Automatiseer bandbreedte-on-demand gebruikscase via gesloten circuit-automatiseringssoftwarestack

Inhoud

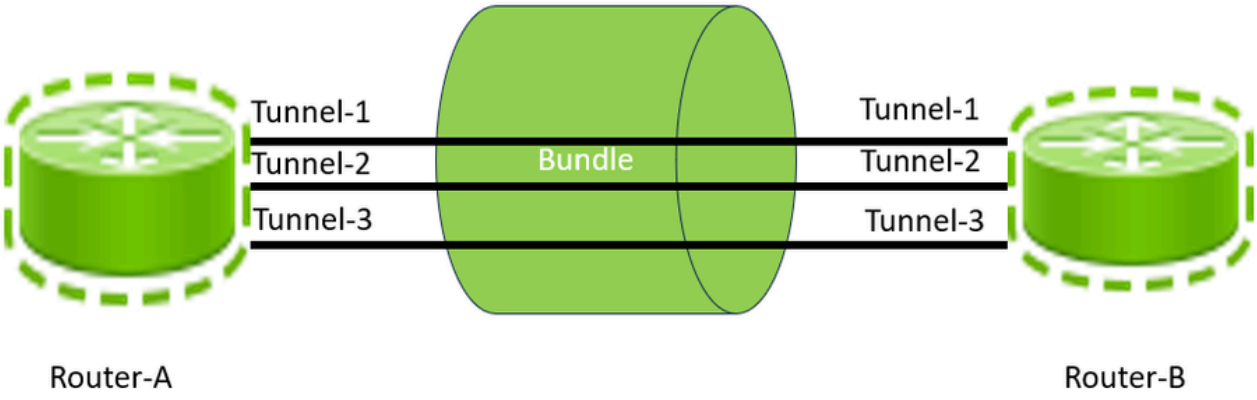
Inleiding

Dit document beschrijft componenten in een Cisco closed-loop automatiseringsoplossing voor GRE-tunnelschalingautomatisering (Generic Routing Encapsulation) en de aanpasbaarheid ervan voor andere cases.

Achtergrondinformatie

Serviceproviders willen de controle over hun bandbreedtetoepassingen over de GRE-tunnels over hun netwerk overnemen en deze nauwgezet monitoren om zo nodig tunnels te schalen met behulp van een slimme, gesloten automatiseringsoplossing.

GRE is een tunnelprotocol dat een eenvoudige generische benadering biedt van transportpakketten van een protocol via een ander protocol via inkapseling. Dit document concentreert zich op het op de GRE-tunnel gebaseerde voorbeeld voor het Cisco IOS® XRv-platform maar kan ook worden generaliseerd naar andere platforms. GRE kapselt een payload in, een binnenpakket dat moet worden geleverd aan een doelnetwerk binnen een extern IP-pakket. De GRE-tunnel gedraagt zich als een virtuele point-to-point link met twee eindpunten die worden geïdentificeerd door de tunnelbron en het doeladres van de tunnel.



GRE-tunnels tussen routers

Het vormen van een tunnel GRE impliceert het creëren van een tunnelinterface en het bepalen van de tunnelbron en de bestemming. Dit beeld toont de configuratie van drie GRE-tunnels tussen router-A en router-B. Voor deze configuratie moet men drie interfaces maken, elk op router-A, zoals Tunnel-1, Tunnel-2 en Tunnel-3, en op dezelfde manier drie interfaces op router-B, zoals Tunnel-1, Tunnel-2 en Tunnel-3. Tussen twee routers voor serviceproviders kunnen er meerdere GRE-tunnels zijn. Elke Tunnel, net als elke andere netwerkinterface, heeft een gedefinieerde capaciteit die is gebaseerd op interfacecapaciteit. Daarom kan een tunnel alleen een maximaal verkeer dragen dat gelijk is aan zijn bandbreedte. Het aantal tunnels is vaak gebaseerd op de initiële voorspelling van verkeersbelasting en bandbreedtegebruik tussen twee locaties (Routers). Met netwerk en netwerkuitbreidingsveranderingen, wordt dit bandbreedtegebruik verwacht om te veranderen. Om optimaal gebruik te maken van de netwerkbandbreedte, is het belangrijk om nieuwe tunnels toe te voegen of extra tunnels tussen twee apparaten te verwijderen gebaseerd op het bandbreedtegebruik dat over alle tunnels tussen de twee apparaten wordt gemeten.

Van dit voorbeeld, kunt u zeggen dat de totale capaciteit van alle drie tunnels tussen router-A en router-B de som capaciteiten van tunnel-1, tunnel-2, en tunnel-3 is, die geaggregeerde bandbreedte of GRE bundel-vlakke bandbreedte wordt genoemd. Houd er rekening mee dat het sleutelwoord 'bundel' hier verwijst naar de tunnels tussen een paar routers; er is geen impliciete relatie met LACP/Etherchannel linkbundeling bedoeld. Ook, is het daadwerkelijke verkeer tussen de twee routers het totale geaggregeerde verkeer over Tunnel-1, Tunnel-2, en Tunnel-3. Meestal, kunt u een concept van bundel-niveau bandbreedtegebruik ontwerpen, dat een verhouding van totaal verkeer door de tunnels aan de totale capaciteit van alle tunnels tussen twee routers kan zijn. Over het algemeen, wil om het even welke dienstverlener saneringsactie door tunnels tussen twee routers toe te voegen of te verwijderen als zij waarnemen dat de bandbreedte overbenut of onderbenut wordt. Houd er echter rekening mee dat voor dit document de onderste drempel 20% is voor weinig gebruik en 80% voor hoog gebruik voor het gebruik op bundelniveau tussen twee routers.

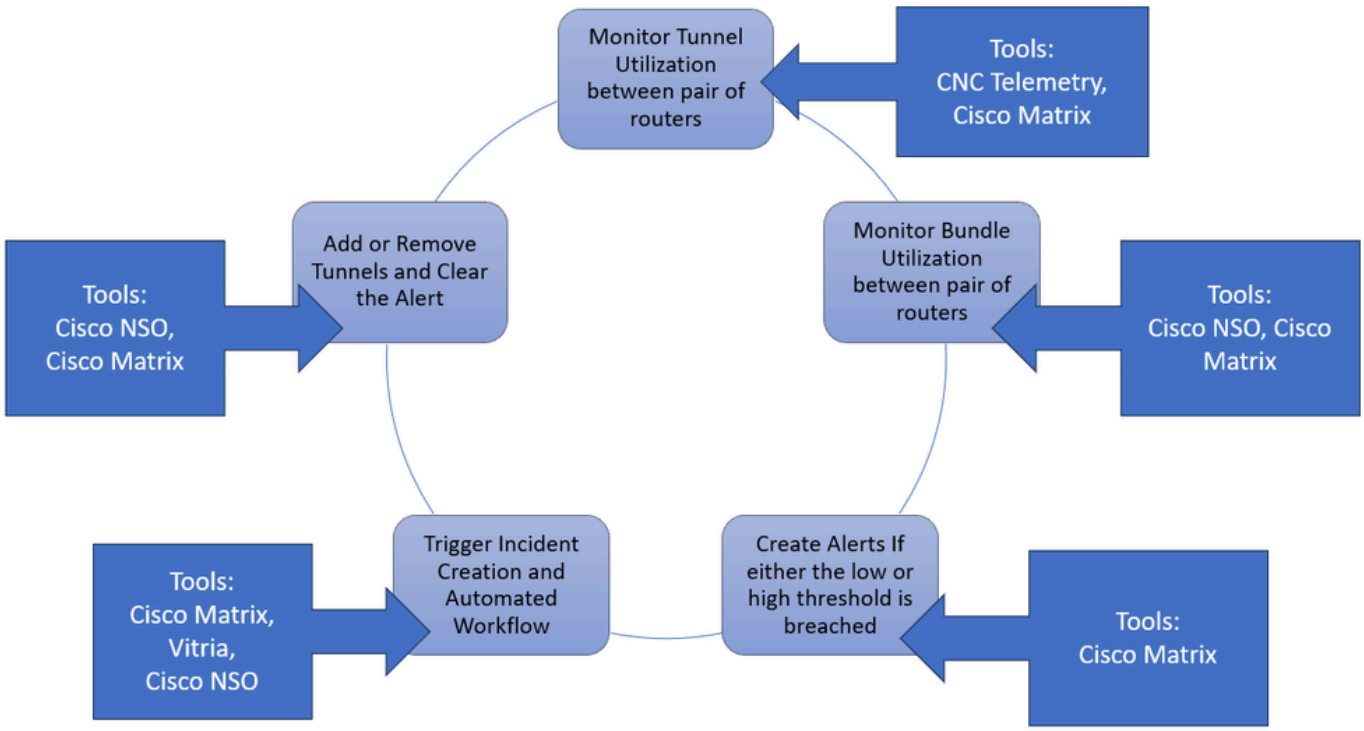
Vereisten

1. De gesloten-lusoplossing is vereist om end-to-end gesloten-automatisering uit te voeren van de GRE-bundel op XRv9K waar het systeem telemetriegegevens kan verzamelen, de gegevens in de vorm van Key Performance Indicators (KPI's) kan bewaken, aggregatie kan toepassen, drempelwaardekruiswaarschuwingen (TCA) kan maken en geautomatiseerde herstelconfiguratie kan uitvoeren en de waarschuwing kan sluiten.
2. De oplossing kan een Network Key Performance Indicator (KPI) berekenen om het individuele Tunnel Ingress (Rx) en Tunnel uitgaande (Tx) bandbreedtegebruik van elke Tunnel te leveren die is gebaseerd op de onbewerkte doorvoersnelheid van tunnels bij een gewenste frequentie.
3. De oplossing kan aangepaste KPI's berekenen om het Tunnel Ingress (Rx) en Tunnel uitgaande (Tx) bandbreedtegebruik van elke Bundle te leveren die het geaggregeerde bandbreedtegebruik van alle tunnels tussen een paar routers is.
4. De oplossing kan waarschuwingen detecteren en maken als de gedefinieerde drempelwaarden voor bundelniveau worden overschreden. Dergelijke signaleringen kunnen worden gevolgd.
5. De waarschuwing moet resulteren in het starten van een geautomatiseerde workflow die verder configuratie op het apparaat kan activeren om op basis van de alarmomstandigheden tunnels toe te voegen of te verwijderen.
6. Tot slot moet het systeem de waarschuwingen automatisch sluiten met de vereiste updates.

Oplossing

De Closed Loop Automation Solution omvat meerdere tools die werken aan het specifieke doel in deze volledige end-to-end oplossing. Dit beeld laat zien welke componenten en tools ons helpen om de uiteindelijke architectuur te bereiken en schetst de rol op hoog niveau. U kunt elke component en het gebruik ervan in de volgende secties bekijken.

Cisco-



oplossing voor

automatisering met

gesloten lijnenCisco-oplossing voor automatisering met gesloten lijnen

Gereedschap	Doel
Cisco Draaiwerk netwerkcontroller (CNC)	Crosswork Network Controller maakt real-time zichtbaarheid mogelijk over de service- en apparaatlevenscyclus, met intuïtieve navigatie over netwerktopologie, serviceinventaris, transportbeleid, servicegezondheid, apparaatgezondheid en meer ondersteuning voor een breed scala aan gebruikscases met een gemeenschappelijke en geïntegreerde gebruikerservaring. In deze oplossing wordt het voornamelijk gebruikt als tool voor het beheer van apparaten en het verzamelen van gegevens over tunnelprestaties met gNMI (gRPC Network Management Interface) of MDT. Meer informatie: https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-controller/index.html
Cisco-matrix	CX analytics services (functiepakketten) worden geleverd met behulp van de Matrix-oplossing, die een multi-leveranciersplane van glas, multi-domein analytics oplossing is.

	In deze oplossing gebruikt de Matrix de gegevens van Kafka die door CNC over de Kafka-onderwerpen zijn verzonden en voert verder aggregatie van tunnelgebaseerde KPI in bundelniveau KPI uit met behulp van topologische zoekacties en slaat het op als tijdreeksgegevens en slaat het op in de Postgres-database. Zodra opgeslagen dergelijke gegevens beschikbaar zijn voor visualisatie en Matrix heeft anomaliedetectie met behulp van drempelkruising waarschuwingen waarmee we drempelwaarden kunnen configureren voor de KPI's die we verzamelen van het netwerk.
Kafka Cluster	Een Kafka-cluster is een systeem dat de onderwerpen van verschillende makelaars en hun respectievelijke partities omvat. Een producent verzendt of schrijft gegevens/berichten naar het onderwerp binnen het cluster. Een consument leest of consumeert berichten uit het Kafka-cluster. In deze oplossing fungeert CNC als de producent die gegevens naar vooraf gedefinieerde Kafka-onderwerpen stuurt in de vorm van JSON-payload na het converteren van gegevens van Telemetry die van routers zijn verzameld. In deze oplossing treedt Matrix op als de Consument die deze gegevens gebruikt, de gegevens verwerkt, aggregeert en opslaat voor verdere verwerking en detectie van abnormaliteiten.
Cisco-netwerkmodule	Cisco Crosswork Network Services Orchestrator (NSO) NSO maakt deel uit van de Kruiswerkportefeuille van automatiseringstools die voor dienstverleners en grote ondernemingen worden gebouwd. In deze oplossing verzamelt NSO informatie met betrekking tot alle tunnels en apparaten en bouwt een aangepaste topologietabel voor deze oplossing. Ook in deze oplossing wordt NSO samen met de mogelijkheden van de Automatisering van het Bedrijfsproces gebruikt om een saneringswerkschema teweeg te brengen en actie te voeren zoals het toevoegen of het verwijderen van een tunnel uit het apparaat en verder ontruimend alarm in de Matrix van Cisco. Meer informatie: https://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html
Vitria VIA AIOps	Vitria VIA AIOps voor Cisco Network Automation levert geautomatiseerde analyse die snelle probleemoplossing bij serviceproblemen in alle technologie- en toepassingslagen mogelijk maakt. In deze oplossing wordt VIA AIOps gebruikt om KPI-drempelgebeurtenissen te correleren die zijn gegenereerd vanuit Cisco Matrix, om een incident te maken, melding te maken en een geautomatiseerde actie te starten naar Cisco NSO om

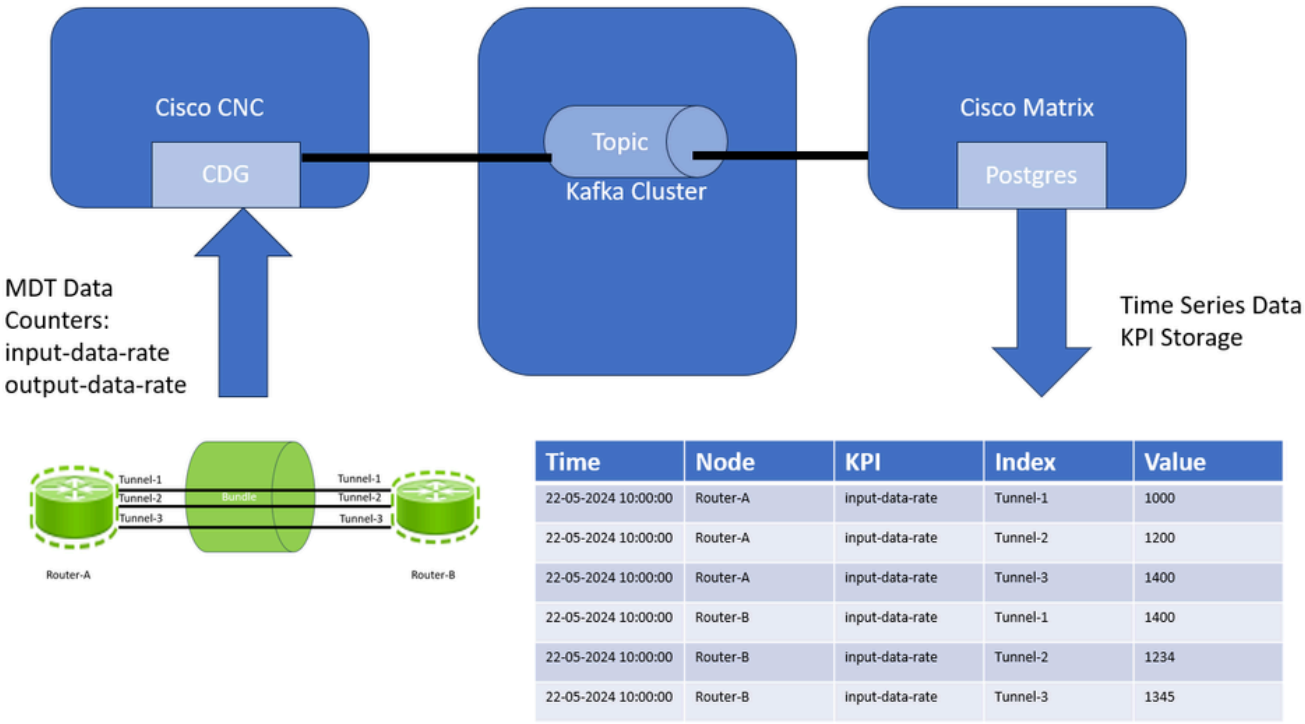
	het aantal GRE-tunnels te verhogen of te verlagen. Meer informatie: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/solution-overview-c22-2403404.html

De oplossing neemt deze stappen om aan deze gebruikscase te voldoen, die in de volgende secties verder wordt uitgewerkt.

1. Gebruik van monitortunnels tussen routers
2. Gebruik van monitorbundel tussen routerparen
3. Waarschuwingen voor drempelwaardeoverschrijding maken
4. Incident met trigger en geautomatiseerde probleemoplossing
5. Tunnels toevoegen of verwijderen en Waarschuwing wissen

Het gebruik van de tunnelbuis van de monitor tussen paren routers

Toepassingen vragen gegevensverzameling via verzameltaken. Cisco Crosswork wijst deze inzamelingstaken vervolgens toe aan een Cisco Crosswork Data Gateway om het verzoek te dienen. Crosswork Data Gateway ondersteunt gegevensverzameling van netwerkapparaten met behulp van Model-Driving Telemetry (MDT) om telemetriestromen rechtstreeks te verbruiken van apparaten (alleen voor Cisco IOS XR-gebaseerde platforms). Met Cisco Crosswork kunt u externe databestemmingen maken die kunnen worden gebruikt door collectietaken om data te deponeren.Kafka kan worden toegevoegd als nieuwe databestemmingen voor REST API-gecreëerde collectietaken. In deze oplossing verzamelt CDG gegevens van routers met betrekking tot de tunnelinterfacestatistieken en verstuurt de gegevens naar Kafta Topic.Cisco Matrix gebruikt de gegevens van het Kafka Topic en wijst de gegevens toe aan de Matrix-werknemerapplicatie die de gegevens verwerkt als een KPI en op een tijdreeksmanier opslaat zoals getoond in het volgende cijfer dat de processtroom weergeeft.



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

Cisco-oplossing voor automatisering met gesloten aansluitingen

De tijdreeksgegevens hebben KPI-kenmerken die in de Matrixdatabase worden opgeslagen.

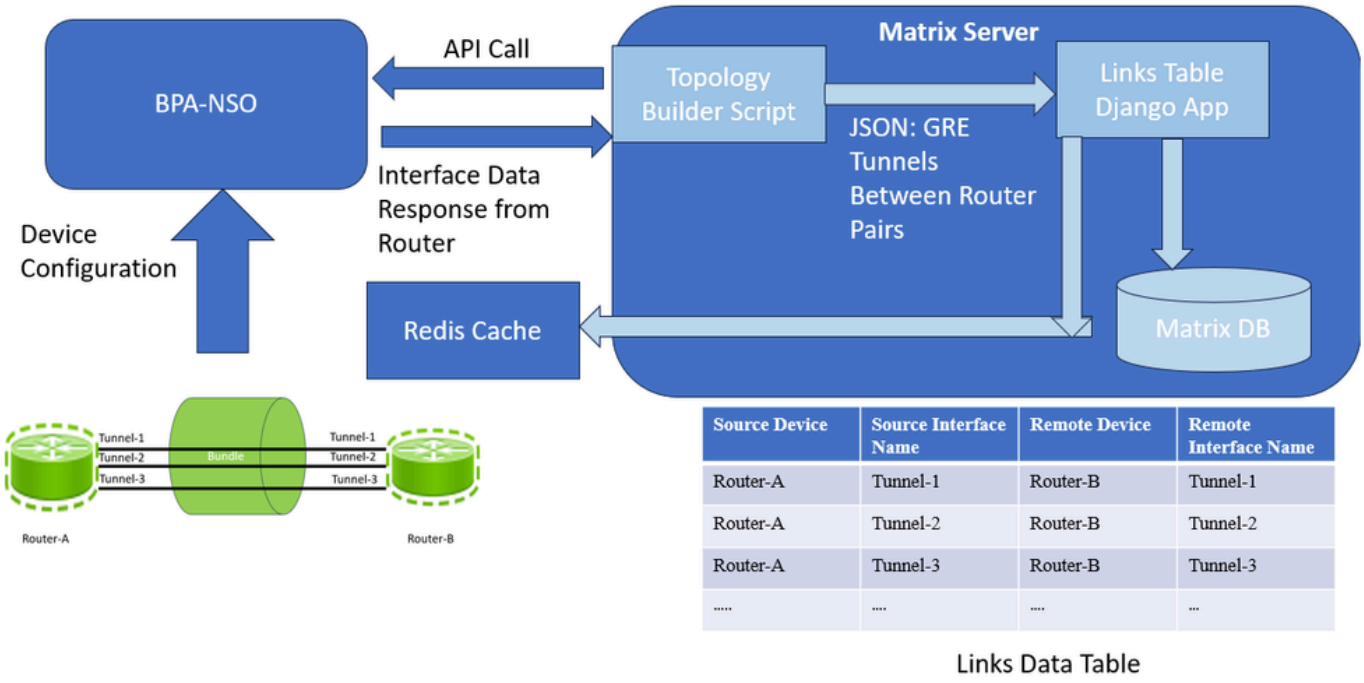
KPI-kenmerken	Doel
Knooppunt	Het apparaat of de bron waarvoor KPI is opgeslagen Voorbeeld: router-A
Tijd	Het tijdstip waarop gegevens worden verzameld Voorbeeld: 22-05-2024 10:00:00
Index	Unieke identificatiecode Voorbeeld: Tunnel-1
Waarde	Waarde van KPI - numerieke waarde
KPI	KPI-naam Voorbeeld: tunnelgebruik

Gebruik van monitorbundels tussen paren routers

Zodra u de tijdreeksgegevens zoals vermeld in de vorige sectie hebt, hebt u de verkeersstatistieken die per tunnelinterface worden verzameld. U moet echter bepalen met welk apparaat de brontunnelinterface is verbonden met welk ander apparaat en wat de naam van de externe interface is. Dit wordt Link Identification genoemd, waar u de naam van het bronapparaat identificeert. Broninterfacenaam, externe apparaatnaam en externe interfacenaam. Om de link informatie en routers nauwkeurig te interpreteren, hebt u een referentievoorbeeld nodig zoals geschetst.

bronapparaat	Naam van broninterface	Extern apparaat	Remote-interfacenaam
router-A	Tunnel-1	router-B	Tunnel-1
router-A	Tunnel-2	router-B	Tunnel-2
router-A	Tunnel-3	router-B	Tunnel-3
....	...	...	..

Om deze topologie links tabel in deze oplossing te bouwen, kunt u een aangepaste tabel, Links Data Table, gebouwd in Matrix bevolken op basis van een script dat elke dag op het gewenste tijdstip op de server loopt. Dit script maakt een API-aanroep naar BPA-NSO en krijgt een JSON-uitgang van GRE-bundels tussen routerparen terug. Dan ontleedt het de interfacegegevens om de topologie in formaat te bouwen JSON. Het script neemt ook deze JSON uitvoer en schrijft het elke dag naar de Links Data Table. Telkens wanneer het nieuwe gegevens in de tabel laadt, schrijft het deze gegevens ook naar een Redis-cache om verdere databaseraadplegingen te beperken en de efficiëntie te verbeteren.



Tabelproces voor links en gegevens

Dus, noodzakelijkerwijs alle koppelingen tussen dezelfde twee apparaten maken deel uit van de bundel die wordt geïdentificeerd om deel uit te maken van dezelfde bundel. Zodra de Raw Tunnel niveau KPI's beschikbaar zijn, dan heb je een aangepaste KPI_aggregaat app op Matrix gebouwd die de taak van het berekenen van de bundel niveau toepassingen en opslaan als een KPI.

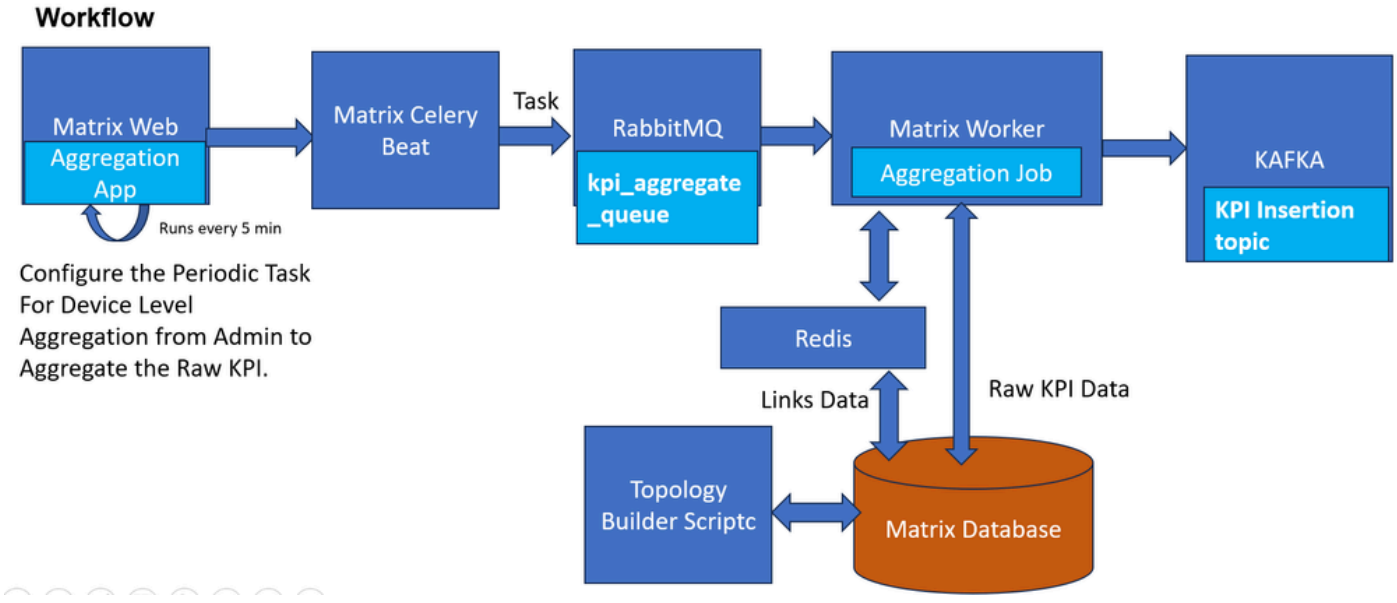
Deze toepassing neemt deze input:

Configuratiekenmerk	Doel
Crontab	De frequentie waarmee de periodieke taak van de aggregatie moet worden uitgevoerd
Selectievakje ingeschakeld	Deze configuratie activeren/deactiveren
Tunnelinterface-KPI-naam	Naam van de ruwe KPI die wordt gebruikt om de totale KPI te berekenen. De geaggregeerde KPI-naam wordt automatisch aangemaakt als <Raw_KPI_Name>_agg
Datumbereik	De frequentie van de ruwe gegevens.

De taak Aggregate neemt de ingangen van de gegevens van KPI Ruwe en het gegevensbestand van Verbindingen identificeert de tunnels die deel van de zelfde bundel uitmaken en voegt hen aan een groep toe die op deze logica wordt gebaseerd.

```
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
```

Bijvoorbeeld, in dit geval, wordt de KPI naam gegenereerd als "tunnel-use_agg" voor de onbewerkte Tunnel KPI tunnelgebruik. Zodra de berekening voor alle onbewerkte KPI-waarden voor alle routers en tunnelcombinaties is voltooid, worden deze gegevens voor elke link naar het Kafka-onderwerp gedrukt, dat hetzelfde onderwerp moet zijn dat de verwerkte KPI opneemt. Op die manier blijft deze informatie bestaan zoals alle andere normale KPI's die van geldige bronnen worden ontvangen. De DB-consument verbruikt van dit onderwerp en houdt de KPI in de KPI-resultatentabel in de Matrixdatabase voor de geaggregeerde KPI's.



KPI-aggregatieproces voor aggregaat KPI voor bundelniveau

Waarschuwingen voor drempelwaardeoverschrijding maken

De KPI-drempel die in Matrix is ingesteld, bedraagt 85%. Dit betekent dat wanneer de waarde van deze KPI de drempel overschrijdt, een kritische waarschuwing wordt gegenereerd en wanneer deze onder de drempel daalt, een duidelijke waarschuwing wordt gegenereerd. Deze

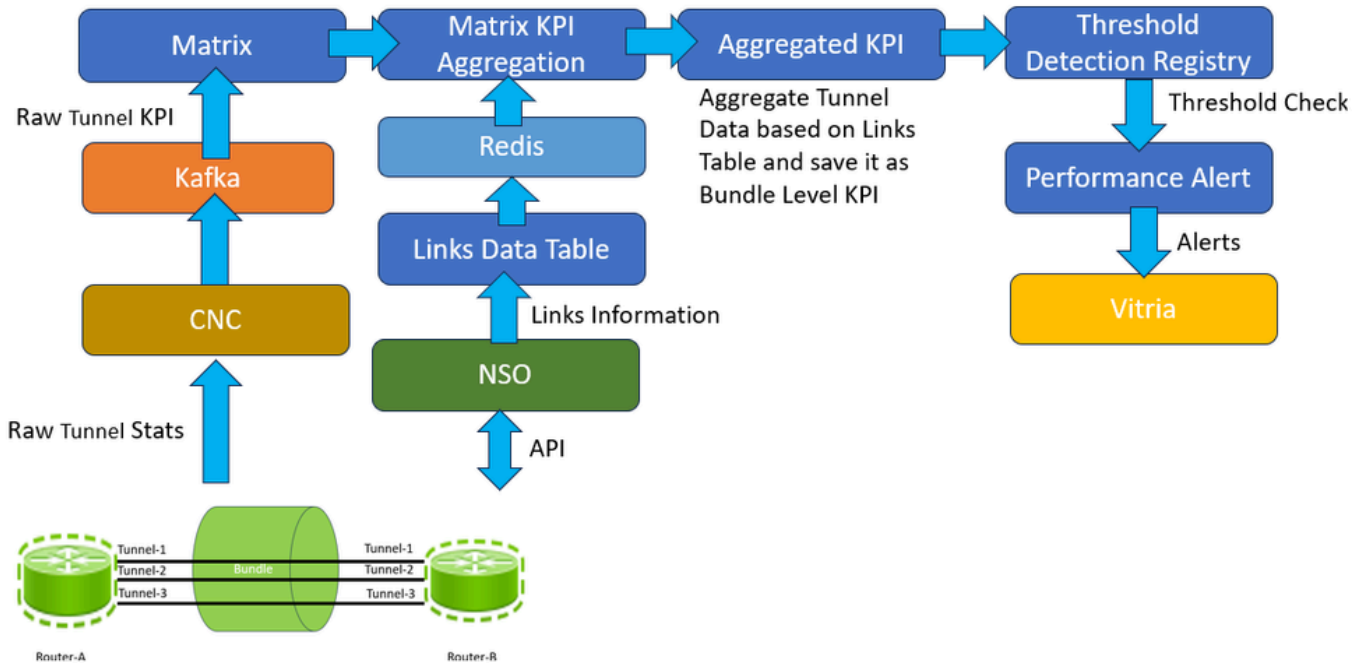
waarschuwingen worden opgeslagen in de Matrix Database en ook doorgestuurd naar Vitria in deze oplossing voor de gesloten-lus automatisering gebruikscase. Indien de berekende waarde van de KPI de drempel overschrijdt, wordt via Kafka een waarschuwing naar Vitria (VIA-AIOP's) gestuurd, waarbij de huidige staat in het bericht als kritisch wordt aangemerkt. Evenzo, als de waarde binnen de drempelwaarden van de kritische waarden terugkeert, moet hij via Kafka een waarschuwing sturen naar VIA-AIOP's met de huidige status als duidelijk in het bericht. Er is een voorbeeldbericht naar het systeem gestuurd, met de volgende kenmerken.


```
{
    "knooppunt": "router-A",
    "knooppunt_type": "router",
    "kpi": "tunnel_use_agg",
    "kpi_Description": "Gebruik bundelniveau",
    "schema": "",
    "index": "router-A_router-B",
    "tijd": "2023-08-09 05:45:00+00:00",
    "waarde": "86.0",
    "Previous_state": "CLEAR",
    "current_state": "KRITISCH",
    "link_name": "router-A_router-B"
}
```


Waarschuwingskenmerk Kafka-bericht	Voorbeeldwaarde	Doel
knoest	router-A	Apparaatnaam netwerk
knoop_type	Router	Apparaattype
KPI	tunnel_benutting_agg	KPI-naam
kpi_beschrijving	Gebruik van bundelniveau	KPI-beschrijving

Schema	NA	NA
index	router-A_router-B	<local_device>-<remote_device>
tijd	"2023-08-09 05:45:00+00:00"	tijd
waarde	86.0	KPI-waarde
Previous_state	HELDER	Vorige staat van signalering
huidige_staat	Critical (Kritiek)	Huidige staat van de signalering
link_name	router-A_router-B	Correlatiekenmerk

link_name attribuut is een alfabetisch gesorteerde naam van de apparaten aanwezig in de indexwaarde. Dit wordt gedaan om correlatie te bereiken op het niveau van de VIA-AIOP's, waar VIA AIOps de meldingen uit dezelfde bundellink moet correleren. Bijvoorbeeld, wanneer er meerdere waarschuwingen komen via AIOP's met dezelfde link_name betekent dit dat de waarschuwingen behoren tot dezelfde bundellink in het netwerk die wordt aangegeven door apparaatnamen in de link naam.



Waarschuwing voor KPI-aggregatie met behulp van matrixdetectieregister

Incident met trigger en geautomatiseerde probleemoplossing

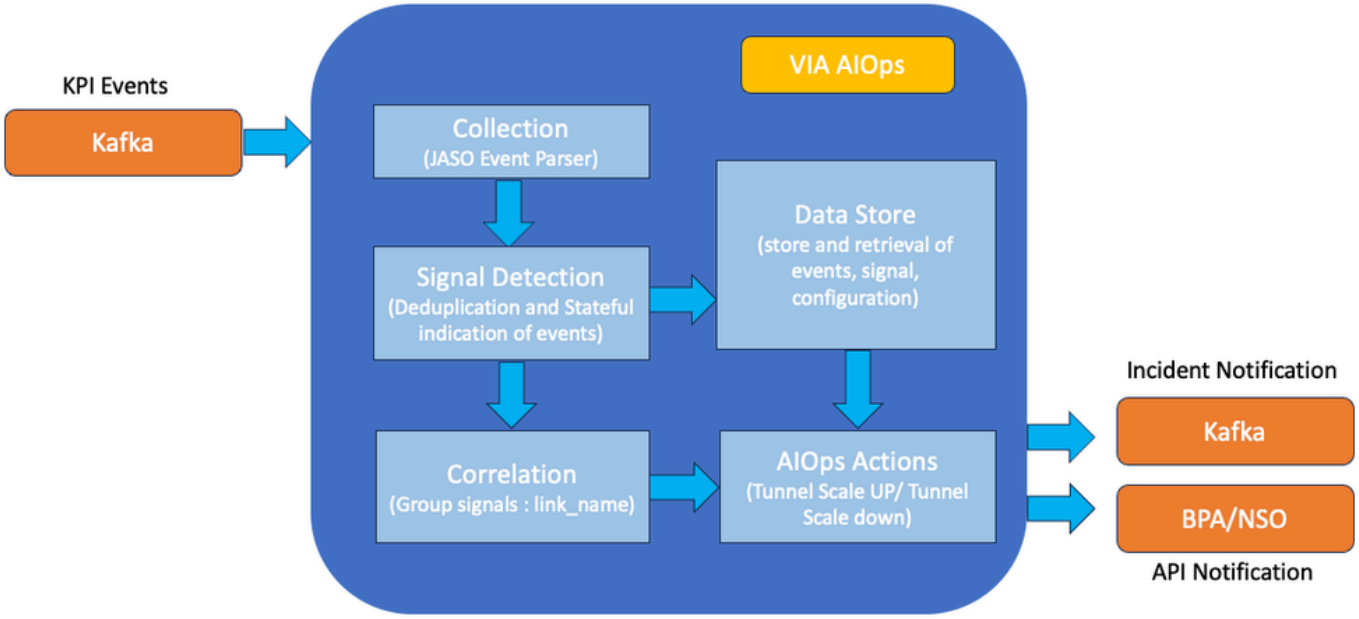
VIA AIOps moet worden geconfigureerd voor het opnemen van anomalieën in de Key Performance Indicator (KPI) van een specifiek Kafka-onderwerp. Deze gebeurtenissen, zoals ontvangen via Kafka berichten, worden verwerkt door VIA AIOps via de JASO Event Parser voor verdere inname. Het is van cruciaal belang voor VIA AIOps om KPI-anomaliegebeurtenissen met betrekking tot GRE-tunnels nauwkeurig te identificeren, hun associatie met specifieke apparaatparen te bepalen (bijvoorbeeld, router A - router B), en na te gaan of de anomalie de initiatie van GRE-tunnelschaling automatisering noodzakelijk maakt - of het een upscale of downscale is.

De JASO Event Parser binnen VIA AIOps moet worden geconfigureerd om relevante dimensies uit de Matrix KPI anomalie gebeurtenis, namelijk de "host", "kpi", "index", en "waarde", te halen en te interpreteren. Een extra dimensie, die 'automation_action' wordt genoemd, moet worden geconfigureerd om dynamisch te worden bijgewerkt door de JASO Event Parser, gebaseerd op de 'waarde' metriek aanwezig in de Matrix KPI anomalie gebeurtenis. Deze dimensie is van cruciaal belang bij het bepalen of een geautomatiseerde respons moet worden uitgevaardigd, met name of de procedures voor "GRE Tunnel Scale Up" of "GRE Tunnel Scale Down" moeten worden geactiveerd door het veld "KPI-waarde" te verwerken. In VIA AIOps vertegenwoordigt een signaal een consolidatie van staten van de gebeurtenissen. Om dit correlatieproces te verbeteren, moeten we duidelijke, stateful signalen configureren die correleren met de 'host', 'link name', 'kpi' en 'automation_action' dimensies. De tabel geeft een voorbeeld van de signalen, correlatiegroepen en hun respectieve correlatieconfiguraties.

Het signaal dat wordt geïdentificeerd als GRE_KPIA_SCALEUP zou bijvoorbeeld worden geïnitieerd na het innemen van een gespecificeerd KPI-anomaliebericht, zoals beschreven in paragraaf 3, door het VIA AIOps-systeem.

VIA AIOps-signaalnaam	Signaalcorrelatiesleutels	Naam correlatiegroepregel
GRE_KPIA_SCALEUP	Host, KPI, Link Name, Automated_action	GRE-tunneluitbreiding
GRE_KPIB_SCALEUP	Host, KPI, Link Name, Automated_action	
GRE_KPIA_SCALEDOWN	Host, KPI, Link Name, Automated_action	GRE-tunnelschaal omlaag
GRE_KPIB_SCALEDOWN	Host, KPI, Link Name, Automated_action	

De regel van de correlatiegroep wordt ontworpen om de samenvoeging van signalen over Apparaat A, Apparaat B, en hun respectieve tunnels A, B, en C in een verenigd incident te vergemakkelijken. Deze correlatieregel zorgt ervoor dat voor elke specifieke koppeling van apparaat A en apparaat B maximaal twee verschillende incidenten worden gegenereerd: één incident voor een GRE Tunnel Scale-Up met apparaat A en apparaat B, en een ander incident voor een GRE Tunnel Scale-Down voor dezelfde apparaatkoppeling. Het VIA AIOps Agent-framework is in staat om te communiceren met Business Process Automation (BPA) en Network Services Orchestrator (NSO).



KPI Event Correlatie en melding met VIA AIOps

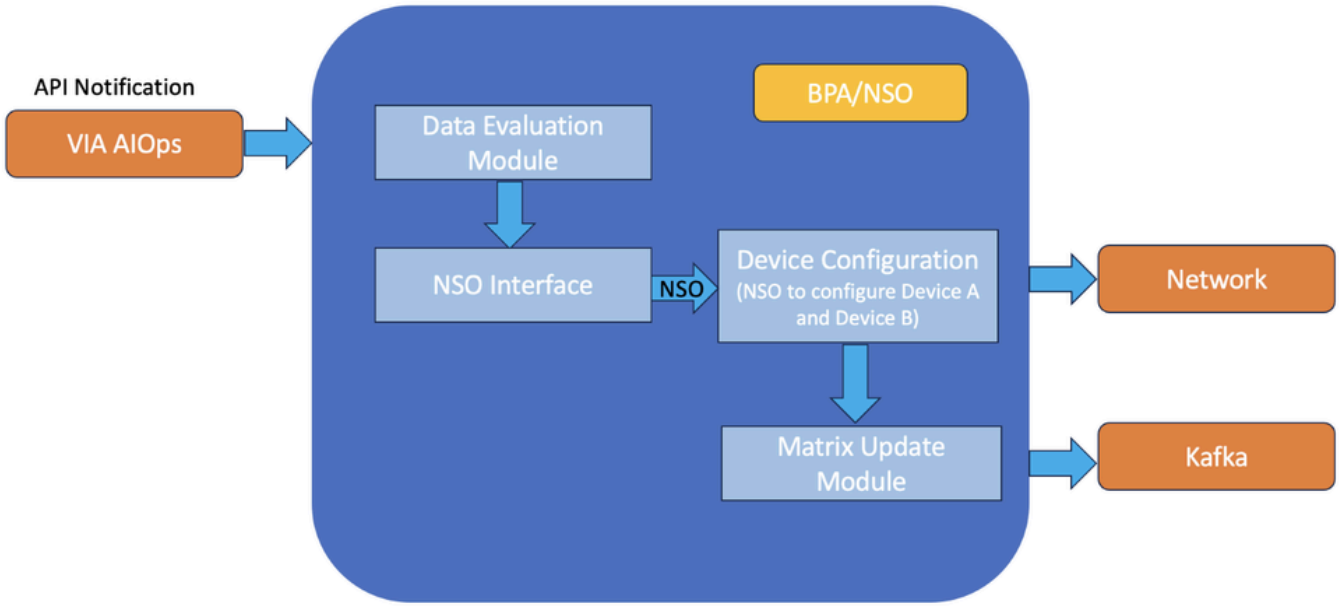
Hier is een voorbeeld van een GRE Tunnel Scale-Up API-melding verzonden naar BPA/NSO van VIA AIOps.

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

```
            { "node": "RouterB", "kpi": "tunnel_utilization_agg" }
          ]
        }
      ]
    }
  ]
}
```

Tunnels toevoegen of verwijderen en Waarschuwing wissen

Na ontvangst van een API-oproep van VIA AIOps, initieert Cisco Business Process Automation (BPA) de benodigde schalingrichtlijnen door middel van interne verzoeken aan de Cisco Network Service Orchestrator (NSO). De BPA beoordeelt de gegevens-payload die door VIA AIOps wordt geleverd, waaronder tunneldetails, een index en Matrixgegevens. De informatie over de index en de tunnelwerking wordt gebruikt om met de NSO te communiceren, en levert parameters voor het schalen van de werking. Gelijktijdig worden de Matrixgegevens verwerkt door de 'Matrix Update Module', die verantwoordelijk is voor het oplossen van eventuele KPI-anomaliegebeurtenissen door de Matrix API's te koppelen.

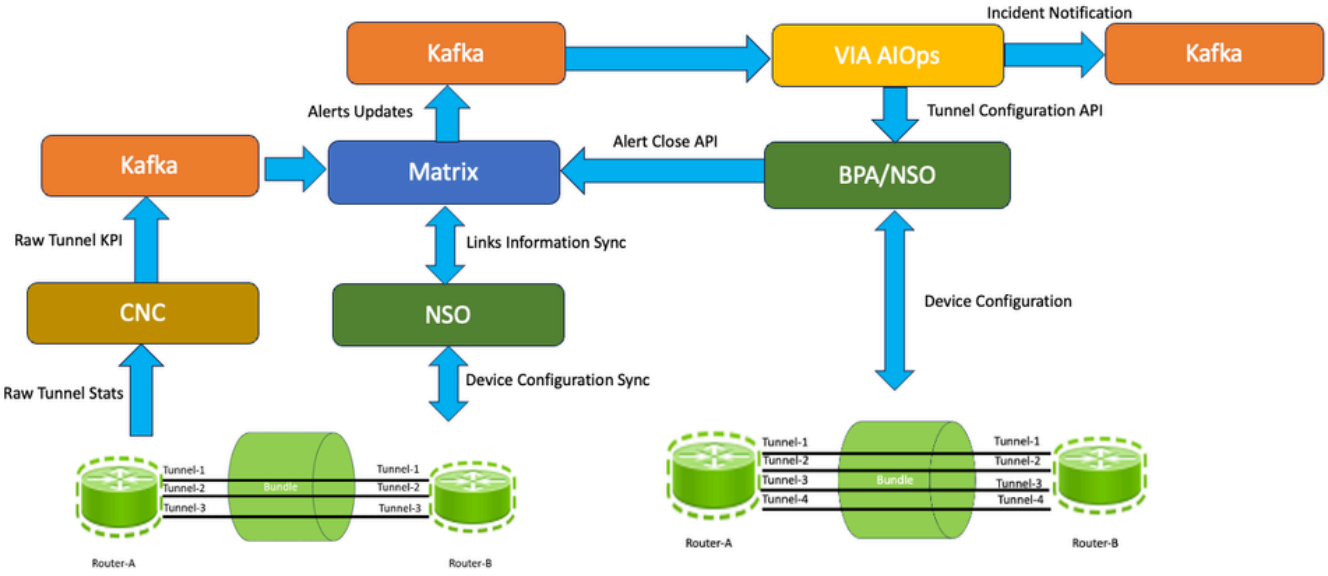


Gegevensvalidatie en apparaatconfiguratie met behulp van BPA-NSO

Voor het initiëren van eventuele schalingoperaties, moet er een YANG actiemodel ontwikkeld worden voor de NSO. Dit model bepaalt de specifieke acties die NSO moet uitvoeren om of de tunneltelling tussen Router A en Router B te verhogen of te verminderen. Het Business Process Automation (BPA)-systeem begint met het schalen van bewerkingen door samen te werken met

de Network Service Orchestrator (NSO) om een 'dry run' uit te voeren. Dit is de eerste fase van de operatie waarin de BPA de NSO verzoekt om de voorgenomen configuratiewijzigingen te simuleren zonder deze toe te passen. De testrun fungeert als een essentiële validatiestap, die ervoor zorgt dat de voorgestelde schaalhandelingen, zoals gedefinieerd door het YANG-actiemodel, kunnen worden uitgevoerd zonder fouten of conflicten in de netwerkconfiguratie te veroorzaken.

Als de testrun als succesvol wordt beschouwd, wat aangeeft dat de schalingacties zijn gevalideerd, gaat de BPA vervolgens verder naar het 'commit' stadium. Op dit punt instrueert de BPA de NSO om de daadwerkelijke configuratiewijzigingen te implementeren die nodig zijn om het aantal GRE-tunnels tussen router A en router B te verhogen of te verlagen. De BPA activeert de 'Matrix Update Module' naar Matrix met behulp van een API-oproep om de KPI-gebeurtenis te sluiten in combinatie met VIA AIOps. Zodra deze anomalie is gesloten op Matrix, stuurt Matrix ook een waarschuwing met strengheid als "Cleared" naar VIA AIOps, die het incident verder sluit op zijn einde. Op deze manier is de herstelcyclus op netwerkniveau voltooid. Een algemene versie van de gegevensstroom binnen de toepassing, die in deze gesloten-lusautomatisering wordt gebruikt, wordt afgebeeld in dit beeld.



Gegevensstroom voor een GRE-tunnelbundel met gesloten lus - automatisering

Het sluiten van de Lijn om Nieuwe Mogelijkheden van Automatische Oplossing te openen

De oplossing die in dit document wordt besproken, wordt doelbewust besproken met één voorbeeld van GRE Bundle-schaling gebaseerd op netwerkanomalieën om ons te helpen in verband te brengen met verschillende bouwstenen van deze oplossing. Het is in een samenvatting bestudeerd hoe Cisco Technology Stack, die Cisco NSO, Cisco Matrix en Cisco BPA omvat, naadloos kan integreren met componenten zoals VIA AIOps, Kafka en een andere softwarestack om ons te helpen netwerkproblemen automatisch te monitoren en te verhelpen. Deze oplossing biedt mogelijkheden voor alle andere netwerkgebruiksgevallen die typische problemen kunnen zijn die zich voordoen in serviceproviders of ondernemingsnetwerken.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.