



ワシントンD.C. Proactive Service Experience Workflows

最終更新日: 2025年12月17日

自動翻訳

これらの資料は、翻訳ソフトウェアを使用してお客様の便宜のために翻訳されています。正確な翻訳をご提供できるよう相当な努力を払っておりますが、いかなる自動翻訳も人間の翻訳者に代わることはなく、そのようなことは意図されておりません。翻訳は「現状のまま」提供されています。他言語への翻訳の的確性、信頼性または正確性については、明示または黙示を問わず、いかなる保証も行われません。翻訳ソフトには限界があるため、一部のコンテンツが正確に翻訳されていない場合があります。これらの資料の公用言語は英語です。翻訳の際に生じる相違または不一致は、コンプライアンスまたは履行の目的に関しては拘束力を有さず、法的効力はないものとします。

ここで示したいくつかの例と図は、説明の目的でのみ提供されています。ServiceNow 製品またはサービスへの実際の関連付けやつながりは意図されておらず、推測されるものではありません。

ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは米国および/またはその他の国における ServiceNow, Inc. の商標または登録商標です。その他の会社名および製品名は、それぞれの所有者の商標です。

下記の ServiceNow ウェブサイト利用規約をお読みください。 www.servicenow.com/terms-of-use.html

自動翻訳

本社
2225 Lawson Lane
Santa Clara, CA 95054
United States
(408) 501-8550

目次

H.....	4
R.....	5
P.....	6
L.....	7
Proactive Service Experience Workflows.....	8
アーキテクチャの Proactive Service Experience Workflows 探索.....	9
Proactive Service Experience Workflows アーキテクチャ.....	10
CMDB の CI クラス Proactive Service Experience Workflows.....	15
Proactive Service Experience Workflows そして インシデント管理、サービスオペレーションワークスペース.....	15
Proactive Service Experience Workflows の構成.....	17
Proactive Service Experience Workflows のインストール.....	17
アサイン先グループにユーザーを追加.....	18
Proactive Service Experience Workflows の使用.....	19
での影響を受けるアカウントの Proactive Service Experience Workflows 特定について インシデント管理.....	19
インシデントのエスカレーションについて.....	23
での顧客またはパートナーアカウントの確認 Proactive Service Experience Workflows.....	25
インシデントからのケースおよび更新の自動作成.....	28
変更要求からのケース作成.....	30
のエスカレーションワークフローで使用されるメッセージについて Proactive Service Experience Workflows.....	31
トラブルチケット通知の処理.....	31
Proactive Service Experience Workflows 参照.....	38
ドメイン分離と Proactive Service Experience Workflows.....	38

R

自動翻訳

L

自動翻訳

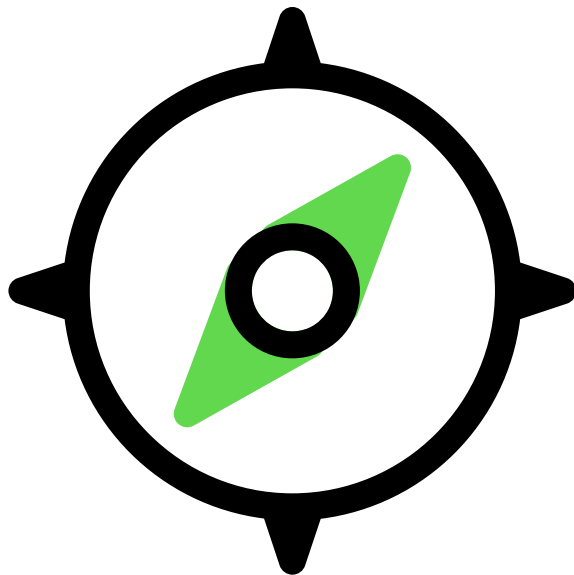
Proactive Service Experience Workflows

エンドツーエンドのサポートを提供すると同時に、顧客への影響を理解し、サポートプロセスに関与するすべての関係者に透明性の高いコミュニケーションを提供します。

次の図は、の主な Proactive Service Experience Workflows機能を示しています。

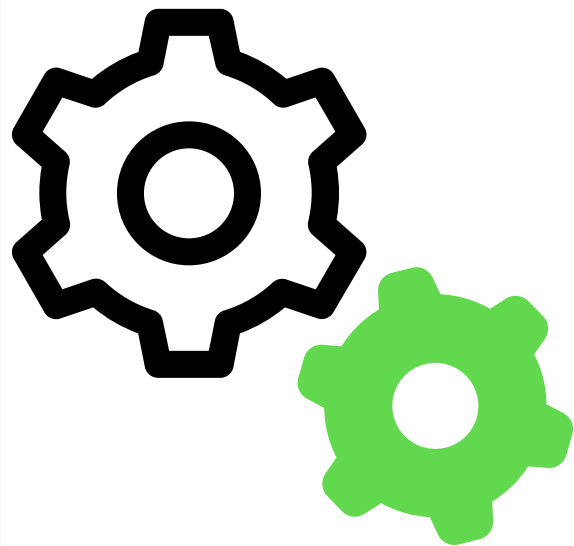


詳細を読む



サービスプロバイダーと顧客による Proactive Service Experience Workflowsの使用方法について説明します。

構成



実装を計画し構成します。

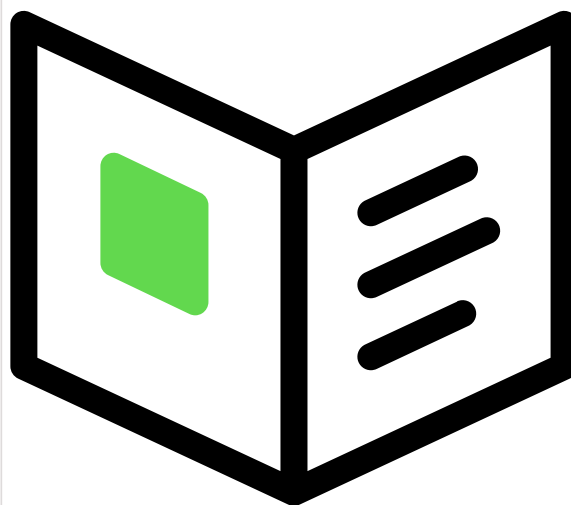
使用

参照

自動翻訳



Proactive Service Experience Workflowsの使用方法について説明します。



の Proactive Service Experience Workflows ドメイン分離に関する詳細を取得します。

アーキテクチャの Proactive Service Experience Workflows 探索

このアプリケーションを使用して、Proactive Service Experience Workflows ネットワークが開始したインシデントを解決するワークフローを自動的に開始し、影響を受ける顧客にプロアクティブに通知する方法について説明します。

ストアでアプリを要求する

ServiceNow Store Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「[ServiceNow Storeバージョン履歴のリリースノート](#)」を参照してください。

Proactive Service Experience Workflows 機能

Proactive Service Experience Workflows エンドツーエンドのサポートを提供すると同時に、顧客への影響を理解し、サポートプロセスに関与するすべての関係者に透明性の高いコミュニケーションを提供します。電気通信、メディア、またはテクノロジーサービスプロバイダーは、次のことができます。

- インストールベースに関連付けられたアップストリームサービスに関連付けられた 1 つ以上の構成アイテムに基づいて、影響を受ける顧客アカウントを特定します。
- Operations Account 360 では、顧客アカウントのデータ ITSM を使用して顧客 CSM アカウントにドリルダウンし、アカウントに関する重要な情報を視覚化します。
- ケースの挿入、インシデントの解決、または変更要求のクローズに関する特定のフィールドの同期を含む、積極的ケースを生成します。
- のインシデントフォームと変更要求フォームの強化により、管理セットアップとオーバーヘッドを削減します サービスオペレーションワークスペース。

- カスタマーサポートエージェントの介入なしで軽微なケースを解決します。
- テクニカルサポートエージェントが、インシデントや変更要求、および関連するケースレコード間を移動することなく外部顧客とやり取りする機能を提供します。
- ビジネスニーズに合わせて変更できる 5 つの一意の フローデザイナー フローを使用します。
- 事前設定された意思決定テーブルに基づいて、インシデントをエスカレートしてアクションを迅速化します。
- SD-Wan Edge インフラストラクチャに共通の拡張 CMDB CI クラスを使用する
- TM フォーラム TMF621 REST API 標準に基づいて、特定の API クライアントからインシデントレコードを作成します。
- テクニカルサポートエージェントが AND CSM と アプリケーションの両方ITSMを表示できるようにする専用のロールを使用します。

アプリケーションのアーキテクチャ コンポーネント Proactive Service Experience Workflows の詳細については、「」を参照してください [Proactive Service Experience Workflows アーキテクチャ](#)。

CI Class Models アプリケーションの一部としてCMDB、SD WAN エッジインフラストラクチャをターゲットとする CI クラスにクラスCMDBを追加することもできます。詳細は、「[CMDB の CI クラス Proactive Service Experience Workflows](#)」を参照してください。

Proactive Service Experience Workflows アーキテクチャ

アプリケーションのアーキテクチャ Proactive Service Experience Workflows は、複数のコンポーネントで構成されています。

主なコンポーネントは次のとおりです。

- フローとサブフロー
- エスカレーションステージ
- 決定表
- メッセージ
- ビジネスルール
- クライアントスクリプト
- システムプロパティ
- ロール
- アサイン先グループ
- サービスオペレーションワークスペース

フローとサブフロー

ワークフローは、インシデントが SD-WAN カテゴリと次の 5 つのサブカテゴリのいずれかで作成されるとトリガーされます。

- リンク障害
- デバイス障害
- プロトコル障害

- ソフト WAN リンク障害
- Software Failure

各カテゴリには、各アサイン先グループのサブフローと、合計 27 のサブフローのエスカレーションレベルがあります。これらのサブフローは、主にネットワーク操作の停止用に作成された開始点ですが、他のユースケースで再利用および拡張できます。

エスカレーションステージ

エスカレーションの 5 つのステージは次のとおりです。

- トリアージ
- L1 調査
- L2 調査
- L3 調査
- 解決

Proactive Service Experience Workflows はこれらのステージ値を使用して、インシデントエスカレーションポリシー [sys_hub_flow] 意思決定テーブルで適切な意思決定をトリガーします。このテーブルは、インシデントのエスカレーション中に正しいサブフローをトリガーします。エスカレーションの各ステージで、そのアサイン先グループのインシデントタスクが作成および管理されます。インシデント情報は、ビジネスルールからインシデントタスクに同期され、次の情報が含まれます。

- 簡単な説明
- 優先度
- ステータス
- アサイン先グループのアサインされたユーザーがインシデントに追加する作業メモ
- ワークフローによってインシデントに埋め込まれたメッセージコンテンツ

決定表

定義された条件に基づいて、フローデザイナー インシデントエスカレーションポリシー [sys_hub_flow] 意思決定テーブルと連携し、特定のエスカレーションポイントで生成するサブフローを決定します。

メッセージ

で Proactive Service Experience Workflows の各サブフローは、ネットワークが開始したインシデントのトラブルシューティング、エスカレーション、および解決にエージェントが使用する指示を提供するメッセージファイルに関連付けられています。内部トラブルシューティングプロセスのデフォルトの手順をカスタマイズする方法の詳細については、次を参照してください [メッセージ・ファイルのカスタマイズ](#)。

ビジネスルール

tsm インシデントタスクに同期するビジネスルールは、インシデントからインシデントタスクに同期する次のような情報を決定します。

- 簡単な説明
- 優先度
- ステータス

- アサイン先グループ
- アサイニー
- アサイン先グループのアサインされたユーザーがインシデントに追加する作業メモ

ロール

sn_ind_tsm_core.noc_agent ロールはアプリケーションで使用できますProactive Service Experience Workflows。このロールを追加すると、テクニカルサポートエージェントがアプリケーション間でITSMCSM関連情報を表示できるようになります。このロールには次のものが含まれます。

- itil
- wm_initiator
- wm_read
- sn_customerservice.case_viewer
- sn_customerservice.customer_data_viewer

このロールにはいくつかのアサイン先グループが含まれており、他のグループも admin ロールを持つことができます。sn_ind_tsm_sdwan.ticket_integrator ロールは、TMF 621 オープン API ユースケースから作成されたトラブルチケットに使用できます。

アサイン先グループ

ワークフローには、ネットワークコーディネーターやエンジニアなど、ネットワーク関連の担当者が関与します。すべてのアサイン先グループには基本 sn_ind_tsm_sdwanがあります。PSEW_USER システムロール。

注:

これらのアサイン先グループは、主にネットワーク運用サポート用に作成された開始点です。

ネットワークコーディネーター

ネットワークコーディネーターのタスクと責任は次のとおりです。

- ネットワーク管理システムからのインシデントの管理とトリアージ
- 影響度の評価とインシデントの優先度の定義
- 影響を受けるサービスを更新し、影響を受ける顧客のケースを作成します
- を使用してインシデントをオープンインシデントまたは変更要求と関連付ける エージェントアシスト
- インシデントをアサインし、ネットワークエンジニアリングと調整する

L1- ネットワークエンジニア

L1 - ネットワークエンジニアのタスクと責任は次のとおりです。

- ネットワークインシデントのトラブルシューティング
- フィールドサービスエージェント、サードパーティベンダー、OEM と連携して、通常のサービス運用を再開する
- および問題管理プロセスのトリガー 変更管理

L2:ネットワークエンジニア

L2 - ネットワークエンジニアのタスクと責任は次のとおりです。

- ネットワークインシデントのトラブルシューティング
- フィールドサービスエージェント、サードパーティベンダー、OEM と連携して通常のサービス運用を復元する
- および問題管理プロセスをトリガー変更管理して、有益な変更を導入したり、根本原因分析を実行したりします

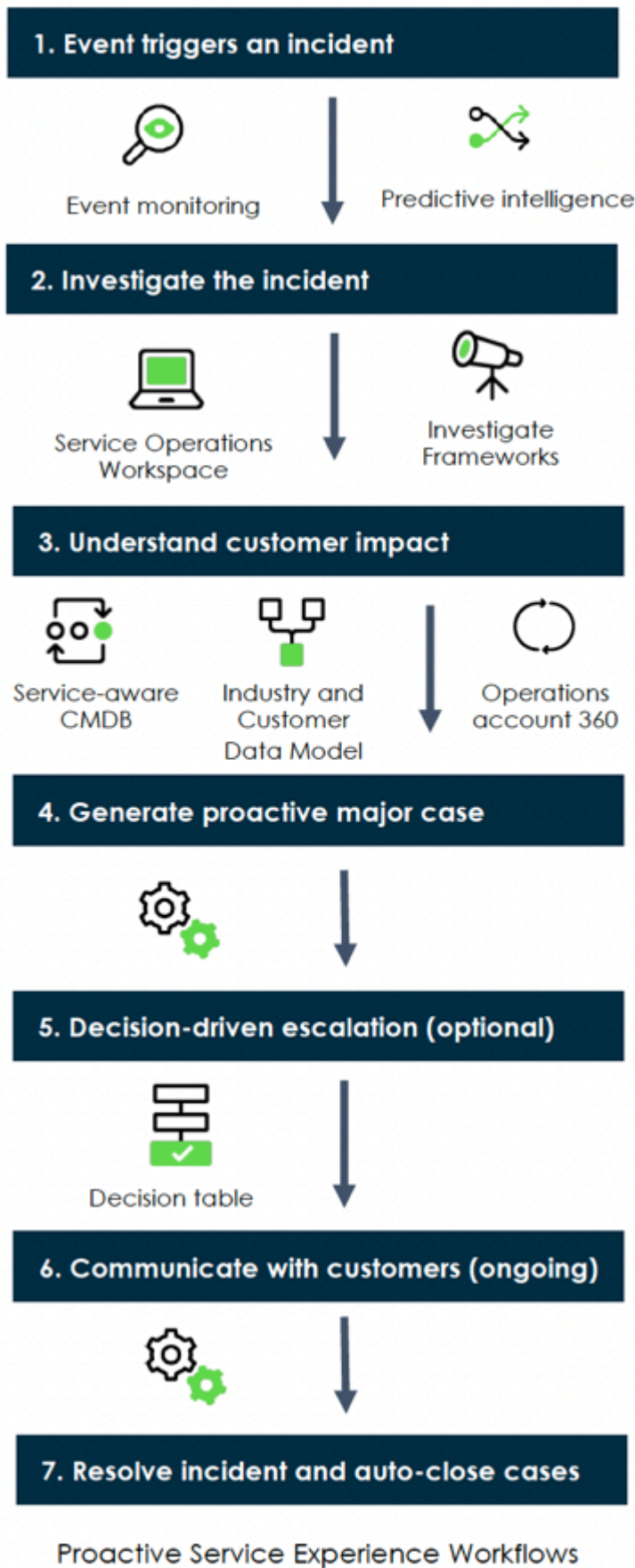
L3:ネットワークエンジニア

L3エンジニアのタスクと責任は次のとおりです。

- ネットワークインシデントのトラブルシューティング
- フィールドサービスエージェント、サードパーティベンダー、OEM と連携して通常のサービス運用を復元する
- および問題管理プロセスをトリガー変更管理して、有益な変更を導入したり、根本原因分析を実行したりします

Proactive Service Experience Workflows プロセス

次の図は、プロセスに関連する Proactive Service Experience Workflows 手順を示しています。



CMDB の CI クラス Proactive Service Experience Workflows

Proactive Service Experience Workflows は、CMDB CI Class Models アプリケーションの一部として、SD WAN エッジインフラストラクチャをターゲットとする 5 つの 構成管理データベース (CMDB) 構成アイテム (CI) クラスを追加します。

i 注:

このアプリケーションの詳細については、「[CMDB CI Class Models](#)」を参照してください。

電気通信保証ワークフローの CMDB CI クラス

クラス	説明	拡張された CI クラス
SD WAN コントローラ	すべての SD-WAN Edge に物理デバイスまたは仮想デバイス管理を提供するデバイス	cmdb_ci_Server_Hardware
SD WAN エッジ	アンダーレイ接続サービスと SD-WAN サービスの間にあるネットワーク機能(物理または仮想)	cmdb_ci_netgear
SD WAN エッジ ポート	外部ネットワークに接続するネットワークデバイスのソケット	cmdb_ci_netgear
ネットワーク回路	電気通信接続サービスを可能にする 2 つ以上のポイント間の個別パス	cmdb_ci
プロバイダーエッジ	SD WAN エッジポートとサービスプロバイダーのコアネットワーク間の接続ポイント	cmdb_ci_netgear

Proactive Service Experience Workflows そして インシデント管理、サービスオペレーションワークスペース

この サービスオペレーションワークスペース アプリケーションを使用して、ネットワークエージェントがタスクに優先順位を付け、インシデントを解決する方法の概要を把握できます。

の表示 サービスオペレーションワークスペース

[ワークスペース] メニューから [**Service Operations Workspace**] を選択し、[ホーム] アイコンを選択します。ネットワークエージェントは、ランディングページからインシデントを分析し、ケースと今後のタスクを表示できます。表示するには:

- リスト: の サービスオペレーションワークスペース[リスト] タブを選択します。ネットワークエージェントは、[リスト] タブで、インシデントとタスクの個々のリストを分析し、適切なアクションを実行できます。

次の例は、[リスト] タブを示しています。

[リスト] タブ

Number	Short description	Caller	Priority	State	Service	Assignment group
INC0010001	Software Failure for vManage_10001.	Abel Tuter	2: High	Resolved	SD WAN Enterprise Solutions	L2 Network Engineering
INC0009009	Unable to access the shared folder.	David Miller	4: Low	New	(empty)	(empty)
INC0009005	Email server is down.	David Miller	1: Critical	New	(empty)	(empty)
INC0009004	Defect tracking tool is down.	David Miller	3: Moderate	Closed	(empty)	(empty)
INC0009003	Cannot sign into the company portal app	David Miller	3: Moderate	Closed	(empty)	(empty)
INC0009002	My computer is not detecting the headphone device	David Miller	3: Moderate	Closed	(empty)	(empty)
INC0009001	Unable to post content on a Wiki page	David Miller	3: Moderate	New	(empty)	(empty)
INC0008112	Assessment : ATF Assessor	survey user	5: Planning	New	(empty)	(empty)
INC0008111	ATF : Test1	System Administrator	5: Planning	New	(empty)	(empty)
INC0008001	ATF:TEST2	survey user	5: Planning	New	(empty)	(empty)
INC0007002	Need access to the common drive.	David Miller	4: Low	New	(empty)	(empty)
INC0007001	Employee payroll application server is down.	David Miller	1: Critical	New	(empty)	Openspace
INC0005505	Software Failure for vManage_10001	Event Management	1: Critical	Closed	SD WAN Enterprise Solutions	L3 Network Engineering

- レコード: 次の例に示すように、任意のタスクレコードを開いてそのレコードビューに移動します。

レコードビュー

Software failure for Vmanage_10001.

Company: ACME South Ame... | Priority: 3: Planning | State: New | Stage: Triage | Needs attention: true | Configuration item: vManage_10001 | Opened: 2022-09-12 09:17...

Summary

Software failure for Vmanage_10001.

Impact 3: Low

Affected CIs: 1 | Impacted Services/CIs: 0 | Affected Accounts: 0

Cases: 0

Compose

Comments | Work notes (Private)

Type your Comments here

Everyone can see this comment | Post Comments

Activity

System | Work notes • 2022-09-12 09:18:23

Check the following information on the incident

- The Alarm details
- Affected Configuration Items
- Execute Refresh Impacted Services
- Identify Impacted Customers

Show more

Record Information

Last updated by system
2022-09-12 09:18:23

Origin

Caller: Abel Tuter
Product Management
Brasilia - 09:18 am America/Los_Angeles
Channel: Alert

Assigned to

This Incident has not been assigned yet

Assign incident

例

Proactive Service Experience Workflowsアラートフローによってシステム内でインシデントが作成されると、アプリケーションが自動的にトリガーされます。テクニカルサポートは、このアラートサービスオペレーションワークスペースを で手動で作成できます。また、TMF 621 統合を使用して、外部の障害管理システムから生成することもできます。

次の例は、ネットワークによって開始された外部インシデントの解決方法 Proactive Service Experience Workflows を示しています。この例では、次のようになります。

1. TMF 621 統合を使用する外部障害管理システムは、次の値を持つインシデントレコードの作成をトリガーするアラートを送信します。
 - 簡単な説明と説明: 変更が実装された後、Vmanage_10001を再起動できませんでした。
 - 構成アイテム: Vmanage_10001 (SD-WAN CI クラス)
 - カテゴリー: SD-WAN

- サブカテゴリ:プロトコル障害
 - 影響を受ける顧客:5
2. テクニカルサポートエンジニアがインシデント サービスオペレーションワークスペース レコードを開くと、影響を受けるサービスとアカウントのリストが [概要] セクションに表示されます。
 3. テクニカルサポートエンジニアは、機能停止のトリガーとなったエージェント支援の最新の変更を確認して、問題をトリアージします。
 4. テクニカルサポートエンジニアは、SD-WANコントローラを再起動し、[ケース]セクションで[プロアクティブなケースの生成]を選択します。1 つの重大なケースと 5 つの子ケースが生成され、影響を受けるアカウントの主要連絡先に通知が送信されます。
 5. 重大なケースが作成されると、テクニカルサポートエンジニアは、重大な機能停止の可能性を重大な問題マネージャーに通知します。重大な問題マネージャーは、重大なケースのレコードと、技術チームおよび影響を受ける顧客とのコミュニケーションを管理します。
 6. テクニカル サポート エンジニア (TSE) は、デバイスを再起動できず、完全に障害が発生している可能性があることに気付きました。TSE は [サブカテゴリ] フィールドを [デバイス障害] に変更し、[エスカレート] **UI** アクションを選択して作業メモを入力します
 7. 次のレベルの L2 サポートチームがインシデントを受信し、レコードのステータスを更新します。
 8. L2テクニカルサポートエンジニアは、SD-WANコントローラの問題のトラブルシューティングを試み、構成アイテムを正常に再起動します。影響を受けた 5 つのアカウントのうち 4 つで問題が解決したと報告されていますが、5 番目のアカウントではまだ問題が発生しています。
 9. 5 番目のアカウントの問題をさらに診断するために、L2 テクニカル サポート エンジニアは次の手順を実行します。
 - [概要] ページのケースレコードの横にあるチェックボックスをオンにします。
 - [通知] **UI** アクションを選択して、追加コメントを介してケースレコードの連絡担当者にメッセージを送信します。
 10. 連絡担当者は追加コメントを受信し、いくつかの追加手順を実行します。サービスが復元されると、連絡先はポータルで CSM ステータスを更新します。
 11. L2 テクニカルサポートエンジニアは、インシデントレコード内の追加のコメントを確認して、[State] フィールドを **[Resolved]** に変更します。

解決情報は各ケースレコードにコピーされ、重大な問題マネージャーは重大なケースレコードと関連するケースを解決します。

Proactive Service Experience Workflows の構成

アサイン先グループにユーザーを追加できるように構成できます Proactive Service Experience Workflows。また、自動的に提供されるワークフローを通じて、ネットワークが開始した問題を解決する際にエンジニアをガイドするカスタム手順を作成することもできます。

Proactive Service Experience Workflows のインストール

システム管理者ロールを持つユーザーの場合は、アプリケーションをインストール Proactive Service Experience Workflows できます。

始める前に

アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認します。詳細については、次を参照してください。 [のエンタイトルメントの取得 ServiceNow 製品またはアプリケーション](#)。

- 必要なロール：admin
- 必要なプラグイン: 次のプラグインがインストールされている必要があります。
 - カスタマーサービス管理 (CSM)
 - サービス管理によるカスタマーサービス
 - サービスオペレーションワークスペース

このタスクについて

Telecom コアアプリケーションは、次のものとともに Proactive Service Experience Workflows インストールされます。

手順

1. 移動先 **すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて**。
2. Proactive Service Experience Workflows フィルター基準と検索バーを使用してアプリケーション (sn_ind_tsm_sdwan) を検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、から ServiceNow Store 要求する必要があります。

[ServiceNow Store](#) Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「[ServiceNow Store バージョン履歴のリリースノート](#)」を参照してください。
3. アプリケーションのインストールダイアログボックスで、アプリケーションの依存関係を確認します。

含まれている、またはインストールする必要があるすべての依存プラグインとアプリケーションがダイアログボックスに一覧表示されます。
4. オプション: デモデータが利用でき、インストールするには、[デモデータのロード] を選択します。

(Optional) デモデータには、一般的なユースケース向けのアプリケーション機能を説明するサンプルレコードが含まれています。開発またはテストインスタンスで初めてアプリケーションをインストールする場合は、デモデータを読み込みます。

重要:

インストール時にデモデータを読み込んでおかないと、後から読み込むことはできません。

5. [インストール] を選択します。

アサイン先グループに **Proactive Service Experience Workflows** ユーザーを追加

ユーザー Proactive Service Experience Workflows をアサイン先グループに追加して、必要なロールを持ち、適切なエスカレーションレベルでネットワーク開始の問題を解決するためにアサインできるようにします。

始める前に

必要なロール：admin

手順

1. 移動先 すべて > ユーザー管理 > グループ.
2. グループ名を選択します。
4 つのアサイン先グループは次のとおりです。
 - ネットワークコーディネーター
 - L1 ネットワークエンジニアリング
 - L2 ネットワークエンジニアリング
 - L3 ネットワークエンジニアリング
3. [グループメンバー] 関連リストで、[編集] を選択します。
4. [コレクション] リストで 1 つ以上の名前を選択します。
5. [追加] を選択します。
6. [保存] を選択します。

Proactive Service Experience Workflows の使用

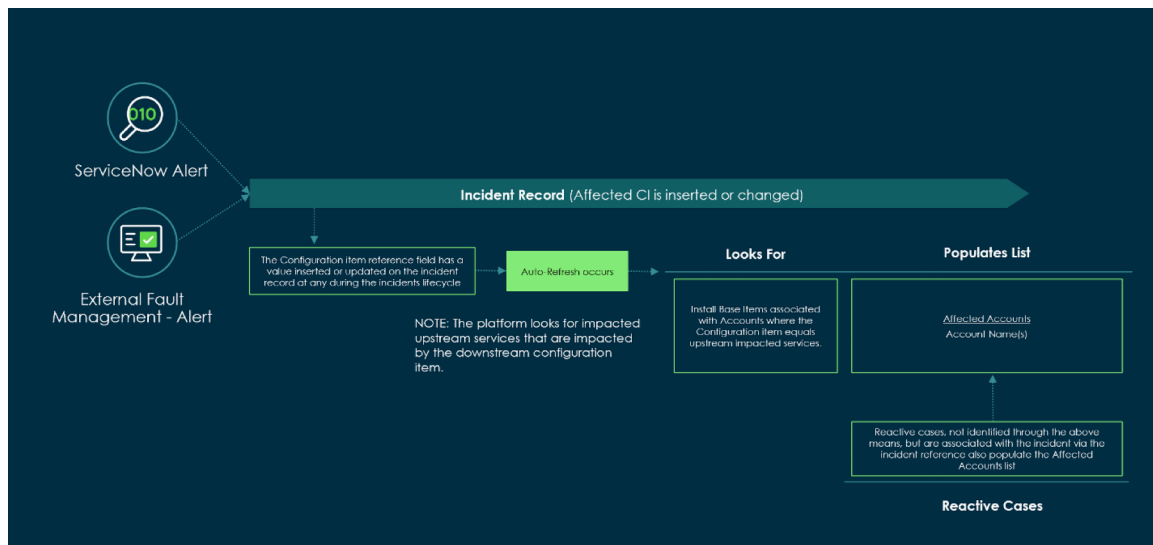
Proactive Service Experience Workflowsを使用すると、ネットワークが開始したインシデントを解決し、影響を受ける顧客に事前に通知することができます。このアプリケーションは、インシデント管理 ネットワーク管理システムによって検出される一般的な SD-WAN サービスの問題に対するアプリケーションを強化します。

での影響を受けるアカウントの Proactive Service Experience Workflows 特定について インシデント管理

イベント管理システムがアラートを生成したときにインシデントレコードが作成され、影響を受けるアカウントを で サービスオペレーションワークスペース表示できます。

テクニカルサポートエンジニアがログイン サービスオペレーションワークスペースすると、影響を受ける構成アイテム、サービス、および顧客が [概要] セクションに一覧表示されます。これらの詳細は、インシデントレコードの構成アイテムが更新されると自動的に更新されます。構成アイテムが更新されると、影響を受けるサービスのリフレッシュ スクリプトが自動的にトリガーされ、機能停止またはデグレードが発生しているサービスが取得されます。アカウントに関連付けられた影響を受けるサービスが特定され、更新されます。さらに、エージェントがケースをインシデントレコードに関連付けると CSM、[影響を受けるアカウント] リストも更新されます。[影響を受けるアカウント] リストが更新されると、顧客への影響がインシデントレコードで作業しているサポートチームに表示されます。

次の図は、インシデントレコードの作成に関連する手順を示しています。



注:

Change Management ワークフローも同じプロセスに従います。変更要求レコードで構成アイテムが更新されると、「影響を受けるサービスのリフレッシュ」スクリプトがトリガーされ、影響を受けるアカウントが取得されます。構成アイテムフィールドは読み取り専用で設定されているため、スクリプトがトリガーされる前にこのフィールドに値が入力されていることを確認する必要があります。詳細は、「[変更要求からのケース作成](#)」を参照してください。

Proactive Service Experience Workflows にインシデントを作成します。

で Proactive Service Experience Workflows インシデントレコードを作成し、顧客が直面している問題を文書化します。

始める前に

必要なロール:sn_ind_tsm_sdwanPSEW_USER、管理者

手順

1. 移動先 ワークスペース > サービスオペレーションワークスペース > インシデント > すべて。
2. インシデントリストビューから [新規] を選択します。
3. フォームのフィールドに入力します。

フォーム

フィールド	説明
簡単な説明	インシデントの簡単な説明
説明	インシデントの詳細な説明
番号	一意のシステム生成インシデント番号。
会社	ネットワークの問題に直面した顧客アカウント。
問い合わせユーザー	問題について連絡したユーザー。
ロケーション	問い合わせユーザーの場所。
チャネル	インシデントの作成に使用されるコミュニケーション方法。使用可能なオプションは、次のとおりです。 ○ チャット ○ メール

フィールド	説明
	- 電話 - Monitoring - セルフサービス - 仮想エージェント - ウォークイン
ステータス	いくつかの解決段階を通じたインシデントのステータス。
影響	インシデントまたは問題の影響度の測定。
緊急度	インシデントまたは問題がビジネスに重大な影響を与えるまで、解決を遅らせることができる時間の測定値。
優先度	影響度、緊急度、および解決をどの程度迅速に完了できるかに基づいています。
サービス	影響を受けるビジネスサービス。
サービスオファリング	可用性、スコープ、価格設定、およびパッケージングオプションのサービスレベルを一意に定義する 1 つ以上のサービスコミットメントで構成されるサービスオファリング。
構成アイテム	影響を受ける構成アイテム。
アサイン先グループ	インシデントを担当するグループ。
アサイン先	このインシデントを担当するユーザー。[アサイン先グループ] が変更された場合、[アサイン先] フィールドはクリアされます。
追加コメント	必要に応じて追加する、問題に関する詳細情報。追加コメントは、インシデントを表示できるすべてのユーザーに表示されます。
作業メモ	インシデントの解決方法に関する情報、またはインシデントの解決のために実行された手順 (該当する場合)。
カテゴリとサブカテゴリ	問題の種類。カテゴリを選択し、該当する場合は次にサブカテゴリを選択します。

4. [Save (保存)] を選択します。

タスクの結果

インシデントが作成されます。

のインシデントレコードからのケース作成 **Proactive Service Experience Workflows**

レコードからケースを作成し、企業顧客のネットワークの問題を特定して解決できるようにします。

始める前に

このタスクは、ワークフローがすでにトリガーされ、アサイン先グループがアサインされていることを前提としています。

必要なロール:sn_ind_tsm_sdwanPSEW_USER

このタスクについて

トリガーの Proactive Service Experience Workflows ワークフローの後、ネットワークの問題によって影響を受ける顧客とシステムを特定できます。その後、影響を受ける顧客の個々のケースを自動的に作成することも、影響を受ける多数の顧客に対して重大なケースと子ケースを作成することもできます。

手順

1. に移動し サービスオペレーションワークスペース、 を選択します リスト > インシデント > オープン。
2. リストからインシデントを選択します。
3. オプション: 既存のインシデントで、インシデントをアサインします。
4. [影響を受ける CI] カードを選択して、影響を受ける構成アイテム (CI) を確認します。
5. [影響するサービス/CI] カードを選択し、[影響を受けたサービスのリフレッシュ] を選択して、影響を受けるサービスを確認します。
6. [影響を受けるアカウント] カードを選択し、[影響を受けるアカウントの識別] を選択して、影響を受けるアカウントを確認します。
®
 ServiceNow インスタンスは、影響を受けるサービスを更新し、影響を受けるアカウントを検索するアクションを開始します。
7. [影響を受けるアカウント] カードを選択し、[名前] 列を確認して、影響を受ける顧客の名前を探します。
 通常、ネットワークコーディネーターは、影響を受ける顧客にネットワークが開始した問題が事前に通知されるようにケースを作成します。
8. [ケース] カードを選択し、[プロアクティブなケースを生成] を選択して、影響を受ける顧客のプロアクティブケースを生成します。
 - 影響を受けるアカウントの数がしきい値よりも少ない場合、このアクションは影響を受けるアカウントごとに 1 つのケースを作成します。それ以外の場合、このアクションは最初に重大なケースを作成してから、子ケース (影響を受けるアカウントごとに 1 つのケース) を作成します。
 - しきい値を変更する場合は、管理者に連絡してシステムプロパティの値 `sn_ind_tsm_core.major_case-affected_account_threshold` を変更してください。
 - [ケース] タブでは、重大なケースは [アカウント] 列と [連絡先] 列に [空] で示されます。その情報が入力されているケースは、その重大なケースの子ケースです。
9. アドホックケースを作成するには、リストからケースを選択し、[新規] を選択します。
10. 顧客に通知するには、ケースを選択し、[顧客に通知] を選択します。
11. [顧客に通知] ポップアップウィンドウで、説明的なメモを入力し、[通知] を選択します。

インシデントレコードの [アクティビティ] フィールドと、選択したケースレコードにもメモが自動的に挿入されます。顧客が何らかのメッセージでケースを更新すると、インシデントレコードとも自動的に同期されます。

i 注:

デフォルトでは、顧客への通知機能はアクティブではありません。管理者は、プロパティ値を `proactive_workflows_for_providers.additional_comments_sync` TRUE に設定する必要があります。この機能を有効にするには、BR (ビジネスルール) `Update case worknote for comments change` をオフにします。

12. インシデントの考えられる原因を更新する場合は、[原因] タブを選択し、メッセージを保存します。
13. インシデントレコードで [解決] を選択して、インシデントを解決します。
[解決 (Resolve)] ポップアップウィンドウで、解決コードと解決メモを入力し、[解決 (Resolve)] を選択します。

i 注:

軽微なケースのみが自動的にクローズされます。重大なケースでは、関連するすべてのケースを手動でクローズする必要があります。

タスクの結果

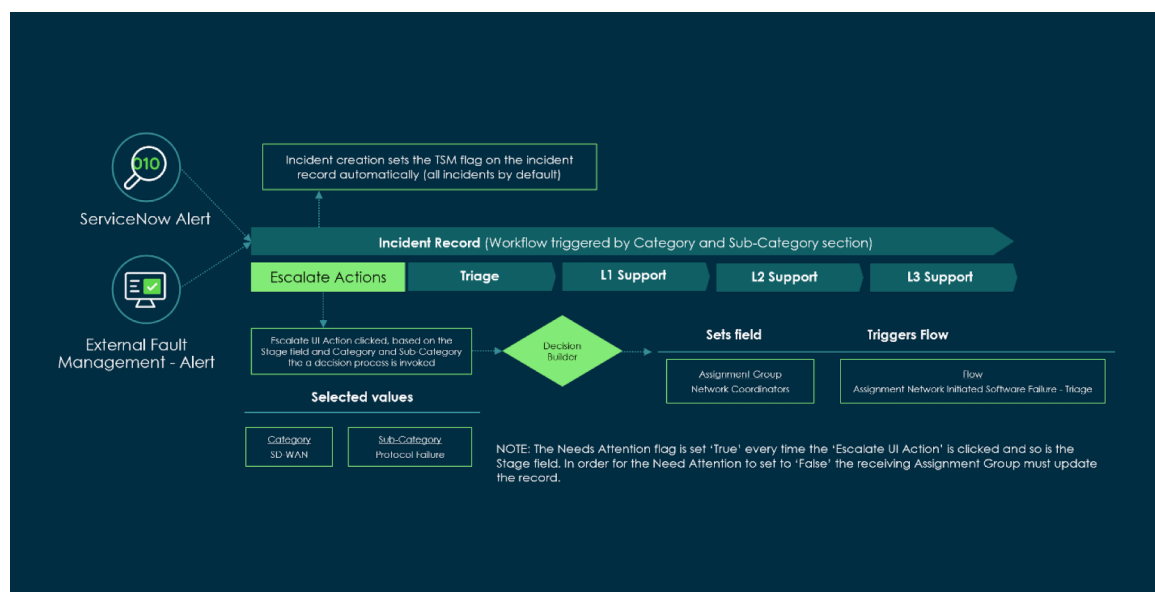
インシデントが解決されると、関連ケースの自動クローズがトリガーされます。

- 重大なケースがない場合、関連する個々のケースはすべて解決され、作業メモで更新されます。親インシデントレコードの次のフィールド値も、関連ケースに入力されます。
 - 解決メモ
 - 解決コード
 - [Probable Cause]
- 重大なケースがある場合、関連するケースは自動解決されず、インシデントレコードの作業メモに「このインシデントに関連付けられた重大なケースがあります。」というメッセージが追加されます。」という親インシデントレコードの次のフィールド値が、関連するすべての重大なケースと子ケースに入力されます。
 - 解決メモ
 - 解決コード
 - [Probable Cause]

インシデントのエスカレーションについて

エスカレーションは、インシデントが適切なカテゴリとサブカテゴリで作成され、その中で サービスオペレーションワークスペース[エスカレート] **UI** オプションがトリガーされたときにトリガーできます。

次の図は、エスカレーションフローを視覚的に表したものです。



ベースシステムでは、次のカテゴリとサブカテゴリの値が使用できます。

- カテゴリ: SD-WAN
- サブカテゴリ:
 - リンク障害
 - デバイス障害
 - プロトコル障害
 - ソフト WAN リンク障害
 - ソフトウェア障害

インシデントテーブルの [ステージ] フィールドでは、次の値を使用できます。

- トリアージ
- L1 調査
- L2 調査
- L3 調査

インシデントエスカレーションポリシー意思決定テーブルは、現在のステージ、カテゴリ、サブカテゴリなどの定義された条件に基づいて、結果と、必要に応じて次のエスカレーションステージを決定します。

Incident Escalation Policy

Created: 2020-06-25 13:43:53 | Application: Telecom Core | Properties | Close

▼ Inputs

Label	Type	Reference	Mandatory
Incident	Reference	Incident [incident]	☒

▼ Decision table

Conditions				Results	
	Category incident.category	Subcategory incident.subcategory	Stage incident.stage	Assignment Group group.name	Flow flow.name
1	SD WAN	Software failure		Network Coordinators	Network Initiated Software Failure - Triage
2	SD WAN	Protocol failure	L1 Investigation	L2 Network Engineering	Network Initiated Protocol Failure - L2
3	SD WAN	Link failure		Network Coordinators	Network Initiated Link Failure - Triage
4	SD WAN	Device failure	L1 Investigation	L2 Network Engineering	Network Initiated Device Failure - L2
5	SD WAN	Link failure	Triage	L1 Network Engineering	Network Initiated Link Failure - L1
6	SD WAN	Protocol failure	L2 Investigation	L3 Network Engineering	Network Initiated Protocol Failure - L3
7	SD WAN	Device failure	Triage	L1 Network Engineering	Network Initiated Device Failure - L1
8	SD WAN	Software failure	Triage	L1 Network Engineering	Network Initiated Software Failure - L1
9	SD WAN	Software failure	L2 Investigation	L3 Network Engineering	Network Initiated Software Failure - L3
10	SD WAN	Soft-WAN link failure		Network Coordinators	Network Initiated Soft-WAN Link Failure - Triage
11	SD WAN	Protocol failure	Triage	L1 Network Engineering	Network Initiated Protocol Failure - L1
12	SD WAN	Software failure	L1 Investigation	L2 Network Engineering	Network Initiated Software Failure - L2
13	SD WAN	Device failure	L2 Investigation	L3 Network Engineering	Network Initiated Device Failure - L3
14	SD WAN	Soft-WAN link failure	L1 Investigation	L2 Network Engineering	Network Initiated Soft-WAN Link Failure - L2

意思決定テーブルはアプリケーションに付属しています Proactive Service Experience Workflows。定義した条件と結果を要件に合わせて変更できます。意思決定テーブルの更新の詳細については、次を参照してください [Decision Tables](#)。

インシデントがエスカレートされると、[要注意] フィールドのステータスが **True** に更新されます。[アサイン先グループ] フィールドのオーナーは、ステータスを **[False]** に変更できます。

注:

システム管理者は、「要注意を **false** に設定」ビジネスルールを設定できます。

でのインシデントのエスカレーション Proactive Service Experience Workflows

インシデントをエスカレートして、そのインシデントの調査と診断を続行します。インシデントをエスカレートすることで、経験豊富なリソースに支援を求めることができ、問題をより迅速に解決することができます。

始める前に

このタスクでは、インシデントの作業が既に行われており、次のエスカレーショングループにエスカレートする必要があることを前提としています。

注:

管理者によってこのロールがエスカレーショングループにアサインされていることを確認してください。管理者がロールを割り当てる方法については、「[グループへのロールの割り当て](#)」を参照してください。

必要なロール:sn_ind_tsm_core.noc_agent

手順

1. で、 サービスオペレーションワークスペース次に移動します: リスト > インシデント > オープン インシデントを選択します
2. インシデントレコードフォームで、右上隅のドロップダウンリストから [エスカレート] を選択します。
3. [エスカレーションのメモをキャプチャ] ポップアップウィンドウで、説明的なメモを入力し、[エスカレート] を選択します。
このアクションにより、次のレベルのエスカレーショングループのサブフローがトリガーされ、アサイン先グループが自動的に次のエスカレーショングループに変更されます。

タスクの結果

- 前のエンジニアのインシデントタスクのステータスが [完了してクローズ] に設定され、作業メモがログに記録されます。
- 新しくアサインされたユーザーに対して、ステータスが [対応中] に設定されたインシデントタスクが作成されます。
- アクティビティストリームの作業メモには、このエスカレーションレベルのエンジニア向けの指示が記載されています。
- インシデントステージは、次のエスカレーションレベルで更新されます。
- アサイン先グループは、エスカレーションレベルに応じて更新されます。

での顧客またはパートナーアカウントの確認 **Proactive Service Experience Workflows**

テクニカルサポートチーム(例: クラウド運用チーム、サーバーチーム、またはネットワーク運用チーム) は、アプリケーションのオペレーションアカウント 360 ビュー Proactive Service Experience Workflows を使用して、顧客またはパートナーのアカウントに関するインサイトを取得できます。

テクニカルサポートエージェントは、で顧客またはパートナーのアカウント サービスオペレーションワークスペースに関連付けられたタスク、エスカレーション、主要な顧客データ、測定基準に関連する情報を収集できます。このデータを使用して、次のタイプの情報を追跡できます。

- 顧客またはパートナーが誰で、どのような製品、サービス、資産、構成アイテムが販売されていますか。
- テクノロジープロバイダーと顧客/パートナーの両方の主要連絡先。
- テクノロジープロバイダーと顧客またはパートナーの CSAT スコアとは何か。
- テクノロジープロバイダーと顧客またはパートナーが、その月の SLA の観点からどのように追跡しているか。
- アカウントに影響を与えている重大なインシデント、ケース、およびエスカレーション。

- クローズされているタスクの数 (タイプ別) および 12 週のローリングベースでオープンされているタスクの数。
- アカウント用に開発された特定のナレッジ記事およびカタログアイテム。この情報を使用して、エージェントは、顧客またはパートナーが何を望んでいるか、およびどのようなアクションを実行する必要があるかについてのインサイトを得ることができます。

運用アカウント 360 ビュー内で サービスオペレーションワークスペース 可視化されるデータは、このビューの起動時に選択したアカウントと会社の値が等しいタスクレコードから派生します。ただし、ナレッジ記事とカタログアイテムは例外です。

さらに、運用アカウント 360 ビューは、クラス値がアカウントに等しい会社レコードに対してのみ機能します。クラス値が会社である会社レコードには、Service Operations Workspace の従来のデフォルトのワークスペースビューが表示されます。

アカウント インサイトの取得の詳細については、次を参照してください [で 360 度ビューを使用してアカウントをレビューする Proactive Service Experience Workflows](#)。

で 360 度ビューを使用してアカウントをレビューする Proactive Service Experience Workflows

内のサービスオペレーションワークスペースアプリケーションによってProactive Service Experience Workflows提供されるオペレーションアカウント 360 ビューを使用して、顧客またはパートナーのアカウントを確認します。顧客またはパートナーに関連するデータとタスクを追跡し、サービスの提供を改善するためのアクションを実行できます。

始める前に

必要なロール:sn_ind_tsm_core_noc_agent

手順

1. 移動先 ワークスペース > サービスオペレーションワークスペース。
2. [Service Operations Workspace **Lists**] タブで、 アカウント > すべて。
3. [アカウント] リストで、顧客アカウントを選択します。

i 注:

このビューには、さまざまなインシデント リスト内またはの サービスオペレーションワークスペースインシデント フォーム内で会社 (アカウント) 名のアカウントをクリックしてアクセスすることもできます。

4. [アカウント情報] ページの [顧客の概要] セクションで、顧客のアクティブ状態、ランク階層、従業員数など、選択したアカウントの一般的な顧客の詳細を確認します。

このアカウントにエスカレーションがある場合は、[エスカレーションの表示] をクリックして表示できます。[概要] セクションで、アカウント情報に関するインサイトを表示します。

[アカウント情報] ページ - [アカウントの概要] タブ

フィールド	説明
アカウントチームメンバー	この顧客のチームメンバー。[すべて表示] をクリックすると、すべてのチーム メンバーの一覧が表示されます。
主要な顧客連絡先	この顧客の重要な連絡先。[すべて表示] をクリックして、すべての主要な顧客連絡先のリストを表示します。

フィールド	説明
単一スコアカード	- 契約 - エンタイトルメント - CSAT i 注: 結果は、コア CSM プラグインによって提供される標準提供の顧客満足度サーベイに関連付けられたアセスメントから得られます。 - エスカレーションケース - 販売済み製品 - インストールベース - 資産 - 構成アイテム
継続的なテクニカルサポート作業	- クローズ済みタスク - 週次新規タスクとクローズ済みタスク - 現在の月のタスク SLA 達成度
変更あり	アカウントで発生した変更要求
問題	アカウントに関連する問題
インシデント	アカウントに関連するインシデント
インシデント SLA	アカウントに関連するインシデント SLA
機能停止	アカウントに関連する機能停止
要求	アカウントに関連する要求
ケース	アカウントに関連するケース
コンテキストサイドパネル	- 添付ファイル - テンプレート - アカウント支援 i 注: 重大なインシデント、重大なケース、ナレッジ、記事、またはカタログアイテムを検索することもできます。

5. [関連レコード] ページには、デフォルトで次のリストが表示されます。

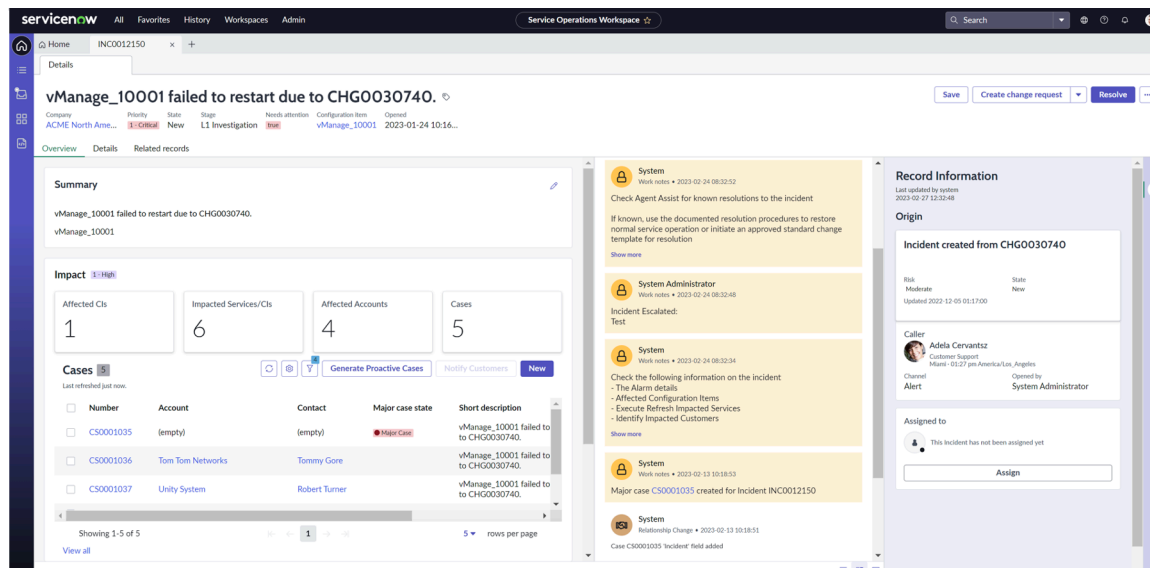
- ユーザー
- 連絡先
- アカウントの住所

- 製品モデル
- ベンダーカタログアイテム

インシデントからのケースおよび更新の自動作成

[プロアクティブなケースを生成] フラグが選択されている場合、ケースがインシデントから自動的に作成されます。

ケースは、 `major_case_affected_account_threshold` システムプロパティで指定された値に基づいて、重大なケースとして指定されます。この値は管理者が変更できます。



しきい値に応じて、さまざまなフローがトリガーされ、重大なインシデントが 1 つまたは複数の個別ケースが作成されます。ケースレコードが入力されます。たとえば、軽微なケースのシナリオでは、次の情報が入力されます。

- 簡単な説明
- 説明
- プロアクティブが true
- チャンネル
- インシデント
- アカウントフィールド

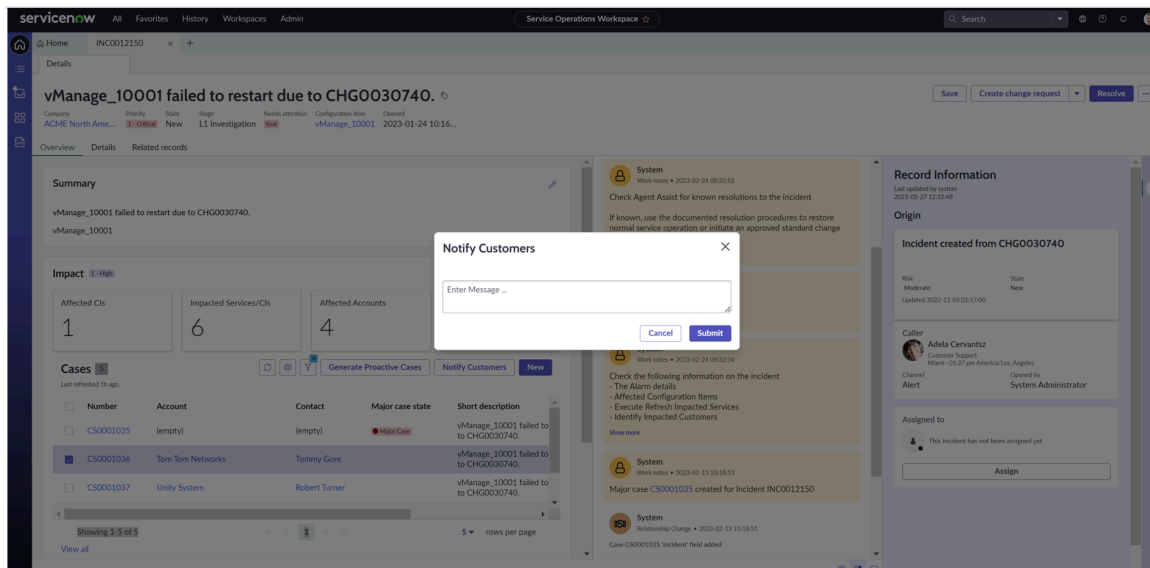
管理者は、業務ニーズに合わせて、親インシデントレコードからケースレコードに渡す必要があるフィールドを指定できます。

ケース情報を顧客に通知

サービスオペレーションワークスペースで、[ケース] セクションから 1 つ以上のケースを選択し、[顧客に通知] を選択できます。

通知メッセージを入力し、[送信] を選択します。メッセージは、ケースレコードと一緒に [追加コメント] セクションに含まれ、顧客に送信されます。顧客がメールまたはポータルのもので CSM これらのコメントに回答すると、これらのコメントがインシデントレコードにコピーされます。テクニカルサポートエンジニアは、ケースの確認中に提供された応答またはその他のフィードバックを表示できます。

自動翻訳



注:

この機能を有効にするには、次の手順を実行します。

- アプリケーションナビゲーターで、「sys_properties.list」と入力します。
- テキストフィールドで `proactive_workflows_for_providers.additional_comments_sync` システムプロパティを検索します。
- システムプロパティを選択してレコードを開きます。
- 「値」フィールドに「true」と入力し、「更新」を選択します。

追加のコメントがインシデントに関連するすべてのケースにコピーされないようにするには、インシデントテーブルの **Update case worknote for comments change** ビジネスルールを非アクティブ化します。

自動生成ケースの重大ケースしきい値の設定

システムプロパティのインシデントから生成される重大なケースのしきい値を設定します。

始める前に

- 必要なロール：admin
- 選択したアプリケーションスコープ: Proactive Service Experience Workflows

このタスクについて

デフォルトのしきい値は、インシデントから重大なケースを生成するように事前定義されています。この値が小さすぎるか、組織で CSM 重大ケース管理機能を使用していない可能性があります。このような場合は、有効にした後 Proactive Service Experience Workflows でシステムプロパティのしきい値を変更できます。

手順

1. アプリケーションナビゲーターで、「sys_properties.list」と入力します。
2. テキストフィールドで システムプロパティ `major_case_affected_threshold` 検索します。
3. システムプロパティをクリックしてレコードを開きます。
4. [値] フィールドのしきい値数値を変更します。

i 注:

整数値が小さいほど、重大なケースをトリガーするために必要なケースの数が多くなります。より大きな数値を指定すると、その逆が真になります。

5. [Update (更新)] をクリックします。**変更要求からのケース作成**

の変更実装が完了した後に、サービス停止とその解決について顧客に通知できるように、の変更 Proactive Service Experience Workflows 要求からケースを作成します。

始める前に

変更ワークフローがトリガーされました。開始予定日と終了予定日を含むアサイン先グループが既に設定されています。

必要なロール：admin

このタスクについて

で Proactive Service Experience Workflows 変更ワークフローがトリガーされた後、変更要求の影響を受ける顧客とシステムを特定できます。その後、影響を受ける顧客の個々のケースを自動的に作成したり、機能停止について顧客に通知したりすることができます。

手順

1. [サービスオペレーションワークスペース] で、次に移動します。 リスト > 変更あり > オープン をクリックし、変更レコードを選択します。
 2. オプション: 既存の変更レコードで、サポート エンジニアに変更要求をアサインします。
 3. [スコープと影響] セクションを展開し、[影響を受ける CI] カードを選択します。
 4. [影響を受けるサービス] カードを選択し、[影響を受けたサービスのリフレッシュ] を選択して、影響を受けるサービスを確認します。
- インスタンスは、影響を受けるサービスを更新し、影響を受けるアカウントを検索するアクションを開始します。
5. [機能停止] カードを選択して、機能停止のリストを表示します。
 6. [影響を受けるアカウント] カードを選択して、影響を受けるアカウントを確認します。
 7. [詳細] セクションで、変更レコードのステータスを [許可] に変更します。
感染した顧客のケースが自動的に作成されます。
 8. 作成されたサポート案件の一覧からサポート案件を選択し、新規 を選択します。
 9. 顧客に通知するには、顧客のケースを選択し、[顧客に通知] を選択します。
 10. [顧客に通知] ポップアップウィンドウで、ケースに関する説明を入力し、[通知] を選択します。

変更レコードの [アクティビティ] フィールドと選択したケースレコードにメモが自動的に挿入されます。顧客がメッセージを使用してケースを更新すると、ケースは自動的に変更レコードと同期されます。

i 注:

デフォルトでは、顧客への通知機能はアクティブではありません。管理者として、これをアクティブにするには、プロパティ値を TRUE に設定し `proactive_workflows_for_providers.additional_comments_sync` から、を選択する `Update case worknote for comments change` 必要があります。

11. 変更マネージャーが変更レコードを許可し、ステータスが [スケジュール済み] に変更されると、[実装] を選択し、[レビュー] を選択してからレコードを保存することで、ステータスを更新できます。
12. ドロップダウンリストから解決コードを選択し、変更要求をクローズする前に解決メモを入力し、[クローズ] を選択してステータスを更新します。

のエスカレーションワークフローで使用されるメッセージについて

Proactive Service Experience Workflows

インシデントのエスカレーションフロー内で使用される複数のメッセージは、ベース Proactive Service Experience Workflows アプリケーションで使用できます。

これらのメッセージは、インシデントのトラブルシューティング、エスカレーション、および解決のためのテクニカルサポートエンジニアへの指示を提供します。ベース システムで提供されるものは、ネットワークによって開始される一般的なインシデントに対処しますが、トラブルシューティング プロセスに合わせて変更できます。

のメッセージ・ファイルのカスタマイズ Proactive Service Experience Workflows

で Proactive Service Experience Workflows、さまざまなサブカテゴリ、エスカレーションのレベル、ペルソナについて、ネットワークによって開始された問題に取り組んでいるネットワークエンジニアへの指示を提供するメッセージをカスタマイズします。

始める前に

必要なロール：admin

このタスクについて

の各 Proactive Service Experience Workflows サブフローは、ネットワークが開始したインシデントのトラブルシューティング、エスカレーション、および解決にエージェントが使用する指示を提供するメッセージファイルを参照します。デフォルトのメッセージテキストを使用することも、内部トラブルシューティングプロセスに合わせてテキストをカスタマイズすることもできます。

手順

1. 移動先 **すべて > システム UI > メッセージ**。
2. **sd_wan**を含むキー値を検索します。
3. カスタマイズするテキストを含むレコードを選択します。
4. [メッセージ] フィールドで、そのサブカテゴリ、ペルソナ、およびエスカレーションのレベルに関する指示を入力します。
5. [更新] を選択します。

トラブルチケット通知の処理

電気通信トラブルチケット通知を使用して、インスタンスで事後対応的または積極的な方法で作成されたインシデントまたはケースについてサードパーティシステムに通知し ServiceNow ます。お客様は、インシデントの更新に関する通知を受け取ります。

概要

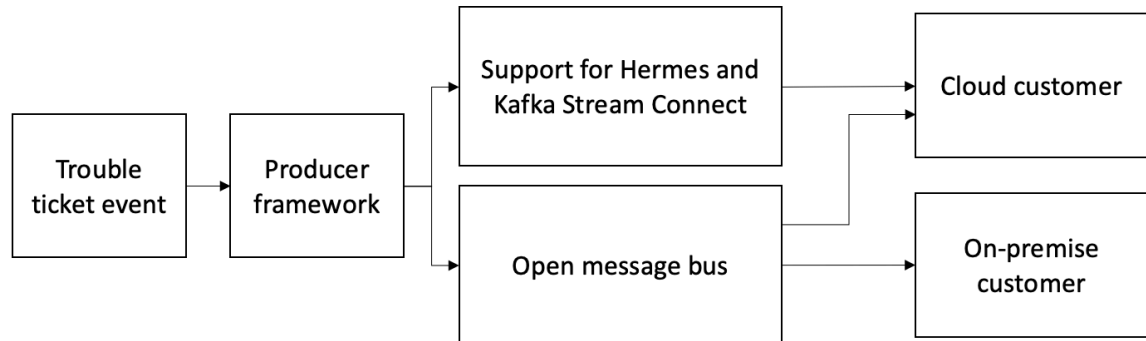
TMF エコシステムのトラブルチケットは、顧客から報告された問題、ネットワーク停止、またはその他の問題を追跡して解決するインシデントです。トラブルチケットインシデントは、事後対応型または積極的な方法で作成できます。事後対応型のアプローチでは、システム障害が原因で報告された

ケースの根本原因分析 (RCA) を実施した後にインシデントが生成されます。プロアクティブなアプローチでは、アラートを受信した後にインシデントが生成されるため、RCA またはサービス影響分析 (SIA) を実行してサービスへの影響を評価できます。トラブルチケット通知機能を使用すると、インシデントの詳細を送信システムに送信できます。

トラブルチケット通知フレームワーク

次の図は、トラブルチケット通知のフレームワーク内のコンポーネントを示しています。

トラブルチケット通知データモデル



トラブルチケット通知は、汎用フレームワークを使用して送信通知を外部システムに送信します。このフレームワークは、次の 2 つのユースケースをサポートしています。

1. Hermes メッセージングサービスを使用して、Hermes Kafka にメッセージを公開します。Hermes Kafka を使用するクラウドの顧客は、このアーキテクチャを使用して通知を受信できます。

詳細については、「[Hermes を使用した送信トラブルチケット通知の生成](#)」を参照してください。

2. 開いているメッセージ バスにメッセージを公開します。このユースケースはメッセージバスに依存しないため、開いているメッセージバスへの通知の公開をサポートします。クラウドとオンプレミスの両方のお客様がこのユースケースを使用できます。詳細については、「[オープン・メッセージ・バスを使用したアウトバウンド・トラブル・チケット通知の生成](#)」を参照してください。

Hermes を使用した送信トラブルチケット通知の生成

Hermes 機能を使用して、インスタンスからの ServiceNow 送信通知を生成します。顧客は、Kafka 環境からのメッセージの詳細を外部システムで使用できます。

概要

このユースケースでは、インスタンスから ServiceNow Hermes クラスターへの通知が生成されます。Hermes から Kafka へのレプリケーションが完了すると、顧客は独自の Kafka からメッセージを消費またはプルできます。

- Hermes Messaging Service の詳細については、「」を参照してください [Hermes Messaging Service](#)。
- Apache Kafka Stream Connect の詳細については、「」を参照してください [Using Stream Connect for Apache Kafka](#)。

Washington DCこのリリースでは、トラブルチケット通知で次のイベントがサポートされています。

- トラブルチケットイベントを作成
- トラブルチケットステータス変更イベント

- トラブルチケット属性変更イベント
- ケースのトラブルチケットイベントを作成

前提条件

送信通知を生成する前に、顧客は Hermes クラスターにトピックを作成する必要があります。Hermes でのトピックの作成の詳細については、次を参照してください [Managing namespaces and topics in Hermes](#)。

ワークフロー

Hermes を使用して送信通知を生成するワークフローには、次のステップが含まれています。

1. トラブルチケットイベントがトリガーされると、システムは適切なビジネスルールを呼び出し、イベントタイプをスタンプします。

インスタンスに追加する ServiceNow 必要があるビジネスルールの詳細については、「」を参照してください [Add a business rule for a new trouble ticket event](#)。

2. システムは、キューとして機能するステージングテーブルに Glide スナップショットとイベントタイプをプッシュします。
3. プロデューサーフレームワークはイベントを選択し、TMF 688 苦情イベントペイロードに変換します。

プロデューサーフレームワーク用に構成する必要があるシステムプロパティの詳細については、次を参照してください [送信通知にプロデューサーフレームワークを使用する](#)。

4. システムは Stream Connect のプロデューサー V2 API を呼び出し、Hermes Kafka トピックでイベントを生成します。
5. Stream Connect は、Hermes Kafka クラスターにイベントをプッシュします。
6. 顧客は、社内の Kafka でメッセージを消費できます。

関連情報

[EventProcessorUtilOOB - Scoped](#)

[EventQueueProcessorOOB - Scoped](#)

オープン・メッセージ・バスを使用したアウトバウンド・トラブル・チケット通知の生成

オープンメッセージバスを使用して、ServiceNow インスタンスからの送信通知を生成します。顧客は、外部システムのメッセージバスからの通知の詳細を消費できます。

概要

このイベント駆動型アーキテクチャでは、インスタンスから ServiceNow オープンメッセージバスへの通知が生成されます。フレームワークには、トピックの同期メカニズムとトピックピッカーメカニズムが含まれています。トピック同期メカニズムは、インスタンスで ServiceNow 作成したトピックをオープンメッセージバスと同期します。フレームワークでイベントが発生すると、トピックピッカーメカニズムによって関連するトピックが選択され、REST プロキシを使用してトピックにメッセージが公開されます。顧客は、外部システムのメッセージバスからの送信通知を消費できます。

Washington DCこのリリースでは、トラブルチケット通知で次のイベントがサポートされています。

- トラブルチケットイベントを作成
- トラブルチケットステータス変更イベント
- トラブルチケット属性変更イベント
- ケースのトラブルチケットイベントを作成

前提条件

送信通知を生成する前に、インスタンスの ServiceNow トピック [sn_api_notif_mgmt_topic] テーブルにエグレストピックを作成する必要があります。エグレストピックを作成すると、システムはビジネスルールを実行し、構成に基づいてトピックをメッセージバスに同期しようとします。トピックテーブルでトピックを手動で作成する方法の詳細については、「」を参照してください [Create a topic](#)。システムは、出力トピックのみを外部システムのメッセージバスと同期します。関連するトピックレコードの **[user_created]** フィールドが true に設定されている。

または、外部システムのメッセージバスにトピックを作成し、インスタンスの ServiceNow トピックテーブルにプッシュすることもできます。顧客が *Event Management Topic Open API* エンドポイント呼び出し、インスタンスのトピック [sn_api_notif_mgmt_topic] テーブル ServiceNow にトピックを格納します。関連するトピックレコードの **[user_created]** フィールドが false に設定されている。*Event Management Topic Open API* エンドポイントの処理時に使用されるメソッドの詳細については、「」を参照してください [Event Management Topic Open API](#)。

ワークフロー

オープン メッセージ バスを使用して送信通知を生成するワークフローには、次の手順が含まれます。

1. トラブルチケットイベントがトリガーされると、システムは適切なビジネスルールを呼び出し、イベントタイプをスタンプします。

インスタンスに追加する ServiceNow 必要があるビジネスルールの詳細については、「」を参照してください [Add a business rule for a new trouble ticket event](#)。

2. システムは、キューとして機能するステージングテーブルに Glide スナップショットとイベントタイプをプッシュします。
3. プロデューサーフレームワークはイベントを選択し、TMF 688 苦情イベントペイロードに変換します。

プロデューサーフレームワークの詳細については、を参照してください [送信通知にプロデューサーフレームワークを使用する](#)。

4. トピックピッカーのメカニズムによって、イベントタイプと互換性のあるトピックが決まります。トピックピッカーは、次の手順を実行してトピックの互換性を確認します。
 - a. トピックテーブルで [タイプ] フィールドが [エグレス] に設定されているトピックがスキャンされます。
 - b. システムは、すべてのエグレストピックのヘッダークエリとコンテンツクエリをチェックし、イベントペイロードとの互換性を照合します。
既存のトピックピッカーメカニズムをカスタマイズする方法の詳細については、「」を参照してください [OpenMessageBusEventPublisherOOB - Scoped](#)。
5. 互換性のあるトピックのリストとイベントペイロードがスポークセクターに送信されます。
6. 顧客が設定したスポークセクターは、各トピックに設定された REST ステップを呼び出し、外部システムのメッセージバス REST プロキシに送信します。

スポークセレクトにメッセージを送信する方法の詳細については、「」および[Configure the Producer Event Notification Framework to use the Open Message Bus](#)「」を参照してください。[OpenMessageBusEventPublisherOOB - Scoped](#)。

7. 顧客はメッセージバス REST Proxy でメッセージを消費できます。

関連情報

[EventProcessorUtilOOB - Scoped](#)

[EventQueueProcessorOOB - Scoped](#)

[Handling the external events using Telecommunications API notification](#)

送信通知にプロデューサーフレームワークを使用する

プロデューサーフレームワークはインスタンスから ServiceNow イベントを選択し、送信通知を外部システムに送信します。外部システムにインストールされているメッセージングサービスからの通知の詳細を消費できます。

システムプロパティ

送信通知にプロデューサーフレームワークを使用するには、システムプロパティを設定する必要があります。次の表では、ジョブスケジュールに設定されているシステムプロパティのリストについて説明します。

プロデューサーフレームワークのシステムプロパティ

プロパティ	説明	タイプ
sn_api_notif_mgmt.event.log	デバッグログに書き込まれるログのレベル。次のロギングレベルを選択できます。 • emerg: 全面的な失敗。 • alert: たとえば、データベースのシステムが破損しています。 • crit: 通常、ハードウェアエラーなどに使用されます。 • err: エラー。 • warning: 警告 • 注意: 必要なアクションは可能ですが、必須ではありません。 • 情報: アクションは必要ありません。 • debug: 通常、障害検出のためにすべてをキャプチャする以外には使用されません。 デフォルト値: err	文字列

プロデューサーフレームワークのシステムプロパティ (続く)

プロパティ	説明	タイプ
sn_api_notif_mgmt.publisher_message_configuration	Message Configuration Service、Open Message Bus、またはその両方のメッセージバスを使用してメッセージを公開するかどうかを定義します。次の値を使用できます。 • openMessageBus • エルメス • 両方とも デフォルト値: openMessageBus	文字列
sn_api_notif_mgmt.inboundQueue.maxRecords	1回のスケジューラー実行でスケジューラーが受信キューからプルするレコードの最大数。この値は、<code>sn_api_notif_mgmt.inboundqueue.batch.limit</code> パラメーターと組み合わせて使用されます。 • デフォルト値: 200 • 使用可能なその他の値: 必要に応じて たとえば、バッチ制限が 50 に設定され、maxrecords が 200 に設定され、受信キュー内のレコードの数が 130 の場合、スケジューラーは 1 回の実行で 3 つの異なるバッチのレコードをプルします。2 つは 50 レコード、もう 1 つは 30 レコードです。受信キューのレコード数が 220 の場合、スケジューラーは 50 レコードの 4 つのバッチをプルし、残りの 20 レコードは次にスケジューラーが実行されるまで処理されません。 この値を設定するときは、スケジューラーが複数のバッチを処理するのにかかる時間も考慮し、それに合わせて <code>sn_api_notif_mgmt.schedule.max.runtime</code> 値を設定する必要があります。	整数
sn_api_notif_mgmt.inboundQueue.batchLimit	スケジューラーが受信キューから 1 つのバッチでプルして処理するレコードの数。	整数

プロデューサーフレームワークのシステムプロパティ (続く)

プロパティ	説明	タイプ
	- デフォルト値: 200 - 使用可能なその他の値: 必要に応じて	
sn_api_notif_mgmt.glide.mutex.acquire.max spins	受信点 max spins でミューテックスロックを取得する最大試行回数 - タイプ: 整数 - デフォルト値: 100 - 使用可能なその他の値: 必要に応じて	整数
sn_api_notif_mgmt.schedule.max runtime	max runtime 設定済みジョブが失敗してエラーを報告するまでに実行できる最大時間 (ミリ秒)。 - タイプ: 整数 - デフォルト値: 90000 - 使用可能なその他の値: 必要に応じて	整数
sn_api_notif_mgmt.glide.mutex.acquire.spin wait	受信点 spin wait のダウンロードに対するミューテックスロックの取得を試行する間に待機する最大時間 (ミリ秒)。 - タイプ: 整数 - デフォルト値: 100 - 使用可能なその他の値: 必要に応じて	整数

プロデューサーフレームワークのワークフロー

イベントがステージングテーブルにプッシュされると、プロデューサーフレームワークメカニズムの一部として次の手順が実行されます。

1. スケジューラーは、事前設定された間隔で多数のレコードを選択し、Glide スナップショットをイベントプロセッサに送信します。
2. イベントタイプに基づいて、Glide スナップショットが TMF 688 苦情イベントペイロードに変換されます。

トラブルチケットイベントの TMF 準拠のペイロードを定義および生成するために使用されるメソッドの詳細については、次を参照してください [TopicAPIUtilsOOB - Scoped](#)。

3. 通知設定の対象が Hermes Kafka 用かオープンメッセージバス用かがチェックされます。

プロデューサーイベント通知フレームワークの構成の詳細については、次を参照してください
[Producer Event Notification Framework developer guide](#)。

関連情報

[Hermes を使用した送信トラブルチケット通知の生成](#)

[オープン・メッセージ・バスを使用したアウトバウンド・トラブル・チケット通知の生成](#)

トラブルチケット通知の非アクティブ化

トラブルチケット通知の受信を停止するには、インシデントテーブルとケーステーブルに関連するビジネスルールを無効にします。トラブルチケット通知機能を利用したくない場合は、ビジネスルールを無効にすることができます。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > システム定義 > ビジネスルール**.
2. 次のビジネスルールを選択し、[アクティブ] チェックボックスの選択を解除します。
 - トラブルチケットイベントを作成
 - トラブルチケットステータス変更イベント
 - トラブルチケット属性変更イベント
 - ケースのトラブルチケットイベントを作成

Proactive Service Experience Workflows 参照

参照トピックには、Proactive Service Experience Workflowsに関する追加情報が記載されています。

ドメイン分離と Proactive Service Experience Workflows

Proactive Service Experience Workflows ではドメイン分離がサポートされています。を使用すると Proactive Service Experience Workflows、ネットワークが開始したインシデントが発生したときに通常のサービス運用を迅速に復元し、それらのインシデントの影響を受ける顧客を事前に特定して通知できます。ドメイン分離では、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：標準

- ベーシックレベルサポートを含みます。
- ビジネスロジック：サービスプロバイダー (SP) によって顧客ごとにプロセスを作成または変更できます。ユースケースには、単一のインスタンスでの複数のサービスプロバイダー顧客によるアプリケーションの正しい使用が反映されています。
- インスタンスのオーナーは、特定のアプリケーションに期待される通りに、テナントごとに MVP ビジネスロジックとデータパラメーターを設定する必要があります。

サンプルユースケース：管理者は、レコードを他のテナントに対してはクローズしないが、1 つのテナントに対してクローズする場合、コメントを必須にすることができる必要があります。

サポートレベルの詳細については、「[アプリケーションでのドメイン分離のサポート](#)」²」を参照してください。

概要

Proactive Service Experience Workflows (TAW) は、インシデント管理 アプリケーション、およびケースマネジメントや フィールドサービス管理 (FSM).Proactive Service Experience Workflowsつまり、基盤アプリケーションが既にそのサポートを提供しているため、追加のドメイン分離サポートは必要ありません。詳細については、「[Proactive Service Experience Workflows](#)」を参照してください。

関連情報

[サービスプロバイダーのドメイン分離](#) ²