ホワイトペーパー

Cisco ACI ファブリックの Nexus ダッシュボード インサイトの準備

2021 年 9 月 15 日

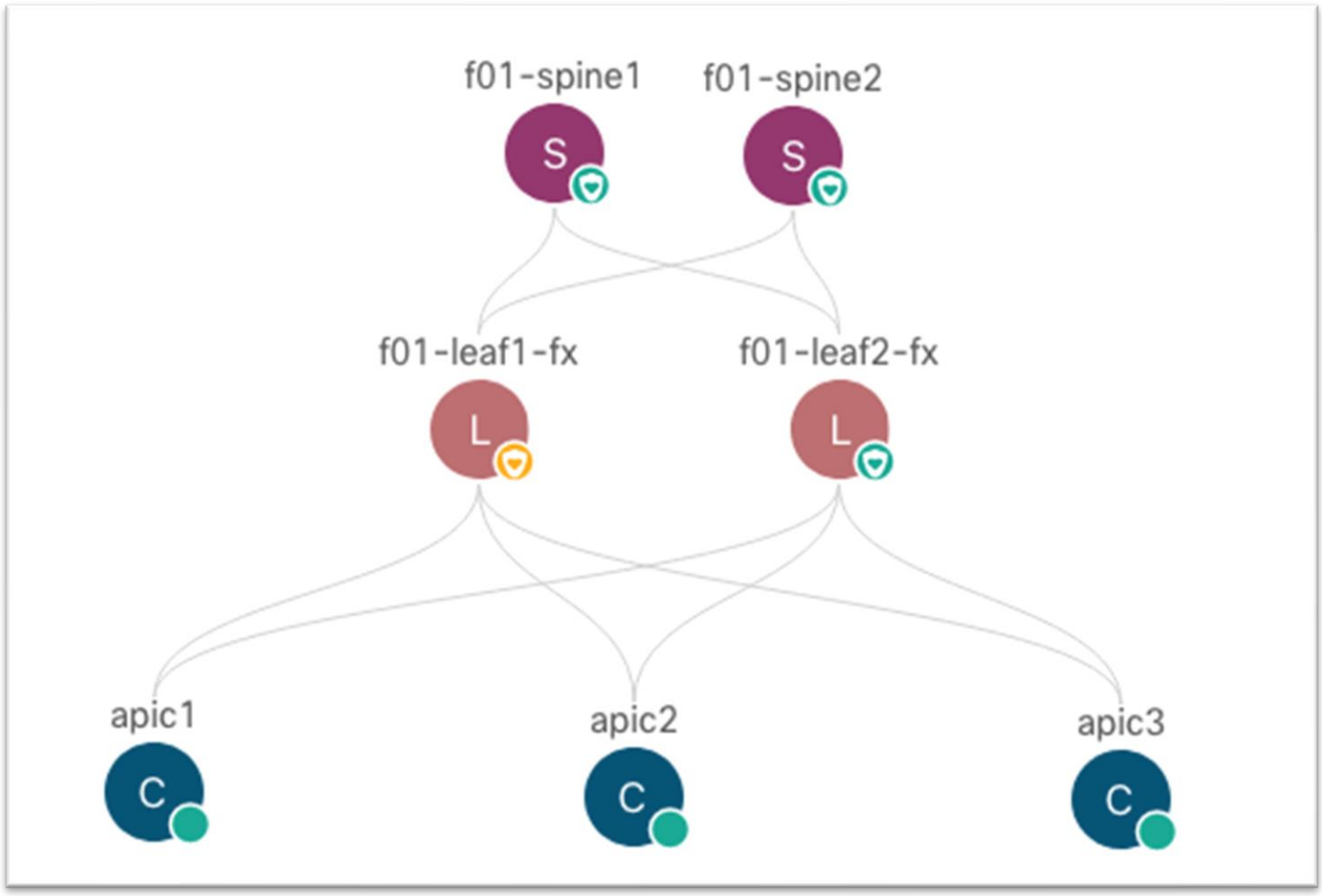
目次

概要

Cisco Nexus Dashboard Insights は、Cisco Data Center ファブリック向けの Day-2-Operations ツールです。Cisco Nexus ダッシュボード Insights は、ネットワークの異常に焦点を当て、最新のスケーラブルなアーキテクチャにより、ネットワークの健全性を迅速に可視化します。詳細については、「Cisco Nexus ダッシュボード Insights ホワイト ペーパー」を参照してください。

このドキュメントは、Cisco Nexus ダッシュボード Insights をサポートするように Cisco ACI ファブリックを設定するためのチェックリストおよびガイドとして使用することを目的としています。このホワイト ペーパーでは、インバンド管理、Cisco Nexus ダッシュボードを Cisco ACI に接続する方法、Network Time Protocol（NTP）、Precision Time Protocol（PTP）、モニタリング ポリシーなどの前提条件について説明します。さらに、オンボード アプリケーションに対する Cisco Nexus ダッシュボードおよび Cisco Nexus ダッシュボード Insights の設定についても説明します。最後に、検証とトラブルシューティングのセクションがあります。

次のトポロジを使用したサンプル ファブリックを使用して、以下の設定を構成します。このファブリックはリリース 5.1(3e) を実行しており、次のようにケーブル接続されています。



Cisco ACI ファブリックの Cisco Nexus ダッシュボード Insights 設定の前提条件

インバンド管理

Cisco Nexus ダッシュボード Insights サービスは、Cisco ACI インバンド管理ネットワークを使用して、Cisco APIC コントローラおよびファブリック内のすべてのスイッチからネットワーク テレメトリ データを受信します。したがって、Cisco ACI ファブリックのインバンド管理を設定する必要があります。インバンド管理設定は、次の主要部分で要約できます。

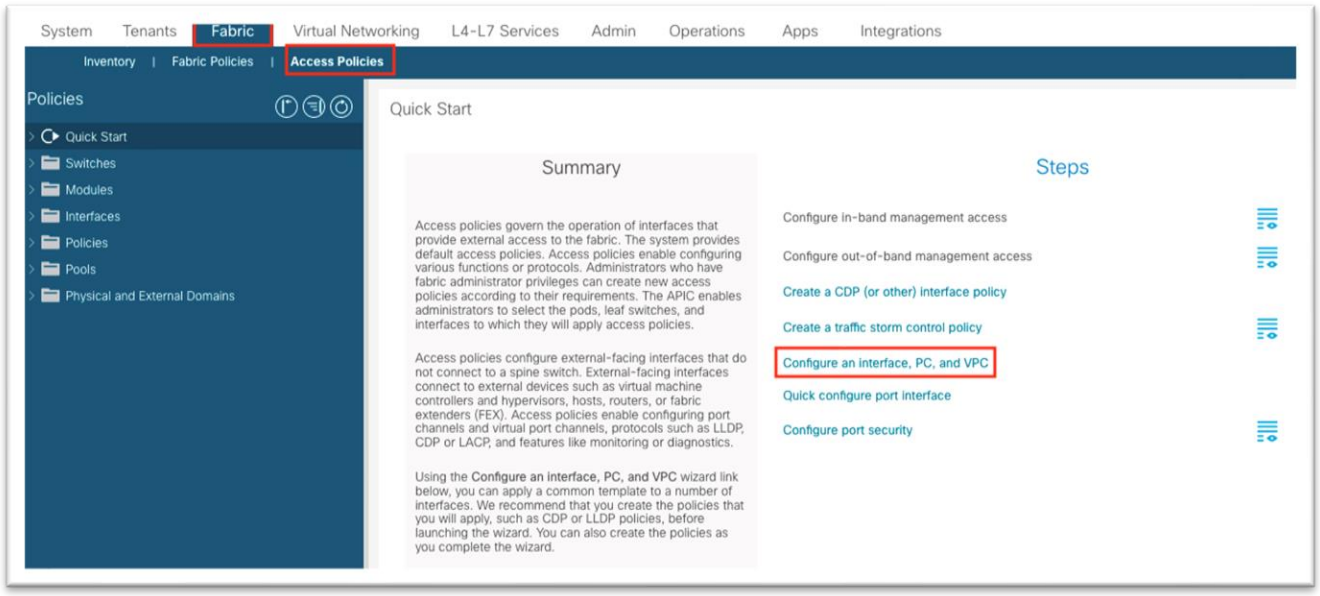
- Cisco APIC インターフェイス（アクセス ポート）のアクセス ポリシー
- サブネットを持つ管理テナント インバンド ブリッジ ドメイン
- 管理テナント ノード管理アドレス（Cisco APIC、リーフ スイッチ、およびスパイン スイッチ）
- インバンド管理用の管理テナント ノード管理 EPG

ここでは、インバンド管理 EPG を設定し、ファブリック デバイスにインバンド IP アドレスを割り当てる方法を示します。詳細については、「Cisco APIC 基本設定ガイド、リリース 5.1(x) - 管理」を参照してください。

設定手順

手順を次に示します。

1. **[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）]** に移動し、**[クイック スタート（Quick Start）]** メニューで **[インターフェイス、PC および vPC を設定する（Configure Interface, PC and vPC）]** を選択します。



2. ダイアログで緑のプラス記号 **[+]** を 2 回クリックしウィザードを展開します。
    a. ドロップダウン リストから、Cisco APIC ポートが接続されている 2 つのスイッチを選択します。
    b. **[スイッチ プロファイル名（Switch Profile Name）]** フィールドに名前を入力します。
    c. **[インターフェイス タイプ（Interface Type）]** から **[個別（Individual）]** に設定します。

d. **[インターフェイス（Interfaces）]** フィールドに、Cisco APIC インターフェイスをカンマ区切りリストまたは範囲として入力します。

e. **[インターフェイス セレクタ名（Interface Selector Name）]** フィールドに名前を入力します。

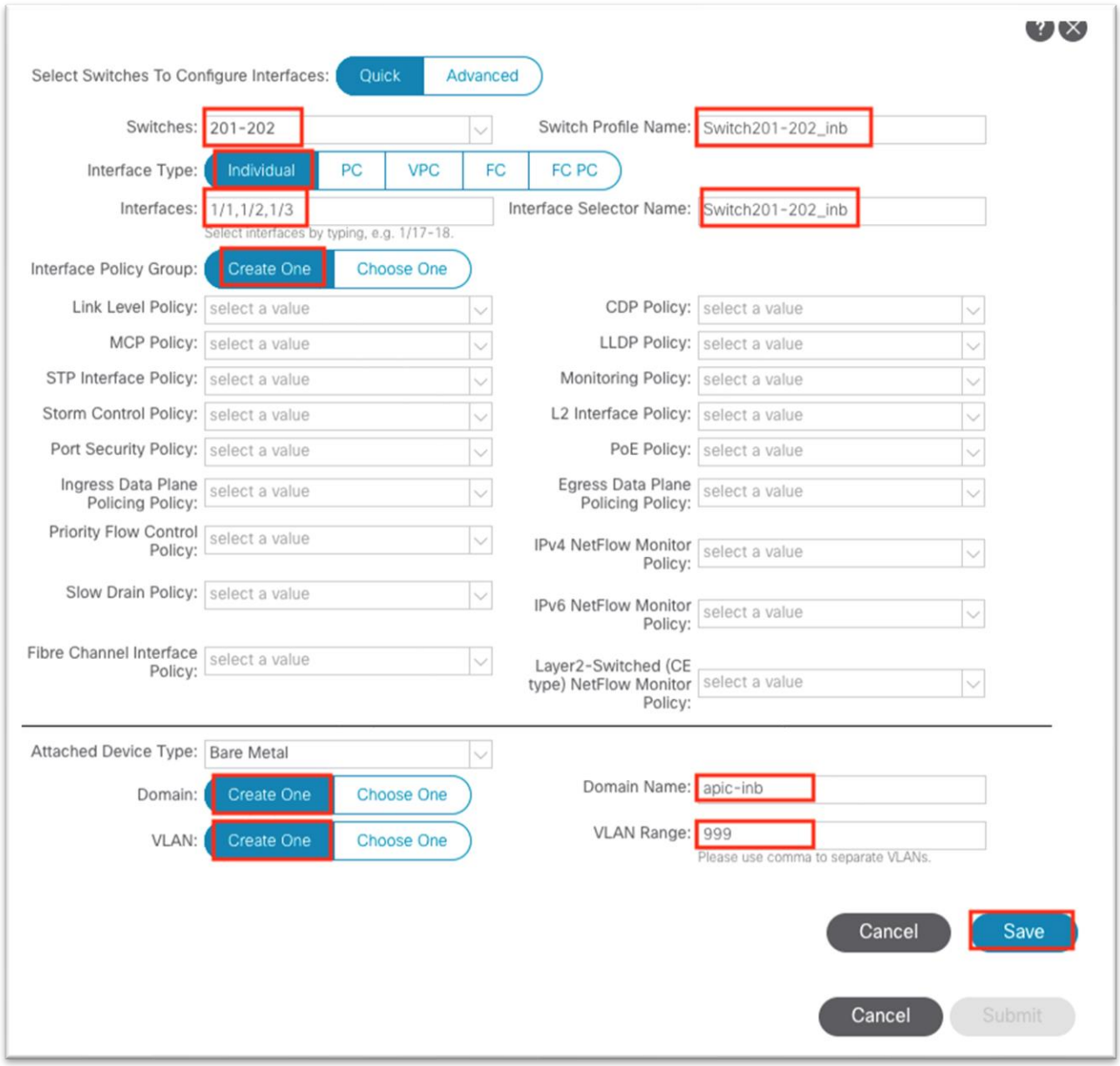
f. **インターフェイス ポリシー グループ**を **[1 個作成（Create One）]** に設定します。インターフェイス レベルのポリシーを選択する必要はありません。デフォルトで十分です。

g. **[接続済みデバイス タイプ（Attached Device Type）]**ドロップダウン リストで、**[ベア メタル（Bare Metal）]** を選択します。

h. **ドメイン**と **VLAN** の両方を **[1 個を作成（Create One）]** に設定する必要があります。

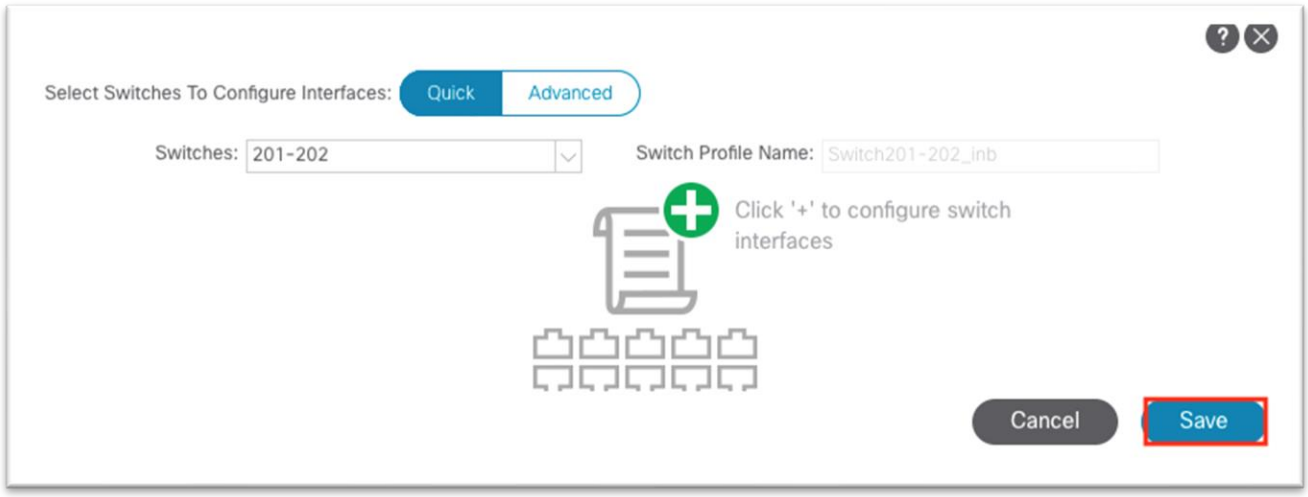
   i. **[ドメイン名（Domain Name）]** フィールドに名前を入力して、インバンド管理に関連付けられている物理ドメインに名前を付けます。

   ii. ファブリック内のインバンド管理に使用される VLAN ID を入力します。

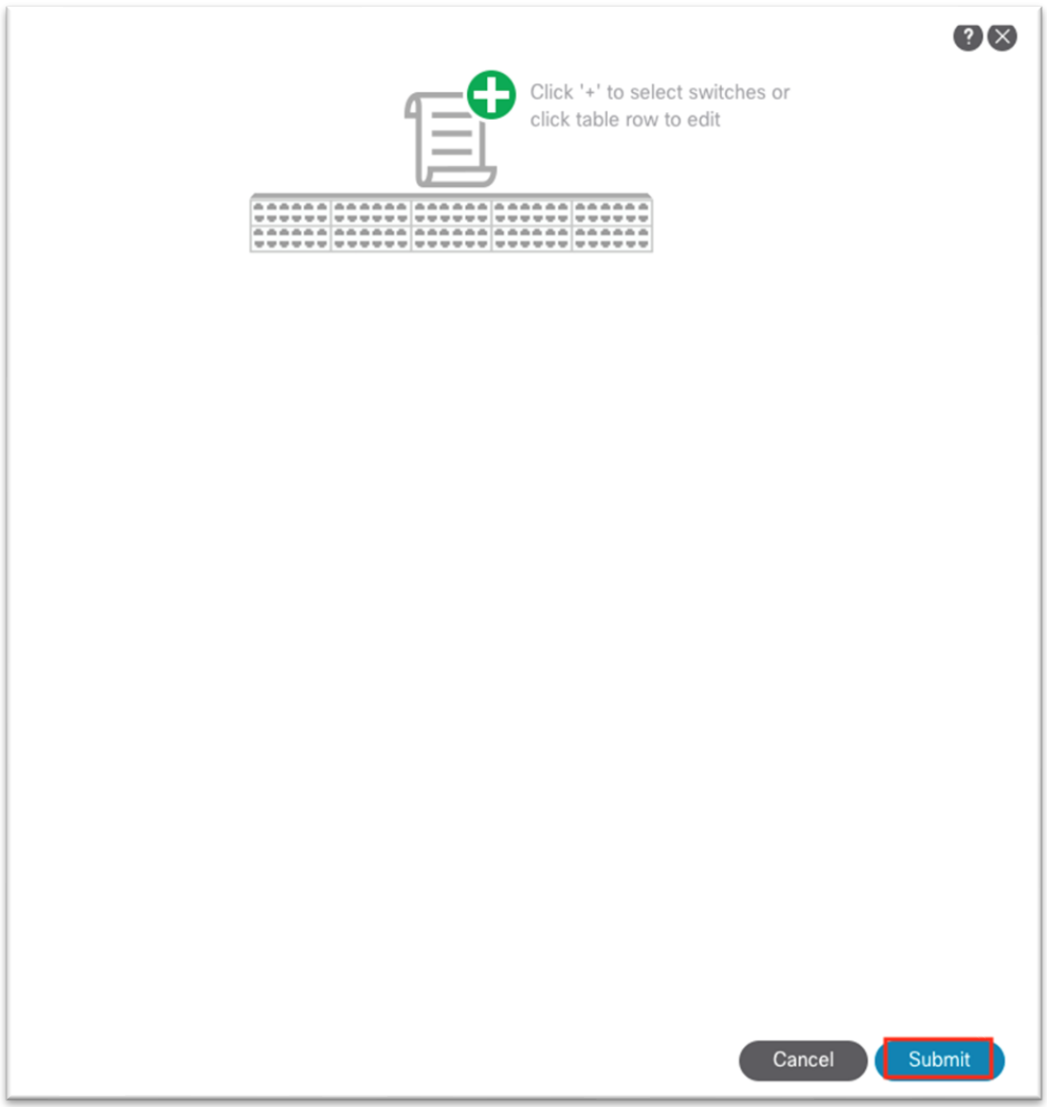


i. [保存（Save）] をクリックします。

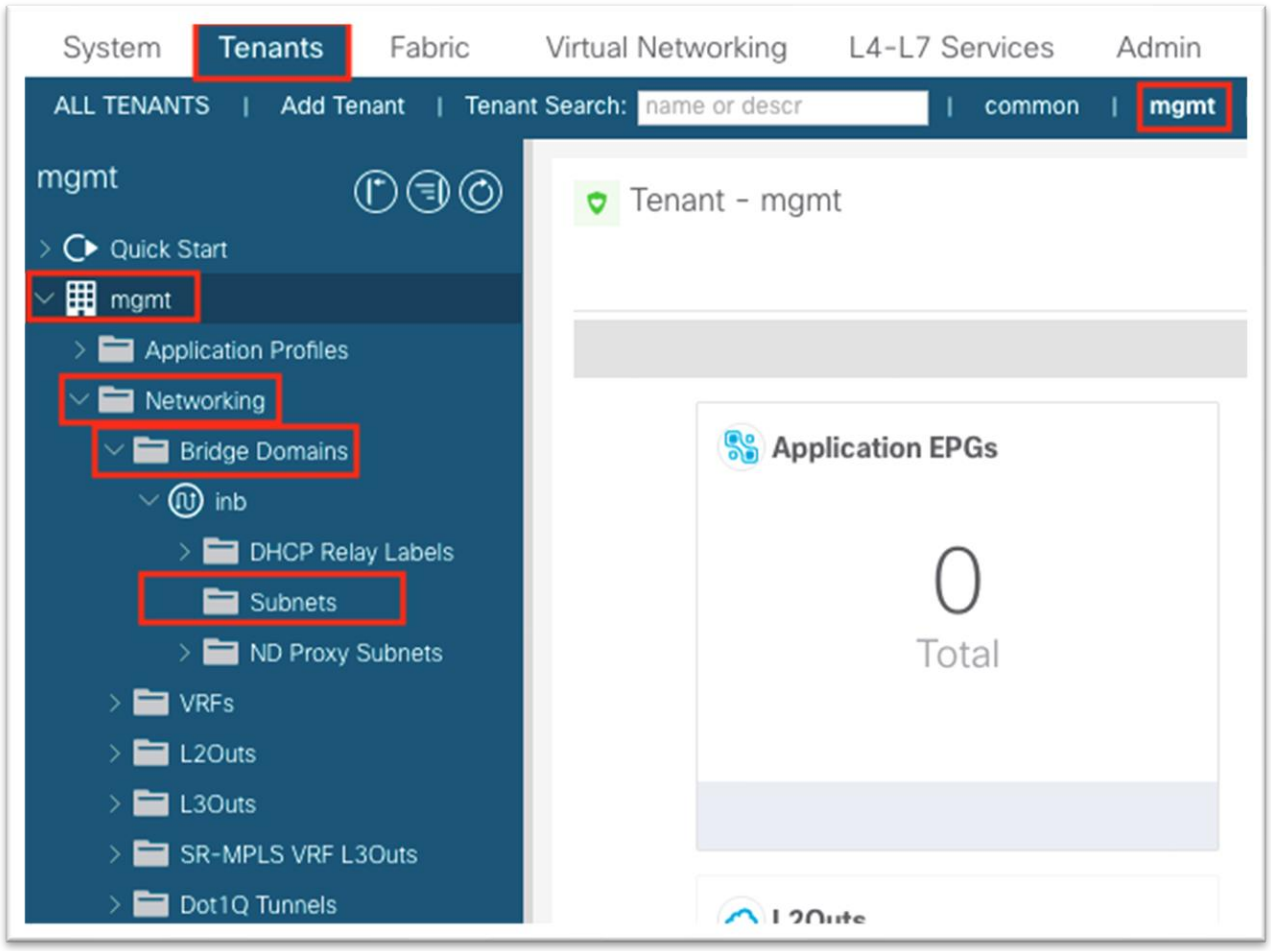
j. もう一度 [保存（Save）] をクリックします。



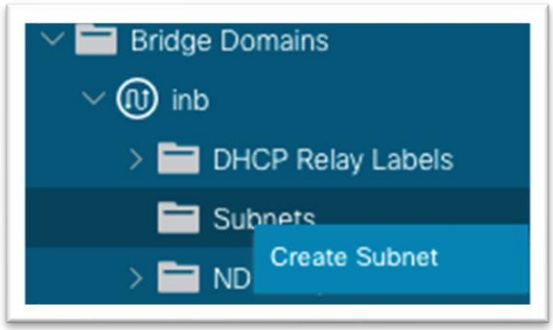
k. [送信（Submit）] をクリックします。



3. **[テナント（Tenants）] > [管理（mgmt）]** に移動します。
4. **[ネットワーキング（Networking）]**、**[ブリッジ ドメイン（Bridge Domains）]**、**[inb]** の順に展開します。

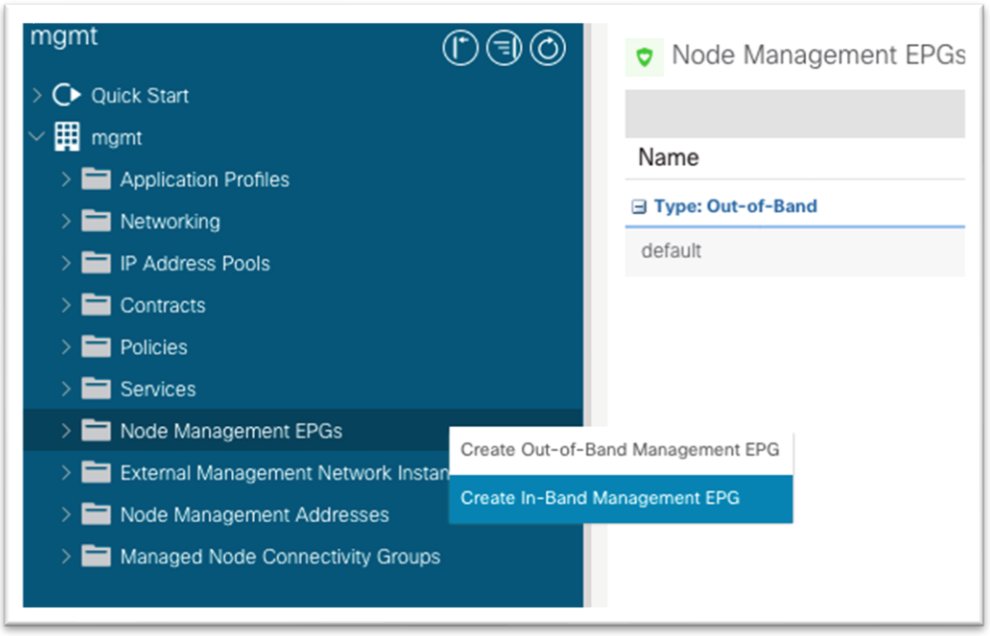


5. **[サブネット（Subnets）]** フォルダを右クリックし、**[サブネットの作成（Create Subnet）]** を選択します。

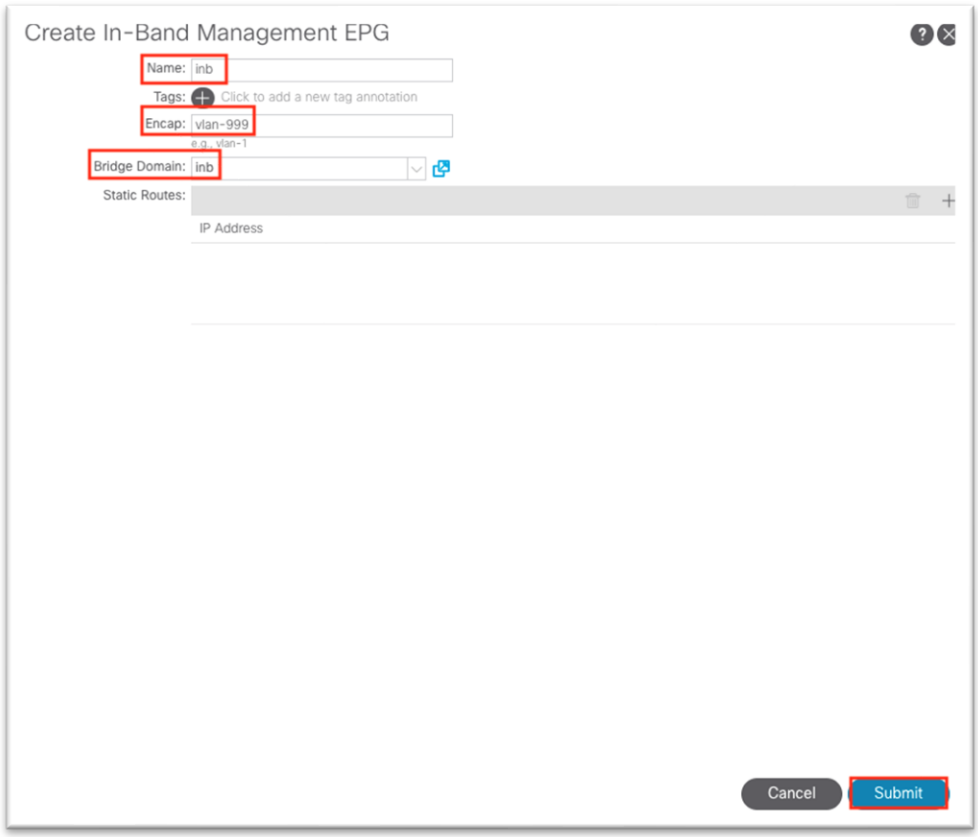


6. ダイアログで、インバンド管理サブネットのゲートウェイ IP アドレスを入力します。
    a. L3Out アドバタイズメントに必要な場合は、**[外部にアドバタイズメント（Advertised Externally）]** を選択します。

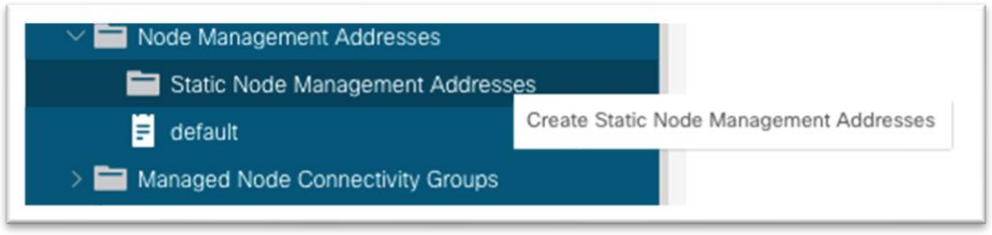
7. [送信（Submit）] をクリックします。
8. 管理テナントで、**[ノード管理 EPG（Node Management EPGs）]** フォルダを右クリックし、**[インバンド管理 EPG の作成（Create In-Band Management EPG）]** を選択します。



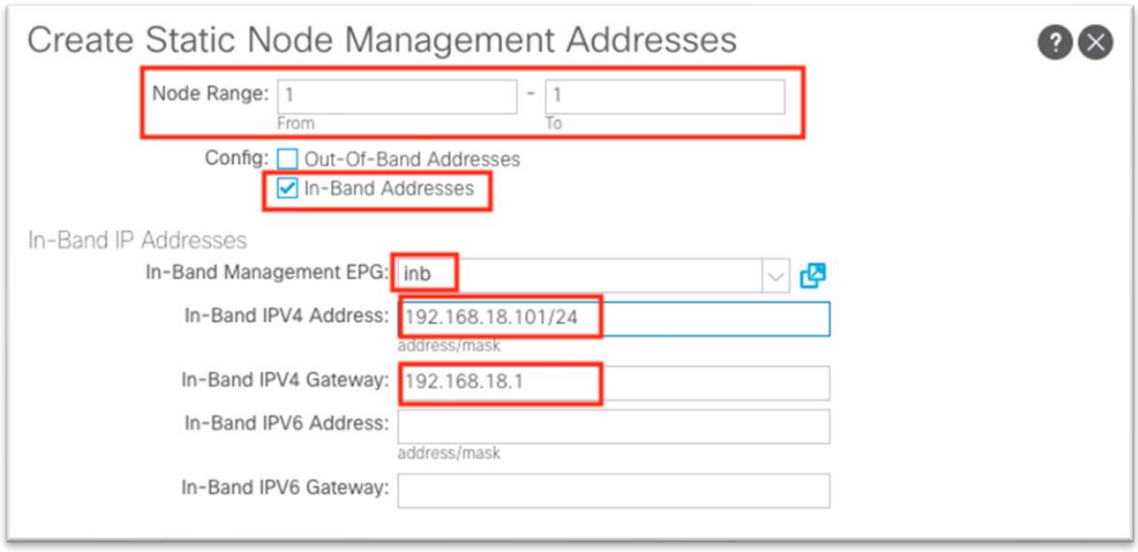
9. このダイアログで以下を行います。
    a. インバンド管理 EPG の名前を入力します。
    b. アクセス ポリシーの設定時に、ステップ 2.h.ii で定義した VLAN を入力します。形式として「VLAN-###」を使用します。
    c. **[ブリッジ ドメイン（Bridge Domain）]** ドロップダウン リストから、インバンド ブリッジ ドメインを選択します。
    d. [送信（Submit）] をクリックします。



10. 管理テナントで、**[ノード管理アドレス（Node Management Addresses）]** を展開します。
11. **[スタティック ノード管理アドレス（Static Node Management Addresses）]** を右クリックし、**[スタティック ノード管理アドレスの作成（Create Static Node Management Addresses）]** を選択します。



12. このダイアログで以下を行います。
    a. **[ノード範囲（Node Range）]** に、1 ～ 1の範囲を入力して Cisco APIC 1 を設定します。
    b. **[インバンド アドレス（In-band Addresses）]** チェックボックスをオンにします。
    c. **[インバンド管理 EPG（In-Band Management EPG）]** ドロップダウン リストで、ステップ 9 で作成した EPG を選択します。
    d. **[インバンド IPv4 アドレス（In-Band IPv4 Address）]** フィールドに、CIDR マスクを持つノードに使用する IP アドレスを入力します。
    e. **[インバンド IPv4 ゲートウェイ（In-Band IPv4 Gateway）]** フィールドに、ステップ 6 でインバンド ブリッジ ドメインに割り当てられたゲートウェイの IP アドレスを入力します。



f. [送信（Submit）] をクリックします。

13. 必要に応じて、ノード ID 1、2、3 などを使用して、Cisco APIC ごとにステップ 12 を繰り返します。同じように、ファブリックのリーフ ノード ID とスパイン ノード ID ごとにステップ 4 を繰り返します。

Cisco ACI インバンド管理ネットワークと Cisco Nexus ダッシュボード データ ネットワークの接続-オプション 1a：物理ドメインおよびスタティック パス バインディングを介して EPG に直接接続

Cisco Nexus ダッシュボード データ インターフェイス ネットワークは、Cisco ACI インバンド ネットワークに到達可能である必要があります。簡単にするために、これを実現するための 2 つの主要な接続オプションがあります。

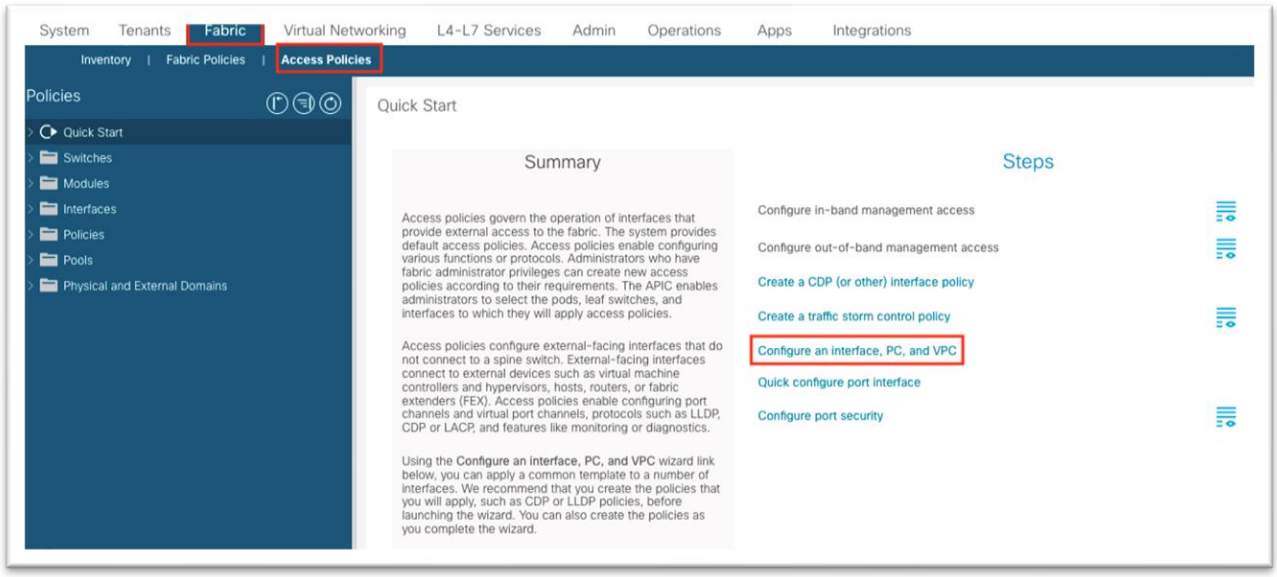
- Cisco ACI 内のエンドポイントとしての Cisco Nexus ダッシュボード。新しい固有のブリッジドメインと EPG の組み合わせに存在します。
- 管理テナント インバンド VRF インスタンスで L3Out を使用した到達可能な Cisco Nexus ダッシュボード

最初のオプションでは、Cisco Nexus ダッシュボードは Cisco ACI のレイヤ 3 エンドポイントとして学習され、Cisco ACI ファブリックは Cisco Nexus ダッシュボードのゲートウェイとして機能する必要があります。インバンド ブリッジ ドメイン サブネットに到達するには、インバンド VRF インスタンスに関連付けられた管理テナント内に Cisco Nexus ダッシュボード ブリッジ ドメインをローカルに展開します。そうしないと、Cisco Nexus ダッシュボード サブネットをインバンド VRF インスタンスににリークするためにルート リークが必要になります。Cisco Nexus ダッシュボード VRFインスタンスへのインバンド ブリッジ ドメイン サブネットも同様です。

設定手順

手順を次に示します。

1. **[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）]** に移動し、**[クイック スタート（Quick Start）]** メニューで **[インターフェイス、PC および vPC を設定する（Configure Interface, PC and vPC）]** を選択します。



2. ダイアログで緑のプラス記号 **[+]** を 2 回クリックしウィザードを展開します。

    a. ドロップダウンリストから、Cisco Nexus ダッシュボード データ ポートが接続されている 2 つのスイッチを選択します。

    b. **[スイッチ プロファイル名（Switch Profile Name）]** フィールドに名前を入力します。

    c. **[インターフェイス（Interface）]** を **[個別（Individual）]** に設定します。

    d. **[インターフェイス（Interfaces）]** フィールドに、Cisco Nexus ダッシュボード インターフェイスをカンマ区切りリストまたは範囲として入力します。

    e. **[インターフェイス セレクタ名（Interface Selector Name）]** フィールドに名前を入力します。

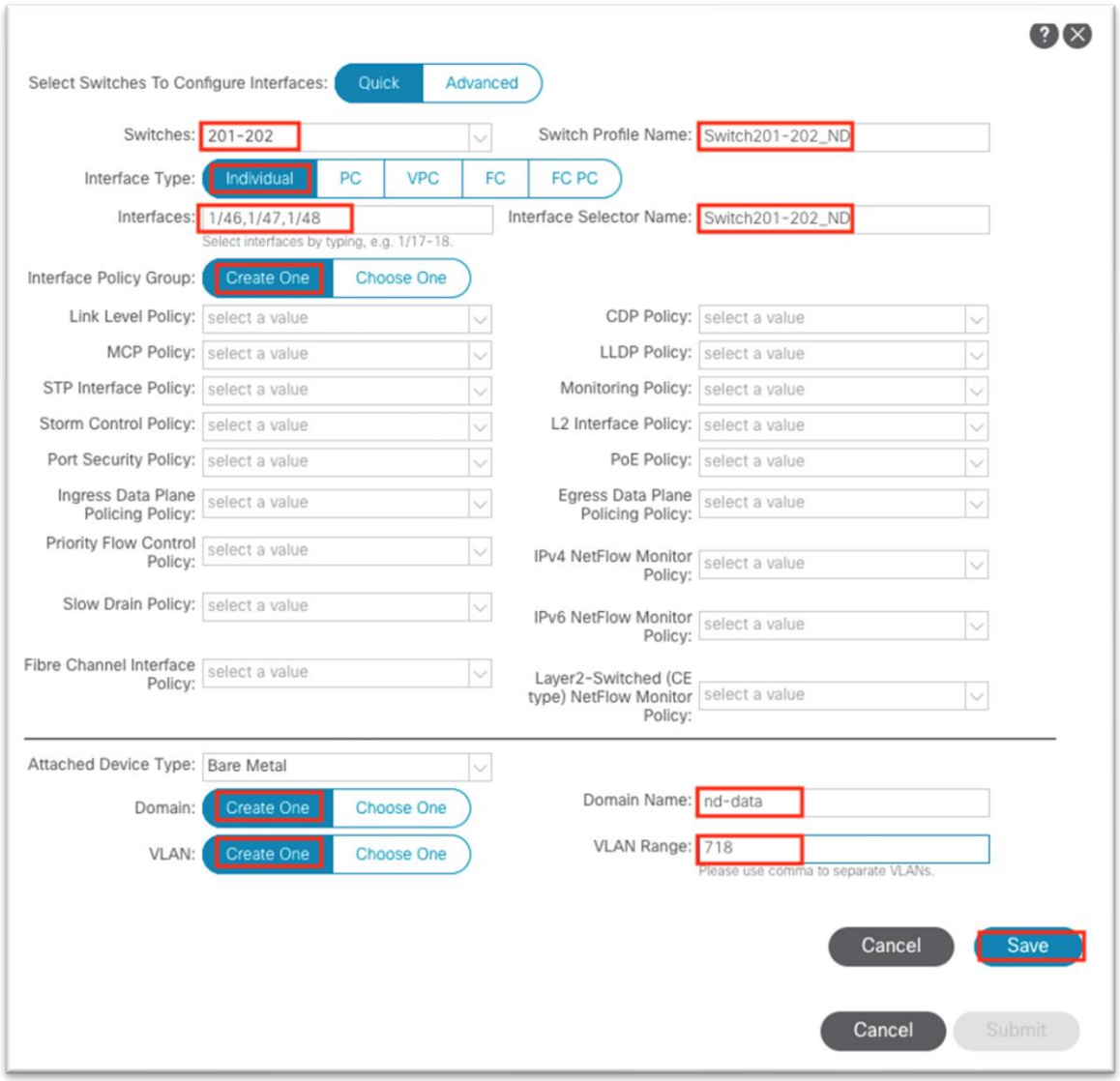
    f. **インターフェイス ポリシー グループ**を **[1 個作成（Create One）]** に設定します。インターフェイス レベルのポリシーを選択する必要はありません。デフォルトで十分です。

    g. **[接続済みデバイス タイプ（Attached Device Type）]**ドロップダウン リストで、**[ベア メタル（Bare Metal）]** を選択します。

    h. **ドメイン**と **VLAN** の両方を **[1 個を作成（Create One）]** に設定する必要があります。

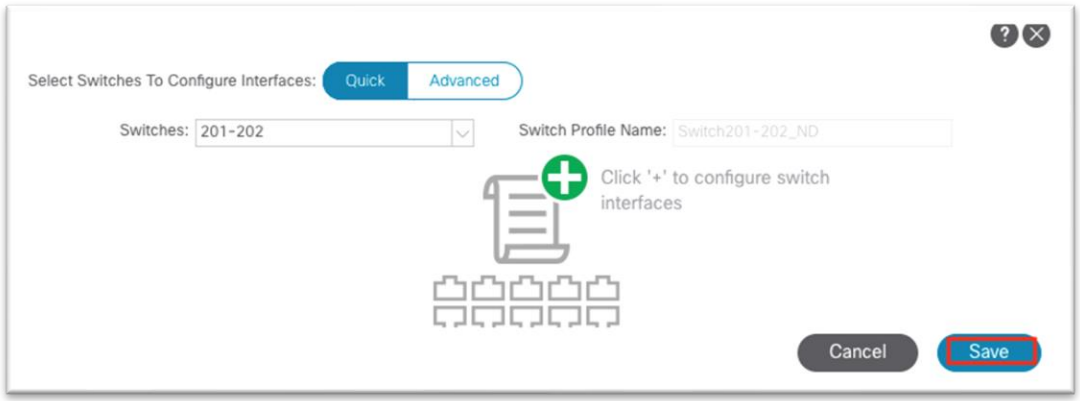
        i. **[ドメイン名（Domain Name）]** フィールドに名前を入力して、インバンド管理に関連付けられている物理ドメインに名前を付けます。

        ii. ファブリックのスタティック パス バインディングに使用される VLAN ID を入力します。

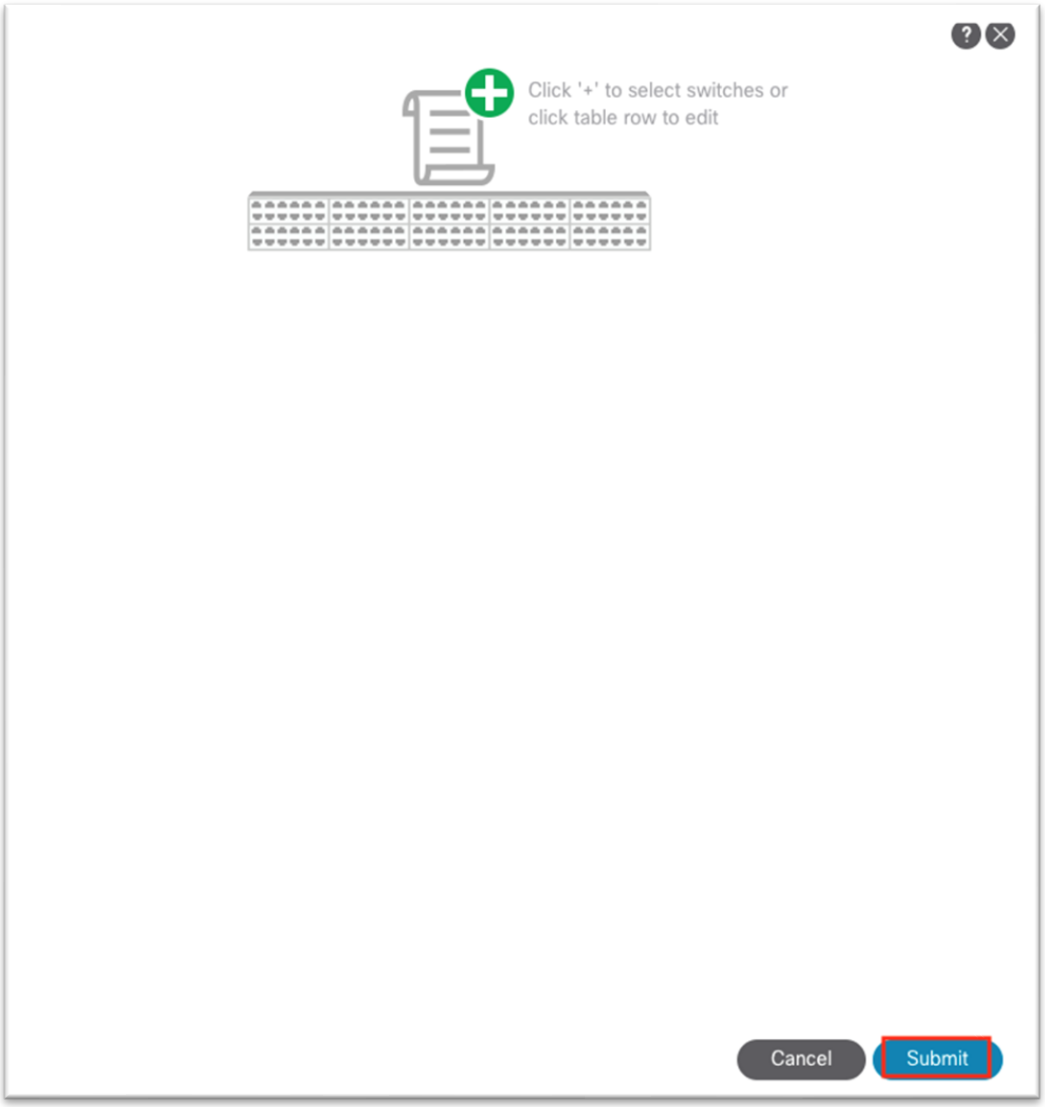


i. [保存（Save）] をクリックします。

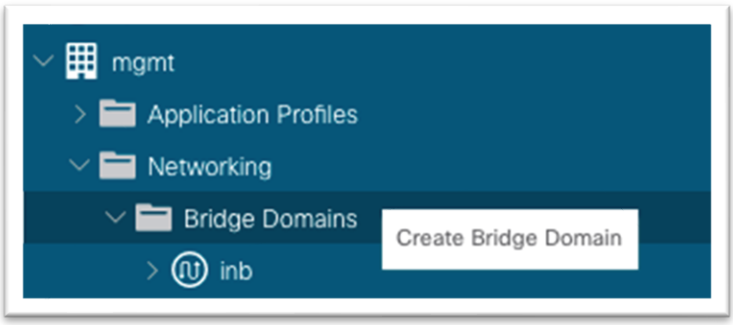
j. もう一度 [保存（Save）] をクリックします。



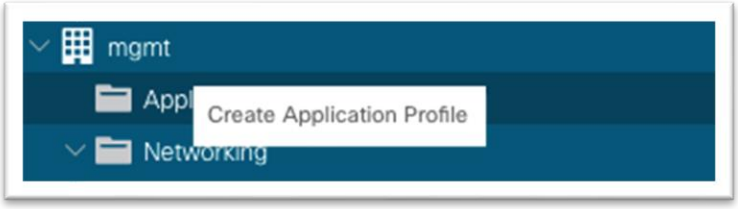
k. [送信（Submit）] をクリックします。



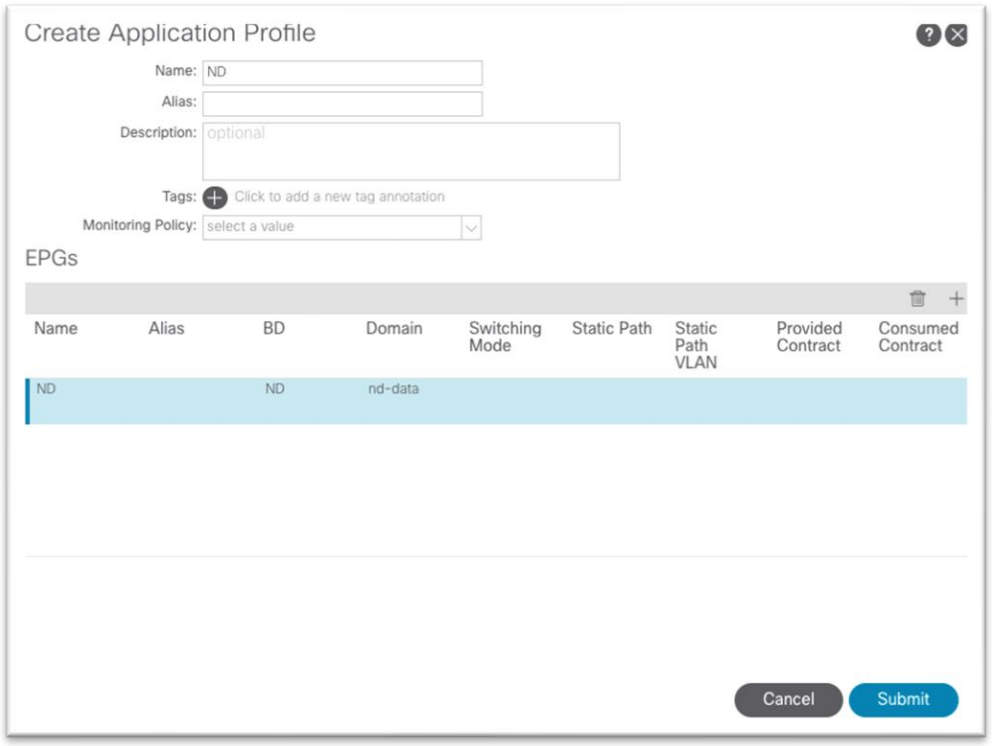
3. **[テナント（Tenants）] > [管理（mgmt）]** に移動します。
4. **[ネットワーキング（Networking）] > [ブリッジ ドメイン（Bridge Domains）]** を展開します。
5. **[ブリッジ ドメイン（Bridge Domains）]** フォルダを右クリックし、**[ブリッジ ドメインの作成（Create Bridge Domain）]** を選択します。



6. ブリッジ ドメイン名を入力します。
    a. **[VRF]** ドロップダウン リストで **[inb]** を選択します。
    b. [次へ（Next）] をクリックします。
    c. **[サブネット（Subnets）]** 領域の **[+]** 記号をクリックして、ダイアログを表示します。
        i. Cisco Nexus ダッシュボード データ ネットワーク ゲートウェイの IP アドレスと CIDR マスクを入力します。
        ii. 必要に応じて、**[外部でアドバタイズ（Advertise Externally）]** を選択します。
        iii. [OK] をクリックします。
    d. 必要に応じて、**[Associated L3Outs]** で **[+]** をクリックし、インバンド **VRF** インスタンス **L3Out** を選択します。
    e. [次へ（Next）] をクリックします。
    f. **[Finish（完了）]** をクリックします。
7. Still under the mgmt tenant, navigate to **Application Profiles** and right-click and choose **Create Application Profile**.]



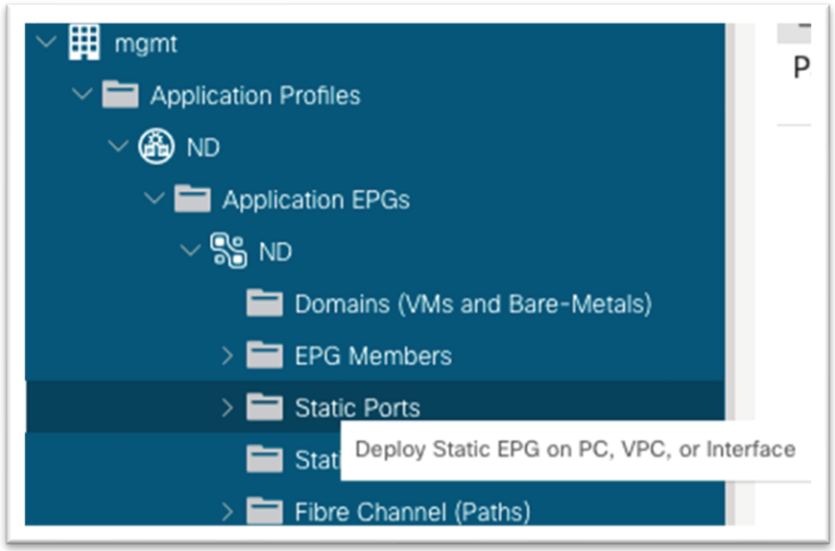
8. ダイアログでアプリケーション プロファイルの名前を入力します。
9. **[EPG]** で、**[+]** 記号をクリックします。
    a. Cisco Nexus ダッシュボード データ インターフェイスが属する EPG の名前を入力します。
    b. ステップ 5 で作成したブリッジ ドメインを選択します。
    c. 前に作成した物理ドメインを選択します。
    d. **Update** をクリックします。



e. [送信（Submit）] をクリックします。

10. 新しく作成した **[アプリケーション プロファイル（Application Profile）] > [アプリケーション EPG（Application EPGs）] > [EPG]** を展開し、**[スタティック ポート（Static Ports）]** フォルダをクリックします。

    a. フォルダを右クリックし、**[PC、vPC、またはインターフェイスでスタティック EPG を展開する（Deploy Static EPG on PC, vPC, or Interface）]** を選択します。



    b. ダイアログで、**[ポート（Port）]** を選択します。

    c. **[ノード（Node）]** ドロップダウン リストで、最初の Cisco Nexus ダッシュボード データ インターフェイスが接続されている最初のリーフ ノードを選択します。

d. **[パス（Path）]**ドロップダウン リストで、ダッシュボード データ インターフェイスが接続されているノードのインターフェイスを選択します。

e. **[ポート エンキャップ（Port Encap）]** フィールドに、アクセス ポリシーで VLAN プールを定義するときに作成した VLAN 番号を入力します。

f. **[展開の即時性（Deployment Immediacy）]** で、**[即時（Immediate）]** を選択します。

g. **[モード（Mode）]** で、Cisco Nexus ダッシュボード アプライアンスの設定方法に基づいて適切なモードを選択します。

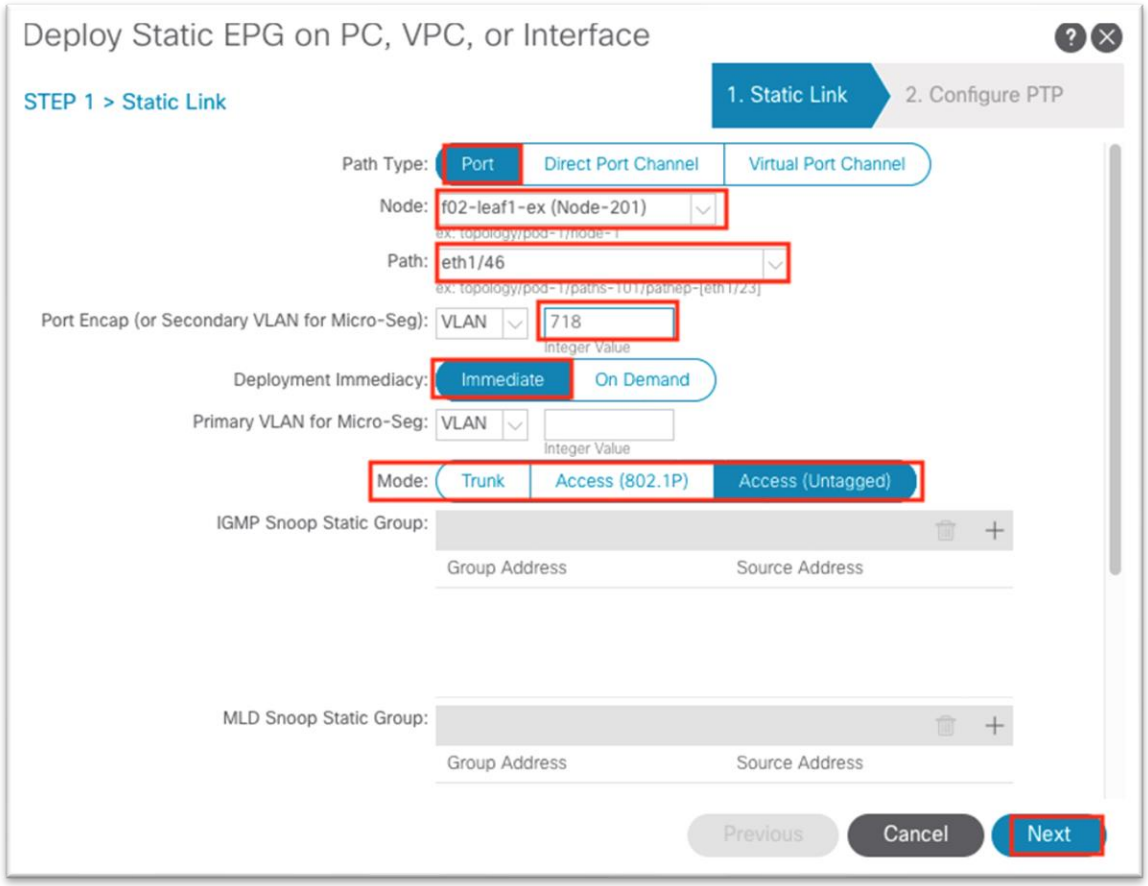
   i. Cisco Nexus ダッシュボードに VLAN TAG が設定されている場合は、**[トランク（Trunk）]** を選択します。

   ii. Cisco Nexus ダッシュボードが VLAN タグなしで設定されている場合は、**[アクセス（Access）]** を選択します。

h. [次へ（Next）] をクリックします。

i. **[Finish（完了）]** をクリックします。

j. ファブリックに接続されているすべての Cisco Nexus ダッシュボード データ インターフェイスに対して、このプロセスを繰り返します。



11. 引き続き管理テナントの下の場合は、**[コントラクト（Contracts）]** にand expand the folder.

12. **[標準（Standard）]** を右クリックし、**[コントラクトの作成（Create Contract）]** を選択します。

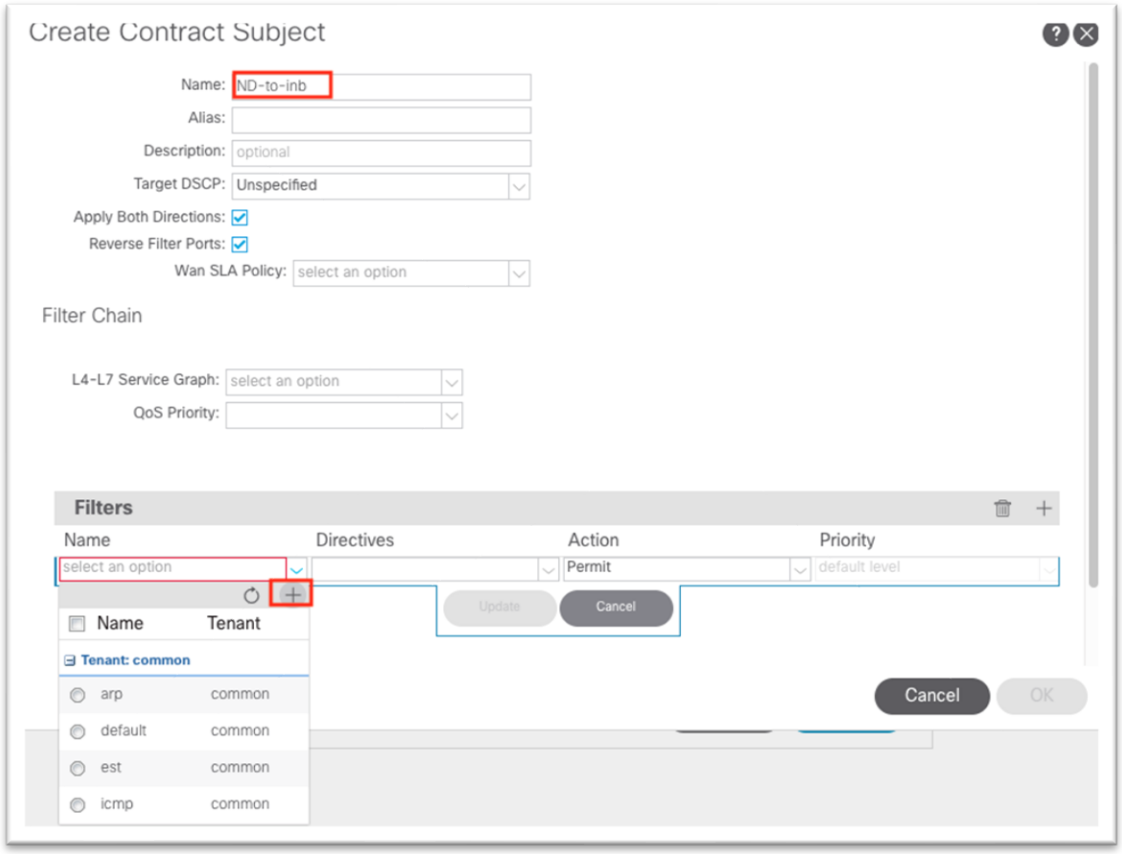
13. ダイアログで、コントラクトに名前を付けます。フローの観点から明確な名前を使用します。例：ND-to-inb。

    a. 件名を作成するには、**[+]** をクリックします。

        i. 新しいダイアログで、件名に名前を付けます。

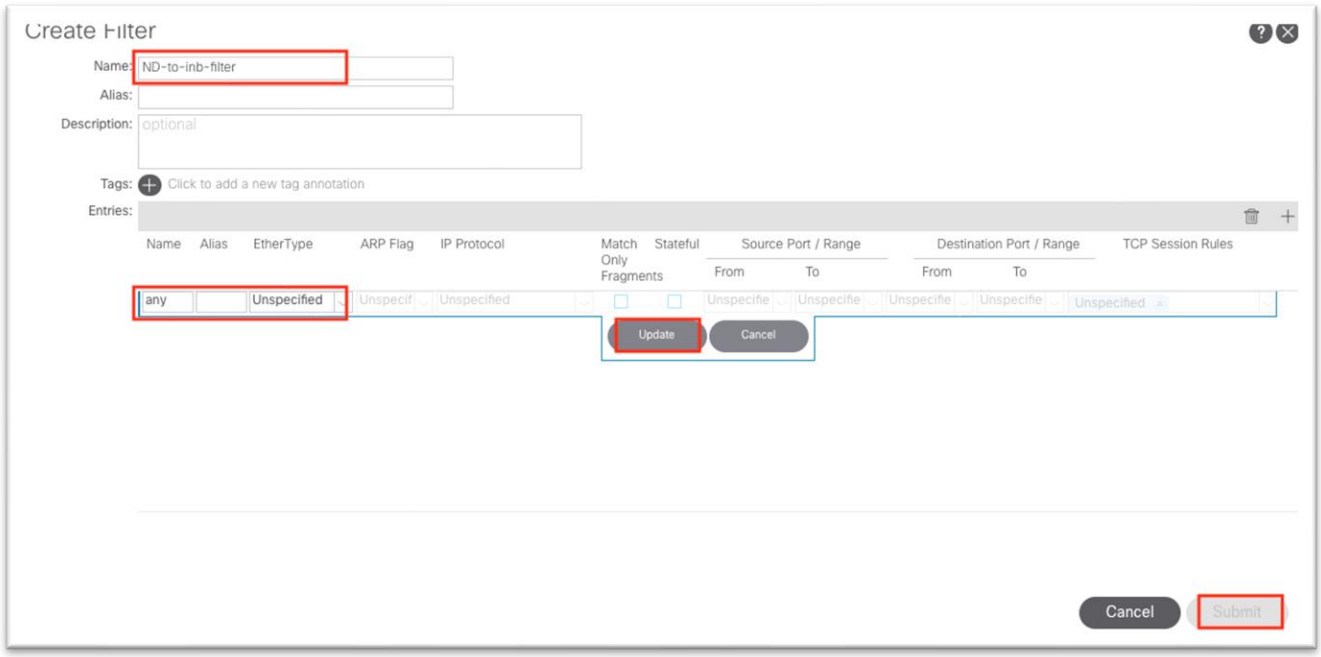
        ii. **[+]** をクリックして、新しいフィルタを作成します。

        iii. **[名前（Name）]** の下のドロップダウン リストを展開し、**[+]** をクリックして新しいフィルタを作成します。



        iv. 新しいダイアログで、フィルタに名前を付けます。

        v. エントリの下の **[+]** をクリックします。



vi. エントリに名前を付けます。

vii. ドロップダウン リストから **[Ether タイプ（Ether Type）]** を選択します。すべての通信を許可するには、値を未指定のままにします。

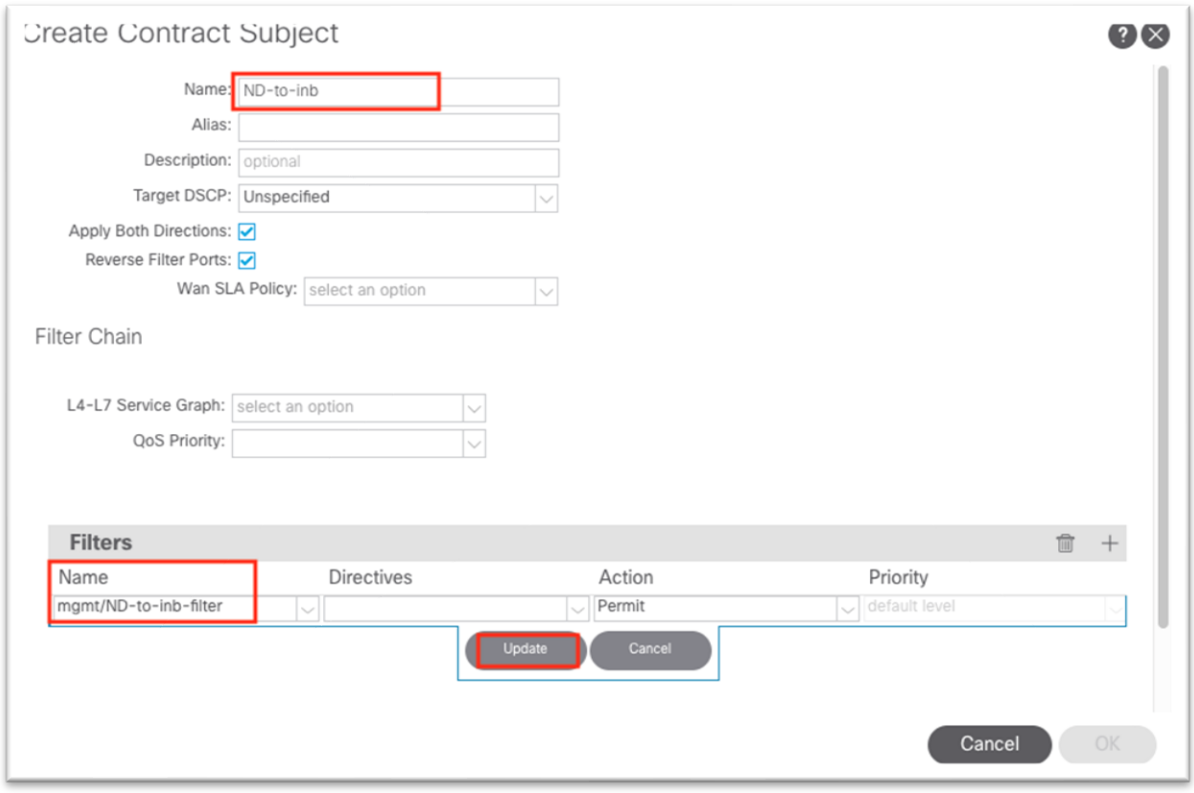
viii. IP プロトコルを選択します。

ix. 接続先ポートを入力します。

x. [更新（Update）] をクリックします。

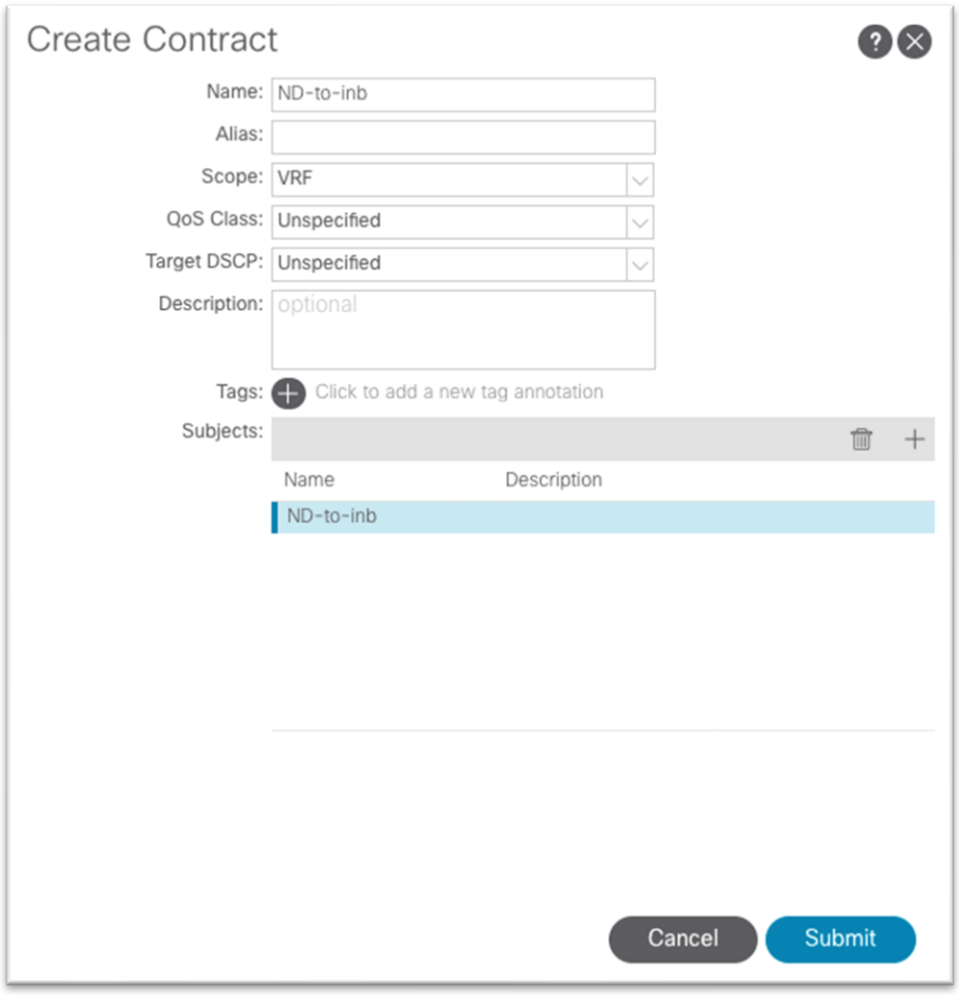
xi. **[フィルタを作成（Create Filter）]** ダイアログで **[送信（Submit）]** をクリックします。**[コントラクト件名の作成（Create Contract Subject）]** で新しいフィルタを選択する必要があります。

b. [更新（Update）] をクリックします。



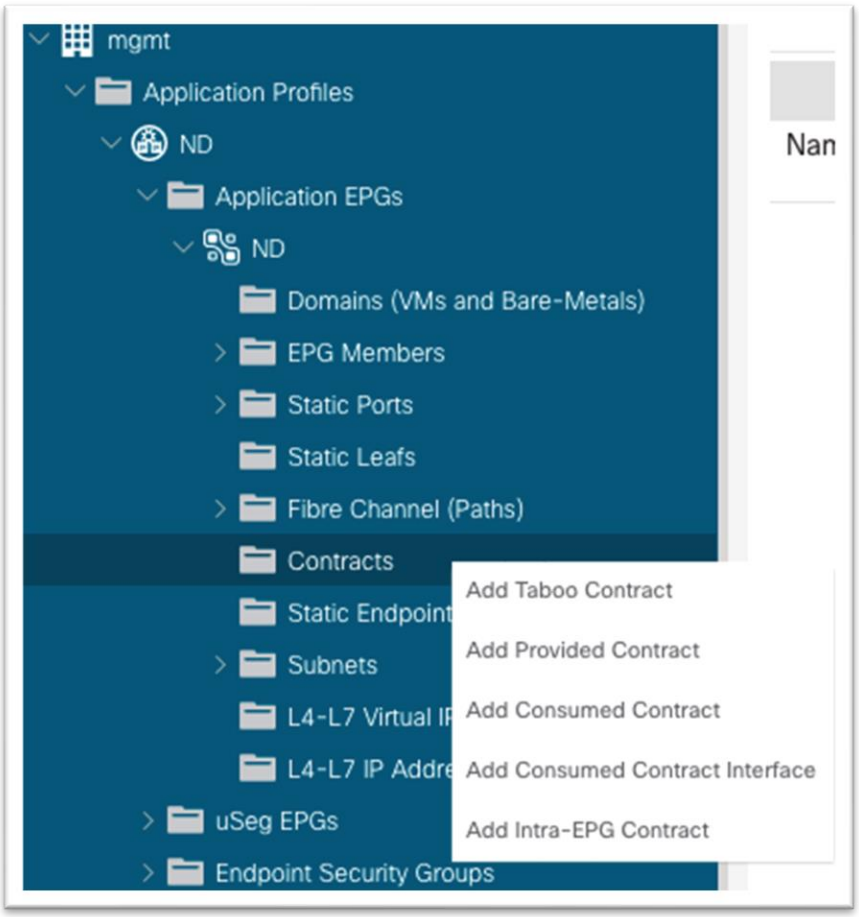
c. **[OK]** をクリックして件名を入力します。

d. 件名は **[コントラクトの作成（Create Contract）]** ダイアログの **[件名（Subjects）]** セクションに表示されます。

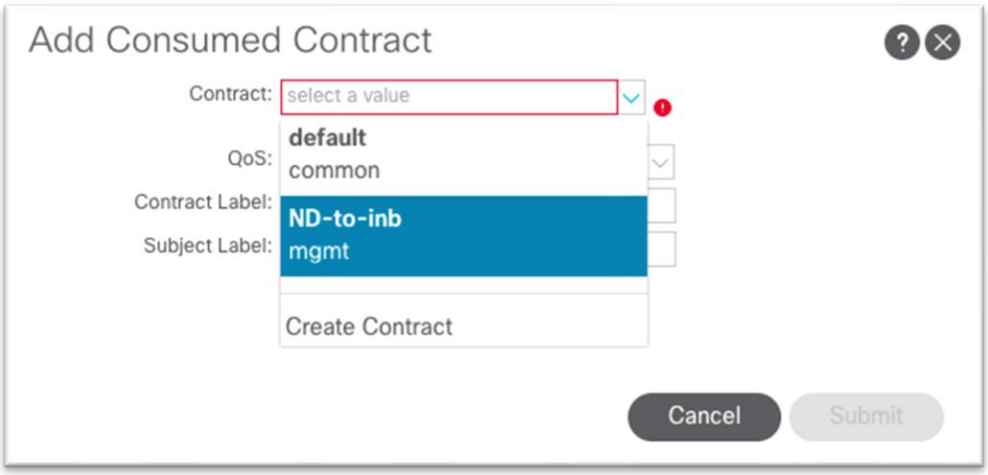


e. [送信（Submit）] をクリックします。

14. 管理テナントで、**[アプリケーション プロファイル（Application Profiles）] > [your-AP-name] > [アプリケーション EPG（Application EPGs）] > [your-EPG-name]** の順に移動し、**[コントラクト（Contracts）]** を右クリックして、**[消費したコントラクトの追加（Add Consumed Contract）]** を選択します。



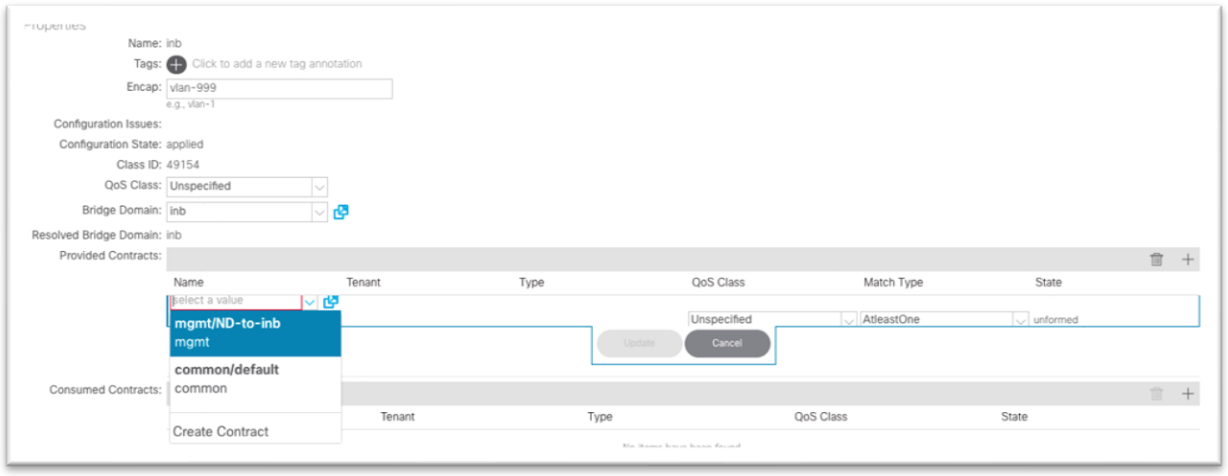
15. ダイアログの **[コントラクト（Contract）]** ドロップダウン リストで、ステップ 13 で作成したコントラクトを選択します。



a. [送信（Submit）] をクリックします。

16. 管理テナントで、**[ノード管理 EPG（Node Management EPGs）]** に移動し、インバンド EPG を選択します。

17. **[指定したコントラクト（Provided Contracts）]** の下の **[+]** をクリックし、**[名前（Name）]** ドロップダウン リストでステップ 13 で作成したコントラクトを選択します。



18. [更新（Update）] をクリックします。

これで、Cisco Nexus ダッシュボードが EPG に直接接続され、インバンド管理が可能になります。

Cisco ACI インバンド管理ネットワークと Cisco Nexus ダッシュボード データ ネットワークの接続：オプション 1b：仮想 Cisco Nexus ダッシュボードの VMM ドメインを使用した EPG への直接接続

Cisco ACI での VMM 統合は、外部仮想化コントローラ ノースバウンド API を活用して、プログラム可能な自動化された拡張性の高い方法でネットワーク構造を管理するプロセスです。複数のハイパーバイザ ベンダーがサポートされています。詳細については「仮想化互換性マトリクス」を参照してください。VMM 統合の詳細については、『Cisco ACI 仮想化ガイド』を参照してください。

Cisco Nexus ダッシュボード リリース 2.1 では、仮想フォームファクタの使用例が Cisco Nexus ダッシュボード Insights に拡張されています。現在、VMware vCenter（.ova）および KVM（.qcow2）仮想マシンがサポートされています。仮想 Cisco Nexus ダッシュボードとその展開の詳細については、『Cisco Nexus ダッシュボード 2.1 展開ガイド』を参照してください。仮想 Cisco Nexus ダッシュボードのデータ インターフェイスは、Cisco ACI のインバンド管理ネットワークにアクセスする必要があります。このドキュメントでは、VMM の統合が VMware vCenter または Red Hat 仮想化に対して行われていることを前提としています。

オプション 1a と同様に、ここでは、仮想 Cisco Nexus ダッシュボードが、サポートされるハイパーバイザを使用してリーフ スイッチに直接接続されるか、または単一の中間スイッチを介して接続されることを前提としています。仮想 Cisco Nexus ダッシュボードは Cisco ACI のレイヤ 3 エンドポイントとして学習され、Cisco ACI ファブリックは Cisco Nexus ダッシュボードのゲートウェイとして機能する必要があります。インバンド ブリッジ ドメイン サブネットに到達するには、インバンド VRF インスタンスに関連付けられた管理テナント内に Cisco Nexus ダッシュボード ブリッジ ドメインをローカルに展開します。そうしないと、Cisco Nexus ダッシュボード サブネットをインバンド VRF インスタンスににリークするためにルート リークが必要になります。Cisco Nexus ダッシュボード VRFインスタンスへのインバンド ブリッジ ドメイン サブネットも同様です。

VMM の統合により、仮想 Cisco Nexus ダッシュボードをホストするハイパーバイザを接続するリーフ スイッチ インターフェイスを手動でプログラムする必要がなくなります。VMM 統合により、VM が検出されたポートで VLAN が動的にプログラムされます。必要なのは、正しいアクセス ポリシーと、VMM ドメインを EPG に関連付けることだけです。

設定手順

前提条件：

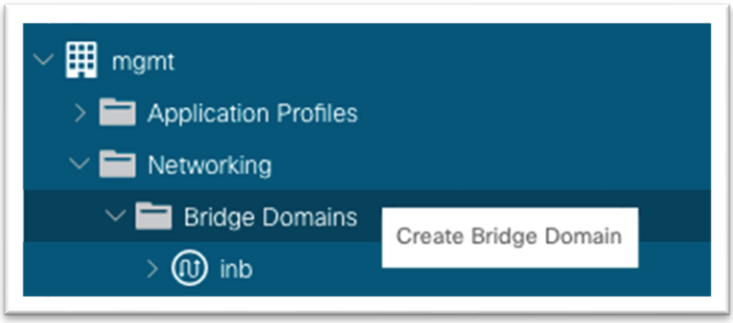
- 既存の VMM ドメイン
    - 既存の VMM ドメインに関連付けられた新しいハイパーバイザのアクセス ポリシー
    - 既存の VMM ドメインに関連付けられたアクセス ポリシーが設定された既存のハイパーバイザ

このセクションでは、次のようなテナントの側面に焦点を当てます。

- テナント ポリシー
    - アプリケーション プロファイル内の Cisco Nexus ダッシュボード データ インターフェイスと一致する EPG のブリッジ ドメイン。
    - Cisco Nexus ダッシュボード データ インターフェイスのブリッジ ドメイン サブネット
    - インバンド（ノード制御）EPG との通信を許可するコントラクト

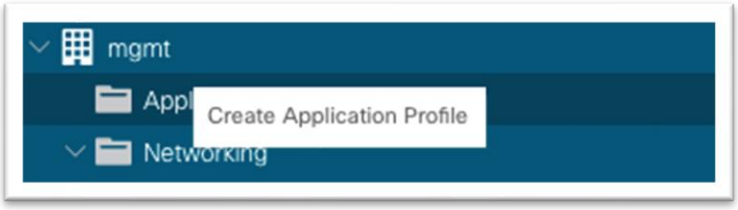
手順を次に示します。

1. **[テナント（Tenants）] > [管理（mgmt）]** に移動します。
2. **[ネットワーキング（Networking）] > [ブリッジ ドメイン（Bridge Domains）]** を展開します。
3. **[ブリッジ ドメイン（Bridge Domains）]** フォルダを右クリックし、**[ブリッジ ドメインの作成（Create Bridge Domain）]** を選択します。

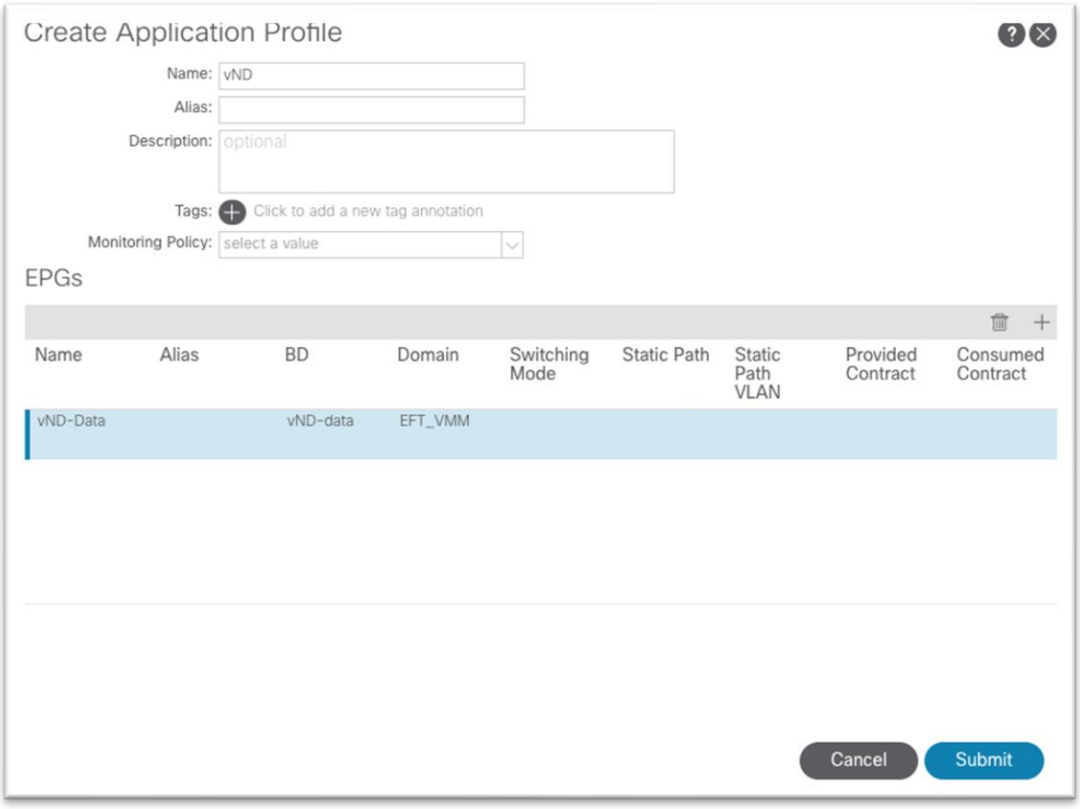


4. ブリッジ ドメイン名を入力します。
    a. **[VRF]** ドロップダウン リストで **[inb]** を選択します。
    b. [次へ（Next）] をクリックします。
    c. **[サブネット（Subnets）]** 領域の **[+]** 記号をクリックして、ダイアログを表示します。
        i. Cisco Nexus ダッシュボード データ ネットワーク ゲートウェイの IP アドレスと CIDR マスクを入力します。
        ii. 必要に応じて、**[外部でアドバタイズ（Advertise Externally）]** を選択します。
        iii. [OK] をクリックします。
    d. 必要に応じて、**[接続済み L3Outs（Associated L3Outs）]** で **[+]** をクリックし、インバンド VRF インスタンス L3Out を選択します。
    e. [次へ（Next）] をクリックします。
    f. **[Finish（完了）]** をクリックします。

5. 引き続き管理テナントの場合は **[アプリケーション プロファイル（Application Profiles）]** に移動し、**[アプリケーション プロファイルの作成（Create Application Profile）]** を選択します。



6. ダイアログでアプリケーション プロファイルの名前を入力します。
7. **[EPG]** で、**[+]** 記号をクリックします。
    a. Cisco Nexus ダッシュボード データ インターフェイスが属する EPG の名前を入力します。
    b. ステップ 5 で作成したブリッジ ドメインを選択します。
    c. VMM ドメインを選択します。
    d. **Update** をクリックします。



    e. [送信（Submit）] をクリックします。
8. 引き続き管理テナントの下の場合は、**[コントラクト（Contracts）]** にand expand the folder.
9. **[標準（Standard）]** を右クリックし、**[コントラクトの作成（Create Contract）]** を選択します。

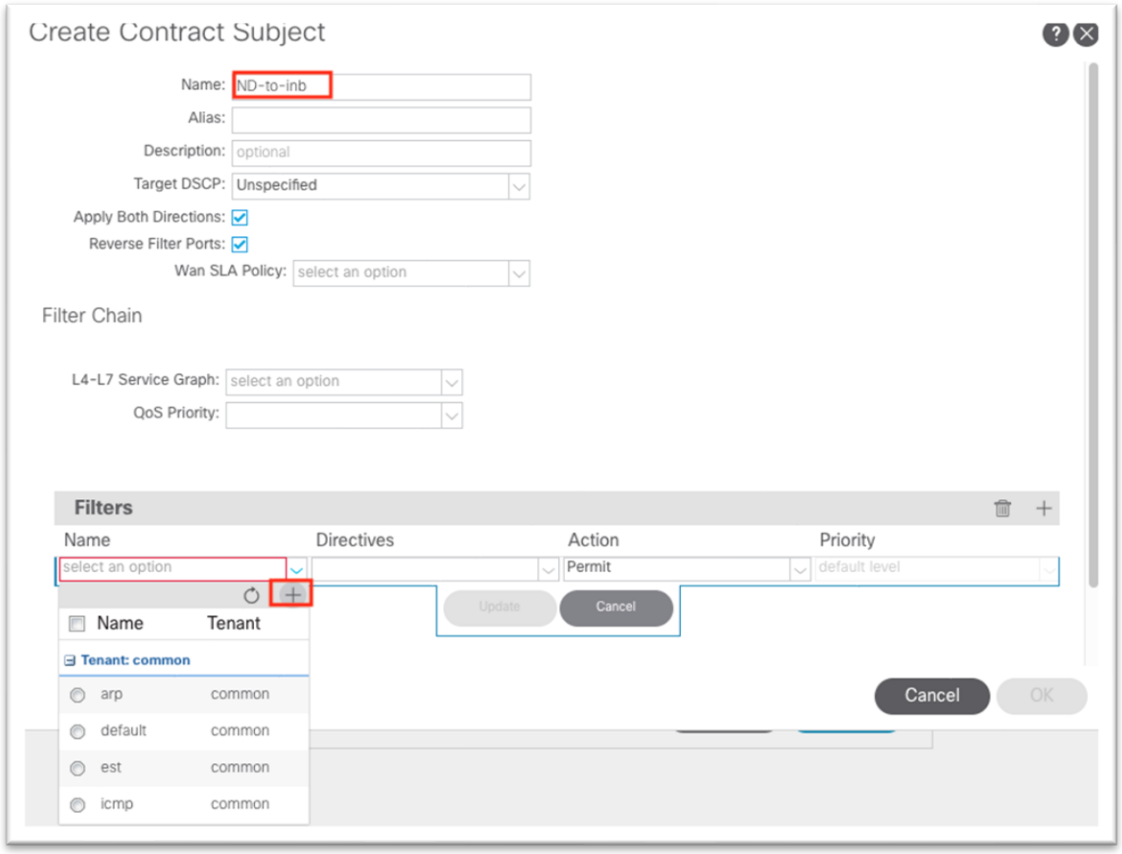
10. ダイアログで、コントラクトに名前を付けます。フローの観点から明確な名前を使用します。例：ND-to-inb。

    a. 件名を作成するには、**[+]** をクリックします。

        i. 新しいダイアログで、件名に名前を付けます。

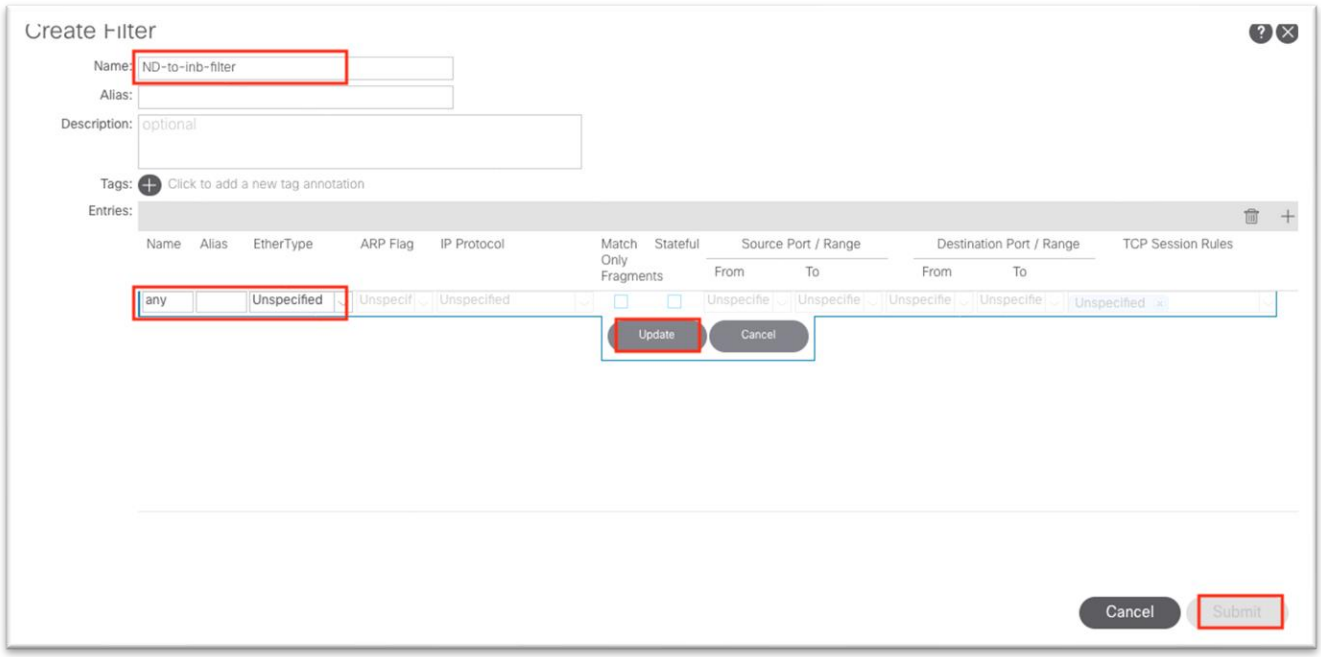
        ii. **[+]** をクリックして、新しいフィルタを作成します。

        iii. **[名前（Name）]** の下にあるドロップダウン リストを展開し、**[+]** をクリックして新しいフィルタを作成します。



        iv. 新しいダイアログで、フィルタに名前を付けます。

        v. **[エントリ（Entries）]** の下の **[+]** をクリックします。



vi. エントリに名前を付けます。

vii. ドロップダウン リストから **[Ether タイプ（Ether Type）]** を選択します。すべての通信を許可するには、値を未指定のままにします。

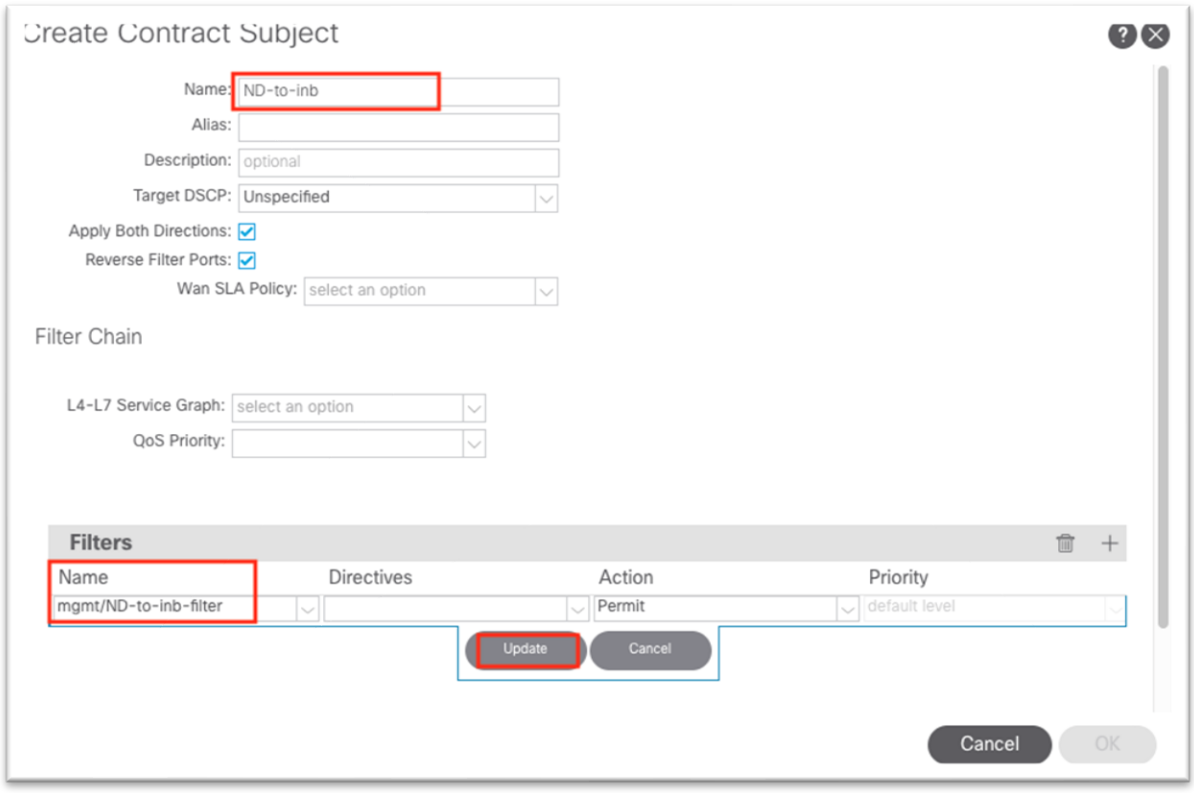
viii. IP プロトコルを選択します。

ix. 接続先ポートを入力します。

x. [更新（Update）] をクリックします。

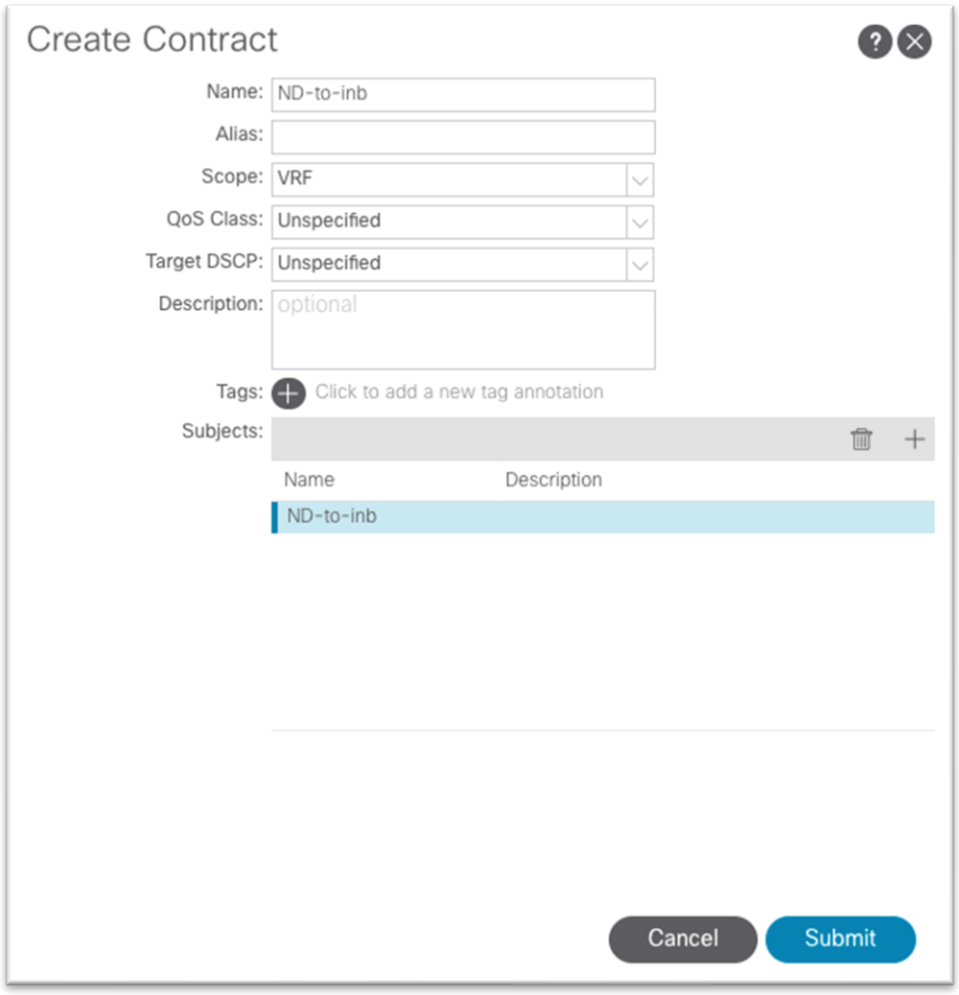
xi. **[フィルタを作成（Create Filter）]** ダイアログで **[送信（Submit）]** をクリックします。**[コントラクト件名の作成（Create Contract Subject）]** で新しいフィルタを選択する必要があります。

b. [更新（Update）] をクリックします。



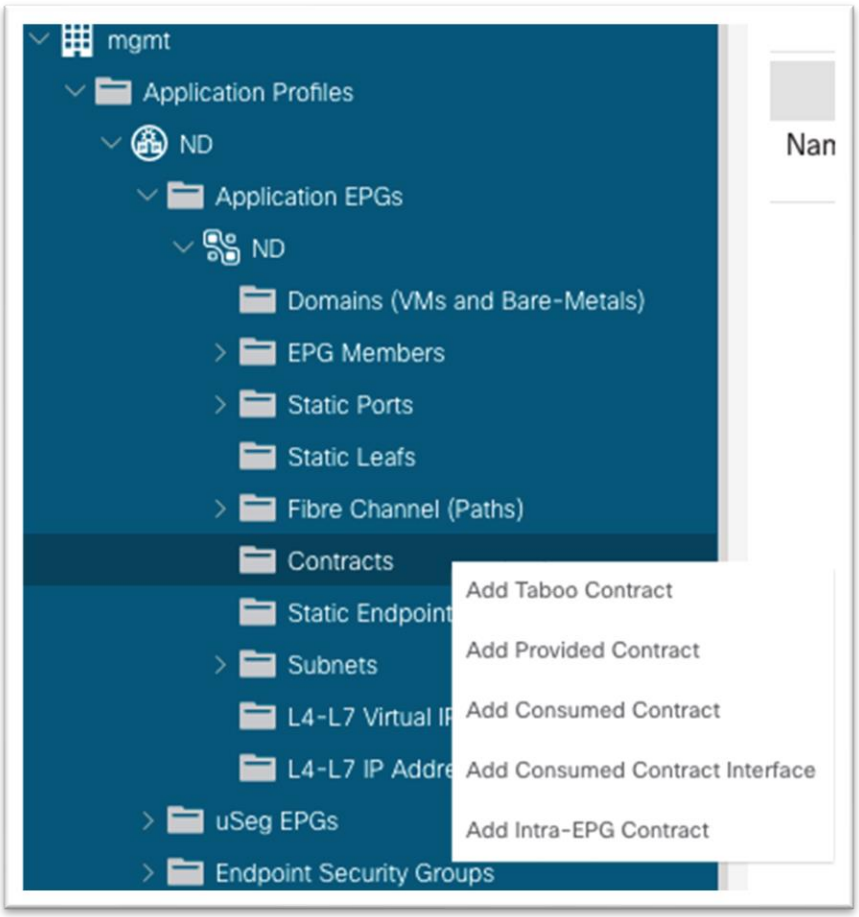
c. **[OK]** をクリックして件名を入力します。

d. 件名は **[コントラクトの作成（Create Contract）]** ダイアログの **[件名（Subjects）]** セクションに表示されます。

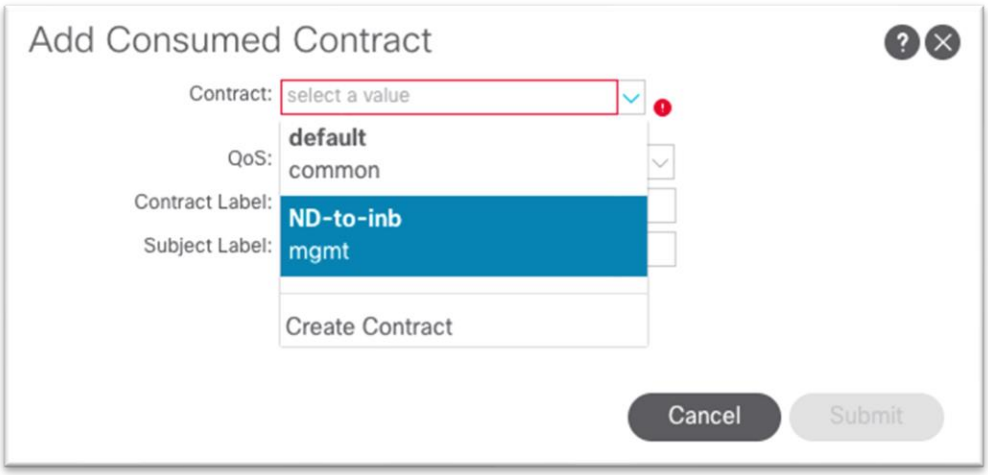


e. [送信（Submit）] をクリックします。

11. 管理テナントで、**[アプリケーション プロファイル（Application Profiles）] > [your-AP-name] > [アプリケーション EPG（Application EPGs）] > [your-EPG-name]** の順に移動し、**[コントラクト（Contracts）]** を右クリックして、**[消費したコントラクトの追加（Add Consumed Contract）]** を選択します。



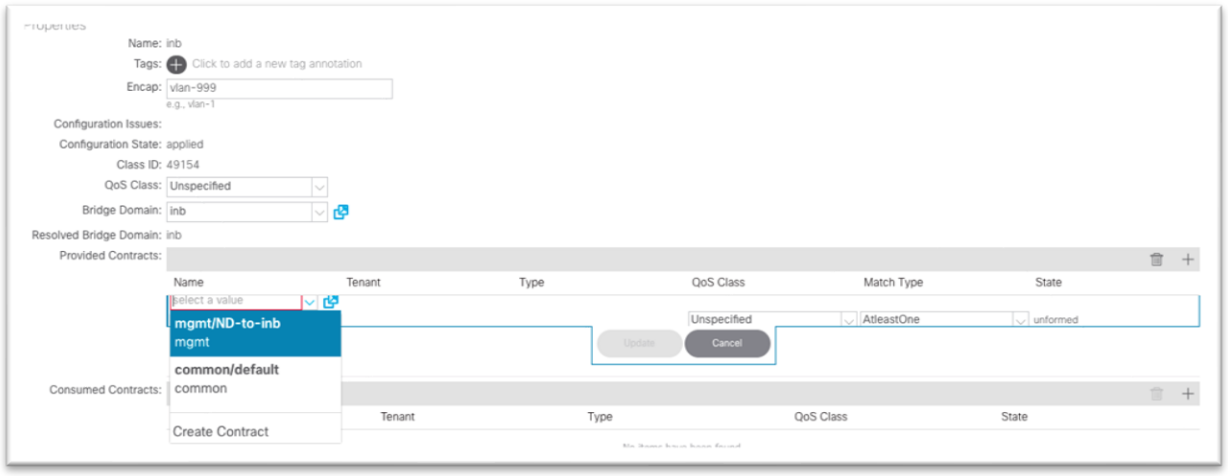
12. ダイアログの **[コントラクト（Contract）]** ドロップダウン リストで、ステップ 13 で作成したコントラクトを選択します。



a. [送信（Submit）] をクリックします。

13. 管理テナントで、**[ノード管理 EPG（Node Management EPGs）]** に移動し、インバンド EPG を選択します。

14. **[指定したコントラクト（Provided Contracts）]** の下の **[+]** をクリックし、**[名前（Name）]** ドロップダウン リストでステップ 13 で作成したコントラクトを選択します。



15. [更新（Update）] をクリックします。

これで、VMM 統合を活用する EPG に直接接続される仮想 Cisco Nexus ダッシュボードの接続セクションが完了します。

Cisco ACI インバンド管理ネットワークと Cisco Nexus ダッシュボード データ ネットワークの接続：オプション 2：Any Infra（L3Out を使用）

この展開モデルでは、Cisco Nexus ダッシュボード データ インターフェイスは、Cisco ACI の外部にあります。データ ネットワークは Cisco ACI インバンド管理ネットワークに到達可能である必要があり、同様に Cisco ACI インバンドは Cisco Nexus ダッシュボード データ インターフェイスに到達可能である必要があります。Cisco ACI 内部 VRF インスタンスが外部ネットワークと通信するには、外部ルータとのピアリングを確立するために L3Out が必要です。

このセクションでは、インバンド管理 VRF インスタンス「inb」の L3Out を設定し、インバンド ブリッジ ドメインのサブネット アウトをアドバタイズするとともに、ポリシーを学習して Cisco Nexus ダッシュボード データ インターフェイスなどの外部サブネットに適用します。

any infra 設定は、次の主要部分で要約できます。

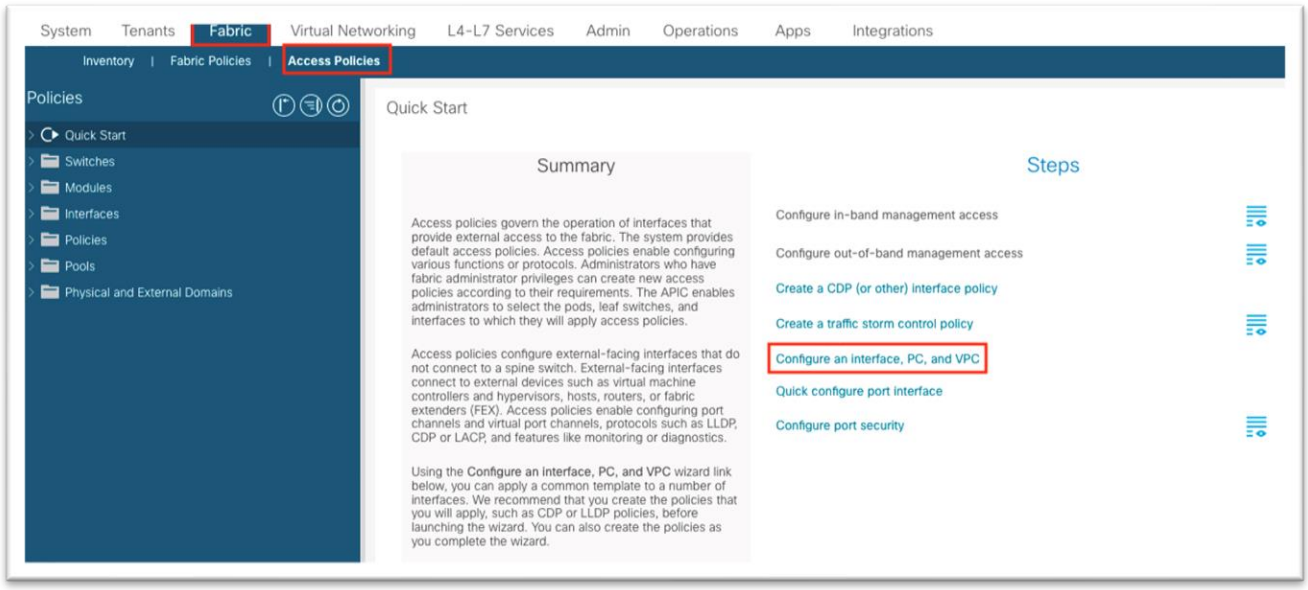
- L3Out のアクセスポリシー
- L3Out の設定
- インバンド EPG と L3Out 外部 EPG 間のコントラクト

詳細については、『Cisco APIC レイヤ 3 ネットワーキング設定ガイド』またはホワイト ペーパー『L3Out ガイド』を参照してください。

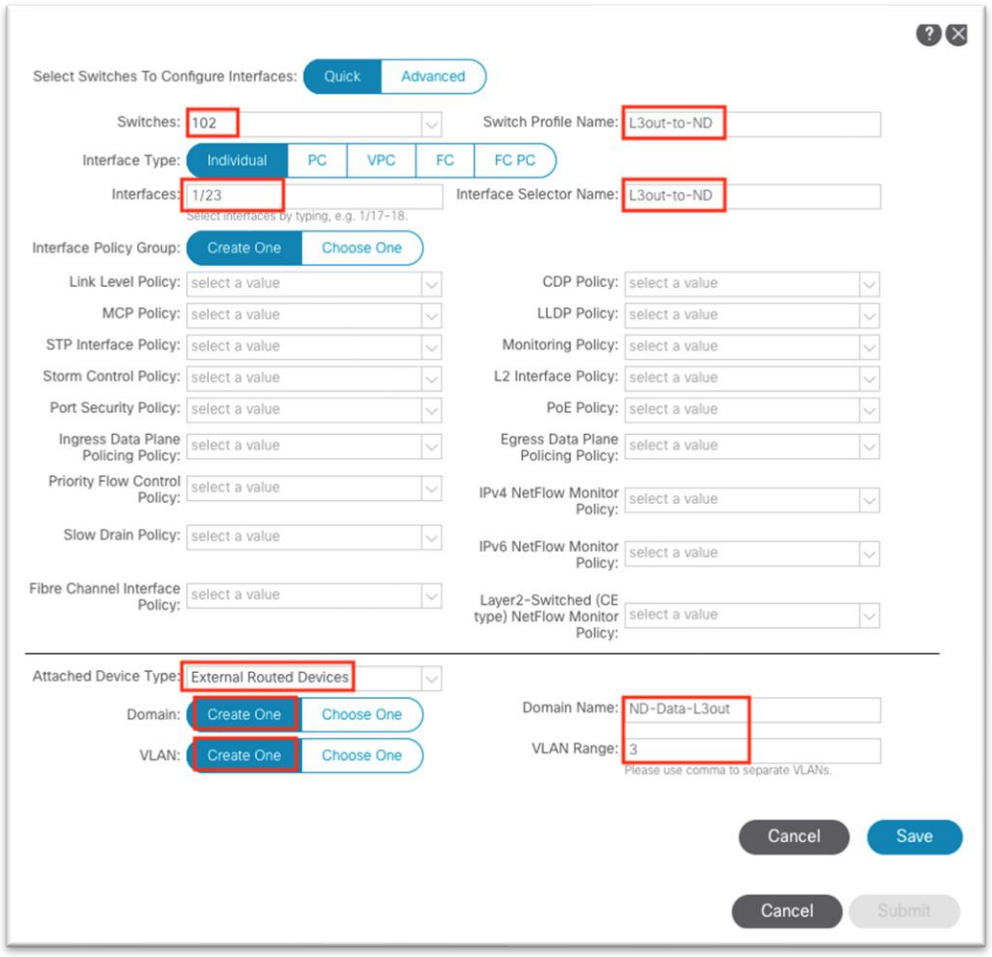
設定手順

手順を次に示します。

1. **[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）]** に移動し、**[クイック スタート（Quick Start）]** メニューで **[インターフェイス、PC および vPC を設定する（Configure Interface, PC and vPC）]** を選択します。

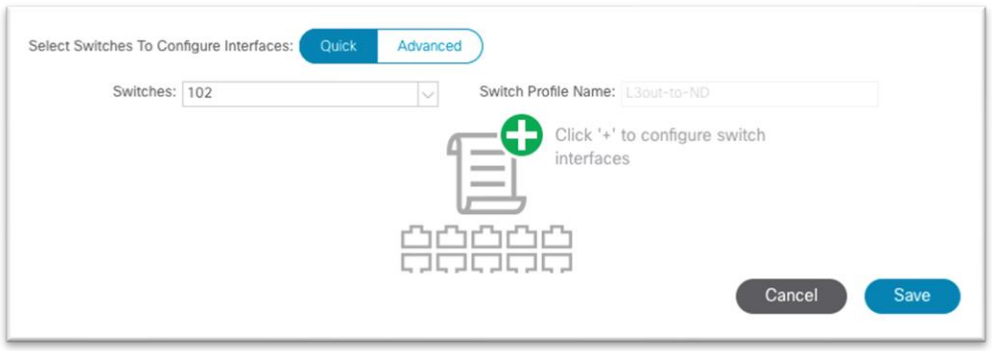


2. ダイアログで、緑のプラス記号 **[+]** を **2 回**クリックしてウィザードを展開します。
    a. ドロップダウン リストから、外部ルータが接続されているスイッチを選択します。
    b. **[スイッチ プロファイル名（Switch Profile Name）]** フィールドに名前を入力します。
    c. **[インターフェイス タイプ（Interface Type）]** から **[個別（Individual）]** に設定します。
    d. **[インターフェイス（Interfaces）]** フィールドに、外部ルータが接続されているポートをカンマ区切りリストまたは範囲として入力します。
    e. **[インターフェイス セレクタ名（Interface Selector Name）]** フィールドに名前を入力します。
    f. **インターフェイス ポリシー グループ**を **[1 個作成（Create One）]** に設定します。外部ルータに必要な適切なインターフェイス レベルのプロパティを選択します。
    g. **[接続済みデバイス タイプ（Attached Device Type）]**ドロップダウン リストで、**[ベア メタル（Bare Metal）]** を選択します。
    h. **ドメイン**と **VLAN** の両方を **[1 個を作成（Create One）]** に設定する必要があります。
        i. **[ドメイン名（Domain Name）]** フィールドに名前を入力して、インバンド管理に関連付けられている物理ドメインに名前を付けます。
        ii. ファブリックでスタティック パス バインディングに使用される VLAN ID を入力します。

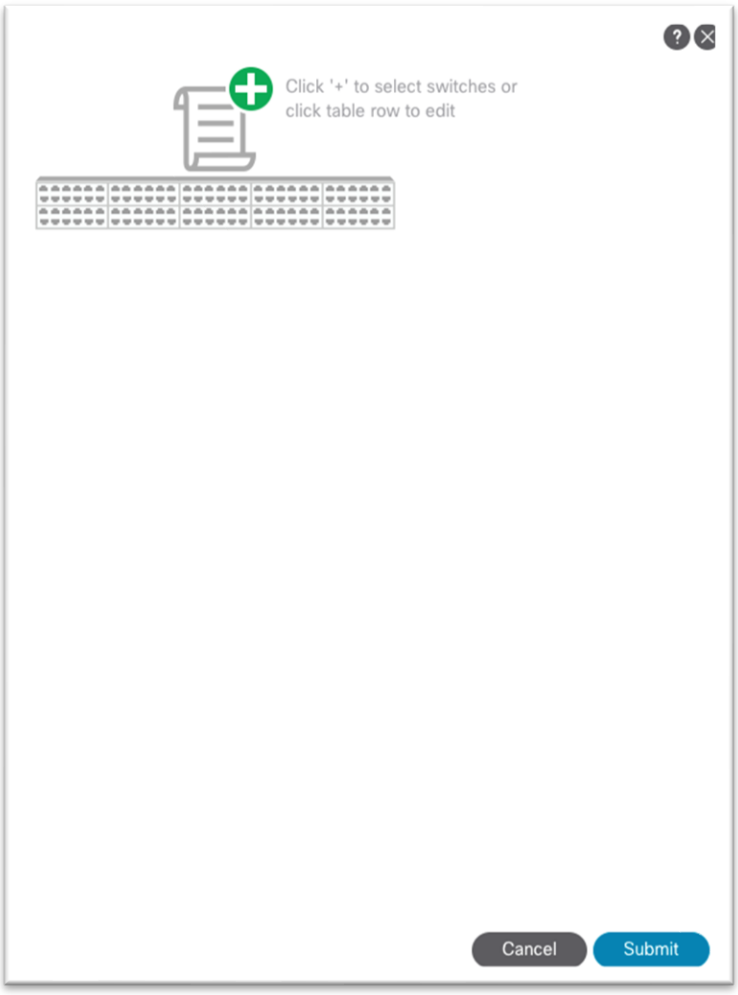


i. [保存（Save）] をクリックします。

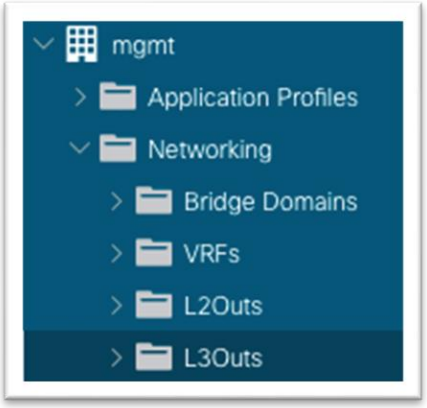
j. もう一度 [保存（Save）] をクリックします。



k. [送信（Submit）] をクリックします。



3. **[テナント（Tenants）] > [管理（mgmt）]** に移動します。
4. **[ネットワーキング（Networking）]** を展開します。
5. **[L3Outs]** フォルダを右クリックし、**[L3Out の作成（Create L3Out）]** を選択します。

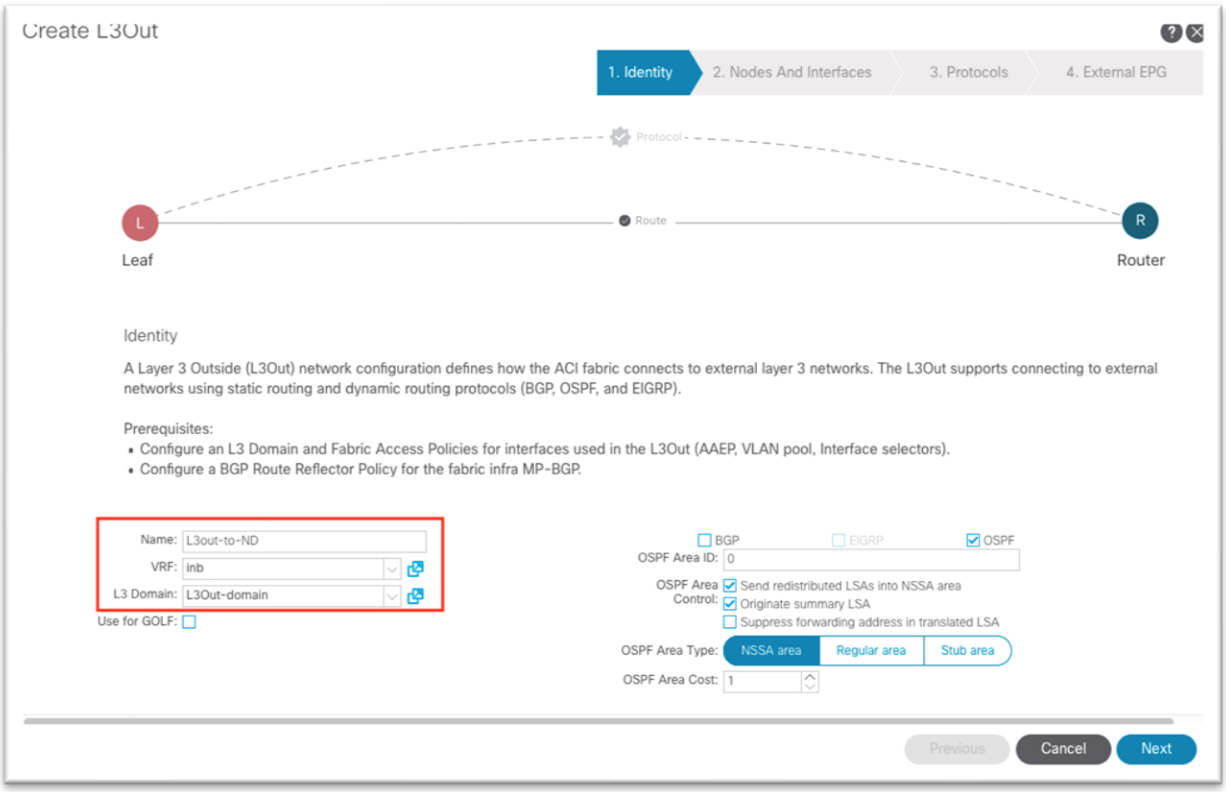


6. 新しいダイアログで、次の手順を実行します。
    a. L3Out の名前を入力します。
    b. VRF インスタンスを選択します。

c. 前の手順で作成したレイヤ 3 ドメインを選択します。

d. ルーティング プロトコルを選択するか、スタティック ルーティングの場合はフィールドを空白のままにします。

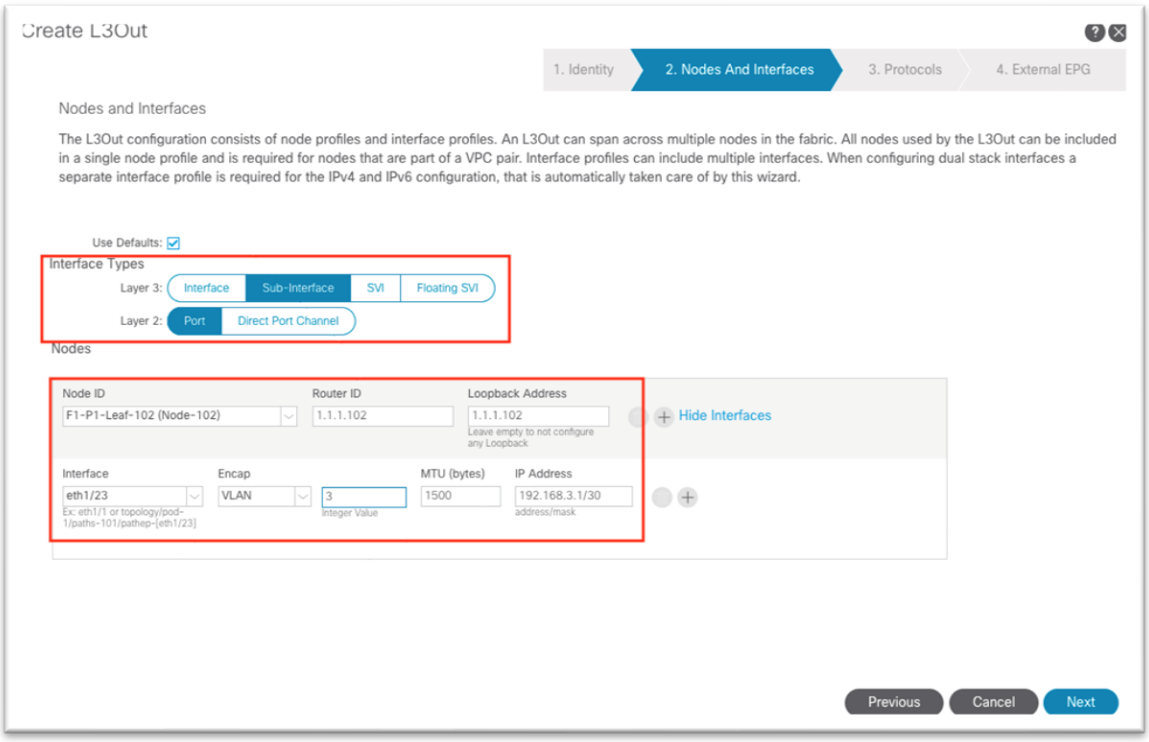
e. [次へ（Next）] をクリックします。



f. **レイヤ 3** および**レイヤ 2** インターフェイス タイプを選択します。

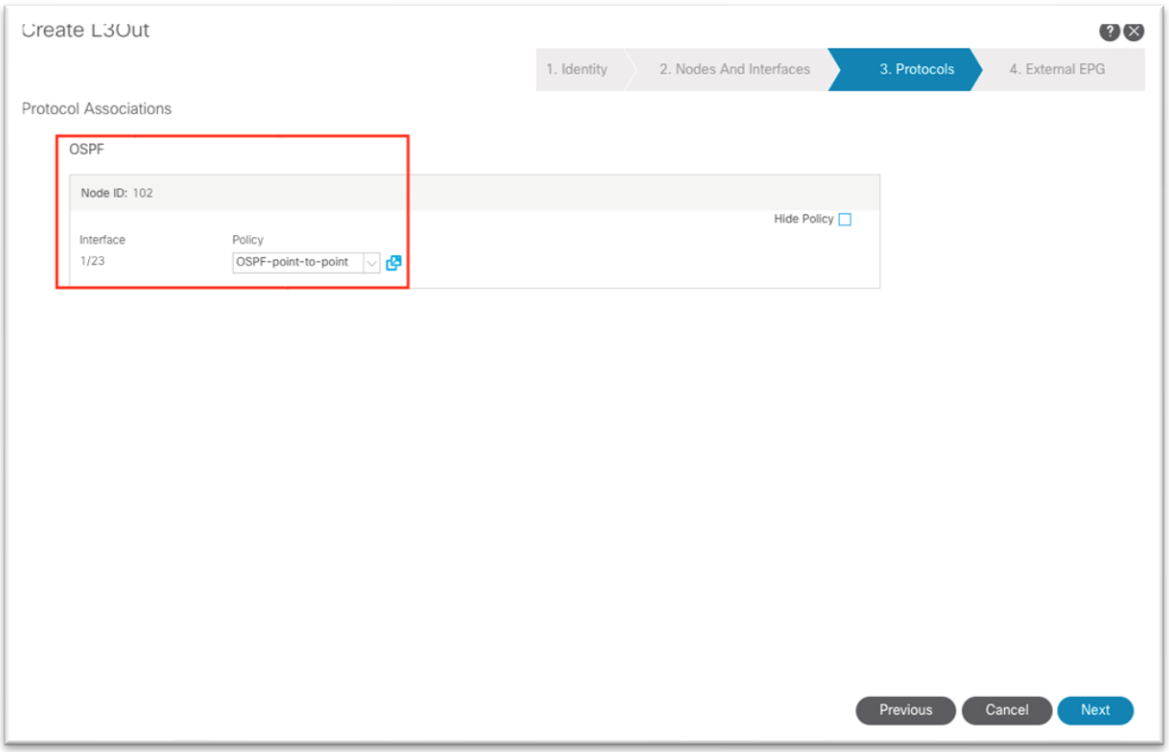
g. ノードを選択し、必要に応じてルータ ID とループバックを入力します。

h. インターフェイスを選択し、適切なパラメータを入力します。



i. [次へ（Next）] をクリックします。

j. ドロップダウン リストを使用して、適切なインターフェイス プロトコル ポリシーを選択します。

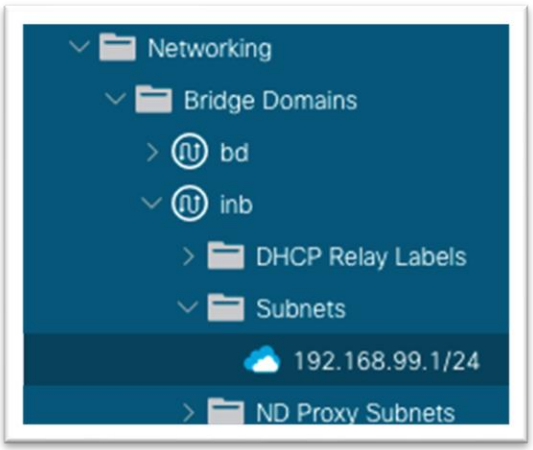


k. [次へ（Next）] をクリックします。

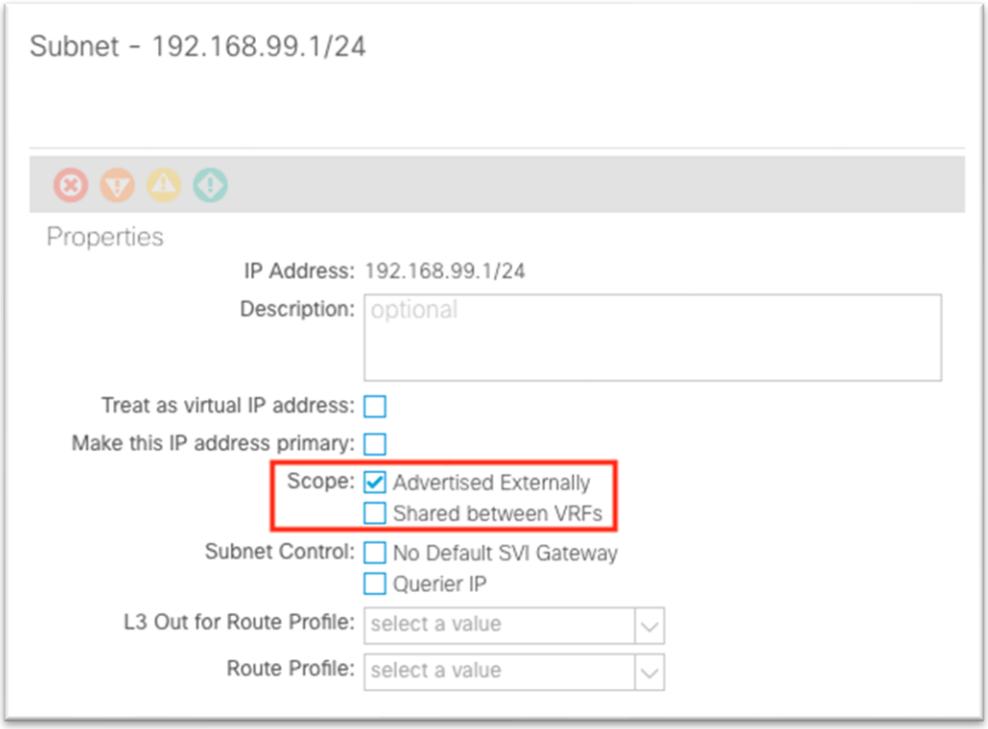
l. 外部 EPG の名前を入力します

m. [完了（Finish）] をクリックします。

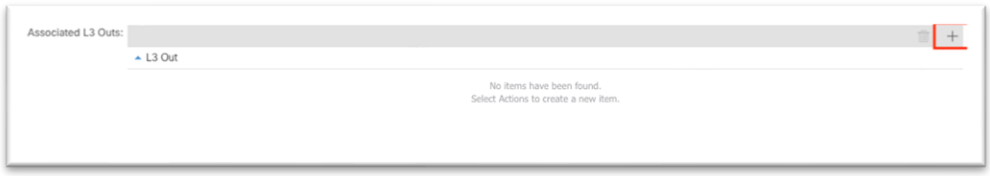
7. 管理テナントで、**[ネットワーキング（Networking）] > [ブリッジ ドメイン（Bridge Domains）] > [inb] > [サブネット（subnets）]** の順に移動し、定義したサブネットをクリックします。



8. 作業ウィンドウで、**[外部にアドバタイズメント（Advertised Externally）]** 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。



9. 「inb」という親ブリッジ ドメイン オブジェクトをクリックし、**作業ウィンドウで [ポリシー（Policy）] タブの [レイヤ 3 設定（Layer 3 Configurations）]** タブをクリックし、**[関連付けられた L3Outs（Associated L3Outs）]** の横にある **[+]** 記号をクリックします。



a. ドロップダウン リストから、前の手順で作成したL3Outを選択します。

b. [更新（Update）] をクリックします。

10. 引き続き管理テナントの下の場合は、**[コントラクト（Contracts）]** に移動し、フォルダを展開します。

11. **[標準（Standard）]** を右クリックし、新しい標準コントラクトを作成します。

12. ダイアログでコントラクトに名前を付けます。

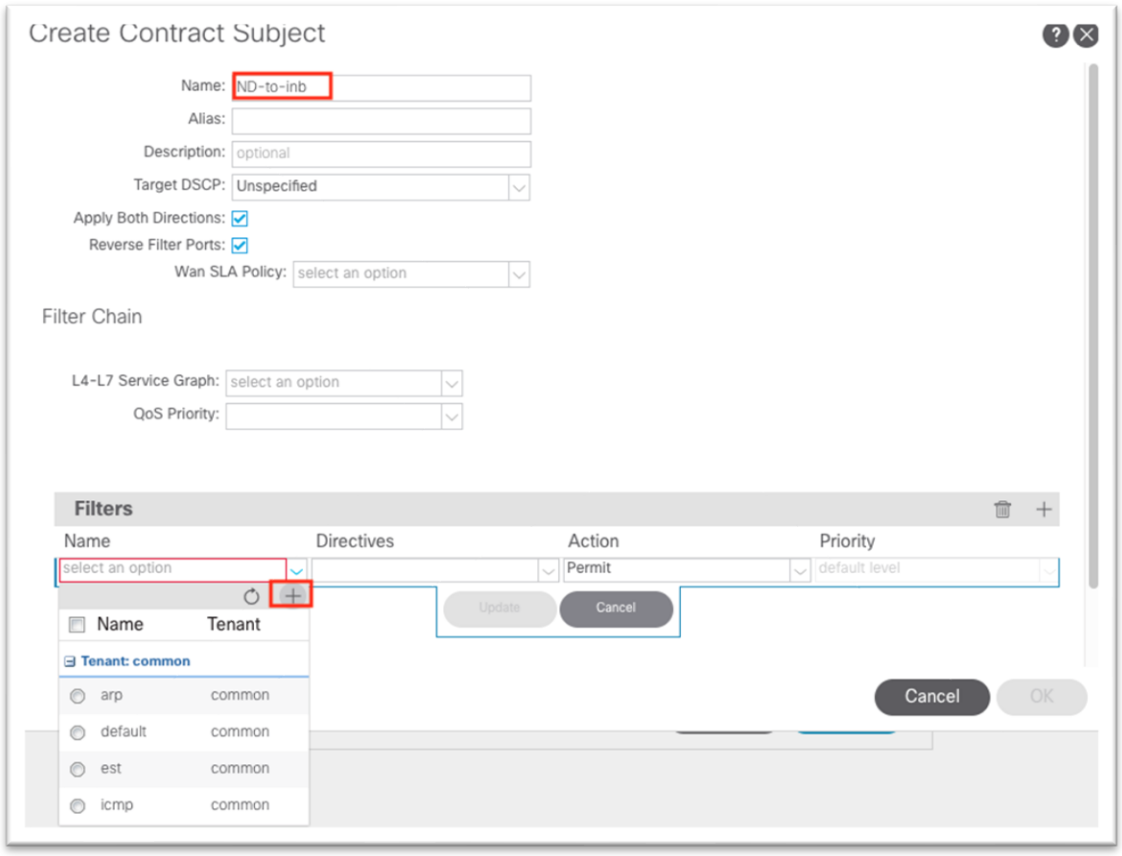
a. フローの観点から明確な名前を使用します。例：ND-to-inb。

b. **[+]** をクリックしてサブジェクトを作成します。

i. 新しいダイアログで、件名に名前を付けます。

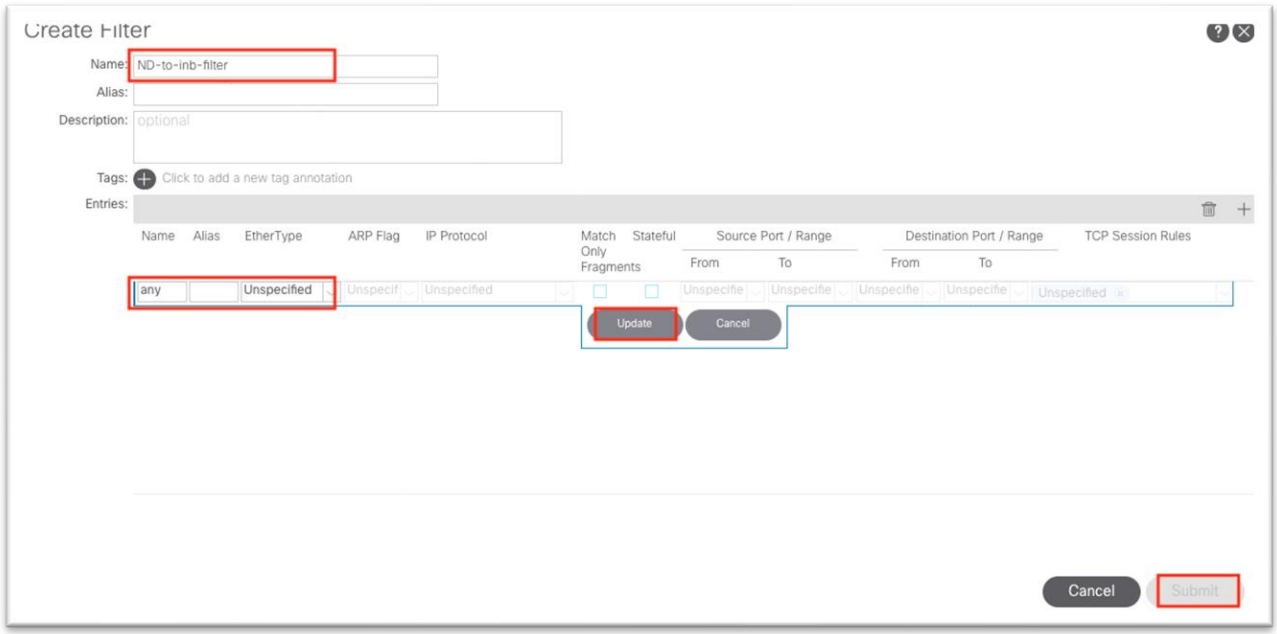
ii. **[+]** をクリックして新しいフィルタを作成します。

iii. **[名前（Name）]** の下にあるドロップダウン リストを展開し、**[+]** をクリックして新しいフィルタを作成します。



iv. 新しいダイアログで、フィルタに名前を付けます。

v. エントリの下の **[+]** をクリックします。



vi. エントリに名前を付けます。

vii. **[EtherType]** ドロップダウン リストでタイプを選択します。すべての通信を許可するには、値を **[未指定（Unspecified）]** のままにします。

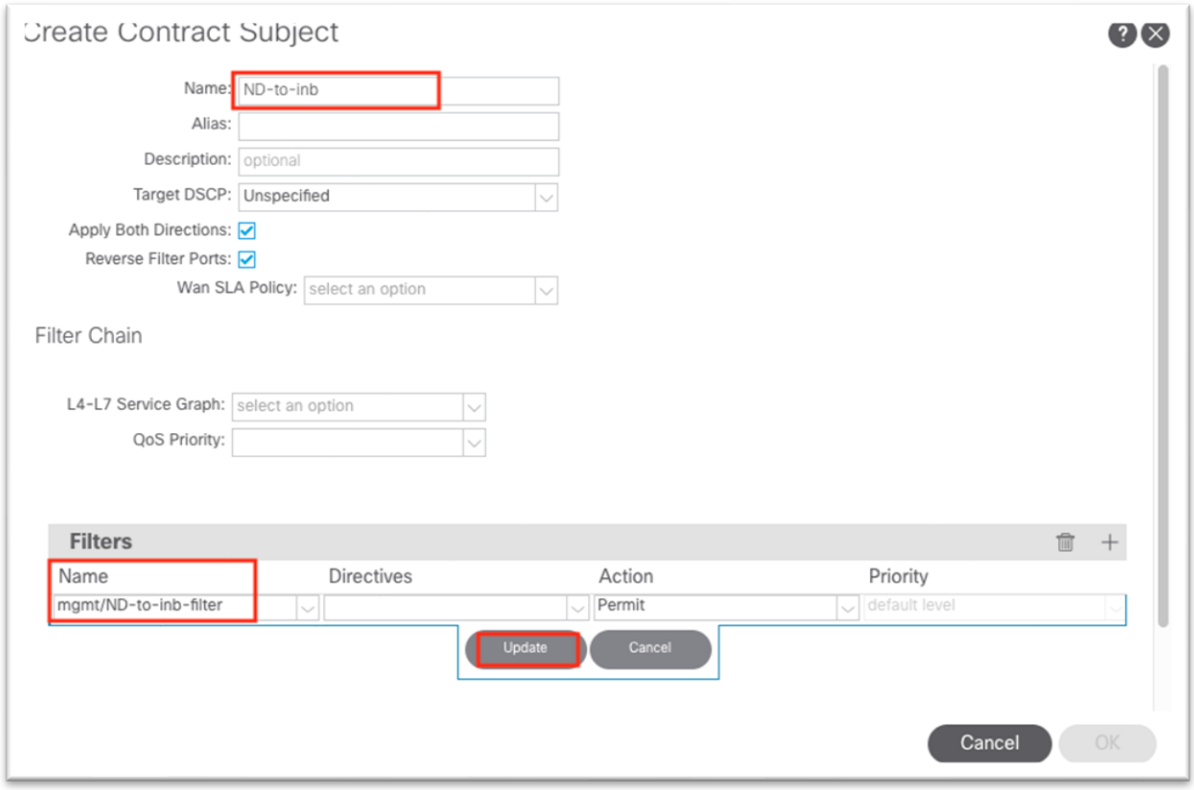
viii. IP プロトコルを選択します。

ix. 接続先ポートを入力します。

x. [更新（Update）] をクリックします。

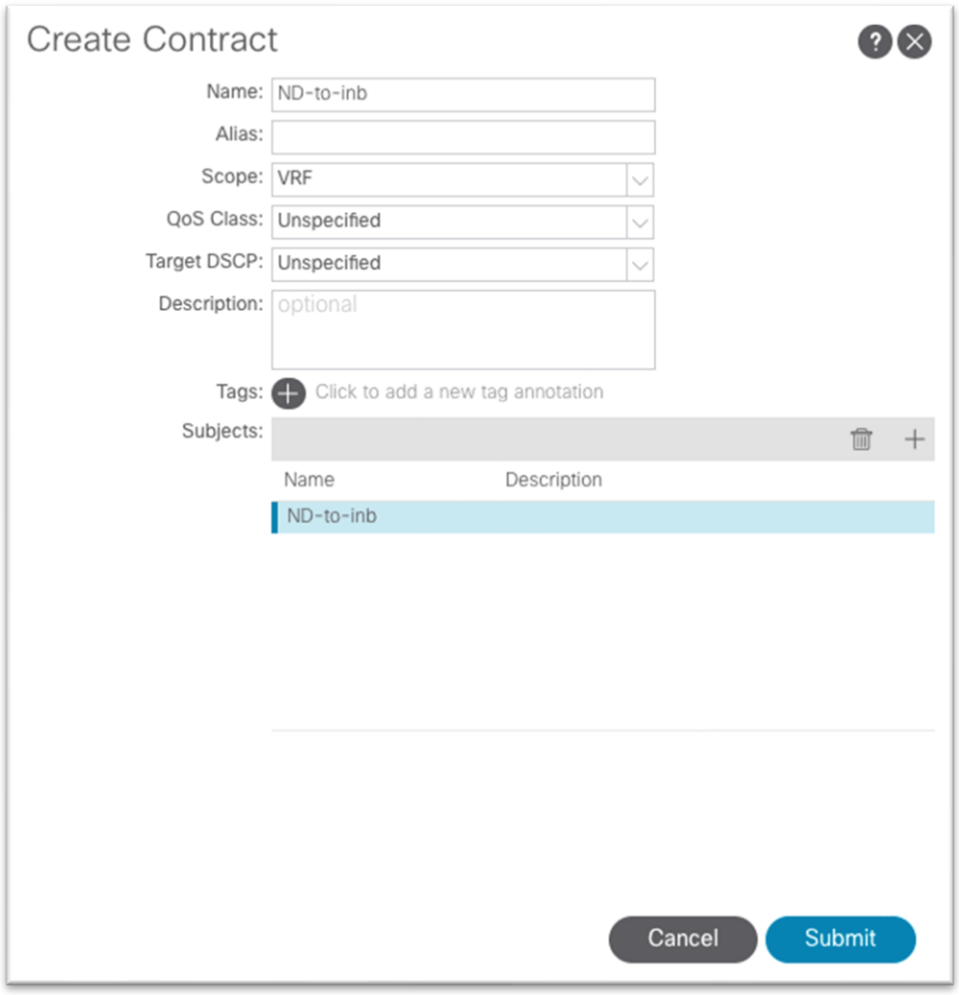
xi. **[フィルタの作成（Create Filter）]** ダイアログで **[送信（Submit）]** をクリックします。**[コントラクト件名の作成（Create Contract Subject）]** で新しいフィルタを選択する必要があります。

c. [更新（Update）] をクリックします。



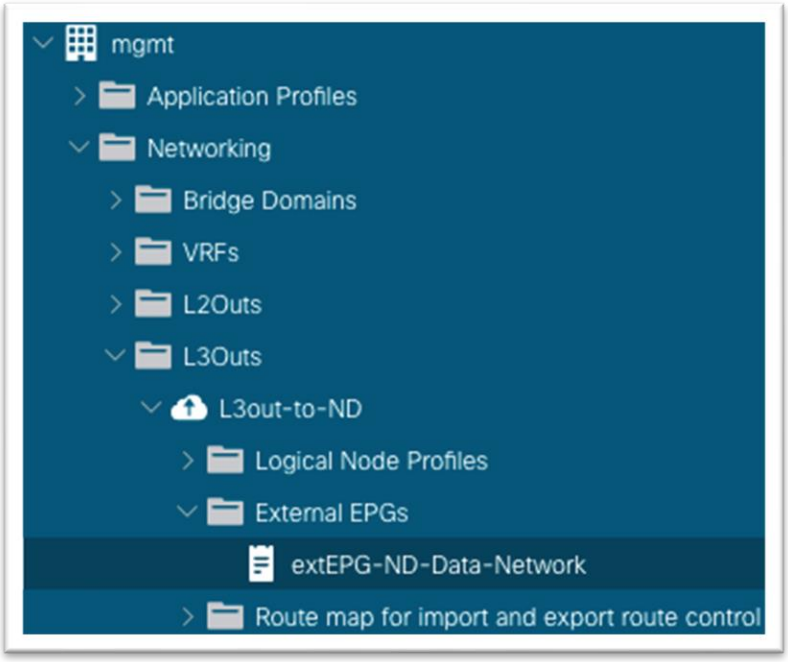
d. **[OK]** をクリックして件名を入力します。

e. 件名は **[コントラクトの作成（Create Contract）]** ダイアログの **[件名（Subjects）]** セクションに表示されます。

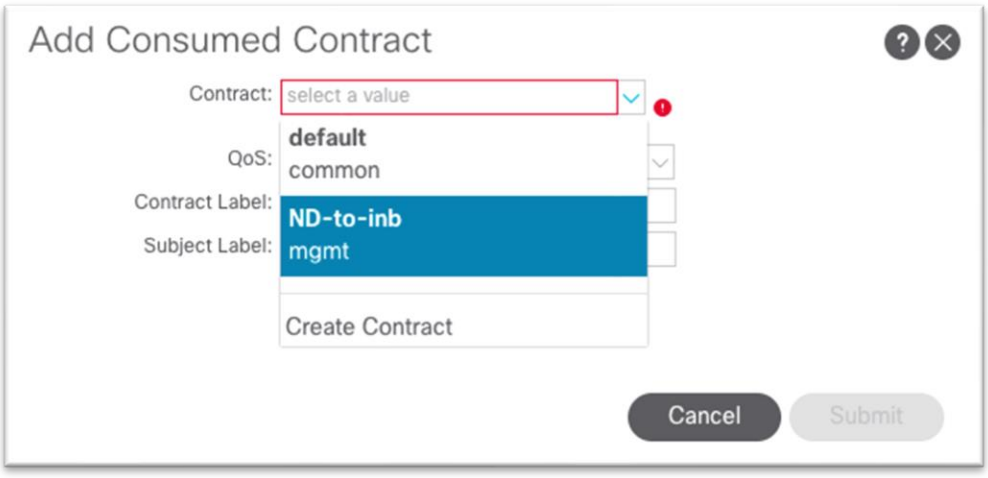


f. [送信（Submit）] をクリックします。

13. 管理テナントで、**[ネットワーキング（Networking）] > [L3Outs] > [your-L3Out] > [外部 EPG（External EPGs）]** の順に移動し、外部 EPG を選択します。



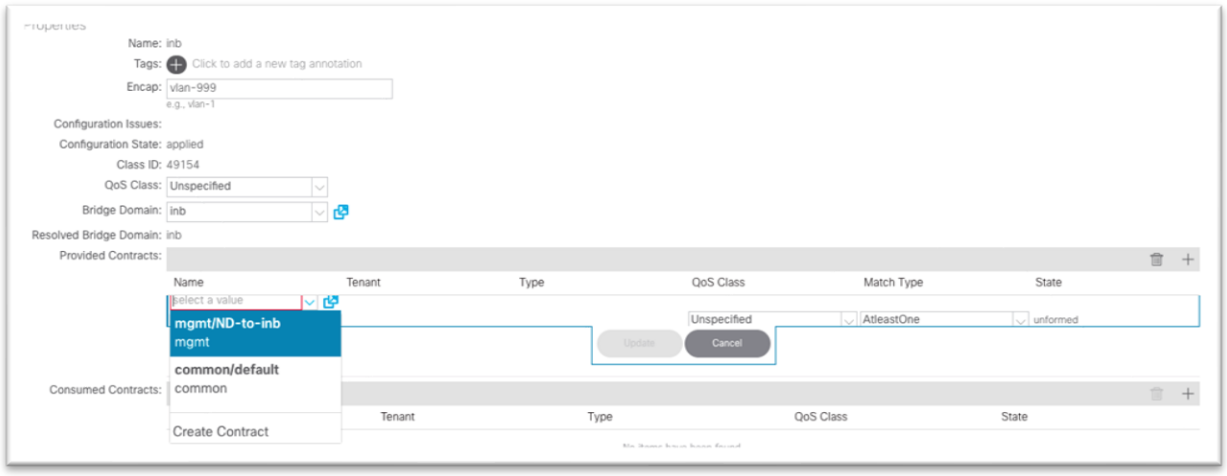
14. 作業ウィンドウで、**[コントラクト（Contracts）]** タブをクリックし、**[アクション（Action）]** ボタンをクリックして、**[消費したコントラクトの追加（Add Consumed Contract）]** を選択します。



a. **[送信（Submit）]** を選択します。

15. 管理テナントで、**[ノード管理 EPG（Node Management EPGs）]** に移動し、インバンド EPG を選択します。

16. **[指定したコントラクト（Provided Contracts）]** の下の **[+]** をクリックし、**[名前（Name）]** ドロップダウン リストで作成したコントラクトを選択します。



17. [更新（Update）] をクリックします。

これで、インバンド管理に向けた Cisco Nexus ダッシュボードの接続セクションが完了しました。

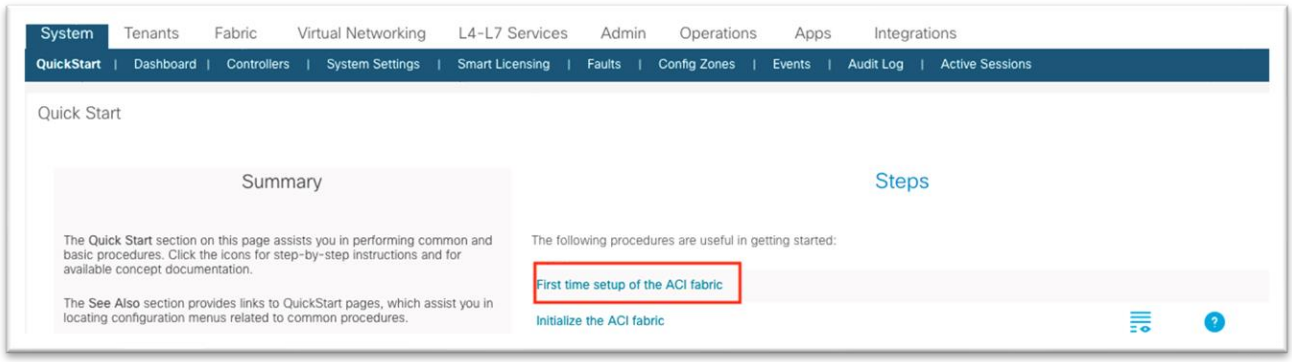
ネットワーク タイム プロトコル

ネットワーク タイム プロトコル（NTP）は、Cisco Nexus ダッシュボード Insights を使用するかどうかに関係なく有効にする必要があるコア Cisco ACI サービスです。Cisco APIC およびスイッチで NTP を有効にすると、ログ メッセージ、障害、イベント、およびデバッグ用の内部アトミック カウンタの一貫性が確保されます。これは、Cisco Nexus ダッシュボード Insights が情報を正しく関連付け、意味のある異常とその関係を示すために必要です。

[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] の下で日時ポリシーを設定して NTP を設定する従来の手順については、『**Cisco APIC 基本設定ガイド、リリース 5.2(x)-コア Cisco ACI ファブリック サービスのプロビジョニング**』を参照してください。次の手順では、新しいウィザードを使用して同じポリシーを設定します。

設定手順

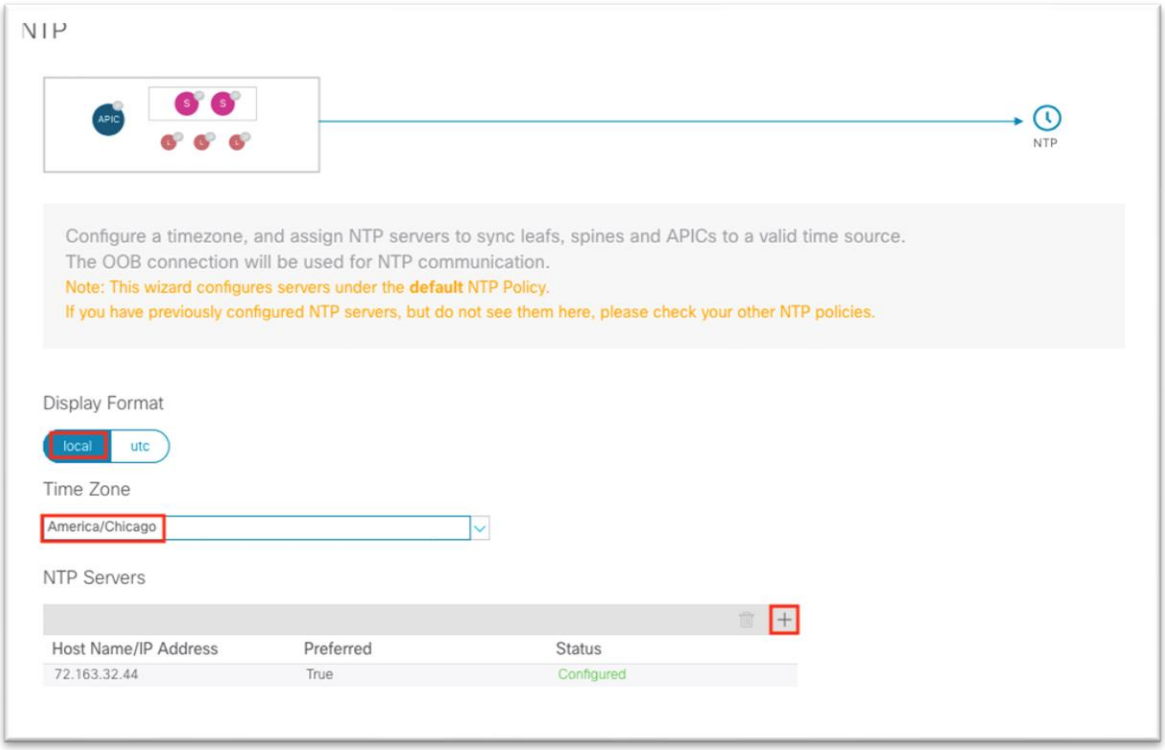
1. メイン メニューで **[システム（System）] > [クイック スタート（Quick Start）]** に移動し、**[ACI ファブリックの初回セットアップ（First time setup of the ACI Fabric）]** を選択します。



2. ダイアログの **[NTP]** で、**[設定の編集（Edit Configuration）]** または **[確認して設定（Review and Configure）]** を選択します（まだ設定されていない場合）。
3. このダイアログで以下を行います。
    a. Cisco APIC の表示形式の設定を選択します。

b. Cisco APIC のタイム ゾーンを選択します。

c. **[NTP サーバ（NTP Servers）]** で **[+]** をクリックして、このサイトで使用する NTP サーバの IP アドレスまたはホスト名を追加します。



d. [保存して続行（Save and Continue）] をクリックします。

4. **[サマリに進む（Proceed to Summary）]** をクリックし、**[閉じる（Close）]** をクリックします。

高精度時間プロトコル

Cisco Nexus ダッシュボード Insights のフロー分析がデータ センター ネットワーク サイトに対して有効になっており、フロー モニタリング ルールがプロビジョニングされている場合、サイト内のすべての Cisco Nexus 9000 シリーズ スイッチは、モニタ対象フローのフロー レコードを毎秒ストリーミングします。フロー レコードには、フローに関するメタデータのセットと高精度時間プロトコル（PTP）タイムスタンプがあります。ネットワーク内のスイッチからストリーミングされたフロー レコードを受信すると、Cisco Nexus ダッシュボード Insights はフロー分析および相関機能を実行して、個々のスイッチからのフロー データをまとめてエンドツーエンドのフローを形成します。フローごとに、Cisco Nexus ダッシュボード Insights は PTP タイムスタンプを使用してエンドツーエンドのフロー遅延を計算します。

フロー遅延計算を正しく機能させるには、ネットワーク スイッチで PTP を有効にし、正しく設定する必要があります。同じ PTP グランドマスターを使用する必要があります。

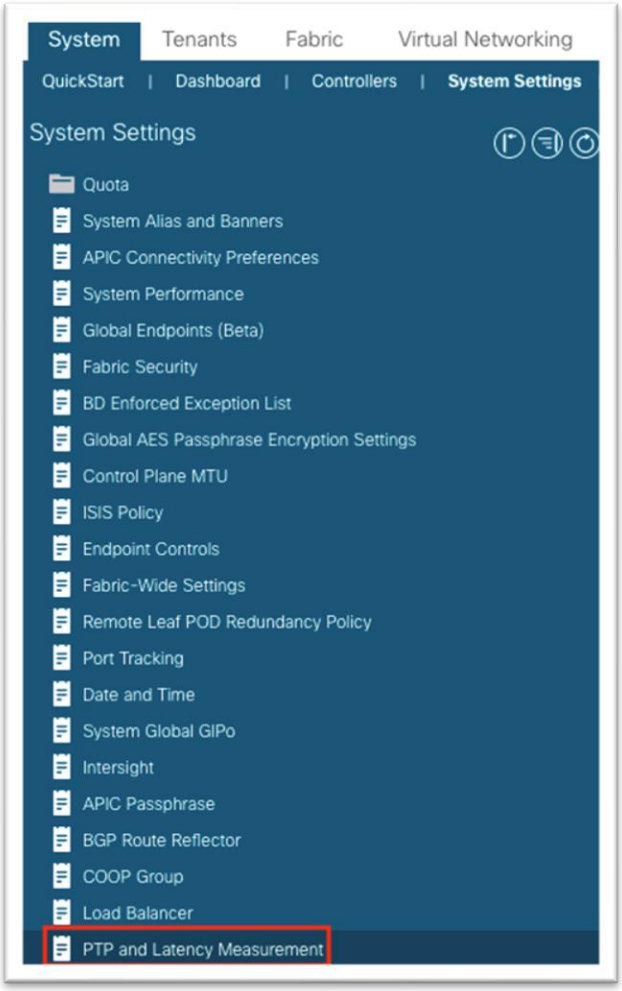
詳細については『Cisco APIC システム管理設定ガイド、リリース 5.1(x) - 正確なタイム プロトコル』を参照してください。

ポッドが 1 つだけの Cisco ACI ファブリックでは、外部グランドマスターを必要とせずに PTP を有効にできます。ファブリックは 1 つのスパイン スイッチをグランドマスターとして機能するように選択し、他のすべてのスイッチはこのグランドマスターに同期します。Cisco ACI マルチポッド ファブリックには外部グランドマスターが必要です。外部 IPN デバイスに接続することをお勧めします。これにより、アクティブなグランドマスターに到達するホップ数が等しくなります。EPG または L3Out を使用して、リーフ スイッチ ポートにグラン

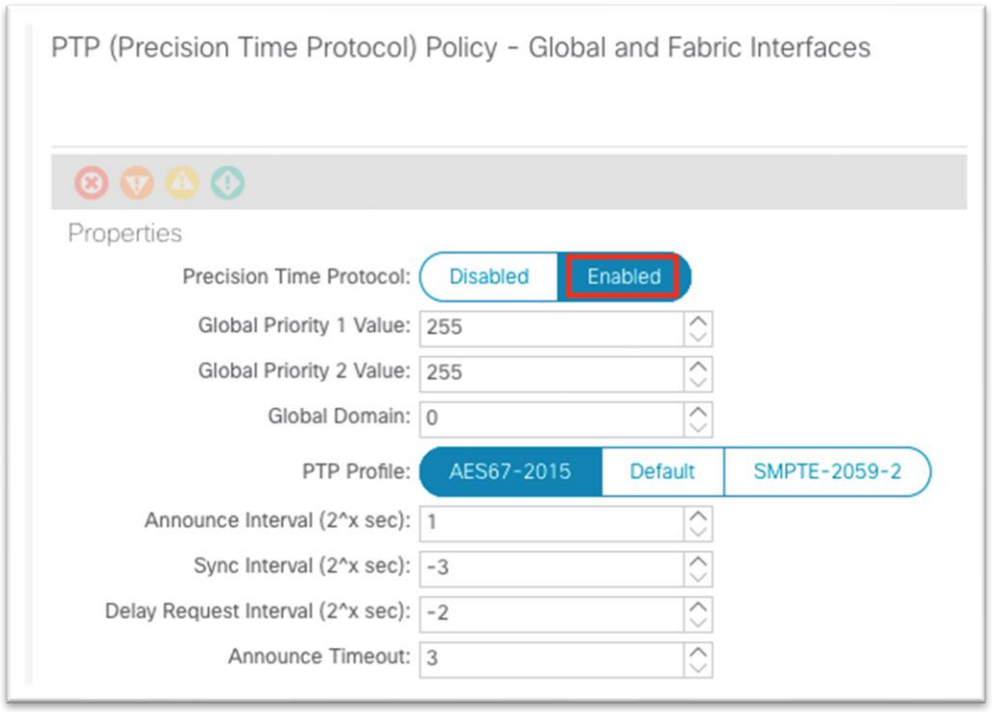
ドマスターを接続することもできます。これは、アクティブなグランドマスターがダウンした場合にグランドマスター候補として使用できます。

単一ポッド グランドマスター設定：

1. メイン メニューで、**[システム（System）] > [システム設定（System Settings）] > [PTP および遅延（PTP and Latency）]**（**[正確なタイム プロトコル（Precision Time Protocol）]** 設定）の順に移動します。



2. 作業ウィンドウの [正確なタイム プロトコル（Precision Time Protocol）] で、**[有効（Enabled）]** を選択します。



3. 下部にある **[送信（Submit）]** をクリックします。

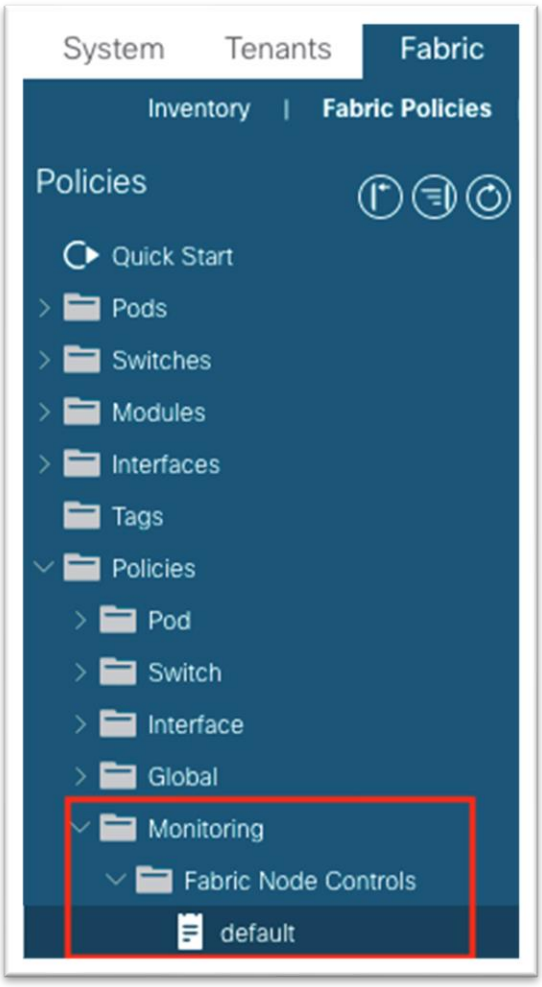
モニタリング ポリシー（ファブリック ノード制御ポリシー）

テレメトリ ポリシー

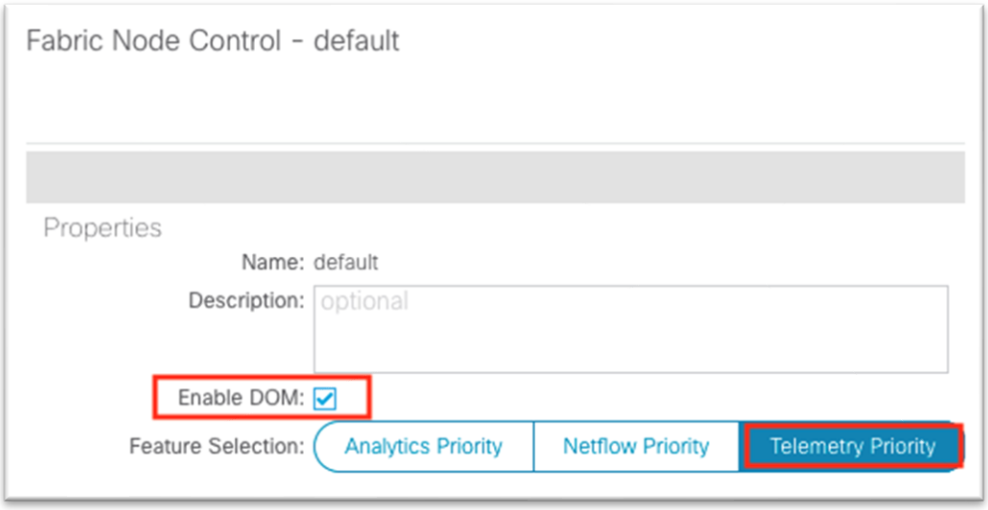
モニタリング ポリシーの詳細については、『Cisco APIC トラブルシューティング ガイド、リリース 4.2 (x)-DOM』を参照してください。

ファブリック ノード制御ポリシーは、デジタル オプティカル モニタリング（DOM）を有効にすると同時に、アナリティクス（Cisco Secure Workspace [Tetration]）、NetFlow、テレメトリ（Cisco Nexus Dashboard Insights）などのフロー収集機能を選択するために使用されます。これは、DOM の有効化に使用されるポリシーと同じです。このポリシーを適用するには、リーフおよびスパイン スイッチのファブリック レベルの スイッチ セレクタとポリシー グループを設定し、このファブリック ノードコントロール ポリシーを参照するポリシー グループを選択する必要があります。

1. **[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [ポリシー（Policies）] > [モニタリング（Monitoring）] > [ファブリック ノード制御（Fabric Node Controls）] > [デフォルト（default）]** に移動します。

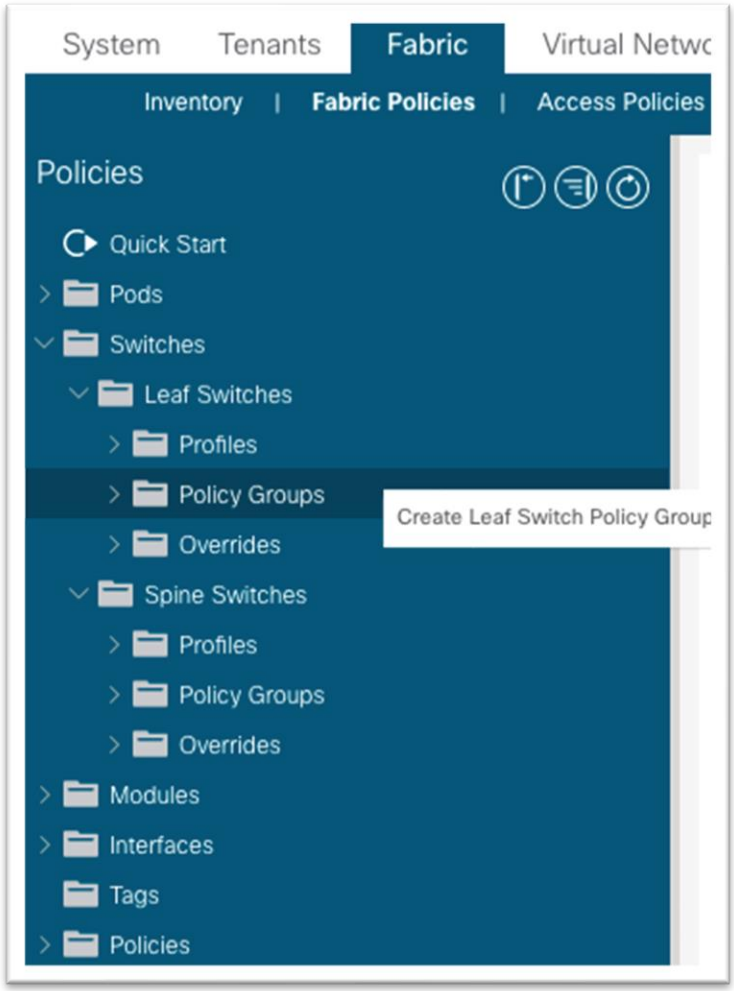


2. 作業ペインで、**[DOM の有効化（Enable DOM）]** チェックボックスをオンにします。
3. **[機能選択（Feature Selection）]** の場合 **[テレメトリの優先順位（Telemetry Priority）]** を選択します。

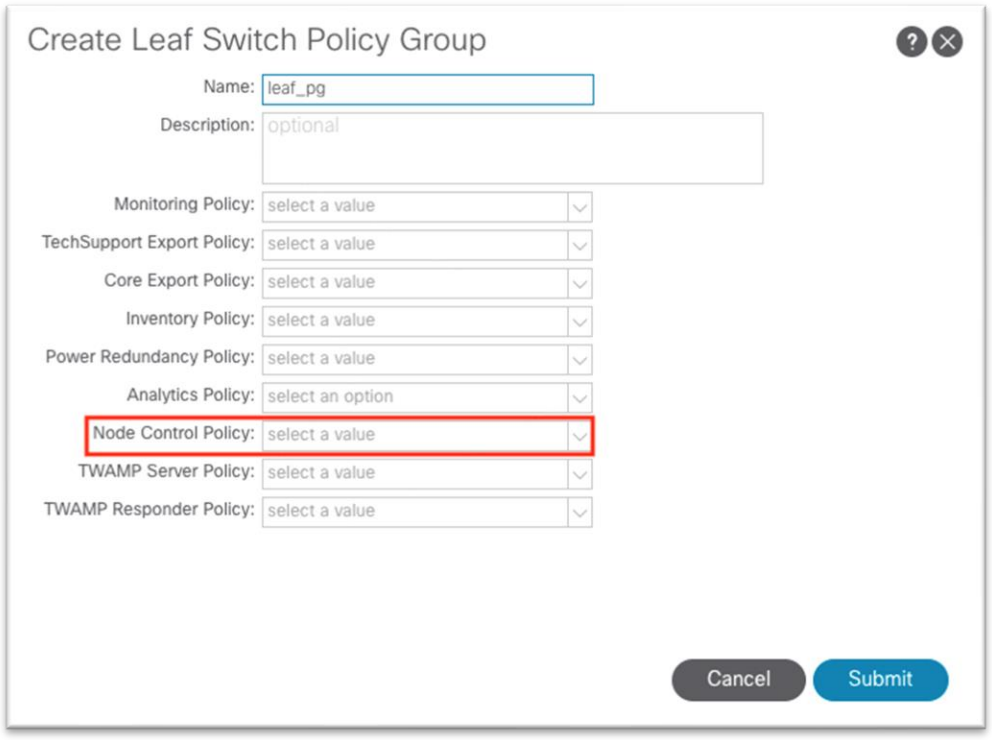


上記の手順を完了した後、は、使い慣れたプロファイル、セレクタ、およびポリシー グループの関連付けを使用してポリシーを適用する必要があります。ただし、今回は、インターフェイスではなくリーフ スイッチおよびスパイン スイッチにポリシーを適用します。まず、リーフ ポリシー グループを作成します。

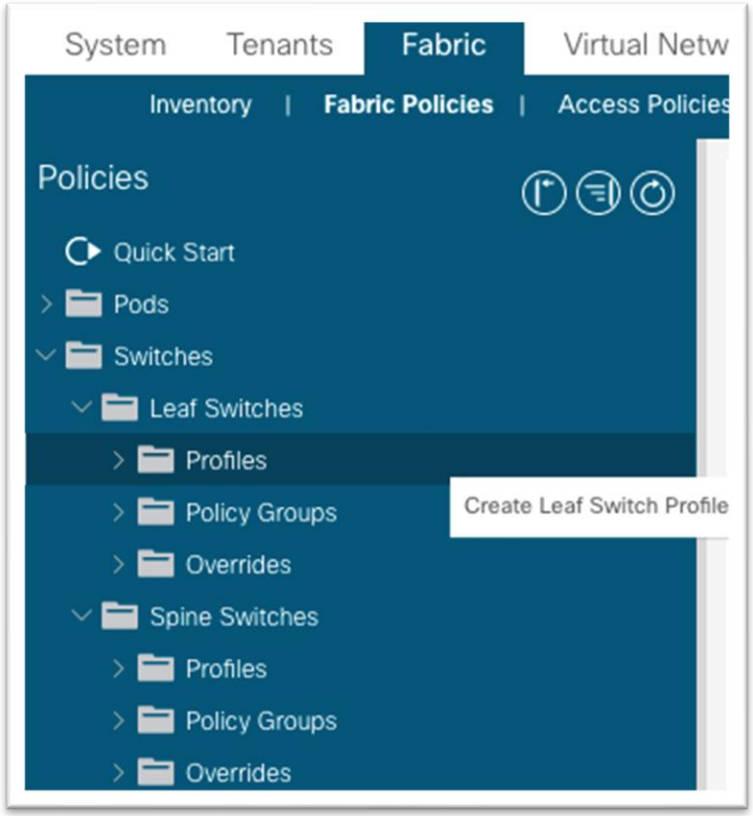
1. **[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [スイッチ（Switches）] > [リーフ スイッチ（Leaf Switches）] > [ポリシー グループ（Policy Groups）]** に移動します。
2. **[ポリシー グループ（Policy Groups）]** を右クリックし、**[作成（Create）] [リーフ スイッチ ポリシー グループ（Leaf Switch Policy Group）]** を選択します。



3. ダイアログで、ポリシー グループに名前を付けます。
    a. ノード制御ポリシーの場合、以前にカスタム ポリシーを作成した場合は、ここでそのポリシーを選択し、**[送信（Submit）]** をクリックします。
    b. それ以外の場合、何も選択されていない場合はデフォルトが使用されます。ポリシー グループを空白にしたまま **[送信（Submit）]** をクリックできます。

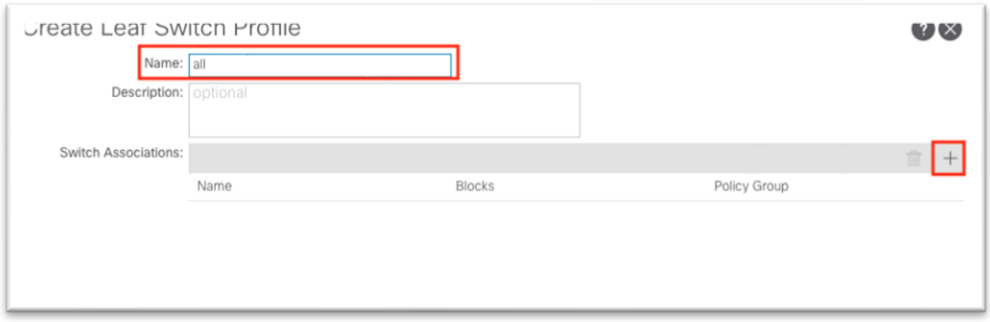


4. 次に、**[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [スイッチ（Switches）] > [リーフ スイッチ（Leaf Switches）] > [プロファイル（Profiles）]** でプロファイルを作成します。



5. ダイアログでプロファイルの名前を入力します。

a. **[スイッチの関連付け（Switch Associations）]** で、**[+]** 記号をクリックして行を追加します。



i. スイッチの関連付けに名前を付けます。

ii. ドロップダウン リストを使用して **[ブロック（Blocks）]** セクションでスイッチを選択し、チェックボックスをオンにしてすべてのリーフ スイッチを選択します。

iii. **[ポリシー グループ（Policy Group）]** ドロップダウン リストで、DOM およびテレメトリが有効になっているポリシー グループを選択します。

iv. [送信（Submit）] をクリックします。

これで、ポリシー グループがすべてのリーフ スイッチに適用されました。すべてのスパイン スイッチに対してこの手順を繰り返す必要があります。これには、ポリシー グループの作成とノード制御ポリシーの参照、スパイン スイッチ プロファイルの作成、スパイン スイッチのブロックへのポリシー グループの関連付けが含まれます。

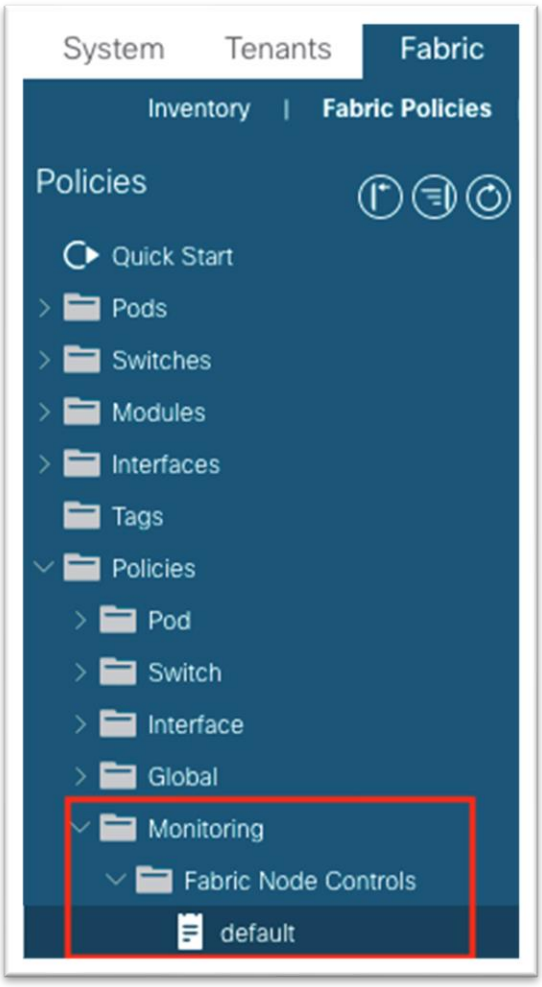
NetFlow ポリシー

モニタリング ポリシーの詳細については、『Cisco APIC トラブルシューティング ガイド、リリース 4.2 (x)-DOM』を参照してください。

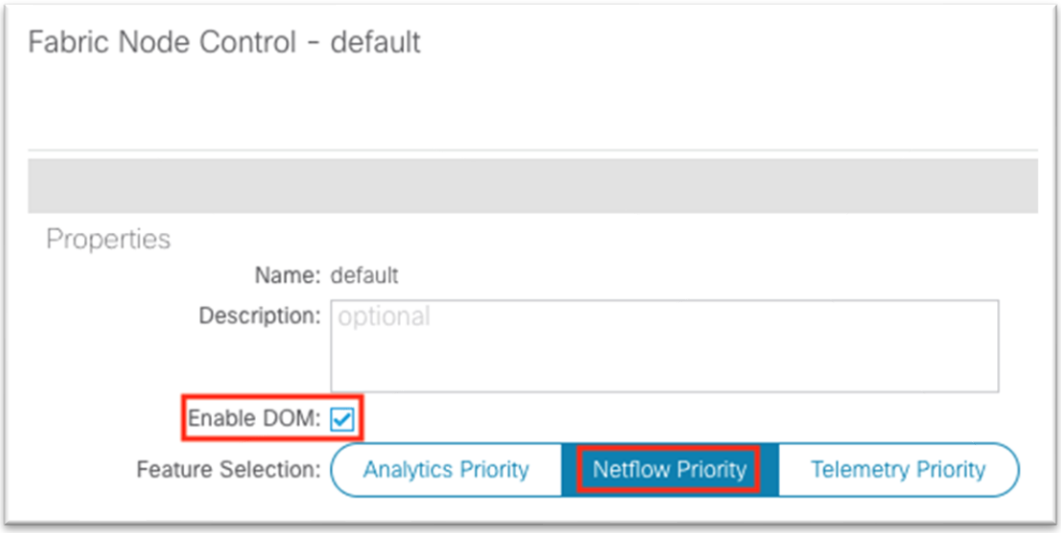
ファブリック ノード制御ポリシーは、デジタル オプティカル モニタリング（DOM）を有効にすると同時に、アナリティクス（Cisco Secure Workspace [Tetration]）、NetFlow、テレメトリ（Cisco Nexus Dashboard Insights）などのフロー収集機能を選択するために使用されます。これは、DOM の有効化に使用されるポリシーと同じです。このポリシーを適用するには、リーフおよびスパイン スイッチのファブリック レベルの スイッチ セレクタとポリシー グループを設定し、このファブリック ノードコントロール ポリシーを参照するポリシー グループを選択する必要があります。

Cisco Nexus ダッシュボード Insights および NetFlow サポートの詳細については、『Cisco Nexus ダッシュボード Insights ユーザ ガイド』を参照してください。

1. **[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [ポリシー（Policies）] > [モニタリング（Monitoring）] > [ファブリック ノード制御（Fabric Node Controls）] > [デフォルト（default）]** に移動します。

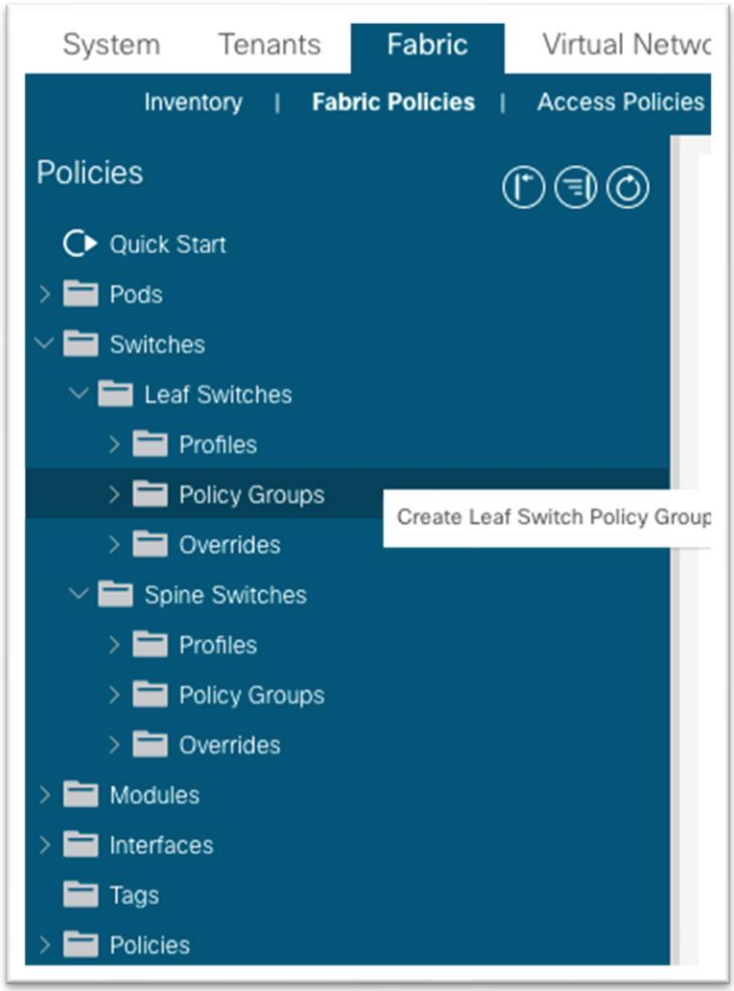


2. 作業ペインで、**[DOM の有効化（Enable DOM）]** チェックボックスをオンにします。
3. **[機能選択（Feature Selection）]** の場合 **[テレメトリの優先順位（Telemetry Priority）]** を選択します。

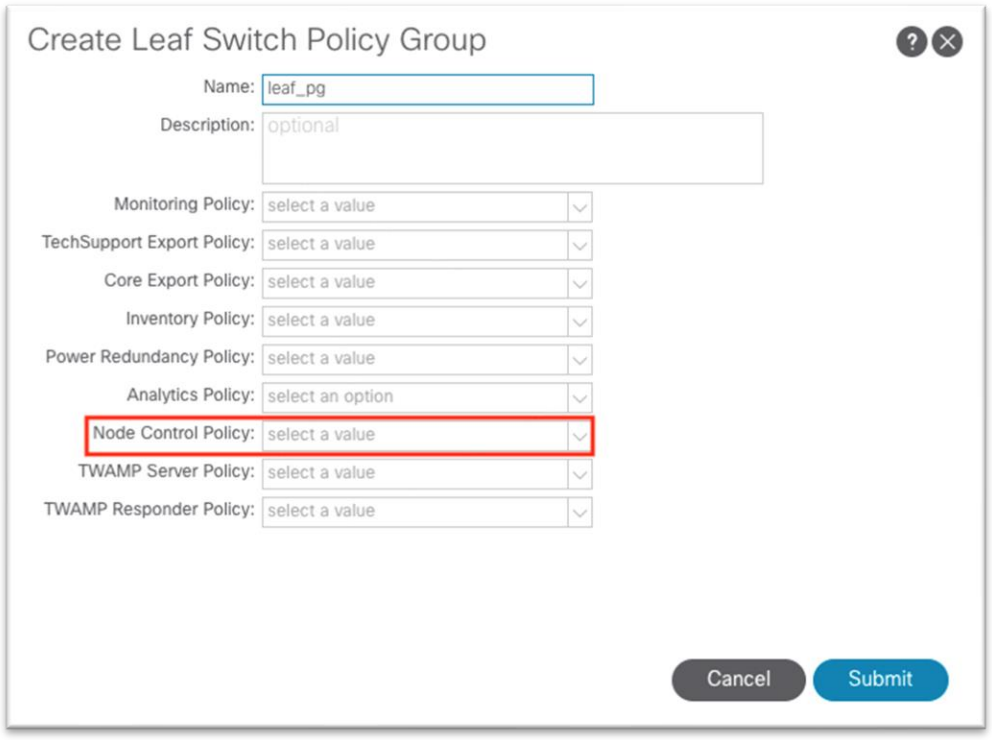


上記の手順を完了した後、は、使い慣れたプロファイル、セレクタ、およびポリシー グループの関連付けを使用してポリシーを適用する必要があります。ただし、今回は、インターフェイスではなくリーフ スイッチおよびスパイン スイッチにポリシーを適用します。まず、リーフ ポリシー グループを作成します。

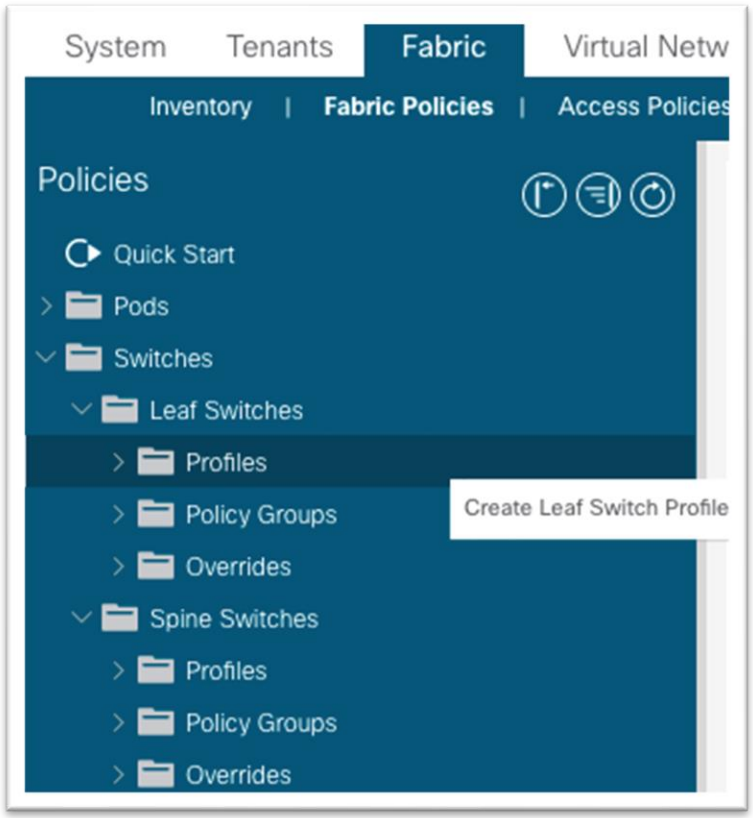
4. **[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [スイッチ（Switches）] > [リーフ スイッチ（Leaf Switches）] > [ポリシー グループ（Policy Groups）]** に移動します。
5. **[ポリシー グループ（Policy Groups）]** を右クリックし、**[作成（Create）] [リーフ スイッチ ポリシー グループ（Leaf Switch Policy Group）]** を選択します。



6. ダイアログでポリシー グループに名前を付けます。
    a. ノード制御ポリシーの場合、以前にカスタム ポリシーを作成した場合は、ここでそのポリシーを選択し、**[送信（Submit）]** をクリックします。
    b. もしくは、何も選択されていない場合デフォルトが使用されます。ポリシー グループを空白にしたまま **[送信（Submit）]** をクリックできます。

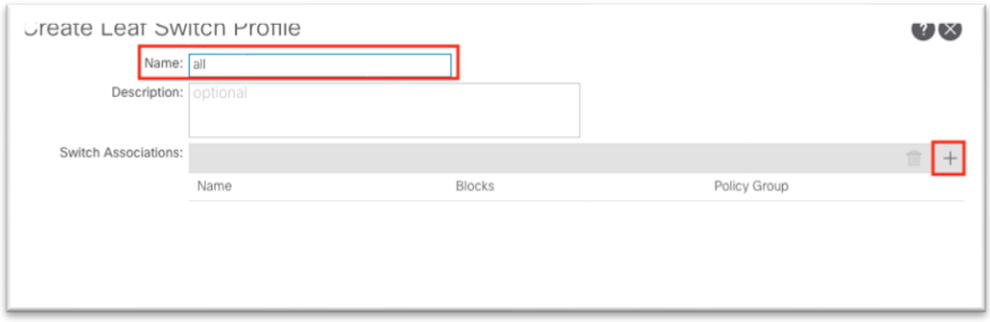


7. 次に、**[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [スイッチ（Switches）] > [リーフ スイッチ（Leaf Switches）] > [プロファイル（Profiles）]** でプロファイルを作成します。



8. ダイアログでプロファイルの名前を入力します。

a. **[スイッチの関連付け（Switch Associations）]** で、**[+]** 記号をクリックして行を追加します。



i. アソシエーションの名前を切り替えます。

ii. ドロップダウン リストを使用して **[ブロック（Blocks）]** セクションでスイッチを選択し、チェックボックスをオンにしてすべてのリーフ スイッチを選択します。

iii. **[ポリシー グループ（Policy Group）]** ドロップダウン リストで、DOM およびテレメトリが有効になっているポリシー グループを選択します。

iv. [送信（Submit）] をクリックします。

ポリシー グループはすべてのリーフ スイッチに適用されています。ステップをすべてのスパイン スイッチに繰り返します。これには、ポリシー グループの作成とノード制御ポリシーの参照、スパイン スイッチ プロファイルの作成、スパイン スイッチのブロックへのポリシー グループの関連付けが含まれます。

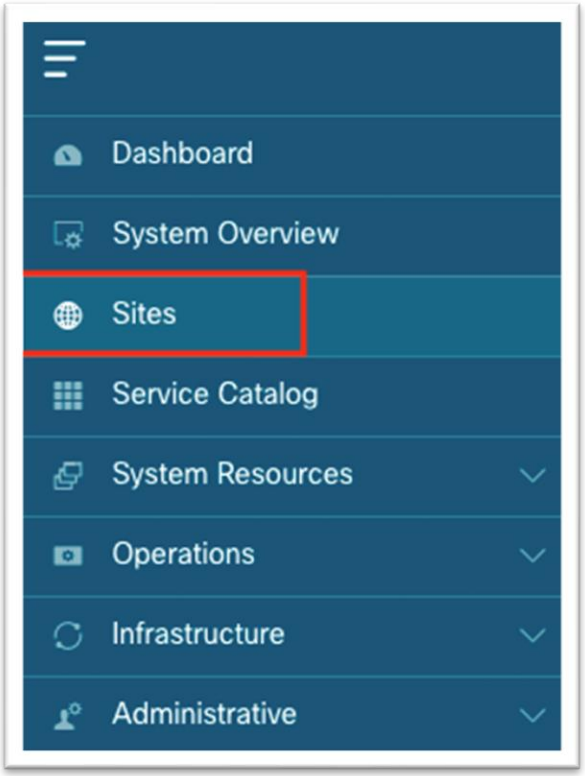
Cisco Nexus ダッシュボードの設定

Cisco Nexus ダッシュボードへの Cisco ACI サイトの追加

この操作は、メニュー バーの **[サイト（Sites）]** オプションを選択して、Cisco Nexus ダッシュボードで実行します。サイトを Cisco Nexus ダッシュボードに追加するときに、以前に設定したノード管理インバンド EPG の名前を入力する必要があります。

Cisco Nexus ダッシュボードおよび Cisco Nexus ダッシュボード Insights の詳細については、『Cisco Nexus ダッシュボード展開ガイド - ファブリックの接続性』および『Cisco Nexus ダッシュボード Insights ユーザ ガイド - インストールおよびセットアップ』を参照してください。

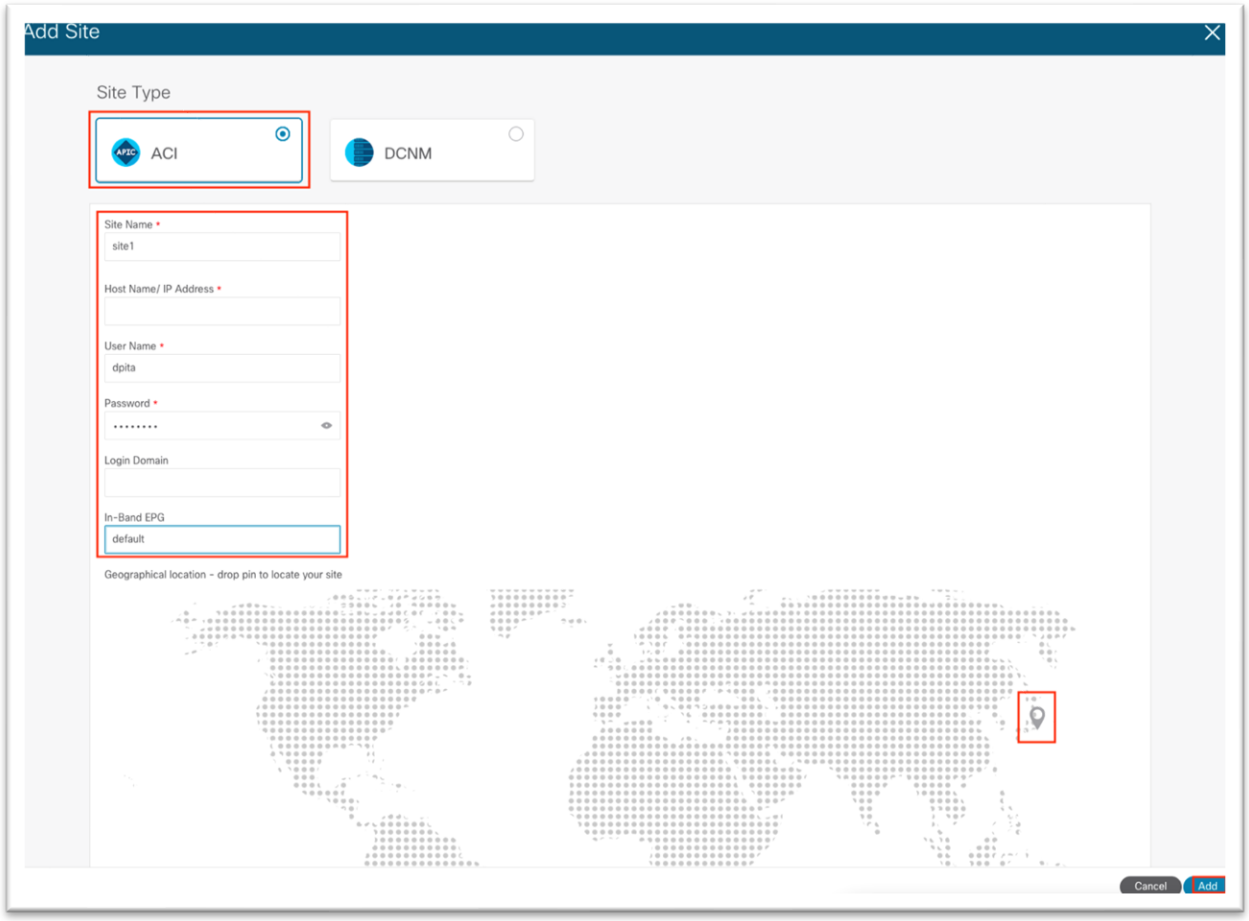
1. ブラウザを使用して、Cisco Nexus ダッシュボード GUI へのセッションを開きます。
2. 左側のメニューで、**[サイト（Sites）]** を選択します。



3. 作業ペインで、**[アクション（Actions）] > [サイトの追加（Add Site）]** を選択します。

4. 新しい画面で、Cisco ACI がサイト タイプとして選択されていることを確認します。
    a. このサイトの名前を入力します。この名前は、Cisco Nexus ダッシュボード Orchestrator や Cisco Nexus Insights などの他のすべてのサービスに引き継がれます。
    b. Cisco APIC のインバンド IP アドレスを入力します。
    c. Cisco APIC に対する認証用のユーザ名を入力します。
    d. 指定したユーザ名のパスワードを入力します。このパスワードは、最初の接続に一度だけ使用されます。その後、Cisco APIC と Cisco Nexus ダッシュボード間で、後続のすべての操作で証明書ベースの認証が使用されます。
    e. ユーザ名のログイン ドメインを指定します。
    f. ノード管理インバンド EPG 名を入力します。
    g. マップにピンをドロップします。

h. 右下隅にある **[追加（Add）]** をクリックします。

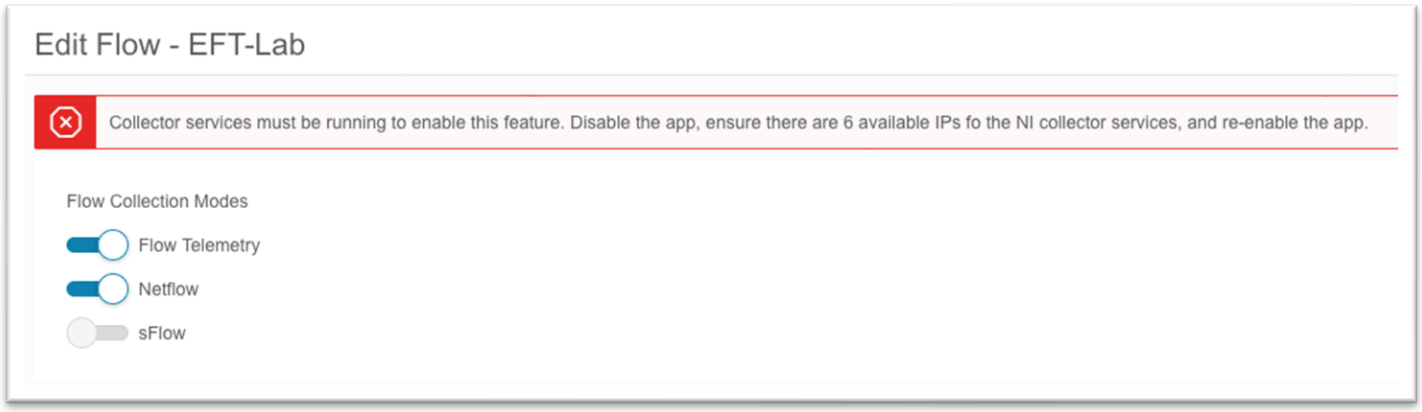


（オプション）外部サービスプールの設定：NetFlow に必要

外部サービス プールは、特定のサービスに使用される永続的な IP アドレスを設定するために使用されます。これらの永続的な IP アドレスは、バックエンド サービスが別の Cisco Nexus ダッシュボード ノードに再配置されても保持されます。詳細については、『Cisco Nexus ダッシュボード ユーザ ガイド』を参照してください。

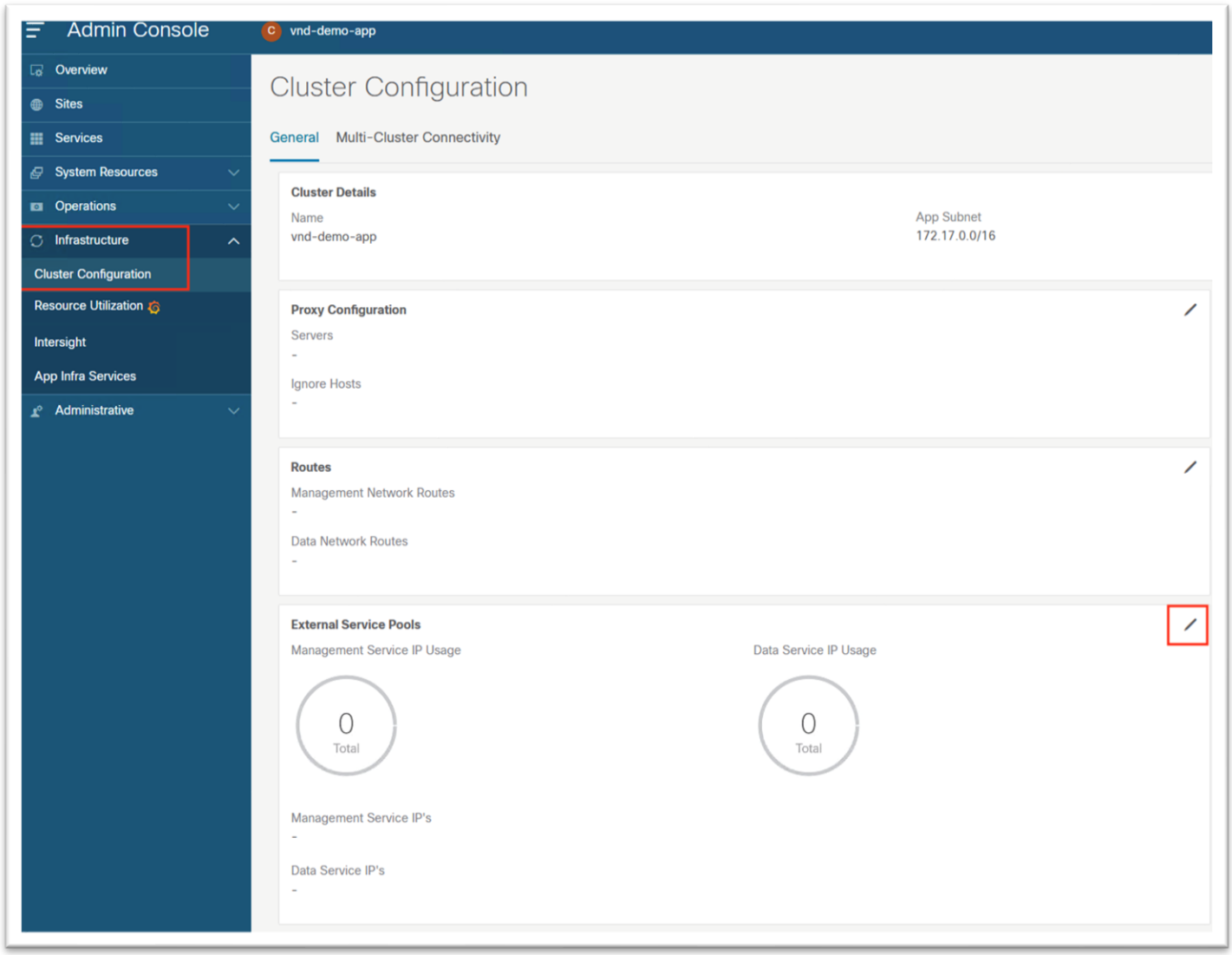
外部サービス プールは NetFlow に必要であり、NetFlow モニタリング ポリシーでフロー エクスポータをプログラミングするときに使用されます。

注：外部サービス プールが作成される前に Cisco Nexus ダッシュボード Insights がすでに実行されている場合、変更を有効にするには、Cisco Nexus ダッシュボード Insights を無効にしてから再度有効にする必要があります。

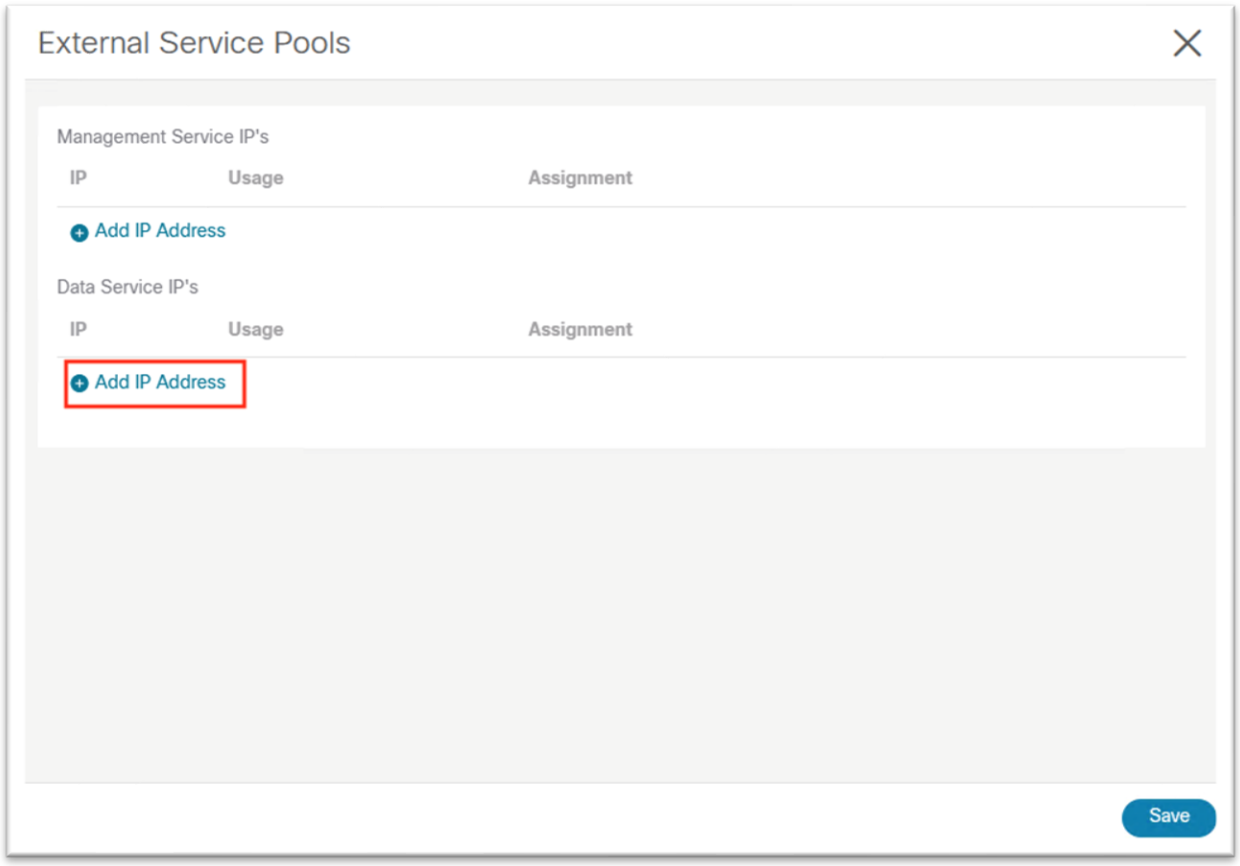


ここでは、Cisco Nexus ダッシュボードで外部サービス プールを設定する手順の概要を示します。詳細なステップはこのマニュアルで後に記載されています。

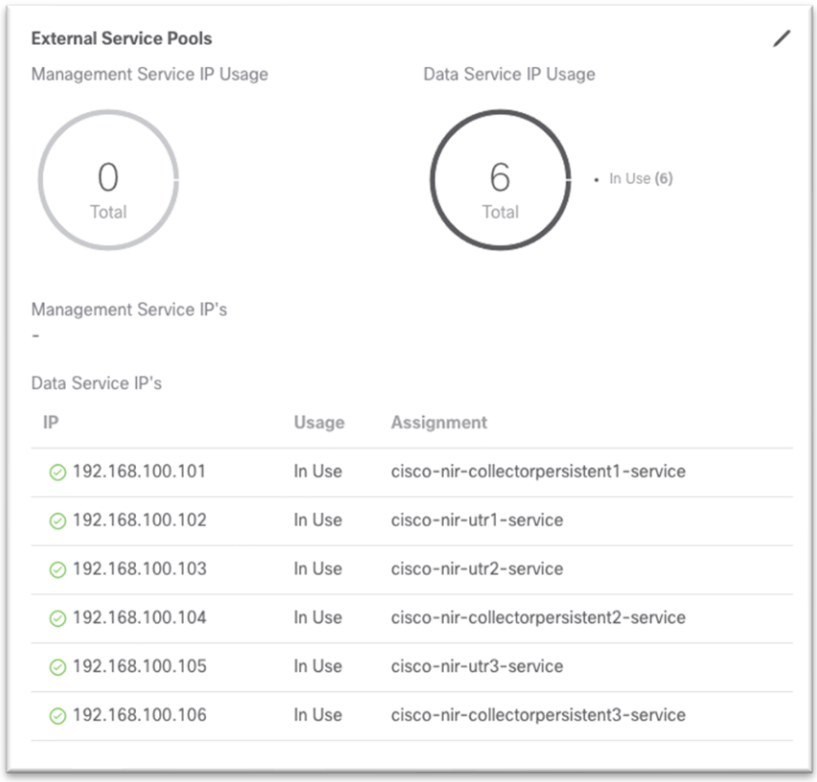
1. ブラウザを使用して、Cisco Nexus ダッシュボード GUI へのセッションを開きます。
2. 左側のメニューで、**[インフラストラクチャ（Infrastructure）] [クラスタ設定（Cluster Configuration）]** を選択します。
3. [外部サービス プール（External Service Pool）] タイルで、鉛筆アイコンをクリックして外部サービス プールを編集します。



4. ポップアップの [データ サービス IP（Data Serivce IP's）] で、**[IP アドレスの追加（Add IP Address）]** をクリックします。



5. テキスト ボックスに IP アドレスを入力し、緑色のチェックマークをクリックしてエントリを保存します。
6. **[IP アドレスの追加（Add IP Address）]** をもう一度クリックし、6 つのデータ サービス IP アドレスを設定するまでプロセスを繰り返します。これらの IP アドレスは、サービスによってランダムに要求されます。



Cisco Nexus ダッシュボード Insights セットアップ

Cisco Nexus ダッシュボードの Insights セットアップは、Cisco Nexus ダッシュボードに登録されているサイトを有効にするために使用されます。

Cisco Nexus ダッシュボード Insightsを最大限に活用するには、次の主要機能を有効にします。

- ソフトウェア分析：スイッチおよび Cisco APIC ソフトウェア分析をCisco Nexus ダッシュボード Insights にストリーミングして、さらに処理、相関、および異常を検出します。これを **[有効（Enabled）]** に設定します。
- フロー分析：ルールを設定し、スイッチでフロー メタデータを Cisco Nexus ダッシュボード Insights にエクスポートします。これを **[有効（Enabled）]** に設定します。
- [マイクロバースト感度（Microburst Sensitivity）]：しきい値のパーセンテージに基づいて、この設定は低、中、または高に設定できます。

Cisco Nexus ダッシュボード Insights 6.0 リリースでは、次の新機能が追加されました。

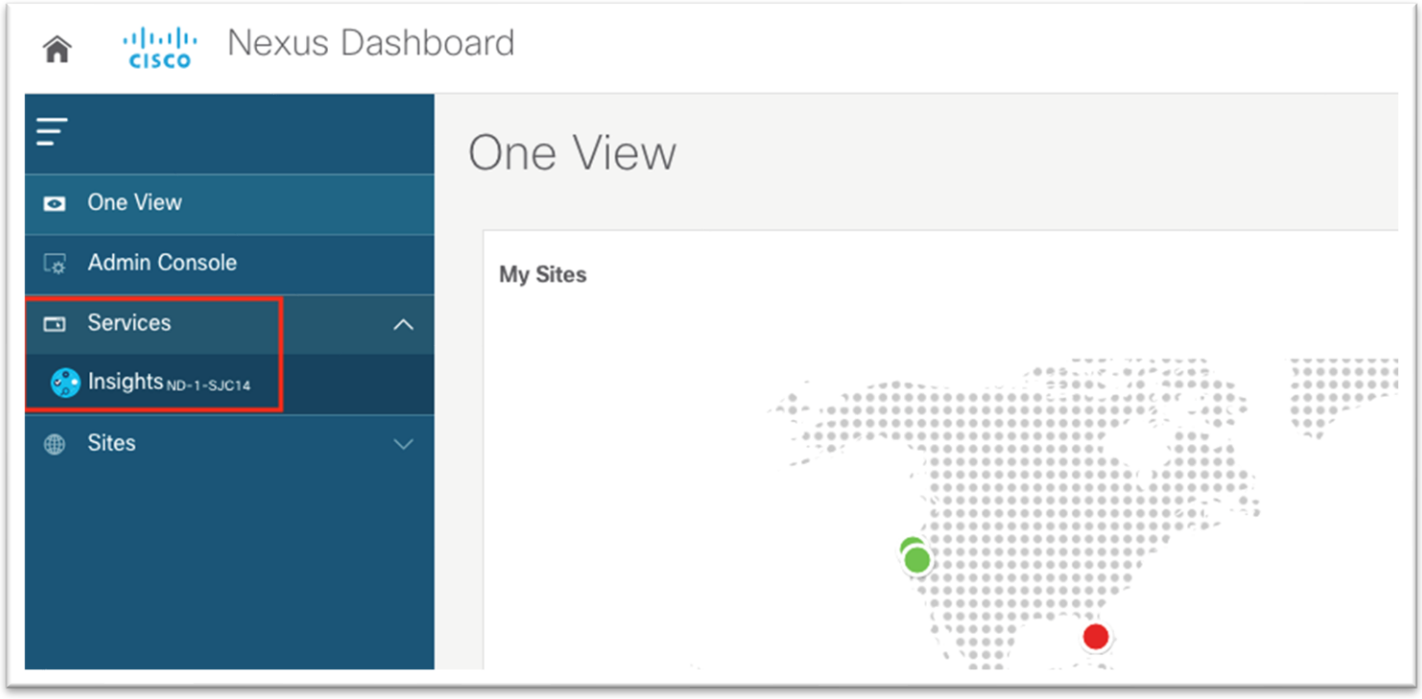
- 複数のサイトを 1 つのサイト グループにグループ化して、関連サイトを全体的に表示できるようになりました。
- バグ スキャンは、シスコ クラウドからダウンロードされた既知の障害についてファブリックをチェックするために、定期的に実行するように有効化できます。
- 保証分析：インテント、ポリシー、およびハードウェアの状態を含むネットワーク ファブリックの詳細なスナップショットを定期的に取得するために使用されます。これらのスナップショットは、差分分析や変更前の分析に使用したり、検索機能で自然言語クエリを使用してモデルをクエリしたりできます。

- アラート ルールを設定して、異常をよりきめ細かく制御し、初期状態を確認応答に設定したり、推奨をカスタマイズしたりできます。
- コンプライアンス要件を有効にして、スナップショットの通信または設定チェックを行い、ビジネス要件と運用要件が既知の標準に準拠していることを確認できます。

Cisco Nexus ダッシュボード Insights 6.x サイト グループの設定手順：

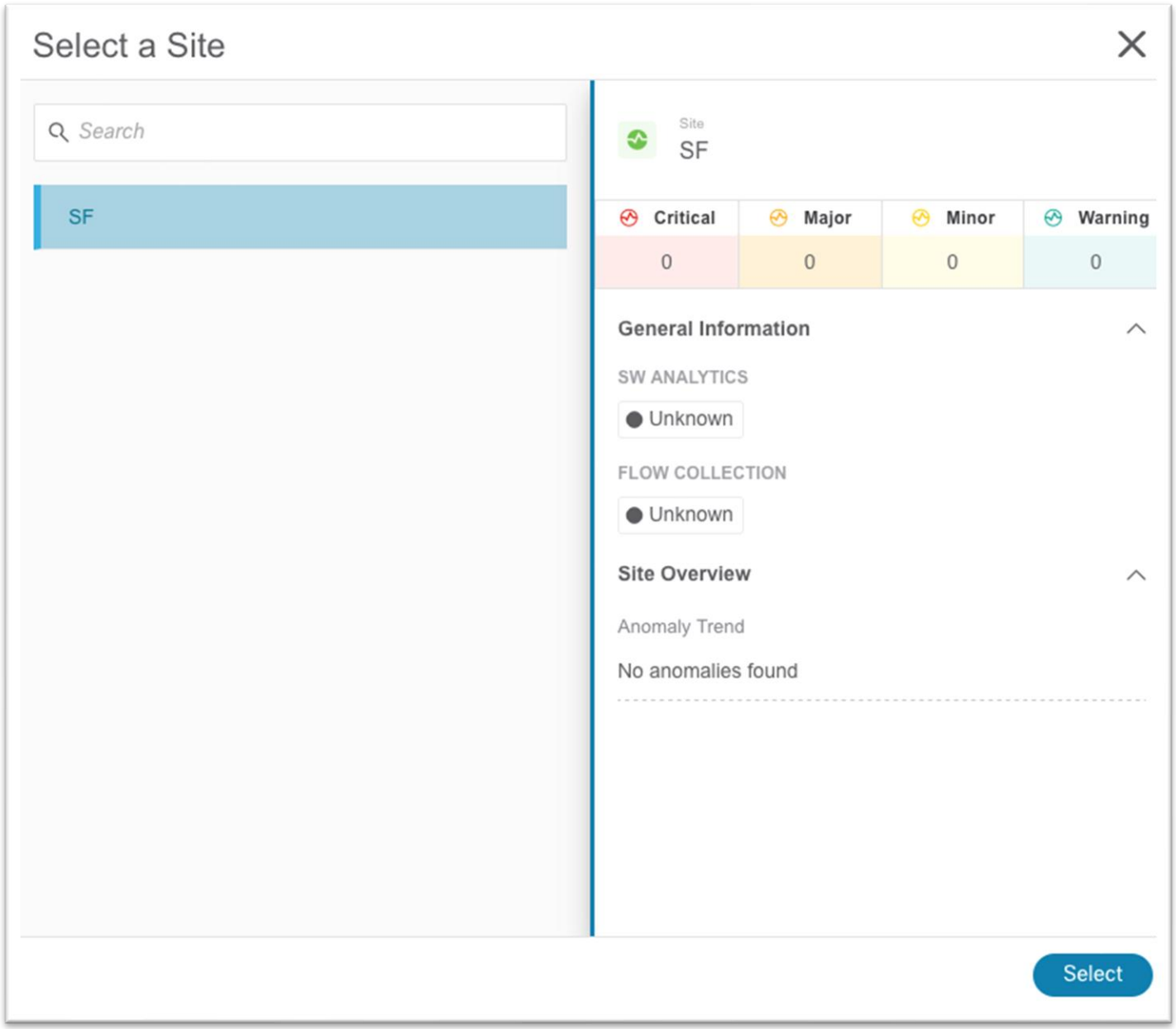
このセクションでは、Cisco Nexus ダッシュボード Insights リリース 6.0 でサイトを有効にするための大まかな手順について説明します。サイト グループの作成または既存のサイト グループへのサイトの追加に関する詳細な手順は、このドキュメントの範囲外です。Cisco Nexus ダッシュボード Insights の設定の詳細については、『Cisco Nexus ダッシュボード Insights 6.x ACI ユーザ ガイド - インストールおよびセットアップ』および必要に応じて『Cisco Nexus ダッシュボード Insights 6.x 展開ガイド』を参照してください。

1. ブラウザを使用して、Cisco Nexus ダッシュボード GUI へのセッションを開きます。
2. 左側のメニューで、**[サービス（Services）]** を選択します。
3. メニューから **[Insights]** を選択します。

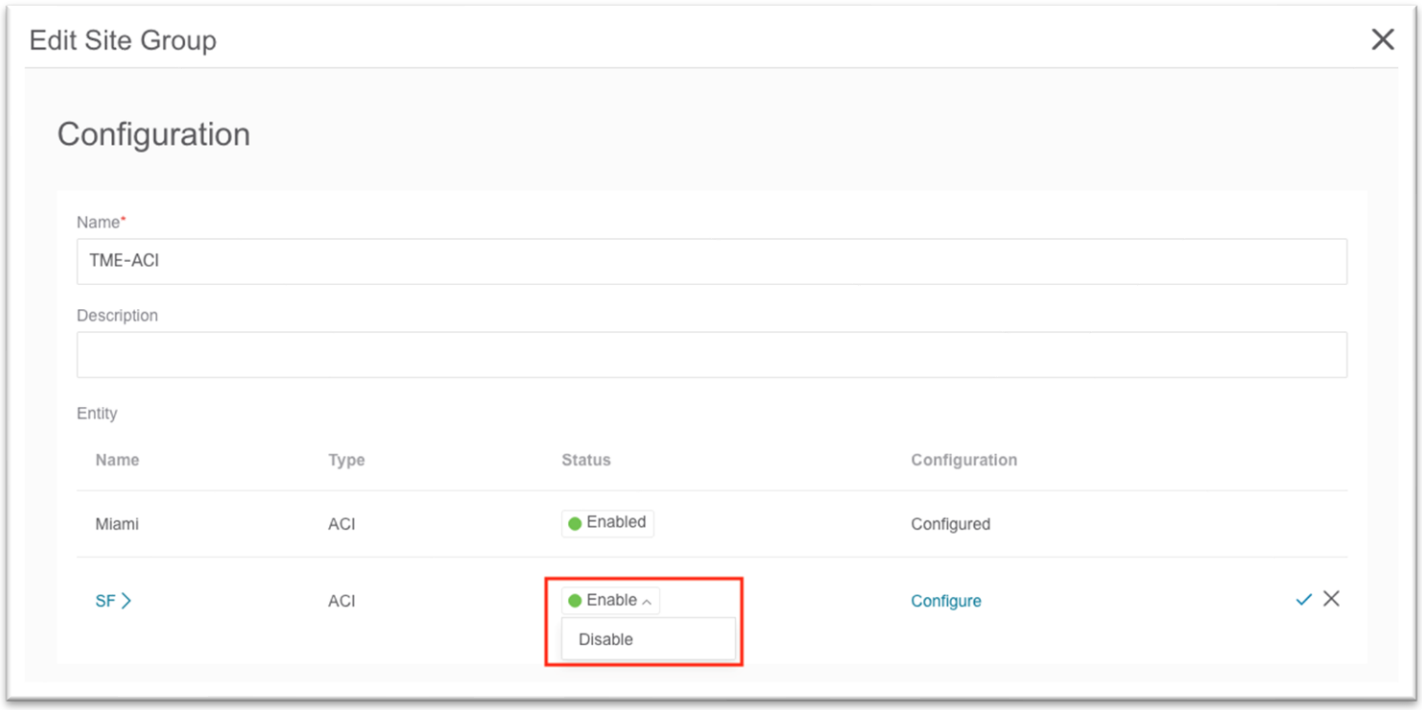


Cisco Nexus ダッシュボード Insights サービスが起動したら、新しいサイト グループを作成するか、既存のサイト グループを編集してメンバーを追加することで、既存のサイト グループを設定します。次の手順は、新しいサイト グループと既存のサイト グループの両方で同等です。

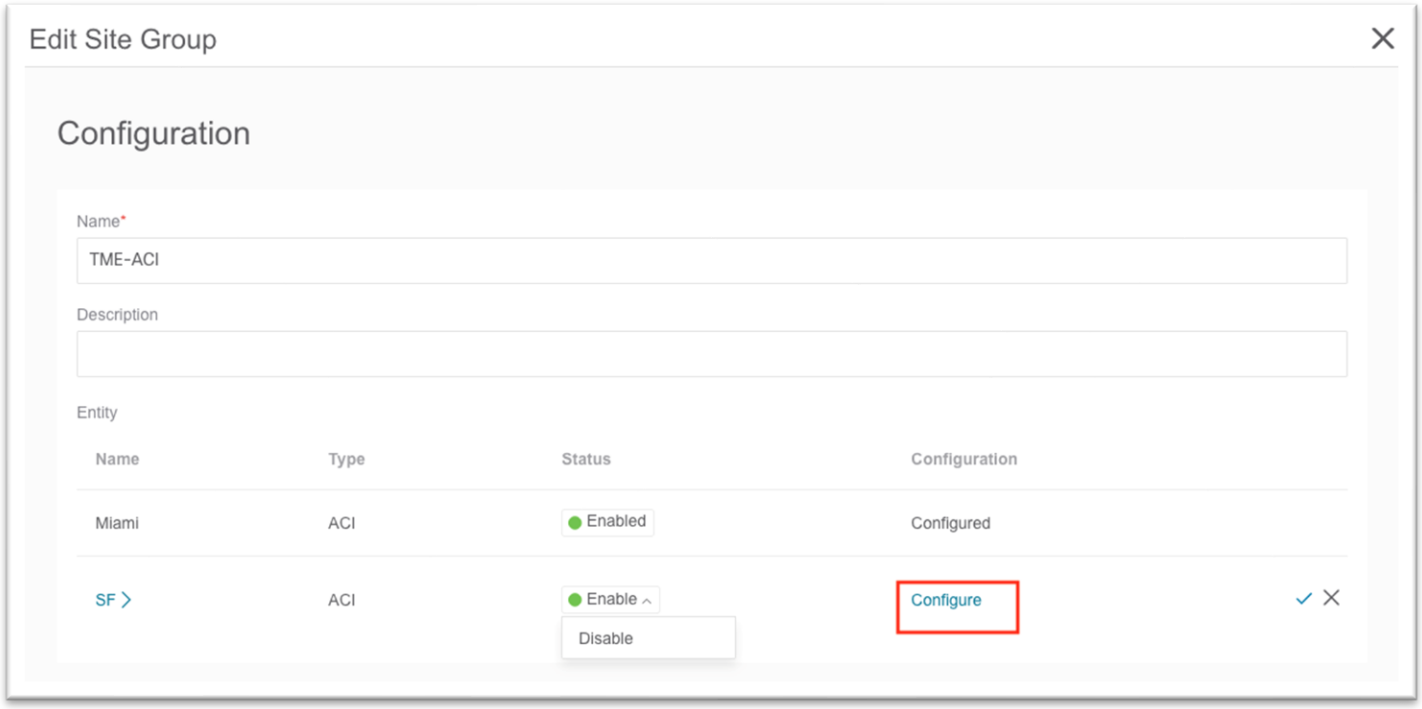
1. [メンバーの選択（Select Member）] を選択すると、使用可能なサイトを示すポップアップが開きます。使用可能なサイトを選択し、**[選択（Select）]** をクリックします。



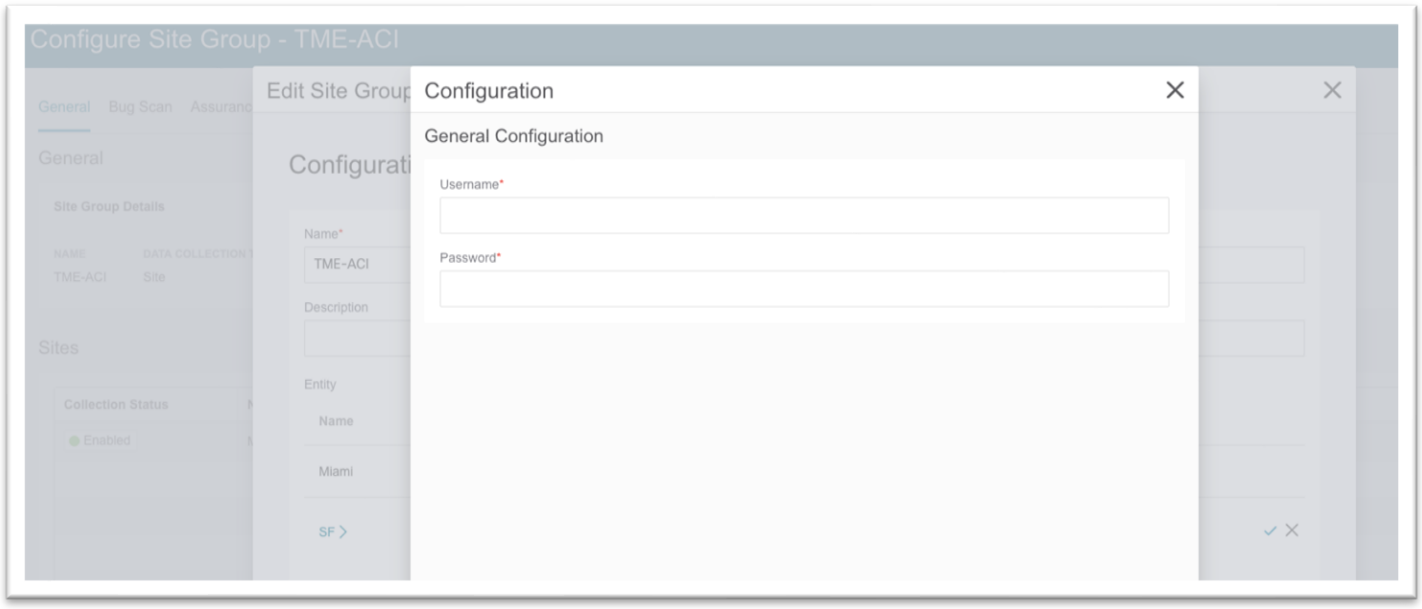
2. **[ステータス（Status）]** を **[有効（Enabled）]** に設定します。



3. **[設定（Configuration）]** 列で **[設定（Configure）]** をクリックします。これにより、新しいポップアップが開きます。

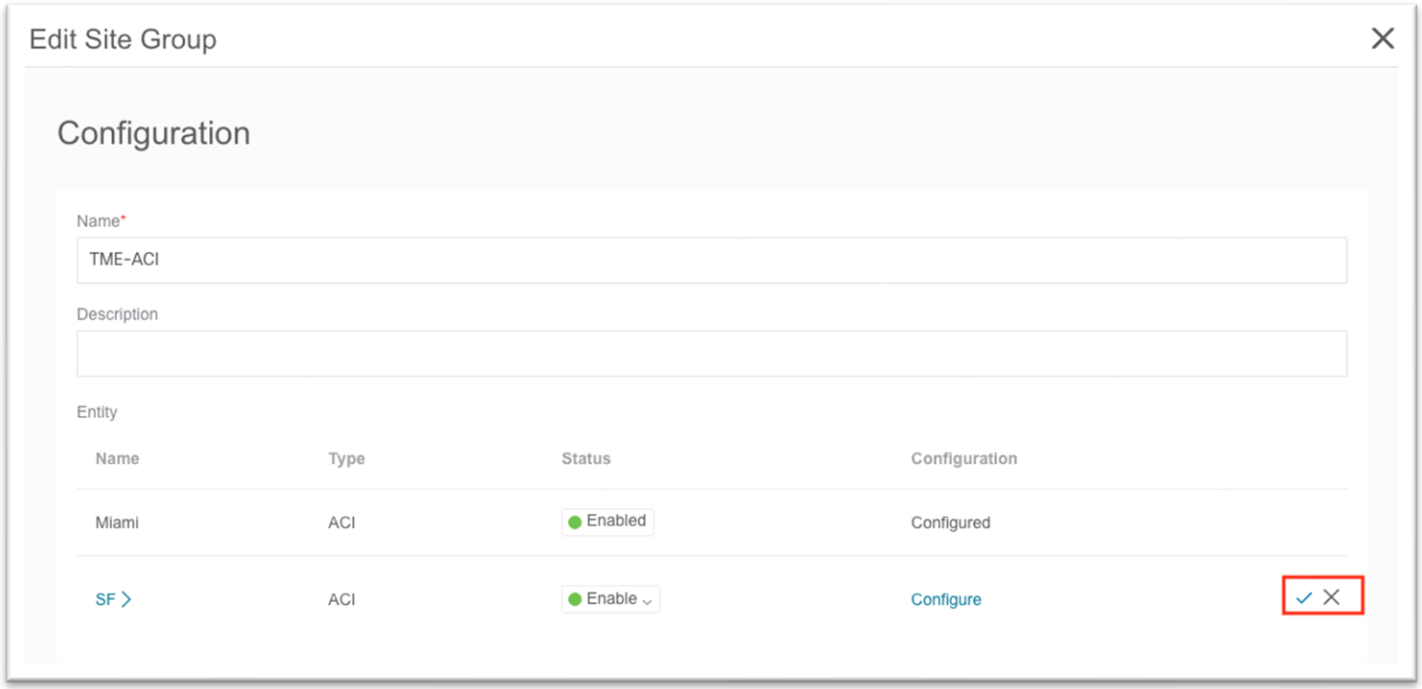


a. このポップアップ入力で、保証分析に使用されるユーザ名とパスワードを入力します。これらのクレデンシャルには、管理者レベルの権限が必要です。



b. [保存（Save）] をクリックします。

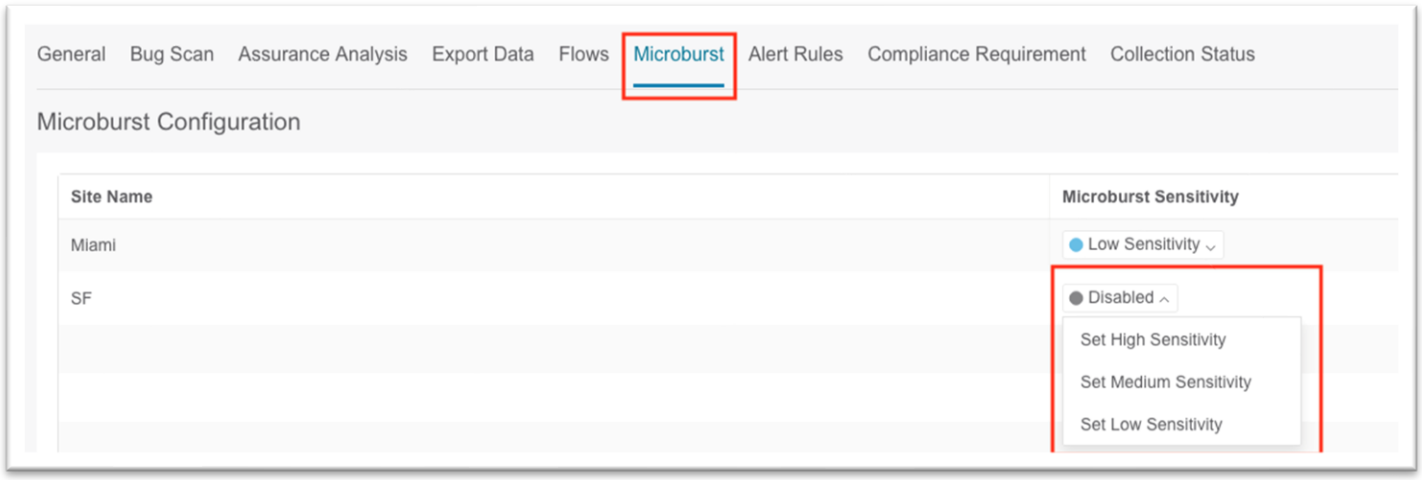
4. チェックマークをクリックして保存します。



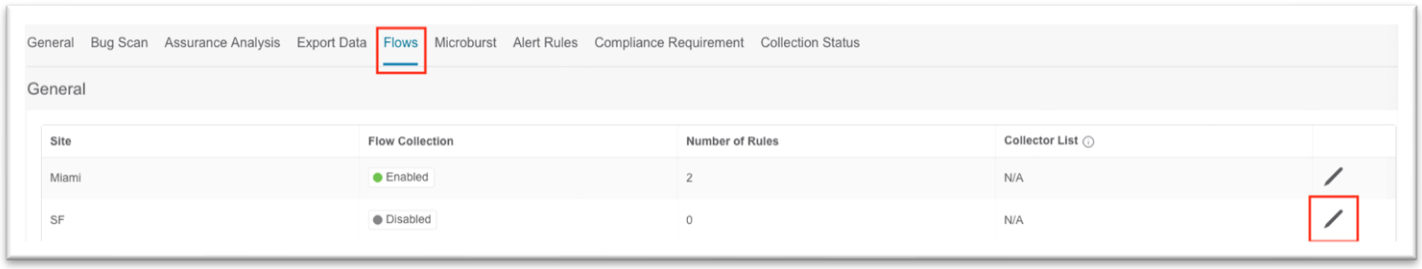
5. 下部にある **[保存（Save）]** をクリックします。

   a. サイトが正常に追加されると、**[収集ステータス（Collection Status）]** 列の値が [追加中（Adding）] から [有効（Enabled）] に変わります。

6. 上部のメニューにある **[マイクロバースト（Microbusrt）]** タブをクリックし、次に感度ドロップダウン リストをクリックして、サイトに必要なマイクロバースト感度を選択します。

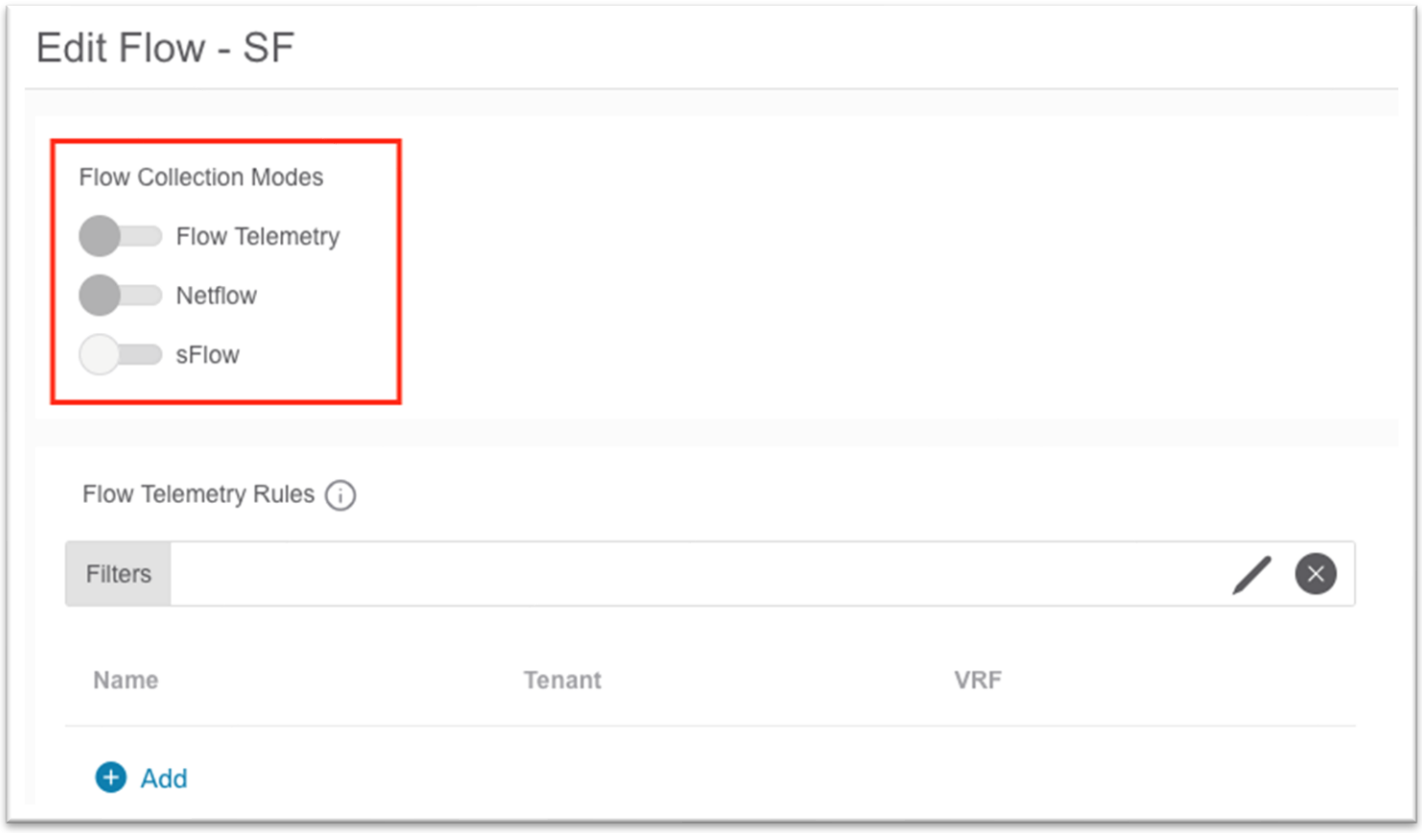


7. トップ メニューの **[フロー（Flows）]** タブをクリックし、鉛筆アイコンをクリックして新しいサイトを編集します。



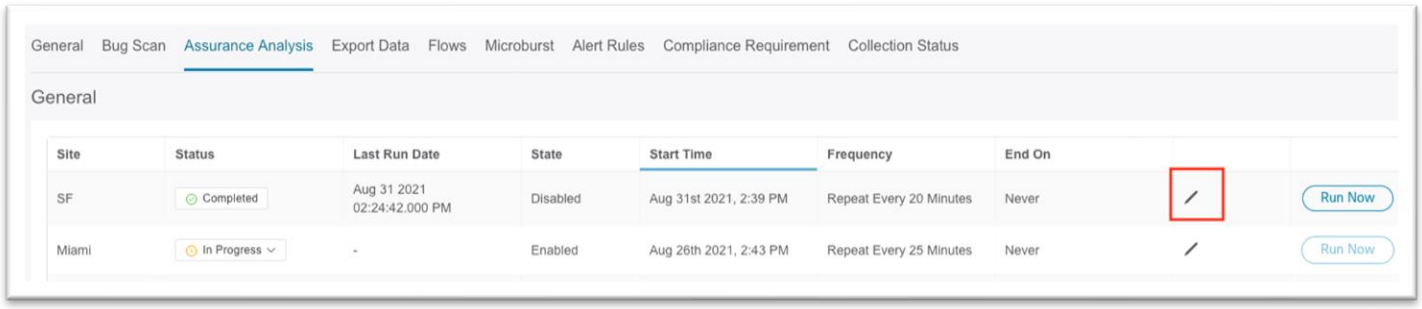
a. ポップアップで、目的のフロー収集モードのトグルを選択します。

b. 必要に応じて、フロー テレメトリ ルールを作成します。



c. 下部にある **[保存（Save）]** をクリックします。

8. トップメニューの **[保証分析（Assurance Analysis）]** タブをクリックし、鉛筆アイコンをクリックして新しいサイトを編集します。

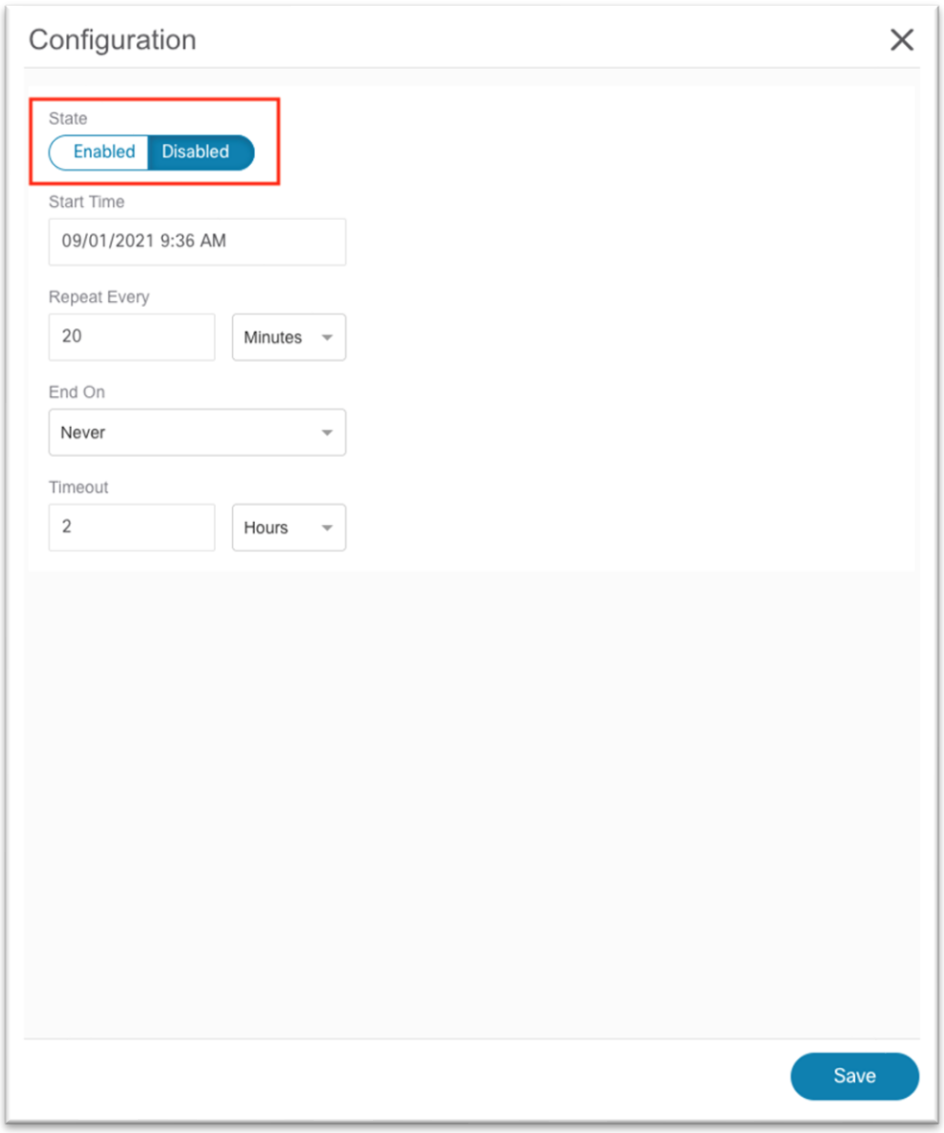


a. ポップアップで、状態を **[有効（Enabled）]** に設定します。

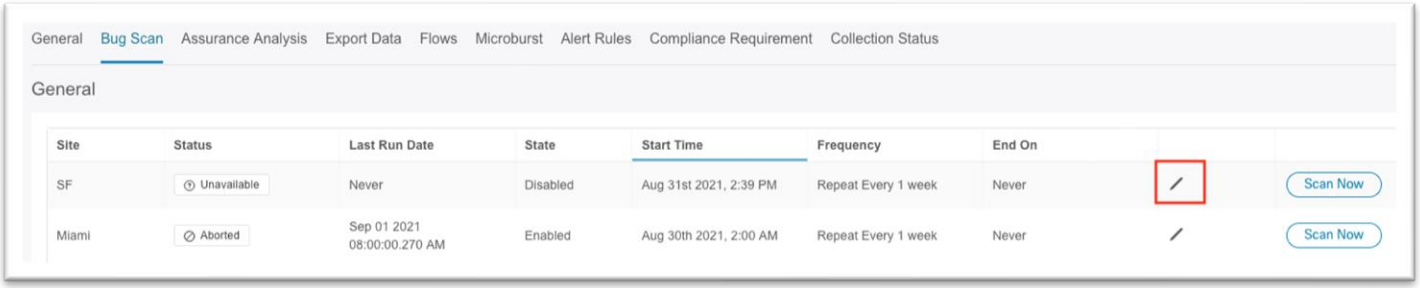
b. 必要に応じて、別のサイトが保証分析を現在実行している場合に備えて、将来の開始時刻を選択します。

c. 繰り返し時間については、大規模なファブリックに十分な時間を割り当てるようにしてください。詳細についてはユーザ ガイドを参照してください。

d. 下部にある **[保存（Save）]** をクリックします。

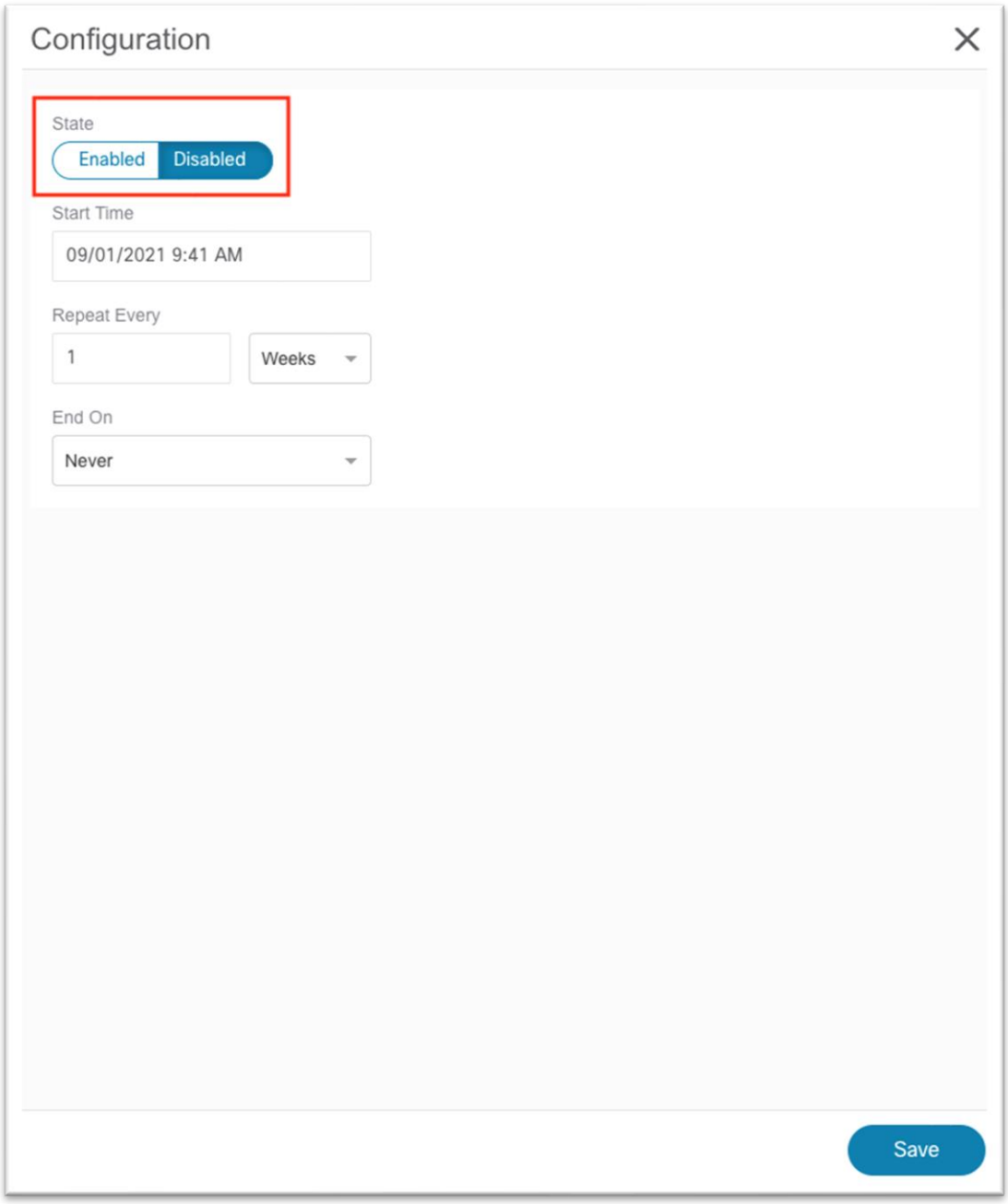


9. トップメニューの **[バグ スキャン（Bug Scan）]** タブをクリックし、鉛筆アイコンをクリックして新しいサイトを編集します。

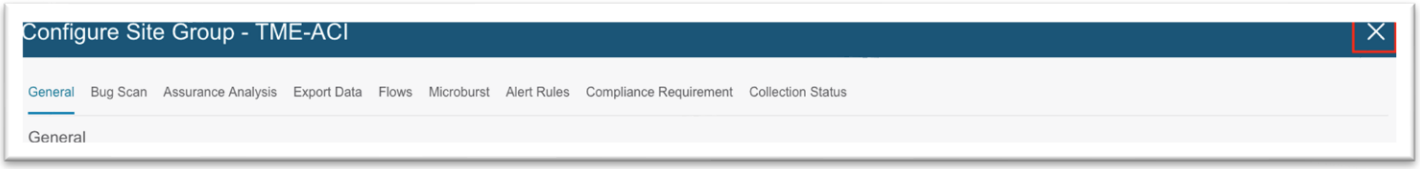


a. ポップアップで、状態を **[有効（Enabled）]** に設定します。

b. 下部にある **[保存（Save）]** をクリックします。



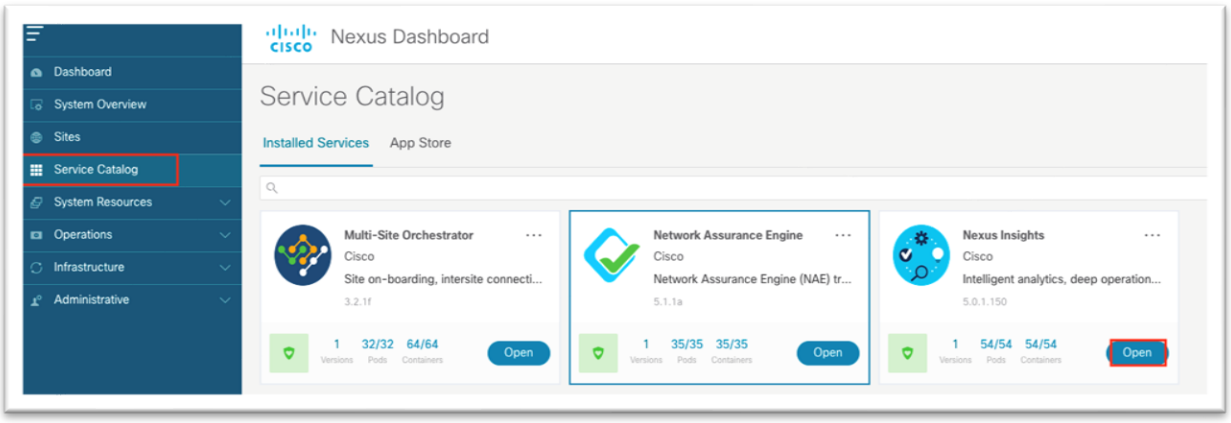
10. 必要な設定をすべて有効にした後、青色のタイトル バーの [X] をクリックして [サイト グループの概要（Site Group Overview）] ページに戻ります。



Cisco Nexus Insights リリース 5.x サイトの設定手順

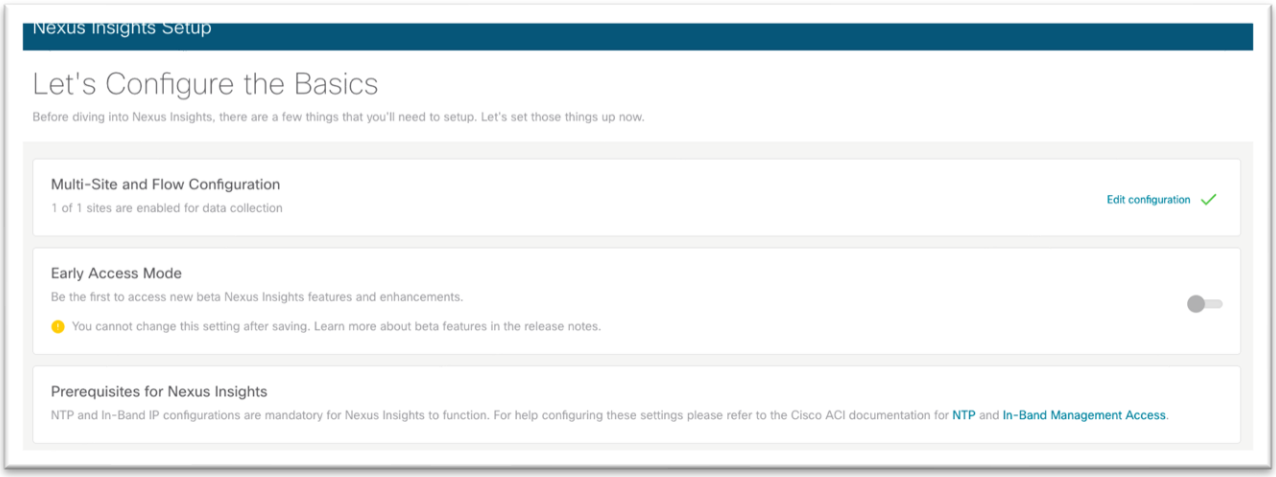
Cisco Nexus ダッシュボード Insightsの設定の詳細については、『Cisco Nexus Insights 5.x ACI ユーザ ガイド インストールおよびセットアップ』を参照してください。

1. ブラウザを使用して、Cisco Nexus ダッシュボード GUI へのセッションを開きます。
2. 左側のメニューで、**[サービス カタログ（Service Catalog）]** を選択します。
3. Cisco Nexus Insights の **[開く（Open）]** をクリックします。

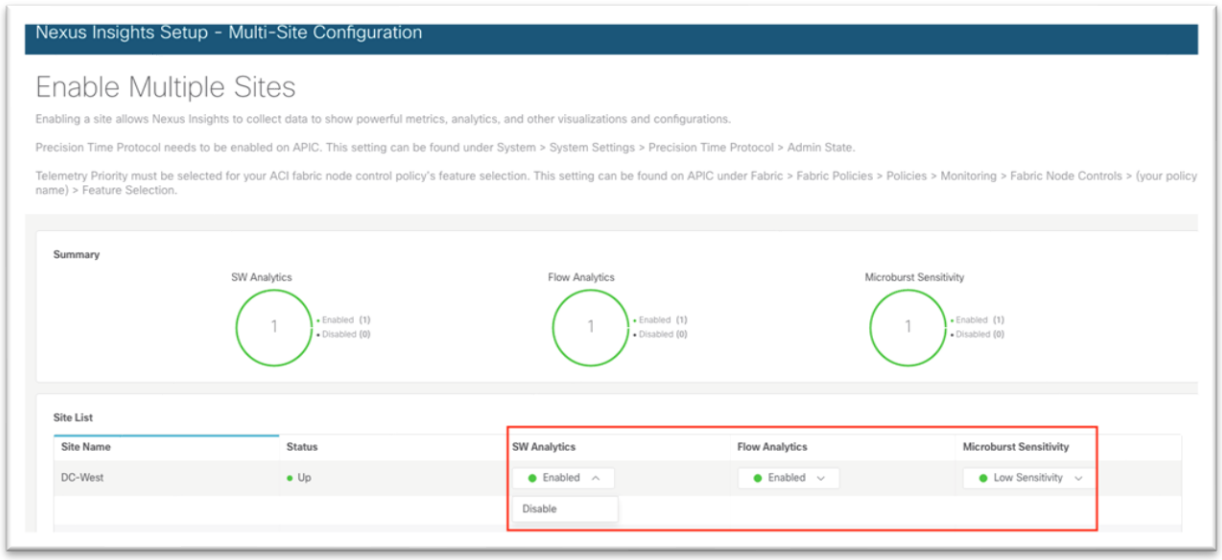


これにより、ブラウザで新しいタブが開きます。Cisco Nexus Insights を初めて設定する場合は、セットアップ ウィザードが表示されます。

4. **[マルチサイトおよびフロー設定（Multi-Site and Flow Configuration）]** セクションで、**[設定の編集（Edit configuration）]** をクリックします。

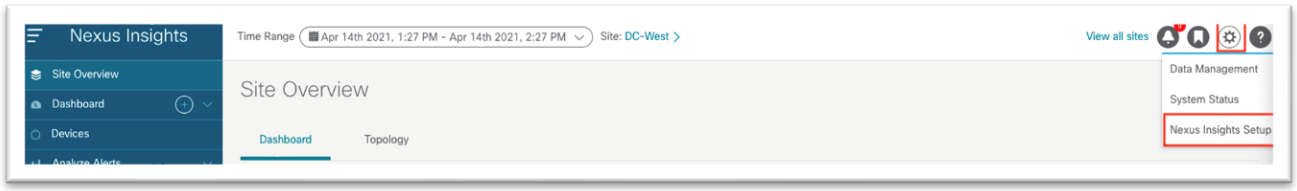


5. **[SW 分析（SW Analytics）]** 列と **[フロー分析（Flow Analytics）]** 列のドロップダウン リストを使用して、必要に応じて **[有効（Enabled）]** を選択します。**[マイクロバースト感度（Microburst Sensitivity）]** カラムで、目的の感度を選択します。



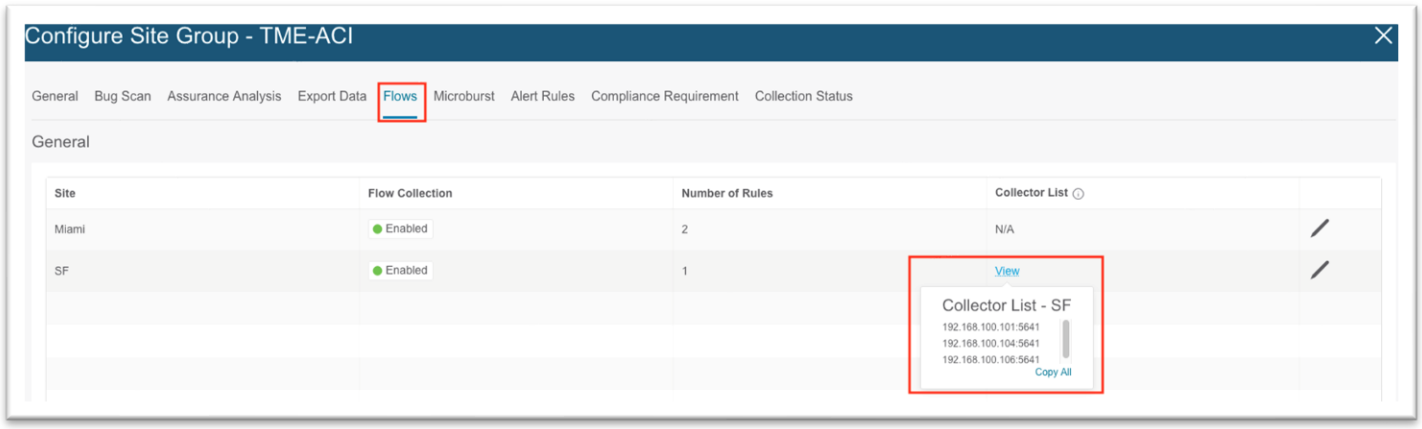
6. **[複数サイトの有効化（Enable Multiple Sites）]** 画面を終了するには、右下隅の **[完了（Done）]** をクリックします。
7. **[完了（Done）]** をもう一度クリックして、**[Insights セットアップ（Insights Setup）]** 画面を終了します。

この時点で、Cisco Nexus ダッシュボード Insights サービスへのデータの入力が開始され、情報が表示されるまでに約 5 ～ 15 分かかります。前の章で説明したように、将来のサイトを Cisco Nexusダ ッシュボードに追加できます。Cisco Nexus Insights の右上のツールバーで、**[歯車/設定（Gear / Settings）]** アイコンをクリックし、**[Nexus Insights セットアップ（Nexus Insights Setup）]** を選択することもできます。



Cisco ACI NetFlow 設定

NetFlow が必要な場合は、Cisco Nexus ダッシュボード外部サービス プールの永続 IP アドレスがデータ ネットワークに割り当てられていることを確認し、サイト グループ フロー収集モードのサイトが NetFlow に設定されていることを確認します。そうである場合、NetFlow エクスポータの IP アドレスは、次に示すように **[コレクタ リスト（Collector List）]** 列に表示されます。



NetFlow の高レベルのワークフローは、テナント NetFlow とアクセス ポリシー NetFlow で一貫しています。ワークフローは、収集対象を定義する NetFlow レコード ポリシーと、送信元と宛先の IP アドレス、NetFlow バージョン、および宛先に到達できる EPG を定義する NetFlow エクスポータで構成されます。最後に、NetFlow レコード ポリシーと NetFlow エクスポータは NetFlow モニタ ポリシーによって参照され、ブリッジ ドメインまたはインターフェイス ポリシー グループに適用されます。

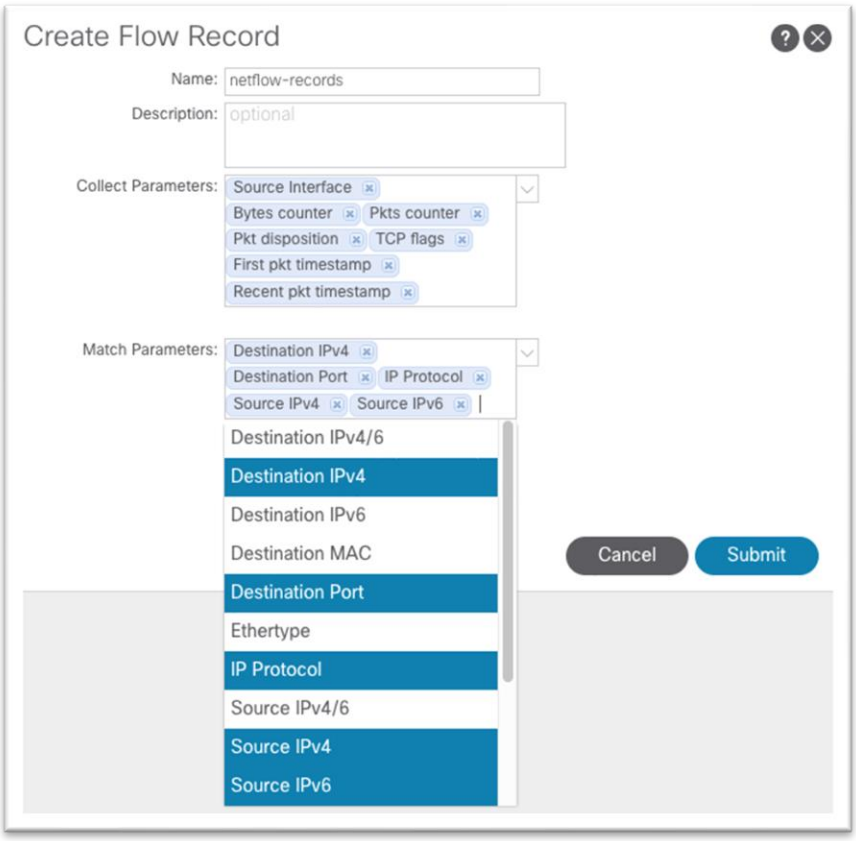
特に Cisco Nexus ダッシュボード Insights の場合、NetFlow エクスポータで使用される宛先ポートは 5641 です。

特定の設定手順は、このドキュメントの範囲外です。NetFlow および Cisco ACI の詳細については、Cisco APIC および NetFlow の技術情報を参照してください。

必要な各ポリシーの例を次に示します。

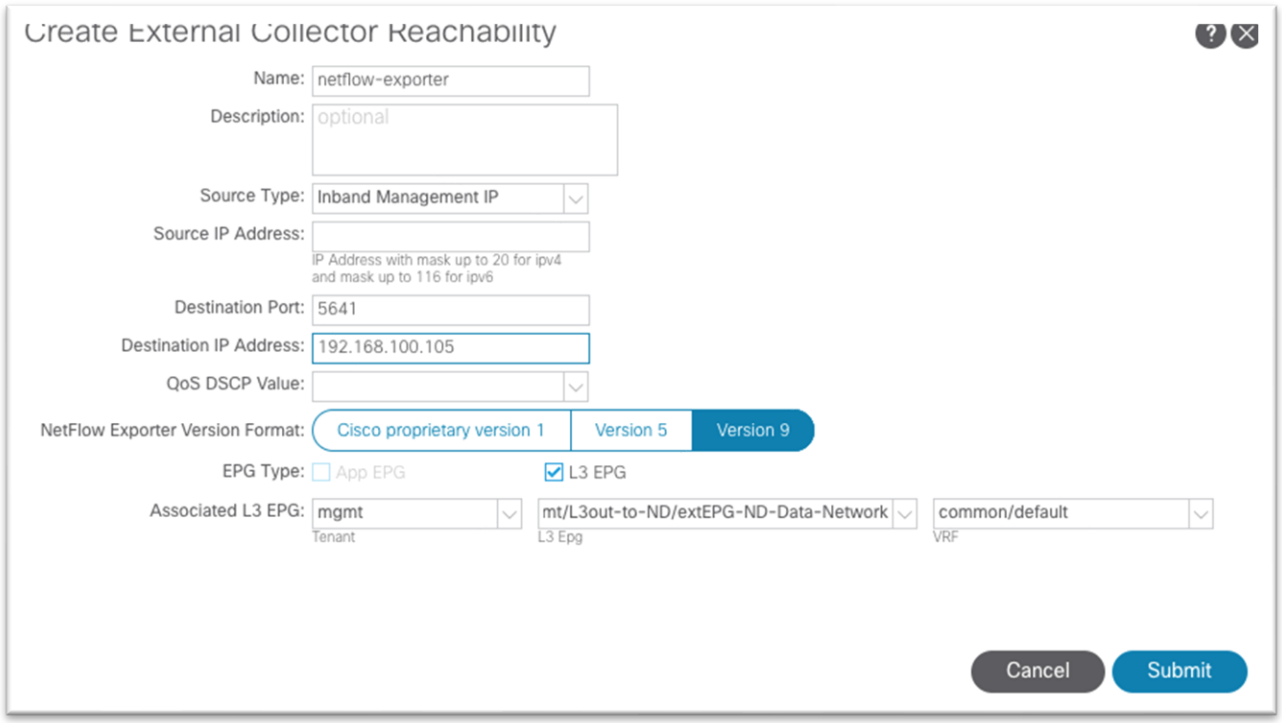
NetFlow レコード ポリシー

ドロップダウン リストを使用して、必要なオプションを選択します。



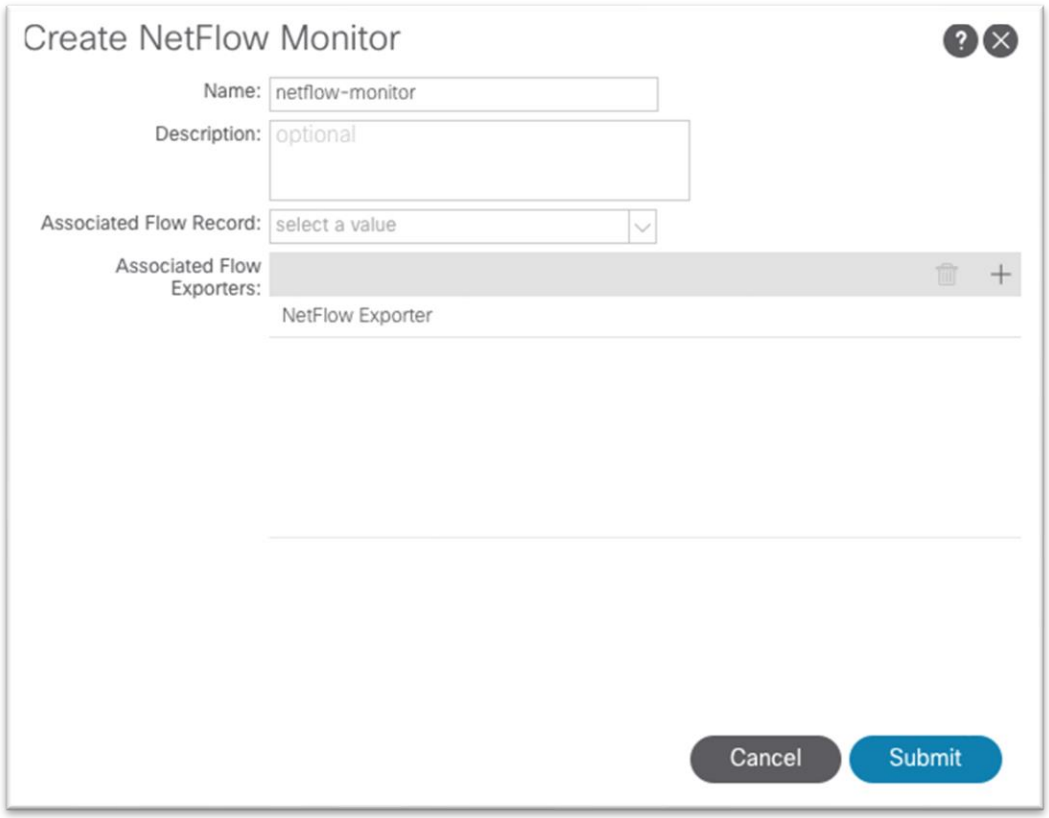
NetFlow エクスポータ ポリシー

[Source Type] = [Inband Management IP] を使用することをお勧めします。このオプションでは、**[送信元 IP アドレス（Source IP Address）]** フィールドに IP アドレスを手動で入力する必要はありません。宛先ポート 5641 およびバージョン 9 が使用されていることを確認します。また、Cisco ACI の NetFlow では、エクスポータ IP アドレスがユーザ VRF インスタンスまたは共通/デフォルト VRF インスタンスにある必要があります。L3out は管理テナントに配置できます。

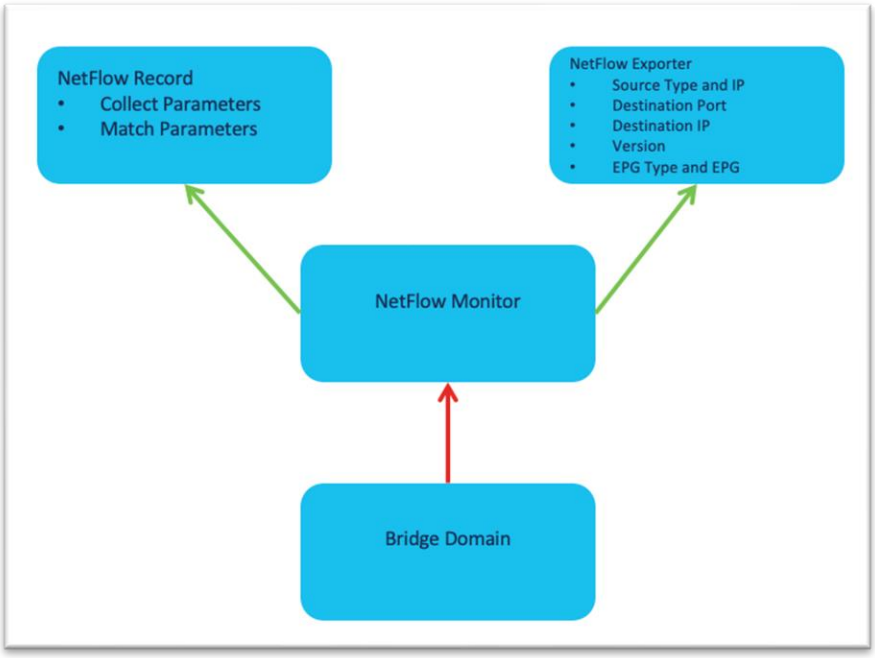


NetFlowモニターポリシー

NetFlow モニタ ポリシーは、単にレコード ポリシーとモニタリング ポリシーを結び付けて、ブリッジ ドメインやインターフェイス ポリシー グループなどの目的のオブジェクトで使用します。



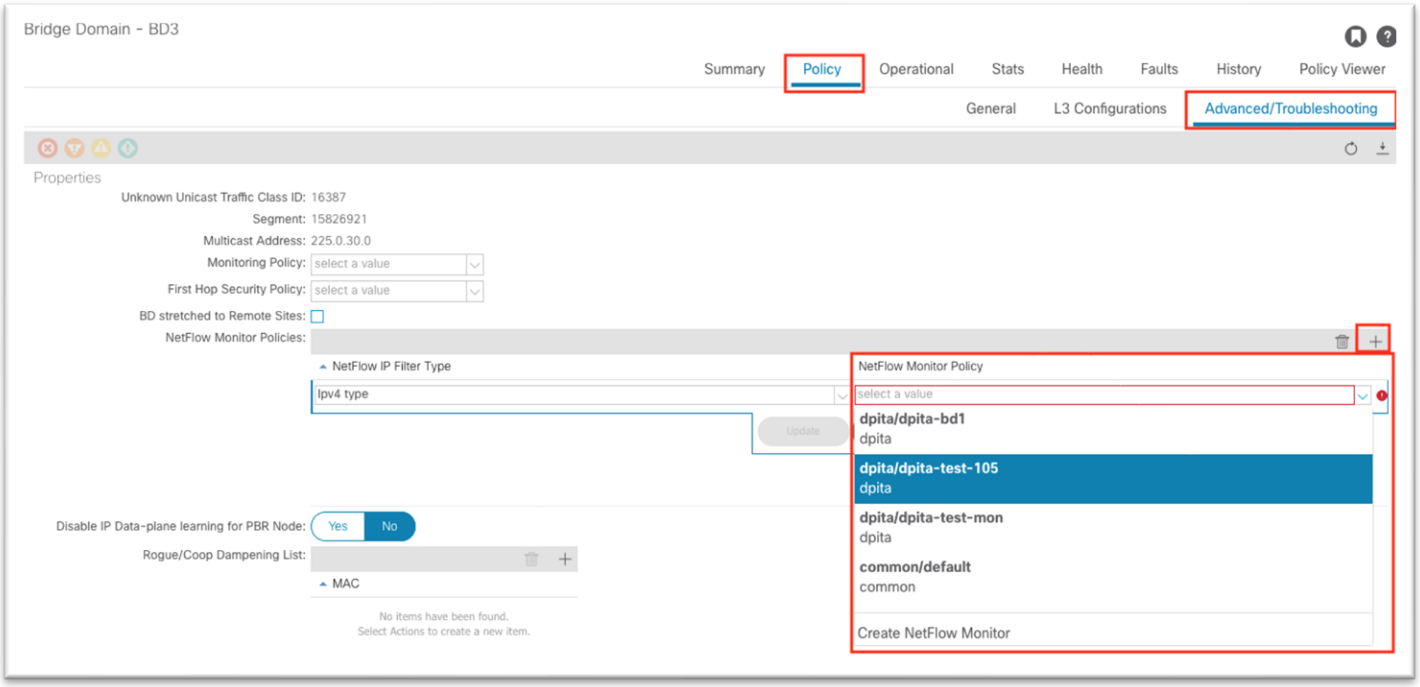
テナント レベルの NetFlow



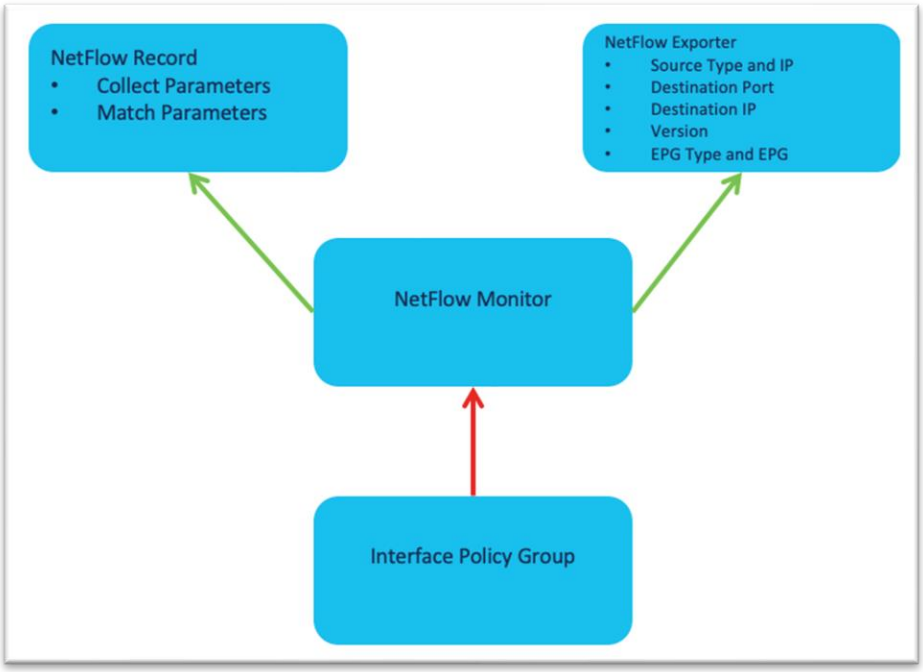
この設定は、**[テナント（Tenant）] > [ポリシー（Policies）] > [NetFlow]** にあります。

次に示すように、NetFlowモニタは、**[ポリシー（Policy）] > [詳細（Advanced）] / [トラブルシューティング（Troubleshooting）]** でブリッジ ドメインに接続されます。

次のスクリーンショットは、Cisco APIC リリース 5.2 で既存のブリッジ ドメインに NetFlow モニタ ポリシーを適用する方法を示しています。



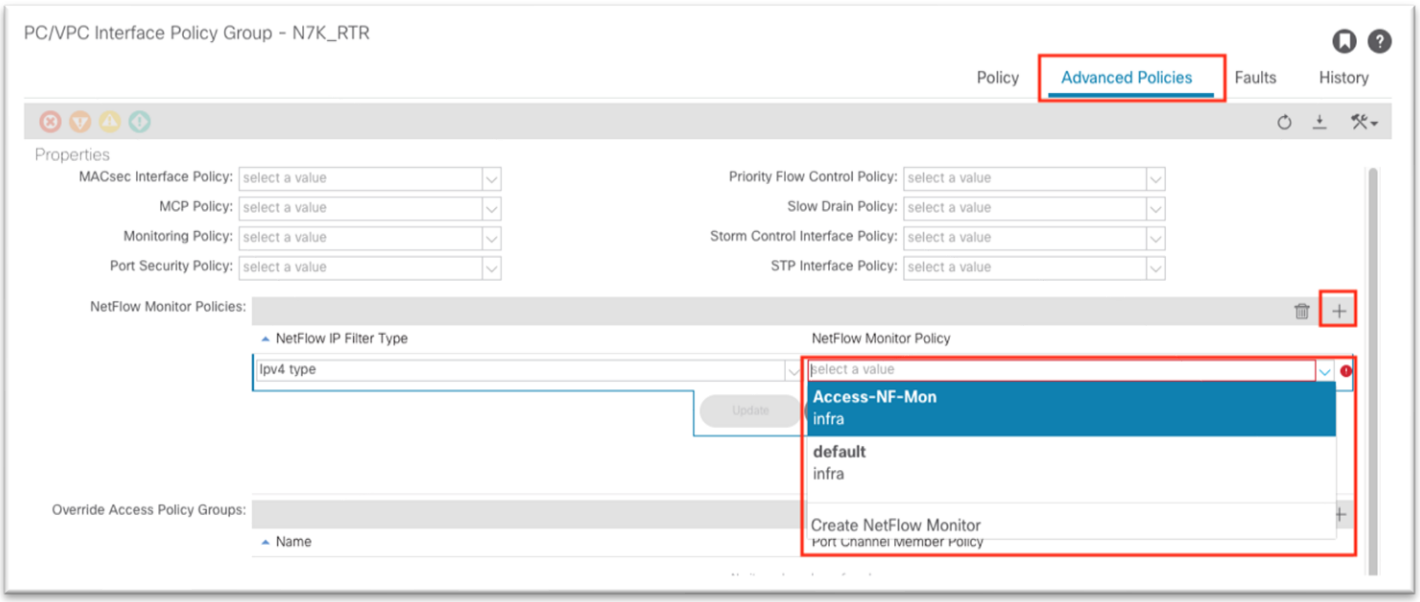
アクセス ポリシー NetFlow



この設定は、**[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [ポリシー（Policies）] > [インターフェイス（Interface）] > [NetFlow]** にあります。

次に示すように、NetFlow モニタがインターフェイスポリシー グループに接続されます。

次のスクリーンショットは、Cisco APIC リリース 5.2 で既存の vPC インターフェイス ポリシー グループに NetFlow モニタ ポリシーを適用する方法を示しています。



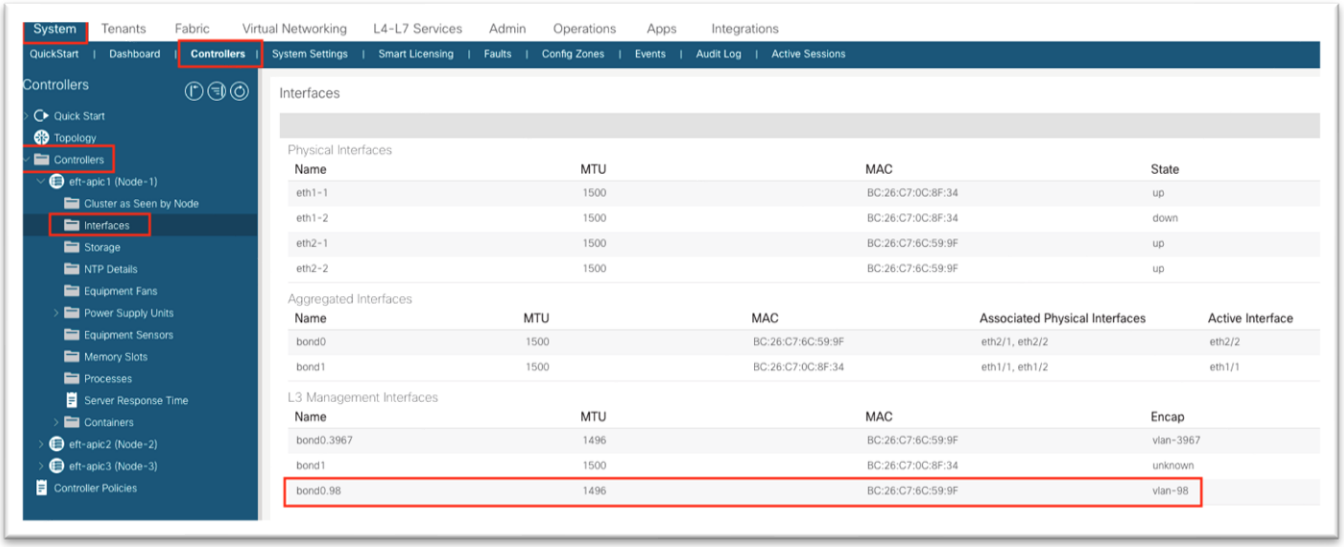
基本検証

インバンド検証

Cisco ACI の設定と同様に、最初に行うことは障害のチェックです。この場合は、管理テナントまたはシステムレベルで障害を確認します。

Cisco APIC 検証

Cisco APIC GUI から、**[システム（System）] > [コントローラ（Controllers）] > [コントローラ（Controllers）] > [インターフェイス（Interfaces）]** に移動し、**[L3 管理インターフェイス（L3 Management Interfaces）]** の下に新しいエントリがあることを確認します。VLAN プールとノード管理 EPG で設定された VLAN を持つ新しい Bond0 が存在する必要があります。



Cisco APIC CLI から、`ifconfig Bond0.98` を実行し、インバンド インターフェイスの IP アドレスを確認します。

```
eft-apic3#ifconfig Bond0.98
bond0.98: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1496
        inet 192.168.98.153 netmask 255.255.255.0 broadcast 192.168.98.255
        inet6 fe80::be26:c7ff:fe6c:5d9f prefixlen 64 scopeid 0x20<link>
        ether bc:26:c7:6c:5d:9f txqueuelen 1000 (Ethernet)
        RX packets 311049 bytes 67220546 (64.1 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 391273 bytes 2151564060 (2.0 GiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
APIC CLI から、インバンド ブリッジ ドメイン サブネットへの ping を試行します。 ping 192.168.98.1 -I 192.168.98.153

eft-apic3# ping 192.168.98.1 -I 192.168.98.153
PING 192.168.98.1 (192.168.98.1) from 192.168.98.153 : 56(84) bytes of data.
64 bytes from 192.168.98.1: icmp_seq=1 ttl=64 time=0.138 ms
64 bytes from 192.168.98.1: icmp_seq=1 ttl=64 time=0.138 ms
64 bytes from 192.168.98.1: icmp_seq=3 ttl=64 time=0.142 ms
64 bytes from 192.168.98.1: icmp_seq=1 ttl=64 time=0.138 ms
```

スイッチの検証

Cisco APIC から `show switch` コマンドを実行すると、インバンド IP 設定をすばやく確認できます。

```
eft-apic3#show sw
```

```
 ID ポッド アドレス インバンド IPv4 OOB IPv4 バージョン フラグ名
 ---- ---- --------------- --------------- ------------ --- --------------- ----- ----------
 111 1 10.0.104.66 192.168.98.171 10.18.188.165 n9000-15.1(4c) asiv Spine111
 112 1 10.0.104.65 192.168.98.172 10.18.188.166 n9000-15.1(4c) asiv Spine112
 301 1 10.0.104.64 192.168.98.161 10.18.188.161 n9000-15.1(4c) aliv Leaf301
 302 1 10.0.104.67 192.168.98.162 10.18.188.162 n9000-15.1(4c) aliv Leaf302
 401 1 10.0.104.68 192.168.98.163 10.18.188.163 n9000-15.1(4c) aliv Leaf401
 402 1 10.0.104.69 192.168.98.164 10.18.188.164 n9000-15.1(4c) aliv Leaf402

Flags - a:Active | l/s:Leaf/Spine | v:Valid Certificate | i:In-Service

eft-apic3#
```

接続のために、Cisco APIC またはアウトオブバンド管理を介してリーフ スイッチに接続し、`show ip int brief vrf mgmt:inb`コマンドを実行します。

```
Leaf301# show ip int brie vrf mgmt:inb
IP Interface Status for VRF "mgmt:inb"(6)
インターフェイス アドレス インターフェイス ステータス
vlan11 192.168.99.1/24 protocol-up/link-up/admin-up
vlan14 192.168.98.161/24 protocol-up/link-up/admin-up
```

この出力から、このリーフ スイッチの VLAN14 がインバンド ブリッジ ドメインの SVI であることがわかります。`show ip int VLAN14` コマンドを実行すると、ゲートウェイがセカンダリとして表示され、プライマリはスイッチ自体のスタティック ノード アドレスになります。

```
Leaf301# show ip int vlan14
VRF "mgmt:inb" の IP インターフェイス ステータス
vlan14, Interface status: protocol-up/link-up/admin-up, iod: 69, mode: pervasive
  IP address: 192.168.98.161, IP subnet: 192.168.98.0/24
  IP address: 192.168.98.1, IP subnet: 192.168.98.0/24 secondary
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 0, tag: 0


Leaf301#
```

最後に、iping で接続をテストします。Cisco APIC インバンド アドレスに ping を送信します。

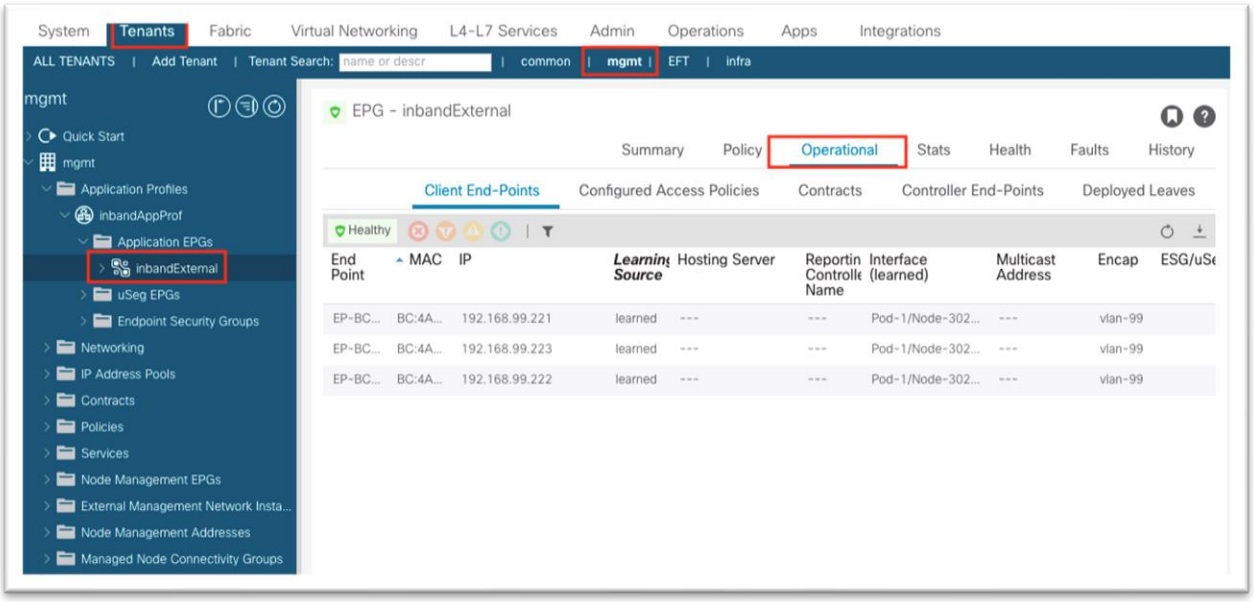
```
Leaf301# iping -V mgmt:inb 192.168.98.153 -S 192.168.98.161
PING 192.168.98.153 (192.168.98.153) from 192.168.98.161: 56 data bytes
64 bytes from 192.168.98.153: icmp_seq=0 ttl=63 time=0.321 ms
64 bytes from 192.168.98.153: icmp_seq=1 ttl=63 time=0.298 ms
64 bytes from 192.168.98.153: icmp_seq=2 ttl=63 time=0.282 ms
64 bytes from 192.168.98.153: icmp_seq=3 ttl=63 time=0.217 ms
64 bytes from 192.168.98.153: icmp_seq=4 ttl=63 time=0.192 ms


--- 192.168.98.153 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.192/0.262/0.321 ms
```

Cisco Nexus ダッシュボード データ インターフェイスの検証への接続

このテストは、Cisco APIC またはリーフ スイッチから実行できます。まず、Cisco Nexus Dashboard が設定されている EPG を確認することで、Cisco ACI が Cisco Nexus Dashboard を学習したかどうかを簡単に確認できます。

エンドポイントを表示するには、**[テナント（Tenants）] > [管理（mgmt）] > [アプリケーション プロファイル（Application Profiles）] > [名前（name）] > [アプリケーション EPG（Application EPGs）] > [名前（name）] > [操作（Operational）]** の順に移動します。



Cisco APIC CLI から、リストされている各 IP アドレスに ping を発行します。

```
eft-apic3# ping 192.168.99.221 -I 192.168.98.153
PING 192.168.99.221 (192.168.99.221) from 192.168.98.153 : 56(84) bytes of data.
64 bytes from 192.168.99.221: icmp_seq=1 ttl=63 time=0.133 ms
64 bytes from 192.168.99.221: icmp_seq=2 ttl=63 time=0.062 ms
64 bytes from 192.168.99.221: icmp_seq=3 ttl=63 time=0.076 ms
64 bytes from 192.168.99.221: icmp_seq=4 ttl=63 time=0.073 ms
64 bytes from 192.168.99.221: icmp_seq=5 ttl=63 time=0.075 ms
```

ping が失敗した場合は、インバンド EPG と Cisco Nexus ダッシュボード EPG の間にコントラクトがあることを確認します。

```
Leaf301# contract_parser.py | grep mgmt:inb
[9:4108] [vrf:mgmt:inb] permit any tn-mgmt/mgmtp-default/inb-In-BandInternal(16386) tn-mgmt/ap-In-BandAppProf/epg-In-BandExternal(49154) [contract:uni/tn-mgmt/brc-In-BandPermit] [hit=57073074,+42]
[9:4109] [vrf:mgmt:inb] permit any tn-mgmt/ap-In-BandAppProf/epg-In-BandExternal(49154) tn-mgmt/mgmtp-default/inb-In-BandInternal(16386) [contract:uni/tn-mgmt/brc-In-BandPermit] [hit=0]
[16:4105] [vrf:mgmt:inb] permit any epg:any tn-mgmt/bd-inb-external(16387) [contract:implicit] [hit=6]
[16:4106] [vrf:mgmt:inb] permit any epg:any tn-mgmt/bd-inb(32771) [contract:implicit] [hit=0]
[16:4103] [vrf:mgmt:inb] permit arp epg:any epg:any [contract:implicit] [hit=0]
[21:4102] [vrf:mgmt:inb] deny,log any epg:any epg:any [contract:implicit] [hit=0]
[22:4104] [vrf:mgmt:inb] deny,log any epg:any pfx-0.0.0.0/0(15) [contract:implicit] [hit=0]
Leaf301#show zoning-rule scope 2949121
+ ------- + ------ + ------ + -------- + ---------- + ------- + ------- + -------------- + -------- + ---------- --- +
|Rule ID|SrcEPG|DstEPG|FilterID| Dir | operSt| Scope | Name | Action | Priority |
+-------+------+------+--------+----------+-------+-------+--------------+--------+--------------------+
| 4102 | 0 | 0 |implicit| uni-dir |enabled|2949121| |deny,log| any_any_any(21) |
| 4103 | 0 | 0 |implarp | uni-dir |enabled|2949121| | permit | any_any_filter(17) |
| 4104 | 0 | 15 |implicit| uni-dir |enabled|2949121| |deny,log|any_vrf_any_deny(22)|
| 4105 | 0 |16387 |implicit| uni-dir |enabled|2949121| | permit | any_dest_any(16) |
| 4106 | 0 |32771 |implicit| uni-dir |enabled|2949121| | permit | any_dest_any(16) |
| 4108 |16386 |49154 |default | uni-dir- |enabled|2949121|mgmt: | permit | src_dst_any(9) |
```

```
| | | | | ignore | | In-BandPermit| | |
| 4109 |49154 |16386 |default | bi-dir |enabled|2949121|mgmt: | permit | src_dst_any(9) |
| | | | | | | In-BandPermit| | |
+-------+------+------+--------+----------+-------+-------+--------------+--------+--------------------+
Leaf301#
```

ネットワーク タイム プロトコル検証

Cisco APIC ネットワーク タイム プロトコルの検証

NX-OS スタイルの CLI から `show ntp` コマンドを実行して、Cisco APIC の設定とステータスを表示します。

```
eft-apic3#show ntp
 nodeid remote refid st t when poll reach auth delay offset jitter
 ------ - ------------ ------ --- -- ------ -------- -------- ---- -------- -------- ------
 3 * 72.163.32.44 .GNSS. 1 u 38 64 377 none 42.783 0.097 0.860
 1 * 72.163.32.44 .GNSS. 1 u 6 64 377 none 41.518 0.001 0.151
 2 * 72.163.32.44 .GNSS. 1 u 33 64 377 none 40.503 -0.066 0.678
eft-apic3#
```

スイッチ ネットワーク タイム プロトコル検証

標準の NX-OS コマンドと一部の Linux コマンドが適用されます。

- show clock
- show ntp peers
- show ntp peer-status
- show ntp statistics peer ipaddr <ip>
- date
- cat /etc/timezone

```
Leaf301# show clock
08:30:48.620137 CDT Thu Apr 15 2021
Leaf301#
Leaf301# show ntp peers
-------------------------------------------------------------------------------
  Peer IP Address Serv/Peer Prefer KeyId Vrf
-------------------------------------------------------------------------------
  72.163.32.44 Server yes None management
Leaf301# show ntp peer-status
合計ピア数：1
* - selected for sync, + - peer mode(active),
- - peer mode(passive), = - polled in client mode
    remote local st poll reach delay vrf
-------------------------------------------------------------------------------
 *72.163.32.44 0.0.0.0 1 64 237 0.044 management
Leaf301# show ntp statistics peer ipaddr 72.163.32.44
remote host: 72.163.32.44
local interface：Unresolved
time last received：0s
time until next send: 2s
reachability change: 349419s
packets sent：28051
packets received: 27957
bad authentication: 0
bogus origin: 59
duplicate: 0
```

```
bad dispersion: 59
bad reference time: 0
candidate order: 6
Leaf301#
Leaf301#date
Thu Apr 15 08:31:12 CDT 2021
Leaf301# cat /etc/timezone
America/Chicago
```

正確なタイム プロトコル検証

標準の NX-OS コマンドが適用されます。

- show ptp parent
- show ptp counters all
- show ptp clock

シングルポッド Cisco ACI では、すべてのスイッチに同じ親クロックが必要です。

```
Leaf301# show ptp parent

PTP PARENT PROPERTIES

Parent Clock:
Parent Clock Identity: b0:8b:cf:ff:fe:76:50:8d
Parent Port Number: 20
Observed Parent Offset (log variance): N/A
Observed Parent Clock Phase Change Rate: N/A

Parent IP: 10.0.104.66
Grandmaster Clock:
Grandmaster Clock Identity: b0:8b:cf:ff:fe:76:50:8d
Grandmaster Clock Quality:
    Class: 248
    Accuracy: 254
    Offset (log variance): 65535
    Priority1: 254
    Priority2: 255

Leaf301# show ptp counters all

インターフェイス Eth1/53 の PTP パケット カウンタ：
--------------------------------------------------------------------
パケット タイプ TX RX
---------------- -------------------- -------------- ------
Announce 2  4177888
Sync 15  66447366
FollowUp 15  66439780
Delay Request 33353837  0
Delay Response 0    33353631
PDelay Request 0    0
PDelay Response 0   0
PDelay Followup 0   0
Management 0    0
インターフェイス Eth1/54 の PTP パケット カウンタ：
--------------------------------------------------------------------
パケット タイプ TX RX
---------------- -------------------- -------------- ------
Announce 4178103    2
Sync 66486827   15
FollowUp 66481600   15
Delay Request 0     33348274
```

```
Delay Response 33348274    0
PDelay Request 0    0
PDelay Response 0   0
PDelay Followup 0   0
Management 0    0

Leaf301# show ptp clock
PTP Device Type : boundary-clock
PTP Device Encapsulation : layer-3
PTP Source IP Address : 10.0.104.64
Clock Identity : 00:3a:9c:ff:fe:19:e8:ff
Clock Domain: 0
Slave Clock Operation : Two-step
Master Clock Operation : Two-step
Slave-Only Clock Mode : Disabled
Number of PTP ports: 2
Configured Priority1 : 255
Priority1 : 255
Priority2 : 255
Clock Quality:
    Class : 248
    Accuracy : 254
    Offset (log variance) : 65535
Offset From Master : -12
Mean Path Delay : 160
Steps removed : 1
Correction range : 100000
MPD range : 1000000000
Local clock time : Wed Aug 4 09:32:31 2021
Hardware frequency correction : NA
```

ファブリック ノード制御の検証

ノード制御ポリシーが正しく適用されたことを確認するスイッチの基本的な検証は、show Analytics hw-profile で、機能の優先順位として「Telemetry」が出力されます。

```
Leaf301#show Analyticss hw-profile


Feature Prio: Telemetry
```

Cisco Nexus ダッシュボード Insights が設定され、サイトに対して有効になった後、show analytics exporter を実行すると、Cisco Nexus ダッシュボード データ インターフェイス IP アドレスがエクスポート先として表示されます。

```
Leaf301# show analytics exporter
Flow exporter 192.168.99.221 :
    Destination : 192.168.99.221
    VRF: mgmt:inb (1)
    宛先 UDP ポート 5640
    Source : 192.168.98.161
    DSCP 44
    エクスポート バージョン 255
Flow exporter 192.168.99.222 :
    Destination : 192.168.99.222
    VRF: mgmt:inb (1)
    宛先 UDP ポート 5640
    Source : 192.168.98.161
    DSCP 44
    エクスポート バージョン 255
Flow exporter 192.168.99.223 :
    Destination : 192.168.99.223
    VRF: mgmt:inb (1)
    宛先 UDP ポート 5640
    Source : 192.168.98.161
```

```
        DSCP 44
        エクスポート バージョン 255


    Feature Prio: Telemetry
```

NetFlow の確認

フロー エクスポータが正しく設定され、フローがキャッシュに収集されていること、および NetFlow パケットが CPU によって生成されエクスポートされていることを確認するためのスイッチでの基本的な検証。

- show flow exporter
- show flow monitor
- show flow cache
- tcpdump -i kpm_inb port 5641

```
F1-P1-Leaf-104# show flow exporter
Flow exporter dpita:dpita-flow-exp:
    Destination: 192.168.100.104
    VRF: common:default (1)
    宛先 UDP ポート 5641
    Source: 192.168.99.104
    DSCP 44
    エクスポート バージョン 9
        シーケンス番号 262
        データ テンプレート タイムアウト 0 秒
エクスポート統計情報
エクスポート済みフロー レコード数 974
エクスポート済みテンプレート数 171
送信エクスポート パケット数 262
送信エクスポート バイト数 56740
宛先到達不能イベント数 0
バッファなしイベント数 0
ドロップしたパケット数（ホストへのルートなし）0
ドロップしたパケット数（その他）0
ドロップしたパケット数（出力ドロップ）0
Time statistics were last cleared: Never
Flow exporter dpita:dpita-test-exp2:
    Destination: 192.168.100.105
    VRF: common:default (1)
    宛先 UDP ポート 5641
    Source: 192.168.99.104
    DSCP 44
    エクスポート バージョン 9
        シーケンス番号 262
        データ テンプレート タイムアウト 0 秒
エクスポート統計情報
エクスポート済みフロー レコード数 974
エクスポート済みテンプレート数 171
送信エクスポート パケット数 262
送信エクスポート バイト数 56740
宛先到達不能イベント数 0
バッファなしイベント数 0
ドロップしたパケット数（ホストへのルートなし）0
ドロップしたパケット数（その他）0
ドロップしたパケット数（出力ドロップ）0
Time statistics were last cleared: Never
```

```
Feature Prio: NetFlow

F1-P1-Leaf-104# show flow monitor
Flow Monitor default:
    Use count: 0
    Flow Record: default
Flow Monitor dpita:dpita-test-mon:
    Use count: 1
    Flow Record: dpita:dpita-test-record
    Bucket Id: 1
    Flow Exporter: dpita:dpita-flow-exp
Flow Monitor dpita:dpita-test-105:
    Use count: 1
    Flow Record: dpita:dpita-test-record
    Bucket Id: 1
    Flow Exporter: dpita:dpita-test-exp2

Feature Prio: NetFlow


F1-P1-Leaf-104# show flow cache
IPV4 エントリ
SIP DIP BD ID S-Port D-Port Protocol Byte Count Packet Count TCP FLAGS if_id flowStart flowEnd

192.168.1.100 192.168.4.100 537 0 0 1 86814 63 0x0 0x16000000 1217618386 1217638714


F1-P1-Leaf-104# tcpdump -i kpm_inb port 5641
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on kpm_inb, link-type EN10MB (Ethernet), capture size 262144 bytes
11:47:40.116456 IP 192.168.99.104.52255 > 192.168.100.104.5641: UDP, length 220
11:47:40.116588 IP 192.168.99.104.39779 > 192.168.100.106.5641: UDP, length 220
```


お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

Printed in USA Cxx-xxxxxx-xx 07/21