

透過閉環自動化軟體堆疊自動按需分配頻寬使用案例

目錄

[簡介](#)

[背景資訊](#)

[需求](#)

[解決方案](#)

[監控成對路由器之間的隧道利用率](#)

[監控成對路由器間的捆綁利用率](#)

[建立超出臨界值的警示](#)

[觸發事件和自動補救工作流程](#)

[增加或刪除隧道和清除警報](#)

[封閉環路，開啟新的自動修正可能性](#)

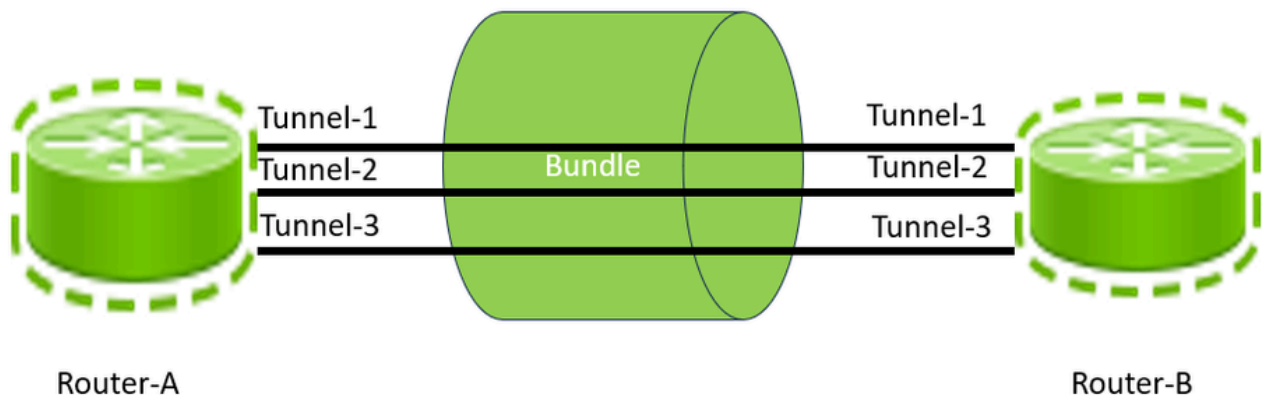
簡介

本檔案介紹適用於通用路由封裝(GRE)通道擴充自動化的思科閉環自動化解決方案中的元件，以及解決方案對其他案例的適應性。

背景資訊

服務提供商希望控制其整個網路中的GRE隧道的頻寬使用情況，並密切監控這些情況，以便使用智慧閉環自動化解決方案根據需要擴展隧道。

GRE是一種通道通訊協定，使用封裝提供一個簡易的通用方法來傳輸另一個通訊協定的封包。本檔案重點介紹適用於Cisco IOS® XRv平台的GRE通道範例，但也可以推廣到其他平台。GRE封裝有效負載，即需要在外部IP資料包中傳送到目的網路的內部資料包。GRE隧道的行為就像一個虛擬點對點鏈路，其兩個端點由隧道源和隧道目標地址標識。



路由器之間的GRE隧道

配置GRE隧道涉及建立隧道介面和定義隧道源和目標。此圖顯示路由器A和路由器B之間的三個GRE隧道的配置。對於此配置，必須在路由器A上建立三個介面，每個介面都為Tunnel-1、Tunnel-2和Tunnel-3；同樣地，必須在路由器B上建立三個介面，例如Tunnel-1、Tunnel-2和Tunnel-3。在兩個服務提供商路由器之間，可以有多個GRE隧道。每個隧道與任何其他網路介面一樣，都有基於介面容量的定義容量。因此，通道只能傳輸等於其頻寬的最大流量。隧道數量通常基於對兩個站點（路由器）之間的流量負載和頻寬利用率的初始預測。隨著網路和網路擴展的變化，預計頻寬利用率也會發生變化。要最佳化網路頻寬的使用，請務必根據在兩台裝置之間所有隧道的頻寬使用率，在兩台裝置之間增加新的隧道或移除額外的隧道。

在本範例中，您可以假設，路由器A和路由器B之間的所有三個通道總容量是通道1、通道2和通道3的容量總和，這稱為彙總頻寬或GRE套件層級頻寬。請注意，此處的「bundle」關鍵字是指一對路由器之間的隧道；沒有與LACP/Etherchannel鏈路捆綁的隱含關係。此外，兩台路由器之間的實際流量是透過Tunnel-1、Tunnel-2和Tunnel-3的總匯聚流量。通常，您可以設計一個捆綁層頻寬使用率的概念，此概念可以是隧道總流量與兩台路由器之間所有隧道總容量的比率。通常，如果發現頻寬過度使用或利用不足，任何服務提供商都希望透過在兩台路由器之間增加或刪除隧道來採取補救操作。但是，對於本文檔，兩個路由器之間的捆綁層利用率如果較低，則閾值下限為20%；如果捆綁層利用率很高，則閾值下限為80%。

需求

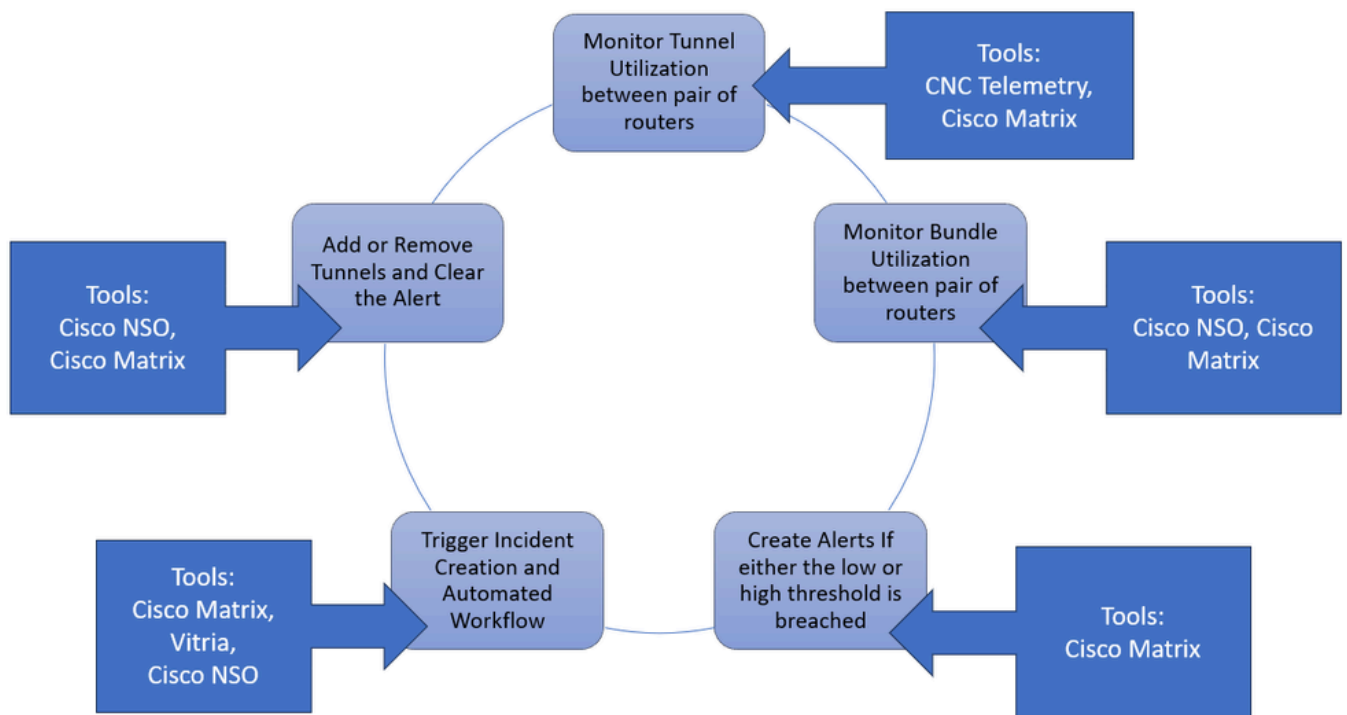
1. 需要閉環解決方案才能對XRv9K上的GRE捆綁包執行端到端閉環自動化，系統可以在其中收集遙測資料、以關鍵效能指標(KPI)的形式監視資料、應用聚合、建立閾值交叉警報(TCA)以及執行自動補救配置和關閉警報。
2. 所述方案可以計算網路關鍵效能指標(KPI)，以提供每個隧道的單獨隧道入口(Rx)和隧道出口(Tx)頻寬利用率，所述頻寬利用率基於期望頻率的隧道的原始吞吐量。
3. 此解決方案能夠計算自定義KPI，以提供每個捆綁的隧道入口(Rx)和隧道出口(Tx)頻寬利用率，這是一對路由器之間所有隧道的聚合頻寬利用率。

4. 如果超過定義的捆綁包級別閾值，該解決方案可以檢測並建立警報。此類警報可用於監控。
5. 警報必須導致觸發自動化工作流程，該工作流程可以進一步觸發裝置上的配置，以便根據警報條件增加或刪除隧道。
6. 最後，系統必須自動關閉具有所需更新的警報。

解決方案

閉環自動化解決方案涉及多個工具，這些工具致力於整個端到端解決方案中的特定目標。此影像顯示哪些元件和工具可協助我們達成最終架構，並概述高階角色。您可以檢視每個元件及其在後續部分中的使用。

思科閉環自動化



解
決方案思科閉環自動化解決方案

工具	目的
Cisco Crosswork 網路控制器 (CNC)	<p>Crosswork 網路控制器可跨網路拓撲、服務清查、傳輸原則、服務健康狀況、裝置健全狀況等提供直覺式導覽，提供跨服務與裝置生命週期的即時可視性，並提供各種使用案例，以及共同且整合的使用者體驗。</p> <p>在此解決方案中，它主要用作一種工具，用於管理裝置和使用 gNMI (gRPC 網路管理介面) 或 MDT 收集隧道效能資料。</p> <p>更多詳細資訊 : https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-controller/index.html</p>

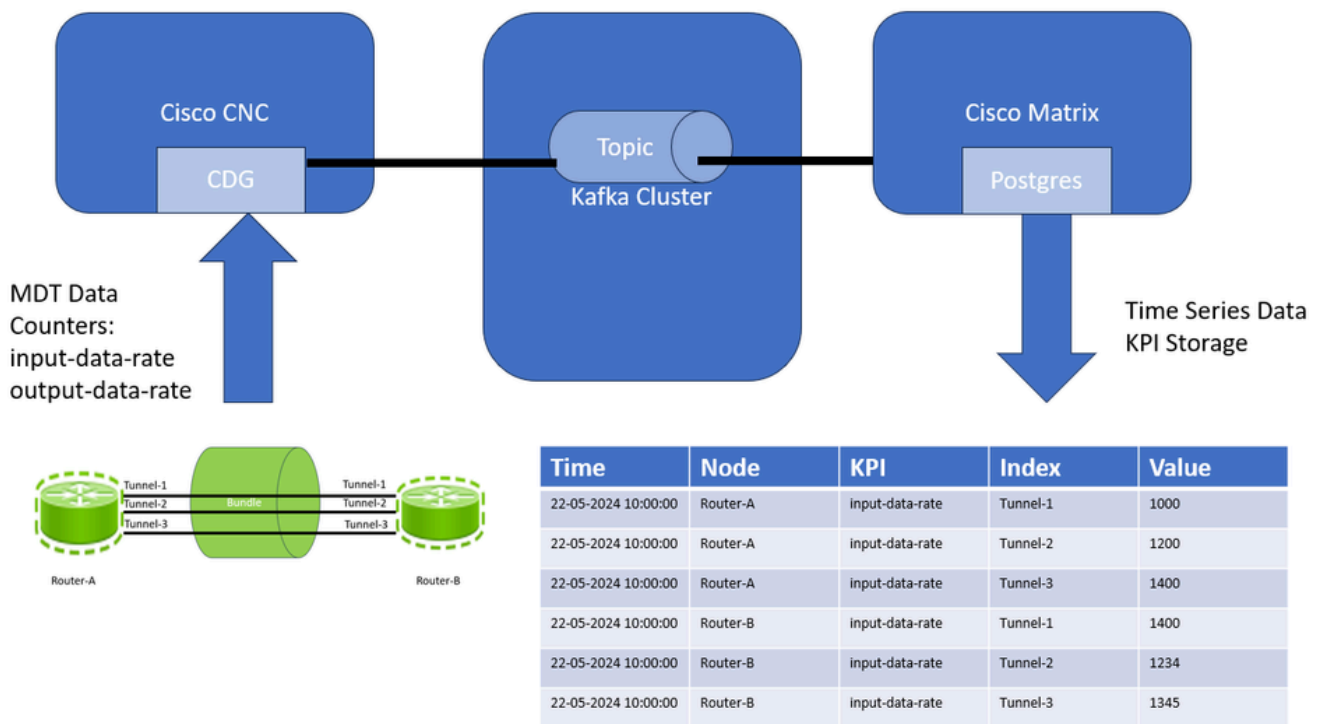
Cisco Matrix	<p>CX分析服務（功能包）使用Matrix解決方案提供，該解決方案是多供應商單一平台的多域分析解決方案。</p> <p>在此解決方案中，Matrix會使用CNC在Kafka主題上傳送的Kafka中的資料，並進一步使用拓撲查詢將基於隧道的KPI聚合到捆綁層級KPI，並將其儲存為時間序列資料並儲存在Postgres資料庫中。一旦儲存此類資料後，即可進行視覺化，Matrix使用閾值交叉警報進行異常檢測，這使我們能夠為從網路收集的KPI配置閾值。</p>
卡夫卡叢集	<p>Kafka叢集是一個包含不同經紀人主題及其各自分割槽的系統。製作者向群集內的主題傳送或寫入資料/消息。消費者讀取或使用Kafka叢集的訊息。</p> <p>在此解決方案中，CNC充當生產者，在轉換從路由器收集到的遙測資料後，以JSON負載形式將資料傳送到預定義的Kafka主題。</p> <p>在此解決方案中，Matrix充當消費者，消費者會消耗此資料，處理資料，聚合資料並將其儲存起來，以進行進一步的處理和異常檢測。</p>
Cisco NSO	<p>Cisco Crosswork網路服務協調器(NSO)</p> <p>NSO是為服務提供商和大型企業構建的自動化工具的Crosswork產品組合的一部分。</p> <p>在此解決方案中，NSO收集與所有隧道和裝置相關的資訊，並為此解決方案構建自定義拓撲表。</p> <p>此外，在此解決方案中，NSO和業務流程自動化功能用於觸發補救工作流程，並採取行動，例如增加或刪除裝置中的隧道以及進一步清除Cisco Matrix中的警報。</p> <p>更多詳細資訊：https://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html</p>
透過AIO的 Vitria	<p>Vitria VIA AIOps for Cisco Network Automation提供自動化分析，可跨所有技術和應用層快速補救影響服務的事件。</p> <p>在此解決方案中，VIA AIOp用於關聯從Cisco Matrix生成的KPI閾值事件，以建立事件、通知並觸發針對Cisco NSO的自動操作，以增加或減少GRE隧道計數。</p> <p>更多詳細資訊：https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/solution-overview-c22-2403404.html</p>

解決方案採取這些步驟來完成此使用案例，將在後續章節中詳述。

1. 監控路由器對之間的隧道利用率
2. 監控成對路由器間的捆綁利用率
3. 建立超出臨界值的警示
4. 觸發事件和自動補救工作流程
5. 增加或刪除隧道和清除警報

監控成對路由器之間的隧道利用率

應用程式透過收集作業請求資料收集。然後，Cisco Crosswork將這些收集作業分配給Cisco Crosswork資料網關以服務於請求。Crosswork資料網關支援使用模型驅動遙測(MDT)從網路裝置收集資料，以直接使用來自裝置的遙測串流（僅適用於基於Cisco IOS XR的平台）。Cisco Crosswork可讓您建立外部資料目的地，供收集工作用來存放資料。Kafka可新增為REST API建立的收集工作的新資料目的地。在此解決方案中，CDG從與隧道介面統計資訊相關的路由器收集資料，並將資料傳送到Kafka主題。Cisco Matrix使用Kafka主題中的資料，並將資料分配給Matrix工作應用程式，該應用程式將資料作為KPI進行處理，並以時間序列方式儲存資料，如隨後顯示流程流的圖中所示。



思科閉環自動化解決方案

時間序列資料具有儲存在矩陣資料庫中的KPI屬性。

KPI屬性	目的
節點	儲存重要績效指標的裝置或來源 示例：路由器A
時間	收集資料的時間 範例：22-05-2024 10:00:00
索引	唯一辨識碼

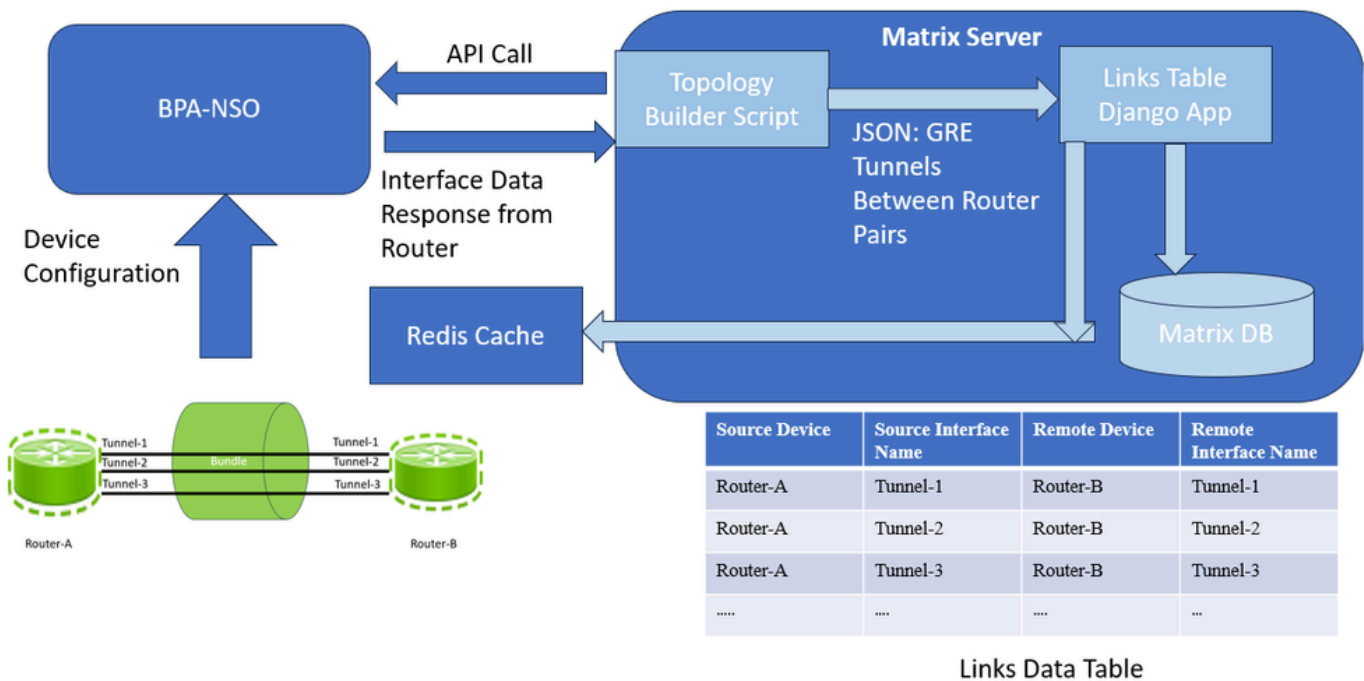
	示例：隧道1
價值	KPI值-數值
KPI	KPI名稱 示例：隧道利用率

監控成對路由器間的捆綁利用率

獲得上一節中提到的Time series資料後，您便可以收集每個隧道介面的流量統計資訊。但是，您需要確定哪個裝置與哪個源隧道介面連線，哪個裝置與哪個裝置連線，以及哪個遠端介面名稱連線。這稱為鏈路標識，您可以在其中標識源裝置名稱。源介面名稱、遠端裝置名稱和遠端介面名稱。要準確解釋鏈路資訊和路由器，您需要一個參考示例，如前所述。

源裝置	來源介面名稱	遠端裝置	遠端介面名稱
路由器A	隧道1	路由器B	隧道1
路由器A	隧道2	路由器B	隧道2
路由器A	隧道3	路由器B	隧道3
....

要在此解決方案中構建此拓撲鏈路表，您可以根據在首選時間每天在伺服器上運行的指令碼填充一個自定義表（即鏈路資料表），該表內建在矩陣中。此指令碼對BPA-NSO執行API呼叫，並返回路由器對之間的GRE捆綁的JSON輸出。然後解析介面資料以JSON格式構建拓撲。指令碼還將獲取此JSON輸出，並每天將其寫入鏈路資料表。每當將新資料載入表格時，它也會將此資料寫入Redis快取記憶體，以減少進一步的資料庫查閱並提高效率。



連結資料表程式

因此，相同兩台裝置之間的所有連結必然是標識為屬於同一捆綁的捆綁的一部分。一旦有原始隧道級別KPI，您就在Matrix上構建了一個自定義KPI_aggregate應用，該應用將執行計算捆綁級別利用率並將它們儲存為KPI的任務。

此應用程式會採用以下輸入：

配置屬性	目的
Crontab	必須執行聚總週期性工作的頻率
啟用核取方塊	啟用/停用此配置
通道介面KPI名稱	用於計算聚總KPI的原始KPI的名稱。 聚總KPI名稱會自動建立為<Raw_KPI_Name>_agg
日期範圍	原始資料的頻率。

「彙總」任務從KPI原始資料和連結資料庫獲取輸入，標識組成同一捆綁的隧道，並根據此邏輯將這些隧道增加到組中。

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

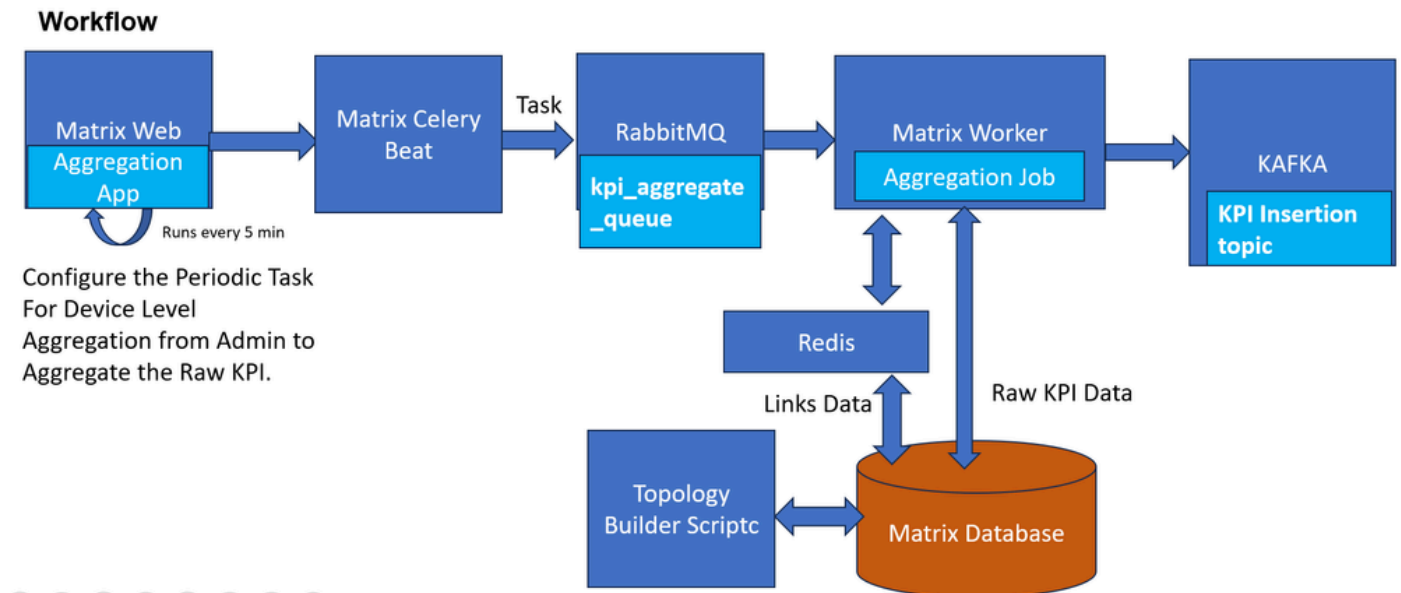
Index: <local device> _<remote device>

Router-A _Router-B

Node: <Local-Device>

Router-A

例如，在此情況下，系統會為原始隧道KPI隧道利用率生成「tunnel-utilization_agg」作為KPI名稱。完成所有路由器和通道組合的所有原始KPI值的計算後，此資料會針對每個連結推送到Kafka主題，該主題必須與接收已處理KPI的主題相同。如此一來，此資訊會像從有效來源接收的任何其他一般KPI一樣持續保留。DB Consumer會從此主題耗用並將該KPI保留到矩陣資料庫中的聚合KPI的KPI結果表中。



捆綁包層的KPI聚合流程聚合KPI

建立超出臨界值的警示

矩陣中配置的KPI閾值為85%，這意味著當此KPI的值超出閾值時，將生成嚴重警報；當該值低於閾值時，將生成清晰警報。這些警報儲存在矩陣資料庫中，並在此解決方案中轉發給Vitria，用於閉環自動化使用案例。如果KPI的計算值超過閾值，則會透過Kafka向Vitria (VIA-AIOP)傳送警報，且消息中的當前狀態為「嚴重」。同樣，如果該值從關鍵值返回閾值範圍內，則必須透過Kafka向VIA-AIOP傳送警報，且消息中的當前狀態為Clear。已將訊息範例傳送至系統，其屬性如下。

```
{
  "node": "Router-A",
  "node_type": "Router",
```



```

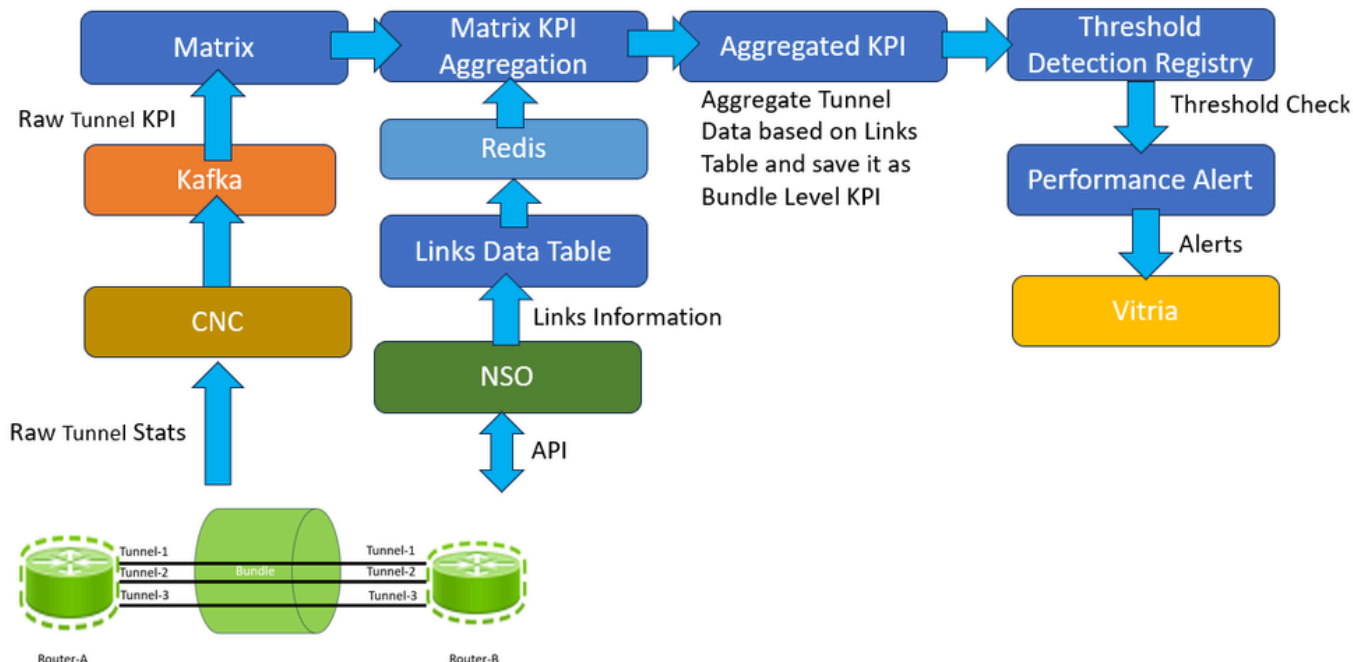
"kpi" : "tunnel_utilization_agg" ,
"kpi_description" : "捆綁包級別利用率" ,
"架構" : "" ,
"index" : "Router-A_Router-B" ,
「時間」 : 「2023-08-09 05:45:00+00:00」 ,
"值" : "86.0" ,
"previous_state" : "CLEAR" ,
"current_state" : "CRITICAL" ,
"link_name" : "Router-A_Router-B"
}

```

Kafka警示訊息屬性	範例值	目的
節點	路由器A	網路裝置名稱
node_type	路由器	裝置型別
KPI	tunnel_utilization_agg	KPI名稱
kpi_description	捆綁包級別利用率	KPI說明
結構描述	NA	NA
索引	Router-A_Router-B	<local_device>-<remote_device>
時間	「2023-08-09 05:45:00+00:00」	時間
價值	86.0	KPI值
previous_state	清除	先前的警示狀態
current_state	嚴重	目前的警示狀態

連結名稱	Router-A_Router-B	相互關聯屬性
------	-------------------	--------

link_name屬性是索引值中按字母順序排列的裝置名稱。這樣做是為了在VIA AIO級別實現關聯，VIA AIO必須關聯來自同一捆綁鏈路的警報。例如，當多個警報使用同一link_name進入VIA AIO時，這意味著這些警報屬於網路中的同一捆綁鏈路，由鏈路名稱中的裝置名稱表示。



使用矩陣檢測登錄檔生成KPI聚合警報

觸發事件和自動補救工作流程

VIA AIOp將配置為從指定的Kafka主題接收關鍵績效指標(KPI)異常事件。這些事件透過Kafka消息接收，由VIA AIOp透過JASO事件解析器進行處理，以備隨後食用。對於VIA AIO而言，關鍵是要準確辨識與GRE隧道相關的KPI異常事件，確定它們與特定裝置對（例如，路由器A -路由器B）的關聯，並確定該異常是否需要啟動GRE隧道擴展自動化（無論是升級還是降級）。

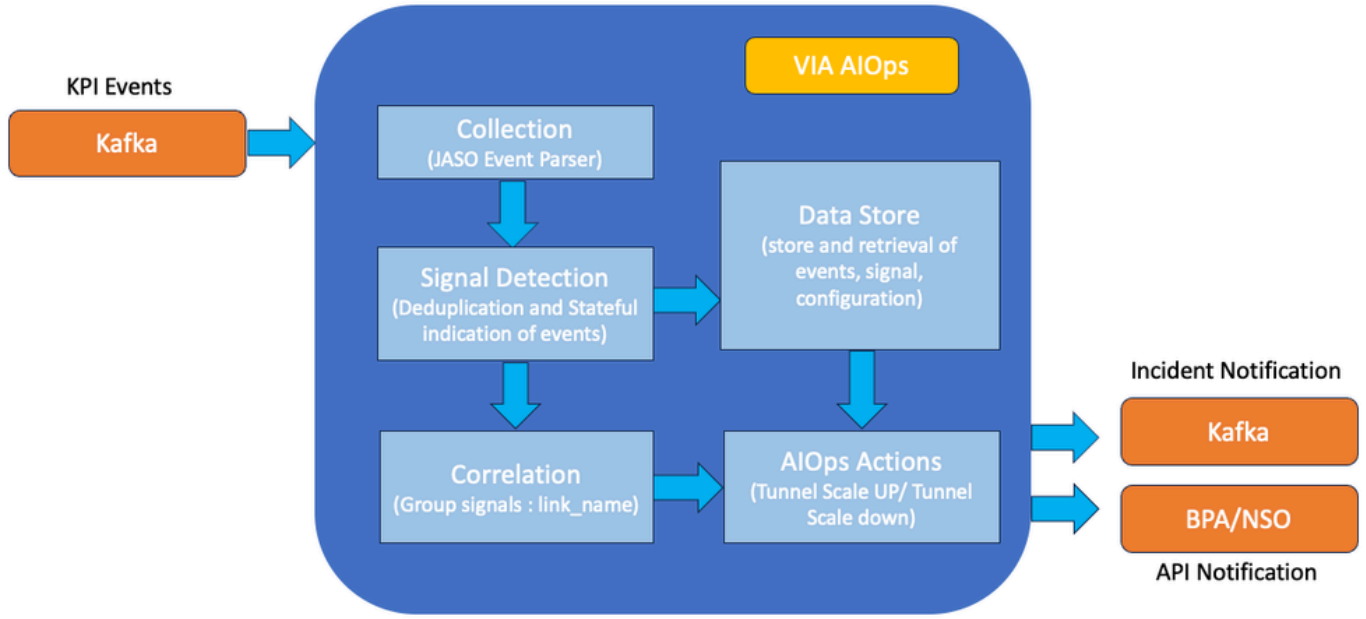
必須將VIA AIOp中的JASO事件解析器配置為從矩陣KPI異常事件中提取並解釋相關維度，即「host」、「kpi」、「index」和「value」。必須配置名為「automation_action」的其他維，以便由JASO事件解析器根據矩陣KPI異常事件中存在的「value」度量進行動態更新。此維度對於判斷是否必須實行自動回應至關重要，特別是要透過處理「KPI值」欄位來觸發「GRE通道擴充」或「GRE通道縮減」程式。在VIA AIOps中，訊號表示事件的狀態合併。要增強此關聯過程，我們必須配置與「host」、「link name」、「kpi」和「automation_action」維相關的不同狀態訊號。該表舉例說明了訊號、相關組及其各自的相關配置。

例如，辨識為GRE_KPIA_SCALEUP的訊號將在VIA AIOps系統接收指定的KPI異常消息（如第3節所述）後啟動。

透過AIOps訊號名稱	訊號相關金鑰	相互關聯群組規則名稱
GRE_KPIA_SCALEUP	主機、kpi、連結名稱、	GRE隧道擴展

	Automated_action	
GRE_KPIB_SCALEUP	主機、kpi、連結名稱、Automated_action	
GRE_KPIA_SCALEDOWN	主機、kpi、連結名稱、Automated_action	GRE隧道縮放
GRE_KPIB_SCALEDOWN	主機、kpi、連結名稱、Automated_action	

關聯組規則旨在便於將有關裝置A、裝置B及其各自的隧道A、B和C的訊號聚合到統一事件中。此關聯規則可確保對於裝置A和裝置B的任何特定配對，最多生成兩個不同的突發事件：一個涉及裝置A和裝置B的GRE隧道規模擴大事件，另一個涉及同一裝置配對的GRE隧道規模縮小事件。VIA AIOps代理架構能夠與業務流程自動化(BPA)和網路服務協調器(NSO)進行互動。



使用AIO的KPI事件關聯和通知

以下是透過AIO從BPA/NSO傳送到BPA/NSO的GRE隧道擴展API通知示例。

```
{
  "create": [
    {
      "gre-tunnels-device-cla": [
```

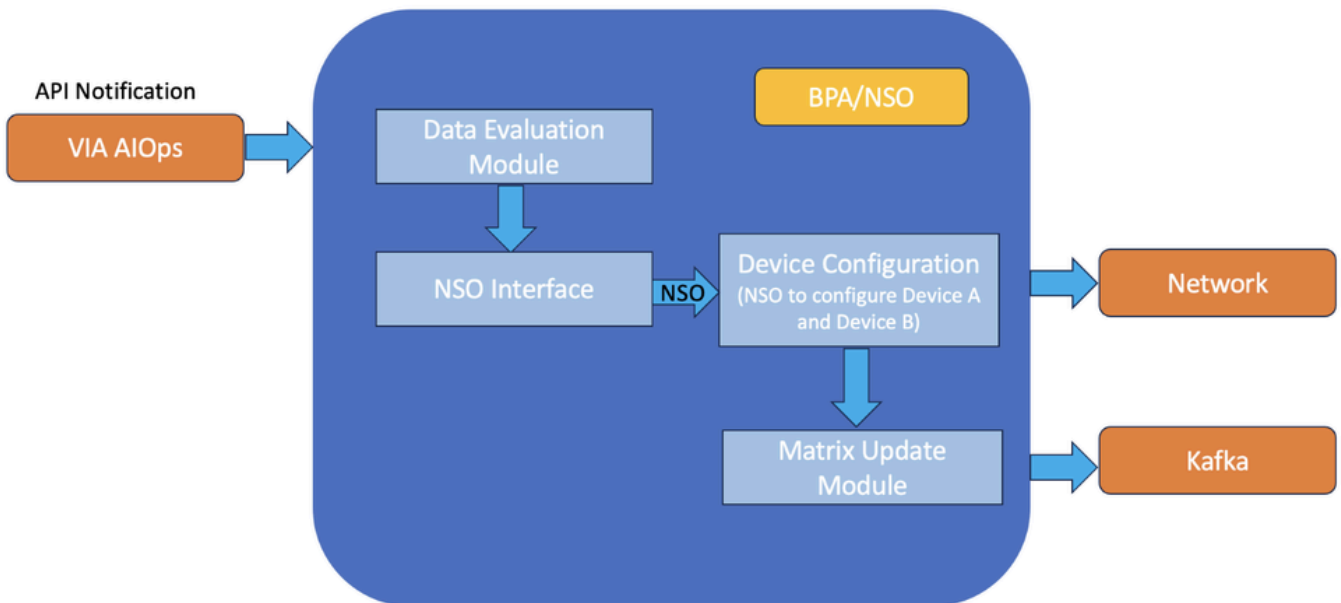
```

{
  "index": "RouterA-RouterB",
  "tunnelOperation": "SCALE UP",
  "MatrixData": [
    { "node": "RouterA", "kpi": "tunnel_utilization_agg" },
    { "node": "RouterB", "kpi": "tunnel_utilization_agg" }
  ]
}
]
}
]
}
}

```

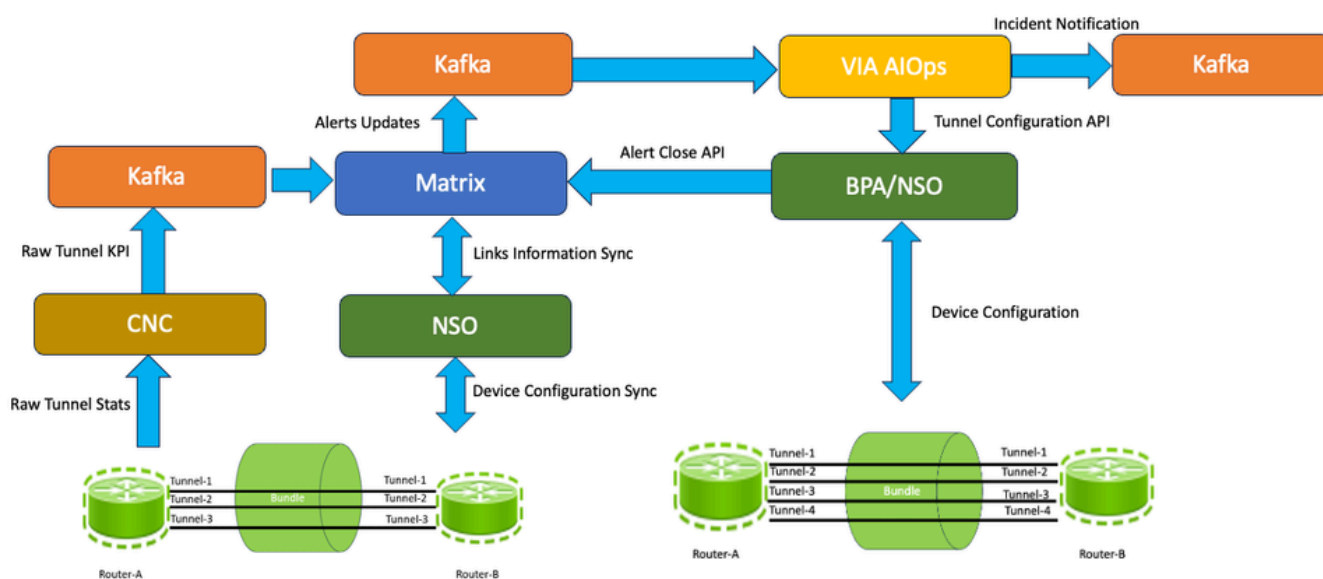
增加或刪除隧道和清除警報

當從VIA AIOs收到API呼叫時，思科業務流程自動化(BPA)透過內部請求向思科網路服務協調器(NSO)發出必要的擴展指令。BPA評估VIA AIOs提供的資料有效負載，包括隧道操作詳細資訊、索引和矩陣資料。利用索引和隧道操作資訊與NSO介面，提供用於縮放操作的引數。同時，矩陣資料由「矩陣更新模組」處理，該模組負責透過與矩陣API介面解決任何KPI異常事件。



在啟動任何擴展操作之前，需要為NSO開發YANG操作模型。此模型定義了NSO必須執行哪些特定操作才能增加或減少路由器A和路由器B之間的隧道計數。業務流程自動化(BPA)系統透過與網路服務協調器(NSO)合作進行「試運行」來擴展操作。這是操作的初始階段，在此階段，BPA請求NSO模擬所需的配置更改，而不應用這些更改。乾運行是重要的驗證步驟，可確保所提議的縮放操作（如YANG操作模型所定義）能夠執行，而不會在網路配置中造成任何錯誤或衝突。

如果乾運行被視為成功，表示已驗證縮放操作，則BPA將前進到「提交」階段。此時，BPA指示NSO實施增加或減少路由器A和路由器B之間的GRE隧道計數所需的實際配置修改。BPA使用API呼叫觸發Matrix的「矩陣更新模組」，以與VIA AIOps一起關閉KPI事件。在Matrix上關閉此異常後，Matrix還會向VIA AIOps傳送嚴重性為「已清除」的警報，VIA AIOps會進一步關閉事件。這樣，網路級別的補救週期就完成了。此圖描述了應用內資料流的通用版本，用於此閉環自動化。



GRE通道套件閉環自動化的資料流

封閉環路，開啟新的自動修正可能性

本文討論的解決方案透過基於網路異常的GRE捆綁擴展的一個示例進行仔細討論，以幫助我們瞭解此解決方案的各種構建塊。我們簡要研究了思科技術堆疊（包括Cisco NSO、Cisco Matrix和Cisco BPA）如何與VIA AIOps、Kafka和其他軟體堆疊等元件無縫整合，以幫助我們自動監控和修復網路問題。此解決方案為服務提供商或企業網路中出現的所有其他網路使用案例提供了可能性。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。