



Zürich Telecommunications Service Operations Management

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

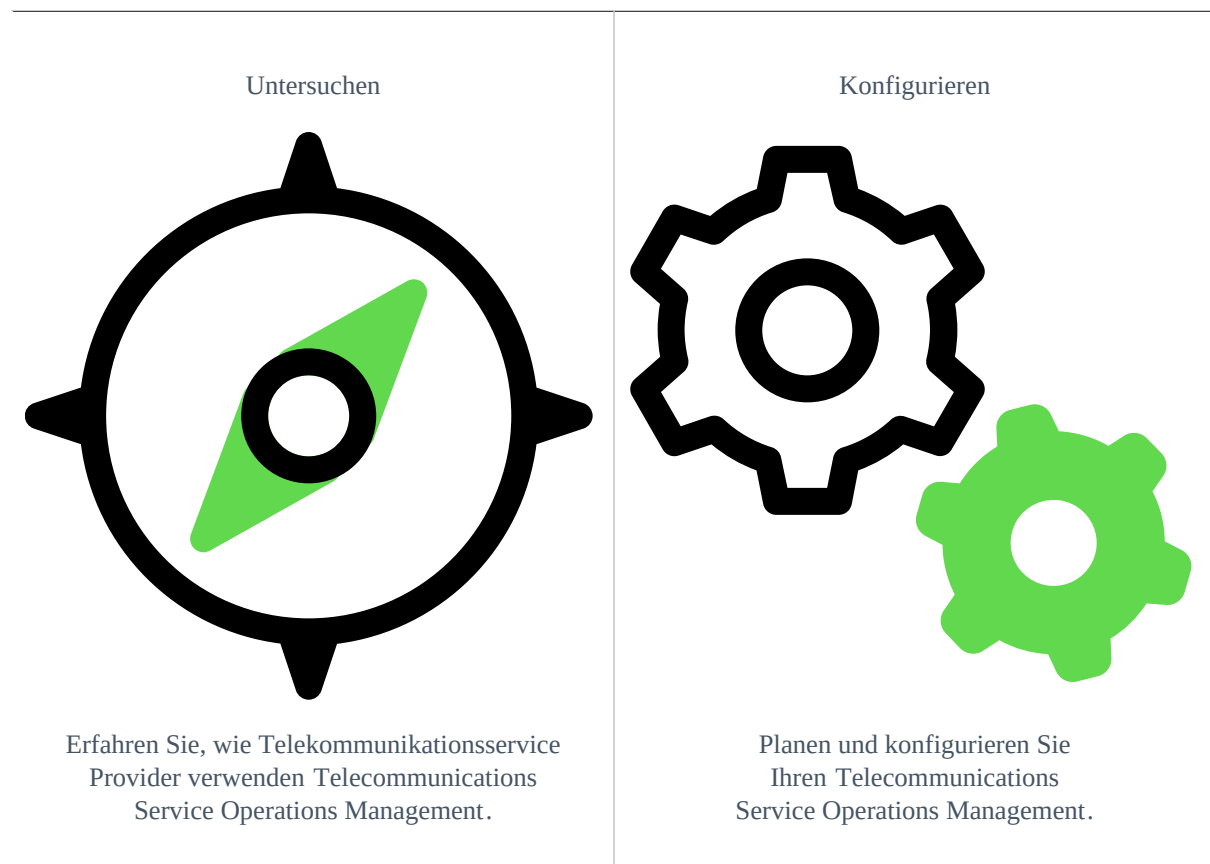
Inhaltsverzeichnis

Telecommunications Service Operations Management.....	4
Telecommunications Service Operations Management erkunden.....	6
Telekommunikations-API-Ereignisbenachrichtigungen.....	9
Telekommunikationstransparenz.....	10
Telecommunications Service Operations Management konfigurieren.....	45
Konfigurieren von Telekommunikations-API-Benachrichtigungen.....	46
Richten Sie die Transparenz der Telekommunikation ein.....	50
Telecommunications Service Operations Management verwenden.....	92
Verwenden von Telecom Discovery-Mustern.....	93
Führen Sie Den Nokia Altiplano-Import Aus.....	98
Validieren von JSON-Nutzlasten mit TSOM-Schemaprüfung.....	99
Führen Sie ein Audit für Telekommunikationsdiskrepanzen aus.....	101
Generieren Sie Berichte für Diskrepanzen bei Attributwerten.....	105
Telecommunications Service Operations Management – Referenz.....	106
Mit Benachrichtigungen der Telekommunikations-API installierte Systemkomponenten.....	106
Mit Nokia Altiplano installierte Systemkomponenten.....	107
Mit Nokia NSP installierte Systemkomponenten.....	108
[store-future: BEGIN review]	
[End]	
Komponenten für Identifizierung und Abgleich von Telekommunikationsdiskrepanzen.....	109

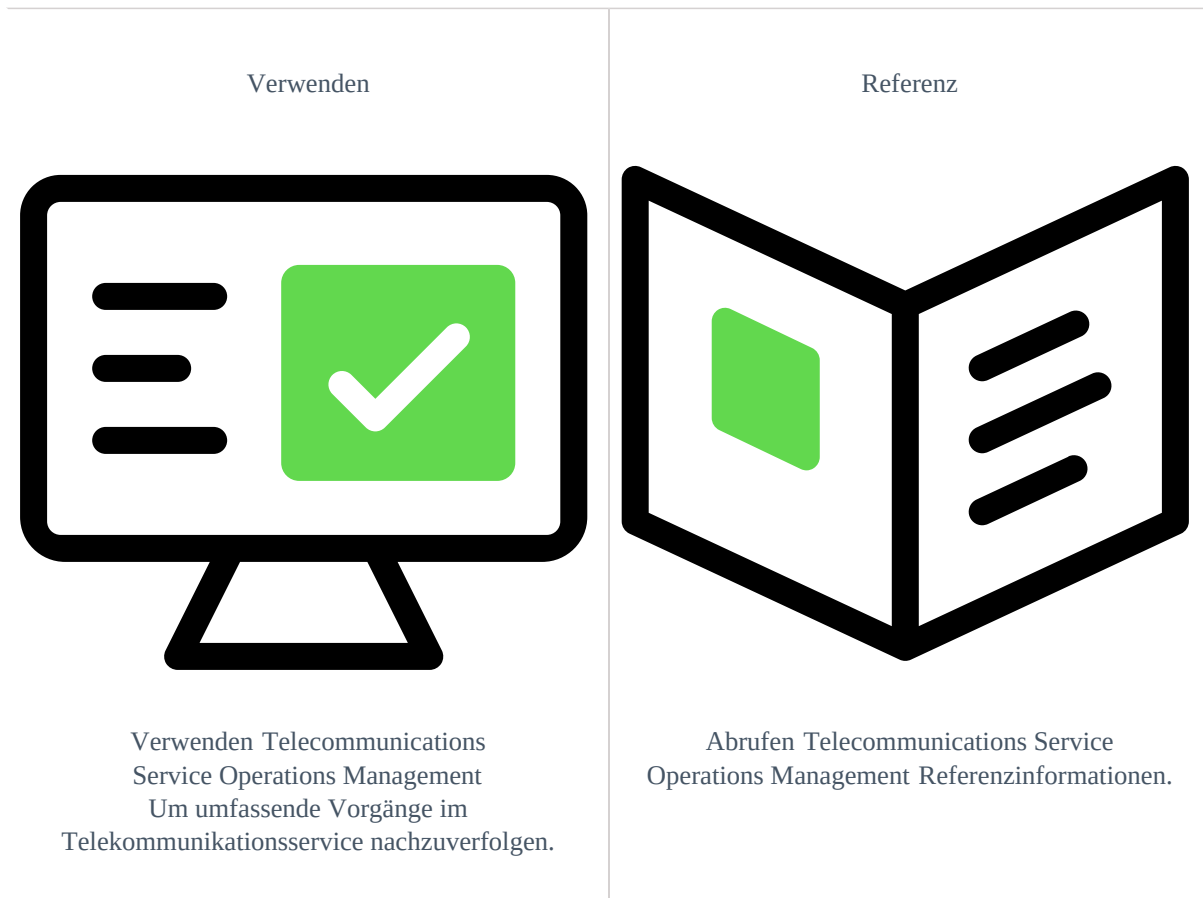
Telecommunications Service Operations Management

Erfahren Sie, wie Telecommunications Service Operations Management(TSOM) ermöglicht es Kommunikationsservice Providern (CSPs), Netzwerk- und Serviceprobleme proaktiv zu überwachen, zu analysieren und zu lösen, bevor sie sich auf Kunden auswirken. Erstellt auf ServiceNow AI Platform, TSOM bietet eine einheitliche Betriebsansicht in verteilten Telekommunikationsumgebungen mit mehreren Domänen und hilft Teams, die Serviceverfügbarkeit, die Betriebseffizienz und die Kundenzufriedenheit zu verbessern.

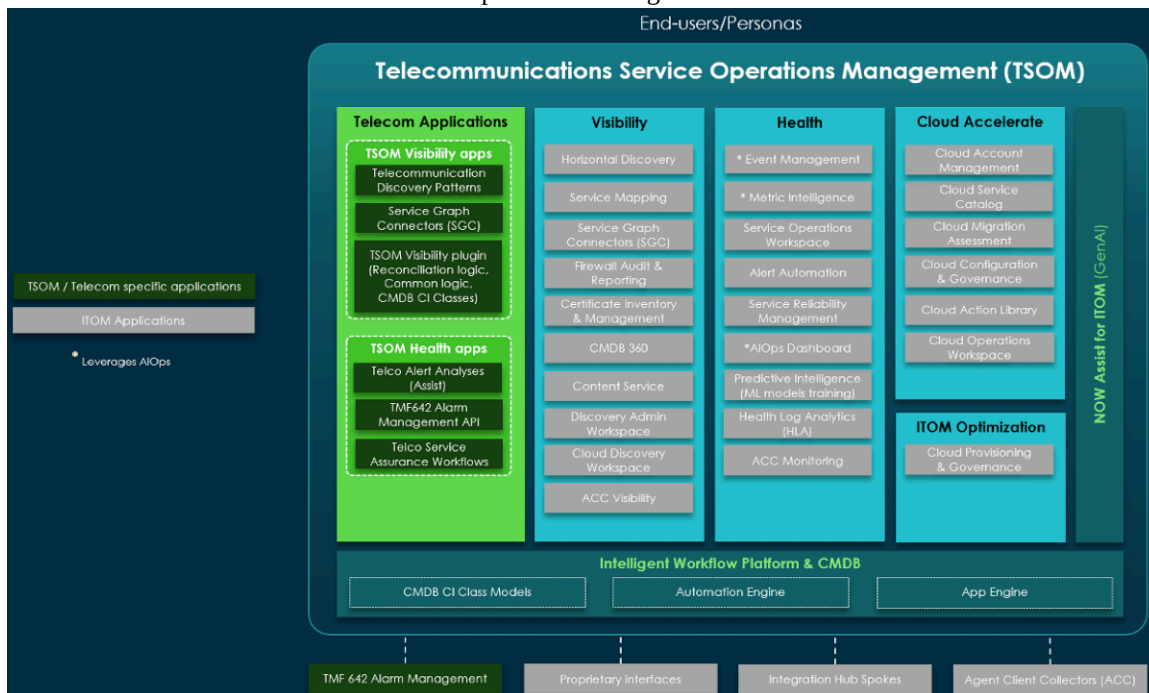
Erste Schritte



Automatische Übersetzung



Die folgende Infografik hilft Ihnen, die Architektur von zu verstehen Telecommunications Service Operations Management



Zusätzliche Ressourcen

Einige ServiceNow Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:



Weitere Informationen zu den Neuerungen und Änderungen in diesem Release finden Sie unter [Telecommunications Service Operations Management \(TSOM\) release notes](#)



ServiceNow Community

Stellen Sie eine Verbindung mit anderen her Telecommunications Service Operations Management Anwender in [ServiceNow Community](#)



Customer Success Center

Finden Sie nützliche Ressourcen im Zusammenhang mit Ihrer Rolle, und erkunden Sie Best Practices im [Customer Success Center](#)



ServiceNow University

Greifen Sie unter auf Echtzeitkurse, Schulungen zum Selbststudium und Karriereressourcen zu [ServiceNow-Universität](#)



Support

Wenden Sie sich unter an den Kundenservice <https://support.servicenow.com/now>

Telecommunications Service Operations Management erkunden

Erfahren Sie, wie Telecommunications Service Operations Management(TSOM) ermöglicht es Kommunikationsservice Providern (CSPs), Netzwerk- und Serviceprobleme proaktiv zu überwachen, zu analysieren und zu lösen, bevor sie sich auf Kunden auswirken. Erstellt auf ServiceNow AI Platform, TSOM bietet eine einheitliche Betriebsansicht in verteilten Telekommunikationsumgebungen mit mehreren Domänen und hilft Teams, die Serviceverfügbarkeit, die Betriebseffizienz und die Kundenzufriedenheit zu verbessern.

Telecommunications Service Operations Management Ist eine Lösung für Telekommunikationsanbieter, die vollständigen Einblick in die Netzwerk- und Serviceintegrität bietet. TSOM erfasst, korreliert und priorisiert Ereignisse aus allen Netzwerkdomänen – z. B. Zugriff, Transport und Core – mithilfe von Standard-APIs und der Leistungsfähigkeit von ServiceNow AI Platform. Durch die Bereitstellung umsetzbarer Echtzeiteinblicke ermöglicht TSOM sowohl Frontline- als auch Back-Office-Teams, Serviceprobleme zu beheben und eine konsistente Leistung zu gewährleisten.

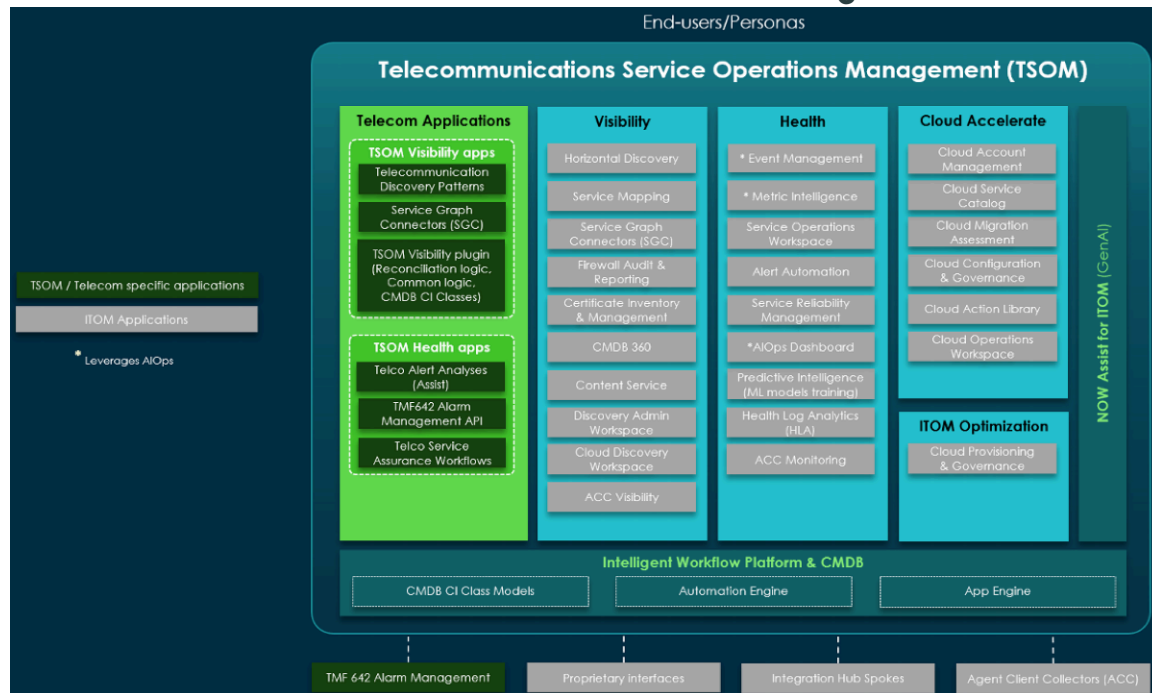
Funktionsweise von TSOM

Telecommunications Service Operations Management Vereinfacht den Telekommunikationsbetrieb, indem eine Verbindung mit vorhandenen Überwachungs- und Telemetrieplattformen hergestellt, umsetzbare Muster identifiziert und Lösungs-Workflows automatisiert werden. Es nutzt:

- Externes Ereignismanagement über Telekommunikations-API-Benachrichtigungen für standardisierte Alarmerfassung.
- Ereignismanagement Für Ereigniskorrelation, -Unterdrückung und -Priorisierung.
- Metrik Intelligence zur Erkennung von Schwellenwertverletzungen, Leistungsverschlechterungen und anomalem Verhalten in Echtzeit.
- Health Log Analytics zum Analysieren von Protokolldaten, Selektierung von Problemen und Identifizieren von Ursachen, bevor Anwender betroffen sind.

- Service-Auswirkungsanalyse zur Bewertung und Nachverfolgung von Serviceunterbrechungen basierend auf der betroffenen Infrastruktur und Business-Services.
- Service Graph Connectors und Discovery zum Erstellen einer dynamischen, Telekom-fähigen CMDB.

TSOM-Architektur und Telekommunikationsanwendungen



Schlüsselfunktionen

TSOM-Schlüsselfähigkeiten

Fähigkeit	Beschreibung
Ereignisüberwachung in Echtzeit	Erfassen Sie Alarmer und Ereignisse aus Mehrdomänennetzwerküberwachungssystemen mit externem Ereignismanagement über Telekommunikations-API-Benachrichtigungen.
Ereigniskorrelation und -Analyse	Nutzen Sie Ereignismanagement und Metrik Intelligence, um zugehörige Ereignisse zu korrelieren, Rauschen zu reduzieren und Anomalien zu erkennen. Weitere Informationen finden Sie unter Event Notification Management Open API .
Telekommunikationstransparenz	Erhalten Sie eine End-to-End-Visualisierung der Netzwerk- und Serviceintegrität, einschließlich Auswirkungsnachverfolgbarkeit.
Service-Auswirkungsanalyse	Verstehen Sie, wie sich Netzwerk- oder Infrastrukturprobleme auf Services auswirken, und priorisieren Sie die Korrektur basierend auf den Geschäftsauswirkungen.
Metrikdaten	Überwachen Sie Leistungstrends, erkennen Sie Schwellenwertverletzungen und Anomalien in Metriken, um Probleme proaktiv zu identifizieren. Weitere Informationen finden Sie unter Metric Intelligence .
Health Log Analytics	Die ServiceNow Health Log Analytics-Anwendung hilft, IT-Probleme zu verhindern, bevor Ihre Anwender betroffen sind. Sie hilft Ihnen, die Ursache eines Problems zu identifizieren, indem Sie zugehörige Protokolle

TSOM-Schlüsselfähigkeiten (Fortsetzung)

Fähigkeit	Beschreibung
	selektieren und die Rohdaten analysieren. Weitere Informationen finden Sie unter Health Log Analytics  .
Automatisierte Korrektur	Verwenden Sie geführte Workflows und Playbooks, um eine schnelle, konsistente und auditierbare Problemlösung zu ermöglichen.
Telekom-fähige CMDB	Verknüpfen Sie Infrastruktur, Services und physische/logische Konfigurationselemente (Configuration Items, CIs) mithilfe eines Telekommunikationsspezifischen Modells, um eine genaue Ursachenanalyse zu ermöglichen.
Warnungs-Management	Verwalten Sie Warnungen effizient mit Korrelations-, Gruppierungs- und automatisierten Antwortaktionen. Weitere Informationen finden Sie unter Manage and monitor alerts  .

Hauptvorteile

- MTTD- und MTTR-Reduzierung: Identifizieren und reagieren Sie auf servicebeeinflussende Probleme vor der Eskalation.
- Verbessern Sie die betriebliche Effizienz: Reduzierung von Lärm und optimieren Sie den Betrieb mit geführten Workflows.
- Verschaffen Sie sich End-to-End-Transparenz: Verstehen Sie, wie Infrastrukturprobleme sich auf kundenorientierte Services auswirken.
- Nahtlose Integration: Erfassen Sie Daten aus veralteten und modernen NMS/EMS-Tools mit offenen Standards.
- Compliance sicherstellen: Entspricht den TM Forum-Standards für Telekommunikationsservice Assurance.

Schlüsselpersonas

- Network Operations Center (NOC)-Agents: Überwachen Sie Netzwerkereignisse, und führen Sie geführte Lösungen aus.
- Service Assurance-Manager: Analysieren Sie Servicetrends, und verfolgen Sie Lösungsmetriken nach.
- Systemintegratoren/Administratoren: Konfigurieren Sie Datenerfassung, Korrelationsregeln und Workflows.
- Back-Office-Analysten: Untersuchen Sie die Ursachen, und verfolgen Sie CI-Beziehungen in der CMDB.

Integration mit ServiceNow AI Platform

TSOM ist in die Now Platform eingebettet und nahtlos in Kernfunktionen integriert, z. B.:

- Discovery
- Service-Mapping
- CMDB
- Flow Designer und Playbooks

Diese Integration bestätigt konsistente Workflows, genaue Servicemodelle und ein einheitliches Betriebsmanagement über Telekommunikationsdomänen hinweg.

Zugehörige Informationen

[Externes Ereignismanagement über Benachrichtigungen der Telekommunikations-API](#)

[Telekommunikationstransparenz](#)

Externes Ereignismanagement über Benachrichtigungen der Telekommunikations-API

Verwenden Sie die Telekommunikations-API-Benachrichtigung, um die externen Ereignisse zu empfangen, die im Netzwerksystem des Kunden auftreten, damit Sie umgehend im darauf reagieren können ServiceNow.

Einführung in die Benachrichtigung der Telekommunikations-API

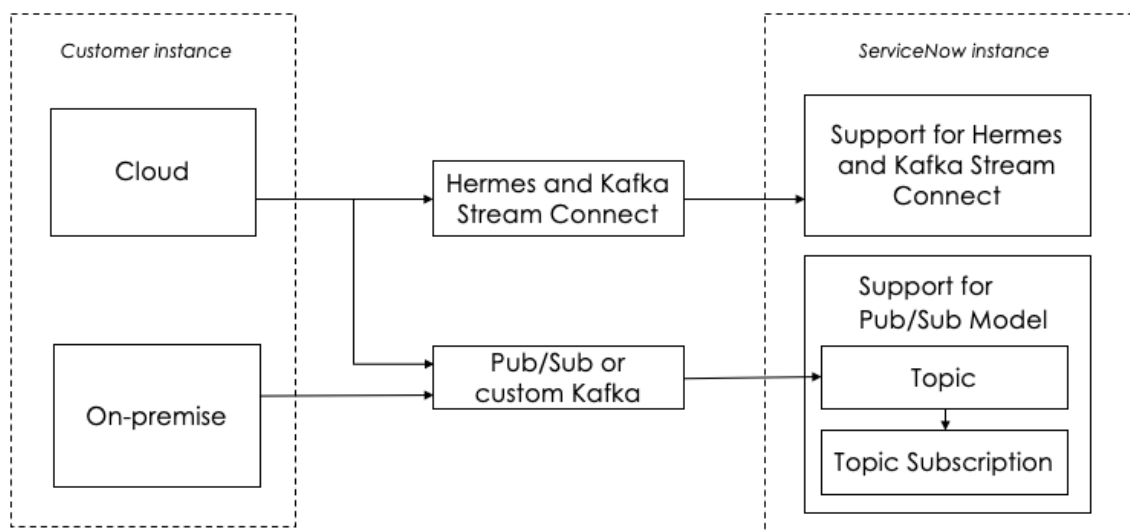
Die Telekommunikations-API-Benachrichtigung ist eine Funktion, die in der Anwendung „Telecommunications Alarm Management Open API“ verfügbar ist. Die Telekommunikations-API-Benachrichtigung aktiviert ServiceNow Um die eingehenden Benachrichtigungen im externen Netzwerksystem zu erhalten und rechtzeitig darauf zu reagieren. Es ermöglicht die Übertragung von Ereignissen an externe Systeme über Plattformfunktionen, indem Punkt-zu-Punkt-Verbindungen überflüssig werden.

Die Telekommunikations-API-Benachrichtigung empfängt eingehende Benachrichtigungen von den externen Systemen, die in Ihrem Netzwerk abonniert sind. Wenn die Benachrichtigungen vom externen System empfangen werden, können Sie die Ereignisse für die Antworten mit erstellen Ereignismanagement Anwendung. Basierend auf den gesammelten Informationen, die Ereignismanagement Stellt Dashboards bereit, die eine konsolidierte Ansicht aller Service-Impact-Ereignisse anzeigen.

Datenmodell für Telekommunikations-API-Benachrichtigung

Das folgende Diagramm zeigt die Komponenten im Datenmodell für die Telekommunikations-API-Benachrichtigung.

Datenmodell der API-Benachrichtigung



Die Telekommunikations-API-Benachrichtigung aktiviert ServiceNow Zum Empfangen eingehender Benachrichtigungen über die ereignisgesteuerten Architekturen wie das

Abonnementmodell „Herausgeber/Abonnent“ (Pub/Sub), Hermes und Kafka Stream Connect. Während Cloud-Kunden die Flexibilität haben, zwischen beiden Architekturen auszuwählen, können lokale Kunden ihr eigenes Kafka- oder Pub-/Sub-Abonnementmodell verwenden.

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

Im Pub-/Untermmodell werden eingehende Benachrichtigungen in Themen kategorisiert. Sie verwenden ServiceNow Um die eingehenden Benachrichtigungen für diese Themen zu veröffentlichen, haben Abonnenten (Kunden) die Flexibilität, die Themen auszuwählen, die sie abonnieren möchten. Mit diesem Prozess können Abonnenten nur die Nachrichten auswählen, die ihren Interessen entsprechen. Wenn beispielsweise 10 Themen für eingehende Nachrichten aus dem externen System vorhanden sind, kann ein Kunde je nach Anforderung zwei von ihnen abonnieren. Wenn daher Benachrichtigungen vom externen System empfangen werden, werden Ereignisse speziell für die beiden Themen generiert, die der Kunde abonniert hat.

Zugehörige Informationen

[Konfigurieren von Telekommunikations-API-Benachrichtigungen](#)

[Mit Benachrichtigungen der Telekommunikations-API installierte Systemkomponenten](#)

Telekommunikationstransparenz

Telekommunikationstransparenz erweitert die Discovery- und Abgleichsfunktionen von ITOM-Transparenz, um die spezifischen Anforderungen von Telekommunikationsdiensteanbietern zu erfüllen. Es ermöglicht einen genauen, Telekommunikationsfähigen Netzwerkbestand, indem Echtzeitnetzwerkdaten erkannt, Inkongruenzen abgeglichen und ein konsistentes Telekommunikationsmodell in Ihrer CMDB und TNI (Telecommunications Network Inventory) beibehalten werden.

Erkennen Sie physische und logische Netzwerkkomponenten in Telekommunikationsdomänen, gleichen Sie Diskrepanzen zwischen Discovery- und Bestandsdaten ab, und pflegen Sie eine Telekommunikations-spezifische CMDB-Struktur, um erweiterte Anwendungsfälle für Automatisierung und Sicherheit zu unterstützen.

Übersicht über Telekommunikationstransparenz

Telekommunikationstransparenz ist eine einheitliche Lösung für die Erkennung und Verwaltung von Telekommunikationsnetzwerkressourcen. Es nutzt bewährte Discovery-Technologien wie Horizontal Discovery, Telecommunications Discovery-Muster und Service Graph Connectors (SGC), um Netzwerkdaten aus verschiedenen Systemen (z. B. CLI/SNMP-basierte eigenständige Geräte oder API-gesteuerte EMS/NMS/Controller) in Ihre CMDB zu übertragen.

Telekommunikationstransparenz hilft Kommunikationsservice Providern (CSPs) und Telekommunikationsbetreibern:

- Erkennen und pflegen Sie den Telekommunikations-spezifischen Netzwerkbestand
- Abgleich von Diskrepanzen zwischen geplantem Bestand/Designbestand und tatsächlichem Netzwerkstatus
- Unterstützen Sie Autonomous Network Operations (ANO)-, Service-Fulfillment- und Assurance-Workflows

Schlüsselfähigkeiten

Schlüsselfähigkeiten von TSOM

Fähigkeit	Beschreibung
Telekommunikations-Discovery mit Mustern	Erkennen Sie eigenständige Netzwerkfunktionen (xNFs) wie Router und Switches mithilfe von SNMP- und CLI-Protokollen über vordefinierte Telecom Discovery-Muster.
Service Graph Connector-Integration	Bringen Sie Bestands- und Konfigurationsdaten von externen EMS/NMS/Controllern mithilfe von APIs nach Norden in CMDB.
Diskrepanzidentifizierung Und -Abgleich	Erkennen und beheben Sie Abweichungen zwischen inventarisierten und erkannten Daten (z. B. fehlende CIs, Modellabweichungen, veraltete Einträge).
Telekommunikationsorientierte Datenmodellierung	Verwalten Sie strukturierte und hierarchische Telekommunikationsdaten, einschließlich Schnittstellenkarten, Slots, Subslots, VLANs und Ports.
CMDB-Integration	Verwenden Sie CMDB 360 und Discovery-Administratorarbeitsbereich, um Discovery-Quellen, Attributänderungen und Abgleichsergebnisse zu überwachen.

Anwendungen und Plugins

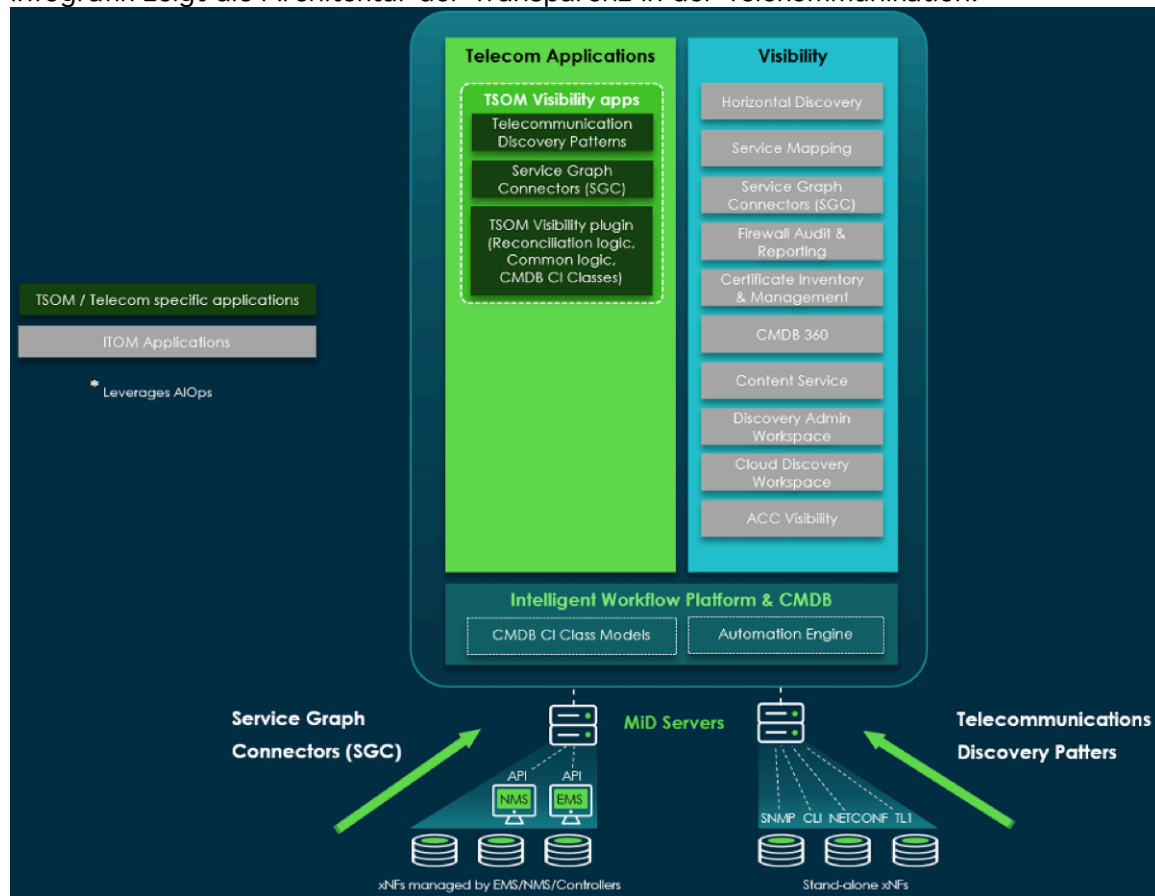
- 1. Horizontale Discovery-Muster für Telekommunikation:** Erkennt Telekommunikationsgeräte (xNFs) wie Router und Switches mithilfe von SNMP/CLI. Ermöglicht genaue Bestandsaktualisierungen durch Scannen der Live-Netzwerkinfrastruktur. Unterstützt lieferantenspezifische Muster, einschließlich:
 - Cisco (ASR1K, 7613, Nexus 9000, Nexus 3548)
 - JUNIPER (MX80, MX104, MX240, MX460)
- 2. Service Graph Connectors (SGCs) für TSOM:** Vorgefertigte Integrationen mit EMS/NMS/Controllern zum Importieren von Bestandsdaten über APIs. Unterstützt:
 - Geplante oder bedarfsgesteuerte Discovery
 - Mehrinstanz-Konfigurationen
 - Integration mit Systemen wie Nokia Altiplano (GPON-Netzwerke)
- 3. Telecom Visibility-Plugin:** Stellt gemeinsam genutzte Logik und grundlegende Komponenten für Discovery und Diskrepanzabgleich bereit. Stellt Folgendes sicher:
 - Konsistentes Verhalten in TSOM-Workflows
 - Wiederverwendbare Komponenten für Abgleich und Korrektur
- 4. CMDB-CI-Klassenmodelle für Telekommunikation (erforderliche Version: 1.69.0):** Erweitert die CMDB um Telekommunikationsspezifische Klassen und Beziehungen, einschließlich:
 - Schnittstellenkarten
 - Slots und Untersteckplätze
 - Netzwerkschnittstellen

Telekom-Sichtbarkeitsarchitektur

Telekommunikationstransparenz kombiniert direkte und indirekte Discovery-Methoden:

- Direkte Discovery mit SNMP/CLI (z. B. eigenständige Router/Switches)
- Indirekte Discovery mithilfe von APIs von EMS/NMS/Controllern (z. B. Nokia Altiplano)

Diese werden in CMDB und TNI eingespeist, die dann Entscheidungs-, Automatisierungs- und Netzwerkvorgänge unterstützen. Die folgende Infografik zeigt die Architektur der Transparenz in der Telekommunikation.



Automatische Übersetzung

Anwendungsfälle

Anwendungsfälle für Telekommunikationstransparenz

Anwendungsfall	Ergebnis
Autonomer Netzwerkbetrieb	Zuverlässiger Netzwerkbestand unterstützt KI/ML-gesteuerte Automatisierung.
Serviceerfüllung	Genauere CMDB/TNI stellt die Genauigkeit der Bestellung und eine schnelle Bereitstellung sicher.
Serviceerbringung	Abgeglichener Bestand reduziert die Problembehandlungszeit und erhöht die Betriebszeit.
Audit Und Compliance	Discovery-Administratorarbeitsbereich und CMDB 360 unterstützen Audit-Bereitschaft und Nachverfolgbarkeit.

Schlüsselpersonas

Telekommunikationstransparenz wird verwendet von:

- Netzwerk- und Infrastrukturteams: Erkennen und verwalten Sie Echtzeit-Netzwerkressourcendaten für Lieferanten und Technologien.
- Bestands- und Erfüllungsteams: Pflegen Sie eine genaue und vollständige CMDB/TNI, um die Serviceerfüllung, das Auftragsmanagement und die Bereitstellung zu unterstützen.
- Plattformadministratoren: Konfigurieren Sie Plugins, verwalten Sie Discovery-Quellen, validieren Sie Abgleichsregeln, und überwachen Sie die Discovery-Leistung.

Überwachungstools

Discovery-Administratorarbeitsbereich: Zentrale Konsole für:

- Überwachen Sie Discovery-Aufgaben
- Validiert Abgleichsprozesse
- Optimieren Sie Zeitpläne, und zeigen Sie Diagnosen an

CMDB 360 – Visualisieren:

- Aktualisierungsverlauf auf Attributebene
- Quellzuordnung
- Abgleichsregeln in Aktion

Hauptvorteile

Wichtige Vorteile der Transparenz in der Telekommunikation

Funktion	Leistung
CLI/SNMP-Discovery	Erweitert die Netzwerkabdeckung, ohne sich auf externe APIs zu verlassen.
Nokia Altiplano-Integration	Unterstützt die GPON-Netzwerk-Discovery über mehrere Controller-Instanzen hinweg.
Diskrepanzabgleich	Hält den Bestand sauber, umsetzbar und am realen Netzwerkstatus ausgerichtet.

Zugehörige Informationen

[Richten Sie die Transparenz der Telekommunikation ein](#)

[Discovery Admin Workspace](#)

Telekommunikationstransparenz vs.. ITOM-Transparenz

Da Telekommunikationsnetzwerke sich weiterentwickeln und hybrider und komplexer werden, ist der Einblick in die Infrastruktur wichtiger denn je. Um die spezifischen Anforderungen verschiedener Umgebungen zu erfüllen, ServiceNow AI Platform Bietet zwei speziell entwickelte Sichtbarkeitslösungen: ITOM-Transparenz und Telekommunikationstransparenz.

Sie basieren zwar auf derselben Grundlage, sind jedoch auf eine andere Welt zugeschnitten – ITOM für traditionelle IT-Infrastruktur und TSOM für Telekommunikationsnetzwerke.

Sowohl ITOM-Transparenz als auch Telekommunikationstransparenz basieren auf denselben zugrunde liegenden Fähigkeiten der ServiceNow Discovery-Engine, der Identifizierungs- und Abgleichsmodul (IRE) und der CMDB. Beide bieten:

- Agent-basierte und agentenlose Discovery.
- Horizontale und musterbasierte Discovery.
- Abgleich erkannter Daten in CMDB.
- Abhängigkeitszuordnung und CI-Beziehungserstellung.
- Integration mit Discovery-Administratorarbeitsbereich und CMDB 360.

Trotz dieser gemeinsam genutzten Architektur unterscheiden sich der Umfang, die Anwendungsfälle und die Datenmodelle, die sie bedienen.

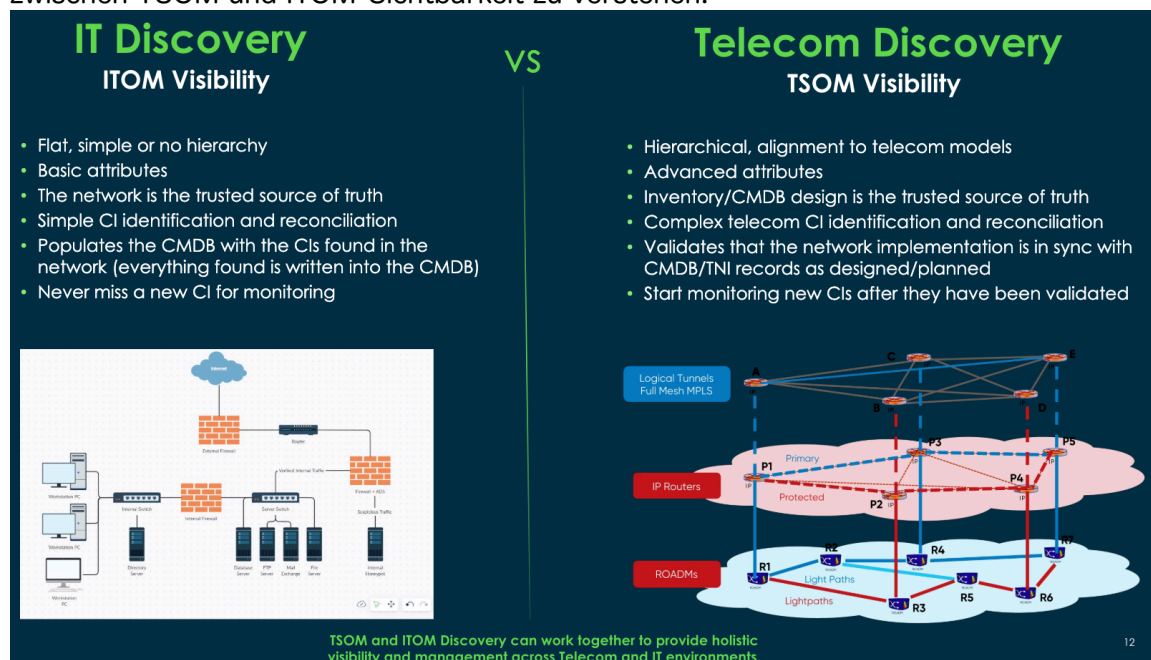
Wichtige Unterschiede zwischen TSOM- und ITOM-Transparenz

Telekommunikationstransparenz vs.. ITOM-Transparenz

Funktion/Fokusbereich	ITOM-Transparenz	Telekommunikationstransparenz
Zielumgebung	Herkömmliche IT-Infrastruktur (Server, Anwendungen, Datenbanken, Cloud-Ressourcen)	Telekommunikationsinfrastruktur (xNFs, Netzwerkelemente, EMS/ NMS-Controller)
Discovery-Methode	Horizontale Discovery mit IT-Mustern	Horizontale Discovery mit Telecommunications Discovery-Mustern (SNMP/CLI) und Service Graph Connectors für Telekommunikation
CMDB-Modell	ITOM-CMDB-Klassen (z. B. Windows Server, Anwendung, Netzwerkadapter)	Telecom-fähige CMDB-Klassen und TNI (Telecom Network Inventory) (z. B. Schnittstellenkarten, Slots, LAGs, Subslots, VLANs)
Erforderliche Plugins	Com.snc.Discovery und com.snc.itom.visibility	sn_tsom_Core, sn_tsom_patterns und Telekom-spezifische SGC-Plugins (z. B. sn_sgc_altiplano_Connector)
Anwendungsfallfokus	Anwendungsabhängigkeitszuordnung, Servicemodellierung, Cloud-Infrastruktur-Discovery	Erkennung, Abgleich, autonomer Netzwerkvorgänge für Telekommunikationsnetzwerke
Diskrepanzbehandlung	Allgemeine Ire-Abgleichsregeln	Telekommunikations-spezifische Diskrepanzidentifizierung und -Abgleich (z. B. Hierarchiekonflikte, Konflikte auf Attributebene)
Lieferantendatenerfassung	Hauptsächlich über Discovery-Muster	Starker Schwerpunkt auf API-Integrationen nach Norden mit SGCs (EMS/NMS/Controller)
Unterstützte Netzwerktypen	Unternehmensnetzwerke, Rechenzentren, Cloud	Telekommunikationsnetzwerke mit mehreren Lieferanten und Domänen (RAN, Core, Transport, Zugriff)

Infografik

Die folgende Infografik hilft Ihnen, die Unterschiede zwischen TSOM und ITOM-Sichtbarkeit zu verstehen.



Hauptvorteile

ITOM-Sichtbarkeit verwenden, wenn:

- Sie erkennen IT-Infrastrukturkomponenten (z. B. Windows-Server, Cloud-VMs, Datenbanken, Lastenausgleichsmodule).
- Zu Ihren primären Zielen gehören Service-Mapping, operative Resilienz oder Cloud-Optimierung.
- Sie konzentrieren sich auf ITSM-, ITOM- oder DevOps-Anwendungsfälle.

Telekommunikationstransparenz verwenden, wenn:

- Sie erkennen die Telekommunikations-Netzwerkinfrastruktur, einschließlich Geräten, die nicht von herkömmlichen IT-Systemen verwaltet werden.
- Sie haben es mit Telekom-spezifischen Netzwerkhierarchien wie Karten, Ports, Subslots und lag zu tun.
- Sie verlassen sich auf EMS/NMS/Controller als autorisierende Datenquellen.
- Sie benötigen Diskrepanzerkennung und -Abgleich, die auf Telekommunikationsbestandsmodelle zugeschnitten sind.
- Sie richten sich an den TM Forum-Standards aus, unterstützen autonomen Netzwerkbetrieb oder aktivieren die geschlossene Sicherung.

Beispiele

Anwendungsfall	ITOM-Transparenz	Telekommunikationstransparenz
Erkennen Sie eine Flotte virtueller Computer in AWS	Ja	Nein

Erfassen Sie Router und wechseln Sie Daten aus einem EMS mithilfe von APIs	Nein	Ja
Identifizieren Sie Abhängigkeiten von Anwendung zu Anwendung	Ja	Nein
Erkennen und Abgleich von Nichtübereinstimmungen in Telekommunikationskartenhierarchien	Nein	Ja

ITOM-Transparenz und Telekommunikationstransparenz dienen zwar beide dazu, eine genaue CMDB auszufüllen und zu pflegen, sie sind jedoch für verschiedene Domänen optimiert. ITOM-Transparenz ist auf IT-Umgebungen in Unternehmen ausgerichtet, während die Transparenz in der Telekommunikation auf die speziellen Anforderungen der Discovery der Telekommunikationsinfrastruktur, des Diskrepanzmanagements und des Bestandsabgleichs zugeschnitten ist.

Wenn Sie die richtige Sichtbarkeitslösung auswählen – oder beides zusammen verwenden –, wird bestätigt, dass Sie vertrauenswürdige, domänenspezifische operative Transparenz in IT- und Telekommunikationslandschaften beibehalten.

Telekommunikations-Discovery

ServiceNow AI Platform Telecom Discovery hilft Ihnen, einen umfassenden Einblick in Ihre Telekommunikationsnetzwerkinfrastruktur zu erhalten, indem die Funktionen von ITOM-Transparenz erweitert werden, um Telekommunikationsspezifische Anwendungsfälle zu unterstützen.

Diese Lösung wurde für Kommunikationsservice Provider (CSPs) entwickelt und ermöglicht die Erkennung und Zuordnung von Netzwerkelementen in Umgebungen mit mehreren Lieferanten mithilfe standardisierter Protokolle und der Integration in Netzwerkverwaltungssysteme.

Durch die Kombination von Telecom Discovery-Plugins mit der Leistung von Service Graph Connectors und Discovery-Mustern können Sie automatisch genaue Datensätze Ihrer Telekommunikationsressourcen in der Configuration Management Database (CMDB) ausfüllen und pflegen, was eine einheitliche Ansicht der IT- und Netzwerkinfrastruktur bietet.

Hinweis:

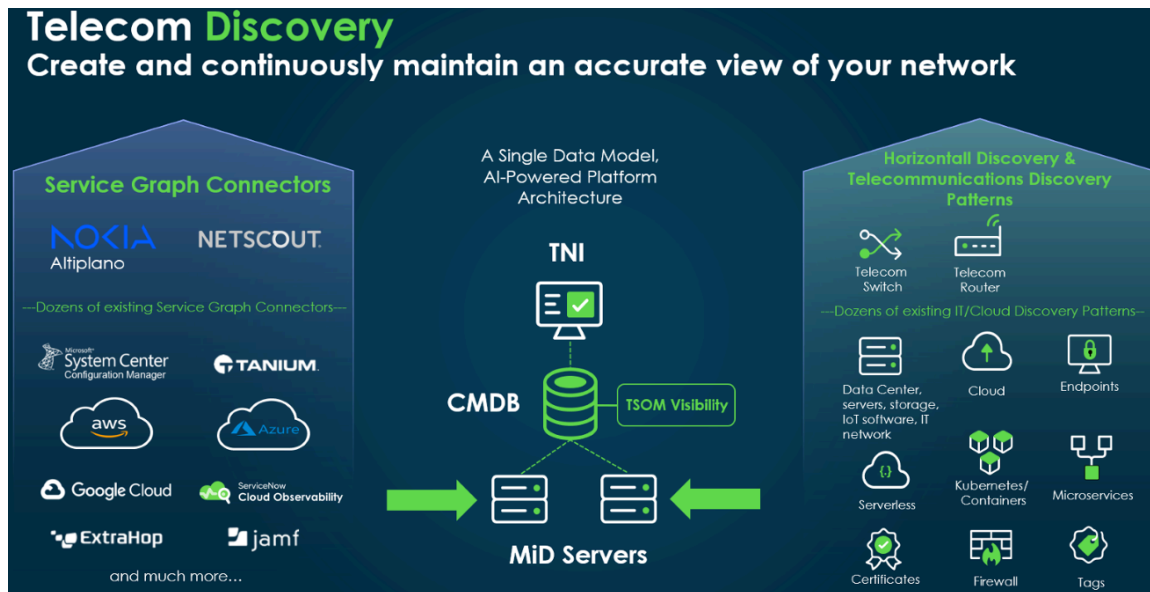
Telecom Discovery ist Teil des TSOM-Transparenzabonnements und richtet sich an das TM Forum Autonomous Network Operations (ANO)-Framework aus.

Mit Telecom Discovery können Sie:

- Erkennen Sie physische und logische Telekommunikationsnetzwerkressourcen über Domänen und Lieferanten hinweg.
- Integration mit Element Management Systems (EMS), Network Management Systems (NMS) und SDN Controllern.
- Füllen Sie CMDB/TNI-Datensätze basierend auf Echtzeitnetzwerkdaten automatisch aus und aktualisieren Sie sie.
- Erkennen Sie eigenständige XNFs mithilfe von SNMP und Befehlszeilenschnittstelle (CLI).
- Erweitern Sie CMDB-Daten mit Service Graph Connectors und spezialisierten Discovery-Mustern.

- Identifizieren Sie Diskrepanzen zwischen erkannten Netzwerkdaten und Bestandsdatensätzen.
- Unterstützen Sie Automatisierungsanwendungsfälle durch konsistente und genaue Transparenz der Infrastruktur.

Telecom Discovery-Architektur



Integration mit ITOM-Transparenz

Telecom Discovery wurde entwickelt, um vorhandene ITOM-Sichtbarkeitsfunktionen zu ergänzen. Sie können:

- Nutzen Sie horizontale Discovery- und ITOM-Fähigkeiten neben TSOM-Plugins.
- Konsistente Discovery-Praktiken für IT- und Telekommunikationsressourcen beibehalten.
- Verwenden Sie dasselbe CMDB-Datenmodell, um die Sichtbarkeit domänenübergreifender Services zu verwalten.

Diese Integration bestätigt ein einheitliches Asset-Management, eine schnellere Problemlösung und einen optimierten Betrieb in IT- und Netzwerkbereichen.

Anpassung mit Low-Code/No-Code-Tools

Stellt intuitive Designtools bereit, um die Discovery-Logik zu erweitern, ohne Code zu schreiben. Sie können:

- Erstellen oder ändern Sie anwenderdefinierte Service Graph Connectors.
- Erweitern Sie Telecommunications Discovery-Muster, um Lieferantenspezifische Anforderungen zu erfüllen.
- Beschleunigen Sie das Onboarding neuer Gerätetypen und Netzwerkbereichen.

Dieser Ansatz ermöglicht es CSPs, bei der Erweiterung ihrer Discovery-Stellfläche agil zu bleiben und die Amortisierungszeit zu verkürzen.

Schlüsselkomponenten

- Discovery-Muster für Telekommunikation (sn_tsom_patterns): Stellt Muster für die SNMP-basierte Discovery von eigenständigen Routern, Switches und xNFs bereit. Enthält Cisco- und Juniper-spezifische Discovery-Logik.
- Service Graph Connector für Nokia Altiplano(sn_sgc_altiplano_Connector): Aktiviert die Datensammlung vom Nokia Altiplano Access SDN-Controller über REST APIs.
- Telecom Core(sn_tsom_Core): Bietet grundlegende Fähigkeiten wie Diskrepanzidentifizierung, Korrekturlogik und gemeinsam genutzte Telekom-Discovery-Funktionen.

Telecom Discovery Builder-Framework

Das Telecom Discovery Builder-Framework ETL (Extrahieren, Transformieren, Laden) ist eine wiederverwendbare und schemaorientierte Komponente, die mit der Core-Anwendung Telecom Service Operations Management (TSOM) geliefert wird. Es bietet eine konsistente und erweiterbare Methode zum Erfassen von Telekommunikationsbestandsdaten in die ServiceNow Configuration Management Database (CMDB) über mehrere Service Graph Connectors (SGCs) hinweg.

Die ETL des Telecom Discovery Builder-Frameworks dient als Baseline-Datenerfassungsdienstprogramm, das zur Verarbeitung von CI-Daten (Configuration Item) für Telekommunikationsdaten entwickelt wurde. Es ermöglicht Connector-Entwicklungsteams, ETLs nicht von Grund auf neu zu erstellen, indem eine standardisierte Transformationslogik angeboten wird, die dupliziert und für jeden Connector angepasst werden kann.

Sobald das TSOM Core-Plugin aktiviert ist, wird das generische ETL automatisch bereitgestellt und wird im IntegrationHub ETL Studio verfügbar, kann wiederverwendet und an die Connector-spezifischen Anforderungen angepasst werden.

Warum und wann das Telecom Discovery Builder-Framework verwendet werden soll

Das Erstellen von ETL-Logik oder Transformationszuordnungen für jeden neuen Telekommunikations-Connector kann zeitaufwändig, fehleranfällig und inkonsistent sein. Das Telecom Discovery Builder-Framework optimiert den Prozess, indem es eine standardisierte, wiederverwendbare Grundlage bietet, die Konsistenz über Implementierungen hinweg gewährleistet.

Verwenden Sie das Telecom Discovery Builder-Framework, wenn Sie:

- Stellen Sie einen neuen Service Graph Connector in einer Telekommunikationsumgebung bereit, und möchten Sie vermeiden, dass ETL von Grund auf neu erstellt wird.
- Sorgen Sie für eine auf das Schema ausgerichtete Konsistenz über mehrere Connectors und Plattforminstanzen hinweg.
- Discovery-Nutzlasten und CI-Beziehungen konform mit TNI (Telecom Network Inventory). Weitere Informationen finden Sie unter [Telecommunications Network Inventory](#).
- Arbeiten Sie innerhalb eines SGC-Anwendungsbereichs (Service Graph Connector), und möchten Sie das ETL-Verhalten anpassen, ohne die Kernlogik zu ändern.
- Profitieren Sie von vordefinierten Zuordnungen, validierter Unterstützung für JSON-Schemata und einer UI-gesteuerten Konfigurationsschnittstelle.

Wichtige Fähigkeiten und Funktionen

- Automatische Bereitstellung mit TSOM-Core: Wird automatisch installiert und ist für Telekommunikations-Connectors einsatzbereit.
- Generische schemabasierte Erfassung: Unterstützt ein einheitliches Datenschema für Telekommunikations-CIs.
- Unterstützt Duplizierung und Anpassung: Duplizieren Sie die ETL des Telecom Discovery Builder-Frameworks mit IntegrationHub ETL Studio in Ihren Anwendungsbereich.
- TNI-Unterstützung: Ausgerichtet auf das TNI-Datenmodell, und die ETL-Logik kann erweitert werden, um TNI-Entitäten zu generieren und zu verknüpfen.
- Flexible Feldzuordnungsschnittstelle: Konfigurieren Sie Importsätze, Datenquellen, Ziele und Transformationslogik über eine UI-gesteuerte Experience.

Hauptvorteile

Verwenden Sie ETL des Telecom Discovery Builder-Frameworks, um Folgendes zu erzielen:

- Konsistenz bei der Strukturierung von Telekommunikations-Konfigurationselementen (CIs) und dem Laden in die CMDB.
- Wiederverwendbarkeit durch Duplizierung und Anpassung über Connectors hinweg.
- Compliance mit TNI-Schemas und Discovery-Modellanforderungen.
- Flexibilität, Datentransformationen zu erweitern und anzupassen, ohne das Basisschema zu gefährden.

Zugehörige Informationen

[Konfigurieren der ETL des Telecom Discovery Builder-Frameworks in einem Connector](#)

[Erweitern Sie die Unterstützung der TNI-Entität für duplizierte ETLs](#)

Leiten Sie die Discovery mithilfe von Discovery-Mustern

Das Plugin „Telecommunications Discovery Patterns“ (auch als TSOM-Muster bezeichnet) wird erweitert ServiceNow AI Platform Telecom Discovery zur Unterstützung der direkten Erkennung eigenständiger Netzwerkelemente wie Router und Switches, ohne auf herkömmliche Netzwerkverwaltungssysteme zu vertrauen. Diese Muster ermöglichen es Communication Service Providern (CSPs), XNFs mehrerer Hersteller mithilfe von Protokollen wie SNMP und CLI mit Unterstützung von NETCONF zu identifizieren und zuzuordnen.

Discovery-Muster für Telekommunikation bieten einen leistungsstarken, musterbasierten Ansatz zur Erkennung und Verwaltung von Telekommunikationsnetzwerkressourcen direkt über Netzwerkelemente. Diese Muster sind besonders nützlich für die Erkennung eigenständiger xNFs (z. B. Router und Switches), die nicht über herkömmliche EMS/NMS-Systeme verwaltet werden.

Diese Fähigkeit verbessert die Transparenz in Telekommunikationsinfrastrukturen und stellt sicher, dass sowohl lieferantenneutrale als auch lieferantenspezifische Gerätedaten erfasst und in der CMDB und dem TNI-Datenmodell (TNI) widerspiegelt werden.

Hinweis:

Discovery-Muster für Telekommunikation sind Teil des TSOM-Transparenzabonnements und als für Kunden sichtbares Plugin im ServiceNow Store verfügbar.

Wichtige Funktionen

- Direkte Netzwerkelement-Discovery
 - Verwenden Sie SNMP, CLI und NETCONF, um direkt mit physischen Netzwerkelementen zu kommunizieren.
 - Erkennen Sie physischen Netzwerkbestand wie Schnittstellenkarten, Steckplätze, Ports und Geräte, ohne sich auf EMS/NMS-Mediation zu verlassen.
- Automatisierte CI-Zuordnung und CMDB-Integration
 - Erkannte Daten werden automatisch CI-Klassen (Configuration Item) zugeordnet.
 - Ist direkt in die Identification and Reconciliation Engine (IRE) integriert, um genaue, nicht duplizierte CI-Datensätze in CMDB und TNI (Telecom Network Inventory) sicherzustellen.
- CMDB-Genauigkeit und -Compliance
 - Muster lösen Audits der CMDB-Compliance-Zertifizierung aus, um Nichtübereinstimmungen oder veraltete Datensätze zu erkennen.
 - Unterstützt die Identifizierung und Behebung von Diskrepanzen und trägt zur Aufrechterhaltung der Datenintegrität bei.
- Low-Code-Musteranpassung: Erweitern oder passen Sie Discovery-Muster mit Low-Code-Musterdesignern an, um Ihre spezifische Netzwerkarchitektur und Geschäftsanforderungen zu erfüllen.

Funktionsweise

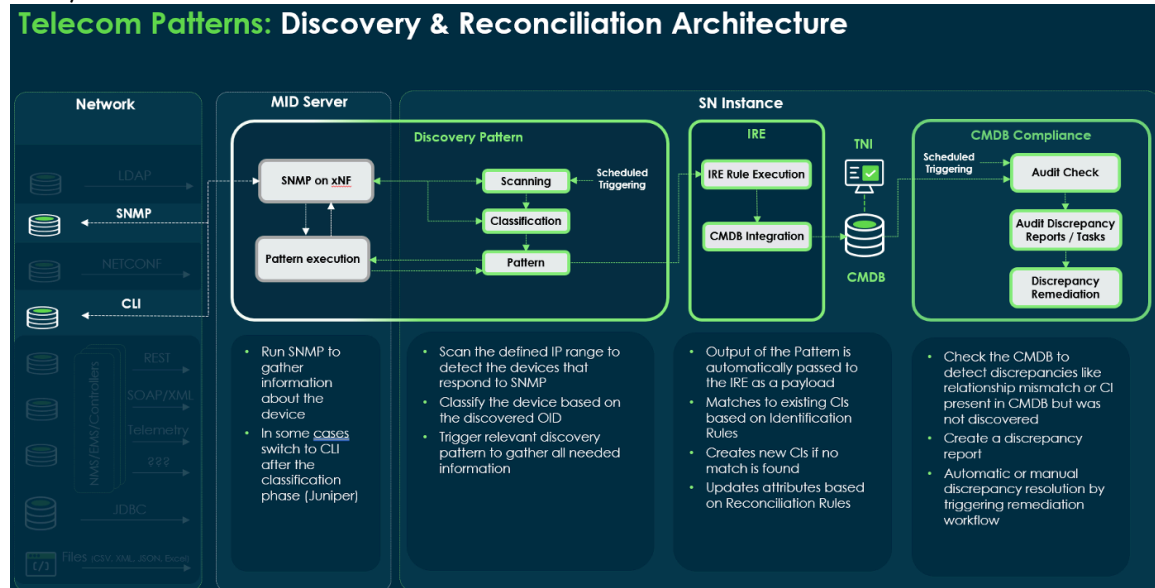
Discovery-Muster für Telekommunikation werden über Horizontal Discovery mit der Nebula Discovery Language (NDL) ausgeführt. Ein Muster ist eine Sequenz von Schritten, die:

- 1.** Stellt eine Verbindung zu einem Zielgerät her.
- 2.** Führt Befehle mit SNMP, CLI oder beidem aus.
- 3.** Extrahiert CI-Attribute und -Beziehungen.
- 4.** Sendet Ergebnisse zum Abgleich und zum Einfügen in CMDB und TNI an IRE.

Die Discovery-Logik folgt dem TNI-Datenmodell, das komplexe CI-Beziehungen (z. B. Karten-auf-Karte-Szenarien) neu strukturiert, um sie an Best Practices für die Telekommunikationsmodellierung anzupassen. Wenn beispielsweise eine untergeordnete Karte innerhalb einer übergeordneten Karte erkannt wird, synthetisiert Telecom Discovery einen Untersteckplatz, um die untergeordnete Karte einzufügen, wodurch eine ungültige Kartenkonfiguration vermieden wird.

Architektur mit Horizontal Discovery- und Telekommunikations-Discovery-Mustern

Die folgende Infografik ist ein Beispiel für die Implementierung von eigenständigen SNMP- oder/und CLI-xNFs.



Horizontale Discovery-Anwendung

Die Anwendung Horizontal Discovery in ServiceNow ist eine vielseitige und hochgradig skalierbare Discovery-Engine, die für den effektiven Betrieb in Netzwerk-, IT- und Cloud-Umgebungen konzipiert ist. Sie erfasst Daten auf mehreren Ebenen, um eine ganzheitliche Ansicht der Infrastruktur zu bieten.

Weitere Informationen finden Sie unter [Horizontal discovery process flow with patterns](#).

Unterstützte Discovery-Muster

Ein Muster ist eine Sequenz von Befehlen, die zum Erkennen von Attributen eines Konfigurationselements (Configuration Item, CI) und seiner ausgehenden Verbindungen konzipiert sind. Telecom Discovery bietet eine Reihe vorkonfigurierter Muster, die eine Vielzahl von Netzwerkelementen abdecken. ServiceNow Bietet mehrere sofort einsatzbereite TSOM-Muster (OOB), einschließlich:

- Telecom-Routermuster: Generische SNMP-basierte Router-Discovery.
- Cisco 7613-Routermuster für Telekommunikation: Für Cisco 7613-Router mit SNMP.
- Telecom Juniper MX SSH-Routermuster: SNMP + CLI-Discovery von Juniper MX-Routern.
- Cisco-Switch-Muster für Telekommunikation: SNMP-basierte Cisco-Switch-Discovery.
- Telekommunikations-Switch-Muster: SNMP-basierte generische Switch-Discovery.

TNI-Entitätserstellung

Wenn Ihre Instanz über verfügt **Telekommunikationsnetzwerkbestand (TNI)** Plugin installiert:

- Jedes erkannte CI führt automatisch zu einem TNI-Entitätsdatensatz.
- Die Ire-Nutzlast enthält die Zuordnung zu beiden cmdb_ci Und tni_Entity Tabellen.

Dies stellt eine nahtlose Ausrichtung zwischen Betriebs- und Bestandssystemen sicher, was für die Auftragserfüllung, die Sicherung und die Netzwerkplanung von entscheidender Bedeutung ist.

MID-Server

MID-Server ist eine Java-Anwendung, die als Windows-Service oder UNIX-Daemon auf einem Server in Ihrem lokalen Netzwerk ausgeführt wird. Die ServiceNow® MID-Server Erleichtert die Kommunikation und Datenübertragung zwischen einer ServiceNow-Instanz und externen Anwendungen, Datenquellen und Services.

Weitere Informationen finden Sie unter [MID Server](#).

Identifizierungs- und Abgleichsmodul (IRE)

IRE bietet ein zentralisiertes Framework zum Identifizieren und Abgleichen von Daten aus mehreren Quellen. Überprüft die Integrität der CMDB und einiger nicht-CMDB-Tabellen, wenn verschiedene Datenquellen zum Erstellen oder Aktualisieren von CI-Datensätzen verwendet werden.

Zugehörige Informationen

[Installieren Sie Horizontal Discovery, und richten Sie Discovery-Muster ein](#)

Telecom-Routermuster

Die ServiceNow® Die Anwendung Telecom Discovery verwendet das Discovery-Muster für Telecom-Router, um SNMP-basierte Router im Netzwerk zu finden. Die Erkennung einiger dieser Ressourcen erfordert die Aktualisierung der Telecommunications Discovery-Muster (TSOM-Muster) aus dem ServiceNow® Speichern.

Telecom Discovery verwendet die Telecom Discovery-Muster, um horizontale Discovery auszuführen. Dieses Telecommunications Discovery-Muster verwendet eine Reihe von SNMP-Anforderungen, um Netzwerkelemente zu finden, zu klassifizieren und zu erkennen.

Das Telecom-Router-Muster ist Teil der Anwendung „Telecommunications Discovery Patterns“ (sn_tsom_patterns), die Teil der TSOM-Sichtbarkeit ist.

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](#).

Voraussetzungen

- Abonnement für TSOM.
- Bestätigen Sie, dass Ihre Netzwerkrouter-Geräte über SNMP-Zugriff verfügen.
- Konfigurieren Sie in der ServiceNow-Instanz SNMP-Anmeldeinformationen. Weitere Informationen finden Sie unter [SNMP support for Discovery](#).
- Informationen zum Einrichten von TSOM-Mustern finden Sie unter [Installieren Sie Horizontal Discovery, und richten Sie Discovery-Muster ein](#).

Betroffene CMDB-CIs und CI-Beziehungen (physische Ebene)

CIs	CI-Beziehungen
IP-Router-CI	IP-Router-Gerät wird durch das IP-Router-CI dargestellt. Tabellenname: cmdb_ci_ip_Router IP-Router-CI enthält Slots oder Netzwerkschnittstellen.
Slot-CI	Slots werden durch das Slot-CI dargestellt. Tabellenname: cmdb_ci_Container_Slot Slot ist im IP-Router enthalten. Slot-CI enthält die Schnittstellenkarte.
Subslot-CI	Subslots werden durch das Subslot-CI dargestellt. Tabellenname: cmdb_ci_Container_subslot Subslot ist im Schnittstellenkarten-CI enthalten. Subslot-CI enthält das Schnittstellenkarten-CI.
Schnittstellenkarten-CI	Verschiedene Arten von Karten werden durch das Schnittstellenkarten-CI dargestellt. Lüfter- und Netzteileinheiten werden auch durch das Karten-CI dargestellt. Tabellenname: cmdb_ci_Interface_Card Schnittstellenkarten sind in Slots oder Subslots enthalten. Schnittstellenkarten können Netzwerkschnittstelle oder Subslots enthalten.
Netzwerkschnittstellen-CI	Jede Art von Netzwerkschnittstelle wird durch das Netzwerkschnittstellen-CI dargestellt. Tabellenname: cmdb_ci_ni_Interface

CI-Beziehungen	CIs
Die Netzwerkschnittstelle ist in der Schnittstellenkarte, dem IP-Router enthalten.	

Cisco 7613-Routermuster Für Telekommunikation

Die ServiceNow® Die Anwendung Telecom Discovery verwendet das Discovery-Muster des Telecom Cisco 7613-Routers, um SNMP-basierte Cisco 7613 im Netzwerk zu finden. Die Erkennung einiger dieser Ressourcen erfordert die Aktualisierung der Telecommunications Discovery-Muster (TSOM-Muster) aus dem ServiceNow® Speichern.

Telecom Discovery verwendet die Telecom Discovery-Muster, um horizontale Discovery auszuführen. Dieses Telecommunications Discovery-Muster verwendet eine Reihe von SNMP-Anforderungen, um Netzwerkelemente zu finden, zu klassifizieren und zu erkennen.

Telecom Cisco 7613 Router Pattern ist Teil der Anwendung Telecom Discovery Patterns (sn_Tsom_patterns), die Teil der TSOM-Transparenz ist.

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](#).

Voraussetzungen

- Abonnement für TSOM.
- Überprüfen Sie, ob Ihre Netzwerkrouter-Geräte über SNMP-Zugriff verfügen.
- Konfigurieren Sie in der ServiceNow-Instanz SNMP-Anmeldeinformationen. Weitere Informationen finden Sie unter [SNMP support for Discovery](#).
- Informationen zum Einrichten von TSOM-Mustern finden Sie unter [Installieren Sie Horizontal Discovery, und richten Sie Discovery-Muster ein](#).

Betroffene CMDB-CIs und CI-Beziehungen (physische Ebene)

CI-Beziehungen	CIs
IP-Router-Gerät wird durch das IP-Router-CI dargestellt. Tabellenname: cmdb_ci_ip_Router IP-Router-CI enthält Slots oder Netzwerkschnittstellen.	IP-Router-CI
Slots werden durch das Slot-CI dargestellt. Tabellenname: cmdb_ci_Container_Slot Slot ist im IP-Router enthalten.	Slot-CI

CI-Beziehungen	CI-Beziehungen
	Slot-CI enthält die Schnittstellenkarte.
Subslot-CI	Subslots werden durch das Subslot-CI dargestellt. Tabellenname: cmdb_ci_Container_subslot Subslot ist im Schnittstellenkarten-CI enthalten. Subslot-CI enthält das Schnittstellenkarten-CI.
Schnittstellenkarten-CI	Verschiedene Arten von Karten werden durch das Schnittstellenkarten-CI dargestellt. Lüfter- und Netzteileneinheiten werden auch durch das Karten-CI dargestellt. Tabellenname: cmdb_ci_Interface_Card Schnittstellenkarten sind in Slots oder Subslots enthalten. Schnittstellenkarten können Netzwerkschnittstelle oder Subslots enthalten.
Netzwerkschnittstellen-CI	Jede Art von Netzwerkschnittstelle wird durch das Netzwerkschnittstellen-CI dargestellt. Tabellenname: cmdb_ci_ni_Interface Die Netzwerkschnittstelle ist in der Schnittstellenkarte, dem IP-Router enthalten.

Telecom Juniper MX SSH-Routermuster

Die ServiceNow® Die Anwendung Telecom Discovery verwendet das Discovery-Muster Telecom Juniper MX SSHRouter, um SNMP- und CLI-basierte Router der Juniper MX-Serie im Netzwerk zu finden. Die Erkennung einiger dieser Ressourcen erfordert die Aktualisierung der Telecommunications Discovery-Muster (TSOM-Muster) aus dem ServiceNow® Speichern.

Telecom Discovery verwendet die Telecom Discovery-Muster, um horizontale Discovery auszuführen. Dieses Telecommunications Discovery-Muster verwendet eine Reihe von SNMP-Anforderungen, um CLI über SSH zu finden und zu klassifizieren, um Netzwerkelemente zu erkennen.

Das Telecom Juniper MX SSH-Routermuster ist Teil der Anwendung „Telecommunications Discovery Patterns“ (sn_Tsom_patterns), die Teil der TSOM-Sichtbarkeit ist.

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](#).

Voraussetzungen

- Abonnement für TSOM.
- Überprüfen Sie, ob Ihre Netzwerkrouter-Geräte über SNMP-Zugriff verfügen.
- Konfigurieren Sie in der ServiceNow-Instanz SNMP-Anmeldeinformationen. Weitere Informationen finden Sie unter [SNMP support for Discovery](#).
- Informationen zum Einrichten von TSOM-Mustern finden Sie unter [Installieren Sie Horizontal Discovery, und richten Sie Discovery-Muster ein](#).

Betroffene CMDB-CIs und CI-Beziehungen (physische Ebene)

CIs	CI-Beziehungen
IP-Router-CI	IP-Router-Gerät wird durch das IP-Router-CI dargestellt. Tabellenname: cmdb_ci_ip_Router IP-Router-CI enthält Slots oder Netzwerkschnittstellen.
Slot-CI	Slots werden durch das Slot-CI dargestellt. Tabellenname: cmdb_ci_Container_Slot Slot ist im IP-Router enthalten. Slot-CI enthält die Schnittstellenkarte.
Subslot-CI	Subslots werden durch das Subslot-CI dargestellt. Tabellenname: cmdb_ci_Container_subslot Subslot ist im Schnittstellenkarten-CI enthalten. Subslot-CI enthält das Schnittstellenkarten-CI.
Schnittstellenkarten-CI	Verschiedene Arten von Karten werden durch das Schnittstellenkarten-CI dargestellt. Lüfter- und Netzteileneinheiten werden auch durch das Karten-CI dargestellt.

Clis	CI-Beziehungen
	Tabellenname: cmdb_ci_Interface_Card Schnittstellenkarten sind in Slots oder Subslots enthalten. Schnittstellenkarten können Netzwerkschnittstelle oder Subslots enthalten.
Netzwerkschnittstellen-CI	Jede Art von Netzwerkschnittstelle wird durch das Netzwerkschnittstellen-CI dargestellt. Tabellenname: cmdb_ci_ni_Interface Die Netzwerkschnittstelle ist in der Schnittstellenkarte, dem IP-Router enthalten.

Cisco-Switch-Muster Für Telekommunikation

Die ServiceNow® Die Telecom Discovery-Anwendung verwendet das Discovery-Muster für Cisco-Switches für Telecom, um SNMP-basierte Cisco-Switches im Netzwerk zu finden. Die Erkennung einiger dieser Ressourcen erfordert die Aktualisierung der Telecommunications Discovery-Muster (TSOM-Muster) aus dem ServiceNow® Speichern.

Telecom Discovery verwendet die Telecom Discovery-Muster, um horizontale Discovery auszuführen. Dieses Telecommunications Discovery-Muster verwendet eine Reihe von SNMP-Anforderungen, um Netzwerkelemente zu finden, zu klassifizieren und zu erkennen.

Das Telecom Cisco Switch-Muster ist Teil der Anwendung „Telecom Discovery Patterns“ (sn_tsom_patterns), die Teil der TSOM-Sichtbarkeit ist.

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](#).

Voraussetzungen

- Abonnement für TSOM.
- Bestätigen Sie, dass Ihre Netzwerkrouter-Geräte über SNMP-Zugriff verfügen.
- Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow®-Instanz. Weitere Informationen finden Sie unter [SNMP support for Discovery](#).
- Informationen zum Einrichten von TSOM-Mustern finden Sie unter [Installieren Sie Horizontal Discovery, und richten Sie Discovery-Muster ein](#).

Betroffene CMDB-CIs und CI-Beziehungen (physische Ebene)

CIs	CI-Beziehungen
IP-Switch-CI	IP-Switch-Gerät wird durch das IP-Switch-CI dargestellt. Tabellenname: cmdb_ci_ip_Switch IP-Switch-CI enthalten Slots oder Netzwerkschnittstellen.
Slot-CI	Slots werden durch das Slot-CI dargestellt. Tabellenname: cmdb_ci_Container_Slot Slot ist im IP-Switch enthalten. Slot-CI enthält die Schnittstellenkarte.
Subslot-CI	Subslots werden durch das Subslot-CI dargestellt. Tabellenname: cmdb_ci_Container_subslot Subslot ist im Schnittstellenkarten-CI enthalten. Subslot-CI enthält das Schnittstellenkarten-CI.
Schnittstellenkarten-CI	Verschiedene Arten von Karten werden durch das Schnittstellenkarten-CI dargestellt. Lüfter- und Netzteileinheiten werden auch durch das Karten-CI dargestellt. Tabellenname: cmdb_ci_Interface_Card Schnittstellenkarten sind in Slots oder Subslots enthalten. Schnittstellenkarten können Netzwerkschnittstelle oder Subslots enthalten.
Netzwerkschnittstellen-CI	Jede Art von Netzwerkschnittstelle wird durch das Netzwerkschnittstellen-CI dargestellt. Tabellenname: cmdb_ci_ni_Interface

CI	CI-Beziehungen
	Die Netzwerkschnittstelle ist in der Schnittstellenkarte, dem IP-Switch enthalten.

Telecom Switch-Muster

Die ServiceNow® Die Anwendung Telecom Discovery verwendet das Discovery-Muster für Telekommunikations-Switches, um SNMP-basierte Telekommunikations-Switches im Netzwerk zu finden. Die Erkennung einiger dieser Ressourcen erfordert die Aktualisierung der Telecommunications Discovery-Muster (TSOM-Muster) aus dem ServiceNow® Speichern.

Telecom Discovery verwendet die Telecom Discovery-Muster, um horizontale Discovery auszuführen. Dieses Telecommunications Discovery-Muster verwendet eine Reihe von SNMP-Anforderungen, um Netzwerkelemente zu finden, zu klassifizieren und zu erkennen.

Das Telecom Switch-Muster ist Teil der Anwendung „Telecommunications Discovery Patterns“ (sn_tsom_patterns), die Teil der TSOM-Sichtbarkeit ist.

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](#).

Voraussetzungen

- Abonnement für TSOM.
- Bestätigen Sie, dass Ihre Netzwerkrouter-Geräte über SNMP-Zugriff verfügen.
- Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow®-Instanz. Weitere Informationen finden Sie unter [SNMP support for Discovery](#).
- Informationen zum Einrichten von TSOM-Mustern finden Sie unter [Installieren Sie Horizontal Discovery, und richten Sie Discovery-Muster ein](#).

Betroffene CMDB-CIs und CI-Beziehungen (physische Ebene)

CI	CI-Beziehungen
IP-Switch-CI	IP-Switch-Gerät wird durch das IP-Switch-CI dargestellt. Tabellenname: cmdb_ci_ip_Switch IP-Switch-CI enthalten Slots oder Netzwerkschnittstellen.
Slot-CI	Slots werden durch das Slot-CI dargestellt. Tabellenname: cmdb_ci_Container_Slot Slot ist im IP-Switch enthalten.

CIs	CI-Beziehungen
	Slot-CI enthält die Schnittstellenkarte.
Subslot-CI	Subslots werden durch das Subslot-CI dargestellt. Tabellenname: cmdb_ci_Container_subslot Subslot ist im Schnittstellenkarten-CI enthalten. Subslot-CI enthält das Schnittstellenkarten-CI.
Schnittstellenkarten-CI	Verschiedene Arten von Karten werden durch das Schnittstellenkarten-CI dargestellt. Lüfter- und Netzteinheiten werden auch durch das Karten-CI dargestellt. Tabellenname: cmdb_ci_Interface_Card Schnittstellenkarten sind in Slots oder Subslots enthalten. Schnittstellenkarten können Netzwerkschnittstelle oder Subslots enthalten.
Netzwerkschnittstellen-CI	Jede Art von Netzwerkschnittstelle wird durch das Netzwerkschnittstellen-CI dargestellt. Tabellenname: cmdb_ci_ni_Interface Die Netzwerkschnittstelle ist in der Schnittstellenkarte, dem IP-Switch enthalten.

Indirekte Discovery mit Service Graph Connectors

Mit der ServiceNow Telecom Discovery mit Service Graph Connectors (SGCs) können Sie Netzwerkinfrastrukturdaten aus externen Managementsystemen wie EMS-, NMS- und SDN-Controllern nahtlos in die Configuration Management Database (CMDB) integrieren.

Dieser Ansatz hilft Kommunikationsservice Providern (CSPs), einen aktuellen und genauen Überblick über ihre Telekommunikationsnetzwerkressourcen, -Services und -Konfigurationen verschiedener Anbieter zu erhalten.

Durch die Nutzung vordefinierter Connectors und robuster Datentransformationstools können Sie Ihren Bestand domänenübergreifend vereinheitlichen und sicherstellen, dass CMDB und TNI (Telecom Network Inventory) Echtzeiteinblicke in das Netzwerk widerspiegeln, die an Ihrem Telekommunikationsdatenmodell ausgerichtet sind.

i Hinweis:

Telecom Service Graph Connectors sind Teil des TSOM-Transparenzabonnements und erweitern die Fähigkeiten des Standard-Service Graph Connector-Frameworks.

Service Graph Connector-Übersicht

Mit Telecom SGC können Sie:

- Erfassen Sie Daten von EMS/NMS/Controllern mithilfe von REST APIs nach Norden.
- Füllen Sie CMDB- und TNI-Datensätze automatisch mit angereicherten, Telekommunikationsdaten aus und aktualisieren Sie sie.
- Synchronisieren Sie eingehende Daten mit vorhandenen CI-Datensätzen mithilfe der Identification and Reconciliation Engine (IRE).
- Generieren Sie TNI-Entitätsdatensätze automatisch, wenn das TNI-Plugin installiert wird.
- Unterstützen Sie die Erkennung und Behebung von Diskrepanzen im Rahmen der Identifizierung und des Abgleichs von Telekommunikationsdiskrepanzen.
- Verwenden Sie Low-Code-Tools, um Ihre Integrationen End-to-End zu konfigurieren, zu testen und zu verwalten

Architekturübersicht

Telecom Service Graph Connectors basieren auf einer modularen und skalierbaren Architektur:

Schlüsselkomponenten von Service Graph Connector

Komponente	Rolle
Service Graph Connector	Definiert die Integrationslogik zum Extrahieren und Bereitstellen von Daten aus EMS/NMS-Systemen (z. B. Nokia Altiplano oder Nokia NSP).
MID-Server	Fungiert als sichere Brücke zwischen Ihrer ServiceNow-Instanz und dem externen Netzwerksystem. Weitere Informationen finden Sie unter IntegrationHub ETL  .
IntegrationHub ETL (3,2)	Bietet eine geführte UI zum Erstellen, Testen und Verwalten von ETL-Transformationszuordnungen. Weitere Informationen finden Sie unter MID Server  .
Robuste Transformations-Engine (RTE)	Wandelt bereitgestellte Quelldaten mithilfe einer definierten ETL-Logik in CMDB-konforme Datensätze um. Weitere Informationen finden Sie unter Create a robust import set transformer  .
Identifizierungs- und Abgleichsmodul (IRE)	Stellt die Datenkonsistenz sicher und verhindert Duplikate, indem CIs identifiziert und abgeglichen werden.

Schlüsselkomponenten von Service Graph Connector (Fortsetzung)

Komponente	Rolle
	Weitere Informationen finden Sie im Abschnitt CMDB Identification and Reconciliation (IRE) ↗ .
CMDB/TNI	Speichert strukturierte, genaue Telekommunikationsinfrastrukturdaten für Transparenz und nachgelagerte Prozesse.

Unterstützte Service Graph Connectors

- Nokia Altiplano SGC (sn_sgc_altiplano_Connector): Wird über REST APIs in den SDN-Controller des Nokia Altiplano Access Network integriert.
- [store-future: BEGIN review]Nokia NSP SGC: Wird in die Nokia Network Services Platform (NSP) integriert, um Transportnetzwerkdaten über REST APIs zu erfassen.[End]

i Hinweis:

Der Connector kann mit IT- und Cloud Service Graph Connectors koexistieren (z. B. für Server, Überwachungstools, IoT usw.).

Hauptvorteile

- Schnelle Amortisierungszeit: Verwenden Sie vordefinierte, unterstützte Connectors, die eine minimale Konfiguration erfordern.
- Unterstützung mehrerer Anbieter: Integration mit verschiedenen Verwaltungsplattformen in Zugriffs-, Kern- und Transportnetzwerken.
- Modellorientierte Transparenz: Stellen Sie sicher, dass die für die Telekommunikation spezifische Hierarchie und Beziehungen in der CMDB genau modelliert werden.
- Diskrepanzerkennung bereit: Geben Sie Netzwerkdaten direkt in die Identifizierung und den Abgleich von Telekommunikationsdiskrepanzen für CMDB-Compliance ein.
- Skalierbare Integration: Nutzen Sie das bewährte Integrations-Framework von ServiceNow, das für Leistung und Erweiterbarkeit entwickelt wurde.

TNI-Datenmodell (Telecom Network Inventory)

Telecom-SGCs enthalten Logik, um die Kompatibilität mit dem TNI-Datenmodell (Telecom Network Inventory) sicherzustellen:

- Wenn das TNI-Plugin installiert ist, enthält jedes erkannte Netzwerkelement automatisch einen TNI-Entitätsdatensatz.
- A `tni_Entity` Wird zusammen mit den entsprechenden erstellt `cmdb_ci` Datensatz mit systemgenerierten Nutzlastzuordnungen (z. B. `Inventory_category`).
- Dadurch wird die Konsistenz über Betriebs- und Planungssysteme hinweg sichergestellt.

Wenn TNI installiert ist, wird der IRE-Nutzlast für jedes Element eine Nutzlast wie die folgende hinzugefügt (mit „Inventory_category“, die basierend auf dem className ausgefüllt wird):

```
related = [{
  "className": "tni_entity",
  "values": {
    "inventory_category": ""
  }
}];
```

Daher befindet sich das erkannte CI sowohl in den Tabellen „cmdb_ci“ als auch „tni_Entity“.

Zugehörige Informationen

[Telecom Discovery über Nokia Altiplano](#)

Telecom Discovery über Nokia Altiplano

Der Service Graph Connector für Nokia Altiplano bietet eine Telekom-fähige Integration, die Echtzeitnetzwerkbestand aus dem Nokia Altiplano Access Network SDN-Controller in Ihre ServiceNow CMDB überführt.

Dieser Connector wurde für Service Provider und Telekommunikationsunternehmen entwickelt und ermöglicht vollständige Transparenz, Kontrolle und Synchronisierung Ihrer physischen und logischen Netzwerkinfrastruktur. Diese Integration verwendet REST-APIs und einen MID-Server, um eine auf das Telekommunikationsmodell ausgerichtete Ansicht Ihres Netzwerks bereitzustellen, die genauere Servicemodelle, Bestandsverwaltung und Betriebseffizienz ermöglicht.

Hauptvorteile

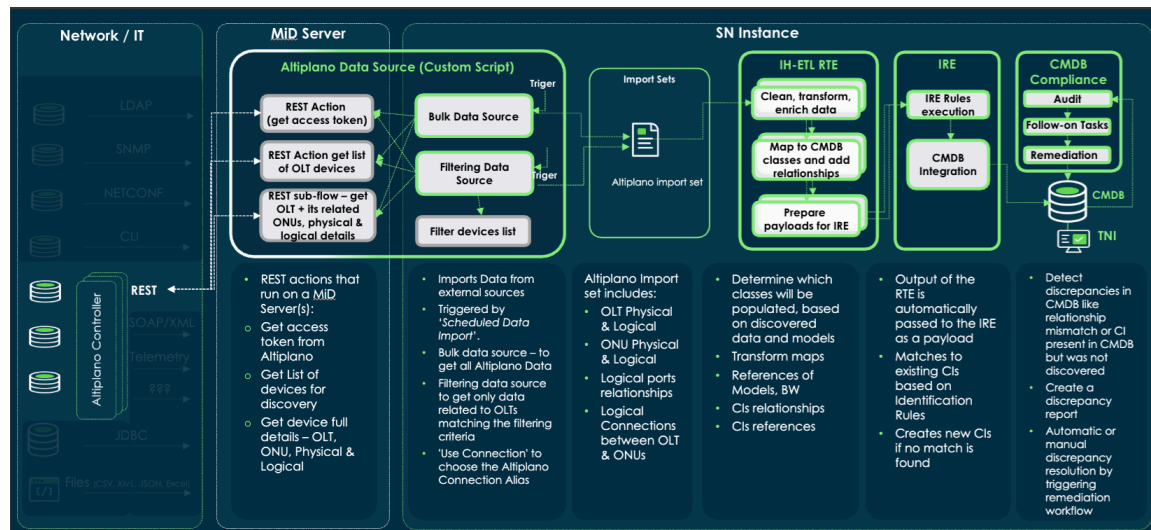
- **Genaue Bestandssynchronisierung:** Füllen Sie die CMDB mithilfe einer sicheren, REST API-basierten Erfassung automatisch mit dem aktuellen physischen und logischen Bestand von Nokia Altiplano aus. Dies umfasst OLTS, ONUS/ONTs, Schnittstellenkarten, Ports, Steckplätze, und logische Verbindungen.
- **Telekom-fähige CI-Modellierung:** Modellieren Sie Ihre Netzwerkinfrastruktur in einem Telekom-orientierten Format mit speziell entwickelten CI-Klassen und -Beziehungen. Der Connector stellt die genaue Darstellung von Geräten und ihren Abhängigkeiten sicher und spiegelt Ihre tatsächliche Netzwerktopologie wider.
- **Vereinfachtes und geführtes Setup:** Reduzieren Sie die Amortisierungszeit mit einem integrierten geführten Setup, das Sie mühelos durch die Verbindungskonfiguration, die Datenquellenverwaltung und die Importplanung führt.
- **Flexible Discovery-Optionen:** Wählen Sie aus, wie und wann die Discovery basierend auf Ihren Anforderungen ausgeführt werden soll – ob es sich um vollständige Massenlasten, gezielte gefilterte Discovery oder phasenbasierte OLT-Importe handelt. Wenden Sie anwenderdefinierte Filter nach Geräte-IP oder -Name an.
- **Unterstützung für mehrere Instanzen:** Skalieren Sie mühelos, indem Sie mehrere Altiplano-Instanzen unabhängig Onboarding durchführen. Konfigurieren Sie Verbindungsaliasse, und definieren Sie Importzeitpläne pro Instanz, um vollständige operative Flexibilität zu gewährleisten.

Hinweis:

Die unterstützte Mindestversion des Nokia Altiplano-Controllers ist 24.6. Eine allgemeine Übersicht über die Service Graph Connector-Technologie finden Sie unter [Getting started with Service Graph Connectors](#) .

Nokia Altiplano SGC-Architektur

Die folgende Infografik hilft Ihnen, die Architektur des Nokia Altiplano Service Graph Connector zu verstehen.



Anwendungsfälle

Im Folgenden finden Sie Beispiele für die Verwendung des Nokia Altiplano Service Graph Connector:

- Erfassen und strukturieren Sie Netzwerkdaten automatisch in der CMDB von ServiceNow für physische und logische Netzwerkelemente: Dadurch wird eine CMDB-Ansicht erstellt, die auf das Telekommunikationsmodell ausgerichtet ist, die Ihre Live-Netzwerkumgebung widerspiegelt.
 - Physische Komponenten: OLTs, ONUs/ONTs, Slots, Subslots, Karten, und Ports
 - Logische Komponenten: Logische Ports, VLANs, Link Aggregation Groups (LAGs) und logische Pfade zwischen Geräten
- Bewahren Sie die Integrität Ihrer Netzwerkdaten mit einem geplanten, automatisierten Abgleich auf, der:
 - Erkennt Änderungen in Echtzeit und reagiert darauf
 - Verhindert Datenabweichungen oder veraltete Datensätze
 - Unterstützt operative Prozesse wie Servicesicherung, Auftragserfüllung und Netzwerkplanung
- Entdecken Sie über die physische Infrastruktur hinaus, indem Sie logische Konnektivität in ServiceNow erfassen und verwalten:
 - Identifizieren und modellieren Sie logische Ports, LAGs und logische Pfade wie PON- und VLAN-Verbindungen
 - Verknüpfen Sie logische CIs mit physischen Komponenten mithilfe von über- und untergeordneten Beziehungen und Mitgliedern von
 - Verbessern Sie Diagnose, Auswirkungsanalyse und Servicemodellierung, indem Sie logische End-to-End-Topologien visualisieren
- Nutzen Sie das integrierte ETL-Framework (Extract, Transform, Load) von ServiceNow, um die Integration zu vereinfachen und zu beschleunigen:

Automatische Übersetzung

- Vordefinierte Transformationszuordnungen und CI-Klassendefinitionen reduzieren den Entwicklungsaufwand
- Verwenden Sie vorhandene CMDB-Strukturen erneut, um die Anpassung zu minimieren
- Integrieren Sie schnell neue Altiplano-Instanzen, und skalieren Sie die gesamte Netzwerkinfrastruktur

Wichtige Fähigkeiten und Komponenten

Wichtige Fähigkeiten und Komponenten

Fähigkeit	Beschreibung	Unterstützende Komponente
Telekom-fähige CMDB-Modellierung	Ordnet physischen und logischen Altiplano-Bestand (OLT, ONU/ONT, Ports, Steckplätze, Karten, Schnittstellen) in CMDB mit Telekommunikations-spezifischen CI-Klassen und -Beziehungen.	RTE-, IRE-, CMDB-TABELLEN (cmdb_ci_Optical_line_Terminal, cmdb_ci_Optical_Network_Terminal, Usw.)
Automatisierte Datenerfassung	Ruft den Gerätebestand von Nokia Altiplano über REST APIs mit sicheren, geplanten Importen ab.	MID-Server, Datenquellen (SGC-Nokia Altiplano Massen/gefilterte Discovery)
Anwenderdefinierte Discovery-Steuerung	Wählen Sie „nur OLT“ aus, oder fügen Sie ONU-Daten ein, wenden Sie Filter nach IP oder Name an, und planen Sie Aufgaben pro Instanz.	Importzeitpläne, Systemeigenschaften (sn_sgc_altiplano.enable_onu_Discovery, Usw.)
Unterstützung für mehrere Instanzen	Konfigurieren und verwalten Sie Discovery unabhängig für mehrere Altiplano-Controller.	Verbindungsaliasse, Anmeldeinformationsaliasse
Parallele Datenverarbeitung	Verbessern Sie die Leistung, indem Sie gleichzeitige Datenquellenaufträge für große Datensätze ausführen.	Systemeigenschaft: sn_sgc_altiplano.parallel_number_of_Data_Sources, Aktivieren Sie Das Parallele Laden
Geführte Konfiguration	Vereinfacht das Setup mit einer schrittweisen Schnittstelle zum Erstellen von Verbindungen, Anmeldeinformationen und Aufträgen.	UI für geführtes Setup (Navigation: Alle > Service Graph Connectors > Nokia Altiplano > Setup)
Modellgesteuerte CI-Klassifizierung	Gleicht erkannte Geräte mit Modellen ab und weist die richtige CI-Klasse (OLT, ONU, ONT) zu, oder greift auf Netzwerkgerät zurück.	Modelltabellen, Systemeigenschaft: sn_sgc_altiplano.onu_ci_class
Beziehung	Stellt Telekommunikations-spezifische CI-Beziehungen her (z. B. Mitglied von, enthält, logischer Pfad).	Ire, CI für logische Verbindungen (cmdb_ci_ni_logical_path)
Dashboards und Überwachung	Zeigen Sie Status, Ergebnisse und Fehler jeder Ausführung an;	Integration Commons für CMDB-Dashboard

Automatische Übersetzung

Wichtige Fähigkeiten und Komponenten (Fortsetzung)

Fähigkeit	Beschreibung	Unterstützende Komponente
	filtern Sie nach Connector oder Zeitrahmen.	
Skalierbare und wiederverwendbare Architektur	Entkoppelte Datenquellen, Transformation und CI-Abgleich für einfache Skalierung und Anpassung.	Importsätze (sn_sgc_altiplano_tsom_Inventory), Transformationszuordnungen, Systemeigenschaften

Dashboard CMDB-Integrationen

Die Store-App „Integration Commons for CMDB“ bietet ein Dashboard mit einer zentralen Ansicht des Status, der Verarbeitungsergebnisse und der Verarbeitungsfehler aller installierten Service Graph Connectors. Sie können Metriken für alle Integrationsausführungen anzeigen. Sie können die Ansicht nach einer bestimmten Integration, einer bestimmten Zeitdauer oder einer bestimmten Integrationsausführung filtern. Weitere Informationen zur Überwachung von Integrationen im Dashboard „CMDB-Integrationen“ finden Sie unter [Integration Commons for CMDB](#) .

Zugehörige Informationen

[Konfigurieren des Nokia Altiplano Service Graph Connector](#)

[Mit Nokia Altiplano installierte Systemkomponenten](#)

[store-future: BEGIN review]

Telekommunikations-Discovery über Nokia NSP

Der Service Graph Connector für Nokia NSP bietet eine Telekom-fähige Integration, die Echtzeitnetzwerkbestand aus dem Nokia NSP Access Network SDN Controller in Ihre ServiceNow CMDB überführt.

Dieser Connector wurde für Service Provider und Telekommunikationsunternehmen entwickelt und ermöglicht vollständige Transparenz, Kontrolle und Synchronisierung Ihrer physischen und logischen Netzwerkinfrastruktur. Diese Integration verwendet REST-APIs und einen MID-Server, um eine auf das Telekommunikationsmodell ausgerichtete Ansicht Ihres Netzwerks bereitzustellen, die genauere Servicemodelle, Bestandsverwaltung und Betriebseffizienz ermöglicht.

Hauptvorteile

- **Genaue Bestandssynchronisierung:** Füllen Sie die CMDB mithilfe einer sicheren, REST API-basierten Erfassung automatisch mit aktuellem physischen und logischen Bestand aus Nokia NSP aus. Dies umfasst IP-Router, Schnittstellenkarten, Ports, Steckplätze und logische Schnittstellen (ENET, lag), logische Verbindungen und Netzwerktopologie.
- **Telekom-fähige CI-Modellierung:** Modellieren Sie Ihre Netzwerkinfrastruktur in einem Telekom-orientierten Format mit speziell entwickelten CI-Klassen und -Beziehungen. Der Connector stellt die genaue Darstellung von Geräten und ihren Abhängigkeiten sicher und spiegelt Ihre tatsächliche Netzwerktopologie wider.
- **Vereinfachtes und geführtes Setup:** Reduzieren Sie die Amortisierungszeit mit einem integrierten geführten Setup, das Sie mühelos durch die Verbindungskonfiguration, die Datenquellenverwaltung und die Importplanung führt.

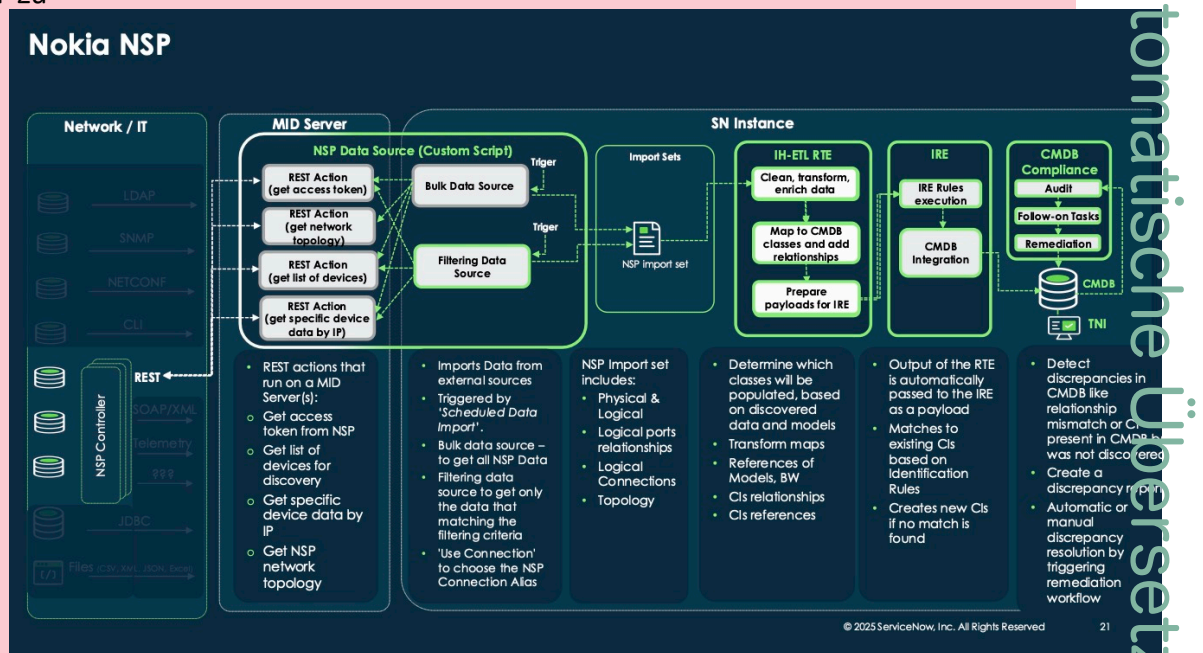
- Flexible Discovery-Optionen: Wählen Sie aus, wie und wann die Discovery basierend auf Ihren Anforderungen ausgeführt werden soll – unabhängig davon, ob es sich um vollständige Massenlasten oder gezielte gefilterte Discovery handelt. Wenden Sie anwenderdefinierte Filter nach Geräte-IP oder -Name an.
- Unterstützung für mehrere Instanzen: Mühelose Skalierung durch unabhängiges Onboarding mehrerer NSP-Instanzen. Konfigurieren Sie Verbindungsaliasse, und definieren Sie Importzeitpläne pro Instanz, um vollständige operative Flexibilität zu gewährleisten.

Hinweis:

Eine allgemeine Übersicht über die Service Graph Connector-Technologie finden Sie unter [Getting started with Service Graph Connectors](#).

Nokia Altiplano SGC-Architektur

Die folgende Infografik hilft Ihnen, die Architektur des Nokia Altiplano Service Graph Connector zu



verstehen.

Anwendungsfälle

Im Folgenden finden Sie Beispiele für die Verwendung des Nokia NSP Service Graph Connector:

- Erfassen und strukturieren Sie Netzwerkdaten automatisch in der CMDB von ServiceNow für physische und logische Netzwerkelemente: Dadurch wird eine CMDB-Ansicht erstellt, die auf das Telekommunikationsmodell ausgerichtet ist, die Ihre Live-Netzwerkumgebung widerspiegelt.
 - Physische Komponenten: IP-Router, Slots, Subslots, Karten und Ports
 - Logische Komponenten: Logische Ports, Link Aggregation Groups (LAGs) und logische Pfade zwischen Geräten, Netzwerktopologie
- Bewahren Sie die Integrität Ihrer Netzwerkdaten mit einem geplanten, automatisierten Abgleich auf, der:

- Erkennt Änderungen in Echtzeit und reagiert darauf
- Verhindert Datenabweichungen oder veraltete Datensätze
- Unterstützt operative Prozesse wie Servicesicherung, Auftragserfüllung und Netzwerkplanung
- Entdecken Sie über die physische Infrastruktur hinaus, indem Sie logische Konnektivität in ServiceNow erfassen und verwalten:
 - Identifizieren und modellieren Sie logische Ports, LAGs und logische Pfade wie ENET- und lag-Verbindungen
 - Verknüpfen Sie logische CIs mit physischen Komponenten mithilfe von über- und untergeordneten Beziehungen und Mitgliedern von
 - Verbessern Sie Diagnose, Auswirkungsanalyse und Servicemodellierung, indem Sie logische End-to-End-Topologien visualisieren
- Nutzen Sie das integrierte ETL-Framework (Extract, Transform, Load) von ServiceNow, um die Integration zu vereinfachen und zu beschleunigen:
 - Vordefinierte Transformationszuordnungen und CI-Klassendefinitionen reduzieren den Entwicklungsaufwand
 - Verwenden Sie vorhandene CMDB-Strukturen erneut, um die Anpassung zu minimieren
 - Integrieren Sie schnell neue NSP-Instanzen, und skalieren Sie die gesamte Netzwerkinfrastruktur

Wichtige Fähigkeiten und Komponenten

Wichtige Fähigkeiten und Komponenten

Fähigkeit	Beschreibung	Unterstützende Komponente
Telekom-fähige CMDB-Modellierung	Ordnet den physischen und logischen NSP-Bestand (IP-Router, Ports, Steckplätze, Karten, Schnittstellen) der CMDB mit Telekommunikations-spezifischen CI-Klassen und -Beziehungen zu.	RTE-, IRE-, CMDB-Tabellen (cmdb_ci_ip_Router usw.)
Automatisierte Datenerfassung	Ruft den Gerätebestand von Nokia NSP über REST APIs mit sicheren, geplanten Importen ab.	MID-Server, Datenquellen (SGC-Nokia NSP Massen/gefilterte Discovery)
Anwenderdefinierte Discovery-Steuerung	Wenden Sie Filter nach IP oder Name an, und planen Sie Aufgaben pro Instanz.	Importzeitpläne, Systemeigenschaften
Unterstützung für mehrere Instanzen	Konfigurieren und verwalten Sie Discovery unabhängig für mehrere NSP-Controller.	Verbindungsaliasse, Anmeldeinformationsaliasse
Parallele Datenverarbeitung	Verbessern Sie die Leistung, indem Sie gleichzeitige Datenquellenaufträge für große Datensätze ausführen.	Systemeigenschaft: <code>sn_sgc_nsp.parallelNumberOfDataSourceJobs</code> , Aktivieren Sie Das Parallele Laden
Geführte Konfiguration	Vereinfacht das Setup mit einer schrittweisen Schnittstelle zum Erstellen von Verbindungen,	UI für geführtes Setup (Navigation: Alle > Service Graph Connectors > Nokia NSP > Setup)

Wichtige Fähigkeiten und Komponenten (Fortsetzung)

Fähigkeit	Beschreibung	Unterstützende Komponente
	Anmeldeinformationen und Aufträgen.	
Modellgesteuerte CI-Klassifizierung	Gleicht erkannte Geräte mit Modellen ab und weist die richtige CI-Klasse (IP-Router) zu, oder greift auf Netzwerkgerät zurück.	Modelltabellen
Beziehung	Stellt Telekommunikations-spezifische CI-Beziehungen her (z. B. Mitglied von, enthält, logischer Pfad).	IRE, CI für logische Verbindungen (cmdb_ci_ni_logical_path)
Dashboards und Überwachung	Zeigen Sie Status, Ergebnisse und Fehler jeder Ausführung an; filtern Sie nach Connector oder Zeitrahmen.	Integration Commons für CMDB-Dashboard
Skalierbare und wiederverwendbare Architektur	Entkoppelte Datenquellen, Transformation und CI-Abgleich für einfache Skalierung und Anpassung.	Importsätze (sn_sgc_nsp_Tsom_Inventory), Transformationszuordnungen, Systemeigenschaften

Dashboard CMDB-Integrationen

Die Store-App „Integration Commons for CMDB“ bietet ein Dashboard mit einer zentralen Ansicht des Status, der Verarbeitungsergebnisse und der Verarbeitungsfehler aller installierten Service Graph Connectors. Sie können Metriken für alle Integrationsausführungen anzeigen. Sie können die Ansicht nach einer bestimmten Integration, einer bestimmten Zeitdauer oder einer bestimmten Integrationsausführung filtern. Weitere Informationen zur Überwachung von Integrationen im Dashboard „CMDB-Integrationen“ finden Sie unter [Integration Commons for CMDB](#) .

Zugehörige Informationen

[Konfigurieren des Nokia NSP-Service Graph-Connectors](#)

[End]

Identifizierung und Abgleich von Telekommunikationsdiskrepanzen

Verwenden Sie die Funktion „Identifizierung und Abgleich von Telekommunikationsdiskrepanzen“, um Ihre CMDB oder Telecommunications Network Inventory (TNI) mit Ihrem Live-Telekommunikationsnetzwerk zu synchronisieren. Durch das kontinuierliche Auditieren und Vergleichen erkannter Daten mit Bestandsdatensätzen hilft diese Lösung Ihnen, Inkonsistenzen zu erkennen, zu klassifizieren und automatisch zu beheben, bevor sie sich auf Servicequalität, -Sicherheit oder -Erfüllungsprozesse auswirken.

Identifizierung und Abgleich von Telekommunikationsdiskrepanzen ist eine Telekommunikationsspezifische Fähigkeit, die im Plugin „TSOM-Transparenz“ enthalten ist. Es hilft, die Integrität Ihres Netzwerkbestands zu bestätigen, indem Diskrepanzen zwischen Echtzeitnetzwerkdaten (von Discovery oder externen Systemen) und Bestandsdatensätzen identifiziert werden, die in der CMDB oder TNI gespeichert sind.

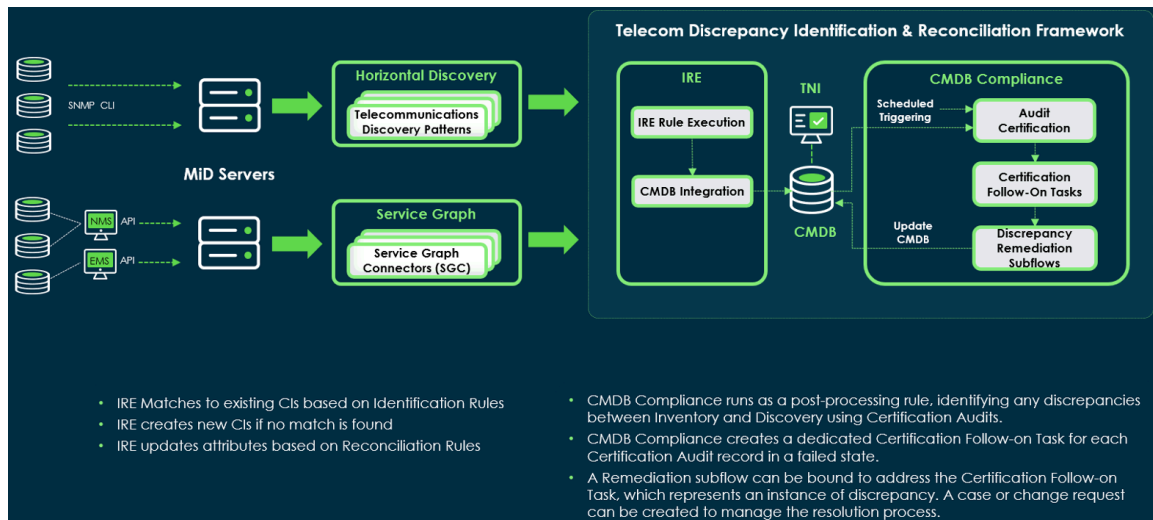
Diese Lösung verwendet:

- Audits der CMDB-Compliance-Zertifizierung zur Erkennung von Anomalien.
- Folgeaufgaben zum Protokollieren und Nachverfolgen von Problemen.
- Automatisierte Nachbesserungs-Subflows zur Behebung von Diskrepanzen.

i Hinweis:

Durch eine genaue Bestandsaufnahme können Sie Automatisierung, Servicefehler reduzieren und die Compliance mit gesetzlichen Vorschriften unterstützen. Es ist auch eine grundlegende Komponente des Autonomous Network Operations (ANO)-Frameworks des TM Forums.

Architektur für Identifizierung und Abgleich von Telekommunikationsdiskrepanzen



Schlüsselfunktionen

Wichtige Funktionen der Identifizierung und des Abgleichs von Telekommunikationsdiskrepanzen

Funktion	Beschreibung
Kontinuierliche Auditprüfungen	Vergleicht erkannte Netzwerkdaten mithilfe von Zertifizierungs-Audits mit Bestandsdatensätzen.
Diskrepanzerkennung	Identifiziert CIs, die in Bezug auf Hierarchie- oder Attributwerte fehlen, falsch konfiguriert oder falsch ausgerichtet sind.
Generierung von Folgeaufgaben	Erstellt automatisch Aufgaben für jede Diskrepanz, um Nachverfolgung und Korrektur zu ermöglichen.
Automatisierte Korrektur	Verwendet Flow Designer-Subflows, um Probleme wie veraltete CIs, ungültige Beziehungen und fehlende Discovery-Daten zu lösen.

Funktionsweise der Identifizierung und des Abgleichs von Telekommunikationsdiskrepanzen

Sobald der Discovery-Prozess abgeschlossen ist, identifiziert das CMDB-Compliance-Framework mithilfe geplanter oder bedarfsgesteuerter Compliance-Audits Abweichungen zwischen erkannten Daten und Bestandsdatensätzen.

- Compliance-Audits: Vergleichen Sie erkannte Netzwerkdaten mit CMDB-Bestandsdatensätzen, um Inkonsistenzen zu erkennen.
- Folgeaufgaben: Automatisch für jedes fehlgeschlagene Audit generiert. Diese Aufgaben dokumentieren und kategorisieren die identifizierten Diskrepanzen.
- Korrektur-Subflows: Von Folgeaufgaben gestartet, um Diskrepanzen durch Aktualisieren, Außerbetriebnahme oder Neuausrichtung von Konfigurationselementen (CIs) zu beheben.

i Hinweis:

Weitere Informationen finden Sie unter [Diskrepanzidentifizierung: Arten von Diskrepanzen](#).

Identifizierung und Abgleich von CMDB-Compliance und Telekommunikationsdiskrepanz

CMDB-Compliance ist ein Toolset, mit dem Administratoren CMDB-Daten auf Richtigkeit zertifizieren und bei Compliance-Audits erkannte Diskrepanzen identifizieren können. Es kann auch automatisch Folgeaufgaben für fehlgeschlagene Audit-Datensätze generieren und zuweisen, die als Aufgaben dienen, um einen entsprechenden Korrektur-Subflow auszulösen, um Diskrepanzen zu korrigieren. CMDB-Compliance-Audits bilden die Grundlage für die Identifizierung und den Abgleich von Telekommunikationsdiskrepanzen.

- CMDB-Compliance führt Audits als Nachverarbeitungsregel aus, um Anomalien (Diskrepanzen) in der CMDB zu identifizieren.
- CMDB-Compliance erstellt eine Folgeaufgabe für jeden Audit-Datensatz mit einem Status „Fehlgeschlagen“ (der Status „Fehlgeschlagen“ ist das Ergebnis eines Audits, das eine Anomalie oder Diskrepanz in der CMDB ermittelt). Ein Korrektur-Flow kann für jede Folgeaufgabe entworfen und ausgelöst werden, um die Diskrepanz zu beheben und zu beheben.

Die Logik für Identifizierung und Abgleich von Telekommunikationsdiskrepanzen sowie die Beispiel-Subflows für die Korrektur werden automatisch mit dem Plugin „TSOM-Transparenz“ verwendet. Weitere Informationen zum allgemeinen Toolset für CMDB-Compliance finden Sie unter [CMDB Compliance](#).

Diskrepanzidentifizierungsszenarien (mithilfe von Compliance-Audits)

Die Diskrepanzidentifizierung in TSOM-Transparenz basiert auf CMDB-Compliance (Zertifizierungs-Audits) und hat sie erweitert, indem eine spezifische Logik hinzugefügt wurde, die Modellbeziehungen und Informationen verwendet, um Nichtübereinstimmungen zu identifizieren. Zur Unterstützung der Korrektur generiert das System bestimmte Abgleichsaufgabentypen für jedes gefundene Problem, z. B.:

- Diskrepanz bei belegten Slots
- Das letzte Discovery-Datum ist nicht festgelegt
- Letztes Discovery-Datum liegt nicht innerhalb des konfigurierten Schwellenwerts
- Modellbeziehungen nicht definiert
- CI-Modell nicht gefunden
- Falsche Anzahl von Beziehungen
- Verweis auf logische Schnittstelle nicht gefunden

Sie können die folgenden Audits verwenden, um die Diskrepanzen in den erkannten physischen und logischen Entitäten zu identifizieren

- Audit Der Telekommunikationsdiskrepanz
- Audit Der Diskrepanz Logischer Verbindungen Der Telekommunikation
- Audit Der Topologie Der Telekommunikationsnetzwerke-Diskrepanz

i Hinweis:

Weitere Informationen zu den allgemeinen Compliance-Audits finden Sie unter [Certification audits](#) .

Automatisierung und UI-Integration

- Jedes fehlgeschlagene Audit erstellt automatisch eine Folgeaufgabe.
- Aufgaben können vordefinierte oder anwenderdefinierte Subflows mit Flow Designer auslösen.
- Die manuelle Korrektur kann über die UI-Aktionsschaltfläche „Nachbesserung“ im Aufgabenformular initiiert werden.
- Korrekturschritte werden in Arbeitsnotizen aufgezeichnet, um Sichtbarkeit und Auditing zu gewährleisten.

i Hinweis:

Weitere Informationen zum Erstellen eines Subflows finden Sie unter [Building subflows](#) .

Folgeaufgabentypen, die für Datensätze mit fehlgeschlagenen Audit-Ergebnissen erstellt wurden

Die folgenden Diskrepanztypen (Audit-Ergebnisse) können für übergeordnete CI und untergeordnete CIs für jeden Beziehungsdatensatz in der CI-Beziehungstabelle (cmdb_rel_ci) gefunden werden, die den Bedingungen entspricht, und die folgenden Folgeaufgaben können für jedes der fehlgeschlagenen Audit-Ergebnisse erstellt werden:

1. Das letzte Discovery-Datum wurde nicht festgelegt – wird generiert, wenn das Feld für das letzte Discovery-Datum im CI fehlt.
2. Das letzte Discovery-Datum, das nicht innerhalb des konfigurierten Schwellenwerts liegt – wird generiert, wenn die Differenz im letzten Discovery-Datum-Feldwert zwischen einem übergeordneten CI und einem untergeordneten CI mehr als 2,5 Tage beträgt. Beispielsweise ist sie standardmäßig in der Systemeigenschaft `sn_tsom_core.discovered_date.diff.threshold.in.days` auf 2,5 Tage festgelegt und kann geändert werden.
3. CI-Modell nicht gefunden –(das Feld „Modell-ID“ ist nicht festgelegt, oder die Daten sind ungültig). Wird generiert, wenn kein entsprechendes CI-Modell gefunden wird. Wenn kein CI-Modell gefunden wird, sind die nächsten Validierungen (4–6) irrelevant, da sie auf CI-Modellen basieren. Wenn ein CI-Modell gefunden wird, wird das Audit mit den nächsten Validierungen (4–6) fortgesetzt.
4. Diskrepanz für belegte Slots: Wird generiert, wenn eine Karte eine falsche Anzahl von Slots belegt.
5. Modellbeziehungen nicht definiert – relevant nur, wenn TNI installiert ist. Wird generiert, wenn das Audit keine Beziehung zwischen übergeordneten und untergeordneten CI-Modellen in der Tabelle „Netzwerkmodellbeziehungen“ finden kann.
6. Falsche Anzahl von Beziehungen – relevant nur, wenn TNI installiert ist. Wird generiert, wenn das Audit feststellt, dass die Anzahl der erkannten untergeordneten CI-Datensätze die maximale Anzahl des entsprechenden übergeordneten CI-Datensatzes im Feld „Anzahl der Modellbeziehungen“ in der Tabelle „Netzwerkmodell-Beziehung“ überschreitet.

7. Falsche Anzahl von Beziehungen – wird während des Audits für logische Verbindungsdiskrepanz generiert, wenn eine logische Schnittstelle mehr als einer logischen Verbindung zugeordnet ist, was gegen die erwartete eins-zu-eins-Zuordnung verstößt.
8. Falsche Anzahl von Beziehungen – wird während des Audits der Netzwerktopologie-Diskrepanz generiert, wenn ein Netzwerktopologiedatensatz die erforderlichen Beziehungskriterien nicht erfüllt. Speziell:
 - Der Datensatz muss mindestens eine Beziehung „enthält:enthalten in“ mit einem Geräte-CI aufweisen.
 - Der Datensatz muss auch mindestens eine Beziehung „Mitglieder:Mitglied von“ mit einem CI für logische Verbindungen aufweisen.
9. Verweis auf logische Schnittstelle nicht gefunden: Wird während des Audits für logische Verbindungsdiskrepanz generiert, wenn einer logischen Verbindung einer der Endpunkte fehlt (Port A oder Port z oder beides).

Telekommunikationsabgleich

Automatisieren Sie den Abgleich von Diskrepanzen im Netzwerkbestand, und verbessern Sie die betriebliche Effizienz. Der Telekommunikationsabgleich hilft bei:

- Identifizieren und beheben Sie Diskrepanzen zwischen Live-Netzwerkbestand und CMDB-Bestand, um die Ausrichtung sicherzustellen und die Produktivität zu steigern
- Ermöglichen Sie Anwendern automatisch generierte Diskrepanzberichte, die die Art der Diskrepanz detaillieren
- Bieten Sie Anwendern empfohlene Korrekturmaßnahmen und die Flexibilität und Kontrolle, um zwischen manuellen oder automatisierten Methoden zur Behebung von Diskrepanzen zu wählen
- Verbessern Sie den Betrieb, indem Sie den Betriebsstatus von Netzwerkressourcen automatisch mit demselben Status in der Bestands-CMDB abstimmen

Zugehörige Informationen

[Diskrepanzidentifizierung: Arten von Diskrepanzen](#)

[Aktivieren Sie die Identifizierung und den Abgleich von Telekommunikationsdiskrepanzen](#)

[Führen Sie ein Audit für Telekommunikationsdiskrepanzen aus](#)

[Mit Telecom Discrepancy Identification and Reconciliation installierte Systemkomponenten](#)

Diskrepanzidentifizierung: Arten von Diskrepanzen

Die Funktion „Identifizierung und Abgleich von Telekommunikationsdiskrepanzen“ identifiziert und klassifiziert Diskrepanzen zwischen dem Netzwerkstatus (wie durch TSOM Discovery oder Service Graph Connectors erkannt) und den in der CMDB oder TNI gespeicherten Bestandsdaten.

Die Identifizierung von Diskrepanzen wird durch das Audit der CMDB-Compliance-Zertifizierung unterstützt, das:

- Wird für CI- und Beziehungsdaten ausgeführt.
- Vergleicht erkannte und inventarisierte Datensätze.
- Generiert Folgeaufgaben, wenn Nichtübereinstimmungen erkannt werden.

Diskrepanztypen

Der Audit-Prozess identifiziert Diskrepanzen, indem erkannte Netzwerkdaten mit dem vorhandenen Bestand in CMDB/TNI verglichen werden. Diskrepanzen fallen in zwei Hauptkategorien:

Fehlt im Netzwerk: Entitäten, die im Bestand vorhanden sind, aber im Netzwerk fehlen

Definition: Ein CI wird von Discovery erkannt, fehlt jedoch entweder in der CMDB/TNI oder ist falsch dargestellt. Beispielsweise erkennt Discovery Card05, die in Slot04 installiert ist, aber die CMDB listet Card04 weiterhin auf, oder schlimmer noch, zeigt sowohl Card04 als auch Card05 im selben Slot an, was Kardinalitäts- oder Modellbeschränkungen verletzt.

Auswirkung:

- Eine Diskrepanzaufgabe wird generiert, um den Datenkonflikt hervorzuheben.
- Optionale Korrektur-Subflows können ausgelöst werden, um die Daten abzugleichen, indem veraltete Datensätze stillgelegt oder Slot-Zuweisungen aktualisiert werden.

Nicht übereinstimmende Konfigurationselemente (CIs): Entitäten, die im Bestand und Netzwerk vorhanden sind, sich jedoch in Attributwerten und hierarchischen Beziehungen unterscheiden

Definition: Das CI ist sowohl in Discovery als auch in CMDB/TNI vorhanden, aber es gibt Diskrepanzen bei Beziehungen, Hierarchie oder Attributwerten. Im Folgenden sind die Untertypen aufgeführt:

- Hierarchiekonflikte: Treten auf, wenn die strukturellen Beziehungen zwischen CIs (z. B. Zuordnungen von über- und untergeordneten Elementen) inkonsistent sind. Im Folgenden finden Sie Beispiele:
 - Ein Gehäuse enthält mehr untergeordnete Karten, als die Modelldefinition zulässt.
 - Eine Karte ist falsch einem Steckplatz in der CMDB zugeordnet, der nicht an Discovery-Daten ausgerichtet ist. Die Validierungsquellen sind:
 - `cmdb_rel_ci` Datensätze für Enthält::enthalten in Beziehungen.
 - `sn_ni_Core_Network_model_Relationship` Tabelle zum Erzwingen modellspezifischer Einschränkungen.
- Attributwert-Nichtübereinstimmungen: Beziehen Diskrepanzen in CI-Eigenschaften auf Feldebene ein. Die häufigsten Probleme sind:
 - Veraltete oder falsche Discovery-Daten.
 - Falsche Modellkonfigurationen.
 - Ungültige Slot-Zuweisungen, die gegen Modellregeln verstoßen.

Die Auswirkung ist, dass die betroffenen Datensätze in Audit-Berichten als fehlgeschlagen markiert werden. Folgeaufgaben können kontextspezifische Korrektursubflows aufrufen, um Bestandsdaten mit dem tatsächlichen Netzwerkstatus neu auszurichten.

Hinweis:

Weitere Informationen finden Sie unter [Konfigurieren Sie die Diskrepanz des Attributwerts in CMDB 360](#).

Zugehörige Informationen

[Aktivieren Sie die Identifizierung und den Abgleich von Telekommunikationsdiskrepanzen](#)

[Führen Sie ein Audit für Telekommunikationsdiskrepanzen aus](#)

Telecommunications Service Operations Management konfigurieren

Konfigurieren Telecommunications Service Operations Management(TSOM) zur Aktivierung der Echtzeitereigniserfassung, Korrelation und automatisierten Korrektur durch Integration mit externen Netzwerküberwachungs- und Discovery-Systemen.

Richten Sie TSOM ein, um End-to-End-Telekommunikationsservicevorgänge zu ermöglichen, einschließlich Alarmerfassung, CMDB-Auffüllung, Diskrepanzerkennung und Transparenz der Serviceauswirkung. Diese Konfiguration umfasst die Aktivierung von Benachrichtigungen über die Telekommunikations-API, die Einrichtung von Discovery- und Service Graph Connectors, die Aktivierung der Transparenz und die Konfiguration von Audit- und Abgleich-Frameworks.

Konfiguration – Übersicht

Telekommunikations-Service Operations-Management (TSOM) erfordert die Konfiguration mehrerer Komponenten für Alarmerfassung, Discovery, Datennormalisierung und Abgleich, um End-to-End-Telekommunikationsvorgänge zu unterstützen. Der Konfigurations-Flow umfasst normalerweise:

- 1.** Aktivieren Sie die folgenden Plugins, um TSOM Core in Ihrem System zu verwenden
 - Musterdesigner (com.snc.pattern.designer)
 - Von ServiceNow IntegrationHub gestartetes Paketinstallationsprogramm (com.glide.hub.integrations)
 - Discovery (com.snc.discovery)
 - CMDB-CI-Klassenmodelle (sn_cmdb_ci_class) 1.69.0
 - Sichtbarkeitsinhalt (sn_pattern_Design) 6.23.0
 - Integration Commons für CMDB (sn_cmdb_int_util) 2.19.0
- 2.** Alarmerfassung aktivieren: Aktivieren Sie die Benachrichtigungen der Telekommunikations-API, und richten Sie Themenabonnements ein, um Alarme von externen Systemen zu erhalten. Weitere Informationen finden Sie unter [Konfigurieren von Telekommunikations-API-Benachrichtigungen](#).
- 3.** Transparenz einrichten: Konfigurieren Sie die Transparenz der Telekommunikation, um Service-zu-Infrastruktur-Zuordnungen anzuzeigen und die Netzwerkintegrität zu überwachen. Weitere Informationen finden Sie unter [Richten Sie die Transparenz der Telekommunikation ein](#)

a. Füllen Sie die Telekom-fähige CMDB aus:

- Installieren und konfigurieren Sie Horizontal Discovery. Weitere Informationen finden Sie unter [Installieren Sie Horizontal Discovery, und richten Sie Discovery-Muster ein.](#)
- Richten Sie ETL-Flows des Telecom Discovery Builder (TDB) in Connectors ein. Weitere Informationen finden Sie unter [Konfigurieren der ETL des Telecom Discovery Builder-Frameworks in einem Connector.](#)
- Verwenden Sie Service Graph Connectors (z. B. Nokia Altiplano), um Topologie- und Konfigurationsdaten zu importieren. Weitere Informationen finden Sie unter [Konfigurieren des Nokia Altiplano Service Graph Connector.](#)

b. Diskrepanzerkennung aktivieren:

- Aktivieren Sie die Identifizierung und den Abgleich von Telekommunikationsdiskrepanzen. Weitere Informationen finden Sie unter [Aktivieren Sie die Identifizierung und den Abgleich von Telekommunikationsdiskrepanzen.](#)
- Definieren Sie Filter für Telekommunikations-Audits, und konfigurieren Sie Diskrepanzprüfungen für Attributwerte in CMDB 360.

Jeder Schritt ist modular und kann basierend auf Ihrer Umgebung und verfügbaren Integrationen konfiguriert werden.

Konfigurieren von Telekommunikations-API-Benachrichtigungen

Konfigurieren Sie die Telekommunikations-API-Benachrichtigung in ServiceNow Instanz.

Modellierung des Benachrichtigungs-Workflows der Telekommunikations-API

Die folgenden Schritte helfen bei der Konfiguration der Telekommunikations-API-Benachrichtigung in ServiceNow Instanz.

1. **Thema erstellen:** Sie können Themen erstellen, indem Sie entweder die Details der externen Nachricht manuell eingeben oder die verfügbaren Themen automatisch aus dem externen System erfassen.
2. **Erstellen Sie ein Themenabonnement:** Sie abonnieren die verfügbaren Themen für eingehende Benachrichtigungen aus dem externen System basierend auf den Kundeneinstellungen. Darüber hinaus generieren Sie die Rückruf-URL und registrieren das Abonnement.
3. **Aktivieren Sie den Endpunkt der offenen API-Verbindung für Telekommunikationsalarmmanagement:** Um Antworten vom externen System zu erhalten, aktivieren Sie die abonnierten Endpunkte der offenen API-Verbindung für Telekommunikationsalarmmanagement in der Workflow-Studio.
4. **Geben Sie die Rückruf-URL für das externe System an, um Benachrichtigungen zu erhalten.** Der Kunde kann die Rückruf-URL auch wiederverwenden. Wenn Anforderungen von TMF 688 die Rückruf-URL erreichen, wird initiiert *Standardauslöser Für Alarmereignisbenachrichtigung* Flow zum Erstellen eines Ereignisses.

Weitere Informationen zu den Funktionen zur Verarbeitung offener API-Anforderungen für das Ereignisbenachrichtigungsmanagement, die durch externe Auslöserdefinitionen zum Erstellen, Aktualisieren und Löschen von Ereignissen ausgelöst werden, finden Sie unter [Event Notification Management Open API](#) und [TMFTopicEventAPIUtilOOB - Scoped](#).

Dieser Workflow erstellt ein Ereignis in der Ereignismanagement Anwendung. Um mehr über die Verwendung von zu erfahren Ereignismanagement, Siehe [Ereignismanagement](#).

Zugehörige Informationen

[Mit Benachrichtigungen der Telekommunikations-API installierte Systemkomponenten](#)

[Externes Ereignismanagement über Benachrichtigungen der Telekommunikations-API](#)

Thema erstellen

Erstellen Sie ein Thema, und veröffentlichen Sie die eingehenden Benachrichtigungen aus dem externen System im Thema. Durch Erstellen der Themen können Abonnenten die Themen auswählen, die sie abonnieren möchten.

Vorbereitungen

Stellen Sie sicher, dass die Anwendung Telecommunications Alarm Management Open API (sn_ind_tm642) mit installiert ist ServiceNow AI Platform.

Erforderliche Rolle: admin, sn_api_notif_mgmt.topic_creator

Warum und wann dieser Vorgang ausgeführt wird

Sie können Themen erstellen, indem Sie entweder die Details der externen Nachricht manuell eingeben oder die verfügbaren Themen automatisch aus dem externen System erfassen. Wenn Sie ein Thema erstellen, wird ein Datensatz in der Tabelle „Thema“ [sn_api_notif_mgmt_topic] erstellt.

Prozedur

1. Alle > Telecom-API-Benachrichtigung > Themenan.

2. Wählen Sie **Neu**.

Wenn Sie in ein externes System integriert haben, können Sie auswählen **Themen Abrufen**

Um die verfügbaren Themen automatisch abzurufen. Diese Aktion löst aus *API zur Ereignisalarmbenachrichtigung* subflow. Weitere Informationen zu den Funktionen, mit denen Sie Datensätze im Thema abfragen und bearbeiten können, finden Sie unter [TopicUtilOOB - Scoped](#) .

3. Füllen Sie im Formular die Felder aus.

Formular „Thema“

Feld	Beschreibung
Themen-ID	Eindeutige Themen-ID
Themenname	Der Name des Themas.
Typ	Typ des Themas. Wählen Sie eine der folgenden Optionen aus: ○ Eingehend: Option für eingehende Benachrichtigung. ○ Ausgang: Option für ausgehende Benachrichtigung.
Header-Abfrage	Codierte Header-Abfrageparameter. Anlea R n weitere Informationen zu den folgenden Abfrageparametern Die TMF 688-Standards, siehe Die TM-Forum .
Inhaltsabfrage	Abfrageparameter für codierte Inhalte.

Feld	Beschreibung
	An lea R n weitere Informationen zu den folgenden Abfrageparametern Die TMF 688-Standards, siehe TM-Forum .
Beschreibung	Eine kurze Beschreibung des Themas.

4. Wählen Sie **Absenden**.

Ergebnisse

Ein Thema wird erstellt.

Nächste Maßnahme

Sie können das Themenabonnement gemäß den Kundenanforderungen erstellen. Weitere Informationen finden Sie unter .

Erstellen Sie ein Themenabonnement

Abonnieren Sie das Thema in ServiceNow AI Platform Dass Sie auf die eingehende Benachrichtigung vom externen System antworten möchten. Durch das Abonnement des Themas erhält der Abonnent die Benachrichtigungen basierend auf den Themen, die Sie abonnieren.

Vorbereitungen

- Stellen Sie sicher, dass die Anwendung Telecommunications Alarm Management Open API (sn_ind_tm642) mit installiert ist ServiceNow AI Platform.
- Erstellen Sie Themen für die eingehenden Benachrichtigungen.

Erforderliche Rolle: admin, sn_api_notif_mgmt.Subscription_Creator

Warum und wann dieser Vorgang ausgeführt wird

Sie abonnieren die verfügbaren Themen für die eingehenden Benachrichtigungen aus dem externen System basierend auf den Kundeneinstellungen. Sie generieren die Rückruf-URL, um sie für die Kunden freizugeben. Wenn eine Anforderung von einem externen System auf die Rückruf-URL trifft, wird die Erstellung eines Ereignisses in initiiert Ereignismanagement Anwendung.

Darüber hinaus registrieren Sie das Themenabonnement, um mit dem Empfang der eingehenden Benachrichtigungen zu beginnen. Wenn Sie ein Themenabonnement erstellen, wird ein Datensatz in der Tabelle „Themenabonnement“ [sn_api_notif_mgmt_Subscription] erstellt. Weitere Informationen zu den Methoden zum Abfragen und Bearbeiten von Datensätzen im Themenabonnement finden Sie unter [TopicSubscriptionUtilOOB - Scoped](#) .

Prozedur

1. Alle > Telecom-API-Benachrichtigung > Abonnementan.

2. Wählen Sie **Neu**.

3. Füllen Sie im Formular die Felder aus.

Formular „Themen-Abonnement“

Feld	Beschreibung
Thema	Thema, das Sie abonnieren möchten.
CallbackURL	Die Rückruf-URL, die Sie für das externe System freigeben, um die eingehende Benachrichtigung zu erfassen. Die URL wird automatisch generiert, wenn Sie auswählen Generieren Sie CallbackURL .
Abfrage filtern	Codierte Inhaltsabfrageparameter aus dem Thema. Sie können auch die Filterabfrage ändern. Weitere Informationen zu den Abfrageparametern, die den TMF 688-Standards entsprechen, finden Sie unter TM-Forum .
Registrierungsstatus	Status der Themenregistrierung beim externen System. Standardmäßig ist es Nicht Registriert . Wenn der Prozess erfolgreich ist, ändert sich der Feldwert in Registriert . Andernfalls ist es Fehler .
Registrierungsnachricht	Registrierungsstatusnachricht vom externen System.
Abonnement-ID	Eindeutige Abonnement-ID aus dem externen System.

4. Rufen Sie die Rückruf-URL ab, indem Sie auswählen **Generieren Sie CallbackURL**.

5. Registrieren Sie das Abonnement, indem Sie auswählen **Registrieren**.

Ergebnisse

Für die Rückruf-URL wird eine Auslöserdefinition erstellt, und das Thema wird im externen System registriert.

Nächste Maßnahme

In Workflow-Studio, Aktivieren Sie die Endpunkte der offenen API-Verbindung für das Telekommunikations-Alarmmanagement. Weitere Informationen finden Sie unter [Aktivieren Sie den Endpunkt der offenen API-Verbindung für Telekommunikationsalarmmanagement](#).

Aktivieren Sie den Endpunkt der offenen API-Verbindung für Telekommunikationsalarmmanagement

Aktivieren Sie den Endpunkt der offenen API-Verbindung für Telekommunikationsalarmmanagement. Durch die Aktivierung des Endpunkts erhalten Sie die eingehenden Benachrichtigungen vom externen System für das von Ihnen registrierte Thema.

Vorbereitungen

- Erstellen Sie das Thema, und abonnieren Sie es, um die eingehenden Benachrichtigungen zu erhalten.
- Generieren Sie eine Rückruf-URL, und registrieren Sie das Themenabonnement.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie aktivieren die abonnierten Endpunkte der offenen API-Verbindung für Telekommunikationsalarmmanagement in der Workflow-Studio Um Antworten vom externen System zu erhalten.

Prozedur

1. Navigieren zu **Alle > Prozessautomatisierung > Flow Designer**an.
2. Auf der **Verbindungen** Wählen Sie die Registerkarte aus **Telekommunikations-Alarmmanagement – API öffnen** .
3. Öffnen Sie den Endpunkt-Datensatz, den Sie aktivieren möchten.
4. Wählen Sie **Aktivieren**.

Richten Sie die Transparenz der Telekommunikation ein

Telekommunikationstransparenz bietet grundlegende Funktionen, die sowohl die Telekommunikations-Discovery als auch die Identifizierung und den Abgleich von Telekommunikationsdiskrepanzen unterstützen. Es umfasst gemeinsam genutzte Logik, erweiterte CI-Klassenmodelle und Updates der Identification and Reconciliation Engine (IRE), die auf Elemente des Telekommunikationsnetzwerks zugeschnitten sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Bestätigen Sie, dass:

- Ihre ServiceNow-Instanz ist für TSOM lizenziert.
- Ihr MID-Server ist betriebsbereit und für die Discovery validiert.
- Sie überprüfen alle anwenderdefinierten IRE-Regeln, die auf Telekommunikations-CIs angewendet werden, um Überschreibungen während des Upgrades zu verhindern.

Warum und wann dieser Vorgang ausgeführt wird

Um die Transparenz der Telekommunikation zu konfigurieren, müssen Sie die erforderlichen Plugins installieren und die CMDB-CI-Klassenmodelle auf Version 1.69.0 aktualisieren, die Telekommunikationsspezifische IRE-Identifizierungsregeln einführt. Dies bestätigt die genaue CI-Identifizierung und den korrekten Abgleich über Telekommunikationsdomänen hinweg.

Hinweis:

Wenn Sie für eines der betroffenen Telekommunikations-CIs angepasste IRE-Identifizierungsregeln haben, kann das Upgrade auf Version 1.69.0 diese Regeln überschreiben oder sich auf diese auswirken.

Die folgenden Funktionen sind im Abonnement für Telekommunikationstransparenz enthalten:

Plugin-Name	Beschreibung	Store-App
Service Graph Connectors sn_sgc_altiplano_Connector	Service Graph Connector für Nokia Altiplano	Ja
Discovery-Muster Für Telekommunikation sn_tsom_patterns	Discovery-Muster Für Telekommunikation	Ja

Plugin-Name	Beschreibung	Store-App
Plugin „Telekommunikations-Sichtbarkeit“ (Core-Logik) <code>sn_tsom_Core</code>	Kernlogik für Transparenz in der Telekommunikation und Diskrepanzabgleich	Nein

Hinweis:

Diese Plugins lösen automatisch die Installation oder Aktualisierung der CMDB CI-Klassenmodelle-Anwendung auf Version 1.69.0 aus.

Prozedur

1. Navigieren zu **Alle > Plugins** an.

2. Suchen und installieren Sie Folgendes:

- a.** Service Graph Connector für Nokia Altiplano (`sn_sgc_altiplano_Connector`)
- b.** Discovery-Muster für Telekommunikation (`sn_tsom_patterns`)
- c.** Telekommunikationstransparenz (Plugin) (`sn_tsom_Core`)

3. Wahlweise: Aktualisieren Sie die CMDB-CI-Klassenmodelle.

- a.** Navigieren zu **Alle > Verfügbare Anwendungen** Liste im ServiceNow Store.
- b.** Suchen Sie nach CMDB-CI-Klassenmodellen (`sn_cmdb_ci_class`).
- c.** Installieren Sie Version 1.69.0 oder führen Sie ein Upgrade auf diese durch.

Hinweis:

Durch die Installation eines der oben aufgeführten TSOM-Plugins wird die Version 1.69.0 der CMDB CI-Klassenmodelle-App automatisch aktualisiert oder installiert. Wenn Ihre Instanz keine TSOM-Plugins enthält oder Sie sich in einem früheren Release von Yokohama befinden (z. B. Washington DC oder Xanadu), können Sie die Store-App manuell installieren oder aktualisieren.

4. Navigieren zu **CMDB > Identifizierungsregeln** an.

a. Überprüfungsregeln im Zusammenhang mit:

- `cmdb_ci_Interface_Card`
- `cmdb_ci_Slot`
- `cmdb_ci_subslot`
- `cmdb_ci_network_adapter`

b. Überprüfen Sie, ob Ihre anwenderdefinierte Logik funktionsfähig bleibt.

c. Aktualisieren oder führen Sie anwenderdefinierte Regeln nach Bedarf zusammen.

Ergebnisse

Bestätigen Sie, dass Folgendes als aktiv aufgeführt ist:

- Telekommunikationstransparenz (`sn_tsom_Core`)
- Discovery-Muster für Telekommunikation (`sn_tsom_patterns`)
- Service Graph Connector für Nokia Altiplano (`sn_sgc_altiplano_Connector`)
- CMDB-CI-Klassenmodelle Version 1.69.0

Zugehörige Informationen

[Telekommunikationstransparenz](#)

Installieren Sie Horizontal Discovery, und richten Sie Discovery-Muster ein

Installieren Sie horizontale Discovery-Muster, die die Abhängigkeiten und Anforderungen verstehen.

Vorbereitungen

Erforderliche Rolle: Administrator

Stellen Sie sicher, dass Sie ein Abonnement für TSOM haben.

Warum und wann dieser Vorgang ausgeführt wird

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](#).

Abhängigkeiten und Anforderungen:

- Telekommunikations-Core (sn_Tsom_Core)
- Discovery Core-Plugin (com.snc.Discovery.Core), das automatisch von Discovery installiert wird.
- Plugin „ITOM Discovery-Lizenz“ (com.snc.itom.discovery.license). Sie müssen dieses Plugin aktivieren.
- Plugin „ITOM-Lizenzierung“ (com.snc.itom.license). Weitere Informationen finden Sie unter [Request Discovery](#).

Musterausführungslogik: Wenn ein TSOM-Muster ausgeführt wird, wird standardmäßig sowohl das TSOM-spezifische als auch das entsprechende ITOM-Muster ausgeführt (z. B. Telco-Router führt Router aus). Dadurch wird sichergestellt, dass freigegebene ITOM-Bibliotheken bei Bedarf wiederverwendet werden. So überschreiben Sie dieses Verhalten:

- Verwenden Sie die Systemeigenschaft `sn_tsom_patterns.itom_pattern_enabled`.
- Wenn Sie diese Eigenschaft auf „falsch“ festlegen, wird nur das TSOM-spezifische Muster ausgeführt.

Prozedur

1. Installieren Sie die Anwendung Horizontal Discovery.
Siehe [Discovery setup](#), Da es für die Ausführung von Telecommunications Discovery-Mustern von grundlegender Bedeutung ist.
2. Telecommunications Discovery-Muster abrufen und installieren:
 - a. Installieren Sie die Telecommunications Discovery-Muster (sn_tsom_patterns) aus dem ServiceNow® Speichern.
3. Richten Sie einen MID-Server und Synchronisierungsmuster ein:

- a. Synchronisieren Sie die installierten Muster mit den entsprechenden MID-Servern, um sicherzustellen, dass sie einsatzbereit sind:

- i. Navigieren zu **Discovery > MID-Server** an.
- ii. Wählen Sie Aus **Mustersynchronisierung mit MID**.

i Hinweis:

Mit dieser Aktion werden sowohl TSOM- als auch ITOM-Muster synchronisiert.

Weitere Informationen zum Konfigurieren eines MID-Servers finden Sie unter [Configuring MID Server](#).

4. TSOM-Systemeigenschaften konfigurieren:

- a. Legen Sie die Systemeigenschaft `sn_tsom_patterns.itom_pattern_enabled` fest, um die Logik zu definieren, ob nur das TSOM-Muster oder eine Kombination aus ITOM- und TSOM-Mustern verwendet werden soll.
 - i. Navigieren Sie zu **Alle > Systemeigenschaften > Alle Eigenschaften** an.
 - ii. Wählen Sie Aus **`sn_tsom_patterns.itom_pattern_enabled`**.
 - iii. Überprüfen Sie, ob der Wert auf festgelegt ist **Wahr** (Standard).

Wenn TSOM nur TSOM-Muster ausführen und ITOM-Muster ausschließen soll, legen Sie den Wert auf fest **Falsch**.

i Hinweis:

Die Standardeinstellung ist so konfiguriert, dass sowohl TSOM- als auch ITOM-Muster verwendet werden.

5. Aktivieren Sie den Ersatz verschiedener ITOM-Muster durch TSOM-Muster auf einem bestimmten MID-Server:

Beispiel: Das Telecom-Router-Muster ersetzt das Netzwerkrouter-Muster für einen bestimmten MID-Server, wenn **Mid.Telekommunikation.Discovery.Muster.aktiviert** ist für diesen MID-Server auf „wahr“ festgelegt.

- a. Wechseln Sie zu **Filternavigator** Und Typ **`ecc_Agent_config.list`**.
- b. Wählen Sie Aus **Mid.Telekommunikation.Discovery.Muster.aktiviert** (Jeder MID-Server hat diesen Parameter.)
- c. Überprüfen Sie, ob der Wert auf festgelegt ist **Wahr**.

Wiederholen Sie diese Konfiguration für jeden MID-Server, den Sie zum Ausführen von TSOM-Mustern verwenden möchten.

Zugehörige Informationen

[Leiten Sie die Discovery mithilfe von Discovery-Mustern](#)

Konfigurieren der ETL des Telecom Discovery Builder-Frameworks in einem Connector

Nutzen Sie das vorgefertigte Telecom Discovery Builder Framework ETL, indem Sie es in Ihren Connector-Bereich duplizieren, die entsprechende Datenquelle zuweisen und als Teil eines neuen Service Graph Connector bereitstellen.

Das Telecom Discovery Builder-Framework ETL, das mit dem TSOM-Core (Telecom Service Operations Management) bereitgestellt wird, ist ein einsatzbereites Framework, das die Datenerfassung in der CMDB über Telekommunikations-Connectors hinweg optimiert. Anstatt sie als Administrator direkt zu konfigurieren, können Sie die ETL in den Anwendungsbereich eines Connectors duplizieren und die Datenquelle so aktualisieren, dass sie an der Discovery-Nutzlast des Connectors ausgerichtet ist.

Schritte zur Verwendung der ETL des Telecom Discovery Builder-Frameworks in einem Connector

1. Temporäre Datenquelle erstellen: Erstellen Sie eine Datenquelle im Anwendungsbereich Ihres Connectors basierend auf der Datenquelle „Generisches Schema mit mehreren Quellen“ aus TSOM Core. Auf diese Weise können Sie die duplizierte ETL mit schemaausgerichteten Platzhalterdaten ausführen und testen. Weitere Informationen finden Sie unter [Erstellen Sie eine Datenquelle, die der Kerndatenquelle „Telekommunikation“ ähnlich ist](#)
2. ETL des Telecom Discovery Builder-Frameworks duplizieren: Greifen Sie auf ETL Studio zu, suchen Sie die ETL des generischen Telco-Schemas, und duplizieren Sie sie im Umfang des Connectors. Während der Duplizierung: Geben Sie einen neuen Namen an. Weisen Sie die temporäre Datenquelle zu. Verwenden Sie „importSet“ als Discovery-Quelle. Weitere Informationen finden Sie unter [Duplizieren Sie die ETL des Telecom Discovery Builder-Frameworks in einem Connector-Bereich](#)
3. Öffnen Sie nach der Duplizierung die neue ETL, und ersetzen Sie die temporäre Datenquelle durch die tatsächliche Discovery-Datenquelle des Connectors. Weitere Informationen finden Sie unter [Aktualisieren Sie die Datenquelle des Connectors](#).
4. Testen oder stellen Sie den Service Graph Connector bereit. Weitere Informationen finden Sie unter [Stellen Sie einen neuen Service Graph Connector mit vorhandener ETL bereit](#)

Erstellen Sie eine Datenquelle, die der Kerndatenquelle „Telekommunikation“ ähnlich ist

Richten Sie im Anwendungsbereich des Connectors eine Schema-konforme Datenquelle ein, um Telekommunikationsdaten zu simulieren und erfolgreiche Tests und Validierung der ETL des Telecom Discovery Builder-Frameworks sicherzustellen, bevor Sie sie in Live-Gerätedaten integrieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Voraussetzungen:

- Zugriff auf die TSOM Core-Anwendung und ihre Datenquellen.
- Wechseln Sie zum Anwendungsbereich des Connectors.
- Haben Sie eine Beispielnutzlast, die dem generischen Telco-Schema entspricht (optional, aber zum Testen empfohlen).

Warum und wann dieser Vorgang ausgeführt wird

Beim Duplizieren der ETL des Telecom Discovery Builder-Frameworks in einen SGC-Anwendungsbereich (Service Graph Connector) müssen Sie zuerst eine Datenquelle erstellen, die die genaue Struktur der TSOM Core-Datenquelle repliziert. Diese duplizierte Datenquelle bietet das erforderliche Schema und die Struktur zum Testen und Validieren der ETL, bevor sie mit Live-Telekommunikationsdaten verbunden wird.

Das Telecom Discovery Builder-Framework erwartet Daten, die dem generischen Telco-Schema entsprechen, wie im Telecom Core definiert. Durch das Duplizieren der ursprünglichen TSOM-Datenquelle wird Folgendes sichergestellt:

- Schemaausrichtung während ETL-Duplizierung.
- Eine gültige Importsatzstruktur zum Testen.
- Trennung von Kern- und Connector-Bereichen für Anpassung und Upgrade-Sicherheit.

Wann eine Datenquelle erstellt werden soll, die der TSOM Core-Datenquelle ähnlich ist:

- Vor dem Duplizieren der ETL des Telecom Discovery Builder-Frameworks.
- Wenn Sie eine Testlast mit simulierten Telekommunikationsdaten oder Platzhalterdaten ausführen möchten.
- Bei der Vorbereitung des Anwendungsbereichs des Connectors für die Erfassungskonfiguration.

Der folgende Screenshot kann Ihnen helfen, das Ausfüllen der Feldwerte beim Erstellen der Datenquelle zu

The screenshot shows the 'Data Source' configuration page in ServiceNow. The 'Name' field is 'NSP Generic Data Source'. The 'Import set table label' is 'NSP Generic Data Source'. The 'Import set table name' is 'sn_sgc_nsp_generic_data_source'. The 'Type' is 'Custom (Load by Script)'. The 'Data in single column' checkbox is checked. The 'Data Loader' dropdown is set to 'Turn on ECMAScript 2021 (ES12) mode'. The 'Properties' field is empty. The 'Data Loader' dropdown is set to 'Turn on ECMAScript 2021 (ES12) mode'. The 'Data Loader' dropdown is set to 'Turn on ECMAScript 2021 (ES12) mode'. The 'Data Loader' dropdown is set to 'Turn on ECMAScript 2021 (ES12) mode'.

verstehen.

Prozedur

1. Navigieren zu **Alle > System-Importsätze > Administration > Datenquellen**an.
2. Suchen Sie nach **Generisches Schema mit mehreren Quellen v2** Oder eine ähnliche Baseline-Quelle, die mit TSOM Core bereitgestellt wird.
3. Öffnen Sie den TSOM Core-Datenquellendatensatz, und kopieren Sie das Skript aus dem **Datenladeprogramm** Feld.
4. Erstellen Sie eine Datenquelle, indem Sie auf klicken **Neu** .
5. Füllen Sie die Felder im Formular aus
Weitere Informationen finden Sie unter [Create a Custom \(Load by Script\) type data source](#) .
6. In **Typ** Feld auswählen **Anwenderdefiniert (nach Skript laden)** .
7. Wählen Sie aus **Daten in einer Spalte** Feld.
8. In **Datenladeprogramm** Feld, fügen Sie das kopierte Skript ein.
9. Wählen Sie **Absenden**.
Die Datenquelle wird erstellt.

10. Wahlweise: So testen Sie das Laden der Datenquelle:

- a. Klicken Sie auf Testladen von 20 Datensätzen (oder Ähnlichem), um einen Importsatz zu generieren.
- b. Stellen Sie sicher, dass Datensätze ohne Fehler erstellt werden.
- c. Vergewissern Sie sich, dass Klassen wie logisches Composite, Netzwerkgerät oder Port in der Bereitstellungstabelle angezeigt werden.

Nächste Maßnahme

Nachdem die Datenquelle erstellt und getestet wurde:

- Verwenden Sie sie beim Duplizieren der generischen ETL für Telco als Importquelle.
- Ersetzen Sie sie durch die tatsächliche Connector-spezifische Datenquelle, sobald die Simulation und Validierung abgeschlossen ist.

Zugehörige Informationen

[Standardisierter allgemeiner JSON-Datensatz zur Unterstützung aller Service Graph Connectors](#)

[Duplizieren Sie die ETL des Telecom Discovery Builder-Frameworks in einem Connector-Bereich](#)

Duplizieren Sie die ETL des Telecom Discovery Builder-Frameworks in einem Connector-Bereich

Das Telecom Discovery Builder-Framework ETL ermöglicht es Service Graph Connector (SGC)-Teams, schnell eine standardisierte, schemakonforme Datenerfassungs-Pipeline zu übernehmen, ohne ETL-Logik von Grund auf neu zu erstellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Stellen Sie Folgendes sicher:

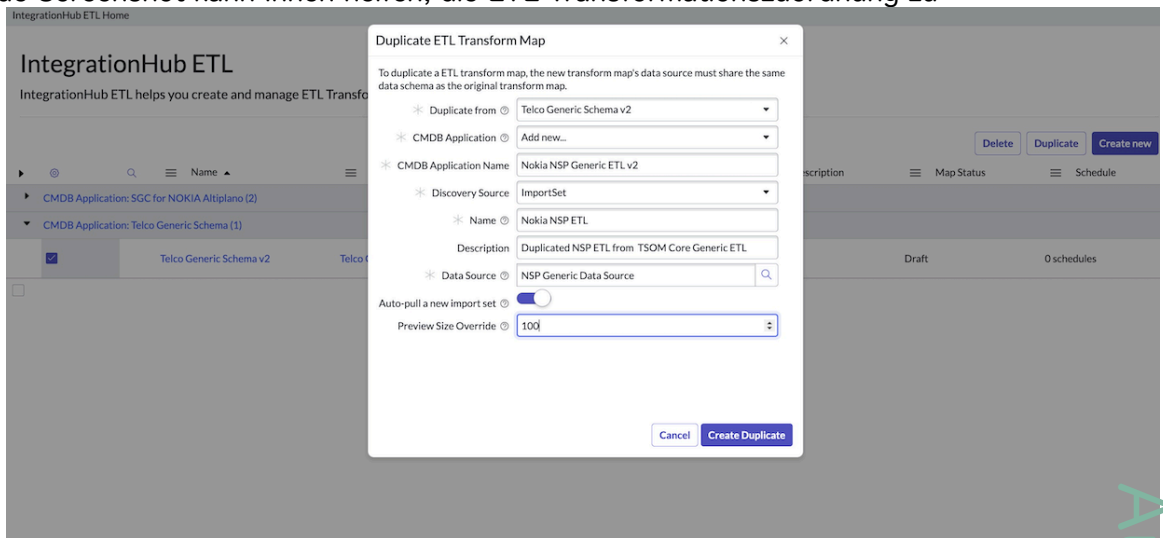
- Das Telecom Core-Plugin ist aktiviert, und das Telco Generic ETL v2 (automatisch installiert) ist verfügbar.
- Sie haben Administratorzugriff auf IntegrationHub ETL Studio.
- Sie haben eine temporäre Datenquelle im Anwendungsbereich des Connectors erstellt. Nach dem Erstellen einer temporären Datenquelle können Sie die generische ETL im Anwendungsbereich Ihres Connectors duplizieren, um sie für Ihren spezifischen Anwendungsfall anzupassen und zu erweitern.

Warum und wann dieser Vorgang ausgeführt wird

Durch das Duplizieren der generischen Telco-ETL können Sie:

- Verwenden Sie standardisierte ETL-Zuordnungen für mehrere Connectors.
- Passen Sie das ETL-Verhalten an, ohne die ursprüngliche Baseline zu ändern, die vom TSOM-Core (Telecom Service Operations Management) bereitgestellt wurde.
- Richten Sie das generische Telco-Schema aus, um Konsistenz und TNI-Compliance zu gewährleisten.
- Sparen Sie Zeit, und reduzieren Sie Fehler, indem Sie mit einem getesteten und bewährten ETL-Framework arbeiten.

Der folgende Screenshot kann Ihnen helfen, die ETL-Transformationszuordnung zu



duplizieren.

Prozedur

1. Navigieren zu **Alle > IntegrationHub ETL** an.

2. Auf der **IntegrationHub ETL** Wählen Sie den Anwendungsbereich des Connectors aus.

i Hinweis:

Beispiel: **Service Graph Connector für Nokia NSP** .

3. Erweitern Sie das generische Schema für CMDB-Anwendung Telco, und wählen Sie aus **Generisches Telco-Schema** Datensatz.

4. Klicken Sie Auf **Duplikat** .

Die Seite „ETL-Transformationszuordnung duplizieren“ wird angezeigt.

5. Konfigurieren Sie die duplizierte ETL-Transformationszuordnung

- a. In **Duplikat Von** Feld, stellen Sie sicher, dass das generische Telco-Schema ausgewählt ist.
- b. Wählen Sie eine vorhandene CMDB-Anwendung aus, oder klicken Sie auf **Neu hinzufügen...** Zum Hinzufügen einer neuen CMDB-Anwendung.
- c. Geben Sie für eine neue CMDB-Anwendung den Namen der CMDB-Anwendung ein (z. B. Nokia NSP Generic ETL v2).
- d. In **Discovery-Quelle** Wählen Sie den Importsatz aus.
- e. In **Name** Feld einen Namen für die doppelte ETL eingeben.
- f. In **Beschreibung** Geben Sie eine Beschreibung für die doppelte ETL ein.
- g. Wählen Sie die Datenquelle aus, die für die doppelte ETL-Transformationszuordnung verwendet wird.

i Hinweis:

Dies muss sich von der vorhandenen Standarddatenquelle unterscheiden, die an die ETL des generischen Telco-Schemas angehängt ist. Weitere Informationen finden Sie unter [Erstellen Sie eine Datenquelle, die der Kerndatenquelle „Telekommunikation“ ähnlich ist.](#)

h. Aktivieren **Neuen Importsatz automatisch abrufen** Option zum automatischen Abrufen von Daten in einen neuen Importsatz.

i. In **Überschreibung Der Vorschaugröße** Feld, legen Sie eine anwenderdefinierte Vorschaugröße für Tests und Validierung fest.

6. Wählen Sie Aus Duplikat Erstellen .

Eine doppelte ETL der generischen Telco-ETL wird erstellt.

7. Wahlweise: Öffnen Sie den duplizierten ETL-Datensatz, und überprüfen Sie die Zuordnungen und Einstellungen.

Nächste Maßnahme

1. Duplizierte ETL testen (optional, aber empfohlen):

- Führen Sie eine Testlast oder eine Simulation mit der temporären Datenquelle aus.
- Überprüfen Sie, ob Importsätze erfolgreich verarbeitet werden, CIs gemäß dem generischen Telco-Schema erstellt werden und Beziehungen ordnungsgemäß eingerichtet sind.

2. Nach erfolgreicher Duplizierung und Tests:

- Aktualisieren Sie die ETL-Datenquellenkonfiguration so, dass sie auf die tatsächliche Produktionsdatenquelle verweist (für echte Gerätedaten).
- Stellen Sie die Connector-Integration in einer Test- oder Produktionsumgebung bereit.
- Überwachen Sie Importausführungen, um zu überprüfen, ob Bestandsdaten korrekt in die CMDB erfasst werden.

Zugehörige Informationen

[Aktualisieren Sie die Datenquelle des Connectors](#)

Beispiel – Duplizieren Sie das generische ETL-Schema für Telco

In diesem Beispiel erfahren Sie, wie Sie die ETL des generischen Telco-Schemas duplizieren, um eine anwenderdefinierte Service Graph Connector-ETL (SGC) für Ihre Telekom-Integration einzurichten. Verwenden Sie dieses Verfahren, wenn Sie eine Baseline-ETL im Anwendungsbereich Ihres Connectors basierend auf dem standardisierten generischen Telco-Schema erstellen möchten, um die Ausrichtung des Schemas, Konsistenz und eine schnellere Bereitstellung sicherzustellen.

Szenario

Sie stellen einen neuen Service Graph Connector bereit und müssen die ETL des generischen Telco-Schemas im Anwendungsbereich Ihres Connectors duplizieren.

Erstellen Sie eine temporäre Datenquelle, duplizieren Sie die ETL, und konfigurieren Sie sie so, dass sie mit den Gerätenutzlasten Ihres Connectors kompatibel ist.

Schritte zum Duplizieren der ETL des generischen Telco-Schemas

- 1.** Wechseln Sie zum Anwendungsbereich des Connectors, in dem Sie die ETL duplizieren möchten (z. B. Nokia NSP Connector).
- 2.** Erstellen Sie die Datenquelle:

- Navigieren Sie zu System-Importsätze > Administration > Datenquellen.
 - Suchen Sie nach der generischen Schema-MultiSource-Datenquelle, die von der TSOM Core-Anwendung bereitgestellt wird.
 - Kopieren Sie diese Datenquelle in den Anwendungsbereich Ihres Connectors.
 - Testen Sie die kopierte Datenquelle, indem Sie Testladen von 20 Datensätzen ausführen, um einen Beispiel-Importsatz zu erstellen.
- 3.** Öffnen Sie das Dialogfeld „ETL-Transformationszuordnung duplizieren“: Wählen Sie in ETL Studio ETL duplizieren aus, um den Duplizierungsprozess zu starten.
 - 4.** In **Duplikat von** Liste, wählen Sie Generisches Telco-Schema.
 - 5.** Wählen Sie Aus **Neu hinzufügen...** Und geben Sie einen Namen für die duplizierte ETL ein.
 - 6.** Wählen Sie „importSet“ als Discovery-Quelle für Ihre duplizierte ETL aus.
 - 7.** Geben Sie einen neuen Namen für die duplizierte Transformationszuordnung ein.
 - 8.** Geben Sie die neu erstellte temporäre Datenquelle an, die Sie aus der MultiSource des generischen Schemas kopiert haben.
 - 9.** Aktivieren Sie optional **Neuen Importsatz automatisch abrufen** Dient zum automatischen Laden neuer Datensätze nach der Duplizierung.
 - 10.** Klicken Sie Auf **Duplikat Erstellen** Um die Duplizierung abzuschließen.
 - 11.** Aktualisieren **Grundlegende Details** :
 - Öffnen Sie nach der Duplizierung die neu erstellte ETL.
 - In Schritt 1: Geben Sie an **Grundlegende Details** , Ersetzen Sie die temporäre Datenquelle durch die Produktionsdatenquelle Ihres Connectors.
 - 12.** ETL-Konfiguration speichern: Klicken Sie auf **Speichern** Um Ihre Änderungen abzuschließen.
 - 13.** Führen Sie aus **Datenquelle** : Führen Sie in Importzeitplänen die Datenquelle Ihres Connectors aus, um echte Gerätedaten zu erfassen.

Ergebnis: Das System erstellt eine neue ETL basierend auf den Einstellungen für das generische Telco-Schema und verarbeitet die Nutzlasten aus der angegebenen Connector-Datenquelle. Die importierten Daten werden in Konfigurationselemente (Configuration Items, CIs) umgewandelt und mit den erwarteten Beziehungen und Strukturen in die ServiceNow-CMDB eingefügt.

Aktualisieren Sie die Datenquelle des Connectors

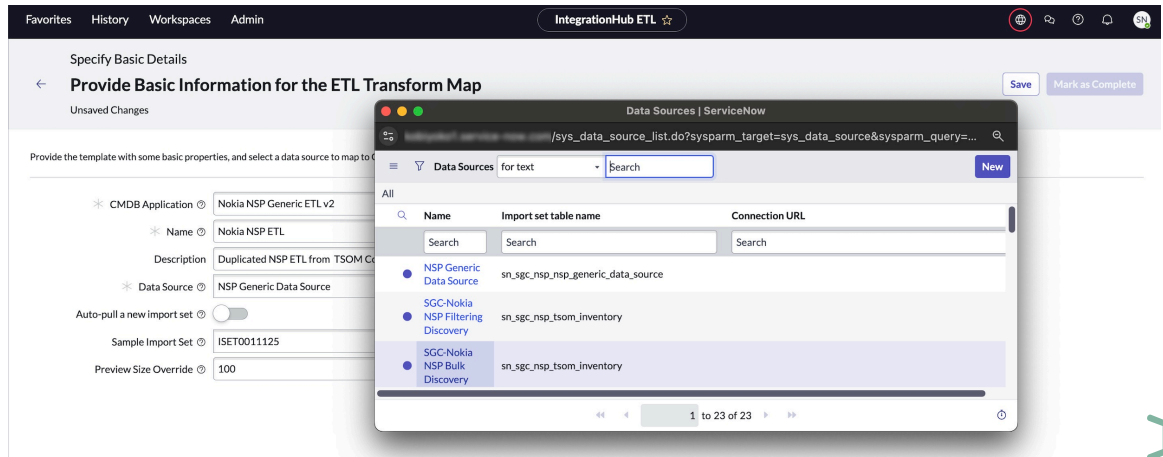
Verknüpfen Sie die duplizierte ETL mit einer gültigen Datenquelle für Ihren spezifischen Connector.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Der folgende Screenshot kann Ihnen helfen, die Standardquelle durch die Datenquelle Ihres Connectors zu



ersetzen.

Prozedur

1. Navigieren zu **Alle > IntegrationHub ETL** an.
2. In **Geben Sie Grundlegende Details An**, Ersetzen Sie die Standarddatenquelle durch die Datenquelle Ihres Connectors.
3. Wählen Sie **Speichern**.
4. Öffnen **Importieren Sie Zeitpläne** und führen Sie Ihre Datenquelle aus.
Das System erstellt eine neue Transformationszuordnung basierend auf den ausgewählten Einstellungen und erstellt aus Ihrer Nutzlast generierte CIs.

Zugehörige Informationen

[Stellen Sie einen neuen Service Graph Connector mit vorhandener ETL bereit](#)

Stellen Sie einen neuen Service Graph Connector mit vorhandener ETL bereit

Ordnen Sie einem vorhandenen ETL einen neuen Service Graph Connector (SGC) zu.

Vorbereitungen

Erforderliche Rolle: Administrator

Stellen Sie sicher, dass das erforderliche Service Graph Connector-Plugin aktiviert ist.

Prozedur

1. Navigieren zu **Alle > IntegrationHub ETL** an.
2. Öffnen Sie die duplizierte ETL-Konfiguration.
3. Wählen Sie die Datenquelle des Service Graph Connector aus, und klicken Sie auf **Speichern**.
4. Wählen Sie Aus **Importieren Sie Zeitpläne** Zum Ausführen der ETL zum Transformieren und Laden der Daten aus dem neuen SGC.
5. Überwachen Sie den Ausführungsstatus.

Ergebnisse

Überprüfen Sie, ob CI-Datensätze und -Beziehungen in der CMDB mithilfe von CMDB-Zuordnungen oder Listenansichten erstellt werden.

Erweitern Sie die Unterstützung der TNI-Entität für duplizierte ETLs

Wenn TNI (Telecom Network Inventory) aktiviert ist, muss jedes Configuration Item (CI), das von einer duplizierten ETL erstellt wird, eine entsprechende TNI-Entität aufweisen.

Vorbereitungen

Erforderliche Rolle: Administrator

- Stellen Sie sicher, dass TNI in Ihrer Instanz installiert und aktiv ist.
- Schließen Sie die Duplizierung der ETL des Telecom Discovery Builder-Frameworks im Zielanwendungsbereich ab.

Prozedur

1. Navigieren zu **Alle > IntegrationHub ETL**an.
2. Wählen Sie die CMDB-Anwendung aus, die der duplizierten ETL zugeordnet ist.
Die CMDB Integration Studio-Anwendung auf einer neuen Seite
3. Überprüfen Sie auf der ETL-Konfigurationsseite **Vor Skript Ausführen** Option.
4. Ersetzen Sie das Standardskript durch Folgendes:

```
(function(input, runId) {
    new
    sn_tsom_core.TelcoGenericMappingHelper().checkAndUpdatePayloadForTni(input);
})(input, runId);
```

5. Klicken Sie Auf **Aktualisieren** Um die Änderungen zu speichern.
Das duplizierte ETL verknüpft TNI-Entitäten für erkannte CIs.

Standardisierter allgemeiner JSON-Datensatz zur Unterstützung aller Service Graph Connectors

Verwenden Sie die TSOM-Architektur, um standardisierte Service Graph Connectors mithilfe eines einheitlichen Schemas und einer wiederverwendbaren ETL-Logik zu unterstützen. Dies reduziert die Onboarding-Zeit für neue Connectors und vereinfacht die Integration mit CMDB.

1. Definieren Sie das allgemeine JSON-Schema

Standardisieren Sie die Ausgabe aller Service Graph Connectors, um sie an einem einzigen JSON-Format auszurichten, das dem TNI-Schema entspricht.

Stellen Sie die folgenden Punkte sicher:

1. Implementieren Sie die Konvertierungslogik im Sammler oder Adapter, um Ausgabedaten im allgemeinen Schema auszugeben.
2. Stellen Sie Sicher:
 - Hierarchien „Slot-on-Slot“ oder „Karte auf Karte“ werden ausgeschlossen.
 - Logische Schnittstellen sind deutlich mit gekennzeichnet Virtual=wahr .
 - Gerätetypen sind an Modellklassen-Zuordnungen ausgerichtet.

i Hinweis:

Das Schema sollte die Laufzeitanpassung an TNI-Changes unterstützen, falls verfügbar.

Im Folgenden finden Sie den allgemeinen Datensatz des JSON-Schemas, der alle TSOM-Service Graph-Connectors unterstützt:

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Telco Generic Schema",
  "version": "2.0.1",
  "oneOf": [
    {
      "type": "object",
      "properties": {
        "logical_composites": {
          "type": "array",
          "items": {
            "$ref": "#/$defs/logical_composite"
          }
        }
      },
      "required": [
        "logical_composites"
      ],
      "additionalProperties": false
    },
    {
      "type": "object",
      "properties": {
        "devices": {
          "type": "array",
          "items": {
            "$ref": "#/$defs/device"
          }
        }
      },
      "required": [
        "devices"
      ],
      "additionalProperties": false
    },
    {
      "type": "object",
      "properties": {
        "logical_connections": {
          "type": "array",
          "items": {
            "$ref": "#/$defs/logical_connection"
          }
        }
      },
      "required": [
        "logical_connections"
      ],
      "additionalProperties": false
    },
    {
      "type": "object",
      "properties": {
        "port_relations": {
```

```

    "type": "array",
    "items": {
      "$ref": "#/$defs/port_relation"
    }
  },
  "required": [
    "port_relations"
  ],
  "additionalProperties": false
},
{
  "type": "object",
  "properties": {
    "logical_connection_relations": {
      "type": "array",
      "items": {
        "$ref": "#/$defs/logical_connection_relation"
      }
    }
  },
  "required": [
    "logical_connection_relations"
  ],
  "additionalProperties": false
},
{
  "type": "object",
  "properties": {
    "numbers": {
      "type": "array",
      "items": {
        "$ref": "#/$defs/number"
      }
    }
  },
  "required": [
    "numbers"
  ],
  "additionalProperties": false
},
{
  "type": "object",
  "properties": {
    "topologies": {
      "type": "array",
      "items": {
        "$ref": "#/$defs/network_topology"
      }
    }
  },
  "required": [
    "topologies"
  ],
  "additionalProperties": false
},
{

```

```

    "type": "object",
    "properties": {
      "topology_relations": {
        "type": "array",
        "items": {
          "$ref": "#/$defs/network_topology_relation"
        }
      }
    },
    "required": [
      "topology_relations"
    ],
    "additionalProperties": false
  }
],
"$defs": {
  "keyRef": {
    "type": "object",
    "properties": { "key": { "type": "string" } },
    "required": [ "key" ],
    "additionalProperties": false
  },
  "optionalKeyRef": { "type": [ "object", "null" ],
    "properties": {
      "key": { "type": "string" }
    },
    "additionalProperties": false
  },
  "value": {
    "type": "object",
    "properties": {
      "from": { "type": [ "integer" ], "default": 0, "minimum": 0 },
      "to": { "type": [ "integer" ], "default": 0, "minimum": 0 }
    },
    "required": [ "from", "to" ],
    "additionalProperties": false
  },
  "logical_composite": {
    "type": "object",
    "properties": {
      "class": { "type": "string", "enum": [ "logical_composite" ] },
      "key": { "type": "string" },
      "name": { "type": [ "string", "null" ] },
      "description": { "type": [ "string", "null" ] },
      "devices": { "type": "array", "items": { "$ref": "#/$defs/keyRef" } },
      "power_units": { "type": "array", "items": { "$ref": "#/$defs/pdu" } },
      "fan_shelves": { "type": "array", "items": { "$ref": "#/$defs/fan_shelf" } } },
    "required": [ "key", "name" ]
  },
  "pdu": {
    "type": "object",
    "properties": {
      "class": { "type": "string", "enum": [ "pdu" ] },
      "key": { "type": "string" },
      "name": { "type": [ "string", "null" ] },
      "description": { "type": [ "string", "null" ] },

```

```

    "model_name": { "type": [ "string", "null" ] },
    "model_number": { "type": [ "string", "null" ] },
    "unit_position": { "type": [ "integer", "null" ], "minimum": 1 },
    "slots": { "type": "array", "items": { "$ref": "#/$defs/slot" } }
  },
  "required": [ "key", "name" ]
},
"fan_shelf": {
  "type": "object",
  "properties": {
    "class": { "type": "string", "enum": [ "fan_shelf" ] },
    "key": { "type": "string" },
    "name": { "type": [ "string", "null" ] },
    "description": { "type": [ "string", "null" ] },
    "slots": { "type": "array", "items": { "$ref": "#/$defs/slot" } }
  },
  "required": [ "key", "name" ]
},
"device": {
  "type": "object",
  "properties": {
    "class": { "type": "string", "enum": [ "device" ] },
    "key": { "type": "string" },
    "name": { "type": [ "string", "null" ] },
    "description": { "type": [ "string", "null" ] },
    "ip_address": { "type": [ "string", "null" ] },
    "mac_address": { "type": [ "string", "null" ] },
    "serial_number": { "type": [ "string", "null" ] },
    "model_name": { "type": [ "string", "null" ] },
    "model_number": { "type": [ "string", "null" ] },
    "manufacturer": { "type": [ "string", "null" ] },
    "firmware_version": { "type": [ "string", "null" ] },
    "slots": { "type": "array", "items": { "$ref": "#/$defs/slot" } },
    "ports": { "type": "array", "items": { "$ref": "#/$defs/port" } }
  },
  "required": [ "key", "name", "serial_number" ]
},
"slot": {
  "type": "object",
  "properties": {
    "class": { "type": "string", "enum": [ "slot" ] },
    "key": { "type": "string" },
    "name": { "type": [ "string", "null" ] },
    "description": { "type": [ "string", "null" ] },
    "model_name": { "type": [ "string", "null" ] },
    "model_number": { "type": [ "string", "null" ] },
    "manufacturer": { "type": [ "string", "null" ] },
    "unit_position": { "type": [ "integer", "null" ], "minimum": 1 },
    "cards": { "type": "array", "items": { "$ref": "#/$defs/card" } }
  },
  "required": [ "key", "name" ]
},
"card": {
  "type": "object",
  "properties": {
    "class": { "type": "string", "enum": [ "card" ] },
    "key": { "type": "string" },
    "name": { "type": [ "string", "null" ] },

```

```

    "description": { "type": [ "string", "null" ] },
    "mac_address": { "type": [ "string", "null" ] },
    "serial_number": { "type": [ "string", "null" ] },
    "firmware_version": { "type": [ "string", "null" ] },
    "model_name": { "type": [ "string", "null" ] },
    "model_number": { "type": [ "string", "null" ] },
    "manufacturer": { "type": [ "string", "null" ] },
    "unit_position": { "type": [ "integer", "null" ], "minimum": 1 },
    "slots": { "type": "array", "items": { "$ref": "#/$defs/slot" } },
    "ports": { "type": "array", "items": { "$ref": "#/$defs/port" } }
  },
  "required": [ "key", "name" ]
},
"port": {
  "type": "object",
  "properties": {
    "class": { "type": "string", "enum": [ "port" ] },
    "key": { "type": "string" },
    "name": { "type": [ "string", "null" ] },
    "description": { "type": [ "string", "null" ] },
    "model_name": { "type": [ "string", "null" ] },
    "ip_address": { "type": [ "string", "null" ] },
    "virtual": { "type": "boolean", "default": false },
    "unit_position": { "type": [ "integer", "null" ], "minimum": 1 },
    "bandwidth_name": { "type": [ "string", "null" ] },
    "bandwidth_group": { "type": [ "string", "null" ] },
    "bandwidth": { "type": [ "integer", "null" ], "minimum": 0 },
    "mtu_size": { "type": [ "integer", "null" ], "minimum": 0 }
  },
  "required": [ "key", "name" ]
},
"number": {
  "type": "object",
  "properties": {
    "class": { "type": "string", "enum": [ "number" ] },
    "key": { "type": "string" },
    "name": { "type": [ "string", "null" ] },
    "related_ci_type": { "type": "string", "enum": [ "Network Interface", "Physical Connection",
"Logical Connection", "Equipment", "Topology" ] },
    "related_ci": { "$ref": "#/$defs/keyRef" },
    "type": { "type": "string", "enum": [ "vlan_range", "vlan_subrange", "vlan", "lag_range",
"lag" ] },
    "vlan_type": { "type": "string", "enum": [ "inner", "outer" ] },
    "value": { "$ref": "#/$defs/value" }
  },
  "required": [ "key", "name", "type", "related_ci_type", "related_ci", "value" ] },
"logical_connection": {
  "type": "object",
  "properties": {
    "class": { "type": "string", "enum": [ "logical_connection" ] },
    "key": { "type": "string" },
    "name": { "type": [ "string", "null" ] },
    "description": { "type": [ "string", "null" ] },
    "model_name": { "type": [ "string", "null" ] },
    "bandwidth_group": { "type": [ "string", "null" ] },
    "bandwidth_name_a_to_z": { "type": [ "string", "null" ] },
    "bandwidth_name_z_to_a": { "type": [ "string", "null" ] },

```

```

    "bandwidth_a_to_z": { "type": [ "integer", "null" ], "minimum": 0 },
    "bandwidth_z_to_a": { "type": [ "integer", "null" ], "minimum": 0 },
    "equipment_a": { "$ref": "#/$defs/optionalKeyRef" },
    "equipment_z": { "$ref": "#/$defs/optionalKeyRef" },
    "port_a": { "$ref": "#/$defs/keyRef" },
    "port_z": { "$ref": "#/$defs/keyRef" }
  },
  "required": [ "key", "name", "equipment_a", "equipment_z", "port_a", "port_z" ]
},
"port_relation": {
  "type": "object",
  "properties": {
    "class": { "type": "string", "enum": [ "port_relation" ] },
    "parent": { "$ref": "#/$defs/keyRef" },
    "child": { "$ref": "#/$defs/keyRef" }
  },
  "required": [ "parent", "child" ]
},
"logical_connection_relation": {
  "type": "object",
  "properties": {
    "class": { "type": "string", "enum": [ "logical_connection_relation" ] },
    "sequence": { "type": [ "integer", "null" ], "minimum": 1 },
    "route": { "type": [ "integer", "null" ], "minimum": 1 },
    "parent": { "$ref": "#/$defs/keyRef" },
    "child": { "$ref": "#/$defs/keyRef" }
  },
  "required": [ "parent", "child" ]
},
"network_topology": {
  "type": "object",
  "properties": {
    "class": { "type": "string", "enum": [ "network_topology" ] },
    "key": { "type": "string" },
    "name": { "type": "string" },
    "model_name": { "type": [ "string", "null" ] },
    "devices": { "type": "array", "items": { "key": "#/$defs/optionalKeyRef" } },
    "logical_connections": { "type": "array", "items": { "key": "#/$defs/optionalKeyRef" } }
  },
  "required": [ "key", "name", "devices", "logical_connections" ]
}
}
}

```

2. Entkoppeln Sie die Konnektivität von ETL

Stellen Sie Flexibilität sicher, indem Sie die Interaktionslogik des Geräts von der Transformationslogik (ETL-Erfassung) trennen. Anwender können ihre eigenen Sammler unabhängig von der ETL-Logik entwickeln.

Stellen Sie die folgenden Punkte sicher:

1. Entwerfen Sie Sammler so, dass sie sich nur auf Konnektivität und Datenkonvertierung in das einheitliche Schema konzentrieren.
2. Verwenden oder wiederverwenden Sie einen EMS/NMS-Adapter (einschließlich Adapter von Drittanbietern wie Atrinet).
3. Verschieben Sie die standardisierten Daten in ServiceNow-Importsätze.

3. Konfigurieren Sie generisches ETL für CMDB-Updates

Verwenden Sie eine einzelne wiederverwendbare ETL, um alle standardisierten Importsätze zu verarbeiten und die CMDB genau zu aktualisieren.

Stellen Sie die folgenden Punkte sicher:

1. Validiert, dass der Importsatz Daten im standardisierten JSON-Format enthält.
2. Verwenden Sie die generische TSOM-ETL, um:
 - Erkennen Sie den Entitätstyp (z. B. Steckplatz, Karte, logische Schnittstelle).
 - Ordnen Sie jede Entität basierend auf der Modellzuordnungslogik der richtigen CI-Klasse zu.
 - Füllen Sie ggf. Felder einschließlich Bestandskategorie aus.

Spezielle Bearbeitung:

- Logische Schnittstellen → Porttabelle (Virtual=wahr)
- Logische Verbindungen → Tabelle für logische Verbindungen
- PDU-Karten → PDU-Tabelle
- Gerät → modellbasierte CI-Klasse (neueste Zuordnung, wenn mehrere vorhanden sind)

4. Konfigurieren Sie die Unterstützung für Multi-Chassis- und Composite-Geräte

Modellieren Sie komplexe Geräte wie Router mit mehreren Gehäusen mit richtigen CMDB-Beziehungen.

Stellen Sie die folgenden Punkte sicher:

1. Verwenden Sie das logische zusammengesetzte Konstrukt, um gruppierte Entitäten wie Router + PDU darzustellen.
2. Definieren Sie einzelne Komponenten (Lüfter, Verwaltung, Slot) in ihrer jeweiligen Hierarchie.
3. Ordnen Sie jede Entität gemäß der TNI-Modellierungsanleitung zu.

Beispiel: Für ein 7750-2s-Gerät mit mehreren Gehäusen:

- Logische Zusammensetzung → enthält Router und PDU
- PDU → enthält Steckplätze → Karten → Untersteckplätze

5. Aktivieren Sie die Erstellung von TNI-Entitäten basierend auf der Installation

Stellen Sie die Konsistenz mit TNI-Standards sicher, ohne unnötige Datensatzerstellung.

Stellen Sie die folgenden Punkte sicher:

- Wenn TNI installiert ist:
 - Erstellen Sie automatisch eine TNI-Entität für jedes erkannte CI.
 - Legen Sie die Bestandskategorie entsprechend fest (z. B. „logische Verbindung“, „Schnittstelle“).
- Wenn TNI nicht installiert ist: Überspringen Sie die Erstellung der TNI-Entität, um verwaiste oder ungültige Datensätze zu vermeiden.

Konfigurieren des Nokia Altiplano Service Graph Connector

Konfigurieren Sie den Nokia Altiplano Service Graph Connector, um physische und logische Bestandsdaten aus dem Nokia Altiplano Access Network SDN Controller in Ihre ServiceNow Configuration Management Database (CMDB) zu importieren.

Diese Integration verwendet REST APIs (über einen MID-Server), um sicherzustellen, dass die CMDB genaue, aktuelle Telekommunikationsbestände widerspiegelt, die an dem TM Forum-basierten Datenmodell ausgerichtet sind.

i Hinweis:

Ein gültiger Telecommunications Service Operations Management Zur Verwendung dieses Connectors ist ein Abonnement erforderlich.

Benötigte Plugins

Plugin	ID
Telecom Service Operations Core	sn_tsom_Core
Musterdesigner	com.snc.pattern.designer
Discovery Core (automatisch mit Discovery installiert)	Com.snc.Discovery.Core
ITOM Discovery-Lizenz	com.snc.itom.discovery.license
ITOM-Lizenzierung	com.snc.itom.license
IntegrationHub ETL (nur für Entwicklungsumgebungen)	sn_int_Studio

i Hinweis:

Externe Anforderungen:

- Eine ausgeführte Nokia Altiplano-Controller-Instanz mit Zugriff auf ihre REST-API nach Norden.
- Ein MID-Server mit sicherer Konnektivität zur Altiplano-Instanz.

Übersicht über Konfigurationsaufgaben

Die folgenden Abschnitte sind im Nokia Altiplano-Navigationsbereich verfügbar. Verwenden Sie die folgende Tabelle für das Setup nach der Anleitung oder das Durchführen manueller Konfigurationen.

Abschnitt	Beschreibung
Setup	Konfigurieren Sie DEN MID-Server, definieren Sie Altiplano-Verbindungen, und planen Sie Importe.

Abschnitt	Beschreibung
Datenquellen	Vordefinierte Datenquellen für Massen- und gefilterte Discovery (SGC-Nokia Altiplano Massen-Discovery, SGC-Nokia Altiplano Filtering Discovery). Aktivieren Sie bei Bedarf das parallele Laden. Weitere Informationen zum parallelen Laden finden Sie unter Konfigurieren Sie den gleichzeitigen Import und das parallele Laden für Nokia Altiplano .
Zeitpläne importieren	Verwalten Sie die Planung für jeden Altiplano-Verbindungsalias. Führen Sie Aufträge manuell oder in definierten Intervallen aus.
Aliasse Für Verbindungen Und Anmeldeinformationen	Definieren Sie Aliasse für jede Altiplano-Instanz. Speichern Sie Verbindungsmetadaten und Anmeldeinformationen.
Verbindungen	Definieren Sie Details der Altiplano-Instanz, z. B. URL, ausgewählter MID-Server, Anmeldeinformationsreferenz und Verbindungsalias-Referenz.
Anmeldeinformationen	Erstellen Sie Altiplano-Anmeldeinformationen mit der Standardauthentifizierung.
Filter	Konfigurieren Sie Filterparameter, die in der gefilterten Discovery verwendet werden (z. B. nach Geräte-IP oder -Name).
Eigenschaften	Ändern Sie das Systemverhalten mithilfe von Connector-spezifischen Eigenschaften. Weitere Informationen finden Sie unter Mit Nokia Altiplano installierte Systemkomponenten .

Unterstützte Nokia Altiplano-Versionen

- Unterstützte Mindestversion: 24,6
- Unterstütztes OLT: Lightspan MF-2

Hinweis:

Weitere Informationen finden Sie unter [Zuordnung von Nokia Altiplano-CIs und -Beziehungen in CMDB](#).

Greifen Sie auf das geführte Setup zu

Verwenden Sie das geführte Setup, um den Konfigurationsprozess zu vereinfachen. Dieses Setup bietet eine organisierte Reihenfolge von Schritten, damit Sie die Integration schnell und korrekt abschließen können. So greifen Sie auf das geführte Setup zu:

1. Navigieren zu **Alle > Service Graph Connectors > Nokia Altiplano > Setup**an.
2. Befolgen Sie die Aufgabensequenz, um MID-Server-Einstellungen, Nokia Altiplano-Verbindungen, Filter und Importzeitpläne zu konfigurieren. Weitere Informationen finden Sie unter [Installieren und konfigurieren Sie Nokia Altiplano](#).

Zugehörige Informationen

[Installieren und konfigurieren Sie Nokia Altiplano](#)

[Richten Sie mehrere Nokia Altiplano-Instanzen ein](#)

[Konfigurieren Sie den gleichzeitigen Import und das parallele Laden für Nokia Altiplano](#)

[Zuordnung von Nokia Altiplano-CIs und -Beziehungen in CMDB](#)

[Import für Nokia Altiplano Service Graph Connector ausführen und überprüfen](#)

Mit Nokia Altiplano installierte Systemkomponenten

Telecom Discovery über Nokia Altiplano

Installieren und konfigurieren Sie Nokia Altiplano

Erfahren Sie, wie Sie Service Graph Connector für Nokia Altiplano installieren und konfigurieren, einschließlich optionaler Demodaten, Konnektivitäts-Setup und Zeitpläne für die Datenerfassung.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Bestätigen Sie, dass Sie im Service Graph Connector für den Nokia Altiplano-Anwendungsbereich arbeiten. So wechseln Sie zum Bereich „Service Graph Connector für Nokia Altiplano“:

1. Wählen Sie die Anwendungsauswahl () Im Header.
2. Suchen Sie nach **Nokia Altiplano** .
3. Wählen Sie Service Graph Connector für Nokia Altiplano aus der Liste aus.

Prozedur

1. Navigieren zu **Alle > Service Graph Connectors > Nokia Altiplano > Setup**an.
 2. Wählen Sie auf der Seite „erste Schritte“ die Option aus **Erste Schritte** .
Die Homepage des geführten Setups wird in einer neuen Registerkarte geöffnet.
 3. **Wahlweise:** Erstellen und konfigurieren MID-Server Oder überspringen Sie basierend auf Ihrer Umgebung.
 - a. Wählen Sie Aus **Konfigurieren** Um den Prozess abzuschließen.
 - b. Befolgen Sie zum Herunterladen und Installieren die Anweisungen auf dem Bildschirm.
 - c. Wählen Sie Aus **Als abgeschlossen markieren** Wenn fertig.
-  Hinweis:**
Weitere Informationen zum Installieren und Konfigurieren DES MID-Servers finden Sie unter [Configuring MID Server](#)  .
- d. Konfigurieren Sie den Validierungsschritt, oder überspringen Sie ihn.
 - e. Wählen Sie Aus **Als abgeschlossen markieren** Nach Validierung.
Sobald alle MID-Server-Schritte abgeschlossen sind, fahren Sie mit fort **Konfigurieren Sie Die Konnektivität** .
4. Erstellen Sie Verbindungsaliasse, Anmeldeinformationen und HTTP-Verbindungen mit Ihrer Nokia Altiplano-Instanz **Konfigurieren Sie Die Konnektivität**
 - a. Wählen Sie Aus **Erste Schritte** .
 - b. Erstellen und konfigurieren Sie Aliasse für die Verbindungen und Anmeldeinformationen:

- i. Wählen Sie **Konfigurieren**.
- ii. In **Name** Feld den Aliasnamen angeben.
- iii. Belassen Sie die restlichen Felder als Standard, und wählen Sie aus **Übermitteln** Und dann **Als abgeschlossen markieren**.

i Hinweis:

Dies ermöglicht die Verwendung der Verbindung nach Name und nicht direkt, sodass der Sammler alle aktiven Aliasse aus der CMDB extrahieren und mit der Datensammlung für die daran gebundene HTTP-Verbindung beginnen kann.

- c. Erstellen Sie die Anmeldeinformationen für den Zugriff auf den Nokia Altiplano-Controller, indem Sie auswählen **Konfigurieren**.

- i. In **Name** Feld den Aliasnamen angeben.
- ii. In **Anwendername** Geben Sie den Anwendernamen der Nokia Altiplano-Instanz an.
- iii. In **Passwort** Geben Sie Ihr Passwort für die Nokia Altiplano-Instanz an.

i Hinweis:

Abhängig von den in Ihrer Nokia Altiplano-Instanz verwendeten Authentifizierungsmethoden sind möglicherweise andere Authentifizierungsfelder erforderlich. Standardmäßig verwenden wir [Basic authentication credentials](#) (Als Teil des geführten Setups).

- iv. Belassen Sie die restlichen Felder als Standard, und wählen Sie aus **Übermitteln** Und wählen Sie dann aus **Als abgeschlossen markieren**.

- d. Erstellen Sie eine HTTP-Verbindung, indem Sie auswählen **Konfigurieren**

- i. In **Name** Feld den Verbindungsnamen angeben.
- ii. Wählen Sie aus **Anmeldeinformationen** Und **Verbindungsalias** Zuvor erstellt.
- iii. Geben Sie an **Verbindungs-URL** Für Nokia Altiplano.
- iv. Überprüfen **MID-Server verwenden** Und wählen Sie eine der folgenden Optionen aus:
 - Automatische Auswahl
 - Spezifischer MID-Server
 - Spezifischer MID-Server-Cluster
- v. Belassen Sie die restlichen Felder als Standard, und wählen Sie aus **Übermitteln** Und wählen Sie dann aus **Als abgeschlossen markieren**.

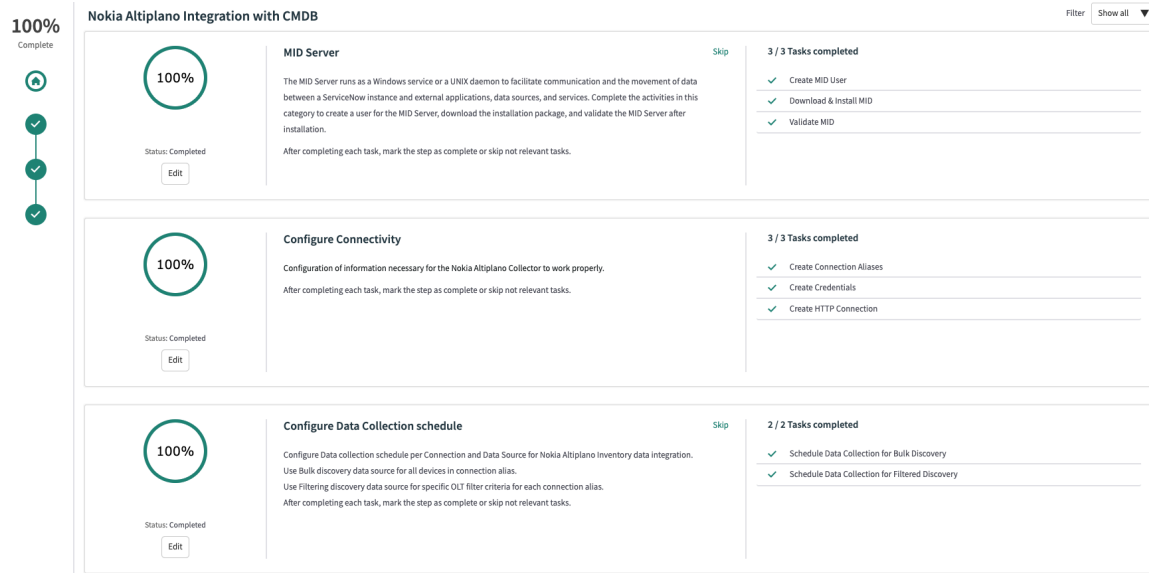
- 5. Konfigurieren Sie den Datensammlungszeitplan entweder für die Massenerkennung oder die gefilterte Discovery, indem Sie auf klicken **Erste Schritte** Und klicken Sie dann auf **Konfigurieren**.

- 6. Wählen Sie Aus **Übermitteln** Und wählen Sie dann aus **Als abgeschlossen markieren**.

Ergebnisse

Auf die konfigurierten Verbindungen, Aliasse, Anmeldeinformationen und Importzeitpläne kann auch über die Navigation zu zugegriffen werden **Alle > Service Graph Connectors > Nokia Altiplano**an.

Der folgende Snapshot hilft Ihnen, die Konfiguration des Nokia Altiplano Service Graph Connector zu bestätigen.



Zugehörige Informationen

[Richten Sie mehrere Nokia Altiplano-Instanzen ein](#)

[Konfigurieren Sie den gleichzeitigen Import und das parallele Laden für Nokia Altiplano](#)

[Zuordnung von Nokia Altiplano-CIs und -Beziehungen in CMDB](#)

[Mit Nokia Altiplano installierte Systemkomponenten](#)

Richten Sie mehrere Nokia Altiplano-Instanzen ein

Erfahren Sie, wie Sie mehrere Nokia Altiplano-Instanzen in einer einzigen ServiceNow-Umgebung konfigurieren und verwalten. Dadurch können Administratoren und Integratoren unabhängige Verbindungsaliasse erstellen und Zeitpläne importieren, die an bestimmte Filter- oder Frequenzanforderungen angepasst sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Bestätigen Sie, dass Sie Folgendes haben:

- Sie arbeiten im Anwendungsbereich Service Graph Connector für NOKIA Altiplano.
- Service Graph Connector für Nokia Altiplano installiert.
- Das geführte Setup für die erste Altiplano-Instanz wurde abgeschlossen.
- MID-Server eingerichtet und validiert.

Sie können zusätzliche Nokia Altiplano-Instanzen konfigurieren oder dieselbe Altiplano-Instanz mit verschiedenen Verbindungsaliasen und Importzeitplänen wiederverwenden. Um eine neue Altiplano-Instanz hinzuzufügen, führen Sie das geführte Setup erneut aus, um einen neuen Verbindungsalias zu konfigurieren. Durchlaufen Sie alle Konnektivitätsphasen im Setup für jeden neuen Alias.

Prozedur

1. Navigieren zu **Alle > Service Graph Connectors > Nokia Altiplano > Setup**an.
2. Wählen Sie auf der Seite „erste Schritte“ die Option aus **Erste Schritte** .
Wiederholen Sie alle Schritte im Abschnitt konfigurierte Konnektivität. Erstellt Konfigurationseinträge für die neue Instanz von Nokia Altiplano. Weitere Informationen finden Sie unter [Installieren und konfigurieren Sie Nokia Altiplano](#).
3. Konfigurieren Sie die Konnektivität, indem Sie einen Verbindungsalias, Anmeldeinformationen und eine HTTP-Verbindung erstellen.
 - a. Wählen Sie im Abschnitt Konnektivität konfigurieren die Option erste Schritte aus.
 - b. Wählen Sie Konfigurieren aus, um einen neuen Verbindungsalias zu erstellen, indem Sie einen eindeutigen Aliasnamen eingeben (z. B. Altiplano_Prod_01).
 - c. Wählen Sie Aus **Übermitteln** Und markieren Sie den Schritt als abgeschlossen.
4. Konfigurieren Sie Anmeldeinformationen für die neue Altiplano-Instanz.
 - a. Geben Sie einen Anwendernamen und ein Passwort für den Altiplano-Controller an.
 - b. Übermitteln Sie den Schritt, und markieren Sie ihn als abgeschlossen.
5. Konfigurieren Sie eine HTTP-Verbindung.
 - a. Geben Sie den Verbindungsnamen an.
 - b. Wählen Sie die neu erstellten Anmeldeinformationen und den Verbindungsalias aus.
 - c. Geben Sie die Verbindungs-URL der Nokia Altiplano-Instanz ein.
 - d. Aktivieren Sie MID-Server verwenden, und wählen Sie die entsprechende MID-Option aus.
 - e. Wählen Sie Aus **Übermitteln** Und markieren Sie den Schritt als abgeschlossen.
6. Planen Sie Datenimporte entweder mit Massen- oder gefilterter Discovery, indem Sie den Importzeitplan konfigurieren.
 - a. Füllen Sie die Felder aus.
Weitere Informationen finden Sie unter [Installieren und konfigurieren Sie Nokia Altiplano](#).
 - b. In **Verbindung verwenden** Wählen Sie die neue Altiplano-Instanz aus.
7. Wählen Sie **Absenden**.

Ergebnisse

Um zu bestätigen, dass das Setup der neuen Instanz erfolgreich ist, können Sie die Konfiguration überprüfen.

- Navigieren Sie zu alle > Service Graph Connectors > Nokia Altiplano > Verbindungsaliasse, und bestätigen Sie, dass der neue Alias aufgelistet ist.
- Navigieren Sie zu alle > Service Graph Connectors > Nokia Altiplano > Importzeitplan, und bestätigen Sie, dass der neue Importzeitplan aufgelistet ist, und bestätigen Sie, dass für jeden Alias entsprechende Aufträge vorhanden sind.

Sie können mehrere Verbindungsaliasse konfigurieren, die mit der Maus auf dieselbe Nokia Altiplano-Instanz zeigen. Diese Flexibilität ermöglicht es Ihnen, Importe mit unterschiedlichen Häufigkeiten auszuführen und auf jeden Alias verschiedene Filter anzuwenden.

Beispiel: Altiplano_Weekly_OLT_10.10.*: Wird wöchentlich ausgeführt, filtert OLTS mit IPs im Bereich 10.10.10.*. Altiplano_Daily_Prod: Wird täglich ausgeführt und filtert OLTS, deren Name „prod_olt“ enthält.

Zugehörige Informationen

[Konfigurieren Sie den gleichzeitigen Import und das parallele Laden für Nokia Altiplano](#)

[Zuordnung von Nokia Altiplano-CIs und -Beziehungen in CMDB](#)

[Mit Nokia Altiplano installierte Systemkomponenten](#)

Konfigurieren Sie den gleichzeitigen Import und das parallele Laden für Nokia Altiplano

Verbessern Sie die Effizienz großer Datenimporte aus Nokia Altiplano, indem Sie gleichzeitige Importe konfigurieren und paralleles Laden aktivieren. Mit dieser Konfiguration kann die Plattform mehrere Datenimport- und -Transformationsaufträge gleichzeitig ausführen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Gleichzeitiges Importieren und paralleles Laden verbessern die Leistung, indem große Datensätze in kleinere Partitionen aufgeteilt werden, sodass mehrere Transformations- und Erfassungsaufträge parallel ausgeführt werden können. Dieses Setup ist nützlich, wenn große Mengen von Geräten, logischen Verbindungen und Netzwerktopologiedaten während Massenerkennungen oder gefilterten Erkennungen importiert werden.

Verwenden Sie die folgende Anleitung, um die Leistung zu optimieren:

- Wenn die Transformation langsam ist: Aktivieren Sie den gleichzeitigen Import im Importzeitplan.
- Wenn die Datensammlung langsam ist: Konfigurieren Sie neben dem Aktivieren des gleichzeitigen Imports das parallele Laden in der Datenquelle, und aktualisieren Sie die Systemeigenschaft.

Hinweis:

Das parallele Laden funktioniert zusätzlich zum gleichzeitigen Import. Er ersetzt ihn nicht.

Prozedur

1. Navigieren zu **Alle > Service Graph Connectors > Nokia Altiplano > Importzeitplan**an.
2. Konfigurieren Sie gleichzeitigen Import oder gleichzeitigen Import

Zugehörige Informationen

[Installieren und konfigurieren Sie Nokia Altiplano](#)

[Zuordnung von Nokia Altiplano-CIs und -Beziehungen in CMDB](#)

[Mit Nokia Altiplano installierte Systemkomponenten](#)

Zuordnung von Nokia Altiplano-CIs und -Beziehungen in CMDB

Verwenden Sie Service Graph Connector für Nokia Altiplano, um erkannte physische und logische Netzwerkressourcen zu CI-Klassen (Telekommunikationsausrichtung Configuration Item) in der CMDB zuzuordnen. Der Connector unterstützt konsistente Servicemodellierung, Transparenz in Komponenten auf Gehäuseebene und Automatisierung logischer und physischer Beziehungen.

Um die genaue CI-Klassifizierung und das Einfügen zu bestätigen, verwendet der Connector die robuste Transformations-Engine (RTE) und die Identification and Reconciliation Engine (IRE).

Der Connector klassifiziert erkannte CIs mithilfe von Telekom-spezifischen Modellen basierend auf Gerätetyp, Funktion und Gehäusestruktur und bezieht sie in Beziehung. Dies trägt dazu bei, eine bereinigte und normalisierte CMDB für alle Lieferanten beizubehalten. Erkannte Modellnamen von Nokia Altiplano werden automatisch in ServiceNow-Standardmodellbezeichner und -Kategorien für Slot- und Subslot-Komponenten umgewandelt.

CI-Zuordnung und -Beziehungen

In den folgenden Tabellen wird beschrieben, wie Altiplano-CIs in der CMDB dargestellt werden und wie sie auf physischen und logischen Ebenen zueinander in Beziehung stehen.

CMDB-CI-Zuordnung und -Beziehungen (physische Ebene)

CI-Typ	CMDB-Tabelle	Beschreibung und Beziehungen
OLT-CI	cmdb_ci_Optical_line_Terminal	Stellt das OLT-Gerät dar. Enthält Slot-CIs und logische Netzwerkschnittstellen-CIs.
ONU/ONT-CI	cmdb_ci_Optical_Network_Terminal Oder cmdb_ci_Optical_Network_unit	Stellt ONU- oder ONT-Geräte dar. Die Klasse wird durch die Systemeigenschaft bestimmt <code>sn_sgc_altiplano.onu_ci_class</code> . Enthält Netzwerkschnittstellen-CIs.
Slot-CI	cmdb_ci_Container_Slot	Stellt Hauptgehäuse-Steckplätze dar. Enthalten in OLT-CIs. Enthält Schnittstellenkarten-CIs (z. B. LT/NT, PSU, Lüfter). Modelltransformationen werden in der Datenquelle angewendet. Weitere Informationen finden Sie in der oben erwähnten Modelltransformation für Slot- und Subslot-CIs-Tabelle.
Subslot-CI	cmdb_ci_Container_subslot	Stellt Unterkomponenten innerhalb von Schnittstellenkarten dar (z. B. Cages für SFPs). Enthalten in LT/NT-Karten. Enthält Transceiver-Karten-CIs. Weitere Informationen finden Sie in der oben erwähnten Modelltransformation für Slot- und Subslot-CIs-Tabelle.
Schnittstellenkarten-CI	cmdb_ci_Interface_Card	Stellt LT/NT-Karten, Transceiver und Steuerungseinheiten dar. Kann Subslots und Netzwerkschnittstellen enthalten.
Netzwerkschnittstellen-CI	cmdb_ci_ni_Interface	Stellt sowohl physische Ports (z. B. PON, Ethernet) als auch logische Ports (z. B. VLAN) dar. Enthalten in Schnittstellenkarten oder ONU/ONT-CIs. Logische Ports beziehen sich auf physische Ports, die Mitglieder::Mitglied von verwenden.
CI für logische Verbindung	cmdb_ci_ni_logical_path	Stellt logische Pfade wie PON oder VLAN zwischen OLT und ONU dar.

CMDB-CI-Zuordnung und -Beziehungen (physische Ebene) (Fortsetzung)

CI-Typ	CMDB-Tabelle	Beschreibung und Beziehungen
		Definiert mit Attributen von Port A und Port Z, die auf beendende Netzwerkschnittstellen-CIs verweisen. VLAN-Pfade verbrauchen PON-Pfade.
IP-Adresse CI	cmdb_ci_ip_address	Stellt erkannte IP-Adressen für OLTS dar. Im Besitz des entsprechenden OLT-CI.

Beispiele Für Schlüsselbeziehungen

- Containment-Beziehungen
 - OLT-CI → enthält Slot-CI
 - Slot-CI → enthält Schnittstellenkarten-CI
 - Schnittstellenkarten-CI → enthält Subslot-CI
 - Subslot-CI → enthält CI der Transceiver-Schnittstellenkarte
 - ONU/ONT CI → enthält Netzwerkschnittstellen-CIs
- Schnittstellenbeziehungen:
 - Logische Verbindungen -> durch Netzwerkschnittstellen beendet
 - Netzwerkschnittstellen:> Mitglieder von Netzwerkschnittstellen
- Logische Pfadbeziehungen:
 - VLAN-Pfad (übergeordnet) → verbraucht → PON-Pfad (untergeordnet)
 - Logische Pfade → beenden bei → Netzwerkschnittstellen-CIs über Port A und Port Z
- Besitz: IP-Adressen-CI → im Besitz des OLT-Geräts

Unterstützte Modelle

- 1. Netzwerkgerätemodelle (sn_ent_nw_Equipment_model)**
 - Das unterstützte OLT ist Nokia Lightspan MF-2, standardmäßig lautet der Modellname „Nokia MF-2“.
 - ONU/ONT-Modelle sind Hersteller + ONU/ONT. Die Systemeigenschaft sn_sgc_altiplano.onu_ci_class definiert, ob ONU oder ONT verwendet wird.
 - Wenn das Modell nicht in der Modelltabelle gefunden wurde, wird im CI ein neues Modell erstellt. Das CI wird als „Netzwerkgerät“ erstellt.
- 2. Gerätehaltermodelle: (sn_ent_nw_holder_model)**
 - Steckplatzmodelle: „Traffic Slot“, „FAN Slot“, „Power Slot“
 - Subslots-Modelle: „SFP-Subslot“
 - Der verwendete Modellname kann vom Kunden über den Altiplano-Erweiterungspunkt (sn_sgc_altiplano.altiplanocustomizedmodels) angepasst werden.
 - Wenn das Modell nicht in der Modelltabelle gefunden wurde, wird im CI ein neues Modell erstellt.
- 3. Netzkartenmodelle (sn_ent_nw_Card_model)**

- Kartenmodelle werden anhand des Modellnamens, des Herstellers und der Modellnummer gefunden, die in der Altiplano-API erkannt wurden
- Wenn das Modell nicht in der Modelltabelle gefunden wurde, wird im CI ein neues Modell erstellt.

4. Netzwerkschnittstellenmodelle: (sn_ent_nw_Interface_model).

- Ethernet-Portmodelle werden in der Spalte „Portbandbreite“ in der Netzwerkschnittstellentabelle (sn_ent_nw_Interface_model) gefunden. Die Portbandbreite des Port-CI wird anhand der erkannten Portgeschwindigkeit in der Tabelle „Bandbreite“ (Bandbreite) ermittelt.
- Modelle für physische PON-Ports: „PON-Zugriffsschnittstelle“, „PON-Netzwerkschnittstellen“
- Logische Portmodelle: „ENET-Schnittstelle“, „VLAN-Schnittstelle“, „lag-Schnittstelle“, „PON-logische Schnittstelle“
- Wenn das Modell nicht in der Modelltabelle gefunden wurde, bleibt der Verweis auf die „Modell-ID“ leer.

5. Logische Netzwerkverbindungsmodelle (sn_ent_logical_nw_connection_model)

- PON-Zugriffspfad
- VLAN-Pfad
- Wenn das Modell nicht in der Modelltabelle gefunden wurde, bleibt der Verweis auf die „Modell-ID“ leer.

i Hinweis:

- Wenn der Connector ein erkanntes Gerät nicht mit einem vorhandenen Modell in der Produktmodelltabelle abgleichen kann, wird das CI als erstellt Netzwerkgerät Standardmäßig.
- Wenn Demodaten installiert sind, werden Standardmodelle für OLT, ONU, ONT, Slots, Subslots erstellt. Karten, Netzwerkschnittstellen und logische Verbindungen.
- Modellnamen für Geräte und Gerätehalter können mithilfe eines Erweiterungspunkts angepasst werden

Modelltransformation für Slot- und Subslot-CIs

Während der Erfassung werden bestimmte erkannte Modellnamen vordefinierten CMDB-Modellbezeichnungen zugeordnet, um eine konsistente Slot-Kategorisierung zu bestätigen. Die Transformationslogik ist in das SGC-Datenquellenskript eingebettet und gilt für die Nokia Altiplano-Quelle.

Steckplatzkomponenten wie Lüfter-, Strom- und Datenverkehrssteckplätze werden dem zugeordnet Slot Kategorie in der CMDB. Subslot-Komponenten wie SFP-Cages oder Synthetic-Subslots werden dem zugeordnet Unterslot Kategorie in der CMDB.

Beispiel: Zuordnungen von Nokia Altiplano-Steckplatz- und Untersteckplatzmodellen

Quelle	Erkannter Modellname	Ziel-CMDB-Modell-ID	Modellkategorie
Altiplano	Slot-Lüfter	Lüftersteckplatz	Slot
Altiplano	Slot-LT	Datenverkehr-Slot	Slot
Altiplano	Käfig	SFP-Subslot	Untersteckplatz

Beispiel: Zuordnungen von Nokia Altiplano-Steckplatz- und Untersteckplatzmodellen (Fortsetzung)

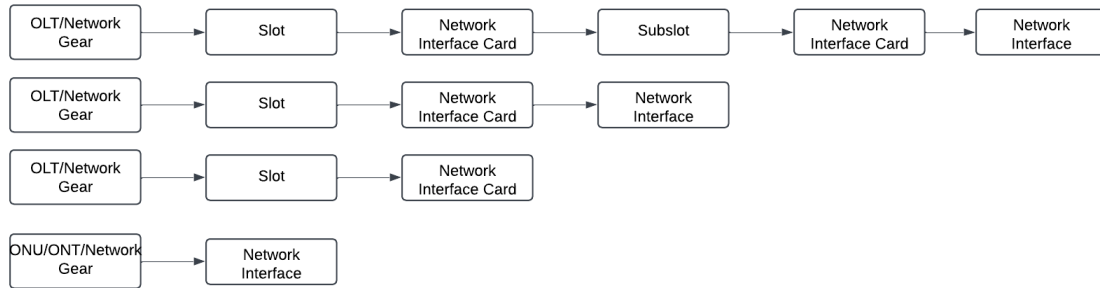
Quelle	Erkannter Modellname	Ziel-CMDB-Modell-ID	Modellkategorie
Altiplano	Slot-NT	Datenverkehr-Slot	Slot
Altiplano	Synthetic NT-Slot	SFP-Subslot	Untersteckplatz
Altiplano	Slot-psu	Stromsteckplatz	Slot

CI-Beziehungsstruktur

Die folgenden Infografiken beschreiben die CI-Beziehungen.

CIs Relationships

Contains::Contained by:



Owns::Owned by (Dependent Relationship)



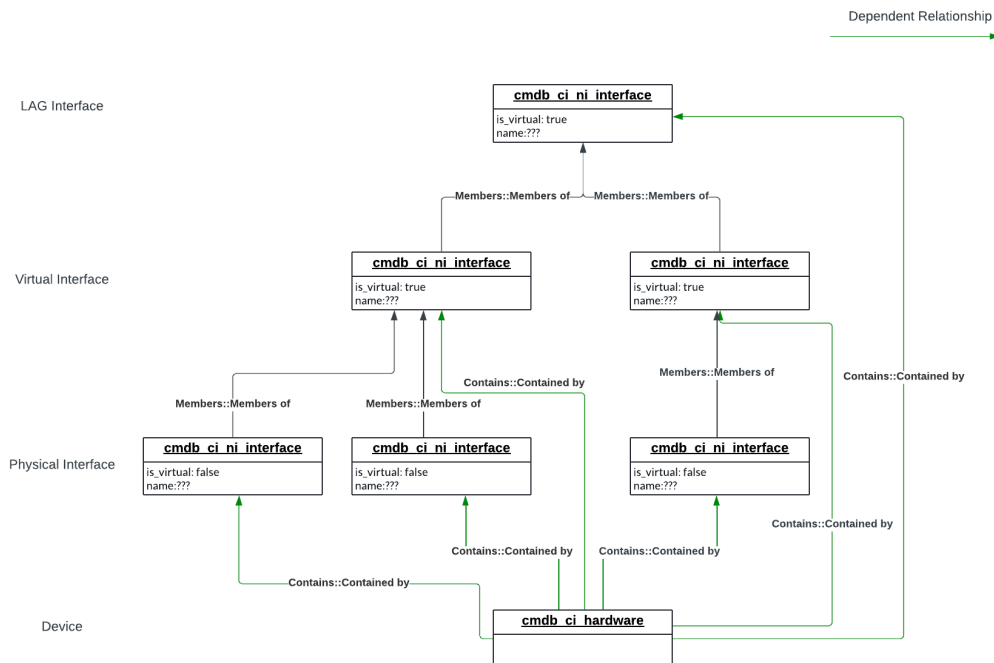
Members::Member of



Consumes::Consumed by

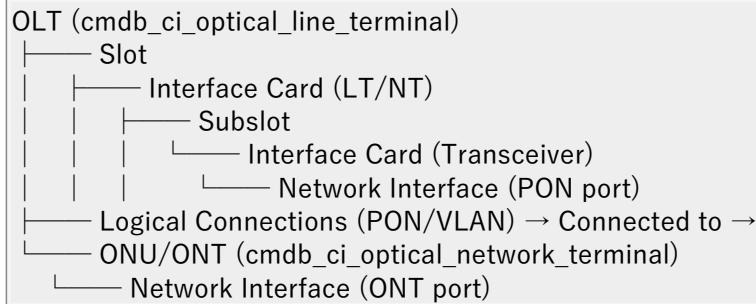


Terminates::Terminated by



Beispiel: OLT-zu-ONU-Struktur

Die folgende Struktur ermöglicht die End-to-End-Rückverfolgbarkeit von OLT über seine Hardwareebenen bis zum verbundenen ONU und den zugehörigen logischen Pfaden.



[store-future: BEGIN review]

Konfigurieren des Nokia NSP-Service Graph-Connectors

Konfigurieren Sie den Nokia NSP Service Graph Connector, um physische und logische Bestandsdaten aus dem Nokia NSP Access Network SDN Controller in Ihre ServiceNow Configuration Management Database (CMDB) zu importieren.

Diese Integration verwendet REST APIs (über einen MID-Server), um sicherzustellen, dass die CMDB genaue, aktuelle Telekommunikationsbestände widerspiegelt, die an dem TM Forum-basierten Datenmodell ausgerichtet sind.

i Hinweis:

Ein gültiger Telecommunications Service Operations Management Zur Verwendung dieses Connectors ist ein Abonnement erforderlich.

Benötigte Plugins

Plugin	ID
Telecom Service Operations Core	sn_tsom_Core
Musterdesigner	com.snc.pattern.designer
Discovery Core (automatisch mit Discovery installiert)	Com.snc.Discovery.Core
ITOM Discovery-Lizenz	com.snc.itom.discovery.license
ITOM-Lizenzierung	com.snc.itom.license
IntegrationHub ETL (nur für Entwicklungsumgebungen)	sn_int_Studio

i Hinweis:

Externe Anforderungen:

- Eine ausgeführte Nokia-NSP-Controller-Instanz mit Zugriff auf ihre REST-API nach Norden.
- Ein MID-Server mit sicherer Konnektivität zur NSP-Instanz.

Übersicht über Konfigurationsaufgaben

Die folgenden Abschnitte sind im Nokia Altiplano-Navigationsbereich verfügbar. Verwenden Sie die folgende Tabelle für das Setup nach der Anleitung oder das Durchführen manueller Konfigurationen.

Abschnitt	Beschreibung
Setup	Konfigurieren Sie DEN MID-Server, definieren Sie Altiplano-Verbindungen, und planen Sie Importe.
Datenquellen	Vordefinierte Datenquellen für Massen- und gefilterte Discovery (SGC-Nokia Altiplano Massen-Discovery, SGC-Nokia NSP Filtering Discovery). Aktivieren Sie bei Bedarf das parallele Laden.
Zeitpläne importieren	Verwalten Sie die Zeitplanung für jeden NSP-Verbindungsalias. Führen Sie Aufträge manuell oder in definierten Intervallen aus.
Aliasse Für Verbindungen Und Anmeldeinformationen	Definieren Sie Aliasse für jede NSP-Instanz. Speichern Sie Verbindungsmetadaten und Anmeldeinformationen.
Verbindungen	Definieren Sie NSP-Instanzdetails, z. B. URL, ausgewählter MID-Server, Anmeldeinformationsreferenz und Verbindungsalias.
Anmeldeinformationen	Erstellen Sie NSP-Anmeldeinformationen mithilfe der Standardauthentifizierung.
Filter	Konfigurieren Sie Filterparameter, die in der gefilterten Discovery verwendet werden (z. B. nach Geräte-IP oder -Name).
Eigenschaften	Ändern Sie das Systemverhalten mithilfe von Connector-spezifischen Eigenschaften. Weitere Informationen finden Sie unter Mit Nokia NSP installierte Systemkomponenten .

Unterstützte Modelle

- Netzwerkschnittstellenmodell
- Produktmodelle
- Modell für logische Verbindungen
- Netzwerktopologiemodell

Wenn ein Gerätemodell fehlt, wird das CI als erstellt **Netzwerkgerät**.

Greifen Sie auf das geführte Setup zu

Verwenden Sie das geführte Setup, um den Konfigurationsprozess zu vereinfachen. Dieses Setup bietet eine organisierte Reihenfolge von Schritten, damit Sie die Integration schnell und korrekt abschließen können. So greifen Sie auf das geführte Setup zu:

1. Navigieren zu **Alle > Service Graph Connectors > Nokia NSP > Setup**.
2. Befolgen Sie die Aufgabensequenz, um MID-Server-Einstellungen, Datenquellen, Anmeldeinformationen, Filter und Importzeitpläne zu konfigurieren. Weitere Informationen finden Sie unter [Installieren und konfigurieren Sie Nokia NSP](#).

[End]

[store-future: BEGIN review]

Installieren und konfigurieren Sie Nokia NSP

Erfahren Sie, wie Sie Service Graph Connector für Nokia NSP installieren und konfigurieren, einschließlich optionaler Demodaten, Konnektivitäts-Setup und Zeitpläne für die Datenerfassung

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Stellen Sie sicher, dass Sie im Anwendungsbereich Service Graph Connector für NOKIA NSP arbeiten. So wechseln Sie zum Bereich „Service Graph Connector für Nokia NSP“:

1. Klicken Sie auf die Anwendungsauswahl () Im Header.
2. Suchen Sie nach **Nokia-NSP** .
3. Wählen Sie Service Graph Connector für Nokia NSP aus der Liste aus.

Prozedur

1. Navigieren zu **Alle > Service Graph Connectors > Nokia NSP > Setup** an.
2. Wählen Sie auf der Seite „erste Schritte“ die Option aus **Erste Schritte** .
Die Homepage des geführten Setups wird in einer neuen Registerkarte geöffnet.
3. **Wahlweise:** Erstellen und konfigurieren MID-Server Oder überspringen Sie basierend auf Ihrer Umgebung
 - a. Wählen Sie Aus **Konfigurieren** Um den Prozess abzuschließen.
 - b. Befolgen Sie zum Herunterladen und Installieren die Anweisungen auf dem Bildschirm.
 - c. Klicken Sie Auf **Als abgeschlossen markieren** Wenn fertig.

(Optional) Weitere Informationen zum Installieren und Konfigurieren DES MID-Servers finden Sie unter [Configuring MID Server](#)  .
 - d. Konfigurieren Sie den Validierungsschritt, oder überspringen Sie ihn.
 - e. Klicken Sie Auf **Als abgeschlossen markieren** Nach Validierung.
Sobald alle MID-Server-Schritte abgeschlossen sind, fahren Sie mit fort **Konfigurieren Sie Die Konnektivität** .
4. Erstellen Sie Verbindungsaliasse, Anmeldeinformationen und HTTP-Verbindungen mit Ihrer Nokia NSP-Instanz **Konfigurieren Sie Die Konnektivität**
 - a. Wählen Sie Aus **Erste Schritte** .
 - b. Erstellen und konfigurieren Sie Aliasse für die Verbindungen und Anmeldeinformationen:
 - i. Wählen Sie **Konfigurieren**.
 - ii. In **Name** Feld den Aliasnamen angeben.
 - iii. Belassen Sie die restlichen Felder als Standard, und wählen Sie aus **Übermitteln** Und dann **Als abgeschlossen markieren** .

i Hinweis:

Dies ermöglicht die Verwendung der Verbindung nach Name und nicht direkt, sodass der Sammler alle aktiven Aliasse aus der CMDB extrahieren und mit der Datensammlung für die daran gebundene HTTP-Verbindung beginnen kann.

- c. Erstellen Sie die Anmeldeinformationen, um auf den Nokia NSP-Controller zuzugreifen, indem Sie auf klicken **Konfigurieren** .

i. In **Name** Feld den Aliasnamen angeben.

ii. In **Anwendername** Geben Sie den Anwendernamen der Nokia NSP-Instanz an.

iii. In **Passwort** Geben Sie Ihr Passwort für die Nokia NSP-Instanz an.

i Hinweis:

Abhängig von den in Ihrer Nokia NSP-Instanz verwendeten Authentifizierungsmethoden sind möglicherweise andere Authentifizierungsfelder erforderlich. Standardmäßig verwenden wir [Basic authentication credentials](#) (Als Teil des geführten Setups).

- iv. Belassen Sie die restlichen Felder als Standard, und wählen Sie aus **Übermitteln** Und klicken Sie dann auf **Als abgeschlossen markieren** .

- d. Erstellen Sie eine HTTP-Verbindung, indem Sie auf klicken **Konfigurieren**

i. In **Name** Feld den Verbindungsnamen angeben.

ii. Wählen Sie aus **Anmeldeinformationen** Und **Verbindungsalias** Zuvor erstellt.

iii. Geben Sie an **Verbindungs-URL** Für Nokia NSP.

- iv. Überprüfen **MID-Server verwenden** Und wählen Sie eine der folgenden Optionen aus:

- Automatische Auswahl
- Spezifischer MID-Server
- Spezifischer MID-Server-Cluster

- v. Belassen Sie die restlichen Felder als Standard, und wählen Sie aus **Übermitteln** Und klicken Sie dann auf **Als abgeschlossen markieren** .

5. Konfigurieren Sie den Datensammlungszeitplan entweder für die Massenerkennung oder die gefilterte Discovery, indem Sie auf klicken **Erste Schritte** Und klicken Sie dann auf **Konfigurieren** .

[End]

[store-future: BEGIN review]

Richten Sie mehrere Nokia NSP-Instanzen ein

Erfahren Sie, wie Sie mehrere Nokia NSP-Instanzen in einer einzigen ServiceNow-Umgebung konfigurieren und verwalten. Dadurch können Administratoren und Integratoren unabhängige Verbindungsaliasse erstellen und Zeitpläne importieren, die an bestimmte Filter- oder Frequenzanforderungen angepasst sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Stellen Sie sicher, dass Sie Folgendes haben:

- Sie arbeiten im Anwendungsbereich Service Graph Connector für NOKIA NSP.
- Service Graph Connector für Nokia NSP installiert.
- Das geführte Setup für die erste NSP-Instanz wurde abgeschlossen.
- MID-Server eingerichtet und validiert.

Sie können zusätzliche Nokia NSP-Instanzen konfigurieren oder dieselbe NSP-Instanz mit verschiedenen Verbindungsaliasen und Importzeitplänen wiederverwenden. Um eine neue NSP-Instanz hinzuzufügen, führen Sie das geführte Setup erneut aus, um einen neuen Verbindungsalias zu konfigurieren. Durchlaufen Sie alle Konnektivitätsphasen im Setup für jeden neuen Alias.

Prozedur

1. Navigieren zu **Alle > Service Graph Connectors > Nokia NSP > Setup** an.
2. Wählen Sie auf der Seite „erste Schritte“ die Option aus **Erste Schritte** .
Wiederholen Sie alle Schritte im Abschnitt konfigurierte Konnektivität. Erstellt Konfigurationseinträge für die neue Instanz von Nokia NSP. Weitere Informationen finden Sie unter [Installieren und konfigurieren Sie Nokia NSP](#).
3. Konfigurieren Sie die Konnektivität, indem Sie einen neuen Verbindungsalias, Anmeldeinformationen und eine HTTP-Verbindung erstellen.
 - a. Klicken Sie im Abschnitt Konnektivität konfigurieren auf erste Schritte.
 - b. Klicken Sie auf Konfigurieren, um einen neuen Verbindungsalias zu erstellen, indem Sie einen eindeutigen Aliasnamen eingeben (z. B. `NSP_Prod_01`).
 - c. Wählen Sie Aus **Übermitteln** Und markieren Sie den Schritt als abgeschlossen.
4. Konfigurieren Sie Anmeldeinformationen für die neue NSP-Instanz.
 - a. Geben Sie Anwendernamen und Passwort für den NSP-Controller an.
 - b. Übermitteln Sie den Schritt, und markieren Sie ihn als abgeschlossen.
5. Konfigurieren Sie die HTTP-Verbindung.
 - a. Geben Sie den Verbindungsnamen an.
 - b. Wählen Sie die neu erstellten Anmeldeinformationen und den Verbindungsalias aus.
 - c. Geben Sie die Verbindungs-URL der Nokia NSP-Instanz ein.
 - d. Aktivieren Sie MID-Server verwenden, und wählen Sie die entsprechende MID-Option aus.
 - e. Wählen Sie Aus **Übermitteln** Und markieren Sie den Schritt als abgeschlossen.
6. Planen Sie Datenimporte entweder mit Massen- oder gefilterter Discovery, indem Sie den Importzeitplan konfigurieren.
 - a. Füllen Sie die Felder aus. weitere Informationen finden Sie unter [Installieren und konfigurieren Sie Nokia NSP](#).
 - b. In **Verbindung verwenden** Wählen Sie die neue NSP-Instanz aus.
7. Wählen Sie **Absenden**.

Ergebnisse

Um zu bestätigen, dass das Setup der neuen Instanz erfolgreich ist, können Sie die Konfiguration überprüfen

- Navigieren Sie zu **alle > Service Graph Connectors > Nokia NSP > Verbindungsaliasse**, und bestätigen Sie, dass der neue Alias aufgelistet ist.
- Navigieren Sie zu **alle > Service Graph Connectors > Nokia NSP > Importzeitplan**, und bestätigen Sie, dass der neue Importzeitplan aufgelistet ist, und stellen Sie sicher, dass für jeden Alias entsprechende Aufträge vorhanden sind.

Sie können mehrere Verbindungsaliasse konfigurieren, die auf dieselbe Nokia NSP-Instanz verweisen. Diese Flexibilität ermöglicht es Ihnen, Importe mit unterschiedlichen Häufigkeiten auszuführen und auf jeden Alias verschiedene Filter anzuwenden.

Zugehörige Informationen

[Telekommunikations-Discovery über Nokia NSP](#)

[Zuordnung von Nokia NSP-CIs und -Beziehungen in CMDB](#)

[End]

[store-future: BEGIN review]

Konfigurieren Sie den gleichzeitigen Import und das parallele Laden für Nokia NSP

Verbessern Sie die Effizienz großer Datenimporte aus Nokia NSP, indem Sie gleichzeitige Importe konfigurieren und paralleles Laden aktivieren. Mit dieser Konfiguration kann die Plattform mehrere Datenimport- und -Transformationsaufträge gleichzeitig ausführen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Gleichzeitiges Importieren und paralleles Laden verbessern die Leistung, indem große Datensätze in kleinere Partitionen aufgeteilt werden, sodass mehrere Transformations- und Erfassungsaufträge parallel ausgeführt werden können. Dieses Setup ist nützlich, wenn große Mengen von Geräten, logischen Verbindungen und Netzwerktopologiedaten während Massenerkennungen oder gefilterten Erkennungen importiert werden.

Verwenden Sie die folgende Anleitung, um die Leistung zu optimieren:

- Wenn die Transformation langsam ist: Aktivieren Sie den gleichzeitigen Import im Importzeitplan.
- Wenn die Datensammlung langsam ist: Konfigurieren Sie neben dem Aktivieren des gleichzeitigen Imports das parallele Laden in der Datenquelle, und aktualisieren Sie die Systemeigenschaft.

Hinweis:

Das parallele Laden funktioniert zusätzlich zum gleichzeitigen Import. Er ersetzt ihn nicht.

Prozedur

1. Navigieren zu **Alle > Service Graph Connectors > Nokia NSP > Importzeitplan**.
2. Konfigurieren Sie gleichzeitigen Import oder gleichzeitigen Import

Zugehörige Informationen

[Installieren und konfigurieren Sie Nokia NSP](#)

[Zuordnung von Nokia NSP-CIs und -Beziehungen in CMDB](#)

[Richten Sie mehrere Nokia NSP-Instanzen ein](#)

[End]

[store-future: BEGIN review]

Zuordnung von Nokia NSP-CIs und -Beziehungen in CMDB

Verwenden Sie Service Graph Connector für Nokia NSP, um erkannte physische und logische Netzwerkressourcen zu CI-Klassen (Configuration Item) in der CMDB zuzuordnen. Der Connector unterstützt konsistente Servicemodellierung, Transparenz in Komponenten auf Gehäuseebene und Automatisierung logischer und physischer Beziehungen.

Um die genaue CI-Klassifizierung und das Einfügen zu bestätigen, verwendet der Connector die robuste Transformations-Engine (RTE) und die Identification and Reconciliation Engine (IRE).

Der Connector klassifiziert erkannte CIs mithilfe von Telekom-spezifischen Modellen basierend auf Gerätetyp, Funktion und Gehäusestruktur und bezieht sie in Beziehung. Dies trägt dazu bei, eine bereinigte und normalisierte CMDB für alle Lieferanten beizubehalten. Erkannte Modellnamen aus Nokia NSP werden automatisch in ServiceNow-Standardmodellbezeichner und -Kategorien für Slot- und Subslot-Komponenten umgewandelt.

CI-Zuordnung und -Beziehungen

In den folgenden Tabellen wird beschrieben, wie NSP-CIs in der CMDB dargestellt werden und wie sie auf physischen und logischen Ebenen zueinander in Beziehung stehen.

CMDB-CI-Zuordnung und -Beziehungen (physische Ebene)

CI-Typ	CMDB-Tabelle	Beschreibung und Beziehungen
IP-Router-CI	cmdb_ci_ip_router	Stellt das IP-Routergerät dar. Enthalten in Netzwerktopologie.enthält Slot-CIs und logische Netzwerkschnittstellen-CIs.
Slot-CI	Slot CICmdb_ci_Container_Slot	Stellt Hauptgehäuse-Steckplätze dar. Enthalten in IP-Router-CIs. Enthält Schnittstellenkarten-CIs.
Subslot-CI	cmdb_ci_Container_subslot	Stellt Unterkomponenten innerhalb der Schnittstelle dar. Enthalten in Schnittstellenkarten. Enthält Transceiver- und Unterkarten-CIs.
Schnittstellenkarten-CI	cmdb_ci_Interface_Card	Stellt Schnittstellenkarten, Transceiver und Steuerungseinheiten dar. Kann Subslots und Netzwerkschnittstellen enthalten.
Netzwerkschnittstellen-CI	cmdb_ci_ni_Interface	Stellt sowohl physische (z. B. Ethernet) als auch logische (z. B. ENET) Ports dar. Enthalten in Schnittstellenkarten oder IP-Router-CIs. Logische Ports beziehen sich auf physische Ports, die Mitglieder::Mitglied von verwenden.
CI für logische Verbindung	cmdb_ci_ni_logical_path	Stellt logische Pfade wie ENET oder lag dar. Definiert mit Attributen von Port A und Port Z,

CMDB-CI-Zuordnung und -Beziehungen (physische Ebene) (Fortsetzung)

CI-Typ	CMDB-Tabelle	Beschreibung und Beziehungen
		die auf beendende Netzwerkschnittstellen-CIs verweisen.
IP-Adresse CI	cmdb_ci_ip_address	Stellt erkannte IP-Adressen für IP-Router dar. Im Besitz des entsprechenden IP-Router-CI.
Netzwerktopologie	cmdb_ci_Network_Topology	Stellt die Netzwerktopologie dar. Enthält IP-Router und logische Verbindungen

Zugehörige Informationen

[Mit Nokia NSP installierte Systemkomponenten](#)

[Konfigurieren des Nokia NSP-Service Graph-Connectors](#)

[End]

Aktivieren Sie die Identifizierung und den Abgleich von Telekommunikationsdiskrepanzen

Aktivieren Sie die Funktion „Identifizierung und Abgleich von Telekommunikationsdiskrepanzen“ (Teil des Plugins „Telecom Visibility“), um die Konsistenz zwischen den im Live-Netzwerk erkannten Telekommunikationsnetzwerkressourcen und den Daten sicherzustellen, die in der CMDB oder im TNI (Telecom Network Inventory) dargestellt werden. Diese Funktion hilft, Diskrepanzen automatisch zu erkennen und zu beheben und unterstützt die Genauigkeit und Datenintegrität in Ihrer Telekommunikationsumgebung.

Vorbereitungen

Erforderliche Rolle: Administrator

Zur Verwendung dieser Funktion muss Ihre Organisation über ein aktives TSOM-Abonnement verfügen. Telecom Discovery, Telecom Visibility und diese Funktion werden zusammen lizenziert.

Warum und wann dieser Vorgang ausgeführt wird

Plugin-Abhängigkeiten: Stellen Sie sicher, dass die folgenden Plugins installiert und aktiviert sind:

Plugin	ID/App-ID	Typ
Telecom Service Operation Core	sn_tsom_Core	Abteilung
CMDB CI Class Models	sn_cmdb_ci_class	Abteilung
Erweiterte Modell- und Asset-Klassen	sn_ent	Abteilung
Sichtbarkeitsinhalt	sn_pattern_Design	Abteilung
Gemeinsame Komponenten für CMDB-Integrationen	sn_cmdb_int_util	Abteilung
Discovery-Core	Com.snc.Discovery.Core	Familie
ITOM Discovery-Lizenz	com.snc.itom.discovery.license	Familie
ITOM-Lizenzierung	com.snc.itom.license	Familie

Prozedur

1. Stellen Sie sicher, dass das Plugin sn_tsom_Core automatisch installiert wird, wenn Sie Telecommunications Discovery-Muster oder Nokia Altiplano Service Graph Connector installieren.
2. Stellen Sie sicher, dass die genannten abhängigen Plugins aktiviert sind.

Zugehörige Informationen

[Diskrepanzidentifizierung: Arten von Diskrepanzen](#)

[Mit Telecom Discrepcy Identification and Reconciliation installierte Systemkomponenten](#)

[Identifizierung und Abgleich von Telekommunikationsdiskrepanzen](#)

[Führen Sie ein Audit für Telekommunikationsdiskrepanzen aus](#)

[Steuern Sie CI-Attributaktualisierungen mithilfe von Abgleichsregeln](#)

Filter für Audit konfigurieren

Definieren Sie Filterbedingungen, um den Umfang von Audits für Telekommunikationsdiskrepanz zu steuern. Diese Filter stellen sicher, dass Audits nur für den gewünschten Satz von CIs ausgeführt werden, wodurch die Leistung und die Genauigkeit der Zielvorgaben verbessert werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Filterbedingungen in Telekommunikations-Diskrepanz-Audits verstehen

- Audits verwenden Filterbedingungen, um den Umfang der auszuwertenden CIs einzugrenzen.
- Filterbedingungen sind wichtig, um Audit-Ziele einzugrenzen.
- Sie können Bedingungen pro Audit-Instanz definieren und ändern, um bestimmte Audit-Anforderungen zu erfüllen.
- Wird gefiltert nach Discovery_Source Ist eine allgemeine Bedingung zum Filtern von Datensätzen, die bestimmten Integrationsquellen zugeordnet sind (z. B. TSOM und Altiplano). Darüber hinaus können Sie den Filter an die Audit-Anforderungen anpassen.
- Jede Version des Audits kann eine andere Filterbedingung haben.

Im Folgenden sind die Audit-Filter aufgeführt:

1. Audit für Diskrepanz logischer Verbindungen in der Telekommunikation: Dieses Audit wird in der Tabelle für logische Verbindungen ausgeführt. Die Standardfilterbedingung ist definiert als Discovery_Source Gefällt TSOM. Diese Bedingung wird auf jedes CI in der Tabelle für logische Verbindungen angewendet.
2. Audit für Diskrepanz der Telecom-Netzwerktopologie: Dieses Audit wird in der Netzwerktopologietabelle ausgeführt. Die Standardfilterbedingung ist definiert als Discovery_Source Gefällt TSOM. Diese Bedingung wird auf jedes CI in der Netzwerktopologietabelle angewendet.
3. Audit der Telekommunikationsdiskrepanz: Dieses Audit wird in der Tabelle „Beziehungen“ ausgeführt. Die Standardfilterbedingung ist definiert als Discovery_Source Gefällt TSOM. Diese Bedingung wird auf jedes CI auf Geräteebeane angewendet.

Der folgende Screenshot hilft, die Anwenderoberfläche des Zertifizierungsfilters zu verstehen

Number: CFLR0010004 Active

Name: Filter for TSOM Logical Connections Discrepancy Audit

Description: Filter for TSOM Logical Connections Discrepancy Audit

Table: Configuration Item [cmdb_ci] Version: 2

Filter condition: No. of records matching the condition: 1

Add Filter Condition Add OR Clause

All of these conditions must be met

Discovery source contains TSOM AND OR

Name is pon_path_PON_L_GPON AND OR

Update

Related Links

Delete inactive versions

Other Versions Version Search

Name	Description	Table	Version
Filter for TSOM Logical Connections Disc...	Filter for TSOM Logical Connections Disc...	Configuration Item [cmdb_ci]	1

1 to 1 of 1

Prozedur

1. Navigieren zu **Alle > Zertifizierung > Filter** an.
2. Wählen Sie **Neu**.
Die Zertifizierungsfilterschnittstelle wird angezeigt.
3. Füllen Sie die Felder aus.
Weitere Anleitungen finden Sie unter [Create a certification filter](#).
4. Fügen Sie die Filterbedingungen hinzu.
Beispielsweise enthält die Discovery-Quelle TSOM.
5. Wählen Sie **Absenden**.
Der Filter wird erstellt.

Ergebnisse

Sie können den Filter im Audit logischer Verbindungen verwenden.

Zugehörige Informationen

- [Führen Sie ein Audit für Telekommunikationsdiskrepanzen aus](#)
- [Beispiel für Audit und Korrektur von Telekommunikationsdiskrepanzen](#)
- [Mit Telecom Discrepacy Identification and Reconciliation installierte Systemkomponenten](#)
- [Konfigurieren Sie die Diskrepanz des Attributwerts in CMDB 360](#)
- [Steuern Sie CI-Attributaktualisierungen mithilfe von Abgleichsregeln](#)

Konfigurieren Sie die Diskrepanz des Attributwerts in CMDB 360

Konfigurieren Sie Attributvergleichseinstellungen in CMDB 360, um Dateninkonsistenzen in mehreren Discovery-Quellen zu erkennen.

Vorbereitungen

Erforderliche Rolle: Administrator

Bestätigen Sie, dass CMDB 360 in Ihrer Instanz aktiviert und konfiguriert ist.

Warum und wann dieser Vorgang ausgeführt wird

Der folgende Screenshot kann Ihnen helfen, die Felder einzurichten, um die Diskrepanz zu

identifizieren.

Prozedur

1. Navigieren Sie zur Tabelle **Alle > cmdb_Multisource_column_metadata.list** an.
2. Wählen Sie Aus **Neu** Zum Erstellen eines neuen Datensatzes.
3. In **Spalte mit mehreren Quellen** Feld das zu vergleichende Attribut auswählen.
4. Wählen Sie die Tabelle aus, um die Attribute mit den Feldern zu vergleichen.

i Hinweis:

Wenn die gewünschte Tabelle nicht aufgeführt ist, wählen Sie die Tabellenbezeichnung aus, halten Sie sie gedrückt (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie aus **Konfigurieren Sie Wörterbuch**.

5. **Wahlweise:** Gehen Sie wie folgt vor, um einen Wörterbucheintrag zu konfigurieren.
 - a. Wählen Sie im Wörterbucheintrag die Option aus **Anzeigen** Und wählen Sie dann aus **Erweitert**.
 - b. In **Attribute** Feld, legen Sie die Attribute als fest Base_Start=wahr Und Allow_public=wahr.

Ergebnisse

Sie können die konfigurierten Attribute in der CMDB 360-Abfrage verwenden.

Zugehörige Informationen

[Steuern Sie CI-Attributaktualisierungen mithilfe von Abgleichsregeln](#)

[Generieren Sie Berichte für Diskrepanzen bei Attributwerten](#)

Steuern Sie CI-Attributaktualisierungen mithilfe von Abgleichsregeln

Um zu verhindern, dass bestimmte Attribute eines Konfigurationselements (Configuration Item, CI) von Discovery oder anderen Datenquellen überschrieben werden, verwenden Sie Abgleichsregeln. Diese Regeln definieren, welche Datenquelle vertrauenswürdig ist, um ein bestimmtes Attribut zu aktualisieren, wenn mehrere Quellen Werte bereitstellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Abgleichsregeln werden von der Identification und Reconciliation Engine (IRE) verarbeitet und sind für die Aufrechterhaltung der Datenintegrität in der CMDB unerlässlich.

Anwendungsfall: Wenn Sie verhindern möchten, dass Discovery einen Satz von Attributen aktualisiert, während Sie zulassen möchten, dass eine andere Quelle (z. B. SCCM oder manuelle Eingabe) sie aktualisiert, definieren Sie eine Regel, die die Discovery-Quelle ausschließt.

i Hinweis:

Nur eine Abgleichsregel darf für eine bestimmte CI-Klasse und -Attributkombination aktiv sein, um Konflikte zu vermeiden.

Prozedur

1. Navigieren zu **Alle > CI-Klassen Manager** an.
2. Wählen Sie die Ziel-CI-Klasse aus (z. B. cmdb_ci_Computer).
3. In **Abgleichsregeln** klicken Sie auf die Registerkarte **Neu** Dient zum Erstellen einer Regel.
4. Geben Sie den Regelnamen an, und wählen Sie die Discovery-Quelle aus, auf die die Regel angewendet werden soll.
5. Geben Sie die Attribute an, die diese Regel steuert.
6. Legen Sie die Quellpriorität so fest, dass nur die ausgewählten Quellen die angegebenen Attribute aktualisieren können.

Ergebnisse

Bestimmte CI-Attribute werden nicht mehr von nicht vertrauenswürdigen Datenquellen oder Datenquellen mit niedrigerer Priorität wie Discovery aktualisiert. Nur die in der Regel definierten Quellen (z. B. SCCM, manuelle Updates) dürfen diese Attribute aktualisieren.

Zugehörige Informationen

[Konfigurieren Sie die Diskrepanz des Attributwerts in CMDB 360](#)

Telecommunications Service Operations Management verwenden

Nutzen Telecommunications Service Operations Management(TSOM) zur proaktiven Überwachung von Telekommunikationsservices, zur Validierung der Datenintegrität und zum Abgleich von Diskrepanzen in Netzwerkbestands- und Discovery-Quellen. TSOM ermöglicht Betriebsteams, eine genaue CMDB mit Telekommunikationsbezug zu verwalten und auf Echtzeiteinblicke in Netzwerke zu reagieren.

Allgemeine operative Aufgaben von TSOM

Sobald TSOM konfiguriert ist, können Sie die Funktionen für Folgendes verwenden:

- Audits für Telekommunikationsdiskrepanz ausführen: Identifizieren Sie Inkonsistenzen in Netzwerkbeziehungen und -Konfigurationen, indem Sie Zertifizierungsaudits basierend auf erkannten Daten und Abgleichsregeln ausführen.
- Nichtübereinstimmungen von Attributwerten in CMDB 360 validieren: Verwenden Sie die Funktion „Attributwertdiskrepanz“ in CMDB 360, um Attributwerte in verschiedenen Discovery-Quellen zu vergleichen und Konflikte oder veraltete Datensätze zu erkennen.
- Telecom Discovery-Muster verwenden: Wenden Sie Telecom Discovery-Muster an, um Telekommunikationsspezifische Konfigurationselemente (Configuration Items, CIs) und ihre Beziehungen genau zu erkennen und auszufüllen.
- Importaufträge aus Service Graph Connectors ausführen und überprüfen: Importzeitpläne manuell auslösen (z. B. für den Nokia Altiplano-Connector), um sicherzustellen, dass Topologie- und Gerätedaten erfolgreich in die CMDB importiert und den richtigen CI-Klassen zugeordnet wurden.

Diese Aufgaben tragen dazu bei, sicherzustellen, dass Ihr Telekommunikationsnetzwerk kontinuierlich synchronisiert, genau und in ServiceNow operativ sichtbar ist.

Verwenden von Telecom Discovery-Mustern

Verwenden Sie Telecom Discovery-Muster, um Netzwerkfunktionen (xNFs) von Lieferantengeräten wie Routern, Cisco und Juniper zu identifizieren und zu klassifizieren. Nutzen Sie die musterbasierte Discovery, um Telekommunikationsressourcen der CMDB zuzuordnen.

Klassifizieren von xNFs für Telekommunikations-Routermuster

Um auf eine vollständige Liste der zu klassifizierenden OIDs zuzugreifen.

Vorbereitungen

Erforderliche Rolle: Administrator

Klassifizierername: **Standard-Netzwerkrouter** .

Prozedur

1. Navigieren zu **Alle > Discovery-Definition > CI-Klassifizierung > SNMP**an.
2. Wählen Sie in der Liste aus **Standard-Netzwerkrouter** .
3. Öffnen Sie die Registerkarte **SNMP-OID-Klassifizierungen**Und sehen Sie sich die Liste der OIDs an.

The screenshot displays the 'SNMP Classification' configuration page for 'Standard Network Router'. The configuration includes fields for Name, Active status, Order, Table, Match criteria, Manufacturer, and Model. Below these fields is a section for 'On classification script' with a sample script: '1 // This script gets run when something gets classified'. At the bottom, the 'Related Links' section shows 'Run Point Scan'. The 'Classification Criteria (1)' tab is selected, showing a table of OIDs and their associated details.

OID	Operator	Table	Manufacturer	Model	Active
1.3.6.1.4.1.141.1.1.3220	Is	IP Router [cmdb_ci_ip_router]	NetScout Systems, Inc.	Packet Probe 3220	true
1.3.6.1.4.1.94.1.2.1.2	Is	IP Router [cmdb_ci_ip_router]	Nokia	IP4xx	true
1.3.6.1.4.1.9.1.2411	Is	IP Router [cmdb_ci_ip_router]	Cisco Systems	ciscoNC5501	true
1.3.6.1.4.1.664.1.466	Is	IP Router [cmdb_ci_ip_router]	Adtran	NETVANTA3205	true
1.3.6.1.4.1.43.1.16.4.2.12	Is	IP Router [cmdb_ci_ip_router]	Hewlett-Packard	R6080	true
1.3.6.1.4.1.9.1.758	Is	IP Router [cmdb_ci_ip_router]	Cisco Systems	1250	true
1.3.6.1.4.1.9.1.1448	Is	IP Router [cmdb_ci_ip_router]	Cisco Systems	ciscoAS5515K7xc	true
1.3.6.1.4.1.2636.1.1.2.24	Is	IP Router [cmdb_ci_ip_router]	Juniper Networks	J2350	true
1.3.6.1.4.1.2636.1.1.1.2.5	Is	IP Router [cmdb_ci_ip_router]	Juniper Networks	M5	true

Hinweis:

Weitere Informationen zum Hinzufügen zusätzlicher OIDs zur Klassifizierung finden Sie unter [Leiten Sie die Discovery mithilfe von Discovery-Mustern](#).

In einer xNF verwendete MIB-Tabellen:

- SystemMIB
- EntitätPhysikalMIB
- IfMIB
- IfXMIB
- IpMIB

Klassifizieren von xNFs für Cisco 7613-Routermuster für Telekommunikation

Um auf eine vollständige Liste der zu klassifizierenden OIDs zuzugreifen.

Vorbereitungen

Erforderliche Rolle: Administrator

Klassifizierername: **Standard-Netzwerkrouter**.

Prozedur

1. Navigieren zu **Alle > Discovery-Definition > CI-Klassifizierung > SNMP** an.
2. Wählen Sie in der Liste aus **Standard-Netzwerkrouter**.
3. Öffnen Sie die Registerkarte **SNMP-OID-Klassifizierungen** und sehen Sie sich die Liste der OIDs an.

After the Sensor processes the results of the SNMP - Classify Probe, secondary to SNMP System OIDs, each SNMP Classification defines the order, match criteria, and Probes to trigger. [More Info](#)

Name: Standard Network Router
 Active: ☒
 Order: 20
 Table: IP Router
 Match criteria: All
 Manufacturer:
 Model:

On classification script

```
// This script gets run when something gets classified
```

Update Delete

Related Links
 Run Point Scan

Classification Criteria (1) **SNMP-OID-Klassifizierungen (199)** Triggers probes (3) Versions (8)

for test Search

Actions on selected rows... New Sync Candidates Sync From CDS

Classifier - Standard Network Router	Old	Operator	Table	Manufacturer	Model	Active
☐	1.3.6.1.4.1.141.1.1.3220	Is	IP Router [cndb_ci_ip_router]	NetScout Systems, Inc.	Packet Probe 3220	true
	1.3.6.1.4.1.94.1.2.1.2.1.2	Is	IP Router [cndb_ci_ip_router]	Nokia	IP4ox	true
	1.3.6.1.4.1.9.1.2411	Is	IP Router [cndb_ci_ip_router]	Cisco Systems	ciscoNCS5011	true
	1.3.6.1.4.1.664.1.466	Is	IP Router [cndb_ci_ip_router]	Adtran	NETVANTA3205	true
	1.3.6.1.4.1.43.1.16.4.2.12	Is	IP Router [cndb_ci_ip_router]	Hewlett-Packard	R6080	true
	1.3.6.1.4.1.9.1.758	Is	IP Router [cndb_ci_ip_router]	Cisco Systems	1250	true
	1.3.6.1.4.1.9.1.1448	Is	IP Router [cndb_ci_ip_router]	Cisco Systems	ciscoASA5515K79c	true
	1.3.6.1.4.1.2636.1.1.1.2.24	Is	IP Router [cndb_ci_ip_router]	Juniper Networks	J2350	true
	1.3.6.1.4.1.2636.1.1.1.2.5	Is	IP Router [cndb_ci_ip_router]	Juniper Networks	M5	true

i Hinweis:

Weitere Informationen zum Hinzufügen zusätzlicher OIDs zur Klassifizierung finden Sie unter [Leiten Sie die Discovery mithilfe von Discovery-Mustern](#).

Die Liste der spezifischen OIDs zum Aufrufen dieses Musters:

Lieferant	Modell	OID	Muster
Cisco	7613	1.3.6.1.4.1.9.1.528	Cisco 7613-Router Für Telekommunikation

In einer xNF verwendete MIB-Tabellen:

- SystemMIB
- EntitätPhysikalMIB
- IfMIB
- IfXMIB
- IpMIB

Klassifizieren von xNFs für Telecom Juniper MX SSH-Routermuster

Um auf eine vollständige Liste der zu klassifizierenden OIDs zuzugreifen.

Vorbereitungen

Erforderliche Rolle: Administrator

Klassifizierername: **Standard-Netzwerkrouter**.

Prozedur

1. Navigieren zu **Alle > Discovery-Definition > CI-Klassifizierung > SNMP**an.
2. Wählen Sie in der Liste aus **Standard-Netzwerkrouter**.
3. Öffnen Sie die Registerkarte **SNMP-OID-Klassifizierungen** und sehen Sie sich die Liste der OIDs an.

After the Sensor processes the results of the SNMP - Classify Probe, secondary to SNMP System OIDs, each SNMP Classification defines the order, match criteria, and Probes to trigger. [More Info](#)

Name: Standard Network Router
 Active: ☒
 Order: 20
 Table: IP Router
 Match criteria: All
 Manufacturer:
 Model:

On classification script

```
1 // This script gets run when something gets classified
```

Update Delete

Related Links
[Run Point Scan](#)

Classification Criteria (1) **SNMP OID Classifications (379)** Triggers probes (3) Versions (8)

Classifier: Standard Network Router

Old	Operator	Table	Manufacturer	Model	Active
1.3.6.1.4.1.141.1.1.3220	Is	IP Router [cndb_ci_ip_router]	NetScout Systems, Inc.	Packet Probe 3220	true
1.3.6.1.4.1.94.1.21.2.1.2	Is	IP Router [cndb_ci_ip_router]	Nokia	IP4xx	true
1.3.6.1.4.1.9.1.2411	Is	IP Router [cndb_ci_ip_router]	Cisco Systems	ciscoNC55011	true
1.3.6.1.4.1.664.1.466	Is	IP Router [cndb_ci_ip_router]	Adtran	NETVANTA3205	true
1.3.6.1.4.1.43.1.16.4.2.12	Is	IP Router [cndb_ci_ip_router]	Hewlett-Packard	R6080	true
1.3.6.1.4.1.9.1.758	Is	IP Router [cndb_ci_ip_router]	Cisco Systems	1250	true
1.3.6.1.4.1.9.1.1448	Is	IP Router [cndb_ci_ip_router]	Cisco Systems	ciscoASA5515K7sc	true
1.3.6.1.4.1.2636.1.1.1.2.24	Is	IP Router [cndb_ci_ip_router]	Juniper Networks	J2350	true
1.3.6.1.4.1.2636.1.1.1.2.5	Is	IP Router [cndb_ci_ip_router]	Juniper Networks	M5	true

i Hinweis:

Weitere Informationen zum Hinzufügen zusätzlicher OIDs zur Klassifizierung finden Sie unter [Leiten Sie die Discovery mithilfe von Discovery-Mustern](#).

Die Liste der spezifischen OIDs zum Aufrufen dieses Musters:

Lieferant	Modell	OID	Muster
Juniper	MX80	1.3.6.1.4.1.2636.1.1.1.2.57	Telecom Juniper MX SSH-Router
Juniper	MX104	1.3.6.1.4.1.2636.1.1.1.2.97	Telecom Juniper MX SSH-Router
Juniper	MX240	1.3.6.1.4.1.2636.1.1.1.2.29	Telecom Juniper MX SSH-Router
Juniper	MX480	1.3.6.1.4.1.2636.1.1.1.2.25	Telecom Juniper MX SSH-Router

MIB-Tabellen, die in einer xNF verwendet werden: SystemMIB.

Verwendete CLI-Befehle.

- Gehäuse-Hardware anzeigen | nicht mehr | XML anzeigen
- Schnittstellenmedien anzeigen | nicht mehr | XML anzeigen

Klassifizieren von xNFs für Cisco-Switch-Muster für Telekommunikation

Um auf eine vollständige Liste der zu klassifizierenden OIDs zuzugreifen.

Vorbereitungen

Erforderliche Rolle: Administrator

Klassifizierername: **Standard-Netzwerk-Switch**.

Prozedur

1. Navigieren zu **Alle > Discovery-Definition > CI-Klassifizierung > SNMP**an.
2. Wählen Sie in der Liste aus **Standard-Netzwerk-Switch**.
3. Öffnen Sie die Registerkarte **SNMP-OID-Klassifizierungen** und sehen Sie sich die Liste der OIDs an.

The screenshot shows the ServiceNow configuration page for an SNMP Classifier named 'Standard Network Switch'. The configuration includes fields for Name, Active status, Order, Table (IP Switch), Match criteria (All), Manufacturer, and Model. Below these is a section for 'On classification script' with a code editor containing a comment: '// This script gets run when something gets classified'.

Below the configuration is a table of 'SNMP OID Classifications' with the following data:

OID	Operator	Table	Manufacturer	Model	Active
1.3.6.1.4.1.1916.2.98	Is	IP Switch [cnmdb_ci_ip_switch]	Extreme Networks	SUMMITX250-24XDC	true
1.3.6.1.4.1.14179.2.2.1.1.22.57	Is	IP Switch [cnmdb_ci_ip_switch]	Airspaces, Inc	Cisco 1830 Unified Access Point	true
1.3.6.1.4.1.9.1.1071	Is	IP Switch [cnmdb_ci_ip_switch]	Cisco Systems	ciscoPwrC3900Poe	true
1.3.6.1.4.1.6527.6.2.1.2.1	Is	IP Switch [cnmdb_ci_ip_switch]	Alcatel-Lucent Enterprise	7210 SAS-E	true
1.3.6.1.4.1.25506.1.246	Is	IP Switch [cnmdb_ci_ip_switch]	Hewlett-Packard	H3C S3100-26TP-EI	true
1.3.6.1.4.1.25506.1.38	Is	IP Switch [cnmdb_ci_ip_switch]	Hewlett-Packard	H3C S3600-52P-EI	true
1.3.6.1.4.1.9.1.1637	Is	IP Switch [cnmdb_ci_ip_switch]	Cisco Systems	ciscoE1400	true
1.3.6.1.4.1.25506.1.654	Is	IP Switch [cnmdb_ci_ip_switch]	H3C Technologies	S3100V2-16TP-SI	true
1.3.6.1.4.1.1991.1.3.39.1	Is	IP Switch [cnmdb_ci_ip_switch]	Brocade Communications Systems	Netron IMR 640 Switch	true
1.3.6.1.4.1.2.6.157	Is	IP Switch [cnmdb_ci_ip_switch]	IBM	8275-416	true

Hinweis:

Weitere Informationen zum Hinzufügen zusätzlicher OIDs zur Klassifizierung finden Sie unter [Leiten Sie die Discovery mithilfe von Discovery-Mustern](#).

Die Liste der spezifischen OIDs zum Aufrufen dieses Musters:

Lieferant	Modell	OID	Muster
Cisco	Nexus 9000	1.3.6.1.4.1.9.12.3.1.3.1954	Cisco-Switch Für Telekommunikation
Cisco	Nexus 3548	1.3.6.1.4.1.9.12.3.1.3.1666	Cisco-Switch Für Telekommunikation

In einer xNF verwendete MIB-Tabellen:

- SystemMIB
- EntitätPhysikalMIB
- IfMIB
- IfXMIB
- IpMIB

Klassifizieren von xNFs für Telekommunikations-Switch-Muster

Um auf eine vollständige Liste der zu klassifizierenden OIDs zuzugreifen.

Vorbereitungen

Erforderliche Rolle: Administrator

Klassifizierername: **Standard-Netzwerk-Switch** .

Prozedur

1. Navigieren zu **Alle > Discovery-Definition > CI-Klassifizierung > SNMP** an.
2. Wählen Sie in der Liste aus **Standard-Netzwerk-Switch** .
3. Öffnen Sie die Registerkarte **SNMP-OID-Klassifizierungen** und sehen Sie sich die Liste der OIDs an.

The screenshot shows the ServiceNow configuration page for a 'Standard Network Switch' classification. The top section shows the configuration form with fields for Name, Active, Order, Table, Match criteria, Manufacturer, and Model. Below this is a section for 'On classification script' with a code editor containing a comment: '// This script gets run when something gets classified'. The bottom section shows a table of 'SNMP OID Classifications' with columns for Old, Operator, Table, Manufacturer, Model, and Active. The table lists various OIDs and their corresponding manufacturers and models.

Old	Operator	Table	Manufacturer	Model	Active
1.3.6.1.4.1.1916.2.98	Is	IP Switch [cndb_ci_ip_switch]	Extreme Networks	SUMMITX250-24XDC	true
1.3.6.1.4.1.14179.2.1.1.22.57	Is	IP Switch [cndb_ci_ip_switch]	Airespace, Inc	Cisco 1830i Unified Access Point	true
1.3.6.1.4.1.9.1.1071	Is	IP Switch [cndb_ci_ip_switch]	Cisco Systems	ciscoPwrC3900Poe	true
1.3.6.1.4.1.6527.6.2.1.2.1	Is	IP Switch [cndb_ci_ip_switch]	Alcatel-Lucent Enterprise	7210 SAS-E	true
1.3.6.1.4.1.25506.1.246	Is	IP Switch [cndb_ci_ip_switch]	Hewlett-Packard	H3C S3100-26TP-EI	true
1.3.6.1.4.1.25506.1.38	Is	IP Switch [cndb_ci_ip_switch]	Hewlett-Packard	H3C S3600-52P-EI	true
1.3.6.1.4.1.9.1.1637	Is	IP Switch [cndb_ci_ip_switch]	Cisco Systems	ciscoE140D	true
1.3.6.1.4.1.25506.1.654	Is	IP Switch [cndb_ci_ip_switch]	H3C Technologies	S3100V2-16TP-SI	true
1.3.6.1.4.1.1991.1.3.39.1	Is	IP Switch [cndb_ci_ip_switch]	Brocade Communications Systems	NetIron IMR 640 Switch	true
1.3.6.1.4.1.2.6.157	Is	IP Switch [cndb_ci_ip_switch]	IBM	8275-416	true

i Hinweis:

Weitere Informationen zum Hinzufügen zusätzlicher OIDs zur Klassifizierung finden Sie unter [Leiten Sie die Discovery mithilfe von Discovery-Mustern](#).

In einer xNF verwendete MIB-Tabellen:

- SystemMIB
- EntitätPhysikalMIB
- IfMIB

Automatische Übersetzung

- IfXMIB
- IpMIB

Import für Nokia Altiplano Service Graph Connector ausführen und überprüfen

Führen Sie einen konfigurierten Importzeitplan für den Nokia Altiplano Service Graph Connector manuell aus. Sie können den Import auch ausführen, um das Connector-Setup zu validieren, Ad-hoc-Importe auszuführen oder neu konfigurierte Verbindungsaliasse zu testen. Diese Aufgabe hilft sicherzustellen, dass Daten aus Altiplano erfolgreich in die CMDB importiert oder aktualisiert werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie den Nokia Altiplano Service Graph Connector konfiguriert und einen oder mehrere Importzeitpläne eingerichtet haben, können Sie einen Importauftrag ausführen. Mit dieser Aufgabe können Sie überprüfen, ob die Integration wie erwartet funktioniert und ob CIs erfolgreich in die CMDB importiert oder aktualisiert wurden.

Sie können entweder aktivieren, dass die Importzeitpläne automatisch basierend auf ihrer definierten Häufigkeit ausgeführt werden, oder sie manuell für die sofortige Ausführung und Validierung auslösen.

i Hinweis:

Wenn Sie mehrere Altiplano-Verbindungsaliasse (für verschiedene Umgebungen oder Filter) konfiguriert haben, vergewissern Sie sich, dass der Importzeitplan für jeden Alias korrekt eingerichtet ist.

Der folgende Screenshot hilft Ihnen, den geplanten Datenimport-Prozess zu verstehen und zeigt die Ausführungen in Form von Importsätzen an.

Scheduled Data Import
Altiplano bulk

Name: Altiplano bulk

Data source: SGC-Nokia Altiplano Bulk Discovery

Run as: [User]

Active: ☒

Use connection: ☒

Connection: sn_sgc_altiplano.Altiplano1

Concurrent Import: ☐

Execute pre-import script: ☐

Execute post-import script: ☐

Application: Service Graph Connector for NOKIA Altiplano

Run: Daily

Time: Hours 00, 00, 00

Conditional: ☐

Buttons: Execute Now, Update, Delete

Related Links: View Dashboard, Run Point Scan, [SN Utils] Versions (4)

Number	Execution Context	Import Set	Created
EXE00001043	EC00001043	Import Set: ISET0010043	2025-07-13 00:00:00
EXE00001042	EC00001042	Import Set: ISET0010042	2025-07-12 23:36:01
EXE00001040	EC00001040	Import Set: ISET0010040	2025-07-12 00:00:00

Prozedur

1. Navigieren zu **Alle > Nokia Altiplano > Zeitpläne importieren** an.
2. Wählen Sie den Importzeitplan aus, den Sie ausführen möchten.
Die Liste der geplanten Datenimporte wird angezeigt.

3. Wählen Sie den geplanten Datenimport aus.
4. Führen Sie einen der folgenden Schritte aus:
 - Wenn der Zeitplan ist **Aktiv**, Der Auftrag wird automatisch im definierten Intervall ausgeführt. Warten Sie also, bis sie ausgeführt wird.
 - Wählen Sie Aus **Jetzt Ausführen** Um den Import sofort auszuführen.
5. So überwachen Sie die Ausführung und überprüfen die Ergebnisse:
 - a. Scrollen Sie nach unten zu **Ausführungen** Liste oder Tabelle, die mit dem Importzeitplan verknüpft ist.
 - b. Öffnen Sie die neueste **Importsatz** Von der Ausführung erstellter Datensatz.
6. Überprüfen Sie das Importsatzprotokoll, um die Anzahl der gelesenen Zeilen, die Anzahl der in die CMDB eingefügten oder aktualisierten Zeilen oder den Status des Transformationserfolgs zu überprüfen.
7. **Wahlweise:** Navigieren zu **Alle > CMDB > CI-Klassen** Oder Ihre anwenderdefinierten Telekommunikationstabellen (z. B. TNI-Basiselement), um zu bestätigen, dass die CIs wie erwartet erstellt oder aktualisiert wurden.

Ergebnisse

Der Importzeitplan wird sofort ausgeführt, und Sie können die Ausführung des Importsatzes und die entsprechenden CI-Updates in der CMDB überprüfen. Wenn er richtig konfiguriert ist, übernimmt der Connector die Netzwerkbestandsdaten aus Nokia Altiplano in Ihre ServiceNow-Instanz.

Beispiel: Nach Ausführung des Importzeitplans:

- Das Protokoll zeigt: „12 Zeilen gelesen, 0 eingefügt/aktualisiert“. Dies gibt an, dass CIs vorhanden sind.
- Wenn Sie vorhandene CIs löschen und den Import erneut ausführen, werden im Protokoll möglicherweise mehrere Einfügungen und Aktualisierungen angezeigt, die die End-to-End-Funktionalität validieren.

i Hinweis:

- Wenn **Gleichzeitiger Import** Die Option ist im Importzeitplan aktiviert. Datensätze werden in angezeigt **Gleichzeitiger Importsatz** Tabelle anstelle der standardmäßigen Importsatztabelle.
- Jeder gleichzeitige Auftrag erstellt einen eigenen Importsatz und einen Protokolleintrag. Die Struktur der Ausführungsdatensätze bleibt unverändert.

Zugehörige Informationen

[Konfigurieren des Nokia Altiplano Service Graph Connector](#)

[Telecom Discovery über Nokia Altiplano](#)

Validieren von JSON-Nutzlasten mit TSOM-Schemaprüfung

Verwenden Sie die Dienstprogrammklasse TsomSchemaValidator, um JSON-Nutzlasten anhand von TSOM-Schemas zu validieren, bevor Sie Daten importieren. Dies hilft, Fehler frühzeitig zu identifizieren, ETL-Fehler zu reduzieren und die Datenqualität zu bestätigen.

Verwenden Sie diese Validierung, um zu überprüfen, ob Ihre JSON-Nutzlasten dem erwarteten Schema für Telekommunikationsobjekte wie Geräte, logische Verbindungen und Topologien entsprechen, bevor Sie Importsätze erstellen. Dieser Vorvalidierungsschritt hilft, Fehler bei der Schemabeinstimmung zu verhindern und das Debugging zu verbessern.

Unterstützte Schematypen

Die Validierung unterstützt mehrere Schematypen für verschiedene Telekommunikationsdatenstrukturen:

- Logische Zusammensetzungen: Stellt Gruppierungen von Komponenten dar: Geräte, PDUs, Lüfterregale
- Geräte: Geräte und ihre enthaltenen Komponenten
- Logische Verbindungen: Verbindungen zwischen Netzwerkschnittstellen
- Portbeziehungen: Beziehungen zwischen Netzwerkschnittstellen: Physisch, logisch, Verzögerungen
- Logische Verbindungsbeziehungen: Beziehungen zwischen logischen Verbindungen
- Topologien: Netzwerktopologie

Klassenstruktur

```
let TsomSchemaValidator = Class.create();
TsomSchemaValidator.prototype = {
  initialize: function() {
    this.schemas = new TsomGenericSchema();
  },
  isValidJson: function(payload) {
    // Validation logic that determines if the JSON structure is valid
    // Returns boolean (true/false)
  },
  checkJsonValidation: function(payload) {
    // Validation logic that determines if the JSON structure is valid
    // Returns a JSON object containing errors (if exist)
  },
  type: 'TsomSchemaValidator'
};
```

Schritte

1. Instanzieren Sie das Schema ValidatorjavascriptCopyEdit

```
var TsomSchemaValidator = new sn_tsom_core.TsomSchemaValidator();
```

2. Führen Sie eine boolesche Validierungsprüfung aus

```
if (!TsomSchemaValidator.isValidJson(target_json)) {
  gs.error('Invalid JSON: ' + JSON.stringify(target_json));
  return;
}
```

3. Führen Sie eine detaillierte Validierungsprüfung aus

```
let result = TsomSchemaValidator.checkJsonValidation(target_json);
if (!result.valid) {
  gs.error('Invalid JSON: ' + JSON.stringify(result, null, 2));
  return;
}
```

Beispielausgabe

Example Output

```
{
  "schemaName": "devices",
  "errors": [
    {
      "message": "Missing required property: model_name",
      "params": { "key": "model_name" },
      "code": 302,
      "dataPath": "/devices/0/ports/0",
      "schemaPath": "/properties/devices/items/properties/ports/items/required/4"
    }
  ],
  "valid": false
}
```

Zugehörige Informationen

[Konfigurieren der ETL des Telecom Discovery Builder-Frameworks in einem Connector](#)

[Telecom Discovery Builder-Framework](#)

Führen Sie ein Audit für Telekommunikationsdiskrepanzen aus

Das Audit der Telekommunikationsdiskrepanz validiert die Integrität von Konfigurationselementen (Configuration Items, CIs) und Beziehungen in Ihrem Telekommunikationsbestand mithilfe des CMDB-Compliance-Frameworks.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Das Audit der Telekommunikationsdiskrepanz ist Teil des CMDB-Compliance-Frameworks und unterstützt phasenbasierte Audits, um Diskrepanzen in CI-Beziehungen und -Attributen zu erkennen und zu beheben, die über ServiceNow Discovery oder Service Graph Connectors (z. B. Nokia Altiplano) erkannt wurden.

Sie können das Audit manuell ausführen oder so festlegen, dass es in regelmäßigen Abständen ausgeführt wird. Während der manuellen Ausführung können Sie aus vorhandenen Filtern auswählen, um den Audit-Umfang auf bestimmte CIs zu beschränken – hilfreich für Tests oder gezielten Abgleich.

Das Audit der Telekommunikationsdiskrepanz funktioniert in zwei Phasen:

1. Erste Compliance-Ausführung: Validiert CI-Beziehungen und ausgewählte CI-Tabellen anhand der folgenden Standardkriterien:
 - Unterstützte CI-Klassen: Steckplatz, Untersteckplatz, Karte, Schnittstelle, Netzwerkgerät (enthält alle Erweiterungstabellen).
 - Quelle: CI wurde über Discovery erkannt (z. B. `Discovery_Source = SG-TSOM-Altiplano`).
 - Beziehungstyp: Enthält::Enthalten In (Anpassbar über `sn_tsom_core.audit.relationship_types` Eigenschaft).

- Nachfolgende Compliance-Ausführungen: Bewertet zusätzlich zu den ersten Prüfungen, ob der aktualisierte Zeitstempel der Beziehung oder der zugehörigen CIs aktueller ist als das Datum der letzten Ausführung im Audit-Datensatz.

Hinweis:

Jedes fehlgeschlagene Audit erstellt eine Folgeaufgabe für die manuelle oder automatisierte Korrektur, wobei bestätigt wird, dass CMDB-Daten für Telekommunikation am Netzwerkstatus ausgerichtet bleiben.

Der folgende Screenshot hilft Ihnen, das Audit der Telekommunikationsdiskrepanz zu

The screenshot shows the configuration page for the 'Telecom Discrepancy Audit' in ServiceNow. The page includes the following fields and options:

- Name:** Telecom Discrepancy Audit
- Filter:** Filter for TSOM Discrepancy Audit - 1
- Table:** Configuration Item [cmdb_ci]
- Application:** Telecom Service Operations Core
- Active:** ☒
- Run:** On Demand
- Last run date:** 2025-06-30 04:07:00
- Create tasks:** ☒
- Assignment type:** User Field
- Assign to:** Assigned to
- Assign to empty:** Create Unassigned Task
- Audit type:** Scripted
- Short description:** Telecom CMDB Discrepancy Audit
- Task description:** Remedy the discrepancies listed in the Audit Results below
- Run this script:** Turn on ECMAScript 2021 (ES12) mode

The script editor shows the following code:

```

1  /* global gs, current, SNC, CertificationProcessing, TsonDiscrepancyAudit, GlideDateTime */
2
3  var certProcessor;
4  if (gs.getCurrentScopeName().includes("global"))
5      certProcessor = new SNC.CertificationProcessing();
6  else
7      certProcessor = new CertificationProcessing();
8
9  //
10 let tsonDiscrepancyAudit = new TsonDiscrepancyAudit();
11 tsonDiscrepancyAudit.printInfoLog("Audit Started.");
12 let auditStartDate = new GlideDateTime();
13 auditStartDate.addSeconds(-1); // change the audit start time to 1 second before the current time, so that
14   relationships added at the current time will be picked up later.
15 let lastAuditRunDate = current.last_run_date.toString();
16 let auditId = current.sys_id;
17 tsonDiscrepancyAudit.initAudit(auditId, certProcessor);
    
```

verstehen.

Prozedur

- Navigieren zu **Alle > Compliance > Audits**
- Öffnen Sie den Datensatz Telecom Discrepancy Audit (Tabelle cert_Audit).
- Wahlweise:** Wählen Sie einen Filter aus.
 - Wenn während der Konfiguration mehrere Audit-Filter definiert wurden, können Sie einen auswählen, bevor Sie das Audit ausführen.
 - Mit Filtern können Sie den Audit-Umfang basierend auf Kriterien wie Discovery-Quelle, CI-Klasse oder bestimmten CI-Attributen einschränken.
 - Dieser Schritt ist besonders nützlich, wenn Sie eine Teilmenge von Datensätzen beheben oder bestimmte Discovery-Ergebnisse validieren.
- Führen Sie einen der folgenden Schritte aus, um das Audit auszuführen.
 - Klicken Sie Auf **Audit Ausführen** Zum Auslösen einer manuellen Ausführung.
 - Konfigurieren Sie das Audit so, dass es geplant ausgeführt wird, indem Sie eine wiederkehrende Aufgabe einrichten.

Das Audit verwendet CMDB-Compliance, um die Beziehung und CI-Integrität im gesamten Telekommunikationsbestand zu validieren.

Ergebnisse

Überprüfen Sie die Audit-Ergebnisse

- Das Audit identifiziert Compliance-Fehler, z. B. fehlende Beziehungen oder falsch ausgerichtete Attribute.
- Für jeden fehlgeschlagenen Audit-Datensatz wird automatisch eine Folgeaufgabe generiert.
- Aufgaben umfassen empfohlene oder automatisierte Korrekturaktionen wie das Aktualisieren oder Außerbetriebnahme von CIs.

Beispiel-Anwendungsfall: Die konfigurierten Filter können für verschiedene Discovery-Quellen verwendet werden. Zum Beispiel Nokia Altiplano. Wenn Sie das Audit manuell ausführen, können Sie den entsprechenden Filter auswählen, um nur die von dieser bestimmten Quelle erkannten CIs zu validieren. Dies bestätigt ein gezieltes und effizientes Auditing.

Zugehörige Informationen

[Filter für Audit konfigurieren](#)

[Beispiel für Audit und Korrektur von Telekommunikationsdiskrepanzen](#)

Beispiel für Audit und Korrektur von Telekommunikationsdiskrepanzen

Das folgende Beispiel veranschaulicht, wie das Audit in einem Szenario funktioniert.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Eine Karte (Card04) wurde anfänglich in Slot04 erkannt. Später wurde Card04 im physischen Netzwerk durch Card05 ersetzt, aber die CMDB zeigt Card04 weiterhin in Slot04 an. Wenn eine neue Discovery-Ausführung ausgeführt wird, wird Card05 erkannt und demselben Steckplatz hinzugefügt, wodurch ein Datenkonflikt in CMDB entsteht.

Audit-Verhalten:

- Das Audit für Telekommunikationsdiskrepanz erkennt diese Inkonsistenz und erstellt einen fehlgeschlagenen Audit-Datensatz (z. B. AUDR0001283).
- Eine Folgeaufgabe wird automatisch erstellt (z. B. TASK0020215) Mit einer detaillierten Beschreibung der Diskrepanz.

Beispiel für Aufgabenbeschreibung (falsche Anzahl von Beziehungen):

Card04 wurde zuletzt vor mehr als 2,5 Tagen erkannt.

Beziehungen zwischen den folgenden CIs

CI	Modell
Slot04	DEMO 20532Tree
Kart04	NOKIA 7360 FANT-F-KARTENMODUL
Karte05	<Modell nicht identifiziert>

Die folgenden Snapshots helfen Ihnen, den Diskrepanz- und Korrekturprozess zu verstehen.

[Run Audit](#)

Related Links
[View Dashboard](#)
[Run Point Scan](#)

Audit Results (45) | Follow On Tasks (39)

Number Search Actions on selected rows...

Created	Document	State	Column name	Desired value	Discrepancy value	Follow on task	Number	Template	Threshold	Stability
2024-11-26 04:34:33	Configuration Item: Card40	Failed	Most recent discovered date	is not within threshold 2024-11-25 00:59:44	2024-11-22 00:59:45	TASK0020215	AUDR0001283	(empty)	Pending	Pending

UI Actions Order Search Actions on selected rows... New

Name	Table	Comments	Form action	List action	Active	Order	Condition	Updated
Follow On Task	Follow On Task (next_follow_on_task)		true	false	true		1,000 new Task Remediation() performed state Conf...	2024-11-21 08:27:48

SM Service-nov: Yaron Nechushtan [maint... Work notes • 2024-11-26 04:37:39

TSOM CI Decommission
 =====
 Card: Card40

LCS set to 'End of life'
 LCSS set to 'Retired'

Relationships removed:
 Slot40 ==> Card40

SA System Administrator Field Changes • 2024-11-26 04:34:33

Description Card40 was last discovered more than 2.5 days ago.
 Relationships between the following CIs:
 CI: Slot40 (8b2beb4247ceda10f04f83ac416d4398), Model: DEMO 20532Tree (1ba577524c1b3110f8772646dabeb9bb),
 CI: Card40 (0b2beb4247ceda10f04f83ac416d4399), Model: Nokia 7360 FANT-F CARD MODULE
 (3af9617de5928110f877657a333391e0),
 CI: Card41 (832beb4247ceda10f04f83ac416d439a), Model: ()

SA System Administrator Field Changes • 2024-11-26 04:34:32

Active	true
Audit	Service Operation CIMDB Compliance Audit
Configuration item	Card40
Impact	3 - Low
Number	TASK0020215
Opened by	System Administrator
Priority	4 - Low
Short description	Most recent discovery date not within configured threshold.
State	Open

Prozedur

1. Navigieren **Alle > Compliance > Audits > Audit Der Telekommunikationsdiskrepanz > Führen Sie Audits Aus**an.

Für jeden fehlgeschlagenen Audit-Datensatz wird automatisch eine Folgeaufgabe erstellt (z. B. TASK0020215).

2. Wählen Sie Aus **TASK0020215** Und überprüfen Sie die Diskrepanzbeschreibung.

i Hinweis:

Dies ist ein Beispiel für die TASK0020215-Beschreibung, die für das Szenario „falsche Anzahl von Beziehungen“ erstellt wurde. Andere Szenarien und Umgebungen können unterschiedliche Beschreibungen haben.

Die Folgeaufgabe enthält eine detaillierte Beschreibung der Diskrepanz. Wie Sie in der Beschreibung sehen können, weist das Card04-CI Diskrepanz auf.

3. Führen Sie die folgenden Schritte aus, um eine Korrektur vorzunehmen:

a. Navigieren **Alle > Systemdefinition > UI-Aktionen**an.

b. Wählen Sie **Beheben** aus.

Die Schaltfläche „Nachbesserung“ ist eine UI-Aktion, die auslöst TSOM-CI-Außerbetriebnahme subflow. Dieser Subflow:

- Legt das veraltete Card04-CI fest.
- Entfernt die falsche Slot04 → Card04-Beziehung.
- Synchronisiert CMDB-Datensätze mit dem Netzwerkstatus.

Ergebnisse

Nach der Korrektur:

- Die Folgeaufgabe (TASK0020215) Wird mit Arbeitsnotizen aktualisiert, die die Lösungsschritte zusammenfassen.
- Das Card04-CI ist als deaktiviert markiert, und falsche Beziehungen werden entfernt.
- CMDB ist jetzt an dem zuletzt erkannten Status aus dem Netzwerk ausgerichtet.

Hinweis:

Korrektur anpassen: Das Audit für Telekommunikations-Diskrepanz wird mit Beispiel-Subflows für Korrektur geliefert. Mit Flow Designer können Sie anwenderdefinierte Subflows erstellen und anhängen, die Ihren betrieblichen Anforderungen entsprechen.

Zugehörige Informationen

[Identifizierung und Abgleich von Telekommunikationsdiskrepanzen](#)

[Diskrepanzidentifizierung: Arten von Diskrepanzen](#)

[Mit Telecom Discrepcy Identification and Reconciliation installierte Systemkomponenten](#)

[Aktivieren Sie die Identifizierung und den Abgleich von Telekommunikationsdiskrepanzen](#)

[Defining UI actions](#) 

Generieren Sie Berichte für Diskrepanzen bei Attributwerten

Verwenden Sie CMDB 360, um Berichte zu generieren, die Diskrepanzen in Attributwerten zwischen verschiedenen Discovery-Quellen oder zwischen einer Discovery-Quelle und der CMDB-Baseline hervorheben.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Attributwert-Diskrepanzberichte helfen bei der Identifizierung in Konflikt stehender Daten aus mehreren Quellen, die dasselbe Konfigurationselement (CI) aktualisieren. Dies ermöglicht eine bessere Datenqualität und -Integrität in Ihrer CMDB.

Prozedur

1. Navigieren zu **Alle > CMDB-Arbeitsbereich > CMDB 360**an.
2. Wählen Sie Aus **Erstellen Sie Eine Abfrage** .
3. Wählen Sie im Fenster Abfragetyp die Option aus **Attributwerte vergleichen** .
4. Definieren Sie die Abfrageparameter:
 - a. Wählen Sie Aus **CI-Klasse** Sie möchten analysieren (z. B. cmdb_ci_Computer).
 - b. Wenden Sie Filter an, um den Umfang einzugrenzen (z. B. enthält die Discovery-Quelle „TSOM“).
 - c. Wählen Sie Attribute aus, um Werte in verschiedenen Discovery-Quellen zu vergleichen.
 - d. Wählen Sie die zu vergleichenden Quellen aus (z. B. Discovery, SCCM).

e. Wahlweise: Wählen Sie Aus **Mit CMDB vergleichen** Dient zum Vergleichen von Discovery-Quelldaten mit der aktuellen CMDB-Baseline.

f. Klicken Sie Auf **Speichern** , Geben Sie einen Namen für die Abfrage an, und klicken Sie dann auf **Ausführen** Um die Ergebnisse zu generieren.

5. Wahlweise: Klicken Sie Auf **Zeitplan** Um die Abfrage so einzurichten, dass sie in definierten Intervallen ausgeführt wird.

Ergebnisse

Der Bericht zeigt einen Vergleich von Attributwerten über Quellen hinweg an:

- Quelle 1: Aktueller CMDB-Datensatz.
- Wert der Quelle 1: Wert, der von der neuesten Discovery-Quelle aktualisiert wurde.
- Quelle 2: Vorherige Discovery-Quelle.
- Wert der Quelle 2: Wert, der von der früheren Discovery-Quelle bereitgestellt wurde.

Jede Diskrepanz wird als separater Datensatz aufgeführt, wenn ein CI von mehreren Quellen aktualisiert wurde.

Zugehörige Informationen

[Konfigurieren Sie die Diskrepanz des Attributwerts in CMDB 360](#)

[Steuern Sie CI-Attributaktualisierungen mithilfe von Abgleichsregeln](#)

Telecommunications Service Operations Management – Referenz

Mit werden verschiedene Arten von Komponenten installiert Telecommunications Service Operations Management Anwendungen und Plugins.

Mit Benachrichtigungen der Telekommunikations-API installierte Systemkomponenten

Administratoren können Anwenderrollen zuweisen, um Zugriff auf die Tabellen der API-Benachrichtigungsdatenbank zu gewähren. Die folgenden Standardrollen für die Tabellen „Thema“ [sn_api_notif_mgmt_topic] und „Themenabonnement“ [sn_api_notif_mgmt_Subscription] sind in enthalten ServiceNow System.

Benachrichtigungsrollen der Telekommunikations-API

Rolle	Beschreibung
sn_api_notif_mgmt.topic_Subscription_Viewer	Rolle, die Lesezugriff auf die Tabellen „Thema“ und „Themenabonnement“ ermöglicht.
sn_api_notif_mgmt.topic_Creator	Rolle, die den Zugriff auf die Thementabelle erstellen, lesen und bearbeiten ermöglicht.
sn_api_notif_mgmt.Subscription_Creator	Rolle, die den Erstellungs- und Lesezugriff auf die Tabelle „Themenabonnement“ ermöglicht.
sn_api_notif_mgmt.Subscription_admin	Rolle, die mit den folgenden Berechtigungen aktiviert:

Benachrichtigungsrollen der Telekommunikations-API (Fortsetzung)

Rolle	Beschreibung
	• Erstellen Sie Lesezugriff auf die Tabellen „Thema“ und „Themenabonnement“. • Ändern Sie den Status der Registrierung, um die Registrierung eines Themenabonnements aufzuheben.

Zugehörige Informationen

[Externes Ereignismanagement über Benachrichtigungen der Telekommunikations-API](#)

[Konfigurieren von Telekommunikations-API-Benachrichtigungen](#)

Mit Nokia Altiplano installierte Systemkomponenten

Systemeigenschaften steuern, wie der Connector funktioniert, einschließlich Discovery-Optionen und Leistungseinstellungen.

Mit Nokia Altiplano installierte Eigenschaften

Eigenschaft	Beschreibung
<code>sn_sgc_altiplano.enable_onu_discovery</code>	Aktivieren oder deaktivieren Sie die Erkennung von ONU-Geräten und logischen Verbindungen zwischen OLT und ONU. • Standardwert: True • Standort: Alle > Service Graph Connectors > Nokia Altiplano > Eigenschaften Oder Systemeigenschaften [sys_properties] Tabellenfilterung nach dem Namen „*altiplano“
<code>sn_sgc_altiplano.devices_list_batch_size</code>	Steuert die Batch-Größe für Altiplano REST API-Aufrufe. • Standardwert: 1000 • Standort: Alle > Service Graph Connectors > Nokia Altiplano > Eigenschaften Oder Systemeigenschaften

Mit Nokia Altiplano installierte Eigenschaften (Fortsetzung)

Eigenschaft	Beschreibung
	[sys_properties] Tabellenfilterung nach dem Namen „*altiplano“
<i>sn_sgc_altiplano.parallel_number_of_data_source_jobs</i>	Anzahl der parallelen Aufträge zum Sammeln von Altiplano-Daten (erfordert die Einstellung „paralleles Laden aktivieren“). • Standardwert: 2 • Standort: Alle > Service Graph Connectors > Nokia Altiplano > Eigenschaften Oder Systemeigenschaften [sys_properties] Tabellenfilterung nach dem Namen „*altiplano“
<i>sn_sgc_altiplano.onu_ci_class</i>	Definiert, ob onus als gespeichert werden ONU Oder ONT CI-Klasse. • Standardwert: ONU • Standort: Alle > Service Graph Connectors > Nokia Altiplano > Eigenschaften Oder Systemeigenschaften [sys_properties] Tabellenfilterung nach dem Namen „*altiplano“

Zugehörige Informationen

[Telecom Discovery über Nokia Altiplano](#)

[Konfigurieren des Nokia Altiplano Service Graph Connector](#)

[store-future: BEGIN review]

Mit Nokia NSP installierte Systemkomponenten

Systemeigenschaften steuern, wie der Connector funktioniert, einschließlich Discovery-Optionen und Leistungseinstellungen.

Mit Nokia NSP installierte Eigenschaften

Eigenschaft	Beschreibung
<code>sn_sgc_nsp.parallelNumberOfDataSourceJobs</code>	Anzahl der parallelen Aufträge zum Sammeln von NSP-Daten (erfordert die Einstellung „paralleles Laden aktivieren“). • Standardwert: 1 • Speicherort: Alle > Service Graph Connectors > Nokia NSP > Tabelle „Eigenschaften“ oder „Systemeigenschaften“ [sys_properties], die nach dem Namen „nsp“ gefiltert wird
[End]	

Mit Telecom Discrepcy Identification and Reconciliation installierte Systemkomponenten

Die Systemeigenschaften sind Teil des Plugins „TSOM-Transparenz“ (sn_tsom_Core) und steuern das Protokoll zur Identifizierung und Abgleich von Telekommunikationsdiskrepanzen (TSOM CMDB-Audit). Das Plugin „TSOM-Transparenz“ dient als Befähiger für die TSOM-Transparenzanwendungen und enthält Logik, die in der Lösung „Telecom Discovery“ und „Telecom Diskrepancy Identification and Reconciliation“ gemeinsam genutzt wird.

Systemeigenschaften für Identifizierung und Abgleich von Telekommunikationsdiskrepanzen (Auswirkungen auf CMDB-Audit)

Eigenschaftsname	Empfohlener/Standardwert	Beschreibung
<code>sn_tsom_core.audit.log.level</code>	Protokollierung Von Telekommunikationsdiskrepanz-Audits.	Debuggen, Info, V Standardwert
<code>sn_tsom_core.audit.relationship_types</code>	Angezeigte Namen von Beziehungstypen, die vom Audit der Telekommunikationsdiskrepanz behandelt werden.	Kommatgetrennte Beziehungstypen Standardwert Enthält::entha
<code>sn_tsom_core.audit.discovered_date.diff.threshold.in.days</code>	Schwellenwert für das letzte erkannte Datum in Tagen. Wird für das Audit der Telekommunikationsdiskrepanz verwendet.	Zeichenfolge Standardwert
<code>sn_tsom_core.audit.suppress_CI_Model_missing_discrepancy_task_creation</code>	Unterdrücken Sie die Erstellung der Aufgabe „fehlende Diskrepanz“ für das CI-Modell für die Tabellen.wird für das Audit der Telekommunikationsdiskrepanz verwendet.	cmdb_ci_ni_tel cmdb_ci_ip_Sw cmdb_ci_ip_Ro cmdb_ci_Contai cmdb_ci_Contai cmdb_ci_Contai

Systemeigenschaften für Identifizierung und Abgleich von Telekommunikationsdiskrepanzen (Auswirkungen auf CMDB-Audit) (Fortsetzung)

Eigenschaftsname	Empfohlener/Standardwert	Beschreibung
sn_tsom_core.audit.equipment_tables	Gerätetabellen, die vom Audit der Telekommunikations-Diskrepanz verarbeitet werden.	cmdb_ci_Interfa cmdb_ci_ni_Inte Kommagetrennt Gerätetabellenn Standardwert cmdb_ci_netg
sn_tsom_core.audit.interface_card_tables	Schnittstellenkarten-Tabellen, die vom Audit der Telekommunikations-Diskrepanz verarbeitet werden.	Kommagetrennt Kartentabellenn Standardwert cmdb_ci_Inter
sn_tsom_core.audit.interface_tables	Netzwerkschnittstellentabellen, die vom Audit der Telekommunikationsdiskrepanz verarbeitet werden.	Kommagetrennt Schnittstellentab Standardwert cmdb_ci_ni_In
sn_tsom_core.audit.slot_tables	Namen der Steckplatztabellen, die vom Audit der Telekommunikationsdiskrepanz verarbeitet werden.	Kommagetrennt Tabellennamen Standardwert cmdb_ci_Con
sn_tsom_core.audit.subslot_tables	Namen der Untersteckplatztabellen, die vom Telecom Discrepancy Audit verarbeitet werden.	Kommagetrennt Liste der Namen Untersteckplatzt Der Standard cmdb_ci_Con

Audits Für Identifizierung Und Abgleich Von Telekommunikationsdiskrepanzen

Audit-Name	Beschreibung
Audit Der Telekommunikationsdiskrepanz	Auditiert Datensätze in cmdb_rel_ci Tabelle. Für jeden von Nokia Altiplano oder NSP werden die übergeordneten und untergeordneten CIs basierend auf validiert: – Neuestes Modellbeziehung (wenn TNI Core installiert ist). i Hinweis: Alle Diskrepanzaudits verwenden einen Filtermechanismus, der für Geräte-CIs gilt. Filterbedingung: Discovery_Source ENTHÄLT TSOM .
Audit Der Diskrepanz Logischer Verbindungen Der Telekommunikation	Auditiert Datensätze in cmdb_ci_ni_logical_path Tabelle. Für jede logische Verbindung NSP erkannt wird, wird Folgendes überprüft: – Leerer Endpunkt (Port A oder Port Z) – j eindeutigen logischen Verbindung verbunden sein.

Audits Für Identifizierung Und Abgleich Von Telekommunikationsdiskrepanzen
(Fortsetzung)

Audit-Name	Beschreibung
Audit Der Topologie Der Telekommunikationsnetzwerke-Diskrepanz	Auditiert Datensätze in cmdb_ci_Network_Topology Tabelle. Für jedes von Nokia AL Netzwerktopologie-CI wird Folgendes überprüft: – Mindestens eines enthält:enthalten in mindestens ein Mitglied:Mitglied der Beziehung zu einer logischen Verbindung.

Zugehörige Informationen

- Identifizierung und Abgleich von Telekommunikationsdiskrepanzen
- Aktivieren Sie die Identifizierung und den Abgleich von Telekommunikationsdiskrepanzen
- Führen Sie ein Audit für Telekommunikationsdiskrepanzen aus

Automatische Übersetzung