Cisco Crosswork Network Controller 4.1 ソリューション ワークフロー ガイド

目次

ソリューションの概要

説明

ネットワークトラフィックの急増と、ネットワークオペレーションを効率的に実行するというプレッシャーから、ネットワークオペレータは大きな課題に直面しています。ネットワーク使用率を最適化する迅速なインテントベースのサービスの提供と、帯域幅と遅延の需要変動にリアルタイムで対応できる機能が、成功に不可欠です。ソフトウェア定義型ネットワーク（SDN）への移行と運用タスクの自動化は、効率性と競争力を高めるのに最適な方法です。

Cisco Crosswork Network Controller は、IP トランスポートネットワークを展開および運用するためのターンキーネットワーク自動化ソリューションです。サービスの俊敏性、コスト効率、最適化の向上を実現し、お客様に届くまでの時間を迅速化して運用コストを削減します。このソリューションは、インテントベースのネットワーク自動化を組み合わせて、サービスのオーケストレーションと実現、ネットワークの最適化、サービスパスの計算、デバイスの展開と管理、および異常検出と自動修復のための重要な機能を提供します。Cisco Crosswork Network Controller は、テレメトリ収集と自動応答を使用して、高度なスキルを持つ専任のスタッフがネットワークを運用している場合でも複製することがほぼ不可能なネットワーク最適化機能を提供します。

この完全に統合されたソリューションは、共通の Crosswork インフラストラクチャにインストールされた複数の Crosswork コンポーネントの機能と、Cisco® Network Services Orchestrator（NSO）および Cisco Segment Routing Path Computation Element（SR-PCE）の業界をリードする機能を組み合わせています。統合されたユーザーインターフェイスが、ネットワークトポロジとサービス、プロビジョニング、モニターリング、および最適化をリアルタイムで視覚化するための単一のペインを提供します。

今回のリリースでの変更点

このリリースの Cisco Crosswork Network Controller は、次の新機能をサポートしています。

- **「ブラウンフィールド」サービスのサポート：**Cisco Customer Experience（CX）スペシャリストの支援により、Cisco Crosswork Network Controller のサービス拡張フレームワークと API を使用して、カスタムモデルに基づいており、Cisco NSO に導入されている、既存の（「ブラウンフィールド」とも呼ばれる）サービスを視覚化できます。
- **Flex-Algo**：Crosswork Network Controller は、各デバイスが参加するフレキシブルアルゴリズムで指定された制約に従って、ネットワーク上の IGP 最短パスをカスタマイズおよび計算するためのセグメントルーティング フレキシブル アルゴリズム（Flex-Algo）の使用をサポートするようになりました。
- **SRv6**：Crosswork Network Controller は、SRv6 を介した L2VPN サービス（L2VPN EVPN VPWS）をサポートするようになりました。
- **EVPN を使用したマルチポイント VPLS**：Cisco Crosswork Network Controller では、L2VPN EVPN VPLS とサービストポロジ（ELAN、ETREE、および Custom）を追加することで、L2VPN EVPN VPWS のサポートが拡張されました。
  - **ELAN any-to-any**：すべてのサイトが相互に通信するフルメッシュトポロジ。すべてのノードに同じ RT が割り当てられます。
  - **ETREE hub-spoke**：ルートターゲットは、スポークがハブと通信できる一方で、相互には通信できない方法で割り当てられます。**node-role** が特定のサイトに対して定義されている場合、スポークが定義されます。
  - Custom：**ユーザーが各サイトの RT 値を手動で定義します。**

- **Tree-SID の可視化：**Tree-SID は、セグメント ルーティング トランスポート ネットワークにマルチキャストツリーを導入するために使用されるテクノロジーです。Cisco Crosswork Network Controller を使用すると、そのようなツリーが可視化されて UI に表示されます。
- **EMS サービスのサポート**：パケットネットワークのサービス主導ワークフローを有効にするために、Element Management System（EMS）サービスが Crosswork Network Controller Advantage パックにバンドルされています。EMS 機能には、インベントリ、障害、およびソフトウェアイメージ管理（SWIM）が含まれます。
  - インベントリサービスにより、詳細なインベントリ収集と Cisco Crosswork のデバイスライフサイクル管理（DLM）が統合されます。これにより、既存のデバイス オンボーディング ワークフローが強化され、デバイスに関する分析情報がより多く収集されます。ユーザーが Crosswork Data Gateway にデバイスを手動で接続する場合、組み込みのデバイスパッケージによって詳細なインベントリ収集が可能になります。コレクションはデータベースに保持され、インベントリ API を使用してモニターされます。
  - 障害サービスは、アラーム管理に関連付けられます。これにより、トポロジ可視化サービスのアラームのサブスクリプション、要求、取得、および自動クリアの API サポートが提供されます。障害サービスでは、障害 API を使用したモニタリングによって、デバイスとリンクのアラームステータスを表示することで、既存のトポロジ表示が改善されます。
  - SWIM は Crosswork Change Automation と統合され、SWIM API で管理されます。これにより、オペレータは、ソフトウェアイメージを表示、インポート、および削除でき、またネットワーク内のデバイスにソフトウェアイメージをプッシュできます。SWIM によって、コンプライアンスが改善され、アップグレードが促進され、ネットワークエンジニアのエクスペリエンスが向上します。
- **構成可能サービスポイント：**構成可能サービスポイント機能を使用すると、ユーザーはサービスポイントのリストを定義し、プロビジョニング UI のサービス プロビジョニング ツリーに表示できます。
- **Service Health：**Service Health モニタリングは、基本モニタリングと詳細モニタリングの両方で使用できます。必要に応じて適切なモニタリングオプションを選択する方法については、「**基本および詳細モニタリングルール**」セクションを参照してください。基本モニタリングと詳細モニタリングで、合計最大 52,000 のサービスをモニターできます。Service Health の詳細については、「**Solution Components and Integrated Architecture」セクションの「Cisco Service Health」を参照してください。**

  注： Service Health は、限定提供で使用できます。詳細については、アカウントチームにお問い合わせください。

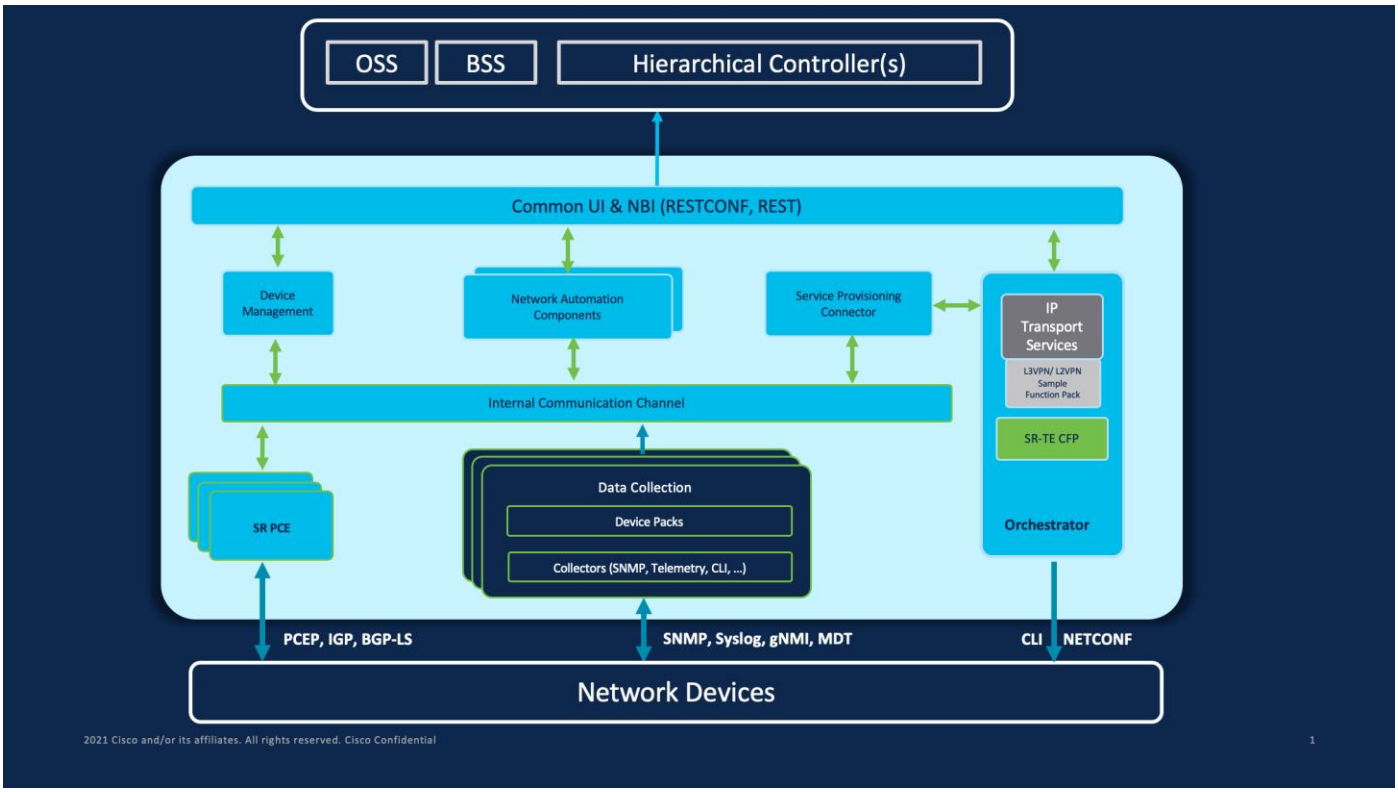
  - サービスヘルスモニタリングの履歴データ容量を拡張するために、内部ストレージと併せて外部ストレージがサポートされます。
  - サービスヘルス収集ジョブの管理オプションによって、より多くの数のジョブがサポートされるパラメータ化されたジョブ（テンプレートベースの収集ジョブ）を表示する機能が提供され、CLI 収集ジョブを表示する機能が追加されます。これは、パラメータ化されたジョブを使用して個々のデバイスの詳細を調べることにより、収集ジョブの問題をトラブルシューティングする場合に役立ちます。デバイスは、それらが GMNI、SNMP、または CLI ベースのジョブであるかどうかを判断するために、そのコンテキスト ID（プロトコル）によって識別されます。

サポートされる使用例

- **オーケストレーションされたサービスプロビジョニング：**UI または API を使用して、SLA を定義、準拠、および維持するためのアンダーレイ トランスポート ポリシーを使用したレイヤ 2 VPN（L2VPN）およびレイヤ 3 VPN（L3VPN）サービスのプロビジョニング。セグメント ルーティング フレキシブル アルゴリズム（Flex-Algo）のプロビジョニングと可視化を使用して、指定された制約に従ってネットワーク上の IGP 最短パスをカスタマイズおよび計算します。
- **リアルタイムのネットワークと帯域幅の最適化：**インテントベースのクローズドループ自動化、輻輳緩和、およびセグメントルーティングと RSVP-TE に基づく動的帯域幅管理。リンクの使用率しきい値を設定し、しきい値を超えたときに戦術的な代替パスを計算することによる、帯域幅リソース使用率の最適化。
- **ローカル輻輳管理：**ローカル輻輳緩和（LCM）は、標準プロトコルを使用して、周囲のインターフェイス内でローカライズされた脅威緩和のための推奨事項を提供します。データはリアルタイムで収集され、輻輳が検出されると、解決策が提案されます。LCM には、ネットワーク内での変更を制御する能力がオペレータの手中にあることを保証する「Human-in-the-Loop（人間がループ内に介在する）」の側面があります。
- **ネットワークとサービスのトポロジとインベントリの可視化：**デバイスとサービスインベントリを可視化し、デバイス、リンク、およびトランスポートまたは VPN サービスとそれらのヘルスステータスを、論理コンテキストまたは地理的コンテキストで可視化します。
- **パフォーマンスベースのクローズドループ自動化：**Key Performance Indicator（KPI）のしきい値を超過した場合に、KPI のカスタマイズと事前定義された修復タスクのモニターリングを可能にすることで、ネットワークの問題を自動的に検出して修復します。この使用例では、Cisco Crosswork Health Insights および Cisco Crosswork Change Automation をインストールする必要があります。
- **ネットワーク メンテナンス タスクの計画、スケジューリング、および自動化：**（WAE Design を使用して）タスクの潜在的な影響を評価した後の、メンテナンスタスクの適切なメンテナンスウィンドウのスケジューリング。プレイブックを使用したメンテナンスタスク（スループットチェック、ソフトウェアアップグレード、SMU インストールなど）の実行の自動化。この使用例では、Cisco Crosswork Health Insights および Change Automation をインストールする必要があります。
- **セキュアなゼロタッチオンボーディングとデバイスのプロビジョニング：**新しい IOS-XR デバイスをオンボーディングし、デイゼロ設定を自動的にプロビジョニングすることで、新しいハードウェアをより低い運用コストで迅速に導入できます。この使用例では、Cisco Crosswork Zero Touch Provisioning をインストールする必要があります。
- **ネイティブ SR パスの可視化：**送信元と宛先間の実際のパスを取得するために traceroute SR-MPLS multipath コマンドを使用してネイティブパスを可視化するには、パスクエリを使用します。Cisco Crosswork Network Controller では、送信元デバイスで traceroute コマンドが宛先 TE ルータ ID に対して実行され、パスの取得を支援します。
- **セグメント ルーテッド ネットワークでの Tree-SID を使用したマルチキャストツリーの検出、分析、および可視化：**ネットワーク内で Tree-SID を使用して、事前にプロビジョニングされたセグメントルーティングパス計算要素（SR-PCE）作成のマルチキャストツリーを可視化することは、マルチキャストプロトコルを使用してトラフィックを複製し、そのトラフィックをネットワーク内のさまざまなポイントに送信する必要があるビデオブロードキャストおよびストリーミングサービスのプロバイダーにとって重要です。Cisco Crosswork Network Controller を使用すると、事前にプロビジョニングされたツリーセグメント識別子（Tree-SID）SR パスを簡単かつ迅速に可視化できます。

ソリューション コンポーネントと統合アーキテクチャ

次の図は、ソリューションの複数のコンポーネントが単一のペイン内で連携し、サポートされている主要な使用例を実行する方法の概要を示しています。



Cisco Crosswork Network Controller 4.1 ソリューションは、次のコンポーネントで構成されています。

注： Crosswork Zero Touch Provisioning、Crosswork Health Insights、Crosswork Network Change Automation、および Service Health はオプションのアドオンコンポーネントです。

-
- Cisco Crosswork アクティブトポロジ
- Cisco Crosswork Optimization Engine
- Cisco Crosswork Data Gateway（CDG）
- Crosswork Common UI および API
- Crosswork Infrastructure および Shared Services
- Cisco Crosswork Health Insights および Cisco Crosswork Change Automation
- Cisco Crosswork Zero-Touch Provisioning（ZTP）
- Cisco Network Services Orchestrator（NSO）
- Cisco セグメントルーティングパス計算要素（SR-PCE）
- Cisco Service Health

Cisco Crosswork アクティブトポロジ

Cisco Crosswork Active Topology の論理マップおよび地理的マップは、物理および論理ネットワークトポロジ、サービスインベントリ、SR-TE ポリシー、および RSVP-TE トンネルをリアルタイムで可視化し、すべてを単独のペイン内に表示します。これにより、オペレータはデバイス、サービス、およびポリシーのステータスと健全性を一目で確認できます。サービスとトランスポートポリシーは、トポロジマップのコンテキスト内でオーバーレイとしてエンドツーエンドの可視化を実現します。Cisco Crosswork Active Topology にはデバイスのグループ化機能が用意されているため、オペレータは自分が担当するデバイス、サービス、ロケーションを正確にモニターリングするようにマップを設定できます。さらに、オペレータはカスタムビューを保存して、継続的に使用しているビューや機能にすばやく簡単にアクセスできます。

Cisco Crosswork Optimization Engine

Cisco Crosswork Optimization Engine は、リアルタイムのネットワーク最適化を提供して、オペレータがネットワーク容量の使用率を効果的に最大化し、サービス速度を高められるようにします。BGP-LS やパス計算要素通信プロトコル（PCEP）などのリアルタイムプロトコル、SR-PCE および Crosswork Optimization Engine を活用することで、ネットワーク状態のクローズドループ追跡を可能にし、自己修復ネットワークをサポートするようにネットワーク状態の変化に迅速に対応します。

Cisco Crosswork Data Gateway（CDG）

Cisco Crosswork Data Gateway は、マルチベンダーデバイスからネットワークデータを収集するためのセキュアな共通の収集プラットフォームです。これは、MDT、SNMP、CLI、標準ベースの gNMI（ダイヤルイン）、および syslog を含む複数のデータ収集プロトコルをサポートするネットワークデバイスの近くに展開される、オンプレミスのアプリケーションです。サポートされているプロトコルのいずれかで配信できるデータであれば、あらゆるタイプのデータを Crosswork Data Gateway で収集できます。これにより、増え続ける一連の使用例とカスタマイズをサポートできます。

規模の課題に対処するために、Cisco Crosswork Data Gateway は多数の VM として実装され、分散アーキテクチャを考慮して設計されています。軽量な VM それぞれがネットワーク全体のサブセットを管理し、ネットワークの成長に合わせて VM を水平方向に追加して、コンピューティングリソースに対する新しい要求に対応できます。また、オペレータのニーズに基づいた柔軟な冗長構成もサポートします。初期設定後、Cisco Crosswork Network Controller は、複数の Cisco Crosswork Data Gateway の VM 間で自動的に収集をオーケストレーションします。新しい収集ジョブ（Cisco Crosswork Network Controller によって構築されたもの以外）を追加して、ネットワークから追加情報を収集する方法を示す API および設定の例をご用意しています。収集されたデータは、承認された宛先にパブリッシュできます。サポートされる宛先は、Kafka および gRPC メッセージングバスです。

Crosswork Common UI および API

Cisco Crosswork Network Controller のすべての機能は、単一の共通グラフィカル ユーザー インターフェイスで提供されます。この共通 UI は、共通のインベントリ、ネットワークトポロジとサービスの可視化、サービスとトランスポートのプロビジョニング、システム管理および管理機能など、すべての Crosswork Network Controller のコンポーネントの機能を統合します。オプションのアドオン Crosswork コンポーネントをインストールすると、その機能も共通の UI に完全に統合されます。個々のアプリケーション UI を個別に操作する代わりに、共通の UI 内ですべての機能を使用することで、運用エクスペリエンスが向上し、生産性が向上します。

共通 API は、Crosswork Network Controller のプログラマビリティを実現します。共通 API は、さまざまな組み込みコンポーネントによって公開されるすべての API のための単一のアクセスポイントを提供します。API は、REST ベースのノースバウンド インターフェイスを外部システム（OSS システムなど）に提供し、Cisco Crosswork Network Controller と統合します。最適化の使用例には RESTCONF および YANG データモデルを使用できます。API の詳細と使用例については、Cisco DevNet の 『Cisco Crosswork Network Automation API Documentation』を参照してください。

Crosswork Infrastructure および Shared Services

Cisco Crosswork Infrastructure は、すべての Cisco Crosswork コンポーネントを展開できる復元力と拡張性を備えたプラットフォームです。このインフラストラクチャと共有サービスは、以下を提供します。

- 展開済みの Crosswork アプリケーションのすべての API にアクセスできる単一の API エンドポイント
- アプリケーション間でデータを渡すための共有 Kafka バス
- アプリケーションがデータを保存するための共有データベース（リレーショナルデータベースやグラフなど）
- ネットワークから収集されたすべての時系列データを保存する単一の共有データベース
- プロセスレベルの復元力を提供する、堅牢な Kubernetes ベースのオーケストレーションレイヤ
- インフラストラクチャおよびそれが存在する仮想マシン（VM）のクラスタの正常性をモニターするためのツール

Cisco Crosswork Health Insights および Cisco Crosswork Change Automation

Cisco Crosswork Health Insights および Cisco Crosswork Change Automation は、オプションで Cisco Crosswork Network Controller とともにインストールできるコンポーネントです。

Cisco Crosswork Health Insights は、リアルタイムの重要業績評価指標（KPI）のモニターリング、アラート、およびトラブルシューティングを実行します。Cisco Crosswork Health Insights は、プログラム可能なモニターリングと分析を可能にします。ネットワーク インフラストラクチャの変更に対応するためのプラットフォームを動的に提供します。Cisco Crosswork Health Insights は、オペレータがユーザー定義のロジックに基づいてネットワークイベントを監視しアラートを生成できる、動的検出および分析モジュールを構築します。

Cisco Crosswork Change Automation は、ネットワークへの変更の展開プロセスを自動化します。組み込みの Ansible Playbook を使用してオーケストレーションを定義し、設定変更を Cisco Network Services Orchestrator（NSO）にプッシュしてネットワークに展開します。

Cisco Crosswork Network Controller 内のこれらのコンポーネントにより、ネットワーク内の問題のクローズドループ検出と修復が可能になります。オペレータは、定義済みの重要業績評価指標（KPI）のしきい値を超えたときに実行される事前定義された修復タスクとアラームを一致させることができます。これにより、ネットワークオペレータの手動介入に起因する人的エラーのリスクを最小限に抑えながら、問題の検出と修復にかかる時間を短縮できます。

Cisco Crosswork Zero-Touch Provisioning（ZTP）

Cisco Crosswork ZTP は、オプションで Cisco Crosswork Network Controller とともにインストールできます。

Cisco Crosswork ZTP は、新しい IOS-XR デバイスを自動的にオンボーディングおよびプロビジョニングするための統合されたターンキーソリューションであり、新しいハードウェアをより低い運用コストで迅速に展開で

きます。オペレータは、シスコ認定のソフトウェアイメージとデイゼロソフトウェア設定を使用して、デバイスを迅速かつ簡単に起動することができます。このような方法でプロビジョニングされると、新しいデバイスは Crosswork デバイスインベントリにオンボーディングされ、他のデバイスと同様に監視および管理できるようになります。

Cisco Crosswork ZTP は、従来の ZTP 機能の他に Secure ZTP 機能も提供します。Secure ZTP は RFC 8572 規格に基づいており、セキュアなトランスポートプロトコルと証明書を使用してデバイスを検証し、ダウンロードを実行します。Secure ZTP は、リモートのネットワークデバイスに到達するためにパブリック インターネット リソースを通過する必要がある場合、またはデバイスがサードパーティ製である場合に役立ちます。Secure ZTP では、デバイスと Cisco Crosswork ZTP ブートストラップサーバーは、デバイスの Secure Unique Device Identifier（SUDI）および Crosswork サーバー証明書を TLS/HTTPS 経由で使用して相互に認証します。セキュアな HTTPS チャネルが確立されると、Crosswork ブートストラップサーバーは、RFC 8572 YANG スキーマに準拠した一連の署名付きイメージと設定アーティファクトをダウンロードして適用するようにデバイスに要求します。イメージ（存在する場合）をダウンロードしてインストールし、デバイスが新しいイメージをリロードすると、デバイスは設定スクリプトをダウンロードして実行します。

Cisco Network Services Orchestrator（NSO）

Cisco Network Services Orchestrator（NSO）は、プラグ可能な機能パックを使用してネットワーク全体のサービスインテントをデバイス固有の設定に変換する、オーケストレーション プラットフォームです。Cisco NSO は、ETSI（European Telecommunications Standards Institute）アーキテクチャ内のネットワーク オーケストレータ（NFVO）の役割を果たし、物理ネットワーク要素とクラウドベースの仮想ネットワーク機能（VNF）全体で柔軟なサービス オーケストレーションとライフサイクル管理を提供します。このソリューションは、物理および仮想の両方のネットワークエレメントに対して一貫した運用モデルを使用することにより、双方のエレメントに対して完全なサポートを提供します。マルチベンダー環境でのオーケストレーションが可能で、複数のテクノロジースタックをサポートしているため、エンドツーエンドの自動化をほぼすべてのユースケースやデバイスに拡張できます。

Cisco NSO には、開発者がサービスアプリケーションを実装できるように設計された豊富な API のセットがあります。カスタマーサービスを実現するために必要な YANG データモデルを定義および実行するためのインフラストラクチャを提供します。また、各ネットワークサービスのライフサイクル全体を管理する役割もあります。

YANG モデリング言語を使用して記述されたサービスモデルとデバイスモデルにより、Cisco NSO はサービスの意図をデバイス機能に効率的に「マッピング」し、ネットワークに展開するために必要な最小限の設定を自動的に生成できます。この機能は、Cisco NSO の FASTMAP アルゴリズムによって促進され、現在の設定状態をサービスの意図と比較し、サービスをネットワーク内でインスタンス化するために必要な最小限の変更を生成することができます。

Cisco Crosswork Network Controller に含まれている、またはオプションのアドオンであるすべての Crosswork コンポーネントは、Cisco Crosswork ZTP を除き、Cisco NSO との統合が必要です。

Cisco Crosswork Network Controller には、次の Cisco NSO 機能パックが必要です。

- SR-TE コア機能パック（CFP）は、SRv6 を含む明示的および動的なセグメント ルーティング ポリシーのプロビジョニング、および特定の色のプレフィックスに対するオンデマンド SR-TE ポリシーのインスタンス化を可能にします。
- IETF に準拠した L2VPN および L3VPN のプロビジョニング用の機能パックの例。これらの機能パックは、IETF NM モデルに基づいて、ベースライン L2VPN および L3VPN のプロビジョニング機能を提供し

ます。カスタマイズの前に、これらのサンプル機能パックを使用して、次の VPN サービスをプロビジョニングできます。

注： Service Health 機能パックは、Cisco Crosswork Network Controller の機能パックとは別にインストールする必要があります。

- L2VPN：
  - ターゲット LDP を使用したポイントツーポイント VPWS
  - EVPN を使用したポイントツーポイント VPWS
  - EVPN を使用したマルチポイント VPLS（サービストポロジ ELAN、ETREE、および Custom）
- L3VPN
- RSVP-TE トンネルプロビジョニングの参照実装として意図された、必要に応じてカスタマイズ可能な IETF 準拠の RSVP-TE 機能パックのサンプル。

注： デフォルトでは、IETF 準拠の NM モデルが使用されます。以前のバージョンで提供されていた Flat モデルを引き続き使用する場合は、手動セットアッププロセスが必要です。詳細については、シスコ カスタマー エクスペリエンスの担当者にお問い合わせください。

注： Cisco NSO 機能パックのサンプルは、Cisco Crosswork Network Controller の VPN サービスプロビジョニング機能の出発点として提供されます。これらのサンプルは、一部の限定されたネットワーク設定では「そのまま」使用できますが、Cisco Crosswork Network Controller の拡張可能な設計を示すことを意図としています。一般的な質問への回答は Cisco Devnet で確認できます。シスコ カスタマー エクスペリエンスの担当者は、サンプルに関する一般的な質問への回答を提供できます。特定のユースケースに合わせたサンプルのカスタマイズについては、シスコアカウントチームを通じてサポートを提供いたします。

注： Cisco NSO は現在、バンドルイーサネット（BE）、ルート識別子（RD）、または L2VPN EVPN での BGP ルートターゲット（RT）機能をサポートしていません。マルチホーミングと L2VPN ルートポリシーはサポートしていますが、EVPN ELAN/ETREE の L2VPN に RD 値を指定するオプションも、ロードバランシングタイプを指定するオプションもありません。これらの機能を実行するには、シスコアカウントチームに連絡して、一連のカスタム構成テンプレートとバンドルを手動で構成するためのアドバイスを受けてください。

Cisco セグメントルーティングパス計算要素（SR-PCE）

Cisco SR-PCE は、セグメントルーティング（SR）とリソース予約プロトコル（RSVP）の両方をサポートする IOS-XR のマルチドメインステートフル PCE です。Cisco SR-PCE は、IOS-XR デバイス内のネイティブのパス計算エンジン（PCE）機能に基づいて構築され、BGP-LS を介してトポロジおよびセグメントルーティング ID を収集し、サービスの SLA に準拠するパスを計算して、セグメントの順序付きリストとして送信元ルータにプログラムします。パス計算クライアント（PCC）が PCC を起点とする PCE ピアへのヘッドエンドトンネルを報告し、制御を委任します。PCC および PCE は、更新をネットワークにプッシュし、必要に応じてパスを再び最適化するために SR-PCE が使用するパス計算要素通信プロトコル（PCEP）の接続を確立します。

Cisco SR-PCE は、仮想化された XRv9000 を使用してサーバーリソースに配置することも、IOS-XR ルータ内で実行される統合アプリケーションとして配置することもできます。

注： 2,000 ノード以降の SR-PCE からスケールノードを自動検出するための静的ルートの追加はサポートされていません。

Cisco Service Health

注： Service Health は、限定提供で使用できます。詳細については、アカウントチームにお問い合わせください。

Service Health により、サービス品質に関する問題の検出とトラブルシューティングに必要な時間が大幅に短縮されます。プロビジョニングされた L2/L3 VPN サービスのヘルスステータスをモニターし、オペレータはサービスが低下した理由と場所を特定できます。また、以下を可視化するヒューリスティックモデルにより、サービス固有のモニターリング、トラブルシューティング、保証、およびプロアクティブな因果関係を提供できます。

- 単一のサービスが選択されている場合の、マップへのサブサービス（デバイス、トンネル）のヘルスステータス
- サービスの論理依存関係ツリー。品質低下が発生した場合のトラブルシューティングにおいて、オペレータが問題の発生場所、可能性のある症状の兆候、品質低下時に影響を与えるメトリックを特定することを支援します。
- サービスヘルスステータスの履歴ビュー（最大 60 日間）

Service Health は次の機能も提供します。

- Service Health モニタリングは、基本モニタリングと詳細モニタリングの両方で使用できます。必要に応じて適切なモニタリングオプションを選択する方法については、「**基本および詳細モニタリングルール**」セクションを参照してください。
- Service Health は、最大 50 GB のモニタリングデータの**内部ストレージ**を提供します。このデータはシステムに保存されます。内部ストレージの制限を超えると、履歴データが失われます。Service Health のストレージ容量を拡張することを選択した場合は、Amazon Web Services（AWS）クラウドアカウントを使用して、クラウドに**外部ストレージ**をオプションで設定できます。外部ストレージを活用することで、既存のすべての内部ストレージデータが外部クラウドストレージに自動的に移動し（詳細については付録「**Service Health 外部ストレージの設定**」を参照）、内部ストレージはキャッシュストレージとしてローカルに機能するようになります。Service Health 用の外部ストレージを設定すると、サービスの正常性をモニターし続けるサービスの履歴データが失われることがなくなり、データの履歴モニタリングサービスを維持するオプションを選択した場合、モニタリングの停止を選択したサービスのサービスヘルスデータが保持されます。内部ストレージと外部ストレージの詳細、および停止時にモニタリングサービスの履歴データを保持する方法については、付録の「**Service Health 外部ストレージの設定**」セクションと「**サービスヘルスモニタリングの停止**」セクションを参照してください。

  注： 多数の Service Health サービスをモニタリングすることが予想される場合、Cisco は、Service Health をインストールした後、サービスのモニタリングを開始する前に、外部ストレージを設定して内部ストレージの超過や履歴データの損失を避けることを推奨します。

- Service Health は、ポイントツーポイント L2VPN をサポートしています。

  注： 現在、Service Health はマルチポイント L2VPN をサポートしていません。

- Service Health L2VPN/L3VPN でサポートされるサブサービスを確認するには、付録の「**Service Health でサポートされるサブサービス**」セクションを参照してください。各 VPN サービスフレーバーでサポートされるサブサービスを明確にする詳細情報が提供されています。
- Cisco Network Services Orchestrator（NSO）Layered Service Architecture（LSA）に対する Service Health のサポートにより、付加的な NSO クラスタインスタンス（CFS タイプ 1 つと RFS タイプ 2 つ）が追加されます。これらの付加的な NSO タイプは、高可用性機能としての役割を果たします。複数のタイプにデバイスを分散させることで、Service Health の LSA 機能により、アシュアランスのための動的な構成が可能になります。Service Health のプロバイダーアクセスを管理するには、[管理（Administration）] > [プロバイダーアクセスの管理（Manage Provider Access）] を選択します。[プロバイダー（Providers）] 画面が表示されます。追加の詳細情報については、Crosswork アドミニストレーション ガイドおよび NSO のドキュメントを参照してください。
- サービスヘルス収集ジョブの管理オプションによって、より多くの数のジョブがサポートされるパラメータ化されたジョブ（テンプレートベースの収集ジョブ）を表示する機能が提供され、CLI 収集ジョブを表示する機能が追加されます。これは、パラメータ化されたジョブを使用して個々のデバイスの詳細を調べることにより、収集ジョブの問題をトラブルシューティングする場合に役立ちます。デバイスは、それらが GMNI、SNMP、または CLI ベースのジョブであるかどうかを判断するために、そのコンテキスト ID（プロトコル）によって識別されます。さらに、収集ジョブ情報をエクスポートして確認することもできます。提供される情報は、エクスポートが開始された時点で .csv ファイルに収集されます。

  注： 収集ステータスをエクスポートする場合は、エクスポートを実行するたびに情報を入力する必要があります。さらに、[収集ステータスのエクスポート（Export Collection Status）] ポップアップで利用可能な [エクスポートされたファイルを復号する手順（Steps to Decrypt Exported File）] を確認して、エクスポートされた情報にアクセスして表示できることを確かめてください。

- Service Health により、Assurance Graph Manager、Expression Orchestrator、および Crosswork Expression Tracker マイクロサービスの冗長性/高可用性（HA）が拡張されます（2 つのインスタンスが利用可能になりました）。表示するには、[管理（Administration）] > [Crosswork Manager] を選択します。[Crosswork の概要（Crosswork Summary）] タブで、[Crosswork Service Health] を選択して、[アプリケーションの詳細（Application Details）] 画面と [マイクロサービス（Microservices）] を表示します。

  ◦ たとえば、[Assurance Graph Manager] の名前をクリックすると、2 つの冗長/高可用性インスタンスが表示されます。特定の状況で、インスタンスの一方がアクティブ-アクティブモードになり、他方がアクティブ-スタンバイモードになります。その結果、1 つのインスタンスがダウンした場合、2 つ目のインスタンスが冗長、HA、バックアップとして機能します。

- ヒューリスティック パッケージ：基本モニタリングレベルルールを支援するために、3 つの付加的なルールが追加されました（Rule-L2VPN-NM-Basic、Rule-L2VPN-NM-P2P-Basic、Rule-L3VPN-NM-Basic）。付加的なルールにより、たとえば Basic L2VPN NM P2P サービスなどのアシュアランスグラフ情報が生成され、2 つのサブサービスとともに使用できます。ヒューリスティック パッケージ メトリックに、CLI ベースのメトリックとパッケージの GMNI フィルタリングカスタマイズの機能が追加されました。

マルチベンダー機能

今日のネットワークは通常、時間をかけて構築され、複数のベンダーと、複数の世代のハードウェアとソフトウェアが組み込まれています。さらに、業界の標準化が不十分であるため、単一のツールを使用してこれらのネットワークをサポートすることは困難です。

サービスプロバイダーは、運用コストとメンテナンスの経費を削減し、単一のネットワークに異なるベンダー製品を展開して保守するためにカスタム運用アプリケーションを構築しなくてもよい、サードパーティ製デバイスを管理するための統合ソリューションを求めています。

Cisco Crosswork Network Controller は、標準ベースのプロトコルを使用するため、次のようなマルチベンダー機能を備えています。

- CLI および Netconf/YANG を使用した Cisco NSO 経由のネットワークサービスのオーケストレーション。Cisco NSO は、マルチベンダー ネットワーク全体のアプリケーションとサービスのプロビジョニング、モニタリング、および管理を自動化するための YANG モデル駆動型プラットフォームです。
- 標準ベースの MIB を備えた SNMP、syslog、および標準の OpenConfig モデル を備えた gNMI を使用したテレメトリデータ収集。Cisco CDG は、カスタムパッケージを採用した外部宛先および独自の SNMP MIB のためのネイティブ YANG データモデルもサポートしています。
- IGP および BGP-LS を使用した SR-PCE 経由のトポロジおよびトランスポート検出。標準 MIB を使用して SNMP 経由でリンク使用率とスループットを収集します。
- PCEP を使用したトランスポートパスの計算。

注： サードパーティのネットワークデバイスのサポートについては、特にレガシープラットフォームや非標準のデバイスやサービスが関係する場合、シスコ カスタマー エクスペリエンス担当者がお客様のマルチベンダー環境内でユースケースを検証する必要があります。

拡張性

Cisco Crosswork Network Controller のプロビジョニング機能は、製品のアプリケーション プログラミング インターフェイス（API）を使用して拡張できます。製品 API の詳細については、Cisco DevNet の『Cisco Crosswork Network Automation API Documentation』を参照してください。

プロビジョニング UI は、YANG モデルに基づいてレンダリングされるため、拡張可能です。新しいサービスが導入されると簡単に組み込むことができます。

UI の概要

ログイン

ブラウザのアドレスバーに次の URL を入力して、Web UI にログインします。

```
https://<Crosswork Management Network Virtual IP (IPv4)>:30603/
```

または

```
https://[<Crosswork Management Network Virtual IP (IPv6)>]:30603/
```

注： URL 内の IPv6 アドレスは括弧で囲む必要があります。

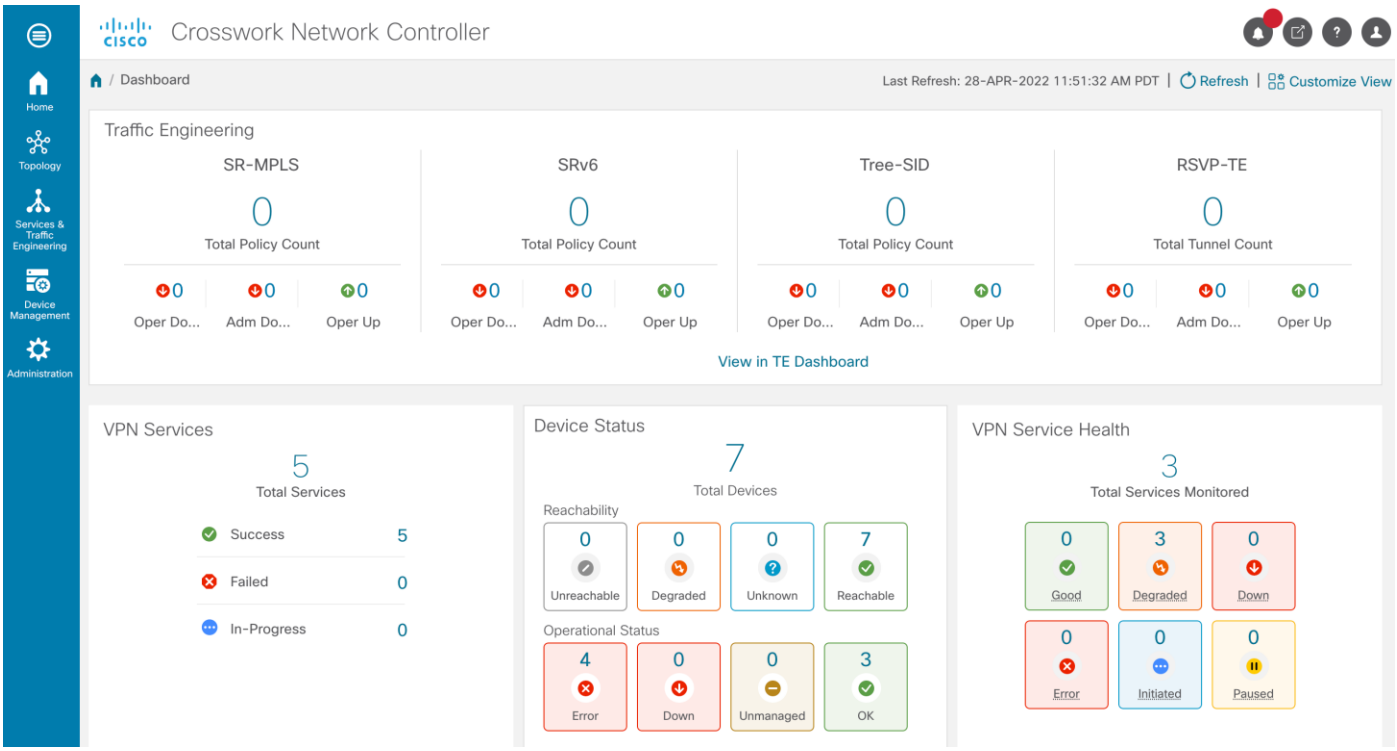
ログインウィンドウで、インストール中に設定したユーザー名とパスワードを入力して [Log In] をクリックします。

自己署名証明書：最初のアクセス時に、一部のブラウザでサイトが信頼できないという警告が表示されます。この場合は、指示に従ってセキュリティ例外を追加し、サーバーから自己署名証明書をダウンロードします。証明書をダウンロードすると、ブラウザは今後のすべてのログイン試行で信頼できるサイトとしてサーバーを受け入れます。

CA 署名付き証明書：実稼働環境で使用する場合は、CA 署名付き証明書をインストールすることをお勧めします。これは、サイトが信頼できないことを示す警告を回避するためです。

ダッシュボード

ログインに成功すると、[Home] ページが開きます。[Home] ページにはダッシュボードが表示され、デバイスの到達可能性や動作ステータスのほか、トランスポートポリシーや VPN サービスなど、管理対象のネットワークの運用がひと目で分かる概要が示されます。ダッシュボードは一連のダッシュレットで構成されています。ダッシュボードに含まれる特定のダッシュレットは、インストールした Cisco Crosswork アプリケーションによって異なります。各ダッシュレットのリンクを使用すると、詳細を詳しく見ることができます。



注： このスクリーンキャプチャにはインストールしていないオプションのコンポーネントも表示されているため、お使いのダッシュボードとは異なる場合があります。

ナビゲーション

ウィンドウの左側にあるメインメニューから、Cisco Crosswork Network Controller のすべての機能と、デバイス管理および管理タスクにアクセスできます。[Home]、[Topology]、[Services & Traffic Engineering]、[Device Management]、および [Administration] メニューオプションは、Cisco Crosswork Network Controller のすべてのネイティブコンポーネントがインストールされている場合に使用できます。インストールされている Cisco Crosswork アドオンアプリケーションに応じて、追加のメニューオプションをメインメニューで使用できます。

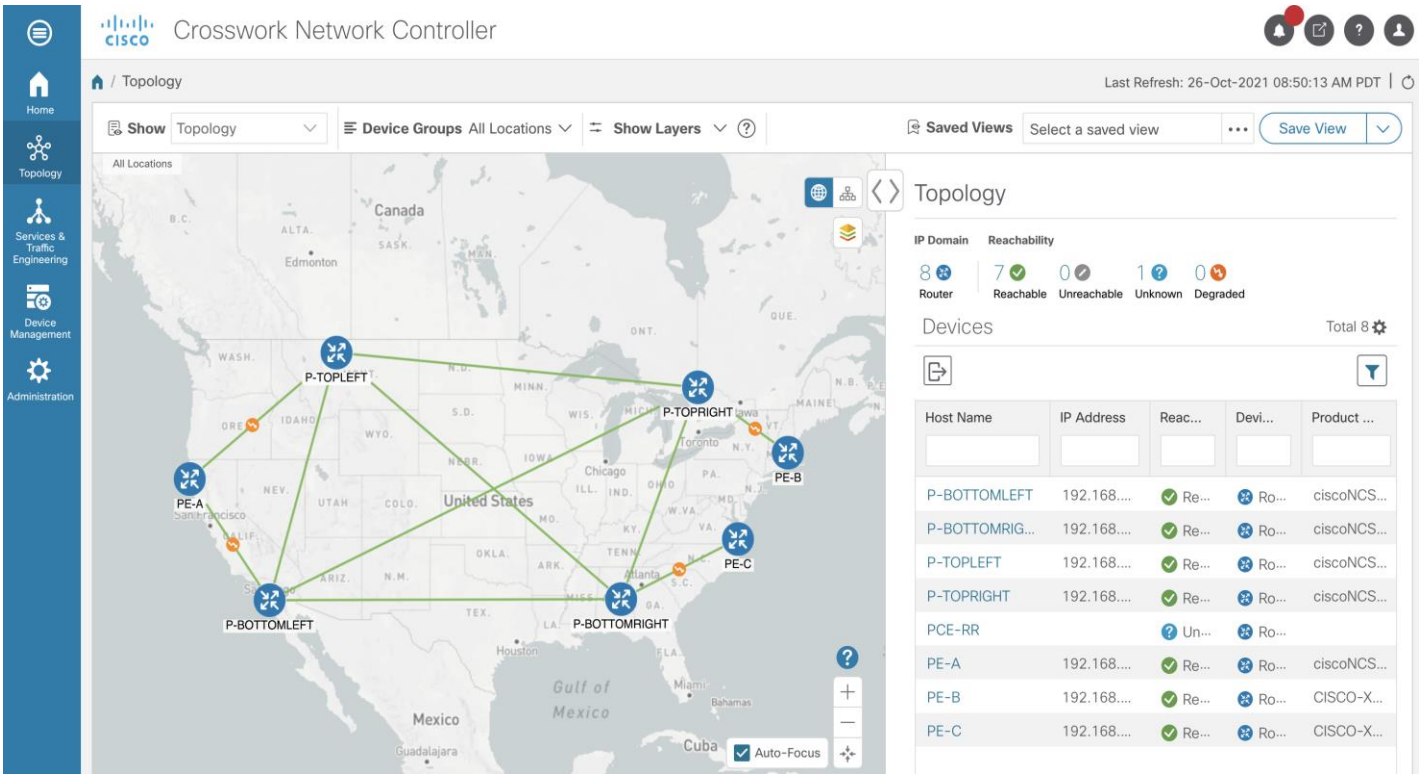
自宅（Home）

「ダッシュボード」で説明したように、ホームページにはダッシュボードが含まれます。

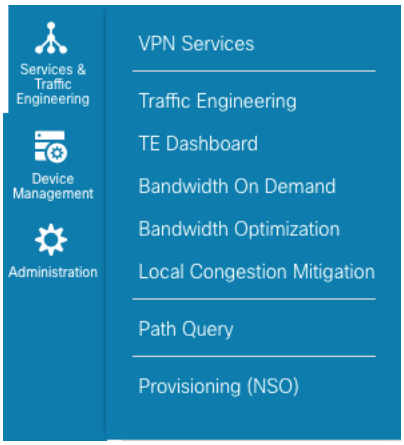
トポロジ

ネットワークトポロジは、論理マップまたは地理的（Geo）マップに表示できます。ここでは、デバイスとリンクが地理的コンテキストで表示されます。論理マップは、自動レイアウトアルゴリズムに従って配置されたデバイスとそれらのリンクを示します。Geo マップは、単一のデバイス、デバイスグループ、デバイスクラスタ、リンク、およびトンネルを世界地図に重ねて表示します。マップ上の各デバイスの位置は、デバイスの GPS 座標（経度と緯度）を反映します。

[Topology] ページは、管理対象デバイスとそれらの間のリンクを示すマップ、および管理対象デバイスをリストするデバイステーブルで構成されます。マップでは、デバイスのステータスとヘルスを一目で確認できます。テーブル内のデバイスをクリックすると、マップ上のデバイスが強調表示され、デバイスとその関連リンクの詳細が表示されます。論理マップ（以下に示す）と地理的マップを切り替えるにはトグルボタンを使用します。マップ内の疑問符をクリックすると、さまざまな記号の詳しい説明とその意味が表示されます。



Services & Traffic Engineering

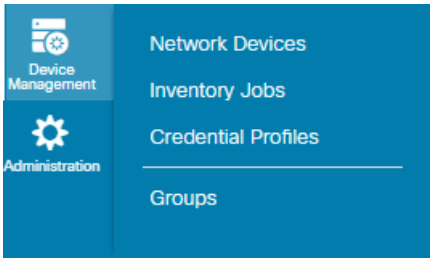


[Services & Traffic Engineering] メニューでは、VPN、トランスポートのプロビジョニングおよび可視化機能、帯域幅管理機能、および機能パックを有効にするために使用する設定ページにアクセスできます。詳細については、『Cisco Crosswork Optimization Engine 4.1 User Guide』を参照してください。

論理マップまたは地理的マップのコンテキスト内で管理対象 VPN サービスまたは SR-TE ポリシー/ RSVP-TE トンネルを表示するには、[VPN services] または [Traffic Engineering] を選択します。

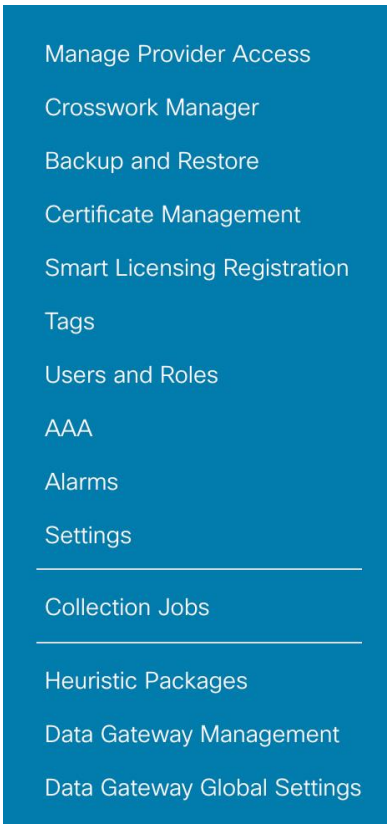
[Provisioning (NSO)] を選択して、Cisco NSO モデルからレンダリングされたプロビジョニング UI にアクセスします。ここでは、L2VPN および L3VPN サービス、SR-TE ポリシー、SR ODN テンプレート、および RSVP-TE トンネルを作成できます。また、これらのサービスおよびポリシーに必要なリソース（リソースプール、L2VPN および L3VPN サービスのルートポリシー、SR-TE ポリシーの SID リストなど）を作成することもできます。SR-TE ポリシーと RSVP-TE トンネルを VPN サービスにアタッチして、ネットワークの変更を追跡し、ネットワークを最適化するために自動的に対応することで、SLA を定義および維持できます。

Device Management



[Device Management] メニューでは、デバイスの追加、管理、グループ化、クレデンシャル プロファイルの作成と管理、デバイス関連ジョブの履歴の表示など、デバイス関連の機能にアクセスできます。

Administration



[Administration] メニューでは、すべてのシステム管理機能、データゲートウェイ管理、Crosswork クラスタとアプリケーションの正常性、バックアップと復元、スマートライセンス、および通常は管理者が実行するその他のセットアップとメンテナンス機能にアクセスできます。

これらの機能の詳細については、『Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide』を参照してください。

オーケストレーションされたサービスプロビジョニング

概要

このセクションで説明するシナリオワークフローを使用して、オペレータの意図した設定を実現するようにシステムを設定する方法の例を示します。これらのシナリオは、Cisco Crosswork Network Controller のすべての機能を示すものではなく、プラットフォームの柔軟性を示すことを目的としています。Cisco DevNet で利用可能なリソースを活用するか、またはシスコ カスタマー エクスペリエンスと連携することで追加のカスタマイズを行うことが可能です。

目的

サービスレベル契約（SLA）を遵守して維持するため、アンダーレイ トランスポート ポリシーを使用して VPN サービスをプロビジョニングします。

Challenge

ネットワークの状態は絶えず変化するため、輻輳を回避し、SLA を維持するのに十分な速度でネットワークの問題を追跡して対応することは簡単ではありません。一般的なライフサイクルには、従来から手動のモニタリングと介入が必要なフィードバックループがあり、時間とリソースを大量に消費します。

ソリューション

ネットワーク自動化の目的は、フィードバックループを自動化して、ネットワークイベントへの迅速な対応と修復を可能にすることです。Cisco Crosswork Network Controller を使用することで、ネットワークオペレータは、プログラム可能なインターフェイスを介して、トランスポートネットワーク全体で L2VPN および L3VPN サービスを非常に迅速かつ効率的にオーケストレーションできます。セグメント ルーティング トラフィック エンジニアリング（SR-TE）ポリシーは、継続的にネットワークの変更を追跡し、自動的に対応してネットワークを最適化するように設定できます。こうした SR-TE ポリシーは、VPN サービスのアンダーレイ設定として機能し、SLA を自動的に維持できます。

このソリューションに必要なサービスは、Cisco Crosswork Network Controller UI を使用して作成および管理できます。L2/L3 VPN YANG モデルベースのサービスインテントは、Cisco NSO サンプル機能パックを使用して実装されます。この機能パックは、顧客のニーズに合わせて拡張および調整できるサンプルサービスモデルを提供します。必要に応じて Service Health モニタリングをイネーブルにすると、どのサービスがプロビジョニングされたとおりに動作しているか、問題にフラグが付けられているかどうか、およびどの症状が詳しく表示されているかを確認し、迅速に対処して修正できます。

注： Cisco NSO 機能パックのサンプルは、Cisco Crosswork Network Controller の VPN サービスプロビジョニング機能の出発点として提供されます。これらのサンプルは、一部の限定されたネットワーク設定では「そのまま」使用できますが、Cisco Crosswork Network Controller の拡張可能な設計を示すことを意図しています。一般的な質問への回答は Cisco Devnet で確認できます。シスコ カスタマー エクスペリエンスは、サンプルに関する一般的な質問への回答を提供できます。特定のユースケースに合わせたサンプルのカスタマイズについては、シスコアカウントチームを通じてサポートを提供いたします。

動作の仕組み

1. ユーザーは、Cisco Crosswork Network Controller の UI または API を使用して、インテント（帯域幅、遅延など）を持つ SR-TE ポリシー/ODN テンプレートを作成します。
2. ユーザーは、UI または API を使用して VPN サービスを作成し、次を指定します。
   - VPN に参加しているエンドポイント
   - その他の必須 VPN パラメータ
   - VPN サービスに関連付けられる SR-TE ポリシー/ODN テンプレート
3. 上記の手順のプロビジョニングプロセス中に、Cisco NSO は指定されたエンドポイントで SR-TE ポリシーと VPN サービスを設定します。
4. サービスがアクティブな場合、ネットワークは SR-PCE と対話して、設定された SR-TE ポリシー/ODN テンプレートのインテントを満たすパスを動的にプログラムします。ヘッドエンドデバイスは、PCEP を介して SR-PCE からのパスを要求します（ダイナミック SR-TE ポリシーの場合）。要求で帯域幅が指定されている場合、SR-PCE は Cisco Crosswork Optimization Engine からパスを取得します。

5. SR-PCE は、PCEP を介してヘッドエンドデバイスにパスを送信し、パスの変更が必要な場合はヘッドエンドを更新します。

使用シナリオ

これから説明する使用シナリオでは、Cisco Crosswork Network Controller UI を使用したオーケストレーションされたサービスプロビジョニングの使用例を示します。

- シナリオ 1：SR-MPLS の L3VPN サービス向けの SLA の実装と保守（ODN を使用）
- シナリオ 2：SRv6 の L3VPN サービス向けの SLA の実装と維持（ODN を使用）
- シナリオ 3：明示的 SR-TE ポリシーを使用した EVPN-VPWS サービスの静的パスの指定
- シナリオ 4：予約済み帯域幅を持つ RSVP-TE トンネルを介した L2VPN サービスのプロビジョニング
- シナリオ 5：最適化の制約を伴うソフト帯域幅保証のプロビジョニング

関連リソース

- セグメントルーティングおよびセグメント ルーティング ポリシーの詳細については、『Cisco Crosswork Optimization Engine User Guide』を参照してください。
- Cisco NSO のドキュメントは、こちらの Cisco NSO 5.7.5.1 イメージに含まれています。

シナリオ 1：SR-MPLS の L3VPN サービス向けの SLA の実装と保守（ODN を使用）

シナリオのコンテキスト

このシナリオでは、特定の SLA 目標が必要な L3VPN サービスをプロビジョニングする手順について説明します。この例では、最小遅延パスを達成することが SLA 目標です。お客様は、優先順位の高いトラフィックに低遅延パスを必要としています。お客様は、共通リンクを回避して単一障害点が発生しないようにするため、ディスジョイントパス、つまり同じ送信元から同じ宛先へのトラフィックを誘導する 2 つの一意のパスを使用したいとも考えています。

これは、セグメントルーティング（SR）オンデマンドネクストホップ（ODN）を使用して実現されます。ODN により、サービスヘッドエンドルータでは、必要に応じて（オンデマンドで）、BGP ネクストホップに対する SR ポリシーを自動的にインスタンス化できます。ヘッドエンドは、SLA を定義する特定の色の ODN テンプレートで設定され、指定された色のプレフィックスを受信したときにトラフィックパスが最適化されます。プレフィックスは、L3VPN に関連付けられたルートポリシーで定義されます。

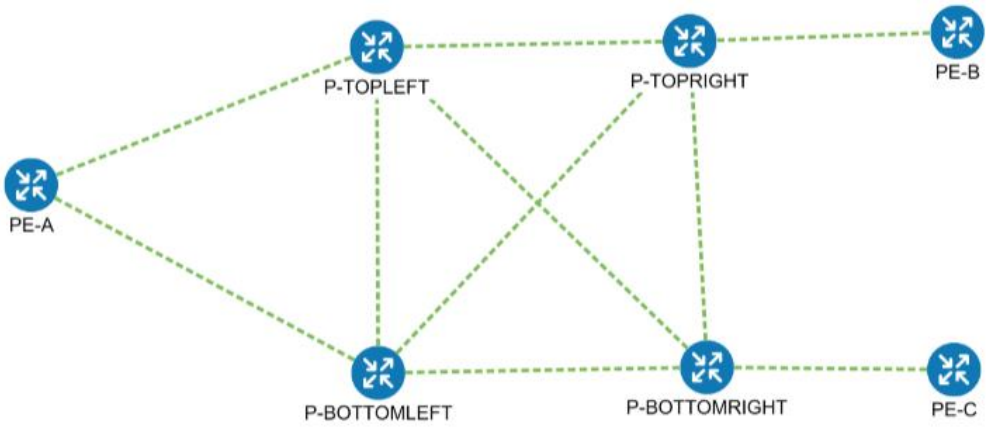
Cisco Crosswork Network Controller は、ネットワークの監視を継続し、定義された SLA に基づいてクローズドループでネットワークを自動的に最適化します。

また、ワークフロー内で Service Health モニタリングを有効にし、Flex Algo を制約として可視化するオプションもあります。Service Health では、サービスのヘルスステータスを監視し、品質が低下したサービスやダウンしたサービスに関するインサイトを活用して視覚化、検査、トラブルシューティングすることで、ネットワークの最適化を改善します。

> **注：** Service Health は、限定提供で使用できます。詳細については、アカウントチームにお問い合わせください。

Flex-Algo では、IGP がメトリックタイプと制約のユーザー定義の組み合わせでパスを計算するユーザー定義アルゴリズムに従って、IGP 最短パス計算をカスタマイズできます。また、特定の Flex-Algo 定義に基づいてフィルタリングされたトポロジを表示できます。

次のトポロジがこのシナリオの基本となります。



このシナリオでは、次の作業を行います。

- エンドポイントで特定の色を使用してセグメントルーティング ODN テンプレートを作成し、指定された色のプレフィックスを受信したときに、トラフィックが LSP（アンダーレイ）内で転送され、ベストパストンネルが動的に作成されるようにします。ODN テンプレートは、パスを最適化する SLA を定義します。この場合は遅延を最適化します。
- 計算されるパスはディスジョイントパスとして指定します。つまり同じリンクを共有しません。
- L3VPN を ODN テンプレートにバインドするために使用するルートポリシーを各エンドポイントに作成します。このルートポリシーは、顧客プレフィックスに色属性を追加し、BGP を介して他のエンドポイントにアドバタイズします。この色属性は、これらのプレフィックスに必要な SLA を示すために使用されます。
- 3 つのエンドポイントを持つ L3VPN サービスを作成し、Service Health モニタリングを有効にします。
- このオーバーレイ/アンダーレイ設定がトラフィックパスを最適化し、サービスの状態を監視しながら SLA を自動的に維持する方法を可視化します。

仮定と前提条件

- ODN を使用するには、プレフィックスの BGP ピアリングをエンドポイントまたは PE 間で設定する必要があります。通常、L3VPN では、VPNv4 および VPNv6 アドレスファミリピアリングとなります。
- Service Health を有効にするには、Service Health をインストールする必要があります。

  注： Service Health は、限定提供で使用できます。詳細については、アカウントチームにお問い合わせください。

- （オプション）Service Health は、最大 50 GB のモニタリングデータの**内部ストレージ**を提供します。このデータはシステムに保存されます。内部ストレージの制限を超えると、履歴データが失われます。Service Health のストレージ容量を拡張することを選択した場合は、Amazon Web Services（AWS）クラウドアカウントを使用して、クラウドに**外部ストレージ**を設定できます。外部ストレージを活用するこ

とで、既存のすべての内部ストレージデータが外部クラウドストレージに自動的に移動し（詳細については付録「**Service Health 外部ストレージの設定**」を参照）、内部ストレージはキャッシュストレージとしてローカルに機能するようになります。Service Health 用の外部ストレージを設定すると、サービスの正常性をモニターし続けるサービスの履歴データが失われることがなくなり、データの履歴モニタリングサービスを維持するオプションを選択した場合、モニタリングを停止を選択したサービスのサービスヘルスデータが保持されます。内部ストレージと外部ストレージの詳細、および停止時にモニタリングサービスの履歴データを保持する方法については、付録の「**Service Health 外部ストレージの設定**」セクションと「**サービスヘルスモニタリングの停止**」セクションを参照してください。

- Service Health の保証グラフを使用する前に、トポロジマップノードが完全に設定され、サービスに関連付けられたプロファイルで作成されていることを確認します。そうでない場合、[Subservice Details] メトリックに、値がまだ報告されていないと表示されます。
- L3VPN サービスモニタリングは XR デバイスをサポートしますが、XD デバイスはサポートしません。そのため、L3VPN サービスが作成され、Service Health モニタリングが有効になった後、プロバイダーとデバイスが削除されてから再び追加された場合、METRIC_SCHEDULER エラーにより、サービスモニタリングの機能低下状態が継続します。回復するには、サービスモニタリングを停止して再起動する必要があります。
- （オプション）フレキシブルアルゴリズム、および使用する ID をネットワークで設定する必要があります。

ワークフロー

- 手順 1：SLA 目標と制約に色をマッピングするための ODN テンプレートを作成する
- 手順 2：L3VPN ルートポリシーの作成
- 手順 3：L3VPN サービスの作成およびプロビジョニング
- 手順 4：Service Health モニターリングの有効化
- 手順 5：マップ上の新しい VPN サービスを可視化してトラフィックパスを確認する
- 手順 6：自動ネットワーク最適化の観察
- 手順 7：Service Health を使用して品質が低下したサービスを検査し、アクティブな症状を判断する

注： サービスとデータを示す画面キャプチャは、あくまで例として使用されるものであり、ワークフローの内容に記載されているデバイスやデータを常に反映しているとは限りません。

ステップ 1. SLA 目標と制約に色をマッピングするための ODN テンプレートを作成する

この手順では、各エンドポイントに ODN テンプレートを作成します。ODN テンプレートは色と目的を指定します。この場合は、遅延と分離（ディスジョイント）です。この ODN テンプレートは、色が一致するプレフィックスが BGP 経由で受信されたときに、トンネルを（オンデマンドで）動的に作成するために使用されます。これらのプレフィックスへのトラフィックは、新しく作成されたトンネルに自動的に誘導されます。これにより、SLA 目標とこれらのプレフィックスを対象とした制約を満たし、BGP ルートで色を使用してシグナリングされます。分離の制約は、ディスジョイントグループ ID を ODN テンプレートに関連付けることによって機能し、同じディスジョイントグループ ID を持つすべてのトンネルは分離されます。つまり、これらのトンネルはディスジョイントグループの設定方法に応じて、異なるリンク、ノード、および共有リスクリンクグループを使用します。

次の ODN テンプレートを作成します。

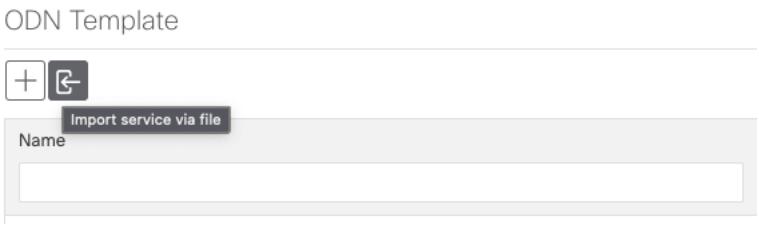
- ヘッドエンド PE-A、色 72、遅延、ディスジョイントパス（リンク）、グループ ID 16：L3VPN_NM-SRTE-ODN_72-a
- ヘッドエンド PE-A、色 71、遅延、ディスジョイントパス（リンク）、グループ ID 16：L3VPN_NM-SRTE-ODN_71-a
- ヘッドエンド PE-B および PE-C、色 70、遅延：L3VPN_NM-SRTE-ODN_70
- ヘッドエンド PE-B、色 72、遅延：L3VPN_NM-SRTE-ODN_72-b
- ヘッドエンド PE-C、色 71、遅延：L3VPN_NM-SRTE-ODN_71-c

例として、最初の ODN テンプレート：L3VPN_NM-SRTE-ODN_72-a を作成する方法を示します。他の ODN テンプレートも同じ手順で作成できます。

手順

1. [Services & Traffic Engineering] > [Provisioning (NSO)] > [SR-TE] > [ODN-Template] に移動します。
2. [+] をクリックして新しいテンプレートを作成し、一意の名前を付けます。
   この場合、名前は **L3VPN_NM-SRTE-ODN_72-a** です。[Continue] をクリックします。

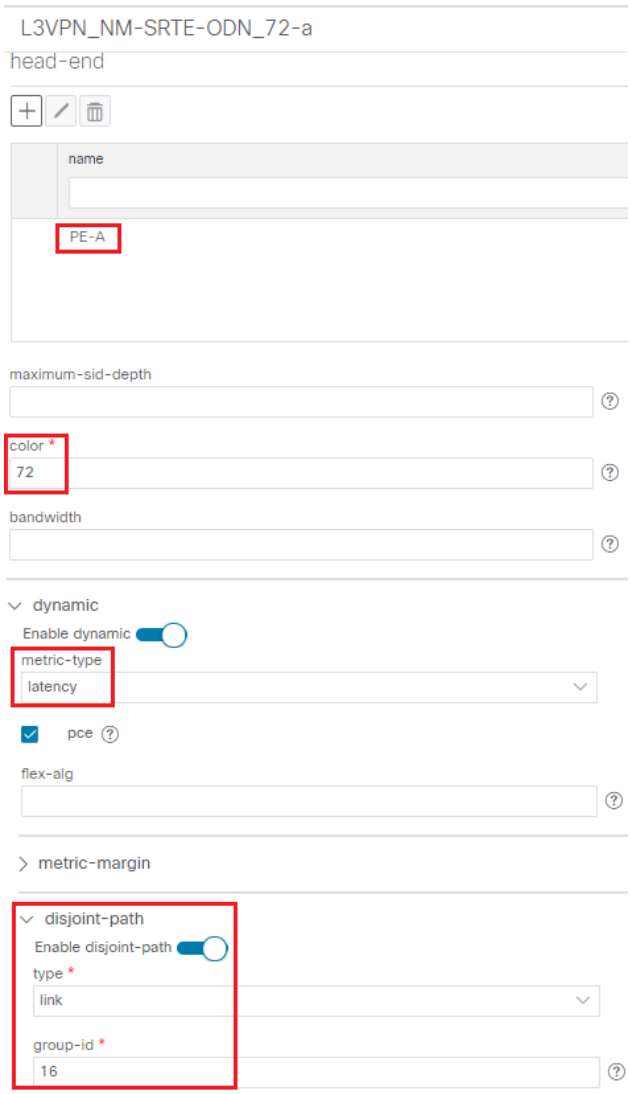
   システム上の既存のテンプレートを参照して、ファイルをインポートすることもできます。インポートされたファイルからの情報がフォームに入力されます。

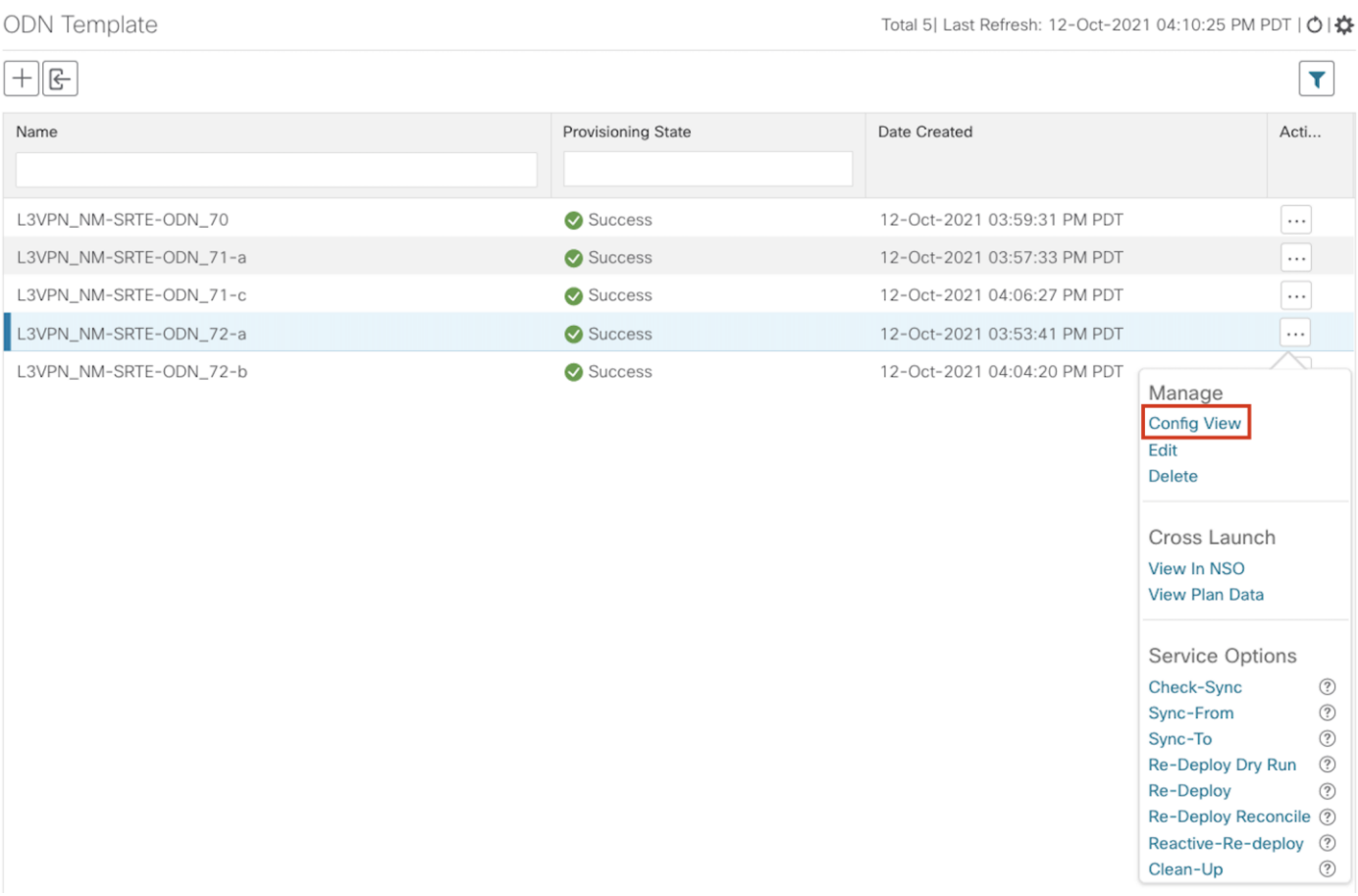
3. ヘッドエンドデバイス **PE-A** を選択し、色 **72** を指定します。
4. [Dynamic] で、メトリックタイプとして [Latency] を選択します。これが最適化の対象となる SLA 目標です。
5. [PCE] チェックボックスをオンにし、パス計算クライアント（PCC）ではなく SR-PCE でパスを計算するように指定します。
6. 必要な制約を定義します。この場合、計算パスはリンクを共有してはならないディスジョイントパスとします。
   [Disjoint-path] で、タイプとして [Link] を選択し、group-id としてグループ ID の数字（この場合は 16）を指定します。

   注： グループ ID は選択できます。同じ group-id で要求されたすべてのパスは、相互にディスジョイントされます。

   注： オプションで、制約として Flex-Algo を設定できます。



7. 変更を確定するか、[Dry Run] をクリックして、確定する前にデバイスに設定される内容を確認します。
8. 新しい ODN テンプレートがテーブルに表示され、そのプロビジョニング状態が [Success] であることを確認します。[Actions] 列の [...] をクリックし、[Config View] を選択して、作成した ODN テンプレートの詳細を示す YANG モデルベースのサービスインテントデータを表示します。



9. 上記の他の ODN テンプレートを同じ方法で作成します。

ステップ 2. L3VPN ルートポリシーの作成

この手順では、各エンドポイントのルートポリシーを作成し、そのエンドポイントの ODN テンプレートで定義したものと同じ色を指定します。ルートポリシーは、SLA が適用されるプレフィックスを定義します。指定したネットワークから一致する色のトラフィックを受信すると、ODN テンプレートで定義された SLA に基づいてパスが計算されます。

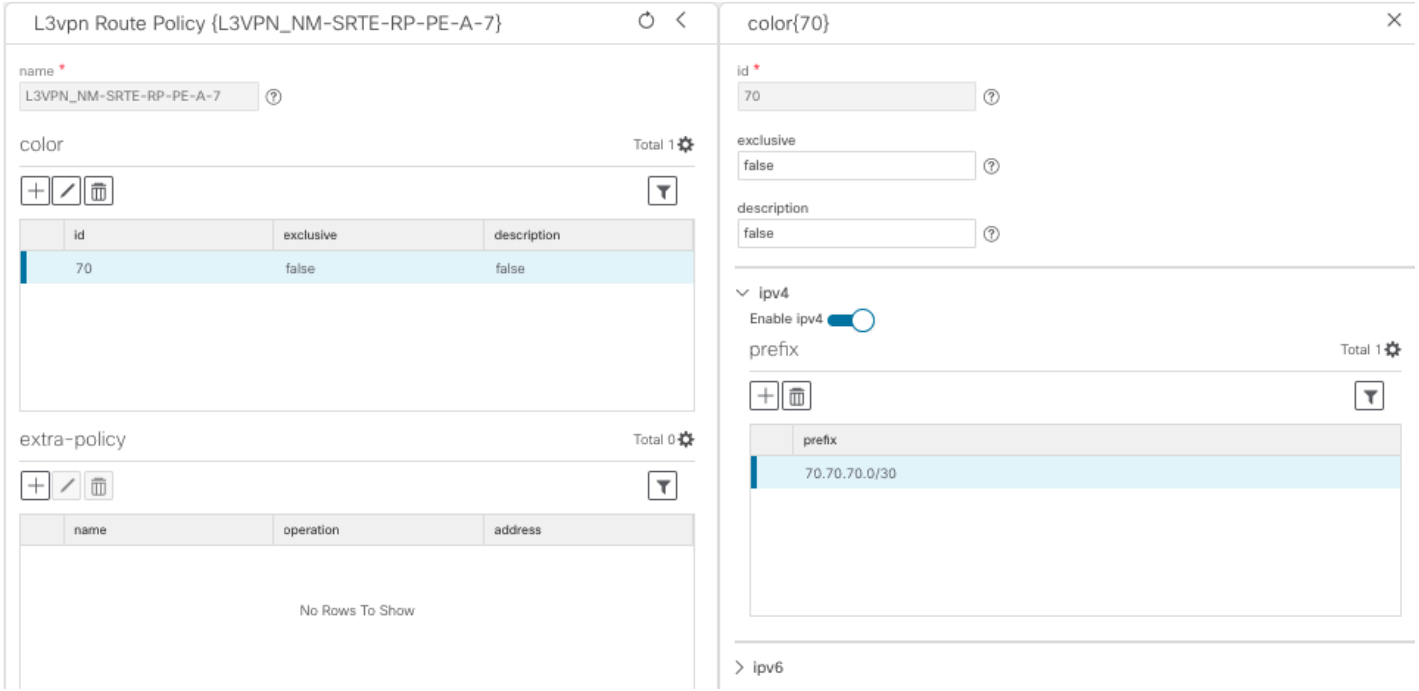
次のルートポリシーを作成します。

- 色 70、IPv4 プレフィックス 70.70.70.0/30：L3VPN_NM-SRTE-RP-PE-A-7
- 色 71、IPv4 プレフィックス 70.70.71.0/30：L3VPN_NM-SRTE-RP-PE-B-7
- 色 72、IPv4 プレフィックス 70.70.72.0/30：L3VPN_NM-SRTE-RP-PE-C-7

例として、最初のルートポリシー：L3VPN_NM-SRTE-PE-A-7 を作成する方法を示します。他のルートポリシーも同じ手順で作成できます。

手順

1. [Services & Traffic Engineering] > [Provisioning (NSO)] > [L3vpn] > [L3vpn Route Policy] に移動します。
2. [+] をクリックして新しいルートポリシーを作成し、一意の名前を付けます。
3. [Color] の下にある [+] をクリックします。PE-A の ODN テンプレートで指定されている色と同じ色 **70** を指定し、[Continue] をクリックします。
4. ネットワークトラフィックを識別するために必要な IPv4 または IPv6 プレフィックスを入力します。たとえば、IPv4 を展開し、[+] をクリックして新しいプレフィックスを作成します。IPv4 プレフィックス **70.70.70.0/30** を入力し、[Continue] をクリックします。



5. 右上隅の [X] をクリックして、[Color] ペインを閉じます。
6. 変更を保存します。

7. 新しいルートポリシーがテーブルに表示されることを確認します。
8. 上記の他のルートポリシーを同じ方法で作成します。

   注： L3VPN ルートポリシーを作成すると、各ルートポリシーの VPN プロファイルが自動的に作成されます。VPN プロファイルは、L3VPN サービスから参照されます。これにより、ルートポリシーが L3VPN サービスにバインドされます。この結果、前の手順で作成した各ルートポリシーの VPN プロファイルが作成されます。

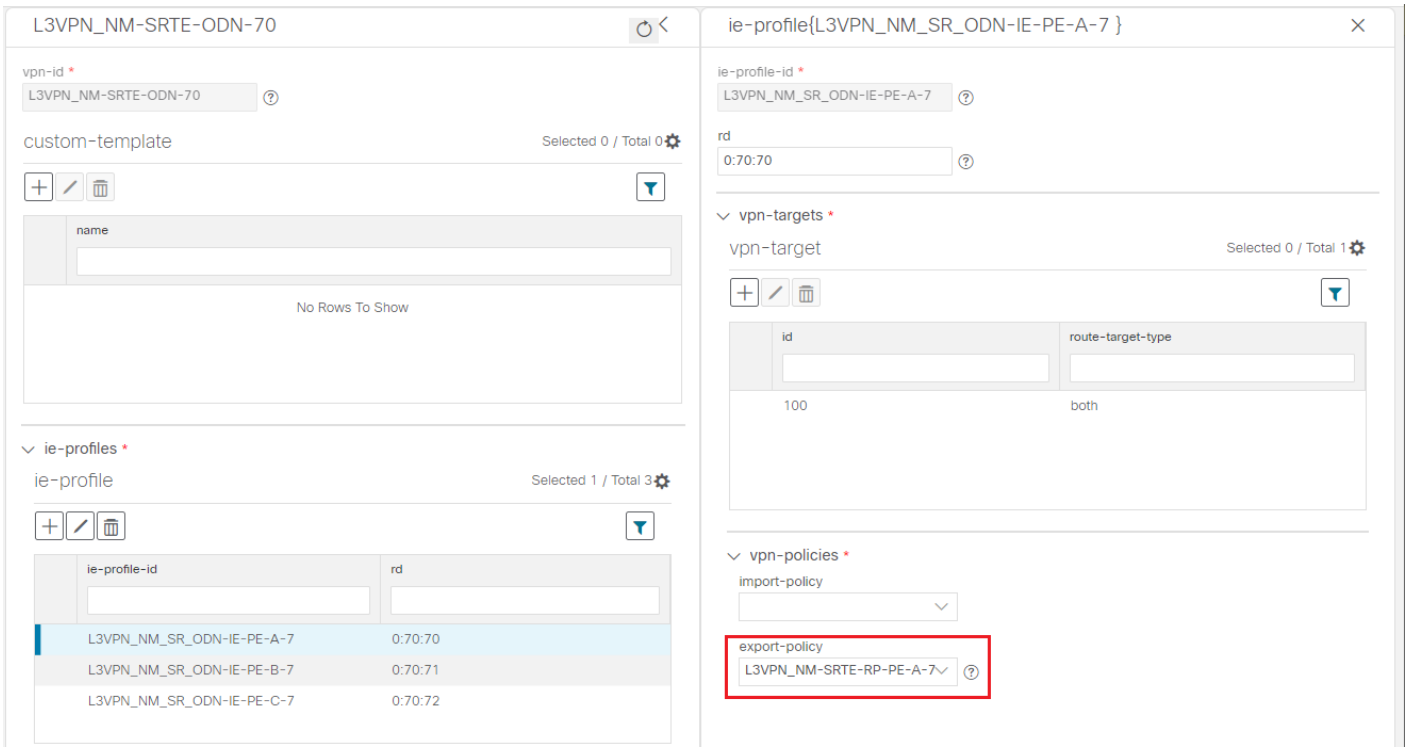
   - L3VPN_NM-SRTE-RP-PE-A-7
   - L3VPN_NM-SRTE-RP-PE-B-7
   - L3VPN_NM-SRTE-RP-PE-C-7

ステップ 3. L3VPN サービスの作成およびプロビジョニング

この手順では、3 つのエンドポイント（PE-A、PE-B、および PE-C）を備えた L3VPN サービスを作成します。各エンドポイントは、IE プロファイルに関連付けられます。IE プロファイルは、ODN テンプレートで指定されたのと同じ色のルートポリシーを含む VPN プロファイルを指します。このようにして、指定されたプレフィックスと色に一致するトラフィックが、SLA 仕様に従って処理されます。

1. [Services & Traffic Engineering] > [Provisioning (NSO)] > [L3vpn] > [L3vpn-Service] に移動します。
2. [+] をクリックして新しいサービスを作成し、一意の名前を付けます。[Continue] をクリックします。
3. IE プロファイルを作成します。これは、ルート識別子（RD）、ルートターゲット、およびエクスポート/インポートルートポリシーを定義するコンテナです。各エンドポイントの IE プロファイルを次のように作成します。
   - L3VPN_NM_SR_ODN-IE-PE-A-7、ルート識別子 0:70:70
   - L3VPN_NM_SR_ODN-IE-PE-B-7、ルート識別子 0:70:71
   - L3VPN_NM_SR_ODN-IE-PE-C-7、ルート識別子 0:70:72

     a. [ie-profile] で、[+] をクリックして新しい IE プロファイルを作成し、一意の名前を付けます。
     b. ルート識別子を入力します。これにより、IP プレフィックスが区別されて一意になります。
     c. ルートターゲットとルートターゲットタイプ（インポート/エクスポート/両方）を含め、必要な VPN ターゲットを定義します。
     d. vpn-policies で、エクスポートポリシーのドロップダウンリストから、関連する VPN プロファイル（ルートポリシーを含む）を選択します。これにより、VPN と、SLA を定義する ODN テンプレートの間の関連付けが形成されます。



e. 完了したら、右上隅の [X] をクリックします。
f. 同様に、別の IE プロファイルを作成します。

4. 各 VPN エンドポイント（PE-A、PE-B、および PE-C）を個別に定義します。

a. [vpn-nodes] で [+] をクリックし、ドロップダウンリストから関連するデバイスを選択して、[Continue] をクリックします。
b. ネットワーク ID のローカル自律システム番号を入力します。
c. 前の手順で作成した IE プロファイルを選択します。
d. PE から CE への通信のためのネットワーク アクセス パラメータを定義します。

◦ [vpn-network-accesses]で、[+] をクリックして、VPN アクセスパラメータの新しいセットを作成し、一意の ID を指定します。[Continue] をクリックします。

◦ [port-id] フィールドに、この VRF 専用のループバック インターフェイスの名前を入力します。

◦ [ip-connection] > [IPv4] > [address-allocation-type] で、[static-address] を選択します。

◦ [static-addresses] の下に、このエンドポイントのネットワークアクセス用の IP アドレスのリストを作成できるテーブルがあります。少なくとも 1 つのアドレスを作成した後、プライマリアドレスを選択できます。アドレステーブルで [+] をクリックして新しいアドレスを作成し、一意の ID を入力します。[Continue] をクリックします。ループバック インターフェイスの IP アドレスとプレフィックス長を指定します。

◦ 右上隅の [X] をクリックして、VPN ネットワーク アクセス パラメータに戻ります。

◦ [primary-address] フィールドのドロップダウンリストから、作成したアドレスを選択します。

◦ ピア AS 番号とローカル AS 番号、IP アドレスタイプ（IPv4）、BGP ネイバーの IP アドレス、BGP ネイバーと PE デバイス間で許可されるホップ数などの BGP ルーティング プロトコル パラメータを定義します。

e. 完了したら、右上隅の [X] をクリックします。

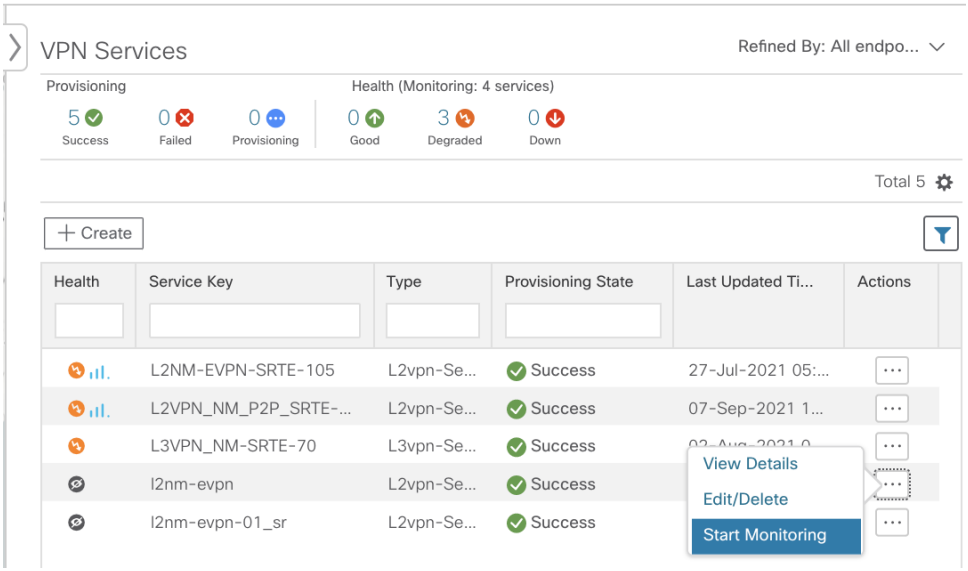
f. エンドポイントごとにこれらの手順を繰り返します。

5. 変更を確定するか、[Dry Run] をクリックして、確定する前にデバイスに設定される内容を確認します。
6. 新しい L3VPN サービスがテーブルに表示され、そのプロビジョニング状態が [Success] であることを確認します。

ステップ 4. Service Health モニターリングの有効化

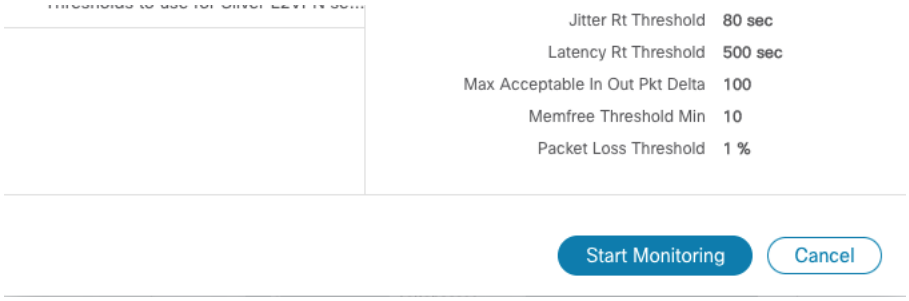
注： Service Health は、限定提供で使用できます。詳細については、アカウントチームにお問い合わせください。

1. [Services & Traffic Engineering] > [VPN Services] に移動します。画面の左側にマップが開き、画面の右側にテーブルが開きます。
2. [Actions] 列で、ヘルスモニターリングを開始する新しいサービスの [...] をクリックします。
3. [モニタ開始（Start Monitoring）] をクリックします。

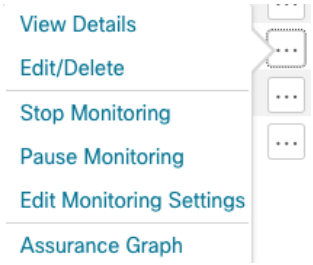


注： [Health] 列の色分けは、サービスの健全性を示します。緑色 = 良好、オレンジ = 低下、赤 = ダウン、グレー = モニターリングなし。

4. [モニターサービス（Monitor Service）] ポップアップで、モニタリングレベルを選択します。必要に応じて適切なモニタリングレベルを選択する方法については、「**基本および詳細モニタリングルール**」セクションを参照してください。



注： このサービスのヘルスモニタリングが開始された後、[アクション（Actions）] 列で [...] をクリックすると、[モニタリングの停止（Stop Monitoring）]、[モニタリングの一時停止（Pause Monitoring）]、[モニタリング設定の編集（Edit Monitoring Settings）]、[アシュアランスグラフ（Assurance Graph）] など、Service Health の追加オプションが表示されます。



注： [モニタリング設定の編集（Edit Monitoring Settings）] を選択すると、モニタリングレベルの設定を [基本モニタリング（Basic Monitoring）] から [詳細モニタリング（Advanced Monitoring）] に、または [詳細モニタリング（Advanced Monitoring）] から [基本モニタリング（Basic Monitoring）] にいつでも更新できます。

注： すでに開始されているサービスの [モニタリングの停止（Stop Monitoring）] を後で決定した場合、停止したサービスの履歴サービスデータを保持するオプションがあります。追加の手順と詳細については、付録の「**Service Health モニタリングの停止**」セクションを参照してください。

5. [モニタ開始（Start Monitoring）] をクリックします。
6. ヘルスモニターリングを開始するサービスごとにこの手順を繰り返します。
7. 完了したら、右上隅の [X] をクリックします。

ステップ 5. マップ上の新しい VPN サービスを可視化してトラフィックパスを確認する

1. [L3VPN サービス（L3VPN Service）] テーブルで、サービス名をクリックするか、[アクション（Actions）] 列の [...] をクリックして、メニューから [詳細の表示（View Details）] を選択します。
   マップが開き、サービスの詳細がマップの右側に表示されます。

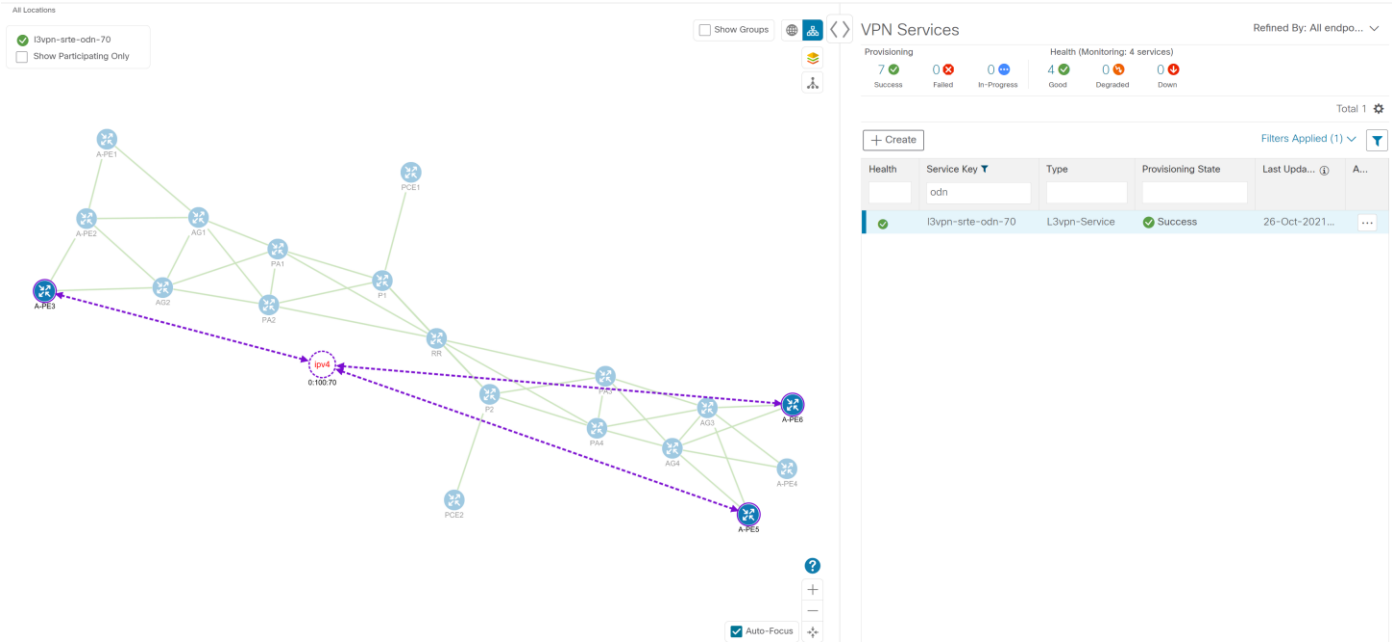
   または

   [Services & Traffic Engineering] > [VPN Services] に移動します。
   マップが開き、マップの右側に VPN サービスのテーブルが表示されます。

[Services] テーブルで [VPN] をクリックします。テーブルに多数のサービスがある場合は、名前、タイプ、またはプロビジョニング状態でフィルタリングして、VPN を見つけることができます。

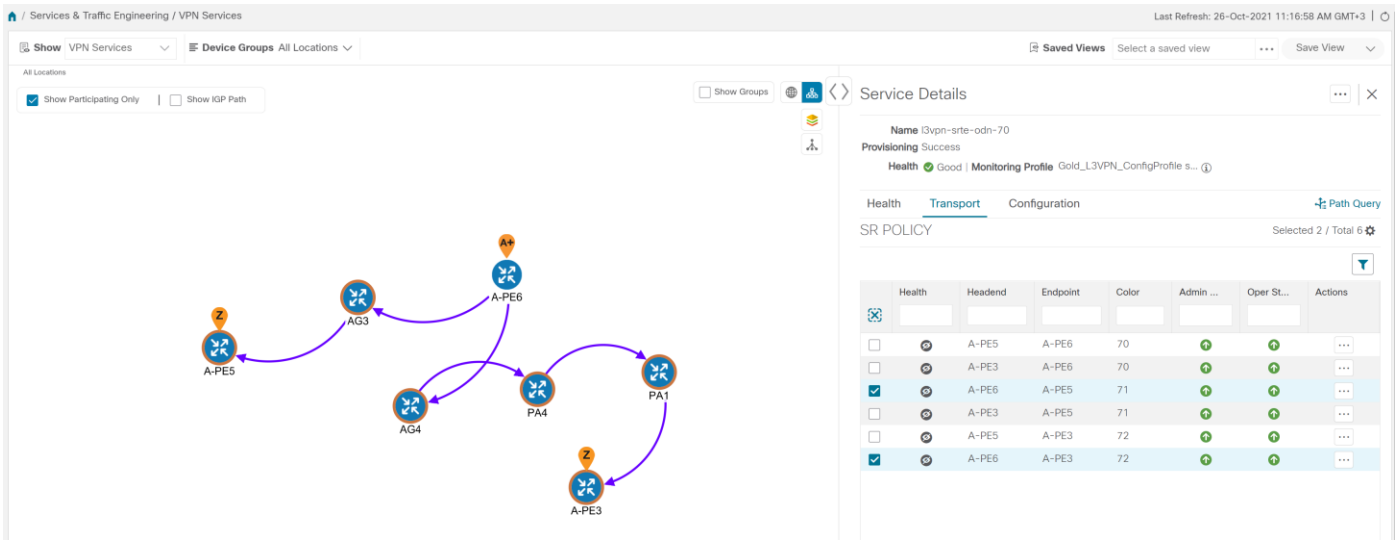
マップでは、トポロジ上のオーバーレイとして VPN が表示されます。3 つのエンドポイントと、仮想パスであることを示す点線が表示されます。

注： 次の図は、論理マップでの VPN のオーバーレイを示しています。論理マップと地理的マップを切り替えるには、マップの右上にあるボタン  を使用します。

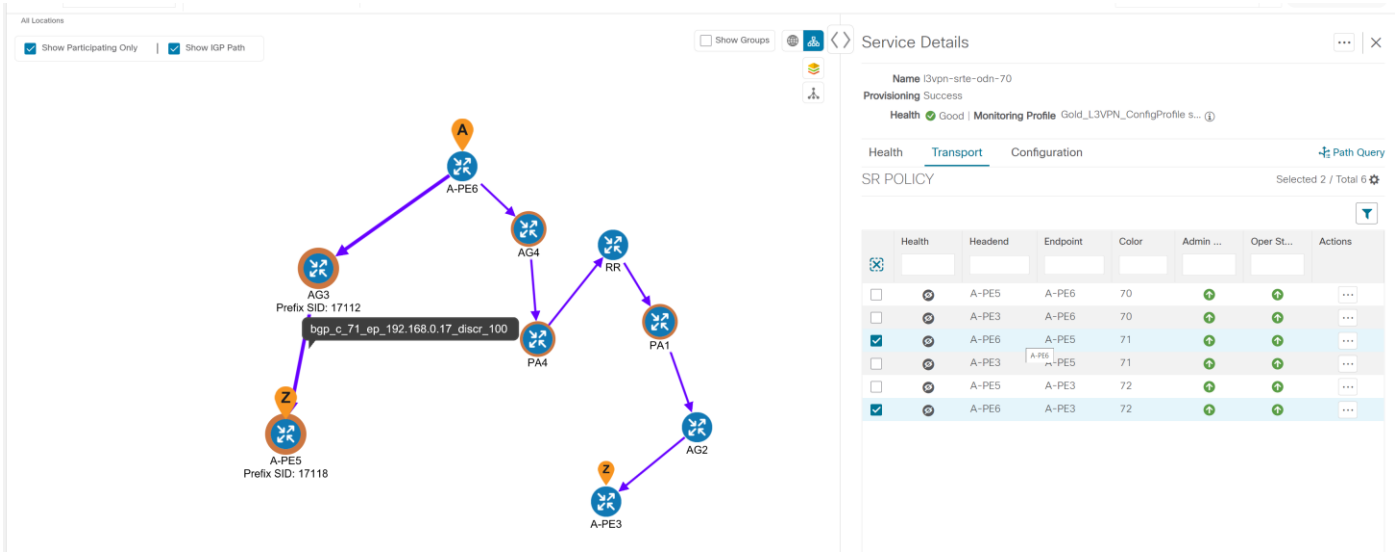


選択した VPN に関係のないデバイスを表示しないようにするには、[Show Participating Only] チェックボックスをオンにします。

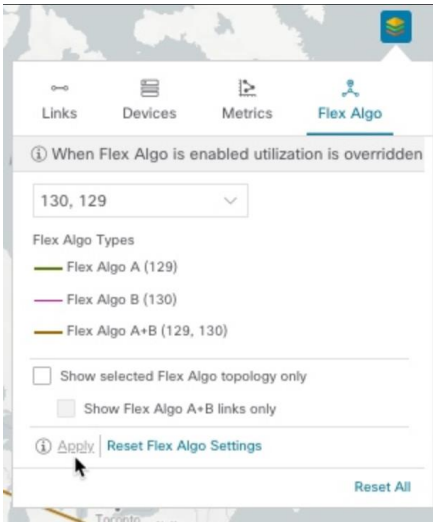
2. [Actions] 列で [...] をクリックすると、デバイス設定や計算されたトランスポートパスなどの VPN サービスの詳細ビューにドリルダウンすることができます。
3. この VPN の計算されたパスを表示するには、[Service Details] ペインの [Transport] タブをクリックします。動的に作成されたすべての SR-TE ポリシーが [Transport] タブに表示されます。1 つ以上の SR-TE ポリシーを選択して、マップ上のエンドポイントからエンドポイントまでのパスを確認します。
この例では、PE-A から PE-B へ、および PE-A から PE-C へと計算されたディスジョイントパスを調べます。



4. エンドポイント間の物理パスを表示するには、マップの左上隅にある [Show IGP Path] チェックボックスをオンにします。テーブル内の選択したポリシーにマウスカーソルを合わせると、マップ内のパスが強調表示され、プレフィックス SID とルーティング情報が表示されます。



5. トポロジを特定の Flex-Algo 制約に対してフィルタリングし、ネットワークで手動で設定したノードとリンクを可視化するには、マップの右上にあるボタン  をクリックし、次の手順を実行します。



a. [Flex Algo] タブをクリックします。
b. ドロップダウンリストから、最大 2 つの Flex-Algo ID を選択します。
c. [Flex-Algo タイプ（Flex-Algo Types）] を表示し、選択内容が正しいことを確認します。各 Flex-Algo ID への色の割り当てにも注意してください。
d. （オプション）[選択された Flex-Algo トポロジのみを表示（Show selected Flex-Algo topology only）] チェックボックスをオンにして、トポロジマップで Flex-Algo ID を分離します。このオプションを有効にすると、SR ポリシーの選択が無効になります。
e. 両方の Flex-Algo に参加しているリンクとノードのみを表示するには、[Flex-Algo A+B リンクのみを表示（Show Flex-Algo A+B links only）] をオンにします。
f. [Apply] をクリックします。Flex-Algo の選択内容に追加の変更を加えるには、[適用（Apply）] をクリックして、トポロジマップの更新内容を確認する必要があります。

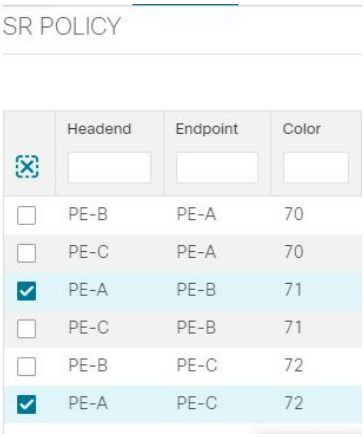
   注：選択したフレキシブルアルゴリズムには条件が定義されているが、その条件に一致するリンクとノードの組み合わせがない場合（たとえば、青色のすべてのノードまたはリンクを含むように定義されたアフィニティ）、トポロジマップは空白になります。選択したフレキシブルアルゴリズムがノードまたはリンクで設定されていない場合は、デフォルトの青色のリンクまたはノードの色が表示されます。
g. （オプション）[Save View] をクリックして、トポロジビューとフレキシブルアルゴリズムの選択を保存します。

ステップ 6. 自動ネットワーク最適化の観察

SR-PCE は常にネットワークをモニターし、定義された SLA に基づいてトラフィックパスを自動的に最適化します。説明のために、リンクのうち 1 つ（この場合は P-BOTTOMLEFT と P-BOTTOMRIGHT の間のリンク）がダウンした場合の動作を見てみましょう。これは、これまで使用していた PE-A から PE-C へのパスが使用できなくなることを意味します。したがって、SR-PCE は、PE-A から PE-C、および PE-A から PE-B への両方の代替パスを計算して、ダウンしているリンクを補正し、ディスジョイントパスを維持します。

再計算されたパス：

送信元と宛先	古いパス	新しいパス
PE-A > PE-C	PE-A > P-BOTTOMLEFT > P-BOTTOMRIGHT > PE-C	PE-A > P-TOPLEFT > P-BOTTOMRIGHT > PE-C
PE-A > PE-B	PE-A > P-TOPLEFT > P-TOPRIGHT > PE-B	PE-A > P-BOTTOMLEFT > P-TOPRIGHT > PE-B



ステップ 7. Service Health を使用して品質が低下したサービスを検査し、アクティブな症状を判断する

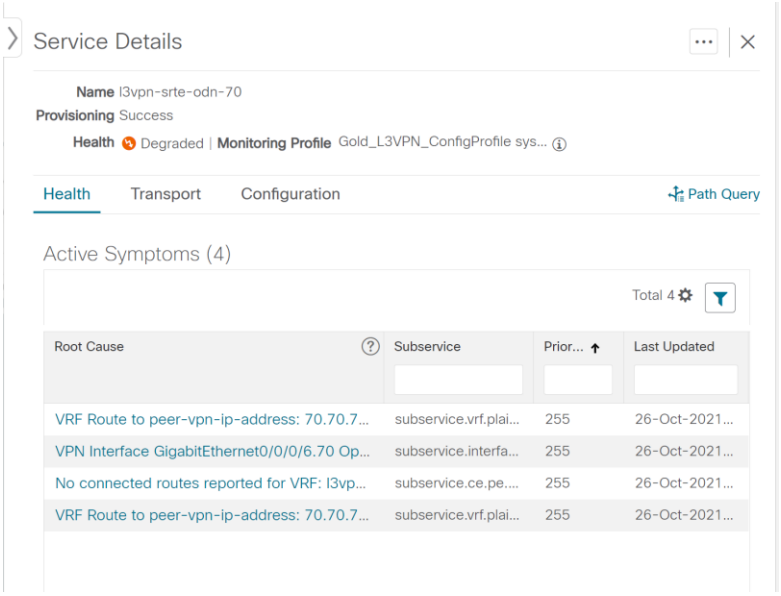
注： Service Health は、限定提供で使用できます。詳細については、アカウントチームにお問い合わせください。

この手順では、アシュアランスグラフ機能を使用して VPN サービスをモニターし、劣化したサービスまたは関連ノードを検査します。報告されたアクティブな症状を引き起こす根本原因と、影響を受けるサービスを調べることで、健全なセットアップを維持するためにまず対処すべき問題と、さらなる検査とトラブルシューティングが必要な問題を特定できます。

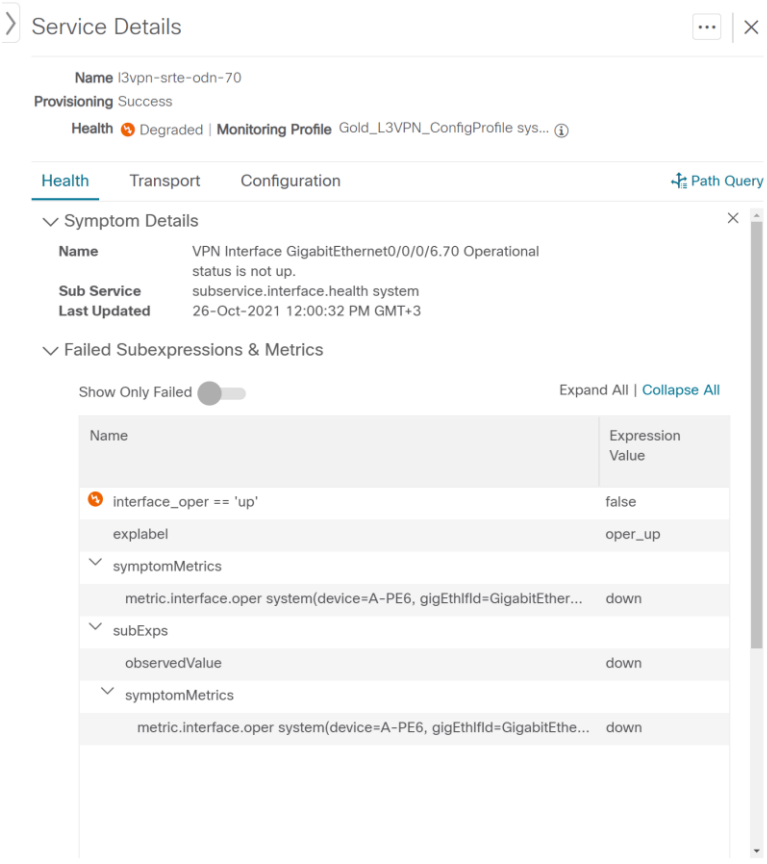
1. 右上隅の [X] をクリックして、[VPN Services] リストに戻ります。
2. 低下と表示されているサービスの名前をクリックします。マップが更新され、選択したサービスが強調表示されます。
   品質が低下したサービスの [Health] 列にオレンジ色のアイコンが表示されます。健全性状態（[Down]、[Degraded]、[Good]）でフィルタリングするには、列の上部にあるスペースをクリックし、適切なフィルタを選択します。フィルタをクリアするには、列の上部にあるスペースに表示される、指定したフィルタの横にある [X] をクリックします。これにより、すべてのフィルタリングが削除され、デフォルトですべての VPN サービスがリストに表示されます。

   注： サービスがまだ監視されていない場合、[Health] 列のアイコンはグレーで表示されます。このようなサービスのモニターリングを有効にするには、[...] をクリックして[Start Monitoring] を選択します。

3. [Actions] 列で [...] をクリックし、[View Details] をクリックします。[Service Details] 画面が右側に表示されます。
4. [Health] タブを選択した状態で、品質が低下したサービスのアクティブな症状（根本原因、サブサービス、優先度、最終更新の詳細を含む）を確認します。これらの情報は、サービスを現在監視中の場合に [Health] タブに表示されます。

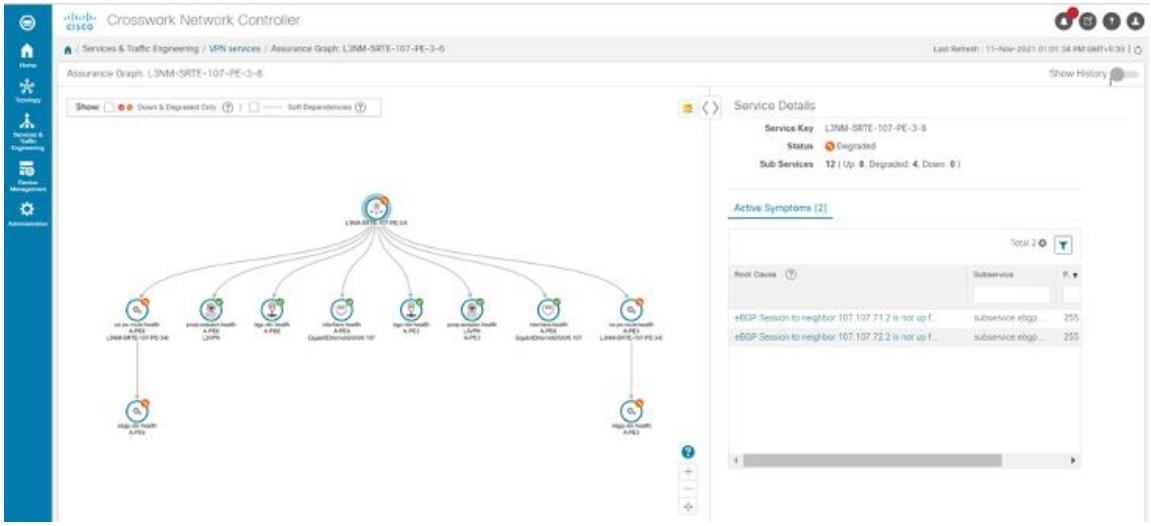


5. [Root Cause] をクリックし、症状の詳細と、失敗した部分式とメトリックに関する情報の両方を確認します。



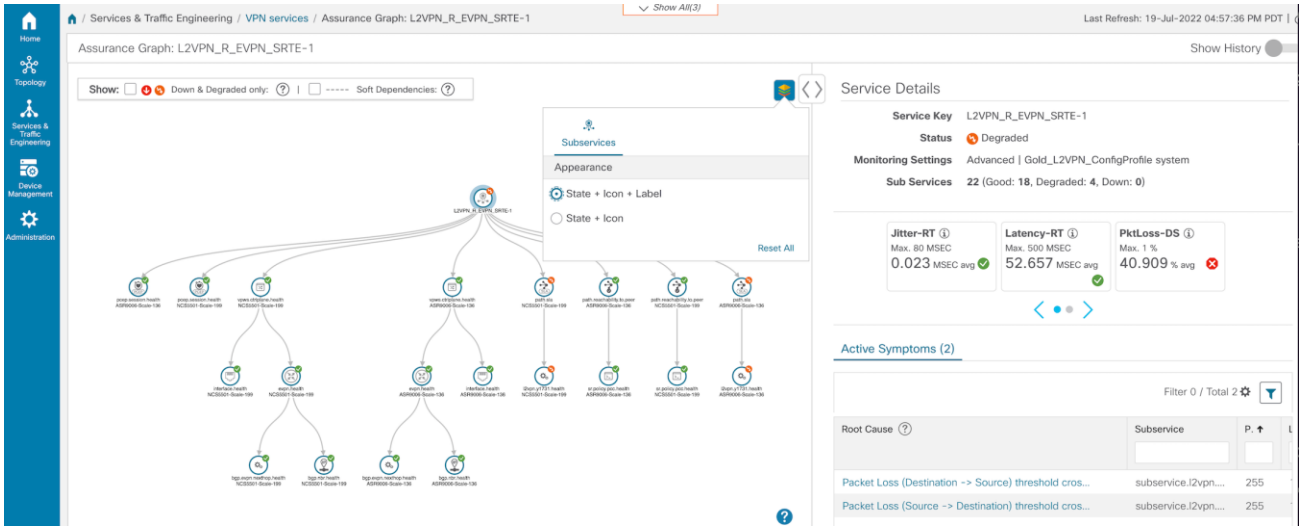
6. [Transport] タブと [Configuration] タブを選択し、表示される詳細を確認します。
7. 品質が低下したサービスの詳細をさらに分離するには、右上隅の [X] をクリックして、[VPN Services] リストに戻ります。

8. 再度、リスト内の品質が低下したサービスの名前をクリックします。[Service Details] パネルが表示され、マップが更新され、そのサービスに参加している対応するデバイスが分離されます。
9. 以下を実行し、マップ内でサービスヘルスのさらなる詳細情報を確認します。
   - マップの左上にある [Show Participating Only] チェックボックスをオンにして、マップに参加しているサービスのみを表示します。
   - マップで、デバイスと小さいバッジ（ヘルスステータスを示す）のいずれかにマウスを合わせ、その到達可能性状態、ホスト名、ノード IP、およびタイプに関連するポップアップ情報を確認します。
10. [Actions] 列で、リスト内の品質が低下したサービスの [...] をクリックし、[Assurance Graph] をクリックします。サービスとサブサービスのトポロジマップが表示され、[Service Details] パネルにサービスキー、ステータス、サブサービス、およびアクティブな症状の詳細が表示されます。



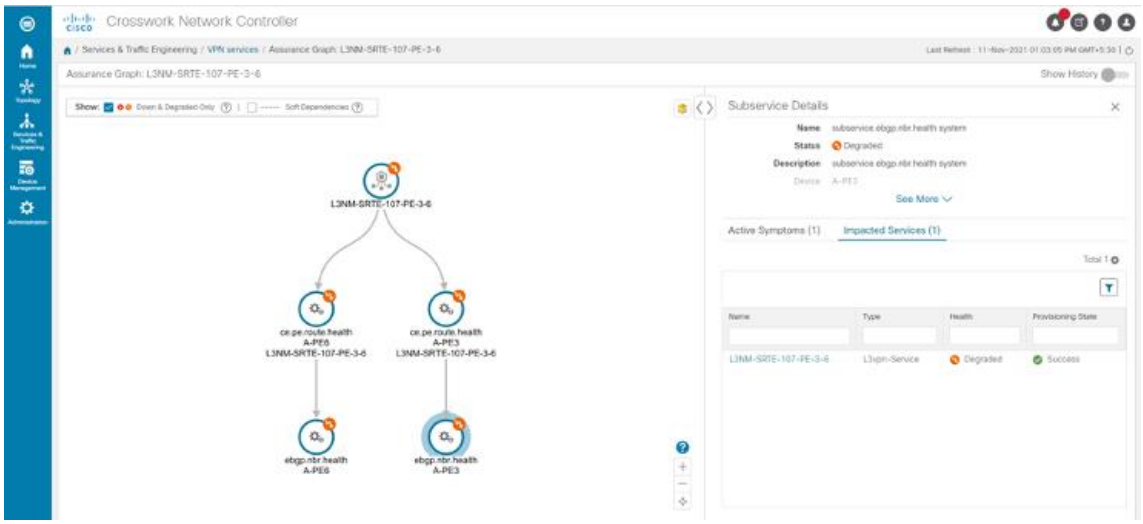
注： サービスのモニターリングが有効になった後の更新には時間がかかります。最大 5 ～ 10 分かかる場合があります。

マップの右上にあるスタックアイコンを選択して、サブサービスの外観オプション（[状態+アイコン+ラベル（State + Icon + Label）] または [状態+アイコン（State + Icon）]）を選択します。次に例を示します。



11. トポロジマップで、品質が低下したサブサービスを選択します。[Subservice Details] パネルが表示され、サブサービスのメトリック、サブサービス固有のアクティブな症状、および影響を受けるサービスの詳細が示されます。
    - **Active Symptoms**：アクティブに監視中のノードに関する症状の詳細を提供します。
    - **Impacted Services**：ヘルスステータスのモニターリング履歴に基づいて、問題によって影響を受けるサービスに関する情報を提供します。

    注： 健全性の低下の詳細については、マップのサブサービスにマウスを合わせます。サブサービスをさらに分離するには、マップの左上で [Down & Degraded Only] または [Soft Dependencies] を選択します。



12. 健全なセットアップを維持するために対処する必要がある問題を特定するために、アクティブな症状と影響を受けるサービスの情報、およびサービス低下に関連する根本原因を調べます。

サービス正常性の問題（データを適切に取得できないために機能が低下しているデバイスなど）をさらにトラブルシューティングするには、次の手順に進み、問題が収集ジョブに関連しているかどうかを調べます。

13. [管理（Administration）] > [収集ジョブ（Collection Jobs）] を選択します。
    [収集ジョブ（Collection Jobs）] 画面が表示されます。
14. [パラメータ化されたジョブ（Parameterized Jobs）] タブを選択します。
15. [パラメータ化されたジョブ（Parameterized Jobs）] リストを確認して、サービス正常性低下の問題が発生している可能性のあるデバイスを特定します。
    [パラメータ化されたジョブ（Parameterized Jobs）] を確認することにより、GMNI、SNMP、および CLI ベースのジョブをコンテキスト ID（プロトコル）によって識別して絞り込み、さらにトラブルシューティングを行うことができます。
16. [ジョブの詳細（Job Details）] パネルで、エクスポートする収集ジョブを選択し、[エクスポート（Export）] ボタンをクリックして、収集ジョブのステータスをダウンロードし、さらに調査を進めます。提供される情報は、エクスポートが開始された時点で .csv ファイルに収集されます。
    [収集ステータスのエクスポート（Export Collection Status）] ポップアップが表示されます。

    注： 収集ステータスをエクスポートする場合は、エクスポートを実行するたびに情報を入力する必要があります。さらに、[収集ステータスのエクスポート（Export Collection Status）] ポップアップで利用可能な [エクスポートされたファイルを復号する手順（Steps to Decrypt Exported File）] を確認して、エクスポートされた情報にアクセスして表示できることを確かめてください。

17. [エクスポート（Export）] をクリックします。
18. エクスポートされた収集ジョブデータのステータスを確認するには、[ジョブの詳細（Job Details）] パネルの右上にある [エクスポートステータスの表示（View Export Status）] をクリックします。
    [ステータスのエクスポートジョブ（Export Status Jobs）] パネルが表示され、エクスポート要求のステータスが示されます。
19. 収集ジョブの詳細とデバイス機能低下の考えられる原因について、エクスポートされた .csv ファイルを確認します。

まとめと結論

この例で確認したように、Cisco Crosswork Network Controller を使用することで、オペレータは SLA を使用して L3VPN をオーケストレーションし、SR-TE ポリシーを使用してこれらの SLA を維持し、ネットワークの状態を継続的に追跡し、自動的に対応してネットワークを最適化できます。この自動化により効率が向上し、手動タスクでは通常回避できない人手によるミスが減少します。プロビジョニングされたサービスを監視するために Service Health を有効にすると、各サービスのより詳細な症状、メトリック、および分析が可能になります。

シナリオ 2：SRv6 の L3VPN サービス向けの SLA の実装と維持（ODN を使用）

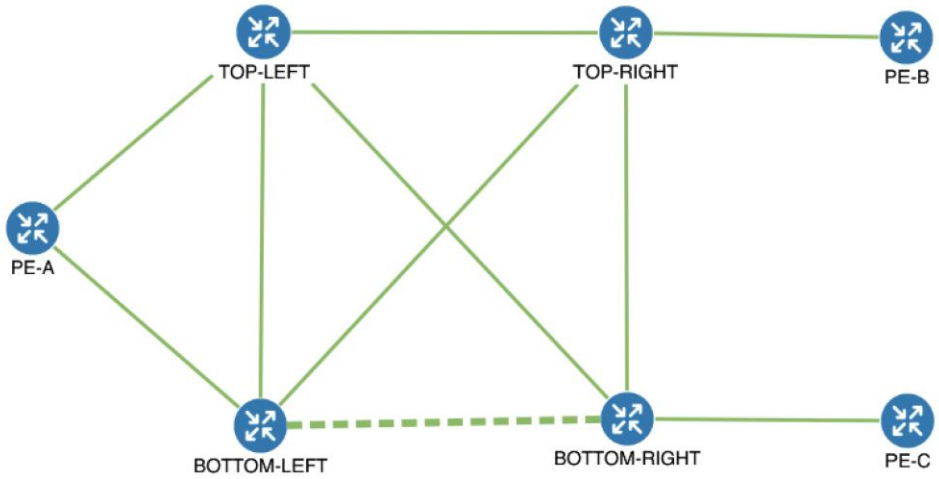
シナリオのコンテキスト

このシナリオでは、特定の SLA 目標が必要な L3VPN サービスをプロビジョニングする手順について説明します。この例では、最小遅延パスを達成することが SLA 目標です。お客様は、優先順位の高いトラフィックに低遅延パスを必要としています。お客様は、共通リンクを回避して単一障害点が発生しないようにするため、ディスジョイントパス、つまり同じ送信元から同じ宛先へのトラフィックを誘導する 2 つの一意のパスを使用したいと考えています。また、SRv6 を有効にしたいとも考えています。SRv6 は、IPv6 プロトコルを使用してパケットをより効率的に処理し、セキュリティとパフォーマンスを向上させ、使用可能なアドレスの数を大幅に増やすことができます。

これは、セグメントルーティング（SR）オンデマンドネクストホップ（ODN）を使用して実現されます。ODN により、サービスヘッドエンドルータでは、必要に応じて（オンデマンドで）、BGP ネクストホップに対する SR ポリシーを自動的にインスタンス化できます。ヘッドエンドは、SLA を定義する特定の色の ODN テンプレートで設定され、指定された色のプレフィックスを受信したときにトラフィックパスが最適化されます。プレフィックスは、L3VPN に関連付けられたルートポリシーで定義されます。

Cisco Crosswork Network Controller は、ネットワークの監視を継続し、定義された SLA に基づいてクローズドループでネットワークを自動的に最適化します。

次のトポロジがこのシナリオの基本となります。



このシナリオでは、次の作業を行います。

- エンドポイントで特定の色を使用してセグメントルーティング ODN テンプレートを作成し、指定された色のプレフィックスを受信したときに、トラフィックが LSP（アンダーレイ）内で転送され、ベストパストンネルが動的に作成されるようにします。サービスとリンクの詳細のため、SRv6（IPv6）を有効にします。ODN テンプレートは、パスを最適化する SLA を定義します。この場合は遅延を最適化します。
- 計算されるパスはディスジョイントパスとして指定します。つまり同じリンクを共有しません。
- L3VPN を ODN テンプレートにバインドするために使用するルートポリシーを各エンドポイントに作成します。このルートポリシーは、顧客プレフィックスに色属性を追加し、BGP を介して他のエンドポイントにアドバタイズします。この色属性は、これらのプレフィックスに必要な SLA を示すために使用されます。
- 3 つのエンドポイント（PE-A、PE-B、および PE-C）を使用して L3VPN サービスを作成します。これはオーバーレイ設定です。
- このオーバーレイ/アンダーレイ設定がトラフィックパスを最適化し、SLA を自動的に維持する方法を可視化します。

仮定と前提条件

- SRv6 で ODN を使用するには、プレフィックスの BGP ピアリングをエンドポイントまたは PE 間で設定する必要があります。通常、L3VPN では、VPNv4 および VPNv6 アドレスファミリピアリングとなり、この BGP ピアリングは IPv6 経由である必要があります。

ワークフロー

- 手順 1：SLA 目標と制約に色をマッピングするための ODN テンプレートを作成する
- 手順 2：L3VPN ルートポリシーの作成
- 手順 3： L3VPN サービスの作成およびプロビジョニング
- 手順 4：マップ上の新しい VPN サービスを可視化してトラフィックパスを確認する
- 手順 5：自動ネットワーク最適化の観察

ステップ 1. SLA 目標と制約に色をマッピングするための ODN テンプレートを作成する

この手順では、各エンドポイントに ODN テンプレートを作成します。ODN テンプレートは色と目的を指定します。この場合は、遅延と分離（ディスジョイント）です。この ODN テンプレートは、色が一致するプレフィックスが BGP 経由で受信されたときに、トンネルを（オンデマンドで）動的に作成するために使用されます。これらのプレフィックスへのトラフィックは、新しく作成されたトンネルに自動的に誘導されます。これにより、SLA 目標とこれらのプレフィックスを対象とした制約を満たし、BGP ルートで色を使用してシグナリングされます。
分離の制約は、ディスジョイントグループ ID を ODN テンプレートに関連付けることによって機能し、同じディスジョイントグループ ID を持つすべてのトンネルは分離されます。つまり、これらのトンネルはディスジョイントグループの設定方法に応じて、異なるリンク、ノード、および共有リスクリンクグループを使用します。

次の ODN テンプレートを作成します。

- ヘッドエンド PE-A、色 72、遅延、ディスジョイントパス（リンク）、グループ ID 16：L3VPN_NM-SRTE-ODN_72-a
- ヘッドエンド PE-A、色 71、遅延、ディスジョイントパス（リンク）、グループ ID 16：L3VPN_NM-SRTE-ODN_71-a
- ヘッドエンド PE-B および PE-C、色 70、遅延：L3VPN_NM-SRTE-ODN_70
  - SRv6 対応 ODN テンプレートに複数のヘッドエンドがある場合、ヘッドエンドルータでは同じロケータ名を設定する必要があります。それ以外の場合は、ヘッドエンドごとに異なる ODN テンプレートを作成する必要があります。
- ヘッドエンド PE-B、色 72、遅延：L3VPN_NM-SRTE-ODN_72-b
- ヘッドエンド PE-C、色 71、遅延：L3VPN_NM-SRTE-ODN_71-c

例として、最初の ODN テンプレート：L3VPN_NM-SRTE-ODN_72-a を作成する方法を示します。他の ODN テンプレートも同じ手順で作成できます。

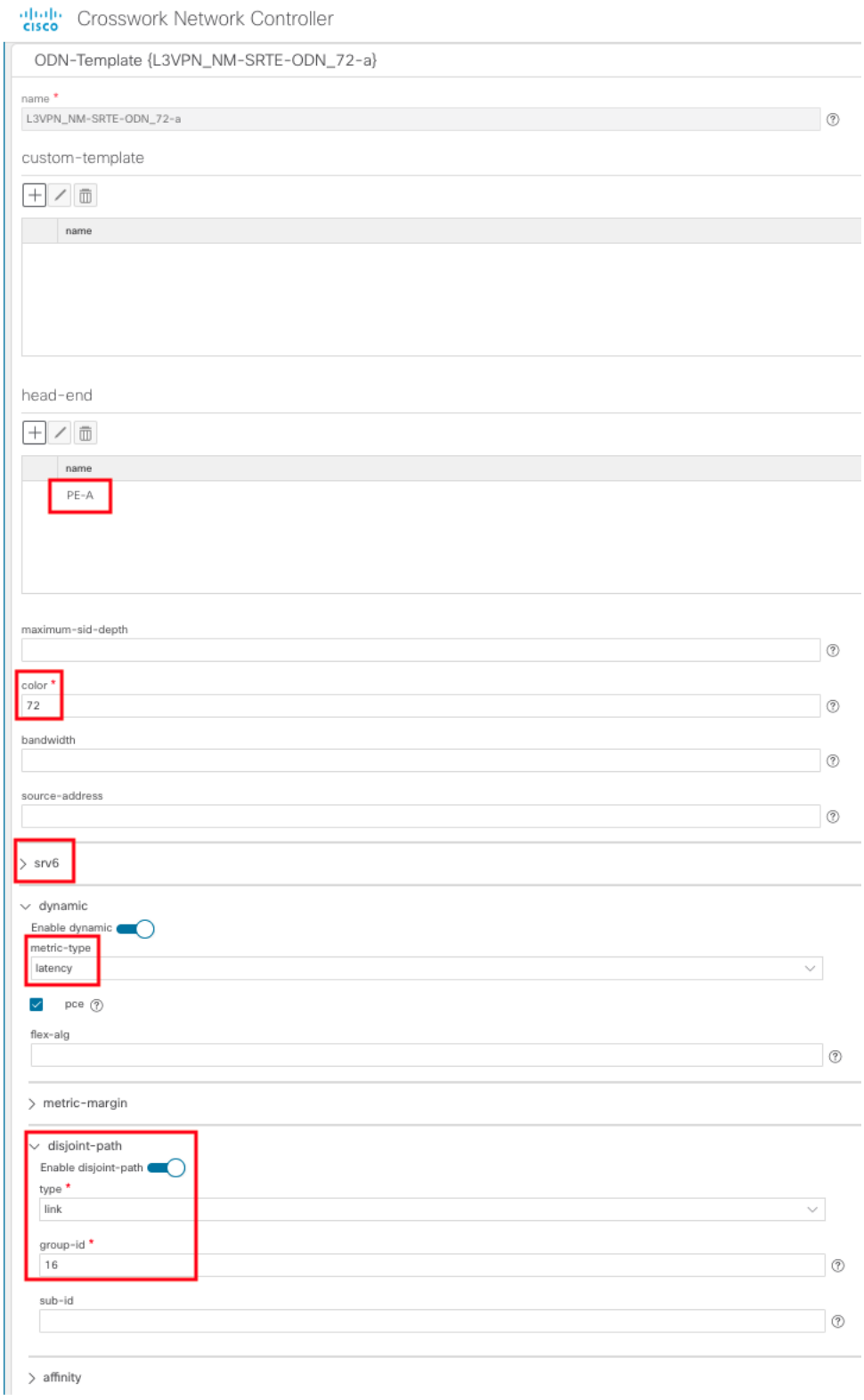
手順

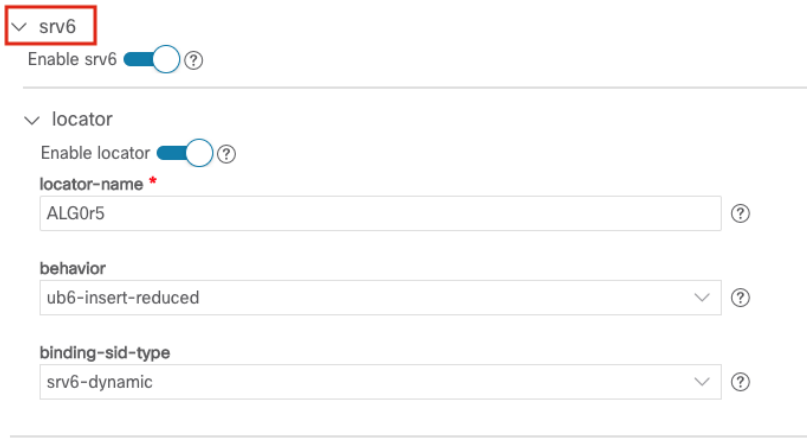
1. [Services & Traffic Engineering] > [Provisioning (NSO)] > [SR-TE] > [ODN-Template] に移動します。
2. [+] をクリックして新しいテンプレートを作成し、一意の名前を付けます。
   この場合、名前は **L3VPN_NM-SRTE-ODN_72-a** です。
3. ヘッドエンドデバイス **PE-A** を選択し、色 **72** を指定します。
4. [srv6] で、[Enable srv6] トグルを選択します。

5. [locator] で、必要な SRv6 の [locator-name] を入力します。

   注： ロケータ名は、ルータで設定されている名前と一致する必要があります。

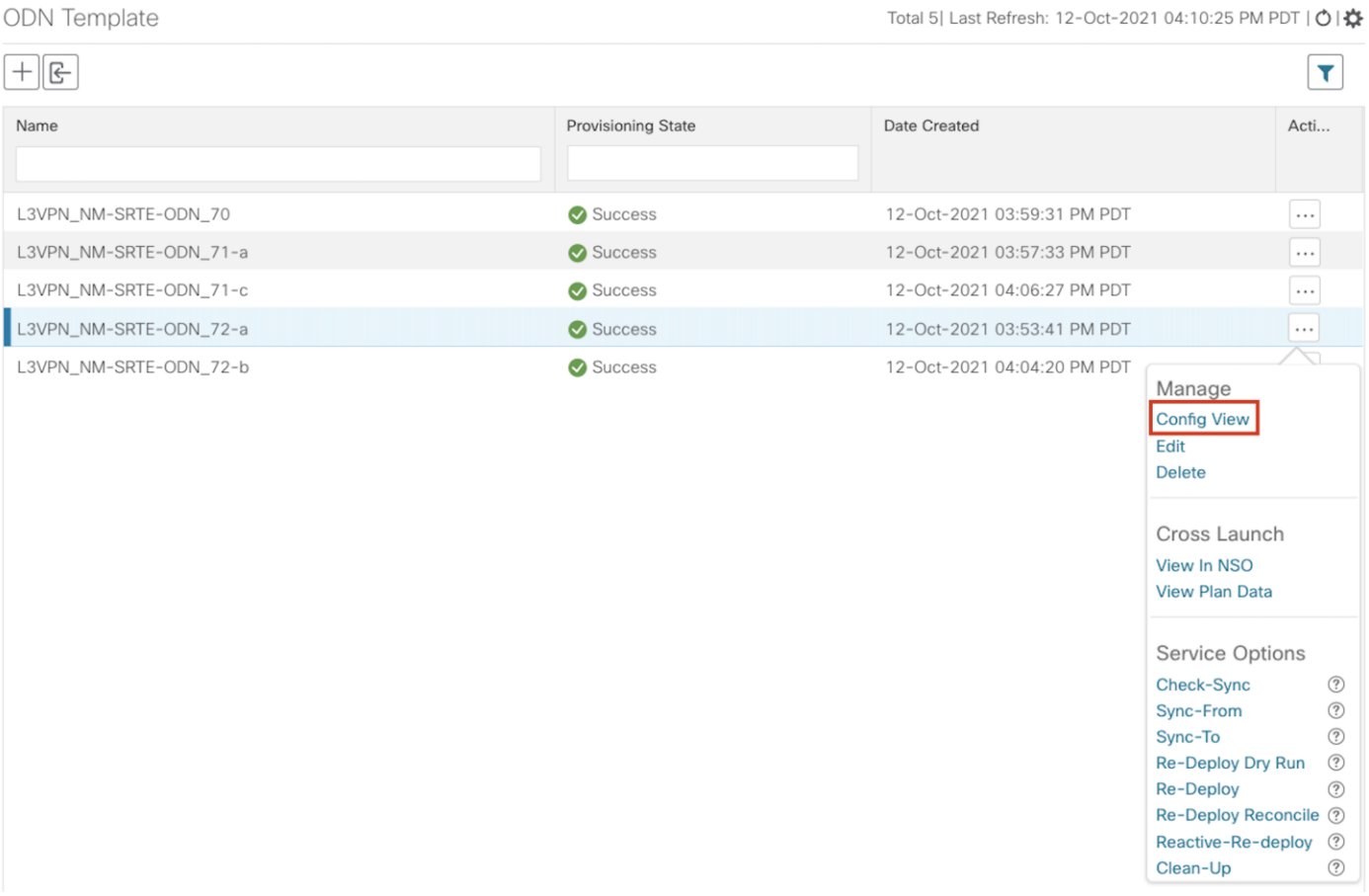
6. [Dynamic] で、メトリックタイプとして [Latency] を選択します。これが最適化の対象となる SLA 目標です。
7. [PCE] チェックボックスをオンにし、パス計算クライアント（PCC）ではなく SR-PCE でパスを計算するように指定します。
8. 必要な制約を定義します。この場合、計算パスはリンクを共有してはならないディスジョイントパスとします。
   [Disjoint-path] で、タイプとして [Link] を選択し、グループ ID の数字（この場合は 16）を指定します。

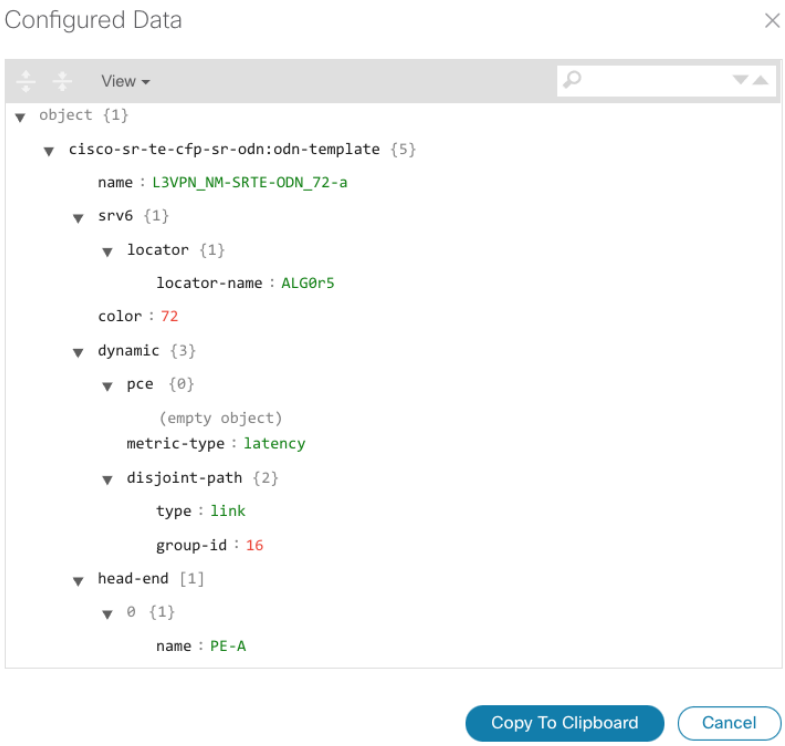




変更を確定するか、[Dry Run] をクリックして、確定する前にデバイスに設定される内容を確認します。

9. 新しい ODN テンプレートがテーブルに表示され、そのプロビジョニング状態が [Success] であることを確認します。[Actions] 列の [...] をクリックし、[Config View] を選択して、作成した ODN テンプレートの詳細を示す YANG モデルベースのサービスインテントデータを表示します。





10. 上記の他の ODN テンプレートを同じ方法で作成します。

ステップ 2. L3VPN ルートポリシーの作成

この手順では、各エンドポイントのルートポリシーを作成し、そのエンドポイントの ODN テンプレートで定義したものと同じ色を指定します。ルートポリシーは、SLA が適用されるプレフィックスを定義します。指定したネットワークから一致する色のトラフィックを受信すると、ODN テンプレートで定義された SLA に基づいてパスが計算されます。

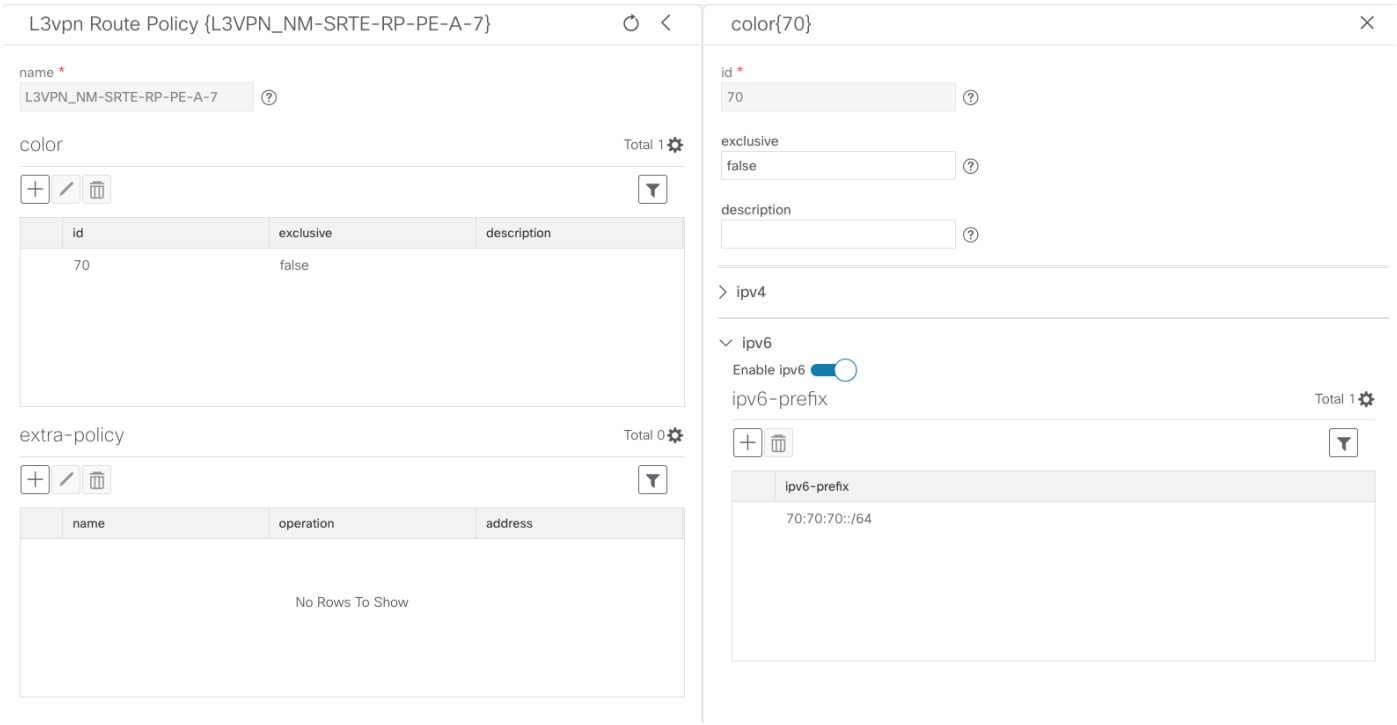
次のルートポリシーを作成します。

- 色 70、IPv6 プレフィックス 70:70:70::0/64：L3VPN_NM-SRTE-RP-PE-A-7
- 色 71、IPv6 プレフィックス 70:70:71::0/64：L3VPN_NM-SRTE-RP-PE-B-7
- 色 72、IPv6 プレフィックス 70:70:72::0/64：L3VPN_NM-SRTE-RP-PE-C-7

例として、最初のルートポリシー：L3VPN_NM-SRTE-PE-A-7 を作成する方法を示します。他のルートポリシーも同じ手順で作成できます。

手順

1. [Services & Traffic Engineering] > [Provisioning] > [L3vpn] > [L3vpn Route Policy] に移動します。
2. [+] をクリックして新しいルートポリシーを作成し、一意の名前を付けます。
3. [Color] の下にある [+] をクリックします。PE-A の ODN テンプレートで指定されている色と同じ色 **70** を指定し、[Continue] をクリックします。
4. ネットワークトラフィックを識別するために必要な IPv6 プレフィックスを入力します。
   この場合、IPv6 プレフィックスは **70:70:70::0/64** です。



5. 右上隅の [X] をクリックして、[Color] ペインを閉じます。
6. 変更を保存します。
7. 新しいルートポリシーがテーブルに表示されることを確認します。
8. 上記の他のルートポリシーを同じ方法で作成します。

   注： L3VPN ルートポリシーを作成すると、各ルートポリシーの VPN プロファイルが自動的に作成されます。VPN プロファイルは、L3VPN サービスから参照されます。これにより、ルートポリシーが L3VPN サービスにバインドされます。この結果、前の手順で作成した各ルートポリシーの VPN プロファイルが作成されます。

   - L3VPN_NM-SRTE-RP-PE-A-7
   - L3VPN_NM-SRTE-RP-PE-B-7
   - L3VPN_NM-SRTE-RP-PE-C-7

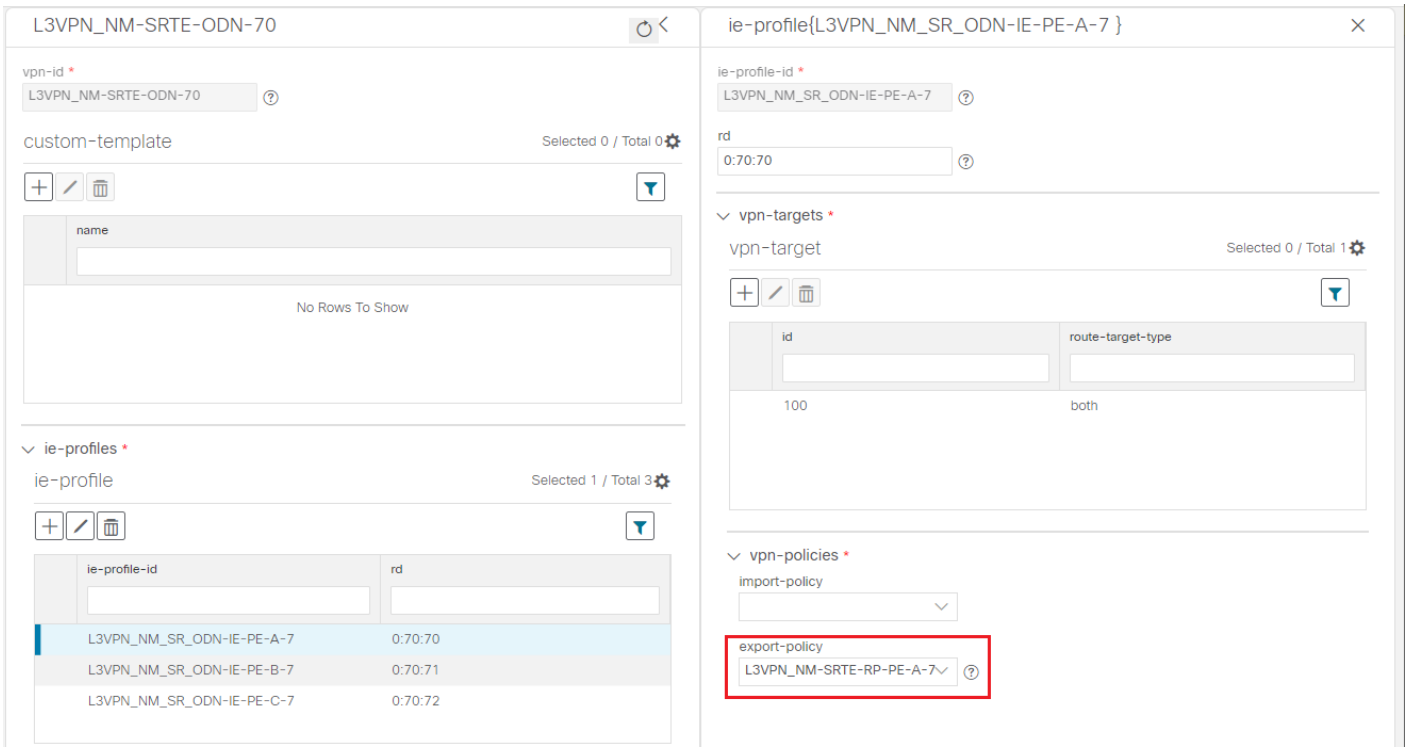
ステップ 3. L3VPN サービスの作成およびプロビジョニング

この手順では、3 つのエンドポイント（PE-A、PE-B、および PE-C）を備えた L3VPN サービスを作成します。各エンドポイントは、IE プロファイルに関連付けられます。IE プロファイルは、ODN テンプレートで指定されたのと同じ色のルートポリシーを含む VPN プロファイルを指します。このようにして、指定されたプレフィックスと色に一致するトラフィックが、SLA 仕様に従って処理されます。

1. [Services & Traffic Engineering] > [Provisioning (NSO)] > [L3vpn] > [L3vpn-Service] に移動します。
2. [+] をクリックして新しいサービスを作成し、一意の名前を付けます。[Continue] をクリックします。
3. IE プロファイルを作成します。これは、ルート識別子（RD）、ルートターゲット、およびエクスポート/インポートルートポリシーを定義するコンテナです。各エンドポイントの IE プロファイルを次のように作成します。

— L3VPN_NM_SR_ODN-IE-PE-A-7、ルート識別子 0:70:70
— L3VPN_NM_SR_ODN-IE-PE-B-7、ルート識別子 0:70:71
— L3VPN_NM_SR_ODN-IE-PE-C-7、ルート識別子 0:70:72

a. [ie-profile] で、[+] をクリックして新しい IE プロファイルを作成し、一意の名前を付けます。
b. ルート識別子を入力します。これにより、IP プレフィックスが区別されて一意になります。
c. ルートターゲットとルートターゲットタイプ（インポート/エクスポート/両方）を含め、必要な VPN ターゲットを定義します。
d. vpn-policies で、エクスポートポリシーのドロップダウンリストから、関連する VPN プロファイル（ルートポリシーを含む）を選択します。これにより、VPN と、SLA を定義する ODN テンプレートの間の関連付けが形成されます。



g. 完了したら、右上隅の [X] をクリックします。
h. 同様に、別の IE プロファイルを作成します。

4. 各 VPN エンドポイント（PE-A、PE-B、および PE-C）を個別に定義します。

a. [vpn-nodes] で [+] をクリックし、ドロップダウンリストから関連するデバイスを選択して、[Continue] をクリックします。
b. ネットワーク ID のローカル自律システム番号を入力します。
c. 前の手順で作成した IE プロファイルを選択します。
d. PE から CE への通信のためのネットワーク アクセス パラメータを定義します。

- [vpn-network-accesses]で、[+] をクリックして、VPN アクセスパラメータの新しいセットを作成し、一意の ID を指定します。[Continue] をクリックします。
- [port-id] フィールドに、この VRF 専用のループバック インターフェイスの名前を入力します。
- [ip-connection] > [IPv6] > [address-allocation-type] で、[static-address] を選択します。

- [static-addresses] の下に、このエンドポイントのネットワークアクセス用の IP アドレスのリストを作成できるテーブルがあります。少なくとも 1 つのアドレスを作成した後、プライマリアドレスを選択できます。アドレステーブルで [+] をクリックして新しいアドレスを作成し、一意の ID を入力します。[Continue] をクリックします。ループバック インターフェイスの IP アドレスとプレフィックス長を指定します。
- 右上隅の [X] をクリックして、VPN ネットワーク アクセス パラメータに戻ります。
- [primary-address] フィールドのドロップダウンリストから、作成したアドレスを選択します。
- ピア AS 番号とローカル AS 番号、IP アドレスタイプ（IPv6）、BGP ネイバーの IP アドレス、BGP ネイバーと PE デバイス間で許可されるホップ数などの BGP ルーティング プロトコル パラメータを定義します。SRv6 を有効にし、アドレスファミリ名とロケータ名を指定します。ロケータ名は、L3VPN PE で設定されているものと一致する必要があります。

e. 完了したら、右上隅の [X] をクリックします。
f. エンドポイントごとにこれらの手順を繰り返します。

5. 変更を確定するか、[Dry Run] をクリックして、確定する前にデバイスに設定される内容を確認します。
6. 新しい L3VPN サービスがテーブルに表示され、そのプロビジョニング状態が [Success] であることを確認します。

ステップ 4. マップ上の新しい VPN サービスを可視化してトラフィックパスを確認する

1. [L3VPN Service] テーブルで、サービス名をクリックするか、[Actions] 列の [...] をクリックして、メニューから [View] を選択します。マップが開き、サービスの詳細がマップの右側に表示されます。

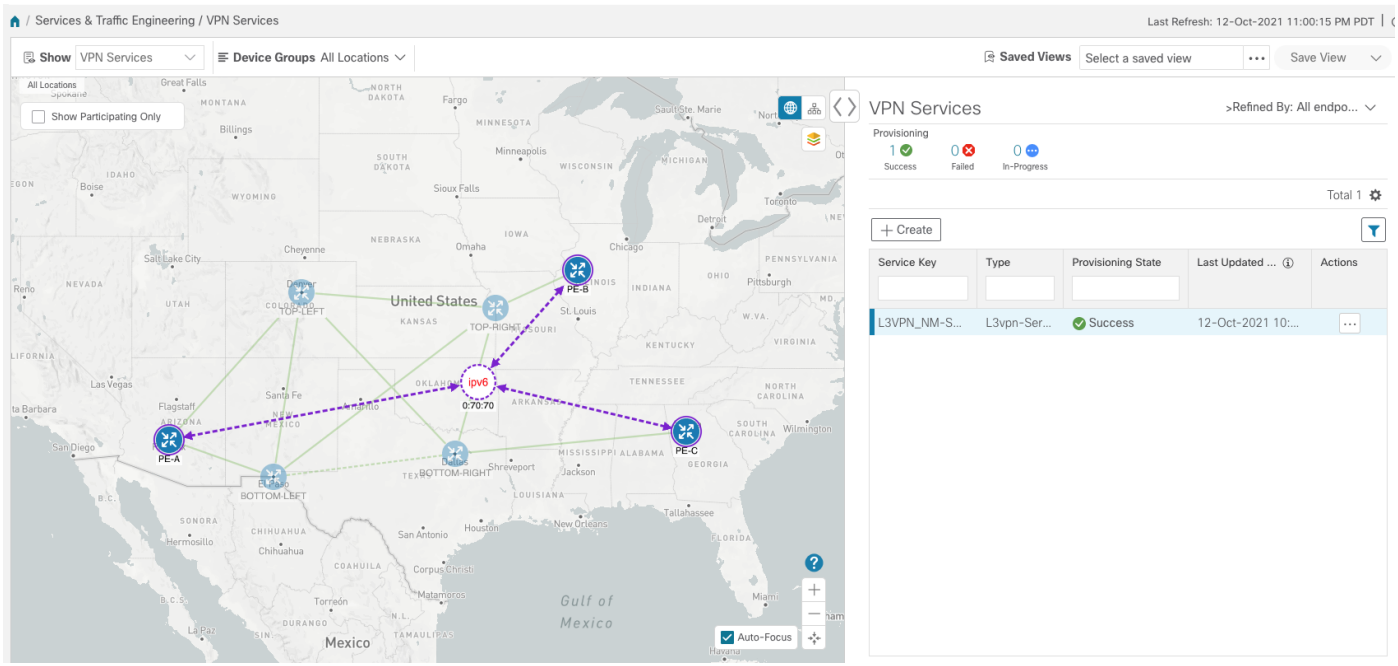
   または

   [Services & Traffic Engineering] > [VPN Services] に移動します。
   マップが開き、マップの右側に VPN サービスのテーブルが表示されます。

   [Services] テーブルで [VPN] をクリックします。テーブルに多数のサービスがある場合は、名前、タイプ、またはプロビジョニング状態でフィルタリングして、VPN を見つけることができます。

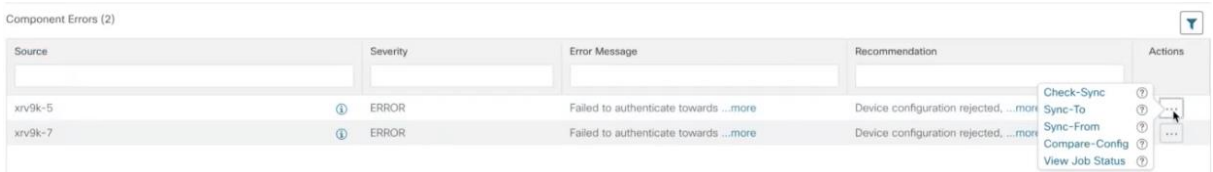
   マップでは、トポロジ上のオーバーレイとして VPN が表示されます。3 つのエンドポイントと、仮想パスであることを示す点線が表示されます。

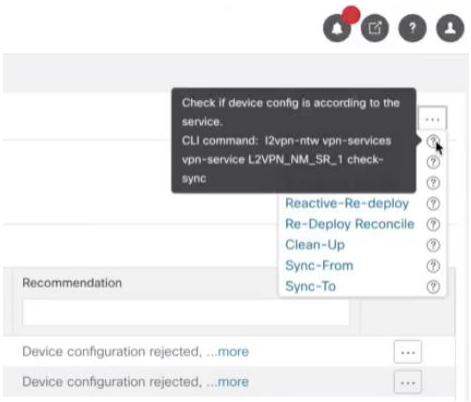
   注： 次の図は、論理マップでの VPN のオーバーレイを示しています。論理マップと地理的マップを切り替えるには、マップの右上にあるボタン  を使用します。



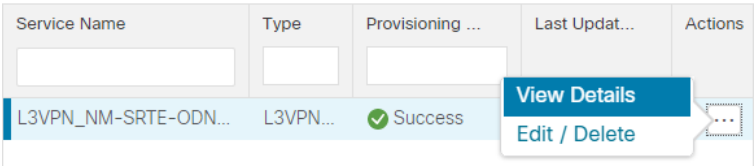
選択した VPN に関係のないデバイスを表示しないようにするには、[Show Participating Only] チェックボックスをオンにします。

注： プロビジョニング状態が「Failed」状態を示すと、情報アイコンが表示されます。これは、[VPN Services]、[Service Details]、およびサービスとそのプロビジョニングステータスのテーブルを表示する多くの [Provisioning] 画面に当てはまります。アイコンを選択すると、障害について説明するエラーメッセージの詳細が表示されます。failure [Show Error Details] リンクをクリックして [Component Errors] 画面を表示し、エラーを修正する措置を実行することもできます。障害が発生したソースごとに、エラーメッセージの詳細と推奨事項が示されます。たとえば、[Component Errors] 画面の障害が発生したソースの [Action] 列で [...] をクリックし、エラーの修正に役立つさまざまなオプションを使用することができます（[Check-Sync]、[Sync-To]、[Sync-From]、[Compare-Config]、[View Job Status] など）。サービスレベルのエラーの修正に役立つ、追加オプションのためのサービスレベルアクションも使用できます（[Re-Deploy]、[Reactive-Re-deploy]、[Re-Deploy Reconcile]、[Clean-up] など）。修正の詳細については、これらのオプションの横に表示される情報アイコンも活用してください。



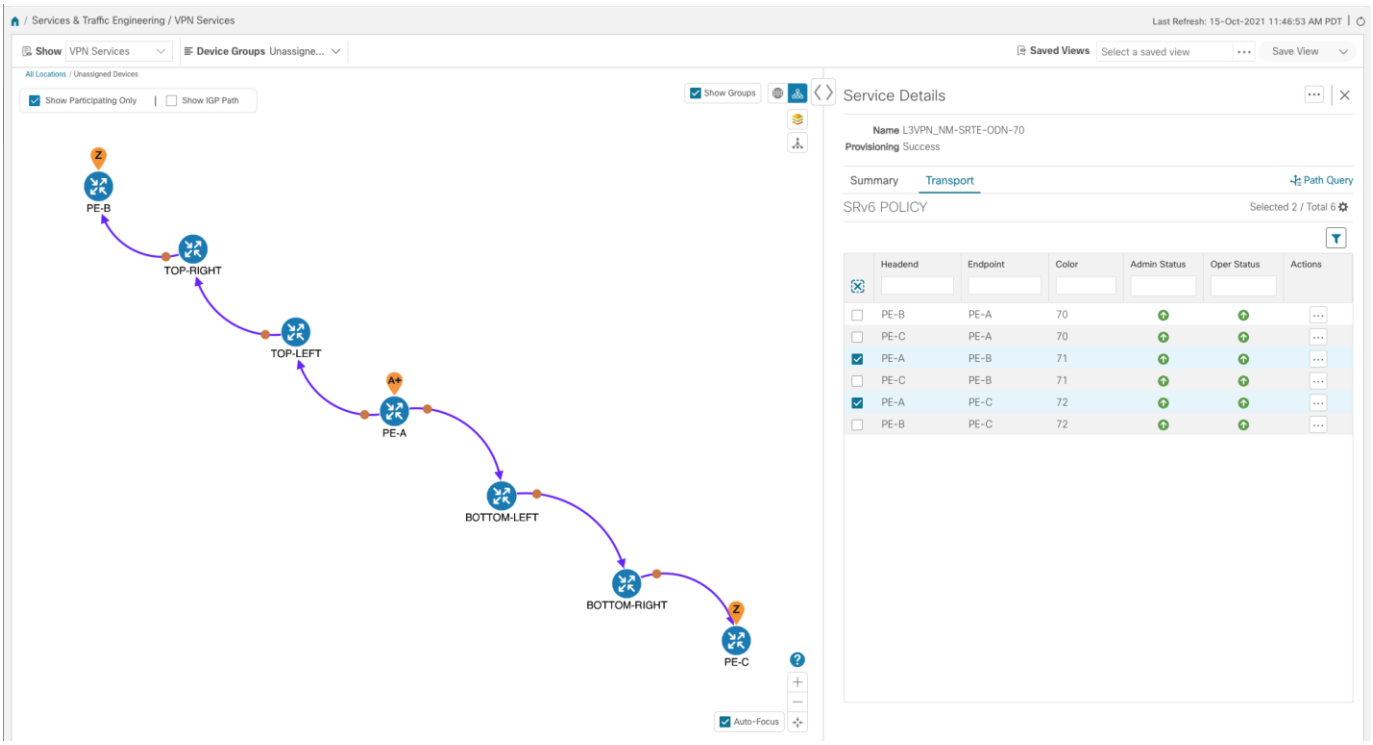


2. [Actions] 列で [...] をクリックすると、デバイス設定や計算されたトランスポートパスなどの VPN サービスの詳細ビューにドリルダウンすることができます。

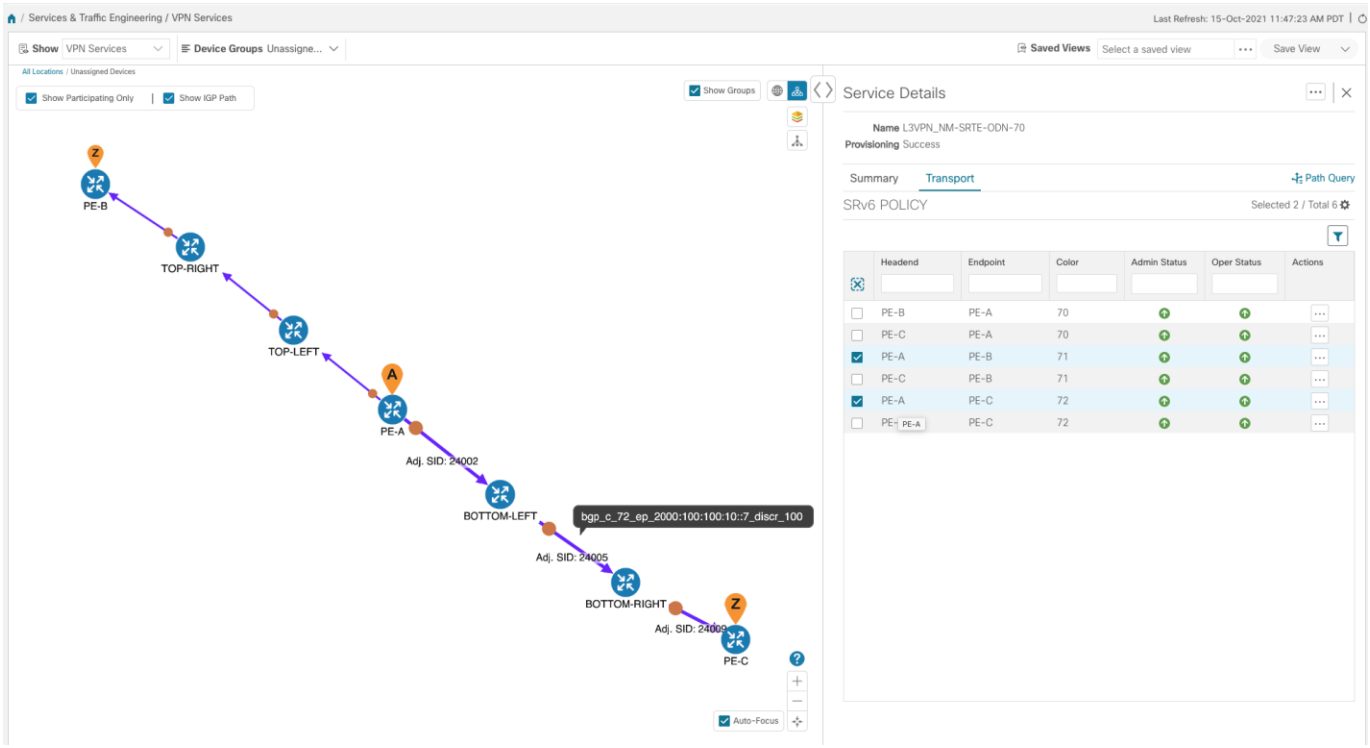


3. この VPN の計算されたパスを表示するには、[Service Details] ペインの [Transport] タブをクリックします。動的に作成されたすべての SR-TE ポリシーが [Transport] タブに表示されます。1 つ以上の SR-TE ポリシーを選択して、マップ上のエンドポイントからエンドポイントまでのパスを確認します。

   この例では、PE-A から PE-B へ、および PE-A から PE-C へと計算されたディスジョイントパスを調べます。



4. エンドポイント間の物理パスを表示するには、マップの左上隅にある [Show IGP Path] チェックボックスをオンにします。テーブル内の選択したポリシーにマウスカーソルを合わせると、マップ内のパスが強調表示され、プレフィックス SID とルーティング情報が表示されます。

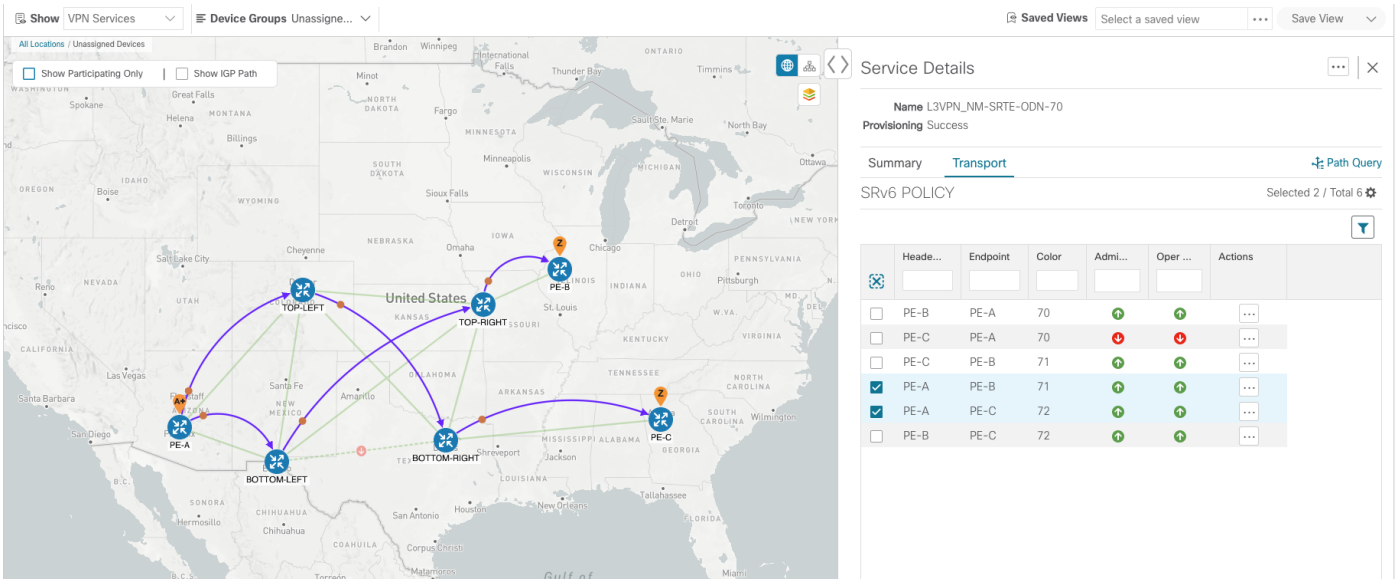


ステップ 5. 自動ネットワーク最適化の観察

SR-PCE は常にネットワークをモニターし、定義された SLA に基づいてトラフィックパスを自動的に最適化します。説明のために、リンクのうち 1 つ（この場合は P-BOTTOMLEFT と P-BOTTOMRIGHT の間のリンク）がダウンした場合の動作を見てみましょう。これは、これまで使用していた PE-A から PE-C へのパスが使用できなくなることを意味します。したがって、SR-PCE は、PE-A から PE-C、および PE-A から PE-B への両方の代替パスを計算して、ダウンしているリンクを補正し、ディスジョイントパスを維持します。

再計算されたパス：

送信元と宛先	古いパス	新しいパス
PE-A > PE-C	PE-A > BOTTOM-LEFT > BOTTOM-RIGHT > PE-C	PE-A > TOP-LEFT > BOTTOM-RIGHT > PE-C
PE-A > PE-B	PE-A > TOP-LEFT > TOP-RIGHT > PE-B	PE-A > BOTTOM-LEFT > TOP-RIGHT > PE-B



まとめと結論

この例で確認したように、Cisco Crosswork Network Controller を使用することで、オペレータは SLA を使用して SRv6 向けに L3VPN をオーケストレーションし、SR-TE ポリシーを使用してこれらの SLA を維持し、ネットワークの状態を継続的に追跡し、自動的に対応してネットワークを最適化できます。この自動化により効率が向上し、手動タスクでは通常回避できない人手によるミスが減少します。

シナリオ 3：明示的 MPLS SR-TE ポリシーを使用した EVPN-VPWS サービスの静的パスの指定

シナリオのコンテキスト

VPN 内のミッションクリティカルなトラフィックが、低容量のインターフェイスではなく、高容量のインターフェイスを通過するようにするため、ポイントツーポイントの EVPN-VPWS サービスを作成し、サービスのインスタンス化のため両方のエンドポイントで優先パス（明示的）MPLS SR-TE ポリシーを関連付けます。このようにして、ミッションクリティカルなトラフィックに対して静的パスを義務付けます。

このシナリオでは、必要なすべての設定を含むファイルをアップロードすることで、SR-TE ポリシーと VPN サービスを簡単かつ迅速に作成する方法を確認します。プロビジョニング UI からサンプルファイル（テンプレート）をダウンロードし、必要なデータを入力して、UI からファイルをインポートします。最後に、Service Health 機能を使用してサービスの健全性を確認し、アシュアランスグラフと過去 24 時間のメトリックを表示して、サービスの健全性の詳細をより適切に分析します。

注： このシナリオで言及する SR-TE とは、特に SR-TE over MPLS を意味します。

このシナリオでは、次の作業を行います。

- SID リスト（プレフィックスまたは隣接セグメント ID のリスト。それぞれがパス上のデバイスまたはリンクを表す）を作成します。
- 明示的な SR-TE ポリシーをプロビジョニングします。このポリシーは SID リストを参照し、EVPN プレフィックスがルーティングされる定義済みのパスを作成します。
- PE-A から PE-C へのポイントツーポイント EVPN-VPWS サービスをプロビジョニングし、明示的な SR-TE ポリシーを適用します。

- サービスのパスを可視化し、サービスの状態を確認します。

仮定と前提条件

- L2VPN サービスへのトランスポートマッピングの場合は、**l2vpn all** コマンドを使用してデバイスを設定する必要があります。
- Service Health を有効にするには、Service Health をインストールする必要があります。

  注： Service Health は、限定提供で使用できます。詳細については、アカウントチームにお問い合わせください。

- （オプション）Service Health は、最大 50 GB のモニタリングデータの**内部ストレージ**を提供します。このデータはシステムに保存されます。内部ストレージの制限を超えると、履歴データが失われます。Service Health のストレージ容量を拡張することを選択した場合は、Amazon Web Services（AWS）クラウドアカウントを使用して、クラウドに**外部ストレージ**を設定できます。外部ストレージを活用することで、既存のすべての内部ストレージデータが外部クラウドストレージに自動的に移動し（詳細については付録「**Service Health 外部ストレージの設定**」を参照）、内部ストレージはキャッシュストレージとしてローカルに機能するようになります。Service Health 用の外部ストレージを設定すると、サービスの正常性をモニターし続けるサービスの履歴データが失われることがなくなり、データの履歴モニタリングサービスを維持するオプションを選択した場合、モニタリングを停止を選択したサービスのサービスヘルスデータが保持されます。内部ストレージと外部ストレージの詳細、および停止時にモニタリングサービスの履歴データを保持する方法については、付録の「**Service Health 外部ストレージの設定**」セクションと「**サービスヘルスモニタリングの停止**」セクションを参照してください。
- Service Health の保証グラフを使用する前に、トポロジマップノードが完全に設定され、サービスに関連付けられたプロファイルで作成されていることを確認します。そうでない場合、[Subservice Details] メトリックに、値がまだ報告されていないと表示されます。
- Service Health では、デバイスに関連付けられた Y1731 プロファイルに 2 つのバケットを設定する必要があります。設定されているバケットが 2 つ未満の場合、Service Health はサービス詳細ページで Y1731 プローブ/KPI を報告できません。

ワークフロー

- 手順 1：SID リストの作成の準備
- 手順 2：プロビジョニング UI での SID リストの作成
- 手順 3：ファイルをインポートして各 VPN エンドポイントの明示的な SR-TE ポリシーを作成する
- 手順 4： L2VPN サービスの作成およびプロビジョニング
- 手順 5：SR-TE ポリシーを L2VPN サービスにアタッチする
- 手順 6：Service Health モニターリングの有効化
- 手順 7：マップでの L2VPN の可視化
- 手順 8：Service Health および過去 24 時間のメトリックを使用して品質が低下したサービスを検査し、問題を特定する

注：　サービスとデータを示す画面キャプチャは、あくまで例として使用されるものであり、ワークフローの内容に記載されているデバイスやデータを常に反映しているとは限りません。

ステップ 1. SID リストの作成の準備

SID リストは、一連のプレフィックスまたは隣接する SID で構成され、それぞれがパス上のノードまたはリンクを表します。各セグメントは、送信元から接続先までのエンドツーエンドのパスであり、ネットワーク内のルータに、IGP によって計算された最短パスではなく指定されたパスに従うように指示します。

SID リストを作成するには、目的の通過パスの MPLS ラベルが必要です。これらのラベルはデバイス自体から取得することも、ノースバウンド Cisco Crosswork Optimization Engine API を呼び出してこの情報を取得することもできます。

API の詳細については、Cisco DevNet の 『Cisco Crosswork Network Automation API Documentation』を参照してください。

手順

1. エンドポイントからエンドポイントへのパスの SID リストを生成するために必要な情報を準備します。次のような各エンドポイントのルータ ID が必要です。

```
'{
  "input": {
    "head-end": "100.100.100.7",
    "end-point": "100.100.100.5",
    "sr-policy-path": {
      "path-optimization-objective": "igp-metric"
    }
  }
}'
```

2. 前の手順で準備した情報を使用して、Cisco Crosswork Network Controller サーバーで API を呼び出します。次に例を示します。

```
curl --location --request POST
'https://10.194.63.198:30603/crosswork/nbi/optima/v1/restconf/operations/cisco-crosswork-
optimization-engine-sr-policy-operations:sr-policy-dryrun' \
--header 'Content-Type: application/yang-data+json' \
--header 'Accept: application/yang-data+json' \
--header 'Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbiIsImlzRnJvbU5ld0xvZ2luIjoidHJ1ZSIsInBvbGljeV9pZCI6ImFkb
WluIiwiYXV0aGVudGljYXRpb25EYXRlIjoiMjAyMS0wMy0yMlQxNjozODozNy43NDY2MTZaW0dNVF0iLCJzdWNjZXNzZnV
sQXV0aGVudGljYXRpb25IYW5kbGVycyI6IlF1ZXJ5RGF0YWJhc2VBdXRoZW50aWNhdGlvbkhhbmRsZXIiLCJpc3MiOiJod
HRwOlwvXC9sb2NhbGhvc3Q6NTQ4OVwvU1NPIiwibGFzdF9uYW1lIjoic21pdGgiLCJjcmVkZW50aWFsVHlwZSI6IlVzZXJ
uYW1lUGFzc3dvcmRDcmVkZW50aWFsIiwiYXVkIjoiaHR0cHM6XC9cLzEwLjE5NC42My4xOTg6MzA2MDNcL2FwcC1kYXNoY
m9hcmQiLCJhdXRoZW50aWNhdGlvbk1ldGhvZCI6IlF1ZXJ5RGF0YWJhc2VBdXRoZW50aWNhdGlvbkhhbmRsZXIiLCJsb25
nVGVybUF1dGhlbnRpY2F0aW9uUmVxdWVzdFRva2VuVXNlZCI6ImZhbHNlIiwiY2hhbmdlX3B3ZCI6ImZhbHNlIiwiZXhwI
joxNjE2NDU5OTIwLCJpYXQiOjE2MTY0MzExMjAsImZpcnN0X25hbWUiOiJqb2huIiwianRpIjoiU1QtODQtOFVlWXMybEt
3R2d1Z3RIYjl4MzVmTFlNTGVVRlp6OURyNGpoeFcxakhsV01VYXdXSWgxbUdTd01aRC1tOEk1S2Z0amI2ZmlWTUhlYnBYY
jBMMFZqRFc2WVppUFVUbHRpNFVpZnNUeG9aQ284WWpPWEc2VlFjS0Mwb29lWjJhc3BWanMzYnA3bHo5VkhySlBCTzl5TDN
GcFRIWXRPeWJtVi1jYXMtMSJ9.Vi4k0w8KsOv5M_O8zBqWochT3k9V9Pn2NjSn5ES9c5Pf-
4ds0o4kk6xuZx5_cggauiEICuUMnzmRzneST-oAuA' \
```

```
--data-raw '{
  "input": {
    "head-end": "100.100.100.5",
    "end-point": "100.100.100.7",
    "sr-policy-path": {
      "path-optimization-objective": "igp-metric"
    }
  }
}'
```

3. API 応答内の SID リスト ID をメモします。これは、次の手順で SID リストを作成するときに使用します。次に例を示します。

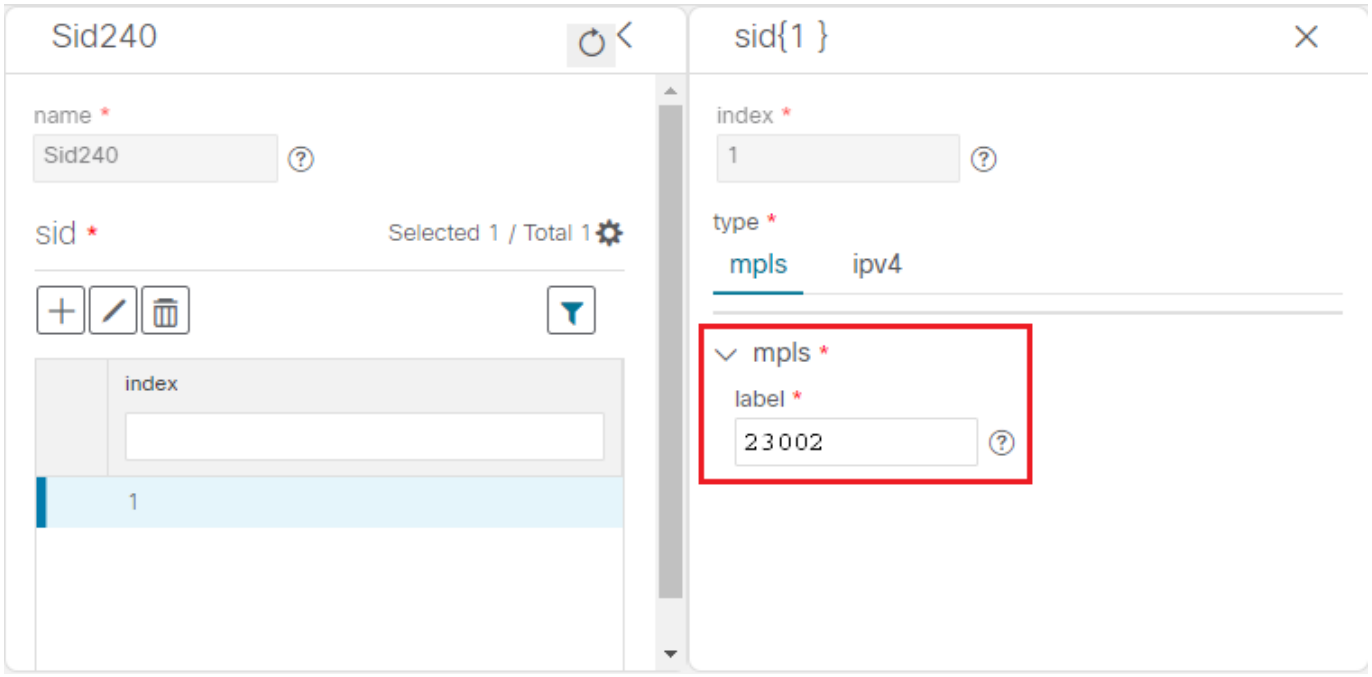
```
{
  "cisco-crosswork-optimization-engine-sr-policy-operations:output": {
    "segment-list-hops": [
      {
        "step": 0,
        "sid": 23002,
        "ip-address": "100.100.100.7",
        "type": "node-ipv4"
      }
    ],
    "igp-route": [
      {
        "node": "PE-A",
        "interface": "GigabitEthernet0/0/0/0"
      },
      {
        "node": "P-TOPLEFT",
        "interface": "GigabitEthernet0/0/0/2"
      },
      {
        "node": "P-BOTTOMRIGHT",
        "interface": "GigabitEthernet0/0/0/3"
      }
    ],
    "state": "success",
    "message": ""
  }
}
```

ステップ 2. プロビジョニング UI での SID リストの作成

このシナリオでは、PE-C から PE-A へのトラフィックの SID リストと、反対方向のトラフィックの別の SID リストを作成します。

手順

1. [Services & Traffic Engineering] > [Provisioning (NSO)] > [SR-TE] > [SID-List] に移動します。
2. [+] をクリックして新しい SID リストを作成し、一意の名前を付けます。この例では、SID リスト名は **L2VPN_NM-P2P-SRTE-PE-C-240** です。[Continue] をクリックします。
3. [SID] で [+] をクリックして新しい SID インデックスを作成し、数値を指定します。[Continue] をクリックします。
4. 手順 1 の API 応答で受信した SID ID を [MPLS] に入力します。



5. 右上隅の [X] をクリックして、SID リストに戻ります。新しい SID がインデックステーブルに表示されます。
6. 必要に応じてこれらの手順を繰り返し、追加の SID インデックスを作成します。
7. 変更を保存します。
8. 新しい SID リストがテーブルに表示されることを確認します。
9. PE-A から PE-C へのトラフィック用に別の SID リストを作成します。この例では、SID リスト名は **L2VPN_NM-P2P-SRTE-PE-A-240** です。

ステップ 3. ファイルをインポートして各 VPN エンドポイントの明示的な SR-TE ポリシーを作成する

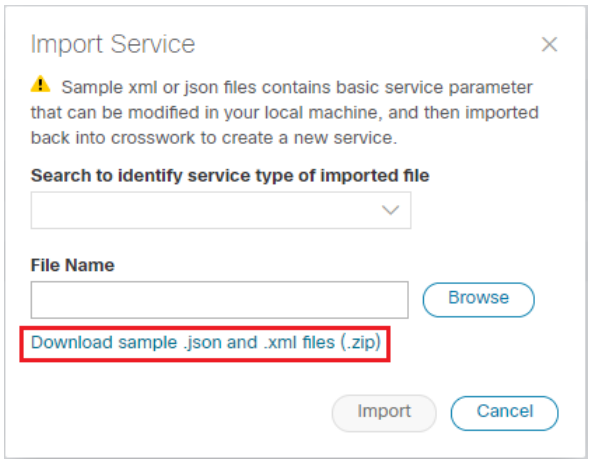
この手順では、手順 1 で作成した SID リストを参照する 2 つの明示的な SR-TE ポリシーをプロビジョニングします。

最初の SR-TE ポリシーは、PE-C をヘッドエンドとして指定し、PE-A の IP アドレスをテールエンドとして提供します。2 番目の SR-TE ポリシーは、PE-A をヘッドエンドとして指定し、PE-C の IP アドレスをテールエンドとして提供します。

プロビジョニング UI の各フィールドに手動で入力する代わりに、SR-TE ポリシーの作成に必要なすべての設定を含む xml ファイルをインポートします。

手順

1. [Services & Traffic Engineering] > [Provisioning (NSO)] > [SR-TE] > [Policy] に移動します。
2. テーブルの上にある [Import] をクリックします。
3. sample.json または .xml ファイルをダウンロードします。このファイルは必要な設定のテンプレートとして機能します。
   [Import Service] ダイアログで、[Download sample.json and.xml files (.zip)] リンクをクリックします。



4. ダウンロードしたファイルを解凍し、XML エディタで sr-Policy.xml を開きます。
5. 必要に応じて xml ファイルを編集します。SR-TE ポリシーの名前を指定し、このポリシーに関連付ける SID リストを指定します。xml ファイルを保存します。

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <sr-te xmlns="http://cisco.com/ns/nso/cfp/cisco-tsdn-sr-te">
    <policies xmlns="http://cisco.com/ns/nso/cfp/cisco-tsdn-sr-te-sr-
policies">
      <policy>
        <name>L2VPN_NM-P2P-SRTE-PE-C-240</name>
        <head-end>
          <name>PE-C</name>
        </head-end>
        <tail-end>100.100.100.5</tail-end>
        <color>240</color>
        <binding-sid>240</binding-sid>
        <path>
          <preference>1</preference>
          <explicit>
            <sid-list>
              <name>L2VPN_NM-P2P-SRTE-PE-C-240</name>
              <weight>1</weight>
            </sid-list>
    </policies>
  </sr-te>
</config>
```

6. [Import Service] ダイアログで、インポートするファイルのタイプとして [Policy] を選択し、編集した xml ファイルを参照して、[Import] をクリックします。ファイルにエラーがある場合は、通知されます。エラーがなければ、ファイルがインポートされます。ポリシーが作成され、それに応じてデバイスが設定されます。
7. 新しい SR-TE ポリシーが [Policy] テーブルに表示され、そのプロビジョニング状態が [Success] であるかどうかを確認します。

8. [Actions] 列の [...] をクリックし、[Config View] を選択して、作成した SR-TE ポリシーの詳細を示す YANG モデルベースのサービスインテントデータを表示します。デバイス自体をチェックして、正しくプロビジョニングされていることを確認することもできます。

ステップ 4. L2VPN サービスの作成およびプロビジョニング

この手順では、エンドポイントとしての PE-A と PE-C を使用して P2P VPN サービスを作成し、プロビジョニングします。VPN サービスは、前の手順で作成した SR-TE ポリシーを参照して、VPN を通過するトラフィックが SID リストで定義されたパスに従うようにします。

SR-TE ポリシーで行ったように、必要なすべての設定を含む xml ファイルをインポートして VPN サービスを作成します。VPN サービスをプロビジョニングしたら、SR-TE ポリシーを関連付けるためにプロビジョニング UI で編集します。

手順

1. [Services & Traffic Engineering] > [Provisioning (NSO)] > [L2vpn] > [L2vpn-Service] に移動します。
2. テーブルの上にある [Import] をクリックします。
3. 手順 3 で sample.json または .xml ファイルをダウンロードしなかった場合は、ここでダウンロードします。
4. XML エディタで l2nm.xml を開きます。
5. 必要に応じて xml ファイルを編集します。L2VPN の名前を指定し、各エンドポイントを設定し、VPN パラメータを定義します。

次に、PE-A の設定例を示します。

```
    vpn-node-id : PE-A
  ▼ signaling-options [1]
    ▼ 0 {2}
        type : vpn-common:t-ldp
      ▼ t-ldp-pwe {1}
        ▼ ac-pw-list [1]
          ▼ 0 {2}
              peer-addr : 100.100.100.5
              vc-id : 240
▼ vpn-network-accesses {1}
  ▼ vpn-network-access [1]
    ▼ 0 {2}
      ▼ connection {2}
          encapsulation-type : vpn-common:dot1q
        ▼ dot1q-interface {2}
            l2-access-type : vpn-common:dot1q
          ▼ dot1q {2}
              c-vlan-id : 240
              physical-inf : GigabitEthernet0/0/0/2
        id  : 240
ne-id : PE-A
```

6. xml ファイルを保存します。
7. [Import Service] ダイアログで、インポートするファイルのタイプとして [l2vpn service] を選択し、編集した xml ファイルを参照して、[Import] をクリックします。ファイルにエラーがある場合は、通知されます。エラーがなければ、ファイルがインポートされます。ポリシーが作成され、それに応じてデバイスが設定されます。
8. 新しい L2VPN サービスが L2VPN Service テーブルに表示され、そのプロビジョニング状態が [Success] であることを確認します。
9. [Actions] 列の [...] をクリックし、[Config View] を選択して、作成した VPN サービスの詳細を示す YANG モデルベースのサービスインテントデータを表示します。デバイス自体をチェックして、正しくプロビジョニングされていることを確認することもできます。

ステップ 5. SR-TE ポリシーを L2VPN サービスにアタッチする

この段階では、作成したプロビジョニング済み L2VPN サービスには、トランスポートパスを定義する SR-TE ポリシーがありません。この手順では、プロビジョニング GUI で L2VPN サービスを編集し、関連する SR-TE ポリシーを各エンドポイントにアタッチして、再プロビジョニングします。

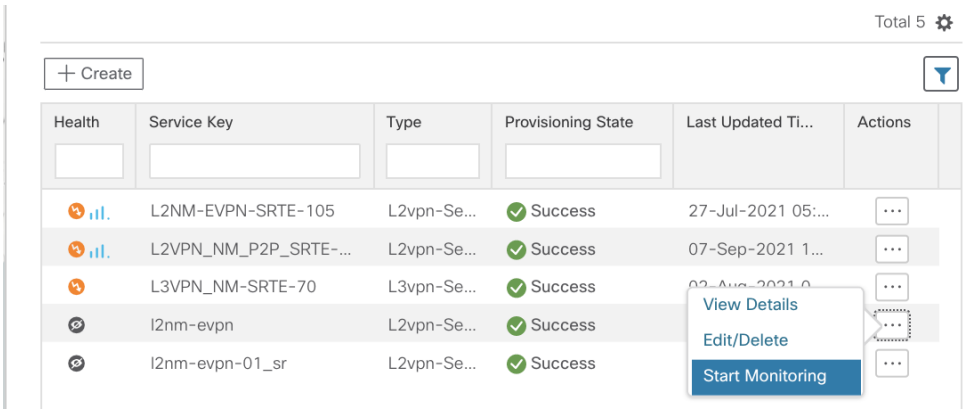
手順

1. [VPN Service] テーブルで L2VPN を探します。
2. [Actions] 列の [...] をクリックし、[Edit] を選択します。
3. [vpn-nodes] で [PE-A] を選択し、テーブルの上の [Edit] ボタンをクリックします。
4. 右側に表示されるペインで、[te-service-mapping] > [te-mapping] セクションを開きます。
5. [sr-policy] タブの [policy] フィールドに、PE-A 用に作成された SR-TE ポリシーの名前を入力します。**L2VPN_NM-P2P-SRTE-PE-A-240**
6. 右上隅の [X] をクリックして、[PE-A] ペインを閉じます。
7. PE-C でも上記の手順を繰り返し、SR-TE ポリシー：**L2VPN_NM-P2P-SRTE-PE-C-240** をアタッチします。
8. [変更内容を確定（Commit Changes）] をクリックします。

ステップ 6. Service Health モニターリングの有効化

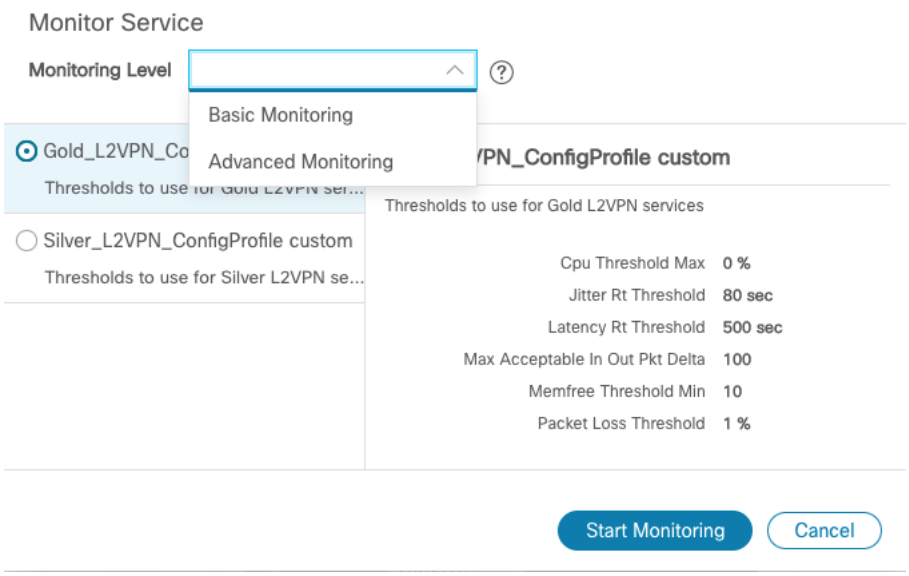
注： Service Health は、限定提供で使用できます。詳細については、アカウントチームにお問い合わせください。

1. [Services & Traffic Engineering] > [VPN Services] に移動します。マップが開き、マップの右側に VPN サービスのテーブルが表示されます。
2. [Actions] 列で、ヘルスモニターリングを開始する新しいサービスの [...] をクリックします。
3. [モニタ開始（Start Monitoring）] をクリックします。

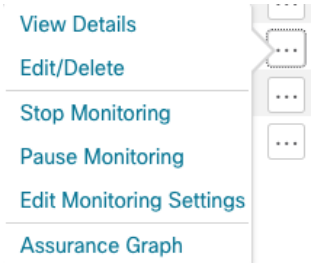


注： [Health] 列の色分けは、サービスの健全性を示します。緑色 = 良好、オレンジ = 低下、赤 = ダウン、グレー = モニターリングなし。

4. [モニターサービス（Monitor Service）] ポップアップで、モニタリングレベルを選択します。必要に応じて適切なモニタリング レベル オプションを選択する方法については、**「基本および詳細モニタリング ルール」**セクションを参照してください。



注： このサービスのヘルスモニタリングが開始された後、[アクション（Actions）] 列で [...] をクリックすると、[モニタリングの停止（Stop Monitoring）]、[モニタリングの一時停止（Pause Monitoring）]、[モニタリング設定の編集（Edit Monitoring Settings）]、[アシュアランスグラフ（Assurance Graph）] など、Service Health の追加オプションが表示されます。



注： [モニタリング設定の編集（Edit Monitoring Settings）] を選択すると、モニタリングレベルの設定を [基本モニタリング（Basic Monitoring）] から [詳細モニタリング（Advanced Monitoring）] に、または [詳細モニタリング（Advanced Monitoring）] から [基本モニタリング（Basic Monitoring）] にいつでも更新できます。

注： すでに開始されているサービスの [モニタリングの停止（Stop Monitoring）] を後で決定した場合、停止したサービスの履歴サービスデータを保持するオプションがあります。追加の手順と詳細については、付録の「**Service Health モニタリングの停止**」セクションを参照してください。

5. [モニタ開始（Start Monitoring）] をクリックします。
6. ヘルスモニターリングを開始するサービスごとにこの手順を繰り返します。
7. 完了したら、右上隅の [X] をクリックします。

ステップ 7. マップでの L2VPN の可視化

この手順では、マップ上の L2VPN の表示を確認し、作成した明示的な SR-TE ポリシーに基づいてトラフィックが PE-A から PE-C へ、およびその逆に PE-C から PE-A へとたどるパスを確認します。

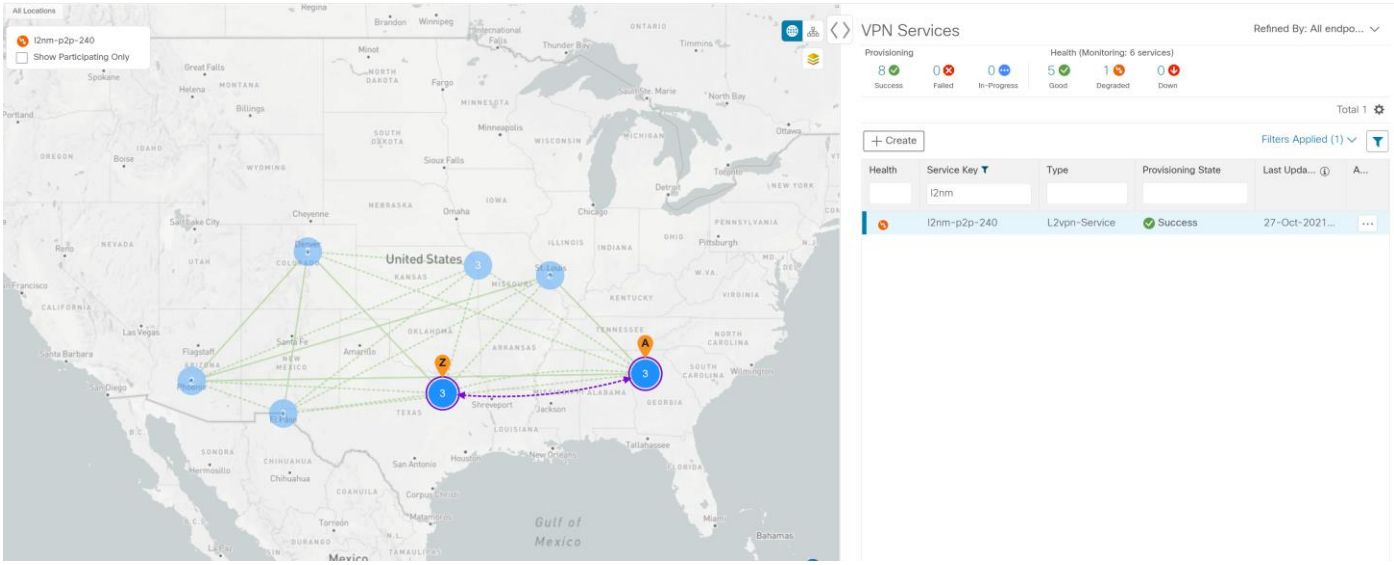
手順

1. [L2VPN Service] テーブルで、新しい VPN の [Actions] 列の [...] をクリックし、メニューから [View Details] を選択します。マップが開き、サービスの詳細がマップの右側に表示されます。

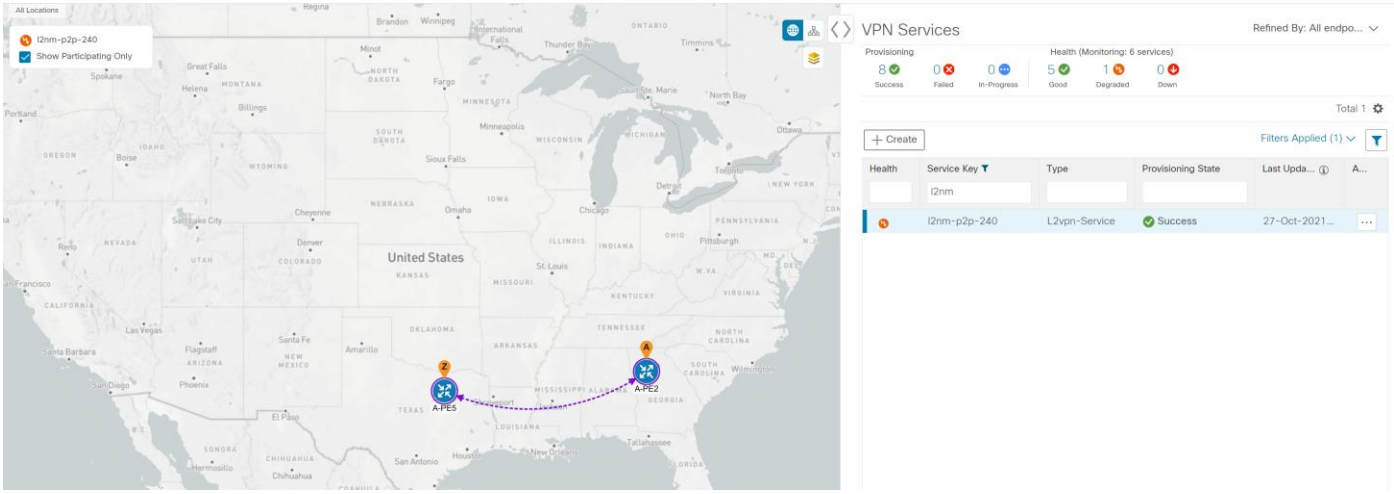
   または

   [Services & Traffic Engineering] > [VPN Services] に移動します。
   マップが開き、マップの右側に VPN サービスのテーブルが表示されます。
   a. [Services] テーブルで [VPN] をクリックします。テーブルに多数のサービスがある場合は、名前、タイプ、またはプロビジョニング状態でフィルタリングして、VPN を見つけることができます。
   b. マップでは、トポロジ上のオーバーレイとして VPN が表示されます。エンドポイントと、仮想パスであることを示す点線が表示されます。

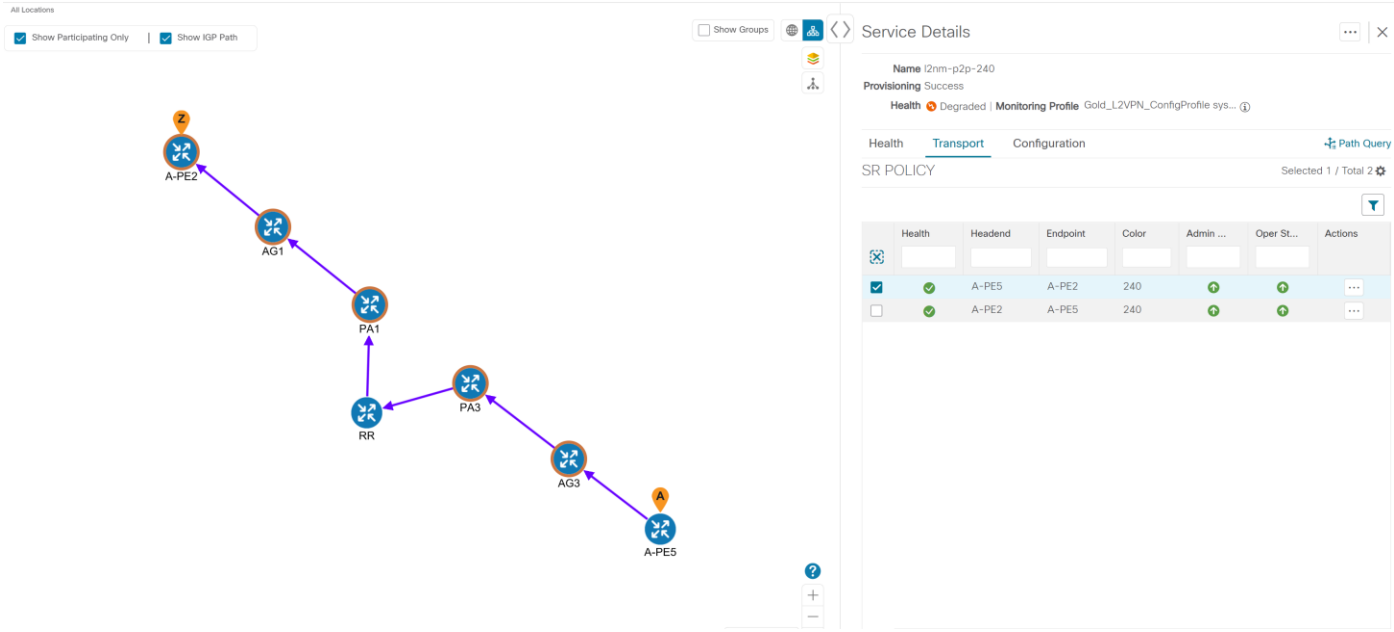
注： 次の図は、地理的マップでの VPN のオーバーレイを示しています。論理マップと地理的マップを切り替えるには、マップの右上にあるボタン を使用します。



c. 選択した VPN に関係のないデバイスを表示しないようにするには、[Show Participating Only] チェックボックスをオンにします。



2. [Actions] 列で [...] をクリックし、[View Details] を選択すると、デバイス設定や計算されたトランスポートパスなどの VPN サービスの詳細ビューにドリルダウンすることができます。
3. [Transport] タブで 1 つ以上の SR-TE ポリシーを選択して、マップ上のエンドポイントからエンドポイントまでのパスを確認します。次の図は、PE-C から PE-A へのパスを示しています。マップの左上隅にある [Show IGP Path] チェックボックスがオンになっているため、物理パスが表示されています。点線は、このリンクが複数のサービスを転送するために使用されていることを示します。



ステップ 8. Service Health および過去 24 時間のメトリックを使用して品質が低下したサービスを検査し、問題を特定する

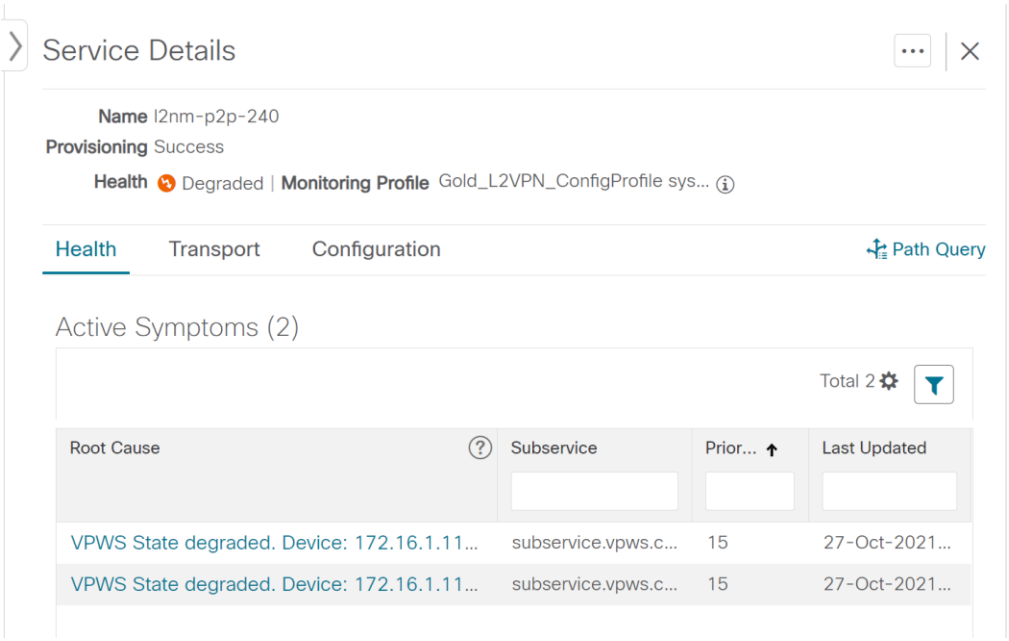
注： Service Health は、限定提供で使用できます。詳細については、アカウントチームにお問い合わせください。

この手順では、Service Health のアシュアランスグラフを確認し、過去 24 時間のメトリックを使用して、特定の時間範囲内の問題を特定します。特定の時間範囲内の問題を分離することで、サービスの低下（またはダウン）を引き起こし、サービスまたはノードのトラブルシューティングにつながる可能性のある詳細情報をドリルダウンして、詳しい症状に対処できます。この例では、低下したサービスを検査します。

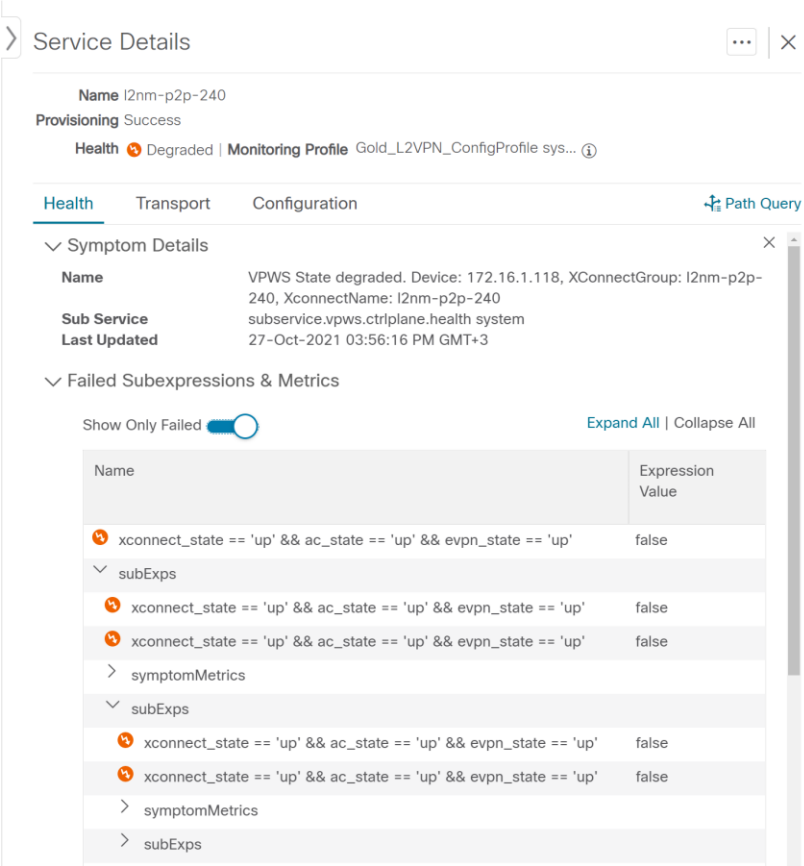
1. 右上隅の [X] をクリックして、[VPN Services] リストに戻ります。
2. 低下と表示されているサービスの名前をクリックします。マップが更新され、選択したサービスが強調表示されます。
   品質が低下したサービスの [Health] 列にオレンジ色のアイコンが表示されます。列の上部にあるスペースをクリックし、適切なフィルタを選択することで、健全性状態ごとにフィルタリングできます。フィルタをクリアするには、列の上部にあるスペースに表示される、指定したフィルタの横にある [X] をクリックします。これにより、すべてのフィルタリングが削除され、デフォルトですべての VPN サービスがリストに表示されます。

   注： サービスがまだ監視されていない場合、[Health] 列のアイコンはグレーで表示されます。このようなサービスのモニターリングを有効にするには、[...] をクリックして[Start Monitoring] を選択します。

3. [Actions] 列で [...] をクリックし、[View Details] をクリックします。右側に [Service Details] パネルが表示されますので、サービスのアクティブな症状（根本原因、サブサービス、優先度、最終更新の詳細を含む）を確認できます。これらの情報は、サービスを現在監視中の場合に [Health] タブに表示されます。表示されている詳細情報を確認します。



4. [Root Cause] をクリックし、症状の詳細と、失敗した部分式とメトリックに関する情報の両方を確認します。



5. 品質が低下したサービスの詳細をさらに分離するには、右上隅の [X] をクリックして、[VPN Services] リストに戻ります。

6. 再度、リスト内の品質が低下したサービスの名前をクリックします。マップが更新され、そのサービスに参加している対応するデバイスが分離されます。以下を実行し、マップ内でサービスヘルスのさらなる詳細情報を確認します。

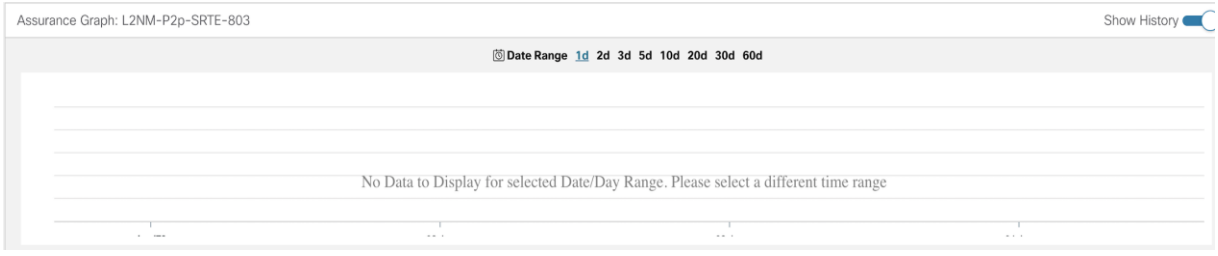
    a. マップで、品質低下と表示されているデバイスと、ヘルスステータスを示す小さなバッジの上にマウスを合わせ、その到達可能性状態、ホスト名、ノード IP、およびタイプに関連するポップアップ情報を確認します。
    b. マップパネルの左上にある [Show Participating Only] チェックボックスをオンにして、マップに参加しているサービスのみを表示することもできます。

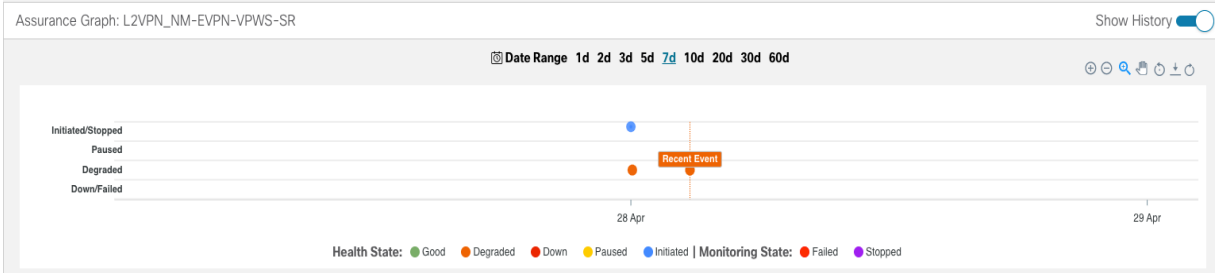
7. [Actions] 列で、リスト内の品質が低下したサービスの [...] をクリックし、[Assurance Graph] をクリックします。サービスとサブサービスのトポロジマップが表示され、[Service Details] パネルにサービスキー、ステータス、およびサブサービスの詳細が表示されます。Jitter-RT（ジッターラウンドトリップ）、Latency-RT（遅延ラウンドトリップ）、PktLoss-DS（宛先から送信元へのパケット損失）、および PktLoss-SD（送信元から宛先へのパケット損失）などのメトリックも表示されます。さらに、根本原因、サブサービス、優先度、および最終更新の詳細が一覧表示されたアクティブな症状の表も表示されます。

    注： サービスのモニターリングが有効になった後の更新には時間がかかります。最大 5 ～ 10 分かかる場合があります。

8. 画面の右上で、[Show History] モード切り替えボタンを選択します。過去の日付範囲グラフが表示されます。このグラフには、1 日（1d）から 60 日間（60d）まで、さまざまな範囲の過去のヘルス サービス モニターリングの詳細が表示されます。
右上の [+] アイコンを選択してイベントを拡大したり、マウスを使用してイベントの上に四角形を描画してさらに拡大したりできます。
連続するイベントは、空白の行として表示される場合があります。

    注： [Show History] を選択すると、デフォルトで 1 日分（**1d**）の [Date Range] グラフが開きます。過去 1 日間または過去数日間（**1d** から **3d** など）に重要なイベントが発生していない場合は、表示できるデータがない可能性があります。表示できるデータ収集範囲を広げるには、**5d** から始まる別の時間範囲を選択します。

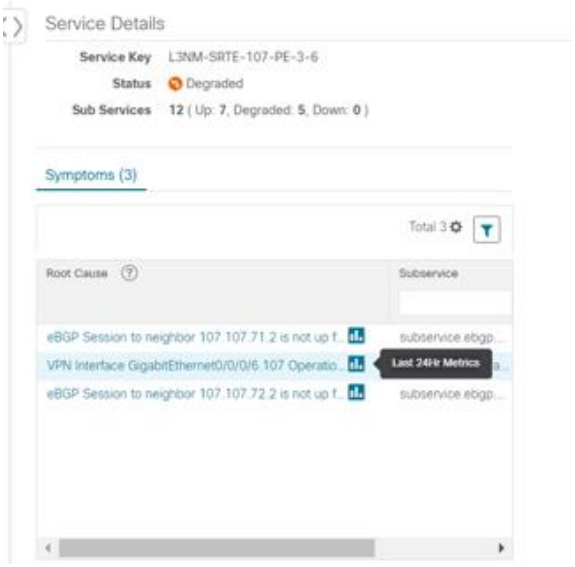




注： [Date Range] グラフでイベントを選択すると、そのイベントに関する情報（イベントの日時、シビラティ（重大度）、症状の数など）を示すツールチップが表示されます。ツールチップを非表示にするには、チャート内の任意の場所をクリックします。

9. 特定の行にマウスを合わせるか、矢印をクリックして [Service Details] パネルを全画面モードに展開することで、根本原因情報を確認します。マウスを使用して列のサイズを変更したり、歯車アイコンを選択して表示列を選択または選択解除したりすることができます。

   注： [Show History] モードを有効にすると、[Active Symptoms] テーブルの根本原因情報に、[Last 24Hr Metrics] の青色のアイコンが表示されます。ただし、最初はデバイスからのデータ受信が遅れ、過去 24 時間のメトリックにデータが入力されるまで多少時間がかかる場合があります。それまでは、値はゼロとして報告されます。



10. マップを使用して品質が低下したノードをクリックすると、[Active Symptoms] と [Impacted Services] の両方のサービス詳細情報が表示されます。

    - **Active Symptoms：**アクティブに監視中のノードに関する症状の詳細を提供します。
    - **Impacted Services：**ヘルスステータスのモニターリング履歴に基づいて、問題によって影響を受けるサービスに関する情報を提供します。

    注： [Subservice Details] パネルを表示すると、各サブサービスメトリック（Jitter-RT、Latency-RT、PktLoss-DS、PktLoss-SD）の初期値はゼロとして報告されます。デバイスの設定によっては、メトリック値の報告が始まるまでに最大 10 分かかる場合があります。

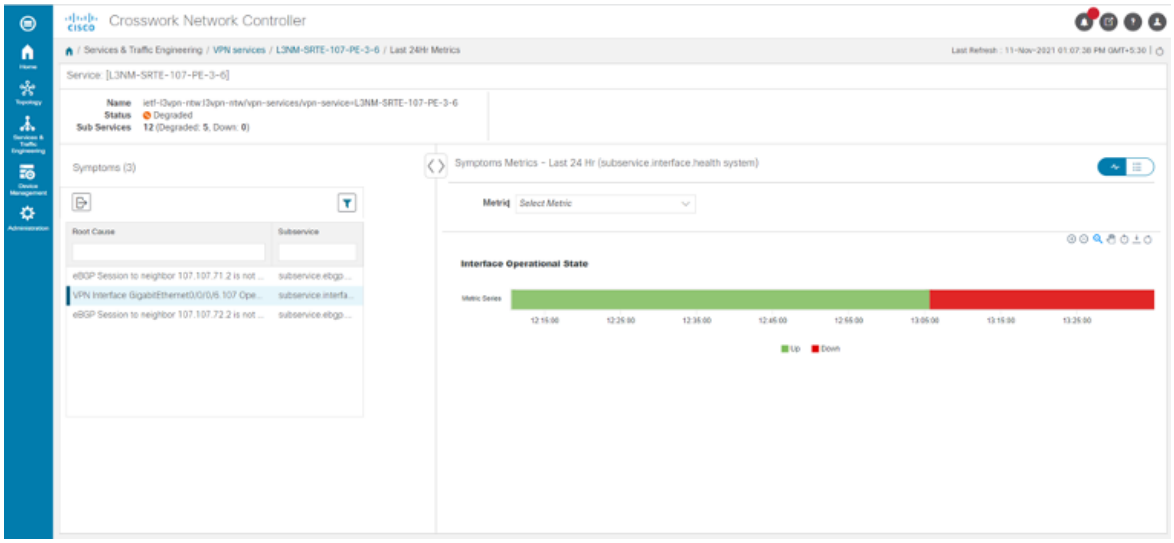
11. アクティブな情報と影響を受ける情報を使用して、品質が低下したサービスの詳細を調べ、サービス低下の原因となった問題を特定します。

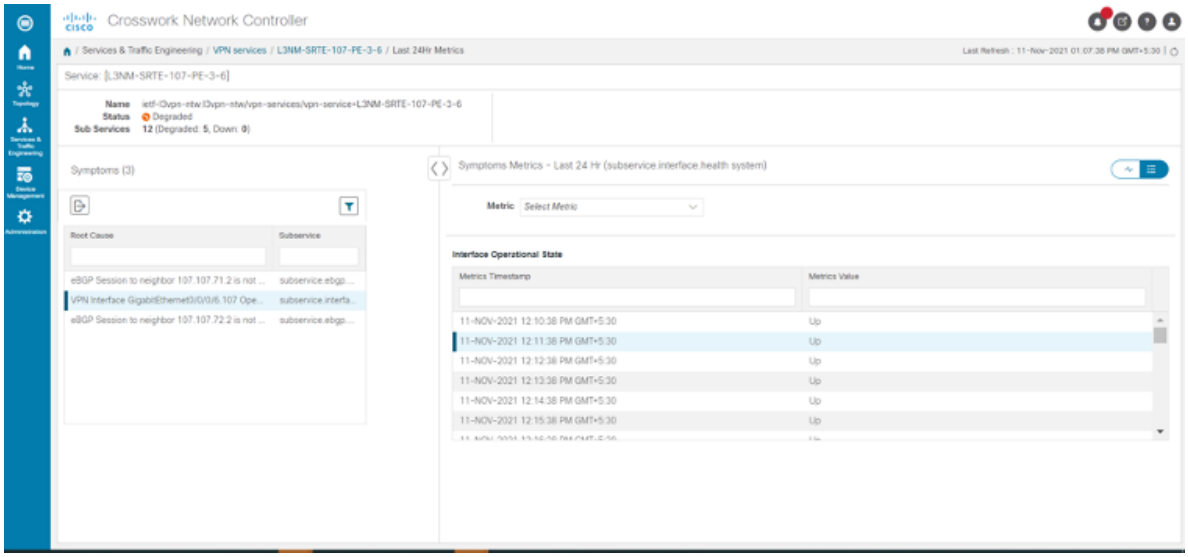
12. 発生する可能性のある問題をさらに分離し、過去 24 時間のメトリックを利用するには、次の手順を実行します。

    a. [Date Range] グラフで、マウスを使用して 1 日（1d）から 60 日間（60d）までの範囲で過去のヘルス サービス モニターリングの詳細を選択します。

注： [Date Range] グラフの右上で、該当するアイコンを選択してズームインまたはズームアウトしたり、日付範囲を横方向にスクロールしたり、グラフを更新して最新のイベントに戻ったりできます。また、マウスを使用してイベントの上に四角形を描画し、性能が低下したデバイスをさらに拡大することもできます。連続するイベントは、空白の行として表示される場合があります。

b. グラフ内の品質が低下したサービスをクリックします。[Service Details] パネルがリロードされ、アクティブな症状と検査が必要な根本原因が表示されます。詳細については、必要に応じてテーブルと情報を展開します。





13. 次に、マップの左上隅にある [Show: Down & Degraded Only] チェックボックスをオンにして、低下しているサブサービスと、依存しているが正常である他のサブサービスのみが表示されるようにします。アクティブな症状とその根本原因を示す [Service Details] パネルを調べます。

14. [Show: Down & Degraded Only] チェックボックスをオフにし、マップの左上隅にある [Soft Dependencies] チェックボックスをオンにします。ソフト依存関係は、子のサブサービスの健全性と、親の健全性との相関が弱いことを意味します。その結果、子の健全性が低下しても、親の健全性は低下しません。
マッピングされたサービスをズームインまたはズームアウトするには、マップの右下隅にある [+] または [-] 記号を使用します。[?] を選択すると、すべてのアイコン、記号、バッジ、色、およびそれらの定義を説明するリンクと色の凡例が表示されます。

    注： マップの右上隅にある [Subservices] アイコンを選択して、サービスの外観オプションを表示することもできます。

15. サブサービスの詳細を確認するには、マップ内の品質が低下したサービスを選択します。
16. 表示されたサービスヘルス情報の根本原因を確認するには [Active Symptoms] タブを選択し、健全性が低下したサービスを確認するには [Impacted Services] タブを選択します。
17. 右上隅の [X] をクリックして[VPN Services] リストに戻ります。[Actions] 列でリスト内の品質が低下したサービスの [...] をクリックし、[Assurance Graph] をクリックして [Service Details] パネルを表示します。
18. 再度、[Service Details] パネルの右上隅にある [Show History] 切り替えボタンを選択してから、[Root Cause] 行の 1 つで青色のメトリックアイコンを選択します。[Symptoms Metrics – Last 24 Hr] の棒グラフが表示されます。
このグラフには、個々の根本原因の症状に対するさまざまなセッション状態（アクティブ、アイドル、失敗など）のメトリックパターンが詳しく表示されるため、優先される問題のトラブルシューティングに役立ちます。詳細を表示するには、グラフにマウスカーソルを合わせます。

パラメータ化されたジョブを使用して、サービス正常性の問題のトラブルシューティングを続行します。

サービス正常性の問題（データを適切に取得できないために機能が低下しているデバイスなど）をさらにトラブルシューティングするには、次の手順に進み、問題が収集ジョブに関連しているかどうかを調べます。

19. [管理（Administration）] > [収集ジョブ（Collection Jobs）] を選択します。
[収集ジョブ（Collection Jobs）] 画面が表示されます。
20. [パラメータ化されたジョブ（Parameterized Jobs）] タブを選択します。
21. [パラメータ化されたジョブ（Parameterized Jobs）] リストを確認して、サービス正常性低下の問題が発生している可能性のあるデバイスを特定します。
[パラメータ化されたジョブ（Parameterized Jobs）] を確認することにより、GMNI、SNMP、および CLI ベースのジョブをコンテキスト ID（プロトコル）によって識別して絞り込み、さらにトラブルシューティングを行うことができます。
22. [ジョブの詳細（Job Details）] パネルで、エクスポートする収集ジョブを選択し、[エクスポート（Export）] ボタンをクリックして、収集ジョブのステータスをダウンロードし、さらに調査を進めます。提供される情報は、エクスポートが開始された時点で .csv ファイルに収集されます。
[収集ステータスのエクスポート（Export Collection Status）] ポップアップが表示されます。

    注： 収集ステータスをエクスポートする場合は、エクスポートを実行するたびに情報を入力する必要があります。さらに、[収集ステータスのエクスポート（Export Collection Status）] ポップアップで利用可能な [エクスポートされたファイルを復号する手順（Steps to Decrypt Exported File）] を確認して、エクスポートされた情報にアクセスして表示できることを確かめてください。

23. [エクスポート（Export）] をクリックします。
24. エクスポートされた収集ジョブデータのステータスを確認するには、[ジョブの詳細（Job Details）] パネルの右上にある [エクスポートステータスの表示（View Export Status）] をクリックします。[ステータスのエクスポートジョブ（Export Status Jobs）] パネルが表示され、エクスポート要求のステータスが示されます。
25. 収集ジョブの詳細とデバイス機能低下の考えられる原因について、エクスポートされた .csv ファイルを確認します。

まとめと結論

このシナリオでは、明示的な SR-TE ポリシーを作成し、それらを L2VPN サービスにアタッチして、ミッションクリティカルなトラフィックに静的パスを義務付けることが簡単に行えることを確認しました。事前定義されたテンプレートを編集し、それをシステムにインポートすることで、サービスと SR-TE ポリシーを迅速かつ簡単にプロビジョニングできることを確認しました。その後、実際のトラフィックパスをマップ上で可視化することができました。最後に、Service Health を使用して、アシュアランスグラフ、過去 24 時間のメトリック、および SubExpressions メトリックを使用して新しいサービスの健全性をモニターし、サービスの稼働、品質低下、またはダウン状態と、どの根本原因が特定されたかを確認しました。

シナリオ 4：予約済み帯域幅を持つ RSVP-TE トンネルを介した L2VPN サービスのプロビジョニング

シナリオのコンテキスト

ビデオや音声といったデータ量が多いメディアタイプで要求される連続ストリーム伝送では、より高いサービス品質を提供するために帯域幅の予約が必要になることがよくあります。Cisco Crosswork Network Controller は、個々のフローに保証帯域幅を予約するための RSVP-TE トンネルの作成と管理をサポートします。RSVP は、フローのパス内のすべてのノードに帯域幅予約を要求する、フロー単位のプロトコルです。エンドポイント、またはエンドポイントに代わる他のネットワークデバイスは、フローが許可される前に予約を確立するためのユニキャスト シグナリング メッセージを送信します。合計帯域幅予約が特定の LSP セグメントで使用可能な帯域幅を超えると、LSP は別の LSR を介して再ルーティングされます。帯域幅予約をサポートできるセグメントがない場合、LSP セットアップは失敗し、RSVP セッションは確立されません。

このシナリオでは、次の作業を行います。

- 予約済み帯域幅を持つ RSVP-TE トンネルを作成します。
- 帯域幅オンデマンド機能を有効にします。
- PE-A から PE-B に VPN サービスをプロビジョニングし、RSVP-TE トンネルをアンダーレイ設定としてアタッチします。
- リンクの使用率が帯域幅のしきい値を下回っている場合のトラフィックのパスを可視化します。リンクの帯域幅使用率が指定されたしきい値を超えると、このパスが変更されます。

仮定と前提条件

- L2VPN サービスへのトランスポートマッピングの場合は、**l2vpn all** コマンドを使用してデバイスを設定する必要があります。
- Service Health を有効にしてサービスの健全性をモニターするには、Service Health をインストールする必要があります。
- （オプション）Service Health は、最大 50 GB のモニタリングデータの**内部ストレージ**を提供します。このデータはシステムに保存されます。内部ストレージの制限を超えると、履歴データが失われます。Service Health のストレージ容量を拡張することを選択した場合は、Amazon Web Services（AWS）クラウドアカウントを使用して、クラウドに**外部ストレージ**を設定できます。外部ストレージを活用することで、既存のすべての内部ストレージデータが外部クラウドストレージに自動的に移動し（詳細については付録「**Service Health 外部ストレージの設定**」を参照）、内部ストレージはキャッシュストレージとしてローカルに機能するようになります。Service Health 用の外部ストレージを設定すると、サービスの正常性をモニターし続けるサービスの履歴データが失われることがなくなり、データの履歴モニタリングサービスを維持するオプションを選択した場合、モニタリングを停止を選択したサービスのサービスヘルスデータが保持されます。内部ストレージと外部ストレージの詳細、および停止時にモニタリングサービスの履歴データを保持する方法については、付録の「**Service Health 外部ストレージの設定**」セクションと「**サービスヘルスモニタリングの停止**」セクションを参照してください。
- （オプション）サービスの正常性をモニターするためのヒューリスティック パッケージの初期化については、付録の「**サービスの正常性をモニターするためのヒューリスティック パッケージの初期化**」セクションを参照し、モニタリングを開始する前に実行すべき詳細な手順を確認してください。

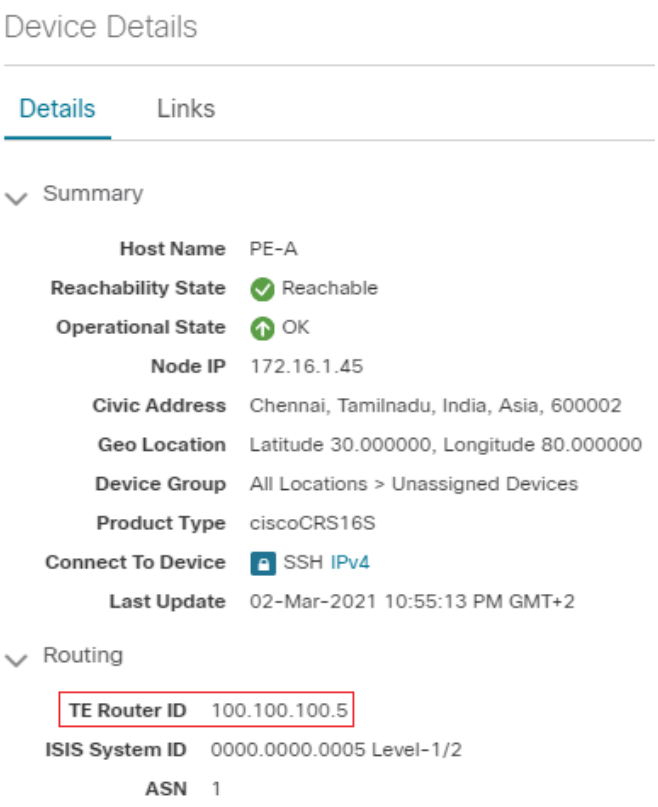
ワークフロー

- 手順 1：L2VPN の両方向に RSVP-TE トンネルを作成する
- 手順 2：L2VPN サービスを作成し、RSVP トンネルをサービスにアタッチする
- 手順 3：マップで L2VPN サービスを可視化する

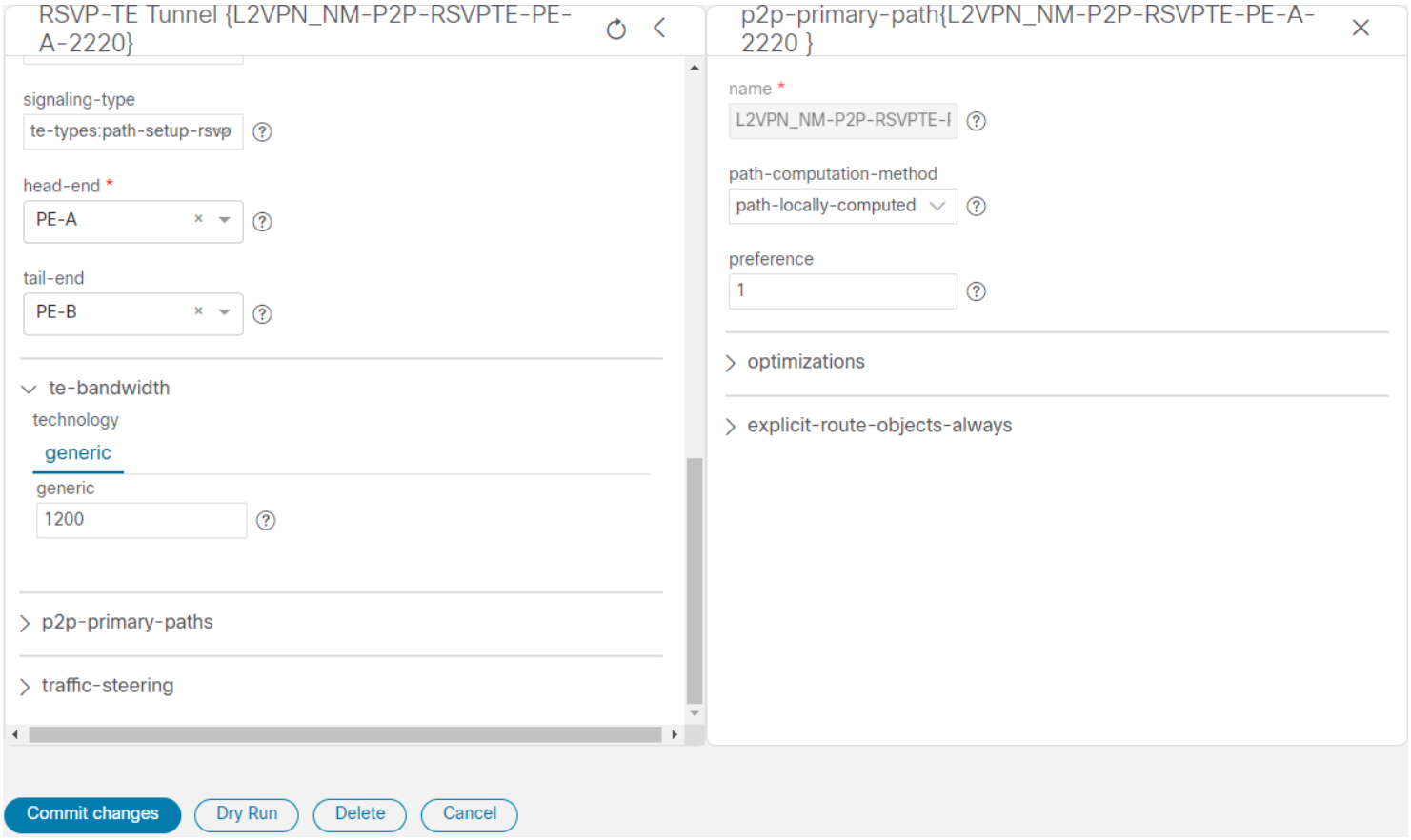
ステップ 1. L2VPN の両方向に RSVP-TE トンネルを作成する

この手順では、PE-A から PE-B、および PE-B から PE-A への RSVP-TE トンネルを作成し、リンク上に帯域幅 1200 を予約します。

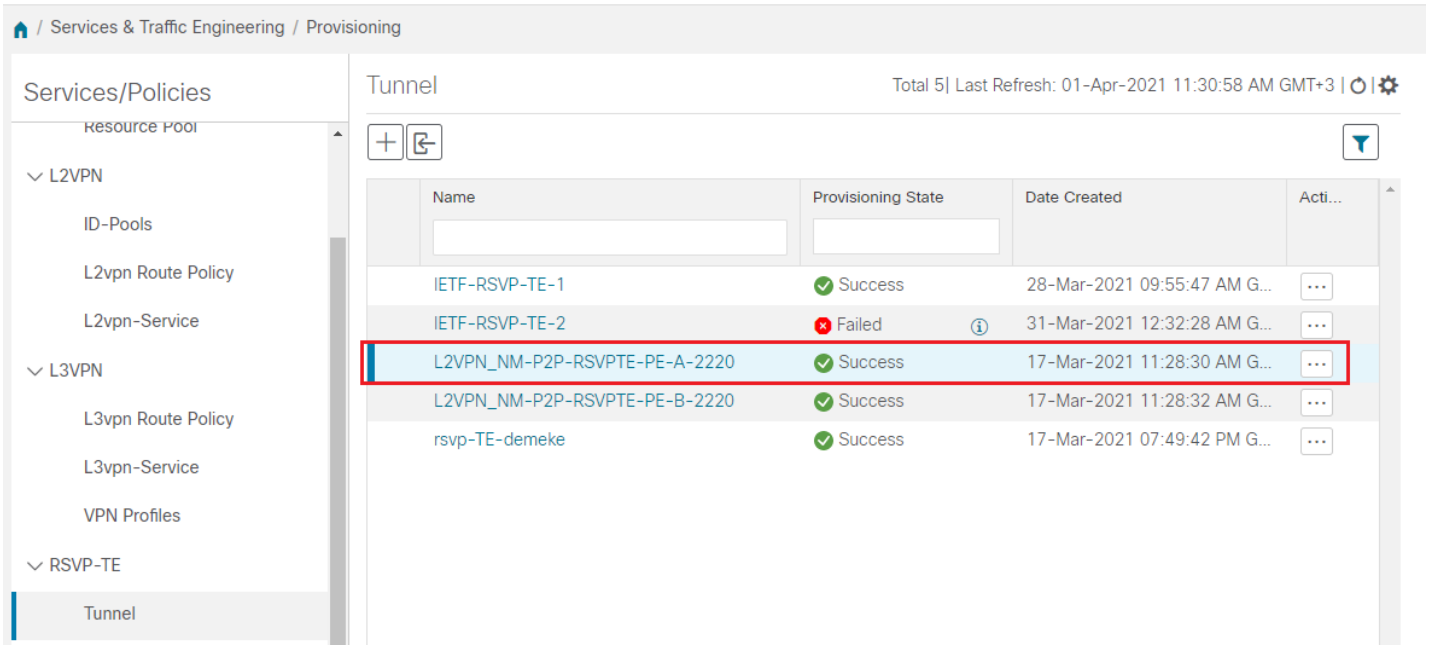
1. [サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [プロビジョニング（NSO） (Provisioning (NSO))] > [RSVP-TE] > [トンネル（Tunnel）] に移動します。
2. [+] をクリックして新しい RSVP-TE トンネルを作成し、一意の名前を付けます。[Continue] をクリックします。
3. [Identifier] フィールドにトンネルの ID の数値を入力します。この識別子は、後でこの RSVP-TE トンネルを L2VPN サービスに関連付けるときに使用します。この例では、識別子は **2220** です。
4. 送信元および宛先フィールドに、送信元（PE-A）および宛先（PE-B）デバイスの loopback0 IP アドレスを入力します。これは TE ルータ ID です。
   TE ルータ ID を検索するには、[Topology] に移動し、マップまたはデバイスのリストでデバイスをクリックします。[Device Details] ペインが開き、[Routing] セクションに TE ルータ ID が表示されます。



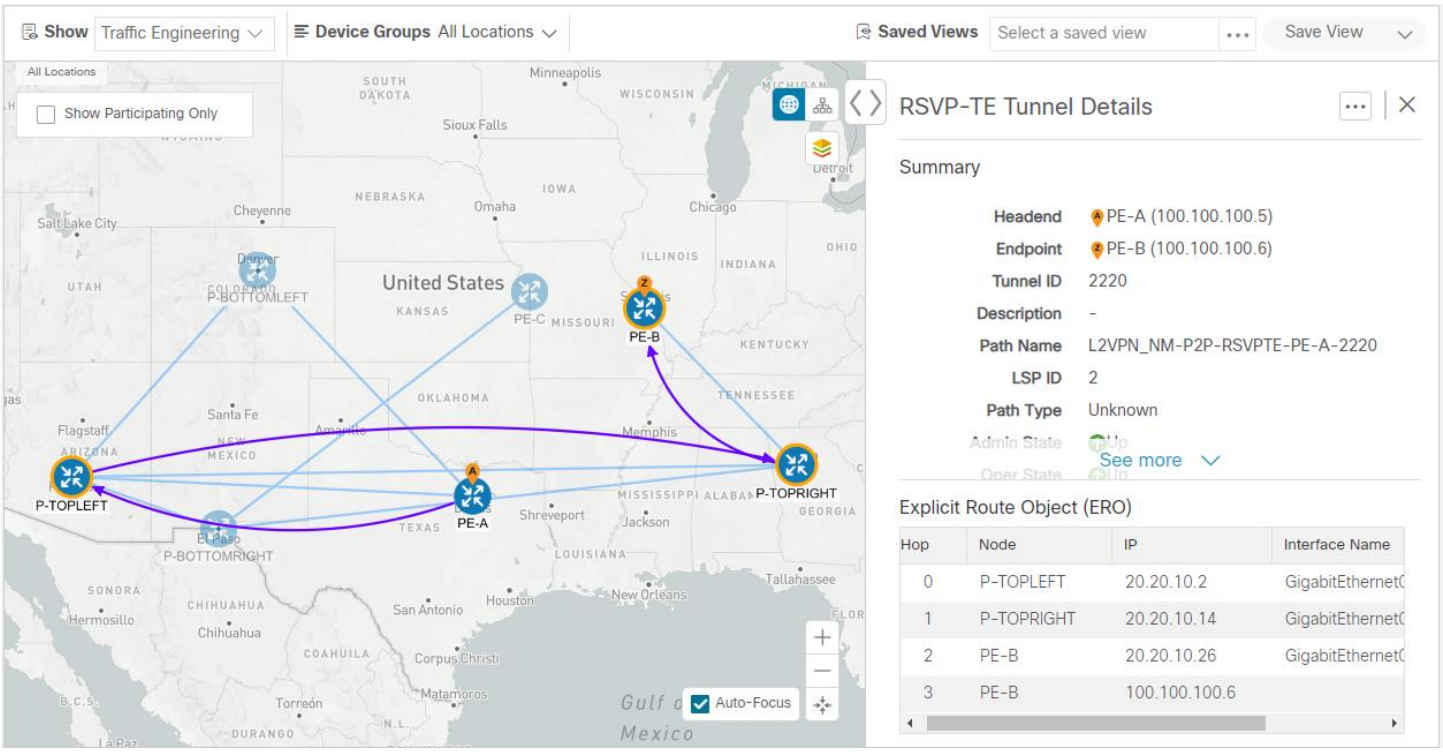
5. エンドポイントの定義：
   a. [head-end] のドロップダウンリストから、ヘッドエンドデバイスを選択します。
   b. [tail-end] のドロップダウンリストから、テールエンドデバイスを選択します。
6. リンクの帯域幅を予約します。[te-bandwidth] > [generic] で、リンクの帯域幅しきい値を入力します。
7. RSVP-TE トンネルのパスを定義します。明示的なパスを定義するか、参加しているデバイスによってローカルにパスを計算するかを選択できます。または、SR-PCE にパスを動的に計算させることもできます。このシナリオでは、パスをローカルに計算します。
   a. [p2p-primary-paths] で、[+] をクリックして新しいパスを作成します。
   b. 右側に表示されるペインで、パスに名前を付けます。
   c. パス計算方式（**path-locally-computed**）を選択します。
   d. パスの優先順位を数値で指定します。数値が小さいほど、優先順位が高くなります。
   e. 最適化メトリックを定義します（この場合は **igp**）。



8. [変更内容を確定（Commit Changes）] をクリックします。
9. RSVP-TE トンネルがトンネルリストに表示され、そのプロビジョニング状態が [Success] であることを確認します。



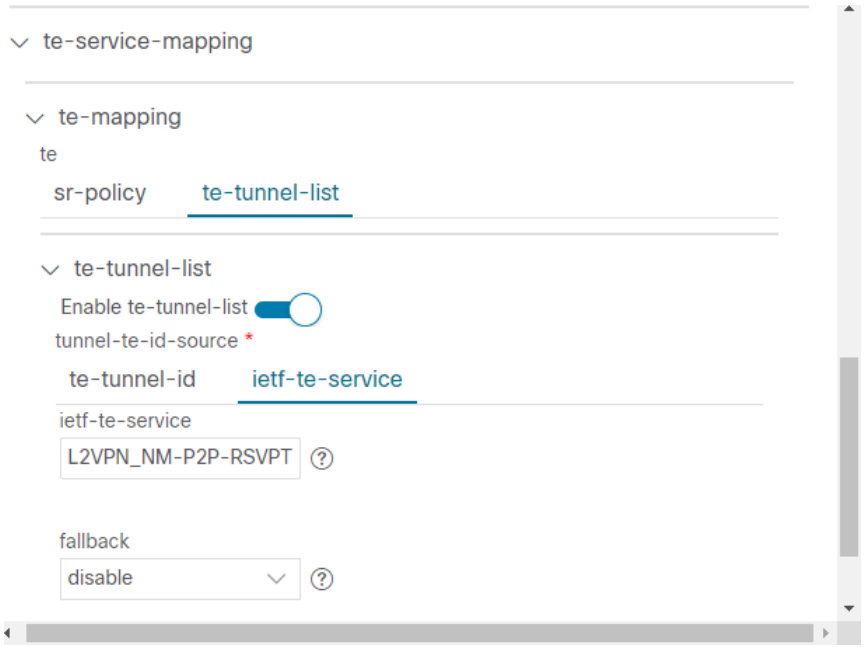
10. トンネル名をクリックすると、トンネルがマップ上に表示され、トンネルの詳細が表示されます。



ステップ 2. L2VPN サービスを作成し、RSVP トンネルをサービスにアタッチする

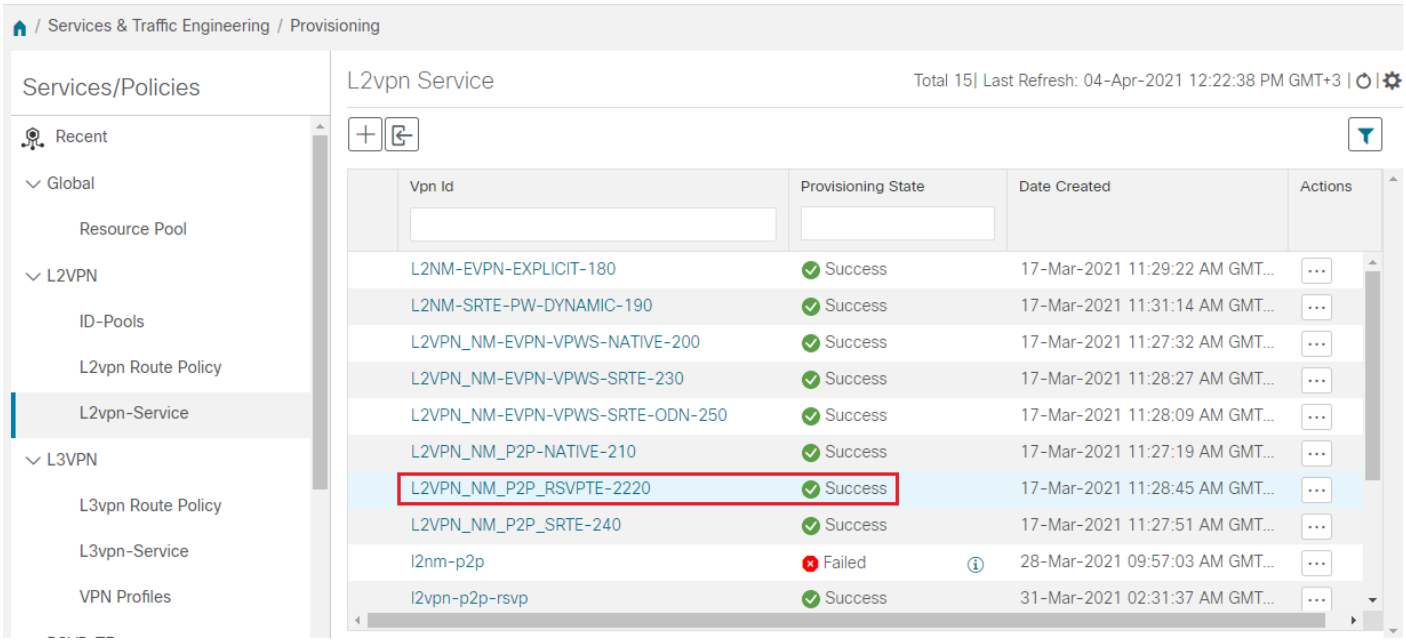
この手順では、プロビジョニング GUI を使用して P2P L2VPN サービスを作成します。テンプレートをインポートしてサービスを作成する場合は、「シナリオ 3：明示的 SR-TE ポリシーを使用した EVPN-VPWS サービスの静的パスの指定」を参照してください。

1. [Services & Traffic Engineering] > [Provisioning (NSO)] > [L2vpn] > [L2vpn Service] に移動します。
2. [+] をクリックして新しいサービスを作成し、一意の名前を付けます。[Continue] をクリックします。
3. [vpn-svc-type] フィールドで [vpn-common:t-ldp] を選択します。
4. 各 VPN エンドポイント（PE-A および PE-B）を個別に定義します。
   a. [vpn-nodes] で [+] をクリックします。
   b. [vpn-node-id] および [ned-id] ドロップダウンリストから関連するデバイスを選択し、[Continue] をクリックします。
   c. ネットワーク ID のローカル自律システム番号を入力します。
5. 1 つ以上の疑似回線を作成して、LDP シグナリングオプションを定義します。この場合は、ピアデバイス（PE-B）の TE ルータ ID を指定し、疑似回線を識別する一意の数値ラベルを指定します。
6. RSVP トンネルをサービスにアタッチします。
   a. [te-service-mapping] > [te-mapping] に移動し、[te-tunnel-list] タブをクリックします。
   b. [ietf-te-service] タブをクリックします。
   c. この L2VPN サービスにアタッチする RSVP-TE トンネルの名前を入力します。トンネル ID はトンネル設定から抽出されます。



注： Cisco Crosswork Network Controller の外部で設定されたデバイスに RSVP-TE トンネルが設定されている場合は、[te-tunnel-id] タブでそのトンネル ID を指定できます。

7. VPN ネットワークアクセスを定義します。この例では、dot1q カプセル化を使用しており、物理インターフェイス（GigabitEthernet0/0/0/2）と VLAN ID（2220）を指定しています。
8. PE-B についても上記の手順を実行します。
9. [Commit Changes] をクリックします。L2VPN が VPN サービスのリストに表示され、そのプロビジョニング状態が [Success] であることを確認します。



ステップ 3. マップで L2VPN サービスを可視化する

この手順では、マップ上の L2VPN の表示を確認して、作成した RSVP-TE トンネルに基づいてトラフィックが PE-A から PE-B に、およびその逆に PE-B から PE-A にたどるパスを確認します。

手順

1. [L2VPN Service] テーブルで、サービス名をクリックします。マップが開き、サービスの詳細がマップの右側に表示されます。

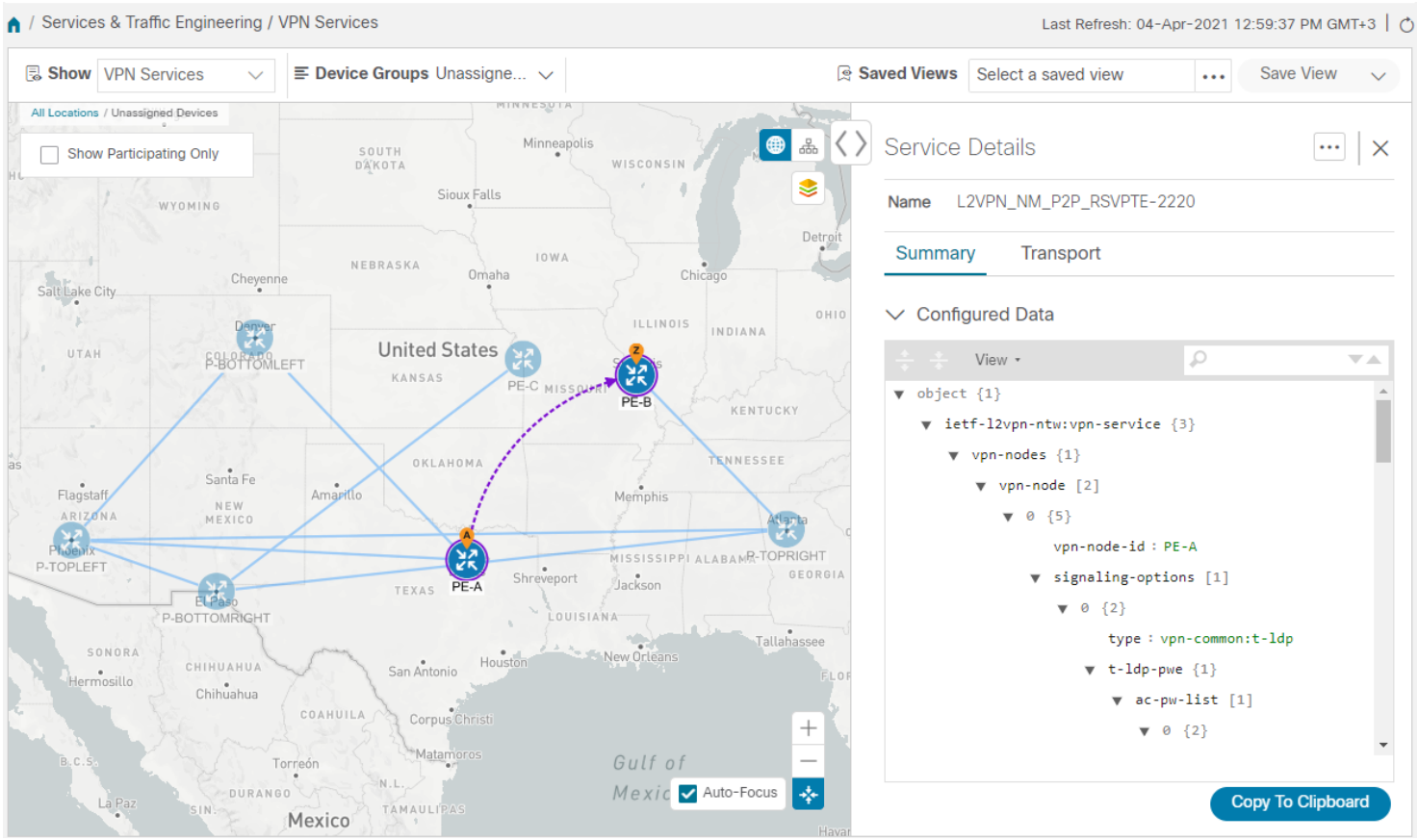
   または

   [Services & Traffic Engineering] > [VPN Services] に移動します。
   マップが開き、マップの右側に VPN サービスのテーブルが表示されます。

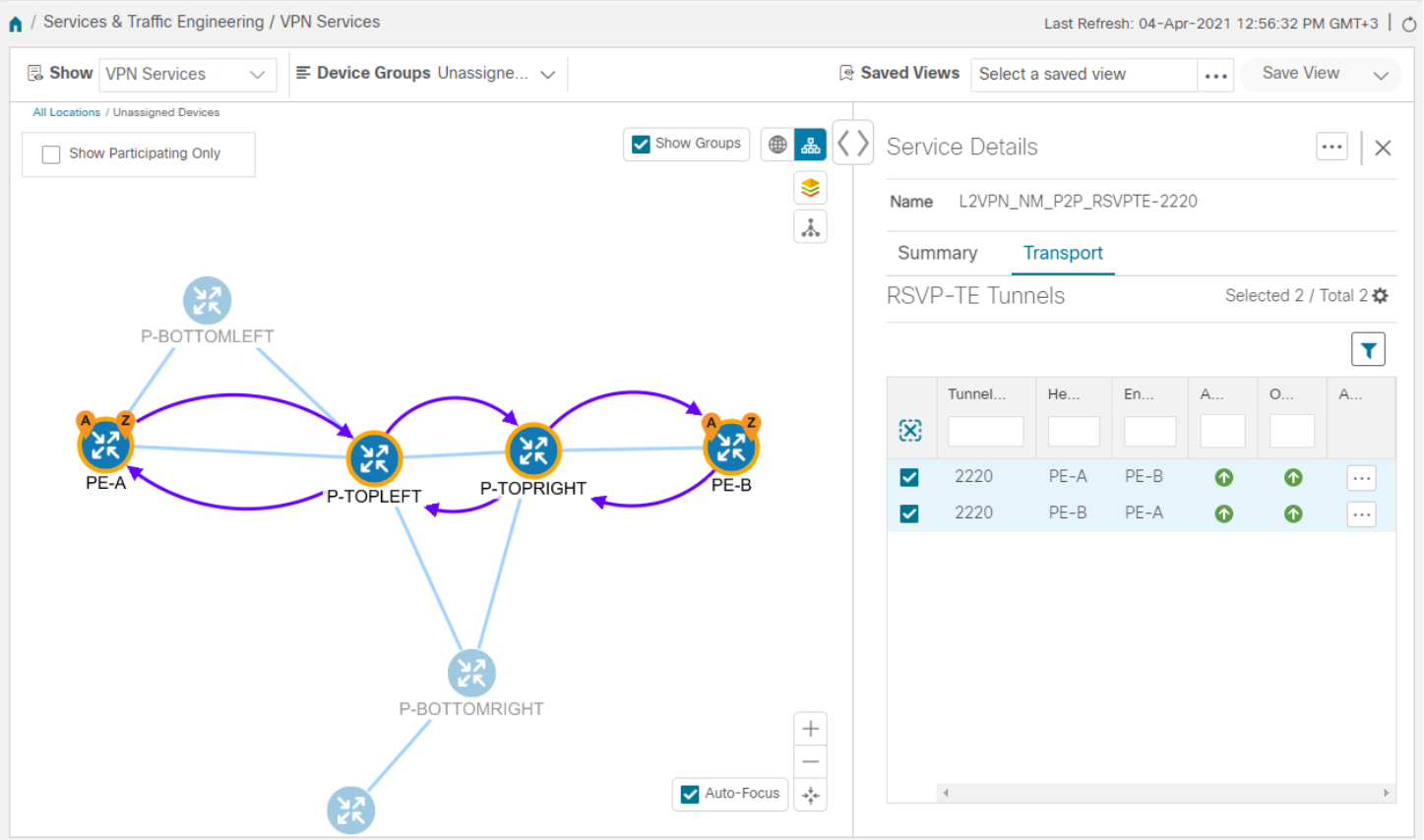
   [Services] テーブルで [VPN] をクリックします。テーブルに多数のサービスがある場合は、名前、タイプ、またはプロビジョニング状態でフィルタリングして、VPN を見つけることができます。

   マップでは、トポロジ上のオーバーレイとして VPN が表示されます。3 つのエンドポイントと、仮想パスであることを示す点線が表示されます。

   注： 次の図は、地理的マップでの VPN のオーバーレイを示しています。論理マップと地理的マップを切り替えるには、マップの右上にあるボタン  を使用します。



2. PE-A と PE-B 間のルートのホップを確認するには、[Transport] タブをクリックし、1 つ以上の基盤となる TE トンネルを選択して、マップ上のエンドポイント間のパスを表示します。次の図は、[Transport] タブで選択した RSVP-TE トンネルと、PE-A から PE-B へのルートと PE-B から PE-A へのルートの両方が論理マップに表示されていることを示しています。



3. RSVP-TE トンネルは予約済み帯域幅で設定されているため、リンク全体の帯域幅使用率が指定された帯域幅を超えると、パスが再ルーティングされます。

まとめと結論

このシナリオでは、予約済み帯域幅を使用して RSVP-TE トンネルを作成し、それらを L2VPN サービスにアタッチして、データ量の多いリッチメディアを連続ストリーミングするための高品質なサービス要件を満たす方法について説明しました。マップ上のパスを確認しました。このパスは、リンクの帯域幅使用率が帯域幅予約しきい値を超えた場合に再計算されます。

シナリオ 5：最適化の制約を伴うソフト帯域幅保証のプロビジョニング

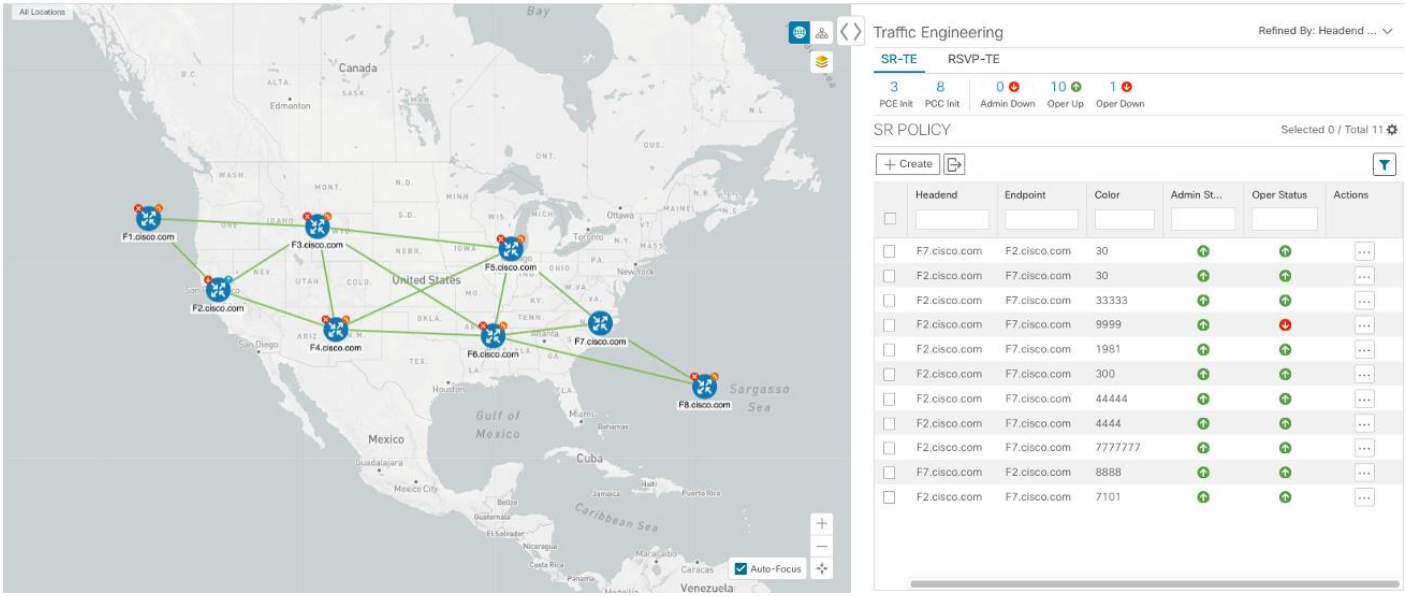
シナリオのコンテキスト

サービスプロバイダは、トラフィック使用時間のピークに対するニーズに対応し、1 日を通じて変化するお客様の優先順位に基づいてサービスを動的に最適化するために、可能な限り低い遅延で高速接続を提供できる必要があります。このために、オペレータは特定のリンクの帯域幅を予約することで、具体的な最適化のために設定された量のトラフィックを処理できる専用パスを確保する必要があります。Cisco Crosswork Network Controller の帯域幅オンデマンド（BWoD）機能により、この機能を実現することができます。要求された帯域幅を持つパ

スがある場合は計算され、要求された帯域幅を保証するパスが見つからない場合は、*ベストエフォート*のパスを見つけようと試みます。

このシナリオでは、BWoD を使用して、2 つのエンドポイント間で使用可能な所定の量の帯域幅を指定した最小 TE メトリックパスを計算します。

次のトポロジが、このシナリオの基本となります。



目標は、F2.cisco.com から F7.cisco.com へのパスを作成し、使用率を 80% に維持しながら 250 Mbps のトラフィックに対応できるようにすることです。BWoD は最初に、使用率のしきい値を超えずに要求された帯域幅に対応できる単一のパスを見つけようと試みます。単一のパスが見つからない場合、BWoD はパスの分割を推奨する場合があります。

このシナリオでは、次の作業を行います。

- 帯域幅と TE の制約を伴う新しい SR-TE ポリシーをオーケストレーションします。
- BWoD を設定して有効にします。
- SR-TE ポリシーの状態を確認し、マップ上のパスを表示します。

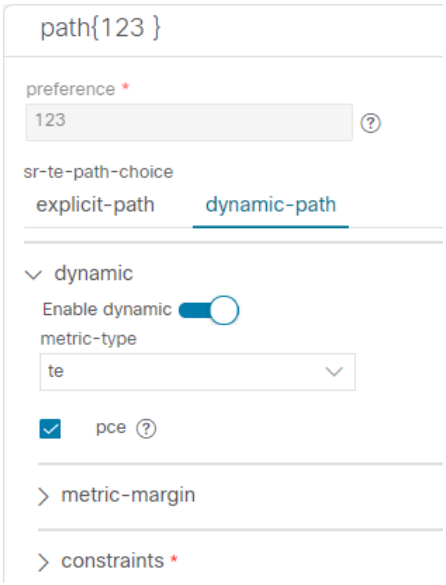
ワークフロー

- 手順 1：要求された帯域幅と最適化インテントを伴う BWoD SR-TE ポリシーを作成する
- 手順 2：BWoD の有効化と設定
- 手順 3：ポリシーの動作状態が稼働中であることを確認し、マップ上のパスを表示する

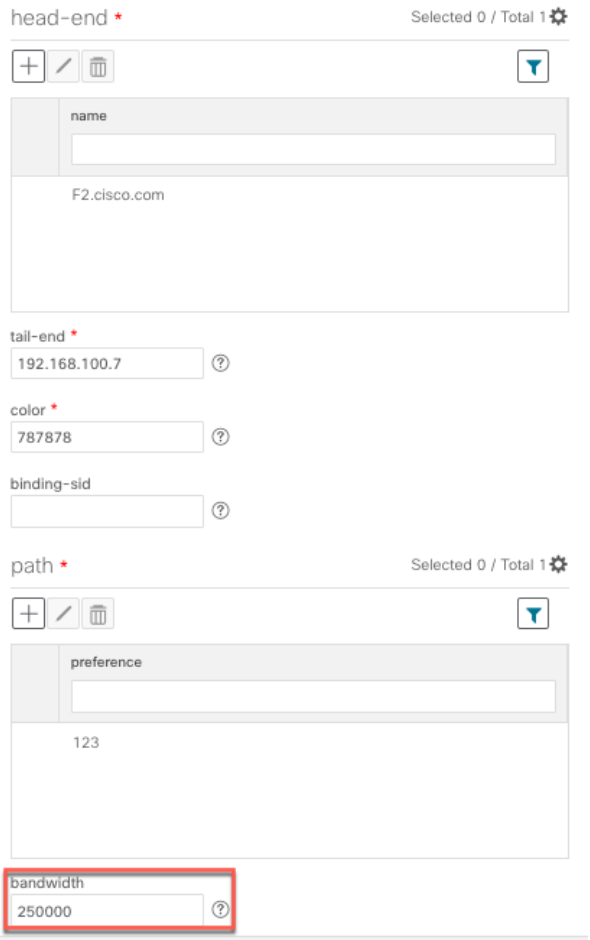
ステップ 1. 要求された帯域幅と最適化インテントを伴う BWoD SR-TE ポリシーを作成する

1. [サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [プロビジョニング（NSO）（Provisioning (NSO)）] > [SR-TE] > [ポリシー（Policy）] に移動します。
2. [+] をクリックして新しい SR-TE ポリシーを作成し、一意の名前を付けます。[Continue] をクリックします。

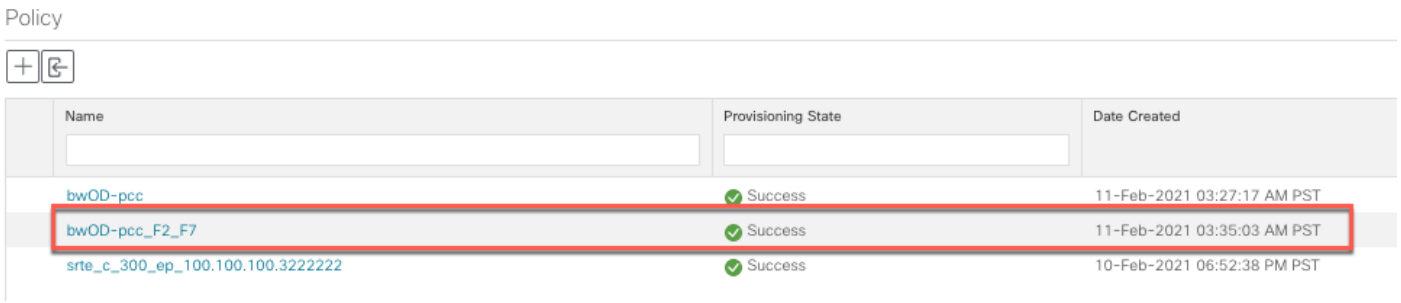
3. エンドポイントの定義：
   a. [head-end] の [+] をクリックし、ドロップダウンリストからヘッドエンドデバイスを選択して、[Continue] をクリックします。[X] をクリックして [Headend] ペインを閉じます。
   b. テールエンドデバイスの IP アドレスを入力します。
   c. トラフィックを識別する色を入力します。
4. パスを計算するパラメータを定義します。
   a. [Path] の下にある [+] をクリックします。
   b. パス設定を入力し、[Continue] をクリックします。
   c. [dynamic-path] タブの [metric-type] ドロップダウンリストで、最適化の目的として [te] を選択します。
   d. SR-PCE にこのポリシーのパスを計算させるには、[pce] チェックボックスをオンにします。



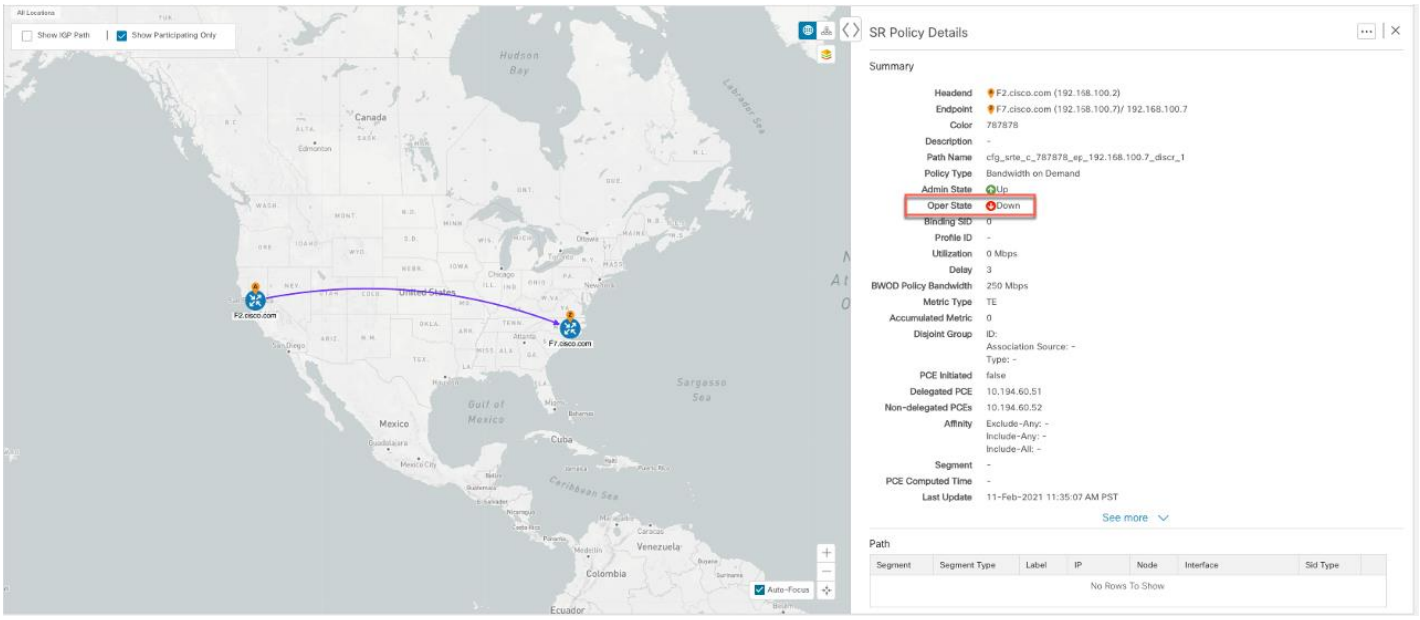
   e. [X] をクリックして [path] ペインを閉じます。
5. [Bandwidth] フィールドに、要求された帯域幅を Kbps 単位で入力します。この例では、**250** Mbps、つまり 250000 Kbps を要求しています。



6. [Commit Changes] をクリックします。新しいポリシーが作成され、SR-TE ポリシーのリストに表示されます。プロビジョニング状態は [Success] である必要があります。

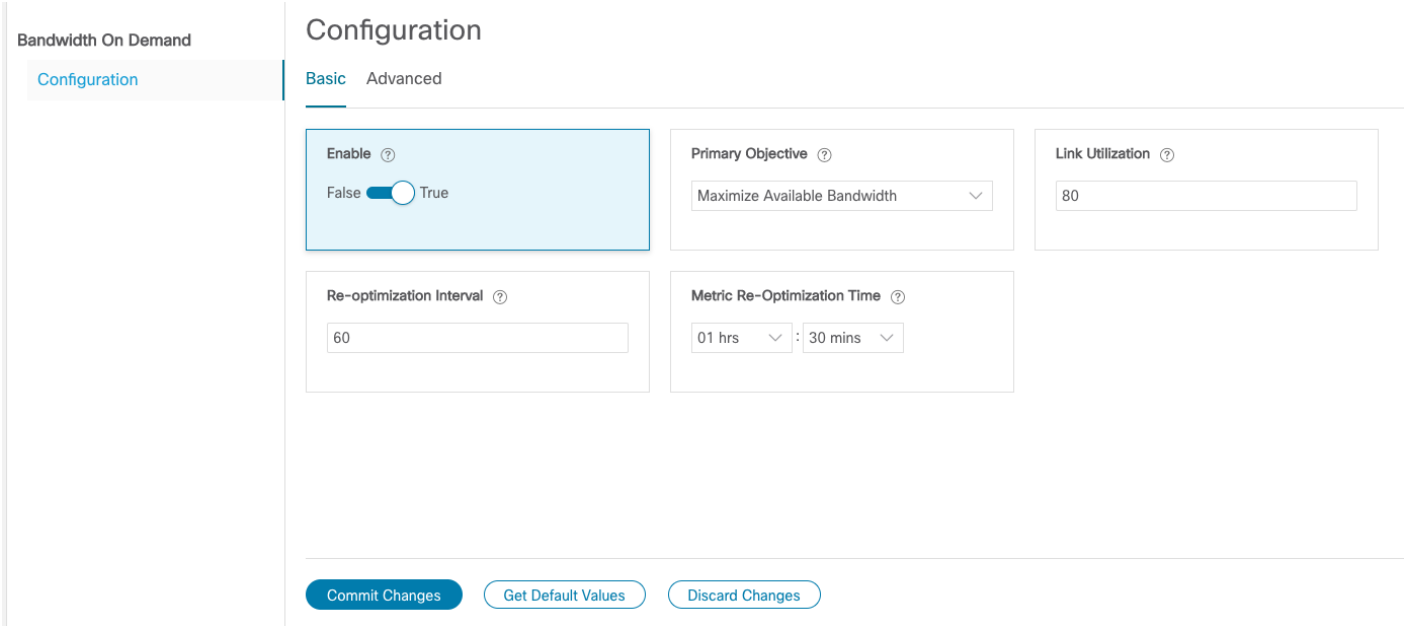


7. 新しいポリシーについて、その詳細とマップ上での表示を確認します。
   a. [Actions] 列の [...] をクリックし、[View] を選択します。
   b. マップが開き、マップの右側に SR-TE ポリシーの詳細が表示されます。
      SR-PCE だけでは帯域幅の計算に対応できないため、Cisco Crosswork Network Controller の BWoD 機能を有効にするまでは、ポリシーの動作状態がダウンとなることに注意してください。



ステップ 2. BWoD の有効化と設定

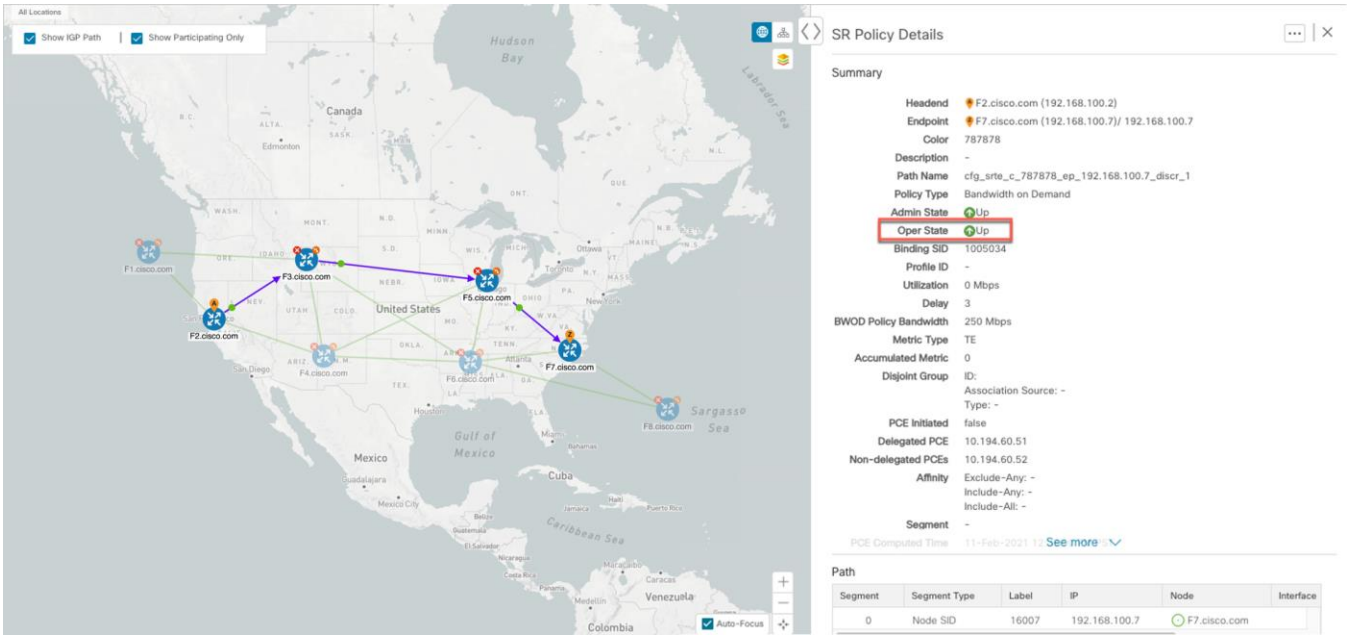
1. [Services & Traffic Engineering] > [Bandwidth on Demand] に移動します。
2. [Enable] スイッチを [True] に切り替え、80 を入力して使用率のしきい値のパーセンテージを設定します。他のオプションの説明を表示するには、? の上にマウスを重ねます。
3. [変更内容を確定（Commit Changes）] をクリックします。



ステップ 3. ポリシーの動作状態が稼働中であることを確認し、マップ上のパスを表示する

1. [Services & Traffic Engineering] > [Provisioning] に移動します。
2. [Policy] テーブルで、エンドポイント用に計算されたパスを見つけて選択します。

3. パスはマップ上にオーバーレイとして表示されます。エンドポイント間の物理パスを表示するには、[Show IGP Path] チェックボックスをオンにします。



まとめと結論

オペレータは、Cisco Crosswork Network Controller で提供される BWoD 機能を使用して、最適化インテントに基づいて帯域幅要件を設定および維持できます。このシナリオでは、特定の帯域幅要件を備えた SR-TE ポリシーをプロビジョニングする方法について説明しました。BWoD 機能を有効にして、帯域幅要件を維持するためにトラフィックが自動的に再ルーティングされるようにする方法について確認しました。この自動化により、SLA によって設定された帯域幅要件に対応するため、パスを手動で追跡および設定する作業の負担が軽減されます。

帯域幅とネットワークの最適化

概要

目的

輻輳時にリアルタイムでネットワークを戦術的に最適化する。

Challenge

ネットワークの輻輳は、エンドカスタマー エクスペリエンスの低下につながります。接続不良、ストリーミングビデオの遅延、パケット損失が発生すると、ユーザーの満足度が低下し、お客様のサービスに対する市場の評価が低下します。最悪のシナリオでは、ネットワークの問題がサービスレベル契約（SLA）違反または契約違反につながり、ブランド価値が失われます。ネットワークオペレータは、オペレータがほぼ介入せずに、帯域幅の最適化を自動化し、効率的にトラフィックを誘導できるようにするためのツールセットを必要としています。

ソリューション

Cisco Crosswork Network Controller は、帯域幅管理と輻輳緩和のためのソリューションとして、ローカル輻輳緩和（LCM）を提供しています。これは、Cisco Crosswork Network Controller 4.1 で導入された拡張機能です。

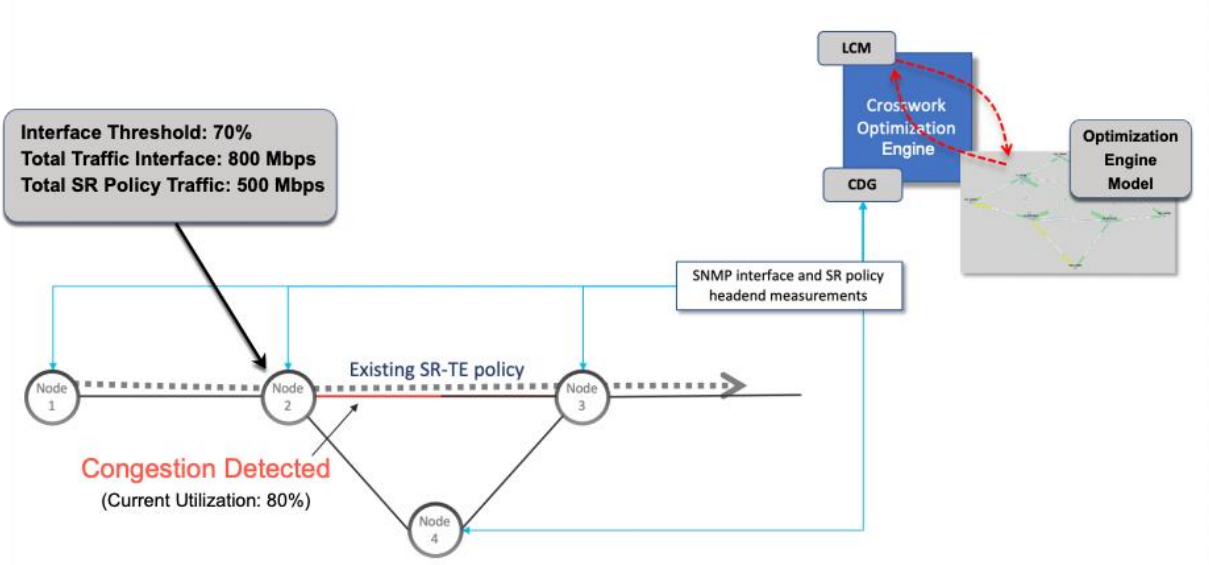
ローカル輻輳緩和（LCM）

LCM では、ネットワーク全体のトラフィックを再ルーティングしてネットワークの帯域幅リソースを最適化する（エンドツーエンドのパスの最適化）代わりに、インターフェイスレベルのキャパシティをローカルに、輻輳エリア内およびその周辺でチェックし、輻輳したインターフェイスのエンドポイント間のトラフィックを再ルーティングします（ローカルなインターフェイスレベルの最適化）。問題に対してローカルに焦点を当てることで、完全なトラフィックマトリックスを使用してネットワーク内のエッジツーエッジのトラフィックフローをシミュレートする必要がなくなります。このシミュレーションは作成するのに手間がかかり、ノード数の増加に伴い拡張性が低くなります。

LCM は、輻輳が発生したインターフェイスから最小量のトラフィックを転送することで輻輳を緩和するための推奨事項を提供します。LCM は、SNMP を介して SR-TE ポリシーおよびインターフェイスカウンタの収集を実行します。転送するトラフィックの量を予想し、ユーザーが承認すると、戦術的トラフィック エンジニアリング（TTE）SR-TE ポリシーの展開を通じて緩和を実行します。輻輳をローカルで緩和するのに、完全なセグメント ルーティング トラフィック マトリックス（SR-TM）を使用する必要はありません。TTE SR-TE ポリシーは、輻輳したリンクのいずれかの側のデバイスでのみ作成され、他の場所ではインターフェイスを輻輳させない最短パスで作成されます。

LCM の仕組み

1. LCM は、まず、Optimization Engine モデル（物理ネットワークのリアルタイムトポロジとトラフィックの表現）を定期的に分析します。
2. この例では、輻輳の確認間隔の後、ノード 2 の使用率が 70% の使用率しきい値を超えると、LCM が輻輳を検出します。



3. LCM は、転送に適したトラフィック量を計算します。

   LCM は、既存の SR ポリシーによってルーティングされていないトラフィックのみを転送します（ラベルなし、IGP ルーティング、または FlexAlgo-0 SID 経由で伝送など）。SR ポリシー内のトラフィックは、LCM 計算には含まれず、元のプログラムされたパスを通過し続けます。

   対象トラフィックは、インターフェイス上のすべてのトラフィックを考慮したインターフェイス トラフィック統計情報を取得し、インターフェイスを通過するすべての SR-TE ポリシーのトラフィック統計情報の合計を引いて計算されます。

   合計インターフェイス トラフィック - SR ポリシートラフィック = 最適化できる対象トラフィック

   このプロセスでは、SR ポリシーの ECMP 分割を考慮して、SR ポリシートラフィックを適切にアカウンティングする必要があります。この例では、輻輳したノード 2 の合計トラフィックは 800 Mbps です。ノード 2 経由でルーティングされるすべての SR ポリシーの合計トラフィックは 500 Mbps です。

   この例で LCM が転送できる合計トラフィックは 300 Mbps（800 Mbps – 500 Mbps = 300 Mbps）です。

4. LCM は、インターフェイス上の合計トラフィックからしきい値相当のトラフィックを差し引くことにより、代替パスを介して送信する必要があるトラフィック量を計算します。この例では、転送される量は 100 Mbps です。

   800 Mbps – 700 Mbps（しきい値 70%）= 100 Mbps

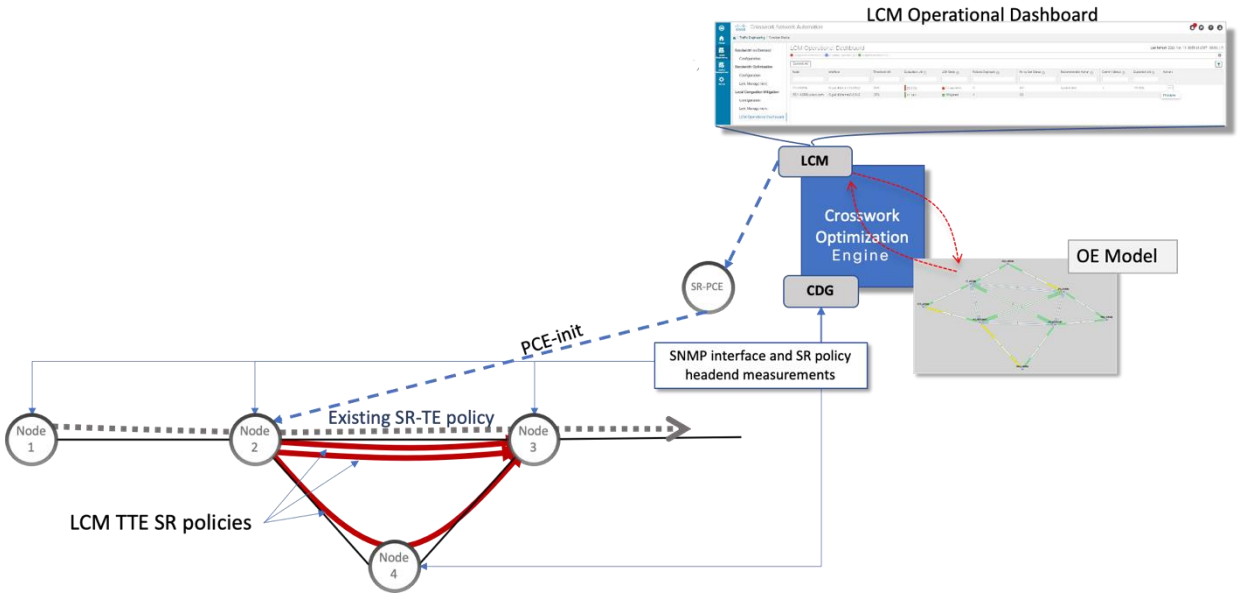
   LCM は、300 Mbps のうちの 100 Mbps（対象トラフィック）を別のパスにルーティングする必要があります。オーバープロビジョニング係数（OPF）のパーセンテージが 10 に設定されている場合、LCM は対象トラフィックの 110（100 Mbps X 1.10）をルーティングする必要があることに注意してください。OPF は、[LCM Configuration] ウィンドウの [Advanced] タブで設定できます。

5. LCM は、必要な TTE SR ポリシーの数とそのパスを決定します。再ルーティングする必要がある量に対して最短パスに留まることができる LCM 対象トラフィックの割合によって、最短パスと代替パスでそれぞれ必要な TTE SR ポリシーの数が決まります。

   この例では、LCM は輻輳したリンクから対象トラフィックの合計の 1/3（300 Mbps のうち 100 Mbps）を転送する必要があります。LCM は完全な ECMP を想定し、このトラフィック分割には 3 つの戦術的 SR-TE ポリシーが必要だと予測します。1 つの戦術的 SR-TE ポリシーが転送パスをとり、2 つの戦術的 SR-TE ポリシーが元のパスをとります。ノード 2 とノード 4 の間のパスに十分な容量があります。したがって、LCM では、SR-PCE を介してノード 2 からノード 3 に展開する 3 つの TTE SR ポリシー（それぞれ約 100 Mbps をルーティングすると想定）を推奨しています。

   - ノード 3（200 Mbps）への直接パスを取る 2 つの TTE SR ポリシー
   - TTE SR ポリシーの 1 つはノード 4（100 Mbps）経由のパスを取ります。

   これらの推奨事項は、[LCM 運用ダッシュボード（LCM Operational Dashboard）] にリストされます。



LCM はこれらの TTE SR ポリシーを展開すると想定して、 展開された TTE ポリシーを引き続きモニターし、[LCM 運用ダッシュボード（LCM Operational Dashboard）] で必要に応じて変更または削除することを推奨します。TTE SR ポリシーの削除は、これらのポリシーが削除された（保留マージンを差し引く）場合に、緩和されたインターフェイスが輻輳しない場合に推奨されます。これにより、LCM の操作全体で不必要な TTE SR ポリシーのチャーンを回避できます。

使用シナリオ

帯域幅に制約のある最適化と LCM の実行を示す次の使用シナリオについて、順を追って説明します。

[シナリオ 6：Local Congestion Mitigation（LCM）を使用して、過剰に使用されているリンク上のトラフィックを再ルーティングする]

関連リソース

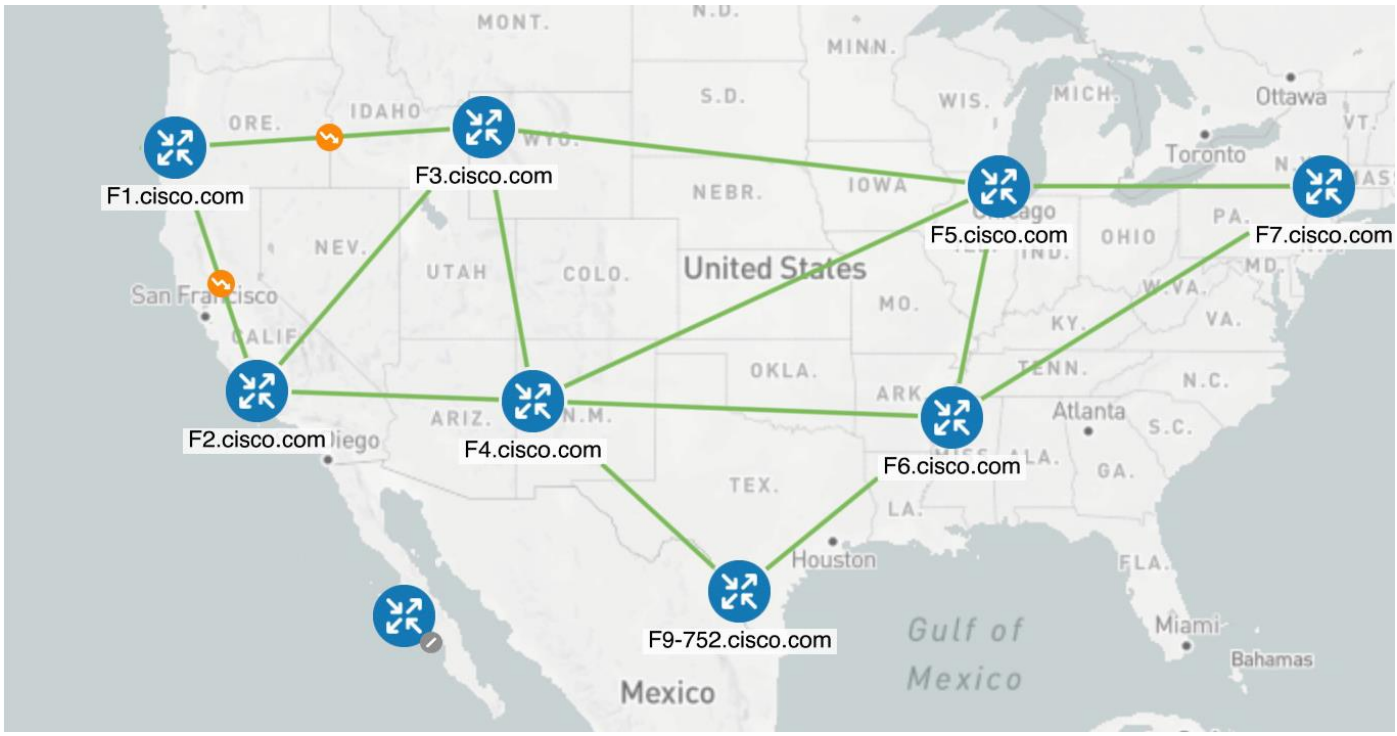
[Cisco Crosswork Optimization Engine ドキュメント]

シナリオ 6：Local Congestion Mitigation（LCM）を使用して、過剰に使用されているリンク上のトラフィックを再ルーティングする

シナリオのコンテキスト

このシナリオでは、LCM を有効にし、定義された使用率のしきい値をデバイスのインターフェイスの使用率が超えた場合に TTE SR ポリシーを展開するための輻輳緩和の推奨事項を確認します。輻輳の緩和をコミットする前に、推奨される TTE SR ポリシーをプレビューします。

この例では、次のトポロジを使用します。



F3.cisco.com と **F5.cisco.com** 間のリンクが過剰に使用された場合に実行されるアクションを確認します。現在、そのリンクには輻輳の兆候がないことに注意してください。

仮定と前提条件

次に、LCM を適切に動作させるための大まかな要件のリストを示します。

輻輳評価

LCM には、次のトラフィック統計情報が必要です。

- SNMP インターフェイス トラフィック の測定値
- SNMP ヘッドエンド SR-TE ポリシートラフィックの設定値

輻輳緩和

ヘッドエンドデバイスは、autoroute のステアリングで PCE によって開始された SR-TE ポリシーをサポートする必要があります。

autoroute を使用して SR-TE ポリシーへのトラフィックステアリングを有効にするには、`force-sr-include` を使用してデバイスを設定する必要があります。次に例を示します。

```
segment-routing traffic-eng pcc profile <id> autoroute force-sr-include
```

- ヘッドエンドデバイスは、複数のパラレル SR-TE ポリシー全体で等コストマルチパス（ECMP）をサポートする必要があります。

詳細については、シスコのアカウント担当者にお問い合わせください。

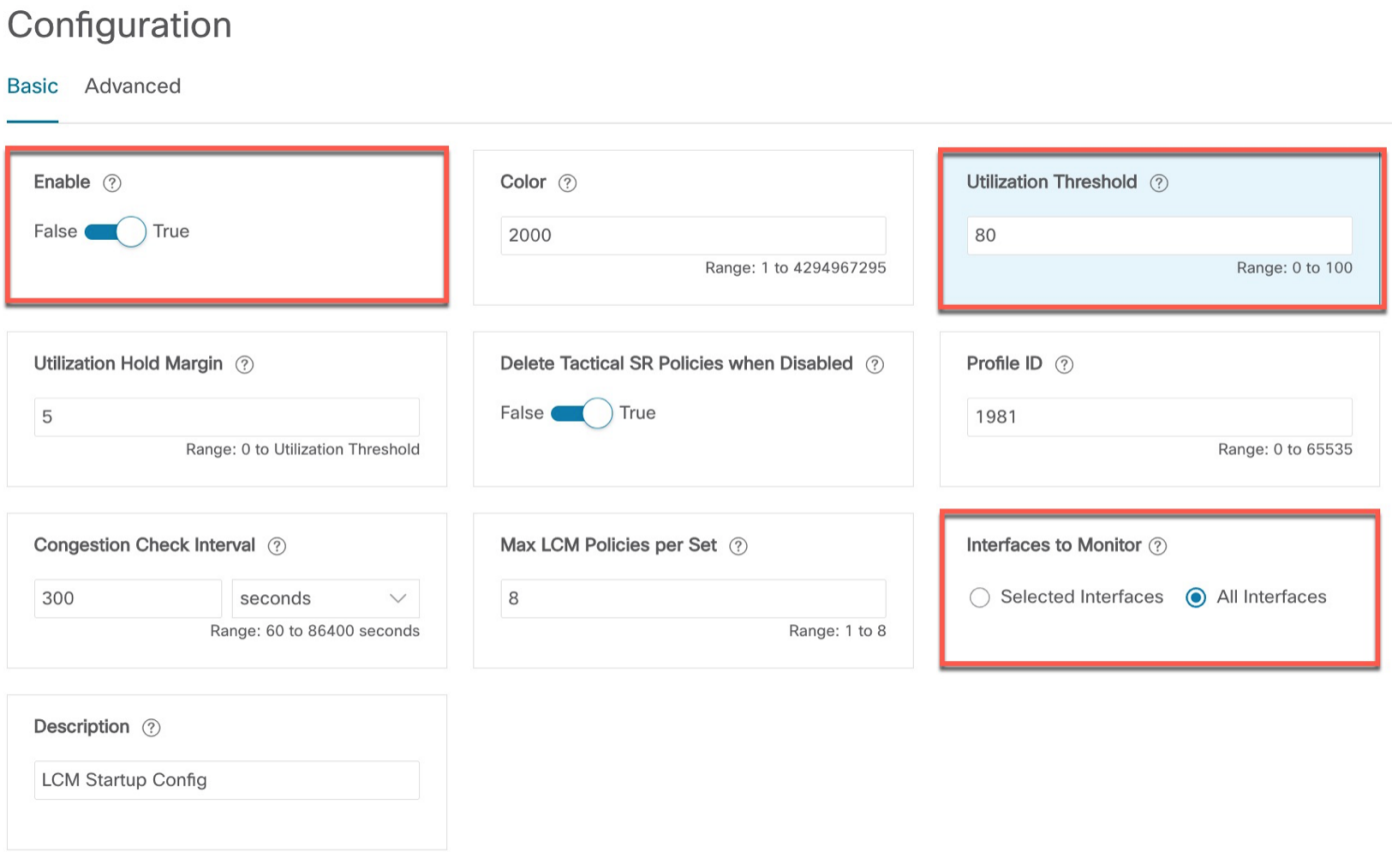
ワークフロー

- 手順 1：LCM を有効にし、グローバル使用率のしきい値を設定する
- 手順 2：マップ上でリンクの輻輳を表示する
- 手順 3：[LCM 運用ダッシュボード（LCM Operational Dashboard）] で TTE SR ポリシーの推奨事項を表示する
- 手順 4：TTE SR ポリシーの展開を検証する
- 手順 5：LCM の推奨に従って TTE SR ポリシーを削除する

ステップ 1. LCM を有効にし、グローバル使用率のしきい値を設定する

1. [サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [ローカル輻輳緩和（Local Congestion Mitigation）] > [ドメイン ID（Domain-ID）] に移動し、[設定（Configuration）] をクリックします。
2. [Enable] スイッチを [True] に切り替え、希望するグローバル使用率しきい値を入力します。この事例では、しきい値を 80% に設定し、[モニターするインターフェイス（Interfaces to Monitor）] > [すべてのインターフェイス（All Interfaces）] オプションを選択します。

   他の設定オプションに関する情報を表示するには、マウスを⑦の上に合わせます。



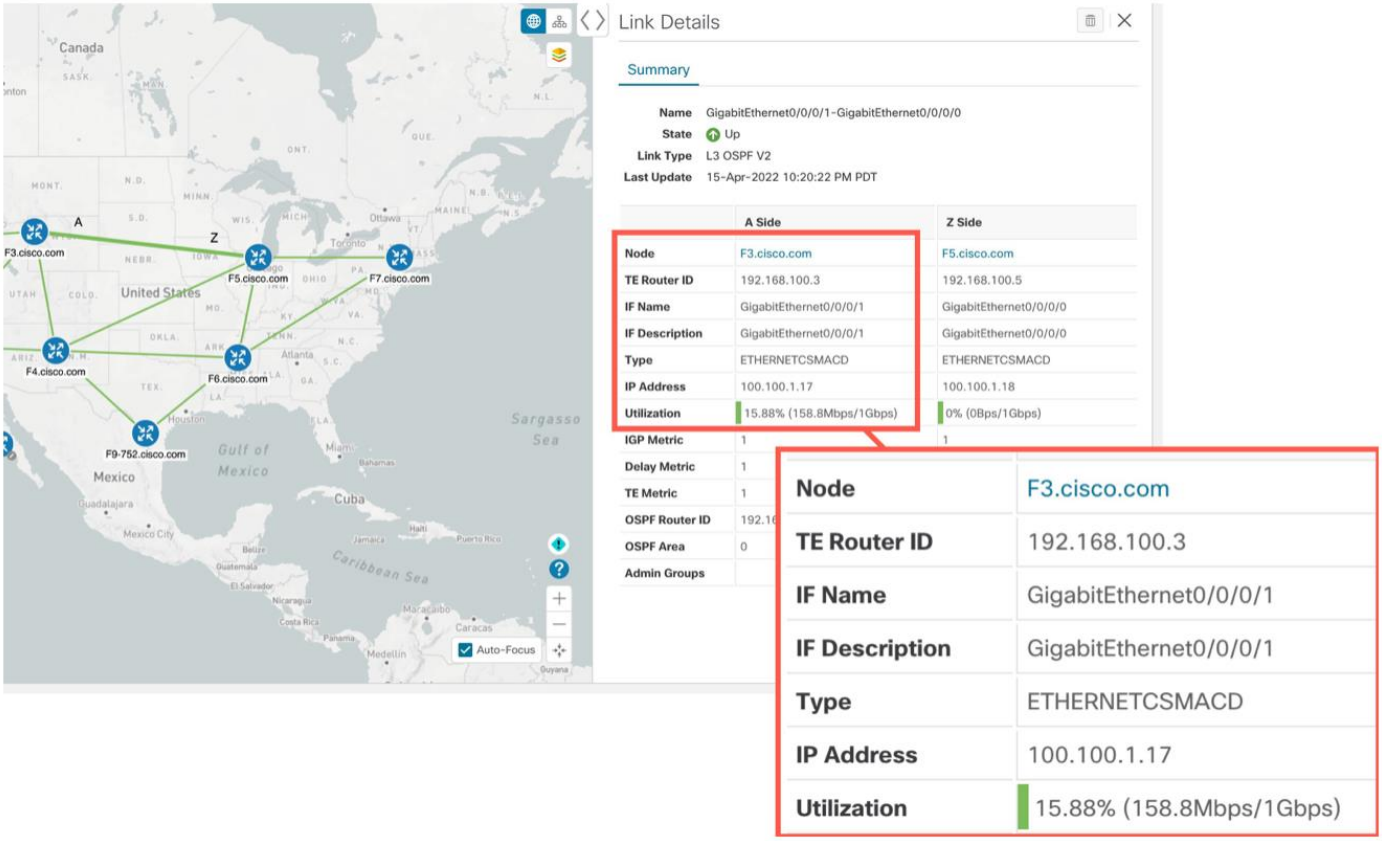
3. [変更を確定（Commit Changes）] をクリックします。

   注： 設定の変更を確定すると、LCM はモニター対象インターフェイスで輻輳が発生した場合、 [LCM 運用ダッシュボード（LCM Operational Dashboard）] に *推奨事項* を表示します。LCM は新しい TTE ポリシーを自動的に確定または展開 *しません*。後で、推奨される TTE ポリシーをプレビューし、それらのポリシーをコミットしてネットワークに展開するかどうかを決定できます。

ステップ 2. マップ上でリンクの輻輳を表示する

F3.cisco.com と **F5.cisco.com** 間のリンクが輻輳しているとします。マップ上で確認してみましょう。

1. [Services & Traffic Engineering] > [Traffic Engineering] に移動します。
2. リンクをクリックすると、使用率情報を含むリンクの詳細が表示されます。P4-NCS5501 インターフェイスの使用率が、13% に定義されたカスタム LCM しきい値を超えていることに注意してください。

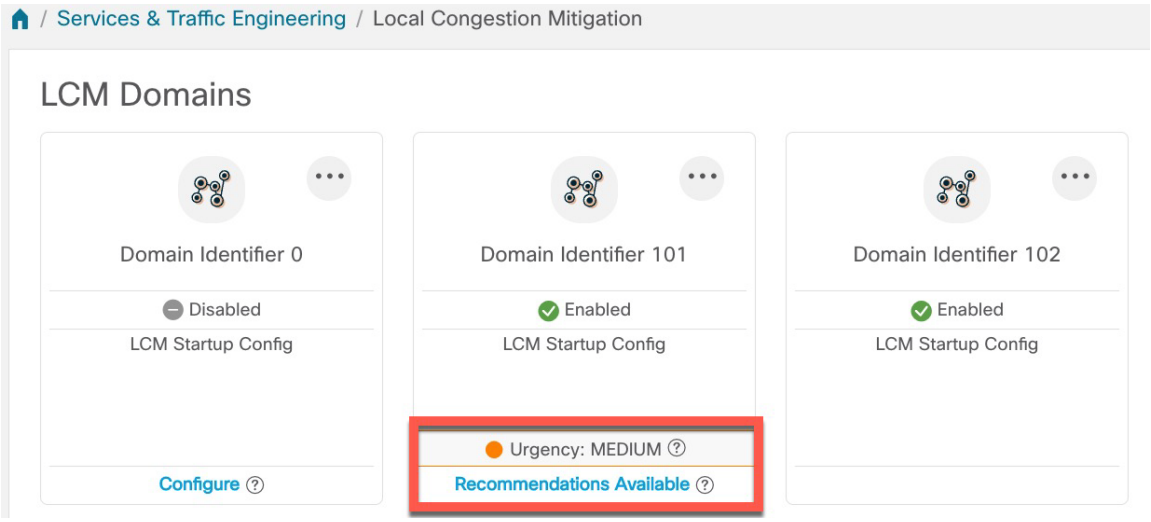


ステップ 3. [LCM 運用ダッシュボード（LCM Operational Dashboard）] で TTE SR ポリシーの推奨事項を表示する

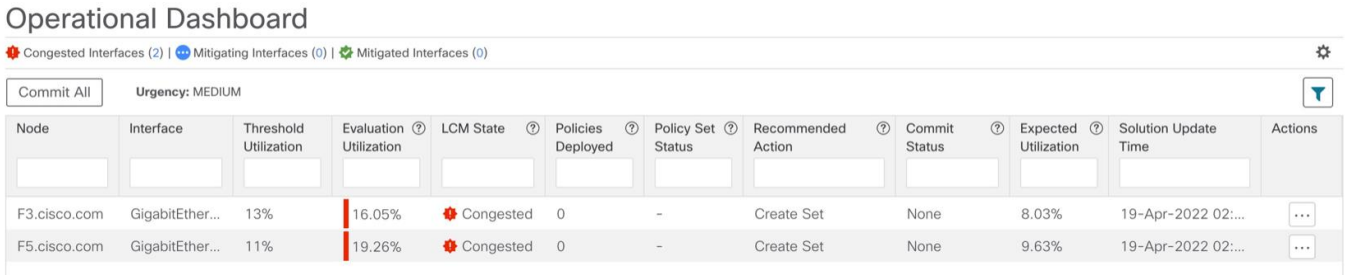
LCM が輻輳を検出し、輻輳を緩和するための戦術ポリシーを計算しました。これらをプレビューして、コミットするかどうかを決定できます。

1. [Services & Traffic Engineering] > [Local Congestion Mitigation] に移動します。

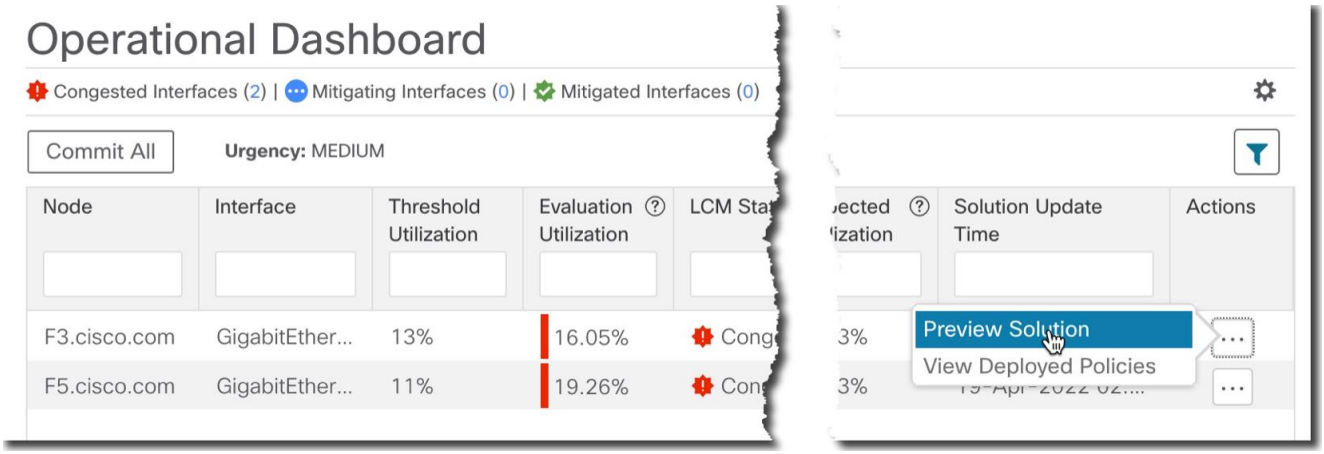
   輻輳が検出されると、ドメインには緊急度のタイプと利用可能な推奨事項が表示されます。疑問符アイコンをクリックすると、緊急度のタイプと、最新の推奨事項が提示された時期に関する詳細が表示されます。



2. [運用ダッシュボード（Operational Dashboard）] を開きます（[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [ローカルでの輻輳緩和（Local Congestion Mitigation）] > [ドメイン ID（Domain-ID）] > [⋯] > [運用ダッシュボード（Operational Dashboard）]）。
ダッシュボードには、F3.cisco.com の使用率が 13% を超えており、16.05% であることが示されます。また、F5.cisco.com の使用率が 11% のしきい値を超えており、現在 19.26% であることも示されています。[推奨アクション（Recommended Action）] 列では、LCM により、インターフェイスの輻輳に対処するために TTE ポリシー ソリューション セット（[セットの作成（Create Set）]）を展開することが推奨されています。[予想使用率（Expected Util）] 列には、推奨アクションが実行された場合の各インターフェイスの予想使用率が表示されます。

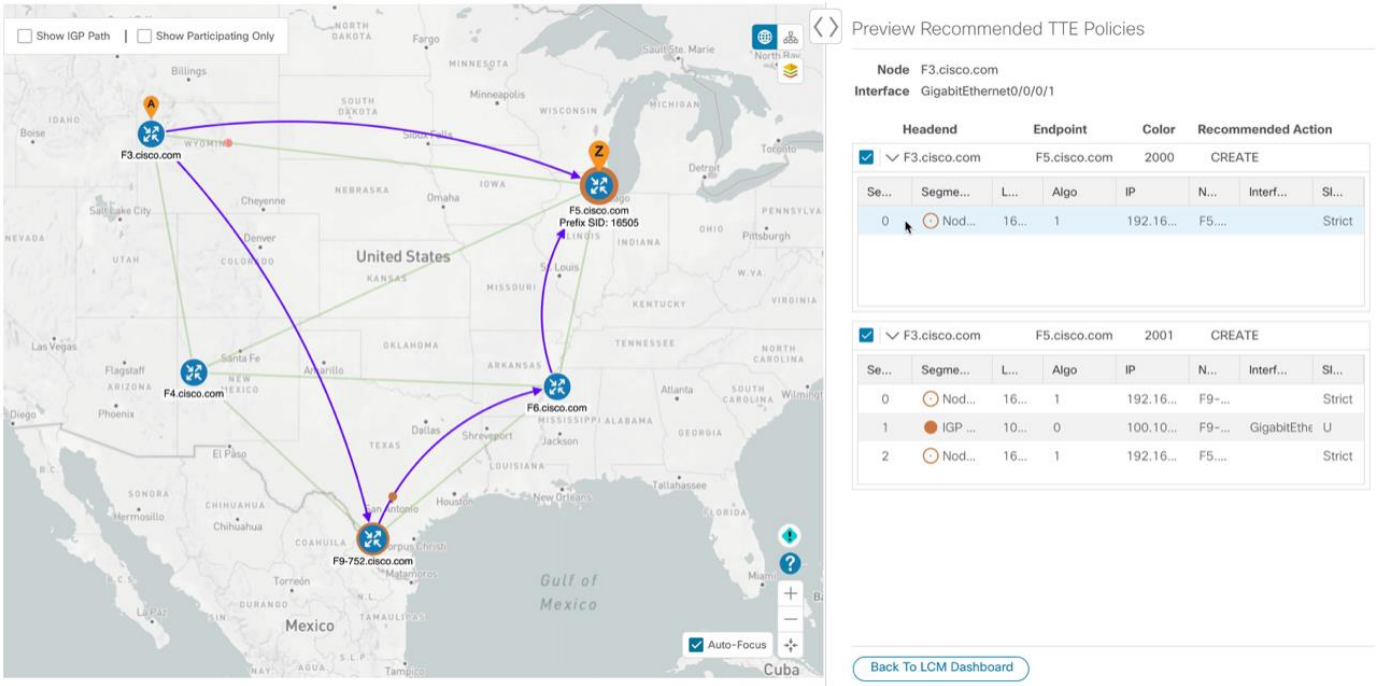


3. TTE ポリシーをコミットする前に、各 TTE ポリシー ソリューション セットの展開をプレビューできます。[アクション（Actions）] 列で [...] をクリックし、 [ソリューションのプレビュー（Preview Solution）] を選択します。



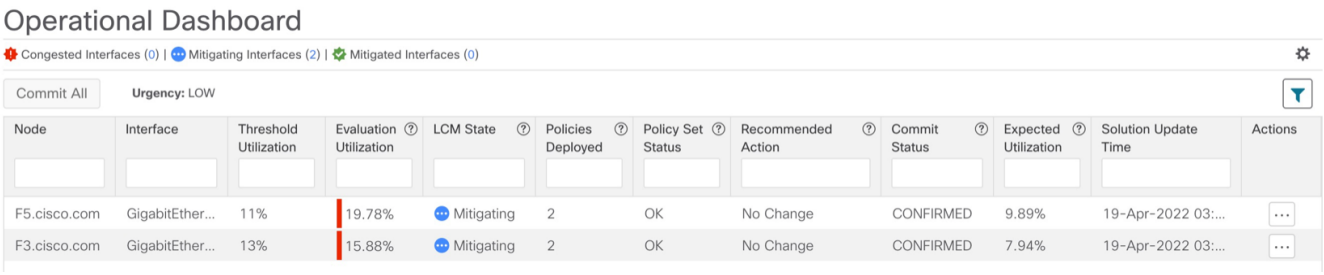
各 TTE ポリシーのノード、インターフェイス、および推奨アクションがウィンドウに表示されます。[Preview] ウィンドウから、個々の TTE ポリシーを選択し、トポロジマップで通常行っているように、さまざまな側面と情報を表示できます。各ポリシーを展開して、個々のセグメントを表示できます。ネットワークへの潜在的な影響を検討してから、LCM が推奨するバイパスポリシーを展開するかどうかを決定できます。

次の図に、ノード F3.cisco.com とインターフェイス GigabitEthernet0/0/0/4 の推奨 TTE ポリシーを示します。上のパスには、ノード SID（オレンジ色のアウトライン）、ヘッドエンド、エンドポイント（A および Z）が表示されます。これはマウスポインタが該当するセグメントの上にあるためです。



4. マップ上で推奨される TTE ポリシーを確認したら、[運用ダッシュボード（Operational Dashboard）] に戻り、[すべて確定（Commit All）] をクリックします。LCM の [ステータス（Status）] 列が [緩和中（Mitigating）] に変化します。

[Operational Dashboard] に示されているとおりに輻輳を緩和し、予想使用率を達成するには、ドメインごとに LCM のすべての推奨事項をコミットする必要があります。緩和ソリューションは、ソリューションセット間の依存関係により、コミットされているすべての LCM 推奨事項に基づいています。



ステップ 4. TTE SR ポリシーの展開を検証する

1. [Events] タブをクリックして、LCM イベントをモニターできる [Events] ウィンドウを開きます。LCM の推奨事項、コミットアクション、および例外のイベントが表示されます。

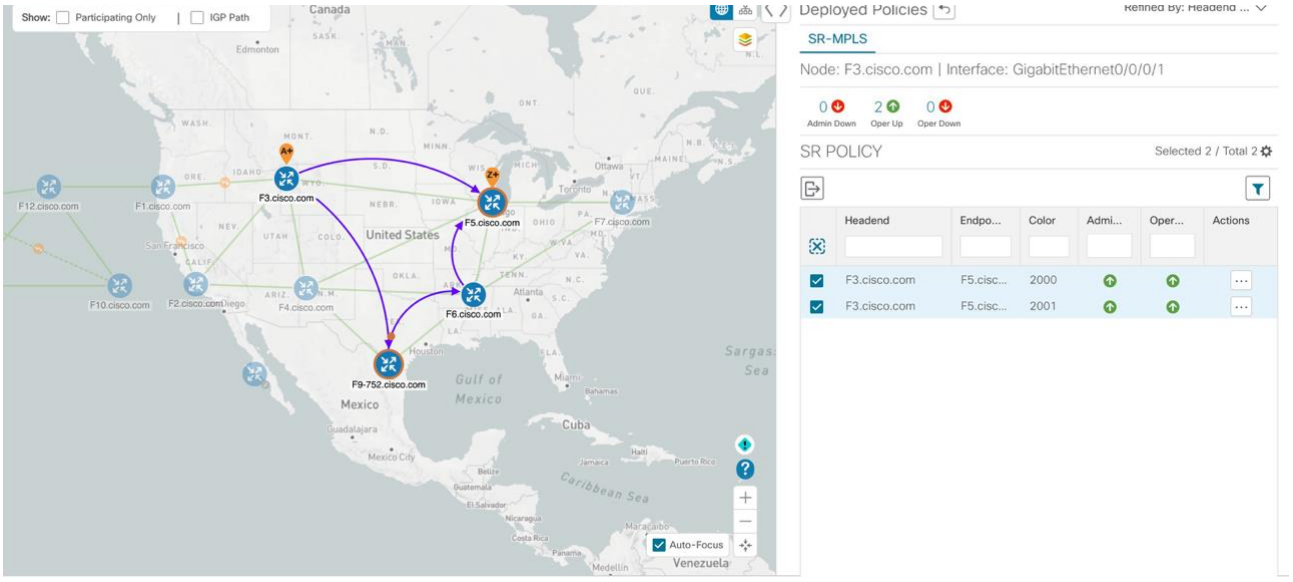
   注： Crosswork Optimization Engine は、有効にしたポリシーと機能に基づいて検出されたネットワークイベントを報告します。たとえば、リンクドロップによって SR-TE ポリシーがダウンした場合や、LCM が輻輳を検出した場合は、イベントが表示されます。これらのアラートは UI で報告され、必要に応じてサードパーティのアラート/モニタリングツールに転送できます。

2. [Operational Dashboard] に戻り、すべての TTE ポリシー ソリューション セットの LCM の状態が [Mitigated] に変化したことを確認します。

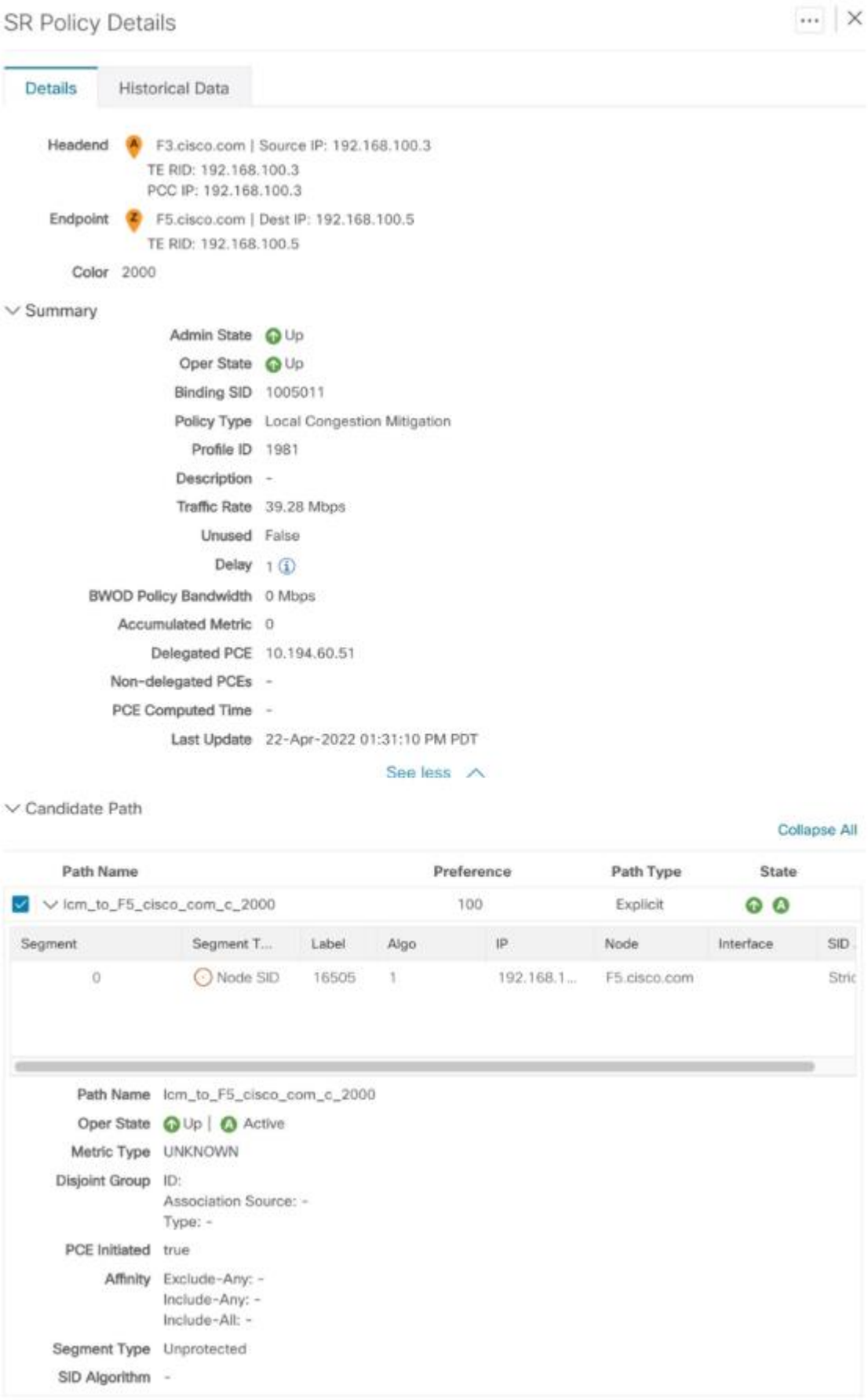
   注： LCM の状態が変化するまでに、SNMP パターンの 2 倍の時間がかかります。

3. トポロジマップを表示して、TTE ポリシーの展開を確認します。

   [アクション（Actions）] 列の [...] をクリックし、[展開されたポリシーを表示（View Deployed Policies）] を選択します。展開されたポリシーは、トポロジマップ内で強調表示されます。他のすべてのポリシーは淡色表示されます。



4. SR ポリシーの詳細を表示します。展開されたポリシーのいずれかの [アクション（Actions）] 列 で、[...] をクリックし、[詳細の表示（View Details）] を選択します。[ポリシータイプ（Policy Type）] が [ローカルでの輻輳緩和（Local Congestion Mitigation）] であることに注意してください。



ステップ 5. LCM の推奨に従って TTE SR ポリシーを削除する

1. しばらくすると、展開された TTE SR ポリシーが不要になる場合があります。これは、LCM によって開始された TTE ポリシーがなくても、使用率がしきい値を下回らない状況が続く場合に発生します。この場合、LCM は TTE SR ポリシーセットを削除するための新しい推奨アクションを生成します。
2. 以前に展開された TTE SR ポリシーを削除するには、[すべて確定（Commit All）] をクリックします。
3. トポロジマップと [SR ポリシー（SR Policy）] テーブルを表示して、削除を確認します。

まとめと結論

このシナリオでは、LCM を活用してネットワークのトラフィックの輻輳を軽減する方法を確認しました。LCM では、手動による追跡と計算は不要であり、同時に輻輳緩和の推奨事項を実装するかどうかを制御できます。推奨事項をプレビューして、展開する前にネットワークでの展開の有効性を確認できます。トラフィックが変化すると、LCM は展開された TTE SR ポリシーを追跡し、それらのポリシーがまだ必要かどうかを判断します。必要でない場合、LCM は削除を推奨します。

ネットワーク メンテナンス ウィンドウ

概要

目的

ネットワークの中断を最小限に抑え、最も効率的な結果を実現するように、メンテナンスワークフローをスケジュールして自動化します。

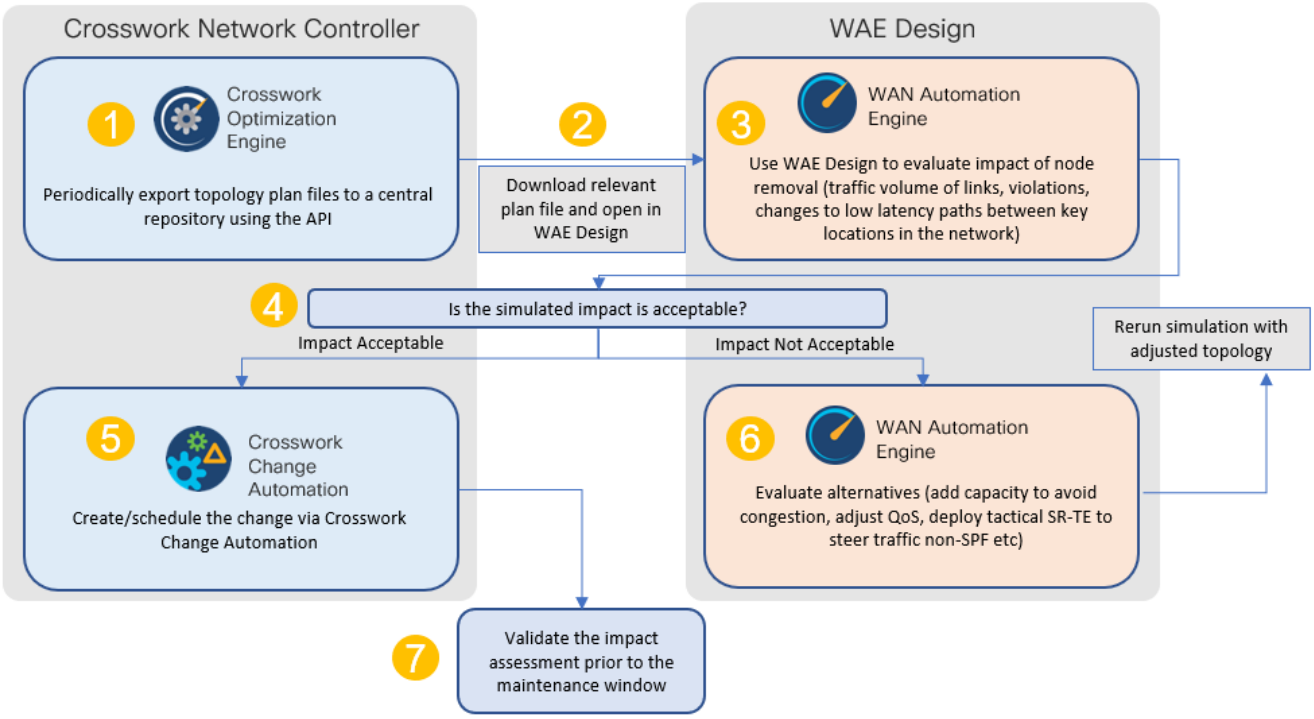
Challenge

メンテナンスアクティビティには、通常、システムのダウンタイムとサービスの一時的な中断が必要です。ダウンタイムや中断を最小限に抑えることは重要ですが、簡単ではありません。したがって、メンテナンスアクティビティは、慎重に計算された最適な時間帯（通常はアクティビティが最も少ない時間帯）に実行する必要があります。

ソリューション

Cisco Crosswork Change Automation および Cisco Crosswork Health Insights は、メンテナンスタスクのスケジューリングと実行を自動化するために必要な機能を提供する、オプションのアドオンアプリケーションです。メンテナンスアクティビティの最適な時間を計画することは、Cisco WAE Design を使用して実行でき、API を使用して Cisco Crosswork Network Controller からエクスポートされた時限トポロジスナップショットに基づいて「what-if」シナリオをシミュレートできます。

動作の仕組み



- Crosswork Network Controller API を使用すると、IGP トポロジやインターフェイスレベルの統計情報（トラフィック負荷）など、特定の時点でのトポロジ状態をキャプチャして表すトポロジスナップショット（計画ファイル）を作成できます。これらのスナップショットは影響分析を目的としており、次のメンテナンスアクティビティで評価対象とする期間を表す必要があります。たとえば、月曜日の深夜にルータのアップグレードを計画している場合は、月曜日の深夜のスナップショットを複数作成して、このタイミングでの一般的なトラフィック負荷を評価します。こうした計画ファイルは中央ストレージリポジトリにエクスポートできます。ここでは、トポロジ計画ファイルのライブラリを指定した期間保存できます。
- Cisco WAE Design では、メンテナンス期間の計画に関連する「what-if」シナリオを検討できます。たとえば、ルータをアップグレードする場合、Cisco WAE Design は、アップグレード中のデバイスからトラフィックが転送された後、残りのデバイスに生じるトラフィック負荷をシミュレートできます。また、戦術的なトラフィック エンジニアリング ポリシーを導入して、メンテナンス期間中にトポロジをさらに最適化する場合の影響を調べることもできます。詳細については、シスコ カスタマー エクスペリエンスの担当者にお問い合わせください。

使用シナリオ

[シナリオ 7：スケジュールされたメンテナンス期間中にプロバイダデバイスでソフトウェアアップグレードを実行する]

関連リソース

[Cisco Crosswork Change Automation and Health Insights ユーザー ガイド]

[Cisco WAE Design ドキュメント]

[Cisco DevNet の Cisco Crosswork Network Automation API ドキュメント]

シナリオ 7：スケジュールされたメンテナンス期間中にプロバイダデバイスでソフトウェアアップグレードを実行する

シナリオのコンテキスト

このシナリオでは、Cisco WAE Design を使用して、特定の期間中にソフトウェアアップグレードを実行するためにネットワークから P ノードを削除した場合の影響を評価済みであると想定します。今回のシナリオでは、デバイスでの SMU の実行を自動化するため、事前定義されたプレイブックを選択し、事前定義されたメンテナンス期間中に実行するようにスケジュールします。

仮定と前提条件

- Cisco Crosswork Change Automation がインストールされ、実行されている必要があります。
- Cisco WAE Design へのアクセス権が必要です。
- Crosswork Network Change Automation を動作させるには、デバイス上書きクレデンシャルを設定する必要があります。[Administration] > [Settings] > [System Settings] > [Network Automation] に移動します。

ワークフロー

- 影響分析のためのトポロジ計画ファイルをダウンロードする
- プレイブックを実行し、SMU をスケジュールして実行する
- SMU インストールジョブの完了ステータスを確認する

ステップ 1. 影響分析のためのトポロジ計画ファイルをダウンロードする

ネットワークへの影響を最小限に抑えるため、メンテナンスのためにデバイスをいつ停止させるべきかを検討する場合は、ターゲット時間でのそのデバイス周辺のトラフィックトレンドに関する情報が必要です。Cisco Crosswork Optimization API を使用すると、そのタイミングでのネットワークトポロジのスナップショットをキャプチャする計画ファイルをダウンロードできます。一定期間にわたって同じタイミングの計画ファイルをダウンロードすると、Cisco WAE Design を使用してトラフィックの傾向を分析できます。この分析に基づいて、ネットワークへの影響が許容可能かどうかを決定できます。

API の詳細については、Cisco DevNet の 『Cisco Crosswork Network Automation API Documentation』を参照してください。

手順

1. 計画ファイルをダウンロードするために必要な情報を準備します。分析に使用する Cisco WAE Design のバージョンと、計画ファイルの形式（txt または pln）を指定する必要があります。

   注： 計画ファイルを txt ファイルとしてダウンロードすると、任意のテキストエディタで表示できます。pln ファイルとしてダウンロードする場合は、Cisco WAE Design でのみ開くことができます。

   このシナリオで入力する情報は次のとおりです。

```
'{
  "input": {
    "version": "7.3.1",
    "format": "txt",
```

```
    }
  }
}'
```

2. 前の手順で準備した情報を使用して、Cisco Crosswork Network Controller サーバーで API を呼び出します。次に例を示します。

```
curl --location --request POST
'https://10.194.63.198:30603/crosswork/nbi/optima/v1/restconf/operations/cisco-crosswork-
optimization-engine-operations:get-plan \
--header 'Content-Type: application/yang-data+json' \
--header 'Accept: application/yang-data+json' \
--header 'Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbiIsImlzRnJvbU5ld0xvZ2luIjoidHJ1ZSIsInBvbGljeV9pZCI6ImFkb
WluIiwiYXV0aGVudGljYXRpb25EYXRlIjoiMjAyMS0wMy0yMlQxNjozODozNy43NDY2MTZaW0dNVF0iLCJzdWNjZXNzZnV
sQXV0aGVudGljYXRpb25IYW5kbGVycyI6IlF1ZXJ5RGF0YWJhc2VBdXRoZW50aWNhdGlvbkhhbmRsZXIiLCJpc3MiOiJod
HRwOlwvXC9sb2NhbGhvc3Q6NTQ4OVwvU1NPIiwibGFzdF9uYW1lIjoic21pdGgiLCJjcmVkZW50aWFsVHlwZSI6IlVzZXJ
uYW1lUGFzc3dvcmRDcmVkZW50aWFsIiwiYXVkIjoiaHR0cHM6XC9cLzEwLjE5NC42My4xOTg6MzA2MDNcL2FwcC1kYXNoY
m9hcmQiLCJhdXRoZW50aWNhdGlvbk1ldGhvZCI6IlF1ZXJ5RGF0YWJhc2VBdXRoZW50aWNhdGlvbkhhbmRsZXIiLCJsb25
nVGVybUF1dGhlbnRpY2F0aW9uUmVxdWVzdFRva2VuVXNlZCI6ImZhbHNlIiwiY2hhbmdlX3B3ZCI6ImZhbHNlIiwiZXhwI
joxNjE2NDU5OTIwLCJpYXQiOjE2MTY0MzExMjAsImZpcnN0X25hbWUiOiJqb2huIiwianRpIjoiU1QtODQtOFVlWXMybEt
3R2d1Z3RIYjl4MzVmTFlNTGVVRlp6OURyNGpoeFcxakhsV01VYXdXSWgxbUdTd01aRC1tOEk1S2Z0amI2ZmlWTUhlYnBYY
jBMMFZqRFc2WVppUFVUbHRpNFVpZnNUeG9aQ284WWpPWEc2VlFjS0Mwb29lWjJhc3BWanMzYnA3bHo5VkhySlBCTzl5TDN
GcFRIWXRPeWJtVi1jYXMtMSJ9.Vi4k0w8KsOv5M_O8zBqWochT3k9V9Pn2NjSn5ES9c5Pf-
4ds0o4kk6xuZx5_cggauiEICuUMnzmRzneST-oAuA' \
--data-raw '{
  "input": {
    "version": "7.3.1",
    "format": "txt",
    "
    }
  }
}'
```

3. API の応答で、計画ファイルの内容をメモしてください。これはセキュリティのためにエンコードされており、コンテンツを表示する前に復号する必要があります。

```
{
  "cisco-crosswork-optimization-engine-operations:output": {
    "status": "accepted",
    "plan-file content": "
PE5ldHdvcms+ClByb3BlcnR5CVZhbHVlClRpdGxlCQpWZXJzaW9uCTcuMy4xCgo8TmV0d29ya09wdGlvbnM+Ck9wdGlvbg
lWYWx1ZQpFbmZvcmNlQWRqU0lETG9jYWxpemF0aW9uCVRSVUUKCjxDaXJjdWl0cz4KTmFtZQl<<<>>>Ob2RlQQlJbnRlcm
ZhY2VBCU5vZGVCCUludGVyZmFjZUIJQ2FwYWNpdHkJRGVsYXkJRGlzdMJTmV0SW50U05NUF9FcnJvcglOZXRJbnRTb3VyY
2UJTmV0SW50UkUwQ1BVMW0JTmV0SW50UkUwQ1BVNWZpZXIJQWxnb3JpdGhtCVJmbGFnCU5mbGFnCVBmbGFnCUVmbGFnCVZ
mbGFnCUxmbGFnCg=="
  }
}
```

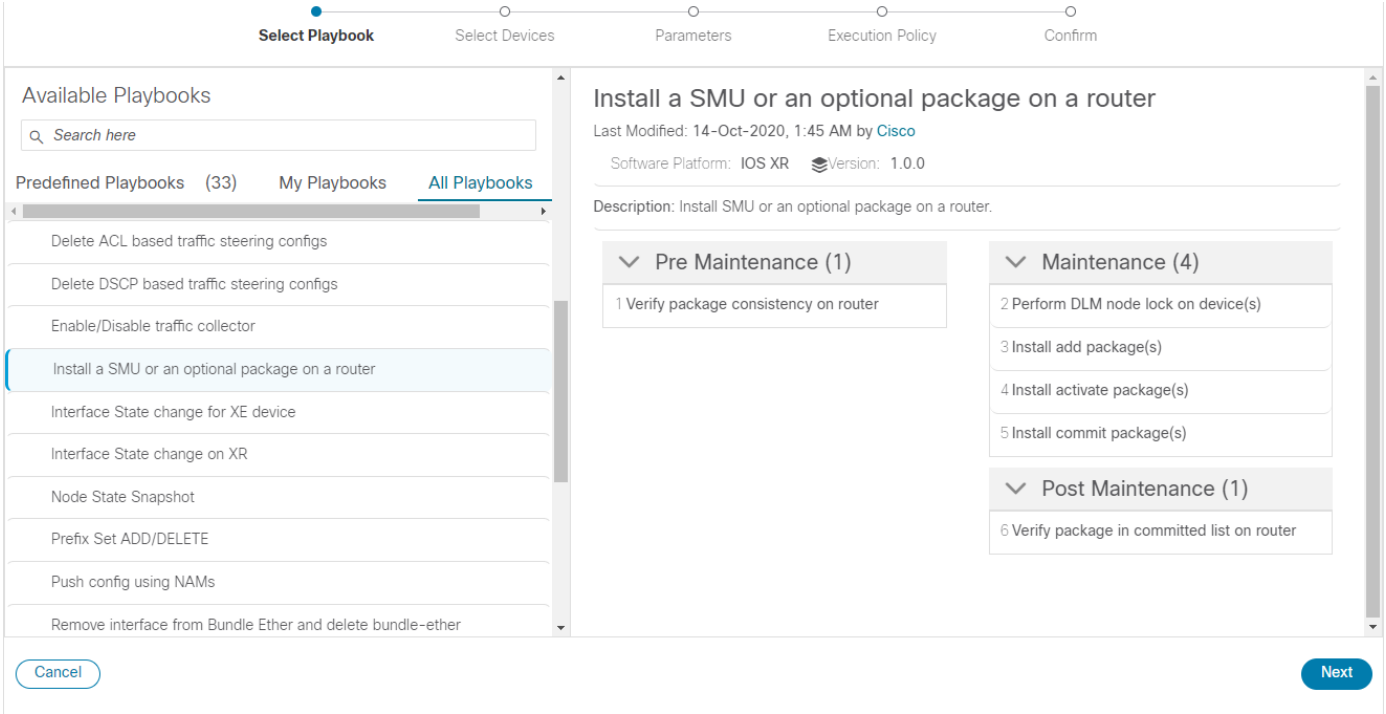
4. スクリプトを使用して計画ファイルを復号するか、計画ファイルの内容をデコーダにコピーします。計画ファイルを復号すると、Cisco WAE Design で使用するモデルの内容を確認できます。これには、デバイス、インターフェイス、リンク、LSP、トラフィックレベル、およびその他の情報を含むトポロジの完全なスナップショットが含まれます。
5. Cisco WAE Design で計画ファイルを開き、デバイスの停止をシミュレートし、ネットワークへの影響を観察します。詳細については、『Cisco WAE Design ドキュメント』を参照してください。
6. 分析に基づいて、SMU を実行する最適な時間を決定します。

ステップ 2. プレイブックを実行し、SMU をスケジュールして実行する

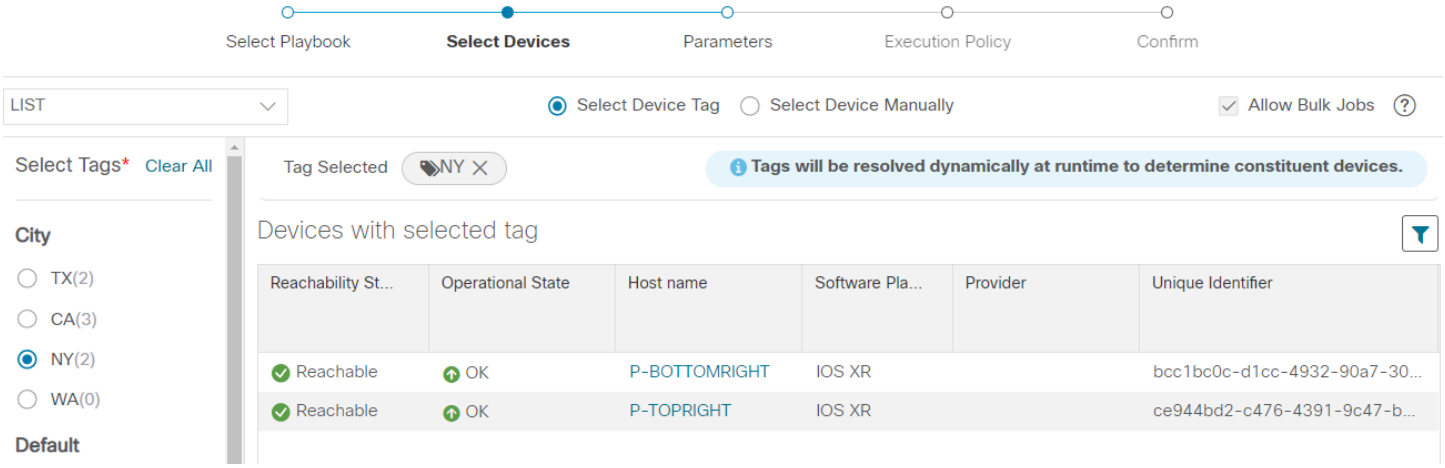
シミュレートした影響が許容できる場合は、Cisco Crosswork Change Automation を介してプレイブックを実行することで、変更を作成およびスケジュールできます。このシナリオでは、事前定義されたプレイブックを実行して、特定の地理的位置（ニューヨーク）がタグ付けされたデバイスにソフトウェア メンテナンス アップデート（SMU）をインストールします。

注： 事前定義された（ストック）プレイとプレイブックが特定のニーズを満たしていない場合は、カスタムプレイとカスタムプレイブックを作成できます。カスタムプレイを作成するには、[ネットワークの自動化（Network Automation）] > [プレイリスト（Play List）] に移動し、カスタムプレイブックを作成するには、[ネットワークの自動化（**Network Automation**）] > **[プレイブックリスト（Playbook List）]** に移動します。

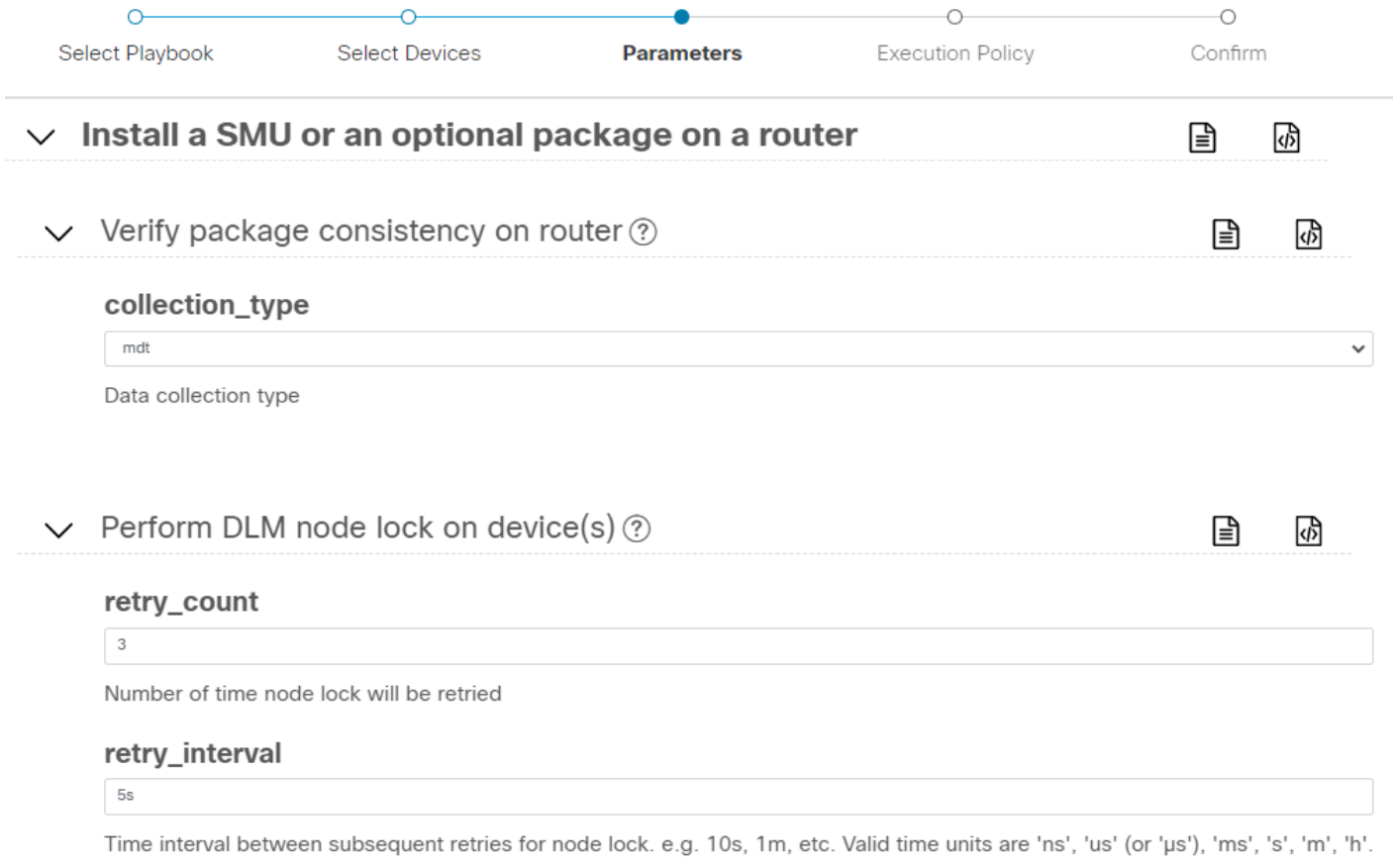
1. [Network Automation] > [Run Playbook] に移動します。
2. [Available Playbook] リストを参照し、[Install a SMU Playbook] をクリックします。また、キーワードを使ってフィルタリングし、プレイブックを特定することもできます。プレイブックの実行段階、サポートされているソフトウェア プラットフォーム、ソフトウェアバージョン、および個々のプレイの詳細が右側に表示されます。



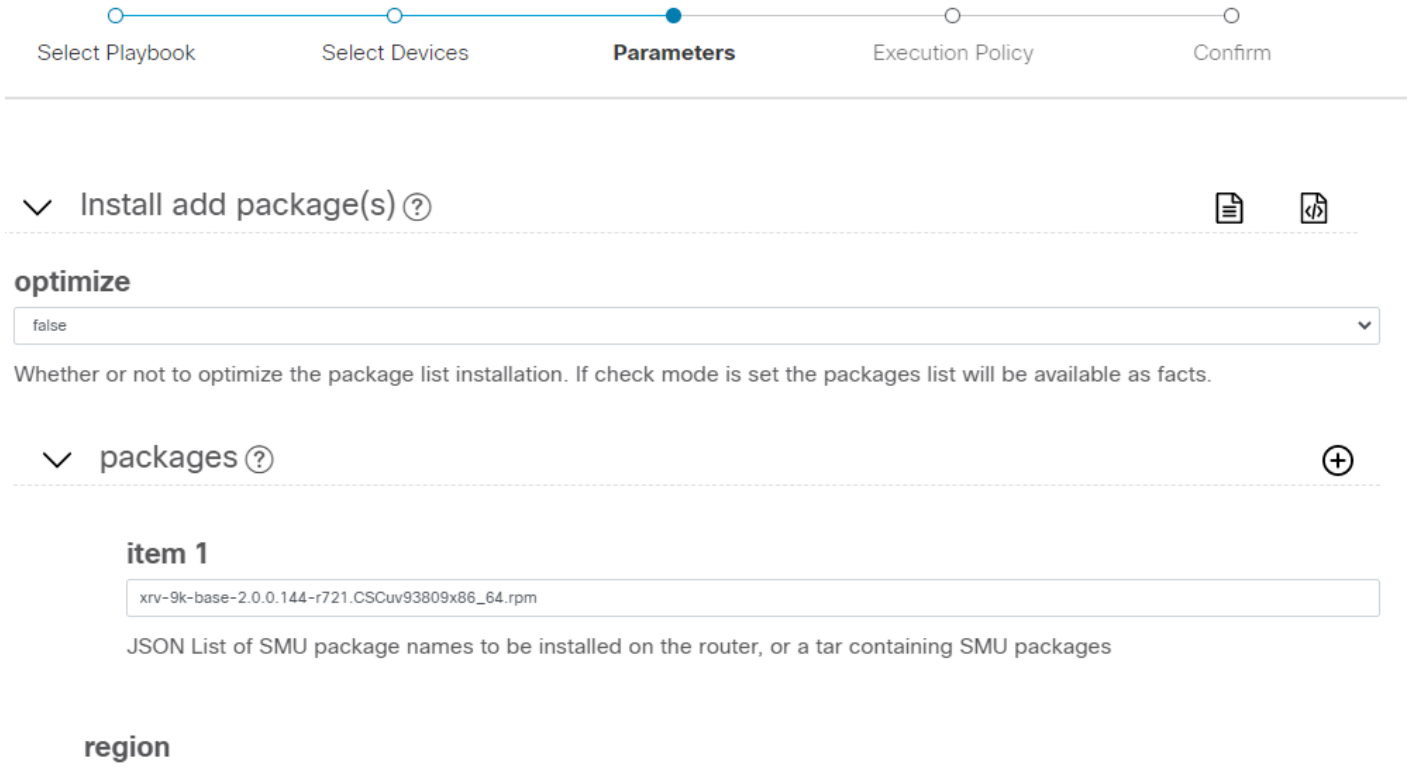
3. [Next] をクリックして、次のタスクである [Select Devices] に進みます。City: NY というタグが付いたすべてのデバイスを、SMU のインストール用に選択します。
4. 左側の [City] タグで、[NY] をクリックします。[NY] のタグが付いたデバイスが右側にリストされ、自動的に選択されます。



5. [Next] をクリックして、次のタスクである [Define Parameters] に進みます。
6. SMU プレイブックを実行するランタイムパラメータを編集します。または、パラメータ値を含む JSON ファイルをアップロードできます。このシナリオでは、特に次の値が使用されます。これらの値は必要に応じて変更できます。
   a. [verify package consistency on the device] プレイで、[collection_type] を [mdt] に設定します。
   b. [perform DLM node lock on device] プレイで、[retry_count] と [retry_interval] をそれぞれ [3] と [5s] に設定します。



c. [Install add package(s)] プレイで、[action] を [add] に、[optimize] を [false] に設定します。[item 1] に <SMU パッケージ名> を入力し、[region] を [NODES] に設定します。

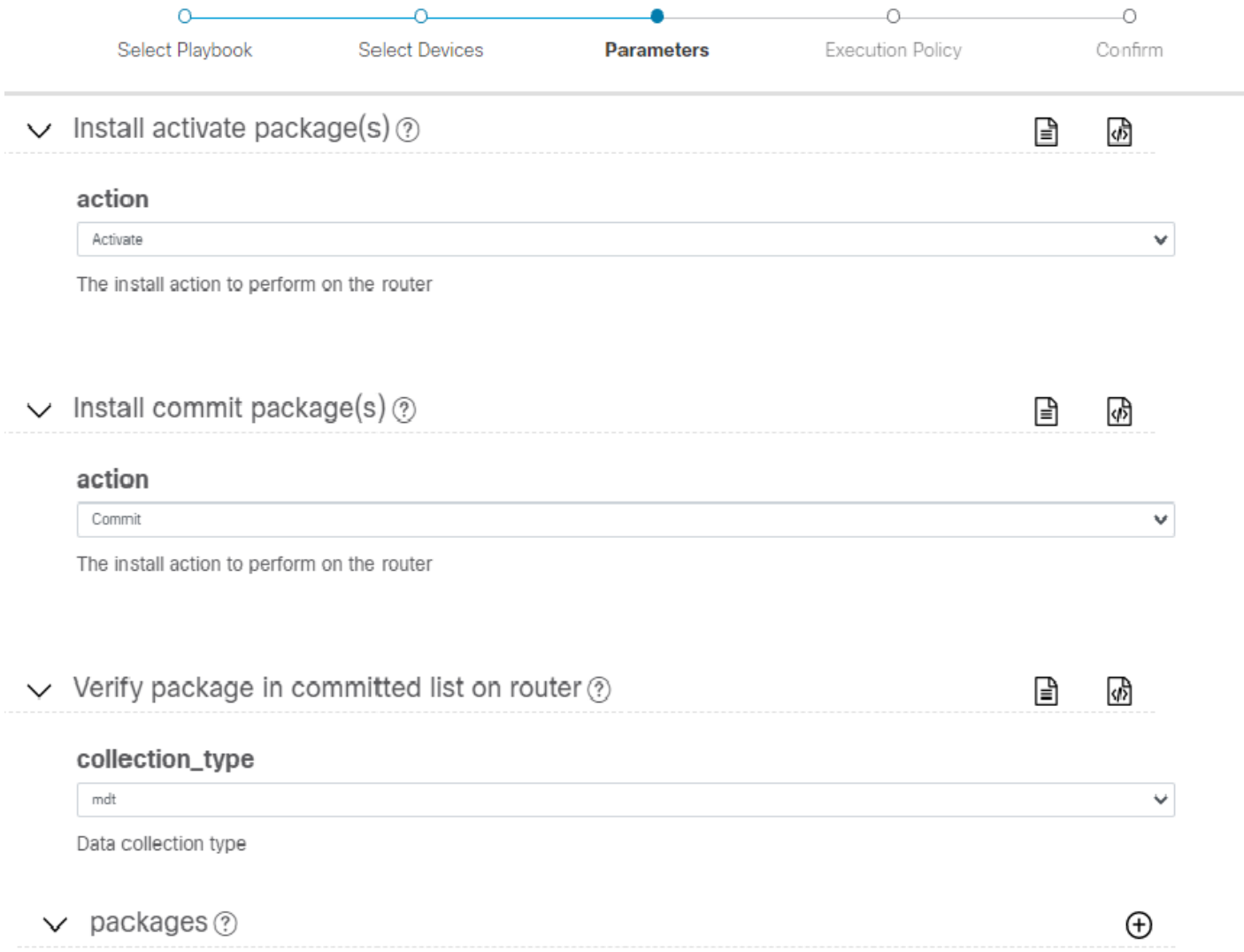


d. [type] を [SCP] に設定し、送信元、アドレス、宛先、および dlm_credential_profile の値を入力します。

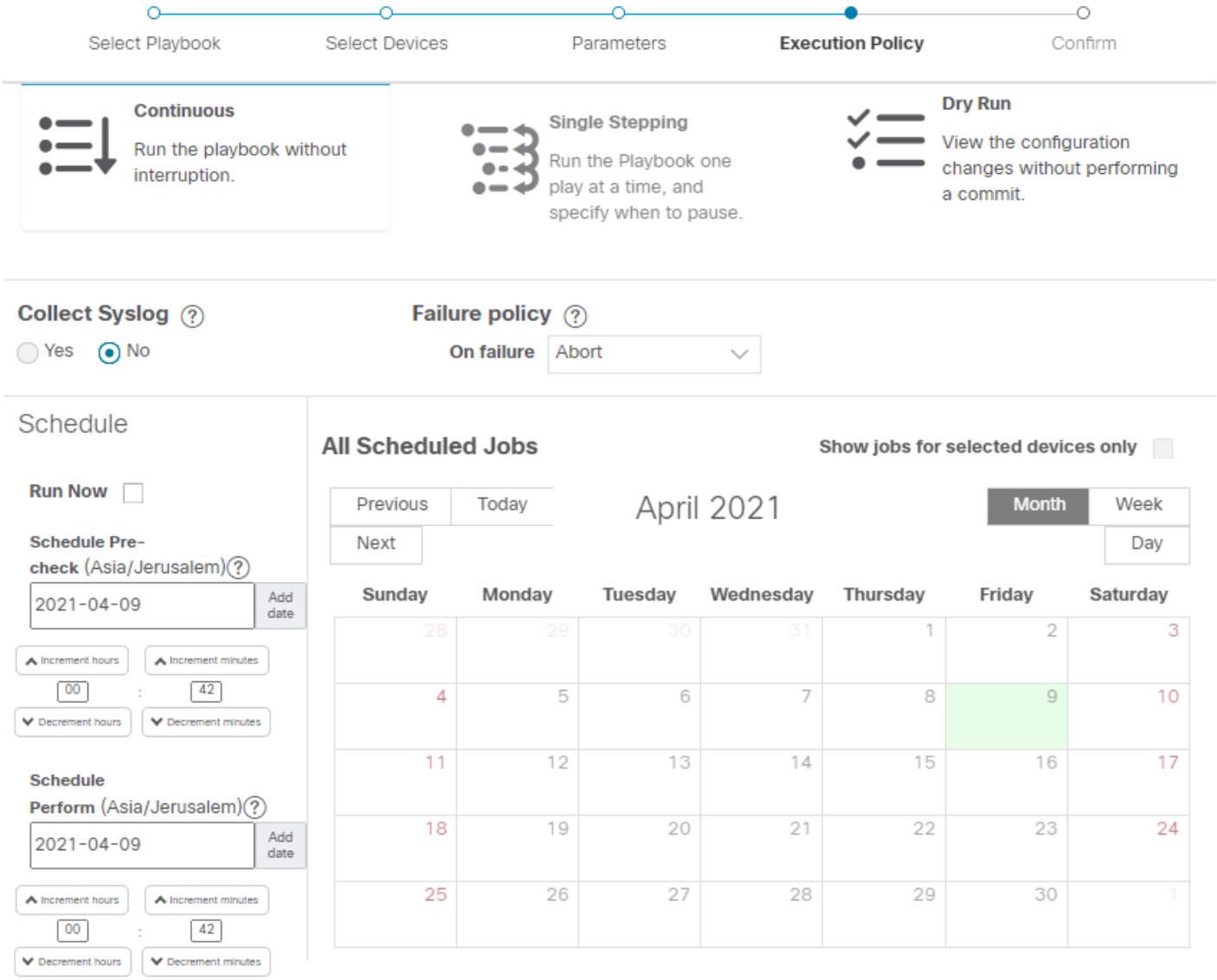
e. [Install activate package(s)] で をクリックし、アクションを選択して、[action] を [Activate] に設定します。

f. [Install commit package (s)] で、[action] を [Commit] に設定します。

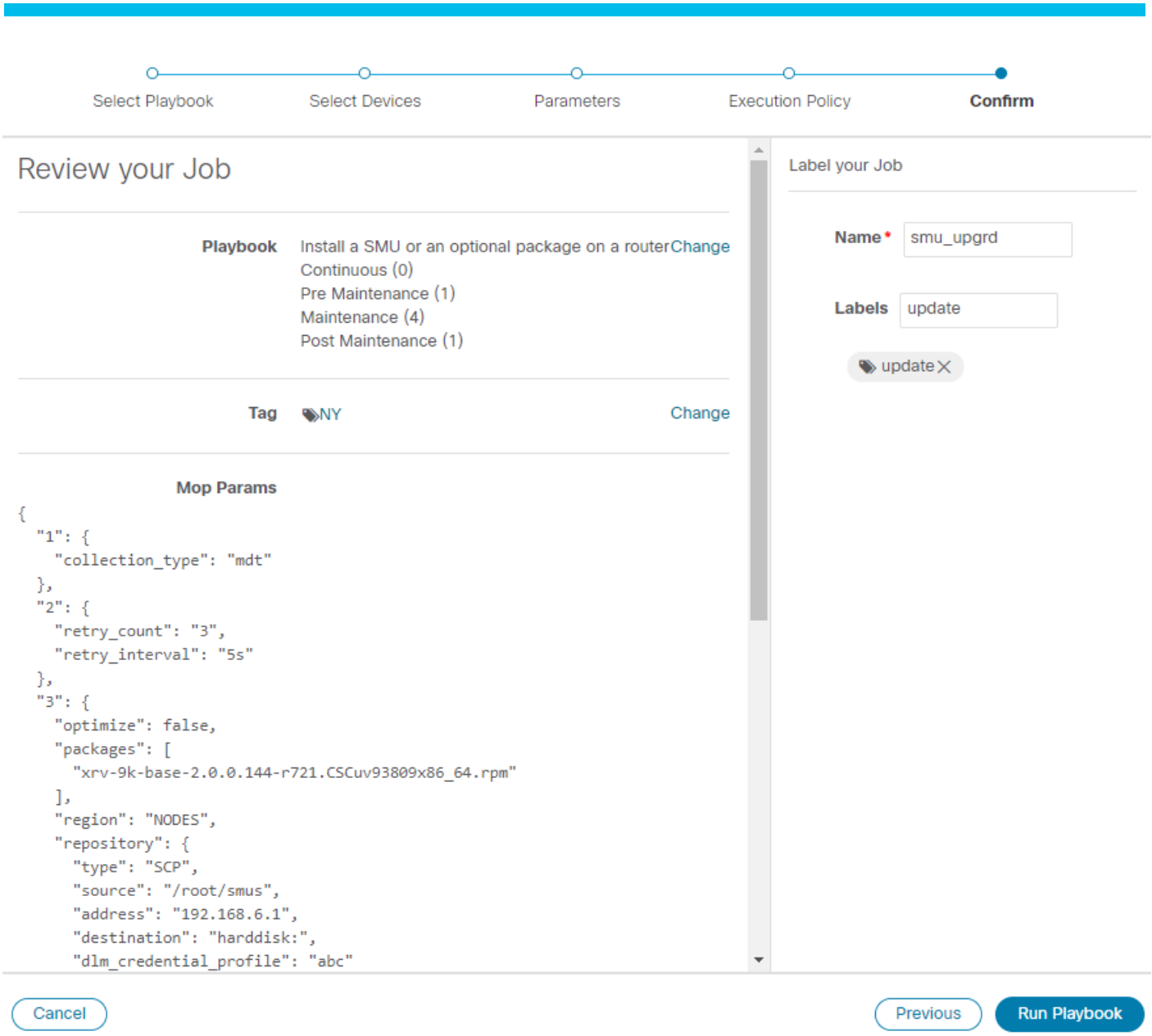
g. [Verify package in commited list on router] で、[collection_type] を [mdt] に設定し、[item 1] に <SMU パッケージ名> を入力します。



7. [Next] をクリックして、次のタスクである [Define Execution Policy] に進みます。
8. 実行モードとして [Continuous] を選択すると、プレイブックが中断することなく実行されます。[Failure policy] で、実行が失敗した場合に行うアクション（中止またはロールバック）を選択します。
9. 影響分析の段階で計算された最適な時間での実行をスケジュールします。[Run Now] オプションをオフにします。事前チェックのスケジュールとプレイの実行のため、カレンダーとタイマーが表示されることに注意してください。スケジュールされたメンテナンスの日時を選択します。

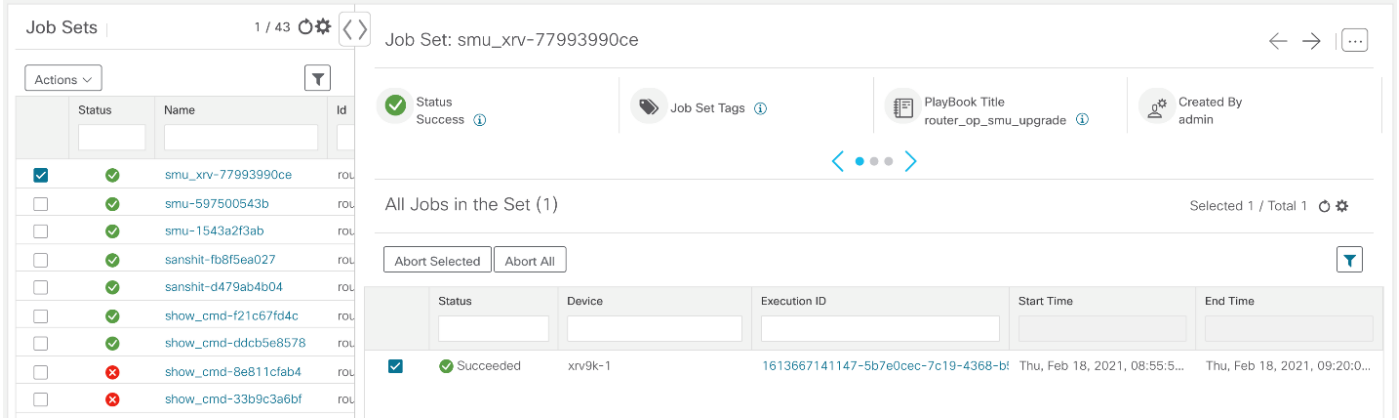


10. [Next] をクリックして、次のタスクである [Confirm Job] に進みます。
11. ジョブの詳細を確認します。ジョブに一意の名前を付けます。[Run Playbook] をクリックします。これで、SMU のインストールが計画されたメンテナンス時間帯に実行されるようにスケジュールが作成されました。

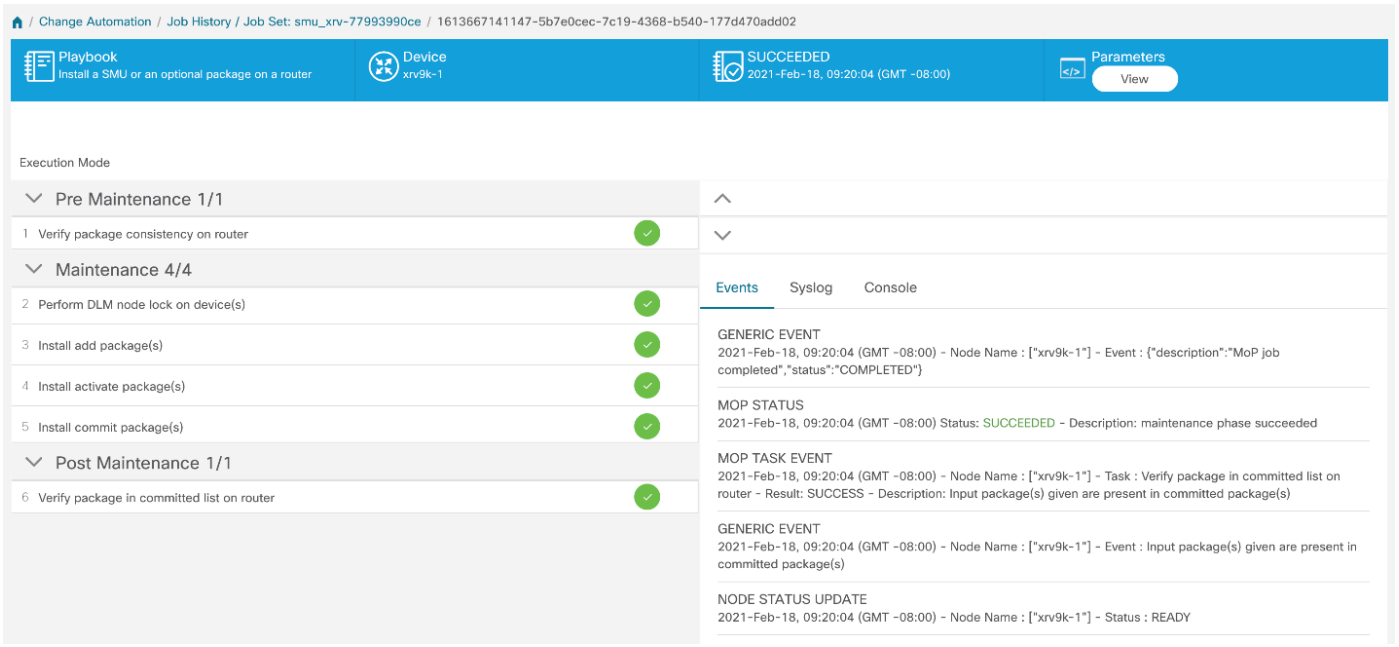


ステップ 3. SMU インストールジョブの完了ステータスを確認する

1. スケジュールされたメンテナンス時間帯の後に、[Network Automation] の [Automation Job History] に移動します。[Job Sets] で、SMU インストールジョブのジョブステータスアイコンが緑色になっていることを確認します。これは、スケジュールされたジョブが正常に実行されたことを示します。



2. SMU インストールジョブを選択します。右側のジョブセットの詳細に注意してください。ジョブの詳細を確認するには、実行 ID をクリックします。



3. デバイスで「show install active summary」コマンドと「show install commit summary」コマンドを実行し、インストールした SMU がリストに表示されることを確認することで、適切な SMU がインストールされていることを再確認します。これらのコマンドの出力例の一部を次に示します。

```
RP/0/RP0/CPU0:CX-AA-PE4#show install active summary
Mon Apr 12 11:09:20.198 EDT
    Active Packages: 12
        ncs5500-xr-6.6.3 version=6.6.3 [Boot image]
        ncs5500-ospf-2.0.0.0-r663
        ncs5500-mpls-2.1.0.0-r663
        ncs5500-eigrp-1.0.0.0-r663
        ncs5500-isis-2.2.0.0-r663
        ncs5500-li-1.0.0.0-r663
        ncs5500-mpls-te-rsvp-4.1.0.0-r663
        ncs5500-mcast-3.1.0.0-r663
        ncs5500-mgbl-3.0.0.0-r663
        ncs5500-k9sec-3.1.0.0-r663
        ncs5500-routing-4.0.0.17-r663.CSCvr43225
        ncs5500-mpls-te-rsvp-4.1.0.17-r663.CSCvr43225

RP/0/RP0/CPU0:CX-AA-PE4#show install committed summary
Mon Apr 12 11:09:27.092 EDT
    Committed Packages: 12
        ncs5500-xr-6.6.3 version=6.6.3 [Boot image]
        ncs5500-ospf-2.0.0.0-r663
        ncs5500-mpls-2.1.0.0-r663
        ncs5500-eigrp-1.0.0.0-r663
        ncs5500-isis-2.2.0.0-r663
        ncs5500-li-1.0.0.0-r663
        ncs5500-mpls-te-rsvp-4.1.0.0-r663
        ncs5500-mcast-3.1.0.0-r663
        ncs5500-mgbl-3.0.0.0-r663
        ncs5500-k9sec-3.1.0.0-r663
        ncs5500-routing-4.0.0.17-r663.CSCvr43225
        ncs5500-mpls-te-rsvp-4.1.0.17-r663.CSCvr43225

RP/0/RP0/CPU0:CX-AA-PE4#
```

まとめと結論

このシナリオでは、デバイスをダウンさせるメンテナンス時間帯を計画し、SMU をインストールする方法について説明しました。ネットワーク内のトラフィックにできるだけ影響を与えないようにすることが目標です。ネットワークへの影響を分析するために、メンテナンス時間帯のターゲット時間にネットワークトポロジのスナップショット（計画ファイル）をダウンロードする方法を示しました。計画ファイルは、Cisco WAE Design を使用して分析できます。影響が許容範囲内であると想定して、SMU を特定のデバイスにインストールするための事前定義されたプレイブックを選択し、ネットワークへの影響が最も少ない計画メンテナンス時間帯にスケジュールしました。

プログラム可能なクローズドループの修復

概要

目的

異常を検出し、オペレータへの通知や自動化ワークフローのトリガーに使用できるアラートを生成します。

Challenge

ネットワーク内の問題を検出して修復するには、通常、ネットワークオペレータの手動での介入が必要であり、時間がかかり、エラーが発生しやすくなります。

ソリューション

Cisco Crosswork Change Automation と Cisco Crosswork Health Insights を Cisco Crosswork Network Controller に組み込むことで、サービスプロバイダは、オペレータにアラームを事前定義された修復タスクに一致させることで、ネットワーク内の問題を検出して修復するプロセスを自動化できます。これらのタスクは、定義された重要業績評価指標（KPI）のしきい値を超えた後に実行されます。修復は、ネットワークオペレータの設定とプリファレンスに応じて、ネットワークオペレータの承認あり/なしのどちらでも実装できます。

このようなクローズドループの修復を使用することで、ネットワークオペレータの手動での介入を通じてミスが発生し、追加のエラーが生じるリスクを最小限に抑えながら、問題の検出と修復にかかる時間を短縮できます。

動作の仕組み

スマートモニターリング

- スマートモニターリング機能は、グラフや表など、オペレータが使用可能な形式でデータを収集、フィルタリング、および表示するのに役立ちます。データ収集に必要な設定が Cisco Crosswork Network Controller、Cisco Crosswork Change Automation、および Cisco Crosswork Health Insights によってゼロタッチテレメトリ機能を使用して行われている間、オペレータはビジネス上の目標に集中することができます。
- 共通のコレクタを使用して、SNMP、CLI、およびモデル駆動型テレメトリを介してネットワークデバイスのデータを収集し、YANG で記述されるモデル化されたデータとして使用できるようにすることで、重複したデータ収集が回避され、デバイスとネットワークの両方の負荷が最適化されます。
- 推奨エンジンは、ネットワークデバイスのハードウェアとソフトウェアの設定を分析し、データマイニングから構築された事前トレーニングモデルを使用して、ユースケースごとのモニターリングを促進する KPI 関連の推奨事項を生成します。
- KPI は、CPU、メモリ、ディスク、レイヤ 1/2/3 ネットワークカウンタから、プロトコルごとの LPTS および ASIC 統計まで、幅広い統計情報をカバーします。

スマートフィルタリング

- Cisco Crosswork Health Insights は、オペレータがユーザー定義のロジック（KPI）に基づいてネットワークイベントのアラートを監視および表示できる、動的検出および分析モジュールを構築します。
- 次のような重要業績評価指標（KPI）のアラートロジックを作成できます。
  - シンプルな静的しきい値（TCA）。たとえば、CPU 負荷が 90% を超過する場合。
  - 移動平均、標準偏差、パーセンタイルベースなど。たとえば、CPU 負荷が平均を上回っており、5 分間そのままである場合。
  - リアルタイムアラートを提供するストリーミングジョブ、または定期的に実行されるバッチジョブ。
  - しきい値と可視化ダッシュボード用にカスタマイズ。
  - ビジネスロジックに基づいてオペレータが作成したカスタマイズされた KPI 。
  - TCA は、HTTP、Slack、およびソケットインターフェイスを介してエクスポートしたり、他のシステムと統合したりできます。
- KPI はダッシュボードに関連付けられ、データと対応する TCA のリアルタイムのビューと過去のビューを提供します。
- また、KPI には専用のダッシュボードが用意されており、トリアージや根本原因となる複雑な問題の分析に役立つさまざまなインフォグラフィックスタイルのチャートとグラフで、生データを超えた有益な情報を提供します。

スマート修復

- Health Insights の KPI は、Cisco Crosswork Change Automation（CCCA）プレイブックに関連付けることができ、このプレイブックを手動または自動修復によって実行することができます。修復ワークフローを使用して、問題を修正したり、ネットワークデバイスからより多くのデータを収集したりできま

す。アドホックのデバッグや予定外のダウンタイムに頼るのではなく、プロアクティブに問題を修復することで、オペレータは時間とコストを節約し、顧客により優れた QOE を提供できます。

- Health Insights は、ネットワークトポロジのアラートまたは異常を相関させ、イベントの影響を簡単に視覚化できるようにします。

シナリオ 8：セグメント ルーティング アフィニティを使用した予測型のトラフィック ロード バランシングの実現

シナリオのコンテキスト

スムーズで最適なトラフィックフローを維持するには、オペレータがインターフェイス上のトラフィックをモニターし、CRC、ウォッチドッグ、オーバーランなどのエラーを特定し、SLA が維持されるようにトラフィックを再ルーティングできる必要があります。Cisco Crosswork Health Insights アプリケーションと Cisco Crosswork Change Automation アプリケーションがインストールされた Cisco Crosswork Network Controller を使用して、このプロセスを自動化することができます。

仮定と前提条件

Cisco Crosswork Health Insights および Cisco Crosswork Change Automation がインストールされ、実行されている必要があります。

ワークフロー

次に、このシナリオを実行するためのワークフローの概要を示します。

1. SR-PCE に委任された動的パス計算と、特定のアフィニティ（たとえば赤色のアフィニティ）でタグ付けされたリンクを除外するように設定された ODN を使用して、エッジノードにデイゼロ ODN テンプレートを展開します。ODN により、サービスヘッドエンドルータでは、必要に応じて（オンデマンドで）、BGP ネクストホップに対する SR ポリシーを自動的にインスタンス化できます。ODN テンプレートは、特定の色を使用して必要な SLA を定義します。

   ODN テンプレートを作成するための手順の例については、「シナリオ 1：SR-MPLS の L3VPN サービス向けの SLA の実装と保守（ODN を使用）」の「SLA 目標と制約に色をマッピングするための ODN テンプレートを作成する」を参照してください。

2. L3VPN ルートポリシーを作成して SLA を適用するプレフィックスを指定し、ODN テンプレートで使用されている色と同じ色でマークします。指定したネットワークから一致する色のトラフィックを受信すると、ODN テンプレートで定義された SLA に基づいてパスが計算されます。

   ルートポリシーを作成するための手順の例については、「シナリオ 1：SR-MPLS の L3VPN サービス向けの SLA の実装と保守（ODN を使用）」の「SLA 目標と制約に色をマッピングするための ODN テンプレートを作成する」を参照してください。

3. 必要なエンドポイント間で L3VPN をプロビジョニングし、VPN とルートポリシー間の関連付けを作成します。これにより、VPN と、SLA を定義する ODN テンプレートの間の接続が構築されます。

   L3VPN をプロビジョニングする手順の例については、L3VPN サービスの作成およびプロビジョニング

4. デバイスの KPI を定義して有効にします。これにより、L3VPN エンドポイントのアップリンク インターフェイスが継続的にモニターされます。

   KPI の定義については、「Cisco Crosswork Change Automation and Health Insights ユーザーガイド」を参照してください。

5. モニター対象インターフェイスでエラーが発生した場合は、ODN テンプレートの仕様に基づいて、ダーティリンクを除外するように赤色のアフィニティを設定します。これを実現するには、カスタムプレイブックを作成します。Cisco Crosswork Network Controller は、エラーに関するアラートを生成するインターフェイスの名前を学習し、これをカスタムプレイブックに入力して、アフィニティ設定を関連するルータにプッシュして、クローズドループの自動化シナリオを形成します。このようにすると、お客様がサービスの停止を経験することがありません。

   プレイブック の定義については、「Cisco Crosswork Change Automation and Health Insights ユーザーガイド」を参照してください。

6. Cisco Crosswork Network Controller は引き続きリンクをモニターし、アラートがなくなったら、赤色のアフィニティタグを削除できます。この目的では別のプレイブックを定義します。

ZTP を使用した IOS-XR デバイスのオンボーディングとプロビジョニングの自動化

概要

目的

ユーザーが新しいデバイスを迅速かつ簡単に、自動的にオンボーディングし、シスコ認定のソフトウェアイメージとデイゼロソフトウェア設定を使用してプロビジョニングできるようにします。

Challenge

ネットワークデバイスの導入と設定は、大変な作業です。知識豊富な担当者による大規模なハンズオンでのプロビジョニングと設定が必要であるため、時間と費用がかかり、エラーも発生しやすくなります。

ソリューション

Crosswork Zero Touch Provisioning（Cisco Crosswork ZTP）を使用して、新しいデバイスのオンボーディングを自動化します。Cisco Crosswork ZTP を使用すると、トレーニングを受けた専門家が現場にいなくても、ネットワークデバイスをリモートでプロビジョニングできます。DHCP サーバーと ZTP アプリケーションでデバイスのエントリを確立したら、オペレータが行う必要があるのは、デバイスをネットワークに接続し、電源を入れ、リセットを押してデバイスをアクティブ化することだけです。認定されたイメージと設定がダウンロードされ、自動的にデバイスに適用されます。このような方法でプロビジョニングされると、新しいデバイスは Crosswork デバイスインベントリにオンボーディングされ、他のデバイスと同様に監視および管理できるようになります。

動作の仕組み

- Classic ZTP：DHCP サーバーは、デバイスのシリアル番号に基づいてデバイスの ID を確認してから、ブートファイルとイメージのダウンロードを提供します。デバイスがイメージ化されると、コンフィギュレーション ファイルがダウンロードされ、実行されます。
- Secure ZTP：デバイスと Cisco Crosswork ZTP ブートストラップサーバーは、デバイスの Secure Unique Device Identifier（SUDI）および Crosswork サーバー証明書を TLS/HTTPS 経由で使用して相互に認証します。セキュアな HTTPS チャネルが確立されると、Crosswork ブートストラップサーバーは、

RFC 8572 YANG スキーマに準拠した一連の署名付きイメージと設定アーティファクトをダウンロードして適用するようにデバイスに要求します。イメージ（存在する場合）をダウンロードしてインストールし、デバイスが新しいイメージをリロードすると、デバイスは設定スクリプトをダウンロードして実行します。

- プラグアンドプレイ（PnP）ZTP：IOS-XE デバイス上の Cisco PnP エージェントと Cisco Crosswork PnP サーバーは、TFTP サーバーで提供される PnP プロファイルを使用して、HTTP 経由で相互に認証します。次に、HTTPS 経由でセキュアな接続を確立し、PnP エージェントがイメージ（オプション）と設定アーティファクトをダウンロードしてインストールします。

関連リソース

詳細については、『Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide』の「ZTP」の章を参照してください。

シナリオ 9：ネットワーク内の新しいデバイスの自動オンボーディングとプロビジョニング

シナリオのコンテキスト

サービス プロバイダ ネットワークの急激な成長と、新しいお客様拠点や新しい場所への急速な拡大に伴い、ますます多数のエッジデバイスを接続するニーズがあります。同時に、機能の高度化が進み、これらのデバイスを設定して新しいサービスをアクティブ化するのにより多くの時間がかかるようになっています。手動のプロセスでは、サービスプロバイダがネットワークを迅速に拡張し、新しいサービスをコスト効率の高い方法で展開する能力が限られます。

このシナリオでは、遠隔地にある新しいお客様拠点をセットアップして稼働させるために必要な、新しい IOS-XR デバイスをオンボーディングします。プロビジョニングを完了させるために熟練した技術者を派遣して、時間とコストのかかるオンサイト訪問を行う必要はありません。

すでにセットアップされ稼働している既存のお客様拠点にあるデバイスの設定を活用することで、デバイスを迅速かつ効率的に稼働させるために必要なすべてが新しいデバイスのデイゼロ設定に含まれるようにします。

仮定と前提条件

- Cisco Crosswork Network Controller のセットアップに Crosswork ZTP をインストールする必要があります。
- Classic ZTP の場合、Crosswork とデバイスはセキュアなネットワークドメインに展開する必要があります。Secure ZTP にはこの要件はありません。ネットワーク全体で安全に使用できます。
- Crosswork サーバーは、アウトオブバンド管理ネットワークまたはインバンドデータネットワークを介してデバイスから到達可能である必要があります。
- デバイスを Cisco NSO にもオンボーディングする場合は、Cisco NSO を Crosswork プロバイダとして設定する必要があります。NSO プロバイダを設定する場合は、必ずプロバイダのプロパティキーを *forward* に設定し、プロパティ値を *true* に設定してください。

ワークフロー

これは、Cisco Crosswork Classic ZTP または Secure ZTP を使用して IOS-XR デバイスをオンボーディングするためのワークフローの概要です。

IOS-XE デバイスをオンボーディングする方法、またはこれらのオプションの詳細については、『Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide』の「ZTP」の章を参照してください。

- 手順 1：ZTP アセットの組み立てとアップロード
- 手順 2：イメージファイルとコンフィギュレーション ファイルを組み合わせた ZTP プロファイルを作成する
- 手順 3：オンボーディング対象のデバイスの ZTP デバイスエントリを準備する
- 手順 4：Crosswork ZTP 用の DHCP のセットアップ
- 手順 5：ZTP の処理を開始してデバイスをオンボーディングする
- 手順 6：ZTP 処理ステータスのモニター
- 手順 7：オンボーディングしたデバイスの確認

ステップ 1. ZTP アセットの組み立てとアップロード

1. 開始する前に、次のアセットを組み立てます。

   ◦（任意）ソフトウェアイメージ。Classic ZTP では、Cisco IOS-XR バージョン 6.6.3、7.0.1、7.0.2、7.0.12、および 7.3.1 以降を使用できます。Secure ZTP では、Cisco IOS-XR 7.3.1 以降を使用します（7.3.2 および 7.4.1 を除く）。

   ◦コンフィギュレーション ファイル：SH、PY、または TXT ファイル。Secure ZTP には、最大 3 つの異なるコンフィギュレーション ファイルを指定できます。

   ◦オンボーディングするデバイスのクレデンシャル

   ◦オンボーディングするデバイスのシリアル番号

   Secure ZTP の場合のみ、以下も組み立てます。

   ◦所有者証明書：組織の CA 署名入りのエンドエンティティ証明書。デバイスにインストールされ、公開キーが組織にバインドされているもの。

   ◦ピン留めドメイン証明書：組織の DNS ネットワークドメインにピン留めされた公開キーを持つ、組織の CA 署名入りまたは自己署名入りのドメイン証明書。PDC（ピン留めドメイン証明書）は、ZTP の処理中にダウンロードおよび適用されたイメージと設定が組織内からのものであることをデバイスが確認する際に役立ちます。

   ◦所有権バウチャー：ZTP でオンボーディングされているデバイスが、組織が所有するドメインにブートストラップされていることを確認するナンスレス監査バウチャー。組織の PDC およびデバイスのシリアル番号と一緒に要求が送信されると、シスコは OV（所有権バウチャー）を提供します。

2. ソフトウェアイメージを適用する場合：ソフトウェアイメージをアップロードします。[Device Management] > [Software Images] に移動します。
3. コンフィギュレーション ファイルをアップロードします。[Device Management] > [ZTP Configuration Files] に移動します。
4. デバイスのシリアル番号をアップロードします。[Device Management] > [Serial Number and Voucher] に移動し、[Add Serial Number] をクリックします。

5. Secure ZTP の場合は、固定されたドメイン証明書と所有者証明書をアップロードします。[Administration] > [Certificate Management] に移動し、証明書を追加します。
6. Secure ZTP の場合は、所有権バウチャーをアップロードします。[Device Manager] > [Serial Number and Voucher] に移動します。

ステップ 2. イメージファイルとコンフィギュレーション ファイルを組み合わせた ZTP プロファイルを作成する

Crosswork は、ZTP プロファイルを使用して、イメージングおよび設定プロセスを自動化します。ZTP プロファイルの作成は任意ですが、Cisco ASR 9000 や Cisco NCS5500 などの製品またはデバイスファミリに基づいて、単一のイメージファイルとコンフィギュレーション ファイルを結合するための最適な方法として推奨されます。デバイスファミリ、ユースケース、またはネットワークでデバイスが機能するロールごとに、デイゼロ ZTP プロファイルを 1 つ作成することをお勧めします。

ZTP プロファイルを作成するには、[Device Management] > [ZTP Profiles] に移動します。

ステップ 3. オンボーディング対象のデバイスの ZTP デバイスエントリを準備する

オンボーディングするデバイスの数に応じて、CSV ファイルを準備してインポートするか、デバイスエントリを個別に作成できます。

1. [Device Management] > [Devices] に移動します。
2. [Zero Touch Devices] タブをクリックします。実行されるアクション

- 多数のデバイスのデバイスエントリファイルを作成するには、[Import] アイコンをクリックし、CSV テンプレートをダウンロードします。テンプレートを編集し、オンボーディングする各デバイスのエントリを追加します。ファイルエントリの詳細については、「ZTP」の章を参照してください。次に、[Import] アイコンをもう一度クリックして、デバイスエントリファイルをインポートします。
- デバイスエントリを 1 つずつ作成するには、[Add] アイコンをクリックします。

ステップ 4. Crosswork ZTP 用の DHCP のセットアップ

ZTP の処理をトリガーする前に、ZTP デバイスエントリの ID と、ZTP リポジトリに保存されているイメージおよびコンフィギュレーション ファイルへのパスを使用して、組織の DHCP サーバー コンフィギュレーション ファイルを更新する必要があります。これにより、Crosswork と DHCP はこれらの ZTP デバイスを識別し、各デバイスのネットワークへの接続要求に正しく応答して、イメージファイルとコンフィギュレーション ファイルをダウンロードできます。DHCP エントリのサンプルについては、「ZTP」の章を参照してください。

ステップ 5. ZTP の処理を開始してデバイスをオンボーディングする

プロビジョニングする各デバイスを再起動して、ZTP の処理を開始します。デバイスを再起動するには、電源を再投入するか、シャーシのリセットボタンを押します。

ステップ 6. ZTP 処理ステータスのモニター

ダッシュボードで ZTP 処理の進行状況をモニターできます。

1. メインメニューで [Home] をクリックし、[Zero Touch Provisioning] ダッシュレットを確認します。

2. [View ZTP devices] リンクをクリックして、個々のデバイスのステータスを確認します。

ステップ 7. オンボーディングしたデバイスの確認

[Device Management] > [Devices] に移動します。[Zero Touch Devices] タブをクリックします。すべてのオンボーディングデバイスが表示されます。

場合によっては、一部のデバイスの情報を編集する必要があります。完全なデバイスレコードに必要な情報の一部は、デバイスのオンボーディングでは不要であるか、または自動化を通じて直接利用できないことがあります。たとえば、GPS 座標セットを使用して定義される地理的位置データなどが該当します。

ZTP デバイスは、オンボーディング後、自動的に Crosswork の共有デバイスインベントリの一部になりますので、他のデバイスと同様に編集できます。

ネイティブ SR パスの可視化

概要

目的

トラフィックが Inter-AS オプション C を介したネイティブ SR IGP パス（SR ポリシーではない）上にある場合でも、実際のパスのトラフィックフローをトポロジマップで物理的に可視化します。

Challenge

ネイティブ SR IGP パスを可視化することは、多くの場合、運用上の課題となります。合理化された使いやすいインターフェイスにアクセスできない場合、効率改善のためのソリューションがないと、ネイティブパスの診断とトラブルシューティングを行うためにネットワークデバイスに繰り返しログインしなければなりません。

ソリューション

パスクエリオプションにより、traceroute SR-MPLS multipath コマンドを使用してネイティブパスを可視化し、送信元と宛先の間の実際のパスを取得することを目指します。Cisco Crosswork Network Controller では、traceroute コマンドが送信元デバイスで宛先 TE ルータ ID に対して実行され、パスを取得することに役立ちます。Crosswork サーバーからネイティブ gRPC コールを使用することで、デバイスからパスを取得できます。これにより、トラフィックが流れるネイティブパスを可視化できます。traceroute コマンドを実行すると、統合に時間がかかる操作が発生する可能性があるため、Cisco Crosswork Network Controller では、この

ような操作の要求を送信し、出力を調べる準備ができたときに通知を受けることができる非同期ユーザーエクスペリエンスが提供されます。

動作の仕組み

- 使用可能なネイティブ SR IGP パスを検索するため、ヘッドエンドデバイスとエンドポイントデバイスを定義する新しいパスクエリを作成します。
- トポロジマップのクエリで定義されている使用可能なネイティブ SR IGP パスを可視化します。
- 使用可能なパスを調べ、出力、ネクストホップ、送信元、宛先、およびホップインデックスの情報を確認します。
- サービスタイプとインスタンスに基づいて、必要に応じて追加のパスクエリを作成し、トポロジマップ上でパスを可視化します。
- 問題のあったパスクエリをトラブルシューティングします。

使用シナリオ

シナリオ 10：Inter-AS オプション C を介したネイティブ SR パス間のパスのトラブルシューティング

シナリオのコンテキスト

パスのトラフィックフローの可視化は、さまざまなソースからの手動タスクなしで簡単に行うことはできません。トラフィックフローパスを取得しても、多くの場合、データは古くなっています。Cisco Crosswork Network Controller は、GUI 内で定義できるパスクエリの作成をサポートします。これにより、トポロジマップ上で送信元と宛先の間の実際の SR IGP パスを可視化できます。Cisco Crosswork Network Controller は、結果を調べる準備ができたときにユーザーに通知する、非同期ユーザーエクスペリエンスを提供します。これにより、ネイティブ トラフィック フローの問題を迅速にトラブルシューティングできます。

仮定と前提条件

- デバイスには IOS XR バージョン 7.3.2 が必要です。
- デバイスで gRPC（リモートプロシージャコール）が有効になっている必要があります。確認するには、デバイスで「show grpc」を実行し、次の手順を実行します。
  - セキュア接続のない gRPC の場合：gRPC が有効ではないと表示されている場合は、次のコマンドを使用して gRPC を有効にします。configure terminal; grpc; no-tls
  - セキュア接続のある gRPC の場合：次のコマンドを使用して、セキュリティ証明書を Cisco Crosswork Network Controller にアップロードしてデバイスに接続します。configure terminal; grpc
- Cisco Crosswork Optimization Engine サーバーには、gNMI（ネットワーク管理インターフェイス）機能とデバイスの gNMI 接続性を備えているデバイスがインポートされている必要があります。
  - クレデンシャルプロファイルに gNMI の接続情報が含まれていることを確認します。[Device Management] > [Credential Profiles] に移動します。[Credential Profiles] 画面が表示されます。編集するプロファイルを選択します。[Edit Profile Devices] 画面で、[+ Add Another] をクリックします。[Connectivity Type] で、[GNMI] を選択します。ユーザー名、パスワード、および確認用パスワード情報を追加します。[Save] をクリックします。

◦ デバイスをアタッチする際は、Cisco Crosswork Network Controller でデバイスの gNMI 機能を有効にする必要があります。[Device Management] > [Network Devices] に移動します。編集するデバイスを選択します。[Edit Device] 画面が表示されます。必要な機能リストから [GNMI] を選択します。[Save] をクリックします。

◦ デバイスの gNMI 接続情報が有効になるはずです。[Device Management] > [Network Devices] に移動します。編集するデバイスを選択します。[Edit Device Details] 画面の [Connectivity Details] で、[+ Add Another] をクリックします。[Protocol] で [GNMI] を選択し、IP アドレス/サブネットマスク情報を追加します。ポート情報を入力し、[Encoding Type] で [JSON] を選択します。[Save] をクリックします。

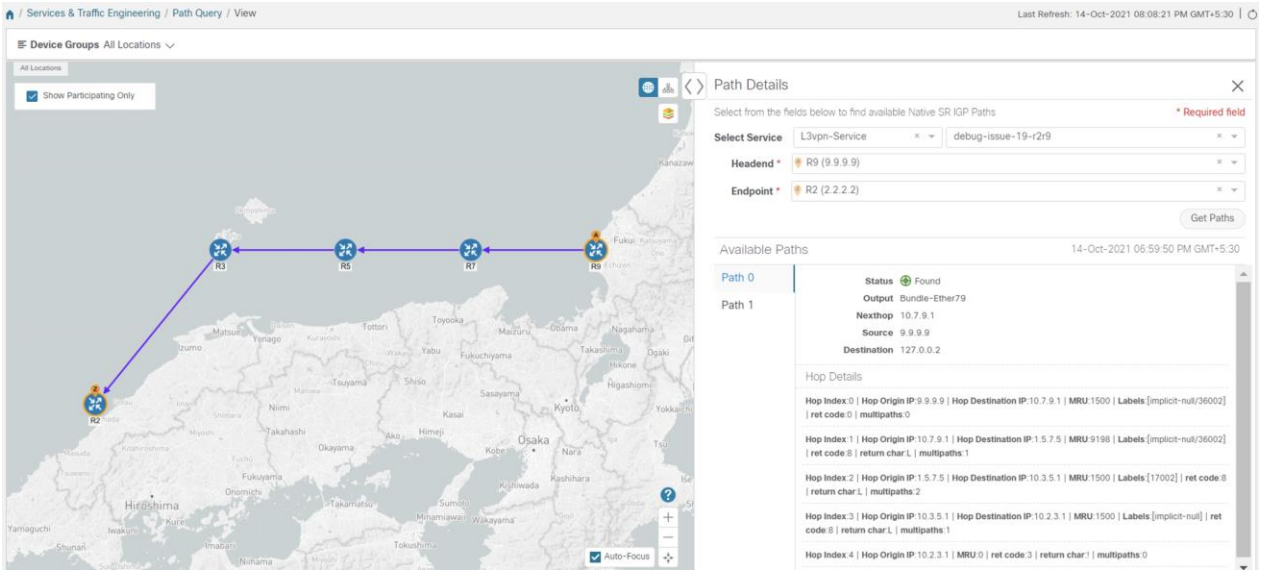
ワークフロー

1. [Services & Traffic Engineering] > [Path Query] を選択します。パスクエリのダッシュボードが表示されます。
2. [New Query] をクリックします。[New Path Query] パネルが右側に表示され、マッピングされた [Device Groups] パネルが左側に表示されます。
3. 必要なフィールドにデバイス情報を入力して、使用可能なネイティブ SR IG パスを検索します。
    a. リストからヘッドエンドデバイスを選択します。この例では、[P-Edge-A1] を選択します。
    b. リストからエンドポイントデバイスを選択します。この例では、[P-Edge-B2] を選択します。
4. [Get Paths] をクリックします。[Running Query ID] ポップアップが表示されます。注：パスクエリが完了するまで時間がかかる場合があります。
   [Running Query ID] ポップアップが表示されたら、[View Past Queries] を選択して、パスクエリダッシュボードに戻ることもできます。リストにすでにパスクエリが含まれている場合は、新しいクエリがバックグラウンドで実行され続けている間に既存のクエリの詳細を確認できます。これは、[Query State] 列の青色の実行アイコンで示されます。新しいクエリの状態が完了を示す緑色になったら、そのクエリを確認できます。
5. [View Results] が [Running Query ID] ポップアップで使用可能になったらクリックします。[Path Details] パネルが表示され、対応する [Available Paths] の詳細が表示されます。左側には、使用可能なネイティブ SR IG パスが定義されたトポロジマップとともに表示されます。
6. [Available Paths] オプション（[Path 0] や [Path 1] など）をクリックして、出力、ネクストホップ、送信元、宛先、およびホップインデックス情報のステータス詳細を確認します。使用可能なパスのいずれかを選択すると、Path 0 と Path 1 の対応するデバイス グループ トポロジ マッピングによりマップが更新されます。

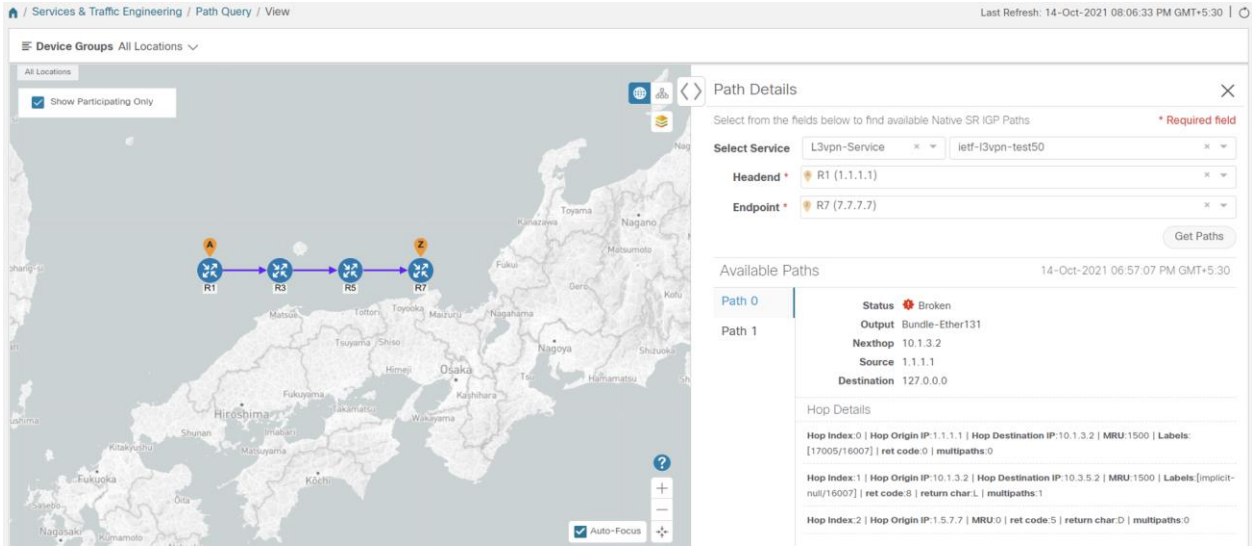
   注： マップの右上隅にある [Show Participating Only] チェックボックスがオンになっていることを確認します。

   注： パスクエリには 3 つのステータス結果があります。以下のスクリーンキャプチャは、このシナリオのワークフローに直接関連しない独立した例です。

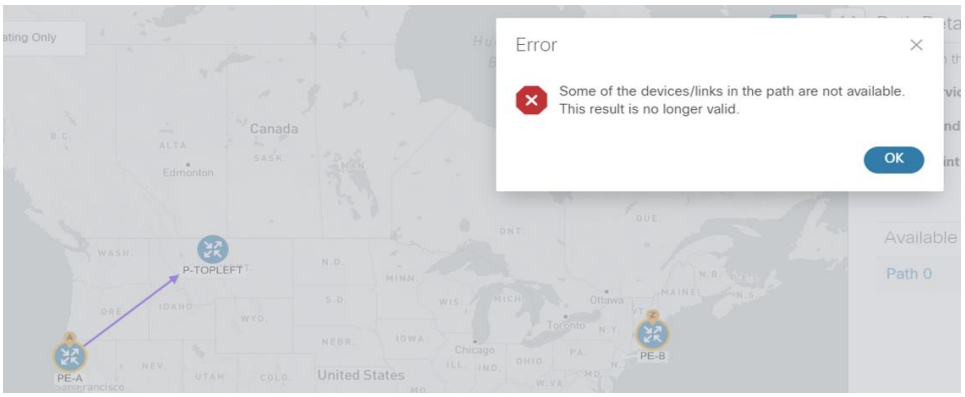
    a. **非分断パス（パスは完結）：パスステータスが [Found] と表示され、パスホップの詳細とオーバーレイが表示されます。**

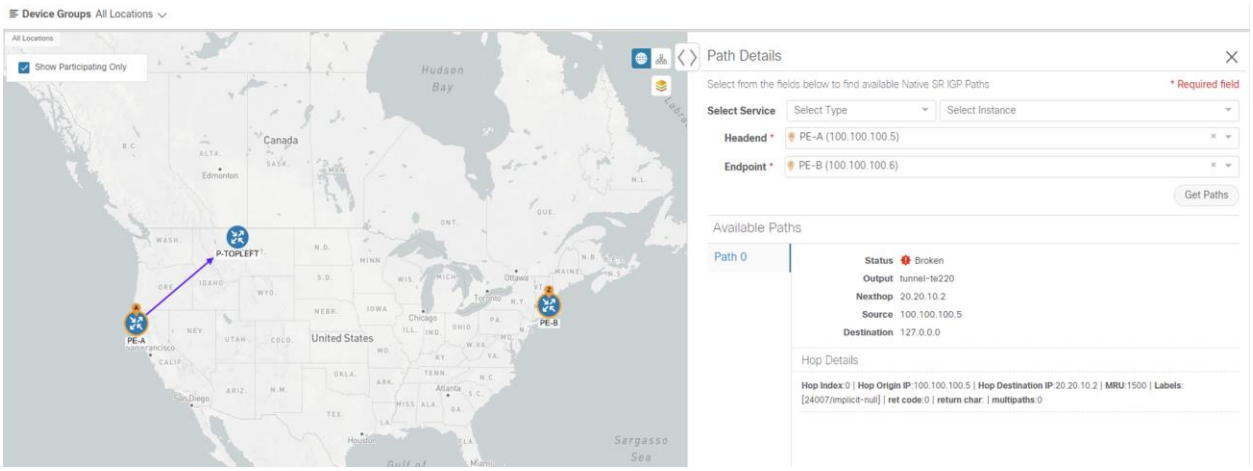


b. **分断パス（パスは完結）：パスステータスが [Broken] と表示され、パスホップの詳細とオーバーレイが表示されます。**



c. **分断パス（パスは未完結）：**パスステータスが [Broken] と表示され、パスホップの詳細が部分的に表示され（traceroute の gNMI 出力に依存します。トラブルシューティングの詳細については手順 17 を参照）、オーバーレイの詳細が部分的に表示されます。デバイスとリンクが使用できないことを示すエラーメッセージが表示されます。





7. [Services & Traffic Engineering] > [Path Query] を選択して、パスクエリダッシュボードに戻ります。
8. 新しいパスの [Query State] 列に、完了済みの緑色のアイコンが表示されていることを確認します。
   テーブル内の新しいパスには、対応するヘッドエンドと宛先エンドポイントの両方のクエリ ID リンクも表示され、どちらのパスでも [Available Paths] 列には [2] と表示されます。

   クエリの状態が壊れている場合は、ワークフローの最後の手順にあるトラブルシューティングの詳細を確認してください。
9. 必要に応じて、[Query ID] リンクをクリックするか、[...] をクリックして [View Details] を選択し、再度 [Path Details] パネルとマップを確認します。
10. [Services & Traffic Engineering] > [Path Query] を選択して、追加のパスクエリを作成します。パスクエリダッシュボードが表示され、以前のパスクエリがクエリ ID ごとにリストされます。

    注： パスクエリダッシュボードで、[Automatically delete query old than every < X >] オプションを必要な時間の範囲内で設定します。指定できる最大時間数は **24** です。

11. [New Query] をクリックします。[New Path Query] パネルが右側に表示され、マッピングされた [Device Groups] パネルが左側に表示されます。
12. [Select Service] で、リストから [Type] を選択します。この例では、[L2VPN-SERVICE] を選択します。
    [Select Service] を使用すると、後でヘッドエンドおよびエンドポイントを選択したときに、関連する VPN サービスタイプに応じてオプションが識別されます。
13. [Select Service] で、リストからインスタンスを選択します。この例では、**L2VPN_NM_P2P-Native-210** を選択します。
    トポロジマップが更新され、両方のサーバー間のパスが表示されます。この例では、論理パスを示すマップ上で **P-Edge-B2** と **P-Edge-C3** が分離されています。
14. リストから次の項目を選択します。
    d. ヘッドエンド：**P-Edge-B2**
    e. エンドポイント：**P-Edge-C3**
15. [Get Paths] をクリックします。
    [Running Query ID] ポップアップが表示されます。
16. 使用可能になったら、[View Results] をクリックします。[Path Details] パネルが表示され、対応する [Available Paths] の詳細が表示されます。左側には、使用可能なネイティブ SR IG パスが定義されたト

ポロジマップとともに表示されます。このビューには、トラフィックを伝送している B2 と C3 間の実際の物理ホップが表示されます。

17. [Path Query Dashboard] の [Query State] 列に表示される失敗したパスクエリをトラブルシューティングするには、[I] アイコンを選択してエラーの詳細を確認します。
この例では、ヘッドエンドの P-BOTTOMLEFT デバイスと、エンドポイントの P-BOTTOMRIGHT デバイスを使用した以前のパスクエリの [Connectivity Details] で、gNMI プロトコルが欠落しています。失敗したパスクエリをトラブルシューティングするには、次の手順を実行します。
    a. [Device Management] > [Network Devices] を選択します。
    b. ホスト名でデバイスを検索し、チェックボックスをオンにします。
    c. テーブルの上部にある編集アイコンをクリックします。[Edit Device Details] ポップアップが表示されます。
    d. この例では、プロトコルの [Connectivity Details] で gNMI が欠落しています。[+さらに追加（+ Add Another）] をクリックし、「GNMI」と入力して、リストに表示されるまで待ちます。これを選択します。
    e. IP アドレス/サブネットマスク情報とポートフィールド情報を入力します。
    f. [タイムアウト（Timeout）] フィールドに「**30**」と入力します。
    g. [エンコーディングタイプ（Endcoding Type）] リストで、「**JSON**」と入力し、リストに表示されるまで待ちます。これを選択して [保存（Save）] をクリックします。
    h. [Services & Traffic Engineering] > [Path Query] を選択します。パスクエリのダッシュボードが表示されます。
    i. [New Query] をクリックします。[New Path Query] パネルが表示されます。
    j. リストから以下を選択します。

        i. ヘッドエンドデバイス：**P-BOTTOMLEFT**
        ii. エンドポイントデバイス：**P-BOTTOMRIGHT**
    k. [パスの取得（Get Paths）] をクリックします。
    [Running Query ID] ポップアップが表示されます。
    l. 使用可能になったら、[View Results] をクリックします。[Path Details] パネルが表示され、対応する [Available Paths] の詳細が表示されます。左側には、使用可能なネイティブ SR IG パスが定義されたトポロジマップとともに表示され、完了状態となります。

マルチパスネットワークにおけるパスの検出、分析、および可視化

概要

事前にプロビジョニングされたツリーセグメント識別子（Tree-SID）セグメントルーティングパスをユーザーが簡単かつ迅速に可視化できるようにします。

目的

Cisco Crosswork Network Controller と Tree-SID を使用して、ネットワーク内の事前にプロビジョニングされたセグメントルーティングパス計算要素（SR PCE）パスを検出、分析、および可視化します。可視化により、ルート、リーフ、およびトランジットノードを表示するとともに、ノード間の各リンクに関する情報を表示できます。

Challenge

ネットワーク内の SR PCE パスを追跡することは、マルチパスプロトコルを使用してトラフィックを複製し、ネットワーク内のさまざまなポイントに送信する必要があるビデオブロードキャストおよびストリーミング サービス プロバイダーにとっての課題です。高レベルのサービス品質を確保するため、プロバイダーは、ポイントツーマルチポイント（P2MP）ネットワーク構成を可視化、更新、および維持管理する際に、難しい手動アプローチを使用する必要があります。その結果、ネットワークの問題への対応が遅くなり、コストが増大します。

ソリューション

Tree-SID は、セグメント化されたルーティングネットワーク上でツリーのようなマルチキャストフローを導入する手法です。Tree-SID を使用して、SDN コントローラ（PCEP を使用して SR-PCE を実行するデバイス）がツリーを計算します。ツリー内の各ノード（デバイス）には、ツリーを介してマルチキャストデータをルーティングする際の特定のロールがあります。これらのロールには、ルートまたはヘッドエンドノードの Ingress、リーフノードではないミッドポイントノードの Transit または Bud、宛先リーフノードの Egress が含まれます。ツリー自体には、ツリー内のすべてのツリーセグメントとデバイスを表す単一の SID ラベルが割り当てられます。SDN コントローラは非常に柔軟で、セグメンテーションを把握しており、ネットワークアーキテクトが指定できるあらゆる種類の制約を使用してルーティングパスを構築できます。

制約ベースの Tree-SID の最も興味深い使用例は、マルチキャスト Live-Live です。この場合、ルータは、異なるパスを介して同じコンテンツを含む 2 つの P2MP ストリームを配信するように設定されます。Live-Live では、マルチキャストフローがネットワーク経由で 2 回転送され、各コピーは固有のパスをたどります。2 つのコピーが同じノードまたはリンクを使用して宛先に到達することはないため、いずれかのパスでのネットワーク障害によるパケット損失が減少します。

現在 Cisco Crosswork Network Controller のこのリリースは、Tree-SID 可視化のみをサポートしており、PCE トポロジと LSP データを使用して Crosswork トポロジサービスマップを構築し、各 Tree-SID ツリーをトラフィック エンジニアリング ポリシーとして使用します。今後の Cisco Crosswork Network Controller リリースでは、Tree-SID 構成がサポートされる予定です。

動作の仕組み

- 事前定義された Live-Live Tree-SID 構成、それらのコンポーネントおよびロールを検出する
- 利用可能な Tree-SID パスの可視化

使用シナリオ

シナリオ 11：ポイントツーマルチポイント パスの検出と可視化

シナリオのコンテキスト

Cisco Crosswork Network Controller がない場合、Tree-SID のポイントツーマルチポイント トラフィック フローの可視化は、さまざまな送信元からの手動タスクを使用する場合にのみ利用できます。手動タスクに制約があるということは、可視化が妨げられることを意味します。これは、トラフィックフローパスの可視化ができるようになるまでに、データが古くなっていることがよくあるためです。Cisco Crosswork Network Controller は、ネットワーク構成から直接 Tree-SID セグメンテーションを検出する方法をサポートしており、データフローマップをすぐに表示します。そのため、Tree-SID トラフィックフローの問題を迅速にトラブルシューティングできます。

Cisco Crosswork Network Controller のトポロジサービスは、PCE トポロジと LSP データを使用して、ネットワーク内の事前設定された Tree-SID ポリシーを検出して可視化します。PCE コントローラは、BGP リンク状態を使用してレイヤ 3 トポロジ、LSP および Tree-SID データを管理し、Tree-SID ツリーの初期検出と通知をサポートします。

仮定と前提条件

このワークフローは、デバイスですでに設定されている PCE および Tree-SID ポリシーがネットワーク上に存在することを前提としています。少なくとも、これは次の基本設定オプションを想定しています。

1. Tree-SID パスに含まれるすべてのノードで、ロールに関係なく、次の操作を実行します。
    a. パス計算要素プロトコル（PCEP）の有効化
    b. 計算クライアント（PCC）の有効化
2. SR-PCE の下、エンドポイントで、P2MP SR の静的または動的ポリシーを設定します。
3. すべてのルートノードとリーフノードで、次の操作を実行します。

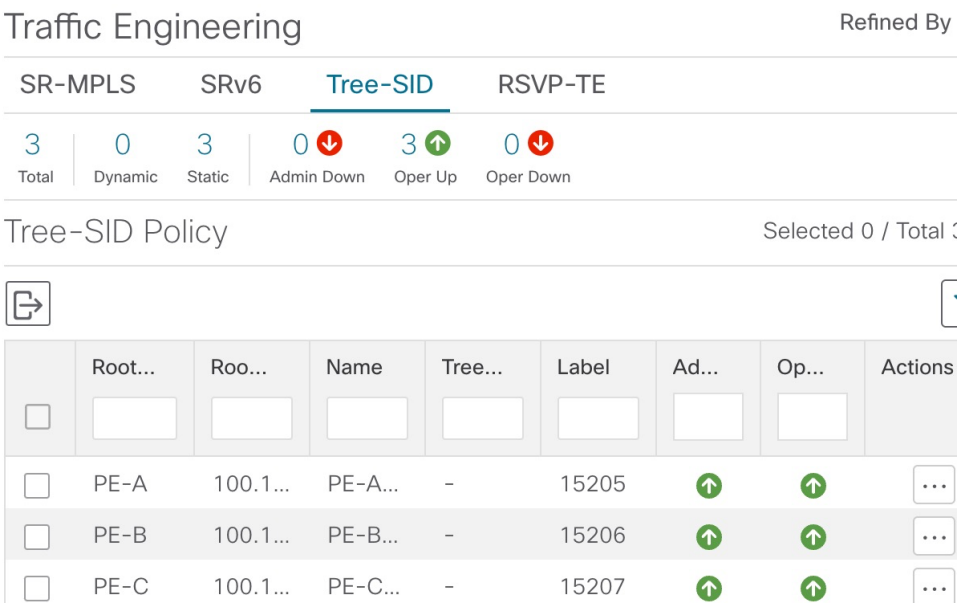
- マルチキャストルーティングの有効化
- `interface vrf <vrf-number>` の設定
- トポロジノードと PCE での `router bgp` の設定 PCE ノードと PCC ノード間の対応するネイバーで、設定された `interface vrf <vrf-number>` に言及
- `route-policy <vrf-number>` および `PASS_ALL` の設定
- セグメント ルーティング トラフィック エンジニアリングで、`ODN color <same as vrf-number>` を設定

4. すべてのリーフノードのみで、ルータ PIM、route-policy TREESID_CORE を設定

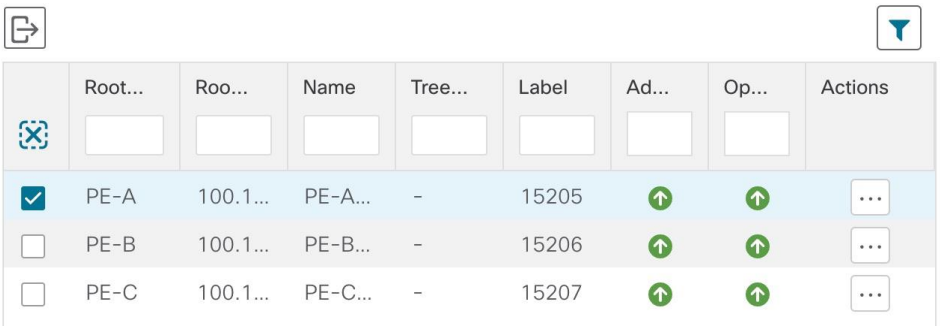
ワークフロー（Workflow）

1. [サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [トラフィックエンジニアリング（Traffic Engineering）] に移動します。
論理マップが開き、[トラフィックエンジニアリング（Traffic Engineering）] パネルがマップの右側に表示されます。

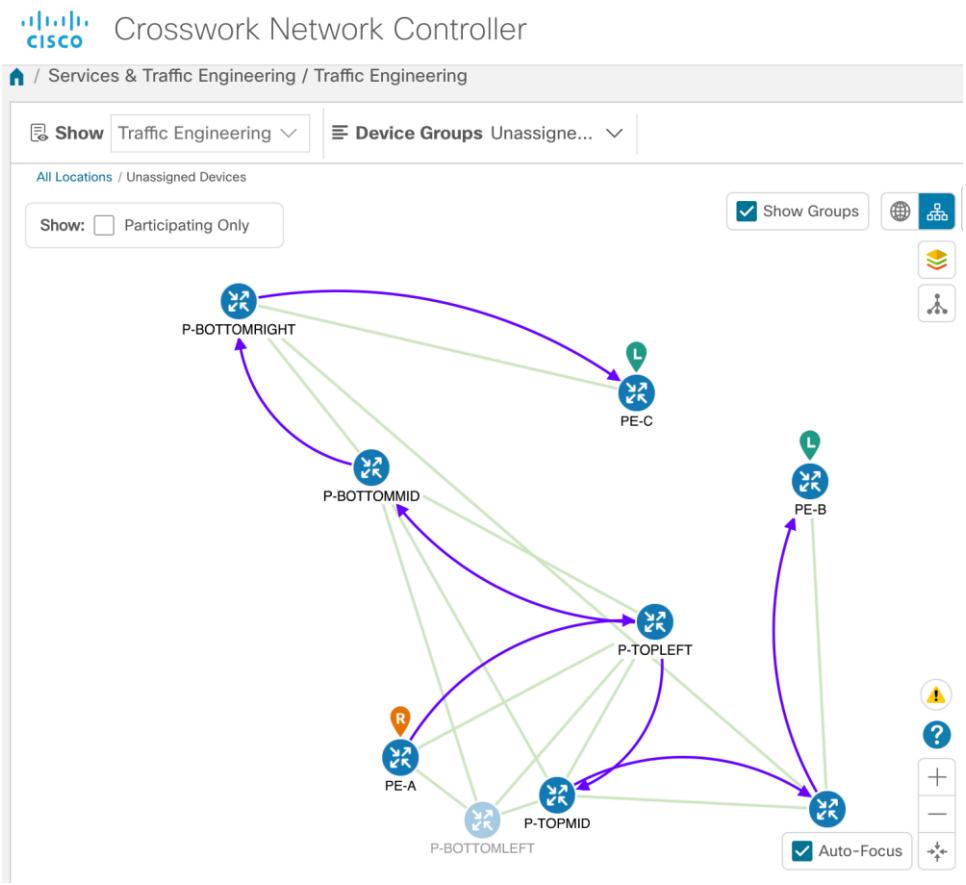
2. [トラフィックエンジニアリング（Traffic Engineering）] パネルで、[Tree-SID] タブを選択します。[Tree-SID ポリシー（Tree-SID Policy）] テーブルが開きます。



3. リストからルート IP Tree-SID ポリシー [PE-A] チェックボックスをオンにします。テーブルに多くのポリシーがある場合は、可視化する Tree-SID を見つけやすくなるように、ルート IP、名前、ラベル、またはその他のパラメータでフィルタリングします。



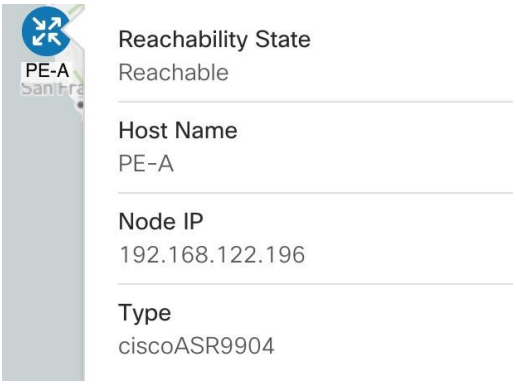
論理マップでは、トポロジ上のオーバーレイとして VPN が表示されます。マップには、ルート R デバイス（PE-A、入力デバイスとも呼ばれる）と 2 つのリーフ L ノード（PC-B と PC-C、出力デバイスとも呼ばれる）を示すアイコンフラグを含む、Tree-SID ポリシールートが示されており、それらの間に中間トランジットノードがあります。各ノードの管理および運用ステータスがテーブルに示されています。



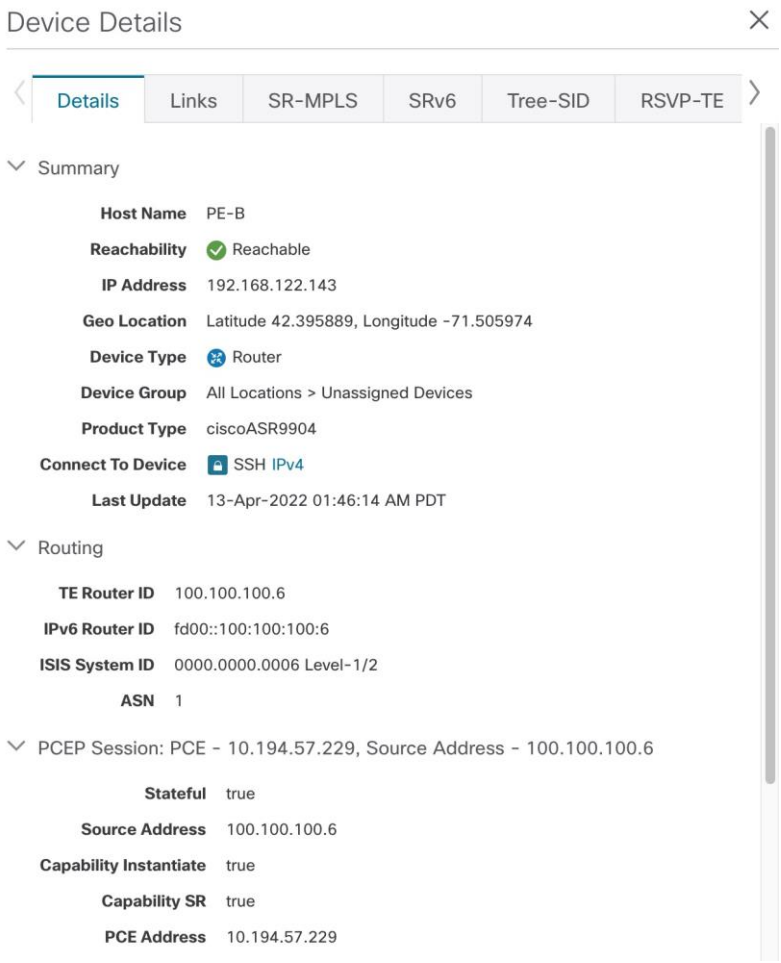
注： 論理マップの右上にあるボタンを使用して、論理マップと地理的マップ  を切り替えたり、表示設定を変更したりできます。

4. [Geo マップ（Geo Map）] ボタンを選択して、選択した Tree-SID サービストポロジを世界地図に重ねて表示します。
5. マップで、[表示：参加デバイスのみ（Show: Participating Only）] チェックボックスをオンにして、選択した Tree-SID ポリシーに参加していないアンダーレイデバイスを非表示にします。次に、マウスを使用して [PE-A] ルートデバイスにカーソルを合わせると、対応する到達可能性の状態、ホスト名、ノード IP、およびデバイスタイプが表示されます。

   参加している Tree-SID デバイスを同じ方法でチェックして、対応する詳細を表示します。

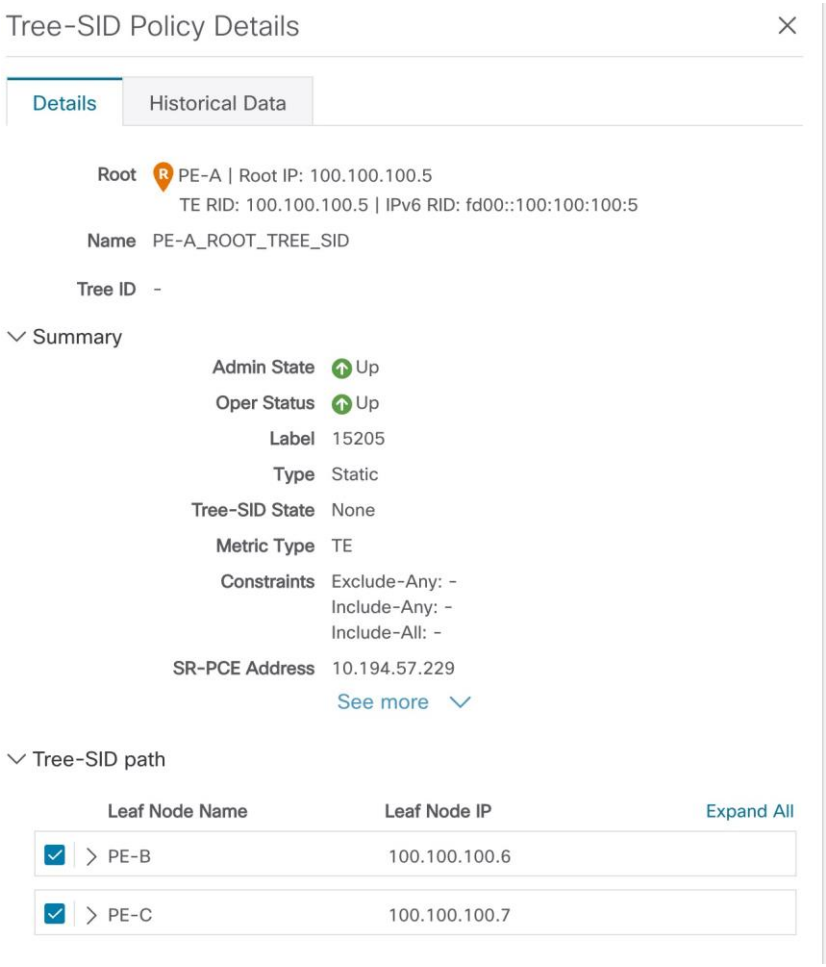


6. マップ中の [PE-B] をクリックします。
[デバイスの詳細（Device Details）] パネルが開き、デバイスの概要、ルーティング、および PCEP セッションごとにまとめられた PE-B 情報が表示されます。



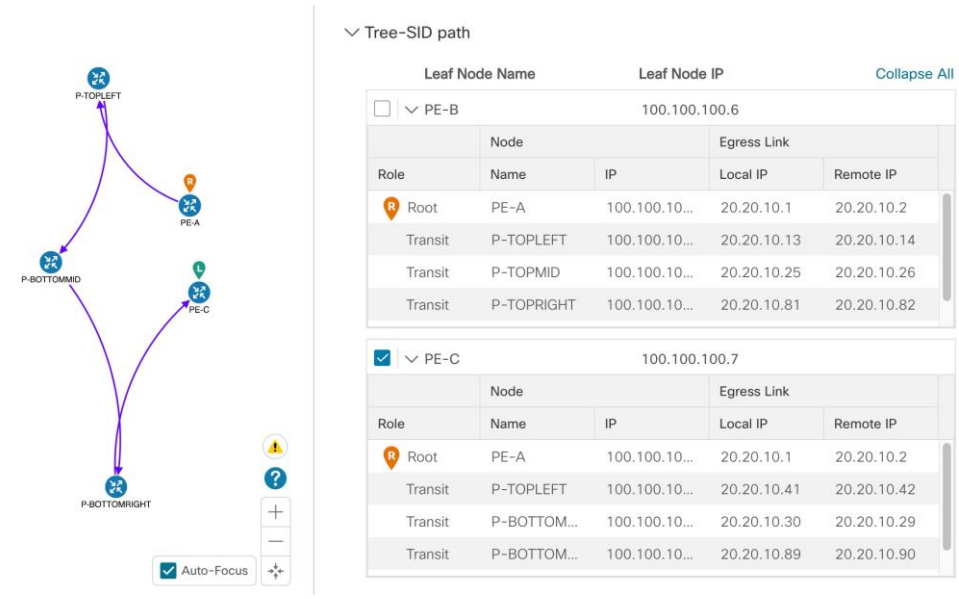
7. 右上隅の [X] をクリックして、[Tree-SID ポリシー（Tree-SID Policy）] リストに戻ります。
8. **PE-A** デバイスの [Tree-SID ポリシー（Tree-SID Policy）] リストで、[アクション（Actions）] 列の [...] をクリックし、[詳細の表示（View Details）] を選択して、デバイスの概要の管理および運用ステータスの詳細を含む、Tree-SID サービスの詳細ビューにドリルダウンします。

[Tree-SID ポリシーの詳細（Tree-SID Policy Details）] テーブルが開きます。

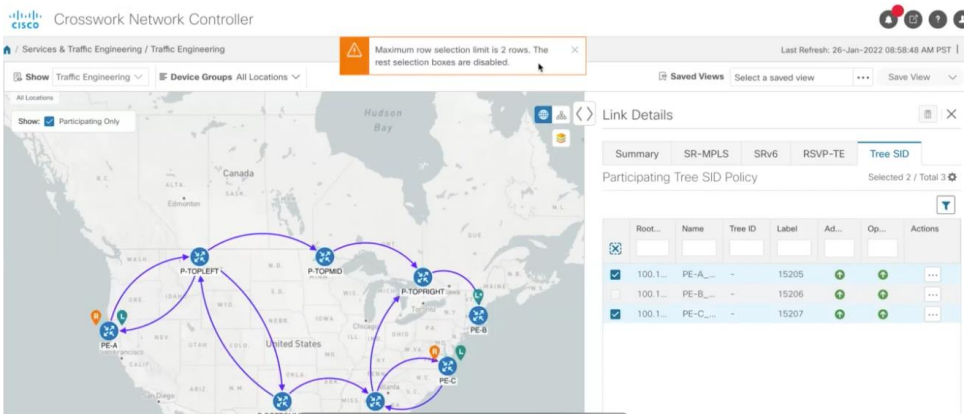


注： [Tree-SID ポリシーの詳細（Tree-SID Policy Details）] をすべて表示するには、[概要（Summary）] セクションの下部にある [詳細を表示（See more）]をクリックします。

9. [Tree-SID パス（Tree-SID path）] セクションで、[すべて展開（Expand All）] をクリックして、PE-B および PE-C リーフノードの Tree-SID パス名と IP を表示します。このリストには、対応するルートノード、すべてのトランジットノード、2 つのリーフノードの詳細と、それらの出力リンクのローカル IP およびリモート IP 情報も表示されます。
10. [PE-C] デバイスのみの Tree-SID パスの詳細を表示するには、[PE-B] チェックボックスをオフにします。マップが更新され、選択した PE-C Tree-SID ルートのみが表示されます。



11. 右上隅の [X] をクリックして、[Tree-SID ポリシー（Tree-SID Policy）] リストに戻ります。
12. リストでルート IP Tree-SID ポリシー [PE-A] チェックボックスをオンにします。次に、[PE-C] をオンにします。マップが更新され、2 つのポリシーとそれぞれの分岐ルートが表示されます。個々のリンクをクリックすると、各リンクが参加している Tree-SID ポリシーの詳細を取得できます。



まとめと結論

上述のように、[Tree-SID] タブとその関連マップを使用して、Tree-SID で定義されたルートを可視化し、ポリシーの分岐ルートを識別して、ルートノードからリーフノードへのトラフィックに影響を与える可能性のあるトランジットノード、インターフェイス、リンクの問題を識別することができます。

付録

サービスの正常性をモニターするためのヒューリスティック パッケージの初期化

目的

Service Health を有効にし、システム設計のヒューリスティック パッケージを使用して新しく作成されたサービスをモニターするか、システムにエクスポートして調整してから Cisco Crosswork Network Controller にインポートし直すことで、サービスの正常性の継続的な詳細モニタリングをカスタマイズできます。

注： Service Health は、限定提供で使用できます。詳細については、アカウントチームにお問い合わせください。

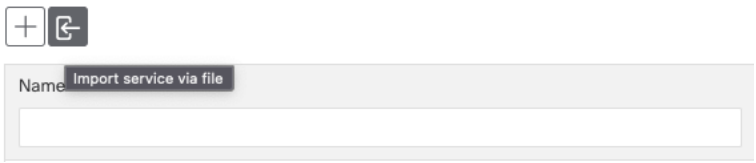
注： 基本モニタリングレベルルールを支援するために、3 つの付加的なルールが追加されました（Rule-L2VPN-NM-Basic、Rule-L2VPN-NM-P2P-Basic、Rule-L3VPN-NM-Basic）。付加的なルールにより、たとえば Basic L2VPN NM P2P サービスなどのアシュアランスグラフ情報が生成され、2 つのサブサービスとともに使用できます。ヒューリスティック パッケージ メトリックに、CLI ベースのメトリックとパッケージの GMNI フィルタリングカスタマイズの機能が追加されました。

ワークフロー

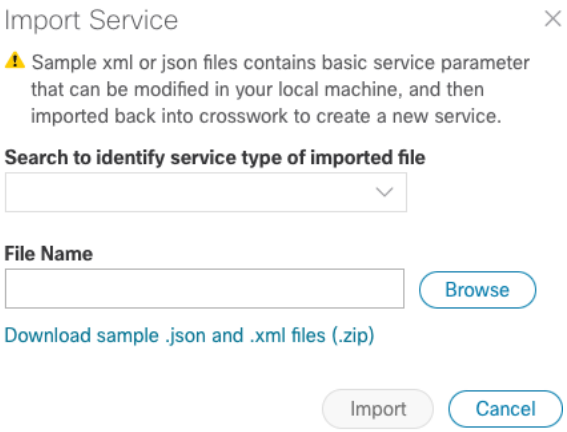
システムまたはカスタム ヒューリスティック パッケージを選択して、新しい VPN サービスの継続的な Service Health による専用モニターリングを行います。

ヒューリスティック パッケージを初期化して、新しいサービスの正常性をモニターします。

1. [管理（Administration）] > [ヒューリスティックパッケージ（Huristic Packages）] に移動します。[Heuristic Packages] 画面が開き、[System] タブと [Custom] タブが表示されます。デフォルトでは、システム定義のヒューリスティック パッケージが使用されます。
2. [System] タブから、各セクションを展開して詳細を確認し、情報アイコン [I] の上にマウスを合わせることで、パッケージの詳細ルール、設定プロファイル、サブサービス、およびメトリックをプレビューできます。
3. [エクスポート（Export）] をクリックしてシステム定義パッケージをお使いのシステムにダウンロードし、.json ファイルを変更してから、カスタマイズパッケージとして Cisco Crosswork Network Controller にインポートできます。
4. カスタマイズ用にシステムファイルをエクスポートした場合、またはシステムにインポートしたいカスタムパッケージがある場合は、[Import] をクリックします。



5. [Import Heuristic Packages] 画面が開いたら、[Browse] をクリックして、システム上のカスタムパッケージの名前を探します。



6. カスタムパッケージを選択し、[Import] をクリックします。注：ヒューリスティック パッケージのインポート中は、サーバーのリソース消費量が多いため、システムのパフォーマンスが影響を受ける可能性があります。
7. [Import Heuristic Packages] 画面で、[Preview] をクリックして、インポートするパッケージの詳細を確認します。パッケージのルール、設定プロファイル、サブサービス、およびメトリックに関する詳細情報が表示されます。
8. カスタムパッケージの詳細をプレビューするには、各オプションを選択します。Cisco Crosswork Network Controller が新しいカスタムパッケージを受け入れてインポートできるようにする前に、詳細を更新する必要がある場合、Cisco Crosswork Network Controller は詳細に関する情報を提供します。
9. カスタムパッケージをインポートしたら、それを選択すると、新しいルールと設定の詳細によって、指定したサービスの健全性の継続的なモニターリングが開始されます。

基本および詳細モニタリングルール

サービスヘルスモニタリングには 2 つのオプションがあります。

- **基本モニタリング**：これらのルールを使用してモニターすると、消費されるコンピューティングリソースは少なくなりますが、詳細にモニターされないサービスが増加します。このモニタリングレベルでは、最大 52,000 のサービスを追加するオプションが提供され、全体的な CPU 使用率が低下し、サブサービスメトリックが制限され、マップ グラフィック レンダリングが小規模になります。
- **詳細モニタリング**：詳細なルールはより多くのリソースを消費しますが、より少ないサービスをより詳細に監視します。このモニタリングレベルでは、最大 2,000 のサービスの追加が可能で、全体的な CPU 使用率が高くなり、サブサービスメトリックの数が増え、マップ グラフィック レンダリングが大規模になります。

モニタリング対象サービスとアラートの生成に使用されるしきい値の正確な詳細については、インストールされているヒューリスティック パッケージ ルールと設定プロファイルを表示します（[管理（Administration）] > [ヒューリスティックパッケージ（Heuristic Packages）] を選択し、[ルール（Rules）] または [設定プロファイル（Configuration Profiles）] ドロップダウンをクリック）。

次の表は、Cisco Network Controller ヒューリスティック パッケージで利用可能な基本および詳細モニタリングルールのそれぞれによって適用されるモニタリング機能とサービスメトリックの詳細を示しています。

ルール名（タイプ）	モニタリング機能	メトリックとサブサービス
Rule-L2VPN-NM-Basic	• VPWS xconnect の状態の正常性をチェックします。	metric.l2vpn.xconnect.state metric.l2vpn.xconnect.ac.state metric.l2vpn.xconnect.pw.state

	• デバイスの正常性（CPU およびメモリ使用率）をモニターします。	subservice.device.health subservice.vpws.ctrlplane.health
Rule-L2VPN-NM（詳細）	• VPWS または EVPN xconnect の状態の正常性をチェックします。 • デバイスの正常性（CPU およびメモリ使用率）をモニターします。 • VPN インターフェイスと疑似回線間で送受信されたパケットの差分をモニターします。 • Y.1731 プローブ統計のジッター、損失、および遅延のメトリックをモニターし、SLA しきい値と比較します。 • インターフェイスメトリックの正常性をチェックします（運用ステータス、インターフェイスイン/アウトエラーパケット、インターフェイスイン/アウトパケット破棄）。 • BGP ネイバーセッションの正常性をチェックします。 • 特定の L2VPN サービスの BGP EVPN ネクストホップすべてが LSP 経由で到達可能かどうかをチェックします。 • このデバイスで設定されているすべてのピアへの PCEP セッション状態をモニターします。 • 2 エンドポイント間のパスの到達可能性をチェックします。 • SR ポリシー（PCC により開始）の正常性ステータス。管理者が UP になっている必要があります。運用が UP になっている必要があります。運用が前回のポーリングから UP になっている必要があります。 • 指定された接続先デバイスへの LSP パスが（デフォルトの VRF に）存在するかどうかをチェックします。	metric.bgp.router.id metric.cef.route.labeled.lsp metric.l2vpn.xconnect.ac.state metric.l2vpn.xconnect.pw.state metric.l2vpn.xconnect.state subservice.bgp.nbr.health subservice.bgp.evpn.nexthop.health subservice.device.health subservice.evpn.health（エンドポイントごとに 1 つ） subservice.fallback.path.health subservice.interface.health（インターフェイスごとに 1 つ） subservice.l2vpn.y1731.health subservice.path.reachability.to.peer（ローカルからリモートおよびリモートからローカル） subservice.path.sla subservice.pcep.session.health（エンドポイントデバイスごとに 1 つ） subservice.plain.lsp.path.health subservice.sr.policy.pce.health（エンドポイントごとに 1 つ） subservice.vpws.ctrlplane.health（ローカル、リモート）
Rule-L2VPN-NM-P2P-Basic	• VPWS xconnect の状態の正常性をチェックします。 • デバイスの正常性（CPU およびメモリ使用率）をモニターします。	subservice.device.health subservice.vpws.ctrlplane.health
Rule-L2VPN-NM-P2P（詳細）	• VPWS xconnect の状態の正常性をチェックします。 • デバイスの正常性（CPU およびメモリ使用率）をモニターします。 • インターフェイスメトリックの正常性をチェックします（運用ステータス、インターフェイスイン/アウトエラーパケット、インターフェイスイン/アウトパケット破棄）。 • Y.1731 プローブ統計のジッター、損失、および遅延のメトリックをモニターし、SLA しきい値と比較します。 ピア VPN ノードへの LSP パスをモニターします。 2 エンドポイント間のパスの到達可能性をモニターします。 指定された宛先 IP アドレスへの LSP パス（デフォルトの VRF）をモニターします • このデバイスで設定されているすべてのピアへの PCEP セッション状態をモニターします。 • SR ポリシー（PCC により開始）の正常性ステータス。管理者が UP になっている必要があります。運用が UP になっている必要があります。	Metric.cef.route.labeled.lsp metric.l2vpn.xconnect.ac.state metric.l2vpn.xconnect.pw.state metric.l2vpn.xconnect.state subservice.device.health subservice.interface.health（インターフェイスごとに 1 つ） subservice.l2vpn.y1731.health subservice.p2p.fallback.path.health Subservice.p2p.path.reachability.to.peer（エンドポイント間のパス到達可能性） subservice.p2p.plain.lsp.path.health subservice.path.sla subservice.pcep.session.health（エンドポイントデバイスごとに 1 つ） subservice.sr.policy.pcc.health subservice.sr.policy.pce.health（エンドポイントごとに 1 つ） subservice.vpws.ctrlplane.health（ローカル、リモート）

	運用が前回のポーリングから UP になっている必要があります。	
Rule-L3VPN-NM-Basic	現在の PE デバイスとそれに接続している CE デバイスとの間の全体的なルート接続の正常性について報告します。 • デバイスの正常性（CPU およびメモリ使用率）をモニターします。	subservice.ce.pe.route.health subservice.device.health
Rule-L3VPN-NM（詳細）	BGP ネイバーセッションの正常性をモニターします。 現在の PE デバイスとそれに接続している CE デバイスとの間の全体的なルート接続の正常性について報告します。 デバイスの正常性（CPU およびメモリ使用率）をモニターします。 eBGP ネイバーセッションの正常性をモニターします。 • インターフェイスメトリックの正常性をチェックします（運用ステータス、インターフェイスイン/アウトエラーパケット、インターフェイスイン/アウトパケット破棄）。 • このデバイスで設定されているすべてのピアへの PCEP セッション状態をモニターします。 特定のデバイスからピア VPN サイトへの（特定の VRF に対する）パス到達可能性を反映する L3VPN アグリゲータサブサービス。 特定の VPN IP アドレスへの特定の VRF 内にプレーン LSP ルートが存在するかどうかをチェックします。	subservice.bgp.nbr.health subservice.ce.pe.route.health subservice.device.health subservice.ebgp.nbr.health subservice.interface.health subservice.pcep.session.health（エンドポイントデバイスごとに 1 つ） subservice.vrf.path.reachability.to.peers subservice.vrf.plain.lsp.reachability

Service Health でサポートされるサブサービス

次の表は、サポートされている Service Health L2VPN/L2VPN フレーバーと関連するサブサービスの詳細を示しています（IOS XE および XR デバイスの場合）。リストに含まれるサブサービスは、Crosswork Automated Assurance からすぐに利用できます。

サポートされている VPN サービスと関連するサブサービス（IOS XE デバイスの場合）：

サポートされている VPN サービス	関連するサブサービス	詳細
SR アンダーレイを使用した L2VPN ポイントツーポイント	パスの到達可能性 Y.1731 正常性 VPN インターフェイスの正常性 デバイスの正常性	XE は、このサブサービスの SNMP/gNMI 収集タイプをサポートしていません（CEF ルート、PCEP セッション状態、SRPolicy 状態、XConnect）。
MPLS LDP による L2VPN ポイントツーポイント	パスの到達可能性 Y.1731 正常性 VPWS コントロールプレーンの正常性	XE は、このサブサービスの SNMP/gNMI 収集タイプをサポートしていません（CEF ルート、XConnect）。

	VPN インターフェイスの正常性 デバイスの正常性	
L2VPN P2P プレーン	パスの到達可能性 Y.1731 正常性 VPN インターフェイスの正常性 デバイスの正常性	XE は、このサブサービスの SNMP/gNMI 収集タイプをサポートしていません（CEF ルート、XConnect）。 **注**：「プレーン」への参照は、L2VPN/L3VPN トラフィックが IGP パスを経由し、SR などのトランスポートを使用しないことを意味します。
L3VPN SR	パスの到達可能性 CE-PE ルートの正常性 eBGP ネイバーの正常性 VPN インターフェイスの正常性 BGP ネイバーの正常性（DynExp）	XE は、このサブサービスの SNMP/gNMI 収集タイプをサポートしていません（CEF ルート、PCEP セッション状態）。SR-ODN もサポートされていません。

サポートされている VPN サービスと関連するサブサービス（IOS XR デバイスの場合）：

サポートされている VPN サービス	**関連するサブサービス**
L2VPN EVPN SR	パスの到達可能性 有効化された/無効化されたフォールバック（DynExp） SR ポリシー：PCC パス SLA Y.1731 正常性 VPWS コントロールプレーンの正常性 VPN インターフェイスの正常性 デバイスの正常性 EVPN 正常性 BGP ネイバーの正常性（DynExp） BGP ネクストホップの正常性（DynExp） PCEP セッションの正常性（DynExp） SR ポリシー：PCE
L2VPN EVPN プレーン	パスの到達可能性 パス SLA プレーン LSP パスの正常性（DynExp） VPWS コントロールプレーンの正常性 VPN インターフェイスの正常性

	デバイスの正常性 EVPN の正常性 BGP ネイバーの正常性（DynExp） BGP ネクストホップの正常性（DynExp） **注**：「プレーン」への参照は、L2VPN/L3VPN トラフィックが IGP パスを経由し、SR などのトランスポートを使用しないことを意味します。
SR アンダーレイを使用した L2VPN ポイントツーポイント	パスの到達可能性 有効化された/無効化されたフォールバック SR ポリシー：PCC パス SLA Y.1731 正常性 VPWS コントロールプレーンの正常性 VPN インターフェイスの正常性 デバイスの正常性 PCEP セッションの正常性（DynExp） SR ポリシー：PCE
MPLS LDP による L2VPN ポイントツーポイント	パスの到達可能性 有効化/無効化されたフォールバック パス SLA Y.1731 正常性 VPWS コントロールプレーンの正常性 VPN インターフェイスの正常性 デバイスの正常性
L2VPN P2P プレーン	パスの到達可能性 プレーン LSP パスの正常性 パス SLA Y.1731 正常性 VPWS コントロールプレーンの正常性 VPN インターフェイスの正常性 デバイスの正常性 **注**：「プレーン」への参照は、L2VPN/L3VPN トラフィックが IGP パスを経由し、SR などのトランスポートを使用しないことを意味します。
L3VPN SR	CE-PE ルートの正常性 eBGP ネイバーの正常性 VPN インターフェイスの正常性

	デバイスの正常性 パスの到達可能性 VRF プレーン LSP パスの正常性 PCEP セッションの正常性（DynExp） BGP ネイバーの正常性（DynExp）

Service Health 外部ストレージの設定

目的

Service Health は、最大 50 GB のモニタリングデータの内部ストレージを提供します。このデータはシステムに保存されます。内部ストレージの制限を超えると、履歴データが失われます。

注： 多数の Service Health サービスをモニタリングすることが予想される場合、Cisco は、Service Health をインストールした後、サービスのモニタリングを開始する前に、外部ストレージを設定して内部ストレージの超過や履歴データの損失を避けることを推奨します。

Service Health のストレージ容量を拡張することを選択した場合は、Amazon Web Services（AWS）クラウドアカウントを使用して、クラウドに外部ストレージを設定できます。外部ストレージを活用することで、既存のすべての内部ストレージデータが外部クラウドストレージに自動的に移動し、内部ストレージはキャッシュストレージとしてローカルに機能するようになります。Service Health 用の外部ストレージを設定すると、サービスの正常性をモニターし続けるサービスの履歴データが失われることがなくなり、データの履歴モニタリングサービスを維持するオプションを選択した場合、モニタリングを停止を選択したサービスのサービスヘルスデータが保持されます。

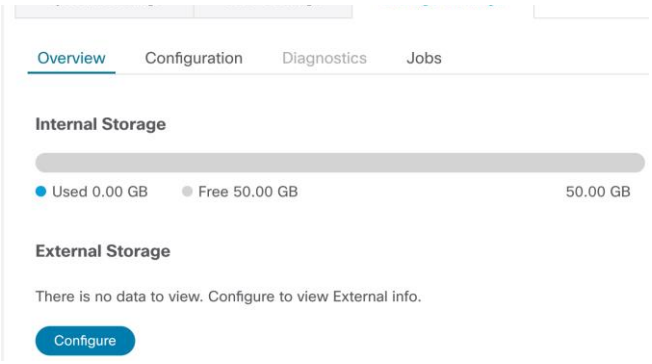
注： Service Health は、限定提供で使用できます。詳細については、アカウントチームにお問い合わせください。

ワークフロー（Workflow）

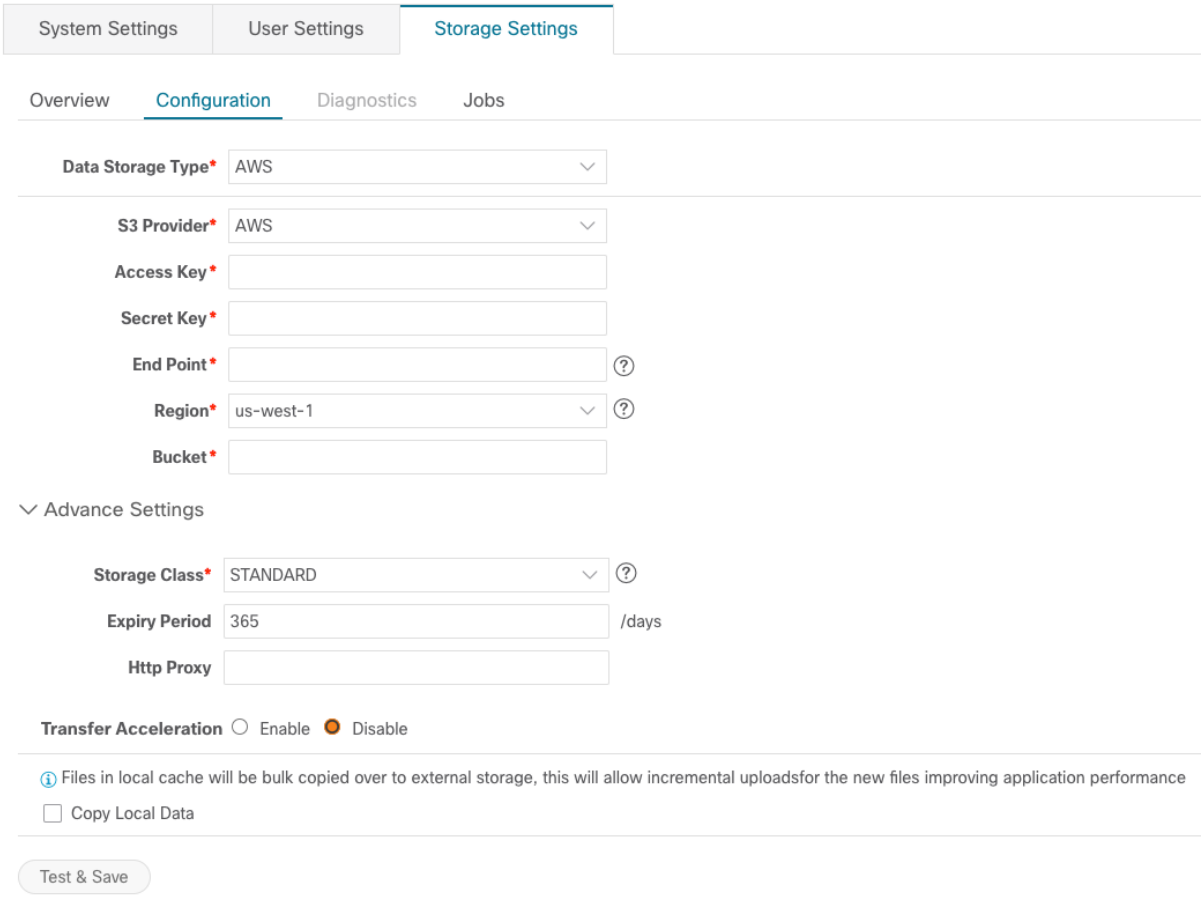
内部ストレージを超えてストレージ容量を拡張するには、AWS アカウントを使用して外部ストレージを設定して、サービスの状態をモニターし続けるサービスの履歴データが失われないようにし、データの履歴モニタリングサービスを保持するオプションの選択時にモニターを停止することにしたサービスのサービス状態データを保持します。

外部ストレージを設定するには、次の手順を実行します。

1. [管理（Administration）] > [設定（Settings）] に移動し、[ストレージ設定（Storage Settings）] タブを選択します。[概要（Overview）] 画面が表示されます。



2. [外部ストレージ（External Storage）] で、[設定（Configure）] をクリックします。[設定（Configuration）] 画面が表示され、[データストレージタイプ（Data Storage Type）] フィールドと [S3 プロバイダー（S3 Provider）] フィールドに AWS（Amazon Web Services）が事前入力されています。



注： 外部ストレージを設定するには、AWS クラウドアカウントを設定する必要があります。詳細については、AWS サイトを参照してください。

3. すべての必須フィールド（[アクセスキー（Access Key）]、[秘密鍵（Secret Key）]、[エンドポイント（End Point）] など）に AWS 認証情報を入力します。

4. 以前ローカルキャッシュに保存されていたすべてのファイルを外部ストレージに一括コピーする場合は、[ローカルデータのコピー（Copy Local Data）] チェックボックスをオンにします。このアクションにより、新しいファイルの増分アップロードが可能になります。

   注： このオプションは、ローカルストレージのみの維持から外部ストレージに移行する場合の 1 回限りのアクションです。このアクションは、アプリケーションのパフォーマンスの向上にも役立ちます。

   注： [有効期限（Expiry Period）] は、履歴データファイルの有効期間の日数です。[有効期限（Expiry Period）] が「1」に設定されている場合、履歴データファイルは 2 日後に削除され、削除は 2 日目の午前 0 時に実行されます。

5. [テストして保存（Test & Save）] をクリックします。
6. ストレージ設定の状態を確認するには、[診断（Diagnostics）] タブを選択し、[テストの実行（Run Test）] をクリックします。
   テストを実行することで、帯域幅、遅延、複数のアクセステストの詳細といった外部ストレージの診断を確認して、考えられるストレージパフォーマンスの問題を特定することができます。

Service Health モニタリングの停止

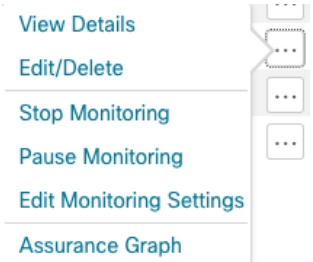
目的

Service Health は、サービスのモニタリングを停止するときに特定のオプションを提示します。サービスのモニタリングを停止すると、Service Health は、モニタリングサービスの履歴データを保持するかどうかを尋ねます。履歴データを保持すると、後でサービスのモニタリングを再開したときに、サービスにより以前のモニタリングで収集されたデータを使用できるようになります。履歴サービスデータを保持せずにサービスのモニタリングを停止することを選択した場合、モニタリング設定は削除され、後でサービスのモニタリングを開始することを選択したときに、履歴サービスデータが期限切れになるか、削除されます。さらに、停止したサービスのアシュアランスグラフは使用できなくなります。

ワークフロー（Workflow）

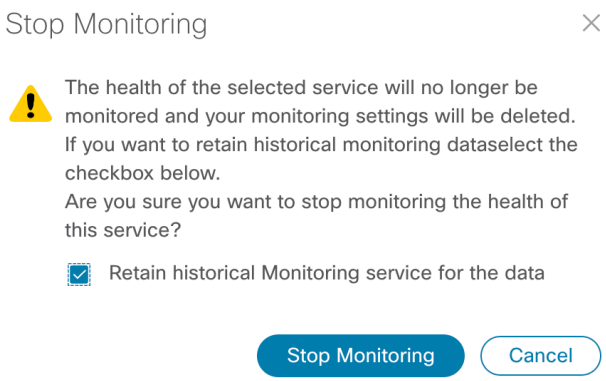
Service Health サービスのモニタリングを停止するとともにモニタリングサービスの履歴データを保持するには、次の手順を実行します。

1. 該当するサービスの [アクション（Actions）] 列で [...] をクリックし、メニューから [モニタリングの停止（Stop Monitoring）] を選択します。



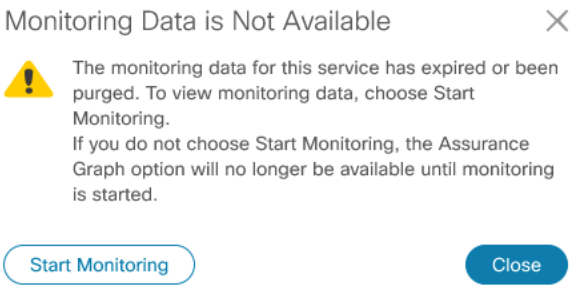
   [モニタリングの停止（Stop Monitoring）] ポップアップが表示されます。

2. そのサービスの履歴サービスデータを保持するには、[データの履歴モニタリングサービスを保持する（Retain historical Monitoring service for the data）] チェックボックスをオンにします。

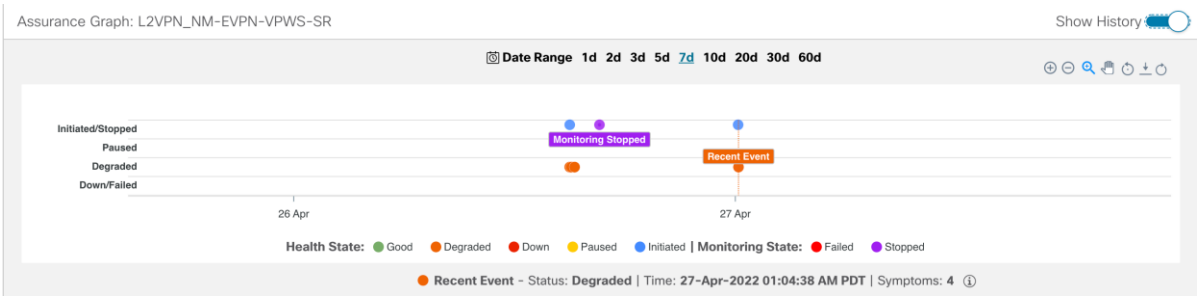


3. [モニタリングの停止（Stop Monitoring）] をクリックします。
サービスの履歴モニタリングデータが保持されます。

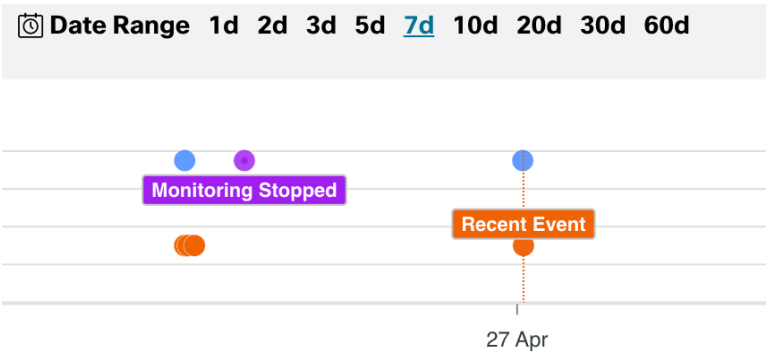
注： サービスのモニタリングを停止したときに、[データの履歴モニタリングサービスを保持する（Retain historical Monitoring service for the data）] チェックボックスを選択しなかった場合、後で停止したサービスの [アシュアランスグラフ（Assurance Graph）] を選択すると、モニタリング設定が削除され、履歴サービスデータが期限切れになるか消去されるため、このグラフは使用できなくなります。サービスの状態のモニタリングを再度開始し、サービスデータの収集を新たに開始することができます。



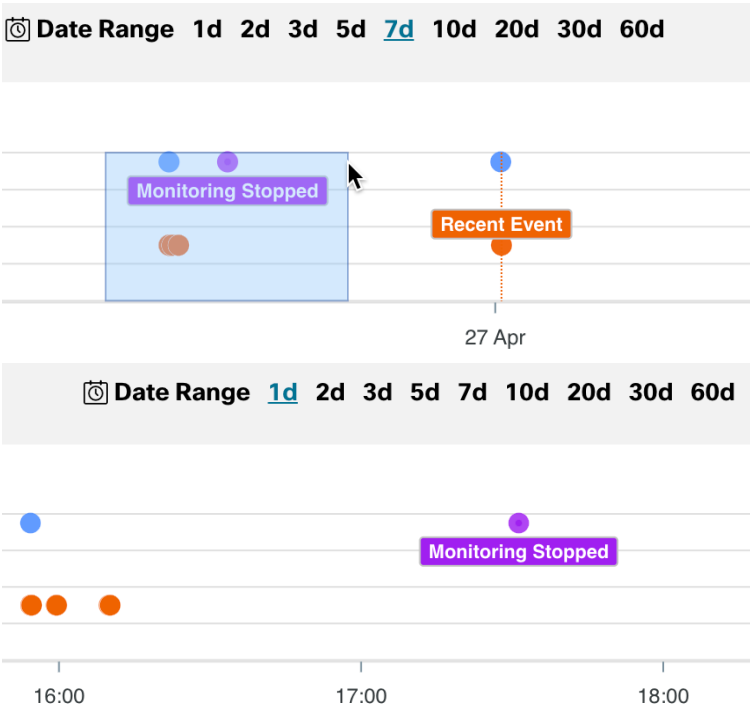
4. 停止したサービスをアシュアランスグラフに表示するには、そのサービスの [アクション（Actions）] 列で [...] をクリックし、メニューから [アシュアランスグラフ（Assurance Graph）] を選択します。
5. [履歴の表示（Show History）] トグルをクリックします。



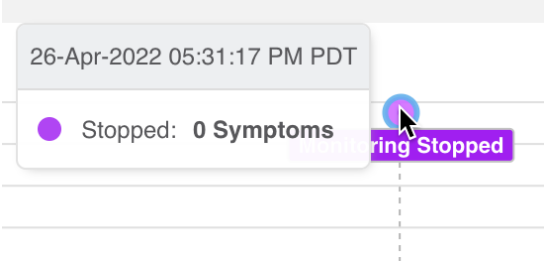
6. [日付の範囲（Date Range）] グラフに、停止されたサービスが表示され、モニタリングが停止していたことが示されます。



7. マウスを使用して、選択された範囲をクリックして [モニタリング停止（Monitoring Stopped）] の対象サービスの上までドラッグし、この時間範囲の表示を拡大します。



8. [モニタリング停止（Monitoring Stopped）] の対象サービスの上にマウスを置くと、サービスが停止されたときの日付スタンプと、停止されたサービスに関連する現象があったかどうかが表示されます。



9. サービスのモニタリングを停止したときに、[データの履歴モニタリングサービスを保持する（Retain historical Monitoring service for the data）] チェックボックスをオンにした場合は、履歴データを引き続き使用した同じサービスのモニタリングを後で開始できます。該当するサービスの [アクション（Actions）] 列で [...] をクリックし、メニューから [モニタリングの開始（Start Monitoring）] を選択します。

   注： 外部ストレージが設定されている状況で、多数のサービスをモニタリングしている場合は、停止された（再び開始された）サービスの履歴データを保持して、継続的なモニタリングと検査を行うことができます。詳細については、**Service Health ストレージの設定**に関するセクションを参照してください。