クローズドループの自動化ソフトウェアスタックにより、オンデマンド帯域幅のユースケースを自動化

内容

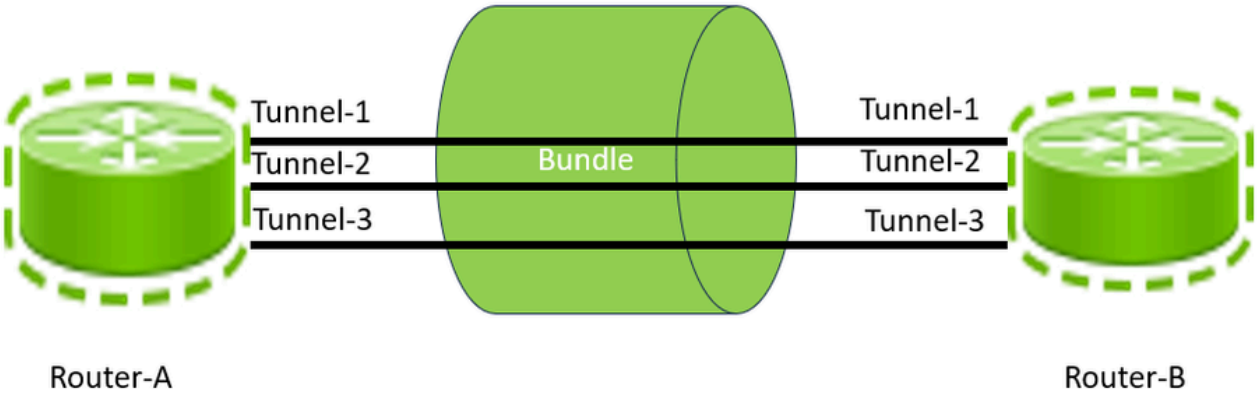
はじめに

このドキュメントでは、総称ルーティングカプセル化(GRE)トンネルの拡張を自動化するCiscoクローズドループ自動化ソリューションのコンポーネントと、その他のケースに対する適応性について説明します。

背景説明

サービスプロバイダーは、スマートなクローズドループ自動化ソリューションを使用して、ネットワーク全体のGREトンネルの帯域幅使用率を制御し、必要に応じてトンネルを拡張できるように綿密に監視したいと考えています。

GREは、カプセル化を使用して1つのプロトコルのパケットを別のプロトコルのパケットに転送するシンプルで一般的な方法を提供するトンネリングプロトコルです。このドキュメントでは、Cisco IOS® XRvプラットフォームのGREトンネルベースの例に焦点を当てていますが、他のプラットフォームにも一般化できます。 GREは、ペイロード（外部IPパケット内の宛先ネットワークに配信される必要がある内部パケット）をカプセル化します。GREトンネルは、トンネルの送信元と宛先アドレスによって識別される2つのエンドポイントを持つ仮想ポイントツーポイントリンクとして動作します。



ルータ間のGREトンネル

GREトンネルの設定には、トンネルインターフェイスの作成と、トンネルの送信元と宛先の定義が含まれます。次の図は、ルータAとルータBの間の3つのGREトンネルの設定を示しています。この設定では、Router-Aに3つのインターフェイス（Tunnel-1、Tunnel-2、Tunnel-3など）を作成し、Router-Bにも3つのインターフェイス（Tunnel-1、Tunnel-2、Tunnel-3など）を作成する必要があります。2つのサービスプロバイダールータ間に、複数のGREトンネルが存在する場合があります。各トンネルには、他のネットワーキングインターフェイスと同様に、インターフェイスのキャパシティに基づいてキャパシティが定義されています。したがって、トンネルは帯域幅に等しい最大トラフィックのみを伝送できます。トンネルの数は、多くの場合、2つのサイト（ルータ）間のトラフィック負荷と帯域幅使用率の初期予測に基づきます。ネットワークやネットワークの拡張が変更されると、この帯域幅使用率も変化すると考えられます。ネットワーク帯域幅を最適に使用するには、2台のデバイス間のすべてのトンネルで測定された帯域幅使用率に基づいて、2台のデバイス間に新しいトンネルを追加するか、余分なトンネルを削除することが重要です。

この例から、Router-AとRouter-Bの間にある3つのトンネルすべての容量の合計は、Tunnel-1、Tunnel-2、Tunnel-3の容量の合計であると言えます。これは、集約帯域幅またはGREバンドルレベルの帯域幅と呼ばれます。ここで使用する「bundle」キーワードは、ルータのペア間のトンネルを指しており、LACPおよびEtherchannelリンクバンドリングとの暗黙的な関係を意図したものではないことに注意してください。また、2つのルータ間の実際のトラフィックは、Tunnel-1、Tunnel-2、およびTunnel-3の合計トラフィックです。通常は、バンドルレベルの帯域幅使用率という概念を考案することができます。これは、2台のルータ間のすべてのトンネルの合計容量に対する、トンネルを通過する合計トラフィックの比率です。一般に、サービスプロバイダーは、2台のルータ間にトンネルを追加または削除して修復措置を講じることを望みます。トンネルを追加または削除したルータで、帯域幅が過剰に使用されていたり、十分に使用されていないことが確認された場合です。ただし、このドキュメントでは、低いしきい値は2台のルータ間のバンドルレベル使用率の20 %で、高い使用率の80 %です。

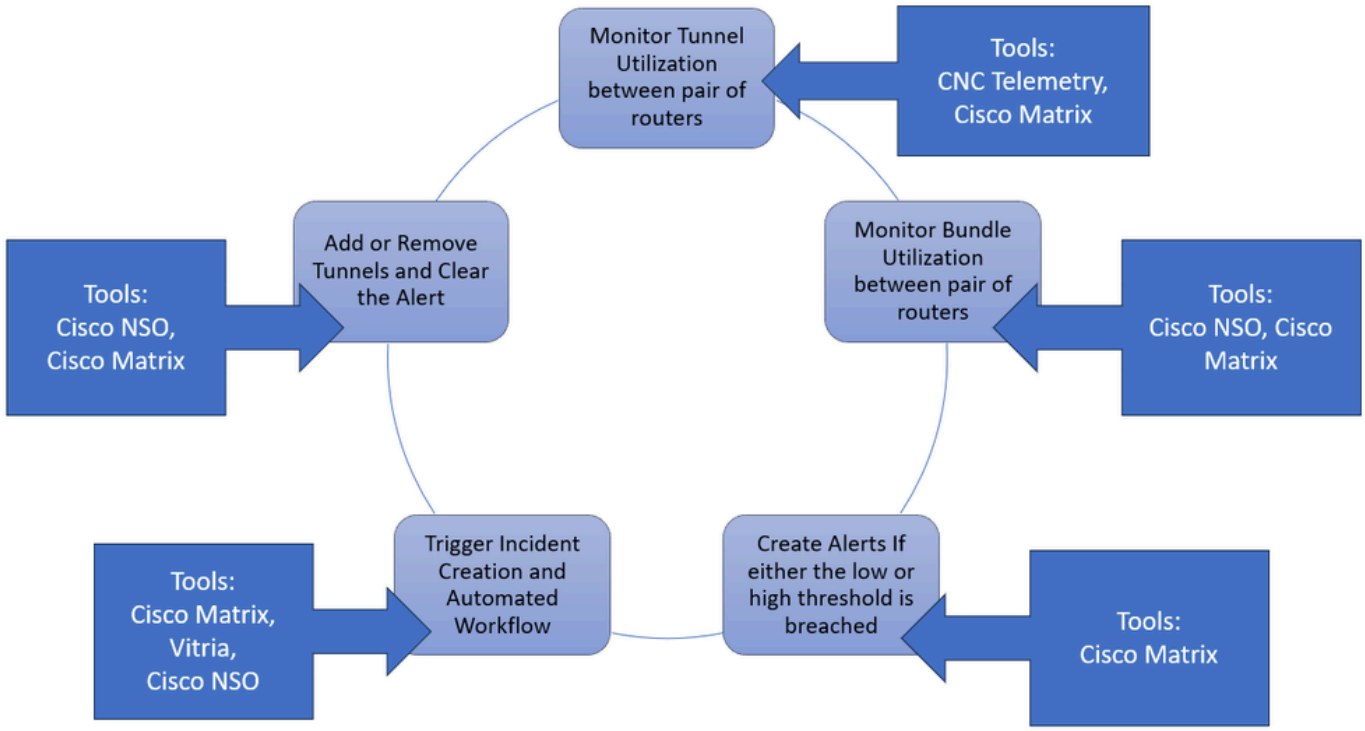
要件

1. クローズドループソリューションは、XRv9KでGREバンドルのエンドツーエンドのクローズドループ自動化を実行するために必要です。この自動化では、システムがテレメトリデータを収集し、重要業績評価指標(KPI)の形式でデータを監視し、集約を適用し、しきい値のクロスアラート(TCA)を作成し、自動修復設定を実行してアラートを閉じることができます。
2. このソリューションでは、Network Key Performance Indicator(KPI)を計算して、任意の周波数でのトンネルの未加工スループットに基づいて、各トンネルの個々のトンネル入力(Rx)およびトンネル出力(Tx)帯域幅使用率を算出できます。
3. このソリューションでは、カスタムKPIを計算して、ルータのペア間のすべてのトンネルの集約帯域幅使用率である各バンドルのトンネル入力(Rx)およびトンネル出力(Tx)帯域幅使用率を表示できます。
4. ソリューションは、定義されたバンドルレベルのしきい値を超えると、アラートを検出して作成できます。このようなアラートはモニタリングに使用できます。
5. このアラートは、アラート条件に基づいてトンネルを追加または削除するデバイスの設定をさらにトリガーできる自動ワークフローをトリガーする必要があります。
6. 最後に、システムは必要な更新を含むアラートを自動的に閉じる必要があります。

解決方法

クローズドループ自動化ソリューションには、このエンドツーエンドソリューション全体の特定の目標に取り組む複数のツールが含まれます。 この図は、最終的なアーキテクチャの構築に役立つコンポーネントとツールを示し、高レベルの役割を示しています。各コンポーネントとその用途については、以降のセクションで説明します。

シスコのクローズドループ自動化



ソリューションシスコのクローズドループ自動化ソリューション

ツール	目的
Cisco Crosswork Network Controller(CNC)	Crosswork Network Controllerは、ネットワークトポロジ、サービスインベントリ、トランスポートポリシー、サービスの状態、デバイスの状態など、幅広いユースケースをサポートする共通の統合ユーザエクスペリエンスを備えた直感的なナビゲーションを使用して、サービスとデバイスのライフサイクル全体にわたるリアルタイムの可視性を実現します。 このソリューションでは、主にデバイスの管理と、gNMI（gRPCネットワーク管理インターフェイス）またはMDTを使用したトンネルパフォーマンスデータ収集の収集のためのツールとして使用されます。 詳細：https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-controller/index.html
シスコのマトリックス	CX分析サービス（機能パック）は、マルチベンダーの単一ペインのマルチドメイン分析ソリューションであるマトリックスソリューションを使用して提供されます。 このソリューションでは、マトリックスはKafkaトピックを介してCNCから送信されたKafkaのデータを使用し、さらにトポロジ検索を使用してトンネルベースのKPIをバンドルレベルのKPIに集約し、時系列データとして保存し、Postgresデータベースに保存します。このようなデータが保存されると視覚化が可能になり、Matrixではしきい値超過アラートを使用して異常検出が行われます。これにより、ネットワークから収集したKPIのしきい値を設定できます。
カフカクラスタ	Kafkaクラスタは、さまざまなブローカーのトピックとそれぞれのパーティションで構成されるシステムです。 プロデューサは、クラスタ内のトピックに対してデータやメッセージを送信または書き込みます。コンシューマは、Kafkaクラスタからメッセージを読み取るか、消費します。 このソリューションでは、CNCはプロデューサとして機能し、ルータから収集されたテレメトリからデータを変換した後、事前定義されたKafkaトピックにJSONペイロードの形式でデータを送信します。 このソリューションでは、Matrixはコンシューマとして機能し、データを消費して処理し、データを集約し、さらに処理と異常検出を行うためにデータを保存します。
シスコNSO	Cisco Crosswork Network Services Orchestrator(NSO) NSOは、サービスプロバイダーや大企業向けに構築された自動化ツールのCrossworkポートフォリオの一部です。 このソリューションでは、NSOがすべてのトンネルとデバイスに関連する情報

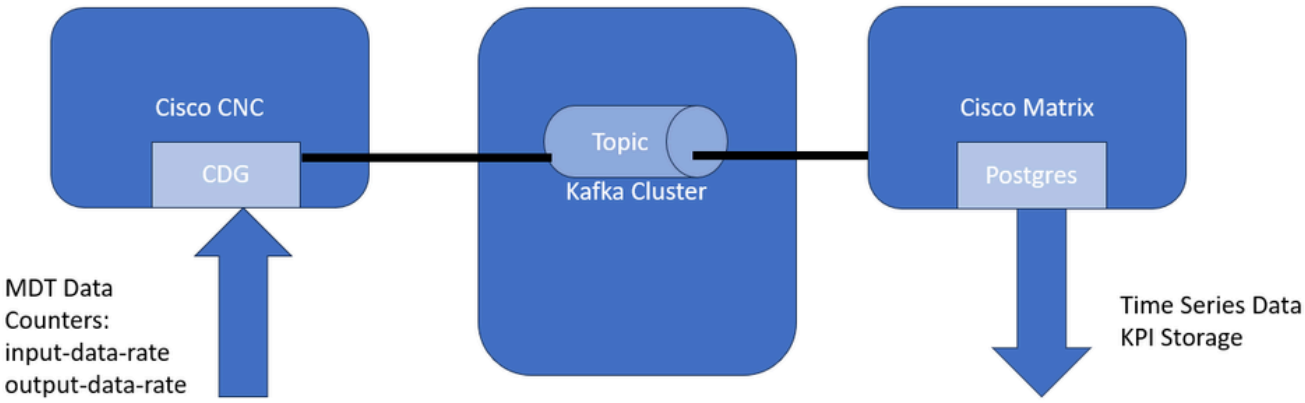
	を収集し、このソリューション用にカスタマイズされたトポロジテーブルを構築します。 また、このソリューションでは、NSOとビジネスプロセス自動化機能を使用して修復ワークフローをトリガーし、デバイスへのトンネルの追加または削除、シスコマトリックスでのアラートのクリアなどのアクションを実行します。 詳細：https://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html
AioP経由のビトリア	Vitria VIA AIOps for Cisco Network Automationは、サービスに影響を与えるイベントの迅速な修復を可能にする自動分析をすべてのテクノロジーおよびアプリケーションレイヤに提供します。 このソリューションでは、VIA AIOpsを使用して、Cisco Matrixから生成されたKPIしきい値イベントを関連付けて、インシデント、通知、およびCisco NSOへの自動アクションをトリガーし、GREトンネル数を増減します。 詳細：https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/crosswork-network-automation/solution-overview-c22-2403404.html

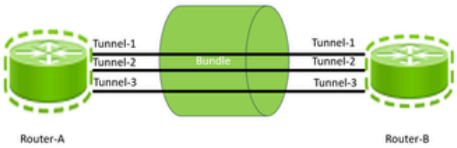
このソリューションでは、この使用例を実現するためにこれらの手順を実行します。これについては、以降のセクションで詳しく説明します。

1. ルータのペア間のトンネル使用率の監視
2. ルータのペア間のバンドル使用率の監視
3. しきい値超過アラートの作成
4. インシデントのトリガーと修復ワークフローの自動化
5. トンネルの追加または削除とアラートのクリア

ルータのペア間のトンネル使用率の監視

アプリケーションは、収集ジョブを介してデータ収集を要求します。次に、Cisco Crossworkはこれらの収集ジョブをCisco Crosswork Data Gatewayに割り当て、要求を処理します。 Crosswork Data Gatewayは、モデル駆動型テレメトリ(MDT)を使用したネットワークデバイスからのデータ収集をサポートし、デバイスからのテレメトリストリームを直接利用します（Cisco IOS XRベースのプラットフォームのみ）。Cisco Crossworkでは、データをデポジットするためにコレクションジョブで使用できる外部データのデポジット先を作成できます。Kafkaは、REST APIで作成されたコレクションジョブの新しいデータのデポジット先として追加できます。このソリューションでは、CDGはトンネルインターフェイス統計情報に関連するルータからデータを収集し、そのデータをKafta Topicに送信します。Cisco MatrixはKafka Topicからのデータを使用し、データをKPIとして処理し、プロセスフローを示す次の図に示すように時系列で保存するMatrixワーカーアプリケーションにデータを割り当てます。





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 Automationソリューション

時系列データにはKPI属性があり、マトリックスデータベースに格納されます。

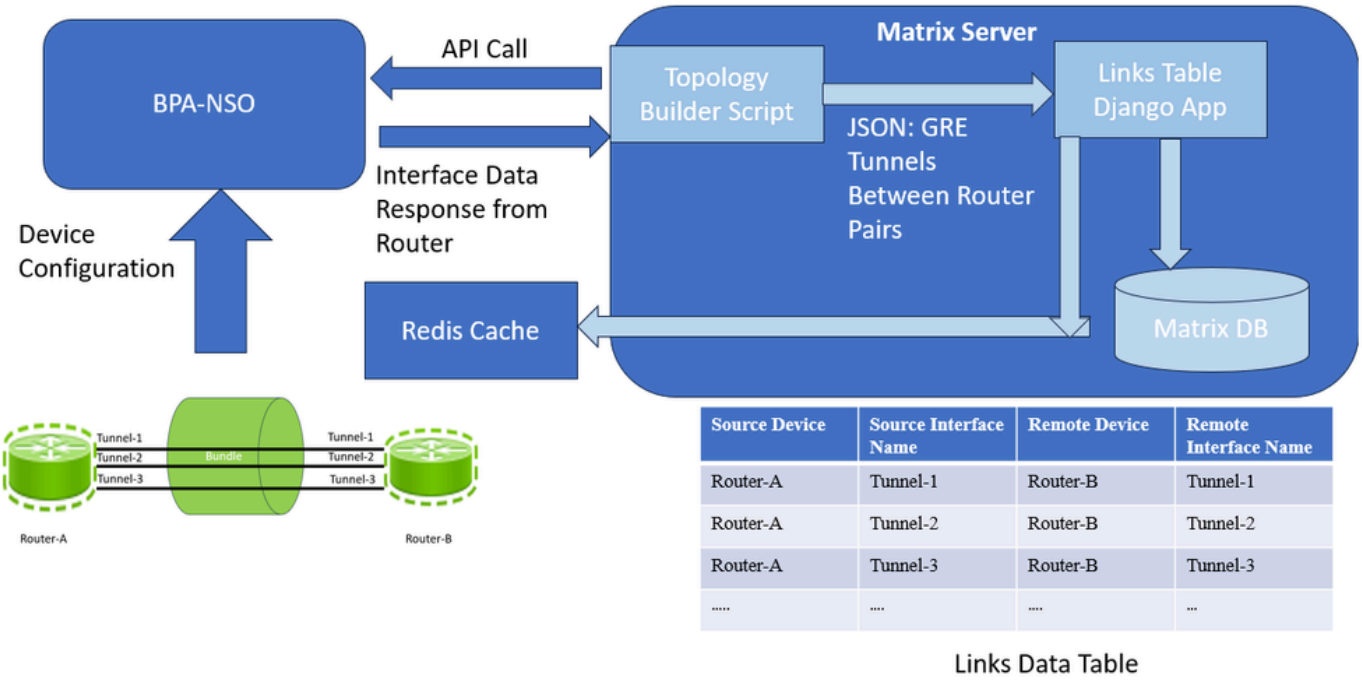
KPI属性	目的
ノード	KPIが保存されているデバイスまたはソース 例：Router-A
時間	データが収集される時間 例： 22-05-2024 10:00:00
インデックス	一意の識別子 例：Tunnel-1
値	KPIの値 – 数値
KPI	KPI名 例：tunnel-utilization

ルータのペア間のバンドル使用率の監視

前のセクションで説明した時系列データを取得すると、トンネルインターフェイスごとに収集されたトラフィック統計情報が得られます。ただし、どちらのデバイスにどの送信元トンネルインターフェイスが接続されているか、またどのデバイスがリモートインターフェイス名であるかを特定する必要があります。これはリンクIDと呼ばれ、送信元デバイス名を識別します。Source Interface Name、Remote Device Name、およびRemote Interface Name。 リンク情報とルータを正確に解釈するには、概要説明した参照例が必要です。

ソース デバイス	送信元インターフェイス名	リモートデバイス	リモートインターフェイス名
ルータ A	トンネル1	Router-B	トンネル1
ルータ A	トンネル2	Router-B	トンネル2
ルータ A	トンネル3	Router-B	トンネル3
0.....	...	...	..

このソリューションでトポロジリンクテーブルを構築するには、毎日指定された時刻にサーバで実行されるスクリプトに基づいて組み込まれたマトリックスを使用して、カスタムテーブルのリンクデータテーブルにデータを入力します。このスクリプトは、BPA-NSOへのAPIコールを行い、ルータペア間のGREバンドルのJSON出力を取得します。次に、インターフェイスデータを解析して、トポロジをJSON形式で構築します。スクリプトもこのJSON出力を取得し、毎日Links Data Tableに書き込みます。新しいデータがテーブルにロードされるたびに、このデータがRedisキャッシュに書き込まれ、データベース検索の回数が減り、効率が向上します。



データ表プロセスをリンク

したがって、同じ2つのデバイス間のすべてのリンクは、必ず同じバンドルに属していると識別されるバンドルの一部です。未加工トンネルレベルのKPIが使用可能になると、Matrix上にカスタムKPI_aggregateアプリケーションを構築し、バンドルレベルの使用率を計算してKPIとして保存する作業を実行します。

このアプリケーションでは、次の入力を行います。

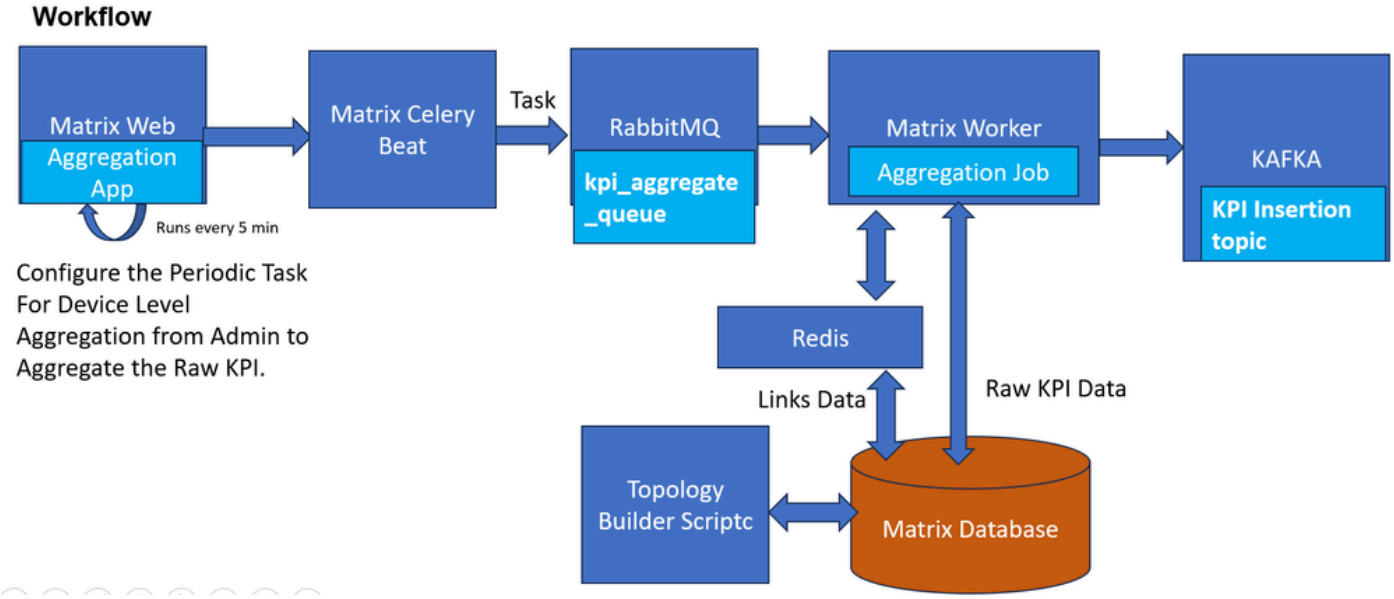
設定属性	目的
Crontab	集約定期タスクを実行する頻度
有効チェックボックス	この構成のアクティブ化/非アクティブ化
トンネルインターフェイスKPI名	集計KPIの計算に使用されるRaw KPIの名前です。 集約KPI名は、<Raw_KPI_Name>_aggとして自動的に作成されます
日付の範囲	Rawデータの頻度。

集約タスクはKPI Rawデータから入力を取得し、リンクデータベースは同じバンドルの一部を形

成するトンネルを特定し、このロジックに基づいてグループに追加します。

```
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
```

たとえば、この場合、KPI名は、未処理のトンネルKPIトンネル使用率に対して「tunnel-utilization_agg」として生成されます。すべてのルータとトンネルの組み合わせのすべてのRaw KPI値の計算が完了すると、このデータはKafkaトピックへのリンクごとにプッシュされます。このトピックは、処理されたKPIを取り込む同じトピックである必要があります。これにより、この情報は有効なソースから受信した他の通常のKPIと同じように保持されます。DBコンシューマはこのトピックから使用し、集計KPIのマトリックス・データベースのKPI結果テーブルにKPIを保持します。



バンドルレベル集計のKPI集計プロセス集計KPI

しきい値超過アラートの作成

Matrixで設定されているKPIしきい値は85%です。このKPIの値がしきい値を超えるとクリティカルなアラートが生成され、しきい値を下回るとクリアなアラートが生成されます。これらのアラートはマトリックスデータベースに保存され、クローズドループ自動化のユースケースのためにこのソリューションでVitriaにも転送されます。KPIの計算値がしきい値を超えると、メッセージ内の現在の状態をCriticalとして、Kafka経由でアラートがVitria(VIA-AIOP)に送信されます。同様

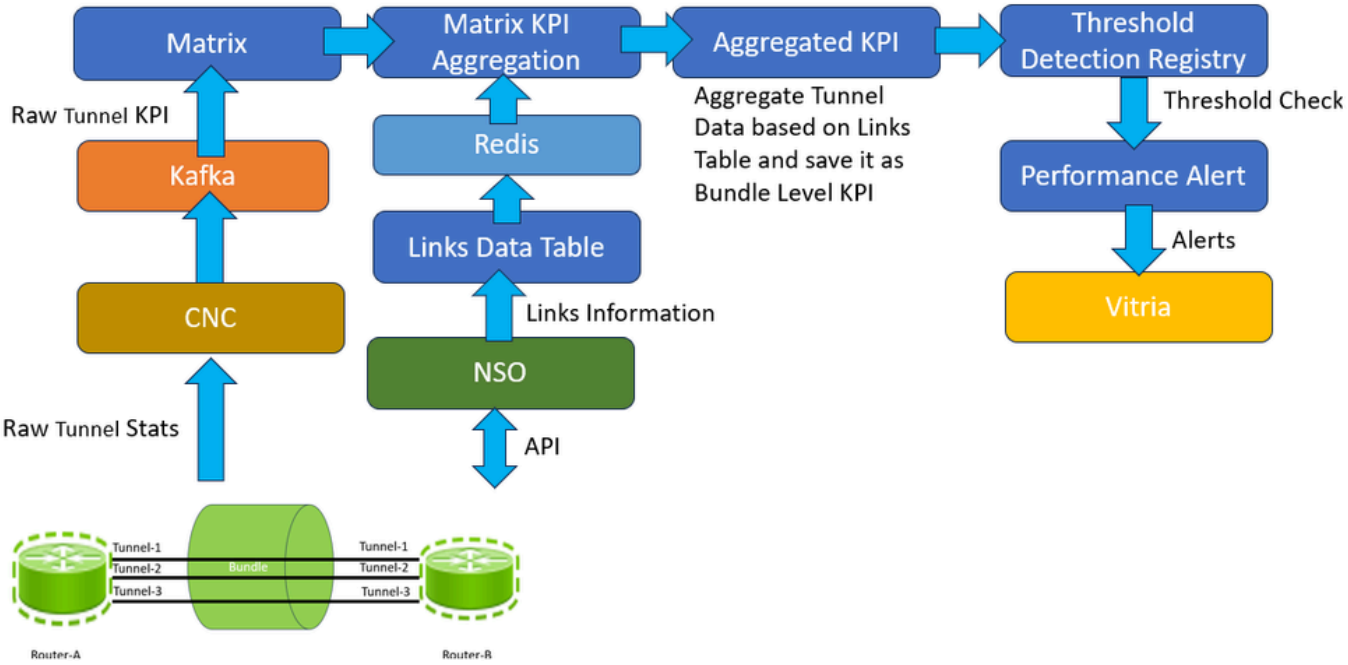
に、値がクリティカル値からしきい値内に戻った場合、メッセージ内の現在の状態をClearとして、Kafka経由でVIA-AIOPにアラートを送信する必要があります。サンプルメッセージがシステムに送信されました。属性は次のとおりです。


```
{
   "ノード": "Router-A",
   "node_type": "ルータ",
   "kpi": "tunnel_utilization_agg",
   "kpi_description": "バンドルレベル使用率",
   "スキーマ": "",
   "index": "Router-A_Router-B",
   "time": "2023-08-09 05:45:00+00:00",
   "値": "86.0",
   "previous_state": "CLEAR",
   "current_state": "CRITICAL",
   「link_name」:「Router-A_Router-B」
}
```


Kafkaアラートメッセージ属性	値の例	目的
ノード	ルータ A	ネットワークデバイス名
ノードタイプ	ルータ	デバイスタイプ
KPI	tunnel_utilization_aggコマンド	KPI名
kpi_description	バンドルレベルの使用率	KPIの説明
スキーマ	適用外	適用外
index	ルータA_ルータB	<local_device>-<remote_device>

時間	"2023-08-09 05:45:00+00:00"	時間
の値を入力します。	86.0	KPI値
前の状態	CLEAR	アラートの前の状態
current_state（現在の状態）	CRITICAL	アラートの現在の状態
リンク名	ルータA_ルータB	相関属性

link_name属性は、インデックス値に存在するデバイスのアルファベット順にソートされた名前です。これは、VIA AIOpが同じバンドルリンクからのアラートを関連付ける必要があるVIA AIOPレベルで関連付けを実現するために行われます。たとえば、同じlink_nameを持つ複数のアラートがVIA AIOPに着信する場合、そのアラートはネットワーク内の同じバンドルリンクに属し、リンク名にはデバイス名で示されます。



マトリックス検出レジストリを使用したKPI集計アラートの生成

インシデントのトリガーと修復ワークフローの自動化

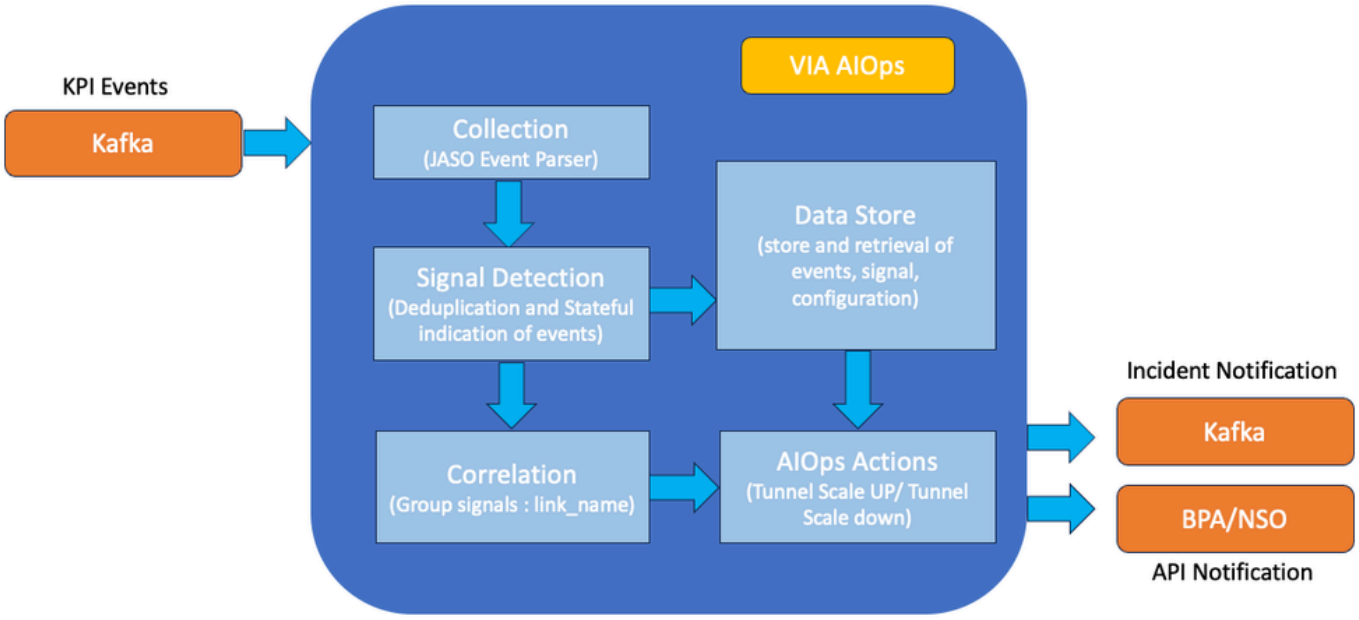
VIA AIOpsは、指定されたKafkaトピックから主要業績評価指標(KPI)の異常イベントを取り込むように設定されます。Kafkaメッセージを通じて受信されたこれらのイベントは、JASOイベントパーサーを通じてVIA AIOpsによって処理され、その後の取り込みに使用されます。VIA AIOpでは、GREトンネルに関連するKPI異常イベントを正確に特定し、特定のデバイスペア（ルータAとルータBなど）との関連付けを判別し、異常によってGREトンネルスケーリングの自動化（アップスケールまたはダウンスケール）の開始が必要かどうかを確認することが重要です。

VIA AIOps内のJASOイベントパーサーは、Matrix KPI異常イベントから関連するディメンション(「host」、「kpi」、「index」、「value」)を抽出して解釈するように設定する必要があります。マトリックスKPI異常イベント内に存在する「値」メトリックに基づいて、JASOイベントパーサーによって動的に更新されるように、「automation_action」と呼ばれる追加のディメンションを構成する必要があります。この側面は、自動対応を実施する必要があるかどうかを判断する上で重要です。具体的には、「KPI値」フィールドの処理によって「GREトンネルスケールアップ」または「GREトンネルスケールダウン」手順をトリガーするかどうかです。VIA AIOpsでは、信号はイベントの状態の統合を表します。この相関プロセスを強化するには、「host」、「link name」、「kpi」、「automation_action」の各次元に相関する個別のステートフル信号を設定する必要があります。この表は、信号、相関グループ、およびそれぞれの相関設定を例示しています。

たとえば、GRE_KPIA_SCALEUPとして識別される信号は、セクション3で説明しているように、指定されたKPI異常メッセージの取り込み後にVIA AIOpsシステムによって開始されます。

VIA AIOpsシグナル名	信号相関キー	相関グループ規則名
GRE_KPIA_スケールアップ	ホスト、kpi、リンク名、Automated_action	GREトンネルスケールアップ
GRE_KPIB_スケールアップ	ホスト、kpi、リンク名、Automated_action	
GRE_KPIA_SCALEDOWN	ホスト、kpi、リンク名、Automated_action	GREトンネルスケールダウン
GRE_KPIB_SCALEDOWN	ホスト、kpi、リンク名、Automated_action	

相関グループルールは、デバイスA、デバイスB、およびそれぞれのトンネルA、B、Cに関する信号を統合インシデントに集約することを容易にするように設計されています。この相関ルールにより、デバイスAとデバイスBの特定のペアに対して、最大2つの個別のインシデント（デバイスAとデバイスBを含むGREトンネルスケールアップのインシデントと、同じデバイスペアに対するGREトンネルスケールダウンのインシデント）が生成されます。VIA AIOpsエージェントフレームワークは、Business Process Automation(BPA)およびNetwork Services Orchestrator(NSO)とのインターフェイス機能を備えています。



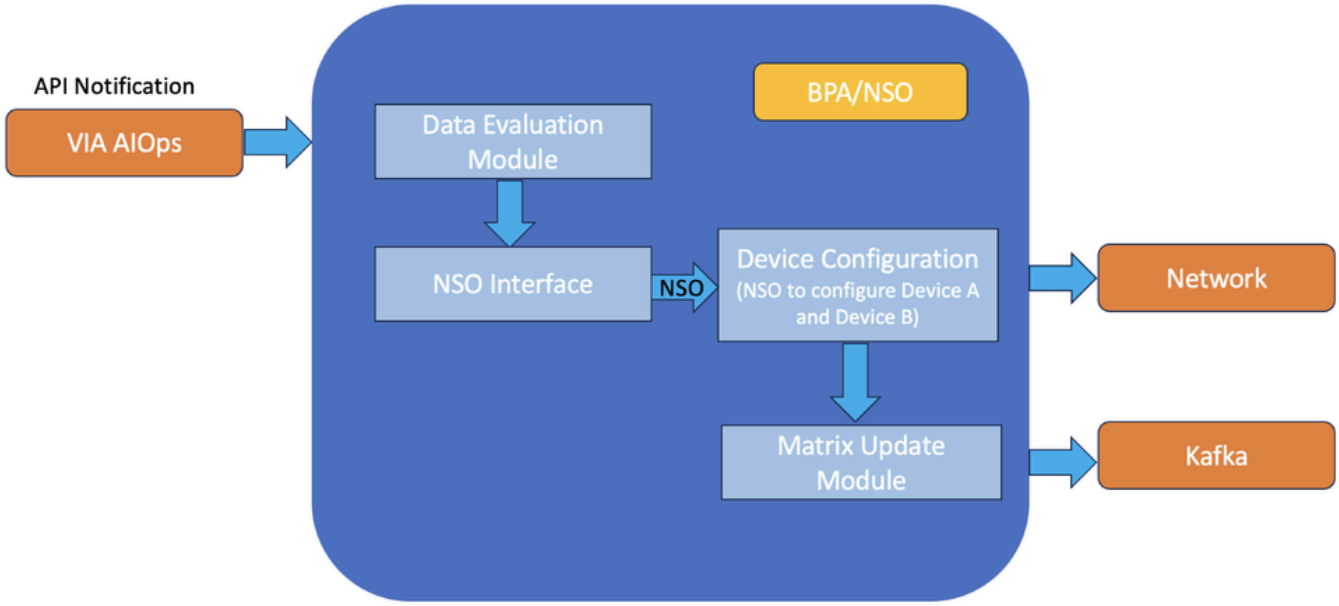
AIOpsを使用したKPIイベントの関連付けと通知

AIOps経由でBPA/NSOに送信されるGREトンネルスケールアップAPI通知の例を次に示します。

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

トンネルの追加または削除とアラートのクリア

AIOps経由でAPIコールを受信すると、Cisco Business Process Automation(BPA)は、Cisco Network Service Orchestrator(NSO)への内部要求を通じて、必要なスケーリングディレクティブを開始します。BPAは、トンネル動作の詳細、インデックス、マトリクスデータを含む、VIA AIOpsによって提供されるデータペイロードを評価します。 インデックスとトンネルの動作情報は、NSOとのインターフェイスに使用され、スケーリング動作のパラメータを提供します。同時に、マトリックスデータは「マトリックス更新モジュール」によって処理されます。このモジュールは、マトリックスAPIとインターフェイスすることでKPI異常イベントを解決します。

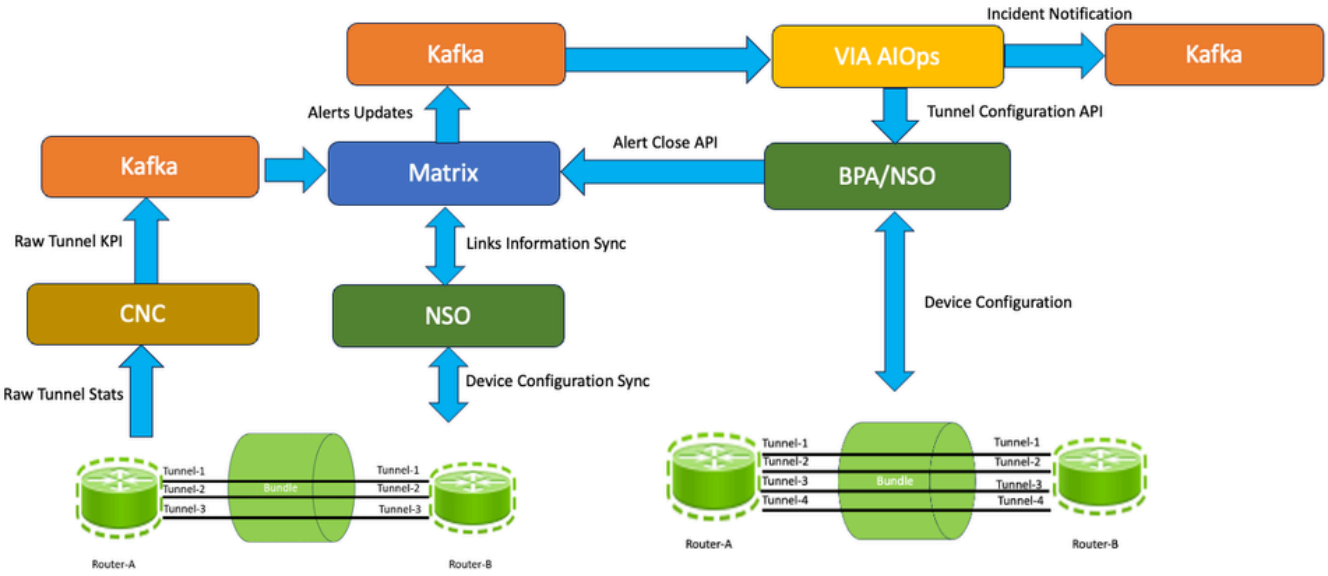


BPA-NSOを使用したデータ検証およびデバイス設定

拡張操作を開始する前に、NSOのYANGアクションモデルを開発する必要があります。このモデルは、ルータAとルータBの間のトンネル数を増減するためにNSOが実行する必要がある特定のアクションを定義します。Business Process Automation(BPA)システムは、Network Service Orchestrator(NSO)と連携して「予行演習」を実行することで、スケーリング操作を開始します。これは、BPAがNSOに対して、意図した設定変更を適用せずにシミュレートするよう要求する、動作の初期フェーズです。YANGアクションモデルで定義されたスケーリングアクションが、ネットワーク構成にエラーや競合を発生させることなく実行できることを確認する重要な検証ステップとして、ドライ作動が機能します。

ドライランが成功し、スケーリングアクションが検証されたことを示す場合、BPAは「コミット」段階に進みます。この時点で、BPAはNSOに対し、ルータAとルータBの間のGREトンネル数を増減するために必要な実際の設定変更を実装するよう指示します。BPAは、APIコールを使用してMatrixに対する「Matrix Update Module」をトリガーし、VIA AIOpsと並行してKPIイベントを閉じます。この異常がMatrixでクローズされると、Matrixから重大度が「Cleared」のアラートがVIA AIOpsに送信され、インシデントが終了します。このようにして、ネットワークレベルの修復サイクルが完了します。この図では、このクローズドループ自動化で使用される、アプリケ

ーション内のデータフローの汎用バージョンが示されています。



GREトンネルバンドルのクローズドループ自動化のデータフロー

ループを閉じて自動修復の新たな可能性を切り開く

この文書で説明するソリューションは、ネットワークの異常に基づくGREバンドルの拡張の一例を使用して慎重に説明されており、このソリューションのさまざまな構成要素との関連付けに役立ちます。Cisco NSO、Cisco Matrix、およびCisco BPAを含むCisco Technology Stackが、VIA AIOps、Kafka、およびその他のソフトウェアスタックなどのコンポーネントとシームレスに統合し、ネットワークの問題を自動的に監視して修復する方法について、まとめています。このソリューションは、サービスプロバイダーまたはエンタープライズネットワークで発生する一般的な問題である可能性がある、他のすべてのネットワーキングのユースケースに可能性を開きます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。