通过闭环自动化软件堆栈实现按需带宽使用案例的自动化

目录

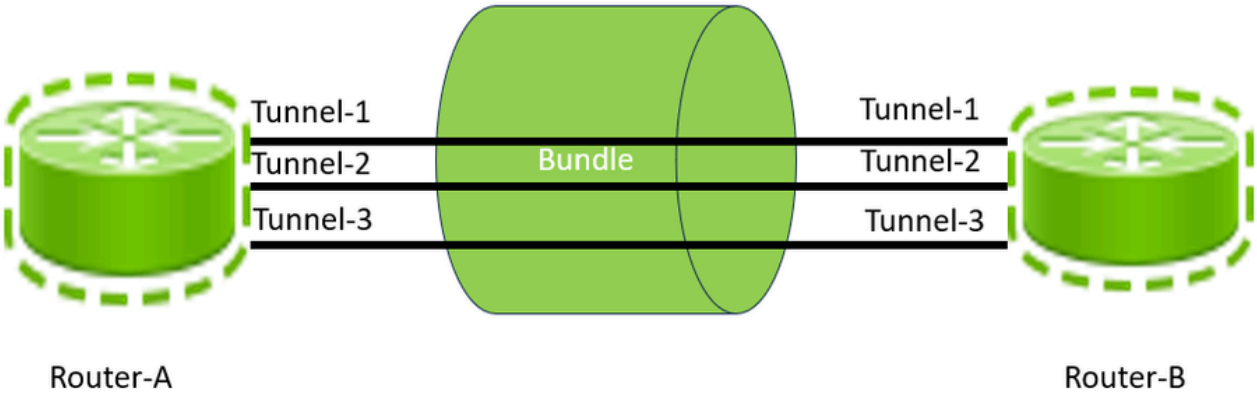
简介

本文档介绍用于通用路由封装(GRE)隧道扩展自动化的思科闭环自动化解决方案中的组件，及其对于其他情况的适应性。

背景信息

服务提供商希望控制其整个网络内GRE隧道的带宽利用率，并密切监控带宽利用率，以便使用智能闭环自动化解决方案根据需要扩展隧道。

GRE是一种隧道协议，它提供了一种简单的通用方法，使用封装传输一个协议的数据包。本文档重点介绍Cisco IOS® XRv平台的基于GRE隧道的示例，但也可以推广到其他平台。 GRE封装有效载荷，即需要在外部IP数据包内部传输到目标网络的内部数据包。GRE隧道充当虚拟点对点链路，两个端点由隧道源和隧道目标地址标识。



路由器之间的GRE隧道

配置GRE隧道涉及创建隧道接口和定义隧道源和目标。下图显示了路由器A和路由器B之间的三个GRE隧道的配置。对于此配置，必须创建三个接口，每个接口在路由器A上，例如Tunnel-1、Tunnel-2和Tunnel-3；同样，在路由器B上创建三个接口，例如Tunnel-1、Tunnel-2和Tunnel-3。在两个服务提供商路由器之间，可以有多个GRE隧道。与任何其它网络接口一样，每个隧道都有基于接口容量的规定容量。因此，隧道只能传输等于其带宽的最大流量。隧道数量通常基于对两个站点（路由器）之间的流量负载和带宽利用率的初始预测。随着网络和网络扩展的变化，这种带宽使用率也会随之改变。为了最佳利用网络带宽，必须根据两台设备之间所有隧道的带宽使用率，在两台设备之间添加新的隧道或移除额外的隧道。

在本例中，您可以说，路由器A和路由器B之间的所有三个隧道的总容量是隧道1、隧道2和隧道3的容量之和，这称为聚合带宽或GRE捆绑级带宽。请注意，此处的“bundle”关键字是指一对路由器之间的隧道；不应使用与LACP/Etherchannel链路捆绑的隐式关系。此外，两个路由器之间的实际流量是通过Tunnel-1、Tunnel-2和Tunnel-3的总汇聚流量。通常，您可以设计一个捆绑级带宽利用率的概念，该概念可以是隧道总流量与两台路由器之间所有隧道总容量的比率。通常，如果发现带宽过度利用或利用不足，任何服务提供商都希望通过在两台路由器之间添加或删除隧道来采取补救措施。但是，对于本文档，请考虑两个路由器之间的捆绑层利用率如果较低，则阈值下限为20%，如果较高利用率，则阈值下限为80%。

要求

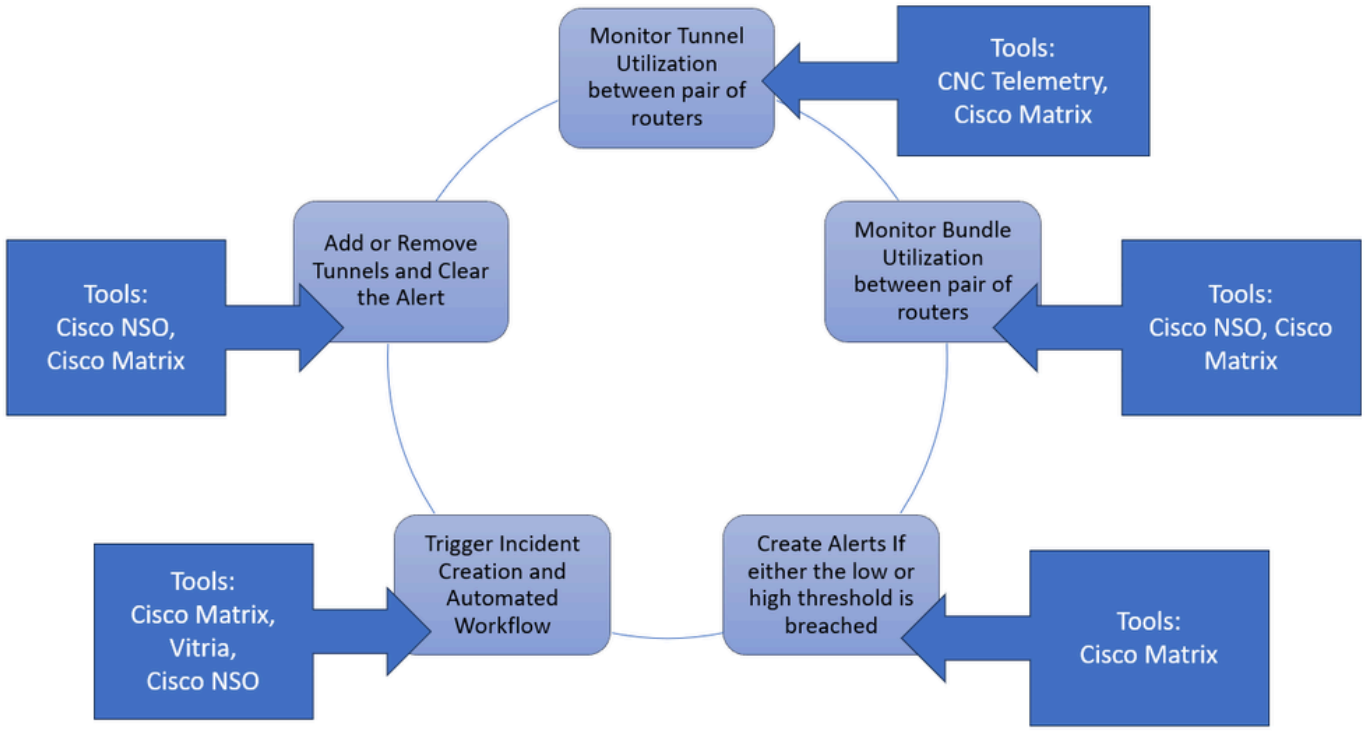
1. 在XRv9K上执行GRE捆绑包端到端闭环自动化需要闭环解决方案，系统可以在其中收集遥测数据、以关键绩效指标(KPI)的形式监控数据、应用汇聚、创建阈值交叉警报(TCA)以及执行自动补救配置和关闭警报。
2. 该解决方案可以计算网络关键性能指标(KPI)，以基于所需频率下的隧道的原始吞吐量，为每个隧道提供单独的隧道入口(Rx)和隧道出口(Tx)带宽利用率。
3. 该解决方案能够计算自定义KPI，为每个捆绑提供隧道入口(Rx)和隧道出口(Tx)带宽利用率，这是一对路由器之间所有隧道的聚合带宽利用率。

4. 如果定义的捆绑包级别阈值被超过，该解决方案可以检测并创建警报。此类警报可用于监控。
5. 警报必须导致触发自动化工作流程，该工作流程可以进一步触发设备上的配置，以便根据警报条件添加或删除隧道。
6. 最后，系统必须自动关闭包含所需更新的警报。

解决方案

闭环自动化解决方案涉及多个工具，这些工具在整个端到端解决方案中致力于实现特定目标。 下图显示了哪些组件和工具可帮助我们实现最终架构，并概述了高级角色。您可以在后续部分中查看每个组件及其用法。

思科闭环自动化解



决方案思科闭环自动化解决方案

工具	目的
思科纵横式网络控制器(CNC)	Crosswork Network Controller可实现跨服务和设备生命周期的实时可视性，可直观地导航网络拓扑、服务库存、传输策略、服务运行状况、设备运行状况等更多支持各种使用案例，并提供通用、集成的用户体验。 在此解决方案中，它主要用作一种工具，用于使用gNMI（gRPC网络管理接口）或MDT管理设备和收集隧道性能数据。 更多详细信息：https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-controller/index.html

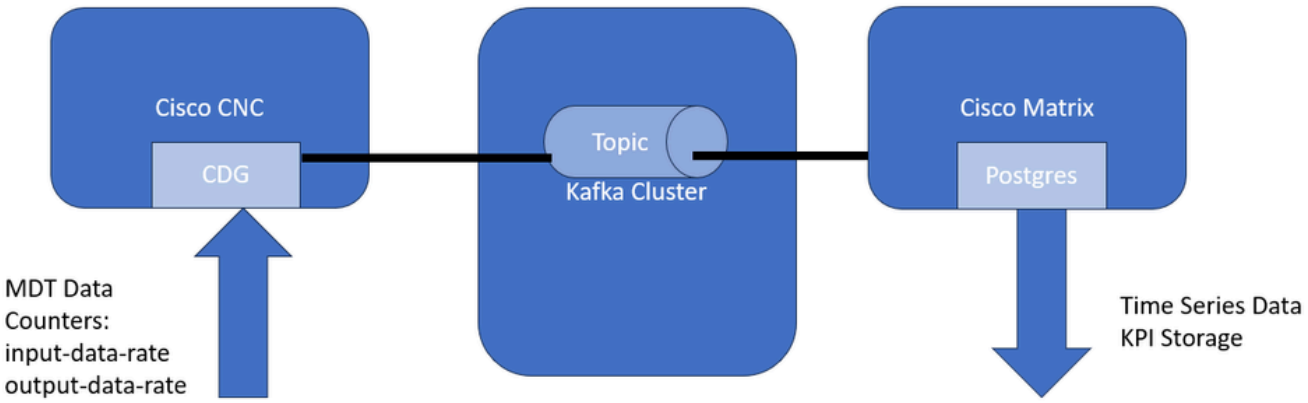
思科矩阵	CX分析服务（功能包）是利用Matrix解决方案提供的，Matrix解决方案是一个多供应商单一管理平台和多域分析解决方案。 在此解决方案中，矩阵使用CNC通过Kafka主题发送的Kafka中的数据，并使用拓扑查找进一步执行基于隧道的KPI到捆绑级别KPI的聚合，并将其作为时间序列数据存储，然后将其存储在Postgres数据库中。存储此类数据后，便可供可视化。Matrix使用阈值交叉警报进行异常检测，这允许我们为从网络收集的KPI配置阈值。
Kafka群集	Kafka集群是一个包含不同代理人的主题及其各自分区的系统。 制作者向群集内的主题发送或写入数据/消息。消费者读取或使用Kafka群集中的消息。 在此解决方案中，CNC充当生成器，在转换从路由器收集到的遥测数据之后，以JSON负载的形式将数据发送到预定义的Kafka主题。 在此解决方案中，Matrix作为消费者，消费此数据，处理此数据，聚合此数据，并将其存储以供进一步处理和异常检测。
思科NSO	思科交叉工作网络服务协调器(NSO) NSO是为服务提供商和大型企业构建的Crosswork自动化工具组合的一部分。 在此解决方案中，NSO收集与所有隧道和设备相关的信息，并为此解决方案构建自定义拓扑表。 此外，在此解决方案中，NSO和业务流程自动化功能用于触发补救工作流程，并采取行动，如添加或删除设备中的隧道以及进一步清除Cisco Matrix中的警报。 更多详细信息：https://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html
通过AIOps的Vitria	Vitria VIA AIOps for Cisco Network Automation提供自动分析，能够跨所有技术和应用层快速补救影响服务的事件。 在此解决方案中，VIA AIOps用于关联从Cisco Matrix生成的KPI阈值事件，以创建事件、通知并触发针对Cisco NSO的自动操作，以增加或减少GRE隧道计数。 更多详细信息：https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/solution-overview-c22-2403404.html

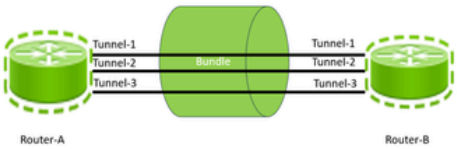
解决方案采取这些步骤来完成此用例，后面的部分将详细介绍这些步骤。

1. 监控路由器对之间的隧道利用率
2. 监控路由器对之间的捆绑利用率
3. 创建阈值超限警报
4. 触发事件和自动修正工作流
5. 添加或删除隧道和清除警报

监控路由器对之间的隧道利用率

应用程序通过收集作业请求数据收集。然后，Cisco Crosswork将这些收集作业分配到Cisco Crosswork数据网关以服务于请求。 Crosswork数据网关支持使用模型驱动遥测(MDT)从网络设备收集数据，以直接从设备使用遥测流（仅适用于基于Cisco IOS XR的平台）。Cisco Crosswork允许您创建收集作业可用于存放数据的外部数据目标。可以将Kafka添加为REST API创建的收集作业的新数据目标。在此解决方案中，CDG从与隧道接口统计信息相关的路由器收集数据，并将数据发送到Kafta主题。Cisco Matrix使用Kafka主题中的数据，并将数据分配给Matrix工作应用程序，该应用程序将数据作为KPI进行处理，并以时间序列方式保存数据，如后面描述流程图所示。





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

思科闭环自动化解决方案

时序数据具有存储在矩阵数据库中的KPI属性。

KPI属性	目的
节点	存储KPI的设备或源 示例：Router-A
时间	收集数据的时间 示例：22-05-2024 10:00:00
索引	唯一标识符

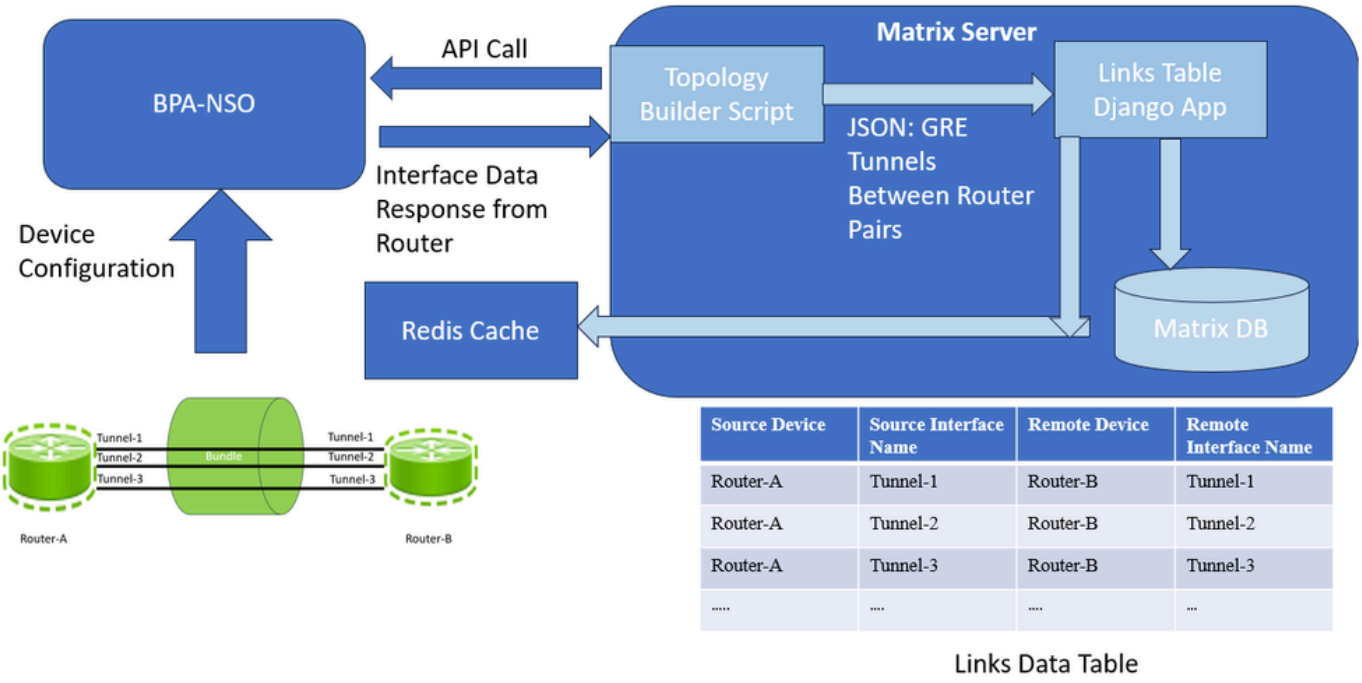
	示例：Tunnel-1
价值	KPI值-数值
KPI	KPI名称 示例：隧道利用率

监控路由器对之间的捆绑利用率

一旦您拥有上一部分中提到的时间序列数据，您就可以按隧道接口收集流量统计信息。但是，您需要确定哪个设备与哪个源隧道接口连接，哪个设备与哪个其他设备连接，以及哪个是远程接口名称。这称为链路标识，您可以在其中标识源设备名称。源接口名称、远程设备名称和远程接口名称。 要准确解释链路信息和路由器，您需要一个参考示例（如图所示）。

源设备	源接口名称	远程设备	远程接口名称
路由器 A	Tunnel-1	路由器B	Tunnel-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
....	...	...	..

要在此解决方案中构建此拓扑链路表，您可以根据每天在首选时间在服务器上运行的脚本填充一个自定义表，即链路数据表，该表内置在矩阵中。此脚本对BPA-NSO执行API调用，并返回路由器对之间GRE捆绑的JSON输出。然后解析接口数据，以JSON格式构建拓扑。该脚本还将接收此JSON输出，并每天将其写入链路数据表。每当它向表中加载新数据时，它也会将此数据写入Redis缓存，以减少进一步的数据库查找和提高效率。



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

链接数据表过程

因此，相同两台设备之间的所有链路必然是捆绑的一部分，该捆绑被标识为属于同一捆绑。原始隧道级别KPI可用后，您即在Matrix上构建了一个自定义KPI_aggregate应用，该应用将执行计算捆绑级别利用率并将它们存储为KPI的工作。

此应用程序采用以下输入：

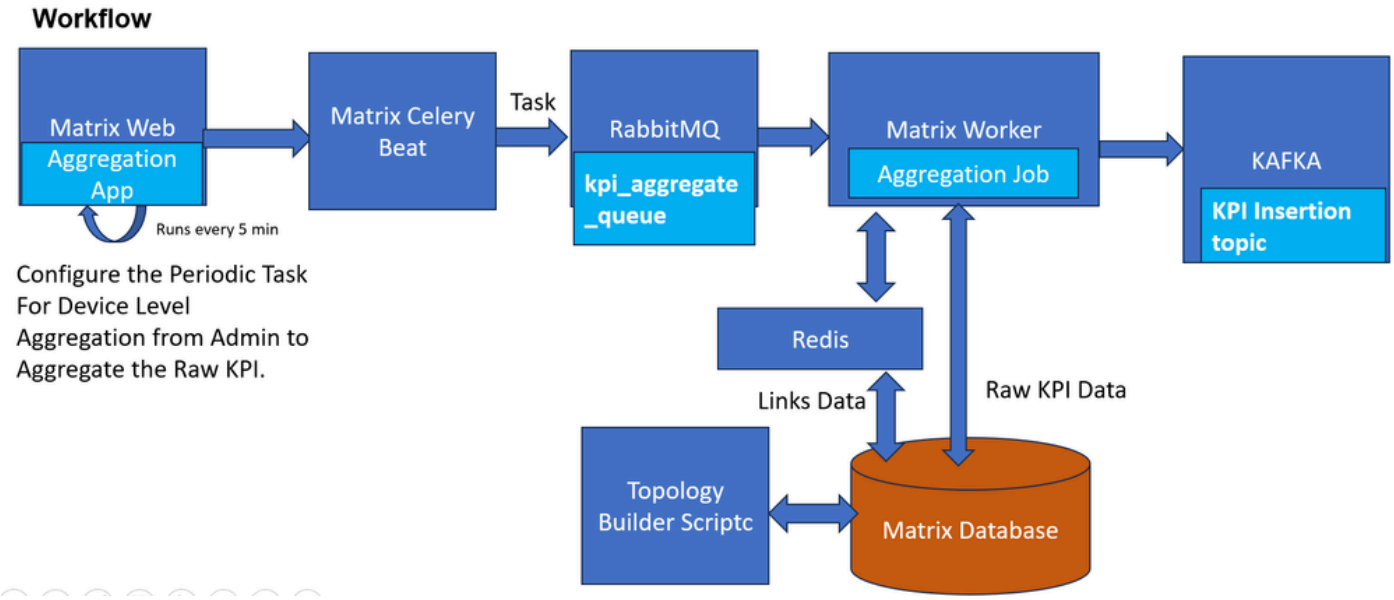
配置属性	目的
Crontab	必须运行聚合定期任务的频率
已启用复选框	激活/停用此配置
隧道接口KPI名称	用于计算聚合KPI的原始KPI的名称。 聚合KPI名称会自动创建为<Raw_KPI_Name>_agg
日期范围	原始数据的频率。

聚合任务从KPI原始数据和链路数据库获取输入，标识构成同一捆绑的一部分的隧道，并根据此逻辑将这些隧道添加到组中。

```
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，在这种情况下，KPI名称会为原始隧道KPI隧道利用率生成“tunnel-utilization_agg”。完成所有路由器和隧道组合的所有原始KPI值的计算后，将为指向Kafka主题的每个链接推送此数据，该主题必须与接收已处理的KPI的主题相同。这样，此信息会像从有效源接收的任何其他正常KPI一样保留。DB使用者使用此主题并将该KPI保留到矩阵数据库中的KPI结果表中，以供聚合KPI使用。



用于捆绑包级别聚合KPI的KPI聚合流程

创建阈值超限警报

矩阵中配置的KPI阈值为85%，这意味着当此KPI的值超过阈值时，将生成严重警报；当该值低于阈值时，将生成清晰警报。这些警报保存在矩阵数据库中，并在此解决方案中转发给Vitria，用于闭环自动化使用案例。如果KPI的计算值超过阈值，系统会通过Kafka将警报发送到Vitria (VIA-AIOPs)，消息中的当前状态为“严重”。同样，如果该值在阈值内从关键值返回，则必须通过Kafka向VIA-AIOP发送警报，消息中的当前状态为Clear。向系统发送了一个示例消息，其属性如下。

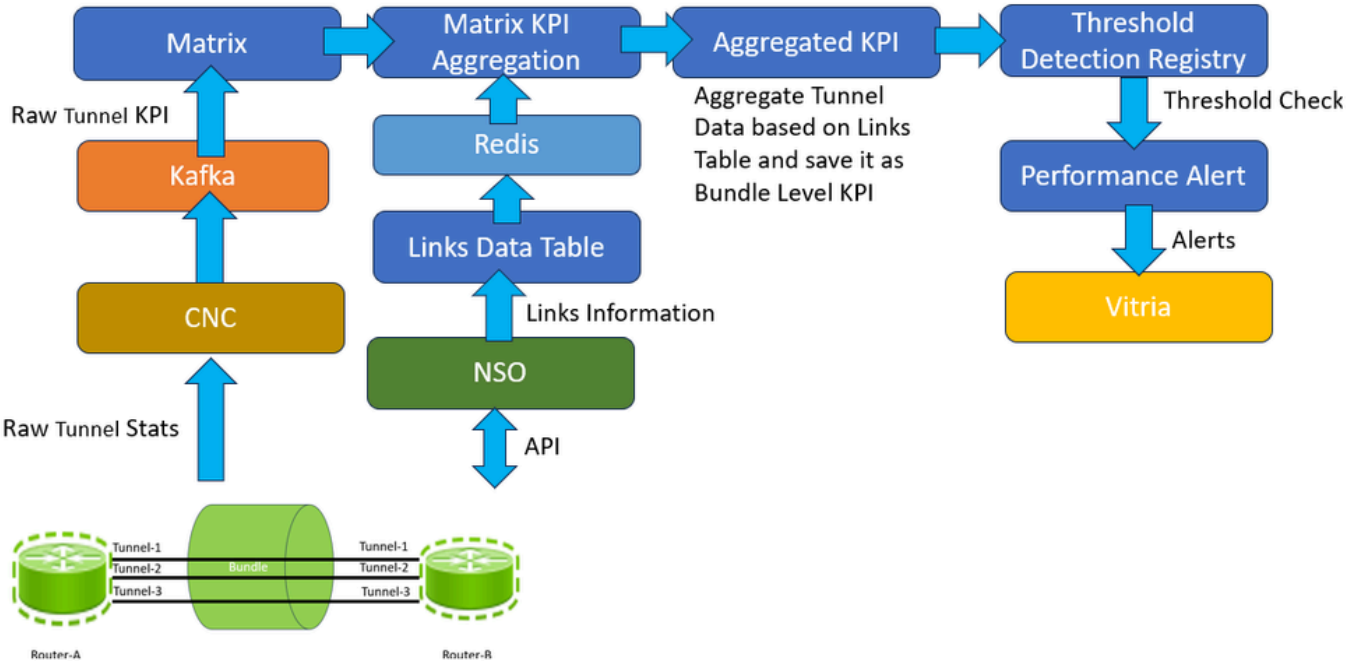
```
{
  "节点"："路由器A"，
  "节点类型"："路由器"，
```

```
  "kpi" : "tunnel_utilization_agg" ,
  "kpi_description" : "捆绑包级别利用率" ,
  "架构" : "" ,
  "index" : "Router-A_Router-B" ,
  “时间” : “2023-08-09 05:45:00+00:00” ,
  "值" : "86.0" ,
  "previous_state" : "CLEAR" ,
  "current_state" : "CRITICAL" ,
  "link_name" : "Router-A_Router-B"
}
```


Kafka警报消息属性	示例值	目的
节点	路由器 A	网络设备名称
node_type	路由器	设备类型
KPI	tunnel_utilization_agg	KPI名称
kpi_description	捆绑包级别利用率	KPI描述
方案	不适用	不适用
索引	Router-A_Router-B	<local_device>-<remote_device>
时间	“2023-08-09 05:45:00+00:00”	时间
价值	86.0	KPI值
previous_state	清除	上一个警报状态
current_state	关键	当前警报状态

link_name	Router-A_Router-B	关联属性

link_name属性是按字母顺序排序的索引值中存在的设备名称。这样做是为了在VIA AIOP级别实现关联，其中VIA AIOp必须关联来自同一捆绑链路的警报。例如，当多个警报以相同的link_name进入VIA AIOP时，这意味着这些警报属于网络中的同一捆绑链路，用链路名称中的设备名称表示。



使用矩阵检测注册表生成KPI聚合警报

触发事件和自动修正工作流

VIA AIOps将配置为从指定的Kafka主题中接收关键绩效指标(KPI)异常事件。通过Kafka消息收到的这些事件由VIA AIOp通过JASO事件解析器进行处理，以便后续接收。对于VIA AIO而言，关键是要准确识别与GRE隧道相关的KPI异常事件，确定它们与特定设备对（例如，路由器A -路由器B）的关联，并确定该异常是否需要启动GRE隧道扩展自动化（升级或降级）。

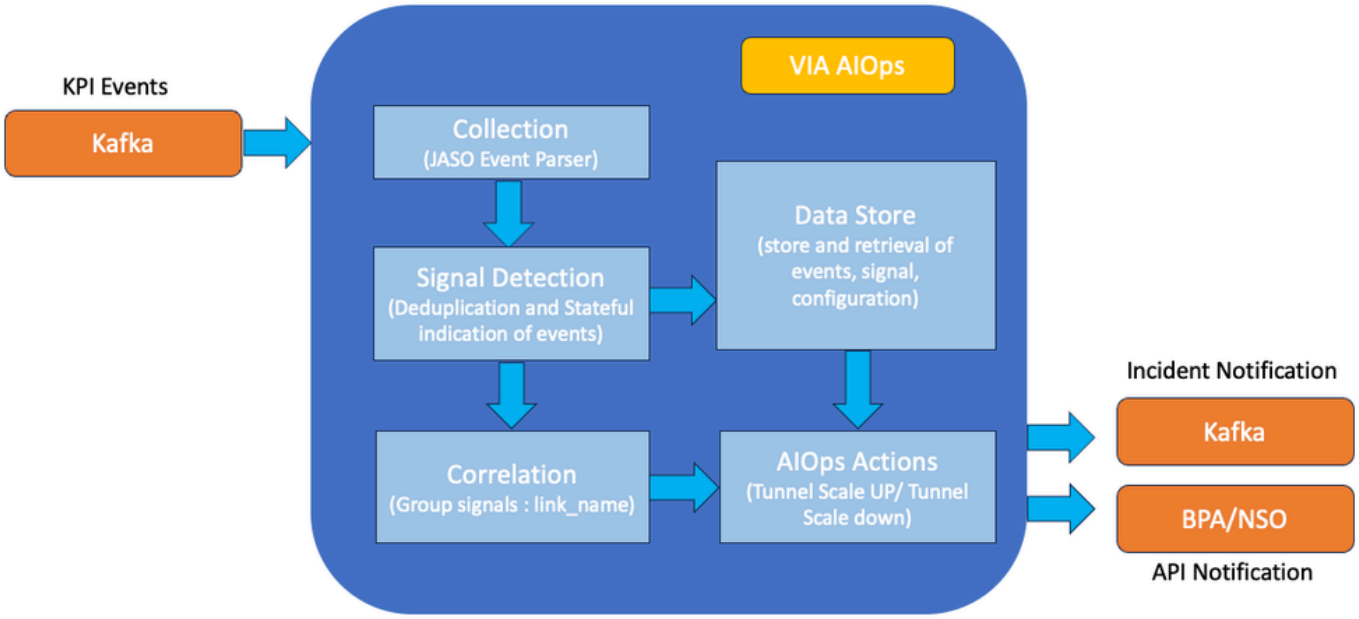
必须将VIA AIOp中的JASO事件解析器配置为从矩阵KPI异常事件中提取并解释相关维度，即“host”、“kpi”、“index”和“value”。必须配置名为“automation_action”的附加维，使其由JASO事件解析器根据矩阵KPI异常事件中存在的“value”度量进行动态更新。在确定是否必须实施自动响应时，此维非常关键，尤其是通过处理“KPI值”字段来触发“GRE隧道扩展”或“GRE隧道缩减”过程。在VIA AIOps中，信号表示事件状态的整合。要增强此关联过程，我们必须配置与“主机”、“链路名称”、“kpi”和“automation_action”维相关的不同状态信号。下表举例说明了信号、相关组及其各自的相关配置。

例如，识别为GRE_KPIA_SCALEUP的信号将在接收指定KPI异常消息（如第3节所述）后由VIA AIOps系统启动。

通过AIOps信号名称	信号相关密钥	关联组规则名称 (Correlation Group Rule Name)

GRE_KPIA_SCALEUP	主机、kpi、链路名称、Automated_action	GRE隧道扩展
GRE_KPIB_SCALEUP	主机、kpi、链路名称、Automated_action	
GRE_KPIA_SCALEDOWN	主机、kpi、链路名称、Automated_action	GRE隧道缩放
GRE_KPIB_SCALEDOWN	主机、kpi、链路名称、Automated_action	

关联组规则用于促进关于设备A、设备B及其各自隧道A、B和C的信号汇聚成统一事件。此关联规则可确保对于设备A和设备B的任何特定配对，最多生成两个不同的事件：一个事件用于涉及设备A和设备B的GRE隧道扩展，另一个事件用于同一设备配对的GRE隧道缩放。VIA AIOps代理框架能够与业务流程自动化(BPA)和网络服务协调器(NSO)交互。



通过AIO使用KPI事件关联和通知

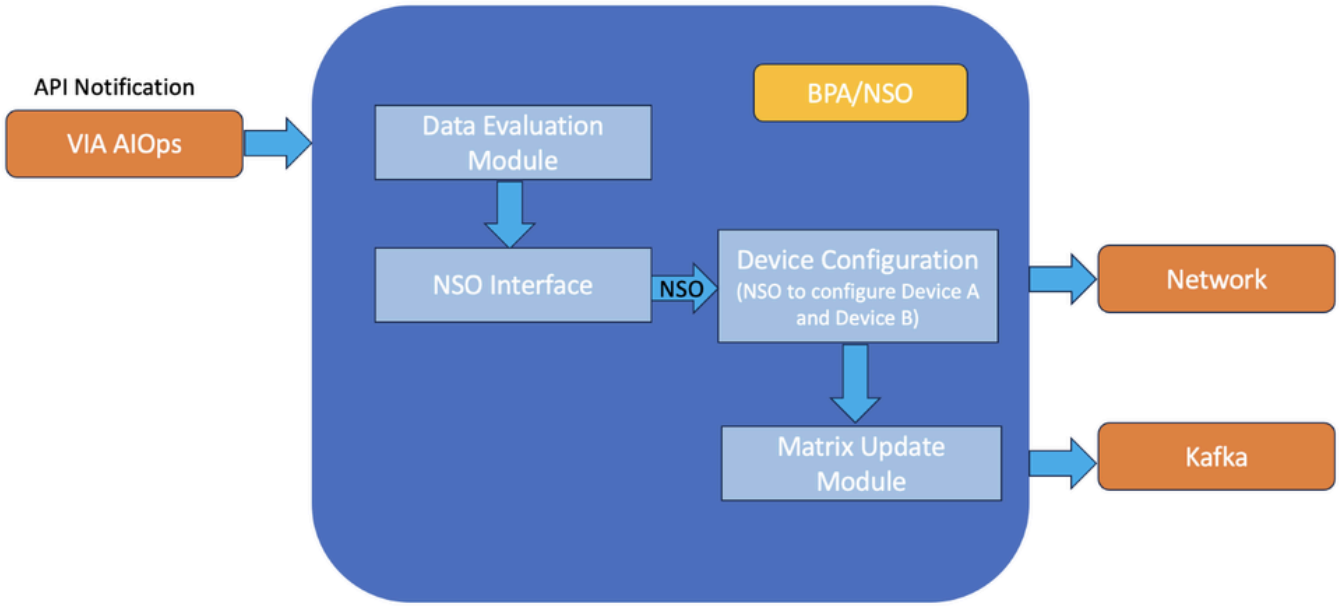
以下是通过AIO从BPA/NSO发送到BPA/NSO的GRE隧道扩展API通知示例。

```
{
  "create": [
    {
```

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

添加或删除隧道和清除警报

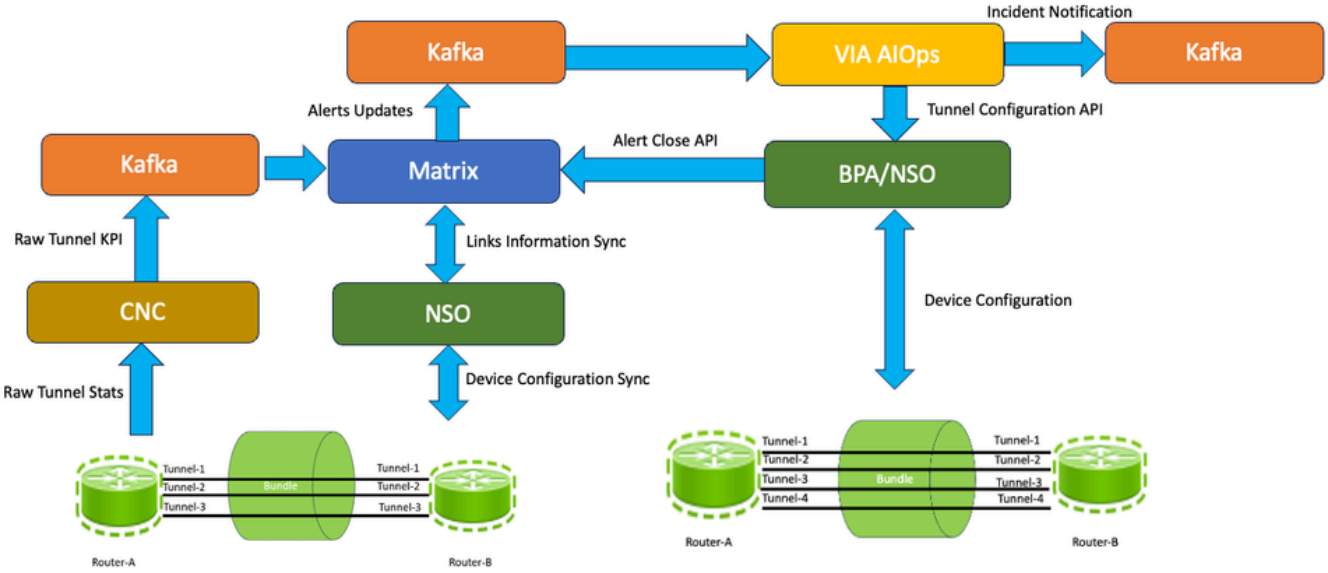
通过AIO收到API调用后，思科业务流程自动化(BPA)会通过内部请求向思科网络服务协调器(NSO)发出必要的扩展指令。BPA评估VIA AIOps提供的数据负载，包括隧道操作详细信息、索引和矩阵数据。 利用索引和隧道操作信息与NSO接口，提供用于缩放操作的参数。同时，矩阵数据由“矩阵更新模块”处理，该模块负责通过与矩阵API的接口解决任何KPI异常事件。



使用BPA-NSO的数据验证和设备配置

在开始任何扩展操作之前，需要为NSO开发YANG操作模型。此模型定义了NSO必须执行以增加或减少路由器A和路由器B之间的隧道计数的特定操作。Business Process Automation (BPA)系统通过与网络服务协调器(NSO)合作进行“试运行”来扩展操作。这是操作的初始阶段，BPA请求NSO模拟预期的配置更改，而不应用这些更改。试运行作为一个基本验证步骤，确保可以执行YANG操作模型定义的建议扩展操作，而不会导致网络配置中出现任何错误或冲突。

如果试运行被视为成功，表明扩展操作已验证，则BPA将前进到“提交”阶段。此时，BPA指示NSO实施必要的实际配置修改，以增加或减少路由器A和路由器B之间的GRE隧道计数。BPA使用API调用触发Matrix的“Matrix Update Module”，与VIA AIOp一起关闭KPI事件。在Matrix上关闭此异常后，Matrix还会向VIA AIOps发送严重性为“已清除”的警报，VIA AIOps会进一步关闭事件。这样，网络级补救周期就完成了。此图显示了此闭环自动化中使用的应用程序内数据流的通用版本。



GRE隧道包闭环自动化数据流

关闭环路以开启新的自动补救可能性

本文讨论的解决方案通过基于网络异常的GRE捆绑扩展的一个示例进行了详细讨论，以帮助我们关联此解决方案的各种构建块。我们简要研究了思科技术堆栈（包括Cisco NSO、Cisco Matrix和Cisco BPA）如何与VIA AIOps、Kafka和其他软件堆栈等组件无缝集成，以帮助我们自动监控和修复网络问题。此解决方案为服务提供商或企业网络中可能出现的所有其他典型网络使用案例提供了可能性。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。