Automazione della larghezza di banda su richiesta grazie allo stack di software di automazione a loop chiuso

Sommario

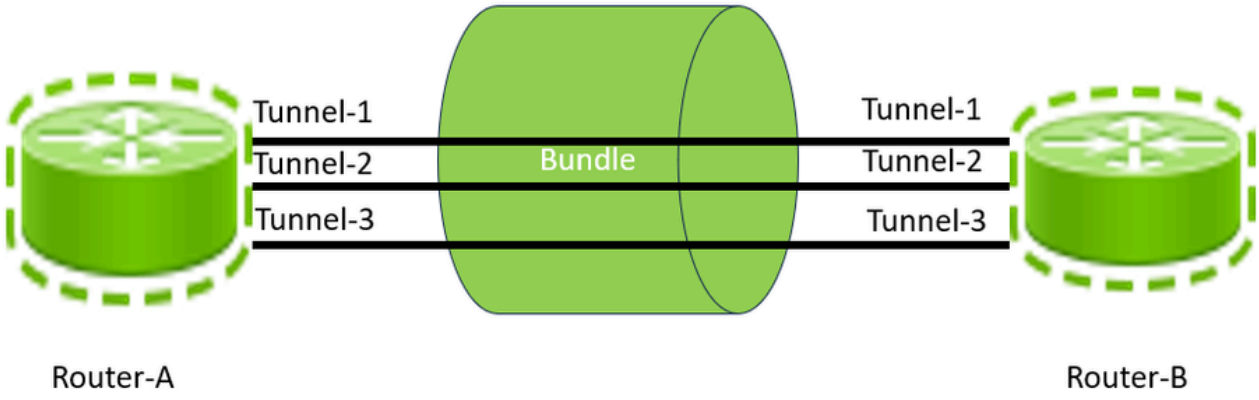
Introduzione

Questo documento descrive i componenti di una soluzione di automazione a loop chiuso Cisco per l'automazione della scalabilità del tunnel GRE (Generic Routing Encapsulation) e la sua adattabilità in altri casi.

Premesse

I provider di servizi desiderano assumere il controllo dell'utilizzo della larghezza di banda nei tunnel GRE della rete e monitorarli da vicino per scalare i tunnel in base alle esigenze utilizzando una soluzione di automazione intelligente a loop chiuso.

GRE è un protocollo di tunneling che fornisce un approccio semplice e generico al trasporto di pacchetti di un protocollo su un altro utilizzando l'incapsulamento. Questo documento è dedicato all'esempio basato sul tunnel GRE per la piattaforma Cisco IOS® XRv, ma può essere generalizzato anche su altre piattaforme. GRE incapsula un payload, un pacchetto interno che deve essere recapitato a una rete di destinazione all'interno di un pacchetto IP esterno. Il tunnel GRE si comporta come un collegamento virtuale point-to-point con due endpoint identificati dall'origine del tunnel e dall'indirizzo di destinazione del tunnel.



Tunnel GRE tra router

La configurazione di un tunnel GRE comporta la creazione di un'interfaccia tunnel e la definizione dell'origine e della destinazione del tunnel. L'immagine mostra la configurazione di tre tunnel GRE tra il router A e il router B. Per questa configurazione, è necessario creare tre interfacce, ciascuna sul router-A, ad esempio Tunnel-1, Tunnel-2 e Tunnel-3, e analogamente creare tre interfacce sul router-B, ad esempio Tunnel-1, Tunnel-2 e Tunnel-3. Tra due router di provider di servizi, possono esistere più tunnel GRE. Ciascun tunnel, come qualsiasi altra interfaccia di rete, ha una capacità definita basata sulla capacità dell'interfaccia. Pertanto, un tunnel può trasportare solo un traffico massimo uguale alla sua larghezza di banda. Il numero di tunnel è spesso basato sulla previsione iniziale del carico di traffico e dell'utilizzo della larghezza di banda tra due siti (router). Con le modifiche alla rete e all'espansione della rete, l'utilizzo della larghezza di banda dovrebbe cambiare. Per utilizzare al meglio la larghezza di banda della rete, è importante aggiungere nuovi tunnel o rimuovere i tunnel aggiuntivi tra due dispositivi in base all'utilizzo della larghezza di banda misurato su tutti i tunnel tra i due dispositivi.

Da questo esempio, si può dire che la capacità totale di tutti e tre i tunnel tra il router A e il router B è la somma delle capacità del tunnel 1, 2 e 3, chiamato larghezza di banda aggregata o larghezza di banda a livello di bundle GRE. Si tenga presente che la parola chiave 'bundle' qui si riferisce ai tunnel tra una coppia di router; non si intende alcuna relazione implicita con il link bundling LACP/Etherchannel. Inoltre, il traffico effettivo tra i due router è il traffico aggregato totale tra il tunnel 1, il tunnel 2 e il tunnel 3. In genere, è possibile concepire un concetto di utilizzo della larghezza di banda a livello di bundle, che può essere un rapporto tra il traffico totale attraverso i tunnel e la capacità totale di tutti i tunnel tra due router. In genere, qualsiasi provider di servizi desidera intraprendere un'azione correttiva aggiungendo o rimuovendo tunnel tra due router se rileva che la larghezza di banda viene sovrautilizzata o sottoutilizzata. Tuttavia, per questo documento, si consideri che la soglia inferiore è del 20% per il basso utilizzo e dell'80% per l'utilizzo elevato per l'utilizzo a livello di bundle tra due router.

Requisiti

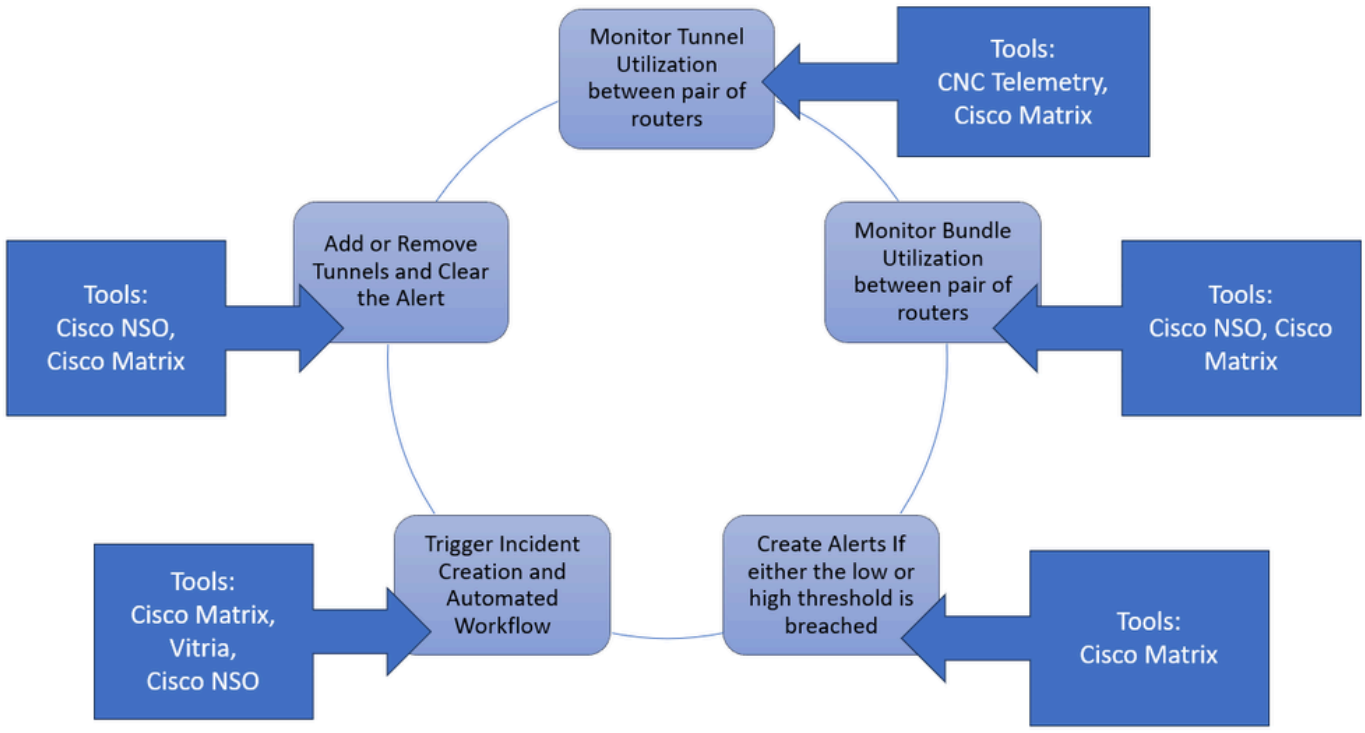
1. La soluzione a loop chiuso è necessaria per eseguire l'automazione end-to-end a loop chiuso del bundle GRE su XRv9K, dove il sistema può raccogliere dati di telemetria, monitorare i dati sotto forma di indicatori di prestazioni chiave (KPI), applicare l'aggregazione, creare avvisi incrociati di soglia (TCA) ed eseguire la configurazione di correzione automatica e chiudere l'avviso.
2. La soluzione può calcolare un indicatore di prestazioni chiave della rete (KPI) per fornire l'utilizzo della larghezza di banda Rx (Tunnel Ingress) e Tx (Tunnel Egress) di ogni tunnel, basato sul throughput raw dei tunnel alla frequenza desiderata.
3. La soluzione può calcolare indicatori KPI personalizzati per fornire l'utilizzo della larghezza di banda in entrata nel tunnel (Rx) e in uscita dal tunnel (Tx) di ogni bundle, che è l'utilizzo della larghezza di banda aggregata di tutti i tunnel tra una coppia di router.
4. La soluzione è in grado di rilevare e creare avvisi se le soglie definite a livello di bundle vengono superate. Tali allarmi sono disponibili per il monitoraggio.
5. L'avviso deve determinare l'attivazione di un flusso di lavoro automatico che può attivare ulteriormente la configurazione sul dispositivo per aggiungere o rimuovere tunnel in base alle condizioni di avviso.
6. Infine, il sistema deve chiudere automaticamente gli avvisi con gli aggiornamenti necessari.

Soluzione

La soluzione di automazione a loop chiuso prevede l'utilizzo di più strumenti che consentono di raggiungere l'obiettivo specifico di questa soluzione completa. In questa immagine vengono illustrati i componenti e gli strumenti che consentono di ottenere l'architettura finale e viene illustrato il ruolo di alto livello. Potete esaminare ciascun componente e il relativo utilizzo nelle sezioni successive.

Soluzione

Cisco



Closed Loop Automation

Strumento	Scopo
Cisco Crosswork Network Controller (CNC)	Crosswork Network Controller consente una visibilità in tempo reale sull'intero ciclo di vita dei servizi e dei dispositivi, con una navigazione intuitiva tra topologia di rete, inventario dei servizi, criteri di trasporto, stato dei servizi, stato dei dispositivi e altro ancora, supportando una vasta gamma di casi di utilizzo con un'esperienza utente comune e integrata. In questa soluzione viene utilizzato principalmente come strumento per la gestione dei dispositivi e la raccolta dei dati sulle prestazioni del tunnel tramite gNMI (gRPC Network Management Interface) o MDT. Ulteriori informazioni: https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-controller/index.html
Cisco Matrix	I servizi di analisi CX (pacchetti di funzioni) vengono forniti utilizzando la soluzione Matrix, una soluzione di analisi multidominio a finestra singola multivendor. In questa soluzione, la matrice utilizza i dati di Kafka inviati da CNC tramite gli argomenti Kafka ed esegue ulteriormente l'aggregazione di KPI basati su tunnel in KPI a livello di bundle utilizzando ricerche di topologia e li memorizza come dati di serie temporali e li memorizza nel database Postgres. Una volta archiviati, tali dati sono disponibili per la visualizzazione e Matrix dispone di un rilevamento delle

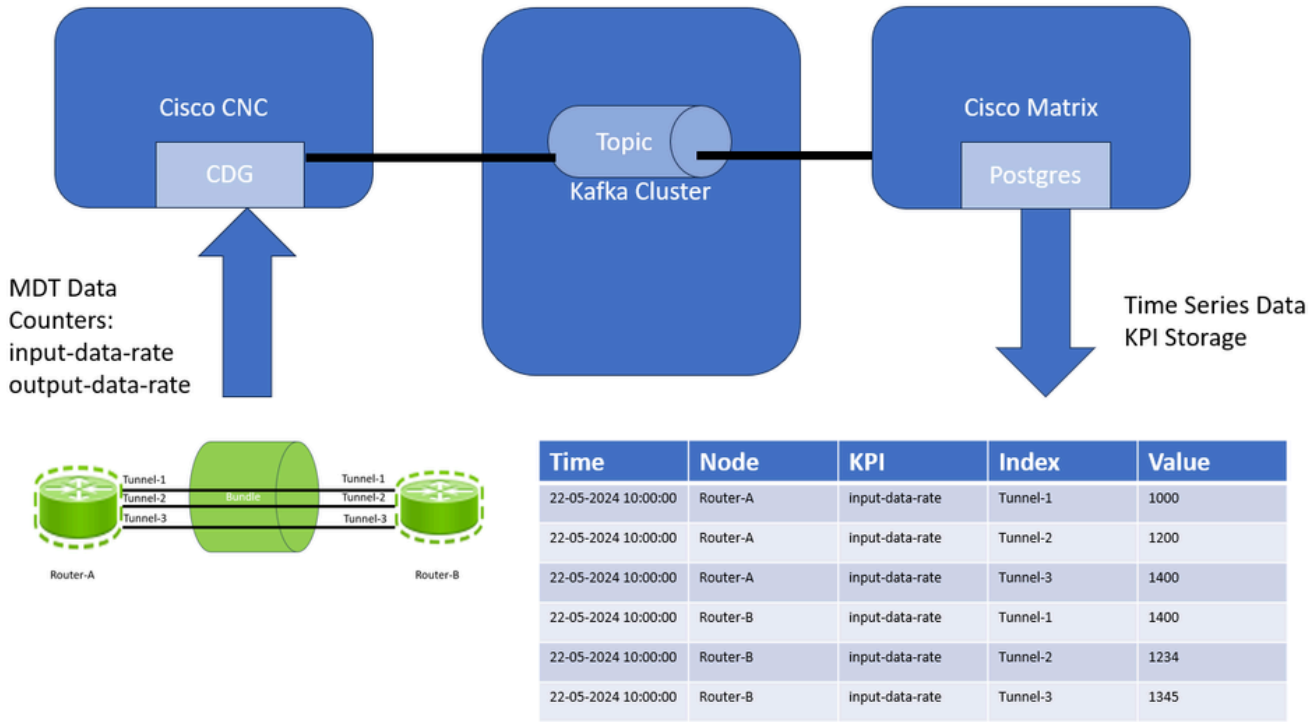
	anomalie mediante avvisi di superamento delle soglie che consente di configurare le soglie per gli indicatori KPI raccolti dalla rete.
Cluster Kafka	Un cluster Kafka è un sistema che comprende diversi argomenti dei broker e le rispettive partizioni. Un producer invia o scrive dati/messaggi all'argomento all'interno del cluster. Un consumer legge o utilizza i messaggi dal cluster Kafka. In questa soluzione, il CNC agisce come il Producer che invia i dati agli argomenti Kafka predefiniti sotto forma di payload JSON dopo la conversione dei dati dalla Telemetria raccolti dai router. In questa soluzione, Matrix agisce da consumer che utilizza i dati, li elabora, li aggrega e li memorizza per ulteriori elaborazioni e rilevamenti di anomalie.
Cisco NSO	Cisco Crosswork Network Services Orchestrator (NSO) NSO fa parte del portafoglio Crosswork di strumenti di automazione progettati per i provider di servizi e le grandi aziende. In questa soluzione, NSO raccoglie le informazioni relative a tutti i tunnel e i dispositivi e crea una tabella di topologia personalizzata per questa soluzione. Inoltre, in questa soluzione, NSO insieme alle funzionalità di Business Process Automation viene utilizzato per attivare un flusso di lavoro di monitoraggio e aggiornamento e per intraprendere azioni quali l'aggiunta o la rimozione di un tunnel dal dispositivo e l'ulteriore cancellazione di avvisi nella Cisco Matrix. Ulteriori informazioni: https://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html
Vitria VIA AIOps	Vitria VIA AIOps per Cisco Network Automation fornisce l'analisi automatizzata che consente di correggere rapidamente gli eventi che hanno un impatto sui servizi in tutti i livelli di tecnologia e applicazioni. In questa soluzione, VIA AIOps viene utilizzato per correlare gli eventi di soglia KPI generati da Cisco Matrix per creare un incidente, una notifica e attivare un'azione automatizzata nei confronti di Cisco NSO per aumentare o ridurre il numero di tunnel GRE. Ulteriori informazioni: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/solution-overview-c22-2403404.html

La soluzione adotta le seguenti misure per soddisfare questo caso di utilizzo, che sono illustrate nelle sezioni successive.

1. Monitoraggio dell'utilizzo del tunnel tra coppie di router
2. Monitoraggio dell'utilizzo del bundle tra coppie di router
3. Crea avvisi di superamento soglia
4. Attivazione di incidenti e risoluzione automatica dei problemi
5. Aggiungi o rimuovi tunnel e cancella avviso

Monitoraggio dell'utilizzo del tunnel tra coppie di router

Le applicazioni richiedono la raccolta dei dati tramite processi di raccolta. Cisco Crosswork assegna quindi questi processi di raccolta a un Cisco Crosswork Data Gateway per soddisfare la richiesta. Crosswork Data Gateway supporta la raccolta di dati da dispositivi di rete utilizzando la telemetria guidata dal modello (MDT) per utilizzare i flussi di telemetria direttamente dai dispositivi (solo per piattaforme Cisco IOS XR). Cisco Crosswork consente di creare destinazioni dati esterne che possono essere utilizzate dai processi di raccolta per depositare i dati.Kafka può essere aggiunto come nuove destinazioni dati per i processi di raccolta creati dall'API REST. In questa soluzione, CDG raccoglie i dati dai router correlati alle statistiche dell'interfaccia del tunnel e li invia all'argomento Kafta. Cisco Matrix utilizza i dati dall'argomento Kafka e li assegna all'applicazione di lavoro Matrix, che elabora i dati come KPI e li salva in una serie temporale, come mostrato nella figura seguente che mostra il flusso del processo.



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

Soluzione Cisco Closed Loop Automation

I dati delle serie temporali dispongono di attributi KPI memorizzati nel database matrice.

Attributi KPI	Scopo
Nodo	Dispositivo o origine per cui è archiviato l'indicatore KPI

	Esempio: Router-A
Ora	Ora di raccolta dei dati Esempio: 22-05-2024 10:00:00
Indice	Identificatore univoco Esempio: Tunnel-1
Valore	Valore indicatore KPI - Valore numerico
KPI	Nome indicatore KPI Esempio: utilizzo del tunnel

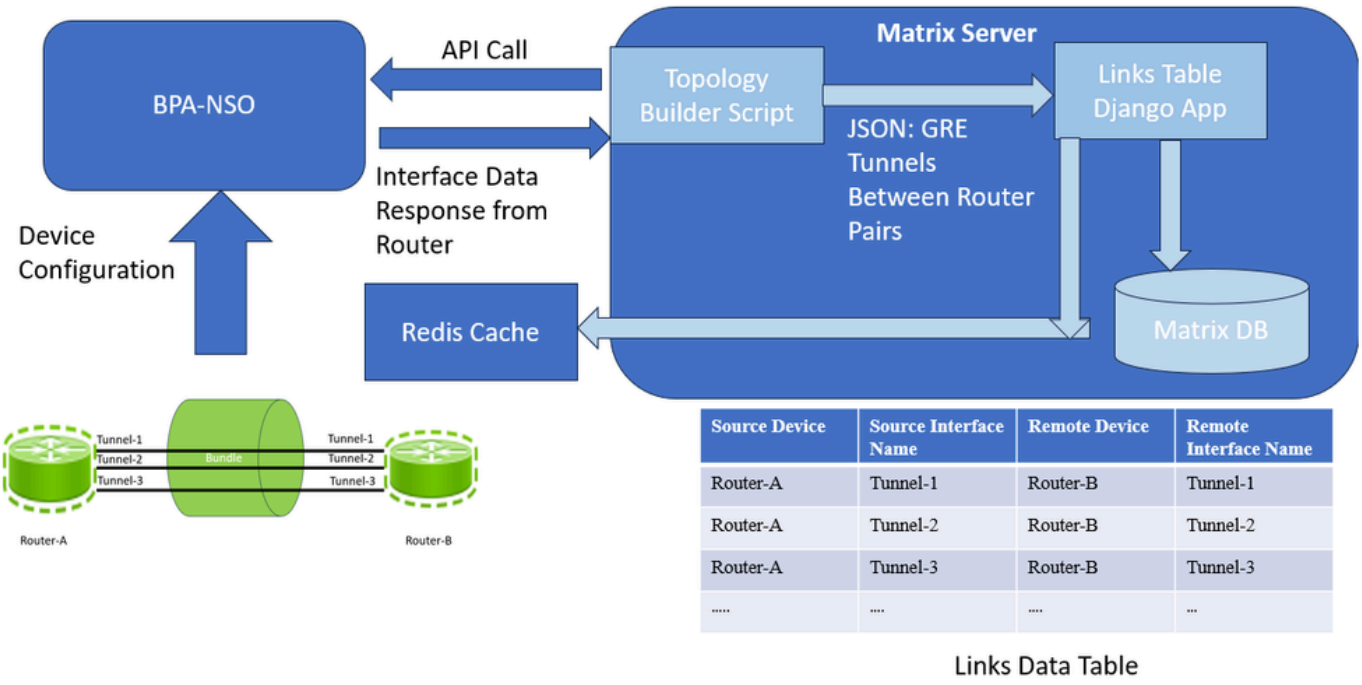
Monitoraggio dell'utilizzo dei bundle tra coppie di router

Una volta ottenuti i dati della serie temporale menzionati nella sezione precedente, si ottengono le statistiche sul traffico raccolte per ciascuna interfaccia del tunnel. Tuttavia, è necessario identificare il dispositivo a cui è collegata l'interfaccia del tunnel di origine, nonché il nome dell'interfaccia remota. Questa operazione è denominata identificazione del collegamento, in cui si identifica il nome del dispositivo di origine. Nome interfaccia di origine, Nome dispositivo remoto e Nome interfaccia remota. Per interpretare correttamente le informazioni sul collegamento e i router, occorre un esempio di riferimento così come descritto.

Dispositivo di origine	Nome interfaccia di origine	Dispositivo remoto	Nome interfaccia remota
Router-A	Tunnel-1	Router-B	Tunnel-1
Router-A	Tunnel-2	Router-B	Tunnel-2
Router-A	Tunnel-3	Router-B	Tunnel-3
...	...	...	..

Per generare la tabella dei collegamenti della topologia in questa soluzione, è possibile popolare una tabella personalizzata, la tabella dei collegamenti dati, incorporata nella matrice basata su uno script in esecuzione sul server ogni giorno all'ora preferita. Questo script effettua una chiamata API a BPA-NSO e restituisce un output JSON dei bundle GRE tra coppie di router.

Quindi analizza i dati dell'interfaccia per creare la topologia in formato JSON. Lo script accetta inoltre questo output JSON e lo scrive nella tabella dei dati dei collegamenti ogni giorno. Ogni volta che carica i nuovi dati nella tabella, questi vengono anche scritti in una cache Redis per ridurre ulteriormente le ricerche nel database e migliorare l'efficienza.



Source Device	Source Interface Name	Remote Device	Remote Interface Name
Router-A	Tunnel-1	Router-B	Tunnel-1
Router-A	Tunnel-2	Router-B	Tunnel-2
Router-A	Tunnel-3	Router-B	Tunnel-3
.....	....	....	...

Links Data Table

Processo della tabella dati dei collegamenti

Quindi, necessariamente tutti i collegamenti tra gli stessi due dispositivi fanno parte del bundle che viene identificato come appartenente allo stesso bundle.Una volta che gli indicatori KPI a livello di tunnel raw sono disponibili, è stata creata un'app KPI_aggregate personalizzata su Matrix che esegue il lavoro di calcolo degli utilizzi a livello di Bundle e di memorizzazione come KPI.

Questa applicazione accetta i seguenti input:

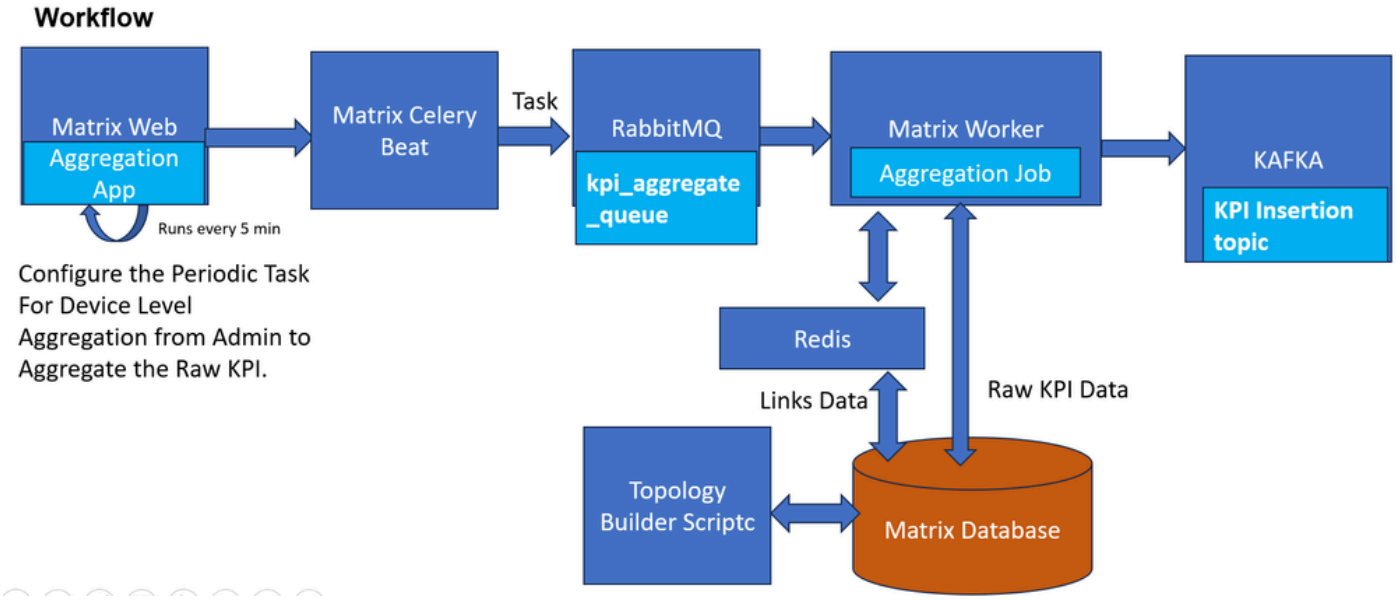
Attributo Configuration	Scopo
Scheda Cronc	Frequenza di esecuzione dell'attività periodica di aggregazione
Casella di controllo Abilitato	Attiva/Disattiva questa configurazione
Nome indicatore KPI interfaccia tunnel	Nome dell'indicatore KPI non elaborato utilizzato per calcolare l'indicatore KPI aggregato. Il nome dell'indicatore KPI aggregato viene creato automaticamente come <Raw_KPI_Name>_agg

Intervallo date	Frequenza dei dati grezzi.

Il task Aggrega accetta gli input dal database dei dati non elaborati e dei collegamenti KPI e identifica i tunnel che fanno parte dello stesso bundle e li aggiunge a un gruppo in base a questa logica.

```
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
```

Ad esempio, in questo caso, il nome dell'indicatore KPI viene generato come "tunnel-usage_agg" per l'utilizzo del tunnel KPI del tunnel raw. Una volta completato il calcolo per tutti i valori degli indicatori KPI non elaborati per tutti i router e le combinazioni di tunnel, i dati vengono sottoposti a push per ogni collegamento all'argomento Kafka, che deve essere lo stesso argomento che acquisisce l'indicatore KPI elaborato. In questo modo, queste informazioni persistono come qualsiasi altro normale indicatore KPI ricevuto da origini valide. Il consumer DB utilizza da questo argomento e mantiene l'indicatore KPI nella tabella dei risultati dell'indicatore KPI nel database matrice per gli indicatori KPI aggregati.



Processo di aggregazione KPI per l'indicatore prestazioni chiave Aggregazione a livello di aggregazione

Crea avvisi di superamento soglia

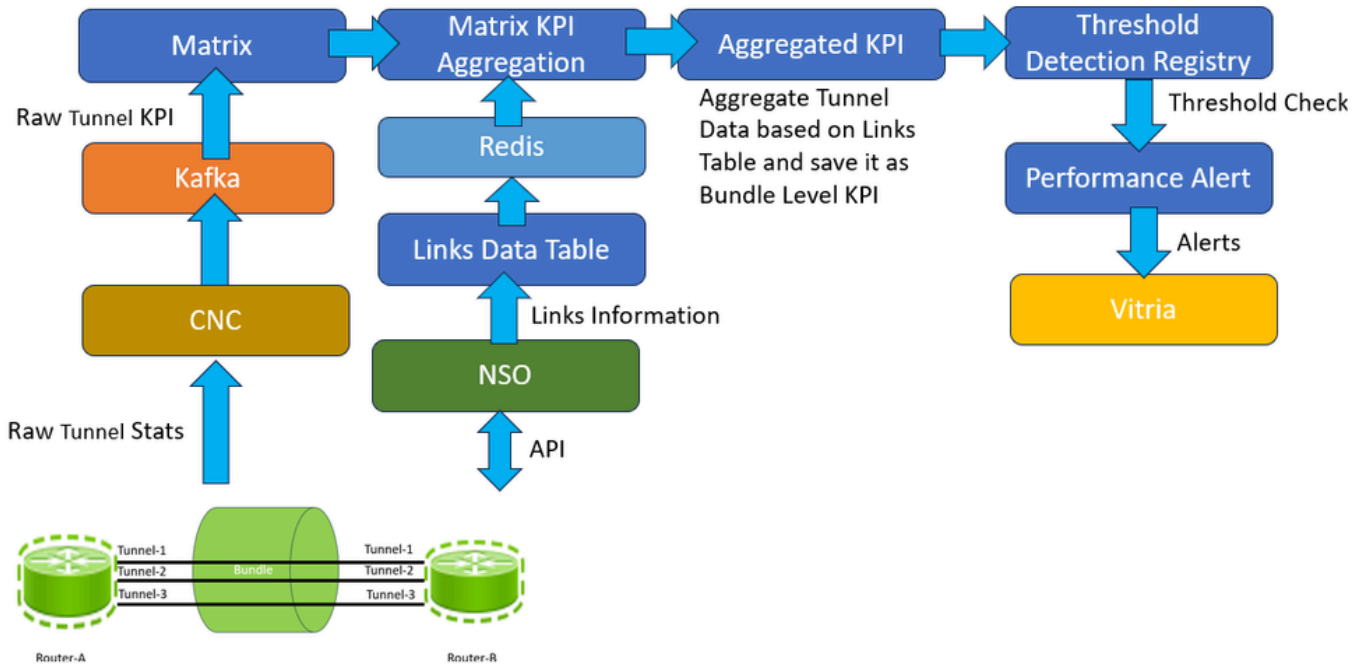
La soglia KPI configurata nella matrice è dell'85%, ovvero quando il valore di questo indicatore KPI supera la soglia, viene generato un avviso critico e quando scende al di sotto della soglia, viene generato un avviso chiaro. Questi avvisi vengono salvati nel database Matrix e inoltrati anche a Vitria in questa soluzione per il caso di utilizzo dell'automazione a loop chiuso. Se il valore calcolato dell'indicatore KPI supera la soglia, viene inviato un avviso a Vitria (VIA-AIOPs) tramite Kafka con lo stato corrente di Critico nel messaggio. Analogamente, se il valore rientra nei valori di soglia rispetto ai valori critici, deve inviare un avviso ai VIA-AIOP tramite Kafka con lo stato corrente impostato su Clear nel messaggio. È stato inviato un messaggio di esempio al sistema con i seguenti attributi.


```
{
   "node": "Router-A",
   "node_type": "Router",
   "kpi": "tunnel_usage_agg",
   "kpi_description": " Utilizzo livello bundle",
   "schema": "",
   "index": "Router-A_Router-B",
   "time": "2023-08-09 05:45:00+00:00",
   "valore": "86,0",
   "PREVIOUS_state": "CLEAR",
   "current_state": "CRITICAL",
   "link_name": "Router-A_Router-B"
}
```


Attributo messaggio avviso Kafka	Valore di esempio	Scopo
nodo	Router-A	Nome dispositivo di rete
tipo_nodo	Router	Tipo di dispositivo
KPI	agg_utilizzo_tunnel	Nome indicatore KPI

descrizione_indicatore	Utilizzo livello bundle	Descrizione indicatore KPI
Schema	N/D	N/D
indice	Router-A_Router-B	<periferica_locale>-<periferica_remota>
tempo	"2023-08-09 05:45:00+00:00"	tempo
valore	86.0	Valore indicatore KPI
stato_precedente	CANCELLA	Stato di allerta precedente
stato_corrente	CRITICO	Stato attuale dell'avviso
nome_collegamento	Router-A_Router-B	Attributo Correlation

l'attributo link_name è un nome in ordine alfabetico dei dispositivi presenti nel valore di indice. Ciò avviene per ottenere la correlazione a livello di VIA AIOP, dove VIA AIOps deve correlare gli allarmi provenienti dallo stesso collegamento di bundle. Ad esempio, quando vengono inviati più alert a VIA AIOP con lo stesso nome_collegamento, gli alert appartengono allo stesso collegamento in bundle nella rete indicato dai nomi dei dispositivi nel nome del collegamento.



Generazione di avvisi di aggregazione KPI tramite il Registro di sistema per il rilevamento della matrice

Attivazione di incidenti e risoluzione automatica dei problemi

La tecnologia VIA AIOps deve essere configurata per l'acquisizione di eventi anomali degli indicatori di prestazioni chiave (KPI) da un argomento Kafka designato. Questi eventi, così come ricevuti tramite messaggi Kafka, vengono elaborati da VIA AIOps tramite JASO Event Parser per la successiva acquisizione. Per VIA AIOps è di fondamentale importanza identificare con precisione gli eventi anomali KPI relativi ai tunnel GRE, determinarne l'associazione con coppie di dispositivi specifiche (ad esempio, router A - router B) e verificare se l'anomalia richiede l'avvio dell'automazione della scalabilità del tunnel GRE, sia in caso di upscale che di downscale.

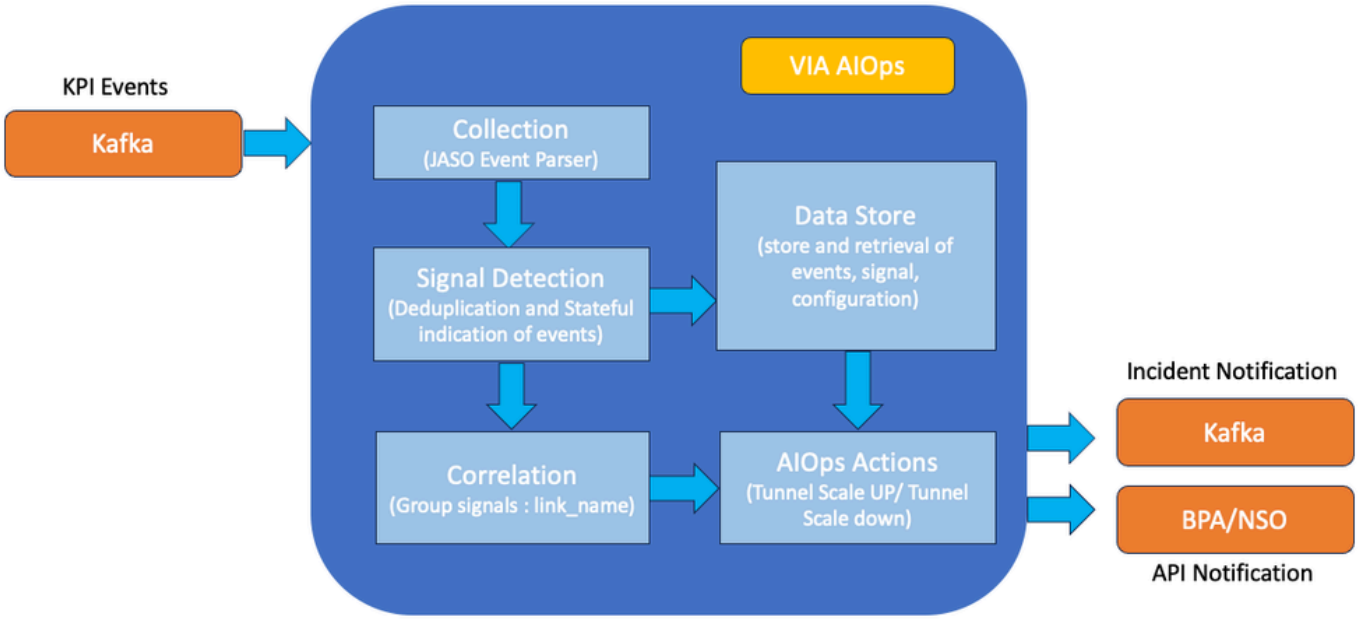
Il parser di eventi JASO all'interno di VIA AIOps deve essere configurato per estrarre e interpretare le dimensioni rilevanti dall'evento di anomalia KPI della matrice, ovvero "host", "kpi", "index" e "value". È necessario configurare una dimensione aggiuntiva, denominata 'automation_action', per l'aggiornamento dinamico da parte del parser di eventi JASO, in base alla metrica 'value' presente nell'evento di anomalia KPI della matrice. Questa dimensione è fondamentale per determinare se è necessario eseguire una risposta automatizzata, in particolare se attivare le procedure 'Scalabilità del tunnel GRE' o 'Scalabilità del tunnel GRE' elaborando il campo 'Valore KPI'. In VIA AIOps, un segnale rappresenta un consolidamento degli stati degli eventi. Per migliorare questo processo di correlazione, è necessario configurare segnali distinti con informazioni sullo stato che siano correlati alle dimensioni 'host', 'nome collegamento', 'kpi' e 'automation_action'. Nella tabella sono illustrati i segnali, i gruppi di correlazione e le rispettive configurazioni di correlazione.

Ad esempio, il segnale identificato come GRE_KPIA_SCALEUP viene attivato dopo l'acquisizione di un messaggio di anomalia KPI specificato, come descritto nella sezione 3, da parte del sistema VIA AIOps.

Nome segnale VIA AIOps	Tasti di correlazione del segnale	Nome regola gruppo di correlazione
GRE_KPIA_SCALEUP	Host,indicatore KPI, Nome collegamento, Azione_automatica	Scalabilità del tunnel GRE
GRE_KPIB_SCALEUP	Host,indicatore KPI, Nome collegamento, Azione_automatica	
GRE_KPIA_SCALEDOWN	Host,indicatore KPI, Nome collegamento, Azione_automatica	Scalabilità orizzontale del tunnel GRE
GRE_KPIB_SCALEDOWN	Host,indicatore KPI, Nome	

	collegamento, Azione_automatica	

La regola del gruppo di correlazione è progettata per facilitare l'aggregazione dei segnali relativi ai dispositivi A, B e ai rispettivi tunnel A, B e C in un incidente unificato. Questa regola di correlazione garantisce che per ogni accoppiamento specifico del dispositivo A e del dispositivo B vengano generati al massimo due incidenti distinti: un incidente per una scalabilità del tunnel GRE che interessa il dispositivo A e il dispositivo B e un altro incidente per una scalabilità del tunnel GRE che interessa lo stesso accoppiamento di dispositivo. Il framework dell'agente VIA AIOps è in grado di interfacciarsi con Business Process Automation (BPA) e Network Services Orchestrator (NSO).



Correlazione e notifica degli eventi KPI tramite VIA AIOps

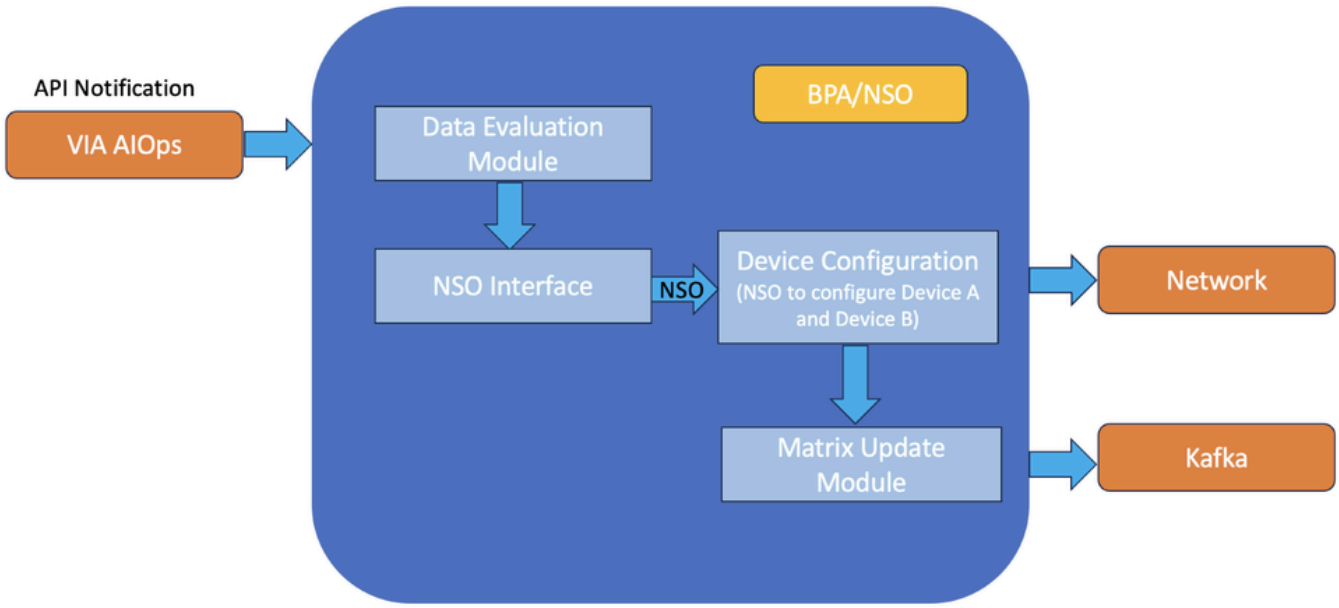
Di seguito è riportato un esempio di notifica API di scalabilità del tunnel GRE inviata a BPA/NSO da VIA AIOps.

```
{
  "create": [
    {
      "gre-tunnels-device-cla": [
        {
          "index": "RouterA-RouterB",
          "tunnelOperation": "SCALE UP",
```

```
          "MatrixData": [
            { "node": "RouterA", "kpi": "tunnel_utilization_agg" },
            { "node": "RouterB", "kpi": "tunnel_utilization_agg" }
          ]
        }
      ]
    }
  ]
}
```

Aggiungi o rimuovi tunnel e cancella avviso

Dopo aver ricevuto una chiamata API da VIA AIOps, Cisco Business Process Automation (BPA) avvia le direttive di scalabilità necessarie, tramite richieste interne indirizzate a Cisco Network Service Orchestrator (NSO). Il BPA valuta il payload dei dati fornito da VIA AIOps, che include i dettagli relativi al funzionamento del tunnel, un indice e i dati della matrice. L'indice e le informazioni sul funzionamento del tunnel vengono utilizzati per interfacciarsi con l'NSO, fornendo parametri per il funzionamento della scalatura. Contemporaneamente, i dati della matrice vengono elaborati dal "Matrix Update Module", che è responsabile della risoluzione di eventuali eventi di anomalie KPI mediante l'interfaccia con le API della matrice.

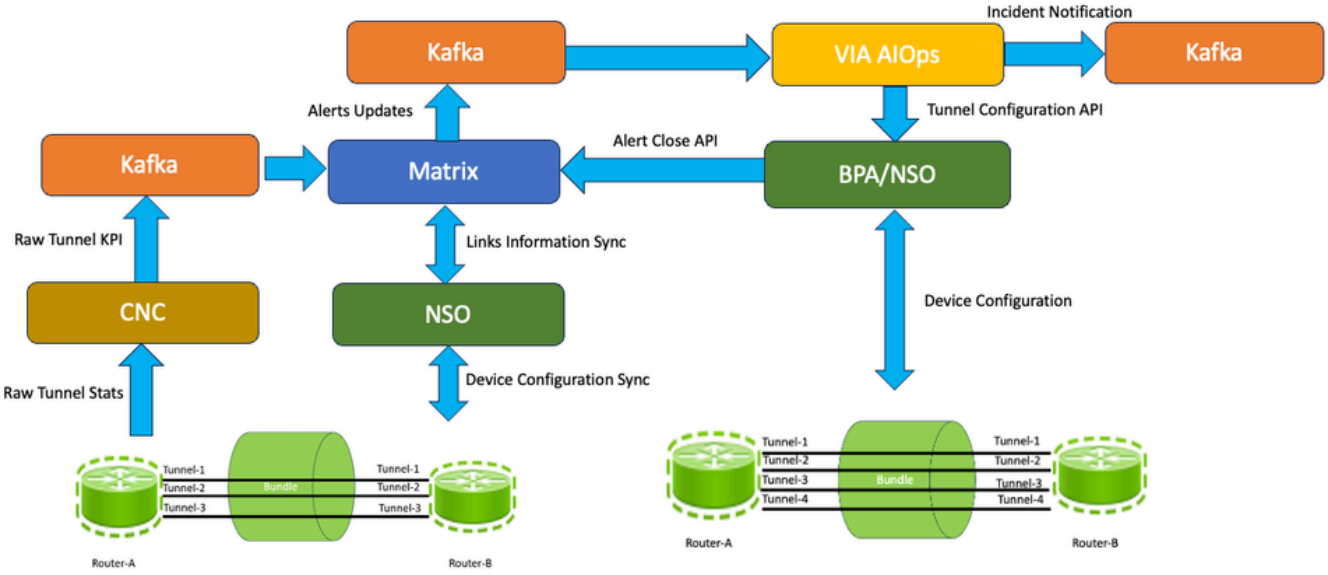


Convalida dei dati e configurazione dei dispositivi tramite BPA-NSO

Prima di iniziare qualsiasi operazione di scalatura, è necessario sviluppare un modello di azione

YANG per l'NSO. Questo modello definisce le azioni specifiche che l'NSO deve eseguire per aumentare o ridurre il numero di tunnel tra il router A e il router B. Il sistema Business Process Automation (BPA) inizia a scalare le operazioni avviando un'interazione con Network Service Orchestrator (NSO) per condurre una "prova". Questa è la fase iniziale dell'operazione in cui BPA chiede all'NSO di simulare le modifiche di configurazione previste senza applicarle. Il funzionamento a secco è una fase di convalida essenziale, che garantisce che le azioni di scalatura proposte, definite dal modello di azione YANG, possano essere eseguite senza causare errori o conflitti nella configurazione di rete.

Se l'esecuzione di prova viene considerata riuscita, a indicare che le azioni di ridimensionamento sono state convalidate, BPA passa quindi alla fase 'commit'. A questo punto, il BPA indica all'NSO di implementare le modifiche effettive alla configurazione necessarie per aumentare o ridurre il numero di tunnel GRE tra il router A e il router B. Il BPA attiva il 'Matrix Update Module' verso Matrix utilizzando una chiamata API per chiudere l'evento KPI in tandem con VIA AIOps. Una volta chiusa l'anomalia su Matrix, Matrix invia anche un avviso con gravità pari a "Cancellato" a VIA AIOps, che chiude ulteriormente l'incidente. In questo modo, il ciclo di monitoraggio e aggiornamento a livello di rete è completato. In questa immagine viene illustrata una versione generalizzata del flusso di dati all'interno dell'applicazione, utilizzata in questa automazione a loop chiuso.



Flusso di dati per l'automazione di un bundle del tunnel GRE a loop chiuso

Chiusura del loop per aprire nuove possibilità di risoluzione automatica

La soluzione discussa in questo documento è deliberatamente discussa con un esempio di scalabilità del pacchetto GRE basata su anomalie di rete per consentire la connessione con diversi elementi di base di questa soluzione. Viene esaminato in sintesi come Cisco Technology Stack, che include Cisco NSO, Cisco Matrix e Cisco BPA, può integrarsi perfettamente con componenti quali VIA AIOps, Kafka e un altro stack software per consentire il monitoraggio e la risoluzione automatica dei problemi di rete. Questa soluzione offre possibilità per tutti gli altri casi

di utilizzo della rete, che possono essere problemi tipici che si verificano nelle reti dei provider di servizi o aziendali.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).