

# Closed Loop Automation 소프트웨어 스택을 통해 온디맨드 대역폭 사용 사례 자동화

## 목차

---

[소개](#)

[배경 정보](#)

[요구 사항](#)

[솔루션](#)

[라우터 쌍 간의 터널 사용을 모니터링](#)

[라우터 쌍 간 번들 사용을 모니터링](#)

[임계값 초과 알림 생성](#)

[인시던트 트리거 및 자동화된 교정 워크플로](#)

[터널 추가 또는 제거 및 경고 지우기](#)

[루프를 닫아 자동 교정의 새로운 가능성 열림](#)

---

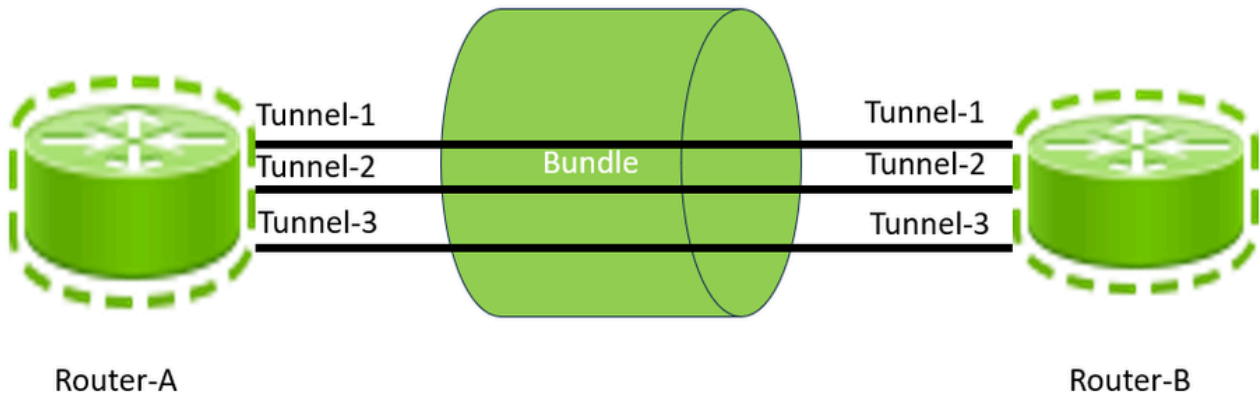
## 소개

이 문서에서는 Cisco GRE(Closed-loop automation solution for Generic Routing Encapsulation) 터널 확장 자동화의 구성 요소 및 기타 경우에 대한 적응성에 대해 설명합니다.

## 배경 정보

통신 사업자는 네트워크의 GRE 터널 전반에서 대역폭 활용을 제어하고 스마트 폐쇄 루프 자동화 솔루션을 사용하여 필요에 따라 터널을 확장하기 위해 이를 면밀히 모니터링하고자 합니다.

GRE는 캡슐화를 사용하여 한 프로토콜의 패킷을 다른 프로토콜로 전송하는 간단한 일반적인 접근 방식을 제공하는 터널링 프로토콜입니다. 이 문서에서는 Cisco IOS® XRv Platform에 대한 GRE 터널 기반 예제를 중점적으로 살펴보지만 다른 플랫폼으로 일반화할 수도 있습니다. GRE는 외부 IP 패킷 내의 목적지 네트워크로 전달되어야 하는 내부 패킷인 페이로드를 캡슐화합니다. GRE 터널은 터널 소스 및 터널 대상 주소로 식별된 두 엔드포인트와 함께 가상 포인트-투-포인트 링크로 작동합니다.



### 라우터 간 GRE 터널

GRE 터널을 구성하려면 터널 인터페이스를 생성하고 터널 소스와 대상을 정의합니다. 이 그림에서는 Router-A와 Router-B 간에 3개의 GRE 터널의 컨피그레이션을 보여줍니다. 이 컨피그레이션에서는 Router-A(예: Tunnel-1, Tunnel-2, Tunnel-3)에 각각 3개의 인터페이스를 생성하고 마찬가지로 Router-B(예: Tunnel-1, Tunnel-2, Tunnel-3)에 3개의 인터페이스를 생성해야 합니다. 두 통신 사업자 라우터 간에는 여러 GRE 터널이 있을 수 있습니다. 다른 네트워킹 인터페이스와 마찬가지로 각 터널에는 인터페이스 용량을 기반으로 하는 정의된 용량이 있습니다. 따라서 터널은 대역폭과 동일한 최대 트래픽만 전달할 수 있습니다. 터널 수는 두 사이트(라우터) 간의 트래픽 로드 및 대역폭 사용률에 대한 초기 예측을 기반으로 하는 경우가 많습니다. 네트워크 및 네트워크 확장이 변경됨에 따라 이러한 대역폭 사용률도 변화할 것으로 예상됩니다. 네트워크 대역폭을 최적으로 사용하려면 두 디바이스 간의 모든 터널에서 측정된 대역폭 사용률을 기준으로 두 디바이스 간에 새로운 터널을 추가하거나 추가 터널을 제거하는 것이 중요합니다.

이 예에서 Router-A와 Router-B 간의 3개 터널 모두 총 용량은 Tunnel-1, Tunnel-2 및 Tunnel-3의 용량을 합한 것이라고 할 수 있습니다. 이를 종합 대역폭 또는 GRE 번들 레벨 대역폭이라고 합니다. 여기서 'bundle' 키워드는 라우터 쌍 간의 터널을 참조하며, LACP/Etherchannel 링크 번들링과 암시적 관계는 없습니다. 또한 두 라우터 간의 실제 트래픽은 Tunnel-1, Tunnel-2 및 Tunnel-3에서 집계된 총 트래픽입니다. 일반적으로 번들 레벨 대역폭 사용률의 개념을 고안할 수 있습니다. 이는 두 라우터 간의 모든 터널의 총 용량에 대한 터널을 통과하는 총 트래픽의 비율일 수 있습니다. 일반적으로 모든 통신 사업자는 대역폭이 초과 사용되거나 충분히 활용되지 않는 것을 관찰할 경우 두 라우터 간에 터널을 추가하거나 제거하여 문제 해결 조치를 취하려고 합니다. 그러나 이 문서의 경우 낮은 임계값은 활용률이 낮은 경우 20%, 두 라우터 간의 번들 레벨 활용률이 높은 경우 80%입니다.

## 요구 사항

1. 시스템이 텔레메트리 데이터를 수집하고, KPI(Key Performance Indicators: 핵심 성과 지표)의 형태로 데이터를 모니터링하고, 어그리게이션을 적용하고, TCA(Threshold Cross Alerts: 임계값 교차 알림)를 생성하고, 자동화된 교정 컨피그레이션을 수행하고 알림을 받을 수 있는

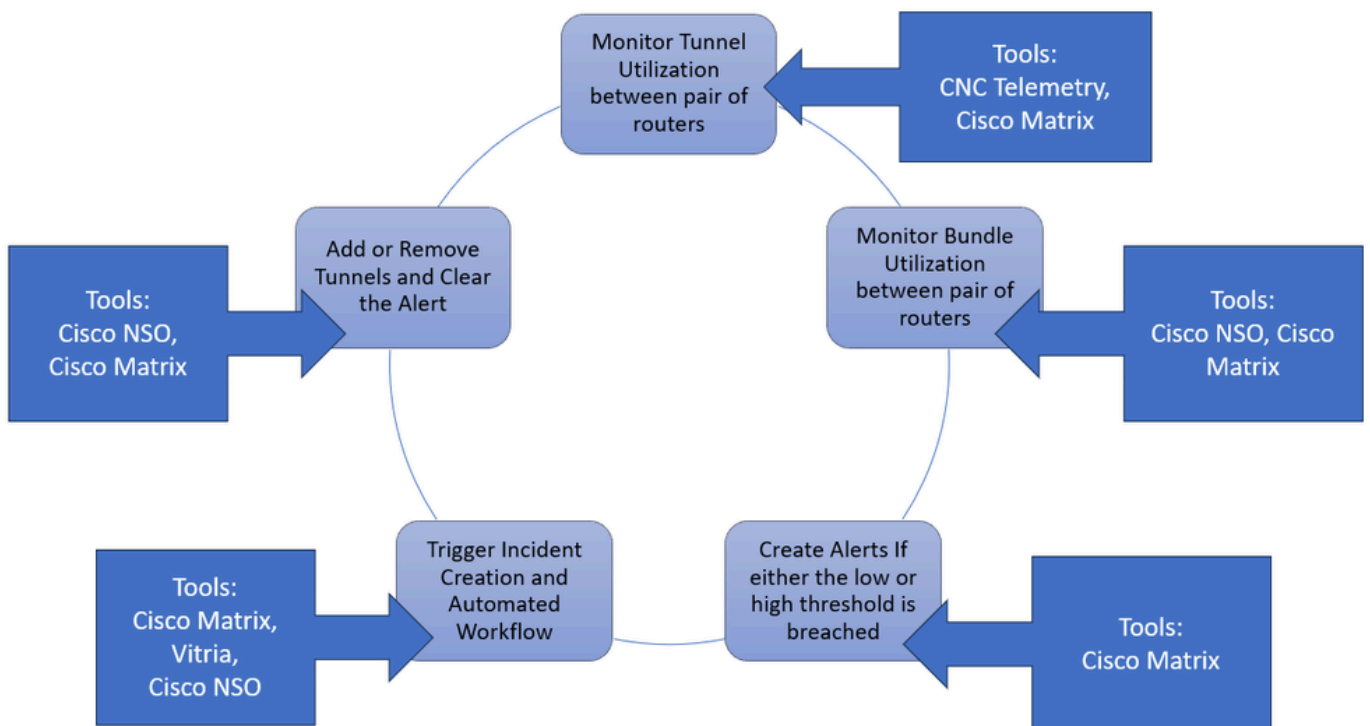
XRv9K에서 GRE 번들의 엔드 투 엔드 페루프 자동화를 수행하려면 페루프 솔루션이 필요합니다.

2. 이 솔루션은 네트워크 KPI(Key Performance Indicator)를 계산하여 원하는 빈도로 터널의 원시 처리량을 기반으로 하는 모든 터널의 개별 Rx(Tunnel Ingress) 및 Tx(Tunnel Egress) 대역폭 사용률을 제공할 수 있습니다.
3. 이 솔루션은 라우터 쌍 간의 모든 터널의 집계된 대역폭 사용률인 모든 번들의 Rx(Tunnel Ingress) 및 Tx(Tunnel Egress) 대역폭 사용률을 제공하기 위해 맞춤형 KPI를 계산할 수 있습니다.
4. 정의된 번들 레벨 임계값이 초과된 경우 솔루션에서 경고를 탐지하고 생성할 수 있습니다. 이러한 경고는 모니터링에 사용할 수 있습니다.
5. 경고는 자동화된 워크플로를 트리거해야 하며, 이는 경고 조건에 따라 터널을 추가 또는 제거하기 위해 디바이스에서 컨피그레이션을 추가로 트리거할 수 있습니다.
6. 마지막으로, 필요한 업데이트가 포함된 알림을 자동으로 받아야 합니다.

## 솔루션

Closed Loop Automation 솔루션에는 이 전체 엔드 투 엔드 솔루션에서 특정 목표를 달성하는 여러 툴이 포함되어 있습니다. 이 그림에서는 최종 아키텍처 달성에 도움이 되는 구성 요소와 툴을 보여주고, 상위 레벨 역할을 간략하게 설명합니다. 다음 섹션에서 각 구성 요소 및 그 사용을 살펴볼 수 있습니다.

### Cisco Closed Loop Automation



솔루션Cisco Closed Loop Automation 솔루션

툴	목적

Cisco CNC(Crosswork Network Controller)	<p>Crosswork Network Controller는 네트워크 토폴로지, 서비스 인벤토리, 전송 정책, 서비스 상태, 장치 상태 전반에 걸쳐 직관적인 탐색을 통해 서비스 및 장치 라이프 사이클 전반에 걸쳐 실시간 가시성을 제공하며, 공통의 통합 사용자 경험을 통해 다양한 사용 사례를 지원합니다.</p> <p>이 솔루션에서는 gNMI(gRPC Network Management Interface) 또는 MDT를 사용하여 디바이스 관리 및 터널 성능 데이터 수집 수집을 위한 툴로 주로 사용됩니다.</p> <p>추가 세부 정보:  <a href="https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-controller/index.html">https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-controller/index.html</a></p>
Cisco 매트릭스	<p>CX 분석 서비스(기능 팩)는 멀티벤더 단일 창 방식 다중 도메인 분석 솔루션인 Matrix 솔루션을 활용하여 제공됩니다.</p> <p>이 솔루션에서 매트릭스는 CNC가 Kafka Topics를 통해 보낸 Kafka의 데이터를 사용하며 토폴로지 조회를 사용하여 터널 기반 KPI를 번들 레벨 KPI로 집계하여 시계열 데이터로 저장하고 Postgres 데이터베이스에 저장합니다. 저장된 데이터는 시각화에 사용할 수 있으며 Matrix는 임계값 초과 알림을 사용하여 이상 징후 탐지를 수행하므로 네트워크에서 수집하는 KPI에 대한 임계값을 구성할 수 있습니다.</p>
카프카 성단	<p>카프카 클러스터는 서로 다른 브로커의 주제 및 각각의 파티션으로 구성된 시스템입니다. 생산자는 클러스터 내의 주제에 데이터/메시지를 보내거나 씁니다. 소비자는 Kafka 클러스터의 메시지를 읽거나 소비합니다.</p> <p>이 솔루션에서 CNC는 라우터에서 수집한 텔레메트리 데이터를 변환한 후 JSON 페이로드 형식으로 미리 정의된 Kafka 주제에 데이터를 전송하는 프로듀서 역할을 합니다.</p> <p>이 솔루션에서 Matrix는 이 데이터를 소비하고, 데이터를 처리하고, 데이터를 집계하고, 추가 처리 및 이상 징후 탐지를 위해 저장하는 소비자 역할을 합니다.</p>
Cisco NSO	<p>Cisco NSO(Crosswork Network Services Orchestrator)</p> <p>NSO는 통신 사업자와 대기업을 위해 구축된 자동화 툴링의 Crosswork 포트폴리오의 일부입니다.</p> <p>이 솔루션에서 NSO는 모든 터널 및 디바이스와 관련된 정보를 수집하고 이 솔루션에 대한 사용자 지정 토폴로지 테이블을 작성합니다.</p> <p>또한 이 솔루션에서는 NSO와 Business Process Automation 기능을 함께 사용하여 교정 워크플로를 트리거하고 디바이스에서 터널을 추가 또는 제거하고 Cisco Matrix에서 경고를 더 삭제하는 등의 조치를 취합니다.</p> <p>추가 세부 정보: <a href="https://www.cisco.com/c/en/us/products/cloud-systems-">https://www.cisco.com/c/en/us/products/cloud-systems-</a></p>

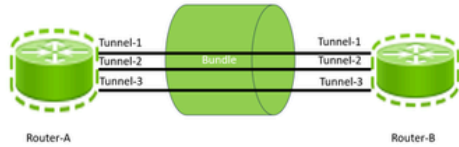
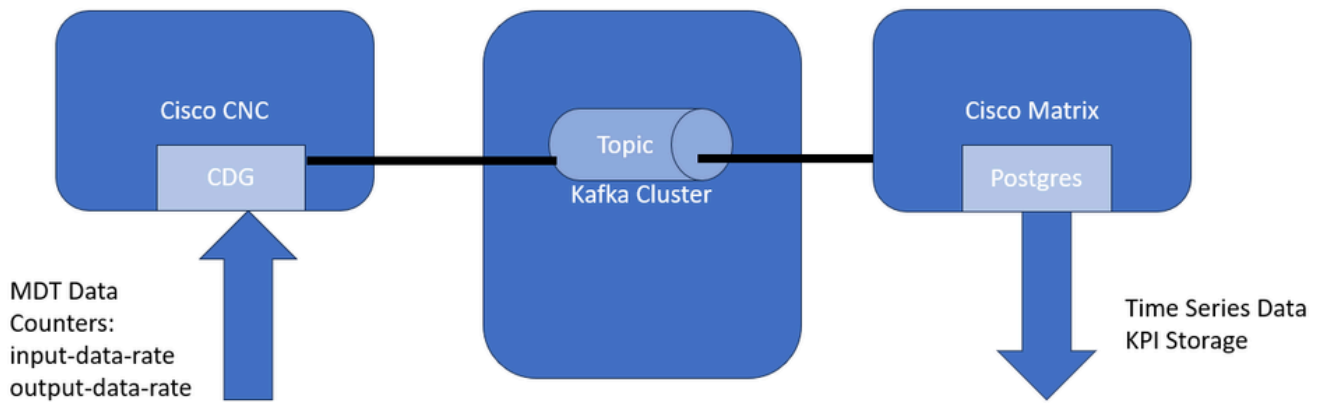
	<a href="https://www.cisco.com/management/network-services-orchestrator/index.html">management/network-services-orchestrator/index.html</a>
비트리아 비아 아이오스	<p>Vitria VIA AIOps for Cisco Network Automation은 모든 기술 및 애플리케이션 레이어에서 서비스에 영향을 미치는 이벤트를 신속하게 교정할 수 있도록 자동화된 분석을 제공합니다.</p> <p>이 솔루션에서는 VIA AIOps를 사용하여 Cisco Matrix에서 생성된 KPI 임계값 이벤트의 상관관계를 분석하고, 인시던트, 알림을 생성하고, Cisco NSO에 대해 자동화된 작업을 트리거하여 GRE 터널 수를 늘리거나 줄입니다.</p> <p>추가 세부 정보: <a href="https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/solution-overview-c22-2403404.html">https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/solution-overview-c22-2403404.html</a></p>

이 솔루션은 이 활용 사례를 이행하기 위해 다음 단계를 수행하는데, 이에 대해서는 후속 섹션에서 자세히 설명합니다.

1. 라우터 쌍 간의 터널 사용률 모니터링
2. 라우터 쌍 간 번들 사용률 모니터링
3. 임계값 초과 알림 생성
4. 인시던트 트리거 및 자동화된 교정 워크플로
5. 터널 추가 또는 제거 및 경고 지우기

## 라우터 쌍 간의 터널 사용률 모니터링

응용 프로그램이 수집 작업을 통해 데이터 수집을 요청합니다. 그런 다음 Cisco Crosswork는 이러한 수집 작업을 Cisco Crosswork Data Gateway에 할당하여 요청을 처리합니다. Crosswork Data Gateway는 MDT(Model-driven Telemetry)를 사용하여 네트워크 디바이스에서 데이터 수집을 지원하여 디바이스에서 직접 텔레메트리 스트림을 사용합니다(Cisco IOS XR 기반 플랫폼에만 해당). Cisco Crosswork를 사용하면 데이터를 저장하기 위해 수집 작업에서 사용할 수 있는 외부 데이터 대상을 생성할 수 있습니다.Kafka는 REST API에서 생성한 수집 작업에 대한 새 데이터 대상으로 추가할 수 있습니다. 이 솔루션에서 CDG는 터널 인터페이스 통계와 관련된 라우터에서 데이터를 수집하고 Kafka Topic에 데이터를 보냅니다. Cisco Matrix는 Kafka Topic의 데이터를 사용하고 데이터를 KPI로 처리한 Matrix 작업자 응용 프로그램에 데이터를 할당하며, 프로세스 흐름을 보여 주는 후속 그림과 같이 시계열 방식으로 저장합니다.



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 Closed Loop 자동화 솔루션

시계열 데이터에는 매트릭스 데이터베이스에 저장된 KPI 특성이 있습니다.

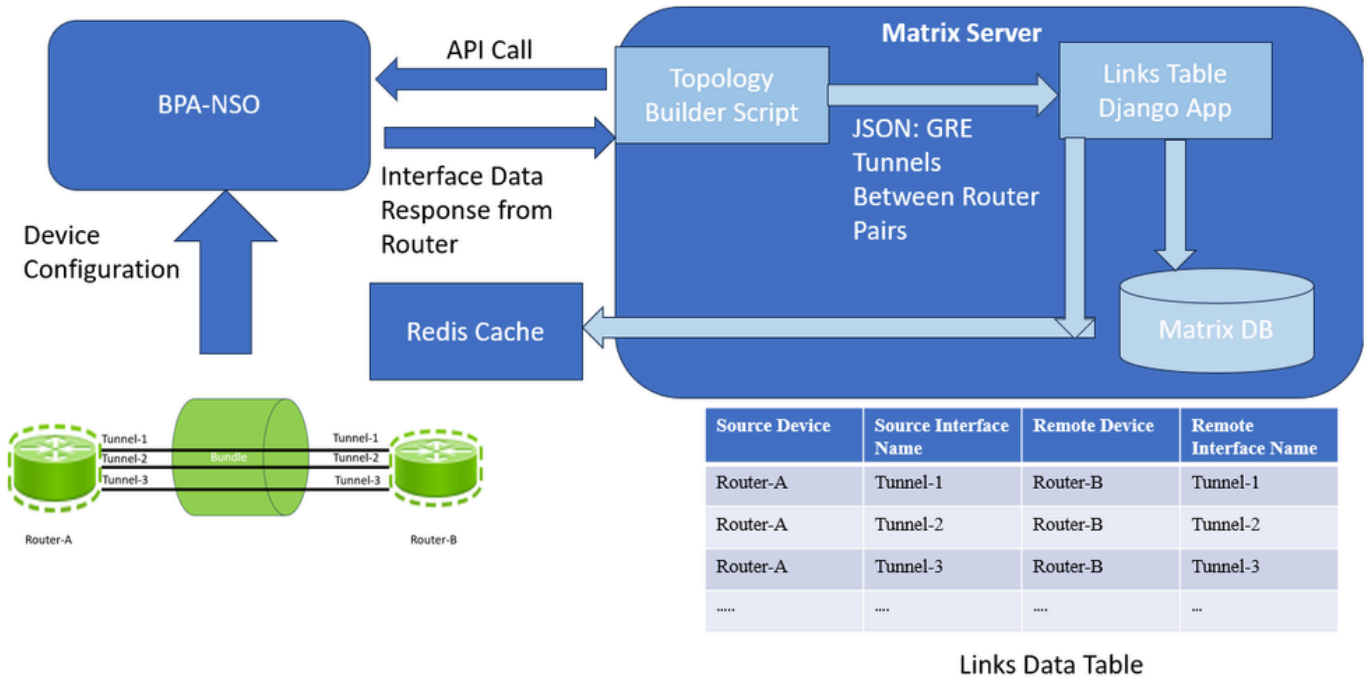
KPI 특성	목적
노드	KPI가 저장되는 장치 또는 원본 예: Router-A
Time	데이터가 수집되는 시간 예: 22-05-2024 10:00:00
색인	고유 식별자 예: Tunnel-1
가치	KPI 값 - 숫자 값
KPI	KPI 이름 예: tunnel-utilization

## 라우터 쌍 간 번들 사용률 모니터링

이전 섹션에서 설명한 대로 시계열 데이터를 갖게 되면 터널 인터페이스별로 트래픽 통계가 수집됩니다. 그러나 어떤 소스 터널 인터페이스가 어떤 다른 디바이스에 연결되었는지, 원격 인터페이스 이름은 무엇인지를 식별해야 합니다. 이를 Link Identification(링크 식별)이라고 하며 소스 디바이스 이름을 식별합니다. 소스 인터페이스 이름, 원격 디바이스 이름 및 원격 인터페이스 이름 링크 정보 및 라우터를 정확하게 해석하려면 설명된 참조 예가 필요합니다.

소스 디바이스	소스 인터페이스 이름	원격 장치	원격 인터페이스 이름
라우터-A	터널 1	라우터-B	터널 1
라우터-A	터널-2	라우터-B	터널-2
라우터-A	터널-3	라우터-B	터널-3
....	...	...	...

이 솔루션에서 이 토폴로지 링크 테이블을 작성하려면 서버에서 매일 기본 시간에 실행되는 스크립트를 기반으로 Matrix에 빌드된 사용자 지정 테이블인 링크 데이터 테이블을 채울 수 있습니다. 이 스크립트는 BPA-NSO에 대한 API 호출을 수행하고 라우터 쌍 간에 GRE 번들의 JSON 출력을 가져옵니다. 그런 다음 인터페이스 데이터를 구문 분석하여 JSON 형식으로 토폴로지를 구축합니다. 스크립트는 또한 이 JSON 출력을 가져와 Links Data Table에 매일 씁니다. 테이블에 새 데이터를 로드할 때마다 이 데이터를 Redis 캐시에 기록하여 추가 데이터베이스 검색을 줄이고 효율성을 향상시킵니다.



링크 데이터 테이블 프로세스

따라서 동일한 두 디바이스 간의 모든 링크는 동일한 번들에 속하는 것으로 식별된 번들의 일부여야 합니다. 원시 터널 레벨 KPI를 사용할 수 있게 되면 Matrix에 사용자 정의 KPI\_aggregate 앱을 빌드하여 번들 레벨 사용률을 계산하고 이를 KPI로 저장합니다.

이 애플리케이션은 다음과 같은 입력을 취합니다.

컨피그레이션 특성	목적
크론탭	집계 정기 작업이 실행되어야 하는 빈도
사용 확인란	이 구성 활성화/비활성화
터널 인터페이스 KPI 이름	집계 KPI 계산에 사용되는 원시 KPI의 이름입니다. 집계 KPI 이름은 <Raw_KPI_Name>_agg로 자동으로 생성됩니다.
날짜 범위	원시 데이터의 빈도입니다.

집계 작업은 KPI 원시 데이터 및 링크 데이터베이스에서 입력을 가져와 동일한 번들의 일부를 구성하는 터널을 식별하고 이 논리를 기반으로 그룹에 추가합니다.

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

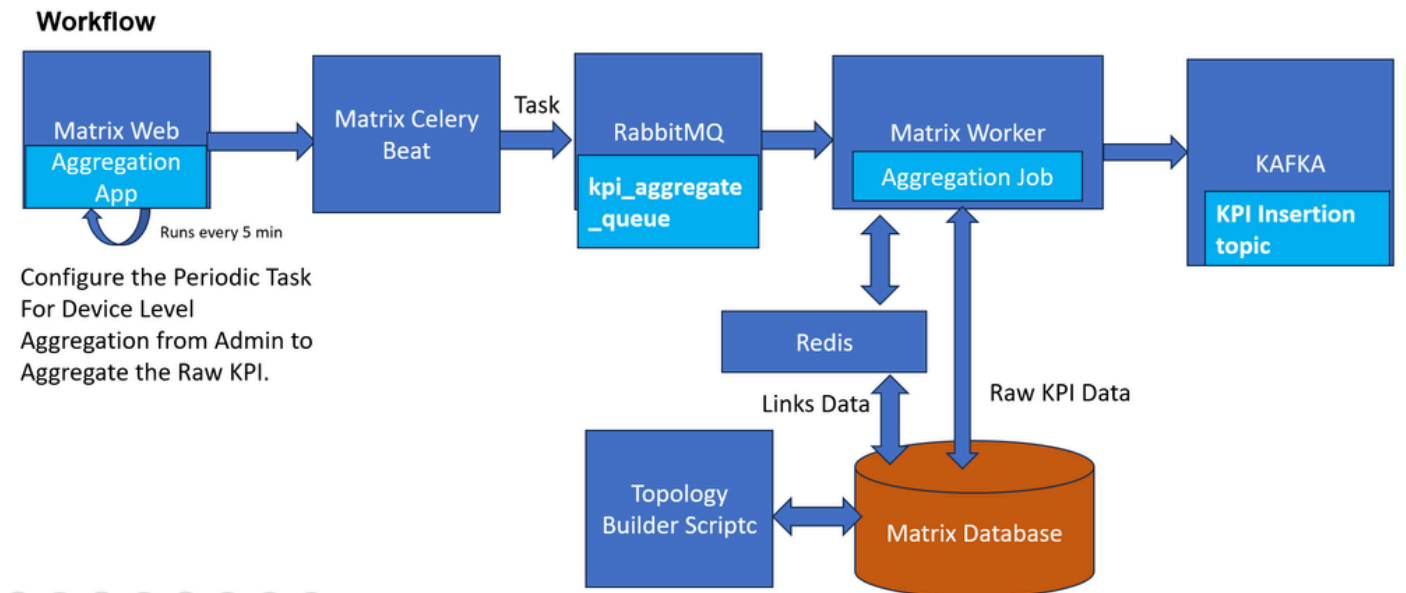
Index: <local device> \_<remote device>

Router-A \_Router-B

Node: <Local-Device>

Router-A

예를 들어, 이 경우 KPI 이름은 원시 터널 KPI 터널 사용률에 대해 "tunnel-utilization\_agg"로 생성됩니다. 모든 라우터 및 터널 조합에 대한 모든 원시 KPI 값에 대한 계산이 완료되면 Kafka 항목의 각 링크에 대해 이 데이터가 푸시됩니다. 이 항목은 처리된 KPI를 가져오는 항목과 동일해야 합니다. 이렇게 하면 이 정보는 유효한 소스에서 받은 다른 일반 KPI처럼 유지됩니다. DB 소비자는 이 항목에서 소비하고 KPI를 집계 KPI에 대한 매트릭스 데이터베이스의 KPI 결과 테이블에 유지합니다.



번들 레벨의 KPI 집계 프로세스 집계 KPI

## 임계값 초과 알림 생성

Matrix에 구성된 KPI 임계값은 85%입니다. 즉, 이 KPI의 값이 임계값을 초과하면 위기 경보가 생성되고 임계값 아래로 내려가면 지우기 경보가 생성됩니다. 이러한 알림은 Matrix Database에 저장되며, 이 솔루션의 Vitria에 전달되어 closed-loop 자동화 활용 사례를 지원합니다. KPI의 계산된 값이 임계값을 초과하면 알림이 Kafka를 통해 Vitria(VIA-AIOPS)로 전송되며, 메시지의 현재 상태는 Critical입니다. 마찬가지로, 값이 임계값에서 임계값 내로 반환되는 경우 메시지에서 현재 상태가 Clear인 상태로 Kafka를 통해 VIA-AIOPS에 알림을 보내야 합니다. 샘플 메시지가 시스템으로 전송되었으며 속성은 다음과 같습니다.

```
{
```

```

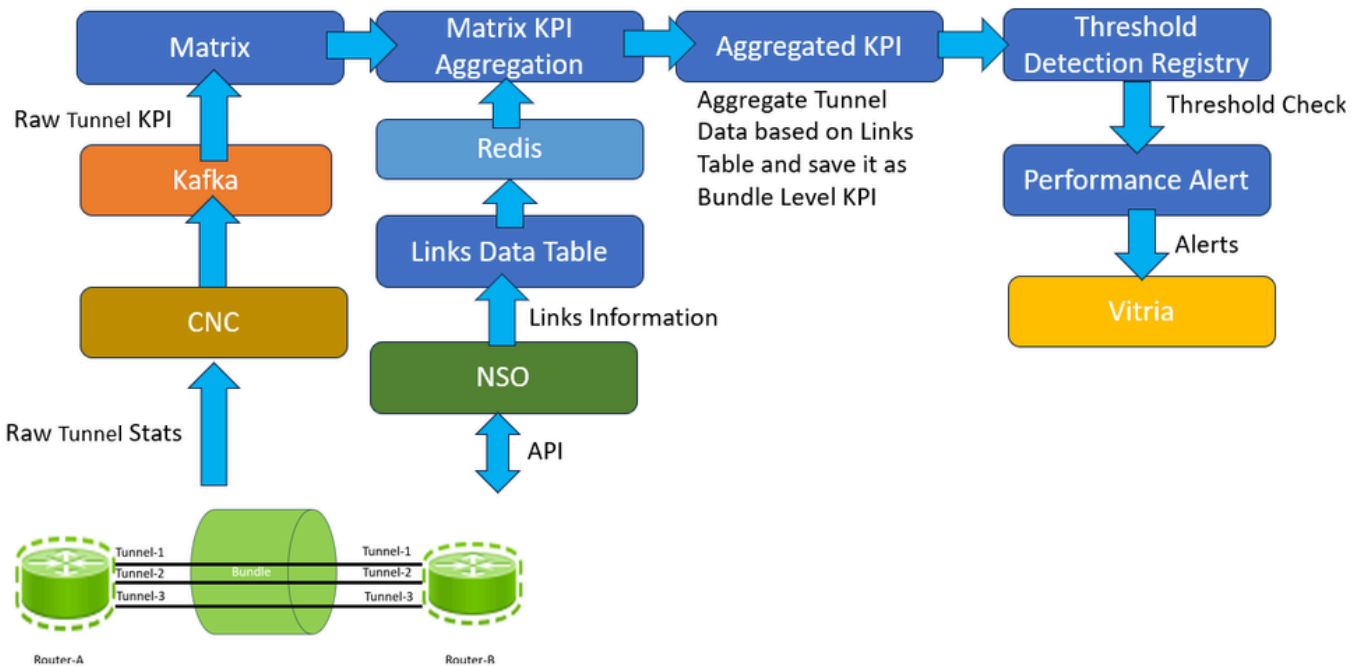
"노드": "라우터-A",
"node_type": "라우터",
"kpi": "tunnel_utilization_agg",
"kpi_description": "번들 레벨 사용률",
"스키마": "",
"index": "Router-A_Router-B",
"시간": "2023-08-09 05:45:00+00:00",
"값": "86.0",
"previous_state": "지우기",
"current_state": "CRITICAL",
"link_name": "Router-A_Router-B"
}

```

Kafka 알림 메시지 특성	값 예	목적
노드	라우터-A	네트워크 장치 이름
노드 유형	라우터	디바이스 유형
KPI	tunnel_utilization_ag	KPI 이름
kpi_설명	번들 레벨 사용률	KPI 설명
스키마	해당 없음	해당 없음
색인	라우터 A_라우터 B	<local_device>-<remote_device>
time	"2023-08-09 05:45:00+00:00"	time
가치	86.0	KPI 값

이전 상태	CLEAR(지우기)	이전 경고 상태
현재 상태	CRITICAL(심각)	현재 경고 상태
링크 이름	라우터 A_라우터 B	상관관계 특성

link\_name 속성은 인덱스 값에 있는 디바이스의 알파벳순으로 정렬된 이름입니다. 이는 VIA AIOs 레벨에서 상관관계를 얻기 위해 수행되며, 여기서 VIA AIOs는 동일한 번들 링크에서 오는 경고의 상관관계를 분석해야 합니다. 예를 들어, 동일한 link\_name을 사용하여 여러 알림이 VIA AIOs로 전송되는 경우 알림이 네트워크의 동일한 번들 링크에 속하며 링크 이름에는 디바이스 이름이 표시됩니다.



매트릭스 탐지 레지스트리를 사용한 KPI 집계 경고 생성

## 인시던트 트리거 및 자동화된 교정 워크플로

VIA AIOs는 지정된 Kafka 항목에서 KPI(핵심 성과 지표) 이상 징후 이벤트를 수집하도록 구성됩니다. Kafka 메시지를 통해 수신된 이러한 이벤트는 후속 수집을 위해 JASO Event Parser를 통해 VIA AIOs에서 처리됩니다. VIA AIOs에서는 GRE 터널과 관련된 KPI 이상 이벤트를 정확하게 식별하고, 특정 디바이스 쌍(예: 라우터 A - 라우터 B)과의 연결을 확인하고, 이상 때문에 GRE 터널 확장 자동화를 시작해야 하는지(업스케일 또는 다운스케일)를 확인해야 합니다.

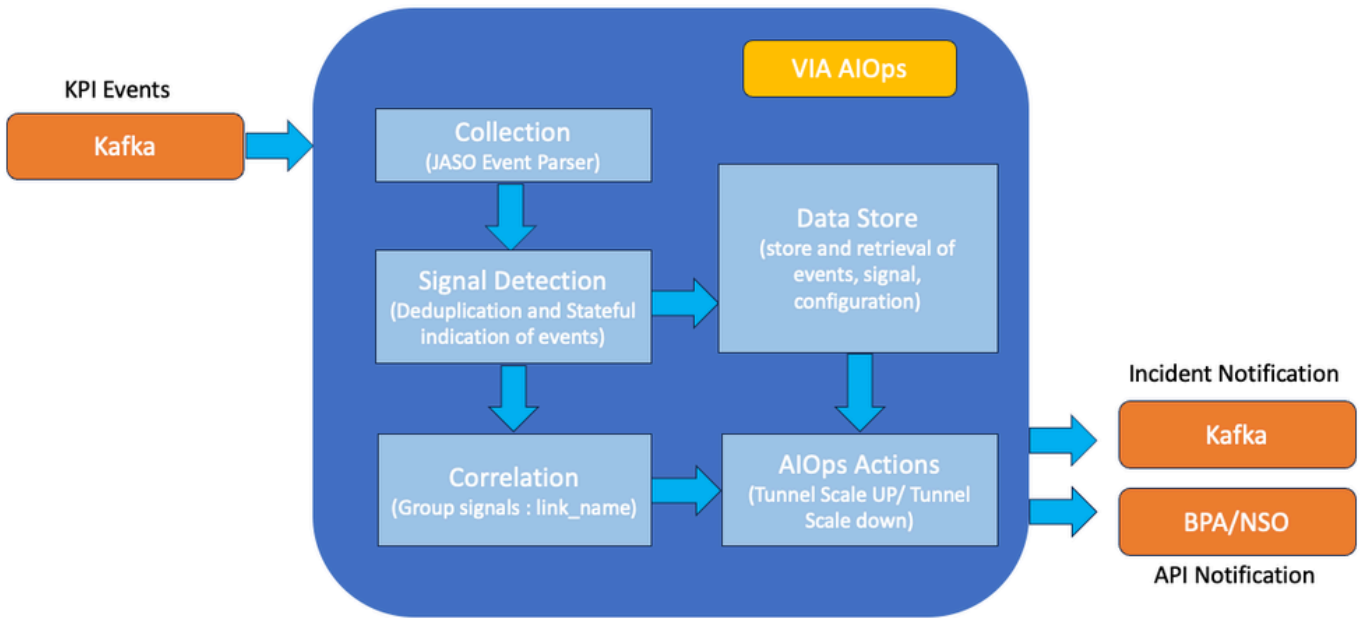
VIA AIOs 내의 JASO 이벤트 파서는 매트릭스 KPI 이상 이벤트, 즉 'host', 'kpi', 'index' 및 'value'에서 관련 차원을 추출하고 해석하도록 구성해야 합니다. 'automation\_action'이라는 추가 차원은 매트릭스 KPI 이상 이벤트 내에 있는 'value' 메트릭을 기반으로 JASO 이벤트 파서에서 동적으로 업데이트되도록 구성되어야 합니다. 이 차원은 'KPI 값' 필드를 처리하여 'GRE Tunnel Scale Up' 또는 'GRE Tunnel Scale Down' 절차를 트리거할 것인지, 특히 자동화된 응답을 제정해야 하는지 여부를 결정하는 데 핵심적인 역할을 합니다. VIA AIOs에서 신호는 이벤트의 상태의 통합을 나타냅니다.

이 상관관계 프로세스를 개선하려면 'host', 'link name', 'kpi' 및 'automation\_action' 차원과 상관관계가 있는 고유한 상태 저장 신호를 구성해야 합니다. 테이블은 신호들, 상관관계 그룹들, 및 그들 각각의 상관관계 구성들을 예시한다.

예를 들어, GRE\_KPIA\_SCALEUP으로 식별된 신호는 VIA AIOps 시스템에 의해 섹션 3에 자세히 설명된 대로 지정된 KPI 이상 메시지의 수집 후에 시작됩니다.

VIA AIOps 신호 이름	신호 상관관계 키	상관관계 그룹 규칙 이름
GRE_KPIA_SCALEUP	호스트,kpi, 링크 이름, Automated_action	GRE 터널 확장
GRE_KPIB_SCALEUP	호스트,kpi, 링크 이름, Automated_action	
GRE_KPIA_SCALEDOWN	호스트,kpi, 링크 이름, Automated_action	GRE 터널 축소
GRE_KPIB_SCALEDOWN	호스트,kpi, 링크 이름, Automated_action	

상관관계 그룹 규칙은 디바이스 A, 디바이스 B 및 각 터널 A, B, C에 대한 신호를 통합 인시던트로 쉽게 집계하도록 설계되었습니다. 이 상관관계 규칙은 디바이스 A와 디바이스 B의 특정 페어링에 대해 최대 2개의 서로 다른 인시던트가 생성되도록 합니다. 하나는 디바이스 A와 디바이스 B를 포함하는 GRE 터널 스케일 업에 대한 인시던트, 다른 하나는 동일한 디바이스 페어링에 대한 GRE 터널 스케일 다운에 대한 인시던트입니다. VIA AIOps 에이전트 프레임워크는 BPA(Business Process Automation) 및 NSO(Network Services Orchestrator)와 상호 작용할 수 있습니다.



AIOps를 통한 KPI 이벤트 상관관계 및 알림

다음은 AIOps를 통해 BPA/NSO로 전송된 GRE 터널 확장 API 알림의 예입니다.

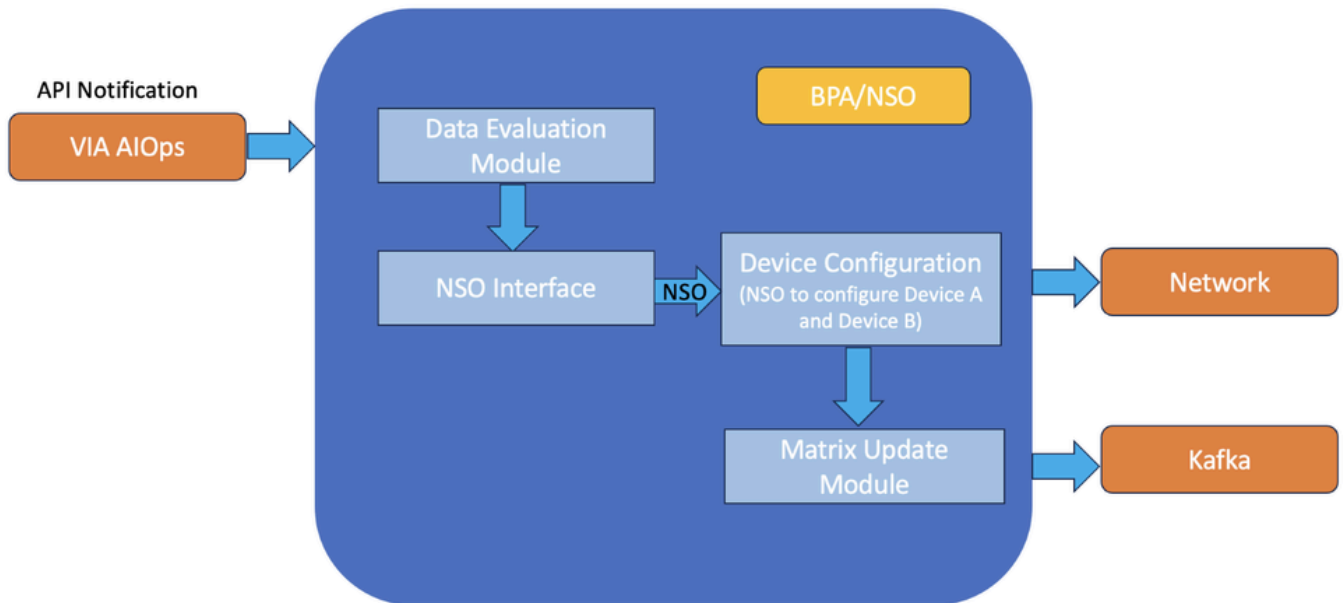
```

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

```

## 터널 추가 또는 제거 및 경고 지우기

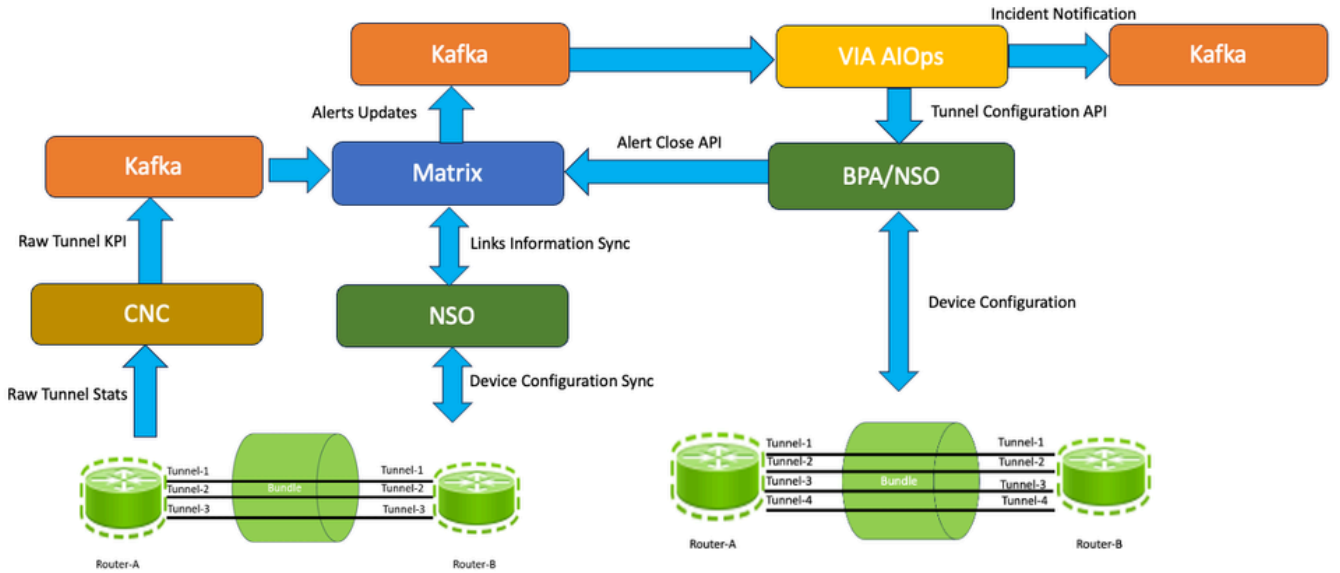
AIOps를 통해 API 호출을 받으면 Cisco BPA(Business Process Automation)는 Cisco NSO(Network Service Orchestrator)에 대한 내부 요청을 통해 필요한 확장 지침을 시작합니다. BPA는 VIA AIOps에서 제공하는 데이터 페이로드를 평가하며, 여기에는 터널 운영 세부사항, 인덱스 및 매트릭스 데이터가 포함됩니다. 인덱스 및 터널 작동 정보는 NSO와 인터페이스하는 데 사용되며, 확장 작동을 위한 매개변수를 제공합니다. 동시에 매트릭스 데이터는 매트릭스 API와 상호 작용하여 KPI 이상 이벤트를 해결하는 역할을 하는 '매트릭스 업데이트 모듈'에서 처리됩니다.



BPA-NSO를 사용한 데이터 검증 및 디바이스 컨피그레이션

스케일링 작업을 시작하기 전에 NSO를 위한 YANG 액션 모델을 개발해야 합니다. 이 모델은 NSO가 라우터 A와 라우터 B 간의 터널 수를 늘리거나 줄이기 위해 수행해야 하는 특정 작업을 정의합니다. BPA(Business Process Automation) 시스템은 NSO(Network Service Orchestrator)와 함께 '리허설'을 진행하는 방식으로 확장 작업을 시작합니다. 이는 BPA가 의도한 컨피그레이션 변경을 적용하지 않고 시뮬레이션하도록 NSO에 요청하는 작업의 초기 단계입니다. Dry Run은 YANG 작업 모델에 정의된 대로 제안된 확장 작업을 네트워크 컨피그레이션에서 오류나 충돌을 일으키지 않고 실행할 수 있도록 하는 필수 검증 단계로 작동합니다.

드라이 실행이 성공적이라 간주되어 확장 작업이 검증되었음을 나타내면 BPA는 '커밋' 단계로 진행합니다. 이때 BPA는 NSO에 라우터 A와 라우터 B 간의 GRE 터널 수를 늘리거나 줄이는 데 필요한 실제 컨피그레이션 수정을 구현하도록 지시합니다. BPA는 API 호출을 사용하여 '매트릭스 업데이트 모듈'을 매트릭스로 트리거하여 VIA AIOps와 함께 KPI 이벤트를 담습니다. Matrix에서 이 이상 징후가 닫히면 Matrix는 심각도가 "Cleared(제거됨)"인 알림을 AIOps를 통해 전송합니다. 그러면 AIOps를 통해 해당 인시던트가 더 종료됩니다. 이러한 방식으로 네트워크 레벨 교정 주기가 완료됩니다. 이러한 페루프 자동화에 활용되는, 애플리케이션 내의 데이터 흐름의 일반화된 버전이 이 이미지에 묘사된다.



GRE 터널 번들 Closed Loop 자동화를 위한 데이터 흐름

## 루프를 닫아 자동 교정의 새로운 가능성 열림

이 백서에서 설명하는 솔루션은 이 솔루션의 다양한 구성 요소에 대한 이해를 돕기 위해 네트워크 이상 현상을 기반으로 한 GRE 번들 확장의 한 가지 예를 통해 의도적으로 설명합니다. Cisco NSO, Cisco Matrix, Cisco BPA가 포함된 Cisco Technology Stack을 VIA AIOps, Kafka 및 다른 소프트웨어 스택과 원활하게 통합하여 네트워킹 문제를 자동으로 모니터링하고 해결하는 방법을 요약하여 살펴보았습니다. 이 솔루션은 통신 사업자 또는 엔터프라이즈 네트워크에서 발생하는 일반적인 문제일 수 있는 다른 모든 네트워킹 사용 사례에 대한 가능성을 열어줍니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.