir de la version Helsinki. Toutefois, si Company Separation est déjà actif lorsque vous activez Domain Separation, les deux modules d'extension sont actifs en même temps. Vous pouvez contrôler l'état d'activation de la séparation de l'entreprise à l'aide de la `glide.db.separation.field` propriété.

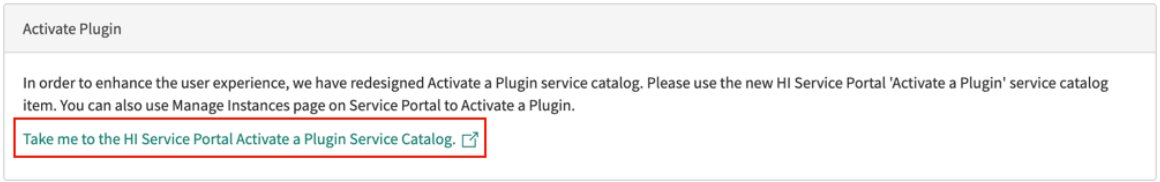
Remarque :
Les chemins de domaine sont utilisés pour tous les clients sur Helsinki et les versions ultérieures. La numérotation de domaine n'est plus utilisée. Service et assistance client peut vous aider dans la mise à niveau.

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.



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.

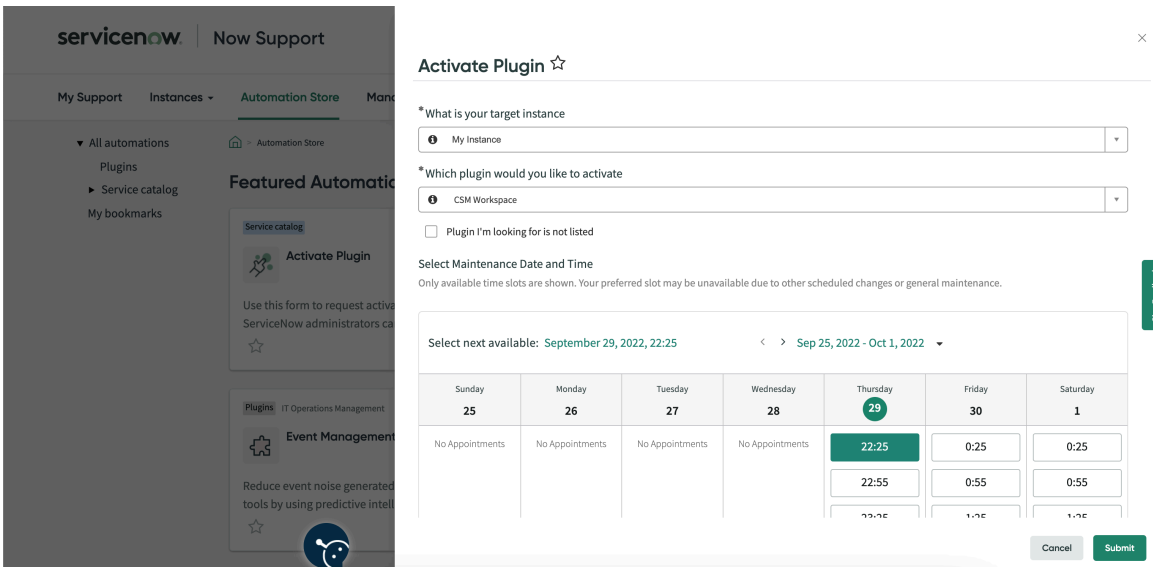
Formulaire Activer le module d'extension

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.

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 Service Catalog [KB0751715] de la Now Support Base de connaissances.

Résultats

L'activation du module d'extension Domain Extension Installer active les fonctionnalités suivantes :

- Domain separation est basée sur la table Domaine [sys_domain].
- L'administration déléguée permet à chaque domaine d'avoir une stratégie 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'utilisation d'un enregistrement d'un domaine différent.

Information associée

Module d'extension Domain Separation

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 Domain Separation.

Pratique recommandée pour l'activation du module d'extension Domain Separation

Dans le cadre du développement de Domain Separation, les administrateurs doivent demander l'activation de ce module d'extension. Pour de meilleurs résultats, activez le module d'extension Domain Separation 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 Domain Extensions Installer (com.glide.domain.msp_extensions.installer) avant d'activer Domain Separation (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, les performances et le processus de votre application sont à risque. Sur les instances établies, en fonction de la façon dont les éléments ont été structurés 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 de domaine, reportez-vous à Exploration de Domain Separation.

Par exemple, lorsque le module d'extension Domain Separation est activé, la colonne **Domaine** (sys_domain) est ajoutée à la table de tâches et tous les enregistrements existants sont automatiquement **placés dans global**. Pour utiliser un script en vue d'affecter tous les enregistrements dans les domaines appropriés, une hiérarchie parent/enfant établie est requise. Ces types d'actions scriptées risquent d'entraîner la corruption ou la perte de données, ainsi que des temps d'arrêt de la production lorsque de grandes quantités de données sont déplacées. Une grande partie du code de la plate-forme est également placée dans **des règles globales**, telles que des règles métier, des scripts clients, des vues de formulaire et des workflows.

Si un client crée du code ou modifie du code, il existe un risque pour les performances et la convivialité de ServiceNow la plateforme. Avec ce type d'approche, les propriétaires d'instances pourraient retarder considérablement leur implémentation ou subir de longs temps d'arrêt.

Fonctionnalités du module d'extension Domain Separation

Ces fonctionnalités sont activées lorsque vous activez le module d'extension :

- Domain separation est basée sur la table Domaine [sys_domain].
- L'administration déléguée permet à chaque domaine d'avoir une stratégie 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'utilisation d'un enregistrement d'un domaine différent.

Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

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 Domain Separation limitent automatiquement le champ d'application du domaine au domaine de l'enregistrement pour toutes les données ou tous les processus associés. Lorsque l'utilisateur affiche un enregistrement dans un formulaire, les données connexes de l'enregistrement (telles que le sélecteur de référence et les données de 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. Si plusieurs onglets contiennent des enregistrements, chaque onglet possède 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 actuelle 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* : true dans les nouvelles activations de domaine 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 propriété ou la `glide.sys.domain.use_record_domain_for_processesglide.sys.domain.use_record_domain_for_` propriété est définie sur **true**, les propriétés suivantes ne sont pas utilisées, quelle que soit leur valeur :

- `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`

Pour obtenir la liste complète des propriétés, reportez-vous à la section Propriétés système disponibles .

Remarque :

Dans les nouvelles activations de Domain Separation 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 true 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 pour les règles métier exécutées sur la table de domaine. Dans les nouvelles activations de Domain Separation, la propriété par défaut est true et les règles métier sont déterminées par le domaine de session. Dans les implémentations existantes, la propriété par défaut est false et les règles métier sont déterminées par la hiérarchie du domaine nouvellement créé. • *Type* : vrai | faux • *Valeur par défaut* : true dans les nouvelles activations de domaine à partir de Jakarta. False dans les implémentations existantes.
glide.sys.domain.skip_non_global_businessrule_if_nodomain	Garantit que seules les règles bus.rules du domaine global sont exécutées lors de l'utilisation de queryNoDomain() ou lorsque la table n'est pas séparée par domaine, de sorte que vous pouvez ignorer toute autre règle métier • *Type* : vrai | faux • Définir la propriété sur false 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 :

Préférences utilisateur pour le 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 false, le champ d'application par défaut

Préférences utilisateur pour le champ d'application de domaine (suite)

Préférence	Catégorie	Mis à jour par	Détails
			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 [domain].

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 (consultez la table).
4. Cliquez sur **Envoyer**.

Champs du formulaire Domaine

Champ	Description
Nom	Saisissez un nom unique pour le domaine.

Champ	Description
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 de la hiérarchie. Le domaine de niveau supérieur n'a que des domaines enfants et aucun domaine parent.
Par défaut	Sélectionnez si ce domaine doit être le domaine par défaut pour votre hiérarchie.
Parent	Sélectionnez le nom du domaine supérieur dans la hiérarchie qui contient ce domaine. Ce champ doit avoir une valeur pour que le domaine apparaisse dans la carte de domaine.
Actif	Cochez la case pour rendre le domaine disponible pour 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 des domaines, accédez à la liste connexe Contient les domaines et sélectionnez les enregistrements de domaine qui sont les domaines enfants (contenus) de la relation contient.

Utiliser par défaut un domaine

Domaine défini comme 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 définir comme domaine par défaut, par exemple, Principal.
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**.

Gérer manuellement le domaine pour des enregistrements particuliers

Par défaut, le système affecte automatiquement un domaine en fonction de l'enregistrement de société de l'utilisateur. Dans certains cas, cependant, les

administrateurs de domaine souhaitent gérer manuellement le domaine auquel 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 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 du 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 de 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 par 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 des noms de colonnes afin de rechercher certaines propriétés ou attributs qui sont inclus dans vos tables. Deux types de tables s'affichent dans la liste :

- Tables qui ont 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 Domain *`domain_master`* separation à partir d'un 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 taper « 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 dans la visionneuse de remplacement de domaine affiche une liste des tables contenant des remplacements d'enregistrement, ainsi qu'un nombre de 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.

La sélection **de la vue Remplacements entraîne** la création d'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 des remplacements sont répertoriées.

Pour en savoir plus, consultez Créer des remplacements de propriété séparés par domaine .

Activer ou désactiver un domaine

Lorsque vous activez ou désactivez un domaine, l'état d'activation se répercute sur les sociétés du domaine.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Lorsque vous activez un enregistrement de société, Domain separation active automatiquement le domaine associé de 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. Décochez ou sélectionnez la case **Active** .
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 nouveau champ** , entrez 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 **de 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**, vous évitant ainsi quelques clics.

L'ajout de domaines aux tables du système de base nécessite des tests approfondis, des mises à jour et l'ajout d'une nouvelle logique prohibitifs. 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 primaire. En outre, chaque domaine de la carte de domaine doit répondre aux critères suivants :

- Le champ **Parent** doit être renseigné (le domaine primaire 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 primaire indique le domaine de niveau supérieur sur la carte de domaine.

Avant de commencer

Rôle requis : admin

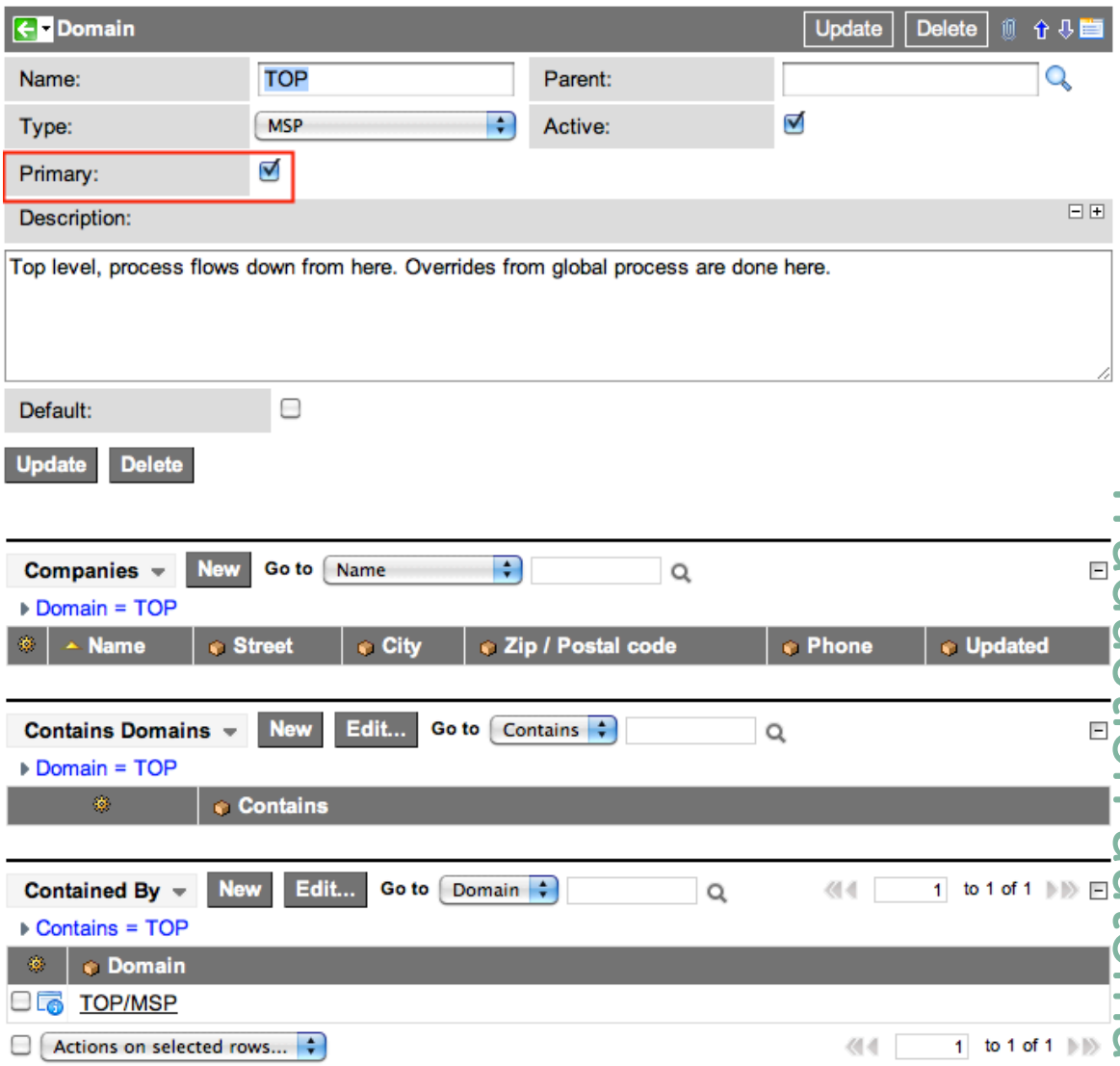
Pourquoi et quand exécuter cette tâche

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 primaire, il remplace le domaine primaire précédent.

Procédure

1. Accédez à la **Tous** > **Administrateur de domaine** > **Domaines**.
2. Sélectionnez le domaine que vous voulez utiliser comme domaine principal, par exemple, TOP.
3. Sélectionnez la case à cocher **Primaire** .

4. Cliquez sur **Mettre à jour**.



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

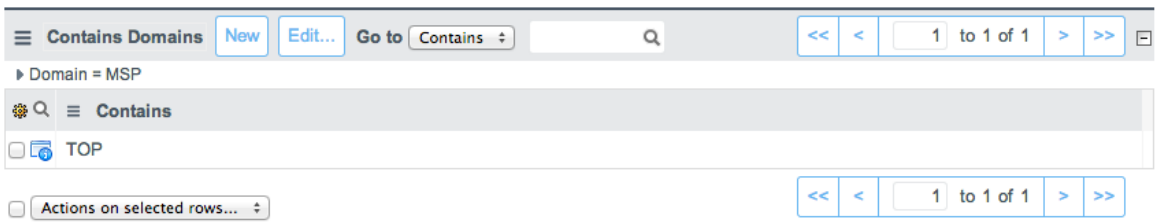
Pourquoi et quand exécuter cette tâche

Les domaines d'une relation contient héritent des paramètres du domaine conteneur. Le domaine conteneur 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 contient.

Procédure

1. Accédez à la table de domaine.
2. Sélectionnez l'enregistrement de domaine qui est le domaine parent (conteneur) de la nouvelle relation contient.

3. Basculez le champ d'application de domaine pour basculer entre le champ d'application de session et le champ d'application d'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 contient. Seuls les domaines enfants apparaissent par défaut lorsque le sélecteur de domaine est défini sur Global. Basculez le champ d'application de domaine pour afficher 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 ne voit que 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 **vrai**.
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 les enregistrements d'un autre domaine, quelle que soit l'appartenance normale de l'utilisateur ou du groupe au domaine.

Avant de commencer

Rôle requis : admin

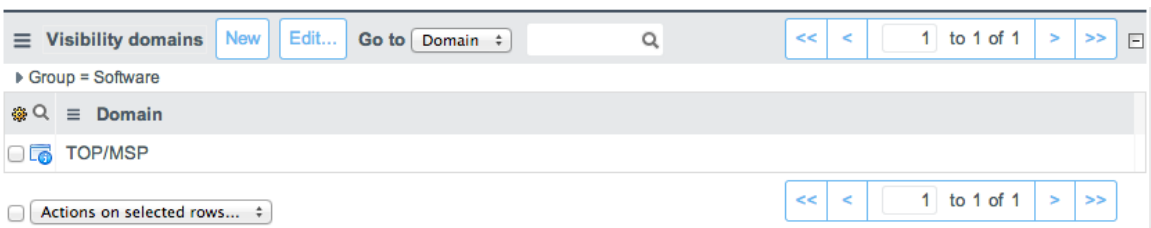
Pourquoi et quand exécuter cette tâche

Il est préférable d'affecter 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 règle de contrôle d'accès d'une table ou d'un enregistrement.

Procédure

1. Accédez à la table des groupes.
2. Sélectionnez le groupe auquel vous souhaitez attribuer 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

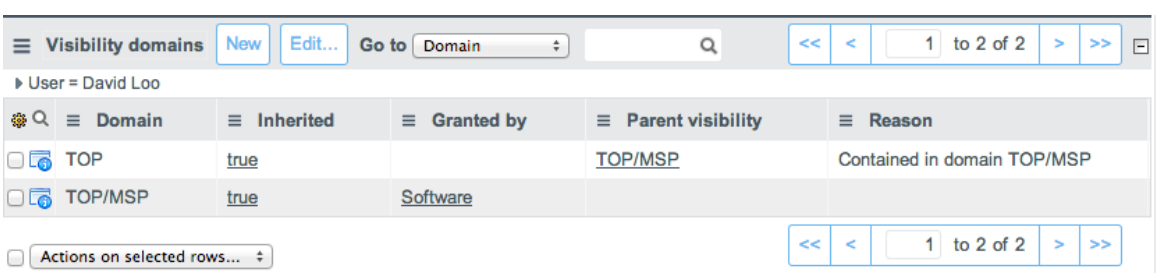
Bien qu'il soit possible d'ajouter des domaines de visibilité pour des utilisateurs spécifiques sur le formulaire Utilisateur, il est préférable de les ajouter uniquement via des groupes. Cela permet de contrôler les autorisations et l'accès au cas où les personnes changeraient de service ou quitteraient l'entreprise.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Utilisateur**.
2. Sélectionnez l'utilisateur pour qui vous souhaitez attribuer 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 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 du domaine ou d'un domaine parent.

Champ	Description
Accordé par	Nom du groupe qui a accordé la visibilité du domaine.
Visibilité du parent	Nom du domaine parent et utilisé pour le regroupement des enregistrements. Si l'enregistrement parent est supprimé, tous les enregistrements ayant le même parent le sont également.

Créer une liste de choix spécifique au domaine

Les administrateurs peuvent configurer des listes de choix pour 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 dans lequel 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. Poussez 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 en tant que choix actif.

Administration avancée de Domain Separation

Les administrateurs peuvent afficher des informations sur Domain Separation, 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 offre 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 fonctionnalité de saisie semi-automatique et de suggestion automatique. Utilisez ce format pour les listes plus longues.

L'emplacement de ces sélecteurs et la procédure pour les afficher ou les masquer diffèrent en fonction de la version de l'interface utilisateur.

Activer les menus de sélection de domaine dans Interface utilisateur principale

L'affichage du sélecteur de domaine dans active le sélecteur de domaine par Interface utilisateur principale 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 :
Domain Separation (module d'extension com.snc.pa.domain_support) est nécessaire pour activer le sélecteur de référence de domaine.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Procédure

1. Cliquez sur l'icône d'engrenage dans l'en-tête.
2. Dans l'onglet Général, cliquez sur le bouton **Afficher le sélecteur de domaine dans l'en-tête** .
   Le sélecteur de domaine apparaît dans Interface utilisateur principale l'en-tête.
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 en regard 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 elle n'est pas déjà présente, ajoutez la propriété `glide.ui.domain_reference_picker.enabled` et définissez sa valeur sur **vrai**.
   c. Actualisez le navigateur.
   Le sélecteur de référence de domaine apparaît dans Interface utilisateur principale l'en-tête.

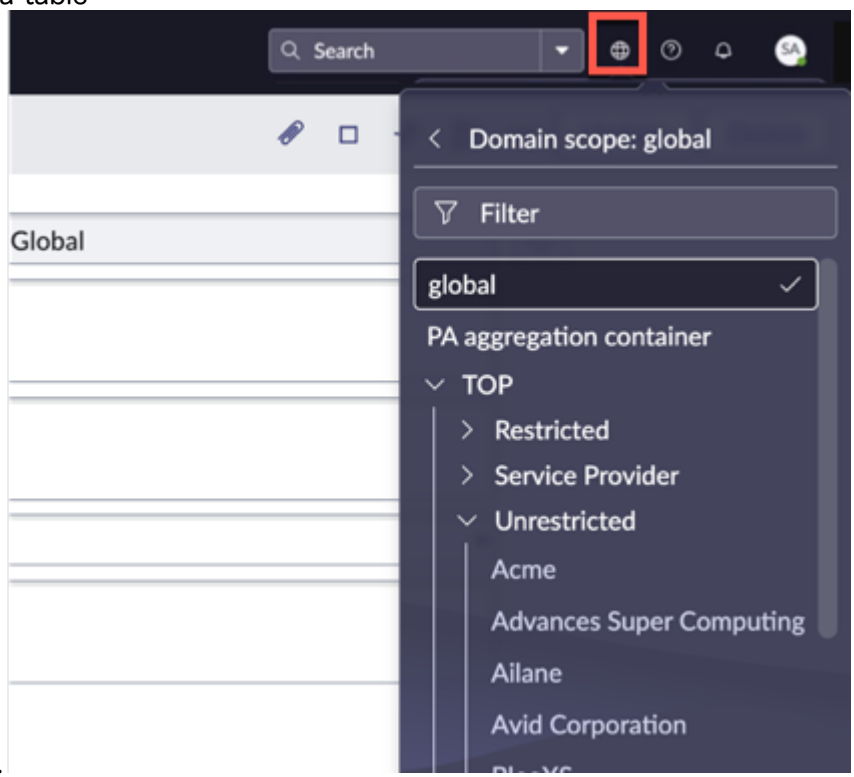
Limiter l'accès au sélecteur de domaine

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 restreindre le rôle aux administrateurs uniquement.

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 : **admin, itil**. Pour en savoir plus, reportez-vous à la section Configurer les sélecteurs Next Experience

Propriétés de l'application Domain Separation

Le module d'extension Domain Separation dispose de deux nouvelles tables pour donner aux fournisseurs de services plus de flexibilité dans la personnalisation de leurs applications qui utilisent Domain Separation. Il s'agit de la table Propriétés d'application système [sys_application_property] et de la table Valeur de propriété d'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 Domain Separation.

Chaque client SP peut souhaiter personnaliser ses applications différemment. Auparavant, les fonctionnalités pouvant être personnalisées n'étaient définies que par 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 à chaque fois que vous souhaitez ajouter ou modifier la fonctionnalité.

Fonctionnement des remplacements dans les nouvelles tables

Les développeurs utilisent généralement la ServiceNow table Propriétés système [sys_properties] pour créer diverses fonctions dans les applications. Si vous vouliez développer une application pour qu'elle se comporte différemment dans différents domaines, vous devriez la personnaliser vous-même.

Dans la version Paris, la nouvelle table Propriétés de l'application [sys_application_property] simplifie cette personnalisation. Au lieu d'aller directement à la table des propriétés système pour une valeur, la table des propriétés de l'application va d'abord à la table d'application système. Cette nouvelle table stocke maintenant 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 Domain Separation, 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 à la table de configuration des propriétés qui peuvent remplacer les propriétés que vous sélectionnez dans la table Propriétés système.

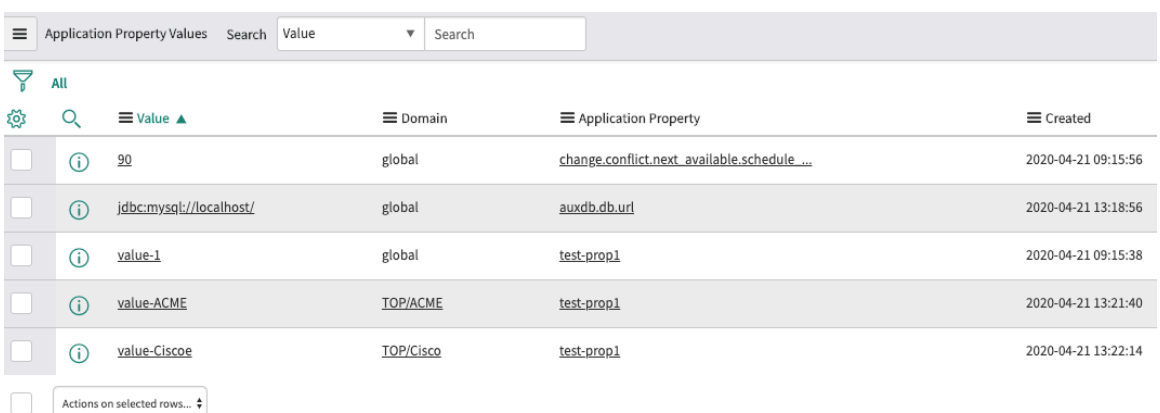
Par exemple, supposons que vous souhaitiez configurer une application avec une fonctionnalité Premier jour de la semaine. Parfois, vous voudrez peut-être que le premier jour de la semaine soit le dimanche. Dans d'autres cas, vous souhaiterez peut-être que le premier jour de la semaine soit le lundi. Dans la table du système de base, il se peut qu'il n'y ait qu'une seule option Jour 1, qui est le dimanche. Avec la nouvelle table, vous pouvez stocker une autre propriété, ce qui fait que le jour 1, le dimanche, et un domaine enfant, le lundi.

Cette figure montre comment le système dessine les propriétés à partir de la table Propriétés d'application avant d'accéder à la table Propriétés système [sys_properties].

Mode de 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 la 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 une incidence sur votre configuration. Le champ d'application peut déterminer quel Jour 1 est défini comme le dimanche et lequel est le lundi. Vous pouvez utiliser la même propriété, mais la personnaliser de sorte que Jour 1, Dimanche soit le domaine parent et Jour 1, Lundi soit le domaine enfant. Dans la nouvelle table, il existe à la fois une colonne de domaine et une colonne de champ d'application, ce qui vous permet de définir ces propriétés pour chacune d'elles.

Vous pouvez utiliser la vue Étendre 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 d'application

La nouvelle table Propriétés d'application système [sys_application_property] contient les champs suivants :

- nom
- description
- type (choix de la chaîne, vrai|faux, 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 d'application système [sys_application_property_value] contient les champs suivants :

- sys_application_property (réf. à sys_application_property)
- sys_domain
- sys_overrides
- valeur
- 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 incluses dans le périmètre. Consultez GlideApplicationProperty - Scoped, 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 Now Platform options. Bien que le module d'extension Domain Separation 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 Domain Migration Tool avant de pouvoir l'utiliser.

L'outil de migration de domaine s'exécute uniquement si la séparation des données et des processus est activée dans l'instance séparée par domaine :

- La `glide.sys.domain.partitioning` propriété de données doit être définie sur **vrai**.
- La `glide.sys.domain.delegated_administration` propriété du processus doit être définie sur **vrai**.

Fonctionnalités 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 (le cas échéant).

- Réduit les données de processus ou, s'il n'est pas possible de les réduire, supprime les données de processus
- Conserve les enregistrements de processus visibles par le domaine cible
- Met à jour les tables spéciales sys_choice, sys_ui_list et sys_ui_related_list
- Nettoie les enregistrements ajoutés par les modules d'extension Domain Separation :
  - Règles métier
  - Actions d'interface utilisateur
  - Travaux planifiés
  - Sorties d'installation
  - Modules de navigation
- Désactive Domain Separation et supprime les domaines de l'instance clonée :
  - Définit ces propriétés sur **false** 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 supplémentaires spécifiés.
- 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. Les tables ont un calendrier de migration, mais la migration n'a pas encore démarré.
Échec	Défaillance au niveau de la table. Si le processus de migration est terminé 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	L'état des tables qui ont migré avec succès.
Terminé avec succès	Le processus de migration s'est terminé 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
  - Consigne chaque table de processus et les enregistrements du domaine en cours d'inactivation ou de suppression.

Ce que l'outil de migration ne fait pas

- Cloner l'instance
- Créer une autre instance séparée par domaine
- Migrez 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 de l'instance source
- Supprimer les données globales, dans le domaine cible ou dans des domaines de données supplémentaires (le cas échéant)

Procédure à suivre après l'exécution de 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 qu'elles fonctionnent pour votre instance dédiée. Par exemple, si vous aviez une règle métier qui définissait le champ de domaine sur les enregistrements, vous souhaiterez peut-être désactiver cette règle métier, car elle n'a plus d'utilité.

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 : security_admin et admin

Procédure

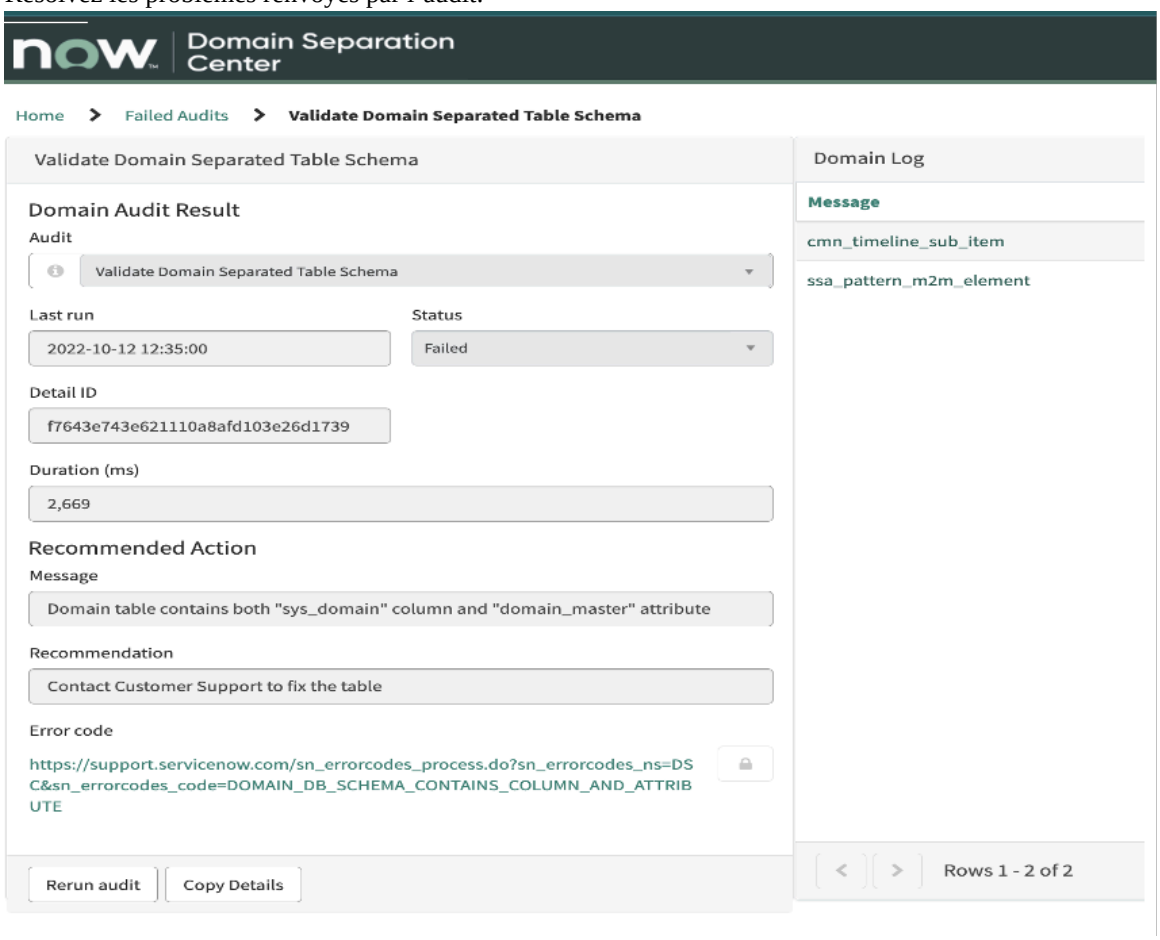
1. Élever au rôle de security_admin.
   Consultez Élever à un rôle privilégié pour en savoir plus.
2. Accédez à la **Tous** > **Administrateur de domaine** > **Outil de migration de domaine**.
   Accès également avec **domain_migration_tool_status.list**.
3. Cliquez sur **Nouveau**.
4. Complétez le formulaire.

Champ	Description
Domaine cible	Spécifiez le domaine utilisé pour le processus et les données que vous souhaitez migrer. Seul le domaine cible est conservé, 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 **Envoyer**.
6. Ouvrez le formulaire que vous venez d'envoyer.
7. Accédez à la **Tous** > **Centre Séparation de domaine** > **Configurer des audits** .
   Consultez Centre Séparation de domaine pour plus d'informations.
8. Définissez l'audit **Valider le schéma de table séparée par domaine** sur **Actif** et affectez un calendrier.

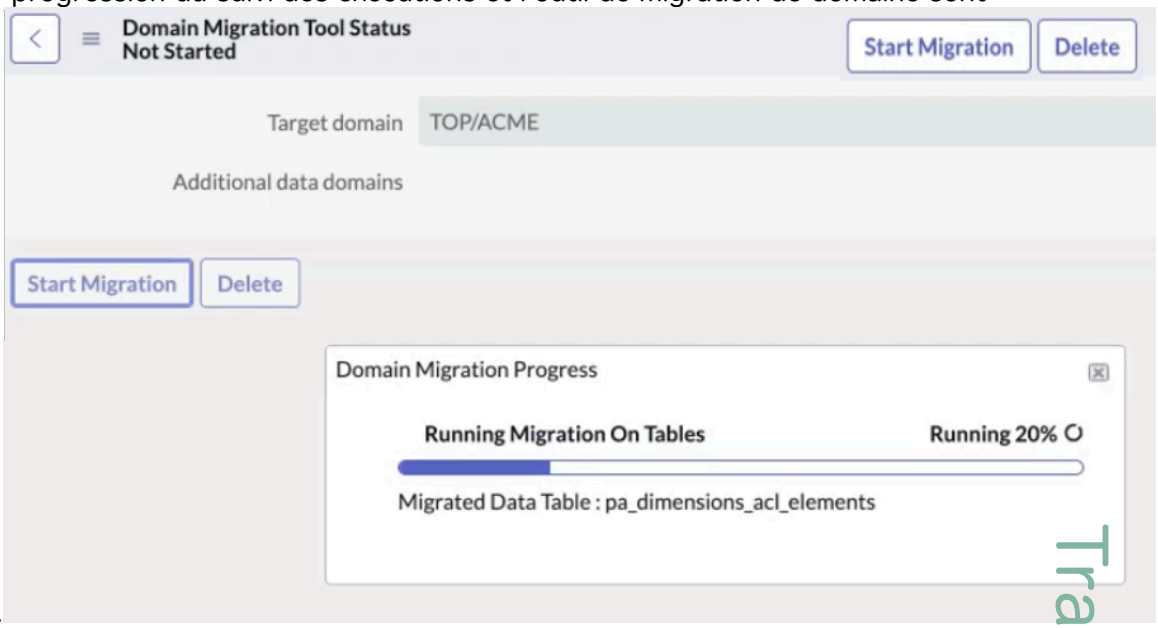
Il s’agit d’un audit de domaine de précaution visant à prévérifier l’intégrité du schéma des tables séparées par domaine. Cela vous permet de corriger les erreurs avant d’exécuter la migration.

9. **Exécutez le calendrier d’audit** qui inclut le schéma.
   Consultez Exécuter les audits immédiatement pour en savoir plus.
10. Résolvez les problèmes renvoyés par l’audit.



11. Sélectionnez **Démarrer la migration**.

- La barre de progression du suivi des exécutions et l'outil de migration de domaine sont déclenchés.



- La table de migration en cours de progression actuelle s'affiche avec le pourcentage total de tables migrées avec succès.
- Table où 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 remplit 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 `de sys_execution_tracker` et recherchez **Migration en cours d'exécution sur les tables** pour vérifier si 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

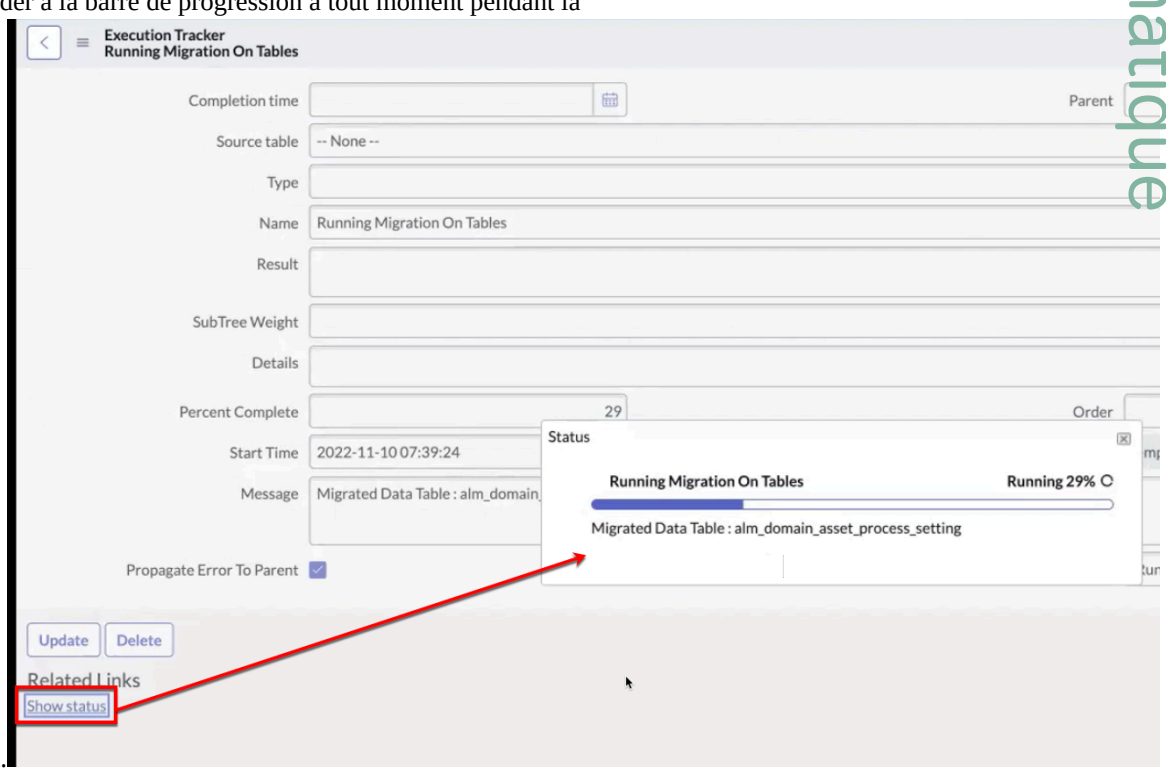
Champ	Description
Statut	Affiche l'état de la migration. ○ **Migration des tables de données...** : état En cours. ○ **Migration réussie** : statut mis à jour après une migration réussie. ○ **Une mauvaise configuration est observée sur l'une des tables séparées par domaine** : Indique un échec de la migration des données. Une erreur de schéma a été trouvée, la migration ne démarre pas. Exécuter l'audit **Validez le schéma de table séparée par domaine**. L'audit échouera et affichera les tables qui ne respectent pas la norme de schéma. ○ **Terminé avec des erreurs dans les tables de revisite** : le nombre de tables pour traiter la migration de schéma est répertorié. Localisez les échecs dans le nombre de tables de revisite et résolvez les problèmes de schéma.

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	Le domaine cible sélectionné pour la migration.
Domaines de données supplémentaires	Se remplit si plusieurs domaines de migration ont été sélectionnés.
Nombre des tables de revisite	Ce champ n'est rempli que si la migration d'une table échoue. S'il n'y a pas d'échecs, 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 actuellement migrée. Une fois la migration réussie, ce champ sera vide.

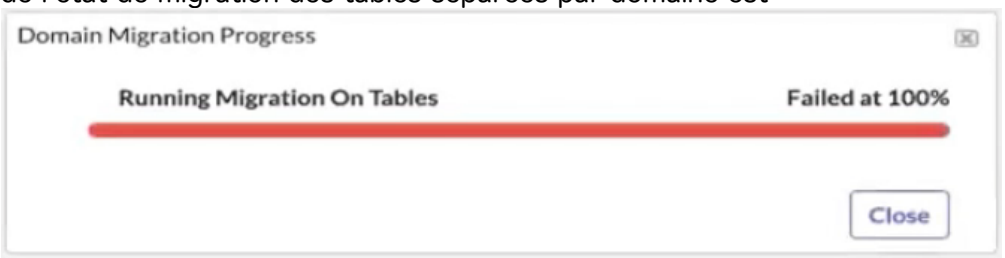
12. Sélectionnez le lien **Cliquez ici** sur la page État de l'outil de migration de domaine pour ouvrir le suivi des exécutions.

Vous pouvez également accéder à la table *sys_execution_tracker* et rechercher **Migration en cours d'exécution sur les tables** pour vérifier si le processus de migration s'exécute en arrière-plan.

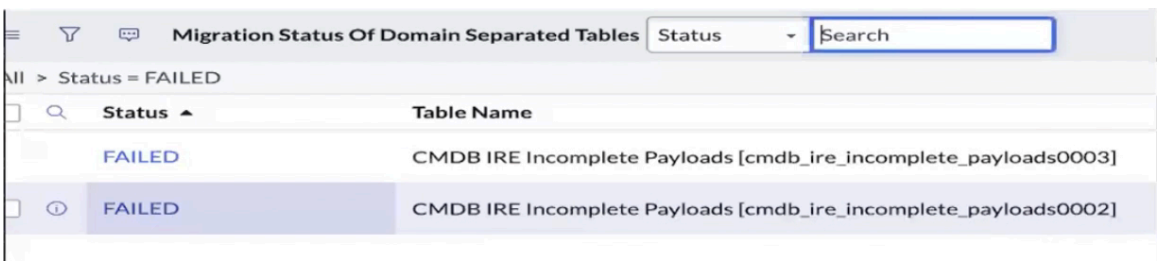
13. Sélectionnez **Afficher l'état** dans la section Liens connexes pour accéder à la barre de progression à tout moment pendant la migration.



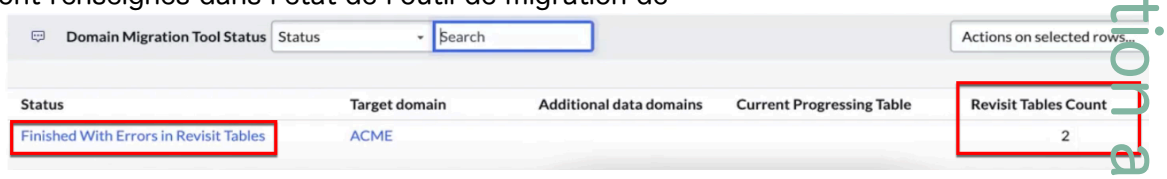
Dans le cas où une table a échoué à la vérification du schéma, l'état global de l'état de migration des tables séparées par domaine est **Échec**.



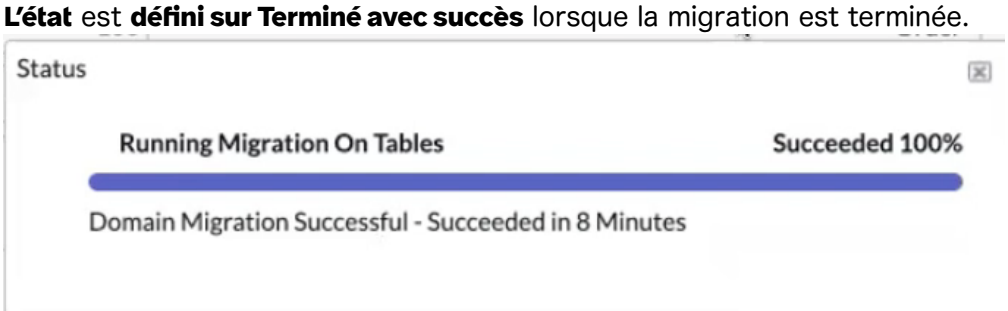
Il y aura **des entrées d'échec** pour chaque table correspondante.



Le reste de la migration se poursuit et un résumé de toutes les tables ayant échoué ainsi que le nombre total de **tables de revisite** sont renseignés 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 au domaine.

Les politiques définies en bas dans la hiérarchie des domaines remplacent les politiques définies en haut dans la hiérarchie des domaines. Lorsqu'ils se trouvent dans un domaine, les administrateurs peuvent définir des versions spécifiques au domaine de ces stratégies et paramètres globaux :

- Scripts clients
- Politiques système
- Noms des applications et des modules

- Rôles d'application
- Filtres de module

> **⚠ Avertissement :**
> Tous les utilisateurs dotés du rôle administrateur ont un accès spécial à l'ensemble des 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 disponibles, quel que soit le domaine affecté. Ils peuvent entrer un domaine spécifique, puis seules les politiques de ce domaine ou d'un domaine supérieur 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. Cela ne modifie pas la politique, l'application ou l'enregistrement de module d'origine. 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 politique. Cette approche crée l'enregistrement de politique dans votre domaine qui remplace l'enregistrement de politique de niveau supérieur d'origine.

Ne modifiez pas la politique de niveau supérieur, puis le champ **Domaine** de cette politique. Cette approche ne crée pas d'enregistrement de politique dans votre domaine de niveau inférieur et ne conserve pas non plus 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 qui appartient à un autre domaine supérieur 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 **de sys_overrides** est défini pour indiquer la politique, l'application ou le module de niveau supérieur qui est remplacé. Plus tard, 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. Si aucune politique n'est trouvée dans le domaine de l'enregistrement, l'administration déléguée recherche les politiques au niveau immédiatement supérieur de la hiérarchie de domaines. La recherche de politiques de domaine se poursuit dans la hiérarchie des domaines jusqu'à atteindre le domaine global. S'il n'existe aucune politique de domaine inférieure 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 d'Acme : Atlanta, d'Acme : San Diego et d'Acme : NY. Lorsque cet utilisateur ouvre un enregistrement dans le domaine ACME : San Diego, l'administration des processus vérifie d'abord les politiques dans le domaine ACME : San Diego. S'il n'existe aucune politique à ce niveau

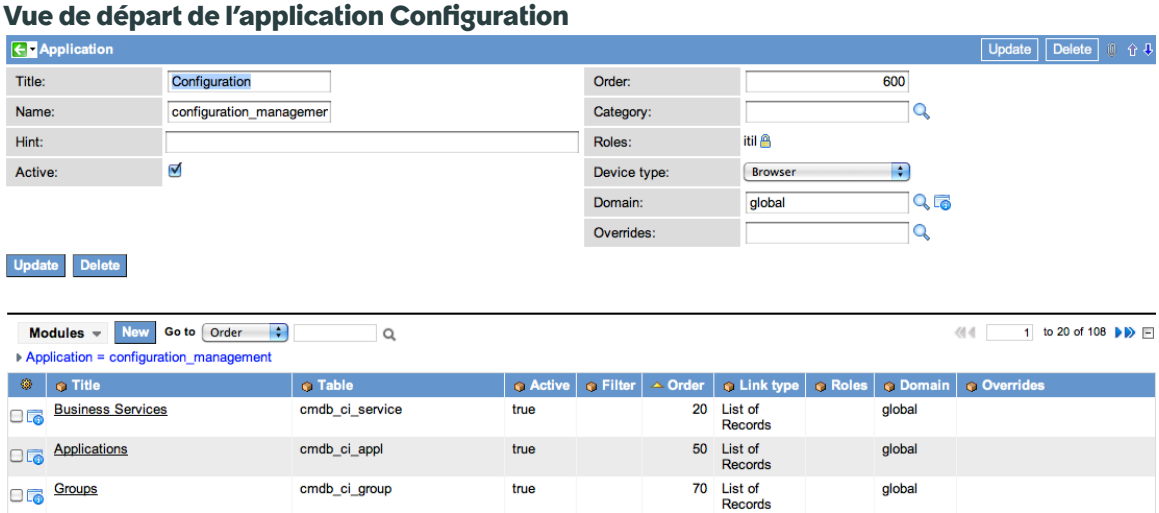
de la hiérarchie des domaines, l'administration des processus recherche les politiques du domaine ACME. S'il n'y a pas de politiques dans le domaine ACME, l'administration des processus utilise les politiques de domaine globales, car il n'y a pas d'autres domaines supérieurs dans la hiérarchie de domaines.

Exemple d'administration de processus avec des applications spécifiques à un domaine

L'exemple suivant illustre l'administration des processus avec des applications et des modules spécifiques au domaine.

En tant qu'administrateur du domaine Oceanic, David Loo décide de personnaliser l'application Configuration. Pour commencer, David passe en revue les modules disponibles dans le module d'application Configuration.

Vue de départ de l'application Configuration



David décide de renommer l'application de configuration en CMDB et d'autoriser le rôle inventory_admin à voir l'application.

Exemples de modifications spécifiques à un domaine de l'application 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 modifier 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 modifications spécifiques à un domaine pour le module État Ouvert - « Nouveau »

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:

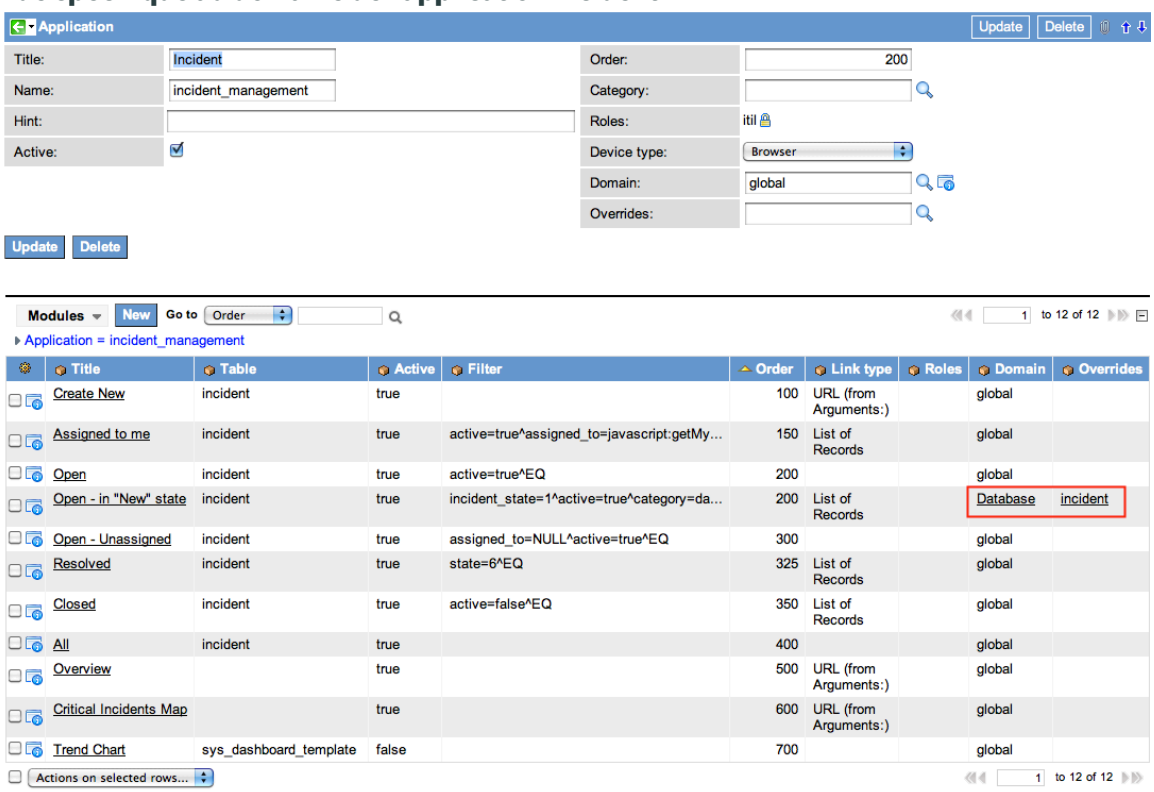
```
incident_state=1^active=true
```

Update | Delete

Traduction automatique

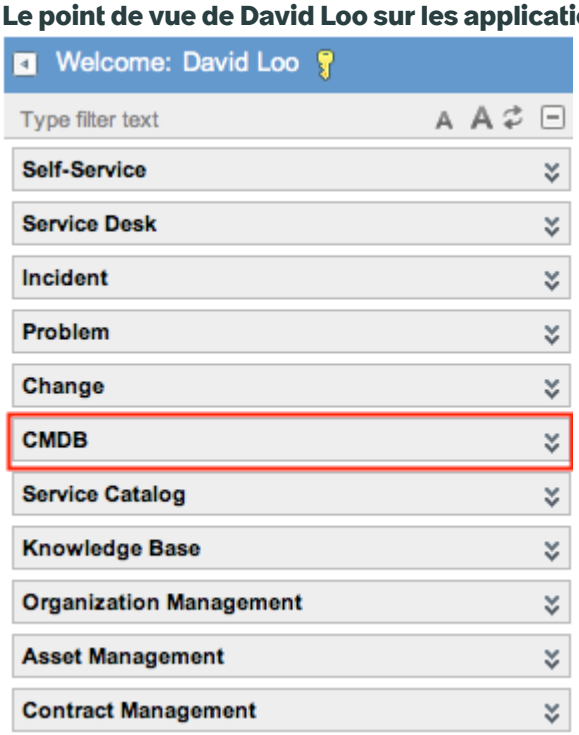
Cela crée une nouvelle entrée de module dans l'application plutôt que de remplacer le module existant dans le domaine global.

Vue spécifique au domaine de l'application Incident



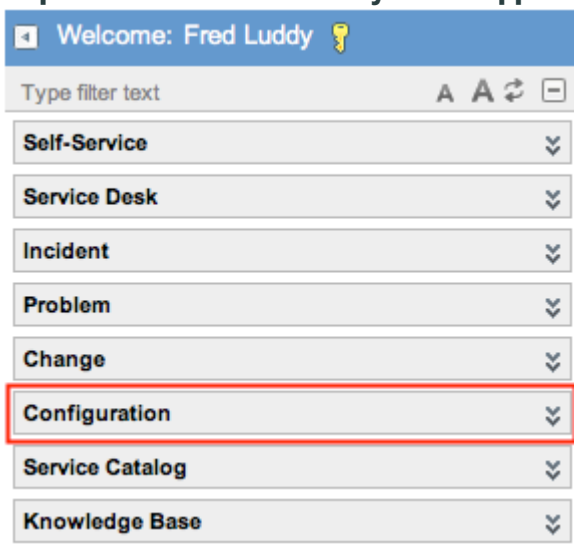
Si un autre administrateur d'un autre domaine, par exemple Fred Luddy, se connecte et consulte l'application Configuration, les paramètres du domaine global s'affichent.

Le point de vue de David Loo sur les applications



Traduction automatique

Le point de vue de Fred Luddy sur les applications



Activer la connexion de domaine détaillée et les messages de débogage

Les messages de journal et de débogage de domaine vous permettent de résoudre les erreurs de configuration de domaine.

Avant de commencer

Rôle requis : admin

Assurez-vous d'utiliser la dernière instance pour obtenir les meilleures performances.

Procédure

1. Dans le centre Domain Separation, 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. Activez la journalisation de domaine détaillée : accédez à **Tous** > **Administrateur de domaine** > **Centre Séparation de domaine** > **Configurer le centre du domaine** > **Active la journalisation détaillée du domaine** > **Oui** (ou définissez la propriété glide.sys.domain.verbose sur **True**).
2. Accédez à la **Diagnostics du système** > **Débogage de session** > **Autoriser tout**.
   Étant donné qu'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. Recherchez le texte Requête par rapport à la table.

   Cette requête trouve les messages de journal au format suivant :

```
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 consultant la table Incident n'a vu que les enregistrements qui correspondaient aux domaines de base de données Base de données Atlanta, Base de données, Base de données San Diego, Global et NY.

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. Activez la journalisation de domaine détaillée : accédez à **Tous** > **Administrateur de domaine** > **Centre Séparation de domaine** > **Configurer le centre du domaine** > **Active la journalisation détaillée du domaine** > **Oui** (ou définissez la propriété glide.sys.domain.verbose sur **True**).
2. Accédez à la **Diagnostics du système** > **Débogage de session** > **Autoriser tout**.
3. Laissez la session de débogage s'exécuter pendant un certain temps, par exemple un jour, avant de vérifier les fichiers journaux.
4. Accédez à la **Journaux système** > **Utilités** > **Téléchargement du fichier journal de nœud**.
5. Ouvrez l'enregistrement pour le 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 de journal au format suivant :

   Requête par rapport à la table Incident restreint par valeurs de domaine [global, Logiciel[8a4dde73c6112278017a6a4baf547aa7]]

   Dans cet exemple, un utilisateur ne voyait que les enregistrements de la table Incident qui correspondaient aux domaines global et logiciel.

Résoudre les erreurs de Domain Separation

Si vous rencontrez des problèmes de Domain Separation, consultez cette liste de solutions.

Erreur ou symptôme	Solution
Un sys_id de domaine 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 actuelle. Il est possible que la sys_id de domaine ait été supprimée accidentellement ou qu'elle fasse référence à une table de domaine précédente si vous avez modifié la table de domaine.

Traduction automatique

Erreur ou symptôme	Solution
	Pour corriger l'erreur, ouvrez une liste pour la table contenant l'erreur, filtrez la valeur de sys_domain non valide. Ensuite, saisissez manuellement la valeur de 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 se produire dans les tables Domaine de visibilité de l'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 des 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 de domainefichier . 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 contenu 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 contenues dans le domaine pour ne pas former de boucle.

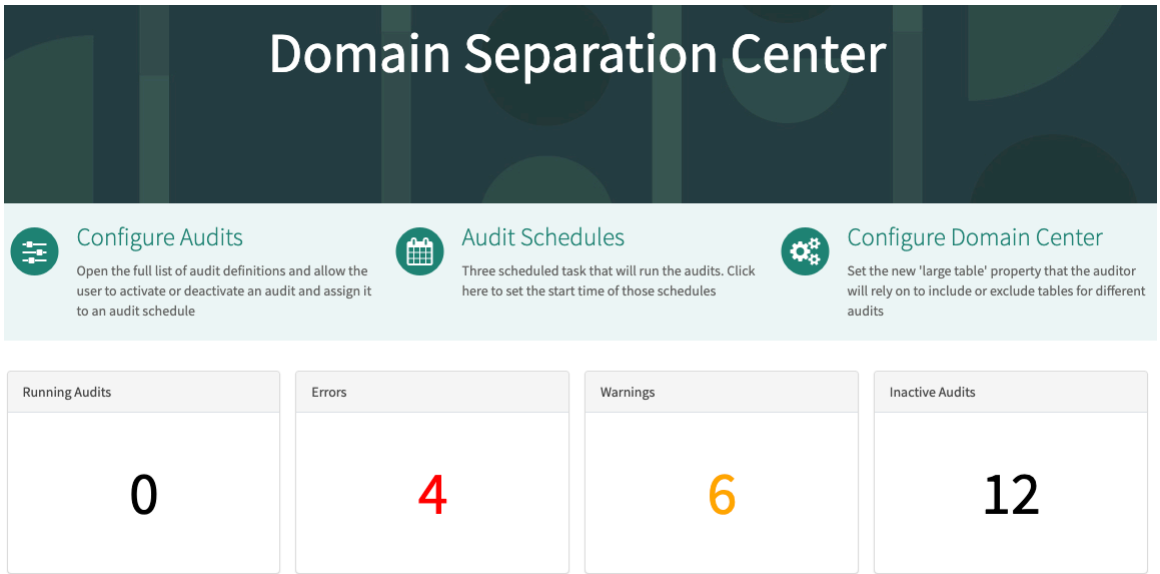
Centre Séparation de domaine

Auditez régulièrement vos domaines pour révéler les problèmes.

Vue d'ensemble

Domain Separation Center 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'analyser plus en détail les erreurs et avertissements de domaine. Le tableau de bord du centre Domain Separation est disponible à l'adresse <ServiceNow-instance-name>/domaincenter.

Domain Separation Center fournit de nombreux audits. Vous ne pouvez pas créer le vôtre. Vous pouvez toutefois configurer leur fréquence d'exécution. Les audits s'exécutent sur tous les domaines stockés dans la table domain_audit_definition.



Configurer des audits

Vous pouvez configurer si un audit est actif et à quelle fréquence il s'exécute.

1. Dans Domain Separation Center, 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** .

      Domain Separation Center exécute tous les audits marqués à la même fréquence en même temps. Ne sélectionnez pas **Quotidien** pour les audits exécutés 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 fonction de l'heure que vous configurez.

1. Dans Domain Separation Center, 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.

Les unités de temps sont mesurées avec l'horloge de 24 heures, c'est-à-dire que 14 est égal 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 de domaine : quotidien**, tous les audits exécutés quotidiennement sont exécutés.

Pour voir l'état d'un audit en cours d'exécution, dans Domain Separation Center, sélectionnez le numéro dans la zone **Audits en cours d'exécution** .

Exécuter les audits immédiatement

Les audits s'exécutent généralement comme prévu. Vous pouvez cependant exécuter tous les audits sur commande.

1. Dans Domain Separation Center, sélectionnez **Calendriers d'audit**.

   La page **Calendrier d'audit** s'affiche.

2. Sélectionnez le nom du calendrier d'audit à exécuter, par exemple Quotidien, Hebdomadaire ou Mensuel.
3. Sélectionnez **Exécuter maintenant**.

Pour voir l'état d'un audit en cours d'exécution, dans Domain Separation Center, sélectionnez le numéro dans la zone **Audits en cours d'exécution** .

Configurer le centre Séparation de domaine

1. Dans le centre Domain Separation, sélectionnez **Configurer le centre du domaine**.
2. Sur la page **Configurer le centre de domaine** , pour **Active la journalisation de domaine détaillée**, sélectionnez **Oui** pour stocker les journaux détaillés qui aident à diagnostiquer les problèmes liés au domaine. La 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, consultez Afficher les audits avec des avertissements et des échecs.

3. Dans la zone de liste double, sélectionnez et déplacez toutes vos grandes tables dans la colonne **Sélectionné** .

   Les audits quotidiens ne doivent pas s'exécuter sur des tables volumineuses. Les noms de table grisés dans la colonne **Sélectionné** sont volumineux et ne peuvent pas être déplacés vers la colonne **Disponible** .

4. Sélectionnez **Mettre à jour**.

Afficher les audits avec des avertissements et des échecs

Sur le tableau de bord, les **erreurs** et avertissements fournissent des informations détaillées sur les **audits** qui ont rencontré des problèmes. Les journaux associés à Domain Separation résident sur votre serveur dans la table syslog_domain.

1. Dans Centre Domain Separation, 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 des **Détails du résultat d'audit** se réfèrent aux valeurs de la table syslog_domain des 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 **ID de détail** d'un avertissement ou d'une erreur dans le panneau de gauche.

   b. Dans le navigateur de filtre de HI, entrez *`syslog_domain.do`*.

      La page Journal de domaine s'affiche.

   c. Dans le champ **de recherche Source** , entrez `=<Detail-ID >` (pas d'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 du 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 (Deactivate Audit**) : désactive un audit.
   - **Copier les détails** : permet de copier 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, selon la planification. Vous pouvez afficher leur état au fur et à mesure de leur exécution.

1. Sélectionnez le nombre dans la zone **Audits en cours d'exécution** pour afficher les audits en cours d'exécution ou en attente d'exécution.

   La page **Audits en cours d'exécution** s'affiche.

2. Sélectionnez un audit pour obtenir plus d'informations à son sujet.

Afficher les audits inactifs

1. Sélectionnez le numéro 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 de domaine

Spécifiez quelles tables dans les 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 à exécuter 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 quotidiens sur de grandes tables. Le lancement d'un nouvel audit dont l'exécution prend plus d'une journée peut avoir des conséquences négatives.

Une journalisation détaillée peut fournir de meilleures informations sur les problèmes détectés lors des audits, mais peut entraîner des problèmes de performance.

Procédure

1. Dans le centre Domain Separation, sélectionnez **Configurer le centre du domaine**.
   La page Configurer le centre du domaine s'affiche.
2. Sélectionnez **Oui** pour **Active la journalisation de domaine détaillée**, 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 des avertissements et des échecs.
3. Dans la liste, déplacez toutes vos grandes tables dans la colonne **Sélectionné** .
   Les audits quotidiens ne doivent pas s'exécuter sur des tables volumineuses. Les noms de table grisés dans 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 des audits

Configurez si un audit est actif et à quelle fréquence il est exécuté.

Avant de commencer

Rôle requis : admin

Procédure

1. Dans Domain Separation Center, cliquez sur **Configurer les audits**.
   T s’affiche.
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** .
      Domain Separation Center exécute tous les audits marqués à la même fréquence en même temps. Ne sélectionnez pas **Quotidien** pour les audits exécutés sur des tables volumineuses.
   d. Répétez les étapes a à c pour chaque audit que vous souhaitez activer.
3. Cliquez sur **Enregistrer**.

Planifier les 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 Domain Separation, 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 est égal 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.

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 qui doivent s'exécuter quotidiennement.

Que faire ensuite
Pour voir l'état d'un audit en cours d'exécution, dans le Centre Domain Separation, cliquez sur le nombre dans la zone **Audits en cours d'exécution** .

Exécuter les audits immédiatement

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, cependant, 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 Domain Separation, 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 voir l'état d'un audit en cours d'exécution, dans le Centre Domain Separation, cliquez sur le nombre dans la zone **Audits en cours d'exécution** .

Afficher les audits avec des avertissements et des erreurs

Le Centre Domain Separation fournit des détails sur les avertissements et les erreurs d'audit.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Sur le tableau de bord Domain Separation Center, les **erreurs** et **avertissements** fournissent des informations détaillées sur les audits qui ont rencontré des problèmes. Les journaux associés à Domain Separation résident sur votre serveur dans la table syslog_domain. Les erreurs sont des problèmes qui nécessitent une attention immédiate. Les avertissements n'entraînent pas d'échecs mais présentent les meilleures pratiques, par exemple, ne pas rendre le nom de domaine trop long.

Procédure

1. Dans le Centre Domain Separation, 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.

La page affiche des informations détaillées sur les problèmes liés à l'audit que vous avez sélectionné. Les messages dans **les détails du résultat 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 **ID de détail** d'un avertissement ou d'une erreur dans le panneau de gauche.

   b. Sur l'instance exécutant le Centre Domain Separation, dans le **navigateur de filtre**, saisissez *`syslog_domain.list`*.
   La page Journal de domaine s'affiche.

   c. Dans le champ de recherche de la colonne **Source** , entrez `=<Detail-ID >` (pas d'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 du domaine. Les informations incluses dans le message correspondent au type d'audit.

4. **Facultatif :** Sélectionnez l'une des options suivantes :
   - **Réexécuter l'audit** : réexécutez un audit pour voir s'il rencontre toujours un avertissement ou une erreur.
   - **Désactiver l'audit** : permet de désactiver l'audit.
   - **Copier les détails** : permet de copier 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 voir 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, selon la planification. 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 d'exécution** pour afficher les audits en cours d'exécution ou en attente d'exécution.
   La page Audits en cours d'exécution s'affiche.
2. Cliquez sur un audit en cours ou en attente pour afficher les informations le concernant.

Afficher les audits inactifs

Vous pouvez afficher tous les audits inactifs au même endroit et les activer éventuellement.

Avant de commencer
Rôle requis : admin

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**.

Identité

En savoir plus sur les identités dans l'instance.

Analyseur d'accès

Access Analyzer est un ServiceNow® App Store qui est un outil de diagnostic d'accès. Il permet de déterminer qui a accès à une ressource.

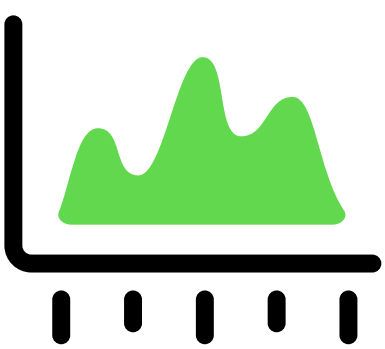
Identité globale

Global Identity est une application ServiceNow® qui permet de mettre à jour les attributs d'utilisateur d'une instance à l'autre (instances multiples). Elle est un outil de stockage

Identity Center

Identity Center vous permet de surveiller, de gérer et de minimiser les risques et les failles de sécurité liés à l'identité.

Système de gestion des identités inter-domaines (SCIM)



Audit d'identité et d'accès

Utilisez l'audit d'identité et d'accès pour comprendre les modifications apportées à un utilisateur, un groupe, un rôle et une ACL.

Traduction automatique

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 les utilisateurs et les groupes à l’aide du protocole SCIM.		

Analyseur d'accès

Access Analyzer est une ServiceNow® application de stockage qui est un outil de diagnostic d’accès. Elle permet de déterminer qui a accès à une ressource.

Identité globale

Global Identity est une ServiceNow® application de stockage qui permet de mettre à jour et de synchroniser les attributs d’utilisateur d’une instance à l’autre (instances multiples).

Audit d'identité et d'accès

Utilisez l’audit d’identité et d’accès pour comprendre les modifications apportées à un utilisateur, un groupe, un rôle et une ACL.

Identity Center

Identity Center vous permet de surveiller, de gérer et de minimiser les risques et les failles de sécurité liés à l’identité.

Système de gestion des identités inter-domaines (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 les utilisateurs et les groupes à l’aide du protocole SCIM.

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

Apprenez à utiliser Access Analyzer.

Évaluation de l’autorisation

Découvrez comment les autorisations sont évaluées.

Forum Aux Questions

Obtenez des détails sur les questions fréquemment posées à propos d’Access Analyzer.

Traduction automatique

Exploration d'Access Analyzer

Analysez les identités sur l'instance ServiceNow® .

ServiceNow Access Analyzer est une application qui aide les administrateurs et les développeurs à afficher les autorisations pour l'utilisateur, le rôle ou le groupe sélectionné.

Remarque :

- Access Analyzer 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.
- Access Analyzer emprunte l'identité de l'enregistrement d'identité pour récupérer des détails sur les 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, quelle que soit la politique d'accès définie pour les utilisateurs, telle 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.
- Access Analyzer a des limites dans l'évaluation précise de l'accès des ressources liées aux ressources de champ d'application géré et au développeur délégué.

Évaluer l'accès

Évaluer l'accès est une fonctionnalité de l'analyseur d'accès ServiceNow , qui aide les administrateurs et les développeurs à afficher 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 d'une table, des includes de script pouvant être appelés par le 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 et leur gestion des risques, atteindre leurs objectifs de conformité et comprendre qui (identité) a accès à quoi (ressources).

Comparer l'accès

Comparer l'accès ServiceNow est une fonctionnalité d'Access Analyzer V2 qui permet aux administrateurs, aux développeurs et aux agents d'assistance de comparer l'accès des utilisateurs et de déterminer le niveau d'accès correct 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.

Compare Access vous permet d'effectuer l'analyse suivante :

- Niveau 1 : comparez les enregistrements utilisateur pour comprendre les attributs, les rôles et les groupes.
- Niveau 2 : comparez les contrôles d'accès pour effectuer l'analyse de la cause première en identifiant les problèmes d'accès.

Avantages

Voici quelques-uns des avantages de l'utilisation de l'analyseur d'accès :

- Analyser l’accès aux ressources (tables).
- Comparez l’accès de 2 utilisateurs.
- Comparez les rôles et les groupes de 2 utilisateurs.
- Empêcher de surprovisionner les autorisations.
- Générez un rapport indiquant si une identité a accès à une ressource (table).
- Identifiez qui a accès pour des questions d’hygiène de sécurité critiques.
- Permet d’éviter le surprovisionnement des autorisations.
- Obtenez les principaux de privilèges minimum lors de l’implémentation de contrôles d’accès.
- Limitez l’accès à certaines données, notamment aux applications, aux tables, aux lignes ou colonnes et à d’autres ressources.
- Fournissez 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 d’Access Analyzer

Analysez les identités et leur accès sur l’instance ServiceNow® .

Avant de commencer

Rôle requis : admin

La procédure suivante décrit les étapes d’accès à Access Analyzer et d’utilisation de diverses fonctionnalités dans Access Analyzer.

Remarque :
Access Analyzer 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.

   Access Analyzer offre les fonctionnalités suivantes :

   - Évaluer l’accès
   - Comparer les enregistrements utilisateur
   - Comparer les contrôles d’accès

2. Sélectionnez l’onglet correspondant pour utiliser l’analyseur d’accès en fonction de vos besoins.

Utiliser Évaluer l’accès

Analysez les identités sur l’instance ServiceNow® .

Avant de commencer

Rôle requis : admin

Dans la procédure suivante, nous vous expliquons les étapes permettant d’accéder à Évaluer l’accès dans l’analyseur d’accès et d’utiliser 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 de l'accès et des autorisations

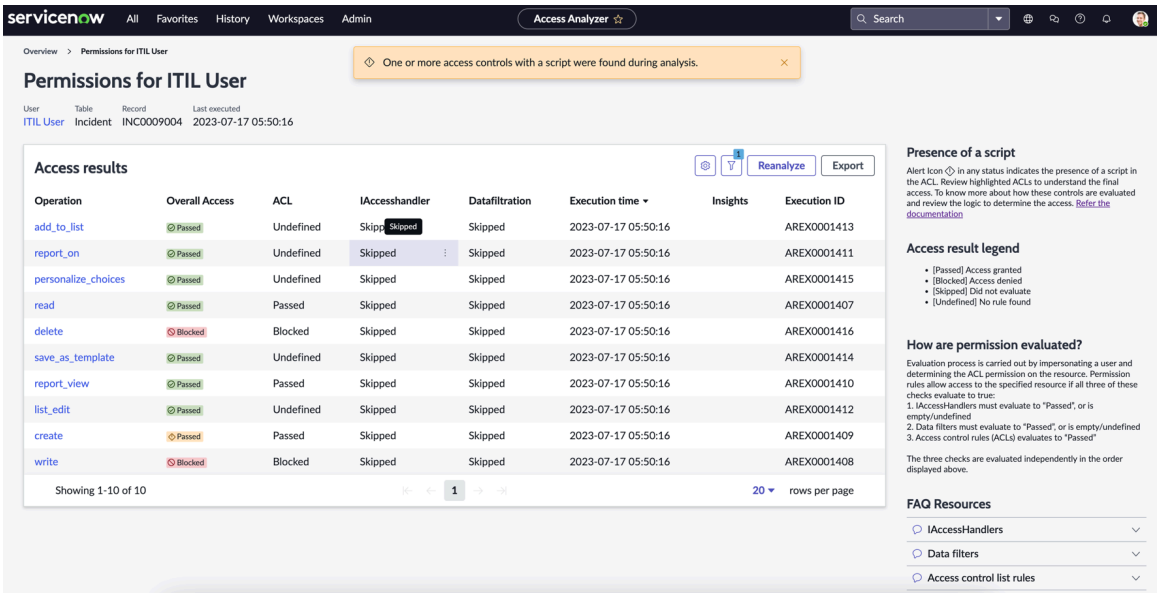
Champ	Description
Analyser par *	Analyser l'accès d'un utilisateur, d'un rôle ou d'un groupe
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste.
Type de règle *	Analysez l'accès pour une table, une page d'interface utilisateur, un point de terminaison REST ou un script include 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 de l'utilisateur sont affichés. De même, vous pouvez analyser les autorisations d'un groupe ou d'un rôle pour les types de règles suivants :

   - Table (enregistrement)
   - Les scripts clients pouvant être appelés comprennent
   - Points de terminaison REST

   Les résultats de l'accès sont affichés.



Le tableau des résultats de l’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.
IAccessHandler	Un contrôle du système interne à l’aide du code source masqué sur la plateforme. IAccessHandler peut accorder ou refuser l’accès à une ressource sans évaluer les ACL. Si IAccessHandler est ignoré, les ACL sont évaluées.
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.
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.

Afficher les autorisations d'un utilisateur

Utilisez l'analyseur d'accès pour afficher les autorisations d'un utilisateur sélectionné.

Avant de commencer
Rôle requis : admin

La procédure suivante décrit les exemples d'étapes permettant d'afficher les autorisations d'un utilisateur sélectionné (**utilisateur ITIL**) afin d'afficher les autorisations de la table **Incident** à l'aide d'évaluer l'accès dans Access Analyzer.

Remarque :
Access Analyzer est un produit du ServiceNow® Store.

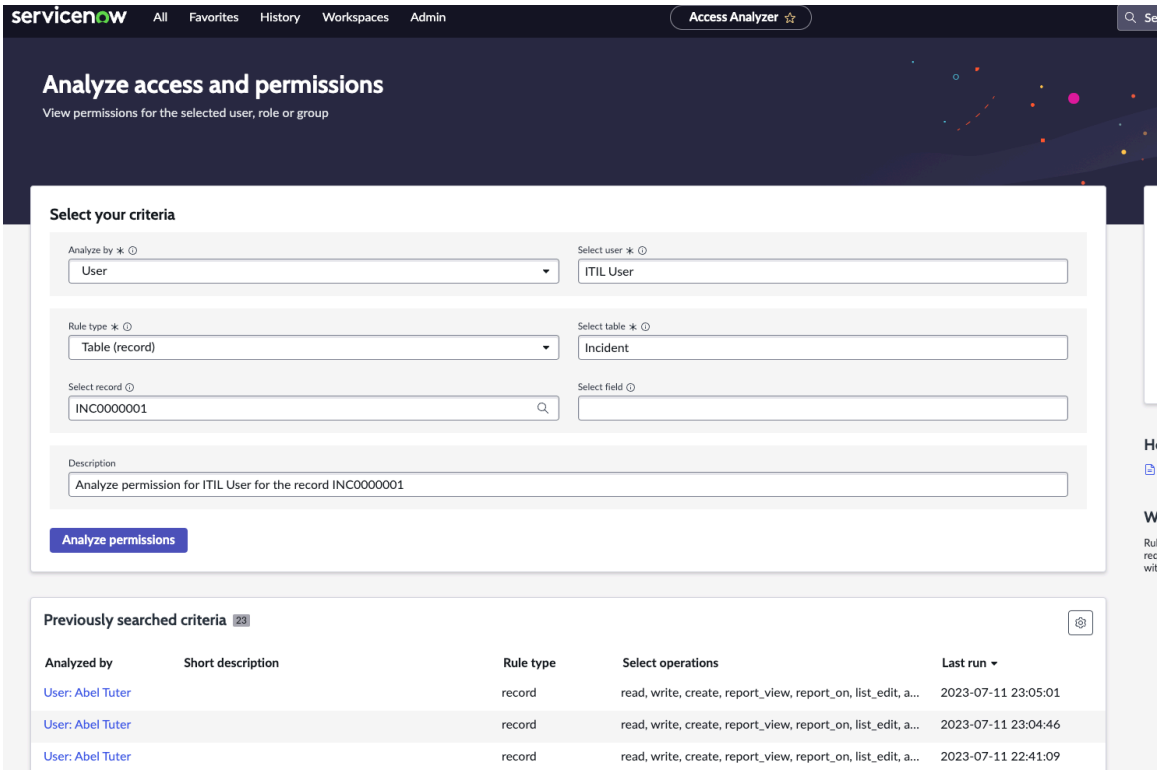
Procédure

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 :

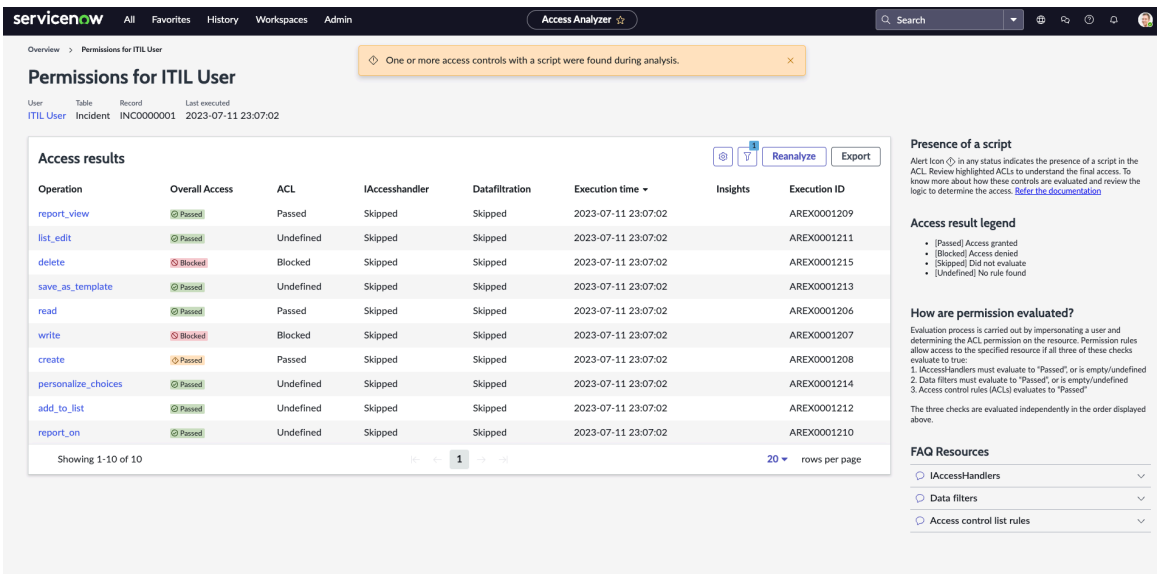
Sélectionnez vos critères d'analyse de l'accès et des autorisations

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 **script include 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 d'un champ. Par exemple, Actif, Créé par, etc.

3. Spécifiez la description dans le champ **Description** .
4. Sélectionnez **Analyser les autorisations**.



Les **résultats de l'accès** pour **l'utilisateur ITIL** s'affichent.



Les résultats peuvent être lus en se référant aux filtres Légendes, Liste de contrôle d'accès (ACL), IAccesshandler et Données.

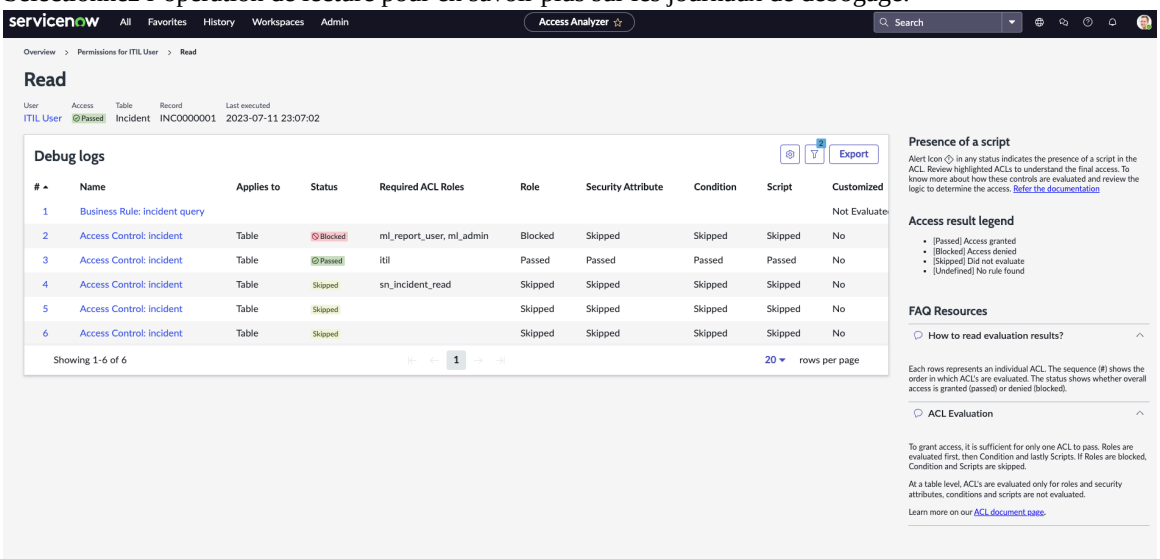
Prenons l'exemple de l'opération **de lecture** . Pour **l'utilisateur ITIL** , l'accès global est Réussi, ce qui signifie que l'utilisateur est en mesure de lire l'enregistrement avec les autorisations appropriées (ACL).

De même, pour l'opération **de création** , l'accès global est transmis avec une icône d'alerte, ce qui signifie qu'un script peut être présent pour l'évaluation de l'ACL.

Traduction automatique

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.

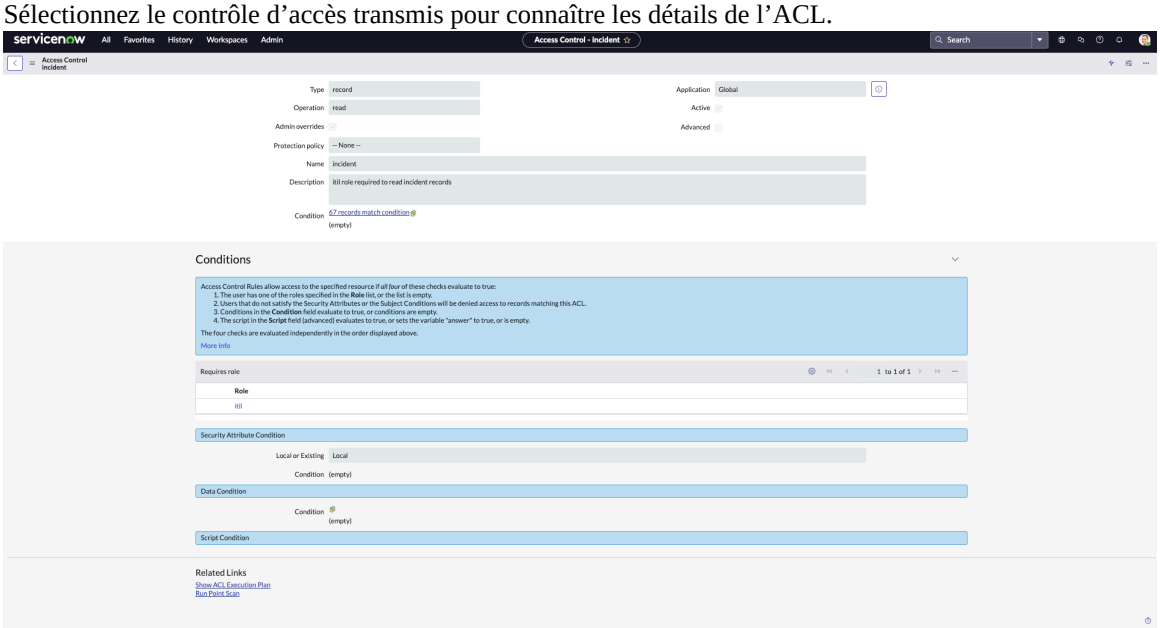


La page Journaux de débogage affichait la règle métier et les ACL associées requises pour effectuer l'opération de **lecture** pour l'enregistrement.

Les journaux de débogage indiquent qu'une règle métier et 4 ACL sont associées à l'opération de lecture.

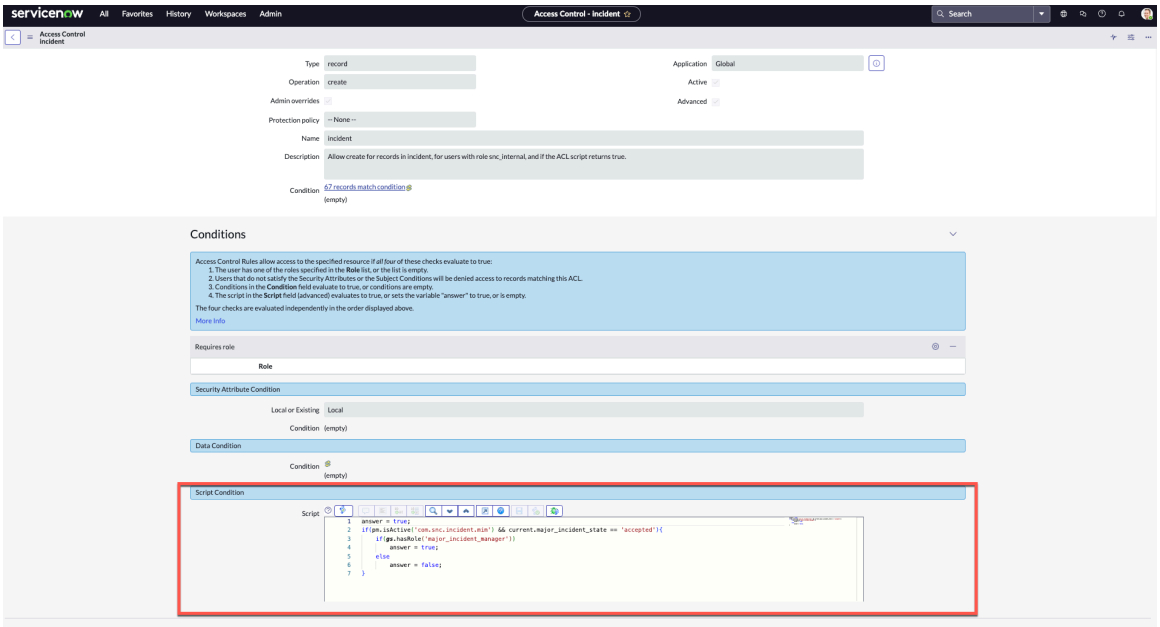
Il existe un état **Transmis** pour l'une des ACL, ce qui signifie que pour lire l'enregistrement sélectionné, l'utilisateur dispose de l'ACL requise et peut lire l'enregistrement. Étant donné que l'une des évaluations ACL est **réussie**, les autres évaluations d'ACL sont **ignorées**.

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 le **Réussi** et la présence d'un script. La page Contrôle d'accès affiche le script associé pour l'enregistrement.



Afficher les autorisations d'un rôle

Utilisez l'analyseur d'accès pour afficher les autorisations d'un rôle sélectionné.

Avant de commencer

Rôle requis : admin

La procédure suivante décrit les exemples d'étapes permettant d'afficher les autorisations pour un rôle sélectionné (**user_admin**) afin d'afficher l'autorisation d'un point de terminaison d'API REST à l'aide de l'outil Évaluer l'accès dans Access Analyzer.

Remarque :
Access Analyzer est un produit du ServiceNow® Store.

Procédure

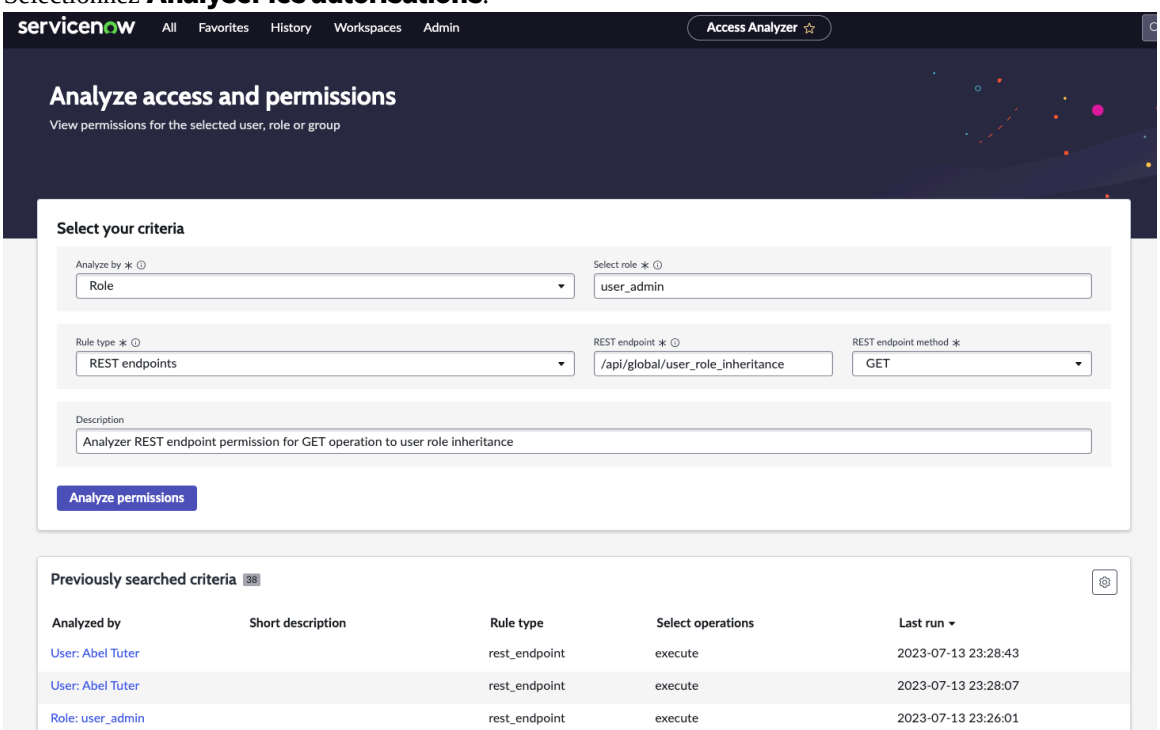
1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez vos critères comme suit :

Sélectionnez vos critères d'analyse de l'accès et des autorisations

Champ	Description
Analyser par *	Sélectionnez **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 script include de client pouvant être appelé. Par exemple, **Point de terminaison REST**.

Champ	Description
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**.



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), IAccesshandler 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

La procédure suivante décrit les exemples d'étapes permettant d'afficher les autorisations d'un groupe sélectionné (**Gestion des incidents**) afin d'afficher les autorisations d'une page de **l'interface utilisateur** d'incident à l'aide d'évaluer l'accès dans l'analyseur d'accès.

Remarque :
Access Analyzer est un produit du ServiceNow® Store.

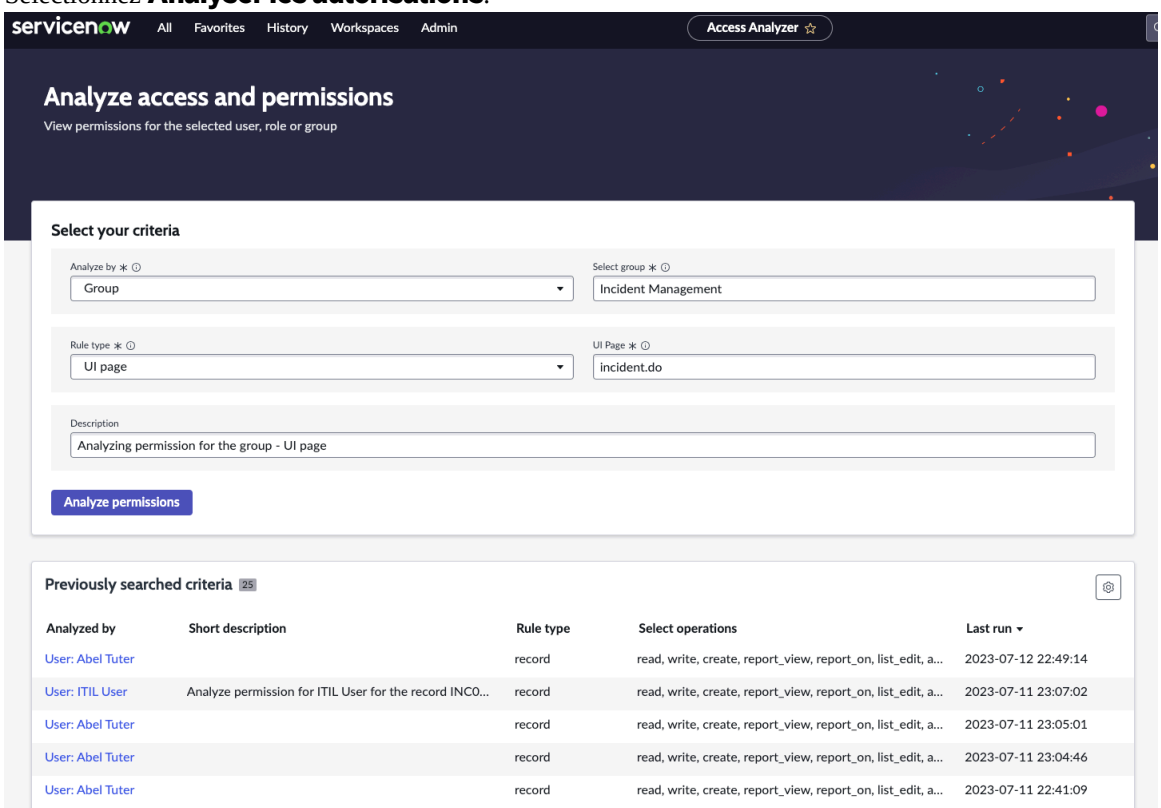
Procédure

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 :

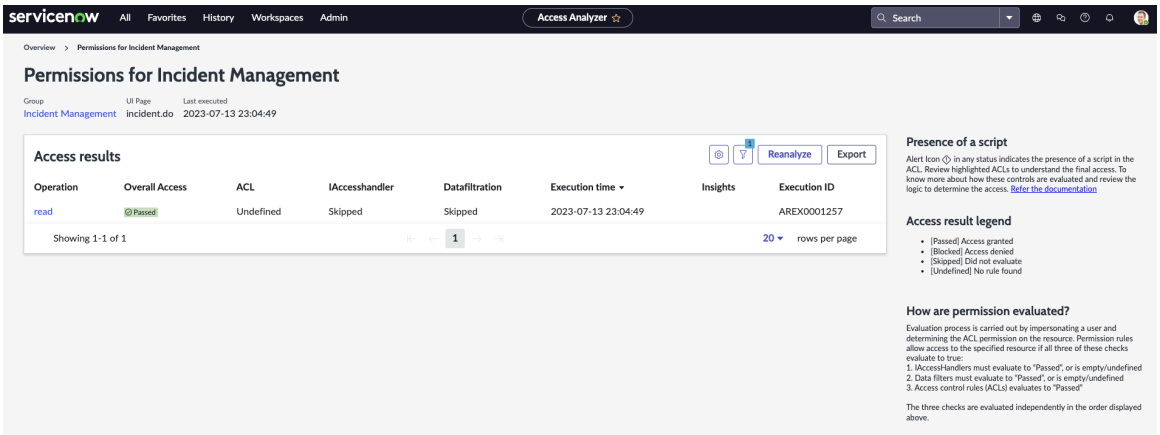
Sélectionnez vos critères d'analyse de l'accès et des autorisations

Champ	Description
Analyser par *	Sélectionnez **un groupe**.
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste. Par exemple, **Incident Management**.
Type de règle *	Analysez l'accès pour une table, une page d'interface utilisateur, un point de terminaison REST ou un script include 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 de l'accès** pour le groupe **Incident Management** s'affichent.



Les résultats peuvent être lus en se référant aux filtres Légendes, Liste de contrôle d'accès (ACL), IAccesshandler et Données.

L'accès global du groupe est transmis, ce qui signifie que les utilisateurs du groupe (**Incident Management**) sont en mesure d'accéder à l'enregistrement d'incident.

Exporter les requêtes de l'analyseur d'accès

Exportez les requêtes analysées à l'aide d'Access Analyzer.

Avant de commencer

Rôle requis : admin

La procédure suivante décrit les étapes d'accès à Access Analyzer et d'utilisation de diverses fonctionnalités dans Access Analyzer.

Remarque :
Access Analyzer est un produit du ServiceNow® Store.

Procédure

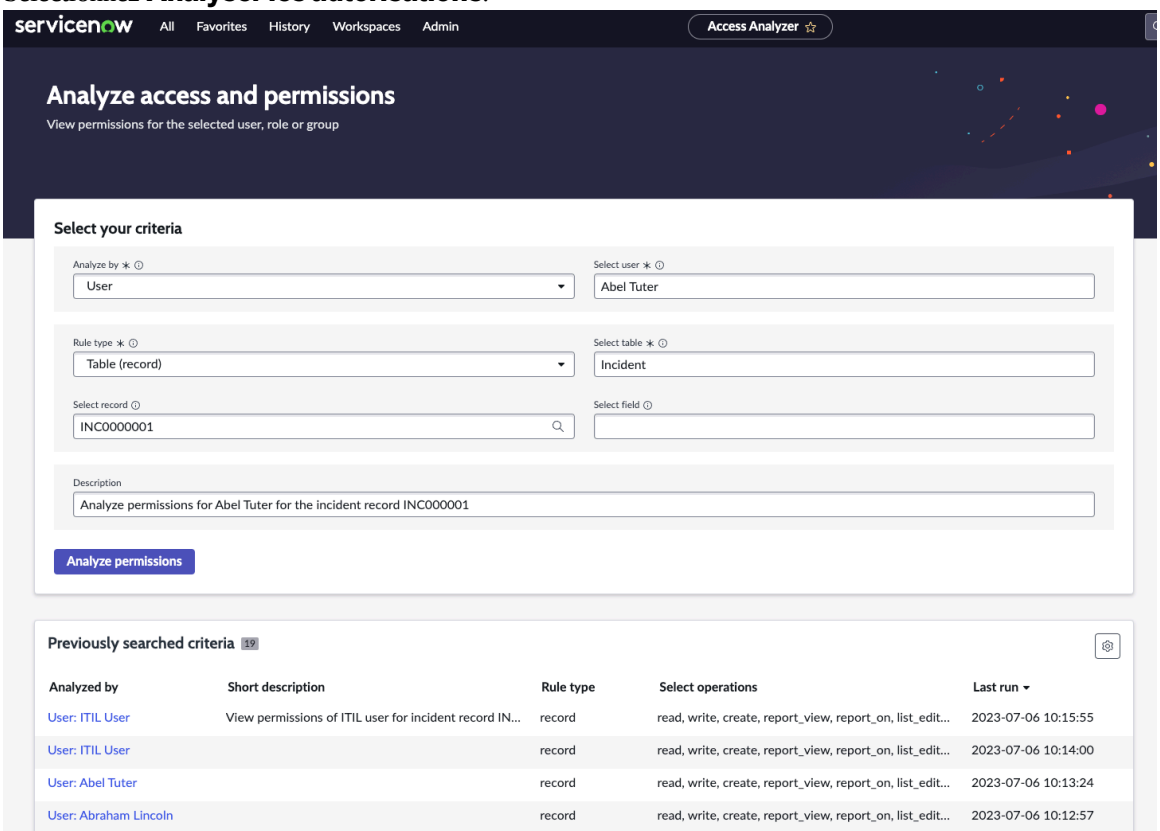
1. Accédez à la **Tous** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez vos critères comme suit :

Sélectionnez vos critères d'analyse de l'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 script include 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.

Champ	Description
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**.

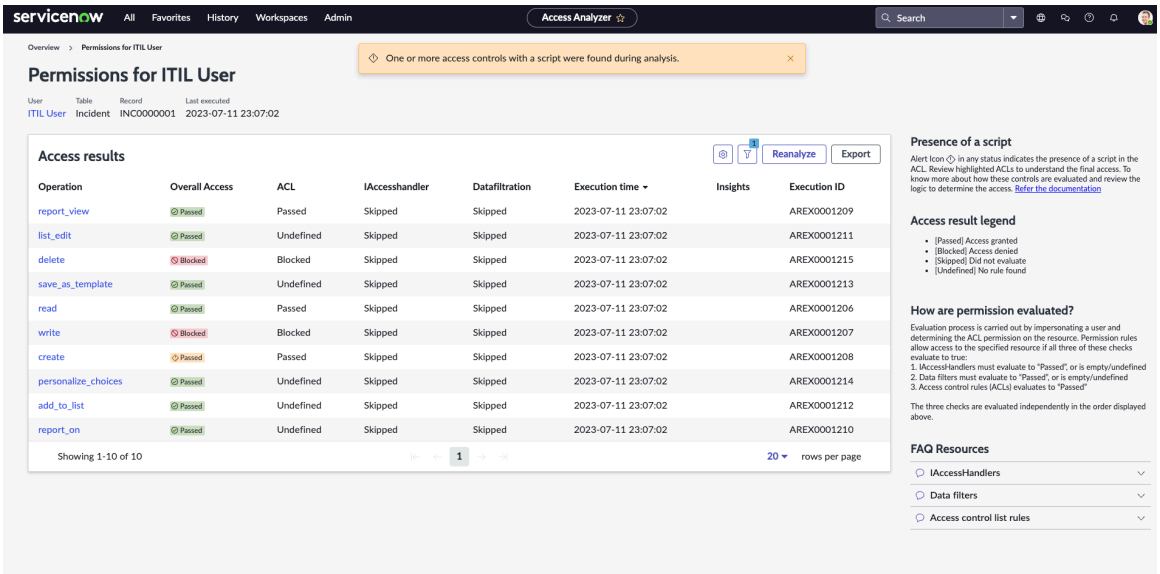


Les résultats d'accès de l'utilisateur sont affichés. De même, vous pouvez analyser les autorisations d'un rôle de groupe pour les types de règles suivants :

- Table (enregistrement)
- Include de script de client pouvant être appelé
- Points de terminaison REST

Les **résultats d'accès** pour le type de règle sélectionné s'affichent.

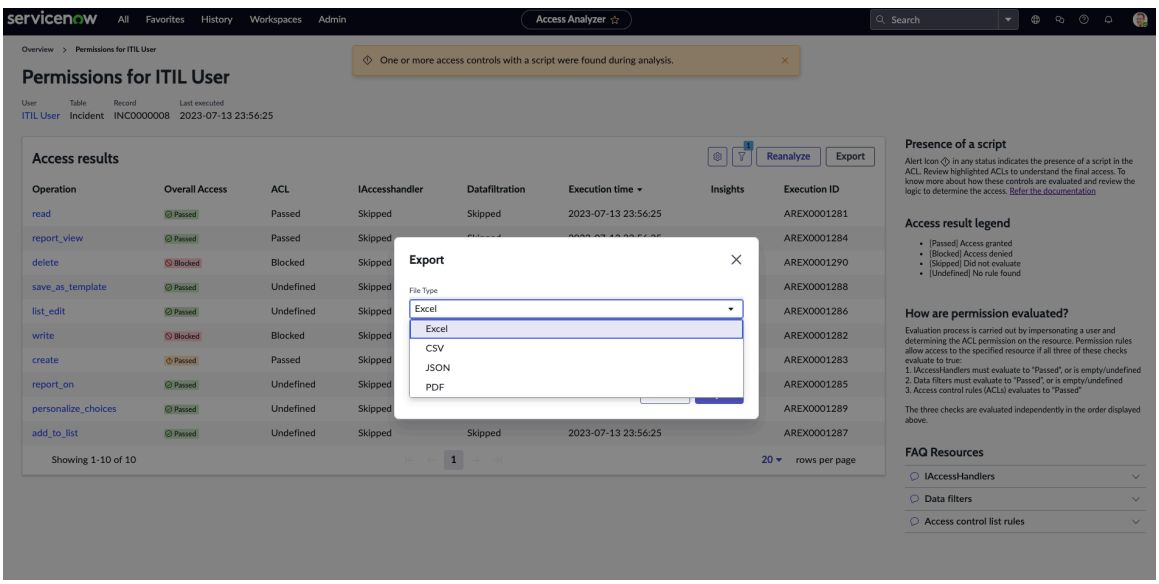
Traduction automatique



5. Cliquez sur **Exporter**.

a. Choisissez le type de fichier.

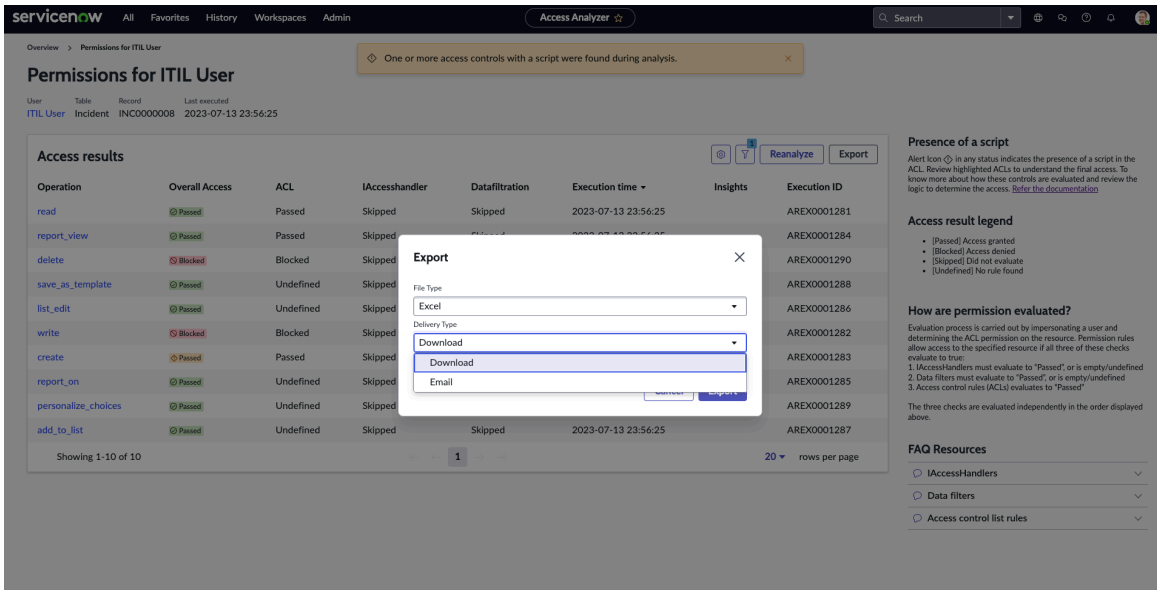
Les types de fichiers disponibles sont Excel, CSV, JSON, PDF.



b. Choisissez le type de livraison.

Traduction automatique

Les types de livraison disponibles sont Téléchargement et E-mail.



Comparaison des enregistrements utilisateur

Comparez les enregistrements utilisateur pour comprendre l'accès entre deux utilisateurs.

Avant de commencer

Rôle requis : admin

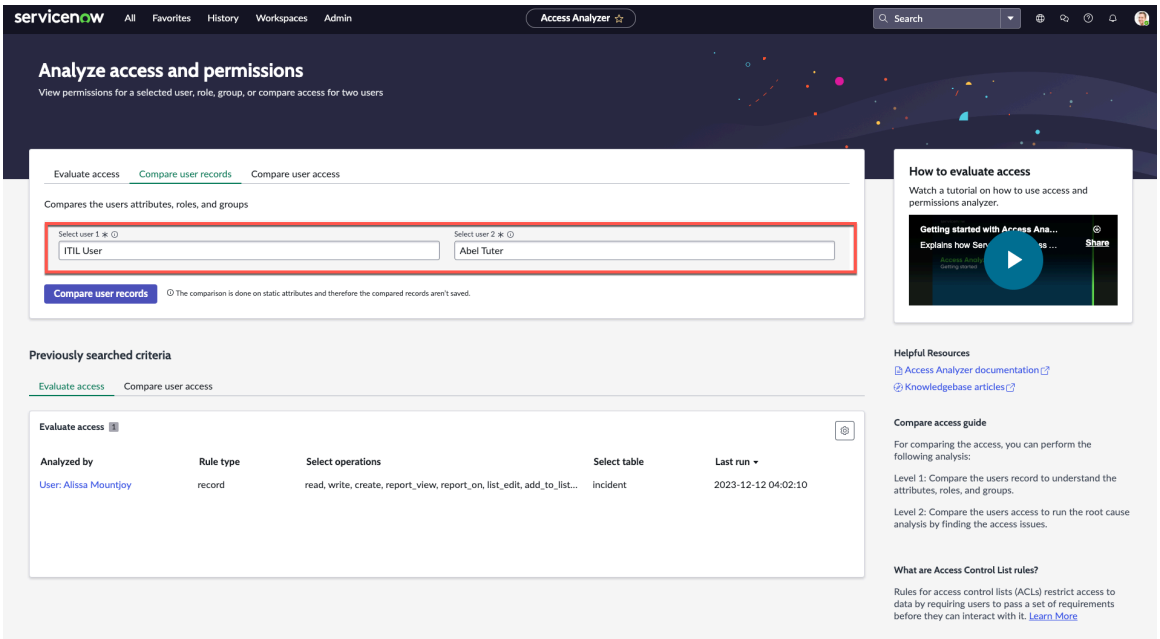
Dans la procédure suivante, nous vous expliquons les étapes de comparaison des enregistrements utilisateur à l'aide de l'analyseur d'accès.

Remarque :
Access Analyzer est un ServiceNow® Store produit.

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 utilisateur** .
3. Sélectionnez **l'utilisateur 1** et **l'utilisateur 2** pour la comparaison.

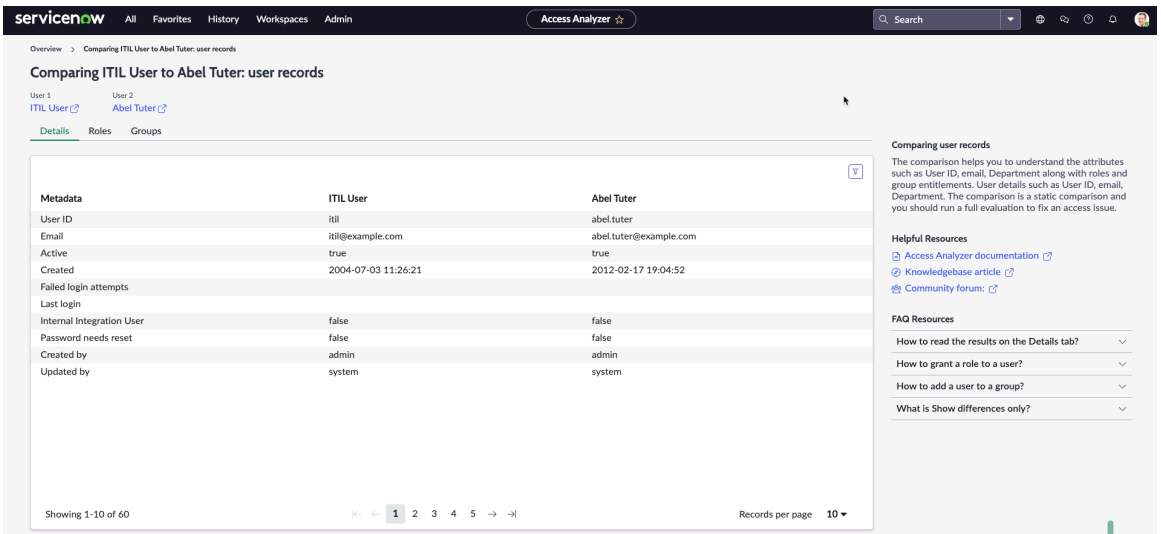
   Par exemple, Utilisateur ITIL en tant **qu'utilisateur 1** et Abel Tuter en tant **qu'utilisateur 2**.



4. Sélectionnez **Comparer les enregistrements utilisateur**.

   Les résultats sont affichés avec les onglets suivants :

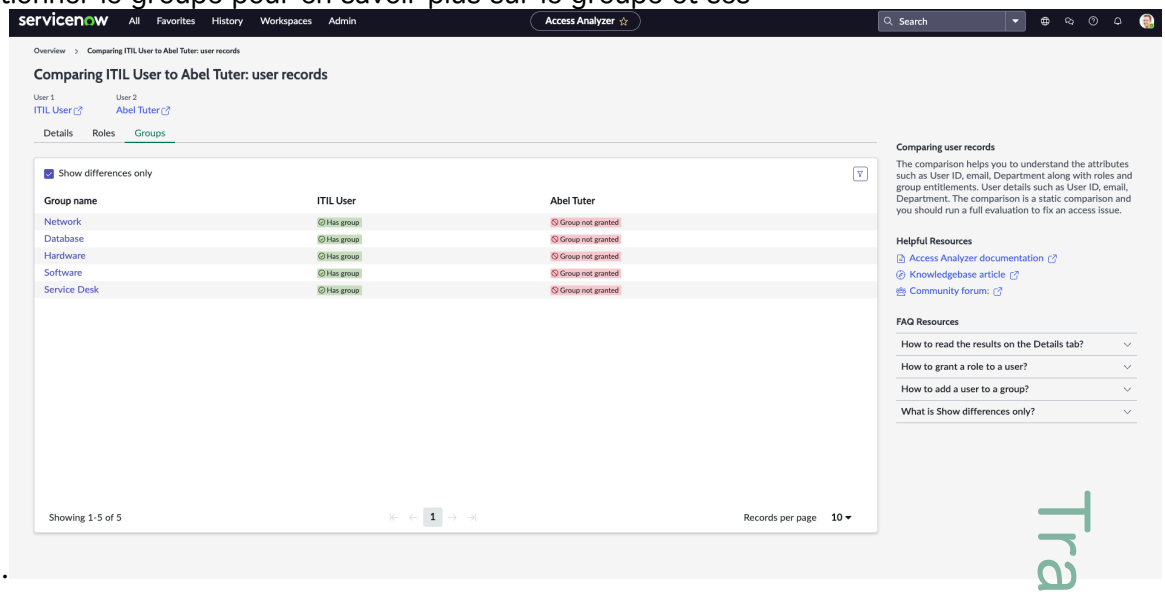
- **Détails** : permet d'afficher les métadonnées de



l'utilisateur.

- **Rôles** : affichez les rôles qui sont affectés à l'utilisateur. Vous pouvez sélectionner le rôle pour en savoir plus sur celui-ci et ses autorisations.

- **Groupes** : affichez les groupes qui sont 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 leur est affecté.

Comparaison de l'accès des utilisateurs

Comparez le contrôle d'accès de l'utilisateur à l'aide de l'analyseur d'accès.

Avant de commencer

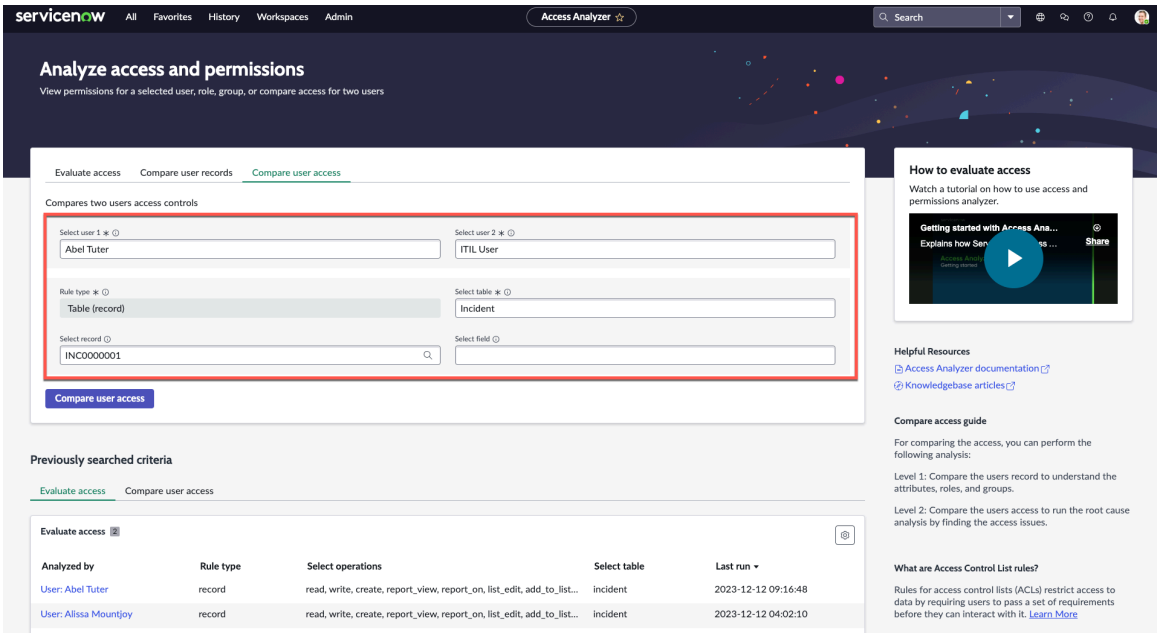
Rôle requis : admin

La procédure suivante décrit les étapes permettant de 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 :



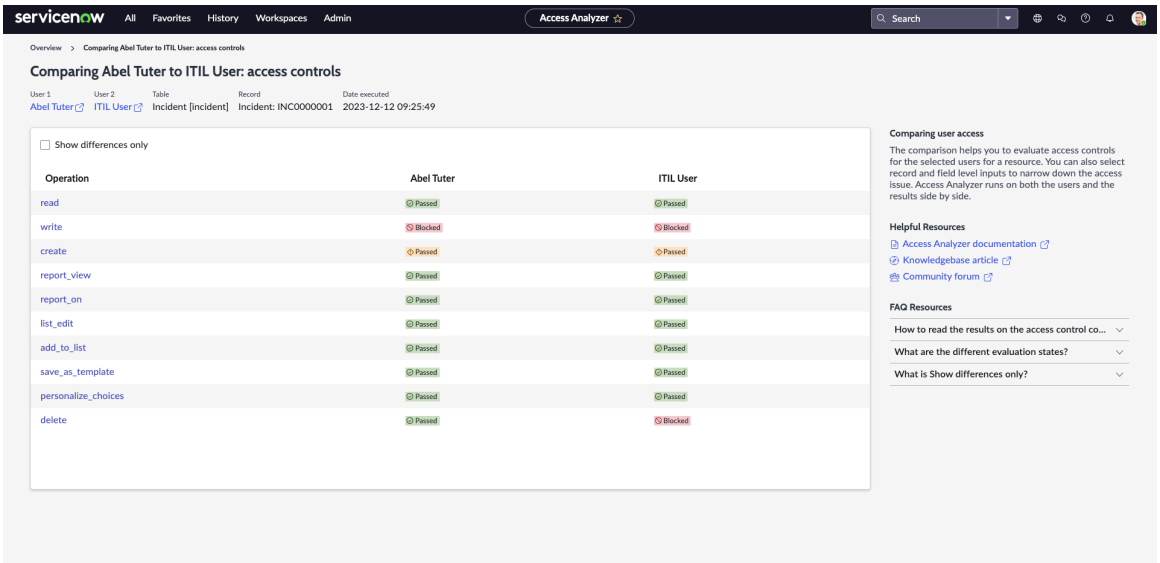
Comparer l’accès des utilisateurs

Champ	Description
Sélectionner l’utilisateur 1*	Spécifiez un nom d’utilisateur à sélectionner dans la liste pour la comparaison.
Sélectionner l’utilisateur 2*	Spécifiez un nom d’utilisateur à sélectionner dans la liste pour comparer avec l’utilisateur 1.
Type de règle*	Analysez les autorisations d’accès pour une table. **Remarque :** Seules les autorisations d’accès pour une table peuvent être utilisées pour **comparer l’accès utilisateur**.
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.

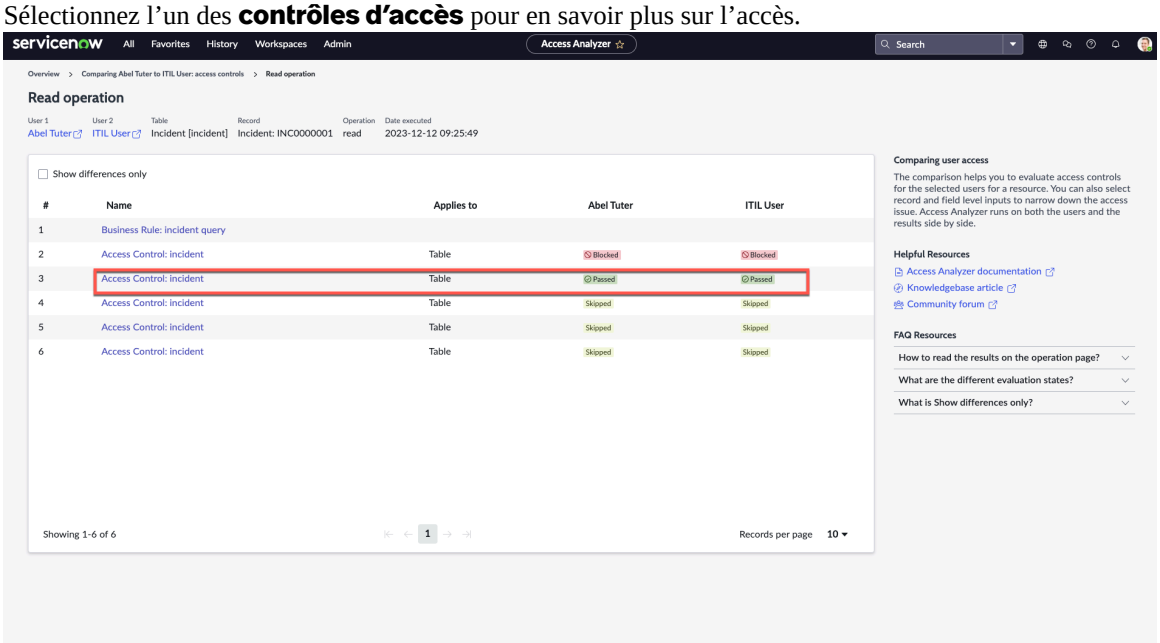
4. Sélectionnez **Comparer l’accès des utilisateurs**.

   Les résultats de **comparaison d’accès utilisateur** pour les utilisateurs sélectionnés s’affichent.

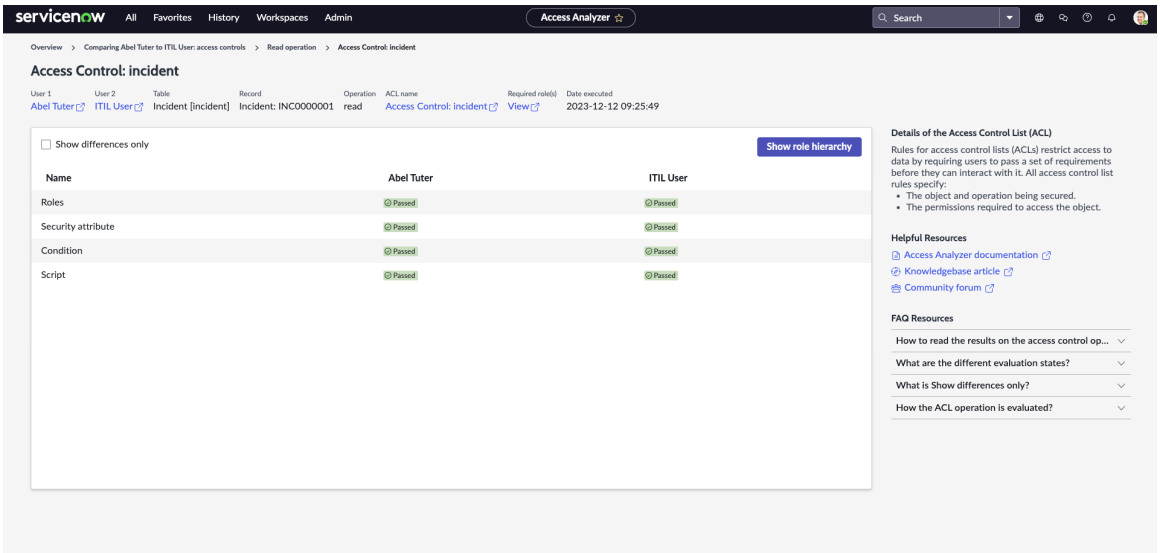
   Les résultats de comparaison de l’accès utilisateur montrent l’état de l’opération et de l’évaluation de l’accès pour les utilisateurs. Par exemple, Abel Tuter et Utilisateur ITIL.



5. Sélectionnez l’opération pour en savoir plus sur l’évaluation des autorisations et les rôles auxquels les utilisateurs sont affectés.
   Par exemple, **opération de lecture** .
6. Sélectionnez l’un des **contrôles d’accès** pour en savoir plus sur l’accès.

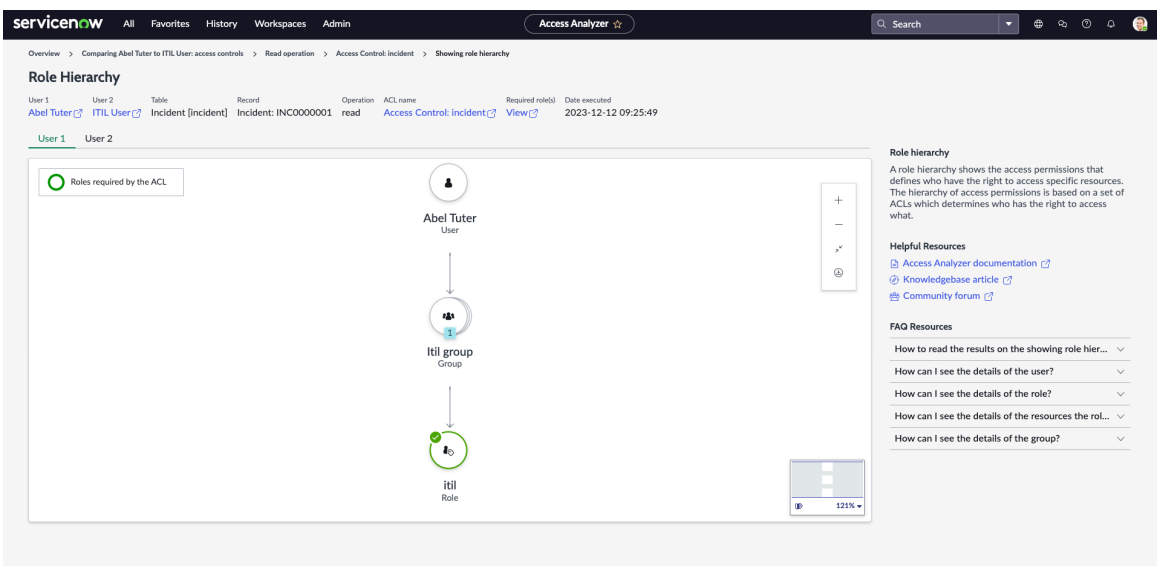


Les détails du contrôle d’accès tels que les rôles, l’attribut de sécurité, la condition et l’état d’évaluation des scripts sont affichés.



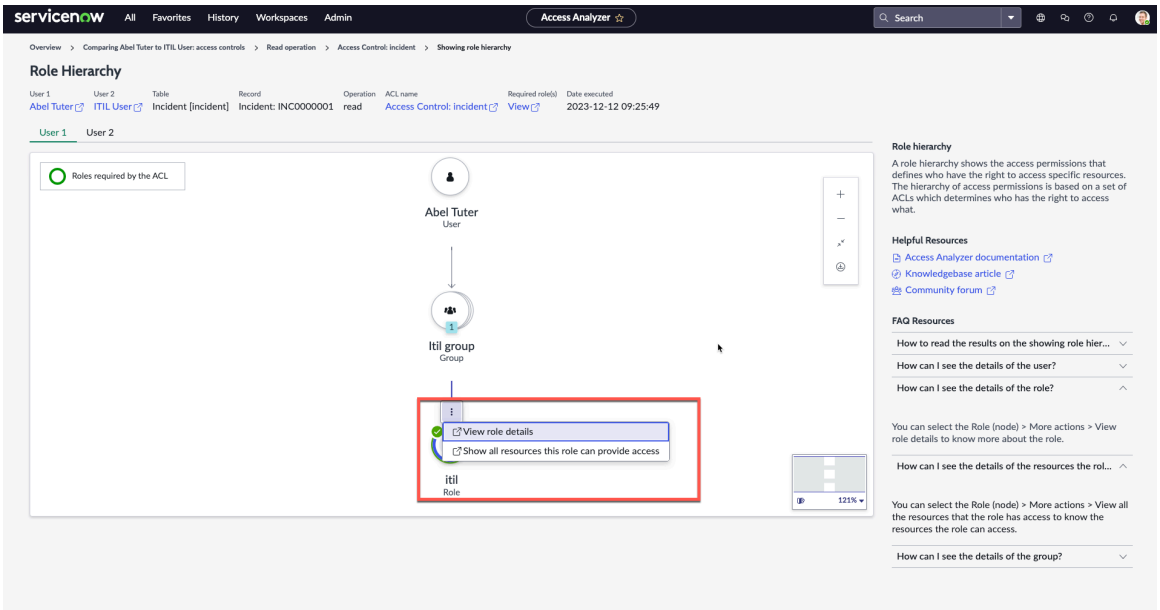
7. Sélectionnez **Afficher la hiérarchie des rôles** pour en savoir plus sur les rôles et les groupes qui sont affectés à l'utilisateur et comparer les deux utilisateurs.

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, un utilisateur ITIL est affecté à **Abel Tuter** et à un utilisateur **ITIL**. Donc, les deux contrôles d'accès ont été passés. 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 le rôle peut accéder ou le groupe.



Affichage des requêtes de l'analyseur d'accès - Critères recherchés précédemment

Affichez les critères d'analyseur d'accès précédemment recherchés.

Avant de commencer

Rôle requis : admin

Remarque :
Access Analyzer est un ServiceNow® Store produit.

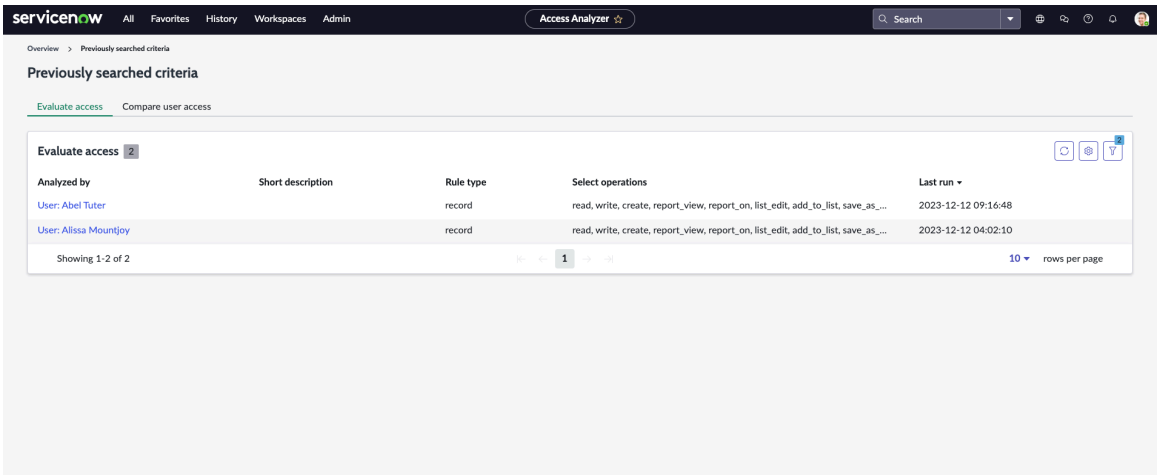
Procédure

1. Accédez à la **Tous** > **Analyseur d'accès** > **Requêtes d'analyseurs d'accès**.

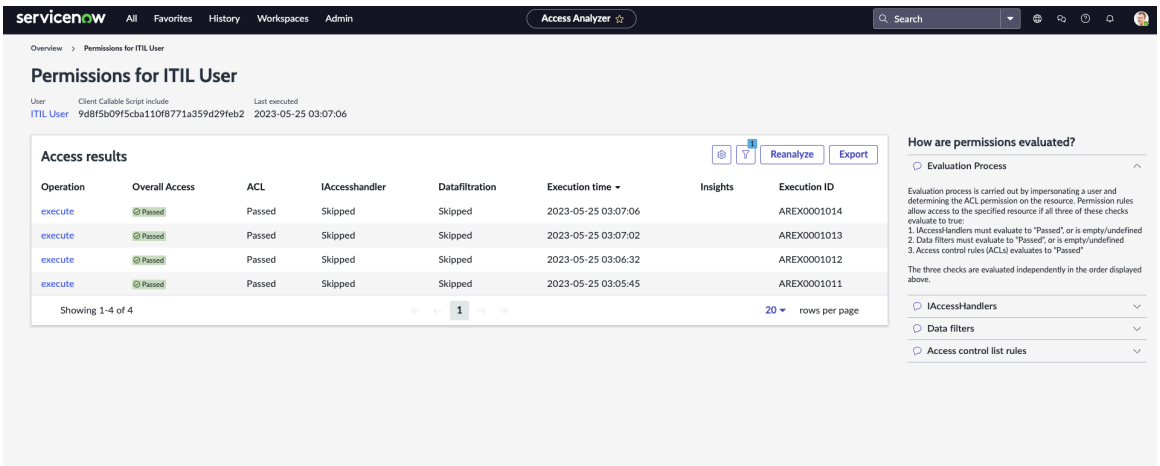
   Les critères recherchés précédemment comportent les sections suivantes :

   - **Évaluer l'accès** : affiche les résultats en fonction des requêtes effectuées via les fonctionnalités **Évaluer l'accès** .
   - **Comparer l'accès des utilisateurs** : affiche les résultats en fonction des requêtes effectuées via les fonctionnalités **Comparer l'accès des utilisateurs** .

   Remarque :
   Les critères précédemment recherchés ne sont pas stockés lors de l'utilisation de la fonctionnalité de comparaison d'enregistrements utilisateur.

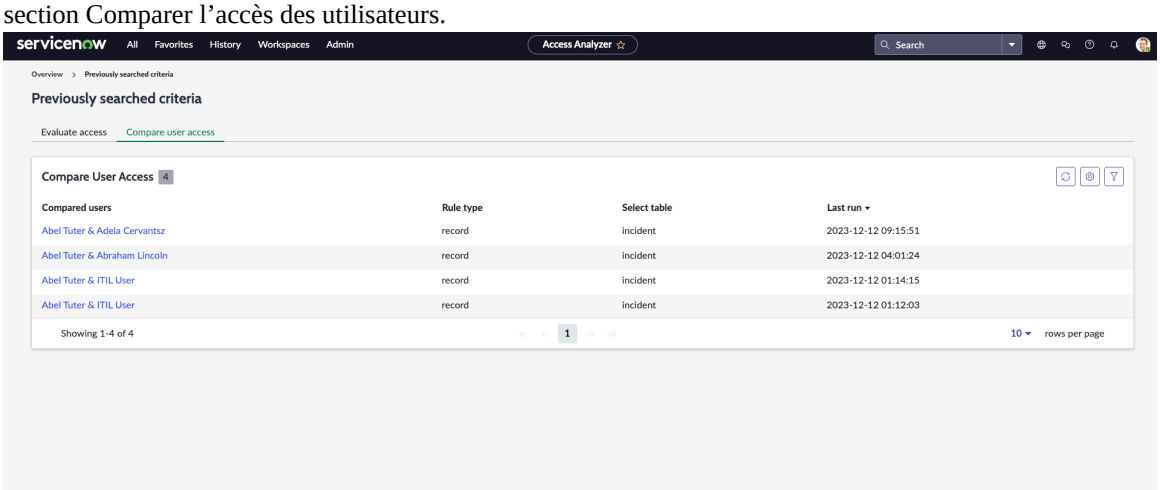


2. Sélectionnez les liens **Analysé par** pour afficher les critères précédemment recherchés dans la section Évaluer l'accès.



Vous pouvez sélectionner **Analyser à nouveau** l'accès pour l'utilisateur. Exportez les détails à l'aide de l'option **Exporter** .

3. Sélectionnez les liens **Utilisateurs comparés** pour afficher les critères précédemment recherchés dans la section Comparer l'accès des utilisateurs.



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 :

- Business rule : une règle métier est un script de 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.
- Filtration 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. Le filtre de données ne prend 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. Au sein d'une ACL, la hiérarchie suivante est évaluée :
  - Rôle
  - Attribut de sécurité
  - Condition
  - Script

Vous pouvez analyser l'accès et les autorisations pour l'utilisateur, le rôle ou le 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 des attributs de rôle et 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.
- **Page d'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
- IAccessHandler
- Filtres de données
- Règles de la liste de contrôle d'accès

Présence d'un script

L'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 examiner la logique de détermination de l’accès, reportez-vous à 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 permettent d’accéder à la ressource spécifiée si les vérifications suivantes sont évaluées comme vraies :

- L’évaluation des IAccessHandler doit retourner la valeur « Réussi », ou est vide ou non définie
- 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 « réussies »

IAccessHandler

Un contrôle du système interne à l’aide du code source masqué sur la plateforme. IAccessHandler peut accorder ou refuser l’accès à une ressource sans évaluer les ACL. Si IAccessHandler est ignoré, les ACL sont évaluées.

Vous ne pouvez pas modifier les vérifications IAccessHandler. 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

Questions fréquemment posées 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 indique l’ordre dans lequel les ACL sont évaluées. L’état indique si l’accès global est accordé (réussi) ou refusé (bloqué).
Comment évalue-t-on les ACL ?	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 Access Analyzer ?	Lors de l’analyse de l’accès et des autorisations, des légendes sont affichées dans le cadre du processus d’évaluation. Les légendes sont les suivantes : • [Réussi] Accès accordé • [Bloqué] Accès refusé • [Ignoré] N’a pas évalué • [Non défini] Aucune règle trouvée
Que signifie l’icône d’alerte dans les résultats d’accès ?	L’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 examiner la logique de détermination de l’accès, reportez-vous à Journaux de débogage d’Analyseur d’accès.
Qu’est-ce que **IAccesshandler** ?	Un contrôle du système interne 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. **IAccessHandler** peut accorder ou refuser

Forum Aux Questions (suite)

Questions	Explication
	l'accès à une ressource sans évaluer les ACL. Si cet **IAccessHandler** est ignoré, les ACL sont évaluées. Vous ne pouvez en aucun cas modifier les vérifications **IAccessHandler** . Par exemple, une **implémentation IAccessHandler** est utilisée pour les contrôles d'accès sur les ressources d'application telles que l'accès en lecture seule.
Qu'est-ce qu'un filtre 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 limités dans le temps affectés à l'utilisateur ici.

Comparer les enregistrements utilisateur

Voici quelques-unes des questions fréquemment posées lors de l'utilisation de la fonctionnalité Comparer l'enregistrement utilisateur dans l'analyseur d'accès :

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 dans lequel l'utilisateur doit être ajouté et ajouter l'utilisateur au groupe.
Qu'est-ce que Afficher la différence uniquement ?	Lorsque vous activez la case à cocher Afficher les différences uniquement, seuls les rôles ou groupes qui sont différents entre l'utilisateur 1 et l'utilisateur 2 s'affichent.

Comparer l'accès des utilisateurs

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 des contrôles 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'affichage des différences uniquement ?	Lorsque vous cochez la case Afficher uniquement les différences, seul l'état d'évaluation de l'opération 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 des listes de contrôle d'accès (ACL) qui restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données. Au sein d'une ACL, la hiérarchie suivante est évaluée : • Rôle • Attribut de sécurité • 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** > **Rôle d'affichage** 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.

Forum Aux Questions (suite)

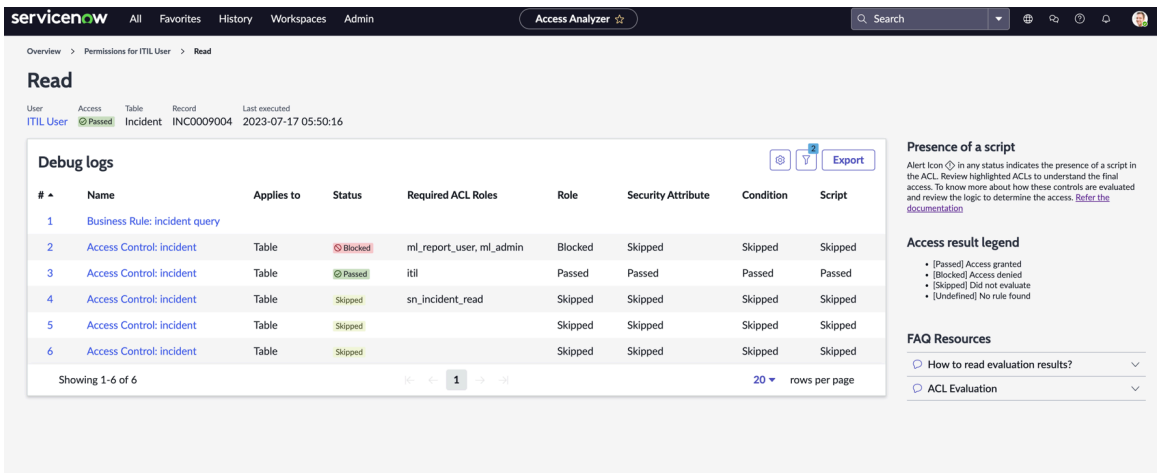
Questions	Explication
Comment puis-je voir les détails du groupe ?	Vous pouvez sélectionner l'icône **Groupe (nœud)** > **Actions supplémentaires** > **Afficher le groupe** détails pour en savoir plus sur le groupe.

Journaux de débogage d'Analyseur d'accès

Les journaux de débogage affichent les détails de l'opération de sélection du résultat d'accès.

Champs dans les journaux de débogage

Les journaux de débogage dans 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.



Voici les champs et leur description dans les journaux de débogage :

Journaux des débogages

Champs	Description
Nom	Les détails sur la règle métier ou l'ACL. Vous pouvez sélectionner la règle métier d'ACL pour plus d'informations.
Concerne	Les détails sur l'application de l'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.
Nécessite une ACL	Rôle requis pour accéder au champ, à l'enregistrement ou à la table.
Rôle	Les détails sur le rôle bloqué, réussi, ignoré pour le contrôle d'accès.
Attribut de sécurité	Les détails sur l'attribut de sécurité Bloqué, Réussi, Ignoré pour le contrôle d'accès.

Journaux des débogages (suite)

Champs	Description
Condition	Le détail de la condition Bloquée, Réussie, Ignorée pour le contrôle d'accès.
Script	Les détails sur le script bloqué, réussi, ignoré pour le contrôle d'accès.
Personnalisé	Détails sur 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 :

- Business rule : une règle métier est un script de 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.
- 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. 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. Au sein d'une ACL, la hiérarchie suivante est évaluée :
  - Rôle
  - Attribut de sécurité
  - Condition
  - Script

Évaluation de la liste de contrôles d'accès

Les ACL pour les opérations sont évaluées dans la séquence comme suit :

- Rôle
- Attribut de sécurité
- Condition
- Script

Présence d'un script

L'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 générique** : au cours de la séquence d'exécution, les ACL héritées sont évaluées en premier, puis les ACL génériques.
- **Une ACL est réussie, 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, à un enregistrement ou à une table pour une identité.
- **Exécution des ACL au niveau du champ et des ACL au niveau de la table** : pendant l'exécution, les ACL au niveau du champ sont exécutées en premier, suivies de l'ACL au niveau de la table pour fournir des résultats plus granulaires lors de l'analyse de l'accès pour une identité.
- **Évaluation en présence d'une ACL scriptée** : lorsqu'un script est présent, l'accès global de l'opération est transmis avec une icône d'alerte pour indiquer le script dans l'ACL.

Identité globale

Global Identity est un ServiceNow® produit qui permet d'identifier des utilisateurs uniques sur plusieurs instances.

L'identité globale permet de gérer les utilisateurs, leurs attributs et d'autres données fondamentales dans plusieurs ServiceNow®ServiceNow® instances.

Explorez l'ID fédéré

Découvrez les principales fonctionnalités et la valeur commerciale de Federated ID.

Accéder à l'ID fédéré

Accéder à l'ID fédéré.

Mise à jour des champs d’ID

Mettez à jour et configurez l’ID fédéré.

Exploration de 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 entre les instances.

L’ID fédéré est utilisé pour identifier les utilisateurs sur l’instance multiple ServiceNow® . L’ID fédéré permet d’identifier l’utilisateur et de déterminer le nombre exact d’utilisateurs sur plusieurs instances. Pour en savoir plus, consultez la section ID fédéré.

Remarque :
Le nom d’utilisateur est requis pour générer des ID fédérés.

L’ID fédéré est un identificateur unique pour une identité à l’aide d’une fonction de hachage dans les ServiceNow® instances.

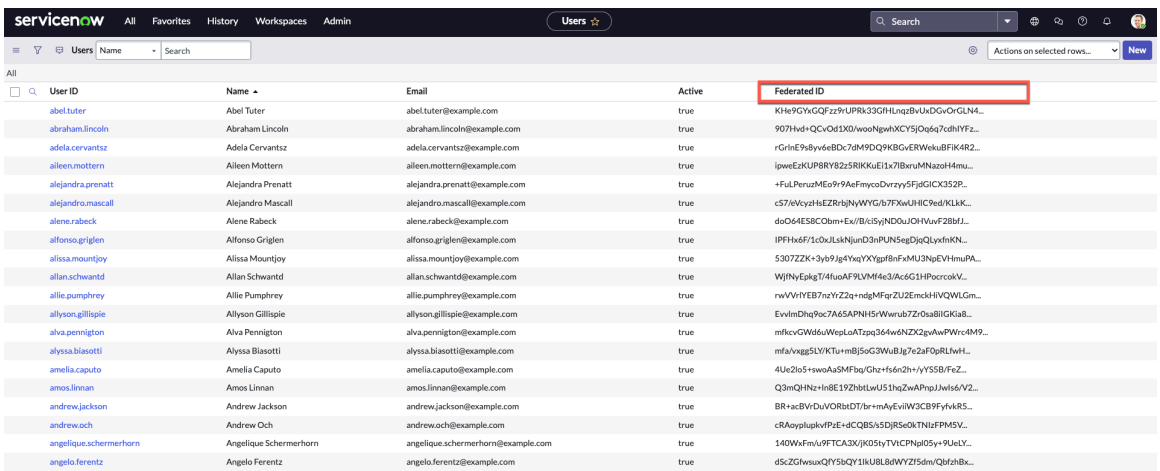
En utilisant **l’ID d’utilisateur** et **l’adresse e-mail** de l’utilisateur dans les instances, l’ID fédéré est créé et affiché dans la table sys_user.

Après la mise à niveau vers la Washington DC version, le module d’extension Génération d’ID fédérés (com.glide.identity.globalid) est installé automatiquement sur toutes les instances.

Traduction automatique

Remarque :

- Le nom d'utilisateur est requis pour générer des ID fédérés.
- Le nom d'utilisateur et l'adresse e-mail sont utilisés pour générer des ID fédérés par défaut. 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.
- Si des utilisateurs ont des noms d'utilisateur et une adresse e-mail en double, l'ID fédéré est généré uniquement pour un seul utilisateur. Si le nom d'utilisateur est nul ou vide, l'ID fédéré est nul.



User ID	Name	Email	Active	Federated ID
abel.tuter	Abel Tuter	abel.tuter@example.com	true	KHe9GYxGQFzz9rUPRk33GfHLnqzBvUxDGvOrGLN4...
abraham.lincoln	Abraham Lincoln	abraham.lincoln@example.com	true	907Hvd+QCvOd1X0/wooNgwhXCY5jOq6q7cdhlYFz...
adela.cervantsz	Adela Cervantsz	adela.cervantsz@example.com	true	rGrlnE9s8yv6eBDc7dM9DQ9KBGvERWekuBFiK4R2...
aileen.mottern	Aileen Mottern	aileen.mottern@example.com	true	ipweEzKUP8RY82z5RIKKuEi1x7lBxruMNazoH4mu...
alejandra.prenatt	Alejandra Prenatt	alejandra.prenatt@example.com	true	+FuLPeruzMEo9r9AeFmycoDvrzyy5FjdGICX352P...
alejandro.mascall	Alejandro Mascall	alejandro.mascall@example.com	true	cS7/eVcyzHsEZRrbjNyWYG/b7FXwUHlC9ed/KLkK...
alene.rabeck	Alene Rabeck	alene.rabeck@example.com	true	doO64ES8CObm+Ex//B/ciSyjND0uJOHVuvF28bfJ...
alfonso.griglen	Alfonso Griglen	alfonso.griglen@example.com	true	IPFHx6F/1c0xJLskNjunD3nPUN5egDjqQLyxfnKN...
alissa.mountjoy	Alissa Mountjoy	alissa.mountjoy@example.com	true	5307ZZK+3yb9Jg4YxqYXYgpf8nFxMU3NpEVHmuPA...
allan.schwantd	Allan Schwantd	allan.schwantd@example.com	true	WjfNyEpkgT/4fuoAF9LVMf4e3/Ac6G1HPocrcokV...
allie.pumphrey	Allie Pumphrey	allie.pumphrey@example.com	true	rwVVrIYEB7nzYrZ2q+ndgMFqrZU2EmckHiVQWLGm...
allyson.gillispie	Allyson Gillispie	allyson.gillispie@example.com	true	EvvlmDhq9oc7A65APNH5rWwrub7Zr0sa8IlGKIa8...
alva.pennigton	Alva Pennigton	alva.pennigton@example.com	true	mfkcvGWd6uWepLoATzpq364w6NZX2gvAwPWrc4M9...
alyssa.biasotti	Alyssa Biasotti	alyssa.biasotti@example.com	true	mfa/vxgg5LY/KTu+mBJ5oG3WuBJg7e2aF0pRLfwH...
amelia.caputo	Amelia Caputo	amelia.caputo@example.com	true	4Ue2lo5+swoAaSMFbq/Ghz+fs6n2h+/yYS5B/FeZ...
amos.linnan	Amos Linnan	amos.linnan@example.com	true	Q3mQHNz+ln8E19ZhbtLwU51hqZwAPnpJJwls6/V2...
andrew.jackson	Andrew Jackson	andrew.jackson@example.com	true	BR+acBVrDuVORbtDT/br+mAyEviIW3CB9FyfvkR5...
andrew.och	Andrew Och	andrew.och@example.com	true	cRAoyplupkvfPzE+dCQBS/s5DjRSe0kTNIzFPM5V...
angelique.schermerhorn	Angelique Schermerhorn	angelique.schermerhorn@example.com	true	140WxFm/u9FTCA3X/jK05tyTVtCPNpl05y+9UeLY...
angelo.ferentz	Angelo Ferentz	angelo.ferentz@example.com	true	dScZGfwsuxQfY5bQY1lkU8L8dWYZf5dm/QbfzhBx...

Les changements de schéma après l'installation du module d'extension sont les suivants :

- Une nouvelle federated_id de colonne est créée dans la table sys_user .
- Nouvelle table : iamsync_type est remplie automatiquement 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 complètent la table sys_user.

Après la mise à niveau vers la Washington DC version, le module d'extension Génération d'ID fédérés (com.glide.identity.globalid) est installé automatiquement sur toutes les instances.

Accéder aux critères d'ID fédéré

Accédez aux critères d'ID fédéré pour connaître les champs d'ID utilisés pour générer l'ID fédéré.

Avant de commencer

Rôle requis : iamsync_admin

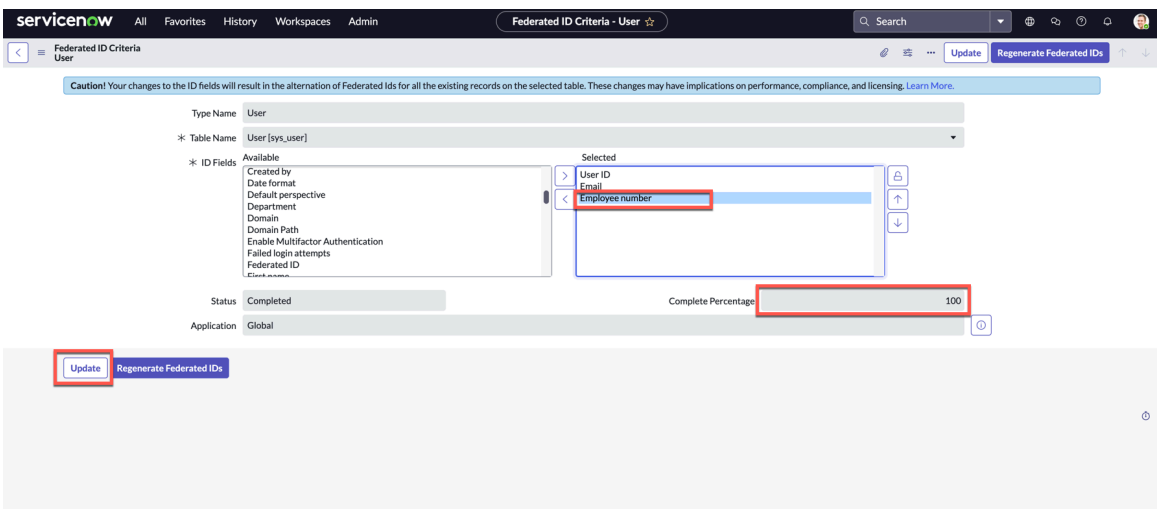
Procédure

1. Accédez à la **Tous** > **Gérer l'ID fédéré** > **Critères d'ID fédéré**.
2. La page Critères d'ID fédérés affiche l'enregistrement avec les détails suivants :

- Nom du type : **utilisateur**
- Nom de 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 de l'ID fédéré). 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'adresse e-mail sont utilisés pour générer des ID fédérés par défaut.



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 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 :
Toute modification des 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 l'octroi de licences.

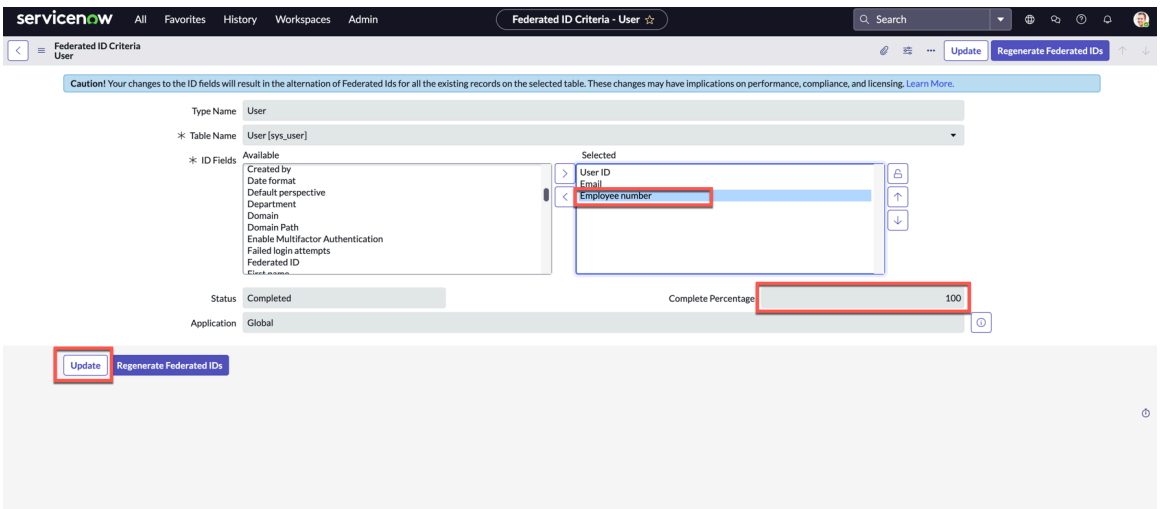
Procédure

1. Accédez à la **Tous** > **Gérer l'ID fédéré** > **Critères d'ID fédéré**.
2. Sélectionnez le nom de type (**Utilisateur**).
3. Sélectionnez les nouveaux champs d'ID dans la page Utilisateur des critères d'ID fédérés que vous souhaitez ajouter à partir de Disponible à Sélectionné à l'aide des boutons fléchés.

Par exemple, **Numéro d'employé**.

Remarque :

- Le nom d'utilisateur est requis pour générer des ID fédérés.
- Le nom d'utilisateur et l'adresse e-mail sont utilisés pour générer des ID fédérés par défaut.
- Si des utilisateurs ont des noms d'utilisateur et une adresse e-mail en double, l'ID fédéré est généré uniquement 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 de niveau système
  - Champs Chiffrement Edge
  - Champs de mot de passe.

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 ou si l'instance ne fonctionne pas correctement. Si vous sélectionnez **Régénérer les ID fédérés**, les ID de tous les utilisateurs sont régénérés à l'aide des critères du champ d'ID actuels.

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 d'Identity and Access Audit.

Configurer

Apprenez à configurer l'audit d'identité et d'accès.

Traduction automatique

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 d'utilisateurs, les groupes et les rôles.

Permet de détecter les utilisateurs malveillants et de suivre les activités inhabituelles dans l'instance, tout en respectant 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 basculant la propriété systèmeglide.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 :

- Consultez les modifications apportées au cours des 30 derniers jours aux utilisateurs, groupes, attributs ACL de rôle, appartenances à des rôles, appartenances à des groupes et rôles ACL.
- Suivez les changements dans votre ServiceNow instance.
- Contribuez à atténuer les risques potentiels en matière de sécurité et de réglementation.
- Démontrer la conformité avec les auditeurs de différents groupes au sein de l'organisation.
- Démontrez que l'organisation n'est pas vulnérable aux menaces liées à un manque de visibilité sur les changements de groupe d'utilisateurs et de rôles.

Profils d'utilisateur dans Identité, accès et audit

Voici les différents profils d'utilisateur dans l'audit d'identité et d'accès :

- **Administrateur** : consulter 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 modifiez 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 d'audit d'identité et d'accès

Identity and Access Audit comporte 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 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.

Résultats d'audit

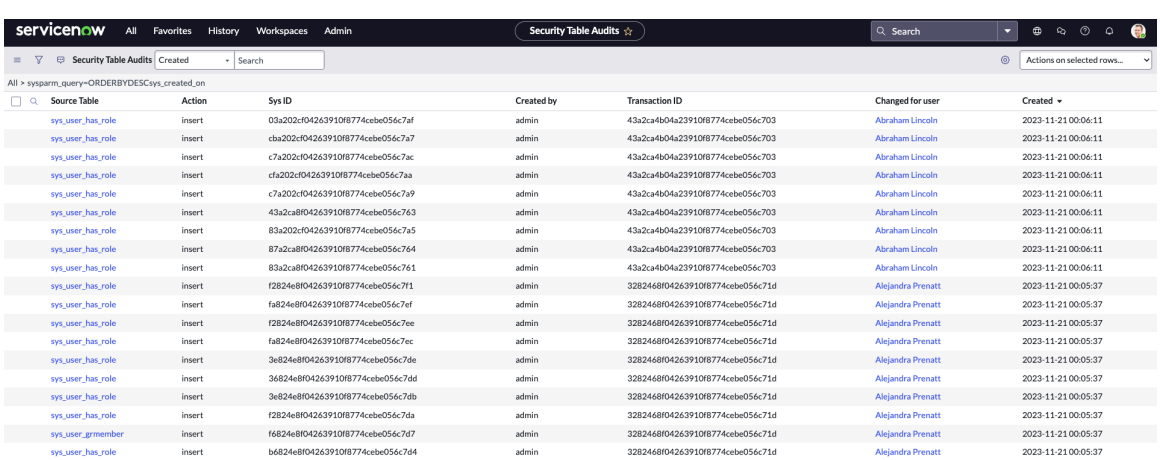
Affiche les audits qui se sont produits dans l'instance ServiceNow® .

Résultats d'audit affiche les changements apportés aux utilisateurs, groupes, rôles et ACL de 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 d'audit.
Sys_id	Détails sur la 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 de l'audit particulier effectué.
Utilisateur concerné par le changement	Nom de l'utilisateur au moment de l'audit.
Créé	Date et heure auxquelles l'audit a été effectué.



Pistes d'utilisateurs

Affiche les audits des utilisateurs dans 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.

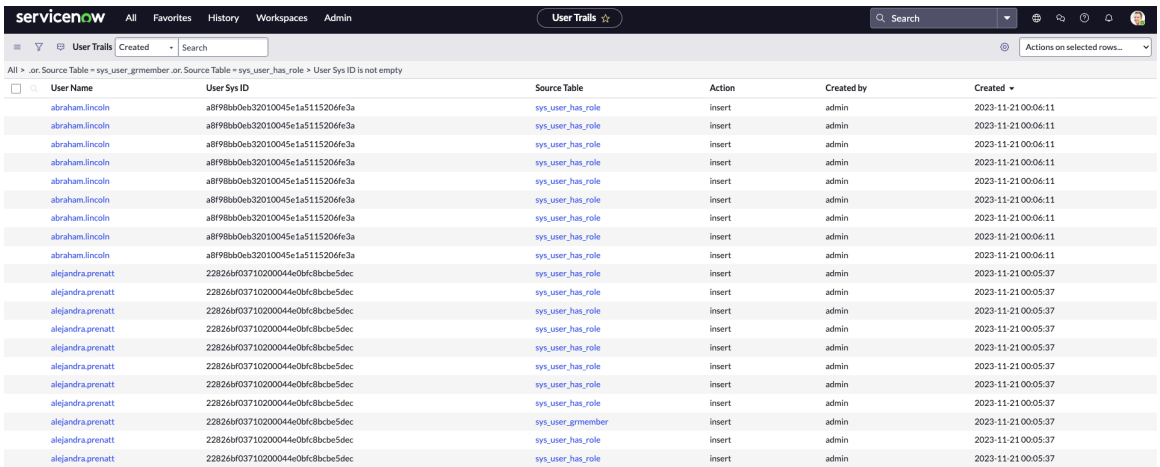
Pour accéder aux pistes d'utilisateurs, accédez à **Tous** > **Sécurité de système** > **Audit d'identité et d'accès** > **Pistes d'utilisateurs**. La page Parcours d'utilisateurs s'affiche avec les informations suivantes.

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.

Pistes d'utilisateurs (suite)

Action	Décrit l'action d'audit.
Créé par	Utilisateur qui a effectué le changement.
Créé	Date et heure auxquelles l'audit a été effectué.



Pistes de groupes

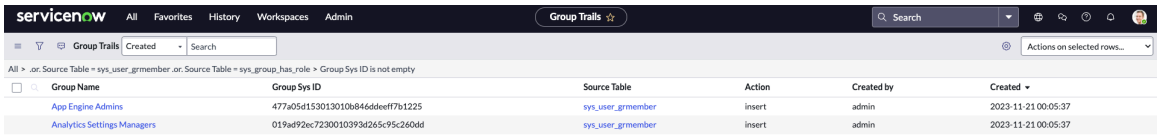
Affiche les audits des groupes dans l'instance ServiceNow® .

Les pistes de groupe affichent les changements d'attributs, les changements d'adhésion et les changements de rôles pour 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 de l'enregistrement audité.
Table source	Détails sur la table source où l'audit a été effectué.
Action	Décrit l'action d'audit.
Créé par	Utilisateur qui a effectué le changement.
Créé	Date et heure auxquelles l'audit a été effectué.



Pistes des rôles

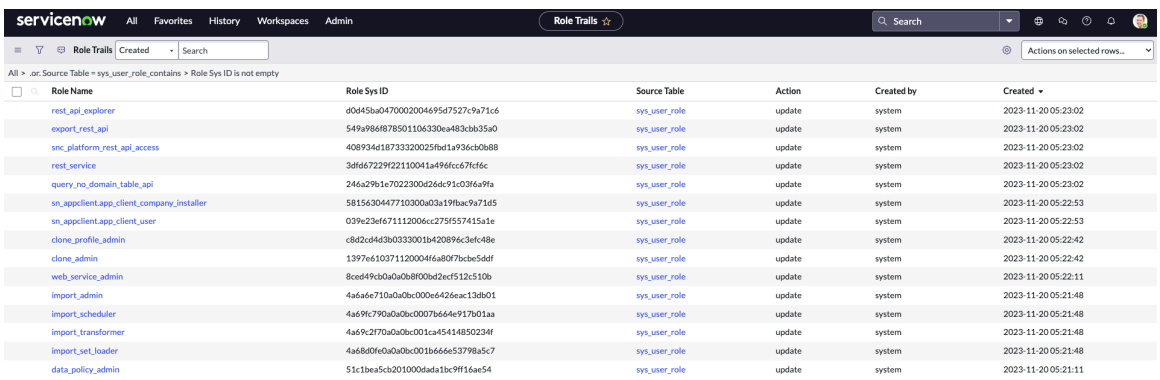
Affiche les audits des rôles dans l'instance ServiceNow® .

Les pistes de rôles 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 de rôles s'affiche avec les informations suivantes.

Pistes des rôles

Nom de rôle	Nom du rôle.
ID système du rôle	Détails sur la sys_id de rôle de l'enregistrement audité.
Table source	Détails sur la table source où l'audit a été effectué.
Action	Décrit l'action d'audit.
Créé par	Utilisateur qui a effectué le changement.
Créé	Date et heure auxquelles l'audit a été effectué.



Pistes ACL

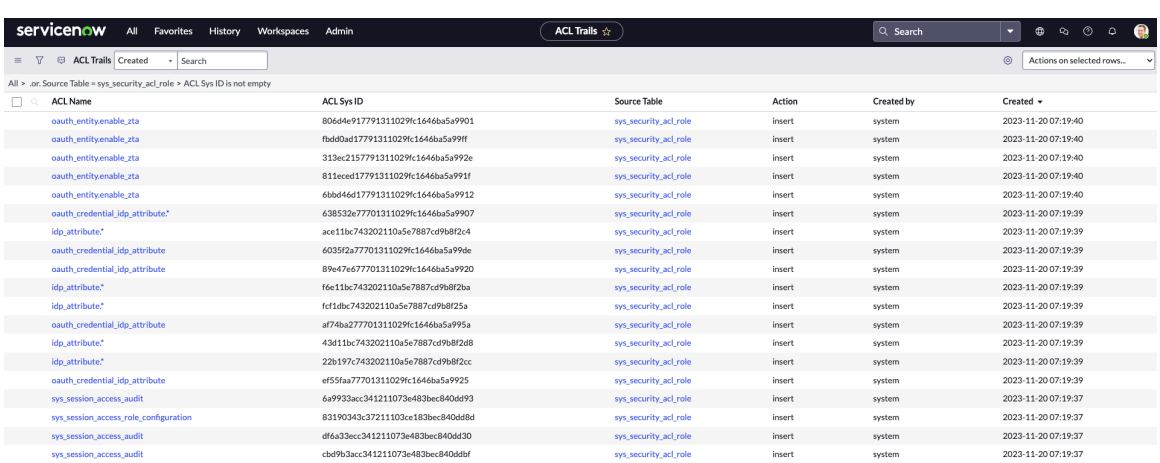
Affiche les audits des ACL dans l'instance ServiceNow® .

Les pistes d'ACL affichent les changements d'attribut et les changements de relation de rôle requis pour une 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 d'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 d'audit.
Créé par	Utilisateur qui a effectué le changement.
Créé	Date et heure auxquelles l'audit a été effectué.



Champs auditables de sécurité

Affiche les détails au niveau de la table et du champ qui seront audités dans l'instance ServiceNow® .

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.
Liste des champs	L'audit sera effectué pour les champs spécifiés dans la liste.

Champs auditables de sécurité (suite)

Nom de colonne	Description
Créer	Auditez les changements associés à l'opération Créer.
Mettre à jour	Auditez les changements associés à l'opération Mettre à jour.
Supprimer	Auditez les changements associés à l'opération de suppression.
Actif	Auditez uniquement si la configuration de la table est active.

Table to Audit	Audit Storage Destination	Field list	Create	Update	Delete	Active
sys_user_group	Database	name,active	false	true	true	true
sys_group_has_role	Database	group,role	true	false	true	true
sys_user_has_role	Database	user,role	true	false	true	true
sys_user_role	Database	name,suffix,grantable,elevated_privilege	false	true	true	true
sys_security_acl	Database	name,active,operation	false	true	true	true
sys_security_acl_role	Database	sys_security_acl,sys_user_role	true	false	true	true
sys_user_role_contains	Database	role,contains	true	false	true	true
sys_user	Database	user_name,active,user_password	false	true	true	true
sys_user_grmember	Database	group,user	true	false	true	true

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 une ACL.

Avant de commencer
Rôle requis : security_admin

Vous devez élever votre rôle au rang 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 :

- Groupe [sys_user_group]
- Rôle [sys_user_role]

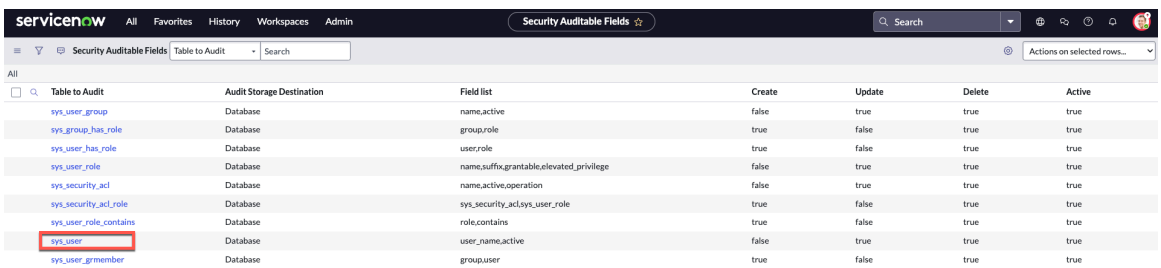
- Contrôle d’accès [sys_security_acl]
- Utilisateur [sys_user]
- Rôle de groupe [sys_group_has_role]
- Rôle d’utilisateur [sys_user_has_role]
- Rôles d’accès [sys_security_acl_role]
- Rôle contenu [sys_user_role_contains]
- Membre du groupe [sys_user_grmember]

Remarque :
Pour savoir quels champs peuvent être configurés pour les tables, reportez-vous à Champs pris en charge et non pris en charge pour l’accès à l’identité et l’audit.

Procédure

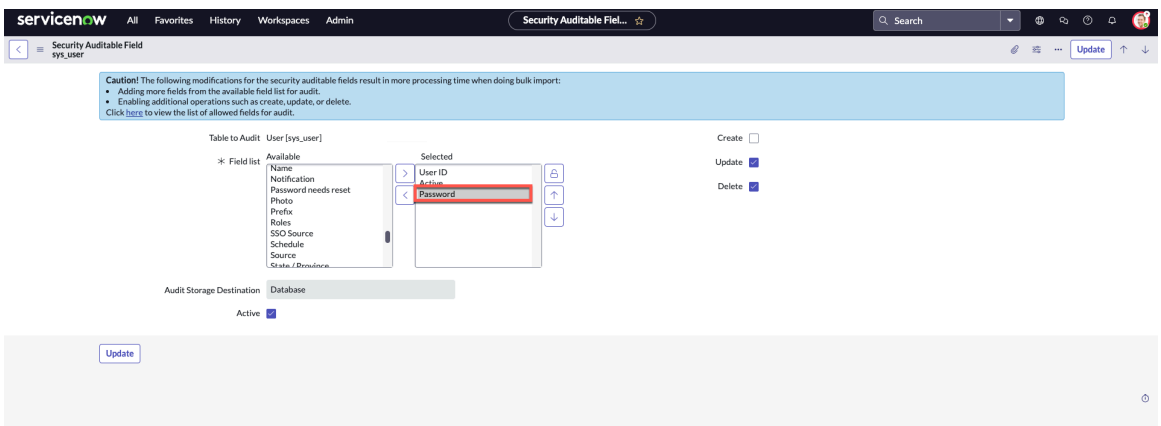
1. Accédez à la **Tous** > **Sécurité de système** > **Audit d'identité et d'accès** > **Configurer les tables et les champs**.
2. Sélectionnez la table à partir de laquelle vous souhaitez auditer un champ.

   Par exemple, **sys_user**.



3. Ajoutez le champ à auditer.

   Par exemple, **Mot de passe**.



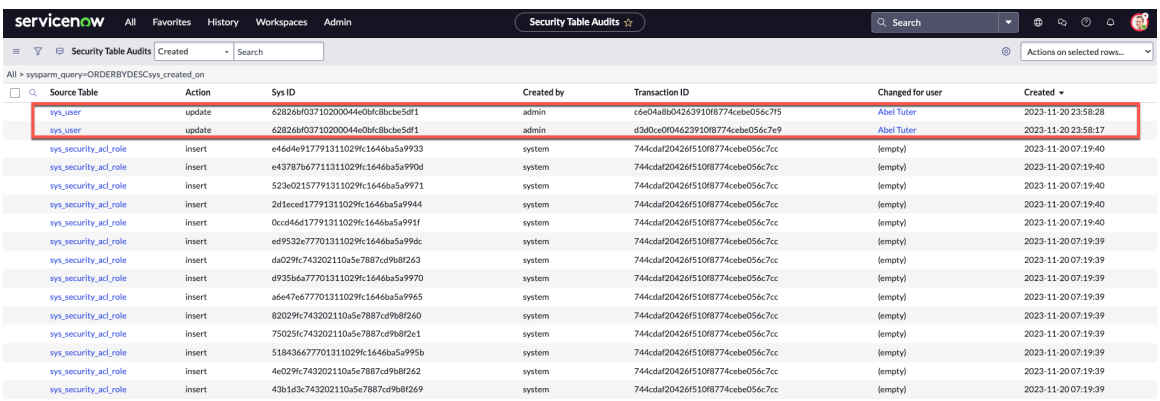
Traduction automatique

Remarque :
Les modifications suivantes apportées aux champs auditables de sécurité entraînent une augmentation du temps de traitement lors de l'importation en bloc :

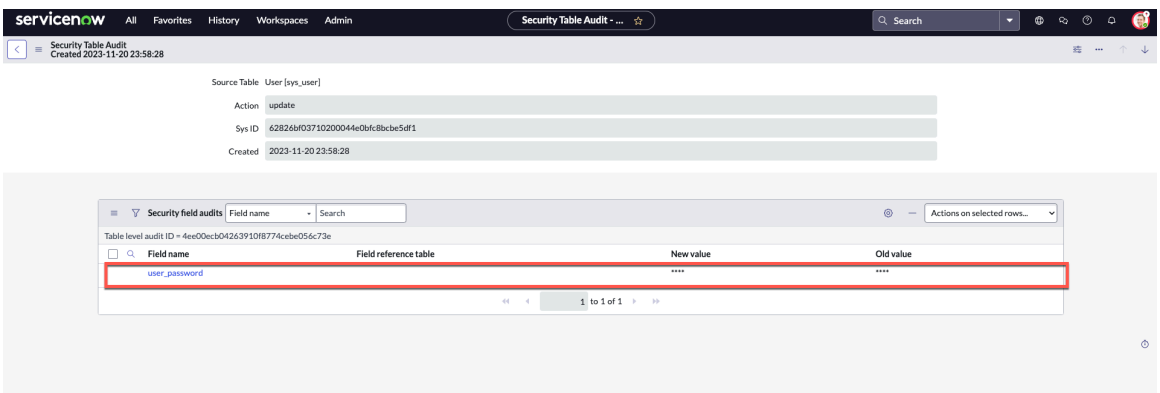
- Ajouter d'autres champs à partir de la liste de champs disponibles pour l'audit.
- Activation d'opérations supplémentaires telles que créer, mettre à jour ou supprimer.

4. Mettez à jour l'enregistrement.

Tout changement apporté au champ mot de passe ajoute un nouvel enregistrement aux audits de la table de sécurité. Dans cet exemple, l'audit affiche un champ de mot de passe modifié pour l'utilisateur **Abel Tuter**.



La sélection de l'enregistrement créé affiche les détails des modifications.



Configurer la période de conservation

Configurez la période de conservation pour l'audit d'identité et d'accès.

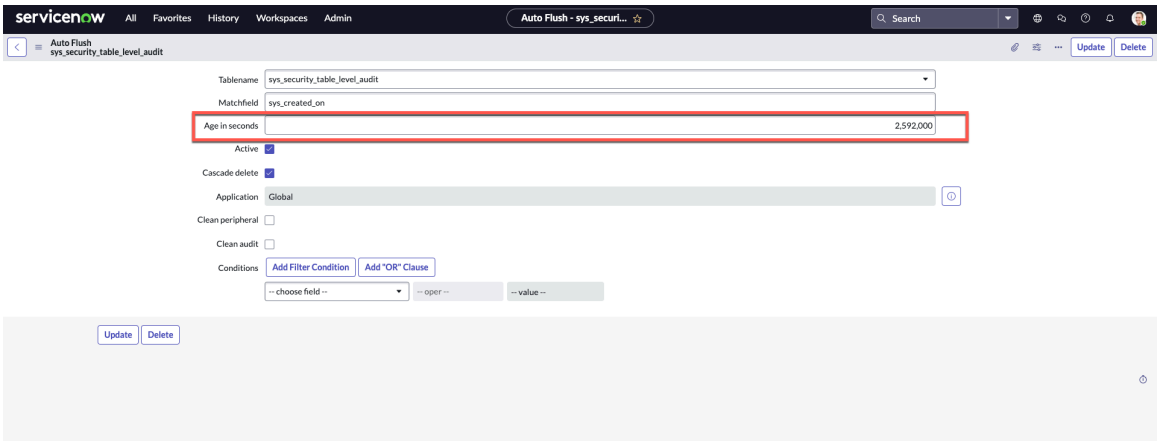
Avant de commencer

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).



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 pour l'accès à l'identité et l'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 des champs de sécurité (sys_sec_field_audit_config).

Champ pris en charge ou non 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) • Équipement de dernière connexion (last_login_device)

Champ pris en charge ou non 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) • Réinitialisation du mot de passe requise (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 changements (sys_mod_count)

Identity Center

Vous permet de surveiller, de gérer et de minimiser les risques et les failles de sécurité liés à l'identité.

Explorer

Découvrez les fonctionnalités et la valeur commerciale d’Identity Center.

Activer

Découvrez comment activer Identity Center.

Mesures d’identité pour les administrateurs

Découvrez comment les autorisations sont évaluées.

Identity Center pour les utilisateurs

Obtenez des détails sur les questions fréquemment posées à propos d’Access Analyzer.

Traduction automatique

Explorer Identity Center

Identity Center est une collection 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 et les failles de sécurité liés à l'identité.

Identity Center est un guichet unique pour surveiller, gérer et réduire les risques et les failles de sécurité liés à l'identité 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 afin d'afficher les détails des sessions actives, de l'historique de connexion et des appareils approuvés 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. Trouvez 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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

Identity Center pour les utilisateurs

Affichez les détails de vos sessions actives, de votre historique de connexion et de vos appareils approuvés avec Identity Center.

Identity Center est une collection d'attributs d'utilisateur, d'appareils, d'historique de connexion, d'activité de sécurité et bien plus encore. Il fournit une vue à volet unique de toutes les données avec des contrôles de sécurité et des options de notification supplémentaires.

Avec Identity Center, vous pouvez afficher les détails de vos sessions actives, de votre historique de connexion et de vos appareils approuvés.

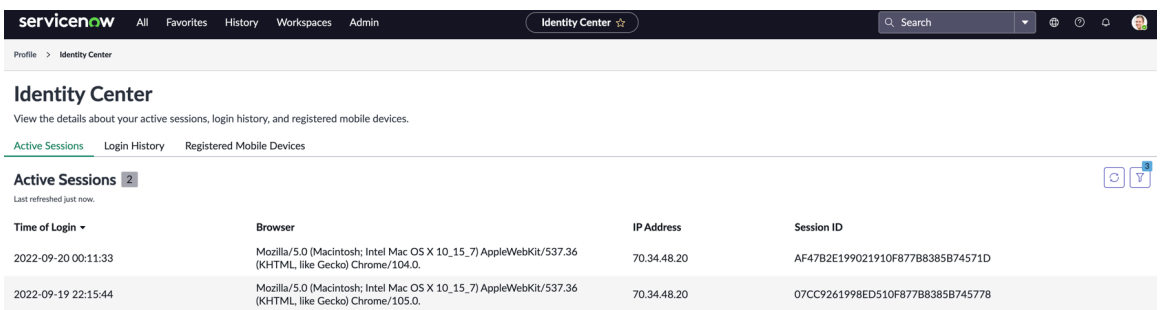
Pour accéder à Identity Center pour les utilisateurs, accédez à l'un des modules suivants :

- Sur Now Platform, accédez à **Tous** > **Libre-service** > **Mon profil** et sélectionnez **Afficher Identity Center** sous 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 :

- Sessions actives
- Historique de connexion
- Équipements mobiles enregistrés

Vous pouvez sélectionner ces onglets pour afficher des détails tels que le navigateur, les destinataires IP, les informations de relation de session, les informations de connexion, vos équipements mobiles enregistrés.

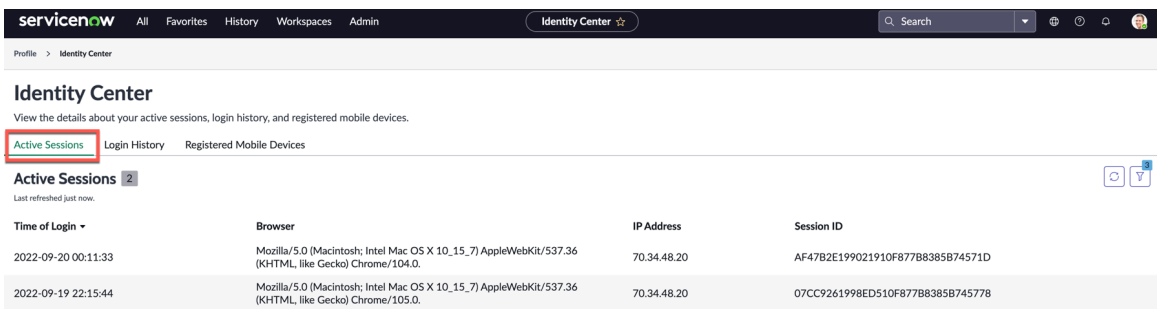
Afficher les sessions actives

Affiche les informations sur les sessions utilisateur.

Les sessions actives sont les sessions qui sont ouvertes sur l'instance actuelle ServiceNow® avec différents navigateurs ou appareils.

L'onglet Sessions actives d'Identity Center vous permet d'identifier vos sessions en fonction du navigateur, de l'adresse IP et de l'ID de sessions. Ces informations vous permettent de prendre les mesures nécessaires, telles que la prolongation ou l'arrêt de la session.

L'utilisation de ces informations peut aider à déterminer si les sessions sont réelles et ne posent pas de problème de sécurité.



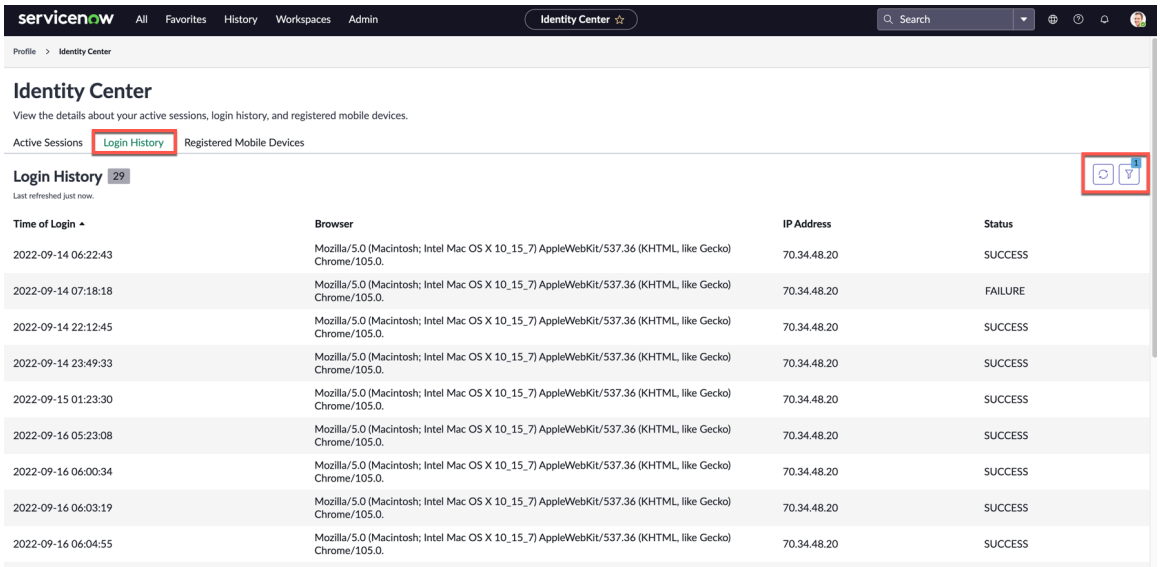
Afficher l'historique de connexion

Fournit des détails sur votre historique de connexion.

L'onglet Historique de connexion d'Identity Center vous aide avec 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.



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.

Afficher les équipements mobiles enregistrés

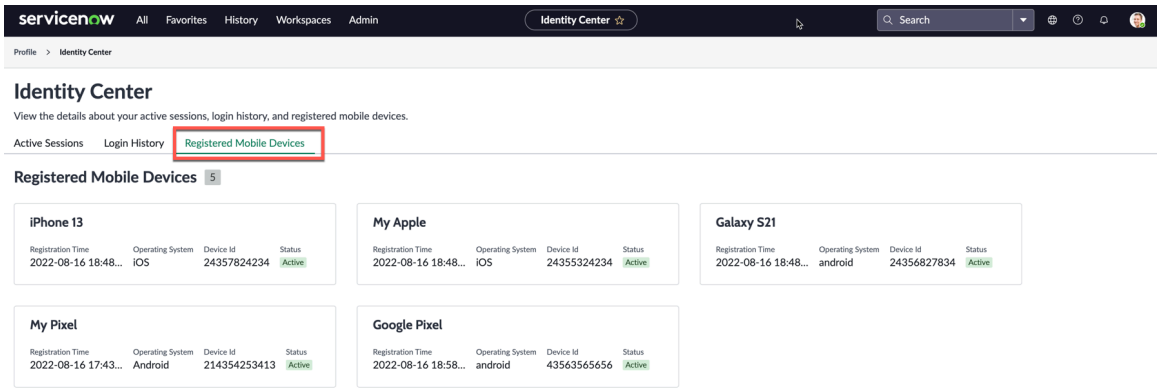
Fournissez des détails sur votre mobile enregistré sur l'instance ServiceNow .

L'onglet Équipements mobiles enregistrés d'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 appareil mobile enregistré l'est également, Identity Center affiche les détails de vos appareils enregistrés.

En outre, il affiche également les détails des 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 Adaptive Authentication (`com.snc.adaptive_authentication`) est installé et que vous avez activé la fonctionnalité Application mobile de confiance. Pour plus d'informations, consultez Activer l'application mobile de confiance.



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 comptes non humains
- Sessions actives
- Sessions inactives

Pour en savoir plus, consultez Mesures du Centre de sécurité.

Système de gestion des identités inter-domaines (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 les utilisateurs et les groupes à l’aide du protocole SCIM.

Traduction automatique

Fournisseur SCIM

Le fournisseur SCIM synchronise les changements apportés aux identités dans l'IdP, 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 conformes à SCIM.

Le protocole SCIM est un protocole basé sur HTTP au niveau de l'application basé sur la norme HTTP (RFC7230). Utilisez cette API pour mettre en service et gérer les données d'identité, telles que les utilisateurs et les groupes. Utilisez l'API sur le Web et dans des environnements inter-domaines, tels que des fournisseurs de services d'entreprise à cloud ou des scénarios inter-cloud.

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 l'API System for Cross-domain Identity Management (SCIM).

Fournisseur SCIM

Le fournisseur de service met en service les utilisateurs et les groupes à l'aide de l'API SCIM.

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

Exploration du fournisseur SCIM

Le fournisseur de service met en service les utilisateurs et les 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 des utilisateurs et des groupes.

Le fournisseur SCIM synchronise les changements apportés aux identités dans l'IdP, 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 à l'annuaire 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 pour le fournisseur SCIM

Pour configurer le fournisseur SCIM, procédez comme suit :

- Activez le module d'extension **SCIM v2 - ServiceNow Cross-domain Identity Management** . Pour en savoir plus, reportez-vous à Activation du module d'extension SCIM.
- Activez les autres modules d'extension qui sont 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, dans lequel l'scmin_admin peut ajouter ou mettre à jour des informations à caractère personnel (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 .

Activation du module d'extension SCIM

Pour activer 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. Trouvez 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.

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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

Didacticiel : Configurer SCIM pour le provisionnement d'utilisateurs avec Azure AD

La configuration d'Azure AD pour SCIM met en service et désapprovisionne automatiquement les utilisateurs et les groupes à ServiceNow l'aide du service d'approvisionnement Azure AD.

Avant de commencer

Installer 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, dans lequel l'scmin_admin peut ajouter ou mettre à jour des informations à caractère personnel (PII).

Pourquoi et quand exécuter cette tâche

Vous pouvez mettre en service des utilisateurs à l'aide de SCIM par les méthodes d'authentification suivantes :

- Authentification de base
- OAuth

Mise en service de l'utilisateur à l'aide de l'authentification de base

La configuration d'Azure AD pour SCIM met en service et désapprovisionne automatiquement les utilisateurs et les groupes à ServiceNow l'aide du service de mise en service Azure AD à l'aide de l'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, dans lequel l'scmin_admin peut ajouter ou mettre à jour des informations à caractère personnel (PII).

- Activer le module d'extension SCIM

Procédure

1. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès REST API** pour vérifier les détails des politiques d'accès des REST APIs.
2. Sur la page Politique d'accès à l'API, cliquez sur l'enregistrement **Politique d'API SCIM** .

3. Vérifiez que l'enregistrement **d'authentification de base de l'API SCIM** est disponible dans les sections Profils d'authentification.
4. Vérifiez si le champ **Authentification de base** est spécifié avec l'enregistrement **d'API SCIM** qui a été précédemment configuré ou vérifié en tant que registre d'application.
5. Connectez-vous au portail Azure .
6. Accédez à la **Applications d'entreprise** > **Toutes les applications**.
7. Dans la liste des applications, sélectionnez ServiceNow ou créez une ServiceNow application.
8. Sélectionnez l'onglet Mise en service et définissez le mode de mise en service sur **Automatique**.
9. Dans la section Informations d'identification de l'administrateur, spécifiez les éléments suivants :
   - Méthode d'authentification : authentification de base
   - Nom d'instance
   - Nom d'utilisateur d'administrateur
   - Mot de passe de l'administrateur
10. Sélectionnez Test de la connexion pour vous assurer qu'Azure AD 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

La configuration d'Azure AD pour SCIM met en service et désapprovisionne automatiquement les utilisateurs et les groupes à l'aide ServiceNow du service d'approvisionnement Azure AD à l'aide d'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, dans lequel l'scmin_admin peut ajouter ou mettre à jour des informations à caractère personnel (PII).

- Activer le module d'extension SCIM

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Registre d'application**.
2. Sur 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 des REST APIs.
5. Sur la page Politique d'accès à l'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** qui a été précédemment configuré ou vérifié en tant que registre d'application.
8. Connectez-vous au portail Azure .
9. Accédez à la **Applications d'entreprise** > **Toutes les applications**.
10. Dans la liste des applications, sélectionnez ServiceNow ou créez une ServiceNow application.
11. Sélectionnez l'onglet Mise en service et définissez le mode de mise en service sur **Automatique**.
12. Dans la section Informations d'identification de l'administrateur, spécifiez les éléments suivants :
    - Méthode d'authentification : OAuth.

      Remarque :
      Pour remplir l'OAuth déposé pour mise en service avec SCIM, vous devez mettre à jour l'application vers le point de terminaison SCIM 2.0. Pour en savoir plus sur la mise à jour, consultez la documentation Azure .

    - Nom d'instance
    - Nom d'utilisateur d'administrateur
    - Mot de passe de l'administrateur
13. Sélectionnez Test de la connexion pour vous assurer qu'Azure AD 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 API REST non valide

Action : entrez une URL d'API valide. Serait en mesure de recouper l'URL REST API dans **l'explorateur d'API REST**.

Aucune URL de redirection n'est définie dans l'instance ServiceNow

Action : Entrez une URL de redirection valide pour l'entité SCIM OAuth 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 demande.

Action : la **« 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 » etServiceNow « URL de redirection »

Lorsqu'un secret client non valide est transmis

Action : la valeur saisie dans « Secret client » doit être identique à celle de l'entité OAuth configurée dans ServiceNow.

Lorsqu'un « ClientId » non valide a été transmis dans Azure « Authorization EndpointPoint »

Action : la valeur saisie pour le paramètre « client_id » dans « Point de terminaison d'autorisation » doit être identique à celle de 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 :

- Prise en charge des champs personnalisés sur les tables sys_user et sys_user_group grâce à la génération dynamique de schémas d'extensions.
- Fournissez la possibilité de remplacer les mappages SCIM par défaut.

Un administrateur SCIM peut définir des schémas d'extension personnalisés pour les ressources d'utilisateurs et de groupes. Les attributs définis dans le schéma d'extension personnalisé peuvent être mappés aux champs des tables sys_user ou sys_user_group.

Configurations pour 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 SCIMreportez-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, consultez l'étape 5Créer une définition SCIM ETLdu .
- Envoyez des attributs de schéma personnalisés 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, tels que définis dans le mappage.

Propriétés et schémas de personnalisation SCIM

La personnalisation SCIM comprend 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.id.conflict`	Résoudre les ressources SCIM en fonction de la définition source du client demandeur si plusieurs

Propriétés (suite)

Nom	Description
	ressources sont trouvées avec un filtre SCIM d'ID externe. **Remarque :** Comme 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	Journalisation détaillée pour les définitions RTE d'utilisateur et de groupe SCIM.
com.snc.integration.scim2.string.field.validation.enabled	Validation de longueur pour les champs. Cette propriété active la validation au lieu de tronquer et d'enregistrer le champ.
com.snc.integration.scim2.provider.customization.script	ID du script pour personnaliser les 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 des ressources.		nom.middleName
urn:ietf:params:scim:schemas:extension:servicenow:2.0:User	Inclut les attributs associés à ServiceNow.		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 ServiceNow du schéma d'extension.	Personnalisation	personnalisé.social

Schéma non pris en charge

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User: inclut les attributs couramment utilisés pour représenter les utilisateurs qui appartiennent à une entreprise ou agissent en son nom.

Remarque :
Le schéma d'entreprise est un schéma valide, mais ses attributs sont mappés à n'importe quelle table. Étant donné que la persistance de la base de données n'est 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 aux champs qui ne sont pas mappés dans le cadre du schéma principal ou du schéma d'extension ServiceNow .

Avant de commencer
Rôle requis : scim_admin

Avertissement :
Accordez ce rôle avec soin. Le rôle scim_admin équivaut à attribuer à l'utilisateur le rôle administrateur, où le rôle scmin_admin peut insérer de nouveaux enregistrements dans les tables afin de contourner la logique métier ou la protection ACL.

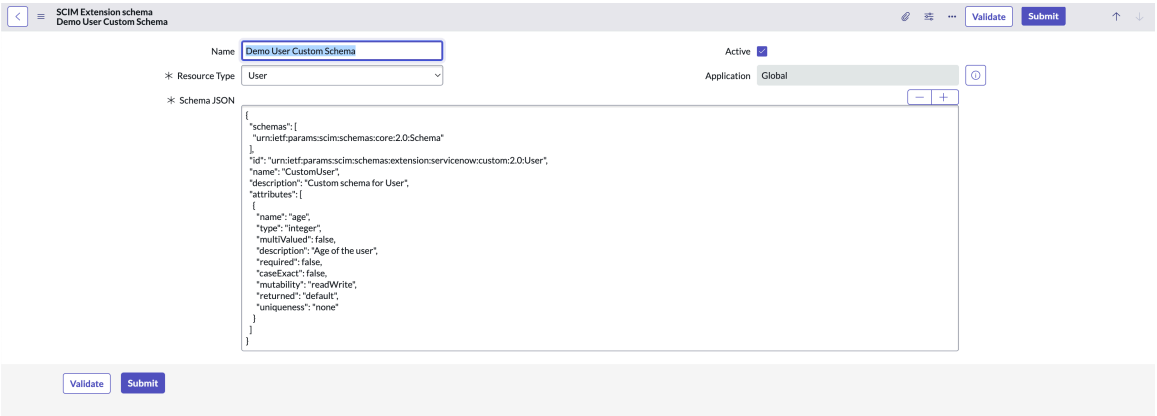
Procédure

1. Accédez à la **Tous** > **SCIM** > **Schémas d'extension SCIM**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Remarque :
Un seul schéma d'extension peut être mappé au champ **Type de ressource** . Par exemple, l'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 d'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, qu'il s'agisse du type Utilisateur ou Groupe.
Type de ressource	Type de ressource qui doit être mappé au schéma d'extension. 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 d'extension avec des attributs personnalisés associés au type de ressource Utilisateur ou Groupe est créé. Utilisez les définitions SCIM ETL pour mapper les ressources en fonction du schéma d'extension sur 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 sur les 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 attribuer à l'utilisateur le rôle administrateur, où le rôle scmin_admin peut insérer de nouveaux enregistrements dans les tables afin de contourner la logique métier ou la protection ACL.

Remarque :

- Les définitions de groupe SCIM et d'utilisateur SCIM ETL font partie du système de base pour le mappage des ressources. Vous pouvez utiliser les mêmes mappages de ressources et modifier les critères au besoin, ou créer de nouveaux mappages de ressources.
- Il n'existe aucune prise en charge des champs [*] via RTE dans le mappage SCIM.

Procédure

1. Suivez les instructions dans les définitions Créer une charge de transformation d'extraction (ETL).
2. Ouvrez l'enregistrement nouvellement créé et consultez 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 utilisateur (sys_user) ou 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.

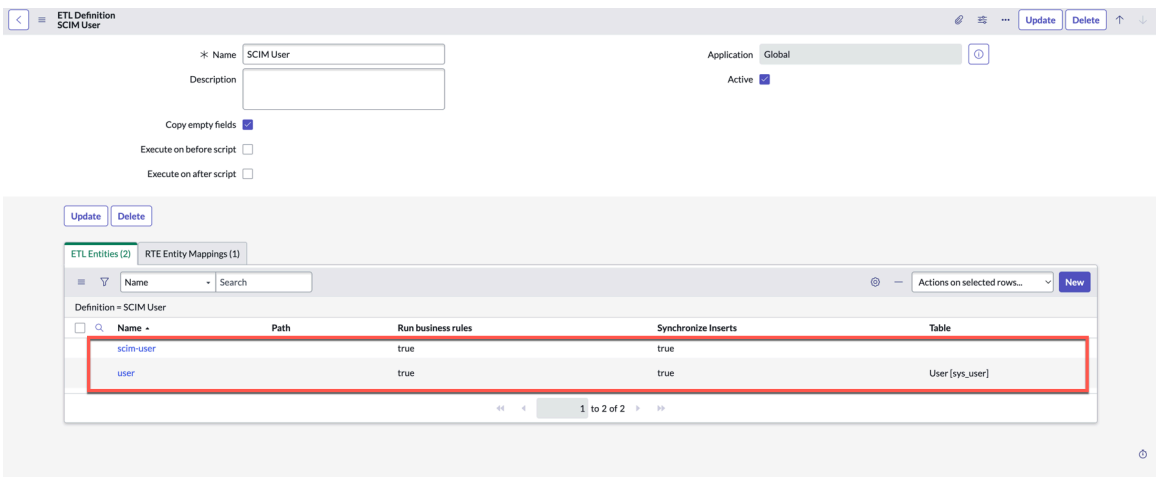
a. Renseignez les champs du formulaire.

Formulaire Entité ETL

Champ	Description
Nom	Nom de l'entité ETL.
Application	Le périmètre de l'application pour cet enregistrement.
Table	Table cible de 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 [*]. Cette exigence s'applique aux entrées intermédiaires et à l'entité de table cible.
Synchroniser les insertions	Option permettant de garantir un seul enregistrement avec des valeurs de champ fusionnées uniques en synchronisant les insertions d'enregistrement.
Exécuter les règles métier	Option pour 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'entités RTE.



4. Créez les entités et mappez-les.

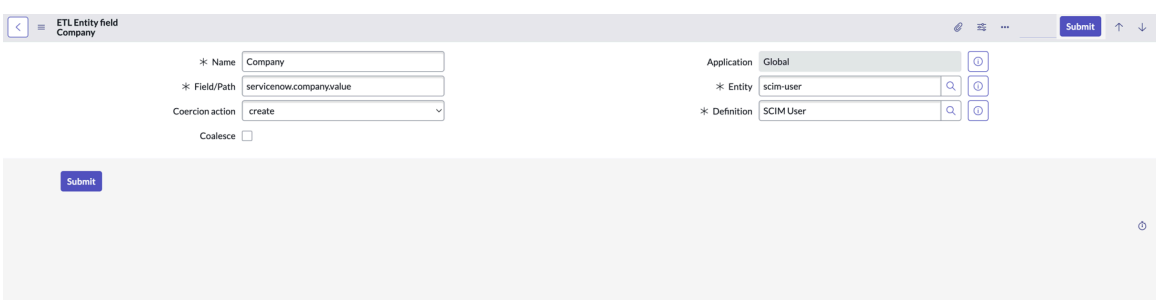
a. Ouvrez l'enregistrement soumis (scim-user et utilisateur).

b. Dans les champs Entité ETL, ajoutez les champs en cliquant sur **Nouveau**.

c. Renseignez les champs du formulaire.

Formulaire Entité ETL

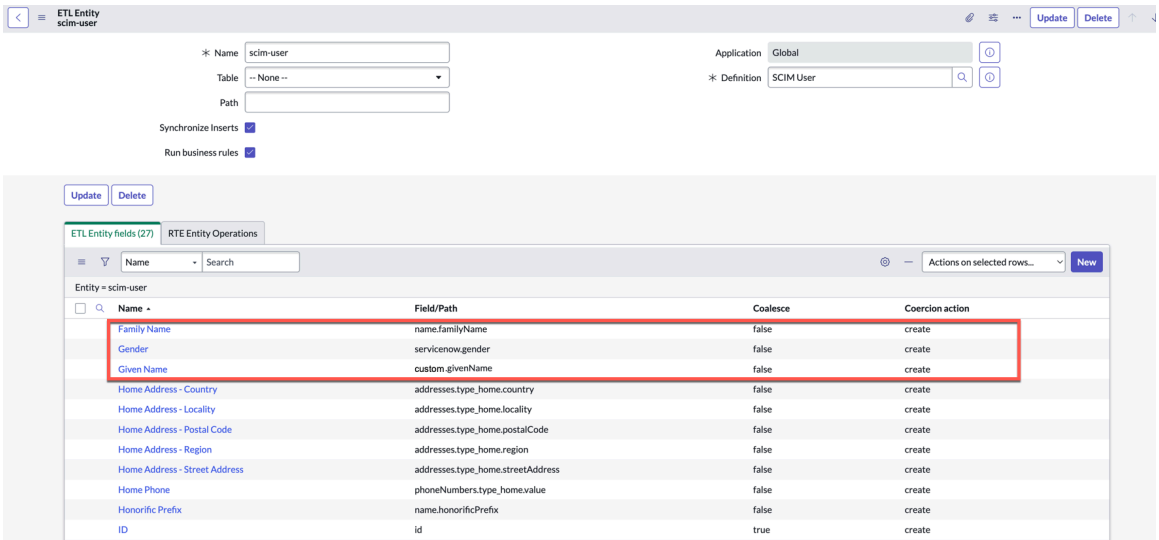
Champ	Description
Nom	Nom de la définition de champ de l'entité ETL.
Application	Entité ETL sélectionnée à laquelle appartient cette définition de champ.
Champ/chemin d'accès	Ce champ est soit une colonne, soit un chemin d'accès. ▪ Le champ est un nom de colonne lorsque l'entité est la table d'importation ou la table cible. ▪ Le champ est un chemin d'accès lorsqu'il 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 est introuvable. Les options sont les suivantes : ▪ **Créer** : créer une référence ou un choix. Affectez la référence ou le choix à l'enregistrement actuel. ▪ **Rejeter** : n'enregistre pas l'enregistrement complet dans la base de données. ▪ **Ignorer** : définit la valeur actuelle sur vide.
Définition	Entité ETL sélectionnée à laquelle appartient cette définition de champ.
Fusion	Option permettant d'interroger les enregistrements existants.



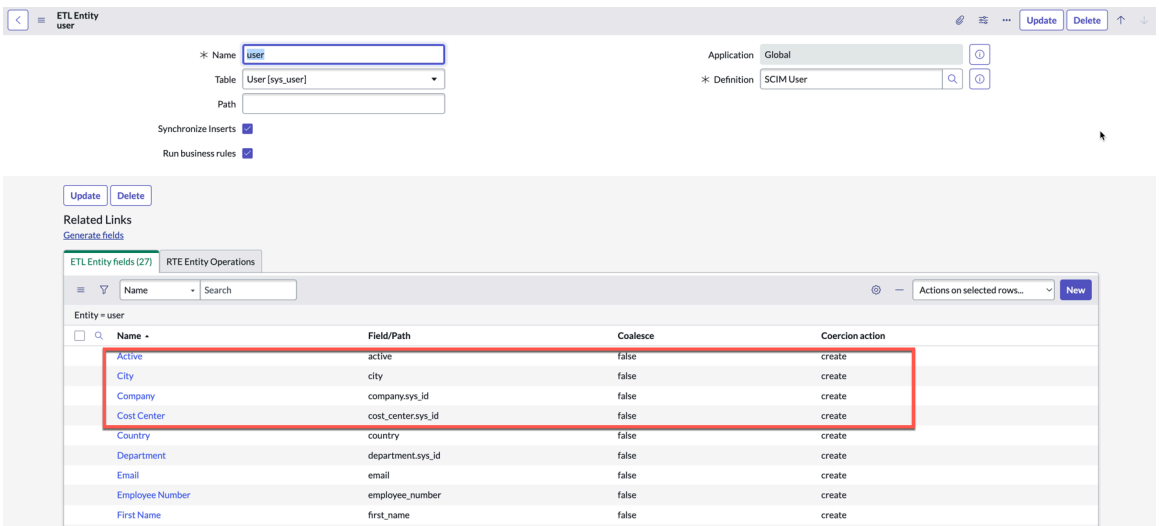
d. Soumettez les entrées en cliquant sur **Soumettre**.

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 (utilisateur), l'extension ou l'extension ServiceNow personnalisée.



L'entité ETL utilisateur peut avoir des entités de la table de base de données. Par exemple, sys_user table.



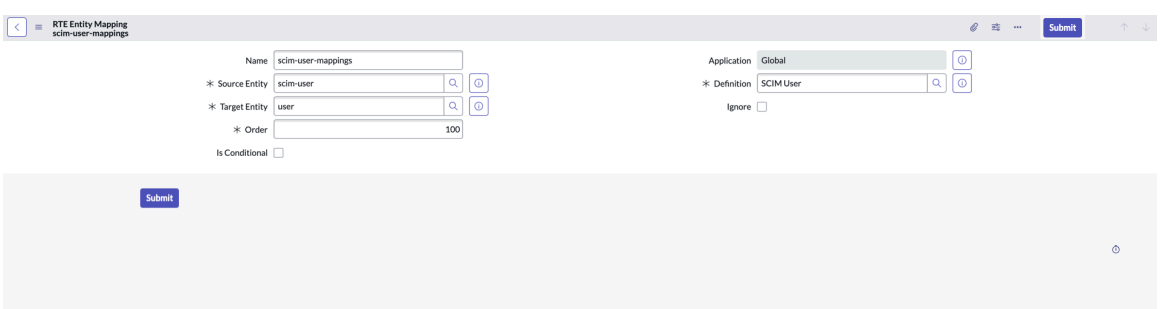
Remarque :
Pour ajouter un filtre dans les champs SCIM entrants, utilisez un trait de soulignement (_). Ce trait de soulignement se traduit par un filtre d'égalisation. Par exemple, l'attribut `email.type_work.value` applique le filtre SCIM de l'e-mail `[type eq "work"].value`.

Une fois les champs créés dans les enregistrements d'entité ETL scim-user et utilisateur, vous devez créer un enregistrement de mappage d'entité RTE. Vous devez ensuite spécifier les définitions source et cible pour mapper les deux champs.

5. Dans la section Mappages d'entités RTE, créez un mappage d'entités en cliquant sur **Nouveau**
6. Renseignez les champs du formulaire.

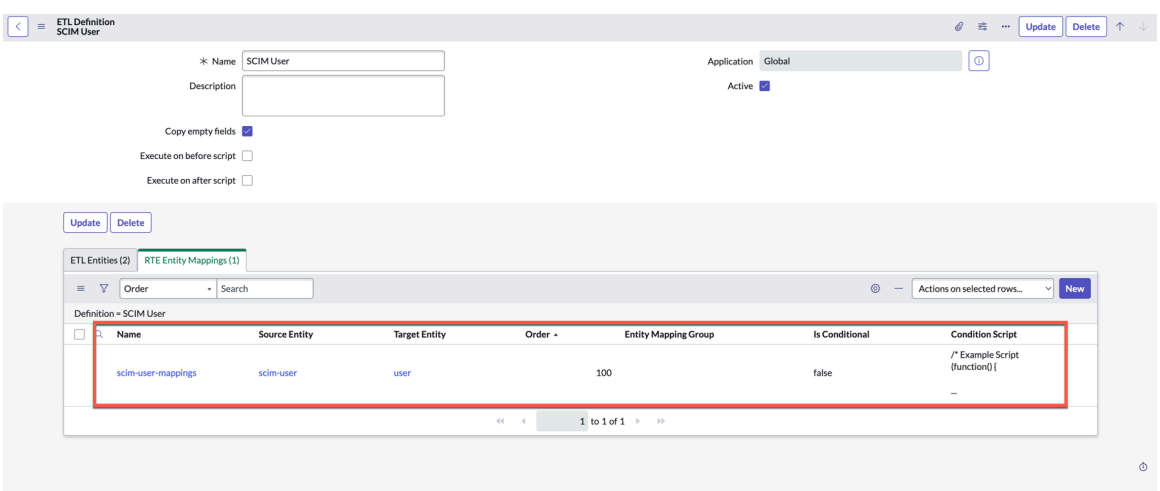
Champ	Description
Nom	Nom du mappage.

Champ	Description
Entité source	Entité source pour le mappage.
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 à indiquer si ce mappage d'entités ETL doit être ignoré lors de l'exécution d'intégrations de données à l'aide de la transformation de jeux d'importation robuste (RTE).



7. Cliquez sur **Envoyer**.

L'exemple suivant montre un enregistrement créé pour le mappage des enregistrements d'entité ETL utilisateur et utilisateur scim.



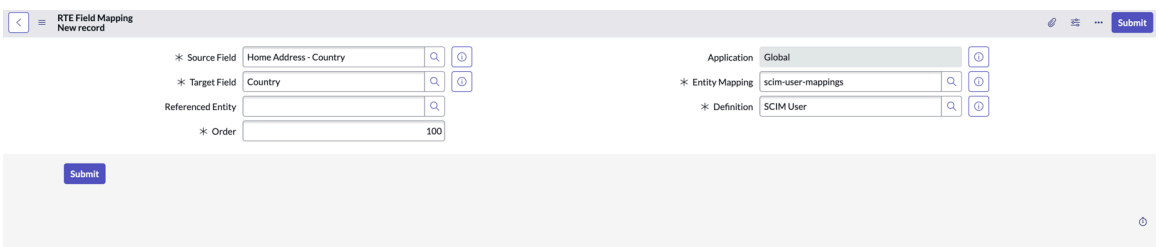
8. Ouvrez l'enregistrement soumis (scim-user-mappings) et créez un mappage entre les enregistrements de l'entité ETL scim-user et user.

   a. Dans la section Mappages de champs RTE, cliquez sur **Nouveau**.

   b. Renseignez les champs du formulaire.

Champs de l'entité ETL

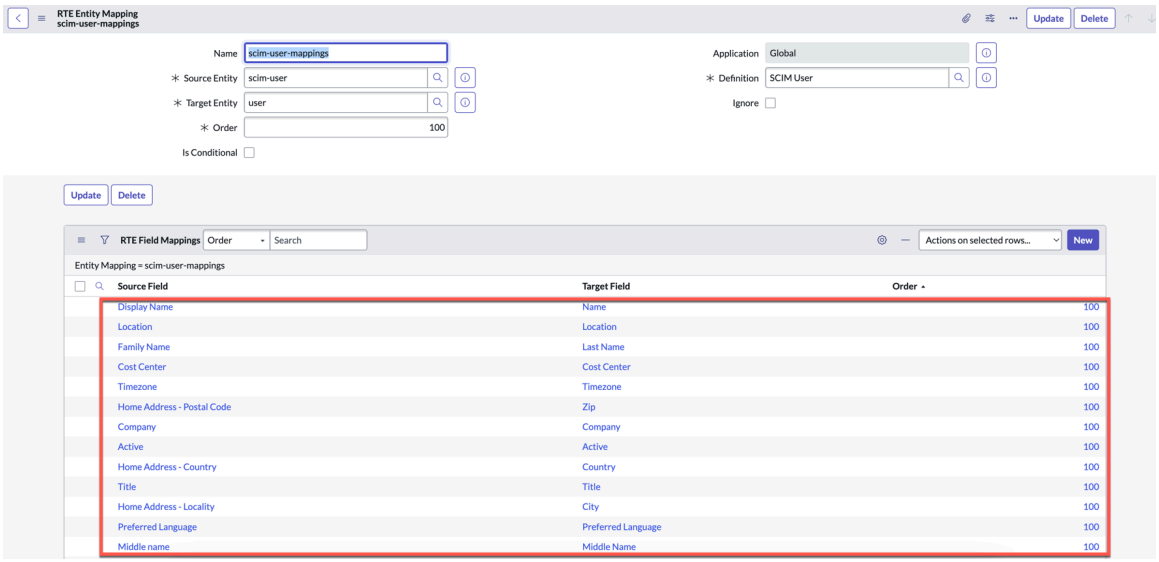
Champ	Description
Champ source	Le périmètre de l'application pour cet enregistrement.
Application	Entité ETL sélectionnée à laquelle appartient cette définition de champ.
Champ cible	Champ ETL de sortie pour l'opération si l'opération utilise une seule sortie.
Mappage d'entités	Mappage d'entités auquel 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 en tant que mappages d'entités RTE en fonction de vos besoins.



Les champs sources et les champs cibles sont mappés tels que 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 les données d'une table source, de transformer les données selon vos besoins et de charger les données dans une table cible.

Information associée

Créer des définitions de charge de transformation d'extraction (ETL)

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 les scripts et *`onAfter`* pour les champs qui ne sont pas mappés dans la *`onBefore`* définition ETL ou RTE.
- L'administrateur SCIM peut remplacer les mappages RTE en ajoutant des scripts personnalisés dans les *`onBefore`* scripts et *`onAfter`* .
- Vous pouvez appeler une API scriptable dans le RTE *`onBefore`* ou *`onAfter`* des scripts pour 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 requête SCIM qui contient l'objet *`scimResource`* . Le *`scimResource`* contexte in représente les éléments suivants dans chaque opération :

- **POST** : ressource SCIM envoyée dans la charge utile de la demande.
- **PUT** : la ressource SCIM actuelle de la base de données remplacée par la ressource SCIM envoyée dans la charge utile de la requête.
- **PATCH** : ressource SCIM actuelle de la base de données après l'exécution des 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.

Tout en étendant le script, l'auteur peut remplacer les *customizeUserResponse* méthodes et *customizeGroupResponse* pour modifier les réponses des ressources Utilisateur et Groupe.

Traduction automatique

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 des réponses.

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'
});
```

Remarque :

- Le paramètre que contiennent les *customizeUserResponse* méthodes and *customizeGroupResponse* est un objet de contexte avec un attribut appelé *scimResource*. Cet attribut possède tous les attributs d'un objet de ressource utilisateur ou groupe.
- Un script include personnalisé ne peut être créé et visualisé que par l'administrateur.
- Si une ressource utilisateur ou groupe est modifiée, vous devez renvoyer le contexte.
- S'il n'y a aucune modification d'attribut dans l'objet de ressource, définissez le sur vide ou renvoyez-le *com.snc.integration.scim2.provider.customization.script.id* à la valeur null.
- Si certains attributs sont conservés via 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 requise afin que le système puisse effectuer les opérations suivantes :
  - Pour obtenir l'objet correct *scimResource* dans *onAfter* les scripts pendant les opérations PUT et PATCH.
  - Pour inclure les attributs qui ont persisté tout au long du *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");	Extrayez l'URN du schéma d'extension personnalisé.
SCIMProviderCustomization.prototype.getServiceNowExtensionUrn.call(this, "User");	Récupérez la valeur de l'URN d'extension ServiceNow .
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User", context);	Récupérez le nœud de valeur personnalisé à partir de la réponse.
SCIMProviderCustomization.prototype.getServiceNowExtensionNodeValue.call(this, "User", context);	Récupérez le nœud de valeur ServiceNow à partir de la réponse
SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(this, "User", context, customExtensionValue);	Définissez le nœud de valeur personnalisé dans la réponse.

Voici un exemple d'utilisation de la fonction d'aide :

```
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);
```

Remarque :
RTE prend en charge la définition des 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, dans lequel l'scmin_admin peut ajouter ou mettre à jour des informations à caractère personnel (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.

Lorsqu'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 source capture les informations de source requises, par exemple en effectuant les actions suivantes :

- 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

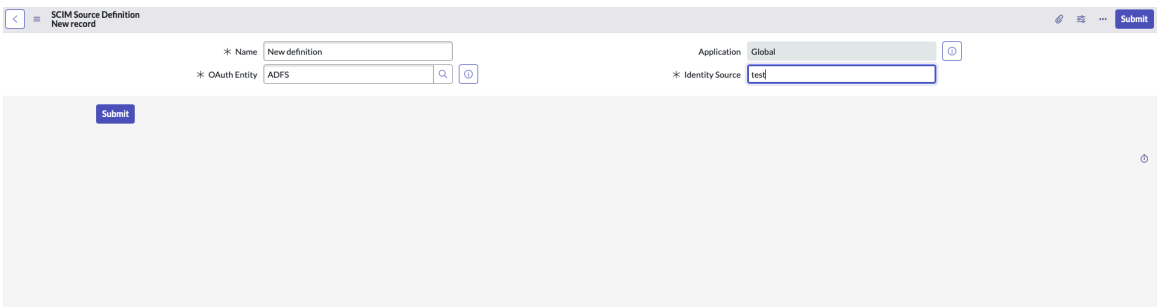
1. Accédez à la **Tous** > **SCIM** > **Définition de la source**.
2. Sur la page Définitions de source SCIM, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Définition de la source SCIM

Champ	Description
Nom	Nom de la définition source.
Application	Le périmètre de l'application pour cet enregistrement.

Champ	Description
Entité OAuth	L’entité OAuth de l’utilisateur d’intégration. L’entité est utilisée pour la mise en service de l’utilisateur par le fournisseur de source d’identité.
Source d'identité	Le nom du fournisseur de la source d’identité. Par exemple, Azure AD, Okta, etc.

Remarque :
Activez la propriété pour renvoyer uniquement les `com.snc.integration.scim2.resolve.externalid.conflict` 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 sur 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 par le biais d’opérations CRUD exposées par le point de terminaison SCIM sur un système externe.

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

Exploration de SCIM Client

Le client SCIM facilite le provisionnement et les mises à jour des ressources d'identité par le biais d'opérations CRUD exposées par le point de terminaison SCIM sur un système externe.

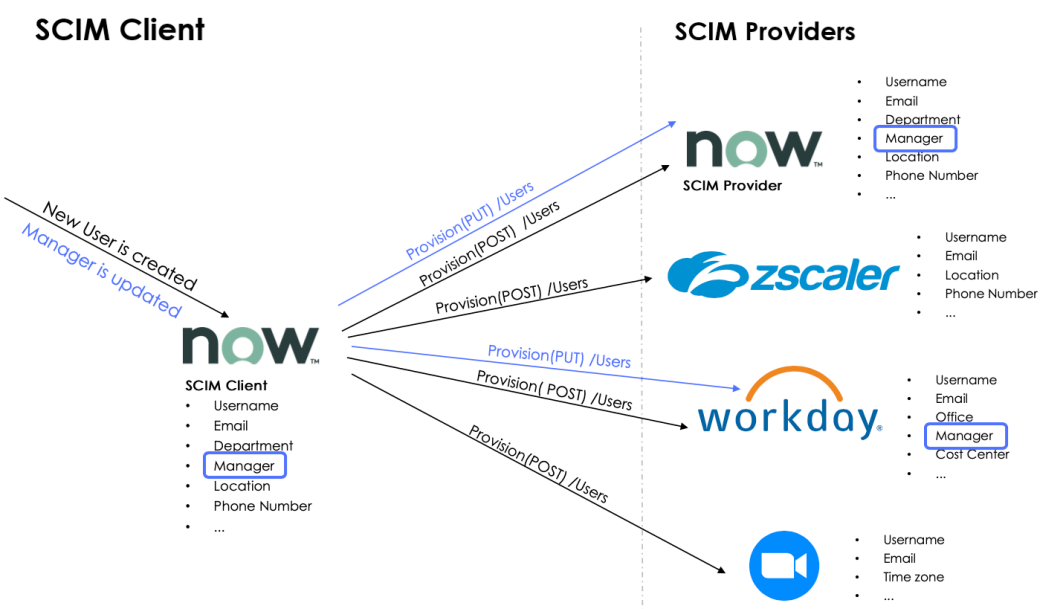
Le client SCIM est utilisé pour créer, mettre à jour et supprimer des ressources d'identité dans un système qui prend en charge les demandes REST conformes à SCIM. Le client est utilisé pour la gestion du cycle de vie des identités et pour la synchronisation des attributs d'identité entre les ServiceNow instances ou entre et 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 fournir l'accès à Git, à Workplace, etc.

Le client SCIM vous permet d'effectuer les actions suivantes :

- Provisionnez les identités et l'accès pour l'appartenance à un utilisateur ou à un groupe.
- Synchronisez l'identité et les ressources associées avec les systèmes conformes à SCIM.
- Intégrez n'importe quel fournisseur SCIM sur ServiceNow®.
- Déprovisionner les identités et l'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 spécifiques. 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 informations sur les types de ressources et les schémas du fournisseur SCIM avec le message REST. Activez la configuration de la

Traduction automatique

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 sur les attributs d'un ServiceNow type de ressource et d'un fournisseur SCIM particuliers. Pour en savoir plus, reportez-vous à Créer un mappage de 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 en savoir plus, reportez-vous à la section Créer un mappage d'attribut SCIM.

Activer le module d'extension client SCIM

Pour activer le client SCIM, 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. Trouvez le module d'extension SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client) 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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

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.

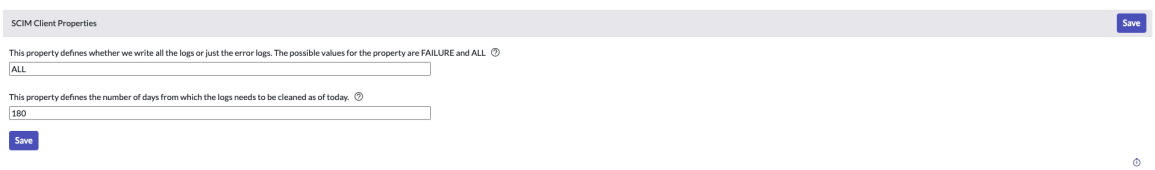
Propriétés

Nom	Description
`com.snc.integration.scim2.client.log.request.status`	Cette propriété détermine s'il convient d'écrire tous les enregistrements de journal ou uniquement les enregistrements de journal d'erreur. Les valeurs possibles sont **FAILURE** ou **ALL.** Valeur par défaut : **TOUS**

Propriétés (suite)

Nom	Description
com.snc.integration.scim2.client.log.cleanup.duration	Cette propriété détermine le nombre de jours d'effacement des 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 de ressources de message REST, etc.
Mappage des ressources de fournisseur SCIM (sys_scim_provider_resource_mapping)	Stocke les informations de table primaire pour chaque nom de fournisseur et de ressource.
Mappage de l'attribut SCIM (sys_scim_attribute_mapping)	Stocke les détails de la source d'où doit provenir chaque valeur d'attribut SCIM, tels que le champ de table, le script, etc.
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 System for Cross-domain Identity Management (SCIM) (rôle serveur) pour créer, mettre à jour ou supprimer des données dans un fournisseur de services (SP). L'API scriptable du client SCIM doit être utilisée dans les scripts exécutés 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 tâches planifiées, etc.

Voici quelques-uns des cas d'utilisation des API scriptables :

- En tant qu'administrateur, mettez en service des informations d'identité à partir de scripts en arrière-plan, de règles métier, d'appels de script include, de workflows, etc.
- En tant qu'administrateur, exécutez une tâche planifiée ou une tâche sur demande pour la mise en service de l'identité.

- Exécutez un workflow ou un sous-workflow avec l'étape Script à l'aide de l'appel d'API scriptable 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 a accès à la récupération des 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. Renseignez 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 REST	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 demande d'API suivant : `Type de contenu : application/scim+json`

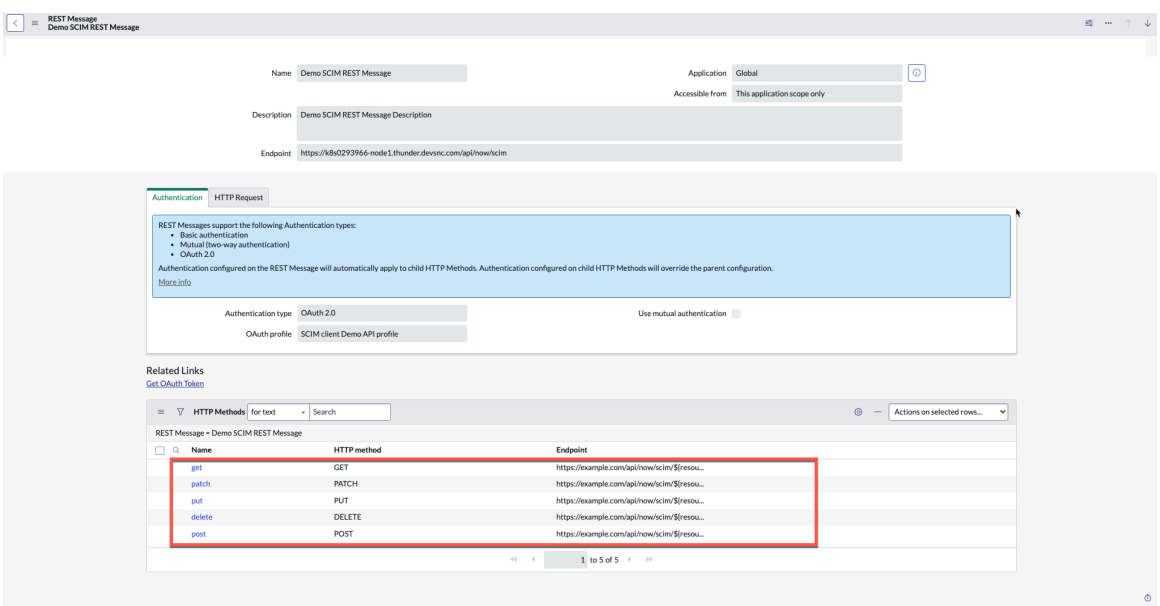
4. Cliquez sur **Nouveau** dans la liste connexe Méthodes HTTP.
5. Configurez les méthodes HTTP suivantes.

> **Remarque :**
> Les URL ont 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 expédié depuis le système de base.



6. Cliquez sur **Envoyer**.

Résultats
L’enregistrement de 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 informations sur les types de ressources et les 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.

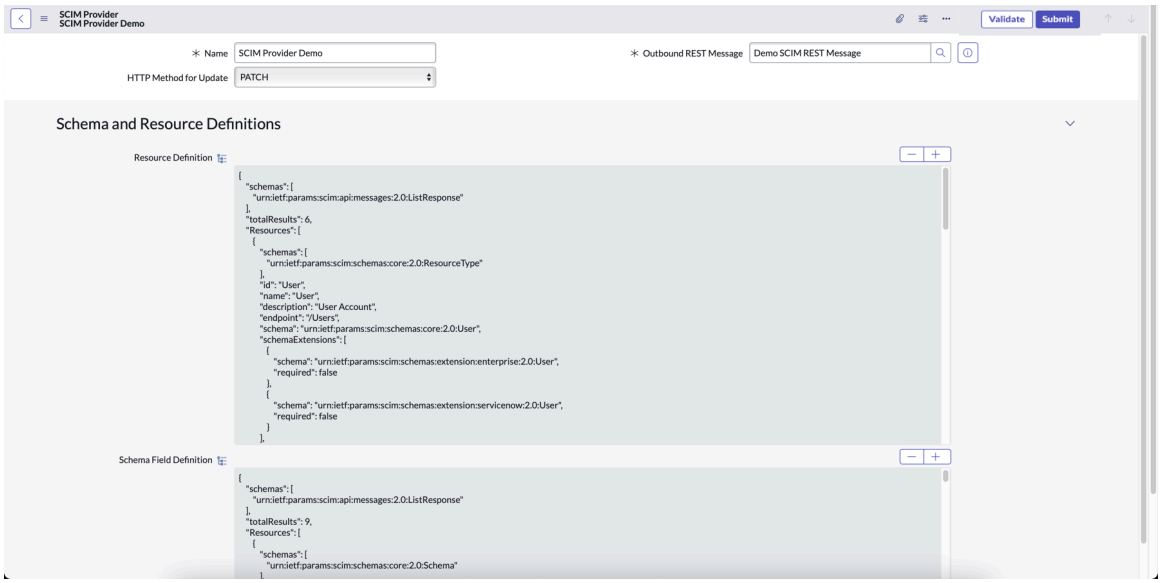
Rôles requis : admin

Procédure
1. Accédez à la **Tous** > **Client SCIM** > **Fournisseur SCIM**.
2. Sur la page Fournisseurs SCIM, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Fournisseur SCIM

Champ	Description
Nom	Nom du fournisseur SCIM
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 utilisée 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 en service d’une ressource déjà existante.

Remarque :
- Les champs **Définition de ressource** et **Définition du champ de schéma** sont récupérés à partir `/ResourceTypes/Schemas` des points de terminaison publics du fournisseur SCIM. Ces champs sont renseignés automatiquement après la sélection du message rest.
- 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 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 du 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 de ressources de fournisseur SCIM.

Créer un mappage de ressources de fournisseur SCIM

Définissez les mappages des attributs SCIM sur les attributs d'un ServiceNow type de ressource et d'un fournisseur SCIM particuliers.

Avant de commencer

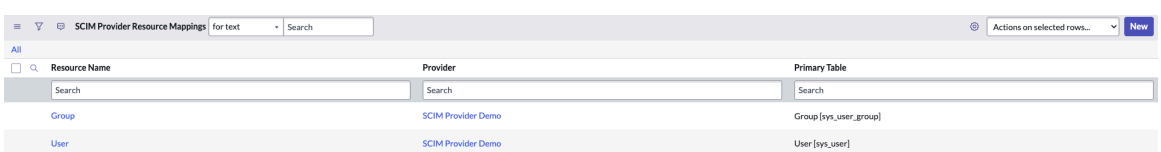
Rôles requis : admin

Procédure

1. Accédez à la **Tous** > **Client SCIM** > **Mappage des ressources de fournisseur SCIM**.

   Le mappage des ressources du fournisseur SCIM est fourni avec le mappage Utilisateur et Groupe par défaut.

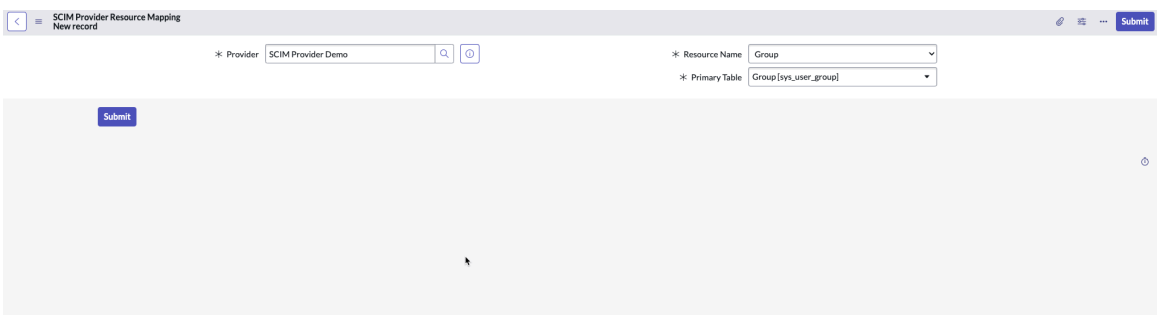
   Remarque :
   Les mappages d'utilisateur ou de groupe contiennent des exemples de mappages que vous pouvez utiliser comme référence. Vous pouvez également créer un mappage en fonction des ressources utilisateur ou groupe.



2. Créez un mappage de ressources en cliquant sur **Nouveau**.
3. Renseignez les champs du formulaire.

Mappage des ressources

Champs	Description
Fournisseur	Nom du fournisseur SCIM. Référez-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 les sys_id de la ressource à mapper.



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 des schémas. Pour plus d'informations, consultez Créer un mappage d'attribut SCIM.

Créer un mappage d'attribut SCIM

Créez un mappage d'attributs SCIM et utilisez-le comme source unique de ressource pour les champs de table ServiceNow .

Avant de commencer
Rôles requis : admin

Pourquoi et quand exécuter cette tâche
Vous trouverez ci-dessous les types de mappage d'attributs et leurs descriptions.

Types de mappage d'attribut

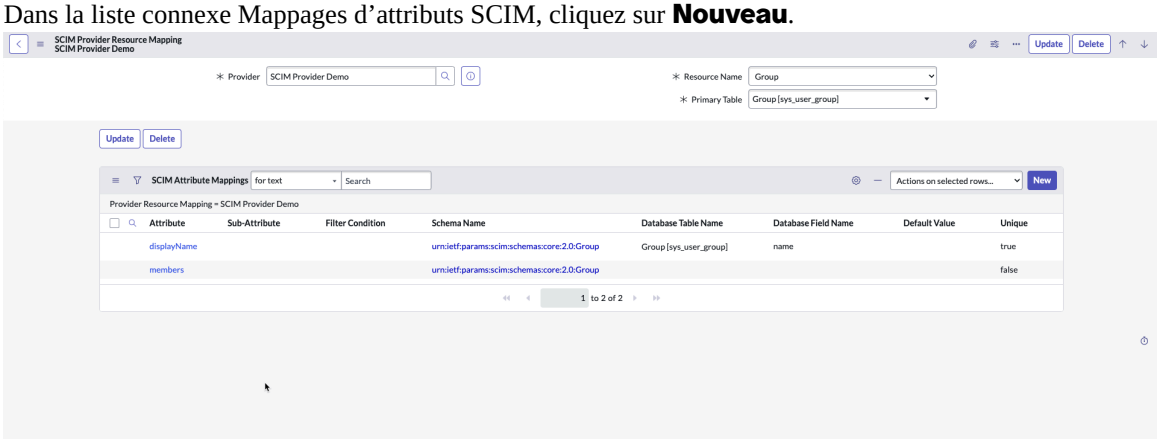
Type de mappage d'attribut	Description
Direct	L'attribut SCIM est renseigné à l'aide des champs Nom de la **table de base** de **données et Nom du champ de base de données** .
Constante	L'attribut SCIM est renseigné à l'aide d'une valeur par défaut spécifiée.
Script/Personnalisé	L'attribut SCIM est renseigné 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 password 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. Sélectionnez le mappage de ressource SCIM créé pour la configuration.
3. Dans la liste connexe Mappages d’attributs SCIM, cliquez sur **Nouveau**.



4. Renseignez les champs du formulaire.

Formulaire Mappages d’attributs SCIM

Champs	Description
Mappage des ressources de fournisseur	Mappage d’attributs pour une combinaison fournisseur-ressource. Si ce champ n’est pas renseigné automatiquement, utilisez l’option de recherche. Sélectionnez l’enregistrement Mappage des ressources de fournisseur.
Nom du schéma	Nom de 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 (cas échéant) pour lequel le mappage doit être défini. Par exemple, s’il existe un attribut de type complexe comme `name.familyName`, alors

Champs	Description
	l'attribut est **name** et le sous-attribut **est familyName**.
Type de champ	Le 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 l'e-mail professionnel, l'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 contenir 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 tels que travail, mobile, domicile, etc
Unique	Option permettant d'identifier de façon unique une ressource entre les systèmes du client SCIM et du 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 attributaire au nom de la ServiceNow table. Si vous choisissez le mappage d'attribut direct, vous devez définir ce champ. Par exemple, l'attribut *`username`* SCIM peut être mappé au champ **Utilisateur** dans le champ **Nom de la table de base de données** .

Champs	Description
Nom du champ de base de données	Le champ Nom de 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 d'attribut direct, 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 de champ doivent être **Aucun**. Par exemple, la valeur du sous-attribut primaire d'un 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 complexe d'attribut, un script peut fournir la valeur au niveau d'un attribut ou d'un sous-attribut. Par exemple, l'attribut **Members** de la ressource de groupe n'a aucune condition de filtre. Ainsi, l'option de script doit être définie au niveau de l'attribut parent de l'attribut **Members** .
Script	Script utilisé pour extraire la valeur d'attribut. Le type de script de retour doit être une chaîne ou un JSON converti en chaîne.

Champs	Description
	La sortie du script doit être au format approprié, comme prévu par le fournisseur pour cet attribut.

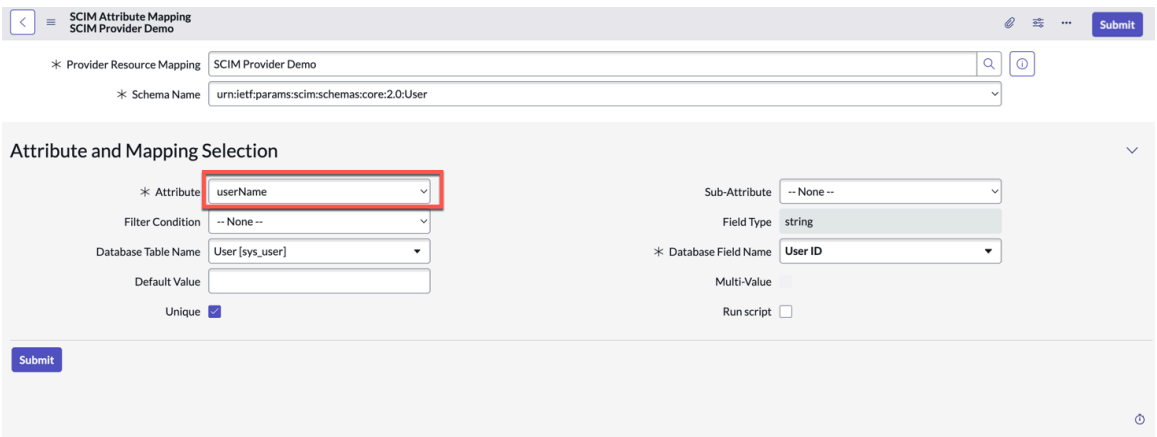
5. Cliquez sur **Envoyer**.

Références de mappage d'attributs

Les mappages d'attributs vous permettent d'utiliser les attributs comme source unique de ressource pour les champs de table ServiceNow .

Attribut

Attribut pour lequel le mappage doit être défini. Par exemple, *`userName`*.

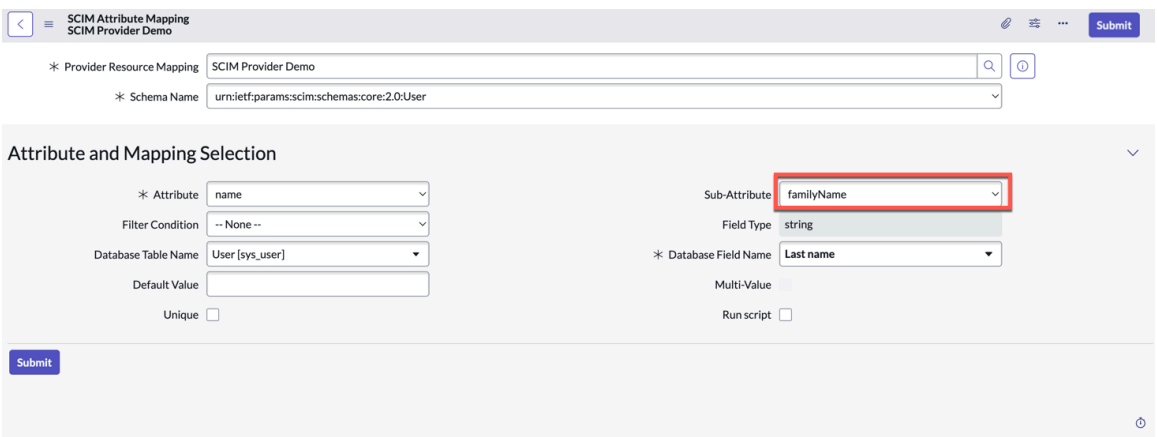


Sous-attribut

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 et le sous-attribut est *`namefamilyName`*.

Pour les attributs simples tels que le nom d'utilisateur, la valeur **du sous-attribut** est **Aucun**.

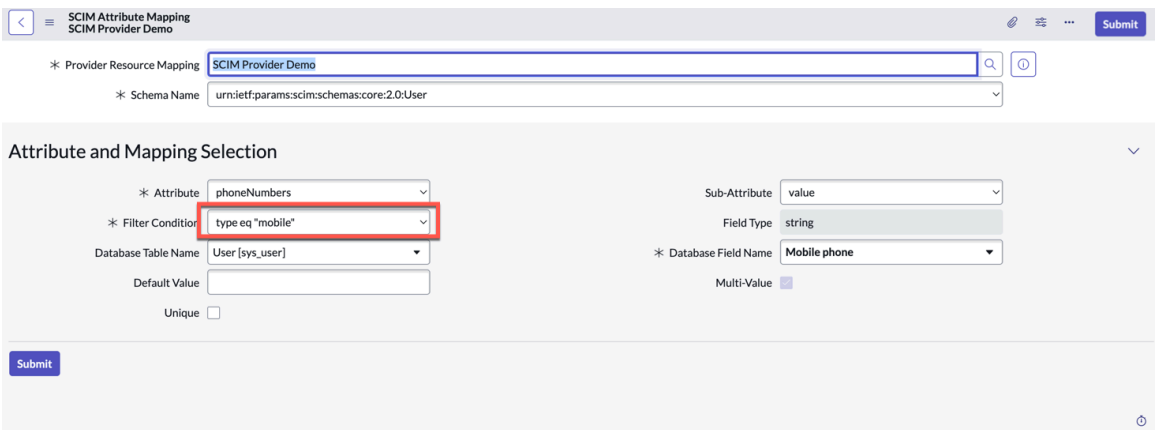


Condition de filtre

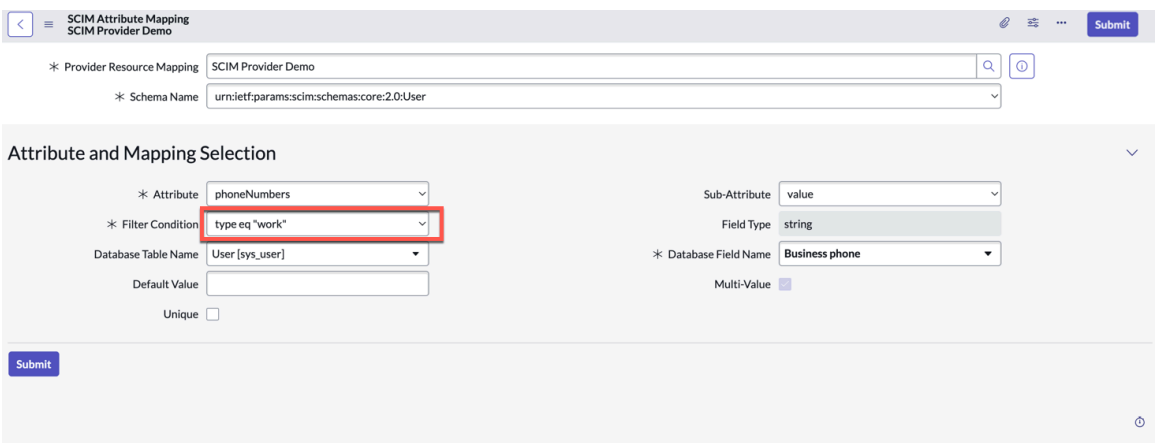
Un attribut à valeurs multiples peut contenir des informations supplémentaires qui peuvent être spécifiées à l'aide d'une condition de filtre. Les choix de condition de filtre sont renseignés à l'aide des schémas définis par le fournisseur SCIM.

Par exemple, l'attribut *phoneNumbers* a plusieurs types tels que travail, mobile, domicile, etc.

Vous pouvez spécifier une condition de filtre à partir d'un ensemble de valeurs possibles. Par exemple, la condition de filtre peut être pour l'attribut *phoneNumber***eq « mobile »**.



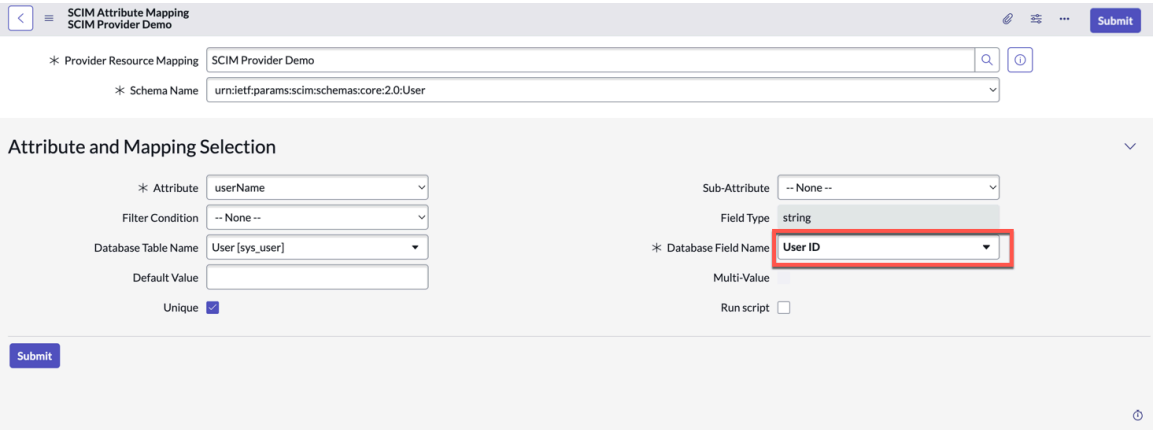
À la place, l'attribut *phoneNumber* peut avoir une condition de filtre de **type eq « work »**.



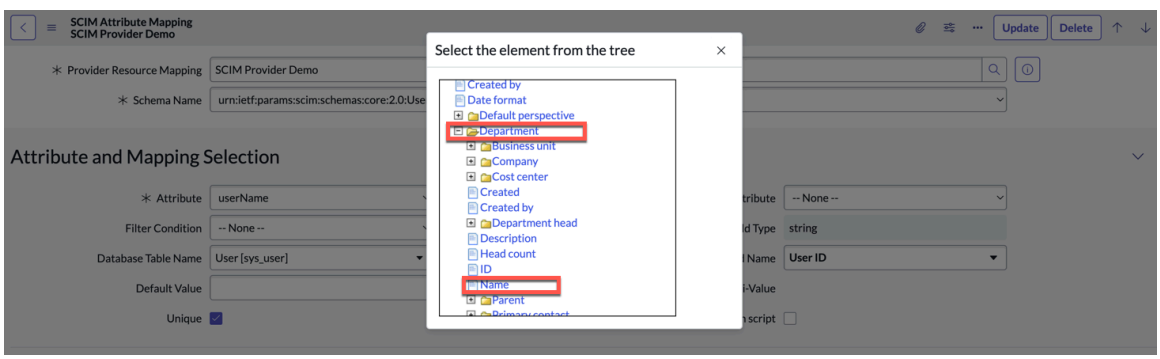
Nom du champ de base de données

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 ServiceNow nom de champ mappé à l'attribut SCIM.

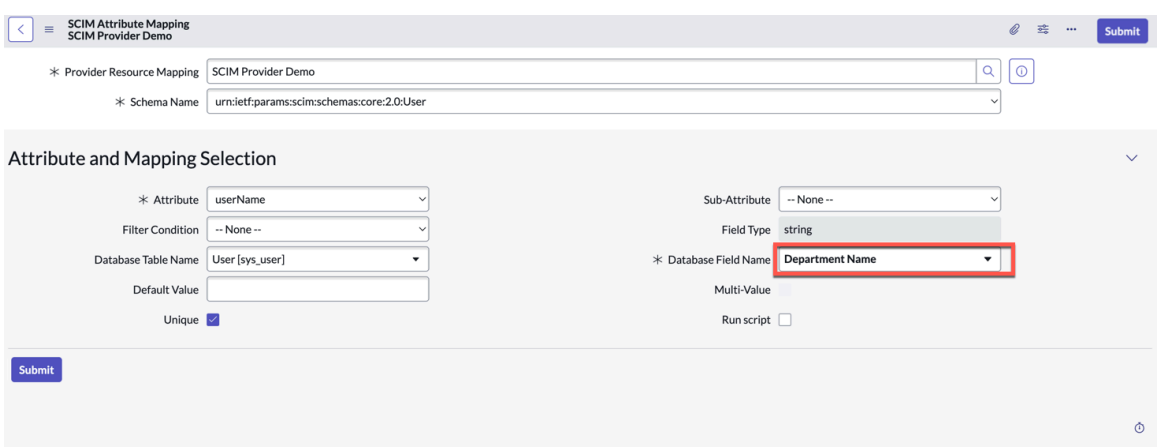
Par exemple, l'attribut *username* SCIM peut être mappé à un utilisateur en tant que champ Nom de la **table de base de données** et au champ ID d'utilisateur en tant que champ **Nom du champ Base de données** .



Vous pouvez également remonter 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 de base de données est **Nom de département**.



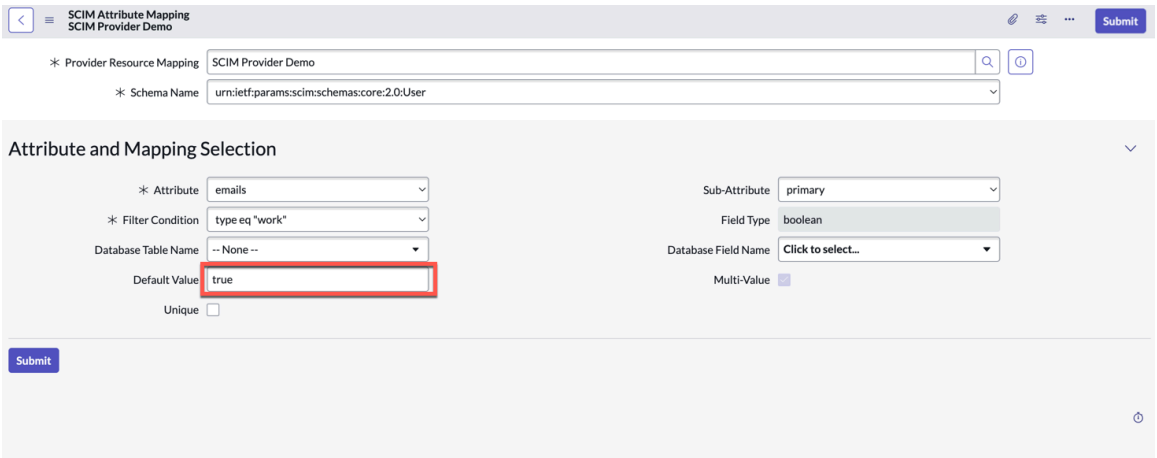
Valeur par défaut

La valeur par défaut est transmise au fournisseur SCIM si le mappage d'attributs directs de ce champ renvoie 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 de champ doivent être **Aucun**.

Par exemple, la valeur du sous-attribut primaire de l'e-mail professionnel peut être codée en dur comme **vrai**.

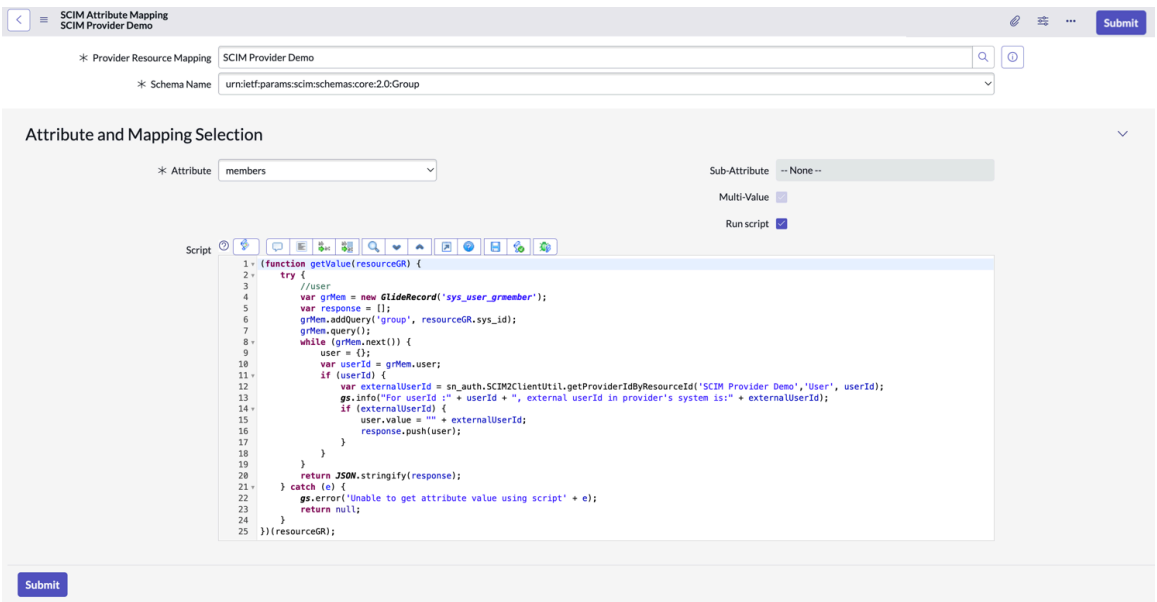
Traduction automatique



Script

Le script est utilisé pour extraire la valeur de l'attribut. Le type de retour du script doit toujours 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.

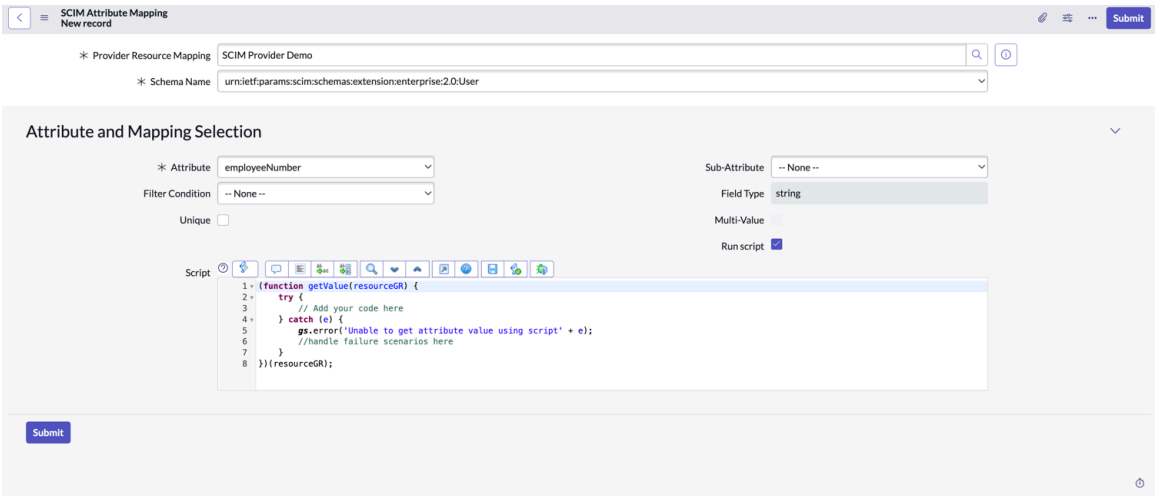
Voici un exemple de script pour un attribut à valeurs multiples.



La sortie du script doit avoir un tableau JSON stringified.

Voici un exemple de script d'un attribut à valeur simple.

Traduction automatique



La sortie du script doit être une chaîne de caractères.

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 ce dernier n'a pas accès à la table. Vous devez vous assurer que l'API scriptable est appelée dans le contexte 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 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 est toujours 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.

Dépannage (suite)

Problème	Action
"detail": "Manager id : 02826bf03710200044e0bfc8bcbe5ds8 doesn't exist"	

Zones à vérifier pour le dépannage

Voici quelques-unes des zones qui peuvent être vérifiées pour détecter les erreurs de dépannage 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 du client SCIM.

Champs de journaux

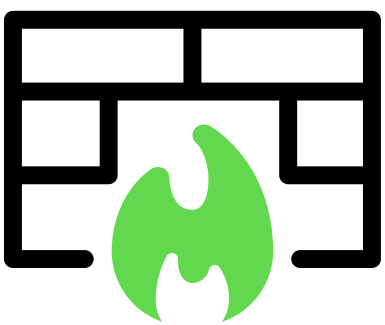
Champ	Description
ID de demande	ID unique qui représente une API scriptable appelée.
Fournisseur SCIM	Nom du fournisseur pour lequel l'API est appelée.
Ressources	Nom de la ressource pour laquelle l'API est appelée.
ID de ressource	ID pour lequel l'API est appelée. Pour la suppression, l'ID représente l'ID de ressource dans le système fournisseur et l'ID est 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 être dû à des problèmes de configuration dans le client SCIM.

- Vérifiez le corps de la demande en configurant et en affichant les appels sortants. Pour en savoir plus, reportez-vous à la rubrique 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 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 .

Gestion des accès

Access Management vous permet d'accéder à l'instance ServiceNow® en toute sécurité.

Authentification

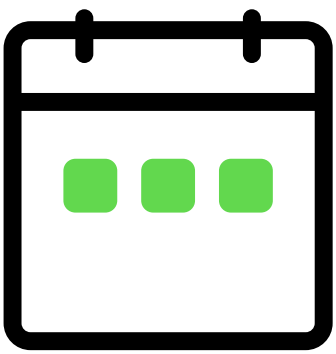


ServiceNow® valide l'identité d'un utilisateur qui accède à une instance, puis autorise l'utilisateur à accéder aux fonctionnalités qui correspondent au rôle ou à la fonction de l'utilisateur.

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 Détection, Mappage des services et Gestion dans le cloud, ou pour travailler avec Orchestration.

Sécurité de connexion et d'authentification



Configurez les options de sécurité de connexion pour contrôler l'accès à votre instance.

Sécurité des services Web

Appliquez la sécurité à l'aide de l'authentification de base, de l'authentification réciproque ou de WS-Security.

Traduction automatique

Authentification

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 l'utilisateur.

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 Détection, Mappage des services et Gestion dans le cloud, ou pour travailler avec Orchestration.

Sécurité de connexion et d'authentification

Configurez les options de sécurité de connexion pour contrôler l'accès à votre instance.

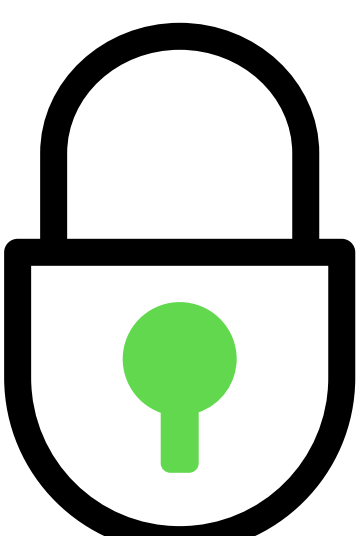
Sécurité des services Web

Appliquez la sécurité à l'aide de l'authentification de base, de l'authentification réciproque ou de WS-Security.

Authentification

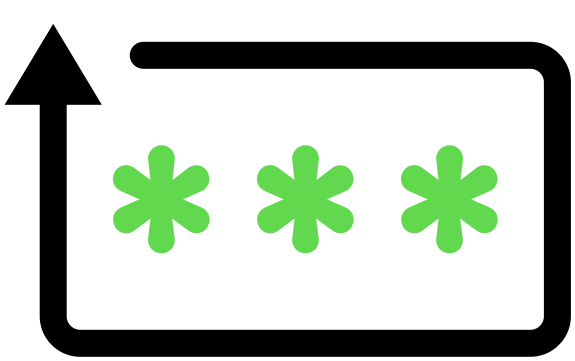
ServiceNow® valide l'identité d'un utilisateur qui accède à une instance, puis autorise l'utilisateur à accéder aux fonctionnalités qui correspondent au rôle ou à la fonction de l'utilisateur.

Premiers pas



Authentification unique (SSO) de plusieurs fournisseurs

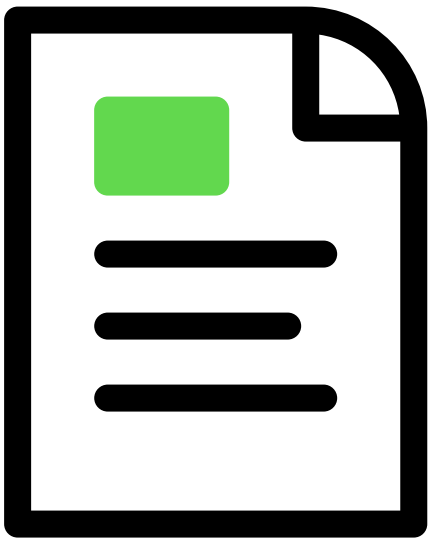
Nom d'utilisateur et mot de passe configurés dans les fournisseurs d'identité, qui ont un compte d'utilisateur correspondant dans la base de données.



OAuth entrant et sortant

Nom d'utilisateur et mot de passe du fournisseur d'identité OAuth qui possède un compte d'utilisateur correspondant dans la base de données.

Traduction automatique

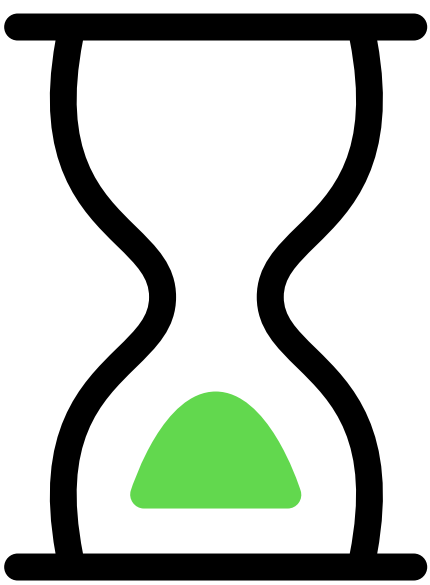


Politique d'accès API

La politique d’accès d’API définit les autorisations et la durée d’accès à une API.

Authentification par jeton Digest

Le nom d’utilisateur et le secret dans la table exécutent une opération de hachage spécifique à l’utilisateur, par exemple 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

Authentification multifacteur (MFA)

Code secret issu du code QR, qui comprend un code secret en bas avec les informations telles que le nom de l’instance, le nom d’utilisateur ou les informations de compte utilisateur, ainsi que le code d’authentification.

Traduction automatique

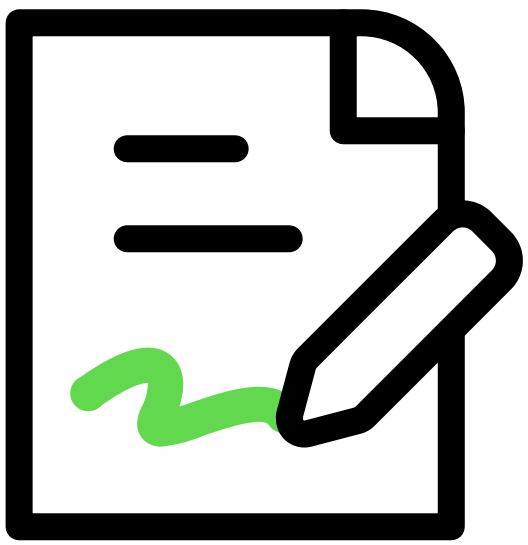
Configurer l’authentification basée sur le lien sur le

[qa: BEGIN review][End]

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.

Authentification basée sur certificat

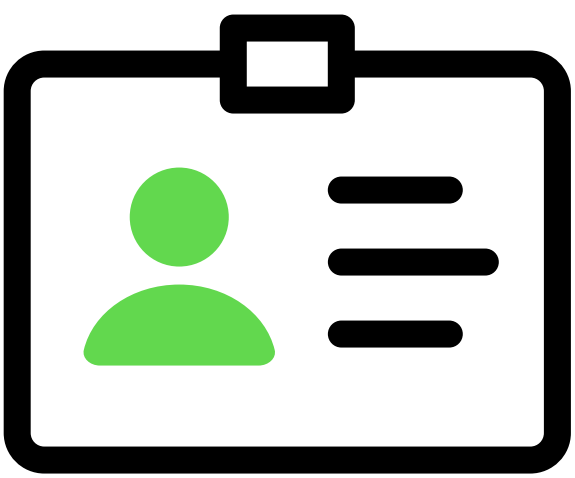
Certificats codés PEM uniques mappés aux utilisateurs plutôt qu’au nom d’utilisateur et au mot de passe.



Auto-inscription

Nom d’utilisateur et mot de passe dans leur enregistrement utilisateur dans la base de données de l’instance.

Accès zéro confiance



LDAP

Traduction automatique

L’accès Zero Trust garantit que tous les accès aux applications et aux données sont accordés sur la base du moindre privilège, uniquement après vérification de l’identité de l’utilisateur et évaluation des risques.	Nom d’utilisateur et mot de passe dans leur compte LDAP, qui a un compte d’utilisateur correspondant dans la base de données.

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.

Remarque :

- Le Okta module d’extension SSO est déconseillé.
- Pour en savoir plus sur les propriétés de sécurité qui affectent le traitement des autorisations, consultez Contrôle d’accès dans Paramètres de renforcement de la sécurité de l’instance.
- Vous pouvez utiliser l’authentification SAML et Digest via l’application Multiple Provider SSO (Authentification unique de plusieurs fournisseurs).

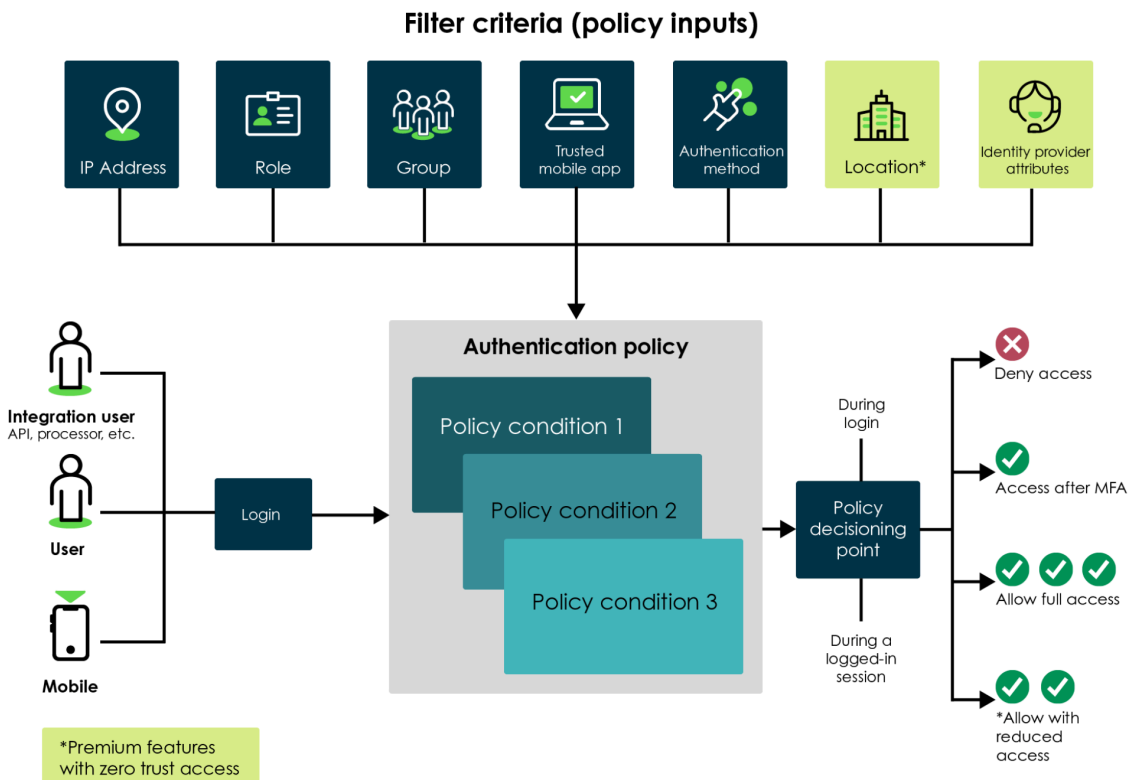
Authentification adaptative

Utilisez le cadre de travail des politiques d’authentification adaptative pour appliquer des contrôles d’authentification contextuelle aux utilisateurs appropriés et 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 des utilisateurs et des API à votre instance 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 exigences de sécurité.

Par exemple, un administrateur peut configurer la pour n’autoriser les *`Allow Access Policy`* connexions qu’aux seuls utilisateurs qui appartiennent à une plage d’adresses IP de confiance et sont membres d’un rôle spécifique. Lorsqu’elle est *`Post-authentication context`*affectée au , 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 sys_ui_message. Lorsque vous vous connectez avec un mot de passe incorrect, le message personnalisé dans la langue préférée s’affiche.



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 **Autoriser 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 faut 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, reportez-vous à Politiques d'authentificationla rubrique .

Contextes des politiques 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 qu'un 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 de détails sur ces contextes, reportez-vous à Contextes des politiques 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

que le rôle d’utilisateur, la plage d’adresses IP et le fournisseur d’identité. Pour en savoir plus sur les critères de filtre, reportez-vous à 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 quand l’accès est bloqué. Pour en savoir plus sur ces propriétés, reportez-vous à Configurer les propriétés d’authentification adaptative.

Politiques d’accès des REST APIs

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 des REST APIs.

Domain Separation 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 la politique affectent le domaine dans le champ **Domaine** d’enregistrements [sys_domain]. Les conditions de politique dans le domaine global affectent tous les domaines.

Activer l’authentification adaptative

Vous pouvez activer le module d’extension Adaptive Authentication (com.snc.adaptive_authentication) pour Adaptive Authentication si vous disposez du rôle administrateur.

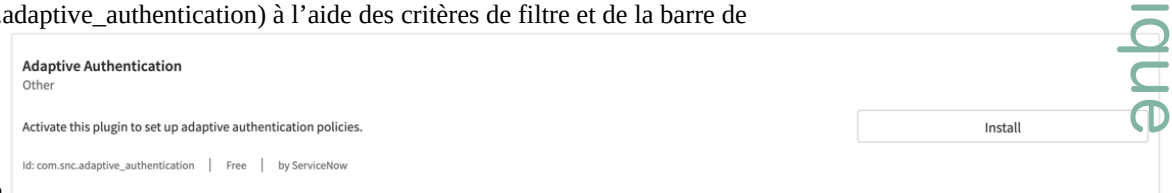
Avant de commencer

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 **Adaptive Authentication** (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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

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 l'authentification** . Pour en savoir plus sur les propriétés d'Adaptive Authentication, reportez-vous à 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.

Utilisez des critères de filtre pour fournir des politiques d'authentification des informations telles que l'adresse IP, les rôles ou les groupes d'un utilisateur. Ajoutez ces critères à la section Conditions de la **police** de vos polices.

Sept types de critères de filtre sont utilisés dans l'authentification adaptative. Vos politiques d'authentification peuvent utiliser un ou plusieurs de ces critères pour évaluer les demandes d'authentification.

Types de critère de filtre

Type	Description
Critère de filtre d'adresses IP	Utilisez les critères de filtre IP pour filtrer les utilisateurs en fonction des adresses IP de l'utilisateur. IPv4 et IPv6 sont pris en charge.
Critère de filtre de rôle	Utilisez des 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 de la localisation	Utilisez les critères de filtre d'emplacement pour filtrer les utilisateurs en fonction de l'emplacement de l'utilisateur.
Critères de filtre d'attribut du fournisseur d'identité	Utilisez les attributs de fournisseur d'identité reçus de la réponse SAML de l'IdP comme critère de filtre pour l'authentification.

Critères génériques

Outre les types précédemment répertoriés, il existe quatre critères de filtre génériques. Ces critères n'apparaissent pas dans votre navigateur de filtre, mais vous pouvez les sélectionner lors de l'ajout d'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 désignent une connexion locale • SSO, qui désigne une connexion basée sur l'authentification unique (SSO, OIDC ou Digest) à plusieurs niveaux.

Types de critères de filtre génériques (suite)

Type	Description
	Remarque : Ces critères de filtre sont disponibles uniquement lorsque le module d'extension **Integration - Multiple Provider Single Sign-On Installer** [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. Utilisez-le 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 :** Ces critères de filtre sont disponibles uniquement lorsque le module d'extension **Integration - Multiple Provider Single Sign-On Installer** [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 basée sur l'utilisateur	Utilisez ce filtre pour filtrer en fonction de la fonctionnalité de 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 de confiance permettant d'activer l'accès à l'instance à partir de l'application mobile.

Filtre d'adresses IP

Utilisez les critères de filtre IP pour filtrer les utilisateurs en fonction des adresses IP de l'utilisateur. IPv4 et IPv6 sont 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 spécifique ou à une plage d'adresses.

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 spécifique ou à une plage d'adresses.

Avant de commencer

Rôle requis : admin

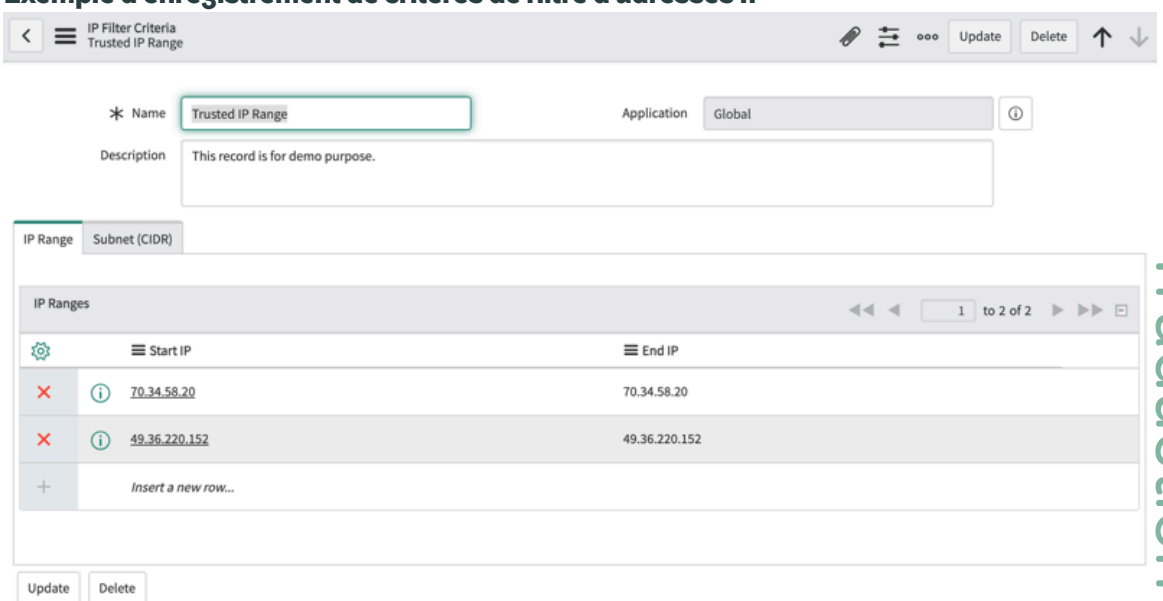
Procédure

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.

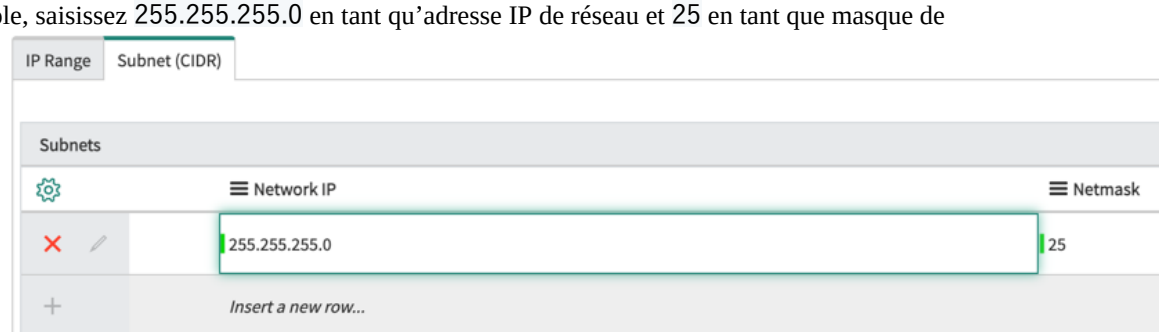
Exemple d'enregistrement de critères de filtre d'adresses IP



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 saisir une seule adresse IP ou plusieurs plages d'adresses IP. Par exemple, pour une plage d'adresses IP, saisissez 192.0.2.0 dans la colonne **Adresse IP de début** et 192.0.2.255 dans la colonne **Adresse IP de fin** .

   Remarque :
   Pour une seule adresse IP, assurez-vous de 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 IP de **fin** vide, puis sauvegardez 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 et le masque réseau au format CIDR (Classless Inter-Domain Routing). Par exemple, saisissez 255.255.255.0 en tant qu'adresse IP de réseau et 25 en tant que masque de réseau.



Filtre de rôle

Utilisez des critères de filtre de rôle pour filtrer les utilisateurs en fonction de leurs rôles.

Les critères de filtre des 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 des 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

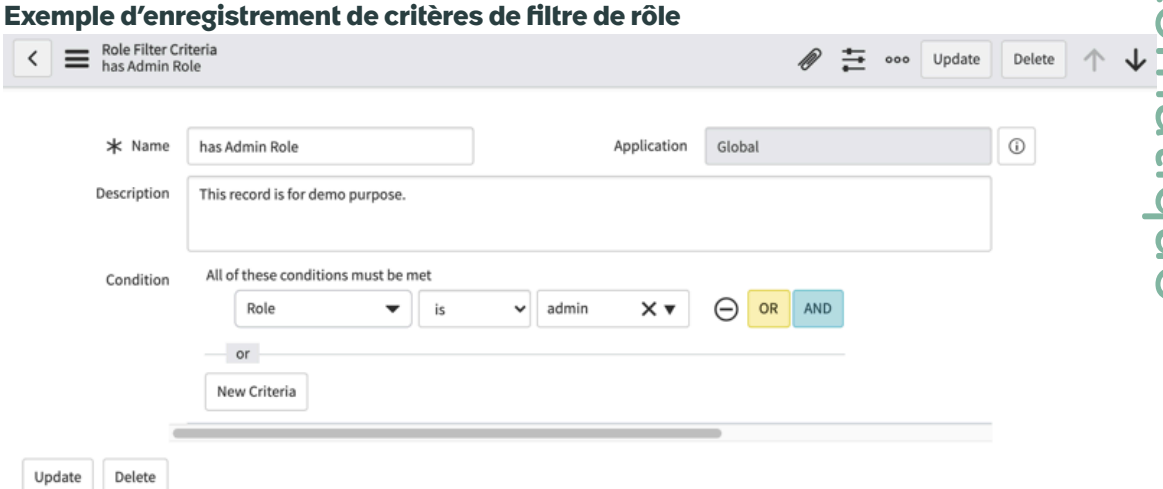
Procédure

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

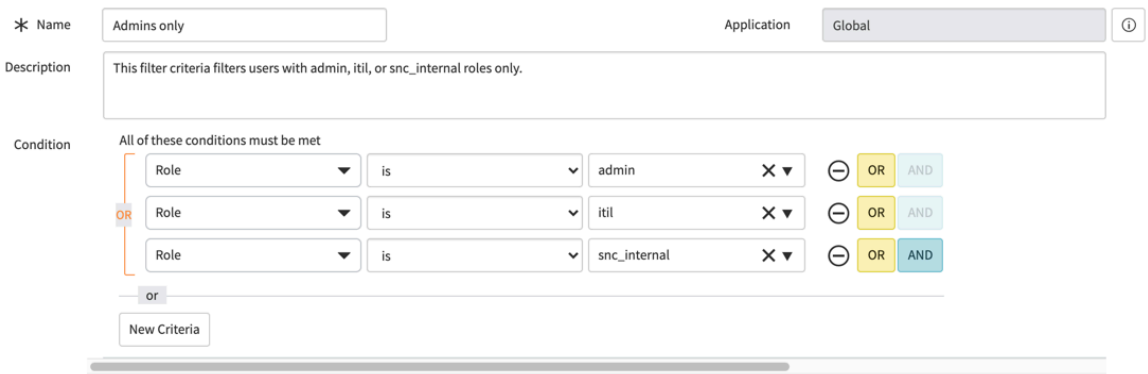
Champ	Description
Nom	Nom permettant d'identifier le rôle.
Application	Périmètre de l'application.
Description	Brève description du rôle.

Exemple d'enregistrement de critères de filtre de rôle



4. Dans la **section 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 condition.
   Par exemple, vous pouvez créer une condition qui autorise uniquement les utilisateurs ayant des rôles administrateur, itil ou snc_internal. Pour plus d'informations sur Condition Builder, consultez Créer une instruction de condition à l'aide du créateur de condition .

Remarque :
Actuellement, la remontée pas à pas n'est pas prise en charge dans les critères de filtre de rôle.



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 des utilisateurs en fonction du groupe d'utilisateurs auquel ils appartiennent.

Créer un critère de filtre de groupe

Les critères de filtre de groupe autorisent ou refusent l'accès des utilisateurs en fonction du groupe d'utilisateurs auquel ils appartiennent.

Avant de commencer
Rôle requis : admin

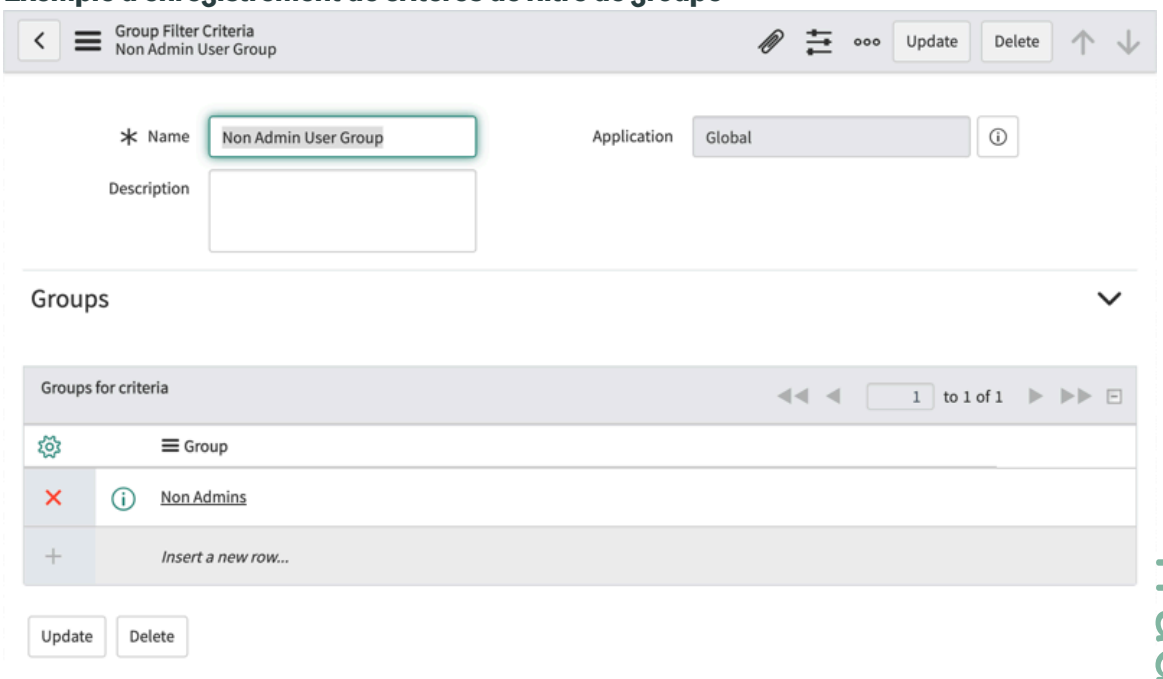
Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Critère de filtre** > **Critères de filtre de groupe**.
2. Cliquez sur **Nouveau**.
3. Renseignez ces champs du formulaire.

Critères 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 **Groupes pour les critères** , double-cliquez sur **Insérer une nouvelle ligne**.
5. Cliquez sur , recherchez et sélectionnez un groupe d'utilisateurs.
6. Cliquez sur l'icône .

Filtre d'emplacement

Les critères de filtre 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 :

- Les critères de filtre d'emplacement sont un plug-in payant qui nécessite une licence.
- L'instance doit être sur ADCv2. Si l'instance n'est pas sur ADCv2, les informations de localisation de l'utilisateur ne sont pas disponibles.

Les critères de filtre d'emplacement vous permettent d'effectuer les opérations suivantes :

- Agir en tant qu'entrée de politique Agir pour les conditions de politique afin de vérifier et répondre aux exigences d'authentification.
- Offrez la possibilité de créer des politiques d'authentification adaptative en fonction du **pays**.
- Autorisez ou non l'accès de l'instance à une zone géographique donnée.
- Utilisez la politique de pré-authentification ou de post-authentification basée sur l'emplacement géographique 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.
- N'autorisez l'accès aux zones que dans la zone de confidentialité applicable et à la discrétion 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 particulier.
- Appliquez l'authentification renforcée ou la MFA pour se connecter en fonction du pays.
- Réduisez ou limitez les rôles de l'utilisateur en fonction du pays.
- Les critères de filtre d'emplacement peuvent être utilisés pour l'authentification 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 l'emplacement 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 VPN (emplacement) est affichée en tant qu'emplacement utilisateur.

Remarque :
Si des emplacements incorrects s'affichent après la configuration du filtre d'emplacement, consultez l'article de la base de connaissances pour résoudre le problème.

Activer l'accès basé sur l'emplacement

Activez l'accès basé sur l'emplacement (com.snc.zero_trust_location_access) Zero Trust 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 sont pas disponibles.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Trouvez 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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

> **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>.

Créer un critère de filtre d'emplacement

Utilisez les critères de filtre d'emplacement pour filtrer l'entrée pour l'authentification des utilisateurs en fonction de leur emplacement.

Avant de commencer

Rôle requis : admin

Module d'extension requis : **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Propriété : activez la propriété d'authentification adaptative.

> **Remarque :**
> Les administrateurs peuvent créer la politique basée sur les filtres d'emplacement uniquement si l'emplacement est disponible pour la session utilisateur actuelle.

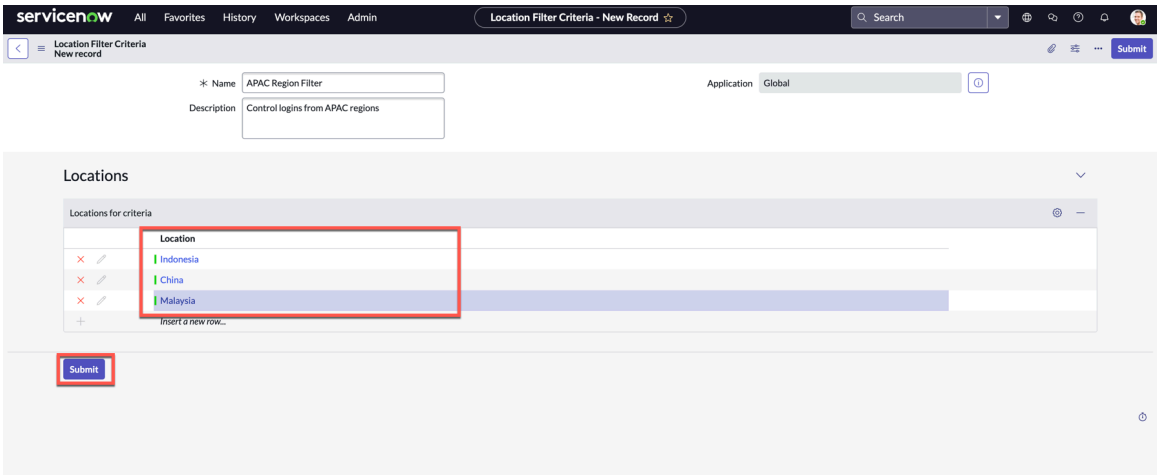
Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Critère de filtre** > **Critère de filtrage d'emplacement**.
2. Sélectionnez **Nouveau**.
3. Renseignez ces champs du formulaire.

Formulaire Critères de filtre 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**.
5. Spécifiez les emplacements.



6. Sélectionnez **Envoyer**.

Didacticiel : Utiliser les critères de filtre 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 - Location Based Access** (com.snc.zero_trust_location_access).

Propriété : activez la propriété d'authentification adaptative.

Remarque :
Les administrateurs peuvent créer la politique basée sur les filtres d'emplacement uniquement si l'emplacement est disponible pour la session utilisateur actuelle.

La procédure suivante décrit comment créer et utiliser les critères de filtre d'emplacement dans une politique d'authentification.

Procédure

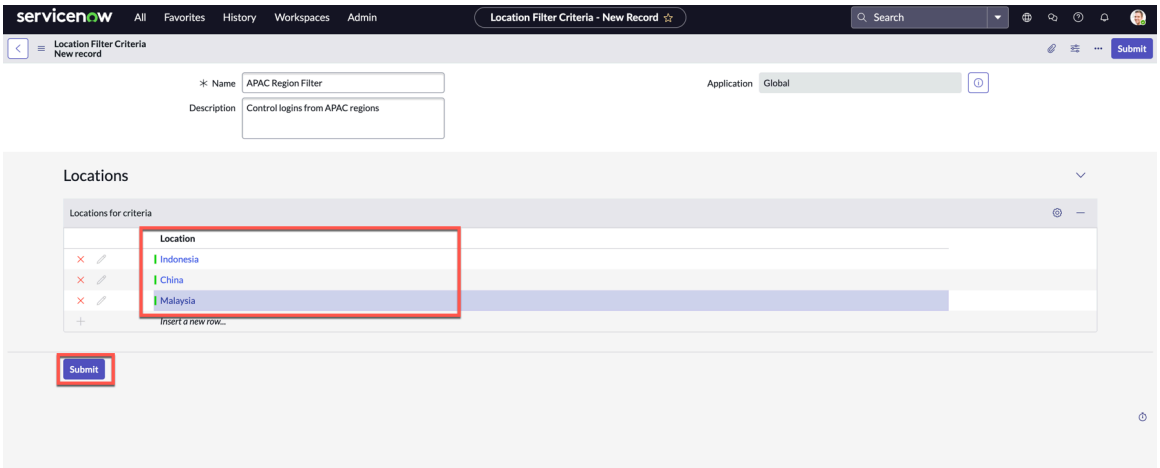
1. Accédez à la **Tous** > **Authentification Adaptative** > **Critère de filtre** > **Filtre d'emplacement**.
2. Sélectionnez **Nouveau**.
3. Renseignez ces champs du formulaire.

Formulaire Critères de filtre 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**.
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 depuis l'Indonésie, la Chine et la Malaisie pour votre instance.

6. Sélectionnez **Envoyer**.
7. Utilisez les critères de filtre créés dans l'un des contextes d'authentification (pré, post, MFA) et d'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 pour 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 - Location Based Access** (com.snc.zero_trust_location_access).

Créez un filtre d'emplacement avec les pays dans lesquels vous souhaitez restreindre l'accès aux utilisateurs en fonction de l'emplacement. Pour plus d'informations, consultez Créer un critère de filtre d'emplacement.

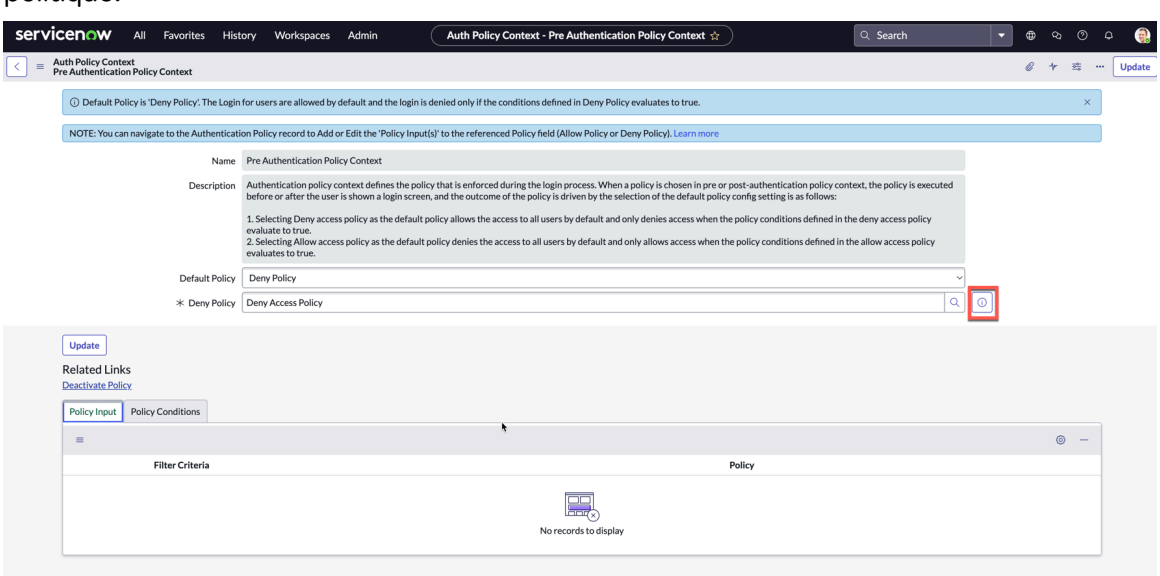
Procédure

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 Autoriser l'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 restreindre les connexions à partir des emplacements spécifiés. Vous pouvez choisir Refuser l'accès et la politique associée (Refuser l'accès) comme politique de pré-authentification et spécifier les entrées et conditions de la politique.

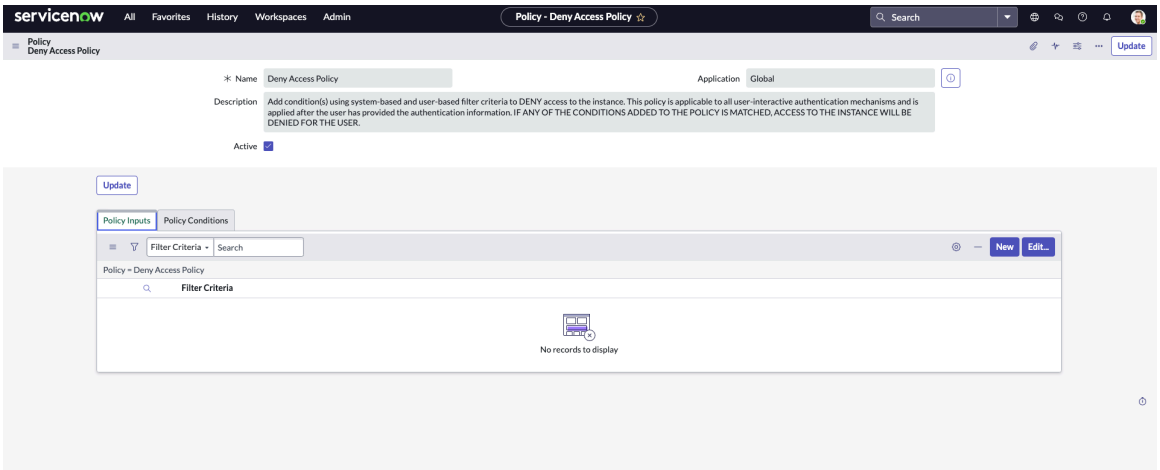


2. Sélectionnez l'icône d'information pour ouvrir l'enregistrement **de politique de refus** .

   Remarque :
   L'exemple décrit dans cette tâche est **Politique de refus**. Vous pouvez également utiliser la **politique d'autorisation** et définir les conditions en conséquence pour contrôler les connexions.

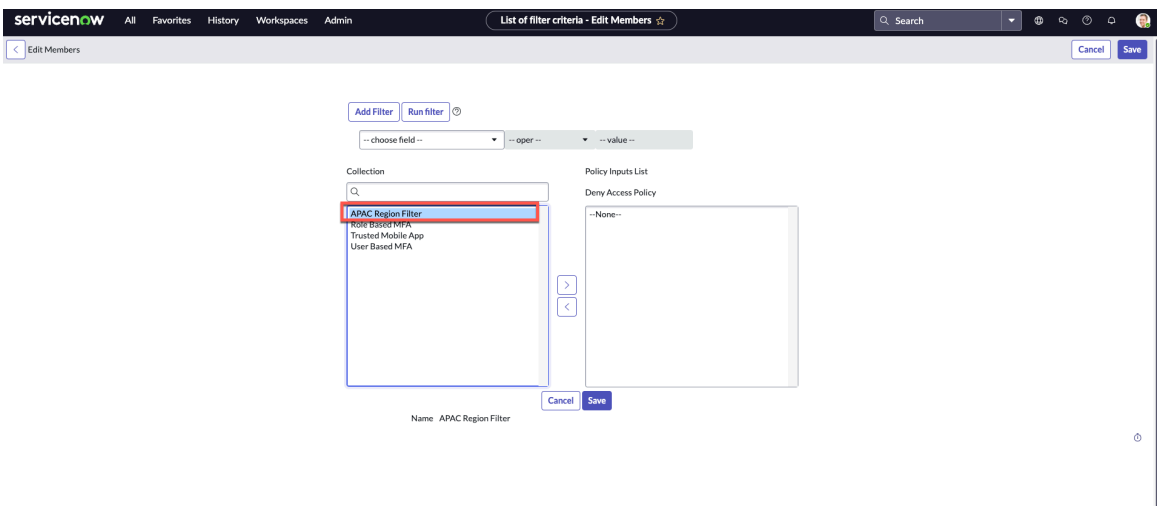
3. Dans la politique de refus d'accès, sous la section Entrées de politique, sélectionnez **Nouveau**.

Traduction automatique



4. Ajoutez l'entrée Filtre d'emplacement et **enregistrez**.

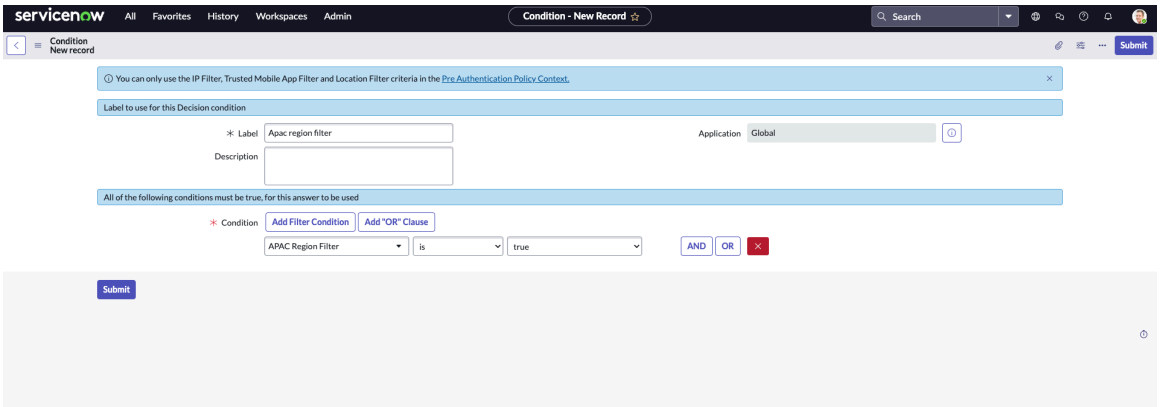
   Par exemple, Région APAC.



   Le filtre est ajouté en tant **qu'entrées de politique**.

5. Sélectionnez l'onglet Conditions de la politique, puis sélectionnez **Nouveau**.

6. Sur la page Conditions, fournissez l'étiquette, les conditions et définissez-les sur vrai.



Remarque :

- Dans cet exemple, la sélection de la condition true 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 false, 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 **Envoyer**.
   Les utilisateurs qui sélectionnent le lien d'instance et se connectent à partir des pays configurés voient 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 filtre d'emplacement Contexte de post-authentification

Utilisez les critères de filtrage d'emplacement créés dans le contexte de post-authentification.

Avant de commencer

Rôle requis : admin

Module d'extension requis : **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Créez un filtre d'emplacement avec les pays dans lesquels vous souhaitez restreindre l'accès aux utilisateurs en fonction de l'emplacement. Pour plus d'informations, consultez Créer un critère de filtre 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 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 Autoriser l'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 configurer un utilisateur ITIL avec une condition pour accéder à l’instance uniquement 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 Autoriser l’accès et la politique associée (Autoriser l’accès) comme politique de post-authentification et spécifier les entrées et conditions de la politique.

2. Sélectionnez l’icône d’information pour ouvrir l’enregistrement **Autoriser la politique** .

> **Remarque :**
> L’exemple décrit dans cette tâche est **Autoriser la politique**. Vous pouvez également utiliser la **stratégie de refus** et définir les conditions en conséquence pour contrôler les connexions.

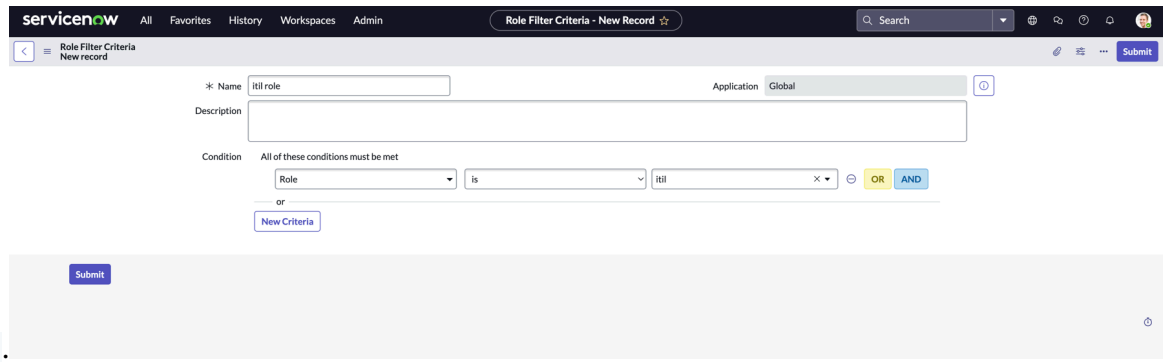
3. Dans Autoriser la politique d’accès, sous la section Entrées de politique, sélectionnez **Nouveau**.

4. Ajoutez les critères de filtre de rôle et les critères de filtre d’emplacement.

Traduction automatique

a. Ajout de critère de filtre de rôle :

- Créer une entrée de filtre de rôle au format



itil.

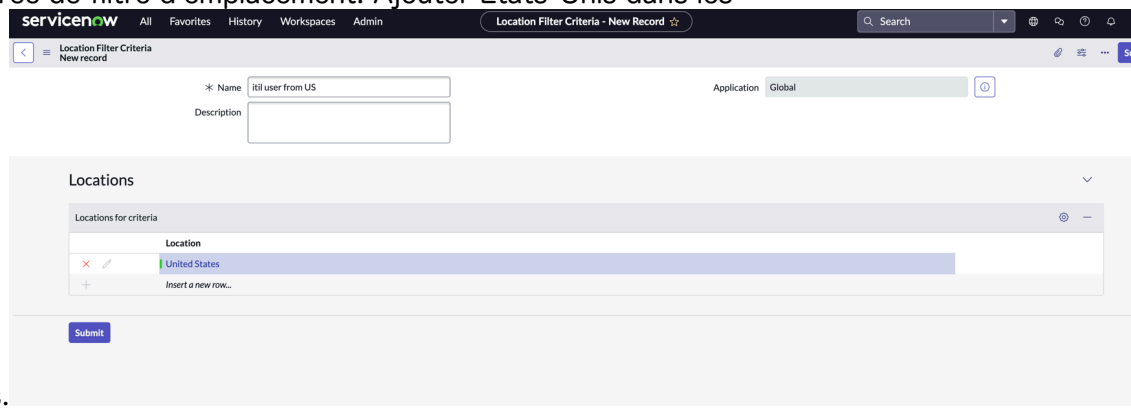
- Créez une condition de filtre de rôle et définissez-la sur

vrai.

Pour en savoir plus sur la création de critères de filtre de rôle, reportez-vous à Créer un critère de filtre de rôle.

b. Ajout de critères de filtre d'emplacement :

- Créez une entrée de filtre d'emplacement. Ajouter États-Unis dans les emplacements.

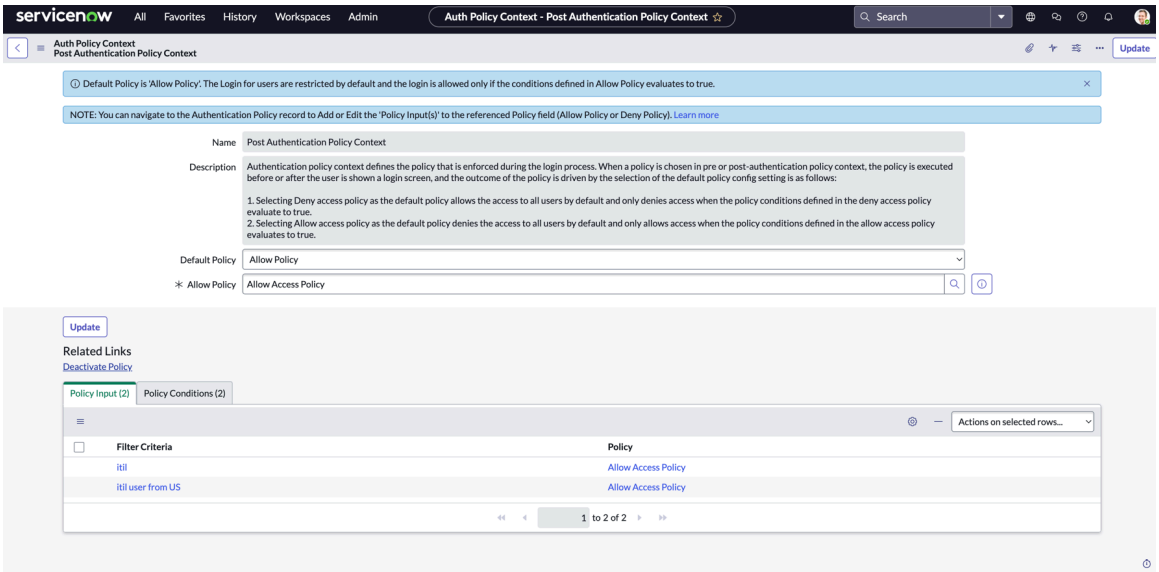


- Créez une condition de filtre d'emplacement et définissez-la sur vrai.

Pour en savoir plus sur la création de critères de filtre de rôle, reportez-vous à Créer un critère de filtre d'emplacement.

La politique d'accès affiche les entrées et conditions de politique qui sont créées dans les étapes précédentes :

- Entrées de la 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.



Remarque :

- Dans cet exemple, la sélection de la condition true implique que les utilisateurs ITIL qui se connectent dans le pays configuré (États-Unis) sont en mesure de 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 d'instance, spécifient leurs informations d'identification, puis se connectent en dehors du pays configuré (États-Unis) voient 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 filtre d'emplacement dans le contexte MFA

Utilisez les critères de filtre d'emplacement créés dans le contexte MFA.

Avant de commencer

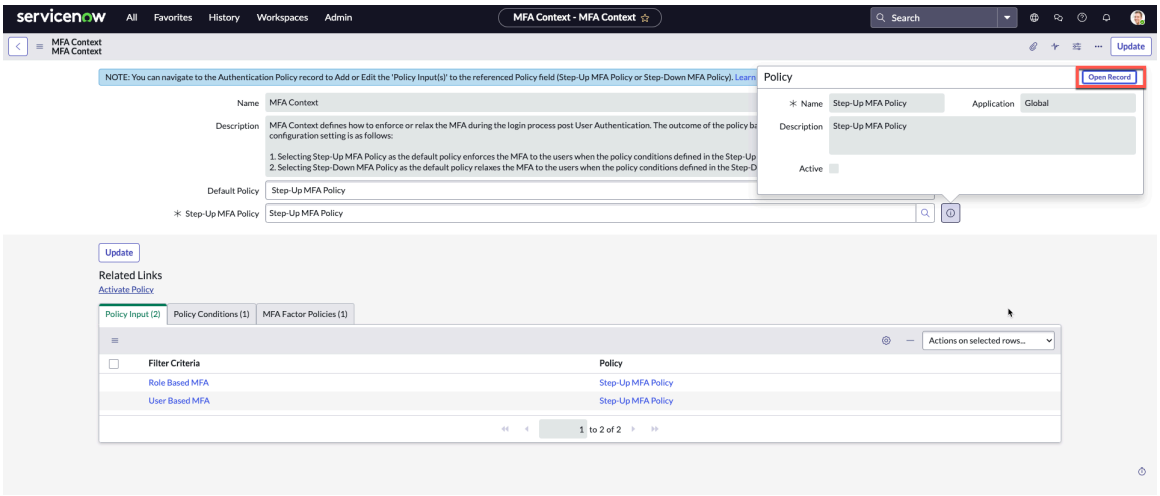
Rôle requis : admin

Module d'extension requis : **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

La procédure suivante décrit comment créer un filtre d'emplacement avec les pays pour lesquels vous souhaitez configurer l'authentification MFA comme deuxième facteur d'authentification auprès des utilisateurs en fonction de l'emplacement.

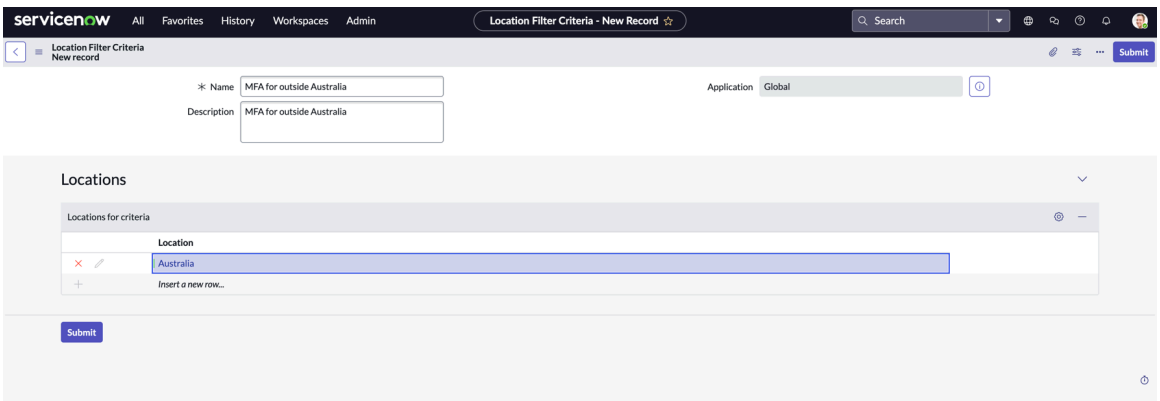
Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Contexte de la politique d'authentification** > **Contexte MFA**.
2. Sur la page **contextuelle MFA** , sélectionnez l'icône **Informations sur la politique MFA ascendante** et ouvrez l'enregistrement.

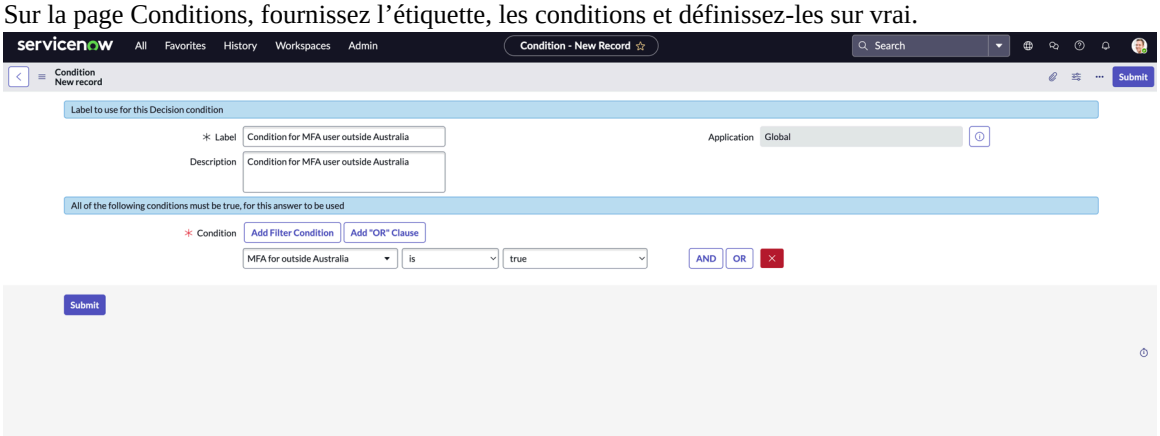


3. Sur la page Politique MFA ascendante, sous l'onglet Entrées de politique, sélectionnez **Nouveau**.
4. Ajoutez l'entrée Filtre d'emplacement et **soumettez**.

   Par exemple, vous souhaitez afficher l'authentification 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 sélectionnez **Nouveau**.
6. Sur la page Conditions, fournissez l'étiquette, les conditions et définissez-les sur vrai.



7. Sélectionnez **Envoyer**.
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.

Traduction automatique

Les utilisateurs situés en dehors du pays configuré (Australie) sélectionnent le lien d'instance, en spécifiant leurs informations d'identification ; s'affichera 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 - Location Based Access** (com.snc.zero_trust_location_access).

La procédure suivante décrit comment créer un filtre d'emplacement avec les pays que vous souhaitez supprimer ou limiter les rôles aux utilisateurs en fonction de l'emplacement.

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 de 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 est connecté, la liste des rôles fournis 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 lui sont fournis 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 des utilisateurs en fonction des pays configurés est la suivante :

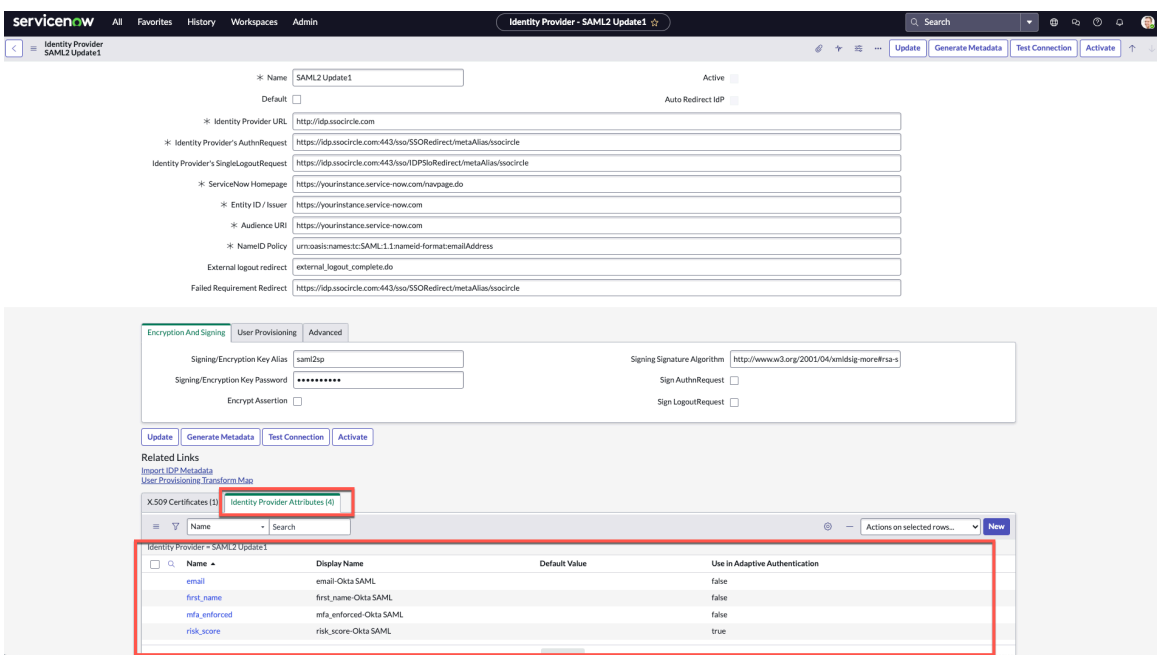
   - Si **l'option Supprimer les rôles**, les utilisateurs des pays configurés dans le filtre d'emplacement seront supprimés avec les rôles configurés pour la session.
   - Si **l'option Limiter aux rôles est définie sur Limiter aux rôles**, les utilisateurs des pays configurés dans le filtre d'emplacement ne disposent que des 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 Utiliser l'accès zéro confiance.

Filtre attributs du fournisseur d'identité

Utilisez les attributs du fournisseur d'identité reçus de la réponse SAML (Security Assertion Markup Language) du fournisseur d'identité (IdP) comme critère 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. Si la connexion est correctement testée, les attributs sont ajoutés dans un nouvel onglet de la page de configuration du fournisseur d'identité.



Vous pouvez également ajouter des attributs en sélectionnant **Nouveau** dans la section Attributs du fournisseur d'identité et utiliser ces attributs pour Authentification adaptative en la définissant sur `vrai`.

Les **attributs du fournisseur d'identité sont affichés** avec les détails suivants :

Formulaire Critères de filtre d'emplacement

Champ	Description
Nom	Nom de l'attribut fourni par le fournisseur d'identité.
Nom d'affichage	Nom d'affichage est le nom détaillé utilisé pour les critères de filtre.

Formulaire Critères de filtre d'emplacement (suite)

Champ	Description
	Remarque : Vous pouvez fournir un nom lisible en tant que nom d'affichage. Dans certains cas, le nom d'affichage fourni par les fournisseurs d'identité est long et non lisible.
Valeur par défaut	La valeur par défaut est utilisée pour l'évaluation des critères de filtre au cas où l'attribut serait manquant dans la réponse SAML.
Utiliser dans Authentification adaptative	Option pour utiliser l'attribut dans l'authentification adaptative.

Remarque :
Le nom et le nom d'affichage des attributs renseignés à partir d'IdP Azure sont 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 Utiliser 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** définie sur vrai. Un nouveau filtre a été créé sur la page Critères de filtre génériques.

Utiliser l'attribut du fournisseur d'identité comme critère de filtre

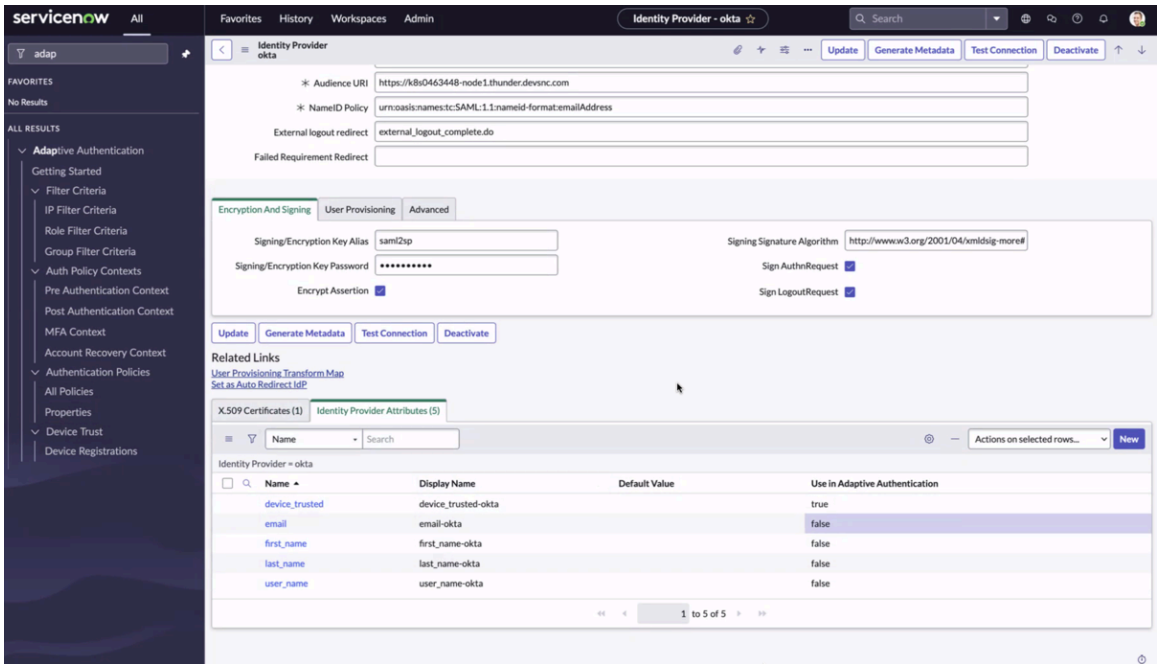
Utilisez l'attribut Fournisseur d'identité (IDP) de la réponse SAML (Security Assertion Markup Language) comme critère de filtre pour la politique d'authentification.

Avant de commencer
Rôle requis : admin

Vous pouvez créer une politique d'accès à la session à l'aide du contexte de politique (pré-authentification, post-authentification, authentification multifacteur) et des critères de filtre (rôle, groupe, adresse IP, emplacement) avec des entrées et des conditions de politique.

La procédure suivante montre les étapes de configuration de l'attribut IdP de la réponse SAML en tant qu'entrée de politique pour contrôler l'authentification dans le **contexte de post-authentification**, le **contexte d'authentification multifacteur (MFA)** et **l'accès à la session Zero Trust - basé sur une politique**.

Les attributs IdP Okta sont affichés dans la capture d'écran suivante. Vous devez définir l'Utilisation dans l'authentification adaptative sur vrai pour l'utiliser dans le **contexte de post-authentification**, le **contexte de l'authentification multifacteur (MFA)** et les politiques **d'accès à la session Zero Trust - basées sur une politique** .



Remarque :
Les politiques d'accès à la session post-autorisation, MFA, Zero Trust - basé sur une politique s'exécutent une fois que les utilisateurs ont entré les informations d'identification ou la réponse SSO.

Procédure

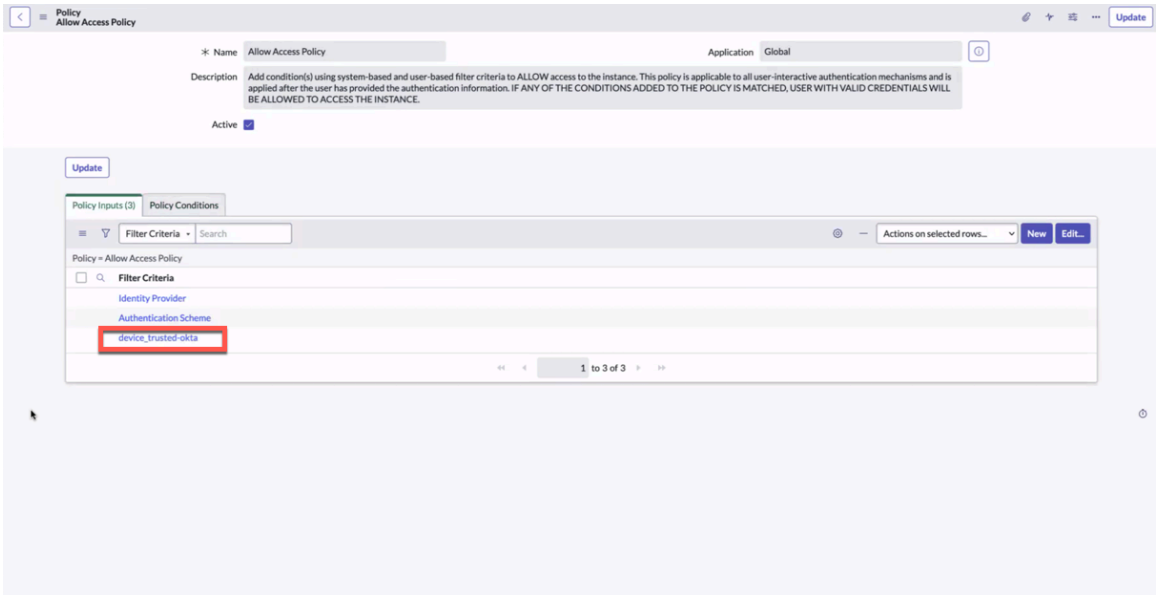
1. Utilisation de l'attribut IdP dans le contexte de la politique de post-authentification.
   Exemple : configuration pour activer les connexions à partir des attributs IdP Okta si l'appareil est approuvé.

   a. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de la politique post-authentification.**.

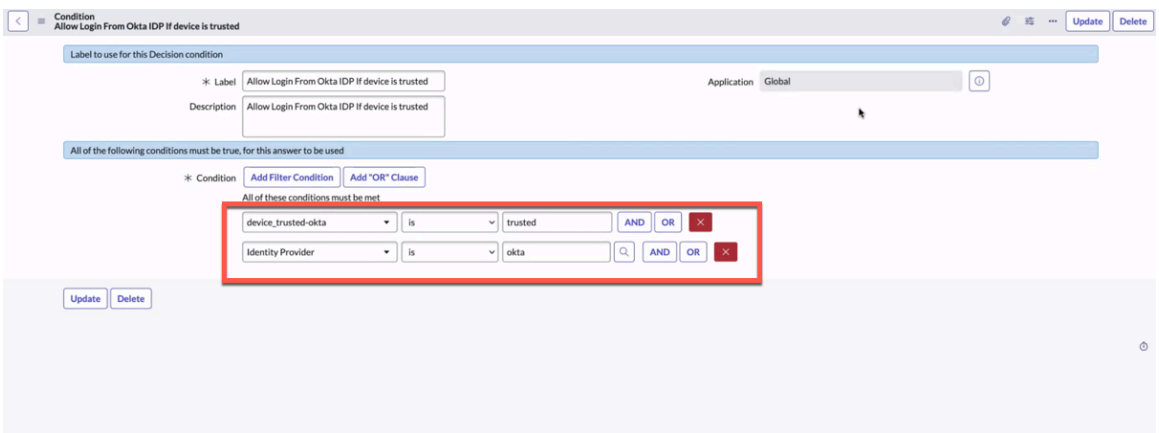
   b. Sélectionnez **Autoriser la politique** et ouvrez l'enregistrement de la politique.

   c. Dans l'entrée Politique, créez l'entrée et la condition de politique.

- **Entrée de politique** : Ajouter **device_trusted-okta**.



- **Conditions de la 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.

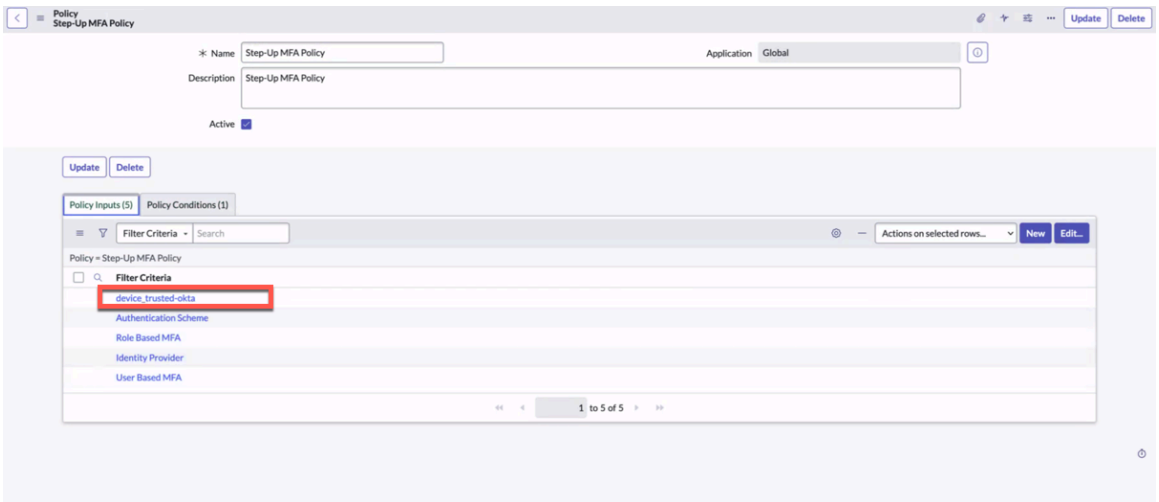
Pour plus d'informations sur la création d'un contexte de post-authentification avec une politique et une condition, reportez-vous à Contexte postérieur à l'authentification.

2. Utilisation de l'attribut IdP dans le contexte de la politique MFA.
Exemple : configuration permettant d'activer l'authentification multifacteur à partir des attributs IdP Okta si l'appareil n'est pas approuvé.

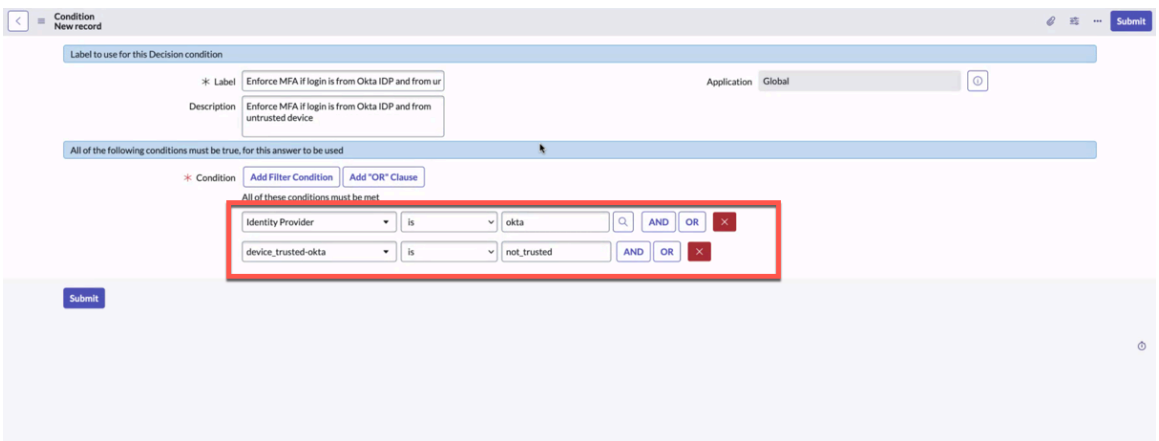
a. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de la politique d'authentification MFA.**.

b. Dans l'entrée Politique, créez l'entrée et la condition de politique.

- **Entrée de politique** : Ajouter **device_trusted-okta**.



- **Conditions de la politique** : **device_trusted-okta** est `not_trusted` et **le fournisseur d'identité** est `okta`.



Selon cette configuration, lorsque l'appareil n'est pas approuvé par Okta (IdP), l'utilisateur affiche une authentification à deuxième facteur pour se connecter à l'instance.

Pour plus d'informations sur la création d'un contexte MFA avec une politique et une condition, reportez-vous à la section Contexte MFA (Multi-Factor Authentication).

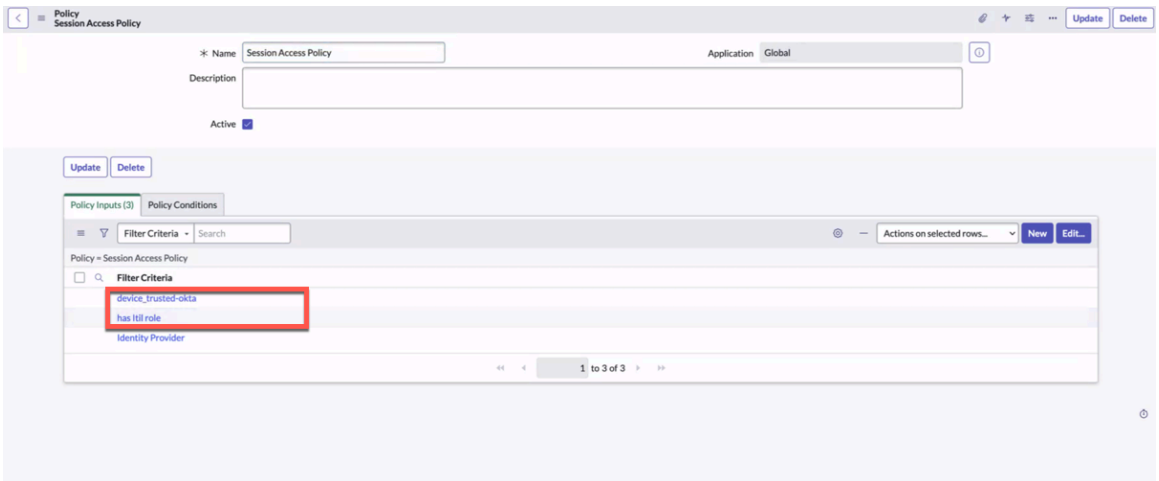
3. Utilisation de l'attribut IdP dans l'accès à la session Zero Trust - Basé sur une politique.
Exemple : configuration pour réduire le privilège du rôle `ITIL` à partir des attributs IdP Okta si l'appareil n'est pas approuvé.

a. Accédez à la **Tous** > **Accès zéro confiance** > **Configurations du rôle d'accès à la session**.

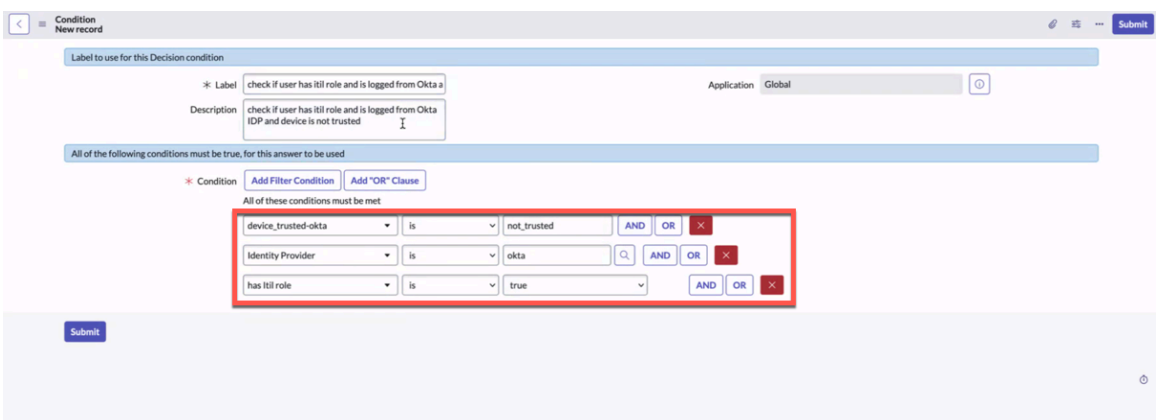
b. Créez une configuration du rôle d'accès à la session.

c. Dans l'entrée Politique, créez l'entrée et la condition de politique.

- **Entrée de politique** : Ajouter **device_trusted-okta** et **dispose d'un rôle itil**.



- **Conditions de la politique** : **device_trusted-okta** est `not_trusted`, **le fournisseur d'identité** est `okta` et **a le rôle itil** est `vrai`.



Selon 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 une session Zero Trust - Basé sur une politique avec une politique et une condition, consultez Accès zéro confiance.

Contextes des politiques d'authentification

Utilisez les contextes de politique d'authentification pour déterminer comment et quand votre instance applique les 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 des entrées et des conditions relatives à la façon dont votre instance gère l'authentification.

Contexte de pré-authentification

Les politiques dans le contexte de la pré-autorisation s'exécutent lorsqu'un utilisateur accède pour la première fois à l'instance, avant qu'un écran de connexion ne s'affiche. Vous pouvez utiliser le contexte de préautorisation pour autoriser ou refuser l'accès avant que vos utilisateurs soient invités à saisir leurs informations d'identification de connexion

en fonction de la politique que vous avez sélectionnée. Étant donné que ces politiques procèdent à une évaluation 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'utilisateurs.

Pour plus de détails sur ce contexte, voir Contexte de pré-authentification.

Contexte postérieur à l'authentification

Les politiques dans le contexte de post-autorisation s'exécutent une fois que les utilisateurs ont entré leurs informations d'identification ou leur réponse SSO. Votre instance autorise ou refuse l'accès en fonction de la politique que vous avez 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 de détails sur ce contexte, voir Contexte postérieur à l'authentification.

Contexte MFA (Multi-Factor Authentication)

Les politiques affectées au contexte MFA définissent s'il faut appliquer la MFA pendant le processus de connexion. La nécessité ou non d'appliquer la MFA par votre instance est déterminée par la configuration des politiques dans ce contexte. Pour plus de détails sur ce contexte, voir Contexte MFA (Multi-Factor Authentication).

Contexte de récupération de compte

Les administrateurs peuvent configurer la récupération de compte (ACR) pour effectuer des activités de récupération telles que le traitement d'une mauvaise 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'il n'y a pas au moins un compte configuré. Pour plus d'informations sur le contexte qui peut être défini, reportez-vous à la section Contexte de récupération de compte.

Contexte de validation de session

Le contexte de validation de session peut être utilisé avec le cadre de travail des politiques 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. Vous trouverez des détails sur ces options dans la documentation décrivant ces contextes individuels.

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 les utilisateurs ne voient un écran de connexion.

Enregistrement de contexte de pré-authentification

Les politiques dans le contexte de la pré-autorisation s'exécutent lorsqu'un utilisateur accède pour la première fois à l'instance, avant qu'un écran de connexion ne s'affiche.

Vous pouvez utiliser le contexte de pré-authentification pour autoriser ou refuser l'accès avant que vos utilisateurs soient invités à saisir leurs informations d'identification de connexion en fonction de la politique que vous avez sélectionnée. Étant donné que ces politiques procèdent à une évaluation 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'utilisateurs.

Utilisez les champs dans l'enregistrement de contexte de la politique de pré-authentification pour définir comment votre instance utilise votre politique.

Formulaire Contexte de pré-authentification

Champ	Description
Nom	Nom du contexte de la 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. **Autoriser la politique** Refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions sélectionnées par la politique 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 **Politique de refus** sont évaluées comme vraies.
Autoriser la politique	La politique utilisée pour 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 pour ce contexte utilise. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Refuser la politique**.

Remarque :

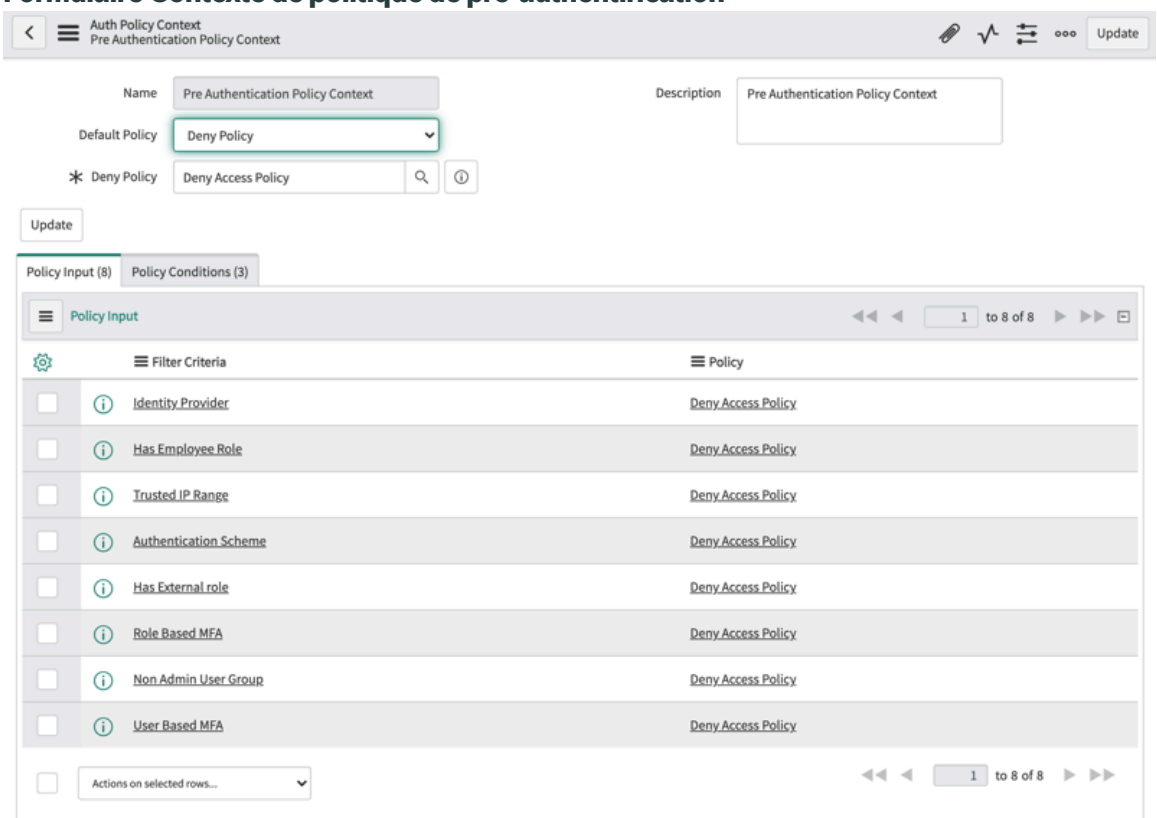
Vous ne pouvez utiliser que les critères Filtre IP, Filtre d'application mobile de confiance et Filtre d'emplacement dans le contexte de la politique de pré-authentification.

Entrées et conditions de la politique

Les onglets **Entrée de politique** et **Conditions de politique** affichent les entrées et 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 votre politique, accédez à la politique à l'aide de l'icône de référence (ⓘ) 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 **stratégie de refus d'accès**. Cette politique dispose d'un ensemble d'entrées et de conditions qui s'affichent dans les onglets **Entrée de politique** et **Condition de politique** .

Formulaire Contexte de politique de pré-authentification



Contexte postérieur à l'authentification

Le contexte de 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 après que vos utilisateurs ont vu un écran de connexion.

Enregistrement de contexte postérieur à l'authentification

Les politiques dans le contexte de post-autorisation s'exécutent une fois que les utilisateurs ont entré leurs informations d'identification ou leur réponse SSO. Votre instance autorise ou refuse l'accès en fonction de la politique que vous avez sélectionnée. Étant donné que vos utilisateurs se sont identifiés via leurs informations d'identification de connexion, la politique 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 politique post-authentification pour définir comment votre instance utilise votre politique.

Formulaire Contexte post-authentification

Champ	Description
Nom	Nom du contexte de la politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte

Formulaire Contexte post-authentification (suite)

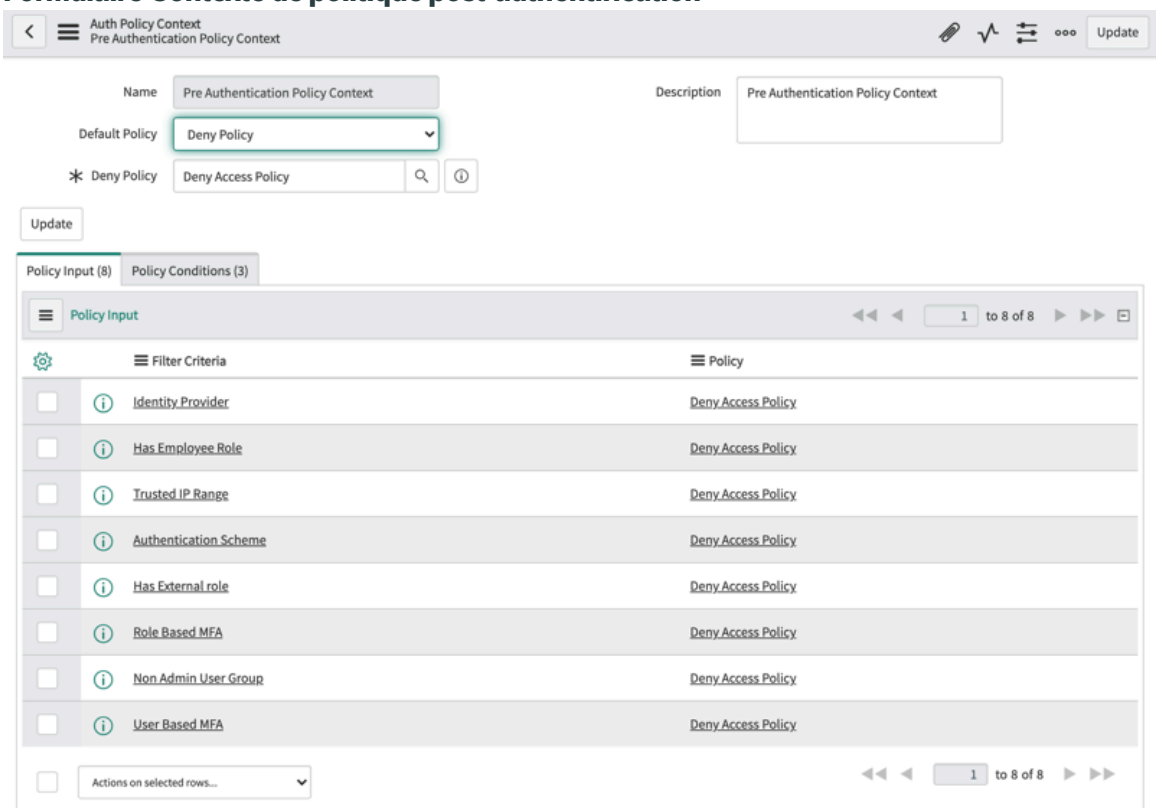
Champ	Description
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez une option parmi les suivantes. **Autoriser la politique** Refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions sélectionnées par la politique 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 **Politique de refus** sont évaluées comme vraies.
Autoriser la politique	La politique utilisée pour 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 pour 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 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 stratégie, accédez à la stratégie à l'aide de l'icône de référence ( ) 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 **stratégie de refus d'accès**. Cette politique dispose d'un ensemble d'entrées et de conditions qui s'affichent dans les onglets **Entrée de politique** et **Condition de politique** .

Formulaire Contexte de politique post-authentification



Contexte MFA (Multi-Factor Authentication)

Le contexte de politique MFA (Multi-Factor Authentication) utilise une politique pour définir comment et quand la MFA est appliquée pendant le processus de connexion.

Enregistrement de contexte MFA

Le contexte de la politique MFA (Multi-Factor Authentication) définit si vos utilisateurs doivent fournir une deuxième forme d'authentification lors de la connexion. Ce contexte ne refuse pas l'accès à votre instance en tant que politiques de post-authentification et de pré-authentification. La politique que vous sélectionnez dans ce contexte prime sur les configurations basées sur les utilisateurs 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 politique post-authentification pour définir comment votre instance utilise votre politique.

Remarque :

- Si la politique par défaut est **Politique MFA ascendante**, les utilisateurs s'affichent avec l'authentification multifacteur si la politique configurée dans la **politique MFA donne la** valeur vrai. 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**).

Formulaire de contexte MFA

Champ	Description
Nom	Nom du contexte de la 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. **Politique MFA ascendante** Applique MFA aux utilisateurs lorsque les conditions de politique définies dans le champ **Politique de MFA ascendante** sont évaluées comme vraies. **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 MFA descendante** sont évaluées comme true.
Politique MFA ascendante	La politique utilisée pour 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 pour ce contexte utilise. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Politique MFA descendante**.

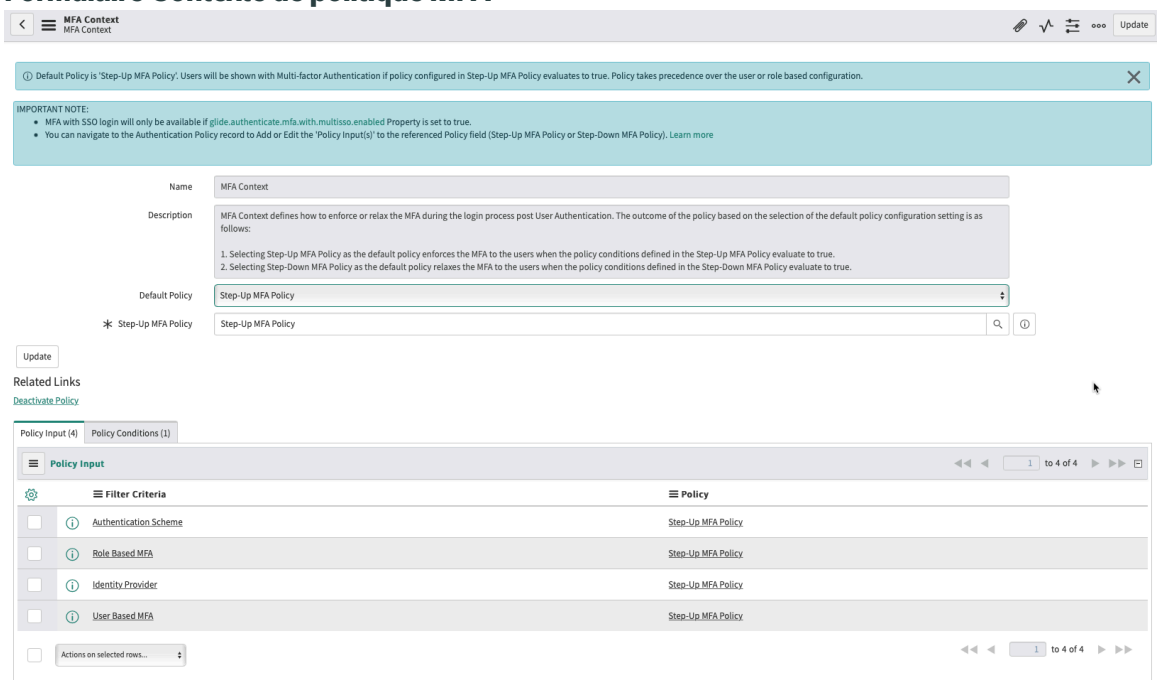
Entrées et conditions de la politique

Les onglets **Entrée de politique** et **Conditions de politique** affichent les entrées et les conditions de la politique sélectionnée dans le champ **Politique MFA ascendante** ou **Politique 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 stratégie, accédez à la politique à l'aide de l'icône de référence ( ) en regard du champ **Politique MFA ascendante** ou **Politique MFA descendante** .

Remarque :
Les conditions de politique peuvent être créées à partir d'ici, mais 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 ascendante**. Cette politique dispose d'un ensemble d'entrées et de conditions qui s'affichent dans les onglets **Entrée de politique** et **Condition de politique** .

Formulaire Contexte de politique MFA



Contexte de récupération de compte

Le contexte de récupération de compte utilise une politique pour définir comment et quand la récupération de 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 **Autoriser la politique** sont évaluées comme vraies.

Utilisez les champs de l'enregistrement de contexte de récupération de compte pour définir la façon dont votre instance utilise la politique.

Formulaire de contexte de récupération de compte

Champ	Description
Nom	Nom du contexte de la 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 : • 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**.

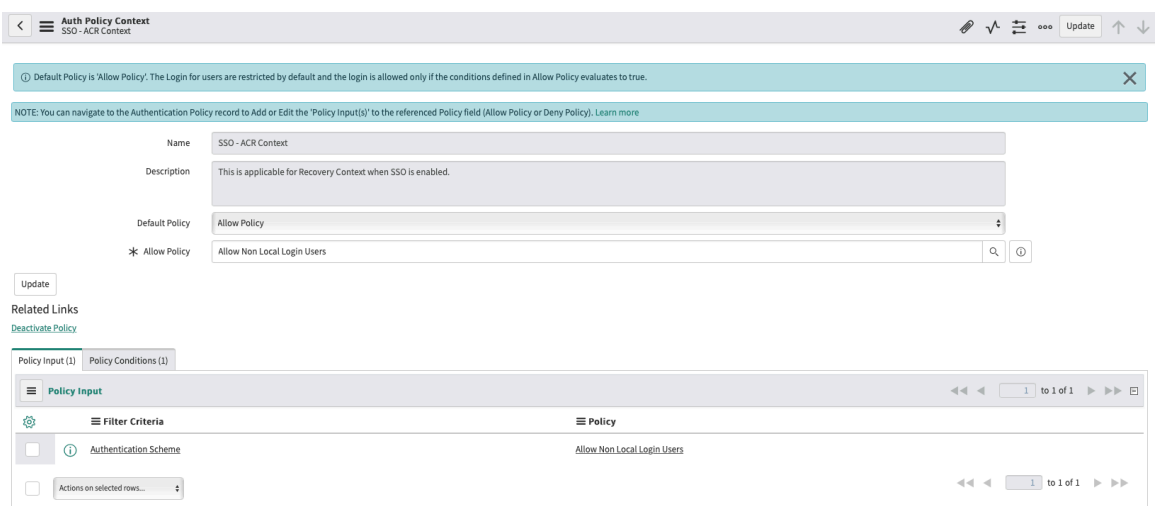
Formulaire de contexte de récupération de compte (suite)

Champ	Description
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 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 stratégie, accédez à la politique à l'aide de l'icône **Afficher l'aperçu de cet enregistrement** en regard du champ **Autoriser la politique** ou **Refuser la politique** .

Remarque :
Les conditions de politique peuvent être créées à partir d'ici, mais 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 des Authentification adaptative politiques. 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.

La stratégie de contexte de validation de session peut être utilisée conjointement avec la stratégie de post-authentification, où un administrateur peut appliquer des restrictions IP à certains ou à tous les utilisateurs pendant la session connectée.

La fonctionnalité de 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 la session sont les suivants :

- Refuser la stratégie : sélectionner la stratégie Refuser l'accès comme stratégie par défaut permet aux utilisateurs de poursuivre la session par défaut. La session n'est interrompue que lorsque l'une des conditions de politique définies dans la politique de refus d'accès est évaluée comme vraie.
- Autoriser la politique : sélectionner la politique d'accès 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 pour une politique d'authentification est défini par défaut sur **Autoriser la politique** .
- Le contexte de validation de session est implémenté via la politique Autoriser. Il n'est pas recommandé de définir le contexte pour 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 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 le suivant :

- Disponible uniquement pour les utilisateurs authentifiés.
- Non applicable pour les sessions d'utilisateurs invités ou les applications Mobile natives.
- Facultative et basée sur l'exigence qu'elle peut être configurée.
- Exécuté uniquement pour les demandes postérieures à la connexion.

Avantages de la validation de session

Le contexte de validation de session présente les avantages suivants :

- Limite l'accès au ServiceNow® moment où les pirates de l'air copient les cookies de session d'un utilisateur d'un appareil à un autre pour usurper l'identité de la session.
- Limite l'accès à la session de l'utilisateur s'il utilise un réseau non sécurisé.
- Configure les différentes règles et plages IP par groupe d'utilisateurs ou par rôle pour les connexions des utilisateurs.

Enregistrement de contexte de validation de session

Les politiques dans le contexte de validation de session exécutent des demandes après la connexion.

Utilisez les champs dans l'enregistrement de contexte de politique de validation de session pour définir comment votre instance utilise votre politique.

Formulaire de contexte de validation de session

Champ	Description
Nom	Nom du contexte de la 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. **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 comme vraies. **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	Politique utilisée pour ce contexte. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Autoriser la politique**.
Refuser la politique	Politique utilisée pour 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 comme Autoriser la politique ou Refuser la politique en fonction de l'entrée et des conditions de la politique.

Remarque :

Vous ne pouvez utiliser que les critères de filtrage 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 conditions de la politique sélectionnée dans le champ Autoriser la **politique** ou Refuser la **politique** . Ces onglets servent de référence ; mais ils ne peuvent pas être utilisés 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 (ⓘ) en regard du champ **Autoriser la politique** ou **Refuser la politique** .

Activer le contexte de validation de session

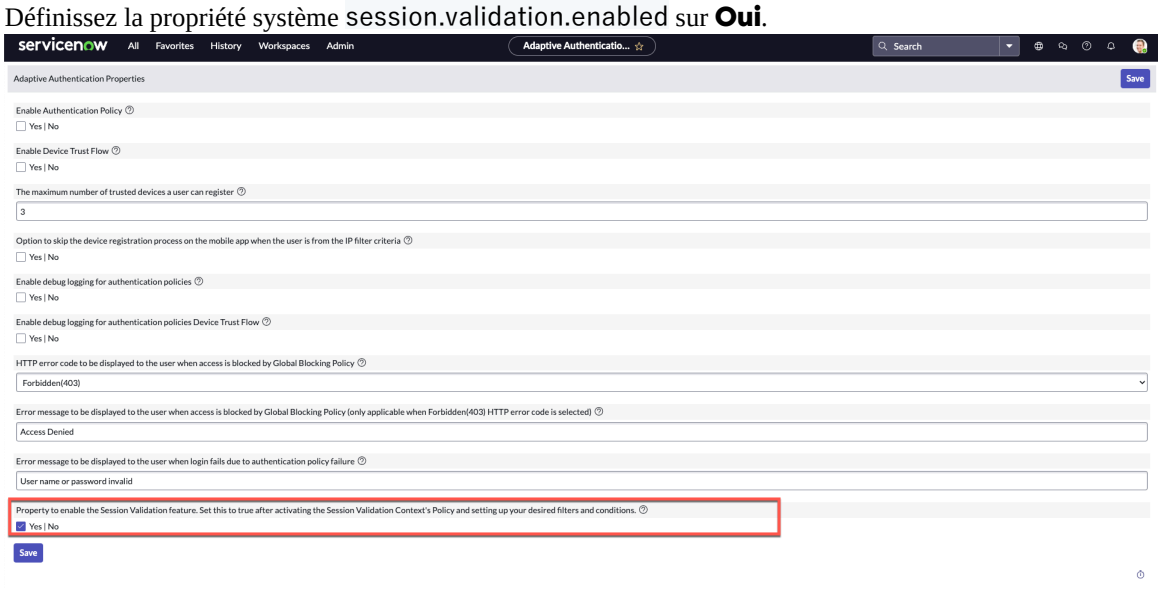
Utilisez le contexte de validation de session pour restreindre l'accès lorsque ServiceNow® les pirates de l'air copient les cookies de session d'un utilisateur d'un appareil à un autre pour usurper l'identité de la session ou restreignent l'accès à la session de l'utilisateur s'il utilise un réseau non sécurisé.

Avant de commencer
Rôle requis : admin

Pour utiliser la validation de session, vous devez effectuer les étapes suivantes :

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les stratégies**.
2. Sélectionnez la **politique de validation** de session sur la page Stratégies (sys_authentication_policy_list.do).
3. Spécifiez **les entrées et les** conditions de **la politique**.
4. Définissez les conditions sur **Vrai** ou **Faux** pour les filtres que vous avez ajoutés.
5. Cochez la case **Actif** pour activer la stratégie après avoir configuré la validation de session La politique est configurée avec des entrées et des conditions de politique.
6. Cochez la 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 la fonctionnalité. Pour en savoir plus, consultez Didacticiel : Configurer la validation de session.

Didacticiel : Configurer la validation de session

Configurez la validation de session dans le cadre de travail d'authentification adaptative pour fournir une couche supplémentaire de protection contre le détournement de session ou de cookies.

Avant de commencer

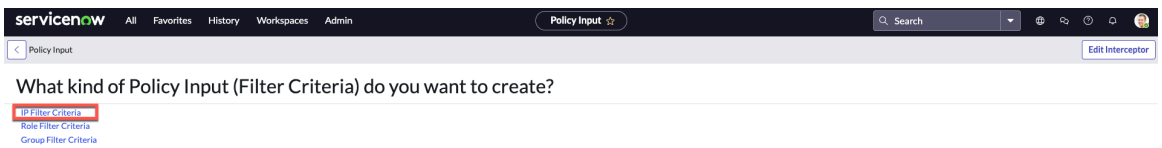
Rôle requis : admin

Module **d'extension requis : Adaptive Authentication** (com.snc.adaptive_authentication)

Pour configurer la validation de session, vous devez effectuer les étapes suivantes :

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les stratégies**.
2. Sélectionnez la **politique de validation** de session sur la page Stratégies (sys_authentication_policy_list.do).
3. Sélectionnez **Entrées de la politique**.
   a. Sélectionnez **Nouveau** ou **Modifier**.
   b. Choisissez le type d'entrée de politique (critères de filtre) que vous souhaitez créer.
   Les options disponibles sont les critères de filtre d'adresse IP, de rôle et de groupe. Choisissons **Critères de filtre**



   IP.

   c. Remplissez le formulaire avec les détails du filtre et fournissez la **plage d'adresses IP**.

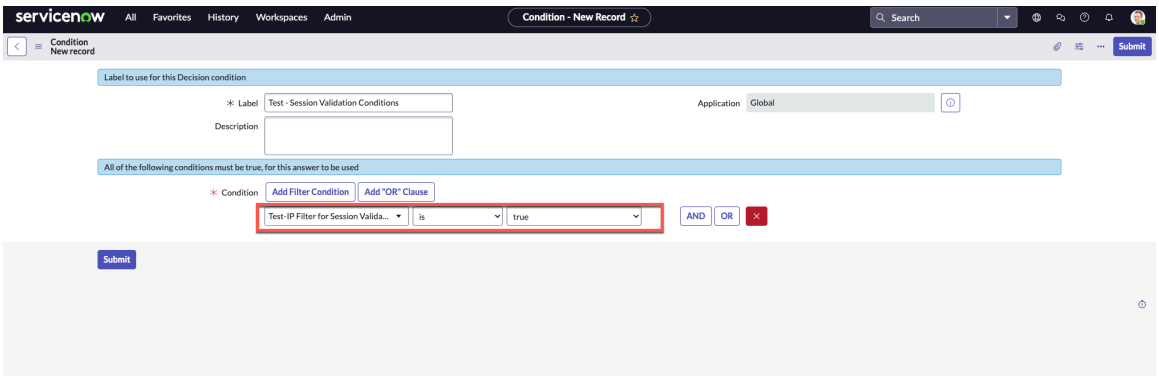
   Pour en savoir plus sur la création d'un filtre IP, reportez-vous à la section Créer un critère de filtre d'adresses IP.

   d. Sélectionnez **Envoyer**.

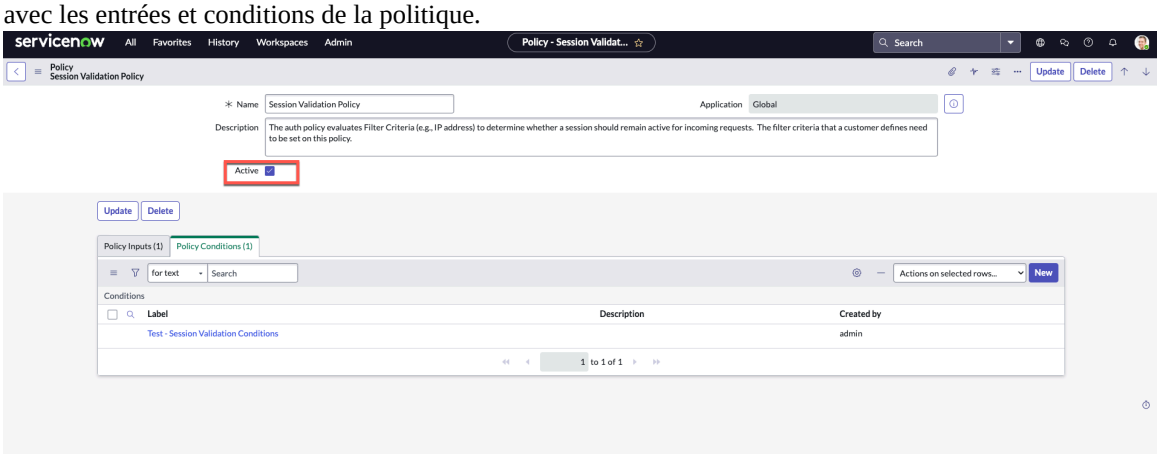
4. Sélectionnez **Conditions de politique** sur la page Politique de validation de session.
   a. Sélectionnez **Nouveau**.
   b. Remplissez le formulaire et définissez la condition pour l'entrée de politique.

Remarque :

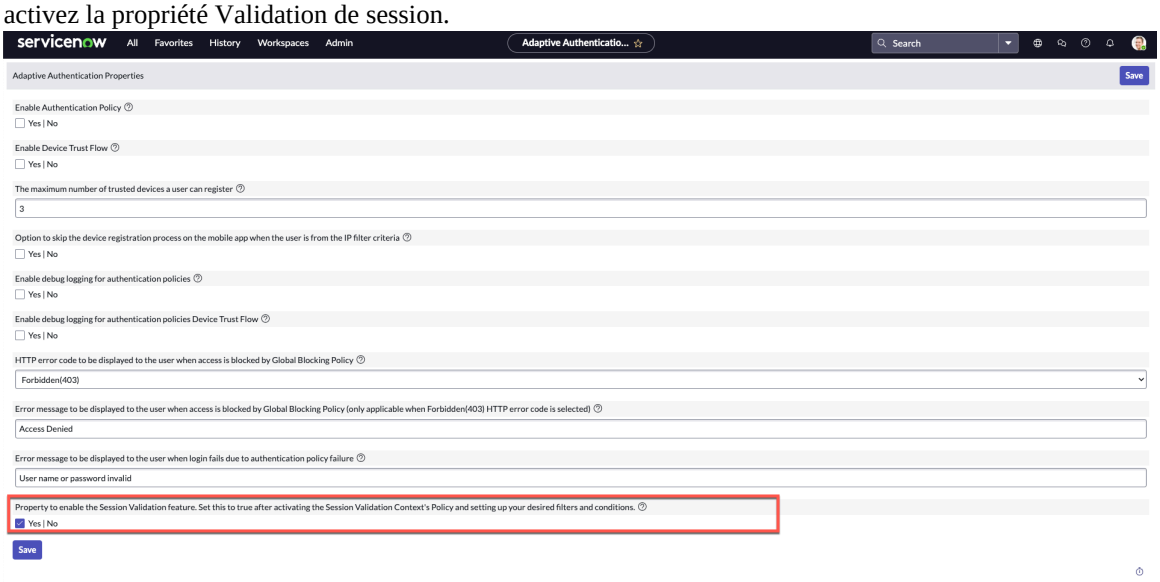
Vous pouvez définir les conditions sur Vrai ou Faux en fonction de la configuration de l'entrée de politique. Dans cet exemple, elle est définie sur true. Dans ce cas, définir la condition sur vrai permet uniquement à l'utilisateur disposant de l'adresse IP configurée de se connecter.



5. Cochez la case Actif pour activer la stratégie une fois que la politique de validation de session est configurée avec les entrées et conditions de la politique.



6. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés** et activez la propriété Validation de session.

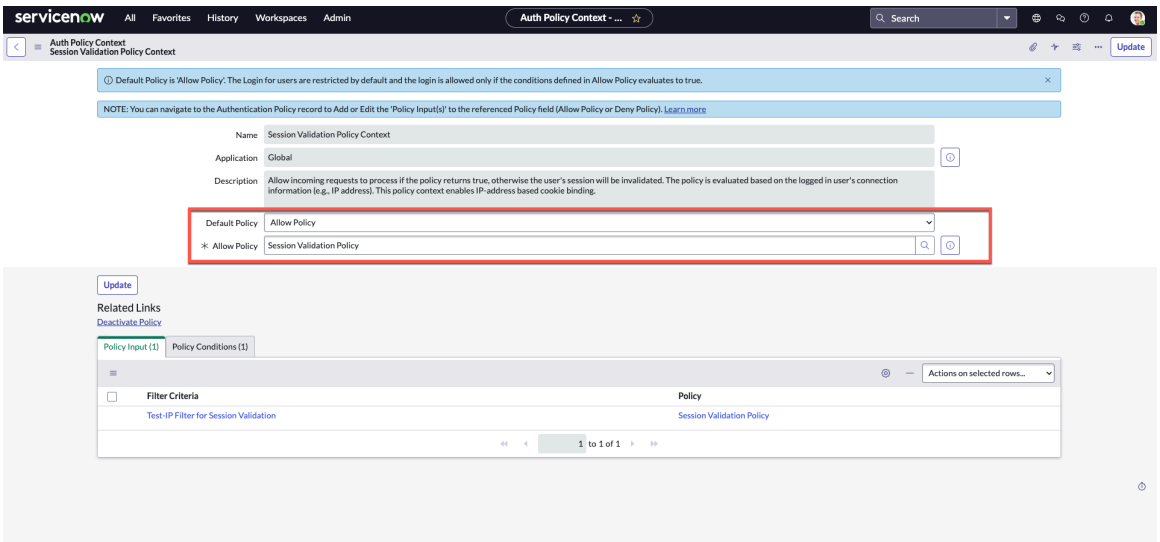


7. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de validation de la session**.

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 ServiceNow® lorsque les 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.
- Limite l'accès à la session de l'utilisateur s'il utilise un réseau non sécurisé.

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 **Autoriser la politique d'accès** sont évaluées comme vraies.

Utilisez les politiques d'authentification intégrées ou créez une politique d'authentification en fonction de vos exigences de sécurité. Vous pouvez trouver les politiques sur votre instance en accédant à **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les stratégies**.

Remarque :
À tout moment, la politique d'autorisation d'accès ou la politique de refus d'accès peuvent être exécutées, mais pas les deux.

Politique	Description
Autoriser la politique d'accès	Rejette par défaut toutes les demandes d'authentification. Autorise uniquement les demandes

Politique	Description
	d'authentification qui correspondent aux conditions de politique spécifiées.
Autoriser la politique de pré-authentification	Autoriser la politique de pré-authentification d'accès.
Autoriser les utilisateurs connectés non locaux	Choisissez cette stratégie pour autoriser les utilisateurs connectés non locaux. 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 stratégie peut être utilisée comme alternative au contrôle d'accès à l'adresse IP.
Politique de validation de la 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 locale de refus de connexion	Choisissez cette stratégie 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 de l'authentification MFA. Lorsque les conditions de politique définies dans la politique MFA ascendante sont évaluées comme true, 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 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 stratégies**.

   Remarque :
   Pour voir des exemples de politiques terminées, vous pouvez passer en revue ces politiques sur votre instance :

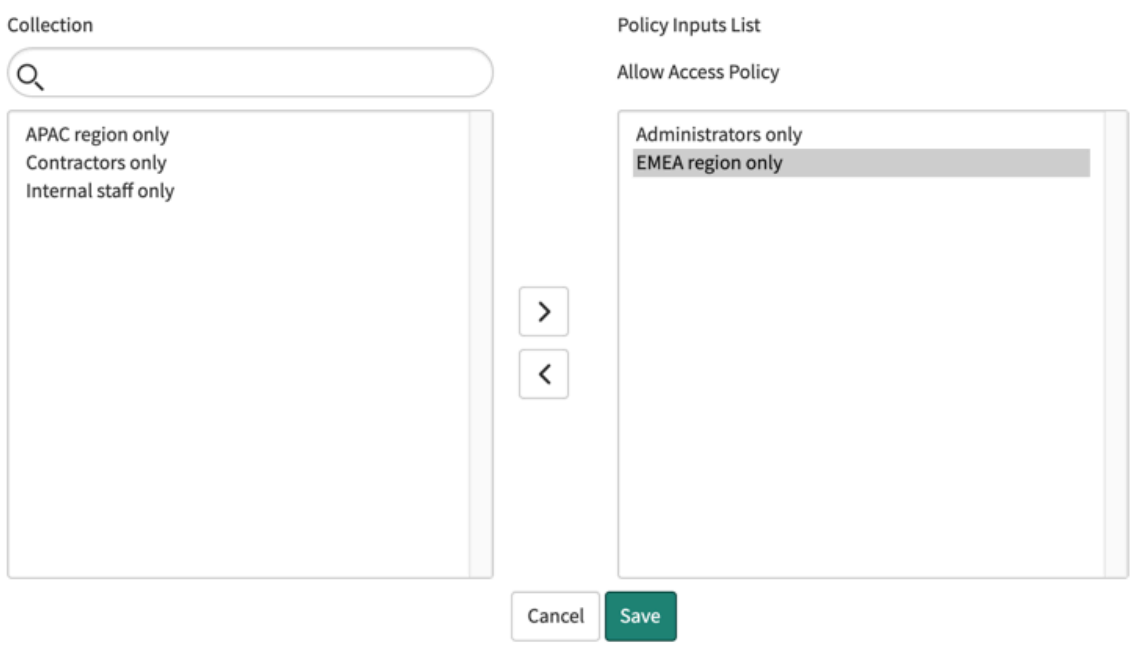
   - STRATÉGIE DE DÉMONSTRATION : autoriser la connexion locale pour les administrateurs à partir de la plage IP de confiance uniquement
   - POLITIQUE DE DÉMONSTRATION : autoriser la connexion locale pour les administrateurs uniquement
   - POLITIQUE DE DÉMONSTRATION : restreindre l'authentification basée sur le nom d'utilisateur et le 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 Politique

Champ	Description
Nom	Nom de votre politique.
Application	L'application incluse dans le périmètre pour la politique. Ce champ est rempli automatiquement avec l'application actuelle.
Description	Description de la politique
Actif	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 **la liste Entrées de politique** de la liste **Politique d'accès autorisé** .



Remarque :
Pour en savoir plus sur la création des critères de filtre à utiliser dans cette section, reportez-vous à la section .

6. Cliquez sur **Nouveau** dans l'onglet **Conditions de la politique**.
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) qui est utilisée pour évaluer les demandes d'authentification. Par exemple, vous pouvez créer des conditions qui n'autorisent que les prestataires d'une liste d'adresses IP fiables.

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 OR de toutes les conditions de politique. Cela signifie que la police 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 utilisateurs ont un accès à l'instance ou si la MFA est appliquée pour vos utilisateurs.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Contextes de politique d'authentification**, puis sélectionnez l'une des entrées en fonction de vos besoins.

Contexte de pré-authentification

Utilisez le contexte de préautorisation 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 post-autorisation pour évaluer votre politique une fois que l'utilisateur a saisi 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 de ce contexte peuvent effectuer son évaluation en fonction des données 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 définie en fonction des conditions définies comme filtre et permettant d'accéder 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 de détails sur ces contextes, reportez-vous à Contextes des politiques 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 **Refuser la politique** ou **Autoriser la politique** , selon la sélection dans le champ **Politique par défaut** .

Contexte MFA

Ce contexte dispose d'un champ **Politique MFA ascendante** ou **Politique MFA descendante** , selon 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** , selon la sélection dans le champ **Politique par défaut** .

4. Cliquez sur **Mettre à jour**.
Après avoir mis à jour l'enregistrement, vous pouvez afficher les entrées et les conditions de votre politique dans les onglets **Entrée de la politique** et **Conditions de la politique** .

Configurer les propriétés d'authentification adaptative

Après l'activation de l'authentification adaptative, configurez les propriétés d'authentification adaptative en fonction de vos exigences de sécurité.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés**.
2. Configurez les propriétés suivantes :

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

Propriété	Description	Valeur
Activer la journalisation du débogage pour les politiques d'authentification (glide.authenticate.policy.debug)	Option permettant d'activer la journalisation de débogage pour les politiques d'authentification.	Oui | Non
Code d'erreur HTTP à afficher à 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 lors de 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 403 Forbidden est sélectionné) (glide.authenticate.global.blocking_policy.error_message)	Message d'erreur qui s'affiche lorsque la politique de blocage globale bloque l'accès.	Champ de texte
Activer le flux de confiance de l'appareil (glide.authenticate.preauth.allow.trusted.device)	Option permettant d'activer le flux d'appareils approuvés.	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
Ignorez l'inscription de l'appareil pour le flux de confiance de l'appareil si l'utilisateur provient du réseau approuvé (glide.authenticate.preauth.skip.user.registration)	Option permettant d'ignorer l'inscription si l'utilisateur tente de s'inscrire à partir du réseau approuvé	Oui | Non
Propriété permettant d'activer la fonctionnalité de validation de session. Définissez-le sur vrai après avoir activé la politique du contexte de validation de session et configuré les filtres et conditions souhaités (session.validation.enabled)	Option permettant d'activer la fonctionnalité de validation de session. Définissez-la sur vrai après l'activation de la politique du contexte de validation de session et la configuration des 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 avoir une instance avec l'authentification adaptative activée. Pour obtenir des détails sur ce processus, consultez Activer l'authentification adaptative.

L'exemple vous guide dans la création d'une nouvelle politique et son application à une instance. Dans ce didacticiel, vous allez :

Créer un enregistrement de critères de filtre

Créez un enregistrement de critères de filtre de groupe à utiliser comme entrée pour votre politique. Cet enregistrement permet à votre politique de déterminer l'accès en fonction du groupe d'utilisateurs. Au fil de ces étapes, vous allez définir le ou les groupes utilisés par la politique 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 fil de

ces étapes, vous définissez également les 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 de critères de filtre.

Créer un enregistrement de critères 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

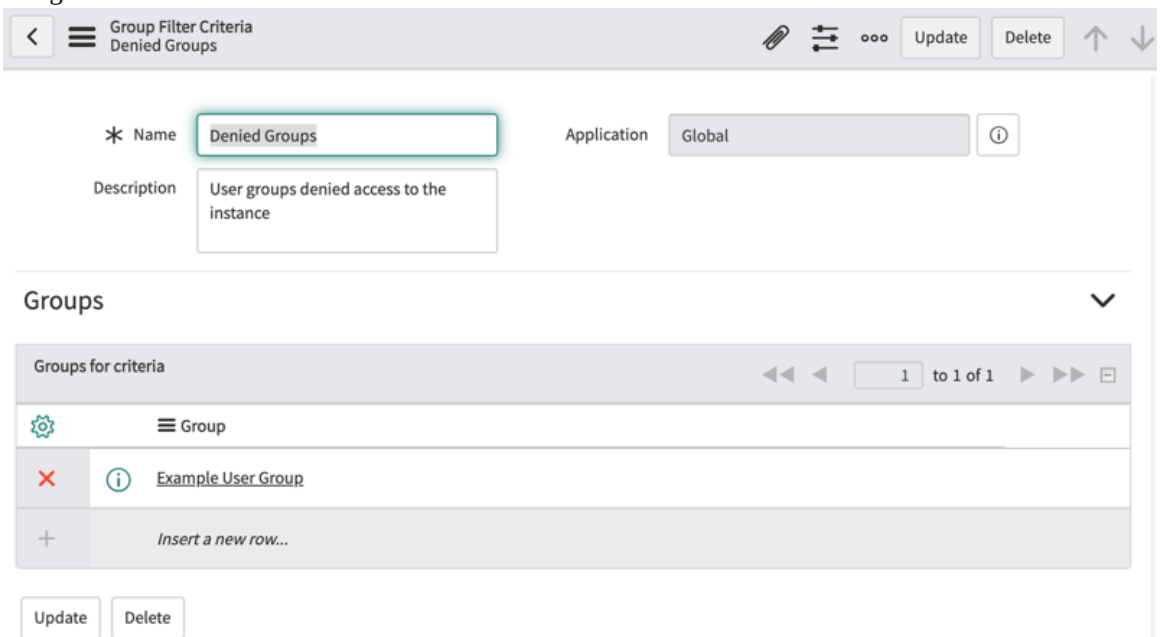
Pour refuser l'accès à votre instance en fonction des groupes d'utilisateurs, vous devez créer un enregistrement de critères de filtre de groupe. Cet enregistrement définit un groupe d'utilisateurs ou un ensemble de groupes d'utilisateurs auxquels votre politique peut accorder ou refuser l'accès. Dans cet exemple, vous allez créer un enregistrement de critères 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 **Groupe 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 ( ) pour sélectionner un groupe dans une liste.
   Si vous souhaitez créer un nouveau groupe d'utilisateurs pour vos critères de filtre, cliquez sur l'icône de référence ( ), puis cliquez sur le bouton **Nouveau** . Pour plus de détails sur la création de groupes d'utilisateurs, consultez 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

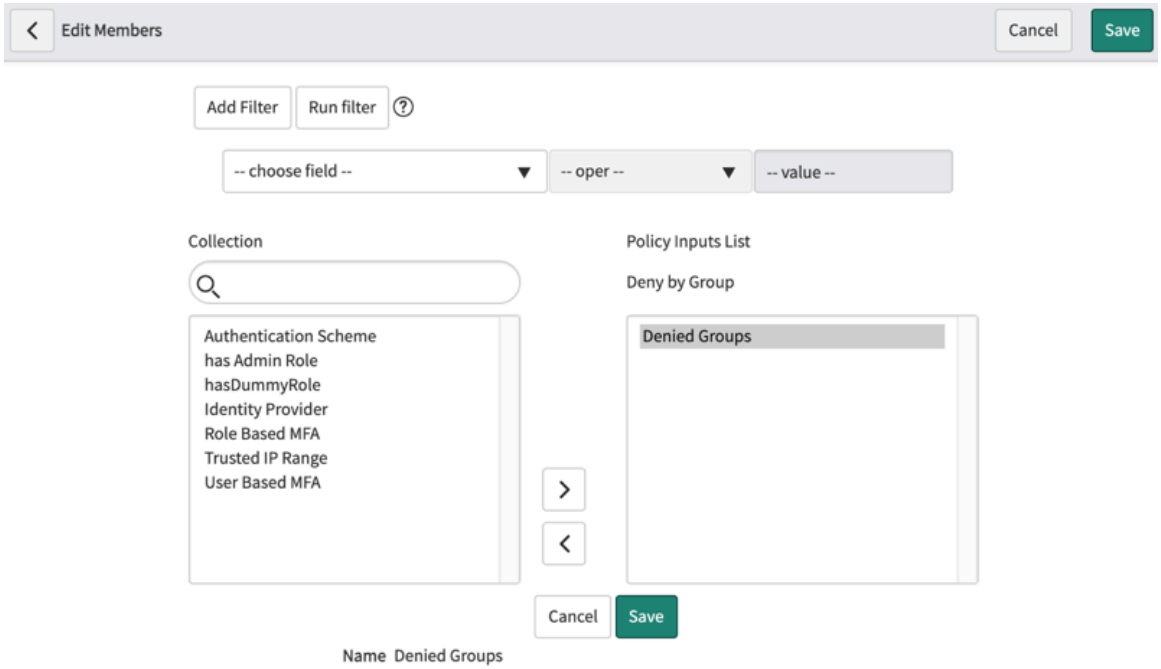
Découvrez comment créer une politique de refus d'accès aux groupes d'utilisateurs définis dans les critères de filtre de votre groupe.

Avant de commencer

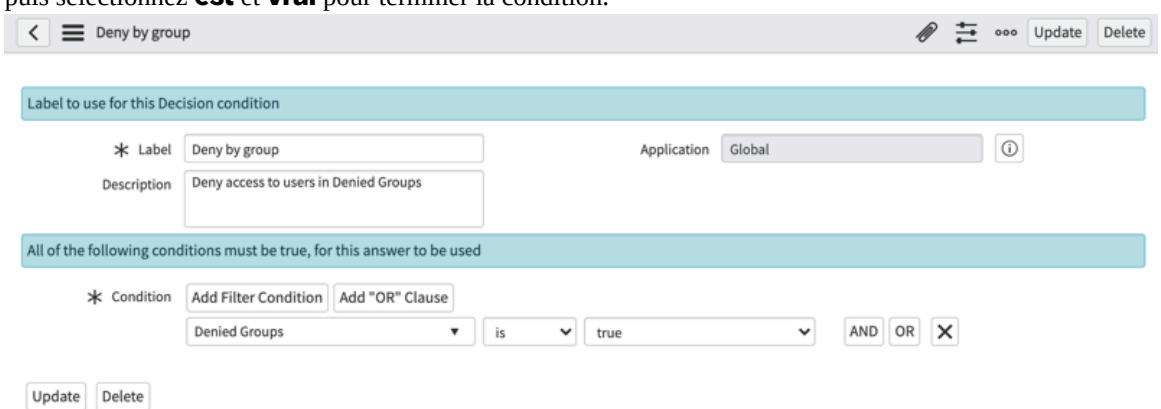
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les stratégies**.
2. Dans la liste **Stratégies** , cliquez sur **Nouveau**.
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 à nouveau l'enregistrement de politique.
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 terminer la condition.



13. Cliquez sur **Enregistrer**.

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 de 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 politique utilisée dans ce didacticiel doit évaluer le groupe dans lequel se trouve un utilisateur. Ces informations ne sont disponibles qu'une fois les informations d'identification saisies.
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 la 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 sauvegarder l'enregistrement du contexte de politique.

Authentification adaptative pour les applications mobiles de confiance

Accédez à vos ServiceNow réseaux non approuvés à l'aide du Application Now Mobilefichier .

Authentification adaptative pour les applications mobiles de confiance

Adaptive Authentication for Trusted Mobile Apps permet aux utilisateurs d'accéder à l'instance à l'aide ServiceNow du Application Now Mobilefichier . 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 Application Now Mobile Employee Service Center (portail) depuis l'extérieur du réseau. Le filtre Application mobile de confiance vous permet d'identifier les demandes entrantes provenant d'une application de confiance Application Now Mobile liée à un compte d'utilisateur.

En tant qu'administrateur, vous pouvez configurer la politique. Cette 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 équipement mobile en scannant le code QR affiché sur l'instance. Après l'inscription, vous pouvez vous connecter à votre instance à partir de , Application Now Mobileà l'aide de vos informations d'identification.

Remarque :
Pour enregistrer l'équipement mobile, vous devez vous connecter à un réseau approuvé. Après l'enregistrement, vous pouvez également vous connecter à l'instance à partir d'autres réseaux.

Fonctionnalités

En tant qu'administrateur, vous pouvez utiliser les fonctionnalités suivantes :

- Configurez les politiques à l'aide de critères de filtre d'applications approuvés.
- Créez des conditions de politique avec un nouveau critère de filtre pour les applications Mobile 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 de confiance.

- Ajoutez des événements de sécurité pour toutes les actions d'inscription ou de révocation des appareils. Les événements peuvent être utilisés pour notifier l'utilisateur.
- Prenez en charge les événements de sécurité pour les échecs de signature, de validation de cookie, de jetons non valides, d'en-têtes ou de paramètres de requête non valides.
- Contrôlez le nombre maximal d'appareils enregistrés.
- Empêchez l'enregistrement d'un nouvel appareil, sauf si l'utilisateur supprime un appareil associé existant.
- Capturez la dernière fois qu'un appareil a été utilisé.

Activer l'application mobile de confiance

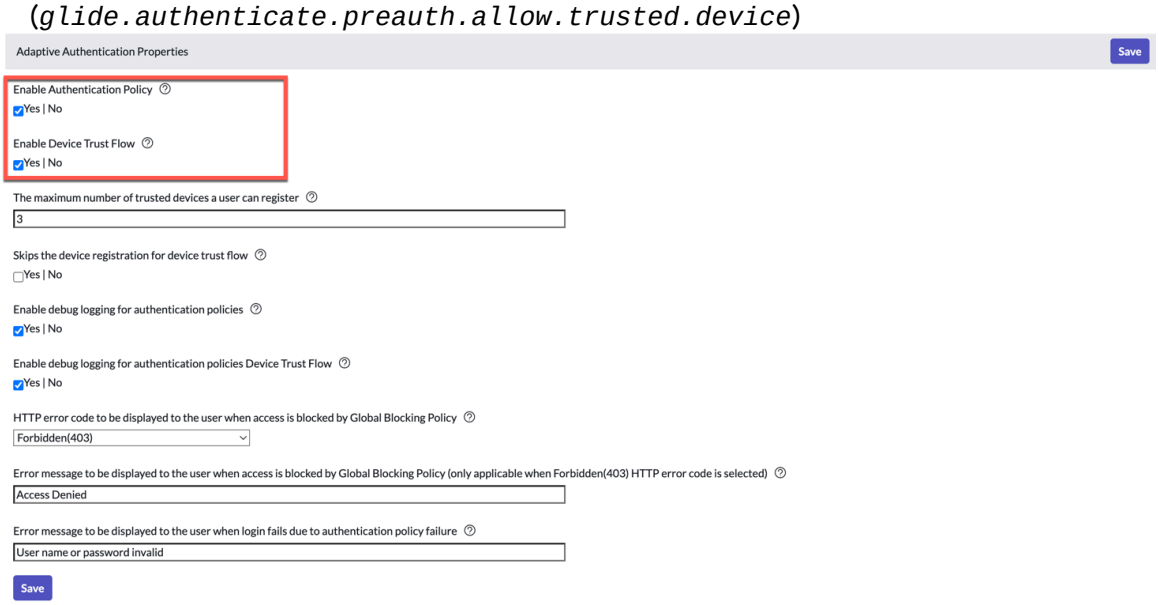
Activez l'authentification adaptative avec l'application mobile de confiance à l'aide de la politique d'authentification et des conditions de filtre.

Avant de commencer
Assurez-vous que le module d'extension Adaptive Authentication (`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 confiance de l'appareil (`glide.authenticate.preauth.allow.trusted.device`)



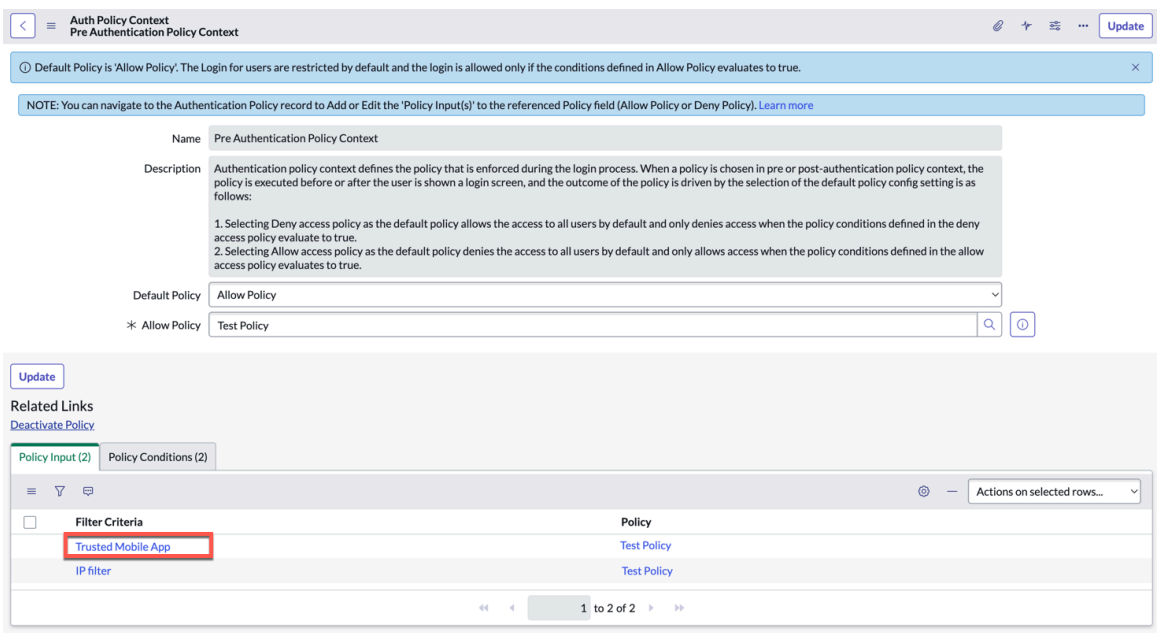
Remarque :
Pour désactiver la propriété de flux de confiance de l'appareil, vous devez supprimer les conditions avec le filtre mobile de confiance. Sinon, un message d'erreur s'affiche pour vous inviter à supprimer les conditions.

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, reportez-vous Contexte de pré-authentificationà .

> **Remarque :**
> Par défaut, la condition de politique est **Refuser la politique**. Vous pouvez passer à **la politique d'autoriser**. Ces politiques sont diamétralement opposées.
>
> - La **politique d'autorisation** permet de refuser l'accès par défaut à tous les utilisateurs et uniquement lorsque les conditions de la politique d'autorisation d'accès sont définies sur true.
> - Avec la **politique de refus,** tous les utilisateurs sont autorisés à accéder par défaut, et elle refuse l'accès uniquement lorsque les conditions de la politique de refus d'accès sont vraies.

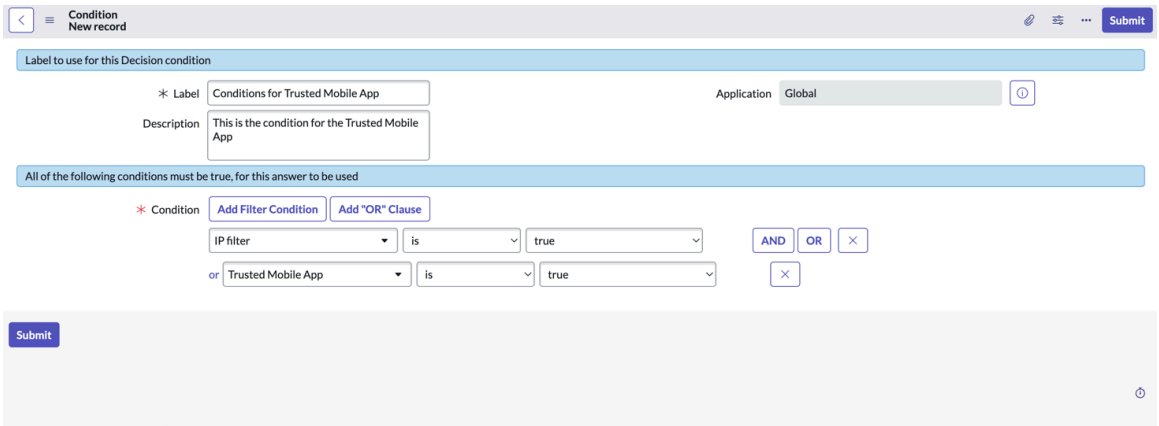
Dans l'entrée de politique, l'entrée **de politique Application mobile de confiance** est une entrée de politique pour l'application mobile de confiance.



5. Dans les Conditions de la politique, créez la condition en cliquant sur **Nouveau**.
6. Renseignez les champs du formulaire.

Formulaire Condition de filtre

Champ	Description
Étiquette	Nom de la condition
Description	Description de la condition
Application	Le périmètre de l'application pour cet enregistrement.
Condition	Conditions basées sur ET et OR. Étant donné que la politique d'authentification est la **politique d'autoriser**, la condition pour l'application mobile de confiance est définie sur true dans l'exemple illustré 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 Périphérique approuvé pour accéder à l'instance ServiceNow à partir de réseaux non approuvés à l'aide de .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

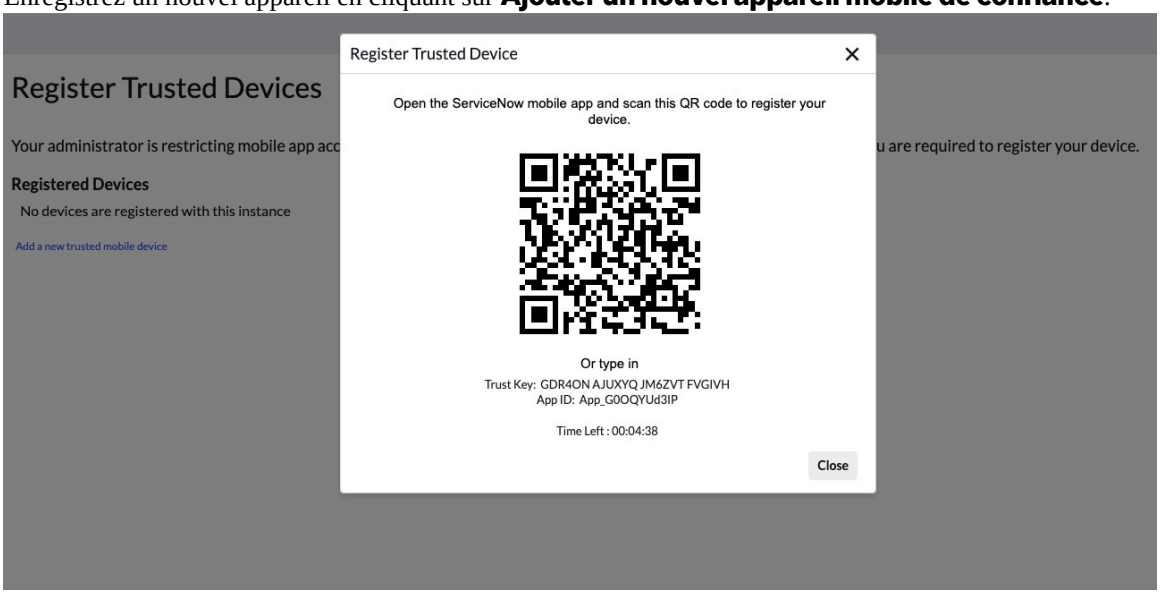
1. Accédez à l'une des options de menu suivantes :

- Sur le , accédez Now Platformà **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.

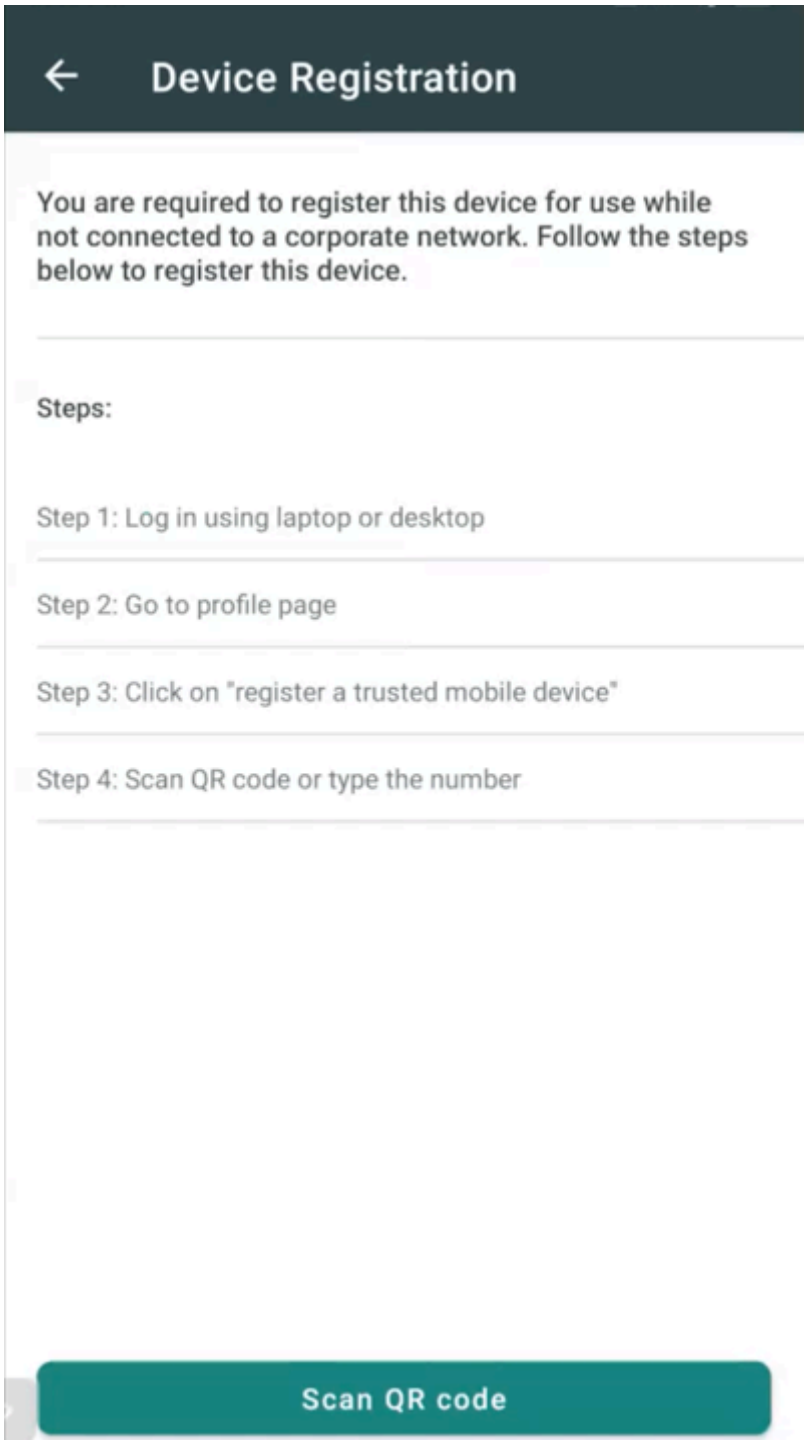
- Sur , Now Supportcliquez sur le profil et sélectionnez **Appareil de confiance**.

2. Dans votre profil d'utilisateur, cliquez sur **Enregistrer un équipement mobile de confiance** dans la section Liens connexes.
   La page Enregistrer les appareils de confiance s'affiche.
3. Enregistrez un nouvel appareil en cliquant sur **Ajouter un nouvel appareil mobile de confiance**.



4. Sur l'écran d'enregistrement du périphérique 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.

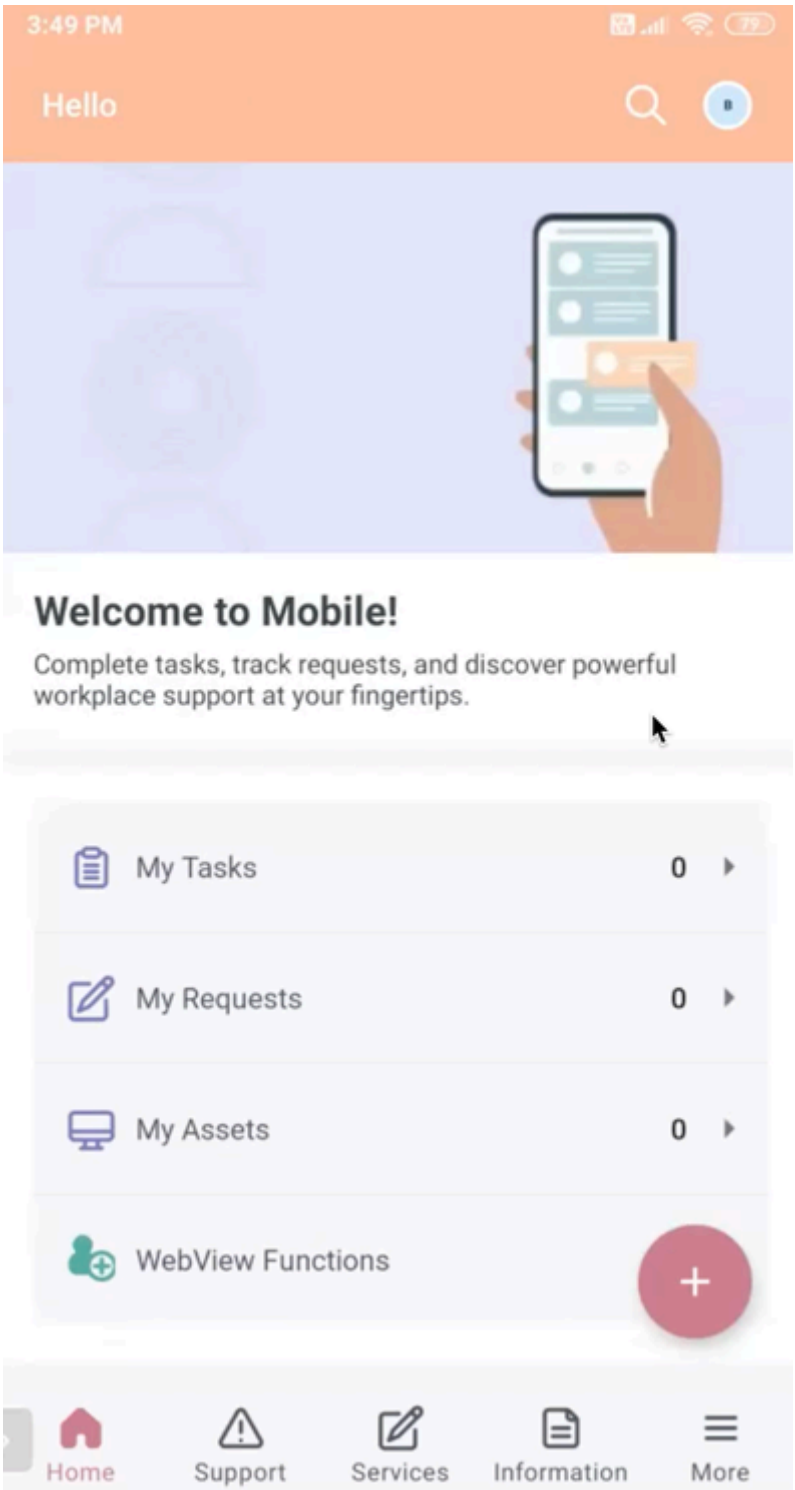
Traduction automatique



Le processus d’inscription se terminera et vous serez invité à accéder à votre page de connexion pour terminer votre authentification.

5. Spécifiez vos informations d’identification et connectez-vous au Application Now Mobile.

L’écran d’accueil Mobile s’affiche.



Résultats

Sur la page Enregistrer des périphériques de confiance sur votre ordinateur portable ou de bureau, l’appareil enregistré s’affiche. 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.

Gérer votre appareil de confiance

Gérez votre appareil de confiance à partir de la page d'inscription de l'appareil de confiance.

Avant de commencer

Rôle requis : aucun

Procédure

1. Accédez à l'une des options de menu suivantes :
   - Sur le , accédez Now Platformà **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.

   - Sur , Now Supportcliquez 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 les appareils de confiance s'affiche.
3. Sur la page Enregistrer des appareils de confiance, supprimez l'appareil en cliquant sur .

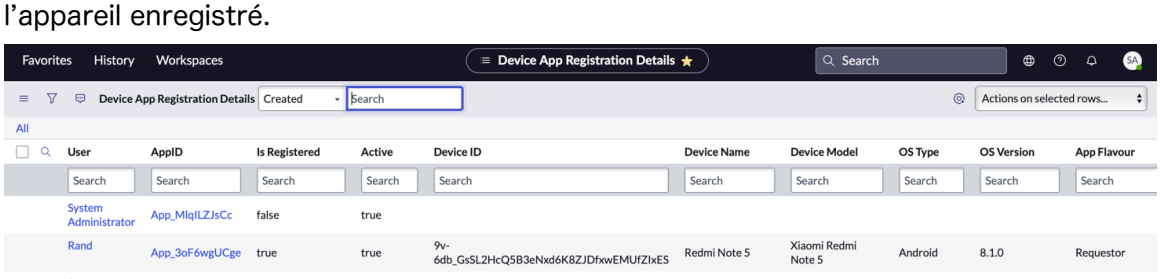
   Remarque :
   L'équipement mobile supprimé doit être enregistré à nouveau pour accéder à l'instance.

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 auprès de l'instance, accédez à **Tous** > **Authentification Adaptative** > **Appareil de confiance** > **Inscription du périphérique**.

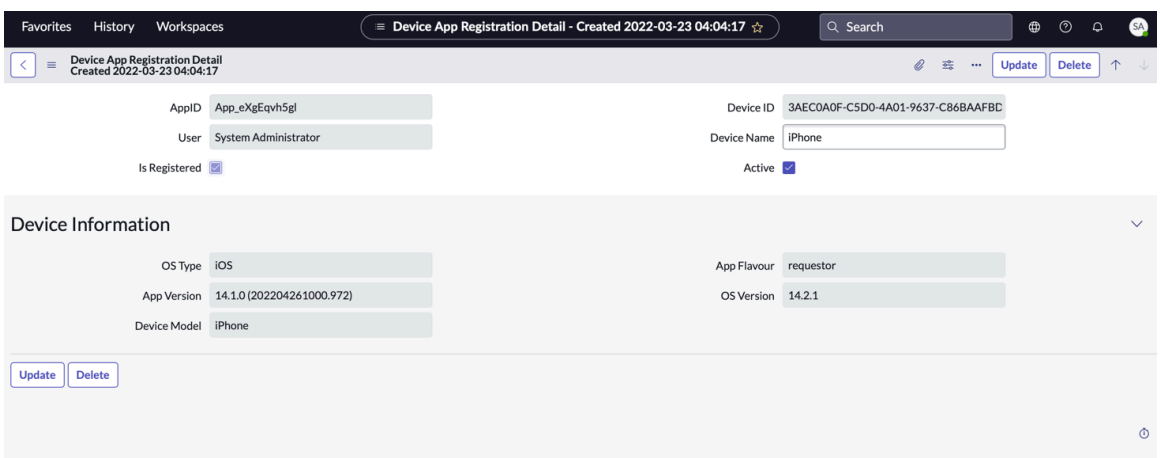
Utilisez le filtre pour identifier l'appareil. Cliquez sur le champ **AppID** pour en savoir plus sur l'appareil enregistré.



Les détails suivants s'affichent pour l'appareil :

- ID application
- ID d'équipement

- 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 d’une application mobile de confiance

Passez en revue ces scénarios de dépannage pour résoudre les problèmes avec l’application mobile de confiance.

Les sections suivantes décrivent certains scénarios de dépannage et les méthodes de dépannage.

Décalage horaire 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 l’utilisation de l’appareil approuvé.

Expiration du code QR dans les cinq minutes

Le code QR de la fonctionnalité Appareil de confiance expire au bout de 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 basée sur la propriété système pour les informations d’identification valides pouvant être utilisées pour la connexion.

Nombre maximal d'appareils enregistrés

Si le nombre maximal d'enregistrements d'appareils 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 API dans valide l'identité d'un utilisateur qui accède à ServiceNow®une instance, puis autorise l'utilisateur à accéder aux fonctionnalités qui correspondent au rôle ou à la fonction de l'utilisateur lorsqu'il effectue un appel d'API à l'instance ServiceNow® .

Voici les types d'authentification API dans ServiceNow®:

- 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 API entrantes à l'aide de certificats provenant d'une autorité de certification (CA) approuvée.

Authentification basée sur certificat pour les services Web entrants

Authentifier les demandes entrantes adressées aux ServiceNow 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 fiducie sur le système à l'aide d'un protocole d'authentification.

OAuth 2.0 - Open Authorization est le protocole standard de l'industrie pour l'autorisation, 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 souhaitent accéder à votre instance. Cela crée un enregistrement d'application cliente OAuth et génère un ID client et un secret client indiquant que le client a besoin pour accéder aux ressources restreintes sur l'instance. Pour plus d'informations, reportez-vous à la section OAuth entrant.

Authentification basée sur un jeton

Authentification basée sur les jetons pour la configuration des API REST entrantes à l'aide d'une clé API ou HMAC.

Prendre en charge les jetons d'API pour les points de terminaison de l'API REST afin que l'authentification utilisateur ServiceNow® .

L'authentification basée sur les jetons pour la configuration des API REST entrantes peut être effectuée sur l'instance ServiceNow® avec la clé API ou le jeton HMAC.

Clé API et authentification HMAC pour les API REST entrantes

Prendre 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 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 l'envoi d'informations sensibles au serveur.

L'installation de la clé API et de l'authentification HMAC dépend des modules d'extension suivants :

- Module d'extension REST API Auth Scope (com.glide.rest.auth.scope)
- Module d'extension REST API Access Policy (com.glide.rest.policy)
- Périmètre d'authentification (com.glide.auth.scope)

Avantages

La clé API et l'authentification HMAC pour les API REST entrantes permettent :

- Possibilité de spécifier la clé API ou le 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 comme paramètre de requête ou en-tête dans l'appel d'API REST.
- Possibilité d'associer le périmètre d'authentification à des configurations de clé API ou de jeton HMAC afin que les clés API puissent uniquement être utilisées pour appeler des API associées à des périmètres particuliers.
- Possibilité d'associer une configuration de clé API ou de jeton HMAC à un profil d'authentification qui peut être utilisé dans les politiques d'accès API.

Activer la clé API et l'authentification HMAC

Vous pouvez activer la clé API du module d'extension 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 HMAC Authentication (com.glide.tokenbased_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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

> **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>.

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)

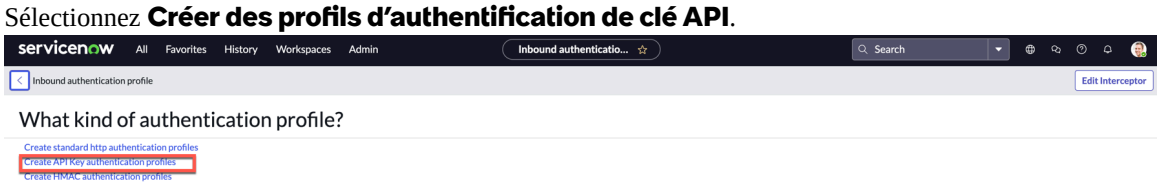
Procédure

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**.



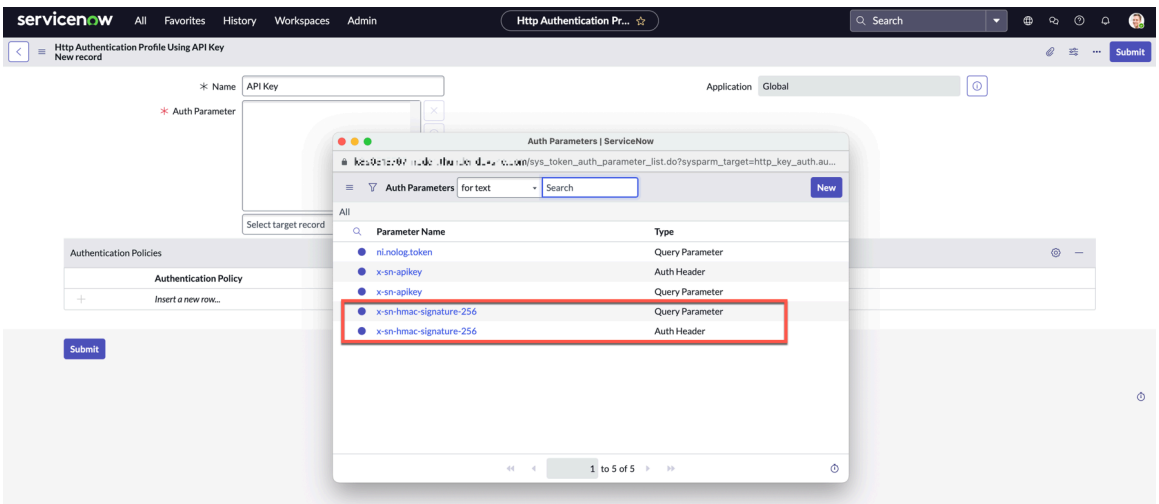
   d. Renseignez les champs du formulaire.

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 pour la demande d'authentification. Vous pouvez sélectionner les options par défaut ou créer un nouveau paramètre d'authentification :

Champ	Description
	▪ 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 le cadre de l'en-tête d'authentification ou du paramètre de requête.



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 :

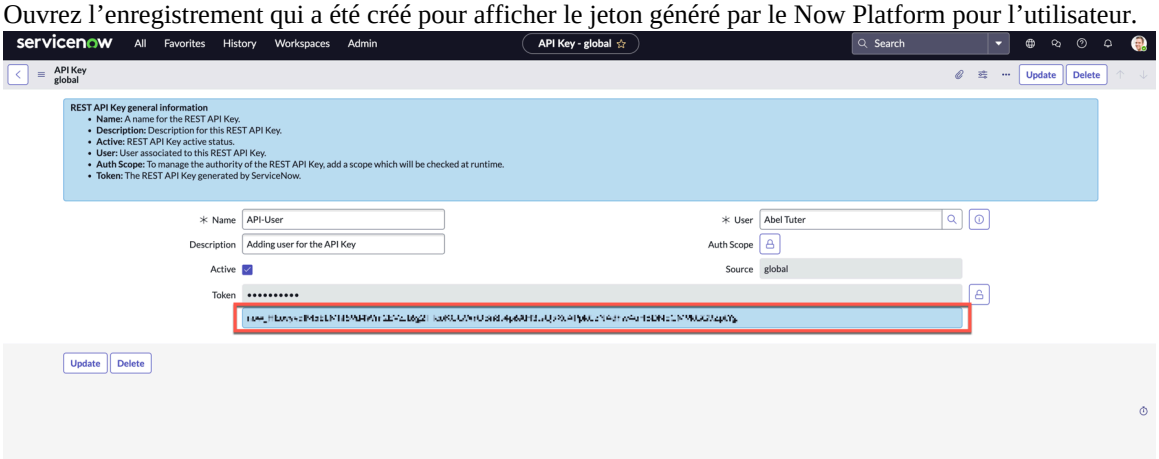
Clé API

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 Now Platformfichier . Copiez la clé à utiliser dans le

Champ	Description
	cadre de l'appel d'API REST dans le paramètre En-tête ou Requête.

d. Envoyez le formulaire.

e. Ouvrez l'enregistrement qui a été créé pour afficher le jeton généré par le Now Platform pour l'utilisateur.



3. Créez une politique d'accès REST API.

a. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès REST API**.

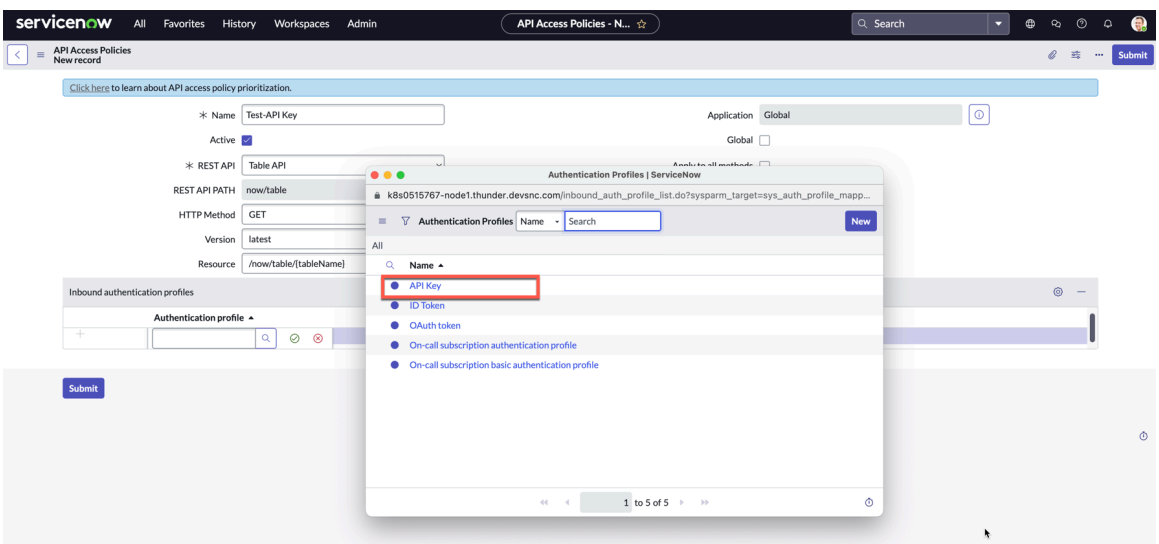
b. Sélectionnez **Nouveau**.

c. Renseignez les champs du formulaire.

Politiques d'accès API

Champ	Description
Nom	Nom unique de la politique d'accès de l'API.
Actif	Option permettant d'activer la politique d'accès API.
API REST	L'API REST à laquelle la politique d'accès est appliquée. Par exemple, **API de pièce jointe**.
CHEMIN REST API	Chemin d'accès de l'API de REST. Ce champ est automatiquement renseigné en fonction de l'API REST sélectionnée. Par exemple, **now/attachment**.
Méthode HTTP	Méthode utilisée pour interagir avec l'API. Ce champ est automatiquement renseigné en fonction de l'API REST sélectionnée.
Version	Version de l'API. Par exemple, **v1**. Ce champ est automatiquement renseigné en fonction de l'API REST sélectionnée.

Champ	Description
	Remarque : Si vous souhaitez créer une politique d'authentification pour toutes les versions d'une REST API, vous devez créer des politiques individuelles pour chaque version.
Ressources	Ressource enfant de l'API REST. Ce champ est automatiquement renseigné 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 l'ensemble des 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.



d. Ajoutez le profil d'authentification d'API qui a été créé.

e. Envoyez le formulaire.

Vous pouvez envoyer l'appel d'API REST avec la clé x-sn-apikey (jeton) qui a été générée par le Now Platform lors de la création de la clé API dans le paramètre En-tête ou Requête en fonction de la configuration de l'authentification.

> **⚠ Avertissement :**
> Utilisez **la demande POST** lors de l'envoi d'informations sensibles au serveur.

Configurer HMAC : authentification basée sur les jetons

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**.

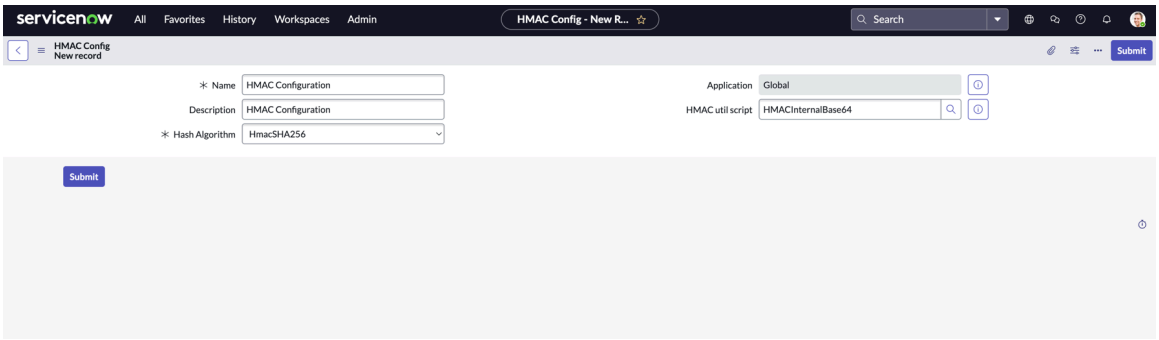
   b. Sélectionnez **Nouveau**.

   > **ⓘ Remarque :**
   > Vous pouvez également utiliser le **codage HMAC SHA256 Base64 par défaut** qui est créé lors de l'installation du module d'extension.

   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 d'utilitaire pour HMAC.



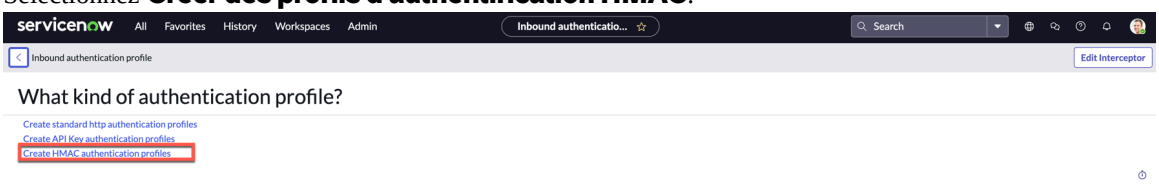
d. Envoyez l'enregistrement.

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**.



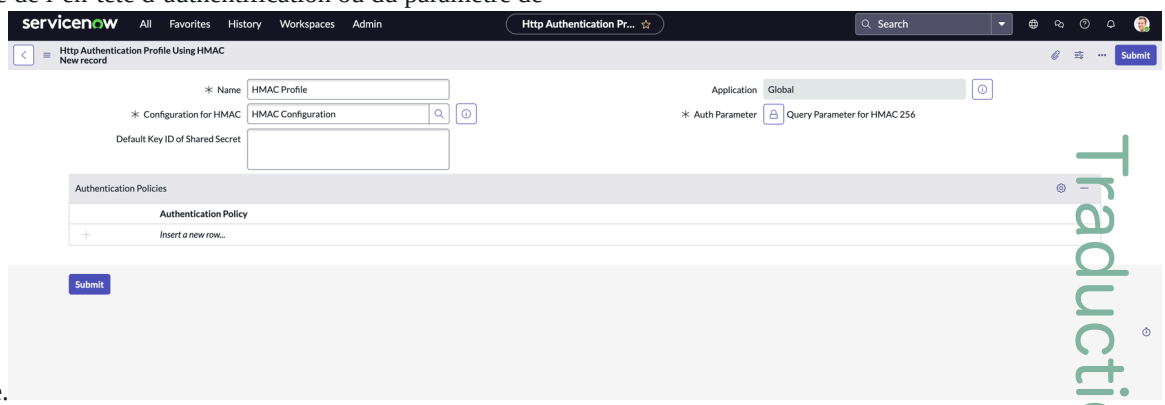
d. Renseignez les champs du formulaire.

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.
Paramètre d'authentification	Sélectionnez le paramètre d’authentification pour la demande d’authentification. Vous pouvez sélectionner les options par défaut ou créer un nouveau paramètre d’authentification :

Champ	Description
	▪ x-sn-hmac-signature-256 : en-tête d'authentification ▪ x-sn-hmac-signature-256 : en-tête du paramètre de requête
ID de clé par défaut du secret partagé	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

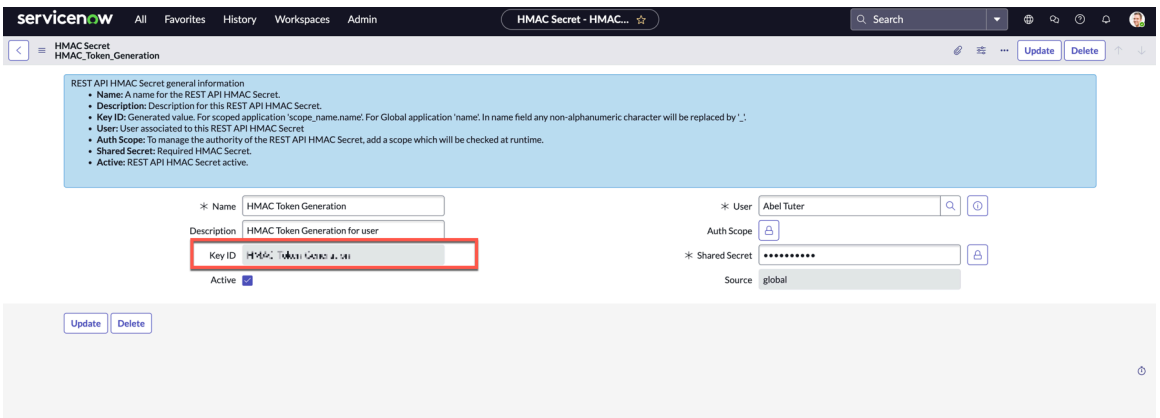
Champ	Description
Nom	Nom permettant d'identifier le secret HMAC de l'API REST.
Description	Description du secret HMAC de l'API REST.
Actif	État du secret HMAC de l'API REST.
Utilisateur	Utilisateur associé au secret HMAC de l'API REST. Utilisez l'icône de recherche pour sélectionner l'utilisateur.
ID clé	ID de clé qui doit être envoyé dans le cadre de l'appel REST. L'ID de clé est généré après l'envoi du formulaire.

Champ	Description
Secret partagé	Secrets partagés de l’utilisateur. Par exemple, le mot de passe.
Source	Source de l’enregistrement.

d. Envoyez le formulaire.

e. Ouvrez l’enregistrement qui a été créé.

Rechercher l’ID de clé généré par le Now Platform pour l’utilisateur



.

Remarque :
Vous pouvez ajouter l’ID de clé qui a été généré pendant l’ID de clé dans le profil d’authentification qui a été créé pour HMAC si vous ne souhaitez pas spécifier le paramètre Auth ou Query pour l’appel d’API.

4. Créez une politique d’accès aux REST APIs.

a. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès REST API**.

b. Sélectionnez **Nouveau**.

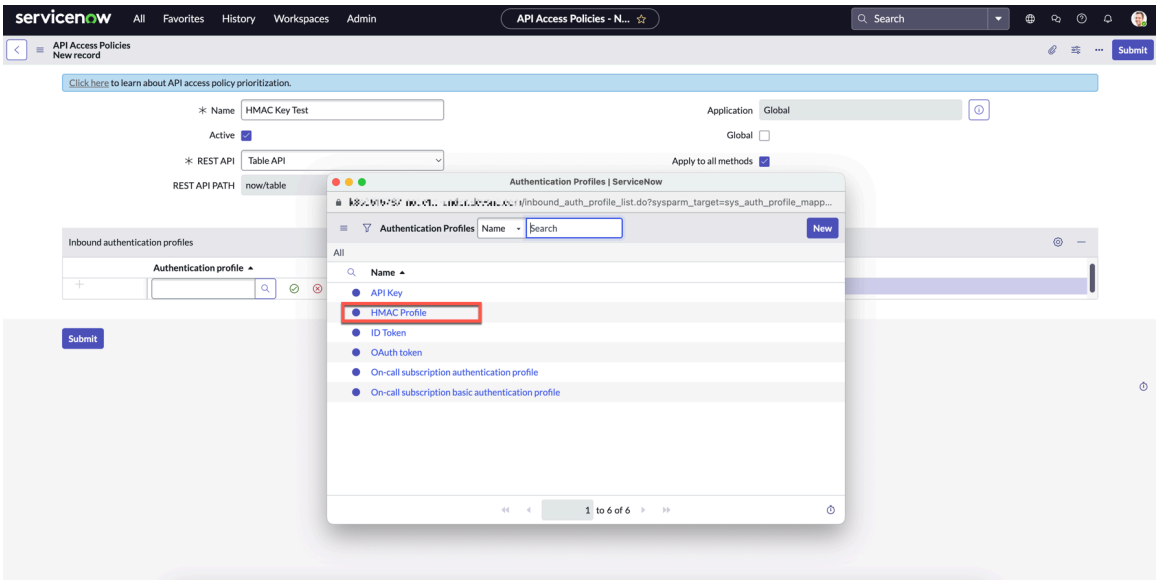
c. Renseignez les champs du formulaire.

Politiques d'accès API

Champ	Description
Nom	Nom unique de la politique d’accès de l’API.
Actif	Option permettant d’activer la politique d’accès API.
API REST	L’API REST à laquelle la politique d’accès est appliquée. Par exemple, **API de pièce jointe**.
CHEMIN REST API	Chemin d’accès de l’API de REST. Ce champ est automatiquement renseigné en fonction de l’API REST sélectionnée. Par exemple, **now/attachment**.

Champ	Description
Méthode HTTP	Méthode utilisée pour interagir avec l'API. Ce champ est automatiquement renseigné en fonction de l'API REST sélectionnée.
Version	Version de l'API. Par exemple, **v1**. Ce champ est automatiquement renseigné en fonction de l'API REST sélectionnée. **Remarque :** Si vous souhaitez créer une politique d'authentification pour toutes les versions d'une REST API, vous devez créer des politiques individuelles pour chaque version.
Ressources	Ressource enfant de l'API REST. Ce champ est automatiquement renseigné 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 l'ensemble des 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.

d. Ajoutez le profil d'authentification d'API qui a été créé.



e. Envoyez le formulaire.
Vous pouvez envoyer l'appel d'API REST :

- Avec x-sn-hmac-signature-256 qui a été généré lors ServiceNow® de la création de la clé API dans le paramètre En-tête ou Requête en fonction de la configuration pour l'authentification.
- Avec script de pré-demande avec secret partagé spécifié dans le cadre de la demande.

> **⚠ Avertissement :**
> Utilisez **la demande POST** lors de l'envoi d'informations sensibles au serveur.

Politique d'accès API

La politique d'accès d'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 les trois niveaux de prise en charge de la politique d'authentification pour les sessions non interactives :

- **API REST** : l'administrateur peut définir une politique d'authentification d'API globale ou une politique d'authentification spécifique à l'API.
- **API SOAP** : l'administrateur peut définir une politique d'authentification d'API globale ou une politique d'authentification spécifique à l'API.
- **Processeur système/exportation** : l'administrateur peut définir cinq profils d'authentification du système de base, qui peuvent être utilisés pour appliquer le profil d'authentification à la politique d'authentification de l'API des processeurs ou à la politique d'authentification spécifique au processeur.

> **ℹ Remarque :**
> Si vous ajoutez une politique d'authentification globale, la politique 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 exigences de sécurité. et appliquez les 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 des REST APIs
- Politiques d'accès de l'API SOAP

Pour en savoir plus sur les politiques relatives aux processeurs d'exportation, reportez-vous à la section Politique d'accès pour les processeurs système/d'exportation.

Politiques d'accès des REST APIs

Les politiques d'accès aux REST APIs vous permettent de restreindre l'accès aux REST APIs entrantes en fonction du type d'authentification et des critères de filtre spécifiés de 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 respecte les directives de style architectural REST. Les API REST offrent un haut degré de flexibilité, ce qui les rend répandues sur le Web.

Les critères de filtre contiennent des conditions ou des requêtes de filtre 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 exigences 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 provenant d'adresses IP autres que celles spécifiées sont refusées.

Activer la politique d'accès REST API

Vous pouvez activer le module d'extension REST API Access Policy (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 de l'API REST :

- 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 REST API Access Policy (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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

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 avec jeton d’ID** et **jeton OAuth** qui sont disponibles par défaut.

Avant de commencer

Rôle requis : admin

Remarque :
Vous pouvez appliquer des politiques d’authentification, une plage d’adresses 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. Renseignez les champs du formulaire.

Formulaire Profil d’authentification standard

Champ	Description
Nom	Nom permettant d’identifier la politique d’authentification.

Champ	Description
Description	Description de la politique d'authentification.
Actif	Option permettant d'activer la politique d'authentification.
Application	Périmètre de la politique d'authentification.
Type	Type de l'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 s'affiche uniquement lorsque **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, puis sélectionnez l'icône .

Remarque :
Ne sélectionnez pas Autoriser la politique d'accès ou Refuser la politique d'accès. Ces politiques sont destinées uniquement aux connexions des utilisateurs.

Vous pouvez ajouter une ou plusieurs politiques d'authentification pour un profil d'authentification.

Remarque :

Authentifier l'en-tête [WWW-Authenticate].

En cas de changement du profil d'authentification, l'en-tête Autorisation renvoie une valeur spécifique aux modifications apportées à ce moment-là. Pour avoir la possibilité d'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 **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 pour une API REST. Par exemple, vous pouvez créer une politique d'accès API qui autorise uniquement l'authentification par jeton d'ID pour une API REST.

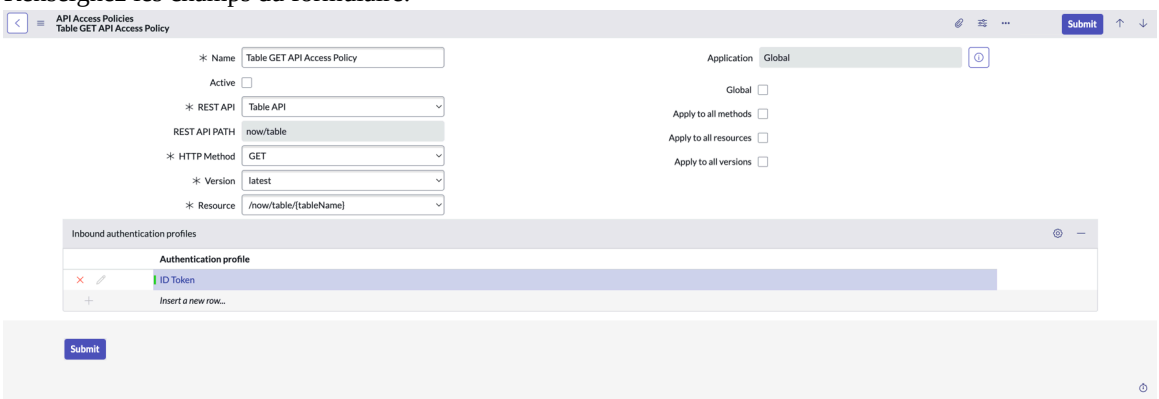
Avant de commencer

- Rôle requis : admin
- Assurez-vous qu'un profil d'authentification est créé. Pour plus d'informations, consultez Créer un profil d'authentification.

Procédure

1. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès REST API**.
2. Cliquez sur **Nouveau**.

3. Renseignez les champs du formulaire.



Politiques d'accès API

Champ	Description
Nom	Nom unique de la politique d’accès de l’API.
Actif	Option permettant d’activer la politique d’accès API.
API REST	L’API REST à laquelle la politique d’accès est appliquée. Par exemple, **API de pièce jointe**.
CHEMIN REST API	Chemin d’accès de l’API de REST. Ce champ est automatiquement renseigné en fonction de l’API REST sélectionnée. Par exemple, **now/attachment**.
Méthode HTTP	Méthode utilisée pour interagir avec l’API. Ce champ est automatiquement renseigné en fonction de l’API REST sélectionnée.
Version	Version de l'API. Par exemple, **v1**. Ce champ est automatiquement renseigné en fonction de l’API REST sélectionnée. **Remarque :** Si vous souhaitez créer une politique d’authentification pour toutes les versions d’une REST API, vous devez créer des politiques individuelles pour chaque version.
Ressources	Ressource enfant de l’API REST. Ce champ est automatiquement renseigné en fonction de l’API REST sélectionnée. Par exemple, **/now/attachment**
Application	Périmètre de l'application.
Global	Activez cette option pour appliquer la politique d’authentification à toutes les méthodes, versions et ressources de l’API.
Appliquer à toutes les méthodes	Activez cette option pour appliquer la politique d’authentification de l’API à l’ensemble des méthodes, versions et ressources de l’API.

Champ	Description
Appliquer à toutes les ressources	Activez cette option pour appliquer la politique d'authentification de l'API à toutes les versions.
Appliquer à toutes les versions	Activez cette option pour appliquer la politique d'authentification de l'API à toutes les ressources.

Remarque :
Pour en savoir plus sur la priorisation de la politique d'accès API, reportez-vous à la section Priorisation de la politique d'accès API.

4. 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 **l'authentification de base**, le **jeton d'ID**, **l'authentification basée sur certificat**, **l'authentification OAuth** ou **l'authentification WSSE**.
   a. Pour ajouter un ou plusieurs profils d'authentification entrants, cliquez sur **Nouveau** pour créer un nouveau profil.
   b. Choisissez **Quels types de profils d'authentification ?**.
      - **Créer des profils d'authentification http standard**
      - **Créer des profils d'authentification WSSE**

   c. Après avoir créé le profil d'authentification, sauvegardez l'enregistrement.
6. Cliquez sur **Envoyer** pour soumettre la politique d'accès à l'API REST.

Priorisation de la politique d'accès API

Découvrez la logique de priorisation 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 définie sur votre ServiceNow® instance.

L'approche consiste à définir différents poids pour chaque partie de l'API, tels que la méthode, la ressource et la version.

La politique d'API est priorisée pour les aspects non globaux d'abord, puis 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.
Méthode+ ressource	2	Si les 2 champs correspondent à la politique, celle-ci 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.
Ressources	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, celle-ci prend la 5e priorité.
Méthode	6	Si le champ et le champ **Appliquer à toutes les ressources correspondent à** la politique, celle-ci 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, celle-ci prend la 7e priorité.
Global et appliquer à toutes les méthodes	8	Si les champs **Global** a la valeur true (Global) et **Apply to all methods (Appliquer à toutes les méthodes**) est false , cette politique prend la 8e priorité.

Ordre de priorité (suite)

Champs	Priorité	Logique de hiérarchisation
Global et appliquer à toutes les méthodes	9	Si les champs **Global** a la valeur true et que **Apply to all methods (Appliquer à toutes les méthodes**) a la valeur true , cette politique prend la 9e priorité.

Critères de filtre pour les API

Les critères de filtre contiennent des conditions ou des requêtes de filtre 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 d'une politique d'authentification. Par exemple, un critère de filtre 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 en fonction de l'adresse IP de l'utilisateur, de son rôle et du groupe d'utilisateurs auquel il appartient.

Remarque :
Vous pouvez également utiliser 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.

Information associée

- Créer un critère de filtre d'adresses IP
- Créer un critère de filtre de rôle
- Créer un critère 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 exigences 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 sont destinées uniquement 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

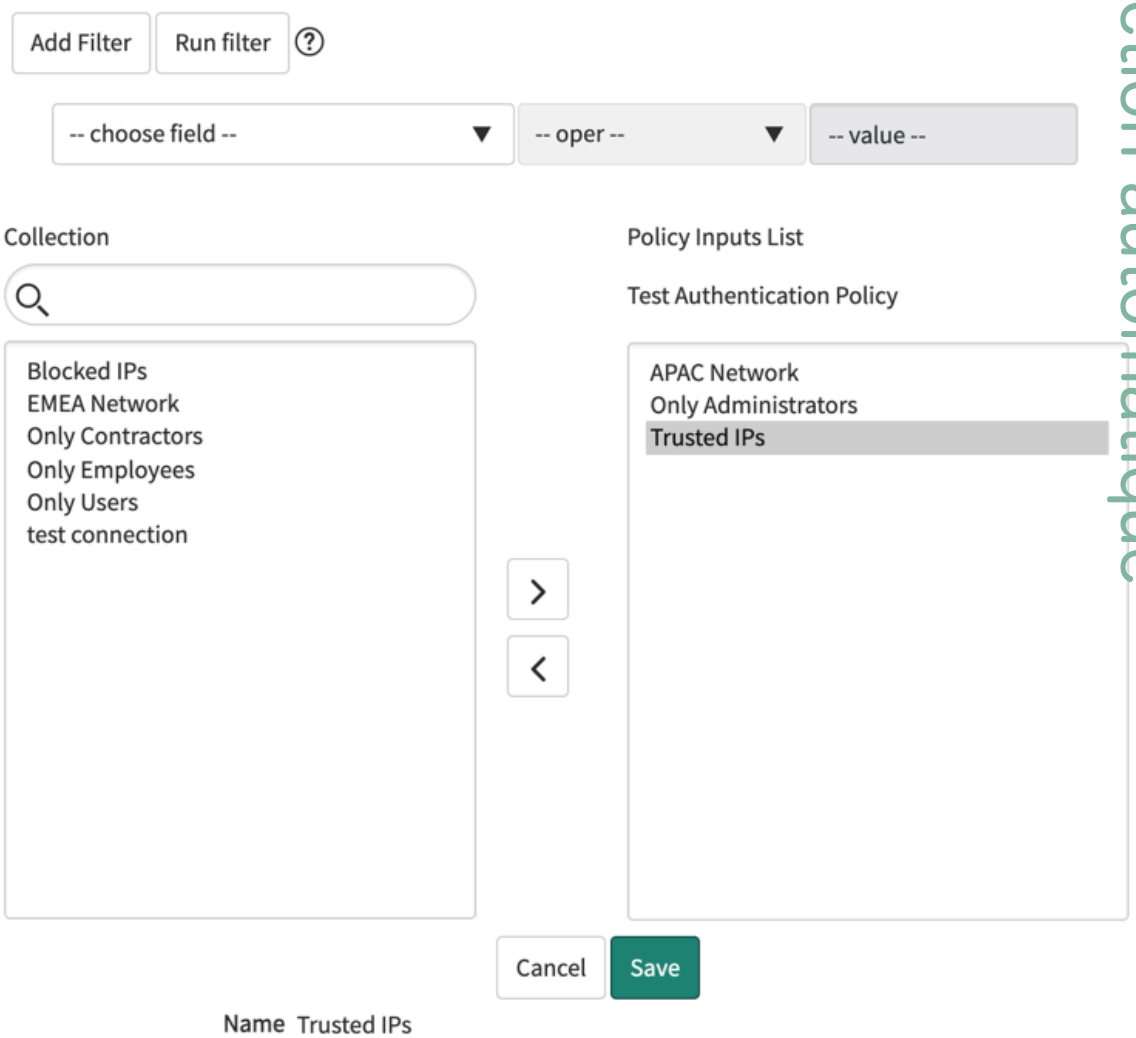
Procédure

1. Accédez à la **Tous** > **Services web du système** > **Politique d'authentification API**.
2. Cliquez sur **Nouveau**.
3. Renseignez ces champs du formulaire.

Formulaire Politique

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 entrée de politique. Pour plus d'informations, consultez Créer des entrées de politique .
6. Déplacez un ou plusieurs critères de filtre de la liste Collections vers la liste Entrées de



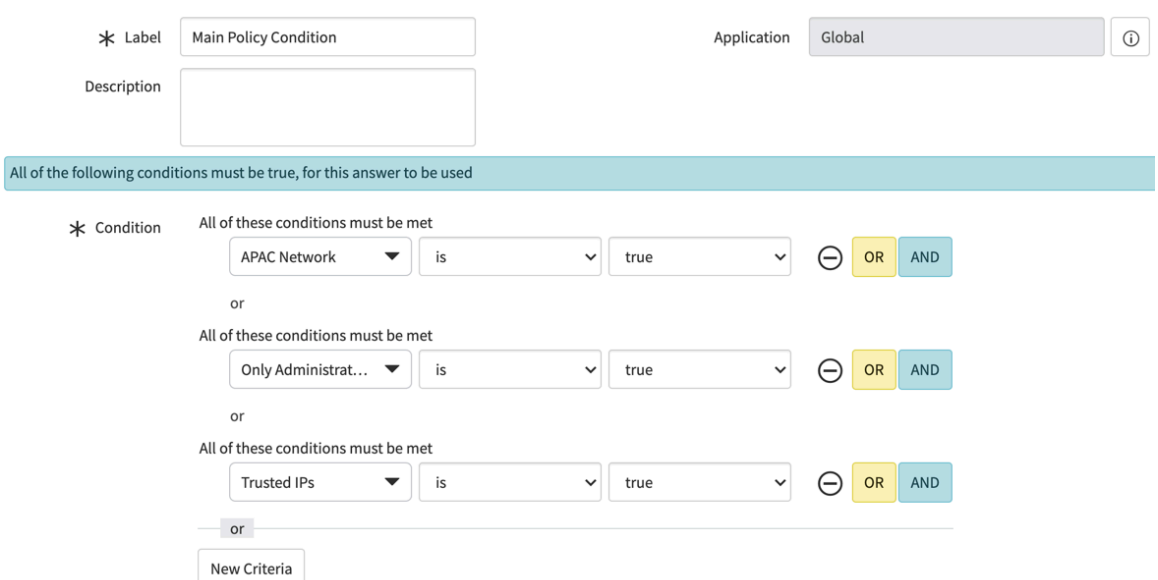
politique.

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 politique.
Description	Brève description de la condition de politique.
Application	Périmètre de l'application.
Condition	Une ou plusieurs conditions combinées avec le filtre **OR** .



10. Sélectionnez **Envoyer**.

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 stratégie peut être utilisée comme alternative au contrôle d’accès à l’adresse IP.

Avant de commencer

Rôle requis : admin

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 **Collecte** et déplacez-les vers la **liste Politique de blocage globale** .
   Vous pouvez également ajouter des filtres supplémentaires.
4. Cliquez sur **Nouveau** dans l’onglet **Conditions de la politique**.
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) qui est utilisée pour évaluer les demandes d'authentification. Par exemple, vous pouvez créer des conditions qui n'autorisent que les prestataires d'une liste d'adresses IP fiables.

Périmètre d'authentification REST API

Prise en charge du périmètre d'authentification pour l'API REST.

Avant Washington DC la mise en production, chaque jeton d'accès ou jeton OIDC est lié au champ d'application useraccount qui dispose d'un accès complet aux API REST de l'utilisateur. À compter de Washington DC la mise en production, pour fournir l'accès uniquement aux API REST particulières, les champs d'application du jeton OAuth sont introduits.

Lorsqu'une entité OAuth est liée à un périmètre d'authentification, jeton émis ou géré par cette entité OAuth et ne peut être utilisé que pour accéder aux REST APIs (une entité OAuth peut être liée à plusieurs périmètres d'authentification). Pour la nouvelle entité OAuth, le périmètre d'authentification par défaut est vide. Vous devez lier manuellement le périmètre d'authentification à l'entité OAuth.

Remarque :

- Une fois le périmètre d'authentification de l'API REST activé et ajouté au périmètre d'authentification de l'API REST, tous les jetons OAuth existants ne sont plus en mesure d'accéder à cette API, sauf si l'administrateur ajoute ce périmètre d'authentification à l'entité OAuth correspondante
- L'administrateur est responsable de s'assurer que l'oauth_entity dispose du bon périmètre d'authentification puis de lier le périmètre d'authentification à l'API REST.
- Les jetons d'accès OAuth émis par ServiceNow prennent en charge le périmètre d'authentification.
- Jeton OIDC qui n'est pas émis par ServiceNow est validé par ServiceNow.
- Le champ d'application du jeton OIDC provient d'IdP lorsque vous avez besoin d'un jeton d'ID. Ici, le champ d'application d'authentification est défini sur au ServiceNow lieu de tiers (IdP).

Configurations du périmètre de l'API REST

Pour configurer le périmètre de l'API REST, effectuez les tâches suivantes :

- Créer un périmètre d'authentification
- Lier le périmètre d'authentification à l'API REST
- Lier le périmètre d'authentification à l'entité OAuth

- Exécuter le flux OAuth pour obtenir le jeton d’accès OAuth
- Utiliser le jeton d’accès OAuth pour effectuer l’appel d’API

Activer le périmètre d’authentification de l’API REST

Vous pouvez activer le module d’extension REST API Auth Scope (com.glide.rest.auth.scope) pour lier l’entité OAuth aux 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. Trouvez le module d’extension REST API *auth Scope (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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

Propriétés et tables du périmètre d’authentification de l’API REST

Le module d’extension REST API Auth Scope (com.glide.rest.auth.scope) inclut les propriétés système, tables et scripts 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. Si la valeur est définie sur false, la vérification du périmètre d'authentification est ignorée pendant l'exécution, qu'elle soit liée ou non à l'API RETS. Par défaut, cette propriété est définie sur true. Ces propriétés sont utilisées lorsque vous souhaitez revenir au comportement de la version précédente.
`com.glide.oauth.token.scope.useraccount`	Cette propriété n'est utilisée que lorsque `useraccount` le périmètre d'authentification est supprimé et rajouté manuellement par l'utilisateur final. Dans ce cas, l'ID système de la `useraccount` est modifié. Vous devez mettre à jour cette propriété vers la nouvelle sys_id. Pendant l'exécution, l'ID système du périmètre d'authentification est utilisé au lieu du nom du périmètre d'authentification.

Tables du périmètre d'authentification de l'API REST

Périmètre d'authentification REST API 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 périmètre d'authentification doit être unique et global.
Périmètre d'authentification 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 avec un champ d'application d'authentification pour gérer l'accès des jetons aux REST APIs liées au champ d'application d'authentification.

Avant de commencer
Installez les modules d'extension suivants :

- OAuth 2.0
- Fournisseur d’API REST
- 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. Renseignez les champs du formulaire.

Périmètre d'authentification REST API

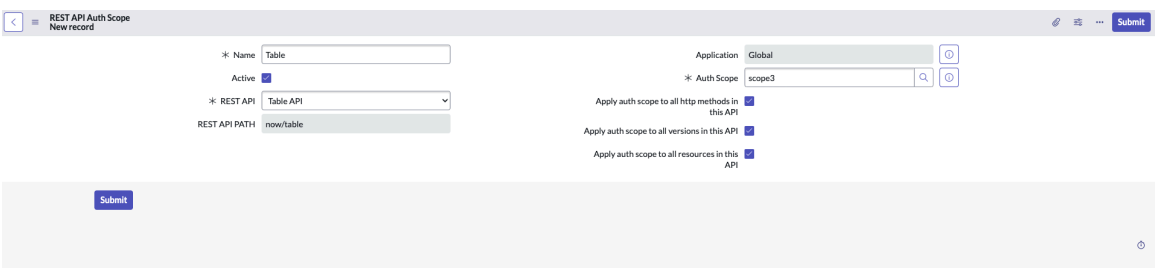
Nom	Nom unique qui identifie le périmètre d’authentification de l’API REST.
Actif	Cochez la case pour activer la configuration.
Application	Champ d'application de l'application en lecture seule.
API REST	L’API REST à laquelle le périmètre d’authentification est appliqué. Par exemple, l’API de table.
Périmètre d'authentification	Sélectionnez le périmètre d’authentification à partir de l’icône de recherche.
CHEMIN REST API	Chemin d’accès de l’API de REST. Ce champ est automatiquement renseigné 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 le **périmètre d’authentification Appliquer à toutes les méthodes http dans** ce champ API du formulaire pour sélectionner la méthode.
Version de REST API	Version de l'API. Par exemple, v1. Ce champ est automatiquement renseigné en fonction de l’API REST sélectionnée. Vous pouvez désactiver manuellement le **périmètre d’authentification Appliquer à**

	toutes les versions dans ce champ API du formulaire pour sélectionner la version.
Ressources	Ressource enfant de l'API REST. Ce champ est automatiquement renseigné en fonction de l'API REST sélectionnée. Par exemple, /now/table. Vous pouvez désactiver manuellement le **champ d'application Appliquer l'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.	Lorsque cette option est activée, applique le périmètre d'authentification à toutes les méthodes http de l'API.
Appliquer le périmètre d'authentification à toutes les versions dans cette API.	Lorsque cette fonctionnalité est activée, 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, le champ d'application d'authentification est appliqué à toutes les ressources de l'API

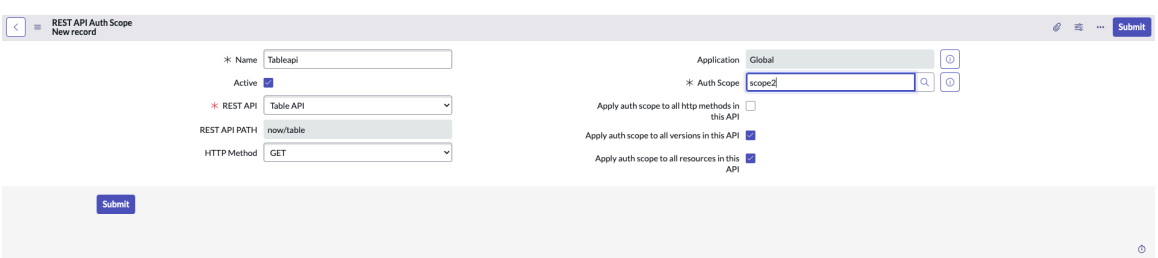
4. Cliquez sur **Envoyer**.
   En fonction de l'API REST et du périmètre d'authentification sélectionnés, les API récupèrent les informations spécifiques au périmètre.

Example: Envisagez de créer trois périmètres d'authentification REST API pour l'API de table

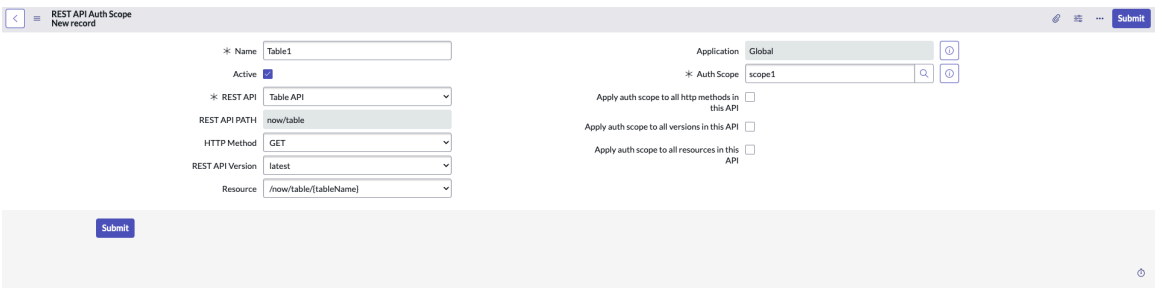
Le premier périmètre d'authentification est mappé à **l'API de table** avec toutes les méthodes, versions et ressources http activées.



Le deuxième périmètre d'authentification est mappé à **l'API Table** avec toutes les versions et ressources activées. Mais, vous choisissez la méthode HTTP, dans cet exemple, la méthode **GET** .



Le troisième périmètre d'authentification est mappé à **l'API de table** sans que les méthodes, versions et ressources HTTP soient 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 **scope3** peut être utilisé.

Résolution des problèmes liés au périmètre de REST API

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 pendant l'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 useraccount .
L'API REST est liée à *auth_scope1*, mais le jeton d'accès qui a *auth_scope2* est également en mesure d'y accéder.	• Vérifiez si cet enregistrement est actif. • Vérifiez ce REST, vérifiez s'il existe d'autres enregistrements qui ont les mêmes API mais qui appliquent des méthodes, des versions ou des ressources différentes.
L'API REST est liée au périmètre d'authentification, mais pendant l'exécution, il n'y a pas de vérification du périmètre d'authentification pour *basicAuth* et *mutualAuth*.	Elle est attendue, car le périmètre d'authentification de l'API REST ne s'applique qu'au jeton d'accès OAuth ou au jeton OIDC. Il n'applique pas l'authentification de base, les cookies de session et l'authentification basée sur les certificats.
L'appel d'API REST renvoie une erreur 403 lors de l'utilisation du jeton d'accès OAuth.	Vérifiez le message d'erreur « Missing required required access scope » (Périmètre d'accès API requis manquant). Si une valeur est trouvée, la vérification

Dépannage (suite)

Problème	Action
	du périmètre d'authentification échoue pour cette REST API
Le compte utilisateur prédéfini est supprimé et pas sûr d'être restauré.	Exportez un compte utilisateur au format XML à partir de l'autre instance et importez-le ou créez un compte utilisateur et modifiez la propriété `glide.oauth.token.scope.useraccount` système dans l'enregistrement de 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 périmètres d'authentification, chaque jeton OAuth émis par ce oauth_entity a les mêmes périmètres d'authentification.

Différents jetons OAuth avec des périmètres d'authentification différents peuvent-ils accéder à la même REST API ?

Oui, pour la même API REST, il est possible d'y accéder via différents champs d'application d'authentification. Tant qu'un champ d'application d'authentification correspond, celui-ci renvoie les résultats.

Le jeton d'accès OAuth avec le périmètre d'authentification useraccount **peut-il accéder à n'importe quelle 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, le champ d'application de l'authentification n'est pas codé en dur avec le jeton d'accès de la table oauth_credential . Au lieu de cela, le champ d'application d'authentification est obtenu à partir de oauth_entity liées pendant l'exécution.

Le jeton OAuth peut-il conserver les mêmes étendues d'authentification après l'actualisation ?

Oui, le champ d'application d'authentification ne changera pas après l'actualisation du jeton, sauf oauth_admin modifier le champ d'application d'authentification lié à oauth_entity.

L'enregistrement du périmètre d'authentification useraccount **prédéfini est supprimé. Est-il possible de créer un nouveau périmètre d'authentification portant le nom** useraccount **?**

La création d'un nouveau champ d'application d'authentification avec le même compte d'utilisateur ne fonctionne pas. Lors de 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 en tant qu'enregistrement de sys_id nouvellement créé.

Si l'administrateur modifie l'authentification dans le champ d'application lié à oauth_entity**, tous les jetons d'accès OAuth existants émis par cette entité OAuth sont-ils également modifiés ?**

Oui, le périmètre d'authentification n'est pas directement lié au jeton d'accès OAuth, il est obtenu à partir de oauth_entity pendant l'exécution.

Différents jetons d'accès OAuth émis par la même oauth_entity **peuvent-ils avoir des périmètres d'authentification différents ?**

Non, tous les accès au jeton sont émis par la même `oauth_entity` et ont toujours les mêmes étendues d'authentification.

Un utilisateur peut-il définir différents périmètres d'authentification pour un point de terminaison particulier ?

Non, il existe une vérification de contrainte unique pour un point de terminaison de REST API particulier. Toutefois, pour le même point de terminaison d'API REST, il peut avoir plusieurs champs d'application d'authentification correspondants.

La vérification du champ d'application d'authentification est-elle également utilisée pour BasicAuth ?

Non, la vérification du périmètre d'authentification concerne uniquement le jeton d'accès OAuth et le 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 aux API SOAP entrantes et aux API SOAP scriptées.

Vous pouvez utiliser des ServiceNow politiques d'accès API telles que la plage 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 de la politique d'accès et du 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 à l'API SOAP et associez-les 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 `standard http` et `WSSE` .

- Créez des politiques d'authentification telles que la plage IP et les restrictions basées sur les rôles, et associez-les 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 de la politique d'accès de l'API SOAP (`com.glide.soap.policy`).

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
L'élément suivant est installé avec le module d'extension SOAP API Access Policy : Politique d'accès au processeur (`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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

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 avec jeton d'ID** et **jeton OAuth** qui sont disponibles par défaut.

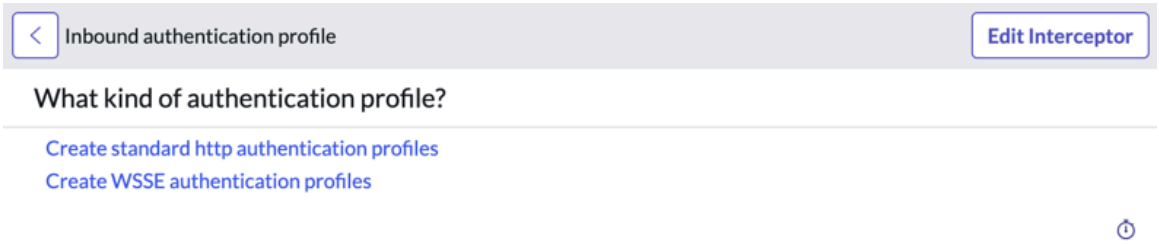
Avant de commencer

Rôle requis : admin

Remarque :
Vous pouvez appliquer des politiques d'authentification, une plage d'adresses 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. Choisissez **Quels types de profils d'authentification ?**.
   - **Créer des profils d'authentification http standard**
   - **Créer des profils d'authentification WSSE**



4. Renseignez les champs du formulaire.

Formulaire Profil d'authentification standard

Champ	Description
Nom	Nom permettant d'identifier la politique d'authentification.
Description	Description de la politique d'authentification.
Actif	Option permettant d'activer la politique d'authentification.
Application	Périmètre de la politique d'authentification.
Type	Type de l'authentification disponible. Vous pouvez sélectionner **l'authentification de base**, le **jeton d'ID**, **l'authentification basée sur certificat**, **OAuth** ou **WSSE** (dans le cas d'un profil d'authentification WSSE).
Entité OAuth	Profil de l'entité OAuth. Ce champ s'affiche uniquement lorsque **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, puis sélectionnez l'icône .

Remarque :
Ne sélectionnez pas **Autoriser la politique d'accès** ou **Refuser la politique d'accès**. Ces politiques sont destinées uniquement aux connexions des utilisateurs.

Vous pouvez ajouter une ou plusieurs politiques d'authentification pour un profil d'authentification.

En cas de changement du profil d'authentification, l'en-tête Autorisation renvoie une valeur spécifique aux modifications apportées à ce moment-

là. Pour avoir la possibilité d'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 **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 de l'API SOAP

Créez une politique d'accès API et mappez un profil d'authentification pour restreindre le type d'authentification pour une API SOAP. Par exemple, vous pouvez créer une politique d'accès à l'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, consultez Créer un profil d'authentification.
- Rôle requis : admin

Procédure

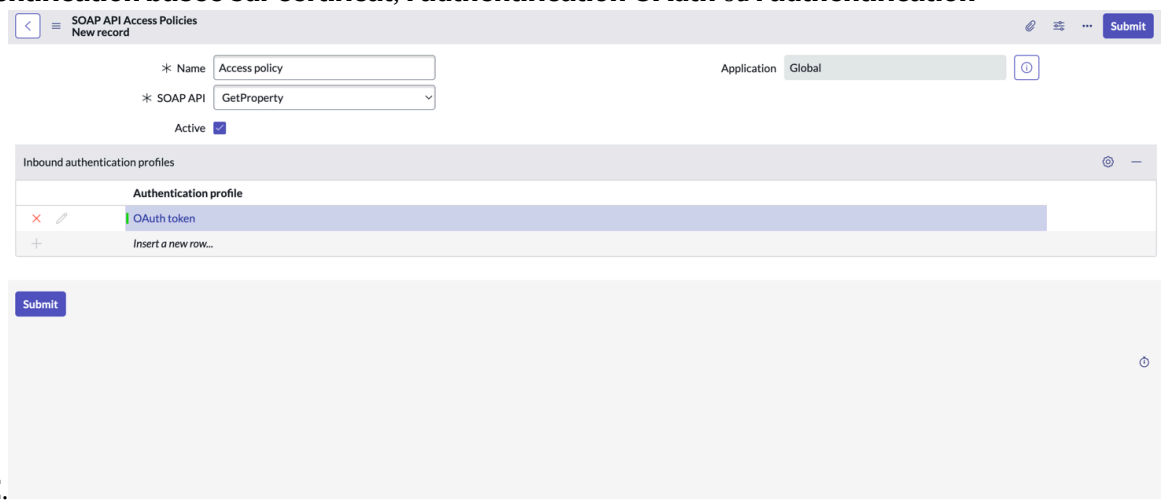
1. Accédez à la **Tous** > **Services web du système** > **Politiques d'accès API** > **Politiques d'accès de l'API SOAP**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Politiques d'accès API

Champ	Description
Nom	Nom unique de la politique d'accès de l'API.
API SOAP	API SOAP à laquelle la politique d'accès est appliquée. Par exemple, **API GetProperty**.
Application	Périmètre de l'application.
Actif	Option permettant d'activer la politique d'accès API.

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 .

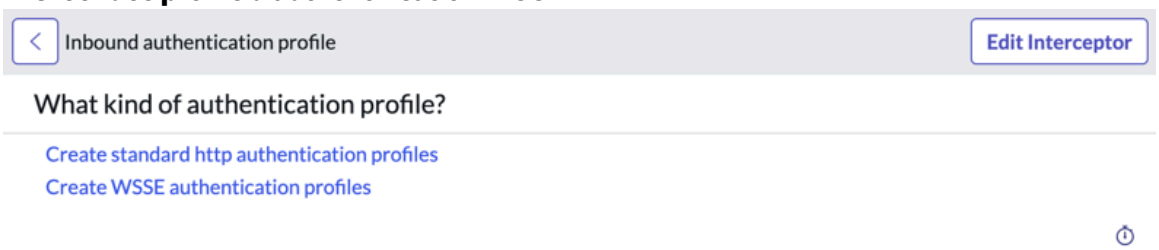
Par exemple, vous pouvez ajouter **l'authentification de base**, le **jeton d'ID**, **l'authentification basée sur certificat**, **l'authentification OAuth** ou **l'authentification WSSE**.



a. Pour ajouter un ou plusieurs profils d'authentification entrants, cliquez sur **Nouveau** pour créer un nouveau profil.

b. Choisissez **Quels types de profils d'authentification ?**.

- **Créer des profils d'authentification http standard**
- **Créer des profils d'authentification WSSE**

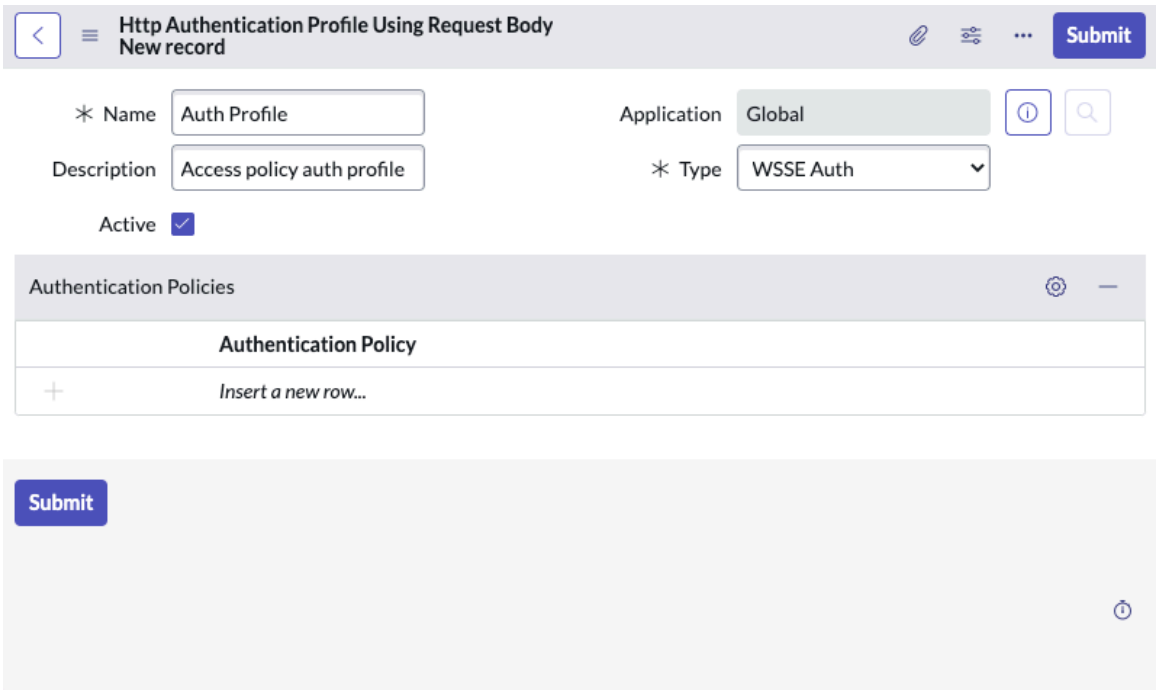


c. Pour créer un profil d'authentification WSSE, renseignez les champs du formulaire.

Profil d'authentification WSSE

Champ	Description
Nom	Nom unique de la politique d'accès de l'API.
Description	Description du profil d'authentification.

Champ	Description
Application	Périmètre de l'application.
Actif	Option permettant d'activer la politique d'accès API.
Type	Authentification WSSE en tant que profil d'authentification WSSE (Web Security).



d. Après avoir créé le profil d'authentification, sauvegardez l'enregistrement.

6. Cliquez sur **Envoyer** pour soumettre la politique d'accès de l'API SOAP.

Créer une politique d'accès API globale 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
- Installez le module **d'extension Processor Access policy** (com.glide.processor.policy)
- Assurez-vous qu'un profil d'authentification est créé. Pour plus d'informations, consultez Créer un profil d'authentification.

Les étapes suivantes décrivent comment créer une politique d'accès globale unique pour protéger toutes les API SOAP.

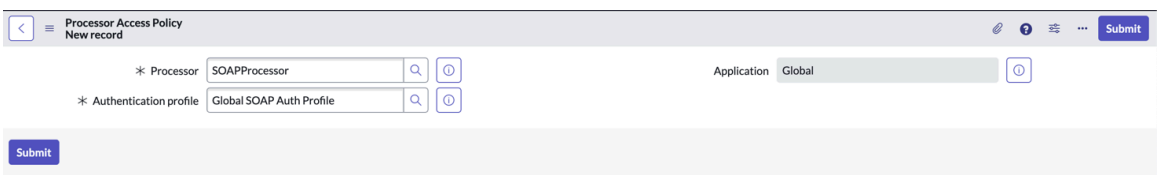
Remarque :
Les politiques définies au niveau de chaque API SOAP remplacent la politique d'accès global au niveau **SOAPProcessor** .

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Politiques d'accès aux processus**.
2. Renseignez les champs du formulaire.

Formulaire 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. Valeur par défaut : globale
Profil d'authentification	Type du profil d'authentifications. Sélectionnez **Profil d'authentification SOAP global**.



3. Sélectionnez **Envoyer**.

Critères de filtre pour les API

Les critères de filtre contiennent des conditions ou des requêtes de filtre 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 d'une politique d'authentification. Par exemple, un critère de filtre 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 en fonction de l'adresse IP de l'utilisateur, de son rôle et du groupe d'utilisateurs auquel il appartient.

Remarque :
Vous pouvez également utiliser 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.

Information associée

- Créer un critère de filtre d'adresses IP
- Créer un critère de filtre de rôle
- Créer un critère 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 exigences 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 sont destinées uniquement 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

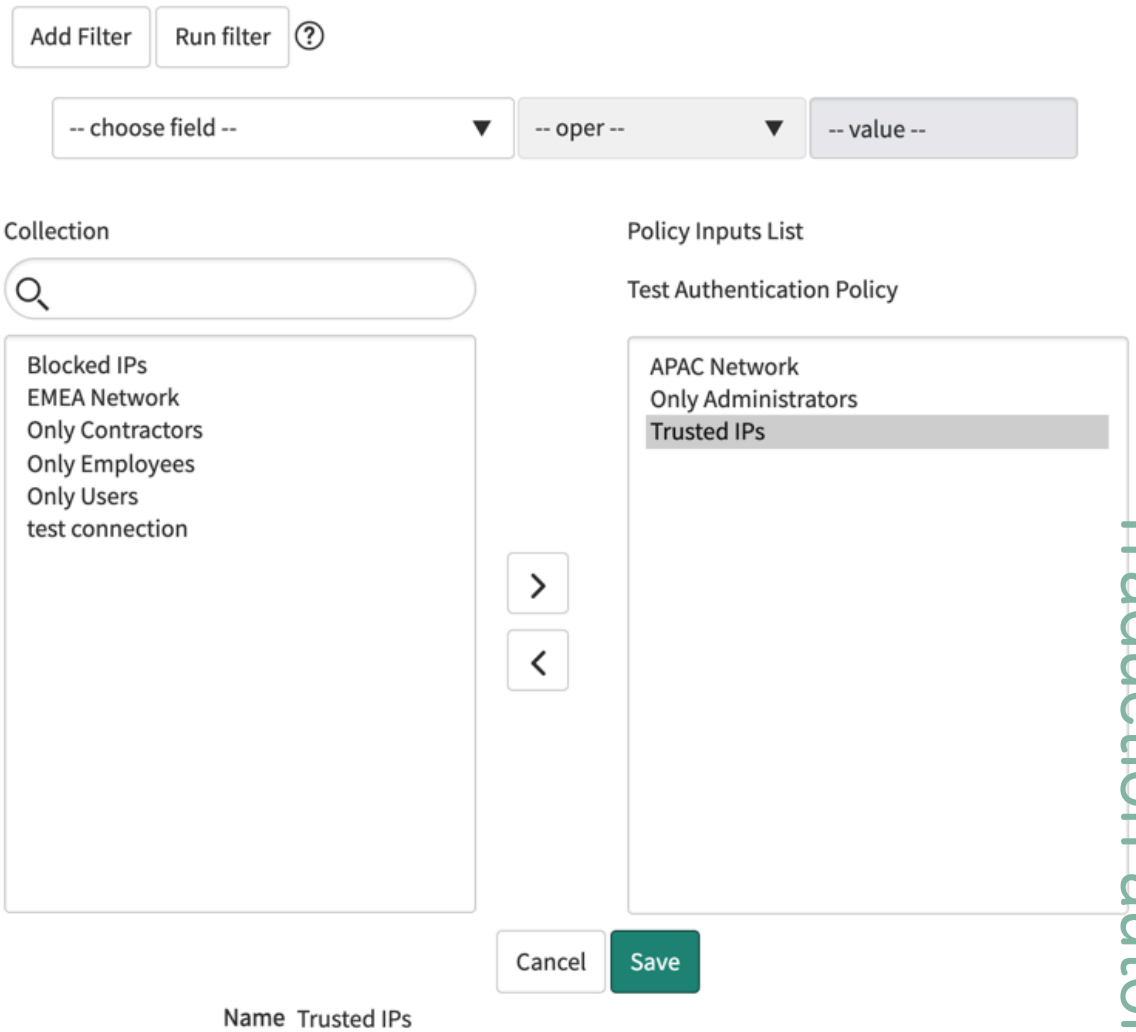
1. Accédez à la **Tous** > **Services web du système** > **Politique d'authentification API**.
2. Cliquez sur **Nouveau**.
3. Renseignez ces champs du formulaire.

Formulaire Politique

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 entrée de politique. Pour plus d'informations, consultez Créer des entrées de politique .

6. Déplacez un ou plusieurs critères de filtre de la liste Collections vers la liste Entrées de

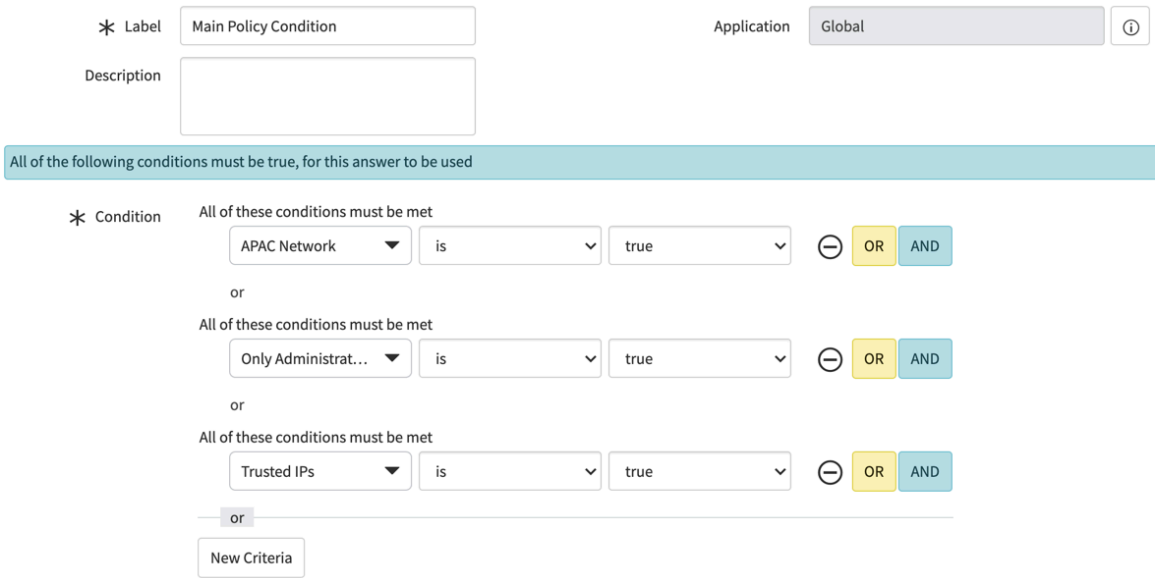


politique.

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 politique.
Description	Brève description de la condition de politique.
Application	Périmètre de l'application.
Condition	Une ou plusieurs conditions combinées avec le filtre **OR** .



10. Sélectionnez **Envoyer**.

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 stratégie peut être utilisée comme alternative au contrôle d'accès à l'adresse IP.

Avant de commencer

Rôle requis : admin

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 **Collecte** et déplacez-les vers la **liste Politique de blocage globale** .
   Vous pouvez également ajouter des filtres supplémentaires.
4. Cliquez sur **Nouveau** dans l'onglet **Conditions de la politique**.
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) qui est utilisée pour évaluer les demandes d'authentification. Par exemple, vous pouvez créer des conditions qui n'autorisent que les prestataires d'une liste d'adresses IP fiables.

Politique d'accès pour les processeurs système/d'exportation

Possibilité pour les processeurs système/d'exportation d'exploiter la politique d'accès au processeur pour sécuriser tous les points de terminaison d'exportation.

Possibilité de sécuriser tous les points de terminaison d'exportation et d'appliquer le profil d'authentification entrant et les politiques d'accès au processeur au niveau global ou de l'instance.

Remarque :

- Les processeurs non publics, y compris les processeurs d'exportation tels que CSV, PDF, etc., sont pris en charge pour les politiques d'accès.
- Les script-processors 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 à l'API.
- L'administrateur peut créer un profil d'authentification avec l'authentification de base et associer une politique d'authentification qui donne toujours la valeur faux.

  Exemple : créez des critères 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 false. De cette façon, les conditions de politique seront toujours évaluées comme fausses et la politique d'accès API bloquera l'accès, quelle que soit l'origine de la demande.

- L'accès au processeur n'est autorisé qu'à partir d'un réseau de confiance.

Activer la politique d'accès au processeur

Pour Processor, installez le module d'extension Processor Access policy (`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. Trouvez 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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

> **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>.

Que faire ensuite

.

Configurez le profil d'authentification pour les processeurs. Pour plus d'informations, Configurer le profil d'authentification pour le processeurconsultez .

Configurer le profil d'authentification pour le processeur

Appliquez le profil d'authentification pour les processeurs d'exportation.

Avant de commencer

Rôle requis : admin

Module d'extension requis : Processor Access Policy (com.glide.processor.policy)

Procédure

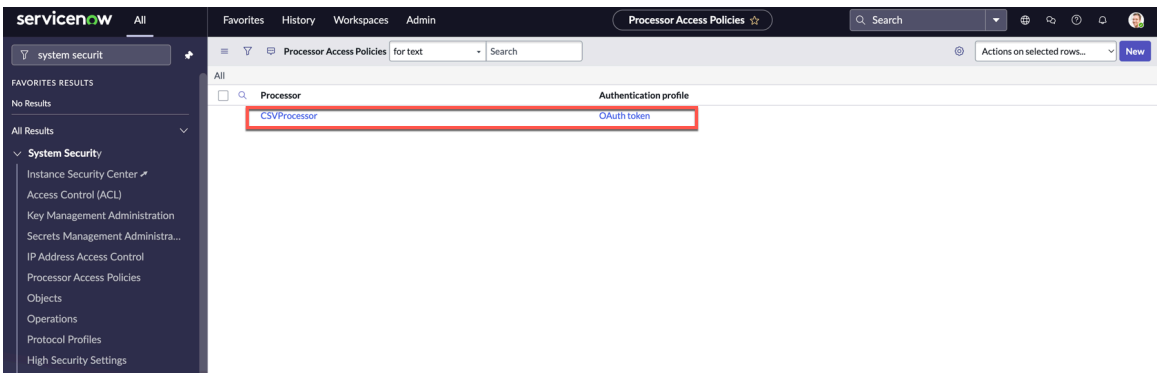
1. Accédez à la **Tous** > **Sécurité de système** > **Politiques d'accès aux processus**.
2. Pour ajouter un profil d'authentification au processeur, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire 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. Valeur par défaut : globale
Profil d'authentification	Type du profil d'authentifications. 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 à l'aide de 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 provenant d'une autorité de certification (CA) approuvée.

Remarque :
L'authentification basée sur certificat n'est pas prise en charge sur l'instance sur site et Edge Encryption activée.

Authentification basée sur certificat pour les connexions à l'interface utilisateur

Permettez aux utilisateurs finaux d'utiliser des cartes PIV (Personal Identity Verification) ou CAC (Common Access Card) pour se connecter à ou Now PlatformPortail de services au lieu d'utiliser un nom d'utilisateur et un mot de passe. Pour configurer l'authentification réciproque pour les connexions à l'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.

Authentification basée sur certificat pour les services Web entrants

Authentifier les demandes entrantes adressées aux ServiceNow 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 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 Now PlatformPortail de services à l’aide de cartes PIV ou CAC. Une fois l’authentification basée sur certificat activée, vous pouvez enregistrer vous-même le certificat PEM ou un administrateur peut mapper le certificat pour vous. Consultez Se connecter à l’aide de l’authentification basée sur certificat.
- Activer 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 Certificate-based authentication (com.glide.auth.mutual) si Now Platform vous disposez du rôle admin.

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 Certificate-based authentication (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.

3. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

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 lorsqu'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 CA** : certificat de l'autorité de certification racine. Peut également inclure des certificats intermédiaires dans la chaîne. Les certificats d'autorité de certification sont automatiquement synchronisés avec l'équilibreur de charge. Dans la mesure du possible, utilisez cette option pour éviter d'omettre un certificat requis dans la chaîne. ○ **Certificat intermédiaire** : certificat intermédiaire dans la chaîne de certificats. Ce certificat reste uniquement sur l'instance et n'est pas synchronisé avec l'équilibreur de charge. Utilisez cette option uniquement si vous avez besoin d'ajouter un certificat intermédiaire à une chaîne existante.
Description brève	Brève description du certificat client utilisateur.

Remarque :
Lors du chargement du certificat, les champs en lecture seule **(Date de début de validité**, **Expire,Expire in days**, **Issuer** et **Objet**), **Chaîne du certificat** et **Certificat PEM** sont extraits et renseignés automatiquement.

4. Cliquez sur **Envoyer**.
5. **Facultatif :** Cliquez sur **Valider les magasins/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 de disposer du certificat PEM (Privacy Enhanced Mail) de l'utilisateur.

Remarque :
Après avoir mappé le certificat PEM à la configuration utilisateur, la « vérification du certificat » échouera. 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 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 lorsqu'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 d'exécution de la demande.
Description brève	Brève description du certificat client 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.

Remarque :
Lors du chargement du certificat, les champs en lecture seule **Valide à partir de**, **Expire,Expire in days**, **Issuer** et Subject (Émetteur) et **Subject (Objet**) sont extraits et renseignés automatiquement.

3. Cliquez sur l'icône des pièces jointes et chargez le certificat.
4. Cliquez sur **Envoyer**.
   Le certificat est validé et mappé sur l'utilisateur spécifié si le certificat provient d'une autorité de certification (CA) approuvée.

Configurer les propriétés de l'authentification basée sur certificat

Utilisez les propriétés système pour activer ou désactiver les fonctionnalités d'authentification basée 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 d'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. Valeur 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-le pour connecter automatiquement l'utilisateur après qu'il a sélectionné un certificat client enregistré et saisi son code PIN. Désactivez-la 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

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).

Enregistrez le certificat client de votre carte PIV ou CAC

Avant de vous connecter à Now Platform à l'aide de 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

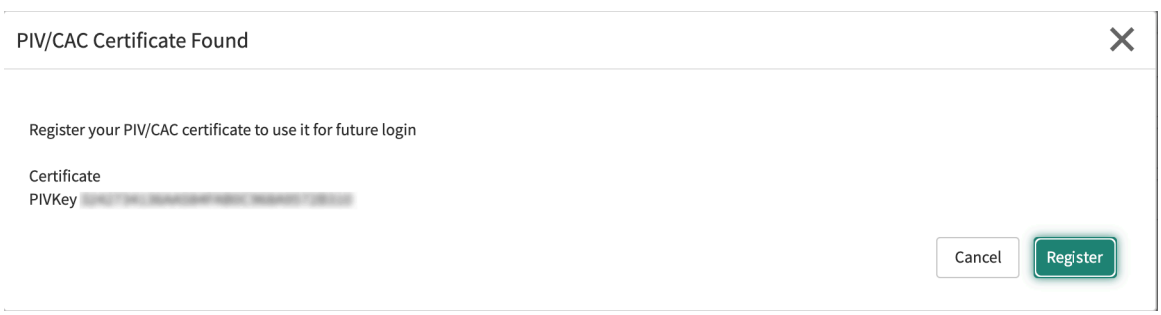
Si vous avez besoin d'un administrateur pour enregistrer votre certificat client, reportez-vous à la section Mapper le certificat PEM à l'utilisateur.

Procédure

1. Connectez-vous à Now Platform à l'aide de votre nom d'utilisateur et de 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**.

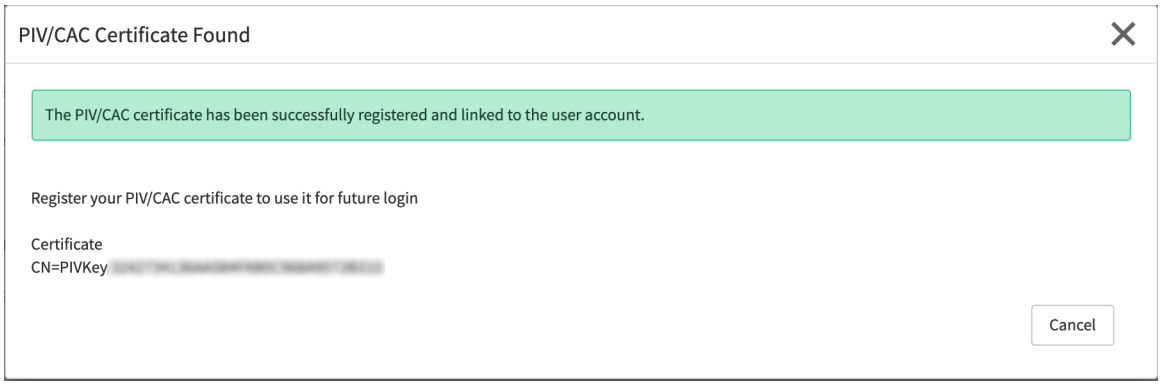
   Si un certificat IS valide est disponible, le message suivant s'affiche :



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.



La prochaine fois que vous vous connecterez à votre Now 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 Now Platform la carte PIV ou CAC.

Connectez-vous à l'aide de Now Platform la 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 Now Platform.

Avant de commencer

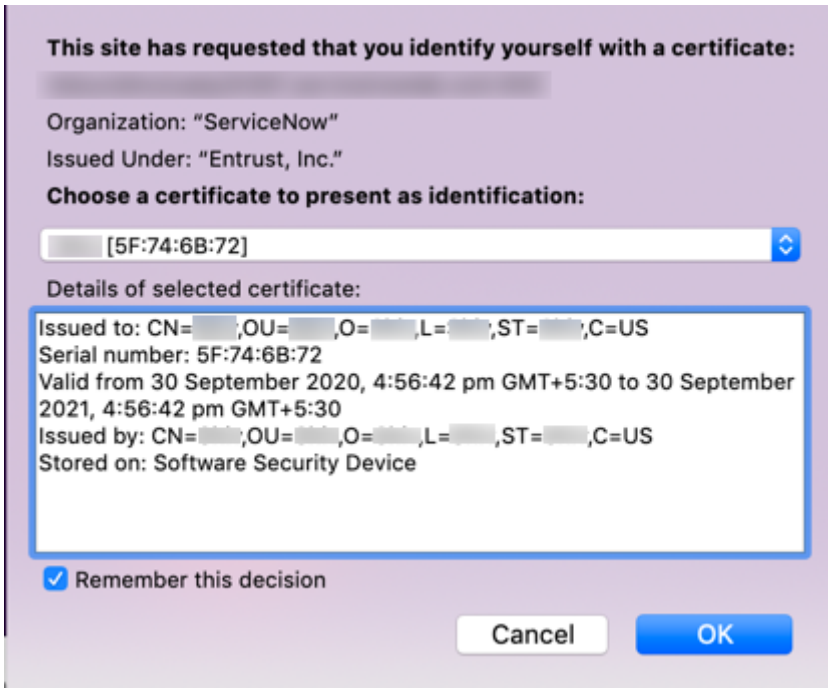
- Rôle requis : aucun
- Assurez-vous que l'authentification basée sur certificat est activée.
- Assurez-vous qu'un lecteur de carte PIV ou CAC est connecté à votre ordinateur.
- Assurez-vous qu'un certificat client de votre carte PIV ou CAC est mappé à vous. Pour plus d'informations, consultez Enregistrer 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 demande 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.

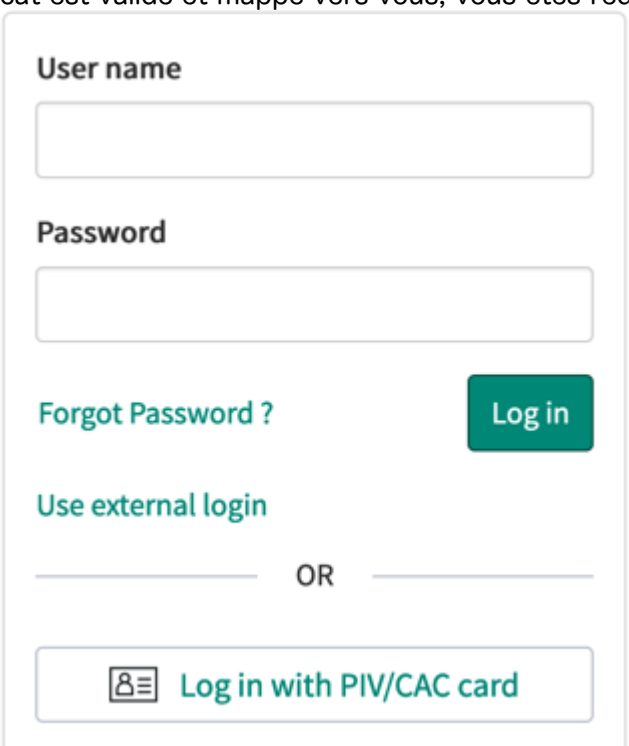
   Remarque :
   Si vous oubliez votre code PIN, contactez votre administrateur.

4. Si vous entrez un code PIN correct, le navigateur affiche une invite pour sélectionner un certificat.



5. Sélectionnez un certificat à partir de l'invite du navigateur.

   Si le certificat est valide et mappé vers vous, vous êtes redirigé vers la page de connexion.



6. Cliquez sur le bouton **Se connecter avec la carte PIV/CAC** .

   Pour vous déconnecter de la Now Platform, vous devez supprimer le PIV ou le CAC du lecteur de carte, puis fermer le navigateur.

Gérer vos certificats clients

Affichez et supprimez les certificats clients associés à votre compte.

Avant de commencer

- Assurez-vous que l'authentification basée sur certificat est activée.
- Rôle requis : aucun

Procédure

1. Connectez-vous à l'aide Now Platform de votre nom d'utilisateur et de 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 du client utilisateur [sys_user_certificate] s'ouvre et affiche les certificats associés à votre compte.
4. Affichez ou supprimez les certificats associés à votre compte.

Association d'URL personnalisées à votre instance

Vous pouvez rendre votre instance accessible à partir d'une URL personnalisée ou personnalisée de l'entreprise ServiceNow .

Vue d'ensemble des URL personnalisées

Vous pouvez utiliser une URL personnalisée pour rendre ServiceNow l'instance accessible à partir d'une ou de plusieurs URL personnalisées ou marquées par l'entreprise.

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 une telle situation, il est nécessaire de rediriger les utilisateurs vers différents IdP pour l'authentification sur la base de l'URL personnalisée à laquelle les utilisateurs accèdent.

Important :

- Ne créez pas d'URL personnalisée avec plus de 100 domaines par instance.
- Vous devez d'abord supprimer l'enregistrement d'URL personnalisé de l'instance ServiceNow , puis supprimer toutes les entrées DNS (Domain Name Server) du serveur DNS.
- Toute suppression d'une entrée DNS du serveur DNS avant la suppression d'un enregistrement d'URL personnalisée de l'instance ServiceNow entraînerait le blocage de la suppression des autres enregistrements d'URL personnalisées correspondants à partir de ServiceNow.

À partir de Tokyo, vous pouvez autoriser les utilisateurs à effectuer une redirection automatique vers les IdP spécifiés définis dans l'enregistrement d'URL personnalisée.

Remarque :
Les URL personnalisées ne sont pas disponibles pour les clients sur site ou les instances de développeur. En outre, l'URL doit être publique.

Seul le propriétaire du domaine de premier niveau (TLD) ou de tout sous-domaine peut configurer l'URL personnalisée vers un sous-domaine DNS. Par exemple, votre instance peut comporter l'URL désignée suivante et des URL personnalisées supplémentaires :

Exemple d'URL personnalisée

Exemples d'URL	Utilisation
https://acme.service-now.com	Le nom de domaine initial d'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	Une 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. Des configurations spécifiques sont également 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 en tant qu'URL d'instance ServiceNow .
Déterminez votre statut VIP dédié	Le statut de VIP.

Remarque :
Lors de la suppression ou de la mise à jour d'enregistrements CNAME qui pointent vers votre instance, vous devez suivre cette séquence pour éviter de faire pendre des enregistrements dans l'instance. Tout d'abord, supprimez les enregistrements CNAME de votre instance, puis supprimez ou mettez à jour le paramètre CNAME chez 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 personnalisé (com.snc.customurl) si vous disposez du rôle administrateur.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Modules d'extension**.
2. Recherchez et cliquez sur le module d'extension **URL personnalisé** .

   Remarque :
   Ne sélectionnez pas le module **d'extension URL personnalisé - Interne** , qui est un composant interne pour les API d'URL personnalisées scriptées.

3. Dans l'enregistrement URL personnalisé, 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 **False**, ce qui signifie que vous ne pouvez pas associer une 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 d'URL personnalisé et avoir acheté ou enregistré une URL avant d'ajouter l'URL personnalisée à votre instance.

Procédure

1. Accédez à la **Tous** > **URL personnalisé** > **URL personnalisées**.
2. Vous devez :
   - Cliquez sur **Nouveau** pour associer un nouveau nom de domaine pour votre instance.
   - Sélectionnez une URL personnalisée déjà configurée pour être l'URL de votre instance.
3. Renseignez les champs appropriés :

Champs d'URL personnalisés

Champ	Description
Nom du domaine	Nom de domaine complet (FQDN) de l'URL personnalisée. Le nom de domaine complet est une redirection CNAME créée dans l'enregistrement du serveur de noms pour le domaine personnalisé. **Remarque :** Par exemple, dans le serveur de noms pour acme.com, vous pouvez créer une entrée : `support.acme.com 300 IN CNAME acme.servicenow.com`
Est une URL d'instance	Case à cocher 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 comme URL d'instance** sur l'enregistrement URL. Toutes les URL personnalisées précédentes sont ensuite 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	Service Portal 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 pour l'URL personnalisée vous permet d'autoriser les utilisateurs à effectuer une redirection automatique vers les IdP spécifiés définis dans l'enregistrement d'URL personnalisée.

Une URL personnalisée doit s'activer dans les six heures sur votre instance. Une tâche en arrière-plan effectue une interrogation pour l'achèvement de la tâche d'URL personnalisée toutes les 30 minutes.

Remarque :

- Vous devez d'abord supprimer l'enregistrement d'URL personnalisé de l'instance ServiceNow , puis supprimer toutes les entrées DNS (Domain Name Server) du serveur DNS.
- Toute suppression d'une entrée DNS du serveur DNS avant la suppression d'un enregistrement d'URL personnalisée de l'instance ServiceNow entraînerait le blocage de la suppression des autres enregistrements d'URL personnalisées correspondants à partir de ServiceNow.

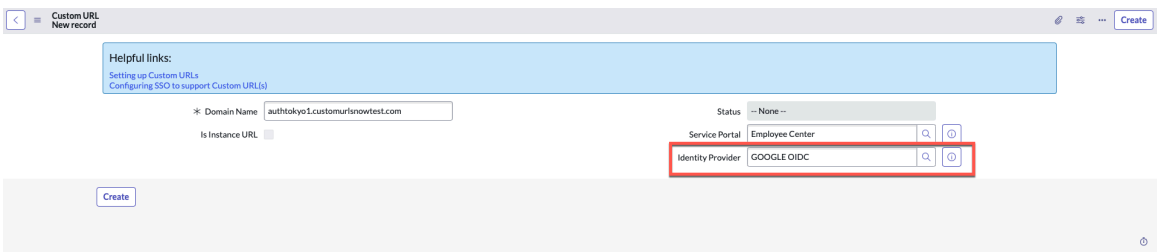
URL personnalisée avec fournisseur d'identité

Définissez votre URL personnalisée avec le fournisseur d'identité pour permettre à l'utilisateur de se connecter avec son IdP.

Avant de commencer
Rôle requis : admin

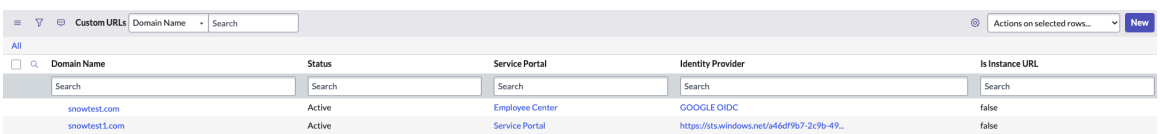
Procédure

1. Accédez à la **Tous** > **URL personnalisé** > **URL personnalisées**.
2. Cliquez sur **Nouveau**.
3. Fournissez les détails de l'IdP dans le champ **Fournisseur d'identité** .
   Pour en savoir plus sur d'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.



   Lors de l'accès à l'URL personnalisée, l'utilisateur est redirigé vers le fournisseur d'identité configuré. Dans ce cas, en accédant au `snowtest.com`, l'utilisateur est dirigé vers **Employee Center**, 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 est défini à la Portail de services fois, lorsque l'utilisateur accède à l'URL personnalisée avec le Portail de services champ qui est défini, il est dirigé vers le fournisseur d'identité configuré.
   - Si le champ Fournisseur d'identité est défini à la Portail de services fois, lorsque l'utilisateur accède à l'URL personnalisée avec l'autre portail 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 du 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.

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 CERT.
Nombre d'interrogations	Nombre de fois où les résultats ont été interrogés pour cette tâche.
Résultat	Vérifie et valide chaque domaine ou URL personnalisée envoyé dans une charge utile.
Statut	État 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 du SP soient générées pour l'IdP avant que l'instance d'URL personnalisée ne soit générée.

Avant de commencer

Rôle requis : admin

L'IdP a besoin des métadonnées du SP pour que l'instance puisse s'authentifier et transmettre les demandes.

Remarque :
L'ajout de l'URL du service consommateur d'assertion (URL de connexion du SP) peut être différent pour chaque IdP (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 du SP de l'instance à partir des paramètres de propriété système.
Authentification unique SAML 2	Accédez à la **Authentification unique SAML 2** > **Métadonnées**. L'intégration génère automatiquement les métadonnées du SP de l'instance à partir des paramètres de propriété système.

2. Copiez les métadonnées du portail de services 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 du SP en ligne.
4. **Facultatif :** Pour configurer des URL personnalisées dans Azure :
   a. Accédez à **Inscriptions des 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 Okta UD.
   b. Une application Okta pour l'URL de l'instance « service-now.com ».
   c. Une application Okta pour l'URL personnalisée.

   Remarque :
   - Désactivez la **désactivation de l'authentification forcée** dans la configuration Okta pour que la **connexion de test** s'exécute correctement.
   - Si vous testez l'enregistrement du fournisseur d'identité associé à l'URL de base, assurez-vous que vous devez vous connecter à l'instance avec l'URL de base.
   - Si vous testez le fournisseur d'identité associé à l'URL personnalisée, connectez-vous 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 de 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 personnalisé

Une liste des erreurs courantes et des correctifs associés pour une configuration et une configuration d'URL personnalisées.

Erreurs lors de l'installation

Message d'erreur	Corriger
Impossible de créer une URL personnalisée. Réessayez ultérieurement.	Il se peut qu'un problème indépendant de votre volonté 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 personnalisé, car une autre demande URL personnalisé pour votre instance est toujours en cours.	Vérifiez l'état de vos tâches URL personnalisées avant d'envoyer une nouvelle demande.
Vous devez effacer les propriétés suivantes pour pouvoir définir l'URL d'instance : proxy Glide, servlet Glide.	
L'approvisionnement des <custom_domain> est toujours en cours. Ce processus peut prendre jusqu'à X heures. Votre administrateur d'instance recevra une notification à l'issue de ce processus.	Une fois que la mise en service sur une instance a démarré pour une URL personnalisée, vous devez attendre que le processus se termine avant que l'état ne change.
<custom_domain> est maintenant définie comme la nouvelle URL d'instance. <base.service-now.com> est toujours en service, mais toutes les nouvelles URL, telles que 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 de l'instance peut utiliser des notifications.
La <custom_domain> URL personnalisée est définie pour être immédiatement supprimée de la configuration d'instance et redevenir <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 que vous avez l'intention de changer votre URL personnalisée. En acceptant cette confirmation, vous initiez le changement de l'URL pour votre instance. Toute URL figurant sur votre liste de noms de domaine, en tant qu'URL personnalisée, peut être active, sauf si vous la supprimez de l'enregistrement CNAME de votre fournisseur.
Vous ne pouvez pas modifier glide.servlet.uri. Cette propriété est définie par l'URL personnalisée.	
Vous ne pouvez pas modifier glide.proxy.host. Cette propriété est définie par l'URL personnalisée.	
L'enregistrement CNAME pour <custom_domain> ne pointe pas vers <base.service-now.com>.	La configuration du côté du fournisseur d'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 pour pouvoir définir l'URL personnalisée pour votre instance.

Intégration 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 l'affectation de rôles. Une intégration LDAP permet au système d'utiliser votre serveur LDAP existant comme source principale de données utilisateur. En règle générale, une intégration LDAP fait également partie de l'implémentation d'une authentification unique.

L'intégration utilise les informations d'identification du compte de service LDAP pour récupérer le nom distinct (ND) de l'utilisateur auprès du serveur LDAP. En fonction de la valeur DN de l'utilisateur, l'intégration redémarre la liaison avec LDAP avec le ND et le mot de passe de l'utilisateur. Le mot de passe saisi par l'utilisateur 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 l'annuaire 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 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 seront pas en mesure de se connecter à l'instance. L'instance ne peut pas modifier le mot de passe Active Directory d'un utilisateur.

Fonctionnalités de l'intégration LDAP

Les fonctionnalités d'intégration LDAP sont les suivantes.

Actualisation LDAP planifiée

Une analyse programmée de votre serveur LDAP est généralement exécutée une fois par nuit. Il interroge tous les attributs des enregistrements d'utilisateurs applicables et les compare avec le compte sur nos serveurs. S'il y a une différence, nous modifions notre enregistrement d'utilisateur avec l'attribut modifié. La charge imposée au serveur LDAP pendant l'actualisation dépend du nombre d'enregistrements interrogés et du nombre d'attributs comparés. Nous vous recommandons de programmer l'actualisation pendant les heures creuses. Une opération d'actualisation volumineuse peut affecter d'autres opérations planifiées, telles que l'exécution de rapports, et doit être planifiée de manière à minimiser les conflits.

Écouteur LDAP

LDAP Listener 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 prenne 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 presque en temps réel des détails du compte de vos utilisateurs, sans avoir à attendre la prochaine actualisation programmée.

Connexion LDAP sur demande

Une fois l'intégration LDAP établie, l'instance peut autoriser les 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 dispose d'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 qui a été saisi. Si un compte LDAP correspondant est trouvé, l'intégration tente de s'authentifier avec le mot de passe saisi par l'utilisateur. Si le mot de passe est valide, l'instance crée un compte pour l'utilisateur, remplit le compte avec toutes les informations LDAP applicables et connecte l'utilisateur à l'instance.

La connexion sur 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 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 des consultants en ServiceNow services professionnels.

Une intégration aux serveurs LDAP vous permet de remplir rapidement et facilement la base de données de l'instance avec des enregistrements utilisateur provenant de la base de données LDAP existante. Pour éviter toute incohérence 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, ce qui permet d'importer 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 de l'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, de sorte que 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 ses informations d'identification réseau sur la page de connexion :

1. L'instance transmet les informations d'identification à un serveur LDAP pour rechercher l'instance.
2. Avec les RDN, il valide la chaîne DN de l'utilisateur. La validation n'est valable que si au moins une des configurations LDAP OU 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 auprès de votre serveur LDAP, les utilisateurs accèdent à la plateforme avec les mêmes informations d'identification que celles qu'ils utilisent pour d'autres ressources internes sur votre domaine réseau. En outre, vous pouvez réutiliser les mots de passe et les politiques de sécurité existants qui sont déjà en place. Par exemple, le serveur LDAP a peut-être déjà 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.

Mises à jour de l'enregistrement utilisateur LDAP

Champ	Description
Source	Identifie 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 de l'enregistrement utilisateur est utilisé pour valider l'utilisateur lors de la connexion.
Serveur LDAP	Identifie le serveur LDAP qui authentifie l'utilisateur lorsqu'il existe plusieurs serveurs LDAP.

Remarque :
Le système ne prend pas en charge l'authentification par mot de passe LDAP via un MID Server. Une instance doit pouvoir se connecter directement à un serveur LDAP pour prendre en charge l'authentification par mot de passe.

Présentation de l'intégration LDAP

Une intégration LDAP permet à votre instance d'utiliser votre serveur LDAP existant comme source principale de données utilisateur.

Prérequis pour l'intégration LDAP

- Le serveur des services de répertoire doit être conforme à LDAP v3
- L'accès au réseau entrant via le pare-feu doit être autorisé (au 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

Délai d'intégration LDAP

Les intégrations LDAP sont généralement effectuées avant la mise en service de l'instance, mais peuvent être intégrées à tout moment.

Intégrité des données du serveur LDAP

Certains utilisateurs craignent qu'un tiers (l'instance en l'occurrence) 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 modifications (y compris les ajouts) apportées à votre serveur LDAP sont disponibles pour l'instance en quelques secondes, en fonction du nombre de composants de l'intégration LDAP complète en place.

Pour maintenir la synchronisation des enregistrements LDAP, 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 à des groupes sont maintenus à jour par le mécanisme d'écoute LDAP et une navigation LDAP complète quotidienne, 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 celui-ci serait effacée ou supprimée. Les éléments de configuration (CI), les accords SLA, les licences de logiciel, les bons de commande et les entrées de Service Catalog ont tous une référence au département. Si le département est supprimé, ces références sont effacées. Il existe de nombreuses références aux utilisateurs, et donc la suppression d'un utilisateur perdrait tout l'historique de ce qu'il a fait. Actuellement, la décision de supprimer ou de ne pas supprimer est prise par nos clients.

Sécurité

La connexion se fait à partir d'une seule machine utilisant 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 le LDAP standard, ou charger le côté public d'un certificat SSL installé sur votre annuaire, auquel cas nous pouvons utiliser LDAPS. Pour ajouter une couche de sécurité supplémentaire, nous offrons également l'option d'un tunnel VPN IPSEC point à point. Adressez-vous à votre chargé de clientèle pour plus de détails et pour connaître les tarifs.

Connexions LDAP sécurisées

Connexion	Description
Serveur MID	Pour protéger votre serveur LDAP du trafic réseau externe, installez un MID Server sur le réseau local et configurez le système pour communiquer avec le MID Server 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 les tarifs.

Un autre aspect de sécurité à prendre en compte est celui des 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.

Importer des données LDAP dans l'instance

Il est recommandé que des attributs soient définis pour importer uniquement les données requises. Les attributs définis sont mappés dans la base de données des utilisateurs de l'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 commerciales.

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 l'interface avec le serveur LDAP. Tant que votre serveur LDAP est conforme à LDAP v3, l'intégration est réussie.

Authentification unique LDAP

En plus de la fonctionnalité de remplissage des données fournie avec l'importation LDAP, vous pouvez utiliser la fonctionnalité d'authentification externe prise en charge par l'application pour éviter que vos utilisateurs aient besoin de 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 des attributs LDAP uniques pour les noms d'utilisateur d'application et d'importer des valeurs de fusion. Un attribut de coalescence 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 requête LDAP (maxPageSize) de 1 000 objets pour empêcher 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 interrogez les objets « b ». La méthode la plus efficace pour les grands environnements consiste à activer la radiomessagerie. 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, alors « aucun » est utilisé, 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 DN de l'utilisateur sur le serveur LDAP. Compte tenu de la valeur DN de l'utilisateur, nous relions la liaison avec LDAP en fonction du DN de l'utilisateur et du mot de passe fourni.

Stockage des mots de passe

Le mot de passe saisi par l'utilisateur est entièrement contenu dans sa session HTTPS. Nous ne stockons ce mot de passe nulle part.

Configurer LDAP Authentication

Ces champs de l'enregistrement utilisateur appartiennent à LDAP :

- **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 de 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 le serveur à utiliser pour authentifier l'utilisateur.

Exigences relatives à l'intégration LDAP

Passez en revue les exigences relatives à l'intégration LDAP, qui comprennent un certificat PKI et un serveur de services d'annuaire compatible LDAP.

L'intégration LDAP nécessite :

- Serveur de services d'annuaire compatible LDAP v3
  - Autorise 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 MID Server.
- Un compte LDAP en lecture seule de votre choix
- Pour plusieurs domaines, accès 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* pour s'interfacer avec le serveur LDAP, l'instance s'est intégrée avec succès aux serveurs suivants :

- Microsoft Active Directory
- Novell
- Domino (Lotus Notes)
- Ouvrir LDAP

Limites de requêtes LDAP

Par défaut, Active Directory 2000/2003 dispose d'une limite de requête LDAP (maxPageSize) de 1 000 objets pour empêcher les charges excessives et les attaques par déni de service. Le système dispose de 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 interrogez les objets b.
- La méthode la plus efficace pour les grands environnements 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 la connexion des utilisateurs à partir de l'annuaire LDAP de leur société.

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 MID Server	Communique par défaut via HTTP sur le port 80. Ce canal de communication ne nécessite pas de certificat. La connexion entre le MID Server et l'instance se fait via HTTPS (port 443). Vous pouvez utiliser le MID Server pour importer des données via LDAP, mais vous ne pouvez pas utiliser le MID Server pour l'authentification LDAP. Poursuivez 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 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 Installer le certificat SSL LDAP X.509 pour obtenir et télécharger le certificat.	Oui	Oui
Connexion VPN	Communique via un tunnel IPSEC. Achetez ou créez un tunnel IPSEC sur votre réseau local. Poursuivez la définition du serveur LDAP.	Oui	Oui

Si vous utilisez un MID Server, ce dernier se connecte à l'instance et MID Server au serveur LDAP. Dans les deux cas, le MID Server initie la connexion :

1. Tout d'abord, le MID Server se connecte au serveur LDAP via LDAP sur le port 389.
2. Ensuite, le MID Server établit une connexion chiffrée HTTPS vers l'instance sur le port 443 pour transmettre les données à l'instance.

Pour plus d'informations sur les VPN, les MID Server 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.

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 **Notifier 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 ayant le rôle administrateur.
Avertissement avant l'expiration (en jours)	Nombre de jours avant l'expiration de l'envoi de la notification par l'instance. Saisissez une valeur d'au moins 20. Les instances mises à niveau vers Istanbul et les versions ultérieures ont cette valeur définie sur 20, sauf si une valeur supérieure est spécifiée.
Actif	Case à cocher pour indiquer que ce certificat est actif.
Format	Le format du certificat.
Type	Le conteneur de certificats. L'instance reconnaît les certificats des magasins de confiance, du magasin de clés Java et des magasins de clés PKCS#12.
Date de début de validité	L'instance ajoute automatiquement la date de début de validité du certificat dans 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 l'objet du certificat dans ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Certificat PEM	Saisissez la valeur du certificat X509.

Remarque :
À l'heure actuelle, l'intégration ne signe pas le certificat dans les communications entre l'instance et l'IdP.

4. Cliquez sur **Enregistrer**.

Que faire ensuite
Cliquez sur **Valider les magasins/certificats** pour tester le magasin de confiance et le certificat.

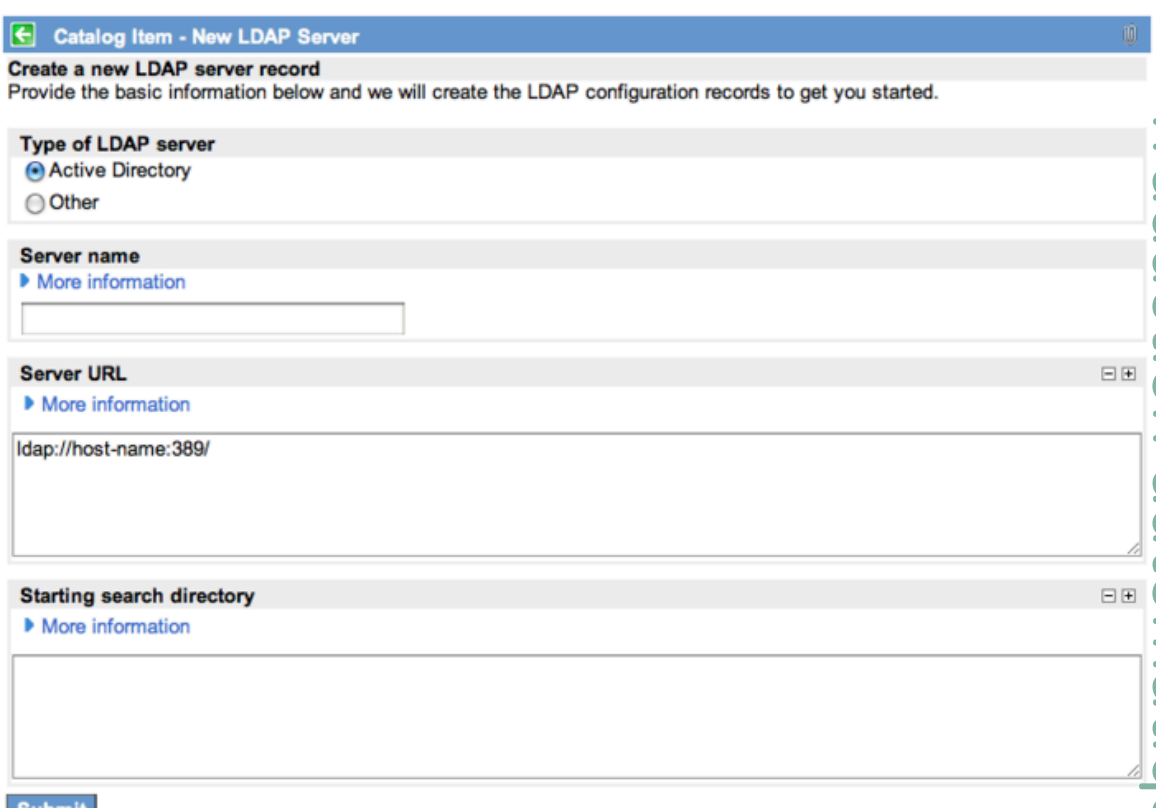
Définir un serveur LDAP

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 état opérationnel, avec les serveurs qui sont **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 décalage entre le changement de l'état de fonctionnement réel et l'affichage.

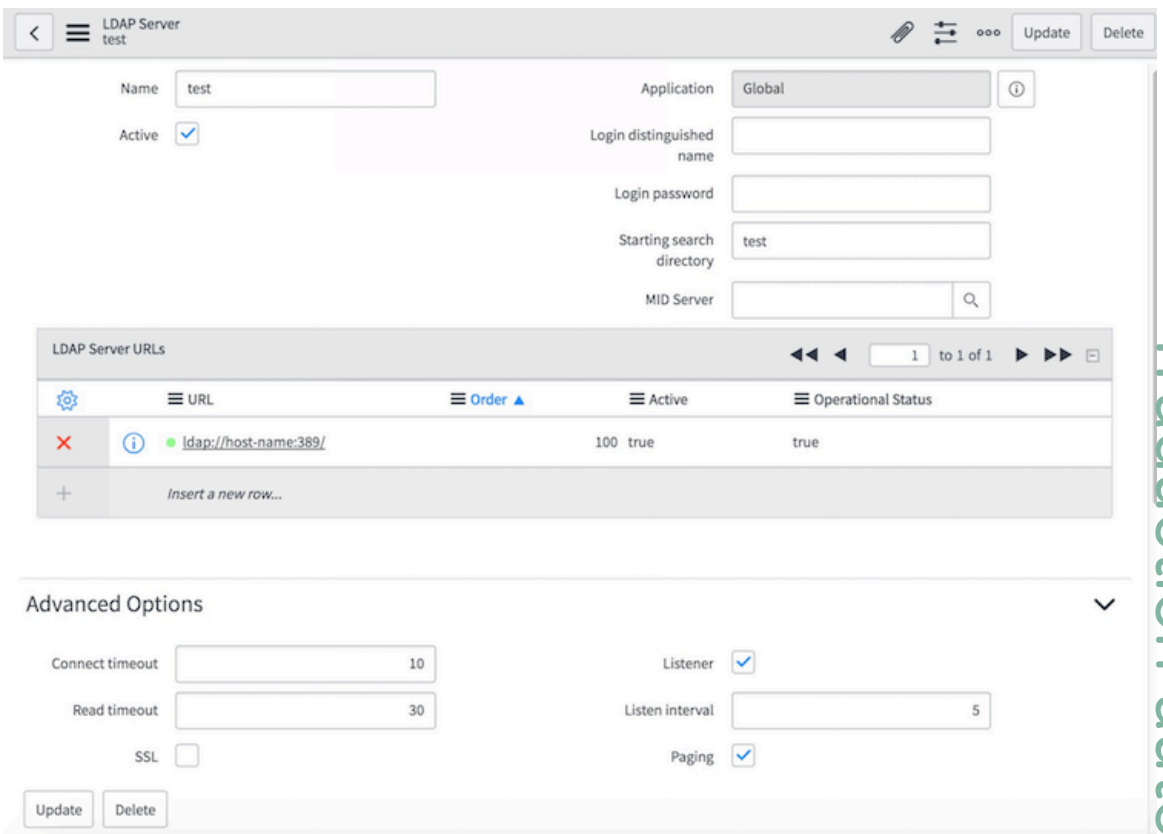
Vous pouvez également ajouter un serveur LDAP redondant en accédant à un enregistrement de serveur LDAP existant et en insérant une ligne dans la liste incorporée des URL des serveurs LDAP.

3. Cliquez sur **Envoyer**.

Remarque :
Vous pouvez également modifier un enregistrement de serveur LDAP existant en accédant à **Système LDAP** > **Serveurs LDAP** et d'apporter les changements nécessaires.

4. Modifiez les champs au besoin.

Formulaire 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 de secours. Les serveurs sont d'abord classés par état opérationnel, avec les serveurs qui sont 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 afficher dans le champ **URL du serveur LDAP** , séparés par un espace et classés par statut opérationnel et valeurs d'ordre des URL.
Nom de connexion distinct	Entrez le nom unique (ND) 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 distinctif complet : `servicenow@service-now.com`

Champ	Description
Mot de passe de connexion	Entrez le mot de passe du serveur.
Répertoire de recherche de départ	Entrez le nom distinct relatif (RDN) du répertoire de recherche par défaut. Toutes les requêtes adressées à ce serveur LDAP commenceront à partir de ce RDN.
Serveur MID	Sélectionnez le MID Server que vous voulez utiliser pour vous connecter au serveur LDAP. L'utilisation d'un MID Server pour établir une connexion LDAP vous évite d'avoir à exposer le serveur LDAP au trafic réseau externe. Il élimine également la nécessité d'établir un tunnel VPN entre votre serveur LDAP et ServiceNow les centres de données. **Remarque :** ◦ L'utilisateur du MID Server doit avoir le rôle user_admin afin de pouvoir lire les enregistrements de configuration du serveur LDAP. ◦ Les éléments suivants ne sont pas disponibles avec le MID Server : ▪ Authentification LDAP ▪ Connexion SSL
Délai de Connexion	Si un MID Server est configuré, la connexion expire au bout de 10 secondes, quel que soit le 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 une fois que la connexion a dépassé le délai d'expiration 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 saisissez des valeurs de délai d'expiration pour ce champ et la propriété système, la valeur de délai d'expiration la plus basse est prioritaire.
SSL	Activez cette case à cocher pour exiger du serveur LDAP qu'il établisse une connexion chiffrée SSL. Si vous avez sélectionné un MID Server, ce champ n'est pas disponible. Si vous utilisez une intégration LDAPS et que le port SSL par défaut est 636, aucune configuration supplémentaire 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 se trouve au sein d'un réseau interne, le pare-feu transfère (ou NAT) l'adresse IP du serveur d'applications à travers 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 des demandes de recherche persistantes. En outre, si vous avez sélectionné un MID Server, la fonctionnalité d'écouteur est

Champ	Description
	disponible pour ce MID Server. Consultez Activer un écouteur LDAP et définir les propriétés système pour plus d'informations.
Intervalle d'écoute (valeur du délai d'expiration)	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 une fois que la connexion a dépassé l'intervalle d'écoute.
Pagination	Cochez cette case pour que le serveur LDAP divise les données d'attribut 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 ou l'intégration ne peut pas se lier au serveur LDAP.

Résultats

Lorsqu'un enregistrement de serveur LDAP est défini sur actif, le système teste automatiquement chaque connexion pour la valider.
Les validations comprennent :

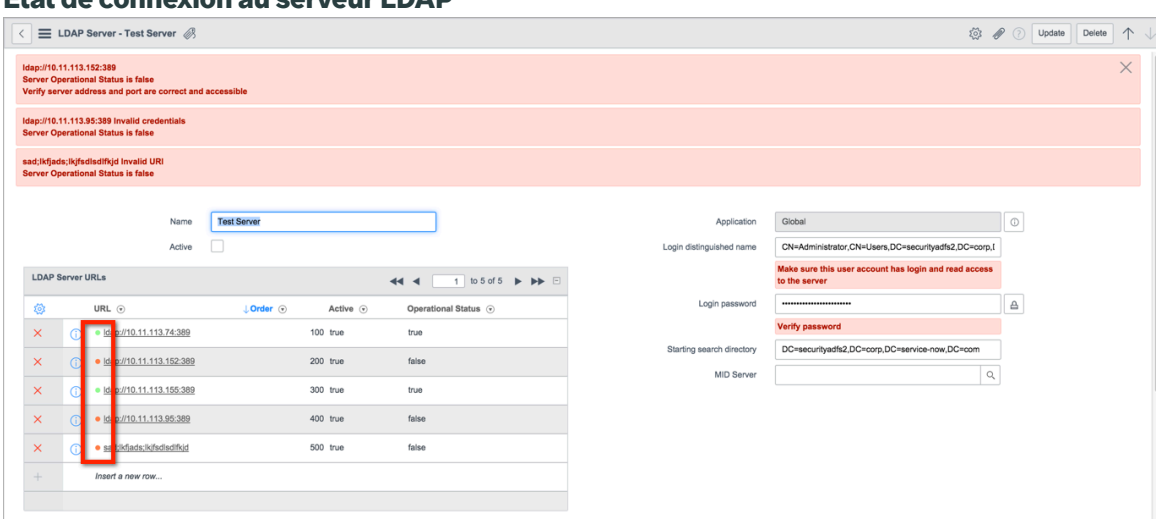
- Le serveur LDAP est accessible via l'URL et le port fournis
- L'URL du serveur LDAP est correctement formatée
- Les informations d'identification de connexion sont valides

À partir de la version Fuji, le système affiche des points de couleur 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 pas 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 option est activée, un écouteur informe le système pour qu'il traite les enregistrements LDAP peu de temps après une mise à jour sur le serveur LDAP.

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 des demandes de recherche persistante (avec OID 2.16.840.1.113730.3.4.3).

Si le serveur LDAP prend en charge une recherche persistante, l'écouteur LDAP reconnaît tous les changements d'utilisateur et de groupe apportés à l'un des comptes LDAP applicables et les transmet à votre instance dans un délai d'environ 10 secondes. Cela permet à l'instance d'avoir une copie presque en temps 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 sur les tables Utilisateur [sys_users] et Groupe [sys_user_group].

Remarque :
Si un utilisateur est ajouté via l'écouteur, mais que l'utilisateur ne remplit pas les conditions définies par le filtre d'unité organisationnelle, 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 OU. Les enregistrements utilisateur entrants qui ne répondent pas aux exigences de filtre 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 OU.

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 démarre en tant que transaction d'arrière-plan. En exécutant l'écouteur LDAP en tant que transaction d'ar plan, la règle de quota Transaction de démarrage/arrêt de l'écouteur LDA

Traduction automatique

Propriété	Description
	annuler la transaction une fois la durée maximale atteinte, soit 5 minutes p défaut. Ce comportement empêche un écouteur LDAP d'attendre indéfini **Remarque :** Cette propriété s'applique uniquement aux connexions LDAP qui n'utilisent pas de MID Server. Utilisez cette propriété `glide.ldap.listener.mid.use_background_transac` pour contrôler le comportement des connexions LDAP qui passent pa MID Server. ○ Type : true | false ○ Valeur par défaut : false ○ Emplacement : ajouter à la table Propriétés système [sys_properties]
glide.ldap.listener.mid.use_background_transaction	Si la valeur est « vrai », l'écouteur LDAP démarre en tant que transaction d'arrière-plan. En exécutant l'écouteur LDAP en tant que transaction en a plan, la règle de quota Démarrer/Arrêter la transaction MID de l'écouteur peut annuler la transaction une fois la durée maximale atteinte, soit 5 minu défaut. Ce comportement empêche un écouteur LDAP d'attendre indéfini **Remarque :** Cette propriété s'applique uniquement aux connexions LDAP qui utilisent un MID Server. Utilisez cette propriété `glide.ldap.listener.use_background_transaction` contrôler le comportement des connexions LDAP qui ne passent pas un MID Server. ○ Type : true | false ○ Valeur par défaut : false ○ Emplacement : ajouter à la table Propriétés système [sys_properties]
glide.ldap.listener.mid.un_écouteur	Si la valeur est vraie, un seul message de file d'attente ECC est créé pour démarrer ou arrêter l'écouteur LDAP via un MID Server. Si la valeur est f plusieurs messages de file d'attente ECC peuvent être créés, ce qui entraîn création de plusieurs threads pour démarrer ou arrêter l'écouteur LDAP. ○ Type : true | false ○ Valeur par défaut : true ○ Emplacement : ajouter à la table Propriétés système [sys_properties]

Spécifier les attributs LDAP

Spécifiez les attributs inclus dans les requêtes du 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

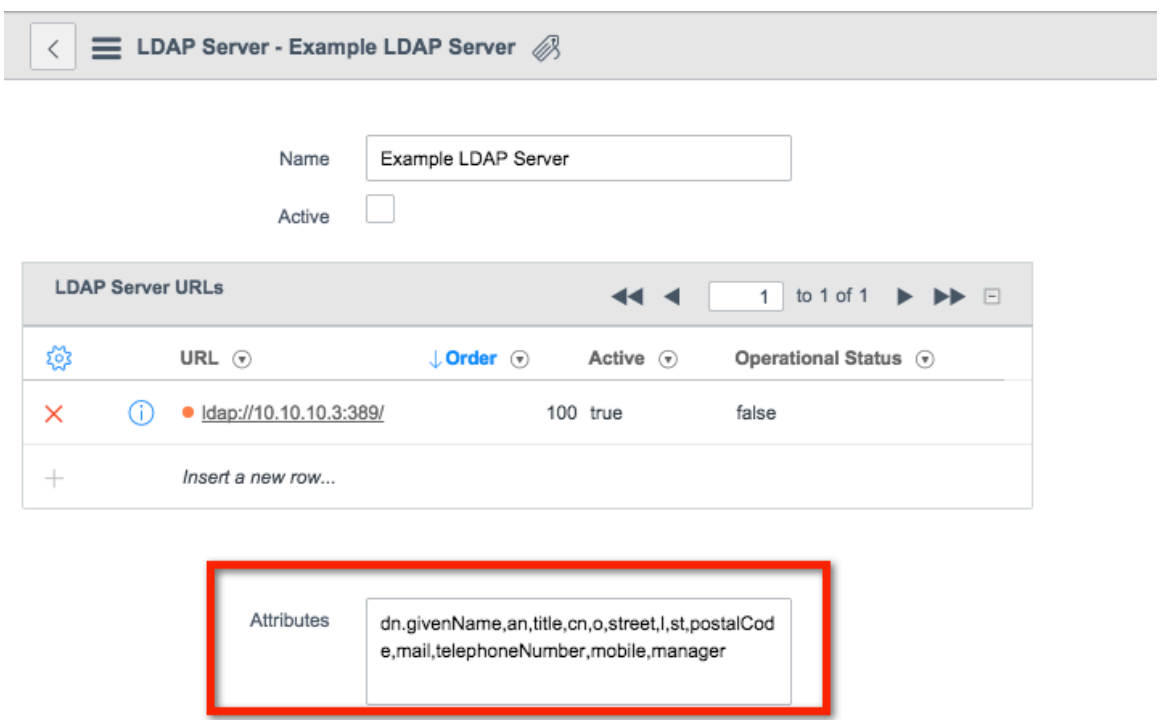
Par défaut, le système charge tous les attributs pour chaque objet qu'il est autorisé à lire à partir de votre serveur LDAP. À l'aide du champ **Attributs** , vous pouvez spécifier et ainsi limiter les attributs renvoyés par la requête LDAP. L'utilisation de cette approche pour les importations LDAP importantes peut améliorer considérablement la vitesse de ces importations.

Procédure

Définissez explicitement les attributs lorsque cela est possible.

S'il existe des informations que vous ne souhaitez pas exposer à l'instance, excluez l'attribut. Si vous ne spécifiez pas d'attributs de serveur LDAP, les transactions utilisateur peuvent être bloquées 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 **dn** (nom unique) dans le champ **Attributs** . Aucun des deux attributs ne doit 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 de 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.

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 **Tester la connexion**.
4. Sous **Liens connexes**, cliquez sur **Parcourir** pour vérifier que la structure du répertoire LDAP appropriée est visible par 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 **RDN** 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 **inactive**, la valeur **d'état opérationnel** passe automatiquement à **actif**. Cette fonctionnalité est prise en charge pour les tests de connexion automatiques et manuels.
- S'il s'avère impossible d'établir une connexion à un serveur dont la valeur **État opérationnel** est **active**, la valeur **État opérationnel** bascule automatiquement sur **Inactif**. 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 d'organisation (OU) spécifie les répertoires sources LDAP disponibles pour l'intégration.

Avant de commencer
Rôle requis : admin.

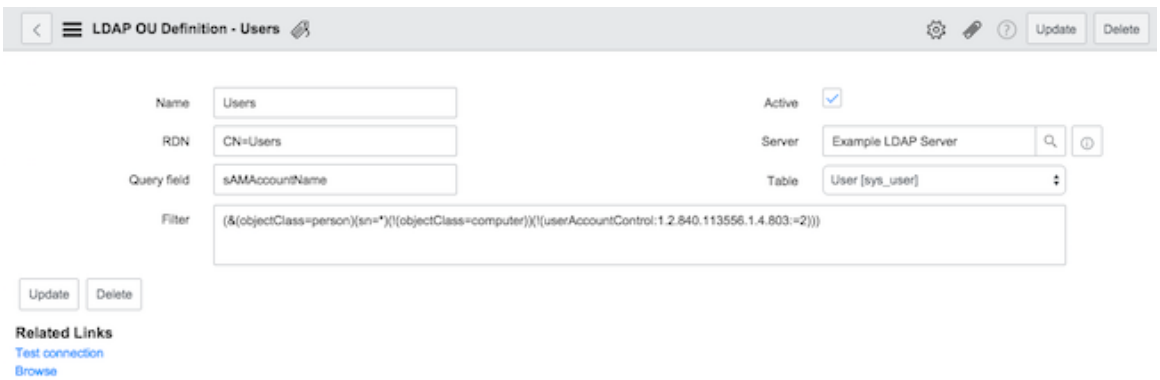
Pourquoi et quand exécuter cette tâche
Les définitions d'unités organisationnelles peuvent contenir des emplacements, des personnes ou des groupes d'utilisateurs. Chaque définition de serveur LDAP contient deux exemples de définitions d'unités organisationnelles : l'une pour l'importation de groupes 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 la définition d'exemple d'unité organisationnelle pour **les groupes** ou les **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 du répertoire LDAP que renvoie la définition d'OU.



Formulaire de définition d'unité organisationnelle

Champ	Description
Nom	Spécifiez le nom que l'intégration utilise lorsqu'elle fait référence à cette unité organisationnelle. Le nom que vous saisissez 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 RDN est combiné avec le répertoire de début de recherche de la définition du serveur LDAP afin d'identifier le sous-répertoire contenant des informations pour cette unité organisationnelle. Par exemple, l'exemple de définition d'OU utilise la valeur RDN `CN=Users` pour rechercher le répertoire LDAP `CN=Users,DC=service-now,DC=com` et tout répertoire en dessous de ce point. Ce champ doit correspondre à un sous-répertoire de 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 façon 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 exister un enregistrement utilisateur avec la valeur **d'ID d'utilisateurjoe.example** et un enregistrement LDAP avec la valeur **sAMAccountNamejoe.example**.
Actif	Cochez cette case pour activer la définition d'unité organisationnelle et permettre aux administrateurs de tester l'importation de données. Toutefois, l'intégration ne peut apporter des données dans le système qu'à partir de définitions d'unités organisationnelles 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	Entrez une chaîne de filtre LDAP pour sélectionner des enregistrements spécifiques à importer à partir de l'OU. Plus la requête de filtre LDAP est spécifique, plus elle est efficace.

Champ	Description
	Par exemple, la définition d'UO LDAP d'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 : (&(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 sur Internet la RFC des filtres LDAP.

Example: Exemples de définitions d'unités organisationnelles

Supposons que vous disposiez d'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 en outre que vous souhaitiez exclure le groupe RH et les utilisateurs RH de l'application. Effectuez les actions suivantes :

1. Créez un enregistrement de serveur LDAP avec un répertoire de recherche de départ dc=mon-domaine,dc=com.
2. Créez un enregistrement de définition OU pour ou=Groups avec un filtre pour exclure cn=HR.
3. Créez un enregistrement de définition OU pour ou=Users avec un filtre excluant ou=HR.

Si vous ne spécifiez pas d'attributs ou de filtres supplémentaires avec une définition d'OU, la requête LDAP renvoie la sous-arborescence complète du répertoire de départ et du RDN.

Dans ces exemples, une définition OU avec la valeur RDN ou=Groups et sans filtre aurait renvoyé tous les groupes. De même, une définition OU avec la valeur RDN ou=Users et sans filtre aurait renvoyé tous les utilisateurs et les unités organisationnelles enfants.

Créer une source de données pour LDAP

Chaque définition d'unité organisationnelle (OU) LDAP possède sa propre liste connexe de sources de données.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Remarque :
Le **serveur LDAP** et la **définition LDAP OU** doivent être actifs pour que l'action de test de chargement fonctionne correctement. Lorsque la charge de test est activée 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 de 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. N'oubliez pas que les 20 enregistrements chargés ne peuvent pas être transformés et ne sont utilisés qu'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 de champ de l'ID d'utilisateur le plus long dans les enregistrements de test.

Pour créer une 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 LDAP OU** , sélectionnez un élément, tel que **Groupes** ou **Utilisateurs**.
4. Cliquez sur **Nouveau** dans la liste connexe **Sources de données**.
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 vérifier 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'il fait référence à cette source de données.
Nom de la table des jeux d'importation	Entrez le nom de la table intermédiaire dans laquelle le système place temporairement les enregistrements et attributs LDAP importés. Passez en revue cette table pour afficher les enregistrements LDAP importés. Vous pouvez utiliser le même nom de table de jeux 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 LDAP OU associée à cette source de données.

Approvisionnement automatique des utilisateurs LDAP

Vous provisionnez automatiquement les utilisateurs qui se trouvent dans le serveur LDAP, mais pas encore dans votre instance.

Avant de commencer
Rôle requis : admin

Procédure

Créez les propriétés suivantes dans la table Propriétés système [sys_properties] :

Propriétés LDAP

Propriété LDAP	Description
glide.ldap.authentication	Active l'authentification LDAP à l'aide de LDAP pour authentifier les utilisateurs. Définissez cette propriété sur **true** (valeur par défaut).
glide.ldap.user.autoprovision	Permet à LDAP 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 **true** (valeur par défaut).

Ces deux propriétés doivent être définies sur **vrai** pour que la mise en service automatique fonctionne.

Intégration LDAP via MID Server

Les administrateurs peuvent réaliser l'intégration à l'aide d'une source de données LDAP sur un MID (Management, Instrumentation, and Discovery).

Le MID Server permet la communication et le mouvement des données entre le et des Now Platform applications, des sources de données et des services externes. Pour en savoir plus sur l'installation d'un MID Server, consultez la rubrique Installation d'un MID Server .

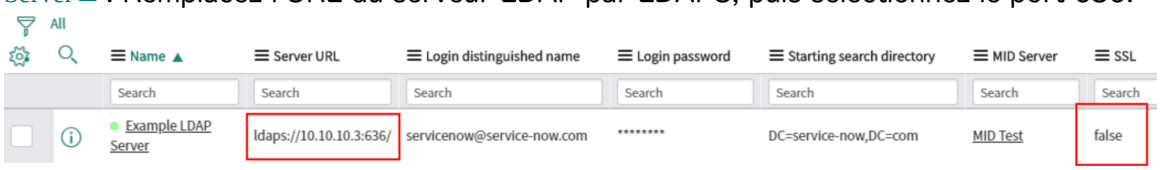
L'utilisation d'un MID Server pour établir une connexion LDAP vous évite d'avoir à exposer le serveur LDAP au trafic réseau externe. Il n'est plus nécessaire d'établir un tunnel VPN entre votre serveur LDAP et les centres de données. L'utilisateur du MID Server doit avoir le rôle user_admin pour pouvoir lire les enregistrements de configuration du serveur LDAP.

Remarque :
Le MID Server n'autorise pas l'utilisation de l'action d'interface utilisateur `<instance>/sys_ui_action.do ?sys_id=1b4f7ef30a0001060058e223c9a5744c` pour actualiser les enregistrements d'utilisateurs et de groupes à partir de LDAP.

Par défaut, une connexion MID Server communique via HTTP sur le port 80. Ce canal de communication ne nécessite pas de certificat. La connexion entre le MID Server 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 via Internet ou via un tunnel VPN.

Remarque :
LDAP ne peut pas communiquer via le MID Server avec l'authentification par mot de passe.

Pour une communication sécurisée via SSL, vous devez ajouter un certificat SSL pour le MID Server . Remplacez l'URL du serveur LDAP par LDAPS, puis sélectionnez le port 636.



Remarque :
Si vous créez un nouveau serveur LDAP, le marqueur SSL du MID Server est défini par défaut sur false. Vous pouvez ignorer ce comportement.

Pour définir les propriétés de connexion d'un serveur LDAP spécifique, reportez-vous à la section Définir un serveur LDAP.

Traduction automatique

Configurer la surveillance des connexions LDAP

Modifiez ou désactivez la surveillance et les notifications de connexion LDAP.

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 de la connexion d'un serveur LDAP. Elle utilise la notification par e-mail , qui est lancée par la tâche planifiée de **test de la connexion LDAP**. Cette notification par e-mail est activée par défaut.

Remarque :
L'instance n'envoie pas la notification par e-mail à moins qu'il n'y ait au moins un membre dans le groupe d'administrateurs LDAP. Assurez-vous de renseigner ce groupe avec les utilisateurs auxquels vous souhaitez envoyer 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 MID Server

En tant qu'administrateur, vous pouvez importer des données d'objets volumineux (BLOB) binaires 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 le `glide.ldap.binary_attributes` des propriétés système.
2. Ajoutez une propriété de MID Server 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 MID Server

Vous pouvez rencontrer des problèmes dans les domaines suivants lors de l'intégration de LDAP via MID Server.

Vous pouvez résoudre ces problèmes en affichant les sorties trouvées dans la file d'attente ECC (External Communication Channel) (**Détection** > **Résultats et artefacts** > **File d'attente ECC**).

Tester les problèmes de connexion

Lors de la définition des unités organisationnelles dans le 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 MID Server, 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 affiche **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 d'unités organisationnelles dans le serveur, une liste connexe **Parcourir** permet d'afficher les enregistrements du répertoire LDAP que renvoie la définition d'unité organisationnelle. 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 que les données ont été renvoyées à partir du MID Server, 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 affiche **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.

Charger les problèmes 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 le nom de rubrique **LDAPProbe**.

Une fois que les données ont été renvoyées à partir du MID Server, 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.

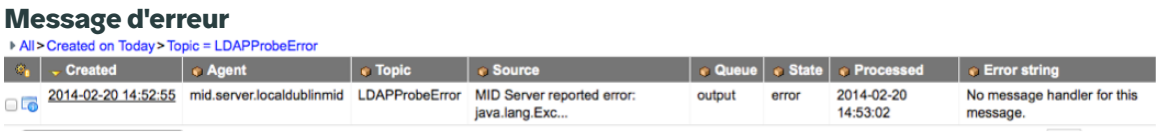
Des messages d'entrée supplémentaires, également nommés **LDAPProbe**, s'affichent. La colonne **Nom** de ce message d'entrée affiche le numéro d'enregistrement le plus élevé du lot. Si le nombre total d'enregistrements retournés est de 258 et que la taille du lot est de 200 (la valeur par défaut), deux 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**.



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 la pagination sur le serveur LDAP est inférieure à 1 000. Définissez la propriété `glide.ldap.max_results` du MID Server sur une valeur inférieure ou égale à la taille de pagination du serveur LDAP.

LDAP échoue dans l'importation 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`du MID Server . Pour l'exemple de photo d'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 avec les champs de votre instance.

Remarque :
Dans la mesure où le mappage LDAP a un effet sur les performances, il est recommandé de le planifier pendant les heures creuses 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.

Le moyen le plus simple de savoir si vous exécutez ou non une version qui utilise l'application système LDAP pour l'intégration LDAP consiste à rechercher l'application à partir du navigateur d'application.

L'option **Exécuter les règles métier** n'est appliquée que pour 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 groupes d'utilisateurs, le groupe doit avoir des rôles définis.

Options de mappage d'importation LDAP

Application LDAP système ?	Carte
Oui	Utilisez une *carte de transformation* pour spécifier votre mappage.
Non	Utilisez un *mappage d'importation LDAP hérité* pour spécifier votre mappage, ou la transformation LDAP par défaut qui est incluse dans les instances de base de référence. N'oubliez pas d'ajuster le champ de **fusion** pour qu'il corresponde aux champs corrects.

Importations planifiées

Une importation planifiée permet aux administrateurs d'importer des données LDAP à intervalles réguliers. Par défaut, l'intégration LDAP comprend deux exemples d'importations planifiées :

- 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 société.

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 standard et des cartes de transformation. Vous pouvez également créer des cartes de transformation LDAP personnalisées.

Important :
Que vous sélectionniez ou que vous créiez des cartes de transformation LDAP personnalisées, il doit y avoir une carte de transformation 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 des 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 utilisateur à partir d'informations d'identification LDAP dans le cadre d'une connexion LDAP à la demande. Contient les mappages d'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'UO LDAP. Contient les mappages d'un serveur LDAP Active Directory.

Remarque :
Par défaut, le système ne dispose pas d'une carte de transformation pour les enregistrements du 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 du groupe importé. Le système utilise ce champ pour déterminer si un utilisateur a besoin d'une authentification LDAP, pour trouver le responsable de l'utilisateur et pour placer les utilisateurs dans des groupes.
ldap_import	Sélectionnez 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

Lorsque vous spécifiez 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 tel que « gestionnaire » est le nom unique (ND) du gestionnaire.

Sans logique supplémentaire, vous pouvez créer 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 utilisateur 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 dispose d'un champ **Carte** qui fait référence au mappage d'importation hérité.

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, désactivez la référence à la carte d'importation héritée.

Paramètres du 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 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 l'importation d'utilisateurs LDAP), l'intégration utilise les mappages par défaut suivants :

Mappage par défaut de l'importation LDAP

Champ ou variable d'utilisateur	Attribut LDAP
user_name	Samaccountname
e-mail	Courrier
Téléphone	numéro de téléphone
home_phone	Téléphone à domicile
mobile_phone	mobile
first_name	givenName
last_name	Sn
Titre	Titre
department	department
responsable	responsable
middle_name	Initiales
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 relie un attribut LDAP importé à un champ approprié dans la table cible (Utilisateur ou Groupe). Par exemple, les données témoins de l'attribut sAMAccountName sont mappées au champ **ID d'utilisateur** dans la table Utilisateur.

Si les données LDAP importées sont mappées à un champ de référence, l'instance recherche un enregistrement correspondant. Si aucun enregistrement correspondant n'existe, l'instance crée un nouvel enregistrement pour le champ de référence, sauf indication contraire du mappage de champ.

Par exemple, supposons que l'attribut LDAP l soit mappé au champ de référence **Emplacement** dans 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 de l'utilisateur importé a maintenant un lien vers le nouvel enregistrement d'emplacement.

Toutefois, il arrive que l'attribut LDAP renvoie un nom distinctif (DN), qui est essentiellement une référence à un autre enregistrement dans le répertoire LDAP. Par exemple, l'attribut gestionnaire contient généralement le nom unique du gestionnaire de l'entrée actuelle du répertoire LDAP. 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, qui peut ne pas être assez longue pour certaines valeurs DN. Le ServiceNow système tronque toute valeur qui dépasse la longueur du champ.

Les administrateurs ne souhaitent généralement pas que le système crée de nouveaux utilisateurs à partir de la valeur DN, car le nouvel utilisateur n'est pas associé à un utilisateur existant. Au lieu de cela, les administrateurs veulent que l'importation localise l'enregistrement utilisateur existant du gestionnaire et l'associe à l'utilisateur nouvellement importé. Le script include LDAPUtils contient les fonctions setManager et processManagers qui peuvent analyser un DN et 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 de l'utilisateur du gestionnaire associé. Pour gérer de tels tickets, vous pouvez appeler la fonction processManagers une fois la transformation terminée. Par exemple, la carte de transformation **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 fonctions setManager et processManagers si votre intégration LDAP n'utilise pas l'attribut manager.

Scripting 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 des scripts de transformation onStart et onAfter .

Le script onStart doit appeler le script include LDAPUtils et démarrer la journalisation. Par exemple, la carte de transformation **Importation d'utilisateur LDAP** a un script onStart qui utilise le code suivant :

```
gs.include ( "LDAPUtils" ) ; var ldapUtils  = new LDAPUtils ( ) ;
ldapUtils. setLog (log ) ;
```

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 les 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 d'utilisateurs si le **contrôle de compte d'utilisateur** signifie un compte AD désactivé.

Utilisez le script suivant pour désactiver automatiquement les utilisateurs lorsque l'utilisateur AD associé est désactivé.

Procédure

1. Configurez le formulaire Utilisateur et créez un champ de nombre entier appelé **Contrôle de compte d'utilisateur**.
2. Ajoutez le mappage de userAccountControl (externe) au nouveau champ.
3. Créez une règle métier avec les propriétés suivantes :

Règle métier Désactiver les 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.company, créez une carte de champ pour le champ de société et ajoutez un script de transformation des types suivants :

```
company = "Don's Sporting Goods";
```

Exclure certains utilisateurs LDAP

Si vous ne pouvez pas filtrer complètement la liste des utilisateurs LDAP à l'aide des propriétés de filtre LDAP, vous pouvez exclure des utilisateurs à l'aide d'un script de carte.

Une fois que vous avez 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 se trouvent pas dans une UO d'utilisateurs. Vous pouvez utiliser ce script si vous avez trop d'UO d'utilisateurs à inclure dans l'option LDAP d'UO 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 de jeux d'importation sont mappés aux champs dans des 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'il existe un nouvel enregistrement dans les données LDAP. Si la carte de transformation LDAP met à jour un champ de référence stockant les données d'une autre table, l'administrateur peut choisir de créer, ignorer ou rejeter de nouveaux enregistrements LDAP.
Par exemple, si l'intégration reçoit un nouvel enregistrement de département qui ne correspond à aucun département existant, vous souhaiterez peut-être 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 aucun enregistrement correspondant n'existe.
   - **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'ensemble de l'enregistrement.

Remarque :
La carte de champs affiche uniquement le champ **d'action 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 préliminaires

- Si le 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 qu'en cas de panne du LDAP, les administrateurs puissent toujours accéder à l'instance.
- Vérifiez le compte de service pour vous assurer qu'il n'a pas expiré ou qu'il n'est pas 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 system_id sur l'enregistrement ldap_server_config . Si vous modifiez la system_id par inadvertance avec un ensemble de mises à jour, system_id pointe vers le mauvais nœud pour l'instance cible et ne fonctionne pas.

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, reportez-vous à la section Codes d'erreur LDAP.

Intégration de plusieurs domaines

Vous pouvez intégrer plusieurs domaines au sein d'une même forêt ou dans des domaines 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. L'utilisation de plusieurs forêts AD via LDAP avec un seul compte LDAP n'est pas prise en charge.

Lorsque vous étendez à plusieurs domaines, il est essentiel d'identifier des attributs LDAP uniques pour les noms d'utilisateur d'application et d'importer des valeurs de fusion. Un attribut de coalescence 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 communs sont e-mail ou userPrincipalName.

Enregistrements entrants

Voir Cartes de transformation LDAP pour définir comment l'intégration traite les enregistrements LDAP entrants pour lesquels il manque des 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 automatiques de connexion LDAP

Vous pouvez tester manuellement les connexions aux serveurs LDAP ou autoriser ServiceNow à tester automatiquement les 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 toutes les 15 minutes par défaut.

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 unique relance le test de connexion après cinq minutes ou la moitié de la valeur **Intervalle de répétition** de la tâche planifiée, selon la première éventualité.

En cas de problème de connexion au serveur LDAP, des messages d'erreur s'affichent sur le formulaire. Les connexions de test pour les serveurs derrière un MID Server sont également prises en charge.

Afficher le moniteur LDAP

Vous pouvez afficher les informations actuelles sur les serveurs et écouteurs LDAP 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...)

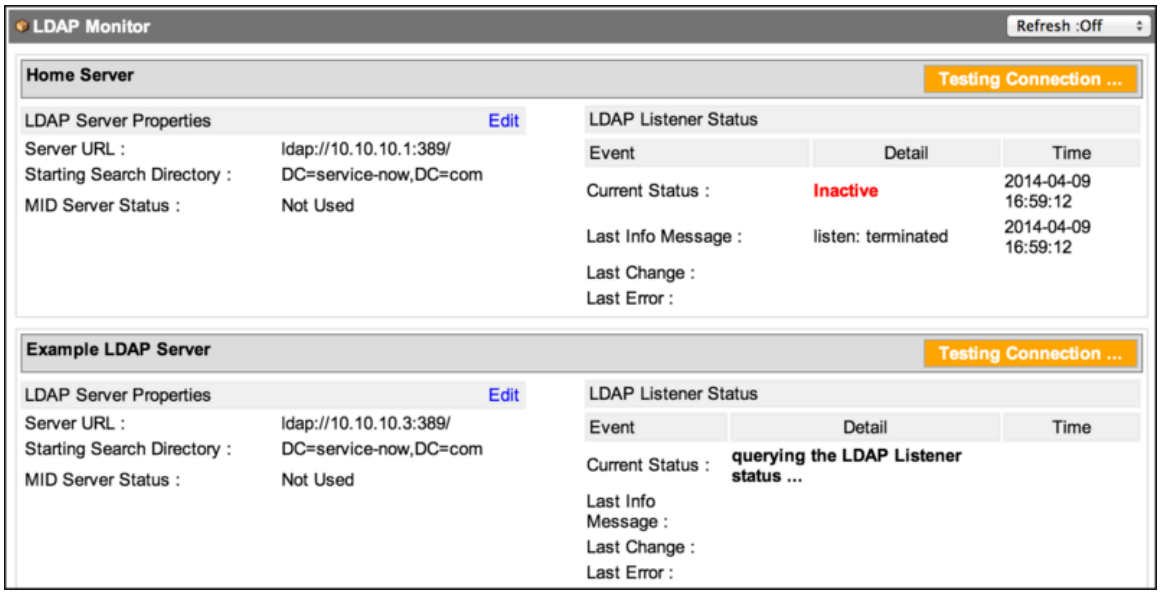
En plus de son état actuel, le moniteur affiche également :

- Dernier message détecté par l'écouteur, par exemple en attente de modifications 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 les descriptions des propriétés et des champs à l'écran.

Surveillance LDAP

Champ	Description
Actualiser	Vous pouvez configurer le taux de rafraîchissement en cliquant sur le champ **Actualiser** dans la barre d'en-tête du 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 case est verte et affiche *Connecté*. Lorsque le serveur n'est pas connecté, la case est rouge et affiche *Non connecté*. Lorsque la connexion au serveur est en cours de test, la zone est jaune et affiche *Test de la connexion*.
Propriétés du serveur LDAP	
Modifier	Lorsque vous surveillez les 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 sur lequel le serveur LDAP écoute. Souvent, le port est défini sur l'une des valeurs suivantes : • 389 : le port par défaut pour la connexion à LDAP en texte clair • 636 : le port standard pour la connexion 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 est 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.

Champ	Description
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 MID Server.
État de l'écouteur LDAP	
État actuel	Cela indique si l'écouteur est actif.
Dernier message d'informations	Il affiche le dernier message reçu par le serveur LDAP concernant les modifications d'utilisateur et de groupe, ainsi que l'heure de réception du message.
Dernier changement	Affiche la dernière modification apportée au serveur LDAP et l'heure à laquelle elle a été effectuée.
Dernière erreur	Affiche la dernière erreur qui s'est produite sur le serveur LDAP et l'heure à laquelle elle s'est produite.

Codes d'erreur LDAP

Le fichier journal LDAP répertorie les codes d'erreur standard du secteur 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 du 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.

Erreurs LDAP standard (suite)

Code d'erreur / de données	Texte	Description
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, pendant une opération de liaison, le client a demandé une méthode d'authentification non prise en charge par le serveur LDAP.
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		Réservés au.
10	LDAP_REFERRAL	N'indique pas une condition d'erreur. Dans LDAPv3, indique que le serveur ne détient pas l'entrée cible de la requête, mais que les serveurs dans le champ de référence le peuvent.
11	LDAP_ADMINLIMIT_EXCEEDED	Indique qu'une limite de serveur LDAP définie par une autorité administrative a été dépassée.
12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION	Indique que le serveur LDAP n'a pas pu satisfaire une demande car une ou plusieurs extensions critiques n'étaient pas disponibles. Soit le serveur ne prend pas en charge le contrôle, soit 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

Erreurs LDAP standard (suite)

Code d'erreur / de données	Texte	Description
		envoyer au serveur le même mécanisme SASL pour poursuivre 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 DN de modification, d'ajout ou de modification enfreint les contraintes placées sur l'attribut. La contrainte peut concerner la taille ou le contenu (chaîne uniquement, aucun 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.
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 : Opérations de recherche qui trouvent la base de recherche, mais ne trouvent aucune entrée qui correspond au filtre de recherche. Lier les opérations.
33	LDAP_ALIAS_PROBLEM	Indique qu'une erreur s'est produite lors du déréférencement d'un alias.
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 ne permettent pas

Erreurs LDAP standard (suite)

Code d'erreur / de données	Texte	Description
		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 terminale. (Ce code n'est pas actuellement dans les spécifications LDAP, mais est réservé à cette constante.)
36	LDAP_ALIAS_DEREF_PROBLEM	Indique que lors d'une opération de recherche, soit le client ne dispose pas des droits d'accès pour lire le nom de l'objet aliasé, soit 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 des éléments suivants est à l'origine de cette erreur : le client renvoie des informations d'identification simples lorsque des informations d'identification solides sont requises... OU... Le client renvoie un DN 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 que l'une des situations suivantes s'est produite au cours d'une opération de liaison : le client a transmis un DN ou un mot de passe incorrect, ou le mot de passe est incorrect car il a expiré, la détection d'intrusion a verrouillé le compte ou une autre raison similaire. Consultez le code de données pour plus d'informations.
49 / 52e	AD_INVALID 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.

Erreurs LDAP standard (suite)

Code d'erreur / de données	Texte	Description
49 / 530	NOT_PERMITTED_TO_LOGON_AT_THIS_TIME	Indique une erreur de données Active Directory (AD) AcceptSecurityContext qui est un échec de connexion causé par le fait que l'utilisateur n'est pas autorisé à se connecter pour le moment. Renvoie uniquement lorsqu'un nom d'utilisateur et des informations d'identification valides lui sont présentés.
49 / 531	RESTRICTED_TO_SPECIFIC_MACHINES	Indique une erreur de données Active Directory (AD) AcceptSecurityContext qui est un échec de connexion causé par le 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 valides lui 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 des informations d'identification valides lui 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 des informations d'identification valides lui sont présentés.
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 lié à l'objet/compte utilisateur LDAP spécifique qui doit être examiné 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 des informations d'identification valides lui sont présentés.
49 / 773	L'UTILISATEUR DOIT RÉINITIALISER LE MOT DE PASSE	Indique une erreur de données Active Directory (AD) AcceptSecurityContext.

Erreurs LDAP standard (suite)

Code d'erreur / de données	Texte	Description
		Le mot de passe de l'utilisateur doit être modifié avant la première connexion. Renvoie uniquement lorsqu'un nom d'utilisateur et des informations d'identification de mot de passe valides lui 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 du 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 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 règles de structure du serveur... OU... La demande de modification d'attribut spécifie des attributs que les utilisateurs ne peuvent pas modifier... OU... Les 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

Erreurs LDAP standard (suite)

Code d'erreur / de données	Texte	Description
		structure du schéma. Par exemple, la demande subordonne l'entrée à un alias. La requête subordonne l'entrée à un conteneur interdit par les règles de confinement. Le RDN pour l'entrée utilise un type d'attribut interdit.
65	LDAP_OBJECT_CLASS_VIOLATION	Indique que l'opération d'ajout, de modification ou de modification 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 terminales. 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 distinctif relatif de l'entrée.
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 Modifier DN déplace l'entrée d'un serveur LDAP à un autre et nécessite 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

Erreurs LDAP standard (suite)

Code d'erreur / de données	Texte	Description
		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 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
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 indisponible

Une propriété LDAP est disponible pour 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, l'utilisateur doit avoir activé les notifications sur son profil d'utilisateur. La notification est un message électronique uniquement. Les 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 de l'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 de définir des indicateurs de données cohérents pour chaque objet utilisateur, d'importer des données LDAP et d'évaluer les 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 entrent dans l'instance via des tables de jeu d'importation où les données peuvent être évaluées et traitées.

Le processus d'importation peut être utilisé Filtres d'actualisation LDAPsur plusieurs tâches d'importation afin de diviser différents types d'enregistrements utilisateur et de séparer les enregistrements pour un traitement distinct.

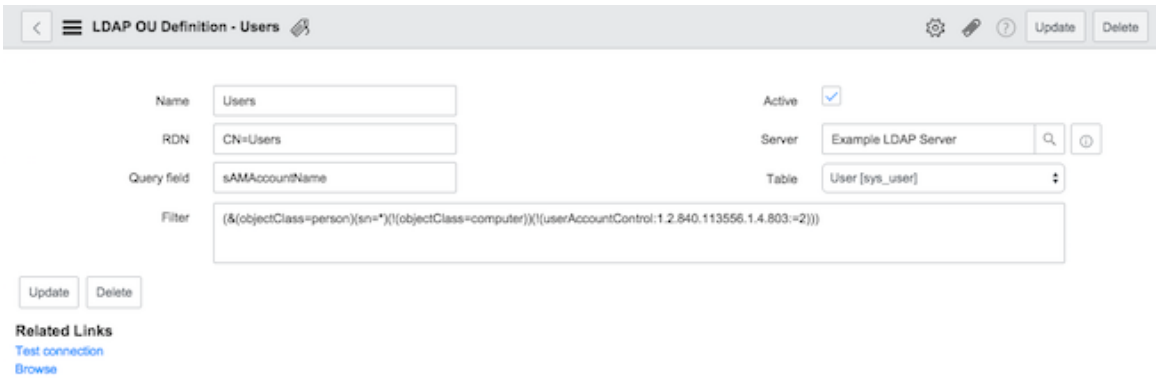
Filtres d'actualisation LDAP

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 transférer toutes les données dans votre table de jeux d'importation (y compris les utilisateurs inactifs), puis spécifier un traitement qui ignore les insertions d'utilisateurs désactivés. L'exemple de définition d'unité organisationnelle « Utilisateurs » que l'instance fournit dans son exemple LDAP prêt à l'emploi contient un filtre.

Ce filtre est important car il définit les enregistrements utilisateur qui sont importés dans la table de jeux d'importation à évaluer. Bien qu'il réduise 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 des utilisateurs inactifs ne sont pas visibles, il est impossible 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. Tous les enregistrements seront alors chargés dans la table temporaire de 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 pouvez 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 désactivé.

Extraction LDAP

Un processus d'extraction LDAP peut être implémenté pour détecter les utilisateurs handicapés.

Un extrait de votre source LDAP peut être filtré pour les utilisateurs désactivés à l'aide d'un marqueur actif qui peut être défini sur « faux » pour chaque enregistrement de l'importation. Spécifiez ('target.active=false') et copiez-la directement dans le champ **Script** sur l'enregistrement Carte de transformation de table.

Avantages

Les avantages de cette méthode sont les suivants :

- Écriture de scripts simple
- Les enregistrements des utilisateurs 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 sont les suivants :

- Un processus supplémentaire est créé
- L'ensemble d'extraits doit être placé dans un emplacement auquel votre source de données peut accéder

Méthode alternative

Filtres d'actualisation LDAP Utilisez plusieurs tâches d'importation pour diviser différents types d'enregistrements utilisateur, en séparant les enregistrements pour un traitement distinct.

Comptes d'utilisateurs LDAP inactifs

Détectez qu'un compte d'utilisateur existant et actuel est inactif ou a été désactivé ou supprimé d'un LDAP Active Directory (AD).

Un problème courant d'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 n'ait pas connaissance des utilisateurs qui sont désactivés ou supprimés dans AD. Le problème est de savoir comment détecter qu'un utilisateur actuel existant est inactif ou a été supprimé d'AD.

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. La suppression d'un enregistrement détruit toutes les relations avec ces autres enregistrements. La désactivation des enregistrements maintient ces relations en place.

Rechercher les 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
L'une des méthodes 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 **userAccountControl** AD.
   Par exemple : `u_ad_user_account`.
2. Créez un script de transformation LDAP pour définir la valeur du champ.

   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'attribut 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 de l'attribut userAccountControl

Cet exemple examine l'attribut userAccountControl, mais ne teste pas certaines valeurs spécifiques. Il offre également la possibilité de réactiver les comptes 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
*/
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 ceux 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 de la flexibilité en ne s'appuyant pas sur les valeurs userAccountControl 546 et 514, mais en vérifiant plutôt 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;
}
```

Mode d'application Active Directory (ADAM)

Active Directory Application Mode (ADAM) est un service d'annuaire conforme au protocole LDAP (Lightweight Directory Access Protocol).

Remarque :
Un niveau de compréhension de base avec Microsoft Windows Server et Active Directory est nécessaire pour comprendre cette rubrique. Vous devez également disposer d'autorisations d'administrateur sur le serveur que vous configurez pour ADAM.

Il s'agit d'exemples de procédures. En raison des variations d'installation et d'environnement, nous ne pouvons pas offrir d'assistance directe. Nous vous recommandons de faire appel à un Microsoft consultant.

ADAM dispose d'une installation simple et s'exécute 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 dispose de 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 Server Windows 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). S'il est interdit d'exposer certains objets ou attributs AD à un fournisseur ou partenaire externe, l'accès aux objets et aux attributs peut être bloqué à l'aide des entrées de contrôle d'accès de sécurité AD (ACE ou ACL). En fonction des 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 LDAP et les authentifications 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 Light-Weight-Directory Service, LDS. L'installation et la configuration sont similaires à celles de Windows Server 2003 R2.

Connaissances recommandées

Pour effectuer cette tâche, vous devez comprendre AD, les classes d'objets et les attributs. Pour réussir l'intégration, vous devez connaître la structure d'objet AD actuelle, les délégations Active Directory et disposer d'une stratégie sur la façon d'utiliser ADAM et à quelles fins. Si vous n'êtes pas familier avec AD ou ADAM, contactez votre administrateur AD pour configurer un nouvel environnement ADAM.

Fiducies

Si *les 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 *les objets userProxy* sont utilisés, l'ordinateur ADAM doit être en mesure de se connecter aux contrôleurs de domaine connexes pour effectuer une authentification par proxy.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Configurer une instance avec ADAM

La première installation copie les fichiers ADAM sur votre ordinateur, enregistre les composants requis et crée les raccourcis d'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.

- Windows Server 2003 R2 - ADAM peut être installé à l'aide de **Panneau de configuration > Ajouter et supprimer des programmes > Gestionnaire de composants optionnel**.
- Windows Server 2000 et Windows XP - Téléchargé http://www.microsoft.com/downloads à partir de Microsoft.

Créez le premier service d'instance qui fonctionne comme le premier service d'annuaire hébergé par ADAM. Effectuez l'une des actions suivantes :

Procédure

- Exécutez *adaminstall.exe* à partir du dossier ADAM.
- Utiliser le raccourci **Créer une instance ADAM** depuis le **Menu Démarrer > programmes > ADAM** Dossier.

1. Sélectionnez l'option **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 de service et le Windows nom d'affichage
Ports	définit les numéros de port à utiliser pour LDAP et les écouteurs LDAPS. Le port LDAP par défaut est 389, LDAPS est 636. Si ces ports sont utilisés sur le serveur, l'assistant d'installation 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. Non 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 remplacez le domaine de plus haut niveau 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 des 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 réplicas, vous devez utiliser un compte qui a accès à toutes les instances ADAM.
Administrateurs ADAM	la délégation sur l'annuaire ADAM qui exploite l'authentification intégrée de Windows. C'est ainsi que l'accès initial est accordé pour l'administration. Une fois les droits accordés au compte initial, cet utilisateur ou groupe délègue les 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.
Importer des fichiers LDIF	Fichiers à importer. MS-UserProxy est le fichier le plus important à importer, mais il 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

L'essentiel de l'administration générale s'effectue à l'aide de la console ADAM ADSI MMC disponible dans le menu Démarrer **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 **ADAM ADSI Edit** 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 d'affectation de nom** 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 à l'intérieur de la partition et des conteneurs par défaut pour LostAndFound, les quotas NTDS et les rôles. Le conteneur de 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 de façon logique les objets stockés dans ADAM dans des conteneurs et des unités d'organisation (OU), comme ils le seraient dans Active Directory.

Avant de commencer

Rôle requis : admin

Procédure

1. Cliquez avec le bouton droit sur la partition racine et accédez à **Nouveau** > **Objet** > **Unité d'organisation**.

   Remarque :
   Vous pouvez également afficher 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 entrer une valeur, entrez le nom de l'UO, par exemple 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 organisationnelles, les nouvelles unités organisationnelles 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 d'OU 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 ont déjà été 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.

Étant donné que 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 permet de s'assurer que les versions des outils sont correctes. DSALCS est utilisé pour afficher et définir les droits d'accès aux objets.

Exemple : « `dsacls \\localhost :50010\dc=myCompany,dc=adam` » affiche les permissions attribuées à la racine de la partition `dc=myCompany,dc=adam` s'exécutant sur le localhost, le port 50010. DSACLS est un outil complexe utilisé pour créer une délégation complexe. `Exécutez « DSACLS / ? »` pour les 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 incluent les objets utilisateur, l'objet UserProxy et les objets de groupe.

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 d'outils de ligne de commande AD, ce qui dépasse le cadre de ce document. Le seul attribut obligatoire pour les nouveaux objets 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 dans l'objet utilisateur.

Objets UserProxy

Pour ServiceNow l'intégration LDAP, nous vous recommandons d'utiliser `des objets UserProxy` dans ADAM, ce qui crée un compte proxy lié au compte d'utilisateur AD associé. ADAM peut ainsi authentifier les informations d'identification 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 les 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 en 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 ceux d'AD et sont utilisés pour intégrer des groupes et des membres à ServiceNow. La plus grande différence réside dans le fait que les groupes ADAM peuvent contenir des membres provenant d'ADAM ou de domaines AD approuvés.

Automatisation de la création d'objets ADAM

Si vous souhaitez synchroniser les 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 domaine et ont des droits sur les objets de la partition courante. De la même manière que pour les forêts AD, vous pouvez également définir un niveau d'autorisation 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 par 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, comme dans Active Directory. D'un point de vue transitif, 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

Test et dépannage de la configuration d'ADAM

L'outil principal utilisé pour le test est LDP. Cela vous permet de tester entièrement l'authentification utilisateur.

La plupart de la gestion des objets peut être effectuée à l'aide de la console ADAM ADSI Edit qui donnera accès à l'ensemble de la collection d'objets et d'attributs. Le plus haut niveau 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 qu'il puisse s'exécuter. 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. Il s'agit également d'un excellent outil pour le dépannage des services ADAM.

Le Windows journal des événements de sécurité est également utile lors du 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, ainsi qu'au résultat ou au code 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 système de fichiers standard.

Redondance

ADAM dispose d'utilitaires de réplication intégrés basés sur la même technologie qu'AD. Une réplique complète en lecture et en écriture d'une partition ADAM peut exister sur le même ordinateur ou sur un ordinateur différent. Vous pouvez utiliser ce réplica de diverses façons pour fournir une intégration LDAP tolérante aux pannes avec l'instance. Une option consiste à exposer les deux partitions à l'instance à travers le pare-feu et à définir les deux serveurs dans le champ serveur Propriétés LDAP.

Information associée

Mode d'application Active Directory (ADAM)

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 des communications LDAPS (LDAP sécurisées). LDAPS nécessite des certificats SSL pour sécuriser le trafic réseau.

Pour supprimer cette exigence, effectuez 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.

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 sur 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 d'infrastructure d'autorité de certification (CA). Si vous disposez déjà d'une autorité de certification, vous pouvez émettre un certificat. Sinon, créez un certificat autosigné.

Création d'un certificat autosigné

Pour utiliser l'utilitaire `selfssl` , Internet Information Services (IIS) doit être installé. Vous pouvez supprimer ce service 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 nouveau site Web afin que les sites actuels ne soient pas impactés lors de la génération de certificats. Selfssl doit joindre temporairement 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 courant 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
/C	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 devez obtenir l'ID de site 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 qui est valide pendant 10 ans. Définissez la valeur sur n'importe quelle durée, mais n'oubliez pas 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 n'importe quel client LDAP pour prendre en charge les liaisons sécurisées et chiffrer les informations d'utilisateur et de mot de passe transmises.

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 créer d'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 du service ADAM Certificats – Service (Nom de service ADAM)\ADAM_ADAM Nom de service\Certificats racine approuvés\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. Affectez 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 afin d'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 qui sera utilisée par les clients.

Procédure

1. Sélectionnez le certificat, cliquez avec le bouton droit de la souris et sélectionnez **toutes les tâches/ exportation**.
   N'exportez pas la clé privée. Sélectionnez le format binaire X.509 codé DER 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 *`d'autorités de certification racine approuvées`* .

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Compte d'accès en mode d'application Active Directory (ADAM)

Le système nécessite un compte d'utilisateur pour lire les informations d'objet du mode d'application Active Directory (ADAM) 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 affectez des autorisations.
- Affectez une autorisation à un Windows compte de domaine sur la partition ADAM.
- Utilisez un compte *`userProxy`* .

Lors de l'utilisation d'ADAM en tant que source LDAP, vous devez spécifier le nom unique entièrement qualifié (FQDN) du compte ADAM dans le champ **Nom unique de connexion** du serveur LDAP de l'instance.

Information associée

Mode d'application Active Directory (ADAM)

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 à la 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 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 affecté 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 client LDAP classiques, sélectionnez l'option Liaison simple. Saisissez un nom unique d'utilisateur ADAM ou `de userProxy` valide dans le champ utilisateur et le mot de passe associé.
   Si vous voyez un message de retour indiquant « Authentifié en tant que :... » alors vous vous êtes 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.

Remarque :

Ce document suppose que vous avez au moins un niveau de compréhension de base avec Microsoft Windows Server, Active Directory et ADAM et que vous disposez déjà d'une instance fonctionnelle Mode d'application Active Directory (ADAM) avec une partition.

Il s'agit d'exemples de procédures. En raison de la 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 Microsoft consultant si vous rencontrez des problèmes.

Une fois qu'ADAM a été installé et que la première partition a été créée, vous pouvez la remplir avec des objets.

Les options suivantes sont disponibles :

- Création manuelle d'objets à l'aide d'une interface graphique ou de scripts. Cette option est lente et inefficace.
- Intégration à Active Directory à l'aide du serveur d'informations d'intégration Microsoft . Cette option offre finalement le plus de flexibilité et de fonctionnalités, mais nécessite certaines configurations avancées. Il existe une version gratuite de MIIS qui est 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 des comptes utilisateur ADAM

Définir des comptes d'utilisateurs dans ADAM. Un compte d'utilisateur est utilisé pour l'instance à laquelle se connecter et l'autre compte d'utilisateur est destiné à ADAMSync.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Ces comptes peuvent être des objets utilisateur ADAM locaux, des objets UserProxy ou un compte Windows d'un domaine de confiance.

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 membre du groupe Lecteurs trouvé 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 définissant l'attribut msDS-UserAccountDisabled sur FALSE.
2. Cliquez avec le bouton droit de la souris sur l'objet utilisateur et réinitialisez le mot de passe.
3. Testez les nouveaux comptes à l'aide de LDP comme défini dans Mode d'application Active Directory (ADAM) 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 volet gauche. Traversez la partition de domaine. Si vous utilisez un nouveau compte ADAM local, il affichera « Aucun enfant », 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 *`ADAMSync User`* compte pour gérer les objets de la partition ADAM. Ce compte nécessite des droits de niveau administrateur puisqu'il créera, mettra à jour et supprimera des objets ADAM.

   ADAMSync utilise le *`ADAMSync AD`* compte pour lire les objets AD qui seront synchronisés avec ADAM.

Configurer ADAMSync

ADAMSync est inclus dans Windows Server 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 server :port et ajouter des informations d'identification si l'utilisateur actuel n'y a pas accès. Pour plus d'informations, consultez le fichier AdamSyncMetadata.ldf.

```
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 changements de schéma supplémentaires que nous recommandons.

1. Ouvrez une nouvelle console MMC et ajoutez le composant logiciel enfichable du schéma ADAM.
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 et ajoutez-en d'autres qui n'existent pas déjà.
   - société
   - department
   - givenNane
   - Courrier
   - physicalDeliveryOfficeName
   - Samaccountname
   - Sn
   - numéro de téléphone
   - Titre
   - 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 pour vous connecter à la console.

```
C:\WINDOWS\adam>adamsync /sync localhost:50000
"ou=users,dc=service-now,dc=adam" /log -
```

3. Examinez 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 Windows synchronisation en tant que tâche planifiée. Vous devez fournir les informations d'identification dans le fichier de configuration, la ligne de commande ou exécuter la tâche planifiée avec un compte disposant d'un accès.

   Remarques spéciales

   - Vous pouvez créer plusieurs fichiers de configuration et tâches planifiées pour synchroniser ADAM à partir de plusieurs sources.

     Cet exemple importe l'attribut sAMAccountName qui peut être utilisé comme ouverture de session de l'application. Si vous synchronisez 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 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 du filtre d'objet.

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 est 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 les commentaires ajoutés.

```
<?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>;
 <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>;
```

Traduction automatique

Filtre LDAP Fichier de configuration

Vous pouvez fournir n'importe quel niveau de filtrage dans la valeur object-filter dans le fichier de configuration. Utilisez la syntaxe de requête LDAP standard avec les caractères d'échappement xml suivants à la place des opérateurs standard.

- AND = « & » 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 en tant qu'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>;
  <aging>;
   <frequency>;0</frequency>;
   <num-objects>;0</num-objects>;
  </aging>;
  <schtasks-cmd>;</schtasks-cmd>;
 </schedule>;
</configuration>;
<synchronizer-state>;
 <dirsync-cookie>;</dirsync-cookie>;
 <status>;</status>;
```

Traduction automatique

```
 <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 LDAP 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 ne disposez pas encore d'une infrastructure d'autorité de certification, deux options s'offrent à vous.
  - Configurer une autorité de certification autonome pour émettre le certificat
  - Demander un certificat tiers
- Si vous disposez déjà d'une autorité de certification, 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 utilisateurs ne peuvent plus se connecter à l'instance. Pour résoudre ce problème, un nouveau certificat doit être émis et installé sur votre instance.

L'expiration par défaut des certificats Microsoft CA est d'un an. Les certificats CA externes sont généralement achetés par incréments d'un an. Notez la date d'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 souciez 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 d'autorité de certification en mode autonome.
3. Vérifiez que l'application Web Services de certification est installée et active.

Que faire ensuite
À l'aide de la console 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 application *CertSrv* répertoriée sous le **site Web par défaut**. Si le site ne fonctionne pas ou si l'application est manquante, vous devez résoudre le problème avant de poursuivre.

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 plate-forme CA interne, contactez 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. Sur la page d'accueil, cliquez sur **Demander un certificat** et sélectionnez *Demande de certificat avancée*.
3. Sur la page Demande de certificat avancée, sélectionnez **Créer** et soumettre une demande à cette autorité de certification.
4. Remplissez la demande de certificat avancée comme suit :

Champs de demande de certificat avancé

Champ	Entrée
Nom	Le nom de domaine complet (FQDN) du contrôleur de domaine qui demande le certificat.
E-mail	L'adresse e-mail de la personne responsable du certificat.
Entreprise	Nom de votre société.
Paramètres des options clés	

Champ	Entrée
Créer un nouvel ensemble de clés	Sélectionnez-le.
Demande de signature de certificat	Fournisseur de chiffrement Microsoft RSA SChannel.
Utilisation de la clé	Échange.
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 le magasin 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 cet ID.
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 la demande que vous venez d'envoyer, cliquez avec le bouton droit de la souris et sélectionnez *Toutes les tâches/Problème pour approuver la demande et émettre le certificat.*
7. Pour récupérer le certificat émis, procédez comme suit :
   a. Dans le collecteur de données 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. Cliquez sur le lien pour **installer ce certificat**.

Que faire ensuite

Vous devez demander un certificat tiers. Les certificats d'autorités de certification externes peuvent être achetés pour aussi peu que 30 $ par an. Pour connaître les procédures détaillées relatives à 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

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, entrez ldp pour démarrer l'outil .

3. Dans la fenêtre *LDP* , sélectionnez **Connexion** > **Connexion** et fournissez le nom de domaine complet local et le numéro de port (636).
   Sélectionnez également le *protocole SSL*.
   En cas de réussite, une fenêtre s'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 de confiance, vous devez exporter le certificat pour l'autorité de certification émettrice afin que nous puissions lui faire confiance et, par association, faire confiance au 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 l'exportation ; sélectionnez l'onglet **Chemin d'accès au certificat** . Vous devez exporter tous les certificats de la chaîne. Vous pouvez trouver le certificat de l'autorité de certification dans le même dossier que le certificat LDAP en recherchant le nom dans le chemin du certificat. Soumettez tous les certificats pour importation vers 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 de la souris sur le certificat et sélectionnez *Toutes les tâches/Exporter*.
5. Exportez 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 d'envoyer le certificat à l'instance.

Que faire ensuite
Une fois cette procédure terminée, importez le certificat de clé publique dans l'application.
Consultez Installer le certificat SSL LDAP X.509 pour télécharger le certificat dans l'application.

Utilisation du catalogue global LDAP

Un contrôleur de domaine peut se voir accorder le rôle de catalogue global (GC). Le rôle Global Catalog (GC) est un répertoire conforme à LDAP consistant en une représentation partielle de chaque objet de chaque domaine d'une forêt.

Les administrateurs configurent Active Directory pour héberger les informations d'annuaire LDAP (Lightweight Directory Access Protocol) à l'aide de l'une des méthodes d'hébergement suivantes.

- La méthode courante d'hébergement des informations d'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'existe aucun moyen d'accéder aux objets d'autres domaines à l'aide de cette méthode.
- Un contrôleur de domaine peut également se voir accorder le rôle de catalogue global (GC). Le rôle Global Catalog (GC) est un répertoire conforme à LDAP consistant en une représentation partielle de chaque objet de chaque domaine de la forêt. Ce répertoire LDAP est accessible via le port 3268, avec LDAPS sur le port 3269. Les exigences en matière de certificat des ports LDAPS et LDAP par défaut sont identiques.

Dépendances LDAP du catalogue global

- Le rôle Catalogue global doit être activé pour le contrôleur de domaine auquel votre instance se connecte.
- Les règles de pare-feu doivent autoriser le trafic entrant vers le contrôleur de domaine sur le port 3268 (LDAP) ou 3269 (LDAPS).

Remarques 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 forêt.
- Les intégrations LDAP standard utilisent généralement sAMAccountName comme ID d'utilisateur de l'instance et comme clé de coalescence dans le mappage d'importation LDAP, car il est garanti qu'il est 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 coalescence. 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, 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 lors des importations. L'adresse e-mail est un attribut commun utilisé pour l'ID utilisateur. Ces décisions ont un impact sur les propriétés LDAP et le mappage LDAP.
- La valeur utilisée pour la clé de coalescence sur le mappage d'importation LDAP doit être unique et exister sur chaque objet en cours d'importation. S'ils ne sont pas uniques ou s'ils n'existent pas, les enregistrements incorrects sont mis à jour avec les changements.
- Si vous disposez déjà d'une intégration LDAP et que vous souhaitez la remplacer par un GC, modifiez la clé de coalescence d'importation. Les nouvelles valeurs de clé doivent être importées avant de pouvoir modifier la clé de coalescence.
- Si vous apportez des modifications à votre intégration LDAP qui interrompent votre intégration, votre première étape doit être d'annuler ces modifications. Après cela, contactez-nous Service et assistance client avec des informations complètes sur ce que vous tentez.

Modification mineure du schéma OpenLDAP

Dans les systèmes OpenLDAP 2.3 qui utilisent le back-bdb (backend Berkley), 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). Il est implémenté uniquement pour la syntaxe generalizedTime et ChangeSequenceNumber. Elle ne peut pas être prise 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'index de présence.

Nous vous 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 de 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 pour l'intégration avec 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. Incluez 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 ) )
```

   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 objectclass 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 moteur de base de données principal.

   Example

   ```
   database bdb (configs here) ....

   index servnowid pres

   (other indexes here) .....
   ```

4. En tant que 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 qu'il est en mode lecture seule avant de démarrer slapindex.

Enregistrer les suppressions LDAP

Par défaut, l'instance ne supprime aucune entrée après leur disparition du 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 logiciel, les bons de commande et les entrées de Service Catalog ont tous une référence au département. Si un département est supprimé, l'intégration efface toutes les références au département. En outre, la suppression d'un utilisateur entraîne la perte de tout l'historique de ce qu'il a fait.

Décidez s'il faut conserver ou supprimer tous les enregistrements d'une 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.

servicenow

Explorer

Découvrez les fonctionnalités et la valeur commerciale de la limite de sessions simultanées.

Activer

Découvrez comment activer la limite de sessions simultanées.

Définir

Définissez la limite de sessions simultanées pour un utilisateur ou un rôle.

Désactiver

Traduction automatique

Exploration de la 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 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. La valeur limit_concurrent_sessions d'un utilisateur ou d'un rôle connecté à l'utilisateur doit être définie sur vrai pour limiter les sessions à initier. Pour la version Jakarta, cette fonctionnalité ne prend pas en charge les sessions créées via l'application Mobile native ou des 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 la session 1 (S1) est créée 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 la session 2 (S2) est créée pour l'utilisateur.
5. Étant donné que l'utilisateur a une limite maximale de sessions simultanées de 1, la session S1 est invalidée 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 sessions simultanées fonctionnent avec tous les mécanismes d'authentification ServiceNow : SAML, LDAP et authentification de la 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 les suivantes :

- Navigateur Web
- Navigateur mobile
- ServiceNow Application mobile
- Non interactif (SOAP, WSDL, OAuth)

Traduction automatique

Activation et configuration du module d'extension Limite de sessions simultanées

Vous pouvez activer le module d'extension Limit Concurrent Sessions (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 le module d'extension Limit Concurrent Sessions et cliquez dessus.
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. Cliquez sur **Activer**.
5. Pour activer cette fonctionnalité et définir une limite maximale de sessions simultanées, accédez à l'onglet Fichiers du module d'extension, recherchez les propriétés suivantes et modifiez les valeurs des paramètres :

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 **False**, ce qui signifie qu'il n'y a aucune limite au nombre de sessions interactives qu'un utilisateur peut avoir. **Remarque :** Pour désactiver cette fonctionnalité, redéfinissez cette propriété sur **Faux**.
glide.authenticate.max.concurrent.interactive-.sessions	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.concurrency	Cette propriété limite les types de sessions. Par défaut, seules les sessions du navigateur Web ont une limite. Les types de sessions incluent : ○ 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.

Option	Description
	Remarque : Seules les sessions de navigateur Web et mobile peuvent avoir une limite. Il n'y a aucune limite pour les sessions provenant de l'application ServiceNow Mobile ou les sessions non interactives.
glide.authenticate.limit.concurrent.sessions-.across.all.nodes	Cette propriété restreint la limite de sessions simultanées par nœud au lieu de les restreindre sur tous les nœuds d'une ServiceNow instance. Par défaut, la valeur est définie sur vrai, ce qui limite les sessions utilisateur dans 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 que les paramètres prennent effet.

Que faire ensuite

Définition d'une limite de sessions simultanées par utilisateur ou rôle.

Information associée

Liste des modules d'extension (Washington DC)

Définition d'une limite de sessions simultanées par utilisateur ou rôle

Vous pouvez définir une limite de sessions simultanées 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 sessions simultanées, 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 qui peuvent être ouvertes à la fois.

Désactivation d'une limite de sessions simultanées par utilisateur ou rôle

Vous pouvez désactiver une limite de sessions simultanées 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 désactiver une limite de sessions simultanées, désactivez la case à cocher **Limiter les sessions simultanées** , puis cliquez sur **Mettre à jour**.
   L'utilisateur ou le rôle n'est pas soumis à une limite quant au nombre de sessions simultanées pouvant être ouvertes à la fois.

Authentification multifacteur (MFA)

Découvrez comment activer et configurer l'authentification multifacteur.

Explorer

Découvrez les fonctionnalités et la valeur commerciale de l'authentification multifacteur.

Activer

Découvrez comment activer l'authentification multifacteur.

Traduction automatique

Utiliser

Configurez et utilisez l’authentification multifacteur.

MFA avec authentification unique (SSO)

Découvrez comment configurer l’authentification multifacteur avec Single Sign-on (SSO).

Découverte de l’authentification multifacteur

Découvrez comment activer et configurer l’authentification multifacteur.

Activation de la MFA

Activez le module **d’extension Integration - Multifactor Authentication** (com.snc.integration.multifactor.authentication) pour commencer à utiliser MFA sur une instance. L’activation de ce module d’extension nécessite le rôle administrateur. Pour obtenir des détails sur ce processus, consultez Activer le module d’extension MFA.

Critère multifacteur

Utilisez des critères multifacteur pour déterminer quels utilisateurs et rôles doivent utiliser la vérification multifacteur en deux étapes. Vous pouvez utiliser l’un de ces critères ou une combinaison de ceux-ci en fonction des besoins de votre entreprise.

Critères multifacteurs basés sur l’utilisateur

Utilisez des critères multifacteur basés sur l’utilisateur pour sélectionner les utilisateurs individuels qui doivent se connecter à l’aide de l’authentification multifacteur. 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.

Critères multifacteurs basés sur les rôles

Utilisez des critères multifacteur basés sur les rôles pour exiger la connexion MFA pour tous les utilisateurs affectés à un rôle spécifique. L'enregistrement **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 en savoir plus sur la gestion de cette liste, reportez-vous à Configurer des critères multifacteur basés sur les rôles.

Critères multifacteurs basés sur une politique d'authentification adaptative

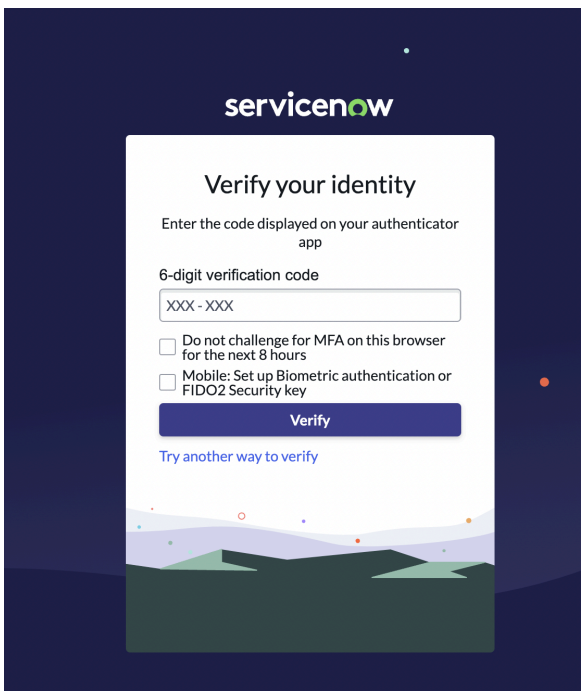
Utilisez l'authentification adaptative pour déterminer quand votre instance a besoin d'une authentification MFA. L'authentification adaptative utilise des politiques d'authentification pour évaluer des critères tels que l'adresse IP d'un utilisateur ou des groupes d'utilisateurs. Pour en savoir plus sur la fonctionnalité d'authentification adaptative, reportez-vous à la section Authentification adaptative.

Méthodes d'authentification multifacteur

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.

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 plus de détails sur ces applications, reportez-vous à Applications d'authentification.



Traduction automatique

Scanners biométriques

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 en savoir plus sur l'enregistrement des authentificateurs biométriques, reportez-vous à la section Enregistrer un authentificateur biométrique.

Clés matérielles

Les clés matérielles sont des matériels physiques que vous pouvez utiliser pour vous authentifier. Les clés matérielles sont insérées dans un port de votre appareil pour fournir une authentification. Pour en savoir plus sur l'enregistrement des clés matérielles, reportez-vous à la section Enregistrer une clé de sécurité matérielle.

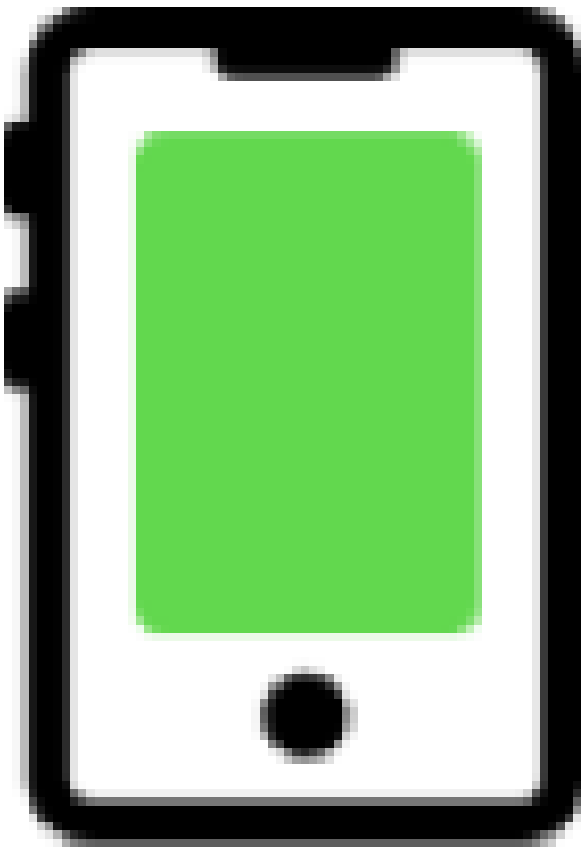
Traduction automatique

SMS

L’administrateur peut configurer ServiceNow l’instance pour exiger des utilisateurs qui tentent de s’y connecter d’utiliser un mot de passe à usage unique basé sur un SMS.

Lorsque les utilisateurs tentent de se connecter à , un mot de passe à ServiceNowusage 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.

Pour plus d'informations, consultez Authentification multifacteur par SMS.



E-mail

L’administrateur peut configurer ServiceNow l’instance pour exiger des utilisateurs qui tentent de s’y connecter d’utiliser un mot de passe à usage unique basé sur une adresse e-mail.

Lorsque les utilisateurs tentent de se connecter à , un mot de passe à ServiceNowusage unique par 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 reçu à l’adresse e-mail et confirmer leur identité.

Pour plus d'informations, consultez Authentification multifacteur avec e-mail.

Propriétés de l'authentification multifacteur

Utilisez les propriétés de l’authentification multifacteur pour activer, désactiver et configurer l’authentification MFA sur votre instance. Pour en savoir plus sur ces propriétés, reportez-vous à Propriétés système de l’authentification multifacteur.

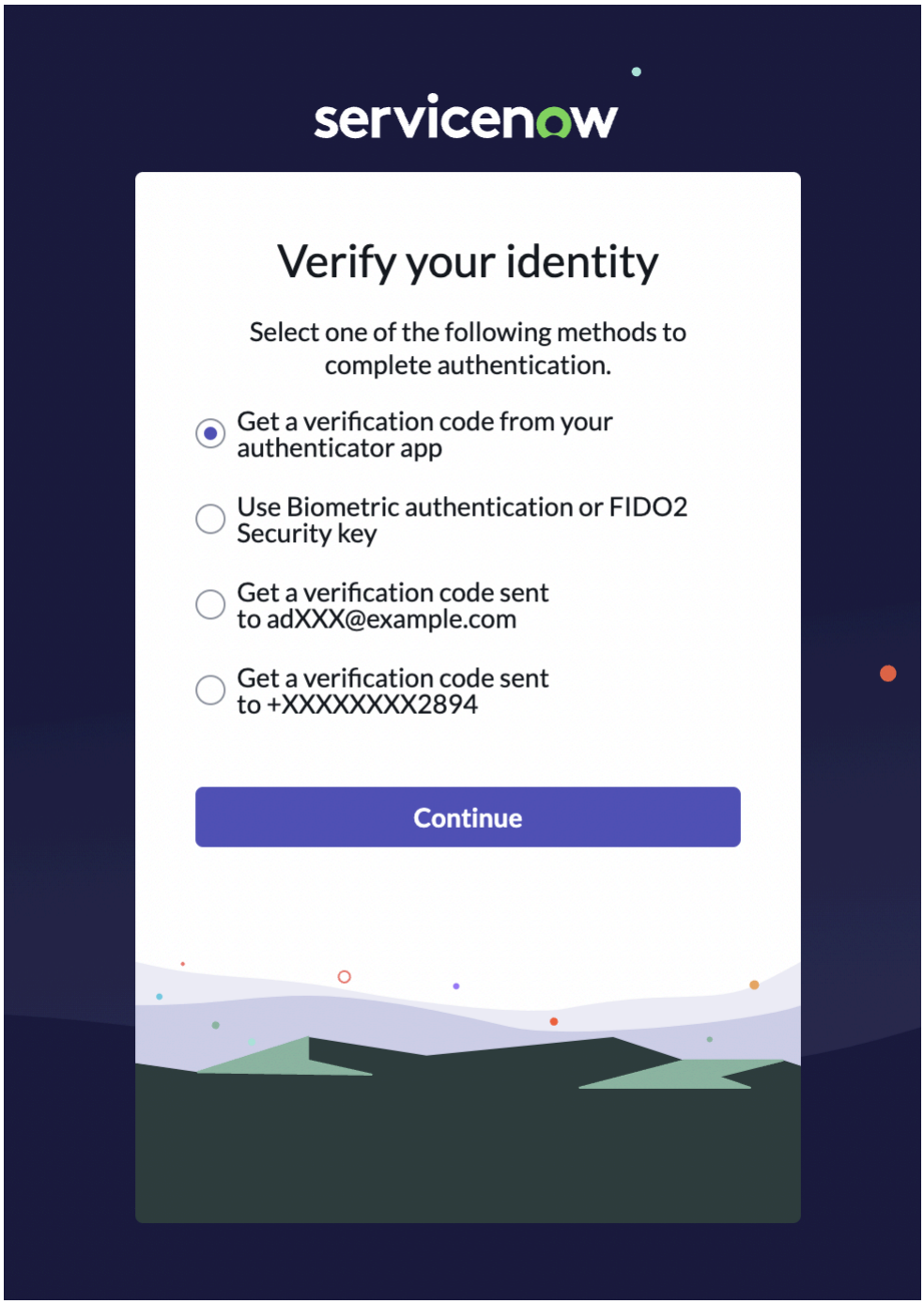
Activation MFA, méthodes prises en charge et workflow

L’authentification MFA, également connue sous le nom de vérification en deux étapes, est une exigence de sécurité qui oblige les utilisateurs à saisir plus d’un ensemble d’informations d’identification pour accéder à une instance.

Le niveau d’authentification de base à une instance est l’authentification de base de données locale où un utilisateur entre une combinaison de nom d’utilisateur et de mot de passe. L’authentification MFA permet aux administrateurs et aux utilisateurs d’exiger un deuxième niveau d’authentification. Cette seconde authentification peut être :

- Code secret d’une application d’authentification
- Clé matérielle
- Un authentificateur biométrique, tel qu’un lecteur d’empreintes digitales ou une reconnaissance faciale.
- Un SMS ou un e-mail

Traduction automatique



Traduction automatique

En tant qu'administrateur, vous pouvez exiger l'authentification MFA pour des utilisateurs individuels ou pour tous les utilisateurs dans un rôle spécifique. Vous pouvez également permettre à vos utilisateurs d'accepter et d'utiliser l'authentification multifacteur.

Activation

Le *`Integration - Multifactor Authentication`* module d'extension (com.snc.integration.multifactor.authentication) est installé par défaut sur votre instance, mais doit être activé par un administrateur à l'aide d'une propriété système. Pour plus de détails, voir Propriétés système de l'authentification multifacteur.

Remarque :
Après le clonage d'une instance, vous devez réactiver la MFA sur l'instance clonée. Pour plus d'informations, consultez ces articles de la base de connaissances KB0657100 , KB0860689 , KB0825390 , KB0779908 , KB0717367 , KB0727991 .

Méthodes d'authentification prises en charge

Vous pouvez utiliser l'authentification MFA avec les méthodes d'authentification suivantes :

- Authentification de la base de données locale (authentification native ServiceNow)
- Intégration LDAP
- SSO SAML
- SSO OIDC

Remarque :
Les utilisateurs doivent configurer une application d'authentification avant de configurer une clé matérielle ou un authentificateur biométrique. Pour en savoir plus sur la configuration de l'application d'authentification, reportez-vous à la section Configurer l'authentification multifacteur sur votre profil d'utilisateur.

Workflow de configuration de l'authentification multifacteur

L'administrateur active l'authentification multifacteur

Le module **d'extension Integration - Multifactor Authentication** (com.snc.integration.multifactor.authentication) est activé sur votre instance par défaut. Pour commencer à utiliser l'authentification multifacteur, les administrateurs doivent activer l'authentification multifacteur à l'aide d'une propriété système. Une fois l'option activée, les administrateurs sélectionnent les utilisateurs ou les rôles qui nécessitent des connexions MFA.

Pour en savoir plus sur la configuration de l'administrateur pour l'authentification multifacteur, reportez-vous à la section Authentification multifacteur (MFA).

Les utilisateurs se connectent à l'aide d'une application d'authentification

Les utilisateurs sont invités à utiliser une application d'authentification la première fois qu'ils se connectent. Cette étape est nécessaire même si vos utilisateurs vont utiliser la biométrie ou une clé matérielle. Les utilisateurs qui se connectent voient un code QR qu'ils peuvent scanner pour configurer rapidement une application d'authentification. Ce processus de connexion initial est détaillé dans Configurer l'authentification multifacteur sur votre profil d'utilisateur.

Les applications d'authentification sont disponibles en tant qu'applications Mobile. Certaines applications d'authentification sont disponibles en tant qu'extensions pour les navigateurs de bureau des utilisateurs qui n'ont pas accès à un équipement mobile.

Après la connexion initiale, les utilisateurs peuvent configurer des authentificateurs supplémentaires

Après la connexion initiale, les utilisateurs peuvent enregistrer des clés matérielles ou des authentificateurs biométriques.

Pour en savoir plus sur ces configurations et d'autres configurations côté utilisateur pour l'authentification multifacteur, reportez-vous à la section Utilisation de l'authentification multifacteur (MFA).

Authentification Web

Activez *`Integration - Web Authentication`* (com.snc.integration.webauthn) pour autoriser l'authentification par clé matérielle ou lecteur biométrique sur votre instance.

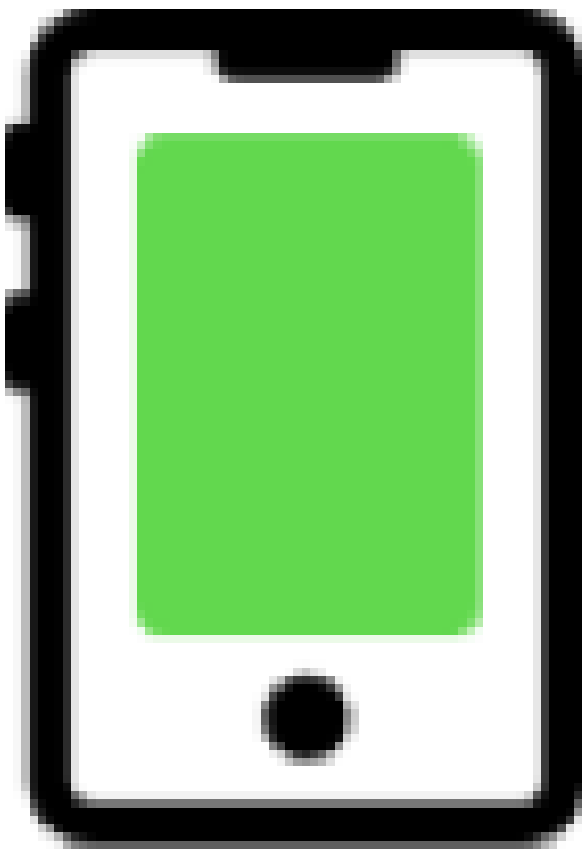
Les clés matérielles sont des matériels physiques que vous pouvez utiliser pour vous authentifier. Les clés matérielles sont insérées dans un port de votre appareil pour fournir une authentification. Pour en savoir plus sur l'enregistrement des clés matérielles, reportez-vous à la section Enregistrer 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 en savoir plus sur l'enregistrement des authentificateurs biométriques, reportez-vous à la section Enregistrer un authentificateur biométrique.

Traduction automatique

SMS ou e-mail (mot de passe à usage unique)

Pour permettre aux utilisateurs de se connecter à une instance et de vivre une ServiceNow expérience plus fluide lors de leurs déplacements, l'authentification MFA est prise en charge par SMS et par e-mail.



L'administrateur peut configurer ServiceNow l'instance pour exiger des utilisateurs qui tentent de s'y connecter d'utiliser un mot de passe à usage unique 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.

Pour plus d'informations, consultez Authentification multifacteur par SMS.

L'administrateur peut configurer ServiceNow l'instance pour exiger des utilisateurs qui tentent de s'y connecter d'utiliser un mot de passe à usage unique basé sur une adresse e-mail.

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. L'utilisateur peut saisir le code de vérification à six chiffres qu'il a envoyé à l'adresse e-mail et vérifier son identité.

Pour plus d'informations, consultez Authentification multifacteur avec e-mail.

Activer le module d'extension MFA

Le module d'extension Integration - Multifactor Authentication est actif par défaut.

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 Integration - Multifactor Authentication** (com.snc.integration.multifactor.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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

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. Modifiez la valeur de la colonne **Activer l'authentification multifacteur** pour les utilisateurs sélectionnés en **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 des 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

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...,** puis saisissez ou sélectionnez un nom de rôle. Cliquez sur **l'icône Enregistrer (icône**) pour enregistrer l'entrée.
Supprimer un rôle	Cliquez sur l'icône de suppression ( ) 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.

Réinitialiser l'authentification multifacteur (MFA) pour les utilisateurs

Les administrateurs peuvent réinitialiser l'authentification multifacteur pour les utilisateurs qui ont supprimé l'application, qui ont perdu l'accès à l'appareil ou qui n'ont pas d'autre authentification multifacteur associée à leur appareil.

Réinitialisation de l'authentification multifacteur assistée par l'administrateur

Avant de commencer
Rôle requis : admin

La procédure suivante décrit comment un ServiceNow® administrateur peut réinitialiser la validation MFA pour débloquer les utilisateurs et leur permettre d'enregistrer à nouveau MFA.

Procédure

1. Accédez à la **Tous** > **Authentification multifacteur** > **Configuration multifacteur pour l'utilisateur**.
2. Dans la table utilisateur, recherchez l'utilisateur que vous souhaitez débloquer.
3. Définissez la valeur **Valider sur Faux**.
   Changer la valeur sur **faux** débloque l'utilisateur et lui permet d'enregistrer à nouveau l'authentification MFA.
   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 MFA.

Configurer des critères multifacteurs basés sur une politique d'authentification adaptative

Utilisez des stratégies adaptatives pour déterminer quels utilisateurs doivent utiliser la vérification multifacteur (MFA) en deux étapes.

Avant de commencer
Rôle requis : admin

Remarque :

- Cette option **s'affiche uniquement lorsque le module d'extension SSO de plusieurs fournisseurs** est actif sur votre instance. Pour plus d'informations sur cette fonctionnalité, consultez Authentification unique (SSO) externe.
- Si la politique par défaut est **Politique MFA ascendante**, les utilisateurs s'affichent avec l'authentification multifacteur si la politique configurée dans la **politique MFA donne la** valeur vrai. 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 **de contexte 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 la politique pour déterminer s'il faut exiger l'authentification MFA.

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 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 MFA ascendante** , sélectionnez une politique à utiliser dans ce contexte.
   Pour obtenir des détails sur les politiques et leur configuration, consultez
4. Cliquez sur **Mettre à jour**.
   Après avoir enregistré l'enregistrement, les listes **Entrée de politique** et **Conditions de politique** sont mises à jour pour afficher les entrées de politique et les conditions associées à la politique sélectionnée dans le champ **Politique MFA ascendante** .

Propriétés système de l'authentification multifacteur

Utilisez les propriétés système pour activer et personnaliser l'authentification multifacteur afin de répondre à vos exigences de sécurité.

Propriétés de l'authentification multifacteur

Propriété	Description
Activer l'authentification multifacteur (*glide.authenticate.multifactor*)	Option qui permet aux utilisateurs et aux administrateurs d'utiliser cette fonctionnalité. La valeur par défaut est activée. Pour en savoir plus sur cette propriété, consultez Activer l'authentification multifacteur (MFA) Paramètres de renforcement de la sécurité de l'instance.
Nombre de fois qu'un utilisateur peut contourner l'authentification multifacteur (*glide.authenticate.multifactor.setup.bypass.count*)	Nombre de fois qu'un utilisateur peut choisir d'ignorer la configuration de MFA. Vos utilisateurs peuvent toujours se connecter à l'instance même s'ils n'ont pas leur équipement mobile sur eux. Si vous désactivez cette fonctionnalité, puis que vous la réactivez, le compteur est réinitialisé. La valeur par défaut est 3.
Durée, en minutes, pendant laquelle le code à usage unique envoyé à l'adresse e-mail de l'utilisateur est valide (*glide.multifactor.onetime.code.validity*)	Nombre de minutes pendant lesquelles le code de réinitialisation est valide. Consultez Connectez-vous avec l'authentification multifacteur. La valeur par défaut est 10.
Temps supplémentaire, en secondes, pendant lequel le code est valide pour prendre en compte le décalage d'horloge. La valeur maximale est de 60 secondes. (*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. L'instance valide le code saisi par l'utilisateur par rapport au code unique généré par l'application qui est généré au moment actuel. Vous pouvez décaler l'intervalle de temps avec cette propriété et permettre qu'un ou plusieurs codes soient générés au cours d'un intervalle de temps 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'heureactuelle + 5 secondes] sont valides. Utilisez cette propriété pour éviter les problèmes de connexion au cours desquels l'utilisateur n'est pas en mesure de saisir le code correct dans le délai par défaut défini.
Activez la fonctionnalité Mémoriser le navigateur pour l'authentification multifacteur. (*glide.authenticate.multifactor.remember.browser.enable*)	Configurez votre instance pour inviter un utilisateur à utiliser MFA lorsqu'il se connecte à partir d'un nouvel appareil ou d'un nouveau navigateur. La valeur par défaut est Oui.
Validité de l'empreinte du navigateur en heures.	Une fois que MFA se souvient du navigateur, l'utilisateur n'est pas sollicité pour MFA dans le

Propriétés de l'authentification multifacteur (suite)

Propriété	Description
(*glide.authenticate.multifactor.browser.fingerprint.validity*)	même navigateur pendant cette durée. La valeur par défaut est de 8 heures.
Nombre maximal de navigateurs dont un utilisateur peut se souvenir. (*glide.authenticate.multifactor.remembered.browser.max.count*)	Nombre de navigateurs dont MFA se souvient pour cet utilisateur.
Valeur par défaut de la case à cocher Mémoriser le navigateur dans la page multifacteur de validation. (*glide.authenticate.multifactor.remember.browser.default*)	Valeur par défaut de la case à cocher remember-browser dans la page multifacteur de validation.
Activez la MFA basée sur l'authentification Web (FIDO2). (*glide.webauthn.enabled*)	Option permettant d'activer les méthodes d'authentification sans mot de passe telles que la clé matérielle et l'authentification biométrique.

Configurer l'authentification multifacteur avec la biométrie

Les administrateurs peuvent utiliser la liste 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 **Informations d'identification publiques de l'utilisateur**[sys_user_public_credential]. Utilisez cette table pour voir quels utilisateurs ont enregistré un authentificateur, ainsi que les types, et quand ils ont été enregistrés et utilisés. Vous pouvez également marquer ces enregistrements comme inactifs pour empêcher les informations d'identification afin d'empêcher les utilisateurs d'utiliser ces informations d'identification.

Formulaire Informations d'identification publiques de l'utilisateur

Champ	Description
Pseudonyme des informations d'identification	Pseudonyme des informations d'identification. Ce pseudo est choisi par l'utilisateur lorsqu'il enregistre un authentificateur.
Utilisateur	Utilisateur associé aux informations d'identification
Actif	Si les informations d'identification sont actives. Les administrateurs peuvent définir un enregistrement sur Inactif pour empêcher un utilisateur de s'authentifier avec ces informations d'identification.
Authentificateur	Le type d'authentificateur enregistré par l'utilisateur.
Heure d'inscription	La date et l'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 restreint

Si vous avez restreint une méthode d'authentification, comme 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 que vous n'établissiez 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 de l'authentificateur 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 Configuration de l'authentificateur

Champ	Description
Type d'authentificateur autorisé	Type d'authentificateurs autorisés à être enregistrés. Sélectionner à partir de : • **Les** authentificateurs de plateforme sont attachés ou intégrés dans 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	La définition de la valeur sur direct ou indirect nécessite l'importation des métadonnées d'authentificateur pour attester la provenance d'un authentificateur pendant l'enregistrement. • Aucun • Direct • Indirect
Auto-attestation de plateforme	Si l'auto-attestation est activée pour les authentificateurs de plateforme.
Auto-attestation entre plateformes	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 effectuer une vérification à l'aide d'un code PIN ou biométrique.

Formulaire Configuration de l'authentificateur (suite)

Champ	Description
Vérifier la présence de l'utilisateur	Si le flux d'authentification Web nécessite la vérification de la 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. La durée est exprimée en millisecondes.

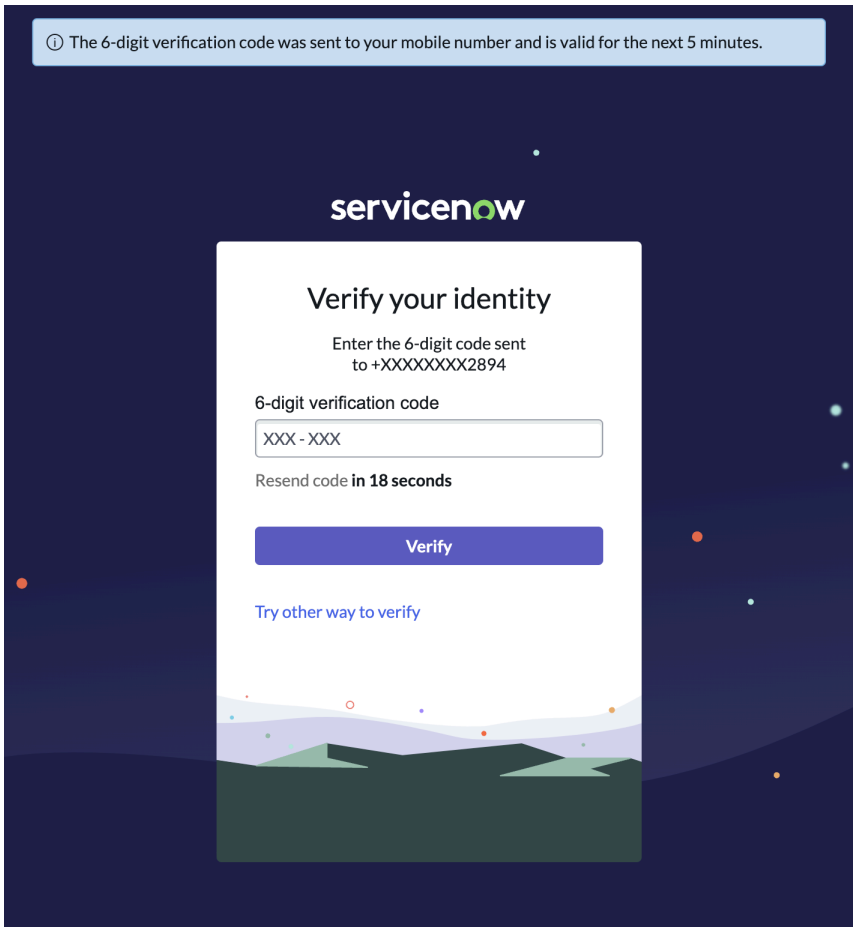
Authentification multifacteur par SMS

Authentification multifacteur (MFA) avec SMS comme facteur d'authentification.

L'administrateur peut configurer ServiceNow l'instance pour exiger des utilisateurs qui tentent de s'y connecter d'utiliser un mot de passe à usage unique 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 l'authentification multifacteur par SMS à l'aide du module prêt 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 de l'entrée et des conditions de la politique à l'aide de critères de filtre. Les types de critères de filtre suivants sont disponibles :

- Critère de filtre d'adresses IP
- Critère de filtre de rôle
- Critères de filtre de groupe

Activer le MFA avec le module d'extension SMS

Pour MFA avec SMS, installez le module d'extension Multi-factor authentication with SMS (com.snc.authentication.sms_mfa).

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
- Notify - Pilote Twilio Direct (com.snc.notify.twilio_direct)

Module d'extension dépendant : Integration - Multifactor Authentication (com.snc.integration.multifactor.authentication)

Traduction automatique

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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

Configurer SMS en tant que facteur MFA

Configurez l'entrée et la condition de politique pour afficher SMS OTP en tant que politique de facteur MFA pour l'authentification.

Avant de commencer

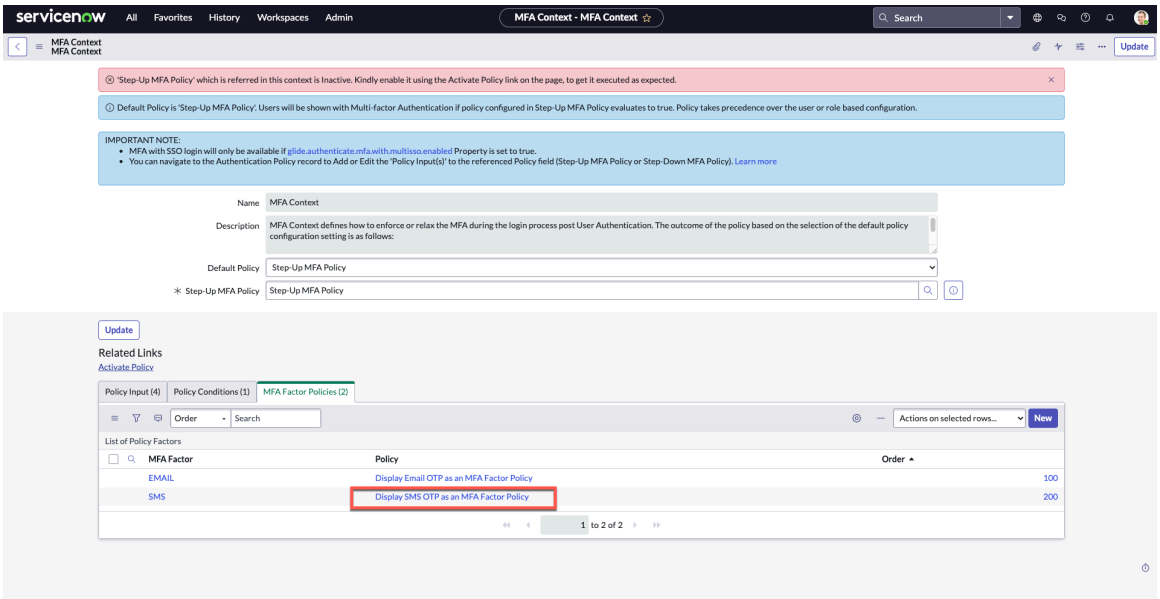
Module d'extension requis : authentification multifacteur par SMS (com.snc.authentication.sms_mfa).

Rôle requis : admin

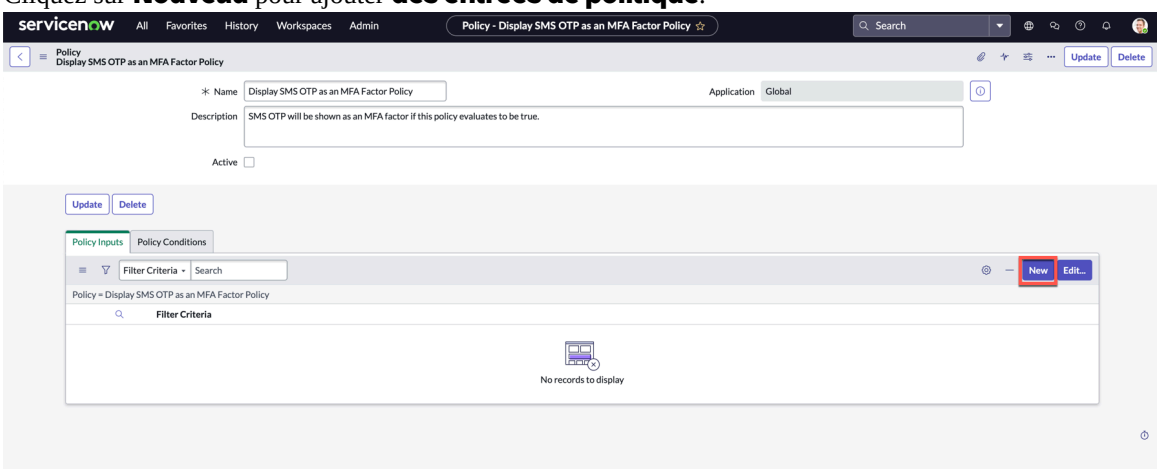
Remarque :
La politique de contexte MFA doit être évaluée comme vraie pour appliquer la politique de facteur SMS.

Procédure

1. Accédez à la **Tous** > **Authentification multifacteur** > **Contexte MFA**.
2. Cliquez sur **l'onglet Politiques de facteur MFA** .
3. Sélectionnez **Afficher SMS OTP en tant que politique de facteur MFA**.



4. Cliquez sur **Nouveau** pour ajouter **des entrées de politique**.

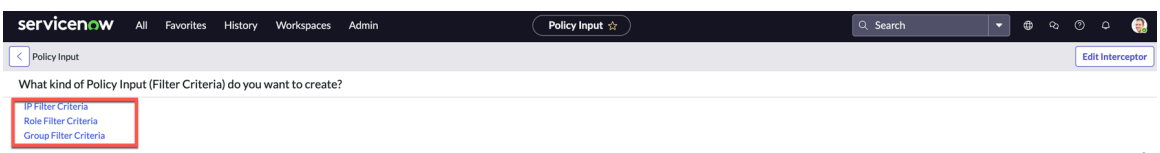


5. Sélectionnez les critères de filtre que vous souhaitez créer.

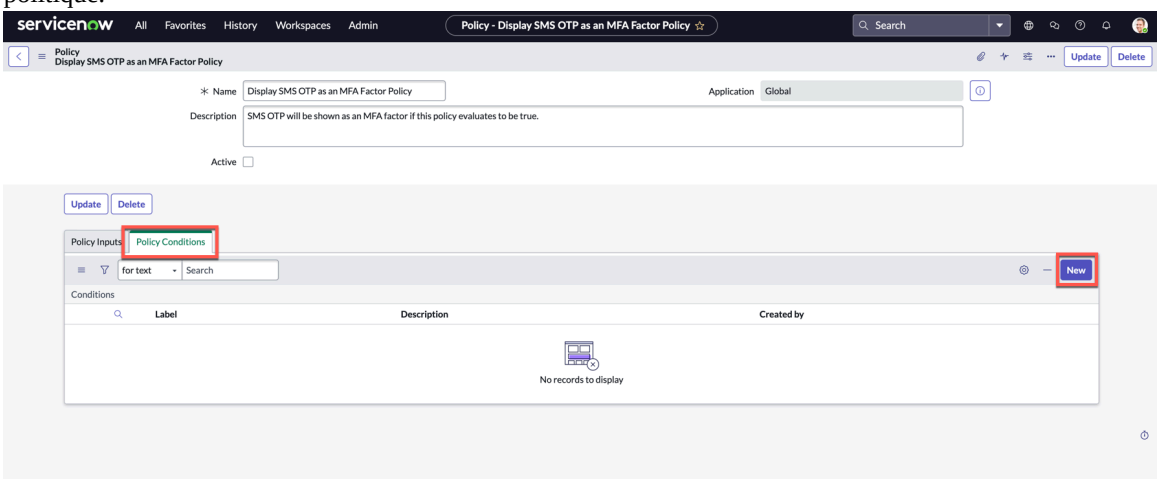
   Les types de critères de filtre suivants sont disponibles :

   - Critère de filtre d'adresses IP
   - Critère de filtre de rôle
   - Critères de filtre de groupe

   Par exemple, Critères de filtre de rôle.



6. Cliquez sur **Critères de filtre de rôle.**
7. 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.
8. Sur la page Politique - Afficher SMS OTP en tant que politique de facteur MFA, cliquez sur Conditions de la politique.



9. Cliquez sur **Nouveau** pour ajouter des **conditions de politique**.
10. 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) qui est utilisée pour évaluer les demandes d'authentification. Sélectionnez la politique de critères de filtre basée sur le rôle qui a été créée pour la condition.

11. Cliquez sur **Envoyer**.
12. **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 OR de toutes les conditions de politique. Cela signifie que la police 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, le SMS en tant que facteur MFA est affiché comme une option d'authentification pour les utilisateurs.

Fournisseurs d'authentification multifacteur

Utilisez les fournisseurs de MFA pour configurer l'authentification par SMS et par e-mail afin de garantir que chaque utilisateur peut se connecter en toute sécurité.

Sur , Now Platformvous pouvez configurer les fournisseurs d'authentification MFA avec le mécanisme d'authentification multifacteur tel que les e-mails et les SMS.

Vous pouvez utiliser la configuration de fournisseur suivante disponible pour MFA dans :Now Platform

- Configuration du fournisseur de messagerie
- Configuration du fournisseur Twilio
- Configuration du fournisseur Infobip.

Remarque :
La configuration des fournisseurs Twilio et Infobip est remplie 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 Notify - Pilote com.snc.notify.twilio_direct direct Twilio ().

Vous pouvez également créer votre propre configuration de fournisseur pour activer l'authentification multifacteur par SMS et par e-mail.

Remarque :
La configuration du fournisseur Infobip est fournie dans le cadre des données de démonstration, vous pouvez modifier les champs en fonction de vos besoins pour configurer 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.

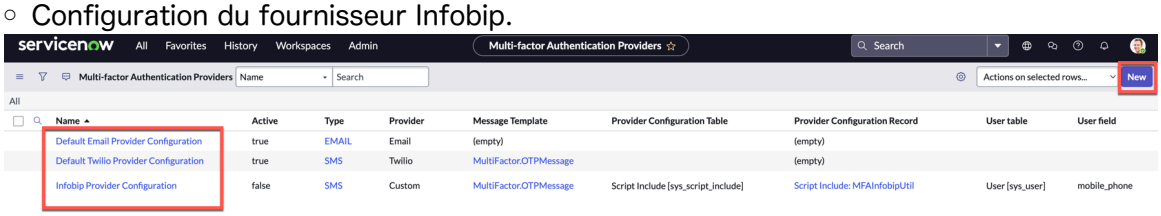
Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification multifacteur** > **Fournisseurs**.

   La configuration du fournisseur suivante est disponible pour MFA dans :Now Platform

   - Configuration du fournisseur de messagerie
   - Configuration du fournisseur Twilio
   - Configuration du fournisseur Infobip.



2. Pour créer un fournisseur, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Traduction automatique

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 Notifier 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	Le 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)

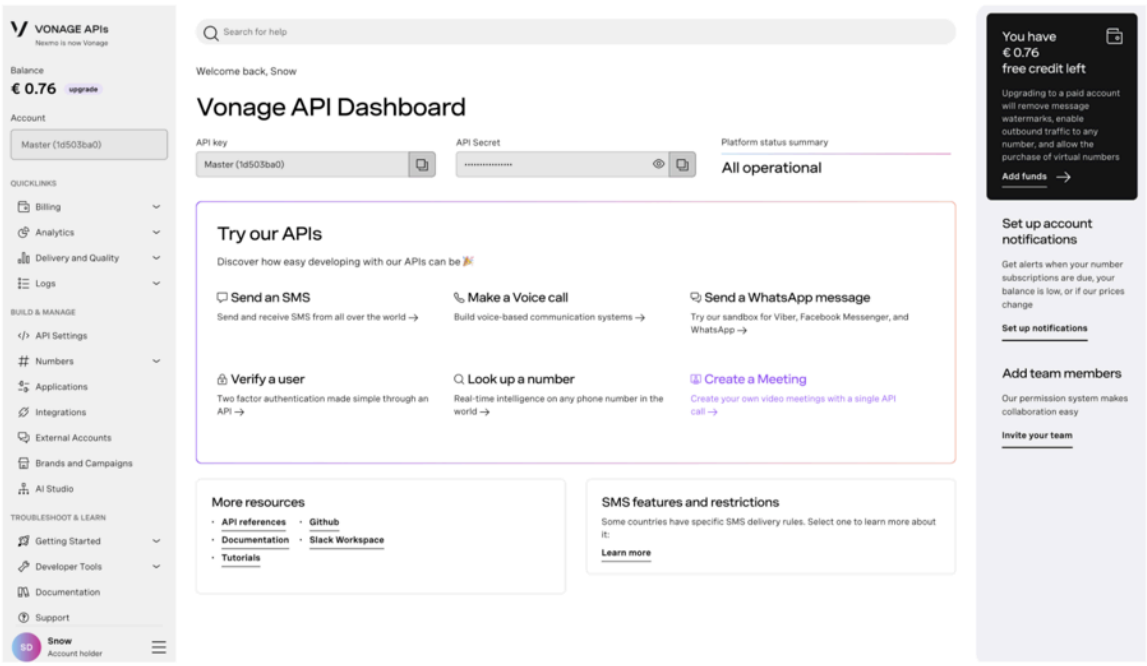
Configurez un SMS avec le fournisseur Vonage pour vous assurer que chaque utilisateur peut se connecter en toute sécurité.

Avant de commencer

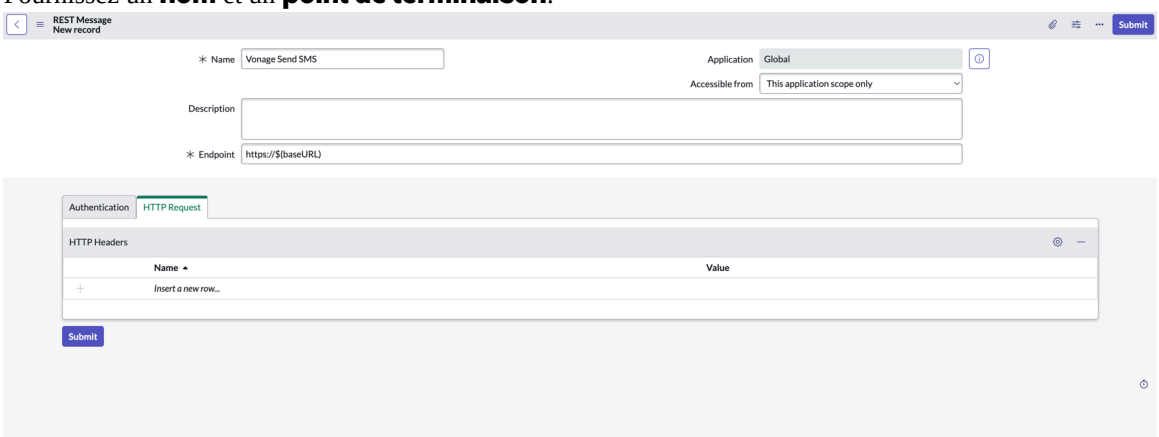
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Services web du système** > **Sortant** > **Message REST** et effectuez la configuration des messages REST en fonction des informations issues du tableau de bord de l'API Vonage.

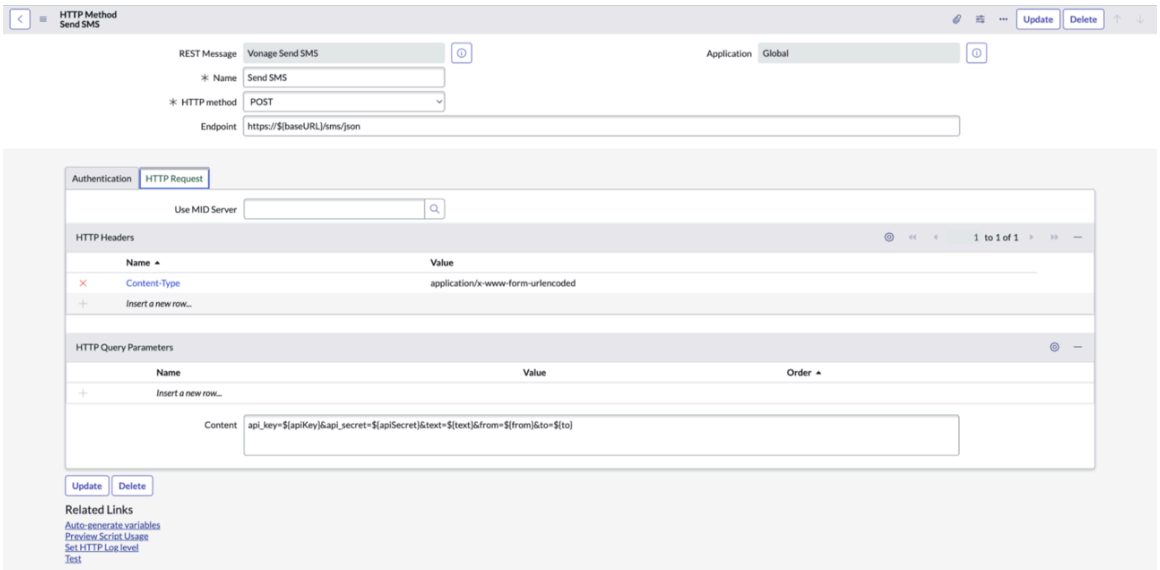


2. Cliquez sur **Nouveau** pour créer un **nouveau message REST**.
3. Fournissez un **nom** et un **point de terminaison**.

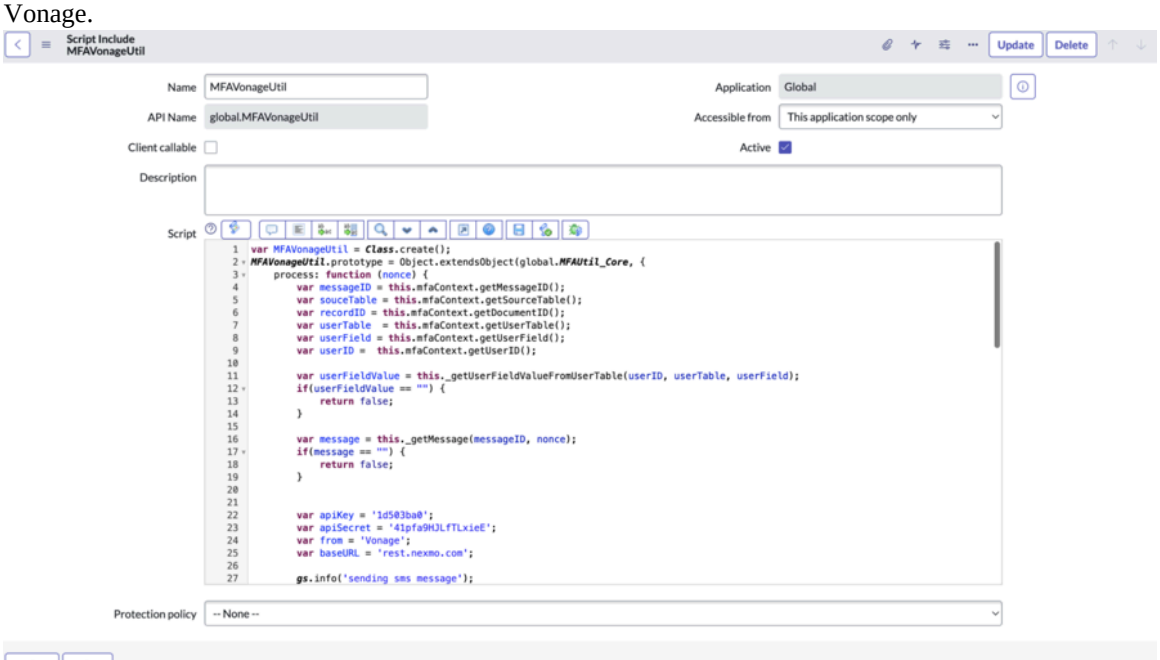


4. Cliquez sur **Envoyer**.
5. Ouvrez l'enregistrement créé, dans la liste connexe **Méthodes HTTP**, cliquez sur **Nouveau** et sélectionnez la méthode HTTP en tant que **POST.**
6. Renseignez les champs suivants :
   - Point de terminaison : `https://${baseURL}/sms/json`
   - Contenu :`api_key=${apiKey}&amp;api_secret=${apiSecret}&amp;text=${texte}&amp;from=${from}&amp;to=${to}`
   - Type de contenu : `application/x-www-form-urlencoded`

Traduction automatique

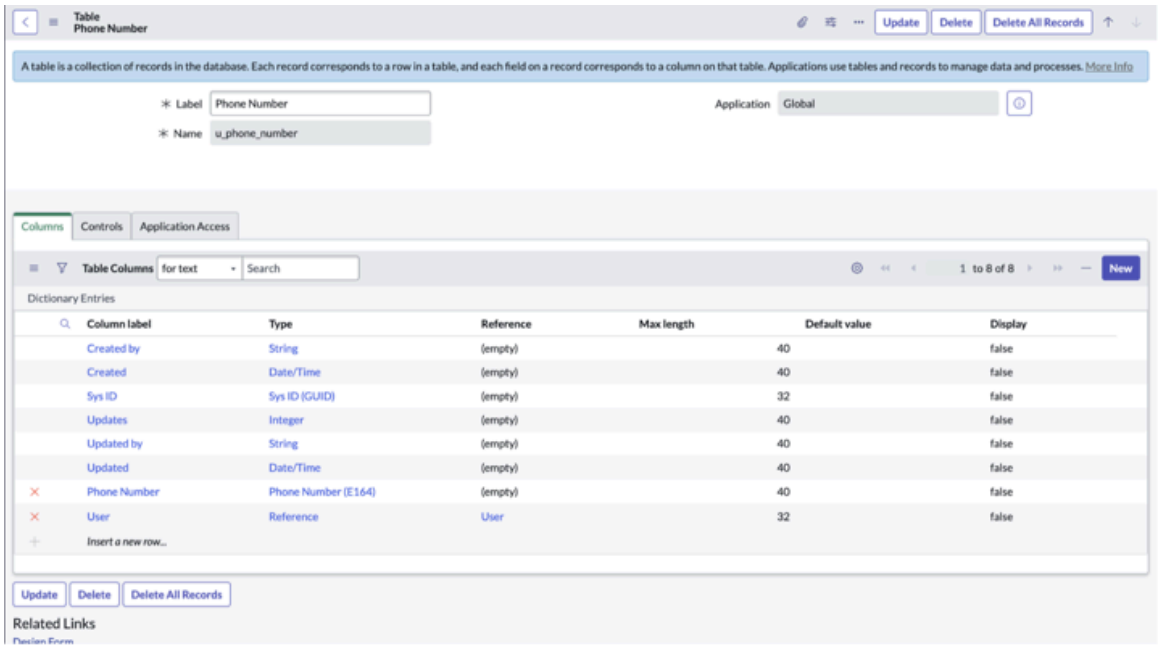


7. Mettez à jour l'enregistrement.
8. Cliquez sur **Générer automatiquement des variables** dans la section **Liens connexes** .
9. Importez le SI partagé dans le dossier et copiez la clé API et le secret à partir du tableau de bord des API Vonage.



10. Créez une table Numéros de téléphone personnalisée 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



11. Créez un fournisseur personnalisé dans la table Fournisseur multifacteur.

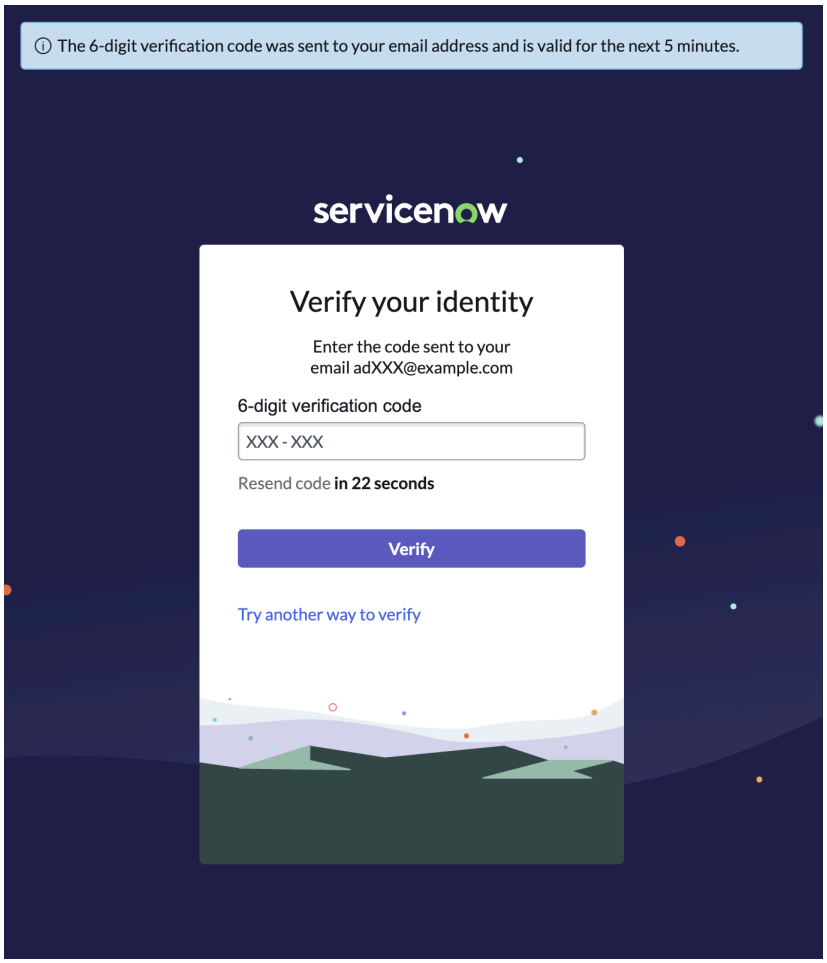
Pour en savoir plus sur la configuration du fournisseur, reportez-vous à Configurer le fournisseur MFA.

Authentification multifacteur avec e-mail

Authentification multifacteur (MFA) avec l'e-mail comme facteur d'authentification.

L'administrateur peut configurer ServiceNow l'instance pour exiger des utilisateurs qui tentent de s'y connecter d'utiliser un mot de passe à usage unique basé sur une adresse e-mail.

Remarque :
MFA avec e-mail est activé avec le module d'extension Integration - Multifactor Authentication (com.snc.integration.multifactor.authentication) par défaut. Vous devez configurer les entrées et les conditions de la politique.



Lorsque les utilisateurs tentent de se connecter à , un mot de passe à ServiceNowusage unique par 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 vérifier 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

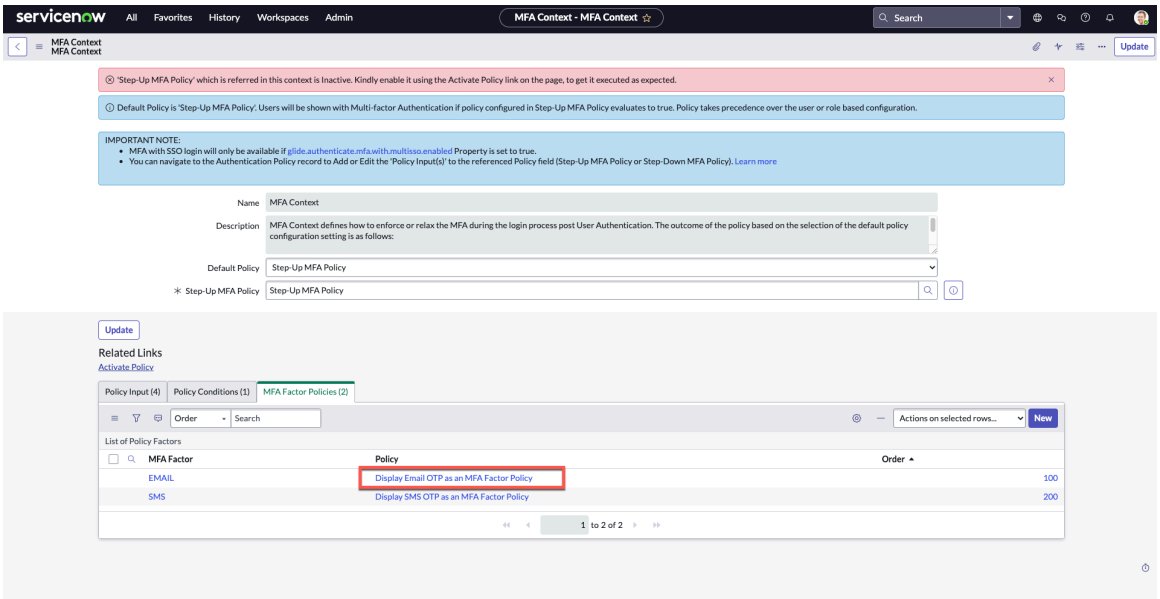
Procédure

1. Accédez à la **Tous** > **Authentification multifacteur** > **Contexte MFA**.
2. Cliquez sur **l'onglet Politiques de facteur MFA** .

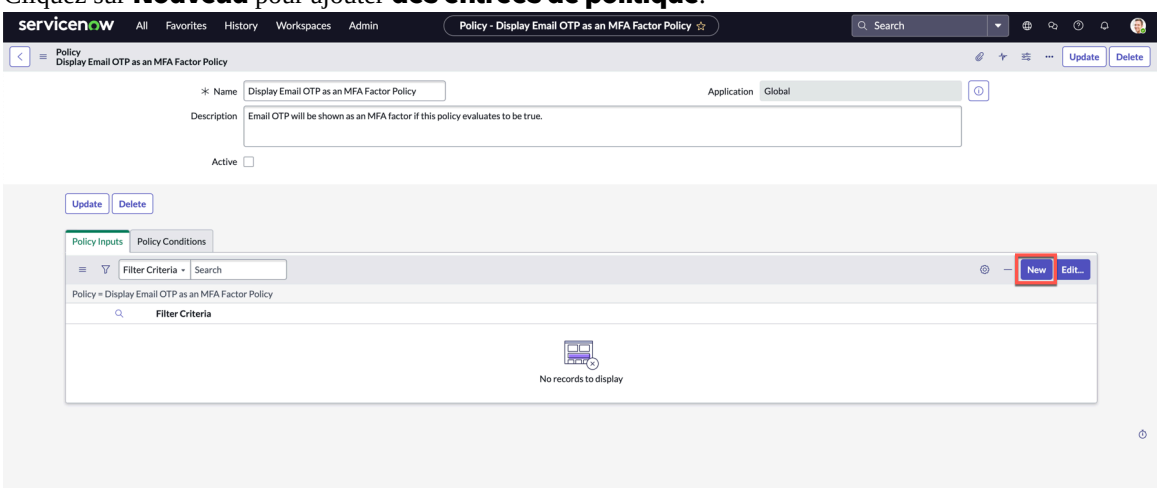
> **Remarque :**
> **L'option E-mail** en tant que **facteur MFA avec une politique** est disponible par défaut. Vous pouvez modifier la politique et spécifier les entrées et les conditions de la politique.

3. Sélectionnez **Afficher l'OTP d'e-mail en tant que politique de facteur MFA**.

Traduction automatique



4. Cliquez sur **Nouveau** pour ajouter **des entrées de politique**.

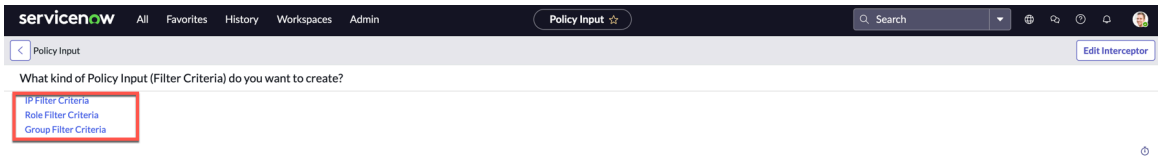


5. Sélectionnez les critères de filtre que vous souhaitez créer.

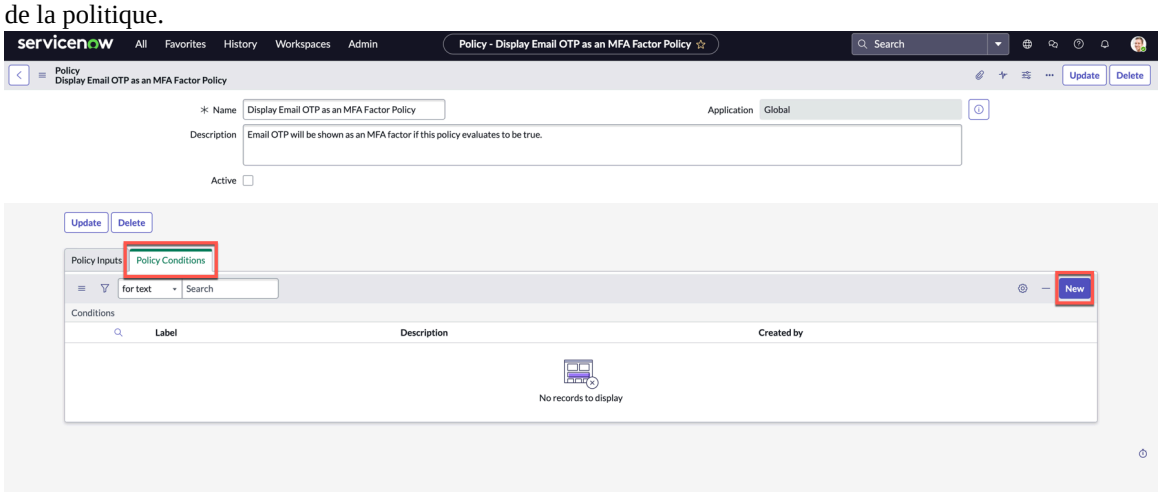
   Les types de critères de filtre suivants sont disponibles :

   - Critère de filtre d'adresses IP
   - Critère de filtre de rôle
   - Critères de filtre de groupe

   Par exemple, Critères de filtre de rôle.



6. Cliquez sur **Critères de filtre de rôle.**
7. 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
8. Sur la page Politique - Afficher l'OTP d'e-mail en tant que politique de facteur MFA, cliquez sur Conditions de la politique.



9. Cliquez sur **Nouveau** pour ajouter des **conditions de politique**.
10. 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) qui est utilisée pour évaluer les demandes d'authentification. Sélectionnez la politique de critères de filtre basée sur le rôle qui a été créée pour la condition.

11. Cliquez sur **Envoyer**.
12. **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 OR de toutes les conditions de politique. Cela signifie que la police 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 si les conditions spécifiées pour le rôle correspondent, le facteur MFA des e-mails est affiché comme une option d'authentification pour les utilisateurs.

Utilisation de l'authentification multifacteur (MFA)

Découvrez comment utiliser les 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.

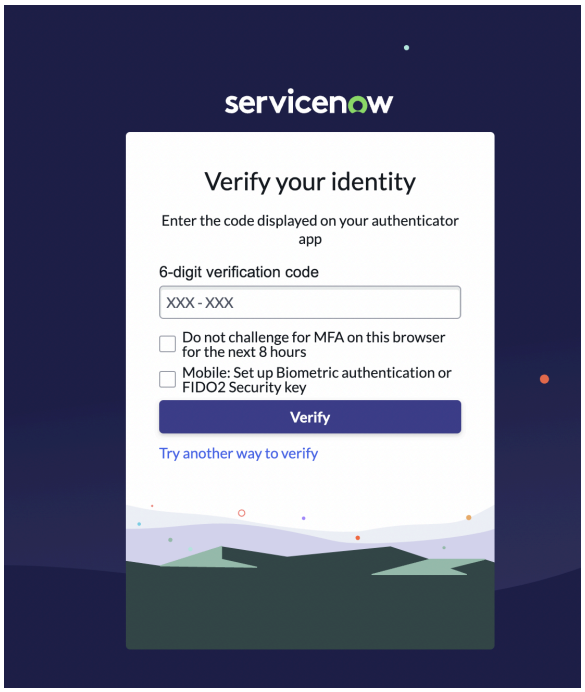
Remarque :
pour en savoir plus sur le changement de comportement spécifique du navigateur, consultez cet article de la base de connaissances .

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 obtenir plus de détails sur le processus de connexion avec l'authentification MFA, consultez Connectez-vous avec l'authentification multifacteur.

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

Validation avec l'application d'authentification

d'authentification. Pour en savoir plus sur cette configuration, consultez Configurer l'authentification multifacteur lors de la connexion initiale.



Saisissez le code affiché sur votre application d'authentification pour vous connecter.

Enregistrer un appareil d'authentification

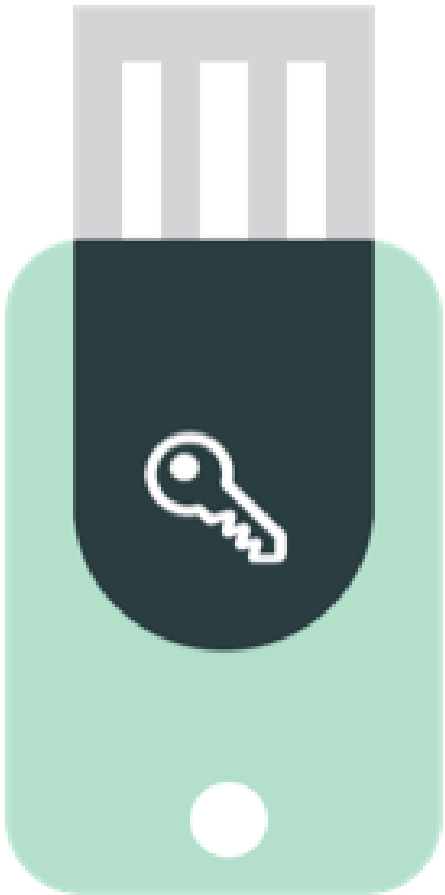
Une fois que vous avez configuré une application d'authentification, vous pouvez enregistrer d'autres méthodes d'authentification.

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.

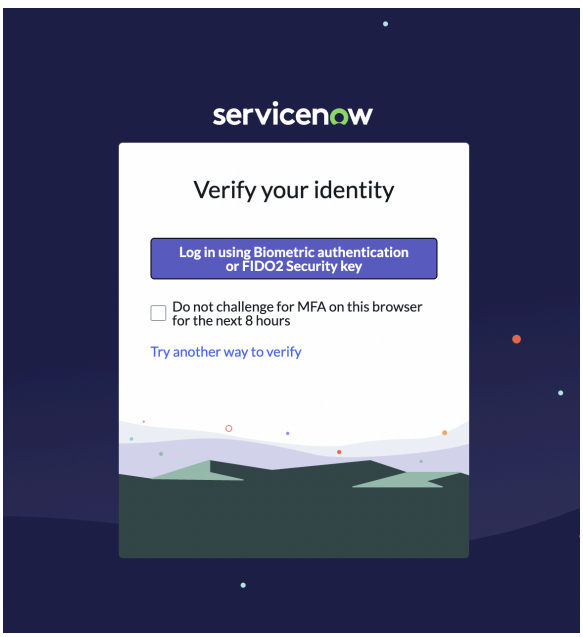
Authentificateurs de clé matérielle

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.



Traduction automatique

Validation avec biométrie ou clé matérielle



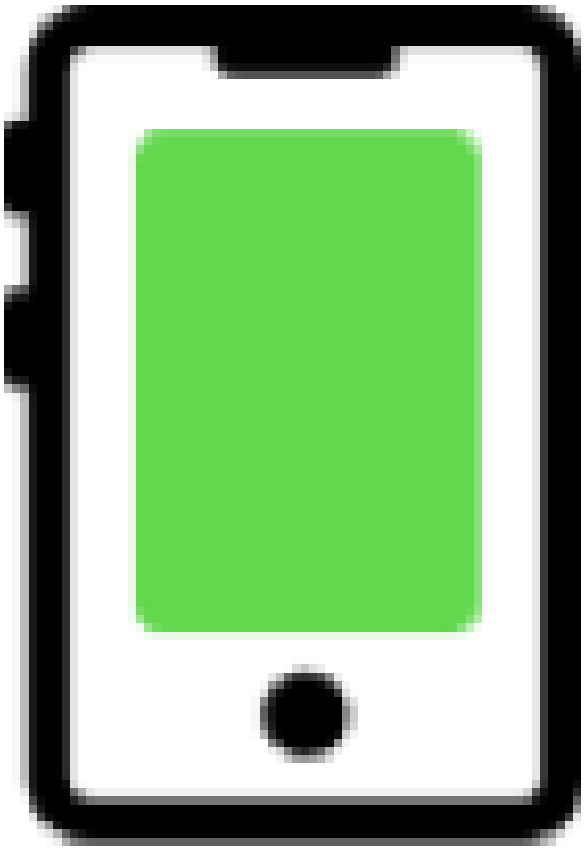
Utilisez la biométrie ou une clé de sécurité pour vous connecter.

Enregistrer un numéro de téléphone pour le mot de passe à usage unique

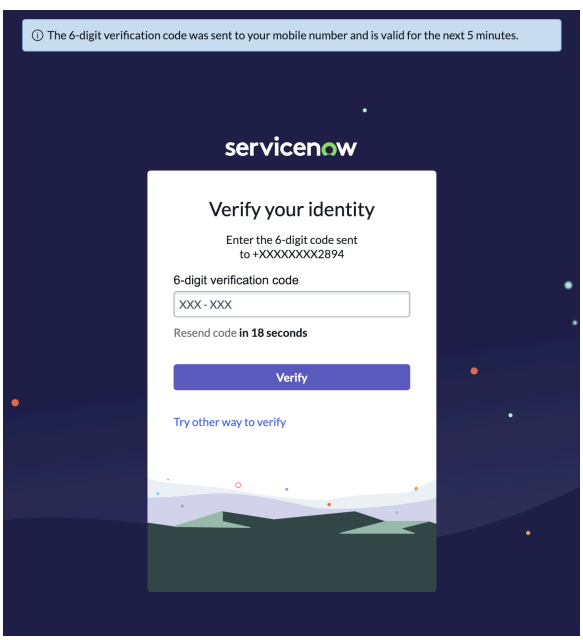
SMS

L'administrateur configure l'instance ServiceNow pour exiger des utilisateurs qui tentent de s'y connecter d'utiliser un mot de passe à usage unique 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.



Validation par SMS



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

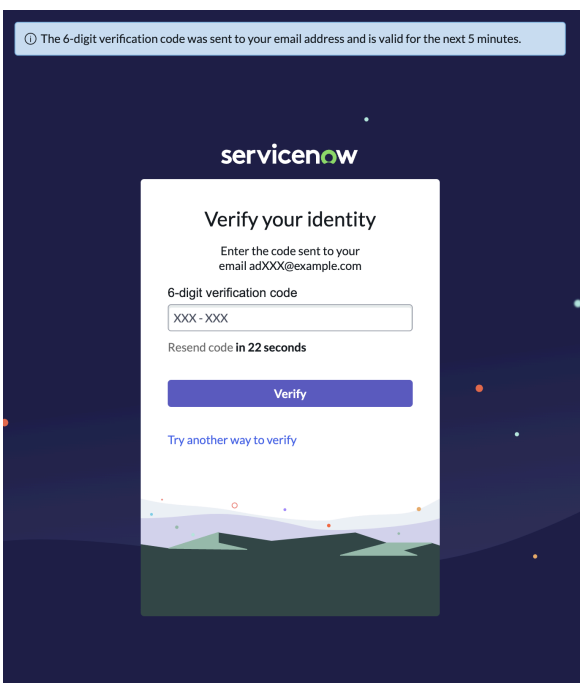
Enregistrer une adresse e-mail pour le mot de passe à usage unique

Adresse e-mail

L'administrateur configure l'instance ServiceNow pour exiger des utilisateurs qui tentent de s'y connecter d'utiliser un mot de passe à usage unique basé sur une adresse e-mail.

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 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 lors de la connexion initiale

Si votre administrateur a activé l'authentification multifacteur sur votre profil, mais que vous n'avez pas encore configuré l'application, vous pouvez le faire lors de la connexion.

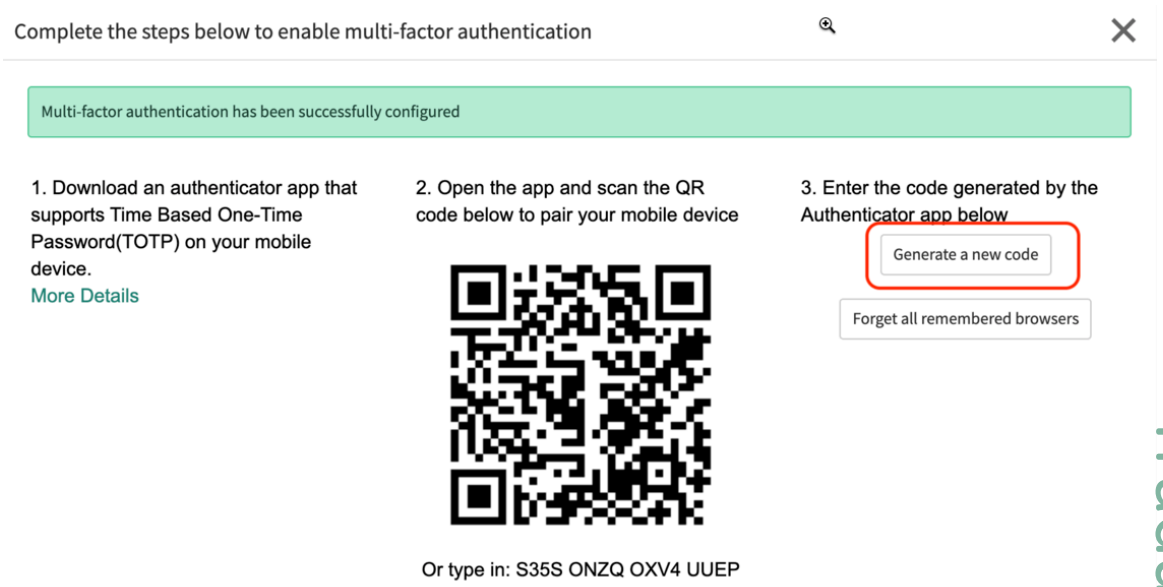
Avant de commencer

Rôle requis : aucun

Traduction automatique

Procédure

1. Connectez-vous à votre instance à l'aide de vos nom d'utilisateur et mot de passe.
   L'écran de configuration de l'authentification multifacteur intercepte votre connexion.



2. 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 autorisé par votre administrateur. Enfin, vous devez configurer l'authentification multifacteur.
3. Prenez une photo du code QC avec l'application Google Authenticator ou saisissez manuellement la chaîne dans l'application.
4. Entrez le code et cliquez sur **Coupler l'appareil et connectez-vous**.

   L'application répond avec un code à six chiffres qui s'actualise toutes les 30 secondes. Si vous avez saisi le code correct, un message s'affiche pour vous indiquer que l'authentification multifacteur est configurée. Si vous avez entré un code non valide, recherchez à nouveau le code sur votre équipement mobile, car il a peut-être été actualisé, puis saisissez le code que vous voyez.

> **Remarque :**
> Pour que le code fonctionne correctement, l'heure système de votre ordinateur doit être dans le même fuseau horaire que l'heure de votre équipement mobile.

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

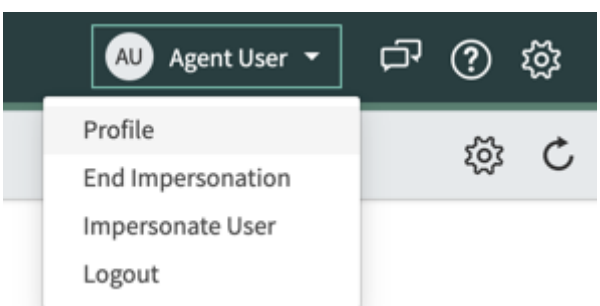
L'authentification multifacteur doit être activée sur votre instance.

Remarque :
Votre administrateur peut exiger que vous utilisiez l'authentification multifacteur. Dans ce cas, vous y êtes automatiquement invité lorsque vous vous connectez. Consultez Configurer l'authentification multifacteur lors de la connexion initiale. Utilisez la procédure ci-dessous si votre administrateur vous autorise à activer l'authentification multifacteur.

Procédure

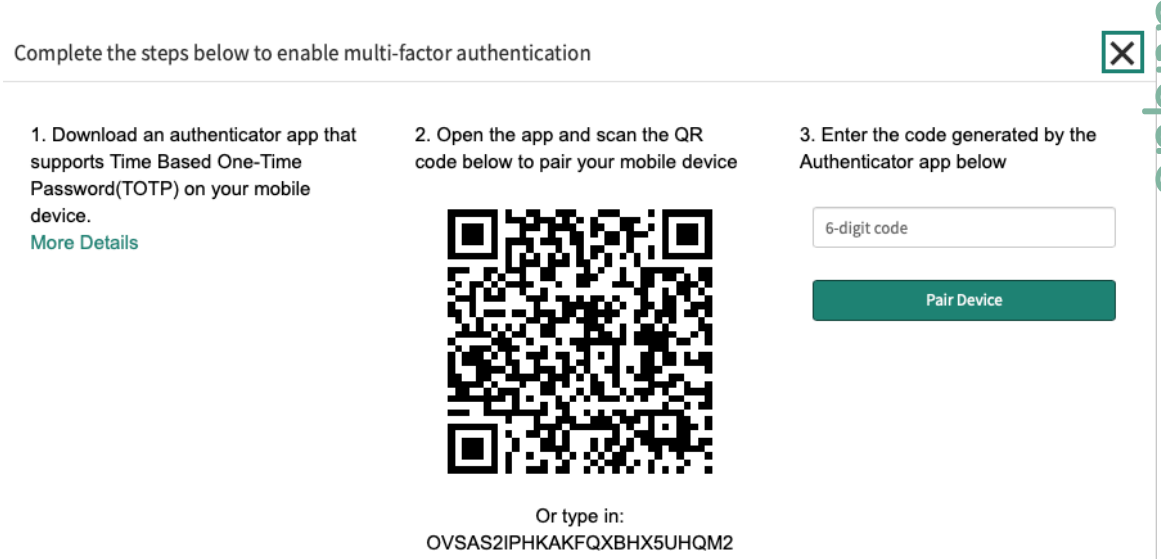
1. Accédez à la **Tous** > **Libre-service** > **Mon profil**.

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 **Authentification multifacteur** ou **Activer la récupération de compte** dans la section **Liens connexes** .
3. Suivez les instructions à l'écran pour enregistrer une application d'authentification.
ServiceNow prend en charge les applications Mobile et les authentificateurs d'extension de navigateur. Pour en savoir plus sur ces applications, reportez-vous à la section Applications d'authentification.

Remarque :
Même si vous envisagez de vous authentifier à l'aide d'une biométrie ou d'une clé matérielle, vous devez d'abord enregistrer une application 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.

Que faire ensuite

Si vous prévoyez d'utiliser une clé matérielle ou un authentificateur biométrique pour vous connecter à votre instance, vous pouvez maintenant enregistrer ces authentificateurs. Pour en savoir plus, reportez-vous aux sections Enregistrer un authentificateur biométrique et Enregistrer une clé de sécurité matérielle.

Connectez-vous avec l'authentification multifacteur

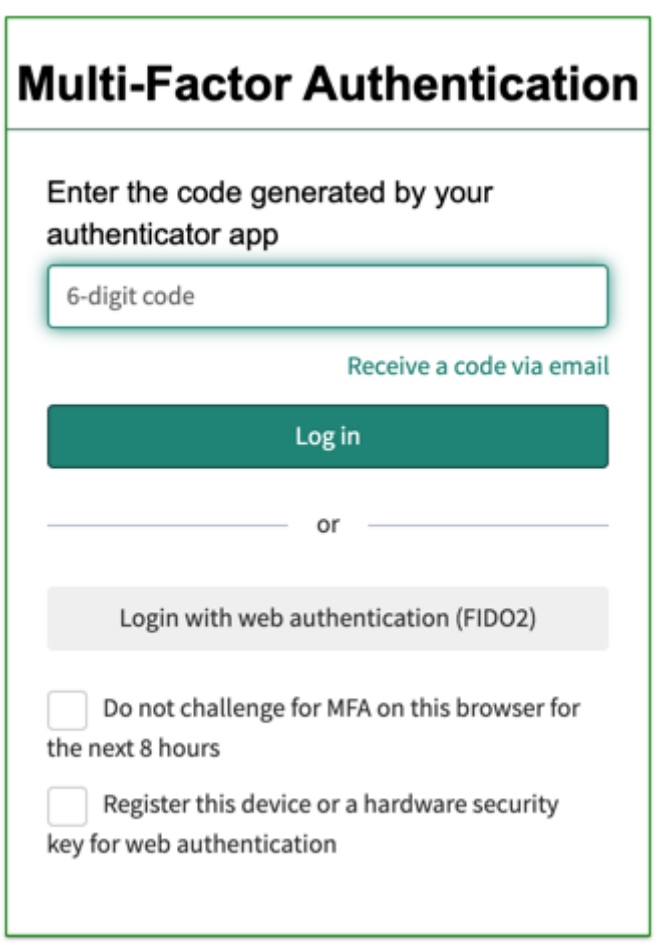
Une fois l'authentification multifacteur activée pour votre profil d'utilisateur, vous pouvez vous connecter en ajoutant le code d'accès fourni par l'application Google Authenticator.

Avant de commencer

L'authentification multifacteur doit être activée 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 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**.
   L'écran d'authentification multifacteur s'affiche.



4. Ouvrez l'authentificateur sur votre appareil mobile ou votre extension de navigateur et notez le numéro.

Remarque :
Ce nombre est actualisé toutes les 30 secondes.

5. Saisissez votre code d'authentification à six chiffres.
6. **Facultatif :** Activez **l'option Ne pas modifier l'authentification multifacteur sur ce navigateur pendant les 8 prochaines heures** pour ignorer l'authentification lors de la connexion pendant les huit heures suivantes.
7. **Facultatif :** Activez **Enregistrer cet appareil ou une clé de sécurité matérielle pour l'authentification Web** afin d'enregistrer un appareil biométrique ou une clé de sécurité matérielle après votre connexion.
8. **Facultatif :** Si vous avez déjà enregistré un scanner biométrique ou une clé matérielle, cliquez sur **Connexion avec authentification Web (FIDO2)** et suivez les instructions pour terminer le processus de connexion.
9. **Facultatif :** Si vous ne vous souvenez pas du code secret ou si vous n'avez pas accès à votre authentificateur, cliquez sur **Recevoir un code par e-mail** .

   L'instance envoie un code secret temporaire à votre adresse e-mail. Vous ne pouvez utiliser ce code secret temporaire qu'une seule fois et il n'est valide que pendant 10 minutes.

   Remarque :
   Vous devez avoir une adresse e-mail configurée dans votre profil d'utilisateur sur l'instance pour recevoir cet e-mail.

10. Cliquez sur **Se connecter**.

Applications d'authentification

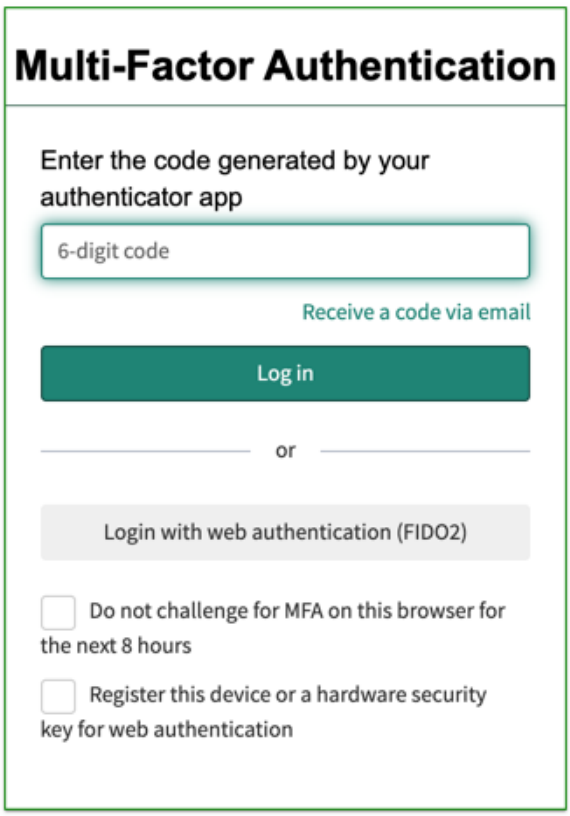
Utilisez des applications d'authentification tierces pour générer des codes d'accès MFA temporaires.

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 l'authentification multifacteur sur votre instance, vous êtes invité à saisir un code secret après avoir saisi votre utilisateur et votre mot de passe pendant la connexion.

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.

Changer l'application d'authentification

Générez un nouveau code pour changer l'application d'authentification sur votre appareil.

Avant de commencer

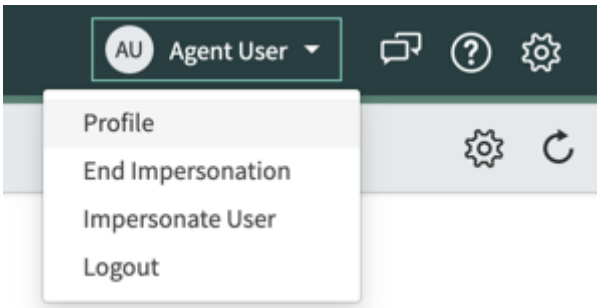
L'authentification multifacteur doit être activée pour votre profil. Vous pouvez l'activer vous-même sur votre profil d'utilisateur ou votre administrateur peut l'activer pour vous.

Rôle requis : aucun

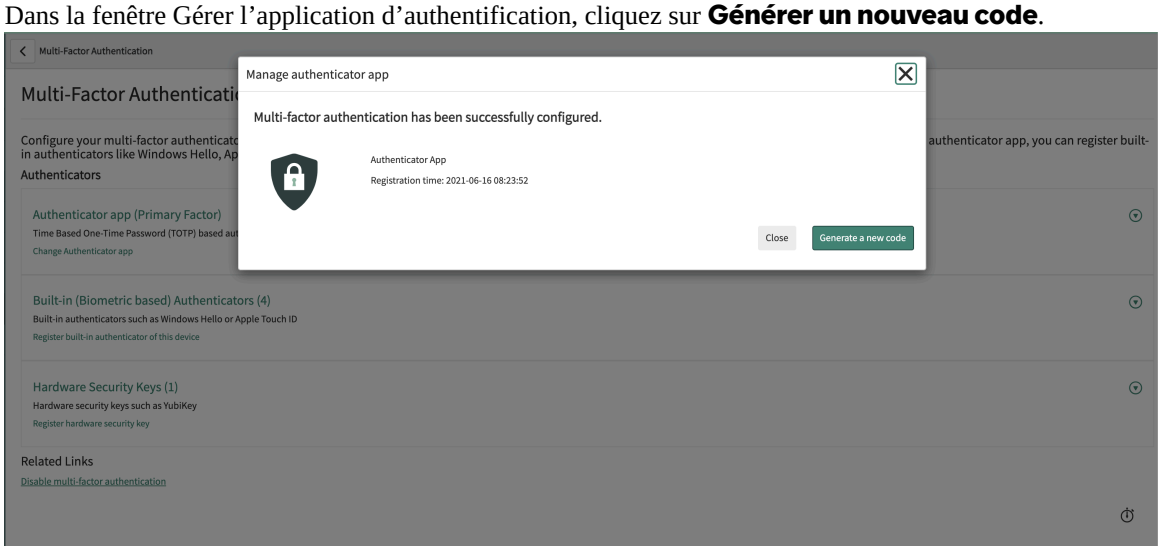
Procédure

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 (facteur primaire),** cliquez sur **Modifier l'application d'authentification**.
4. Dans la fenêtre Gérer l'application d'authentification, cliquez sur **Générer un nouveau code**.



5. Suivez les instructions à l'écran pour enregistrer une application d'authentification avec l'appareil.

Authentification Web

Les utilisateurs peuvent utiliser des clés matérielles ou les lecteurs biométriques de leur appareil (FIDO2) pour s'authentifier auprès d'une instance.

Traduction automatique

Clés matérielles

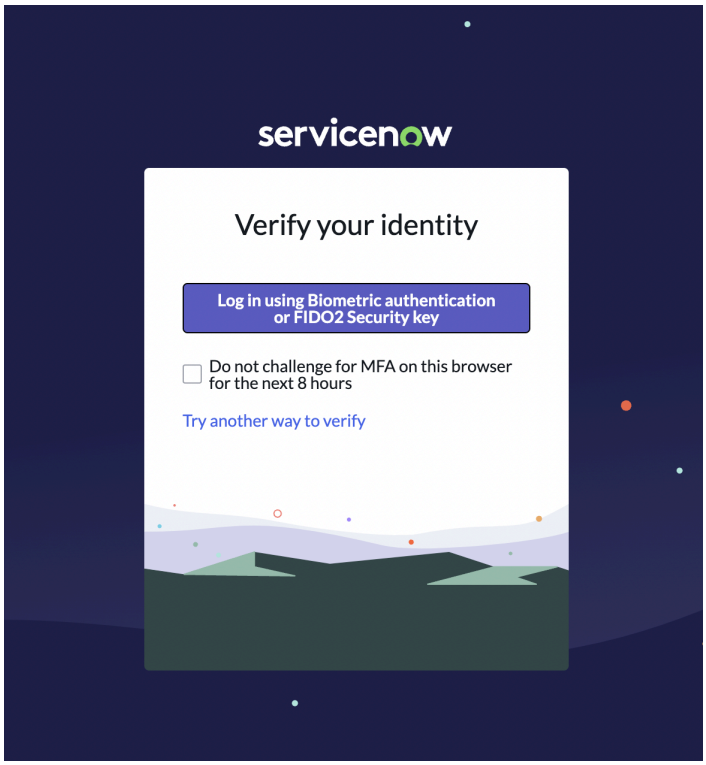
Les clés matérielles sont des matériels physiques que vous pouvez utiliser pour vous authentifier. Les clés matérielles sont insérées dans un port de votre appareil pour fournir une authentification. Pour en savoir plus sur l'enregistrement des clés matérielles, reportez-vous à la section Enregistrer 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 en savoir plus sur l'enregistrement des authentificateurs biométriques, reportez-vous à la section Enregistrer un authentificateur biométrique.

Traduction automatique

Choisissez le deuxième facteur que vous souhaitez authentifier et authentifiez auprès de votre instance.



Pour configurer le module d'extension d'authentification Web, reportez-vous à la section Activer le module d'extension d'authentification Web.

Activer le module d'extension d'authentification Web

Le module d'extension Intégration - Authentification Web doit être activé pour l'authentification Web (FIDO2).

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 Integration - Web Authentication** (com.snc.integration.webauthn) 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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

Enregistrer un authentificateur biométrique

Enregistrez un authentificateur biométrique à utiliser dans le cadre de votre connexion à l'authentification multifacteur.

Avant de commencer

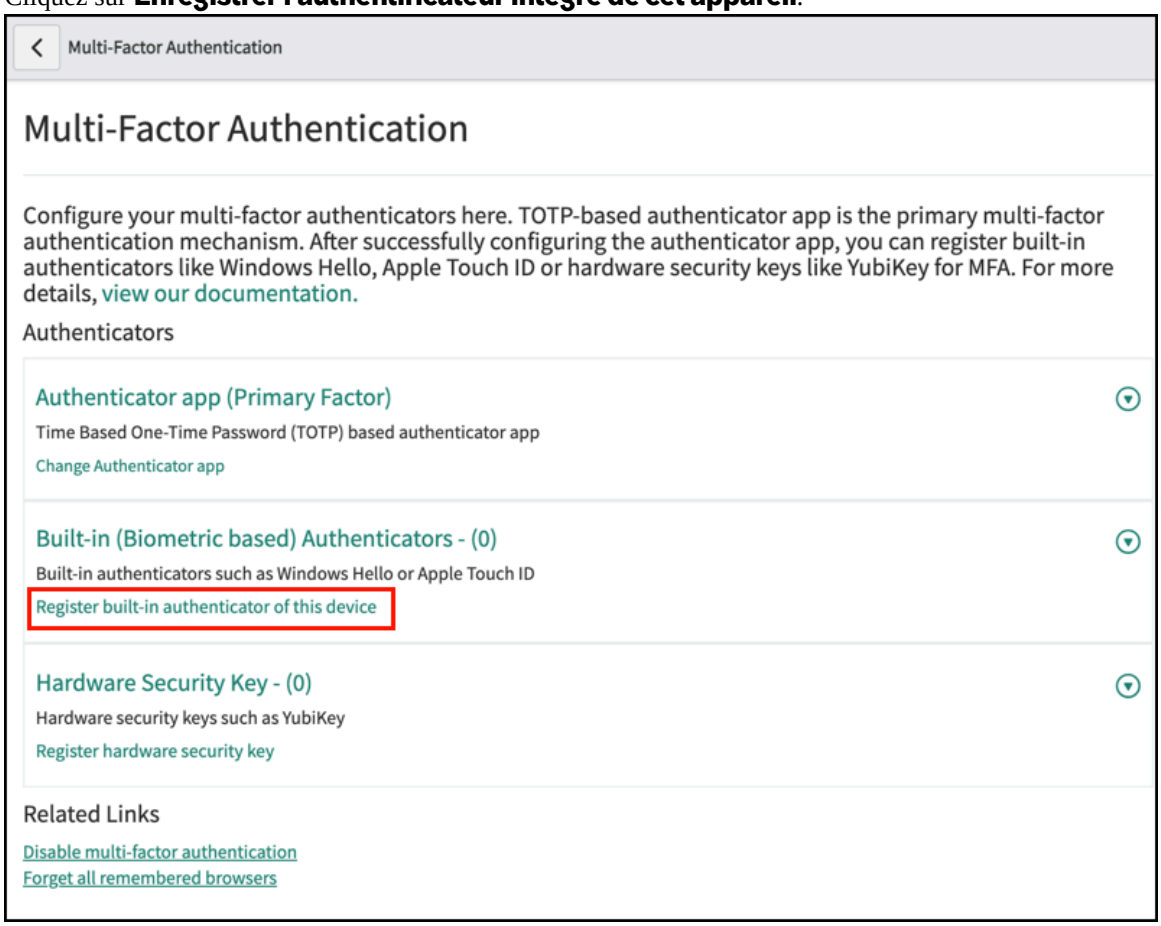
Rôle requis : aucun

Remarque :

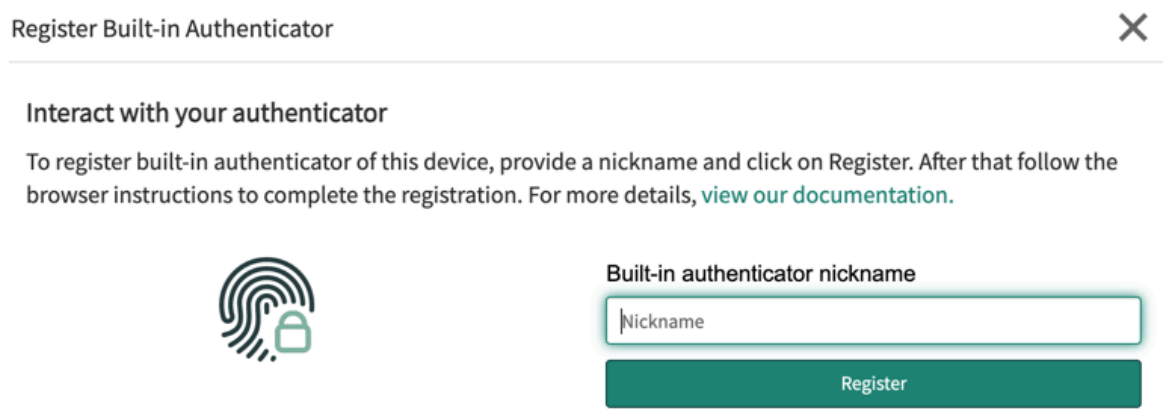
Les utilisateurs doivent d'abord configurer une application d'authentification avant de configurer un authentificateur biométrique. Pour en savoir plus sur la configuration de l'application d'authentification, reportez-vous à la section Configurer l'authentification multifacteur sur votre profil d'utilisateur.

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'authentificateur intégré de cet appareil**.

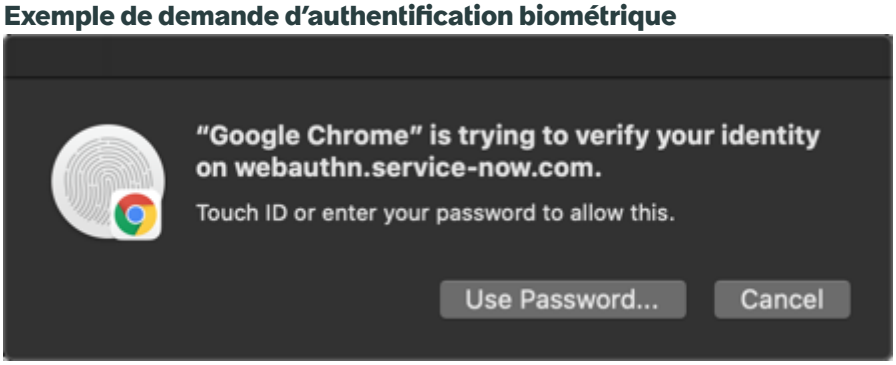


4. Entrez un surnom pour votre authentificateur et cliquez sur **Enregistrer**.



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



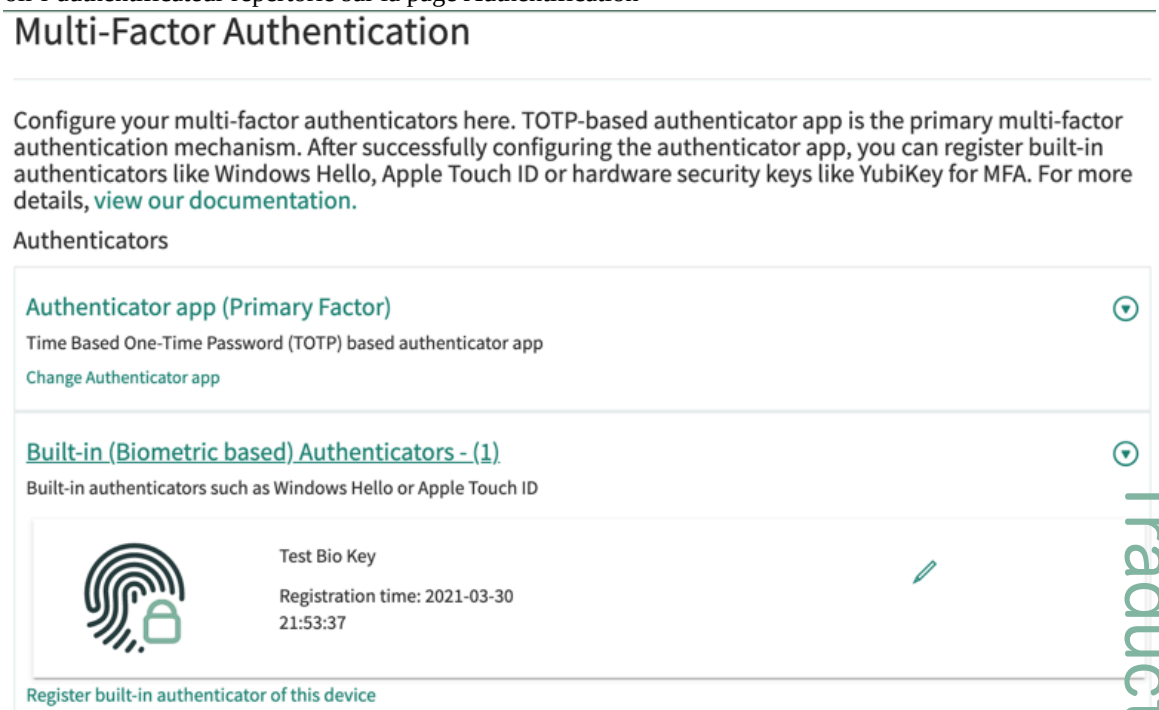
   Une fois l'authentification réussie, une fenêtre de confirmation s'affiche.

6. Fermez la fenêtre de confirmation.

Traduction automatique

Résultats

Votre authentificateur biométrique est enregistré. Vous pouvez maintenant voir l'authentificateur répertorié sur la page Authentification multifacteur.



Enregistrer une clé de sécurité matérielle

Enregistrez une clé matérielle à utiliser dans le cadre de votre connexion à l'authentification multifacteur.

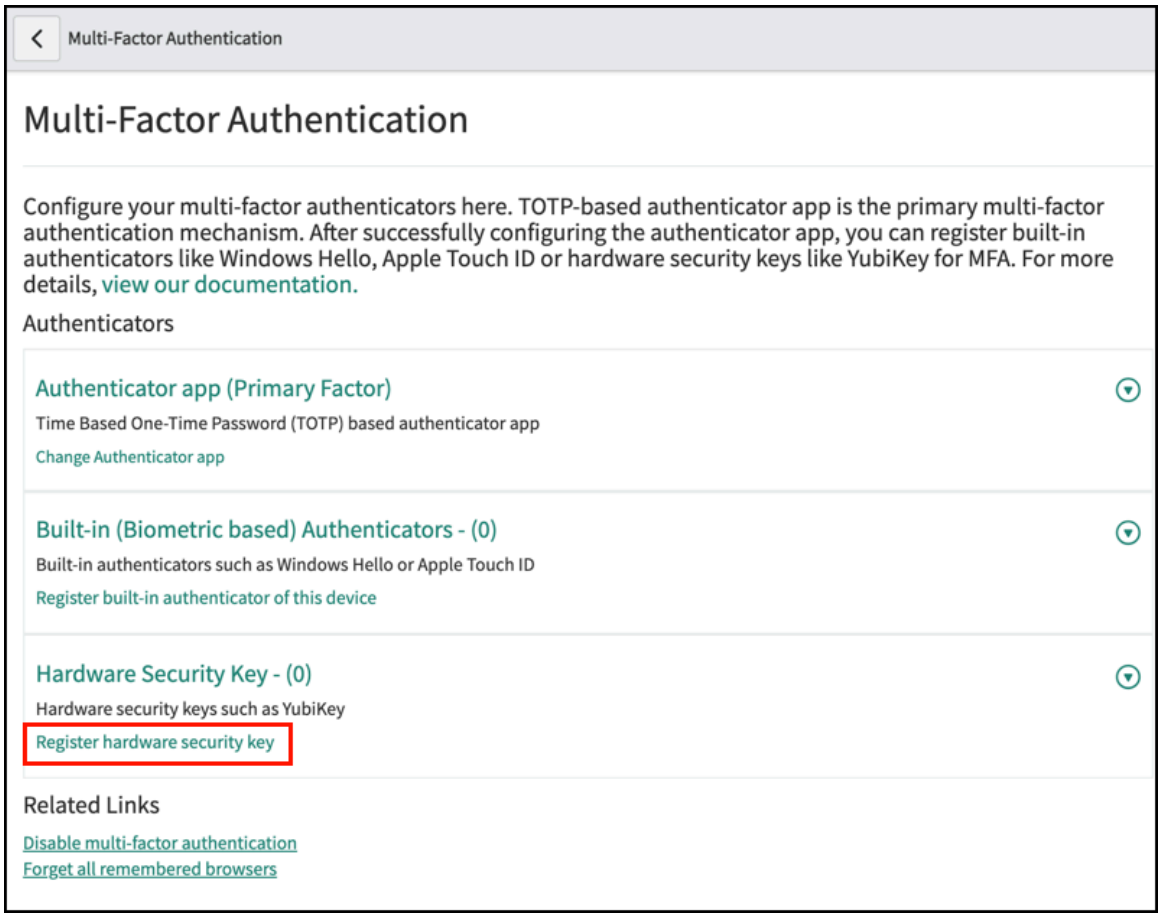
Avant de commencer

Rôle requis : aucun

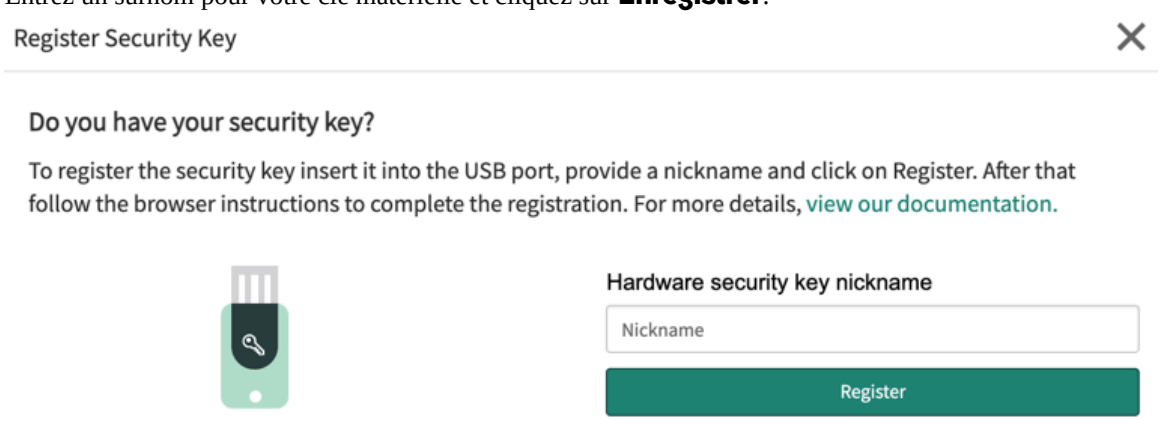
Remarque :
Les utilisateurs doivent d'abord configurer une application d'authentification avant de configurer une clé matérielle. Pour en savoir plus sur la configuration de l'application d'authentification, reportez-vous à la section Configurer l'authentification multifacteur sur votre profil d'utilisateur.

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.
6. Fermez la fenêtre de confirmation.

Résultats

Votre clé matérielle est enregistrée. Vous pouvez maintenant voir la clé répertoriée dans la page Authentification multifacteur.

Authentification multifacteur avec Single Sign-On

Configurez l'authentification multifacteur (MFA) avec un fournisseur SSO (Single Sign-On) 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, le besoin d'une authentification sécurisée est renforcé.

L'authentification MFA associée à l'authentification unique offre une sécurité renforcée pour votre instance. Cette option offre la flexibilité nécessaire pour activer l'authentification multifacteur sous condition pour les utilisateurs.

Remarque :

- ServiceNow La MFA est appliquée après que l'utilisateur a été redirigé après l'authentification réussie auprès du fournisseur d'identité.
- L'authentification MFA n'était pas appliquée avec l'authentification unique 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 uniquement à ces utilisateurs. De cette façon, vous pouvez ajouter des capacités d'authentification supplémentaires et contrôler l'accès de vos utilisateurs.

Pour la connexion basée sur SSO telle que SAML, OpenID Connect et Digest, vous pouvez appliquer MFA pour l'authentification.

L'authentification MFA avec SSO peut être configurée à la demande en fonction de vos besoins. À l'aide de schémas d'authentification et de fournisseurs d'identité, vous pouvez appliquer l'authentification multifacteur pour des utilisateurs spécifiques avec un mécanisme de connexion spécifique.

Vous pouvez appliquer la MFA dans les conditions suivantes :

- Schéma d'authentification
- Fournisseur d'identité

La MFA avec SSO est proposée dans le cadre du module d'extension Adaptive Authentication (com.snc.adaptive_authentication). Pour en savoir plus sur la configuration de l'authentification adaptative, reportez-vous à Authentification adaptative.

Configurer MFA avec SSO

Appliquez la MFA avec SSO pour vos utilisateurs au sein ou en dehors de votre organisation.

Avant de commencer

L'authentification MFA avec fonctionnalité SSO est proposée dans le cadre du module d'extension Adaptive Authentication (com.snc.adaptive_authentication). Vous devez activer la propriété d'authentification adaptative pour utiliser MFA avec la fonctionnalité SSO. Pour en savoir plus sur la configuration de l'authentification adaptative, reportez-vous à Authentification adaptative.

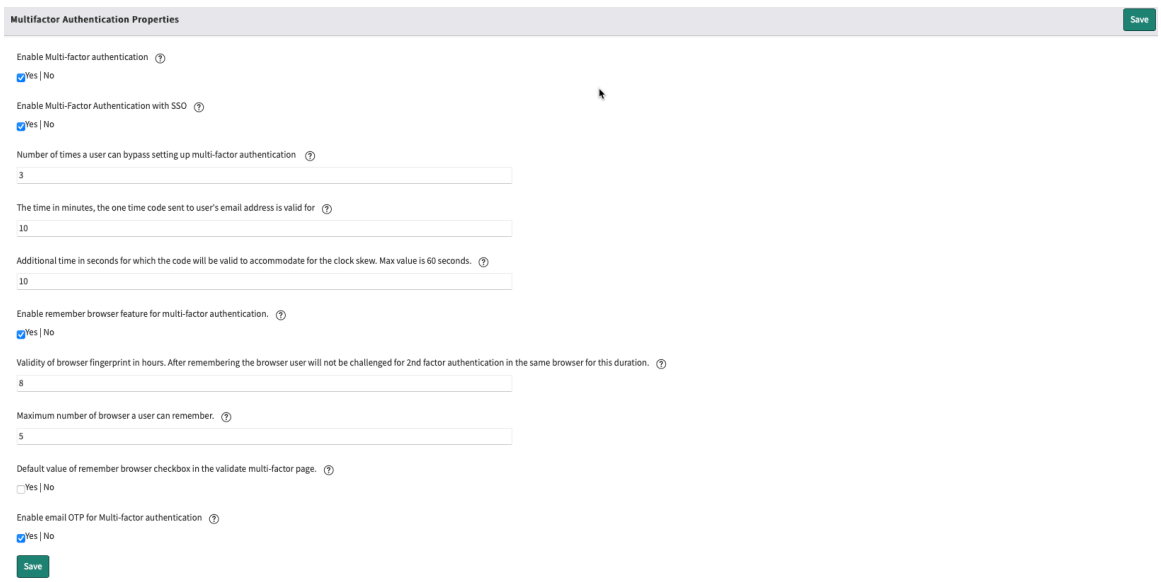
Remarque :

MFA avec connexion SSO est disponible si la `glide.authenticate.mfa.with.multisso.enabled` propriété est définie sur **vrai**.

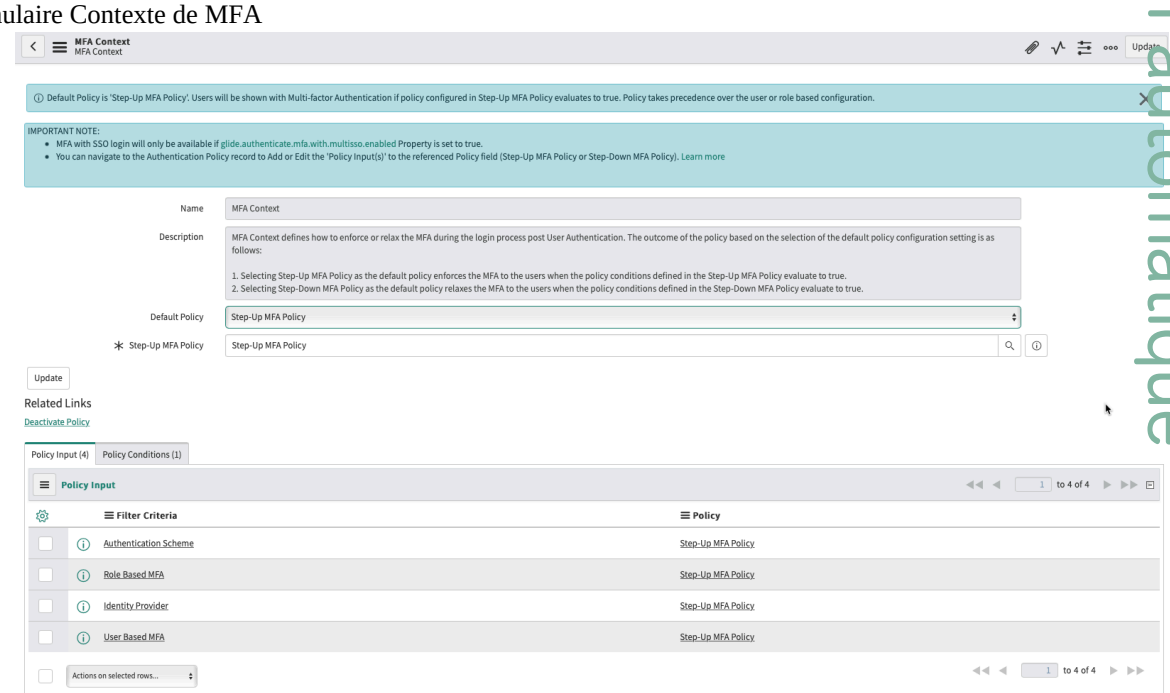
Rôle requis : admin

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 de MFA



s'affiche.

> **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 MFA donne lavaleur vrai**. La politique a priorité sur la configuration basée sur l'utilisateur ou le rôle.

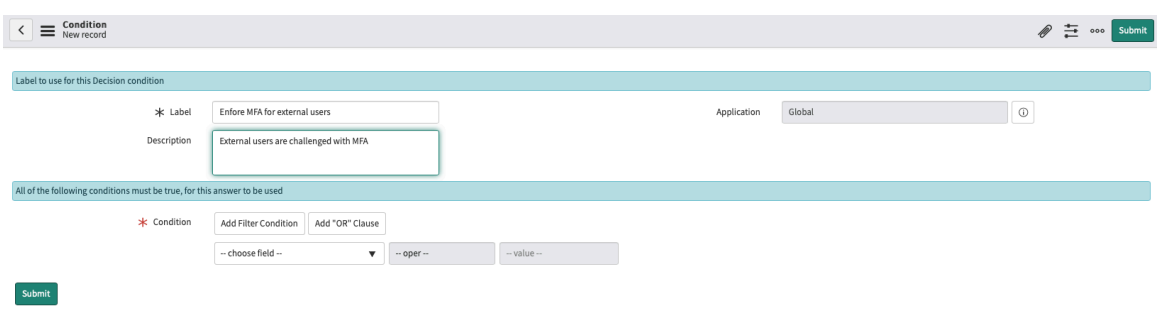
5. **Facultatif :** Pour modifier une politique, revenez à l'enregistrement de politique d'authentification, modifiez les conditions, puis revenez en arrière.

Lorsque vous accédez à l'enregistrement Politique d'authentification, vous pouvez ajouter ou modifier les « Entrées de politique » aux champs de politique **référencés, Politique de MFA ascendante** ou **Politique de MFA descendante**.

6. Pour définir une nouvelle condition de police, cliquez sur **Conditions de la police**.
7. Cliquez sur **Nouveau**.
8. Renseignez les champs du formulaire.

Formulaire de conditions

Champs	Description
Étiquette	Nom unique de la condition que vous souhaitez créer pour l'étiquette.
Description	Description des conditions de la politique.
Conditions	Type de condition que vous souhaitez appliquer à 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.



Example

Pour configurer vos conditions, prenez l'exemple suivant. Supposons que vous souhaitez le schéma d'authentification avec le fournisseur d'identité comme condition pour les utilisateurs externes. Vous pouvez définir les conditions comme suit :

a. Sélectionnez **Schéma d'authentification** et définissez les critères sur **Authentification unique** ou **Nom d'utilisateur et mot de passe**.

   Sur la base de cette sélection, l'utilisateur reçoit une connexion basée sur l'authentification unique ou un formulaire de connexion spécifiant le nom d'utilisateur et le mot de passe.

b. Sélectionnez **Fournisseur d'identité** et spécifiez le fournisseur en tant qu'enregistrement IdP pour lequel vous souhaitez activer l'authentification multifacteur. Par exemple, **Okta**.

Selon cette sélection, si l'utilisateur se connecte avec SSO, il n'est pas confronté à la MFA. En revanche, si l'utilisateur se connecte à l'aide Oktade , il est confronté à un problème avec MFA.

9. Cliquez sur **Envoyer**.

Information associée

Authentification adaptative

Activer le module d'extension MFA

Authentification multifacteur avec Single Sign-On

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.

L'intégration prend en charge n'importe quelle combinaison de méthodes d'authentification locales et externes sur une seule instance :

- SAML 2.0
- Authentification Digest
- OpenID Connexion

Vous devez effectuer plusieurs étapes pour configurer l'authentification unique (SSO) de plusieurs fournisseurs, notamment la configuration des propriétés, la création de fournisseurs d'identité (IdP) et la configuration des utilisateurs pour l'utilisation de la SSO.

Par exemple, une entreprise dispersée à l'échelle mondiale peut avoir besoin d'un fournisseur SSO pour ses employés, d'un autre pour ses fournisseurs et d'une authentification de base de données locale pour ses administrateurs. Alternativement, une entreprise peut implémenter des solutions d'authentification par jeton SAML 2.0 et Digest sur la même instance.

Propriétés, tables et scripts de l'authentification unique (SSO) de plusieurs fournisseurs

Le module d'extension Integration - Multiple Provider Single Sign-On Installer inclut les propriétés système, les tables et les scripts suivants.

Propriétés

L'authentification unique de plusieurs fournisseurs ajoute les propriétés système suivantes.

Propriétés de l'authentification unique (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.

Propriétés de l'authentification unique (SSO) de plusieurs fournisseurs (suite)

Nom	Description
	• Type : true | false • Valeur par défaut : false
glide.authenticate.multisso.enabled	Active (vrai) ou désactive (faux) l'authentification unique (SSO) de plusieurs fournisseurs. • Type : true | false • Valeur par défaut : false **Remarque :** définir cette propriété sur faux ne désactivera pas l'authentification unique 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, 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 la récupération de compte.
glide.authenticate.multissov2_feature.enabled	Cette propriété détermine si la version MultiSSOv2 est activée dans l'instance.

Tables

L'authentification unique (SSO) de plusieurs fournisseurs ajoute les tables suivantes.

Tables SSO de plusieurs fournisseurs

Nom	Description
Propriétés SSO [sso_properties]	Stocke les données pour chaque IdP, schéma, données SSO communes, etc.
Propriétés SAML 2 Update 1 [saml2_update1_properties]	Stocke les données pour les configurations SAML 2.0 Update 1 telles que les certificats SAML.
Propriétés de synthèse [digest_properties]	Stocke les données pour les configurations d'authentification par jeton Digest.
Fédération SSO [sso_federation]	Stocke les données pour chaque fédération SSO.
Fournisseur d'identité OIDC [oidc_identity_provider]	Stocke les données pour les fournisseurs d'identité basés sur Open ID Connect.

Scripts

L’authentification unique 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 d’authentification unique défini pour chaque 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.
MultiSSO_OIDC_custom	Permet à un utilisateur de définir un script Single Sign-on 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 d’appel client pour l’authentification unique (SSO) de plusieurs fournisseurs.
MultiSSO_DigestedToken	Fournit une logique 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 multilocataire.

Activer le module d’extension SSO de plusieurs fournisseurs

Cette intégration nécessite le module d’extension Integration - Multiple Provider Single Sign-On Installer (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. Trouvez le module d’extension Integration - Multiple Provider Single Sign-On Installer (com.snc.integration.sso.multi.installer) 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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

> **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>.

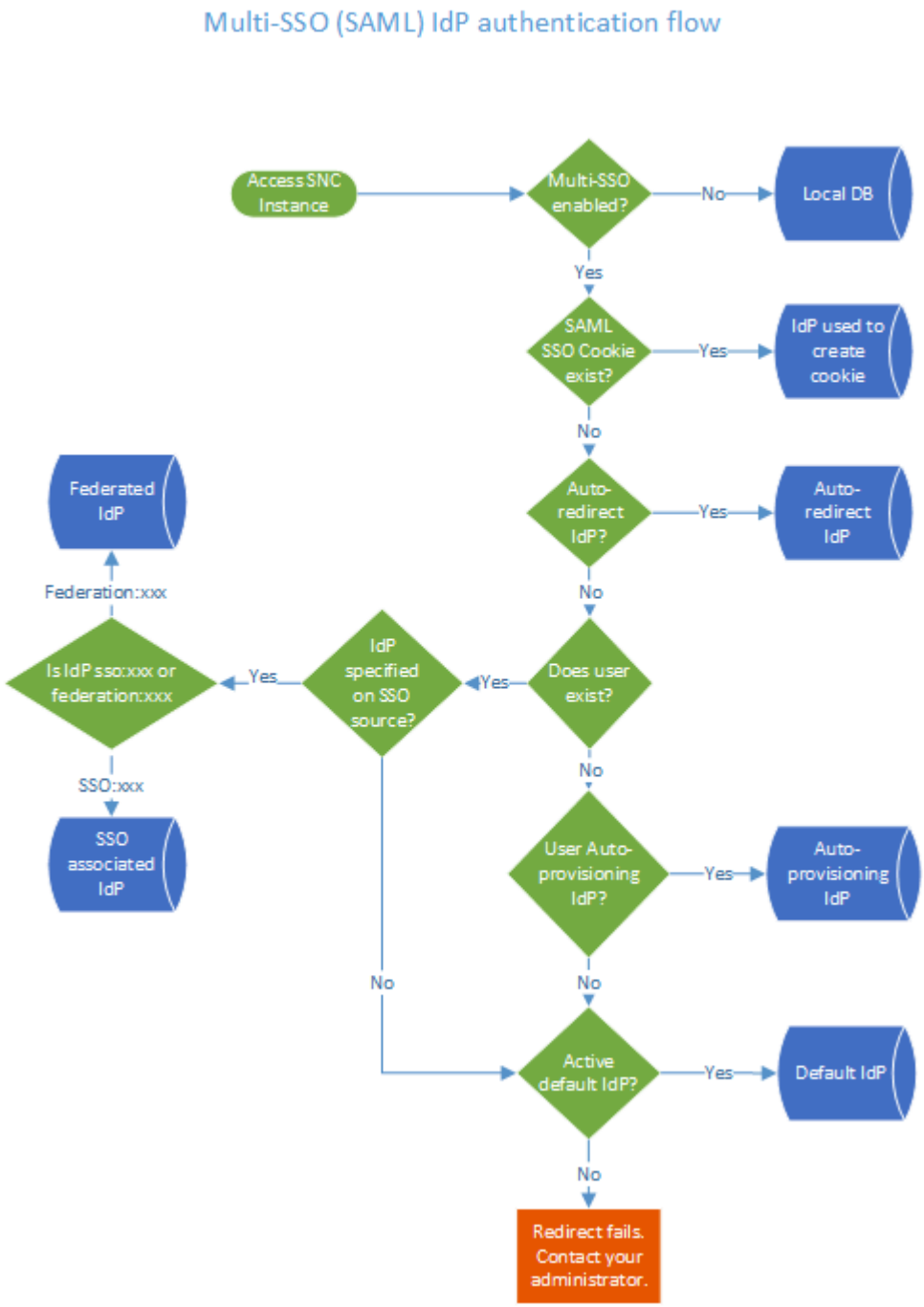
Configurations de l’authentification unique (SSO) de plusieurs fournisseurs

Vous devez effectuer plusieurs étapes pour configurer l’authentification unique (SSO) de plusieurs fournisseurs, notamment la configuration des propriétés, la création de fournisseurs d’identité (IdP) et la configuration des utilisateurs pour l’utilisation de la SSO.

Flux d’authentification IdP pour l’authentification de plusieurs fournisseurs SSO (SAML)

Décrit les différentes entités qui peuvent authentifier un utilisateur via l’authentification unique (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).



Traduction automatique

Local DB

Si la SSO à fournisseurs multiples n'est pas activée, l'authentification est dirigée vers une base de données locale.

SAML SSO Cookie IdP

Si un cookie SAML SSO existe, l'IdP spécifié avec ce cookie authentifie l'utilisateur.

IdP de redirection automatique

Si l'IdP de redirection automatique est activé, cet IdP authentifie l'utilisateur.

IdP fédéré

Si le navigateur de l'utilisateur est redirigé vers l'écran de connexion d'autorisation externe (login_locate_sso.do) et que l'utilisateur existe dans la table des utilisateurs avec l'IdP défini dans le champ **Source SSO** en tant que fédération : xxx, l'IdP fédéré authentifie l'utilisateur.

IdP associé

Si le navigateur de l'utilisateur est redirigé vers l'écran de connexion d'autorisation externe (login_locate_sso.do) et que l'utilisateur existe dans la table des utilisateurs avec l'IdP défini dans le champ **Source SSO** en tant que 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 d'autorisation externe (login_locate_sso.do) et que l'utilisateur n'existe pas dans la table des utilisateurs, mais que la mise en service automatique est activée, l'IdP de mise en service automatique authentifie l'utilisateur.

Remarque :
Si plusieurs IdP d'approvisionnement automatique sont activés, l'utilisateur peut choisir l'IdP d'approvisionnement automatique qu'il peut utiliser.

IdP par défaut

Si le navigateur de l'utilisateur est redirigé vers l'écran de connexion d'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 ou de la société source SSO et il existe un IdP par défaut actif

l'IdP par défaut authentifie alors l'utilisateur.

Configurer les propriétés de l'authentification unique (SSO) de plusieurs fournisseurs

Configurez les propriétés SSO et ajoutez également une propriété à la table Propriétés système pour configurer une liste d'inclusion IdP.

Avant de commencer

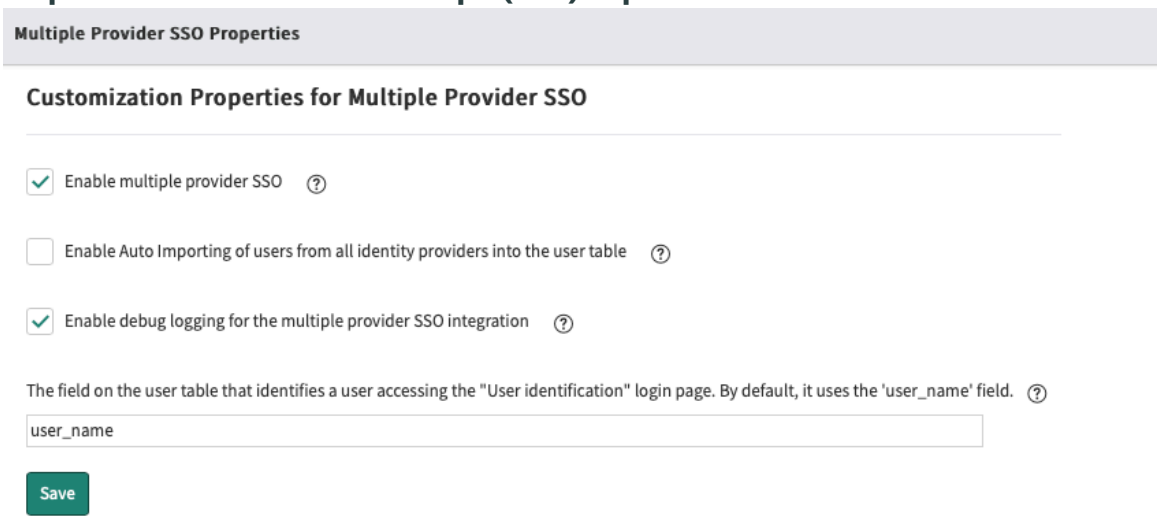
Rôle requis : admin

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 des utilisateurs avec les utilisateurs dans l'IdP, sélectionnez l'option **Activer l'importation automatique** .
   Pour plus d'informations sur la mise à jour de la table utilisateur, reportez-vous à Administrer la mise en service des utilisateurs SAML.
4. Pour activer l'affichage des messages de débogage en bas du cadre de contenu, cochez la case **Activer la journalisation du débogage pour l'intégration de l'authentification unique (SSO) de plusieurs fournisseurs** .
   Si la case est cochée, la fonctionnalité de journalisation de débogage ralentit les performances et utilise de l'espace disque pour générer des journaux.
5. Dans la propriété **Champ de la table utilisateur qui identifie un utilisateur accédant à la page de connexion 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**.

Propriétés de l'authentification unique (SSO) de plusieurs fournisseurs



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 Digest.

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 jetons 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.
3. Pour créer un fournisseur d'identité, cliquez sur **Nouveau**.

- Pour les configurations de jetons Digest : Cliquez sur **SSO Digest** et entrez les propriétés Digest pour l'authentification unique (SSO) 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 entrez 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 actif.

   Remarque :
   Le processus d'importation des métadonnées crée automatiquement un enregistrement de certificat pour le fournisseur d'identité. Accédez au module **Certificat x509** pour afficher le certificat.

   Remarque :
   Les certificats pour l'authentification unique doivent toujours être au format PEM pour fonctionner avec des certificats SAML.

5. Si la signature électronique est active, configurez le formulaire Fournisseur d'identité et ajoutez **l'URL de consommateur d'assertion pour le champ d'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 que vous n'utilisez pas l'authentification unique de plusieurs fournisseurs, configurez l'URL du consommateur d'assertion avec les propriétés SAML de signature électronique.

Générer les métadonnées du fournisseur de service d'instance (SP) pour SAML

Dans le cadre de votre configuration SSO, vous pouvez générer les métadonnées du 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 de l'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 du SP de l'instance à partir des paramètres de propriété système.
Authentification unique SAML 2	Accédez à la **Authentification unique SAML 2** > **Métadonnées**. L'intégration génère automatiquement les métadonnées du SP de l'instance à partir des paramètres de propriété système.

2. Copiez les métadonnées du portail de services 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 du SP en ligne.

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 appartenant à une entreprise. 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 de société.
5. Configurez le formulaire et ajoutez le champ **Source SSO** .
6. Dans le champ **Source SSO** , saisissez l'un des éléments suivants :
   - **Utilisateurs SAML** : entrez **sso :** suivi du sys_id de l'enregistrement du fournisseur d'identité.
   - **Utilisateurs de fédération SSO** : entrez **fédération :** suivi de la sys_id de l'enregistrement de fédération.
7. Cliquez sur **Mettre à jour**.

Test des connexions IdP

Le test de la connexion à un IdP 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 d'actualisation des métadonnées IdP à fournisseurs multiples récupère et met à jour le certificat pour l'IdP lors de la création, de la mise à jour ou du test de la connexion.

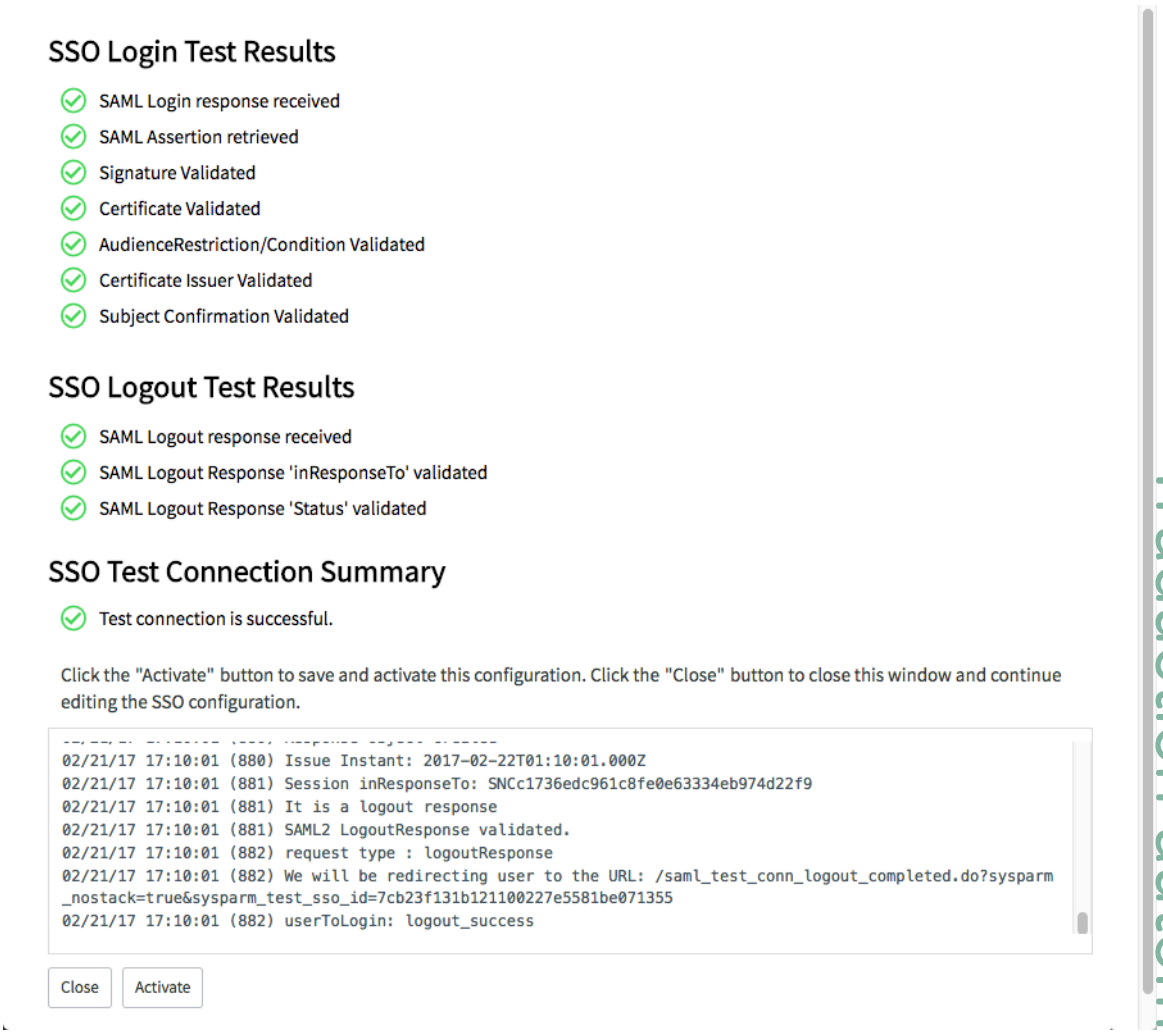
Remarque :
Pour certains tickets IdP, si la connexion de test échoue, ils doivent créer glide.authenticate.multisso.test.connection.mandatory avec la valeur faux et vous pouvez activer l'IdP sans la connexion de test.

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 définir un nouvel IdP.
3. **Facultatif :** Configurez un fournisseur d'identité si vous configurez un nouveau fournisseur d'identité.
4. Cliquez sur **Test de la connexion**, 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 mettre 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 **Résumé/résultats des tests SSO** ou **Journaux de test SSO** pour afficher les messages du journal.

En cas d’erreurs, reportez-vous à la section Erreurs et correctifs de Multi-SSO (SAML 2.0)

6. Cliquez sur **Annuler** lorsque le test est terminé.



Erreurs de connexion IdP courantes

Le tableau suivant décrit certaines des erreurs de connexion IdP les plus 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 non valide « <nom de champ> » n’est pas un champ de sys_user table.	Vérifiez que le contenu du champ Table d’utilisateur que vous avez sélectionné correspond au jeton NameID SAML.
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 de l’audience** contient une URL valide pour votre instance.
Impossible de se déconnecter de la session de l’IdP.	Vérifiez que l’URL **SingleLogoutRequest** contient une URL valide pour le service de déconnexion de votre fournisseur d’identité.

Dépannage des connexions de test IdP (suite)

Messages d'erreur	Solution
La signature n'a pas été validée sur la clé des informations d'identification.	Vérifiez qu'un certificat valide est installé sur l'IdP.

Erreurs et correctifs de Multi-SSO (SAML 2.0)

Une liste des erreurs courantes et des correctifs associés pour une installation et une configuration de l'authentification unique (SAML 2.0).

Erreurs lors de la configuration de SSO à fournisseurs multiples (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 dans l'instance.
Les certificats ne correspondent pas. Attendu : <certStr>, réel : <inboundCert>.	Vérifiez que le certificat IDP x509 est présent, valide et actif.	N. A.	Le certificat disponible dans SNC ne correspond pas au certificat dans l'assertion. Les causes sont les suivantes : • Le certificat est mis à jour sur l'IdP, mais pas dans l'instance ServiceNow. • Le format du certificat n'est pas correct.	Vérifiez que la chaîne au format PEM dans l'enregistrement de certificat SAML 2.0 correspond au certificat X509 dans SAMLResponse pour l'IdP d'utilisateur.

Erreurs lors de la configuration de SSO à fournisseurs multiples (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
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 possède le même certificat que l'instance SNC.
InResponseTo dans l'incompatibilité de SubjectConfirmationData. Attendu : <inResponseTo>, réel : <inResponseTo>.	Échec de la validation de la confirmation de l'objet.	N. A.	Cette erreur s'affiche si l'une des situations suivantes se produit : • L'IdP renvoie une réponse SAML pour une autre requête SAMLRequest • Un utilisateur place un signet sur l'URL avec SAMLRequest au lieu de l'URL d'instance uniquement • Si une valeur null est attendue, la réponse peut être envoyée à un autre nœud lorsque l'instance dispose de plusieurs nœuds.	L'administrateur IdP doit confirmer que la réponse SAML attendue est renvoyée. Il peut s'agir d'un problème d'équilibreur de charge ou d'infrastructure.
Valeur SessionIndex 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.

Erreurs lors de la configuration de SSO à fournisseurs multiples (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
Aucune confirmation d'objet valide trouvée.	Échec de la validation de la confirmation de l'objet.	N. A.	Des conditions peuvent être manquantes en raison d'une erreur sur l'IdP. Le StatusCode de la réponse contient Répondeur au lieu de la valeur Succès attendu.	Passez en revue SAMLResponse pour déterminer si les conditions sont incluses dans SAMLResponse. Les données de confirmation d'objet valides peuvent être expirées ou non destinées à la bonne audience.
Incohérence de l'audience d'assertion. Attendu : <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 d'audience configurée pour l'instance SNC doit correspondre à la valeur de l'IdP.	Recherchez <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. Attendu : <valeur sur l'instance>, réel : <valeur renvoyée par l'IdP>	L'émetteur de l'assertion n'est pas valide.	URL du fournisseur d'identité qui émet le jeton de sécurité SAML2 avec les informations de l'utilisateur.	L'ID d'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 (URL du fournisseur d'identité qui émet le jeton de sécurité SAML2 avec les informations de l'utilisateur) est définie correctement.

Erreurs lors de la configuration de SSO à fournisseurs multiples (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
L'objet est valide dans le futur. Maintenant : <maintenant>, NotBefore : <notBefore > ou L'objet a expiré. Maintenant : <now>, 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 du SP.	Mettez à jour la propriété SAML glide.authenticate.sso.saml2.clockskew vers une valeur plus grande. La valeur par défaut est 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 du SP	Mettez à jour la propriété SAML vers une valeur plus grande. 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 de connexion et d'IdP courantes

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* sans ajouter le nom d'hôte	Définissez (ou créez) la propriété système glide.authenticate.failed_redirect pour rediriger les demandes d'authentification ayant échoué vers cette URL.

Erreurs de connexion et d'IdP courantes (suite)

Erreur ou symptôme	Diagnostic	Corriger
	IdP à la valeur de la propriété. **Remarque :** Pour en savoir plus sur cette propriété, consultez Liste d'autorisation d'URL pour les redirections de déconnexion 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 lequel n'est pas l'algorithme de signature attendu http://www.w3.org/2000/09/xmldsig#rsa-sha1.	Consultez l'onglet Contexte de l'alerte pour connaître les détails de 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 de journal système (syslog).	Lorsque votre IdP (par exemple, ADFS) répond avec l'état `oasis :names :tc :SAML :2.0 :status :Requester`, cela signifie que l'IdP a rejeté la connexion en raison d'un problème avec la demande qui lui a été envoyée. Malheureusement, la réponse SAML reçue de l'IdP ne fournit pas plus de détails sur l'erreur.	Examinez la demande SAML envoyée à l'IDP et collaborez avec l'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 connaître la raison de l'échec de la connexion.

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 où vous activez l'authentification unique multiple et si vous avez déjà personnalisé les sorties d'installation.

Avant de commencer

Rôle requis : admin

Procédure

1. Sauvegardez le SAML2SingleSignon_update1 de sortie de l'installation modifiée et le script include SAML2_update1.
2. Rétablissez à la fois la sortie d'installation et le script include à la version disponible avec le système de base de référence.
3. Activez ou mettez à niveau le module **d'extension Integration - Multiple Provider Single Sign-On Installer** .
   Le système met à niveau SAML et tous les fichiers nécessaires vers SAML 2 Update 1.

4. Ouvrez la page de propriétés de l'authentification unique multiple 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 de script include de base **de référence et les changements de script include de SAML2_update1** dans le script include de SAML2_update1 de base de référence.

Se connecter à l'aide de l'authentification unique (SSO) de plusieurs fournisseurs

La méthode la plus 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 configurée spécifiquement.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Une fois l'authentification unique 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>
```

Une fois qu'un utilisateur s'est connecté avec succès 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 pour se connecter au serveur IdP, qui se connecte automatiquement à l'instance.

Si aucun paramètre d'URL n'est défini ou si le cache du navigateur a été effacé, les utilisateurs peuvent également effectuer les actions 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. Entrez la valeur du champ spécifié sur la table utilisateur que vous avez configurée 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 avec succès à un IdP, ils sont automatiquement redirigés vers cet IdP chaque fois qu'ils tentent d'accéder à l'instance. Pour qu'un utilisateur accède à un autre IdP, envoyez-lui une URL avec les nouvelles informations 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 l'IdP auquel se connecter.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche

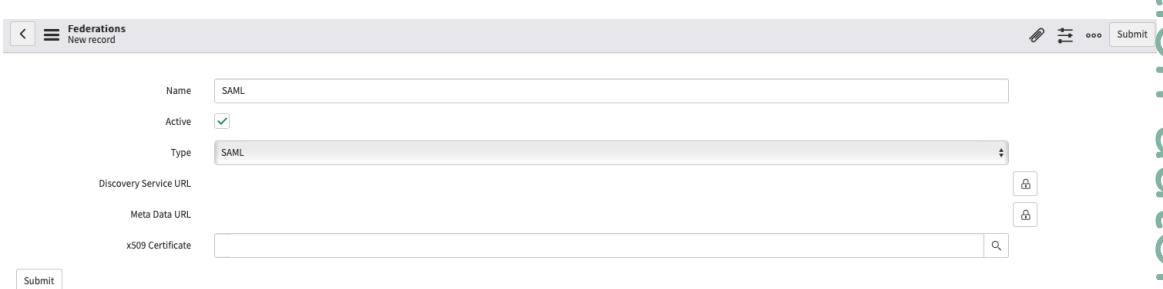
Les fédérations SSO regroupent les métadonnées de plusieurs IdP et fournisseurs de services, y compris votre instance. Les fédérations publient ensuite les métadonnées sous forme de fichier XML, qui comprend des informations telles que les noms et les certificats IdP. Les administrateurs peuvent ensuite 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.

Remarque :
Utilisez le sys_ID de l'enregistrement de fédération que vous venez de créer.

Pour plus d'informations, voir Flux d'authentification IdP pour l'authentification de plusieurs fournisseurs SSO (SAML)



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 détection 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	Entrez 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.
Détection Service URL	Entrez l'URL du service de détection 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.

Champ	Description
Domaine	Sélectionnez le domaine auquel les données appartiendront.

Remarque :
L'IdP de gestion des identités fédérées InCommon est préconfiguré.

À utiliser Portail de services avec l'authentification unique de plusieurs fournisseurs pour rediriger une URL

Portail de services utilise une combinaison de propriétés système et de script includes 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 effectuer une redirection automatique vers votre fournisseur d'identité (IdP) principal, alors Portail de services vous êtes automatiquement redirigé vers ce fournisseur d'identité.
Si vous avez plusieurs IdP, Portail de services affiche un lien sur la page de connexion pour **utiliser une connexion externe**.

Procédure

1. Configurer la page de connexion de Service Portal
2. Rediriger vers Service Portal 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 mauvaise 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 Single Sign-on (SSO) pour résoudre les problèmes de 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 en tant que récupération de compte.
- Les flux ACR permettent aux administrateurs d'utiliser des fonctionnalités en libre-service pour traiter la récupération de compte en cas de besoin de récupération (par exemple, erreur de configuration SSO, certificats expirés).
- Réduisez les accès non autorisés à l'instance et fournissez une base solide pour l'utilisation d'ACR en dehors des cas d'utilisation SSO.

Instance fraîche

Pour qu'une nouvelle instance utilise ACR, vous devez effectuer les opérations suivantes :

- Activez le module d'extension Multi-SSO (`com.snc.integration.sso.multi.installer`)
- Activer ACR (`glide.sso.acr.enabled`) : activé par défaut dans le cas d'une nouvelle instance.

- 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 désactivera pas l'authentification unique 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, 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 la récupération de compte.

- L'administrateur doit définir un mot de passe pour la connexion locale et enregistrer 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 effectuer les opérations suivantes :

- Activez le module d'extension Multi-SSO (com.snc.integration.sso.multi.installer)
- Activer ACR (glide.sso.acr.enabled)

Remarque :
En cas de mise à niveau de l'instance, 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 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'il n'y a pas au moins un compte 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 continuera de fonctionner sans qu'un utilisateur de récupération ne soit configuré.

Configuration de la récupération du compte

La fonctionnalité de récupération de compte est incluse dans le **module d'extension Integration - Multiple Provider Single Sign-On Installer (com.snc.integration.sso.multi.installer).** La fonctionnalité est activée par défaut. Vous pouvez modifier ce paramètre et d'autres paramètres de récupération de compte à l'aide des propriétés système. Pour en savoir plus sur ces propriétés, reportez-vous à Propriétés de la 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 de contexte SSO - ACR** . Pour plus d'informations sur le contexte, reportez-vous à Contexte de récupération de compte.

Pour en savoir plus sur le fonctionnement des politiques 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 mauvaise configuration SSO ou le traitement de certificats expirés.

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, vous devez effectuer les opérations suivantes :

- Activez le module d'extension Multi-SSO (com.snc.integration.sso.multi.installer)
- Activer ACR (glide.sso.acr.enabled) : activé par défaut dans le cas d'une nouvelle instance.
- 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 MFA avant de s'inscrire en tant qu'utilisateur ACR.

Pour qu'une instance mise à niveau utilise ACR, vous devez effectuer les opérations suivantes :

- Activez le module d'extension Multi-SSO (com.snc.integration.sso.multi.installer)
- Activer ACR (glide.sso.acr.enabled)

  Remarque :
  En cas de mise à niveau de l'instance, 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 désactivera pas l'authentification unique 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, 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 la récupération de compte.

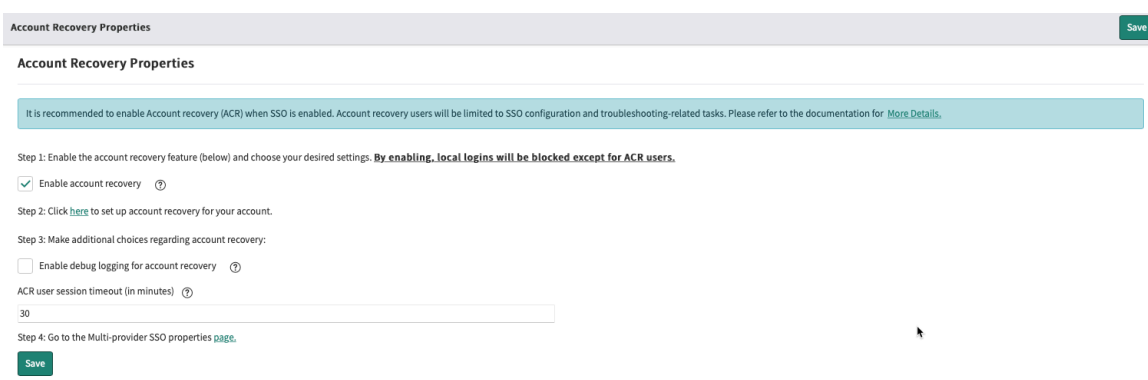
- L'administrateur doit définir un mot de passe pour la connexion locale et enregistrer MFA avant de s'inscrire en tant qu'utilisateur ACR.

Procédure

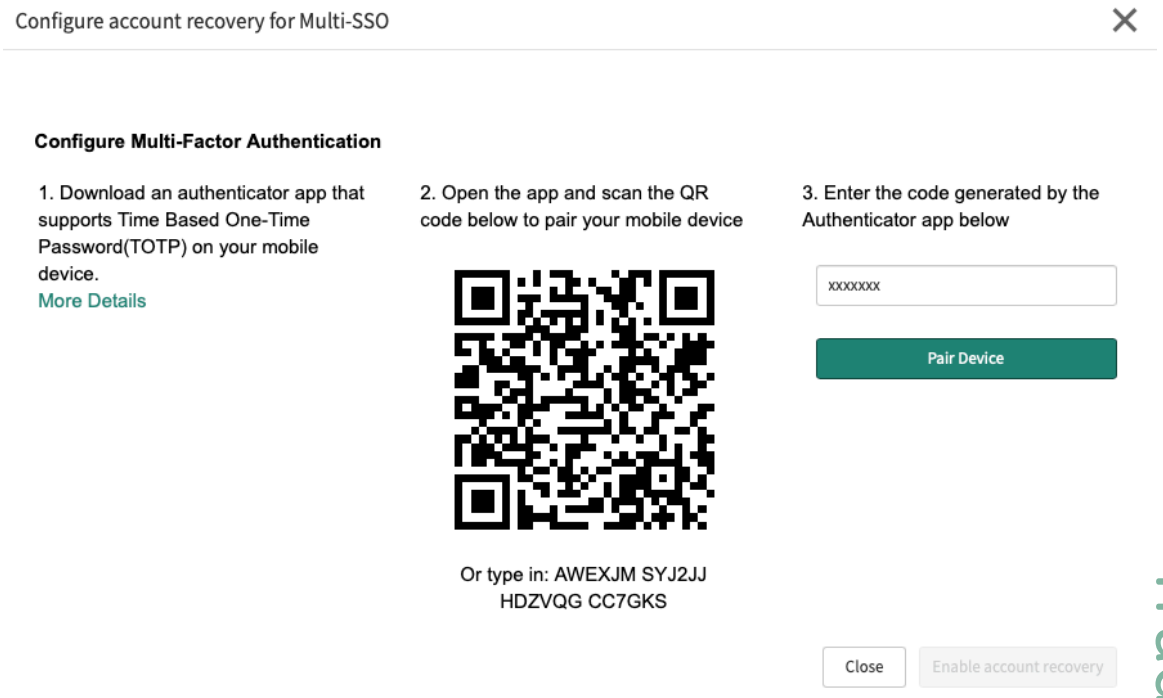
1. Accédez à la **Tous** > **Récupération de compte** > **Propriétés**.
2. Cliquez sur **Activer la récupération de compte**.

Remarque :
Vous devez activer la récupération de compte lorsque la SSO est activée. Les utilisateurs de la récupération de compte seront limités à la configuration SSO et aux tâches liées au dépannage.

3. Cliquez sur le texte **ici** à l'étape 2.



4. Suivre les instructions à l'écran dans le modal **Configurer la récupération de compte pour l'authentification unique (SSO) à fournisseurs multiples** .



Après avoir terminé les étapes à l'écran, **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

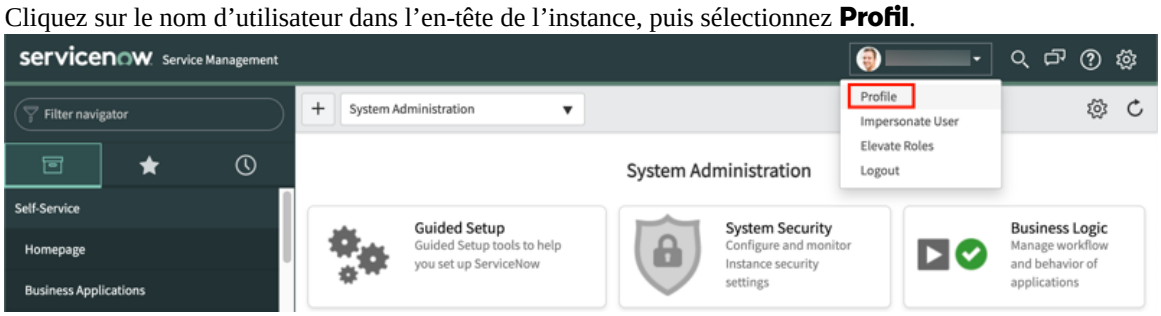
Configurez un administrateur en tant qu'utilisateur de récupération de compte à partir du profil d'utilisateur administrateur.

Avant de commencer

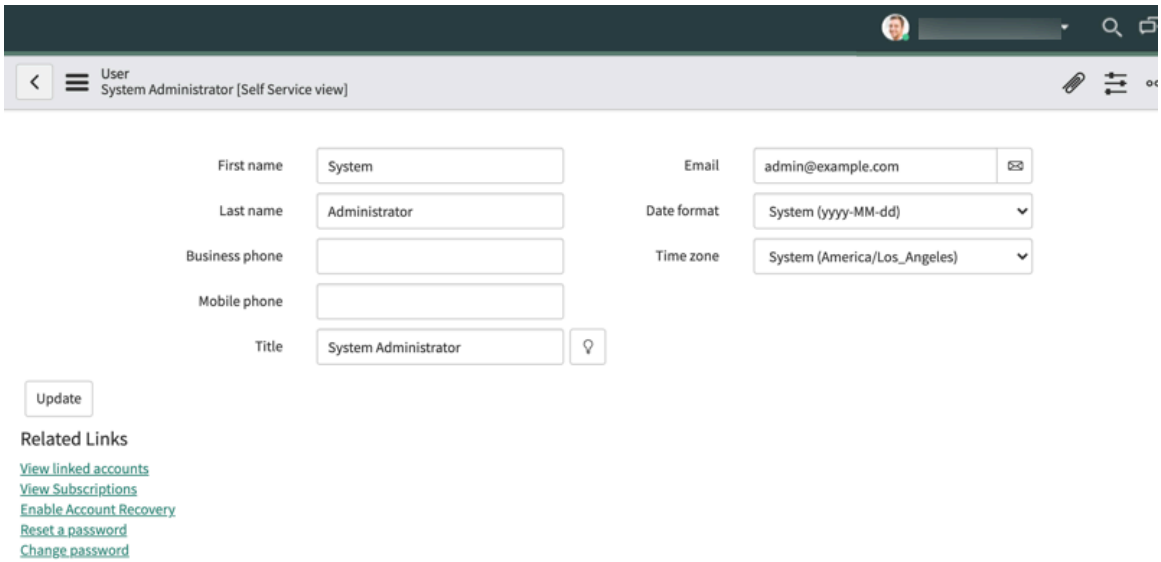
Rôle requis : admin

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**.



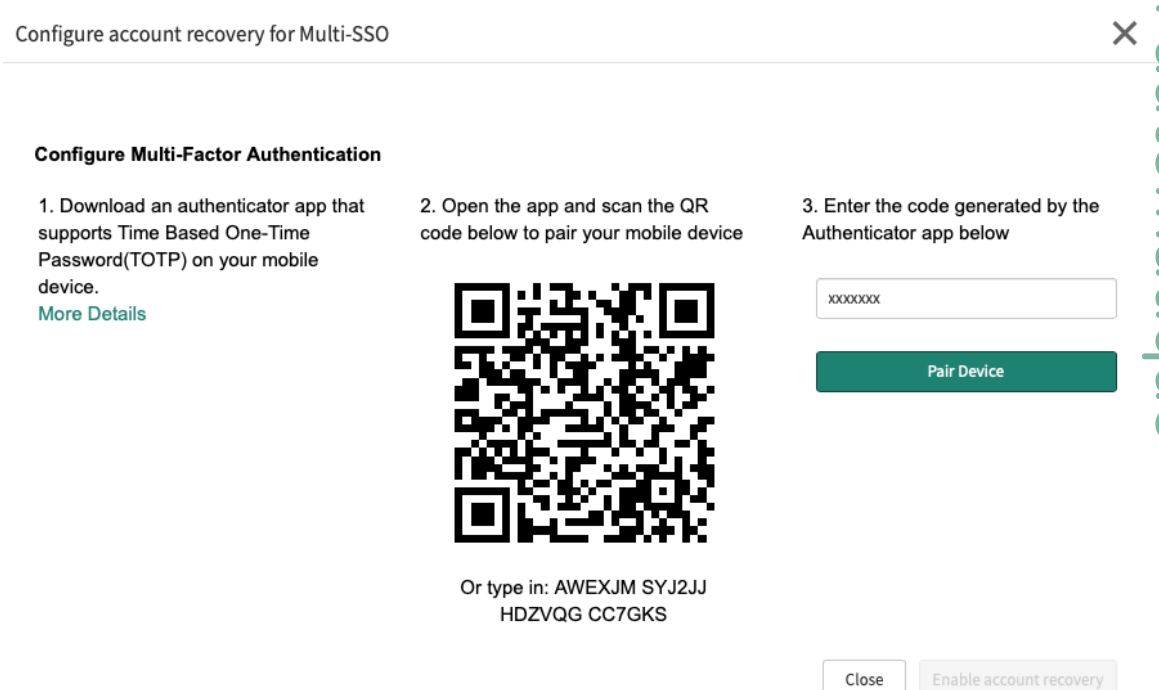
3. Dans le formulaire **Utilisateur** , cliquez sur **Activer la récupération de compte** dans la section **Liens connexes** .



Remarque :

Si la récupération de compte est déjà activée pour l'utilisateur sélectionné, **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. Suivre les instructions à l'écran dans le modal **Configurer la récupération de compte pour l'authentification unique (SSO) à fournisseurs multiples** .



Après avoir terminé les étapes à l'écran, **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 la récupération de compte

Utilisez les propriétés système pour configurer la récupération de 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]	Si la fonctionnalité de récupération de compte est activée sur votre instance. Cette propriété est activée par défaut.
Activer la journalisation de débogage pour la récupération de compte [glide.sso.acr.debug.log.enabled]	Si votre instance inclut des informations de récupération de compte dans la journalisation du débogage. Cette propriété est désactivée par défaut.
Délai d'expiration de la 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. Cette propriété a une valeur par défaut de 30.

Signature électronique pour l'authentification unique (SSO) de plusieurs fournisseurs

La signature électronique avec l'authentification unique 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 de l'authentification unique (SSO) pendant l'authentification et pour exiger des utilisateurs qu'ils fournissent leurs informations d'identification avant d'envoyer leur signature électronique, vous pouvez configurer l'authentification pour demander les informations d'identification de l'utilisateur avant d'envoyer une signature.

Vous pouvez installer le module d'extension Approvals with e-signature (com.glide.e_signature_approvals) pour configurer la signature électronique pour les connexions SSO.

Remarque :
Vous devez installer les signatures de signature de code (com.glide.code_signing.signatures) pour installer le module d'extension de signature électronique.

Activer le module d'extension Approbation avec signature électronique

Le module d'extension Approbation avec signature électronique (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 les signatures de signature de code (com.glide.code_signing.signatures) pour installer le module d'extension de 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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

Utiliser l'authentification unique (SSO) de plusieurs fournisseurs afin de 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

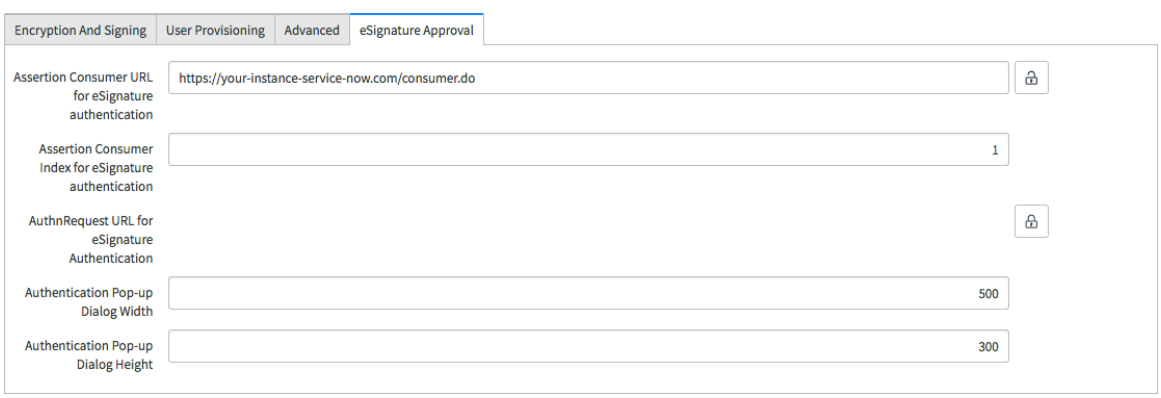
Pourquoi et quand exécuter cette tâche
L'IdP SAML doit prendre en charge et respecter l'attribut forceAuthn dans les demandes d'assertion SAML. La signature électronique ne fonctionne pas sans ce paramètre IdP. Configurez une approbation avec signature électronique à l'aide des informations d'identification issues d'une authentification SAML 2.0.

Procédure

1. Activez ou mettez à niveau vers SAML 2.0 avec le module d'extension Activate Multi-Provider SSO.
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 que l'onglet Avancé de la configuration de votre IdP SAML 2.0 affiche l'attribut **Forcer l'AuthnRequest** coché.
   votre IdP SAML 2.0 doit prendre en charge l'attribut **Forcer AuthnRequest** , sinon la signature électronique n'est pas prise en charge.
4. Dans l'onglet Approbation de signature électronique, entrez les propriétés SAML de signature électronique suivantes.

Option	Description
URL de consommateur d'assertion pour l'authentification de signature électronique	Cette propriété est définie par défaut sur l'URL appropriée. Pour configurer cette propriété, sélectionnez l'icône de verrou pour 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

Option	Description
	utiliser pour les signatures électroniques, en commençant par l'index 1 ou plus.
URL AuthnRequest pour l'authentification de signature électronique	Vous pouvez saisir l'URL qui pointe sur l'URL AuthnRequest de l'IdP SAML 2.0 pour l'authentification de signature électronique. Si l'URL est la même que l'URL de consommateur d'assertion, vous pouvez laisser ce paramètre vide.
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 un utilisateur peut entrer des 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 un utilisateur peut entrer des informations d'identification. Ce paramètre contrôle la hauteur de cette boîte de dialogue. La valeur par défaut est 300.



5. Sélectionnez le bouton **Générer les métadonnées** sous les onglets pour régénérer les métadonnées du fournisseur de services.
6. Copiez les métadonnées du fournisseur de service et mettez-les à jour sur l'IdP SAML.

Utiliser l'authentification unique 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

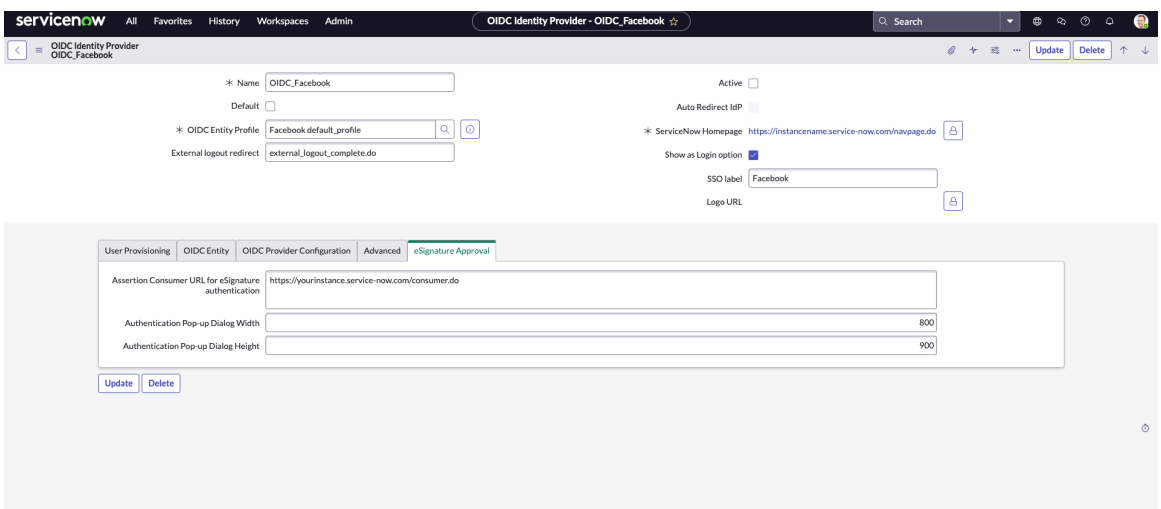
Pourquoi et quand exécuter cette tâche

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 issues 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, entrez les propriétés SAML de signature électronique suivantes.

Option	Description
URL de consommateur d'assertion pour l'authentification de signature électronique	Cette propriété est définie par défaut sur l’URL appropriée. Pour configurer cette propriété, sélectionnez l’icône de verrou pour 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 un utilisateur peut entrer des 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 un utilisateur peut entrer des informations 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 d’OIDC ou **Mettre à jour** si vous souhaitez mettre à jour les détails dans la signature électronique.

OpenID Connect (OIDC) en tant que fournisseur d’identité (IdP) Single Sign-On (SSO)

OpenID Connect (OIDC) est une couche d’identité construite sur le protocole OAuth, qui vous offre, ainsi qu’à vos utilisateurs finaux, une expérience d’authentification unique (SSO) moderne et intuitive. OIDC améliore également l’expérience de connexion pour les applications mobiles en permettant aux utilisateurs de se connecter aux applications à ServiceNow 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 comme Google pour vos utilisateurs B2C (business-to-customer) et des fournisseurs d'identité d'entreprise comme Okta , Microsoft Azure AD pour vos utilisateurs business-to-business.

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 l'authentification unique (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.
- Activer le module d'extension SSO de plusieurs fournisseurs
- Configurer les propriétés de l'authentification unique (SSO) de plusieurs fournisseurs
- 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 :
L'option de connexion avec l'IdP OIDC n'est pas prise en charge si le module d'extension Domain Separation est installé.

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 à l'aide de l'une des méthodes suivantes.

Option	Description
Importer la configuration connue OpenID Connexion	Si vous disposez de l'URL de configuration connue, ainsi que des informations d'identification du client associées, vous pouvez importer directement une configuration OIDC.

Option	Description
	Remarque : Si vous importez la configuration connue OIDC, tous les champs connexes sont renseignés automatiquement.
Configurer manuellement le formulaire Fournisseur d'identité OIDC	Si vous n'avez pas d'entité OIDC OAuth existante, fermez la fenêtre contextuelle Importer la configuration connue OpenID Connect et renseignez manuellement les champs du formulaire Fournisseur d'identité OIDC.

Importer les champs de configuration connus OpenID Connect

Propriété	Description
Nom	Nom unique pour la configuration du fournisseur d'identité OIDC.
ID client	ID client de l'application enregistrée 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 bien connue	URL qui contient des métadonnées sur le fournisseur d'identité OIDC tiers.

Tous les champs requis doivent être remplis 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'accord du profil d'entité OAuth doit comporter un code d'autorisation. Pour plus d'informations, consultez Configurer un fournisseur OIDC OAuth sur la Now 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 Multiple Provider Single Sign-On Installer.

Champs Fournisseur d'identité OIDC

Propriété	Description
Nom	Nom de l'enregistrement de fournisseur d'identité OIDC.
Actif	Option permettant d'activer la configuration d'IdP OIDC. **Remarque :** Cette option ne peut être activée qu'après un test de connexion réussi.
Par défaut	Option permettant de définir la configuration d'IdP OIDC par défaut lorsqu'il existe plusieurs configurations OIDC.

Propriété	Description
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 dans la section Liens connexes. **Remarque :** Si vous activez une nouvelle configuration d'IdP de redirection automatique, le `glide_sso_id` cookie est automatiquement mis 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	L'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 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 apparaît sous la forme du bouton **Connexion avec le fournisseur d'identité** .
Étiquette SSO	Étiquette de l'IdP OIDC affiché 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 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 l'attribution automatique des utilisateurs pendant la connexion de l'utilisateur. Lorsque la mise en service automatique des utilisateurs 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 l'attribution automatique des utilisateurs. Cette propriété crée un utilisateur dans la table Utilisateur de l'instance (sys_user) lorsque l'utilisateur quitte l'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 les deux jetons d'ID et informations utilisateur vers un 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 de transformations.

Propriété	Description
Mettre en service la source de données	Source de données de jeton d'ID utilisée pour la mise en service de l'utilisateur.
Source d'informations de l'utilisateur	Source de données du point de terminaison d'informations utilisateur utilisée pour la mise en service de l'utilisateur. Ce champ s'affiche lorsque les champs Informations sur l'utilisateur ou Jeton d'ID et Informations sur l'utilisateur sont sélectionnés pour la **mise en service à l'aide** du champ.
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, une fois qu'un utilisateur est connecté, son enregistrement sera 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 bien connue de la validation de la demande de jeton d'IdP ou d'ID OIDC.
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 MultiSSO_OIDC_custom.
Script de déconnexion	Script qui s'exécute une fois que l'utilisateur s'est déconnecté. Ce champ est automatiquement défini sur MultiSSO_OIDC_logout_custom.

8. **Facultatif :** Dans l'onglet Approbation de la signature électronique, configurez la signature électronique pour l'Idp OIDC.

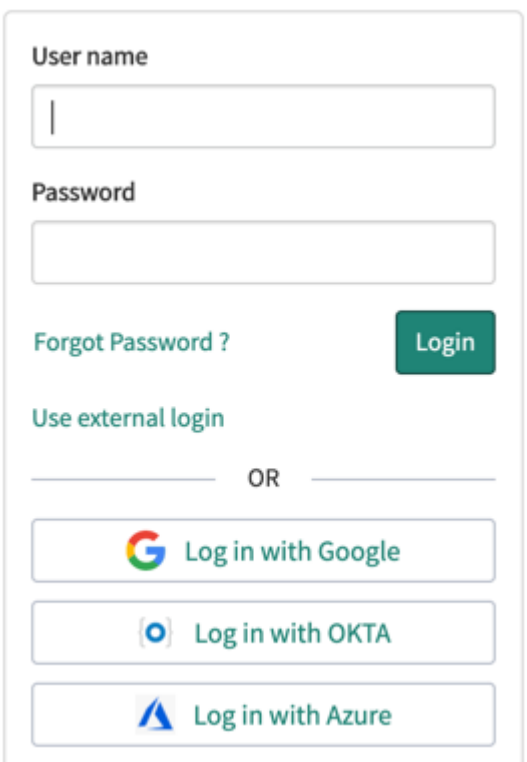
   Remarque :
   L'onglet Approbation de signature électronique s'affiche uniquement lorsque vous installez le module **d'extension Approbation avec signature électronique** (com.glide.e_signature_approvals).

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 de l'URL est `https://yourinstance.service-now.com/consumer.do`
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`.

9. **Facultatif :** Accédez à la page de connexion de l'instance pour vérifier que IdP apparaît comme option de connexion.
   Le format de l'URL doit être le 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 basée sur Facebook est fournie avec votre ServiceNow instance.

Vous pouvez définir les configurations du fournisseur d'identité (IdP) sur 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 :

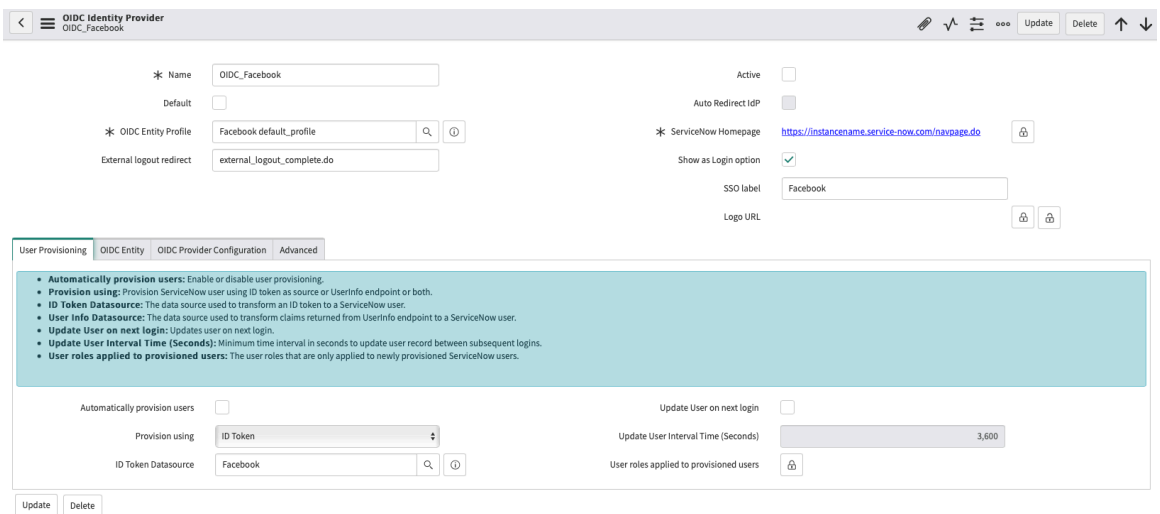
Remarque :

- La plupart des champs sont renseignés automatiquement lors de l'utilisation de l'IdP par défaut.
- Les détails de la page d'accueil ServiceNow doivent être fournis.
- Les détails relatifs à l'utilisateur, tels que l'ID client et le secret Facebook client, doivent être fournis dans l'IdP.

Détails du fournisseur d'identité OIDC_Facebook

Champ	Description
Nom	Nom de l'enregistrement IdP OIDC. Saisissez OIDC_Facebook.
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 l'authentification unique. 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 d'IdP OIDC.

Champ	Description
	Remarque : Cette option ne peut être activée 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	L'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 **Se connecter avec Facebook** .
Étiquette SSO	Étiquette de l'IdP OIDC affiché 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 IdP OIDC. Ce champ s'affiche uniquement lorsque **l'option Afficher comme connexion** est activée.



4. **Facultatif :** Ouvrez l'onglet **Attribution d'utilisateurs** et remplissez les champs.

Remarque :
Vous devez configurer les informations liées à OIDC telles que l'ID client et le secret client de vos utilisateurs à partir de Facebook.

Traduction automatique

Onglet Attribution d'utilisateurs

Champ	Description
Attribuer automatiquement les utilisateurs	Option permettant d'activer l'attribution automatique des utilisateurs. 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 l'attribution automatique des utilisateurs pendant la connexion de l'utilisateur. Lorsque l'attribution automatique d'utilisateurs est activée, un enregistrement utilisateur est automatiquement créé dans l'instance ServiceNow si cet enregistrement n'existe pas.
Mise en service à l'aide de	La source de données à utiliser pour effectuer la ServiceNow transformation en utilisateur. 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 de transformations.
Mettre en service la source de données	La source de données du jeton d'ID utilisée pour la mise en service de l'utilisateur.
Source d'informations de l'utilisateur	Source de données de point de terminaison d'informations utilisateur utilisée pour la mise en service de l'utilisateur. Ce champ s'affiche uniquement si **Informations sur l'utilisateur** ou **Jeton d'ID et Informations utilisateur** sont sélectionnés dans le champ Utilisation de la **mise en service** .
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 minimum (en secondes) pour mettre à jour un enregistrement utilisateur entre deux connexions. Ce champ est automatiquement défini sur 3 600 secondes. Par exemple, une fois qu'un utilisateur est connecté, son enregistrement sera 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 relatives à la configuration OIDC, consultez Configurer un fournisseur OIDC OAuth sur le Now Platform

Traduction automatique

6. Dans l'onglet **Configuration du fournisseur OIDC** , affichez et modifiez l'URL de configuration bien connue de l'IdP OIDC.
7. **Facultatif :** Ouvrez l'onglet **Avancé** et remplissez 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 **Activer**.
9. Pour mettre à jour l'enregistrement, cliquez sur **Mettre à jour**.
L'option de connexion basée sur Facebook s'affiche sur le formulaire de connexion.
10. Lorsque vous vous connectez au formulaire de connexion, procédez comme suit :
    a. Sélectionnez l'option Facebook .
    b. Pour vous connecter à l'instance, spécifiez vos Facebook informations d'identificationServiceNow.

Configurer une authentification unique (SSO) basée sur Facebook

Configurez une authentification unique basée sur Facebook pour votre ServiceNow instance.

Avant de commencer

Vous devez disposer d'un ID client valide configuré en tant qu'IdP à partir de Facebook.

Activez les propriétés suivantes :

- Activez l'authentification unique (SSO) de plusieurs fournisseurs.
- Activez la journalisation de débogage pour les intégrations SSO de plusieurs fournisseurs.

Rôle requis : admin

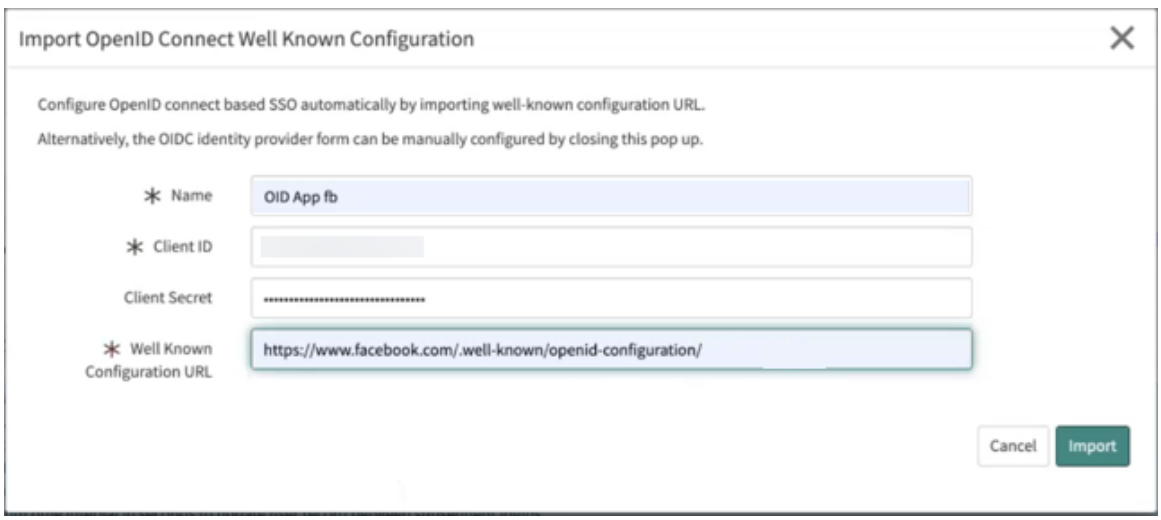
Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Pour créer un fournisseur d'identité Facebook , cliquez sur **Nouveau**.
3. Cliquez sur **OpenID Connect**.
4. Renseignez les champs du formulaire.

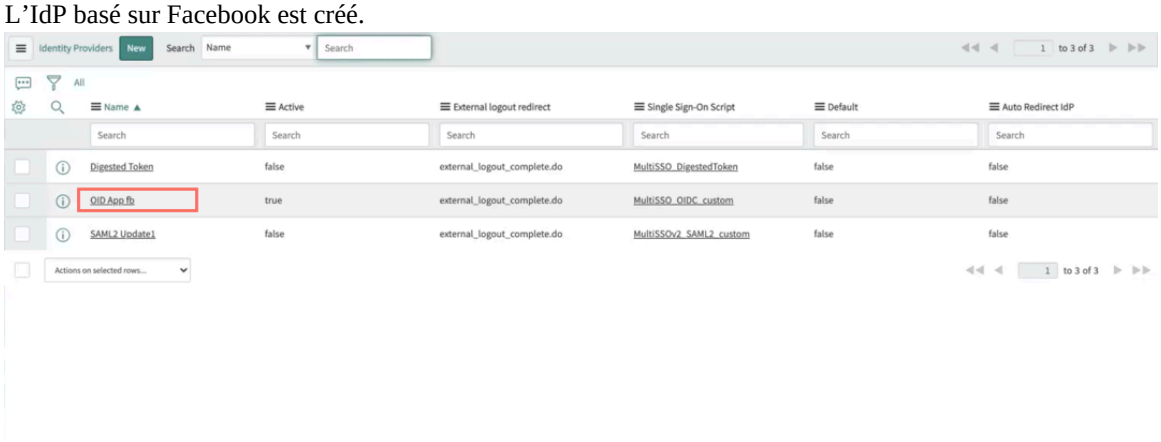
Formulaire Importer la configuration connue OpenID Connect

Champs	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.

Champs	Description
Secret client	Le secret client de l’application enregistrée dans le fournisseur d’identité OIDC tiers.
URL de configuration bien connue	URL qui contient les métadonnées sur le fournisseur d’identité OIDC tiers.

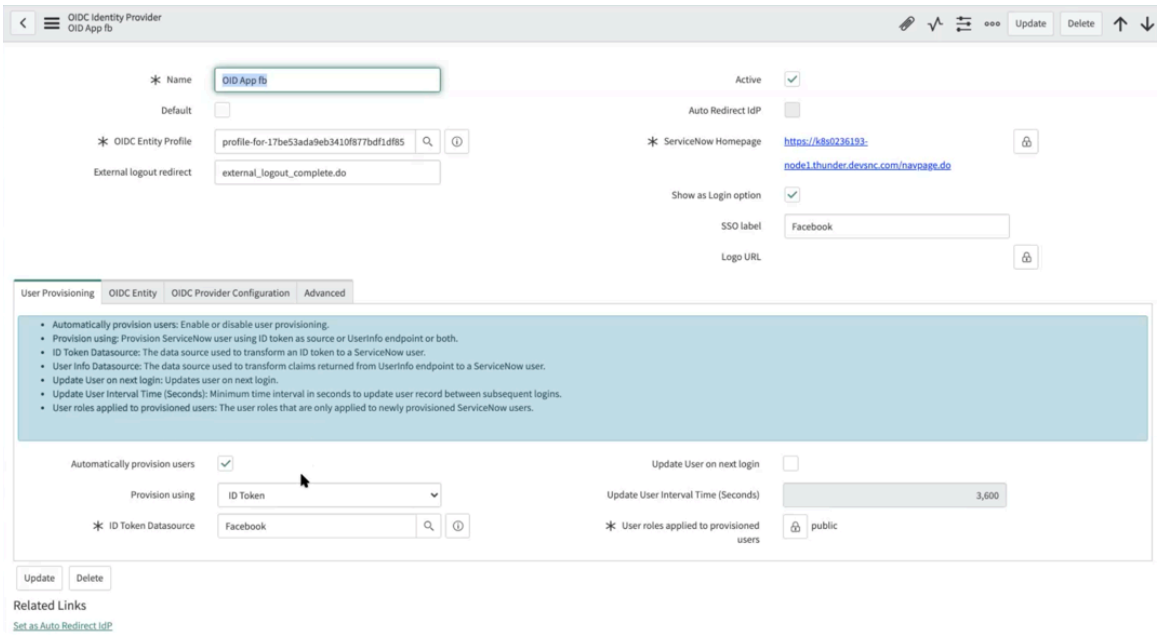


5. Cliquez sur **Importer**.
   L’IdP basé sur Facebook est créé.



6. Sélectionnez l’IdP Facebook .
7. Dans l’IdP Facebook , procédez comme suit :
   a. Validez tous les champs tels que **Nom**, **Profil d’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 avec des rôles et des mises en service d’utilisateurs spécifiques.

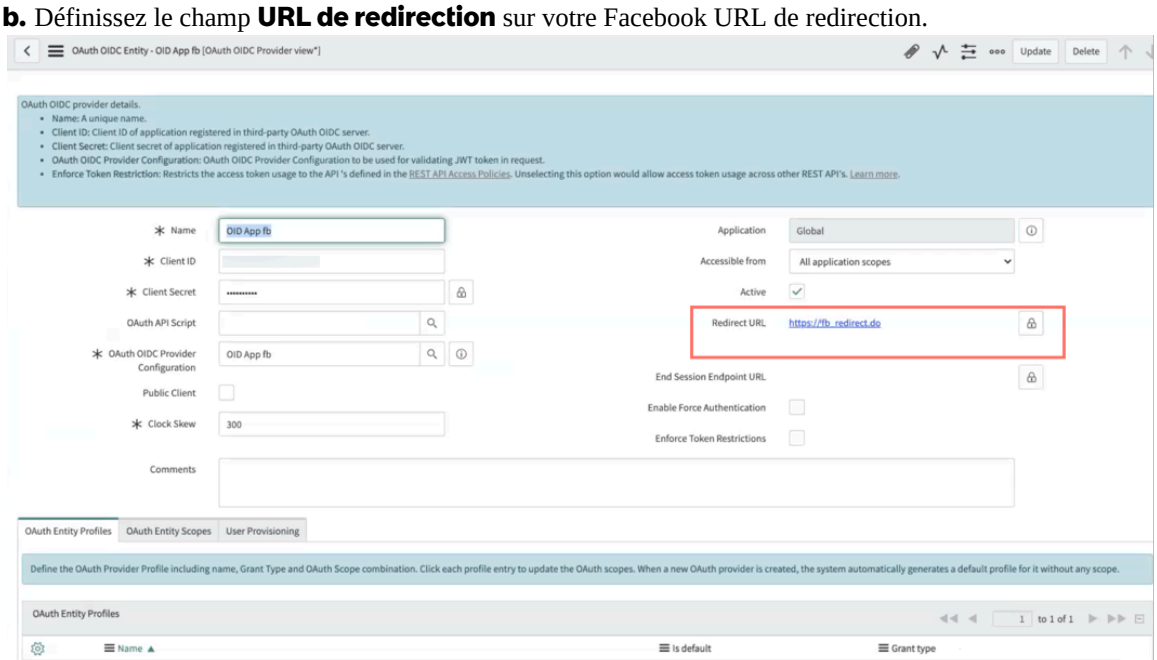
   Seuls les champs obligatoires sont obligatoires. Vous pouvez spécifier les champs restants en fonction de vos besoins.



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.

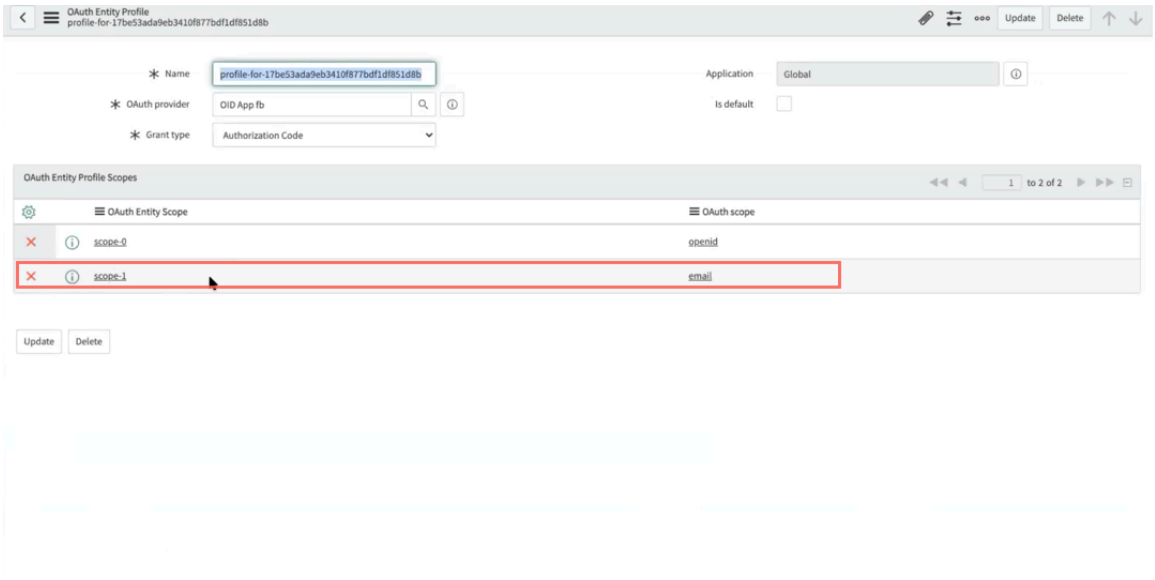


10. Dans l'onglet **Profils des entités OAuth** , procédez comme suit :

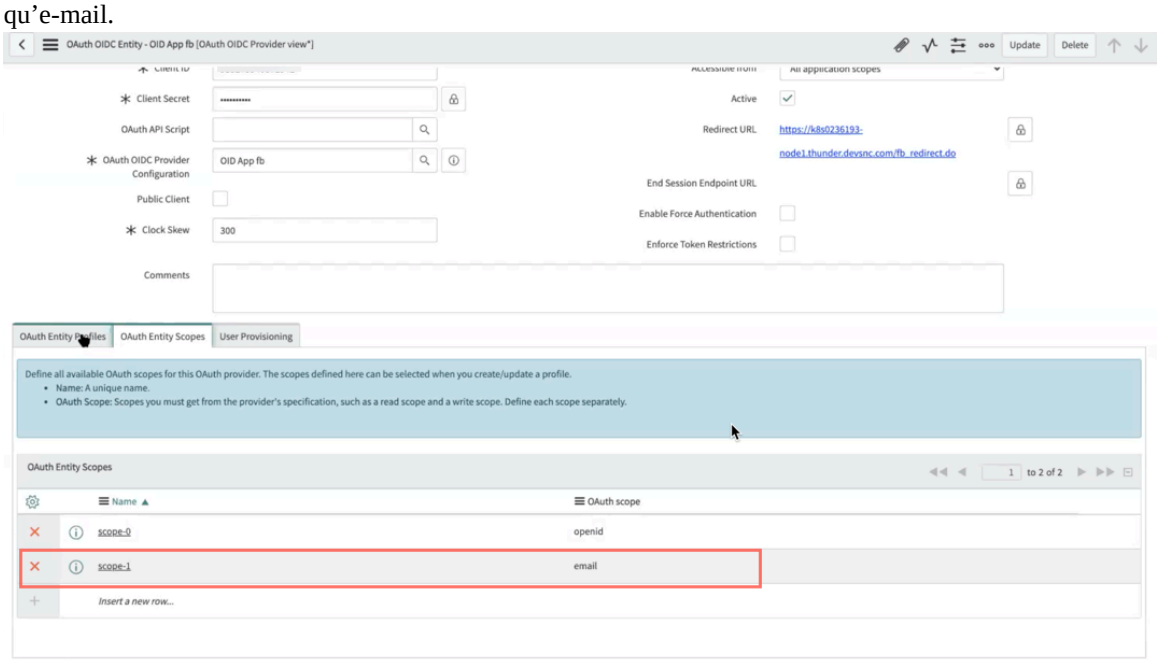
    a. Dans les détails du profil, cliquez sur un profil.

    b. Sélectionnez un périmètre et vérifiez les détails.
    Par exemple, sélectionnez **scope-1**

Traduction automatique



11. Dans l'onglet **Périmètres des entités OAuth**, cliquez sur le lien **scope-1** et ajoutez le périmètre en tant qu'e-mail.

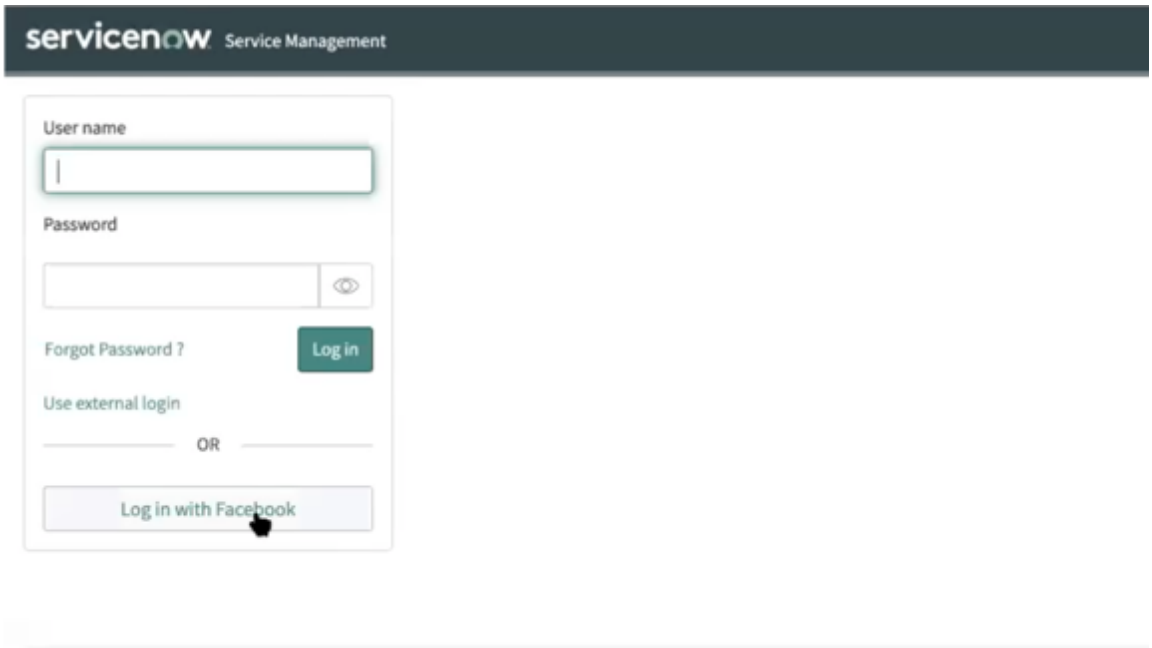


12. Pour enregistrer la configuration, cliquez avec le bouton droit sur l'en-tête, puis cliquez sur **Enregistrer**.
13. Pour définir la configuration comme active, sélectionnez **Actif**.

Résultats

Les utilisateurs s'affichent avec l'option Facebook SSO sur le formulaire de connexion.

Traduction automatique



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 l'authentification unique (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.
- Activer le module d'extension SSO de plusieurs fournisseurs
- Configurer les propriétés de l'authentification unique (SSO) de plusieurs fournisseurs
- 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 :
L'option de connexion avec l'IdP OIDC n'est pas prise en charge si le module d'extension Domain Separation est installé.

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 à l'aide de l'une des méthodes suivantes.

Option	Description
Importer la configuration connue OpenID Connexion	Si vous disposez de l'URL de configuration connue, ainsi que des informations d'identification du client associées, vous pouvez importer directement une configuration OIDC. **Remarque :** Si vous importez la configuration connue OIDC, tous les champs connexes sont renseignés automatiquement.
Configurer manuellement le formulaire Fournisseur d'identité OIDC	Si vous n'avez pas d'entité OIDC OAuth existante, fermez la fenêtre contextuelle Importer la configuration connue OpenID Connect et renseignez manuellement les champs du formulaire Fournisseur d'identité OIDC.

Importer les champs de configuration connus OpenID Connect

Propriété	Description
Nom	Nom unique pour la configuration du fournisseur d'identité OIDC.
ID client	ID client de l'application enregistrée 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 bien connue	URL qui contient des métadonnées sur le fournisseur d'identité OIDC tiers.

Tous les champs requis doivent être remplis 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'accord du profil d'entité OAuth doit comporter un code d'autorisation. Pour plus d'informations, consultez Configurer un fournisseur OIDC OAuth sur la Now 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 Multiple Provider Single Sign-On Installer.

Champs Fournisseur d'identité OIDC

Propriété	Description
Nom	Nom de l'enregistrement de fournisseur d'identité OIDC.
Actif	Option permettant d'activer la configuration d'IdP OIDC. **Remarque :** Cette option ne peut être activée qu'après un test de connexion réussi.
Par défaut	Option permettant de définir la configuration d'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 dans la section Liens connexes. **Remarque :** Si vous activez une nouvelle configuration d'IdP de redirection automatique, le `glide_sso_id` cookie est automatiquement mis 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	L'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 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 apparaît sous la forme du bouton **Connexion avec le fournisseur d'identité** .
Étiquette SSO	Étiquette de l'IdP OIDC affiché 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 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 l'attribution automatique des utilisateurs pendant la connexion de l'utilisateur. Lorsque la mise en service automatique des utilisateurs 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 l'attribution automatique des utilisateurs. Cette propriété crée un utilisateur dans la table Utilisateur de l'instance (sys_user) lorsque l'utilisateur quitte l'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 les deux jetons d'ID et informations utilisateur vers un 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 de transformations.
Mettre en service la source de données	Source de données de jeton d'ID utilisée pour la mise en service de l'utilisateur.
Source d'informations de l'utilisateur	Source de données du point de terminaison d'informations utilisateur utilisée pour la mise en service de l'utilisateur. Ce champ s'affiche lorsque les champs Informations sur l'utilisateur ou Jeton d'ID et Informations sur l'utilisateur sont sélectionnés pour la **mise en service à l'aide** du champ.
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, une fois qu'un utilisateur est connecté, son enregistrement sera 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 bien connue de la validation de la demande de jeton d'IdP ou d'ID OIDC.
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 MultiSSO_OIDC_custom.
Script de déconnexion	Script qui s'exécute une fois que l'utilisateur s'est déconnecté. Ce champ est automatiquement défini sur MultiSSO_OIDC_logout_custom.

8. **Facultatif :** Dans l'onglet Approbation de la signature électronique, configurez la signature électronique pour l'Idp OIDC.

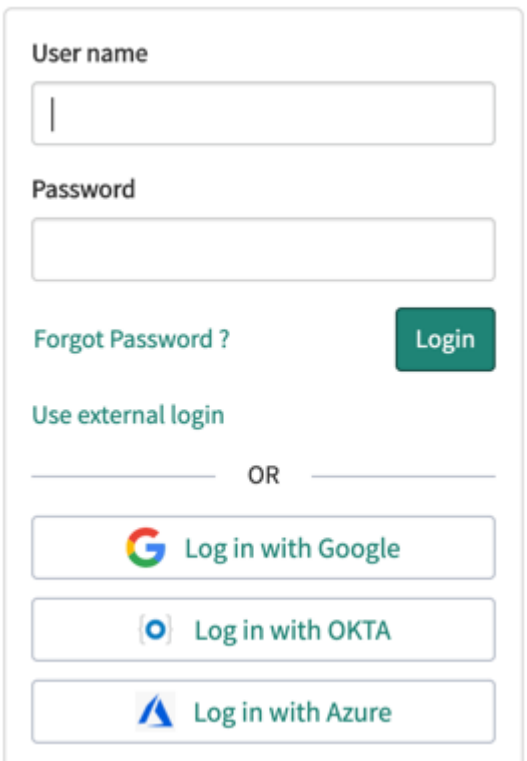
Remarque :
L'onglet Approbation de signature électronique s'affiche uniquement lorsque vous installez le module **d'extension Approbation avec signature électronique** (com.glide.e_signature_approvals).

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 de l'URL est https://yourinstance.service-now.com/consumer.do
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.

9. **Facultatif :** Accédez à la page de connexion de l'instance pour vérifier que IdP apparaît comme option de connexion.
Le format de l'URL doit être le 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.



SAML

SAML (Security Assertion Markup Language) est une norme basée sur 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 mis en œuvre, SAML est l'une des méthodes d'authentification unique (SSO) les plus sécurisées du marché.

L'intégration SAML 2.0 active l'authentification unique (SSO) 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 connecte 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, il interfère avec le partage d'informations de session qui a lieu entre l'instance et le fournisseur d'identité. Les utilisateurs disposant du privilège élevé security_admin 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.

Activer et configurer SAML 2.0

SAML 2.0 s'active via le module d'extension Integration - Multiple Provider Single Sign-On Installer.

Avant de commencer

Remarque :

Rôle requis : admin

Activez le module d'extension Integration - Multiple Provider Single Sign-On Installer pour configurer l'authentification SAML 2.0. Reportez-vous à ce module d'extension lorsque vous êtes invité à rechercher et à cliquer sur le nom du module d'extension.

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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

   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>.

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 ces entrées :

- L'élément `SingleSignOnService` avec un attribut `Binding` qui contient une valeur `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 `HTTP-Redirect`. L'attribut `Location` répertorie l'URL requise par l'intégration pour le service SingleLogoutRequest.

Remarque :
L'intégration SAML 2.0 prend uniquement en charge la liaison aux services IdP par redirection HTTP.

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 de l'IdP

Fournissez l'URL aux IdP qui émettront le jeton de sécurité.

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*, entrez l'URL de votre fournisseur d'identité.

   Chaque URL IdP doit être unique. Par défaut, l'intégration contient l'URL de 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 demande 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 en tant que paramètre* SAMLRequest, entrez l'URL de la liaison HTTP-Redirect obtenue à partir de l'élément SingleSignOnService .
2. Cochez la case en regard de *Signer l'AuthnRequest* pour activer le service d'authentification unique du fournisseur d'identité pour recevoir une 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 de 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 de service de demande pour l'IdP de l'intégration à l'aide des métadonnées de l'IdP.

Avant de commencer
Rôle requis : admin

Procédure

1. *URL de base vers le 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 en tant que paramètre SAMLRequest. Par défaut, l'intégration contient l'URL du service SSOCircle.
2. Dans *l'URL de redirection des utilisateurs après la déconnexion, généralement vers le portail ayant activé la propriété SSO (par exemple, http://portal.companya.com/logout)*, saisissez l'URL vers laquelle vous souhaitez rediriger les utilisateurs une fois qu'ils se sont déconnectés.

   Si votre IdP utilise l'authentification basée sur un formulaire, saisissez l'URL du formulaire de connexion de votre IdP. 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 ne se connectent pas à nouveau. Par défaut, l'intégration contient l'URL vers la page d'interface utilisateur statique external_logout_complete.do.

(Facultatif) Activer les demandes de déconnexion signées

Certains IdP 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 IdP nécessite des demandes de déconnexion signées, utilisez les données météorologiques de l'IdP 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 IdP nécessite 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 *Protocole de liaison pour le 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 ».)* , saisissez l'une des valeurs prises en charge répertoriées dans Attribut de liaison à partir de l'élément SingleLogoutService .

   Par défaut, l'intégration utilise une liaison de redirection HTTP.
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.

Suivez le processus séquentiel pour définir 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 ServiceNow (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 de l'entité ou l'émetteur*, saisissez l'URL de base (hors 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 le destinataire souhaité 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 de l'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 services.

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 dans 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 de `emailAddress`.
   La valeur de cet élément est le format par défaut utilisé par l'intégration.
2. Passez en revue les 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 d'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 de sélectionner dans la table Utilisateur un champ qui correspond au format du jeton `NameID` . En règle générale, les IdP 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 à utiliser comme jeton `NameID` . Pour utiliser un autre champ de la table Utilisateur comme jeton `NameID` , vérifiez d'abord que l'IdP propose 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 de l'élément `NameIDFormat` de l'IdP aux champs de la table Utilisateur.
2. Sélectionnez un format `NameID` où il existe 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* , saisissez 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 NameID de l'IdP

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.

Procédure

1. Dans la propriété *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 User afin de rechercher l'utilisateur.* , saisissez 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 dans le champ Table d'utilisateur pour SAML

Assurez-vous que le champ Table d'utilisateurs de l'intégration contient les valeurs correspondantes appropriées.

Par exemple, si l'intégration utilise le champ e-mail comme jeton `NameID` , assurez-vous que l'instance répertorie la même adresse e-mail que l'IdP. L'intégration échoue à authentifier un utilisateur qui n'a pas de valeur correspondante pour le jeton `NameID` .

(Facultatif) Activer la fourniture d'une classe de contexte d'authentification pour SAML

Vous pouvez permettre à l'instance d'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 IdP 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*, saisissez l'URN de la classe de contexte que *vous souhaitez utiliser pour l'authentification (voir tableau) dans la méthode AuthnContextRef que nous demanderons dans notre SAML 2.0 AuthnRequest au fournisseur d'identité* .

Options d'URN AuthnContextClass

Type d'authentification	URN de classe de contexte d'authentification
Authentification basée sur les formulaires	`urn :oasis :names :tc :SAML :2.0 :ac :classes :PasswordProtectedTransport`
Authentification basée sur Kerberos	`urn :federation :authentication :windows`

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 la signature des 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 de vos certificats d'autorité de certification signés.

Avant de commencer
Rôle requis : admin

Procédure

1. Dans la propriété *L'alias de saisie de clé stocké dans le magasin de clés SAML 2.0 SP utilisé pour signer les demandes SAML 2*, saisissez le nom de l'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 *Mot de passe de saisie de clé stocké dans le magasin de clés SAML 2.0 SP utilisé pour signer les demandes SAML 2*, saisissez le mot de passe de votre magasin de clés SAML 2.0.
   Par défaut, le mot de passe est le même que le nom de l'alias par défaut.
3. Cliquez sur **Mettre à jour**.
4. Régénérez les métadonnées de votre portail de services.
   Pour plus d'informations, consultez Métadonnées du portail de services.

Créer un magasin de clés de fournisseur de service pour SAML

Pour que votre instance puisse signer les demandes de déconnexion, vous devez créer un magasin de clés Java contenant les éléments suivants.

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 publique et privée

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 principal 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 une connaissance technique des certificats de sécurité. L'assistance technique ne peut pas vous aider à créer les certificats.

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 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
```

Installer un magasin de clés de fournisseur de service pour la signature des demandes SAML

Utilisez 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 **Fournisseurs multiples** > **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 davantage la sécurité et de déboguer l'intégration.

Paramètres avancés

Accédez à la **Tous** > **Authentification unique SAML 2** > **Propriétés**.

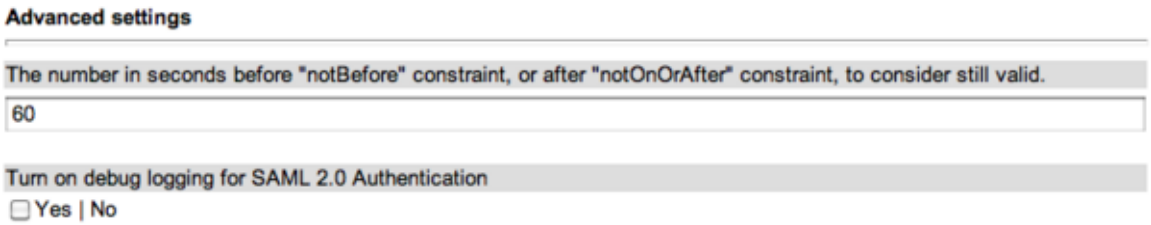


Table des propriétés système avancées

Propriété	Description
Nombre de secondes pendant lesquelles considérer toujours valide la contrainte « notBefore », ou après la contrainte « notOnOrAfter »	Entrez 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 requêtes qui ne sont pas effectuées dans les délais spécifiés. Si l'horloge IdP et l'horloge SP sont significativement 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 les 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'identification puisse vérifier les communications avec le fournisseur de service.

Avant de commencer

Rôle requis : admin

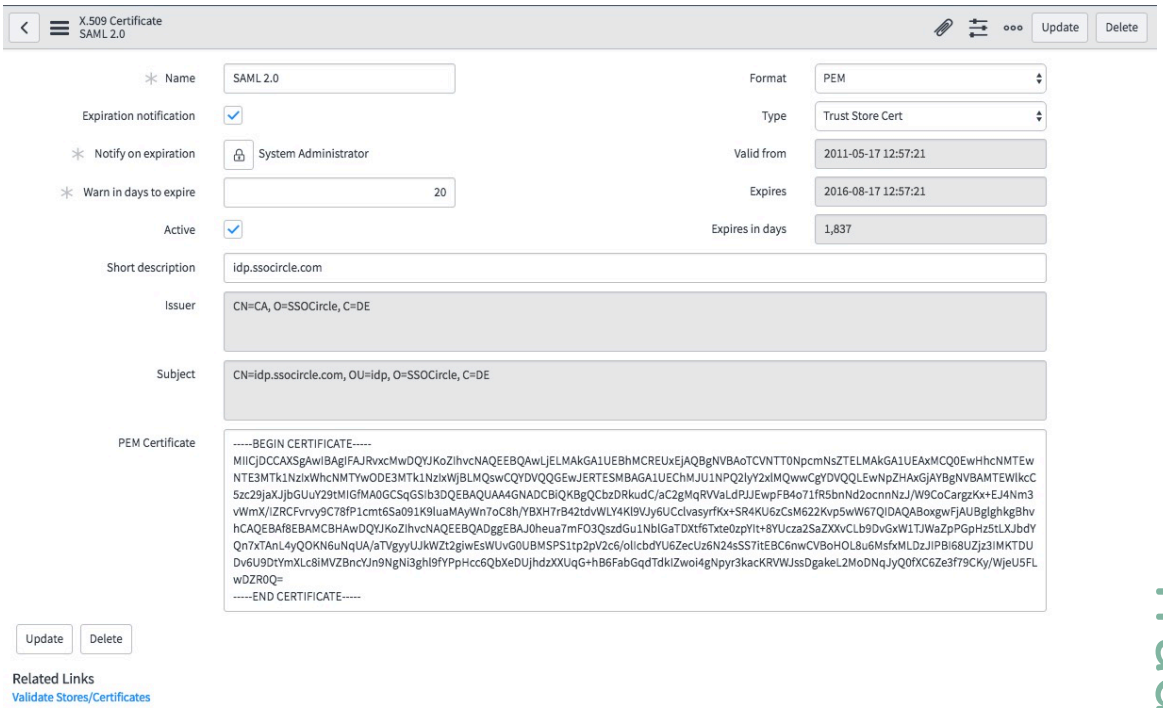
Pourquoi et quand exécuter cette tâche

Le certificat de l'IdP se trouve dans les métadonnées de l'IdP. Le développeur IdP détermine où résident les métadonnées du 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 des 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**.



Remarque :
À l’heure actuelle, l’intégration ne signe pas 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 puisse l’utiliser. Cette condition n’est vraie que si vous n’utilisez Authentification unique (SSO) de plusieurs fournisseurspas .
Notification d'échéance	Sélectionnez cette option pour envoyer une notification aux utilisateurs sélectionnés dans le champ **Notifier 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 ayant le rôle administrateur.
Avertissement avant l'expiration (en jours)	Nombre de jours avant l’expiration de l’envoi de la notification par l’instance. Saisissez une valeur d’au moins 20. Les instances mises à niveau vers Istanbul et les versions ultérieures ont cette valeur définie sur 20, sauf si une valeur supérieure est spécifiée.
Actif	Case à cocher pour indiquer que ce certificat est actif.
Format	Le format du certificat. SAML utilise le format **PEM** .
Type	Le conteneur de certificats. L’instance reconnaît les certificats des magasins de confiance, du magasin de clés Java et des magasins de clés PKCS#12.
Date de début de validité	L’instance ajoute automatiquement la date de début de validité du certificat dans 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.

Champ	Description
Échéance en jours	Nombre calculé de jours jusqu'à l'expiration.
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 l'objet du certificat dans ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Certificat PEM	Saisissez la valeur du certificat X509.

Que faire ensuite

Cliquez sur **Valider les magasins/certificats** pour tester le magasin de confiance et le certificat.

Remplacement d'un certificat manquant pour SAML

Si le module **Certificat** affiche une page vide, l'enregistrement de 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 n'est vraie que si vous n'utilisez Authentification unique (SSO) de plusieurspas .

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 IdP.
5. Cliquez sur **Enregistrer**.

Installer un magasin de clés de fournisseur de service pour la signature des demandes SAML

Utilisez 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 **Fournisseurs multiples** > **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**.

Tester l'intégration SAML

Testez l'intégration SAML une fois que vous avez terminé toutes les autres tâches de configuration.

Avant de commencer
Rôle requis : admin

Procédure

1. Connectez-vous à l'instance en tant qu'utilisateur doté du rôle administrateur.
2. Accédez à la **Authentification unique SAML 2** > **Propriétés**.
3. Dans la propriété *Activer l'authentification externe*, sélectionnez **Oui**.

Remarque :

L'activation de l'authentification externe requiert que tous les utilisateurs utilisent l'authentification unique SAML 2.0. Si quelqu'un tente d'accéder à l'application avec un état non authentifié, l'instance envoie automatiquement une demande d'authentification à l'IdP et redirige l'utilisateur vers la page d'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 de Multi-SSO (SAML 2.0)

Erreurs et correctifs de Multi-SSO (SAML 2.0)

Une liste des erreurs courantes et des correctifs associés pour une installation et une configuration de l'authentification unique (SAML 2.0).

servicenow

Erreurs lors de la configuration de SSO à fournisseurs multiples (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 dans l'instance.
Les certificats ne correspondent pas. Attendu : <certStr>, réel : <inboundCert>.	Vérifiez que le certificat IDP x509 est présent, valide et actif.	N. A.	Le certificat disponible dans SNC ne correspond pas au certificat dans l'assertion. Les causes sont les suivantes : • Le certificat est mis à jour sur l'IdP, mais pas dans l'instance ServiceNow. • Le format du certificat n'est pas correct.	Vérifiez que la chaîne au format PEM dans l'enregistrement de certificat SAML 2.0 correspond au certificat X509 dans SAMLResponse pour l'IdP d'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	N. A.	L'assertion peut être signée avec un certificat différent.	Vérifiez si l'IdP possède le même certificat que l'instance SNC.

Traduction automatique

Erreurs lors de la configuration de SSO à fournisseurs multiples (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
	IDP x509 est présent, valide et actif.			
InResponseTo dans l'incompatibilité de SubjectConfirmationData. Attendu : <inResponseTo>, réel : <inResponseTo>.	Échec de la validation de la confirmation de l'objet.	N. A.	Cette erreur s'affiche si l'une des situations suivantes se produit : • L'IdP renvoie une réponse SAML pour une autre requête SAMLRequest • Un utilisateur place un signet sur l'URL avec SAMLRequest au lieu de l'URL d'instance uniquement • Si une valeur null est attendue, la réponse peut être envoyée à un autre nœud lorsque l'instance dispose de plusieurs nœuds.	L'administrateur IdP doit confirmer que la réponse SAML attendue est renvoyée. Il peut s'agir d'un problème d'équilibreur de charge ou d'infrastructure.
Valeur SessionIndex 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 de l'objet.	N. A.	Des conditions peuvent être manquantes en raison d'une erreur sur l'IdP. Le StatusCode de la réponse contient Répondeur au lieu de la valeur Succès attendu.	Passez en revue SAMLResponse pour déterminer si les conditions sont incluses dans SAMLResponse. Les données de confirmation d'objet valides peuvent être expirées ou non destinées à la bonne audience.

Erreurs lors de la configuration de SSO à fournisseurs multiples (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
Incohérence de l'audience d'assertion. Attendu : <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 d'audience configurée pour l'instance SNC doit correspondre à la valeur de l'IdP.	Recherchez <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. Attendu : <valeur sur l'instance>, réel : <valeur renvoyée par l'IdP>	L'émetteur de l'assertion n'est pas valide.	URL du fournisseur d'identité qui émet le jeton de sécurité SAML2 avec les informations de l'utilisateur.	L'ID d'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 (URL du fournisseur d'identité qui émet le jeton de sécurité SAML2 avec les informations de l'utilisateur) est définie correctement.
L'objet est valide dans le futur. Maintenant : <maintenant>, NotBefore : <notBefore > ou L'objet a expiré. Maintenant : <now>, 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 du SP.	Mettez à jour la propriété SAML glide.authenticate.sso.saml2.clockskew vers une valeur plus grande. La valeur par défaut est 180 secondes. Certains cas nécessitent un paramètre de 300 ou plus. Vous devrez peut-être également vérifier l'heure sur votre serveur IdP.

Erreurs lors de la configuration de SSO à fournisseurs multiples (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
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 du SP	Mettez à jour la propriété SAML vers une valeur plus grande. 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 de connexion et d'IdP courantes

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` sans ajouter le nom d'hôte IdP à la valeur de la propriété. **Remarque :** Pour en savoir plus sur cette propriété, consultez Liste d'autorisation d'URL pour les redirections de déconnexion Paramètres de renforcement de la sécurité de l'instance.	Définissez (ou créez) la propriété système glide.authenticate.failed_redirect pour rediriger les demandes d'authentification ayant échoué vers cette URL.
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 lequel n'est pas l'algorithme de signature attendu http://	Consultez l'onglet Contexte de l'alerte pour connaître les détails de 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.

Erreurs de connexion et d'IdP courantes (suite)

Erreur ou symptôme	Diagnostic	Corriger
www.w3.org/2000/09/xmldsig#rsa-sha1.		
Le message d'erreur urn :oasis :names :tc :SAML :2.0 :status :Requester s'affiche dans votre table de journal système (syslog).	Lorsque votre IdP (par exemple, ADFS) renvoie l'état oasis :names :tc :SAML :2.0 :status :Requester, cela signifie que l'IdP a rejeté la connexion en raison d'un problème avec la demande qui lui a été envoyée. Malheureusement, la réponse SAML reçue de l'IdP ne fournit pas plus de détails sur l'erreur.	Examinez la demande SAML envoyée à l'IDP et collaborez avec l'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 connaître 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 les inviter à 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. De même, 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 l'authentification unique. La page login.do est toujours accessible et les utilisateurs peuvent se connecter au système s'ils ont défini un mot de passe local.

Propriétés de la redirection

Lorsqu'un utilisateur se déconnecte, ou en cas d'échec de sa tentative de connexion à l'aide de SSO, vous pouvez définir l'endroit vers lequel l'utilisateur sera redirigé ensuite, par exemple vers une page de portail principale ou un article de la base de connaissances contenant les 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 créer la propriété.

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 vers laquelle rediriger les utilisateurs après la déconnexion, généralement vers le portail ayant activé la connexion Single Sign-on (par exemple, http://portal.companya.com/logout).

glide.authentication.external.disable_local_login

Lorsque la valeur est définie sur vrai, elle nécessite des informations d'identification SSO 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

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 fournisseur SSO où la co et où les informations d'i collectées.
failed_authentication	*glide.authenticate.failed_redirect*	Lorsque cette valeur est r indique que les informatio SSO fournies ont échoué l'utilisateur n'existe pas o est verrouillé. La connexi session est redirigée vers par la propriété. Il s'agit g l'URL du fournisseur SS est contestée et où les info d'identification sont colle
<*user_id*>	N. A.	Connexion autorisée pour par <*user_id*>. Cett au nom de champ défini d *glide.authenticat* SSO (« nom de champ de en correspondance avec l'

Restriction de la connexion locale

Par mesure de sécurité, vous ne devez pas vous contenter de vous fier aux propriétés de redirection pour interdire la connexion locale. Si un utilisateur ne doit jamais se connecter localement et qu'il 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 le 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

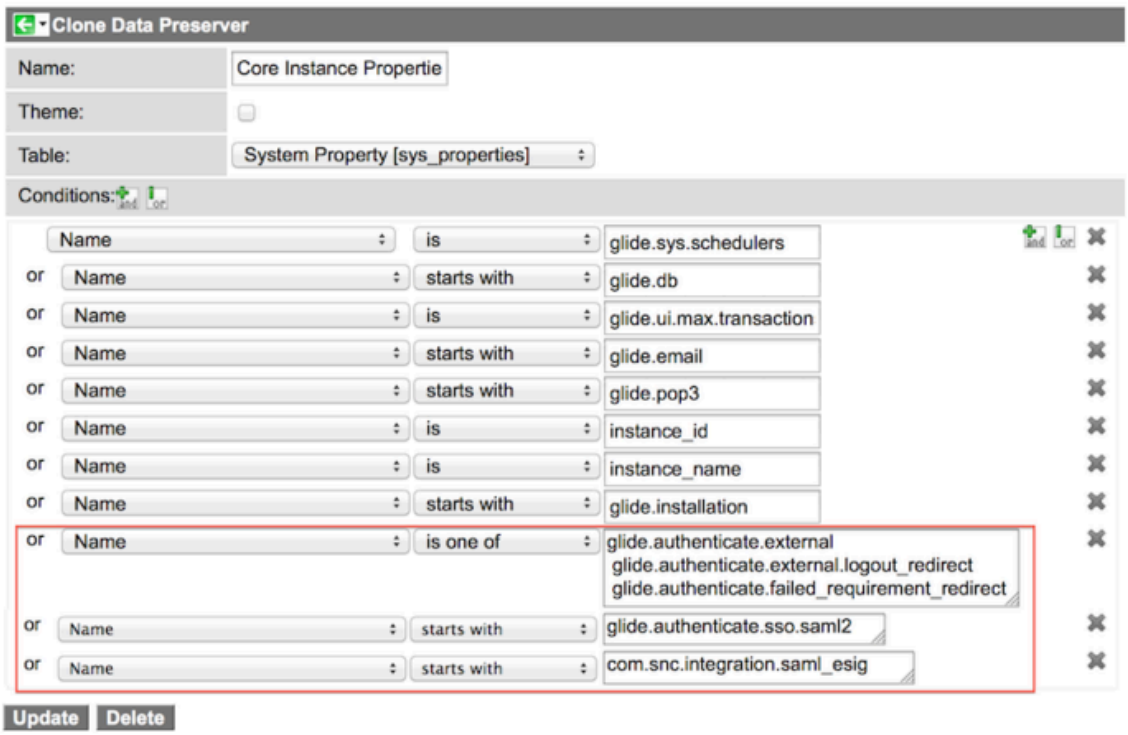
Clonez une instance avec une intégration SAML. Avant de cloner une instance qui utilise SAML 2.0, conservez les paramètres liés à l'authentification unique SAML sur l'instance cible, sinon vous risquez de rendre l'instance cible inaccessible.

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 SSO SAML suivantes sont préservées à l'aide de conditions.
   - glide.authenticate
   - glide.security
   - glide.entry
   - glide.script
   - glide.session
   - 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 à 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 d'instance.

3. Sur l'instance source, accédez à **Clone système** > **Conserver les données** pour préserver les certificats SAML sur les sys_certificate et les utilisateurs SAML sur les sys_user liées à SAML/SSO/Multi SSO.

   Si vous en avez besoin, exportez-les au format 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 pourra pas s'authentifier et votre instance cible deviendra inaccessible. De plus, ne modifiez pas l'sys_id de l'enregistrement de votre fournisseur Multi SSO ; Cela obligera vos utilisateurs à vider leurs cookies. Pour plus d'informations sur les précautions à prendre en matière 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 façon 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 ou SAML) sur l'instance cible et avec un sys_id qui n'existe pas sur l'instance source.
7. Cliquez sur **Mettre à jour**.

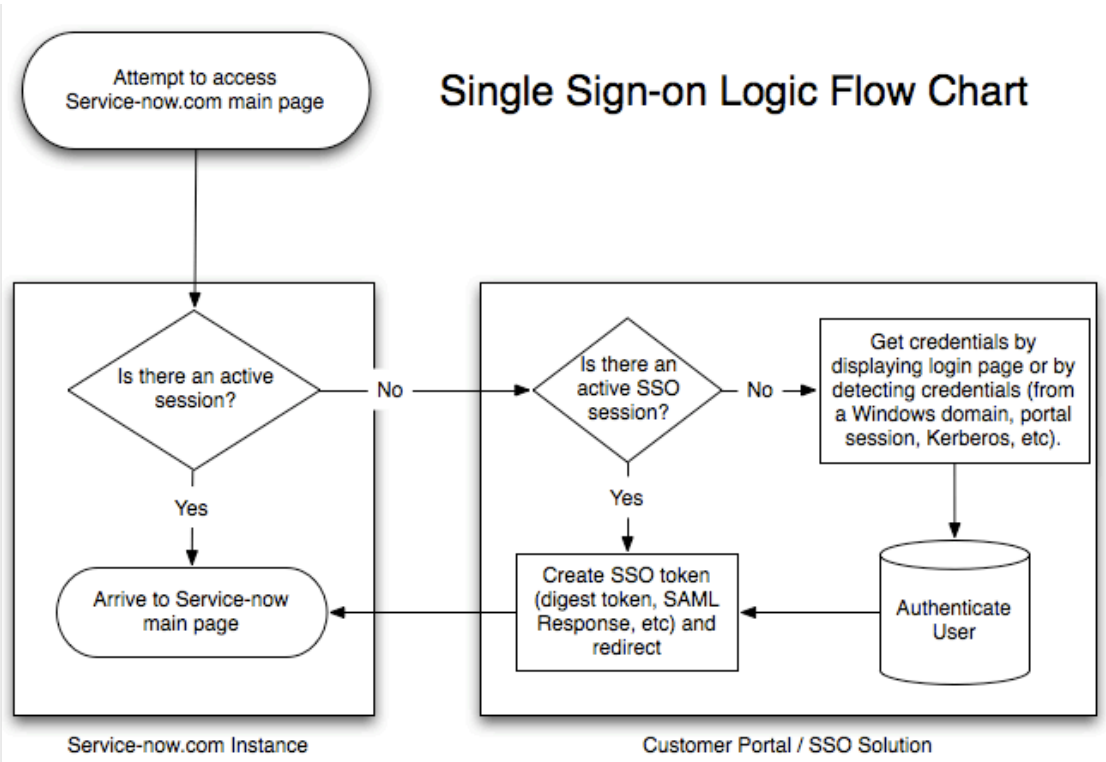
Concepts de SAML 2.0

Familiarisez-vous avec ces concepts SAML.

Flux de processus SAML classique (diagramme)

Un flux logique SSO classique implique de rechercher une session active, de vérifier les informations d'identification de l'utilisateur et de créer le jeton nécessaire.

Norme SSO



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 niveau du portail de services

Le principal demande une ressource cible auprès du 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'ils existent, l'utilisateur a déjà validé avec l'IdP et peut ignorer les étapes 2 à 6.

Problème 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 URL `RelayState` .

Le jeton `RelayState` est une référence opaque aux informations d'état conservées chez le fournisseur de services. La valeur du paramètre `SAMLRequest` est la valeur déflatée et codée 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 encode ensuite l'élément <samlp :AuthnRequest> et l'envoie comme paramètre d'URL SAMLRequest .

Le service SSO traite l'élément <samlp :AuthnRequest> en procédant au décodage d'URL, au décodage 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 identifie l'utilisateur en le demandant ses informations d'identification de connexion. Si l'utilisateur est déjà connecté, l'IdP répond simplement avec les paramètres d'URL SAMLResponse<tt> et <tt>RelayState (voir l'étape 3).

Répondre avec une réponse SAML 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
 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 SAMLResponse

La valeur de la réponse SAML est décodée et gonflée en base64 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.

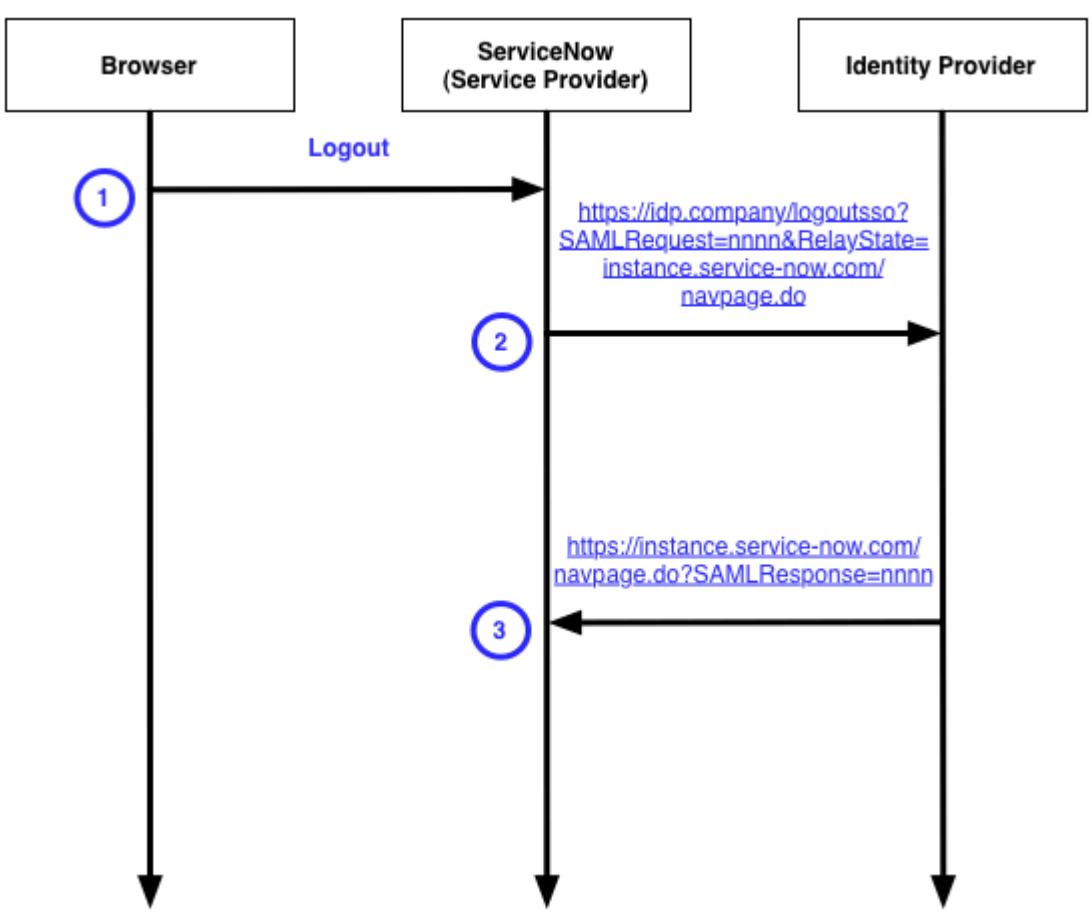
Le script de connexion extrait également l'ID de session de l'élément //AuthnStatement/@SessionIndex et le stocke pour la LogoutRequest.

Flux de processus de déconnexion (LogoutRequest)

Pendant la déconnexion, l'instance émet l'appel de service SAML 2.0 *LogoutRequest* à l'IdP.

Ce service déconnecte l'utilisateur, puis le redirige vers l'URL de déconnexion spécifiée.

Déconnexion SAML 2



Traduction automatique

L'utilisateur clique sur le bouton de déconnexion

L'utilisateur clique sur le bouton **Déconnexion** , et l'instance exécute le script de déconnexion.

LogoutRequest émise

Le script de déconnexion construit une `LogoutRequest` SAML 2.0 et la publie sur le service SAML 2.0 SingleLogoutRequest préconfiguré au niveau de l'IdP. L'IdP dégonfle la demande, puis base64 la code. Voici un exemple de `LogoutRequest` :

```
<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>
```

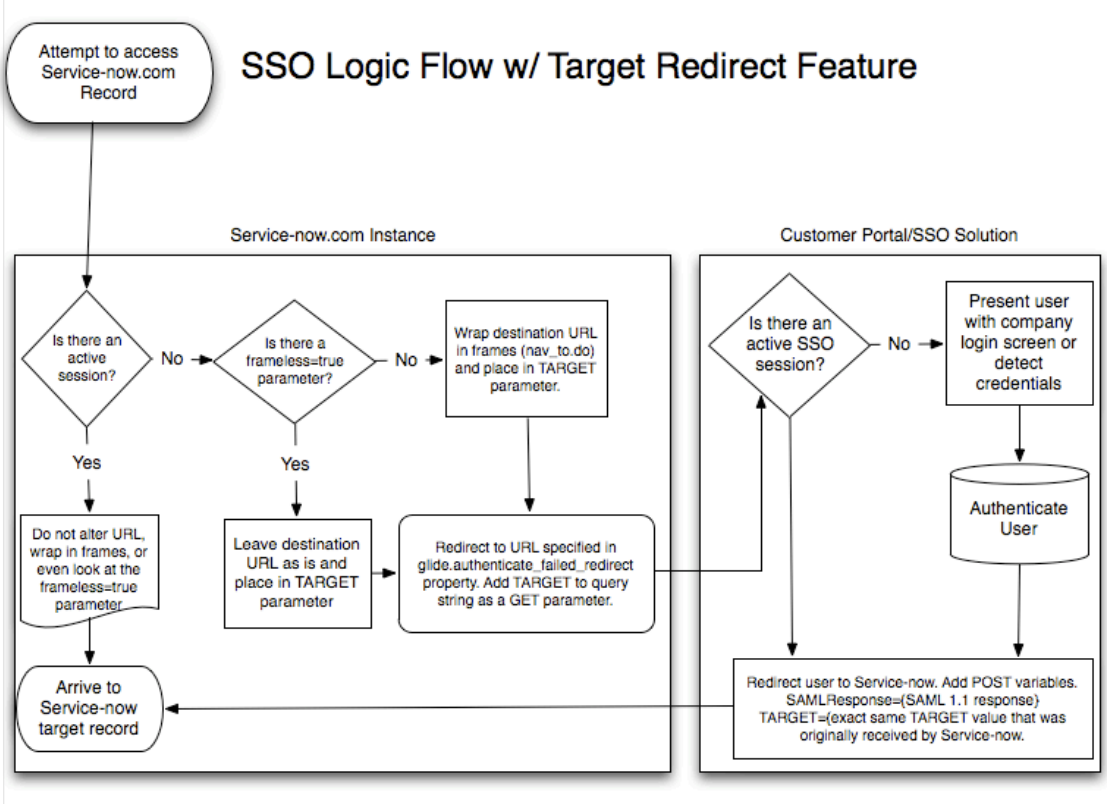
L'utilisateur se déconnecte

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 cible SSO



Les valeurs de retour de sortie d'installation ont été améliorées pour transmettre une URL à la place ou en plus de l'URL définie par les propriétés. Généralement, vous devez renvoyer 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 l'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 réussi.

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

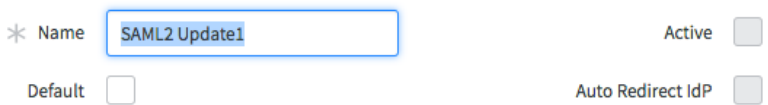
Remarque :
Nouveau dans la Jakarta version, vous devez valider votre configuration à l'aide de la fonctionnalité Test de la connexion avant de pouvoir activer votre configuration IdP. Vous pouvez toujours utiliser la fonctionnalité Mettre à jour pour enregistrer vos données de configuration, mais il 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. Pour une nouvelle configuration, entrez les informations IdP via l'une des méthodes suivantes :

Option	Description
Utilisation d'une URL de descripteur de métadonnées	Cochez la case URL et saisissez 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.

Tous les champs obligatoires doivent être renseignés dans le formulaire Fournisseur d'identité.



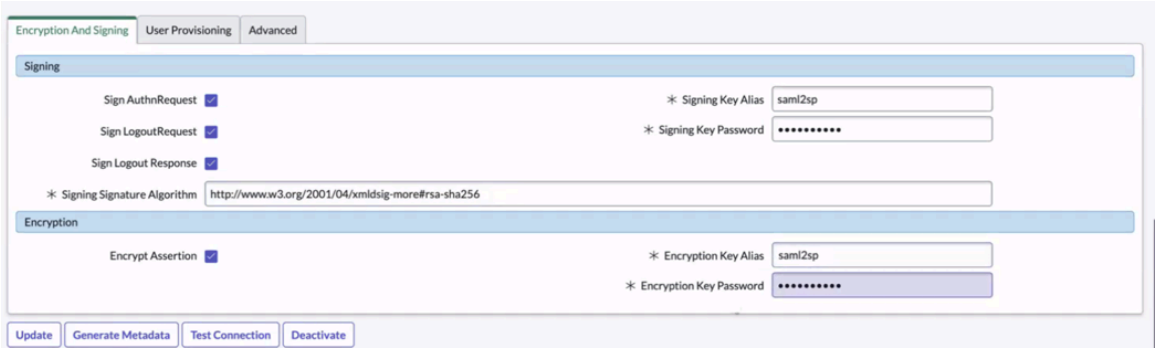
Champs d'authentification unique de plusieurs fournisseurs

Propriété	Obligatoire	Description
Nom	Oui	Entrez 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. **Remarque :** La possibilité de définir cette propriété n'est disponible qu'après un test de connexion réussi.
Par défaut	Non	L'IdP de redirection automatique, anciennement connu sous le nom d'IdP principal, redirige automatiquement les utilisateurs pour accéder à l'URL de l'instance de base. Cette propriété définit cette configuration IdP comme configuration par défaut.

Propriété	Obligatoire	Description
Rediriger automatiquement l'IdP	Non	Définit cette configuration IdP 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, activée automatiquement, contrôle cette fonctionnalité.
URL du fournisseur d'identité	Oui	Entrez l'URL de votre fournisseur d'identité. 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.

4. **Facultatif :** Onglet Chiffrement et signature

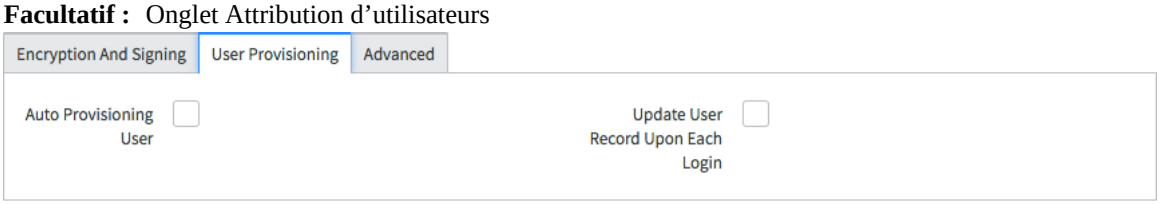
Remarque :
Il est recommandé d'utiliser vos propres certificats pour le chiffrement et la signature.



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	Saisissez 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	Saisissez le mot de passe de chiffrement de l'entrée de clé stockée dans le magasin de clés SAML 2.0 SP.
Chiffrer l'assertion	Cochez la case pour chiffrer l'assertion dans la réponse SAML. Les métadonnées générées pour l'IDP intègrent 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 permettre au service d'authentification unique IdP de recevoir une demande AuthnRequest signée.
Signer la LogoutRequest	Cochez la case pour permettre au service d'authentification unique IdP de recevoir une LogoutRequest signée.
Signer la réponse de déconnexion	Cochez la case pour permettre au service d'authentification unique IdP de recevoir une réponse de déconnexion signée.

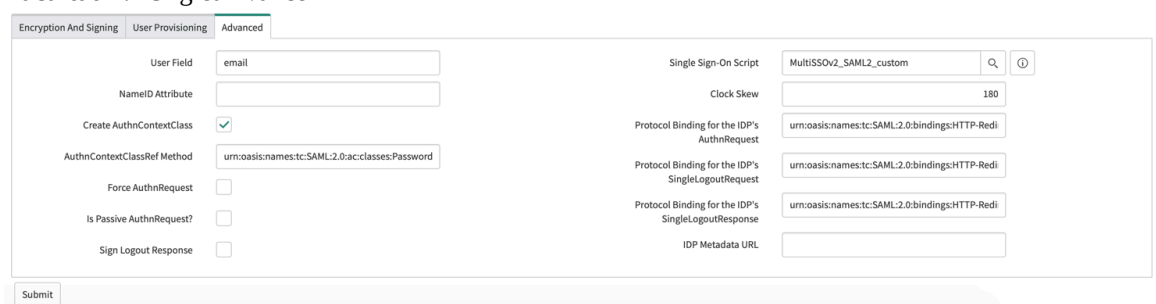
5. **Facultatif :** Onglet Attribution d'utilisateurs



Champs d'attribution d'utilisateurs

Propriété	Description
Mise en service automatique de l'utilisateur	Activez l'attribution automatique des utilisateurs, crée les utilisateurs lorsque l'utilisateur n'existe pas dans la table Utilisateur de l'instance en fonction des informations fournies par 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 dont l'IdP a besoin 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 des utilisateurs système, cet ID unique correspond aux détails de l'utilisateur.
Attribut NameID	Laissez ce champ vide à moins que vous ne configuriez une nouvelle politique NameID. Si vous configurez une nouvelle politique, le système requiert la table Utilisateurs qu'il doit utiliser pour identifier l'utilisateur qui se connecte. Ici, le système fait correspondre le jeton NameID au nom de ce champ de la table Utilisateur.
Créer une AuthnContextClass	Cochez la case pour spécifier une classe de contexte particulière, telle que Transport protégé par mot de passe. Si la case est décochée, 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 la case pour forcer l'exécution des AuthnRequests.
Est une AuthnRequest passive	Cochez la case si la demande AuthnRequest est passive.
Script d'authentification unique	Sélectionnez le script Single Sign-on. La valeur par défaut est *MultiSSOV2_SAML2_custom*.
Signer la réponse de déconnexion	Entrez les détails de la réponse de déconnexion dans ce champ.

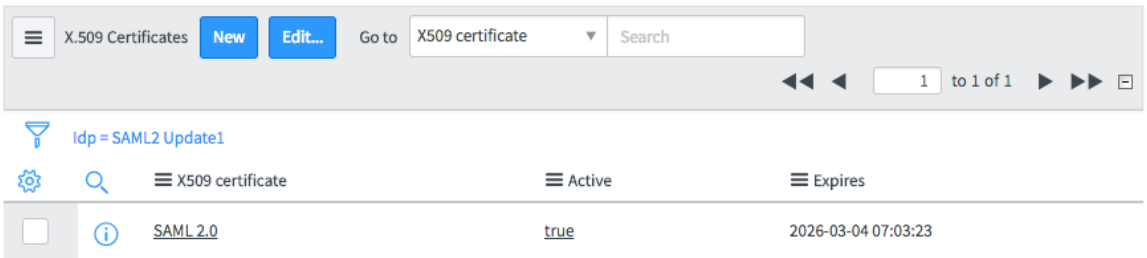
Propriété	Description
Décalage d'horloge	Entrez le nombre de secondes entre les deux attributs qui composent la réponse SAMLResponse nonce. La valeur par défaut est 60. Une réponse SAML valide doit se situer entre les valeurs de date/heure *notBefore* et *notOnOrAfter* . Consultez Exemple de réponse SAML 2 avec les éléments SubjectConfirmation et SubjectConfirmationData et Exemple de réponse SAML 2 avec les éléments AudienceRestrictions et Audience pour obtenir 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 défini, 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 ne s'affiche pas automatiquement.
Demande	ID unique Dans le cadre de la demande, l'ID peut être le nom d'utilisateur, l'ID d'employé, etc. **Remarque :** La redirection et la post-liaison sont prises en charge pour la demande. L'option permettant de définir ce champ n'apparaît qu'après un test de connexion réussi. Pour plus d'informations, reportez-vous à la section Test des connexions IdP.
Réponse	ID unique Dans le cadre de la réponse, l'ID peut être le nom d'utilisateur, l'ID d'employé, etc. **Remarque :** La redirection et la liaison postérieure sont prises en charge pour la réponse. L'option permettant de définir ce champ n'apparaît qu'après un test de connexion réussi. Pour plus d'informations, reportez-vous à la section Test des connexions IdP.

Certificats X.509 pour SAML

Stockez et activez les certificats 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 des métadonnées à partir duquel les propriétés IDP sont importées**, le système interroge automatiquement l'IdP pour obtenir un certificat actuel et 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 se produit si l'IdP est accessible en dehors de votre réseau.



Visite guidée SAML

Utilisez la visite guidée SAML pour configurer SAML pour l'authentification unique.

La visite guidée SAML vous aide à suivre une formation et à configurer l'authentification unique (SSO) pour votre ServiceNow® instance. Les administrateurs peuvent sélectionner la visite guidée pour connaître rapidement les actions requises lors de la configuration de la 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 apprendre à 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 Single Sign-on (SSO) avec ServiceNow®
- Ping: Configurer l'authentification unique SAML avec ServiceNow®
- ADFS : intégration à SAML 2.0

Pour utiliser la visite guidée SAML, activez le module d'extension Integration - Multiple Provider Single Sign-On Installer. 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 **d'aide** .
5. Cliquez sur **Take a Tour (Visite guidée**).

La visite guidée SAML utilise une série d'étapes réparties 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 guidée. Pour en savoir plus sur la configuration SAML, reportez-vous à Configuration SAML 2.0 à l'aide de l'authentification unique (SSO) de plusieurs fournisseurs.

Intégration de SAML 2.0 avec d'autres fonctionnalités

Vous pouvez intégrer votre solution SAML 2.0 à d'autres fonctionnalités telles que la signature électronique, les liens profonds et ADFS.

Ajouter la prise en charge des liens profonds pour SAML

Le lien profond permet aux instances de prendre en charge les liens directs par e-mail vers un enregistrement spécifique dans le système.

Lorsque l'intégration SAML 2.0 est activée, les URL de liens profonds doivent passer un contrôle d'authentification avant que l'IdP ne redirige l'utilisateur vers l'URL initialement demandée. Prenons l'exemple d'un e-mail contenant l'URL suivante : 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 des liens profonds, 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 l'intégration de l'authentification unique (SSO) SAML 2. à Microsoft ADFS.

Pour plus d'informations sur l'installation et la configuration d'ADFS, consultez 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 SAML 2.0 SSO avec ADFS 2.0, 3.0, Azure AD.ributes ne prend pas en charge la réponse SAML dans

Configurer ADFS pour SAML

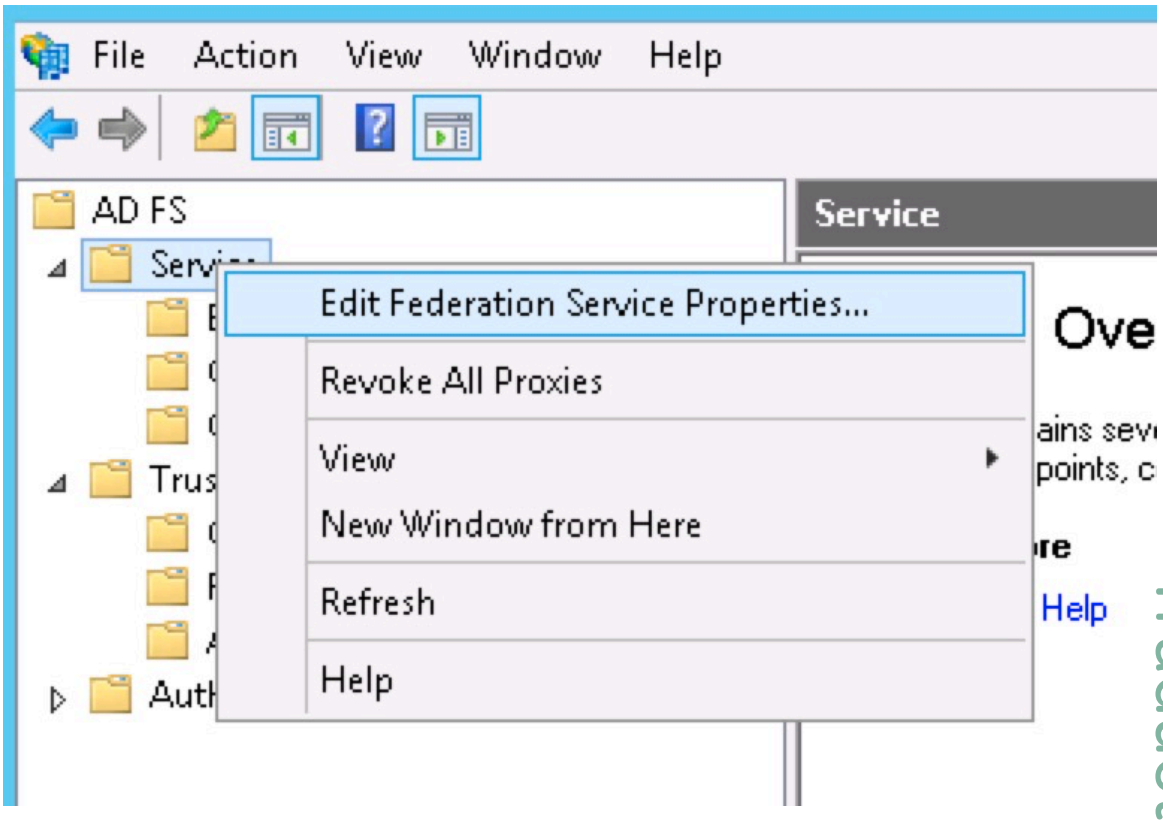
Configurez ADFS pour SAML. Cette procédure utilise ADFS 2.0 et affiche samportal.example.com comme le site Web ADFS. Remplacez-la par l'adresse de votre site Web ADFS.

Avant de commencer

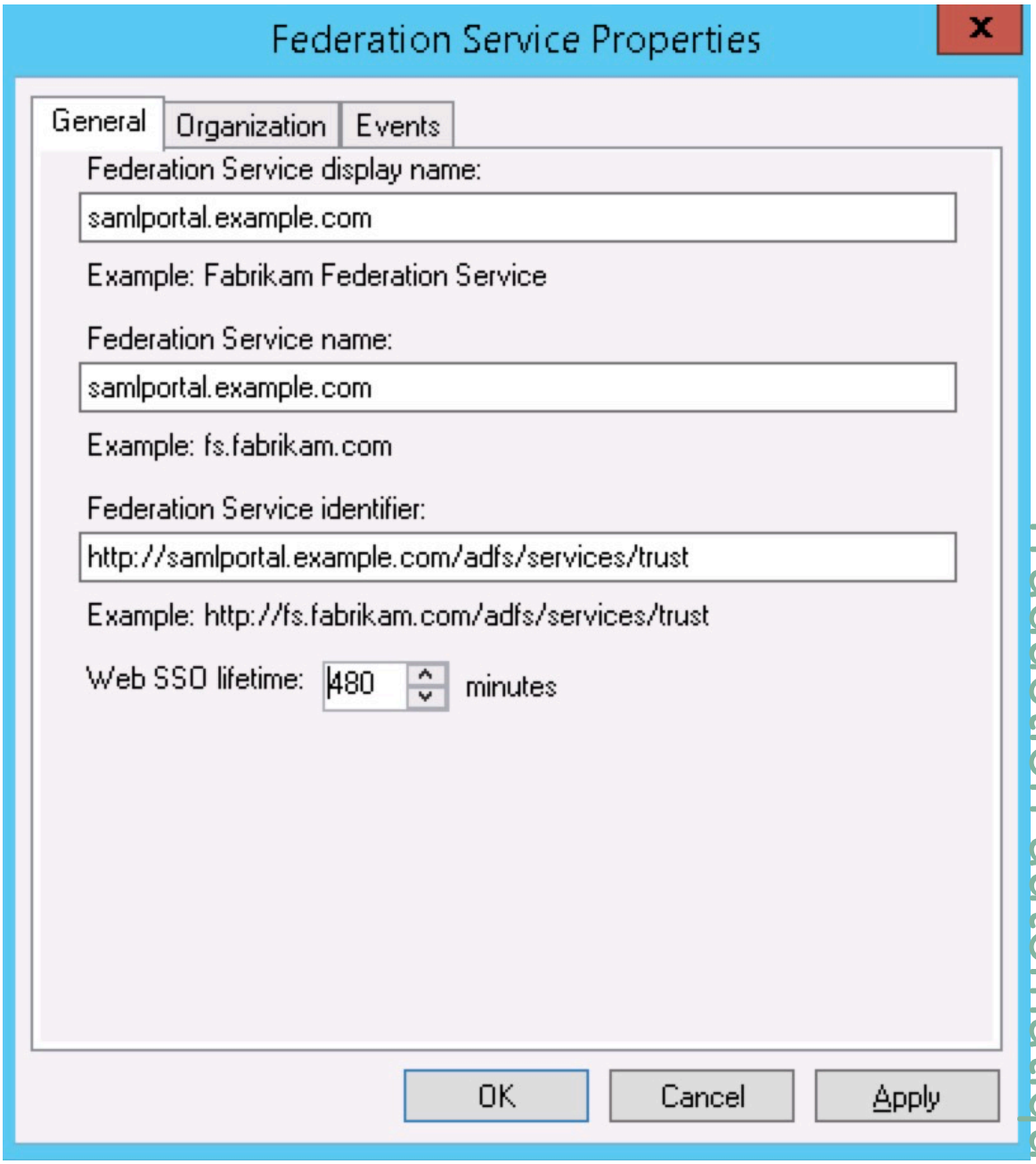
Rôle requis : admin

Procédure

1. Connectez-vous au serveur ADFS 3.0 et ouvrez la console de gestion.
2. Cliquez avec le bouton droit sur **Service** , puis sélectionnez **Modifier les propriétés de service de fédération**.



3. Vérifiez que les paramètres généraux correspondent à vos entrées DNS et à vos noms de certificat.



4. Accédez aux certificats et exportez le certificat de signature de jeton.

   a. Cliquez avec le bouton droit de la souris sur le certificat, puis sélectionnez **Afficher le certificat**.

   b. Sélectionnez l'onglet **Détails**.

   c. Cliquez sur **Copier dans le fichier**.
   L'assistant d'exportation de 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**.

f. Sélectionnez **le binaire codé DER X.509 (.cer),** puis cliquez sur **Suivant**.

g. Sélectionnez l'emplacement où vous souhaitez enregistrer le fichier, donnez-lui un nom, puis cliquez sur **Suivant**.

h. Sélectionnez **Finish** (Terminer).
L'instance exige 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/binaire 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
Effectuez ces étapes uniquement une fois que vous avez configuré ADFS pour SAML. Pour obtenir des détails sur ce processus, consultez Configurer ADFS pour SAML.

Rôle requis : admin

Procédure

1. S'il n'est pas déjà activé, activez le module d'extension Integration - Multiple Provider Single Sign-On Installer.
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** ont des valeurs et qu'il n'y a pas d'erreurs.
En cas d'erreur, ouvrez le certificat au format PEM enregistré dans le Bloc-notes et copiez-collez le certificat dans le champ Certificat PEM.
5. Vérifiez que la sortie d'installation SAML2SingleSignon_update1 est active.
6. Poursuivez la configuration de SAML 2.0.

Remarque :
Lorsqu'un certificat est mis à jour sur le serveur ADFS, vous devez également charger un certificat mis à jour sur 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 implémenter.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité** > **Mise à jour 1 de SAML2** > **Chiffrement et signature** et vérifiez que la propriété SAML Sign 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.

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 **Approbations de partie de confiance**.
5. Sélectionnez **Ajouter l'approbation de la partie de confiance** dans le coin supérieur droit de la fenêtre.

   L'assistant d'ajout s'affiche.
6. Cliquez sur **Démarrer** pour commencer.
7. Utilisez l'option **Importer un fichier** pour importer le fichier de métadonnées.
8. Attribuez-lui un nom d'affichage tel que ServiceNow et saisissez 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 défini sur le service qui a déjà été exporté. La définition d'un certificat empêche une communication appropriée 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 comme identificateur de confiance de la 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 décochez la case **Ouvrir les réclamations lorsque cette opération est terminée** .
15. Fermer cette page.
    La nouvelle approbation de la 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 des parties de confiance ADFS

Modifiez les règles de réclamation pour permettre une communication appropriée avec l'instance.

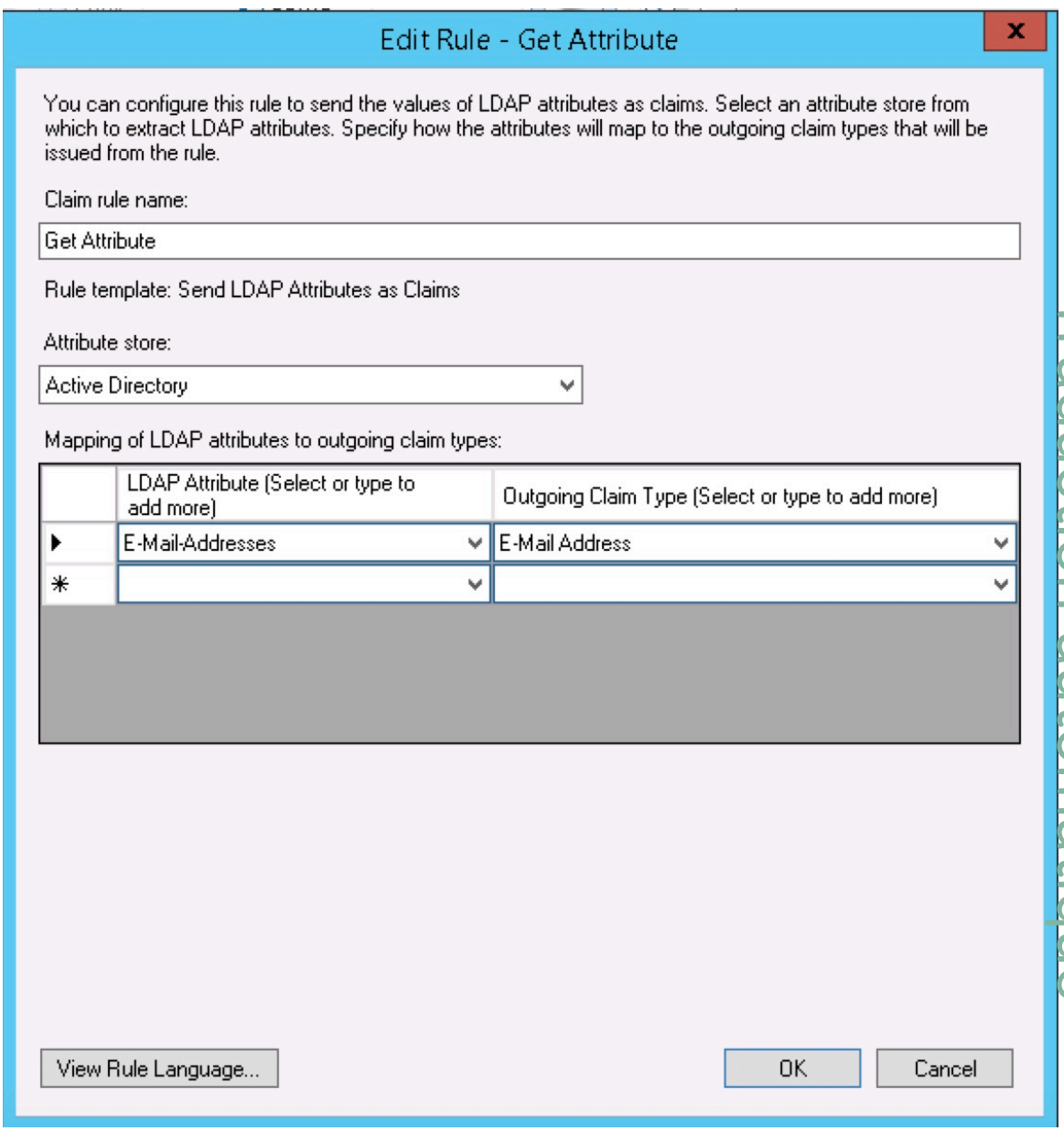
Avant de commencer

Rôle requis : admin

Procédure

1. Connectez-vous au serveur ADFS et ouvrez la console de gestion.
2. Cliquez avec le bouton droit de la souris sur la fiducie 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 un nom à la réclamation, par exemple `Obtenir des attributs LDAP`.
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`.



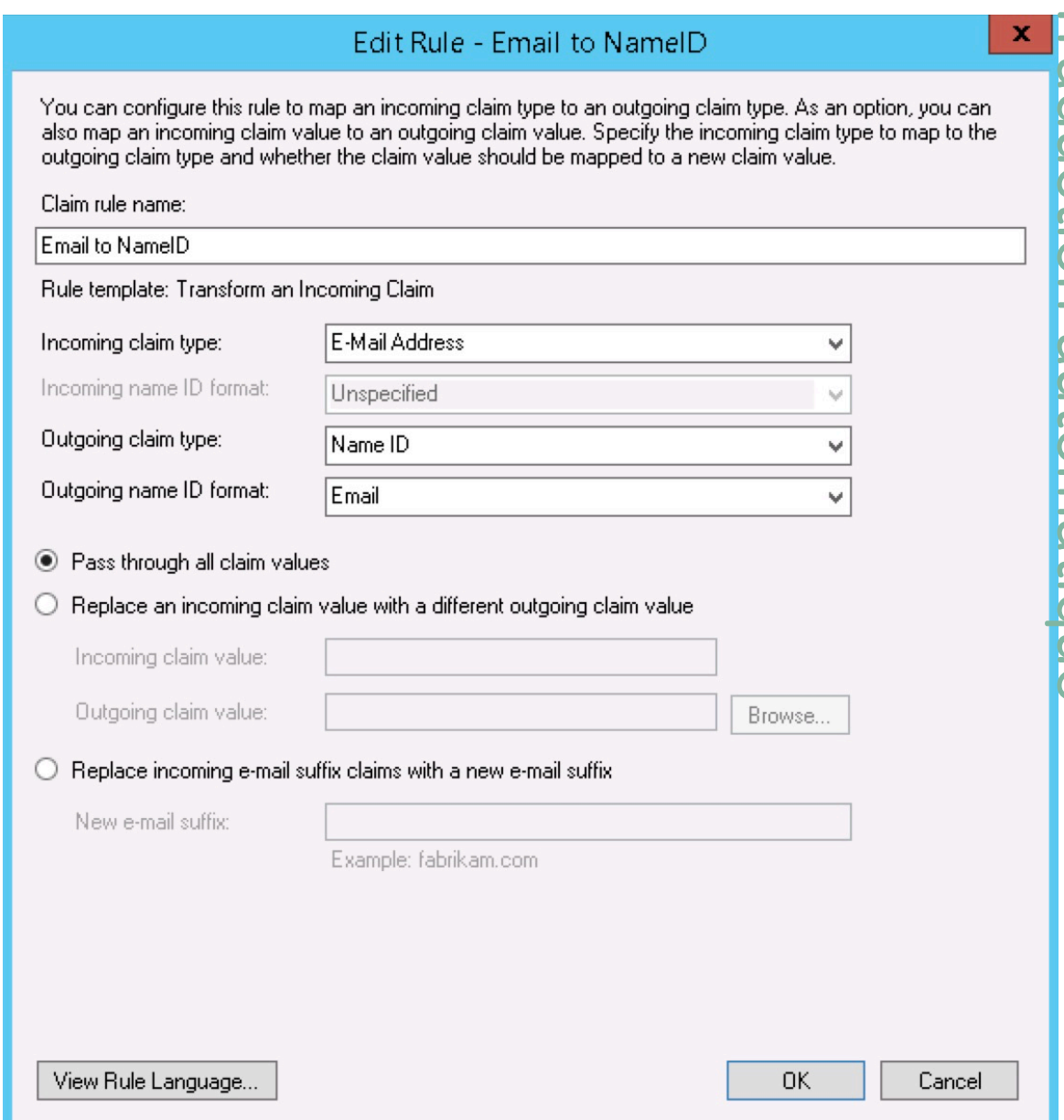

```
c:[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer
 == "AD AUTHORITY"]
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
query = ";mail;{0}", param = c.Value);
```

8. Sélectionnez **Finish** (Terminer).
9. Sélectionnez **Ajouter des règles**.

10. Sélectionnez **Transformer une réclamation entrante** en tant que modèle de règle de réclamation à utiliser.
11. Attribuez un nom à la réclamation, par exemple `Email to Name ID`.
12. Définissez le **type de réclamation entrante** sur le **type de réclamation sortante** dans la règle précédente.
    Par exemple, `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 définissez pendant la configuration SAML 2.0.

14. Sélectionnez **Transmettre toutes les valeurs de réclamation**.



Cette règle de revendication doit ressembler au langage 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"]
= "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 la déconnexion unique.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Consultez cet article sur la déconnexion ADFS pour plus d'informations .

Procédure

1. Accéder à **Gestionnaire ADFS** > **Relations de confiance** > **Approbations de parties de confiance** > **Propriétés de**.
2. Sous l'onglet Points de terminaison, cliquez sur **Ajouter SAML.**
3. Configurez les paramètres :
   - **Type de point de terminaison** : déconnexion SAML
   - **Reliure** : POST
   - **URL de confiance** : 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**.

Si vous avez configuré correctement 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 n'avez pas SAML 2.0 Update 1. Ce problème peut se produire si les utilisateurs tentent d'ignorer l'authentification IdP et accèdent directement à 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 pour créer une demande AuthnContextClass.
  Consultez Activer et configurer SAML 2.0.
- Modifiez le script **include 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 vers 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 des formulaires ». Dans ce contexte d'authentification, l'IdP doit présenter aux utilisateurs un formulaire d'informations d'identification. 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 auprès de l'IdP.

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 valeurs 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

Intégration ServiceNow à Azure Active Directory (Azure AD).

L'intégration ServiceNow à Azure AD vous permet d'effectuer les actions suivantes :

- Contrôler dans Azure AD qui a accès à ServiceNow.
- Autorisez les utilisateurs à se connecter ServiceNow automatiquement avec leur compte Azure AD.
- Gérez vos comptes dans le portail Azure.

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.
- Une ServiceNow authentification unique (SSO) est activée.
- Une ServiceNow instance ou un locataire qui prend en charge les ServiceNow versions San Diego ou ultérieures.
- Un ServiceNow locataire doit avoir activé le module d'extension d'authentification unique de plusieurs fournisseurs.
- Pour une configuration automatique, activez le module d'extension multifournisseur pour ServiceNow.

Ensemble d'actions pour la configuration

Voici l'ensemble des actions à effectuer pour configurer Azure AD :

- Ajouter ServiceNow à partir de la galerie à Azure AD.
- Configurer l'authentification unique Azure AD
- Créer un utilisateur de test Azure AD
- Affecter l'utilisateur de test Azure AD
- Configurer ServiceNow

Ajouter ServiceNow à partir de la galerie

Ajoutez ServiceNow à partir de la galerie à votre liste d'applications SaaS gérées sur Azure AD.

Avant de commencer

Rôle requis : admin 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 l'authentification unique Azure AD

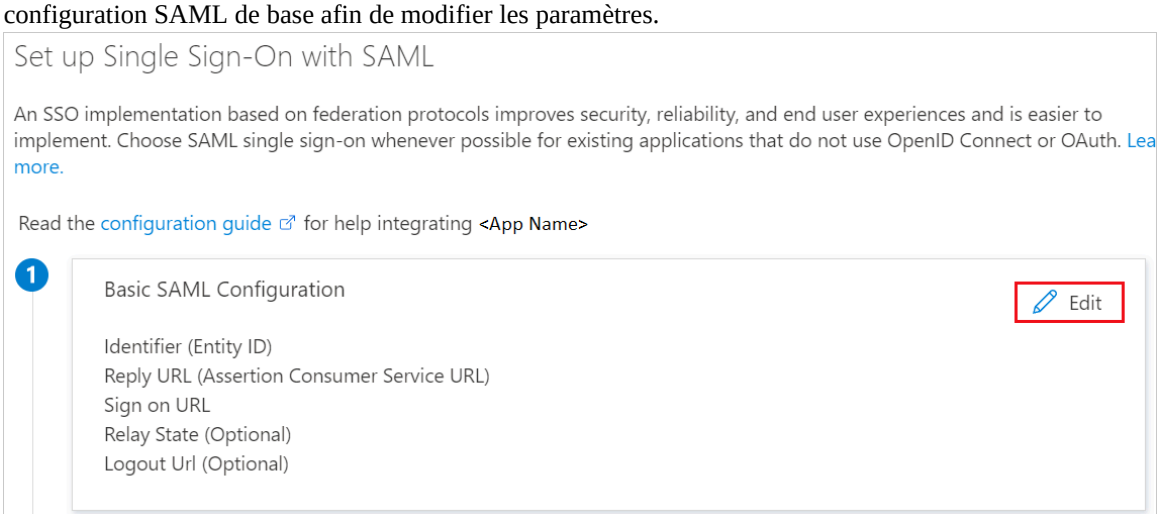
Configurez l'authentification unique Azure AD dans le portail Azure.

Avant de commencer

Rôle requis : admin Azure

Procédure

1. Dans le portail Azure, sur la page d'intégration de l'application ServiceNow , 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 de stylo pour la configuration SAML de base afin de modifier les paramètres.



4. Dans la section Configuration SAML de base, procédez comme suit :

Traduction automatique

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 l'sys_id dans cette URL.

b. Dans Identificateur (ID d'entité), entrez une URL avec le modèle : https://<instance-name>.service-now.com.

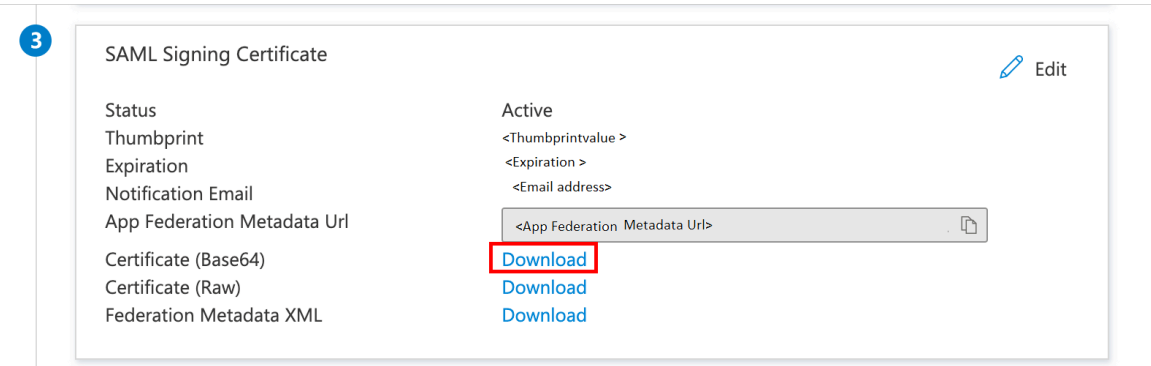
c. Pour **URL de réponse**, saisissez l'un des modèles d'URL suivants :

```
https://<instancename>.service-now.com/navpage.do
https://<instancename>.service-now.com/customer.do
```

d. Dans URL de déconnexion, saisissez une URL avec le modèle suivant : https://<instancename>.service-now.com/navpage.do

Remarque :
Vous devez mettre à jour l'URL de connexion, l'URL de réponse, l'URL de déconnexion et l'identificateur. les valeurs affichées 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).**

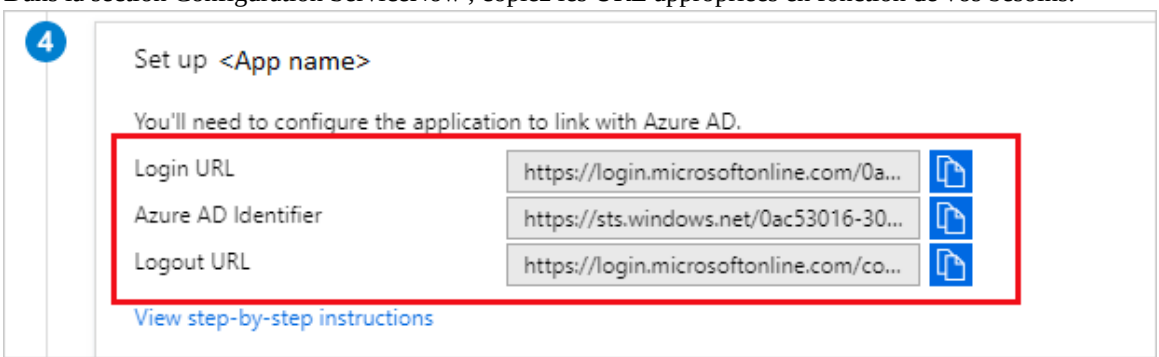


a. Sélectionnez le bouton Copier pour copier **l'URL des métadonnées de fédération d'applications** et collez-la dans le Bloc-notes.
Cette URL est requise pour la configuration ultérieure.

b. Sélectionnez **Télécharger** pour télécharger le certificat (Base64).

Traduction automatique

6. Dans la section Configuration 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 : admin 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 de l'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 accordant l'accès à ServiceNow.

Avant de commencer
Rôle requis : admin 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 `de test` qui a été créé dans la liste d'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**.

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 vers la table utilisateur**.
- Sélectionnez **Activer la journalisation de débogage pour l'intégration de l'authentification unique (SSO) de plusieurs fournisseurs**.
- Entrez **l'e-mail**, le 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 l'importation des métadonnées du fournisseur d'identité, vous pouvez effectuer les opérations suivantes :
   - **URL** : URL des métadonnées de fédération d'applications pour renseigner automatiquement les détails sur la page de configuration du fournisseur d'identité.
   - **Importer** : importez le XML pour importer les détails sur la page de configuration du fournisseur d'identité.
5. Cliquez avec le bouton droit sur le haut de l'écran, cliquez sur **Copier sys_id** et utilisez cette valeur dans **l'URL de connexion** dans la section **Configuration SAML de base** .
6. Renseignez les champs du formulaire.

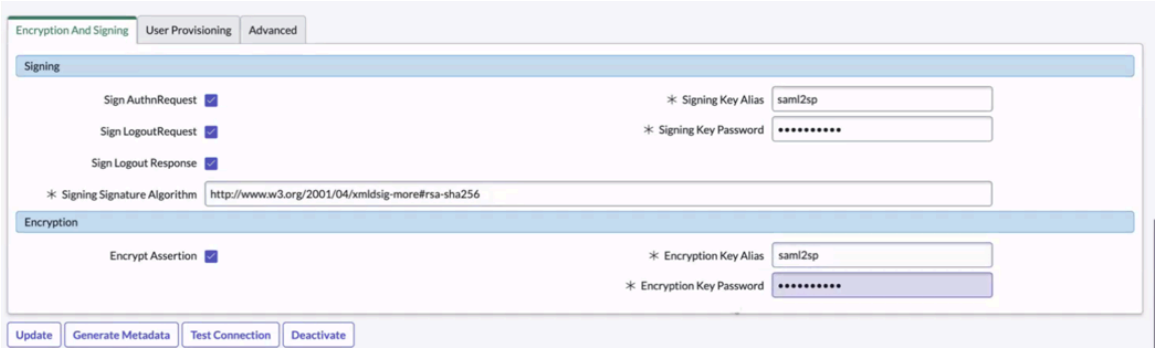
Champs d'authentification unique de plusieurs fournisseurs

Propriété	Obligatoire	Description
Nom	Oui	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. **Remarque :** La possibilité de définir cette propriété n'est disponible qu'après un test de connexion réussi.
Par défaut	Non	L'IdP de redirection automatique, anciennement appelé IdP principal, redirige automatiquement les utilisateurs pour accéder à l'URL de l'instance de base. Cette propriété définit cette configuration IdP comme configuration par défaut.

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, activée automatiquement, contrôle cette fonctionnalité.
URL du fournisseur d'identité	Oui	URL vers votre fournisseur d'identité. Chaque URL IdP doit être unique.
Service AuthnRequest du fournisseur d'identité	Oui	URL de 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, excluant 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, excluant 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

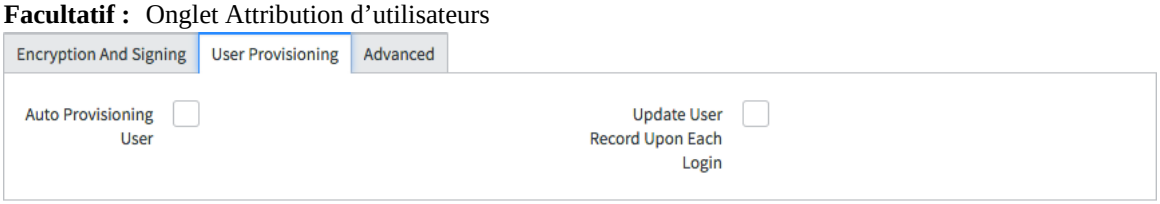
Remarque :
Utilisez vos propres certificats pour le chiffrement et la signature.



Champs de chiffrement et de signature

Propriété	Description
Alias de la Clé de signature/Clé de 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 intègrent 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 vers le consommateur AuthnRequest du fournisseur d'identité SAML 2.0 pour l'authentification de signature électronique.
Signer l'AuthnRequest	Case à cocher pour permettre au service d'authentification unique IdP de recevoir une demande AuthnRequest signée.
Signer la LogoutRequest	Case à cocher pour permettre au service d'authentification unique IdP de recevoir une LogoutRequest signée.

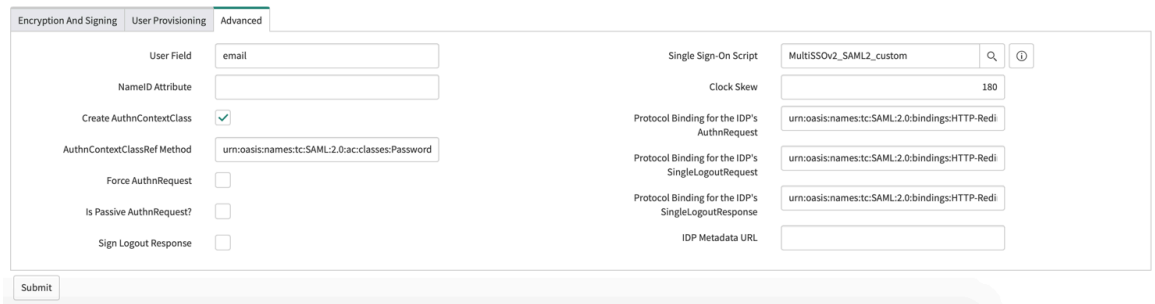
8. **Facultatif :** Onglet Attribution d'utilisateurs



Champs d'attribution d'utilisateurs

Propriété	Description
Mise en service automatique de l'utilisateur	L'attribution automatique d'utilisateurs crée les utilisateurs lorsque l'utilisateur n'existe pas dans la table Utilisateur de l'instance en fonction des informations fournies par IdP.
Mettre à jour l'enregistrement utilisateur à chaque connexion	Mettez à jour les informations utilisateur dans la table Utilisateur d'instance avec les informations dans l'IdP chaque fois que l'utilisateur se connecte à l'aide de SAML.

9. **Facultatif :** Onglet Avancé



Champs avancés

Propriété	Description
Champ d'utilisateur	Champ de la table Utilisateur qui contient la valeur dont l'IdP a besoin 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 des utilisateurs système, cet ID unique correspond aux détails de l'utilisateur.
Attribut NameID	Champ que vous laissez vide à moins que vous ne configuriez une nouvelle politique NameID. Si vous configurez une nouvelle politique, le système requiert la table Utilisateurs qu'il doit utiliser pour identifier l'utilisateur qui se connecte. Le système fait correspondre le jeton NameID au nom de ce champ de la 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 est décochée, 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 pour forcer l'exécution des AuthnRequests.
Est une AuthnRequest passive	Case à cocher 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 réponse de déconnexion dans ce champ.
Décalage d'horloge	Nnombre de secondes entre les deux attributs qui composent la réponse SAMLResponse nonce. La valeur par défaut est 60. Une réponse SAML valide doit se situer entre les valeurs de date/heure *notBefore* et *notOnOrAfter* . Consultez Exemple de réponse SAML 2 avec les éléments SubjectConfirmation et SubjectConfirmationData et Exemple de réponse SAML 2 avec les éléments AudienceRestrictions et Audience pour obtenir 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	Importation des propriétés IdP à partir de cette URL. Si défini, il active l'importation automatique du certificat SAML à partir de l'IdP si le certificat précédent a expiré.

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 ne s'affiche pas automatiquement.
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 post-liaison sont prises en charge pour la demande. L'option permettant de définir ce champ n'apparaît qu'après un test de connexion réussi. Pour plus d'informations, consultez Test des 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 postérieure sont prises en charge pour la réponse. L'option permettant de définir ce champ n'apparaît qu'après un test de connexion réussi. Pour plus d'informations, consultez Test des connexions IdP.

10. Sélectionnez **Tester la connexion** dans le coin supérieur droit de la page.
11. Entrez vos informations d'identification.
    Les résultats du test de déconnexion de l'authentification unique (SSO) 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 du jeton digestif, cependant, 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 d'informations d'identification SSO. Vous trouverez ci-dessous des exemples pour 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 n'accède pas à l'enregistrement spécifique) :

```
https://<instance
 name>.service-now.com/?
SM_USER=user_name&DE_USER=lQjIVp7aRJtyPx5+2O/vgU24tbE=
```

- Lien (dans une notification par e-mail) vers 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
```

Vous devez définir la `glide.email.override.url` propriété dans votre instance pour qu'elle contienne l'URL de la page du portail de l'entreprise. 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 Signature électronique avec SAML (Security Assertion Markup Language) 2.0 mise à jour 1.

Lorsque la signature électronique est active avec l'authentification unique (SSO) à plusieurs niveaux, les propriétés SAML ne sont pas utilisées. Le système ajoute des propriétés de signature électronique à la table Propriétés de 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 pour l'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 du secteur des sciences de la vie et que vous utilisez la signature électronique, désactivez la règle métier Prévention du verrouillage automatique par l'utilisateur.

Migration d'une intégration SAML 1.1 existante vers SAML 2.0

Pour migrer d'une intégration SAML 1.1 vers une intégration SAML 2.0, contactez le support client.

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 et assistance client pour demander le module d'extension *SAML 2.0 Single Sign-On - Update 1 : Security enhancements* . Le module d'extension applique les versions mises à jour de la sortie d'installation de *SAML2SingleSignon* (script de connexion), de la sortie d'installation de *SAML2Logout* (script de déconnexion) et du script include *SAML2* (objet de script).

Fusionnez 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 des scripts de sortie d'installation existants dans de nouveaux scripts

Nom du script de sortie de l'installation d'origine	État du script d'origine	Nom du script de sortie de la nouvelle installation	État du nouveau script
SAML2SingleSignon	Inactif	SAML2SingleSignon_update1	Actif
SAML2	Inactif	SAML2_update1	Actif
SAML2Déconnexion	Inactif	SAML2Logout_update1	Actif

Vous pouvez accéder aux scripts de fermeture et de sortie de l'installation de connexion et de déconnexion SAML 2.0 à l'aide des 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 au script include SAML 2.0 mise à jour 1 à l'aide des chemins 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. Essayez de vous connecter à 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 typiques.
   Pour plus d'informations, consultez Erreurs et correctifs de 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 émetteur

La réponse SAML 2 suivante utilise l'élément *Émetteur* .

```
<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 restrictions d'audience et les éléments d'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 se trouvent pas dans votre instance, le provisionnement d'utilisateurs SAML peut créer automatiquement les utilisateurs dans la table Utilisateur [sys_user] de votre instance.

Le provisionnement des utilisateurs SAML est pris en charge pour SAML 2.0 Update 1 lorsque la SSO à fournisseurs multiples est activée.

Fonctionnement de l'attribution d'utilisateurs SAML

Lorsque l'attribution 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.

- Le système présente une liste de tous les IdP qui sont en mesure d'utiliser l'attribution d'utilisateurs SAML. S'il n'y a qu'un seul IdP qui peut utiliser l'attribution 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 l'attribution d'utilisateurs via les paramètres IdP à SSO multiple.

Avant de commencer

Configurez votre mappage 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 des utilisateurs** (`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 du fournisseur d'identité que vous souhaitez utiliser.
6. Créez un enregistrement dans la table Utilisateur lorsque l'utilisateur n'existe pas déjà en sélectionnant **Mise en service automatique des utilisateurs**.
   Si vous avez effectué une mise à niveau vers cette version, vous devez configurer le formulaire et ajouter ce champ.
7. Activez 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 **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 dans la table de jeux d'importation à partir du fichier metadata.xml.

Remarque :
Vous ne pouvez pas mapper les champs à partir de la table IdP tant que le premier utilisateur n'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.

Remarque :
L'instance ne prend pas en charge les solutions fournies par des sites externes.

Consultez l'article suivant de la base de connaissances : 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 semblable à 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 manquant. Contactez l'assistance technique pour redémarrer les nœuds dépourvus du module d'extension.
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, modifiez la page publique *view_content.do* de *active=true* à *active=false*.
Impossible de rediriger un utilisateur vers une page CMS après une 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 de l'IdP. SSO 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 accéder à une URL telle que */nav_to.do ?uri=/ess*, qui utilise une syntaxe de liens profonds. Toutefois, cela place le portail ESS à l'intérieur de l'IFrame de contenu de navigation principal. En d'autres termes, le site n'occupe pas la page entière, mais se charge plutôt comme une page dans votre instance. Pour plus d'informations, consultez

Autres problèmes courants (suite)

Erreur ou symptôme	Solution
	Sites CMS et Single Sign-On. Si vous modifiez la page d'entrée CMS pour la rendre privée en définissant *view_content.do* sur *active=false*, le comportement de lien profond nécessite alors une personnalisation du script *de connexion Installation Exit (Quitter l'installation*). Créez un script qui recherche la partie *URI* de l'URL et construit un paramètre d'URL *RelayState* contenant le chemin d'accès de l'URL relative pour rediriger les utilisateurs après l'authentification au niveau de l'IdP.
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, comme 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 d'événements 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 d'événements pour détecter les échecs de connexion

Nom d'événement	Description	Enregistrement	Paramètre 1	Paramètre 2
`external.authentication.succeeded`	L'authentification externe a réussi	ID de session	ID d'utilisateur	L'URL à laquelle l'utilisateur

Surveillance de la file d'attente d'événements pour détecter les échecs de connexion (suite)

Nom d'événement	Description	Enregistrement	Paramètre 1	Paramètre 2
	et l'utilisateur a accédé à l'URL de l'instance.		de l'utilisateur qui s'est connecté avec succès	a accédé (qui peut être un lien profond)
external.authentication.failed	Les exigences relatives à l'authentification unique ne sont pas présentes ou sont absentes.		ID de session	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 « L'utilisateur est 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.

Se connecter aux événements d'activités

Nom d'événement	Description	ID utilisé avec l'événement	Chaîne d'événement
saml2.logout.validation.failed	La réponse de déconnexion de l'IdP n'a pas été validée par rapport à 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	Chaîne « Échec de la validation de SAML2 LogoutResponse ».
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 de l'instance.	ID de session et ID d'utilisateur de l'utilisateur qui s'est	L'URL à laquelle l'utilisateur a accédé (qui peut être un lien profond)

Se connecter aux événements d'activités (suite)

Nom d'événement	Description	ID utilisé avec l'événement	Chaîne d'événement
		connecté avec succès	
external.authentication.failed	Les exigences relatives à l'authentification unique ne sont pas présentes ou sont absentes.	ID de session	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 »

Modifications apportées à SAML 2.0 et configuration des jetons Digest

L'authentification unique (SSO) de plusieurs fournisseurs permet aux administrateurs de configurer SAML 2.0 Update 1 et le jeton Digest en tant que méthodes d'authentification.

L'authentification unique (SSO) de plusieurs fournisseurs doit être activée avant de configurer vos propriétés de jeton SAML 2.0 Update 1 et Digest. Une fois que vous avez demandé et activé l'authentification unique (SSO) de plusieurs fournisseurs, vous devez la configurer. Après avoir configuré l'authentification unique (SSO) de plusieurs fournisseurs, vous pouvez créer ou mettre à jour les configurations de jeton SAML 2.0 Update 1 et Digest. Vous pouvez utiliser l'une ou l'autre des solutions d'authentification, ou les deux, avec l'authentification unique (SSO) de plusieurs fournisseurs.

Remarque :
Le module d'extension Integration - Multiple Provider Single Sign-On Installer supprime l'application SAML du navigateur. Les paramètres SAML nécessaires sont migrés vers l'application SSO de plusieurs fournisseurs dans la table MIGRÉ SAML2. Vous pouvez toujours modifier des éléments tels que le certificat x509, les détails IdP, etc., via l'application SSO de plusieurs fournisseurs.

Authentification entrante et sortante OAuth

L'authentification basée sur OAuth valide l'identité du client qui tente d'établir une fiducie sur le système à l'aide d'un protocole d'authentification.

OAuth 2.0 - Open Authorization est le protocole standard de l'industrie pour l'autorisation, 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 pour le compte d'un utilisateur.

Au lieu d'utiliser les informations d'identification de l'utilisateur de ressources pour accéder aux ressources protégées, le client obtient un jeton d'accès. Les jetons d'accès sont émis pour les clients tiers avec l'approbation de l'utilisateur, le client utilise ensuite le jeton d'accès pour accéder aux ressources protégées.

Entrant

Créez un point de terminaison pour les clients externes qui souhaitent accéder à votre instance. Cela crée un enregistrement d'application cliente OAuth et génère un ID client et un secret client indiquant que le client a besoin pour accéder aux ressources restreintes sur l'instance. Pour plus d'informations, reportez-vous à la section OAuth entrant.

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 de l'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 authentifier l'utilisateur pour la première fois afin de récupérer le jeton, ce qui signifie que vous n'avez pas besoin de vous authentifier à l'aide d'un compte d'utilisateur avant l'expiration du jeton.

Les frameworks de sécurité simple et de haute sécurité prennent tous deux en charge OAuth 2.0. Une haute sécurité est recommandée. Consultez pour plus d'informations sur les versions dont la sécurité élevée est déjà active et sur la façon d'activer la sécurité élevée.

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 *un utilisateur final*. Le propriétaire de la 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 et de répondre aux demandes de ressources protégées.
Serveur d'autorisation	Serveur qui émet des jetons d'accès au client après avoir authentifié le propriétaire de la ressource et obtenu l'autorisation.
Demande d'autorisation	Autorisation requise par un client pour accéder à une ressource protégée. La demande d'autorisation est toujours un message HTTP POST qui contient l'ID du client qui agit au nom du propriétaire de la ressource et les informations d'identification qui autorisent la demande.

Concept	Description
Octroi d'autorisation	Informations d'identification qui représentent l'autorisation du propriétaire de la ressource d'accéder à une ressource. L'autorisation accordée est soit les informations d'identification de connexion de l'utilisateur, soit un jeton d'actualisation.
Jeton d'accès	Chaîne sécurisée qu'un client utilise pour accéder aux ressources protégées. Une instance émet des jetons d'accès aux clients disposant d'une autorisation valide. Chaque jeton d'accès a un champ d'application, une durée de vie et d'autres attributs spécifiques. 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'il est autorisé pour la première fois à disposer d'un jeton d'accès. Par défaut, une instance émet des jetons d'actualisation d'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	Le Now Platform ne prend pas en charge les certificats autosignés. Le client OAuth n'utilise pas le magasin de certificats de confiance et n'autorise pas la connexion à des points de terminaison OAuth qui incorporent un certificat autosigné.
Agent utilisateur	Utilisateur qui délègue les droits d'accès à une application cliente, qui est 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'octroi* désigne la manière dont le client obtient le jeton d'accès. Les types de subventions 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'autorisation* ou *flux de code d'autorisation*.
- **Informations d'identification du mot de passe du propriétaire** de la ressource : le consommateur de la ressource possède déjà les 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 déjà configurés dans le registre d'application.

Stockage des informations d'identification d'authentification

Le secret client OAuth est stocké sous la forme d'un `password2` champ type, chiffré avec KMF. Les mots de passe utilisateur, qui sont utilisés pour vérifier les demandes de point de terminaison entrantes, sont stockés sous forme de valeur de hachage dans la table Utilisateur dans un `password` champ de 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 permettant aux applications clientes externes d'accéder à l'instance et définissez les paramètres OAuth.

Avant de commencer

Rôle requis : admin

Procédure

1. Assurez-vous que le module d'extension OAuth est actif et que la propriété d'activation OAuth est définie sur true.
2. Créez un registre d'application OAuth à l'aide de l'une des méthodes suivantes :
   - Créez un point de terminaison pour les clients externes qui souhaitent accéder à votre instance. Cela crée un enregistrement **d'application cliente OAuth** et génère un ID client et un secret client indiquant que 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 spécifiez 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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

Définir la propriété OAuth

Pour générer des jetons OAuth 2.0 vers les applications enregistrées, la propriété com.snc.platform.security.oauth.is.active doit être active pour l'instance.

Avant de commencer

Rôle requis : admin

Procédure

1. Pour utiliser OAuth 2.0, saisissez **sys_properties.list** dans le navigateur de filtre d'espace de travail et cliquez sur **Nouveau**.
2. Remplissez le formulaire avec les paramètres suivants :
   - **Nom** : com.snc.platform.security.oauth.is.active
   - **Type** : vrai | faux
   - **Valeur** : vrai

Changer 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 via 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'subventions pris en charge. Les types de subventions 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 true 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 true.

OAuth entrant

L'entrée OAuth fournit un point de terminaison permettant aux clients tiers d'extraire les données de l'instance.

Vous devez disposer du rôle security_admin pour gérer l'intégration OAuth.

Vous pouvez configurer l'intégration de **scénarios de clients externes OAuth** (entrants) lorsque vous souhaitez que votre instance fournisse un point de terminaison permettant aux clients tiers d'extraire des données de l'instance.

Remarque :
Vous devez authentifier l'utilisateur pour la première fois afin de récupérer le jeton, ce qui signifie que vous n'avez pas besoin de vous authentifier à l'aide d'un compte d'utilisateur avant l'expiration du jeton.

Vous pouvez effectuer la configuration entrante OAuth en fonction du type d'accord suivant :

- **Code d'autorisation** : pour un flux d'octroi initié par l'utilisateur, où l'utilisateur peut configurer une URL autorisée pour l'authentification sans avoir à saisir un nom d'utilisateur ou un mot de passe, mais via le jeton d'accès. Pour plus d'informations, consultez Flux d'octroi du code d'autorisation OAuth.
- **Informations d'identification du mot de passe du propriétaire de ressource** : pour un flux d'octroi initié par l'utilisateur, où une interaction de l'utilisateur est requise pour l'authentification. Pour plus d'informations, consultez Configuration du flux d'octroi de mot de passe .

  Remarque :
  Pour le flux de code d'autorisation, l'utilisateur doit terminer l'authentification par connexion locale, SSO ou MFA, puis donner son consentement.

- **JWT Bearer** : Pour une intégration de système à système, où une intervention de l'utilisateur n'est pas nécessaire. Pour plus d'informations, consultez Configuration du flux d'attribution de support JWT .
- **Flux de jetons d'ID** : pour utiliser un jeton d'ID émis par des fournisseurs OIDC tiers tels qu'Okta ou Azure. Pour plus d'informations, consultez Flux de jetons d'ID pour l'authentification.
- **Concessions implicites OAuth** : permet de donner le jeton d'accès directement à l'application cliente via l'agent utilisateur, qui est généralement le navigateur Web ou l'équipement mobile. Pour plus d'informations, consultez Subventions implicites OAuth.
- **Informations d'identification du client** : pour l'utilisation du type d'attribution des informations d'identification du client OAuth pour les intégrations entrantes d'un client OAuth tiers vers la ServiceNow® plateforme. Pour plus d'informations, consultez Informations d'identification du client.

Périmètres OAuth

Vous pouvez définir le périmètre de prise en charge du périmètre de suthentication 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.

Flux d'octroi du code d'autorisation OAuth

Le flux d'octroi de code d'autorisation permet à un utilisateur d'accéder à une ressource en s'authentifiant directement auprès d'un serveur OAuth qui approuve la ressource, contrairement à l'authentification avec des informations d'identification de 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 plutôt que de demander à l'utilisateur de saisir un nom d'utilisateur/mot de passe. Le nom d'utilisateur et le mot de passe ne sont jamais visibles par le client qui demande l'accès à la ressource.

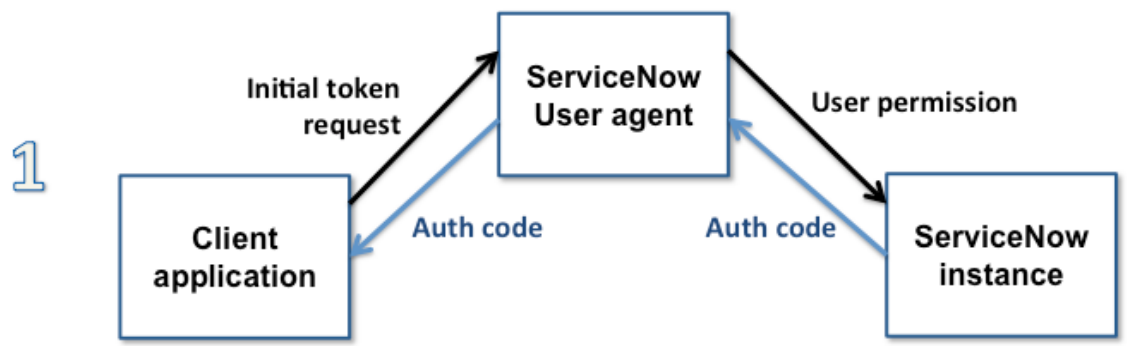
Une ServiceNow instance en tant que serveur d'autorisation

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 du code d'autorisation.

L'utilisateur qui possède 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 de code d'autorisation

Le processus de flux d'octroi de code d'autorisation se compose des trois étapes suivantes :



À la première étape, l'application ou le site Web client 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 initié lorsque l'utilisateur final clique sur un bouton ou un lien sur l'application cliente ou le site Web 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 le secret client. Pour obtenir des explications sur ces éléments, consultez les descriptions de champ 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 client à l'instance :

```
https://myinstance.service-now.com/oauth_auth.do?response_type=code&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```

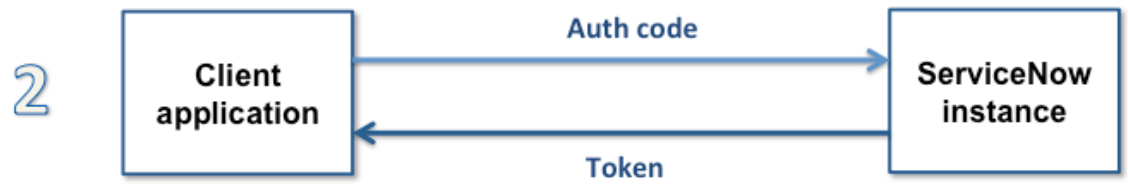
Remarque :
La **response_type** doit être **codée** pour utiliser le flux d'octroi de code OAuth standard.

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** . Reportez-vous aux instructions.

L'élément auquel l'application cliente demande réellement le jeton est l'enregistrement du registre d'application du fournisseur OAuth que vous avez créé, également connu sous le nom de 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 ou du site Web client.

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, elle utilise le code pour demander le jeton d'accès. Le code d'autorisation prouve que l'utilisateur a donné son consentement à l'étape 1.

Exemple de demande POST de l'application client vers 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_sec
ret={client_secret_value}
```

Le point de terminaison sur l'instance renvoie un jeton d'accès et un jeton d'actualisation. Le jeton d'actualisation peut être utilisé pour demander des jetons d'accès supplémentaires.

Vous pouvez gérer les jetons, y compris révoquer le jeton, dans l'instance. Reportez-vous à la section Gérer les jetons OAuth.

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 des données de 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 subventions implicites OAuth, également connues sous le nom de flux de code d'attribution implicite.

Aide à l'intégration

Le flux de code d'autorisation prend en charge les intégrations suivantes sur l'instance :

- Authentification unique (SSO) de plusieurs fournisseurs
- SAML 2.0 Mise à jour 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 propriétaires d'une ressource protégée sur l'instance doivent autoriser l'accès ServiceNow à la ressource avant que l'instance puisse fournir le jeton d'accès.

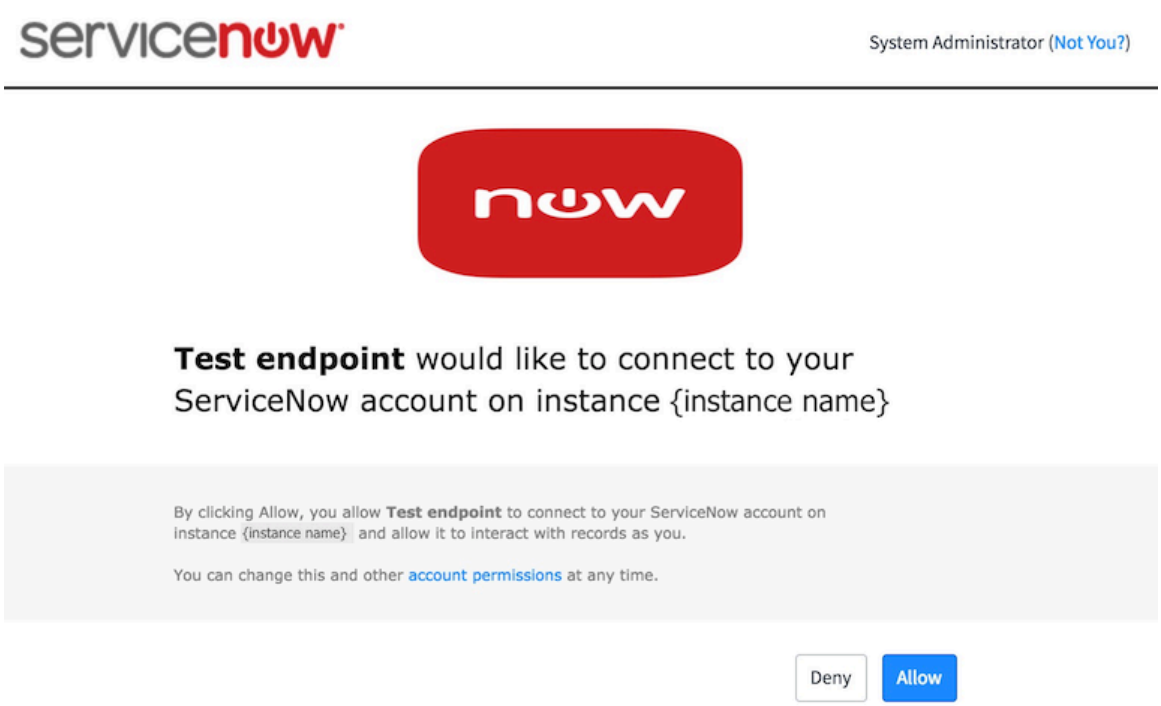
Avant de commencer

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 sur l'application cliente dans laquelle vous demandez l'accès à la ressource protégée sur l'instance.
   Cela donne le coup d'envoi de 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 Message REST.
2. Si vous n'êtes pas connecté, connectez-vous maintenant.
   Si vous n'êtes pas le même utilisateur que l'utilisateur spécifié dans le coin supérieur droit, cliquez sur **Pas vous ?** et connectez-vous.
3. Cliquez sur autorisations de 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 des jetons d'applications.
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'octroi 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 apparaître. Si vous demandez l'accès à partir du formulaire Message REST sur une instance, le message suivant apparaît 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 State 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 State pour une demande OAuth. Pour les instances zbooted, la propriété est true. Pour les instances mises à niveau, la propriété n'est pas présente, par conséquent le paramètre État n'est pas activé. Le paramètre State est une valeur de chaîne et ne doit pas contenir de caractères spéciaux. Le paramètre State ne peut pas être vide ou " « .

Validation du paramètre d'état

Créez un point de terminaison pour que les clients accèdent à l'instance. Lancez un flux de code d'autorisation pour une oauth_auth.do. Par exemple :

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=
e9dba45b380d1300e676ccc91cef468f&response_type=code
```

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 State 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 régulier 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_message&oauth_requestor=eab8341fec0d1300964f214a2c2fcf67&oauth_provider_profile=dfa8f01fec0d1300964f214a2c2fcf51&response_type=code
```

Le paramètre State est automatiquement ajouté lorsqu'il est redirigé par oauth_auth.do.

```
http://myinstance.service-now.com/oauth_auth.do?response_type=code&state=-790938844&redirect_uri=http://10.11.95.5:16001/oauth_redirect.do&client_id=e9dba45b380d1300e676ccc91cef468f
```

Exemple de flux de code d'autorisation : ServiceNow instance en tant que serveur d'autorisation

Vous pouvez utiliser une instance en tant que 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 sur les deux instances.

Procédure

1. Sur l'instance du serveur d'autorisation (exécutant la version Istanbul ou une version ultérieure), accédez à **OAuth système** > **Registre d'application** 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 de l'application OAuth comme décrit à la section Créer un point de terminaison pour que les clients accèdent 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** Cliquez sur **Nouveau**.
5. **Cliquez sur Se connecter à un fournisseur OAuth tiers**.
6. Renseignez les champs de formulaire de l'enregistrement de l'application OAuth comme décrit à la section . Notez les valeurs de champ suivantes :
   - **Nom** : nom unique qui identifie l'application pour laquelle vous avez besoin d'un accès OAuth.
   - **ID client** : ID client de l'enregistrement du registre d'application que vous avez créé pour le serveur d'autorisation.
   - **Secret client** : [Lecture seule] ID unique généré automatiquement de l'application. L'instance utilise l'ID client lors de la demande d'un jeton d'accès.
   - **Type d'accord par défaut** : sélectionnez **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 pour accorder à une application cliente l'accès à une ressource restreinte sur l'instance.
- **URL de jeton** : URL de l'instance qui est 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'attribution de 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 que les clients accèdent à l'instance

Créez un point de terminaison d'application OAuth permettant 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** 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 renseignez 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 généré automatiquement pour l'application. 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 elles. L'instance utilise le secret client lors de la demande d'un jeton d'accès. Laissez ce champ vide pour que l'instance génère automatiquement un secret client. Pour afficher les secrets clients 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, ajoutées 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 fait correspondre l'URL 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	L'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 pour accorder à une application cliente l'accès à une ressource restreinte sur l'instance.
Actif	Cochez la case pour activer le registre d'application.
Durée de vie du jeton d'actualisation	Nombre de secondes pendant lesquelles un jeton d'actualisation est valide. L'instance utilise la valeur de durée de vie lors de la demande d'un jeton d'actualisation. Par défaut, les jetons d'actualisation expirent après 100 jours (8640 000 secondes).

Champ	Description
Appliquer les restrictions de jeton	Sélectionnez cette option pour autoriser uniquement l'utilisation des jetons avec des API définies pour autoriser le profil d'authentification. Vous pouvez définir l'octroi d'accès à l'aide d'une politique 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 de 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).
Commentaires	Informations supplémentaires à associer à l'application.

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 des jetons et des codes d'autorisation, ils sont stockés dans la table. Consultez Gérer les jetons OAuth pour plus d'informations.

Paramètres de réponse de l'API OAuth

L'API OAuth 2.0 génère une réponse JSON contenant les paramètres suivants sous forme de paires nom-valeur.

Paramètres de réponse de 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 obtenu 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. Voir 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 dans 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 JSON.

Remarque :
Si un fournisseur OAuth envoie le corps de la réponse comme « content-type » au lieu de « Content-Type », le client HTTP OAuth peut ne pas analyser correctement la réponse. 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 en savoir plus sur la création de propriétés système, reportez-vous à la rubrique 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 d'API OAuth

Découvrez les paramètres de demande d'API OAuth utilisés par les demandes de jetons 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.

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 d'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 entre elles.

Paramètres de demande de jeton d'accès (suite)

Paramètre de demande	Description
nom d'utilisateur	Nom du compte utilisateur qui autorise la demande de jeton d'accès. Ce paramètre est requis pour les demandes de jetons d'accès avec un **grant_typede mot de passe**.
mot de passe	Mot de passe du compte d'utilisateur qui autorise la demande de jeton d'accès. Ce paramètre est requis pour les demandes de jetons d'accès avec un **grant_typede 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 jetons d'accès avec un **grant_type** de **refresh_token**.

Demandes à l'aide des informations d'identification de l'utilisateur

L'instance exige que les clients fournissent les informations d'identification de connexion de l'utilisateur lors de la première autorisation du client ou lors de l'autorisation de la création d'un jeton d'actualisation. Ce type de requête renvoie toujours deux jetons :

- Un jeton d'accès
- 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 false, l'instance ne génère pas de jeton d'accès. Les demandes d'accès effectuées pendant le délai d'expiration du jeton d'accès renvoient toujours le jeton d'accès actuel.

Remarque :
Ce type d'octroi d'autorisation repose 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 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
```

Demandes utilisant un jeton d'actualisation

L'instance peut utiliser un jeton d'actualisation existant pour créer un 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 de jetons d'actualisation 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 d'actualisation 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=w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FMxHW40H8yOO3Hoe"
https://instancename.service-now.com/oauth_token.do
```

Créer un point de terminaison d'API JWT OAuth pour les clients externes

Créez un point de terminaison d'API OAuth JSON Web Token (JWT) pour permettre aux clients externes d'accéder à votre ServiceNow instance à l'aide de jetons Web.

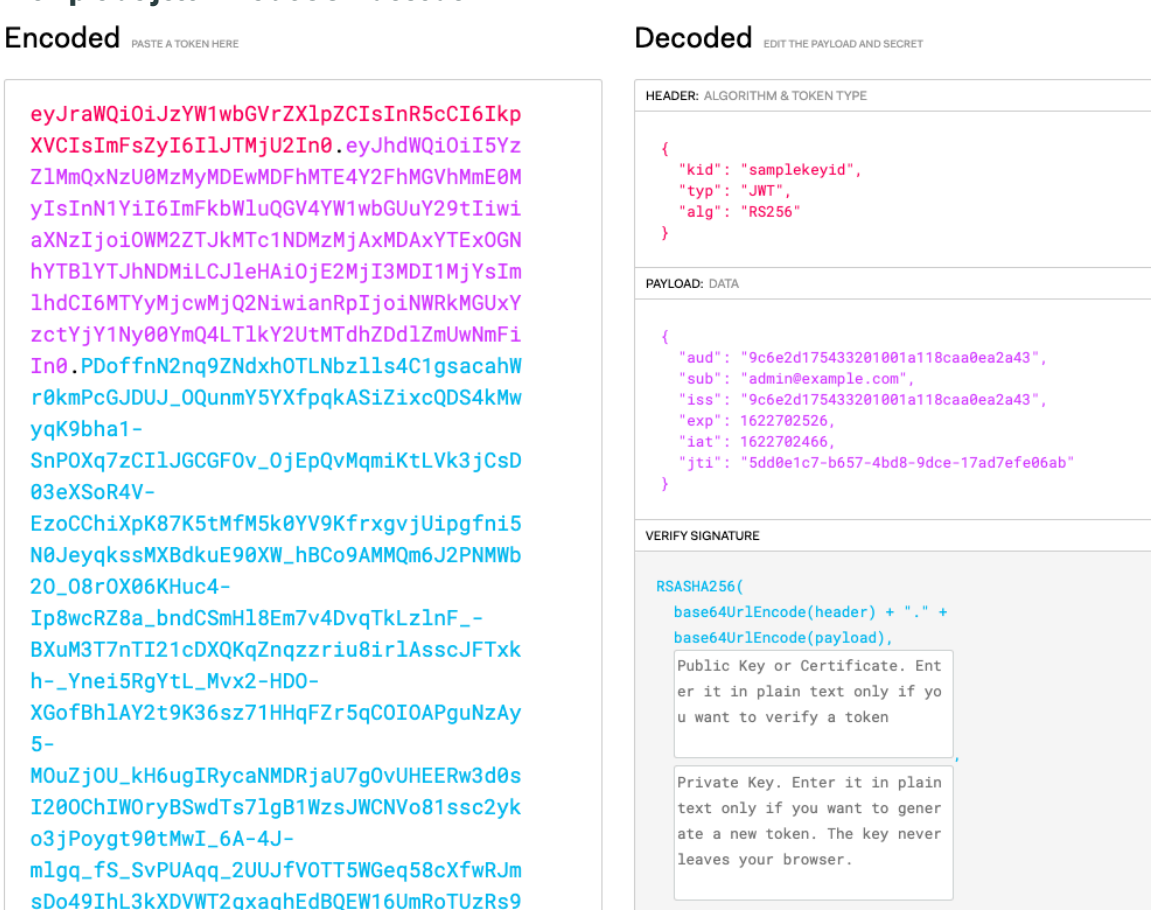
Avant de commencer

Rôle requis : admin

Générer un jeton Web JSON (JWT) avec les revendications suivantes :

- `aud` : doit correspondre à la valeur de l'ID client.
- `sub` : doit être un identificateur d'utilisateur, tel que l'e-mail de l'utilisateur auquel vous souhaitez associer le jeton.
- `iss` : recommandé pour correspondre à la valeur de l'ID client.
- `exp` : n'importe quelle expiration souhaitée.

Exemple de jeton Web JSON décodé



Pour plus d'informations sur les jetons Web JSON, consultez https://jwt.io/ .

Pourquoi et quand exécuter cette tâche

Autorisez les applications Web externes à 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. L'utilisation du type d'attribution JWT n'inclut pas le mot de passe dans la demande, ce qui 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.

Procédure

1. Créez une paire de clés et ajoutez la clé publique à la table Certificats X.509 (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.

Table OAuth JWT

Champ	Description
Nom	Nom unique qui identifie l'application pour laquelle vous avez besoin de l'accès JWT OAuth.
ID client	ID unique généré automatiquement pour l'application. 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 affirmations 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 elles. Laissez ce champ vide pour que l'instance génère automatiquement un secret client. Pour afficher les secrets clients existants, cliquez sur l'icône de verrouillage. **Remarque :** Si **Client public** est sélectionné, vous pouvez omettre le **secret client**.
URL du logo	L'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 pour accorder à une application cliente l'accès à une ressource restreinte sur l'instance.
Champ d'utilisateur	Champ dans la table Utilisateur (sys_user) que le système utilise pour faire correspondre la valeur de la réclamation concernée dans le JWT. Par exemple, si vous ajoutez un jeton dont la valeur de revendication de l'objet est user.name@example.com, définissez 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 : cette option est sélectionnée.
Application	Champ d'application de l'application en lecture seule.
Accessible depuis	Politique d'accès entre périmètres. Pour plus d'informations, consultez Paramètres d'accès à l'application .

Champ	Description
Durée de vie du jeton d'accès	Durée de validité du jeton. Unité : Secondes
Décalage d'horloge	Décalage horaire autorisé entre les horloges du serveur et du client lors de la validation des réclamations `exp` et `nbf` dans le JWT. Unité : Secondes Par défaut : 300
Appliquer les restrictions de jeton	Sélectionnez cette option pour autoriser uniquement l'utilisation des jetons avec des API définies pour autoriser le profil d'authentification. Vous pouvez définir l'octroi d'accès à l'aide d'une politique 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.

d. Enregistrez le formulaire.

e. Ajoutez des enregistrements à la liste connexe des cartes de vérificateur Jwt pour vérifier la signature JWT.

Table des cartes de vérificateur Jwt

Champ	Description
Nom	Nom de l'enregistrement de mappage JWT.
Enfant	ID de clé du JWT.
Clé partagée	Clé partagée pour l'ID de clé spécifié.
Application	Champ d'application de l'application en lecture seule.
Certificat système	Enregistrement de certificat dans la table Certificats X.509 (sys_certificate).

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 réclamations requises suivantes :

- Iss
- Aud
- sous-marin
- Exp

Table des validations de réclamation OAuth JWT

Champ	Description
Mon client externe	Renseigné 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 à partir 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_bndCSmHl8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
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 les 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
nmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvMqmiKtLVk3jCsD03
eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0JeyqkssMXBdkuE90XW_hBCo9AM
MQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHl8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
s7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58
```

```
cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16UmRoTUzRs9A9sOm18y3skmOVtnEOm-MIJM
FQZ754UMzbiH0ZsMmk1ivCGIjex5J0_IDjKElWF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqP
dS2vzg2m1eKGUwr3m6uNs_HflcDystwVdMZ7nLIBG4"
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

Voici une commande cURL permettant d'accéder à la table d'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 autorise l'accès à la ressource demandée.

Configurer un fournisseur OIDC OAuth sur le Now Platform

Vous pouvez configurer un fournisseur OIDC OAuth pour accepter les jetons d'identité générés par un fournisseur OIDC tiers à l'aide d'appels d'API entrants ou de notre option Single Sign-On (authentification unique de plusieurs fournisseurs).

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Le prend Now Platform en charge OIDC via notre implémentation externe Single Sign-On (SSO) en plus des appels d'API entrants. Pour obtenir un exemple de configuration de fournisseur OIDC, consultez Configurer Azure AD. Pour obtenir un exemple spécifique à SSO de configuration de fournisseur OIDC, consultez Créer une configuration OpenID Connect (OIDC) pour Single Sign-On (SSO).

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Registre d'application**.
   - Cliquez sur **Nouveau**, sur **Configurer un fournisseur OIDC pour vérifier les jetons d'ID**, puis renseignez le formulaire.
   - Sélectionnez un modèle existant pour un fournisseur OIDC (ADFS, Auth0, Azure AD, Google, Okta), puis renseignez 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	ID client de l'application enregistrée sur le serveur OAuth OIDC tiers. L'instance utilise l'ID client lors de la demande d'un jeton d'accès.
Secret client	Le secret client de l'application enregistrée sur le serveur OAuth OIDC tiers.
Script de l'API OAuth	Script que vous pouvez utiliser pour personnaliser les demandes et les réponses à un fournisseur OAuth externe.
Configuration du fournisseur OIDC OAuth	Le fournisseur OIDC (ADFS, Auth0, Azure AD, Google, Okta) peut être utilisé pour valider le jeton JWT. Cliquez sur l'enregistrement de la configuration de votre fournisseur OIDC pour valider que la **réclamation de l'utilisateur** et le **champ d'utilisateur** sont correctement définis. Si vous cochez la case Activer la vérification de la **réclamation JTI**, la validation du ServiceNow jeton JWT valide également la JTI envoyée 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.
Décalage d'horloge	Nombre en secondes pour que la contrainte soit considérée comme valide. La valeur par défaut est 300.
Commentaires	Informations supplémentaires à associer à l'application.
Application	Nom de l'application contenant cette entité.
Accessible depuis	Sélectionnez une option pour la rendre accessible à partir de tous les périmètres de l'application, ou à partir de ce périmètre de l'application uniquement.
Appliquer les restrictions de jeton	Sélectionnez cette option pour autoriser uniquement l'utilisation des jetons avec des API définies pour autoriser le profil d'authentification. Vous pouvez définir l'octroi d'accès à l'aide d'une politique d'accès API. Pour plus d'informations, consultez Créer une politique d'accès REST API. Par défaut : non sélectionné.
Actif	Cochez la case pour activer l'application OAuth.
URL de redirection	URL de l'application OAuth pour la réception du code d'autorisation.
Terminer la session de l'URL	Le point de terminaison de l'URL qui s'active après la fin d'une session.

Champ	Description
du point de terminaison	
Activer l'authentification forcée	Option permettant d'activer l'authentification forcée pour les utilisateurs.

2. Cliquez sur **Envoyer**.
   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 périmètre.
   Vous pouvez modifier ou ajouter un profil de fournisseur OAuth incluant le nom, le type d'accord et le champ d'application OAuth.
4. **Facultatif :** Accédez à la liste connexe sur l'enregistrement Périmètres des entités OAuth pour définir tous les périmètres 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 à partir de la spécification du fournisseur, par exemple un champ d'application de lecture ou d'écriture.
   Chaque périmètre doit être défini séparément.
5. **Facultatif :** Accédez à la liste connexe sur 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 ServiceNow 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 de transformations. Lors de la configuration du mappage de transformation, les champs sources proviennent de , `JWT token`les champs cibles proviennent de la `sys_user` table.
Rôles d'utilisateur appliqués aux utilisateurs attribués	Les rôles d'utilisateur appliqués aux utilisateurs nouvellement mis ServiceNow en service.

Subventions implicites OAuth

ServiceNow Les instances prennent en charge l'octroi implicite d'un jeton d'accès.

Le type d'octroi implicite, également connu sous `implicit grant code flow`le nom de , permet de donner le jeton d'accès directement à l'application cliente via l'agent utilisateur, qui est généralement le navigateur Web ou l'équipement mobile. Aucun jeton d'actualisation n'est accordé. L'utilisateur final doit toujours accorder l'accès à la ressource protégée sur l'instance, comme avec le fichier .

Processus de flux d'octroi implicite OAuth

Comme pour le processus de flux de code d'autorisation standard, l'application cliente émet 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 veut accéder.
- response_type=jeton. Il est obligatoire de demander directement le jeton d'accès (par opposition à un code d'autorisation). La valeur doit être jeton pour les subventions implicites. Dans l'exemple du 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 des 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}
```

Gérer les jetons OAuth

Ouvrez les jetons OAuth pour fournir l'accès aux ressources restreintes.

Avant de commencer

Rôle requis : n'importe quel utilisateur ou admin

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 instance.
- Type : détermine si le jeton est un jeton d'accès ou un jeton d'actualisation.
- Expire : date/heure d'expiration du jeton d'accès ou d'actualisation.
- 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 d'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 afficher les jetons créés par l'instance lorsque vous avez accordé l'accès à une ressource sur l'instance.
   - **OAuth système** > **Gérer les jetons** pour afficher 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.
4. Vous pouvez également afficher d'autres informations sur le jeton, notamment le champ d'application auquel il permet d'accéder et la date d'expiration.

Révoquer un jeton OAuth

Vous pouvez vouloir révoquer un accès OAuth ou actualiser un 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 dans laquelle votre instance agit en tant que serveur de ressources OAuth. Vous pouvez révoquer le jeton via une URL ou via .

Procédure

Accédez à votre instance à l'aide de oauth_revoke_token.do et ajoutez le jeton d'accès ou d'actualisation.

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.

Informations d'identification du client

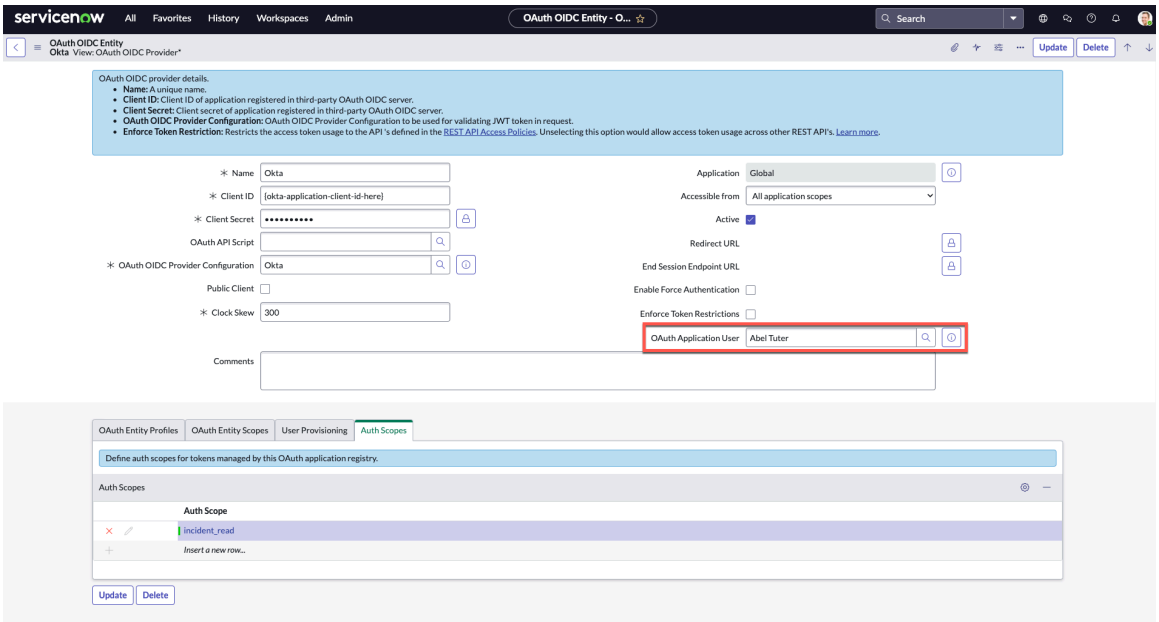
Utilisez le type d'accord Informations d'identification du client OAuth pour les intégrations entrantes à partir d'un client OAuth tiers vers la ServiceNow® plateforme.

Les administrateurs peuvent utiliser le type d'accord d'informations d'identification du client (CC) pour permettre l'intégration d'un client OAuth tiers à la ServiceNow plateforme.

Le type d'attribution Informations d'identification du client entrant est une option qui peut être contrôlée via une propriété système. Par défaut, la propriété système est false.

Pour utiliser le type d'attribution Informations d'identification client, vous devez effectuer les étapes suivantes :

- 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'attribution Informations d'identification du client pour les intégrations entrantes OAuth.

Avant de commencer

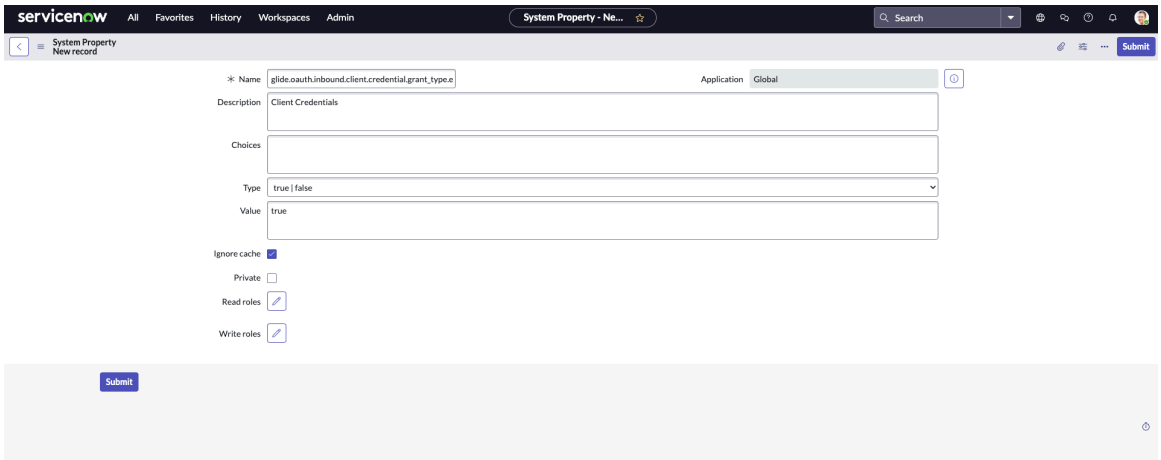
Rôle requis : admin

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.
Valeur	Définissez la valeur souhaitée pour la propriété. Dans ce cas, sélectionnez vrai pour activer le type d'accord Informations d'identification du client pour les intégrations entrantes OAuth.



Remarque :
D’autres champs du formulaire, tels que Choix, Ignorer le cache, Privé, Rôles de lecture et Rôles d’écriture, peuvent être configurés en fonction de vos besoins.

4. Sélectionnez **Envoyer**.

Remarque :
Si la case **Ignorer le cache** est cochée, le système vide le cache du serveur lorsque le paramètre est modifié.

Ensuite, vous devez 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

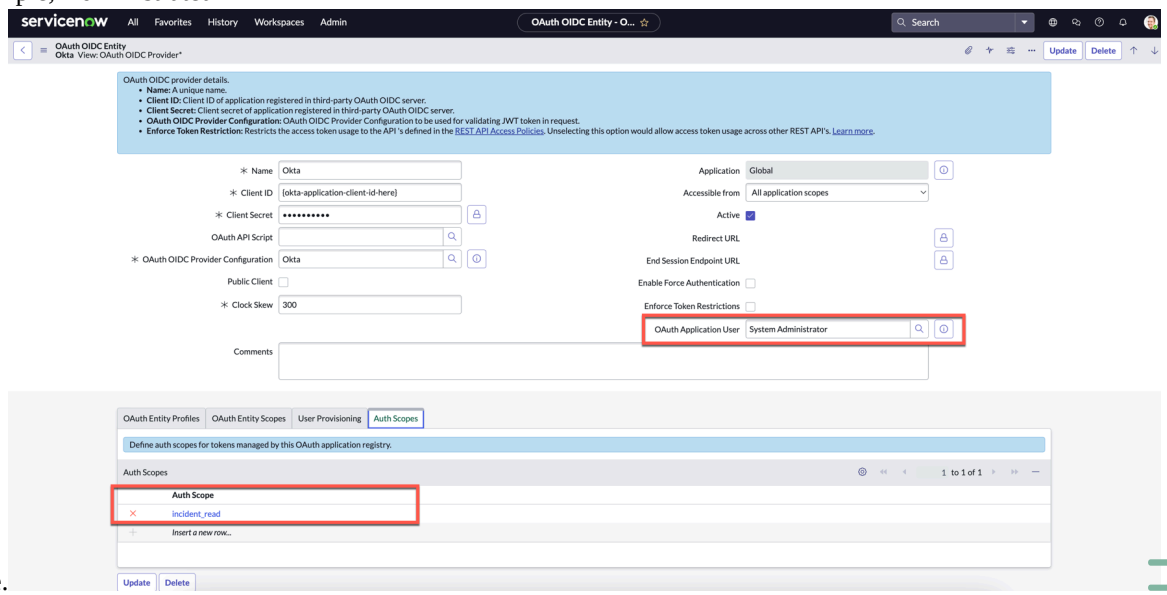
Module d’extension requis : OAuth 2.0.

Vous devez créer un client OAuth. Pour plus d'informations, consultez Créer un point de terminaison pour que les clients accèdent 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 la page.
3. Sélectionner **Configurer** > **Conception de formulaire**.
4. Sur la page Conception de formulaire, ajoutez un **utilisateur d’application OAuth** à partir de la liste des champs.
5. Enregistrez ou mettez à jour le formulaire.
6. Sélectionnez l’utilisateur de **l’application OAuth**.

Par exemple, Administrateur



système.

> **Remarque :**
> Vous devez utiliser le champ d'application d'authentification de l'API REST avec le type d'attribution 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 ayant pour **type d'accord** informations **d'identification client**, **ID client** et **secret** est transmise pour l'utilisateur de l'application OAuth associée dans ServiceNow®.

> **Remarque :**
> Si l'utilisateur de l'application OAuth n'est pas sélectionné sur l'enregistrement client OAuth ou si la propriété Informations d'identification du client est définie sur false, la demande d'autorisation n'est pas transmise.

Sortant OAuth

Le trafic sortant OAuth vous permet d'extraire les 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 client et le secret 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 titulaire JWT.
- **Support SAML2** : génère l'assertion SAML2, puis échange l'assertion contre les jetons d'accès avec le fournisseur.

Remarque :
Pour la demande sortante, utilisez le **support SAML2** comme type d'attribution SuccessFactors par défaut. Pour en savoir plus sur la configuration du **support SAML2**, reportez-vous à l'exemple de la section Set up the v4.x.x .

- **Code d'autorisation** : code qui est 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 tente d'obtenir l'accès à la ressource.
- **Informations d'identification du client** : ID client et secret client, qui sont tous deux utilisés pour obtenir le jeton d'accès. Cette méthode ne fournit pas de jetons d'actualisation.

Vous pouvez configurer le **scénario du fournisseur OAuth** (sortant) : votre instance extrait les données d'un fournisseur tiers.

Remarque :
Vous devez authentifier l'utilisateur pour la première fois afin de récupérer le jeton, ce qui signifie que vous n'avez pas besoin de vous authentifier à l'aide d'un compte d'utilisateur avant l'expiration du jeton.

Se connecter à un fournisseur OAuth tiers

Configurez la manière dont l'ID client et le secret sont envoyés à votre fournisseur OAuth.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Registre d'application** Cliquez sur **Nouveau**.
2. Sur la page de l'intercepteur, cliquez sur **Se connecter à un fournisseur OAuth tiers**, puis renseignez le formulaire.

Champ	Description
Nom	Nom unique de la connexion OAuth tierce.
ID client	ID client de l'application enregistrée dans le serveur OAuth tiers.
Secret client	Le secret client de l'application enregistrée dans 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	Type d'attribution par défaut utilisé pour établir le jeton. Les choix sont les suivants : ○ **Code d'autorisation** : code qui est 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).

Champ	Description
	○ **Informations d'identification du mot de passe du propriétaire** de ressource : nom d'utilisateur et mot de passe de l'utilisateur qui tente d'obtenir l'accès à la ressource. ○ **Informations d'identification du client** : ID client 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 avec le fournisseur. **Remarque :** Pour la demande sortante, utilisez le **support SAML2** comme type d'attribution SuccessFactors par défaut.
Durée de vie du jeton d'actualisation	Durée, en secondes, pendant laquelle le jeton d'actualisation est valide. Le temps par défaut est de 8 640 0000 secondes.
Client public	Permet aux clients publics d'exiger PKCE pour une autorisation. **Remarque :** Vous ne pouvez utiliser que le code d'autorisation lorsque PKCE *`Default Grant type`* est activé.
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 de l'application qui contiennent cet enregistrement.
Accessible depuis	Rendre cette application accessible à partir de tous les périmètres de l'application ou à partir de ce périmètre uniquement.
Actif	Cochez la case pour activer l'application.
URL d'autorisation	Point de terminaison du code d'autorisation OAuth.
URL de jeton	Point de terminaison du jeton du serveur OAuth.
URL de révocation du jeton	Le point de terminaison de révocation du jeton du serveur OAuth.
URL de redirection	Point de terminaison de rappel OAuth. Si le 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.

Champ	Description
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

Le système crée un enregistrement dans la table Registres d'application [oauth_entity] avec le type Fournisseur OAuth.

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 champ d'application.
   Vous pouvez modifier ou ajouter un profil de fournisseur OAuth incluant le nom, le type d'accord et le champ d'application OAuth.
4. **Facultatif :** Accédez à la liste connexe sur l'enregistrement Périmètres des entités OAuth pour définir tous les périmètres OAuth disponibles pour ce fournisseur OAuth.
   Vous pouvez sélectionner les champs d'application lorsque vous créez ou mettez à jour un profil. Chaque champ d'application OAuth contient un nom et un champ d'application que vous devez obtenir à partir de la spécification du fournisseur, par exemple un champ de lecture ou un champ d'écriture. Chaque périmètre doit être défini séparément.

Support JWT

Les jetons Web JSON (JWT) permettent de configurer des interactions d'API de serveur à serveur entre ServiceNow des fournisseurs d'API externes sans aucune intervention de l'utilisateur.

L'octroi 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'attribution 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 OAuth 2.0 JWT pour le message rest sortant.

Configurer le fournisseur OAuth avec le type d'attribution titulaire JWT

Les jetons Web JSON (JWT) permettent de configurer des interactions d'API de serveur à serveur entre ServiceNow des fournisseurs d'API externes sans aucune intervention de l'utilisateur. Cette prise en charge active Hub d'intégration d'autres tâches automatisées utilisant JWT pour configurer les intégrations d'API et de service avec différents fournisseurs.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les tâches suivantes montrent comment ServiceNow configurer les JWT pour les autorisations d'authentification et d'autorisation des clients OAuth 2.0. ServiceNow est le client OAuth, et vous pouvez configurer un fournisseur OAuth, tel que Box ou Docusign.

Procédure

1. Charger le certificat Java Key Store
   Joignez un certificat JKS à votre instance à utiliser 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 titulaire JWT comme type d'attribution par défaut dans le registre d'application ServiceNow .
5. Spécifier un profil OAuth
   Ouvrez le profil d'entité OAuth du fournisseur OAuth et affectez un fournisseur JWT.

Charger le certificat Java Key Store

Vous pouvez joindre un certificat Java KeyStore (JKS) à votre instance 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.

Option	Description
Nom	Nom unique de 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 certificat avant l'expiration de votre certificat.
Actif	Permet d'utiliser le certificat pour les demandes de jetons.
Type	Type de certificat que vous chargez.
Échéance en jours	Nombre de jours avant l'expiration du certificat.
Mot de passe de magasin de clés	Le 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 attribuer à votre certificat Java KeyStore (JKS),

Avant de commencer

Rôle requis : admin

Remarque :
Si vous souhaitez ajouter l'empreinte digitale du **certificat X.509 SHA-1 int (x5t)** à l'en-tête dans le cadre de la clé JWT, vous devez configurer le formulaire et ajouter le champ **int 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	Magasin de clés désigné lors de la signature de l'accord JWT.
ID clé	L'ID de clé (enfant) permet d'identifier quelle clé est utilisée lorsque plusieurs clés sont utilisées pour signer les jetons. **Remarque :** Si vous configurez ce champ, la demande d'ID de clé est incluse dans le JWT. Si vous ne configurez pas ce champ, votre JWT n'aura pas de demande 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 JSON Web Token (JWT) à votre ServiceNow instance.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Fournisseur JWT**.
2. Renseignez le formulaire et cliquez sur **Envoyer**.

Option	Description
Nom	Nom unique pour la configuration de votre fournisseur JWT.

Option	Description
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 la clé de signature JWT à appliquer.

Générer un jeton Web JSON (JWT)

Créez un jeton Web JSON (JWT) pour représenter en toute sécurité des réclamations entre deux parties sur le Now Platform.

L'API GlideJWT est une API incluse dans le champ d'application, pouvant contenir des scripts, 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 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 revendications standard et personnalisées lors de la configuration d'un fournisseur JWT. Vous pouvez transmettre des revendications 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 client OAuth fournit des méthodes pour demander et révoquer des 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 gestion des demandes des clients.
- GlideOAuthClientResponse : méthodes de gestion des réponses des clients.
- GlideOAuthToken : méthodes de récupération du jeton d'accès et des informations sur le jeton d'accès.

Vous pouvez également personnaliser le script include OAuthUtil pour intercepter les paramètres de requête et analyser les réponses des fournisseurs OAuth externes.

Lorsque vous utilisez des classes OAuth dans un script inclus dans le périmètre, utilisez l'identificateur d'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 quel profil OAuth 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`*.

Paramètres OAuth pour la prise en charge des profils par défaut

Paramètre	Description
`oauth_requestor`	La sys_id de l'objet, qui peut être un enregistrement utilisateur ou un compte de messagerie.
`oauth_requestor_context`	Descripteur qui fournit le contexte pour le demandeur OAuth. Il est recommandé d'utiliser 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'attribution 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 *`setScope`* et *`setGrantType`* de l'API GlideOAuthClientRequest. Pour plus d'informations, consultez setScope et setGrantType .

Prise en charge de la clé privée JWT pour l'authentification client OAuth 2.0

Prise en charge de JWT Prise en charge de l'authentification client OAuth 2.0.

L'authentification client JWT de clé privée 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 requises

pour JWT pour l'authentification private_key_jwt , reportez-vous à la section Authentification client dans la documentation principale d'OpenID Connect .

Remarque :
Le jeton d'authentification doit être envoyé comme 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 du 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 la clé privée JWT pour effectuer les opérations suivantes :

- Authentification unique basée sur OIDC
- Intégrations OAuth sortantes

Configurer la clé privée JWT pour l'authentification unique basée sur OIDC

Configurez la clé privée JWT pour les intégrations SSO basées sur OIDC.

Avant de commencer
Rôle requis : admin

Vous devez effectuer les tâches suivantes avant de choisir Private Key JWT for OIDC based SSO.

- Charger le certificat Java Key Store: 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'empreinte digitale du **certificat X.509 SHA-1 int (x5t)** à l'en-tête dans le cadre de la clé JWT, vous devez configurer le formulaire et ajouter le champ **int d'empreinte SHA-1 du certificat X.509 (x5t).**

- Créer un fournisseur JWT avec une clé de signature JWT: ajoutez un fournisseur JWT à votre ServiceNow instance.

Pour inclure une clé JWT pour le fournisseur d'identité OIDC, vous devez :

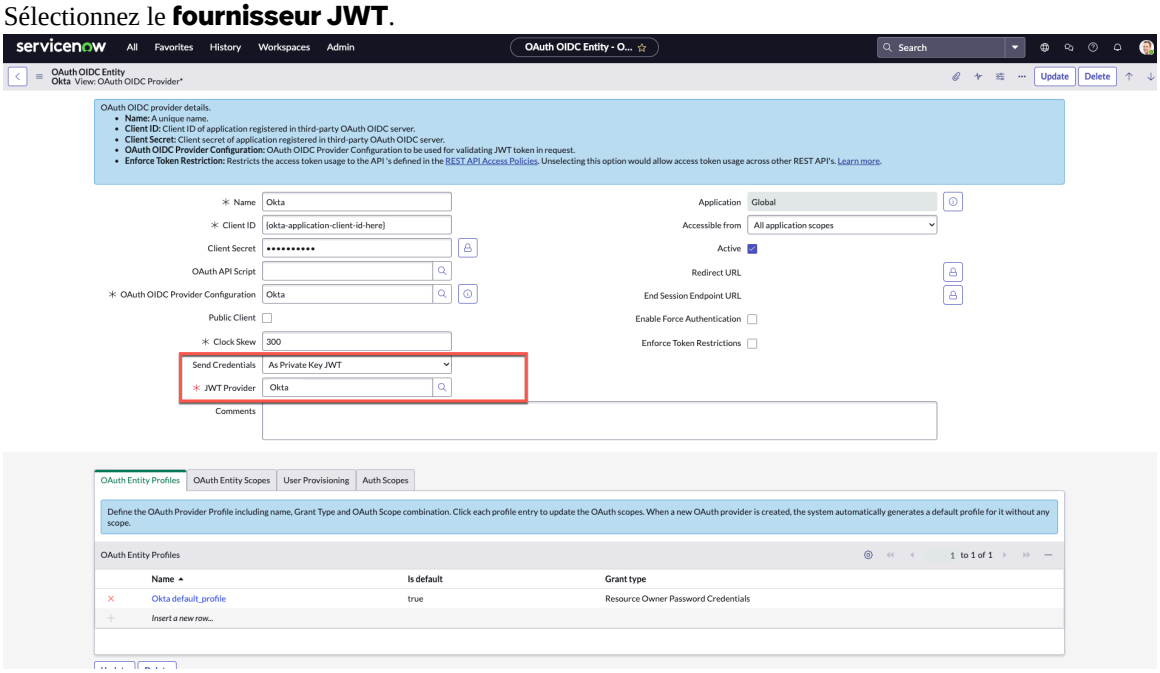
- Installez le module **d'extension Integration - Multiple Provider Single Sign-On Installer** (com.snc.integration.sso.multi.installer).
- Activez les propriétés pour les **propriétés SSO de plusieurs fournisseurs**. Pour plus d'informations, consultez Propriétés, tables et scripts de l'authentification unique (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 OIDC.

4. Choisissez En **tant que clé privée JWT** pour Envoyer les informations d'identification.
5. Sélectionnez le **fournisseur JWT**.



Lorsque l'utilisateur s'authentifie, la page d'authentification dispose d'options de connexion via Okta.

Configurer la clé privée JWT pour l'OAuth sortant

Configurez la clé privée JWT pour les intégrations OAuth sortantes.

Avant de commencer

Rôle requis : admin

Avant de configurer Private Key JWT pour les intégrations OAuth sortantes, vous devez effectuer les tâches suivantes :

- Charger le certificat Java Key Store: 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'empreinte digitale du **certificat X.509 SHA-1 int (x5t)** à l'en-tête dans le cadre de la clé JWT, vous devez configurer le formulaire et ajouter le champ **int d'empreinte SHA-1 du certificat X.509 (x5t).**

- Créer un fournisseur JWT avec une clé de signature JWT: ajoutez un fournisseur JWT à votre ServiceNow instance.

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Registre d'application** Cliquez sur **Nouveau**.
2. Sur la page de l'intercepteur, cliquez sur **Se connecter à un fournisseur OAuth tiers**, puis renseignez 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.

Champ	Description
Nom	Nom unique de la connexion OAuth tierce.
ID client	ID client de l'application enregistrée dans le serveur OAuth tiers.
Secret client	Le secret client de l'application enregistrée dans 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** : ID client et 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, en secondes, pendant laquelle le jeton d'actualisation est valide. Le temps par défaut est de 8 640 000 secondes.
Client public	Permet aux clients publics d'exiger PKCE pour une autorisation. **Remarque :** Vous ne pouvez utiliser que le code d'autorisation lorsque PKCE *`Default Grant type`* est activé.
Commentaires	Ajoutez des commentaires concernant l'application OAuth.
Application	Application et périmètre de l'application qui contiennent cet enregistrement.

Champ	Description
Accessible depuis	Rendre cette application accessible à partir de tous les périmètres de l'application ou à partir de ce périmètre uniquement.
Actif	Cochez la case pour activer l'application.
URL d'autorisation	Point de terminaison du code d'autorisation OAuth.
URL de jeton	Point de terminaison du jeton du serveur OAuth.
URL de révocation du jeton	Le point de terminaison de révocation du jeton du serveur OAuth.
URL de redirection	Point de terminaison de rappel OAuth. Si le 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 : **Comme clé privée JWT**
Fournisseur JWT	Détails du fournisseur JWT. Vous pouvez utiliser la fonction de recherche pour sélectionner le fournisseur JWT.

Le système crée un enregistrement dans la table Registres d'application [oauth_entity] de type Fournisseur OAuth qui peut être utilisé pour l'authentification de clé privée JWT.

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** Cliquez sur **Nouveau**.
2. Renseignez les champs de formulaire de l'enregistrement de l'application OAuth comme décrit à la section . Notez les valeurs de champ suivantes :
   - **Point de terminaison** : URL de l'instance qui est le serveur d'autorisation.
   - **Type d'authentification** : **OAuth 2.0**.
   - **Profil OAuth** : profil OAuth que vous avez créé pour le serveur client.
3. Sur l'enregistrement de message REST, cliquez sur **Obtenir le 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 auprès de l'instance.
   - Le nom d'utilisateur et le mot de passe de l'IdP sont activés. 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 Flux d'octroi du code d'autorisation OAuth.

Exigences de complexité des mots de passe

Les mots de passe de votre ServiceNow® instance doivent répondre à des exigences de complexité.

Explorer	Activer
	
Découvrez les fonctionnalités et la valeur commerciale des exigences de complexité des mots de passe.	Découvrez comment répondre aux exigences de complexité des mots de passe.

Configurer

Configurez les exigences de complexité des mots de passe.

Référence : caractères de mot de passe non pris en charge

Connaître les caractères de mot de passe non pris en charge.

Traduction automatique

Exploration des exigences de complexité des mots de passe

Les mots de passe de votre ServiceNow® instance doivent répondre à des exigences de complexité.

Le paramètre de politique Exigences de complexité des mots de passe détermine si les mots de passe doivent répondre à une série de directives en matière de mots de passe forts.

Les exigences de complexité des mots de passe s'appliquent lorsqu'un mot de passe est modifié ou créé.

Les exigences de complexité des mots de passe sont respectées et fonctionnent sur la base des éléments suivants :

- 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. Pendant 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.
- Des mots de passe dans les BMP autorisés peuvent être définis pour votre instance. Les mots de passe qui ne respectent pas ces PGO ne sont pas autorisés.

Si nécessaire, vous pouvez exiger que les mots de passe soient changés régulièrement, au moins tous les 90 jours.

Conditions requises et caractères interdits

Pour mettre en place 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 permettent d'empêcher les utilisateurs non autorisés qui utilisent généralement des méthodes manuelles ou automatisées de 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 en minuscules et en 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 d'employé ou noms d'utilisateur.
- Noms de marques ou de produits pertinents.
- Emplacements, tels que le siège social de l'entreprise, 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 les contrôles de la politique de mot de passe lors de la connexion. Forcer les utilisateurs à changer leur mot de passe si ce dernier ne répond pas aux critères de politique de mot de passe.

Avant de commencer

Rôle requis : admin

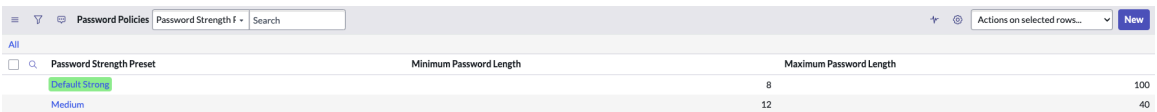
Pourquoi et quand exécuter cette tâche

Le module d'extension Password Policy (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 **Niveau de sécurité du mot de passe prédéfini** est automatiquement défini sur **Niveau de sécurité 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 propriété de banque `pwd_cred_store` d'identifiants `ValidatePasswordStronger` Réinitialisation

du mot de passe, consultez les propriétés de la politique de mot de passe pour savoir comment implémenter une politique de mot de passe pour votre instance.

Remarque :
La politique de mot de passe active est mise en surbrillance pour l'instance, comme illustré.



Pour modifier la politique de mot de passe, accédez à **Tous** > **Réinitialisation du mot de passe** > **Banques d'identifiants**, sélectionnez les informations d'identification et remplacez le champ **Politique de mot de passe** par 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 **Paramètre de sécurité du mot de passe** .

   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 préréglages à l'exception **de 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 préréglages à l'exception **de 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.

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 entrez `@$ !`, les utilisateurs ne peuvent pas utiliser « @ », « $ » et « ! » comme caractères spéciaux dans leurs mots de passe. **Remarque :** Cette option est disponible si la *`glide.password_policy.use_excluded_special_ch`* propriété est activée.
Interdire les données utilisateur	Option permettant d'interdire les données utilisateur liées à l'authentification.
Seuil de longueur de séquence	La longueur de 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 avoir un maximum de huit caractères. Ces champs vous permettent de limiter les combinaisons faibles de mots de passe ayant des séquences prévisibles et répétitives telles que « 123456 », « qwerty », « !@#$%^ », « aaaaa », etc. ◦ Si le **paramètre Force du mot de passe prédéfini** 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	Indiquez votre mot de passe réel dans ce champ.

6. Cliquez sur **Tester votre mot de passe**.

7. Une fois que la validité du mot de passe a été vérifiée, 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 **true**. **Remarque :** • Si votre instance est personnalisée, via la sortie d'installation ou votre `ValidatePasswordStronger` banque d'identifiants 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 `ValidatePasswordStronger` sortie d'installation, vous deviez créer la propriété Politique de mot de passe pour que la politique de mot de passe fonctionne. • À partir de la Orlando version, il n'y a pas de personnalisation de sortie d'installation. Les propriétés de la politique de mot de passe fonctionnent par défaut. Ces propriétés peuvent être désactivées manuellement.
glide.enable.blacklist_password	Il est interdit d'utiliser des 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 **true**.
glide.apply.password_policy.on_login	Force 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.

Propriété	Description
	Cette propriété est automatiquement définie sur **faux**. Lorsque la valeur est **définie sur vrai** , une politique de mot de passe est appliquée lors de la connexion. **Remarque :** L'activation de cette propriété peut forcer un nombre important d'utilisateurs qui ne respectent pas 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 Politique de mot de passe.
glide.validate.sys_utilisateur.mot de passe.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** dans 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 du débogage pour la politique de mot de passe.

Configuration de 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 de mot de passe.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Le module d'extension Password Policy [com.glide.password_policy] est activé par défaut. Il entre en vigueur lorsqu'un utilisateur modifie ou réinitialise le mot de passe. Si vous avez personnalisé votre instance, via la sortie d'installation de ValidatePasswordStronger ou votre banque d'identifiants Password Reset [pwd_cred_store], consultez les propriétés de la stratégie de mot de passe.

Procédure

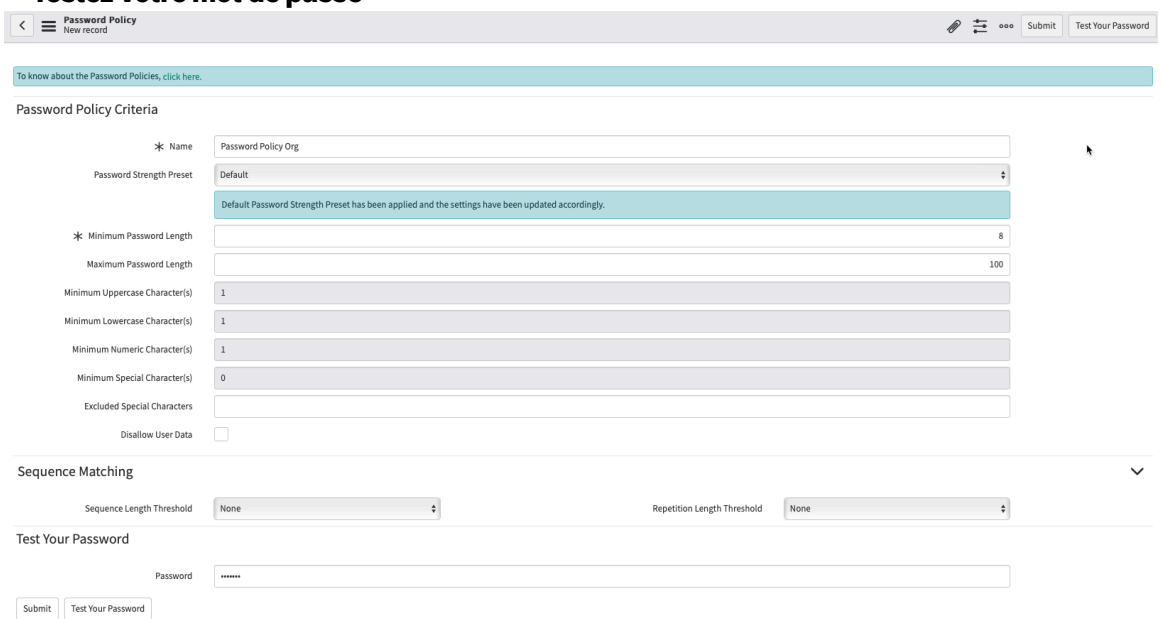
1. Accédez à la **Tous** > **Politique de mot de passe** > **Politiques de mot de passe**.

   Remarque :
   Préréglage fort par défaut dans Activé comme critère d'acceptation du mot de passe par défaut. Si vous souhaitez ajouter un nouveau critère, vous pouvez effectuer les étapes suivantes.

2. Cliquez sur **Nouveau**.

   La page de nouvel enregistrement de la politique de mot de passe comporte les sections suivantes que vous devez spécifier pour définir votre mot de passe :

- **Critères de politique du 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 de niveau de sécurité du mot de passe**.
   Les préréglages 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 automatiquement renseignés comme suit : ○ Un caractère majuscule minimum ○ Un caractère minuscule minimum ○ Un caractère numérique minimum
Moyenne	Si vous sélectionnez **Moyen** , les caractères de mot de passe requis sont renseignés 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 du mot de passe sont renseignés automatiquement comme suit :

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 la **valeur par défaut forte** , les caractères de mot de passe requis sont renseignés 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 renseignés 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 **de Paramètres avancés** affiche **le script de règle de mot de passe** et le **script de force de 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 préréglages à l'exception **de Avancé**.

Champ	Description
	Remarque : **La 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 préréglages à l'exception **de Avancé**. **Remarque :** **La longueur maximale du mot de passe** est un champ facultatif. 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 ne peuvent utiliser que « $ » 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 utilisateurs ne doivent pas pouvoir utiliser « @ », « $ » et « ! » comme caractères spéciaux dans leurs mots de passe. **Remarque :** Cette option est disponible si la propriété glide.password_policy.use_excluded_special_char est activée.
Interdire les données utilisateur	Il est activé pour interdire les données utilisateur.

6. Dans la section Correspondance de séquence, spécifiez le **seuil de longueur de séquence** et le **seuil de longueur de répétition**.

Remarque :

- Le seuil de longueur de séquence et le seuil de longueur de répétition peuvent avoir un maximum de huit caractères. Ces champs vous permettent de limiter les combinaisons faibles de mots de passe ayant des séquences prévisibles et répétitives telles que « 123456 », « qwerty », « !@#$%^ », « aaaaa », etc.
- Pour **Fort par défaut**, la longueur du seuil de longueur de séquence et du seuil de longueur de répétition est sélectionnée en 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 vos utilisateurs pour l'instance en fonction de la politique de mot de passe configurée.

Avant de commencer

Utilisateurs créés pour définir le mot de passe pour leur première connexion. Pour plus d'informations, consultez Créer un utilisateur .

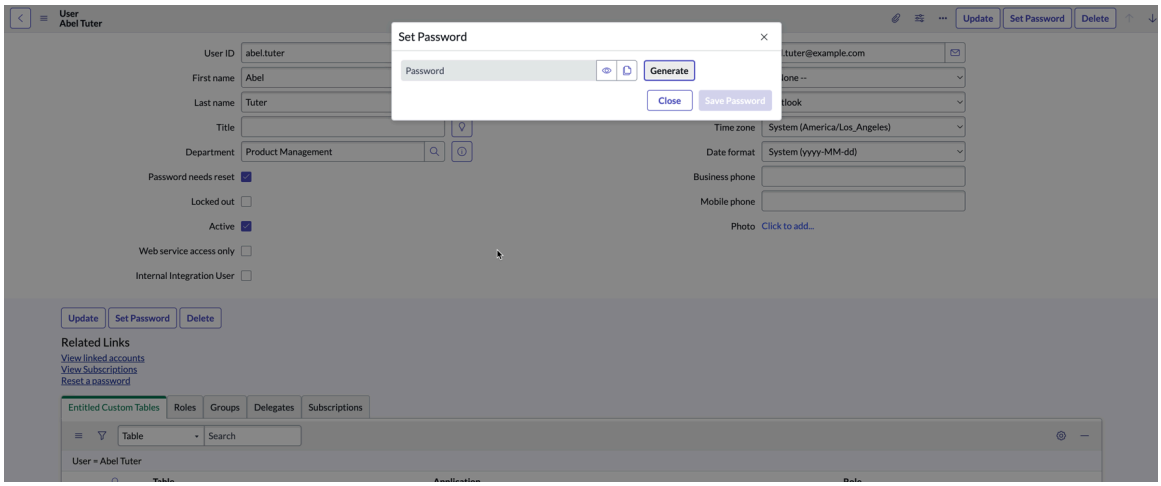
Pour renseigner le champ **Mot de passe** directement sur le formulaire utilisateur, activez **l'option Activer afin d'afficher le champ Mot de passe sur le formulaire sys_user** (glide.user.show.password.field). Pour en savoir plus sur les propriétés, reportez-vous à Propriétés de la politique de mot de passe.

Rôle requis : admin

Procédure

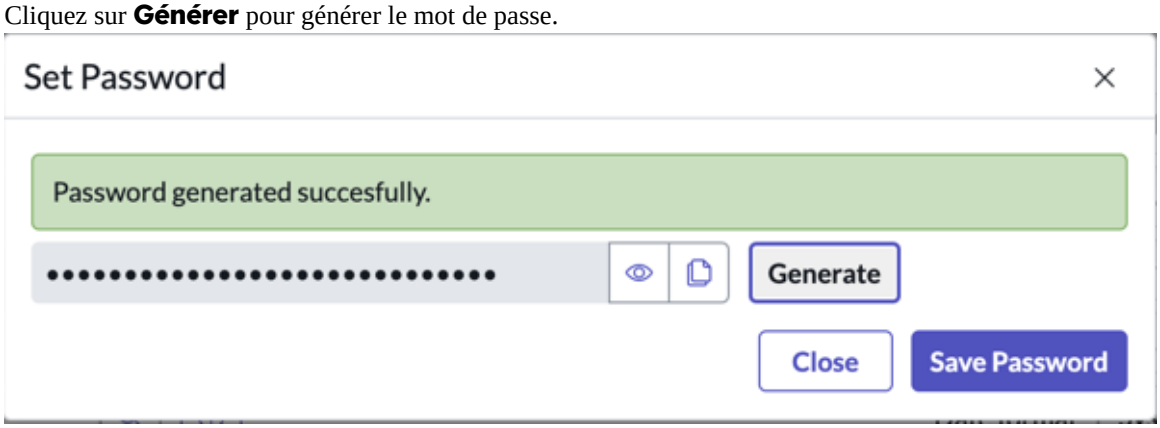
1. Accédez à la **Tous** > **Administration utilisateurs** > **Utilisateurs**.
2. Sélectionnez l'utilisateur dans la liste de la page Utilisateurs.
3. Pour définir le mot de passe en fonction de la politique de mot de passe, cliquez sur **Définir le mot de passe**.

   La fenêtre contextuelle Définir le mot de passe s'affiche.

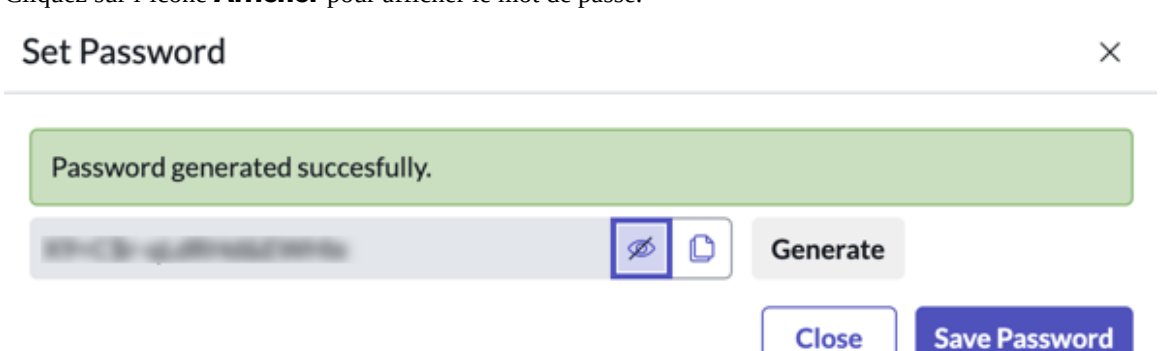


4. Dans Définir le mot de passe, procédez comme suit.

a. Cliquez sur **Générer** pour générer le mot de passe.

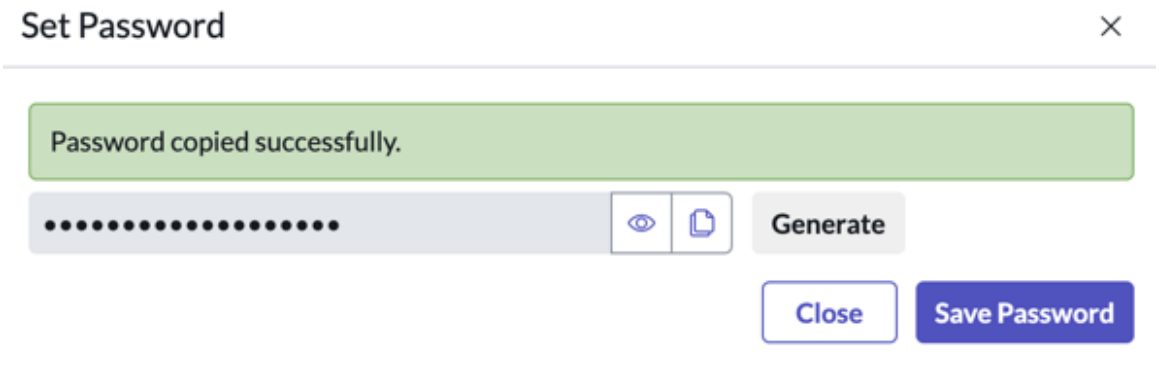


b. Cliquez sur l'icône **Afficher** pour afficher le mot de passe.



Traduction automatique

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 Mot de passe doit rester est automatiquement activée.

   Lors de la première connexion, l'utilisateur doit utiliser le même mot de passe pour se connecter et modifier le mot de passe lors de la connexion, conformément à la politique de mot de passe configurée par les administrateurs.

Exclure les mots de passe via des 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 sur votre instance.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Vous pouvez interdire autant de mots de passe que nécessaire. En voici quelques exemples :

- Séquences prévisibles et répétitives, telles que « 123456 », « qwerty », « !@#$%^ », « aaaaa », etc.
- Nom d'employé ou noms d'utilisateur.
- Noms de marques ou de produits pertinents.
- Emplacements, tels que le siège social d'une société, la ville, le 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 gérer 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** comporte environ 5000 mots de passe couramment utilisés.

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 mettre en place 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 permettent d'empêcher les utilisateurs non autorisés qui utilisent généralement des méthodes manuelles ou automatisées de 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 fournie 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 Exclure le mot de passe.

Pour plus d'informations sur les propriétés de la politique de mot de passe, consultez Propriétés de la politique de mot de passe.

S'enregistrer automatiquement dans l'instance ServiceNow

Utilisez l'enregistrement automatique des utilisateurs externes pour intégrer un grand volume d'utilisateurs externes à votre instance. Cette fonctionnalité améliore la vérification d'identité pour améliorer l'expérience utilisateur et prend en charge les flux d'inscription couramment utilisés.

Explorer

Découvrez les fonctionnalités et la valeur commerciale de l'auto-enregistrement.

Activer

Traduction automatique

Découvrez comment activer l’auto-enregistrement externe.

Configurer

Configurez l’enregistrement automatique.

Activer

Renseignez-vous sur les propriétés dans l’auto-enregistrement.

Traduction automatique

Explorer l’auto-enregistrement

Utilisez l’enregistrement automatique des utilisateurs externes pour intégrer un grand volume d’utilisateurs externes à votre instance. Cette fonctionnalité améliore la vérification d’identité pour améliorer l’expérience utilisateur et prend en charge les flux d’inscription couramment utilisés.

L’enregistrement automatique des utilisateurs externes 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 sur le campus. Chaque étudiant se verrait accorder un ensemble limité de privilèges spécifiques au stationnement et suivrait un processus d’inscription automatisé. Ce système pouvait générer un numéro de stationnement, unique à chaque élève, et s’assurer qu’il disposait d’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 configurerait l’inscription, y compris un flux de pré-inscription, un mappage de champs, un mappage post-inscription, un captcha, un mappage de rôles et un flux post-inscription.

Activation de l’enregistrement automatique des utilisateurs externes

Vous pouvez activer le module d’extension d’enregistrement automatique des utilisateurs externes (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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

Rôles externes en auto-inscription

Pour éviter de fournir l'accès par inadvertance aux utilisateurs externes, vous pouvez affecter le rôle de snc_external à tous les utilisateurs externes.

Les utilisateurs externes qui s'enregistrent automatiquement doivent se voir affecter le rôle snc_external, qui a 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 :

- Ressources Scripted REST API qui ne sont pas marquées comme étant externes.
- 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 Now Intelligence.

À partir de la version Paris, vous devez activer une propriété de liste d'exclusion pour appliquer l'affectation explicite de snc_external rôles. Pour plus d'informations sur l'activation de la propriété, consultez Empêcher les futures affectations de rôles internes pour les utilisateurs externes .

Configuration d'une configuration d'enregistrement utilisateur pour les utilisateurs externes

Créez un enregistrement de configuration de l'inscription de l'utilisateur pour amorcer le processus d'intégration des utilisateurs externes à des applications personnalisées ServiceNow . Ce formulaire guide les utilisateurs externes tout au long du processus d'auto-inscription.

Avant de commencer

- Rôle requis : admin
- Activation de l’enregistrement automatique des utilisateurs externes

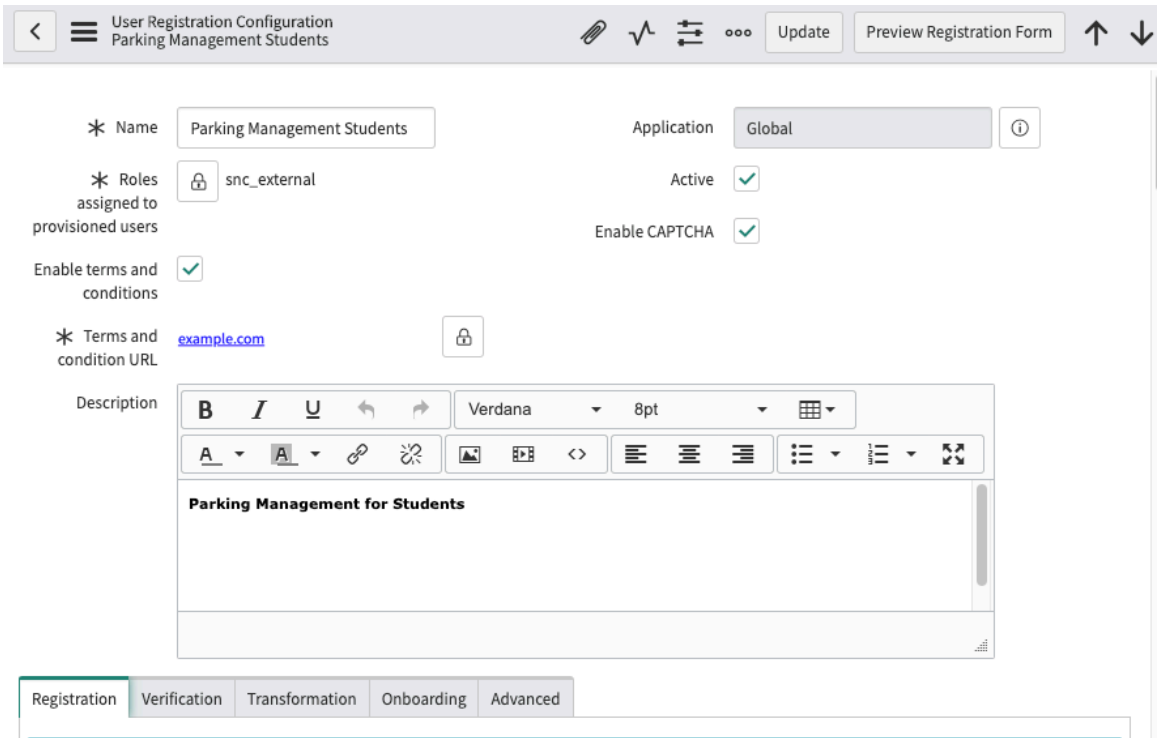
Procédure

1. Accédez à la **Tous** > **Enregistrement utilisateur externe automatique** > **Configurations de l'inscription de l'utilisateur** et cliquez sur **Nouveau**.
2. Renseignez les champs du formulaire.

Formulaire Configuration de l’inscription de l’utilisateur

Champ	Description
Nom	Nom du formulaire d’inscription. Par exemple, une inscription de stationnement étudiant 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 un `snc_external` pour noter un utilisateur externe. Si vous avez des rôles préconfigurés, les rôles doivent être accessibles lorsque vous déverrouillez les rôles et recherchez des utilisateurs.
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 s’affiche uniquement lorsque **l’option Activer les termes et conditions** est sélectionnée.
Description	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’enregistrement de l’utilisateur, suivez les étapes décrites dans Configurer Google reCAPTCHA pour l’enregistrement automatique des utilisateurs externes.

3. Cliquez sur **Envoyer**.
   Une configuration d’enregistrement utilisateur avec les paramètres par défaut est créée.



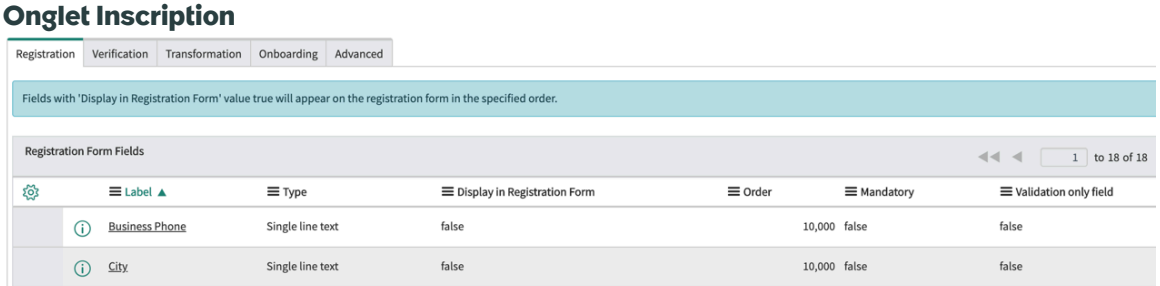
4. **Facultatif :** Configurez l'onglet **Inscription** pour afficher les champs et l'ordre dans lequel ils apparaissent :

Champs de formulaire d'inscription

Colonne	Description
Afficher dans le formulaire d'inscription	Définissez n'importe quel champ que vous souhaitez afficher comme Vrai.
Ordre	Définissez un numéro d'ordre pour afficher les champs sur votre formulaire.
Obligatoire	Définissez n'importe quel champ que vous souhaitez rendre obligatoire sur True.
Champ de validation uniquement	Définissez n'importe quel champ que vous souhaitez utiliser uniquement pour la validation. Par exemple, 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 du formulaire d'inscription par défaut.

Onglet Inscription



Traduction automatique

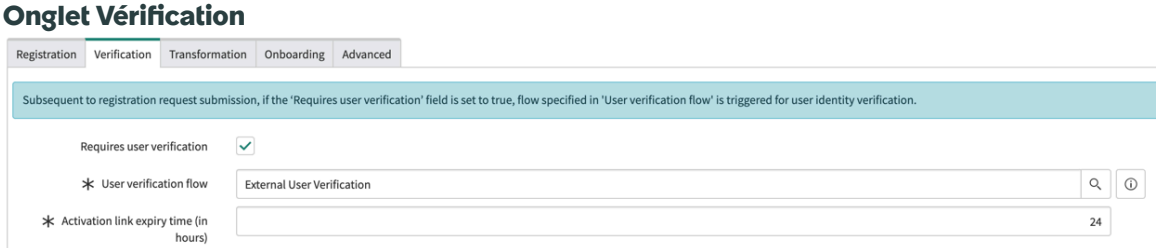
Vous pouvez également ajouter des champs de formulaire d'inscription personnalisés. Pour plus d'informations, consultez Ajouter un champ de formulaire d'inscription personnalisé.

5. **Facultatif :** Configurez l'onglet **Vérification** pour vérifier l'identité des utilisateurs enregistrés. Lorsque le flux de vérification d'utilisateur se déclenche, un lien d'activation est envoyé à l'adresse e-mail enregistrée de l'utilisateur.

Champs de l'onglet Vérification

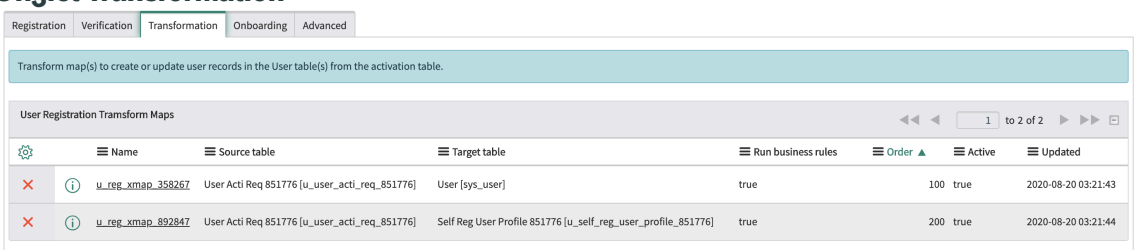
Champ	Description
Requiert une vérification de l'utilisateur	Option permettant de déclencher un flux secondaire de vérification de l'utilisateur qui s'exécute après l'inscription de l'utilisateur. Le flux secondaire est destiné à la vérification de l'identité de l'utilisateur.
Flux de vérification de 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 la Concepteur de flux modifier en fonction de vos besoins. Pour plus d'informations, consultez Flow 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 l'expiration d'un lien d'activation. 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_[nombre]) qui mappent automatiquement les utilisateurs enregistrés de la table Utilisateur acti Req [numéro] à la table Utilisateur [nombre] enregistré automatiquement. 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, reportez-vous à la section Cartes de transformation.

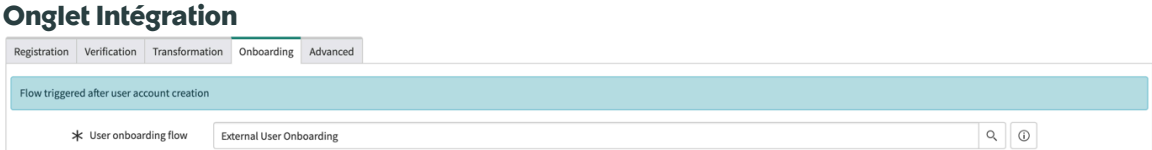
Onglet Transformation



7. Configurez l'onglet **Intégration** pour déclencher des flux secondaires pour les utilisateurs activés d'intégration.
   Le flux secondaire **d'intégration d'utilisateur externe** par défaut envoie à l'utilisateur un e-mail contenant un lien pour réinitialiser son mot de passe. Vous pouvez créer une copie du flux secondaire par défaut et la modifier en fonction de vos besoins.

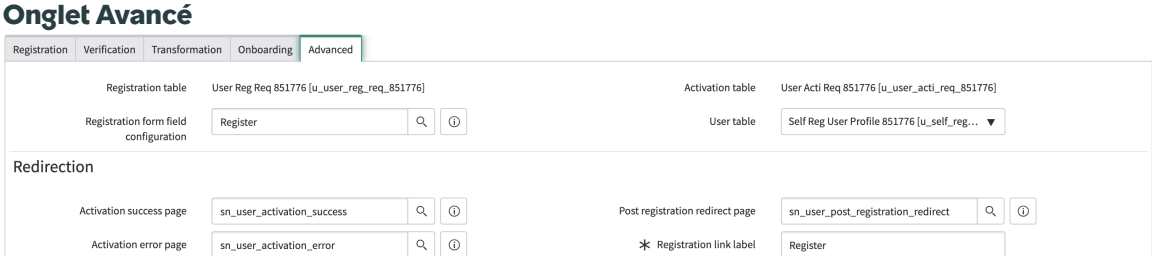
> **Remarque :**
> Lorsque le flux secondaire **Intégration d'un utilisateur externe** se déclenche, le flux secondaire envoie un e-mail contenant un lien à l'utilisateur pour réinitialiser le mot de passe.

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



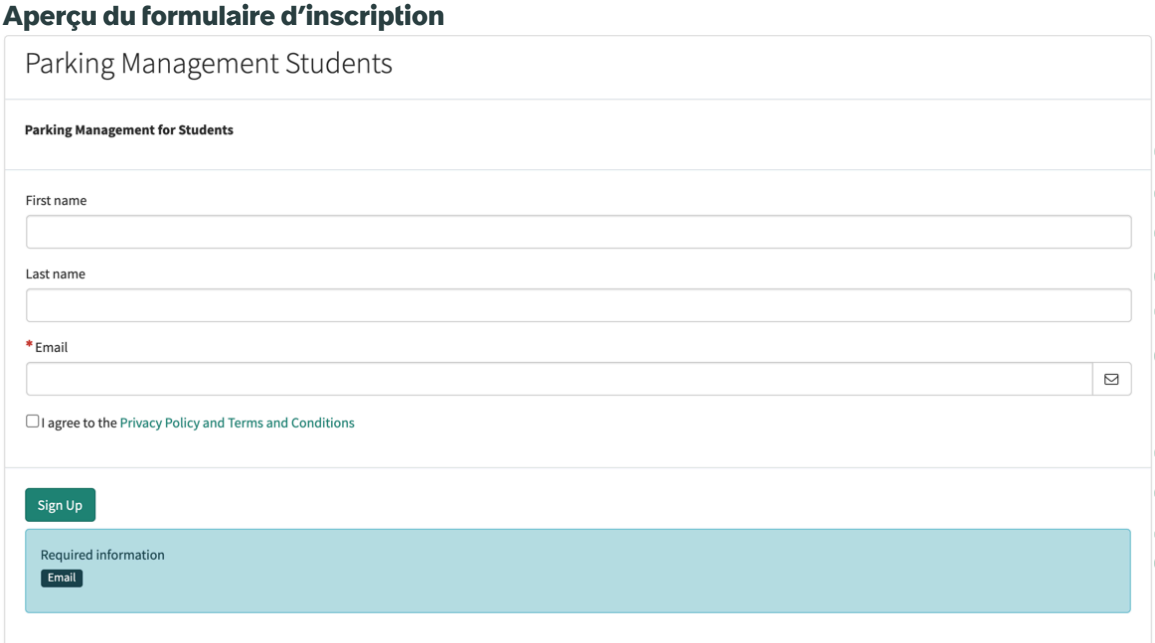
Onglet Avancé

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	L'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 terminé la vérification.
Table des utilisateurs	Étiquette et nom de la table de profils d'utilisateurs.
Page de réussite d'activation	La page vers laquelle un utilisateur est redirigé après l'activation.

Champ	Description
Page d'erreur d'activation	La page vers laquelle un utilisateur est redirigé lorsque l'activation échoue.
Page de redirection post-inscription	La 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 dans la configuration de l'inscription de l'utilisateur, vous pouvez utiliser le bouton **Prévisualiser le formulaire d'inscription** pour prévisualiser les modifications dans le formulaire d'inscription.

Aperçu du formulaire d'inscription



Configurer Google reCAPTCHA pour l'enregistrement automatique des utilisateurs externes

Pour utiliser le Google reCAPTCHA service, vous devez demander une paire de clés API à Google , puis configurer les propriétés système connexes.

Avant de commencer

- Demandez une paire de clés API (une clé de site et un secret) depuis Google au https://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	La clé de site utilisée pour appeler le service reCAPTCHA sur votre page d'inscription. Type : chaîne
glide.user.registration.captcha.widget	La Sys_ID du widget captcha. Type : chaîne

Champs du 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

Étiquette de champ	Type
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 , etc.	Zone de sélection
État / Province	Texte sur ligne unique
Rue	Texte sur ligne unique large
Titre : fonction	Zone de sélection
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 d'utilisateur requise.
3. Accédez à la fin de la section Champs du formulaire d'inscription et cliquez sur **Insérer une nouvelle ligne...**
4. Saisissez le nom du champ sous la colonne **Étiquette** et cliquez sur la 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	Le 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

Colonne	Description
	○ 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	La séquence dans laquelle les champs de formulaire apparaissent sur le formulaire d'inscription. Le champ ayant la valeur d'ordre la plus basse apparaît en premier et le champ ayant la valeur d'ordre la plus élevée apparaît en dernier. La valeur par défaut est 10 000.
Obligatoire	Option pour rendre un champ obligatoire sur le formulaire d'inscription.
Champ de validation uniquement	Option pour utiliser un champ uniquement à des fins de validation. Par exemple, code d'inscription. Lorsqu'il est défini sur vrai, ce champ n'est pas enregistré dans la table Utilisateur (sys_user).

5. Enregistrez ou mettez à jour les modifications.

Activer l'enregistrement automatique des utilisateurs externes 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 Configuration de **l'inscription de l'utilisateur externe** du formulaire.

   Sélectionnez une configuration d'inscription utilisateur.
4. Cliquez sur **Mettre à jour**.

Résultats
Le widget de connexion inclut un lien vers le formulaire d'inscription que vous avez précédemment configuré.

Rôles externes en auto-inscription

Pour éviter de fournir l'accès par inadvertance aux utilisateurs externes, vous pouvez affecter le rôle de snc_external à tous les utilisateurs externes.

Les utilisateurs externes qui s'enregistrent automatiquement doivent se voir affecter le rôle snc_external, qui a 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 :

- Ressources Scripted REST API qui ne sont pas marquées comme étant externes.
- 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 Now Intelligence.

À partir de la version Paris, vous devez activer une propriété de liste d’exclusion pour appliquer l’affectation explicite de snc_external rôles. Pour plus d’informations sur l’activation de la propriété, consultez Empêcher les futures affectations de rôles internes pour les utilisateurs externes .

Vérifier les demandes d’inscription automatique de l’utilisateur

Lorsqu’un utilisateur s’est inscrit à partir de , Portail de servicesun enregistrement utilisateur est ajouté au module Demandes d’enregistrement. Vous pouvez afficher la liste des utilisateurs enregistrés qui se sont correctement inscrits 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 utilisateur s’affiche.
2. **Facultatif :** Examinez les enregistrements utilisateur individuels et modifiez-les en fonction de vos besoins. Par exemple, vous pouvez modifier l’état d’un formulaire d’enregistrement utilisateur **En attente** en **Traité**.

Authentification basée sur un jeton (connexions utilisateur)

Améliorez le mécanisme de sécurité permettant aux utilisateurs d’accéder à un réseau à l’aide d’une authentification basée sur un jeton.

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.

Elle permet d’améliorer le mécanisme de sécurité permettant aux utilisateurs d’accéder à un réseau.

Utilisation de l’authentification du 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

Prise en charge de l’authentification limitée dans le temps pour votre ServiceNow instance.

Traduction automatique

Explorer

Découvrez les fonctionnalités et la valeur commerciale de l’authentification limitée dans le temps.

Activer

Découvrez comment activer l’authentification limitée dans le temps.

Didacticiel : Authentification temporelle limitée

Traduction automatique

Exploration de l'authentification temporelle limitée

Prise en charge de l'authentification limitée dans le temps pour votre ServiceNow instance.

Remarque :
L'authentification temporelle limitée est très spécifique à l'instance ServiceNow , les liens personnalisés pour les utilisateurs ne peuvent être créés que dans ServiceNow.

Les administrateurs peuvent configurer l'authentification basée sur le 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 par les politiques d'authentification adaptative configurées sur l'instance ServiceNow .

L'authentification basée sur le temps vous permet d'effectuer les opérations suivantes :

- L'administrateur peut configurer l'authentification basée sur le 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 pour l'authentification avec la liaison TLA.

Activer l'authentification temporelle limitée

L'authentification limitée dans le temps s'active via le module d'extension Integration - Multiple Provider Single Sign-On Installer.

Avant de commencer
Rôle requis : admin

Remarque :
L'authentification temporelle limitée est très spécifique à l'instance ServiceNow , 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. Trouvez 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.

   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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

> **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>.

Authentification temporelle limitée avec SMS - Twilio Tutoriel

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 temporelle limitée)
- `com.snc.authentication.sms_mfa` (authentification multifacteur par SMS)

> **Remarque :**
> L'authentification temporelle limitée (TLA) est 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 correcte, le système génère un lien, puis partage ce lien avec l'utilisateur via le canal de notification (e-mail/SMS). En sélectionnant le lien, l'utilisateur est invité à spécifier le facteur OTP envoyé par e-mail ou SMS en fonction du rôle d'utilisateur (configuration).

> **Remarque :**
> - Le TLA doit toujours être suivi de MFA et le MFA doit être activé par un administrateur qui utilise Adaptive Authentication pour la connexion TLA. Pour en savoir plus sur la configuration de l'authentification MFA avec Adaptive Authentication, reportez-vous à Contexte MFA (Multi-Factor Authentication).
> - TLA doit être utilisé pour les utilisateurs qui ont des privilèges limités.

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** (origine de Twiliocréation), puis sauvegardez l'enregistrement.

Remarque :
Vous pouvez créer votre propre configuration de fournisseur et l'utiliser pour TLA. Dans cet exemple, il s'agit de Twilio. Pour en savoir plus sur la création d'une configuration de fournisseur MFA, reportez-vous à Configurer le fournisseur MFA.

2. Configurez et activez l'enregistrement d'authentification limitée dans le temps (TLA).

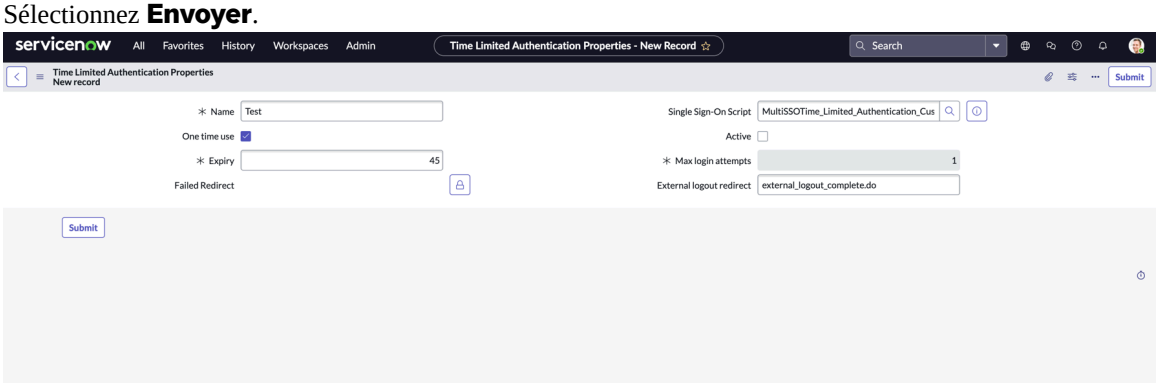
a. Accédez à la **Tous** > **Enregistrements de configuration de l'authentification temporelle limitée** et sélectionnez **Nouveau**.

b. Renseignez les champs du formulaire.

Propriétés d'authentification temporelle limitée

Champ	Description
Nom	Nom de l'enregistrement.
Utilisation ponctuelle	Sélectionnez cette option pour utiliser le lien TLA une seule fois.
Expiration	Spécifiez les secondes pour l'expiration du lien. La valeur par défaut est de 45 minutes.
Échec de la redirection	Entrez l'URL vers laquelle rediriger les 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	Entrez l'URL pour rediriger les utilisateurs après la déconnexion.

c. Sélectionnez **Envoyer**.



d. Accédez à la **Tous** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Administration** > **Propriétés** et activez la propriété **Activer l'authentification unique de plusieurs fournisseurs** et cliquez **sur Enregistrer**.

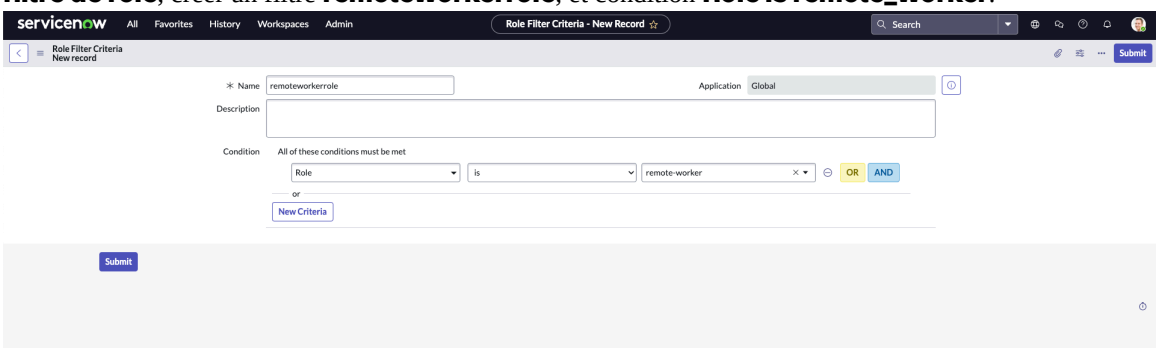
3. Autoriser TLA uniquement à un profil d'utilisateur spécifique à l'aide de la politique de contexte post-authentification.

   a. Accédez à **Rôles** et créez un rôle.
   Par exemple : remote_worker.

   b. Créez un utilisateur avec un ID d'e-mail et un numéro de téléphone mobile valides.
   Pour savoir comment créer un utilisateur, consultez Créer un utilisateur .

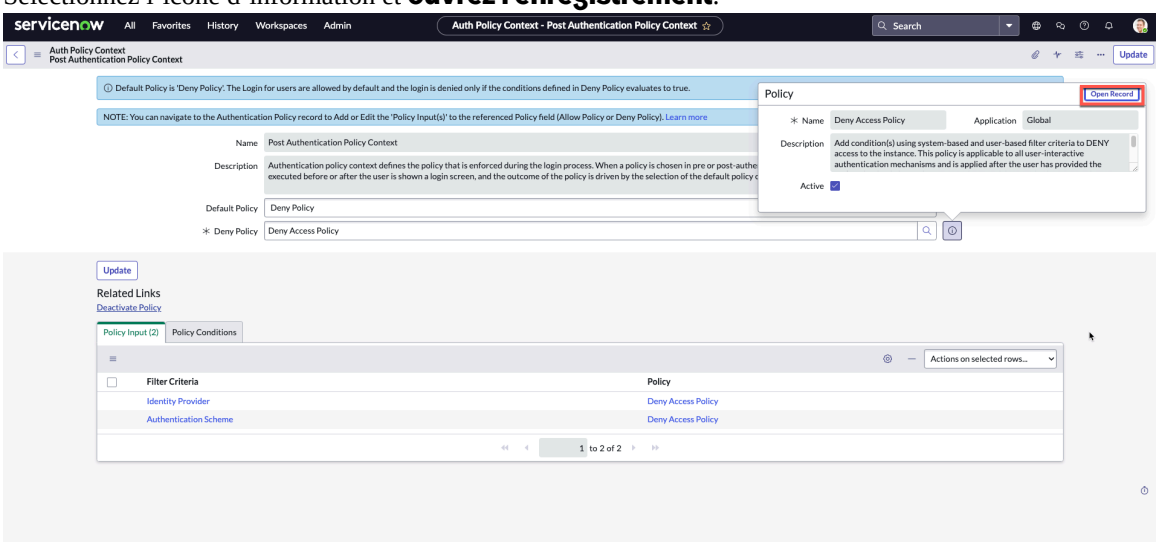
   c. Affectez le rôle à l'utilisateur.
   Pour savoir comment affecter le rôle à l'utilisateur, consultez Affecter un rôle à un utilisateur .

   d. Pour créer des critères de filtre de rôle, accédez à **Tous** > **Authentification Adaptative** > **Critère de filtre de rôle**, créer un filtre **remoteworkerrole**, et condition **Role is remote_worker**.



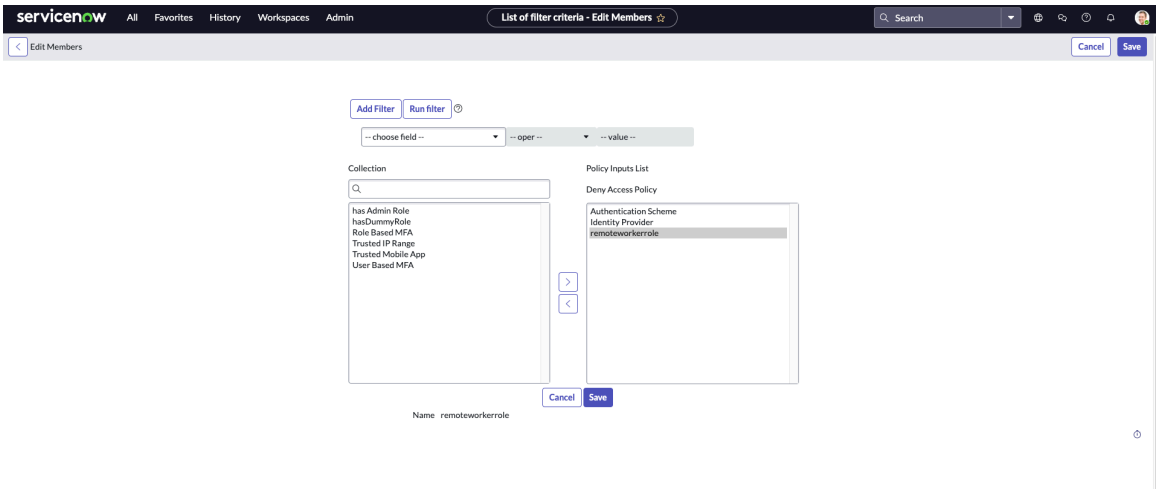
   e. Pour ajouter une condition de politique basée sur le contexte de la politique de refus en fonction des critères de filtre d'IdP et de rôle, accédez à **Tous** > **Authentification Adaptative** > **Contexte de post-authentification**.

   f. Sélectionnez l'icône d'information et **ouvrez l'enregistrement**.



   g. Dans l'entrée Politique, sélectionnez **Modifier** et ajoutez le rôle (remoteworkerrole), puis **cliquez sur Enregistrer**.

Traduction automatique

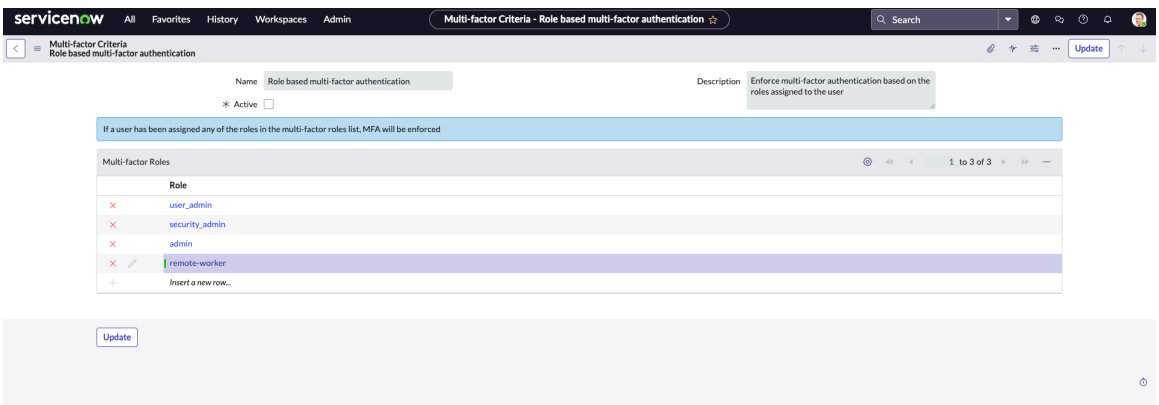


h. Dans la condition de politique, ajoutez la condition pour l'entrée de politique et **envoyez** l'enregistrement.

4. Configurer la politique d'authentification ascendante - Contexte MFA.

a. Accédez à la **Tous** > **Critère multifacteur**.

b. Sélectionnez **l'authentification multifacteur basée sur les rôles** et ajoutez le rôle sous la section Rôles multifacteur et **mettre à jour**.
Dans cet exemple : **remote_worker**.



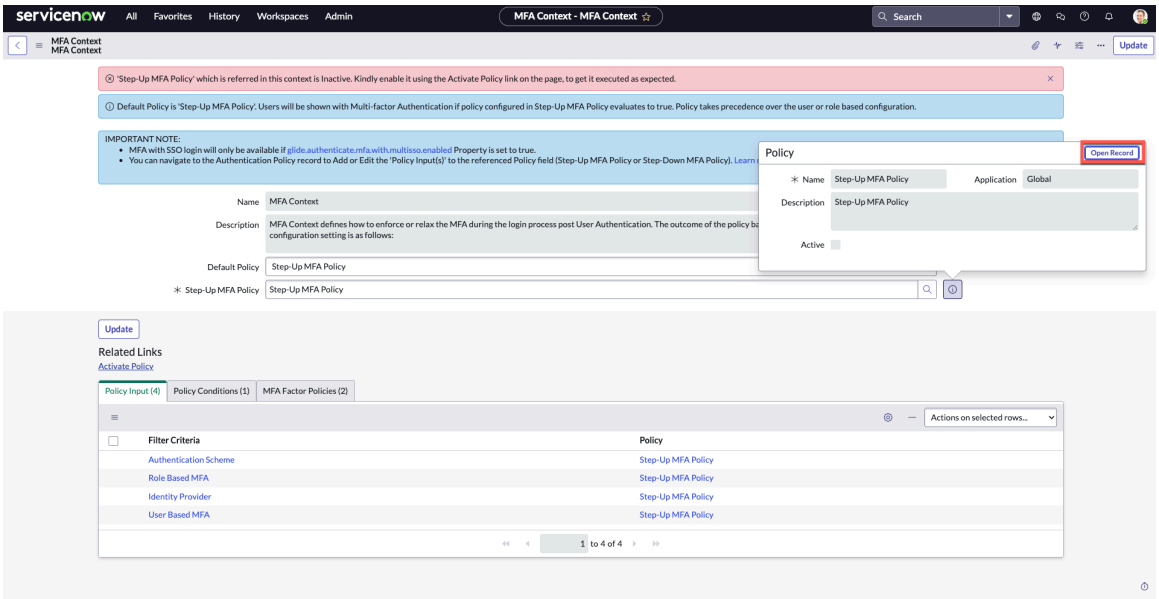
c. Accédez à la **Tous** > **Authentification Adaptative** > **Contexte MFA**.

d. Assurez-vous que ces champs sont définis comme suit :

- Le champ Politique par défaut est **Politique MFA ascendante**
- La politique MFA ascendante est **une politique MFA ascendante**

e. Sélectionnez l'icône Information et **ouvrez l'enregistrement**.

Traduction automatique



f. Dans le formulaire Politique MFA ascendante, dans les entrées de politique, sélectionnez **Modifier**.

g. **Ajoutez l'authentification multifacteur basée sur les rôles** à la liste et **enregistrez**.
Dans cet exemple, **remoteworkerrole**.

h. Dans la condition de stratégie, sélectionnez **Appliquer la MFA si les paramètres MFA basés sur le rôle ou l'utilisateur sont vrais**.

i. Sur la page Appliquer la MFA si les paramètres MFA basés sur le rôle ou l'utilisateur sont vrais, assurez-vous que **MFA basé sur les rôles** est **défini sur true**.

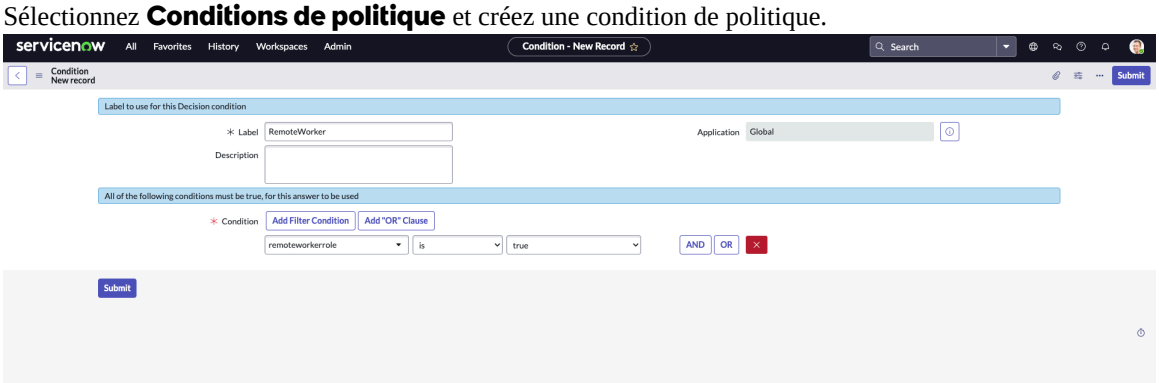
5. Forcez la MFA pour utiliser SMS comme politique de facteur MFA.

a. Accédez à la **Tous** > **Authentification Adaptative** > **Contexte MFA**.

b. Sur la page Contexte MFA, sélectionnez **Politiques de facteur MFA** , puis sélectionnez une politique **Afficher SMS OTP en tant que politique de facteur MFA**.

c. Sélectionnez **Modifier** et ajouter **remoteworkerrole** dans les **entrées de politique**.

d. Sélectionnez **Conditions de politique** et créez une condition de politique.



Traduction automatique

e. Sélectionnez **Envoyer**.

Le lien TLA généré et partagé avec les utilisateurs affectés avec **remoteworkerrole** en tant que rôle est promu pour utiliser le code SMS comme deuxième facteur de connexion dans l'instance.

6. Activez les 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. Générer un lien TLA – Exemple.

a. Accédez à la **Tous** > **Définition du système** > **Scripts – Arrière-plan**.

b. Utilisez l'API suivante en fournissant l'sys_id d'utilisateur et l'ID de configuration.
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 ci-dessous :
nonce=VCeinfboDt0M&glide_sso_id=b3277f1b44351110f8779b5a2d9909f3&user=3b0277d3443511

d. Créez une URL au format suivant :
https://<instance-url> /login_with_sso.do ?uri=<url codée>&
nonce=2olIQSxdgkjs&glide_sso_id=0c15bf09c3711110c5ec4e483c40dd7a&user=62826bf03710200

8. Sélectionnez l'URL, et 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

Apprenez à configurer l'authentification par jeton Digest.

Exploration de l'authentification par jeton Digest

L'instance lit la valeur de l'en-tête HTTP et compare sa valeur de hachage calculée du jeton Digest. 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 a été pré-authentifié et se connecte.

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 les liens d'expiration basés sur le temps. Pour en savoir plus, reportez-vous à Authentification temporelle limitée.

Conditions d'intégration

Une intégration de l'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 des formats suivants
  - En-tête 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)

Configuration des propriétés Digest pour l'authentification unique (SSO) de plusieurs fournisseurs

Après l'activation d'un script d'installation Digest, configurez les propriétés pour 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 (SSO) 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. Renseignez les champs du formulaire Propriétés de synthèse.

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 le jeton condensé que vous avez créé. Par exemple, SM_USER.
Phrase de sécurité secrète	Entrez la clé secrète à utiliser pour coder les clés de synthèse. Par exemple, 32 caractères ou plus.
Champ de redirection SSO échoué	Entrez l'URL vers laquelle rediriger les utilisateurs après un échec d'authentification.
Redirection de déconnexion externe	Entrez l'URL de redirection des utilisateurs après une déconnexion.
Script d'authentification unique	Sélectionnez **MultiSSO_DigestedToken**.

3. Cliquez sur **Mettre à jour**.
4. Définissez votre jeton de synthèse 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 associé à l'authentification unique (SSO) de plusieurs fournisseurs est activé, seuls les enregistrements associés à l'authentification unique (SSO) de plusieurs fournisseurs sont utilisés.

   Les enregistrements de jetons Digest qui existent dans la table des propriétés Digest peuvent être appelés individuellement en ajoutant l'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=<digest

Exemple d'implémentations de jetons de synthèse

Voici plusieurs exemples de création d'un jeton de synthèse.

Exemple d'implémentations d'authentification Digest

Digest créé avec	Valeur de 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 Java Digest pour le chiffrement

Cet algorithme Java illustre la création d'un jeton de synthèse à partir d'un en-tête HTTP.

Cet exemple suppose que :

- 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 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)));
    }
}
```

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 digest.

Cet exemple suppose que :

- 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 :

            b64SHA1Message  = "Unknown Encryption Method" ; break ;

        }


      TextBoxBase64. Text = b64SHA1Message ; return b64SHA1Message ;

    }
```

Accès zéro confiance

Zero Trust Unccess (ZTA) est un modèle de sécurité qui suppose qu'aucun utilisateur ou appareil n'est approuvé par défaut.

Explorer

Découvrez les fonctionnalités et la valeur commerciale de l'accès Zero Trust.

Activer

Découvrez comment activer l'accès Zero Trust.

Traduction automatique

Configurer

Configurez l’accès Zero Trust.

Référence – Propriétés

Renseignez-vous sur les propriétés de l’accès Zero Trust.

Traduction automatique

Exploration de 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.

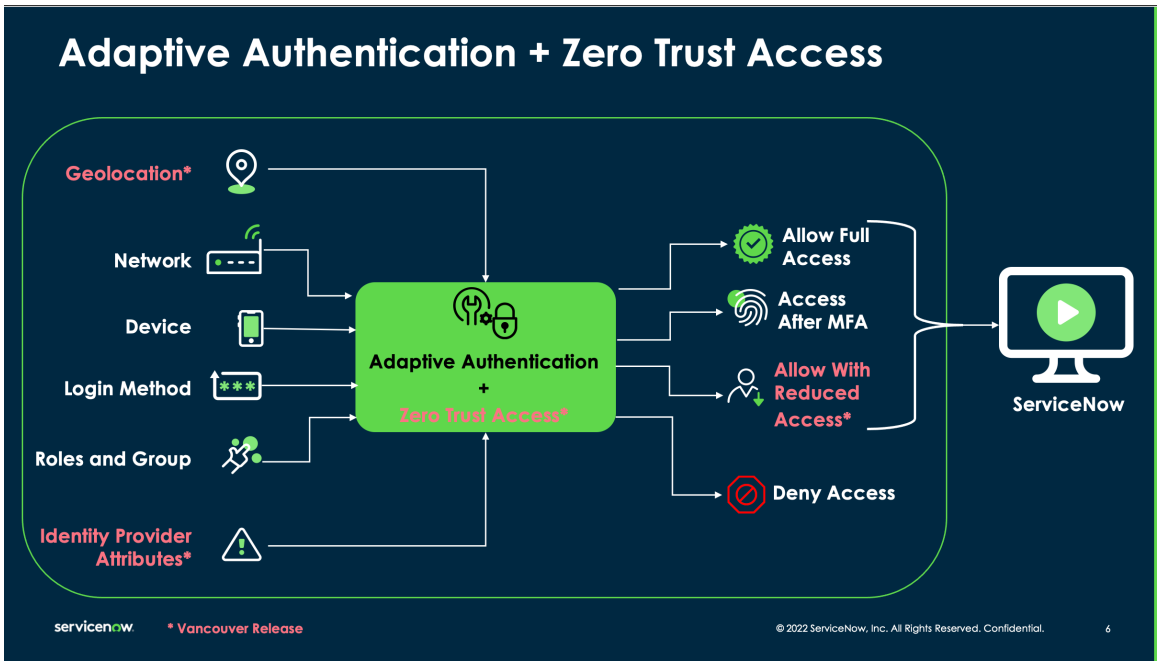
ZTA garantit que tous les accès aux applications et aux données sont accordés sur la base du moindre privilège, uniquement après vérification de l’identité de l’utilisateur et évaluation des risques.

Zero Trust - Accès à la session basé sur une politique

ServiceNow® Zero Trust - Policy Based Session Access (Session Access) permet aux organisations de réduire dynamiquement les privilèges des utilisateurs 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 authentification multifacteur 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 des utilisateurs hautement privilégiés accèdent aux applications à partir d’appareils ou d’emplacements non approuvés.

Zero Trust - Accès à la session basé sur une politique

Il permet aux administrateurs de sécurité de réduire ou de limiter l’accès des utilisateurs à 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 adaptatives.



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 apporté 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 prenne effet.
- L'accès à la session n'a aucun impact lorsque l'utilisateur se trouve dans un réseau approuvé et qu'il passe ultérieurement 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. Toute modification des paramètres de risque au cours de la session n'entraîne pas une réduction de l'accès. Par exemple, un utilisateur qui passe d'un réseau d'entreprise à un réseau non approuvé après avoir établi la session n'entraîne pas de réduction d'accès, sauf s'il se déconnecte et se reconnecte.

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 au rôle de prestataire qui se connecte en dehors du réseau approuvé peut être configuré pour avoir uniquement 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 IdP 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 approuvé, tous les privilèges existants sont affectés pour une session.

Plusieurs conditions IP et plusieurs affectations de rôles ou de groupes peuvent être définies dans le cadre de la politique.

Accès Zero Trust - Mobile

Vous pouvez utiliser la stratégie Accès zéro confiance - Accès à la session dans la stratégie d'authentification adaptative pour réduire les rôles ou privilèges de la session spécifique dans l'application Mobile.

Accès Zero Trust - Accès à la session Mobile peut être activé en activant le **glide.authenticate.session_access.mobile.enabled** à partir de la table des propriétés système.

Pour utiliser Zero Trust Access - 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 .

Activer l'accès Zero Trust

Activez la politique de com.snc.zero_trust_session_access**Zero Trust - Accès à la session basé sur une politique** pour permettre aux administrateurs de sécurité de réduire ou de limiter l'accès des utilisateurs à 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

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Trouvez 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. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

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>.

Configuration du rôle d'accès à la session

Configurez l'accès à la session pour réduire l'accès de l'utilisateur 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

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 apporté à la session connectée. L'utilisateur continuera d'accéder à l'instance avec les privilèges qui lui ont été 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 prenne effet.
- L'accès à la session est appliqué au moment de la connexion. Toute modification des paramètres de risque au cours de la session n'entraîne pas une réduction de l'accès. Par exemple, un utilisateur qui passe d'un réseau d'entreprise à un réseau non approuvé après avoir établi la session n'entraîne pas de réduction d'accès, sauf s'il se déconnecte et se reconnecte.

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

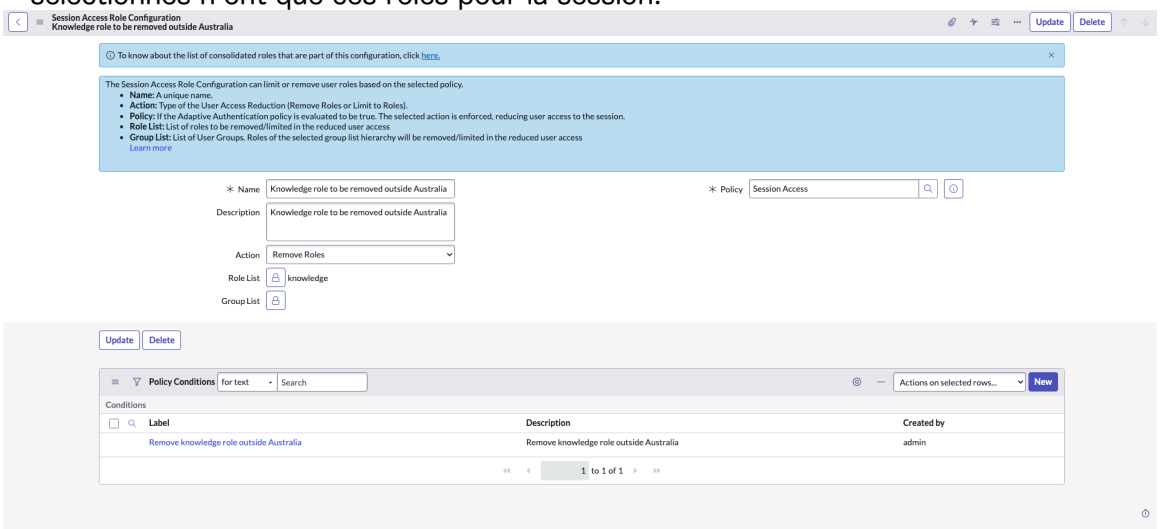
Champ	Description
Nom	Nom de la configuration
Description	Brève description de la configuration.
Politique	Choisissez la politique d'authentification adaptative. Utilisez l'icône de recherche pour afficher la liste des politiques.
Action	**Supprimez les rôles** ou **limitez-les aux rôles**. ○ **Supprimer les rôles** : lorsque l'utilisateur configuré se connecte, la liste des rôles fournis 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 sélectionnés sont fournis à l'utilisateur et tous les autres rôles sont supprimés pour la session.

Champ	Description
Liste de rôles	Choisissez des rôles dans la liste des rôles.
Liste de groupes	Choisissez dans la liste de groupes les rôles que vous souhaitez supprimer ou limiter à l'utilisateur.

4. Sélectionner, **soumettre**.

   La connexion des utilisateurs en fonction des pays configurés est la suivante :

   - Dans **Supprimer les rôles**, les utilisateurs des pays configurés disposant des rôles sélectionnés ne disposent plus de ces rôles pour la session.
   - Dans **Limiter aux rôles**, les utilisateurs des pays configurés disposant des rôles sélectionnés n'ont que ces rôles pour la session.

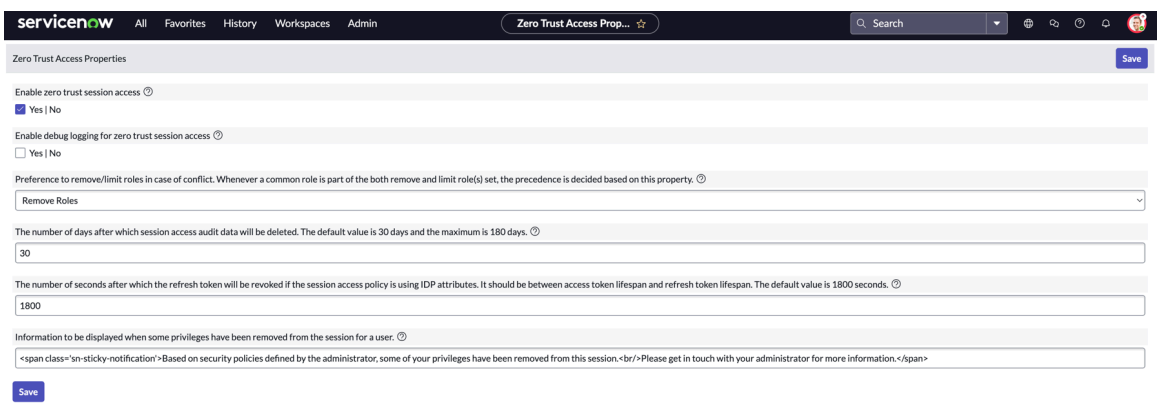


   Pour en savoir plus sur la suppression ou la limitation des rôles pour une session expliquée à l'aide d'un exemple de cas d'utilisation, consultez Utiliser l'accès zéro confiance.

Propriétés système d'accès Zero Trust

Utilisez les propriétés système pour activer et personnaliser l'accès Zero Trust afin de répondre à vos exigences de sécurité.

Propriétés



Propriétés système d'accès Zero Trust

Propriété	Description
Activer l'accès à la session Zero Trust	Option qui permet aux administrateurs d'utiliser la fonctionnalité d'accès à la session Zero Trust. Par défaut, la valeur est `false`.
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. Chaque fois qu'un rôle commun fait partie d'un ou de plusieurs rôles de suppression et de limite définis, la priorité est définie en fonction de cette propriété.	**Supprimer des 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 est 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 s'agit de 1 800 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 des privilèges. Description de l'échantillon : `Certains de vos rôles ont été supprimés de cette session en fonction des politiques de sécurité définies par l'administrateur. Veuillez contacter votre administrateur pour plus d'informations.`

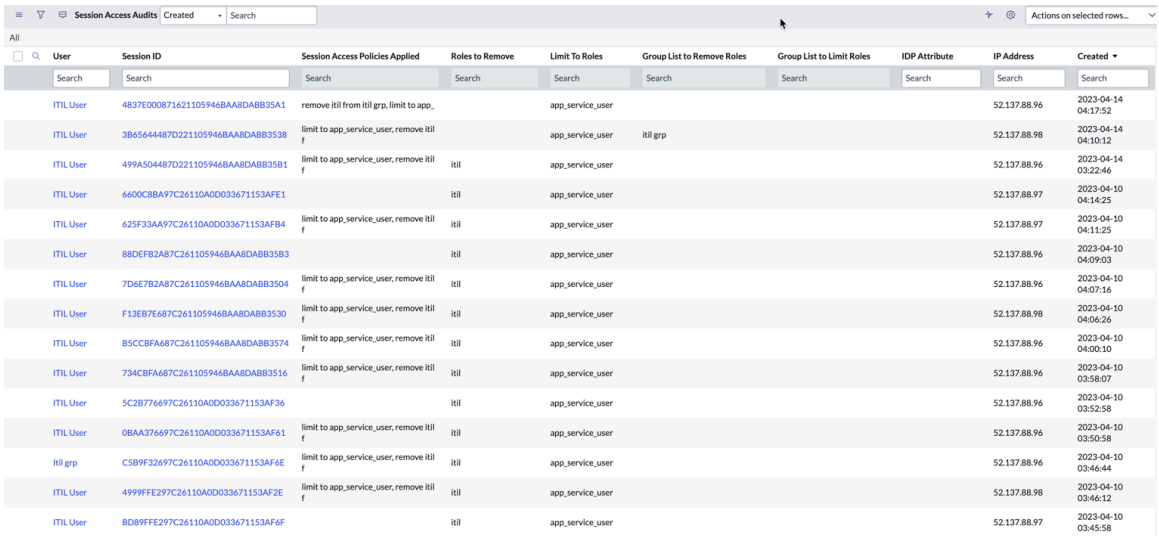
Audits d'accès à la session

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.

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 de l'audit.



Audits d'accès à la session

Champ	Description
Utilisateur	Détails de l'utilisateur.
ID de session	Détails sur la session affichés en tant qu'ID unique.
Client mobile	Les détails du client mobile. **ServiceNow Agent** (Now Agent) et **ServiceNow Request** (Now Mobile).
Politiques d'accès à la session appliquées	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 étaient limités à l'utilisateur lors de la connexion.
Liste de groupes pour supprimer les rôles	Informations sur le groupe qui a supprimé des rôles pour l'utilisateur.
Liste de groupes pour limiter les rôles	Informations sur le groupe dont les rôles de l'utilisateur sont limités.
Client mobile	Détails de l'utilisateur connecté via un équipement 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.
Créé	Détails de la date et de l'heure de l'enregistrement utilisateur créé.

Utiliser l'accès zéro confiance

Utilisez la fonctionnalité d'accès Zero Trust 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 apporté à la session connectée. L'utilisateur continuera d'accéder à l'instance avec les privilèges qui lui ont été 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 prenne effet.
- L'accès à la session est appliqué au moment de la connexion. Toute modification des paramètres de risque au cours de la session n'entraîne pas une réduction de l'accès. Par exemple, un utilisateur qui passe d'un réseau d'entreprise à un réseau non approuvé après avoir établi la session n'entraîne pas de réduction d'accès, sauf s'il se déconnecte et se reconnecte.

L'accès à la session est une fonctionnalité qui permet aux administrateurs de réduire ou de restreindre dynamiquement un ensemble de rôles accordés à l'utilisateur, lorsque celui-ci tente de se connecter à l'instance à partir de différents environnements, par exemple une connexion à partir d'un réseau non approuvé, une connexion à partir d'un autre appareil, 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 true et que l'action des rôles est définie sur **Supprimer les rôles**, 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 true et que l'action des rôles est définie sur **Limiter aux rôles**, seuls les rôles sélectionnés et leurs rôles enfants associés sont affectés à l'utilisateur lors de la tentative de connexion à l'instance.

La procédure suivante décrit une configuration de bout en bout de la configuration de l'accès à la session en fonction de laquelle le rôle est limité à l'utilisateur qui se connecte à 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 Configurations des rôles d'accès à la session, sélectionnez **Nouveau**.
3. Pour limiter un rôle de l'utilisateur, renseignez les champs suivants du formulaire :
   - Nom
   - Description
   - Politique
   - Action
   - Liste de rôles
   - Liste de groupes

a. Choisissez **Limit To Roles (Limiter aux rôles**) pour limiter les rôles de l'utilisateur. Par exemple, **itil**.

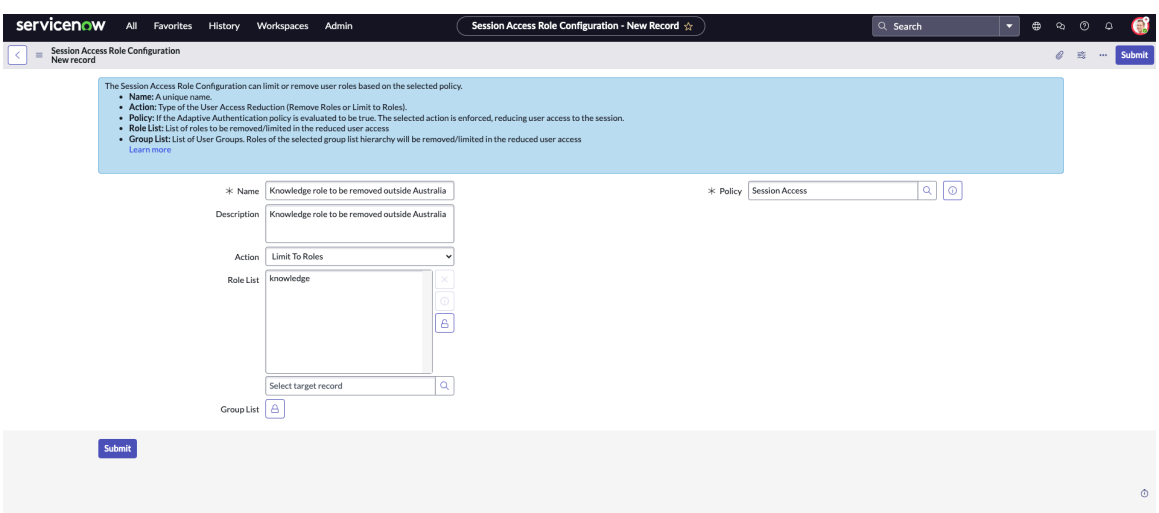
b. Choisissez **un rôle de connaissances** dans la liste des rôles.

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 **Limiter aux rôles**.
Si la politique est définie sur true, seuls les rôles sélectionnés et leurs rôles enfants associés sont disponibles pour l'utilisateur lorsqu'il essaie de se connecter à l'instance.

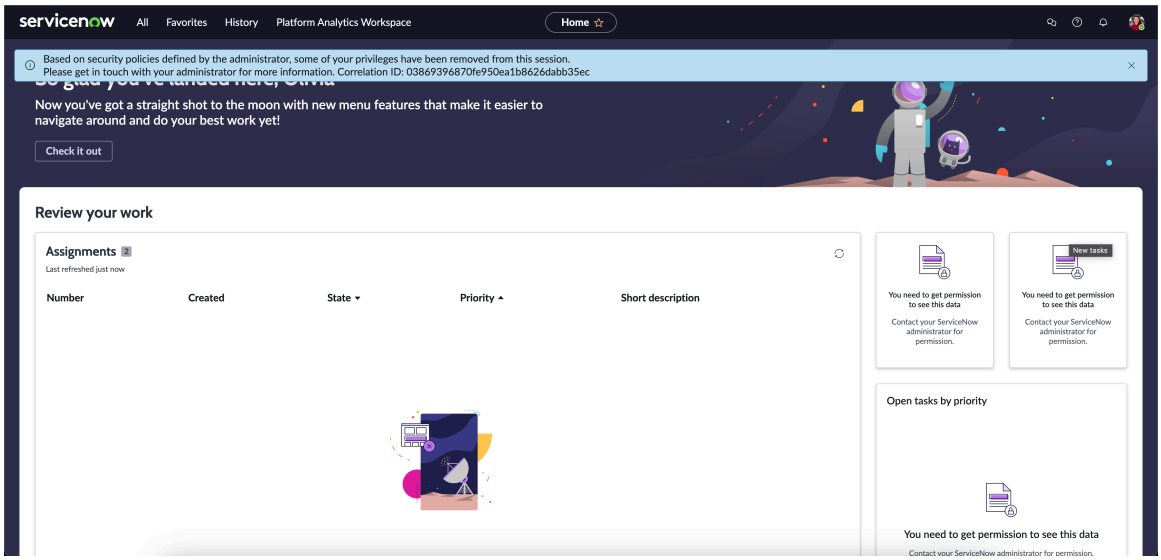


e. Sélectionnez **Envoyer**.

De même, vous pouvez choisir le groupe dans la liste de 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, seuls le rôle **Knowledge** et ses rôles enfants associés sont affectés pour la session journalisée et les autres rôles de l'utilisateur sont restreints.

Une fois 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 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 IdP pour l'accès à la session

Utilisez l'attribut de fournisseur d'identité (IDP) créé à partir de la réponse SAML (Security Assertion Markup Language) pour supprimer ou restreindre l'accès à la session de l'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 Accès à la session, vous devez élever votre rôle au rang de 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 :

- Si la politique a la valeur true et que l'action des rôles est définie sur **Supprimer les rôles** avec l'entrée et la condition de l'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 a la valeur true 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 leurs 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 d'une entrée de politique de réponse SAML 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 Configurations des rôles d'accès à la session, sélectionnez **Nouveau**.

3. Pour supprimer n'importe quel 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**.

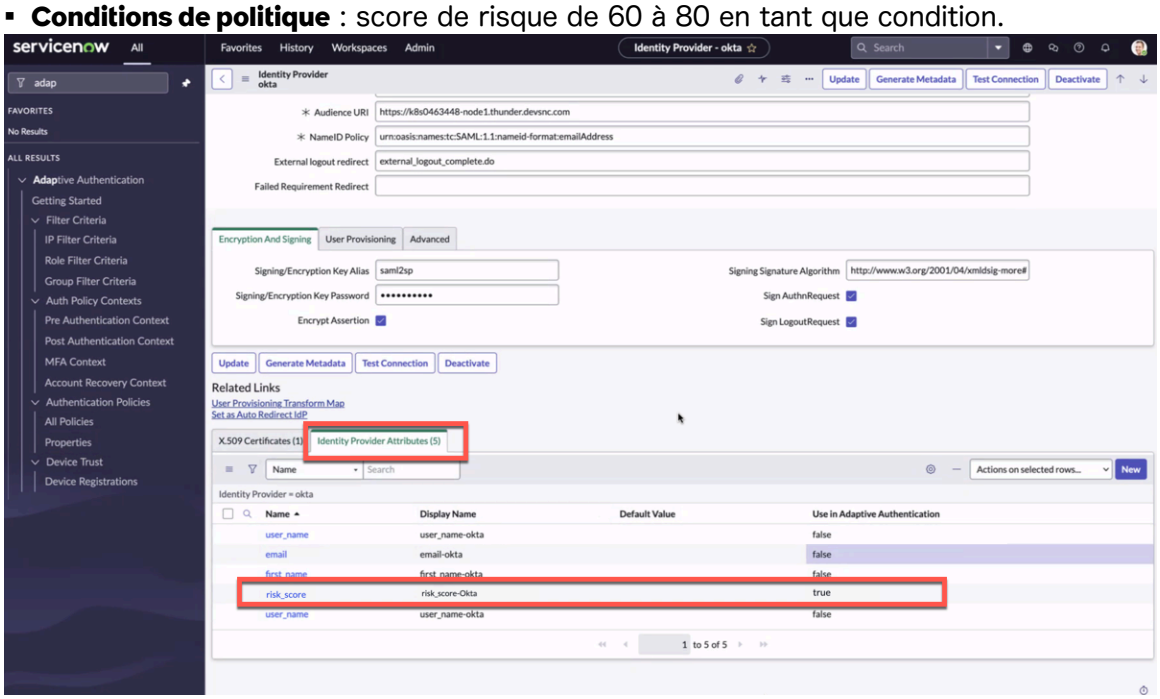
b. Choisissez le rôle **ITIL** dans la liste des rôles.

c. Choisissez la **politique**.
Pour en savoir plus sur la création de politiques à l'aide de différents critères de filtre à l'aide de la création de stratégies d'authentification adaptative, reportez-vous à Critère de filtre.

d. Choisissez Action as Remove roles (Supprimer les rôles).
Si la politique est définie sur true et que l'action des 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 et la condition de politique.
Par exemple :

- **Entrée Politique** : attribut de score de risque d'Okta (IDP).
- **Conditions de politique** : score de risque de 60 à 80 en tant que condition.



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 à l'instance, l'utilisateur est uniquement authentifié avec

les 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 stratégie de contexte de post-authentification avec les entrées et la condition de stratégie, reportez-vous à la section Contexte postérieur à l'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 **Envoyer**.

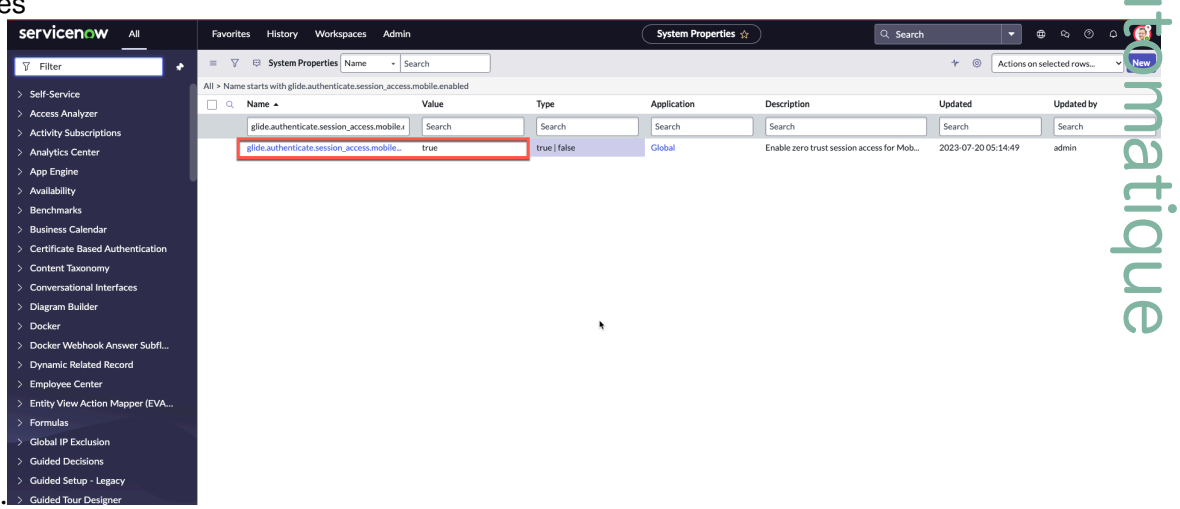
Accès zéro confiance pour mobile

L'accès zéro confiance (ZTA) est un modèle de sécurité qui suppose qu'aucun utilisateur ou appareil n'est approuvé par défaut.

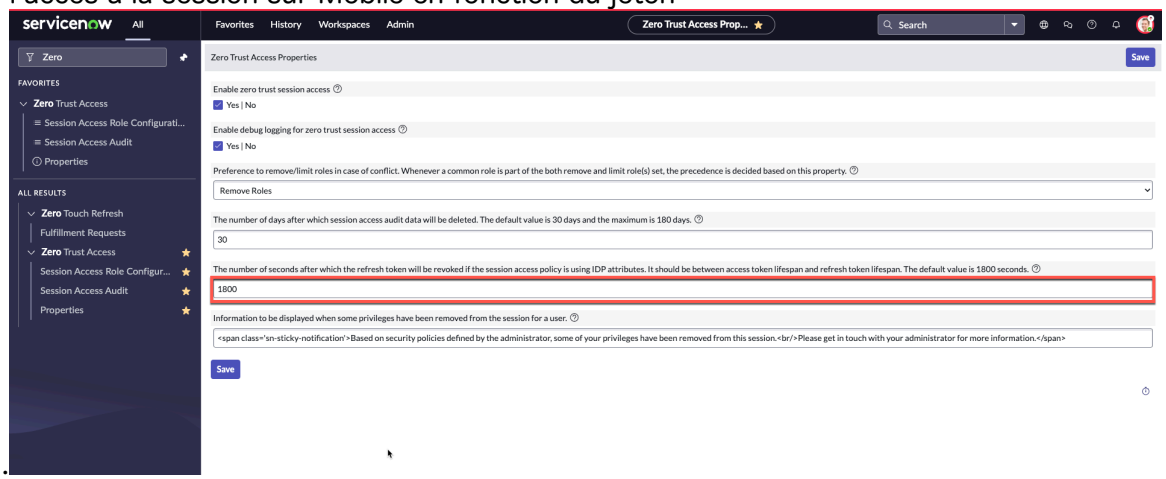
Vous pouvez utiliser la politique Accès zéro confiance - Accès à la session dans la stratégie d'authentification adaptative pour réduire les rôles ou privilèges de la session particulière dans Mobile pour les utilisateurs.

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 d'accès à la **session Zero Trust - Basé sur une politique**.
- Activez le **glide.authenticate.session_access.mobile.enabled** à partir de la table des propriétés système.

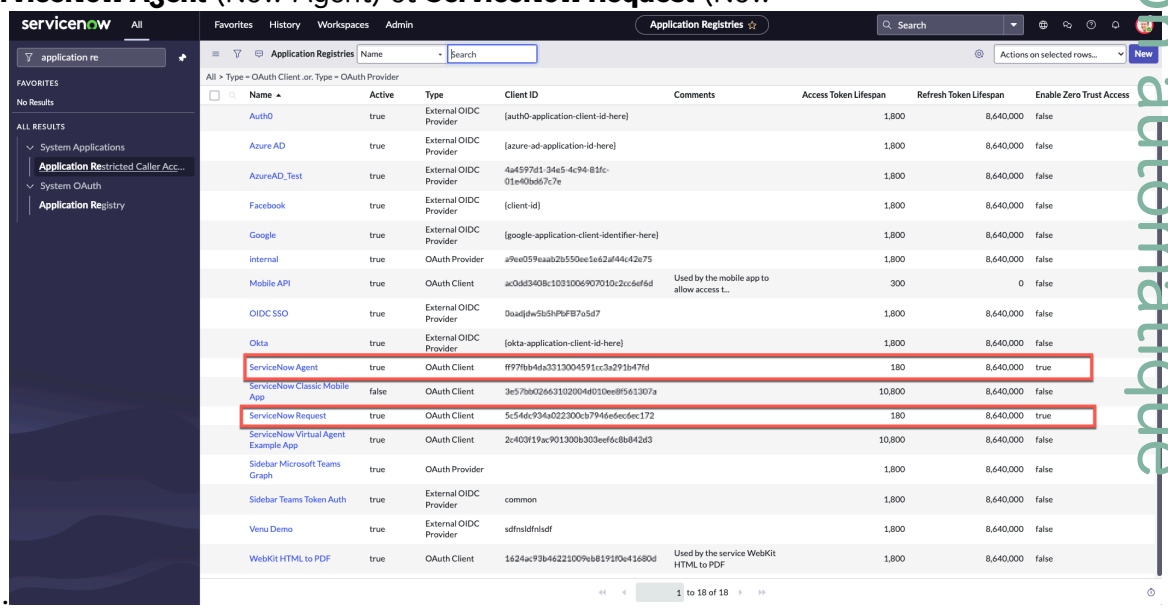


- Configurez le champ **glide.authenticate.session_access.mobile.refresh_token_interval** pour contrôler l'accès à la session sur Mobile en fonction du jeton d'actualisation.



Remarque :
Vous devez configurer les secondes de 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 Mobile après 1 800 secondes (30 minutes).

- L'option Activer l'accès zéro confiance est activée sous **Registres d'application** pour l'application client mobile (client OAuth). Dans ce cas, **ServiceNow Agent** (Now Agent) et **ServiceNow Request** (Now Mobile).



- Configurez le rôle d'accès à la session pour réduire ou supprimer des rôles pour la journalisation des utilisateurs en fonction des entrées et des conditions de la politique. Pour en savoir plus sur la configuration, reportez-vous à 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 des conditions de politique. Pour plus d'informations, consultez Configure Zero Trust Access for mobile .

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 Détection, Mappage des services et Gestion dans le 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 généré.

Explorer	Configurer
	
En savoir plus sur les informations d'identification.	Configurez les informations d'identification.

Traduction automatique

Référence

Obtenez des détails sur les informations d’identification.

Dépannage

Découvrez comment résoudre les problèmes de connexion et d’informations d’identification.

Explorer les informations d’identification, les connexions et les alias

Toutes les intégrations d’applications utilisent des connexions, des informations d’identification Now Platformet des alias pour permettre aux applications d’accéder aux ressources.

Avant de pouvoir exécuter une intégration d’application dans , vous devez créer et configurer les informations de connexion, les informations d’identification Now Platformcorrespondantes et ajouter un alias. Pour comprendre comment ServiceNow définit ces termes :

Connexion

Une *connexion* est une intégration à un système, tel qu’une adresse IP ou un point de terminaison avec des protocoles. Elle contient des détails spécifiques, tels que les détails de la base de données, lors de l’intégration à une base de données.

Informations d'identification

Les *informations d’identification* sont les données d’authentification nécessaires pour établir la connexion, telles qu’un ID et un mot de passe.

Alias

Un *alias* est une convention d’affectation de noms, ou balise, liée 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 d’entrer ces informations à chaque intégration, vous pouvez utiliser un alias. Par exemple, vous pouvez désigner un alias pour héberger vos informations d’identification d’assurance qualité, de développement et de production pour la même intégration d’application. L’alias résout l’intégration de l’application pour chaque environnement.

On Now Platform distingue différents types d’alias :

Alias d'informations d'identification

Cet alias s’associe uniquement aux données d’identification et se résout pendant l’exécution.

Alias de connexion et d'informations d'identification

Cet alias s’associe aux informations de connexion et aux données d’identification requises pour effectuer 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 de la 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 transportent leurs propres informations de connexion et d’informations 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 d’un service externe
- Définir une fois et réutiliser pour plusieurs fonctionnalités de la plateforme
- Réduire la configuration des autres fonctionnalités de la plateforme
- 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 dans le cloud
- Détection
- Orchestration
- Mappage des services

Vous pouvez configurer des alias sur le Now Platform de l’une des deux façons suivantes :

- Utilisation 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 Hub d'intégration. Reportez-vous à la section Ajouter une connexion .

Remarque :
Hub d'intégration nécessite un abonnement distinct. Pour plus d'informations, consultez Demande Hub d'intégration .

Synchronisation des informations d'identification sur les MID Servers

Chaque *MID Server*de votre réseau synchronisé avec l'instance conserve une copie de toutes les informations d'identification que vous créez. Management, Instrumentation, and Discovery (MID) Server est une application Java qui permet la communication et le mouvement des 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 Détection ou Mappage des services ont besoin d'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 MID Server d'effectuer un appel SOAP à 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 en savoir plus, consultez Serveur MID .

La réponse SOAP que votre instance envoie à chaque MID Server inclut également les 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 MID Servers. Pour contrôler cela, ajoutez manuellement ces propriétés à la table Propriétés système [sys_properties] :

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 personnalisé des formulaires d'informations d'identification qui incluent des champs de référence pour des tables qui ont également des champs de référence.

Propriété	Description
	• **Type** : nombre entier • **Valeur par défaut** : 3

Protections du périmètre 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 Discovery [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 Washington DC, mais vous pouvez facilement l'y ajouter. Pour en savoir plus sur ces types d'enregistrement et sur l'ajout du champ à leurs formulaires d'interface utilisateur, consultez :

- Mise en route des connexions
- Introduction aux informations d'identification
- Alias d'informations d'identification pour la détection
- 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 incluent ou HR Service DeliverySecurity Operations Les enregistrements Connexion et 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 Connexion et informations d'identification à un périmètre d'application spécifique offre les protections suivantes :

- Applique les règles des listes de contrôle d'accès (ACL) aux champs d'application restreints. Pour en savoir plus sur les ACL incluses dans le champ d'application, consultez Règles relatives aux listes de contrôle d'accès.

  Remarque :
  Certaines applications utilisant l'administration du périmètre et la sécurité appliquée peuvent nécessiter une configuration supplémentaire. Pour en savoir plus, consultez 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 s'il y est autorisé.

Vous pouvez personnaliser et accorder l'accès aux enregistrements restreints aux requêtes à l'aide de l'accès restreint pour l'appelant. Pour en savoir plus, reportez-vous à la section 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 Discovery [discovery_credentials]. Les champs vides et 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 le périmètre de son application incluse dans le périmètre, il n'y a pas de restriction automatique du périmètre.

Domain Separation et Informations d'identification et connexions

Domain Separation est pris 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 la prise en charge de niveau **Basique**.
- 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.

Vue d'ensemble

Les informations d'identification sont liées à diverses ServiceNow fonctionnalités qui accèdent aux 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 dans lequel exécuter une activité.

Fonctionnement de Domain separation dans Informations d'identification et connexions

Les informations d'identification accèdent aux ressources en dehors de l'instance et sont utilisées par les services Discovery , Orchestration , Mappage des services , et Cloud Provisioning and Governance Applications. Ces informations d'identification ne sont pas liées à un domaine spécifique, elles peuvent plutôt être liées à une application, puis suivre la séparation de domaine que l'application utilise. Les informations d'identification peuvent également être affectées à un MID Server , 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 d'action ou un développeur peut utiliser un modèle de configuration pour configurer le spoke au même endroit, et le système crée les enregistrements associés.

Avantages

Les modèles de configuration permettent :

- Administrateurs ou concepteurs de flux pour configurer des intégrations complexes à l'aide d'un formulaire unique.
- Les développeurs définissent des valeurs statiques dans une intégration, simplifiant ainsi 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 les types d'informations d'identification suivants :

- Authentification de base
- Clé API
- Type d'attribution titulaire OAuth JWT
- Type d'accord du code d'autorisation OAuth
- Authentification personnalisée

Composants du modèle 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 dans 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.

Données de démonstration

La table Modèles de connexion et d'informations d'identification [sys_alias_templates] comprend des exemples de modèles permettant de configurer des modèles pour les types d'authentification courants. Utilisez ces exemples comme guide lorsque vous créez les vôtres.

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 du modèle de données par défaut crée un enregistrement associé. Le modèle comprend les sections suivantes :

- `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 faut faire de ces enregistrements.

L'exemple suivant crée les enregistrements requis pour l'authentification du 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,
     "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>"
}
}
```


Traduction automatique

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",
    "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"
  },
  {
    "name": "credential.jwt_provider.jwt_keystore_aliases.signing_keystore",
    "label": "Key Store",
    "type": "file"
  }
 ]
}
```

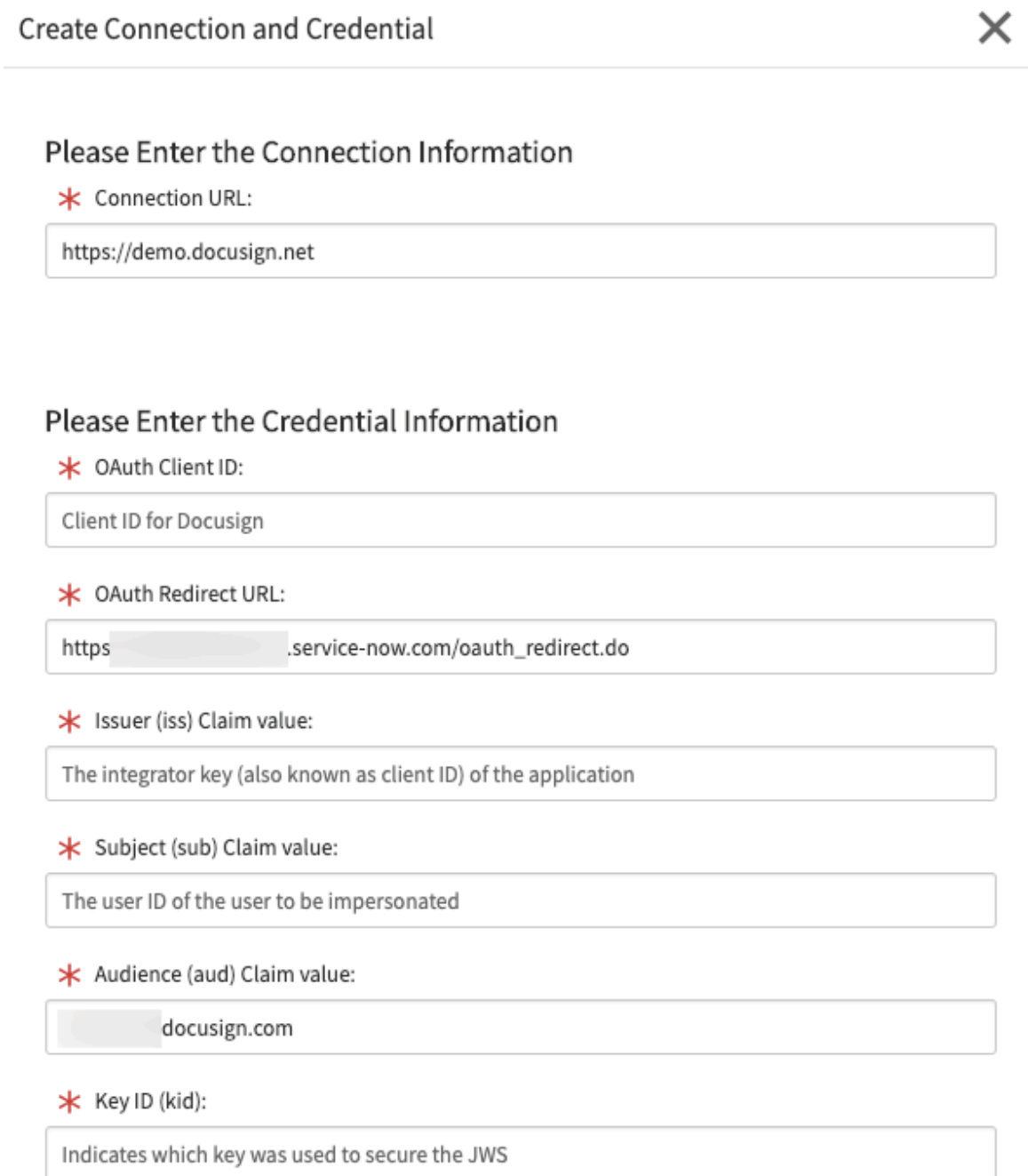
Script de post-traitement

Le script de post-traitement suivant mappe les entrées 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 Configuration de la connexion et des informations d'identification DocuSign qui en résulte

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

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 les valeurs qui s'appliquent à chaque intégration. Définissez des paires clé-valeur dynamiques pour recueillir les entrées de l'utilisateur et définissez 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 : concepteur d'action ou admin

Procédure

1. Accédez à la **Tous** > **Centre d'intégration** > **Connexions et informations d'identification** > **Modèles de configuration**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez le type de modèle de configuration que vous souhaitez créer.
   La sélection d'un type fournit des données de démarrage pour vous aider à configurer le modèle.
4. Dans le champ **Nom** , ajoutez un nom pour identifier le modèle.
5. Dans le champ **Modèle de données par défaut** , apportez les modifications nécessaires.
   Ce champ 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.

   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 les données d'une table personnalisée et utiliser le script de post-traitement pour insérer les données dans la table.

Remarque :
Dans le modèle de données par défaut pour le type d'attribution de code d'autorisation OAuth, les valeurs des clés de `oauth_entity_profile_scope` et de `oauth_entity_scope` doivent correspondre. Dans l'exemple suivant, les deux clés ont la valeur `Lire l'e-mail de l'utilisateur` .

```
"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 dynamiques** , apportez les modifications requises.
   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 les propriétés suivantes :

   - `name` : champ auquel l'entrée de l'utilisateur est mappée. Par exemple, pour mapper l'entrée utilisateur au champ URL de connexion dans l'enregistrement de connexion, saisissez `connection.connection_url`.
   - `étiquette` : l'étiquette de champ que l'utilisateur voit lorsqu'il remplit le modèle.
   - `type` : type de champ. Assurez-vous que ce type de données correspond au type de données du champ auquel vous mappez la valeur.
   - `defaultValue` : facultatif. Valeur par défaut du champ. Si aucune valeur par défaut n'est fournie, l'astuce s'affiche.
   - `Astuce` : Facultatif. Texte de conseil à afficher en l'absence de valeur par défaut.

Remarque :
Si vous configurez un modèle pour l'authentification de type d'attribution titulaire OAuth JWT, vous souhaiterez peut-être saisir une entrée utilisateur pour une paire clé-valeur unique dans le tableau `jwt_claim_validation` . Vous pouvez faire référence à une paire clé-valeur unique 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 (ID de connexion)	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 issu du champ **Modèle de données dynamiques** au format Chaîne.

8. Dans le champ **Script de pré-édition** , ajoutez un script pour pré-remplir les champs supplémentaires lorsque vous modifiez une connexion.

Ce script renvoie un tableau d'objets. Chaque objet dispose d'une paire nom-valeur pour remplir 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 (ID de connexion)	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 issu du champ **Modèle de données dynamiques** au format Chaîne.

Chaque objet du script possède les propriétés suivantes :

- `name` : nom du champ personnalisé pour spécifier la valeur dans la connexion.
- `Valeur` : valeur que vous souhaitez mapper afin de 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 Faux.
Numéro	Valeur numérique.
Date	Valeur de date au format aaaa-mm-jj. Vous pouvez également utiliser l'objet GlideDate.
Choix	Liste des choix valides définis dans le champ **Schéma de données dynamiques**.
Référence	GlideRecord valide.
Groupe de cases d'option	Groupes contenant un ensemble de champs différent. Ces groupes sont disponibles en tant que choix 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, considérons la structure suivante du groupe de cases d'option définie dans le champ **Schéma de données dynamiques** : `{ "name": "radio_groups", "label": "Radio Groups", "type": "radio",`

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, reportez-vous à la rubrique Remontée pas à pas .

Conseil :
Si les valeurs pré-remplies 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. Ajoutez le modèle à un alias de connexion et d'informations d'identification.
   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 recueillir ses informations. Si vous avez créé un modèle pour le type d'attribution 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 et en sélectionnant **Créer une nouvelle connexion et des 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 des connexions pour configurer une connexion de base, JMS, JDBC ou HTTP(s) à un hôte cible.

Table de connexion

La table 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 des alias de connexion, qui couple l'alias de connexion aux informations de connexion. Chaque connexion enregistre les informations suivantes :

Propriétés de 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 lors de l'exécution. Une seule connexion est active par alias de connexion à la fois.
Actif	Cochez cette case pour activer la connexion actuelle.
Domaine	Domaine auquel appartient la connexion.

Les informations d'identification sont uniques parmi les connexions actives, si elles ne sont pas vides.

Mise à niveau des informations de connexion

- Les tables Connexion JDBC [jdbc_connection] et Connexion JMS [orch_jms_ds] sont des tables de connexion Orchestration existantes qui s'étendent maintenant à partir de la table Connexion [sys_connection]. À l'origine, les tables s'étendaient de sys_metadata. Les données associées sys_metadata sont supprimées.
- Les tables passent du module d'extension d'exécution Orchestration [com.snc.runbook_automation.runtime] au module d'extension Credentials & Connections.
- Le processus de mise à niveau obtient les informations de connexion JDBC et JMS et crée les alias de connexion correspondants et affecte l'alias à sa connexion correspondante.
- Le nom du champ JDBC change :
  - 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. Complétez 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 sur lequel 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. Flow Designer ne prend pas en charge Domain Separation et ignore ce champ.
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.

Champ	Description
Utiliser Serveur MID	Sélectionnez cette option pour vous connecter à l'hôte cible via un Serveur MIDfichier . Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée du MID Server. **Remarque :** PowerShell nécessite un fichier Serveur MID.
Sélection de MID	Option permettant de sélectionner le MID Server ou la grappe MID spécifique. ○ **Sélectionner automatiquement un MID Server** : sélectionne automatiquement le MID Server. ○ **MID Server spécifique** : utilise le MID Server que vous sélectionnez. ○ **Grappe MID spécifique** : utilise la grappe MID que vous sélectionnez. Ce champ est disponible lorsque **l'option Utiliser un MID** Server est sélectionnée. **Remarque :** Assurez-vous que l'enregistrement de Hub 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 laquelle Serveur MID est sélectionnée lors de l'exécution. Pour en savoir plus sur la façon dont un est sélectionné pendant l'exécution, reportez-vous à la section Sélection d'un Serveur MID MID Server. 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 .
Serveur MID	Spécifique Serveur MID sur lequel l'étape s'exécute. Ce champ n'est visible que **lorsqu'un MID Server spécifique** est sélectionné dans la liste Sélection MID.
Grappe MID	Grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser un MID** Server est sélectionnée et **qu'une grappe MID spécifique** est sélectionnée dans la liste Sélection MID.

5. Cliquez sur **Envoyer**.

servicenow

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**, puis 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. Cette option n'est pas cochée par défaut. Si cette option est cochée, l'URL de connexion est calculée à partir des champs suivants : ◦ Authentification réciproque : case à cocher si l'authentification réciproque est utilisée. ◦ Protocole : si l'authentification réciproque n'est pas utilisée, entrez le protocole. La valeur par défaut est HTTPs. ◦ Profil de protocole : si l'authentification réciproque est utilisée, entrez le profil de protocole à partir de sys_protocol_profile. ◦ Hôte ◦ Port ◦ Chemin d'accès de base : chemin d'accès de la chaîne de connexion. **Remarque :** Si l'authentification réciproque est cochée, l'URL de connexion est créée : protocole + :// + hôte :port +URL. Si l'authentification réciproque n'est pas cochée, l'URL de connexion est créée : profil de protocole + :// + hôte :port +URL
URL de connexion	Si l'option Générateur d'URL n'est pas cochée, saisissez l'URL de connexion dans ce champ. **Remarque :** Si l'authentification réciproque est cochée, l'URL de connexion est créée : protocole + :// + hôte :port +URL. Si l'authentification réciproque n'est pas cochée, l'URL de connexion est créée : profil de 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.

Champ	Description
Utiliser Serveur MID	Cochez cette case pour utiliser un MID Server pour cette action ou cette activité. Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée du MID Server.
Sélection de MID	Option permettant de sélectionner le MID Server ou la grappe MID spécifique. ○ **Sélectionner automatiquement un MID Server** : sélectionne automatiquement le MID Server. ○ **MID Server spécifique** : utilise le MID Server que vous sélectionnez. ○ **Grappe MID spécifique** : utilise la grappe MID que vous sélectionnez. Ce champ est disponible lorsque **l'option Utiliser un MID** Server est sélectionnée. **Remarque :** Assurez-vous que l'enregistrement de Hub 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 laquelle Serveur MID est sélectionnée lors de l'exécution. Pour en savoir plus sur la façon dont un est sélectionné pendant l'exécution, reportez-vous à la section Sélection d'un Serveur MID MID Server. 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 .
Serveur MID	Spécifique Serveur MID sur lequel l'étape s'exécute. Ce champ n'est visible que **lorsqu'un MID Server spécifique** est sélectionné dans la liste Sélection MID.
Grappe MID	Grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser un MID** Server est sélectionnée et **qu'une grappe MID spécifique** est sélectionnée dans la liste 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.

3. Cliquez sur **Envoyer**.
   Vous êtes prêt à 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 qu'il s'agisse d'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, SQLServer 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

Pourquoi et quand exécuter cette tâche

Les informations d'identification JDBC sont récupérées séparément par le modèle de concepteur d'activité et prennent en charge le stockage des informations d'identification externe, tel 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 la base de données dans le champ **Format** détermine quels champs sont 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 d'expiration de requête	Tous	Temps maximal écoulé pendant lequel la requête JDBC est autorisée à s'exécuter sans réponse.
Délai de connexion	Tous	Nombre de secondes pendant lesquelles le système attend une connexion JDBC 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.
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. Les choix par défaut sont les suivants : ○ **MySQL** ○ **Oracle**

Champ	Format de base de données	Description
		○ **SQL Server** ○ **Aucun** Vous pouvez ajouter **Sybase** ou **DB2 Universal** à la liste de choix en chargeant le fichier JAR du pilote JDBC approprié dans 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	L'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 du SQL Server sélectionné
URL de connexion	Tous	URL que le MID Server 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 l'URL de connexion manuellement afin que le MID Server sache comment créer la connexion.
Pilote JDBC	Aucun, DB2 universel, 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 saisir le nom du pilote dans ce champ et charger le fichier JAR du pilote dans l'instance.
Utiliser un MID Server	Tous	Cochez cette case pour utiliser un MID Server pour cette action ou cette activité. Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée du MID Server.
Sélection de MID	Tous	Option permettant de sélectionner le MID Server ou la grappe MID spécifique.

Champ	Format de base de données	Description
		○ **Sélectionner automatiquement un MID Server** : sélectionne automatiquement le MID Server. ○ **MID Server spécifique** : utilise le MID Server que vous sélectionnez. ○ **Grappe MID spécifique** : utilise la grappe MID que vous sélectionnez. Ce champ est disponible lorsque **l'option Utiliser un MID** Server est sélectionnée. **Remarque :** Assurez-vous que l'enregistrement de Hub 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 laquelle Serveur MID est sélectionnée lors de l'exécution. Pour en savoir plus sur la façon dont un est sélectionné pendant l'exécution, reportez-vous à la section Sélection d'un Serveur MID MID Server. 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 MID Server spécifique** est sélectionné dans la liste Sélection MID.
Grappe MID	Tous	Grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser un MID** Server est sélectionnée et **qu'une grappe MID spécifique** est sélectionnée dans la liste 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 MID Server doit disposer des instanciateurs de connexions JMS appropriés pour votre organisation. Configurez ces valeurs dans la `mid.property.jms.command.allowed_factory_names` propriété, trouvée 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 annoncée par le fournisseur JMS tiers.

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 instanciateur de connexions.
Informations d'identification	Ajouter 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.
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://ipAddressOrHostName:61616.
Actif	Cochez la case pour activer cette connexion.

Option	Description
Domaine	Déterminez le domaine dans lequel l'action ou l'activité s'exécute.
Utiliser un MID Server	Cochez cette case pour utiliser un MID Server pour cette action ou cette activité. Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée du MID Server.
Sélection de MID	Option permettant de sélectionner le MID Server ou la grappe MID spécifique. ○ **Sélectionner automatiquement un MID Server** : sélectionne automatiquement le MID Server. ○ **MID Server spécifique** : utilise le MID Server que vous sélectionnez. ○ **Grappe MID spécifique** : utilise la grappe MID que vous sélectionnez. Ce champ est disponible lorsque **l'option Utiliser un MID** Server est sélectionnée.
Grappe MID	Grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser un MID** Server est sélectionnée et **qu'une grappe MID spécifique** est sélectionnée dans la liste 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. 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** > **Identifiants**.
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 êtes prêt à créer une action ou une activité JMS personnalisée.

Créer des attributs de connexion pour IntegrationHub

Définissez des variables spécifiques à la connexion que vous pouvez utiliser dans les étapes d'intégration Hub d'intégration.

Avant de commencer

Rôle requis :

- Le rôle admin est requis pour créer des attributs de connexion.
- Le rôle connection_admin ou admin est requis pour affecter des valeurs d'attribut.
- Le rôle action_designer ou admin 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 Hub d'intégration. Pour plus d'informations sur l'activation Hub d'intégrationde , consultez Demander un Hub 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. Concepteur de flux 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 Concepteur de flux , consultez Concepteur d'action .

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. Cliquez sur **Nouveau** dans la liste connexe Attributs de connexion.
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 Vue avancée pour définir les préférences de dictionnaire avancées pour l'attribut. Par exemple, pour créer un attribut avec une valeur calculée dynamiquement. Voir le formulaire d'entrée du dictionnaire .
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 des attributs de connexion.

d. Enregistrez l'enregistrement.
L’onglet Attributs est renseigné avec les attributs de connexion définis dans l’enregistrement d’alias.

e. Définissez des valeurs pour les attributs.
Si l’option **Prendre en charge plusieurs connexions actives** est activée pour l’alias, vous pouvez associer plusieurs enregistrements de connexion à un alias et définir des valeurs d’attribut 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. Ajoutez l’alias à une étape d’intégration dans Concepteur d'action.
   a. Accédez à Concepteur de flux une action et créez ou sélectionnez une action.
   b. Ajoutez une étape d’intégration à l’action.
   c. Sous Détails de la 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 n’effectue pas de suivi des modifications apportées aux étiquettes d’attributs de connexion et aux types de données après l’association de 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 MID Server utilise les informations d’identification que vous créez dans la table Informations d’identification [discovery_credentials] pour accéder aux ressources de Discovery, Orchestration, Service Mapping et Cloud Management.

Comment les MID Servers utilisent les informations d’identification

Par défaut, les MID Servers Windows utilisent les informations d’identification de connexion du service MID Server sur l’ordinateur hôte pour détecter Windows les appareils du réseau. Vous devez configurer les informations d’identification du service Serveur MID Windows afin qu’elles disposent au moins des privilèges d’administrateur local. Pour Linux les UNIX ordinateurs et les périphériques réseau, le MID Server utilise les informations d’identification SSH et SNMP configurées dans l’instance dans **Détection** > **Identifiants**.

Les MID Servers qui Orchestration 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 Détection, 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 de la table Informations d’identification [discovery_credentials]. Une fois qu’ils sont entrés, ils ne peuvent pas être visualisés.

Lorsque le MID Server demande des informations d'identification, il Now 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 chiffrées à nouveau sur l'instance avec la clé publique du MID Server.
3. Les informations d'identification sont chiffrées sur l'équilibreur de charge avec SSL.
4. Les informations d'identification sont déchiffrées sur le MID Server avec SSL.
5. Les informations d'identification sont déchiffrées sur le MID Server avec la clé privée de ce dernier.

Remarque :
La plateforme ne dispose pas de clés de chiffrement distinctes pour les instances mutualisées.

Ordre des informations d'identification

Une valeur d'ordre peut être affectée aux informations d'identification dans le formulaire Informations d'identification, ce qui oblige l'application à essayer toutes les informations d'identification à sa disposition dans un certain ordre. Si vous ne spécifiez pas de valeur d'ordre, l'application essaie les informations d'identification de la table Informations d'identification [discovery_credential] de manière aléatoire, jusqu'à ce qu'elle en trouve une qui fonctionne. Par exemple, quand :

- 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, Détection créez une relation entre les informations d'identification et l'appareil à l'aide de la table Affinité des informations d'identification [dscy_credentials_affinity]. Toutes les détections ou activités d'orchestration suivantes tentent de faire correspondre les informations d'identification de cette table avec un appareil pour lequel il existe une affinité. Si les informations d'identification d'un appareil changent et qu'Orchestration essaie Détection à nouveau toutes les informations d'identification disponibles jusqu'à ce qu'une nouvelle relation soit créée.

Remarque :
Si Orchestration et Détection sont installés et que l'alias d'informations d'identification est activé, plusieurs relations peuvent exister. Dans ce cas, la plateforme recherche les informations d'identification de chaque relation et insère les informations d'identification de la relation avec l'ordre le plus bas dans la sonde.

La commande des informations d'identification est utile dans les situations suivantes :

- La table Informations d'identification contient de nombreuses informations d'identification, certaines étant utilisées plus fréquemment que d'autres. Par exemple, la table contient 150 informations d'identification SSH, et cinq d'entre elles sont utilisées pour se connecter à 90 % des appareils. Il est recommandé de configurer ces cinq informations d'identification avec des numéros d'ordre inférieur, qui les placent en haut de la liste d'exécution. Détection et Orchestration fonctionnent plus rapidement lorsqu'ils essaient d'abord ces informations d'identification courantes. Après la première connexion réussie, le sait Now Platform quelles informations d'identification utiliser la prochaine fois pour chaque appareil.

- Il Now Platform dispose d'une sécurité de connexion agressive. Par exemple, configurez les informations d'identification de la base de données avec une valeur d'ordre inférieur si les serveurs de base de données Solaris du réseau ne fournissent que trois tentatives de connexion infructueuses avant de verrouiller le MID Server.

Alias d'informations d'identification

Les alias d'informations d'identification sont disponibles pour Discovery et Orchestration.

Les alias pour Discovery permettent à un administrateur d'effectuer les opérations suivantes :

- Utilisez un comportement de filtrage des informations d'identification avec des niveaux de conformité configurables.
- Affectez plusieurs alias d'informations d'identification à un calendrier Discovery.
- Empêchez la création d'affinités d'informations d'identification qui utilisent des informations d'identification inappropriées ou sensibles. Pour en savoir plus, consultez Relations avec les informations d'identification.

Les alias pour Orchestration permettent aux créateurs de workflows :

- Affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration
- Affecter des informations d'identification individuelles à n'importe quelle action dans Flow Designer
- 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 de concepteur.

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 magasins externes peuvent être configurés 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 admin est requis pour créer un alias.
- Les rôles credential_admin et connection_admin disposent d'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 définit 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 modifié le nom pour respecter les restrictions de dénomination.
ID	Identificateur unique de l'alias de connexion et d'informations d'identification, basé sur le format `scope_name.alias_name`. ○ Si le champ d'application est Global, l'ID est le nom de l'alias. Par exemple, si vous créez un alias Workday dans le champ d'application global, il définit l'ID sur `Workday`. ○ Si vous créez un alias Workday dans le champ d'application de l'application RH, il définit l'ID 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 par rapport auquel l'alias de connexion et d'informations d'identification est affecté. Le périmètre de session actuel que vous avez sélectionné pour la dernière fois 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 comment les sélectionner, consultez : ▪ Périmètre de l'application ▪ Sélectionner une application dans le sélecteur d'application
Type de connexion	Nom du type de connexion : De base, HTTP, JDBC, JMS ou Kafka. La valeur par défaut est HTTP.
Prendre en charge plusieurs connexions actives	Désignateur qui indique 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.

Champ	Description
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 connexes 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 les données spécifiques à une connexion et utilisez-les dans une étape d'intégration Hub d'intégration . Pour plus d'informations, consultez Créer des attributs de connexion pour IntegrationHub.
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.

Liste connexe	Description
Connexions	Enregistrements de connexion connexes 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 les données spécifiques à une connexion et utilisez-les dans une étape d'intégration Hub d'intégration . Pour plus d'informations, consultez Créer des attributs de connexion pour IntegrationHub.

5. **Facultatif :** Si vous souhaitez créer des informations d'identification et une connexion associées à votre alias d'informations d'identification, sous `Related Links`, cliquez sur **Créer une nouvelle connexion et de nouvelles informations d'identification**.
   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, sélectionnez **Nouveau** sous la liste connexe **Alias enfants**.

   a. Entrez un nom pour 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'informations d'identification.

Que faire ensuite

Créez un ou plusieurs enregistrements de connexion à associer à l'alias ou aux alias enfant. Pour en savoir plus sur la création de connexions, reportez-vous à Mise en route des connexions.

Ajoutez des attributs de connexion à l'alias pour rendre les métadonnées de connexion disponibles pour les flux dans Concepteur de flux.

Alias d'informations d'identification pour la détection

Alias d'informations d'identification pour Détection permettre à 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 Discovery 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 détection est autorisé à utiliser et empêchent l'exposition inutile des informations d'identification avec des privilèges élevés.

Fonctionnement des alias d'informations d'identification

Une règle métier appelée *Insérer des alias de relation de détection et d'informations d'identification* (précédemment *appelée Insérer des relations de détection*) s'exécute lorsqu'un enregistrement est inséré dans la file d'attente ECC. La règle métier joint les alias d'informations d'identification définis dans le calendrier Discovery à la sonde, afin que le MID Server puisse effectuer le filtrage des informations d'identification. La première tâche du MID Server consiste à créer la liste des informations d'identification à rechercher. Il filtre les informations d'identification par relation , puis par balises, le cas échéant. Les affinités vont en haut de la liste et les balises correspondantes vont en bas de la liste. Le MID Server parcourt la liste jusqu'à ce qu'il trouve des informations d'identification qui fonctionnent. Le MID Server crée alors une relation pour ces informations d'identification.

Remarque :
Les informations d'identification doivent correspondre à toutes les balises d'informations d'identification.

Si la règle métier détermine qu'il existe une relation pour l'appareil, elle identifie le *credential_id* approprié à utiliser. Il s'agit du *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 tel est le cas, la règle métier sélectionne *l'credential_id* de l'alias et transmet cette valeur au MID Server. Si les informations d'identification n'ont pas l'alias d'informations d'identification spécifié, toutes les autres relations existantes pour le système cible sont vérifiées.

Créer un alias d'informations d'identification Discovery

Créez l'alias, puis ajoutez-le à vos informations d'identification dans l'enregistrement d'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 Discovery 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 ignore toute relation d'informations d'identification précédemment existante entre les informations d'identification et la cible qui est détectée dans un calendrier configuré pour utiliser cet alias d'informations d'identification.

Procédure

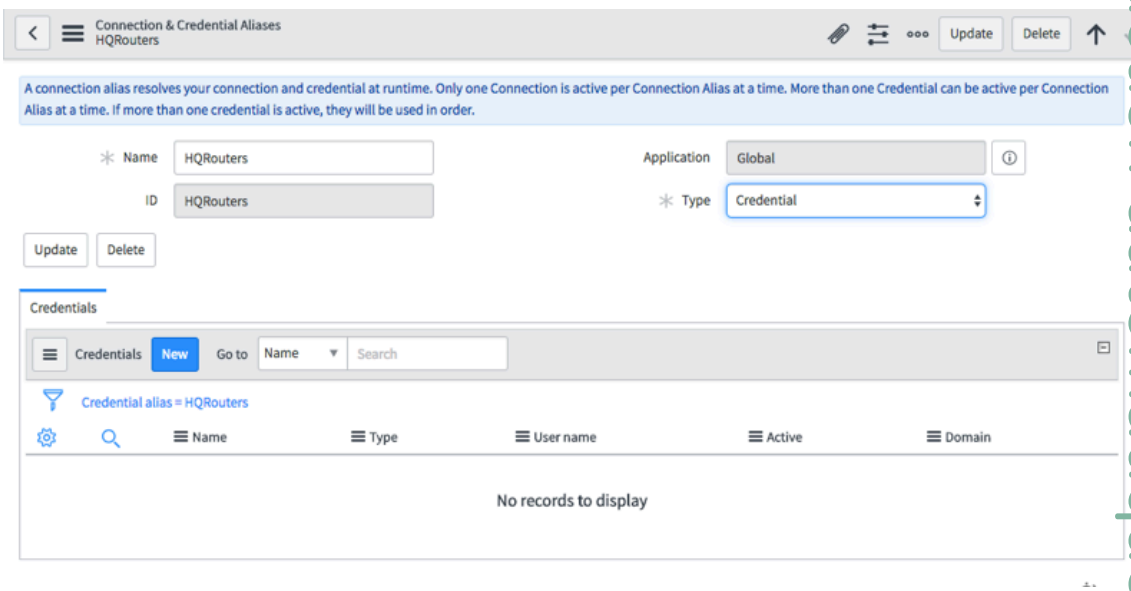
1. Créez un alias.

   a. Accédez à la **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.

   b. Cliquez sur **Nouveau**.

   c. Entrez un nom unique pour l'alias et sélectionnez **Informations d'identification** pour le **type d'alias**.

   d. Cliquez sur **Envoyer**.
   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.

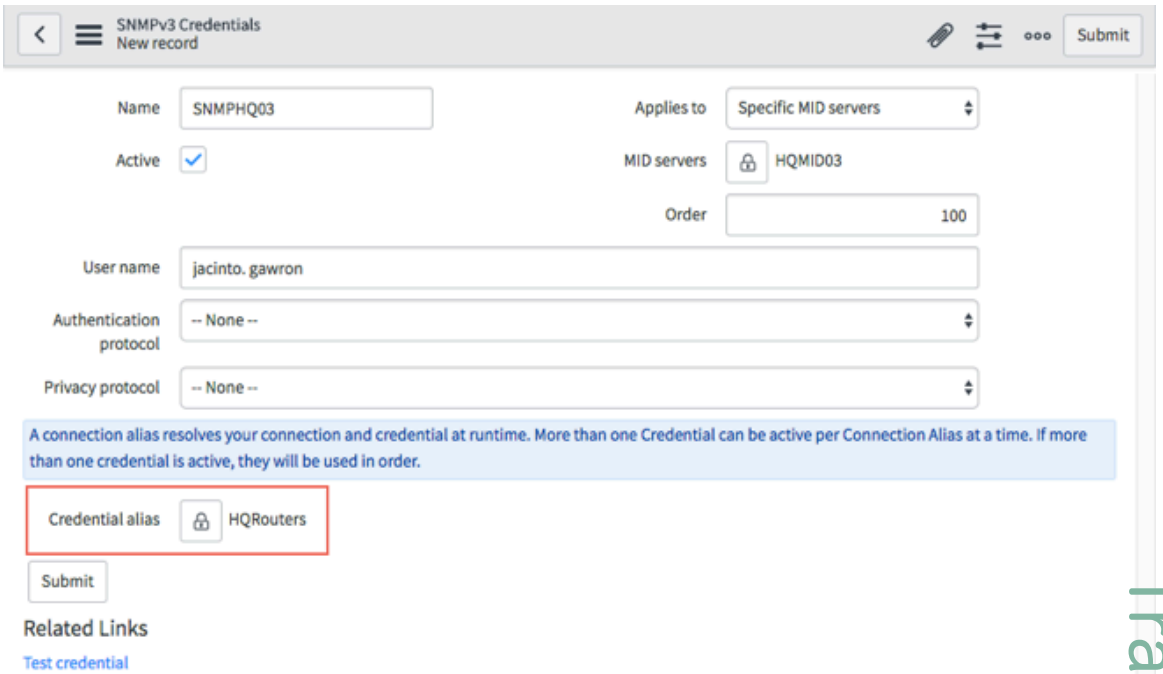


2. Configurez des informations d'identification pour le nouvel alias.

   a. Accédez à la **Connexions et informations d'identification** > **Identifiants**.

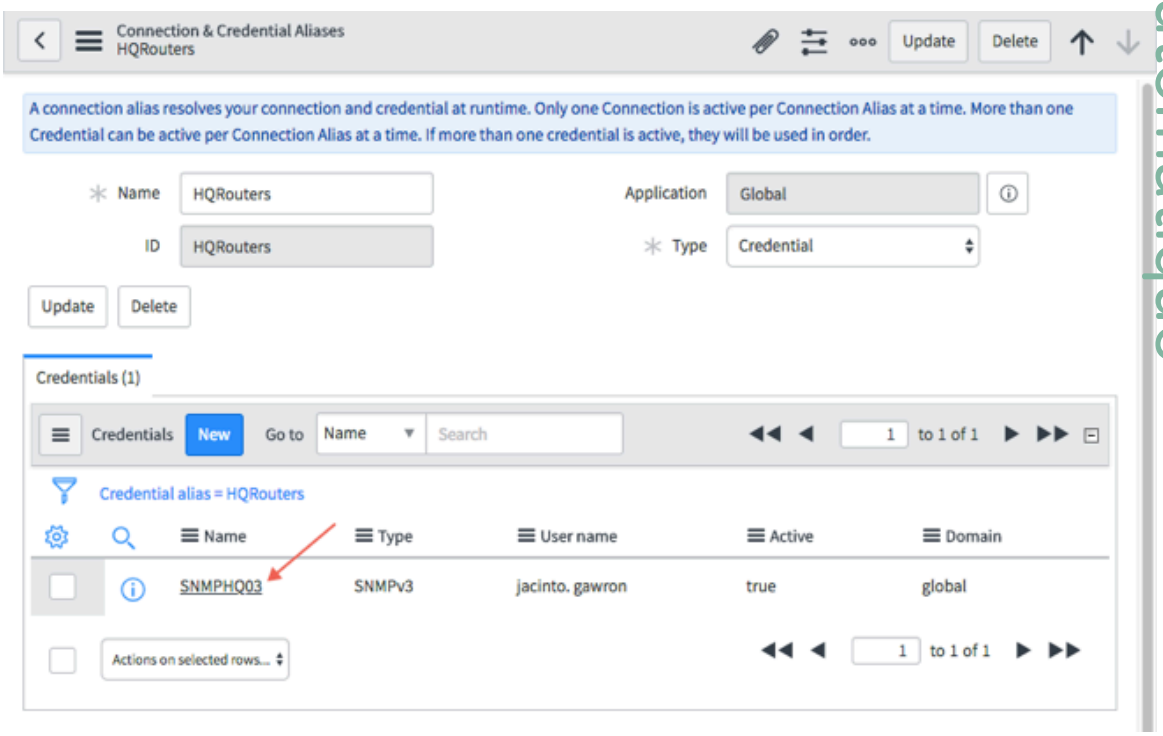
   b. Sélectionnez des informations d'identification existantes dans la liste ou cliquez sur **Nouveau** pour créer de nouvelles informations d'identification.

   c. Dans l'enregistrement Informations d'identification, déverrouillez le champ **Alias d'informations d'identification** et sélectionnez l'alias que vous avez créé.



d. Enregistrez ou envoyez l'enregistrement.

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 détection* (renommée 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 le *credential_id* approprié (le *sys_id* de l'enregistrement dans la table Informations d'identification [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 tel est le cas, la règle métier sélectionne *l'credential_id* de l'alias d'informations d'identification et transmet cette valeur au MID Server. Si les informations d'identification ne possèdent pas l'alias d'informations d'identification spécifié, toutes les autres relations existantes pour le système cible seront vérifiées. Si aucune relation ne fait référence à des informations d'identification balisées de manière appropriée, le MID Server parcourt la table Informations d'identification *[discovery_credentials]* et sélectionne les informations d'identification avec la balise appropriée. Le MID Server crée alors une nouvelle relation pour ces informations d'identification.

Créer et tester vos informations d'identification

Créez et testez les informations d'identification dont Discovery, Service Mapping, Cloud Management et Orchestration ont besoin pour accéder au matériel et aux logiciels de votre réseau.

Avant de commencer

Rôle requis : admin

Passez en revue votre politique et vos options de sécurité avec l'équipe de sécurité de votre organisation.

Pourquoi et quand exécuter cette tâche

Cette tâche contient des procédures générales pour la création d'informations d'identification. Consultez la documentation relative à votre type d'informations d'identification pour en savoir plus sur les champs et les exigences spécifiques.

Types d’informations d’identification pris en charge

Informations d'identification applicatives	Informations d’authentification de base	Informations d’identification du serveur Chef
Informations d'identification CIM	Informations d'identification dans le cloud	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 périmètre des informations d’identification à un MID Server ou à un calendrier spécifique afin d’éviter les informations d’identification inutiles.

Procédure

1. Accédez à l’un de ces modules :
   - **Détection** > **Identifiants**
   - **Mappage des services** > **Identifiants**
   - **Orchestration** > **Identifiants**
2. Cliquez sur **Nouveau**.
3. Sur la page Informations d’identification, cliquez sur un lien correspondant au type d’informations d’identification et remplissez le formulaire.

   Pour en savoir plus, consultez la documentation correspondant au type d’informations d’identification que vous avez sélectionné.

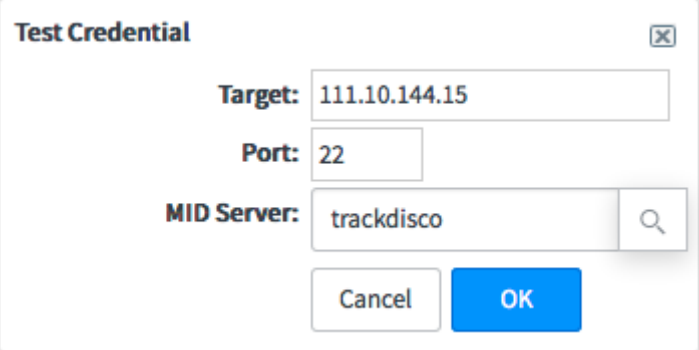
   Vous pouvez d’abord soumettre un enregistrement d’informations d’identification puis le tester ultérieurement, ou tester les informations d’identification immédiatement avant de les enregistrer.

   Le test des informations d’identification est pris en charge pour les types d’informations d’identification suivants :
   - 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 dans la boîte de dialogue Tester les informations d’identification.

Boîte de dialogue Tester les informations d'identification



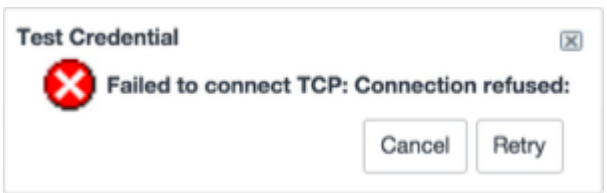
Champs de test d'informations d'identification

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. **Remarque :** Pour JMS, il s'agit de l'URL du fournisseur. Les informations contenues dans cette URL indiquent à JNDI comment trouver et accéder au fournisseur JMS. Un exemple de valeur pour la connexion à ActiveMQ V5.1 est `tcp://ipAddressOrHostName:61616`.	Tous
Port	Port sur la cible à utiliser pour ce test. Le système pré-remplit ce champ avec le port par défaut pour le type d'informations d'identification sélectionné.	Tous
Serveur MID	Serveur MID à utiliser pour ce test. Vous devez utiliser un MID Server 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

Champ	Description	Type d'informations d'identification
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 initiale**, divers objets JMS, tels que JMS Connection, sont créés. Par exemple, pour vous connecter à ActiveMQ V5.10 (fournisseur JMS), la valeur de ce champ serait org.apache.activemq.jndi.ActiveMQInitialContextFactory	JMS

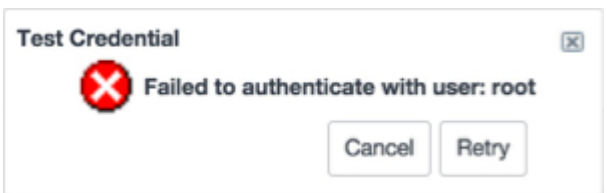
6. Cliquez sur **OK** pour commencer le test.
   Un indicateur s'affiche, montrant que le système tente de contacter la cible à l'aide des informations d'identification que vous avez fournies. Lorsque l'instance se connecte à la cible, un message de réussite s'affiche. Si l'instance rencontre un problème avec les entrées de test que vous avez fournies, elle affiche le message d'erreur approprié. Vous trouverez ci-dessous des messages d'erreur courants.
   - Numéro de cible ou de port incorrect :

     Échec de la connexion TCP

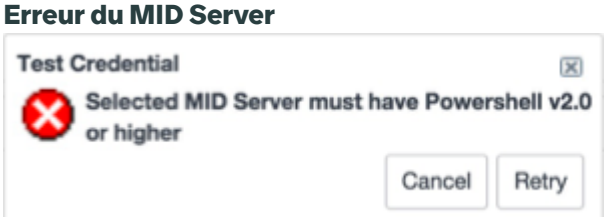
   - Nom d'utilisateur ou mot de passe incorrect :

     Échec de l'authentification

   - Informations d'identification MID Server pour Windows incorrectes :

     Erreur du MID Server

7. Cliquez sur **Réessayer** pour ouvrir la boîte de dialogue des informations d'identification de test et corriger l'erreur d'entrée.

8. Si 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 Discovery 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 dans le 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.
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 qui est transmis à une API pour identifier l'application ou l'utilisateur appelant.

Informations d'identification de clé API

Champs du 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 workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un flux ou d'un workflow, ou affectez 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 le Serveurs MID qui doit utiliser ces informations d'identification dans le champ **MID Servers** .

Champs du formulaire Informations d'identification de clé API (suite)

Champ	Valeur d'entrée
Ordre	Ordre (séquence) utilisé Détection pour essayer ces informations d'identification 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.

Généralement, les informations d'identification contiennent un nom d'utilisateur et un mot de passe pour 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 d'identification applicatives en plus des informations d'identification de l'hôte SSH ou Windows pour le serveur qui héberge ASCS.

Remarque :
ServiceNow désignent les appareils et les applications dont les éléments de configuration (CI) contiennent un service d'application.

Comme pour les informations d'identification de l'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 Application ASCS SAP [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. Si plusieurs informations d'identification sont configurées pour ce type de CI, le système essaie Serveur MID d'utiliser ces informations d'identification dans l'ordre que vous définissez jusqu'à ce qu'il trouve les informations d'identification adaptées.

Vérifiez les informations sur les besoins Détection 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 Détection 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 dans le nom des informations d'identification.

Champs du formulaire Informations d'identification applicatives (suite)

Champ	Description
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 dans 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 • 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 le Serveurs MID qui doit utiliser ces informations d'identification dans le champ **MID Servers** .
Ordre	Ordre (séquence) utilisé Détection pour essayer ces informations d'identification 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

Champs du formulaire Informations d'identification applicatives (suite)

Champ	Description
	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’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	Entrez la clé unique configurée pour ces informations d’identification dans le système de stockage des informations d’identification externes CyberArk . L’ID d’informations d’identification peut être utilisé comme remplacement sécurisé lorsque plusieurs coffres-forts sont utilisés. Par défaut, la syntaxe dans le champ **ID d’informations d’identification** est la suivante : `<safe name>:<Credential ID>`. Si le nom fiable est omis, il doit y avoir un nom fiable défini dans le fichier config.xml . Pour remplacer le caractère de séparation par deux points 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) utilisé Détection pour essayer ces informations d’identification 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 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	Saisissez la clé privée RSA générée par le serveur Chef lors de la création de l'administrateur.
Nom de validateur	Entrez le validateur.
Clé de validateur	Saisissez la clé privée RSA générée par le serveur Chef lors de la création d'une organisation.
Nom du certificat	Saisissez le nom de la certification.
Clé du certificat	Saisissez la clé de certification.

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 Discovery.

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.

Champ	Description
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. Pour plus d'informations, consultez Changer les informations d'identification sur une valeur autre que celle par défaut.
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 le Serveurs MID qui doit utiliser ces informations d'identification 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**. **Remarque :** La sélection **de MID Servers spécifiques** n'affecte pas la sélection de MID Server. Il est utilisé uniquement pour décider quels MID Servers 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) utilisé Détection pour essayer ces informations d'identification 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 appareils de stockage NetApp pour les informations d'identification CIM

Les périphériques de stockage NetApp nécessitent une configuration supplémentaire pour Détection pouvoir les explorer.

Avant de commencer

Rôle requis : admin

Procédure

1. Installez l'agent SMI-S sur l'hôte de l'appareil de stockage.

   Reportez-vous au Guide d'installation et de configuration de Data ONTAP SMI-S Agent 5.2 pour connaître les instructions et les exigences.

   Remarque :

   ServiceNow ne gère 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 dans le cloud gèrent l'accès aux applications basées sur le cloud, y compris Amazon Web Services et le cloud Microsoft Azure.

Rôles AWS Identity and Access Management (IAM)

Si vous avez un MID Server installé sur Amazon EC2 dans un cloud AWS et que ce MID Server est configuré pour détecter les 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 changent automatiquement selon un intervalle configurable. Lorsqu'un rôle IAM est défini sur le MID Server. Pour en savoir plus, consultez Configurer le MID Server pour les rôles AWS IAM .

Discovery ignore les informations d'identification stockées sur l'instance au profit 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.

Champs du formulaire Informations d'identification AWS (suite)

Champ	Valeur d'entrée
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 du 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 dans le 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 dans le 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. Ce champ s'affiche lorsque la **Méthode d'authentification** est **Secret client**.

Informations d'identification de l'Azure Enterprise Agreement

Les informations d'identification du Contrat Entreprise Azure sont nécessaires pour la fonctionnalité de facturation fournie par l'application Gestion dans le cloud.

Champs du 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 dans le cloud

Ce type d'informations d'identification est disponible pour Orchestration.

Champs du formulaire Informations d'identification de Gestion dans le 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 entrer **Vendredi est un bon jour**.
Clé privée SSH	Saisissez 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	Entrez 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 cryptage 192 bits • **AES256** pour AES avec cryptage 256 bits • **DES** pour le 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 le Serveurs MID qui doit utiliser ces informations d'identification dans le champ **MID Servers** .
Classification	Entrez la classification d'application pour la détection de CI.

Champs du formulaire Informations d'identification de Gestion dans le cloud (suite)

Champ	Valeur d'entrée
Ordre	Ordre (séquence) utilisé Détection pour essayer ces informations d'identification 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 de Gestion dans le cloud (CMP)

Les informations d'identification du nœud de Gestion dans le cloud (CMP) associent les informations d'identification d'un serveur virtuel que Gestion dans le cloud met en service. L'application Gestion dans le cloud crée automatiquement ces informations d'identification.

Remarque :
Vous devrez peut-être désactiver ces informations d'identification si vous ne souhaitez plus les utiliser, modifier l'ordre de priorité ou sélectionner un MID Server 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.
Actif	Si les informations d'identification sont actives.
Concerne	Choisissez si ces informations d'identification sont disponibles pour un MID Server spécifique ou pour tous les MID Servers.
Ordre	Ordre (séquence) utilisé Détection pour essayer ces informations d'identification 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	Le nom d'utilisateur et le 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	La clé privée et la phrase de sécurité qui protège la clé si le serveur virtuel l'exige.

Champs du formulaire Informations d'identification du nœud CMP (suite)

Champ	Description
et clé d'authentification	
Protocole de confidentialité et clé de confidentialité	Protocole de chiffrement utilisé avec le serveur virtuel et saisissez 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 de Cloud Management (CMP)

Les paires de clés SSH Cloud Management (CMP) stockent les clés que l'application Cloud Management 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 les utiliser. Sinon, vous n'avez pas besoin de créer ou de modifier manuellement ce type d'informations d'identification.

Champs du formulaire Informations d'identification de la paire de clés SSH CMP

Champ	Description
Nom	Nom généré automatiquement.
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 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 MID Server spécifique ou pour tous les MID Servers.

Champ	Description
Ordre	Ordre (séquence) utilisé Détection pour essayer ces informations d'identification 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. Ordre (séquence) utilisé Détection pour essayer ces informations d'identification 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 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 Java Database Connectivity (JDBC). Ce type d'informations d'identification est disponible pour Discovery 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.

Champ	Description
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. Pour plus d'informations, consultez Changer les informations d'identification sur une valeur autre que celle par défaut.
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 le Serveurs MID qui doit utiliser ces informations d'identification 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**. **Remarque :** La sélection **de MID Servers spécifiques** n'affecte pas la sélection de MID Server. Il est utilisé uniquement pour décider quels MID Servers 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) utilisé Détection pour essayer ces informations d'identification 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 Informations d’identification JMS gère l’accès à un service de messagerie Java (JMS). Ce type d’informations d’identification est disponible pour Discovery 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.
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. Pour plus d’informations, consultez Changer les informations d’identification sur une valeur autre que celle par défaut.
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 le Serveurs MID qui doit utiliser ces informations d’identification 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

Champ	Description
	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 utilisé uniquement pour décider quels MID Servers 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) utilisé Détection pour essayer ces informations d'identification 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 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.

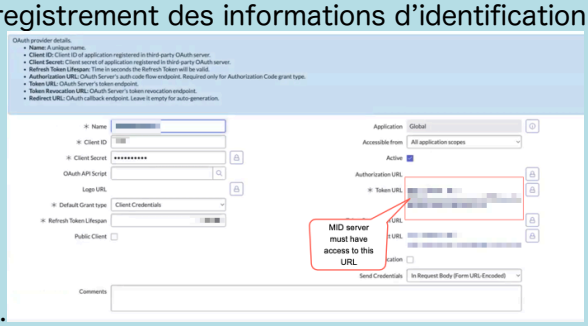
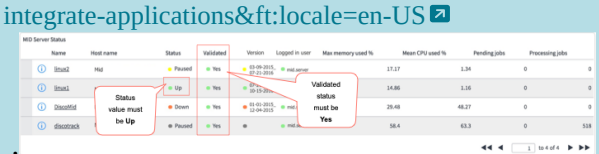
Formulaire Informations d'identification OAuth 2.0

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	Spécifiez si ces informations d'identification sont actives.
Profil de l'entité OAuth	Un profil OAuth est une combinaison d'un type d'accord et d'au moins un champ d'application.
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 MIDserveur . Il peut également connecter votre ServiceNow instance à un serveur OAuth basé sur le cloud via un MID Server. Lorsque cette option est activée, la demande de jeton OAuth est envoyée via le Serveur MID.

Formulaire Informations d'identification OAuth 2.0 (suite)

Champ	Valeur d'entrée
	Important : • L'option s'affiche lorsque la valeur du champ **Type d'accord** dans le profil de l'entité OAuth est définie sur **Informations d'identification du client**. Pour apprendre à 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 le MID Server** , vous devez identifier l'élément requis Serveur MID ou Serveurs MID dans la liste **S'applique à** .
Concerne	Spécifiez si l'enregistrement des informations d'identification s'applique à tous les MID Servers, ou à un MID Server spécifique. S'ils sont spécifiques, ajoutez les MID Servers au besoin.

Formulaire Informations d'identification OAuth 2.0 (suite)

Champ	Valeur d'entrée
	Important : Assurez-vous d'être conscient de ces considérations si vous avez coché la case **Se connecter au serveur d'authentification via MID Server** . • Assurez-vous que tous les éléments Serveurs MID sélectionnés dans S'applique à peuvent communiquer avec le serveur d'authentification. Cela est nécessaire pour exécuter la demande de jeton par rapport à **l'URL de jeton** mentionnée dans l'enregistrement du fournisseur OAuth (qui est lié au profil d'entité OAuth spécifié dans l'enregistrement des informations d'identification OAuth 2.0).  • Assurez-vous qu'il y en a au moins un (dans l'élément Serveur MIDServeurs MID sélectionné dans **S'applique à**) avec ces configurations : ◦ La valeur du champ **État** est **Haut**. ◦ La valeur du champ **Validé** est **Oui**. ◦ L'option de l'option Serveur MID est définie sur **REST** ou **ALL.** Pour apprendre à configurer le MID Server, reportez-vous à https://www.webstg.servicenow.com/docs/access?context=configure-capabilities&version=washingtondc&pubname=washingtondc-integrate-applications&ft:locale=en-US  . Pour en savoir plus sur ces états, reportez-vous à MID Server dashboard .
Ordre	Ordre (séquence) utilisé Détection pour essayer ces informations d'identification 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

Formulaire Informations d'identification OAuth 2.0 (suite)

Champ	Valeur d'entrée
	d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
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 pour les informations d'identification. Invoquez une 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** : extraire les informations de jeton en fonction du profil du demandeur. • **Personnel** : extrait les informations de jeton spécifiques à l'utilisateur. Utilisateur qui lance la session. Si cette **personne** est sélectionnée sur la page Profil du demandeur OAuth, un marqueur supplémentaire appelé **Personnel** s'affiche. **Remarque :** • Toutes les informations relatives 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 session, vous devez sélectionner **Exécuter en tant que** classé dans les propriétés du flux en tant **qu'utilisateur qui initie 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 Discovery 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.
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.

Champ	Description
	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. Pour plus d'informations, consultez Changer les informations d'identification sur une valeur autre que celle par défaut.
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 le Serveurs MID qui doit utiliser ces informations d'identification 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**. **Remarque :** La sélection **de MID Servers spécifiques** n'affecte pas la sélection de MID Server. Il est utilisé uniquement pour décider quels MID Servers 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) utilisé Détection pour essayer ces informations d'identification 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	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Champ	Description
Serveur MID Windows	

Informations d'identification SNMP

Détection explore de nombreux types d'appareils (commutateurs, routeurs, imprimantes, etc.) à l'aide du protocole SNMP. Les informations d'identification pour SNMP n'incluent pas un nom d'utilisateur, seulement un mot de passe, appelé *`chaîne de communauté`*.

La chaîne de communauté en lecture seule par défaut pour de nombreux appareils SNMP est publique et Détection l'essaie automatiquement. Entrez les informations d'identification SNMP appropriées si elles sont différentes de la chaîne de communauté *`publique`* .

Détecter Le protocole 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 nécessite 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 pour détecter de nombreux types d'équipements (commutateurs, routeurs, imprimantes, etc.) à l'aide du protocole SNMP. Ce type d'informations d'identification est disponible pour Détection, Mappage des servicesetOrchestration.

Les informations d'identification pour SNMP n'incluent pas de nom d'utilisateur, seulement un mot de passe (la chaîne de communauté). La chaîne de communauté en lecture seule par défaut pour de nombreux appareils 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 de 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.
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.

Champ	Description
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. Pour plus d'informations, consultez Changer les informations d'identification sur une valeur autre que celle par défaut.
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 le Serveurs MID qui doit utiliser ces informations d'identification 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**. **Remarque :** La sélection **de MID Servers spécifiques** n'affecte pas la sélection de MID Server. Il est utilisé uniquement pour décider quels MID Servers 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) utilisé Détection pour essayer ces informations d'identification 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 SNMPv3

Les informations d’identification SNMPv3 acceptent un protocole de confidentialité et une clé de confidentialité supplémentaire, et sont disponibles pour Discovery 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 SNMP v3.

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) utilisé Détection pour essayer ces informations d’identification 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 • SHA-224 • SHA-256 • SHA-384 • SHA-512
Clé d'authentification	Entrez la clé d'authentification à utiliser pour ces informations d'identification.

Champs d'informations d'identification SNMPv3 (suite)

Champ	Valeur d'entrée
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.
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.

Champs d'informations d'identification SNMPv3 (suite)

Champ	Valeur d'entrée
	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. Pour plus d'informations, voir Nom de contexte et ID de contexte. 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

Détection, Orchestration et Hub d'intégration explorer et Linux utiliser UNIX les 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 Détection, Orchestration ou Hub 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. Détection, Orchestration ou Hub 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 Détection, Orchestration ou Hub d'intégration ont les informations d'identification racine pour n'importe quel système UNIX ou Linux, aucune autre configuration n'est nécessaire.

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 du MID Server .

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, car elles offrent une meilleure sécurité que les informations d'identification de mot de passe SSH.

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	Entrez une clé privée sécurisée, RSA, DSA ou ECDSA qui peut être utilisée à la place d’un mot de passe pour les connexions SSH.
	
	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-----`
	
	Exemple d’une clé DSA :
	`-----BEGIN DSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3`
	`IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END DSA PRIVATE KEY-----`
	
	Et un exemple de clé ECDSA :
	`-----BEGIN EC PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3`
	`IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END EC PRIVATE KEY-----`
	
	Le Now 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 :

Champ	Valeur d'entrée
	• Ouvrez votre clé privée dans PuTTYGen. • Exportez-le au format OpenSSH à partir du menu **Conversions** > **Exporter la clé OpenSSH**. • Enregistrez la nouvelle clé OpenSSH.
Certificat SSH	Entrez un certificat OpenSSH basé sur RSA pour une connexion SSH à l'aide de certificats. Lors de la saisie du certificat, 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.
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 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. Pour plus d'informations, consultez Changer les informations d'identification sur une valeur autre que celle par défaut.
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 le Serveurs MID qui doit utiliser ces informations d'identification 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

Champ	Description
	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) utilisé Détection pour essayer ces informations d'identification 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 Hub 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. • **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 Hub d'intégration
chpasswd	Modifie les mots de passe utilisateur. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/chpasswd • **Utilisée par** : Orchestration et Hub d'intégration
Toutes les versions Linux	

Commandes UNIX et Linux nécessitant des privilèges racine (suite)

Commande	Objectif
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
Linux et Solaris	
dmsetup	Examine un volume de faible niveau. • **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

Commandes UNIX et Linux nécessitant des privilèges racine (suite)

Commande	Objectif
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 sur les connexions TCP. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/pfiles • **Utilisée par** : Discovery
PGREP (en anglais seulement)	Utilisé pour répertorier les ID de processus d'une région particulière sur laquelle exécuter pfiles. • **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 Détection, Orchestration et Hub 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 une liste des commandes privilégiées dont vous avez besoin pour Discovery et Service Mapping, consultez Service Mapping commands requiring a privileged user afin de voir la liste des commandes qui nécessitent des droits élevés pour détecter et mapper les hôtes basés sur 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 Détection 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
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 Discovery d’explorer le vCenter de VMware en cours d’exécution sur un ordinateur Windows pour détecter les machines

ESX, les ordinateurs virtuels et les pools de ressources. L'API VMware Détection et d'automatisation (API vCenter) fournit désormais le numéro de série unique global 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 Détectionlorsque des informations d'identification VMware valides sont utilisées.

Important :
N'utilisez pas les informations d'identification de type **VMware** pour les activités Orchestration qui travaillent 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.
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 un ou plusieurs Serveurs MID fichiers dans la liste des fichiers .Serveurs MID Les informations d'identification configurées dans cet enregistrement sont disponibles dans Serveurs MID cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.
Ordre	Ordre (séquence) utilisé Détection pour essayer ces informations d'identification 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 Discovery et Orchestration.

Exigences en matière d'informations d'identification

Détection et Orchestration ont les exigences suivantes pour Windows les informations d'identification :

- Installez un MID Server 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 MID Server à exécuter en tant qu'utilisateur Windows spécifique ou compte de domaine.

Accorder les autorisations appropriées

Pour fournir des autorisations suffisantes, Windows les informations d'identification doivent être l'une des suivantes :

- un utilisateur de domaine avec un accès administrateur local sur les hôtes Windows cibles ;
- Un compte local avec des privilèges d'administrateur et le contrôle d'accès utilisateur (UAC) désactivés sur le même hôte cible.
- Un utilisateur qui répond aux exigences des Windows sondes et des autorisations (Détection 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 améliorée en utilisant des profils JEA pour exécuter Détection. Pour plus d'informations, consultez Microsoft Just Enough Administration (JEA) pour Discovery .

Ordinateurs de groupes de travail

Pour exécuter les commandes PowerShell et détecter un ordinateur de groupe de travail, configurez les informations d'identification du MID Server pour l'un des utilisateurs suivants :

- Compte administrateur intégré sur l'ordinateur Workgroup.
- Utilisateur de domaine sur l'ordinateur du groupe de travail.

Configuration multi-domaines

Pour permettre aux informations d'identification Windows de fonctionner dans plusieurs domaines, assurez-vous d'utiliser les formats de nom et la configuration de MID Server corrects.

Détection et Orchestration prennent en charge Windows les informations d'identification de domaine dans les formats **de nom d'utilisateur principal** et **de nom d'utilisateur de connexion de niveau inférieur** . 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 de Serveur MID sur le même domaine que la Windows cible.	Aucun
Hôte de Serveur MID sur un domaine différent de la Windows cible.	Assurez-vous que PowerShell 3.0 (ou une version ultérieure jusqu'à 5.1) est installé sur l'hôte du MID Server.
Hôte de Serveur MID sur un domaine différent de la cible Microsoft SQL Server.	Reportez-vous à la section Détection de serveurs MSSQL .

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. Pour plus d'informations, consultez Changer les informations d'identification sur une valeur autre que celle par défaut.
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.

Champ	Description
	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 le Serveurs MID qui doit utiliser ces informations d'identification 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**. **Remarque :** La sélection **de MID Servers spécifiques** n'affecte pas la sélection de MID Server. Il est utilisé uniquement pour décider quels MID Servers 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) utilisé Détection pour essayer ces informations d'identification 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 MID Server

Configurez le MID Server pour utiliser 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 MID Server pour utiliser les informations d'identification du compte de service du MID Server.
   a. Définissez les informations d'identification du service Configurer Windows MID Server sur un utilisateur qui répond aux exigences 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 l'utilisation des informations d'identification du MID Server à partir de la table Informations d'identification [discovery_credentials].

a. Ajoutez 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 respecte les exigences de format de nom.
- Vérifiez que chaque information d'identification répond aux exigences du Windows domaine.

b. **Facultatif :** Configurez le MID Server pour utiliser PowerShell en définissant le paramètre mid.use_powershell sur **vrai**.
Reportez-vous à la section Configuration des MID Servers .

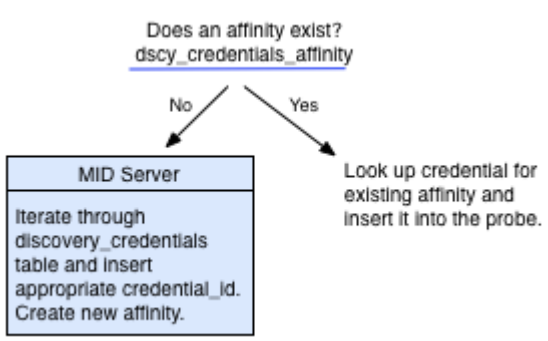
c. Cochez la case Compte de service du Serveur MID Windows pour créer des informations d'identification qui représentent le compte de service du Serveur MID Windows à exécuter en tant qu'utilisateur ou compte de domaine Windows spécifique.

Relation d'informations d'identification pour Discovery et Orchestration

L'affinité d'informations d'identification est une association entre un ensemble d'informations d'identification et un appareil de votre réseau.

Lorsqu'Orchestration Détection tente pour la première fois d'accéder à un appareil, il essaie toutes les informations d'identification disponibles jusqu'à ce qu'il trouve les informations d'identification correctes. Après avoir identifié les informations d'identification d'un appareil et Orchestration, Détection créez une relation entre les informations d'identification et l'appareil à l'aide de la table Affinité des informations d'identification [dscy_credentials_affinity]. Toutes les détections ou activités d'orchestration suivantes tentent de faire correspondre les informations d'identification de cette table avec un appareil pour lequel il existe une affinité. Si les informations d'identification d'un appareil changent et qu'Orchestration essaie Détection à nouveau toutes les informations d'identification disponibles jusqu'à ce qu'une nouvelle relation soit créée.

Diagramme d'affinité des informations d'identification



Traduction automatique

Remarque :
Si Orchestration et Détection sont installés et que l'alias d'informations d'identification est activé, plusieurs relations peuvent exister. Dans ce cas, la plateforme recherche les informations d'identification de 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 avec les 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. Consultez la section <credentials_debug> pour consulter des informations détaillées sur la recherche d'informations d'identification.

La section <credentials_debug> apparaît dans la charge utile si :

- Échec des informations d'identification pour les sondes WMIRunner, PowerShell, JMS ou SSHCommand.
- Vous définissez le *credentials_debug* paramètre sur **true** pour les sondes WMIRunner, PowerShell ou SSHCommand. Si vous définissez le paramètre sur vrai, la section de <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) que le MID Server a utilisé, y compris le type, la classification, la balise, le nom, l'ID système et l'ID d'informations d'identification externe le cas échéant.

Exemple de charge utile montrant des informations d'identification non valides

Payload XML


```
1 <?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
```


Des détails s'affichent pour le paramètre PowerShell :

Traduction automatique

- Si les informations d'identification du MID Server 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 celui sur lequel se trouve le MID Server.
- Si le paramètre mid.powershell.use_credentials est défini sur vrai.

Les détails s'affichent pour la commande SSHC :

- 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.

Remarque :
Le MID Server enregistre les adresses IP pour les recherches d'informations d'identification ayant échoué dans une liste d'exclusion de la mémoire cache. Cette liste d'exclusion spécifie les appareils auxquels le MID Server doit cesser d'essayer d'accéder. Les adresses IP sont ajoutées à la liste d'exclusion lorsque chaque identifiant a échoué. Les adresses IP sont effacées du cache de la liste d'exclusion au bout de cinq minutes, si le MID Server est redémarré ou si les enregistrements d'informations d'identification sur l'instance sont mis à jour.

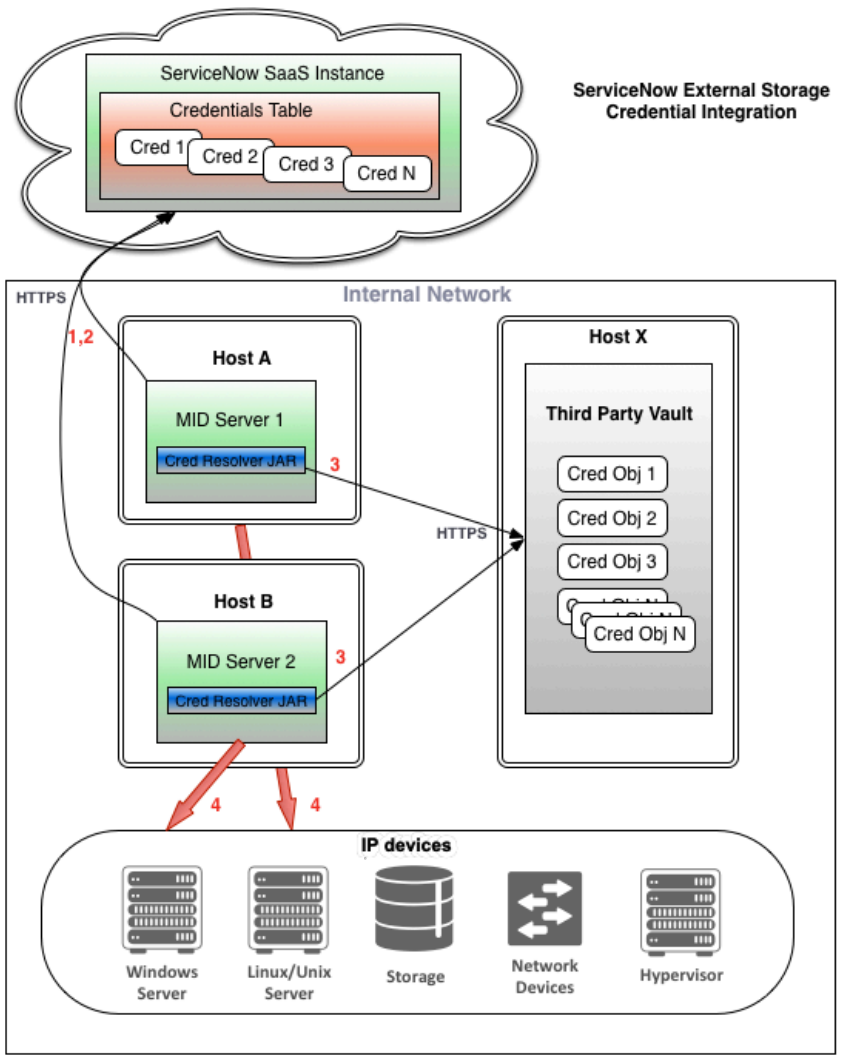
Stockage des informations d'identification externe

Une instance peut stocker les informations d'identification utilisées par DétectionOrchestration et Mappage des services dans un référentiel d'informations d'identification externe plutôt que directement dans un ServiceNow enregistrement d'informations d'identification.

L'instance conserve un identificateur unique pour chaque information d'identification, le type d'informations d'identification (tels que SSH, SNMP ou Windows) et toutes les relations d'informations d'identification. Le MID Server obtient l'identificateur d'informations d'identification 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 pour le stockage des informations d'identification externes.

Architecture de stockage des informations d'identification externe

Architecture de stockage des informations d'identification externe



Flux de processus des informations d'identification

Le MID Server récupère les informations d'identification à partir d'un magasin externe à l'aide du processus suivant :

1. Le MID Server télécharge les objets d'informations d'identification de la ServiceNow table Informations d'identification [discovery_credentials] qui contiennent l'ID d'informations d'identification correspondant à partir du coffre cible.
2. Au fur et à mesure que chaque sonde ou modèle s'exécute à partir de ou Orchestration de Détection tâches, le MID Server 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 de l'outil de résolution des informations d'identification. Les détails sur l'objet d'informations d'identification à récupérer dans le coffre-fort sont déterminés par l'outil 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 en cours d'exécution sur le même ordinateur que le MID Server. Cette application peut souvent être configurée pour mettre 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 des appels réseau inutiles au coffre chaque fois que MID Server demande des informations d'identification. 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. réels.

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 maximum en utilisant le chiffrement dans la mémoire de processus du MID Server. Cela signifie que le MID Server peut envoyer 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 des fournisseurs tiers pour obtenir des informations sur les implémentations de mise en cache pour d'autres outils de résolution des informations d'identification.

3. Le MID Server exécute la sonde avec les informations d'identification appropriées.

Remarque :
L'affinité d'identifiant s'applique toujours. Le mécanisme reste le même, car la seule différence réelle du point de vue du MID Server est que les véritables détails d'identification (nom d'utilisateur et mot de passe) proviennent du coffre-fort tiers.

Journalisation du stockage des informations d'identification externe

Le MID Server publie des messages de journal concernant le stockage des informations d'identification externe.

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 Stockage des informations d'identification externe

Règle métier

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 de voir 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 après son activation. L'établissement est situé à **Définition de Détection** > **Propriétés** et **Orchestration** > **Propriétés de Serveur MID**et est activé lorsque vous activez le module d'extension.

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 redéfinit pas les enregistrements d'informations d'identification externes comme étant actifs. Vous devez réactiver manuellement chaque enregistrement d'informations d'identification.

Demander un stockage des informations d'identification externe pour Discovery et Orchestration

Le module d'extension External Credential Storage est disponible sur demande.

Avant de commencer

Rôle requis : admin

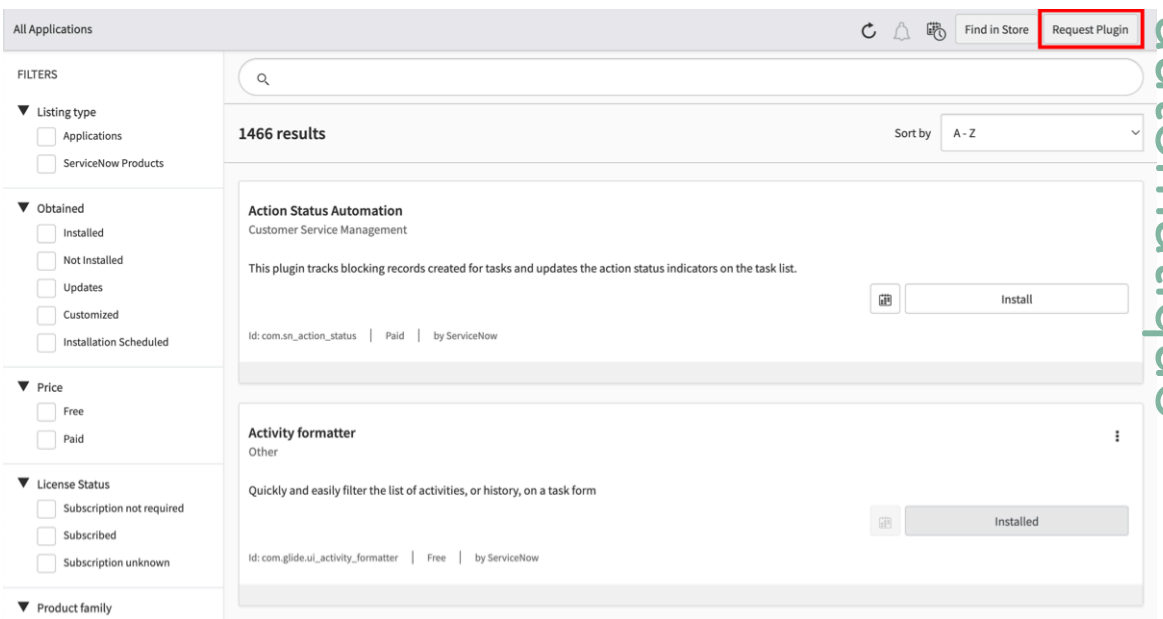
Pourquoi et quand exécuter cette tâche

Il existe deux façons de demander un module d'extension :

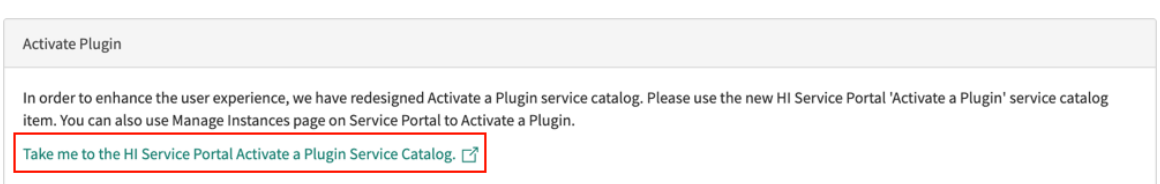
- Accéder directement au Now Support Service Catalog en sélectionnant **Tout** > **Catalogue de services** > **Activer le module d'extension** sur Now Support.
- Accéder au Catalogue de services de Now Support via la page Toutes les applications de votre instance en suivant ces étapes.

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.



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.

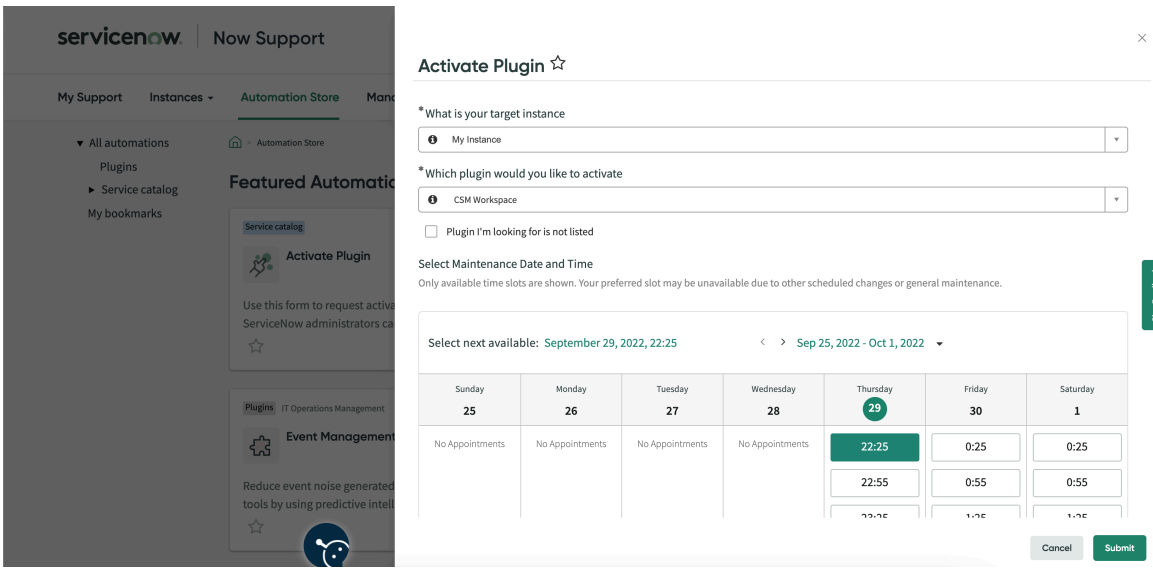
Formulaire Activer le module d'extension

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.

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 Service Catalog [KB0751715] de la Now Support Base de connaissances.

Configuration du stockage des informations d'identification externe

Configurez votre instance pour obtenir des 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 externes à la fois : un outil de résolution d'informations d'identification CyberArk par défaut et un programme de résolution d'informations d'identification externe personnalisé. La création d'un résolveur d'informations d'identification CyberArk personnalisé utilise toujours le deuxième coffre-fort externe personnalisé, et aucun coffre-fort 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 à partir du MID Server dans les 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 :

Procédure

Utilisez les modèles fournis sur GitHub ServiceNow ou l'exemple de fichier Java.

> **⚠ ATTENTION :**
> Ces exemples sont fournis uniquement à titre de modèle. **N'utilisez PAS** ce code en production sans le modifier pour votre environnement.

a. Téléchargez les fichiers JAR open source avec les instructions du ServiceNow github :

- 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";
```

```
// 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();
 }
}

 /**
```

```
 * 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'informations d'identification envoyés à partir du MID Server dans les informations d'identification réelles du référentiel.

Avant de commencer
Rôle requis : agent_admin ou admin

Après avoir créé le fichier JAR, importez-le dans l'instance, où il devient accessible au MID Server.

Procédure

1. Après avoir créé le fichier JAR et les fichiers de propriétés, copiez le fichier de propriétés sur le MID Server.
2. Accédez à la **Serveur MID** > **Fichiers JAR**.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs suivants :

Champ	Description
Nom	Un 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 rôle dans l'instance.

5. Cliquez sur l'icône de trombone dans la bannière et joignez le fichier JAR à l'enregistrement.

Example

Joindre un fichier JAR

6. Cliquez sur **Envoyer**.
7. Redémarrez le service MID Server.
   La plateforme met le fichier JAR à la disposition de n'importe quel MID Server configuré pour communiquer avec l'instance.

Configurer l'identificateur des 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 détection du stockage des informations d'identification externe est activée.

Procédure

1. Accédez à la **Tous** > **Détection** > **Identifiants** ou **Orchestration** > **Identifiants**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez un type d'informations d'identification.
4. Cochez la case **Banque d'identifiants externes** .
   Les champs **Nom d'utilisateur** et **Mot de passe** disparaissent, et les menus **Champ ID d'informations d'identification** et **Coffre de stockage des informations d'identification** apparaissent.

5. Dans le menu **Coffre-fort de stockage des informations d'identification** , sélectionnez Aucun, le coffre-fort CyberArk ou un coffre-fort de stockage d'informations d'identification externe personnalisé.

   Remarque :

   Si CyberArk vault est sélectionné, le menu **Clé de recherche** s'affiche avec quatre choix de clés de recherche : ID d'informations d'identification, Clé de recherche, FQDN et Tous les éléments ci-dessus. La sélection de toutes les options ci-dessus peut dégrader les performances, car elle nécessite d'accéder au coffre plusieurs fois.

   a. Pour utiliser un coffre de stockage des informations d'identification externes personnalisé, accédez à Configurations du coffre [vault_configuration.list] dans l'instance.

   b. Créez un enregistrement à l'aide d'un nom associé à un fichier JAR importé pour un outil 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 plus d'informations sur la création d'un coffre-fort de stockage des informations d'identification externe personnalisé.

6. Remplissez le formulaire Informations d'identification à l'aide des 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 MID Server 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.

Champ	Description
Chambre forte de stockage des informations d'identification	Choisissez le coffre de stockage des informations d'identification externe dans une liste de coffres disponibles. Le menu est composé d'enregistrements provenant des configurations du coffre-fort [vault_configuration.list]. Vous pouvez ajouter de nouveaux enregistrements et utiliser des noms associés à des fichiers JAR personnalisés pour le programme de résolution des informations d'identification. 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 plus d'informations sur la création d'un coffre-fort 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 (la séquence) selon 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.

7. Cliquez sur **Envoyer**.

Configurer l'identificateur d'informations d'identification pour AWS

Configurez votre instance pour obtenir des 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 MID Server a été installé :

- Discovery (com.snc.discovery)
- Cloud Provisioning and Governance [com.snc.cloud.mgmt]
- Stockage des 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.

Procédure

1. Accédez à la **Tous** > **Détection** > **Identifiants**.
2. Sélectionnez des informations d'identification que votre fournisseur de stockage d'informations d'identification externe prend en charge.
3. Remplissez le formulaire à l'aide des champs de la table.

Champ	Description
Nom	Nom unique et descriptif pour ces informations d'identification. Par exemple, Amazon Web Services.
Concerne	Sélectionnez les MID Servers qui peuvent utiliser ces informations d'identification. Vous pouvez sélectionner **Tous les MID Servers** ou **MID Servers spécifiques**. Si vous sélectionnez cette dernière option, le champ **MID Servers** s'affiche.
Actif	Case à cocher pour activer ou désactiver les informations d'identification.
Compte AWS	Saisissez votre ID de compte AWS si vos informations d'identification AWS se trouvent sur un fournisseur de stockage externe.
Serveurs MID	Sélectionnez un ou plusieurs MID Servers qui peuvent utiliser ces informations d'identification.
ID de certification	Entrez le nom sous lequel ces informations d'identification sont stockées dans le fournisseur de stockage des informations d'identification externe.
ID d'informations d'identification de confidentialité	Saisissez le nom d'une clé de confidentialité SNMPv3 de 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	Sélectionnez un alias pour ces informations d'identification qui contient des comportements spécifiques. Consultez Alias d'informations d'identification pour la détection pour plus d'informations.
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.
Type de banque d'identifiants	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.

4. Cliquez sur **Envoyer**.

CyberArk Intégration de stockage des informations d'identification

L'intégration Serveur MID avec le CyberArk coffre permet ServiceNow® Orchestrationà , ServiceNow® Détectionet ServiceNow® Mappage des services de s'exécuter sans stocker d'informations d'identification sur l'instance.

Introduction à CyberArk

CyberArk Le produit Application Identity Management (AIM) utilise la solution de sécurité des comptes privilégiés pour éliminer le besoin de stocker les mots de passe d'application intégrés dans les applications, les scripts ou les fichiers de configuration, et permet à ces mots de passe hautement sensibles d'être stockés, consignés et gérés de manière centralisée dans le CyberArk coffre-fort. Cette approche permet aux organisations de se conformer aux exigences internes et réglementaires en matière 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 conserve un identificateur unique pour chaque information d'identification, le type d'informations d'identification (tel que SSH, SNMP ou Windows), ainsi que toutes les relations d'informations d'identification. Le service obtient Serveur MID l'identificateur d'informations d'identification, le type d'informations d'identification et l'adresse IP à partir de l'instance, puis utilise le CyberArk coffre-fort 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.

L'intégration CyberArk nécessite le ServiceNow® module d'extension Stockage des informations d'identification externe, qui est disponible dans **Définitions du système** > **Modules d'extension**. CyberArk Le Serveur MID client et le client AIM/API doivent être installés sur le même ordinateur. Les fournisseurs d'informations d'identification CyberArk Application Access Manager (AAM) version 12.0.1 et versions ultérieures sont pris 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 de voir la colonne ID d'informations d'identification dans la liste.
  - Indique à l'utilisateur Serveur MID d'actualiser son cache d'informations d'identification non externes en vue de changer 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 Détection** > **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 externe 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 redéfinit pas les enregistrements d'informations d'identification externes comme étant actifs. Vous devez réactiver manuellement chaque enregistrement d'informations d'identification.

Types d'informations d'identification pris en charge

L'intégration CyberArk prend en charge les types d'informations d'identification suivants ServiceNow :

- 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

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 en savoir plus, consultez Résolveur d'informations d'identification GCP ServiceNow à l'aide de CyberArk .

Now Platform Les fonctionnalités qui utilisent ces protocoles réseau prennent également en charge l'utilisation des informations d'identification stockées sur un CyberArk coffre-fort.

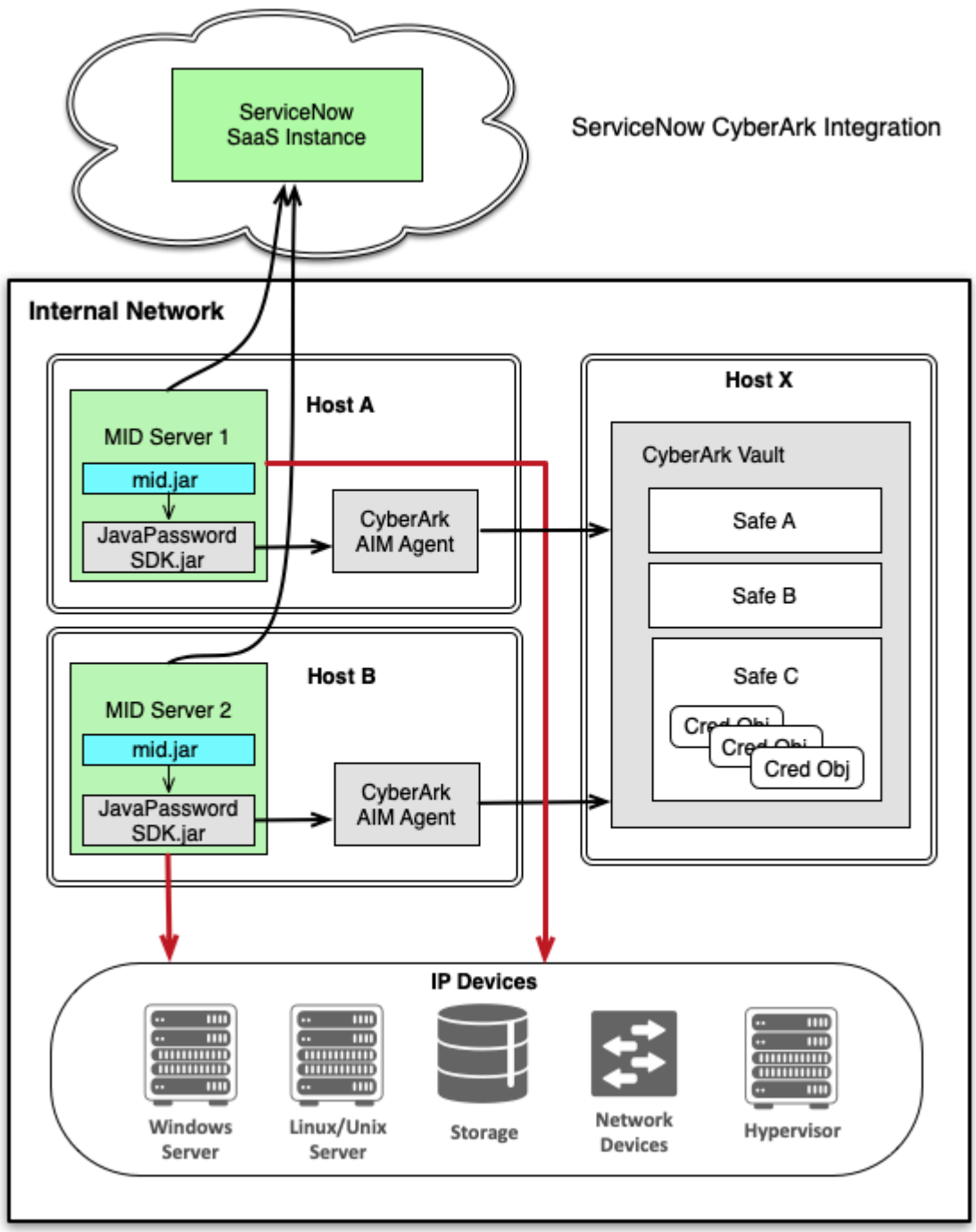
Informations d'identification prises en charge par le protocole réseau

Protocole réseau	ServiceNow® Concepteur de flux 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-fort et un système de stockage d'informations d'identification externe personnalisé à l'aide du même Serveur MID. CyberArk Le Serveur MID client et le client AIM/API doivent être installés sur le même ordinateur.

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 gère Serveur MID 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** du

CyberArk coffre-fort. Si une correspondance est trouvée, les 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'adresses IP correspond à plusieurs informations d'identification, par exemple Windows sur Tomcat le même serveur, la recherche échoue. Pour éviter ce problème, définissez le paramètre dans le *ext.cred.type_specifier*Serveur MID fichier config.xml **sur true** pour forcer CyberArk le renvoi des 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'informations d'identification de renvoie uniquement les Windows informations d'identificationWindows.

Configuration de l'intégration de CyberArk

Ces procédures comprennent à la fois des tâches de configuration CyberArk et ServiceNow, y compris des références à la documentation CyberArk appropriée.

L'identificateur d'informations d'identification configuré dans l'instance ServiceNow doit être mappé au nom des informations d'identification dans le coffre-fort CyberArk. Lors de la recherche d'informations d'identification, le MID Server 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 MID Server 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. C'est le cas, par exemple, lorsqu'un serveur Windows et vCenter s'exécutent tous deux sur la même adresse IP. Pour prendre en charge les exigences strictes en matière d'informations d'identification dans un environnement SSH, un paramètre de configuration du MID Server vous permet d'exiger que le type d'informations d'identification demandé corresponde au type renvoyé par CyberArk.

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 d'informations d'identification SNMPv3 et de l'utilisation 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 en vue d'obtenir des informations d'identification à partir 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 autoriser l'accès au MID Server et installez l'API AIM de CyberArk sur l'ordinateur du MID Server.

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 fournisseurs d'informations d'identification CyberArk Application Access Manager (AAM) version 12.0.1 et versions ultérieures sont pris en charge.

Procédure

1. Configurez le coffre-fort CyberArk avec l'ID d'application et les détails d'authentification que tous les MID Servers demandant des informations d'identification utiliseront.
   Pour plus de détails, reportez-vous au Guide de mise en œuvre de CyberArk pour les fournisseurs d'informations d'identification et l'ASCP.

   a. Assurez-vous que CyberArk est configuré pour permettre au MID Server d'accéder au coffre-fort en créant un identifiant d'application dans CyberArk appelé `ServiceNow_MID_Server`.

   b. Assurez-vous que toutes les informations d'identification dont le MID Server a besoin ont accès à l'ID d'application `ServiceNow_MID_Server` .

   Remarque :
   Vous pouvez remplacer **l'ID** d'application ServiceNow_MID_Server par défaut dans le fichier de config.xml du MID Server à l'aide du paramètre ext.cred.app_id . Si vous modifiez la valeur de ce paramètre, veillez à configurer une valeur correspondante dans le coffre-fort.

2. Installez le fournisseur d'informations d'identification CyberArk, y compris l'API AIM, sur chaque ordinateur qui héberge un service MID Server utilisé pour accéder à la banque d'identifiants.
3. Provisionnez des comptes CyberArk et définissez des autorisations pour accéder aux applications.
   Pour plus de détails, reportez-vous au Guide de mise en œuvre de la sécurité des comptes privilégiés de CyberArk.

   a. Dans CyberArk Password Safe, créez les comptes privilégiés requis par Discovery, 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-forts de mots de passe où les mots de passe de l'application sont stockés.

Importer le fichier JAR de CyberArk

Importez le fichier JavaPasswordSDK.jar CyberArk dans l'instance pour le rendre accessible au MID Server.

Avant de commencer

Rôle requis : agent_admin ou admin

Avant de commencer cette procédure, assurez-vous que CyberArk est configuré pour permettre au MID Server d'accéder aux informations d'identification. Assurez-vous que l'API AIM de CyberArk est installée sur chaque serveur hébergeant un MID Server utilisé pour accéder au coffre-fort.

Pourquoi et quand exécuter cette tâche

Utilisez ce processus même si le fichier JavaPasswordSDK.jar existe déjà sur le MID Server.

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, le cas échéant.
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 rôle dans l'instance.

4. Joignez le fichier JAR à cet enregistrement.
   Le fichier de JavaPasswordSDK.jar AIM est fourni avec les fichiers d'installation du SDK AIM et se trouve généralement sur le MID Server dans le répertoire d'installation d'AIM à l'adresse <install_dir>/CyberArk/ApplicationPasswordSdk.
5. Cliquez sur **Envoyer**.
6. Redémarrez le service MID Server.
   La plateforme met le fichier JAR à la disposition de n'importe quel MID Server configuré pour communiquer avec l'instance.

Configurer le MID Server pour CyberArk

Configurez le fichier config.xml pour permettre au MID Server d'accéder au coffre-fort CyberArk.

Avant de commencer

Rôle requis : admin

Avant de commencer cette procédure, importez le fichier JavaPasswordSDK.jar dans l'instance.

Procédure

Configurer manuellement le MID Server Ajoutez un fichier de paramètres MID Server 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	NomDeDossier	Dossier à utiliser pour toutes les recherches d'informations d'identification. Par exemple, **root**.
ext.cred.use_cyberark	VRAI	Paramètre booléen indiquant que ce MID Server est intégré à CyberArk.

Paramètres de configuration facultatifs

Paramètre	Valeur	Description
ext.cred.safe_timeout	5 (seconde)	Délai d'expiration de chaque recherche d'informations d'identification dans le coffre-fort, spécifié en secondes.
ext.cred.safe_name	NameOfSafe (en anglais seulement)	Nom sûr par défaut utilisé pour toutes les recherches d'informations d'identification.

Paramètre	Valeur	Description
		Si les paramètres se trouvent dans plusieurs coffres-forts, l'ID d'informations d'identification peut être spécifié au format *<safeName>:<CredentialID>*. Lorsqu'il est configuré de cette manière, le champ **NameOfSafe** est ignoré. Si tous les ID d'informations d'identification sont spécifiés au format pour toutes les informations d'identification externes, laissez de côté le champ **NameOfSafe** . **Remarque :** Par défaut, le caractère séparateur dans ce format est un deux-points. Pour affecter n'importe quel caractère que vous voulez 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 l'autorisation au MID Server d'accéder au coffre-fort CyberArk. La valeur par défaut, **ServiceNow_MID_Server**, doit être définie dans le coffre-fort CyberArk. Vous pouvez utiliser ce paramètre pour remplacer la valeur par défaut et spécifier votre propre App-ID. Si vous modifiez l'ID d'application dans ce paramètre, assurez-vous de configurer CyberArk pour qu'il corresponde.
ext.cred.type_specifier	VRAI	Force une recherche d'adresse IP à renvoyer des informations d'identification qui correspondent à la fois à l'ID de plateforme CyberArk et à l'adresse IP. Par exemple, si une adresse IP est partagée par Windows et Tomcat, les informations d'identification dont l'ID de plateforme commence **par Win** renvoient uniquement les informations d'identification Windows. Lorsque ce paramètre est défini sur true, 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 true, elle nécessite que le type d'informations d'identification SSH retournées par CyberArk corresponde 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 CyberArk pour les informations d'identification SNMPv2

Si votre système utilise SNMPv2, vous pouvez créer un fichier spécial pour mapper l'attribut d'informations d'identification à la chaîne de communauté.

Avant de commencer

Rôle requis : admin

Avant de commencer cette procédure, configurez le MID Server pour qu'il ait accès au coffre-fort CyberArk.

Pourquoi et quand exécuter cette tâche

Remarque :
Si la chaîne de communauté apparaît dans le champ du 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 le code suivant : `SNMPv2.Community=attribute_name`
2. Enregistrez le fichier dans le répertoire `/agent` de votre installation MID Server.
   Lors de la recherche d'informations d'identification, le MID Server tente de trouver cet attribut pour les informations d'identification. Si l'attribut est introuvable, le MID Server recherche alors dans le champ de mot de passe. Si le champ Mot de passe est vide, la recherche d'informations d'identification échoue.

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, vérifiez 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 vrai.

Procédure

1. Accédez à la **Tous** > **Détection** > **Identifiants** ou **Orchestration** > **Identifiants**.
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. Cochez la case **Banque d'identifiants externes** .
   Les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification** .

Remarque :
Si la case à cocher 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** , entrez une expression utilisant l'un de ces formats :
   - Si toutes vos informations d'identification se trouvent dans le même fichier sécurisé, configurez ce nom fiable dans le fichier de config.xml du MID Server 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 réside dans un safe spécifique, définissez l'ID d'informations d'identification comme **<safe> :<credential ID> :<platform ID**>.
   - 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 identifiant de plateforme dans le même coffre-fort, utilisez le format suivant : **::<platform ID**>
   - Si vous souhaitez que CyberArk recherche les informations d'identification dans un coffre-fort configuré à l'aide de l'adresse IP plutôt que de l'identifiant des informations d'identification, laissez ce champ vide. Il s'agit de la bonne pratique pour gérer les installations dans lesquelles chaque serveur dispose d'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.

   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 les 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 SNMPv3 de CyberArk 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 une utilisation par votre instance.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Stockez les informations d'identification en tant que clé SSH dans le coffre-fort CyberArk. Lorsque vous configurez l'accès au coffre sur votre instance, le nom que vous donnez à la clé SSH doit également être utilisé comme ID d'informations d'identification.

Procédure

1. Dans CyberArk, accédez à **Comptes** > **Ajouter une clé SSH**.
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**.
ID de clé d'accès AWS	Saisissez la clé d'accès AWS, telle que fournie par AWS.
Nom d'utilisateur AWS IAM	Saisissez le nom d'utilisateur AWS IAM, tel que configuré dans CyberArk.
Mot de passe	Saisissez la clé d'accès secrète AWS, telle que fournie par AWS.
Nom	Entrez un nom pour cette clé.

3. Choisissez **Save (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 une utilisation 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.

Procédure

1. Connectez-vous à CyberArk en mode Administration.
2. Accédez à l'onglet **Administration** .
3. Dans **Configuration système**, modifiez **Gestion de la plateforme**.
4. Accédez au **modèle de 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. Appliquez les changements.
8. Accédez à la section **Compte** et 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 précédemment modifié.
12. Renseignez les champs **ID client**, **ID de locataire** et **Mot de passe** .
13. Sélectionnez **Enregistrer**.

Algorithmes d'authentification

Vérifier l'identité de l'expéditeur à l'aide d'algorithmes d'authentification

Autorisez les étapes d'intégration à s'authentifier avec 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 Étapes d'intégration

Types d'algorithmes d'authentification

- **Amazon Signature Version 4** : il s'agit d'un algorithme d'authentification prédéfini pour 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 une partie des scripts d'instance 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 d'une signature AWS V4 ou d'une authentification personnalisée envoyée avec une demande sortante.
RequestAuthAWSV4Signataire	Script étendant RequestAuthInternal pour implémenter le signataire afin de générer une signature AWS V4.
RequestAuthTwitterSignataire	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 une partie des scripts MID de la *ecc_agent_script_include* table.

Scripts d'authentification MID

RequestAuthInternal	Script en lecture seule sur MID, qui prend en charge la génération de signature AWS V4 ou d'une authentification personnalisée envoyée avec une demande sortante.
RequestAuthAWSV4MIDSigner	Script étendant RequestAuthInternal pour implémenter le signataire afin de générer une signature AWS V4.
RequestAuthTwitterSignataire	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.

API JavaScript

Voici les API JavaScript pour l'algorithme d'authentification.

- AuthCredential (Informations d'identification auth)
- HttpRequestAuthedData
- Données de demande de données
- RequestAuthAPI (API d'authentification de demande)

Configurer un algorithme d'authentification

Configurez un algorithme d'authentification afin de pouvoir signer les requêtes HTTP sortantes.

Avant de commencer

Vous devez avoir configuré un script include 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. Renseignez les champs du formulaire.
   La sélection de la base de données dans le champ **Format** détermine quels champs sont disponibles.

Formulaire d'authentification

Champ	Description
Nom	Nom unique de cet algorithme.
Algorithme	Type de demande sortante.
Description	Description de l'action de votre algorithme.
Application	Périmètre dans lequel votre application s'exécute.
Script d'authentification d'instance	Script que vous sélectionnez dans la table Script Includes.
Script d'authentification MID	Script que vous sélectionnez dans la table Script Includes de MID Server [vue Discovery].

3. Cliquez sur **Envoyer**.

Configurer un algorithme personnalisé basé sur les Amazon signatures

Générez les données basées sur les signatures nécessaires pour vous authentifier auprès d'un service Web en exécutant le Amazon script.

Avant de commencer

- Connaissances JavaScript
- Base de connaissances REST
- Base de connaissances de l'API de service Web cible
- Connaissances sur les connexions, les informations d'identification et les alias
- Rôle requis : développeur

Pourquoi et quand exécuter cette tâche

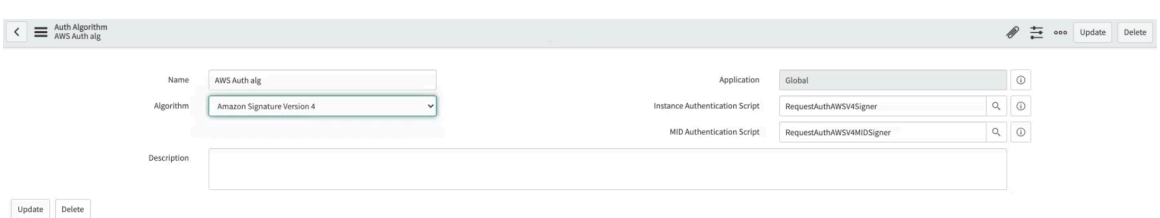
Utilisez un alias de connexion et d'informations d'identification et Amazon un algorithme basé sur la version de signature 4 pour l'authentification.

Procédure

1. Accédez à la **Tous** > **Informations d'identification et connexions** > **Algorithmes d'authentification**, puis cliquez sur **Nouveau**.
2. Renseignez les champs du formulaire.
   La sélection de la base de données dans le champ **Format** détermine quels champs sont disponibles.

Formulaire d'authentification

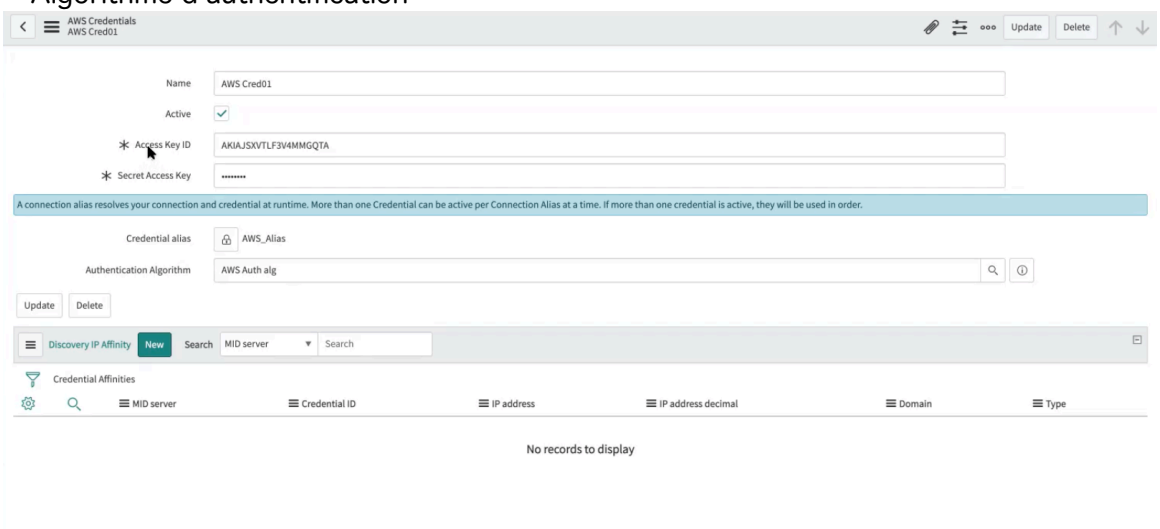
Champ	Description
Nom	Nom unique de cet algorithme.
Algorithme	Type de demande sortante. Sélectionnez **Amazon Signature Version 4**.
Description	Description de l'action de votre algorithme.
Application	Périmètre dans lequel votre application s'exécute.
Script d'authentification d'instance	Script que vous sélectionnez dans la table Script Includes. Dans le cas de l'algorithme **Amazon Signature Version 4** , choisissez **RequestAuthAWSV4Signer**. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signataire ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSignataire **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'origine accessible, le script, etc., s'affichent.
Script d'authentification MID	Script que vous sélectionnez dans la table Script Includes de MID Server [vue Discovery]. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signataire ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSignataire



3. Cliquez sur **Mettre à jour**.
4. Accédez à la **Tous** > **Connexions et informations d'identification** > **Identifiants**.
5. Cliquez sur **Nouveau**.
6. Créez AWS des 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 **clé d'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 du ServiceNow fournisseur (dans ce cas).AWS

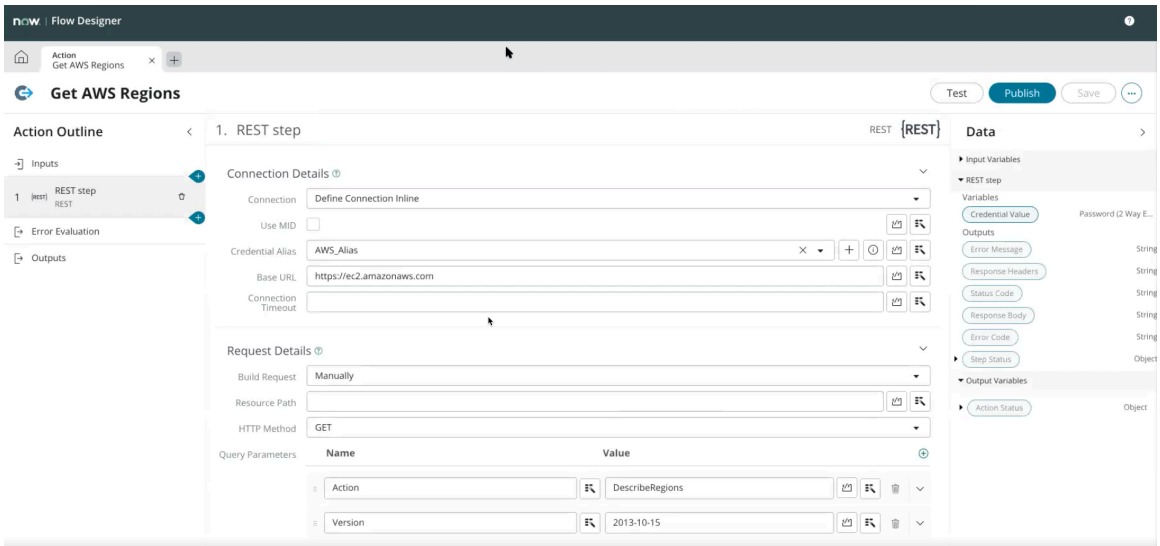
Example: Étape REST avec AWS

Remarque :
Amazon L'authentification basée sur les signatures V4 peut également être utilisée à partir de l'arrière-plan de script.

Action : obtenir les AWS régions

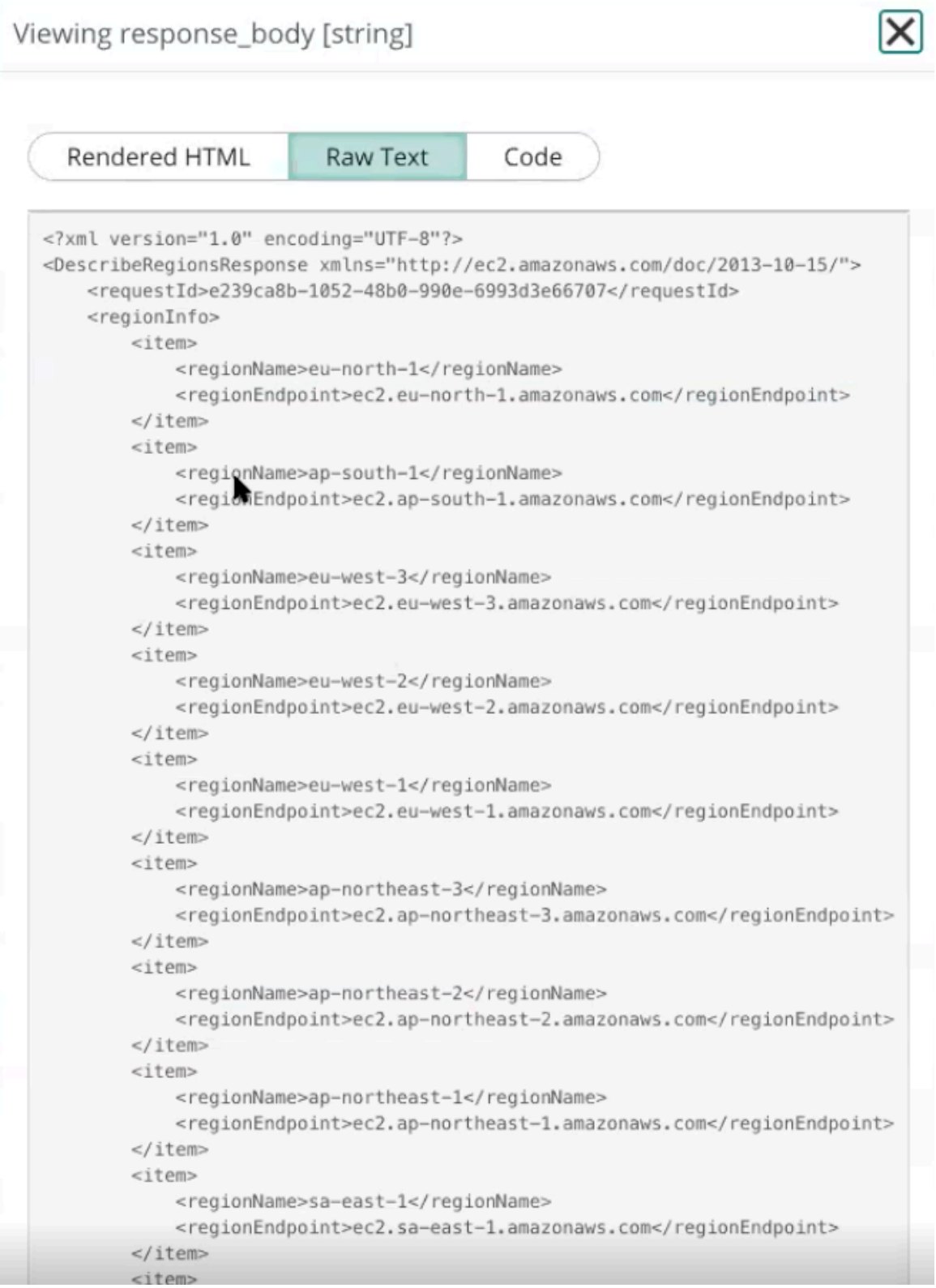
Entrez l'étape REST comme AWS suit :

- **Alias d'informations d'identification** : 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



Amazon V4 est défini avec un ensemble standard d'algorithmes qui prend en charge le mécanisme d'authentification. Cet algorithme, lorsqu'il est utilisé, ajoute la signature comme en-tête d'autorisation pour l'authentification (demande 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 le script.

Avant de commencer

- Connaissances JavaScript
- Base de connaissances REST
- Base de connaissances de l'API de service Web cible
- Connaissances sur les connexions, les informations d'identification et les alias
- Rôle requis : développeur

Pourquoi et quand exécuter cette tâche

Utilisez un alias de connexion et d'informations d'identification et un algorithme d'authentification personnalisé pour l'authentification.

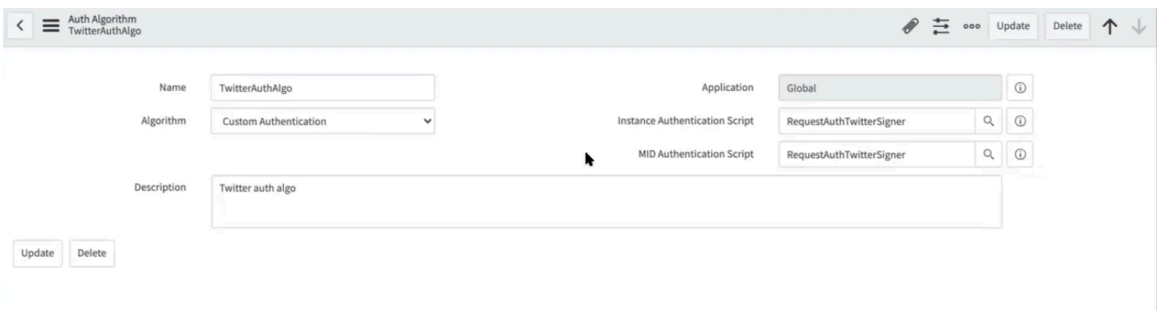
Procédure

1. Accédez à la **Tous** > **Informations d'identification et connexions** > **Algorithmes d'authentification**, puis cliquez sur **Nouveau**.
2. Renseignez les champs du formulaire.
   La sélection de la base de données dans le champ **Format** détermine quels champs sont disponibles.

Formulaire d'authentification

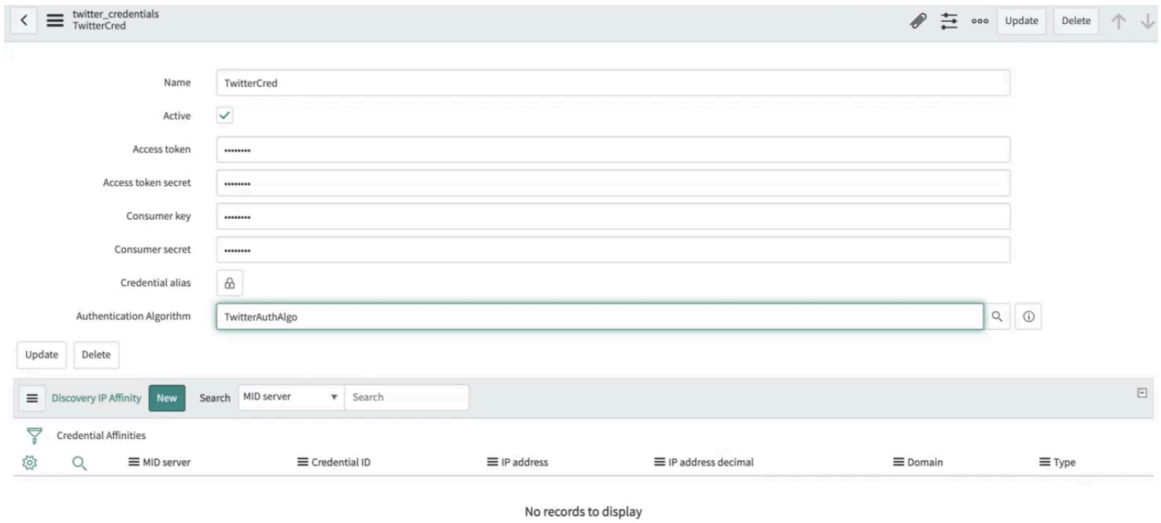
Champ	Description
Nom	Nom unique de cet algorithme.
Algorithme	Type de demande sortante. Sélectionnez **Authentification personnalisée**.
Description	Description de l'action de votre algorithme.
Application	Périmètre dans lequel votre application s'exécute.
Script d'authentification d'instance	Script que vous sélectionnez dans la table Script Includes. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signataire ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSignataire **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'origine accessible, le script, etc., s'affichent. ○ Dans le cas d'une 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** et **le jeton d'accès et le secret** qui peuvent être utilisées pour créer des signatures à transmettre dans un en-tête d'autorisation. Pour plus d'informations, consultez Authentification dans Twitter .

Champ	Description
Script d'authentification MID	Script que vous sélectionnez dans la table Script Includes de MID Server [vue Discovery]. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signataire ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSignataire



En fonction des scripts et de l'algorithme d'authentification sélectionnés, les informations d'identification configurées sont envoyées en tant que demande sortante du ServiceNow fournisseur.

3. Cliquez sur **Mettre à jour**.
4. Accédez à la **Tous** > **Connexions et informations d'identification** > **Identifiants**.
5. Cliquez sur **Nouveau**.
6. Créez Twitter des informations d'identification avec l'algorithme d'authentification.
   En l'occurrence, **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



8. Cliquez sur **Mettre à jour**.

Example: Étape REST avec Twitter

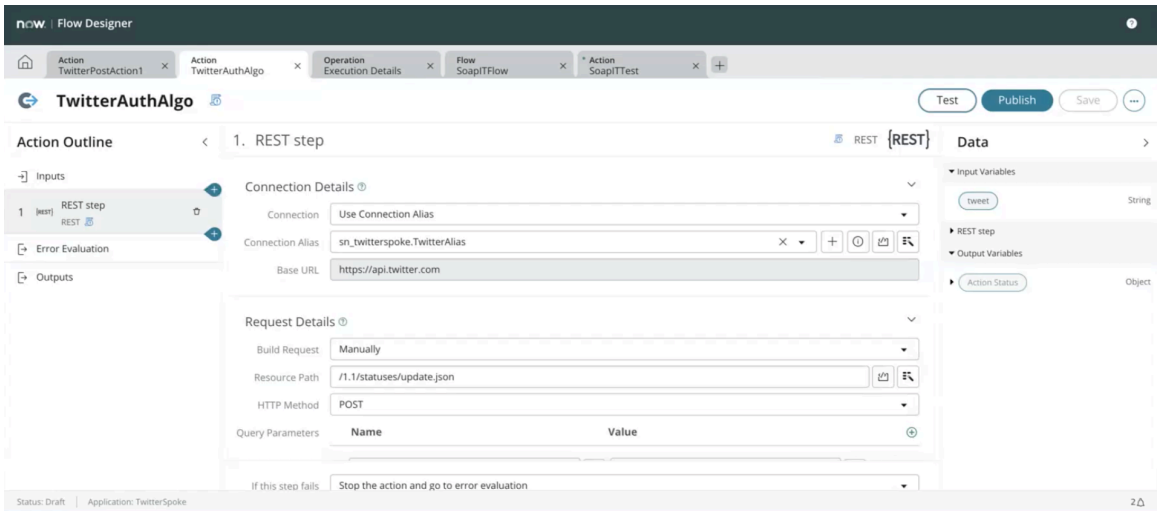
Dans le cas de Twitter, vous devez vous assurer que les spokes ou informations d'identification suivants sont disponibles :

- Jeton d'accès
- Secret du jeton d'accès
- Clé du consommateur
- Secret du consommateur
- Algorithme d'authentification

Mesure : TwitterAuthAlgo.

Entrez l'étape REST comme Twitter suit :

- **Alias d'informations d'identification** : 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. Publier un tweet.
- **Paramètres de requête** : **Action** en tant que **tweet**.



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 Détection de mémoriser le dernier port de l'adresse IP ayant été détecté. Par défaut, cette propriété est définie sur **faux**.

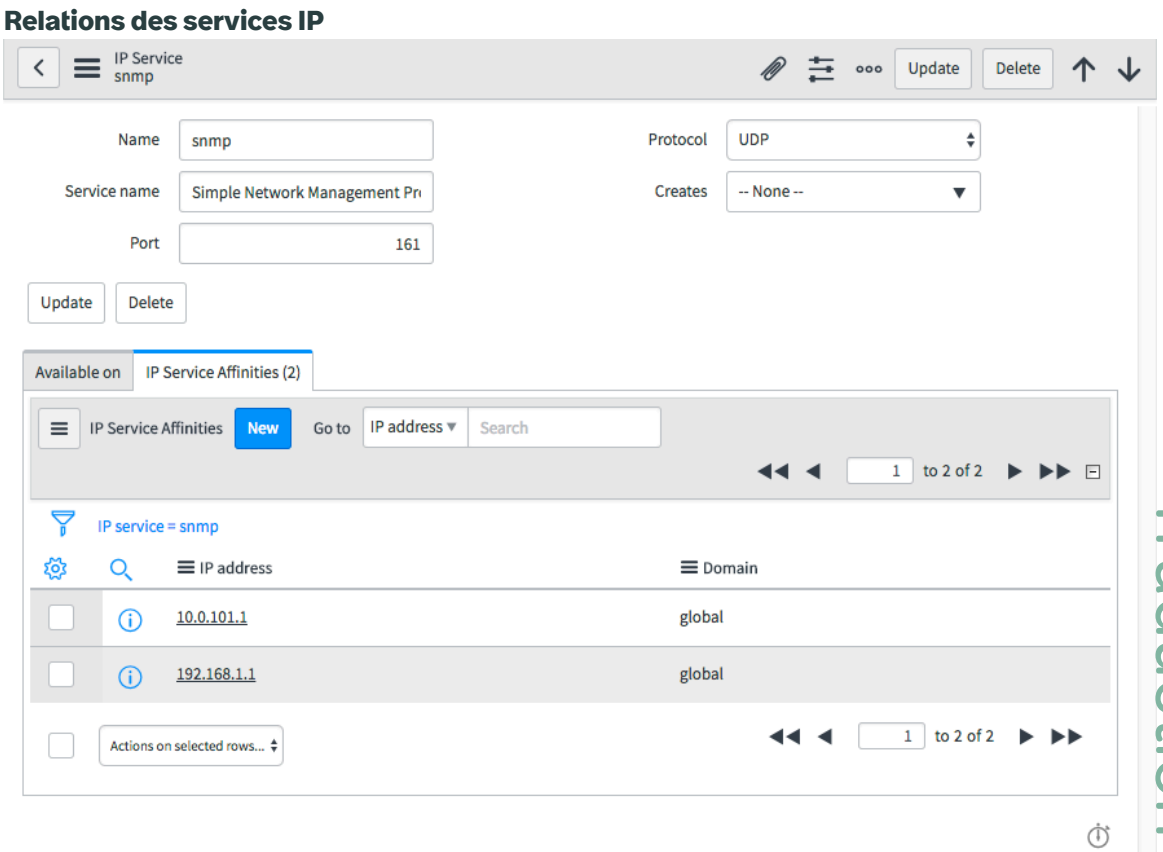
Important :
Vous ne devez pas modifier les services IP à moins que votre organisation n'utilise des ports personnalisés.

Procédure

1. Accédez à la **Tous** > **Définition de Détection** > **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

4. Cliquez sur l'onglet **Relations des services IP** pour obtenir la liste d'adresses IP associées à ce service.



Sécurité de connexion et d'authentification

Configurez les options de sécurité de connexion pour contrôler l'accès à votre instance.

Explorer la sécurité de connexion et d'authentification

Configurez votre sécurité de connexion

Découvrez les fonctionnalités et les valeurs commerciales de la sécurité de connexion.

Découvrez comment configurer la sécurité de connexion.

Définir des scénarios de connexion

Définir des scénarios de connexion.

Réinitialisation du mot de passe

En savoir plus sur la réinitialisation des mots de passe de connexion.

Traduction automatique

Découverte de la sécurité de connexion et d'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 la connexion et de l'authentification des utilisateurs :

Fonctionnalité	Description	Rubriques connexes
Contrôles de connexion et de déconnexion	Contrôlez plusieurs dimensions du processus de connexion et de déconnexion pour les utilisateurs, telles que la spécification d'une page de destination à laquelle l'utilisateur accède en se connectant et contrôlez la façon dont les utilisateurs se déconnectent.	• Définir des scénarios de connexion • Configuration de l'invite de confirmation de déconnexion

Fonctionnalité	Description	Rubriques connexes
		• Supprimer le bouton Déconnexion • Sorties d'installation • Spécifier le verrouillage en cas d'échec de tentative de connexion
Sécurité de l'authentification	Contrôlez le processus de réinitialisation du mot de passe et les 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 par synthèse d'authentification unique.	• Configuration de votre politique de mot de passe • Renforcer les règles de validation des mots de passe • Exemple de référence : Processus en libre-service Réinitialisation du mot de passe par défaut • Modifier les paramètres de la case à cocher Mémoriser mon nom et du cookie • Authentification basée sur la plage IP • Implémentation d'une valeur de circonstance

Configuration de 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 fonctionne uniquement 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 **Demander à l'utilisateur de 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.

Configurer Réinitialisation du mot de passe les propriétés

Vous pouvez spécifier des propriétés qui configurent l'expérience pour les 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 entrer pour les propriétés, envisagez d'utiliser uniquement des valeurs entières positives à partir de 1. Lorsque vous déterminez la limite de la plage supérieure d'une propriété, tenez compte de la tâche que l'utilisateur accomplit.

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 voulez peut-être pas obliger 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 plus d'informations sur les Réinitialisation du mot de passe propriétés, voir Réinitialisation du mot de passe Propriétés globales .
2. Mettez à jour les paramètres selon vos besoins, puis cliquez sur **Enregistrer**.

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 actions suivantes :

1. Accède à la valeur de la propriété `glide.entry.page.script`. La valeur par défaut de la propriété est dérivée d'un script include 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, des règles de connexion s'appliquent. Si cette valeur est nulle, le système utilise navpage.do comme page d'entrée. N'entrez pas de page de connexion ici ; Dans le cas contraire, les utilisateurs doivent se connecter deux fois.

   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 global unique (sys_id), tel que http://{instance}.service-now.com/incident.do?sys_id={sys_id}, le système effectue les actions 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 actions suivantes :

   - S'il y a une valeur dans le champ *Page de connexion* sur le portail de services ou le formulaire de site CMS, elle 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, elle dirige l'utilisateur vers la valeur dans le champ *Page d'accueil* du formulaire du portail de services ou du site CMS.

   Connexion au Service Portal ou à un site CMS pour accéder à un enregistrement :

   Lorsque les utilisateurs se connectent au Service Portal 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 redirige finalement l'utilisateur vers l'enregistrement. Si l'utilisateur ne dispose pas des droits d'accès à l'enregistrement, un message de refus d'accès s'affiche.

Identifiants et portail libre-service employé

Le système garde la trace de la première page de démarrage à laquelle un utilisateur tente d'accéder, même s'il souhaite se connecter au portail libre-service Employés.

Examinez les scénarios suivants.

Exemple 1 :

1. Un utilisateur n'est pas connecté et tente ensuite 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 tente d'accéder à un autre site, tel que le portail libre-service employé (/ess).

4. Le système redirige à nouveau 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, plutôt que vers le portail libre-service Employés.

Exemple 2 :

1. Un utilisateur n'est pas connecté et tente ensuite d'accéder à un enregistrement à l'aide d'un ID système spécifique dans l'URL via le portail libre-service employé (/ess).
2. Le système redirige l'utilisateur vers la page de connexion.
3. Plutôt que de se connecter, l'utilisateur tente d'accéder à un autre enregistrement via le portail libre-service des employés.
4. Le système redirige à nouveau 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 Content Management.

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** , entrez le nom de la page que tous les utilisateurs voient lors de la connexion.

   Utilisez <nom de la page>.do ; vous pouvez omettre la partie http ://"instance".service-now.com/ de l'URL. Pour déterminer le nom de la 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 du tableau de bord, définissez la propriété sur $dashboards.do ?dashboard=<SYS_ID>. Remplacez <SYS_ID> par la sys_id du tableau de bord.

   Pour diriger les utilisateurs vers le portail de services, définissez la propriété sur /sp

   Remarque :
   Cette propriété s'applique à l'ensemble du système, donc sa définition affecte tous les utilisateurs. Pour définir une connexion spécifique pour les utilisateurs n'ayant aucun rôle, 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 Content Management.

Spécifier le verrouillage en cas d'échec de tentative de connexion

Le système fournit des actions de script inactives qui vous permettent de spécifier le nombre de tentatives de connexion infructueuses avant qu'un compte utilisateur ne soit verrouillé et de réinitialiser ce 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.

Remarque :
À partir de la Kingston version, après un zBoot, les actions des scripts **SNC User Lockout Check avec Auto Unlock** et **SNC User Clear** sont activées.

Pour en savoir plus sur les propriétés qui affectent les tentatives de connexion infructueuses, consultez Gestion des tentatives de connexion infructueuses (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 échecs de tentatives de connexion. • 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 de tentatives de connexion infructueuses et verrouille le compte utilisateur après un nombre spécifié de tentatives de connexion infructueuses (par défaut : 5).
Effacer l'utilisateur SNC	Met à jour l'enregistrement utilisateur après une connexion réussie : réinitialise le nombre de tentatives de connexion infructueuses 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 échouées.

1. Accédez à la **Politique système** > **Journaux des événements**.
2. Filtre **pour login.failed** dans le champ **Nom** . Vous pouvez afficher le nom, la date et l'adresse IP de la tentative de connexion journalisés 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 besoin de se connecter pour les afficher, telles que 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.

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 si vous souhaitez que la page soit privée.

4. Cliquez sur **Enregistrer**.
   Si vous définissez active sur true, la page devient publique et toute personne visitant `<instance_name>/sp` ou `<instance_name>/$sp.do` peut y accéder.

Exemple de référence : Processus en libre-service Réinitialisation du mot de passe par défaut

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 d'agents du Service Desk.

Example: Flux de réinitialisation de 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 s'agit bien de 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 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 ses 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.expiry**).
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 les éléments suivants :

- 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 - Saisir l'adresse e-mail qui spécifie le flux de réinitialisation du mot de passe en trois étapes.

Consultez Configurer votre processus de réinitialisation de 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 saisissent 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 les mots 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. Reportez-vous à la section Notifications basées sur l'abonnement . Les administrateurs peuvent 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 la 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 obtenir des informations sur la configuration d'autres aspects de la notification, consultez Créer une notification par e-mail .

Supprimer le bouton Déconnexion

Vous pouvez supprimer le bouton **Déconnexion** pour éviter les déconnexions involontaires.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Remarque :
La procédure suivante ne fonctionne pas dans Interface utilisateur principale.

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Préférences utilisateur**.
2. Supprimez la préférence `user.can.logout`système.

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 et mot de passe et s'authentifie avec l'objet utilisateur
Déconnecter	Dirige l'utilisateur vers la page d'accueil lorsqu'il se déconnecte ; peut être remplacé par LogoutRedirect
LogoutRedirect	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	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
ValidatePassword (ValiderMot de passe)	Active par défaut, à partir de la Helsinki version ; permet aux clients de définir leur propre validation de mot de passe ; peut être remplacée par ValidatePasswordStronger
ValiderMot de passePlus fort	Exige que les mots de passe comprennent au moins 8 caractères dont un chiffre, une lettre majuscule et une lettre minuscule

Sortie de l'installation	Description
GetIntegrationSessionTimeout	Implémente le comportement par défaut du délai d'expiration de la session d'intégration.

Modifications de connexion

La modification suivante apportée à la sortie **d'installation de connexion** définit la valeur de délai d'expiration de session de chaque utilisateur au moment où l'utilisateur se connecte. Dans cet exemple particulier, si le nom d'utilisateur est *admin*, la session expire au bout de 30 secondes.

```
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 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
        // 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

Appliquer des mots de passe forts

Renforcer les règles de validation des mots de passe

Vous pouvez personnaliser les règles de validation du niveau de sécurité du mot de passe pour l'écran de changement du mot de passe en remplaçant la sortie d'installation associée à la validation du mot de passe.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Sorties d'installation**.
2. Localisez **ValidatePassword** (inactif par défaut) et **ValidatePasswordStronger** (actif par défaut, à partir de la Helsinki version).
3. Le script `ValidatePasswordStronger` (ci-dessous) est un exemple de script qui remplace le script `ValidatePassword` à l'aide d'expressions régulières pour exiger que les mots de passe comportent au moins 8 caractères, qu'ils contiennent un chiffre numérique et qu'ils contiennent des majuscules et des majuscules.

```
gs.include("PrototypeServer");
 var ValidatePasswordStronger = Class.create();
 ValidatePasswordStronger.prototype = {
     process : function() {
       var user_password = request.getParameter("user_password");
       var min_len = 8;
       var rules = "Password must be at least " + min_len +
         " characters long and contain a digit, an uppercase letter, and a lowercase letter.";
       if (user_password.length() < min_len) {
         gs.addErrorMessage("TOO SHORT: " + rules);
         return false;
       }
       var digit_pattern = new RegExp("[0-9]", "g");
       if (!digit_pattern.test(user_password)) {
         gs.addErrorMessage("DIGIT MISSING: " + rules);
         return false;
       }
       var upper_pattern = new RegExp("[A-Z]", "g");
       if (!upper_pattern.test(user_password)) {
         gs.addErrorMessage("UPPERCASE MISSING: " + rules);
         return false;
       }
       var lower_pattern = new RegExp("[a-z]", "g");
       if (!lower_pattern.test(user_password)) {
         gs.addErrorMessage("LOWERCASE MISSING: " + rules);
         return false;
       }
       return true; // password is OK
     }
 }
```

La variable de script créée par `Class.create()` doit avoir le même nom que la sortie d'installation elle-même – « ValidatePasswordStronger » dans cet exemple. Le script implémente la fonction `process()` qui renvoie true si le mot de passe est acceptable et false si le mot de passe doit être révisé. La fonction `gs.addErrorMessage` peut être utilisée pour renvoyer des messages d'erreur sur l'écran de changement de mot de passe. Vous pouvez essayer cette sortie d'installation dans votre instance en cochant

le marqueur *actif* et en mettant à jour l'enregistrement. Assurez-vous de vider le cache après avoir fait cela afin que le changement soit reconnu.

Gardez également à l'esprit que la modification de ces scripts ne modifie pas le comportement par défaut ServiceNow : les mots de passe vides sont toujours interdits par défaut et les champs Mot de passe et Mot de passe de vérification doivent correspondre.

Résultats
Pour effectuer le test, cochez la case **Mot de passe à réinitialiser** sur l'enregistrement d'un utilisateur, puis connectez-vous avec cet utilisateur. La validation aura lieu au moment où l'utilisateur tentera de définir le mot de passe. La validation ne s'applique pas lorsqu'un utilisateur administrateur met directement à jour le mot de passe dans l'enregistrement utilisateur (l'administrateur peut mettre n'importe quoi dans le champ Mot de passe).

Remarque :
L'écran de changement de mot de passe s'applique uniquement aux clients qui n'utilisent pas l'authentification unique et qui ne sont pas intégrés à leur LDAP local.

Modifier les paramètres de la case à cocher Mémoriser mon nom et du cookie

Lorsque la case **à cocher 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 de visites ultérieures.

Si l'utilisateur se déconnecte, le cookie est détruit. La valeur par défaut de la case à cocher **Mémoriser** mon nom est contrôlée par une propriété, et l'affichage ou non de la case à cocher sur la page de connexion est contrôlé par une propriété différente.

Deux propriétés, `glide.ui.user_cookie.life_span_in_days` et `glide.ui.user_cookie.max_life_span_in_days` de contrôler la valeur d'expiration du cookie généré 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 de durée de vie maximale (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 :

- Délai absolu de la session
- Délai d'expiration de la fenêtre de session

Modifier la valeur par défaut de la case à cocher Mémoriser mon nom

Vous pouvez modifier la valeur par défaut de la case à cocher **Mémoriser mon** nom.

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`).

3. Pour définir la valeur par défaut de la case à cocher **Mémoriser mon** nom sur **Non**, décochez la case de propriété.
4. Pour restaurer la valeur par défaut de la case à cocher **Mémoriser** mon nom sur **Oui**, cochez la case de propriété.

Décochez la case Se souvenir de moi

Vous pouvez décocher la case **Mémoriser** mon nom afin 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 **Mémoriser** mon nom, invalide les cookies existants et désactive entièrement la fonctionnalité Se souvenir de moi.
5. Pour restaurer la case à cocher **Mémoriser** mon nom sur la page de connexion, désactivez la case à cocher de la propriété.

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 spécifique ou à une plage d'adresses 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 d'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 :

- Le système ne vous laissera pas vous verrouiller, donc si vous essayez d'ajouter une règle de sorte 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 configuration 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 réellement sur Internet. Votre entreprise proxys et/ou NAT convertit probablement votre adresse en un ensemble prévisible d'adresses sortantes que vous devrez probablement demander à votre équipe réseau.

- Un utilisateur dont l'accès est restreint en fonction d'une règle d'accès reçoit une erreur 403 sur son navigateur.
- Les utilisateurs restreints n'utilisent pas de transactions, de sémaphores et ne comptent pas dans le décompte des 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 accéder à notre centre de données. Il s'agit d'une vérification supplémentaire qui doit être effectuée en plus des contrôles d'accès que nous avons éventuellement mis 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 l'est en fait.
- Les astérisques et les blocs CIDR ne sont actuellement pas pris en charge.
- 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 effectuer le transfert des 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 sur l'adresse IP de votre instance, connectez-vous à ServiceNow - Support NOW et recherchez l'élément de catalogue de services **Mes informations IP** .

Remarque :
Pour en savoir plus sur les propriétés et `glide.ip.authenticate.strict` qui restreignent l'accès `com.snc.ipauthenticator` de l'instance à des plages IP spécifiques, consultez les rubriques suivantes dans Paramètres de renforcement de la sécurité de l'instance :

- Restreindre l'accès à des plages IP spécifiques
- Restriction IP stricte

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 associée n'existe. Par défaut, il n'existe aucune restriction d'accès à votre instance.

Avant de commencer

Rôle requis : admin

Remarque :
Utilisez la politique de contexte de pré-authentification d'Authentification adaptative (AA) pour appliquer des authentifications basées sur IP et des restrictions pour des options supplémentaires. Pour plus d'informations, consultez Authentification adaptative.

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 IP Range Based Authentication [com.snc.ipauthenticator].

2. Complétez le formulaire.

Remarque :
Pour trouver les informations sur l'adresse IP de votre instance, connectez-vous à ServiceNow - Support NOW et recherchez l'élément de catalogue de services **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 interagir avec cette instance que si elle est répertoriée dans une règle d'autorisation. En outre, lors de l'ajout de 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 et assistance client, certaines ServiceNow adresses IP internes ne peuvent pas être bloquées par des règles de refus.
Direction	Direction de la règle de contrôle d'accès IP. ○ **Entrantes** : autorise ou refuse les transactions entrantes. Il s'agit de transactions initiées en dehors de votre instance. ○ **Sortantes** : 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. **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 des adresses IP à autoriser ou refuser. **Remarque :** Pour limiter l'accès à des adresses VPN spécifiques, saisissez une plage de refus comprise entre **0.0.0.0** et **255.255.255.255** dans le champ **Refuser** , et n'entrez que les plages VPN autorisées spécifiques.

3. Cliquez sur **Envoyer**.

Rechercher les adresses IP refusées

Recherchez les adresses IP refusées dans les fichiers journaux du nœud de l'instance.

Avant de commencer
Rôle requis : admin.

Pourquoi et quand exécuter cette tâche
Les entrées de journal pour les adresses IP bloquées 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 du nœud de l'instance visibles, qui ne sont pas visibles à partir des journaux système.

Procédure

1. Accédez à la **Tous** > **Journaux système** > **Utilités** > **Navigateur de fichiers journaux de nœuds.**.
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**.

Implémentation d'une valeur de circonstance

Vous pouvez implémenter un nonce à utiliser avec l'authentification Digest Authentification unique.

Pour utiliser un nonce avec les méthodes de jeton non chiffré ou de jeton chiffré de l'authentification unique, les étapes suivantes s'appliquent avec quelques modifications mineures seulement.

Remarque :
La valeur de circonstance n'est utilisée que pour les demandes de connexion, et non pour tout autre type de demande. Si le système reçoit une valeur de circonstance après la connexion, la valeur de circonstance n'est pas consommée.

Avantages

L'utilisation d'un nonce interdit à un utilisateur malveillant d'effectuer une attaque par relecture afin de se connecter à votre système.

Flux de processus de la valeur de circonstance

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 transfère la réponse d'authentification via la chaîne de requête, elle peut ressembler à quelque chose comme ceci :

```
SM_USER=itil&DE_USER=V1QuWMmxSfBgfRS099X0cAjKo5Q=&NONCE=1407743018
```

L'instance reçoit cette demande et récupère les variables d'authentification. Avant de tenter 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 le nonce n'existe pas dans cette table, il est alors ajouté à la table et le processus d'authentification est autorisé à se poursuivre. Toutefois, si cette valeur de nonce existe déjà dans la table, la tentative d'authentification est annulée et un code d'erreur de failed_missing_requirement est renvoyé, ce qui ramène généralement l'utilisateur à la page de connexion.

Implémenter une valeur de circonstance

Ajoutez un nonce cryptographique à l'en-tête d'authentification pour vous assurer qu'il ne peut être utilisé 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, par exemple NONCE ou NCE.
- Créez une table appelée u_authentication_nonce. Ajoutez un champ à la table appelée 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 portion de script du DigestSingleSignOnNonce nouvellement créé.

```
gs.include("PrototypeServer");

var DigestSingleSignOnNonce = Class.create();
DigestSingleSignOnNonce.prototype = {

 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();
     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";
 }
},
```

Traduction automatique

```
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;
 }
};
```

- Une fois que vous avez enregistré votre nouvelle sortie d'installation, accédez à la sortie d'installation de DigestSingleSignOn et assurez-vous qu'elle est définie sur Active=false.

Votre instance doit maintenant être configurée pour implémenter un nonce.

Sécurité des services Web

Appliquez la sécurité à l'aide de l'authentification de base, de l'authentification réciproque ou de WS-Security.

Explorez la sécurité du Web

Découvrez les fonctionnalités et les valeurs commerciales de la sécurité des services Web.

Configurer l’authentification réciproque

Découvrez comment utiliser et configurer l’authentification réciproque.

Sécurité des services Web

En savoir plus sur la sécurité des services Web.

Traduction automatique

Exploration de la sécurité des services Web

Appliquez la sécurité à l'aide de l'authentification de base, de l'authentification réciproque ou de WS-Security.

Authentification de base

Pour appliquer l'authentification de base à chaque demande de document WSDL ou validation de messages SOAP, vous pouvez définir la propriété *glide.basicauth.required* sur true. Dans ce cas, chaque requête WSDL ou SOAP devra contenir l'en-tête « Autorisation » tel que spécifié dans le protocole d'authentification de base . Étant donné que la demande n'est pas interactive, l'en-tête **d'autorisation** est toujours requis au cours d'une demande.

La fourniture d'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'appel du service Web sont effectuées pour le compte 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 journal affichent 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 script includes nécessaires au traitement de l'authentification. Par défaut, cette propriété comporte les valeurs suivantes :

- BasicAuth
- Authentification personnalisée

Ajoutez d'autres script includes selon vos besoins.

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 par rapport à 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 ) { }
```

- Lors de l'utilisation de 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 les éléments suivants et remplacez `None` par `Basic` :

```
<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
        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 qui en résulte lorsque l'authentification de base est activée et qu'aucune information d'identification n'est fournie ressemble à ce qui suit :

```
<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 >
```

Configuration de l'authentification réciproque

L'authentification mutuelle établit la confiance grâce à l'échange de certificats SSL (Secure Sockets Layer).

Avant de se connecter à un serveur, le client demande un certificat SSL. Le serveur répond en demandant au client d'envoyer son propre certificat. Les deux répondent en validant les certificats et en envoyant des accusés de réception avant d'initier une connexion HTTPS.

Les administrateurs effectuent les tâches préliminaires de configuration d'un magasin de clés et de génération de certificats avant que les demandes de certification ne soient satisfaites.

⚠ Avertissement :
Cette fonctionnalité active uniquement l'authentification réciproque sur les connexions https sortantes.

Création du magasin de clés

L'instance prend actuellement en charge le chargement d'un fichier de magasin de clés Java devant contenir la clé privée, la paire de certificats publics et ses certificats signés.

Les étapes suivantes utilisent des commandes qui vous permettent de générer un nouveau fichier de magasin de clés Java Keytool, de créer une demande de signature de certificat (CSR) et d'importer des certificats. Tous les certificats racines ou intermédiaires doivent être importés avant d'importer le certificat principal pour votre domaine. Tapez ces commandes dans une interface de ligne de commande.

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 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
```

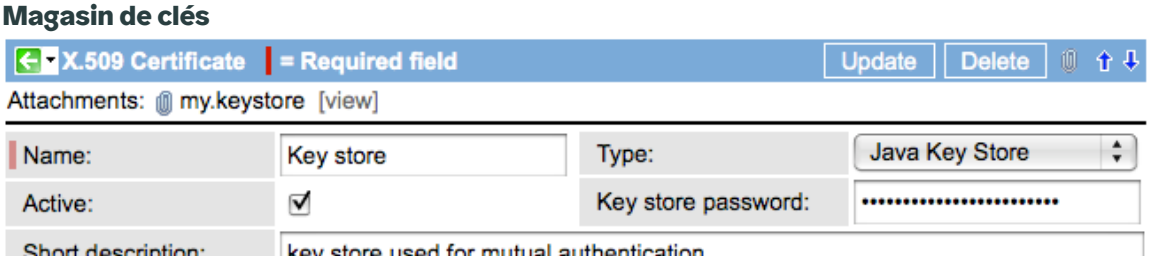
Configurer le magasin de clés

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**.
- **Définissez 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.

Cliquez sur **Envoyer** pour créer l'entrée Java Key Store.

Magasin de clés



Spécification d'un certificat de serveur de confiance

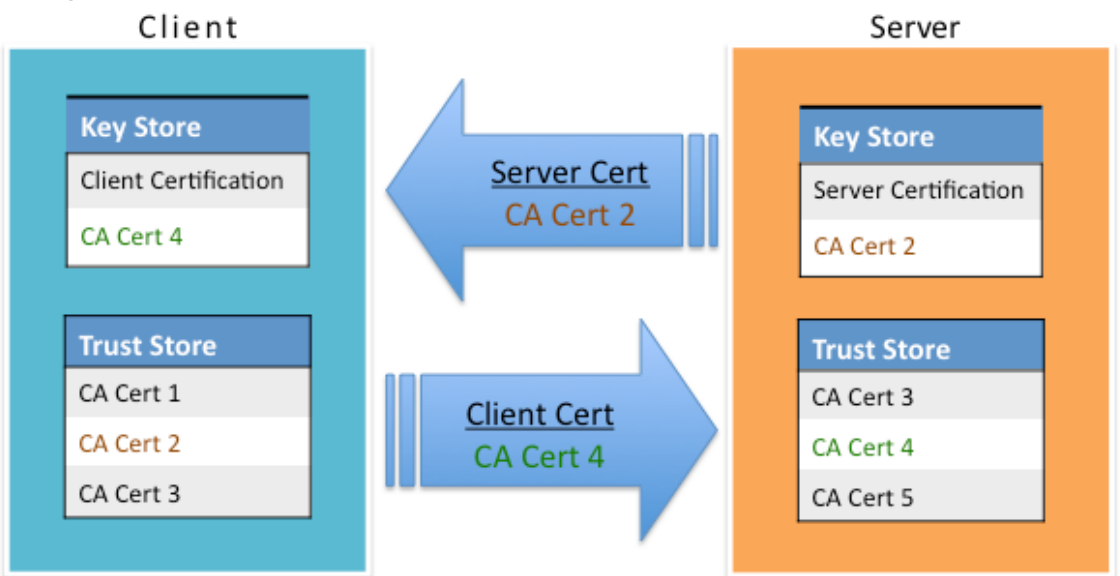
Lors d'une connexion SSL sortante, c'est-à-dire un appel de service Web HTTPS, il est possible de spécifier un certificat fourni par le fournisseur de services qui assure la validité du fournisseur de services lors de la connexion SSL. Par exemple, un navigateur qui tente de se connecter à un service sécurisé et qui s'identifie par un certificat.

En téléchargeant le certificat du serveur approuvé, ServiceNow garantit que le service auquel il se connecte est valide et sécurisé.

Créez une nouvelle entrée de certificat avec le type « Trust Store Cert » et joignez un certificat au format DER, ou copiez-collez son format PEM dans le champ **Certificat PEM** .

Traitement des demandes d'authentification réciproque

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 au 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 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 fait correspondre 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.

Voici un exemple de commande qui enregistre MYHTTPS avec l'usine de sockets `com.glide.certificates.DBKeyStoreSocketFactory` sur le port 443. L'usine de magasins de clés de base de données est utilisée pendant le processus d'échange SSL pour offrir un certificat client pour l'authentification réciproque.

```
glide.httpclient.protocol.myhttps.class = "com.glide.certificates.DBKeyStoreSocketFactory"
glide.httpclient.protocol.myhttps.port = "443"
```

Avoir la configuration ci-dessus affecte toute URL de myhttps://host.domain.com/target sortante pour utiliser l'instanciateur de socket personnalisé et échanger des certificats pendant SSL.

Remarque :
Le remplacement de l'instanciateur de sockets du protocole HTTPS par défaut affecte toutes les connexions HTTPS sortantes. Ce n'est généralement pas souhaitable.

Le serveur répond en envoyant un certificat. S'agit-il d'un certificat accepté par le client ? Si c'est le cas, un message est envoyé au serveur acceptant le certificat et un canal sécurisé est lancé. Si le certificat n'est pas accepté, cela peut signifier que l'autorité racine est nécessaire pour la certification.

Référence : WS-Security

La prise en charge de WS-Security 1.1 sous la forme d'un profil de jeton WSS X.509 et d'un profil de jeton de nom d'utilisateur WSS est disponible pour les demandes SOAP entrantes.

La configuration pour utiliser WS-Security est distincte de l'exigence d'application de l'authentification de base et est appliquée lorsque l'enveloppe SOAP contient les en-têtes WS-Security.

Profils de sécurité WS

Le module **Profil de sécurité WS** répertorie les profils de sécurité WS actuellement en vigueur. **L'ordre** des profils indique l'ordre d'authentification qui est vérifié, tous les profils sont vérifiés lors de la demande SOAP entrante, lorsqu'un profil échoue à l'authentification, il n'exécute pas le suivant dans l'ordre. La case à cocher **Lier la session** indique quel profil utiliser pour assumer l'identité de la session, il ne peut y avoir qu'une seule session « liée ».

Profil de jeton WSS X.509

Utilisez le cadre de travail d'authentification X.509 tel que défini par la spécification Sécurité des services Web : sécurité des messages SOAP. Un certificat X.509 spécifie une liaison entre une clé publique et un ensemble d'attributs qui comprend (au moins) un nom d'objet, un nom d'émetteur, un numéro de série et un intervalle de validité. Un certificat X.509 est utilisé pour valider une clé publique qui est utilisée pour signer le message SOAP entrant. Chargez le certificat dans le module **Certificat** et référencez-le dans le champ **Certificat X509** . S'il s'agit d'une session liée, sélectionnez l'utilisateur dont l'identité doit être empruntée en cas d'échec de l'authentification WS-Security.

Consultez le document suivant : http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf

Profil de jeton de nom d'utilisateur WSS

En plus de spécifier le profil de jeton X.509, un UsernameToken peut également être fourni dans la demande SOAP. Un UsernameToken est utilisé comme moyen d'identifier le demandeur par « nom d'utilisateur » et, éventuellement, à l'aide d'un mot de passe (ou d'un secret partagé ou d'un mot de passe équivalent) pour authentifier cette identité auprès de l'instance. Le profil UsernameToken ne peut pas être utilisé indépendamment du profil de jeton X.509 actuellement.

1. Authentifiez-vous à l'aide du nom d'utilisateur de la demande SOAP entrante pour rechercher un utilisateur par le **champ Utilisateur spécifié afin de faire correspondre la valeur UserName** . La valeur de mot de passe dans le jeton de nom d'utilisateur entrant est utilisée pour authentifier la demande. Lorsque l'option **Lier la session** est sélectionnée, l'utilisateur qui s'authentifie avec succès est utilisé pour la session.
2. Authentifiez-vous à l'aide d'une paire nom d'utilisateur/mot de passe distincte qui n'est pas liée aux utilisateurs de la table Utilisateur. Lorsque l'option **Lier la session** est sélectionnée, l'utilisateur spécifié dans le champ **Exécuter en tant qu'utilisateur** est utilisé pour la session.

Exemples d'en-têtes d'enveloppe SOAP WS-Security

Remarque :

Cet exemple a été formaté avec des retours à la ligne pour adapter le contenu dans le cadre.

```
<SOAP-ENV:Header><wsse:Securityxmlns:wsse =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
SOAP-ENV:mustUnderstand = "1" ><wsse:BinarySecurityTokenxmlns:wsu =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"E
ncodingType =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0
#Base64Binary"ValueType =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X50
9v3"wsu:Id = "CertId-2D914AB929A6719E7F13068829874641"xmlns:wsse =
 "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
 >
  MIIEgzCCA2ugAwIBAgILAQAAAAABLOZQMtEwDQYJKoZIhvcNAQ
  EFBQAwQDEXMBUGA1UEChMOQ3liZXJ0cnVzdCBJbmMxJTAjBg
  NVBAMTHEN5YmVydHJ1c3QgU3VyZWNyZWRlbnRpYWwgQ0Ew
  HhcNMTAxMjE0MTgyMjU1WhcNMTECMjE0MTgyMjU1WjB3MQsw
  CQYDVQQGEwJVUzEUMBIGA1UEChMLU2VydmljZS1Ob3cxKDA
  mBgkqhkiG9w0BCQEWGWRhdmlkLmxvb0BzZXJ2aWNlLW5vdy5jb
  20xKDAmBgNVBAMTH1NlcnZpY2UtTm93IFBhcn3uZXIgRGV2ZWx
  vcG1lbnQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
  AQCvtcRlb6zkGnN9uyhtcSDNSIuCW6FgnTbTDUvw2nGlNA9y9iEV
  wTp5TG3eELOOFBCuRLeY5x28lN+cJ72v+zCwi/rZcbEPj8oWyLVA
  OqJThgrzhDabj0vDM/zU8bvAXcw6FoCUDFKkc64WC7Y4HpBdfW4
  JT7FBgDQ3LEudq80Up+TfETiGwrEA3jRgy9fF92TKD7MN3Vkyhz2
  xZLOFiN5HJixl9juNJmLWugqqIG04yZSuCutc1gjCy0U+f0NXKgh0Q
  rRheNpwcqWbbJvLbR9Ybso6l3UAYCQ09hrRnI7VaPvfiueUvuLopap
  o4Kel6iL8aMUAfEUDtkf1AbqRIIQ5AgMBAAGjggFFMIIBQTAfBgNVH
  SMEGDAWgBRJTJlLzUojts557p5VM2taRMAClTA7BgNVHR8ENDA
  yMDCgLqAshipodHRwOi8vY3JsLm9tbmlyb290LmNvbS9TdXJlQ3JlZ
  GVudGlhbC5jcmwwHQYDVR0OBBYEFB+OqIvcdiYmq0enW6mgaV
  wZp9eaMA8GA1UdEwEB/wQFMAMCAQAwDgYDVR0PAQH/BAQD
  AgTwMBEGCWCGSAGG+EIBAQQEAwIFoDBJBg3rBgEFBQcBA1Q
  9MDswOQYIKwYBBQUHMAKGLWh0dHA6Ly9jYWNlcnQub21uaXJv
  b3QuY29tL3N1cmVjcmVkZW50aWFsLmNydDAkBgNVHREEHTAbg
  RlkYXZpZC5sb29Ac2VydmljZS1ub3cuY29tMB0GA1UdJQQWMBQG
  CCsGAQUFBwMCBggrBgEFBQcDBDANBgkqhkiG9w0BAQUFAAO
  CAQEAmeoP0Bgtx2JN1ldLnnK6WLEqDk25zaHP5wTxqVlFxzJy1zi6
  A0lk5U0T5LKYjjGWRIOoSeK8iBU0p7Mq4PE8QCETkjYNyuWJd9zm
  7GPCHdOoL18rQHQRsU8pTDHA10zG+i3zdxAMrHl/H673E4myzvU
  DkJnxNAZdw4h4Ba/Y1+VFCWhOm2GwZdXtzklyZaKtMp+31qmf3bG
  OSU34M/dW40pXgfLDqdGD+6YDQPg25aYeCqcNhwg6VlAWG566g
  aWXYxRaVj0qotSDMdaK8b+7Vlo7KhGGaE62v7f44OSekJeBvTfZCR
  7zRSK8N+0qUpqP/n8vgDkmYIE5IQrRE0rEWA==
 </wsse:BinarySecurityToken><ds:Signature xmlns:ds =
"http://www.w3.org/2000/09/xmldsig#"Id = "Signature-2" ><ds:SignedInfo xmlns:ds
= "http://www.w3.org/2000/09/xmldsig#" ><ds:CanonicalizationMethodAlgorithm
= "http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:ds =
"http://www.w3.org/2000/09/xmldsig#" /><ds:SignatureMethod
Algorithm = "http://www.w3.org/2000/09/xmldsig#rsa-sha1"xmlns:ds =
"http://www.w3.org/2000/09/xmldsig#" /><ds:Reference URI = "#Timestamp-1"
xmlns:ds = "http://www.w3.org/2000/09/xmldsig#" ><ds:Transforms
xmlns:ds = "http://www.w3.org/2000/09/xmldsig#" ><ds:Transform
Algorithm = "http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:ds =
"http://www.w3.org/2000/09/xmldsig#" /></ds:Transforms><ds:DigestMethod
```

Traduction automatique

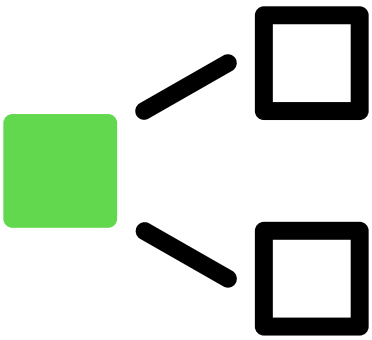
Paramètres généraux de sécurité de la plateforme

En savoir plus sur les paramètres généraux de sécurité de la plateforme.

Options d'analyse antivirus

Utilisez cette fonction Analyse anti-virus 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.

Assainisseur HTML

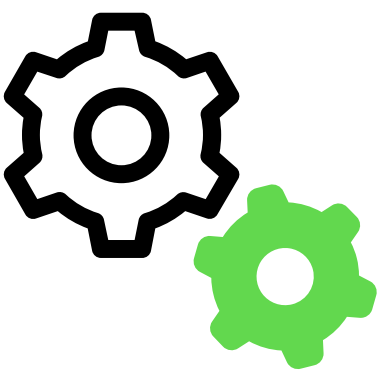


Supprimez tout code indésirable et protégez-vous contre les problèmes de sécurité tels que les attaques de script site à site en assainissant le balisage HTML dans les champs HTML et les champs HTML traduits.

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.

ServiceNow® Contrôle d'accès

VPN (Virtual Private Network)

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

Traduction automatique

Le module d'extension SNC Access Control vous permet de contrôler quels employés Service et assistance client peuvent accéder à votre instance et à quel moment.

Autres paramètres et ressources de sécurité

Définissez des propriétés de sécurité en dehors d'Instance Security Center ainsi que d'autres ressources liées à la sécurité.

Analyse anti-virus

Utilisez Analyse anti-virus 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.

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.

Contrôle d'accès ServiceNow®

Le module d'extension SNC Access Control vous permet de contrôler quels employés Service et assistance client peuvent accéder à votre instance et à quel moment.

Autres paramètres et ressources de sécurité

Définissez des propriétés de sécurité en dehors d'Instance Security Center ainsi que d'autres ressources liées à la sécurité.

VPN (Virtual Private Network)

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

Analyse anti-virus

Utilisez Analyse anti-virus 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 d’Antivirus Scanning.

Configurer la protection antivirus

Apprenez à configurer la protection antivirus.

Traduction automatique

Résoudre les fichiers infectés

Découvrez ce qu'il faut faire avec les fichiers infectés.

Référence pour l'analyse antivirus

En savoir plus sur les attributs du dictionnaire pour l'analyse antivirus.

Traduction automatique

Exploration de l'analyse antivirus

Utilisez Analyse anti-virus 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 anti-virus 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 Analyse antivirus.

Le Protection antivirus module d'extension (com.glide.snap) est activé par défaut sur votre instance. En tant qu'administrateur, vous pouvez désactiver et réactiver la Analyse anti-virus fonctionnalité sur l'ensemble de votre instance d'un simple clic, définir des options de configuration et examiner l'activité antivirus sur l'instance.

Remarque :

- Analyse anti-virus est également disponible pour les clients dans l'environnement Government Community Cloud (GCC) et commercial. Les utilisateurs doivent définir la propriété (com.glide.snap.fed_enable_scan) sur Vrai pour commencer à utiliser la fonctionnalité.
- 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 quotidiennement.
- Tout fichier d'une taille supérieure à 100 Mo n'est pas analysé.

Analyse des e-mails et des pièces jointes

Les e-mails entrants sont analysés pour détecter les éventuels virus par les filtres de messagerie du système, et non par Analyse anti-virus.

Par défaut, seules les pièces jointes jointes aux tables zz_yylive_profile sont analysées. Pour analyser d'autres tables qui ont le type **de colonne file_attachment** créez la propriété `glide.snap.scan.zz_yytable` système et insérez le nom de la table.

Si les noms de table sont zz_yyincident et zz_yycase, la valeur de la propriété doit être `zz_yyincident,zz_yycase`.

Une fois cette propriété définie, les pièces jointes des 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 charge sans le savoir un fichier infecté dans un enregistrement.
2. Le système analyse le fichier et le met en quarantaine.
3. Le fichier apparaît dans la fenêtre Pièces jointes, où il est marqué comme non disponible.
4. L'utilisateur sélectionne le fichier et le message d'erreur suivant s'affiche : La Infected_testing.txt de fichier n'a pas réussi l'analyse de sécurité. Veuillez supprimer le fichier du INC0000059 de l'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 est renvoyé 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 au 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 réussi l'analyse et n'a donc pas été inclus dans le fichier ZIP.
5. L'utilisateur ouvre à nouveau l'enregistrement et constate que le fichier indisponible a été déplacé dans la section **Risques de sécurité potentiels** de la fenêtre Pièces jointes et ne peut pas être téléchargé.

Configurer Analyse anti-virus

Configurez Analyse anti-virus sur l'ensemble de votre instance et au niveau de la table.

Avant de commencer

Rôle requis : antivirus_admin ou admin

Pourquoi et quand exécuter cette tâche

Analyse anti-virus est actif par défaut dans votre instance, où il analyse automatiquement les pièces jointes pour identifier tous les fichiers infectés par des virus. Configurez la fonctionnalité en vous assurant que l'analyse est activée sur l'ensemble de 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 les tables de l'analyse antivirus en les ajoutant à la **liste des tables exclues**.

a. Accéder au **dictionnaire** de **→ de définition du système**

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 `True` dans le champ **Valeur** .

e. Sélectionnez **Envoyer**.

Résultats
Analyse anti-virus est activé dans votre instance et la **liste des tables exclues** de la page Configuration antivirus est renseignée avec toutes les tables que vous avez exclues de l'analyse.

Examen des fichiers mis en quarantaine

Examinez les pièces jointes mises en quarantaine et prenez les mesures nécessaires.

Avant de commencer
Rôle requis : antivirus_admin ou admin

Pourquoi et quand exécuter cette tâche
Surveillez les entrées de vos fichiers mis 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 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 l'entrée en quarantaine de la ligne sélectionnée.

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

Examen de l'activité antivirus

Passez en revue 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 détection, la suppression et d'autres événements possibles de fichier 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. Reportez-vous à la section Examiner les fichiers mis en quarantaine

Connaître les attributs du dictionnaire pour Analyse anti-virus

Les attributs de dictionnaire modifient le comportement de la table ou de l'élément décrit dans l'enregistrement du dictionnaire. En tant qu'administrateur, vous pouvez définir les valeurs des attributs de dictionnaire pour modifier le comportement de la configuration Antivirus Scanning par défaut.

Attributs du dictionnaire pour Analyse anti-virus

Nom	Valeur	Élément cible	Description
Exclude_from_antivirus_scan	vrai/faux	N'importe quelle table	Si vrai, les pièces jointes de fichier de la table sont exclues de l'analyse antivirus. Reportez-vous à la rubrique Configurer Analyse anti-virus.
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.

Information associée

Attributs du dictionnaire

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

Apprenez à configurer l’audit.

Vue

Passez en revue les tables Audit Sys et Changement de relation d’audit.

Référence

Connaître les ensembles d’historique.

Traduction automatique

Découverte de 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.

L'activation de l'audit permet de suivre la création, la mise à jour et la suppression de tous les enregistrements de la table. Si vous souhaitez auditer des champs individuels d'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 :

- La table d'audit .
- La Connaître les ensembles d'historique table.

⚠ Avertissement :
L'audit des tables système qui reçoivent une grande quantité de trafic, telles que les contextes de workflow [wf_context] ou les alertes Event Management [em_alert], peut avoir un impact sur les performances. Pour cette raison, vous ne pouvez pas auditer la table em_alert dans son ensemble. Vérifiez plutôt les champs d'intérêt sélectionnés. Défini `audit=true` à la fois sur la table em_alert et sur les champs sélectionnés. Essayez d'auditer le moins de champs possible.

Audit des tables parent et enfant

Les tables ne dérivent pas les marqueurs d'audit des tables auditées parents 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 tous les champs de la table Ordinateurs [cmdb_ci_computer] dérivés de la table Éléments de configuration [cmdb_ci].

Audit des tables 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.

Audit des suppressions à partir d'un formulaire ou d'une liste

Par défaut, le système vérifie les suppressions d'enregistrements individuels d'un formulaire. Pour empêcher l'audit, définissez l'attribut `no_audit_delete`de dictionnaire de la table .

Le système vérifie 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. Toutefois, 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_auc 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/ tâche planifiée.

Informations vérifiées

L'audit suit les changements d'enregistrement suivants :

- 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 mises à jour de cet enregistrement et de ce champ
- Date et heure auxquelles le changement s'est produit
- Utilisateur ayant effectué le changement
- Motif du changement (si un motif est 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. C'est pourquoi vous pouvez voir 132 mises à jour dans l'historique d'un enregistrement, mais seulement sept mises à jour vérifiées.

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 des tables parent ou enfant.
- Champs avec l'attribut de dictionnaire no_audit.
- Les tables système ne sont pas répertoriées dans la `glide.ui.audit_deleted_tables` liste des 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'enregistrement sans créer de journal d'audit.

- Chaque fois qu'un moniteur d'inactivité touche un enregistrement. Cela vous empêche de voir des centaines de mises à jour répertoriées par rapport à un incident, le bruit noyant les données utiles.
- Changements manuels des Analyse des performances scores.

Audit d'une table

Pour obtenir des instructions sur l'audit d'une table, reportez-vous à Configurer 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 l'une des deux façons suivantes :

- 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 Exclusion d'un champ de l'audit (liste d'exclusion).
- Vous pouvez activer l'audit pour la table, mais uniquement pour les champs spécifiés. Cette propriété 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 la façon d'inclure un champ à l'aide d'une liste d'inclusion, reportez-vous à la rubrique Inclusion d'un champ de table dans l'audit (liste d'inclusion).

Enregistrements d'audit non annulables

Réduisez les risques 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 que les opérations d'écriture d'enregistrement cible. Si l'enregistrement cible est supprimé, l'audit est quand même créé et conservé sous le module **de suppression d'audit de test NCA** .

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 mise en Washington DC production, 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 l'annulation avant la création de l'audit. Désormais, les audits sont créés immédiatement après la modification de l'enregistrement, ce qui réduit les risques qu'une transaction annulée annule l'opération 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 True à False. Cette propriété 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 déjà être présente et définie sur True, ce qui signifie que ces instances ne seront pas en mesure d'utiliser ce changement pour auditer le comportement.

Remarque :
Il est recommandé de supprimer cette propriété pour tirer parti de la mise à jour.

Configurer 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

Rôle requis : admin.

Remarque :
Les champs chiffrés ne sont pas audités de par leur conception. Ce comportement n'est pas configurable.

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, d'une ligne pour 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 liste d'inclusion pour une table. Si vous souhaitez auditer la plupart des champs, mais en exclure certains, reportez-vous à la section Exclusion d'un champ de l'audit (liste d'exclusion).

Activer l'audit de liste d'inclusion pour une table

Permettez à une table d'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

Rôle requis : admin
La table doit être activée pour l'audit.

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, d'une ligne pour une colonne de la table, en recherchant la ligne avec le nom de table correct, une entrée vide pour le nom de colonne et un type de *`collection`*.
4. Dans le champ **Attributs** de cette ligne, saisissez *`audit_type=whitelist`*.

Que faire ensuite
Désignez les champs que vous souhaitez auditer dans cette table.

Exclusion d'un champ de l'audit (liste d'exclusion)

Empêchez le suivi d'un Now Platform sous-ensemble de champs dans une table auditée en excluant ces champs d'un audit.

Avant de commencer
Rôle requis : admin
Pour exclure un champ d'une table de l'audit, vous devez d'abord activer l'audit pour cette table.

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 souhaitez auditer uniquement quelques champs, suivez plutôt la procédure de liste d'inclusion .

Remarque :
La désactivation de l'audit sur les champs basés sur un journal peut avoir un impact sur la fonctionnalité des 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`.

Inclusion d'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
Rôle requis : admin
Pour ajouter des champs d'une table à une liste d'inclusion, vous devez d'abord avoir activé l'audit pour cette table et activé l'audit de liste d'inclusion pour cette table.

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 afin d'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 de 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) qui auront la propriété de suppression auditée** .
3. Ajoutez ou supprimez des noms de tables.
   Les noms de table doivent être séparés par des virgules, sans aucun espace.
4. Cliquez sur **Enregistrer**.

Remarque :
Pour plus d'informations sur l'audit, consultez Présentation de la table d'audit système.

Affichage des tables Audit Sys et Changement de relation d'audit

Il Now Platform suit 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).

Elle suit les Now Platform tables d'audit. Pour suivre les tables, cochez la case **Audit** dans l'enregistrement de dictionnaire pour définir la valeur sur vrai. Par défaut, il n'audite pas les enregistrements des tables système, telles que les tables d'ensembles de mises à jour.

Remarque :
Pour éviter les problèmes de performances et les boucles infinies, le système ignore toute règle métier ou tout workflow déclenché par des insertions dans la table Audit système.

Colonnes de la table d'audit sys

Les colonnes suivantes apparaissent dans les enregistrements de la table sys_audit :

Champ	Description
Nom de la table	Table à laquelle l'enregistrement d'audit se rapporte (par exemple, « `incident` »)
Nom de champ	Colonne de la table à laquelle se rapporte 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 .

Champ	Description
Valeur précédente	Ancienne valeur du changement de champ représenté par cet enregistrement de sys_audit. • Champs de référence : valeur de sys_id unique de l'enregistrement modifié. • Champs de date et d'heure : valeur en heure universelle coordonnée (UTC) telle qu'elle est stockée dans la base de données.
Nouvelle valeur	Nouvelle valeur du changement de champ représenté par cet enregistrement sys_audit. • Champs de référence : valeur de sys_id unique de l'enregistrement modifié. • Champs de date et d'heure : valeur en heure universelle coordonnée (UTC) telle qu'elle est 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 l'activité des tables qui sont marquées pour l'audit. Cette activité comprend les entrées de champ journal et les jeux d'historique. La table Changement de relation d'audit [sys_audit_relation] suit les changements de relation entre les enregistrements de table sys_audit 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 dans une table, une relation est créée entre les différentes tables d'origine vers le magasin qui enregistre les données. Ces informations sur la 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 de sys_audit_relation avec de nouveaux ID de document.

Connaître les ensembles d'historique

Le système génère automatiquement des enregistrements d'ensemble d'historique selon les besoins à partir de la table d'audit lorsqu'un utilisateur crée un enregistrement ou affiche son historique.

Si un enregistrement se trouve dans une table auditée, son jeu d'historique est généré lorsque l'enregistrement est inséré ou lorsqu'un utilisateur consulte l'enregistrement.

Remarque :
N'utilisez pas d'ensembles d'historiques pour générer des rapports.

Plusieurs champs d'informations sont capturés dans l'enregistrement Ensemble d'historique, affiché dans la vue de liste.

Champs d'enregistrement de la vue de liste

Champ	Valeur d'entrée
ID	ID de document pour l'enregistrement dont l'historique est enregistré.
Table	Table auditée pour l'enregistrement dont l'historique est enregistré.
Temps de chargement	Temps nécessaire pour générer l'ensemble d'historique.

Champs d'enregistrement de l'historique d'audit

Champ	Valeur d'entrée
Étiquette	Étiquette du champ qui a été modifié.
Ancien	Valeur avant le 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	Le nombre de fois que ce champ a été modifié. La valeur -1 indique la date de création ou de suppression de l'enregistrement.
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 jeu 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 incompatibilité de date se produit dans les cas suivants : • Vous affichez un ensemble d'historiques après qu'une modification a été apportée à un enregistrement, mais • Avant qu'une autre modification ne lui soit apportée lors d'une future mise à niveau.
Nom d'utilisateur	Nom de l'utilisateur qui a créé le changement.

Ensembles d'historique dans une vue Calendrier

Une fois que les jeux d'historique sont actifs, le choix du menu contextuel Historique est rempli à l'aide des informations du jeu d'historique, plutôt qu'à partir de la table de `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 comprend une vue 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 de données historiques.

Affichage des jeux d'historique

Il existe deux façons d'afficher l'ensemble de l'historique, accessibles via l'action **Historique** du menu contextuel.

Différences entre les ensembles d'audit et d'historique

Les tables Audit [sys_audit], Jeux 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 indéfiniment 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 de plus en 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 plus petits enregistrements de sous-ensemble pour lesquels vous souhaitez réellement afficher des informations historiques.

Table de l'ensemble d'historique [sys_history_set]

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 qui se sont produits au niveau des valeurs de champ.

- Le système génère automatiquement des enregistrements de l'ensemble d'historiques et d'historiques selon les besoins à partir de la table d'audit lorsqu'un utilisateur crée un enregistrement ou demande son historique.
- Plutôt que de contenir un historique complet de toutes les modifications apportées au système, les enregistrements d'ensemble et d'historique ne contiennent qu'un sous-ensemble récent d'informations historiques pour les enregistrements pour lesquels des utilisateurs ont créé ou demandé de telles informations.
- En plus des données d'audit, les jeux d'historique incluent également les informations définies lors de l'insertion de l'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 écritures de journal apparaissent dans des jeux d'historique avec la même heure de création et créées par données que l'enregistrement associé lui-même.

Le système limite les enregistrements de l'ensemble d'historique et d'historique selon les critères suivants :

- 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 tables pour alterner entre quatre tables d'historique tous les sept jours. Le système supprime les enregistrements d'historique datant de plus de 28 jours.

Si quelqu'un a besoin d'informations historiques 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 jeu d'historique, le menu contextuel sélectionnant **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 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 , `List of roles (comma-separated) that can access the history of a record`sélectionnez les rôles d'utilisateur auxquels vous souhaitez accéder à l'historique.
4. Sélectionnez **Enregistrer**.

Résultats

Toute modification apportée à un champ est omise si un utilisateur sans accès en lecture consulte 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

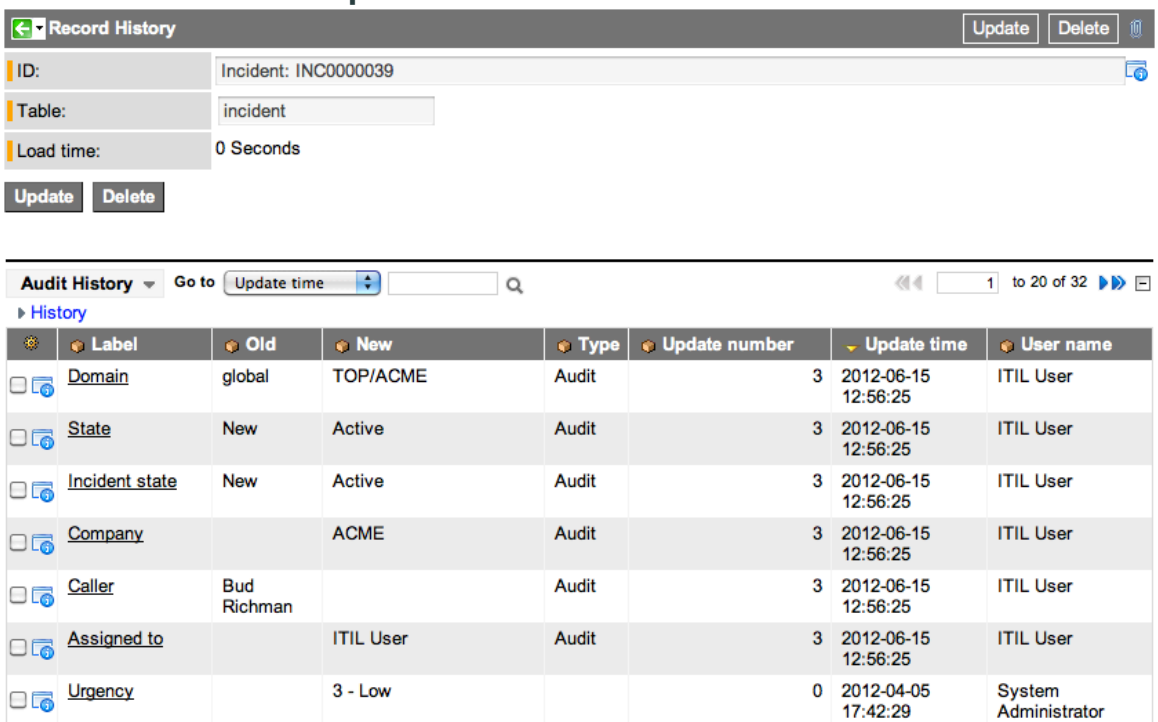
Procédure

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

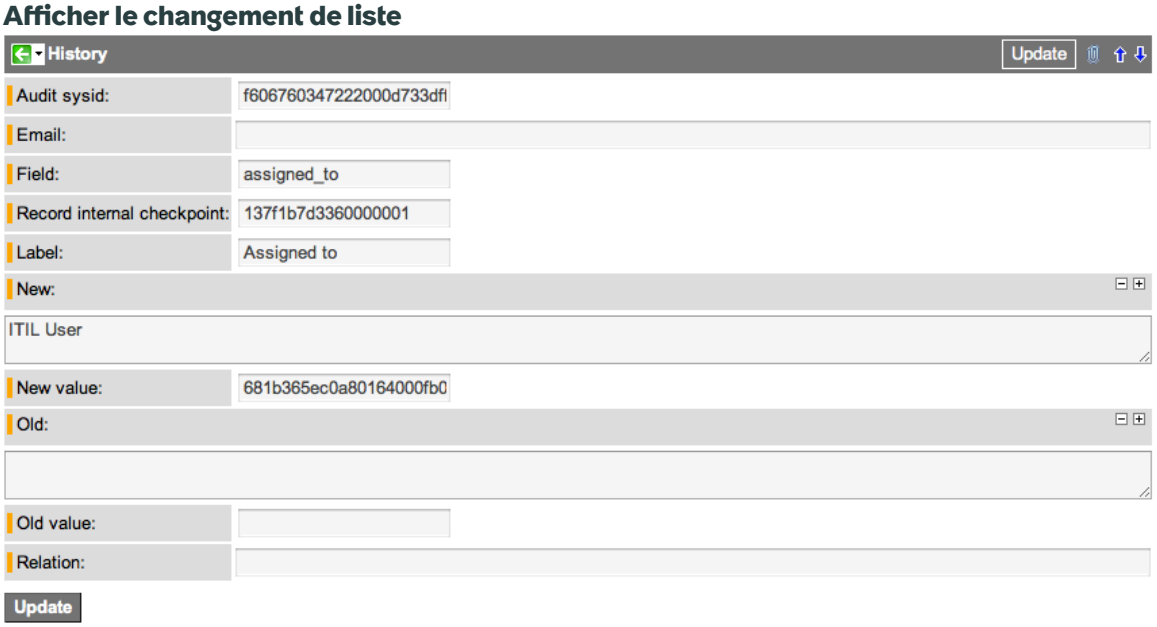
La liste de l'historique affiche chaque changement sous la forme d'une ligne distincte dans la liste des changements.

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, vous devez remplir les conditions suivantes.

Audit

L'audit de la table doit être activé pour afficher une liste d'historique.

ACL

Par défaut, l'option *Historique de la liste* n'est disponible que pour les utilisateurs disposant du rôle d'utilisateur administrateur. Pour permettre aux non-administrateurs d'activer cette

option, créez une règle ACL personnalisée accordant un accès en lecture à la table Historique des enregistrements [sys_history_set].

Rôles

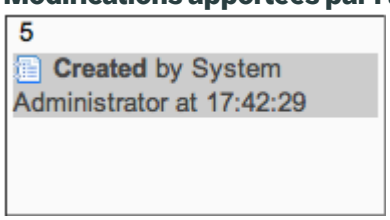
Au moins un des rôles dont dispose l'utilisateur doit être inclus dans la `glide.history.role` propriété, qui inclut le rôle itil par défaut.

Calendrier de l'historique

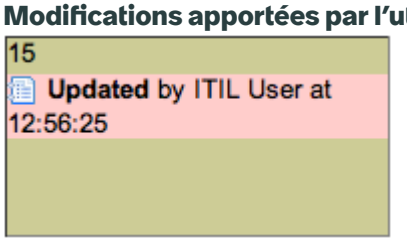
Le calendrier de l'historique indique les jours où l'enregistrement a été changé, la personne qui a effectué le changement et le moment où elle l'a effectué.

Le calendrier de l'historique est trié par numéro de mise à jour. Chaque utilisateur se voit attribuer une couleur afin que vous puissiez savoir 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



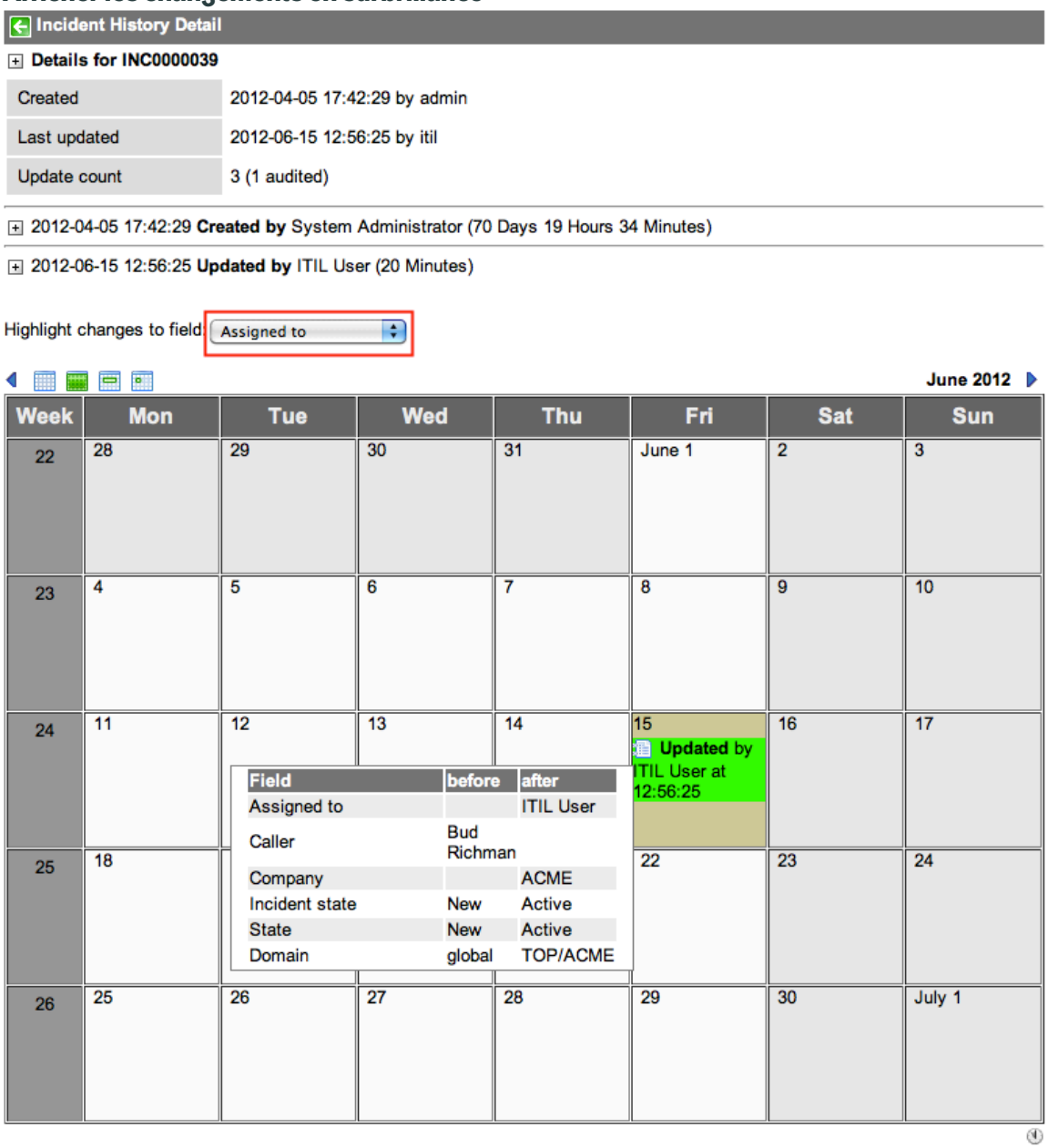
Modifications apportées par l'utilisateur ITIL



Pour mettre en surbrillance les modifications apportées à un champ particulier, sélectionnez le champ dans la zone de sélection **Mettre en surbrillance les modifications apportées au champ** . Si vous sélectionnez un champ dans cette zone de sélection, le calendrier apparaît en surbrillance avec les heures auxquelles ce champ a été modifié. Passez la souris sur le texte de l'un des changements mis en surbrillance pour voir le changement de valeur.

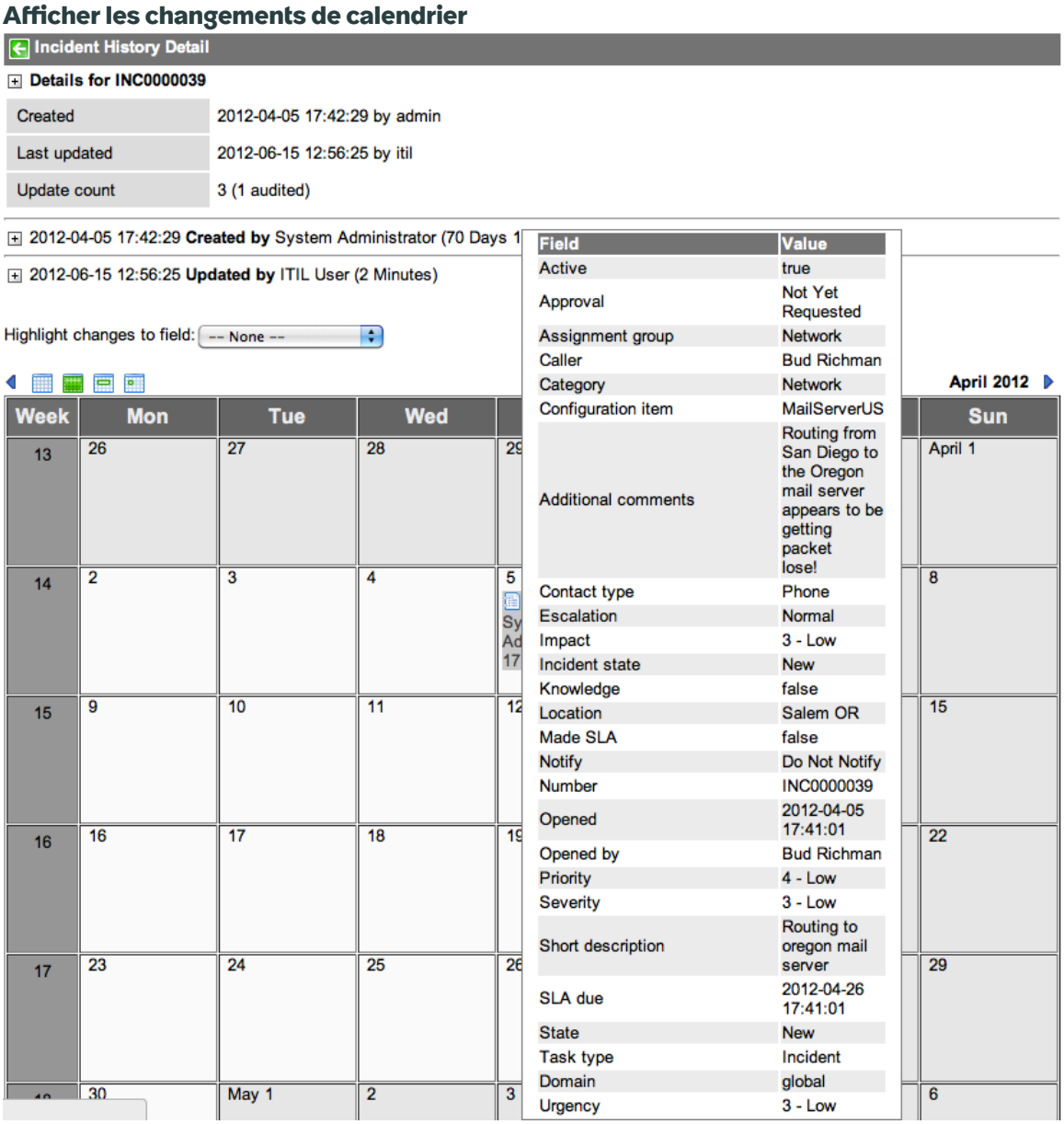
Traduction automatique

Afficher les changements en surbrillance



Si vous passez la souris sur l'icône dans une entrée, une fenêtre contextuelle affiche toutes les valeurs modifiées. Il s'agit des mêmes informations qui sont affichées dans la partie supérieure du formulaire.

Traduction automatique



Traduction automatique

Vous pouvez cliquer sur le numéro du jour pour voir les changements effectués ce jour-là. 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 afficher les changements.

Chronologie de l'historique

Vous pouvez afficher une chronologie des changements pour un CI et pour ses enregistrements, relations, bases de référence et changements proposés connexes pour le CI. Les chronologies sont disponibles pour les CI de 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, définie par défaut sur ITIL. En outre, l'utilisateur doit disposer d'un accès en lecture à la table Ensemble d'historique [sys_history_set], qui est accordée par défaut à l'administrateur.

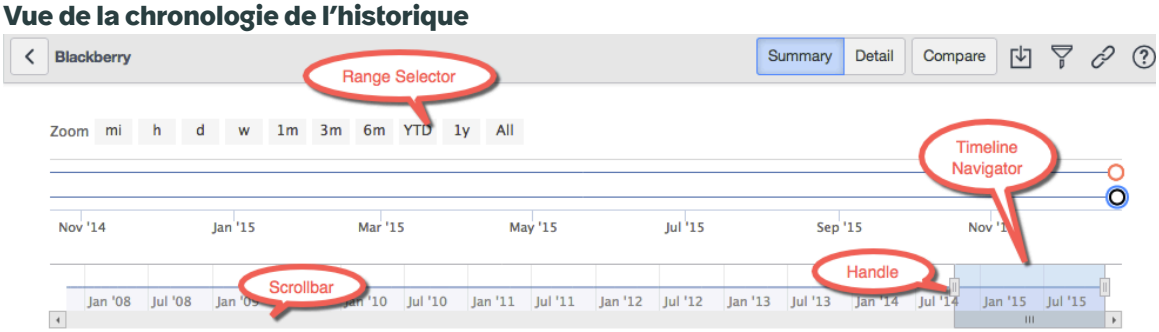
Vous pouvez ouvrir une chronologie lorsque vous affichez l'historique d'un CI. Vous pouvez spécifier la période, la plage horaire et les propriétés qui s'affichent dans la chronologie. Vous pouvez afficher ce qui a changé dans un ensemble de changements particulier ou afficher l'intégralité du CI pour mieux résoudre les problèmes. Vous pouvez également

afficher une chronologie des changements apportés aux enregistrements connexes du CI, ainsi qu'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 différent de changement, et la couleur de chaque bulle indique si le changement est valide ou non valide. Les bases de référence des 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 vers une bulle pour afficher des détails sur l'ensemble de changements.

Un changement apporté à une relation n'est considéré comme valide que s'il a été appliqué via Change Management. Si le changement a été appliqué via le cadre de travail des changements proposés, il est valide. Pour obtenir d'autres étapes de validation, reportez-vous à 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 dates futures.

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 vers 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. À côté 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.

Si le CI change beaucoup au cours de la période, les bulles affichées risquent d'être trop encombrées. Vous pouvez effectuer un zoom avant ou arrière pour étaler les bulles de l'une ou l'autre méthode :

- Modifiez l'intervalle de temps sur la chronologie. Au fur et à mesure que vous raccourcissez l'intervalle de temps, vous effectuez un zoom avant, puis à mesure que 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 sont affichées. 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 **Détail** et **Résumé** mettent en évidence les propriétés modifiées dans le périmètre de votre filtre. Les propriétés modifiées sont mises en surbrillance en bleu clair.

Dans la vue **de 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 de résumé, les propriétés modifiées sont répertoriées avant les propriétés inchangées.

Vue de résumé

La vue **Résumé** affiche les instantanés des CI représentés par chaque bulle. Chaque instantané affiche les changements apportés aux champs et aux 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 **<** situés de part et d'autre de l'écran de l'instantané pour faire défiler les enregistrements de jeu de changements suivants et précédents dans l'ordre chronologique.

Vue détaillée

La vue **Détail** affiche les instantanés du CI qui correspondent aux bulles. Chaque instantané inclut les champs qui se trouvent dans le champ d'application du filtre de propriété, affichant les propriétés qui ont changé avec un arrière-plan bleu clair. Cliquez sur une bulle pour afficher l'instantané correspondant du CI. Les données qui s'affichent sont en lecture seule.

Utilisez les boutons **>** et **<** des deux côtés pour faire défiler les enregistrements d'ensemble de modifications suivants et précédents dans l'ordre chronologique.

Afficher la chronologie des changements apportés aux enregistrements connexes

Sur 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

- Table cible : l'enregistrement CI doit se trouver dans la table Élément de configuration [cmdb_ci] ou dans 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 la case 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 dans le focus ou que vous effectuez un zoom avant ou arrière, cela affecte simultanément la chronologie du CI et la chronologie des enregistrements connexes.

Exporter un instantané d'un CI

Vous pouvez exporter un instantané d'un CI à partir de sa chronologie.

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.

Pourquoi et quand exécuter cette tâche

Vous pouvez exporter un instantané du CI au format XML, PDF (portail) ou PDF (paysage).

Procédure

1. Ouvrez la chronologie du CI.
2. Sélectionnez la bulle représentant l'heure pendant laquelle vous souhaitez exporter un instantané du CI.
3. Cliquez sur l'icône d'exportation ( ).
4. 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.

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 n'audite pas les changements lorsque la valeur d'affichage d'un champ de référence change.

Considérez la situation suivante. Un utilisateur change son nom de Jane Smith à 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 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'afficheront que le nouveau nom Jane Miller. Par défaut, le système ne permet pas de distinguer les modifications effectuées sous le nom d'utilisateur d'origine de celles effectuées avec le nouveau nom d'utilisateur.

Si votre politique d'audit nécessite un suivi des changements de nom d'utilisateur, vous pouvez :

- Créez un nouvel enregistrement d'utilisateur pour le nouveau nom et désactivez l'enregistrement d'utilisateur précédent. Le système conserve les enregistrements d'audit pour l'ancien nom d'utilisateur et crée les futurs enregistrements d'audit avec le nouveau nom d'utilisateur.
- Créez des champs personnalisés et une règle métier pour enregistrer le nom précédent 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 une situation classique, les insertions peuvent représenter plus de 80 % de la taille de la table d'audit.

L'absence d'insertions de suivi permet d'améliorer les performances et d'avoir 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 modifications apportées à une relation CI (relations CI, relations CI/utilisateur ou relations CI/groupe) apparaissent dans l'historique des éléments des deux côtés de la relation modifiée, que la modification soit manuelle ou le résultat de Détection.

Par exemple, si l'ordinateur alpha a une relation de CI utilisé par avec la version bêta de l'ordinateur, l'historique de l'alpha contient un enregistrement de la date d'établissement de la relation avec l'alpha, de même que l'historique de la version bêta indique le moment où la relation avec l'alpha a été établie. Cet exemple illustre l'historique affiché lorsque des relations de CI sont établies, puis que l'une d'entre elles 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 créée indique la date de création du CI, de l'utilisateur ou du groupe. La dernière puce d'activité fait référence à la dernière modification des relations. 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]).

Paramètres de sécurité élevée

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

Explorer le paramètre de haute sécurité

Activer les paramètres de sécurité élevée

Découvrez les fonctionnalités et les valeurs commerciales des paramètres de sécurité élevée.

Activez les paramètres de sécurité élevée.

Configurer les paramètres de sécurité élevée

Découvrez comment configurer les paramètres de sécurité élevée.

Exploration des paramètres de sécurité élevée

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

Le module Paramètres de haute sécurité est activé avec le module d'extension Paramètres de haute sécurité, 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 Module d'extension de haute sécurité Paramètres de renforcement de la sécurité de l'instance. Les propriétés des types de paramètres de sécurité élevée suivants 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 emplacement 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 à la table.
- Rôle d'administrateur de sécurité : permet d'empêcher la modification des paramètres et des ressources de sécurité clés. Le rôle d'administrateur de sécurité n'est pas hérité du rôle administrateur et doit être explicitement affecté.
- 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.

Traduction automatique

- 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 manière dont ils peuvent y accéder.

Remarque :

- Les paramètres de sécurité élevée activent également automatiquement le module d'extension Contextual Security, 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 Now Platform. Pour en savoir plus sur chacune de ces propriétés, reportez-vous à Paramètres de la sécurisation pour la sécurité de l'instance.
- Pour en savoir plus sur chacune de ces propriétés, reportez-vous à Paramètres de la sécurisation pour la sécurité de l'instance.

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 la **liste sys_properties.list** et recherchez la propriété que vous souhaitez définir ou modifier.

  Les options de la table Propriétés système [sys_properties.list] sont **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 activés :

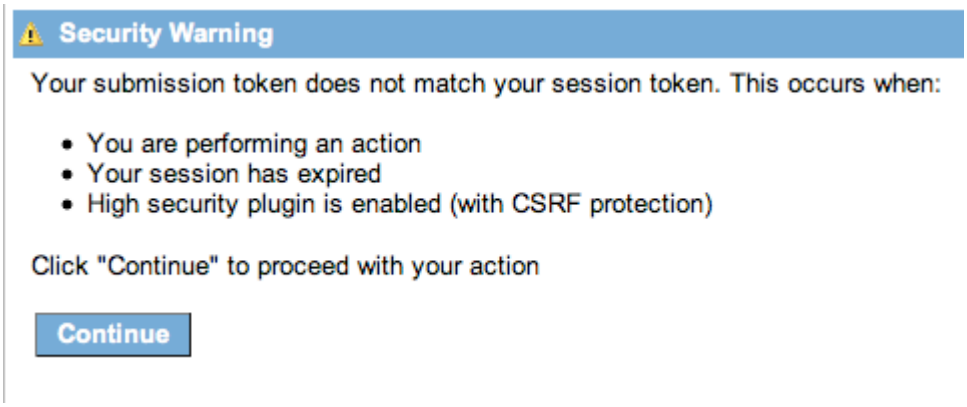
- **read_roles** liste de rôles séparés par des virgules autorisés à lire tous les champs de cette propriété.
- **write_roles** : liste de rôles séparés par des virgules autorisés à écrire/modifier tous les champs de cette propriété.

Les propriétés répertoriées dans la table Propriétés ont **read_roles** d'administrateur et **write_roles** de security_admin. Les utilisateurs dotés du rôle administrateur peuvent afficher et lire les valeurs des propriétés, mais doivent s'élever 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.

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 pour l'interface utilisateur. Empêche les attaques de script de site à site réfléchies et stockées. Cette propriété n'est pas applicable dans Service Portal. **Remarque :** Cette propriété est définie sur **true** par défaut dans Vancouver la version et les 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 client.	Oui	XML
glide.ui.escape_all_script	Force l'échappement par défaut de toutes les expressions dans Jelly JavaScript	Oui dans les nouvelles instances	Échapper à Jelly

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 de 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 failles 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 Single Sign-on, définissez cette propriété sur Non. Sinon, il 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 : Activez une sécurité par cookie supplémentaire. Si **oui**, la validation stricte des cookies de session est appliquée.	Oui	Cookies de session sécurisés

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 la sécurité des transactions entrantes lors de la soumission du formulaire (les droits sont toujours vérifiés lors de la génération du formulaire). **Remarque :** Cette propriété est définie sur **true** par défaut dans Vancouver la version et les 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 client.	Oui	Double vérification des transactions entrantes
glide.security.strict.actions	Vérifiez les conditions des actions d'interface utilisateur avant leur exécution. Normalement, les conditions ne sont vérifiées que pendant le rendu du formulaire.	Oui	Vérifier l'action d'interface utilisateur avant son exécution
glide.security.use_csrf_token	Activez l'utilisation d'un jeton de sécurité pour	Oui	Jeton anti-CSRF

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 intersite.		
glide.ui.escape_html_list_field	HTML d'échappement pour les champs HTML d'une vue de liste.	Oui	Échapper au HTML
glide.html.escape_script	Balises JavaScript d'échappement dans les champs HTML.	Oui	Javascript d'échappement
glide.ui.forgetme	Décochez la case **Mémoriser** mon nom 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 nom d'utilisateur et mot de passe. **Remarque :** Cette propriété est obsolète.	Oui	Authentification SMTP (obsolète)
glide.script.use.sandbox	Exécutez des scripts générés par le client (AJAXEvaluate et conditions de requête) dans un bac à sable à droits réduits. Si **oui**, seules les règles métier et les includes de script lorsque la case **Client joignable** est définie sur **Oui** sont disponibles, et certains appels d'API back-end sont interdits. Pour plus d'informations,	Oui	Bac à sable pour les scripts générés par le client

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	consultez Configuration de la propriété de bac à sable de script.		
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 aux tables et aux champs, et vérifie que les utilisateurs SOAP possèdent les rôles appropriés pour utiliser le service Web.	Oui	Sécurité stricte des requêtes SOAP
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 Access Control (ACL) pour permettre aux utilisateurs invités d'accéder au contenu WSDL.	Oui	Autorisation de demande WSDL
glide.basicauth.required.csv	Exiger une autorisation de base pour les demandes CSV entrantes .	Oui	Autorisation des demandes de CSV

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
glide.basicauth.required.excel	Demandez une autorisation de base pour les demandes Excel entrantes.	Oui	Autorisation des demandes d'Excel
glide.basicauth.required.importprocessor	Demandez l'autorisation de base pour les demandes d'importation entrantes.	Oui	Autorisation des demandes d'importation
glide.basicauth.required.pdf	Demandez une autorisation de base pour les demandes PDF entrantes.	Oui	Autorisation de demande de PDF
glide.basicauth.required.rss	Demandez l'autorisation de base pour les demandes RSS entrantes.	Oui	Autorisation de demande de RSS
glide.basicauth.required.scriptedprocessor	Demandez une autorisation de base pour les demandes de script entrantes.	Oui	Autorisation de demande de script
glide.basicauth.required.soap	Demandez l'autorisation de base pour les demandes SOAP entrantes.	Oui	Authentification de base : demandes SOAP
glide.basicauth.required.unl	Demandez l'autorisation de base pour les demandes de déchargement entrantes.	Oui	Autorisation de la demande de déchargement
glide.basicauth.required.xml	Demandez une autorisation de base pour les demandes XML entrantes.	Oui	Autorisation de demande XML
glide.basicauth.required.xsd	Demandez l'autorisation de base pour les demandes XSD entrantes.	Oui	Autorisation de la demande XSD

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
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 **ce n'est pas le cas**, toutes les URL sont autorisées, ce qui peut permettre la liaison à du contenu externe non autorisé.	Oui	Renforcer les liens relatifs
glide.set_x_frame_options	Activez cette propriété pour définir l'en-tête de réponse X-Frame-Options sur SAMEORIGIN 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 rendre une page dans un <frame> ou <iframe>. Les sites peuvent utiliser cette propriété pour éviter les attaques de détournement de clic en s'assurant que leur contenu n'est pas intégré dans d'autres sites. https://developer.mozilla.org/en/the_x-frame-options_response_header	Oui	X-Frame-Options: SAMEORIGIN
glide.ui.attachment.download_mime_types	Une liste de types MIME de pièces jointes séparés par des virgules qui ne	texte/html,image/svg,image/svg+xml	Forcer les types MIME de téléchargement

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	sont pas alignés dans le navigateur. Prévient les attaques de script de site à site. Par exemple, text/html force les fichiers HTML à être téléchargés sur le client en tant que pièces jointes plutôt que d'être affichés dans le navigateur.		
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 groupes en fonction des données réelles des groupes.	Oui	Aucun
glide.security.diag_txns_acl	Si **oui**, seuls l'utilisateur administrateur ou l'utilisateur dont l'adresse IP est autorisée peuvent accéder à stats.do, threads.do et replication.do.	Non	Surveillance des performances (ACL)
glide.ui.security.codetag.allow_script	Autorisez le HTML incorporé (utilisant des balises [code]) à contenir des balises JavaScript.	Non	Autoriser le code HTML intégré

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	Remarque : Cette propriété est définie sur **true** par défaut dans Vancouver la version et les 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 client.		
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	Activer AJAXEvaluate
glide.login.autocomplete	Autorisez les navigateurs à utiliser la saisie semi-automatique sur les champs de mot de passe des formulaires de connexion.	Non	Saisie semi-automatique du champ Mot de passe

Les propriétés suivantes sont définies dans la table sys_properties, mais ne sont pas visibles sur la page Paramètres de sécurité élevée.

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	VRAI	Aucun

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	contre les attaques de l'homme du milieu (MITM). Pour plus de détails, consultez Configurer le spoke Kubernetes **Remarque :** Cette propriété remplace la propriété com.glide.communications.trustmanager_trust_all.		
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 intersite.	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 la session utilisateur expire, le jeton de sécurité expire avec elle, sauf si la `glide.security.csrf_previous.allow` propriété est activée et si elle est comprise dans la période décrite par cette propriété. Ce	86400 **Remarque :** Valeur en secondes. Équivalent à 1 jour.	Aucun

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	jeton est utilisé pour éviter les attaques de contrefaçon de requête intersite.		
glide.security.csrf.strict.validation.mode	Applique une validation stricte aux jetons CSRF afin que les utilisateurs ne puissent pas soumettre à nouveau une demande si le jeton CSRF ne correspond pas.	faux	Validation stricte du CSRF
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

Configuration de la propriété de bac à sable de script

Activez la propriété sandbox de script (`glide.script.use.sandbox`) pour exécuter des scripts générés par le client dans un bac à sable disposant de droits restreints.

Il existe deux cas dans le système qui permettent au client d'envoyer des scripts au serveur pour évaluation.

- Filtres et/ou requêtes : Il est légal d'envoyer un filtre au serveur tel que : `assigned_to=javascript :getMyGroups()`.
- API système : L'appel `d'API AJAXEvaluate` permet au client d'exécuter des scripts arbitraires sur le serveur et de recevoir une réponse.

Si vous activez la propriété sandbox de script (`glide.script.use.sandbox`), le script évalué via l'un de ces deux points d'entrée s'exécute dans un sandbox à droits réduits avec les caractéristiques suivantes :

- Seules les règles métier marquées **Client pouvant être appelé** sont disponibles dans le bac à sable.
- Seules les includes de script marquées **Client pouvant être appelé** sont disponibles dans le bac à sable.
- Certains appels d'API (en grande partie, mais pas entièrement, ceux traitant d'un accès direct à la base de données) ne sont pas autorisés.
- Les données ne peuvent pas être insérées, mises à jour ou supprimées depuis le bac à sable. Tous les appels à `current.update(),` par exemple, sont ignorés.

Remarque :
Pour en savoir plus sur cette propriété, consultez Bac à sable pour les scripts générés par le client Paramètres de renforcement de la sécurité de l'instance.

Ces méthodes ne sont pas autorisées dans les scripts générés par le client lorsque le sandboxing de script est activé.

Méthodes restreintes

Classe	Méthode
GlideRecord	• `deleteMultiple()` • `deleteRecord()` • `getRowCount()` • `insérer()` • `update()` • `updateMultiple()`
Système Glide (gs)	• `addErrorMessage()` • `addInfoMessage()` • `addMessage()` • `eventQueue()` • `flushMessages()` • `getEscapedProperty()` • `getProperty()` • `log()` • `logError()` • `logWarning()` • `setProperty()` • `setRedirect()` • `setReturn()` • `workflowFlush()`
ScopedGlideRecord (en anglais seulement)	• `deleteMultiple()` • `deleteRecord()` • `insérer()` • `update()` • `updateMultiple()`
ScopedGlideSystem (gs)	• `addErrorMessage()` • `addInfoMessage()` • `debug()` • `eventQueue()`

Méthodes restreintes (suite)

Classe	Méthode
	• `executeNow()` • `getProperty()` • `getSessionToken()` • `info()` • `setRedirect()`
Date de Glide GlideDateTime Temps Glide	• `ajouter()` • `addDays()` • `addDaysLocalTime()` • `addDaysUTC()` • `addMonthsLocalTime()` • `addMonths()` • `addSeconds()` • `addWeeks()` • `addYears()` • `compareTo()` • `getByFormat()` • `getDate()` • `getDayOfWeek()` • `getDayOfWeekUTC` • `getDayOfWeekLocalTime()` • `getDayOfMonth()` • `getDayOfMonthLocalTime()` • `getDayOfMonthNoTZ()` • `getDayOfWeek()` • `getDayOfWeekLocalTime()` • `getDayOfWeekUTC()` • `getHourOfDayLocalTime()` • `getHourOfDayUTC()` • `getDaysInMonth()` • `getDaysInMonthUTC()` • `getDaysInMonthLocalTime()` • `getDisplayValueInternal()` • `getDisplayValue()`

Méthodes restreintes (suite)

Classe	Méthode
	• `getHourLocalTime()` • `getLocalDate()` • `getLocalTime()` • `getMinutesLocalTime()` • `getMinutesUTC()` • `getMonthLocalTime()` • `getMonthNoTZ()` • `getMonthUTC()` • `getNumericValue()` • `getSeconds()` • `getTime()` • `getTZOffset()` • `getValue()` • `getYear()` • `getUserTimeZone()` • `getWeekOfYearLocalTime()` • `getWeekOfYearUTC()` • `getYearUTC()` • `getYearLocalTime()` • `isDST()` • `onOrAfter()` • `onOrBefore()` • `setDayOfMonthUTC()` • `setDisplayValue()` • `setMonth()` • `setValeurNumérique()` • `setTZ()` • `setValue()` • `setValueUTC()` • `soustraire()` • `toString()`
GlideSchedule	• `ajouter()` • `isInSchedule()`

Méthodes restreintes (suite)

Classe	Méthode
	• `load()` • `quandNext()`

Remarque :
Les méthodes GlideSystem (gs) `log()`, `logError()` et `logWarning()` peuvent être activées avec le sandboxing de script en définissant la `glide.security.sandbox_no_logging` propriété système sur `faux`.

Si vous exécutez le système sans activer le sandboxing de script, aucune de ces restrictions ne s'applique.

Remarque :
Cette propriété est activée par défaut lorsque vous activez le module d'extension Paramètres de sécurité élevée. n'activez pas cette propriété en dehors du module d'extension.

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 :

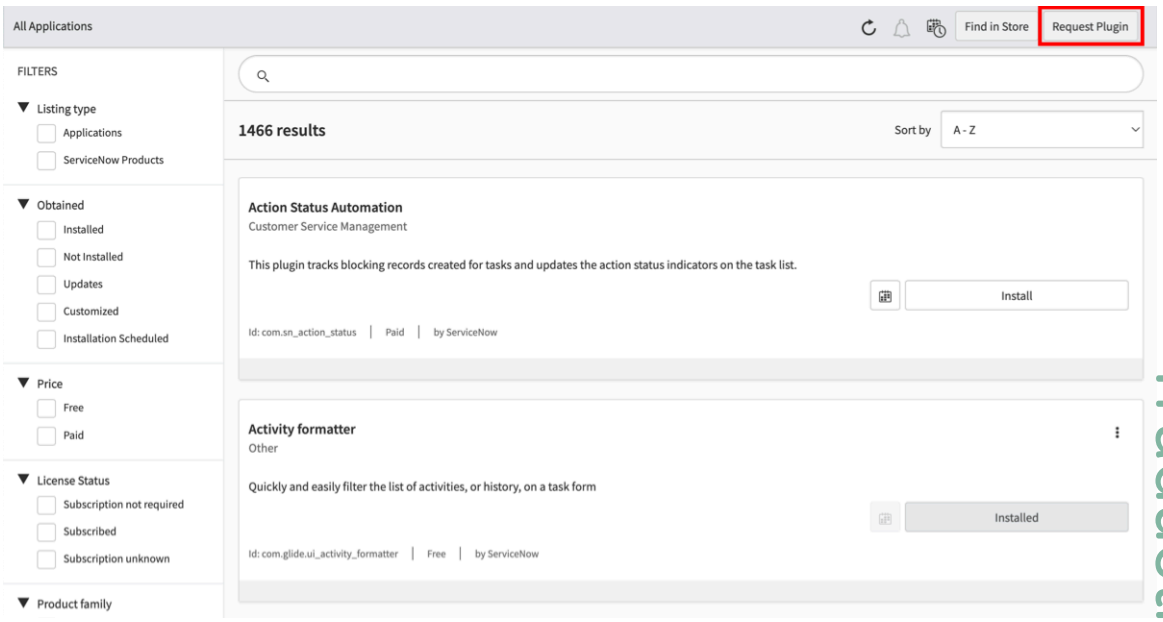
1. Examinez les informations suivantes pour comprendre le nouveau comportement :
   - Règles des listes de contrôles d'accès
   - Paramètres de sécurité élevée
   - Propriété de refus par défaut
2. Activez le module d'extension sur une instance de non-production. Un clone récent de production est préférable.
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 Module d'extension de haute sécurité Paramètres de renforcement de la sécurité de l'instance.

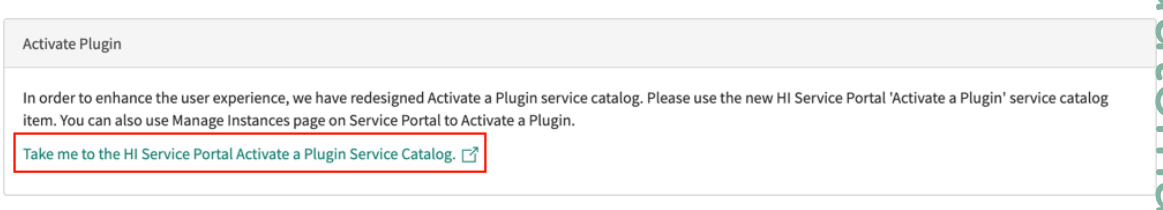
Rôle requis : admin

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.

Formulaire Activer le module d'extension

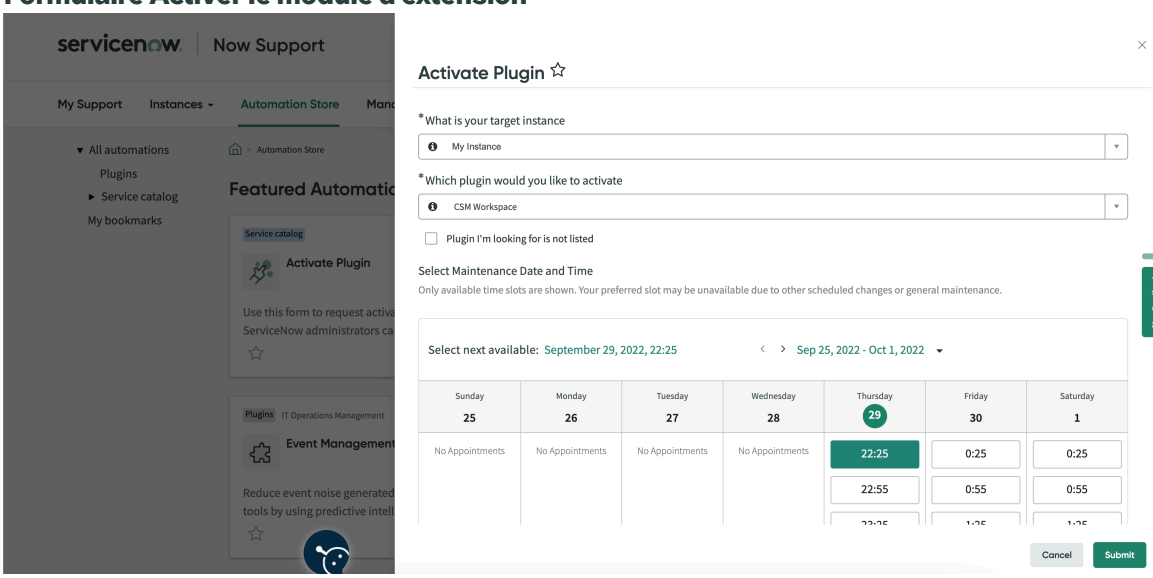
Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer.

Champ	Description
	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



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 Service Catalog [KB0751715] de la Now Support Base de connaissances.

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.

Explorez l’assainisseur HTML

Découvrez comment fonctionne l’assainisseur HTML.

Configurer l’assainisseur HTML

Configurez l’assainisseur HTML.

Activer l’assainisseur HTML

Découvrez comment activer l’assainisseur HTML.

Traduction automatique

Exploration de 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 au sein de votre instance ne contient pas de contenu potentiellement dangereux. L'assainissement HTML fonctionne en supprimant 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 de sécurité qui contrôlent la mise en forme de votre contenu sont conservées. En tant qu'administrateur, vous pouvez personnaliser le contenu à supprimer ou à conserver. 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 le script `include HTMLSanitizerConfig` que les administrateurs peuvent utiliser pour modifier la liste d'inclusion intégrée. Les 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 les protocoles suivants :

- `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 Assainisseur HTML les paramètres de renforcement de la sécurité de l'instance.

Configurer urlAttributes et les protocoles

Vous pouvez configurer urlAttributes et leurs protocoles dans le script **include HTMLSanitizer** . Par exemple :

```
HTML_WHITELIST : {
urlAttributes: { "protocols" : [ "file", "notes" ] },
          - -
          - -
    }
```

Étant donné que `les notes` se trouvent dans la liste d'inclusion de cet exemple, cette URL n'est pas nettoyée :

Traduction automatique

```
<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 par les utilisateurs dans 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"]},

   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","accessk
ey","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:{},

    body:{},    caption:{},    head:{},    title:{},  shape:{},},
```

Configuration de l’assainisseur HTML

Vous devez modifier un script include 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 d'attribut aux paires attribut-valeur-regex-modèle. Le modèle attribute-value-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:{
         attribute:["style","align"],
         attributeValuePattern:{src:".*jpeg"}},
      iframe:{},}
```

Il ajoute les éléments suivants à la liste d'inclusion :

- ID et nom des attributs globaux. Il s'agit d'une liste de chaînes qui peuvent être appliquées globalement à tous les éléments.
- L'élément img où les attributs sont style et align.
- L'élément img où l'attribut source de l'image est un fichier avec l'extension .jpeg. Voici 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, la 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`* sur *`glide.translated_html.sanitize_all_fields`***true**.

> **Remarque :**
> Pour en savoir plus sur cette propriété, consultez Assainisseur HTML 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 dans 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 d'assainisseur sur faux, puis activer l'assainisseur pour chaque champ pour n'importe quel formulaire.

Procédure

1. Accédez à la table sys_properties et définissez le *`glide.html.sanitize_all_fields`* sur **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 de dictionnaire s'ouvre pour le champ HTML.
4. Saisissez l'un des éléments suivants dans le champ Attributs :
   - Pour désactiver l'assainissement, entrez `html_sanitize=faux`
   - Pour activer l'assainissement, entrez `html_sanitize=vrai`
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**.

Activation de la journalisation de 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

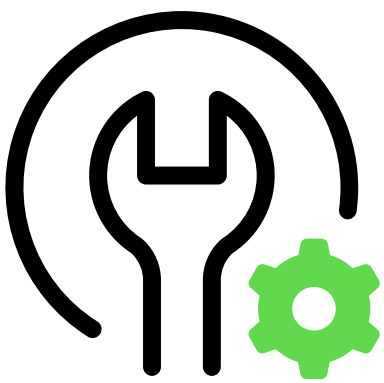
Pourquoi et quand exécuter cette tâche
Vous pouvez examiner ces éléments nettoyés en ajoutant /syslog_list.do ?sysparm_query=source%3DHTMLSanitizer à l'URL de votre instance.

Procédure

1. Pour examiner ces éléments nettoyés, 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 cette valeur sur **vrai** (activé) ou **faux** (désactivé).
   Cette propriété est par défaut définie sur **true**.

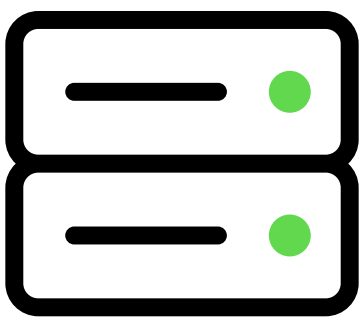
Autres paramètres et ressources de sécurité

Cette section contient les propriétés de sécurité que vous définissez en dehors d'Instance Security Center, ainsi que d'autres ressources liées à la sécurité.



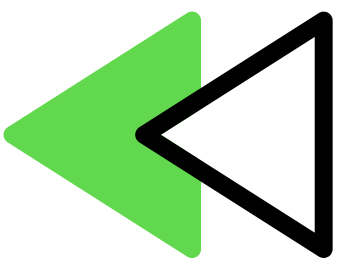
Propriétés système de sécurité

Les paramètres de sécurité fournissent plusieurs propriétés pour contrôler le niveau de sécurité de votre instance.



Guide de déploiement du MID Server

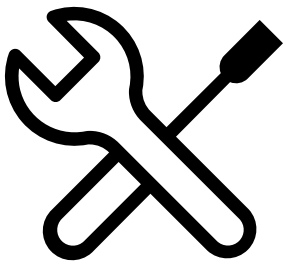
ServiceNow Management, Integration, and Discovery (MID) Server est une application Java légère qui s'exécute en tant que service Windows ou démon UNIX sur du matériel standard, y compris des ordinateurs virtuels.



Comportement réversible

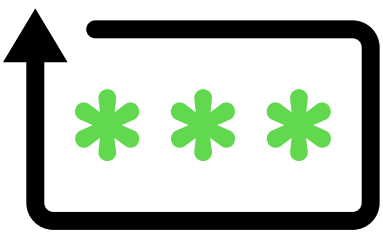
Certaines propriétés système sont classées comme « safe_overrides » ou « no_db_override ».

Traduction automatique



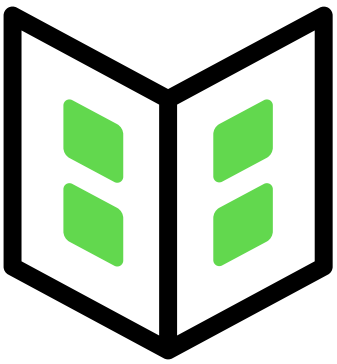
Propriétés de sécurité obsolètes

Ces propriétés de sécurité ont été déconseillées dans les versions antérieures.



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 dans votre instance.



Autres ressources sur la sécurisation renforcée

Sources supplémentaires d'informations sur le renforcement des contrôles de sécurité, en lien avec Now 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 la **liste sys_properties.list** et recherchez la propriété que vous souhaitez définir ou modifier.

  Les options de la table Propriétés système [sys_properties.list] sont **vrai** ou **faux**.

- Accédez à la **Sécurité de système** > **Centre de sécurité de l'instance**, puis sur **Sécurisation renforcée**.

  Vous pouvez configurer les paramètres pour les 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 Now Platform. Pour en savoir plus sur chacune de ces propriétés, reportez-vous à Paramètres de la sécurisation pour la sécurité de l'instance.

⚠ 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 de code HTML à l'aide de la balise [code]. Valeur par défaut : oui **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Autoriser le code HTML intégré
glide.ui.security.codetag.allow_script	Permet au HTML incorporé (utilisant des balises [code]) de contenir des balises Javascript. **Remarque :** Cette propriété est définie sur **true** par défaut dans Vancouver la version et les 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 client. Pour en savoir plus, voir Autoriser les balises JavaScript dans le HTML intégré.
glide.ui.escape_all_script	Force l'échappement par défaut de toutes les expressions dans Jelly JavaScript <![CDATA[<script type="text/javascript">]]> . Applique l'échappement uniquement si l'attribut type de 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 : vrai ◦ Instances mises à niveau : faux • Valeur recommandée : oui **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Échapper à Jelly

Limites et comportement des pièces jointes

com.glide.attachment.max_taille	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 renforcement de la sécurité de l'instance : Restreindre les extensions de fichiers
glide.ui.attachment.force_download_all_mime_types	Force le téléchargement de tous les fichiers en pièce jointe de type MIME (Multipurpose Internet Mail Extensions). Valeur par défaut : • Instances nouvelles/zbootées : oui • Instances mises à niveau : non **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Forcer les types MIME de téléchargement
glide.security.file.mime_type.validation	Active (**Oui**) ou désactive (**Non**) la validation de type MIME pour les pièces jointes de fichiers. Le type MIME est vérifié pendant le chargement pour les extensions de fichier configurées `glide.attachment.extensions` via le type. Valeur par défaut : • Instances nouvelles/zbootées : oui • Instances mises à niveau : non **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Restriction de type MIME de téléchargement

Chargements du client

Ces propriétés affectent uniquement les chargements 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 pouvant être téléchargés, lorsqu'ils ont été chargés à l'aide de la fonctionnalité Charger un fichier de .Now Platform Utilisé avec `glide.ui.strict_customer_uploaded_content_types` **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Activer les restrictions de téléchargement de fichiers
glide.ui.strict_customer_uploaded_content_types	Lorsque ce paramètre inclut une liste de types de fichiers délimités par des virgules, des fichiers qui ont été téléchargés à l'aide de la fonctionnalité Charger un fichier de , Now Platformseuls ces types de fichiers peuvent être téléchargés à partir de l'instance. **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Spécifier les types de fichiers téléchargeables

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 lors de la soumission du formulaire. Les droits sont toujours vérifiés lors de la génération de formulaires. **Remarque :** Cette propriété est définie sur **true** 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 client. Pour en savoir plus, voir Double vérification des transactions entrantes.
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 renforcement de la sécurité de l'instance : Vérifier l'action d'interface utilisateur avant son exécution
glide.security.granular.create	Applique les règles de création aux 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 sur les éléments de formulaire verrouillés.

Cookies

glide.ui.forgetme	Supprime la case **à cocher Mémoriser** mon nom de page de connexion lorsque l'instance utilise des connexions LDAP ou BD. 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 (nouvelles instances et instances démarrées Z) **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Supprimer Se souvenir de moi
glide.ui.secure_cookies	Active les cookies de session sécurisés pour renforcer la sécurité des cookies. Si **oui**, la validation stricte des cookies de session est appliquée. Avec les cookies de version 3 activés, des exigences de sécurité supplémentaires sont également appliquées. **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Cookies de session sécurisés
glide.secure_cookie.debug	Débogage des cookies de session sécurisés. Sélectionnez cette option pour activer la journalisation de débogage étendue des opérations de cookies de session sécurisée.

Restrictions de sécurité pour l'exécution de scripts en provenance du client

glide.script.use.sandbox	Exécutez des scripts générés par le client (AJAXEvaluate et conditions de requête) dans un bac à sable à droits réduits. Si cette option est activée, seules les règles métier et les includes de script pour lesquels la case **Client pouvant être appelé** est cochée sont disponibles, et certains appels d'interface de programmation d'application (API) back-end sont interdits. **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Bac à sable pour les scripts générés par le client
glide.script.allow.ajaxevaluate	Active le processeur AJAXEvaluate. **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Activer AJAXEvaluate
glide.script.secure.ajaxgliderecord	Applique des listes de contrôle d'accès de sécurité (ACL) standard aux appels AJAXGlideRecord. Valeur par défaut : oui, pour les instances nouvelles et mises à niveau. (Si **oui**, ne peut pas être remplacé par **Non**.) **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Activation de la vérification de l'ACL de AJAXGlideRecord

Divers

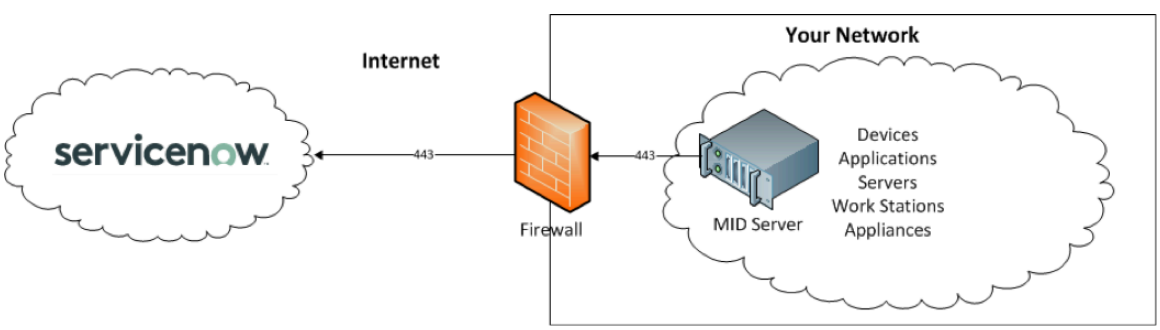
com.glide.communications.trustmanager_trust_all	Par défaut, l'instance fait confiance à l'autorité de certification (CA) d'un certificat. Garantit que l'instance accepte les certificats auto-émis. Pour valider l'autorité de certification d'un certificat, définissez cette propriété sur **Non** **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Certificat de confiance

glide.outbound.sslv3.disabled	Lorsqu'il est actif, il force les connexions sortantes d'une instance à utiliser le protocole TLS (Transport Layer Security) au lieu du protocole SSL (Secure Sockets Layer). **Remarque :** Paramètres de renforcement de la sécurité de l'instance : Désactivation de SSLv2/SSLv3

Des propriétés supplémentaires sont disponibles pour Paramètres de sécurité élevée.

Guide de déploiement sécurisé du MID Server (renforcement de la sécurité de l'instance)

Le ServiceNow Management, Integration, and Discovery (MID) Server est une application Java légère qui s'exécute comme un service Windows ou un démon UNIX sur du matériel standard, y compris des ordinateurs virtuels.



Il s'authentifie en toute sécurité auprès de votre instance dans le ServiceNow Cloud à l'aide de ses propres identifiants de connexion et facilite la transmission des données avec vos applications, sources de données et services. Plusieurs MID Servers peuvent être déployés dans différents segments de réseau pour offrir une évolutivité supplémentaire.

Tenez compte des facteurs suivants concernant la sécurité de votre MID Server :

Sécurité physique

Sécurisez le matériel physique qui héberge le MID Server ou l'hyperviseur pour les MID Servers virtualisés.

- Placez le matériel dans un endroit sécurisé qui le protège contre tout accès non autorisé.
- Protégez l'accès à cet emplacement à l'aide d'un lecteur de carte électronique et d'une surveillance CCTV.
- Placez le matériel physique dans une cage verrouillée ou un rack avec un contrôle d'accès par clé physique.

Sécurité de l'infrastructure virtuelle

Utilisez la virtualisationavec la possibilité d'installer plusieurs MID Servers 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 MID Server 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 de confiance interne pour la console de gestion, tel que ESX Server et VirtualCenter.
- Utilisez les VLAN pour vous prémunir contre les attaques réseau.
- Suivez les consignes de sécurité publiées dans les guides de sécurisation renforcée des fournisseurs.

Sécurité du système d'exploitation

Découvrez comment le MID Server stocke son nom d'utilisateur et son Now Platform mot de passe dans son fichier de configuration, nommé config.xml, pour une authentification sécurisée à l'instance.

Le MID Server doit être déployé dans un système d'exploitation sécurisé et renforcé pour assurer la protection contre tout accès non autorisé aux informations d'identification :

- 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 MID Server.
- Installez régulièrement les correctifs de sécurité du système d'exploitation avec les logiciels antivirus les plus récents et mettez régulièrement à jour les définitions antivirus.
- Le MID Server nécessite un cadre de travail Java actuel pour s'exécuter. Maintenez Java à jour régulièrement.
- Supprimez ou désactivez les services et applications inutiles.
- Installez un pare-feu du système d'exploitation pour limiter l'accès aux ports non autorisés.
- Suivez les consignes de sécurité publiées dans les guides de sécurisation renforcée du système d'exploitation des fournisseurs.

Sécurité réseau

Le MID Server communique sur le port 443 à l'aide du protocole SSL vers l'instance et ne nécessite aucune connexion entrante.

Pour sécuriser correctement votre MID Server dans un réseau, procédez comme suit :

- Installez le MID Server 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 le MID Server pour qu'il n'accepte aucune connexion entrante autre que celles requises pour la gestion d'entreprise du système d'exploitation et du matériel.
- Le système qui héberge le MID Server doit être en mesure d'accéder au ServiceNow site de téléchargement à **install.servicenow.com**.

> **Remarque :**
> Cette URL renvoie vers le site de téléchargement, qui n'est ServiceNow pas accessible à partir de cette rubrique.

L'ordinateur hôte MID Serve doit être en mesure d'accéder à ce site pour télécharger le package d'installation. Il contacte **install.servicenow.com** 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 du MID Server a également lieu lorsque vous mettez à niveau une instance.

Pare-feu

Configurez votre pare-feu pour autoriser le trafic réseau sortant du MID Server vers votre instance et mettre à niveau automatiquement le serveur.

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`

Administrer et gérer

Cette section décrit les pratiques de sécurité et les directives pour l'administration et la gestion du MID Server 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 les instructions suivantes :

- N'utilisez pas de compte administratif dans l'instance pour le MID Server.
- Utilisez une longueur et une complexité de mot de passe suffisantes pour le compte de MID Server.
- Le mot de passe doit comporter au moins 12 caractères avec des majuscules, des minuscules, des chiffres et des caractères spéciaux.
- Utilisez différents comptes MID Server avec des mots de passe uniques pour différents MID Servers dans une instance.
- Utilisez la fonctionnalité de sécurité SOAP stricte pour protéger toutes les tables avec des listes de contrôle d'accès (ACL) en l'activant *`Enforce strict security on incoming SOAP requests`* dans **Propriétés système** > **Services web**.
- Changez les mots de passe du MID Server à la fréquence qui respecte la politique de mot de passe de votre organisation.

Remarque :
Pour en savoir plus, consultez Créer l'utilisateur du MID Server et lui accorder le rôle .

Configurer un MID Server sur un hôte Windows

Lorsque vous installez le MID Server sur un hôte Windows, il crée un service Windows. 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 MID Server sur l'hôte Windows.

1. Accédez à la **Gestion des ordinateurs** > **Services et applications** > **Services**.
2. Cliquez avec le bouton droit sur **ServiceNow MID Server**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Se connecter** 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 **ServiceNow MID Server**, puis cliquez sur **Redémarrer**.
8. Assurez-vous que le MID Server a pu redémarrer et se connecter à l'instance.

Informations d'identification Windows Discovery and Orchestration

Configurez un compte Windows ou Active Directory local sur les systèmes cibles avec le moins de privilèges nécessaires. Il n'est peut-être pas nécessaire d'utiliser les informations d'identification de l'administrateur du domaine.

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 pour la détection Linux et l'orchestration

Utilisez un compte non racine avec des privilèges sudo limités sur les systèmes Linux cibles lors de la détection et de l'orchestration.

Appliquez les consignes 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 majuscules, des minuscules, des chiffres et des caractères spéciaux.
- Lors de la configuration des autorisations sudo, les chemins d'accès locaux aux fichiers exécutables binaires peuvent différer en fonction de la distribution Linux que vous exécutez, consultez Commandes privilégiées du MID Server .

Chiffrer les informations d'identification de connexion au MID Server

Par défaut, les informations d'identification de connexion au MID Server 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, en utilisant la syntaxe suivante :

```
&lt;parameter name=&amp;quot;MID.instance.username » value=&amp;quot;MIDsrvadmin » />
```

```
&lt;parameter name=&amp;quot;MID.instance.password » encrypt=&amp;quot;true » value=&amp;quot;$ECUREpassw 0rd&amp;quot;/>
```

Remarque :
Le chiffrement des informations d'identification de connexion au MID Server ne remplace pas un hôte de serveur non sécurisé avec une sécurité physique et réseau médiocre. Le mot de passe stocké dans le fichier config.xml est chiffré au premier démarrage du MID Server ou, s'il s'agit d'un MID Server 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 MID Server pour lequel vous souhaitez désactiver cette fonctionnalité.
3. Dans la configuration du MID Server, cliquez sur le bouton **Nouveau** en regard de Paramètres de configuration.
4. Dans Paramètre de configuration du MID Server, configurez les paramètres suivants :
   - **Nom de paramètre** mid.ssh.dh_group_length_min
   - **Valeur** 2048

Désactiver le SSL sortant

Vous pouvez désactiver SSLv2 et SSLv3 dans le Now Platform. La définition de cette propriété force le MID Server à utiliser TLS, profitant de sa sécurité accrue, lors des connexions sortantes, telles que les 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** : vrai

Désactiver les algorithmes faibles

Vous pouvez désactiver les algorithmes les plus faibles afin que les requêtes adressées 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, en utilisant 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 devez donc avoir un processus en place pour remettre à jour ce fichier après chaque mise à niveau.

Les utilisateurs de Powershell doivent consulter leur administrateur pour obtenir de l'aide Windows afin de désactiver les versions inférieures de TLS. Pour savoir quelles versions de TLS sont 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 de remplacement sécurisé.

Attribut	Catégorie
Refus par défaut	Contrôle d'accès
Activation de la vérification de l'ACL de AJAXGlideRecord	Contrôle d'accès
La protection de la vie privée sur les includes de script pouvant être appelés par le client comprend	Contrôle d'accès
Bac à sable pour les scripts générés par le client	Validation de l'entrée
Remplacement du mode de collecte (obsolète)	Liste d'inclusion de sécurité

Aucun remplacement de base de données

Les valeurs existantes de ces propriétés ne peuvent pas être modifiées ou remplacées.

Attribut	Catégorie
Activer les restrictions de téléchargement de fichiers	Pièces jointes

Propriétés de sécurité déconseillées

Ces propriétés de sécurité ont été déconseillées dans les versions antérieures.

Remplacement du mode de collecte (obsolète)

La `glide.whitelist.manager.collection_mode.override` propriété a été conçue pour fournir une rétrocompatibilité pour des 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 package 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

Attribut	Description
	sont considérés comme dangereux du point de vue de la sécurité. Validez-les pour l'autorisation et la restriction d'accès aux objets sensibles.
Références	https://support.servicenow.com/kb_view.do?sysparm_article=KB0621483

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 remis 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 jusqu'à ce que vous définissiez la propriété et fournissiez 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 du contrôle d'accès au contenu JavaScript

Si vous êtes un client ayant effectué une mise 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 ayant effectué une mise 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 ServiceNow® l'assistance pour obtenir de l'aide.

Rôle requis : admin

Procédure

1. Dans Application Navigator, recherchez `sys_js_content_provider_rule.list`.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Règle du fournisseur de contenu JavaScript

Champ	Description
Actif	Option qui, lorsqu'elle est sélectionnée, active la règle. Lorsque cette option est désactivée, si aucune autre règle ne correspond, l'URL **du chemin d'accès** est admise.
Chemin d'accès	URL absolue vers 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 Not Found** 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. ○ **Rediriger** : le serveur renvoie le contenu d'un autre fichier 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 périmètre/de l'application ou du domaine.
Chemin de redirection	Champ qui clarifie le chemin vers lequel la redirection s'effectue.

Champ	Description
	Lorsque **l'option Action** est définie sur **Rediriger**, le contenu de cette URL est proposé à une demande pour l'URL du **chemin d'accès** .

4. Cliquez sur **Envoyer**.

Autres ressources sur la sécurisation renforcée

Vous trouverez ci-dessous d'autres sources d'information sur le renforcement des contrôles de sécurité en ce qui concerne le Now Platform.

Ressources	Description
Portail de test de sécurité	Portefeuille de services de sécurité sur HI
KB0538598	Test d'intrusion de l'application client | Politique et procédure
KB0546756	Désactivation de l'accès public au système de gestion de contenu (CMS)
KB0550071	ServiceNow, Inc. Révision du contrôle d'accès à l'instance
KB0550613	Identification et activation des restrictions d'adresse IP
KB0550828	Auditer et examiner les transactions GlideAjax
KB0550837	Correction 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. Monitoring - Vue d'ensemble et aperçu
KB0564232	Utilisation de ServiceNow, Inc. l'application Mobile avec authentification externe
Sécurité et risque	ServiceNow, Inc. Communauté

Contrôle d'accès ServiceNow®

Le module d'extension SNC Access Control (com.snc.snc_access_control) vous permet de contrôler quels Service et assistance client employés peuvent accéder à votre instance et à quel moment.

Explorer le contrôle d’accès ServiceNow

Découvrez les fonctionnalités du contrôle d’accès ServiceNow® .

Activer le 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

Découvrez et examinez la journalisation d’audit du contrôle d’accès ServiceNow® .

Traduction automatique

Explorer le ServiceNow® contrôle d'accès

Le module d'extension SNC Access Control (com.snc.snc_access_control) vous permet de contrôler quels Service et assistance client employés peuvent accéder à votre instance et à quel moment.

Lorsque vous activez le module d'extension pour la première fois, Service et assistance client les employés ne peuvent pas se connecter à l'instance. Tous les employés actuellement connectés Service et assistance client 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 et assistance client 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, ainsi qu'à vérifier l'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 d'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, ce qui peut affecter les niveaux de service de support et le SLA de disponibilité. Le SLA de disponibilité est ensuite mesuré à partir du moment où le personnel d'assistance reçoit l'accès à votre instance.

Sécurité de connexion

La sécurité des connexions des employés autorisés Service et assistance client aux instances utilise des jetons chiffrés générés par un serveur sécurisé. Seuls les employés correctement authentifiés Service et assistance client ont accès à une instance. Sans le module d'extension SNC Access Control, le serveur de sécurité s'assure 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 dans 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 et assistance client employés peuvent accéder à leurs instances, et à quel moment.

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 ServiceNow le 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 ce compartimentage (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 et assistance client de se connecter à leur instance ne nécessite pas la mise en service d'un compte sur cette instance. Il n'existe aucun enregistrement utilisateur mis en service et aucune information d'identification permanente ou persistante. Au lieu de cela, un utilisateur synthétique est créé pour chaque Service et assistance client connexion d'employé. Cet utilisateur n'existe qu'en mémoire et ne fournit aucun privilège continu. Si le module d'extension SNC Access Control est activé, vous pouvez retirer l'autorisation d'un Service et assistance client employé à tout moment.

Jetons

Les jetons de sécurité sont spécifiques à une instance et à un employé particulier Service et assistance client . En outre, le mécanisme qui génère les jetons ne fonctionne qu'avec les connexions réelles Service et assistance client 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 et assistance client 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 et assistance client employés aux instances sont enregistrées comme un événement de connexion.

- Chaque action effectuée par l'employé connecté Service et assistance client 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 des ServiceNow employés.
- Service et assistance client Les connexions et les actions des employés sont facilement identifiables, car les noms d'utilisateur se terminent tous par @snc (comme frodo.baggins@snc).

Ces actions vous fournissent une journalisation de sécurité facile à utiliser, robuste et fiable pour l'accès des non-employés.

Flux de traitement de sécurité

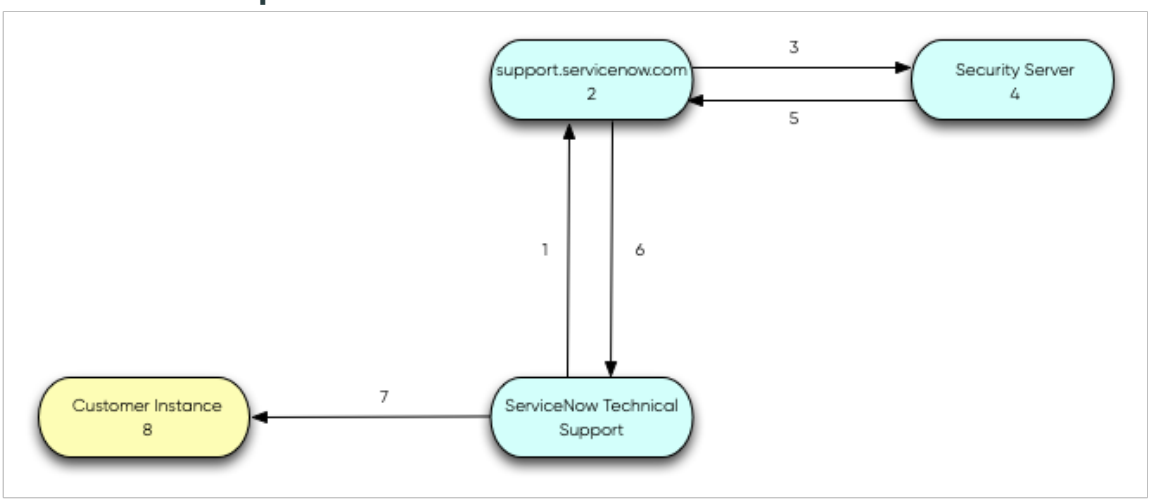
Lorsqu'un Service et assistance client employé souhaite se connecter à une instance, le flux de traitement de sécurité est le suivant :

1. Un Service et assistance client technicien demande une connexion pour l'instance par le biais de hi.service-now.com.
2. HI vérifie que le technicien dispose du rôle approprié autorisant 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 construit 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 d'assistance.
7. Le navigateur du technicien d'assistance initie une connexion à 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 met en correspondance avec le nom d'utilisateur fourni lors de l'étape précédente, l'ID d'instance et la fenêtre de temps autorisée. Si le module d'extension SNC Access Control est activé, l'instance vérifie que l'utilisateur :

- Énuméré(e/s)
- Actif
- Configuré pour accéder à l'instance dans la fenêtre horaire 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 de la limite de temps, l'utilisateur se déconnecte ou l'instance est redémarrée.

ServiceNow Flux de processus d'accès de sécurité



Journalisation d'audit

La journalisation suivante suit les connexions et l'activité des Service et assistance client employés :

- Journaux des événements : les journaux des événements affichent toutes les Service et assistance client connexions à une instance.
- Journaux de transactions : les journaux de transactions montrent toute l'activité sur l'instance, y compris toute tentative de suppression de journal.

Remarque :
Pour en savoir plus sur ce module d'extension, consultez Module d'extension SNC Access Control Paramètres de renforcement de la sécurité de l'instance.

Activation du contrôle d'accès ServiceNow®

Vous demandez l'activation du module d'extension SNC Access Control (com.snc.snc_access_control).

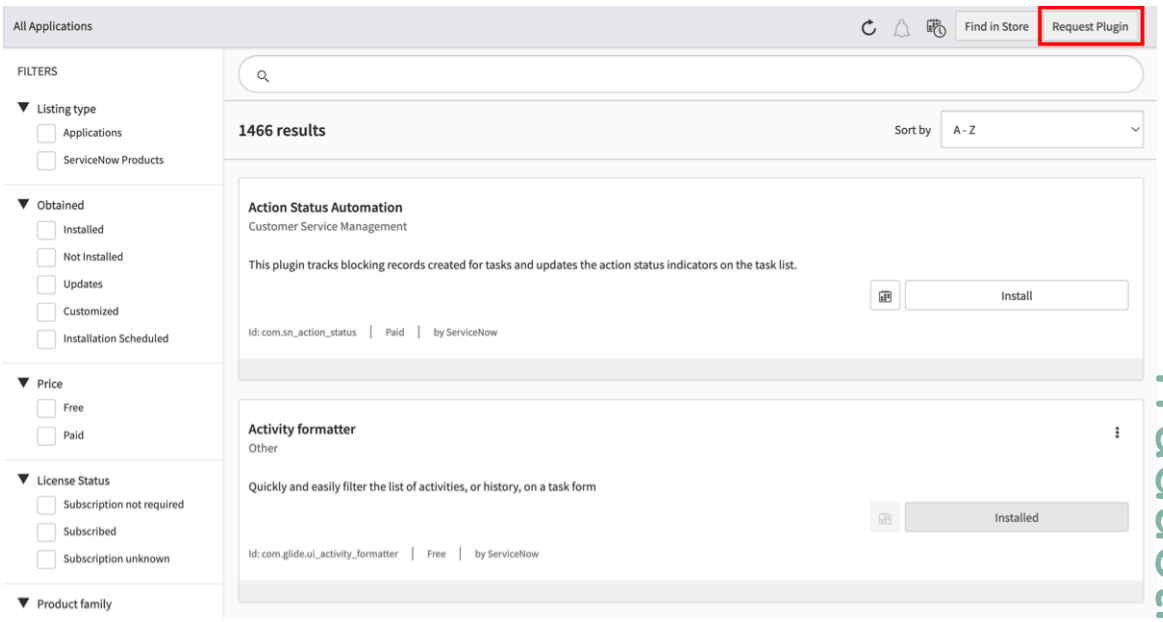
Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Il existe deux façons de demander un module d'extension :

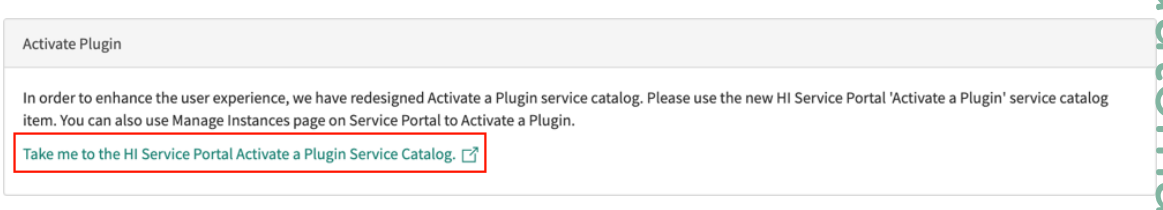
- Accéder directement au Now Support Service Catalog en sélectionnant **Tout** > **Catalogue de services** > **Activer le module d'extension** sur Now Support.
- Accéder au Catalogue de services de Now Support via la page Toutes les applications de votre instance en suivant ces étapes.

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.



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

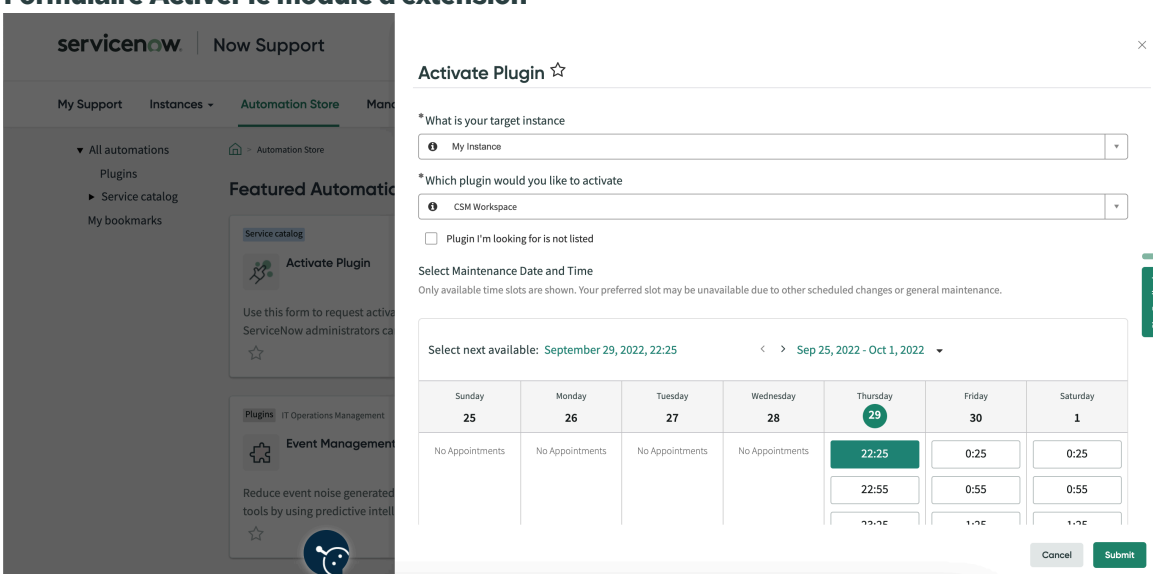
Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer.

Champ	Description
	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



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 Service Catalog [KB0751715] de la Now Support Base de connaissances.

Configuration ServiceNow® du contrôle d'accès

Configurez un enregistrement de contrôle d'accès pour spécifier un ou plusieurs Service et assistance client employés qui ont l'autorisation de se connecter à votre instance.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Remarque :
Le module d'extension SNC Access Control (com.snc.snc_access_control) empêche Service et assistance client 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 d'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, ce qui peut affecter les niveaux de service de support et le SLA de disponibilité. Le SLA de disponibilité est ensuite mesuré à partir du moment où le personnel d'assistance reçoit l'accès 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**.

Contrôle d'accès SNC

Champs de formulaire	Description
Nom	Nomme chaque Service et assistance client employé ayant l'autorisation de se connecter dans cette instance. ○ Exprimez les noms sous la forme prénom.nom en minuscules, séparés par un point (par exemple, jean.forgeron). Chaque nom doit avoir un enregistrement utilisateur correspondant dans *support.servicenow.com*. ○ Si plusieurs employés ont l'autorisation Service et assistance client 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 et assistance client employés pour accéder à l'instance, saisissez un astérisque (*) à la place du nom. ○ Si vous avez l'intention de restreindre l'accès des Service et assistance client employés à l'instance, les valeurs du champ **Nom** ne doivent pas comporter d'astérisque (*).
Motif	Champ explicite qui décrit la raison pour laquelle vous accordez l'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 et assistance client ont accès à la connexion. Il s'agit d'un champ obligatoire.

Champs de formulaire	Description
Fin	Spécifie la date et l’heure de fin de la période pendant laquelle les employés spécifiés Service et assistance client ont un accès à la connexion. Il s'agit d'un champ 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 de transactions affichent toutes les activités sur l’instance, y compris les efforts de suppression de journaux.

VPN (Virtual Private Network)

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

Explorez

Découvrez les fonctionnalités et les valeurs commerciales du réseau privé virtuel.

Activer Activer

Active le réseau privé virtuel.

Configurer

Apprenez à configurer un réseau privé virtuel.

Exploration du 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.

Toutefois, il peut exister des exigences en matière de sécurité ou d'architecture réseau qui dictent l'utilisation d'une connexion de réseau privé virtuel (VPN) de sécurité du protocole Internet (IPSEC) de site à site entre les centres de données et vos réseaux professionnels. Le VPN prend en charge la communication chiffrée nécessaire entre l'instance et votre réseau.

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 une pièce de matériel. Étant donné que chaque client dispose d'une configuration unique, l'instance dispose d'une solution VPN flexible. l'instance a construit 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 de trafic entrant dans votre réseau. Souvent, les intégrations qui utilisent le VPN n'ont pas de chiffrement 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 aucune intégration entrante vers ServiceNow ou tout trafic de l'utilisateur final vers ServiceNow à traverser une connexion VPN. Cette communication restreinte inclut 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 MID Server . 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 de 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 autres que RFC-1918 des deux côtés du tunnel.

ServiceNow fournit une adresse IP unique pour la source des requêtes dans votre réseau. Vous devez fournir des adresses NAT (Network Address Translation), 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. En outre, 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 :

- En utilisant le même domaine de chiffrement derrière vos deux pairs. C'est la méthode à privilégier.
- 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 homologues pour créer un chemin de connexion à l'aide de cette adresse vers votre serveur. Le chemin d'accès à votre serveur peut être le même ordinateur physique ou un miroir qui fournit des services identiques. Avec cette méthode, votre instance utiliserait la même adresse IP pour se connecter à vos serveurs, que votre tunnel principal 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 nécessite 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 offrent un moyen plus simple de connecter votre instance aux ressources des ServiceNow centres de données et fournissent un meilleur chiffrement. En outre, vous pouvez éviter tous les problèmes que les temps d'arrêt VPN pourraient causer, tels que rendre votre instance indisponible pour les utilisateurs en cas de problème avec le tunnel VPN.

Authentification unique et MID Server

Envisagez d'utiliser une combinaison d'authentification unique (SSO) pour l'authentification et du MID Server 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 certificat.

Vous pouvez utiliser l'écouteur LDAP sur un MID Server 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 gérer. 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

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 zone DMZ en utilisant uniquement les adresses sources de l'instance et les ports de destination de votre choix. Étant donné que les ports pour LDAP sont configurables dans votre instance, vous pouvez effectuer une traduction d'adresse de port (PAT) si vous le souhaitez. LDAPS vous permet de contrôler le certificat qui est téléchargé sur un canal chiffré vers l'instance (reportez-vous à la section 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 déchiffrement plus fort. Un VPN ne peut chiffrer 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 pré-partagée 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 version 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 vers votre site actif ou du site actif vers votre site DR, etc.).

Il est recommandé que le domaine de chiffrement soit aussi spécifique que possible. Idéalement, le domaine de chiffrement inclurait uniquement les hôtes spécifiques requis pour les intégrations. Un grand domaine de chiffrement peut créer des opportunités de divergences de routage (VPN ou Internet).

Pour créer le VPN, l'instance effectue les opérations suivantes :

1. Fournit les adresses d'homologue et d'hôte VPN de chaque centre de données.
2. Crée la connectivité VPN nécessaire à partir de deux centres de données dans votre réseau. Pour prendre en charge les exigences de redondance et de reprise après sinistre (DR), les VPN peuvent être provisionnés à partir de deux centres de données dans deux réseaux.

L'instance ne prend pas en charge la création 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 du trafic ou mise en forme du trafic au sein de votre propre réseau interne, plutôt que d'avoir plusieurs tunnels VPN.

Activation d'un service VPN

Pour toutes les demandes VPN, y compris la mise en service, les modifications ou les questions générales, utilisez le formulaire Demande de VPN de Service Catalog.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à https://support.servicenow.com/now?draw=case.
2. Sélectionnez l'onglet **Magasin d'automatisation** .
3. Utilisez l'arborescence de gauche pour naviguer jusqu'à **Toutes les automatisations** > **Catalogue de services** > **Infrastructure de cloud**.
4. **Sélectionner les requêtes 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 bien le trafic. Pour vous assurer que vous obtenez une réponse à vos questions en temps opportun, veuillez répondre aux questions liées au VPN au cours de ce processus.

Configuration d'une adresse pour la communication VPN

Pour éviter tout conflit ou chevauchement 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 autres que 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 dans votre réseau.

Procédure

Fournissez des adresses NAT (Network Address Translation) non RFC-1918 pour chaque hôte qui s’intègre à l’instance.