Automatisierung eines Fallbeispiels für Bandwidth-on-Demand über Closed Loop Automation Software Stack

Inhalt

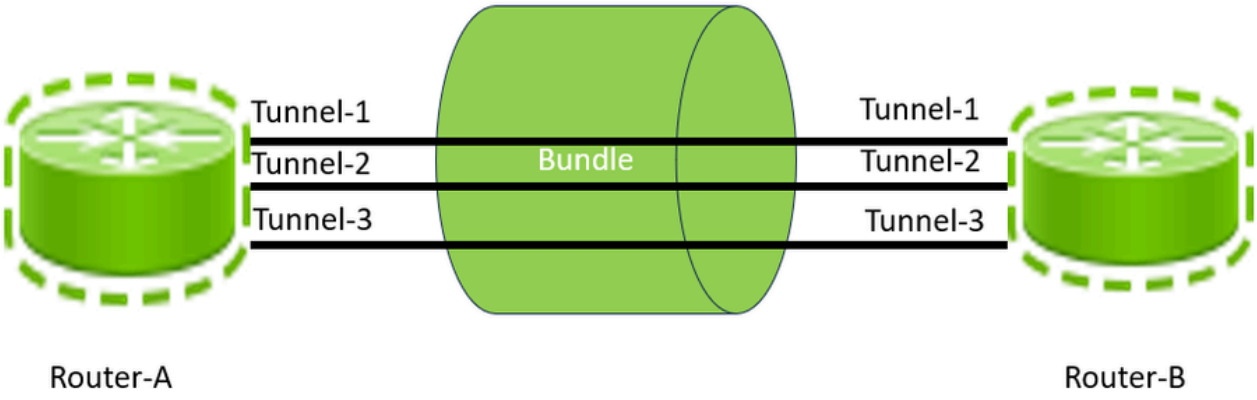
Einleitung

In diesem Dokument werden die Komponenten einer Cisco Closed-Loop-Automatisierungslösung für die Automatisierung der Generic Routing Encapsulation (GRE)-Tunnelskalierung sowie deren Anpassbarkeit an andere Fälle beschrieben.

Hintergrundinformationen

Service Provider möchten die Kontrolle über die Bandbreitennutzung in den GRE-Tunneln im gesamten Netzwerk übernehmen und diese genau überwachen, um die Tunnel nach Bedarf zu skalieren. Dazu wird eine intelligente Automatisierungslösung mit geschlossenem Regelkreis eingesetzt.

GRE ist ein Tunneling-Protokoll, das einen einfachen generischen Ansatz für die Übertragung von Paketen eines Protokolls über ein anderes mithilfe der Kapselung bietet. Dieses Dokument konzentriert sich auf das GRE-Tunnel-basierte Beispiel für die Cisco IOS® XRv-Plattform, kann jedoch auch auf andere Plattformen verallgemeinert werden. GRE kapselt eine Nutzlast, ein inneres Paket, das innerhalb eines äußeren IP-Pakets an ein Zielnetzwerk übermittelt werden muss. Der GRE-Tunnel verhält sich wie eine virtuelle Point-to-Point-Verbindung mit zwei Endpunkten, die durch die Tunnelquelle und die Tunnelzieladresse identifiziert werden.



GRE-Tunnel zwischen Routern

Zum Konfigurieren eines GRE-Tunnels müssen Sie eine Tunnelschnittstelle erstellen und Tunnelquelle und -ziel definieren. Dieses Bild zeigt die Konfiguration von drei GRE-Tunneln zwischen Router-A und Router-B. Für diese Konfiguration müssen Sie drei Schnittstellen auf Router-A erstellen, z. B. Tunnel-1, Tunnel-2 und Tunnel-3, und auf ähnliche Weise drei Schnittstellen auf Router-B erstellen, z. B. Tunnel-1, Tunnel-2 und Tunnel-3. Zwischen zwei Service-Provider-Routern können mehrere GRE-Tunnel vorhanden sein. Jeder Tunnel verfügt wie jede andere Netzwerkschnittstelle über eine definierte Kapazität, die auf der Schnittstellenkapazität basiert. Daher kann ein Tunnel nur einen maximalen Datenverkehr in Höhe seiner Bandbreite übertragen. Die Anzahl der Tunnel basiert häufig auf der anfänglichen Prognose der Datenverkehrslast und der Bandbreitennutzung zwischen zwei Standorten (Routern). Bei Veränderungen der Netzwerk- und Netzwerkerweiterung wird sich die Bandbreitennutzung voraussichtlich ändern. Für eine optimale Nutzung der Netzwerkbandbreite ist es wichtig, neue Tunnel hinzuzufügen oder zusätzliche Tunnel zwischen zwei Geräten zu entfernen. Dies hängt von der Bandbreitennutzung ab, die in allen Tunneln zwischen den beiden Geräten gemessen wird.

In diesem Beispiel können Sie sagen, dass die Gesamtkapazität aller drei Tunnel zwischen Router-A und Router-B die Summe der Kapazitäten von Tunnel-1, Tunnel-2 und Tunnel-3 ist, die als aggregierte Bandbreite oder Bandbreite auf GRE-Bündelebene bezeichnet wird. Bitte beachten Sie, dass sich das Schlüsselwort "Bundle" hier auf die Tunnel zwischen zwei Routern bezieht. Es ist keine implizite Beziehung zur LACP/Etherchannel-Link-Bündelung vorgesehen. Der tatsächliche Datenverkehr zwischen den beiden Routern ist der gesamte aggregierte Datenverkehr zwischen Tunnel-1, Tunnel-2 und Tunnel-3. In der Regel können Sie ein Konzept für die Bandbreitennutzung auf Bündelebene entwickeln, das ein Verhältnis des gesamten Datenverkehrs durch die Tunnel zur Gesamtkapazität aller Tunnel zwischen zwei Routern darstellen kann. Im Allgemeinen möchte ein Service Provider Abhilfemaßnahmen ergreifen, indem er Tunnel zwischen zwei Routern hinzufügt oder entfernt, wenn er feststellt, dass die Bandbreite überlastet oder nicht ausgelastet ist. Beachten Sie in diesem Dokument jedoch, dass der untere Schwellenwert bei niedriger Auslastung 20 % und bei hoher Auslastung 80 % für die Auslastung

auf Bündelebene zwischen zwei Routern beträgt.

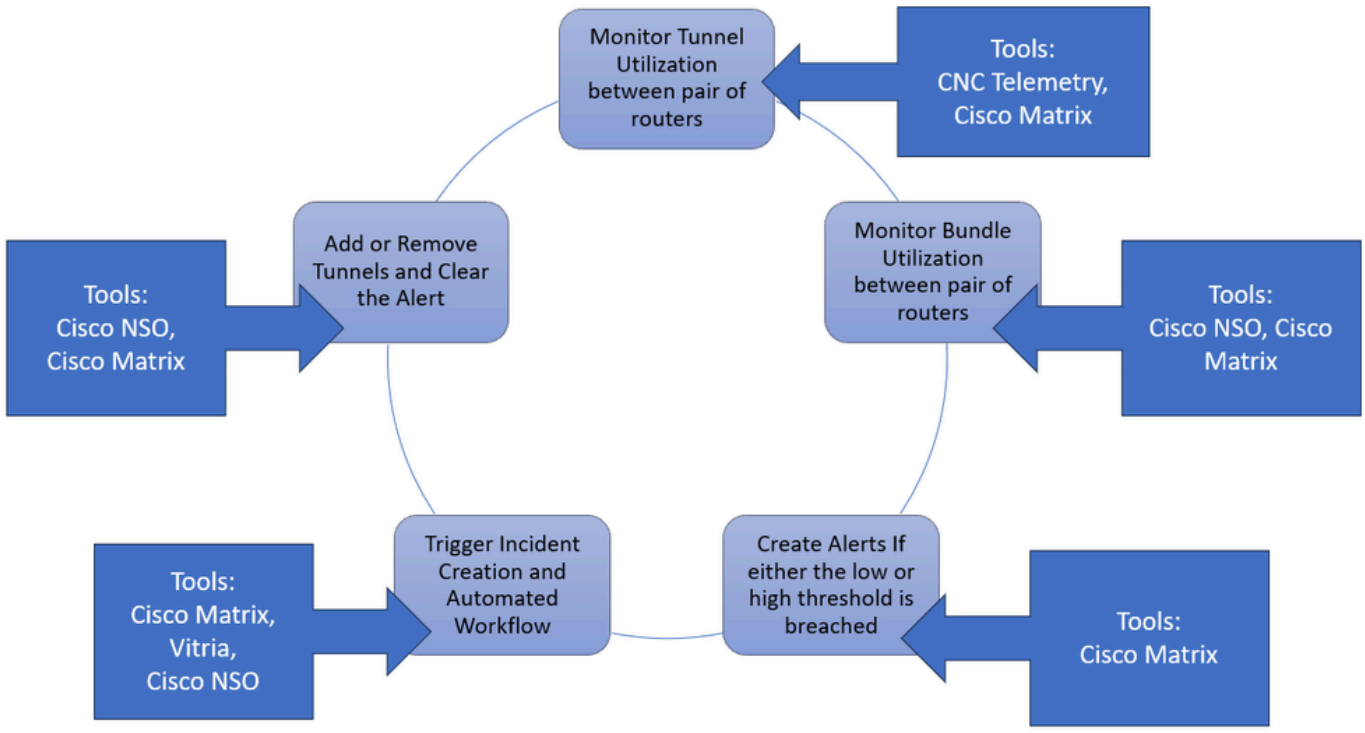
Anforderungen

1. Die Closed-Loop-Lösung ist für die End-to-End-Automatisierung des GRE-Pakets auf XRv9K erforderlich. Das System kann Telemetriedaten erfassen, die Daten in Form von Key Performance Indicators (KPIs) überwachen, Aggregation anwenden, Threshold Cross Alerts (TCA) erstellen, eine automatisierte Behebungskonfiguration durchführen und die Warnmeldung schließen.
2. Die Lösung kann einen Network Key Performance Indicator (KPI) berechnen, um die Bandbreitennutzung der einzelnen Tunnel-Eingangs- (Rx) und Tunnel-Ausgangstunnel (Tx) für jeden Tunnel bereitzustellen, die auf dem Rohdurchsatz der Tunnel mit einer gewünschten Frequenz basiert.
3. Die Lösung kann benutzerdefinierte KPIs berechnen, um die Bandbreitennutzung für den Tunneleingang (Rx) und den Tunnelausgang (Tx) jedes Pakets bereitzustellen, d. h. die aggregierte Bandbreitennutzung aller Tunnel zwischen zwei Routern.
4. Die Lösung kann Warnmeldungen erkennen und erstellen, wenn die festgelegten Schwellenwerte für Paketstufen überschritten werden. Solche Warnmeldungen stehen für die Überwachung zur Verfügung.
5. Die Warnmeldung muss einen automatisierten Workflow auslösen, der die Konfiguration auf dem Gerät weiter auslösen kann, sodass entsprechend den Warnmeldungsbedingungen Tunnel hinzugefügt oder entfernt werden können.
6. Schließlich muss das System die Warnmeldungen mit den erforderlichen Aktualisierungen automatisch schließen.

Lösung

Die Closed Loop-Automatisierungslösung umfasst mehrere Tools, die an der Umsetzung des spezifischen Ziels dieser End-to-End-Lösung arbeiten. Dieses Bild zeigt, welche Komponenten und Tools uns dabei helfen, die endgültige Architektur zu erreichen, und beschreibt die übergeordnete Rolle. Sie können jede Komponente und ihre Verwendung in den nachfolgenden Abschnitten betrachten.

Cisco Closed Loop Automation-



LösungCisco Closed Loop Automation-Lösung

Tool	Zweck
Cisco Crosswork Network Controller (CNC)	Der Crosswork Network Controller sorgt für Echtzeit-Transparenz über den Service- und Geräte-Lebenszyklus hinweg. Er ermöglicht eine intuitive Navigation über die Netzwerktopologie, den Servicebestand, Transportrichtlinien, den Service-Status, den Gerätestatus und vieles mehr und unterstützt so eine breite Palette von Anwendungsfällen mit einer gemeinsamen und integrierten Benutzererfahrung. In dieser Lösung wird sie hauptsächlich zur Verwaltung von Geräten und zur Erfassung von Leistungsdaten für Tunnel unter Verwendung von gNMI (gRPC Network Management Interface) oder MDT verwendet. Weitere Informationen: https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-controller/index.html
Cisco Matrix	Die CX-Analyseservices (Funktionspakete) werden mit der Matrix-Lösung bereitgestellt, einer zentralen, anbieterübergreifenden Lösung für Analysen mit mehreren Domänen. In dieser Lösung verwendet die Matrix die von CNC über die Kafka-Themen gesendeten Daten von Kafka und führt ferner die Aggregation tunnelbasierter KPI in den KPI auf Bündelebene mithilfe von Topologiesuchen durch, speichert sie als Zeitreihendaten und speichert sie in der Postgres-Datenbank. Sobald diese Daten

	gespeichert sind, können sie visualisiert werden. Matrix erkennt Abweichungen anhand von Warnmeldungen bei Überschreitungen von Grenzwerten. Auf diese Weise können Grenzwerte für die Kennzahlen konfiguriert werden, die wir vom Netzwerk erfassen.
Kafka-Cluster	Ein Kafka-Cluster ist ein System, das verschiedene Broker-Themen und ihre jeweiligen Partitionen umfasst. Ein Produzent sendet oder schreibt Daten/Nachrichten an das Thema innerhalb des Clusters. Ein Verbraucher liest oder verwendet Nachrichten aus dem Kafka-Cluster. Bei dieser Lösung agiert CNC als Hersteller, der Daten in Form von JSON-Nutzdaten an vordefinierte Kafka-Themen sendet, nachdem er Daten aus Telemetriedaten konvertiert hat, die von Routern gesammelt wurden. Bei dieser Lösung agiert Matrix als Verbraucher, der diese Daten verbraucht, verarbeitet, aggregiert und zur weiteren Verarbeitung und Erkennung von Anomalien speichert.
Cisco NSO	Cisco Crosswork Network Services Orchestrator (NSO) NSO ist Teil des Crosswork-Portfolios von Automatisierungstools für Service Provider und große Unternehmen. Bei dieser Lösung sammelt der NSO Informationen zu allen Tunneln und Geräten und erstellt eine angepasste Topologietabelle für diese Lösung. Darüber hinaus werden bei dieser Lösung der NSO und die Automatisierungsfunktionen für Geschäftsprozesse eingesetzt, um einen Workflow für die Problembehebung auszulösen und Maßnahmen wie das Hinzufügen oder Entfernen eines Tunnels zum Gerät und das Löschen weiterer Warnmeldungen in der Cisco Matrix zu ergreifen. Weitere Informationen: https://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html
Vitria VIA AIOps	Vitria VIA AIOps für Cisco Network Automation ermöglicht die automatisierte Analyse, die eine schnelle Behebung von Ereignissen ermöglicht, die sich auf alle Technologie- und Anwendungsebenen auswirken. Bei dieser Lösung werden VIA AIOps verwendet, um KPI-Schwellenwertereignisse, die von Cisco Matrix generiert werden, zu korrelieren, einen Vorfall zu generieren, eine Benachrichtigung zu senden und eine automatisierte Aktion gegenüber dem Cisco NSO auszulösen, um die Anzahl der GRE-Tunnel zu erhöhen oder zu verringern. Weitere Informationen: https://www.cisco.com/c/en/us/products/collateral/cloud-

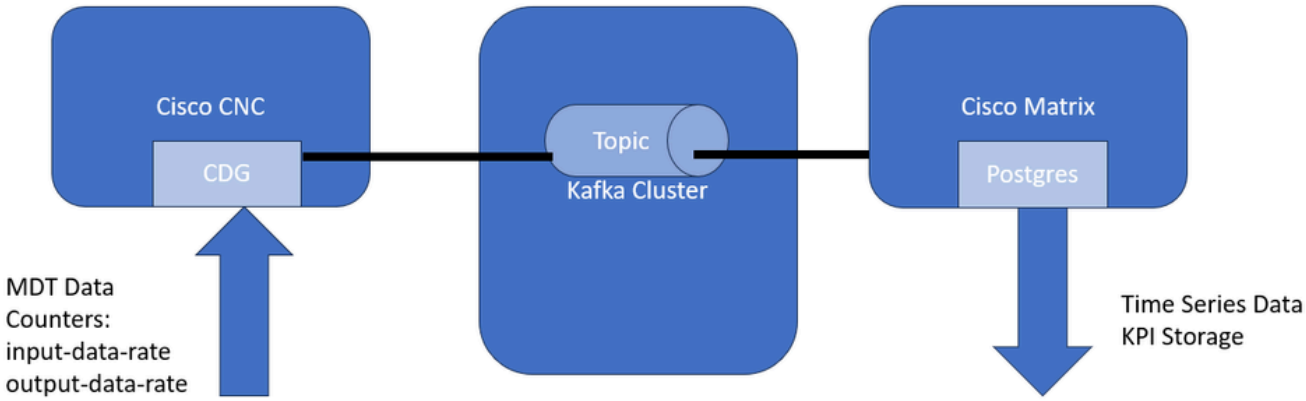
	systems-management/crosswork-network-automation/solution-overview-c22-2403404.html

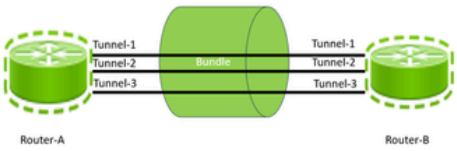
Die Lösung unternimmt diese Schritte, um diesen Anwendungsfall zu erfüllen, der in den nachfolgenden Abschnitten näher erläutert wird.

1. Überwachung der Tunnelauslastung zwischen Routerpaaren
2. Überwachung der Paketauslastung zwischen Routerpaaren
3. Warnungen für Schwellenwertüberschreitung erstellen
4. Trigger für Incident- und automatisierte Behebungs-Workflows
5. Hinzufügen oder Entfernen von Tunneln und Warnung löschen

Überwachung der Tunnelauslastung zwischen Routerpaaren

Anwendungen fordern die Datenerfassung über Erfassungsaufträge an. Cisco Crosswork weist diese Erfassungs-Jobs dann einem Cisco Crosswork Data Gateway zu, um die Anforderung zu erfüllen. Das Crosswork Data Gateway unterstützt die Datenerfassung von Netzwerkgeräten mithilfe von MDT (Model-based Telemetry), um Telemetrie-Streams direkt von Geräten zu nutzen (nur für Plattformen, die auf Cisco IOS XR basieren). Mit Cisco Crosswork können Sie externe Datenziele erstellen, die von Erfassungsaufträgen zum Hinterlegen von Daten verwendet werden können.Kafka kann als neue Datenziele für durch REST API erstellte Erfassungsaufträge hinzugefügt werden. Bei dieser Lösung sammelt CDG Daten von Routern, die sich auf die Tunnelschnittstellenstatistiken beziehen, und sendet die Daten an Kafta Topic.Cisco Matrix verbraucht die Daten aus dem Kafka Topic und weist sie der Matrix-Worker-Anwendung zu, die die Daten als KPI verarbeitet und in einer Zeitreihe speichert, wie in der folgenden Abbildung, die den Prozessablauf darstellt, dargestellt ist.





Time	Node	KPI	Index	Value
22-05-2024 10:00:00	Router-A	input-data-rate	Tunnel-1	1000
22-05-2024 10:00:00	Router-A	input-data-rate	Tunnel-2	1200
22-05-2024 10:00:00	Router-A	input-data-rate	Tunnel-3	1400
22-05-2024 10:00:00	Router-B	input-data-rate	Tunnel-1	1400
22-05-2024 10:00:00	Router-B	input-data-rate	Tunnel-2	1234
22-05-2024 10:00:00	Router-B	input-data-rate	Tunnel-3	1345

Die Zeitreihendaten weisen KPI-Attribute auf, die in der Matrix-Datenbank gespeichert sind.

KPI-Attribute	Zweck
Knoten	Das Gerät oder die Quelle, für das/die KPI gespeichert ist Beispiel: Router-A
Zeit	Zeitpunkt der Datenerfassung Beispiel: 22-05-2024 10:00:00
Index	Eindeutiger Bezeichner Beispiel: Tunnel-1
Wert	Wert der Kennzahl - Numerischer Wert
KPI	KPI-Name Beispiel: Tunnelauslastung

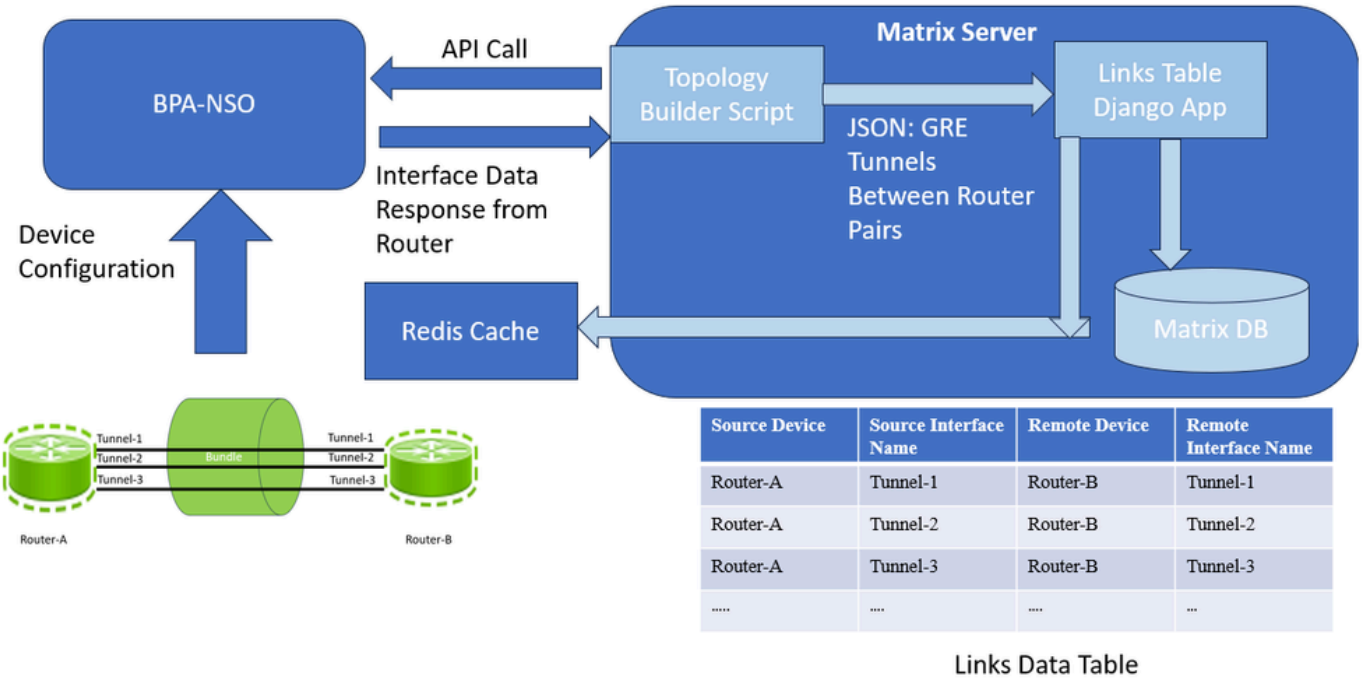
Überwachung der Paketauslastung zwischen Routerpaaren

Sobald Sie die Daten der Zeitreihe wie im vorherigen Abschnitt beschrieben haben, können Sie die Statistiken zum Datenverkehr für jede Tunnelschnittstelle erfassen. Sie müssen jedoch angeben, welches Gerät mit welcher Quell-Tunnelschnittstelle mit welchem anderen Gerät verbunden ist und wie der Name der Remote-Schnittstelle lautet. Dies wird als Link Identification bezeichnet, bei der Sie den Namen des Quellgeräts angeben. Name der Quellschnittstelle, Name des Remote-Geräts und Name der Remoteschnittstelle. Zur korrekten Interpretation der Verbindungsinformationen und Router ist ein Referenzbeispiel wie folgt erforderlich:

Quellgerät	Name der Quellschnittstelle	Remote-Gerät	Name der Remote-Schnittstelle
Router A	Tunnel-1	Router B	Tunnel-1
Router A	Tunnel-2	Router B	Tunnel-2
Router A	Tunnel-3	Router B	Tunnel-3

....	...	...	..

Um diese Topologie-Linktabelle in dieser Lösung zu erstellen, können Sie eine benutzerdefinierte Tabelle, "Links Data Table", erstellen. Diese Tabelle ist in Matrix integriert und basiert auf einem Skript, das täglich zum gewünschten Zeitpunkt auf dem Server ausgeführt wird. Dieses Skript führt einen API-Aufruf an den BPA-NSO aus und erhält eine JSON-Ausgabe der GRE-Pakete zwischen Routerpaaren zurück. Anschließend werden die Schnittstellendaten analysiert, um die Topologie im JSON-Format zu erstellen. Das Skript nimmt auch diese JSON-Ausgabe und schreibt sie jeden Tag in die Links Data Table. Wenn die neuen Daten in die Tabelle geladen werden, werden diese Daten auch in einen Redis-Cache geschrieben, um weitere Datenbanksuchvorgänge zu reduzieren und die Effizienz zu verbessern.



Linkdatentabellen-Prozess

Daher sind notwendigerweise alle Links zwischen den gleichen beiden Geräten Teil des Pakets, das zum gleichen Paket gehört.Sobald die Kennzahlen auf Rohtunnelebene verfügbar sind, haben Sie eine benutzerdefinierte App KPI_aggregate für Matrix erstellt, die die Aufgabe der Berechnung der Auslastungen auf Paketebene und deren Speicherung als Kennzahlen übernimmt.

Diese Anwendung verarbeitet die folgenden Eingaben:

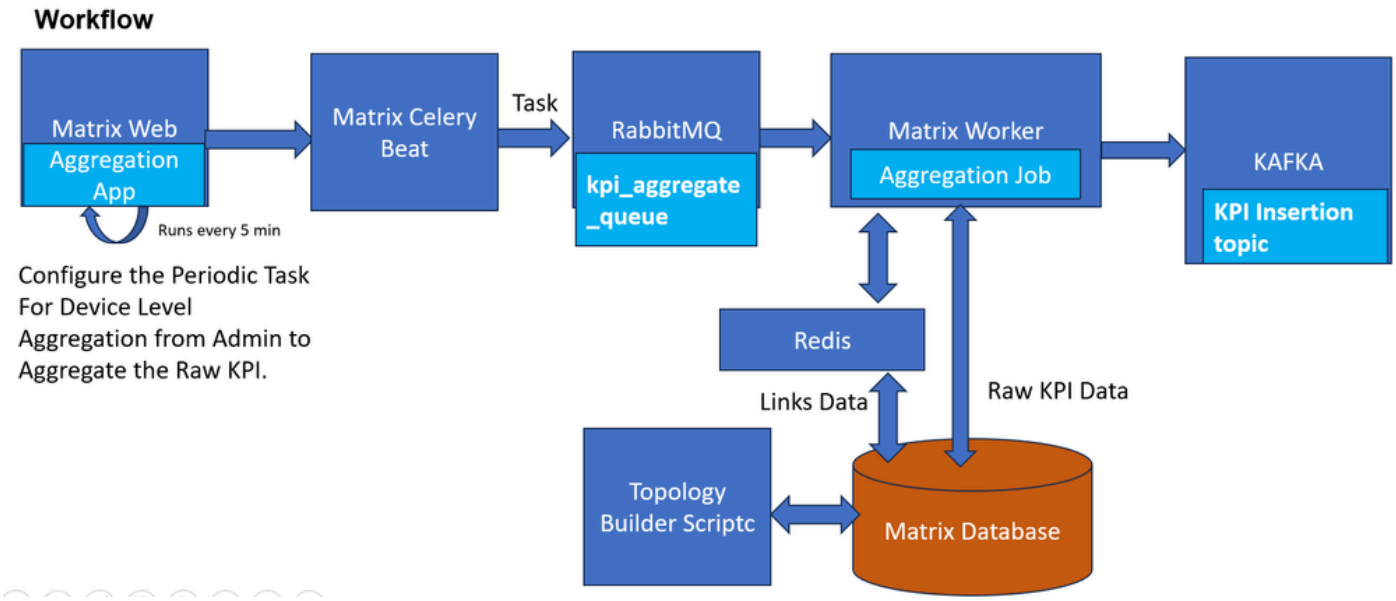
Konfigurationsattribut	Zweck
Crontab	Die Häufigkeit, mit der die periodische Aggregationsaufgabe ausgeführt werden muss.

Kontrollkästchen aktiviert	Diese Konfiguration aktivieren/deaktivieren
KPI-Name der Tunnelschnittstelle	Name des Rohfaktors, der zur Berechnung des Gesamtfaktors verwendet wird. Der KPI-Name wird automatisch als <Raw_KPI_Name>_agg erstellt.
Datumsbereich	Die Häufigkeit der Rohdaten

Die Aggregat-Aufgabe ermittelt die Eingaben aus der KPI-Rohdaten- und Link-Datenbank und identifiziert die Tunnel, die Teil desselben Bündels sind, und fügt sie einer Gruppe auf der Grundlage dieser Logik hinzu.

```
KPI Name: <Raw_KPI_Name>_agg

Example: tunnel_utilization_agg

Value = sum (tunnel_interface_tx_link_utilization of all the interfaces on the device connected to same

Index: <local device> _<remote device>

Router-A _Router-B

Node: <Local-Device>

Router-A
```

In diesem Fall wird der KPI-Name z. B. als "tunnel-usage_agg" für die Roh-Tunnel-KPI-Tunnelauslastung generiert. Sobald die Berechnung für alle Rohwerte der KPIs für alle Router und Tunnelkombinationen abgeschlossen ist, werden diese Daten für jede Verbindung zum Kafka-Thema weitergeleitet, das mit dem verarbeiteten KPI identisch sein muss. Auf diese Weise bleiben diese Informationen wie alle anderen normalen KPIs, die von gültigen Quellen empfangen werden, erhalten. Der DB-Consumer verwendet dieses Thema und behält den KPI in der KPI-Ergebnistabelle in der Matrix-Datenbank für die aggregierten KPIs bei.



KPI-Aggregationsprozess für Aggregation auf Paketebene - KPI

Warnungen für Schwellenwertüberschreitung erstellen

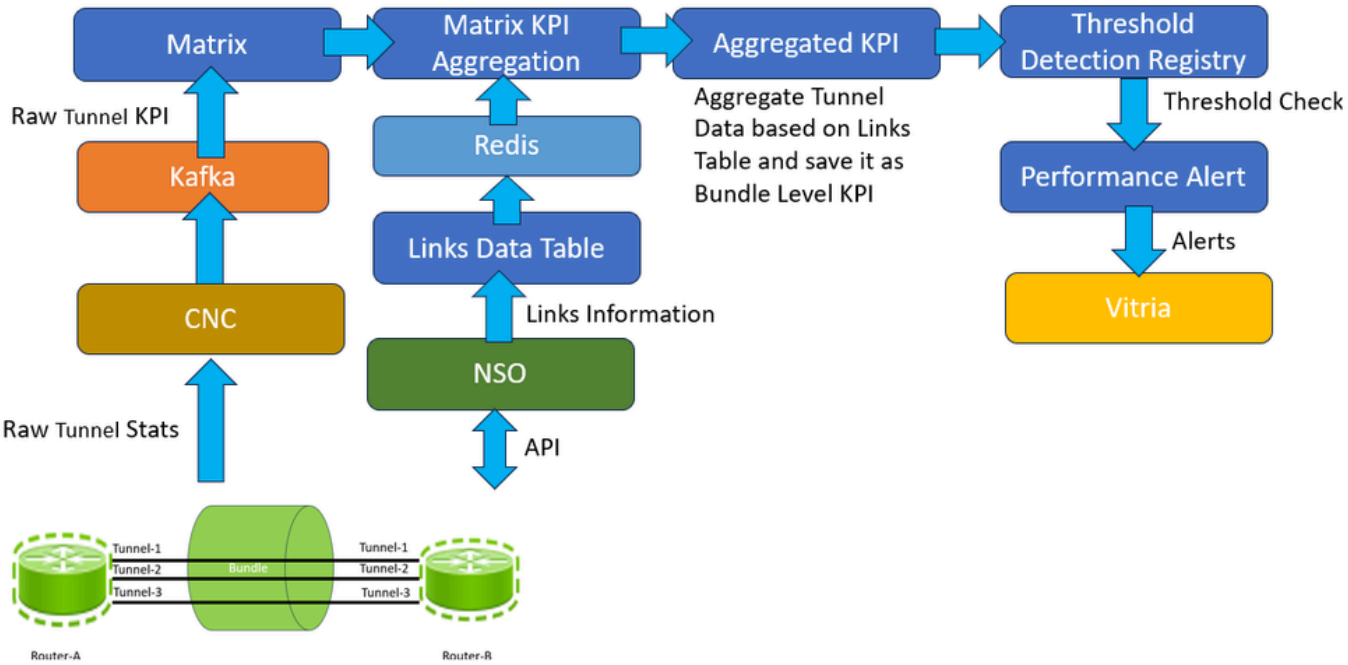
Der in Matrix konfigurierte KPI-Grenzwert beträgt 85 %. Das bedeutet, wenn der Wert dieses KPI den Grenzwert überschreitet, wird eine kritische Warnung generiert, und wenn der Grenzwert unterschritten wird, wird eine klare Warnung generiert. Diese Warnungen werden in der Matrix-Datenbank gespeichert und in dieser Lösung für den Anwendungsfall der Closed-Loop-Automatisierung an Vitria weitergeleitet. Überschreitet der errechnete Wert des KPI den Schwellenwert, wird über Kafka eine Warnmeldung an Vitria (VIA-AIOPs) mit dem aktuellen Status Kritisch in der Meldung gesendet. Wenn der Wert innerhalb der Schwellenwerte von den kritischen Werten zurückkehrt, muss er eine Warnung an VIA-AIOPs über Kafka mit dem aktuellen Status Clear in der Nachricht senden. Eine Beispielnachricht wurde an das System gesendet, und die Attribute lauten wie folgt:


```
{
  "node": "Router-A",
  "node_type": "Router",
  "kpi": "tunnel_usage_agg",
  "kpi_description": "Auslastung auf Paketebene",
  "Schema": "",
  "index": "Router-A_Router-B",
  "Zeit": "2023-08-09 05:45:00+00:00",
  "Wert": "86,0",
```

```
   "vorheriger_Zustand": "LÖSCHEN",
   "current_state": "CRITICAL",
   "link_name": "Router-A_Router-B"
}
```


Kafka-Warnmeldungsattribut	Beispielwert	Zweck
Knoten	Router A	Name des Netzwerkgeräts
Knotenart	Router	Gerätetyp
KPI	tunnel_usage_agg	KPI-Name
KPI_Beschreibung	Auslastung auf Paketebene	KPI-Beschreibung
Schema	NA	NA
Index	Router-A-Router-B	<Lokales Gerät>-<Remote-Gerät>
Zeit	"2023-08-09 05:45:00+00:00"	Zeit
wert	86.0	KPI-Wert
vorheriger_Zustand	LÖSCHEN	Vorheriger Alarmstatus
aktueller Zustand	Critical (Kritisch)	Aktueller Alarmstatus
Link-Name	Router-A-Router-B	Korrelationsattribut

link_name-Attribut ist ein alphabetisch sortierter Name der im Indexwert vorhandenen Geräte. Auf diese Weise wird eine Korrelation auf der Ebene der VIA AIOPs erreicht, auf der VIA AIOps die Warnungen korrelieren müssen, die vom gleichen Paket-Link stammen. Wenn beispielsweise mehrere Warnungen an VIA AIOPs mit demselben Link_Name gesendet werden, bedeutet dies, dass die Warnungen zu demselben Bündel-Link im Netzwerk gehören, das im Link-Namen durch Gerätenamen gekennzeichnet ist.



Generierung von KPI-Aggregationswarnungen mithilfe der Matrix-Erkennungsregistrierung

Trigger für Incident- und automatisierte Behebungs-Workflows

VIA AIOps ist für die Erfassung von Key Performance Indicator (KPI)-Anomalie-Ereignissen aus einem benannten Kafka-Thema zu konfigurieren. Diese Ereignisse, die über Kafka-Nachrichten empfangen werden, werden von VIA AIOps über den JASO Event Parser für die spätere Aufnahme verarbeitet. VIA AIOps müssen KPI-Anomalie-Ereignisse in Bezug auf GRE-Tunnel genau identifizieren, ihre Zuordnung zu bestimmten Gerätepaaren (z. B. Router A-Router B) ermitteln und feststellen, ob diese Anomalie die Initiierung einer Automatisierung der GRE-Tunnelskalierung erfordert - entweder eine Up- oder eine Downscale-Automatisierung.

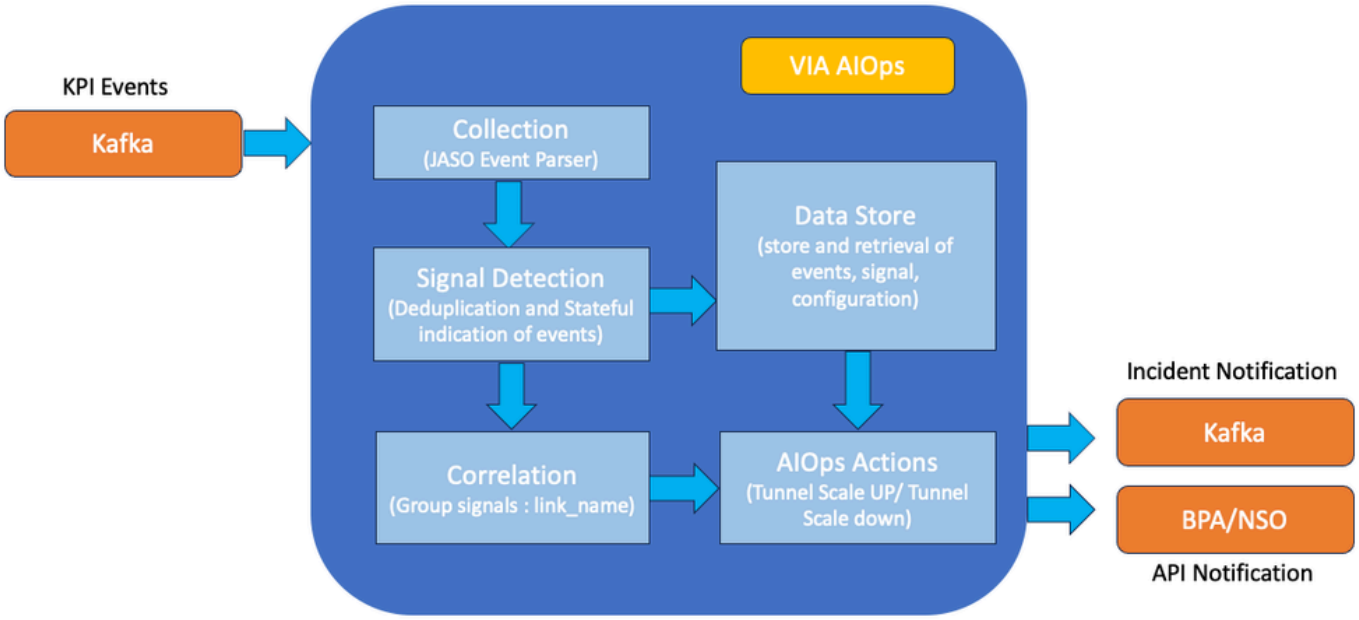
Der JASO Event Parser in VIA AIOps muss so konfiguriert werden, dass relevante Dimensionen aus dem Matrix KPI-Anomalie-Ereignis extrahiert und interpretiert werden, nämlich "host", "kpi", "index" und "value". Eine zusätzliche Dimension, die als 'automation_action' bezeichnet wird, muss so konfiguriert werden, dass sie vom JASO Event Parser dynamisch aktualisiert wird. Dies basiert auf der 'value'-Metrik, die im Matrix KPI-Anomalie-Ereignis vorhanden ist. Diese Dimension ist von entscheidender Bedeutung für die Entscheidung, ob eine automatisierte Antwort erforderlich ist, und zwar für die Auslösung der Verfahren "GRE Tunnel Scale Up" oder "GRE Tunnel Scale Down" durch Verarbeitung des Felds "KPI value". In VIA AIOps stellt ein Signal eine Konsolidierung der Zustände der Ereignisse dar. Um diesen Korrelationsprozess zu verbessern, müssen wir eindeutige Stateful-Signale konfigurieren, die mit den Dimensionen 'host', 'link name', 'kpi' und 'automation_action' korrelieren. Die Tabelle veranschaulicht die Signale, Korrelationsgruppen und ihre jeweiligen Korrelationskonfigurationen.

Beispielsweise würde das als GRE_KPIA_SCALEUP identifizierte Signal nach der Aufnahme einer spezifizierten KPI-Anomalie-Nachricht, wie in Abschnitt 3 beschrieben, durch das VIA AIOps-System initiiert.

VIA AIOps-Signalname	Signalkorrelationsschlüssel	Name der

		Korrelationsgruppenregel
GRE_KPIA_SKALEUP	Host, kpi, Link-Name, Automated_action	GRE-Tunnel-Skalierung
GRE_KPIB_SKALEUP	Host, kpi, Link-Name, Automated_action	
GRE_KPIA_SKALEDOWN	Host, kpi, Link-Name, Automated_action	GRE-Tunnelskalierung nach unten
GRE_KPIB_SKALEDOWN	Host, kpi, Link-Name, Automated_action	

Die Korrelationsgruppenregel soll die Aggregation von Signalen über Gerät A, Gerät B und deren jeweilige Tunnel A, B und C zu einem einheitlichen Vorfall erleichtern. Diese Korrelationsregel stellt sicher, dass für eine bestimmte Paarung von Gerät A und Gerät B maximal zwei unterschiedliche Vorfälle generiert werden: ein Vorfall für eine GRE-Tunnel-Skalierung mit Gerät A und Gerät B und ein anderer Vorfall für eine GRE-Tunnel-Skalierung für dieselbe Gerätepaarung. Das VIA AIOps Agent-Framework ist mit Business Process Automation (BPA) und Network Services Orchestrator (NSO) kompatibel.



KPI-Ereigniskorrelation und -benachrichtigung mit VIA AIOps

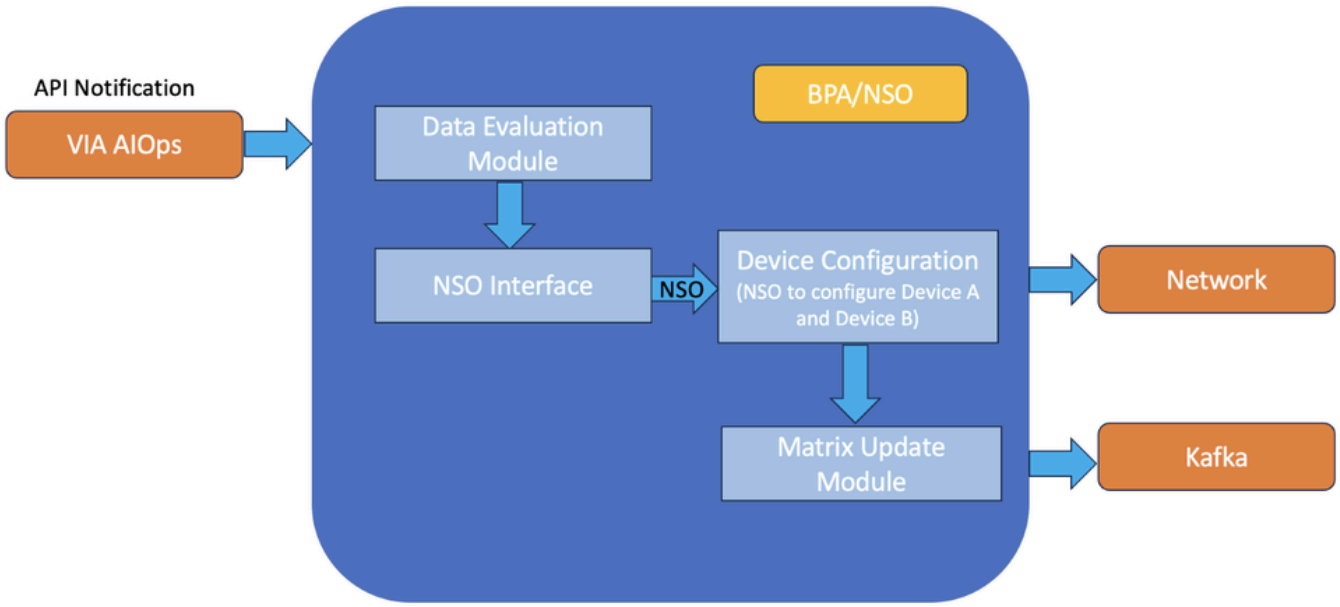
Das folgende Beispiel zeigt eine GRE Tunnel Scale-Up API-Benachrichtigung, die von VIA AIOps

an BPA/NSO gesendet wurde.

```
{
  "create": [
    {
      "gre-tunnels-device-cla": [
        {
          "index": "RouterA-RouterB",
          "tunnelOperation": "SCALE UP",
          "MatrixData": [
            { "node": "RouterA", "kpi": "tunnel_utilization_agg" },
            { "node": "RouterB", "kpi": "tunnel_utilization_agg" }
          ]
        }
      ]
    }
  ]
}
```

Hinzufügen oder Entfernen von Tunneln und Warnung löschen

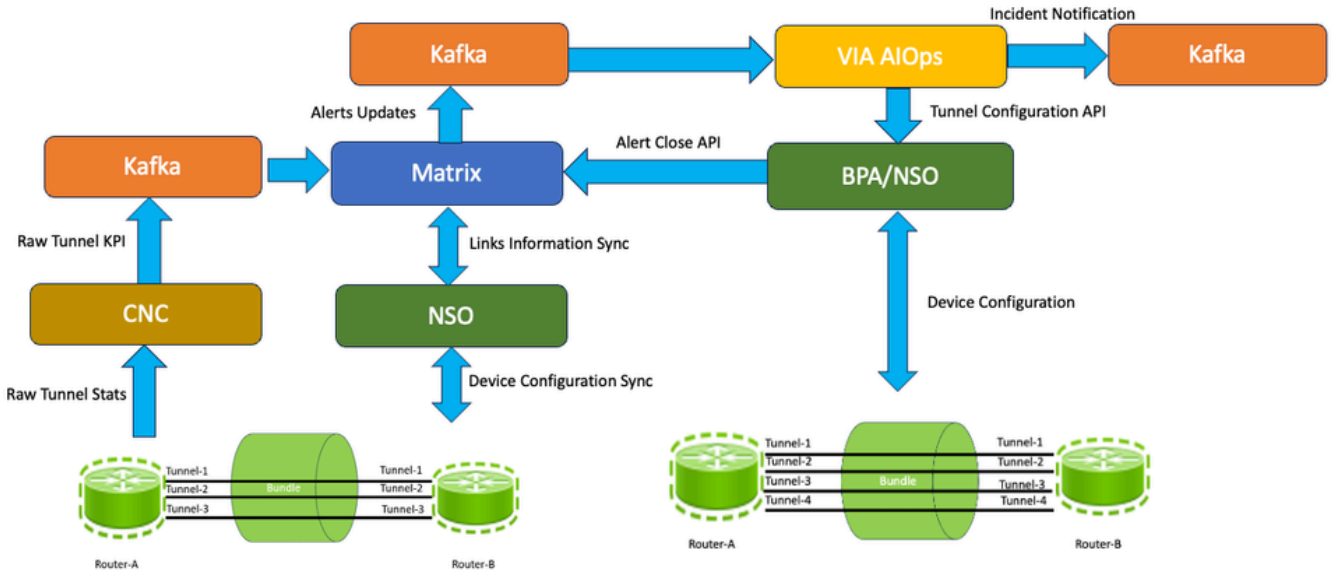
Nach Erhalt eines API-Anrufs von VIA AIOps leitet die Cisco Business Process Automation (BPA) die erforderlichen Skalierungsrichtlinien durch interne Anfragen an den Cisco Network Service Orchestrator (NSO) ein. Die BPA bewertet die von VIA AIOps bereitgestellte Daten-Nutzlast, die Tunnelbetriebsdetails, einen Index und Matrix-Daten umfasst. Die Index- und Tunnelbetriebsinformationen werden für die Schnittstelle zum NSO verwendet und liefern Parameter für den Skalierungsbetrieb. Gleichzeitig werden die Matrixdaten vom 'Matrix Update Module' verarbeitet, das für die Behebung von KPI-Anomalie-Ereignissen durch die Verbindung mit den Matrix-APIs zuständig ist.



Datenvalidierung und Gerätekonfiguration mit BPA-NSO

Bevor Skalierungsoperationen initiiert werden können, muss ein YANG-Aktionsmodell für den NSO entwickelt werden. Dieses Modell definiert die spezifischen Aktionen, die der NSO ausführen muss, um die Tunnelanzahl zwischen Router A und Router B zu erhöhen oder zu verringern. Das Business Process Automation (BPA)-System beginnt mit der Skalierung, indem es den Network Service Orchestrator (NSO) zur Durchführung eines Testlaufs kontaktiert. Dies ist die Anfangsphase des Vorgangs, in der die BPA den NSO auffordert, die beabsichtigten Konfigurationsänderungen zu simulieren, ohne sie anzuwenden. Der Trockenlauf dient als wesentlicher Validierungsschritt und stellt sicher, dass die vorgeschlagenen Skalierungsaktionen, wie sie im YANG-Aktionsmodell definiert sind, ohne Fehler oder Konflikte in der Netzwerkkonfiguration ausgeführt werden können.

Wenn der Trockenlauf als erfolgreich eingestuft wird, was darauf hinweist, dass die Skalierungsaktionen validiert werden, geht der BPA zur Commit-Phase über. Zu diesem Zeitpunkt weist der BPA den NSO an, die tatsächlichen Konfigurationsänderungen zu implementieren, die erforderlich sind, um die Anzahl der GRE-Tunnel zwischen Router A und Router B zu erhöhen oder zu verringern. Das BPA löst das Matrix-Update-Modul mithilfe eines API-Aufrufs in Richtung Matrix aus, um das KPI-Ereignis zusammen mit VIA AIOps zu schließen. Sobald diese Anomalie in Matrix behoben wurde, sendet Matrix auch eine Warnung mit dem Schweregrad "Gelöscht" an VIA AIOps, wodurch der Vorfall an seinem Ende weiter geschlossen wird. Auf diese Weise ist der Wiederherstellungszyklus auf Netzwerkebene abgeschlossen. In diesem Bild ist eine generalisierte Version des Datenflusses innerhalb der Anwendung dargestellt, die bei dieser Closed-Loop-Automatisierung genutzt wird.



Datenfluss für ein GRE-Tunnelpaket Closed Loop Automation

Den Kreislauf schlieen und neue Mglichkeiten der automatischen Problembehebung erffnen

Die in diesem Dokument beschriebene Lösung wird absichtlich mit einem Beispiel für die Skalierung von GRE-Paketen anhand von Netzwerkanomalien erörtert, um uns bei der Beziehung zu verschiedenen Bausteinen dieser Lösung zu unterstützen. Zusammenfassend wird untersucht, wie Cisco Technology Stack mit Cisco NSO, Cisco Matrix und Cisco BPA nahtlos in Komponenten wie VIA AIOps, Kafka und einen weiteren Software-Stack integriert werden kann, um Netzwerkprobleme automatisch zu überwachen und zu beheben. Diese Lösung eröffnet Möglichkeiten für alle anderen Netzwerkanwendungsfälle, die typische Probleme in Service Provider- oder Enterprise-Netzwerken sein können.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.