



Washington, D.C Proactive Service Experience Workflows

Zuletzt aktualisiert: 17.12.2025

Automatische Übersetzung

Diese Materialien wurden für Sie mit einer Übersetzungssoftware übersetzt. Es wurden angemessene Anstrengungen unternommen, um Ihnen eine akkurate Übersetzung zu liefern. Jedoch können menschliche Übersetzer nicht durch automatisierte Übersetzungstechnologien ersetzt werden. Die Übersetzungen werden ungeprüft bereitgestellt. Es wird keinerlei Gewährleistung, weder ausdrücklich noch implizit, für die Genauigkeit, Zuverlässigkeit und Richtigkeit von Übersetzungen in andere Sprachen übernommen. Manche Inhalte wurden aufgrund der Beschränkungen der Übersetzungssoftware möglicherweise nicht präzise übersetzt. Die Ausgangssprache dieser Dokumente ist Englisch. Jegliche Diskrepanzen oder Unterschiede, die bei der Übersetzung entstehen, sind nicht verbindlich und haben keine Rechtswirkung für die Einhaltung oder Durchsetzung von Rechten.

Einige Beispiele und Grafiken, die hier dargestellt sind, dienen nur der Veranschaulichung. Eine echte Zuordnung oder Verbindung zu ServiceNow-Produkten oder -Services ist nicht beabsichtigt und sollte nicht abgeleitet werden.

ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc., in den USA und/oder anderen Ländern. Andere Unternehmens- und Produktnamen können Marken der jeweiligen Unternehmen sein, denen sie zugeordnet sind.

Bitte lesen Sie die Nutzungsbedingungen für die ServiceNow-Website unter www.servicenow.com/terms-of-use.html

Firmensitz
2225 Lawson Lane
Santa Clara, CA 95054
USA
(408) 501-8550

Inhaltsverzeichnis

H.....	4
R.....	5
P.....	6
L.....	7
Proactive Service Experience Workflows.....	8
Proactive Service Experience Workflows -Architektur erkunden.....	9
Proactive Service Experience Workflows-Architektur.....	10
CMDB CI-Klassen für Proactive Service Experience Workflows.....	15
Proactive Service Experience Workflows und Incident-Management innerhalb von Service Operations-Arbeitsbereich.....	15
Proactive Service Experience Workflows konfigurieren.....	17
Proactive Service Experience Workflows installieren.....	18
Fügen Sie Benutzer zu Zuweisungsgruppen hinzu.....	19
Arbeiten mit Proactive Service Experience Workflows.....	19
Über das Identifizieren betroffener Accounts mit Proactive Service Experience Workflows in Incident-Management.....	19
Über die Eskalation von Incidents.....	23
Kunden- oder Partner-Accounts werden in überprüft Proactive Service Experience Workflows.....	26
Automatische Erstellung von Fällen und Updates aus Incidents.....	29
Erstellt einen Fall aus einer Change-Anforderung.....	31
Informationen zu Nachrichten, die in Eskalations-Workflows in verwendet werden Proactive Service Experience Workflows.....	32
Umgang mit Problemticketbenachrichtigungen.....	33
Proactive Service Experience Workflows-Referenz.....	40
Domänentrennung und Proactive Service Experience Workflows.....	40

R

Automatische Übersetzung

L

Automatische Übersetzung

Proactive Service Experience Workflows

Bieten Sie End-to-End-Support, verstehen Sie die Auswirkungen auf die Kunden und bieten Sie allen am Supportprozess beteiligten Parteien eine transparente Kommunikation.

Die folgende Abbildung zeigt die wichtigsten Funktionen von Proactive Service Experience Workflows.

Proactive Service Experience Workflows

As a Telecommunications, Media, and Technology service provider deliver purpose built technical support workflows to external customers.

Core Capabilities

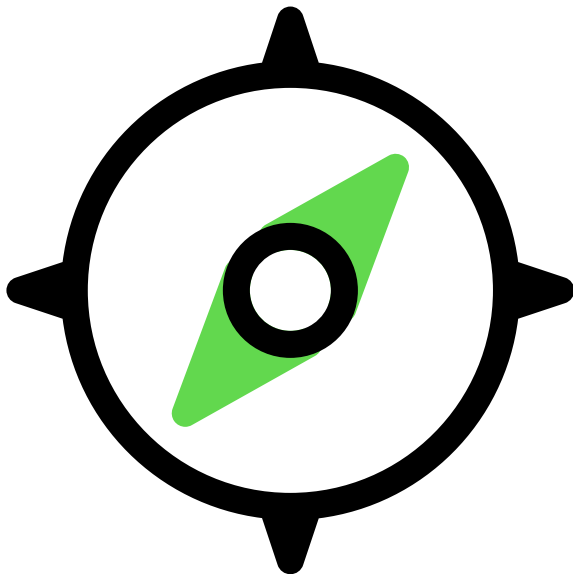
- Enhanced IT Service Management forms inside of Service Operations Workspace
- Operations Account 360
- Decision driven incident escalation workflows
- TMF 621 API Open Incident Support

Dependencies

- Customer Service Management
- IT Service Management
- Service Operations Workspace plugin
- Proactive Service Experiences Workflow plugin

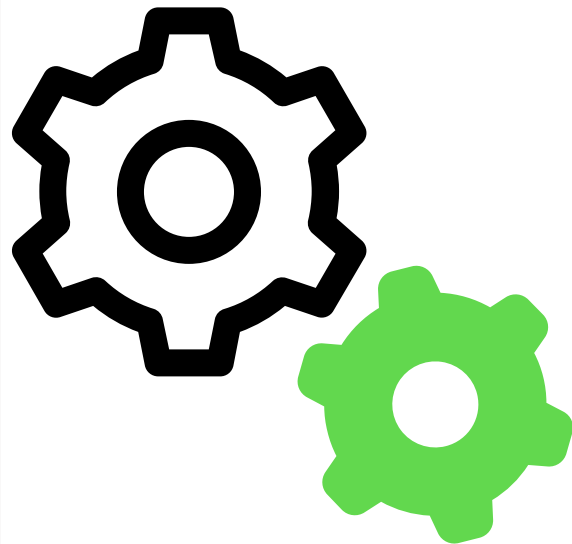
Automatische Übersetzung

Erkunden



Erfahren Sie, wie Service Provider und Kunden Proactive Service Experience Workflows verwenden.

Konfigurieren



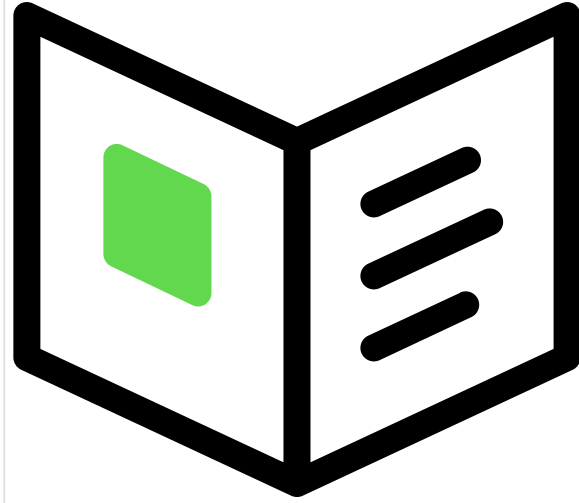
Planen und konfigurieren Sie Ihre Implementierung.

Verwenden



Informieren Sie sich über den Einsatz von Proactive Service Experience Workflows.

Referenz



Ruft Details zur Domänentrennung für Proactive Service Experience Workflows ab .

Proactive Service Experience Workflows -Architektur erkunden

Erfahren Sie, wie Sie die Anwendung Proactive Service Experience Workflows verwenden können, um automatisch Workflows zu initiieren, die vom Netzwerk initiierte Incidents zu lösen und betroffene Kunden proaktiv zu benachrichtigen.

Apps im Store anfordern

Besuchen Sie die [ServiceNow Store](#) -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum [ServiceNow Store-Versionsverlauf](#) .

Proactive Service Experience Workflows capabilities

Proactive Service Experience Workflows bieten End-to-End-Support, verstehen die Auswirkungen auf Kunden und bieten transparente Kommunikation für alle am Supportprozess beteiligten Parteien. Telekommunikations-, Medien- oder Technologiedienstleister können:

- Identifizieren Sie betroffene Kunden-Accounts basierend auf einem oder mehreren Konfigurationselementen, die mit vorgelagerten Services verknüpft sind, die an eine Installationsbasis gebunden sind.
- Verwenden Sie mit Account 360 für Vorgänge Daten aus ITSM und CSM, um Detailinformationen zu Kunden-Accounts anzuzeigen und wichtige Informationen zum Account zu visualisieren.

- Generieren Sie proaktive Fälle, die die Synchronisierung bestimmter Felder beim Einfügen von Fällen, bei der Lösung von Incidents oder beim Schließen einer Change-Anforderung umfassen.
- Reduzieren Sie die administrative Einrichtung und den Overhead mit erweiterten Incident- und Change-Anforderungsformularen in Service Operations-Arbeitsbereich.
- Lösen Sie geringfügige Fälle ohne Eingreifen von Kundensupport-Mitarbeitern.
- Stellen Sie Mitarbeitern des technischen Supports Funktionen für die Kommunikation mit externen Kunden bereit, ohne zwischen Incident- oder Change-Anforderungen und zugehörigen Falldatensätzen navigieren zu müssen.
- Verwenden Sie fünf eindeutige Flow Designer -Flows, die an Ihre Geschäftsanforderungen angepasst werden können.
- Eskalieren Sie Incidents für schnellere Aktionen basierend auf einer vorkonfigurierten Entscheidungstabelle.
- Verwenden Sie erweiterte CMDB CI-Klassen, die in der SD-Wan-Edge-Infrastruktur üblich sind
- Erstellen Sie Incident-Datensätze von bestimmten API-Clients basierend auf den REST-API-Standards TMF621 des TM Forums.
- Verwenden Sie dedizierte Rollen, mit denen Mitarbeiter des technischen Supports die Anwendungen ITSM und CSM und anzeigen können.

Weitere Informationen zu den Architekturkomponenten der Anwendung Proactive Service Experience Workflows finden Sie unter [Proactive Service Experience Workflows-Architektur](#).

Sie können den CMDB CI-Klassen auch Klassen hinzufügen, die auf die SD-WAN-Edge-Infrastruktur als Teil der Anwendung CMDB CI Class Models abzielen. Unter [CMDB CI-Klassen für Proactive Service Experience Workflows](#) finden Sie weitere Details.

Proactive Service Experience Workflows-Architektur

Es gibt mehrere Komponenten, aus denen die Architektur der Anwendung Proactive Service Experience Workflows besteht.

Die Hauptkomponenten sind:

- Flows und Subflows
- Eskalationsstufen
- Entscheidungstabellen
- Nachrichten
- Business Rule
- Clientskripts
- Systemeigenschaften
- Rollen
- Zuweisungsgruppen
- Service Operations-Arbeitsbereich

Flows und Subflows

Ein Workflow wird ausgelöst, wenn ein Incident mit der SD-WAN-Kategorie und einer der folgenden fünf Unterkategorien erstellt wird:

- Verknüpfungsfehler
- Gerätefehler
- Protokollfehler
- Soft-WAN-Linkfehler
- Softwarefehler

Jede Kategorie hat Subflows für jede Zuweisungsgruppe und eine Eskalationsebene für insgesamt 27 Subflows. Diese Subflows sind ein Ausgangspunkt, der hauptsächlich für Ausfälle von Netzwerkvorgängen erstellt wurde, können jedoch für andere Anwendungsfälle wiederverwendet und erweitert werden.

Eskalationsstufen

Die fünf Stufen der Eskalation sind:

- Selektierung
- L1-Ermittlung
- L2-Ermittlung
- L3-Ermittlung
- Lösung

Proactive Service Experience Workflows verwendet diese Stufenwerte, um die entsprechende Entscheidung in der Entscheidungstabelle „Richtlinie für Incident-Eskalation“ [sys_hub_flow] auszulösen. Diese Tabelle löst während der Incident-Eskalation den richtigen Subflow aus. Während jeder Eskalationsstufe wird eine Incident-Aufgabe erstellt und für diese Zuweisungsgruppe verwaltet. Die Incident-Informationen werden aus einer Geschäftsregel mit der Incident-Aufgabe synchronisiert und umfassen Folgendes:

- Kurzbeschreibung
- Priorität
- Status
- Arbeitsnotizen, die die zugewiesene Person in der Zuweisungsgruppe dem Incident hinzufügt
- Nachrichteninhalte, der durch den Workflow in den Incident eingebettet wird

Entscheidungstabellen

Basierend auf der definierten Bedingung arbeitet Flow Designer mit der Entscheidungstabelle „Richtlinie für Incident-Eskalation“ [sys_hub_flow] zusammen, um zu bestimmen, welcher Subflow an bestimmten Eskalationspunkten generiert werden soll.

Nachrichten

Jeder Subflow in Proactive Service Experience Workflows ist einer Nachrichtendatei zugeordnet, die Anweisungen für Service Desk-Mitarbeiter zur Problembehandlung, Eskalation und Lösung von netzwerkinitiierten Incidents enthält. Weitere Informationen zum Anpassen

der Standardanweisungen für Ihre internen Problembehandlungsprozesse finden Sie unter [Passen Sie Nachrichtendateien an](#).

Business-Regeln

Die Geschäftsregel Mit TSM-Incident-Aufgabe synchronisieren bestimmt die Informationen, die vom Incident mit der Incident-Aufgabe synchronisiert werden, einschließlich:

- Kurzbeschreibung
- Priorität
- Status
- Zuweisungsgruppe
- Beauftragter
- Arbeitsnotizen, die die zugewiesene Person in der Zuweisungsgruppe dem Incident hinzufügt

Rollen

Die Rolle „sn_ind_tsm_core.noc_agent“ ist mit der Anwendung Proactive Service Experience Workflows verfügbar. Wenn diese Rolle hinzugefügt wird, stellt sie sicher, dass der Mitarbeiter des technischen Supports die relevanten Informationen zwischen den Anwendungen ITSM und CSM anzeigen kann. Diese Rolle umfasst Folgendes:

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

Mehrere Zuweisungsgruppen sind in dieser Rolle enthalten, und andere Gruppen können auch die Administratorrolle haben. Die Rolle sn_ind_tsm_sdwan.ticket_integrator kann für Problemtickets verwendet werden, die aus den TMF 621 Open API-Anwendungsfällen erstellt wurden.

Zuweisungsgruppen

An Workflows sind netzwerkbezogene Mitarbeiter beteiligt, einschließlich Netzwerkkoordinatoren und Techniker. Alle Zuweisungsgruppen haben die Basis-Systemrolle sn_ind_tsm_sdwan.PSEW_USER.

i Hinweis:

Diese Zuweisungsgruppen sind ein Ausgangspunkt, der hauptsächlich für die Unterstützung des Netzwerkbetriebs erstellt wurde.

Netzwerkkoordinator

Die Aufgaben und Zuständigkeiten des Netzwerkkoordinators lauten wie folgt:

- Verwalten und selektieren Sie Incidents aus den Netzwerkverwaltungssystemen
- Bewerten Sie die Auswirkungen, und definieren Sie die Incident-Priorität

- Aktualisieren Sie die betroffenen Services, und erstellen Sie Fälle für die betroffenen Kunden
- Korrelieren Sie mithilfe von Incidents mit offenen Incidents oder Change-Anforderungen Agent Assist
- Weisen Sie Incidents zu und stimmen Sie sich mit der Netzwerktechnik ab

L1: Netzwerktechniker

Die Aufgaben und Zuständigkeiten des L1-Netzwerktechnikers sind:

- Beheben Sie Probleme mit Netzwerk-Incidents
- Wenden Sie sich an Außendienst Service Desk-Mitarbeiter, Drittanbieter und OEMs, um den normalen Servicebetrieb wieder aufzunehmen
- Lösen Sie die Prozesse Change-Management und Problem-Management aus

L2: Netzwerktechniker

Die Aufgaben und Zuständigkeiten des L2-Netzwerktechnikers sind:

- Beheben Sie Probleme mit Netzwerk-Incidents
- Wenden Sie sich an Außendienst Service Desk-Mitarbeiter, Drittanbieter und OEMs, um den normalen Servicebetrieb wiederherzustellen
- Lösen Sie die Prozesse Change-Management und Problem-Management aus, um vorteilhafte Änderungen einzuführen oder Ursachenanalysen durchzuführen

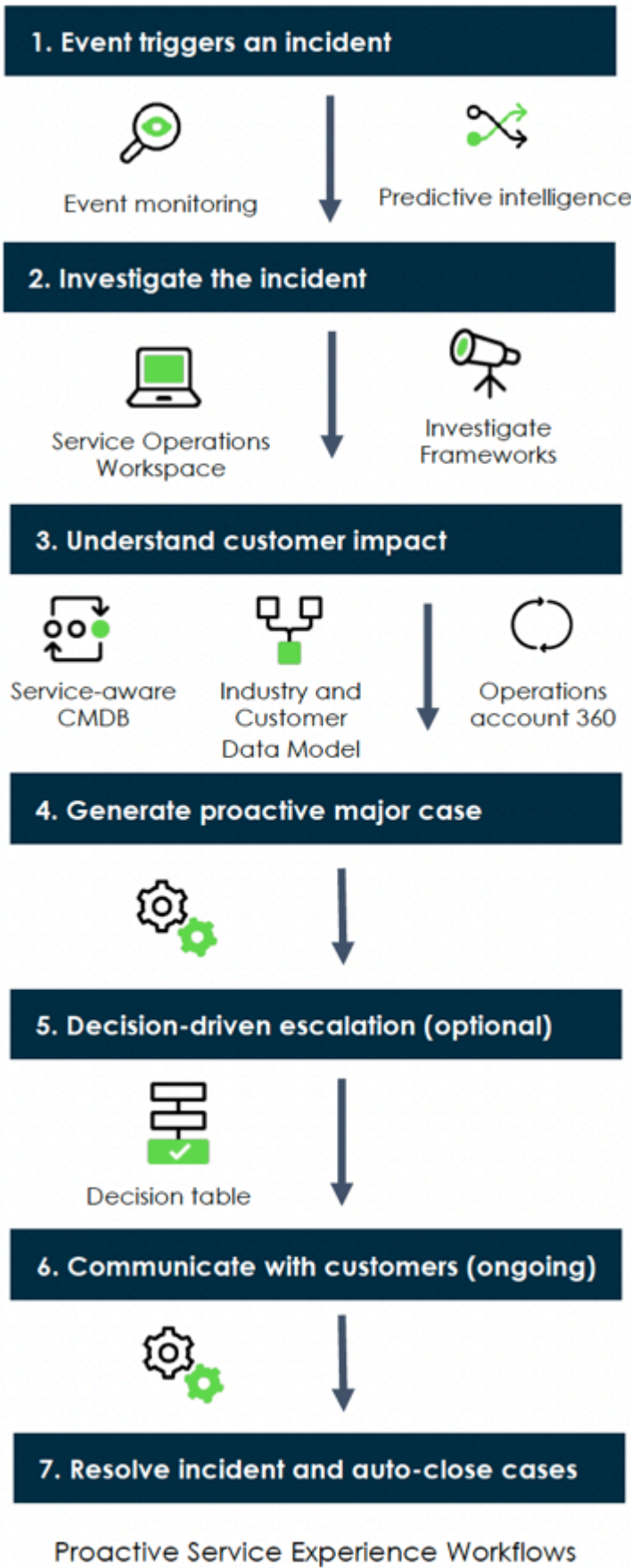
L3: Netzwerktechniker

Die Aufgaben und Zuständigkeiten des L3-Ingenieurs lauten wie folgt:

- Beheben Sie Probleme mit Netzwerk-Incidents
- Wenden Sie sich an Außendienst Service Desk-Mitarbeiter, Drittanbieter und OEMs, um den normalen Servicebetrieb wiederherzustellen
- Lösen Sie die Prozesse Change-Management und Problem-Management aus, um vorteilhafte Änderungen einzuführen oder Ursachenanalysen durchzuführen

Proactive Service Experience Workflows Prozess

Das folgende Diagramm zeigt die Schritte des Prozesses Proactive Service Experience Workflows.



Automatische Übersetzung

CMDB CI-Klassen für Proactive Service Experience Workflows

Proactive Service Experience Workflows fügt fünf Configuration Management Database (CMDB) Configuration Item (CI)-Klassen hinzu, die als Teil der CMDB CI Class Models-Anwendung auf die SD-WAN-Edge-Infrastruktur abzielen.

i Hinweis:

Weitere Informationen zu dieser Anwendung finden Sie unter [CMDB CI Class Models](#).

CMDB-CI-Klassen für Telekommunikations-Assurance-Workflows

Klasse	Beschreibung	CI-Klasse erweitert
SD-WAN-Controller	Gerät, das die Verwaltung physischer oder virtueller Geräte für alle SD-WAN-Edges bereitstellt	cmdb_ci_Server_Hardware
SD-WAN-Edge	Netzwerkfunktionen (physisch oder virtuell), die sich zwischen dem Underlay Connectivity-Service und dem SD-WAN-Service befinden	cmdb_ci_netgear
SD-WAN-Edge-Port	Socket auf einem Netzwerkgerät, das eine Verbindung zu einem externen Netzwerk herstellt	cmdb_ci_netgear
Netzwerkleitung	Diskreter Pfad zwischen zwei oder mehr Punkten, die Telekommunikationskonnektivitätsservices ermöglichen	cmdb_ci
Provider-Edge	Verbindungspunkt zwischen dem SD-WAN-Edge-Port und dem Kernnetzwerk des Service Providers	cmdb_ci_netgear

Automatische Übersetzung

Proactive Service Experience Workflows und Incident-Management innerhalb von Service Operations-Arbeitsbereich

Sie können die Anwendung Service Operations-Arbeitsbereich verwenden, um sich einen Überblick darüber zu verschaffen, wie ein Netzwerkmitarbeiter Aufgaben priorisieren und Incidents lösen kann.

Anzeigen von Service Operations-Arbeitsbereich

Wählen Sie im Menü „Arbeitsbereiche“ die Option **Service Operations Workspace** aus, und klicken Sie auf das **Startseitensymbol**. Über die Zielseite kann ein Netzwerkmitarbeiter Incidents analysieren und Fälle und bevorstehende Aufgaben anzeigen. Zum Anzeigen:

- **Listen:** Wählen Sie die Registerkarte **Listen** in Service Operations-Arbeitsbereich aus. Auf der Registerkarte Listen kann ein Netzwerkmitarbeiter die einzelnen Listen von Incidents und Aufgaben analysieren und dann die entsprechende Aktion ausführen.

Das folgende Beispiel zeigt die Registerkarte Liste.

Registerkarte „Liste“

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

- Datensätze: Öffnen Sie einen beliebigen Aufgabendatensatz, um zu seiner Datensatzansicht zu navigieren, wie im folgenden Beispiel gezeigt.

Datensatzansicht

Beispiel

Die Anwendung Proactive Service Experience Workflows wird automatisch ausgelöst, wenn im System ein Incident durch einen Warnungs-Flow erstellt wird. Ein technischer Support kann diese Warnung manuell in Service Operations-Arbeitsbereiche stellen. Sie kann auch aus einem externen Fehlermanagementsystem mithilfe der TMF 621-Integration generiert werden.

Das folgende Beispiel zeigt, wie Proactive Service Experience Workflows zur Lösung eines vom externen Netzwerk initiierten Incident verwendet wird. In diesem Beispiel

1. Ein externes Fehlermanagementsystem mit TMF 621-Integration sendet eine Warnung, die die Erstellung eines Incident-Datensatzes mit den folgenden Werten auslöst:
 - Kurzbeschreibung und Beschreibung: Vmanage_10001 konnte nicht neu gestartet werden, nachdem ein Change implementiert wurde.
 - Konfigurationselement: Vmanage_10001 (SD-WAN CI-Klasse)
 - Kategorie: SD-WAN

Automatische Übersetzung

- Unterkategorie: Protokollfehler
 - Betroffene Kunden: 5
2. Ein Techniker des technischen Supports öffnet den Incident-Datensatz in Service Operations-Arbeitsbereich und zeigt die Liste der betroffenen Services und Konten im Abschnitt „**Übersicht**“ an.
 3. Der Techniker des technischen Supports selektiert die Probleme, indem er die letzten Änderungen in Agent Assist überprüft, die den Ausfall ausgelöst haben.
 4. Der Techniker des technischen Supports startet dann den SD-WAN-Controller neu und wählt im Abschnitt „Fälle“ die **Option Proaktive Fälle generieren** aus. Ein schwerwiegender Fall und fünf untergeordnete Fälle werden generiert, und Benachrichtigungen werden an die primären Kontakte für die betroffenen Accounts gesendet.
 5. Wenn ein schwerwiegender Fall erstellt wurde, benachrichtigt der Techniker des technischen Supports den Manager für schwerwiegende Probleme über einen potenziell schwerwiegenden Ausfall. Der Manager für schwerwiegende Probleme verwaltet den Datensatz für schwerwiegende Fälle und die Kommunikation mit technischen Teams und betroffenen Kunden.
 6. Der Techniker des technischen Supports (TSE) erkennt, dass das Gerät nicht neu gestartet werden kann und möglicherweise vollständig ausgefallen ist. Die TSE ändert das Feld Unterkategorie in Gerätefehler, wählt die **UI** -Aktion Eskalieren aus und gibt eine Arbeitsnotiz ein
 7. Das nächste L2-Supportteam erhält den Incident und aktualisiert den Datensatzstatus.
 8. Der Techniker des technischen Supports von L2 versucht, die Probleme auf dem SD-WAN-Controller zu beheben, und startet das Konfigurationselement erfolgreich neu. Vier von fünf betroffenen Accounts melden, dass das Problem gelöst wurde, aber beim fünften Account sind immer noch Probleme aufgetreten.
 9. Um weitere Probleme mit dem fünften Konto zu diagnostizieren, führt der Techniker des technischen Supports von L2 die folgenden Schritte aus:
 - Aktiviert das Kontrollkästchen neben dem Falldatensatz auf der Seite „Übersicht“.
 - Wählt die **Notify-UI** -Aktion aus, um eine Nachricht mit zusätzlichen Kommentaren an die Kontaktperson im Falldatensatz zu senden.
 10. Die Kontaktperson erhält den zusätzlichen Kommentar und führt einige zusätzliche Schritte aus. Wenn der Service wiederhergestellt wird, aktualisiert der Kontakt den Status im CSM -Portal.
 11. Angesichts der zusätzlichen Anmerkungen im Incident-Datensatz ändert der Techniker des technischen Supports für L2 das Feld Status in **Gelöst**.

Die Lösungsinformationen werden in jeden Falldatensatz kopiert, während der Major Issue Manager den Datensatz des schwerwiegenden Falls und alle zugehörigen Fälle löst.

Proactive Service Experience Workflows konfigurieren

Sie können Proactive Service Experience Workflows so konfigurieren, dass Sie Benutzer zu Zuweisungsgruppen hinzufügen können. Sie können auch benutzerdefinierte Anweisungen für Techniker erstellen, um sie bei der Lösung von Netzwerk-initiierten Problemen durch automatisch bereitgestellte Workflows zu unterstützen.

Proactive Service Experience Workflows installieren

Wenn Sie ein Benutzer mit der Rolle „Systemadministrator“ sind, können Sie die Anwendung Proactive Service Experience Workflows installieren.

Vorbereitungen

Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter [Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung](#) .

- Erforderliche Rolle: admin
- Erforderliche Plugins: Die folgenden Plugins müssen installiert sein:
 - Kundenservice-Management
 - Kundenservice mit Servicemanagement
 - Service Operations-Arbeitsbereich

Warum und wann dieser Vorgang ausgeführt wird

Die Telecom-Core-Anwendung wird mit Proactive Service Experience Workflows installiert:

Prozedur

1. Navigieren zu **Alle > Systemanwendungen > Alle verfügbaren Anwendungen > Alle**.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Proactive Service Experience Workflows (sn_ind_tsm_sdwan).

Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über ServiceNow Storeanfordern.

Besuchen Sie die [ServiceNow Store](#) -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum [ServiceNow Store-Versionsverlauf](#) .

3. Überprüfen Sie im Dialogfeld „Anwendungsinstallation“ die Anwendungsabhängigkeiten.

Alle abhängigen Plugins und Anwendungen, die enthalten sind oder installiert werden müssen, werden im Dialogfeld aufgelistet.

4. **Wahlweise:** Wenn Demodaten verfügbar sind und Sie sie installieren möchten, wählen Sie **Demodaten laden** aus.

(Optional) Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für häufige Anwendungsfälle veranschaulichen. Das Laden von Demodaten wird empfohlen, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

Wichtig:

Wenn Sie die Demodaten nicht während der Installation laden, stehen sie nicht zum späteren Laden zur Verfügung.

5. Wählen Sie **Installieren** aus.

Fügen Sie Benutzer zu Zuweisungsgruppen Proactive Service Experience Workflows hinzu

Fügen Sie Benutzer zu Zuweisungsgruppen Proactive Service Experience Workflows hinzu, damit sie über die erforderliche Rolle verfügen und zur Lösung von Netzwerk-initiierten Problemen auf der entsprechenden Eskalationsebene zugewiesen werden können.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle > Benutzeradministration > Gruppen**.
2. Wählen Sie den Gruppennamen aus.
Die vier Zuweisungsgruppen lauten wie folgt:
 - Netzwerkkoordinatoren
 - L1 Netzwerktechnik
 - L2 Netzwerk-Engineering
 - L3 Netzwerk-Engineering
3. Wählen Sie **Bearbeiten** in der zugehörigen Liste „Gruppenmitglieder“.
4. Wählen Sie einen oder mehrere Namen in der Liste Sammlung aus.
5. Wählen Sie **Hinzufügen**.
6. Wählen Sie **Speichern**.

Arbeiten mit Proactive Service Experience Workflows

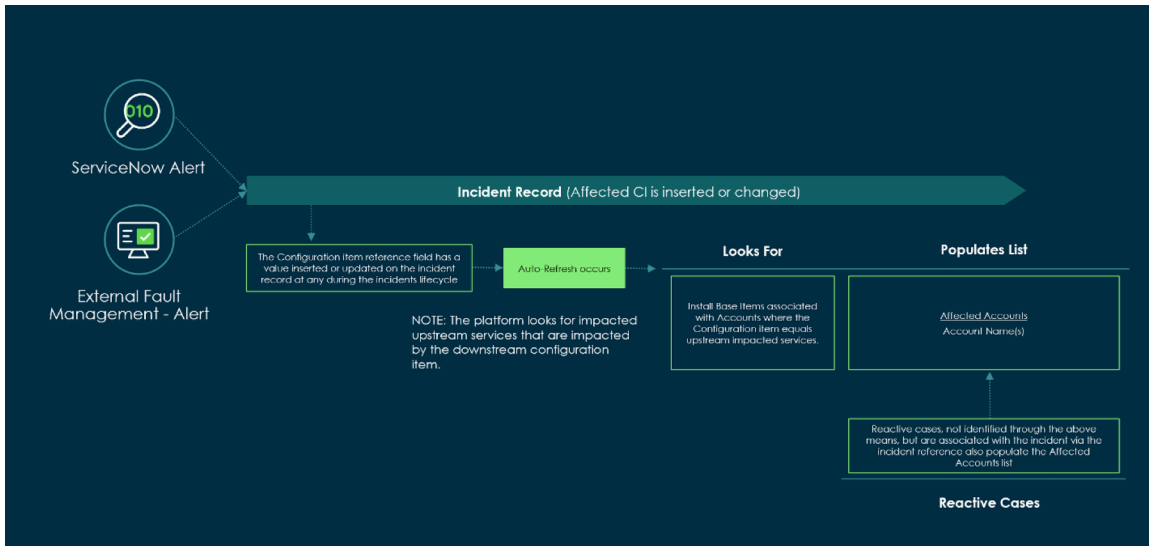
Durch die Verwendung von Proactive Service Experience Workflows können Sie helfen, vom Netzwerk initiierte Incidents zu beheben und betroffene Kunden proaktiv zu benachrichtigen. Diese Anwendung erweitert die Anwendung Incident-Management in Bezug auf häufige SD-WAN-Serviceprobleme, die von Netzwerkverwaltungssystemen erkannt werden.

Über das Identifizieren betroffener Accounts mit Proactive Service Experience Workflows in Incident-Management

Ein Incident-Datensatz wird erstellt, wenn ein Event-Management-System eine Warnung generiert und die betroffenen Accounts in Service Operations-Arbeitsbereich angezeigt werden können.

Wenn sich der Techniker des technischen Supports bei Service Operations-Arbeitsbereich anmeldet, werden das betroffene Konfigurationselement, die Services und die Kunden im Abschnitt „Übersicht“ aufgelistet. Diese Details werden automatisch aktualisiert, wenn das Konfigurationselement im Incident-Datensatz aktualisiert wird. Wenn das Konfigurationselement aktualisiert wird, wird das Skript „**Betroffene Services** aktualisieren“ automatisch ausgelöst und ruft Services ab, bei denen ein Ausfall oder eine Verschlechterung auftritt. Die betroffenen Services, die den Accounts zugeordnet sind, werden identifiziert und aktualisiert. Wenn ein CSM -Mitarbeiter einen Fall mit dem Incident-Datensatz verknüpft, wird außerdem die Liste Betroffener Account aktualisiert. Wenn die Liste „Betroffener Account“ aktualisiert wird, ist die Auswirkung auf den Kunden für die Supportteams sichtbar, die an dem Incident-Datensatz arbeiten.

Das folgende Diagramm zeigt die Schritte zum Erstellen eines Incident-Datensatzes.



i Hinweis:

Der Change Management-Workflow folgt demselben Prozess. Wenn ein Konfigurationselement in einem Change-Anforderungsdatensatz aktualisiert wird, wird das Skript „Betroffene **Services** aktualisieren“ ausgelöst, und die betroffenen Accounts werden abgerufen. Da das Konfigurationselementfeld schreibgeschützt ist, müssen Sie sicherstellen, dass dieses Feld ausgefüllt wird, bevor das Skript ausgelöst wird. Unter [Erstellt einen Fall aus einer Change-Anforderung](#) finden Sie weitere Details.

Incident in Proactive Service Experience Workflows erstellen

Erstellen Sie einen Incident-Datensatz in Proactive Service Experience Workflows, um ein Problem Ihres Kunden zu dokumentieren.

Vorbereitungen

Erforderliche Rolle: sn_ind_tsm_sdwan.PSEW_USER, admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich* > **Incidents** > **Alle**.
2. Wählen Sie in der Incident-Listenansicht **Neu** aus.
3. Füllen Sie die Felder des Formulars aus.

Incident-Formular

Feld	Beschreibung
Kurzbeschreibung	Eine kurze Beschreibung des incident.
Beschreibung	Detaillierte Erklärung zu dem Incident.
Nummer	Eindeutige vom System generierte Incident-Nummer.
Unternehmen	Kunden-Account, bei dem ein Netzwerkproblem aufgetreten ist.
Anrufer	Benutzer, der Sie bezüglich eines Problems kontaktiert hat.
Standort	Standort des Anrufers.
Kanal	Kommunikationsmethode, die zum Erstellen des Incident verwendet wird. Verfügbare Optionen:

Automatische Übersetzung

Feld	Beschreibung
	<ul style="list-style-type: none"> ○ Chat ○ E-Mail ○ Telefon ○ Überwachung ○ Self-Service ○ Virtual Agent ○ Walk-in
Status	Status des Incident durch mehrere Lösungsphasen.
Auswirkung	Maß für die Auswirkung eines Incident oder Problems.
Dringlichkeit	Maß dafür, wie lange die Lösung hinausgeschoben werden kann, bis ein Incident oder Problem erhebliche geschäftliche Auswirkungen hat.
Priorität	Basierend auf Auswirkung, Dringlichkeit und wie schnell die Lösung abgeschlossen werden kann.
Service	Betroffener Business-Service.
Serviceangebot	Serviceangebot, das aus einer oder mehreren Servicezusagen besteht, die das Serviceniveau für die Optionen für Verfügbarkeit, Umfang, Preisgestaltung und Paketierung eindeutig definieren.
Konfigurationselement	Betroffenes Konfigurationselement.
Zuweisungsgruppe	Gruppe, die an dem Incident arbeitet.
Zugewiesen an	Benutzer, der an diesem Incident arbeitet. Wenn sich die Zuweisungsgruppe ändert, wird das Feld Zugewiesen an gelöscht.
Zusätzliche Kommentare	Weitere Informationen zum Problem nach Bedarf. Alle Benutzer, die die Incidents anzeigen können, können die zusätzlichen Anmerkungen sehen.
Arbeitsnotizen	Informationen darüber, wie der Incident gelöst werden kann, oder die Schritte, die unternommen wurden, um ihn zu beheben, falls zutreffend.
Kategorie und Unterkategorie	Die Art des Problems. Nachdem Sie die Kategorie ausgewählt haben, wählen Sie gegebenenfalls die Unterkategorie aus.

4. Wählen Sie **Speichern**.

Ergebnisse

Der Incident wird erstellt.

Erstellen Sie Fälle aus einem Incident-Datensatz in Proactive Service Experience Workflows

Erstellen Sie Fälle aus Datensätzen, damit Sie Netzwerkprobleme für Ihre Unternehmenskunden identifizieren und lösen können.

Vorbereitungen

Diese Aufgabe setzt voraus, dass bereits ein Workflow ausgelöst und eine Zuweisungsgruppe zugewiesen wurde.

Erforderliche Rolle: sn_ind_tsm_sdwan.PSEW_USER

Warum und wann dieser Vorgang ausgeführt wird

Nachdem ein Workflow in Proactive Service Experience Workflows ausgelöst wurde, können Sie die Kunden und Systeme identifizieren, die vom Netzwerkproblem betroffen sind. Sie können dann entweder automatisch die einzelnen Fälle für die betroffenen Kunden erstellen oder einen schwerwiegenden Fall und untergeordnete Fälle für eine größere Anzahl von betroffenen Kunden erstellen.

Prozedur

1. Navigieren Sie zu *Service Operations-Arbeitsbereich* und wählen Sie **Liste > Incidents > Offen**.
2. Wählen Sie einen Incident aus der Liste aus.
3. **Wahlweise:** Weisen Sie einen vorhandenen Incident zu.
4. Zeigen Sie die betroffenen Konfigurationselemente (CIs) an, indem Sie die Karte **Betroffene CIs** auswählen.
5. Zeigen Sie die betroffenen Services an, indem Sie die Karte **Betroffene Services/CIs** auswählen und Betroffene **Services** aktualisieren auswählen.
6. Zeigen Sie die betroffenen Accounts an, indem Sie die Karte **Betroffene Accounts** auswählen und **Betroffene Accounts identifizieren** auswählen.

Die Instanz ServiceNow® initiiert eine Aktion, um die betroffenen Services zu aktualisieren und die betroffenen Konten zu finden.

7. Suchen Sie nach den Namen der betroffenen Kunden, indem Sie die Karte **Betroffene Accounts** auswählen und die Spalte Name überprüfen.
Normalerweise erstellt der Netzwerkkoordinator Fälle, damit die betroffenen Kunden proaktiv über die vom Netzwerk initiierten Probleme informiert werden.
8. Generieren Sie proaktive Fälle für die betroffenen Kunden, indem Sie die Karte „Fälle“ auswählen und **Proaktive Fälle generieren** auswählen.
 - Wenn die Anzahl der betroffenen Accounts unter dem Schwellenwert liegt, erstellt diese Aktion einen Fall für jeden betroffenen Account. Andernfalls erstellt diese Aktion zuerst einen schwerwiegenden Fall und dann untergeordnete Fälle (einen Fall für jeden betroffenen Account).
 - Wenn Sie den Schwellenwert ändern möchten, wenden Sie sich an Ihren Administrator, um den Wert der Systemeigenschaft `sn_ind_tsm_core.major_case-affected_account_threshold` zu ändern.
 - Auf der Registerkarte **Fälle** wird der schwerwiegende Fall in den Spalten Account und Kontakt durch **[leer]** gekennzeichnet. Fälle, in denen diese Informationen ausgefüllt werden, sind untergeordnete Fälle dieses schwerwiegenden Falls.
9. Erstellen Sie einen Ad-hoc-Fall, indem Sie einen Fall aus der Liste auswählen und **Neu** wählen.
10. Benachrichtigen Sie einen Kunden, indem Sie einen Fall auswählen und **Kunden benachrichtigen** auswählen.
11. Geben Sie im Pop-up-Fenster „Kunden benachrichtigen“ eine beschreibende Notiz ein, und wählen Sie **Notify** aus.

Eine Notiz wird automatisch in das Feld **Aktivität** des Incident-Datensatzes und auch in den ausgewählten Falldatensatz eingefügt. Wenn Ihr Kunde den Fall mit einer Nachricht aktualisiert, wird er automatisch auch mit dem Incident-Datensatz synchronisiert.

i Hinweis:

Standardmäßig ist die Funktion „Kunden benachrichtigen“ nicht aktiv. Als Administrator müssen Sie den Eigenschaftswert `proactive_workflows_for_providers.additional_comments_sync` auf WAHR festlegen. Deaktivieren Sie BR (Geschäftsregel) `Update case worknote for comments change`, um diese Funktionalität zu aktivieren.

12. Wenn Sie die wahrscheinliche Ursache des Incident aktualisieren möchten, wählen Sie die Registerkarte **Ursache** aus, und speichern Sie Ihre Nachricht.

13. Lösen Sie einen Incident, indem Sie im Incident-Datensatz auf Lösen **klicken**.

Geben Sie im Popup-Fenster „Lösen“ den **Lösungscode** und die Lösungsnotizen ein, und wählen Sie Lösen aus.

i Hinweis:

Nur geringfügige Fälle werden automatisch geschlossen. Bei schwerwiegenden Fällen müssen Sie alle zugehörigen Fälle manuell schließen.

Ergebnisse

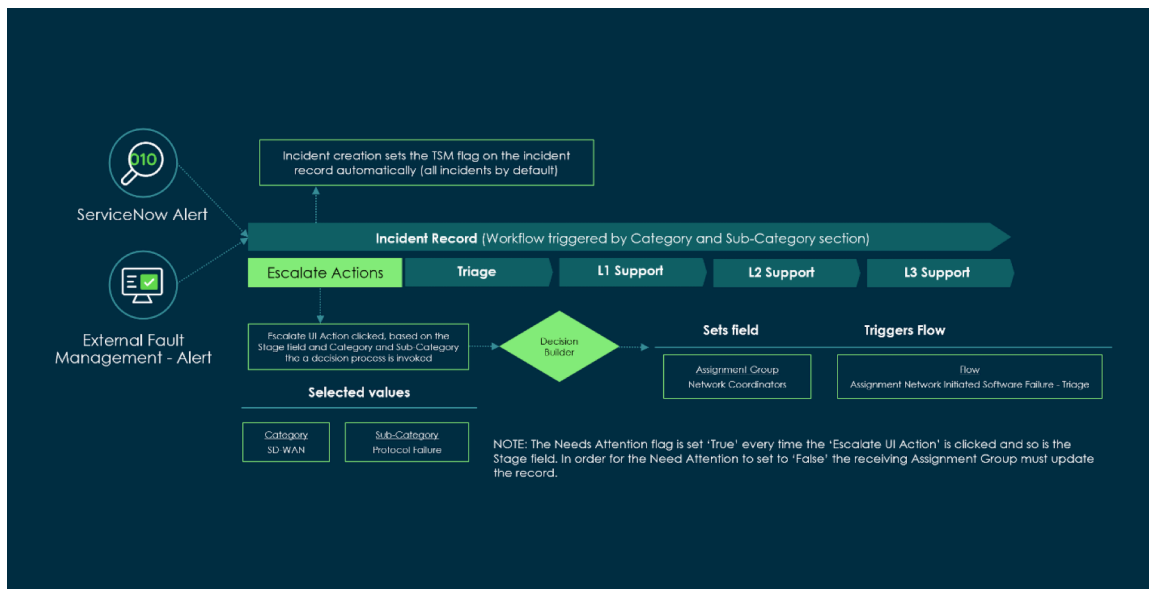
Wenn der Incident gelöst ist, wird der automatische Abschluss zugehöriger Fälle ausgelöst.

- Wenn es keinen schwerwiegenden Fall gibt, werden alle zugehörigen Einzelfälle gelöst und mit den Arbeitsnotizen aktualisiert. Die folgenden Feldwerte aus dem übergeordneten Incident-Datensatz werden auch in den zugehörigen Fällen ausgefüllt:
 - Details
 - Lösungscode
 - Wahrscheinliche Ursache
- Wenn ein schwerwiegender Fall vorliegt, werden die zugehörigen Fälle nicht automatisch gelöst, und den Arbeitsnotizen des Incident-Datensatzes wird die folgende Meldung hinzugefügt: „Mit diesem Incident ist ein schwerwiegender Fall verknüpft“.Die folgenden Feldwerte aus dem übergeordneten Incident Datensatz werden in allen zugehörigen schwerwiegenden und untergeordneten Fällen ausgefüllt:
 - Details
 - Lösungscode
 - Wahrscheinliche Ursache

Über die Eskalation von Incidents

Eine Eskalation kann ausgelöst werden, wenn ein Incident mit der entsprechenden Kategorie und Unterkategorie erstellt wird und die **UI**- Option Eskalieren in Service Operations-Arbeitsbereich ausgelöst wird.

Das folgende Diagramm bietet eine visuelle Darstellung des Eskalations-Flows.



Die folgenden Kategorie- und Unterkategoriewerte sind mit dem Basissystem verfügbar:

- Kategorie: SD-WAN
- Unterkategorie:
 - Linkfehler
 - Gerätefehler
 - Protokollfehler
 - Soft-WAN-Linkfehler
 - Softwarefehler

Die folgenden Werte sind für das Feld Stufe in der Incident-Tabelle verfügbar:

- Selektierung
- L1-Ermittlung
- L2-Ermittlung
- L3-Ermittlung

Basierend auf den definierten Bedingungen, z. B. aktuelle Stufe, Kategorie und Unterkategorie, bestimmt die Entscheidungstabelle „Incident-Eskalationsrichtlinie“ die Ergebnisse und gegebenenfalls die nächste Eskalationsstufe.

Incident Escalation Policy

Created: 2020-09-25 12:43:53 | Application: Telecom Core | Properties | Close

Inputs [Add](#)

Label	Type	Reference	Mandatory
Incident	Reference	Incident [incident]	<input type="checkbox"/>

[Add an input](#)

Decision table

Conditions		Results			
	Category <small>incident (incident * category)</small>	Subcategory <small>incident (incident * subcategory)</small>	Stage <small>incident (incident * sn_ind_tsm_core_stage)</small>	Assignment Group <small>Group (sys_user_group)</small>	Flow <small>Flow (sys_hub_flow)</small>
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

Die Entscheidungstabelle wird mit der Anwendung Proactive Service Experience Workflows bereitgestellt. Sie können die definierten Bedingungen und die Ergebnisse an Ihre Anforderungen anpassen. Weitere Informationen zum Aktualisieren von Entscheidungstabellen finden Sie unter [Decision Tables](#) .

Wenn ein Incident eskaliert wird, wird der Status des Felds Handlungsbedarf auf **True** aktualisiert. Der Status kann vom Besitzer des Felds „Zuweisungsgruppe“ in „ **False** “ geändert werden.

i Hinweis:

Als Systemadministrator können Sie die Business Rule „Handlungsbedarf festlegen“ auf „falsch“ konfigurieren.

Eskalieren Sie einen Incident in Proactive Service Experience Workflows

Eskalieren Sie einen Incident, um die Untersuchung und Diagnose dieses Incident fortzusetzen. Durch die Eskalation eines Incident können Sie eine erfahrenere Ressource um Hilfe bitten, damit das Problem schneller gelöst wird.

Vorbereitungen

Diese Aufgabe setzt voraus, dass Sie an einem Incident gearbeitet haben und ihn an die nächste Eskalationsgruppe eskalieren müssen.

i Hinweis:

Stellen Sie sicher, dass der Administrator diese Rolle den Eskalationsgruppen zugewiesen hat. Weitere Informationen dazu, wie Administratoren Rollen zuweisen, finden Sie unter [Einer Gruppe eine Rolle](#) zuweisen.

Erforderliche Rolle: sn_ind_tsm_core.noc_agent

Prozedur

1. Navigieren Sie in *Service Operations-Arbeitsbereich* zu **Liste > Incidents > Offen** und wählen Sie einen Incident aus.
2. Wählen Sie im Incident-Datensatzformular in der Dropdown-Liste oben rechts die **Option Eskalieren aus**.

- 3.** Geben Sie im Popup-Fenster „Notizen für die Eskalation erfassen“ eine beschreibende Notiz ein, und wählen **Sie Eskalieren aus.**

Diese Aktion löst den Subflow für die nächste Ebene der Eskalationsgruppe aus, und die Zuweisungsgruppe wird automatisch in die nächste Eskalationsgruppe geändert.

Ergebnisse

- Der Status der Incident-Aufgabe für den vorherigen Techniker wird auf „Abgeschlossen“ gesetzt, und die Arbeitsnotiz wird protokolliert.
- Für den neu zugewiesenen Benutzer wird eine Incident-Aufgabe erstellt, deren Status auf In Bearbeitung gesetzt wird.
- Eine Arbeitsnotiz im Aktivitätenstrom enthält Anweisungen für den Techniker auf dieser Eskalationsebene.
- Die Incident-Stufe wird mit der nächsten Eskalationsstufe aktualisiert.
- Die Zuweisungsgruppe wird entsprechend der Eskalationsebene aktualisiert.

Kunden- oder Partner-Accounts werden in überprüft Proactive Service Experience Workflows

Erfahren Sie, wie Ihre Teams des technischen Supports (z. B. Cloud Ops-, Server- oder Netzwerkbetriebsteams) können die Ansicht „Operations Account 360“ in der Anwendung Proactive Service Experience Workflows verwenden, um Einblicke in die Accounts von Kunden oder Partnern zu erhalten.

Als Mitarbeiter des technischen Supports können Sie Informationen zu Aufgaben, Eskalationen, wichtigen Kundendaten und Metriken sammeln, die den Accounts Ihrer Kunden oder Partner in Service Operations-Arbeitsbereich zugeordnet sind. Mit diesen Daten können Sie die folgenden Arten von Informationen nachverfolgen:

- Wer der Kunde oder Partner ist und welche Produkte, Services, Assets und Konfigurationselemente an ihn verkauft wurden.
- Wer die wichtigsten Kontakte für den Technologieanbieter und den Kunden oder Partner sind.
- Was ist die CSAT-Punktzahl für den Technologieanbieter und den Kunden oder Partner?
- Wie der Technologieanbieter und der Kunde oder Partner aus SLA-Perspektive für den Monat nachverfolgen.
- Welche schwerwiegenden Incidents, Fälle und Eskalationen sich auf die Accounts auswirken.
- Wie viele Aufgaben werden nach Typ geschlossen und wie viele werden alle 12 Wochen geöffnet?
- Spezifische Wissensartikel und Katalogelemente, die für den Account entwickelt wurden. Mit diesen Informationen können Ihre Service Desk-Mitarbeiter Einblicke darüber erhalten, was der Kunde oder Partner möchte und welche Maßnahmen ergriffen werden müssen.

Die Daten, die in der Ansicht „Operations Account 360“ in Service Operations-Arbeitsbereich visualisiert werden, werden aus Aufgabendatensätzen abgeleitet, in denen der Unternehmenswert dem beim Start dieser Ansicht ausgewählten Account entspricht. Eine Ausnahme bilden Wissensartikel und Katalogelemente.

Darüber hinaus funktioniert die 360-Grad-Ansicht „Account für Vorgänge“ nur für Unternehmensdatensätze, deren Klassenwert „account“ ist. Unternehmensdatensätze mit

dem Klassenwert „company“ zeigen die traditionelle Standardarbeitsbereichsansicht von Service Operations Workspace an.

Weitere Informationen zum Abrufen von Account-Einblicken finden Sie unter [Überprüfen Sie einen Account mit der 360-Grad-Ansicht in Proactive Service Experience Workflows](#).

Überprüfen Sie einen Account mit der 360-Grad-Ansicht in Proactive Service Experience Workflows

Überprüfen Sie den Account eines Kunden oder Partners mithilfe der Ansicht „Operations Account 360“, die von der Anwendung Proactive Service Experience Workflows in Service Operations-Arbeitsbereich bereitgestellt wird. Sie können Ihre Daten und Aufgaben im Zusammenhang mit Kunden oder Partnern nachverfolgen und dann Maßnahmen ergreifen, um Ihre Servicebereitstellung zu verbessern.

Vorbereitungen

Erforderliche Rolle: sn_ind_tsm_core_noc_agent

Prozedur

1. Navigieren zu **Arbeitsbereiche > Service Operations-Arbeitsbereich**.
2. Klicken Sie auf der Registerkarte Service Operations Workspace **Listen** auf **Accounts > Alle**.
3. Wählen Sie in der Liste „Accounts“ einen Kunden-Account aus.

i Hinweis:

Sie können diese Ansicht auch aufrufen, indem Sie in den verschiedenen Incident-Listen oder im Incident-Formular in Service Operations-Arbeitsbereich auf einen Unternehmensnamen (Account) klicken.

4. Überprüfen Sie auf der Seite „Account-Informationen“ im Abschnitt „Kundenzusammenfassung“ die allgemeinen Kundendetails für den ausgewählten Account, z. B. Status „Aktiv“ des Kunden, Rangstufe und die Anzahl der Mitarbeiter.

Wenn für diesen Account Eskalationen vorliegen, können Sie diese anzeigen, indem Sie auf **Eskalationen** anzeigen klicken. Zeigen Sie im Abschnitt „Übersicht“ die Einblicke in Kontoinformationen an.

Seite „Account-Informationen“ – Registerkarte „Account-Übersicht“

Feld	Beschreibung
Konto-Teammitglieder	Teammitglieder dieses Kunden. Klicken Sie auf Alle anzeigen, um die Liste aller Teammitglieder anzuzeigen.
Wichtige Kundenkontakte	Wichtige Kontakte dieses Kunden. Klicken Sie auf Alle anzeigen, um die Liste aller wichtigen Kundenkontakte anzuzeigen.
Einzelne Punktzahlkarten	<ul style="list-style-type: none"> ○ Verträge ○ Berechtigungen ○ CSAT

Feld	Beschreibung
	<p>i Hinweis: Die Ergebnisse stammen aus den Bewertungen, die an die sofort einsatzbereite Kundenzufriedenheitsumfrage gebunden sind, die vom Core CSM-Plugin bereitgestellt wird.</p> <ul style="list-style-type: none"> ○ Eskalationsfälle ○ Verkaufte Produkte ○ Installationsbasis ○ Assets ○ Configuration Items
Laufende Arbeit des technischen Supports	<ul style="list-style-type: none"> ○ Abgeschlossene Aufgaben ○ Wöchentliche neue Aufgaben vs. geschlossene Aufgaben ○ Aufgaben-SLA-Erfolg für aktuellen Monat
Changes	Von Ihrem Account ausgelöste Change-Anforderungen
Probleme	Probleme im Zusammenhang mit dem Account
Incidents	Incidents im Zusammenhang mit dem Account
Incident-SLA	Incident-SLAs im Zusammenhang mit dem Account
Ausfälle	Ausfälle im Zusammenhang mit dem Account
Anforderungen	Anforderungen im Zusammenhang mit dem Account
Fälle	Fälle im Zusammenhang mit dem Account
Kontextbezogener Seitenbereich	<ul style="list-style-type: none"> ○ Anhänge ○ Vorlagen ○ Account Assist <p>i Hinweis: Sie können auch nach schwerwiegenden Incidents, schwerwiegenden Fällen, Wissen, Artikeln oder Katalogelementen suchen.</p>

5. Auf der Seite „Zugehörige Datensätze“ werden folgende Standardlisten bereitgestellt:

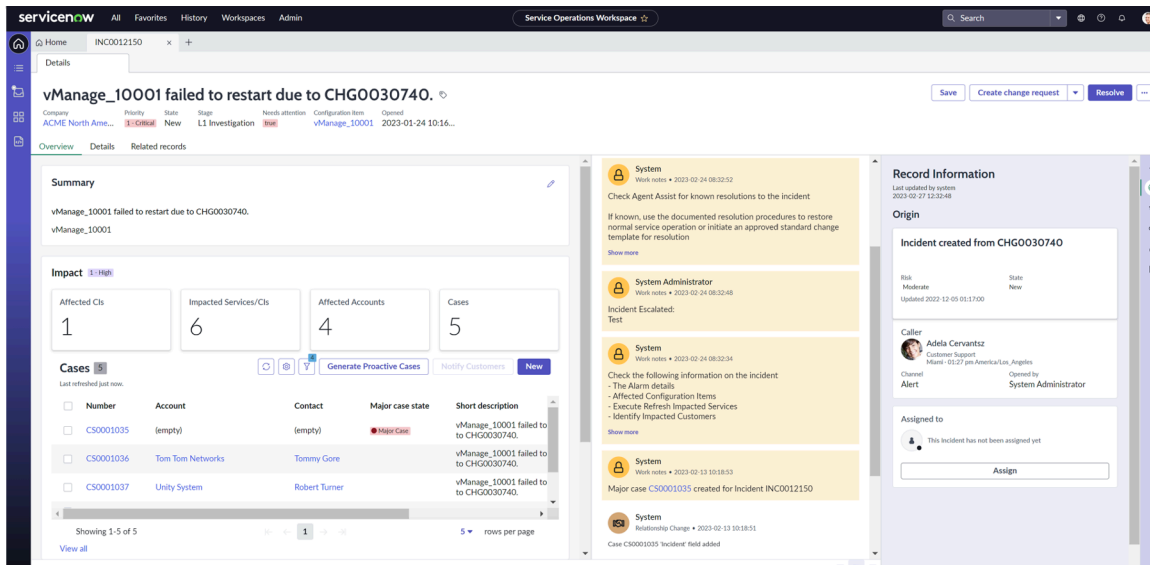
- Benutzer
- Kontakte
- Account-Adressen

- Produktmodelle
- Lieferantenkatalogartikel

Automatische Erstellung von Fällen und Updates aus Incidents

Fälle werden automatisch aus Incidents erstellt, wenn die Kennzeichnung **Proaktive Fälle generieren** ausgewählt ist.

Ein Fall wird basierend auf dem Wert, der in der Systemeigenschaft `major_case_affected_account_threshold` angegeben ist, als schwerwiegender Fall festgelegt. Dieser Wert kann vom Administrator geändert werden.



Automatische Übersetzung

Abhängig vom Schwellenwert werden verschiedene Flows ausgelöst, um entweder einen schwerwiegenden Incident oder mehrere einzelne Fälle zu erstellen. Der Falldatensatz wird dann ausgefüllt. In Szenarien mit geringfügigen Fällen werden beispielsweise die folgenden Informationen ausgefüllt:

- Kurzbeschreibung
- Beschreibung
- Proaktiv ist „true“.
- Kanal
- Incident
- Feld „Account“.

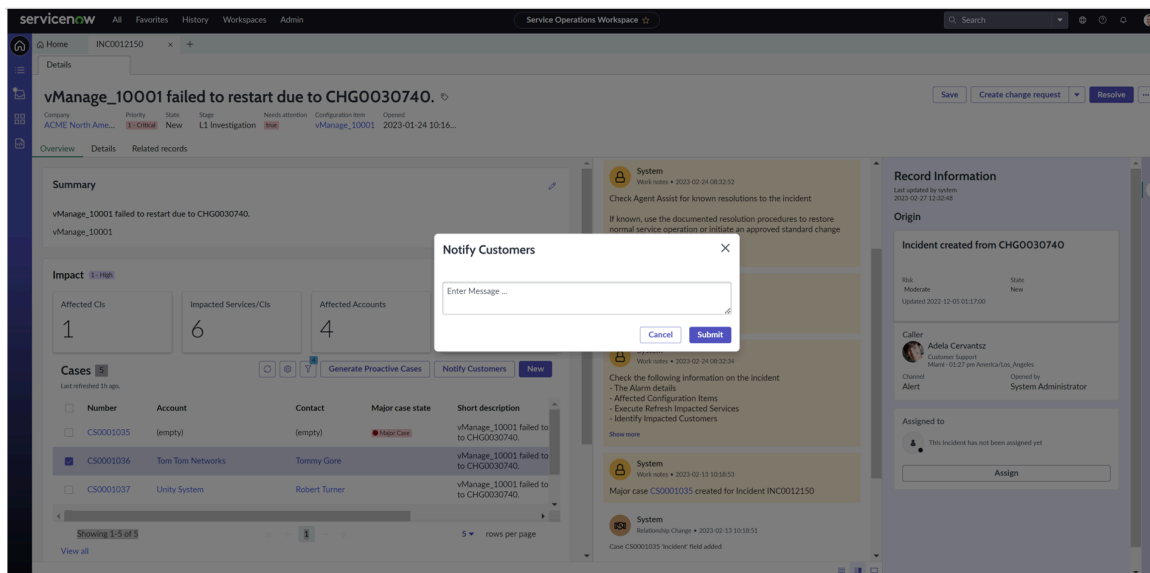
Der Administrator kann die Felder angeben, die aus dem übergeordneten Incident-Datensatz an die Falldatensätze übergeben werden müssen, um den geschäftlichen Anforderungen zu entsprechen.

Notify-Fallinformationen an Kunden

In Service Operations-Arbeitsbereich können Sie einen oder mehrere Fälle aus dem Abschnitt Fälle auswählen und **Kunden benachrichtigen** auswählen.

Geben Sie Ihre Benachrichtigungsnachricht ein, und wählen Sie **Absenden**. Die Nachricht wird im Abschnitt „Zusätzliche Kommentare“ in den Falldatensatz eingefügt und an den Kunden gesendet. Wenn ein Kunde auf diese Kommentare entweder per E-Mail oder

über das CSM -Portal antwortet, werden diese Kommentare in den Incident-Datensatz kopiert. Der Techniker des technischen Supports kann die Antwort oder anderes Feedback anzeigen, das bei der Überprüfung des Falls bereitgestellt wurde.



Hinweis:

Führen Sie die folgenden Schritte aus, um diese Funktion zu aktivieren:

- Geben Sie im Anwendungsnavigator `sys_properties.list` ein.
- Suchen Sie im Textfeld nach der Systemeigenschaft `proactive_workflows_for_providers.additional_comments_sync`.
- Wählen Sie die Systemeigenschaft aus, um den Datensatz zu öffnen.
- Geben Sie **true** in das Feld Wert ein, und wählen Sie **Aktualisieren** aus.

Um zu verhindern, dass zusätzliche Kommentare in alle mit dem Incident verbundenen Fälle kopiert werden, deaktivieren Sie die Geschäftsregel **Fall-Arbeitsnotiz für Kommentare aktualisieren** in der Incident-Tabelle.

Schwellenwert für schwerwiegenden Fall für automatisch generierte Fälle festlegen

Legen Sie den Schwellenwert für schwerwiegende Fälle fest, die aus Incidents in den Systemeigenschaften generiert werden.

Vorbereitungen

- Erforderliche Rolle: admin
- Ausgewählter Anwendungsbereich: Proaktive Service-Experience-Workflows

Warum und wann dieser Vorgang ausgeführt wird

Ein Standardschwellenwert wurde vordefiniert, um schwerwiegende Fälle aus Incidents zu generieren. Dieser Wert ist möglicherweise zu niedrig, oder Ihre Organisation verwendet nicht die CSM-Funktion für die Verwaltung schwerwiegender Fälle. In solchen Fällen können Sie den Schwellenwert in den Systemeigenschaften ändern, nachdem Proactive Service Experience Workflows aktiviert wurde.

Prozedur

1. Geben Sie im Anwendungsnavigator `sys_properties.list` ein.
2. Suchen Sie im Textfeld nach der Systemeigenschaft „`major_case_affected_threshold`“.
3. Klicken Sie auf die Systemeigenschaft, um den Datensatz zu öffnen.
4. Ändern Sie den Schwellenwert im Feld Wert.

i Hinweis:

Je niedriger der ganzzahlige Wert, desto höher die Anzahl von Fällen, die erforderlich ist, um einen schwerwiegenden Fall auszulösen. Wenn eine höhere Zahl angegeben wird, ist die Umkehrung „true“.

5. Klicken Sie auf **Aktualisieren**.

Erstellt einen Fall aus einer Change-Anforderung

Erstellen Sie einen Fall aus einer Change-Anforderung in Proactive Service Experience Workflows, damit Sie Ihre Kunden nach Abschluss der Change-Implementierung über einen Serviceausfall und dessen Lösung benachrichtigen können.

Vorbereitungen

Ein Change-Workflow wurde ausgelöst. Eine Zuweisungsgruppe mit den geplanten Start- und Enddaten wurde bereits festgelegt.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Nachdem ein Change-Workflow in Proactive Service Experience Workflows ausgelöst wurde, können Sie die Kunden und Systeme identifizieren, die von der Change-Anforderung betroffen sind. Sie können dann entweder automatisch die einzelnen Fälle für die betroffenen Kunden erstellen oder Ihre Kunden über die Ausfälle benachrichtigen.

Prozedur

1. Navigieren Sie in *Service Operations-Arbeitsbereich* zu **Liste > Changes > Offen** und wählen Sie einen Change-Datensatz aus.
2. **Wahlweise:** Weisen Sie die Change-Anforderung in einem vorhandenen Change-Datensatz einem Support-Techniker zu.
3. Erweitern Sie den Abschnitt Umfang und Auswirkung, und wählen Sie die Karte **Betroffene CIs** aus.
4. Überprüfen Sie, welche Services betroffen sind, indem Sie die Karte **Betroffene Services** auswählen und dann **Betroffene Services aktualisieren** auswählen.

Die Instanz initiiert eine Aktion, um die betroffenen Services zu aktualisieren und die betroffenen Konten zu finden.

5. **Zeigen** Sie die Liste der Ausfälle an, indem Sie die Karte Ausfälle auswählen.
6. Zeigen Sie an, welche Konten betroffen sind, indem Sie die Karte **Betroffene Konten** auswählen.
7. Ändern Sie im Abschnitt „Details“ den Status des Change-Datensatzes in **Autorisieren**. Die Fälle für die betroffenen Kunden werden automatisch erstellt.
8. Wählen Sie einen Fall aus der Liste der erstellten Fälle aus, und wählen Sie dann **Neu**.
9. Benachrichtigen Sie einen Kunden, indem Sie den Fall des Kunden auswählen und **Kunden benachrichtigen** auswählen.

10. Geben Sie im Popup-Fenster „Kunden benachrichtigen“ eine beschreibende Notiz zum Fall ein und wählen Sie **Notify** aus.

Eine Notiz wird automatisch in das Feld **Aktivität** des Change-Datensatzes und in die ausgewählten Falldatensätze eingefügt. Wenn Ihr Kunde den Fall mit einer Nachricht aktualisiert, wird der Fall automatisch mit dem Change-Datensatz synchronisiert.

i Hinweis:

Standardmäßig ist die Funktion „Kunden benachrichtigen“ nicht aktiv. Um sie zu aktivieren, müssen Sie als Administrator den Eigenschaftswert `proactive_workflows_for_providers.additional_comments_sync` auf TRUE festlegen und dann `Update case worknote for comments change` auswählen.

11. Wenn der Change Manager den Change-Datensatz autorisiert und sich der Status in **Geplant** ändert, können Sie den Status aktualisieren, indem Sie **Implementieren** und **Überprüfen** auswählen und den Datensatz speichern.
12. Wählen Sie den Lösungscode aus der Dropdown-Liste aus, geben Sie die Lösungsnotizen ein, bevor Sie die Change-Anforderung schließen, und aktualisieren Sie den Status, indem Sie **Schließen** wählen.

Informationen zu Nachrichten, die in Eskalations-Workflows in verwendet werden Proactive Service Experience Workflows

Mit der Basisanwendung Proactive Service Experience Workflows sind mehrere Nachrichten verfügbar, die in den Incident-Eskalationsabläufen verwendet werden.

Diese Nachrichten enthalten Anweisungen für Techniker des technischen Supports zur Problembehandlung, Eskalation und Lösung von Incidents. Die mit dem Basissystem bereitgestellten Incidents befassen sich mit allgemeinen netzwerkinitiierten Incidents, können jedoch für Ihre Problembehandlungsprozesse geändert werden.

Passen Sie die Nachrichtendateien für an Proactive Service Experience Workflows

Passen Sie die Nachrichten mit Anweisungen für die Netzwerktechniker an, die an netzwerkinitiierten Problemen für verschiedene Unterkategorien, Eskalationsebenen und Personas in Proactive Service Experience Workflows arbeiten.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Jeder Subflow in Proactive Service Experience Workflows verweist auf eine Nachrichtendatei, die Anweisungen für Service Desk-Mitarbeiter zur Problembehandlung, Eskalation und Lösung von netzwerkinitiierten Incidents enthält. Sie können den Standardnachrichtentext verwenden oder den Text für Ihre internen Problembehandlungsprozesse anpassen.

Prozedur

1. Navigieren zu **Alle > System-UI > Nachrichten**.
2. Suchen Sie nach Schlüsselwerten, die `sd_wan` enthalten.
3. Wählen Sie den Datensatz mit dem Text aus, den Sie anpassen möchten.

4. Geben Sie im Feld **Nachricht** Anweisungen für die Unterkategorie, die Persona und die Eskalationsebene dieses Subflows an.
5. Wählen Sie **Aktualisieren**.

Umgang mit Problemticketbenachrichtigungen

Verwenden Sie die Benachrichtigung für Telekommunikations-Problemtickets, um Systeme von Drittanbietern über die Incidents oder Fälle zu informieren, die reaktiv oder proaktiv in der Instanz ServiceNow erstellt werden. TDer Kunde erhält Benachrichtigungen über Aktualisierungen des Incident.

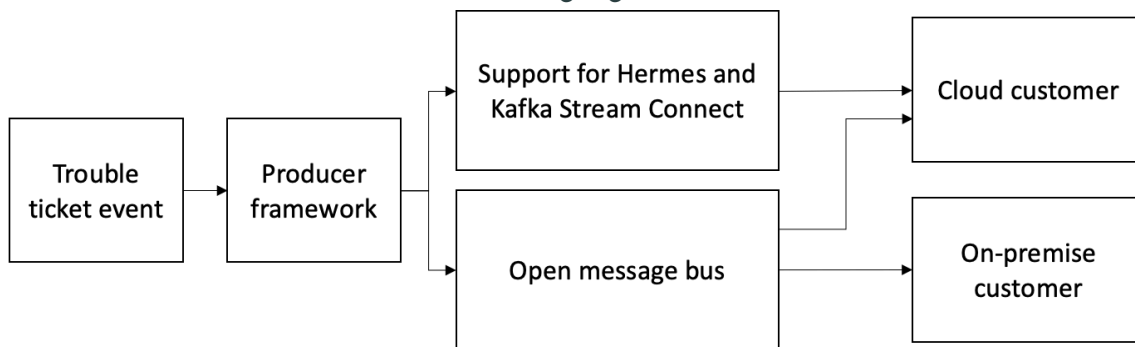
Übersicht

Ein Problemticket im TMF-Ökosystem ist ein Incident, der vom Kunden gemeldete Probleme, Netzerkennungsausfälle oder andere Probleme nachverfolgt und löst. Ein Problemticket-Incident kann in entweder reaktiv oder proaktiv erstellt werden. Beim reaktiven Ansatz wird ein Incident nach einer Ursachenanalyse (RCA) für einen Fall generiert, der aufgrund eines Systemfehlers gemeldet wird. Beim proaktiven Ansatz wird nach dem Empfang von Warnungen ein Incident generiert, sodass die Leistung von RCA oder Service Impact Analysis (SIA) die Auswirkungen auf die Services bewerten kann. Mit der Funktion für Problemticketbenachrichtigungen können Sie die Details des Incidents an die ausgehenden Systeme senden.

Framework für Problemticketbenachrichtigungen

Das folgende Diagramm zeigt die Komponenten im -Framework für die Problemticketbenachrichtigung.

Datenmodell für Problemticketbenachrichtigungen



Die Problemticketbenachrichtigung verwendet ein generisches Framework, um die ausgehenden Benachrichtigungen an das externe System zu senden. Dieses Framework unterstützt zwei Anwendungsfälle:

1. Veröffentlichen Sie Nachrichten mit dem Hermes-Messaging-Service in Hermes Kafka. Cloud-Kunden, die Hermes Kafka verwenden, können diese Architektur verwenden, um die Benachrichtigung zu erhalten.

Weitere Informationen finden Sie unter [Ausgehende Problemticketbenachrichtigungen mit Hermes erstellen](#).

2. Veröffentlichen Sie Nachrichten, um den Nachrichtenbus zu öffnen. Dieser Anwendungsfall ist vom Nachrichtenbus-unabhängig und unterstützt daher die Veröffentlichung der Benachrichtigung in einem beliebigen offenen Nachrichtenbus.

Sowohl Cloud- als auch On-Premise-Kunden können diesen Anwendungsfall verwenden. Weitere Informationen finden Sie unter [Ausgehende Problemticketbenachrichtigungen mit dem offenen Nachrichtenbus erstellen](#).

Ausgehende Problemticketbenachrichtigungen mit Hermes erstellen

Erstellen Sie mithilfe der Hermes-Fähigkeit eine ausgehende Benachrichtigung aus der Instanz ServiceNow. Kunden können die Details der Nachricht aus der Kafka-Umgebung in ihrem externen System verarbeiten.

Übersicht

In diesem Anwendungsfall werden die Benachrichtigungen von Ihrer ServiceNow -Instanz an den Hermes-Cluster gesendet. Nach Abschluss der Replikation von Hermes zu Kafka können Kunden die Nachrichten von ihrem eigenen Kafka verbrauchen oder abrufen.

- Weitere Informationen zum Hermes Messaging Service finden Sie unter [Hermes Messaging Service](#) .
- Weitere Informationen zu Apache Kafka Stream Connect finden Sie unter [Using Stream Connect for Apache Kafka](#) .

Im Release Washington DC werden die folgenden Events für die Problemticketbenachrichtigung unterstützt.

- Problemticket-Ereignis erstellen
- Change-Ereignis des Problemticketstatus
- Ereignis „Änderung des Problemticketattributs“.
- Erstellt ein Problemticketereignis für den Fall

Voraussetzungen

Vor der Erstellung einer ausgehenden Benachrichtigung muss der Kunde das Thema im Hermes-Cluster erstellen. Weitere Informationen zum Erstellen eines Themas in Hermes finden Sie unter [Managing namespaces and topics in Hermes](#) .

Workflow

Der Workflow zum Erstellen der ausgehenden Benachrichtigung mit Hermes enthält die folgenden Schritte:

1. Beim Auslösen des Problemticketereignisses ruft das System die entsprechende Geschäftsregel auf und stempelt den Ereignistyp.

Weitere Informationen zu Business Rules, die Sie Ihrer ServiceNow -Instanz hinzufügen müssen, finden Sie unter [Add a business rule for a new trouble ticket event](#) .

2. Das System übermittelt den Glide-Snapshot und den Event-Typ in der Staging-Tabelle, die als Warteschlange fungiert.
3. Das Ersteller-Framework wählt das Event aus und konvertiert es in eine TMF 688-Beschwerde-Event-Nutzlast.

Weitere Informationen zu den Systemeigenschaften, die Sie für das Ersteller-Framework konfigurieren müssen, finden Sie unter [Verwenden des Ersteller-Frameworks für ausgehende Benachrichtigungen](#).

4. Das System ruft die Producer V2-API von Stream Connect auf und erzeugt Event für das Hermes Kafka-Thema.
5. Stream Connect sendet das Event im Hermes Kafka-Cluster.
6. Die Kunden können die Nachricht in ihrem internen Kafka verwenden.

Zugehörige Informationen

[EventProcessorUtilOOB - Scoped](#)

[EventQueueProcessorOOB - Scoped](#)

Ausgehende Problemticketbenachrichtigungen mit dem offenen Nachrichtenbus erstellen

Erstellen Sie mithilfe des offenen Nachrichtenbusses eine ausgehende Benachrichtigung aus der Instanz ServiceNow. Kunden und können die Details der Benachrichtigung aus dem Nachrichtenbus in ihrem externen System verarbeiten.

Übersicht

In dieser eventgesteuerten Architektur werden die Benachrichtigungen an den offenen Nachrichtenbus von Ihrer ServiceNow -Instanz gesendet. Das Framework enthält Mechanismen für Themensynchronisierung und Themenauswahl. Der Themensynchronisierungsmechanismus synchronisiert die Themen, die Sie in der Instanz ServiceNow erstellt haben, mit dem offenen Nachrichtenbus. Wenn das Event im -Framework auftritt, wählt der Themenauswahlmechanismus das relevante Thema aus und veröffentlicht die Nachricht im Thema mithilfe eines REST-Proxy. Kunden können die ausgehende Benachrichtigung über den Nachrichtenbus in ihrem externen System verarbeiten.

Im Release Washington DC werden die folgenden Events für die Problemticketbenachrichtigung unterstützt.

- Problemticket-Ereignis erstellen
- Change-Ereignis des Problemticketstatus
- Ereignis „Änderung des Problemticketattributs“.
- Erstellt ein Problemticketereignis für den Fall

Erforderliches


Bevor ausgehende Benachrichtigungen erstellt werden, müssen die Ausgangsthemen in der Thementabelle [sn_api_notif_mgmt_topic] in der Instanz ServiceNow erstellt werden. Wenn Sie ein Ausgangsthema erstellen, führt das System eine Geschäftsregel aus und versucht, das Thema basierend auf der Konfiguration mit dem Nachrichtenbus zu synchronisieren. Weitere Informationen zum manuellen Erstellen eines Themas in der Thementabelle finden Sie unter [Create a topic](#). Das System synchronisiert nur das Ausgangsthema mit dem Nachrichtenbus im externen System. Das Feld **user_created** im zugeordneten Themendatensatz wird auf „true“ festgelegt.

Alternativ können Sie die Themen im Nachrichtenbus in Ihrem externen System erstellen und in die Thementabelle in der Instanz ServiceNow verschieben. Die Kunden rufen den *Event Management Topic Open-API*- Endpunkt auf, der das Thema in der Thementabelle [sn_api_notif_mgmt_topic] der Instanz ServiceNow speichert. Das Feld **user_created** im zugeordneten Themendatensatz ist auf „false“ festgelegt. Weitere Informationen zu den Methoden, die bei der Verarbeitung des *Event Management Topic Open-API*- Endpunkts verwendet werden, finden Sie unter [Event Management Topic Open API](#).

Workflow

Der Workflow zum Erstellen der ausgehenden Benachrichtigung mithilfe des offenen Nachrichtenbusses enthält die folgenden Schritte:

1. Beim Auslösen des Problemticketereignisses ruft das System die entsprechende Geschäftsregel auf und stempelt den Ereignistyp.

Weitere Informationen zu der Business Rule, die Sie Ihrer ServiceNow -Instanz hinzufügen müssen, finden Sie unter [Add a business rule for a new trouble ticket event](#) .

2. Das System übermittelt den Glide-Snapshot und den Event-Typ in der Staging-Tabelle, die als Warteschlange fungiert.
3. Das Ersteller-Framework wählt das Event aus und konvertiert es in eine TMF 688-Beschwerde-Event-Nutzlast.

Weitere Informationen zum Ersteller-Framework finden Sie unter [Verwenden des Ersteller-Frameworks für ausgehende Benachrichtigungen](#).

4. Der Themenauswahlmechanismus bestimmt die Themen, die mit dem Event-Typ kompatibel sind. Die Themenauswahl führt die folgenden Schritte aus, um die Kompatibilität der Themen zu überprüfen:
 - a. Das System durchsucht die Themen, bei denen das Feld **Typ** in der Thementabelle als **Ausgehend** festgelegt ist.

- b. Das System überprüft die Header- und Inhaltsabfrage aller Ausgangsthemen und gleicht die Kompatibilität mit der Event-Nutzlast ab.

Weitere Informationen zum Anpassen des vorhandenen Themenauswahlmechanismus finden Sie unter [OpenMessageBusEventPublisherOOB - Scoped](#) .

5. Das System sendet die Liste der kompatiblen Themen und die Event-Nutzlast an die Spoke-Auswahl.
6. Die vom Kunden konfigurierte Spoke-Auswahl ruft den REST-Schritt auf, der für jedes Thema konfiguriert ist, und sendet ihn an den Nachrichtenbus-REST-Proxy im externen System.

Weitere Informationen zur Methode zum Senden von Nachrichten an die Spoke-Auswahl finden Sie unter [OpenMessageBusEventPublisherOOB - Scoped](#)  und [Configure the Producer Event Notification Framework to use the Open Message Bus](#) .

7. Die Kunden können die Nachricht in ihrem Nachrichtenbus-REST-Proxy verarbeiten.

Zugehörige Informationen

[EventProcessorUtilOOB - Scoped](#) 

[EventQueueProcessorOOB - Scoped](#) 

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

Verwenden des Ersteller-Frameworks für ausgehende Benachrichtigungen

Das Ersteller-Framework wählt das Event aus der Instanz ServiceNow aus und sendet die ausgehende Benachrichtigung an das externe System. Sie können die Details der Benachrichtigung aus dem Messaging-Service abrufen, der in Ihrem externen System installiert ist.

Systemeigenschaften

Sie müssen die Systemeigenschaften konfigurieren, um das Ersteller-Framework für ausgehende Benachrichtigungen zu verwenden. In der folgenden Tabelle wird die Liste der Systemeigenschaften erläutert, die für die geplanten Aufgaben festgelegt werden.

Systemeigenschaften des Produzenten-Frameworks

Eigenschaft	Beschreibung	Typ
sn_api_notif_mgmt.event.log	<p>Protokollierungsebene, die in die Debug-Protokolle geschrieben werden soll. Sie können die folgenden Protokollierungsebenen auswählen:</p> <ul style="list-style-type: none"> • notfall: Gesamtausfall. • Warnung: Systembeschädigung einer Datenbank, z. B. • crit: Wird normalerweise für Hardwarefehler verwendet, z. B. • err: Beliebige Fehler. • warning: Alle Warnungen • Hinweis: Mögliche Aktion erforderlich, aber nicht unbedingt. • Info: Keine Aktion erforderlich. • debuggen: Wird im Allgemeinen nicht verwendet, außer um alles für die Fehlersuche zu erfassen. <p>Standardwert: err</p>	Zeichenfolge
sn_api_notif_mgmt.publisher_message_definer.config	<p>Definiert die Nachrichten mit dem Hermes Messaging Service, dem Open Message Bus oder beiden Nachrichtenbussen veröffentlicht werden. Sie können die folgenden Werte verwenden:</p> <ul style="list-style-type: none"> • openMessageBus • hermes • beides 	Zeichenfolge

Systemeigenschaften des Produzenten-Frameworks (Fortsetzung)

Eigenschaft	Beschreibung	Typ
	Standardwert: openMessageBus	
sn_api_notif_mgmt.inboundqueue.maxrecords	<p>Maximale Anzahl von Datensätzen, die der Planer für eine Planerausführung aus der eingehenden Warteschlange abrufen. Dieser Wert wird in Verbindung mit dem Parameter <code>sn_api_notif_mgmt.inboundqueue.batch.limit</code> verwendet.</p> <ul style="list-style-type: none"> • Standardwert: 200 • Andere mögliche Werte: nach Bedarf <p>Beispiel: Wenn die Batch-Grenze auf 50 und maxrecords auf 200 festgelegt ist und die Anzahl der Datensätze in der eingehenden Warteschlange 130 beträgt, ruft der Scheduler drei verschiedene Datensatz-Batches in einer einzigen Ausführung ab: zwei mit 50 Datensätzen und einer mit 30 Datensätzen. Wenn die Anzahl der Datensätze in der eingehenden Warteschlange 220 beträgt, ruft der Planer vier Stapel mit 50 Datensätzen ab, und die verbleibenden 20 Datensätze werden erst bei der nächsten Ausführung des Planers verarbeitet.</p> <p>Beim Festlegen dieses Werts müssen Sie auch die Zeit berücksichtigen, die der Scheduler für die Verarbeitung mehrerer Batches benötigt, und den Wert <code>sn_api_notif_mgmt.schedule.max.runtime</code> entsprechend festlegen.</p>	Ganzzahl
sn_api_notif_mgmt.inboundqueue.batchlimit	Anzahl der Datensätze, die der Planer in einem Batch aus der eingehenden Warteschlange abrufen und verarbeitet.	Ganzzahl

Systemeigenschaften des Produzenten-Frameworks (Fortsetzung)

Eigenschaft	Beschreibung	Typ
	<ul style="list-style-type: none"> • Standardwert: 200 • Andere mögliche Werte: nach Bedarf 	
sn_api_notif_mgmt.glide.mutex.script_max_retries	<p>Maximale Anzahl von Versuchen, eine Mutex-Sperre in den Datensätzen der eingehenden Warteschlange zu erfassen.</p> <ul style="list-style-type: none"> • Typ: Ganzzahl • Standardwert: 100 • Andere mögliche Werte: nach Bedarf 	Ganzzahl
sn_api_notif_mgmt.schedule.max_run_time	<p>Die maximale Zeit in Millisekunden, die die geplante Aufgabe ausgeführt werden kann, bevor sie fehlschlägt und einen Fehler meldet.</p> <ul style="list-style-type: none"> • Typ: Ganzzahl • Standardwert: 90.000 • Andere mögliche Werte: nach Bedarf 	Ganzzahl
sn_api_notif_mgmt.glide.mutex.script_min_wait	<p>Minimale Wartezeit in Millisekunden zwischen Versuchen, eine Mutex-Sperre für die Datensätze in der eingehenden Warteschlange zu erfassen.</p> <ul style="list-style-type: none"> • Typ: Ganzzahl • Standardwert: 100 • Andere mögliche Werte: nach Bedarf 	Ganzzahl

Workflow des Produzenten-Frameworks

Wenn das System ein Event an die Staging-Tabelle sendet, werden die folgenden Schritte als Teil des Ersteller-Framework-Mechanismus ausgeführt:

1. Der Scheduler wählt eine Anzahl von Datensätzen in einem vorkonfigurierten Intervall aus und sendet dann Glide-Snapshots an den Event-Prozessor.
2. Das System konvertiert den Glide-Snapshot basierend auf dem Event-Typ in eine TMF 688-Beschwerdeereignisnutzlast.

Weitere Informationen zu den Methoden zum Definieren und Generieren der TMF-konformen Nutzlasten für Problemticket-Ereignisse finden Sie unter [TopicAPIUtilsOOB - Scoped](#) .

3. Das System überprüft, ob die Benachrichtigungskonfiguration für Hermes Kafka oder den offenen Nachrichtenbus vorgesehen ist.

Weitere Informationen zum Konfigurieren des Frameworks für Ersteller-Event-Benachrichtigungen finden Sie unter [Producer Event Notification Framework developer guide](#) .

Zugehörige Informationen

[Ausgehende Problemticketbenachrichtigungen mit Hermes erstellen](#)

[Ausgehende Problemticketbenachrichtigungen mit dem offenen Nachrichtenbus erstellen](#)

Deaktivieren Sie die Problemticketbenachrichtigung

Deaktivieren Sie die Geschäftsregeln in Bezug auf die Incident- und Falltabellen, um den Empfang von Problemticketbenachrichtigungen zu beenden. Kunden können die Geschäftsregeln deaktivieren, wenn sie die Funktion zur Benachrichtigung über Problemtickets nicht nutzen möchten.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle > Systemdefinition > Business-Regeln**.
2. Wählen Sie die folgenden Geschäftsregeln aus, und deaktivieren Sie das Kontrollkästchen **Aktiv**.
 - Problemticket-Ereignis erstellen
 - Change-Ereignis des Problemticketstatus
 - Ereignis „Änderung des Problemticketattributs“.
 - Erstellt ein Problemticketereignis für den Fall

Proactive Service Experience Workflows-Referenz

Referenzthemen enthalten zusätzliche Informationen zu Proactive Service Experience Workflows.


Domänentrennung und Proactive Service Experience Workflows

Domänentrennung wird für Proactive Service Experience Workflows unterstützt. Mit Proactive Service Experience Workflows können Sie den normalen Servicebetrieb schnell wiederherstellen, wenn vom Netzwerk initiierte Incidents auftreten, und proaktiv die von diesen Incidents betroffenen Kunden identifizieren und benachrichtigen. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Standard

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter [Anwendungssupport für die Domänentrennung](#) .

Übersicht

Proactive Service Experience Workflows (TAW) ist eine Reihe von Workflows, die die Anwendung Incident-Management und ihre Integration in Kunden-Workflow-Prozesse wie Case Management und Außendienst-Management verbessern. Das bedeutet, dass Proactive Service Experience Workflows keine zusätzliche Unterstützung für die Domänentrennung erfordert, da die Grundlagenanwendungen diese Unterstützung bereits bieten. Weitere Informationen finden Sie unter [Proactive Service Experience Workflows](#).

Zugehörige Informationen

[Domänentrennung für Service Provider](#) .