Automatice el caso práctico de Bandwidth on Demand mediante la pila de software de automatización de bucle cerrado

Contenido

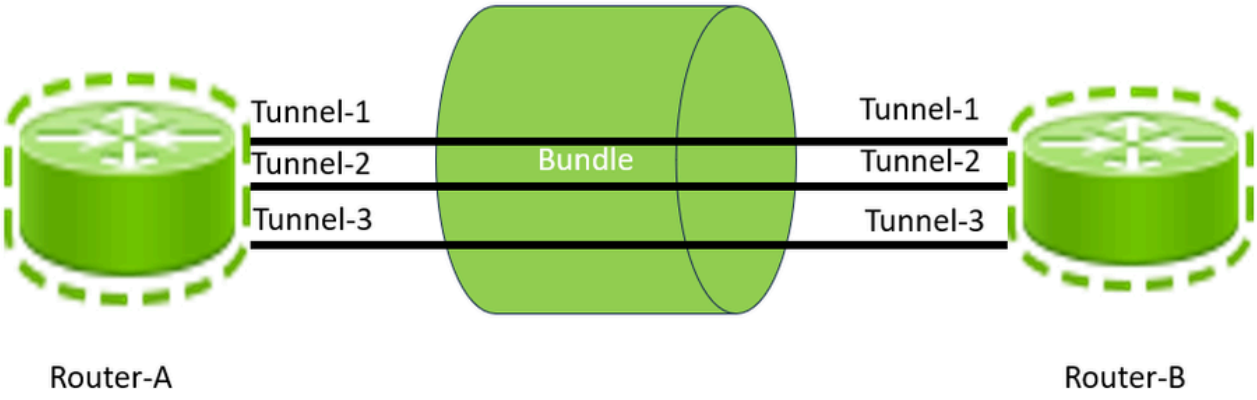
Introducción

Este documento describe los componentes de una solución de automatización de bucle cerrado de Cisco para la automatización de la ampliación de túneles de Generic Routing Encapsulation (GRE) y su adaptabilidad para otros casos.

Antecedentes

Los proveedores de servicios desean tomar el control de la utilización de su ancho de banda a través de los túneles GRE de su red y supervisarlos estrechamente para ampliar los túneles según sea necesario mediante una solución inteligente de automatización de bucle cerrado.

GRE es un protocolo de tunelización que proporciona un enfoque genérico simple para transportar paquetes de un protocolo sobre otro mediante encapsulación. Este documento se centra en el ejemplo basado en el túnel GRE para la plataforma Cisco IOS® XRv, pero también se puede generalizar a otras plataformas. GRE encapsula una carga útil, un paquete interno que debe entregarse a una red de destino dentro de un paquete IP externo. El túnel GRE se comporta como un link punto a punto virtual con dos puntos finales identificados por la dirección de origen y destino del túnel.



Túneles GRE entre routers

La configuración de un túnel GRE implica la creación de una interfaz de túnel y la definición del origen y el destino del túnel. Esta imagen muestra la configuración de tres túneles GRE entre el router A y el router B. Para esta configuración, se deben crear tres interfaces, cada una en el Router-A, como el Túnel-1, el Túnel-2 y el Túnel-3, y de manera similar crear tres interfaces en el Router-B, como el Túnel-1, el Túnel-2 y el Túnel-3. Entre dos routers de proveedores de servicios, puede haber varios túneles GRE. Cada túnel, al igual que cualquier otra interfaz de red, tiene una capacidad definida que se basa en la capacidad de la interfaz. Por lo tanto, un túnel sólo puede transportar un tráfico máximo igual a su ancho de banda. El número de túneles suele basarse en la predicción inicial de la carga de tráfico y la utilización del ancho de banda entre dos sitios (routers). Con los cambios en la red y la expansión de la red, se espera que esta utilización del ancho de banda cambie. Para hacer un uso óptimo del ancho de banda de la red, es importante agregar nuevos túneles o eliminar túneles adicionales entre dos dispositivos en función de la utilización del ancho de banda medida en todos los túneles entre los dos dispositivos.

En este ejemplo, puede decir que la capacidad total de los tres túneles entre el Router-A y el Router-B es la suma de las capacidades del Túnel-1, Túnel-2 y Túnel-3, que se denomina ancho de banda agregado o ancho de banda de nivel de agrupamiento GRE. Tenga en cuenta que la palabra clave 'bundle' aquí se refiere a los túneles entre un par de routers; no se pretende ninguna relación implícita con el agrupamiento de enlaces LACP/Etherchannel. Además, el tráfico real entre los dos routers es el tráfico agregado total a través del Túnel-1, Túnel-2 y Túnel-3. Normalmente, puede concebir un concepto de utilización del ancho de banda a nivel de conjunto, que puede ser una relación entre el tráfico total a través de los túneles y la capacidad total de todos los túneles entre dos routers. Por lo general, cualquier proveedor de servicios desea tomar medidas correctivas agregando o quitando túneles entre dos routers si observa que el ancho de banda se está sobreutilizando o infrautilizando. Sin embargo, para este documento, tenga en cuenta que el umbral inferior es del 20% para una utilización baja y del 80% para una utilización alta para la utilización de nivel de agrupamiento entre dos routers.

Requirements

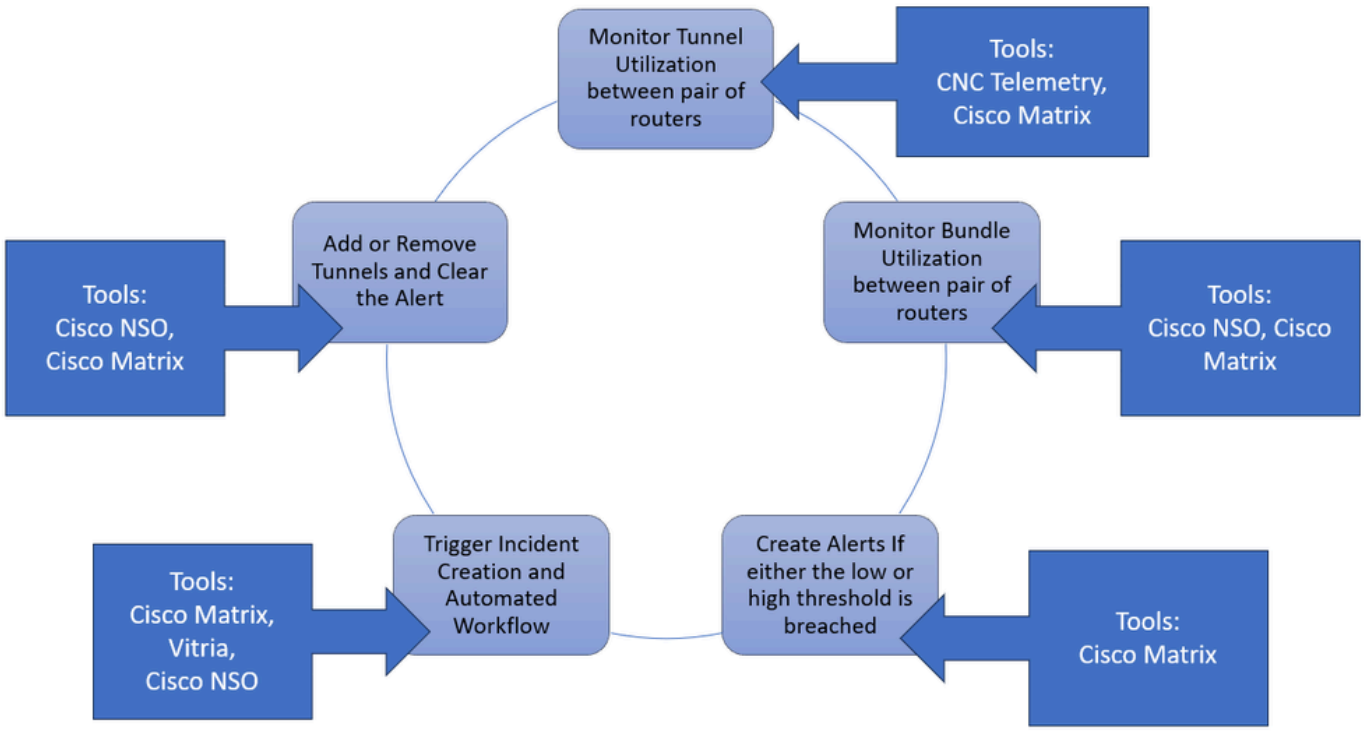
1. La solución de bucle cerrado es necesaria para llevar a cabo la automatización de bucle cerrado de extremo a extremo del paquete GRE en el XRv9K, donde el sistema puede recopilar datos de telemetría, supervisar los datos en forma de indicadores de rendimiento clave (KPI), aplicar agregación, crear alertas cruzadas de umbral (TCA) y realizar una configuración de remediación automatizada, así como cerrar la alerta.
2. La solución puede calcular un indicador clave de rendimiento (KPI) de red para proporcionar la utilización del ancho de banda de entrada de túnel (Rx) y salida de túnel (Tx) individual de cada túnel, que se basa en el rendimiento bruto de los túneles a la frecuencia deseada.
3. La solución puede calcular KPI personalizados para proporcionar el uso del ancho de banda de entrada de túnel (Rx) y salida de túnel (Tx) de cada paquete, que es el uso de ancho de banda agregado de todos los túneles entre un par de routers.
4. La solución puede detectar y crear alertas si se superan los umbrales de nivel de paquete definidos. Dichas alertas están disponibles para su supervisión.
5. La alerta debe dar lugar a la activación de un flujo de trabajo automatizado que pueda activar aún más la configuración en el dispositivo para añadir o eliminar túneles en función de las condiciones de la alerta.
6. Por último, el sistema debe cerrar automáticamente las alertas con las actualizaciones necesarias.

Solución

La solución de automatización de bucle cerrado incluye varias herramientas que trabajan en el objetivo específico de toda esta solución integral. Esta imagen muestra qué componentes y herramientas nos ayudan a lograr la arquitectura final y describe el papel de alto nivel. Puede ver cada componente y su uso en las secciones siguientes.

Solución

Cisco Closed Loop Automation



Solución Cisco Closed Loop Automation

Herramienta	Propósito
Controlador de red Cisco Crosswork (CNC)	Crosswork Network Controller ofrece visibilidad en tiempo real del ciclo de vida de los dispositivos y servicios, con navegación intuitiva por la topología de la red, el inventario de servicios, las políticas de transporte, el estado de los servicios, el estado de los dispositivos, etc., lo que permite una amplia gama de casos prácticos con una experiencia de usuario común e integrada. En esta solución, se utiliza principalmente como herramienta para la administración de dispositivos y la recopilación de datos de rendimiento de túnel mediante gNMI (gRPC Network Management Interface) o MDT. Más detalles: https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-controller/index.html
Matriz de Cisco	Los servicios de análisis de CX (paquetes de funciones) se ofrecen mediante la solución Matrix, que es una solución de análisis de múltiples dominios y panel de acceso único de varios proveedores. En esta solución, la matriz consume los datos de Kafka enviados por CNC sobre los temas de Kafka y además realiza la agregación de KPI basado en túneles en el KPI de nivel de paquete usando búsquedas de topología y almacenarlo como datos de serie de tiempo y almacenarlo en la base de datos Postgres. Una vez almacenados,

	estos datos están disponibles para su visualización y Matrix detecta anomalías mediante alertas de traspaso de umbrales, lo que nos permite configurar umbrales para los KPI que recopilamos de la red.
Clúster Kafka	Un cluster Kafka es un sistema que comprende diferentes temas de corredores, y sus respectivas particiones. Un productor envía o escribe datos o mensajes en el tema del clúster. Un consumidor lee o consume mensajes del clúster de Kafka. En esta solución, CNC actúa como el productor que envía datos a temas predefinidos de Kafka en forma de carga útil JSON después de convertir los datos de telemetría recopilados de los routers. En esta solución, Matrix actúa como el Consumidor que consume estos datos, procesa los datos, los agrega y los almacena para su posterior procesamiento y detección de anomalías.
Cisco NSO	Cisco Crosswork Network Services Orchestrator (NSO) NSO forma parte de la cartera Crosswork de herramientas de automatización diseñadas para proveedores de servicios y grandes empresas. En esta solución, NSO recopila información relacionada con todos los túneles y dispositivos y crea una tabla de topología personalizada para esta solución. Además, en esta solución, NSO, junto con las funciones de automatización de procesos empresariales, se utiliza para activar un flujo de trabajo de remediación y realizar acciones como añadir o eliminar un túnel del dispositivo y borrar más alertas en la matriz de Cisco. Más detalles: https://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html
Vitria VIA AIOps	Vitria VIA AIOps para Cisco Network Automation ofrece análisis automatizados que permiten una rápida remediación de los eventos que afectan al servicio en todas las capas de tecnología y aplicaciones. En esta solución, se utiliza VIA AIOps para correlacionar los eventos de umbral de KPI generados a partir de Cisco Matrix, crear un incidente, una notificación y desencadenar una acción automatizada hacia Cisco NSO para aumentar o disminuir el recuento de túneles GRE. Más detalles: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/solution-overview-c22-2403404.html

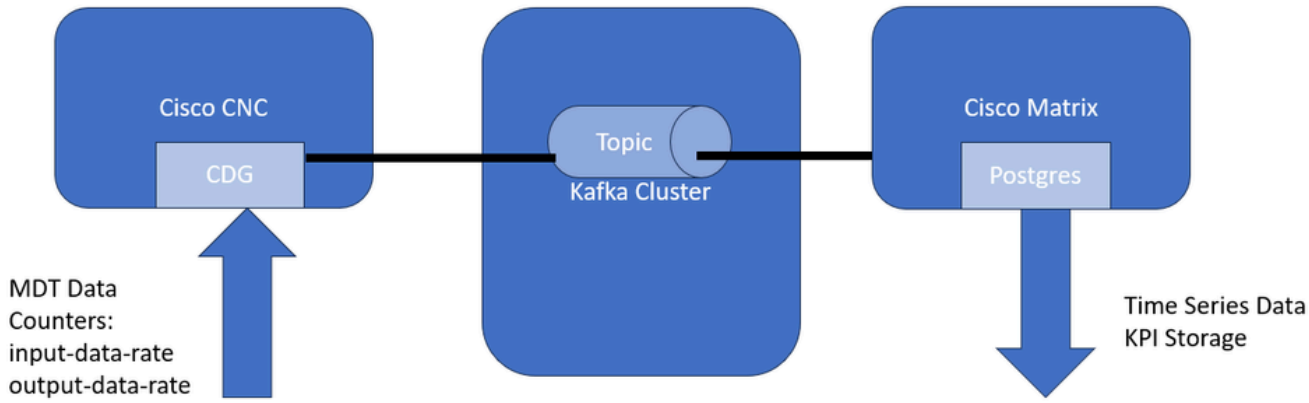
La solución realiza estos pasos para cumplir este caso práctico, que se explican en las secciones

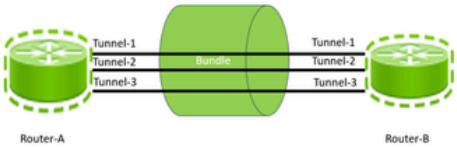
siguientes.

1. Supervisión de la utilización del túnel entre pares de routers
2. Supervisión de la utilización del paquete entre pares de routers
3. Crear alertas de traspaso de umbrales
4. Flujo de trabajo de resolución automatizada e incidentes clave
5. Agregar o quitar túneles y borrar alerta

Supervisión de la utilización de túneles entre pares de routers

Las aplicaciones solicitan la recopilación de datos mediante trabajos de recopilación. A continuación, Cisco Crosswork asigna estos trabajos de recopilación a un Cisco Crosswork Data Gateway para atender la solicitud. Crosswork Data Gateway admite la recopilación de datos de dispositivos de red mediante telemetría basada en modelos (MDT) para consumir flujos de telemetría directamente desde dispositivos (solo para plataformas basadas en Cisco IOS XR). Cisco Crosswork le permite crear destinos de datos externos que pueden ser utilizados por los trabajos de recolección para depositar datos.Kafka se puede agregar como nuevos destinos de datos para los trabajos de recolección creados por API REST. En esta solución, CDG recopila datos de los routers relacionados con las estadísticas de la interfaz de túnel y envía los datos al tema Kafta.Cisco Matrix consume los datos del tema Kafka y asigna los datos a la aplicación de trabajo Matrix que procesa los datos como KPI y los guarda en una serie de tiempo como se muestra en la siguiente figura que representa el flujo de proceso.





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

Solución Cisco Closed Loop Automation

Los datos de la serie de tiempo tienen atributos KPI que se almacenan en la base de datos de matrices.

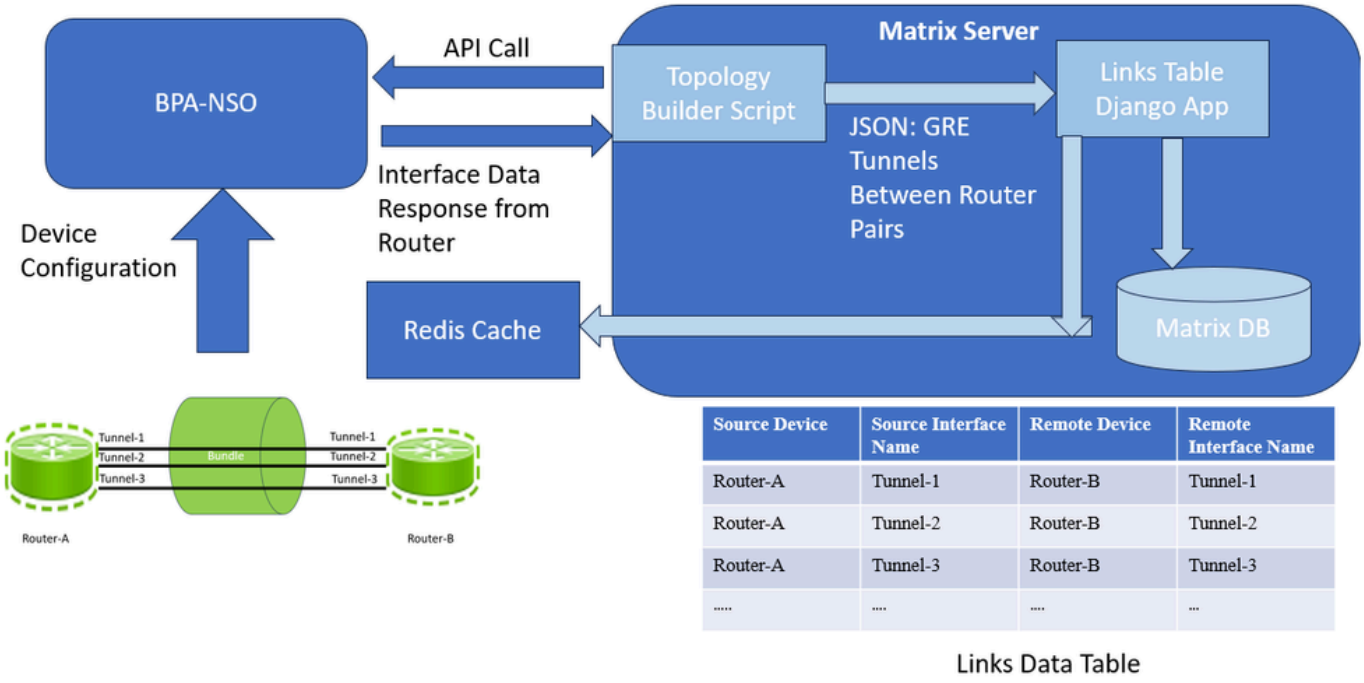
Atributos KPI	Propósito
Nodo	El dispositivo o el origen para el que se almacena KPI Ejemplo: Router-A
Hora	El momento en el que se recopilan los datos Ejemplo: 22-05-2024 10:00:00
Índice	Identificador único Ejemplo: túnel-1
Valor	Valor de KPI - Valor numérico
KPI	Nombre de KPI Ejemplo: uso de túnel

Supervisión de la utilización del paquete entre pares de routers

Una vez que tenga los datos de la serie de tiempo como se mencionó en la sección anterior, tendrá las estadísticas de tráfico recopiladas por interfaz de túnel. Sin embargo, debe identificar qué dispositivo con qué interfaz de túnel de origen está conectado a qué otro dispositivo y cuál es el nombre de la interfaz remota. Esto se denomina Identificación de link donde se identifica el nombre del dispositivo de origen. Nombre de interfaz de origen, Nombre de dispositivo remoto y Nombre de interfaz remota. Para interpretar con precisión la información de enlace y los routers, necesita un ejemplo de referencia como se describe.

Dispositivo de origen	Nombre de interfaz de origen	Dispositivo remoto	Nombre de interfaz remota
Router-A	Túnel-1	Router B	Túnel-1
Router-A	Túnel-2	Router B	Túnel-2
Router-A	Túnel-3	Router B	Túnel-3
....	...	...	..

Para generar esta tabla de vínculos de topología en esta solución, puede rellenar una tabla personalizada, Tabla de datos de vínculos, integrada en Matrix, basada en un script que se ejecuta en el servidor todos los días a la hora preferida. Este script realiza una llamada API a BPA-NSO y obtiene una salida JSON de paquetes GRE entre pares de routers. Luego analiza los datos de la interfaz para construir la topología en formato JSON. El script también toma esta salida JSON y la escribe en la Tabla de datos de links todos los días. Siempre que carga los nuevos datos en la tabla, también escribe estos datos en una memoria caché de Redis para reducir más búsquedas en la base de datos y mejorar la eficacia.



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

Proceso de tabla de datos de vínculos

Por lo tanto, necesariamente todos los enlaces entre los mismos dos dispositivos son parte del paquete que se identifica como perteneciente al mismo paquete.Una vez que los KPIs de nivel de túnel sin procesar están disponibles, entonces ha creado una aplicación KPI_aggregate personalizada en Matrix que realiza el trabajo de calcular las utilizaciones de nivel de paquete y almacenarlas como KPI.

Esta aplicación toma estas entradas:

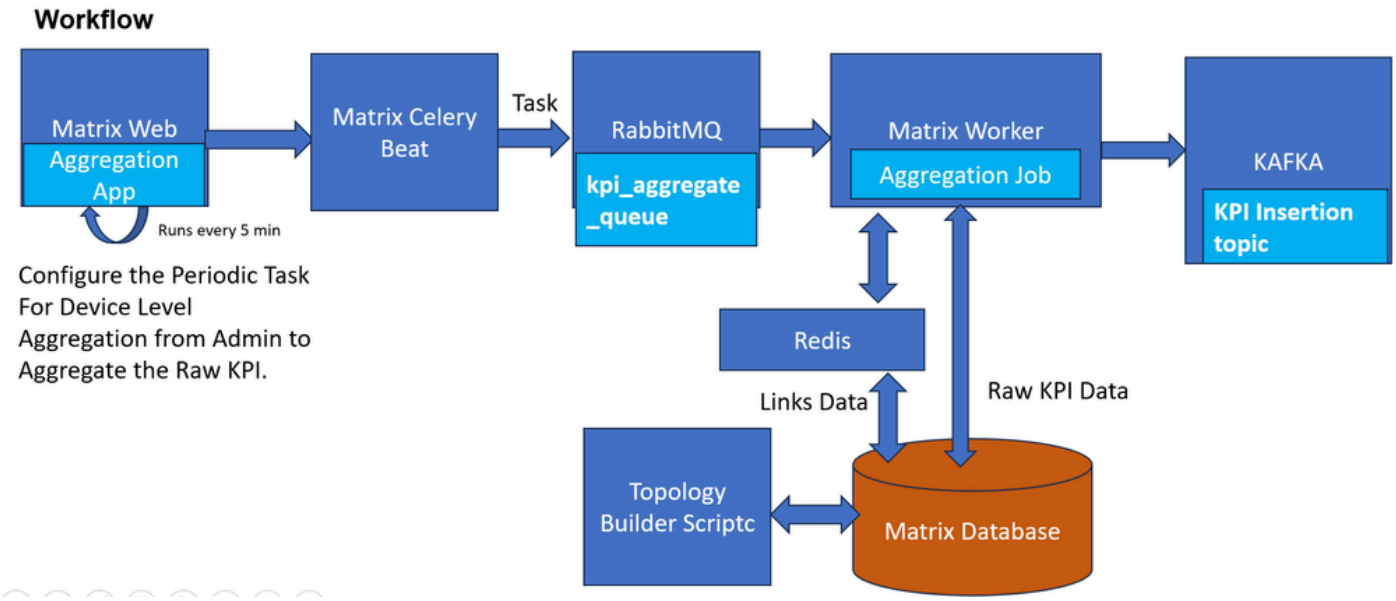
Atributo de configuración	Propósito
Crontab	Frecuencia con la que debe ejecutarse la tarea periódica de agregación
Casilla de verificación	Activar/desactivar esta configuración

Habilitado	
Nombre de KPI de interfaz de túnel	Nombre del KPI sin formato que se utiliza para calcular el KPI agregado. El nombre de KPI agregado se crea automáticamente como <Raw_KPI_Name>_agg
Intervalo de fechas	Frecuencia de los datos sin procesar.

La tarea Agregado toma las entradas de la base de datos de datos sin procesar y de vínculos de KPI, identifica los túneles que forman parte del mismo conjunto y los agrega a un grupo basado en esta lógica.

```
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
```

Por ejemplo, en este caso, el nombre de KPI se genera como "tunnel-utilization_agg" para la utilización de túneles de KPI de túnel sin procesar. Una vez completado el cálculo de todos los valores KPI sin procesar para todas las combinaciones de routers y túneles, estos datos se envían para cada vínculo al tema Kafka, que debe ser el mismo tema que ingiere el KPI procesado. De esta manera, esta información se conserva como cualquier otro KPI normal recibido de orígenes válidos. El consumidor de la base de datos consume de este tema y conserva el KPI en la tabla de resultados de KPI de la base de datos de matrices para los KPI agregados.



Proceso de agregación de KPI para KPI de agregación de nivel de paquete

Crear alertas de traspaso de umbrales

El umbral de KPI configurado en Matriz es del 85%, lo que significa que cuando el valor de este KPI supera el umbral, se genera una alerta crítica y, cuando disminuye por debajo del umbral, se genera una alerta clara. Estas alertas se guardan en la base de datos Matrix y también se reenvían a Vitria en esta solución para el caso práctico de automatización de bucle cerrado. Si el valor calculado del KPI cruza el umbral, se envía una alerta a Vitria (VIA-AIOP) a través de Kafka con el estado actual como Crítico en el mensaje. Del mismo modo, si el valor regresa dentro de los valores de umbral de los valores críticos, debe enviar una alerta a los VIA-AIOPs a través de Kafka con el estado actual como Clear en el mensaje. Se envió un mensaje de ejemplo al sistema y sus atributos son los siguientes.

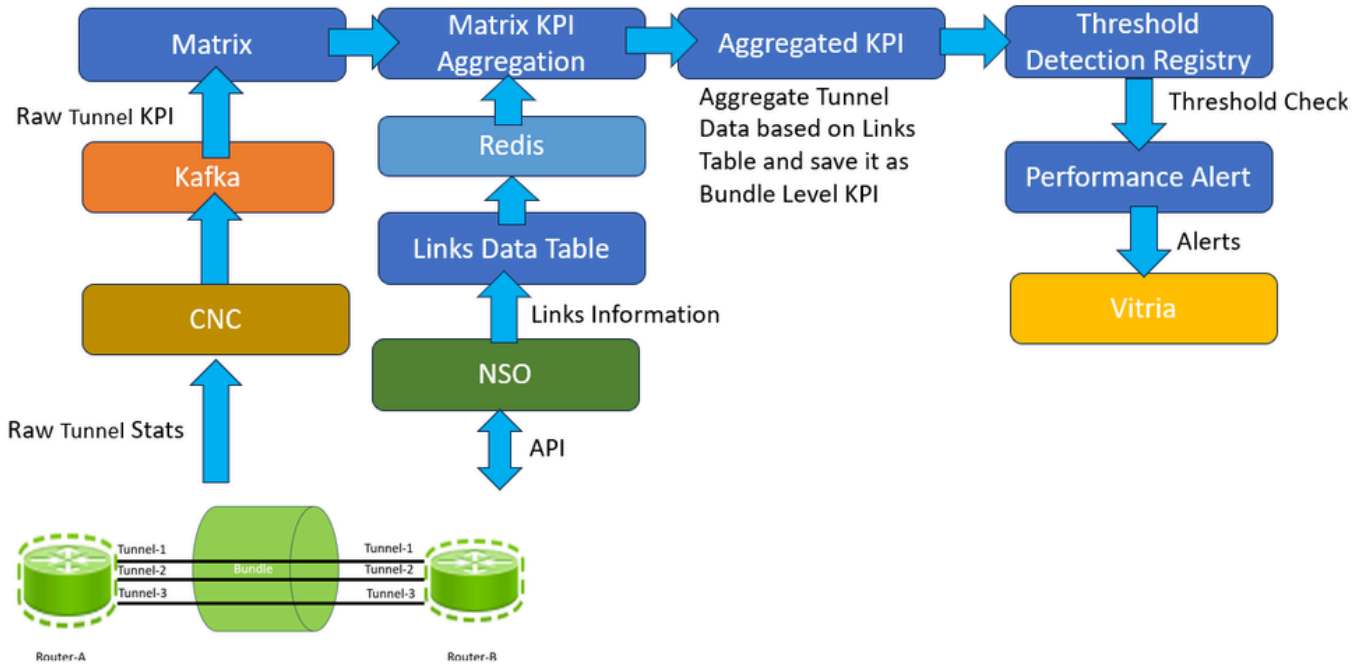

```
{
   "node": "Router-A",
   "node_type": "Router",
   "kpi": "tunnel_utilization_agg",
   "kpi_description": "Utilización del nivel de paquete",
   "schema": "",
   "index": "Router-A_Router-B",
   "hora": "2023-08-09 05:45:00+00:00",
   "value": "86.0",
   "previous_state": "CLEAR",
```

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


Atributo de mensaje de alerta Kafka	Valor de ejemplo	Propósito
nodo	Router-A	Nombre de dispositivo de red
node_type	Router	tipo de dispositivo
KPI	tunnel_utilization_agg	Nombre de KPI
kpi_description	Utilización de nivel de paquete	Descripción de KPI
Esquema	NA	NA
índice	Router-A_Router-B	<local_device>-<remote_device>
hora	"2023-08-09 05:45:00+00:00"	hora
valor	86.0	valor KPI
estado_anterior	CLEAR	Estado de alerta anterior
current_state	CRÍTICO	Estado actual de alerta
link_name	Router-A_Router-B	Atributo de correlación

el atributo link_name es un nombre ordenado alfabéticamente de los dispositivos presentes en el valor del índice. Esto se hace para lograr la correlación en el nivel de AIOP VIA, donde los AIO VIA deben correlacionar las alertas que provienen del mismo enlace del paquete. Por ejemplo, cuando llegan varias alertas a través de AIOP con el mismo link_name significa que las alertas pertenecen al mismo link de conjunto en la red indicado por los nombres de dispositivo en el

nombre del link.



Generación de alertas de agregación de KPI mediante el Registro de detección de matrices

Flujo de trabajo de resolución automatizada e incidentes clave

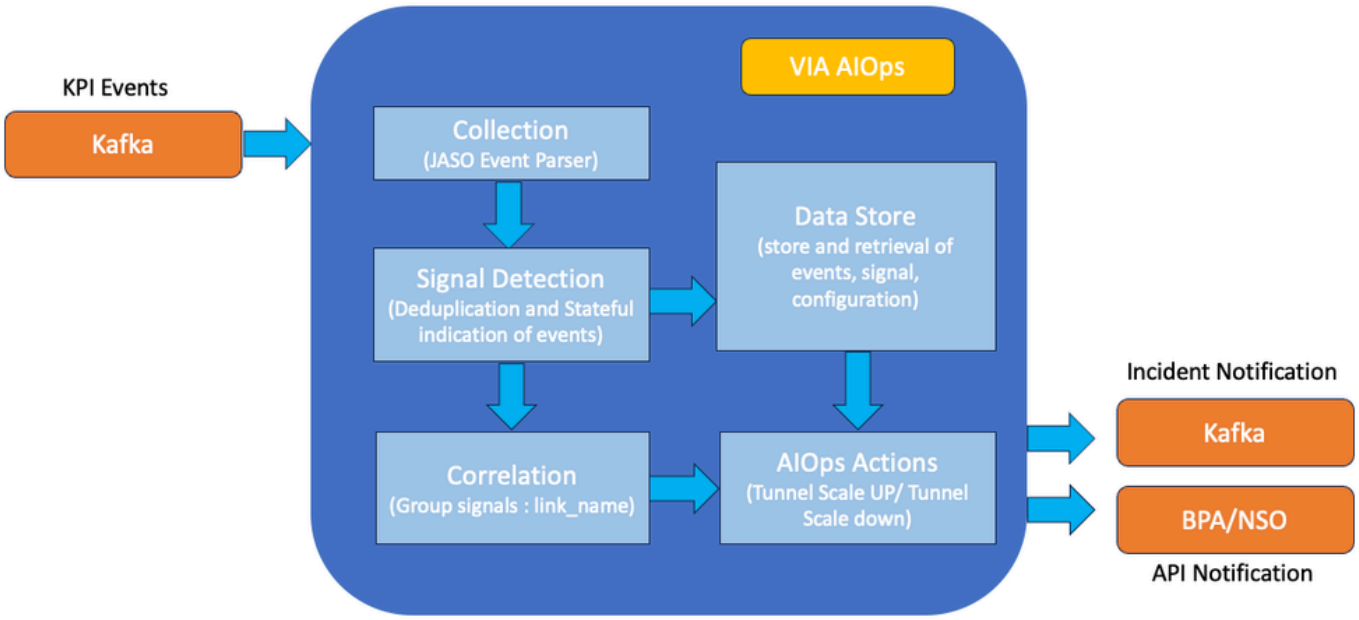
VIA AIOps debe configurarse para la ingestión de eventos de anomalía del indicador clave de rendimiento (KPI) de un tema Kafka designado. Estos eventos, tal como se reciben a través de mensajes Kafka, son procesados por AIOps VIA a través del analizador de eventos JASO para su posterior ingestión. Es fundamental que los AIO de VIA identifiquen con precisión los eventos de anomalía de KPI relacionados con los túneles GRE, determinen su asociación con pares de dispositivos específicos (por ejemplo, router A - router B) y comprueben si la anomalía requiere el inicio de la automatización de la ampliación del túnel GRE, ya sea una ampliación a un nivel superior o inferior.

El analizador de eventos JASO de VIA AIOps debe configurarse para extraer e interpretar las dimensiones relevantes del evento de anomalía de KPI de matriz, es decir, el "host", "kpi", "índice" y "valor". Se debe configurar una dimensión adicional, denominada "automation_action", para que el analizador de eventos JASO la actualice dinámicamente, en función de la métrica "value" presente en el evento de anomalía de KPI de matriz. Esta dimensión es fundamental para determinar si se debe aplicar una respuesta automatizada, en concreto si se deben activar los procedimientos de "ampliación del túnel GRE" o "reducción del túnel GRE" mediante el procesamiento del campo "Valor KPI". En VIA AIOps, una señal representa una consolidación de los estados de los eventos. Para mejorar este proceso de correlación, debemos configurar señales distintas y con estado que se correlacionen con las dimensiones 'host', 'link name', 'kpi' y 'automation_action'. La tabla ejemplifica las señales, los grupos de correlación y sus respectivas configuraciones de correlación.

Por ejemplo, la señal identificada como GRE_KPIA_SCALEUP se iniciaría después de la ingestión de un mensaje de anomalía de KPI especificado, como se detalla en la sección 3, por el sistema AIOps VIA.

Nombre de la señal AIOps VIA	Teclas de correlación de señales	Nombre de regla de grupo de correlación
GRE_KPIA_SCALEUP	Host, kpi, Nombre de vínculo, Acción_automatizada	Ampliación del túnel GRE
GRE_KPIB_SCALEUP	Host, kpi, Nombre de vínculo, Acción_automatizada	
GRE_KPIA_SCALEDOWN	Host, kpi, Nombre de vínculo, Acción_automatizada	Escalabilidad descendente del túnel GRE
GRE_KPIB_SCALEDOWN	Host, kpi, Nombre de vínculo, Acción_automatizada	

La regla de grupo de correlación está diseñada para facilitar la agregación de señales sobre el Dispositivo A, el Dispositivo B y sus respectivos túneles A, B y C en un incidente unificado. Esta regla de correlación garantiza que, para cualquier emparejamiento específico de dispositivos A y B, se generen un máximo de dos incidentes distintos: un incidente para una ampliación de túnel GRE que afecta al dispositivo A y al dispositivo B, y otro incidente para una ampliación de túnel GRE para el mismo emparejamiento de dispositivos. El marco del agente VIA AIOps puede interactuar con Business Process Automation (BPA) y Network Services Orchestrator (NSO).



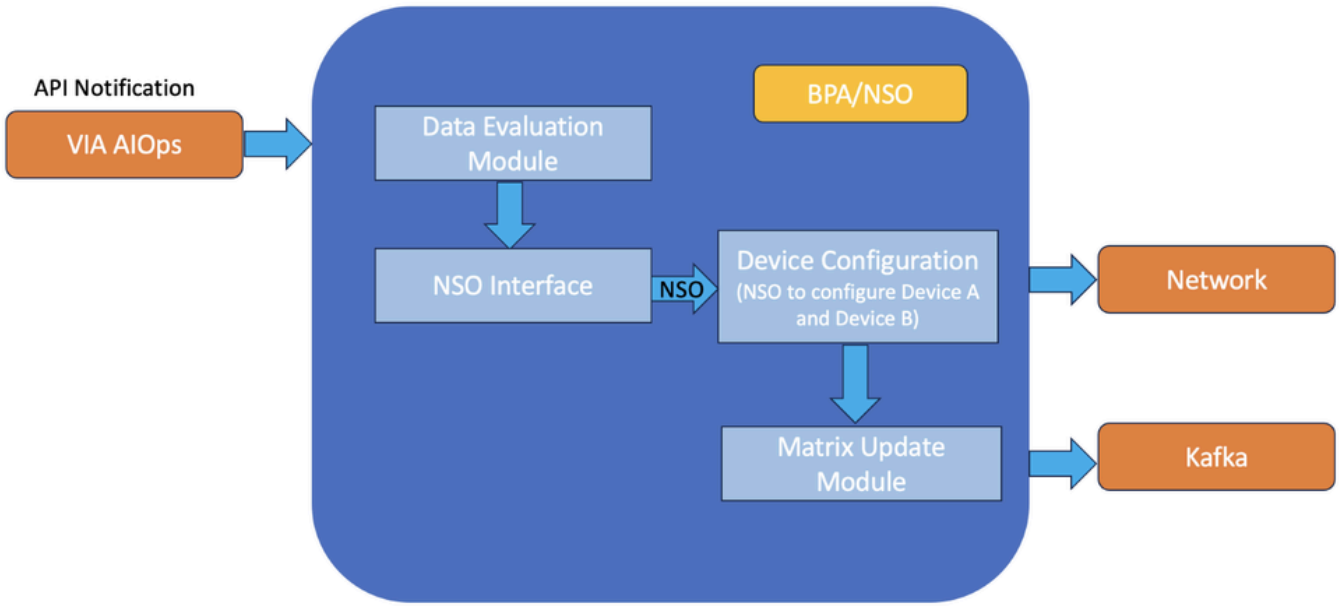
Correlación y notificación de eventos KPI mediante AIOps VIA

Este es un ejemplo de una notificación de API de ampliación de túnel GRE enviada a BPA/NSO desde AIOps VIA.

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

Agregar o quitar túneles y borrar alerta

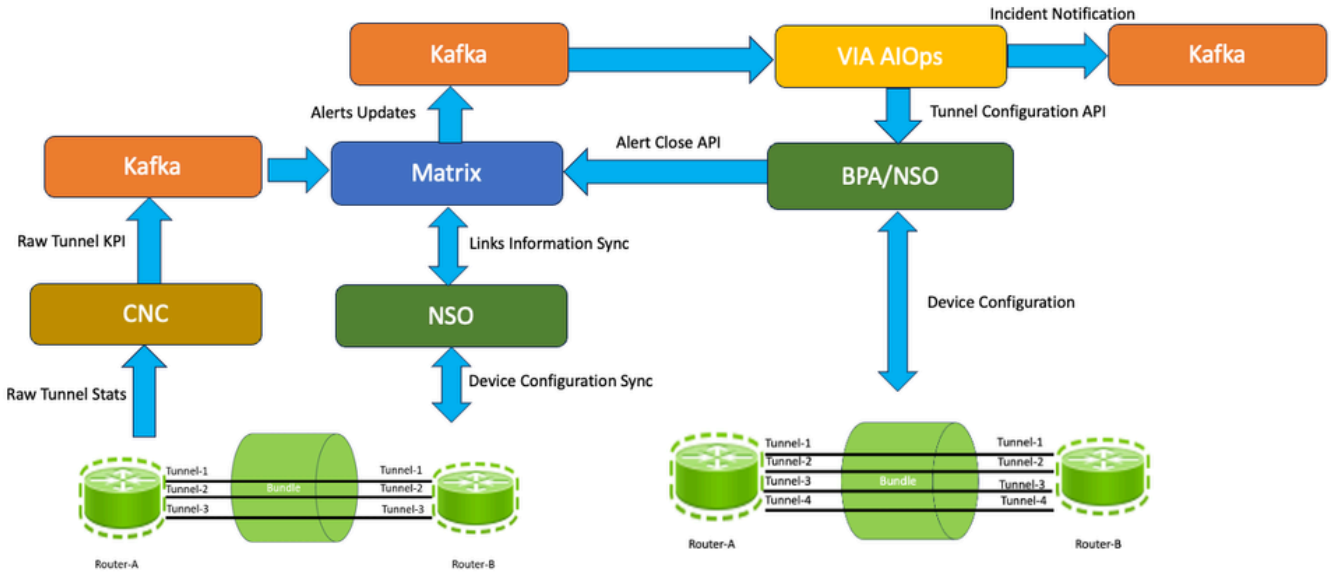
Al recibir una llamada API de VIA AIOps, Cisco Business Process Automation (BPA) inicia las directivas de ampliación necesarias mediante solicitudes internas a Cisco Network Service Orchestrator (NSO). El BPA evalúa la carga útil de datos proporcionada por los AIOps de VIA, que incluye los detalles de funcionamiento del túnel, un índice y datos de la matriz. La información de operación de túnel e índice se utiliza para interactuar con NSO, proporcionando parámetros para la operación de escalado. Simultáneamente, los datos de la matriz son procesados por el 'Módulo de actualización de la matriz', que es responsable de resolver cualquier evento de anomalía de KPI interactuando con las API de la matriz.



Validación de datos y configuración de dispositivos mediante BPA-NSO

Antes de iniciar cualquier operación de escalado, es necesario desarrollar un modelo de acción YANG para NSO. Este modelo define las acciones específicas que debe realizar NSO para aumentar o disminuir el recuento de túneles entre el router A y el router B. El sistema de automatización de procesos empresariales (BPA) comienza a escalar las operaciones colaborando con Network Service Orchestrator (NSO) para llevar a cabo un "simulacro". Esta es la fase inicial de la operación en la que el BPA solicita al NSO que simule los cambios de configuración previstos sin aplicarlos. El simulacro funciona como un paso de validación esencial, asegurando que las acciones de escalado propuestas, según lo definido por el modelo de acción YANG, se puedan ejecutar sin causar errores o conflictos en la configuración de la red.

Si la ejecución en seco se considera exitosa, lo que indica que las acciones de escalado se validan, el BPA avanza a la etapa de "confirmación". En este momento, el BPA indica al NSO que implemente las modificaciones de configuración reales necesarias para aumentar o disminuir el recuento de túneles GRE entre el router A y el router B. El BPA activa el 'Módulo de actualización de matriz' hacia Matrix mediante una llamada de API para cerrar el evento KPI junto con AIOps de VIA. Una vez que se cierra esta anomalía en Matrix, Matrix también envía una alerta con la gravedad "Borrado" a VIA AIOps, que cierra aún más el incidente en su extremo. De este modo, se completa el ciclo de remediación a nivel de red. En esta imagen se muestra una versión generalizada del flujo de datos dentro de la aplicación, utilizada en esta automatización de bucle cerrado.



Flujo de datos para la automatización de un bucle cerrado del paquete de túnel GRE

Cierre del bucle para abrir nuevas posibilidades de remediación automática

La solución descrita en este documento se analiza de forma deliberada con un ejemplo de ampliación del paquete GRE basada en anomalías de la red para ayudarnos a relacionarnos con los distintos bloques de creación de esta solución. En resumen, se estudia cómo Cisco Technology Stack, que incluye Cisco NSO, Cisco Matrix y Cisco BPA, puede integrarse sin problemas con componentes como VIA AIOps, Kafka y otra pila de software para ayudarnos a supervisar y solucionar automáticamente los problemas de red. Esta solución abre posibilidades para el resto de casos prácticos de redes, que pueden ser problemas típicos que se producen en las redes empresariales o de proveedores de servicios.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).