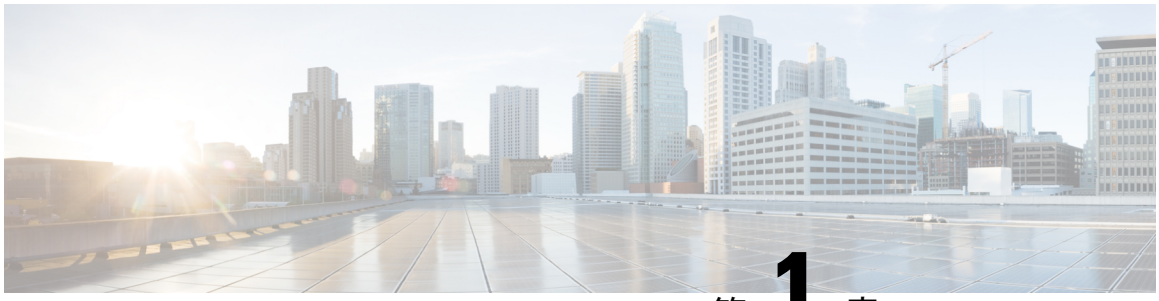
『Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics、Release 4.0（x）』

最終更新：2025 年 5 月 19 日

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
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

次の表に、このガイドの最初に発行されたリリースから現在のリリースまでに、このガイドの編成と機能に加えられた大幅な変更の概要を示します。テーブルは、ガイドに加えられたすべての変更のすべてを網羅したリストを提供しているわけではありません。

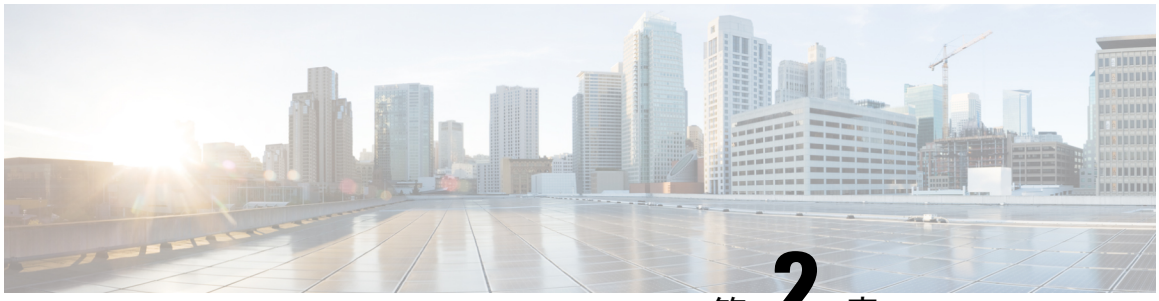
表 *1*: 最新のアップデート

リリース	新機能またはアップデート	参照先
4.0(1)	このドキュメントの最初のリリース。	--

新機能および変更された機能に関する情報

第 I 部

アプリケーションとファブリック管理



第 2 章

テナント と テナントポリシー

テナントの概要

テナントは、アプリケーションポリシーの論理コンテナで、管理者はドメインベースのアクセスコントロールを実行できます。テナントはポリシーの観点から分離の単位を表しますが、プライベート ネットワークは表しません。テナントは、サービス プロバイダーの環境ではお客様を、企業の環境では組織またはドメインを、または単にポリシーの便利なグループ化を表すことができます。

3 つのデフォルト テナントが事前に設定されています。

- `common`：ACI ファブリックの他のテナントに「共通」のサービスを提供するための特別なテナント。共通テナントの基本原則はグローバルな再利用です。一般的なサービスには、共有 L3Out、DNS、DHCP、Active Directory、共有プライベート ネットワークまたはブリッジドメインなどがあります。

- `dcnm-default-tn`：Cisco NDFC ファブリックの設定を提供する特別なテナント。

- `infra`：トンネルやポリシー展開など、ファブリック内部の通信に使用されるインフラストラクチャ テナント。これには、スイッチ間の切り替えと APIC 通信への切り替えが含まれます。`infra`テナントは、ユーザー空間（テナント）には公開されず、独自のプライベート ネットワーク空間とブリッジ ドメインを備えています。ファブリックの検出、イメージ管理、ファブリック機能用の DHCP は、すべてこのテナント内で処理されます。

  Nexus Dashboard Orchestrator を使用して Cisco NDFC ファブリックを管理する場合は、常にデフォルトの `dcnm-default-tn` テナントを使用します。

（注） Nexus Dashboard Orchestrator は APIC の管理テナントをテナントしたり、 NDO で mgmt と呼ばれる新しいテナントを作成したりすることはできません。

テナントを管理するには、パワー ユーザまたはサイトとテナント マネージャの読み取り/書き込みロールのいずれかが必要です。

テナント ポリシー テンプレート

リリース 4.0（1）では、テナント ポリシー テンプレートが追加されています。これにより、次のテナント全体のポリシーを構成できます。

- マルチキャストのルート ポリシー
- ルート制御のルート マップ ポリシー
- カスタム QoS ポリシー
- DHCP リレー ポリシー
- DHCP オプション ポリシー
- IGMP インターフェイス ポリシー
- IGMP スヌーピング ポリシー
- MLD スヌーピング ポリシー

詳細については、テナント ポリシー テンプレートを作成 （8 ページ） を参照してください。

新しいテナントの作成

このセクションでは、Nexus ダッシュボード オーケストレータ GUI を使用して新しいテナントを追加する方法について説明します。ファブリックから既存のテナントを一つ以上インポートしたい場合、既存テナントのインポート （8 ページ） に記されているステップに従います。

始める前に

テナントの作成および管理には、パワー ユーザまたはサイト マネージャの読み取り/書き込みロールを持つユーザが必要です。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 新しいテナントを作成。

a) 左側のナビゲーション メニューで、**[アプリケーション管理（Application Management）]** > **[テナント（Tenants）]** を選択します。
b) メイン ペインの右上にある **[テナントの追加 (Add Tenant)]** をクリックします。

[テナントの追加 (Add Tenant)] 画面が開きます。

ステップ 3 テナントの詳細を入力します。

a) **[表示名 (Display Name)]** とオプションの **[説明 (Description)]** を入力します。

Orchestrator の GUI 全体で、テナントが表示されるたびに、テナントの**表示名**が使用されます。ただし、APIC でのオブジェクトの命名要件により、無効な文字は削除され、その結果として得られた**内部名**が、サイトにテナントをプッシュするときに使用されます。テナントの作成時に使用される**内部名**は、**[表示名 (Display Name)]** テキストボックスの下に表示されます。

（注）
テナントの**表示名**はいつでも変更できますが、テナントの作成後に**内部名**を変更することはできません。

b) **[関連付けられたサイト (Associated Sites)]** セクションで、このテナントに関連付けるすべてのサイトをオンにします。

選択したサイトのみが、このテナントを使用している任意のテンプレートで使用可能になります。

c) （オプション）選択したサイトごとに、その名前の横にある**[編集（Edit）]**ボタンをクリックし、1つ以上のセキュリティ ドメインを選択します。

制限付きセキュリティ ドメインを使用すると、テナント A などのファブリック管理者は、両方のグループのユーザーに同じ権限が割り当てられている場合、あるユーザー グループがテナント B などの別のセキュリティ ドメインのユーザー グループによって作成されたオブジェクトを表示または変更できないようにすることができます。たとえば、テナント A の制限付きセキュリティ ドメインのテナント管理者は、テナント B のセキュリティ ドメインで構成されたポリシー、プロファイル、またはユーザーを表示できません。テナント B のセキュリティ ドメインも制限されていない限り、テナント B は、テナント A で設定されたポリシー、プロファイル、またはユーザーを表示できます。 ユーザーが適切な権限を持つシステム作成の設定に対して、ユーザーは常に読み取り専用で閲覧可能であることに注意してください。制限付きセキュリティドメインのユーザーには、そのドメイン内で幅広いレベルの特権を与えることができます。ユーザーが別のテナントの物理環境に不注意で影響を与える心配はありません。

セキュリティ ドメインは APIC GUI を使用して作成し、アクセスをコントロールするために、さまざまな APIC ポリシーに割り当てることができます。詳細については、*Cisco APIC* 基本設定ガイドを参照してください。

d) **[関連付けられたユーザー (Associated Users)]** セクションで、テナントへのアクセスが許可されている Nexus Dashboard Orchestratorユーザーを選択します。

テンプレートを作成するときに選択したユーザのみが、このテナントを使用できます。

ステップ 4 **[保存 (Save)]** をクリックして、テナントの追加を終了します。

既存テナントのインポート

このセクションでは、1 つ以上の既存のテナントをインポートする方法について説明します。Nexus Dashboard Orchestrator を使用して新しいテナントを作成する場合は、代わりに 新しいテナントの作成 （6 ページ） で説明されている手順に従ってください。

始める前に

テナントの作成および管理には、パワー ユーザまたはサイト マネージャの読み取り/書き込みロールを持つユーザが必要です。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 左側のナビゲーションメニューで、**[サイト（Sites）]** をクリックします。

ステップ 3 テナントのインポート元のサイトを見つけ、その**[アクション（Actions）]**（**...**）メニューをクリックして、**[テナントのインポート（Import Tenants）]** を選択します。

一度に 1 つのサイトからテナントをインポートできます。

ステップ 4 **[インポート テナント（Import Tenants）]** ダイアログ内で、インポートする一つ以上のテナントを選択して**Ok**をクリックします。

選択したテナントが Nexus ダッシュボード オーケストレータにインポートされ、**[アプリケーション管理（Application Management）]** > **[テナント（Tenants）]**ページに表示されます。

ステップ 5 これらの手順を繰り返して、他のサイトからテナントをインポートします。

テナント ポリシー テンプレートを作成

このセクションでは、1つ以上のテナント ポリシーテンプレートを作成する方法について説明します。テナント ポリシー テンプレートを使用すると、次のポリシーを作成および構成できます。

- マルチキャストのルート マップ ポリシー
- ルート制御のルート マップ ポリシー
- カスタム QoS ポリシー
- DHCP リレー ポリシー
- DHCP オプション ポリシー

- IGMP インターフェイス ポリシー
- MLD スヌーピング ポリシー

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 新しいテナント ポリシー テンプレートを作成します。

a) 左側のナビゲーション メニューで、**[アプリケーション管理（Application Management）]** > **[テナント ポリシー（Tenant Policies）]** を選択します。

b) **[テナント ポリシー テンプレート（Tenant Policy Template）]**ページ内で**[テナント ポリシー テンプレートを追加（Add Tenant Policy Template）]**をクリックします。

c) **[テナント ポリシー（Tenant Policies）]** ページの右のプロパティ サイトバーにテンプレートの **[名前（Name）]** を入力します。

d) **[テナントの選択（Select a Tenant）]**ドロップダウンから、このテンプレートに関連付けるテナントを選択します。

次の手順で説明するように、このテンプレートで作成するすべてのポリシーは、選択したテナントに関連付けられ、テンプレートを特定のサイトにプッシュすると、テナントに展開されます。

デフォルトでは、新しいテンプレートは空であるため、次のステップに従って 1 つ以上のテナント ポリシーを追加する必要があります。テンプレートで使用可能なすべてのポリシーを作成する必要はありません。このテンプレートとともに展開する各タイプのポリシーを1つ以上定義できます。特定のポリシーを作成したくない場合は、説明されている手順をスキップしてください。

ステップ 3 テンプレートを 1 つ以上のサイトに割り当てます。

サイトにテナント ポリシー テンプレートを割り当てるプロセスは、サイトにアプリケーション テンプレートを割り当てる方法と同じです。

a) **[テンプレート プロパティ（Template Properties）]** 表示内で **[アクション（Actions）]** をクリックして **[サイトの関連付け（Sites Association）]** を選択します。

[<template-name> にサイトの関連付け（Associate Sites to <template-name>）] ウィンドウが開きます。

b) **[サイトの関連付け（Associate Sites）]** ウィンドウで、テンプレートを展開するサイトの横のチェックボックスをオンにします。

テナント ポリシー テンプレートは、オンプレミス ACI サイトにのみサポートされることにご注意ください。そして、割り当て可能です。

c) **Ok** をクリックして保存します。

ステップ 4 マルチキャストのルート マップ ポリシーを作成します。

このポリシーは、包括的なレイヤ3マルチキャスト ユース ケースの一部です。このセクションにある情報を参照資料として使用することができます。しかし資料のレイヤ3マルチキャスト（283ページ）章の機能とユース ケース セクションの全てのステップのセットに従うことをおすすめします。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[マルチキャストのルート マップ ポリシー（Route Map Policy for Multicast）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) **[+ マルチキャスト エントリのルート マップを追加（+Add Route Map for Multicast Entries）]** をクリックし、ルート マップ情報を指定します。

   ルート マップごとに、1 つ以上のルート マップ エントリを作成する必要があります。次の情報によると各コンテキストは、1 つ以上の一致基準に基づいてアクションを定義するルールです：

   - **順序** – 順序は、ルールを評価する順序を決定するために用いられます。
   - **グループ IP**、 **Src IP** と **RP IP** – 同じマルチキャスト ルート マップのポリシー UI は 2 つの方法で使用できます。マルチキャスト トラフィックのフィルタのセットを設定すること、またはランデブー ポイントの構成をマルチキャスト グループの特定のセットに制限することです。設定する使用例によっては、この画面のフィールドの一部だけを指定すればよい場合もあります。
     - マルチキャスト フィルタリングの場合には、フィルタを定義するために、**[ソース IP (Source IP)]** と **[グループ (Group IP)]** フィールドを使用します。これらのフィールドの少なくとも 1 つを提供できますが、両方を含むことを選択できます。フィールドの 1 つが空白のままの場合は、すべての値と一致します。

       グループ IP の範囲は `224.0.0.0` ～ `239.255.255.255` で、ネットマスクは `/4` ～ `/32` である必要があります。サブネット マスクを指定する必要があります。

       RP IP (ランデブー ポイントの IP) は、マルチキャスト フィルタリング ルート マップでは使用しないので、このフィールドはブランクのままにします。

     - ランデブー ポイントの設定では、**[グループ IP (Group IP)]** フィールドを使用して RP のマルチキャスト グループを定義できます。

       グループ IP の範囲は `224.0.0.0` ～ `239.255.255.255` で、ネットマスクは `/4` ～ `/32` である必要があります。サブネット マスクを指定する必要があります。

       ランデブー ポイント設定の場合、**RP IP** は RP 設定の一部として設定されます。ルート マップをグループ フィルタリングに使用する場合は、ルート マップに RP IP アドレスを設定する必要はありません。この場合には、**[RP IP]** と **[ソース IP (Source IP)]** フィールドを空白のままにします。

   - **アクション** – アクションは、一致が検出された場合に実行するアクションの許可または拒否を定義します。

e) チェックマーク アイコンをクリックして、エントリを保存します。
f) 前のサブステップを繰り返して、同じポリシーの追加のルート マップ エントリを作成します。
g) **[保存（Save）]** をクリックしてポリシーを保存し、テンプレート ページに戻ります。
h) この手順を繰り返して、マルチキャスト ポリシーの追加のルート マップを作成します。

ステップ 5 ルート制御のルート マップ ポリシーを作成。

このポリシーは、包括的なSR-MPLSの使用例の一部です。このセクションにある情報を参照資料として使用することができます。しかし資料のマルチサイトとSR-MPLS L3Outハンドオフ（335ページ）章の機能とユース ケース セクションの全てのステップのセットに従うことをおすすめします。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[ルート コントロールのルート マップ ポリシー（Route Control Policy for Multicast）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) **[+エントリを追加（+Add Entry）]** をクリックして、ルート マップ情報を入力します。

ルート マップごとに、1 つ以上のコンテキスト エントリを作成する必要があります。次の情報によると各コンテキストは、1 つ以上の一致基準に基づいてアクションを定義するルールです：

- **コンテキストの順序** – コンテキストの順序は、コンテキストが評価される順序を決定するために使用されます。値は 0 ～ 9 の範囲内である必要があります。
- **コンテキスト アクション** – コンテキスト アクションは、一致が検出された場合に実行するアクションの 許可 または 拒否 を定義します。

コンテキストの順序とアクションを定義したら、コンテキストを一致させる方法を選択します。

- **[+ 属性の追加 (+Add Attibute)]** をクリックして、コンテキストが一致する必要があるアクションを指定します。

  次のアクションのうちの 1 つを選択できます。

  - コミュニティの設定
  - ルート タグの設定
  - ダンプニングを設定します
  - ウェイトの設定
  - ネクスト ホップの設定
  - プリファレンスの設定
  - メトリックの設定
  - メトリック タイプの設定
  - AS パス の設定
  - 追加のコミュニティを設定

  属性を構成したら、**[保存（Save）]** をクリックします。

- IP アドレスまたはプレフィックスに基づいてアクションを照合する場合は、**[IP アドレスの追加 (Add IP Address)]** をクリックします。

  [プレフィックス (prefix)] フィールドに、IP アドレス プレフィックスを入力します。IPv4 と IPv6 の両方のプレフィックスがサポートされています (例:2003:1:1a5:1a5::/64または205.205.0.0/16)。

特定の範囲の IP を集約する場合は、**[集約 (aggregate)]** チェックボックスをオンにして、範囲を指定します。たとえば、`0.0.0.0/0` プレフィックスを指定して任意の IP に一致させるか、`10.0.0.0/8` プレフィックスを指定して任意の `10.xxx` アドレスに一致させることができます。

- コミュニティリストに基づいてアクションを照合する場合は、**[コミュニティの追加 (Add community)]** をクリックします。

  [コミュニティ (Community)] フィールドに、コミュニティ文字列を入力します。たとえば、`regular:as2-as2-nn2:200:300` などです。

  次に、**[範囲（Scope）]**を選択します：推移性は、コミュニティが eBGP ピアリング全体（自律システム（AS）全体）に伝播することを意味し、非推移性は、コミュニティが伝播しないことを意味します。

e) 前のサブステップを繰り返して、同じポリシーの追加のルート マップ エントリを作成します。
f) **[保存（Save）]** をクリックしてポリシーを保存し、テンプレート ページに戻ります。
g) この手順を繰り返して、ルート コントロール ポリシーの追加のルート マップを作成します。

ステップ 6 カスタム QoS ポリシーを作成。

Cisco APIC でカスタム QoS ポリシーを作成して、DSCP または CoS 値に基づいて入力トラフィックを分類し、それを QoS 優先度レベル （QoS ユーザー クラス） に関連付けて、ACI ファブリック内で適切に処理することができます。DSCP の値が IP ヘッダーにある場合および/または CoS の値が入力トラフィックのイーサネット ヘッダーにあるのみ、分類はサポートされます。さらに、カスタム QoS ポリシーを使用して、入力トラフィックのヘッダー内の DSCP および/または CoS 値を変更できます

たとえば、カスタム QoS ポリシーを使用すると、IP ヘッダーのないレイヤ 2 パケットなど、CoS 値のみに基づいてトラフィックをマークするデバイスから ACI ファブリック トラフィックに着信するトラフィックを分類できます。

ACI ファブリック内の QoS 機能の詳細については*Cisco APIC と QoS*を参照します。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[カスタム QoS ポリシー（Custom QoS Policy）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション)**[説明を追加（Add Description）]**をクリックして、このポリシーの説明を入力します。
d) **[+ DSCP マッピングを追加（+Add DSCP Mappings）]** をクリックして、必要な情報を入力します。

DSCPマッピング構成を使用すると、マッピングで指定された範囲内にDSCP値がある入力トラフィックを指定された QoS 優先度レベル（クラス）に関連付けることができます。また、入力トラフィックの DSCP および/または CoS 値を設定して、トラフィックがファブリックを出るときにそれらの値を保持できるようにすることもできます。

（注）
出力トラフィックのターゲット CoS 値を保持するには、NDO ファブリック ポリシーの一部である「CoS を保持する」ポリシーを構成する必要があります。

「DSCP ターゲット」および/または「ターゲット CoS」の値が DSCP マッピングと CoS マッピングの両方の一部として設定されている場合、DSCP マッピングで指定された値が優先されます。

マッピングごとに、次のフィールドを指定できます：

- **DSCP から** – DSCP 範囲の開始。
- **DSCP へ** – DSCP 範囲の終わり。
- **DSCP ターゲット** – 出力トラフィックのために保持される入力トラフィックに設定する DSCP 値。
- **ターゲット CoS** – 「CoS を保持」が有効になっている場合に、出力トラフィックのために保持される入力トラフィックに設定する CoS 値。
- **優先度** – トラフィックが割り当てられる QoS 優先度クラス。

マッピングを指定したら、チェックマーク アイコンをクリックして保存します。次に、**[+DSCP マッピングの追加（+Add DSCP Mappings）]** をクリックして、同じポリシー内に追加のマッピングを提供できます。

e) **[追加（Add）]** をクリックしてポリシーを保存し、テンプレート ページに戻ります。

f) **[+ CoS マッピングを追加（+Add CoS Mappings）]** をクリックして、必要な情報を入力します。

DSCPマッピング構成を使用すると、マッピングで指定された範囲内にDSCP値がある入力トラフィックを指定された QoS 優先度レベル（クラス）に関連付けることができます。また、入力トラフィックの DSCP および/または CoS 値を設定して、トラフィックがファブリックを出るときにそれらの値を保持できるようにすることもできます。

（注）
出力トラフィックのターゲットCoS値を保持するには、NDO ファブリック ポリシーの「CoS を保持する」ポリシーを構成する必要があります。

また、「DSCP ターゲット」および/または「ターゲット CoS」の値が DSCP マッピングと CoS マッピングの両方の一部として設定されている場合、DSCPマッピングで指定された値が優先されます。

マッピングごとに、次のフィールドを指定できます：

- **Dot1P から** – CoS 範囲の開始。
- **Dot1P へ** – CoS 範囲の終わり。
- **DSCP ターゲット** – 出力トラフィックのために保持される入力トラフィックに設定する DSCP 値。
- **ターゲット CoS** – 「CoS を保持」が有効になっている場合に、出力トラフィックのために保持される入力トラフィックに設定する CoS 値。
- **優先度** – トラフィックが割り当てられる QoS 優先度クラス。

マッピングを指定したら、チェックマーク アイコンをクリックして保存します。次に、**[+Cos マッピングの追加（+Add Cos Mappings）]** をクリックして、同じポリシー内に追加のマッピングを提供できます。

g) **[追加（Add）]** をクリックしてポリシーを保存し、テンプレート ページに戻ります。

h) この手順を繰り返して、ルート コントロール ポリシーの追加のルート マップを作成します。

ステップ 7 DHCP リレー ポリシーの作成。

このポリシーは、包括的なDHCP リレーユース ケースの一部です。このセクションにある情報を参照資料として使用することができます。しかし資料のDHCPリレー （217 ページ）章の 機能とユース ケース セクションの全てのステップのセットに従うことをおすすめします。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[DHCP リレー ポリシー（DHCP Relay Policy）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) **[プロバイダーの追加（Add Provider）]** をクリックして、エンドポイントによって発信されたDHCP 要求をリレーする DHCP サーバーを構成します。
e) プロバイダ タイプを選択します。

リレー ポリシーを追加するときには、次の 2 つのタイプのうちの 1 つを選択できます。

- アプリケーション EPG ：DHCP 要求をリレーする DHCP サーバーを含むアプリケーション EPG を指定します。
- L3 外部ネットワーク — ファブリックの外部のネットワークの場所 でもあるDHCP サーバーが接続されている場所へのアクセスに使用されるL3Outに関連付けられた外部EPGを指定します。

（注）
Orchestrator をサイトにまだ展開していない場合でも、Orchestratorで作成され、指定したテナントに割り当てられている EPG または外部 EPG を選択できます。展開されていない EPG を選択した場合でも、DHCP リレー構成を完了することができますが、リレーが使用可能になる前に EPG を展開する必要があります。

f) **[アプリケーション EPG を選択（Select an Application EPG）]** または **[外部 EPG を選択（Select an External EPG）]**（選択したプロバイダータイプに基づく）をクリックし、プロバイダーEPGを選択します。
g) **[DHCP サーバ アドレス]** フィールドに、DHCP サーバの IP アドレスを入力します。
h) 必要に応じて、**DHCP サーバー VRF プリファレンス** オプションを有効にします。

この機能は、Cisco APIC リリース 5.2（4）に紹介されています。必要な使用例の詳細については、Cisco APIC 基本構成ガイドを参照してください。

i) **[OK]** をクリックして、プロバイダー情報を保存します。
j) 同じDHCPリレーポリシー内の追加のプロバイダーについて、前のサブステップを繰り返します。
k) このステップを繰り返して、追加の DHCP リレー ポリシーを作成します。

ステップ 8 DHCP オプション ポリシーの作成。

このポリシーは、包括的な DHCP リレーの使用例の一部です。このセクションにある情報を参照資料として使用することができます。しかし資料のDHCPリレー （217 ページ）章の 機能とユース ケース セクションの全てのステップのセットに従うことをおすすめします。

a) **[+オブジェクトの作成]** ドロップダウンから、**[DHCP オプション ポリシー]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション)**[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。

d) [Add Option] をクリックします。
e) オプションの詳細を入力します。

DHCP オプションごとに、以下を指定します：

- **Name** – 技術的には要求されていませんが、RFC 2132 にリストされたオプションに同じ名前を使用することをお勧めします。

  たとえば、ネーム サーバ が挙げられます。

- **ID** – オプションが値を要求した場合はそれを指定します。

  たとえば、[ネーム サーバ] オプションのクライアントに使用可能なネーム サーバのリスト。

- **Data** – オプションが値を要求した場合はそれを指定します。

  たとえば、[ネーム サーバ] オプションのクライアントに使用可能なネーム サーバのリスト。

f) [OK] をクリックして保存します。
g) 同じ DHCP オプション ポリシー内の追加オプションについて、前のサブステップを繰り返します。
h) このステップを繰り返して、追加の DHCP オプション ポリシーを作成します。

ステップ 9 IGMP インターフェイス ポリシーを作成します。

IGMP スヌーピングは、ブリッジ ドメイン内の IP マルチキャスト トラフィックを調べて、該当する受信側が常駐するポートを検出します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセスブリッジ ドメイン環境における帯域幅消費量を削減し、ブリッジ ドメイン全体へのフラッディングを回避します。

ACI ファブリックでの IGMP スヌーピングの詳細については、使用しているリリースの *Cisco APIC Layer 3 Networking Configuration Guide* の「IGMP Snooping」の章を参照してください。

a) **[+オブジェクトの作成]** ドロップダウンから、**[IGMP インターフェイス ポリシー]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) ポリシーの詳細を入力します。

- **バージョン 3 ASM を許可** – SSM 範囲外のマルチキャスト グループの IGMP バージョン 3 送信元固有レポートの受け入れを許可します。この機能がイネーブルの場合、グループが設定された SSM 範囲外であっても、グループと送信元の両方を含む IGMP バージョン 3 レポートを受信すると、スイッチは（S,G）mroute エントリを作成します。ホストが SSM 範囲外の（*,G）レポートを送信する場合、または SSM 範囲の（S,G）レポートを送信する場合、この機能は不要です

- **高速脱退** – デバイスからグループ固有のクエリーが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間を最小限にできるオプション。高速脱退を有効にすると、デバイスではグループに関する脱退メッセージの受信後、ただちにマルチキャスト ルーティング テーブルからグループ エントリが削除されます。デフォルトではディセーブルになっています。

  これは、所定のグループに対する BD/インターフェイスの背後にただ 1 つの受信者しか存在しない場合に使用します。

- **レポート リンクローカル グループ** – 224.0.0.0/24 に含まれるグループに対して、レポート送信を有効にします。非リンク ローカル グループには、常にレポートが送信されます。デフォルトでは、リンク ローカル グループにレポートは送信されません。
- **IGMP バージョン**–ブリッジ ドメインまたはインターフェイスでイネーブルにする IGMP のバージョン。有効な IGMP バージョンは 2 または 3 です。デフォルトは 2 です。
- **高度な設定** – このセクションの隣の→をクリックして、展開してください。
  - **グループ タイムアウト** – ルータによって、ネットワーク上にグループのメンバーまたは送信元が存在しないと見なされるまでのグループ メンバーシップ インターバル。有効範囲は 3 ～ 65,535 秒です。デフォルト値は 260 秒です。
  - **クエリ インターバル** – IGMP ホスト クエリ メッセージの送信頻度を設定します。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 125 秒です。
  - **クエリ応答インターバル** – IGMP クエリでアドバタイズされる応答時間を設定します。有効範囲は 1 ～ 25 秒です。デフォルトは 10 秒です。
  - **最終メンバー カウント** – ホストの Leave メッセージを受信してから、IGMP クエリーが送信される回数を設定します。有効範囲は 1 ～ 5 です。デフォルトは 2 です。
  - **最終メンバー応答時間** – メンバーシップ レポートを送信してから、ソフトウェアがグループ ステートを解除するまでのクエリー インターバルを設定します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
  - **スタートアップ メンバー カウント** – マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、起動時に送信されるクエリー数に対してスヌーピングを設定します。有効範囲は 1 ～ 10 です。デフォルト値は 2 メッセージです。
  - **スタートアップ クエリ インターバル** – 起動時の IGMP スヌーピング クエリ間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。デフォルト値は 125 秒です。
  - **クエリア タイムアウト** – クエリアとして処理を引き継ぐかどうかをソフトウェアが判断するための、クエリア タイムアウト値を設定します。有効範囲は 1 ～ 65,535 秒です。デフォルト値は 255 秒です。
  - **ロバストネス変数** – ロバストネス変数を設定します。ネットワークのパケット損失が多い場合は、この値を大きくします。有効値の範囲は、1 ～ 7 です。デフォルトは 2 です。
  - **ステート リミットルート マップ** – 予約済みマルチキャスト エントリ機能で使用

    ルート マップ ポリシーは、ステップ 2 の説明に従ってすでに作成されている必要があります。
  - **レポート ポリシー ルート マップ** – ルート マップ ポリシーに基づく IGMP レポートのポリシーにアクセスします。IGMP グループ レポートは、ルートマップで許可されたグループに対してのみ選択されます

    ルート マップ ポリシーは、ステップ 2 の説明に従ってすでに作成されている必要があります。

- **スタティック レポート ルート マップ** – マルチキャスト グループを発信インターフェイスに静的にバインドし、スイッチ ハードウェアで処理されます。グループ アドレスのみを指定した場合は、（*, G）ステートが作成されます。送信元アドレスを指定した場合は、（S, G）ステートが作成されます。グループ プレフィックス、グループ範囲、および送信元プレフィックスを示すルートマップ ポリシー名を指定できます。IGMPv3 をイネーブルにした場合にのみ、（S, G）ステートに対して送信元ツリーが作成されます。

  ルート マップ ポリシーは、ステップ 2 の説明に従ってすでに作成されている必要があります。

- **最大マルチキャスト エントリ** – IGMP レポートによって作成される BD またはインターフェイスの mroute 状態を制限します。デフォルトは無効にされ、制限は設定されません。有効な範囲は 1 ～ 4294967295 です。

e) このステップを繰り返して、追加の IGMP インターフェイス ポリシーを作成します。

ステップ 10 MLD スヌーピング ポリシーを作成します。

マルチキャスト リスナー検出（MLD）スヌーピングにより、ホストとルータ間で IPv6 マルチキャスト トラフィックを効率的に配信できます。これは、MLD クエリまたはレポートを送受信したポートのサブセットにブリッジ ドメイン内の IPv6 マルチキャスト トラフィックを制限する レイヤ 2 機能です。このように、MLD スヌーピングは、マルチキャスト トラフィックの受信に関心を示しているノードがないネットワークのセグメントでは帯域幅を節約できるという利点があります。これにより、ブリッジ ドメインでフラッディングが生じることがなく、帯域幅の使用量が削減され、ホストとルータで不要なパケット処理を節約できます。

ACI ファブリックでの MLD スヌーピングの詳細については、使用しているリリースの *Cisco APIC Layer 3 ネットワーキング構成ガイド* の「MLD スヌーピング 」の章を参照してください。

a) **[+オブジェクトの作成]** ドロップダウンから、**[MLD スヌーピング ポリシー]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) ポリシーの詳細を入力します。

- **Admin State** – MLD スヌーピング機能を有効または無効にします。
- **高速脱退コントロール** – ブリッジ ドメインごとに高速脱退機能をオンまたはオフにできます。これは MLDv2 ホストに適用され、1 つのホストだけがそのポートの背後で MLD を実行することがわかっているポートで使用されます。

  デフォルトは無効です。

- **クエリア コントロール** – MLD スヌーピング クエリア処理を有効または無効にします。MLD スヌーピング クエリアは、マルチキャスト トラフィックをルーティングする必要がないため、PIM および MLD を構成していないブリッジ ドメイン内で MLD スヌーピングをサポートします。

  デフォルトは無効です。

- **クエリア バージョン** – クエリア バージョンを選択できます。

  デフォルトは、Version2です。

- **高度な設定** – このセクションの隣の→をクリックして、展開してください。
  - **クエリ インターバル** – MLD ホスト クエリ メッセージをソフトウェアが送信する頻度を設定します。有効範囲は 1 ～ 18,000 秒です。

    デフォルト値は 125 秒です。
  - **クエリ応答インターバル** – MLD クエリでアドバタイズされる応答時間を設定します。有効範囲は 1 ～ 25 秒です。

    デフォルトは 10 秒です。
  - **最終メンバー クエリ インターバル** – メンバーシップ レポートを送信してから、ソフトウェアがグループ ステートを削除するまでのクエリー応答時間を設定します。有効範囲は 1 ～ 25 秒です。

    デフォルト値は 1 秒です。
  - **スタート クエリ カウント** – マルチキャスト トラフィックをルーティングする必要がないため、PIM を有効にしていない場合に、起動時に送信される多くのクエリに対してスヌーピングを構成します。有効範囲は 1 ～ 10 です。

    デフォルトは 2 です。
  - **スタート クエリ インターバル —** マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、起動時のスヌーピング クエリー インターバルを構成します。有効範囲は 1 ～ 18,000 秒です。

    デフォルト値は 31 秒です。

e) 追加のMLD スヌーピング ポリシーを作成するために、このステップを繰り返します。

ステップ 11 テンプレートの変更内容を保存するために**[保存（Save）]** をクリックします。

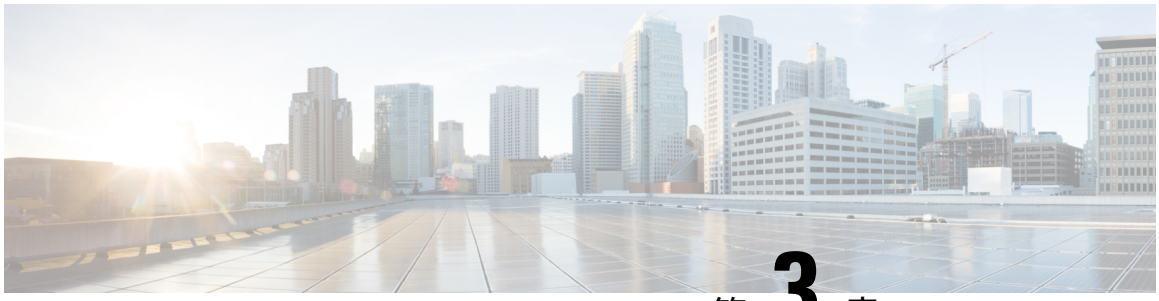
（注）
テンプレートを 1 つ以上のサイトに保存（または展開）すると、オーケストレータ は、指定されたノードやインターフェースがサイトに対して有効であることを確認し、エラーを返します。

ステップ 12 関連サイトに新しいテンプレートを展開するために**[展開（Deploy）]** をクリックします。

テナント ポリシー テンプレートの展開方法とアプリケーション テンプレートの展開方法は同じです。

以前にこのテンプレートを展開したが、それ以降に変更を加えていない場合は、**[展開]** の概要に変更がないことが示され、テンプレート全体を再展開することを選択できます。この場合は、この手順をスキップできます。

或いは、**[サイトに展開 (Deploy to Sites)]** ウィンドウには、サイトに展開される構成の違いの概要が表示されます。この場合、構成の違いのみがサイトに展開されることにご注意ください。テンプレート全体を再展開したい場合、違いを同期するために1回展開をする必要があります。そして、前のパラグラフに記されている通り、構成全体をプッシュするためにまた再展開する必要があります。



第 3 章

スキーマ

スキーマとテンプレート設計上の考慮事項

Nexus ダッシュボード オーケストレータには、1 つ以上のポリシーを一緒に定義し、それらを 1 つ以上のサイトに同時に展開できる多数のポリシー テンプレートが用意されています。これらには、テナント ポリシー テンプレート、ファブリックおよびファブリック 情報技術 ポリシー テンプレート、モニタリング テンプレートおよびアプリケーション テンプレートが含まれます。スキーマは、アプリケーション ポリシーの定義に使用されるアプリケーション テンプレートの集合であり、各テンプレートは特定のテナントに割り当てられます。展開の使用例に固有のスキーマとアプリケーションテンプレートの構成を作成する際に、複数のアプローチを実行できます。ここでは、マルチサイト環境でスキーマ、テンプレート、およびポリシーを定義する方法を決定する際に実行できる、いくつかの簡単な設計方針について説明します。

スキーマを設計する際には、スキーマ、テンプレート、およびスキーマあたりのオブジェクトの数に対してサポートされているスケーラビリティ制限を考慮する必要があることに注意して

ください。検証済みスケーラビリティ制限の詳細については、お使いのリリースの『*Cisco Multi-Site Verified Scalability Guides*』を参照してください。

アプリケーション テンプレート

Nexus ダッシュボード オーケストレータ では、それぞれ特定の目的のために設計されたアプリケーションテンプレートとも知られている3種類のスキーマテンプレートを使用できます。

- **ACI マルチクラウド** — Cisco ACI オンプレミスおよびクラウド サイトに使用されるテンプレート。このテンプレートは、次の 2 つの展開タイプをサポートしています。
  - [マルチサイト（Multi-Site）]：テンプレートは、単一のサイト（サイトローカル ポリシー）または複数のサイト（拡張ポリシー）に関連付けることができます。マルチサイト ネットワーク（ISN）または複数のサイトの間にテンプレートとオブジェクト ストレッチングを許可するために VXLAN サイト間通信用にオプションを選択する必要があります。
  - [自律（Autonomous）]：テンプレートは、独立して運用され、サイト間ネットワークを介して接続されていない（サイト間 VXLAN 通信なしの）1 つ以上のサイトに関連付けることができます。

    自律サイトは、孤立されていると定義されていてサイト間接続が一切ないので、サイトに渡ってシャドウ オブジェクト 構成はありません。そしてpctag のクロスプログラムまたは、サイト間トラフィック フローのスパイン スイッチ内に VNID はありません。

    自律 テンプレートは、かなり高い展開拡張を許可します。

  次のセクションでは、主にこのタイプのテンプレートに焦点を当てます。
- **[NDFC]**：Cisco Nexus Dashboard ファブリック コントローラ（以前のデータセンター ネットワーク マネージャ）サイト用に設計されたテンプレート。

  このガイドでは、オンプレミスの Cisco ACI ファブリック向けの Nexus Dashboard Orchestrator 構成について説明しています。Cisco NDFC サイトの操作については、代わりに『*Cisco Nexus Dashboard Orchestrator Configuration Guide for NDFC Fabrics*』を参照してください。
- **[クラウド ローカル（Cloud Local）]**：Google Cloud サイト接続など、特定のクラウド ネットワーク コントローラのユース ケース向けに設計されたテンプレートであり、複数のサイト間で拡張することはできません。

  このガイドでは、オンプレミスの Cisco ACI ファブリック向けの Nexus Dashboard Orchestrator 構成について説明しています。クラウド ネットワーク コントローラ ファブリックの操作については、代わりに Nexus Dashboard Orchestrator のユース ケース ライブラリを参照してください。

スキーマとアプリケーションテンプレートを作成するときは、次の単純なアプローチのいずれかを採用することを選択できます。

- **[単一テンプレートの展開（Single Template Deployment）]**

スキーマ設計の最も簡単なアプローチは、単一のスキーマで単一のテンプレートを導入することです。単一のテンプレートを含む単一のスキーマを作成し、そのテンプレートにすべてのVRF、ブリッジドメイン、EPG、コントラクト、およびその他の要素を追加して、1 つまたは複数のサイトに展開することができます。

Multi-Site スキーマを作成する最も簡単な方法は、同じスキーマとテンプレート内にすべてのオブジェクトを作成することです。ただし、サポートされているスキーマの数に制限があるため、このアプローチは大規模な展開に適していない場合があります。これは、これらの制限を超える可能性があります。

また、このアプローチでは、テンプレートで定義されたすべてのオブジェクトが「ストレッチオブジェクト」になり、テンプレートに加えられたすべての変更が、そのようなテンプレートに関連付けられたすべてのサイトに常に同時に展開されることに注意してください。

- **[ネットワーク分離での複数テンプレート（Multiple Templates with Network Separation）]**

  スキーマ設計のもう1つのアプローチは、ネットワーク オブジェクトをアプリケーション ポリシー設定から分離することです。ネットワーク オブジェクトには、VRF、ブリッジドメイン、サブネットなどがあり、アプリケーションポリシーオブジェクトには EPG 、コントラクト、フィルタ、外部 EPG、およびサービス グラフが含まれます。

  最初に、ネットワーク要素を含むスキーマを定義します。すべてのネットワーク要素を含む単一のスキーマを作成するか、または、それらを参照するアプリケーション、またはネットワークが拡張するサイトに基づいて、複数のスキーマに分割します。

  その後、各アプリケーションのポリシー オブジェクトを含む、1つ以上の個別のスキーマを定義します。この新しいスキーマは、前のスキーマで定義されたブリッジ ドメインなどのネットワーク要素を参照できます。

  ポリシー スキーマとテンプレートを作成して展開すると、ネットワーク スキーマのネットワーキング オブジェクトに、ポリシー スキーマ要素による外部参照の数が表示されます。外部参照を含むオブジェクトは、リボンのアイコンでも示されます。

  この方法で設計されたスキーマは、ネットワーキング オブジェクトをポリシー オブジェクトから論理的な分離します。ただし、これにより、各スキーマで外部参照されたオブジェクトの追跡はさらに複雑になります。

- **[オブジェクトの関係性に基づく複数テンプレート（Multiple Templates Based On Object Relationships）]**

  共有オブジェクト参照を使用して複数のスキーマを設定する場合、それらのオブジェクトを変更する際に注意を払うことが大切です。たとえば、共有ネットワーク オブジェクトを変更または削除すると、1 つ以上のサイトのアプリケーションに影響を与える可能性があります。そのため、サイトとそのアプリケーションで使用されているオブジェクト(VRF、BD、EPG、コントラクト、フィルタなど) のみを含む、個々のサイトのためのテンプレートを作成するのがよいでしょう。それから、共有オブジェクトを含む別のテンプレートを作成します。

  例えば、サイト1にローカルなオブジェクトとそのサイトだけに展開されているテンプレートのみを含む[サイト（Site1）]テンプレートを作成することができます。同様に、[サイト

2 （site2）]テンプレートにはSite2に関連するオブジェクトのみが含まれており、そのサイトのみに展開されます。これらのテンプレートのいずれかのオブジェクトに変更を加えても、他のテンプレートのオブジェクトには影響しません。そして、サイト間で共有されているオブジェクトが含まれる**共有**テンプレートを作成することができます。

このシナリオは、次のテンプレート レイアウトを持つ追加サイトに拡張できます。

- サイト 1 テンプレート
- サイト 2 テンプレート
- サイト 3 テンプレート
- サイト 1 と 2 の共有テンプレート
- サイト 1 と 3 の共有テンプレート
- サイト 2 と 3 の共有テンプレート
- すべての共有テンプレート

同様に、展開されているサイトに基づいてオブジェクトを分離するのではなく、個々のアプリケーションに基づいてスキーマとテンプレートを作成することもできます。これにより、各アプリケーションプロファイルを簡単に特定し、それらをスキーマとサイトにマッピングし、さらには各アプリケーションをローカルまたは拡張されたサイト全体のものとして設定することができます。

ただし、これはスキーマごとのテンプレート数の制限（使用しているリリースの Verified Scalability Guide に記載）をすぐに越えてしまう可能性があるため、複数の組み合わせに対応するために追加のスキーマを作成することが必要になります。これにより、複数のスキーマとテンプレートが追加され、さらに複雑になりますが、サイトまたはアプリケーションに基づいてオブジェクトを正確に分離できます。

ファブリック ポリシー テンプレート

リリース 4.0（1）では、3 種類のアプリケーションテンプレートに加えて、ファブリック全体のポリシー用に設計された 3 つの新しいテンプレートが追加されています。

- **[ファブリック ポリシー（Fabric Policies）]** テンプレートは、次のファブリック全体のポリシーの管理に使用できます。
  - VLAN Pool
  - 物理ドメイン
  - SyncE インターフェイス ポリシー
  - インターフェイス設定
  - ノード 設定
  - ポッド設定
  - MACsec

- NTP ポリシー
- PTP ポリシー
- QoS DSCP ポリシー
- QoS SR-MPLS ポリシー
- QoS クラス ポリシー

詳細については、ファブリック ポリシーを作成 （87 ページ） を参照してください。

- **[ファブリック情報技術ポリシー（Fabric Resource Policies）]** テンプレートは、次のファブリック全体のポリシーの管理に使用できます。
  - 物理インターフェイス
  - ポート チャネル インターフェイス
  - 仮想ポート インターフェイス
  - ノードプロファイル

  これらのテンプレート参照ポリシーはファブリック ポリシー テンプレートで定義されているため、これらのテンプレートを最初に作成して展開する必要があります。詳細については、ファブリック 技術情報 ポリシーを作成 （101 ページ） を参照してください。
- **[モニタリング ポリシー（Monitoring Policy）]** テンプレートは、`[テナント SPAN（Tenant SPAN）]` または `[アクセス SPAN（）]` ポリシーの管理に使用できます。

  詳細については、モニタリング ポリシーを作成 （106 ページ） を参照してください。

テンプレート デザイン ベストプラクティス

リリース 4.0（1）以降、Nexus ダッシュボード オーケストレータは、テンプレートの設計と展開に関して、いくつかのベストプラクティスを検証して適用します。作成するテンプレートの種類に関係なく、次の点に注意してください。

- すべてのポリシー オブジェクトは、依存関係に応じた順序で**[展開（deployed）]**する必要があります。

  たとえば、ブリッジ ドメイン（BD）を作成するときは、それを VRF に関連付ける必要があります。この場合、BD には VRF 依存関係があるため、VRF は BD の前または一緒にファブリックに展開する必要があります。これらの 2 つのオブジェクトが同じテンプレートで定義されている場合、Orchestrator は展開時に VRF が最初に作成され、ブリッジ ドメインに関連付けられるようにします。

  ただし、これら 2 つのオブジェクトを別々のテンプレートで定義し、最初に BD を使用してテンプレートを展開しようとすると、関連付けられている VRF がまだ展開されていないため、Orchestrator は検証エラーを返します。この場合、最初に VRF テンプレートを展開してから、BD テンプレートを展開する必要があります。

- すべてのポリシー オブジェクトは、依存関係に応じた順序で**[展開解除（undeployed）]**する必要があります。展開された順序と逆の順序で展開する必要があります。

  上記の結果から、テンプレートを展開解除するときは、他のオブジェクトが依存しているオブジェクトを展開解除してはなりません。たとえば、VRF が関連付けられている BD を展開解除する前に、VRF を展開解除することはできません。

- 複数のテンプレートにまたがる循環的な依存関係は許可されません。

  ブリッジ ドメイン (`bd1`) に関連付けられた VRF (`vrf1`) の場合を考えてみます。これは、次に EPG (`epg1`) に関連付けられます。`[テンプレート 1（template1）]` に `vrf1` を作成してそのテンプレートをデプロイし、次に `[テンプレート 2（template2）]` に `bd1` を作成してそのテンプレートをデプロイすると、オブジェクトが正しい順序でデプロイされるため、検証エラーは発生しません。ただし、その後 `[テンプレート1（template1）]` に `epg1` を作成しようとすると、2 つのテンプレート間に循環依存関係が作成されるため、Orchestrator は、EPG の `[テンプレート1（template1）]` 追加を保存することを許可しません。

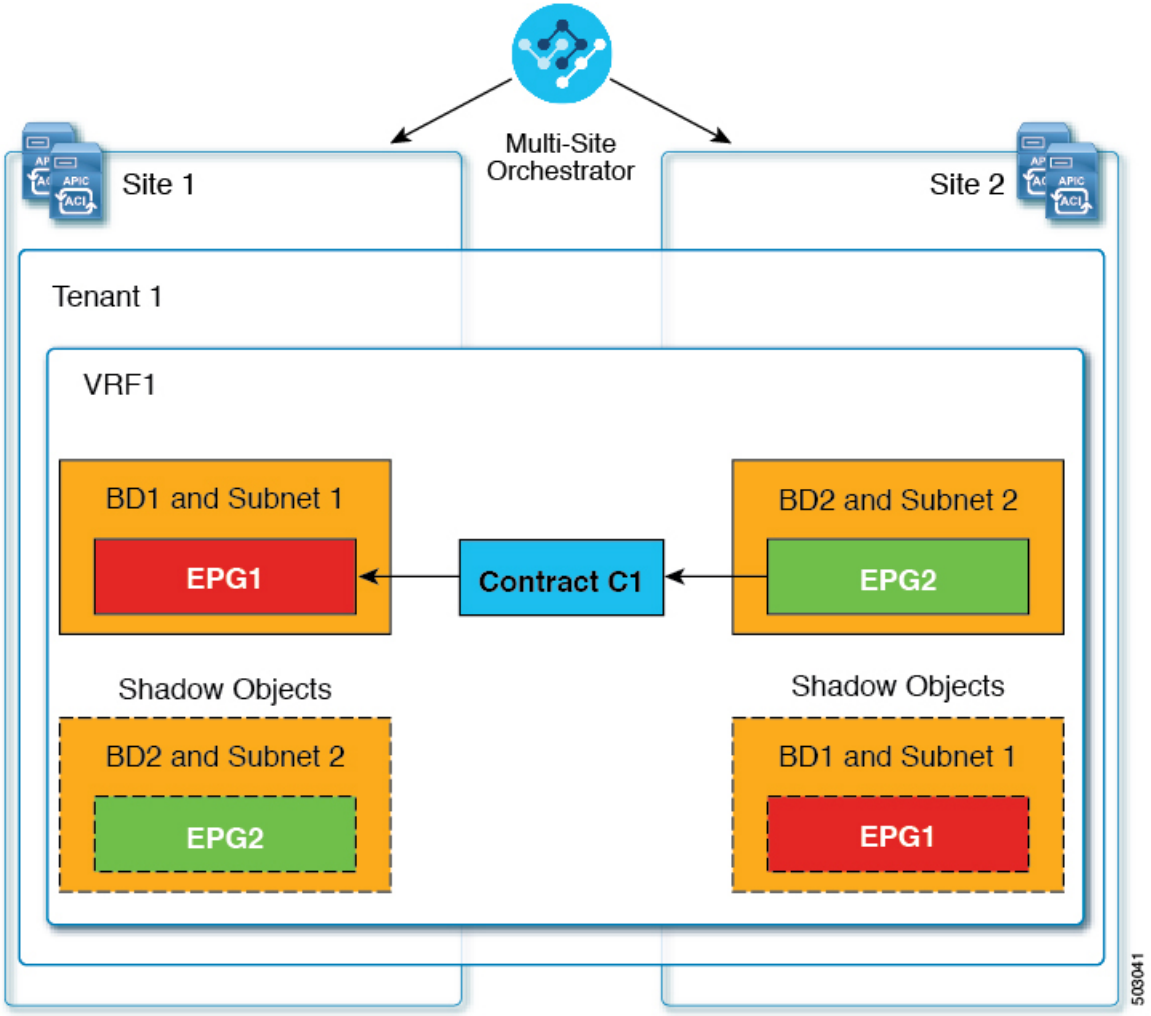
シャドウ オブジェクト

プロバイダとコンシューマーが異なる VRF にあり、テナント コントラクトを介して通信する拡張 VRF または共有サービスの使用例で、サイト ローカル EPG 間にコントラクトが存在する場合、EPG とブリッジ ドメイン (BD) はリモート サイトにミラーリングされます。ミラーされたオブジェクトは、これらのサイトのそれぞれのコントローラで展開されているかのように表示される一方で、実際にはサイトの 1 つでだけ展開されています。これらのミラーされたオブジェクトは、「シャドウ」オブジェクトと呼ばれます。

（注） シャドウ オブジェクトは、APIC GUI を使用して削除する必要があります。

たとえば、テナントと VRF が Site1 と Site2 の間でストレッチされ、プロバイダ EPG とそのブリッジ ドメインが Site2 のみに展開され、コンシューマ EPG とそのドメインが Site1 のみに展開される場合、対応するシャドウ ブリッジ ドメインと EPG は次の図のように展開されます。これらは、直接展開されている各サイトでの名前と同じ名前で表示されます。

図 *1* : 基本的なシャドウ *EPG*



次のオブジェクトはシャドウ オブジェクトになる場合があります。

- VRF
- ブリッジ ドメイン (BD)
- L3Out
- 外部 EPG
- アプリケーション プロファイル
- アプリケーション EPG
- コントラクト（ハイブリッド クラウド展開）

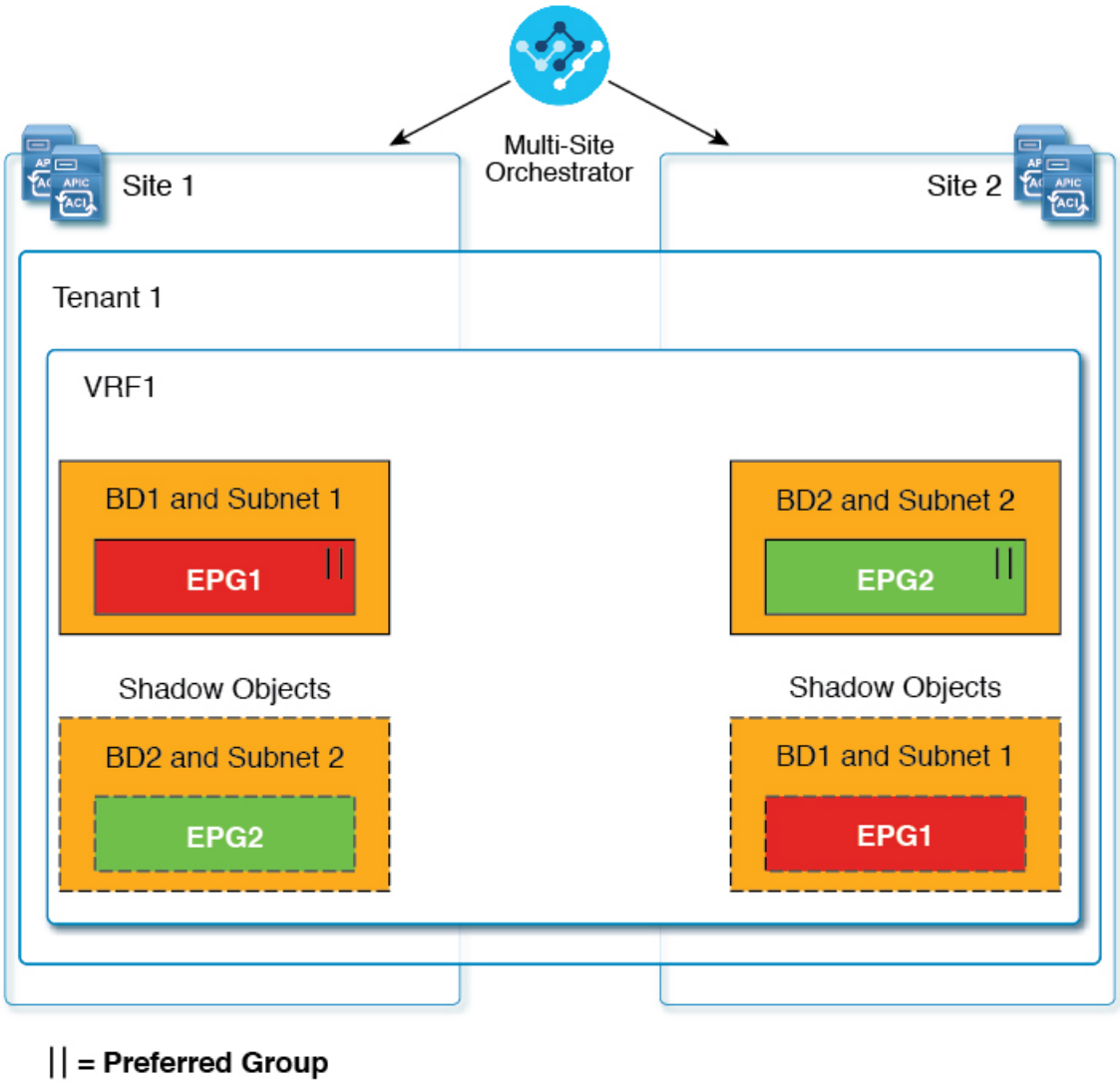
ファブリックが APIC リリース 5.0(2) 以降で実行されている場合、APIC GUI でシャドウ オブジェクトを選択すると、 が表示されます。これはサイト間ポリシーをサポートするために、MSC からプッシュ

されたシャドウ オブジェクトです。このオブジェクトを変更または削除しないでください。 メイン GUI ペイン上部の警告。さらに、VMM ドメインの一部ではないシャドウ EPG にはスタティック ポートがないいぽプで、シャドウ BD は、APIC GUI で **[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)]**のオプションがあります。

シャドウ オブジェクトのその他の使用例

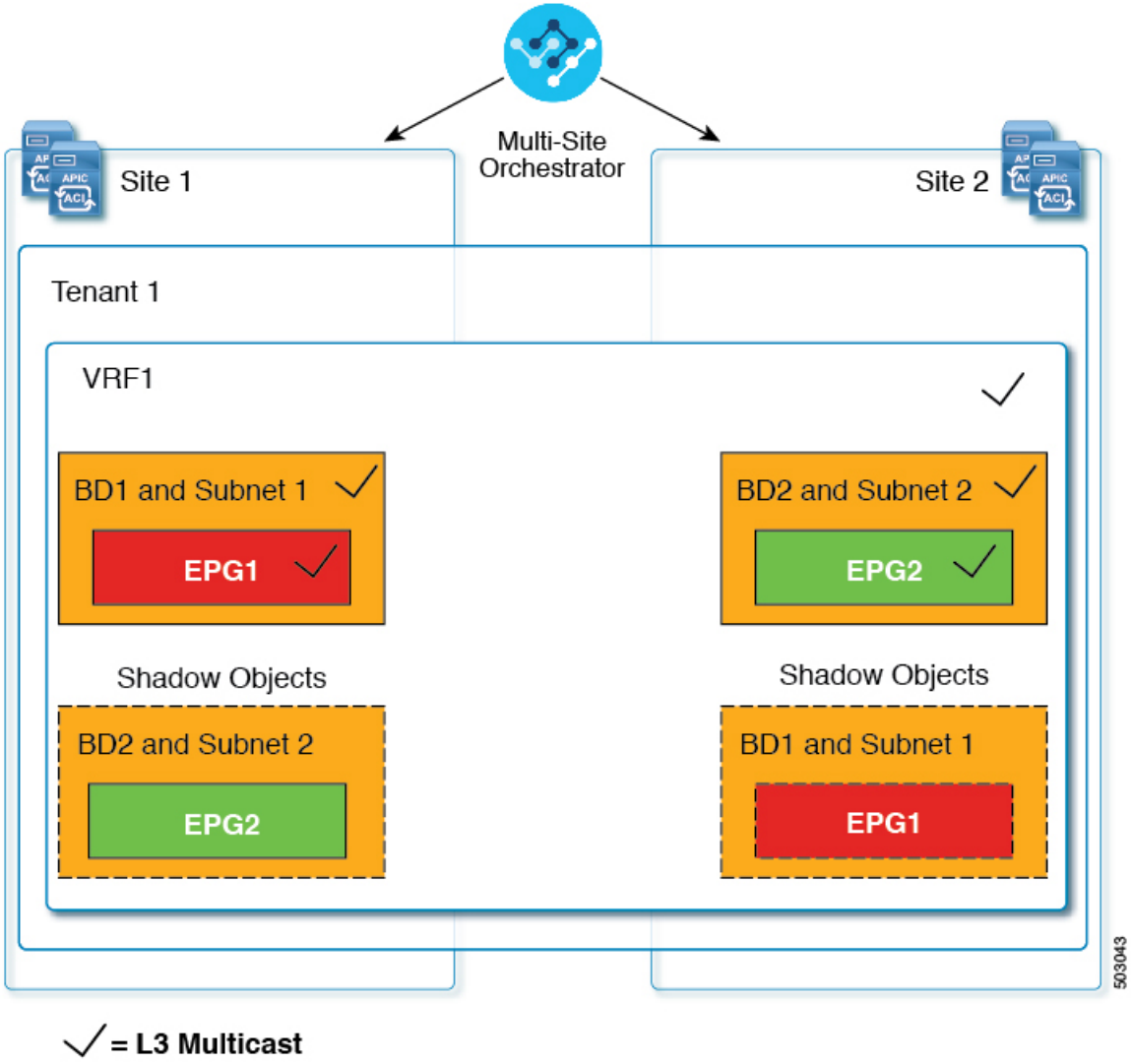
シャドウ オブジェクトは、次の図に示すように、[優先グループ (Preferred Group)]、[vzAny]、[レイヤ3マルチキャスト (Layer 3 Multicast)]、およびハイブリッド クラウドなど、さまざまな使用例でも作成されます。

図 *2:* 優先グループ



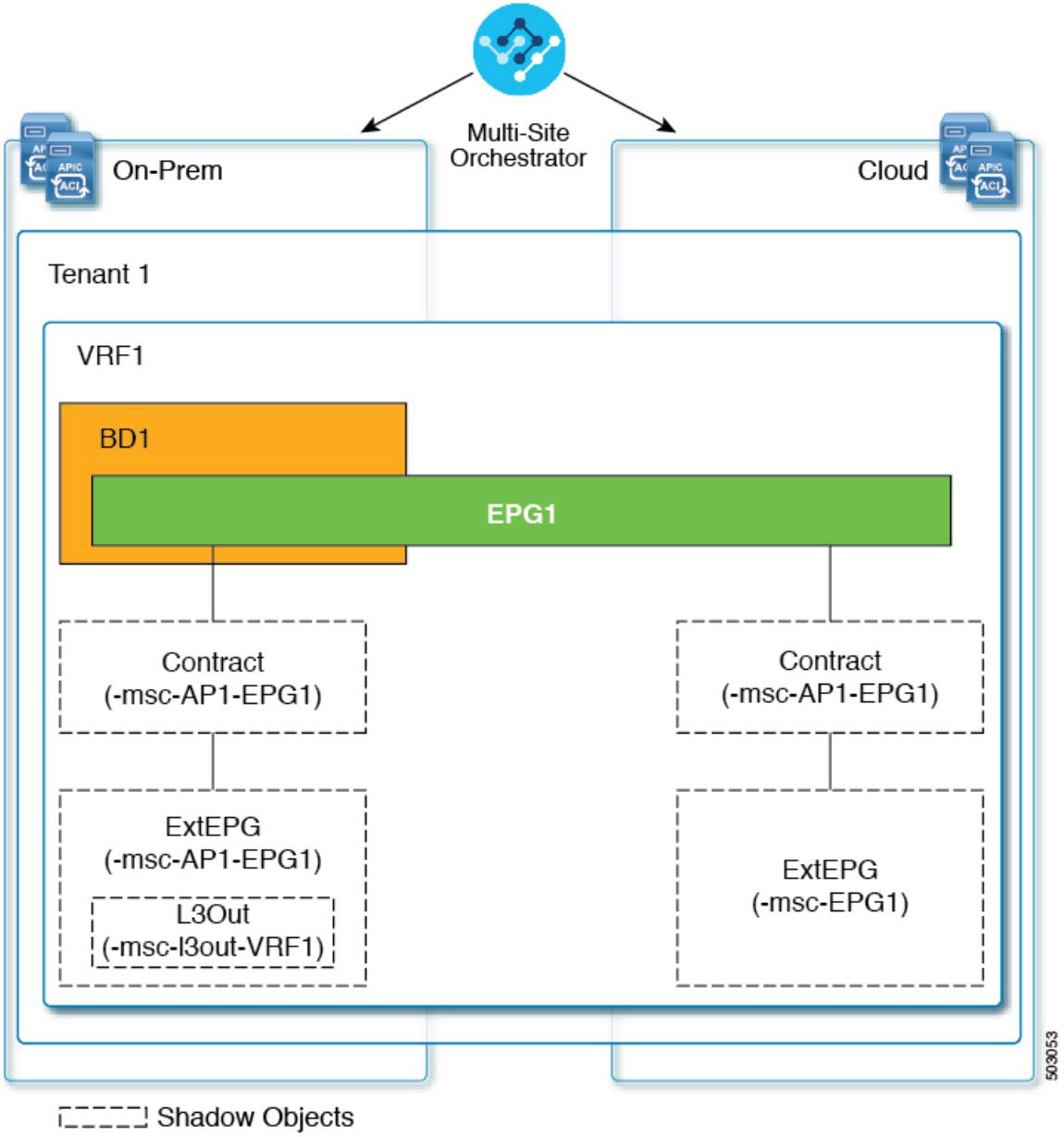
マルチキャストの場合、シャドウ オブジェクトは、マルチキャスト ソースが接続され、オプションが EPG レベルで明示的に設定されている EPG/BDに対してのみ作成されます。

図 *3 : L3* マルチキャスト



ハイブリッドクラウド展開の場合、ストレッチされたオブジェクトであっても、暗黙のコントラクトが存在するシャドウ オブジェクトを作成します。たとえば、EPG がオンプレミス サイトとクラウドサイトの間でストレッチされた場合、シャドウ外部 EPG は各サイトで作成され、ストレッチされた EPG とシャドウ外部 EPG の間に暗黙的なシャドウ コントラクトが作成されます。

図 *4:* ハイブリッドクラウド



Cisco APIC リリース 5.2(3) 以降、シャドウ オブジェクトは Cisco APIC GUI で一意のアイコンで示されます。通常の Orchestrator で作成されたオブジェクトは緑のクラウドの記号で表示されますが、シャドウ オブジェクトはグレーのクラウドのアイコンで表示されます。

APIC GUI でシャドウ オブジェクトを非表示にする

APIC リリース 5.0(2) 以降では、オンプレミス サイトの APIC GUI で Nexus Dashboard Orchestrator によって作成されたシャドウ オブジェクトを表示するか非表示にするかを選択できます。Cloud ネットワーク コントローラ のシャドウ オブジェクトは常に非表示です。

GUI からシャドウ オブジェクトを非表示にするには、次の点に注意してください。

- このオプションは、Orchestratorからグローバルに設定することはできません。また、このセクションで説明するように、各サイトの APIC で直接設定する必要があります。
- シャドウ オブジェクトを表示するオプションはすべての新しい APIC リリース 5.0(2) のインストールとアップグレードのデフォルトでオフに設定されているため、以前に表示されていたオブジェクトが非表示になる可能性があります。
- シャドウ オブジェクトの非表示は、Orchestrator リリース 3.0 (2) 以降で使用可能な、Nexus Dashboard Orchestrator によって設定されるフラグに依存しています。
  - シャドウ オブジェクトが以前の Orchestrator バージョンによって展開されている場合は、必要なタグがなく、APIC GUI に常に表示されます。
  - Shadow オブジェクトが Orchestrator バージョン 3.0(2) 以降で導入されている場合は、タグが付けられ、APIC GUI 設定を使用して非表示または表示にできます。
  - Nexus Dashboard Orchestrator をアップグレードする前に、各ファブリックを APIC リリース 5.0(2) にアップグレードすることをお勧めします。

    Nexus Dashboard Orchestrator をリリース 3.0(2) にアップグレードすると、APIC リリース 5.0(2) 以降を実行しているサイトに展開されたオブジェクトは、適切なタグでタグ付けされ、再展開しなくても、APIC GUI を使用して表示または非表示にできます。

    ファブリックの APIC の前に Orchestrator をアップグレードする場合、サイトのオブジェクトはタグ付けされず、フラグを設定するためにファブリックをアップグレードした後に設定を手動で再展開する必要があります。
- リリース 5.0(2) よりも前のリリースにファブリックをダウングレードした場合、シャドウオブジェクトは非表示にならず、APIC GUI に異なるアイコンが表示されることがあります。

手順

ステップ 1 サイトの APIC にログインします。

ステップ 2 右上隅にある **[マイ プロファイルの管理 (Manage my profile)]** アイコンをクリックし、**[設定 (Settings)]** を選択します。

ステップ 3 **[アプリケーション設定 (Application Settings)]** ウィンドウで、**[非表示のポリシーを表示 (Show Hidden Policies)]** チェックボックスをオンまたはオフにします。

この設定はユーザ プロファイルに保存され、ユーザごとに個別に有効または無効になります。

ステップ 4 その他の APIC サイトについては、このプロセスを繰り返します。

設定の同時更新

Nexus ダッシュボード オーケストレータ GUI は、同じサイトまたはスキーマオブジェクトでの同時更新が意図せずに相互に上書きされることがないようにします。自分が開いた後に別のユーザによって更新されたサイトまたはテンプレートに変更を加えようと、GUIはそれ以降の変更を拒否し、追加の変更を行う前にオブジェクトを更新するように求める警告を表示します。テンプレートを更新すると、その時点までに行った編集内容は失われるため、再度変更する必要があります。

ただし、既存のアプリケーションとの下位互換性を維持するために、デフォルトの REST API 機能は変更されていません。つまり、UI はこの保護を常に有効にしていますが、設定変更を追跡するためには、NDO の API コールに対しても明示的に有効にする必要があります。

（注） この機能を有効にする場合は、次の点に注意してください。

- このリリースでは、サイト オブジェクトとスキーマ オブジェクトの競合する設定変更の検出のみがサポートされています。
- `PUT` および `PATCH API` コールのみがバージョンチェック機能をサポートします。
- API コールでバージョン チェック パラメータを明示的に有効にしていない場合、NDO は内部的に更新を追跡しません。その結果、設定の更新は、後続の API コールまたは GUI ユーザの両方によって上書きされる可能性があります。

設定のバージョン チェックを有効にするには、使用している API エンドポイントの末尾に `enableVersionCheck = true` パラメータを追加して、API コールにこのパラメータを渡します。次の例をご覧ください。

`https://<mso-ip-address>/mso/api/v1/schemas/<schema-id>?`**`enableVersionCheck=true`**

例

スキーマ内のテンプレートの表示名を更新する簡単な例を使用して、 PUT または PATCH コールでバージョンチェック属性を使用する方法を示します。

最初に、変更するスキーマを GET します。これにより、コールの応答で現在の最新バージョンのスキーマが返されます。

```
{
    "id": "601acfed38000070a4ee9ec0",
    "displayName": "Schema1",
    "description": "",
    "templates": [
        {
            "name": "Template1",
            "displayName": "current name",
            [...]
        }
    ],
    "_updateVersion": 12,
    "sites": [...]
}
```

次に、リクエストURLに、2つの方法のいずれかで、enableVersionCheck = true を追加して、スキーマを変更します。

（注） ペイロードの _updateVersion フィールドの値が、元のスキーマで取得した値と同じであることを確認する必要があります。

- PUT API を使用して、更新されるスキーマ全体ペイロードとします。

```
PUT /v1/schemas/601acfed38000070a4ee9ec0?enableVersionCheck=true
```

```
{
    "id": "601acfed38000070a4ee9ec0",
    "displayName": "Schema1",
    "description": "",
    "templates": [
        {
            "name": "Template1",
            "displayName": "new name",
            [...]
        }
    ],
    "_updateVersion": 12,
    "sites": [...]
}
```

- PATCH API 操作のいずれかを使用して、スキーマ内のオブジェクトの 1 つに特定の変更を加えます。

```
PATCH /v1/schemas/601acfed38000070a4ee9ec0?enableVersionCheck=true
```

```
[
    {
        "op": "replace",
        "path": "/templates/Template1/displayName",
        "value": "new name",
        "_updateVersion": 12
```

```
        }
    ]
```

リクエストが行われると、APIは現在のスキーマバージョンを 1 ずつ増やし（12 から 13 など）、新しいバージョンのスキーマの作成を試みます。（enableVersionCheck が有効で）新しいバージョンがまだ存在しない場合、操作は成功し、スキーマは更新されます。別の API コールまたは UI がその間にスキーマを変更していた場合、操作は失敗し、API コールは次の応答を返します。

```
{
    "code": 400,
    "message": "Update failed, object version in the DB has changed, refresh your client
 and retry"
}
```

スキーマとテンプレートの作成

始める前に

- サイトに組み込むには、少なくとも 1 つの使用可能なテナントが必要です。

  詳細については、テナント と テナントポリシー （5 ページ） を参照してください。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 スキーマを新規作成します。

a) 左側のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

b) [スキーマ (Schema)] ページで、**[スキーマの追加 (Add Schema)]** をクリックします。

c) スキーマ作成ダイアログで、スキーマの **[名前 (Name)]** と説明（オプション）を入力し、**[追加（Add）]** をクリックします。

デフォルトでは、新しいスキーマは空であるため、1 つ以上のテンプレートを追加する必要があります。

ステップ 3 テンプレートを作成します。

a) スキーマのページで、**[新しいテンプレートの追加（Add New Template）]** をクリックします。

b) **[テンプレート タイプの選択（Select a Template type）]** ウィンドウで、ACI Multi-Cloud を選択し、**[追加（Add）]** をクリックします。

- [ACI マルチクラウド（ACI Multi-Cloud）] ：Cisco ACI オンプレミスおよびクラウド サイトに使用されるテンプレート。これにより、複数のサイト間でテンプレートとオブジェクトを拡張できます。このテンプレートは、次の 2 つの展開タイプをサポートしています。

- [マルチサイト（Multi-Site）]：テンプレートは、単一のサイト（サイトローカル ポリシー）または複数のサイト（拡張ポリシー）に関連付けることができます。マルチサイト ネットワーク（ISN）または複数のサイトの間にテンプレートとオブジェクト ストレッチングを許可するために VXLAN サイト間通信用にオプションを選択する必要があります。
- [自律（Autonomous）]：テンプレートは、独立して運用され、サイト間ネットワークを介して接続されていない（サイト間 VXLAN 通信なしの）1 つ以上のサイトに関連付けることができます。

  自律サイトは、孤立されていると定義されていてサイト間接続が一切ないので、サイトに渡ってシャドウ オブジェクト 構成はありません。そしてpctag のクロスプログラムまたは、サイト間トラフィック フローのスパイン スイッチ内に VNID はありません。

  自律 テンプレートは、かなり高い展開拡張を許可します。

次のセクションでは、主にこのタイプのテンプレートに焦点を当てます。

- **[NDFC]**：Cisco Nexus Dashboard ファブリック コントローラ（以前のデータセンター ネットワーク マネージャ）サイト用に設計されたテンプレート。

  このガイドでは、オンプレミスの Cisco ACI ファブリック向けの Nexus Dashboard Orchestrator 構成について説明しています。Cisco NDFC サイトの操作については、代わりに『*Cisco Nexus Dashboard Orchestrator Configuration Guide for NDFC Fabrics*』を参照してください。

- **[クラウド ローカル（Cloud Local）]**：Google Cloud サイト接続など、特定のクラウド ネットワーク コントローラのユース ケース向けに設計されたテンプレートであり、複数のサイト間で拡張することはできません。

  このガイドでは、オンプレミスの Cisco ACI ファブリック向けの Nexus Dashboard Orchestrator 構成について説明しています。クラウドネットワーク コントローラ ファブリックの操作については、代わりに Nexus Dashboard Orchestrator のユース ケース ライブラリを参照してください。

c) 右側のサイドバーで、テンプレートの **[表示名（ Display Name）]** を入力します。

d) （任意）**[説明 (Description)]** を入力します。

e) **[テナントの選択 (Select a Tenant)]**ドロップダウンから、このテンプレートのテナントを選択します。

新しいスキーマを作成するために使用しているユーザ アカウントは、そのスキーマに追加しようとしているテナントに関連付けられている必要があることに注意してください。そうしないと、テナントはドロップダウン メニューで使用できなくなります。ユーザ アカウントとテナントの関連付けについては、テナント と テナントポリシー （5 ページ） を参照してください。

f) テンプレート ビュー ページで、**[保存（Save）]** をクリックします。

追加のオプション（サイトの関連付けなど）を使用できるようにするには、この初期構成の後にテンプレートを保存する必要があります。

g) この手順を繰り返して、追加のテンプレートを作成します。

スキーマとテンプレートの設計の詳細については、スキーマとテンプレート設計上の考慮事項 （19 ページ） を参照してください。

ステップ 4 テンプレートをサイトに割り当てます。

ファブリック構成を展開するには、一度に1つのテンプレートを1つ以上のサイトに展開します。それで、設定を展開する少なくとも 1 つのサイトにテンプレートを関連付ける必要があります。

a) テンプレート ビュー ページで、**[アクション（Actions）]** をクリックし、**[サイトの関連付け（Site Association）]** を選択します。

b) **[サイトを <テンプレート> に追加（Add Sites to <template>）]** ダイアログで、テンプレートを展開する 1 つ以上のサイトを選択し、**[OK]** をクリックします。

次のタスク

スキーマと 1 つ以上のテンプレートを作成したら、特定のユース ケースに基づいて、このドキュメントの次のセクションで説明するように、テンプレートの編集に進むことができます。構成の定義が完了したら、テンプレートの展開 （60 ページ）で説明されているようにテンプレートを展開できます。

APIC サイトからのスキーマ要素のインポート

新しいオブジェクトを作成し、1 つまたは複数のサイトに公開できます。または、サイトローカルの既存のオブジェクトをインポートし、マルチサイト Orchestrator を使用して管理できます。ここでは、1 つ以上の既存のオブジェクトをインポートする方法について説明します。このドキュメントでは、新しいオブジェクトを作成する方法について説明します。

APIC から NDO にポリシーをインポートする際の一般的な方法は、VRF やコントラクトなどの一部のオブジェクトをストレッチテンプレートにインポートし、その他のオブジェクト（非ストレッチ EPG や BD など）をサイトローカル テンプレートにインポートすることです。

リリース3.1(1)より前は、ストレッチテンプレートの一部である別のオブジェクトを参照するサイトローカルテンプレートにオブジェクトをインポートすると、次のような特定の問題がありました。

- 参照オブジェクトがすでにNDOに存在し、**[関係を含める (Include Relationships)]** オプションを有効にして新しいオブジェクトをインポートすると、参照オブジェクトがすでに存在するため、オブジェクトの重複が原因で NDO がエラーをスローします。
- ただし、参照オブジェクトをインポートしない場合 (**[関係を含める (Include Relationships)]** オプションが無効になっている場合)、管理者はインポート後に参照オブジェクトとの手動マッピングを実行する必要があります。

リリース3.1(1)以降では、（同じまたは異なるスキーマ内の）異なるテンプレートの一部である別のオブジェクトとの参照を持つサイトローカルテンプレートにオブジェクトをインポートすると、参照は NDO によって自動的に解決されます。このような場合、インポートされているオブジェクトのUIで **[関係をインポート (Import Relationships)]** オプションがグレー表示され、*[参照されたオブジェクト (Referenced Object)]* が *[テンプレート (Template)]* にすでに存在するなどの追加情報が提供されます。既存の関係はデフォルトでインポートされます。このようなオブジェクトはデフォルトで関係とともにインポートされますが、インポート操作が完了したら、BD を別の

VRFに再マッピングするなどして、参照を変更できます。新しい動作は、インポート可能なすべての設定オブジェクトに適用されます。

サイトから 1 つ以上のオブジェクトをインポートするには、次の手順を実行します。

手順

ステップ 1 [**スキーマ (Schema)**] ページで、オブジェクトをインポートするスキーマを選択します。

ステップ 2 左側のサイドバーで、オブジェクトをインポートする**テンプレート**を選択します。

ステップ 3 メインペインで**[インポート (Import)]** ボタンをクリックし、インポート元の**[サイト (Site)]** を選択します。

ステップ 4 **[インポート元 (Import from)]** <***site-name***> ウィンドウが開いたら、インポートするオブジェクトを 1 つまたは複数選択します。

（注）
NDOにインポートするオブジェクトの名前は、すべてのサイトにわたって一意にする必要があります。重複する名前を持つ別のオブジェクトをインポートすると、スキーマ検証エラーとなり、インポートに失敗します。同じ名前のオブジェクトをインポートする必要がある場合は、先に名前を変更してください。

ステップ 5 （オプション）**[関係のインポート (Import relations)]** ノブを有効にして、すべての関連オブジェクトをインポートします。

たとえば、BD をインポートする場合、**[関係のインポート (Import Relationships)]** ノブを有効にすると、関連する VRF もインポートされます。

（注）
前述したように、関連オブジェクトがすでにNDOに存在するオブジェクトに対しては、**[関係のインポート (Import Relationships)]**ノブはデフォルトで有効になり、無効にできません。

VRF の設定

このセクションでは、VRF の設定方法を説明します。

始める前に

スキーマとテンプレートの作成 （32 ページ）の説明に従って、スキーマとテンプレートを作成し、テンプレートにテナントを割り当てる必要があります。

手順

ステップ 1 VRF を作成するためのスキーマとコントラクトを選択します。

a) メインペインで、**[+ オブジェクトの作成 (+Create Object)]** > **[VRF]**を選択します。

または、**[VRF]** エリアまでスクロール ダウンし、タイルの上にマウスを移動して、**[VRF の追加 (Add VRF)]** をクリックします。

b) 右側のペインで、VRF の **[表示名 (Display Name)]** を入力します。

c) （任意）**[説明 (Description)]** を入力します。

ステップ 2 VRF の **[オンプレミス プロパティ(On-Premises Properties)]** を設定します。

a) **[ポリシー制御適用の選択 (Policy Control Enforcement Preference)]** を指定します。

新しく作成された VRF のポリシー制御の適用は変更できず、設定は適用モードにロックされます。

ただし、これを使用して、インポート後、非適用として設定されている APIC サイトからインポートした VRF を適用モードに移行することができます。一般的な使用例は、既存の VRF を強制モードに変換してサイト間での拡張をサポートする必要がある、ブラウンフィールド展開です。インポートした VRF を NDO で非適用から適用に移行すると、このフィールドをさらに変更することはできなくなります。

- [適用 (Enforced)]：セキュリティ ルール（コントラクト）が適用されます。
- [非適用 (Unenforced)]：セキュリティ ルール（コントラクト）は適用されません。

b) （任意）**[IPデータプレーン学習 (IP Data-Plane Learning)]** を有効にします。

IP アドレスが VRF のデータプレーン パケットを通じて学習されるかどうかを定義します。

無効の場合、IP アドレスはデータプレーン パケットから学習されません。ローカルおよびリモート MAC アドレスは学習されますが、ローカル IP アドレスはデータ パケットから学習されません。

このパラメータが有効か無効かに関係なく、ローカル IP アドレスはARP、GARP、および ND から学習できます。

c) (オプション) VRF の **[レイヤ 3 マルチキャスト (L3 Multicast)]**を有効にします。

詳細については、レイヤ 3 マルチキャスト （283 ページ） を参照してください。

d) （オプション）VRF の **[vzAny]** を有効にします。

詳細については、vzAny コントラクト （357 ページ） を参照してください。

e) （オプション）VRF の **[優先するグループ（Preferred Group）]** を有効化します。

詳細は、EPG 優先のグループ概要と制限 （227 ページ）を参照してください。

ブリッジ ドメインの設定

このセクションでは、ブリッジ ドメイン (BD) を設定する方法について説明します。

始める前に

- スキーマとテンプレートの作成 （32 ページ）の説明に従って、スキーマとテンプレートを作成し、テンプレートにテナントを割り当てる必要があります。

• VRF の設定 （35 ページ）の説明に従って VRF を作成する必要があります。

手順

ステップ 1 ブリッジ ドメインを作成するためのスキーマとコントラクトを選択します。

ステップ 2 ブリッジ ドメインを作成します。

a) メインペインで、**[+ オブジェクトの作成 (+Create Object)]** > **[ブリッジ ドメイン (Bridge Domains)]**を選択します。

または、**[ブリッジ ドメイン (Bridge Domains)]** エリアまでスクロール ダウンし、タイルの上にマウスを移動して、**[ブリッジ ドメインの追加 (Add Bridge Domains)]** をクリックします。

b) 右側のペインで、ブリッジ ドメインの **[表示名 (Display Name)]** を入力します。

c) （任意）**[説明 (Description)]** を入力します。

ステップ 3 **[オンプレミス プロパティ(On-Premises Properties)]** を設定します。

a) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、ブリッジ ドメインを選択します。

b) （オプション）**[L2 ストレッチ(L2 Stretch)]** を有効にします。

c) （オプション）**[サイト間 BUM トラフィック許可 (Intersite BUM Traffic Allow)]** を有効にします。

このオプションは、**L2 ストレッチ**を有効にした場合に使用可能になります。

d) （オプション）**[最適化された WAN 帯域幅 (Optimized WAN Bandwidth)]** を有効にします。

このオプションは、**L2 ストレッチ**を有効にした場合に使用可能になります。

e) （オプション）**[ユニキャスト ルーティング (Unicast Routing)]** を有効にします。

この設定が有効で、サブネットアドレスが構成されている場合、ファブリックがデフォルト ゲートウェイ機能を提供し、トラフィックをルーティングします。ユニキャストルーティングを有効にすると、マッピングデータベースがこのブリッジドメインのエンドポイントに付与された IP アドレスと VTEP の対応関係を学習します。IP 学習は、ブリッジドメイン内にサブネットが構成されているかどうかに左右されません。

f) （オプション）BD の **[L3 マルチキャスト (L3 Multicast)]** を有効にします。

Layer 3 マルチキャストの詳細については、レイヤ 3 マルチキャスト （283 ページ）を参照してください。

g) （オプション）**[L2 不明なユニキャスト (L2 Unknown Unicast)]** モードを選択します。

デフォルトでは、ユニキャストのトラフィックは、レイヤ 2 ポートに対してフラッディングされます。該当する場合、特定のポートでユニキャスト トラフィック フラッディングがブロックされ、ポート上に存在する既知の MAC アドレスを持つ出力トラフィックのみが許可されます。可能な方式は `[フラッディング (Flood)]` または `[ハードウェア プロキシ (Hardware Proxy)]` です。

BD が L2 Unknown Unicast を持っており、それが Flood に設定されている場合、エンドポイントが削除されると、システムはそれを両方のローカル リーフ スイッチから削除します。そして、Clear

Remote MAC Entries を選択すると、BD が展開されているリモートのリーフ スイッチからも削除されます。この機能を使用しない場合、リモート リーフは、タイマーが時間切れになるまで、学習したこのエンドポイントの情報を保持します。

（注）
L2 Unknown Unicast の設定を変更すると、このブリッジ ドメインに関連付けられた EPG にアタッチされているデバイスのインターフェイス上で、トラフィックがバウンスします (アップ ダウンします)。

h) （オプション）**[不明なマルチキャスト フラッディング (Unknown Multicast Flooding)]** モードを選択します。

これは、IPv4 の不明マルチキャスト トラフィックに適用される、レイヤ 3 不明マルチキャスト宛先のノード転送パラメータです。

- [フラッド (Flood)]（デフォルト）：不明な IPv4 マルチキャスト トラフィックは、このブリッジ ドメインに関連付けられた EPG に接続されたすべての前面パネル ポートでフラッディングされます。フラッディングは、ブリッジ ドメインの M ルータポートだけに制限されません。
- [最適化されたフラッド（Optimized Flood）] — ブリッジドメイン内のMルータポートにのみデータを送信します。

i) （オプション）**[IPv6 不明マルチキャスト フラッディング (IPv6 Unknown Multicast Flooding)]** モードを選択します。

これは、IPv6不明マルチキャストトラフィックに適用され、レイヤ3不明マルチキャスト宛先のノード転送パラメータです。

- [フラッド (Flood)]（デフォルト）：不明な IPv6 マルチキャストトラフィックは、このブリッジ ドメインに関連付けられたすべての前面パネルポートでフラッディングされます。フラッディングは、ブリッジ ドメインの M ルータポートだけに制限されません。
- [最適化されたフラッド（Optimized Flood）] — ブリッジドメイン内のMルータポートにのみデータを送信します。

j) （オプション）**[複数宛先フラッディング (Multi-Destination Flooding)]** モードを選択します。

レイヤ 2 マルチキャストおよびブロードキャストトラフィックの複数宛先転送方式です。

- [BD のフラッド (Flood in BD)]：同じブリッジ ドメイン上のすべてのポートにデータを送信します。
- [ドロップ (drop)]：パケットをドロップします。他のポートにデータを送信しません。
- [カプセル化のフラッド (Flood in Encapsulation)]：ブリッジ ドメイン全体にフラッディングされるプロトコル パケットを除き、ブリッジ ドメイン内の同じ VLAN を持つすべての EPG ポートにデータを送信します。

  （注）
  このモードは、**[L2 ストレッチ (L2 Stretch)]** オプションが無効になっている場合にのみサポートされ、サイト間でストレッチされる BD ではサポートされません。

k) （オプション）**[ARP フラッディング (ARP Flooding)]** を有効にします。

これによって ARP フラッディングが有効になり、レイヤ 2 ブロードキャスト ドメインが IP アドレスをMACアドレスにマッピングします。フラッディングがディセーブルである場合、ユニキャスト ルーティングはターゲット IP アドレスで実行されます。

ARP要求がレイヤ2ブロードキャストドメイン内でフラッディングされるように、ARPフラッディングを有効にします。BD がサイト間で拡張されている場合、ARP フラッディングを有効にできるのは、**[サイト間 BUM トラフィック許可 (Intersite BUM Traffic Allow)]**を有効にした場合のみです。ARP フラッディングが無効な場合、ローカルに接続されたエンドポイントから ARP 要求を受信するリーフは、ARP 要求のターゲット エンドポイントが接続されているリモート リーフに直接転送するか（リモート エンドポイントの IP がエンドポイント テーブルで既知の場合）、またはスパインへ転送します（リモートエンドポイントのIPがエンドポイントテーブルで不明な場合）。

[L2 不明なユニキャスト (L2 Unknown Unicast)] モードを `[フラッド (Flood)]` に設定した場合、**[ARP フラッディング (ARP Flooding)]** は無効にできません。**[L2 不明なユニキャスト (L2 Unknown Unicast)]** モードを `[ハードウェア プロキシ (Hardware Proxy)]` に設定した場合、ARP フラッディングは有効または無効にできます。

l) （オプション）**[仮想 MAC アドレス (Virtual MAC Address)]** を入力します。

BD の仮想MACアドレスとサブネットの仮想IPアドレスは、ブリッジ ドメインのすべての ACI ファブリックで同じにする必要があります。複数のブリッジ ドメインを、接続されている ACI ファブリック間で通信するように設定できます。仮想 MAC アドレスと仮想 IP アドレスは、ブリッジ ドメイン間で共有できます。

（注）
仮想 MAC と仮想 IP サブネットは、個々のサイトを NDO 編成のマルチサイト ファブリックに移行する場合にのみ使用してください。移行が完了したら、これらのフラグを無効にできます。

ステップ 4 BD の 1 つ以上の **[サブネット (Subnets)]** を追加します。

a) **[+ サブネットの追加 (+ Add Subnet)]** をクリックします。

[サブネットの新規追加 (Add New Subnet)] ウィンドウが開きます。

b) サブネットの **[ゲートウェイ IP (Gateway IP)]** アドレスと追加するサブネットの **[説明 (Description)]** を入力します。

c) 必要に応じて、**[仮想 IP アドレスとして扱う (Treat as virtual IP address)]** オプションを有効にします。

このオプションは、BD の**[仮想 MAC アドレス（Virtual MAC Address）]** とともに、個々の共通パーベイシブ ゲートウェイ構成から NDOに管理された Multi-Site 展開への移行シナリオに使用できます。

d) サブネットの **[範囲 (Scope)]** を選択します。

これはサブネットのネットワーク可視性です。

- `[VRF に対してプライベート (Private to VRF)]`：サブネットが L3Out を介して外部ネットワーク ドメインにアナウンスされないようにします。
- `外部にアドバタイズ (Advertised Externally)`：サブネットはL3Outを介して外部ネットワークドメインに向けてアナウンスできます。

e) （任意）**[VRF 間で共有 (Shared Between VRFs)]** をオンにします。

`[VRF 間で共有 (Shared Between VRF)]`：サブネットは、同じテナント内で、または共有サービスの一部としてテナントを越えて、複数のコンテキスト（VRF）で共有し、それらにエクスポートすることができます。共有サービスの例は、別のテナントの別のコンテキスト（VRF）に存在するEPGへのルーテッド接続です。これにより、トラフィックはコンテキスト（VRF）間で双方向に通過できます。共有サービスを提供する EPG は、その EPG の下で（ブリッジ ドメインの下ではなく）サブネットを設定する必要があり、そのスコープは外部にアドバタイズするように設定し、VRF 間で共有する必要があります。

共有サブネットは、通信に含まれるコンテキスト（VRF）全体で一意でなければなりません。EPG 下のサブネットがレイヤ 3 外部ネットワーク共有サービスを提供する場合、このようなサブネットは、ACI ファブリック内全体でグローバルに一意である必要があります。

f) **[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)]** オプションはオフのままにします。

このオプションを有効にすると、リーフルートにプロキシルート（スパインプロキシへのサブネットルート）だけがプログラムされ、SVIは作成されません。つまり、SVIはゲートウェイとして使用できません。

EPG サブネットはルート リークにのみ使用されるため、ゲートウェイとして BD サブネットによって SVI を作成し、EPG で **[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)]**オプションを有効にすることをお勧めします。

g) （オプション）**[クエリア (Querier)** オプションを有効にします。

サブネットでの [IGMP スヌーピング (IGMP Snooping)] を有効にします。

h) （オプション）**[プライマリ (Primary)]** オプションを有効にして、サブネットをプライマリとして指定します。

1 つのプライマリ IPv4 サブネットと 1 つのプライマリ IPv6 サブネットが可能です。

i) **[保存（Save）]** をクリックします。

ステップ 5 （オプション）**[IGMP インターフェイス ポリシー（IGMP Interface Policy）]**を追加します。

リリース 4.0（1）以降、多数のテナント ポリシー テンプレートを構成し、それらをポリシー オブジェクトに関連付けることができます。詳細については、テナント ポリシー テンプレートを作成 （8 ページ）を参照してください。

ステップ 6 （オプション）**[IGMP スヌープ ポリシー（IGMP Snoop Policy）]**を追加します。

リリース 4.0（1）以降、多数のテナント ポリシー テンプレートを構成し、それらをポリシー オブジェクトに関連付けることができます。詳細については、テナント ポリシー テンプレートを作成 （8 ページ）を参照してください。

ステップ 7 （オプション）**[MLD スヌープ ポリシー（MLD Snoop Policy）]**を追加します。

リリース 4.0（1）以降、多数のテナント ポリシー テンプレートを構成し、それらをポリシー オブジェクトに関連付けることができます。詳細については、テナント ポリシー テンプレートを作成 （8 ページ）を参照してください。

ステップ 8 （オプション）**[DHCP ポリシー (DHCP Policy)]** を追加します。

詳細については、DHCPリレー （217 ページ） を参照してください。

ステップ 9 必要に応じて、ブリッジ ドメインのサイトローカル プロパティを設定します。

ブリッジドメインのサイトローカルプロパティの設定 （41 ページ）で説明されているように、テンプレート レベルの設定に加えて、ブリッジ ドメインの 1 つ以上のサイトローカル プロパティを定義することもできます。

ブリッジドメインのサイトローカル プロパティの設定

テンプレートでオブジェクトを作成するときにオブジェクトに対して通常設定するテンプレート レベルのプロパティに加えて、テンプレートを割り当てる各サイトに固有の1つ以上のプロパティを定義することもできます。

オブジェクトを複数のサイトに展開すると、同じテンプレート レベルの設定がすべてのサイトに展開され、サイトローカルの設定はそれらの特定のサイトにのみ展開されます。

始める前に

次のものが必要です。

- ブリッジ ドメインの設定 （36 ページ）の説明に従って、ブリッジ ドメインを作成し、そのテンプレート レベルのプロパティを設定していること。
- ブリッジ ドメインを含むテンプレートを 1 つ以上のサイトに割り当てていること。

手順

ステップ 1 ブリッジ ドメインを含むテンプレートを含むスキーマを開きます。

ステップ 2 左側のサイドバーで、設定する特定のサイトの下のブリッジ ドメインを含むテンプレートを選択します。

ステップ 3 メイン ペインで、ブリッジ ドメインを選択します。

ほとんどのフィールドでは、テンプレート レベルで設定した値が表示されますが、ここでは編集できません。

ステップ 4 **[+ L3Out]** をクリックして L3Out を追加します。

これは、リモート L3Out から BD サブネットをアドバタイズし、ローカル L3Out に障害が発生した場合でも BD へのインバウンド トラフィックを維持できるようにするために必要です。この場合、サブネットに `[外部にアドバタイズ (Advertised Externally)]` フラグを設定する必要もあります。詳細に関しては、サイト間 L3Out （231 ページ）ユース ケースの例を参照してください。

ステップ 5 **[ホストルート (Host Route)]** を有効にします。

これにより、ブリッジ ドメインでホスト ベース ルーティングが有効になります。このノブを有効にすると、ボーダー リーフ スイッチは、サブネットとともに個々のエンドポイント（EP）ホストルート（/32 または /128 プレフィックス）もアドバタイズします。ルート情報は、ホストがローカル POD に接続されている場合にのみアドバタイズされます。EP がローカル Pod から離れた、または EP が EP データベースから削除された場合、ルート アドバタイズメントはその時に撤回されます。

ステップ 6 必要に応じて、**[SVI MACアドレス (SVI MAC Address)]** を変更します。

仮想 MAC および仮想 IP が Common Pervasive Gateway（CPG）シナリオで有効になっている場合、SVI MAC アドレスはサイトごとに一意である必要があります。このフィールドは、BD のデフォルト ルータ MAC を変更する CPG が有効になっていない場合にも使用できます。

ステップ 7 BD の 1 つ以上の **[サブネット (Subnets)]** を追加します。

この概念は、サブネットがこの特定のサイトのブリッジドメインにのみ設定されることを除き、テンプレート レベルで BD にサブネットを追加することと同じです。

a) **[+ サブネットの追加 (+ Add Subnet)]** をクリックします。

[サブネットの新規追加 (Add New Subnet)] ウィンドウが開きます。

b) サブネットの **[ゲートウェイ IP (Gateway IP)]** アドレスと追加するサブネットの **[説明 (Description)]** を入力します。

c) サブネットの **[範囲 (Scope)]** を選択します。

これはサブネットのネットワーク可視性です。

- `[VRF に対してプライベート (Private to VRF)]`：サブネットはテナント内でのみ適用されます。
- `[外部にアドバタイズ (Advertised Externally)]`：サブネットをルーテッド接続にエクスポートできます。

d) （任意）**[VRF 間で共有 (Shared Between VRFs)]** をオンにします。

`[VRF 間で共有 (Shared Between VRF)]`：サブネットは、同じテナント内で、または共有サービスの一部としてテナントを越えて、複数のコンテキスト（VRF）で共有し、それらにエクスポートすることができます。共有サービスの例は、別のテナントの別のコンテキスト（VRF）に存在するEPGへのルーテッド接続です。これにより、トラフィックはコンテキスト（VRF）間で双方向に通過できます。共有サービスを提供する EPG は、その EPG の下で（ブリッジ ドメインの下ではなく）サブネットを設定する必要があり、そのスコープは外部にアドバタイズするように設定し、VRF 間で共有する必要があります。

共有サブネットは、通信に含まれるコンテキスト（VRF）全体で一意でなければなりません。EPG 下のサブネットがレイヤ 3 外部ネットワーク共有サービスを提供する場合、このようなサブネットは、ACI ファブリック内全体でグローバルに一意である必要があります。

e) （オプション）**[デフォルトの SVI ゲートウェイなし (No Default SVI Gateway)]** を有効にします。

このオプションを有効にすると、リーフルートにプロキシルート（スパインプロキシへのサブネットルート）だけがプログラムされ、SVIは作成されません。つまり、SVIはゲートウェイとして使用できません。

EPG サブネットはルート リークにのみ使用されるため、ゲートウェイとして BD サブネットによって SVI を作成し、EPG で **[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)]**オプションを有効にすることをお勧めします。

f) （オプション）**[クエリア (Querier)]** を有効にします。

サブネットでの [IGMP スヌーピング (IGMP Snooping)] を有効にします。

g) （オプション）**[プライマリ (Primary)]** オプションを有効にして、サブネットをプライマリとして指定します。

1 つのプライマリ IPv4 サブネットと 1 つのプライマリ IPv6 サブネットが可能です。

h) [保存（Save）] をクリックします。

アプリケーション プロファイルと EPG の設定

このセクションでは、アプリケーション プロファイルと EPG を設定する方法について説明します。

始める前に

スキーマとテンプレートの作成 （32 ページ）の説明に従って、スキーマとテンプレートを作成し、テンプレートにテナントを割り当てる必要があります。

このセクションでは、契約とブリッジドメインが作成されていることも前提としています。

手順

ステップ 1 スキーマを選択し、アプリケーション プロファイルを作成するテンプレートを選択します。

ステップ 2 アプリケーション プロファイルを作成します。

a) メインペインで、**[+ オブジェクトの作成 (+Create Object)]** > **[アプリケーション プロファイル (Application Profile)]**を選択します。

または、**[アプリケーション プロファイル (Application Profile)]** エリアまでスクロール ダウンし、タイルの上にマウスを移動して、**[アプリケーション プロファイルの追加 (Add Application Profile)]** をクリックします。

b) 右側のペインで、アプリケーション プロファイルの **[表示名 (Display Name)]** を入力します。

競合することなく、異なるテンプレートに同じ名前のアプリケーションプロファイルを作成できます。ただし、同じサイトおよびテナントに展開する場合は、異なるテンプレートで同じ名前を持つ他のオブジェクト（VRF、BD、EPGなど）を作成することはできません。

c) （任意）**[説明 (Description)]** を入力します。

ステップ 3 EPG を作成します。

a) メインペインで**[+オブジェクトの作成(Create Object)]**>**[EPG]**を選択し、EPGを作成するアプリケーションプロファイルを選択します。

または、特定の**[アプリケーション プロファイル (Application Profile)]** エリアまでスクロール ダウンし、**[EPGs]** タイルの上にマウスを移動して、**[EPG の追加 (Add EPG)]** をクリックします。

b) 右側のペインで、EPG の **[表示名 (Display Name)]** を入力します。

c) （任意）**[説明 (Description)]** を入力します。

ステップ 4 EPG のコントラクトを追加します。

コントラクトとフィルタの作成については、コントラクトとフィルタの設定（49ページ）で詳しく説明しています。コントラクトを作成済みの場合：

a) **[+ コントラクト (+ Contract)]** をクリックします。

b) [**コントラクトの追加 (Add Contract)]** ダイアログで、コントラクトの名前とタイプを入力します。

c) **[保存 (SAVE)]** をクリックします。

ステップ 5 **[ブリッジ ドメイン (Bridge Domain)]** ドロップダウンで、この EPG のブリッジ ドメインを選択します。

オンプレミスの EPG を設定する場合は、ブリッジ ドメインに関連付ける必要があります。

ステップ 6 (オプション) **[+ サブネット (+ Subnet)]** をクリックして、EPG にサブネットを追加します。

たとえば、VRF ルートリークのユースケースとして、ブリッジ ドメイン レベルではなく EPG レベルでサブネットを設定することもできます。

a) **[サブネットの追加 (Add Subnet)]** ダイアログで、**[ゲートウェイ IP (Gateway IP)]** アドレスと追加予定のサブネットの説明を入力します。

b) **[範囲 (Scope)]** フィールドで **[VRF にプライベート (Private to VRF)]** または **[外部にアドバタイズ (Advertised Externally)]** のどちらかを選択します。

c) 適切な場合、**[VRF 間で共有 (Shared Between VRFs)]** チェックボックスをチェックします。

d) 必要に応じて、**[デフォルトの SVI ゲートウェイなしデフォルト (No Default SVI Gateway)]** をオンにします。

e) **[OK]**をクリックします。

ステップ 7 (オプション) マイクロセグメンテーションを有効にします。

マイクロセグメンテーション EPG (uSeg) を設定する場合は、エンドポイントを EPG に一致させるために 1 つ以上の uSeg 属性を指定する必要があります。

a) **[uSeg EPG]** チェックボックスをオンにします。

b) **[+uSeg EPG]**] をクリックします。

c) uSeg 属性の **[名前 (Name)]** と **[タイプ (Type)]** を入力します。

d) 選択した属性タイプに基づいて、属性の詳細を指定します。

たとえば、属性タイプとして `1[MAC]` を選択した場合は、この EPG でエンドポイントを識別する MAC アドレスを指定します。

e) **[保存 (SAVE)]** をクリックします。

ステップ 8 (オプション) EPG 内分離を有効にします。

デフォルトでは、EPG 内のエンドポイントが自由に相互に通信できます。エンドポイントを互いに分離するには、分離モードを **[強制 (Enforced)]** に設定します。

EPG 内エンドポイント分離ポリシーにより、仮想エンドポイントまたは物理エンドポイントが完全に分離されます。分離を適用した状態で稼働している EPG 内のエンドポイント間の通信は許可されません。分離を適用した EGP では、多くのクライアントが共通サービスにアクセスするときに必要な EPG カプセル化の数は低減しますが、相互間の通信は許可されません。

ステップ 9 (オプション) EPG のレイヤ 3 マルチキャストを有効にします。

Layer 3 マルチキャストの詳細については、次を参照してください: レイヤ 3 マルチキャスト （283 ページ）

ステップ 10 (オプション) EPG の優先グループメンバシップを有効にします。

優先グループ機能を使用すると、単一の VRF 内に複数の EPG を含めて、コントラクトを作成しなくても、それらの間の完全な通信を可能にすることができます。EPG 優先グループの詳細については、次を参照してください: EPG 優先のグループ概要と制限 （227 ページ）

ステップ 11 必要に応じて、EPGのサイトローカル プロパティを設定します。

EPG のサイトローカル プロパティの設定 （45 ページ）で説明しているように、テンプレート レベルの設定に加えて、EPG の 1 つ以上のサイトローカル プロパティを定義することもできます。

EPG のサイトローカル プロパティの設定

テンプレートでオブジェクトを作成するときにオブジェクトに対して通常設定するテンプレート レベルのプロパティに加えて、テンプレートを割り当てる各サイトに固有の1つ以上のプロパティを定義することもできます。

オブジェクトを複数のサイトに展開すると、同じテンプレート レベルの設定がすべてのサイトに展開され、サイトローカルの設定はそれらの特定のサイトにのみ展開されます。

始める前に

次のものが必要です。

- アプリケーション プロファイルと EPG の設定 （43 ページ）の説明に従って作成されたアプリケーションプロファイルとEPG。テンプレートレベルでプロパティが設定されていることも必要です。
- ブリッジ ドメインを含むテンプレートを 1 つ以上のサイトに割り当てていること。

手順

ステップ 1 EPGでテンプレートを含むスキーマを開きます。

ステップ 2 左側のサイドバーで、設定する特定のサイトの下の EPG を含むテンプレートを選択します。

ステップ 3 メインペインで、EPG を選択します。

ほとんどのフィールドでは、テンプレート レベルで設定した値が表示されますが、ここでは編集できません。

ステップ 4 EPG に 1 つ以上の**サブネット**を追加します。

a) **[+ サブネットの追加 (+ Add Subnet)]** をクリックします。

[サブネットの新規追加 (Add New Subnet)] ウィンドウが開きます。

b) サブネットの **ゲートウェイ IP** アドレスと追加するサブネットの説明を入力します。

c) サブネットの **[範囲 (Scope)]** を選択します。

これはサブネットのネットワーク可視性です。

- `[VRF に対してプライベート (Private to VRF)]`：サブネットが L3Out を介して外部ネットワーク ドメインにアナウンスされないようにします。
- `外部にアドバタイズ (Advertised Externally)`：サブネットはL3Outを介して外部ネットワークドメインに向けてアナウンスできます。

d) （任意）**[VRF 間で共有 (Shared Between VRFs)]** をオンにします。

`[VRF 間で共有 (Shared Between VRF)]`：サブネットは、同じテナント内で、または共有サービスの一部としてテナントを越えて、複数のコンテキスト（VRF）で共有し、それらにエクスポートすることができます。共有サービスの例は、別のテナントの別のコンテキスト（VRF）に存在するEPGへのルーテッド接続です。これにより、トラフィックはコンテキスト（VRF）間で双方向に通過できます。共有サービスを提供する EPG は（EPG ではなく）BD でサブネットを設定する必要があり、そのスコープは外部にアドバタイズされ、VRF 間で共有されるように設定する必要があります。

共有サブネットは、通信に含まれるコンテキスト（VRF）全体で一意でなければなりません。EPG 下のサブネットがレイヤ 3 外部ネットワーク共有サービスを提供する場合、このようなサブネットは、ACI ファブリック内全体でグローバルに一意である必要があります。

e) （オプション）**[デフォルトの SVI ゲートウェイなし (No Default SVI Gateway)]** を有効にします。

このオプションを有効にすると、リーフルートにプロキシルート（スパインプロキシへのサブネットルート）だけがプログラムされ、SVIは作成されません。つまり、SVIはゲートウェイとして使用できません。

EPG サブネットではこのオプションを有効にすることをお勧めします。このオプションは、ルートリークにのみ使用し、BD サブネットではこのオプションを無効のままにして、SVI をゲートウェイとして使用できるようにします。

f) **Ok** をクリックして保存します。

ステップ 5 1 つ以上の**スタティックポート**を追加します。

a) **[+ スタティック ポートの追加 (+Static Port)]** をクリックします。

b) **[パスタイプ (Path Type)]** ドロップダウンから、ポートのタイプを選択します。

c) 物理インターフェイスを構成する場合は、**[ポッド（Pod）]** を選択します。

d) 単一のポートを構成するか、ポートの範囲を構成するかを選択します。

インターフェイス設定については、単一のリーフとパスを入力するか、リーフの範囲（例：120 - 125 およびパス）を入力して（例：1/17 - 20）するオプションがあります。また、リーフの範囲を入力して 1 つの単一のパスに関連付けるか、1 つの単一のリーフのパスの範囲を入力するオプションもあります。

ただし、構成後も UI には個別のポートとして表示され、今後の更新では個別の変更が必要になります。

e) **[ポート カプセル化 VLAN (Port Encap VLAN)]** を選択します。

EPG のドメインでポート カプセル化を手動で設定する場合、VLAN ID はダイナミック VLAN プール内のスタティック VLAN ブロックに属している必要があります。

EPG でテンプレート レベルでのマイクロセグメンテーションが有効になっている場合、**プライマリ MICRO-SEG VLAN** が設定されると、ポート カプセル化 VLAN はプライマリ VLAN の独立した**セカンダリ VLAN** として設定されます。トラフィックはセカンダリ VLAN を使用してホストからリーフに送信され、リーフからホストへのリターン トラフィックはプライマリ VLAN を使用して送信されます。

f) （任意）**プライマリ MICRO-SEG VLAN (Primary MICRO-SEG VLAN)** を選択します。

マイクロセグメンテーションの VLAN 識別子

g) （オプション）**[展開の即時性 (Deployment Immediacy)]** を選択します。

ポリシーがリーフ ノードにダウンロードされたときに、ポリシーがハードウェア ポリシー CAM にプッシュされるタイミングは、展開の即時性によって指定できます。

- [即時（Immediate）]：リーフ ソフトウェアにダウンロードされたポリシーがハードウェアのポリシー CAM ですぐにプログラミングされるように指定します。
- [オン デマンド（On Demand）]：最初のパケットがデータ パス経由で受信された場合にのみポリシーがハードウェアのポリシー CAM でプログラミングされるように指定します。このプロセスは、ハードウェアの領域を最適化するのに役立ちます。

h) （オプション）**[モード (Mode)]** を選択します。

パスのスタティック アソシエーションのモードを選択します。EPG のタグ付けとは、EPG で次のようにスタティック パスを設定することです。

- `[トランク (Trunk)]`：これはデフォルトの展開モードです。ホストからのトラフィックに VLAN ID がタグ付けされている場合、このモードを選択します。
- `[アクセス (802.1P) (Access (802.1P))`：ホストからのトラフィックが 802.1P タグでタグ付けされている場合、このモードを選択します。アクセス ポートにネイティブ 802.1p モードの EPG を 1 つ設定すると、そのパケットはタグなしの状態でポートを退出します。ネイティブ 802.1p モードの EPG を 1 つと、VLAN タグが付いた複数の EPG をアクセス ポートに設定すると、ネイティブ 802.1p モードで設定された EPG については、そのアクセス ポートを退出するすべてのパケットに VLAN 0 がタグ付けされ、退出する他のすべての EPG パケットにはそれぞれの VLAN タグが付けられます。1 つのアクセス ポートにつき、ネイティブ 802.1p EPG は 1 つだけ許可されることに注意してください。

- [アクセス（タグなし）(Access (Untagged))]：ホストからのトラフィックがタグ付けされていない場合（VLAN ID なし）、このモードを選択します。ある EPG が使用するすべてのポートについて、この EPG にタグ付けしないようリーフ スイッチを設定すると、パケットはタグなしの状態でスイッチから送出されます。EPG をタグなしとして展開する際は、その EPG を同じスイッチの他のポート上にタグ付きとして展開することは避ける必要があることに注意してください。

ステップ 6 1 つ以上の**スタティック リーフ**ノードを追加します。

a) **[+ スタティック リーフの追加 (+Static Leaf)]** をクリックします。
b) **[リーフ (Leaf)]** ドロップダウンから、追加するリーフ ノードを選択します。
c) （任意）**[VLAN]** フィールドに、タグ付きトラフィックの VLAN ID を入力します。

ステップ 7 1 つ以上の**ドメイン** ノードを追加します。

a) **[+ ドメイン (+Domain)]** をクリックします。
b) **[ドメイン関連付けタイプ (Domain Association Type)]** を選択します。

これは、追加するドメインのタイプです。

- VMM
- Fibre Channel
- L2 外部
- L3 外部
- 物理

c) **[ドメイン プロファイル (Domain Profile)]** の名前を選択します。
d) **[展開の即時性 (Deployment Immediacy)]** を選択します。

導入の即時性で、ポリシーがプッシュされるタイミングを指定できます。

- [即時（Immediate）]：リーフ ソフトウェアにダウンロードされたポリシーがハードウェアのポリシー CAM ですぐにプログラミングされるように指定します。
- [オン デマンド（On Demand）]：最初のパケットがデータ パス経由で受信された場合にのみポリシーがハードウェアのポリシー CAM でプログラミングされるように指定します。このプロセスは、ハードウェアの領域を最適化するのに役立ちます。

e) **[解決の即時性 (Resolution Immediacy)]** を選択します。

ポリシーをすぐに解決するか、必要に応じて解決するかを指定します。次のオプションがあります。

- [即時 (Immediate)]：ハイパーバイザが VMware vSphere Distributed Switch（VDS）に接続されると、EPG ポリシーがリーフ スイッチ ノードにプッシュされるように指定します。LLDP または OpFlex 権限は、ハイパーバイザ/リーフ ノード接続を解決するために使用されます。
- [オン デマンド (On Demand)]：ハイパーバイザが VDS に接続され、VM がポート グループ（EPG）に配置されている場合にのみ、EPG ポリシーがリーフ スイッチノードにプッシュされるように指定します。

- [事前プロビジョニング (Pre-provision)]：ハイパーバイザがVDSに接続される前でも、EPGポリシーがリーフ スイッチ ノードにプッシュされるように指定します。スイッチ上の設定がダウンロードにより事前プロビジョニングされます。

コントラクトとフィルタの設定

ここでは、コントラクトとフィルタを設定し、フィルタをコントラクトに割り当てる方法について説明します。フィルタはアクセス コントロール リスト (ACL) に似ています。これはEPGに関連付けられた契約を通して、トラフィックをフィルタします。

手順

ステップ 1 スキーマを選択し、コントラクトとフィルタを作成するテンプレートを選択します。

コントラクトは、適用するオブジェクト（EPGおよび外部EPG）と同じテンプレートでも異なるテンプレートでも作成できます。コントラクトを使用するオブジェクトが異なるサイトに展開されている場合は、複数のサイトに関連付けられたテンプレートでコントラクトを定義することをお勧めします。ただし、これは必須ではありません。コントラクトとフィルタがSite1のローカル オブジェクトとしてのみ定義されている場合でも、Site2のローカルEPGまたは外部EPGがそのコントラクトを使用または提供する必要がある場合、NDOはそれらのオブジェクトをリモートSite2に作成します。

ステップ 2 フィルタを作成します。

a) メインペインで、**[+ オブジェクトの作成 (+Create Object)]** > **[フィルタ (Filter)]**を選択します。

または、**[フィルタ (Filters)]** エリアまでスクロール ダウンし、タイルの上にマウスを移動して、**[フィルタの追加 (Add Filter)]** をクリックします。

b) 右側のペインで、フィルタの **[表示名 (Display Name)]** を入力します。

c) （任意）**[説明 (Description)]** を入力します。

ステップ 3 フィルタ エントリを作成します。

a) 右側のペインで、**[+ エントリを追加（+ Add Entry）]** をクリックします。

フィルタ エントリは、ネットワーク トラフィックの分類プロパティの組み合わせです。次の手順の説明に従って、1 つ以上のオプションを指定できます。

b) フィルタの **[名前 (Name)]** を指定します。

c) **[イーサー タイプ (Ether Type)]** を選択します。

たとえば [ip] です。

d) **[IP プロトコル (IP Protocol)]** を選択します。

たとえば [icmp] です。

e) **[宛先ポート範囲の開始 (Destination Port Range From)]** と **[宛先ポート範囲の終了 (Destination Port Range To)]** を選択します。

宛先ポート範囲の開始と終了です。開始フィールドと終了フィールドに同じ値を指定すれば、単一のポートの指定になります。または、0 から 65535 の範囲内で、ポートの範囲を定義することもできます。また、特定のポート番号（http など）の代わりに、いずれかのサーバ タイプを指定することもできます。

f) **[フラグメントのみの一致 (Match only fragment)]** オプションを有効にします。

有効の場合、オフセットが 0 より大きいすべての IP フラグメント（最初のフラグメントを除くすべての IP フラグメント）にこのルールが適用されます。無効の場合、TCP/UDP ポート情報は最初のフラグメントでしかチェックできないため、オフセットが 0 より大きい IP フラグメントにルールは適用されません。

g) **[ステートフル (Stateful)]** オプションを有効にします。

このオプションを有効にする場合には、プロバイダーからコンシューマに戻るすべてのトラフィックは、常にパケットに ACK ビットが設定されている必要があります。そうでないと、パケットはドロップされます。

h) **[ARP フラグ (ARP flag)]**：（Address Resolution Protocol）を指定します。

ARPフラグは、ARP の特定のフィルタを作成するときに使用され、ARP 要求または ARP 応答を指定できます。

i) **[送信元ポート範囲の開始 (Source Port Range From)]** と **[送信元ポート範囲の終了 (Source Port Range To)]** を指定します。

送信元ポート範囲の開始と終了です。開始フィールドと終了フィールドに同じ値を指定すれば、単一のポートの指定になります。または、0 から 65535 の範囲内で、ポートの範囲を定義することもできます。また、特定のポート番号（http など）の代わりに、いずれかのサーバ タイプを指定することもできます。

j) **[TCP セッション ルール (TCP session rules)]** を指定します。

TCPセッションルールは、TCP トラフィックのフィルタを作成するときに使用され、ステートフル ACL の動作を設定できます。

k) **Ok** をクリックして、フィルタを保存します。

l) このフィルタの追加のフィルタ エントリを作成するには、この手順を繰り返します。

フィルタごとに複数のフィルタ エントリを作成して割り当てることができます。

ステップ 4 コントラクトの作成

a) メインペインで、**[+ オブジェクトの作成 (+Create Object)]** > **[コントラクト (Contract)]**を選択します。

または、**[コントラクト (Contract)]**エリアまでスクロールダウンし、タイルの上にマウスを移動して、**[コントラクトの追加 (Add Contract)]** をクリックします。

b) 右側のペインで、コントラクトの**表示名**を指定します。

c) （任意）**[説明 (Description)]** を入力します。

d) コントラクトの適切な **[範囲 (Scope)]** を選択します。

コントラクトの範囲によって、コントラクトのアクセシビリティが制限されます。契約は、プロバイダ EPG の範囲外のコンシューマ EPG には適用されません。

- アプリケーション プロファイル
- VRF
- テナント
- グローバル

e) コンシューマからプロバイダーへの方向とプロバイダーからコンシューマへの方向の両方に同じフィルタを適用する場合は、**[両方向に適用 (Apply both directions)]** ノブを切り替えます。

このオプションを有効にした場合は、フィルタを 1 回だけ指定することが必要となり、両方向のトラフィックに適用されます。このオプションを無効のままにした場合は、各方向に 1 つずつ、2 セットのフィルタ チェーンを指定する必要があります。

（注）
[両方向に適用 (Apply both directions)] を有効にしてコントラクトを作成および展開する場合は、単にオプションを無効にしたり、変更を適用して再展開したりすることはできません。すでに展開されているコントラクトでこのオプションを無効にするには、コントラクトを削除し、テンプレートを展開してから、オプションを無効にしてコントラクトを再作成し、ファブリックの設定を正しく変更する必要があります。

f) （オプション）**[サービス グラフ (Service Graph)]** ドロップダウンから、このコントラクトのサービス グラフを選択します。

g) （オプション）**[QoS レベル (QoS Level)]** ドロップダウンから、このコントラクトの値を選択します。

この値には、このコントラクトを使用してトラフィックに割り当てられる ACI QoS レベル を指定します。詳細については、IPN 全体での QoS の保持 （297 ページ）を参照してください。

これを [未指定 (Unspecified)] のままにすると、デフォルトの QoS レベル 3 がトラフィックに適用されます。

ステップ 5 コントラクトにフィルタを割り当てる

a) テンプレートのメイン ペインで、コントラクトを選択します。右側のペインで、**[フィルタ チェーン（Filter Chain）]** エリアまでスクロールし、**[+ フィルタを追加（+ Add Filter）]** をクリックしてフィルタをコントラクトに追加します。

b) 開いた **[フィルタ チェーンの追加]** ウィンドウで、**[名前 (Name)]** ドロップダウン メニューから前の手順で追加したフィルタを選択します。

c) フィルタの **[アクション (Action)]** を選択します。

フィルタを追加するときに、フィルタ条件に一致するトラフィックを許可するか拒否するかを選択できます。[拒否 (deny)] フィルタの場合、[デフォルト (default)]、[低 (low)]、[中 (medium)]、または [高 (high)] の 4 段階のレベルのいずれかにフィルタの優先順位を設定できます。[許可 (permit)] フィルタは常にデフォルトの優先順位を持ちます。ACIコントラクトとフィルタの詳細については、『*Cisco ACI Contract Guide*』を参照してください。

d) **Ok** をクリックして、フィルタをコントラクトに追加します。
e) コントラクトで [両方向に適用 (Apply both directions)] オプションを無効にした場合は、他のフィルタチェーンに対してこの手順を繰り返します。
f) （オプション）複数のフィルタを作成して各コントラクトに割り当てることができます。

同じコントラクトに追加のフィルタを作成する場合：

- ステップ 2 とステップ 3 を繰り返して、フィルタ エントリとともに別のフィルタを作成します。
- この手順を繰り返して、このコントラクトに新しいフィルタを割り当てます。

オンプレミス外部接続の設定

Cisco ACI では、境界リーフ スイッチを介してオンプレミス ACI ファブリックの外部のネットワークへの接続を確立できます。この接続は、セキュリティとルートマップを定義するために必要な設定オプションを提供する L3Out と外部 EPG の 2 つの構造を使用して定義されます。

このセクションでは、Nexus Dashboard Orchestrator GUI を使用して L3Out と外部 EPG を追加する方法について説明します。次に、Orchestrator で、テンプレートを展開する APIC サイトにおいてオブジェクトを作成します。Orchestrator から L3Out を作成する場合、APIC では L3Out コンテナ オブジェクトのみが作成されることに注意してください。この場合も、サイトの APIC で、完全な L3Out の構成 (ノード、インターフェイス、ルーティングプロトコルなど) を直接実行する必要があります。

ほとんどの場合、L3Out は APIC レベルで直接作成され、その後、Orchestrator で作成した外部 EPG に関連付けられます。L3Out をOrchestrator から作成した VRF に直接関連付ける場合には、ここで両方を作成すると便利です。

始める前に

- スキーマとテンプレートの作成 （32 ページ）の説明に従って、スキーマとテンプレートを作成し、テンプレートにテナントを割り当てる必要があります。
- VRF の設定 （35 ページ）の説明に従って、L3Out の VRF を作成する必要があります。

手順

ステップ 1 編集するスキーマとテンプレートに移動します。

ステップ 2 L3Out を作成します。

a) [スキーマ編集 (schema edit)] ビューで、**[L3Out]** エリアまで下にスクロールし、+をクリックして新しい L3Out を追加します。
b) 右側のプロパティ ペインで、L3Out の [表示名 (Display Name)] を入力します。

c) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、先ほど作成した VRF を選択します。

（注）
外部 EPG および L3Out がサイトに展開されたら、L3out または外部 EPG の VRF を変更する場合は、最初に既存のオブジェクトを展開解除し、L3Out と外部 EPG の両方で VRF を変更してから、2 つのオブジェクトを再展開します。

ステップ 3 外部 EPG を作成します。

a) [スキーマ編集 (Schema edit)] ビューで、**[外部 EPG (External EPG)]** エリアまでスクロールし、[+ をクリックして、新しい外部 EPG をクリックします。

b) 右側のプロパティ ペインで、サイト タイプとして **[オンプレミス (On-Prem)]** を選択します。

ステップ 4 外部 EPG の基本的なプロパティを設定します。

a) 右側のプロパティ サイドバーで、外部 EPG の表示名を指定します。

b) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、先ほど作成した VRF を選択します。

これは、L3Out に関連付けた VRF と同じである必要があります。

（注）
外部 EPG および L3Out がサイトに展開されたら、L3out または外部 EPG の VRF を変更する場合は、最初に既存のオブジェクトを展開解除し、L3Out と外部 EPG の両方で VRF を変更してから、2 つのオブジェクトを再展開します。

c) **[+ コントラクトを追加（+ Add Contract）]** をクリックして、外部 EPG が他の EPG と通信するためのコントラクトを追加します。

すでにコントラクトを作成している場合は、ここでコントラクトを割り当てることができます。それ以外の場合、後ほど作成する予定のコントラクトは、この画面に戻って割り当てることができます。

コントラクトを割り当てる場合：

- 契約をプロバイダとしての外部 EPG に関連付ける場合には、外部 EPG に関連付けられているテナントから、コントラクトだけを選択します。その他のテナントからは、コントラクトを選択しないでください。
- コントラクトをコンシューマとしての外部 EPG に関連付ける場合には、利用可能な任意のコントラクトから選択できます。

ステップ 5 オンプレミス ファブリックの外部 EPG を設定する場合は、**[サイト タイプ (Site Type)]**を `［オンプレミス (on-prem)］` に設定し、外部 EPG のオンプレミス プロパティを設定します。

a) **[L3Out]** ドロップダウン メニューから、前の手順で作成した L3Out を選択します。

（注）
テンプレート レベルまたはサイトローカル レベルで L3Out を選択できます。サイトローカル レベルで外部 EPG の L3Out を設定することを推奨します。これを行うには、割り当てられているサイトの下の左側のサイドバーでテンプレートを選択します。次に、外部 EPG を選択し、L3Out をそれに関連付けます。

b) **[+ サブネット (+Subnet)]** をクリックしてサブネットを追加します。

これは、分類サブネットまたはルート制御に使用されるサブネットです。

c) **[サブネット追加 (Add Subnet)]** ウィンドウで、サブネットのプレフィックスを入力します。

d) 必要な **[ルート制御 (Route Control)]** オプションを選択します。

次のいずれかのオプションを 1 つ、または複数選択できます。

- **[エクスポート ルート制御 (Export Route Control)]** より、ルートマップを有効にして、指定されたサブネット プレフィックスに一致する外部プレフィックスを L3Out からアドバタイズできるようにしいます。これらは、中継ルーティングの使用例で他の L3Out から学習したプレフィックスです。

  `0.0.0.0/0` サブネットを追加し、エクスポート ルート制御オプションを有効にすると、**[集約エクスポート (Aggregate Export)]** オプションが使用可能になります。これにより、他の L3Out から学習したすべての外部プレフィックスをアドバタイズできます。このオプションを無効のままにすると、他の L3Out から学習したデフォルト ルートのみがこの L3Out からアドバタイズされます。

- **[インポート ルート制御 (Import Route Control)]** は、入力ルートマップを設定して、L3Out からファブリックにインポートするプレフィックスを制御します。**[インポート ルート制御 (Import Route Control)]** は、L3Out でルーティング プロトコルとして BGP を使用する場合にのみ使用できます。

  `0.0.0.0/0` サブネットを追加し、インポート ルート制御オプションを有効にすると、**[集約インポート (Aggregate Import)]** オプションが使用可能になります。これは、入力ルートを除き、エクスポート ルート制御の場合と同様に機能します。

- **[共有ルート制御 (Shared Route Control)]** は、共有 L3Out の使用例で使用され、外部ルータから学習したプレフィックスを、この L3Out を使用する他の VRF にアドバタイズできます。

  共有ルート制御オプションを有効にすると、**[集約教諭ルート]** オプションが使用可能になります。繰り返しますが、これは前の2つの集約ルートオプションに似ています。ただし、`0.0.0.0/0` 以外のサブネットで使用できます。

e) **[外部 EPG 分類 (External EPG Classification)]** オプションを選択します。

外部エンティティをこの特定の外部 EPG にマッピングできるようにするには、設定されたサブネットの **[外部 EPG 向けの外部サブネット(External Subnets for External EPG)]** オプションをオンにする必要があります。これにより、これらの外部ネットワークとファブリック内で定義された EPG に属するエンドポイント間にセキュリティポリシー（コントラクト）を適用できます。`0.0.0.0/0` プレフィックスに対してこのフラグを有効にすると、すべての外部宛先がこの外部 EPG の一部と見なされます。

このオプションを有効にすると、**[共有セキュリティインポート (Shared Security Import)]** オプションが使用可能になり、サブネットから VRF 間（共有サービス）での使用例のエンドポイントへのアクセスが可能になります。

これらの両方のオプションでは、アクセスは引き続きコントラクト ルールに従います。

ステップ 6 クラウド ファブリックの外部 EPG を設定する場合は、**[サイト タイプ (Site Type)]** を `[クラウド (cloud)]` に設定し、外部 EPG のクラウド プロパティを設定します。

a) **[アプリケーション プロファイル (Application Profile)]** ドロップダウンから、アプリケーション プロファイルを選択します。
b) **[+ セレクタの追加 (+ Add Selector)]** をクリックして、EPG のクラウド エンドポイント セレクタを追加します。

ステップ 7 （オプション）優先グループにこの外部EPGを含める場合は、**[優先グループに含める（Include in Preferred Group）]** チェックボックスをオンにします。

EPG優先グループの詳細については、EPG 優先のグループ概要と制限（227 ページ）を参照してください。

スキーマの表示

1 つまたは複数のスキーマを作成すると、[ダッシュボード (Dashboard)] および [スキーマ (Schemas)] ページの両方に表示されます。

これら 2 つのページで使用可能な機能を使用して、展開時の使用率とスキーマの状態をモニタできます。Nexus Dashboard Orchestrator GUI を使用して、実装されたスキーマ ポリシーの特定の領域にアクセスして編集することもできます。

テンプレート オブジェクトの一括更新

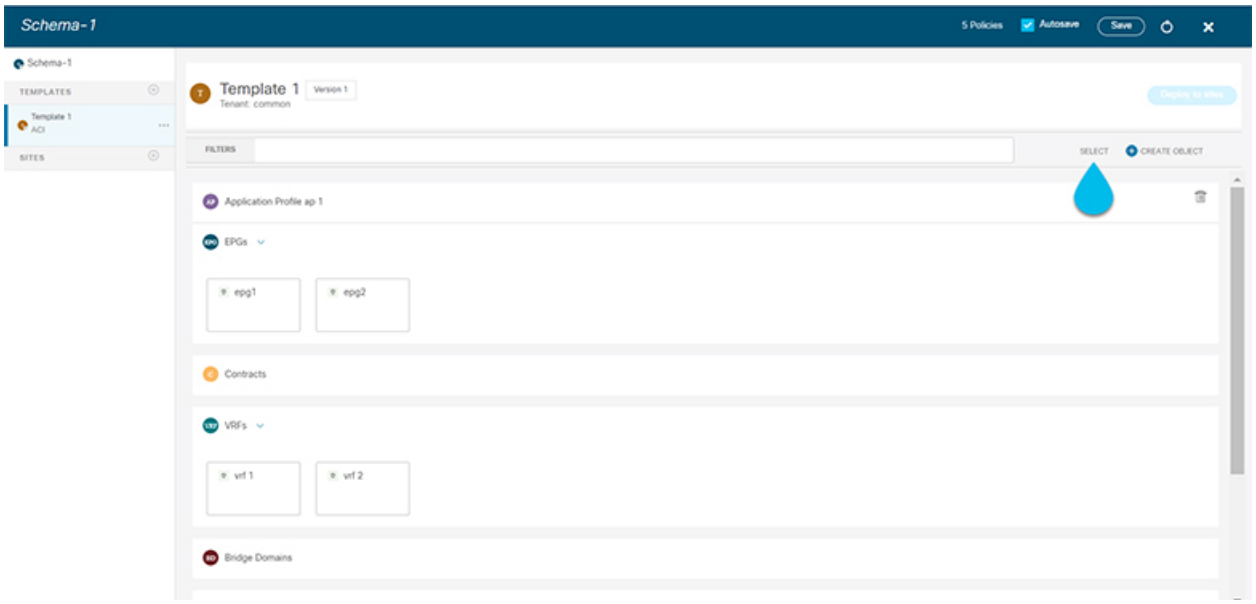
一括更新機能を使用すると、テンプレート内の同じタイプの複数の異なるオブジェクトの複数のプロパティを一度に更新できます。たとえば、各オブジェクトを個別に変更する代わりに、同時に 2 つ以上の EPG にインフラ EPG 分離を適用できます。このワークフローを使用する場合、選択したすべてのオブジェクトは同じタイプである必要があります。たとえば、EPG と BD を同時に更新することはできません。

選択したオブジェクトにすでに別のプロパティ値が構成されている場合、更新により、それらのプロパティが指定した値で上書きされます。この機能により、オンプレミスのテンプレート レベルのオブジェクト プロパティを更新できます。サイトローカル プロパティとクラウド プロパティの更新はサポートされていません。

（注） この機能は、Cisco APIC および Cisco NDFC ファブリックでのみサポートされています。 Cisco Cloud Network Controller サイトではサポートされていません。

手順

ステップ 1 更新するオブジェクトが含まれているスキーマとテンプレートに移行します。
ステップ 2 メインのペインから、**[選択（Select）]** を選択します。同じタイプのオブジェクトを複数選択できます。

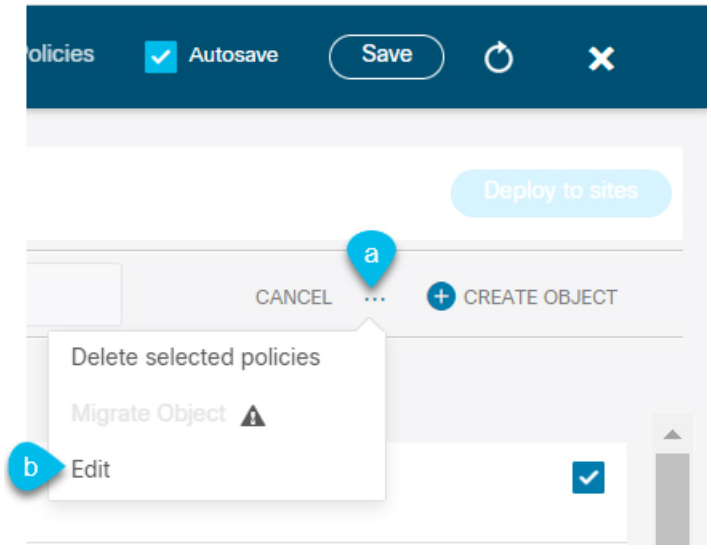


ステップ 3 更新するすべてのオブジェクトを選択した後。

a) キャンセル オプションの横にある [...] を選択します。

b) ドロップダウンから [編集（Edit）] を選択します。

異なるタイプのオブジェクトを選択した場合、ドロップダウンに [編集（Edit）] オプションは表示されません。



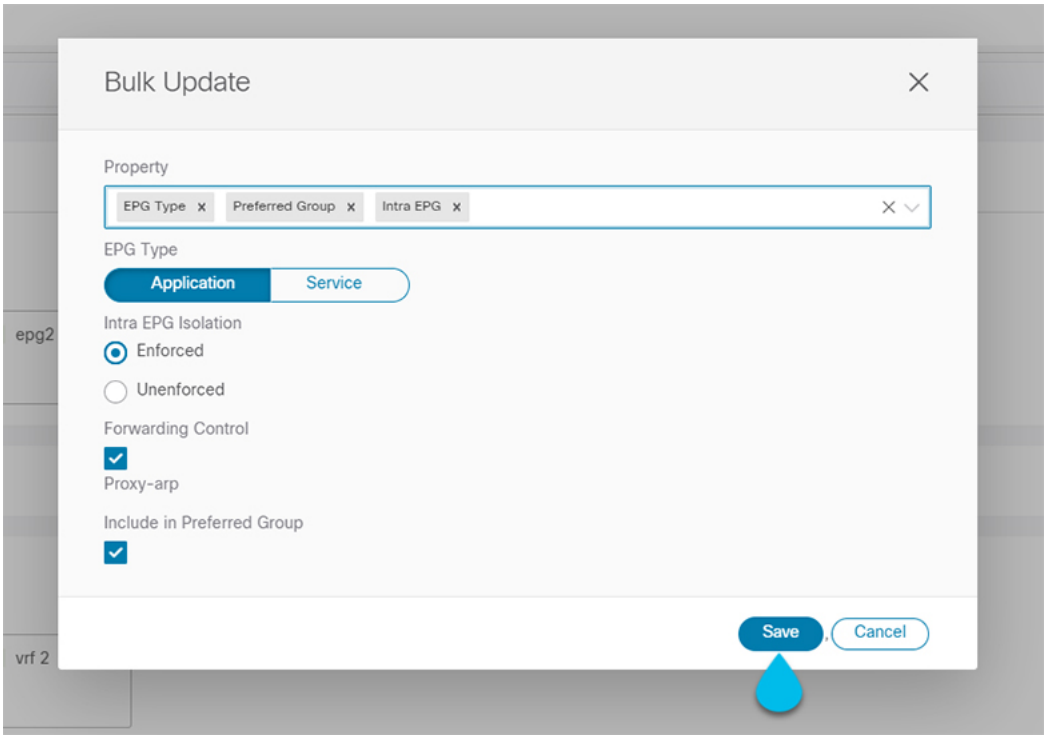
ステップ 4 [編集（Edit）] を選択すると、ポップアップが表示されます。選択したオブジェクトのプロパティのサブセットが表示されます。

選択したオブジェクトのタイプに基づいて、次のプロパティを更新できます。

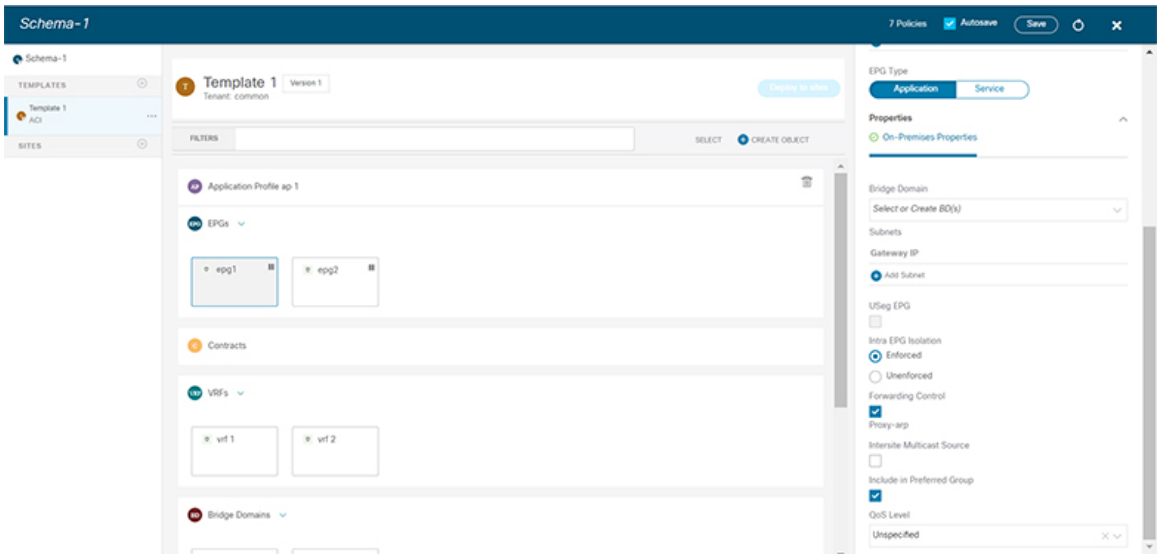
1. **[EPG]**：ブリッジ ドメイン、コントラクト、EPG タイプ、インフラ EPG、優先グループ。

2. **[コントラクト（Contracts）]**：範囲、フィルターチェーン、QOS レベル。
3. **[VRF]**：IP データ プレーン学習。
4. **[ブリッジ ドメイン（Bridge Domain）]**：仮想ルーティングとフォワーワーディング、L2 ストレッチ、L2 不明なユニキャスト、不明なマルチキャスト フラッディング、IPv6 不明なマルチキャスト フラッディング、複数宛先フラッディング、DHCP ポリシー、ユニキャスト ルーティング。
5. **[外部 EPG（External EPG）]**：コントラクト、外部 EPG タイプ、優先グループ。

ステップ 5 すべてのフィールドを選択したら、更新します。[保存（Save）] を選択すると、先ほど行った更新が実装されます。



ステップ 6 更新を保存すると、行った変更を確認できます。



サイトへのテンプレートの割り当て

ここでは、サイトにテンプレートを割り当てる方法について説明します。

始める前に

このドキュメントの前のセクションで説明したように、作成されたサイトには、展開するスキーマ、テンプレート、およびオブジェクトが必要です。

手順

ステップ 1 展開する 1 つ以上のテンプレートを含むスキーマに移動します。

ステップ 2 左側のサイドバーで、サイトに割り当てるテンプレートを選択します。

ステップ 3 **[テンプレート プロパティ（Template Properties）]** 表示内で **[アクション（Actions）]** をクリックして **[サイトの関連付け（Sites Association）]** を選択します。

[<template-name> にサイトの関連付け（Associate Sites to <template-name>）] ウィンドウが開きます。

ステップ 4 **[サイトの関連付け（Associate Sites）]** ウィンドウで、テンプレートを展開するサイトの横のチェックボックスをオンにします。

選択したテンプレートのタイプとサイト間のサイト間接続によっては、一部のサイトを割り当てに使用できない場合があることに注意してください。

- クラウド ローカル テンプレートを割り当てる場合は、単一のクラウド サイトにのみ割り当てることができます。

- テンプレートを複数のサイトに割り当てる場合、BGP-EVPN プロトコルを使用して、それらのサイト間のサイト間接続を確立する必要があります。パーシャル メッシュ接続があるサイトを選択した場合、サイト間接続がないサイト、またはBGP-IPv4 を使用してサイト間接続が確立されているサイトはグレー表示され、割り当てに使用できません。

ステップ 5 [OK] をクリックします。

一度に 1 つのテンプレートを展開するため、展開できるようにするには、少なくとも 1 つのサイトにテンプレートを関連付ける必要があります。

サイトからのテンプレートの関連付け解除

展開を解除せずに、サイトからテンプレートの関連付けを解除することもできます。これにより、NDO からサイトに展開された設定を保持しながら、スキーマのテンプレートとサイトの関連付けを削除できます。管理対象オブジェクトとポリシーの所有権が NDO からサイトのコントローラに移されます。

始める前に

- テンプレートとその設定がサイトにすでに展開されている必要があります。
- テンプレートは、単一のサイトにのみ展開し、サイト間で展開しないようにする必要があります。
- テンプレートで定義されたオブジェクトは、他のサイトのシャドウオブジェクトとして展開しないでください。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

ステップ 3 関連付けを解除するテンプレートを含むスキーマをクリックします。

ステップ 4 スキーマ ビューで、関連付けを解除する特定のサイトの下のテンプレートを選択します。

ステップ 5 **[アクション (Actions)]** メニューから **[テンプレートの関連付け解除 (Disassociate Template)]** を選択します。

ステップ 6 確認ウィンドウで、**[アクションの確認 (Confirm Action)]** をクリックします。

テンプレートの展開

ここでは、新しいポリシーまたは更新されたポリシーをACIファブリックに展開する方法について説明します。

始める前に

- このドキュメントの前のセクションで説明したように、作成されたサイトには、展開するスキーマ、テンプレート、およびオブジェクトと、1つまたは複数のサイトに割り当てられるテンプレートが必要です。
- テンプレートのレビューと承認 （70 ページ）で説明しているように、テンプレートの確認と承認が有効になっている場合は、必要な数の承認者によってテンプレートがすでに承認されている必要があります。
- スキーマとテンプレート設計上の考慮事項 （19 ページ）で説明されている必要な展開の順序とオブジェクトの依存関係を理解していることを確認してください。

手順

ステップ 1 展開するテンプレートを含むスキーマに移動します。

ステップ 2 **[表示（View）]** ドロップダウン メニューから、展開するテンプレートを選択します。

ステップ 3 テンプレート ビューで、**[サイトに展開（Deploy to site）]** をクリックします。

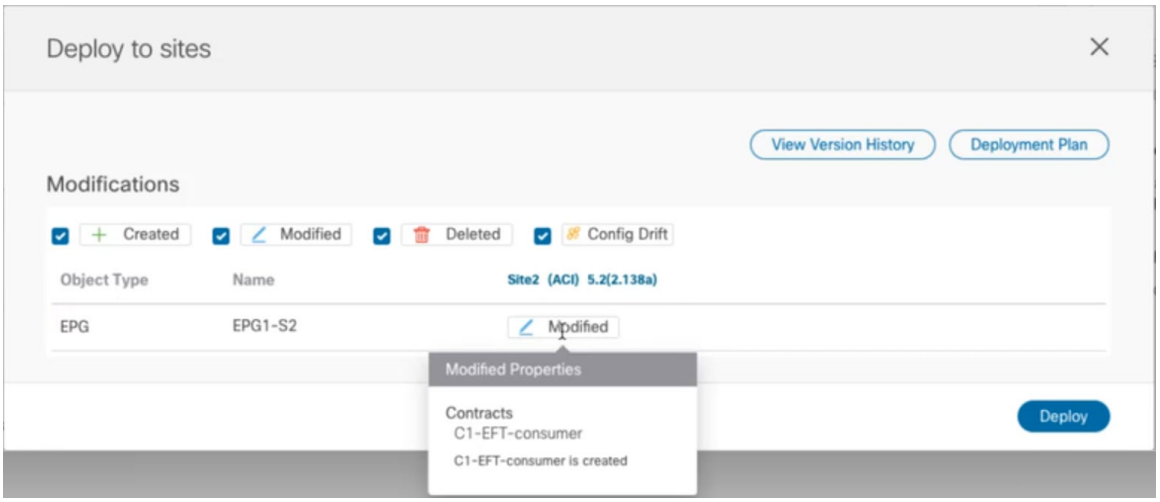
[サイトに展開 (Deploy to Sites)] ウィンドウが開き、展開するオブジェクトの概要が表示されます。

ステップ 4 テンプレートに変更を加えた場合は、**[展開の計画（Deployment Plan）]** を確認して新しい構成を確認します。

以前にこのテンプレートを展開したが、それ以降に変更を加えていない場合は、**[展開]** の概要に変更がないことが示され、テンプレート全体を再展開することを選択できます。この場合は、この手順をスキップできます。

[サイトに展開 (Deploy to Sites)] ウィンドウには、サイトに展開される構成の違いの概要が表示されます。次のスクリーンショットは、サイト 2 の既存の EPG（EPG1-S2）にコンシューマコントラクトを追加する簡単な例を示しています。

（注）
この場合、構成の違いのみがサイトに展開されます。テンプレート全体を再展開したい場合、違いを同期するために1回展開をする必要があります。そして、前のパラグラフに記されている通り、構成全体をプッシュするためにまた再展開する必要があります。



情報目的で [作成日 (Created)]、[変更日 (Modified)]、および [削除済み (Deleted)] チェックボックスを使用してビューをフィルタリングすることもできますが、**[展開(Deploy)]**をクリックするとすべての変更が展開されることに注意してください。

ここでは、次のことも選択できます。

- **[バージョン履歴の表示(View Version History)]** を選択すると、完全なバージョン履歴とバージョンアップグレードで行われた更新内容を表示します。バージョン履歴の詳細については、履歴の表示と以前のバージョンの比較 （66 ページ）を参照してください。
- **[展開プラン(Deployment Plan)]**を確認して、このテンプレートから展開される構成の可視化とXMLペイロードを表示します。

  この機能により、テンプレートに変更を加えて1つ以上のサイトに展開した後に、Orchestratorがマルチサイトドメインの一部であるさまざまなファブリックにプロビジョニングする構成の変更を、より適切に可視化できます。

  テンプレートとサイト構成に加えられた特定の変更のリストを引き続き提供していたNexus Dashboard Orchestratorの以前のリリースとは異なり、展開プランでは、テンプレートの展開によってさまざまなファブリック全体にプロビジョニングされる、すべてのオブジェクトに対する完全な可視性が提供されます。たとえば、変更内容によっては、特定の変更が1つのサイトのみに適用された場合でも、シャドウオブジェクトが複数のサイトに作成される場合があります。

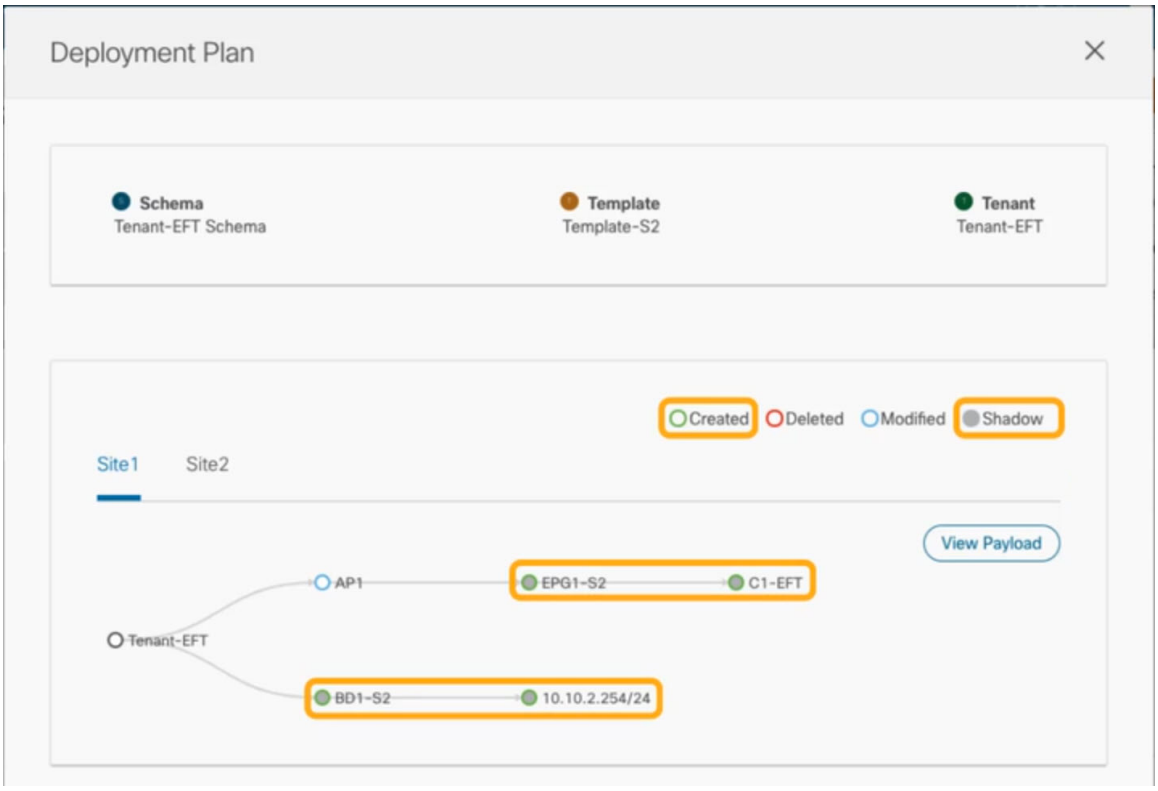
  （注）
  テンプレートを展開する前に、この手順で説明されているように、展開プランを使用して変更を確認することをお勧めします。構成変更の視覚的に示すことは、意図しない構成変更の展開による潜在的なエラーを低減するのに役立ちます。

a) [**展開プラン（Deployment Plan**）] ボタンをクリックします。

   前のステップで示したのと同じ例で続けると、コンシューマコントラクトがサイト 2 の既存の EPG に追加され、展開計画では、サイト 2 への変更の結果として、サイト 1 に展開される追加の変更があることも確認できます。

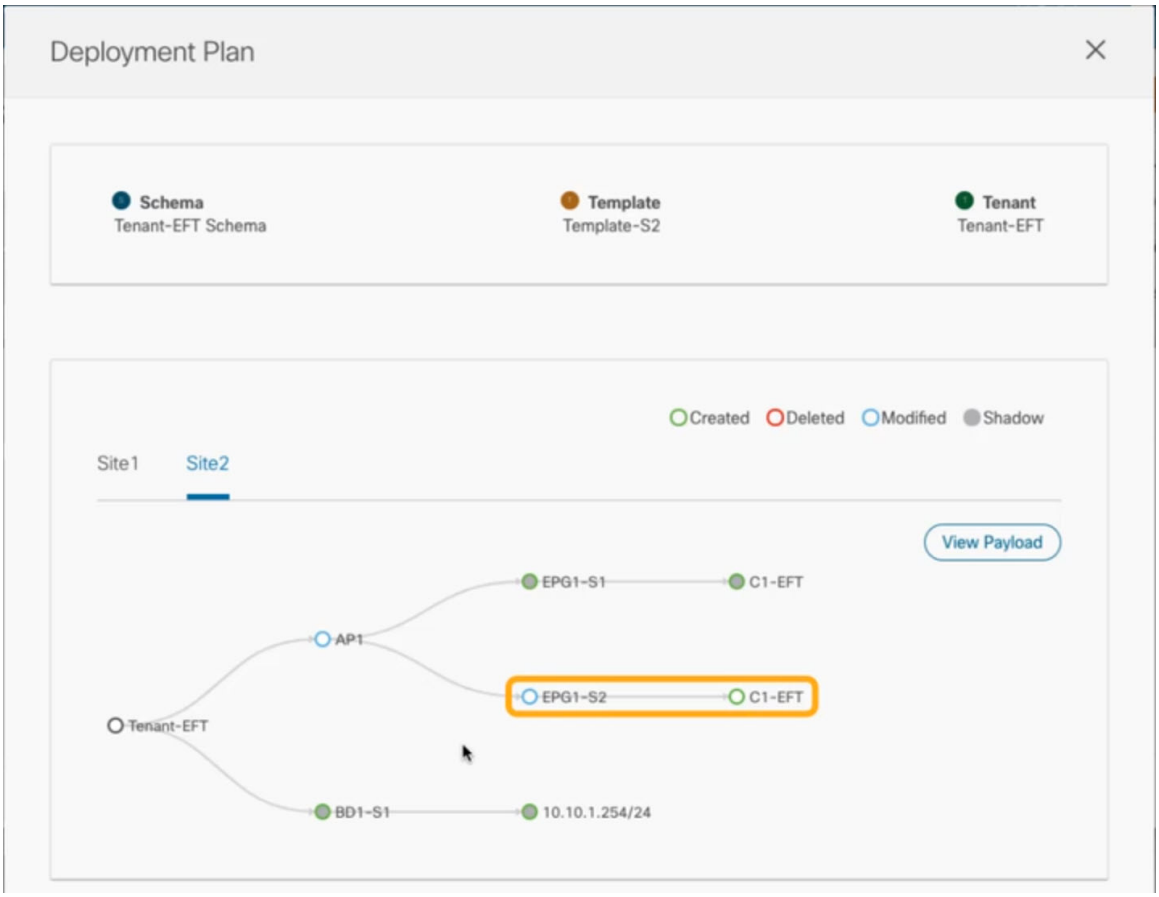
b) 最初にリストされたサイトで変更を確認します。

強調表示された凡例に基づいて、Orchestrator がサイト 2 の EPG に追加したコントラクトに必要なシャドウ オブジェクトをサイト 1 に作成することがわかります。



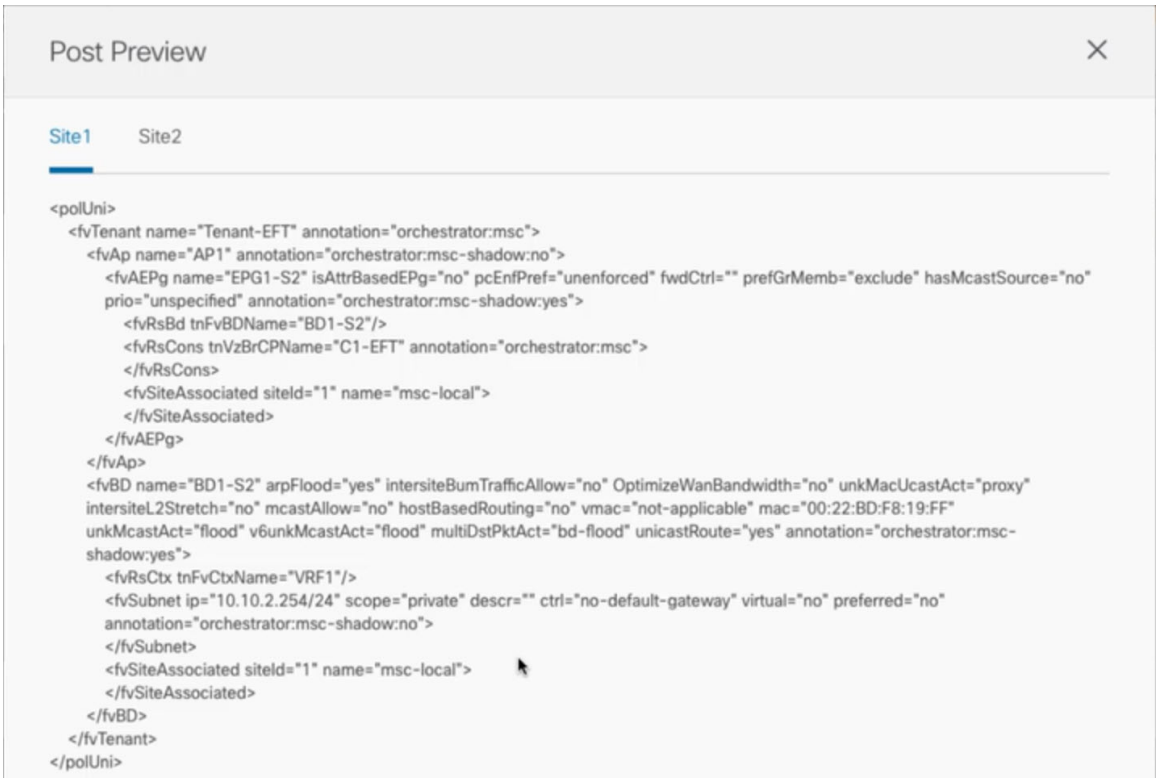
c) 前のサブステップを繰り返して、他のサイトの変更を確認します。

ここでは、コントラクト（C1-EFT）をサイト 2 に割り当てたときに、サイト 2 の EPG（EPG1-S2）に明示的に加えた変更と、そのコントラクトを提供している他のサイトの EPG（EPG1-S1）のシャドウオブジェクトを確認できます。



d) （オプション）[**ペイロードの表示（View Payload**）] をクリックすると、各サイトの XML ペイロードを表示できます。

新規および変更されたオブジェクトの視覚的表現に加えて、各サイトの変更について [**ペイロードの表示（View Payload**）] を選択することもできます。



e) 変更の確認が完了したら、[x] アイコンをクリックして [**展開プラン（Deployment Plan**）] 画面を閉じます。

ステップ 5 [**サイトに展開（Deploy to sites**）] ウィンドウで、[**展開（Deploy**）] をクリックしてテンプレートを展開します。

テンプレートの展開解除

ここでは、サイトからテンプレートを展開解除する方法について説明します。

始める前に

- テンプレートを最後に展開してから、テンプレートに変更を加えていないことを確認します。

  最後に展開された後に変更されたテンプレートを展開解除すると、テンプレートに展開されたオブジェクトのセットが、テンプレートに変更を加えた後に展開解除しようとするオブジェクトのセットと異なるため、設定がずれる可能性があります。

- ルート リーク構成で使用される VRF を含むテンプレートを展開解除する場合、そのテンプレートを展開解除する前に、ルート リークを削除する必要があります。

手順

ステップ 1 展開解除するテンプレートを含むスキーマを選択します。

ステップ 2 **[表示（View）]** ドロップダウンから、展開を解除するテンプレートを選択します。

ステップ 3 **[アクション（Action）]** メニューで、**[すべてのサイトから展開を解除する（Undeploy from all sites）]** をクリックします。

テンプレートのバージョニング

テンプレートが保存されるたびに、新しいバージョンのテンプレートが作成されます。NDO UI 内から、テンプレートのすべての設定変更の履歴を、変更者と変更日時に関する情報とともに表示できます。以前のバージョンを現在のバージョンと比較することもできます。

新しいバージョンはスキーマ レベルではなくテンプレート レベルで作成されるため、各テンプレートを個別に設定、比較、ロールバックできます。

テンプレート バージョンは、次のルールに従って作成および管理されます。

- すべてのテンプレート バージョンは、Deployed または Intermediate のいずれかです。

  Deployed — サイトに展開されたテンプレートのバージョン。

  Intermediate — 変更および保存されたが、サイトに展開されていないテンプレートのバージョン。

- テンプレートごとに最大 20 の Deployed バージョンと 20 の Intermediate バージョンをいつでも保存できます。
- 20 バージョンの制限を超える新しい Intermediate バージョンが作成されると、最も古い既存の Intermediate バージョンが削除されます。
- テンプレートが展開され、新しい Deployed バージョンが作成されると、すべての Intermediate バージョンが削除されます。新しい Deployed バージョンが 20 バージョン制限を超えると、最も古い既存の Deployed バージョンが削除されます。
- バージョンに Golden のタグを付けても、保存されているテンプレート バージョンの数には影響しません。
- `Golden` のタグが付いたテンプレートは削除できません。

  テンプレートを削除する前に、まずタグを解除する必要があります。

- テンプレートが変更されて保存または展開されると、20 の Deployed および 20 の Intermediate スケールを超えるバージョンは、上記のルールに従って削除されます。
- 4.0(1) より前のリリースからリリース 4.0(1) 以降にアップグレードする場合、テンプレートの最新バージョンのみが保持されます。

タギング テンプレート

任意の時点で、テンプレートの現在のバージョンに「ゴールデン」のタグを付けることができます。たとえば、完全に検証された設定で確認、承認、および展開されたバージョンを示すために、今後の参照用に選択できます。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

ステップ 3 表示するテンプレートを含むスキーマをクリックします。

ステップ 4 [スキーマ (Schema)]ビューで、確認するテンプレートを選択します。

ステップ 5 テンプレートのアクション（**...**）メニューから、**[タグ（Tag）]** を選択します。

テンプレートがすでにタグ付けされている場合、オプションは**[タグを解除（Un-Tag）]** に変更され、現在のバージョンからタグを削除できます。

タグ付けされたバージョンは、テンプレートのバージョン履歴画面でスターアイコンで示されます。

履歴の表示と以前のバージョンの比較

ここでは、テンプレートの以前のバージョンを表示し、現在のバージョンと比較する方法について説明します。

手順

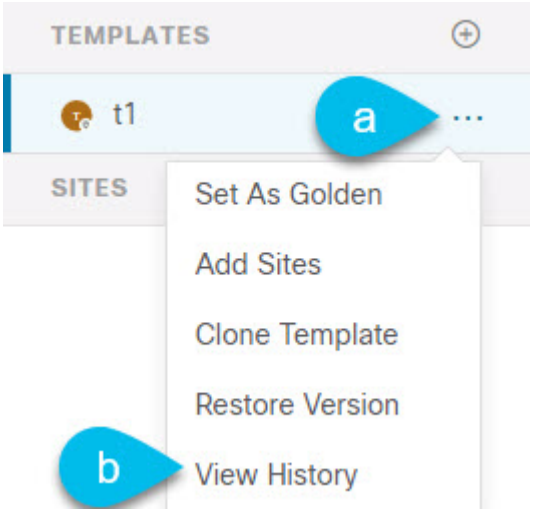
ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

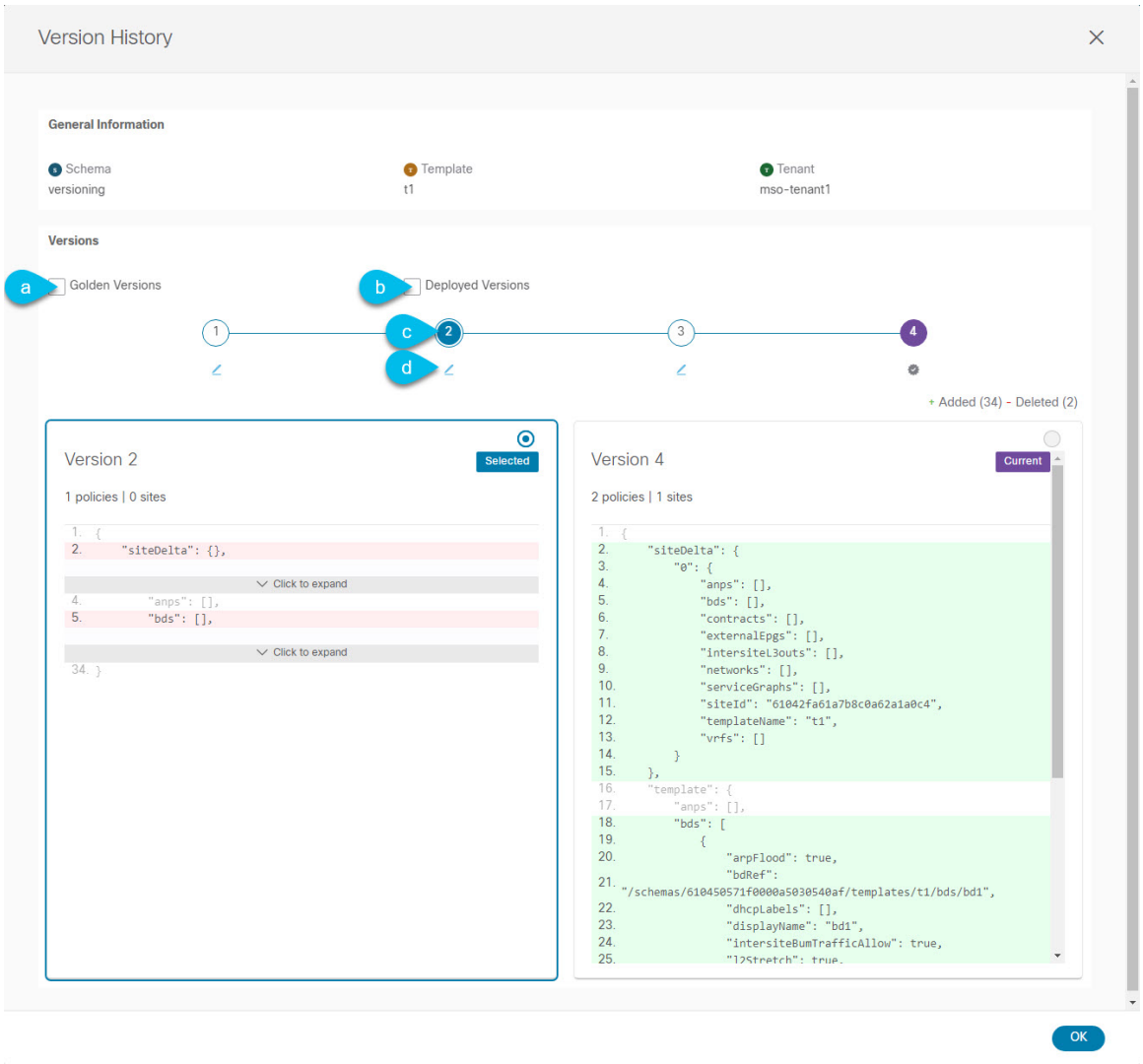
ステップ 3 表示するテンプレートを含むスキーマをクリックします。

ステップ 4 [スキーマ (Schema)]ビューで、確認するテンプレートを選択します。

ステップ 5 テンプレートのアクション（**...**）メニューから、**[履歴（History）]** を選択します。



ステップ 6 **[バージョン履歴 (Version History)]** ウィンドウで、適切な選択を行います。



a) **[ゴールデン バージョン (Golden Versions)]** チェックボックスをオンにして、以前のバージョンのリストをフィルタリングし、`Golden` としてマークされていたこのテンプレートのバージョンのみを表示します。

「Golden」としてのテンプレートのタグ付けについては、タギング テンプレート （66 ページ）を参照してください。

b) 以前のバージョンのリストをフィルタリングして、サイトに展開されていたこのテンプレートのバージョンのみを表示するには、**[展開済みバージョン (Deployed Versions)]**チェックボックスをオンにします。

新しいテンプレート バージョンは、テンプレートが変更され、スキーマが保存されるたびに作成されます。ある時点でサイトに実際に展開されたテンプレートのバージョンのみを表示するように選択できます。

c) 特定のバージョンをクリックして、現在のバージョンと比較します。

選択したバージョンは、常にテンプレートの現在のバージョンと比較されます。**[ゴールデンバージョン (Golden Versions)]** または **[導入済みバージョン (Deployed Versions)]** フィルタを使用してリストをフィルタリングした場合でも、導入済みまたはゴールデンとしてタグ付けされていない場合でも、現在のバージョンが常に表示されます。

d) **[編集 (Edit)]** アイコンの上にマウスを置くと、バージョンの作成者と作成日時に関する情報が表示されます。

ステップ 7 **[OK]** をクリックして、バージョン履歴ウィンドウを閉じます。

以前の製品バージョンへの復元

ここでは、以前のバージョンのテンプレートを復元する方法について説明します。テンプレートを元に戻す場合、次のルールが適用されます。

- ターゲットバージョンが存在しないオブジェクトを参照している場合、復元操作は許可されません。
- ターゲットバージョンが NDO で管理されなくなったサイトを参照している場合、復元操作は許可されません。
- 現在のバージョンが、ターゲットバージョンが展開されていない1つ以上のサイトに展開されている場合、復元操作は許可されません。

  テンプレートを元に戻す前に、まずそれらのサイトから現在のバージョンを展開解除する必要があります。
- ターゲットバージョンが、現在のバージョンが展開されていない1つ以上のサイトに展開されている場合、復元操作は許可されます。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

ステップ 3 表示するテンプレートを含むスキーマをクリックします。

ステップ 4 [スキーマ (Schema)]ビューで、確認するテンプレートを選択します。

ステップ 5 **[アクション（Actions）]**（**[...]**）メニューから、**[ロールバック（Rollback）]** を選択します。

ステップ 6 **[ロールバック（Rollback）]** ウィンドウで、復元する以前のバージョンのいずれかを選択します。

[ゴールデン バージョン (Golden Versions)] チェックボックスと**[展開済みバージョン (Deployed Versions)]** チェックボックスを使用して、バージョンのリストをフィルタリングできます。

バージョンを選択すると、そのバージョンのテンプレート設定をテンプレートの現在のバージョンと比較できます。

ステップ 7 **[復元 (Restore)]** をクリックして、選択したバージョンを復元します。

以前のバージョンを復元すると、前の手順で選択したバージョンと同じ設定の新しいバージョンのテンプレートが作成されます。

たとえば、最新のテンプレートバージョンが 3 で、バージョン 2 を復元すると、バージョン 4 が作成されます。バージョン 2 の設定と同じだからです。復元を確認するには、テンプレートのバージョン履歴を参照し、現在の最新バージョンと復元時に選択したバージョンを比較します。

テンプレートのレビューと承認（変更管理）が無効になっており、アカウントにテンプレートを展開するための適切な権限がある場合は、復元したバージョンを展開できます。

ただし、変更制御が有効になっている場合は、次のようになります。

- 以前に展開したバージョンに戻し、アカウントにテンプレートを展開するための正しい権限がある場合は、すぐにテンプレートを展開できます。
- 以前に展開されていなかったバージョンに戻す場合、またはアカウントにテンプレートを展開するための適切な権限がない場合は、復元されたバージョンを展開する前にテンプレートの承認を要求する必要があります。

  レビューと承認プロセスに関する追加情報については、テンプレートのレビューと承認 （70ページ）セクションを参照してください。

テンプレートのレビューと承認

テンプレートのレビューと承認（変更管理）ワークフローは、テンプレートの設計者、レビュー担当者、承認者、およびテンプレートの導入者に指定されたロールを設定し、また、導入した設定が検証プロセスを確実にパスできるようにします。

テンプレート設計者は、NDO UI 内から、作成したテンプレートのレビューを要求できます。その後、レビュー担当者は、テンプレートのすべての設定変更の履歴と、誰がいつ変更したかに関する情報を表示できます。この時点で、テンプレートの現在のバージョンを承認または拒否できます。テンプレート設定が拒否された場合、テンプレート設計者は必要な変更を行い、レビューを再要求できます。テンプレートが承認されると、展開担当者のロールを持つユーザがサイトに展開できます。最後の点として、導入者自身が承認済みテンプレートの導入を拒否し、レビュー プロセスを最初からやり直すことができます。

ワークフローはスキーマ レベルではなくテンプレート レベルで実行されるため、各テンプレートを個別に設定、確認、承認できます。

テンプレート承認要件の有効化

テンプレートの設定と展開に確認と承認のワークフローを使用するには、Nexus Dashboard Orchestrator のシステム設定でこの機能を有効にする必要があります。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション メニューで、**[インフラストラクチャ (Infrastructure)]** > **[システムの設定 (System Configuration)]**を選択します。

ステップ 3 **[変更制御 (Change Control)]** タイルで、**[編集 (Edit)]** アイコンをクリックします。

ステップ 4 **[コントロールを変更（Change Control）]** ウィンドウで、**[有効（Enabled）]** を選択して機能を有効にします。

ステップ 5 **[承認者 (Approvers)]** フィールドに、テンプレートを展開する前に必要な一意の承認の数を入力します。

ステップ 6 [保存（Save）] をクリックして、変更内容を保存します。

必要なロールを持つユーザの作成

テンプレートの設定と展開のため、レビューと承認のワークフローを実施する前に、NDO サービスが展開されているNexusダッシュボードで必要な権限を持つユーザーを作成する必要があります。

手順

ステップ 1 Nexus Dashboard の GUI にログインします。

NDO GUI でユーザーを作成または編集することはできません。サービスが展開されている Nexus ダッシュボード クラスタに直接ログインする必要があります。

ステップ 2 左のナビゲーション メニューから、**[管理 コンソール（Admin Console）]** > **[管理ユーザー（Administrative Users）]** > **[ユーザー（Users）]**を選択します。

ステップ 3 必要なユーザーを作成します。

ワークフローは、テンプレート設計者、承認者、および展開者という 3 つの異なるユーザー ロールに依存します。各ロールを異なるユーザーに割り当てることも、同じユーザーにロールの組み合わせを割り当てることもできます。管理者権限を持つユーザは、3 つのアクションすべてを実行できます。

Nexus Dashboard にはデザイナー ロールが事前定義されていないため、デザイナーの義務は、デフォルトの管理者ユーザーロールに加えて、書き込み権限を持つテナント マネージャーまたはサイト マネージャー ユーザーに割り当てられます。

- テナント マネージャーは、デザイナーが特定のテナント（またはテナントのサブセット）にのみ関連付けられているテンプレートに変更を加える必要がある場合に使用する必要があります。この場合、ユーザーを特定のテナントにマッピングする必要があります。
- サイト マネージャーは、デザイナーが異なるテナントに属するテンプレートに変更を加える必要がある場合使用する必要があります。

デザイナー ロールとは対照的に、Nexus Dashboard には、ユーザーに関連付けることができる事前定義された承認者および展開者の役割があります。承認者および展開者のロールは、設計上、特定のテナントにバインドされていません。ただし、デザイナーと承認者（またはデザイナーと展開者）の両方の権限を持つユーザーロールを作成する場合は、上記と同じガイドラインに従ってください。

ローカルまたはリモートの Nexus ダッシュボード ユーザーのユーザーとその権限の設定の詳細については、『Nexus Dashboard User Guide』を参照してください。

承認者ロールを持つ別個のユーザーが、テンプレート承認要件の有効化 （70 ページ）で設定した承認の最小数と同数以上必要です。

（注）
変更制御ワークフロー機能を無効にすると、承認者と展開者のユーザーは Nexus Dashboard Orchestrator に読み取り専用でアクセスできます。

テンプレートのレビューと承認の要求

ここでは、テンプレートのレビューと承認を要求する方法について説明します。

始める前に

次のものが必要です。

- 承認要件のグローバル設定を有効にした（テンプレート承認要件の有効化 （70 ページ）を参照）。
- 承認者ロールと展開者ロールを使用してNexusダッシュボードでユーザを作成または更新した（必要なロールを持つユーザの作成 （71 ページ）を参照）。
- 1 つ以上のポリシー設定を含むテンプレートを作成し、1 つ以上のサイトに割り当てた。

手順

ステップ 1 テナント マネージャ、サイト マネージャ、または管理者 ロールを持つユーザーとして Nexus Dashboard Orchestrator GUI にログインします。

ステップ 2 テナント マネージャ ロールを割り当てた場合は、ユーザーをテナントに関連付けます。

サイト マネージャ または 管理者 ロールを使用していた場合は、この手順をスキップしてください。

テナント マネージャ ロールを割り当てる場合は、ユーザーが管理する特定のテナントにユーザーを関連付ける必要もあります。

a) 左型のナビゲーションメニューから、**[アプリケーション管理（Application Management）]**>**[テナント（Tenants）]** を選択します。
b) ユーザーが管理するテナントを選択します。
c) Nexus Dashboard で作成したデザイナー ユーザーの横にあるチェックボックスをオンにします。

d) ユーザーが管理する他のすべてのテナントについて、この手順を繰り返します。

ステップ 3 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 4 承認を要求するテンプレートを含むスキーマをクリックします。

ステップ 5 スキーマビューで、テンプレートを選択します。

ステップ 6 メイン ペインで、**[承認のために送信 (Send for Approval)]** をクリックします。

[承認のために送信 (Send for Approval)] ボタンは、次の場合には使用できません。

- グローバル変更制御オプションが有効になっていない
- テンプレートにポリシー設定がないか、どのサイトにも割り当てられていない
- ユーザにテンプレートを編集する権限がない
- テンプレートは承認のためにすでに送信されている
- テンプレートが承認者ユーザによって拒否された

テンプレートのレビューと承認

ここでは、テンプレートのレビューと承認を要求する方法について説明します。

始める前に

次のものが必要です。

- 承認要件のグローバル設定を有効にした（テンプレート承認要件の有効化 （70 ページ）を参照）。
- 承認者ロールと展開者ロールを使用してNexusダッシュボードでユーザを作成または更新した（必要なロールを持つユーザの作成 （71 ページ）を参照）。
- 1 つ以上のポリシー設定を含むテンプレートを作成し、1 つ以上のサイトに割り当てた。
- テンプレートのレビューと承認の要求 （72 ページ）に記載されているように、スキーマエディタによってテンプレートの承認が要求されました。

手順

ステップ 1 承認者 (Approver) または管理者 (admin) ロールを持つユーザとして Nexus Dashboard Orchestrator GUIにログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 3 確認して承認するテンプレートを含むスキーマをクリックします。

ステップ 4 スキーマビューで、テンプレートを選択します。

ステップ 5 メインペインで、**[承認 (Approve)]** をクリックします。

すでにテンプレートを承認または拒否している場合は、テンプレートデザイナが変更を行い、再確認のためにテンプレートを再送信するまで、このオプションは表示されません。

ステップ 6 **[テンプレートの承認 (Approving template)]** ウィンドウでテンプレートを確認し、**[承認 (Approve)]** をクリックします。

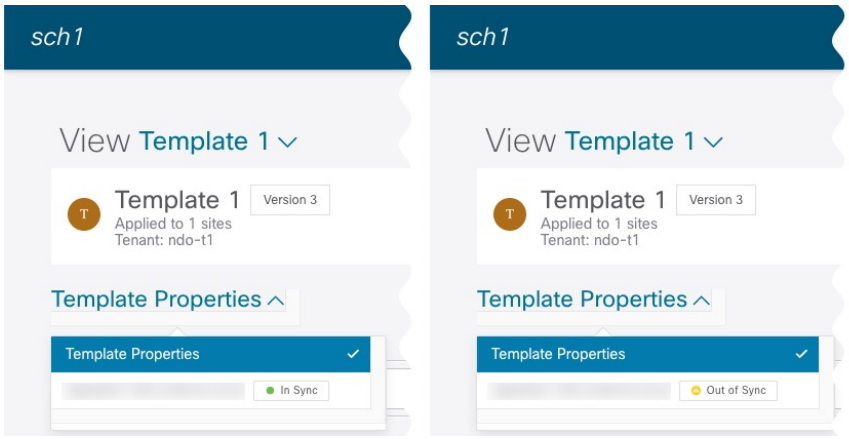
承認画面には、テンプレートがサイトに展開するすべての変更が表示されます。

[バージョン履歴の表示 (View Version History)] をクリックすると、完全なバージョン履歴と、バージョン間で行われた増分変更を表示できます。バージョン履歴の詳細については、履歴の表示と以前のバージョンの比較 （66 ページ）を参照してください。

[展開計画 (Deployment Plan)] をクリックして、このテンプレートから展開される設定の可視化と XML を表示することもできます。[展開計画 (Deployment Plan)] ビューの機能は、現在展開されている設定の表示（81 ページ）で説明した、すでに導入されているテンプレートの [展開ビュー (Deployed View)] に似ています。

設定のばらつき

APIC ドメインに実際に展開された設定が、Nexus Dashboard Orchestrator でそのドメインに対して定義された設定と異なる場合があります。これらの構成の不一致は、**[構成のばらつき（Configuration Drifts）]** と呼ばれ、次の図に示すように、テンプレート ビュー ページのサイト名の横に[同期されていません（Out of Sync）]の注意で示されます。



設定のばらつきは、さまざまな理由で発生する可能性があります。構成のばらつきを解決するために必要な実際の手順は、その原因によって異なります。最も一般的なシナリオとその解決策を次に示します。

- **NDO で設定が変更された**：NDO GUIでテンプレートを変更すると、変更をサイトに展開するまでは、設定のばらつきとして表示されます。

このタイプの設定のずれを解決するには、テンプレートを展開して変更をサイトに適用するか、スキーマの変更を元に戻します。

- **設定がサイトの APIC で直接変更された**：NDO から展開されたオブジェクトは、サイトの APIC で警告アイコンとテキストで示されます。管理ユーザー、設定のずれの原因に対し、引き続き変更を加えられます。

（注） APIC でオブジェクトが変更されるたびに、APIC は Nexus Dashboard Orchestrator に通知を送信します。通知を受信すると、Nexus Dashboard Orchestrator は 30 秒のタイマーを開始し（さらに通知が届くのを待ちます）、そのようなタイマーの期限が切れると、APIC への API 呼び出しを実行して、通知を受信したすべてのオブジェクトに加えられた変更に関する詳細情報を取得します。これにより、Nexus Dashboard Orchestrator は、それらのオブジェクトが定義されているすべてのテンプレートの UI にばらつきのシンボルを表示できます。この動作の唯一の例外は、Nexus Dashboard Orchestrator が、特定のテンプレートで定義されたオブジェクトのすべて（またはそのサブセット）の構成を展開する場合です。その場合、60 秒間、Nexus Dashboard Orchestrator は、それらの特定のオブジェクトに関して APIC から受信した通知を無視し、その結果、UI にばらつきのシンボルを表示できません。

- **NDO 設定がバックアップから復元された**：NDO のバックアップから設定を復元すると、バックアップが作成されたときのオブジェクトとその状態のみが復元され、復元された設定は自動的に再展開されません。そのため、バックアップが作成されてから構成に変更が加えられ、APIC に展開された場合、バックアップを復元すると構成のばらつきが作成される可能性があります。
- **NDO 設定は、古いリリースで作成されたバックアップから復元された**：新しいリリースで、以前のリリースではサポートされていなかったオブジェクトプロパティのサポートが追加された場合、これらのプロパティによって設定がずれる可能性があります。通常、これは、サイトの APIC GUI で新しいプロパティが直接変更され、Nexus Dashboard Orchestrator の想定値がデフォルトと異なる場合に発生します。
- **NDO が以前のリリースからアップグレードされた**：このシナリオは、新しいオブジェクトプロパティが新しいリリースに追加された場合に、既存の設定がずれている可能性がある、前のシナリオと似ています。

構成ドリフトを確認することをお勧めし、必要ならば、ドリフトの原因に対してもっと可視化して調整するためにテンプレートの「ばらつきの調整」ワークフローを実行します。この推奨事項は、このセクションで前述したすべてのばらつきのシナリオに適用されます。

設定のばらつきの調整

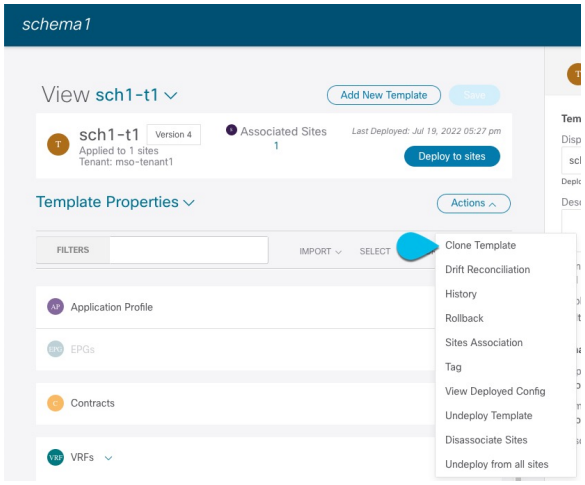
Nexus ダッシュボードオーケストレータへマルチサイトドメインの一部のサイトの APIC コントローラ内の適用された構成で定義されているようにテンプレートの構成を比べるためにばらつきの調整ワークフローを使用することができます。これにより、Nexus ダッシュボードオーケストレータまたは APIC で直接行われた可能性のある変更をよりよく可視化し、それらのドリフトを正しく解決する機会を提供します。

（注） テンプレートは、調整ワークフローの最後に **[保存（Save）]** または **[展開（Deploy）]** を選択した後にのみ更新および保存されます。ワークフローの途中で、すでに選択した変更を元に戻したい場合は、スキーマを閉じてから再度開いて、元の構成を復元できます。その後、ワークフローを最初から再実行できます。

手順

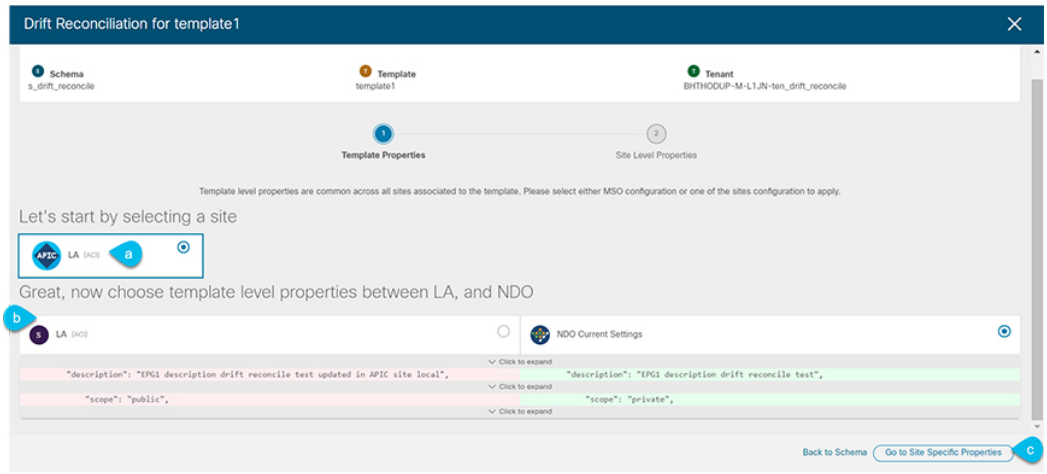
ステップ 1 設定のばらつきを確認するテンプレートを含むスキーマに移動します。

ステップ 2 テンプレートの **[アクション (Actions)]** メニューから、**[ばらつきの調整 (Reconcile Drift)]** を選択します。



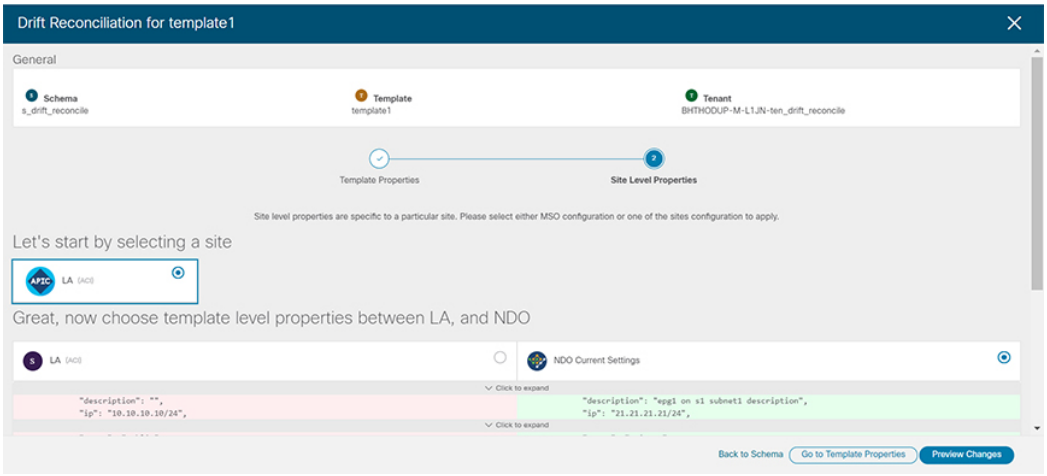
[ばらつきの調整 (Reconcile Drift)] ウィザードが開きます。

ステップ 3 **[ばらつきの調整 (Reconcile Drift)]** 画面で、各サイトのテンプレートレベルの構成を比較し、希望のものを選択します。



テンプレートレベルのプロパティは、テンプレートに関連付けられているすべてのサイトに共通です。Nexus Dashboard Orchestrator で定義されたテンプレート レベルのプロパティを各サイトでレンダリングされた構成と比較し、Nexus Dashboard Orchestrator テンプレートの新しい構成を決定できます。サイト構成の選択は、既存の Nexus Dashboard Orchestrator テンプレートのこれらのプロパティを変更し、その場合、Nexus Dashboard Orchestrator の構成を選択すると、既存の Nexus Dashboard Orchestrator テンプレートの設定はそのまま残されます

ステップ 4 **[サイト特有のプロパティに移動（Go to Site Specific Properties）]** をクリックして、サイトレベルの構成に切り替えます。



特定のサイトの構成を比較するために、サイトを選択できます。テンプレートレベルの設定とは異なり、各サイトの Nexus Dashboard Orchestrator 定義または実際の既存の設定を個別に選択して、そのサイトのテンプレートのサイトローカル プロパティとして保持できます。

ほとんどのシナリオでは、テンプレートレベルとサイトレベルの両方の構成で同じ選択を行いたとしても、ばらつきの調整ウィザードでは、サイトのコントローラで「テンプレートのプロパティ」レベルで定義された構成と Nexus Dashboard Orchestratorで定義された構成またはその逆を選択できます。

ステップ 5 **[変更のプレビュー（Preview Changes）]** をクリックして、選択内容を確認します。

プレビューは **[ばらつきの調整 (Reconcile Drift)]** ウィザードの選択肢に基づいて調整された完全なテンプレート構成を表示します。その後、**[サイトに展開（Deploy to site）]** をクリックして構成を展開し、そのテンプレートのばらつきを調整できます。

スキーマの複製

このセクションでは、**[スキーマ (Schemas)]** 画面の [スキーマの複製 (Clone Schema)] 機能を使用して、既存のスキーマとそのすべてのテンプレートのコピーを作成する方法について説明します。

（注） テンプレートを複製し、異なる設定で同じサイトに展開しようとすると、名前の重複エラーが原因で展開が失敗する可能性があります。複製されたテンプレートのオブジェクト名を変更すると、表示名のみが更新されます。データベース レコードは変更されないため、このシナリオでは展開が失敗します。

手順

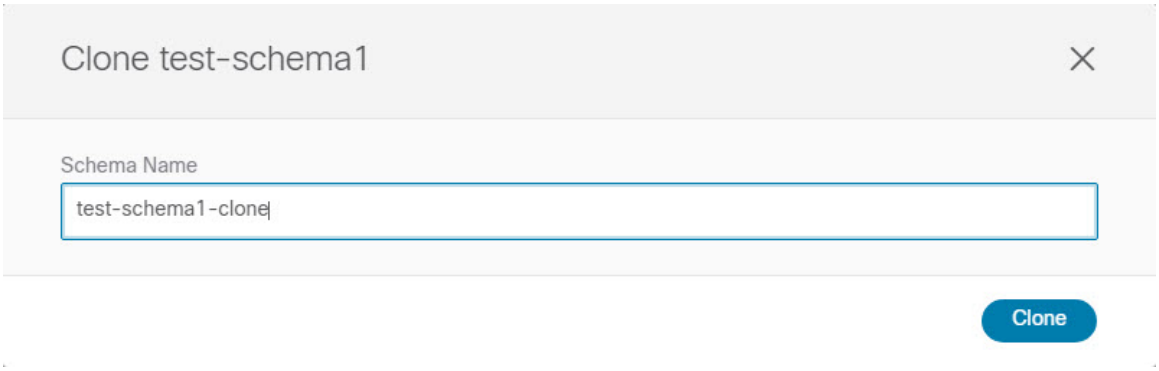
ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 複製するスキーマを選択します。

a) 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

b) 複製するスキーマ名の横にある **[アクション（Actions）]** メニューから、**[複製（Clone）]** を選択します。

ステップ 3 新しいスキーマの名前を入力し、**[複製 (Clone)]** をクリックします。



[複製 (Clone)] をクリックすると、UI に `[<スキーマ名の複製に成功しました (Cloning of <schema-name> was successful)]` というメッセージが表示され、新しいスキーマが **[スキーマ (Schemas)]** 画面に表示されます。

新しいスキーマは、元のスキーマとまったく同じテンプレート（およびそのテナントの関連付け）、オブジェクト、およびポリシー設定で作成されます。

テンプレート、オブジェクト、および設定はコピーされますが、サイトの関連付けは保持されないため、それらを展開するサイトに複製されたスキーマのテンプレートを再度関連付ける必要があります。同様に、テンプレートオブジェクトをサイトに関連付けた後に、テンプレートオブジェクトのサイト固有の設定を指定する必要があります。

ステップ 4 （オプション）スキーマとそのすべてのテンプレートがコピーされたことを確認します。

2 つのスキーマを比較することで、操作が正常に完了したことを確認できます。

テンプレートの複製

ここでは、スキーマ ビューで [テンプレートの複製 (Clone Template)]機能を使用して既存のテンプレートのコピーを作成する方法について説明します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 3 複製するテンプレートを含むスキーマをクリックします。

ステップ 4 [表示（View）] メニューで、テンプレートを選択して開きます。

ステップ 5 **[アクション (Actions)]** メニューから **[テンプレートのクローン (Clone Template)]** を選択します。

ステップ 6 クローンの複製先の詳細を入力します。

a) **[複製先スキーマ (Destination Schema)]** ドロップダウンから、テンプレートのクローンを作成するスキーマの名前を選択します。

このテンプレートのクローンを含めるために、同じスキーマまたは異なるスキーマを選択できます。まだ存在しないスキーマにテンプレートを複製する場合は、スキーマの名前を入力し、`[作成 (Create) <schema-name>]` オプションを選択して新しいスキーマを作成できます。

（注）
異なるスキーマ間で複製する場合、テンプレートには他のテンプレートのオブジェクトを参照するオブジェクトを含めることはできません。

b) [テンプレート名（Template Name）] フィールドに、テンプレートの名前を入力します。

c) **[保存 (Save)]** をクリックして、クローンを作成します。

新しいテンプレートが、選択したテナントと元のテンプレートとまったく同じオブジェクトおよびポリシー設定で複製先スキーマに作成されます。

選択した複製先スキーマがソーステンプレートと同じスキーマである場合、スキーマ ビューがリロードされ、新しいテンプレートが左側のサイドバーに表示されます。別のスキーマを選択した場合は、そのスキーマに移動して新しいテンプレートを表示および編集できます。

テンプレート オブジェクトと設定はコピーされますが、サイトの関連付けは保持されないため、複製したテンプレートを展開するサイトに再度関連付ける必要があります。同様に、テンプレート オブジェクトをサイトに関連付けた後に、テンプレート オブジェクトのサイト固有の設定を指定する必要があります。

テンプレート間でのオブジェクトの移行

ここでは、テンプレートまたはスキーマ間でオブジェクトを移動する方法について説明します。1 つ以上のオブジェクトを移動すると、次の制約事項が適用されます。

- テンプレート間で移動できるのは、EPG および Bridge Domain (BD) オブジェクトのみです。
- クラウド ネットワーク コントローラ サイトとの間でのオブジェクトの移行はサポートされていません。

  オンプレミスサイト間でのみオブジェクトを移行できます。
- 送信元と宛先のテンプレートは同じスキーマにも異なるスキーマにもすることができますが、テンプレートは同じテナントに割り当てる必要があります。
- 宛先テンプレートが作成され、少なくとも 1 つのサイトに割り当てられている必要があります。
- 宛先テンプレートが展開されておらず、他のオブジェクトがない場合、そのテンプレートは、オブジェクトの移行後に自動的に展開されます。
- 1 つのオブジェクト移行を開始すると、同じ送信元またはターゲット テンプレートを含む別の移行を実行することはできません。テンプレートがサイトに展開されると、移行が完了します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから **[スキーマ(Schemas)]** を選択します。

ステップ 3 移行するオブジェクトが含まれているスキーマをクリックします。

ステップ 4 [スキーマ (Schema)] ビューで、移行するオブジェクトが含まれているテンプレートを選択します。

ステップ 5 メインペインの右上にある **[選択 (Select)]** をクリックします。

これにより、移行する 1 つ以上のオブジェクトを選択できます。

ステップ 6 移行する各オブジェクトをクリックします。

選択したオブジェクトには、右上隅にチェックマークが表示されます。

ステップ 7 メインペインの右上にある [アクション (actions)] (**...**) アイコンをクリックし、[**オブジェクトの移行 (Migrate Objects)**] を選択します。

ステップ 8 [**オブジェクトの移行 (Migrate objects**)] ウィンドウで、オブジェクトを移動する宛先スキーマとテンプレートを選択します。

リストには、少なくとも 1 つのサイトが接続されているテンプレートのみが表示されます。ドロップダウンリストにターゲットテンプレートが表示されない場合は、ウィザードをキャンセルし、そのテンプレートを少なくとも 1 つのサイトに割り当てます。

ステップ 9 [**OK**] をクリックし、[**はい (YES)**] をクリックしてオブジェクトを移動することを確認します。

オブジェクトは、ソーステンプレートから選択した宛先テンプレートに移行されます。設定を展開すると、ソーステンプレートが展開され、宛先テンプレートが展開されているサイトに追加されるサイトから、オブジェクトが削除されます。

ステップ 10 移行が完了したら、ソースと宛先の両方のテンプレートを再展開します。

宛先テンプレートが展開されておらず、他のオブジェクトがない場合、そのテンプレートはオブジェクトの移行後に自動的に展開されるため、この手順をスキップできます。

現在展開されている設定の表示

特定のテンプレートからサイトに現在展開されているすべてのオブジェクトを表示できます。任意のテンプレートを何度でも展開、展開解除、更新、および再展開できますが、この機能では、これらすべてのアクションの結果としての最終的な状態のみが表示されます。たとえば、`Template1` に `VRF1` オブジェクトのみが含まれ、`Site1` に展開されている場合、API はそのテンプレートの `VRF1` 蚤を返します。その後、`BD1` を追加して再展開すると、その時点から、API は `BD1` と `VRF1` の両方のオブジェクトを返すようになります。

この情報は Orchestrator データベースから取得されるため、サイトのコントローラで直接行われた変更によって発生する可能性のある設定の変動は考慮されません。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーションメニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 3 表示するテンプレートを含むスキーマをクリックします。

ステップ 4 左側のサイドバーで、テンプレートを選択します。

ステップ 5 そのテンプレートの **[展開ビュー (Deployed View)]** を開きます。

a) テンプレートの名前の横にある **[アクション (Actions)]** メニューをクリックします。
b) **[展開ビュー (Deployed View)]** をクリックします。

ステップ 6 **[展開ビュー (Deployed View)]** 画面で、情報を表示するサイトを選択します。

サイトにすでに展開されているものと、テンプレートで定義されているものとのテンプレート設定の比較がグラフィカルに表示されます。

a) 色分けされた凡例は、この時点でテンプレートを展開する場合に作成、削除、または変更されるオブジェクトを示します。

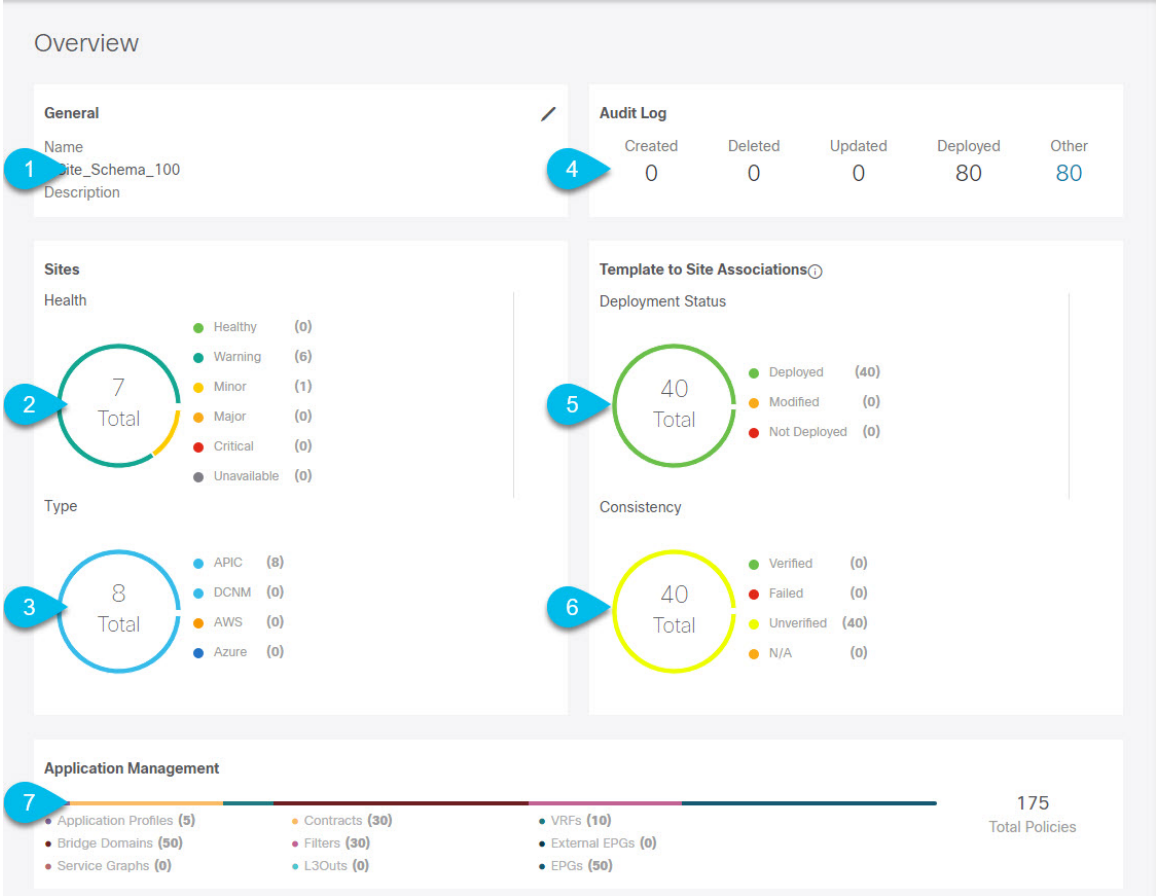
テンプレートの最新バージョンがすでに展開されている場合、ビューには色分けされたオブジェクトは含まれず、現在展開されている設定が表示されます。

b) サイト名をクリックすると、その特定のサイトの設定を表示できます。
c) **[XML/JSON 表示 (View XML/JSON)]** をクリックすると、選択したサイトに展開されているすべてのオブジェクトの XML 設定が表示されます。

スキーマの概要と展開ビジュアライザ

1つ以上のオブジェクトが定義され、1つ以上のACIファブリックに展開されたスキーマを開くと、スキーマの **[概要 (Overview)]** ページに展開の概要が表示されます。

図 *5 :* スキーマの概要



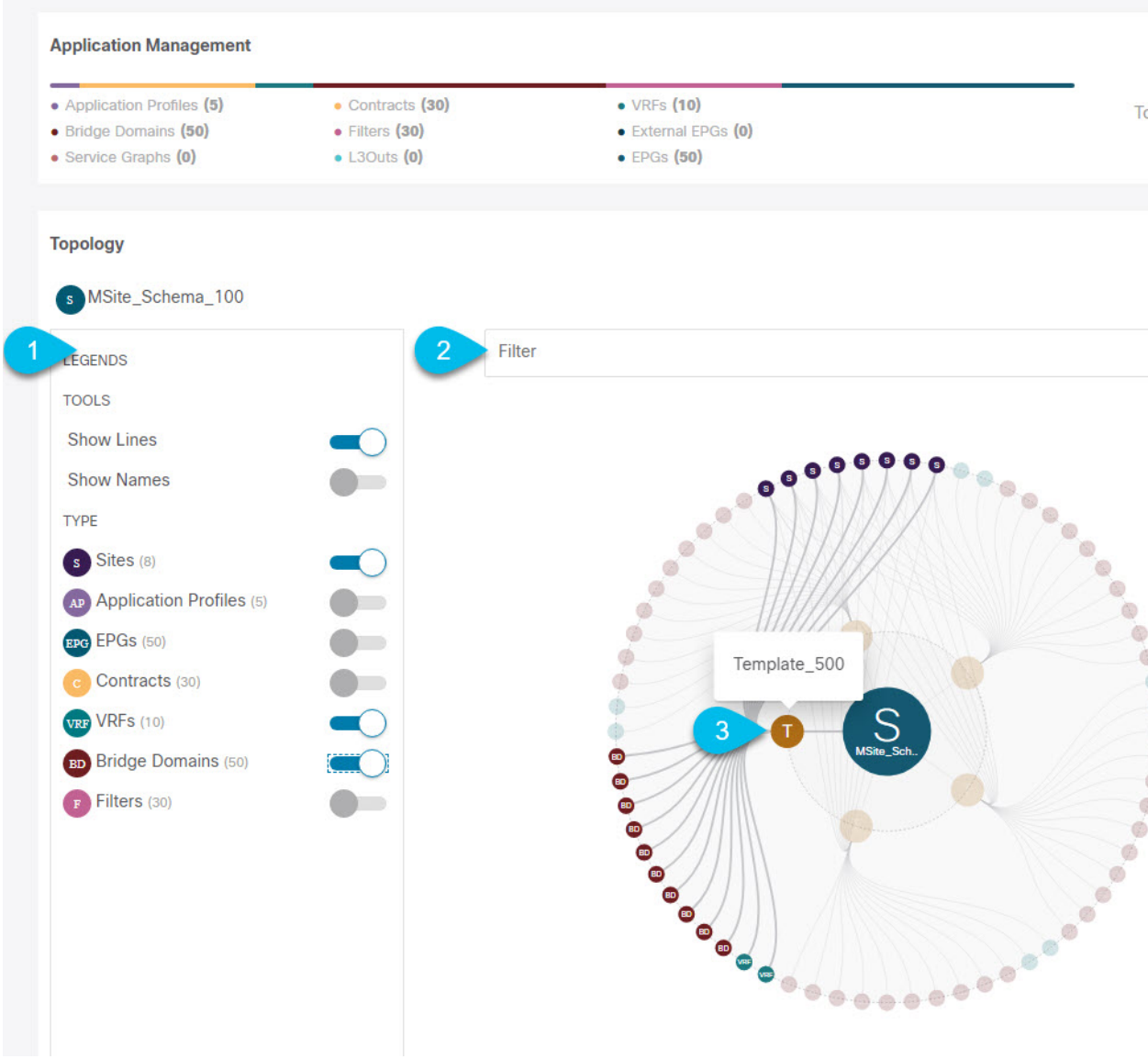
このページには、次の詳細が表示されます。

1. **[一般 (General)]**：名前や説明など、スキーマの一般情報を提供します。
2. **[監査ログ (Audit Log)]**：スキーマで実行されたアクションの監査ログの概要を提供します。
3. **[サイト (Sites)]** > **[正常性 (Health)]**：サイトの正常性ステータスでソートされた、このスキーマのテンプレートに関連付けられているサイトの数を提供します。
4. **[サイト (Sites)]** > **[タイプ (Type)]**：サイトのタイプでソートされた、このスキーマのテンプレートに関連付けられているサイトの数を提供します。
5. **[テンプレートとサイトの関連付け (Template to Site Associations)]** > **[展開ステータス (Deployment Status)]**：1 つ以上のサイトに関連付けられているこのスキーマ内のテンプレートの数とその展開ステータスを提供します。
6. [テンプレートとサイトの関連付けの整合性（Template to Site Associations Consistency）]：展開されたテンプレートで実行された整合性チェックの数とそのステータスを提供します。 >

7. **[アプリケーション管理 (Application Management)]**：このスキーマのテンプレートに含まれる個々のオブジェクトの概要を提供します。

[トポロジ (Topology)] タイルでは、次の図に示すように、1 つ以上のオブジェクトを選択してダイアグラムに表示することで、トポロジ ビジュアライザを作成できます。

図 *6*：展開ビジュアライザ

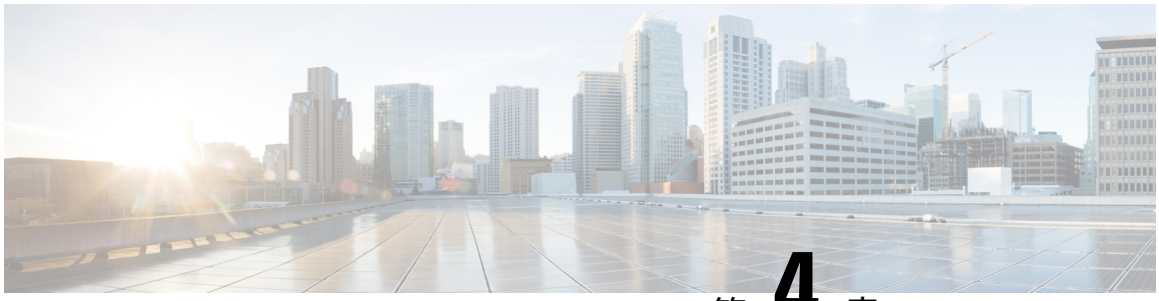


1. **凡例 (Legent)**：次のトポロジ図に表示するポリシーオブジェクトを選択できます。
2. **[フィルタ (Filter)]**：表示されるオブジェクトを名前に基づいてフィルタリングできます。
3. **[トポロジ図 (Topology Diagram)]**：サイトに割り当てられているすべてのスキーマ テンプレートで設定されたポリシーを視覚的に表示します。

上記の **[設定オプション (Configuration Options)]** を使用して、表示するオブジェクトを選択できます。

また、オブジェクトの上にマウスを置くと、すべての依存関係を強調表示できます。

最後に、図内の任意のオブジェクトをクリックすると、他のオブジェクトとの関係だけが表示されます。たとえば、テンプレートをクリックすると、その特定のテンプレート内のすべてのオブジェクトのみが表示されます。



第 4 章

ファブリック管理

ファブリック ポリシーを作成

このセクションでは、1つ以上のファブリック ポリシー テンプレートを作成する方法について説明します。ファブリック ポリシー テンプレートを使用すると、次のファブリック ポリシーを作成および構成できます。

- VLAN Pool
- 物理ドメイン
- SyncE インターフェイス ポリシー
- インターフェイス設定
- ノード 設定
- ポッド設定
- MACsec
- NTP ポリシー
- PTP ポリシー
- QoS DSCP ポリシー
- QoS SR-MPLS ポリシー
- QoS クラス ポリシー

ファブリック ポリシー テンプレート ポリシーを作成するときは、次の点を考慮してください。

- ファブリック ポリシー テンプレートをテナントに関連付ける必要はありませんが、展開するには、少なくとも 1 つのサイトにマップする必要があります。

- これらのポリシーの構成は、特定のサイト レベルではなく、テンプレート レベルでのみ可能です。
- ファブリック ポリシー テンプレートを展開解除すると、APIC で関連付けられたポリシーが保持されます。つまり、APIC でのこれらのポリシーの構成は、デフォルト値、またはオーケストレータがそれらの管理を開始する前に APIC で構成された値に戻されません。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 新しいファブリック ポリシー テンプレートを作成。

a) 左側のナビゲーション メニューで、**[ファブリック管理（Fabric Management）]** > **[ファブリック ポリシー（Fabric Policies）]** を選択します。

b) **[ファブリック ポリシー テンプレート（Fabric Policy Template）]**ページ内で**[ファブリック ポリシー テンプレートを追加（Add Fabric Policy Template）]**をクリックします。

c) **[ファブリック ポリシー（Fabric Policies）]** ページの右のプロパティ サイトバーにテンプレートの **[名前（Name）]** を入力します。

デフォルトでは、新しいテンプレートは空であるため、次のステップに従って 1 つ以上のファブリック ポリシーを追加する必要があります。テンプレートで使用可能なすべてのポリシーを作成する必要はありません。このテンプレートとともに展開する各タイプのポリシーを 1 つ以上定義できます。特定のポリシーを作成したくない場合は、説明されている手順をスキップしてください。

ステップ 3 テンプレートを 1 つ以上のサイトに割り当てます。

サイトにテナント ポリシー テンプレートを割り当てるプロセスは、サイトにアプリケーション テンプレートを割り当てる方法と同じです。

a) **[テンプレート プロパティ（Template Properties）]** 表示内で **[アクション（Actions）]** をクリックして **[サイトの関連付け（Sites Association）]** を選択します。

[<template-name> にサイトの関連付け（Associate Sites to <template-name>）] ウィンドウが開きます。

b) **[サイトの関連付け（Associate Sites）]** ウィンドウで、テンプレートを展開するサイトの横のチェックボックスをオンにします。

テナント ポリシー テンプレートは、オンプレミス ACI サイトにのみサポートされることにご注意ください。そして、割り当て可能です。

c) **Ok** をクリックして保存します。

ステップ 4 VLAN プールを作成。

VLAN プールは、VLAN ID または、物理または VMM ドメインが消費する VLAN カプセル化に使用されている範囲を指定します。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[VLAN セッション プール（VLAN Pool）]** を選択します。

b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) **[+VLAN 範囲の追加（+Add VLAN Range）]** をクリックして範囲を指定し、チェックマーク アイコンをクリックして保存します。
e) 前のサブステップを繰り返して、同じポリシー内に追加の VLAN 範囲を作成します。
f) この手順を繰り返して、追加の VLAN プールを作成します。

ステップ 5 物理 ドメインを作成。

物理ドメインプロファイルは、ベア メタル サーバ接続と管理アクセスに使用します。ドメインはVLAN プールに関連付けられるように設定されます。その後、EPG は、ドメインに関連付けられている VLAN を使用するように設定されます

a) **[+オブジェクトを作成（+Create Object）]** ドロップダウンから、**[物理ドメイン（Physical Domain）]** を選択します。
b) 右のプロパティのサイドバーでは、ドメイン の**[名前（Name）]**を指定します。
c) （オプション）**[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) **[VLAN プール ポリシーを選択（Select a VLAN Pool Policy）]** をクリックし、このドメインの VLAN プールの 1 つを選択します。

ステップ 3 の説明に従って、VLAN プールがすでに作成されている必要があります。

e) この手順を繰り返して、追加の物理ドメインを作成します。

ステップ 6 SyncE インターフェイス ポリシーを作成します。

サービスプロバイダー ネットワークで、Synchronous Optical Networking（SONET）と同期デジタル階層（SDH）機器を段階的に置き換えるイーサネット機器を使用する場合、イーサネット ポート経由で高品質なクロック同期を提供するためには周波数を同期化することが必要です。周波数またはタイミング同期は、ネットワーク全体に精密周波数を配布する機能です。同期イーサネット（SyncE）により、物理レベルで必要な同期化が実現します。SyncE を使用するイーサネット リンクは、SONET/SDH と同じ方法で、つまり高品質なストラタム 1 追跡可能クロック信号とビット クロックのタイミングを取ることで同期されます。

ACI ファブリックの SyncE の詳細については、ご使用のリリースの *Cisco APIC* システム管理構成ガイドの「同期イーサネット（SyncE）」の章を参照してください。

a) **[+オブジェクトを作成（+Create Object）]** ドロップダウンから、**[SyncE インターフェイス ポリシー（SyncE Interface Policy）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) ポリシーの詳細を入力します。

- **管理状態** –ポリシーの有効または、無効化。

  デフォルトは無効です。

- **Sync 状態 Msg** – チェックを外さない場合、ESMC パケットの送信が無効化され、受信した ESMC パケットもすべて無視されます。

- **選択入力** – インターフェイスの周波数送信元の優先順位の構成を有効にします。
- **Src 優先順位** – Tインターフェイスの周波数送信元の優先順位。この値は、クロック選択アルゴリズムで同じ QL がある 2 つの送信元間から選択するために使用されます。

  値は、1（最高プライオリティ）から254（最低プライオリティ）の範囲で設定できます。デフォルト値は 100 です。

  選択入力 が有効な場合にのみ構成できます。
- **復旧するのに待つ** – T分単位の復元までの待機時間は、インターフェイスが起動し、周波数同期に使用されるまでの時間です。有効値の範囲は、0 ～ 12 です。デフォルト値は 5 です。

  選択入力 が有効な場合にのみ構成できます。

e) この手順を繰り返して、追加の SyncE インターフェイス ポリシーを作成します。

ステップ 7 インターフェイス設定ポリシーを作成します。.

このインターフェイスに SyncE または MACsec を構成する場合は、対応する手順の説明に従って、これらのポリシーをすでに作成しておく必要があります。

インターフェイス設定ポリシーを使用すると、1つ以上のスイッチの1つ以上のポートに後で展開できる共通インターフェイス設定のセットを定義して、それら全体で一貫した構成を行うことができます。

a) **[+オブジェクトを作成（+Create Object）]** ドロップダウンから、**[インターフェイスの設定（Interface Settings）]** を選択します。
b) 設定しているインターフェイスの**タイプ**を選択します。
c) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
d) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
e) ポリシーの詳細を入力します。

- **速度** – ポートのデータ転送レート。これは、ポートがリンクされている接続先と一致する必要があります。速度は特定のポートのみで変更できます。すべての速度がすべてのシステムで使用できるわけではありません。詳細については、使用しているスイッチのハードウェア設置ガイドを参照してください。
- **自動ネゴシエーション** – ポートに対するネゴシエーションを有効にします。
- **[VLAN 範囲 (VLAN Scope)]** ー レイヤ 2 インターフェイスのVLAN 範囲。

  [グローバル範囲 (Global scope)] – リーフごとに 1 つの EPG のみにマッピングするように VLAN カプセル化値を設定します。

  [ポート ローカル 範囲 (Port Local scope)] –入力方向と出力方向の両方で個別の（ポート、VLAN）変換エントリを割り当てることができます。EPGが単一のブリッジドメインに属している場合、この設定は無効です。
- **[CDP 管理状態 (CDP Admin State)]** – インターフェイスで Cisco Discovery Protocol（CDP）を有効にします。
- **LLDP** – インターフェイスのリンク層検出プロトコル（LLDP）をイネーブルにします。

- **[MCP 管理状態 (MCP Admin State)]** ー インターフェイスで MisCabling Protocol（MCP）を有効にします。
- **ドメイン** – このインターフェイス ポリシーを関連付ける 1 つ以上のドメインを選択します。

  ドメインの指定は必須ではありません。インターフェイス ポリシーを作成して、関連付けられたドメインがなくてもサイトに展開できます。
- **詳細設定** – このセクションの横にある矢印をクリックして展開します。
  - **SyncE** – SyncE ポリシーを定義し、それをこのインターフェイス設定ポリシーに割り当てる場合は、ドロップダウンから選択します。
  - **デバウンス間隔** – ポート デバウンス時間は、リンクがダウンしたことをスーパーバイザに通知するためにインターフェイスが待機する時間です。この時間、インターフェイスはリンクがアップ状態に戻ったかどうかを確認するために待機します。
  - **遅延の設定** – ポートがアップ状態になったときに、判定フィードバック イコライザ（DFE）の調整を遅延させる時間を、ミリ秒単位で指定します。遅延は、一部のサードパーティ製アダプタを使用する場合に、リンクの起動中に CRC エラーを回避するために使用されます。

    遅延は必要な場合にのみ設定してください。ほとんどの場合、遅延を設定する必要はありません。
  - **FEC** – 転送エラー訂正（FEC）は、送信元（送信側）がエラー修正コードを使用して冗長な方法でデータをエンコードし、宛先（受信側）がそれを認識する、信頼できないチャネルまたはノイズの多いチャネルを介したデータ送信でエラー制御を取得する方法です。再送信を必要とせずにエラーを修正します。
  - **QinQ** – 通常のインターフェイス、PC、または vPC で入力される二重タグ付き VLAN トラフィックを EPG にマッピングできます。この機能が有効で、二重タグ付きトラフィックが EPG のネットワークに入ると、両方のタグがファブリック内で個別に処理され、ACI スイッチの出力時に二重タグに復元されます。単一タグおよびタグなしのトラフィックの入力はドロップします。
  - **リフレクティブ リレー]** – すべてのトラフィックを外部スイッチに転送します。外部スイッチはポリシーを適用し、必要に応じてサーバー上の宛先またはターゲットVMにトラフィックを送信します。ローカルスイッチングはありません。ブロードキャストまたはマルチキャスト トラフィックは、リフレクティブ リレーは、各 VM サーバでローカルにパケットのレプリケーションを提供します。

    リフレクティブ リレーの利点の 1 つは、スイッチング機能および管理機能、Vm をサポートするサーバ リソースを解放するための外部スイッチを活用しています。リフレクティブ リレーでは、ポリシー、同じサーバ上の Vm の間のトラフィックに適用する Cisco APIC で設定することもできます。

    Cisco ACI、入ってきたの同じポートからオンに戻すにトラフィックを許可する、リフレクティブ リレーを有効にできます。レイヤ 2 インターフェイス ポリシーとして individual ports（個々のポート、個別ポート）、ポート チャネルまたは仮想ポート チャネルでリフレクティブ リレーを有効にすることができます。

デフォルト値は [無効（Disabled）] です。

- **LLDP 送信状態** – インターフェイスから Link Layer Discovery Protocol（LLDP）パケットを送信できるようにします。

  LLDP 受信/送信状態フラグは、LLDP がインターフェイス ポリシーでグローバルに有効になっている場合にのみ構成できます。

- **LLDP 受信状態** – インターフェイスで LLDP パケットを受信できるようにします。
- **BPDU フィルタ** – ブリッジプロトコルデータユニット（BPDU）フィルタは、ポート上のすべての BPDU をフィルタリングします。

  BPDU フィルタは、インバウンド BPDU とアウトバウンド BPDU の両方を防止します。受信した BPDU はドロップされ、BPDU は送信されません。

- **BPDU ガード** – BPDU ガードは、ポートが BPDU を受信するのを防ぎます。ポートで BPDU を受信すると、ポートは `errdisable` モードになります。
- **LLFC 送信状態** – リンク レベル フロー制御（LLFC）パケットをインターフェイスから送信できるようにします。
- **LLFC 受信状態** – インターフェイスが LLFC パケットを受信できるようにします。
- **アクセス MACsec ポリシー** – アクセス MACsec ポリシーを定義し、それをこのインターフェイス設定ポリシーに割り当てる場合は、ドロップダウンから選択します。

f) このステップを繰り返して、追加の インターフェイス設定ポリシーを作成します。

ステップ 8 ノード設定ポリシーを作成します。

ノード設定ポリシーを使用すると、共通のノード設定のセットを定義できます。これを後で 1 つまたは複数のスイッチに展開して、それら全体で一貫した構成を実現できます。

このリリースでは、ノード設定ポリシーは、SyncE および PTP 機能の有効化をサポートしています。

a) **[+オブジェクトを作成（+Create Object）]** ドロップダウンから、**[ノードの設定（Node Settings）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) **SyncE** 構成をノードに展開する場合は、SyncE を有効にして設定を指定します。

SyncE の詳細については、ご使用のリリースの *Cisco APIC* システム管理構成ガイド の「同期イーサネット（SyncE）」の章を参照してください。

- **管理状態** –ポリシーの有効または、無効化。
- **品質レベル オプション** – クロックの正確度を指定します。この情報は、ESMC に運ばれている SSM を使用してネットワークに渡って送信されシステム内のデバイスが同期できる最適な利用可能な送信元を決定するために使用されます。

e) **PTP** 構成をノードに展開する場合は、PTP を有効にして設定を指定します。

PTP の詳細については、ご使用にリリースの「*Cisco APIC システム管理構成ガイド*の「正確な時間プロトコル」章 」を参照します。

f) このステップを繰り返して、追加の ノード設定ポリシーを作成します。

ステップ 9 ポッド設定ポリシーを作成します。

ポッド設定ポリシーを作成する前に、対応する手順で説明されているように、そのポリシー用に NTP ポリシーを作成しておく必要があります。

ポッド全体の MACsec ポリシーを構成する場合は、対応する手順の説明に従って、MACsec ポリシーを作成しておく必要があります。

Pod 設定ポリシーを使用すると、共通のポッド設定のセットを定義できます。これを後でファブリック内の 1 つ以上のポッドに展開して、それら全体で一貫した構成を実現できます。

a) **[+オブジェクトを作成（+Create Object）]** ドロップダウンから、**[ポッドの設定（Pod Settings）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) **[NTP ポリシーの選択（Select a NTP Policy）]** をクリックして、NTP ポリシーを選択します。
e) **[ファブリック MACsec ポリシー（Fabric MACsec Policy）]** ドロップダウンから、MACsec ポリシーを選択します。
f) このステップを繰り返して、追加のポッド設定ポリシーを作成します。

ステップ 10 MACsec ポリシーを作成します。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。

ACI ファブリックの MACsec の詳細については、ご使用のリリースの 「*Cisco APIC システム管理構成ガイド*」 の「MACsec」の章を参照してください。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**MACsec** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) ポリシーの詳細を入力します。

- **タイプ** – このポリシーが適用されるインターフェースのタイプを定義します。

  スパイン スイッチ上のすべてのリンクは、ファブリック リンクと見なされます。ただし、スパイン スイッチ リンクを IPN 接続のために使用している場合、そのリンクはアクセス リンクとして扱われます。これらのリンクで MACsec を展開するには、MACsec アクセス ポリシーを使用する必要があります。

- **管理状態** –ポリシーの有効または、無効化。

- **暗号スイート** – 暗号スイート AES 128 または 拡張パケット ナンバリング（XPN）のない AES 256 を選択する場合は、セキュリティ関連キー（SAK）の有効期限を明示的に指定する必要があります。SAK の有効期限値をデフォルト（「無効」）のままにすると、インターフェイスがランダムにアウトオブサービスになる可能性があります。

- **ウィンドウ サイズ** –フレームの順序が変更されるプロバイダーネットワーク上で MACsec の使用をサポートするには、リプレイウィンドウが必要です。ウィンドウ内のフレームは順不同で受信できますが、リプレイ保護されません。デフォルトのウィンドウ サイズは 64 です。Cisco APIC GUI または CLI を使用する場合、リプレイ ウィンドウのサイズは、0 ー 2^{32-1} の範囲で設定できます。XPN 暗号スイートの場合、最大リプレイ ウィンドウ サイズは 2^{30-1} です。これより大きなウィンドウ サイズを設定しても、ウィンドウ サイズは 2^{30-1} に制限されます。暗号スイートを非 XPN 暗号スイートに変更した場合、制限はなく、設定されたウィンドウ サイズが使用されます

- **セキュリティ ポリシー** – APIC MACsec では、2 つのセキュリティ モードをサポートしています。MACsec セキュリティで保護する必要がある 中に、リンクの暗号化されたトラフィックのみを許可する セキュリティで保護する必要がある により、両方のクリアし、リンク上のトラフィックを暗号化します。たとえば、ポートをオンにできますで MACsec セキュリティで保護する必要がある モードがピアがしているリンクでのキーチェーンを受信する前にします。この問題に対処するには、MACsec を `Should-Secure` モードで展開し、すべてのリンクがアップしたらセキュリティ モードを `Must-Secure` に変更することをお勧めします。

  （注）
  セキュリティで保護する必要があるモードで MACsec を展開する前にキーチェーンは、影響を受けるインターフェイスに導入する必要があります、またはインターフェイスがダウンします。

- **SAK 失効時間** – 暗号スイート AES 128 または拡張パケット ナンバリング（XPN）のない AES 256 を選択する場合は、セキュリティ関連キー（SAK）の有効期限を明示的に指定する必要があります。SAK の有効期限値をデフォルトのままにすると、インターフェイスがランダムにアウトオブサービスになる可能性があります。

- **キー名** – MACsec キーを作成できます。APIC はまたは責任を負う MACsec キーチェーン ディストリビューションのポッド内のすべてのノードに特定のポートのノードになります。
  - **[+MACsec キーの追加（+Add MACsec Key）]** をクリックします。
  - **キー名**を入力します。
  - **PSK** フィールドに事前共有キーを指定します。
  - **開始時間** フィールドで、キーが有効になる日付を入力します。
  - **終了時間** フィールドで、キーの有効期限が切れる日付を入力します。
  - **Ok** をクリックしてキーを保存します。
  - 提供する追加のキーについて、この手順を繰り返します。

e) 追加のMACsec ポリシーを作成するために、このステップを繰り返します。

ステップ 11 NTP 設定ポリシーを作成します。

ACI ファブリックにおいて、時刻の同期は、モニタリング、運用、トラブルシューティングなどの多数のタスクが依存している重要な機能です。クロック同期は、トラフィック フローの適切な分析にとって重要であり、複数のファブリック ノード間でデバッグとフォールトのタイム スタンプを関連付けるためにも重要です。

ACI ファブリックの NTP の詳細については、ご使用のリリースの「Cisco APIC 基本構成ガイド」の「プロビジョニング *ACI* ファブリック サービス」の章を参照してください。

a) **[+オブジェクトを作成（+Create Object）]** ドロップダウンから、**[NTP の設定（NTP Settings）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) ポリシーの詳細を入力します。

- **[+ キーの追加（+Add Key）]** をクリックして、NTP クライアント認証キーを提供します。
- **詳細設定** – このセクションの横にある矢印をクリックして展開します。
  - **管理状態** – NTP ポリシーの有効または、無効化。
  - **サーバー状態** によって、ACI リーフ スイッチを NTP サーバーとして動作し、下流のクライアントに NTP 情報を提供できるようにします。

    有効にすると、ダウンストリーム クライアントは、接続先のリーフ スイッチのインバンド/アウトオブバンド管理 IP アドレスを NTP サーバーとして使用できます。
  - **マスター モード** – これを使用すれば、指定された NTP サーバーが、下流のクライアントに対し、構成されたストラタム番号とともに、調整されていないローカル クロック時刻を提供することが可能になります。たとえば、NTP サーバとして動作しているリーフ スイッチは、クライアントとして動作しているリーフスイッチに対し、調整されていないローカル クロック時刻を提供できます。これが適用できるのは、サーバーのクロックが調整されていない場合のみです。
  - **ストラタム** – NTP クライアントが同期した時刻を取得するときのストラタム番号を指定します。

    サーバー状態 オプションが有効になっていて、ACI リーフ スイッチに接続されているクライアントが、スイッチの管理 IP アドレスを NTP サーバとして使用するように設定されている場合、クライアントは stratum+1 で NTP 情報を受信します。

    範囲は 1 ～ 14 です。
  - **認証状態** – 証明書ベースの認証を有効にします。

    このオプションを有効にする場合は、上記の **[+ キーを追加（+Add Key）]** オプションを使用してキーを指定する必要があります。
- NTP サーバー情報を指定するために **[+ プロバイダーを追加（+Add Provider）]** をクリックします。

  表示される [プロバイダーの追加] ウィンドウで、サーバーのホスト名/IP アドレス、管理 EPG の名前、および管理 EPG タイプを指定する必要があります。

  （注）
  選択した特定のタイプの管理 EPG は、このテンプレートが関連付けられているサイトの APIC ですでに構成されている必要があります。

複数のプロバイダーを作成する場合は、最も信頼できる NTP 時刻源の **[優先]** オプションをオンにします。

e) このステップを繰り返して、追加の NTP設定ポリシーを作成します。

ステップ 12 PTP設定ポリシーを作成します。

高精度時間プロトコル（PTP）はネットワークに分散したノードの時刻同期プロトコルです。PTP を使用すると、イーサネット ネットワークを介して 1 マイクロ秒未満の精度で、分散したクロックを同期できます。PTP の正確さは、ACI ファブリック スパインおよびリーフスイッチでの PTP のハードウェア サポートによるものです。

ACI ファブリックの PTP の詳細については、ご使用にリリースの「*Cisco APIC システム管理構成ガイド*の「正確な時間プロトコル」章 」を参照します。

a) **[+オブジェクトを作成（+Create Object）]** ドロップダウンから、**[PTP の設定（PTP Settings）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) ポリシーの詳細を入力します。

- **管理状態** –ポリシーの有効または、無効化。
- **グローバル優先度 1** – このクロックをアドバタイズするときに使用される値を指定します。優先順位 1 はベスト マスター クロック 選択のためにデフォルトの条件（例えば、クロック品質とクロック クラス）をオーバーライドします。

  有効な値は 0 ～ 255 です。デフォルト値は 128 です。低い値が優先されます。
- **グローバル優先度 2** – このクロックをアドバタイズするときに使用される値を指定します。優先度 2 は、デフォルト条件で同等になる 2 台のデバイスのうち、どちらを優先するかを決めるために使用されます。

  有効な値は 0 ～ 255 です。デフォルト値は 128 です。低い値が優先されます。
- **グローバル ドメイン** – PTP ドメイン番号を指定します。Cisco ACI では複数の PTP ドメインはサポートされていませんが、使用中のドメイン番号を変更することはできます。すべてのリーフスイッチとスパイン スイッチで同じ値が使用されます。

  0 ～ 128 の範囲の値を指定できます。デフォルトは 0 です。
- **ファブリック プロファイル テンプレート** – 以下の間隔設定のデフォルト値を定義する PTP プロファイルを指定します。プロファイルは、PTP のさまざまなユースケースに最適化されたさまざまなパラメータを定義するために使用されます。これらのパラメータの一部には、PTP メッセージ間隔の適切な範囲と PTP トランスポートプロトコルが含まれますが、これらに限定されません。PTP プロファイルは、さまざまな業界の多くの組織/標準規格によって定義されています。
  - **AES67-2015**：AES67-2015。これは、オーディオ オーバー イーサネットおよびオーディオ オーバー IP の相互運用性の標準です。
  - **デフォルト**：IEEE 1588-2008。これは、クロック同期のデフォルトの PTP プロファイルです。

- **SMPTE-2059-2**：SMTPE ST2059-2015、これはビデオ オーバー IP の標準です。
- **Telecom-8275-1**：ITU-T G.8275.1。これは、完全なタイミング サポートを備えた電気通信の標準的な推奨事項です。

  フル タイミング サポートは、すべてのホップで PTP G.8275.1 プロファイルをデバイスに提供できる電気通信ネットワークを表すために ITU によって定義された用語です。ACI でサポートされていない G.8275.2 は、パスに PTP をサポートしないデバイスが含まれる可能性がある部分的なタイミング サポート用です。

- **ファブリック アナウンス間隔** – マスター ポートがアナウンス メッセージを送信するための平均間隔の対数を秒単位で指定します。底は 2 です。範囲は、選択したプロファイルによって異なります。
- **ファブリック同期間隔** – マスター ポートが同期メッセージを送信するための平均間隔の対数を秒単位で指定します。底は 2 です。範囲とデフォルトは、選択した PTP プロファイルによって異なります。
- **ファブリック遅延間隔** – スレーブ ポートが遅延要求メッセージを送信するための、基数 2 の秒単位の平均間隔の対数を指定します。範囲は、選択した PTP プロファイルによって異なります。
- **ファブリック アナウンス タイムアウト** – PTP アナウンス メッセージが期限切れと見なされる前にシステムが待機するアナウンス メッセージの数を指定します。範囲とデフォルトは、選択した PTP プロファイルによって異なります。
- **詳細設定** – このセクションの横にある矢印をクリックして展開します。

  1. **[+プロファイルの追加（+Add Profile）]** をクリックして PTP プロファイルを追加します。プロファイルは、PTP のさまざまなユースケースに最適化されたさまざまなパラメータを定義するために使用されます。これらのパラメータの一部には、PTP メッセージ間隔の適切な範囲と PTP トランスポートプロトコルが含まれますが、これらに限定されません。PTP プロファイルは、さまざまな業界の多くの組織/標準規格によって定義されています
  2. **[プロファイルの追加（Add Profile）]** ダイアログ内に **[名前（Name）]**を入力します。
  3. **[プロファイル テンプレート（Profile Template）]** ドロップダウンから、使用可能なプロファイルの 1 つを選択します。

     プロファイルの詳細については、「*Cisco APIC システム管理構成ガイド*」を参照してください。
  4. 特定のユース ケースの必要に応じて、デフォルトのプロファイル値を更新します。

e) このステップを繰り返して、追加の PTP 設定ポリシーを作成します。

ステップ 13 QoS DSCP ポリシーを作成します。

このポリシーは、IPN ユース ケース全体での包括的な QoS 保持の一部です。このセクションにある情報を参照資料として使用することができます。しかし資料のIPN 全体での QoS の保持 （297 ページ）章の機能とユース ケース セクションの全てのステップのセットに従うことをおすすめします。

a) **[+オブジェクトを作成（+Create Object）** ドロップダウンから**QoS SDSCP**を作成します。

b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) ポリシーの詳細を入力します。

- **管理状態** –ポリシーの有効または、無効化。
- **詳細設定** – このセクションの横にある矢印をクリックして展開します。

  各 ACI QoS レベルの DSCP 値を選択します。各ドロップダウンには、使用可能な DSCP 値のデフォルトリストが含まれています。レベルごとに一意の DSCP 値を選択する必要があります。

e) 追加の QoS DSCP ポリシーを作成するために、このステップを繰り返します。

通常、マルチサイト ドメインの一部であるすべてのサイトにこのポリシーを一貫して適用することをお勧めします。

ステップ 14 QoS SR-MPLS ポリシーの作成

このポリシーは、包括的な SR-MPLS の使用例の一部です。このセクションにある情報を参照資料として使用することができます。しかし資料のマルチサイトと SR-MPLS L3Out ハンドオフ （335 ページ）章の機能とユース ケース セクションの全てのステップのセットに従うことをおすすめします。

a) **[+オブジェクトを作成（+Create Object）** ドロップダウンから**QoS SR-MPLS**を作成します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) 入力 QoS 変換ルールを追加するには、**[+入力ルールの追加（+Add Ingress Rule）]** をクリックします。

これらのルールは MPLS ネットワークから ACI ボーダー リーフ スイッチへ入力しているのトラフィックに適用されます。そして、着信パケットの EXP ビット（EXP）の ACI QoS レベルへのマップに使用されています。それとともに Differentiated Services Code Point（DSCP; DiffServ コードポイント）および/またはオリジナル トラフィックの CoS 値の設定に使用されます。指定された CoS 値が ACI リーフ ノードを出るトラフィックに使用されるようにするには、「QoS クラス ポリシー」の一部として CoS 保持機能も構成する必要があります。

カスタム ポリシーが定義されていないか、一致していない場合、デフォルトのQoSレベル（`Level 3`）が割り当てられます。

1. **[EXP 照合開始 (Match Exp From)]** と **[EXP 照合終了 (Match EXP To)]** フィールドで、照合する入力 MPLS パケットの EXP 範囲を指定します。
2. **[キューの優先順位 (Queuing Priority)]** ドロップダウンから、マッピングする ACI QoS レベルを選択します。

   これは、ACI ファブリック内のトラフィックに割り当てる QoS レベルで、ACI はファブリック内のトラフィックのプライオリティを決めるために使用します。オプションの範囲は `レベル 1` ー `レベル 6`です。デフォルト値は、`レベル 3`です。このフィールドで選択しない場合、トラフィックには自動的に `レベル 3` の優先順位が割り当てられます。
3. **[設定 DSCP（Set DSCP）]** ドロップダウンから、接続先 ACI リーフ スイッチから送信されるときにトラフィックに割り当てる DSCP 値を選択します。

指定されたDSCP値は、外部ネットワークから受信した元のトラフィックに設定されるため、トラフィックが宛先 ACI リーフ ノードで VXLAN カプセル化解除された場合にのみ再公開されます。

値を [未指定 (Unspecified)] に設定すると、パケットの元の DSCP 値が保持されます。

4. **[設定 CoS（Set CoS）]** ドロップダウンから、接続先 ACI リーフ スイッチから送信されるときにトラフィックに割り当てる CoS 値を選択します。

   指定された CoS 値は、接続先 ACI リーフ スイッチを出るトラフィックに設定されます。これには、CoS 保存を有効にする必要があります。

   値を [未指定 (Unspecified)] に設定すると、パケットの元の CoS 値が保持されますが、これはファブリックで CoS 保存オプションが有効になっている場合のみです。CoS 保存の詳細については、「*Cisco APIC and QoS*」を参照してください。

5. チェックマーク アイコンをクリックして、ルールを保存します。
6. 追加の入力 QoS ポリシー ルールについて、これらの手順を繰り返します。

e) 出力 QoS 変換ルールを追加するには、**[出力ルールの追加 (Add Egress Add Rule)]** をクリックします。

これらのルールは、MPLS L3Out を介して ACI ファブリックを離れるトラフィックの境界リーフ スイッチに適用され、パケットの DSCP 値を照合するために使用され、一致が見つかった場合は、次の構成されたポリシーに基づいて MPLS EXP および CoS 値を設定します。

カスタム ポリシーが定義されていないか、一致していない場合、デフォルトの EXP 値 0 がすべてのラベルでマークされます。EXP 値は、デフォルト ポリシー シナリオとカスタム ポリシー シナリオの両方でマークされ、パケット内のすべての MPLS ラベルで行われます。

カスタム MPLS 出力ポリシーは、既存の EPG、L3Out、および契約 QoS ポリシーをオーバーライドできます。

1. **[DSCP 照合開始 (MATCH DSCP From)]** と **[DSCP 照合終了 (MATCH DSCP To)]**] ドロップダウンを使用して、出力MPLSパケットのプライオリティを割り当てるために一致させるのDSCP範囲を指定します。
2. **[MPLS EXP の設定 (SET MPLS EXP)]** ドロップダウンから、出力 MPLS パケットに割り当てる EXP 値を選択します。
3. **[CoS の設定(Set CoS)]** ドロップダウンから、出力 MPLS パケットに割り当てる CoS 値を選択します。
4. チェックマーク アイコンをクリックして、ルールを保存します。
5. 追加の出力 QoS ポリシー ルールについて、この手順を繰り返します。

f) 追加の QoS SR-MPLS ポリシーを作成するために、このステップを繰り返します。

ステップ 15 QoS クラス ポリシー ポリシーを作成します。

Cisco ACI には、ユーザーが構成可能な QoS レベルが多数用意されています。Cisco APIC リリース 4.0（1）以降では、6 つのユーザ構成可能な QoS レベルがサポートされていますが、以前のリリースでは 3

がサポートされています。この手順では、Nexus ダッシュボード オーケストレータ を使用して、これらの各レベルの特定の設定を構成する方法について説明します。

ACI ファブリック内の QoS 機能の詳細については*Cisco APIC と QoS*を参照します。

これらのポリシーの最も一般的な使用例は、ACI ファブリックに着信するトラフィックの CoS 保存を有効にすることです。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[QoS クラス ポリシー（QoS Class Policy）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション)**[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) 必要に応じて、**CoS の保持**を有効にします。

トラフィックが ACI ファブリックに入ると、構成された QoS ポリシーに基づいて、各パケットを ACI QoS レベルにマッピングできます。これらの QoS レベルは、パケットの外部ヘッダーの CoS フィールドと DE ビットに格納され、元のヘッダーは破棄されます。入力パケットの元の CoS 値を保持し、パケットがファブリックを離れるときにそれを復元する場合は、802.1p サービス クラス（CoS）の保持をこの設定を利用することで有効にすることができます。

e) **[+レベルの追加（+Add Level）]** をクリックして、特定の QoS クラスの構成の詳細を定義します。

[QoS レベル構成を追加（Add QoS Level Configuration）] ウィンドウが開きます。

f) **[QoS レベル設定の追加（Add QoS Level Configuration）]** ウィンドウで、構成する QoS **レベル** を選択し、構成の詳細を指定します。

- **MTU** – この QoS クラスのパケットに使用される最大伝送単位。
- **最小バッファー** – 予約済みバッファーの最小数。数値は 0 から 3 の間で指定できます。

  デフォルト値は 0 です。
- **輻輳アルゴリズム** – この QoS レベルに使用される輻輳アルゴリズム。
- **スケジューリング アルゴリズム** – この QoS レベルに使用されるスケジューリング アルゴリズム。
- **割り当てられた帯域幅** – この QoS レベルに割り当てられた合計帯域幅の割合。値は 0 から 100 の間で指定できます。

  デフォルト値は 20 です。
- **PFC 管理状態** – FCoE トラフィックに適用されるプライオリティフロー制御ポリシーの管理状態。
- **管理状態** –ポリシーの有効または、無効化。
- **ドロップ Cos 無し** –FCoE トラフィックの輻輳の場合でも FCoE パケット処理をドロップしない CoS レベル。
- **PFC 範囲** – 優先フロー制御（PFC）の範囲。ファブリック全体のファブリック全体の `PFC`、またはスパイン スイッチのみの `IntraTor PFC`。

g) 追加の QoS クラス ポリシーを作成するために、このステップを繰り返します。

ステップ 16 テンプレートの変更内容を保存するために**[保存（Save）]** をクリックします。

ステップ 17 関連サイトに新しいテンプレートを展開するために**[展開（Deploy）]** をクリックします。

テナント ポリシー テンプレートの展開方法とアプリケーション テンプレートの展開方法は同じです。

以前にこのテンプレートを展開したが、それ以降に変更を加えていない場合は、**[展開]** の概要に変更がないことが示され、テンプレート全体を再展開することを選択できます。この場合は、この手順をスキップできます。

或いは、**[サイトに展開 (Deploy to Sites)]** ウィンドウには、サイトに展開される構成の違いの概要が表示されます。この場合、構成の違いのみがサイトに展開されることにご注意ください。テンプレート全体を再展開したい場合、違いを同期するために1回展開をする必要があります。そして、前のパラグラフに記されている通り、構成全体をプッシュするためにまた再展開する必要があります。

ファブリック 技術情報 ポリシーを作成

このセクションでは、1 つ以上のファブリック技術情報テンプレートを作成する方法について説明します。ファブリック技術情報テンプレートを使用すると、次のものを作成および構成できます。

- 物理インターフェイス
- ポート チャネル インターフェイス
- 仮想ポート インターフェイス
- ノードプロファイル
- ポッド プロファイル

始める前に

- ほとんどのファブリック 技術情報 ポリシーには 1 つ以上のファブリック ポリシーが必要なため、ファブリック ポリシーを作成 （87 ページ）で説明されているように、それらのファブリック ポリシーがすでに定義されている必要があります。

  たとえば、インターフェイス ポリシー（物理、ポート チャネル、または仮想ポート チャネル）を作成する場合は、インターフェイス設定ポリシーがすでに作成されている必要があります。

- ファブリック 技術情報 ポリシーに必要なファブリック ポリシーを含むテンプレートは、ファブリック 技術情報 ポリシー テンプレートの前に展開する必要があります。
- ファブリック 技術情報 ポリシー テンプレートは、テナントに関連付ける必要はありませんが、展開するには、少なくとも 1 つのサイトにマッピングする必要があります。

- 一般的な展開では、マルチサイト ドメインの一部である各サイトに個別のファブリック技術情報 ポリシー テンプレートを関連付けることをお勧めします。

  この場合、関連するポリシーの構成を、サイト レベルではなく常にグローバルテンプレート レベルでプロビジョニングすることもお勧めします。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 新しいファブリック技術情報ポリシー テンプレートを作成します。

a) 左側のナビゲーション メニューで、**[ファブリック管理（Fabric Management）]** > **[ファブリック技術情報ポリシー（Fabric Resource Policies）]** を選択します。

b) **[ファブリック技術情報テンプレート（Fabric Resource Templates）]** ページで、**[ファブリック技術情報 ンプレートの追加（Add Fabric Resource Template）]** をクリックします。

c) **[情報技術ポリシー（Resouce Policies）]** ページの右のプロパティ サイトバーにテンプレートの **[名前（Name）]** を入力します。

デフォルトでは、新しいテンプレートは空であるため、次のステップに従って 1 つ以上のファブリックポリシーを追加する必要があります。テンプレートで使用可能なすべてのポリシーを作成する必要はありません。このテンプレートとともに展開する各タイプのポリシーを 1 つ以上定義できます。特定のポリシーを作成したくない場合は、説明されている手順をスキップしてください。

ステップ 3 テンプレートを 1 つ以上のサイトに割り当てます。

サイトにテナント ポリシー テンプレートを割り当てるプロセスは、サイトにアプリケーション テンプレートを割り当てる方法と同じです。

a) **[テンプレート プロパティ（Template Properties）]** 表示内で **[アクション（Actions）]** をクリックして **[サイトの関連付け（Sites Association）]** を選択します。

[<template-name> にサイトの関連付け（Associate Sites to <template-name>）] ウィンドウが開きます。

b) **[サイトの関連付け（Associate Sites）]** ウィンドウで、テンプレートを展開するサイトの横のチェックボックスをオンにします。

テナント ポリシー テンプレートは、オンプレミス ACI サイトにのみサポートされることにご注意ください。そして、割り当て可能です。

c) **Ok** をクリックして保存します。

ステップ 4 物理インターフェイス ポリシーを作成します。

物理インターフェイス ポリシーを作成する前に、ファブリック ポリシーを作成 （87 ページ）で説明されているように、インターフェイス設定 （物理） ポリシーを作成しておく必要があります。

a) **[+オブジェクトを作成（+Create Object）]** ドロップダウンから、**[物理インターフェイス（Physical Interface）]** を選択します。

b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。

c) (オプション)**[説明を追加（Add Description）]**をクリックして、このポリシーの説明を入力します。

d) **[ノード（Nodes）]**フィールドで、この物理インターフェイス ポリシーが展開される 1 つ以上のノード識別子を指定します。

ノード ポリシーの構成は、テンプレートのサイト ローカル ビューでも実行できます。その場合、サイト レベルの構成は、グローバル テンプレート レベルの構成を上書きします。前述のように、異なるテンプレートが作成され、マルチサイト ドメインの一部である各サイトに関連付けられる特定のシナリオでは、グローバル テンプレート レベルでのみノード ポリシーを構成することをお勧めします。

たとえば、101、102 と 103 です。

e) **[インターフェース（Interfaces）]**フィールドに、ポリシーが展開されるインターフェース名を指定します。

たとえば、1/1、1/2-4 と 1/5 です。

f) **[選択した物理ポリシーはない（No selected Physical Policy）]**をクリックし、作成したインターフェイス設定ポリシーを選択します。

インターフェイス設定ポリシーで定義されたインターフェイス設定は、前のサブステップで指定したノード（101、102 と 103）上のインターフェイス（1/1、1/2-4、1/5）に適用されます。

g) この手順を繰り返して、追加の物理インターフェイス ポリシーを作成します。

たとえば、各ノードで一意の物理インターフェイスのセットを構成する必要がある場合など、別のポリシーが必要になる可能性があります。その場合、特定のノードごとに一意の物理インターフェイス ポリシーを定義します。

ステップ 5 ポート チャネル インターフェイス ポリシーを作成します。

ポート チャネル インターフェイス ポリシーを作成する前に、ファブリック ポリシーを作成 （87 ページ）で説明されているように、インターフェイス設定（PC/VPC）ポリシーを作成しておく必要があります。

a) **[+オブジェクトを作成（+Create Object）]**ドロップダウンから、**[ポート チャンネル インターフェイス（Port Channel Interface）]**を選択します。

b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]**を指定します。

c) (オプション)**[説明を追加（Add Description）]**をクリックして、このポリシーの説明を入力します。

d) **[ノード（Node）]**フィールドで、この物理インターフェイス ポリシーが展開されるスイッチののノード識別子を指定します。

ノード ポリシーの構成は、テンプレートのサイト ローカル ビューでも実行できます。その場合、サイト レベルの構成は、グローバル テンプレート レベルの構成を上書きします。前述のように、異なるテンプレートが作成され、マルチサイト ドメインの一部である各サイトに関連付けられる特定のシナリオでは、グローバル テンプレート レベルでのみノード ポリシーを構成することをお勧めします。

たとえば、104。

e) **[インターフェイス（Interfaces）]**フィールドに、ポート チャネルの一部であるインターフェイスのインターフェイス名を指定します。

たとえば、1/6 と 1/7 です。

f) **[選択した PC/VPC ポリシーはない（No selected PC/VPC Policy）]** をクリックし、作成したインターフェイス設定ポリシーを選択します。

インターフェイス設定ポリシーで定義されたポート チャネル設定は、前のサブステップで指定したノード（104）上のインターフェイス（1/6 と 1/7）に適用されます。

g) この手順を繰り返して、追加のポート チャネル インターフェイス ポリシーを作成します。

たとえば、各ノードでポート チャネル インターフェイスの一意のセットを設定する必要がある場合など、別のポリシーが必要になることがあります。その場合、特定のノードごとに一意のポートチャネル インターフェイス ポリシーを定義します。

ステップ 6 仮想ポート チャネル インターフェイス ポリシーを作成します。

仮想ポート チャネル インターフェイス ポリシーを作成する前に、ファブリック ポリシーを作成 （87 ページ）で説明されているように、インターフェイス設定（PC/VPC）ポリシーを作成しておく必要があります。

a) **[+オブジェクトを作成（+Create Object）]** ドロップダウンから、**[仮想ポート チャンネル インターフェイス（Virtual Port Channel Interface）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) **[ノード 1（Node 1）]** フィールドに、仮想ポート チャネルの一部であるインターフェイスを含む最初のスイッチのノード識別子を指定します。

たとえば、105。

e) **[ノード 1 のインターフェース（Interfaces on Node 1）]** フィールドで、最初のスイッチのインターフェースを指定します。

たとえば、1/8 と 1/9 です。

f) **[ノード 2（Node 2）]** フィールドに、仮想ポート チャネルの一部であるインターフェイスを含む 2 番目のスイッチのノード識別子を指定します。

ノード ポリシーの構成は、テンプレートのサイト ローカル ビューでも実行できます。その場合、サイト レベルの構成は、グローバル テンプレート レベルの構成を上書きします。前述のように、異なるテンプレートが作成され、マルチサイト ドメインの一部である各サイトに関連付けられる特定のシナリオでは、グローバル テンプレート レベルでのみノード ポリシーを構成することをお勧めします。

たとえば、106。

g) **[ノード 2 のインターフェース（Interfaces on Node 2）]** フィールドで、2 番目のスイッチのインターフェースを指定します。

たとえば、1/8 と 1/9 です。

h) **[選択した PC/VPC ポリシーはない（No selected PC/VPC Policy）]** をクリックし、作成したインターフェイス設定ポリシーを選択します。

インターフェイス設定ポリシーで定義されたポート チャネル設定は、前のサブステップで指定したノード上のインターフェイスに適用されます。

i) この手順を繰り返して、追加の仮想ポート チャネル インターフェイス ポリシーを作成します。

ステップ 7 ノード プロファイル ポリシーを作成します。

ノード プロファイル ポリシーを作成する前に、ファブリック ポリシーを作成 （87 ページ）で説明されているように、ノード設定ポリシーを作成しておく必要があります。

このリリースでは、ノード設定ポリシーを使用して、SyncE および/または PTP 機能を有効にすることができます。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[ノード プロファイル（Node Profile）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) **[ノード（Nodes）]** フィールドに、このノード プロファイル ポリシーを展開するスイッチのノード識別子を指定します。

ノードポリシーの構成は、テンプレートのサイト ローカル ビューでも実行できます。その場合、サイト レベルの構成は、グローバル テンプレート レベルの構成を上書きします。前述のように、異なるテンプレートが作成され、マルチサイト ドメインの一部である各サイトに関連付けられる特定のシナリオでは、グローバル テンプレート レベルでのみノード ポリシーを構成することをお勧めします。

e) **[選択したノード ポリシーはない（No selected Node Policy）]** をクリックし、作成したノード設定ポリシーを選択します。

ノード設定ポリシーで定義されたノード設定は、前のサブステップで指定したすべてのノードに適用されます。

特定のノード プロファイルでは、単一のノード設定ポリシーのみを参照できます。つまり、特定のノード（またはノードのセット）に対して SyncE ポリシーと PTP ポリシーの両方を有効にする場合は、両方の機能を同時に有効にした対応するノード設定ポリシーを（ファブリック ポリシー テンプレートの一部として）作成し、ノード プロファイルで参照される必要があります。

f) 追加のノード プロファイル ポリシーを作成するためにこのステップを繰り返します。

特定のノード（またはノードのセット）に関連付けることができるノード プロファイル ポリシーは 1 つだけです。

ステップ 8 ポッド プロファイル ポリシーを作成します。

ポッド プロファイル ポリシーを作成する前に、ファブリック ポリシーを作成 （87 ページ）で説明されているように、ポッド設定ポリシーを作成しておく必要があります。このリリースでは、Pod 設定ポリシーを使用して NTP 機能を有効にできます。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[ポッド プロファイル（Pod Profile）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。

d) **[タイプ（Type）]** ドロップダウンから、ポリシーを［すべて（All）］のポッドに適用するか、ポッドの［範囲（Range）］に適用するかを選択します。

e) **[タイプ（Type）]** で［範囲（Range）］を選択した場合は、このポリシーを適用するポッドの範囲を指定します。

f) **[選択したポッド ポリシーはない（No selected Pod Policy）]** をクリックし、作成したポッド設定ポリシーを選択します。

ポッド設定ポリシーで定義されたポッド設定は、前のサブステップで指定したすべてのノードに適用されます。

g) 追加のポッド プロファイル ポリシーを作成するためにこのステップを繰り返します。

特定のポッド（またはポッドのセット）関連付けることができるポッド プロファイル ポリシーは 1 つだけです。

ステップ 9 テンプレートの変更内容を保存するために**[保存（Save）]** をクリックします。

（注）
テンプレートを 1 つ以上のサイトに保存（または展開）すると、オーケストレータ は、指定されたノードやインターフェースがサイトに対して有効であることを確認し、有効でなければエラーを返します。

ステップ 10 関連サイトに新しいテンプレートを展開するために**[展開（Deploy）]** をクリックします。

テナント ポリシー テンプレートの展開方法とアプリケーション テンプレートの展開方法は同じです。

以前にこのテンプレートを展開したが、それ以降に変更を加えていない場合は、**[展開]** の概要に変更がないことが示され、テンプレート全体を再展開することを選択できます。この場合は、この手順をスキップできます。

或いは、**[サイトに展開 (Deploy to Sites)]** ウィンドウには、サイトに展開される構成の違いの概要が表示されます。この場合、構成の違いのみがサイトに展開されることにご注意ください。テンプレート全体を再展開したい場合、違いを同期するために1回展開をする必要があります。そして、前のパラグラフに記されている通り、構成全体をプッシュするためにまた再展開する必要があります。

モニタリング ポリシーを作成

このセクションでは、モニタリング ポリシー テンプレートを使用して 1 つ以上の SPAN セッション ポリシーを作成する方法について説明します。

始める前に

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 新しいテナント ポリシーを作成。

a) 左側のナビゲーション メニューで、**[ファブリック管理（Fabric Management）]** > **[モニタリング ポリシー（Monitoring Policies）]** を選択します。

b) **[モニタリング ポリシー テンプレート（Monitoring Policy Template）]**ページ内で**[モニタリング ポリシー テンプレートを追加（Add Monitoring Policy Template）]**をクリックします。

c) このテンプレートの SPAN セッション タイプを選択します。

次のいずれかを選択できます。

- **テナント** – このタイプの SPAN セッションは通常 ERSPAN セッションと呼ばれ、ファブリック内の任意の場所にある指定されたテナントに属する EPG を SPAN セッションの送信元として構成し、同じまたは異なるテナントに属する別の EPG を接続先として構成できます。
- **アクセス** – 次の 2 つのシナリオのいずれかを構成できます。
  - アクセス ポート、ポート チャネル、および vPC を送信元として、接続先を物理/ポート チャネルインターフェイスとして使用します。この場合、送信元インターフェイスと接続先インターフェイスは同じスイッチ上にある必要があります。
  - アクセス ポート、ポート チャネル、および vPC を送信元として、接続先を EPG として使用します。この場合、これは ERSPAN セッションであり、SPAN 接続先をファブリック内の任意の場所に接続できます。

d) セッション タイプとしてテナントを選択した場合は、モニタリング ポリシーを関連付ける**テナント**を選択します。

e) モニタリング ポリシーを関連付ける **サイト** を選択します。

f) **[モニタリング ポリシー（Monitoring Policies）]** ページの右のプロパティ サイトバーにテンプレートの **[名前（Name）]** を入力します。

デフォルトでは、新しいテンプレートは空であるため、次のステップに従って 1 つ以上のファブリック ポリシーを追加する必要があります。

ステップ 3 テンプレートを 1 つ以上のサイトに割り当てます。

サイトにテナント ポリシー テンプレートを割り当てるプロセスは、サイトにアプリケーション テンプレートを割り当てる方法と同じです。

a) **[テンプレート プロパティ（Template Properties）]** 表示内で **[アクション（Actions）]** をクリックして **[サイトの関連付け（Sites Association）]** を選択します。

[<template-name> にサイトの関連付け（Associate Sites to <template-name>）] ウィンドウが開きます。

b) **[サイトの関連付け（Associate Sites）]** ウィンドウで、テンプレートを展開するサイトの横のチェック ボックスをオンにします。

テナント ポリシー テンプレートは、オンプレミス ACI サイトにのみサポートされることにご注意ください。そして、割り当て可能です。

c) **Ok** をクリックして保存します。

ステップ 4 テナント タイプ テンプレートの SPAN セッション ポリシーを作成します。

テンプレート タイプに ファクセス を選択した場合は、代わりに次の手順を使用します。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[SPAN セッション（SPAN Session）]** を選択します。

b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。

c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。

d) **管理状態（Admin State）]** チェックボックスを有効にします。

管理状態が無効に設定されている場合、構成されたモニターにデータは送信されません。

e) **[+ 送信元の追加（+Add Source）]** をクリックして、SPAN 送信元情報を指定します。

送信元情報については、次の情報を提供します。

- **名前**
- 方向 – SPAN 送信元 パケットの方向。次のいずれかになります。
  - 両方 – 送信元に着信し、送信元から発信するパケットを複製して転送します。
  - 着信 – 送信元に着信するパケットを複製して転送します。
  - 発信 – 送信元から発信されるパケットを複製して転送します。
- **送信元 EPG** – SPAN トラフィックの送信元。

  テナント タイプ テンプレートの場合、送信元は常に EPG です。

[OK] をクリックして、送信元を保存します。次に、必要に応じて **[+ 送信元の追加（+Add Source）]** をクリックして、追加の送信元を提供できます。

f) **[接続先グループ（Destination Group）]** セクションから、複製されたパケットの転送先となる**テナント**、**接続先 EPG**、および**接続先 IP アドレス**を指定します。

このフィールドでは、IPv4 および IPv6 の IP アドレスがサポートされています。ただし、**接続先 IP** に IPv4 を使用し、**送信元 IP プレフィックス**に IPv6 を使用すること、またはその逆を混在させてはなりません。

g) **[送信元 IP プレフィックス]** に入力します。

特定の IP アドレスが構成されている場合、すべての ERSPAN トラフィックはその IP から発信されます（たとえば、ERSPAN トラフィックを発信するすべての ACI リーフ スイッチの場合）。代わりにプレフィックスが構成されている場合、各 ACI リーフ スイッチには、送信元 ERSPAN トラフィックへのそのプレフィックスの一部である一意の IP が割り当てられます。これは、接続先スイッチで ERSPAN トラフィックの発信元を区別するのに役立ちます。

h) **SPAN バージョン**を選択します。

i) （オプション）必要な場合、**詳細設定**を構成します。

- **SPAN バージョンを施行** – 有効にすると、選択した SPAN バージョンを強制します。

  有効の場合、ハードウェアがサポートしている場合、SPAN セッションは指定された SPAN バージョンを使用します。そうしないと、セッションは機能不全になります。

無効でバージョン 2 が指定されているが、ハードウェアでサポートされていない場合は、バージョン 1 が使用されます。

- **フロー ID** – ERSPAN パケットの識別子。

  パケットがコピーされ、ERSPAN 経由で送信されると、パケットは ERSPAN ヘッダーでカプセル化されます。フロー ID は、これらのパケットがコピーされた ERSPAN セッションを識別するための ERSPAN ヘッダー内の番号です。

  指定できる範囲は 1 ～ 1023 です。デフォルトは 1 です。

- **TTL** – 存続可能時間 （TTL） または 1 ～ 255 ホップの範囲のホップ制限。ゼロに設定すると、TTL は指定されません。デフォルトのホップ カウントは 64 です。

- **DSCP** – ERSPAN パケットの IP ヘッダーに設定されている DSCP 値。

- **MTU** – ERSPAN で生成されたパケットの MTU。

  範囲は 64 ～ 9216 です。デフォルトは、 1518 です。

  ERSPAN の場合、ERSPAN カプセル化が追加されるため、接続先デバイスが受信する実際の MTU は、構成された MTU より大きくなります。ERSPAN バージョン 2 では、さらに 46 バイトが追加されます。ERSPAN バージョン 1 の場合、さらに 34 バイトが追加されます。その結果、デフォルトの MTU が 1518 の場合、エンド デバイスは実際にバージョン 2 の場合は 1564（1518 + 36）、バージョン 1 の場合は 1552（1518 + 34）をサポートする必要があります。

  キャプチャされたフレームが構成された MTU より大きい場合、フレームは複製時に MTU 長に切り捨てられます。パケット/フレームのペイロードは不完全ですが、ヘッダーは分析のためにそのままの状態である必要があります。

j) 追加のテナント SPAN セッション ポリシーを作成するためにこのステップを繰り返してください。

ステップ 5 アクセス タイプ テンプレートの SPAN セッション ポリシーを作成します。

テンプレート タイプに [テナント] を選択した場合は、代わりに前の手順を使用します。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[SPAN セッション（SPAN Session）]** を選択します。
b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。
c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) **管理状態（Admin State）]** チェックボックスを有効にします。

管理状態が無効に設定されている場合、構成されたモニターにデータは送信されません。

e) **[+ 送信元の追加（+Add Source）]** をクリックして、SPAN 送信元情報を指定します。

送信元情報については、次の情報を提供します。

- **名前**
- **[+ アクセス パスの追加（+Add Access Path）]** をクリックして、リーフ スイッチに 1 つ以上のパスを追加します。次のパスがサポートされます：
  - [ポート（Port）]

- [ポート チャネル （Port Channel）]
- 仮想ポートチャネル
- VPC コンポーネント PC

  vPC を送信元として構成し、物理/ポートチャネル インターフェイスを接続先として構成する場合は、VPC コンポーネント PC オプションを使用できます。このユース ケースでは、すべてのインターフェイスが同じスイッチ上にある必要があるため、vPC を送信元として選択してはならず、接続先が接続されている同じスイッチ上のその vPC のインターフェイスを表す VPC コンポーネント PC オプションを選択する必要があります。つまり、vPC ドメインの一部である 2 番目のスイッチに 2 番目の SPAN セッションを作成して、ローカルの接続先に向かうそのスイッチの vPC の一部である送信元インターフェイスにトラフィックをスパンできるようにする必要があります。

- 方向 – SPAN 送信元 パケットの方向。次のいずれかになります。
  - 両方 – 送信元に着信し、送信元から発信するパケットを複製して転送します。
  - 着信 – 送信元に着信するパケットを複製して転送します。
  - 発信 – 送信元から発信されるパケットを複製して転送します。

- **[+フィルタを追加（+Add Filter）]** をクリックして、SPAN トラフィック フィルタ処理情報を提供します。

  トラフィック フィルタ処理はオプションであり、フィルタが指定されていない場合、すべてのトラフィックがスパンされます。

  次の属性に基づいてフィルタ処理を有効化できます：
  - **Src IP プレフィックス**
  - **Src ポートから**
  - **Src ポートへ**
  - **Dst IP プレフィックス**
  - **Dst ポートから**
  - **Dst ポートへ**
  - **IP プロトコル**

- **SPAN ドロップ パケット** – SPAN は、通常の SPAN ではキャプチャされないドロップされたパケットの一部をキャプチャできますが、「フォワード ドロップ」としてドロップされたパケットに限定されます。

  有効にすると、ドロップされたパケット**のみ**のスパニングが許可され、ドロップされなかったトラフィックは許可されません。

  無効の場合、SPAN はドロップされなかったトラフィック**のみ**をキャプチャします。

  デフォルト値は Disabled です。

- **EPG フィルタ – SPAN ドロップ パケット**が無効になっている場合、送信元の EPG に基づいて送信元 パケットをフィルタ処理できます。フィルタを有効にするには、**EPG** を選択し、**送信元 EPG** ドロップダウンから特定の EPG を選択します。

  以前に設定された送信元インターフェイスで送受信されるトラフィックは、指定された EPG に属している場合にのみスパンされます。

[OK] をクリックして、送信元を保存します。次に、必要に応じて **[+ 送信元の追加（+Add Source）]** をクリックして、追加の送信元を提供できます。

f) **接続先タイプ**を選択します。

複製されたパケットは、EPG または特定のアクセス インターフェイスに転送できます。最初のケースでは、ファブリック内の任意の場所に接続された接続先にスパン トラフィックを送信するために ERSPAN セッションが作成されます。後者の場合、接続先は、送信元インターフェイスと同じスイッチ上の物理/ポート チャネル インターフェイスに接続されている必要があります。

g) **接続先タイプ**に `EPG` を選択した場合は、次の情報を提供します。

- 複製されたパケットの転送先となる**テナント**、**接続先 EPG**、および**接続先 IP アドレス**。

  このフィールドでは、IPv4 または IPv6 IP アドレスがサポートされています。ただし、**接続先 IP** に IPv4 を使用し、**送信元 IP プレフィックス**に IPv6 を使用すること、またはその逆を混在させてはなりません。

- **送信元 IP プレフィックス** – 送信元パケットの IP サブネットのベース IP アドレスです。
- **SPAN バージョン**
- （オプション）**[詳細設定（Advanced Settings）]**
  - **SPAN バージョンを施行** – 有効にすると、選択した SPAN バージョンを強制します。

    `有効`の場合、ハードウェアがサポートしている場合、SPAN セッションは指定された SPAN バージョンを使用します。そうしないと、セッションは機能不全になります。

    `無効`でバージョン 2 が指定されているが、ハードウェアでサポートされていない場合は、バージョン 1 が使用されます。

  - **フロー ID** – ERSPAN パケットの識別子。

    パケットがコピーされ、ERSPAN 経由で送信されると、パケットは ERSPAN ヘッダーでカプセル化されます。フロー ID は、これらのパケットがコピーされた ERSPAN セッションを識別するための ERSPAN ヘッダー内の番号です。

    指定できる範囲は 1 ～ 1023 です。デフォルトは 1 です。

  - **TTL** – 存続可能時間 （TTL） または `1 ～ 255` ホップの範囲のホップ制限。ゼロに設定すると、TTL は指定されません。デフォルトのホップ カウントは 64 です。

  - **DSCP** – ERSPAN パケットの IP ヘッダーに設定されている DSCP 値。

  - **MTU** – ERSPAN で生成されたパケットの MTU。

    範囲は 64 ～ 9216 です。デフォルトは、 `1518` です。

ERSPAN の場合、ERSPAN カプセル化が追加されるため、接続先デバイスが受信する実際の MTU は、構成された MTU より大きくなります。ERSPAN バージョン 2 では、さらに 46 バイトが追加されます。ERSPAN バージョン 1 の場合、さらに 34 バイトが追加されます。その結果、デフォルトの MTU が 1518 の場合、エンド デバイスは実際にバージョン 2 の場合は 1564（1518 + 36）、バージョン 1 の場合は 1552（1518 + 34）をサポートする必要があります。

キャプチャされたフレームが構成された MTU より大きい場合、フレームは複製時に MTU 長に切り捨てられます。パケット/フレームのペイロードは不完全ですが、ヘッダーは分析のためにそのままの状態である必要があります。

h) それ以外の場合、**接続先タイプ**にアクセス インターフェイスを選択した場合は、代わりに次の情報を提供します：

- **パス タイプ** – インターフェイスのタイプ。ポートまたはポート チャネルです。
- ポート インターフェイスの場合は、**ノード**と**パス**を選択します。
- ポート チャネル インターフェイスの場合、ポート チャネルの名前を選択します。
- **MTU** – ERSPAN で生成されたパケットの MTU。

  範囲は 64 ～ 9216 です。デフォルトは、 1518 です。

  ERSPAN の場合、ERSPAN カプセル化が追加されるため、接続先デバイスが受信する実際の MTU は、構成された MTU より大きくなります。ERSPAN バージョン 2 では、さらに 46 バイトが追加されます。ERSPAN バージョン 1 の場合、さらに 34 バイトが追加されます。その結果、デフォルトの MTU が 1518 の場合、エンド デバイスは実際にバージョン 2 の場合は 1564（1518 + 36）、バージョン 1 の場合は 1552（1518 + 34）をサポートする必要があります。

  キャプチャされたフレームが構成された MTU より大きい場合、フレームは複製時に MTU 長に切り捨てられます。パケット/フレームのペイロードは不完全ですが、ヘッダーは分析のためにそのままの状態である必要があります。

i) 追加のアクセス SPAN セッション ポリシーを作成するためにこのステップを繰り返してください。

ステップ 6 テンプレートの変更内容を保存するために**[保存（Save）]** をクリックします。

ステップ 7 関連サイトに新しいテンプレートを展開するために**[展開（Deploy）]** をクリックします。

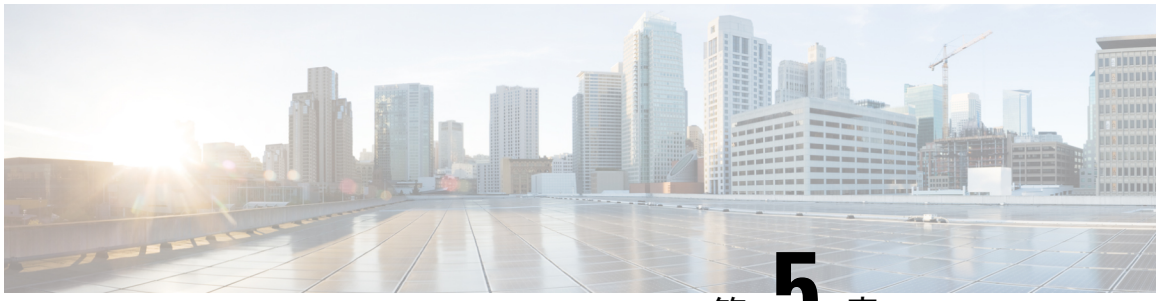
テナント ポリシー テンプレートの展開方法とアプリケーション テンプレートの展開方法は同じです。

以前にこのテンプレートを展開したが、それ以降に変更を加えていない場合は、**[展開]** の概要に変更がないことが示され、テンプレート全体を再展開することを選択できます。この場合は、この手順をスキップできます。

或いは、**[サイトに展開 (Deploy to Sites)]** ウィンドウには、サイトに展開される構成の違いの概要が表示されます。この場合、構成の違いのみがサイトに展開されることにご注意ください。テンプレート全体を再展開したい場合、違いを同期するために1 回展開をする必要があります。そして、前のパラグラフに記されている通り、構成全体をプッシュするためにまた再展開する必要があります。

第 II 部

操作



第 5 章

監査ログ

監査ログ

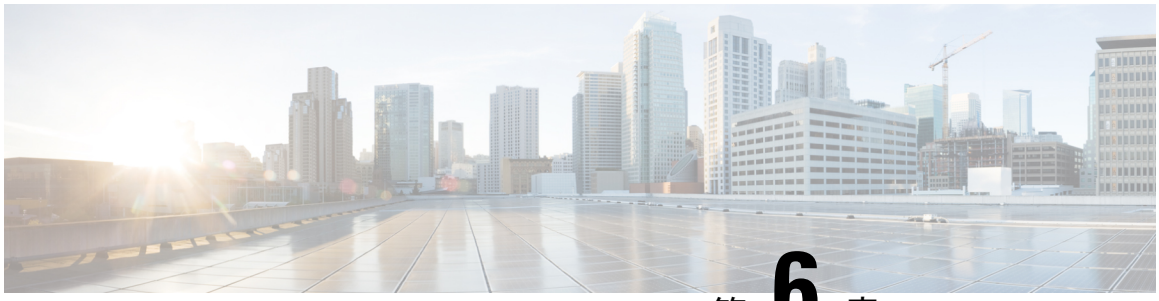
Nexus Dashboard Orchestrator のシステム ロギングは、最初に Orchestrator クラスタをデプロイしたときに自動的に有効になり、環境内で発生したイベントと障害をキャプチャします。

GUI 内で直接 Nexus Dashboard Orchestrator のログを表示するには、メインのナビゲーション メニューから **[操作 (Operations)]** > **[監査ログ (Audit logs)]** を選択します。

[**監査ログ (Audit Logs)**] ページで、**最新のフィールド**をクリックして、ログを表示する特定の期間を選択できます。たとえば、2017 年 11 月 14日から 2017 年 11 月 17日までの範囲を選択し、[**適用 (Apply)**] をクリックすると、この期間の監査ログの詳細が [**監査ログ (Audit Logs)**] ページに表示されます。

次の基準に従ってログの詳細のフィルタ処理を行うには、[**フィルタ (Filter)**] アイコンをクリックします。

- **ユーザ(User)**: ユーザ タイプに基づいて監査ログのフィルタ処理を行うには、このオプションを選択し、[**適用 (Apply)**] をクリックします。
- **タイプ (Type)** : 監査ログをポリシータイプ（サイト、ユーザ、テンプレートなど）でフィルタリングするには、このオプションを選択して、**[適用 (Apply)]** をクリックします。
- **アクション(Action)**: アクションに基づいて監査ログをフィルタ処理するには、このオプションを選択します。使用可能なアクションとしては作成、更新、削除、追加、関連付け、関連付けの解除解除、展開、展開の解除、ダウンロード、アップロード、復元、ログイン、ログの失敗があります。アクションに従ってログの詳細をフィルタ処理するには、アクションを選択して **Apply** をクリックします。



第 6 章

バックアップと復元

構成のバックアップと復元に関するガイドライン

Nexus Dashboard Orchestrator の障害またはクラスタの再起動からのリカバリを容易にする、Orchestrator 設定のバックアップを作成できます。Orchestrator の各アップグレードまたはダウングレードの前で、各設定の変更または展開後に、設定のバックアップを作成することを推奨します。バックアップは常に、Nexus Dashboard Orchestratorで定義されているリモート サーバ（Nexus Dashboard クラスタ以外）に作成されます。定義については、続くセクションで説明します。

構成のバックアップを作成する際には、次のガイドラインが適用されます。

- より新しいリリースから作成されたバックアップのインポートおよび復元はサポートされていません。

  たとえば、Nexus Dashboard Orchestrator を以前のリリースにダウングレードした場合、それ以降のリリースで作成された設定のバックアップを復元することはできません。

- リリース 4.0(1) より前のリリースで作成された構成バックアップの復元は、このリリースへの最初のアップグレード時にのみサポートされます。

  リリース 4.0(1) より前のリリースからこのリリースにアップグレードする場合は、*Cisco Nexus Dashboard Orchestrator* 導入ガイドの「Nexus ダッシュボードでの NDO サービスのアップグレード」の章を参照してください。

- バックアップを保存すると、設定は展開されたのと同じ状態で保存されます。バックアップを復元すると、展開されたすべてのポリシーが展開済みとして表示されますが、展開されていなかったポリシーは未展開の状態のままになります。
- バックアップ アクションの復元では、Nexus Dashboard Orchestrator のデータベースを復元しますが、各サイトのコントローラ（APIC、クラウド ネットワーク、NDFC など）データベースは変更されません。

  Orchestratorデータベースを復元した後、このガイドの「構成のばらつき」セクションで説明されているように、テンプレートに表示される可能性のある構成のばらつきを解決してから、既存のテンプレートを再展開して、Nexus Dashboard と各サイトのコントローラの間でポリシーが一致しない可能性を回避することをお勧めします。
- 構成のバックアップを作成するとき、ファイルは最初にOrchestratorsのローカル ドライブに作成され、リモートの場所にアップロードされた後、ローカル ストレージから削除されます。十分なローカル ディスク領域がない場合、バックアップは失敗します。
- リリース4.0(1)以降にアップグレードする前に、ローカルバックアップを作成できるようバックアップ スケジューラを有効にしていた場合、アップグレード後に無効になります。

  アップグレード後、セットアップしたリモート ロケーションを再度追加してから、バックアップ スケジューラを再度有効にする必要があります。
- UI を使用してバックアップを削除すると、バックアップ ファイルもリモート ロケーションから削除されます。

構成のバックアップを復元する際には、次のガイドラインが適用されます。

- バックアップが作成されてから復元されるまでの間にポリシーの変更がない場合は、追加の考慮事項は必要ありません。また、バックアップの復元（121 ページ） の説明に従って設定を復元するだけです。
- 設定のバックアップが作成されてから復元された時間までの間に設定変更が行われた場合は、次の点を考慮してください。
  - バックアップを復元しても、サイトのオブジェクト、ポリシー設定は変更されません。バックアップ以降に作成および展開された新しいオブジェクトまたはポリシーは、展開されたままになります。

    Orchestrator データベースを復元した後、このガイドの「構成のbaratukiドリフト」セクションで説明されているように、テンプレートに表示される可能性のある構成のドリフトを解決してから、既存のテンプレートを再デプロイして、Nexusダッシュボード間でポリシーが一致しない可能性を回避することをお勧めします。 オーケストレーターと各サイトのコントローラー。We recommend that after you restore the Orchestrator database you resolve any configuration drifts that may appear in the templates, as described in "Configuration Drifts" section of this guide, and then re-deploy the existing templates to avoid potentially mismatching policies between the Nexus Dashboard Orchestrator and each site's controller.

    または、すべてのポリシーを最初に展開解除することもできます。これにより、バックアップから設定が復元された後に、古いオブジェクトの潜在的な問題が回避されま

す。ただし、これにより、これらのポリシーによって定義されたトラフィックまたはサービスの中断が発生します。

- 設定のバックアップを復元するために必要な手順については、バックアップの復元（121 ページ） で説明しています。
- 復元した設定バックアップが、サイトに展開される前に保存されたものであった場合、未展開状態で復元されるので、必要に応じてサイトに展開できます。
- 復元した設定バックアップが、設定がすでに展開されているときに保存されたものであった場合、サイトにどの設定もまだ存在していなかったとしても、展開済み状態で復元されます。

  この場合、このガイドの「構成のばらつき」セクションで説明されているように、テンプレートに表示される可能性のある構成のばらつきを解決し、テンプレートを再展開して、Nexus Dashboard Orchestrator の構成をサイトと同期します。
- バックアップの作成時に管理されていたサイトがNexusダッシュボードに存在しない場合、復元は失敗します。
- バックアップ後にサイトのステータス（管理対象と非管理対象）を変更していて、サイトがNexusダッシュボードにまだ存在している場合、ステータスはバックアップ時の状態に復元されます。

バックアップのリモート ロケーションの設定

このセクションでは、設定バックアップをエクスポートできる Nexus Dashboard Orchestrator のリモート ロケーションの設定方法を説明します。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 左側のナビゲーション ペインで、**[操作 (Operations)]** > **[リモート ロケーション (Remote Loacation)]**を選択します。

ステップ 3 メイン ウィンドウの右上隅で、[**リモート ロケーションの追加 (Add Remote Location)**] をクリックします。

[新規リモート ロケーションの追加 (Add New Remote Location)] 画面が表示されます。

ステップ 4 リモート ロケーションの名前と説明 (任意) を入力します。

現在、2 つのプロトコルが設定バックアップのリモート エクスポートに対してサポートされています。

- SCP
- ステップ

（注）

SCPは Windows 以外のサーバーでのみサポートされます。リモートロケーションが Windows サーバーの場合は、SFTP プロトコルを使用する必要があります。

ステップ 5 リモート サーバのホスト名または IP アドレスを指定します。

[**プロトコル (Protocol)**] セクションに基づいて、指定するサーバーでは SCP または SFTP 接続を許可する必要があります。

ステップ 6 バックアップを保証するリモート サーバーのディレクトリにフル パスを指定します。

パスの先頭にはスラッシュ (/) 文字を使用し、ピリオド (.) とバックスラッシュ (\) を含むことはできません。例: */backups/multisite*

（注）
ディレクトリは、リモート サーバにすでに存在しなければなりません。

ステップ 7 リモート サーバに接続するために使用するポートを指定します。

デフォルトで、ポートは 22 に設定されます。

ステップ 8 リモート サーバに接続するときに使用される認証タイプを指定します。

次の 2 つの認証方式のうちの 1 つを使用して設定できます。

- パスワード—リモート サーバにログインするために使用されるユーザ名とパスワードを指定します。
- SSH プライベート ファイル—ユーザ名とリモート サーバにログインするために使用される SSH キー/パスフレーズのペアを指定します。

ステップ 9 [**保存 (Save)**] を使用して、リモート サーバを追加します。

バックアップの作成

ここでは、Nexus Dashboard Orchestrator 設定の新しいバックアップを作成する方法について説明します。

始める前に

バックアップのリモートロケーションの設定（119ページ）の説明に従って、最初にリモートロケーションを追加する必要があります。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 既存の展開設定をバックアップします。

a) 左側のナビゲーション ペインで、**[操作 (Operations)]** > **[バックアップと復元 (Backups & Restore)]**を選択します。

b) メイン ウィンドウ ペインで、**[新規バックアップ (New Backup)]** をクリックします。

[新規バックアップ (New Backup)] ウィンドウが開きます。

c) バックアップ情報を提供します。

- **[名前 (Name)]** フィールドに、バックアップ ファイルの名前を入力します。

  名前には、最大 10 文字の英数字を使用できますが、スペースまたはアンダースコア (_) は使用できません。

- **[リモートロケーション (Remote location)]** ドロップダウンから、バックアップを保存するために構成したリモートロケーションを選択します。

- （オプション）**[リモートパス（Remote Path）]** では、バックアップを保存する先のリモートサーバーの特定のディレクトリを提供します。

  指定するディレクトリはすでに存在している必要があります。

d) **[保存（Save）]** をクリックして、バックアップを作成します。

バックアップの復元

このセクションでは、Orchestrator 設定を前の状態に復元する方法について説明します。

始める前に

- バックアップのリモート ロケーションの設定 （119 ページ） で説明されているように、NDO バックアップを保存するためのリモート ロケーションを構成しておく必要があります。
- バックアップをリモート ロケーションへインポートする （127 ページ） の説明に従って、復元するバックアップがリモート ロケーション サーバーにあることを確認するか、バックアップをリモート ロケーションにインポートします。

（注） バックアップ アクションの復元では、Nexus Dashboard Orchestrator のデータベースを復元しますが、各サイトのコントローラ（APIC、クラウド ネットワーク、NDFC など）データベースは変更されません。

Orchestrator データベースを復元した後、このガイドの「構成のばらつき」セクションで説明されているように、テンプレートに表示される可能性のある構成のばらつきを解決してから、既存のテンプレートを再展開して、Nexus Dashboard と各サイトのコントローラの間でポリシーが一致しない可能性を回避することをお勧めします。

特定の構成の不一致とそれぞれに関連する望ましい復元手順の詳細は、構成のバックアップと復元に関するガイドライン （117 ページ）を参照してください。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 必要に応じて、既存のポリシーの展開を解除します。

バックアップが作成されたときから現在の設定までに、設定に新しいオブジェクトまたはポリシーが追加されている場合は、この手順を実行することをお勧めします。追加情報については、構成のバックアップと復元に関するガイドライン （117 ページ） を参照してください。

ステップ 3 左側のナビゲーション メニューで、**[操作 (Operations)]** > **[バックアップと復元 (Backups & Restore)]**を選択します。

ステップ 4 メイン ウィンドウで、復元するバックアップの隣のアクション **(...)** アイコンをクリックし、**[このバックアップにロールバック (Rollback to this backup)]** を選択します。

選択したバックアップのバージョンが、実行中の Nexus Dashboard Orchestrator のバージョンと異なる場合、ロールバックが原因で、バックアップされたバージョンには存在しない機能が削除される可能性があります。

ステップ 5 **[はい (Yes)]** をクリックして、選択したバックアップを復元することを確認します。

[はい (Yes)] をクリックすると、システムは現在のセッションを終了して、ユーザはログアウトされます。

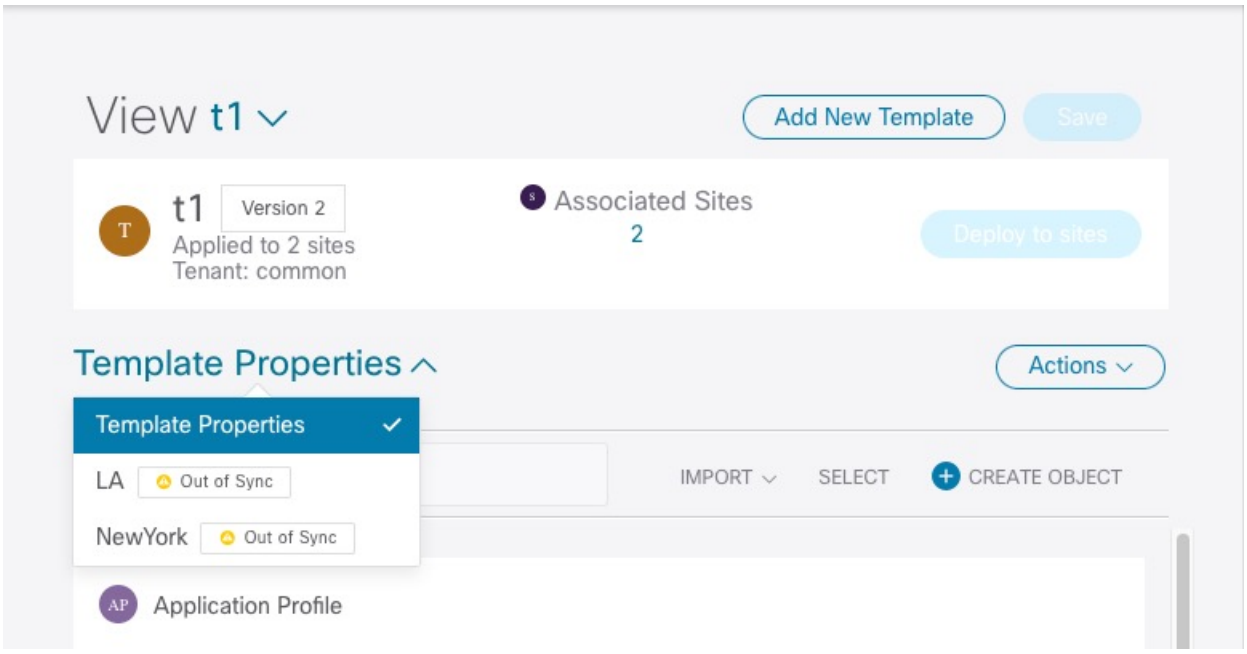
（注）
設定の復元プロセス中に複数のサービスが再起動されます。その結果、復元された設定がNDO GUIに正しく反映されるまでに最大 10 分の遅延が発生することがあります。

ステップ 6 テンプレートに構成のばらつきがあるかどうかを確認してください。

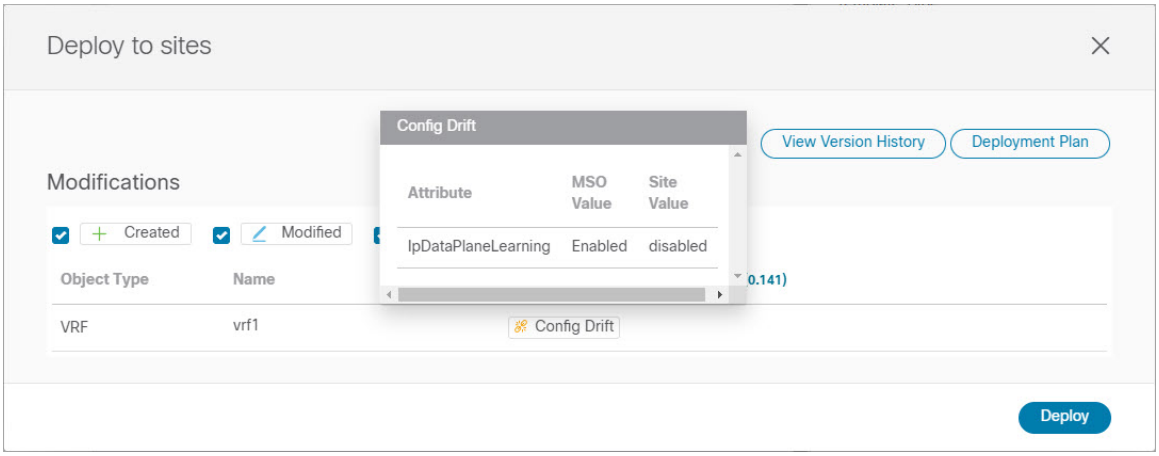
展開のスキーマとテンプレートごとに次の手順を繰り返します

次の 2 つの方法のいずれかで、構成のばらつきをチェックできます。

- テンプレートが割り当てられている各サイトのテンプレート展開ステータスアイコンを確認します。



- テンプレートを選択して **[サイトへの展開 (Deploy to sites)]** をクリックして、構成のばらつきが含まれているオブジェクトをチェックするために、構成比較画面を呼び出します。



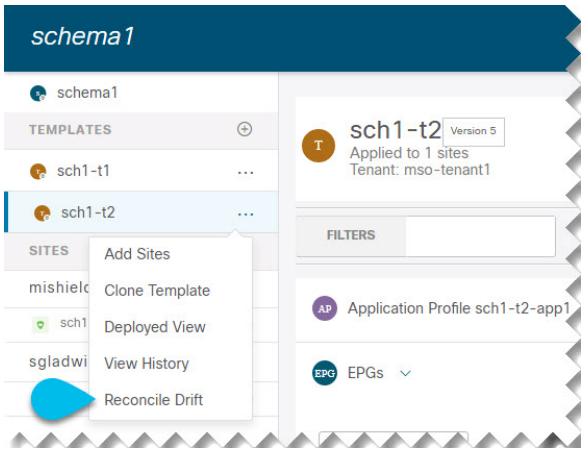
ステップ 7 テンプレートのどれかに構成のばらつきが含まれている場合は、競合を解決します。

構成のばらつきの詳細については、『*Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics*』の「構成のばらつき」の詳細を確認してください。

a) テンプレート展開ダイアログを閉じて、スキーマ表示に戻ります。

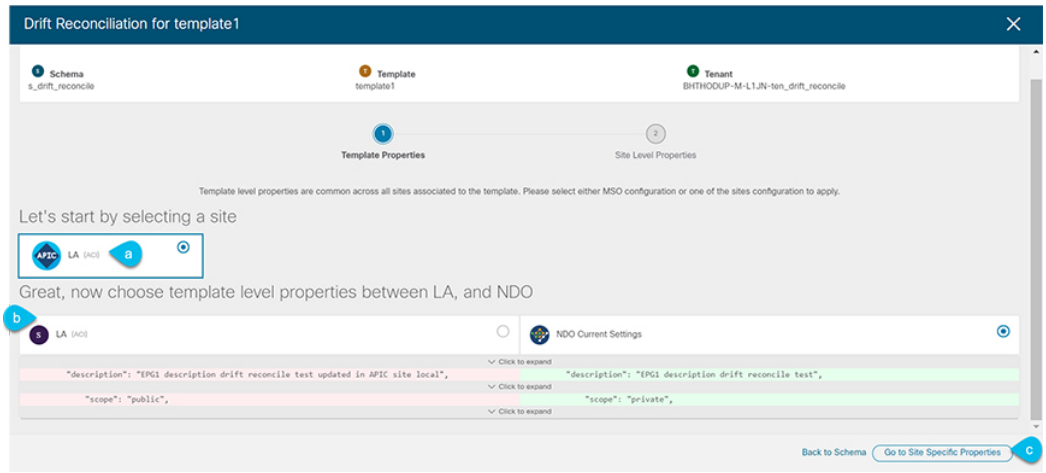
この時点でテンプレートを展開すると、Orchestrator データベースの値をプッシュして、ファブリックの既存の設定を上書きします。

b) テンプレートの **[アクション (Actions)]** メニューから、**[ばらつきの調整 (Reconcile Drift)]** を選択します。



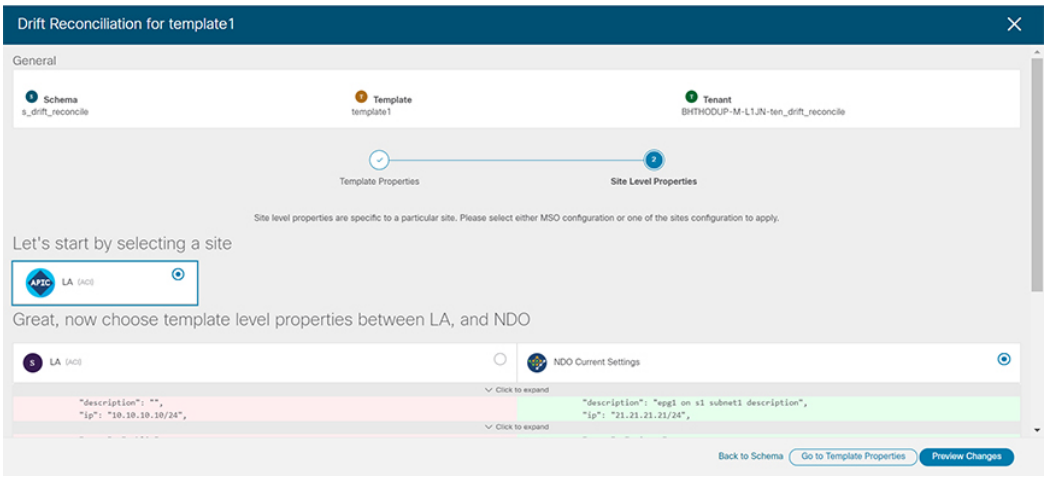
[ばらつきの調整 (Reconcile Drift)] ウィザードが開きます。

c) **[ばらつきの調整 (Reconcile Drift)]** 画面で、各サイトのテンプレートレベルの構成を比較し、希望のものを選択します。



テンプレートレベルのプロパティは、テンプレートに関連付けられているすべてのサイトに共通です。Nexus Dashboard Orchestrator で定義されたテンプレート レベルのプロパティを各サイトでレンダリングされた構成と比較し、Nexus Dashboard Orchestrator テンプレートの新しい構成を決定できます。サイト構成の選択は、既存の Nexus Dashboard Orchestrator テンプレートのこれらのプロパティを変更し、その場合、Nexus Dashboard Orchestrator の構成を選択すると、既存の Nexus Dashboard Orchestrator テンプレートの設定はそのまま残されます

d) **[サイト特有のプロパティに移動（Go to Site Specific Properties）]** をクリックして、サイトレベルの構成に切り替えます。



特定のサイトの構成を比較するために、サイトを選択できます。テンプレートレベルの設定とは異なり、各サイトのNexus Dashboard Orchestrator定義または実際の既存の設定を個別に選択して、そのサイトのテンプレートのサイトローカル プロパティとして保持できます。

ほとんどのシナリオでは、テンプレートレベルとサイトレベルの両方の構成で同じ選択を行いたとしても、ばらつきの調整ウィザードでは、サイトのコントローラで「テンプレートのプロパティ」レベルで定義された構成とNexus Dashboard Orchestratorで定義された構成またはその逆を選択できます。

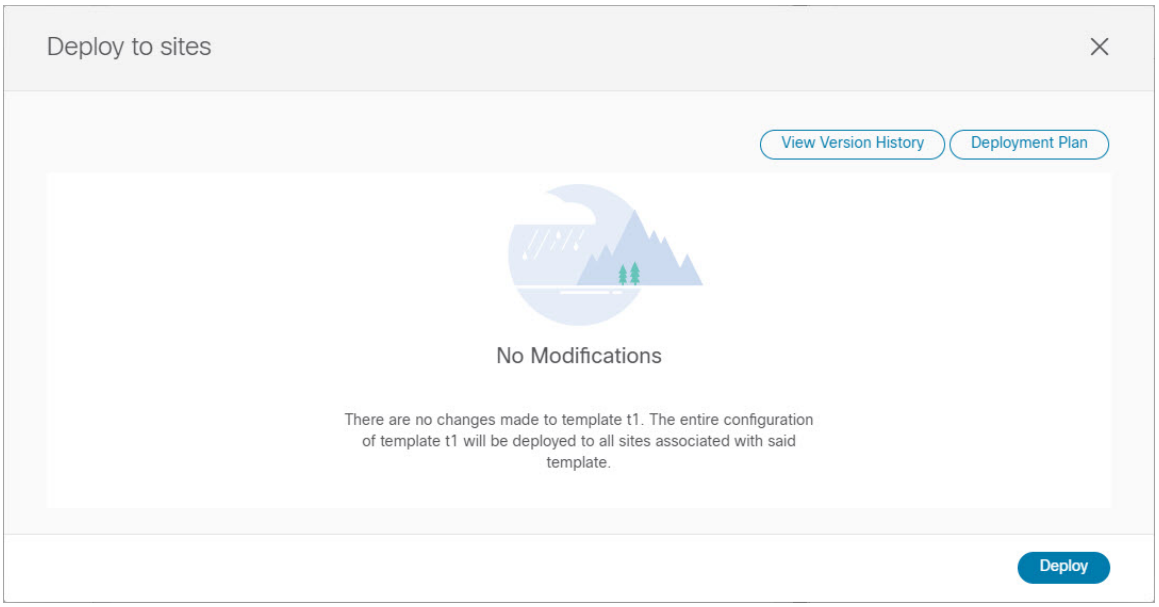
e) **[変更のプレビュー（Preview Changes）]** をクリックして、選択内容を確認します。

プレビューは**[ばらつきの調整 (Reconcile Drift)]** ウィザードの選択肢に基づいて調整された完全なテンプレート構成を表示します。その後、**[サイトに展開（Deploy to site）]** をクリックして構成を展開し、そのテンプレートのばらつきを調整できます。

ステップ 8 すべての構成のばらつきを解決した後で、**[サイトへの展開（Deploy to sites）]** ダイアログに変更が表示されていない場合、テンプレートの完全な再展開を実行します。

（注）
リリース3.7(1)のデータベース変換のため、各テンプレートの完全な再展開を実行する必要があります。

[サイトへの展開（Deploy to sites）] ダイアログに、次の図で表示される変更が含まれない場合、**[展開（Deploy）]** をクリックして、完全な構成を再展開します。



ステップ 9 Nexus Dashboard Orchestrator で各スキーマとテンプレートに対して上記の手順を繰り返します。

ステップ 10 監査ログをチェックして、すべてのテンプレートが再展開されていることを確認します。

[オペレーション（Operations）]タブの監査ログを表示できます。

[監査ログ（Audit Logs）]ページで、すべてのテンプレートが `[再展開済み（Redeployed）]` と表示され、完全な再展開が正常に完了したことを確認します。

バックアップのエクスポート（ダウンロード）

ここでは、Nexus Dashboard Orchestrator からバックアップをダウンロードする方法について説明します。

始める前に

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション メニューで、**[操作 (Operations)]** > **[バックアップと復元 (Backups & Restore)]**を選択します。

ステップ 3 メイン ウィンドウで、ダウンロードするバックアップの隣のアクション (...) アイコンをクリックし、**[ダウンロード (Download)]**を選択します。

これにより msc-backups-<タイムスタンプ>.tar.gz 形式でシステムにバックアップ ファイルがをダウンロードされます。その後、ファイルを抽出してその内容を表示することができます。

バックアップをリモートロケーションへインポートする

ここでは、以前にダウンロードした既存の設定バックアップをアップロードし、Nexus Dashboard Orchestratorで設定されたリモートロケーションのいずれかにインポートする方法について説明します

始める前に

次の設定が済んでいる必要があります。

- バックアップの作成 （120ページ） およびバックアップのエクスポート（ダウンロード）（126 ページ） の説明に従って、設定のバックアップを作成されていること。

  リリース3.4(1)以降で作成したバックアップなど、バックアップがすでにリモート ロケーションにある場合は、ローカル マシンにダウンロードして、別のリモート ロケーションにアップロードできます。

- バックアップのリモート ロケーションの設定 （119ページ） の説明に従って、バックアップのためのリモート ロケーションが追加されていること。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション ペインで、**[操作 (Operations)]** > **[バックアップと復元 (Backups & Restore)]**を選択します。

ステップ 3 メインペインで、**[アップロード (Upload)]** をクリックします。

ステップ 4 開いた **[ファイルからのアップロード (Upload from file)]** ウィンドウで、**[ファイルを選択 (Select File)]** を選択して、インポートするバックアップ ファイルを選択します。

バックアップをアップロードすると、**[バックアップ (Backups)]**ページに表示されるバックアップのリストに追加されます。

ステップ 5 **[リモート ロケーション (Remote location)]** ドロップダウンメニューから、リモート ロケーションを選択します。

ステップ 6 (オプション) リモート ロケーションのパスを更新します。

リモート バックアップのロケーションを作成するときに設定したリモート サーバ上のターゲット ディレクトリが、**[リモート パス (Remote Path)]** フィールドに表示されます。

パスにはサブディレクトリを追加することができます。ただし、ディレクトリはデフォルトの設定済みパスの下にある必要があり、すでにリモート サーバで作成されている必要があります。

ステップ 7 **[アップロード (Upload)]** をクリックしてファイルをインポートします。

バックアップのインポートは、[**バックアップ (Backups)**]ページに表示されたバックアップのリストにそれを追加します。

バックアップは NDO UI に表示されますが、リモート サーバーにのみ存在することに注意してください。

バックアップ スケジューラ

ここでは、定期的に完全な設定バックアップを実行するバックアップスケジューラを有効または無効にする方法について説明します。

始める前に

バックアップのリモート ロケーションの設定（119ページ） の説明に従って、バックアップのためのリモート ロケーションを追加してある必要があります。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション メニューで、**[操作 (Operations)]** > **[バックアップと復元 (Backups & Restore)]**を選択します。

ステップ 3 メイン ペインの右上にある **[スケジューラ (Scheduler)]** をクリックします。

[バックアップ スケジューラ設定 (Backup Scheduler Settings)] ウィンドウが開きます。

ステップ 4 バックアップ スケジューラをセットアップします。

a) **[スケジューラの有効化 (Enable Scheduler)]** チェックボックスをオンにします。

b) **[開始日の選択 (Select Start Date)]** フィールドに、スケジューラを開始する日を指定します。

c) **[時間の選択 (Select Time)]** フィールドに、スケジューラを開始する時刻を入力します。

d) **[頻度の選択 (Select Frequency)]** ドロップダウンから、バックアップを実行する頻度を選択します。

e) **[リモート ロケーション (Remote Location)]** ドロップダウンから、バックアップを保存する場所を選択します。

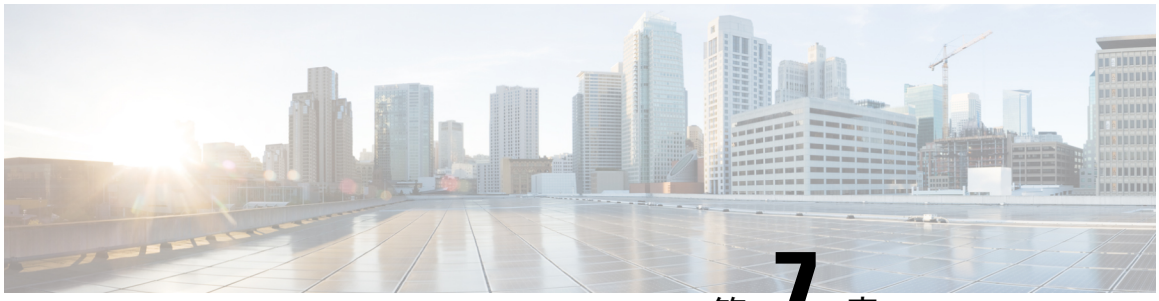
f) （オプション）**[リモート パス (Remote Path)]** フィールドで、バックアップが保存されるリモート ロケーションのパスを更新します。

リモートバックアップのロケーションを作成するときに設定したリモートサーバ上のターゲットディレクトリが、**[リモート パス (Remote Path)]** フィールドに表示されます。

パスにはサブディレクトリを追加することができます。ただし、ディレクトリはデフォルトの設定済みパスの下にある必要があり、すでにリモート サーバで作成されている必要があります。

g) [OK] をクリックして終了します。

ステップ 5 バックアップ スケジューラを無効にする場合は、上記の手順で**[スケジューラの有効化 (Enable Scheduler)]** チェックボックスをオフにします。



第 7 章

サイトのアップグレード

概要

（注） この機能は、Cisco APIC サイトでのみサポートされます。Cisco クラウド ネットワーク コントローラ または Cisco NDFC ファブリックではサポートされていません。

リリース 3.1(1) よりも前は、Cisco Multi-Site を導入する際に、各サイトの APIC クラスタおよびスイッチ ノード ソフトウェアをサイト レベルで個別に管理する必要がありました。Multi-Site ドメイン内のサイトの数が増えると、リリースのライフサイクルとアップグレードは、リリースと機能の互換性のために手動で調整および管理する必要があるため、複雑になる可能性があります。

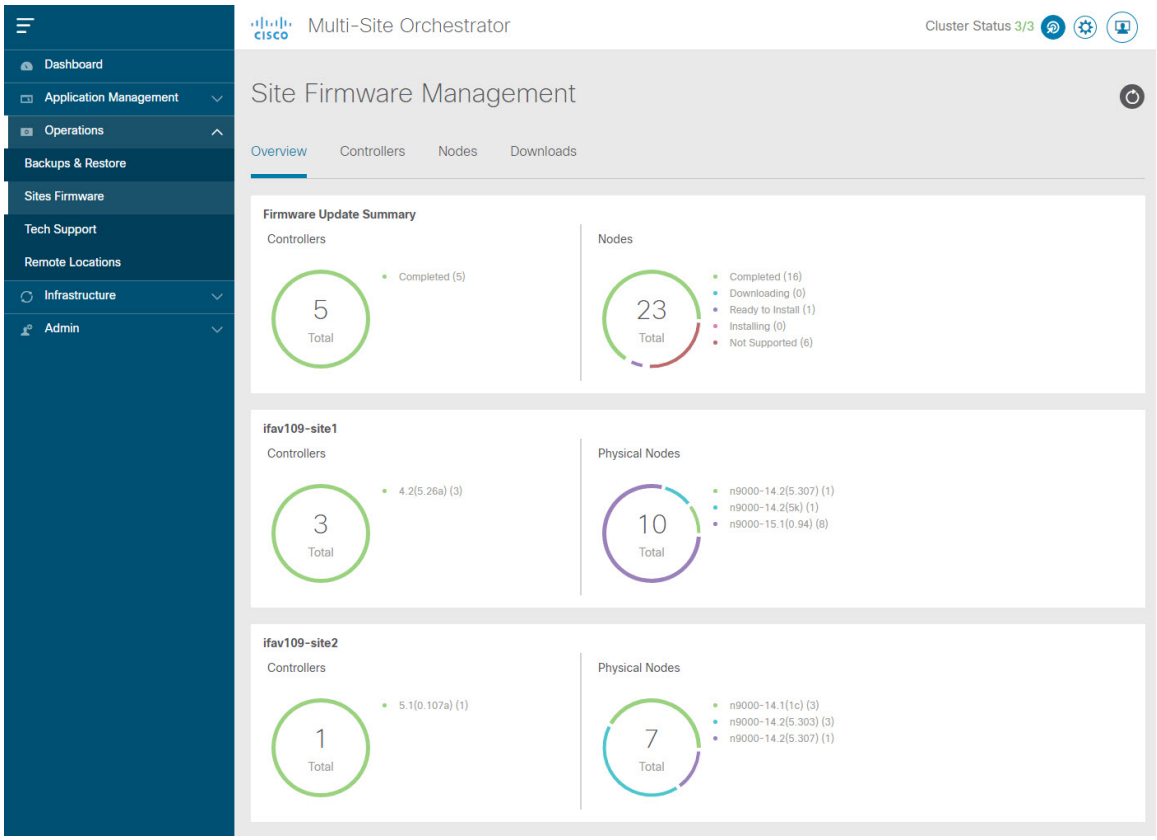
リリース 3.1(1) 以降、Cisco Nexus Dashboard Orchestrator は、すべてのサイトのソフトウェア アップグレードを単一のポイントから管理できるワークフローを提供します。複数のサイト管理者がソフトウェア アップグレードを手動で調整する必要がなく、アップグレードに影響する可能性のある、潜在的な問題を把握できます。

[操作 (Operations)] > **[サイトのファームウェア (Sites Firmware)]**に移動して、サイトのアップグレード画面にアクセスできます。このページには4つのタブがあります。このセクションと次のセクションで説明します。

[概要 (Overview)] タブには、Multi-Site ドメイン内のサイトと、展開されている、または展開の準備ができているファームウェア バージョンに関する情報が表示されます。[サイト ファームウェア (Sites Firmware)] サービスは、5 分ごとにサイトをポーリングして、アップグレード ポリシーの最新のステータスなどの新しいデータまたは変更されたデータを探します。メイン

ペインの右上隅にある **[更新 (Refresh)]** ボタンをクリックすると、手動で更新をトリガーできます。

図 7: サイトのファームウェアの概要



ページは次の 3 つの領域に分かれています。

- **[ファームウェア アップデートの概要 (Firmware Update Summary)]**：Cisco APICおよびスイッチ ファームウェアを含む、Multi-Site ドメイン内のすべてのサイトに存在するファームウェア イメージの全体的な概要を提供します。

  イメージのタイプごとに、各状態のイメージ数を含む、固有の情報が表示されます。

  - [完了 (Completed)]：イメージは現在、コントローラまたはスイッチに展開されています。
  - [ダウンロード中 (Downloading)]（スイッチノードのみ）：イメージはスイッチ ノードにダウンロード中です。
  - [インストールの準備完了 (Ready to Install)]（スイッチノードのみ）：イメージはスイッチノードに正常にダウンロードされ、インストールの準備ができています。
  - [インストール (Installing)]：コントローラまたはスイッチノードに現在イメージを展開中です。

- [未サポート (Not Supported)]：リリース 4.2(5) より前のリリースなど、リモート ファームウェア アップグレードをサポートしていないイメージ。

- **[サイト固有の情報 (Site-specific information)]**：ページの追加のセクションには、個々のサイトに関する情報が表示されます。これには、現在展開されているソフトウェアのバージョンと、コントローラまたはノードの数が含まれます。

注意事項と制約事項

Nexus Dashboard Orchestrator からファブリック アップグレードを実行する場合、次の制限が適用されます。

- 「Upgrade and Downgrading the Cisco APIC and Switch Software」（『*Cisco APIC Installation、Upgrade、and Downgrade Guide*』）に記載されている Cisco APIC アップグレード プロセスに固有のガイドライン、推奨事項、および制限事項を確認し、それに従う必要があります。

- Nexus Dashboard Orchestrator を Cisco Nexus Dashboard に展開する必要があります。

  サイトのアップグレード機能は、VMware ESXのNDO導入では使用できません。また、『*Cisco APIC Installation、Upgrade、and Downgrade Guide*』に記載されている標準のアップグレード手順に従う必要があります。

- ファブリックは、Cisco APIC リリース 4.2(5) 以降を実行している必要があります。

  以前の APIC リリースを実行しているファブリックは、アップグレード ワークフロー中に選択できません。『*Cisco APIC Installation、Upgrade、and Downgrade Guide*』に記載されている標準のアップグレード手順に従います。

- サイトのアップグレードは、これらのファブリックを管理するサイト管理者と調整することを推奨します。潜在的な問題が発生した場合は、トラブルシューティングのためにコントローラまたはスイッチ ノードにアクセスする必要があります。

- アップグレード プロセスの途中でファブリック スイッチ ノードが非アクティブ状態になった場合（たとえば、ハードウェアまたは電源障害）、プロセスは完了できません。この間、ノード アップグレード ポリシーを削除または変更することはできません。これは、NDO がノードがダウンしたか、または単にアップグレードのリブート中かを区別できないためです。

  この問題を解決するには、非アクティブ ノードを APIC から手動でデコミッションする必要があります。この時点で、NDO アップグレードポリシーは変更を認識し、失敗ステータスを返します。その後、NDO のアップグレード ポリシーを更新してスイッチを削除し、アップグレードを再実行できます。

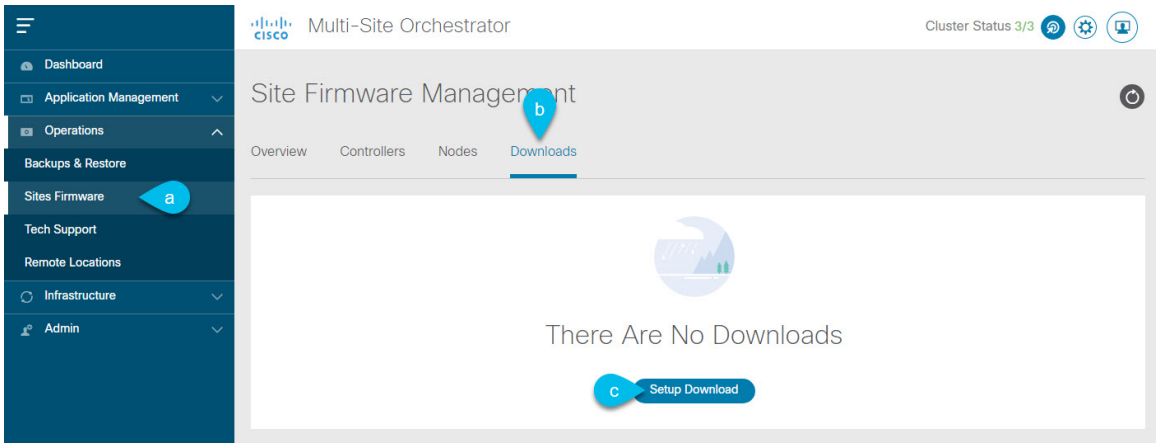
コントローラとスイッチノードのファームウェアをサイトにダウンロードする

アップグレードを実行する前に、コントローラとスイッチ ソフトウェアをファブリック内のすべてのサイト コントローラにダウンロードする必要があります。次の手順を完了すると、後ほど、ダウンロードしたイメージを使用してアップグレード プロセスを開始できます。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 ファームウェア ダウンロードをセットアップします。



a) 左側のナビゲーション ペインで**[操作 (Operations)]** > **[サイト ファームウェア (Sites Firmware)]**を選択します。

b) メインウィンドウで **[ダウンロード (Downloads)]** タブを選択します。

c) **[ダウンロードのセットアップ (Setup Downloads)]** タブをクリックします。

以前に 1 つ以上ダウンロードをセットアップしていた場合は、代わりに、メインペインの右上にある **[ダウンロードのセットアップ (Setup Downloads)]** ボタンをクリックします。

[イメージを APIC へダウンロード (Download Image to APIC)] 画面が表示されます。

ステップ 3 サイトを選択します。

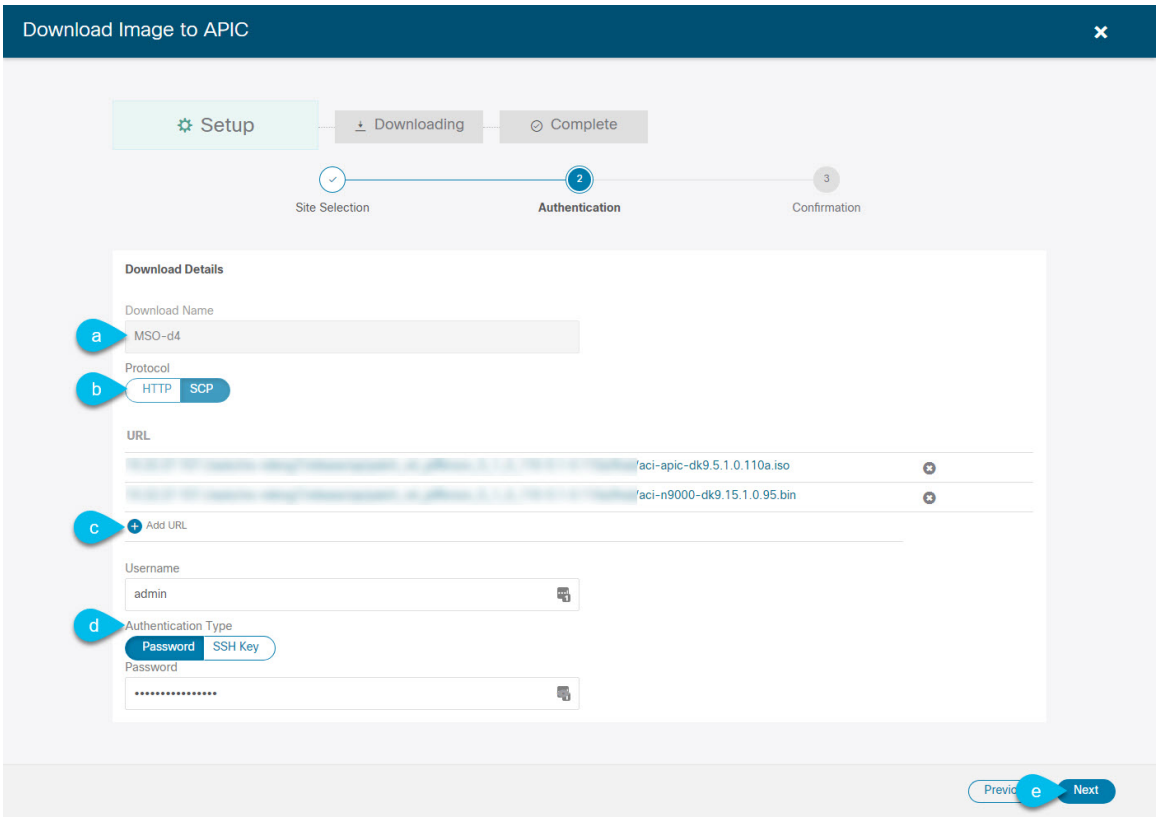
ここで選択したすべてのサイトの Cisco APIC にイメージがダウンロードされます。

a) **[サイトの選択 (Select Sites)]** をクリックします。

b) **[サイトの選択 (Select Sites)]** ウィンドウで、1 つ以上のサイトをオンにし、**[追加して閉じる (Add and Close)]** をクリックします。

c) [次へ（Next）] をクリックして続行します。

ステップ 4 詳細を入力します。



a) **[名前 (Name)]** を入力します。

ダウンロードを追跡するためのわかりやすい名前を指定します。

b) プロトコルを選択します。

HTTP または SCP 経由でイメージをダウンロードすることを選択できます。

c) **[+ URLの追加 (+ Add URL)]** をクリックして、イメージの場所を指定します。

APIC とスイッチ ファームウェア イメージの両方を提供できます。

d) **SCP** を選択した場合は、認証情報を入力します。

ログインする **[ユーザ名 (Username)]**（admin など）を入力する必要があります。

[認証タイプ (Authentication Type)] を選択します。

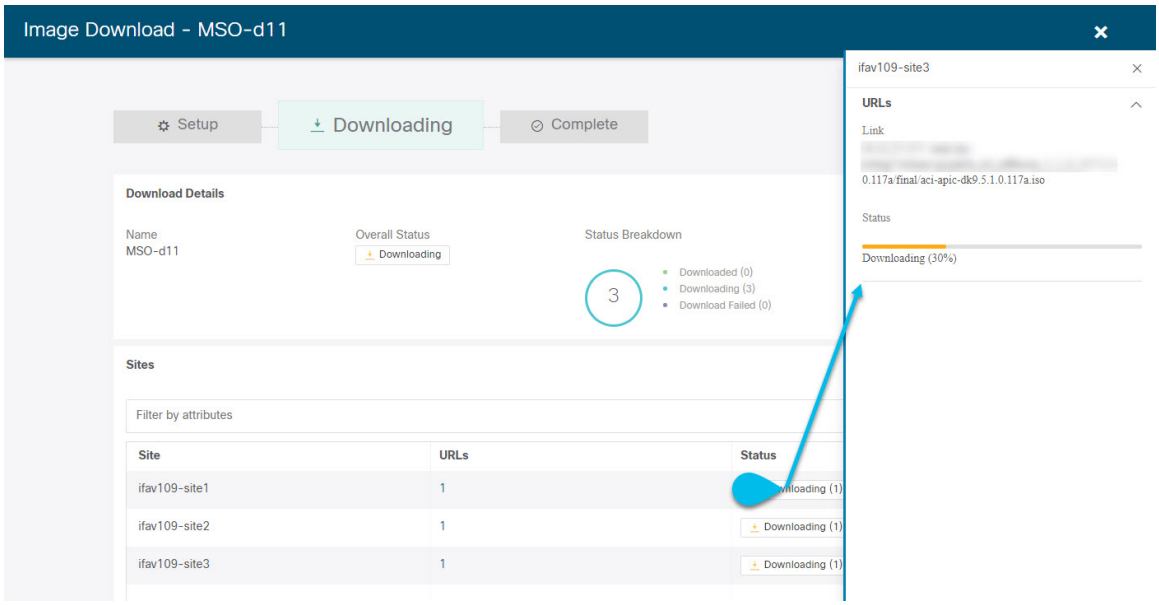
- **パスワード認証**の場合は、前に指定したユーザ名のパスワードを入力します。
- **SSH キー**認証の場合は、**SSH キー**と **SSH キー パスフレーズ**を入力する必要があります。

e) [次へ（Next）] をクリックして続行します。

ステップ 5 確認画面で情報を確認し、[送信（Submit）]をクリックして続行します。

表示される **[ダウンロード中 (Downloading)]** 画面で、イメージのダウンロードのステータスを確認できます。

ステータスをクリックして、進行状況の詳細を表示することもできます。



すべてのダウンロードが完了すると、**[完了 (Completed)]** 画面に移行します。**[ダウンロード (Downloading)]** 画面で待機する必要はありません。前の手順で指定したダウンロード名をクリックすると、**[ダウンロード (Downloads)]** タブからいつでも戻ることができます。

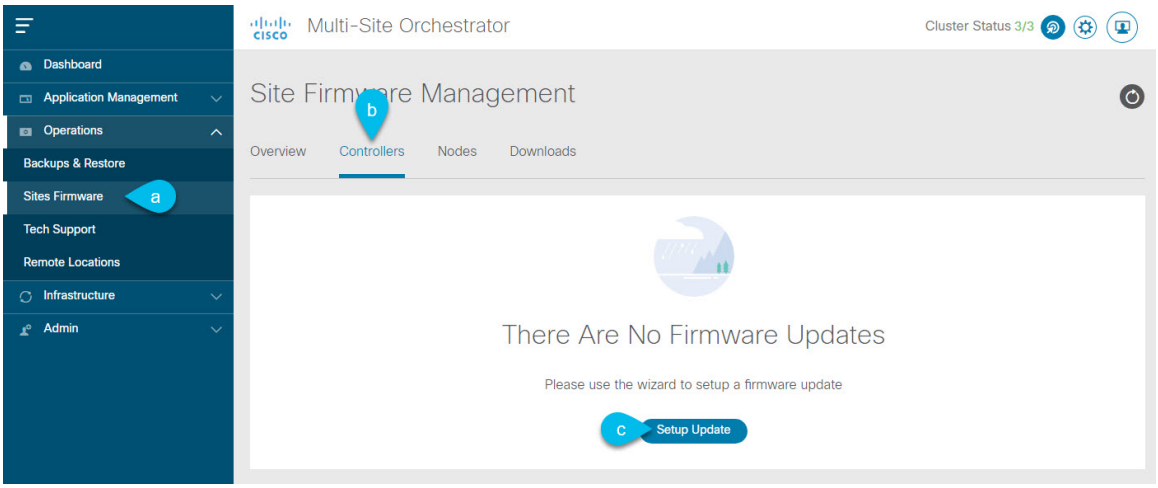
コントローラのアップグレード

ここでは、サイトの APIC クラスタのソフトウェア アップグレードを設定する方法について説明します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 APIC クラスタのアップグレードをセットアップします。



a) 左側のナビゲーション ペインで**[操作 (Operations)]** > **[サイト ファームウェア (Sites Firmware)]**を選択します。

b) メインウィンドウで **[コントローラ (Controllers)]** タブを選択します。

c) **[更新のセットアップ (Setup Update)]** をクリックします。

以前に1つ以上の更新を設定している場合は、代わりにメインペインの右上にある **[更新のセットアップ (Setup Update)]** ボタンをクリックします。

[サイト ファームウェアの更新のセットアップ（Setup Site Firmware Update ）] 画面が開きます。

ステップ 3 アップグレードの詳細を入力します。

a) **[名前 (Name)]** を入力します。

これは、いつでもアップグレードの進行状況を追跡するために使用できる、コントローラのアップグレード ポリシー名です。

b) **[サイトの選択 (Select Sites)]** をクリックします。

[サイトの選択 (Select Sites)] ウィンドウが表示されます。

c) **[サイトの選択 (Select Sites)]** ウィンドウで、1 つ以上のサイトをオンにし、**[追加して閉じる (Add and Close)]** をクリックします。

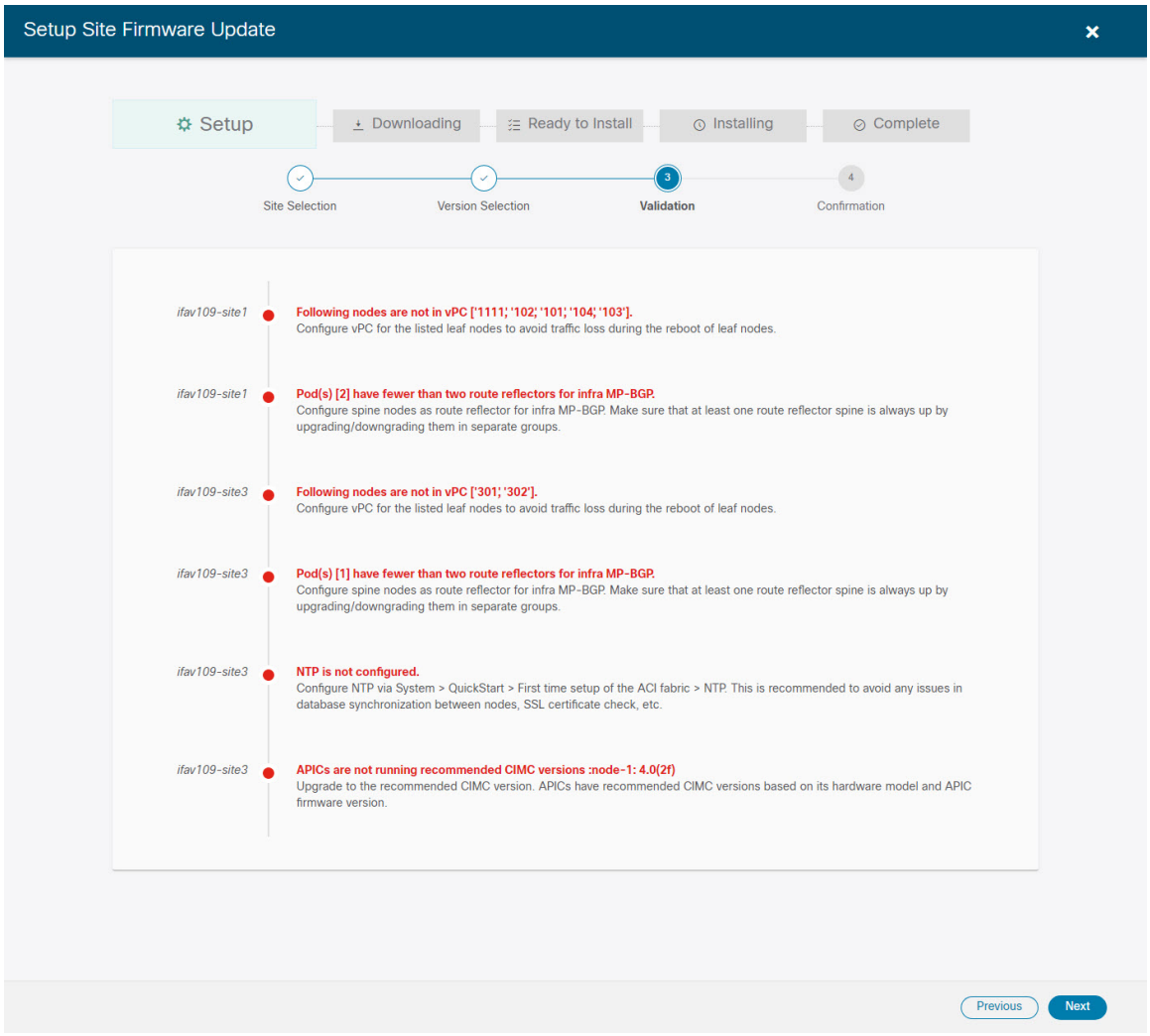
d) [次へ（Next）] をクリックして続行します。

ステップ 4 **[バージョンの選択 (Version Selection)]** 画面で、アップロードしたファームウェア バージョンを選択し、**[次へ (Next)]** をクリックします。

ここで使用可能にするためには、ファームウェアをサイトにダウンロードする必要があります。前のセクションで設定したダウンロードが正常に完了したものの、ここでイメージを使用できない場合は、**[ファームウェアの更新のセットアップ (Setup Site Firmware Update)]** 画面を閉じ、**[操作 (Operations)]** > **[サイトのファームウェア (Sites Firmware)]** > **[コントローラ (Controllers)]**タブに戻り、**[更新 (Refresh)]** ボタンをクリックして、使用可能な最新情報をリロードします。それからサイトのアップグレード手順をもう一度開始します。

ステップ 5 **[確認 (Validation)]** 画面で情報を確認し、**[次へ (Next)]** をクリックします。

障害がないことを確認し、アップグレードに影響する可能性がある追加情報を確認します。



ステップ 6 **[確認 (Confirmation)]** 画面で情報を確認し、**[送信 (Submit)]** をクリックしてアップグレードを開始します。

ステップ 7 **[インストールの準備完了 (Ready to Install)]**画面で、**[インストール (Install)]** をクリックします。

アップグレード プロセス中に NDO からサイトへの接続が失われると、GUI には、接続が失われる前の、アップグレードの最新の既知ステータスが表示されます。接続が再確立されると、アップグレードのステータスが更新されます。接続が失われた後、メインペインの右上にある **[更新 (Refresh)]** ボタンをクリックすると、手動で更新できます。

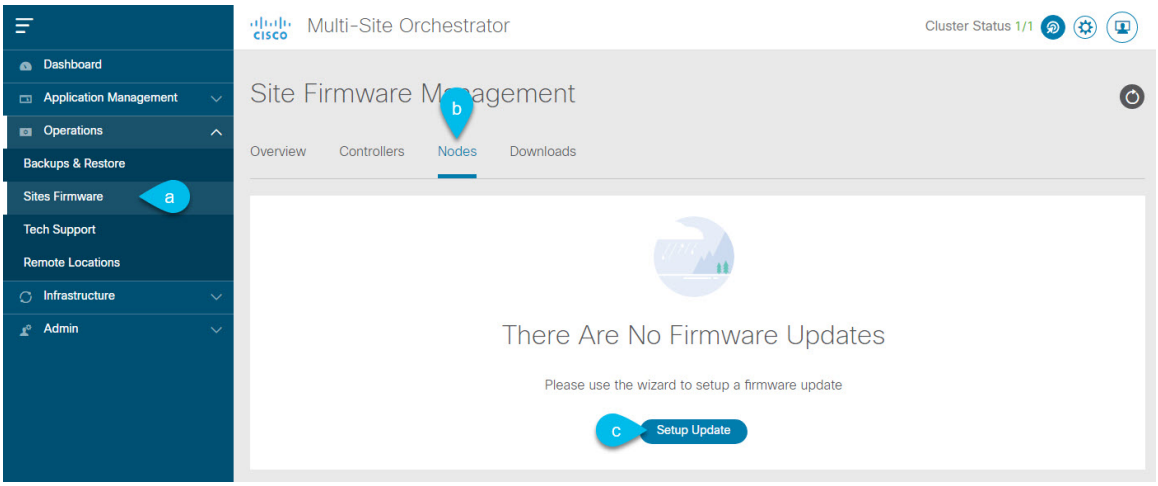
ノードのアップグレード

ここでは、サイトのスイッチ ノードのソフトウェア アップグレードを設定する方法について説明します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 スイッチ ノードのアップグレードをセットアップします。



a) 左側のナビゲーション ペインで**[操作 (Operations)]** > **[サイト ファームウェア (Sites Firmware)]**を選択します。

b) メイン ウィンドウで **[ノード (Node)]** タブを選択します。

c) **[更新のセットアップ (Setup Update)]** をクリックします。

以前に1つ以上の更新を設定している場合は、代わりにメインペインの右上にある **[更新のセットアップ (Setup Update)]** ボタンをクリックします。

[ノード ファームウェアの更新のセットアップ（Setup Node Firmware Update ）] 画面が開きます。

ステップ 3 アップグレードの詳細を入力します。

a) **[名前 (Name)]** を入力します。

これは、いつでもアップグレードの進行状況を追跡するために使用できるアップグレードポリシー名です。

b) **[ノードの選択 (Select Nodes)]** をクリックします。

[ノードの選択 (Select Nodes)] ウィンドウが表示されます。

c) サイトを選択し、そのサイトのスイッチノードを選択して、**[追加して閉じる (Add and Close)]** をクリックします。

一度に1つのサイトからスイッチノードを追加できます。他のサイトからスイッチを追加する場合は、この手順を繰り返します。

d) 他のサイトのノードについて、前のサブステップを繰り返します。

e) [次へ（Next）] をクリックして続行します。

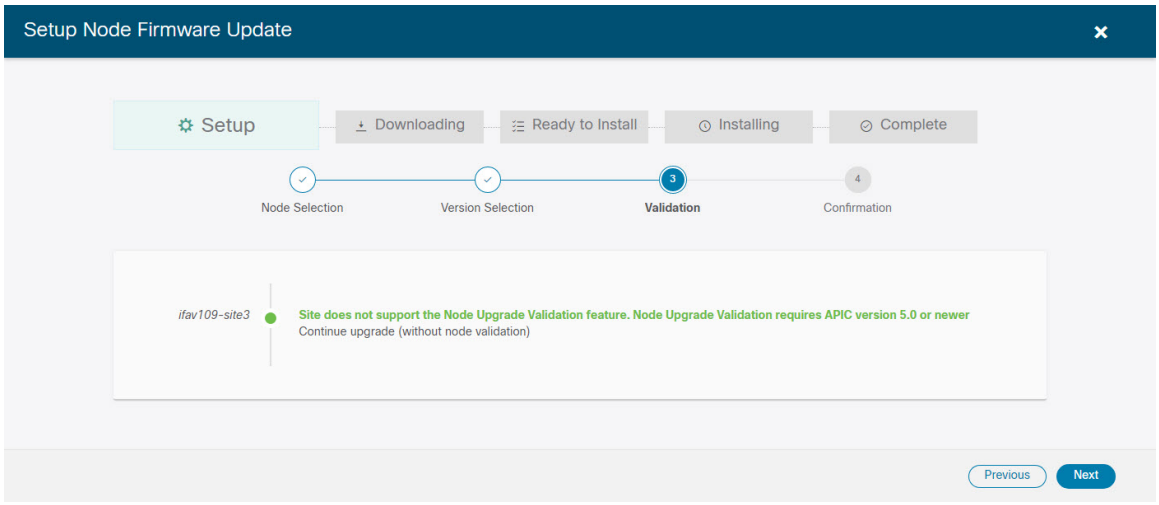
ステップ 4 **[バージョンの選択 (Version Selection)]** 画面で、アップロードしたファームウェア バージョンを選択し、**[次へ (Next)]** をクリックします。

ここで使用可能にするためには、ファームウェアをサイトにダウンロードする必要があります。前のセクションで設定したダウンロードが正常に完了したものの、ここでイメージを使用できない場合は、**[ファームウェアの更新のセットアップ (Setup Site Firmware Update)]** 画面を閉じ、**[操作 (Operations)]** > **[サイトのファームウェア (Sites Firmware)]** > **[ノード (Nodes)]**タブに戻り、**[更新 (Refresh)]** ボタンをクリックして、使用可能な最新情報をリロードします。それからサイトのアップグレード手順をもう一度開始します。

ステップ 5 **[検証 (Validation)]** 画面で、障害が発生していないことを確認し、**[次へ (Next)]** をクリックします。

障害がないことを確認し、アップグレードに影響する可能性がある追加情報を確認します。

（注）
リリース 5.0(1) より前のリリースを実行しているサイトはノード検証をサポートしていないため、NDO からのアップグレードを開始する前に、サイトの APIC でスイッチ ノードの障害をチェックすることを推奨します。



ステップ 6 **[確認 (Confirmation)]** 画面で情報を確認し、**[送信 (Submit)]** をクリックして続行します。

これにより、選択したすべてのノードにイメージが事前にダウンロードされます。ダウンロードが完了すると、画面が **[インストール準備完了 (Ready to Install)]** に遷移し、次の手順に進むことができます。

ステップ 7 （オプション）**[詳細設定 (Advanced Settings)]**を変更します。

（注）
詳細オプションを変更する前に、 Upgrade and Downgrading the Cisco APIC and Switch Software（*Cisco APIC Installation*、*Upgrade*、*and Downgrade Guide*）で説明されているCisco APICアップグレードプロセスのガイドライン、推奨事項、および制限事項を確認してください。

[インストールの準備完了 (Ready to Install)]画面で、**[詳細設定 (Advanced Settings)]**メニューを開いて追加のオプションを表示できます。

- **[互換性チェックを無視 (Ignore Compatibility Check)]**：デフォルトでは、このオプションは[いいえ (No)]に設定され、互換性チェックが有効になっています。システムの現在実行中のバージョンから指定された新しいバージョンへのアップグレードパスがサポートされているかどうかが確認されます。

  [互換性チェックを無視 (Ignore Compatibility Check)] フィールドで [はい (Yes)] にして互換性チェック機能を無効にした場合、システムでサポートされていないアップグレードが実行されるリスクがあり、システムが利用できない状態になる可能性があります。

- **[グレースフル チェック (Graceful Check)]**：デフォルトでは、このオプションは [いいえ (No)] に設定されています。アップグレードプロセスでのアップグレード実行前には、どのスイッチもグレースフル挿入/取り外し（GIR）モードになりません。

  このオプションを有効にすると、アップグレードの実行中にノードをグレースフルに（GIRを使用して）ダウンさせることができ、アップグレードによるトラフィック損失が減少します。

- **[実行モード (Run Mode)]**：デフォルトでは、このオプションは [失敗時に続行 (Continue on Failure)] に設定されており、ノードのアップグレードが失敗すると、次のノードに進みます。または、このオプションを [失敗時に一時停止 (Pause on Failure)]に設定すると、いずれかのノードのアップグレードが失敗した場合にアップグレード プロセスを停止できます。

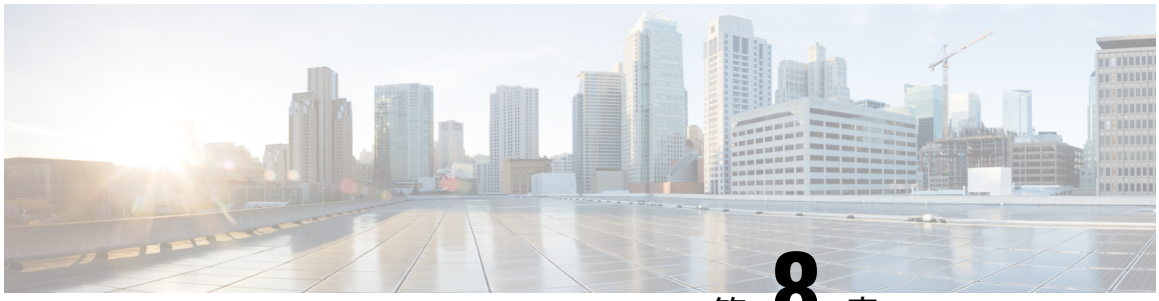
ステップ 8 [Failed] とマークされたノードをアップグレードから削除します。

アップグレードポリシーに、ファームウェアのダウンロードに失敗した 1 つ以上のノードが含まれている場合、アップグレードを続行できません。[失敗 (Failed)] ステータスにカーソルを合わせると、詳細情報と失敗の理由が表示されます。

アップグレードからノードを削除するには、**[アップデートの詳細を編集 (Edit Update Details)]** のリンク（**[インストールの準備完了 (Ready to Install)]** 画面）をクリックします。

ステップ 9 **[インストール (Install)]** をクリックしてアップグレードを開始します。

アップグレード プロセス中に NDO からサイトへの接続が失われると、GUI には、接続が失われる前の、アップグレードの最新の既知ステータスが表示されます。接続が再確立されると、アップグレードのステータスが更新されます。接続が失われた後、メインペインの右上にある **[更新 (Refresh)]** ボタンをクリックすると、手動で更新できます。



第 8 章

[Tech Support]

テクニカル サポートおよびシステム ログ

Nexus Dashboard Orchestrator のシステム ロギングは、最初に Orchestrator クラスタをデプロイしたときに自動的に有効になり、環境内で発生したイベントと障害をキャプチャします。

追加のツールを使用して重要なイベントを遅延なく迅速に解析、表示、応答する必要がある場合は、いつでも、ログをダウンロードするか、Splunk などの外部ログ アナライザにストリーミングするかを選択できます。

リリース 3.3(1) 以降、テクニカル サポートログは 2 つの部分に分割されています。

- 以前のリリースと同じ情報を含む、オリジナルのデータベース バックアップ ファイル
- 可読性を高めた、JSON ベースのデータベース バックアップ

各バックアップ アーカイブには、次の内容が含まれています。

- *xxxx*：バックアップ時に使用可能なコンテナ ログ用の *xxxx* 形式の 1 つ以上のファイル。
- `msc-backup-<date>_temp`：以前のリリースと同じ情報を含む、オリジナルのデータベース バックアップ。
- `msc-db-json-<date>_temp`：JSON 形式のバックアップコンテンツ。

  例：

```
msc_anpEpgRels.json
msc_anpExtEpgRels.json
msc_asyncExecutionStatus.json
msc_audit.json
msc_backup-versions.json
msc_backupRecords.json
msc_ca-cert.json
msc_cloudSecStatus.json
msc_consistency.json
...
```

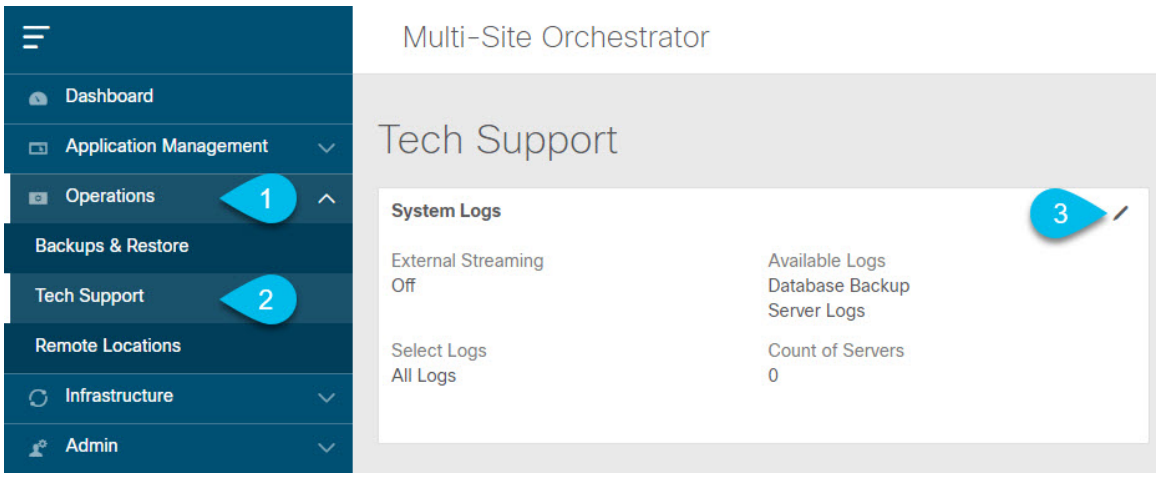
システム ログのダウンロード

このセクションでは、Nexus Dashboard Orchestrator により管理されているすべてのスキーマ、サイト、テナント、およびユーザのトラブルシューティング レポートとインフラストラクチャ ログ ファイルを生成します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 **[システムログ (System Logs)]** 画面を開きます。



a) メインメニューで、**[操作 (Operations)]** > **[テクニカル サポート (Tech Support)]**を選択します。

b) **[システム ログ (System Logs)]** フレームの右上隅にある編集ボタンをクリックします。

ステップ 3 **[ログのダウンロード (Download Log)]** ボタンをクリックしてログをダウンロードします。

アーカイブがシステムにダウンロードされます。この章の最初のセクションで説明されているすべての情報を含んでいます。

外部アナライザへのストリーミング システム ログ

Nexus Dashboard Orchestrator を使用すると、Orchestrator ログを外部のログアナライザー ツールにリアルタイムで送信できます。生成されたイベントをストリーミングすることにより、追加のツールを使用して、遅延なしで重要なイベントをすばやく解析、表示、および対応できます。

ここでは、Nexus Dashboard Orchestrator が外部アナライザツール (Splunk や syslog など) にログをストリーミングできるようにする方法について説明します。

始める前に

- このリリースでは、外部ログ アナライザーとして Splunk と `syslog` のみがサポートされています。
- このリリースの、Nexus Dashboard 展開での Cisco Nexus Dashboard Orchestrator 向けには、`syslog` のみがサポートされています。
- このリリースは、最大 5 台の外部サーバをサポートします。
- Splunk を使用する場合は、ログ アナライザー サービス プロバイダをセットアップして構成します。

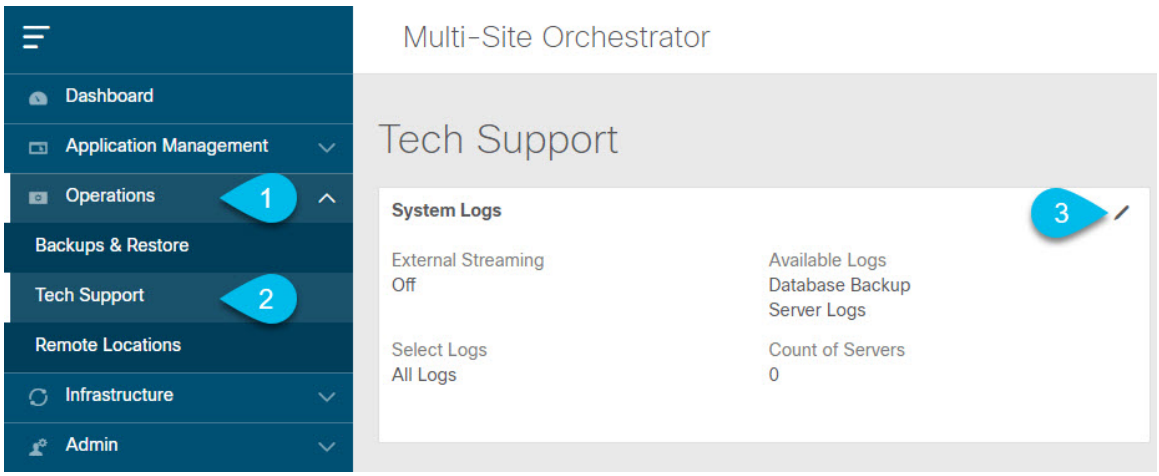
  外部ログ アナライザーの設定方法の詳細については、マニュアルを参照してください。
- Splunk を使用する場合は、サービス プロバイダの認証トークンを取得します。

  分裂サービスの認証トークンの取得については、「分裂」のマニュアルで詳しく説明していますが、要するに、**[設定 (Settings)]** > **[データ入力 (Data Inputs)]** > **[HTTP イベントコレクタ (Data input HTTP Event Collector)]**を選択し、[**新規トークン (New token**)] をクリックして、認証トークンを取得できます。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 **[システムログ (System Logs)]** 画面を開きます。



a) メインメニューで、**[操作 (Operations)]** > **[テクニカル サポート (Tech Support)]**を選択します。

b) **[システム ログ (System Logs)]** フレームの右上隅にある編集ボタンをクリックします。

ステップ 3 **[システムログ (System Logs)]** ウィンドウで、外部ストリーミングを有効にし、サーバを追加します。

a) **[外部ストリーミング (External Streaming)]** ノブを有効にします。

b) **[すべてのログ (All Logs)]** をストリーミングするか、**[監査ログ (Audit Logs)]** のみをストリーミングするかを選択します。

c) **[サーバーの追加 (Add Server)]** をクリックして、外部ログ アナライザ サーバーを追加します。

ステップ 4 Splunk サーバーを追加します。

Splunk サービスを使用する予定がない場合は、この手順をスキップします。

a) サーバーのタイプとして `[Splunk]` を選択します。

b) プロトコルを選択します。

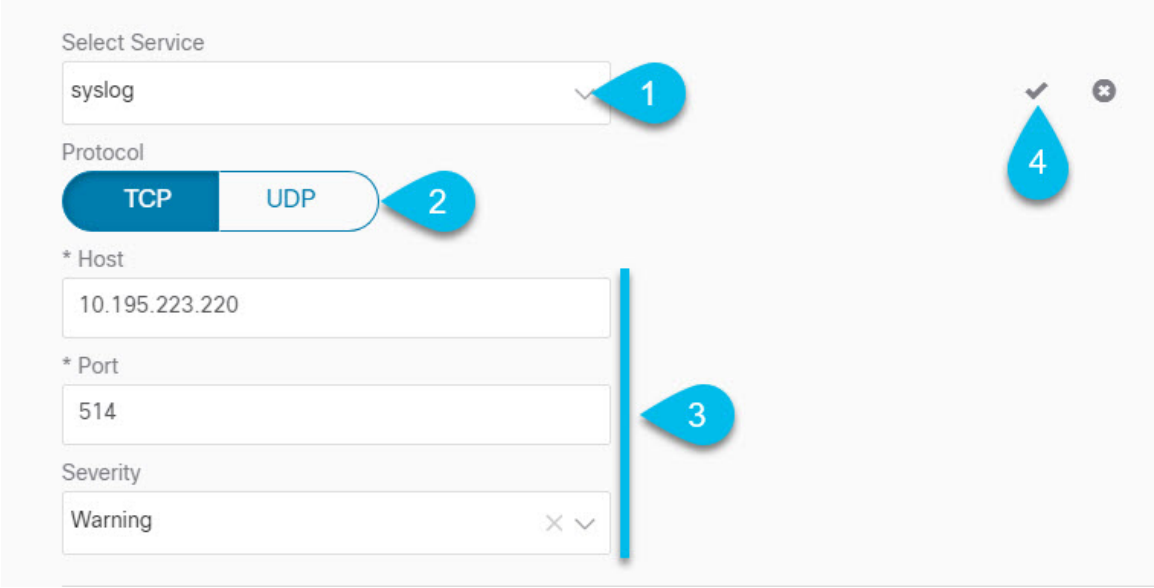
c) Splunk サービスから取得したサーバ名または IP アドレス、ポート、および認証トークンを入力します。

Splunk サービスの認証トークンの取得については、Splunk のマニュアルで詳しく説明していますが、要するに、**[設定 (Settings)]** > **[データ入力 (Data Inputs)]** > **[HTTP イベントコレクタ (HTTP Event Collector)]** を選択し、**[新規トークン (New token)]** をクリックして、認証トークンを取得できます。

d) チェックマーク アイコンをクリックして、サーバーの追加を終了します。

ステップ 5 `syslog` サーバーを追加します。

`syslog` を使用しない場合は、この手順をスキップします。



a) サーバーのタイプとして `[syslog]` を選択します。

b) プロトコルを選択します。

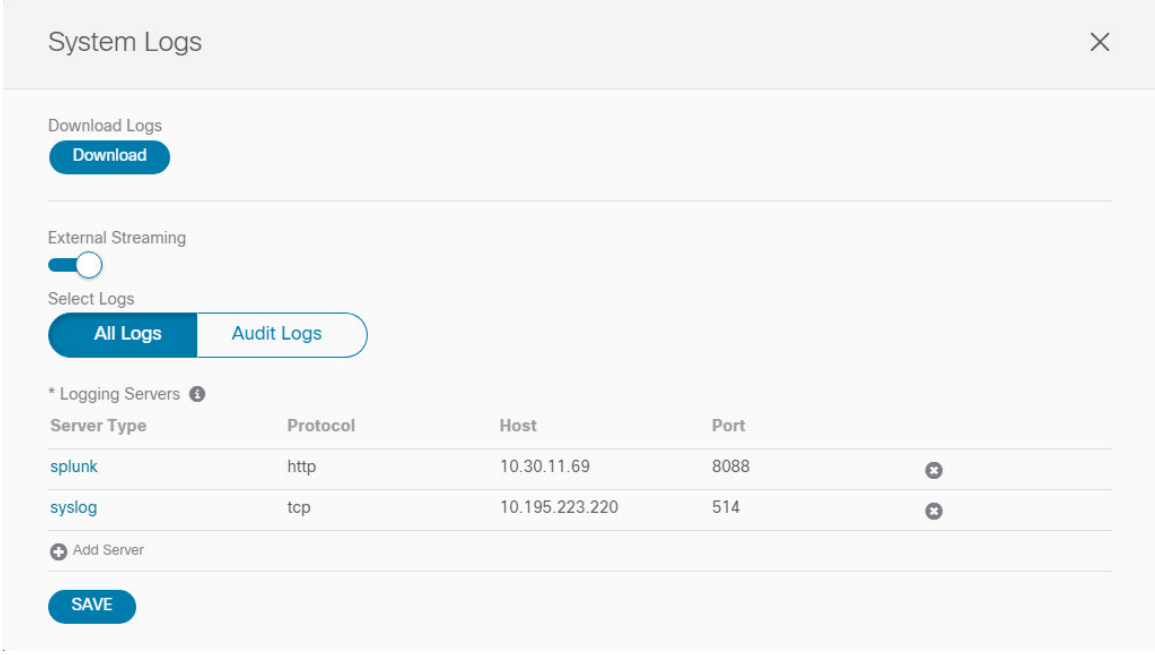
c) サーバー名またはIPアドレス、ポート番号、およびストリーミングするログ メッセージのシビラティ（重大度）を指定します。

d) チェックマーク アイコンをクリックして、サーバーの追加を終了します。

ステップ 6 複数のサーバーを追加する場合は、この手順を繰り返します。

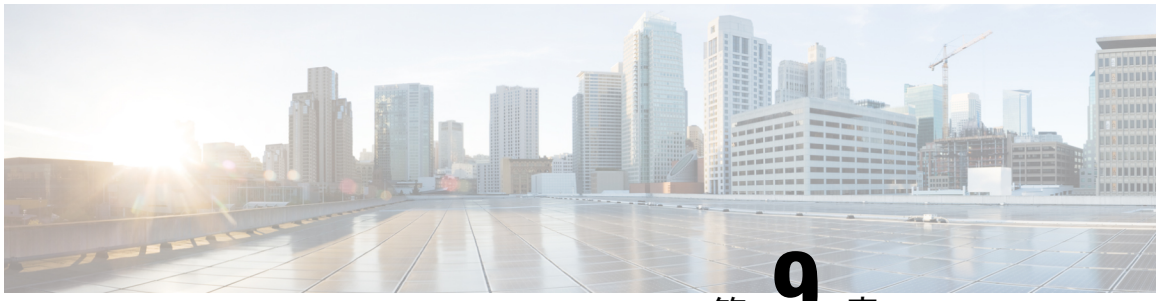
このリリースは、最大 5 台の外部サーバ0をサポートします。

ステップ 7 [保存（Save）] をクリックして、変更内容を保存します。


System Logs
Download Logs
Download
External Streaming
Select Logs
All Logs
Audit Logs
* Logging Servers
Server Type
Protocol
Host
Port
splunk
http
10.30.11.69
8088
syslog
tcp
10.195.223.220
514
Add Server
SAVE

第 III 部

インフラストラクチャ管理



第 9 章

システム設定

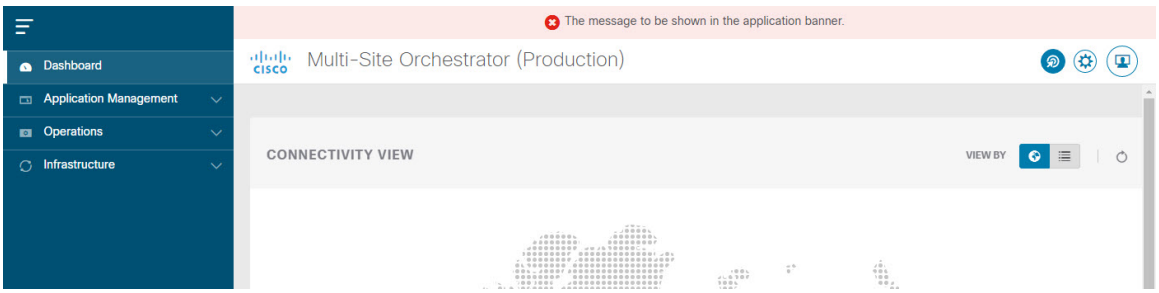
システム設定

次のセクションで説明するように、Multi-Site Orchestrator に対して設定できる、 **管理 > システム設定**で使用可能なグローバルシステム設定が多数あります。

システム エイリアスとバナー

このセクションでは、Nexus Dashboard Orchestrator のエイリアスを設定する方法と、次の図に示すように、GUI 全体で画面の上部に表示されるカスタムのバナーを有効にする方法について説明します。

図 *8 :* システム バナーの表示



手順

ステップ 1 Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインから**[管理 (Admin)] > [システム設定 (System Configuration)]** を選択します。.

ステップ 3 **[編集 (Edit)]** のアイコンをクリックします。これは **[システム エイリアスとバナー System Alias & Banners)]** 領域の右にあります。

[システム エイリアスとバナー System & Banners)] の設定ウィンドウが表示されます。

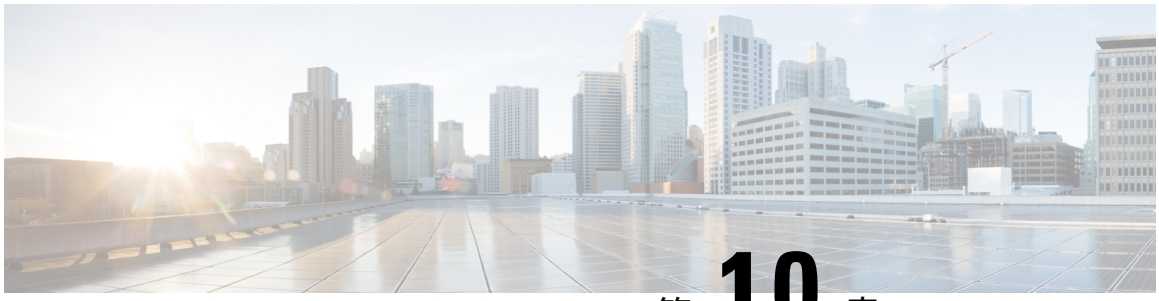
ステップ 4 **[エイリアス (Alias)]** フィールドで、システムのエイリアスを指定します。

ステップ 5 GUI バナーを有効にするかどうかを選択します。

ステップ 6 バナーを有効にする場合には、バナーに表示されるメッセージを指定する必要があります。

ステップ 7 バナーを有効にする場合には、バナーのシビラティ（重大度）を意味する色を選択する必要があります。

ステップ 8 [保存（Save）] をクリックして、変更内容を保存します。



第 10 章

Cisco APIC サイトの準備

ポッド プロファイルとポリシー グループ

各サイトの APIC には、ポッド ポリシー グループを持つポッド プロファイルが 1 つ必要です。サイトにポッド ポリシー グループがない場合は、作成する必要があります。通常、これらの設定はすでに存在していて、ファブリックを最初に展開したときに設定したとおりになっているはずです。

手順

ステップ 1 サイトの APIC GUI にログインします。

ステップ 2 ポッド プロファイルにポッド ポリシー グループが含まれているかどうかを確認します。

[ファブリック (Fabric)] > **[ファブリック ポリシー (Fabric Policies)]** > **[ポッド (Pods)]** > **[プロファイル (Profiles)]** > **[ポッドのプロファイルのデフォルト (Pod Profile default)]**に移動します。

ステップ 3 必要であれば、ポッド ポリシー グループを作成します。

a) **[ファブリック (Fabric)]** > **[ファブリック ポリシー (Fabric Policies)]** > **[ポッド (Pods)]** > **[ポリシー グループ (Policy Groups)]**に移動します。

b) **[ポリシー グループ (Policy Groups)]** を右クリックし、**[ポッド ポリシー グループの作成 (Create Pod Policy Groups)]** を選択します。

c) 適切な情報を入力して、[Submit] をクリックします。

ステップ 4 新しいポッド ポリシー グループをデフォルトのポッド プロファイルに割り当てます。

a) **[ファブリック (Fabric)]** > **[ファブリック ポリシー (Fabric Policies)]** > **[ポッド (Pods)]** > **[プロファイル (Profiles)]** > **[ポッド プロファイルのデフォルト (Pod Profile default)]** に移動します。

b) デフォルトのプロファイルを選択します。

c) 新しいポッド ポリシー グループを選択し、**[更新 (Update)]** をクリックします。

すべての APIC サイトのファブリック アクセス ポリシーの設定

APIC ファブリックを Nexus Dashboard Orchestrator に追加し、Nexus Dashboard Orchestrator により管理できるようにするには、サイトごとに設定することが必要な、ファブリック固有の多数のアクセス ポリシーがあります。

ファブリック アクセス グローバル ポリシーの設定

このセクションでは、Nexus Dashboard Orchestrator に追加し、管理する前に、APIC サイトごとに作成する必要があるグローバル ファブリック アクセス ポリシーの設定について説明します。

手順

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メイン ナビゲーション メニューから、**[ファブリック (Fabric)]** > **[アクセス ポリシー (Access Policies)]** を選択します。

サイトを Nexus Dashboard Orchestrator に追加するには、いくつかのファブリックポリシーを設定する必要があります。APIC の観点からは、ベアメタル ホストを接続していた場合と同様に、ドメイン、AEP、ポリシー グループ、およびインターフェイス セレクタを設定することができます。同じマルチサイト ドメインに属するすべてのサイトに対して、スパイン スイッチインターフェイスをサイト間ネットワークに接続するための同じオプションを設定する必要があります。

ステップ 3 VLAN プールを指定します。

最初に設定するのは、VLAN プールです。レイヤ 3 サブインターフェイスは VLAN 4 を使用してトラフィックにタグを付け、スパインスイッチをサイト間ネットワークに接続します。

a) 左側のナビゲーション ツリーで、**[プール (Pools)]** > **[VLAN]** を参照します。

b) **[VLAN]** カテゴリを右クリックし、**[VLAN プールの作成 (Create VLAN Pool)]** を選択します。

[**VLAN プールの作成 (CREATE VLAN Pool)**] ウィンドウで、次の項目を指定します。

- [**名前 (name)**] フィールドで、VLAN プールの名前 (たとえば、 `msite`) を指定します。
- [**Allocation Mode (割り当てモード)**]の場合は、[スタティック割り当て(`Static Allocation`)]を指定します。
- [**Encap ブロック(Encap Blocks)**] の場合は、単一の VLAN 4 だけを指定します。両方の [**Range (範囲)**] フィールドに同じ番号を入力することによって、単一の VLAN を指定できます。

ステップ 4 接続可能アクセス エンティティ プロファイル (AEP) を作成します。

a) 左側のナビゲーションツリーで、**[グローバル ポリシー (Global Policies)]** > **[接続可能なアクセス エントリ プロファイル (Attachable Access Entity Profiles)]** を参照します。

b) **[接続可能なアクセス エンティティ プロファイル (Attachable Access Entry Profiles)]** を右クリックして、**[接続可能なアクセス エンティティ プロファイルの作成 (Create Attachable Access Entity Profiles)]** を選択します。

[接続可能アクセス エンティティ プロファイルの作成(Create Attachable Access Entity Profiles)] ウィンドウで、AEP の名前 (例：`msite-aep`) を指定します。

c) [**次へ(Next)**] をクリックして [**送信(Submit)**] します。

インターフェイスなどの追加の変更は必要ありません。

ステップ 5 ドメインを設定します。

設定するドメインは、このサイトを追加するときに、Nexus Dashboard Orchestratorから選択するものになります。

a) ナビゲーション ツリーで、**[物理的ドメインと外部ドメイン (Physical and External Domains)]** > **[外部でルーテッド ドメイン (External Routed Domains)]** を参照します。

b) [**外部ルーテッド ドメイン(External Routed Domains)**] カテゴリを右クリックし、[**レイヤ 3 ドメインの作成 (Create Layer 3 Domain)**] を選択します。

[**レイヤ 3 ドメインの作成 (Create Layer 3 Domain)**] ウィンドウで、次の項目を指定します。

- [**名前 (name)**] フィールドで、ドメインの名前を指定します。たとえば、 `msite-l3`です。
- **関連付けられている接続可能エンティティ プロファイル**の場合は、ステップ 4で作成した AEP を選択します。
- **VLAN プール**の場合は、ステップ 3で作成した VLAN プールを選択します。

c) [**送信 (Submit)**] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

次のタスク

グローバルアクセス ポリシーを設定した後も、ファブリック アクセス インターフェイス ポリシーの設定 （155 ページ） の説明に従って、インターフェイス ポリシーを追加する必要があります。

ファブリック アクセス インターフェイス ポリシーの設定

このセクションでは、各 APIC サイトの Nexus Dashboard Orchestrator で行わなければならないファブリック アクセス インターフェイスの設定について説明します。

始める前に

サイトの APIC では、ファブリック アクセス グローバル ポリシーの設定 （154 ページ） の説明に従って、VLAN プール、AEP、および ドメインなどのグローバル ファブリック アクセス ポリシーを設定しておく必要があります。

手順

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メイン ナビゲーション メニューから、**[ファブリック (Fabric)]** > **[アクセス ポリシー (Access Policies)]** を選択します。

前のセクションで設定した VLAN、AEP、およびドメインに加えて、サイト間ネットワーク (ISN) に接続するファブリックのスパイン スイッチ インターフェイスに対してインターフェイス ポリシーを作成します。

ステップ 3 スパイン ポリシー グループを設定します。

a) 左ナビゲーション ツリーで、**[インターフェイス ポリシー (Interface Policie)]** > **[ポリシー グループ (Policy Groups)]** > **[スパイン ポリシー グループ (Spine Policy Groups)]** を参照します。

これは、ベアメタルサーバを追加する方法と類似していますが、リーフ ポリシー グループの代わりにスパイン ポリシー グループを作成する点が異なります。

b) **[スパイン ポリシー グループ (Spine Policy Groups)]** カテゴリーを右クリックして、**[スパイン アクセス ポート ポリシー グループの作成 (Create Spine Access Port Policy Group)]** を選択します。

[**スパイン アクセス ポリシー グループの作成 (Create Spine Access Port Policy Group)**]ウィンドウで、以下のとおり指定します。

- **[名前 (Name)]** フィールドの場合、ポリシー グループの名前を指定します。たとえば `Spine1-PolGrp` です。
- [**リンク レベル ポリシー (Link Level Policy)**] フィールドには、スパイン スイッチと ISN の間のリンク ポリシーを指定します。
- **[CDP ポリシー (CDP Policy)]** の場合、CDP を有効にするかどうかを選択します。
- **[添付したエンティティ プロファイル (Attached Entity Profiel)]**の場合、前のセクションで設定した AEP を選択します。たとえば `msite-aep` です。

c) [**送信 (Submit)**] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

ステップ 4 スパイン プロファイルを設定します。

a) 左ナビゲーション ツリーで、**[インターフェイス ポリシー (Interface Policies)]** > **[ポリシー グループ (Profiles)]** > **[スパイン ポリシー グループ (Spine Profiles)]** を参照します。

b) **[プロファイル (Profiles)]** カテゴリを右クリックし、**[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile]** を選択します。

[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)] ウィンドウで、次のとおり指定します。

- **[名前 (name)]** フィールドに、プロファイルの名前 (`Spine1`など) を指定します。
- **[インターフェイス セレクタ (Interface Selectors)]**では、+ 記号をクリックして、ISN に接続されるスパイン スイッチ上のポートを追加します。次に、**[スパイン アクセス ポート セレクターの作成 (Create Spine Access Port Selector)]** ウィンドウで、次のように指定します。
  - **[名前 (name)]** フィールドに、ポート セレクタの名前を指定します (例: `Spine1`)。
  - **[インターフェイス ID (Interface IDs)]** に、ISN に接続するスイッチ ポートを指定します (例 `5/32`)。
  - **[インターフェイス ポリシー グループ (Interface Policy Group)]** に、前の手順で作成したポリシー グループを選択します (例: `Spine1-PolGrp`)。

  それから、**[OK]** をクリックして、ポート セレクタを保存します。

c) **[送信 (Submit)]** をクリックしてスパイン インターフェイス プロファイルを保存します。

ステップ 5 スパイン スイッチ セレクター— ポリシーを設定します。

a) 左ナビゲーション ツリーで、**[スイッチ ポリシー (Switch Policies)]** > **[プロファイル (Profiles)]** > **[スパイン プロファイル (Spine Profiles)]** を参照します。

b) **[スパイン プロファイル (Spine Profiles)[** カテゴリを右クリックし、**[スパイン プロファイルの作成 (Create Spine Profile)]** を選択します。

[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)] ウィンドウで、次のように指定します。

- **[名前 (name)]** フィールドに、プロファイルの名前を指定します (例: `Spine1`)。
- **[スパインセレクタ (Spine Selectora)]**で、**[+]** をクリックしてスパインを追加し、次の情報を入力します。
  - **[名前 (name)]** フィールドで、セレクタの名前を指定します (例: `Spine1`) 。
  - **[ブロック (Blocks)]** フィールドで、スパイン ノードを指定します (例: `201`)。

c) **[更新 (Update)]** をクリックして、セレクタを保存します。

d) **[次へ (Next)]** をクリックして、次の画面に進みます。

e) 前の手順で作成したインターフェイス プロファイルを選択します。

たとえば、`Spine1-ISN`などです。

f) **[完了 (Finish)]** をクリックしてスパイン プロファイルを保存します。

リモート リーフ スイッチを含むサイトの設定

Multi-Site アーキテクチャはリモート リーフスイッチを持つ APIC サイトをサポートします。次のセクションでは、Nexus Dashboard Orchestrator がこれらのサイトを管理できるようにするために必要な注意事項、制限事項、および設定手順を説明します。

リモート リーフの注意事項と制限事項

Nexus Dashboard Orchestrator により管理されるリモート リーフをもつ APIC サイトを追加する場合、次の制約が適用されます。

- Cisco APICはリリース 4.2(4) 以降にアップグレードする必要があります。
- このリリースでは、物理リモート リーフ スイッチのみがサポートされます
- -EX および -FX 以降のスイッチのみが、マルチサイトで使用するリモートリーフスイッチとしてサポートされています。
- リモートリーフは、IPN スイッチを使用しないバックツーバック接続サイトではサポートされていません
- 1 つのサイトのリモート リーフ スイッチで別のサイトの L3Out を使用することはできません
- あるサイトと別のサイトのリモート リーフ間のブリッジ ドメインの拡張はサポートされていません。

また、Nexus Dashboard Orchestrator でサイトを追加して管理するには、その前に次のタスクを実行する必要があります。

- 次の項で説明するように、リモートリーフの直接通信をイネーブルAPICにし、サイト内でルーティング可能なサブネットを直接設定する必要があります。
- リモート リーフ スイッチに接続しているレイヤ 3 ルータのインターフェイスに適用されている DHCP リレー設定で、Cisco APIC ノードのルーティング可能な IP アドレスを追加する必要があります。

  各 APIC ノードのルーティング可能な IP アドレスは、**[ルーティング可能 IP (Routable IP)]** フィールド (APIC GUI の **[システム (System)]** > **[コントローラ (Controllers)]** > **<コントローラ名>**画面) に表示されます。

リモート リーフ スイッチのルーティング可能なサブネットの設定

1 つ以上のリモート リーフ スイッチを含むサイトを Nexus Dashboard Orchestrator に追加するには、その前に、リモート リーフ ノードが関連付けられているポッドのルーティング可能なサブネットを設定する必要があります。

手順

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メニュー バーから、**[ファブリック (Fabric)]** > **[インベントリ (Inventory)]** を選択します。

ステップ 3 [ナビゲーション (Navigation)] ウィンドウで、**[ポッド ファブリック セットアップ ポリシー (Pod Fabric Setup Policy)]** をクリックします。

ステップ 4 メイン ペインで、サブネットを設定するポッドをダブルクリックします。

ステップ 5 **ルーティング可能なサブネット**エリアで、 + 記号をクリックしてサブネットを追加します。

ステップ 6 **IP**アドレスと**予約アドレスの数**を入力し、状態をアクティブまたは非アクティブに設定してから、**[更新 (Update)]** をクリックしてサブネットを保存します。

ルーティング可能なサブネットを設定する場合は、 /22~/29の範囲のネットマスクを指定する必要があります。

ステップ 7 [送信（Submit）] をクリックして設定を保存します。

リモート リーフ スイッチの直接通信の有効化

1 つ以上のリモート リーフ スイッチを含むサイトを Nexus Dashboard Orchestrator に追加するには、その前に、そのサイトに対して直接リモート リーフ通信を設定する必要があります。リモートリーフ直接通信機能に関する追加情報については、*Cisco APIC* レイヤ *3* ネットワーク コンフィギュレーション ガイドを参照してください。ここでは、Multi-Site との統合に固有の手順とガイドラインの概要を説明します。

（注） リモート リーフ スイッチの直接通信を有効にすると、スイッチは新しいモードでのみ機能します。

手順

ステップ 1 サイトの APIC に直接ログインします。

ステップ 2 リモート リーフ スイッチの直接トラフィック転送を有効にします。

a) メニュー バーから、**[システム (System)]** > **[システムの設定 (System Settings)]** に移動します。

b) 左側のサイドバーのメニューから **[ファブリック全体の設定 (Fabric Wide Setting)]** を選択します。

c) **[リモート リーフ 直接トラフィック転送 (Enable Remote Leaf Direct Traffice Forwarding)]** チェックボックスをオンにします。

（注）
有効にした後は、このオプションを無効にすることはできません。

d) **[送信 (Submit)]** をクリックして変更を保存します。

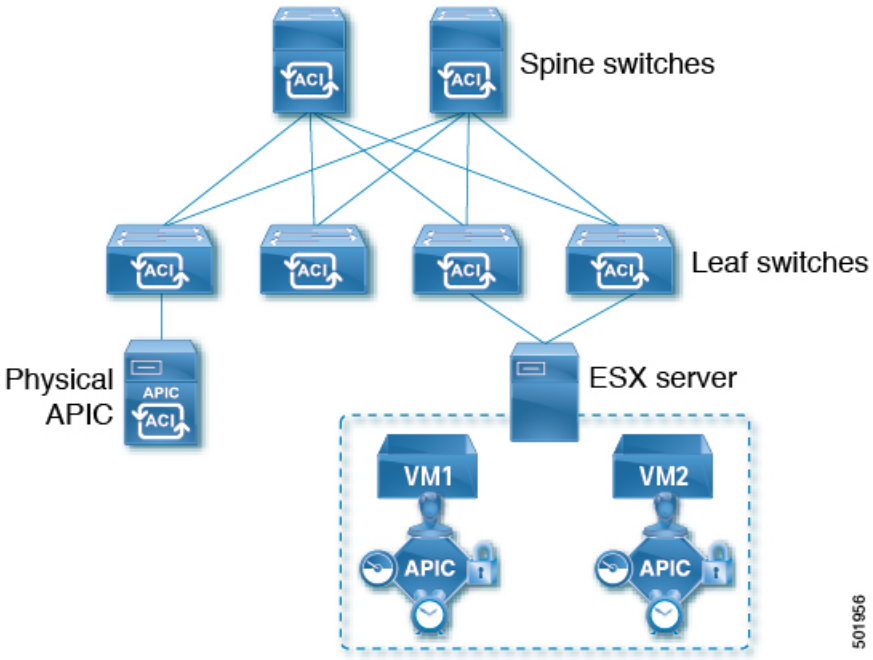
Cisco Mini ACI ファブリック

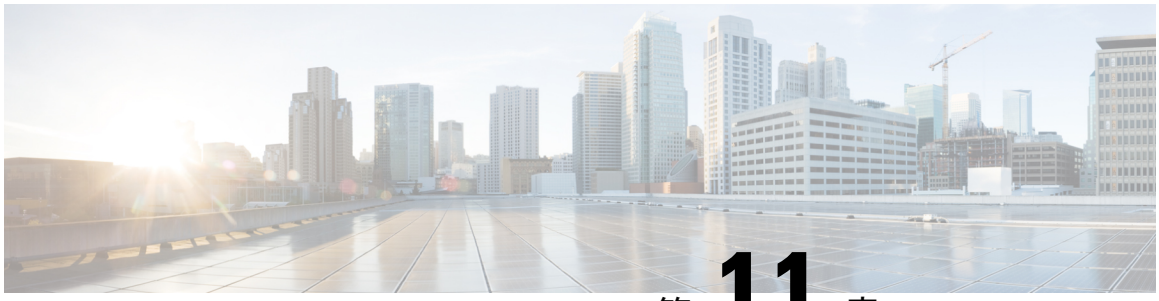
Cisco Multi-Site は、追加の設定を必要とせずに、一般的なオンプレミス サイトとして Cisco Mini ACI ファブリックをサポートします。ここでは、Mini ACI ファブリックの概要について説明します。このタイプのファブリックの導入と設定に関する詳細情報は、『*Cisco Mini ACI ファブリックおよび仮想 APIC*』に記述されています。

Cisco ACI リリース 4.0(1) では、小規模導入向けに Mini ACI ファブリックが導入されました。Mini ACI ファブリックは、仮想マシンで実行される1つの物理 APIC と 2 つの仮想 APIC（vAPIC）で構成される Cisco APIC クラスタで動作します。これにより、APIC クラスタの物理的なフットプリントとコストが削減され、ACI ファブリックを、物理的な設置面積や初期コストのために、フルスケールの ACI インストールが実用的でないような、ラック スペースや初期予算が限られたシナリオ（コロケーション施設やシングルルームデータセンターなど）に導入できるようになります。

次の図に、物理 APIC と 2 つの仮想 APIC（vAPIC）を備えたミニCisco ACIファブリックの例を示します。

図 *9 : Cisco Mini ACI* ファブリック





第 11 章

サイトの追加と削除

Cisco NDO と APIC の相互運用性のサポート

Cisco Nexus Dashboard Orchestrator（NDO）では、すべてのサイトで特定のバージョンの APIC を実行する必要はありません。各サイトの APIC クラスタと NDO 自体は、Nexus Dashboard Orchestrator サービスがインストールされている Nexus ダッシュボードにファブリックをオンボードできる限り、相互に独立してアップグレードし、混合動作モードで実行することができます。そのため、常に Nexus Dashboard Orchestrator の最新リリースにアップグレードしておくことをお勧めします。

ただし、1 つまたは複数のサイトで APIC クラスタをアップグレードする前に NDO をアップグレードすると、新しい NDO の機能の一部が、以前の APIC リリースでまだサポートされていないという状況が生じ得ることに注意してください。この場合、各テンプレートでチェックが実行され、すべての設定済みオプションがターゲットサイトでサポートされていることを確認します。

このチェックは、テンプレートを保存するか、テンプレートを展開するときに実行されます。テンプレートがすでにサイトに割り当てられている場合、サポートされていない設定オプションは保存されません。テンプレートがまだ割り当てられていない場合は、サイトに割り当てることができますが、サイトがサポートしていない設定が含まれている場合は、スキーマを保存したり展開したりすることはできません。

サポートされていない設定が検出されると、エラーメッセージが表示されます。例: `この APIC サイトバージョン<site version>は、NDO ではサポートされていません。この<feature>に必要な最小バージョンは<required-version>以降です。`

次の表に、各機能と、それぞれに必要な最小限の APIC リリースを示します。

（注） 次の機能の一部は、以前の Cisco APIC リリースでサポートされていますが、Nexus ダッシュボードにオンボードし、このリリースの Nexus Dashboard Orchestrator で管理できる最も古いリリースは、リリース 4.2(4) です。

機能	最小バージョン
ACI マルチポッドのサポート	リリース 4.2(4)
サービス グラフ (L4 ~ L7 サービス)	リリース 4.2(4)
外部 EPG	リリース 4.2(4)
ACI 仮想エッジ VMM のサポート	リリース 4.2(4)
DHCP Support	リリース 4.2(4)
整合性チェッカー	リリース 4.2(4)
vzAny	リリース 4.2(4)
ホストベースのルーティング	リリース 4.2(4)
CloudSec 暗号化	リリース 4.2(4)
レイヤ 3 マルチキャスト	リリース 4.2(4)
OSPF の MD5 認証	リリース 4.2(4)
EPG 優先グループ	リリース 4.2(4)
サイト内 L3Out	リリース 4.2(4)
QoS の優先順位	リリース 4.2(4)
コントラクト QoS 優先順位	リリース 4.2(4)
シングル サインオン（SSO）	リリース 5.0(1)
マルチキャスト ランデブー ポイント（RP）のサポート	リリース 5.0(1)
AWS および Azure サイトのトランジット ゲートウェイ（TGW）サポート	リリース 5.0(1)
SR-MPLS サポート	リリース 5.0(1)
クラウド ロードバランサ 高可用性ポート	リリース 5.0(1)

機能	最小バージョン
UDR を使用したサービスグラフ（L4-L7 サービス）	Release 5.0(2)
クラウドでのサードパーティデバイスのサポート	Release 5.0(2)
クラウドロードバランサのターゲット接続モード機能	Release 5.1(1)
Express Route 経由で到達可能な非 ACI ネットワークの Azure でのセキュリティおよびサービス挿入サポート	Release 5.1(1)
CSR プライベート IP サポート	Release 5.1(1)
Azure のクラウド ネイティブ サービスの ACI ポリシー モデルと自動化の拡張	Release 5.1(1)
Azure の単一 VNET 内での複数の VRF サポートによる柔軟なセグメンテーション	Release 5.1(1)
Azure PaaS およびサードパーティ サービスのプライベート リンク自動化	Release 5.1(1)
ACI-CNI を使用した Azure での OpenShift 4.3 IPI	Release 5.1(1)
クラウド サイト アンダーレイの設定	リリース 5.2(1)

Cisco ACI サイトの追加

ここでは、Nexus Dashboard GUI を使用して Cisco APIC または Cloud Network Controller サイトを追加し、そのサイトを Nexus Dashboard Orchestrator で管理できるようにする方法について説明します。

始める前に

- この章の前のセクションで説明したように、オンプレミスの ACI サイトを追加する際には、各サイトの APIC でサイト固有の構成を完了している必要があります。
- 追加するサイトがリリース 4.2(4) 以降を実行していることを確認する必要があります。

手順

ステップ 1 Nexus Dashboard にログインして **[管理コンソール（Admin Console）]**を開きます。

ステップ 2 左のナビゲーションメニューから **[サイト（Sites）]** を選択し、**[サイトを追加（Add Site）]**をクリックします。

ステップ 3 サイト情報を入力します。

a) **[サイト タイプ（Site Type）]** で、追加する ACI ファブリックのタイプに応じて **[ACI]** または **[Cloud Network Controller]** を選択します。

b) コントローラ情報を入力します。

- ACI ファブリックを現在管理している APIC コントローラについて、**[ホスト名/IP アドレス (Host Name/IP Address)]**、**[ユーザー名 (User Name)]**、および **[パスワード (Password)]** を入力する必要があります。用です。

  （注）
  APIC ファブリックでは、Nexus Dashboard Orchestrator サービスのみでサイトを使用する場合、APIC のインバンドまたはアウトオブバンド IP アドレスを指定できます。Nexus Dashboard Insights でもサイトを使用する場合は、インバンド IP アドレスを指定する必要があります。

- Cisco APIC によって管理されるオンプレミス ACI サイトの場合、このサイトを Nexus Insights などのデイ 2 オペレーション アプリケーションで使用する場合は、追加する Nexus ダッシュボードをファブリックに接続するために使用する**インバンド EPG** 名も指定する必要があります。それ以外の場合、このサイトを Nexus Dashboard Orchestrator でのみ使用する場合は、このフィールドを空白のままにすることができます。

- Cloud Network Controller サイトの場合、プロキシ経由でクラウド サイトに到達できる場合は、**[プロキシを有効（Enable Proxy）]**にします。

  プロキシは、Nexus Dashboard のクラスタ設定ですでに設定されている必要があります。管理ネットワーク経由でプロキシに到達できる場合は、プロキシIPアドレス用のスタティック管理ネットワークルートも追加する必要があります。プロキシとルートの構成の詳細については、お使いのリリースの Nexus Dashboard ユーザー ガイドを参照してください。

c) **[保存（Save）]** をクリックして、サイトの追加を終了します。

この時点で、サイトは Nexus ダッシュボードで使用できるようになりますが、次の手順で説明するように、Nexus Dashboard Orchestrator の管理用にそれらのサイトを有効にする必要があります。

ステップ 4 追加する任意の ACI または、Cloud Network Controller サイトに対して前の手順を繰り返します。

ステップ 5 Nexus Dashboard の**[サービス（Services）]**から、Nexus Dashboard Orchestrator サービスを開きます。

Nexus ダッシュボード ユーザーのクレデンシャルを使用して自動的にログインします。

ステップ 6 Nexus Dashboard Orchestrator GUIで、サイトを管理します。

a) 左のナビゲーションメニューから **[サイト (Sites)]** を選択します。

b) メインペインで、NDOで管理する各ファブリックの **[状態 (State)]** を［非管理対象 (Unmanaged)］から［管理対象 (Managed)］に変更します。

サイトを管理するときは、サイトごとに一意のサイト ID を指定する必要があります。

（注）
オーケストレーションを有効にするときの問題を回避するために、ACI サイト名が 125 文字以下に制限されていることを確認します。

サイトの削除

ここでは、Nexus Dashboard Orchestrator GUI を使用して 1 つ以上のサイトのサイト管理を無効にする方法について説明します。サイトは Nexus ダッシュボードに残ります。

始める前に

削除するサイトに関連付けられているすべてのテンプレートが展開されていないことを確認する必要があります。

手順

ステップ 1 Nexus Dashboard Orchestrator GUI を開きます。

Nexus ダッシュボードの**サービス カタログ**から NDO サービスを開きます。Nexus ダッシュボードユーザーのクレデンシャルを使用して自動的にログインします。

ステップ 2 すべてのテンプレートからサイトを削除します。

サイトを管理解除して Nexus Dashboard から削除する前に、関連付けられているすべてのテンプレートからサイトを削除する必要があります。

a) **[アプリケーション管理 (Application Management)[** > **[スキーマ (Schemas)]**の順に移動します。
b) サイトに関連付けられた 1 つ以上のテンプレートを含むスキーマをクリックします。
c) 左側のサイドバーの **[サイト（Sites）]** 領域で、サイトに関連付けられているテンプレートを選択し、テンプレートの横にあるオプションメニュー（**...**）をクリックして、**[テンプレートの展開解除（Undeploy Template**）] を選択します。

これにより、このテンプレートを使用してこのサイトに展開された構成が削除されます。

（注）
拡張されていないテンプレートの場合は、[テンプレートの展開 **解除（Undeploy Template）]** の代わりに **[テンプレートの関連付け解除（Dissociate Template）]**を選択して設定を保持することもできますが、拡張されたテンプレートは展開解除する必要があります。

d) このスキーマおよび他のすべてのスキーマで管理解除するサイトに関連付けられているすべてのテンプレートについて、この手順を繰り返します。

ステップ 3 サイトのアンダーレイ設定を削除します。

a) 左のナビゲーションメニューから、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。
b) メイン ペインにある **[構成（Configure）]** をクリックします。
c) 左側のサイドバーで、管理対象から外すサイトを選択します。
d) 右側のサイドバーの **[サイト間接続]** タブで、**[マルチサイト]** チェックボックスを無効にします。
e) **[展開する（Deploy）]** をクリックして、変更をサイトに展開します。

ステップ 4 Nexus Dashboard Orchestrator GUI で、サイトを無効にします。

a) 左のナビゲーションメニューから、**[インフラストラクチャ (Infrastructure)]** > **[サイト (Sites)]**を選択します。
b) メイン ペインで、非管理対象に設定したいサイトに対して **[状態 (State)]** を [非管理対象 (Unmanaged)] から [管理対象 (Managed)] に変更します。

（注）
前の手順で示したように、サイトが1つ以上の展開済みテンプレートに関連付けられている場合、それらのテンプレートを展開解除するまで、その状態を [非管理対象 (Unmanaged)] に変更することはできません。

ステップ 5 Nexus ダッシュボードからサイトを削除します。

このサイトを管理したり、他のアプリケーションで使用したりする必要がなくなった場合は、Nexus ダッシュボードからもサイトを削除できます。

（注）
この時点で、このサイトは、Nexus Dashboard クラスタにインストールされているどのサービスでも使用されていてはならないことに注意してください。

a) 上部のナビゲーション バーで **[ホーム]** アイコンをクリックして、Nexus Dashboard GUI に戻ります。
b) NexusダッシュボードGUIの左側のナビゲーションメニューから、**[サイト (Sites)]** を選択します。
c) 削除するサイトを1つ以上選択します。
d) メインペインの右上にある**[アクション (Actions)]** > **[サイトの削除 (Delete Site)]**をクリックします。
e) サイトのログイン情報を入力し、**[OK]** をクリックします。

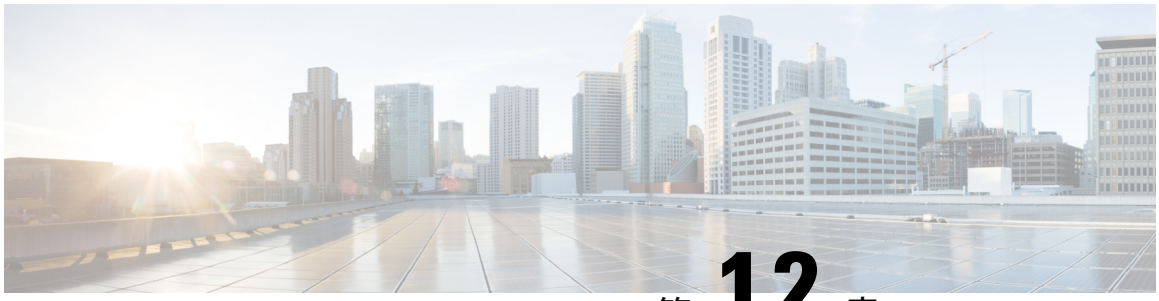
Nexus ダッシュボードからサイトが削除されます。

ファブリック コントローラへの相互起動

Nexus Dashboard Orchestrator は現在、ファブリックのタイプごとに多数の設定オプションをサポートしています。追加の多くの設定オプションでは、ファブリックのコントローラに直接ログインする必要があります。

NDO の**[インフラストラクチャ (Infrastucture)]** > **[サイト (Sites)]**画面から特定のサイト コントローラのGUIにクロス起動するには、サイトの横にあるアクション（...）メニューを選択し、ユーザー インターフェイスで **[開く (Open)]** をクリックします。クロス起動は、ファブリックのアウトオブバンド（OOB）管理IPで動作することに注意してください。

Nexus Dashboardとファブリックで同じユーザが設定されている場合、Nexus Dashboardユーザと同じログイン情報を使用して、ファブリックのコントローラに自動的にログインします。一貫性を保つために、Nexusダッシュボードとファブリック全体で共通のユーザによるリモート認証を設定することを推奨します。



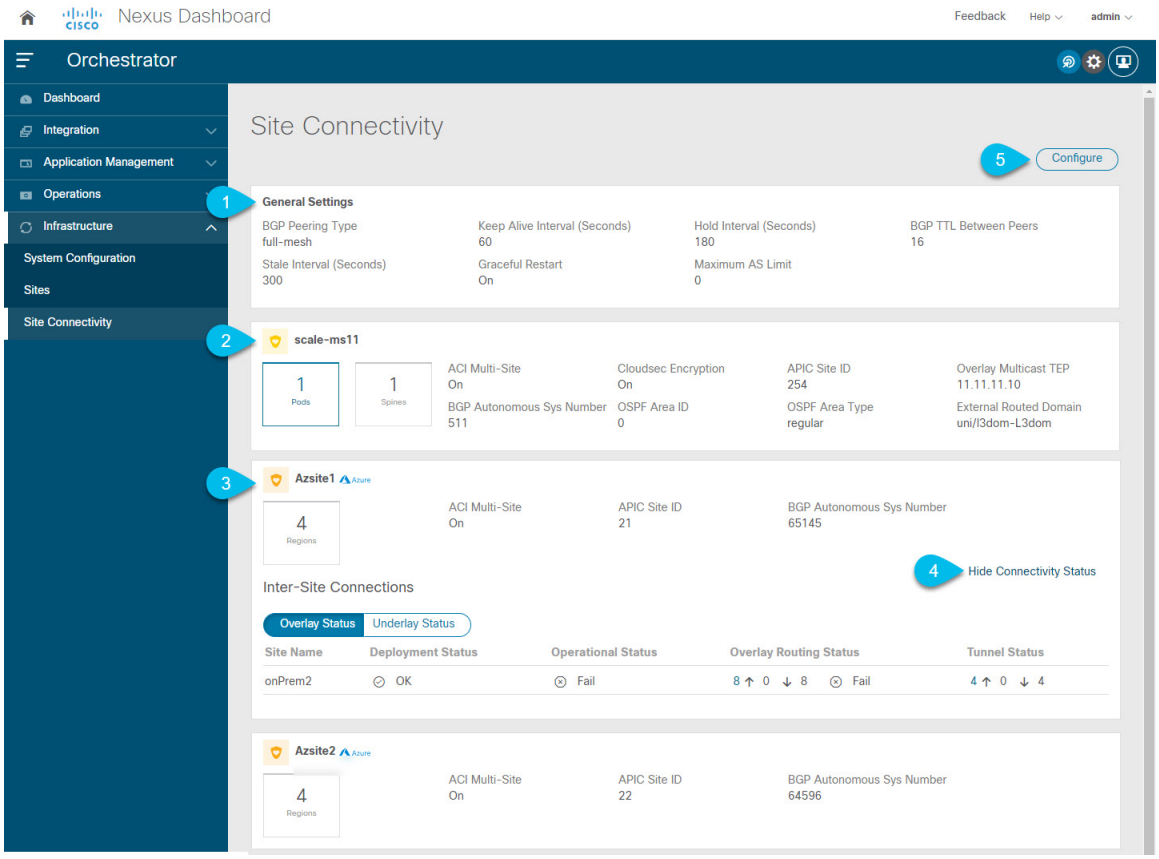
第 12 章

インフラ一般設定

インフラ設定ダッシュボード

[インフラ設定 (Infra Configuration)] ページには、Nexus Dashboard Orchestrator 展開環境のすべてのサイトとサイト間接続の概要が表示されます。

図 *10* : インフラ設定の概要



1. **[全般設定 (General Settings)]** タイルには、BGP ピアリング タイプとその設定に関する情報が表示されます。

   詳細については、次のセクションで説明します。

2. **[オンプレミス (On-Premises)]** タイルには、ポッドとスパイン スイッチの数、OSPF 設定、およびオーバーレイ IP とともに、Multi-Site ドメインの一部であるすべてのオンプレミス サイトに関する情報が表示されます。

   サイト内のポッドの数を表示する**[ポッド (Pods)]** タイルをクリックすると、各ポッドのオーバーレイ ユニキャスト TEP アドレスに関する情報を表示できます。

   詳細については、Cisco APIC サイトのインフラの設定 （177 ページ）を参照してください。

3. **[クラウド (Cloud)]** タイルには、Multi-Site ドメインの一部であるすべてのクラウド サイトに関する情報と、リージョン数および基本的なサイト情報が表示されます。

   詳細については、Cisco Cloud Network Controller サイトのインフラの構成 （185 ページ）を参照してください。

4. **[接続ステータスの表示]** をクリックして、特定のサイトのサイト間接続の詳細を表示できます。

5. **[構成]** ボタンを使用して、サイト間接続構成に移動できます。これについては、次のセクションで詳しく説明します。

次のセクションでは、全般的なファブリック インフラ設定を行うために必要な手順について説明します。ファブリック固有の要件と手順は、管理するファブリックの特定のタイプに基づいて、次の章で説明します。

インフラの設定を進める前に、前のセクションで説明したようにサイトを設定して追加する必要があります。

加えて、スパイン スイッチの追加や削除、またはスパイン ノード ID の変更などのインフラストラクチャの変更には、一般的なインフラの設定手順の一部として、サイト接続性情報の更新（177 ページ） に記載されているような、 Nexus Dashboard Orchestrator のファブリック接続情報の更新が必要です。

パーシャル メッシュ サイト間接続

Nexus Dashboard Orchestrator が管理するすべてのサイトから他のすべてのサイトへのサイト間接続を構成するフル メッシュ接続に加えて、このリリースではパーシャル メッシュ構成もサポートしています。パーシャル メッシュ構成では、他のサイトへのサイト間接続を持たないスタンドアロン モードでサイトを管理したり、サイト間構成をマルチサイト ドメイン内の他のサイトのサブセットのみに制限したりできます。

Nexus Dashboard Orchestrator リリース 3.6(1) より前では、サイト間のサイト間接続が構成されていなくても、サイト間でテンプレートを拡張し、他のサイトに展開された他のテンプレートからポリシーを参照でき、それらのサイト間のサイト間接続が構成されていなくても、サイト間で動作しない意図したトラフィック フローが発生します。

リリース 3.6(1) 以降、Orchestrator では、それらのサイト間のサイト間接続が適切に構成および展開されている場合にのみ、（他のサイトに展開されている）他のテンプレートからテンプレートとリモート参照ポリシーを 2 つ以上のサイト間で拡張できます。

次のセクションで説明するように、Cisco APIC および Cisco Cloud Network Controller サイトのサイト インフラストラクチャを構成する場合、サイトごとに、他のどのサイト インフラストラクチャ接続を確立するかを明示的に選択し、その構成情報のみを提供できます。

パーシャル メッシュ接続のガイドライン

パーシャル メッシュ接続を構成するときは、次のガイドラインを考慮してください。

- パーシャル メッシュ接続は、2 つのクラウド サイト間、またはクラウドとオンプレミスのサイト間でサポートされています。

  すべてのオンプレミス サイト間で完全なメッシュ接続が自動的に確立されます。

- パーシャル メッシュ接続は、BGP-EVPN または BGP-IPv4 プロトコルを使用してサポートされています。

ただし、テンプレートのストレッチは、BGP-EVPNプロトコルを使用して接続されているサイトに対してのみ許可されることに注意してください。BGP-IPv4 を使用して 2 つ以上のサイトを接続している場合、それらのサイトのいずれかに割り当てられたテンプレートは、1 つのサイトにのみ展開できます。

インフラの設定: 一般設定

ここでは、すべてのサイトの一般的なインフラ設定を構成する方法について説明します。

（注） 次の設定には、すべてのサイトに適用されるものと、特定のタイプのサイト（Cloud Network Controller サイトなど）に必要なものとがあります。各サイト固有のサイト ローカル設定に進む前に、インフラ一般設定で必要なすべての設定を完了していることを確認します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインにある **[構成（Configure）]** をクリックします。

ステップ 4 左側のサイドバーで、**[全般設定（General Settings）]**を選択します。

ステップ 5 **[コントロール プレーン設定（Control Plane Configuration）]** を指定します。

a) **[コントロール プレーン設定（Control Plane Configuration）]** タブを選択します。

b) **[BGP ピアリング タイプ（Bgp Peering Type）]** を選択します。

- `full-mesh`：各サイトのすべてのボーダー ゲートウェイ スイッチは、リモート サイトのボーダー ゲートウェイ スイッチとのピア接続を確立します。

  `full-mesh` 構成では、Nexus Dashboard Orchestrator は ACI 管理ファブリックのスパイン スイッチと NDFC 管理ファブリックのボーダー ゲートウェイを使用します。

- `[route-reflector]`：route-reflector オプションを使用すると、各サイトが MP-BGP EVPN セッションを確立する 1 つ以上のコントロール プレーン ノードを指定できます。ルート リフレクタ ノードを使用すると、NDO によって管理されるすべてのサイト間で MP-BGP EVPN フル メッシュ隣接関係が作成されなくなります。

  ACIファブリックの場合、`[route-reflector]` オプションは、同じ BGP ASN の一部であるファブリックに対してのみ有効です。

c) **[キープアライブ間隔 (秒) (Keepalive Interval (Seconds))]** フィールドに、キープアライブ間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

d) **[保留間隔 (秒) (Hold Interval (Seconds))]** フィールドに、保留間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

e) **[失効間隔 (秒) (Stale Interval (Seconds))]** フィールドに、失効間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

f) **[グレースフル ヘルパー (Graceful Helper)]** オプションをオンにするかどうかを選択します。

g) **[AS 上限（Maximum AS Limit）]**を入力します。

デフォルト値を維持することを推奨します。

h) **[ピア間のBGP TTL（BGP TTL Between Peers）]** を入力します。

デフォルト値を維持することを推奨します。

i) **[OSPF エリア ID (OSPF Area ID)]** を入力します。

Cloud Network Controller サイトがない場合、このフィールドは UI に表示されません。

これは、オンプレミス IPN ピアリングのためにクラウド サイトで使用される OSPF エリア ID です。

j) (オプション) CloudSec 暗号化の **[IANA 割り当てポート（IANA Assigned Port）]**を有効にします。

デフォルトでは、CloudSec は独自の UDP ポートを使用します。このオプションを使用すると、サイト間の CloudSec 暗号化に公式の IANA 予約ポート 8017 を使用するように CloudSec を構成できます。

（注）
IANA 予約ポートは、リリース 5.2(4) 以降を実行している Cisco APIC サイトでサポートされています。

この設定を変更するには、すべてのサイトで CloudSec を無効にする必要があります。IANA 予約ポートを有効にしたいが、すでに 1 つ以上のサイトで CloudSec 暗号化を有効にしている場合は、すべてのサイトで CloudSec を無効にし、**[IANA 予約 UDP ポート（IANA Reserve UDP Port）]** オプションを有効にしてから、必要なサイトで CloudSec を再度有効にします。

CloudSec を構成するための詳細情報と手順については、『*ACI ファブリック用のNexus Dashboard Orchestrator 構成ガイド（Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics）*』の「CloudSec 暗号化」の章を参照してください。

ステップ 6 **[IPN デバイス情報]** を入力します。

オンプレミスとクラウドサイト間のサイト間接続を設定する予定がない場合は、この手順をスキップできます。

後のセクションで説明するように、オンプレミスとクラウドサイト間のサイトアンダーレイ接続を設定する場合は、クラウド CSR への接続を確立するオンプレミス IPN デバイスを選択する必要があります。これらのIPNデバイスは、オンプレミスサイトの設定画面で使用可能になる前に、ここで定義する必要があります。詳細はインフラの設定: オンプレミス サイトの設定 （178 ページ）を参照してください。

a) **[オンプレミス IPSec デバイス（On Premises IPSec Devices）]** タブを選択します。

b) **[+オンプレミス IPSec デバイスを追加（+Add On-Premises IPSec Device）]** をクリックします。

c) デバイスが**[管理対象外（Unmanaged）]**か**[管理対象（Managed）]**かを選択し、デバイス情報を提供します。

これは、デバイスが NDFC によって直接管理されるかどうかを定義します。

- **[管理対象（Managed）]** IPN デバイスにはシンプルにデバイスの**[名前（Name）]** と **[IP アドレス（IP Address）]** を入力してください。

  指定した IP アドレスは、IPN デバイスの管理 IP アドレスではなく、クラウド CSR からのトンネル ピア アドレスとして使用されます。

- **[管理対象（Managed）]** IPN デバイスには、デバイスが入っているNDFC **[サイト（Site）]** を選択し、そのサイトの **[デバイス（Device）]** を選択します。

  次に、インターネットに接続しているデバイスの**[インターフェイス（Interface）]**を選択し、インターネットに接続しているゲートウェイの IP アドレスである**[ネクスト ホップ（Next Hop）]** IP アドレスを指定します。

d) チェック マーク アイコンをクリックして、デバイス情報を保存します。
e) 追加する IPN デバイスについて、この手順を繰り返します。

ステップ 7 **[外部 デバイス（External Devices）]** 情報を入力します。

Cloud Network Controller サイトがない場合、このタブは UI に表示されません。

Multi-Site ドメインに Cloud Network Controller サイトがない場合、またはクラウド サイトとブランチ ルータまたはその他の外部デバイス間の接続を設定する予定がない場合は、この手順をスキップできます。

次の手順では、クラウドサイトからの接続を設定するブランチルータまたは外部デバイスに関する情報を指定する方法について説明します。

a) **[外部デバイス（External Devices）]** タブを選択します。

このタブは、Multi-Site ドメインに少なくとも 1 つのクラウドサイトがある場合にのみ使用できます。

b) **[外部デバイスの追加（Add External Device）]** をクリックします。

[外部デバイスの追加（Add External Device）] ダイアログが開きます。

c) デバイスの **[名前（Name）]**、**[IP アドレス（IP Address）]**、および **[BGP 自律システム番号（BGP Autonomous System Number）]** を入力します。

指定した IP アドレスは、デバイスの管理 IP アドレスではなく、Cloud Network Controller の CSR からのトンネル ピア アドレスとして使用されます。接続は、IPSec を使用してパブリック インターネット経由で確立されます。

d) チェック マーク アイコンをクリックして、デバイス情報を保存します。
e) 追加する IPN デバイスについて、この手順を繰り返します。

すべての外部デバイスを追加したら、次の手順を完了して、IPSec トンネル サブネット プールにこれらのトンネルに割り当てられる内部 IP アドレスを指定します。

ステップ 8 **[IPSecトンネル サブネット プール（IPSec Tunnel Subnet Pools）]** 情報を入力します。

Cloud Network Controller サイトがない場合、このタブは UI に表示されません。

ここで指定できるサブネットプールには、次の 2 つのタイプがあります。

- **外部サブネット プール**：クラウド サイトの CSR と他のサイト（クラウドまたはオンプレミス）間の接続に使用されます。

  これらは、Nexus Dashboard Orchestrator によって管理される大規模なグローバル サブネット プールです。Orchestrator は、これらのプールからより小さなサブネットを作成し、サイト間 IPsec トンネルと外部接続 IPsec トンネルで使用するサイトに割り当てます。

  1 つ以上のクラウド サイトから外部接続を有効にする場合は、少なくとも 1 つの外部サブネット プールを提供する必要があります。

- **サイト固有のサブネット プール**：クラウド サイトの CSR と外部デバイス間の接続に使用されます。

  これらのサブネットは、外部接続IPsecトンネルが特定の範囲内にあることが必要な場合に定義できます。たとえば、外部ルータにIPアドレスを割り当てるために特定のサブネットがすでに使用されており、それらのサブネットを NDO およびクラウド サイトの IPsec トンネルで引き続き使用する場合です。これらのサブネットはOrchestratorによって管理されず、各サブネットはサイト全体に割り当てられ、外部接続 IPsec トンネルにローカルで使用されます。

  名前付きサブネット プールを指定しない場合でも、クラウド サイトの CSR と外部デバイス間の接続を設定すると、外部サブネット プールが IP 割り当てに使用されます。.

（注）
両方のサブネット プールの最小マスク長は `/24` です。

1 つ以上の**外部サブネット プール**を追加するには：

a) **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** タブを選択します。
b) **[外部サブネット プール（External Subnet Pool）]** エリアで、**[+ IP アドレスの追加（+Add IP Address）]** をクリックして、1 つ以上の外部サブネット プールを追加します。

   このサブネットは、以前の Nexus Dashboard Orchestrator リリースでサイト間接続用に Cloud Network Controller で以前に設定した、オンプレミス接続に使用されるクラウド ルータの IPsec トンネル インターフェイスとループバックに対処するために使用されます。

   サブネットは、他のオンプレミス TEP プールと重複してはならず、`0.xxx` または `0.0.xx`で 始まってはならず、`/16` と `/24` の間のネットワーク マスク（`30.29.0.0/16` など）が必要です。

c) チェックマーク アイコンをクリックして、サブネット情報を保存します。
d) 追加するサブネット プールについて、これらのサブステップを繰り返します。

1 つ以上の **[サイト固有のサブネット プール（Site-Specific Subnet Pools）]** を追加するには：

a) **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** タブを選択します。
b) **[サイト固有のサブネット プール（Site-Specific Subnet Pools）]** エリアで、**[+ IP アドレスの追加（+Add IP Address）]** をクリックして、1 つ以上の外部サブネット プールを追加します。

   [名前付きサブネットプールの追加（Add Named Subnet Pool）] ダイアログが開きます。

c) サブネットの **[名前（Name）]** を入力します。

   後ほど、サブネットプールの名前を使用して、IP アドレスを割り当てるプールを選択できます。

d) **[+ IP アドレスの追加 (+ Add IP Address)]**をクリックして、1 つ以上のサブネット プールを追加します。

サブネットには /16 と /24 の間のネットワークが必要で、0.x.x.x または 0.0.x.x で始めることはできません。たとえば、30.29.0.0/16 のようにします。

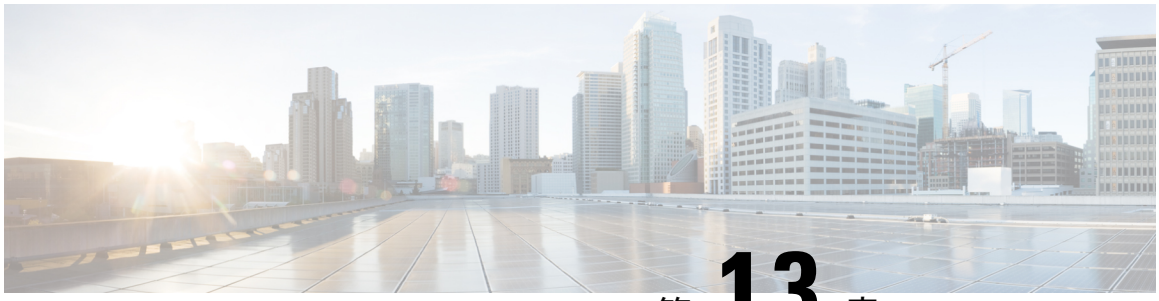
e) チェックマーク アイコンをクリックして、サブネット情報を保存します。

同じ名前付きサブネット プールに複数のサブネットを追加する場合は、この手順を繰り返します。

f) **[保存（Save）]** をクリックして、名前付きサブネット プールを保存します。
g) 追加する名前付きサブネット プールについて、これらのサブステップを繰り返します。

次のタスク

全般的なインフラ設定を構成した後も、管理するサイトのタイプ（ACI、Cloud Network Controller、またはNDFC）に基づいて、サイト固有の設定に関する追加情報を指定する必要があります。次の項で説明する手順に従って、サイト固有のインフラストラクチャ設定を行います。



第 13 章

Cisco APIC サイトのインフラの設定

サイト接続性情報の更新

スパインの追加や削除、またはスパイン ノードの ID 変更などのインフラストラクチャへの変更が加えられた場合、Multi-Site ファブリック接続サイトの更新が必要になります。このセクションでは、各サイトの APIC から直接最新の接続性情報を取得する方法を説明します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のサイトを選択します。

ステップ 5 メイン ウィンドウで、APIC からファブリック情報を取得するために **[更新 (Refresh)]** ボタンをクリックします。

ステップ 6 （オプション）オンプレミス サイトの場合、廃止されたスパイン スイッチノードの設定を削除する場合は、**[確認 (Confirmation)]** ダイアログでチェックボックスをオンにします。

このチェックボックスを有効にすると、現在使用されていないスパイン スイッチのすべての設定情報がデータベースから削除されます。

ステップ 7 最後に、**[はい (Yes)]** をクリックして確認し、接続情報をロードします。

これにより、新しいスパインや削除されたスパインを検出し、すべてのサイトに関連したファブリックの接続を APIC からインポートし直します。

インフラの設定: オンプレミス サイトの設定

ここでは、オンプレミスサイトにサイト固有のインフラ設定を構成する方法について説明します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のオンプレミス サイトを選択します。

ステップ 5 **[サイト間接続（Inter-Site Connectivity）]** 情報を入力します。

a) 右側の **<サイト *(Site)*> [設定 (Settings)]** ペインで、**[マルチサイト (Multi-Site)]** ノブを有効にします。

これは、オーバーレイ接続がこのサイトと他のサイト間で確立されるかどうかを定義します。

b) (オプション n) **[CloudSec 暗号化 (CloudSec Encryption)]** ノブを有効にして、サイトを暗号化します。

CloudSec 暗号化は、サイト間トラフィックの暗号化機能を提供します。この機能の詳細については、*Cisco Multi-Site Configuration Guide* の「Infrastructure Management」の章を参照してください。

c) **[オーバレイ マルチキャスト TEP (Overlay Multicast TEP)]** を指定します。

このアドレスは、サイト間の L2 BUM および L3 マルチキャスト トラフィックのために使用されます。この IP アドレスは、単一のポッドまたはマルチポッド ファブリックであるかどうかには関わりなく、同じファブリックの一部であるすべてのスパイン スイッチに展開されます。

このアドレスは、元のファブリックのインフラ TEP プールのアドレス空間または `0.x.x.x` の範囲から取得することはできません。

d) **[BGP 自律システム番号 (BGP Autonomous System Number)]** を指定します。

e) （オプション）**[BGP パスワード (BGP Password)]** を指定します。

f) **[OSPF エリア ID (OSPF Area ID)]** を入力します。

サイトと IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの設定は、インフラの設定: スパイン スイッチ （182 ページ）で説明されているように、ポート レベルで行われます。

g) ドロップダウン メニューから **[OSPF エリア タイプ (OSPF Area Type)]**を選択します。

サイトと IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの設定は、インフラの設定: スパイン スイッチ （182 ページ）で説明されているように、ポート レベルで行われます。

OSPF エリアタイプは、次のいずれかになります。

- `nssa`
- `regular`

h) サイトの OSPF ポリシーを設定します。

サイトと IPN 間のアンダーレイ接続に OSPF プロトコルを使用する場合は、次の設定が必要です。代わりに BGP を使用する場合は、この手順を省略できます。BGP アンダーレイの設定は、インフラの設定: スパイン スイッチ （182 ページ）で説明されているように、ポート レベルで行われます。

既存のポリシー (たとえば `msc-ospf-policy-default`) をクリックして修正することも、**[+ ポリシー追加(+Add Policy)]** をクリックして新しい OSPF ポリシーを追加することもできます。それから、**[ポリシーの追加/更新(Add/Update Policy)]** ウィンドウで、以下を指定します。

- **[ポリシー名（Policy Name）]** フィールドにポリシー名を入力します。
- **[(ネットワーク タイプ (Network Type)]** フィールドで、`[ブロードキャスト (broadcast)]`、`[ポイントツーポイント (point-to-point)]`、または `[未指定 (unspecified)]` のいずれかを選択します。

  デフォルトは `[ブロードキャスト (broadcast)]` です。
- **[優先順位 (Priority)]** フィールドに、優先順位番号を入力します。

  デフォルトは `1` です。
- **[インターフェイスのコスト (Cost of Interface)]** フィールドに、インターフェイスのコストを入力します。

  デフォルト値は `0` です。
- **[インターフェイス コントロール(Interface Controls)]** ドロップダウン メニューで、以下のいずれかを選択します。
  - **アドバタイズサブネット (advertise-subnet)**
  - **BFD (bfd)**
  - **MTU 無視 (mtu-ignore)**
  - **受動的参加 (passive-participation)**
- **[Hello 間隔 (秒) (Hello Interval (Seconds))]** フィールドに、hello 間隔を秒単位で入力します。

  デフォルト値は `10` です。
- **[Dead 間隔 (秒) (Dead Interval (Seconds))]** フィールドに、dead 間隔を秒単位で入力します。

  デフォルト値は `40` です。

- **[再送信間隔 (秒) (Retransmit Interval (Seconds))]** フィールドに、再送信間隔を秒単位で入力します。

  デフォルト値は 5 です。

- **[転送遅延 (秒) (Transmit Delay (Seconds))]** フィールドに、遅延を秒単位で入力します。

  デフォルトは 1 です。

i) （オプション）**[外部ルート ドメイン (External Routed Domain)]** ドロップダウンから、使用するドメインを選択します。

Cisco APIC GUI で作成した外部ルータ ドメインを選択します。使用している APIC リリースに固有の詳細については、『*Cisco APIC Layer 3 Networking Configuration Guide*』を参照してください。

j) （オプション）サイトの **[SDA 接続（SDA Connectivity）]**を有効にします。

サイトが SDA ネットワークに接続されている場合は、**SDA 接続**ノブを有効にして、**外部ルーテッド ドメイン**、**VLAN プール**、および **VRF Lite IP プール範囲**の情報を提供します。

サイトの SDA 接続を有効にする場合は、『*Cisco Multi-Site Configuration Guide for ACI Fabrics*』の「SDA 使用例」の章で説明されている追加構成を行う必要があります。

k) （オプション）サイトの **[SR-MPLS 接続 (SR-MPLS Connectivity)]**を有効にします。

サイトが MPLS ネットワークを介して接続されている場合には、**[SR-MPLS 接続性 (SR-MPLS Connectivity)]** ノブを有効にして、セグメント ルーティング グローバル ブロック (SRGB) の範囲を指定します。

セグメント ルーティング グローバル ブロック（SRGB）は、ラベル スイッチング データベース (LSD) でセグメント ルーティング (SR) 用に予約されているラベル値の範囲です。これらの値は SR 対応ノードへのセグメント識別子（SID）として割り当てられ、ドメイン全体でグローバルな意味を持ちます。

デフォルトの範囲は 16000 ～ 23999 です。

サイトのMPLS接続を有効にする場合は、『*Cisco Multi-Site Configuration Guide for ACI Fabrics*』の「Sites Connected via SR-MPLS」の章で説明されている追加設定を行う必要があります。

ステップ 6 オンプレミスとクラウド サイト間のサイト間接続を設定します。

オンプレミス サイトとクラウドサイトの間にサイト間接続を作成する必要がない場合（たとえば、導入にクラウドのみまたはオンプレミス サイトのみが含まれる場合）は、この手順をスキップします。

オンプレミスとクラウド サイト間のアンダーレイ接続を設定する場合は、Cloud Network Controller の CSR がトンネルを確立する IPN デバイスの IP アドレスを指定し、クラウド サイトのインフラ設定を行う必要があります。

a) **[+ IPN デバイスの追加 (+ Add IPN Device)]** をクリックして、IPNデバイスを指定します。

b) ドロップダウンから、前に定義した IPN デバイスのいずれかを選択します。

IPNデバイスは、**[一般設定 (General Settings)]** > **[IPN デバイス (IPN Devices)]**リストですでに定義されている必要があります。 インフラの設定: 一般設定 （172 ページ）を参照してください。

c) クラウド サイトのサイト間接続を設定します。

クラウド サイトからこのオンプレミス サイトへの以前に設定された接続はすべてここに表示されますが、追加の設定は、Cisco Cloud Network Controller サイトのインフラの構成 （185 ページ）の説明に従ってクラウド サイト側から行う必要があります。

次のタスク

必要なサイト間接続情報をすべて設定しましたが、まだサイトにプッシュされていません。インフラ設定の展開 （189 ページ）の説明に従って、設定を展開する必要があります。

インフラの設定: ポッドの設定

このセクションでは、各サイトでポッド固有の設定を行う方法について説明します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のサイトを選択します。

ステップ 5 メイン ウィンドウで、ポッドを選択します。

ステップ 6 右の **[ポッドのプロパティ (Pod Properties)]** ペインで、ポッドについてオーバーレイ ユニキャスト TEP を追加できます。

この IP アドレスは、同じポッドの一部であるすべてのスパイン スイッチに展開され、レイヤ 2 およびレイヤ 3 ユニキャスト通信用の VXLAN カプセル化トラフィックの送信と受信に使用されます。

ステップ 7 **[+ TEP プールの追加 (+Add TEP Pool)]** をクリックして、ルーティング可能な TEP プールを追加します。

外部ルーティング可能な TEP プールは、IPN 経由でルーティング可能な IP アドレスのセットを APIC ノード、スパイン スイッチ、および境界リーフ ノードに割り当てるために使用されます。これは、Multi-Site アーキテクチャを有効にするために必要です。

以前に APIC でファブリックに割り当てられた外部 TEP プールは、ファブリックが Multi-Site ドメインに追加されると、NDO によって自動的に継承され、GUI に表示されます。

ステップ 8 サイトの各ポッドに対してこの手順を繰り返します。

インフラの設定: スパイン スイッチ

このセクションでは、Cisco Multi-Siteのために各サイトのスパイン スイッチを設定する方法について説明します。スパイン スイッチを設定する場合、各サイトのスパインと ISN 間の接続を設定することで、Multi-Site ドメイン内のサイト間のアンダーレイ接続を効果的に確立できます。

リリース 3.5(1) より前は、OSPF プロトコルを使用してアンダーレイ接続が確立されていました。一方、このリリースでは、OSPF、BGP（IPv4 のみ）、または混合プロトコルを使用できます。混合とは、一部のサイトではサイト間アンダーレイ接続に OSPF を使用し、一部のサイトでは BGP を使用することです。両方ではなく OSPF または BGP のいずれかを設定することを推奨します。両方のプロトコルを設定した場合には、BGP が優先され、OSPF はルートテーブルにインストールされません。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト（Sites）]** の下で、特定のオンプレミス サイトを選択します。

ステップ 5 メイン ペインで、ポッド内のスパイン スイッチを選択します。

ステップ 6 右側の **[<スパイン> 設定 (Settings)]** ペインで、**[+ ポート追加(Add Port)]** をクリックします。

ステップ 7 **[ポートの追加 (Add Port)]** ウィンドウで、アンダーレイの接続情報を入力します。

IPN 接続用に APIC で直接設定されているポートがインポートされ、リストに表示されます。NDO から設定する新しいポートについては、次の手順を使用します。

a) 次の一般情報を指定します。

- **[イーサネット ポート ID (Ethernet Port ID)]** フィールドに、ポート ID、たとえば `1/29` を入力します。

  これは、IPN への接続に使用されるインターフェイスです。

- **[IP アドレス (IP Address)]** フィールドに、IP アドレス/ネットマスクを入力します。

  Orchestrator によって、指定された IP アドレスを持ち、指定されたポートを使用する、VLAN 4 のサブインターフェイスが作成されます。

- **[MTU]** フィールドに、サーバの MTU を入力します。MTUを9150Bに設定する継承を指定するか、`576` ー `9000` の値を選択します。

  スパイン ポートの MTU は、IPN 側の MTU と一致させる必要があります。

ステップ 8 アンダーレイ プロトコルを選択します。

a) アンダーレイ接続に OSPF プロトコルを使用する場合は、**[OSPF]** を設定します。

代わりに、アンダーレイ接続に BGP プロトコルを使用する場合は、この部分をスキップし、次のサブステップで必要な情報を入力します。

- **[OSPF]** を [有効 (Enabled)] に設定します。

  OSPF 設定が使用可能になります。

- **[OSPF ポリシー (OSPF Policy)]** ドロップダウンで、インフラの設定: オンプレミス サイトの設定（178 ページ） で設定したスイッチの OSPF ポリシーを選択します。

  OSPF ポリシーの OSPF 設定は、IPN 側と一致させる必要があります。

- **[OSPF 認証 (OSPF Authentication)]** では、[なし (none)] または以下のいずれかを選択します。
  - MD5
  - Simple

- **[BGP]** を [無効 (Disabled)] に設定します。

b) アンダーレイ接続に BGP プロトコルを使用する場合は、**[BGP]** を有効にします。

アンダーレイ接続に OSPF プロトコルを使用しており、前のサブステップですでに設定している場合は、この部分をスキップします。

（注）
次の場合、BGP IPv4 アンダーレイはサポートされません。

- マルチサイト ドメインに 1 つ以上の Cloud Network Controller サイトが含まれている場合、オンプレミスからオンプレミスおよびオンプレミスからクラウド サイトの両方のサイト間アンダーレイ接続に OSPF プロトコルを使用する必要があります。
- いずれかのファブリックの WAN 接続に GOLF（ファブリック WAN のレイヤ 3 EVPN サービス）を使用している場合。

上記の場合、スパインに展開された Infra L3Out で OSPF を使用する必要があります。

- **[OSPF]** を [無効 (Disabled)] に設定します。

  両方ではなく OSPF または BGP のいずれかを設定することを推奨します。両方のプロトコルを設定した場合には、BGP が優先され、OSPF はルート テーブルにインストールされません。ISN デバイスとの EBGP 隣接関係だけがサポートされるからです。

- **[BGP]** を [有効 (Enabled)] に設定します。

  BGP 設定が使用可能になります。

- **[ピア IP (Peer IP)]** フィールドに、このポートの BGP ネイバーの IP アドレスを入力します。

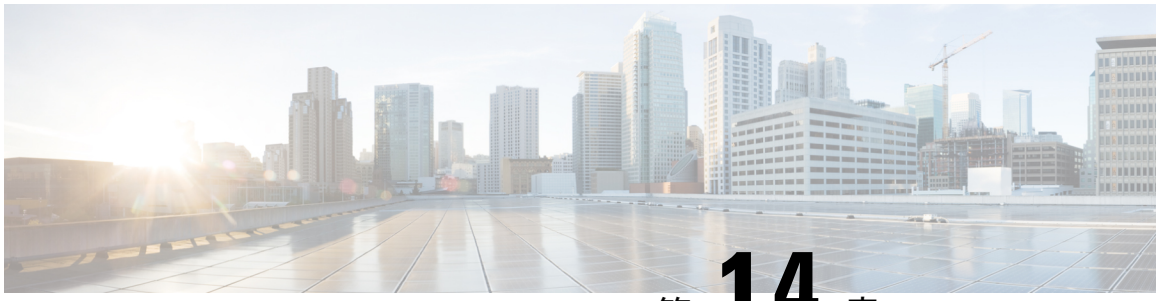
  BGP アンダーレイ接続では、IPv4 IP アドレスのみがサポートされます。

- **[ピア AS 番号 (Peer AS Number)]** フィールドに、BGP ネイバーの自律システム（AS）番号を入力します。

  このリリースでは、ISN デバイスとの EBGP 隣接関係のみがサポートされます。

- **[BGP パスワード (BGP Password)]** フィールドに、BGP ピア パスワードを入力します。
- 必要に応じて追加のオプションを指定します。
  - [双方向フォワーディング検出 (Bidirectional Forwarding Detection)]：双方向フォワーディング検出（BFD）プロトコルを有効にして、このポートと IPN デバイスの物理リンクの障害を検出します。
  - [管理状態 (Admin State)]：ポートの管理状態を有効に設定します。

ステップ 9 IPN に接続するすべてのスパイン スイッチおよびポートに対してこの手順を繰り返します。



第 14 章

Cisco Cloud Network Controller サイトのインフラの構成

クラウド サイト接続性情報の更新

CSR やリージョンの追加や削除などのインフラストラクチャの変更には、Multi-Site ファブリック接続サイトの更新が必要です。このセクションでは、各サイトの APIC から直接最新の接続性情報を取得する方法を説明します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のサイトを選択します。

ステップ 5 メインウィンドウで **[更新 (Refresh)]** ボタンをクリックして、新規または変更されたCSRおよびリージョンを検出します。

ステップ 6 最後に、**[はい (Yes)]** をクリックして確認し、接続情報をロードします。

これにより、新規または削除された CSR およびリージョンが検出されます。

ステップ 7 **[導入 (Deploy)]** をクリックして、クラウドサイトの変更を、接続している他のサイトに伝達します。

クラウドサイトの接続を更新し、CSR またはリージョンが追加または削除された後、インフラ設定を展開して、そのクラウドサイトへのアンダーレイ接続がある他のサイトが更新された設定を取得する必要があります。

インフラの設定: クラウド サイトの設定

ここでは、Cloud Network Controller サイト固有のインフラ設定を構成する方法について説明します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のクラウド サイトを選択します。

ステップ 5 **[サイト間接続（Inter-Site Connectivity）]** 情報を入力します。

a) 右側の ***[<Site>* 設定 (Settings)]** ペインで、**[サイト間接続 (Inter-Site Connectivity)]** タブを選択します。

b) **マルチサイト** ノブを有効にします。

これは、オーバーレイ接続がこのサイトと他のサイト間で確立されるかどうかを定義します。

オーバーレイ構成は、次の手順で説明するようにアンダーレイ サイト間接続が確立されていないサイトにはプッシュされないことに注意してください。

c) （オプション）**[BGP パスワード (BGP Password)]** を指定します。

ステップ 6 サイト固有の **[サイト間接続 (Inter-Site Connectivity)]** 情報を入力します。

a) クラウド サイトの右側のプロパティ サイドバーで、**[サイトの追加]** をクリックします。

[サイトの追加（Add Site）] ウィンドウが表示されます。

b) **[サイトへの接続]** で、**[サイトの選択]** をクリックし、構成しているサイト (たとえば、 `Site1`) からの接続を確立するサイト (たとえば、 `Site2`) を選択します。

リモート サイトを選択すると、[サイトの追加（Add Site）] ウィンドウが更新され、両方向の接続が反映されます : [サイト1（Site1）] > [サイト2（Site2）] および [サイト2（Site2）] > [サイト1（Site1）]。

c) [サイト1（Site1）] > [サイト2（Site2）] エリアで、[接続タイプ（Connection Type）] ドロップダウンから、サイト間の接続のタイプを選択します。

次のオプションを使用できます。

- `[パブリックインターネット (Public Internet)]` : 2 つのサイト間の接続は、インターネットを介して確立されます。

  このタイプは、任意の 2 つのクラウド サイト間、またはクラウド サイトとオンプレミス サイト間でサポートされます。

- `[プライベート接続 (Private Connection)]` : 2 つのサイト間のプライベート接続を使用して接続が確立されます。

このタイプは、クラウド サイトとオンプレミス サイトの間でサポートされます。

- [クラウド バックボーン (Cloud Backbone)]：クラウドバックボーンを使用して接続が確立されます。

  このタイプは、Azure-to-AzureやAWS-to-AWSなど、同じタイプの 2 つのクラウド サイト間でサポートされます。

複数のタイプのサイト（オンプレミス、AWS、Azure）がある場合、サイトの異なるペアは異なる接続タイプを使用できます。

d) これら 2 つのサイト間の接続に使用する**プロトコル**を選択します。

BGP-EVPN 接続を使用している場合は、オプションで **IPSec** を有効にして、使用する Internet Key Exchange (IKE) プロトコルのバージョンを選択できます。構成に応じて、IKEv1 (バージョン 1) または IKEv2 (バージョン 1) です。

- パブリック インターネット接続の場合、IPsec は常に有効です。
- クラウド バックボーン接続の場合、IPsec は常に無効です。
- プライベート接続の場合、IPsec は有効または無効にすることができます。

代わりに **BGP-IPv4** 接続を使用する場合は、構成しているクラウド サイトからのルート リーク構成に使用される外部 VRF を提供する必要があります。

Site1 > Site2 の接続情報が提供された後、**Site2 > Site1** 領域は、反対方向の接続情報を反映します。

e) **[保存 (Save)]** をクリックして、設定を保存します。

Site1 から Site2 への接続情報を保存すると、Site2 から Site1 へのリバース接続が自動的に作成されます。これは、他のサイトを選択し、右側のサイドバーにある **[サイト間接続（Inter-site Connectivity）]** 情報を選択することで確認できます。

f) 他のサイトのサイト間接続を追加するには、この手順を繰り返します。

Site1 から Site2 へのアンダーレイ接続を確立すると、リバース接続が自動的に行われます。

ただし、Site1 から Site3 へのサイト間接続も確立する場合は、そのサイトに対してもこの手順を繰り返す必要があります。

ステップ 7 **[外部接続 (External Connectivity)]** 情報を入力します。

NDOによって管理されていない外部サイトまたはデバイスへの接続を設定する予定がない場合は、この手順をスキップできます。

外部接続のユース ケースの詳細な説明は、「*Nexus Dashboard Orchestrator* を使用したクラウド *CSR* からの外部接続の設定」ドキュメントで入手できます。

a) 右側の ***[<Site> 設定 (Settings)]*** ペインで、**[外部接続 (External Connectivity)]** タブを選択します。
b) **[外部接続の追加 (Add External Connectivity)]** をクリックします。

[外部接続の追加 (Add External Connectivity)] ダイアログが開きます。

c) **[VRF]** ドロップダウンから、外部接続に使用する VRF を選択します。

これは、クラウド ルートをリークするために使用される VRF です。**[リージョン (Regions)]** セクションには、この設定を適用する CSR を含むクラウド リージョンが表示されます。

d) **[外部デバイス (External Devices)]** セクションの **[名前 (Name)]** ドロップダウンから、外部デバイスを選択します。

これは、一般的なインフラストラクチャ設定時に**[一般設定 (General Settings)]** > **[外部デバイス (External Devices)]** リストに追加した外部デバイスであり、インフラの設定: 一般設定 （172 ページ）の説明に従ってすでに定義されている必要があります。

e) **[トンネル IKE バージョン (Tunnel IKE Version)]** ドロップダウンから、クラウド サイトの CSR と外部デバイス間の IPSec トンネルの確立に使用する IKE バージョンを選択します。

f) （任意）**[トンネル サブネット プール (Tunnel Subnet Pool)]** ドロップダウンから、名前付きサブネット プールのいずれかを選択します。

名前付きサブネット プールは、クラウド サイトの CSR と外部デバイス間の IPSec トンネルに IP アドレスを割り当てるために使用されます。ここで**名前付き**サブネット プールを指定しない場合、**外部**サブネット プールが IP 割り当てに使用されます。

外部デバイス接続用の専用サブネット プールを提供することは、特定のサブネットがすでに外部ルータに IP アドレスを割り当てるために使用されており、それらのサブネットを NDO およびクラウド サイトのIPSecトンネルに引き続き使用する場合に役立ちます。

この接続に特定のサブネット プールを提供する場合は、インフラの設定: 一般設定 （172 ページ）の説明に従って作成済みである必要があります。

g) （オプション）**[事前共有キー (Pre-Shared Key)]** フィールドに、トンネルの確立に使用するカスタム キーを入力します。

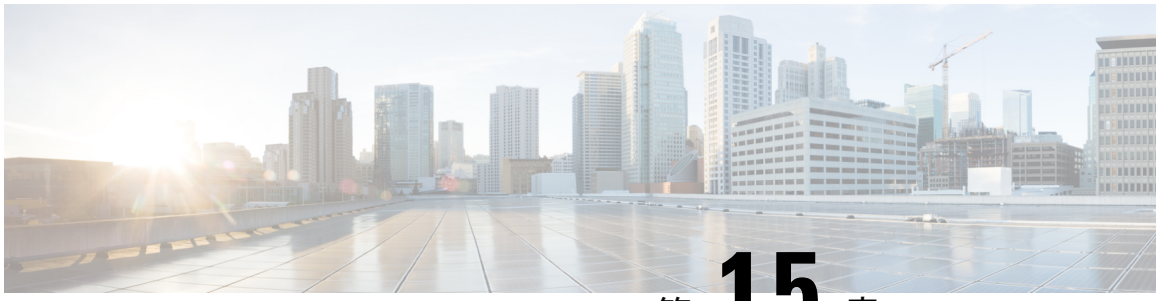
h) 必要に応じて、同じ外部接続（同じ VRF ）に対して追加する外部デバイスについて、前のサブステップを繰り返します。

i) 必要に応じて、追加の外部接続（異なる VRF ）に対してこの手順を繰り返します。

CSR と外部デバイス間のトンネルエンドポイントには 1 対 1 の関係があるため、異なる VRF を使用して追加の外部接続を作成できますが、同じ外部デバイスに追加の接続を作成することはできません。

次のタスク

必要なサイト間接続情報をすべて設定しましたが、まだサイトにプッシュされていません。インフラ設定の展開 （189 ページ）の説明に従って、設定を展開する必要があります。



第 15 章

ACI サイト向けのインフラ設定の展開

インフラ設定の展開

ここでは、各 APIC サイトにインフラ設定を展開する方法について説明します。

手順

ステップ 1 メインペインの右上にある **[展開 (deploy)]** をクリックして、設定を展開します。

オンプレミスまたはクラウドサイトのみを設定した場合は、**[展開 (Deploy)]** をクリックしてインフラ設定を展開します。

ただし、オンプレミスとクラウド サイトの両方がある場合は、次の追加オプションを使用できます。

- **[展開 & IPN デバイス設定ファイルをダウンロード (Deploy & Download IPN Device config files):]** オンプレミスの APIC サイトと Cloud Network Controller サイトの両方に設定をプッシュし、オンプレミスとクラウド サイト間のエンドツーエンド インターコネクトを有効にします。

  さらに、このオプションでは、IPN デバイスから Cisco クラウド サービス ルータ（CSR）への接続できるようにするための設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

- **[展開 & IPN デバイス設定ファイルをダウンロード (Deploy & Download IPN Device config files):]** 両方の Cloud Network Controller サイトに設定をプッシュし、クラウド サイトと外部デバイス間のエンドツーエンド インターコネクトを有効にします。

  さらに、このオプションでは、外部デバイスから、自分のクラウドサイトに展開された Cisco クラウドサービス ルータ（CSR）へ接続できるようにするための、設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

- **[IPN デバイス設定ファイルのみをダウンロード (Download IPN Device config files only):]** 構成情報を含む zip ファイルをダウンロードします。これは、IPN デバイスから Cisco Cloud Services Router（CSR）への接続を、構成を展開することなく可能にするために用いるものです。
- **[外部デバイス設定ファイルのみをダウンロード (Download External Device config files only):]** 構成情報を含む zip ファイルをダウンロードします。これは、外部デバイスから Cisco Cloud Services Router（CSR）への接続を、構成を展開することなく可能にするために用いるものです。

ステップ 2 確認ウィンドウで **[はい (Yes)]** をクリックします。

`[展開が開始されました。個々のサイトの展開ステータスメッセージについては、左側のメニューを参照してください (Deployment started, refer to left menu for individual site deployment status)]` というメッセージにより、インフラ構成の展開が開始されたことが示されます。左側のペインのサイト名の横に表示されるアイコンで、各サイトの進行状況を確認できます。

次のタスク

インフラ オーバーレイとアンダーレイの構成設定が、すべてのサイトのコントローラとクラウドCSR に展開されます。残った最後の手順では、サイト接続性情報の更新（177 ページ）で説明するように、IPN デバイスをクラウド CSR のトンネルを使用して設定します。

オンプレミスとクラウド サイト間の接続の有効化

オンプレミス サイトまたはクラウド サイトのみがある場合は、このセクションをスキップできます。

ここでは、オンプレミス APIC サイトと Cloud Network Controller サイト間の接続を有効にする方法について説明します。

デフォルトでは、Cisco Cloud Network Controller は冗長 Cisco Cloud サービス ルータ 1000v のペアを展開します。この項の手順では、2つのトンネルを作成します。1つはオンプレミスの IPsec デバイスからこれらの各 Cisco Cloud サービス ルータ 1000v 対する IPsec トンネルです。複数のオンプレミス IPsec デバイスがある場合は、各オンプレミスデバイスの CSR に同じトンネルを設定する必要があります。

次の情報は、オンプレミスの IPsec ターミネーション デバイスとして Cisco Cloud サービス ルータ 1000v のコマンドを提供します。別のデバイスまたはプラットフォームを使用している場合は、同様のコマンドを使用します。

手順

ステップ 1 クラウド サイトに導入された CSR とオンプレミスの IPsec ターミネーション デバイスとの間の接続を有効にするために必要な必要な情報を収集します。

インフラ設定の展開 （189 ページ）の手順の一部として、Nexus Dashboard Orchestrator の **[IPN デバイス設定ファイルの展開とダウンロード (Deploy & Download IPN Device config files)]** オプションまたは **[IPN デバイス設定ファイルのダウンロード (IPN Device config files only)]** オプションを使用して、必要な設定の詳細を取得できます。

ステップ 2 オンプレミスの IPsec デバイスにログインします。

ステップ 3 最初の CSR のトンネルを設定します。

最初の CSR の詳細は、Nexus Dashboard Orchestrator からダウンロードした ISN デバイスのコンフィギュレーションファイルで確認できますが、次のフィールドには、特定の展開の重要な値が示されます。

- <*first-csr-tunnel-ID*>：このトンネルに割り当てる一意のトンネル ID です。
- <*first-csr-ip-address*>：最初の CSR の 3 番目のネットワーク インターフェイスのパブリック IP アドレスです。

  トンネルの宛先は、アンダーレイ接続のタイプによって異なります。

  - アンダーレイがパブリック インターネット経由の場合、トンネルの宛先はクラウド ルータ インターフェイスのパブリック IP です。
  - アンダーレイがプライベート接続（AWS の DX や Azure の ER など）を介している場合、トンネルの宛先はクラウド ルータ インターフェイスのプライベート IP です。

- <*first-csr-preshared-key*>：最初の CSR の事前共有キーです。
- <*onprem-device-interface*> は、Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000v への接続に使用されるインターフェイスです。
- <*onprem-device-ip-address*> は、Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000v への接続に使用される <*interface*> インターフェイスです。
- <*peer-tunnel-for-onprem-IPsec-to-first-CSR*>：最初のクラウド CSR に対してオンプレミスの IPsec デバイスのピア トンネル IP アドレスとして使用されます。
- <*process-id*> ：OSPF プロセス ID です。
- <*area-id*>：OSPF エリア ID です。

次の例は、Nexus Dashboard Orchestrator リリース 3.3(1) および Cloud Network Controller リリース 5.2(1) 以降でサポートされている IKEv2 プロトコルを使用したサイト間接続設定を示しています。IKEv1 を使用している場合は、NDO からダウンロードした IPN 設定ファイルの外観が若干異なる場合がありますが、原則は同じです。

```
crypto ikev2 proposal ikev2-proposal-default
    encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
    integrity sha512 sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-policy-default
    proposal ikev2-proposal-default
exit
```

```
crypto ikev2 keyring key-ikev2-infra:overlay-1-<first-csr-tunnel-id>
    peer peer-ikev2-keyring
        address <first-csr-ip-address>
        pre-shared-key <first-csr-preshared-key>
    exit
exit

crypto ikev2 profile ikev2-infra:overlay-1-<first-csr-tunnel-id>
    match address local interface <onprem-device-interface>
    match identity remote address <first-csr-ip-address> 255.255.255.255
    identity local address <onprem-device-ip-address>
    authentication remote pre-share
    authentication local pre-share
    keyring local key-ikev2-infra:overlay-1-<first-csr-tunnel-id>
    lifetime 3600
    dpd 10 5 on-demand
exit

crypto ipsec transform-set infra:overlay-1-<first-csr-tunnel-id> esp-gcm 256
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<first-csr-tunnel-id>
    set pfs group14
    set ikev2-profile ikev2-infra:overlay-1-<first-csr-tunnel-id>
    set transform-set infra:overlay-1-<first-csr-tunnel-id>
exit

interface tunnel 2001
    ip address <peer-tunnel-for-onprem-IPsec-to-first-CSR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <onprem-device-interface>
    tunnel destination <first-csr-ip-address>
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-<first-csr-tunnel-id>
    ip mtu 1400
    ip tcp adjust-mss 1400
    ip ospf <process-id> area <area-id>
    no shut
exit
```

例：

```
crypto ikev2 proposal ikev2-proposal-default
    encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
    integrity sha512 sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-policy-default
    proposal ikev2-proposal-default
exit

crypto ikev2 keyring key-ikev2-infra:overlay-1-2001
    peer peer-ikev2-keyring
        address 52.12.232.0
        pre-shared-key 144904725321902286651389219409672714611O
    exit
exit

crypto ikev2 profile ikev2-infra:overlay-1-2001
    ! Please change GigabitEthernet1 to the appropriate interface
    match address local interface GigabitEthernet1
    match identity remote address 52.12.232.0 255.255.255.255
    identity local address 128.107.72.62
```

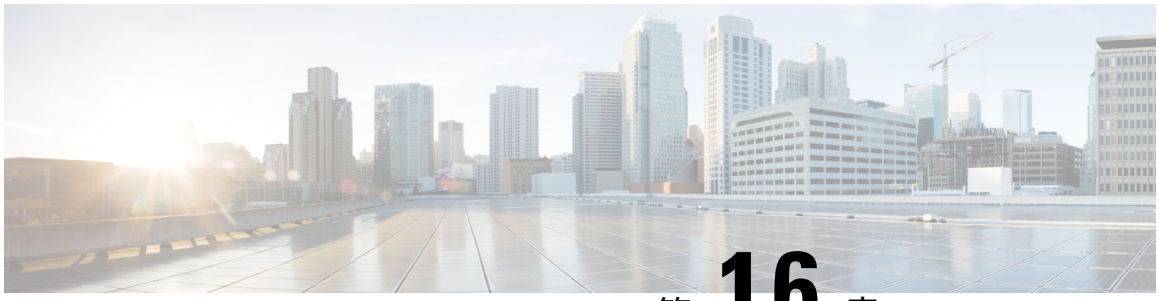
```
    authentication remote pre-share
    authentication local pre-share
    keyring local key-ikev2-infra:overlay-1-2001
    lifetime 3600
    dpd 10 5 on-demand
exit

crypto ipsec transform-set infra:overlay-1-2001 esp-gcm 256
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-2001
    set pfs group14
    set ikev2-profile ikev2-infra:overlay-1-2001
    set transform-set infra:overlay-1-2001
exit

! These tunnel interfaces establish point-to-point connectivity between the on-prem device and the
 cloud Routers
! The destination of the tunnel depends on the type of underlay connectivity:
! 1) The destination of the tunnel is the public IP of the cloud Router interface if the underlay
is via internet
! 2) The destination of the tunnel is the private IP of the cloud Router interface if the underlay
 is via private
     connectivity like DX on AWS or ER on Azure

interface tunnel 2001
    ip address 5.5.1.26 255.255.255.252
    ip virtual-reassembly
    ! Please change GigabitEthernet1 to the appropriate interface
    tunnel source GigabitEthernet1
    tunnel destination 52.12.232.0
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-2001
    ip mtu 1400
    ip tcp adjust-mss 1400
    ! Please update process ID according with your configuration
    ip ospf 1 area 0.0.0.1
    no shut
exit
```

ステップ 4 2 番目、および設定する必要があるその他の CSR について、これらの手順を繰り返します。

ステップ 5 オンプレミスの IPsec デバイスでトンネルがアップしていることを確認します。

現在のステータスを表示するには、次のコマンドを使用します。両方のトンネルがアップとして表示されていない場合は、この項の手順で入力した情報を確認して、問題が発生している可能性がある場所を確認します。両方のトンネルがアップとして表示されるまで、次のセクションに進まないでください。

```
ISN_CSR# show ip interface brief | include Tunnel
Interface              IP-Address      OK? Method Status                Protocol
Tunnel1000             30.29.1.2         YES manual up                    up
Tunnel1001             30.29.1.4         YES manual up                    up
```



第 16 章

CloudSec 暗号化

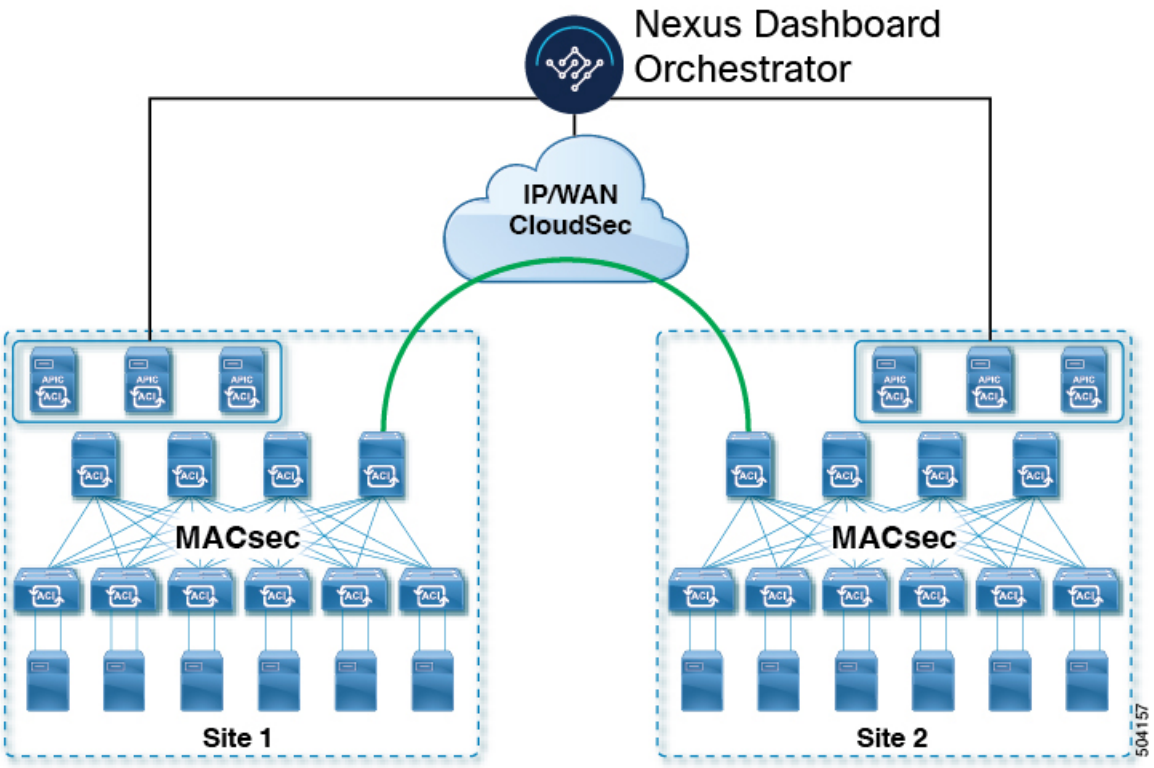
Cisco ACI CloudSec 暗号化

ほとんどの Cisco ACI 展開で、ディザスタリカバリとスケーリングに対処する Multi-Site アーキテクチャを採用しているため、ローカルサイト内で MACsec 暗号化を使用する現在のセキュリティ実装は、複数のサイトにわたるデータセキュリティと整合性を保証するには不十分になっています。それらのサイトは、安全でない外部 IP ネットワークによって接続されており、個別のファブリックを相互接続しているからです。Nexus Dashboard Orchestrator リリース 2.0(1) は、トラフィックのサイト間暗号化を提供するために設計された CloudSec 暗号化を導入しています。

Multi-Site トポロジはサイト間の接続を提供するために、3 つのトンネル エンドポイント (TEP) IP アドレス（Overlay Multicast TEP、Overlay Unicast TEP、および External TEP Pool）を使用します。これらの TEP アドレスは、 Nexus Dashboard Orchestrator の管理者により設定され、各サイトの Cisco APIC にプッシュ ダウンされ、その後スパイン スイッチで設定されます。これらの 3 つのアドレスは、トラフィックがリモートサイトに送信されるタイミングを決定するために使用されます。この場合、2 つのスパイン スイッチ間に暗号化された CloudSec トンネルが作成され、サイト間ネットワーク (ISN) を介して 2 つのサイト間の物理接続が提供されます。

次の図は、ローカルサイト トラフィックの MACsec とサイト間トラフィックの暗号化に CloudSec を組み合わせた全体的な暗号化アプローチを示しています。

図 *11 : CloudSec* 暗号化



要件と注意事項

CloudSec 暗号化を設定する場合は、次の注意事項が適用されます。

- CloudSec は、Nexus 9000 サイト間ネットワーク（ISN）インフラストラクチャを使用して検証されています。ISN インフラストラクチャがさまざまなデバイスで構成されている場合、またはデバイスが不明な場合（サービスプロバイダーから購入した回線の場合など）、ASR1K ルーターは、ACI スパイン（各サイトに展開された ASR1K デバイスの個別のペアを使用）、または Nexus 9000 ISN ネットワークに直接接続するファースト ホップ デバイスである必要があります。パディング フィックスアップが有効になっている ASR1K ルーターにより、CloudSec トラフィックはサイト間の任意の IP ネットワークを通過できます。

  ASR1K ルーターを構成するには：

  1. デバイスにログインします。
  2. UDP ポートを構成します。

（注）
- リリース 3.7（1）以降を実行していて、IANA が割り当てたポート「8017」を使用するように CloudSec を構成する場合は、代わりに次のコマンドでそのポートを指定します。
- ASR1K ルータで **platform cloudsec padding-fixup** コマンドを実行するには、Advanced Enterprise ライセンスまたは Advanced IP Services ライセンスが必要です。

```
ASR1K(config)# platform cloudsec padding-fixup dst-udp-port 9999
```

3. 設定を確認します。

次の出力で、前の手順で構成したポート（8017 または 9999）が表示されていることを確認します。

```
ASR1K# show platform software ip rp active cloudsec
  CloudSec Debug: disabled
  CloudSec UDP destination port: enabled
  1st UDP destination port: 9999
  2nd UDP destination port: 0
  3rd UDP destination port: 0

ASR1K# show platform software ip fp active cloudsec
  CloudSec Debug: disabled
  CloudSec UDP destination port: enabled
  1st UDP destination port: 9999
  2nd UDP destination port: 0
  3rd UDP destination port: 0
```

- CloudSec暗号化を無効にしようとしたときに1つ以上のスパインスイッチがダウンした場合、スイッチがアップするまで、これらのスイッチでディセーブルプロセスは完了しません。これにより、スイッチが再起動したときにパケットがドロップされることがあります。

  CloudSec暗号化を有効または無効にする前に、ファブリック内のすべてのスパインスイッチが稼働していること、または完全に停止していることを確認することを推奨します。

- Nexus Dashboard Orchestrator リリース 3.7(1) 以降では、IANA が割り当てたポートを使用するように CloudSec 暗号化を構成できます。

  デフォルトでは、CloudSec は独自の UDP ポートを使用します。Orchestrator リリース 3.7(1) 以降は、サイト間の CloudSec 暗号化に IANA が予約した公式ポート 8017 を使用するように構成できます。

（注） IANA 予約ポートは、リリース 5.2(4) 以降を実行している Cisco APIC サイトでサポートされています。

この設定を変更するには、すべてのサイトで CloudSec を無効にする必要があります。IANA 予約ポートを有効にしたいが、すでに 1 つ以上のサイトで CloudSec 暗号化を有効にしている場合は、すべてのサイトで CloudSec を無効にし、**[IANA 予約 UDP ポート（IANA Reserve UDP Port）]** オプションを有効にしてから、必要なサイトで CloudSec を再度有効にします。

- CloudSec 暗号化機能は、次の機能ではサポートされません。
  - 高精度時間プロトコル（PTP）
  - リモート リーフ ダイレクト
  - 仮想ポッド（vPod）
  - SDA
  - リモート リーフまたはマルチポッド構成
  - サイト間 L3Out（サイトが 5.2(4) より前の Cisco APIC リリースを実行している場合）。

    CloudSec は、リリース 5.2(4) 以降を実行している APIC サイトのサイト間 L3Out でサポートされています。

要件

CloudSec 暗号化機能では、次のものが必要です。

- Cisco ACI スパイン/リーフアーキテクチャと 1 台の Cisco APIC クラスタ（各サイト用）
- 各サイトを管理する Cisco Nexus Dashboard Orchestrator
- ファブリックのデバイス（リーフのみ）ごとに 1 つの **Advantage** または **Premier** ライセンス
- デバイスが固定スパインである場合には、暗号化のため、デバイスごとに 1 つの **ACI-SEC-XF** アドオン ライセンス
- デバイスがモジュール スパインである場合には、暗号化のため、デバイスごとに 1 つの **ACI-SEC-XM** アドオン ライセンス

次の表に、CloudSec 暗号化に対応したハードウェア プラットフォームとポート範囲を示します。

ハードウェア プラットフォーム	ポート範囲
N9K C9364C スパインスイッチ	ポート 49-64

ハードウェア プラットフォーム	ポート範囲
N9K-C9332C スパインスイッチ	ポート 25-32
N9K-X9736C-FX ラインカード	ポート 29-36

CloudSec がサイトに対して有効になっているが、暗号化がポートでサポートされていない場合、サポートされていないインターフェイスのエラーメッセージで障害が発生します。

CloudSec 暗号化のパケット カプセル化は、DWDM-C SFP10G などの Cisco QSFP から SFP へのアダプタ (QSA) がサポートされている光ファイバで使用されている場合にサポートされます。サポートされている光ファイバの完全なリストは、https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html のリンクから入手できます。

IANA が割り当てたポートと Orchestrator のダウングレードの使用

次のセクションで説明されているように、IANA が割り当てたポートを使用するように CloudSec 暗号化を構成した場合、Orchestrator サービスをリリース 3.7(1) より前のリリースにダウングレードする場合、いくつかの手順を実行する必要があります。

Nexus Dashboard Orchestrator を IANA ポートがサポートされていないリリースにダウングレードする前に:

1. すべての管理対象サイトの CloudSec 暗号化を無効にします。
2. インフラ構成設定で IANA 予約済み UDP ポート オプションを無効にします。
3. 以前に有効にしたすべてのサイトで CloudSec 暗号化を再度有効にします。
4. 通常どおり、Orchestrator サービスをダウングレードします。

CloudSec 暗号化に関する用語

CloudSec 暗号化機能は、サイト間の初期キーとキー再生成の要件に対して、安全なアップストリーム対称キーの割り当てと配布方法を提供します。この章では、次の用語を使用します。

- アップストリーム デバイス – CloudSec 暗号化ヘッダーを追加し、ローカルで生成された対称暗号化キーを使用してリモート サイトへの送信時に VXLAN パケット ペイロードの暗号化を行うデバイス。
- ダウンストリーム デバイス – CloudSec 暗号化ヘッダーを解釈し、リモート サイトで生成された暗号化キーを使用して受信時に VXLAN パケットペイロードの復号化を行うデバイス。
- アップストリーム サイト – 暗号化された VXLAN パケットを発信するデータ センター ファブリック。
- ダウンストリーム サイト – 暗号化されたパケットを受信して復号するデータ センター ファブリック。

- TX キー – クリアな VXLAN パケット ペイロードを暗号化するために使用される暗号化キー。ACI では、1 つの TX キーがすべてのリモート サイトに対してアクティブであることができます。
- RX キー – 暗号化された VXLAN パケット ペイロードを復号するために使用される暗号化キー。ACI では、2 つの RX キーをリモート サイトごとにアクティブにできます。

  2 つの RX キーをキーの再生成プロセス中に同時にアクティブにすることができます。ダウンストリームサイトは、新しいキーの展開が一定期間終了した後、古い RX キーと新しい RX キーを保持し、いずれかのキーを適切に復号することで、順序どおりでないパケット配信が可能になるようにします。
- 対象キー – 同じ暗号化キーを使用して、アップストリーム デバイスとダウンストリーム デバイスによるパケットストリームの暗号化(TX キー)と復号(RX キー)をそれぞれ行う場合。
- キーの再生成 – 古いキーの有効期限が切れた後、すべてのダウンストリーム サイトの古いキーを新しいキーに置き換えるためにアップストリームサイトによって開始されたプロセス。
- 安全なチャネル識別子 (SCI) – サイト間のセキュリティ関連付けを表す 64 ビット識別子。CloudSec ヘッダーの暗号化されたパケットで送信され、パケットの復号化のためにダウンストリームデバイスの RX キーを取得するために使用されます。
- アソシエーション番号値 (AN) – 暗号化されたパケットのCloudSecヘッダーで送信される2ビットの数値(0, 1, 2, 3)。これは、復号化のために SCI とともにダウンストリームデバイスでキーを導出するために使用されます。これにより、ダウンストリームデバイスで複数のキーをアクティブにして、キーの再生成操作の後で、同じアップストリームデバイスからの異なるキーを使用したパケットの順序どおりでない到着を処理できます。

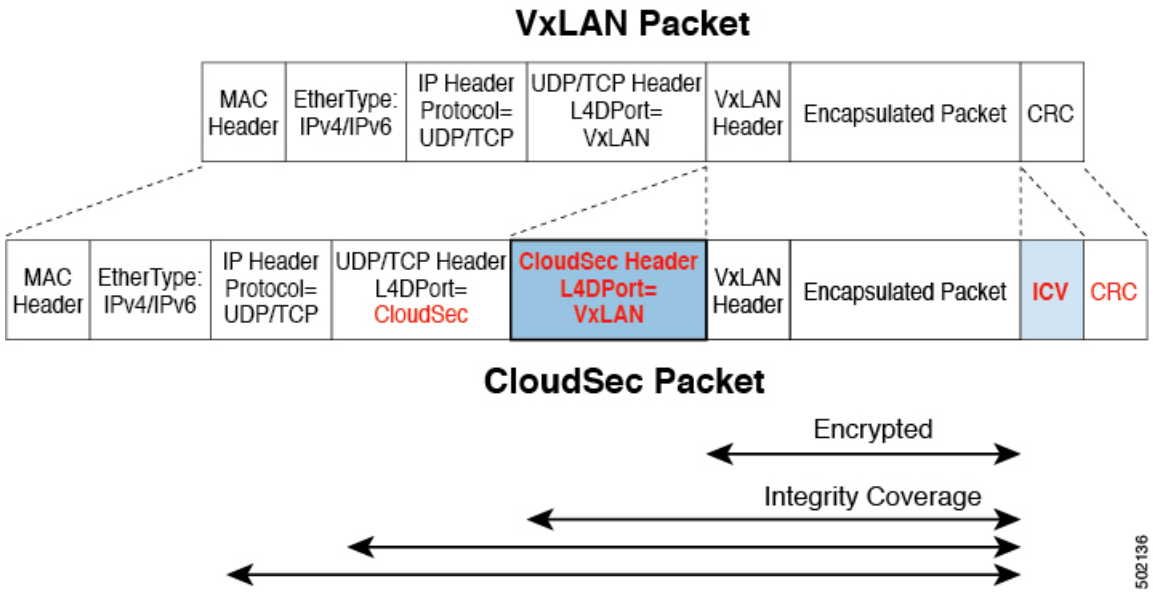
  ACI では、2 つのアクティブな RX キーには 2 つのアソシエーション番号値（0 または 1 1）のみが使用され、TX キーには常に 1 つのアソシエーション番号値（0 または 1）のみが使用されます。
- 事前共有キー (PSK) – CloudSec TX および RX キーを生成するためのランダム シードとして使用するには、Cisco APIC GUI で 1 つ以上のキーを設定する必要があります。複数の PSK が設定される場合、各キーの再生成プロセスはインデックスの順序で次の PSK を使用します。さらに高いインデックスの PSK がない場合、最下位のインデックスの PSK が使用されます。各 PSK は、64文字の長さの16進数ストリングでなければなりません。Cisco APIC は最大256の事前共有キーをサポートします。

CloudSec の暗号化と復号の処理

リリース2.0(1)以降では、データセキュリティと整合性の両方に対応する、完全に統合されたシンプルでコスト効率の高いソリューションを提供するために、Multi-Site は Multi-Site ファブリック間の送信元から宛先への完全なパケット暗号化を可能にする CloudSec 暗号化機能を提供します。

次の図は、CloudSec カプセル化の前後のパケット ダイアグラムと、その後の暗号化および復号化プロセスの説明を示しています。

図 *12 : CloudSec* パケット



パケット暗号化

次に、CloudSec が発信トラフィック パケットを処理する方法の概要を示します。

- パケットは、外部 IP ヘッダ宛先アドレス フィールドとレイヤ 4 宛先ポート情報を使用してフィルタ処理され、フィルタされたパケットは暗号化の対象としてマークされます。
- 暗号化に使用するオフセットは、パケットのフィールドに基づいて計算されます。たとえば、オフセットは、802.1q VLAN があるかどうか、またはパケットが IPv4 または IPv6 パケットであるかどうかによって異なります。

  オフセットは自動的に決定され、ユーザーには表示されません。
- 暗号キーはハードウェア テーブルでプログラムされ、パケット IP ヘッダーを使用してテーブルから検索されます。

パケットに暗号化のマークが付けられると、暗号キーがロードされ、暗号化を開始するパケットの先頭からのオフセットが判明すると、次の追加の手順が実行されます。

- UDP 宛先ポート番号は、UDP ヘッダーから CloudSec フィールドにコピーされ、パケットが暗号解読されるときにリカバリされます。
- UDP 宛先ポート番号は、CloudSec パケットであることを示すために上書きされます。

  3.7(1) より前のリリースでは、ポートは Cisco 独自のレイヤ 4 ポート番号 9999 で上書きされます。

IANA が割り当てたポート 8017 を使用するように CloudSec を構成できるリリース 3.7(1) 以降では、使用される宛先ポート番号は、このオプションを有効にしているかどうかに応じて 9999 または 8017 のいずれかです。

- [UDP 長(UDP length)] フィールドは、追加されるバイト数を反映するように更新されます。
- CloudSec ヘッダーは、UDP ヘッダーの後に直接挿入されます。
- 整合性チェック値 (ICV) は、ペイロードと CRC の間のパケットの最後に挿入されます。
- ICV では、128 ビットの初期化ベクトルを構築する必要があります。CloudSec の場合、ICV のために送信元 MAC アドレスを使用すると、SCI ごとのプログラム可能な値に置き換えられます。
- CRC は、パケットのコンテンツの変更を反映するように更新されます。

パケットの暗号解読

CloudSec が受信パケットを処理する方法は、上記で説明した発信パケット アルゴリズムと対称的です。

- 受信したパケットが CloudSec パケットである場合は、暗号解読され、ICV が検証されます。

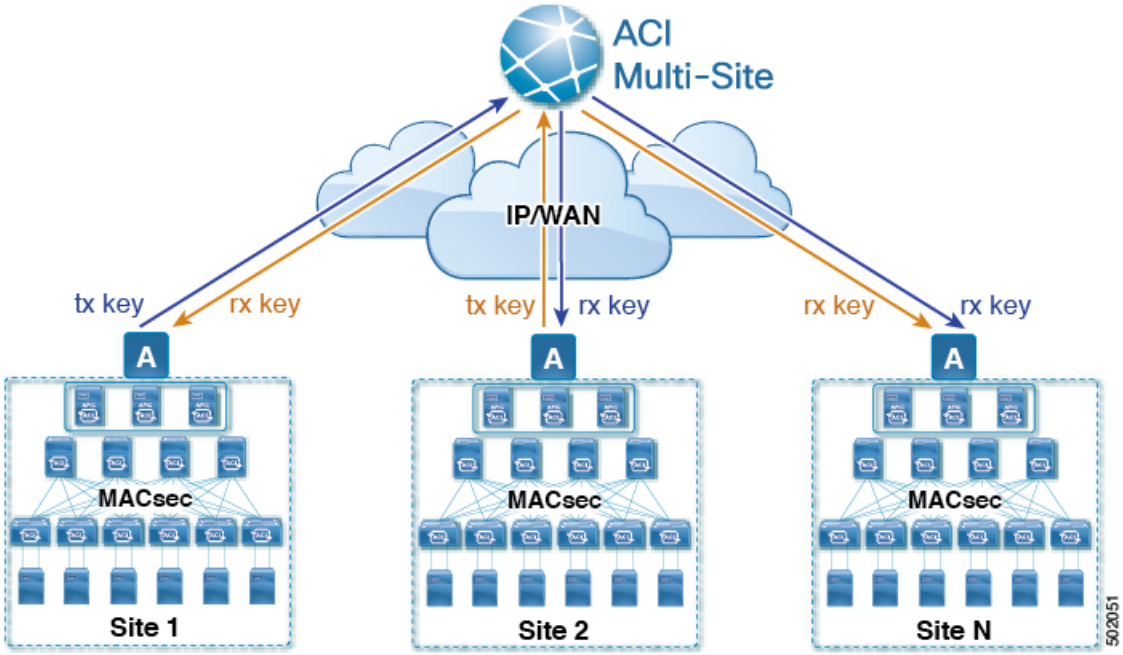
  ICV 検証に合格すると、追加フィールドが削除され、UDP 宛先ポート番号が CloudSec ヘッダーから UDP ヘッダーに移動され、CRC が更新され、パケットの暗号解読と CloudSec ヘッダーの削除後に宛先に転送されます。そうでない場合、パケットはドロップされます。

- 復号化キーは、受信した CloudSec パケットの外部 IP ヘッダーのソース アドレス フィールド、CloudSec ヘッダーの SCI、および AN 番号フィールドを使用してキー ストアから取得されます。
- パケットが CloudSec パケットでない場合、パケットはそのまま残ります。

CloudSec 暗号化キーの割り当てと配布

初期キー構成

図 *13 : CloudSec* キーの配布



次に、上記の図に示されている CloudSec 暗号キーの初期割り当ておよび配信プロセスの概要を示します。

- アップストリームサイトの Cisco APIC は、サイトから送信された VXLAN パケットのデータ暗号化に使用されるためのローカル対称キーを生成します。アップストリームサイトが暗号化に使用するのと同じキーが、ダウンストリームリモート受信サイトのパケットの復号に使用されます。

  各サイトはほかのサイトに送信するトラフィックのためのアップストリームサイトです。複数のサイトが存在する場合、各サイトは独自のサイトツーサイトキーを生成し、そのキーを暗号化に使用してからリモートサイトに送信します。

- 生成された対称キーは、ダウンストリーム リモート サイトに配布するために、アップストリーム サイトの Cisco APIC によって Nexus Dashboard Orchestrator (NDO) にプッシュされます。

- NDO はメッセージ ブローカとして機能し、生成された対称キーをアップストリーム サイトの Cisco APIC から収集し、それをダウンストリーム リモート サイトの Cisco APIC に配布します。

  キーは、キー暗号化キー (KEK) を使用して暗号化され、TLS ベースのチャネルを介して配布されます。

- 各ダウンストリーム サイトの Cisco APIC は、受信したキーを、キーを生成したアップストリームサイトからのトラフィックを受信することを目的としたローカル スパイン スイッチの RX キーとして設定します。
- 各ダウンストリーム サイトの Cisco APIC は、ローカル スパイン スイッチから RX キーの展開ステータスを収集し、NDO にプッシュします。
- NDO は、すべてのダウンストリーム リモート サイトからアップストリーム サイトの Cisco APIC に戻って、主要な展開ステータスを中継します。
- アップストリームサイトはCisco APIC 、すべてのダウンストリーム リモート サイトから受信したキー展開ステータスが成功したかどうかを確認します。
  - ダウンストリームデバイスから受信した展開ステータスが成功した場合、アップストリーム サイトはスパイン スイッチの TX キーとしてローカル対称キーを展開し、ダウンストリーム サイトに送信される VXLAN パケットの暗号化を有効にします。
  - ダウンストリームデバイスから受け取った展開ステータスが失敗した場合、失敗した Cisco APIC サイトで障害が発生し、NDO で構成された「セキュア モード」設定に基づいて処理されます。「セキュアが必須 (must secure)」モードでは、パケットはドロップされ、「セキュアであるべき (should secure)」モードでは、パケットは宛先サイトに平文 (暗号化されていない) で送信されます。

（注） 現在のリリースでは、モードは常に「セキュアであるべき (should secure)」に設定されており、変更できません。

キー再生成プロセス

生成された各 TX / RX キーは、設定された時間が経過すると有効期限が切れます。デフォルトでは、キーの有効期限は 15 分に設定されています。TX/RX キーの初期セットが期限切れになると、キー再生成プロセスが行われます。

キーの再割り当てプロセスには、同じ一般的なキーの割り当てと配布フローが適用されます。キー再生成プロセスは「ブレーク前に作成 (make before break)」ルールに従います。つまり、新しい TX キーがアップストリーム サイトに展開される前に、ダウンストリーム サイトのすべての RX キーが展開されます。これを実現するために、アップストリームサイトは、ローカル アップストリーム サイトのデバイスに新しい TX キーを構成する前に、ダウンストリーム サイトからの新しい RX キーの展開ステータスを待ちます。

ダウンストリームサイトが新しい RX キーの展開で障害ステータスを報告した場合、キー再生成プロセスは終了し、古いキーはアクティブなままになります。ダウンストリームサイトは、新しいキーの展開が一定期間終了した後、古い RX キーと新しい RX キーを保持し、いずれかのキーを適切に復号することで、順序どおりでないパケット配信が可能になるようにします。

（注） スパイン スイッチのメンテナンス中のキー再生成プロセスに関しては、特別な注意が必要です。詳細については、スパイン スイッチ メンテナンス中のキー再生成プロセス （212 ページ）を参照してください。

キー再生成プロセスの失敗

ダウンストリーム サイトがキー再生成プロセスによって生成された新しい暗号化キーの展開に失敗した場合、新しいキーは破棄され、アップストリーム デバイスは以前の有効なキーを TX キーとして引き続き使用します。このアプローチにより、アップストリーム サイトは、ダウンストリーム サイトのセットごとに複数の TX キーを維持する必要がなくなります。ただし、このアプローチでは、いずれかのダウンストリーム サイトでキー再生成の展開エラーが発生し続ける場合、キー更新プロセスが遅延する可能性もあります。マルチサイト管理者は、キー再生成を成功させるために、キーの展開の失敗の問題を修正するための行動を取ることが期待されています。

Cisco APICキー管理のロール

Cisco APIC は、キー割り当て(初期キーとキー再配布の両方)、スパイン スイッチからのキー展開ステータス メッセージの収集、および他のサイトへの配布のための各キーのステータスに関する Nexus Dashboard Orchestrator への通知に責任をもちます。

キー管理における Nexus Dashboard Orchestrator の役割

Nexus Dashboard Orchestrator は、アップストリーム サイトから TX キー（初期キーと後続のキーの再生成の両方）を収集し、RX キーとして展開するためにすべてのダウンストリーム サイトに配布します。NDO はまた、ダウンストリーム サイトから RX キーの展開ステータス情報を収集し、成功した RX キー展開ステータスで TX キーを更新するために、アップストリーム サイトに通知します。

アップストリーム モデル

MPLS など、ダウンストリーム キー割り当てを使用する他のテクノロジーとは対照的に、CloudSec のアップストリーム モデルには次の利点があります。

- このモデルはシンプルで、運用とネットワークへの導入が容易です。
- モデルは、マルチサイトのユース ケースに適しています。
- 複数の宛先サイトに送信される複製パケットの各コピーに同じキーと CloudSec ヘッダーを使用できるため、マルチキャスト トラフィックに利点があります。ダウンストリーム モデルでは、各コピーは暗号化中にサイトごとに異なるセキュリティ キーを使用する必要があります。
- 障害が発生した場合のトラブルシューティングが容易になり、複製されたユニキャスト パケットとマルチキャスト パケットの両方に対して、送信元から宛先へのパケットのトレーサビリティが一貫して向上します。

CloudSec 暗号化のための Cisco APIC の設定

CloudSec 暗号と復号キーを生成するために、Cisco APIC で使用する 1 個以上の事前共有キー（PSK）を構成する必要があります。PSK は再キー プロセス中のランダム シードとして使用されます。複数の PSK が設定される場合、各再キープロセスはインデックスの順序で次の PSK を使用します。さらに高いインデックスの PSK がない場合、最下位のインデックスの PSK が使用されます。

暗号キーの生成に対するシードとして PSK が使用されるため、複数の PSK の設定では生成された暗号キーの長時間にわたる脆弱性を下げることにより、追加のセキュリティを提供します。

（注） Cisco APIC で事前共有キーが構成されていない場合、CloudSec はそのサイトに対して有効にはなりません。その場合、マルチサイトで CloudSec 設定をオンにすると、障害が生じます。

いつでも新しい PSK で前に追加した PSK を更新したい場合、新しいキーを追加するときと同様の手順を繰り返すだけですが、インデックスは既存のものを指定してください。

1 つ以上の事前共有キーを次の 3 通りの方法のいずれかを使用して設定できます。

- GUI を使用した CloudSec 暗号化の Cisco APIC の設定 （206 ページ） で説明されている Cisco APIC GUI の使用
- NX-OS Style CLI を使用した CloudSec 暗号化に対する Cisco APIC の設定 （207 ページ） で説明されている Cisco APIC NX-OS スタイルの CLI の使用
- REST API を使用した CloudSec 暗号化の Cisco APIC の設定 （208 ページ）で説明されている Cisco APIC REST API の使用

GUI を使用した CloudSec 暗号化の Cisco APIC の設定

このセクションは、Cisco APIC GUI を使用して 1 つ以上の事前共有キー (PSK) を設定する方法について説明します。

手順

ステップ 1 APIC にログインします。

ステップ 2 **[テナント] > [インフラ] > [ポリシー] > [CloudSec 暗号化] に移動します。**

ステップ 3 **SA キーの有効期限**を指定します。

このオプションは、各キーが有効な時間 (分) を指定します。それぞれの生成された TX/RX キーは、再キープロセスをトリガした後指定の時間で期限切れになります。期限の時間は、5～1440 分の範囲で入力できます。

ステップ 4 **[事前共有キー]**テーブルの + アイコンをクリックします。

ステップ 5 追加する事前共有キーの**インデックス**を指定し、その後、**事前共有**キー自体を指定します。

[インデックス (Index)] フィールドは、事前共有キーを使用する順序を指定します。最後 (最高位のインデックス) キーが使用された後で、プロセスは最初 (最下位のインデックス) キーで続けられます。Cisco APIC は最大256個の事前共有キーをサポートするので、PSKインデックスチは1～256でなければなりません。

各**事前共有キー**は、64 文字の 16 進数文字列である必要があります。

NX-OS Style CLI を使用した CloudSec 暗号化に対する Cisco APIC の設定

このセクションでは、 Cisco APIC NX OS Style CLI を使用して1つ以上の事前共有キー (PSK) を設定する方法について説明します。

手順

ステップ 1 Cisco APIC NX-OS style CLI にログインします。

ステップ 2 コンフィギュレーション モードを入力します。

例：

```
apic1# configure
apic1 (config)#
```

ステップ 3 デフォルト CloudSec プロファイルのコンフィグレーション モードを入力します。

例：

```
apic1(config)# template cloudsec default
apic1(config-cloudsec)#
```

ステップ 4 事前共有キー (PSK) の有効期限を指定します。

このオプションは、各キーが有効な時間(分) を指定します。それぞれの生成されたTX/RXキーは、再キープロセスをトリガした後指定の時間で期限切れになります。期限の時間は、5～1440 分の範囲で入力できます。

例：

```
apic1(config-cloudsec)# sakexpirytime <duration>
```

ステップ 5 1 つまたは複数の事前共有キーを指定します。

次のコマンドでは、設定している PSK のインデックスと PSK 文字列自体を指定します。

例：

```
apic1(config-cloudsec)# pskindex <psk-index>
apic1(config-cloudsec)# pskstring <psk-string>
```

<psk-index> パラメータは、事前共有キーが使用される順序を指定します。最後 (最上位のインデックス) キーが使用された後で、プロセスは最初 (最下位のインデックス) キーで続けられます。Cisco APIC は最大 256 個の事前共有キーをサポートするので、PSK インデックスチは 1 ～ 256 でなければなりません。

<*psk-string*>パラメータは、実際の PSK を指定します。これは、64 文字の 16 進数文字列である必要があります。

ステップ 6 (オプション) 現在の PSK 設定を表示します。

現在設定されている PSK の数とその期間を表示するには、次のコマンドを使用します。

例：

```
apic1(config-cloudsec)# show cloudsec summary
```

REST API を使用した CloudSec 暗号化の Cisco APIC の設定

このセクションは、Cisco APIC REST API を使用して 1 つ以上の事前共有キー (PSK) を設定する方法について説明します。

手順

PSK 有効期限、インデックス、文字列を設定します。

次の XML POST で、次を置換します。

- 各 PSK の期限をもつ **sakExpiryTime** の値。

  この **sakExpiryTime** パラメータは各キーが有効な時間 (分) を指定します。それぞれの生成された TX/RX キーは、再キー プロセスをトリガした後指定の時間で期限切れになります。期限の時間は、5 ～1440 分の範囲で入力できます。

- 設定している PSK のインデックスをもつ **インデックス** の値。

  インデックス パラメータは、事前共有キーが使用される順序を指定します。最後 (最高位のインデックス) キーが使用された後で、プロセスは最初 (最下位のインデックス) キーで続けられます。Cisco APIC は最大 256 個の事前共有キーをサポートするので、PSK インデックスチは 1 ～ 256 でなければなりません。

- 設定している PSK のインデックスをもつ **pskString** の値。

  pskString パラメータは実際の PSK を指定します。これは 16 進文字列で長さ 64 文字でなければなりません。

例：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">

    <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey= "false" status=""
 >
        <cloudsecPreSharedKey index="1"
pskString="1234567812345678123456781234567812345678123456781234567812345678" status=""/>
```

```
    </cloudsecIfPol>
</fvTenant>
```

Nexus Dashboard Orchestrator 内の CloudSec 暗号の有効化

CloudSec 暗号化は、サイトごとに個別に有効または無効にすることができます。ただし、2 つのサイト間の通信は、この機能が両方のサイトで有効になっている場合にのみ暗号化されます。

始める前に

2つ以上のサイト間でCloudSec暗号化を有効にする前に、次のタスクを完了しておく必要があります。

- 『*Cisco APIC* のインストール、アップグレード、ダウングレードガイド』で説明されているように、複数のサイトに Cisco APIC クラスタをインストールして設定します。
- 『*Cisco Nexus Dashboard Orchestrator* インストレーションおよびアップグレード ガイド』の説明に従って、Nexus Dashboard Orchestrator をインストールし、設定します。
- 『*Cisco ACI* マルチサイト コンフィギュレーション ガイド』の説明に従って、各 Cisco APIC サイトを Nexus Dashboard Orchestrator に追加します。

手順

ステップ 1 Nexus Dashboard Orchestrator にログインします。

ステップ 2 左のナビゲーション メニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ウィンドウの右上にある **[構成（Configure）]** ボタンをクリックします。

ステップ 4 （オプション）[一般設定（General Settings）] ページの [コントロール プレーンの構成（Control Plane Configuration）] タブで、[IANA 予約済み UDP ポート（IANA Reserved UDP Port）] オプションを有効にします。

デフォルトでは、CloudSecは独自のUDPポートを使用します。このオプションを使用すると、サイト間の CloudSec 暗号化に公式の IANA 予約ポート 8017 を使用するように CloudSec を構成できます。

（注）
IANA 予約ポートは、リリース 5.2(4) 以降を実行している Cisco APIC サイトでサポートされています。

この設定を変更するには、すべてのサイトで CloudSec を無効にする必要があります。IANA 予約ポートを有効にしたいが、すでに 1 つ以上のサイトで CloudSec 暗号化を有効にしている場合は、すべてのサイトで CloudSec を無効にし、**[IANA 予約 UDP ポート（IANA Reserve UDP Port）]** オプションを有効にしてから、必要なサイトで CloudSec を再度有効にします。

ステップ 5 左側のサイドバーから、CloudSec 設定を変更するサイトを選択します。

ステップ 6 右側のサイドバーで、**[Cloudsec 暗号化（Cloudsec encryption）]** 設定を切り替えて、サイトの CloudSec 暗号化機能を有効または無効にします。

スイッチでの CloudSec 構成の確認

次のコマンドを使用すると、Nexus Dashboard Orchestrator から CloudSec 暗号化を有効にした後、スパイン スイッチに展開された現在の CloudSec 構成を確認できます。

手順

ステップ 1 スパイン スイッチにログインします。

ステップ 2 `show cloudsec sa interface all` コマンドを実行して、CloudSec 構成を表示します。

次の出力で、各インターフェイスについて次のことを確認します。

- [動作ステータス（Operational Status）] の値は UP を示します。
- [制御（Control）] 値は、CloudSec 暗号化に現在使用されている UDP ポートを示すため、すべての CloudSec 対応サイトのすべてのインターフェイスで同じです。

  次の例は、デフォルトのシスコ独自の UDP ポート（deprecatedUdpPort）を示しています。IANA が割り当てたポート 8017 を使用するように CloudSec を構成すると、**[制御（Control）]** フィールドには代わりに ianaUdpPort が表示されます。

```
spine1# show cloudsec sa interface all
================================================================================
Interface: Eth1/49.49(0x1a030031) Physical Interface: Eth1/49(0x1a030000)
    Operational Status: UP Retry: Off Control: deprecatedUdpPort
--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.204.0/24 Type: ext-routable-tep-pool Operational Status: UP
    Pod-Id: 1
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 0 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.520-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs
--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.202.1/32 Type: msite-unicast-tep Operational Status: UP
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 2 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.563-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs
    RX Key: ******************************** Assoc Num: 1 Sci: 0x20001
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 3 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.442-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs
```

```
    RX Key: ******************************** Assoc Num: 0 Sci: 0x20001
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
       Hardware Index: 2 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.453-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs

--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.201.1/32 Type: msite-multicast-tep Operational Status: UP
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 1 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.549-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs
    RX Key: ******************************** Assoc Num: 1 Sci: 0x20001
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 1 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:36.501-08:00 Retry: Off
       Uptime: 11 hours 30 mins 46 secs
    RX Key: ******************************** Assoc Num: 0 Sci: 0x20001
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
       Hardware Index: 0 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.495-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs

================================================================================
Interface: Eth1/50.50(0x1a031032) Physical Interface: Eth1/50(0x1a031000)
    Operational Status: UP Retry: Off Control: deprecatedUdpPort
--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.204.0/24 Type: ext-routable-tep-pool Operational Status: UP
    Pod-Id: 1
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 1 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.577-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs
--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.201.1/32 Type: msite-multicast-tep Operational Status: UP
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 0 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.537-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs
    RX Key: ******************************** Assoc Num: 1 Sci: 0x20001
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 1 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:36.463-08:00 Retry: Off
       Uptime: 11 hours 30 mins 46 secs
    RX Key: ******************************** Assoc Num: 0 Sci: 0x20001
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
       Hardware Index: 0 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.416-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs

--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.202.1/32 Type: msite-unicast-tep Operational Status: UP
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 2 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.593-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs
```

```
RX Key: ******************************** Assoc Num: 0 Sci: 0x20001
   Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
   Hardware Index: 2 Operational Status: UP Control: NONE
   Last Updated: PST 2022-01-11 23:26:37.481-08:00 Retry: Off
   Uptime: 11 hours 30 mins 45 secs
RX Key: ******************************** Assoc Num: 1 Sci: 0x20001
   Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
   Hardware Index: 3 Operational Status: UP Control: NONE
   Last Updated: PST 2022-01-11 23:26:37.507-08:00 Retry: Off
   Uptime: 11 hours 30 mins 45 secs
```

スパインスイッチ メンテナンス中のキー再生成プロセス

次に、この機能が有効になっているスパイン スイッチの一般的なメンテナンス シナリオでの CloudSec キー再生成プロセスの概要を示します。

- **通常の解放**: CloudSec 対応スパイン スイッチがデコミッションされると、 CloudSec キー再生成プロセスが自動的に停止します。解放されたノードが再起動されるか、解放されたノード ID が次から削除されるまで、キー再生成プロセスは再度開始されません: Cisco APIC
- **スパイン スイッチのソフトウェア アップグレード**: スパイン スイッチがソフトウェアのアップグレードによりリロードされると、CloudSec キー再生成プロセスは自動的に停止します。キー再生成プロセスは、スパイン スイッチのリロードが完了すると、再開されます。
- **メンテナンス (GIR モード)** : CloudSec キー再生成プロセスは、NX-OS Style CLI を使用してキーの再生成プロセスを無効にして再度有効にする （212 ページ）に記載されている手順を使用して、手動で停止する必要があります。キー再生成は、ノードがトラフィックを転送する準備が再度整った後にのみ、有効にできます。
- **Cisco APICからの解放と削除** : CloudSec キー再生プロセスは、NX-OS Style CLI を使用してキーの再生成プロセスを無効にして再度有効にする （212 ページ） に記載されている手順を使用して、手動で停止する必要があります。キー再生成は、Cisco APIC からノードが削除された後にのみ有効にできます。

NX-OS Style CLI を使用してキーの再生成プロセスを無効にして再度有効にする

キーの再生成プロセスを手動で停止し再開することが可能です。特定の状況でキーの再生成プロセスを手動で管理することが必要な場合があります。たとえば、でコミッションとメンテナンスの切り替えなどです。このセクションは、 Cisco APIC NX-OS Style CLI を使用して設定を切り替える方法を説明します。

手順

ステップ 1 Cisco APIC NX-OS style CLI にログインします。

ステップ 2 コンフィギュレーション モードを入力します。

例：

```
apic1# configure
apic1(config)#
```

ステップ 3 デフォルト CloudSec プロファイルのコンフィグレーション モードを入力します。

例：

```
apic1(config)# template cloudsec default
apic1(config-cloudsec)#
```

ステップ 4 キーの再生成プロセスを停止するか、再開します。

キーの再生成を停止するには:

例：

```
apic1(config-cloudsec)# stoprekey yes
```

キーの再生成プロセスを再開するには:

例：

```
apic1(config-cloudsec)# stoprekey no
```

REST API を使用したキー再生成プロセスの無効化と再有効化

キーの再生成プロセスを手動で停止し再開することが可能です。特定の状況でキーの再生成プロセスを手動で管理することが必要な場合があります。たとえば、でコミッションとメンテナンスの切り替えなどです。このセクションでは、Cisco APICREST API を使用して設定を切り替える方法について説明します。

手順

ステップ 1 キー再生成プロセスは、次のXML メッセージを使用して無効にすることができます。

例：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">

    <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey= "true" status=""
 />
</fvTenant>
```

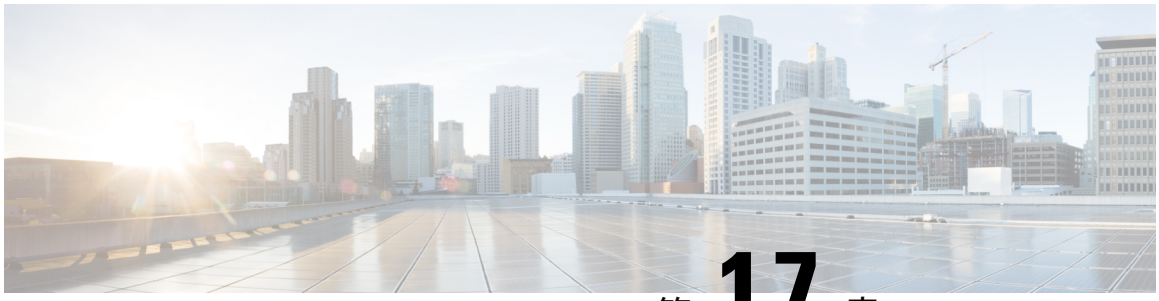
ステップ 2 キー再生成プロセスは、次のXML メッセージを使用して有効にすることができます。

例：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">

    <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey= "false" status=""
 />
</fvTenant>
```

第 IV 部

機能と使用例



第 17 章

DHCPリレー

DHCP リレー ポリシー

通常、DHCP サーバが EPG の下に配置されている場合、その EPG 内のすべてのエンドポイントがアクセス権を持ち、DHCP を介して IP アドレスを取得できます。ただし、多くの導入シナリオでは、DHCP サーバが必要なすべてのクライアントと同じ EPG、BD、または VRF に存在していない可能性があります。このような場合、1つの EPG 内のエンドポイントが別のサイトに配置された別の EPG/BD にあるサーバから、またはファブリックに外部に接続され、L3Out 接続を介して到達可能なサーバから IP アドレスを取得できるように、DHCP リレーを設定できます。

Orchestrator GUI で DHCP リレー ポリシーを作成してリレーを設定できます。また、DHCP オプション ポリシーを作成して、特定の設定の詳細を提供するためにリレーポリシーで使用できる追加オプションを設定することもできます。使用可能なすべての DHCP オプションについては、 RFC 2132 を参照してください。

DHCP リレーポリシーを作成する場合は、DHCP サーバが存在する EPG (たとえば、 `epg1`) または外部 EPG (たとえば、`ext epg1`) を指定します。DHCP ポリシーを作成した後、それをブリッジドメインに関連付けます。これにより、その EPG 内のエンドポイントが DHCP サーバに到達できるようになります。これにより、別の EPG (たとえば、`epg2`) に関連付けられます。最後に、リレー EPG (`epg1`または`epg1`) とアプリケーション EPG (`epg2`) 間の契約を作成し、通信を可能にします。作成した DHCP ポリシーは、ポリシーが関連付けられているブリッジ ドメインがサイトに展開されるときに、APIC にプッシュされます。

注意事項と制約事項

DHCP リレーポリシーは、次の警告でサポートされます。

- DHCP リレーポリシーは、Cisco APIC リリース 4.2(1) 以降を実行しているファブリックでサポートされています。
- DHCP サーバは、DHCP リレー エージェント情報オプション (オプション 82) をサポートしている必要があります。

  ACI ファブリックが DHCP リレーとして動作する場合、DHCP リレーエージェント情報オプションは、クライアントの代わりにプロキシする DHCP 要求に挿入されます。応答（DHCP オファー）がオプション 82 なしで DHCP サーバから返された場合、その応答はファブリックによってサイレントにドロップされます。
- DHCP リレー ポリシーは、ユーザ テナントまたは共通テナントでのみサポートされます。DHCP ポリシーは、インフラまたは管理テナントではサポートされていません。

  ACI ファブリックで共有リソースとサービスを設定する場合は、共通テナントでこれらのリソースを作成することをお勧めします。これは、どのユーザ テナントでも使用できます。
- DHCP リレー サーバは、DHCP クライアントまたは共通テナントと同じユーザ テナントに存在する必要があります。

  サーバとクライアントは、異なるユーザ テナントに配置することはできません。
- DHCP リレー ポリシーは、プライマリ SVI インターフェイスにのみ設定できます。

  リレーポリシーを割り当てるブリッジドメインに複数のサブネットが含まれている場合、追加した最初のサブネットは SVI インターフェイスのプライマリ IP アドレスになりますが、追加のサブネットはセカンダリ IP アドレスとして設定されます。複数のサブネットを持つブリッジドメインを使用した設定のインポートなどの特定のシナリオでは、SVI のプライマリ アドレスがセカンダリ アドレスの1つに変更されることがあり、そのブリッジドメインの DHCP リレーが中断されることがあります。

  `Show ip interface vrf all` コマンドを使用して、SVI インターフェイスの IP アドレスの割り当てを確認できます。
- ブリッジドメインに割り当てた後に DHCP ポリシーを変更し、ブリッジ ドメインを 1 つ以上のサイトに展開した場合は、各サイトの APIC で DHCP ポリシーの変更を更新するために、ブリッジ ドメインを再展開する必要があります。
- L3Out 経由で到達可能な DHCP サーバとの VRF 間 DHCP リレーの場合、DHCP リレー パケットは、DHCP サーバに到達するためにサイト ローカル L3Out を使用する必要があります。異なるサイト (サイト間 L3Out) の L3Out を使用するパケットはサポートされていません。
- 次の DHCP リレー設定はサポートされていません。
  - L3Out インターフェイスの DHCP リレー ラベル。

- APIC から既存の DHCP ポリシーをインポートしています。
- グローバルファブリックアクセスポリシーでのDHCPリレーポリシーの設定はサポートされていません
- 同じ DHCP リレーポリシー内の複数の DHCP サーバと EPG。

  同じ DHCP リレーポリシーで複数のプロバイダを設定する場合は、それぞれ異なる EPGs または外部 EPGs にする必要があります。

DHCP リレー ポリシーの作成

このセクションでは、DHCP リレー ポリシーの作成方法について説明します。

（注） ブリッジ ドメインに DHCP ポリシーを割り当て、ブリッジ ドメインを 1 つ以上のサイトに展開した後で DHCP ポリシーに変更を加えた場合、DHCP ポリシーの変更が各サイトの APIC で更新されるように、ブリッジ ドメインを再展開する必要があります。

始める前に

次のものが必要です。

- 環境でセットアップして設定された DHCP サーバ。
- DHCP サーバーがアプリケーション EPG の一部である場合には、その EPG が Nexus Dashboard Orchestrator ですでに作成されている必要があります。
- DHCP サーバーがファブリックの外部にある場合には、DHCP サーバーにアクセスするために使用される L3Out に関連付けられた外部 EPG が、すでに作成されている必要があります。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 新しいテナント ポリシーを作成。

a) 左側のナビゲーション メニューで、**[アプリケーション管理（Application Management）]** > **[テナント ポリシー（Tenant Policies）]** を選択します。

b) **[テナント ポリシー テンプレート（Tenant Policy Template）]**ページ内で**[テナント ポリシー テンプレートを追加（Add Tenant Policy Template）]**をクリックします。

c) テナント ポリシー ページの右のプロパティ サイトバーにテナントの **[名前（Name）]** を入力します。

d) **[テナントの選択（Select a Tenant）]**ドロップダウンから、このテンプレートに関連付けるテナントを選択します。

次の手順で説明するようにテンプレートで作成したすべてのポリシーは、テンプレートを特定のサイトにプッシュするとそれに展開され、選択したテナントに関連付けられます。

ステップ 3 DHCP リレー ポリシーの作成。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[DHCP リレー ポリシー（ DHCP Relay Policy）]** を選択します。

b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。

c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。

d) **[プロバイダーの追加（Add Provider）]** をクリックして、エンドポイントによって発信された DHCP 要求をリレーする DHCP サーバーを構成します。

e) プロバイダ タイプを選択します。

リレー ポリシーを追加するときには、次の 2 つのタイプのうちの 1 つを選択できます。

- アプリケーション EPG ：DHCP 要求をリレーする DHCP サーバーを含むアプリケーション EPG を指定します。
- L3 外部ネットワーク — ファブリックの外部のネットワークの場所 でもあるDHCP サーバーが接続されている場所へのアクセスに使用される L3Out に関連付けられた外部 EPG を指定します。

（注）
Orchestrator をサイトにまだ展開していない場合でも、Orchestratorで作成され、指定したテナントに割り当てられている EPG または外部 EPG を選択できます。展開されていない EPG を選択した場合でも、DHCP リレー構成を完了することができますが、リレーが使用可能になる前に EPG を展開する必要があります。

f) **[アプリケーション EPG を選択（Select an Application EPG）]** または **[外部 EPG を選択（Select an External EPG）]**（選択したプロバイダー タイプに基づく）をクリックし、プロバイダー EPG を選択します。

g) **[DHCP サーバ アドレス]** フィールドに、DHCP サーバの IP アドレスを入力します。

h) 必要に応じて、**DHCP サーバー VRF プリファレンス** オプションを有効にします。

この機能は、Cisco APIC リリース 5.2（4）に紹介されています。必要な使用例の詳細については、Cisco APIC 基本構成ガイドを参照してください。

i) **[OK]** をクリックして、プロバイダー情報を保存します。

j) 同じ DHCP リレー ポリシー内の追加のプロバイダーについて、前のサブステップを繰り返します。

k) このステップを繰り返して、追加の DHCP リレー ポリシーを作成します。

DHCP オプション ポリシーの作成

このセクションでは、DHCP オプション ポリシーの作成方法について説明します。DHCP オプションは、DHCP サーバとクライアントが交換するメッセージの末尾に追加され、DHCP サーバに追加の設定情報を提供するために使用されます。各 DHCP オプションには、オプションポ

リシーを追加するときに指定する必要がある特定のコードがあります。DHCP オプションとコードの完全なリストの場合は、RFC 2132 を参照してください。

始める前に

次のものをあらかじめ設定しておく必要があります。

- 環境で DHCP サーバをセットアップして設定します。
- Nexus Dashboard Orchestrator ですでに作成してある DHCP サーバを含む EPG。
- DHCP リレー ポリシーの作成 （219 ページ） の説明に従って作成された DHCP リレー ポリシー。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 新しいテナント ポリシーを作成するか、既存のテナント ポリシーを更新します。

a) 左側のナビゲーション メニューで、**[アプリケーション管理（Application Management）]** > **[テナント ポリシー（Tenant Policies）]** を選択します。

b) **[テナント ポリシー テンプレート（Tenant Policy Template）]**ページ内で既存のポリシーまたは、**[テナント ポリシー テンプレートを追加（Add Tenant Policy Template）]**を選択します。

c) 新しいポリシーを作成するには、テナント ポリシー ページの右のプロパティ サイトバーにテナントの **[名前（Name）]** を入力します。

d) 新しいポリシーを作成するには、**[テナントの選択（Select a Tenant）]**ドロップダウンから、このテンプレートに関連付けるテナントを選択します。

次の手順で説明するようにテンプレートで作成したすべてのポリシーは、テンプレートを特定のサイトにプッシュするとそれに展開され、選択したテナントに関連付けられます。

ステップ 3 DHCP オプション ポリシーの作成。

a) **[+オブジェクトの作成]** ドロップダウンから、**[DHCP オプション ポリシー]** を選択します。

b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。

c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。

d) [Add Option] をクリックします。

e) オプションの詳細を入力します。

DHCP オプションごとに、以下を指定します：

- **Name** – 技術的には要求されていませんが、RFC 2132 にリストされたオプションに同じ名前を使用することをお勧めします。

  たとえば、ネーム サーバ が挙げられます。

- **ID** – オプションが値を要求した場合はそれを指定します。

  たとえば、[ネーム サーバ] オプションのクライアントに使用可能なネーム サーバのリスト。

- **Data** – オプションが値を要求した場合はそれを指定します。

  たとえば、[ネーム サーバ] オプションのクライアントに使用可能なネーム サーバのリスト。

f) [OK] をクリックして保存します。
g) 同じ DHCP オプション ポリシー内の追加オプションについて、前のサブステップを繰り返します。
h) このステップを繰り返して、追加の DHCP オプション ポリシーを作成します。

DHCP ポリシーの割り当て

この項では、ブリッジ ドメインを作成する方法について説明します。

（注） ブリッジドメインに割り当てた後に DHCP ポリシーを変更し、ブリッジ ドメインを 1 つ以上のサイトに展開した場合は、各サイトの APIC で DHCP ポリシーの変更を更新するために、ブリッジ ドメインを再展開する必要があります。

始める前に

次のものをあらかじめ設定しておく必要があります。

- DHCP リレー ポリシーの作成 （219 ページ） の説明に従って、DHCP リレー ポリシー。
- (オプション) DHCP オプション ポリシーの作成 （220 ページ） の説明に従って、DHCP オプション ポリシー。
- スキーマとテンプレートの作成 （32 ページ） 章の説明に従って、DHCP ポリシーに割り当てられたブリッジ ドメイン。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

ステップ 3 ブリッジド メインが定義されているスキーマを選択します。

ステップ 4 **[[ブリッジ ドメイン (Bridge domain)]** エリアまで下にスクロールし、ブリッジド メインを選択します。

ステップ 5 右側のサイドバーで、下にスクロールして、 **[DHCP ポリシー (DHCP Policy)]** オプション チェックボックスをオンにします。

ステップ 6 **[DHCP リレーポリシー (DHCP Relay policy)]** ドロップダウンから、この BD に割り当てる DHCP ポリシーを選択します。

ステップ 7 (オプション)**[DHCP オプションポリシー (DHCP Option policy)]** ドロップダウンから、オプション ポリシーを選択します。

DHCP オプション ポリシーは、DHCP リレーに渡す追加のオプションを提供します。詳細については、DHCP オプション ポリシーの作成 （220 ページ）を参照してください。

ステップ 8 リレー経由でDHCPサーバにアクセスする必要があるすべてのEPGにブリッジ ドメインを割り当てます。

DHCP リレー コントラクトの作成

DHCP パケットはコントラクトによりフィルタリングされませんが、VRF 内および VRF 間でルーティング情報を伝播するには、多くの場合コントラクトが必要です。DHCP パケットはフィルタリングされませんが、クライアント EPG と DHCP リレー ポリシーでプロバイダとして設定された EPG の間のコントラクトを設定することをお勧めします。

このセクションでは、DHCP サーバーを含む EPG と、リレーを使用する必要のあるエンドポイントを含む EPG の間でコントラクトを作成する方法について説明します。DHCP ポリシーを作成してブリッジ ドメインに、また、ブリッジ ドメインをクライアントの EPG にすでに割り当てている場合でも、クライアントからサーバーへの通信を可能にするルートのプログラミングを有効にするには、コントラクトを作成して割り当てる必要があります。

始める前に

次のものをあらかじめ設定しておく必要があります。

- DHCP リレー ポリシーの作成 （219 ページ） の説明に従って、DHCP リレー ポリシー。
- (オプション) DHCP オプション ポリシーの作成 （220 ページ） の説明に従って、DHCP オプション ポリシー。
- DHCP ポリシーの割り当て （222 ページ） の説明に従って、DHCP ポリシーに割り当てられたブリッジ ドメイン。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから **[スキーマ(Schemas)]** を選択します。

ステップ 3 コントラクトを作成したいスキーマを選択します。

ステップ 4 コントラクトを作成します。

DHCP パケットはコントラクトによってフィルタリングされていないため、特定のフィルタは必要ありませんが、有効なコントラクトが作成され、割り当てられて、適切な BD およびルート展開を保証する必要があります。

a) [**コントラクト (Contracts)**] エリアまで下方にスクロールし、+ をクリックして、コントラクトを作成します。
b) 右のプロパティのサイドバーでは、コントラクトの**表示名**を指定します。
c) [**範囲 (Scope)**] ドロップダウンから、適切な範囲を選択します。

DHCP サーバ EPG とアプリケーション EPG は同じテナントになければならないため、次のうちの 1 つを選択できます。

- `vrf`。両方の EPG が同じ VRF にある場合
- テナント。EPG が異なる VRF にある場合

d) [**両方向に適用 (Apply Both Directions)**] ノブをオンのままにすることができます。

ステップ 5 DHCP リレー EPG にコントラクトを割り当てます。

a) EPG が配置されているテンプレートを参照します。
b) DDHCP サーバが常駐する EPG または外部 EPG を選択します。

これは、DHCP リレー ポリシーを作成するときに選択したものと同じ EPG です。

c) 右側のサイドバーで、[**+コントラクト (+Contract)**] をクリックします。
d) 作成したコントラクトとそのタイプのプロバイダを選択します。

ステップ 6 エンドポイントが DHCP リレー アクセスを必要とするアプリケーション EPG にコントラクトを割り当てます。

a) アプリケーション EPG が配置されているテンプレートを参照します。
b) アプリケーション EPG を選択します。
c) 右側のサイドバーで、[**+コントラクト (+Contract)**] をクリックします。
d) 作成したコントラクトとそのタイプのコンシューマを選択します。

APIC での DHCP リレー ポリシーの確認

ここでは、Nexus Dashboard を使用して作成および展開した DHCP リレーポリシーが各サイトの APIC に正しくプッシュされることを確認する方法について説明します。作成する DHCP ポリシーは、ポリシーが関連付けられているブリッジドメインがサイトに展開しているときに、APIC にプッシュされます。

手順

ステップ 1 サイトの APIC GUI にログインします。

ステップ 2 上部のナビゲーションバーから、[**テナント(tenant)**] > **<テナント名>**を選択します。

DHCP ポリシーを展開したテナントを選択します。

ステップ 3 APIC で DHCP リレー ポリシーが設定されていることを確認します。

左側のツリー ビューで、**<テナント名>** > **ポリシー (Policies)** > **プロトコル (Protocol)** > **DHCP** > **リレー ポリシー(Relay policies)**に移動します。次に、設定した DHCP リレー ポリシーが作成されていることを確認します。

ステップ 4 DHCP オプション ポリシーが APIC で設定されていることを確認します。

DHCP オプション ポリシーを設定していない場合は、この手順をスキップできます。

左側のツリー ビューで、**<テナント名>** > **ポリシー (Policies)** > **プロトコル (Protocol)** > **DHCP** > **オプション ポリシー(Option Policies)**に移動します。次に、設定した DHCP オプション ポリシーが作成されていることを確認します。

ステップ 5 DHCP ポリシーがブリッジ ドメインに正しく関連付けられていることを確認します。

左側のツリー ビューで、**<テナント名>** > **ネットワーク** > **ブリッジ ドメイン** > **<ブリッジ ドメイン名>** > **DHCP リレー ラベル**に移動します。展開されたブリッジ ドメインにも DHCP ポリシーが関連付けられていることを確認します。

既存の DHCP ポリシーの編集または削除

このセクションでは、DHCP リレーまたはオプション ポリシーを編集または削除する方法について説明します。

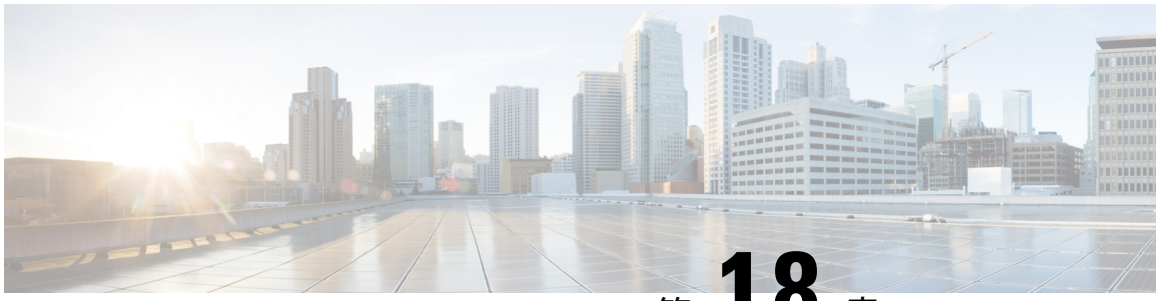
（注）
- ブリッジ ドメインに割り当てた後に DHCP ポリシーを変更し、ブリッジ ドメインを 1 つ以上のサイトに展開した場合は、DHCP ポリシーの変更が各サイトの APIC で更新されるように再展開する必要があります。
- 1つ以上のブリッジドメインに関連付けられているポリシーを削除することはできません。最初に、すべてのブリッジドメインからポリシーの割り当てを解除する必要があります。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから **[ポリシー]** を選択します。

ステップ 3 DHCP ポリシーの横にある [アクション] メニューをクリックし、**[編集 (Edit)]** または **[削除 (Delete)]** を選択します。



第 18 章

EPG 優先グループ

EPG 優先のグループ概要と制限

デフォルトでは、Multi-Site アーキテクチャは EPG 間でコントラクトが設定されている場合のみ、EPG 間の通信を許可します。EPG 間にコントラクトがない場合は、EPG 間の通信は明示的に無効になります。優先グループ（PG）機能を使用すると、同じ VRF の一部である複数の EPG を指定して、コントラクトを作成する必要なく、それらの間の完全な通信を可能にすることができます。

優先グループ 対 コントラクト

コントラクト優先グループが設定されている VRF で、EPG に利用可能なポリシー施行には 2 種類あります。

- **EPG を含む** – 優先グループのメンバーである EPG は、コントラクトなしでグループ内の他のすべての EPG と自由に通信できます。通信は、`source-any-destination-any-permit` のデフォルト ルールと適切な Multi-Site 変換に基づいています。
- **EPG を除外** - 優先グループのメンバーではない EPG は、相互に通信するためにコントラクトが必要です。そうしない場合、デフォルトの `source-any-destination-any-deny` ルールが適用されます。

コントラクト優先グループ機能を使用すると、拡張 VRF コンテキストのサイト間での EPG 間の通信をより詳細に制御し、設定を容易にすることができます。拡張 VRF の 2 つ以上の EPG がオープン通信を要求する一方で、他は制限された通信しかもてない場合、コントラクト優先グループとフィルタ付きのコントラクトの組み合わせを設定し、EPG 内の通信を正確に制御できます。優先グループから除外されている EPG は、`source-any-destination-any-deny`デフォルト ルールを上書きするコントラクトがある場合にのみ、他の EPG と通信できます。

拡張 対 シャドウ

複数のサイトの EPG が同じコントラクト優先グループの一部になるように構成されている場合、Nexus Dashboard Orchestrator は他のサイトに各サイトの EPG のシャドウを作成して、EPG からサイト間接続を正しく変換およびプログラムします。次に、コントラクト優先グループポリシーコンストラクトが、EPG 間通信の実際の EPG とシャドウ EPG の間の各サイトに適用されます。

たとえば、Site1 のウェブサービス EPG1 と Site2 のアプリサービス EPG2 がコントラクト優先グループに追加される場合を考察します。次に、EPG1 が EPG2 にアクセスする場合は、最初にサイト 2 のシャドウ EPG1 に変換され、次にコントラクト優先グループを使用して EPG2 と通信できるようになります。適切な BD は、その下の EPG がコントラクト優先グループの一部である場合、拡張されるか、シャドウされます。

VRF 優先グループ設定

優先グループを APIC で直接設定する場合は、個々の EPG で PG メンバーシップを有効にする前に、まず VRF で設定を明示的に有効にする必要があります。VRF の PG 設定が無効になっている場合、EPG はその VRF の優先グループの一部であっても、コントラクトなしでは通信できません。

（注） リリース 4.0（1）以降、NDO の PG 構成は、APIC の場合と同じアプローチに従います。つまり、VRF の PG 構成は、その VRF の一部である EPG が PG 構成を使用するために明示的に有効にする必要があります。

Nexus ダッシュボードオーケストレータのリリース 4.0（1）以前のリリースでは、GUI で VRF の PG 設定を管理することはできませんが、代わりに次のように動的に設定を調整します。

- NDO から VRF を作成および管理する場合、NDO は、その VRF に属する EPG が優先グループの一部であるかどうかに基づいて、VRF PG 値を動的に有効または無効にします。

  つまり、1 つ以上の EPG を優先グループに追加すると、NDO は VRF の PG 設定を自動的に有効にします。優先グループから最後の EPG を削除すると、NDO は VRF フラグを無効にします。

- VRF で PG オプションを永続的に有効にするには、最初に APIC で VRF の PG を直接有効にしてから、その VRF を NDO にインポートします。

  VRF の優先グループからすべての EPG を削除しても、NDO は設定を保持し、自動的に無効にしません。

- 最初に PG 設定を変更せずに APIC から VRF をインポートすると、NDO はオブジェクトを NDO から作成されたかのように管理し、EPG メンバーシップに基づいて PG 設定を動的に上書きします。

制限事項

EPG の優先グループを使用するとき次のガイドラインと制限を使用します：

- 優先グループは、サイト間 L3Out 外部 EPG ではサポートされません。
- 特定の VRF の EPG および外部 EPG オブジェクトは、その VRF の vzAny がすでにコントラクトを使用または提供している場合、優先グループの一部として設定しないでください。

優先グループに対する EPG の設定

このセクションでは、VRF および EPG で優先グループ（PG）構成を有効にする方法について説明します。

始める前に

スキーマ テンプレートに 1 つ以上の EPG を追加する必要があります。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 左側のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 3 VRF で PG を有効にします。

a) 優先グループに含める EPG によって使用される VRF を含むスキーマを開きます。

b) **[概要を表示（View Overview）]** ドロップダウンから、VRF を含むテンプレートを選択します。

c) VRF を選択します。

d) 右のプロパティ サイドバー内の**[優先されるグループ（Preferred Group）]** チェックボックスをチェックします。

これにより、その VRF の PG 構成が有効になりました。次の手順で説明するように、優先グループの一部にする 2 つ以上の EPG で PG 設定を有効にする必要があります。

e) **[保存（Save）]** をクリックして、テンプレートの変更を保存します。

ステップ 4 優先グループの一部として、1 つ以上の EPG を構成します。

（注）
一部の EPG が Nexus ダッシュボード オーケストレータによって管理され、一部がAPIC によってローカルに管理される優先グループを設定することはできません。

APIC のいずれかに既存の優先グループがあり、その優先グループから Nexus Dashboard Orchestrator に EPG をインポートすることを計画している場合は、グループ内のすべての EPG をインポートする必要があります。

a) 優先グループに含める EPG が別のスキーマまたはテンプレートにある場合は、そのテンプレートに移動します。

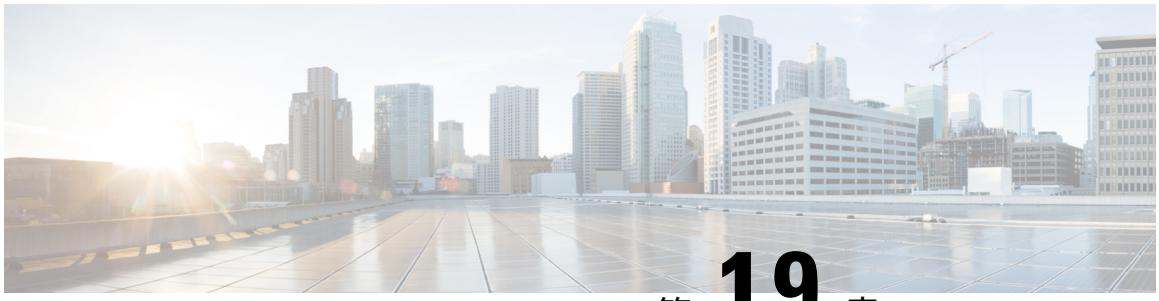
b) EPGを選択します。

c) 右側のプロパティ バーで、**[優先グループに含める（Include in Preferred Group）]** チェックボックスをオンにします。

d) **[保存（Save）]** をクリックして、テンプレートの変更を保存します。

ステップ 5 （オプション）すべての EPG が優先グループに追加されていることを確認します。

VRF を選択し、右側のプロパティサイドバーで **[優先されるグループ EPG（Preferred Group EPGs）]** リストを確認すると、優先グループの一部として構成されている EPG の完全なリストを表示できます。



第 19 章

サイト間 L3Out

サイト間 L3Out の概要

リリース 2.2(1) 以前、Nexus Dashboard Orchestrator により管理される各サイトでは、トラフィックをファブリックの外にルートするために設定された固有のローカル L3Out が必要で、それによりしばしば 1 つのサイトのエンドポイントと別のサイトの L3Out に接続されたサービス (ファイアウォール、サーバロードバランサー、またはメインフレーム) の間のコミュニケーションの欠如を導くことがありました。

リリース 2.2(1) は、1 つのサイトにあるエンドポイントが、外部ネットワーク、メインフレーム、またはサービス ノードなどのリモート L3Out を通じて到達可能なエンティティとの接続を確立する多くのシナリオを有効にする機能を追加します。

このような要素として、次のものが挙げられます。

- サイト間の L3Out：別のサイトの L3Out を使用した 1 つのサイトのアプリケーション EPG のエンドポイント。
- サイト間中継ルーティング：異なるサイトに展開された L3Out（同じ VRF の両方の L3Out）の背後に接続されたエンティティ（エンドポイント、ネットワークデバイス、サービス ノードなど）間の通信を確立します。
- サイト間 L3Out の共有サービス：リモート E3Out へのアプリケーション EPG またはサイト間中継ルーティング。

次のセクションは、サイト間L3Outの使用例の実装に必要なオブジェクトを作成するために実行できる一般的な GUI 手順に分かれています。その後、サポートされる各使用例のシナリオに固有の概要とワークフローを示します。

（注） 「サイト間 L3Out」という用語は、リモート サイトの L3Out 接続を介して到達可能な外部リソースへの通信を可能にする機能を指します。ただし、このドキュメントでは、この用語は特定のリモート L3Out オブジェクトを示すためにも使用されることがあります。

サイト内 L3Out のガイドラインと制約事項

サイト間 L3Out を構成するときは、次のことを考慮する必要があります。

- サイト間 L3Out は IPv4 と IPv6 に対してサポートされています。
- サイト間 L3Out では、Multi-Site トポロジ内のサイト間で常に確立される BGP eVPN セッションに加えて、サイト間 L3Out 機能をサポートするために MP BGP VPNv4（または VPNv6）セッションが作成されます。
- リリース 2.2(1) 以前のリリースからアップグレードしている場合、サイト ローカル レベルの既存の外部 EPG から L3Out への関連付けは保持されます。さらに、Nexus Dashboard Orchestrator は L3Out の作成とテンプレート レベルでの外部 EPG との関連付けをサポートするようになりました。

  スキーマ テンプレートで新しい L3Out を作成し、既存の外部 EPG に関連付ける場合：

  - L3Out が APIC ですでに定義されている L3Out と**同じ名前**の場合、Orchestrator その L3Outの所有権を取得しますが、L3Out ノードプロファイル、インターフェースプロファイル、プロトコル設定、またはルート制御設定の構成を管理しません。

（注） L3Out が APIC にすでに存在する場合は、NDO から同じ名前の新しい L3Out を作成するのではなく、関連付けられた外部 EPG とともに Nexus Dashboard Orchestrator にインポートすることをお勧めします。

    次に、Orchestrator からこの L3Out を削除することにすると、それは Orchestrator により管理されなくなりますが、以前から存在する L3Out の構成は APIC に保存されます。

  - L3Out が L3Out で定義された APIC とは **異なる名前** がある場合、外部 EPG は、APIC で定義された L3Out から削除され、Orchestrator で定義された L3Out に追加されます。これが APIC で定義された L3Out での唯一の外部 EPG である場合、これにより設定が境界リーフから削除され、トラフィックに影響を与える可能性があります。

- リリース 2.2(1) より前のリリースにダウングレードすることを選択した場合、Orchestrator NDO で作成された L3Out はテンプレートに存在しなくなるため、外部 EPG と L3Out 間のテンプレート レベルの関連付けは削除されます。この場合、サイト ローカル レベルで、外部 EPG と L3Out の関連付けを手動で再構成する必要があります。ダウングレード中、サイトローカルの関連付けは保持されます。
- これで、1 つのサイトのブリッジ ドメインを別のサイトの L3Out に関連付けることができますが、両方が同じ VRF にある必要があります。

  この関連付けはサイトローカル レベルで実行され、リモート L3Out から BD サブネットをアドバタイズし、ローカル L3Out に障害が発生した場合でも BD へのインバウンド トラフィックを維持できるようにするために必要です。
- サイト間 L3Out に関連付けられた VRF のポリシー制御施行方向は、デフォルトの入力モードで構成されたままにする必要があります。
- 次のシナリオは、サイト間 L3Out およびリモートリーフ (RL) ではサポートされていません。
  - 別々のサイトに関連付けられた RL ペアにデプロイされた L3Out 間のトランジット ルーティング
  - リモート サイトに関連付けられた RL ペアに展開された L3Out と通信するサイトに関連付けられた RL ペアに接続されたエンドポイント
  - リモート サイトに関連付けられた RL ペアに展開された L3Out と通信するローカル サイトに接続されたエンドポイント
  - リモート サイトに展開された L3Out と通信するサイトに関連付けられた RL ペアに接続されたエンドポイント
- 次の他の機能は、ACI Multi-Site のサイト間 L3Out ではサポートされていません。
  - 別のサイト L3Out を介して外部ソースからマルチキャストを受信するサイト内のマルチキャスト レシーバー。サイトで外部ソースから受信したマルチキャストが他のサイトに送信されることはありません。サイトのレシーバーが外部ソースからマルチキャストを受信する場合、ローカルの L3Out で受信する必要があります。
  - PIM-SM Any Source Multicast (ASM) を使用して外部レシーバーにマルチキャストを送信する内部マルチキャスト ソース。内部マルチキャスト ソースは、ローカル L3Out から外部ランデブー ポイント (RP) に到達できる必要があります
  - GOLF
  - 外部 EPG の優先グループ

外部 TEP プールの設定

サイト間 L3Out には、各ポッドの境界リーフ スイッチに外部 TEP アドレスが必要です。外部 TEP プールがすでに設定されている場合(たとえば、リモート リーフなどの別の機能のために)は、同じプールを使用できます。既存の TEP プールは Nexus Dashboard Orchestrator に継承され、インフラストラクチャ設定の一部として GUI に表示されます。それ以外の場合は、この項で説明されているように、GUI で TEP プールを追加できます。

（注） すべてのポッドに一意の TEP プールを割り当てる必要があり、ファブリック内の他の TEP プールと重複しないようにする必要があります。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）] > [サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のサイドバーで、設定するサイトを選択します。

ステップ 5 メイン ウィンドウで、サイト内のポッドをクリックします。

ステップ 6 右側のサイドバーで、**[+ TEP プールを追加 (+Add TEP Pool)]** をクリックします。

ステップ 7 **[TEP プールの追加 (Add TEP pool)]** ウィンドウで、そのサイトに対して設定する外部 TEP プールを指定します。

（注）
追加しようとしている TEP プールが他の TEP プールまたはファブリックアドレスと重複していないことを確認する必要があります。

ステップ 8 このプロセスを、サイト間の L3Outs を使用する予定のサイトおよびポッドごとに繰り返します。

サイト間 L3Out および VRF の作成またはインポート

ここでは、L3Out を作成し、それを Orchestrator GUI で VRF に関連付ける方法について説明します。これは APIC サイトにプッシュされるか、または APIC サイトの 1 つから既存の L3Out をインポートします。次に、この L3Out を外部 EPG に関連付け、その外部 EPG を使用して特定のサイト間 L3Out の使用例を設定します。

（注） L3Out に割り当てる VRF は、任意のテンプレートまたはスキーマにすることができますが、L3Out と同じテナントに存在する必要があります。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 3 [スキーマ (schema)] を選択し、VRF と L3Out を作成またはインポートするテンプレートを選択します。

1 つのサイトに関連付けられているテンプレートで L3Out を作成することを推奨します。この場合、そのサイトでのみ L3Out が作成されます。

または、複数のサイトに関連付けられているテンプレートでL3Outを作成することもできます。この場合、すべてのサイトで同じ名前で L3Out が作成されます。これにより、この章で後述するように、いくつかの機能制限が生じる可能性があります。

ステップ 4 新しい VRF と L3Out を作成します。

既存の L3Out をインポートする場合は、この手順をスキップします。

（注）
Orchestrator で L3Out オブジェクトを作成し、それを APIC にプッシュすることはできますが、L3Out の物理設定は APIC で実行する必要があります。

a) **[VRF]** エリアまで下にスクロールし、+ アイコンをクリックして新しい VRF を追加します。

L3Out に使用する予定の VRF がすでにある場合は、このサブステップをスキップします。

右側のサイドバーで、VRF の名前を入力します (例: `vrf-l3out`)。

b) **[L3Out]** 領域まで下にスクロールし、+ アイコンをクリックして新しい L3Out を追加します。

右側のスライダで、必要な情報を入力します。

c) L3Out の名前を指定します (例: `l3out-intersite`。

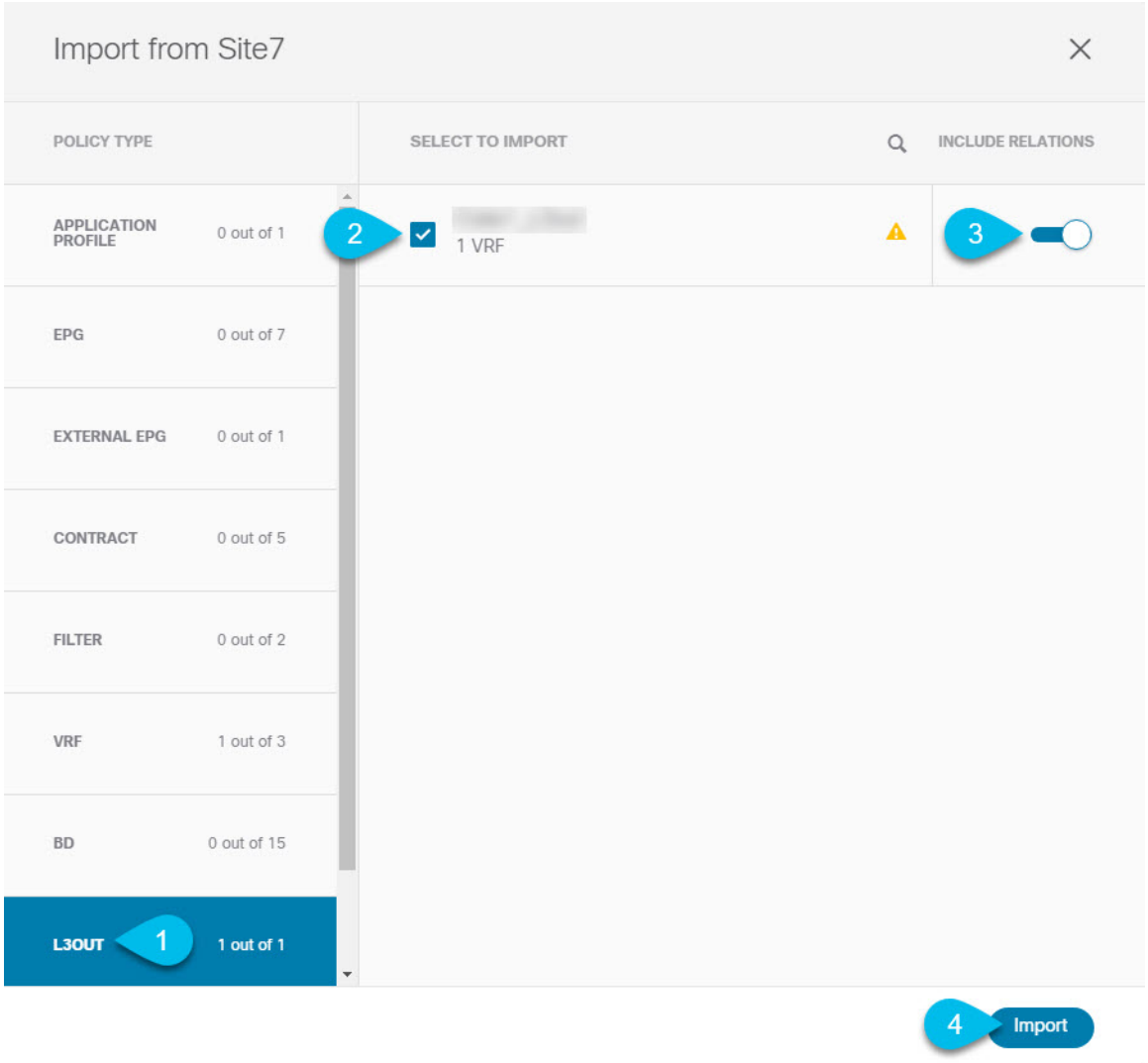
d) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、VRF を選択します。

最初のサブステップで作成した VRF を選択するか、既存の VRF を選択します。

ステップ 5 既存の VRF および L3Out をインポートします。

前の手順で新しい L3Out を作成した場合は、この手順をスキップします。

メイン ウィンドウ ペインの **[インポート (Import)]** をクリックして、



a) メイン テンプレート ビューの上部で、**[インポート (Import)]** をクリックします。

b) L3Out をインポートするサイトを選択します。

c) [インポート (Import)] ウィンドウの **[ポリシー タイプ(Policy Type)]** メニューで、[**L3Out**] を選択します。

d) インポートする L3Out をチェックします。

デフォルトでは、L3Outをインポートすると、対応するVRFもインポートされます。これは、サイト固有のテンプレートでL3Outをインポートする場合、通常は複数のサイトに関連付けられた拡張テンプレートでVRFを定義するため、望ましくない場合があります。この場合、L3Outをインポートする前に[Include Relationships]オプションを無効にします。この場合、インポート後にL3Outを正しいVRFに再マッピングする必要もあります。

e) [インポート（Import）] をクリックします。

f) L3Outのみをインポートした場合は、テンプレートビューでそれを選択し、適切なVRFに関連付けます。

サイト間 L3Out を使用するための外部 EPG の設定

このセクションでは、サイト間L3Outと関連付ける外部EPGの作成方法について説明します。その後、この外部 EPG とコントラクトを使用すれば、あるサイトのエンドポイント用の特定のユース ケースを設定し、別のサイトの L3Out を使用することができます。

始める前に

L3Out を作成し、サイト間L3OutおよびVRFの作成またはインポート （234ページ）に説明されている方法で VRF と関連付けます。

手順

ステップ 1 外部 EPG を作成するテンプレートを選択します。

複数のサイトと関連付けられているテンプレート内で外部 EPG を作成した場合、その外部 EPG は、それらすべてのサイト上で作成されます。これは、外部 EPG の L3Out が WAN などの一連の共通外部リソースへのアクセスを提供する場合に推奨されます。

単一のサイトと関連付けられているテンプレート内で外部 EPG を作成した場合、その外部 EPG は、そのサイト内でのみ作成されます。これは、外部 EPG の L3Out がそのサイトからのみアクセス可能な外部リソースへのアクセスを提供する場合に推奨されます。

ステップ 2 **[外部 EPG (External EPG)]** エリアまで下方にスクロールして、+ アイコンをクリックして外部 EPG を追加します。

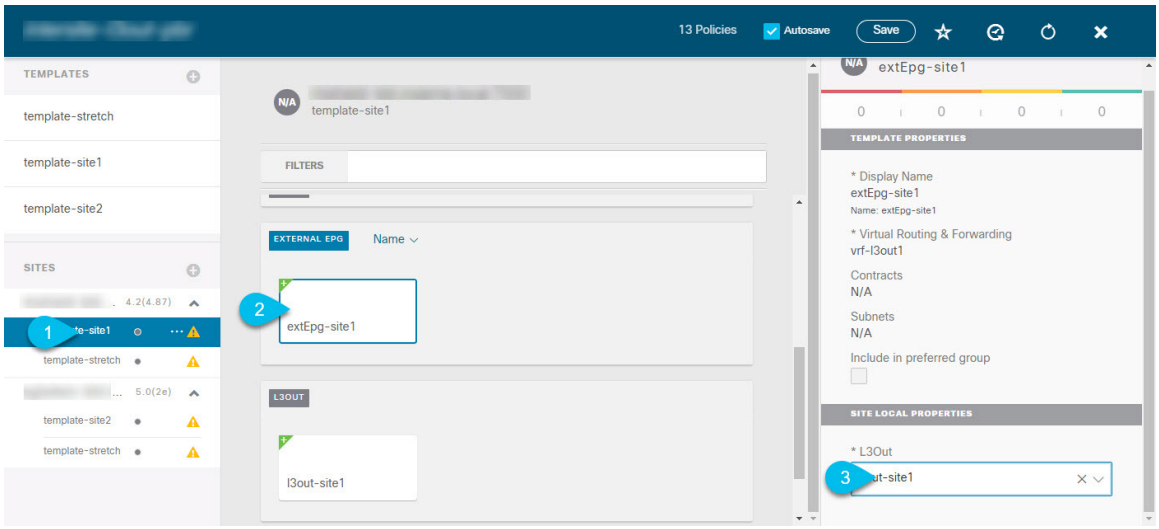
右側のスライダで、必要な情報を入力します。

a) 外部 EPG の名前を入力します。たとえば `[eepg-intersite-l3out]` のようにします。
b) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、先ほど作成した、L3Out 用の VRF を選択します。

ステップ 3 外部 EPG を L3Out にマッピングします。

サイトレベルまたはテンプレートレベルで、外部EPGをL3Outにマッピングできます。通常、各サイトはローカルL3Outを一意の名前で定義するため、外部EPG自体が拡張されているかどうかに関係なく、外部EPGを各サイト固有のL3Outに選択的にマッピングできます。それで、サイトレベルでマッピングを作成することをお勧めします。

L3Out をサイトローカル レベルで外部 EPG に関連付けるには、次の手順に従います。



a) スキーマ ビューの左サイドバーで、外部 EPG が配置されているテンプレートを選択します。

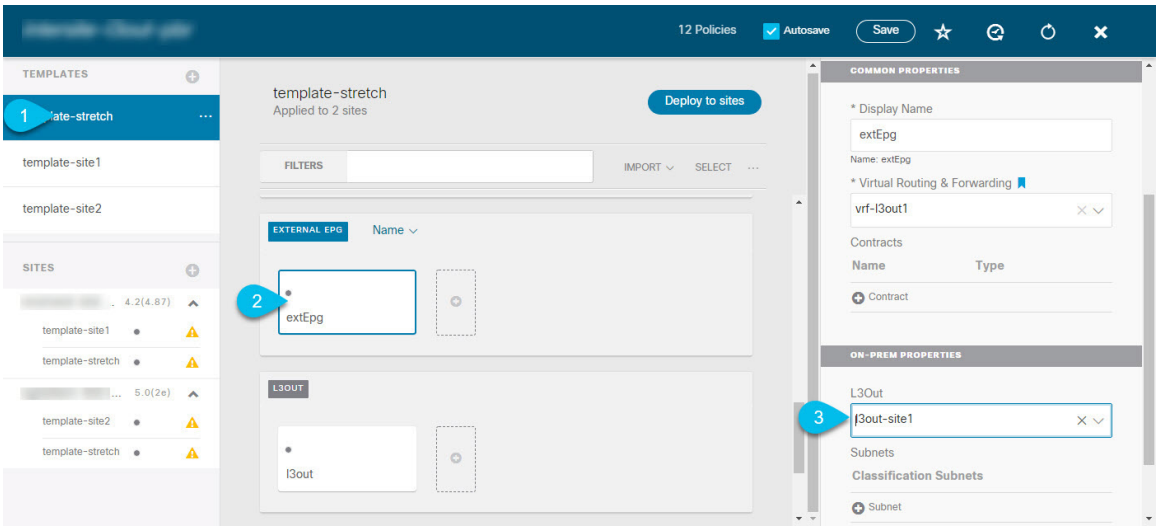
b) **[外部 EPG (External EPG)]** エリアまで下方にスクロールして、外部 EPG を選択します。

c) 右サイドバーで、**[L3Out]** ドロップダウンまで下方にスクロールして、作成したサイト間 L3Out を選択します。

この場合、APIC で管理されている L3Out と、オーケストレーションで管理されている L3Out の両方が選択できます。前のセクションでこの目的のため特に作成した L3Out、またはサイトの APIC 内にすでにある L3Out のいずれかを選択します。

サイト レベルまたはテンプレート レベルで、外部 EPG を L3Out にマッピングできます。これにより、複数のサイトで同じ L3Out 名が定義されている展開での設定が容易になりますが、マルチ サイト ドメインや および外部ルーテッド ネットワークの一部であるファブリック間で確立できる接続タイプの柔軟性が低下するため、このアプローチは推奨されません。たとえば、特定の BD のサブネットがアドバタイズされる場所を制御することはできません。これは、L3Out に BD をマッピングすると、すべての L3Out が同じ名前を持つため、すべてのサイトのすべての L3Out から BD サブネットがアドバタイズされるためです。

テンプレート レベルで L3Out を外部 EPG に関連付けるには、次の手順を実行します。



a) スキーマ ビューの左サイドバーで、外部 EPG が置かれているテンプレートを選択します。

b) **[外部 EPG (External EPG)]** エリアまで下方にスクロールして、外部 EPG を選択します。

c) 右サイドバーで、**[L3Out]** ドロップダウンまで下方にスクロールして、作成したサイト間 L3Out を選択します。

また、テンプレート レベルで L3Out に最初に関連付けられた外部 EPG の設定を、サイトレベルのマッピングに移行することもできます。これを行うには、外部 EPG の VRF 関連付けを削除し、外部 EPG を同じ VRF に再び関連付け、それからサイトレベルで L3Outs をマッピングします。このプロセスがテンプレートを展開する前に一度に完了しておけば、APIC 側で実際に変更が適用されないため、新しい設定をプッシュする際にトラフィックに影響はありません。

ステップ 4 外部 EPG に 1 つ以上のサブネットを設定します。

a) 外部 EPG を選択します。

b) 右側のサイドバーで、**[+ サブネットを追加 (+Add Subnet)]** をクリックします。

c) **[サブネットを追加 (Add Subnet)]** ウィンドウで、分類サブネットと必要なオプションを入力します。

設定するプレフィックスとオプションは、使用例によって異なります。

- 着信トラフィックを外部 EPG に属するものとして分類するには、指定したプレフィックスの **[外部 EPG の外部サブネット (External Subnets for External EPG)]** フラグを選択します。使用例に応じて、内部 EPG またはリモート L3Out 経由で到達可能な外部ネットワーク ドメインとの契約を適用できます。

- この L3Out から（同じサイトまたはリモート サイト内の）別の L3Out から学習した外部プレフィックスをアドバタイズするには、指定したプレフィックスの **[エクスポート ルート制御 (Export Route Control)]** フラグを選択します。`0.0.0.0/0` プレフィックスを指定する場合は、L3Out からのすべてのプレフィックスをアドバタイズするために **[集約エクスポート (Aggregate Export)]** フラグを選択できます。 **[集約エクスポート (Aggregate Export)]** フラグが有効になっていない場合、デフォルト ルートの `0.0.0.0/0` だけがアドバタイズされます（ボーダー リーフ ノードのルーティング テーブルに存在する場合）。

- 外部ネットワークから受信した特定のルートを除外するには、指定したプレフィックスの **[ルート制御のインポート (Import Route Control)]** フラグを選択します。`0.0.0.0/0` を指定する場合は、**[集約インポート (Aggregate Import)]** オプションを選択することもできます。

  これは、BGP を外部ルータとピアリングする場合にのみ可能であることに注意してください。

- 異なるVRFにルートをリークするには、**[共有ルート制御 (Shared Route Control)]** と関連する **[集約共有ルート(Aggregate Shared Routes)]** フラグ、および **[共有セキュリティ インポート (Shared Security Import)]** フラグを選択します。これらのオプションは、VRF 間共有 L3Out および VRF 間サイト間中継ルーティングの特定の使用例に必要です。

サイト間 L3Out のコントラクトの作成

ここでは、サイトに展開されたアプリケーション EPG と、別のサイトの L3Out に関連付けられた外部 EPG（サイト間 L3Out 機能）との間の通信を可能にするために使用するフィルタとコントラクトを作成する方法について説明します。

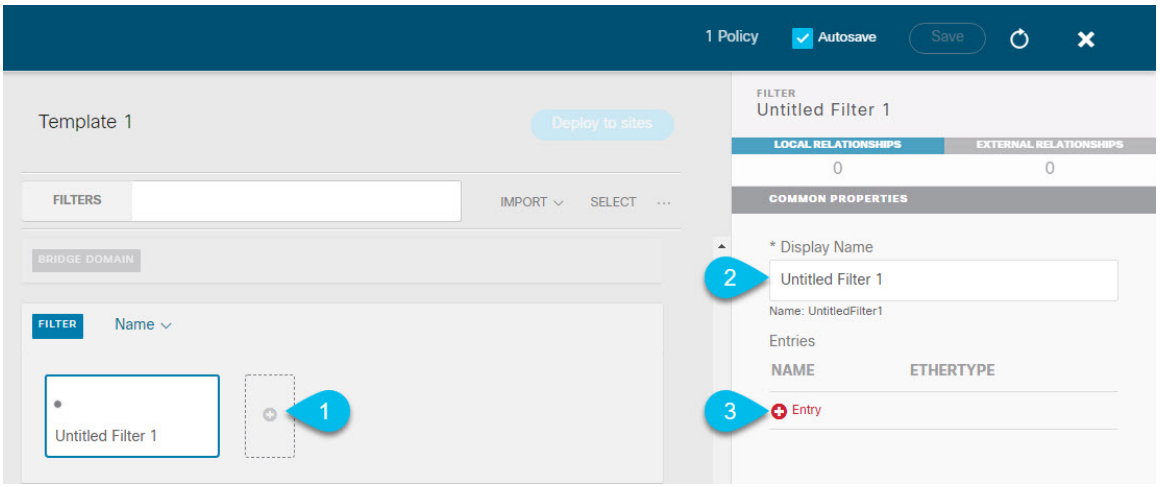
手順

ステップ 1 コントラクトとフィルタを作成するためのテンプレートを選択します。

L3Out、VRF、および外部 EPG を作成したのと同じスキーマとテンプレートを使用できます。または、別のスキーマとテンプレートを選択することもできます。

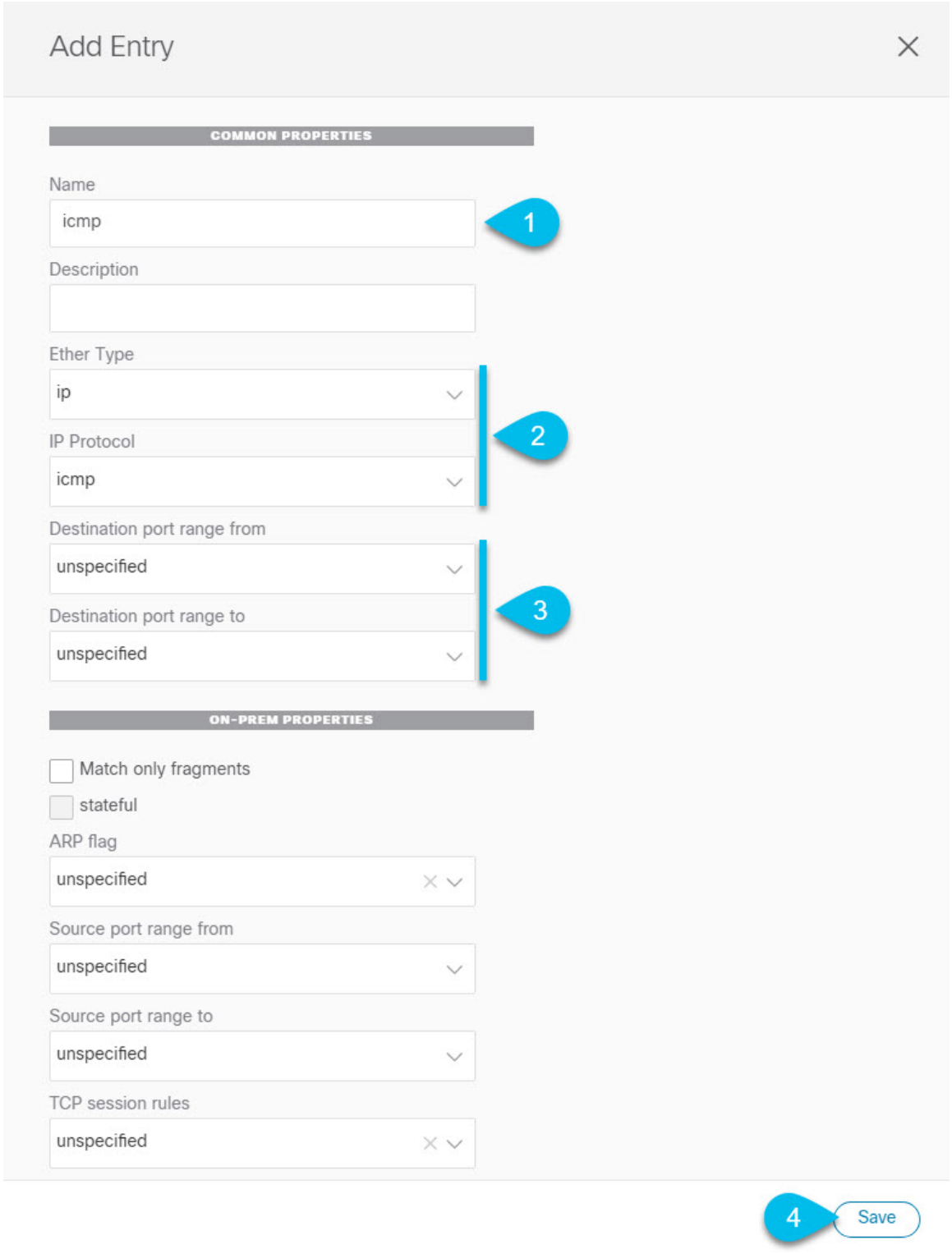
コントラクトは異なるサイトに展開されたオブジェクト（EPG および外部 EPG）に適用されるため、複数のサイトに関連付けられたテンプレートで定義することを推奨します。ただし、これは必須ではありません。コントラクトとフィルタが Site1 のローカル オブジェクトとしてのみ定義されている場合でも、 Site2 のローカル EPG または外部 EPG がそのコントラクトを消費または提供する必要がある場合、NDO はリモート Site2 に対応するシャドウ オブジェクトを作成します。 。

ステップ 2 フィルタを作成します。



a) **[Filter (フィルタ)]** エリアまでスクロールし、**[+]** をクリックしてフィルタを作成します。
b) 右側のペインで、フィルタの **[表示名 (Display Name)]** を入力します。
c) 右側のペインで、**[+ エントリ (+ Entry)]** をクリックします。

ステップ 3 フィルタの詳細を入力します。



a) フィルタの **[名前 (Name)]** を指定します。
b) **[イーサー タイプ (Ether Type)]** を選択します。

たとえば [ip] です。

c) **[IP プロトコル (IP Protocol)]** を選択します。

たとえば [icmp] です。

d) 他のプロパティは未指定のままにします。

e) **[保存 (Save)]** をクリックしてフィルタを保存します。

ステップ 4 コントラクトの作成

a) 中央ペインで、**[コントラクト (Contracts)]** エリアまで下方にスクロールし、**[+]** をクリックして、コントラクトを作成します。

b) 右側のペインで、コントラクトの **[表示名 (Display Name)]** を入力します。

c) コントラクトの適切な **[範囲 (Scope)]** を選択します。

サイト間 L3Out の別の VRF にある共有サービス エンドポイントを設定する場合にはは、その範囲の テナント を選択する必要があります。それ以外の場合、両方が同じ VRF 内にある場合は、範囲を vrf に設定できます。

d) コンシューマからプロバイダーへの方向とプロバイダーからコンシューマへの方向の両方に同じフィルタを適用する場合は、**[両方向に適用 (Apply both directions)]** ノブを切り替えます。

このオプションを有効にした場合は、フィルタを 1 回だけ指定することが必要となり、両方向のトラフィックに適用されます。このオプションを無効のままにした場合は、各方向に 1 つずつ、2 セットのフィルタ チェーンを指定する必要があります。

ステップ 5 コントラクトにフィルタを割り当てる

a) 右側のペインで、**[フィルタ チェーン (Filter Chain)]** 領域までスクロールし、**[+ フィルタ (+ Filter)]** をクリックしてフィルタをコントラクトに追加します。

コントラクトで [両方向に適用 (Apply both directions)] オプションを無効にした場合は、他のフィルタ チェーンに対してこの手順を繰り返します。

b) 開いた **[フィルタ チェーンの追加]** ウィンドウで、**[名前 (Name)]** ドロップダウン メニューから前の手順で追加したフィルタを選択します。

c) **[保存 (Save)]** をクリックして、フィルタをコントラクトに追加します。

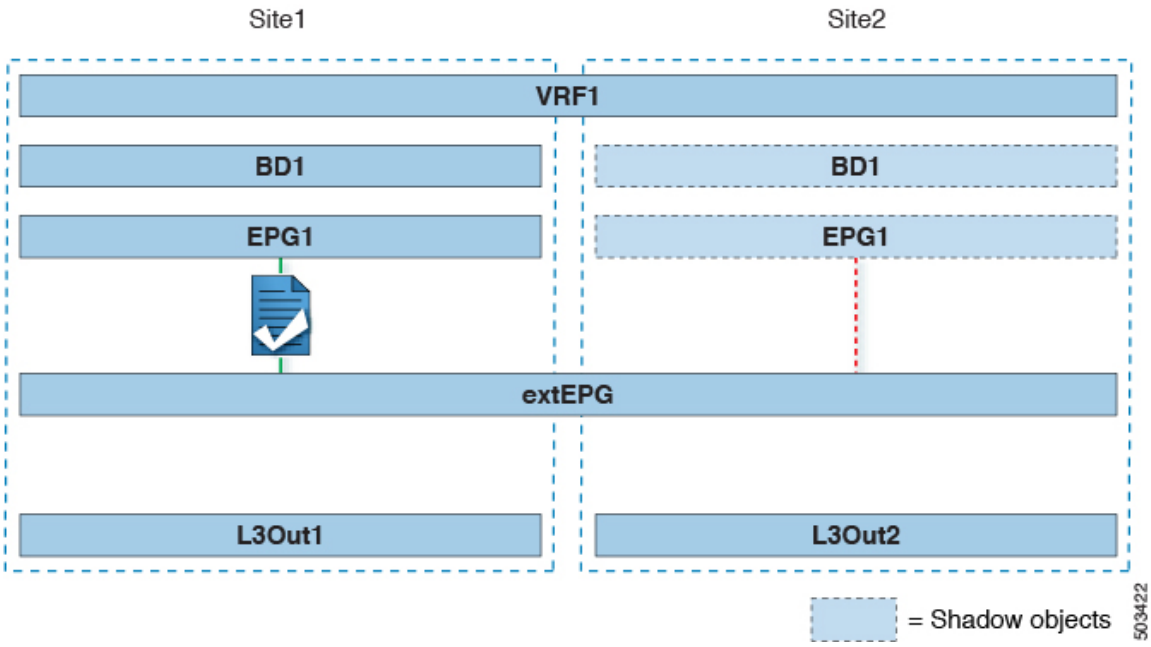
使用例

アプリケーション EPG のサイト間 L3Out（VRF内）

ここでは、アプリケーション EPG の一部であるエンドポイントが、同じ VRF（intra-VRF）内にある別のサイトに展開された L3Out を介して到達可能な外部ネットワークドメインと通信できるようにするために必要な設定について説明します。

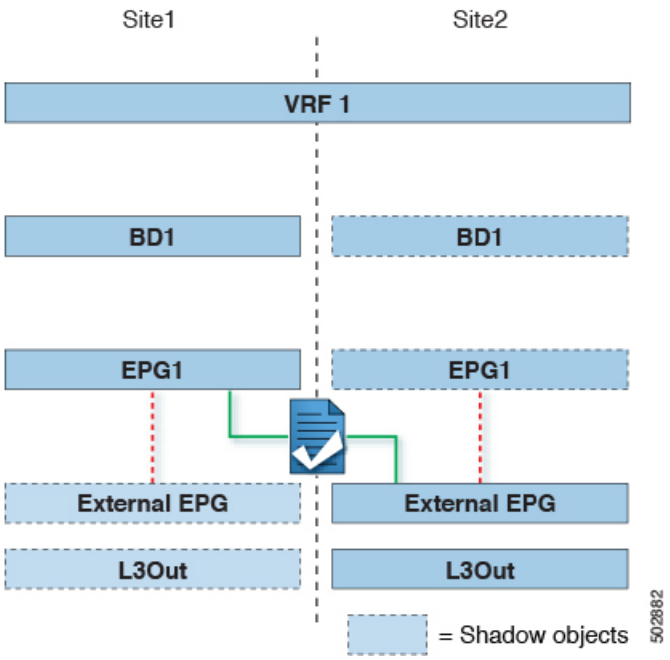
最初の図は、拡大された外部 EPG と、両方のサイトで作成される関連づけられた L3Out を示しています。アプリケーション EPG (EPG1) はサイト 1 で作成され、外部 EPG とのコントラクトがあります。この使用例は、別のサイトの L3Out が外部リソースの共通セットへのアクセスを提供する場合に推奨されます。ポリシー定義と外部トラフィック分類が簡素化され、独立した APIC ドメインの各 L3Out に個別にルートマップポリシーを適用できます。

図 *14* : 拡張された外部 *EPG*



次の 2 番目の図は、同様の使用例を示していますが、外部 EPG は物理 L3Out が配置されているサイトだけに導入されています。アプリケーション EPG とコントラクトは、1 つのサイトの EPG と他方の物理 L3Out 間のトラフィックフローを可能にするのと全く同じ方法で設定します。

図 *15* : 拡張されていない (サイトローカルの) 外部 *EPG*



次の手順では、最も一般的なシナリオである図1に示す使用例を実装するために必要な設定について説明します。図2に示すユースケースを導入する場合は、若干の変更を加えて手順を調整できます。

始める前に

次のものがすでに設定されている必要があります。

- 3 つのテンプレートを持つスキーマ。

  アプリケーションEPGやL3Outsなど、そのサイトに固有のオブジェクトを設定する各サイトのテンプレート（`template-site1` や `template-site2` など）を作成します。さらに、ストレッチされたオブジェクト（この場合は外部 EPG）に使用する別のテンプレート（`template-stretched` など）を作成します。

- サイト間L3OutおよびVRFの作成またはインポート（234ページ）セクションで説明されている各サイトのL3Outs。

  この使用例では、各サイト固有のテンプレートに個別のL3Outがインポートまたは作成されます。

- サイト間 L3Out を使用するための外部 EPG の設定 （237 ページ） で説明されているように、サイト間 L3Out の外部 EPG。

  この使用例では、外部EPGは、ストレッチされたテンプレート（`template-stretched`）で定義されたストレッチされたオブジェクトとして設定されます。外部EPGが外部アドレス空間全体へのアクセスを提供すると仮定すると、より具体的なプレフィックスの長いリストを指定しないように、`0.0.0.0/0` プレフィックスを分類用に設定することを推奨します。

- サイト間 L3Out のコントラクトの作成 （240 ページ） で説明されているように、アプリケーション EPG と L3Out 外部 EPG の間で使用するコントラクト。

  ストレッチテンプレート（template-stretched）でコントラクトとフィルタを作成することをお勧めします。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 3 アプリケーション EPG とブリッジ ドメインのスキーマとテンプレートを選択します。

この使用例では、テンプレートを Site1 に関連付けます。

ステップ 4 L3Out とは別の VRF に属するアプリケーション EPG とそのブリッジ ドメインを設定します。

サイト間 L3Out を使用する EPG がすでにある場合は、この手順をスキップできます。

通常のように、EPG およびブリッジ ドメインを新規に作成するか、既存のものをインポートします。

ステップ 5 アプリケーション EPG にコントラクトを割り当てます。

a) EPG を選択します。
b) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
c) 前のセクションで作成したコントラクトとそのタイプを選択します。

アプリケーション EPGがコンシューマかプロバイダかを選択できます。

ステップ 6 コントラクトを、リモート L3Out にマップされた外部 EPG に割り当てます。

a) 外部 EPG が配置されている template-stretched を選択します。
b) 外部 EPG を選択します。
c) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
d) 前のセクションで作成したコントラクトとそのタイプを選択します。

アプリケーション EPG をコンシューマとして選択した場合は、外部 EPG のプロバイダを選択します。それ以外の場合は、外部 EPGのコンシューマを選択します。

ステップ 7 アプリケーション EPG のブリッジ ドメインを L3Out に関連付けます。

これにより、BD サブネットを L3Out から外部ネットワーク ドメインにアドバタイズできます。BD に関連付けられたサブネットは、L3Out からアドバタイズされるように **[外部アドバタイズ (Advertised Externally)]** オプションを使用して設定する必要があります。

a) 左側のサイドバーの **[サイト (Sites)]** の下で、アプリケーション EPG のテンプレートを選択します。
b) アプリケーション EPG に関連付けられたブリッジ ドメインを選択します。
c) 右側のサイドバーで、**[+ L3Out]** をクリックします。
d) 作成したサイト間 L3Out を選択します。

図1に示す使用例では、BD を Site1 と Site2 で定義された両方の L3Out に関連付けて、外部ネットワークが両方のパスから EPG にアクセスできるようにします。特定のポリシーを L3Out または外部ルータに関連付けて、特定の L3Out パスが着信トラフィックに通常優先されるようにすることができます。リモート サイトの L3Out を介した最適ではないインバウンド トラフィック パスを回避するために、EPG と BD が（特定の例のように）サイトに対してローカルである場合、これを推奨します。

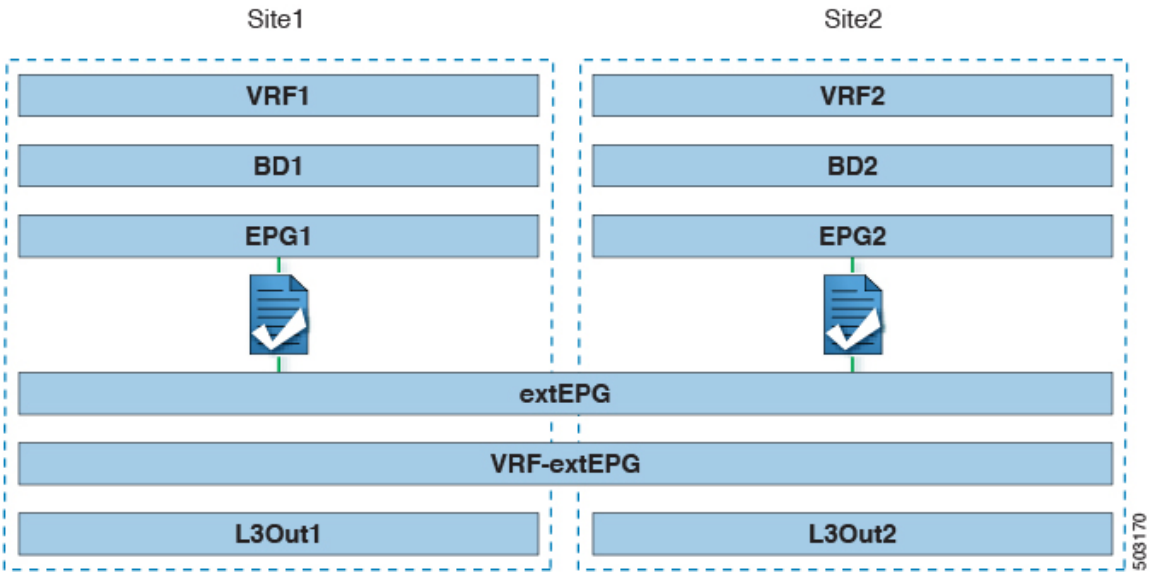
ステップ 8 スキーマを展開します。

アプリケーションEPGのサイト間L3Outとの共有サービス（Inter-VRF）

ここでは、1 つの VRF のアプリケーション EPG の一部であるエンドポイントが、別のサイトに展開された L3Out を介して到達可能な外部ネットワーク ドメインと通信できるようにするために必要な設定について説明します。これは「共有サービス」とも呼ばれます。

このシナリオは、別のサイトの L3Out が外部リソースの共通セットへのアクセスを提供する場合に推奨されます。ポリシー定義と外部トラフィック分類が簡素化され、独立した APIC ドメインの各 L3Out に個別にルートマップポリシーを適用できます。

図 *16*：ストレッチ外部*EPG*、サイト ローカル *L3Out*、およびアプリケーション *EPG* のいずれかになります。



次の手順では、図 3 に示す使用例を実装するために必要な設定について説明します。

始める前に

次のものがすでに設定されている必要があります。

- 3 つのテンプレートを持つスキーマ。

  アプリケーション EPG や L3Outs など、そのサイトに固有のオブジェクトを設定するサイトごとのテンプレート（`template-site1` や `template-site2` など）を作成します。さらに、

ストレッチされたオブジェクト（この場合は外部 EPG）に使用する別のテンプレート（template-stretched など）を作成します。

- サイト間 L3Out および VRF の作成またはインポート （234 ページ）セクションで説明されている各サイトの L3Outs。

  この使用例では、各サイト固有のテンプレートに個別の L3Out がインポートまたは作成されます。

- サイト間 L3Out を使用するための外部 EPG の設定 （237 ページ） で説明されているように、サイト間 L3Out の外部 EPG。

  この使用例では、外部EPGは、ストレッチされたテンプレート（template-stretched）で定義されたストレッチされたオブジェクトとして設定されます。外部EPGが外部アドレス空間全体へのアクセスを提供すると仮定すると、より具体的なプレフィックスの長いリストを指定しないように、0.0.0.0/0プレフィックスを分類用に設定することを推奨します。

  この特定の共有サービスの使用例では、リモート L3Out の外部 EPG に関連付けられたサブネットの**共有ルート制御**フラグと**共有セキュリティインポートフラグ**を有効にする必要があります。外部EPGの分類に0.0.0.0/0プレフィックスを使用している場合は、**共有ルート制御**フラグに加えて、**集約共有ルート**フラグも有効にします。

- サイト間 L3Out のコントラクトの作成 （240 ページ） で説明されているように、アプリケーション EPG と L3Out 外部 EPG の間で使用するコントラクト。

  ストレッチテンプレート（template-stretched）でコントラクトとフィルタを作成することをお勧めします。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 3 アプリケーション EPG とブリッジ ドメインのスキーマとテンプレートを選択します。

この使用例では、テンプレートを Site1 に関連付けます。

ステップ 4 L3Out とは別の VRF に属するアプリケーション EPG とそのブリッジドメインを設定します。

サイト間 L3Out を使用する EPG がすでにある場合は、この手順をスキップできます。

通常のように、EPG およびブリッジ ドメインを新規に作成するか、既存のものをインポートします。

ステップ 5 アプリケーション EPG にコントラクトを割り当てます。

a) EPG を選択します。
b) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
c) 前のセクションで作成したコントラクトとそのタイプを選択します。

アプリケーション EPGがコンシューマかプロバイダかを選択できます。

（注）
アプリケーション EPG をプロバイダとして設定する場合は、そのルートを L3Out VRF にリークするために、EPG の下でも BD ですでに定義されているサブネットを設定する必要があります。サブネットの BD で使用されるのと同じフラグも EPG で設定する必要があります。さらに、EPG の下のサブネットでは、デフォルト ゲートウェイ機能が BD レベルで有効になっているため、**[デフォルト SVI ゲートウェイなし (No default SVI Gateway)]** フラグも有効にする必要があります。

ステップ 6 コントラクトを、L3Out にマップされた外部 EPG に割り当てます。

a) 外部 EPG が配置されている `template-stretched` を選択します。
b) 外部 EPG を選択します。
c) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
d) 前のセクションで作成したコントラクトとそのタイプを選択します。

アプリケーション EPG をコンシューマとして選択した場合は、外部 EPG のプロバイダを選択します。それ以外の場合は、外部 EPGのコンシューマを選択します。

ステップ 7 アプリケーション EPG のブリッジ ドメインを L3Out に関連付けます。

これにより、BD サブネットを L3Out から外部ネットワーク ドメインにアドバタイズできます。BD に関連付けられたサブネットは、L3Out からアドバタイズされるように **[外部アドバタイズ (Advertised Externally)]** オプションを使用して設定する必要があります。

a) 左側のサイドバーの **[サイト (Sites)]** の下で、アプリケーション EPG のテンプレートを選択します。
b) アプリケーション EPG に関連付けられたブリッジ ドメインを選択します。
c) 右側のサイドバーで、**[+ L3Out]** をクリックします。
d) 作成したサイト間 L3Out を選択します。

図1に示す使用例では、BD を Site1 と Site2 で定義された両方の L3Out に関連付けて、外部ネットワークが両方のパスから EPG にアクセスできるようにします。特定のポリシーを L3Out または外部ルータに関連付けて、特定の L3Out パスが着信トラフィックに通常優先されるようにすることができます。リモート サイトの L3Out を介した最適ではないインバウンド トラフィック パスを回避するために、EPG と BD が（特定の例のように）サイトに対してローカルである場合、これを推奨します。

ステップ 8 スキーマを展開します。

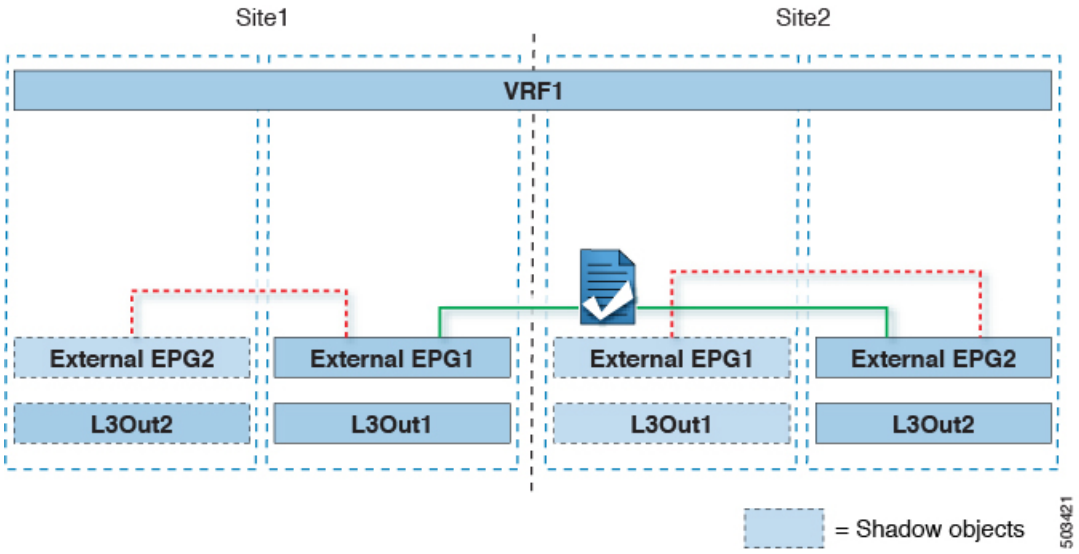
サイト間中継ルーティング

このセクションでは、マルチサイト ドメインが分散ルータとして機能し、異なるサイトに展開された L3Out の背後に接続されているエンティティ（エンドポイント、ネットワーク デバイス、サービス ノードなど）間の通信を可能にする使用例について説明します。この機能は通常、サイト間中継ルーティングと呼ばれます。 。サイト間中継ルーティングは、VRF 内および VRF 間のユースケースでサポートされます。

次の図は、異なるサイトに設定されている2つの L3Outs (`l3out1` と `l3out2`) を示しています。各 L3Out はそれぞれの外部 EPG (`ExtEPG1` および `ExtEPG2`) に関連付けられています。2 つの外部

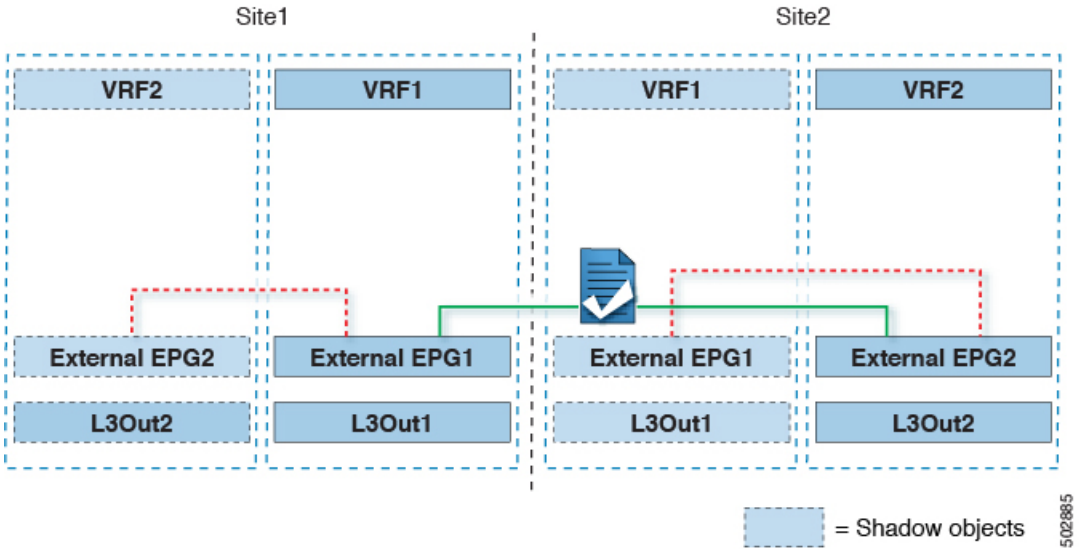
EPG 間のコントラクトにより、2 つの異なるサイトの 2 つの異なる L3Outs の背後にあるエンドポイント間の通信が可能になります。

図 *17 : VRF* サイト内中継ルーティング



各サイトの L3Out が異なる VRF にある場合も、同様の設定を使用できます。

図 *18 : VRF* サイト間中継ルーティング



図では、外部 EPG と、関連付けられた L3Out がサイトローカルのオブジェクトとして展開される、2つのシナリオを示しています。サイト間中継ルーティングは、サイト間でEPGがストレッチされていない場合、一方がストレッチされている場合、両方がストレッチされている場合という、すべての組み合わせをサポートしています。

サイト間中継ルーティングを導入する場合、サイト間で定義された異なる外部 EPG が異なる外部アドレス空間へのアクセスを提供する（明らかに重複しない）ことが前提となります。したがって、分類に使用されるプレフィックスの設定には、いくつかのオプションがあります。

- 両方の外部 EPG で同じ `0.0.0.0/0` プレフィックスを定義して、L3Out1 の境界リーフ ノードで受信した着信トラフィックが Ext-EPG1 にマッピングされ、L3Out2 で受信した着信トラフィックが Ext-EPG2 にマッピングされるようにします。L3Out は別のファブリックで定義されているため、この設定で競合の問題は発生しません。

  `L3Out1`で受信した外部プレフィックスは、`L3Out2` からアドバタイズする必要があります。その逆も同様です。両方の外部 EPG で `0.0.0.0/0` を分類サブネットとして使用している場合は、**[エクスポート ルート制御 (Export Route Control)]** および **[集約エクスポート (Aggregate Export)]** フラグを有効にするだけで十分です。

- 外部 EPG ごとに特定のプレフィックスを定義します。この場合、ローカル外部 EPG とリモート外部 EPG 間のコントラクトのためにシャドウ外部 EPG がそのサイトで作成されるときに、サイトの APIC によって障害が発生するのを回避するために、プレフィックスが重複していないことを確認する必要があります。

  特定のプレフィックスを使用する場合は、`外部 EPG1` で分類用に設定したの同じプレフィックスを、**[エクスポートルート制御 (Export Route Control)]** フラグを立てて、`外部 EPG2` で設定する必要があります。逆の場合も同じです。

（注） 2 つの分類アプローチのどちらを導入する場合でも、VRF 間シナリオでは、**[共有ルート制御 (Shared Route Control)]**（加えて **[集約共有ルート (Aggregate Shared Routes)]** も `0.0.0.0/0` を使用する場合には必要）および **[共有セキュリティ インポート (Shared Security Import)]** の各フラグを設定する必要があります。

始める前に

次のものがすでに設定されている必要があります。

- 3 つのテンプレートを持つスキーマ。

  アプリケーション EPG や L3Outs など、そのサイトに固有のオブジェクトを設定するサイトごとのテンプレート（`template-site1` や `template-site2` など）を作成します。さらに、ストレッチされたオブジェクト（この場合は外部 EPG）に使用する別のテンプレート（`template-stretched` など）を作成します。

- サイト間L3OutおよびVRFの作成またはインポート （234ページ）セクションで説明されている各サイトのL3Outs。

  この使用例では、各サイト固有のテンプレートに個別のL3Outがインポートまたは作成されます。

- 異なるサイトにある2つの異なる L3Outs 用の 2 つの異なる外部 EPG。サイト間 L3Out を使用するための外部 EPG の設定 （237 ページ） の説明に従って、同じ手順を使用して両方の外部 EPG を作成できます。

- サイト間L3Outのコントラクトの作成（240ページ）で説明されているように、サイトごとに定義されたL3Out外部EPGの間でコントラクトを使用します。

  ストレッチテンプレート（`template-stretched`）でコントラクトとフィルタを作成することをお勧めします。

手順

ステップ1 Cisco Nexus Dashboard Orchestrator のGUIにログインします。

ステップ2 左型のナビゲーションメニューで、**[アプリケーション管理(Application Management)]**>**[スキーマ(Schemas)]**を選択します。

ステップ3 いずれかの外部EPGにコントラクトを割り当てます。

a) 外部EPGが配置されているスキーマとテンプレートを選択します。
b) 外部EPGを選択します。
c) 右側のサイドバーで、**[+コントラクト(+Contract)]**をクリックします。
d) 前のセクションで作成したコントラクトとそのタイプを選択します。

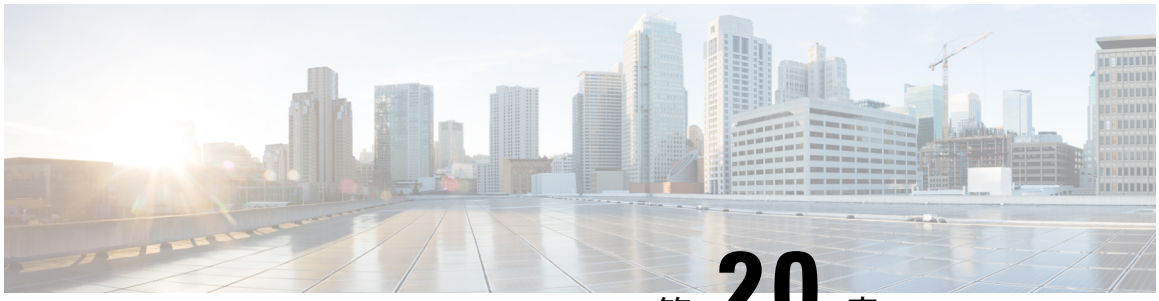
コンシューマまたはプロバイダを選択します。

ステップ4 他の外部EPGにコントラクトを割り当てます。

a) 外部EPGが配置されているスキーマとテンプレートを選択します。
b) 外部EPGが配置されているテンプレートを参照します。
c) 外部EPGを選択します。
d) 右側のサイドバーで、**[+コントラクト(+Contract)]**をクリックします。
e) 前のセクションで作成したコントラクトとそのタイプを選択します。

プロバイダまたはコンシューマを選択します。

ステップ5 適切なサイトにテンプレートを展開します。



第 20 章

PBR を使用したサイト間 L3Out

PBR を使用したサイト間 L3Out

Cisco Application Centric Infrastructure（ACI）ポリシーベース リダイレクト（PBR）は、ファイアウォールやロードバランサなどのサービス アプライアンス、および侵入防御システム（IPS）のトラフィック リダイレクションを可能にします。一般的な使用例としては、プールしてアプリケーション プロファイルに合わせて調整すること、また容易にスケーリングすることができ、サービス停止の問題が少ないサービス アプライアンスのプロビジョニングがあります。PBR により、コンシューマとプロバイダ エンドポイントの間のコントラクトに基づくサービス アプライアンスの挿入は簡素化されます。このことは、それらすべてが同じ仮想ルーティングおよびフォワーディング（VRF）インスタンスに存在する場合でも成り立ちます。

PBR の展開には、ルート リダイレクト ポリシーおよびクラスタのリダイレクト ポリシーの設定と、これらのポリシーを使用するサービス グラフ テンプレートの作成が含まれます。サービスグラフ テンプレートを展開した後、EPG 間のコントラクトにアタッチして、そのコントラクトに従うすべてのトラフィックが、作成した PBR ポリシーに基づいてサービス グラフ デバイスにリダイレクトされるようにすることができます。これにより、同じ2つのEPG間のどのタイプのトラフィックをL4-L7デバイスにリダイレクトし、どのタイプのトラフィックを直接許可するかを選択できます。

サービス グラフおよびPBRに固有の詳細情報については、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』を参照してください。

マルチサイト展開での PBR のサポート

Cisco Multi-Site は以前より、Cisco APIC リリース 3.2(1) 以降、PBR との EPG 間（East-West）および L3Out-to-EPG（North-South）コントラクトをサポートしています。ただし、サイト間の L3Out-to-EPG（`site1`の外部エンドポイントから `site2` のエンドポイントへのトラフィック）のケースは、両方のサイトにローカル L3Out がある場合にのみサポートされていました。サイト間L3Outの使用例は、サイト間 L3Out （231 ページ）の章で説明した例と設定に限定されていました。同様に、PBR とのサービスグラフ統合はありますが、サイト間L3Outはありません。詳細については、 *『Cisco Multi-Site and Service Node Integration White Paper』*を参照してください。

Cisco APIC リリース 4.2(5) 以降では、サイトを越えて PBRを使用する L3Out-to-EPG（サイト間 L3Out）の使用例が拡張され、アプリケーション EPG にローカル L3Out がない場合や、ローカル L3Out がダウンしている場合に対応できるようになりました。

サポートされる使用例

次の図は、アプリケーション EPG の ACI 内部エンドポイントと、サポートされているサイト間 L3Out with PBR 使用例の別のサイトの L3Out を経由する外部エンドポイント間のトラフィック フローを示しています。

これらの例を設定するワークフローは同じですが、オブジェクトを同じ VRF で作成するか、異なる VRF で作成するか（VRF 間と VRF 内）、およびオブジェクトを展開する場所（ストレッチか非ストレッチか）のみが異なります。

1. L4-L7 デバイスおよび PBR ポリシーの作成と設定 （260 ページ）の説明に従って、サイトの APIC で L4-L7 デバイスを直接作成します。

   Nexus Dashboard Orchestrator からデバイスと PBR ポリシーを作成することはできないため、これらのオプションを設定するには、各サイトの APIC に直接ログインする必要があります。

2. テンプレートの作成 （264 ページ）の説明に従って、必要なテンプレートを作成します。

   すべてのサイトに展開されたすべてのオブジェクトを含む単一の拡張テンプレートを作成することをお勧めします。次に、各サイト専用のオブジェクトを含む各サイトの追加テンプレート。

3. サービス グラフの設定 （265 ページ）の説明に従って、サービスグラフを作成して設定します。

4. コントラクトのフィルタの作成 （267 ページ）の説明に従って、アプリケーション EPG と別のサイトの L3Out を含む外部 EPG 間のすべてのトラフィックに使用するコントラクトとフィルタを作成します。

5. アプリケーション プロファイルと EPG の作成 （274 ページ）の説明に従って、VRF とブリッジドメインを使用してアプリケーション EPG を作成します。

アプリケーションEPGを拡張するかどうかに応じて、これらのオブジェクトを異なるテンプレートで作成します。同様に、アプリケーション EPG と L3Out に同じ VRF または異なる VRF を使用することもできます。

6. サイト間L3OutおよびVRFの作成またはインポート（276ページ）の説明に従って、L3Outを作成します。
7. サイト間 L3Out を使用するための外部 EPG の設定（237 ページ）の説明に従って、L3Outの外部 EPG を作成します。

Inter-VRF と Intra-VRF

アプリケーション EPG と外部 EPG を作成および設定する場合、アプリケーション EPG のブリッジドメインと L3Out に VRF を提供する必要があります。同じ VRF（intra-VRF）を使用するか、異なるVRF（inter-VRF）を使用するかを選択できます。

EPG 間のコントラクトを確立する場合は、1 つの EPG をプロバイダとして指定し、もう 1 つの EPG をコンシューマとして指定する必要があります。

- 両方の EPG が同じ VRF にある場合、どちらか一方がコンシューマまたはプロバイダになることができます。
- EPG が異なる VRF にある場合は、外部 EPG がプロバイダーであり、アプリケーション EPG がコンシューマである必要があります。

拡張された EPG

この使用例は、2 つのサイト間で拡張される単一のアプリケーション EPG と、1 つのサイトでのみ作成される単一の L3Out を示しています。アプリケーション EPG のエンドポイントが L3Out と同じサイトにあるか、他のサイトにあるかに関係なく、トラフィックは同じ L3Out を通過します。ただし、トラフィックは常にエンドポイントのサイトに対してローカルなサービス ノードを通過します。

（注） 外部 EPG が拡張され、各サイトに独自の L3Out があるが、トラフィックの発信元または宛先であるサイトの L3Out がダウンしている場合も、同じフローが適用されます。

図 *19 :* インバウンド トラフィック

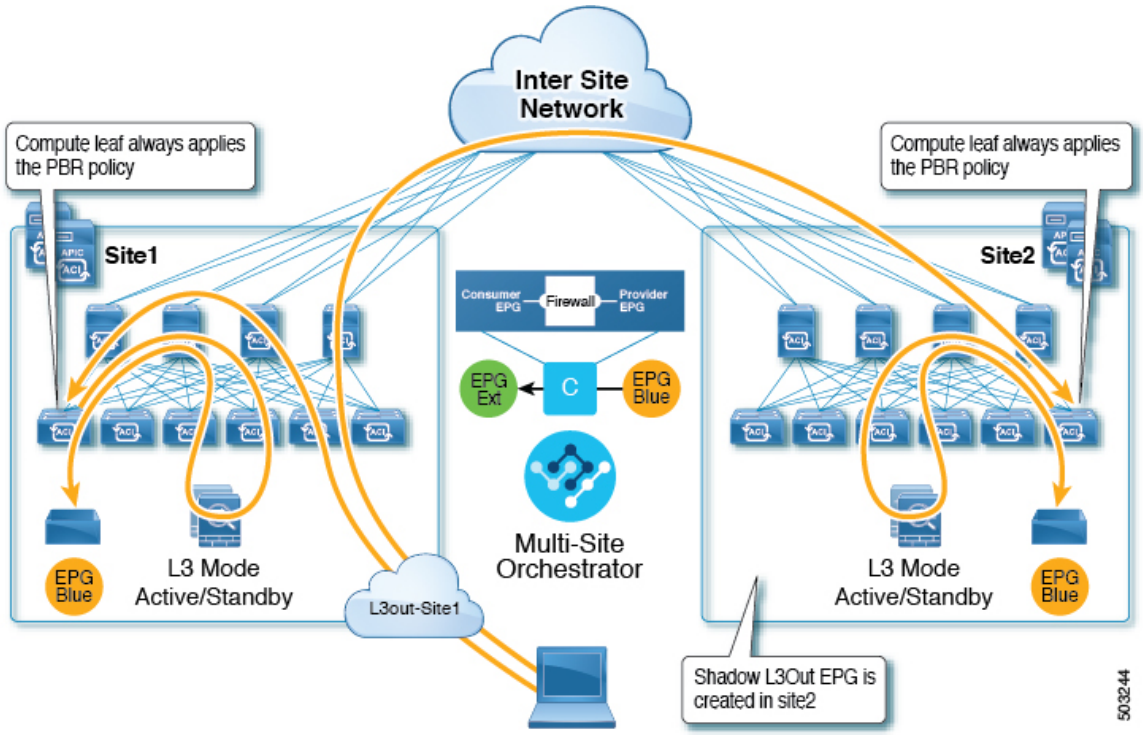
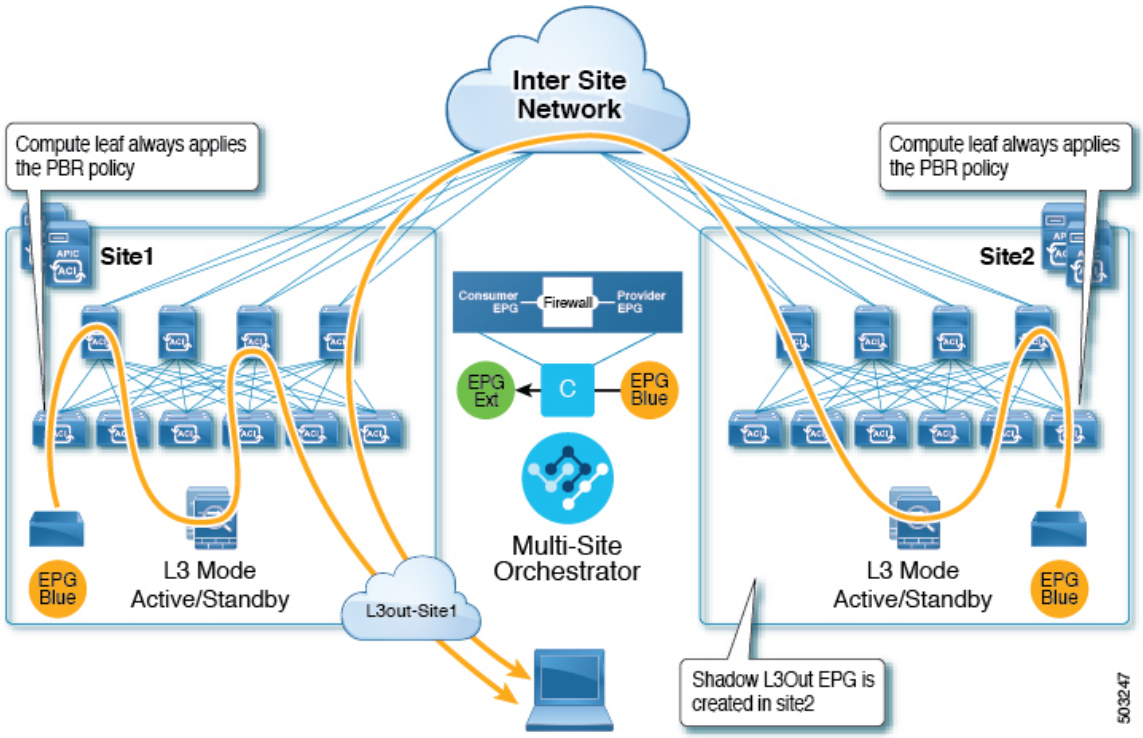


図 *20 :* アウトバウンド トラフィック



サイトローカル EPG

この使用例は、North-South トラフィックに他のサイトの L3Out を使用するサイトローカル アプリケーション EPG を示しています。前の例と同様に、すべてのトラフィックは EPG のサイトローカル サービス グラフ デバイスを使用します。

（注） 外部 EPG が拡張され、各サイトに独自の L3Out があり、EPG のローカル L3Out がダウンしている場合も、同じフローが適用されます。

図 *21* : インバウンド トラフィック

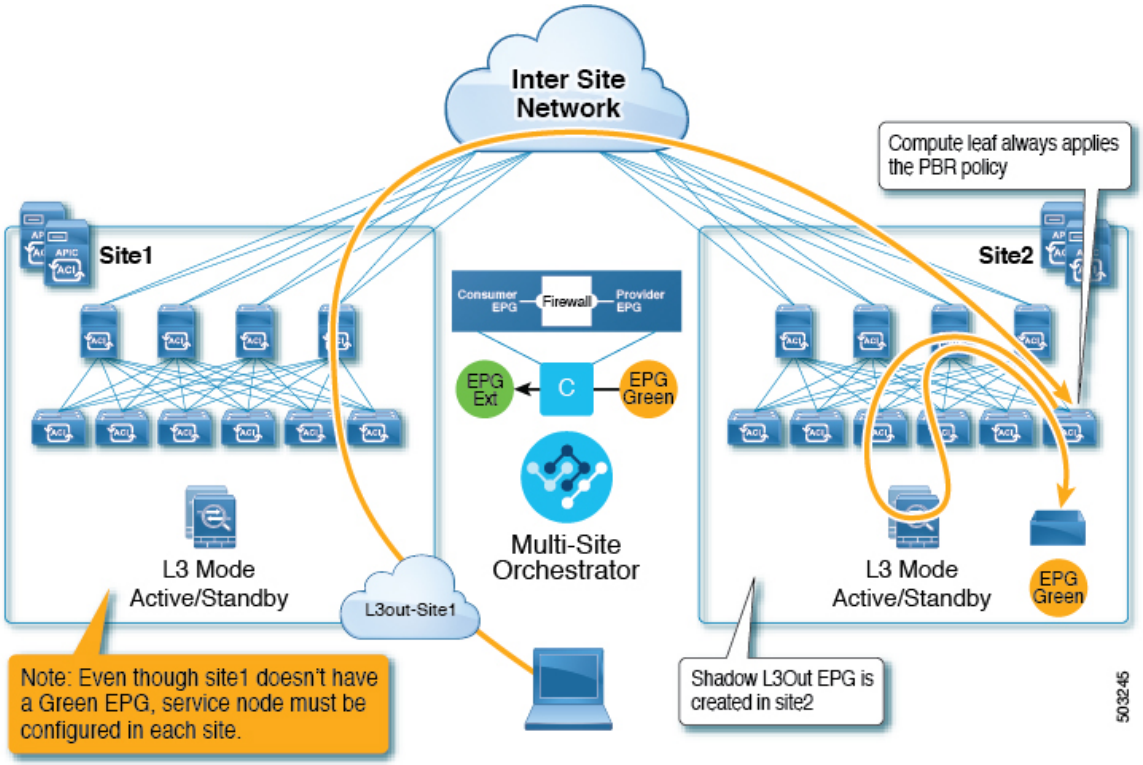
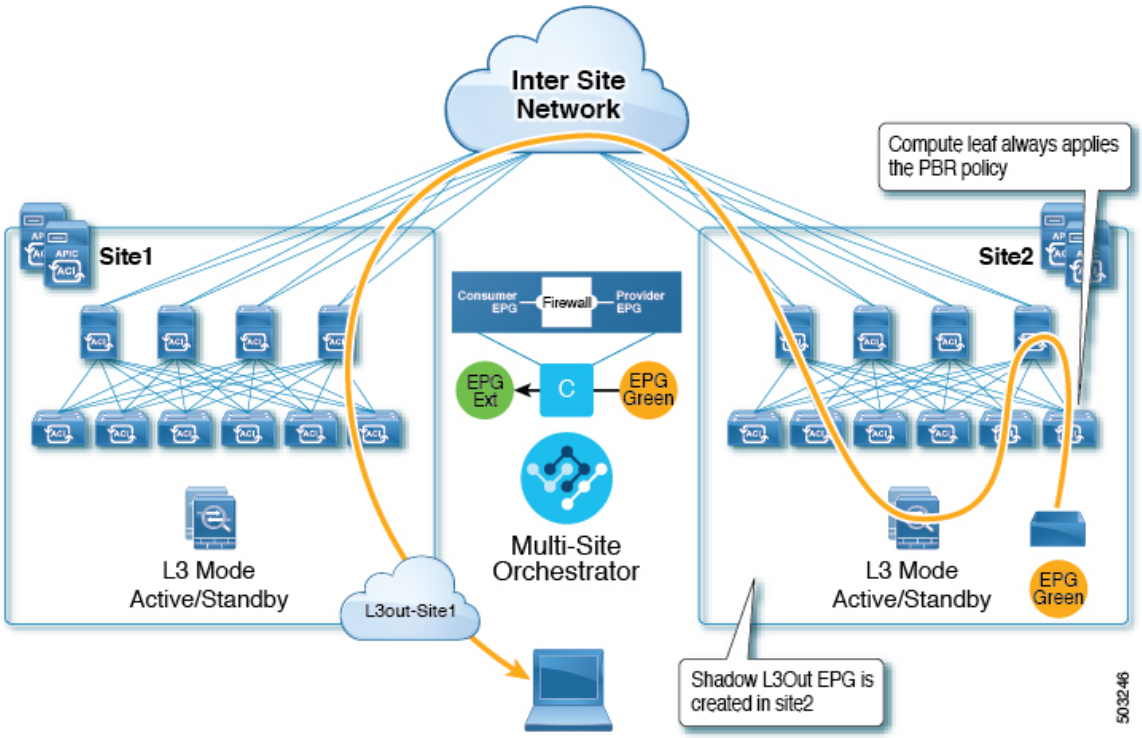


図 *22*: アウトバウンド トラフィック



注意事項と制約事項

サイト間 L3Out を設定する際には次の制約事項が適用されます。

- エンドポイント グループ（EPG）間で MultiSite ポリシーベース リダイレクト（PBR）を設定する場合、次の機能は特定の IP エンドポイントまたはホスト プレフィックス（IPv4 の場合は /32、IPv6 の場合は /128）ではサポートされません。
  - ブリッジ ドメインのスタティック ルート（NH 到達可能性）
  - Microsoft ネットワーク ロード バランシング
  - エニーキャストMAC
- PBR を使用しないサイト間 L3Out の使用例については、サイト間 L3Out （231 ページ）を参照してください。
- PBR を使用したサイト間 L3Out では、次の使用例がサポートされています。
  - アプリケーション EPG をコンシューマとする Inter-VRF サイト間 L3Out。

    VRF 間コントラクトの場合、L3Out がプロバイダである必要があります。
  - アプリケーション EPG がプロバイダまたはコンシューマのいずれかである VRF 内サイト間 L3Out

- PBR を使用したサイト間中継ルーティング（L3Out-to-L3Out）はサポートされていません。

- 上記の使用例は、Cisco APIC リリース 4.2(5) またはリリース 5.1(x) を実行しているサイトでサポートされています。Cisco APIC リリース 5.0(x) を実行しているサイトではサポートされません。
- サポートされるすべてのケースで、アプリケーション EPG をストレッチすることも、ストレッチしないこともできます。
- サービス グラフ デバイスは、サイト間 L3Out 外部 EPG と PBR コントラクトを持つアプリケーション EPG を持たないサイトを含め、各サイトで定義する必要があります。
- ワンアーム展開モデルとツーアーム展開モデルの両方がサポートされています。

  ワンアーム展開では、サービス グラフの内部インターフェイスと外部インターフェイスの両方が同じブリッジ ドメインに接続されます。ツーアーム展開では、サービス グラフ インターフェイスは個別の BD に接続されます。
- PBR を使用してロード バランサを設定する場合、ロード バランサと仮想 IP（VIP）の実サーバは同じサイトに存在する必要があります。PBR がディセーブルの場合、ロードバランサと実サーバは異なるサイトに存在できます。
- PBR を設定する場合、宛先は L1、L2、または L3 です。

APIC サイトの設定

外部 TEP プールの設定

サイト間 L3Out には、各ポッドの境界リーフ スイッチに外部 TEP アドレスが必要です。外部 TEP プールがすでに設定されている場合 (たとえば、リモート リーフなどの別の機能のために) は、同じプールを使用できます。既存の TEP プールは Nexus Dashboard Orchestrator に継承され、インフラストラクチャ設定の一部として GUI に表示されます。それ以外の場合は、この項で説明されているように、GUI で TEP プールを追加できます。

（注） すべてのポッドに一意の TEP プールを割り当てる必要があり、ファブリック内の他の TEP プールと重複しないようにする必要があります。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のサイドバーで、設定するサイトを選択します。

ステップ 5 メイン ウィンドウで、サイト内のポッドをクリックします。

ステップ 6 右側のサイドバーで、**[+ TEP プールを追加 (+Add TEP Pool)]** をクリックします。

ステップ 7 **[TEP プールの追加 (Add TEP pool)]** ウィンドウで、そのサイトに対して設定する外部 TEP プールを指定します。

（注）
追加しようとしている TEP プールが他の TEP プールまたはファブリックアドレスと重複していないことを確認する必要があります。

ステップ 8 このプロセスを、サイト間の L3Outs を使用する予定のサイトおよびポッドごとに繰り返します。

L4-L7 デバイスおよび PBR ポリシーの作成と設定

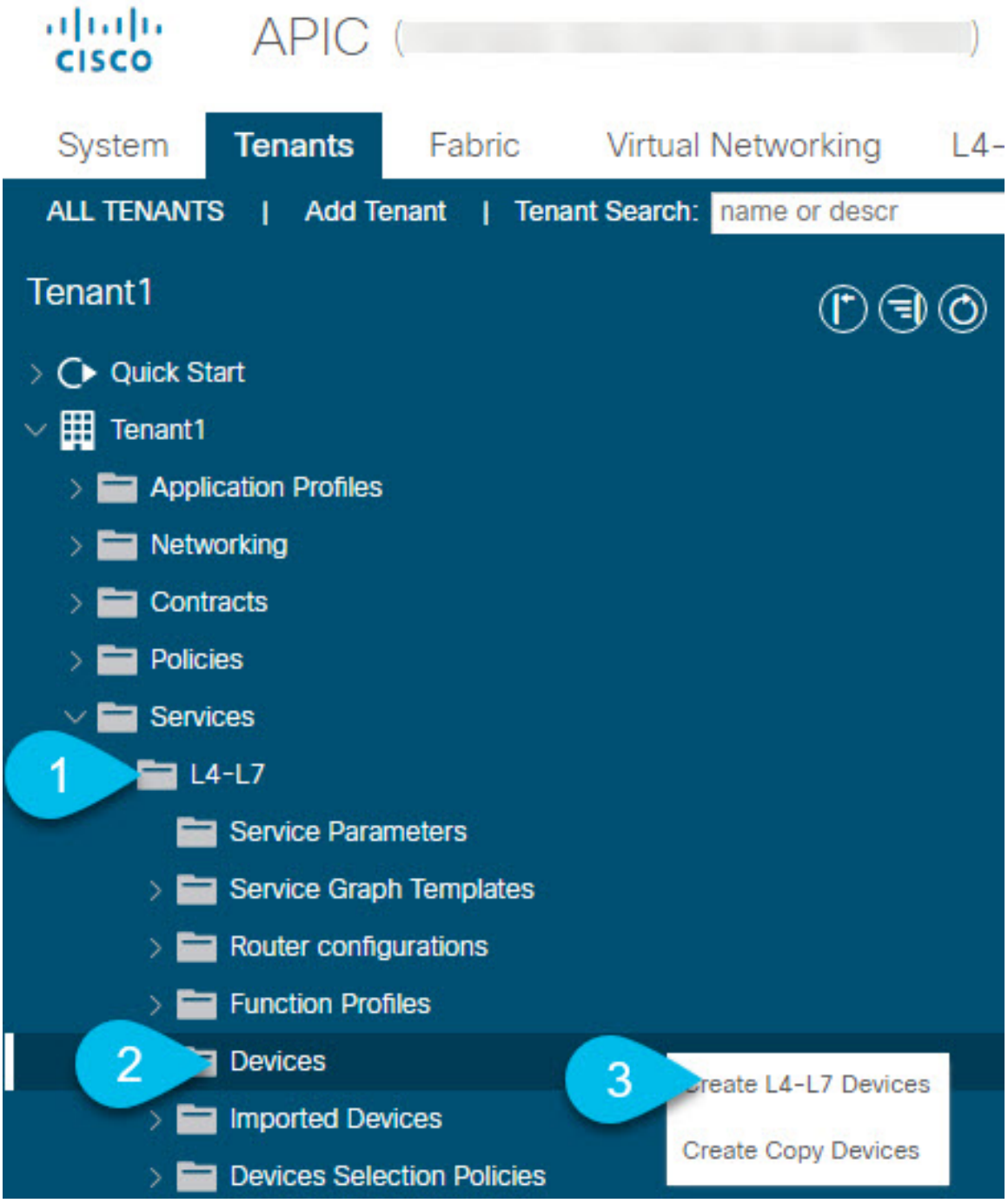
サービス グラフ デバイスを作成し、各サイトの APIC で PBR ポリシーを直接定義する必要があります。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 上部のメニューバーで **[テナント (Tenants)]** をクリックし、デバイスを作成するテナントを選択します。

ステップ 3 L4-L7 デバイスを作成します。

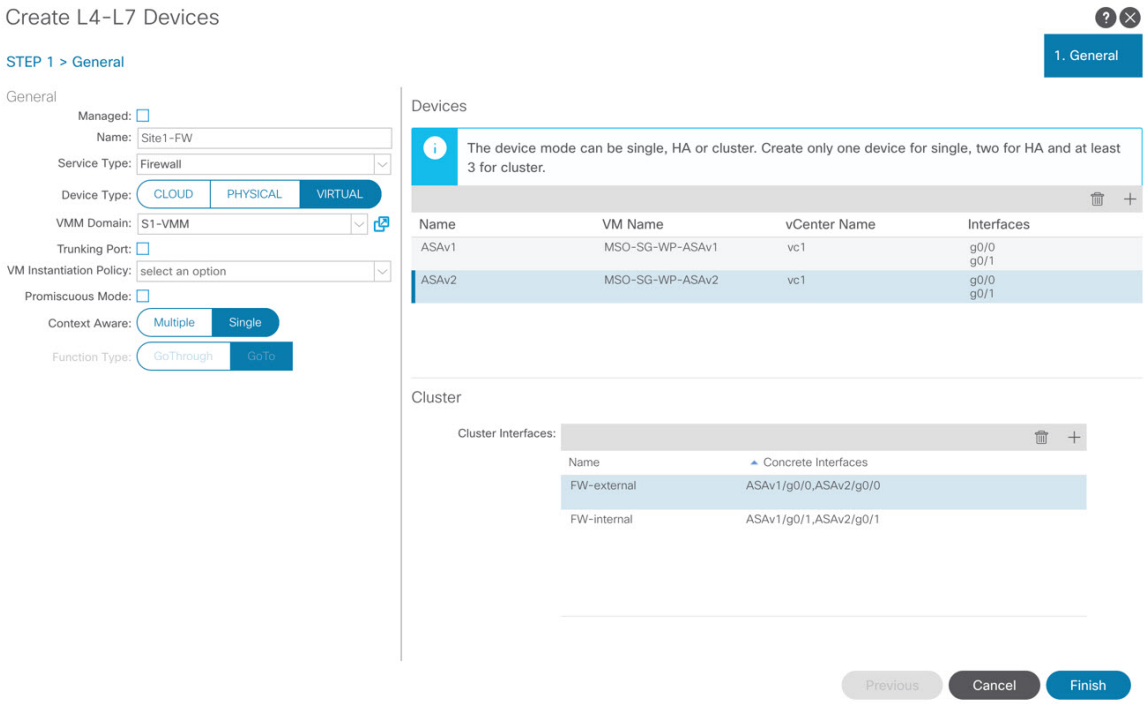


a) 左側のサイドバーで、**<tenant-name>** > **[サービス (Services)]** > **[L4-L7]** カテゴリを展開します。
b) **[デバイス (Devices)]** カテゴリを右クリックします。
c) **[L4-L7 デバイスの作成 (Create L4-L7 Devices)]** を選択します。

[L4-L7 デバイスの作成 (Create L4-L7 Devices)] の設定ダイアログが開きます。

ステップ 4 L4-L7 デバイスを設定します。

次の図は、デバイスの設定サンプルを示しています。構成設定は、デバイスのタイプと目的によって異なります。



ステップ 5 PBR ポリシーを作成します。

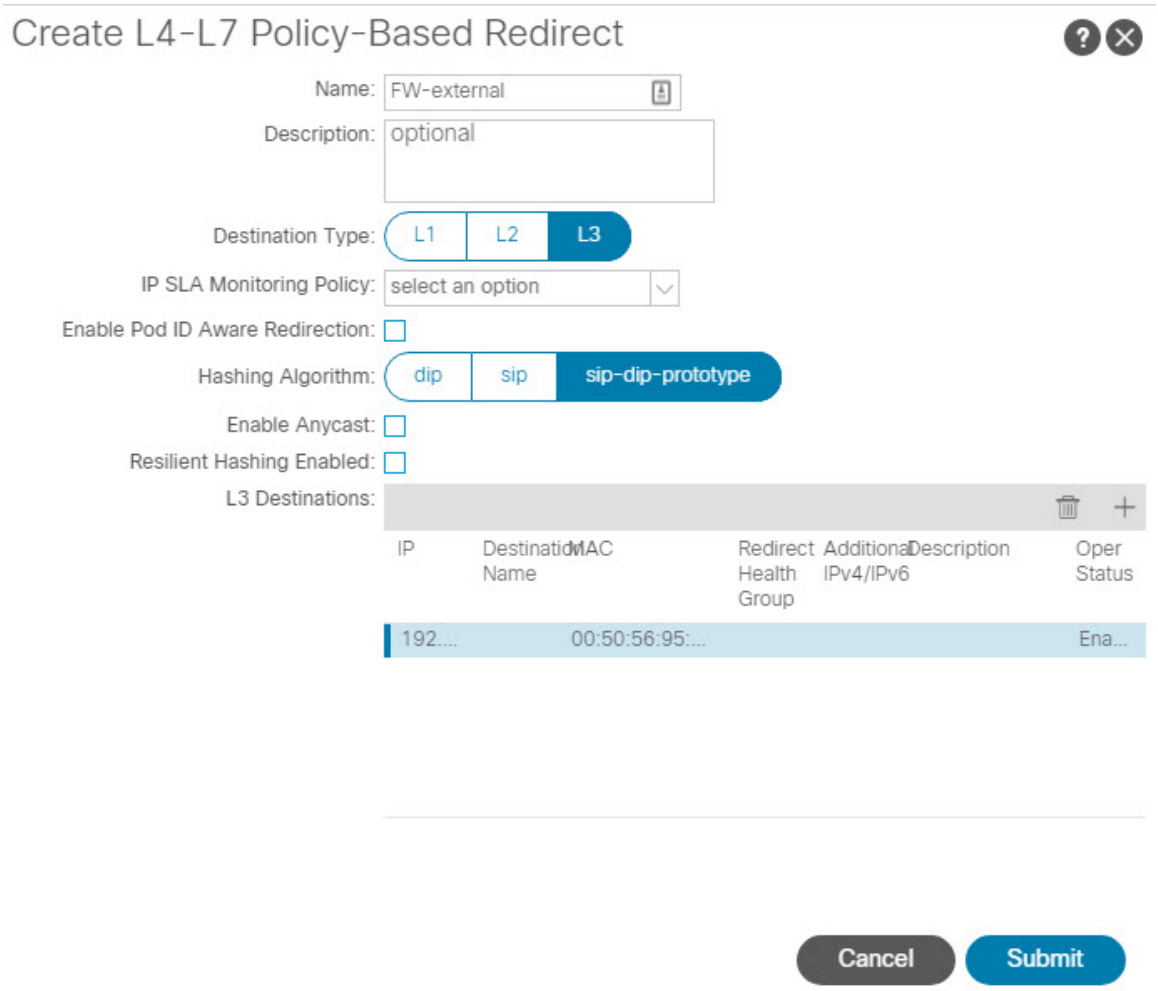
a) 左側のサイドバーで、**<tenant-name>** > **[ポリシー(Policies)]** > **[プロトコル (Protocol)]** カテゴリを展開します。
b) **[L4-L7 ポリシーベース リダイレクト (L4-L7 Policy-Based Redirect)]** カテゴリを右クリックします。
c) **[L4-L7 ポリシーベース リダイレクトの作成 (Create L4-L7 Policy-Based Redirect)]** を選択します。

[L4-L7 ポリシーベース リダイレクトの作成 (Create L4-L7 Policy-Based Redirect)] の設定ダイアログが開きます。

ステップ 6 PBR ポリシーを設定します。

次の図は、宛先 IP と MAC が追加されたサンプル PBR ポリシー設定を示しています。

構成設定は、作成するデバイスとポリシーのタイプと目的によって異なります。たとえば、PBR ポリシーでは、IP-SLA、ハッシュ アルゴリズム、レジリエント ハッシュなどの追加オプションを設定できます。



ステップ 7 他のサイトで必要なデバイスと PBR ポリシーを作成するには、前の手順を繰り返します。

テンプレートの作成

スキーマとテンプレートを作成する場合は、次の方法でテンプレートを分離することをお勧めします。

- すべてのサイト間で拡張されるすべてのオブジェクトを含む、単一の共有テンプレート。
- そのサイトにのみ展開するオブジェクトを含む、サイトごとに 1 つのテンプレート。

この例では、2 つのサイトを使用するため、合計 3 つのテンプレートを作成します。各サイトに 1 つと、ストレッチされた 1 つです。

始める前に

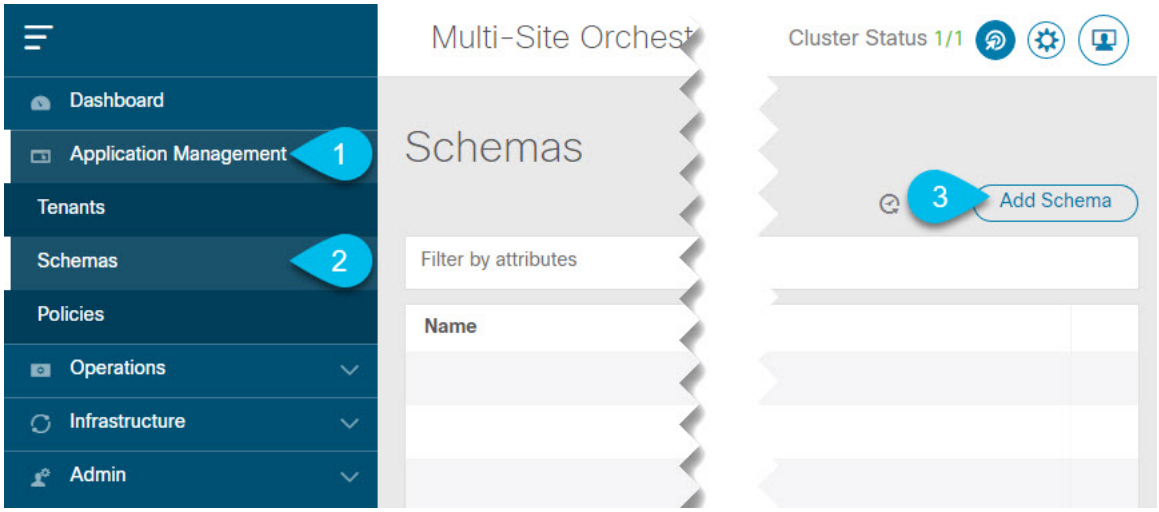
次のものが必要です。

- 注意事項と制約事項 （258 ページ）を確認し、そこにリストされているすべての前提条件を完了していること。
- 外部 TEP プールの設定 （234 ページ）およびL4-L7 デバイスおよびPBR ポリシーの作成と設定 （260 ページ）の説明に従って、個々の APIC サイトの設定を完了していること。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 スキーマを新規作成します。



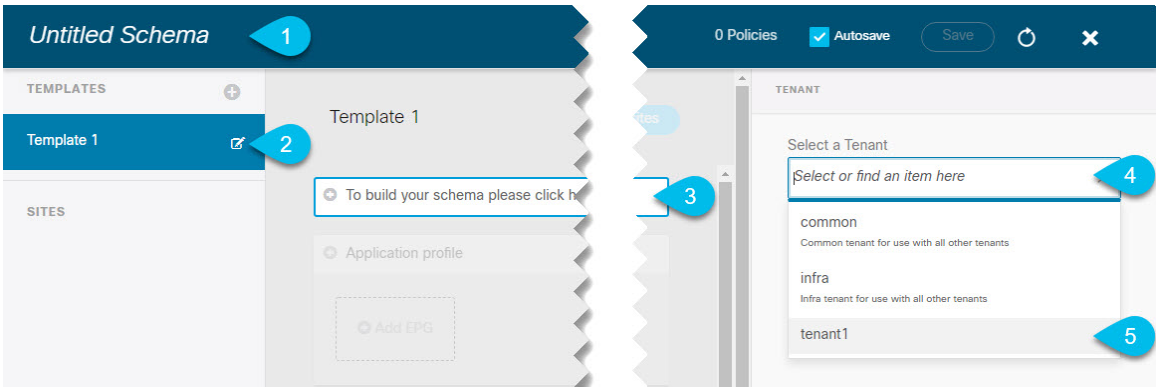
a) 左側のナビゲーションサイドバーで、**[アプリケーション管理 (Application Management)]** カテゴリを展開します。

b) **[スキーマ (Schemas)]** を選択します。

c) **[スキーマの追加 (Add Schema)]** をクリックして、新しいスキーマを作成します。

[スキーマの編集 (Edit Schema)] ウィンドウが開きます。

ステップ 3 スキーマに名前を付け、テナントを選択します。



a) **[名称未設定のスキーマ (Untitled Schema)]** をスキーマの名前に置き換えます。

`[名称未設定のスキーマ (Untitled Schema)]` の名前をクリックして編集します。

b) テンプレートの名前を変更します。

左側のサイドバーで、テンプレートの上にマウスを移動し、**[編集 (Edit)]** アイコンをクリックします。

たとえば、`template-stretched`です。

c) メイン ペインで、**[スキーマを作成するエリアをクリックしてテナントを選択してください (To build your schema please click here to select a tenant)]** をクリックします。

d) 右側のサイドバーで、**[テナントの選択 (Select a Tenant)]** ドロップダウンをクリックします。

e) テナントを選択します。

ステップ 4 追加のテンプレートを作成します。

左側のサイドバーで、プラス（+）アイコン（**[テンプレート (Templates)]** の横にあるもの）をクリックして、サイト固有のテンプレートを追加します。次に、前述の手順と同じ手順に従ってテンプレートに名前を付け、テナントを選択します。

たとえば、`template-site1` と `template-site2` です。

サービス グラフの設定

次のものが必要です。

- L4-L7デバイスおよびPBRポリシーの作成と設定 （260ページ）の説明に従い、サイトのAPICごとに直接作成されたL4-L7デバイス。
- テンプレートの作成 （264ページ）の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。

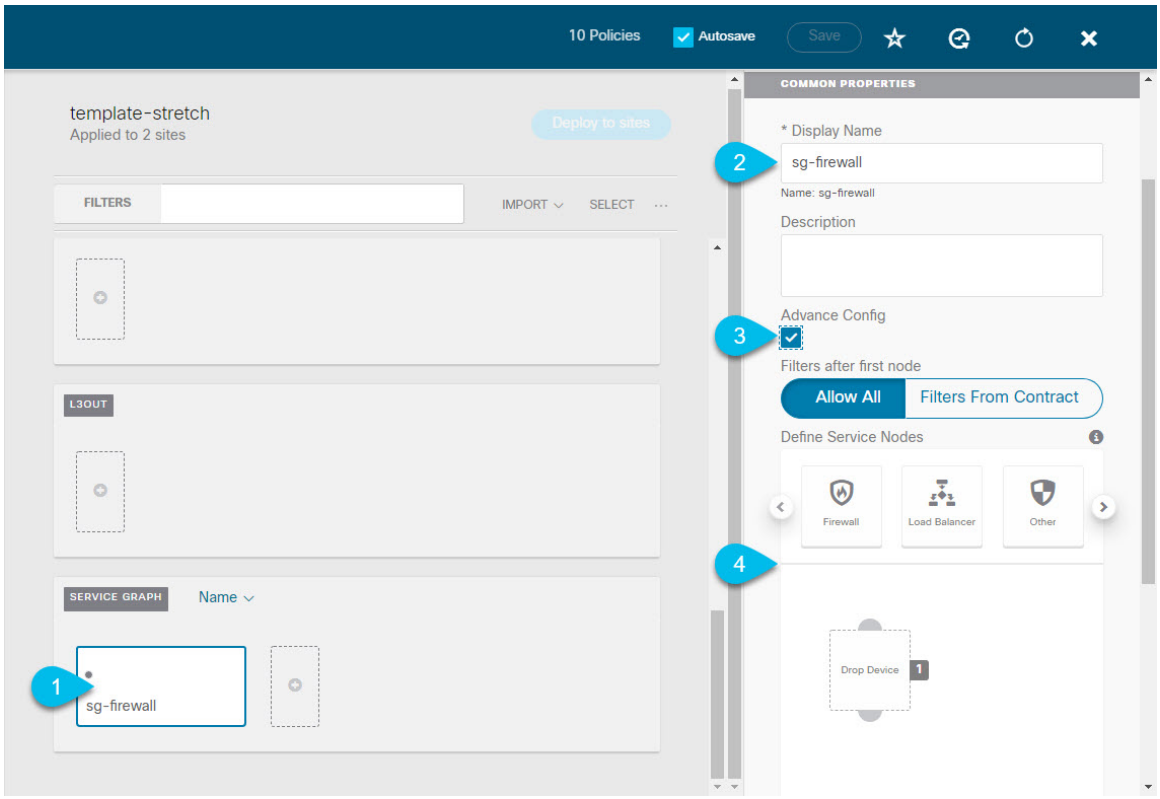
ここでは、サービスグラフの1つ以上のデバイスを設定する方法について説明します。

手順

ステップ 1 サービス グラフを作成するテンプレートを選択します。

`template-stretch`で単一のサービス グラフを作成しますが、この手順の後半で説明するように、サイトローカルデバイスを設定します。

ステップ 2 サービス グラフを作成します。



a) メインペインで、**[サービス グラフ (Service Graph)]** 領域までスクロールダウンして、**[+]** アイコンをクリックして新しいコントラクトを作成します。

b) サービス グラフの **[表示名 (Display Name)]** を入力します。

c) （オプション）**[詳細設定 (Advanced Config)]** オプションをオンにします。

このオプションでは、最初のサービス グラフ ノードの後にトラフィックを制限するかどうかを設定できます。このオプションを有効にしない場合、デフォルトでは、最初のサービス グラフ ノード以降のすべてのトラフィックが許可されます。

[詳細設定 (Advanced Config)] を有効にする場合は、次の 2 つのオプションのいずれかを選択します。

- **[すべて許可 (Allow All)]**：契約サブジェクトの特定のフィルタの代わりにデフォルト（permit-all）フィルタを使用します。

これは、**[詳細設定 (Advanced Config)]** を無効にした場合と同じ動作です。

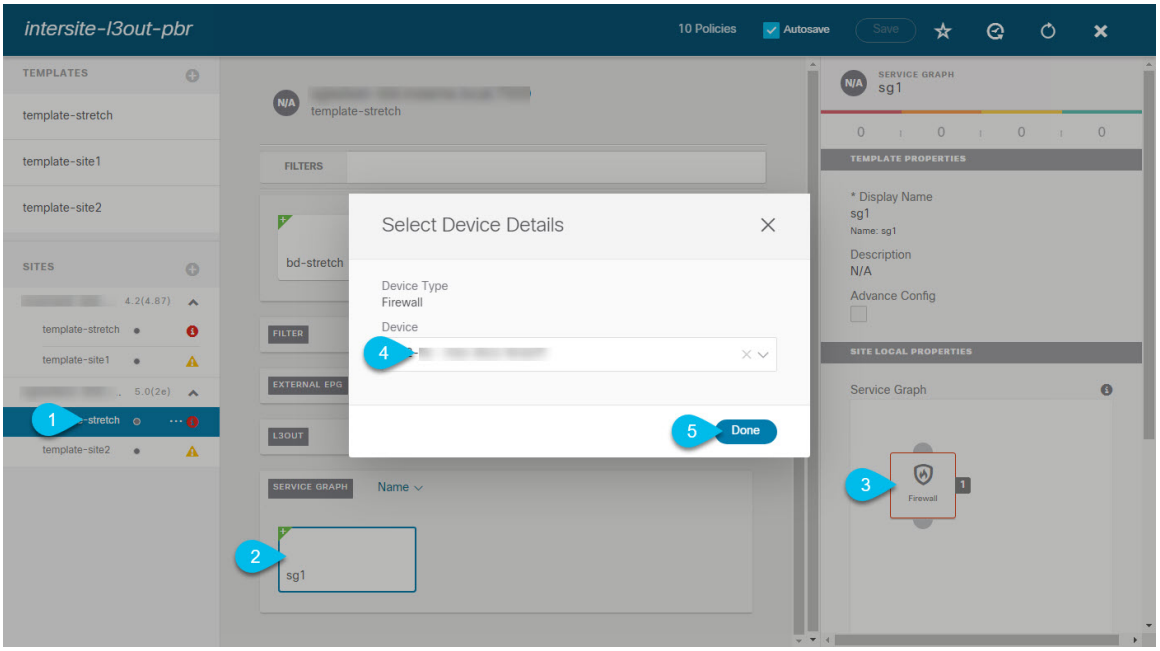
- **[契約からのフィルタ (Filters From Contract)]**：コントラクトの件名から特定のフィルタを使用します。

d) 右側のサイドバーで、**[サービスノードの定義 (Define Service)]**領域までスクロールし、1 つ以上のノードを **[デバイスのドロップ (Drop Device)]** ボックスにドラッグアンドドロップします。

Multi-Siteは、サービス グラフごとに最大 2 つのノードをサポートします。

ステップ 3 サービス グラフのサイトローカル デバイスを設定します。

この手順は、Multi-Site ドメインの一部であるすべてのサイトに対して実行する必要があります。



a) 左側のサイドバーから、このサービス グラフを展開するサイトの 1 つを選択します。

b) メイン ペインで、作成したサービス グラフを選択します。

c) 右側のサイドバーで、サービス グラフ ノードをクリックします。

d) **[デバイスの詳細の選択 (Select Device Details)]** ウィンドウで、サイトの APIC で作成したデバイスを選択します。

コントラクトのフィルタの作成

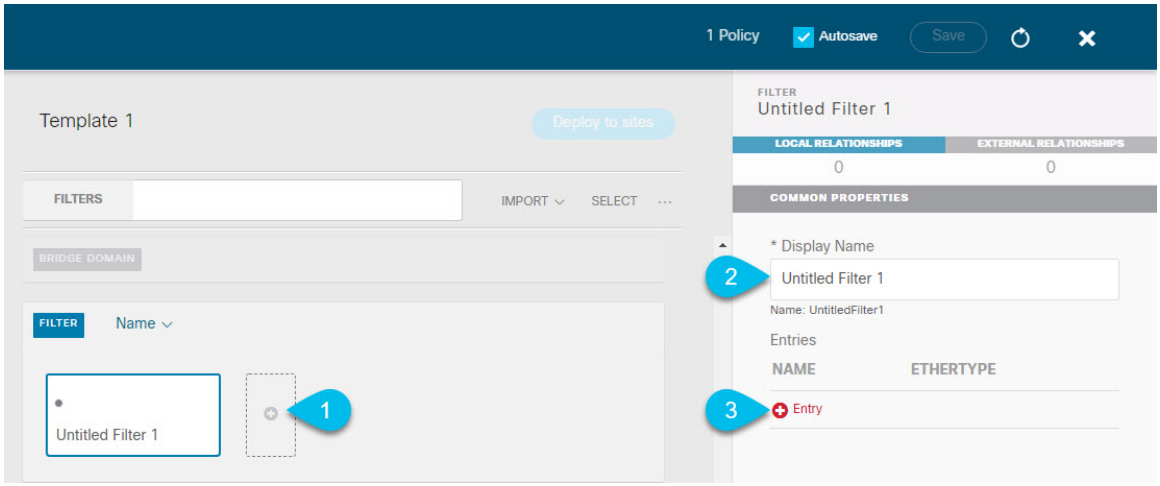
次のものが必要です。

- テンプレートの作成 （264 ページ）の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。

このセクションでは、サービスグラフを介してアプリケーションEPGとL3Out間のトラフィックに使用されるコントラクトとフィルタの作成方法について説明します。

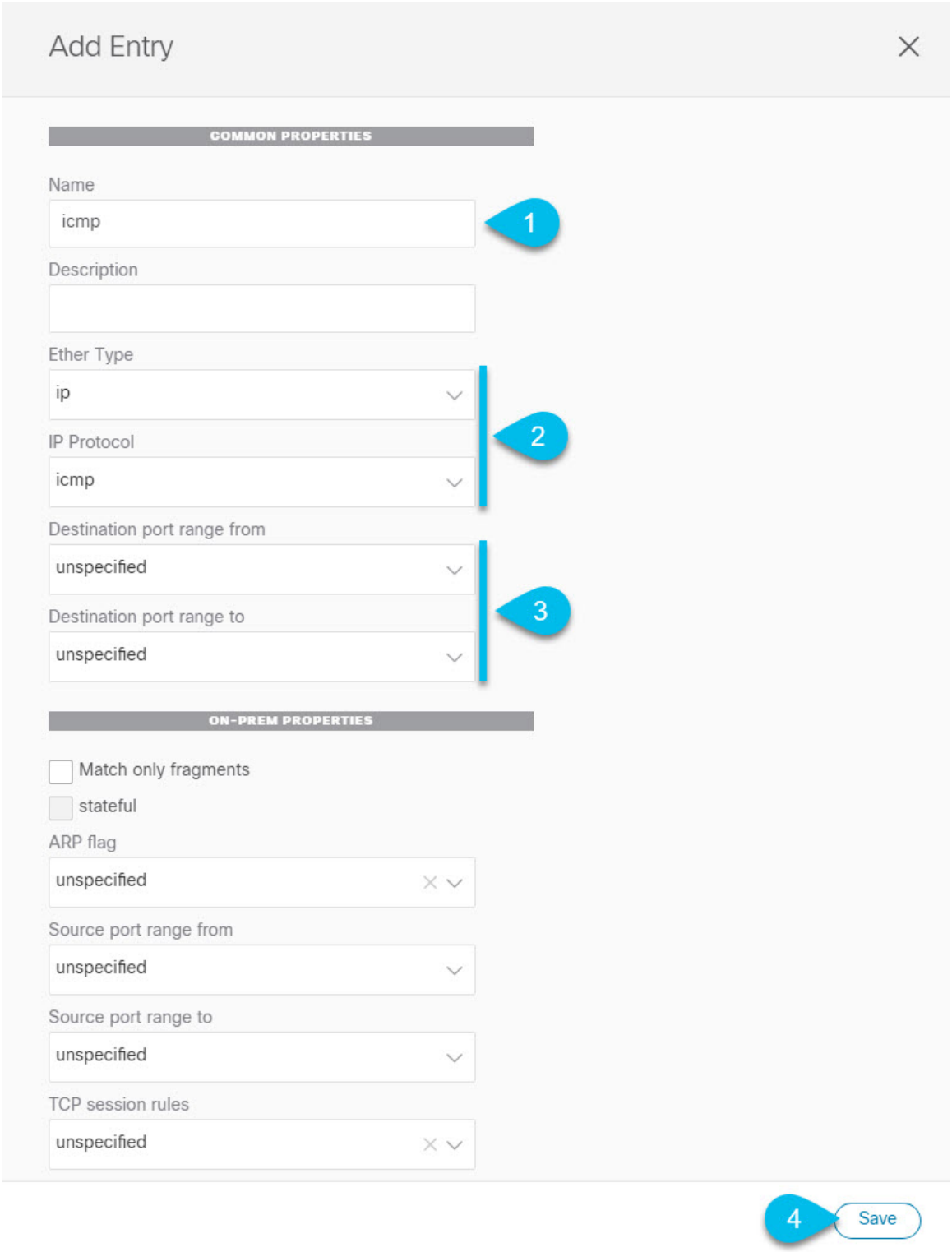
手順

ステップ1 フィルタを作成します。



a) **[Filter (フィルタ)]** エリアまでスクロールし、**[+]** をクリックしてフィルタを作成します。
b) 右側のペインで、フィルタの **[表示名 (Display Name)]** を入力します。
c) 右側のペインで、**[+ エントリ (+ Entry)]** をクリックします。

ステップ2 フィルタの詳細を入力します。



a) フィルタの **[名前 (Name)]** を指定します。

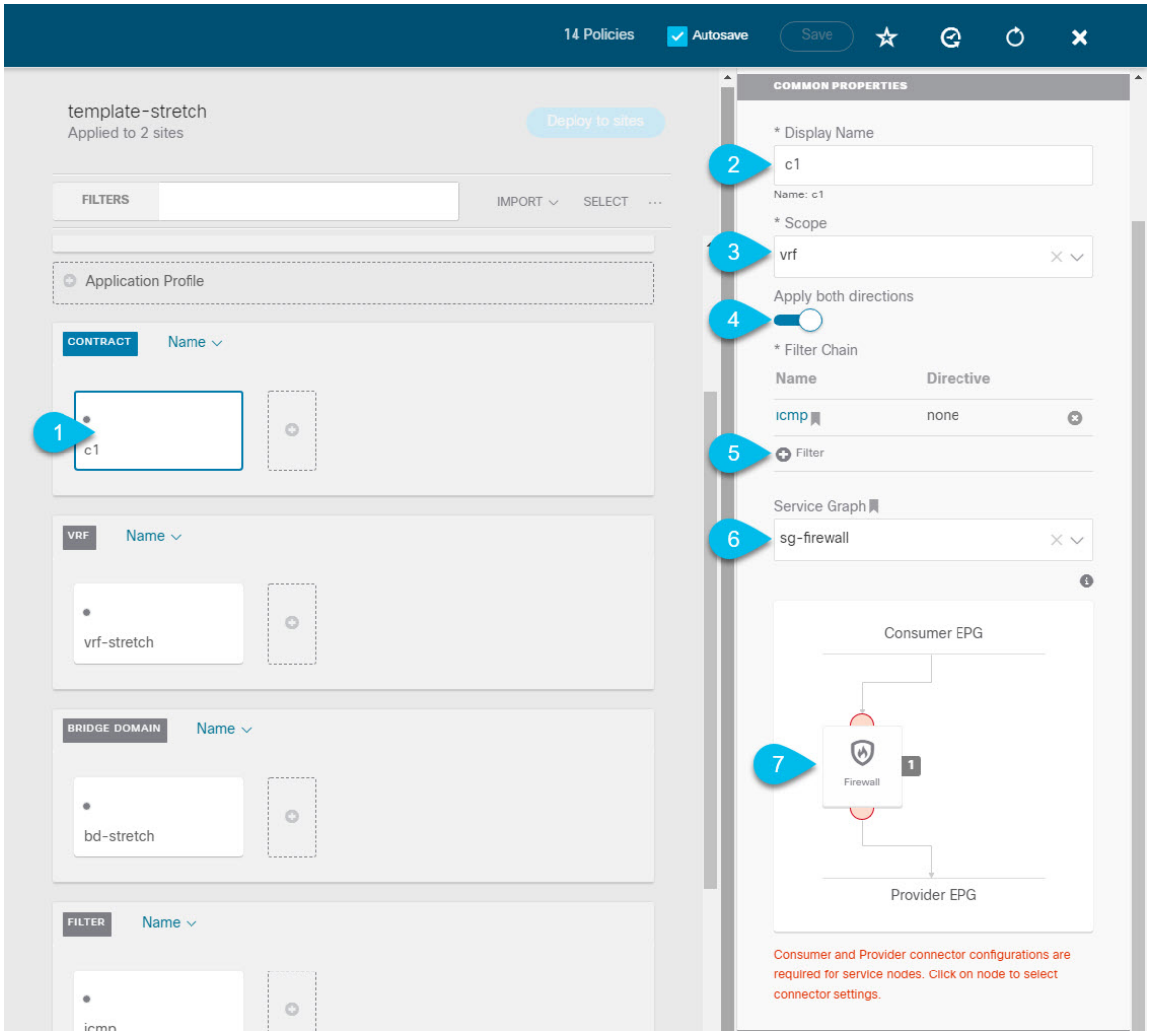
b) **[イーサー タイプ (Ether Type)]** と **[IP プロトコル (IP Protocol)]** を選択します。

たとえば、[ip] と [icmp] です。

c) 他のプロパティは [未指定 (unspecified)] のままにします。

d) **[保存 (Save)]** をクリックしてフィルタを保存します。

ステップ 3 コントラクトの作成



a) 中央ペインで、**[コントラクト (Contracts)]** エリアまで下方にスクロールし、**[+]** をクリックして、コントラクトを作成します。

b) 右側のペインで、コントラクトの **[表示名 (Display Name)]** を入力します。

c) **[範囲 (Scope)]** ドロップダウン メニューから、コントラクトの範囲を選択します。

アプリケーション EPG と L3Out が同じ VRF にある場合は、[vrf] を選択します。それ以外の場合は、[inter-VRF] 使用例を設定します。

d) **[両方向に適用 (Apply both directions)]** が有効になっていることを確認します。

これにより、コンシューマからプロバイダへの方向とプロバイダからコンシューマへの方向の両方に同じフィルタを適用できます。

e) 右側のペインで、**[フィルタ チェーン (Filter Chain)]** 領域までスクロールし、**[+ フィルタ (+ Filter)]** をクリックしてフィルタをコントラクトに追加します。

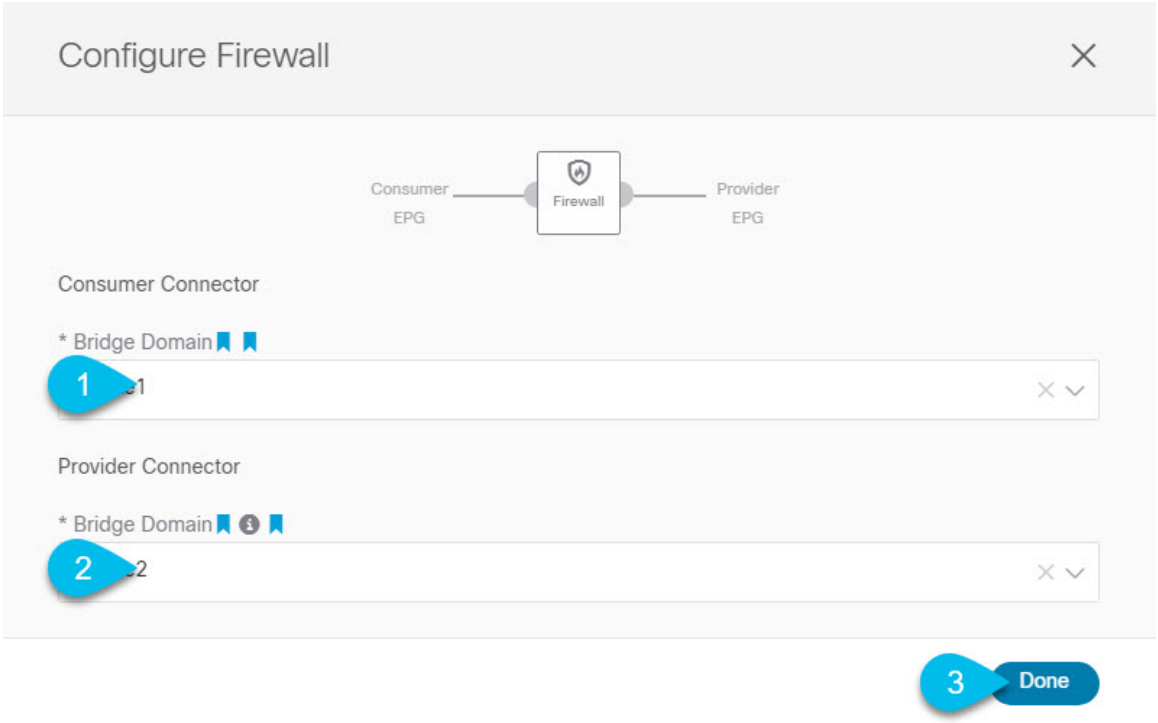
表示される **[フィルタ チェーンの追加 (Add Filter Chain)]** ウィンドウで、**[名前 (Name)]** ドロップダウン メニューから前のセクションで追加したフィルタを選択します。

コントラクトで `[両方向に適用 (Apply both directions)]` オプションを無効にした場合は、他のフィルタ チェーンに対してこの手順を繰り返します。

f) **[サービス グラフ (Service Graph)]** ドロップダウンから、前のセクションで作成したサービスグラフを選択します。

g) サービス グラフ ノードをクリックしてコネクタを設定します。

ステップ 4 サービス グラフ ノードのコネクタのブリッジ ドメインを選択します。

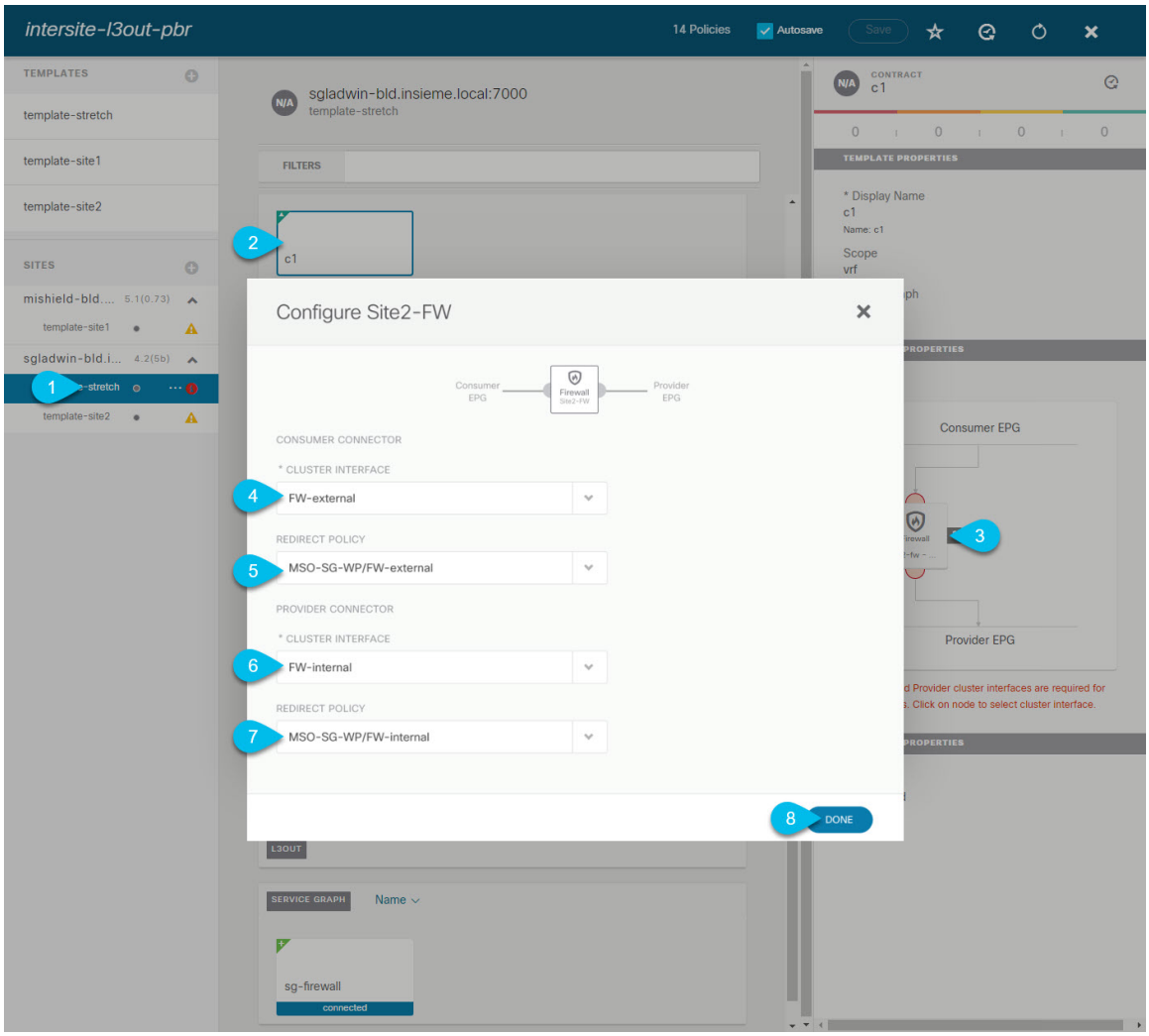


a) **[コンシューマ コネクタ (Consumer Connector)]** ブリッジ ドメインを指定します。

b) **[プロバイダ コネクタ (Provider Connector)]** ブリッジ ドメインを指定します。

c) **[完了（Done）]** をクリックして保存します。

ステップ 5 コントラクトのサイトローカル プロパティを設定します。



a) 左側のサイドバーで、割り当て先のサイトの下にあるテンプレートを選択します。
b) メイン ペインで、コントラクトを選択します。
c) 右側のサイドバーで、サービス グラフ ノードをクリックします。
d) **[クラスタ インターフェイス (Cluster Interface)]** を **[コンシューマ コネクタ (Consumer Connector)]** として選択します。
e) **[リダイレクト ポリシー (Redirect Policy)]** を **[コンシューマ コネクタ (Consumer Connector)]** として選択します。
f) **[クラスタ インターフェイス (Cluster Interface)]** を **[プロバイダ コネクタ (Consumer Connector)]** として選択します。
g) **[リダイレクト ポリシー (Redirect Policy)]** を **[プロバイダ コネクタ (Consumer Connector)]** として選択します。
h) **[完了 (Done)]**をクリックして、変更内容を保存します。
i) すべてのサイトに対してこの手順を繰り返します。

アプリケーション EPG の作成

アプリケーション EPG の VRF およびブリッジ ドメインの作成

ここでは、アプリケーション EPG の VRF およびブリッジ ドメイン (BD) を作成する方法について説明します。

始める前に

次のものが必要です。

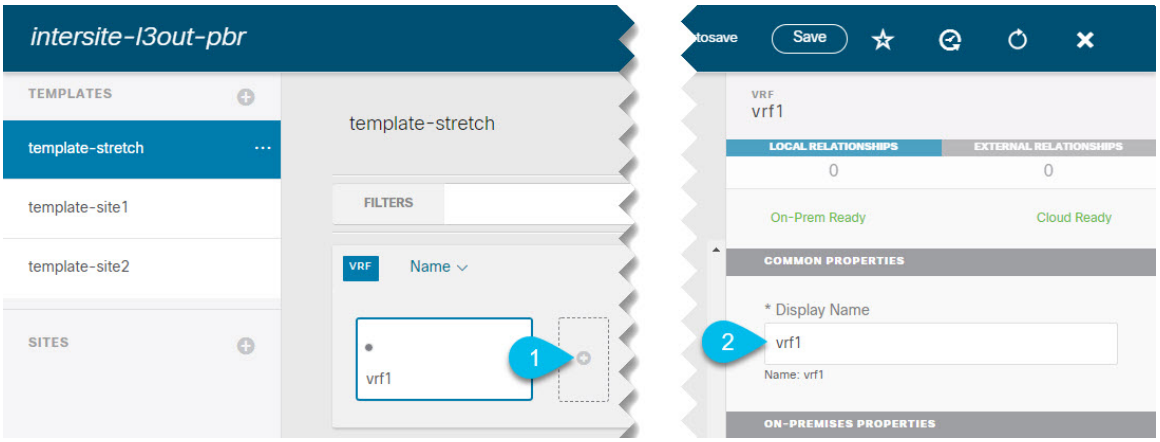
- テンプレートの作成 （264 ページ）の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。

手順

ステップ 1 VRF および BD を作成するテンプレートを選択します。

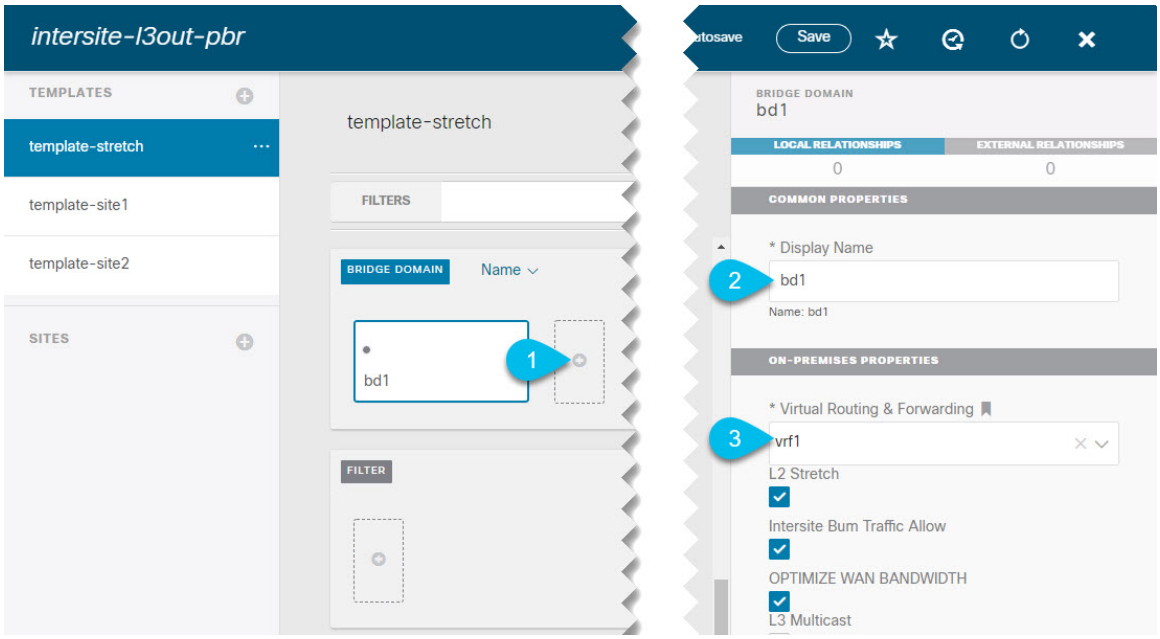
VRF および BD を拡張する場合は、`template-stretch` テンプレートを選択します。それ以外の場合は、サイト固有のテンプレートのいずれかを選択します。

ステップ 2 VRF を作成します。



a) メイン ペインの **[VRF]** 領域で、プラス (+) 記号をクリックして VRF を追加します。
b) 右側のサイドバーで、フィルタの **[表示名 (Display Name)]** を入力します。
c) 展開に対して適切である他の VRF 設定を指定します。

ステップ 3 BD を作成します。



a) メイン ペインの **[BD]** 領域で、プラス (+) 記号をクリックしてBDを追加します。
b) 右側のサイドバーで、フィルタの **[表示名 (Display Name)]** を入力します。
c) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、前のステップで作成された VRF を選択します。
d) 展開に対して適切である他の BD 設定を指定します。

アプリケーション プロファイルと EPG の作成

このセクションでは、サービスグラフでサイト間 L3Out を使用するために後で設定するアプリケーション EPG を作成する方法について説明します。

始める前に

次のものが必要です。

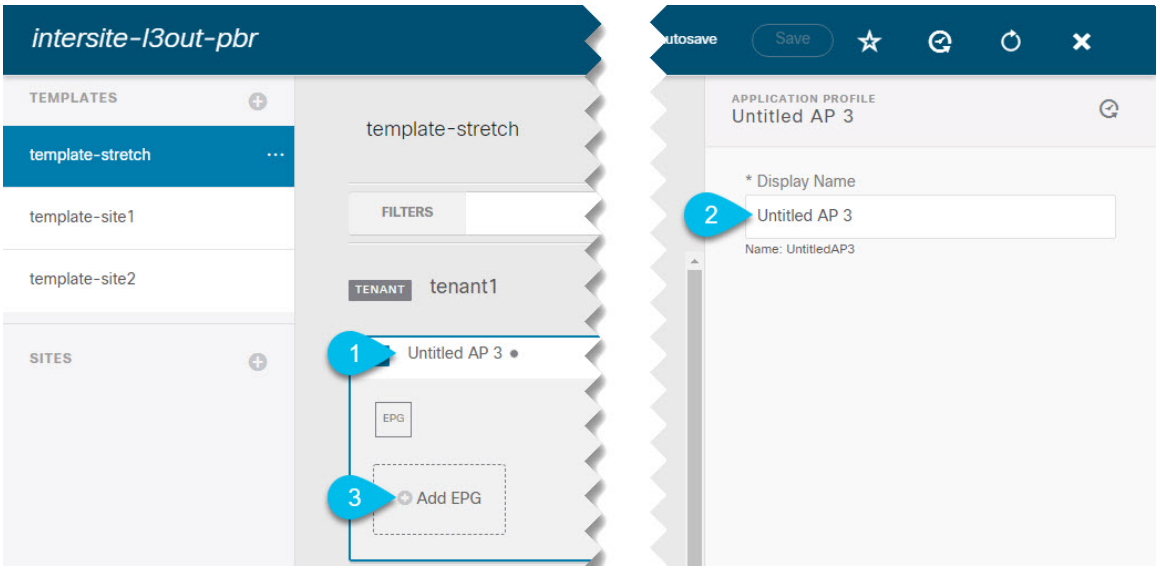
- テンプレートの作成 （264 ページ）の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。
- コントラクトのフィルタの作成 （267 ページ）の説明に従って、アプリケーション EPG と外部 EPG の間での通信のために使用するコントラクトを作成していること。
- アプリケーション EPG の VRF およびブリッジ ドメインの作成 （273 ページ）の説明に従って、EPG に使用する VRF と BD を作成していること

手順

ステップ 1 オブジェクトを作成するテンプレートを選択します。

アプリケーション EPG を拡張する場合は、拡張テンプレートで作成します。アプリケーション EPG をサイトローカルにする場合は、サイト固有のテンプレートで作成します。

ステップ 2 アプリケーション プロファイルと EPG を作成します。

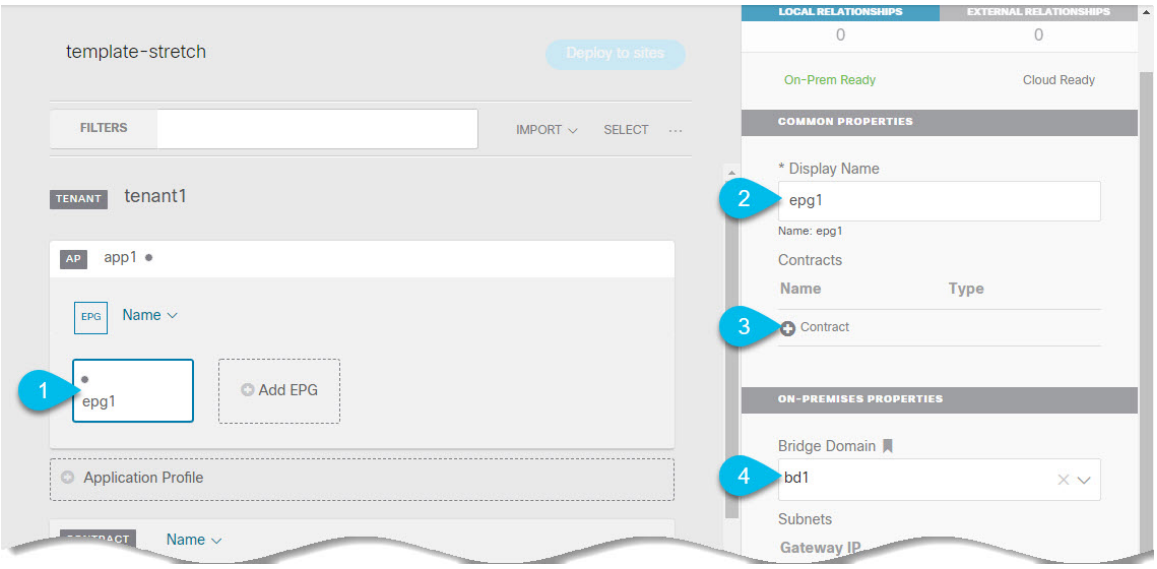


a) メイン ペインで、**[+ アプリケーション プロファイル (+ Application profile)]** をクリックします。

b) 右側のサイドバーで、プロファイルの **[表示名 (Display Name)]** を入力します。

c) メイン ペインで、**[+ EPGの追加 (+Add EPG)]** をクリックします。

ステップ 3 EPG を設定します。



a) メインペインで、アプリケーション EPG を選択します。
b) 右側のサイドバーで、EPG の **[表示名 (Display Name)]** を入力します。
c) **[+コントラクト (+Contract)]** をクリックし、コントラクトを選択します。

EPG 通信用に作成したコントラクトを選択し、そのタイプを設定します。

アプリケーション EPG と L3Out 外部 EPG に同じ VRF を使用している場合は、どちらかをコンシューマまたはプロバイダーとして選択できます。ただし、それらが異なるVRFにある場合は、アプリケーション EPG のコントラクトタイプにコンシューマを選択する必要があります。

d) **[ブリッジ ドメイン (Bridge Domain)]** ドロップダウンで、BD を選択します。
e) 展開に適した他の EPG 設定を指定します。

L3Out 外部 EPGの作成

サイト間 L3Out および VRF の作成またはインポート

ここでは、L3Out を作成し、それを Nexus Dashboard Orchestrator（NDO）GUI で VRF に関連付ける方法について説明します。これは APIC サイトにプッシュされるか、または APIC サイトの 1 つから既存の L3Out をインポートします。次に、この L3Out を外部 EPG に関連付け、その外部 EPG を使用して特定のサイト間 L3Out の使用例を設定します。

（注） L3Out に割り当てる VRF は、任意のテンプレートまたはスキーマにすることができますが、L3Out と同じテナントに存在する必要があります。

始める前に

次のものが必要です。

- テンプレートの作成 （264 ページ）の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]**>**[スキーマ (Schemas)]** を選択します。

ステップ 3 [スキーマ (schema)] を選択し、VRF と L3Out を作成またはインポートするテンプレートを選択します。

複数のサイトに関連付けられているテンプレートで L3Out を作成すると、L3Out がそれらすべてのサイトに作成されます。1 つのサイトに関連付けられているテンプレートで L3Out を作成すると、そのサイトでのみ L3Out が作成されます。

ステップ 4 新しい VRF と L3Out を作成します。

既存の L3Out をインポートする場合は、この手順をスキップします。

（注）
NDO で L3Out オブジェクトを作成し、それを APIC にプッシュすることはできますが、L3Out の物理設定は APIC で実行する必要があります。

a) **[VRF]** エリアまで下にスクロールし、+ アイコンをクリックして新しい VRF を追加します。

右側のサイドバーで、VRF の名前を入力します (例: `vrf-l3out`)。

b) **[L3Out]** 領域まで下にスクロールし、+ アイコンをクリックして新しい L3Out を追加します。

右側のスライダで、必要な情報を入力します。

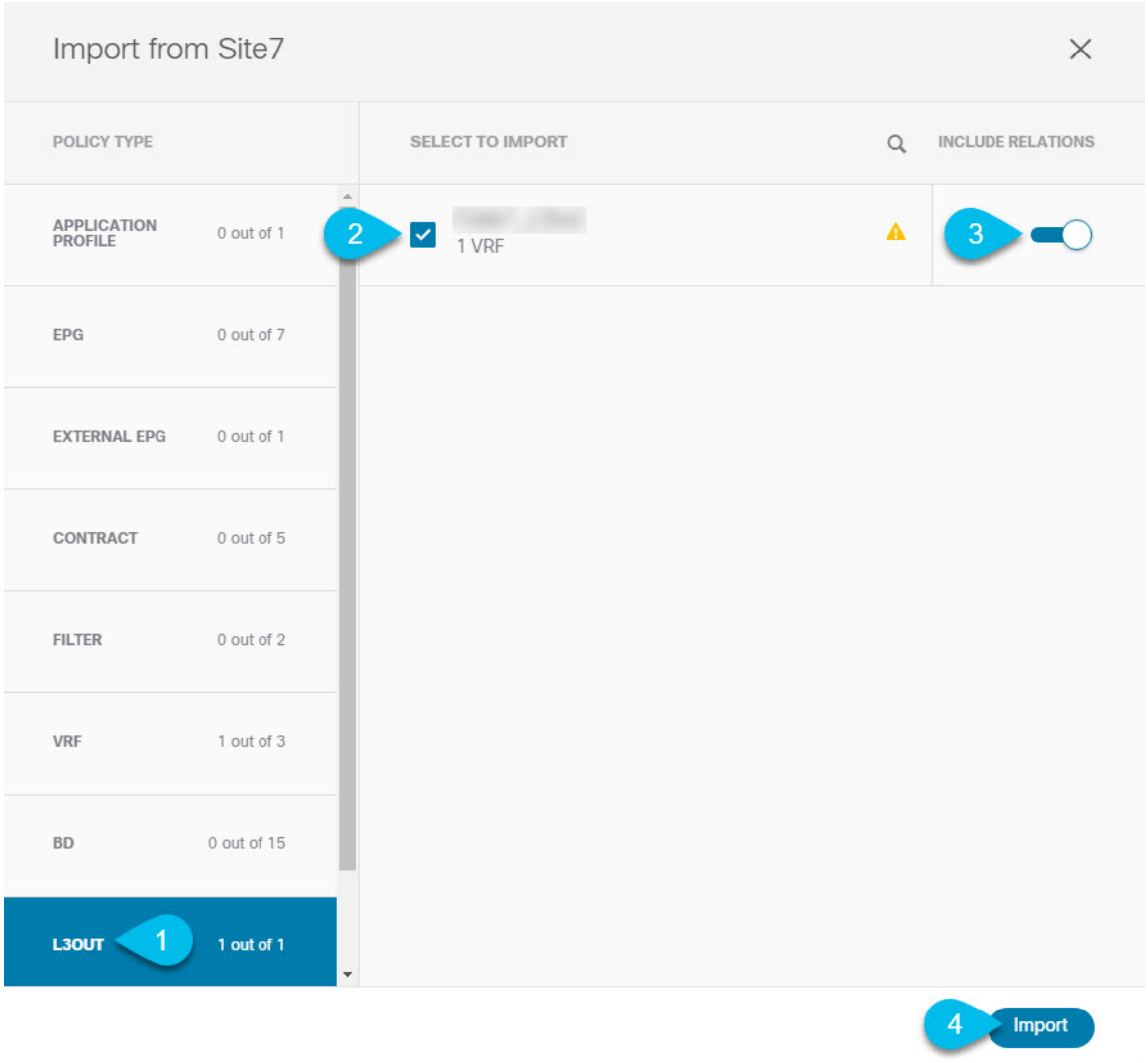
c) L3Out の名前を指定します (例: `l3out-intersite`。

d) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、前のステップで作成された VRF を選択します。

ステップ 5 既存の L3Out をインポートします。

前の手順で新しい L3Out を作成した場合は、この手順をスキップします。

メインテンプレートビューの上部で **[インポート (Import)]** をクリックし、インポート元のサイトを選択します。



a) [インポート (Import)] ウィンドウの **[ポリシー タイプ(Policy Type)]** メニューで、[**L3Out**] を選択します。
b) インポートする L3Out をチェックします。
c) （オプション）L3Out に関連付けられているすべてのオブジェクトをインポートする場合は、**[関係を含める (Include Relationships)]** ノブを有効にします。
d) [インポート（Import）] をクリックします。

外部 EPG の設定

このセクションでは、サイト間 L3Out と関連付ける外部 EPG の作成方法について説明します。その後、この外部 EPG とコントラクトを使用すれば、あるサイトのエンドポイント用の特定のユース ケースを設定し、別のサイトの L3Out を使用することができます。

始める前に

次のものが必要です。

- テンプレートの作成 （264 ページ）の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。
- サイト間 L3Out および VRF の作成またはインポート （276 ページ）の説明に従って作成された、またはインポートされた L3Out と VRF。

手順

ステップ 1 外部 EPG を作成するテンプレートを選択します。

複数のサイトと関連付けられているテンプレート内で外部 EPG を作成した場合、その外部 EPG は、それらすべてのサイト上で作成されます。単一のサイトと関連付けられているテンプレート内で外部 EPG を作成した場合、その外部 EPG は、そのサイト内でのみ作成されます。

ステップ 2 **[外部 EPG (External EPG)]** エリアまで下方にスクロールして、+ アイコンをクリックして外部 EPG を追加します。

右側のスライダで、必要な情報を入力します。

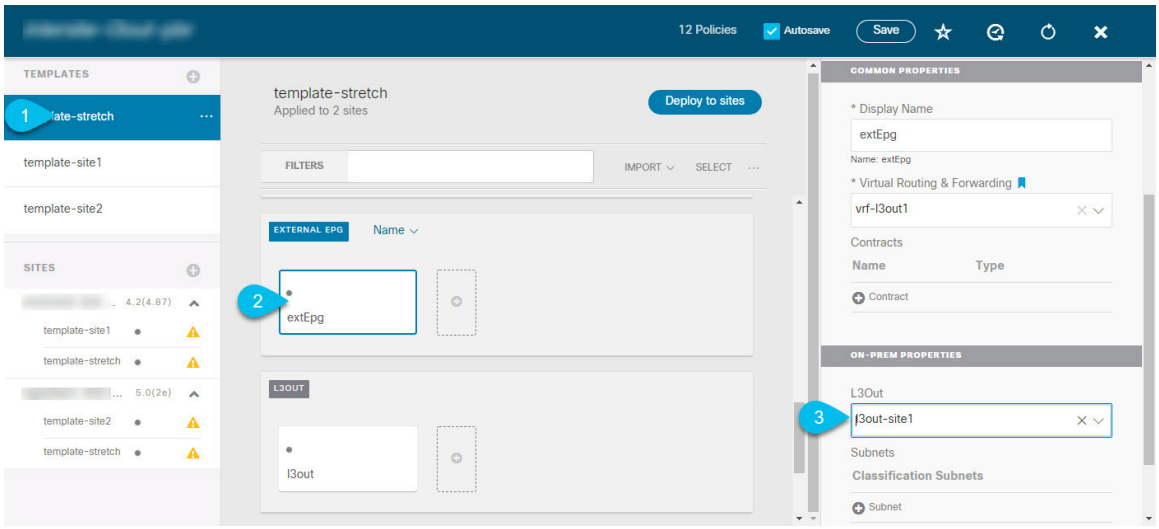
a) 外部 EPG の名前を入力します。たとえば `extEpg` のようにします。
b) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、先ほど作成した、L3Out 用の VRF を選択します。
c) **[+コントラクト (+Contract)]** をクリックし、コントラクトを選択します。

EPG 通信用に作成したコントラクトを選択し、そのタイプを設定します。

アプリケーション EPG と L3Out 外部 EPG に同じ VRF を使用している場合は、どちらかをコンシューマまたはプロバイダーとして選択できます。ただし、それらが異なる VRF にある場合は、外部 EPG のコントラクト タイプのプロバイダを選択する必要があります。

ステップ 3 L3Out をテンプレート レベルで割り当てるには...

外部 EPG 用の L3Out は、テンプレート レベルで選択し、設定できます。その場合、L3Out をサイトローカル レベルで設定することはできません。



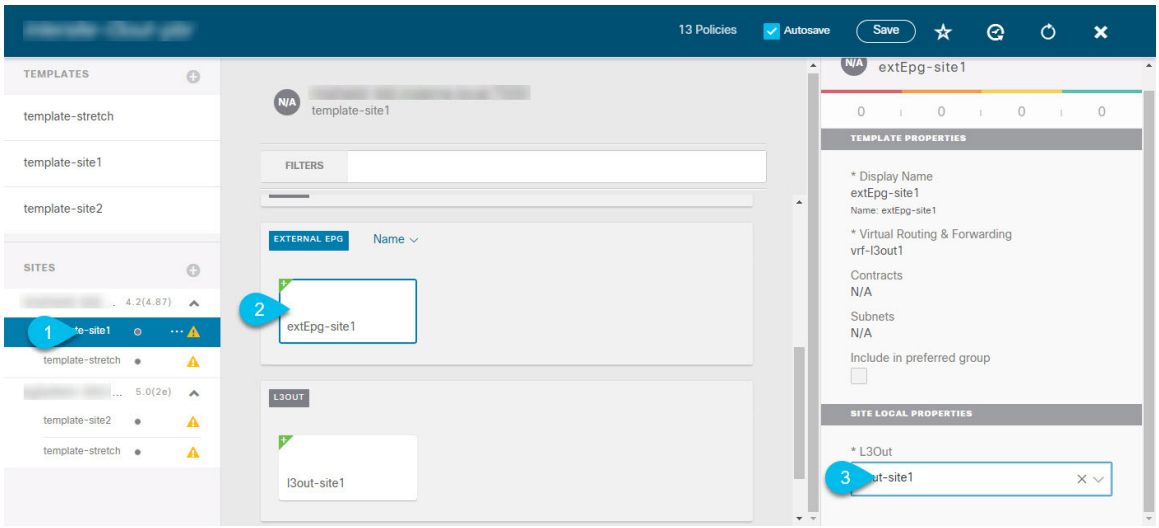
a) スキーマ ビューの左サイドバーで、外部 EPG が置かれているテンプレートを選択します。

b) **[外部 EPG (External EPG)]** エリアまで下方にスクロールして、外部 EPG を選択します。

c) 右サイドバーで、**[L3Out]** ドロップダウンまで下方にスクロールして、作成したサイト間 L3Out を選択します。

ステップ 4 L3Out をサイトローカル レベルで割り当てるには...

代わりに、L3Out をサイトローカル レベルで外部 EPG に関連付けることもできます。

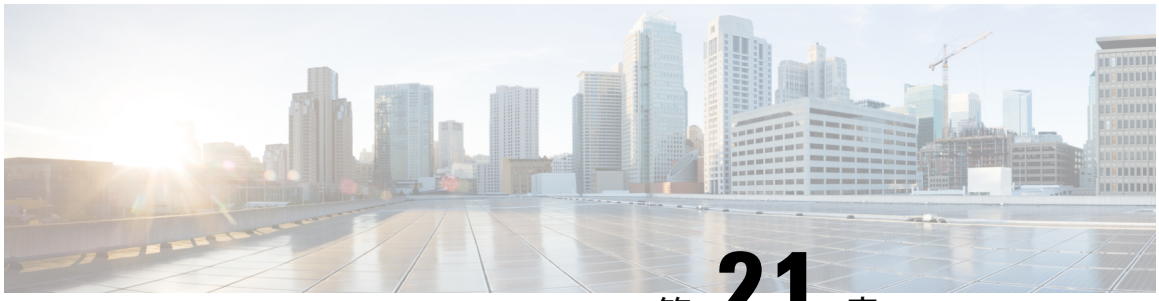


a) スキーマ ビューの左サイドバーで、外部 EPG が配置されているテンプレートを選択します。

b) **[外部 EPG (External EPG)]** エリアまで下方にスクロールして、外部 EPG を選択します。

c) 右サイドバーで、**[L3Out]** ドロップダウンまで下方にスクロールして、作成したサイト間 L3Out を選択します。

この場合、APIC で管理されている L3Out と、オーケストレーションで管理されている L3Out の両方が選択できます。前のセクションでこの目的のため特に作成した L3Out、またはサイトの APIC 内にすでにある L3Out のいずれかを選択します。



第 21 章

レイヤ 3 マルチキャスト

レイヤ 3 マルチキャスト

Cisco マルチキャスト レイヤ 3 マルチキャストは、VRF、ブリッジ ドメイン (BD)、およびマルチキャスト ソースが存在している任意の EPG という、3 つのレベルで有効または無効にできます。

トップ レベルでは、マルチキャスト ルーティングは、任意のマルチキャストが有効な BD を持つ VRF で有効にする必要があります。マルチキャストが有効な VRF では、マルチキャストが有効な BD と、マルチキャスト ルーティングが無効な BD の組み合わせにすることができます。Cisco Nexus Dashboard Orchestrator GUI で VRF のマルチキャスト ルーティングを有効にすると、VRF が拡張されている APIC サイトで有効になります。

いったんマルチキャストで VRF を有効にすると、VRF の下の個別の BD では、マルチキャスト ルーティングを有効にすることができます。BD でレイヤ 3 マルチキャストを設定すると、その BD 上では、プロトコル独立ルーティング (PIM) が有効になります。デフォルトでは、PIM はすべての BD で無効になっています。

特定のサイトローカル EPG に属するソースがリモートサイトにマルチキャスト トラフィックを送信する場合、Nexus Dashboard Orchestrator はシャドウ EPG を作成し、ソース EPG のリモートサイトで対応するサブネット ルートをプログラムする必要があります。リモート Top-of-Rack（TOR）スイッチに適用される設定変更を制限するには、マルチキャスト送信元が存在するローカル EPG でレイヤ 3 マルチキャストを明示的に有効にする必要があります。これにより、これらの EPG に必要な設定のみがリモート サイトにプッシュされます。マルチキャストの受信者が存在する EPG では、レイヤ 3 マルチキャストを有効にする必要はありません。

マルチサイトは、以下のレイヤ 3 マルチキャスト送信元と受信者のすべての組み合わせをサポートしています。

- ACI ファブリック内のマルチキャスト送信元と受信者
- ACI ファブリック外のマルチキャスト送信元と受信者
- ACI ファブリック内のマルチキャスト送信元と外部受信者
- ACI ファブリック内のマルチキャスト受信者と外部送信元

レイヤ3マルチキャスト ルーティング

次に示すのは、サイト間レイヤ 3 マルチキャスト ルーティングの高レベルでの概要です。

- マルチキャスト送信元がエンドポイント (EP) として ACI ファブリックに 1 つのサイトで接続され、マルチキャストフローのストリーミングを開始すると、送信元VRFの指定フォワーダとして選択された特定のサイトのスパイン スイッチは、すべてのリモート サイトにマルチキャストトラフィックを転送します。これらのサイトでは、ヘッド エンド レプリケーション(HREP)を使用してソースのVRFがストレッチされます。特定のリモートサイトにその特定のグループのレシーバが存在しない場合。トラフィックは受信スパインノードでドロップされます。少なくとも1つのレシーバがある場合、トラフィックはサイトに転送され、すべてのリーフ ノードに到達します。ここでは VRF が展開されており、その時点でのグループ メンバーシップ情報に基づいてプルーニング/転送が行われます。
- Cisco ACI リリース 5.0(1) よりも前では、マルチキャスト ルーティング ソリューションは、外部マルチキャスト ルータが、PIM-SM エニーソース マルチキャスト（ASM）が展開されたランデブー ポイント（RP）である必要がありました。それぞれのサイトは、指定された拡張VRFに対し、同じRPアドレスをポイントしている必要があります。RPは、サイトローカルの L3Out を介して、各サイトに到達できる必要があります。
- 送信元がファブリックの外側、受信者が内側にある場合、受信者は、RPに対するPIMジョインとしてのサイトローカルのL3Outを介してトラフィックをプルします。送信元は常にサイトローカルの L3Out を介して送信されます。
- 各サイトの受信者には、外部の送信元からのトラフィックを、サイトローカルのL3Outを介して取り込むことが期待されます。そのため、あるサイトのL3Outで受信したトラフィックを他のサイトに送信することはできません。このことは、スパインにおいて、HREP トンネルへ複製中のマルチキャストトラフィックをプルーニングすることによって行われます。

  これを可能にするために、外部送信元から発信され、ローカルL3Outで受信されるすべてのマルチキャストトラフィックは、外部VXLANヘッダーの特別なDSCP値で再マーキングされます。スパインはその特定のDSCP値と一致するため、トラフィックがリモートサイトに複製されることはありません。
- サイトに接続された送信元から発信されたトラフィックは、ローカルL3Outまたはリモートサイトに展開された L3Out を介して外部レシーバに送信できます。これに使用される

特定の L3Out は、外部ネットワークからその特定のマルチキャストグループの PIM Join を受信したサイトにのみ依存します。

- BD と Nexus Dashboard Orchestrator 上の EPG でマルチキャストが有効にされている場合、BD のすべてのサブネットは、境界リーフ (BL) ノードを含めて、すべてのリーフ スイッチのルーティング テーブルにプログラミングされます。これにより、リーフ スイッチにアタッチされた受信者は、送信側 BD がリーフ スイッチに存在しない場合に、マルチキャスト ソースの到達可能性を判定することができます。BL に対して適切なポリシーが設定されていた場合、サブネットは外部ネットワークにアドバタイズされます。ホストベースのルーティングが BD で設定されている場合、/32 ホストルートがアドバタイズされます。

マルチキャスト ルーティングについての詳細は、IP マルチキャストのセクションを参照してください。これは*Cisco APIC* レイヤ *3* ネットワーク コンフィギュレーション ガイドに記されています。

ランデブー ポイント

マルチキャスト トラフィック ソースは、マルチキャスト アドレス グループにパケットを送信し、そのグループに参加するすべてのユーザーがパケットを受信できるようにします。1 つまたは複数のグループからのトラフィックを受信する受信者はは、通常は Internet Group Management Protocol (IGMP) を使用して、グループへの参加を要求できます。受信者がグループに参加するたびに、そのグループに対してマルチキャスト配信ツリーが作成されます。ランデブー ポイント（RP）は、PIM-SM マルチキャスト ドメイン内にあるルータで、マルチキャスト共有ツリーの共有ルートとして動作します。

ネットワークに冗長 RP 機能を提供する一般的な方法は、ネットワーク内の 2 つ以上の RP が同じエニーキャスト IP アドレスを共有できるようにする、エニーキャスト RP と呼ばれる機能を導入することです。これにより、冗長性とロード バランシングが提供されます。1つの RP デバイスに障害が発生した場合、他の RP はサービスを中断せずに引き継ぐことができます。マルチキャスト ルータは、ネットワーク内のエニーキャスト RP のいずれかに接続して、最も近い RP に転送される join 要求を使用して、マルチキャスト共有ツリーに参加することもできます。

Nexus Dashboard Orchestrator では、次の 2 種類の RP 設定がサポートされています。

- **静的 RP**—RP が ACI ファブリックの外部にある場合。
- **ファブリック RP**：ACI ファブリック内の境界リーフ スイッチがエニーキャスト RP として機能する場合。

任意の数のルータを RP として機能するように設定できます。また、異なるグループ範囲をカバーするようにそれらを設定できます。ACI ファブリック内部で RP を定義する場合には、グループのリストを含むルートマップ ポリシーを作成し、それを VRF に追加するときにこのポリシーを RP にアタッチすることで、RP がカバーするグループを設定できます。ルートマップの作成についてはマルチキャスト ルート マップ ポリシーの作成 （289 ページ） で説明しており、VRF の設定については Any-Source Multicast（ASM）マルチキャストの有効化 （291 ページ） で説明しています。

スタティック RP とファブリック RP の両方で、マルチキャストルーティングが有効になっている VRF に PIM 対応境界リーフ スイッチが必要です。L3Out の設定は、L3Out の PIM の有効化を含め、各サイトの APIC から現在ローカルに設定されています。L3Out での PIM の設定の詳細については、*Cisco APIC Layer 3 Networking Configuration Guide*を参照してください。

マルチキャスト フィルタ処理

マルチキャストフィルタリングは、Cisco APIC リリース 5.0(1) およびNexus Dashboard Orchestrator リリース 3.0(1) 以降で使用可能なマルチキャスト トラフィックのデータプレーン フィルタリング機能です。

Cisco APIC は、誰がマルチキャスト フィードを受信でき、どのソースから受信できるかを制御するために使用できるコントロール プレーン構成をサポートしています。一部の展開で、データプレーン レベルでマルチキャスト ストリームの送信および/または受信を制限することが望ましい場合があります。たとえば、LAN 内のマルチキャスト送信者が特定のマルチキャスト グループにのみ送信できるようにするか、受信者が特定の送信元からのみマルチキャストを受信できるようにする必要がある場合があります。

Nexus Dashboard Orchestrator からのマルチキャスト フィルタリングを構成するには、送信元と宛先のマルチキャスト ルート マップを作成します。それぞれのマップには、マルチキャスト トラフィックの送信元 IP および / またはアクション (許可 (Permit) または 拒否 (Deny)) が関連付けられたグループに基づく 1 つ以上のフィルタ エントリが含まれています。次に、ルート マップをブリッジ ドメインにアタッチして、ブリッジ ドメインでフィルタリングを有効にします。

マルチキャスト ルート マップを作成すると、1 つ以上のフィルタ エンティティを定義できます。一部のエントリは 許可(Permit) アクションで設定でき、その他のエントリは 拒否(Deny) アクションで設定できます。すべてが同じルートマップ内で行われます。各エントリに対して、**送信元 IP** と **グループ IP** を提供して、フィルタに一致するトラフィックを定義できます。これらのフィールドの少なくとも 1 つを提供できますが、両方を含むことを選択できます。フィールドの 1 つが空白のままの場合は、すべての値と一致します。

マルチキャスト送信元フィルタリングとマルチキャスト受信先フィルタリングの両方を同じブリッジ ドメインで有効にできます。この例では、1 つのブリッジ ドメインが送信元のみならず、受信先の両方に対してフィルタ処理を提供できます。

BD に対してルート マップを提供しない場合、デフォルト アクションはブリッジ ドメインですべてのマルチキャスト トラフィックを許可することです。しかし、ルート マップを選択する場合、デフォルト アクションはルート マップのフィルタ エントリに明示的に一致しないトラフィックを拒否するように変更されます。

送信元のフィルタ処理

ブリッジ ドメインでトラフィックを送信する任意のマルチキャスト ソースの場合、1 つ以上の送信元とグループ IP フィルタが定義されているルート マップ ポリシーを設定できます。次に、トラフィックはルートマップのすべてのエントリと照合され、次のいずれかのアクションが実行されます。

- トラフィックがルートマップの許可（Permit）アクションを持つフィルタ エントリと一致する場合、ブリッジドメインはそのソースからそのグループへのトラフィックを許可します。
- トラフィックがルートマップの拒否（Deny）アクションを持つフィルタ エントリと一致する場合、ブリッジドメインはそのソースからそのグループへのトラフィックを拒否します。
- トラフィックがルート マップの任意のエントリと一致しない場合、デフォルトの 拒否（Deny）アクションが適用されます。

送信元フィルタは、送信元が接続されている ACI リーフノードで表されるファーストホップ ルータ (FHR) のブリッジ ドメインに適用されます。フィルタは、異なるブリッジ ドメイン内の受信先、同じブリッジ ドメイン内の受信先、および外部受信先がマルチキャストを受信するのを防ぎます。

宛先 (受信先) フィルタ処理

宛先 (受信先) フィルタ処理は、受信先がマルチキャスト処理グループに参加することを妨げません。マルチキャスト トラフィックは、代わりに、送信元 IP とマルチキャスト グループの組み合わせに基づいて、データプレーンで許可またはドロップされます。

送信元フィルタ処理と同様に、マルチキャスト トラフィックが宛先フィルタと一致するとき、次のアクションの一つが起こります。

- トラフィックがルート マップの許可（Permit）アクションを持つフィルタ エントリと一致する場合、ブリッジ ドメインはその送信元から受信先へのトラフィックを許可します。
- トラフィックがルート マップの拒否（Deny）アクションを持つフィルタ エントリと一致する場合、ブリッジドメインはその送信元から受信先へのトラフィックを拒否します。
- トラフィックがルート マップの任意のエントリと一致しない場合、デフォルトの 拒否（Deny）アクションが適用されます。

宛先フィルタは、ACI リーフ ノードが代表する、ラストホップ ルーター (LHR) 上のブリッジ ドメインに適用されるため、その他のブリッジ ドメインはマルチキャスト トラフィックを引き続き受信できます。

Layer 3 マルチキャストに関するガイドラインと制限事項

現在のソフトウェアリリースまでは、Cisco Nexus Dashboard Orchestrator を使用して、IGMP または PIM 関連のポリシーなどの特定のマルチキャスト コントロール プレーン フィルタリング ポリシーを各サイトに展開することはできません。したがって、エンドツーエンド ソリューションが機能するためには、各 APIC サイトでの使用例に必要な追加ポリシーを個別に設定する必要があります。各サイトでこれらの設定を構成する方法の詳細については、『*CISCO APIC Layer 3 Network Configuration Guide*』を参照してください。

また、すべてのファブリックのQoS DSCP変換ポリシーが一貫して設定されていることを確認する必要があります。ACIファブリックでカスタムQoSポリシーを作成する場合、ACI QoSレベルと、ファブリックに出入りするパケットのパケットヘッダーDSCP値との間のマッピングを作成できます。マルチキャストトラフィックがサイト間を通過するには、すべてのサイトで同じACI QoSレベルを同じDSCP値にマッピングする必要があります。各サイトでこれらの設定を構成する方法の詳細については、*CISCO APIC and QoS* を参照してください。

マルチキャスト フィルタ処理

マルチキャスト フィルタ処理を有効にすると、次の追加のガイドラインが適用されます。

- マルチキャスト フィルタ処理は、IPv4 でのみサポートされています。
- 同じブリッジドメインで、マルチキャスト送信元フィルタ処理または受信者フィルタ処理のいずれかまたは両方を有効にできます。
- ブリッジ ドメインにマルチキャスト フィルタを設定しない場合は、そのブリッジドメインで送信元フィルタまたは宛先フィルタ ルート マップを設定しないでください。

  デフォルトでは、ルートマップはブリッジドメインに関連付けられていません。これは、すべてのマルチキャストトラフィックが許可されることを意味します。ルートマップがブリッジ ドメインに関連付けられている場合、そのルートマップ内の permit エントリだけが許可され、その他のすべてのマルチキャスト トラフィックはブロックされます。

  空のルートマップをブリッジ ドメインに接続すると、ルートマップはデフォルトで `deny all` を想定するため、すべての送信元とグループがそのブリッジ ドメインでブロックされます。
- マルチキャストフィルタリングはBD レベルで実行され、BD 内のすべての EPG に適用されます。そのため、同じ BD 内の異なる EPG に対して異なるフィルタリング ポリシーを設定することはできません。EPG レベルでより詳細にフィルタリングを適用する必要がある場合は、EPG を個別の BD に設定する必要があります。
- マルチキャスト フィルタ処理は、任意の送信元マルチキャスト (ASM) 範囲にのみ使用することを目的としています。Source-Specific Multicast（SSM）は送信元フィルタリングではサポートされず、受信者フィルタリングでのみサポートされます。
- 送信側と受信側両方のフィルタ処理の場合、ルート マップ エントリはエントリの指定された順序に基づいて照合され、最も小さい番号が最初に一致します。これは、より低い順序のエントリが、リスト内で最長一致でない場合でも、最初に一致することを意味し、より高い順序のエントリは考慮されません。

  たとえば、 `192.0.3.1/32` ソースに対して次のルートマップがあるとします。

順位	送信元 IP	アクション
1	192.0.0.0/16	Permit
2	192.0.3.0/24	拒否

2番目のエントリ (192.0.3.0/24) が送信元 IP と一致する場合でも、最初のエントリ (192.0.0.0/16) は、下位の番号が原因で照合されます。

マルチキャスト ルート マップ ポリシーの作成

このセクションでは、マルチキャスト ルート マップ ポリシーを作成する方法について説明します。ルート マップを作成する理由としては、次のものが考えられます。

- マルチキャスト ソース フィルタリングのためにフィルタのセットを定義する。
- マルチキャスト デスティネーション フィルタリングのためにフィルタのセットを定義する。
- ランデブー ポイント (RP) のためのグループ IP のセットを定義する。

  VRF 用の RP を設定する場合、ルート マップを指定しなければ、RP はその VRF のすべてのマルチキャスト グループ範囲（224.0.0.0/4） に合わせて定義されます。または、定義済みのグループまたはグループ範囲を持つルート マップを指定して、RP をそのグループのみに制限することができます。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 新しいテナント ポリシーを作成。

a) 左側のナビゲーション メニューで、**[アプリケーション管理（Application Management）]** > **[テナント ポリシー（Tenant Policies）]** を選択します。

b) **[テナント ポリシー テンプレート（Tenant Policy Template）]**ページ内で**[テナント ポリシー テンプレートを追加（Add Tenant Policy Template）]**をクリックします。

c) テナント ポリシー ページの右のプロパティ サイトバーにテナントの **[名前（Name）]** を入力します。

d) **[テナントの選択（Select a Tenant）]**ドロップダウンから、このテンプレートに関連付けるテナントを選択します。

次の手順で説明するようにテンプレートで作成したすべてのポリシーは、テンプレートを特定のサイトにプッシュすると、展開された選択したテナントに関連付けられます。

デフォルトでは、新しいテンプレートは空であるため、次のステップに従って 1 つ以上のテナント ポリシーを追加する必要があります。テンプレートで使用可能なすべてのポリシーを作成する必要はないことに注意してください。マルチキャストのユース ケースに対して 1 つのルート マップ ポリシーだけでテンプレートを作成できます。

ステップ 3 マルチキャストの ルートマップ ポリシーの作成

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[マルチキャストのルート マップ ポリシー（Route Map Policy for Multicast）]** を選択します。

b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。

c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。
d) **[+ マルチキャスト エントリのルート マップを追加（+Add Route Map for Multicast Entries）]** をクリックし、ルート マップ情報を指定します。

ルート マップごとに、1 つ以上のルート マップ エントリを作成する必要があります。次の情報によると各コンテキストは、1 つ以上の一致基準に基づいてアクションを定義するルールです：

- **順序** – 順序は、ルールを評価する順序を決定するために用いられます。
- **グループ IP**、 **Src IP** と **RP IP** – 同じマルチキャスト ルート マップのポリシー UI は 2 つの方法で使用できます。マルチキャスト トラフィックのフィルタのセットを設定すること、またはランデブー ポイントの構成をマルチキャスト グループの特定のセットに制限することです。設定する使用例によっては、この画面のフィールドの一部だけを指定すればよい場合もあります。
  - マルチキャスト フィルタリングの場合には、フィルタを定義するために、**[ソース IP (Source IP)]** と **[グループ (Group IP)]** フィールドを使用します。これらのフィールドの少なくとも 1 つを提供できますが、両方を含むことを選択できます。フィールドの 1 つが空白のままの場合は、すべての値と一致します。

    グループ IP の範囲は `224.0.0.0` ～ `239.255.255.255` で、ネットマスクは `/4` ～ `/32` である必要があります。サブネット マスクを指定する必要があります。

    RP IP (ランデブー ポイントの IP) は、マルチキャスト フィルタリング ルート マップでは使用しないので、このフィールドはブランクのままにします。
  - ランデブー ポイントの設定では、**[グループ IP (Group IP)]** フィールドを使用して RP のマルチキャスト グループを定義できます。

    グループ IP の範囲は `224.0.0.0` ～ `239.255.255.255` で、ネットマスクは `/4` ～ `/32` である必要があります。サブネット マスクを指定する必要があります。

    ランデブー ポイント設定の場合、**RP IP** は RP 設定の一部として設定されます。ルート マップをグループ フィルタリングに使用する場合は、ルート マップに RP IP アドレスを設定する必要はありません。この場合には、**[RP IP]** と **[ソース IP (Source IP)]** フィールドを空白のままにします。
- **アクション** – アクションは、一致が検出された場合に実行するアクションの`許可`または`拒否`を定義します。

e) チェックマーク アイコンをクリックして、エントリを保存します。
f) 前のサブステップを繰り返して、同じポリシーの追加のルート マップ エントリを作成します。
g) **[保存（Save）]** をクリックしてポリシーを保存し、テンプレート ページに戻ります。
h) この手順を繰り返して、マルチキャスト ポリシーの追加のルート マップを作成します。

Any-Source Multicast（ASM）マルチキャストの有効化

以下の手順では、Nexus Dashboard Orchestrator GUI を使用して、VRF、BD、および EPG で ASM マルチキャストを有効にする方法を説明しています。SSMマルチキャストを有効にする場合は、代わりにソース固有マルチキャスト（SSM）の有効化（293 ページ）の手順に従います。

始める前に

- Layer 3 マルチキャストに関するガイドラインと制限事項（287 ページ） で説明されている情報を読んで、従っていることを確認してください。
- マルチキャストのフィルタリングを有効にする予定の場合には、マルチキャスト ルート マップ ポリシーの作成（289 ページ） で説明されているように、必要なマルチキャスト ルート マップを作成します。
- ファブリック RP が有効になっている場合、VRF でサイトローカル L3Out の PIM を有効にする必要があります。

  これについては、次の手順のステップ 6 で説明します。L3Out 上での PIM の設定の詳細については、*Cisco APIC レイヤ 3 ネットワーク コンフィギュレーション ガイド*を参照してください。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のサイドバーから、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** ビューを選択します。

ステップ 3 変更するスキーマをクリックします。

ステップ 4 VRD でレイヤ 3 マルチキャストを有効にします。

まず、サイト間で拡張されている VRF でレイヤ 3 マルチキャストを有効にします。

a) レイヤ 3 マルチキャストを有効にする VRF を選択します。
b) 右のプロパティ サイドバーで、**[L3 マルチキャスト (L3 Multicast)]** チェックボックスをオンにします。

ステップ 5 1 つ以上のランデブー ポイント (RP) を追加します。

a) VRF を選択します。
b) 右のプロパティ サイドバーで、**[ランデブー ポイントの追加 (Add Rendezvous Points)]** をクリックします。
c) VRF を選択したまま、右のサイドバーで**[ランデブー ポイントの追加 (Add Rendezvous Points)]** をクリックします。
d) **[ランデブー ポイントの追加 (Add Rendezvous Points)]** ウィンドウで、RP の IP アドレスを入力します。
e) RP のタイプを選択します。

- **静的 RP**—RP が ACI ファブリックの外部にある場合。

- **ファブリック RP**—RP が ACI ファブリック内にある場合。

f) (オプション) **[マルチキャスト ルートマップ ポリシー (Multicast Route-Map Policy)]** ドロップダウンから、以前に設定したルートマップ ポリシーを選択します。

デフォルトでは、入力した RP IP は、ファブリックのすべてのマルチキャスト グループに適用されます。RP を、特定のマルチキャスト グループのセットに制限する場合は、ルート マップ ポリシーでそれらのグループを定義し、ここでそのポリシーを選択します。

ステップ 6 L3Out で PIM を有効にします。

スタティック RP とファブリック RP の両方で、マルチキャストルーティングが有効になっている PIM 対応ボーダー リーフ スイッチが必要です。現在、L3Out 設定は Nexus Dashboard Orchestrator から実行できないため、サイトの APIC で PIM が有効になっていることを直接確認する必要があります。L3Out 上での PIM の設定の詳細については、*Cisco APIC レイヤ 3 ネットワーク コンフィギュレーション ガイド*を参照してください。

a) サイトの Cisco APIC にログインします。
b) 上部のメニューで **[テナント (Tenants)]** をクリックし、L3Out を含むテナントを選択します。
c) 左側のナビゲーションメニューで、**[ネットワーキング (Networking)]** > **[L3Outs]** > ***<l3out-name>*** を選択します。
d) メイン ペインで、**[ポリシー (Policy)]** タブを選択します。
e) **[PIM]** オプションを確認します。

Multi-Site は IPv4 マルチキャストのみをサポートします。

ステップ 7 BD でレイヤ 3 マルチキャストを有効にします。

いったん ＶＲＦ で L3 マルチキャストを有効にすると、L3 マルチキャストをブリッジ ドメイン (BD)レベルで有効にすることができます。

a) レイヤ 3 マルチキャストを有効にする BD を選択します。
b) 右のプロパティ サイドバーで、**[L3 マルチキャスト (L3 Multicast)]** チェックボックスをオンにします。

ステップ 8 (オプション) マルチキャスト フィルタ処理を設定する場合は、送信元と接続先のフィルタ処理のためのルートマップを指定します。

a) BD を選択します。
b) 右のプロパティ サイドバーで、**[ルートマップの送信元フィルタ (Route-Map Source Filter)]** と **[ルートマップの接続先フィルタ (Route-Map Destination Filter)]** を選択します。

同じブリッジ ドメインで、マルチキャスト送信元フィルタ処理または受信者フィルタ処理のいずれかまたは両方を有効にできます。

ルートマップを選択しなかった場合、デフォルトの動作は、「ブリッジ ドメインですべてのマルチ トラフィックを許可する」になります。一方、ルートマップを選択すると、デフォルトの動作は、「ルート マップのフィルタ エントリに明示的にマッチしないすべてのトラフィックを拒否」に変わることに注意してください。

ステップ 9 マルチキャスト ソースが 1 つのサイトにあり、他のサイトに拡張されていない場合は、EPG でサイト間マルチキャスト ソース オプションを有効にします。

BD でL3マルチキャストを有効にしたら、マルチキャスト ソースが接続されている EPG（マルチキャスト対応 BD の一部）でもマルチキャストを有効にする必要があります。

a) レイヤ 3 マルチキャストを有効にする EPG を選択します。
b) 右のサイドバーで、**[サイト間マルチキャスト送信元 (Intersite Multicast Source)]** チェックボックスをオンにします。

ソース固有マルチキャスト（SSM）の有効化

以下の手順では、Nexus Dashboard Orchestrator GUI を使用して、VRF、BD、およびEPG でSSM マルチキャストを有効にする方法を説明しています。ASM マルチキャストを有効にする場合は、代わりにAny-Source Multicast（ASM）マルチキャストの有効化 （291 ページ）の手順に従います。

始める前に

- Layer 3 マルチキャストに関するガイドラインと制限事項 （287 ページ） で説明されている情報を読んで、従っていることを確認してください。
- マルチキャストのフィルタリングを有効にする予定の場合には、マルチキャスト ルート マップ ポリシーの作成 （289 ページ） で説明されているように、必要なマルチキャスト ルート マップを作成します。
- サイトローカル レベルでマルチキャスト対応 BD の IGMPv3 インターフェイス ポリシーを設定する必要があることに注意してください。

  これについては、次の手順のステップ 8 で説明します。追加情報については、*Cisco APIC レイヤ 3 ネットワーク コンフィギュレーション ガイド*を参照してください。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のサイドバーから、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** ビューを選択します。

ステップ 3 変更するスキーマをクリックします。

ステップ 4 VRD でレイヤ 3 マルチキャストを有効にします。

まず、サイト間で拡張されている VRF でレイヤ 3 マルチキャストを有効にします。

a) レイヤ 3 マルチキャストを有効にする VRF を選択します。
b) 右のプロパティ サイドバーで、**[L3 マルチキャスト (L3 Multicast)]** チェックボックスをオンにします。

ステップ 5 （任意）SSM リスナーのカスタム範囲を設定します。

デフォルトの SSM 範囲は 232.0.0.0/8 で、ファブリック内のスイッチで自動的に設定されます。SSM を使用している場合は、この範囲のグループに参加するようにリスナーを設定することを推奨します。この場合は、この手順をスキップできます。

何らかの理由でリスナー設定を変更しない場合は、最大4つの範囲を含むルートマップを作成して、VRF 設定で SSM 範囲を追加できます。新しい範囲を追加すると、その範囲が SSM 範囲になり、ASM に同時に使用できないことに注意してください。

カスタム SSM 範囲の設定は、サイトの APIC で直接行う必要があります。

a) サイトの Cisco APIC にログインします。
b) 上部のメニューで **[テナント (Tenants)]** をクリックし、VRF を含むテナントを選択します。
c) 左側のナビゲーションメニューで、**[ネットワーキング (Networking)]** > **[VRFs]** > ***<VRF-name>*** > **[マルチキャスト (Multicast)]**を選択します。
d) メイン ペインで、**[パターン ポリシー (Pattern Policy)]** タブを選択します。
e) **[ルート マップ (Route Map)]** ドロップダウン (**[ソース固有のマルチキャスト (Source Specific Multicast (SSM))]** 領域) から、既存のルート マップを選択するか、**[マルチキャストのためのルート マップ ポリシーの作成 (Create Route Map Policy for Multicast)]** オプションをクリックして、新しいルート マップ ポリシーを作成します。

   既存のルート マップを選択した場合は、ドロップダウンの横にあるアイコンをクリックして、ルート マップの詳細を表示します。

   開いたルート マップの詳細ウィンドウまたは **[マルチキャストのためのルート マップ ポリシーの作成 (Create Route Map Policy for Multicast)]** ウィンドウで **[+]** をクリックしてエントリを追加します。次に、グループ IP を設定します。新しい範囲を定義するのに必要なのは、グループ IP アドレスだけです。

ステップ 6 （任意）サイトの L3Out で PIM を有効にします。

マルチキャストの送信元や受信者を外部ネットワーク ドメインに接続する場合は、サイトの L3Out でも PIM を有効にする必要があります。現在、L3Out 設定は Nexus Dashboard Orchestrator から実行できないため、サイトの APIC で PIM が有効になっていることを直接確認する必要があります。L3Out 上での PIM の設定の詳細については、*Cisco APIC レイヤ 3 ネットワーク コンフィギュレーション ガイド*を参照してください。

a) サイトの Cisco APIC にログインします。
b) 上部のメニューで **[テナント (Tenants)]** をクリックし、L3Out を含むテナントを選択します。
c) 左側のナビゲーションメニューで、**[ネットワーキング (Networking)]** > **[L3Outs]** > ***<l3out-name>*** を選択します。
d) メイン ペインで、**[ポリシー (Policy)]** タブを選択します。
e) **[PIM]** オプションを確認します。

   Multi-Site は IPv4 マルチキャストのみをサポートします。

ステップ 7 BD でレイヤ 3 マルチキャストを有効にします。

いったん ＶＲＦ で L3 マルチキャストを有効にすると、L3 マルチキャストをブリッジ ドメイン (BD)レベルで有効にすることができます。

a) レイヤ 3 マルチキャストを有効にする BD を選択します。
b) 右のプロパティ サイドバーで、**[L3 マルチキャスト (L3 Multicast)]** チェックボックスをオンにします。

ステップ 8 レシーバが接続されているブリッジ ドメインで IGMPv3 インターフェイス ポリシーを有効にします。

SSM を設定しているため、IGMPv3 インターフェイス ポリシーも BD に割り当てる必要があります。デフォルトでは、PIM がイネーブルの場合、IGMP も SVI で自動的にイネーブルになりますが、デフォルト バージョンは IGMPv2 に設定されます。IGMP インターフェイス ポリシーを明示的に IGMPv3 に設定する必要があります。これは、サイトローカル レベルで実行する必要があります。

a) サイトの Cisco APIC にログインします。
b) 上部のメニューで **[テナント (Tenants)]** をクリックし、BD を含むテナントを選択します。
c) 左側のナビゲーションメニューで、**[ネットワーキング (Networking)]** > **[ブリッジ ドメイン (Bridge Domains)]** > **<*BD-name*>** を選択します。
d) メイン ペインで、**[ポリシー (Policy)]** タブを選択します。
e) **[IGPM ポリシー (IGMP Policy)]** ドロップダウンから IGMP ポリシーを選択するか、**[IGMP インターフェイス ポリシーの作成 (Create IGMP Interface Policy)]** をクリックして新しいポリシーを作成します。

既存のポリシーを選択した場合は、ドロップダウンの横にあるアイコンをクリックして、ポリシーの詳細を表示します。

開いているポリシーの詳細ウィンドウまたは**[マルチキャストのためのルート ポリシーの作成 (Create Route Map Policy for Multicast)]** ウィンドウで、**[バージョン (Version)]** フィールドが `[バージョン 3 (Version 3)]` に設定されていることを確認します。

ステップ 9 (オプション) マルチキャスト フィルタ処理を設定する場合は、送信元と接続先のフィルタ処理のためのルートマップを指定します。

a) BD を選択します。
b) 右のプロパティ サイドバーで、**[ルートマップの送信元フィルタ (Route-Map Source Filter)]** と **[ルートマップの接続先フィルタ (Route-Map Destination Filter)]**を選択します。

同じブリッジ ドメインで、マルチキャスト送信元フィルタ処理または受信者フィルタ処理のいずれかまたは両方を有効にできます。

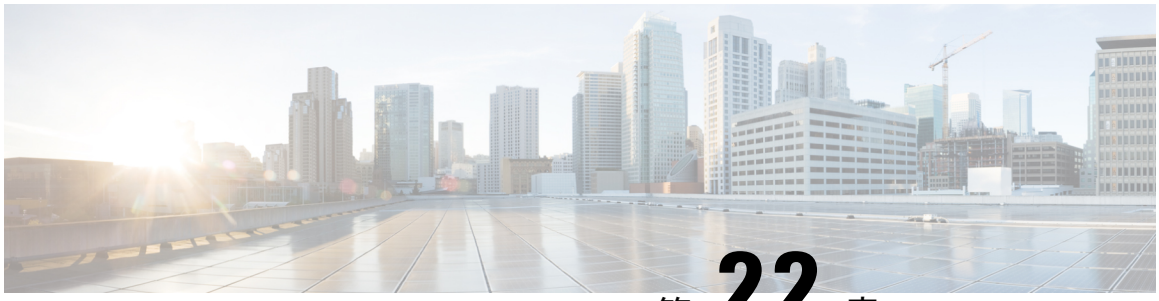
ルート マップを選択しなかった場合、デフォルトの動作は、「ブリッジ ドメインですべてのマルチトラフィックを許可する」になります。一方、ルート マップを選択すると、デフォルトの動作は、「ルート マップのフィルタ エントリに明示的にマッチしないすべてのトラフィックを拒否」に変わることに注意してください。

ステップ 10 マルチキャスト ソースが 1 つのサイトにあり、他のサイトに拡張されていない場合は、EPG でサイト間マルチキャスト ソース オプションを有効にします。

BD で L3 マルチキャストを有効にしたら、マルチキャスト ソースが接続されている EPG（マルチキャスト対応 BD の一部）でもマルチキャストを有効にする必要があります。

a) レイヤ 3 マルチキャストを有効にする EPG を選択します。

b) 右のサイドバーで、**[サイト間マルチキャスト送信元 (Intersite Multicast Source)]** チェックボックスをオンにします。



第 22 章

IPN 全体での QoS の保持

QoS およびグローバル DSCP ポリシー

Cisco ACI Quality of Service（QoS）機能を使用すると、ファブリック内のネットワーク トラフィックを分類し、トラフィック フローの優先順位付けとポリシングを行って、ネットワークの輻輳を回避できます。トラフィックがファブリック内で分類されると、QoS 優先度レベルが割り当てられます。この優先度レベルは、ネットワーク全体で最も望ましいパケットフローを実現するためにファブリック全体で使用されます。

Nexus Dashboard Orchestrator のこのリリースは、ソース EPG または特定のコントラクトに基づく QoS レベルの設定をサポートします。追加のオプションは、各ファブリックで直接使用できます。ACI QoSの詳細については、*Cisco APICおよびQoS* を参照してください。

Cisco ACI ファブリック内でトラフィックが送受信される場合、QoS レベルは VXLAN パケットの外部ヘッダーの CoS 値に基づいて決定されます。マルチポッドやリモート リーフ トポロジなどの特定の使用例では、トラフィックはサイト間ネットワークを通過する必要があります。この場合、Cisco APIC の管理下にないデバイスはパケット内の CoS 値を変更できます。このような場合、パケット内の Cisco ACI QoS レベルと DSCP 値の間のマッピングを作成することで、同じファブリックまたは異なるファブリックの部分間で ACI QoS レベルを維持できます。

DSCP ポリシーの注意事項と制限事項

グローバル DSCP 変換ポリシーを設定する場合は、次の注意事項が適用されます。

（注） SD-WAN 統合とともにグローバル DSCP 変換ポリシーを使用する場合は、この章をスキップし、注意事項と制限事項の完全なリストを含むすべての情報について、SD-WAN の統合 （325 ページ） 章を参照してください。

- グローバル DSCP ポリシーは、オンプレミス サイトでのみサポートされます。
- グローバル DSCP ポリシーを定義する場合は、QoS レベルごとに一意の値を選択する必要があります。
- QoS レベルを割り当てる場合、特定のコントラクトまたは EPG 全体に割り当てることができます。

  特定のトラフィックに複数の QoS レベルを適用できる場合は、次の優先順位を使用して 1 つだけが適用されます。

  - コントラクト QoS レベル：コントラクトで QoS が有効になっている場合は、コントラクトで指定された QoS レベルが使用されます。
  - 送信元 EPG QoS レベル：コントラクトに QoS レベルが指定されていない場合、送信元 EPG に設定された QoS レベルが使用されます。
  - デフォルトの QoS レベル：QoS レベルが指定されていない場合、トラフィックにはデフォルトでレベル 3 の QoS クラスが割り当てられます。

グローバル DSCP ポリシーの設定

Cisco ACI ファブリック内でトラフィックが送受信される場合、VXLAN パケットの外部ヘッダーの CoS 値に基づいて決定される ACI QoS レベルに基づいて優先順位が付けられます。マルチポッドおよびリモート リーフ トポロジなど、サイト間ネットワークに向けてトラフィックが ACI ファブリックを出ると、QoS レベルは VXLAN カプセル化パケットの外部ヘッダーに含まれる DSCP 値に変換されます。

ここでは、ACI ファブリックを出入りするトラフィックの DSCP 変換ポリシーを定義する方法について説明します。これは、トラフィックが非 ACI ネットワークを通過する必要がある場合に必要です。この場合、Cisco APIC の管理下にないデバイスは、通過するパケットの CoS 値を変更できます。

始める前に

- ACI ファブリック内の Quality of Service（QoS）機能に精通している必要があります。

  QoS の詳細については、*Cisco APIC and QoS* を参照してください。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 新しいテナント ポリシーを作成。

a) 左側のナビゲーション メニューで、**[アプリケーション管理（Application Management）]** > **[テナント ポリシー（Tenant Policies）]** を選択します。

b) **[テナント ポリシー テンプレート（Tenant Policy Template）]**ページ内で**[テナント ポリシー テンプレートを追加（Add Tenant Policy Template）]**をクリックします。

c) **[テナント ポリシー（Tenant Policies）]** ページの右のプロパティ サイトバーにテンプレートの **[名前（Name）]** を入力します。

d) **[テナントの選択（Select a Tenant）]**ドロップダウンから、このテンプレートに関連付けるテナントを選択します。

次の手順で説明するようにテンプレートで作成したすべてのポリシーは、テンプレートを特定のサイトにプッシュするとそれに展開され、選択したテナントに関連付けられます。

デフォルトでは、新しいテンプレートは空であるため、次のステップに従って 1 つ以上のテナント ポリシーを追加する必要があります。テンプレートで使用可能なすべてのポリシーを作成する必要はありません。このテンプレートとともに展開する各タイプのポリシーを 1 つ以上定義できます。特定のポリシーを作成したくない場合は、説明されている手順をスキップしてください。

ステップ 3 QoS DSCP ポリシーを作成します。

a) **[+オブジェクトを作成（+Create Object）** ドロップダウンから**QoS SDSCP**を作成します。

b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。

c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。

d) ポリシーの詳細を入力します。

- **管理状態** –ポリシーの有効または、無効化。
- **詳細設定** – このセクションの横にある矢印をクリックして展開します。

各 ACI QoS レベルの DSCP 値を選択します。各ドロップダウンには、使用可能な DSCP 値のデフォルトリストが含まれています。レベルごとに一意の DSCP 値を選択する必要があります。

e) 追加の QoS DSCP ポリシーを作成するために、このステップを繰り返します。

通常、マルチサイト ドメインの一部であるすべてのサイトにこのポリシーを一貫して適用することをお勧めします。

ステップ 4 ポリシーを 1 つ以上のサイトに割り当てます。

a) ファブリック ポリシー テンプレート ビューで、**[アクション（Actions）]** > **[サイトの関連付け（Sites Association）]** を選択します。

b) **<*tempalte*> にサイトを関連** ダイアログ内でこのポリシー テンプレートのために一つ以上のサイトを選択し **Ok** をクリックします。

c) ファブリック ポリシー テンプレート ビューで、**[展開（Deploy）]** をクリックします。

保存して展開すると、DSCPポリシー設定が各サイトにプッシュされます。設定を確認するには、サイトのAPICにログインし、**[テナント (Tenants)]** > **[インフラ (infra)]** > **[ポリシー (Policies)]** > **[プロトコル (Protocol)]** > **[L3 トラフィックの DSCP クラス CoS 変換ポリシー (DSCP class-CoS translation policy for L3 traffic)]**に移動します。

次のタスク

グローバル DSCP ポリシーを定義したら、EPG およびコントラクトの QoS レベルの設定 （300 ページ） の説明に従って、ACI QoS レベルを EPG またはコントラクトに割り当てることができます。

EPG およびコントラクトの QoS レベルの設定

ここでは、ファブリック内のトラフィックの ACI QoS レベルを選択する方法について説明します。個々のコントラクトまたは EPG 全体に対して QoS を指定できます。

始める前に

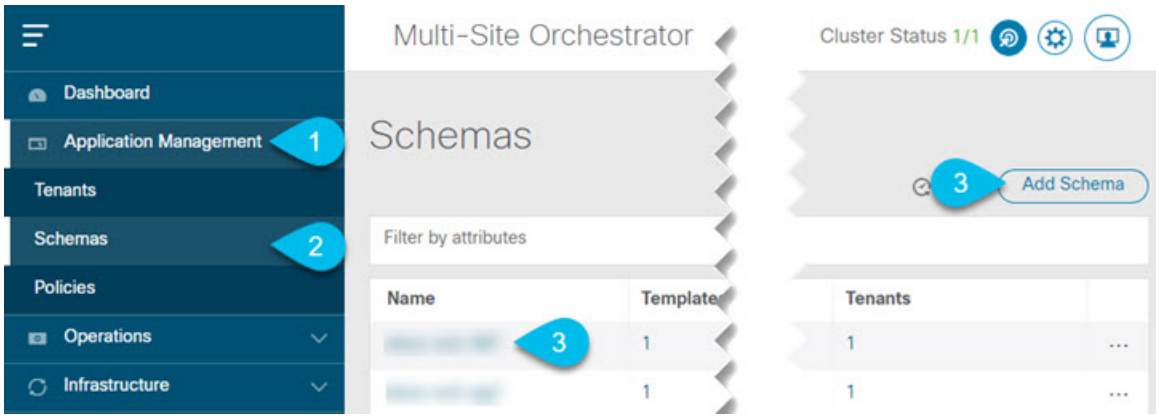
- グローバル DSCP ポリシーの設定 （298 ページ）の説明に従って、グローバル DSCP ポリシーを定義しておく必要があります。
- ACI ファブリック内の Quality of Service（QoS）機能に精通している必要があります。

  QoS の詳細については、*Cisco APIC and QoS* を参照してください。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 編集するスキーマを選択します。

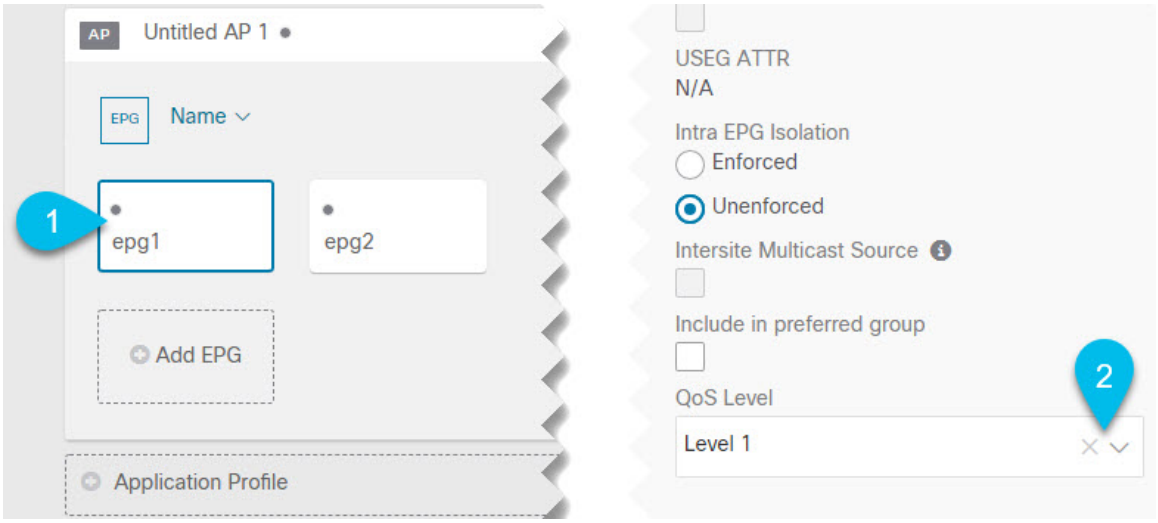


a) **[アプリケーション管理 (Application Management)[** > **[スキーマ (Schemas)]** > の順に移動します。

b) 編集するスキーマの名前をクリックするか、**[スキーマの追加 (Add Schema)]** をクリックして新しいスキーマを作成します。

[ポリシーの編集 (Edit Policy)] ウィンドウが開きます。

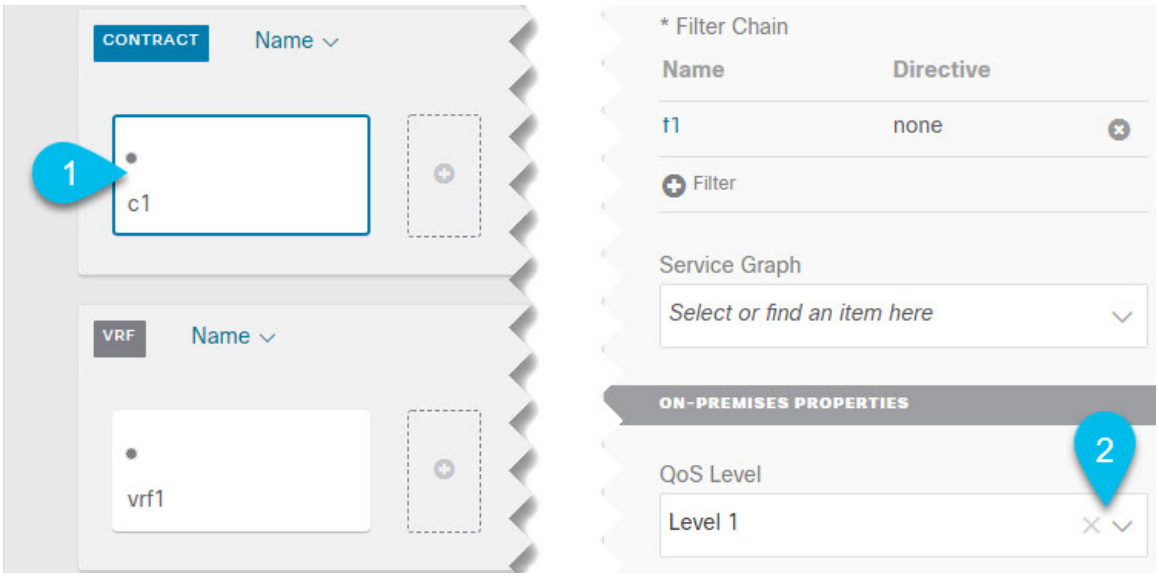
ステップ 3 EPG の QoS レベルの選択



a) メインペインで、**[EPG]** エリアまでスクロールダウンして EPG を選択するか、**[EPG の追加 (Add EPG)]** をクリックして新しい EPG を作成します。

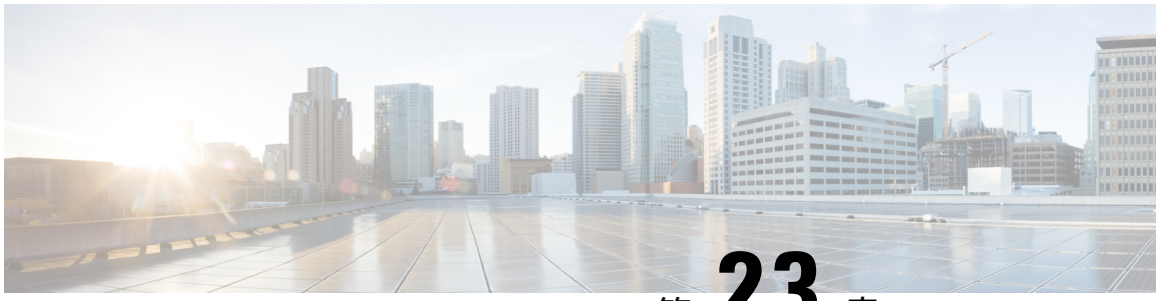
b) 右側のサイドバーで **[QoS レベル (QoS Level)]** ドロップダウンまでスクロールし、EPG に割り当てる QoS レベルを選択します。

ステップ 4 EPG の QoS レベルの選択



a) メインペインで、**[コントラクト (Contract)]** 領域までスクロールダウンしてコントラクトを選択するか、**[+]** アイコンをクリックして新しいコントラクトを作成します。

b) 右側のサイドバーで、**[QoS レベル (QoS Level)]** ドロップダウンまでスクロールし、コントラクトに割り当てる QoS レベルを選択します。



第 23 章

SD-Access と ACI 統合

Cisco SD-Access と Cisco ACI の統合

（注） Cisco Nexus Dashboard と Cisco DNAC の統合により、Nexus とキャンパス SD Accessファブリックの展開全体で、ネットワーク接続のサブセットとマクロセグメンテーション シナリオの自動化が可能になります。この統合は、限られた可用性の下にあります。詳細についてはシスコの担当者にお問い合わせください。

Cisco Software-Defined Access（SD Access または SDA）は、Cisco Digital Network Architecture（DNA）内のソリューションであり、Cisco のインテントベース ネットワーク（IBN）フレームワークを実装するキャンパスおよびブランチ アーキテクチャを定義します。Cisco SD-Access は、セキュリティ、自動化、およびアシュアランスによってビジネスニーズを満たす、統一されたポリシー ベースの有線およびワイヤレスネットワーク ファブリックを定義します。Cisco Identity Services Engine（ISE）と組み合わせた、Cisco Digital Network Architecture Controller（DNAC）は、Cisco SD-Access ファブリックの自動化と管理の統合ポイントです。

Cisco Nexus Dashboard Orchestrator（NDO）のリリース 3.7(1) では、Cisco SD-Access および Cisco ACI 統合のサポートが追加されています。SD Access および ACI 統合の目的は、キャンパスおよびブランチ ネットワークをデータセンター ネットワークにセキュアに接続することです。リリース 3.7(1) では、NDO は次の機能を実行できます。

- 両方のドメインからネットワークとリソースの情報を収集する
- ACI 側で VRF-Lite ドメイン間接続を自動的に設定する
- SD Access ボーダーノードに接続されているネクスト ホップ デバイスの構成を提供します。
- クロスドメインの可視性を提供する

マクロセグメンテーション

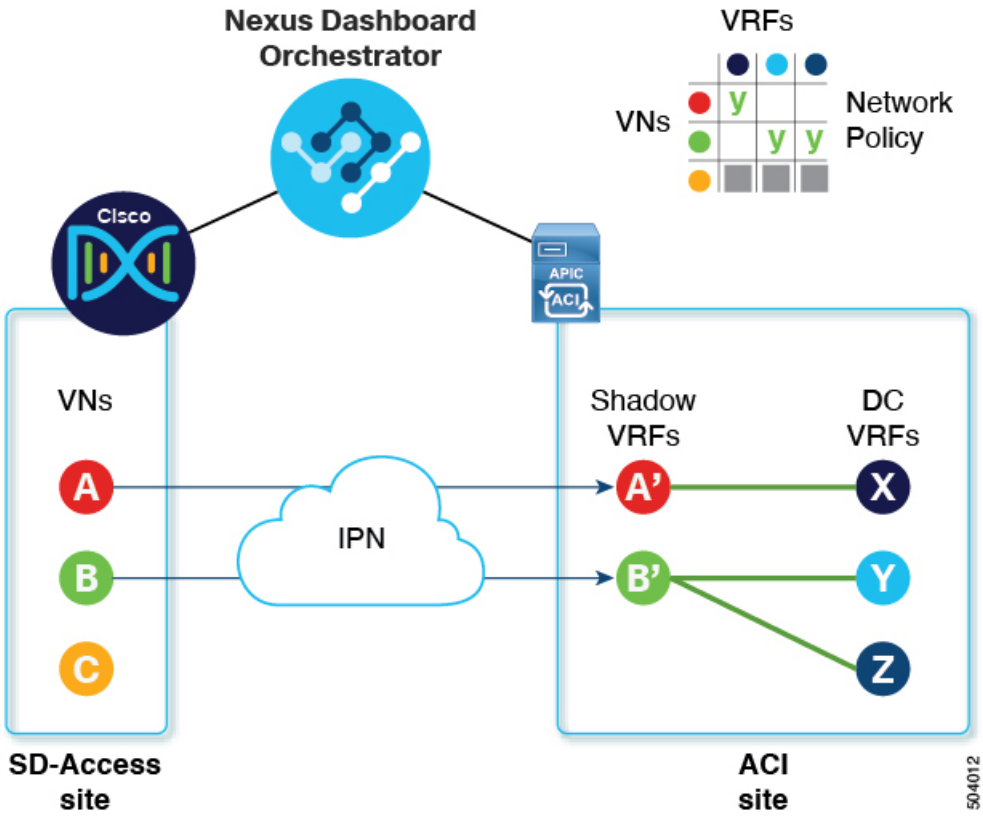
Cisco Nexus Dashboard Orchestrator（NDO）の統合機能により、ACI ドメインとドメイン間のネットワーク要素のマクロセグメンテーションが可能になります。Cisco SD-AccessCisco ACISD Access

ACI ドメインでは、EPG、サブネット、VLAN などのエンティティは、仮想ルーティングおよび転送インスタンス（VRF）の一部としてグループ化されます。VRF が外部通信を必要とする場合、VRF は ACI ボーダー リーフ（BL）の IP インターフェイス（L3Out）に関連付けられます。ドメインでは、ユーザー、サブネット、IP プールなどのエンティティを仮想ネットワーク（VN）としてグループ化できます。SD AccessVN が外部通信を必要とする場合、VN は IP ハンドオフのためにボーダーノード（BN）インターフェイスに関連付けられます。SD Access2 つのドメイン、ACI のボーダー インターフェイスは、IP ネットワーク（IPN）を介して物理的に接続できますが、この基本的な接続は VRF と VN 間の接続を提供しません。SD AccessCisco Nexus Dashboard Orchestrator Cisco SD-Access および Cisco ACI インテグレーションにより、管理者は、VRF を VN にマッピング（または「ステッチ」）するポリシーを作成できます。

マクロセグメンテーション ワークフロー

一般的なCisco SD-Access および Cisco ACI インテグレーション ワークフローは、次の図を参照する次の手順で構成されます。

図 *23 : SD-Access-to-ACI* 統合のための *NDO* を使用したマクロセグメンテーション



- 既存の SD Access サイトでは、Cisco Digital Network Architecture Controller（DNAC）管理者がキャンパス ファブリックを構成しており、一部のエンティティはデータセンターへのアクセスなどの外部アクセスを必要とします。DNAC 管理者は、次のタスクを実行します。
  - 作成済みの仮想ネットワーク（VN）
  - それらの VN に関連付けられた IP アドレスプール
  - 構成された L3 ボーダーノードおよび関連するインターフェイス
  - 作成済み IP（レイヤ 3）ハンドオフ トランジットネットワーク
  - 外部接続を必要とする VN 用に設定されたレイヤ 3 ハンドオフ

  これらのタスクは通常の DNAC 管理タスクであり、インテグレーションのために特別な変更は行われていないことに注意してください。Cisco SD-AccessCisco ACI

- NDO オペレーターは、DNAC ログイン情報を使用して、DNAC にログインして導入準備します。

  オンボーディング プロセスでは、NDO は自動的に DNAC の REST API にアクセスして、サイト、VN、およびボーダーノード デバイスをクエリします。これらのエンティティを検出すると、NDO はどの VN が外部接続（L3 ハンドオフ）用に構成され、どのボーダー

ノードであるかを学習し、それらのサブネットを学習します。Cisco SD-Access図 23 : SD-Access-to-ACI 統合のための NDO を使用したマクロセグメンテーション （305 ページ）に示す例では、VN A と B は L3 ハンドオフ用に設定されており、これらの VN は ACI サイトに拡張するために使用できます。VN C は L3 ハンドオフ用に構成されておらず、ACI サイトで使用できません。

NDO は、SD Access ファブリック内の進行中の構成変更について DNAC に定期的にクエリを実行し続けます。

- NDO オペレーターは、1 つ以上の ACI サイトと 1 つ以上の SD Access サイト間の接続を構成します。これには、ACI サイトのボーダー リーフスイッチとインターフェイス、およびボーダー リーフ インターフェイスでの VRF-Lite 構成に使用される VLAN と IP プールの指定が含まれます。直接接続されたインターフェイス（IPN なし）の場合、VRF-Lite 構成は、SDA ボーダーノードでの IP ハンドオフのために DNAC によってプロビジョニングされた構成から取得され、VLAN と IP アドレスはこれらのプールから取得されません。

  NDO は、拡張 SD Access VN のネクストホップ デバイス構成を生成して表示します。この構成は、必要に応じて IPN デバイスに手動で適用できます。NDO は IPN デバイスをプロビジョニングしません。

- NDO オペレーターは VN をデータセンターに拡張し、VN を ACI ドメイン内の VRF に接続できるようにします。

  VN を拡張すると、ACI ドメイン上の VN を表す VN の内部表現（ミラーリングされた「シャドウ VRF」）が作成されます。図 1 の例では、シャドウ VRF A' と B' が ACI サイトに自動的に作成され、拡張 SD Access VN A と B を表します。これらのシャドウ VRF は、SD Access ドメインとの接続を必要とする ACI ドメイン内のすべてのサイトとポッドに拡張されます。NDO は、これらのシャドウ VRF が構成されているスキーマとテンプレートを自動的に作成します。自動作成されたスキーマとテンプレートは NDO に表示されますが、読み取り専用です。テンプレートは「共通」テナントに関連付けられており、「SDA 接続」が有効なすべてのサイトに関連付けられています。

- NDO オペレーターは、拡張 SD Access VN をデータセンター VRF または VN がアクセスする必要のある VRF にマッピングするネットワーク ポリシーを作成します。このアクションは、「VRF スティッチング」とも呼ばれます。データセンターの VRF は、さまざまな「アプリ テナント」の一部にすることができます。これは、設計によるこの統合により、VRF 間接続（通常は「共有サービス」と呼ばれる機能）を確立できることを意味します。

  図 1 の例では、示されているネットワーク ポリシーは、拡張 SD Access VN A（VRF A' として拡張）をデータセンター VRF X に、VN B（VRF B' として拡張）をデータセンター VRF Y および Z にステッチしています。

  このマッピングの結果として、すべてのトラフィックを許可するセキュリティポリシー関係が、拡張 SD Access VN に関連付けられた L3Out の外部 EPG とデータセンター VRF を表す vzAny 論理オブジェクトとの間に自動的に確立されます。この契約の適用により、拡張 SD Access VN のすべてのサブネットと、VRF 間で漏洩するように明示的に構成されたデータセンター VRF のすべてのサブネットとの間で無料の接続が可能になります。

Cisco SD-Access およびCisco ACI インテグレーション ガイドライン

- ACI サイトと SD Access サイトは、外部 IP ネットワーク（IPN）を介して間接的に接続することも、ACI ボーダー リーフから SD Access ボーダーノードへのバックツーバック接続で直接接続することもできます。
  - サイトが直接接続されている場合、2 つのドメイン間の接続は、コントロールプレーンとデータプレーンの両方を含め、自動的に構成されます。
  - サイトが IPN を使用して接続されている場合、IPN デバイスは VRF Lite をサポートする必要があります。NDO および DNAC は IPN デバイスをプロビジョニングしませんが、NDO は、ACI ボーダー リーフおよび SD Access ボーダーノードに直接接続されている IPN デバイスに適用できるサンプル構成を提供します。
- いずれかのドメインに複数のサイトが存在する場合は、次のガイドラインに注意してください。
  - SD Access サイトは別の SD Access サイト（SDA トランジット）を使用して ACI サイトに接続できます。
  - SD Access（キャンパス）ドメインに複数のサイトが存在する場合、各キャンパス サイトはデータセンター ドメインに直接接続するか（ダイレクト ピアリング）、汎用 IP ネットワーク（IPN）などの中間ネットワークを介して、または別のキャンパス サイトを介して（間接ピアリング）接続できます。
  - マルチサイト展開では、SD Access（キャンパス）ドメインとの直接または間接接続を必要とする各 ACI ファブリックは、ローカル L3Out 接続を展開する必要があります。ACI ファブリックがマルチポッドファブリックの場合、L3Out 接続は、同じファブリックの一部であるポッドまたはポッドのサブセットにのみ展開できます。
- SD Access と ACI 統合の拡張性 （308 ページ） で説明されている制限内で、VN から VRF への M:N マッピングがサポートされています。
- で説明されている制限内で、サイトから ACI サイトへの M:N マッピングがサポートされています。SD AccessSD Access と ACI 統合の拡張性 （308 ページ）
- DNAC から、NDO はすべての SD Access（キャンパス）VN とそのサブネットについて学習します。VN が ACI サイトに拡張されると、NDO は、その拡張された VN のすべてのサブネットが ACI 境界リーフから到達可能であると想定します。NDO は、ACI ボーダー リーフにこれらのサブネットが存在するかどうかを定期的に確認します。拡張 VN の [インテグレーション（Integrations）] > [DNAC] > [仮想ネットワーク（Virtual Networks）] テーブルの [ステータス（Status）] 列で、NDO はまだ到達できないサブネットを報告します。

- デフォルトでは、拡張 VN が DC VRF にマッピングされている場合、ACI サイトは通過ルートを VN にアドバタイズしません。NDO 管理者は、どの ACI サブネットが VN のシャドウ VRF にリークされるかを次のように制御します。
  - ACI VRF の内部にある BD サブネットは、サブネットが「VRF 間で共有」で設定されている場合にのみリークされます。

（注） SD Access VN が複数の ACI VRF にマッピングされている場合、マッピングされたすべての ACI VRF で重複しないプレフィックスのみを「VRF 間で共有」として設定する必要があります。

  - ACI VRF で設定された L3Out から学習した外部サブネットは、サブネットが「共有ルート制御」で設定されていて、トランジットルーティングが有効になっている場合にのみリークされます。

詳細については、トランジットルーティングの設定（319ページ）を参照してください。

- SD Access サイトは、ACI サイトへのインターネット接続を提供できません。
- IPv6 接続の自動化はサポートされていません。
- マルチキャスト トラフィックはドメイン間でサポートされていません。

SD Access と ACI 統合の拡張性

- NDO および ACI 統合にオンボーディングできる DNAC は 1 つだけです。SD Access
- 単一の DNAC で管理されている場合、複数の（キャンパス）サイトがサポートされます。SD Access
- ピアリングでは、最大 2 つの ACI サイトがサポートされます。SD Access各 ACI サイトは、単一のポッドファブリックまたはマルチポッドファブリックにすることができます。
- 仮想ネットワーク（VN）は、最大 10 個の ACI VRF にマッピングできます。
- ドメインから最大 32 個の仮想ネットワーク（VN）を ACI ドメインに拡張できます。SD Access

ソフトウェアの互換性

マクロセグメンテーションと ACI 統合をサポートする最小ソフトウェア バージョンを次の表に示します。SD Access

製品	サポート対象の製品バージョン
NDO	3.7 以降のリリース
ACI	4.2 以降のリリース
DNAC	2.3.3 以降のリリース

DNA センターのオンボーディング

このセクションでは、Nexus Dashboard Orchestrator（NDO）を設定して DNA センター（DNAC）にログインする方法について説明します。ログイン後、NDO はドメインと ACI ドメイン間のネットワーク接続を作成するために必要なサイト構成情報をインポートできます。SD AccessSD Access

手順

ステップ 1 NDO にログインします。

ステップ 2 左側のナビゲーション ペインで、[**インテグレーション（Integrations）] > [DNAC**] を選択します。

ステップ 3 メイン ペインで、[DNAC の追加（Add DNAC）] をクリックして DNA センターをオンボードします。

[**DNAC の追加（Add DNAC**）] ダイアログボックスが開きます。

ステップ 4 [**DNAC の追加（Add DNAC**）] ダイアログボックスで、次の手順を実行します。

a) DNA センターの [**名前（Name**）] を入力します。
b) DNA センターの URL または IP アドレスをデバイス IP として入力します。
c) DNA センターにログインするための **[ユーザー名（Usesrname**）] 資格情報を入力します。

読み取り専用アクセスで十分です。

d) DNA センターにログインするための **[パスワード（Password**）] 資格情報を入力します。
e) **[Confirm Password（パスワードの確認）]** に、もう一度パスワードを入力します。
f) **[追加（Add）]** をクリックします。

NDO は、REST API を介して DNAC に自動的にログインし、DNAC によって制御されるドメイン内の仮想ネットワーク（VN）およびボーダーノード デバイスの構成を照会します。SD Access

次のタスク

- ACI サイトからサイトまたは IPN への接続を構成します。SD Access
- DNAC のドメインの VN と ACI ドメインの VRF 間の通信を許可するネットワーク ポリシーを作成します。SD Access

SD Access ドメインへの接続の構成

このセクションでは、ACI 統合のために NDO で実行されるインフラストラクチャ レベルの構成について説明します。Cisco SD-Access ACI ファブリックごとに、ドメインへの接続を提供す

るボーダー リーフ ノードとそれらに関連付けられたインターフェイスを選択する必要があります。Cisco SD-Access

始める前に

DNA センターをオンボーディングしておく必要があります。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション ペインで、[**インテグレーション（Integrations）] > [DNAC**] を選択します。

ステップ 3 メイン ペインで、**[概要（Overview）]** タブをクリックします。

DNA Center のダッシュボードが表示されます。

ステップ 4 [DNAC の詳細（DNAC Details）] ボックスの右側で、[接続の構成（Configuring Connectivity）] のリンクをクリックします。

[ファブリック接続インフラ (Fabric Connectivity Infra)] ページが表示されます。

ステップ 5 左側のナビゲーションペインの [サイト（Sites）] で、接続する ACI サイトを選択します。

[サイト接続（Site Connectivity）] ペインが右側に表示されます。

ステップ 6 [サイト接続（Site Connectivity）] ウィンドウで、[SDA 接続（SDA Connectivity）] コントロールまで下にスクロールし、[有効（Enabled）] に設定します。

[SDA 接続（SDA Connectivity）] コントロールの下にいくつかのフィールドが表示されます。以下のサブステップで設定を構成します。

a) **[外部ルーテッド ドメイン（External Routed Domain）]** ドロップダウン リストから、接続する外部ルーテッド ドメイン（L3 ドメイン）を選択します。

このルーテッド ドメインは、APIC ですでに定義されている必要があります。

b) **[VLAN プール（VLAN Pool）]** フィールドに、VLAN の番号の範囲を入力します。

このプールの VLAN 番号は、キャンパス VN をデータセンターに拡張するときに、サブインターフェイスまたは SVI に割り当てられます。VLAN プールは、前の手順で選択した外部ルーテッド ドメインに関連付けられた VLAN プールと同じか、そのサブセットである必要があります。

ACI から SD Access への接続がバックツーバックで、IPN がない場合、VLAN ID はこのプールから割り当てられません。代わりに、VLAN ID は、SD Access ボーダーノードでの IP ハンドオフのために DNAC によってプロビジョニングされたものによって決定されます。

c) [VRF Lite IP プール範囲（VRF Lite IP Pool Ranges）] で、[VRF Lite IP プール範囲を追加（Add VRF Lite IP Pool Range）] の横にある [+] 記号をクリックし、[IP アドレス（IP Address）] フィールドに IP サブネットを入力します。

このサブネットの IP アドレスは、キャンパス VN をデータセンターに拡張するときに、サブインターフェイスまたは SVI に割り当てられます。

ACI から SD Access への接続がバックツーバックで、IPN がない場合、これらのプールは使用されません。この場合、サブインターフェイスの IP アドレスは、SD Access ボーダーノードでの IP ハンドオフのために DNAC によってプロビジョニングされたものによって決定されます。

ステップ 7 ACI サイトのポッドが表示されている中央のペインで、サイトに接続するポッドの下にある [リーフ ノードの追加（Add Leaf Node）] をクリックします。SD Access

[リーフの選択（Select a Leaf）] ペインが右側に表示されます。以下のサブステップで設定を構成します。

a) [リーフの選択（Select a Leaf）] ペインの [リーフノード（Leaf Node）] ドロップダウン リストから、ドメインに接続するボーダーリーフスイッチを選択します。SD Access
b) **[ルータ ID（Router ID）]** フィールドに、ボーダーリーフ ルータ ID を入力します。
c) [インターフェース（Interfaces）] で、[インターフェースの追加（Add Interface）] の横にある [+] 記号をクリックします。

[Add Interface] ダイアログボックスが表示されます。

d) **[インターフェイス ID（Interface ID）]** を入力します。
e) [インターフェイス タイプ（Interface Type）] ドロップダウンリストから [サブインターフェイス（Sub-Interface）] または [SVI] を選択します。
f) **[リモート自律システム番号（Remote Autonomous System Number）]** を入力します。

ACI から SD Access への接続が IPN を使用する場合、この番号は IPN の ASN と一致する必要があります。

ACI から SD Access への接続が IPN なしでバックツーバックである場合、この番号は SD Access ボーダーノードの ASN と一致する必要があります。

g) [保存（Save）] をクリックします。

ステップ 8 [ファブリック接続インフラ（Fabric Connectivity Infra）] ページの上部のバーで、[展開（Deploy）] をクリックします。

この時点では、構成はまだ APIC にプッシュされていません。最初の VN が拡張されると、SD Access 接続が自動的に構成されます。

ACI 統合への SD Access のステータスの表示

[インテグレーション（Integrations）]>[DNAC] メニューには、統合ステータスに関する詳細が表示され、使用可能な仮想ネットワーク（VN）のインベントリが提供されます。

[概要（Overview）] タブ

[概要（Overview）] タブは、次の情報ウィンドウを表示します。

- [DNAC 詳細（DNAC Details）]：接続されている DNAC の全体的なステータス、IP アドレス、およびバージョンを表示します。このウィンドウには、[接続の構成（Configure Connectivity）] へのリンクも含まれています。

- 次のリソースの概要グラフィック ダッシュボード：
  - [DNAC 可能なサイト（DNAC Enabled Sites）]：DNAC によって管理されているサイトの数とタイプ。SD Accessサポートされているサイト タイプは、オンプレミス、AWS、および NDFC です。
  - [仮想ネットワーク（Virtual Networks）]：使用可能な VN の数、および拡張または拡張されていない数。
  - [DC VRF]：共有に使用できるデータセンター VRF の数、およびそれらがマッピングされているかどうか。

[仮想ネットワーク（Virtual Networks）] タブ

[仮想ネットワーク（Virtual Networks）] タブをクリックして、VN に関する詳細を表示します。

ページの上部のウィンドウには、[概要（Overview）] タブからの概要グラフィック情報が繰り返されます。

このページの [仮想ネットワーク（Virtual Networks）] ウィンドウには、ボーダー ノードでの IP ハンドオフ用に DNAC によって構成された仮想ネットワーク（VN）が一覧表示されます。SD AccessVN のテーブルには、VN ごとに次の情報が表示されます。

- [ステータス（Status）]：VN の現在の統合ステータスと、ステータスの重大度を示す色分けされたアイコン。状態を次の表に示します。

ステータス	アイコンの色（重大度）	説明
検出済	緑色（正常）	VN は SDA ボーダー ノードで検出されます。
処理中	グレー （情報）	構成変更後の VN の最新ステータスを読み取ります。これは一時的な状態です。 **ヒント** ページの右上隅にある [更新] アイコンをクリックして、ステータスの即時ポーリングを強制することができます。
成功	緑色（正常）	VN は正常に拡張されました。
[BGPSessionIssues]	黄色（警告）	すべてのインターフェイスで BGP セッションが確立されているわけではありません。詳細については、各 DC ボーダー リーフの状態を確認してください。
[RouteLeakPartial]	黄色（警告）	VN サブネットは、DC ボーダー リーフ ノードに部分的に伝達されます。詳細については、各 DC ボーダー リーフの状態を確認してください。

ステータス	アイコンの色（重大度）	説明
[RouteLeakNone]	赤（失敗）	VN サブネットはまだ DC ボーダー リーフ ノードに伝達されていません。VN テーブルで [DC サイト（DC Sites）] をクリックして、DC ボーダー リーフ インターフェイスに問題がないか確認します。
[MappedVRFConfigFailure]	赤（失敗）	マッピングされた VRF で設定が失敗しました。マッピングを再試行します。
[DCSiteConfigFailure]	赤（失敗）	DC サイトで VN 拡張が失敗しました。VN の拡張を解除して、再度拡張します。

VN のステータス アイコンをクリックして、警告やエラーのトラブルシューティングに役立つ追加の詳細を含むサイドバーを表示します。

- [名前（Name）]：DNAC 管理者によって VN に割り当てられた名前。
- [拡張済み（Extended）]：VN が拡張されているかどうかを示します。
- [DC マップ済みの VRF（DC Mapped VRFs）]：VN がマップされるデータセンター VRF の数。この番号をクリックしてサイドバーを開き、マッピングされたデータセンター VRF の関連スキーマ、テンプレート、およびテナントを表示します。
- [DC サイト（DC Site）]：VN がマップされているデータセンター サイトの数。この番号をクリックしてサイドバーを開き、ボーダー リーフ インターフェイス、BGP ピアリング ステータス、ネクストホップ デバイス情報など、データセンター サイトの詳細を表示します。

ヒント　IPN 接続のボーダー リーフ インターフェイスの場合、サイドバーの [ピア デバイスの構成（Peer Device Configuration）] で、[詳細の表示（Show Details）] をクリックして、このサイトに接続されている IPN デバイスの構成例を表示します。

- [キャンパス サイト（Campus Sites）]：この VN に関連付けられているキャンパス サイトの数。この番号をクリックしてサイドバーを開き、ボーダー ノード インターフェイス、BGP ピアリング ステータス、ネクストホップ デバイス情報など、キャンパス サイトの詳細を表示します。

ヒント　IPN 接続のボーダー ノード インターフェイスの場合、サイドバーの [ピア デバイスの構成（Peer Device Configuration）] で、[詳細の表示（Show Details）] をクリックして、このサイトに接続されている IPN デバイスの構成例を表示します。

- […（アクション アイコン）（… (actions icon)）]：アイコンをクリックして、この VN のアクションにアクセスします。

  使用可能なアクションは、VN の現在のステータスによって異なりますが、次のものが含まれる場合があります。

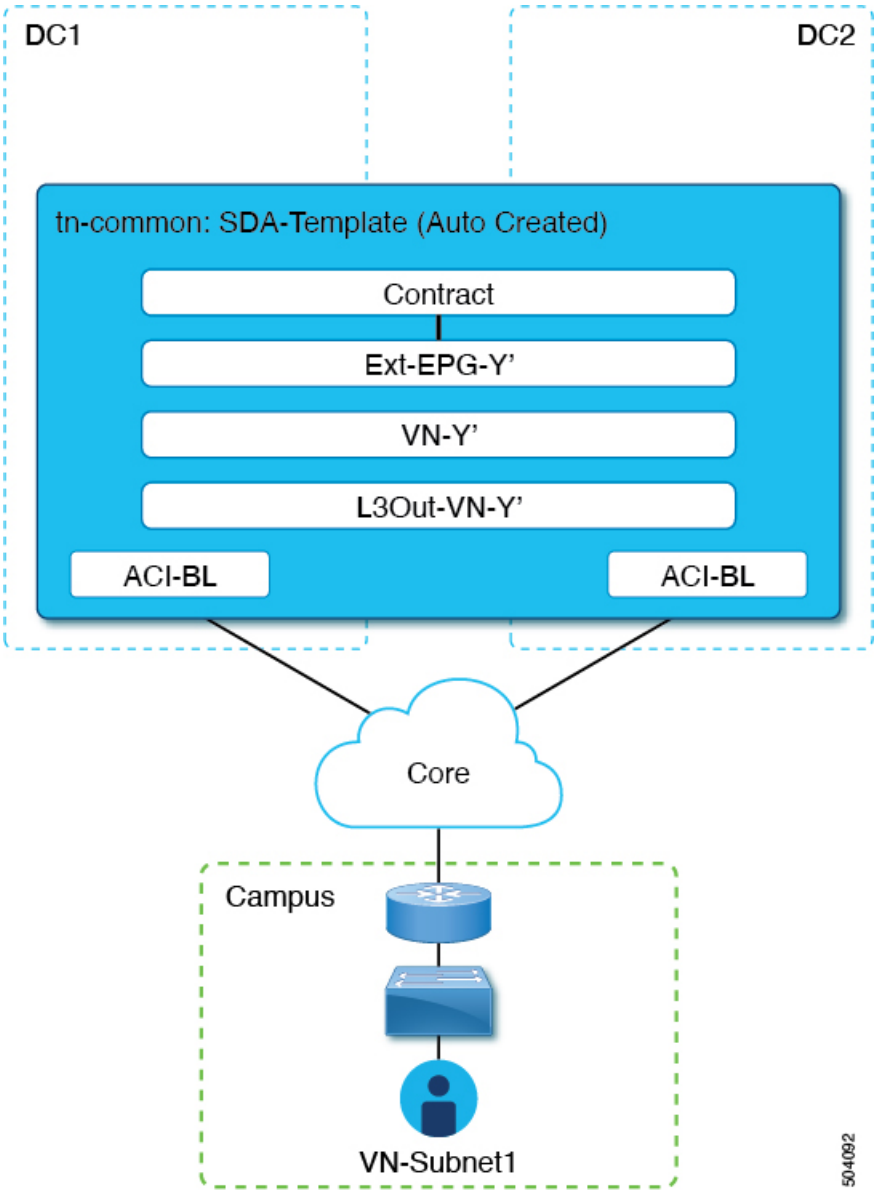
  - VN の拡張 / 拡張解除
  - DC VRF のマッピング / マッピング解除
  - トランジット ルートの有効化 / 無効化

キャンパス VN をデータセンター VRF にマッピングすると、[仮想ネットワーク（Virtual Networks）] ページの [関連付けテンプレート（Associated Templates）] ウィンドウが表示されます。

仮想ネットワークの拡張

このセクションでは、SD Access（キャンパス）VN を ACI（データセンター）ファブリックに拡張する方法について説明します。このアクションにより、DC 側のキャンパス VN のミラーリングされたイメージを表す VRF（および 図 24 : VN の拡張 （315 ページ） に示す他の関連する設定オブジェクト）が作成されます。作成されたオブジェクトは、「共通」テナントに関連付けられた自動生成テンプレートで定義されます。

図 *24 : VN* の拡張



始める前に

- DNA センター（DNAC）をオンボーディングしておく必要があります。
- ACI サイト レベルでドメインへの接続を構成しておく必要があります。SD Access

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション ペインで、[**インテグレーション（Integrations）] > [DNAC**] を選択します。

ステップ 3 メイン ペインで、**[仮想ネットワーク（Virtual Networks）]** タブをクリックします。

仮想ネットワーク（VN）のテーブルが表示され、ボーダーノードでの IP ハンドオフ用に DNAC によって構成されたすべての VN が表示されます。SD Access

ステップ 4 拡張する VN の行で、アクション メニュー（**[...]**）をクリックし、**[拡張（Extend）]** を選択します。

ダイアログ ボックスが開き、VN が拡張される ACI サイトとインターフェイスが表示されます。この情報は、SD Access ドメインへの接続の構成 （309 ページ）の構成設定を反映しています。

VN の拡張を後で取り消す場合は、アクション メニュー（**[...]**）をクリックし、[拡張解除（Unextend）] を選択します。

ステップ 5 ダイアログボックスで、**[はい（Yes）]** をクリックします。

VN は、接続が有効になっているすべての ACI サイトに拡張されますが、まだどの ACI VRF にもマッピングされていません。SD Access

ステップ 6

次のタスク

ACI ボーダー リーフ インターフェイスの BGP ピアリング ステータスを確認します。

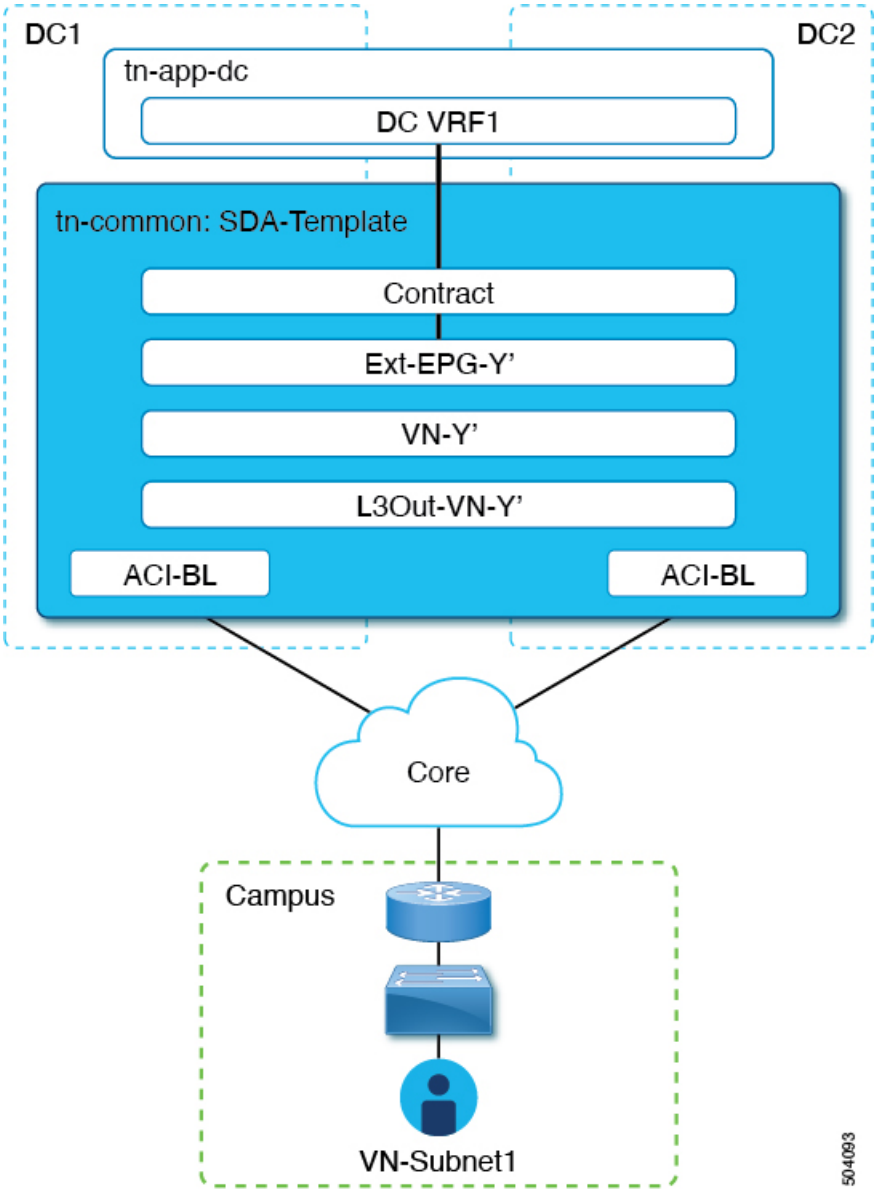
- ボーダーノードと ACI ボーダー リーフが直接（バックツーバック）接続されている場合は、キャンパス VN を拡張した結果として、これらのデバイス間で BGP セッションが確立されていることを確認します。SD Access[統合（Integrations）] > [DNAC] > [仮想ネットワーク（Virtual Networks）] で、[DC サイト（DC Sites）] 番号をクリックしてサイドバーを開き、ACI ボーダー リーフ インターフェイスの詳細を表示します。ボーダー リーフ インターフェイスの BGP Peering Status が「Up」を示していることを確認します。
- IPN がドメイン間に展開されている場合は、構成サンプルを取得して、ボーダーノードおよび ACI ボーダー リーフに直接接続されているネクストホップ デバイスの構成を支援します。SD Access[統合（Integrations）] > [DNAC] > [仮想ネットワーク（Virtual Networks）] で、[DC サイト（DC Sites）] 番号をクリックしてサイドバーを開き、ACI ボーダー リーフ インターフェイスの詳細を表示します。IPN 接続された境界リーフ インターフェイスの場合は、[ピアリング デバイス構成] の横にある [詳細を表示] リンクをクリックして、サンプルの IPN デバイス構成を表示します。IPN デバイスを設定したら、境界リーフ インターフェイスの BGP ピアリング ステータスが「Up」を示していることを確認します。

VN の VRF へのマッピングまたはマッピング解除 （317 ページ） で説明されているように、拡張 VN を 1 つ以上の ACI VRF にマッピングします。

VN の VRF へのマッピングまたはマッピング解除

このセクションでは、仮想ネットワーク（VN）を ACI ファブリック内の 1 つ以上のデータセンター（DC）VRF にマッピング（「ステッチ」）する方法について説明します。図 25 : VRF へのマッピング（317ページ）に示すように、VRF へのマッピングにより、DC VRF（「vzAny」オブジェクトによって表される）と「共通」テナントで以前にプロビジョニングされた外部 EPG との間の契約関係が確立されます。

図 *25 : VRF* へのマッピング



始める前に

VN を ACI サイトに拡張しておく必要があります。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション ペインで、**[インテグレーション（Integrations）] > [DNAC]** を選択します。

ステップ 3 メイン ペインで、**[仮想ネットワーク（Virtual Networks）]** タブをクリックします。

仮想ネットワーク（VN）のテーブルが表示され、ボーダーノードでの IP ハンドオフ用に DNAC によって構成されたすべての VN が表示されます。SD Access

ステップ 4 マッピングする VN の行で、アクション メニュー（[...]）をクリックし、[DC VRF のマッピング / マッピング解除（Map/Un-Map DC VRFs）] を選択します。

[DC VRF のマップ/マップ解除（Map/Un-Map DC VRFs）] ダイアログ ボックスが開きます。

ステップ 5 [DC VRF のマップ / マップ解除（Map/Un-Map DC VRFs）] ダイアログボックスで、[DC VRF のマップの追加（Add Mapped DC VRF）] の横にある [+] アイコンをクリックします。

ステップ 6 VRF のドロップダウンリストから VRF を選択します。

選択した VRF がテーブルに追加され、VRF のテンプレートも表示されます。後の手順で必要になるため、テンプレート名を書き留めておいてください。

VN を追加の VRF にマッピングする場合は、[+] アイコンを再度クリックして、ドロップダウンリストから追加の VRF を選択します。

既存のマッピングを削除して、DC VRF のマッピングを解除することもできます。DC VRF のマッピングを解除するには、VRF の行にあるごみ箱アイコンをクリックします。

ステップ 7 [保存（Save）] をクリックし、VN ステータスが「成功」に変わるまで待ちます。

（注）
この時点で、VN ステータスが「成功」を示していても、拡張 VN と DC VRF 間のデータ接続はまだ確立されていません。マッピング操作により、マッピングされた VRF に関連付けられたテンプレートが変更されました。接続が確立される前に、テンプレートを再展開する必要があります。VN テーブルの下の [関連付けられたテンプレート（Associated Templates）] テーブルに、マッピングされた VRF に関連付けられたテンプレートが表示されます。

ステップ 8 [インテグレーション（Integrations）] > [DNAC] > [仮想ネットワーク（Virtual Networks）] タブの [関連付けられたテンプレート（Associated Templates）] テーブルで、マッピングされた VRF に関連付けられたテンプレートのリンクをクリックします。

スキーマとテンプレート ページが開きます。

ステップ 9 スキーマとテンプレートのページで、[サイトに配置（Deploy to sites）] をクリックします。

ステップ 10 テンプレートのレビューと承認（変更管理）が有効になっている場合は、変更管理ワークフローに従ってテンプレートを再展開します。それ以外の場合、**[展開（Deploy）]** をクリックして、テンプレートを再展開します。

次のタスク

（注） DC VRF のマッピングを解除した場合、[関連付けられたテンプレート（Associated Templates）] テーブルにテンプレートは表示されません。ただし、[アプリケーション管理（Application Management）]>[スキーマ（Schemas）] に移動して、関連付けられたテンプレートを再展開して、vzAny 構成を削除する必要があります。それ以外の場合、データ プレーン通信は有効のままです。

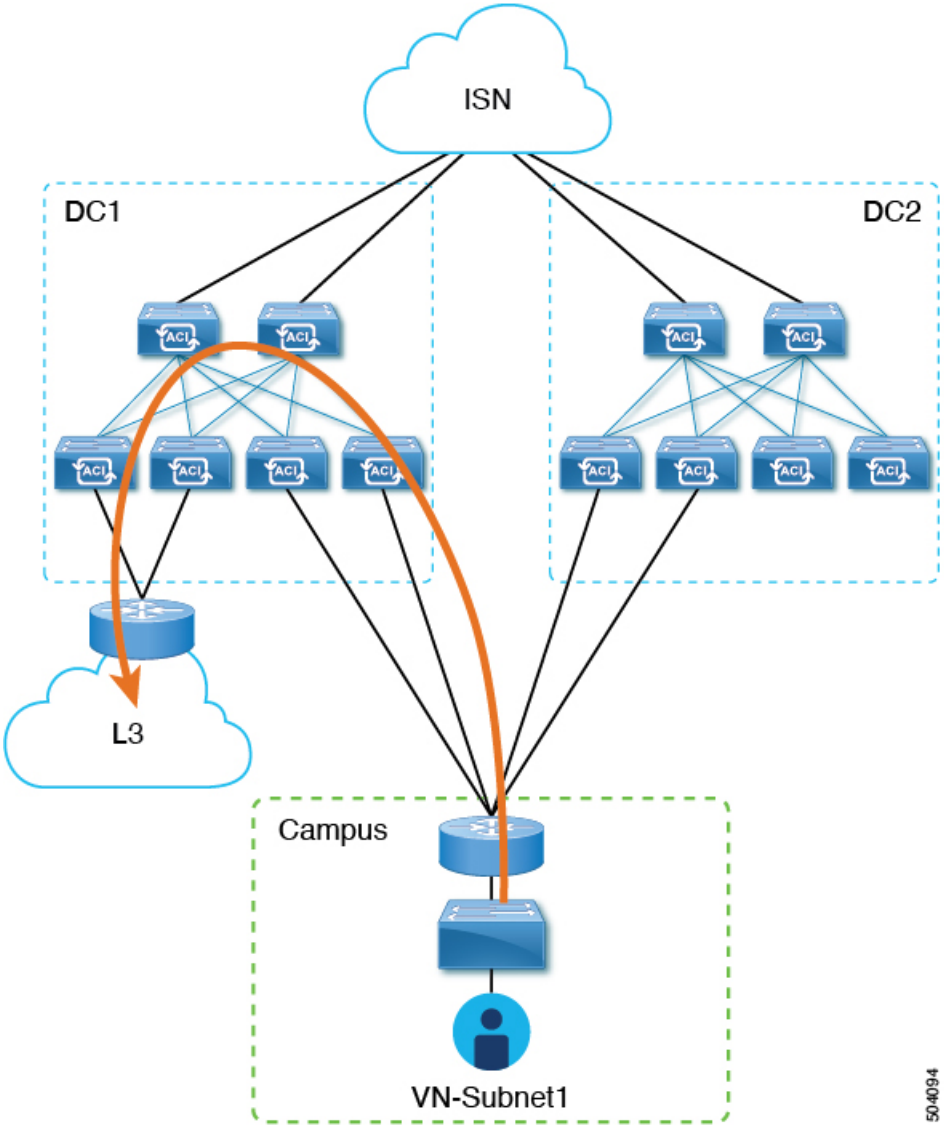
トランジット ルーティングの設定

拡張（キャンパス）VN が ACI（データセンター）VRF にマッピングされると、「外部でアドバタイズされる」フラグと「VRF 間で共有される」フラグが設定されている DC VRF の BD サブネットは、「共通」テナント VRF にリークされ、その後ドメインに向けてアドバタイズされます。SD AccessSD Accessこれにより、キャンパス ユーザーは DC VRF でプロビジョニングされたアプリケーションにアクセスできるようになります。

（注） SD Access VN が複数の ACI VRF にマップされた場合、すべてのマッピング済み ACI VRF のうち非オーバーラッピング プレフィクスのみ、「VRF 間で共有」として構成される必要があります。

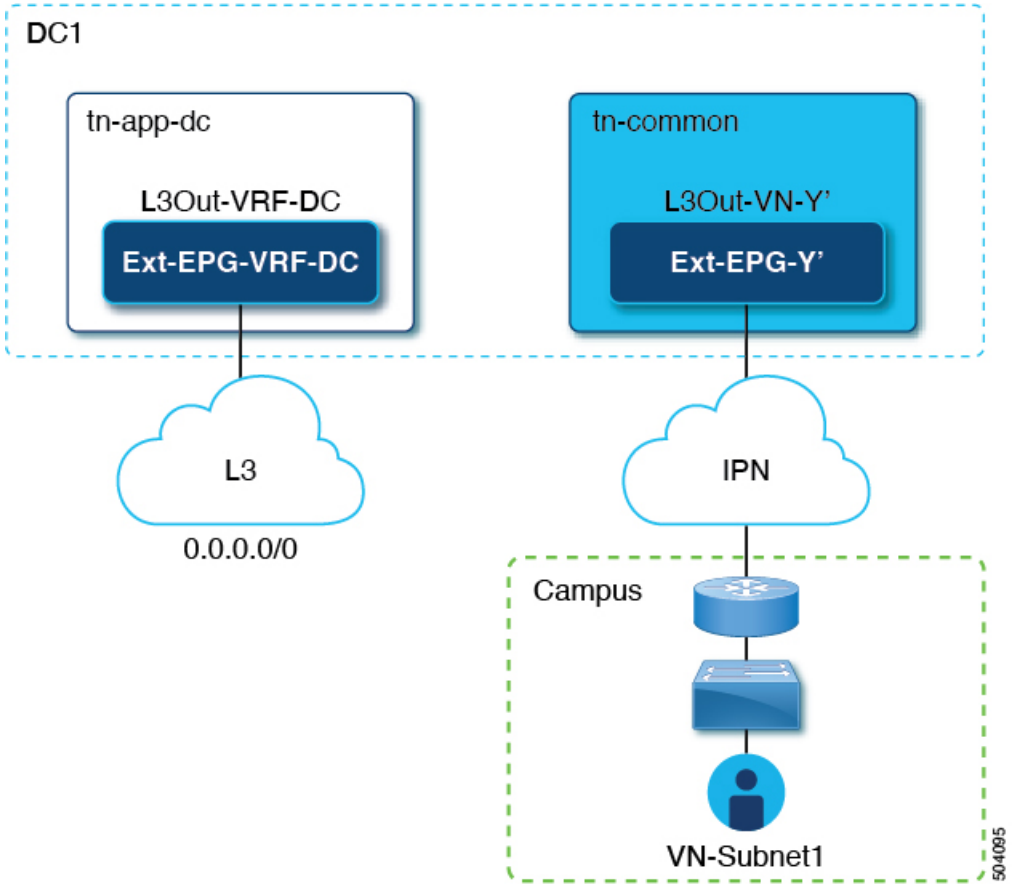
これらの BD サブネットのアドバタイズに加えて、キャンパス ユーザーが ACI ドメインをトランジットとして使用して外部 L3 ネットワーク ドメインにアクセスする必要がある場合があります（図 26 : トランジットとしての ACI ドメイン （320 ページ））。

図 *26 :* トランジットとしての *ACI* ドメイン



このシナリオでは、DC VRF（L3Out-DC-VRF）に関連付けられた L3Out 接続は、通常、外部ドメインへの接続を許可するためにプロビジョニングされ、外部ルート（図 27 : L3Out 接続（321 ページ） の例では単純な 0.0.0.0/0 デフォルト）が DC VRF ルーティング テーブル（tn-app-dc の一部）にインポートされます。

図 *27 : L3Out* 接続



キャンパス ユーザーがデータセンター経由で外部 L3 ドメインに接続できるようにするには、外部ルートを tn-common VRF にリークして、DC へのキャンパス VN 拡張の結果として自動生成された L3Out 接続（L3Out-VN-Y'）を介してキャンパス ドメインに向けてアドバタイズできるようにする必要があります。

外部ルートのリークを有効にするには、次の手順に従います。

始める前に

拡張キャンパス VN をデータセンター VRF にマッピングし、接続を確立しておく必要があります。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

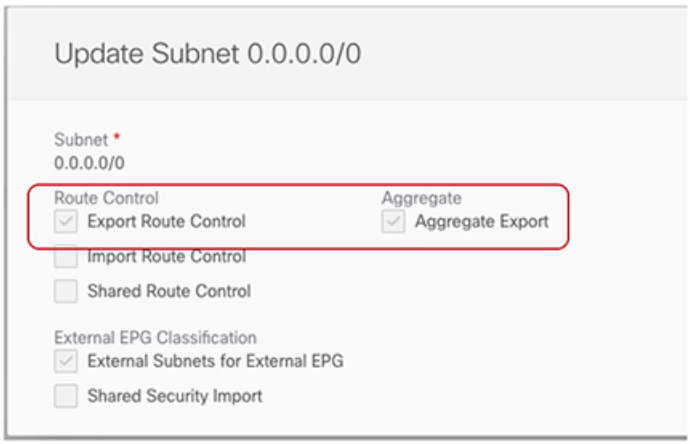
ステップ 2 左側のナビゲーション ペインで、**[インテグレーション（Integrations）] > [DNAC]** を選択します。

ステップ 3 メイン ペインで、**[仮想ネットワーク（Virtual Networks）]** タブをクリックします。

ステップ 4 正常にマッピングされたキャンパス VN の行で、アクション メニュー（[...]）をクリックし、[トランジット ルートを有効にする（Enable Transit Route）] を選択します。

この構成（図 28 : エクスポート ルート制御 （322 ページ））は、Ext-EPG-Y' の下に 0.0.0.0/0 プレフィックスを作成し、次の「ルート制御」フラグを設定して、tn-app-dc テナントからリークされたすべての外部ルートの IPN へのアドバタイジングを許可します。

図 *28 :* エクスポート ルート制御



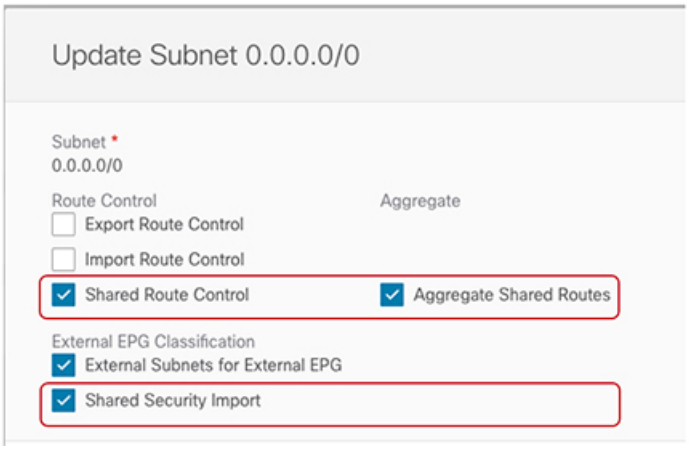
トランジット ルーティングを無効にするには、アクション メニュー（[...]）をクリックし、[トランジット ルートを無効にする（Disable Transit Route）] を選択します。

（注）
いずれかの設定（有効または無効）で、キャンパス サイトは ACI VRF 内部の共有 BD サブネットにアクセスできます。

ステップ 5 左側のナビゲーション ペインから、[アプリケーション管理（Application Management）] > [スキーマ（Schemas）] を選択し、データセンター テナント アプリケーションを構成するためのテンプレートに移動します。

ステップ 6 データセンター テナント アプリケーション テンプレートで、DC VRF の Ext-EPG-VRF-DC に関連付けられた 0.0.0.0/0 プレフィックスの下にフラグを設定して、インターネットから学習した外部ルートを tn-common にリークできるようにします（図 29 : 共有ルート コントロール （323 ページ））。

図 29 : 共有ルート コントロール

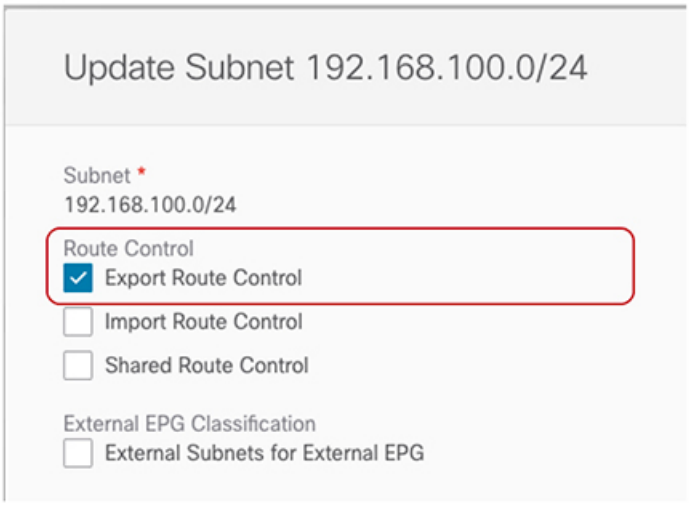


（注）
示されている設定により、L3Out-VRF-DC で受信されたすべての外部プレフィックスが tm-common にリークされるため、キャンパス ドメインに向けてアドバタイズされます。この設定により、L3 ドメインから受信した場合、0.0.0.0/0 デフォルト ルートのリークも許可されます。必要に応じて、外部プレフィックスのサブセットのみを tn-common にリークできる、より詳細な構成を適用できます。これは、プレフィックスのこれらのサブセットに一致する特定のエントリを作成し、それらのエントリに「ここに」示されているのと同じフラグ構成を適用することによって実現されます。

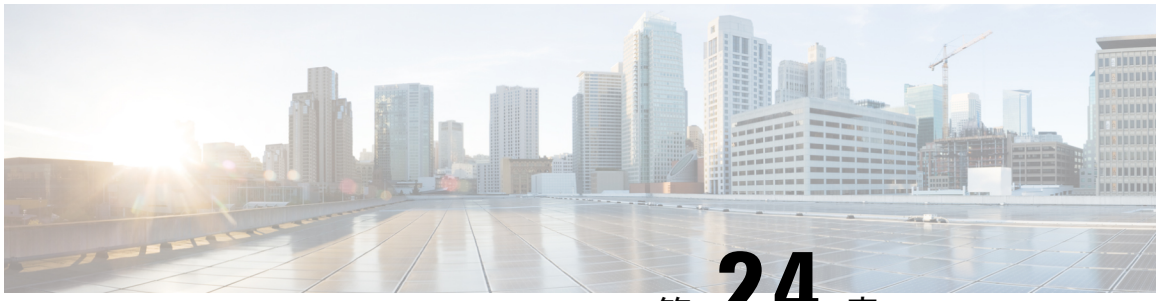
ステップ 7 データセンター テナント アプリケーション テンプレートで、外部 L3 ドメインに向けてアドバタイズされるキャンパス VN サブネット（またはサブネットのセット）に一致する Ext-EPG-VRF-DC の下に特定のプレフィックスを定義します。

図 30 : サブネットの更新 （323 ページ） に示す例では、この設定は特定の 192.168.100.0/24 プレフィックスに適用されます。

図 30 : サブネットの更新



（注）
VN サブネットに個別のプレフィックスを作成すると、外部 L3 ドメインへのキャンパス VN サブネットのアドバタイズを最も詳細なレベルで制御できます。このような細かい制御が必要ない場合は、代わりに 0.0.0.0/0 プレフィックスに関連付けられた「ルート制御のエクスポート」フラグを設定できます。これにより、tn-common から tn-app-dc に漏えいしたすべてのキャンパス VN サブネットを外部ドメインに送信できます。



第 24 章

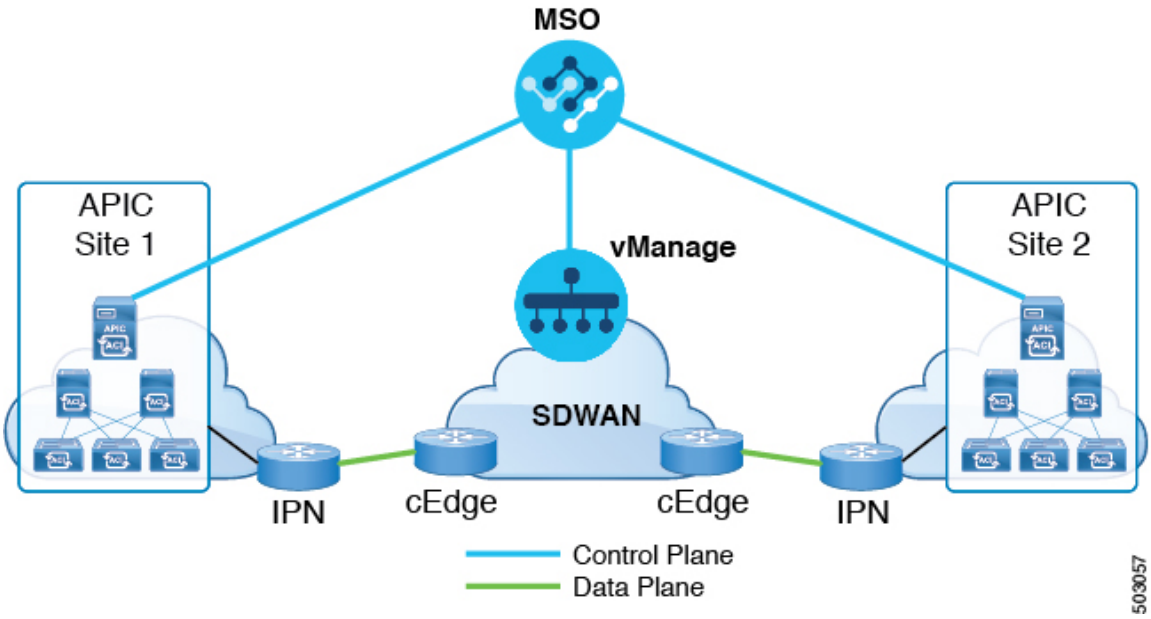
SD-WAN の統合

SD-WAN の統合

Cisco ソフトウェア定義ワイド エリア ネットワーク（SD-WAN）は、クラウド提供型のオーバーレイ WAN アーキテクチャです。単一のファブリックにより、ブランチをデータセンターとマルチクラウド環境に接続できるのが特長です。Cisco SD-WAN は、アプリケーションの予測可能なユーザエクスペリエンスを保証し、SaaS、IaaS、および PaaS 接続を最適化し、オンプレミスまたはクラウドで統合セキュリティを提供します。分析機能による可視化とインサイトは、問題を切り分けて迅速に解決するために役立ちます。プランニングと what-if シナリオ分析に欠かせない、高度なデータ解析も提供します。

データプレーン側では、SD-WAN は ASR または ISR ルータをエッジデバイスとして展開し（次の図では cEdge として表示）、各ファブリックのスパイン スイッチはこれらのエッジ デバイスに接続します。SD-WANは vManage と呼ばれる別のコントローラによって管理されます。これにより、サービスレベル契約（SLA）ポリシーを定義して、DSCP 値に基づいて SD-WAN 内の各パケットのパスを選択する方法を決定できます。

図 *31 : Multi-Site* と *SD-WAN* の統合



Cisco Nexus Dashboard Orchestrator のリリース 3.0(2) では、SD-WAN 統合のサポートが追加されています。vManage コントローラから SLA ポリシーをインポートし、各 SLA ポリシーに DSCP 値を割り当て、vManage コントローラに DSCP から SLA へのマッピングを通知するように NDO を設定できます。これにより、事前設定された SLA ポリシーを適用して、SD-WAN 上のサイト間トラフィックのパケット損失、ジッター、および遅延のレベルを指定できます。SD-WAN 機能を提供する外部デバイスマネージャとして設定されている vManage コントローラは、SLA ポリシーで指定された損失、ジッター、および遅延パラメータを満たす最適な WAN リンクを選択します。

マルチサイト SD-WAN の統合により、複数のファブリック間のトラフィックが SD-WAN ネットワークを通過できるようになり、リモートサイトからのリターントラフィックが割り当てられた ACI QoS レベルを維持できるようになります。Cisco NDO を vManage に登録すると、SLA ポリシーがインポートされ、ACI QoS レベルを適切な DSCP 値に変換できます。NDO は、SD-WAN を通過するトラフィックに DSCP 変換ポリシーを適用して、リターントラフィックで Quality of Service を有効にします。

リリース 3.0(2) では、NDO GUI で契約および EPG に直接 ACI QoS レベルを割り当てることもできます。トラフィックがファブリックを離れるたびに、その QoS レベルが DSCP 値に変換され、vManage が SD-WAN 経由のトラフィックのパスを選択するために使用されます。

SD-WAN 統合の注意事項と制約事項

Multi-Site と SD-WAN の統合を有効にする場合は、次のガイドラインが適用されます。

- サイト間の east-west トラフィックに対して均一なユーザー QoS レベルと DSCP 変換を有効にするには、各ファブリックのスパイン スイッチを直接または複数のホップを介して SD-WAN エッジ デバイスに接続する必要があります。

  これは、リーフ スイッチを SD-WAN エッジ デバイスに接続する必要がある north-south トラフィックの APIC SD-WAN 統合の既存の実装とは対照的です。

- グローバル DSCP ポリシーは、オンプレミス サイトでのみサポートされます。

- SD-WAN 統合は、Cisco Application Services Engine の Nexus Dashboard Orchestrator 展開でのみサポートされます。

  詳細については、Deployment Overviewの章（*Cisco Nexus Dashboard Orchestrator Installation and Upgrade Guide*）を参照してください。

- グローバル DSCP ポリシーを定義する場合は、QoS レベルごとに一意の値を選択する必要があります。

- 既存の DSCP ポリシー値に加えて、vManage から最大 4 つの SLA ポリシーをインポートできます。値は、41、42、43、45、47、49のいずれかです。

- SLA ポリシーは、Cisco vManage ですでに定義されている必要があります。

- QoS レベルを割り当てる場合、特定のコントラクトまたは EPG 全体に割り当てることができます。

  特定のトラフィックに複数の QoS レベルを適用できる場合は、次の優先順位を使用して 1 つだけが適用されます。

  - コントラクト QoS レベル：コントラクトで QoS が有効になっている場合は、コントラクトで指定された QoS レベルが使用されます。
  - 送信元 EPG QoS レベル：コントラクトに QoS レベルが指定されていない場合、送信元 EPG に設定された QoS レベルが使用されます。
  - デフォルトの QoS レベル：QoS レベルが指定されていない場合、トラフィックにはデフォルトでレベル 3 の QoS クラスが割り当てられます。

vManage コントローラの追加

このセクションでは、vManage コントローラを Nexus Dashboard Orchestrator に追加して、設定済みの SLA ポリシーをインポートする方法について説明します。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 vManage コントローラを追加します。

a) [インテグレーション（Integration）] > [SD-WAN] に移動します。 >
b) **[ドメイン コントローラの追加 (Add Domain Controller)]** をクリックします。

[ドメインの追加 (Add Domain)] ウィンドウが開きます。

ステップ 3 vManage コントローラ情報を入力します。

表示された **[エントリの追加 (Add Entry)]** ウィンドウで、次の情報を入力します。

- NDO に表示する vManage ドメインの名前。
- デバイスの IP アドレスまたは完全修飾ドメイン名（FQDN）。
- vManage コントローラへのログインで使用するユーザ名とパスワード。

[追加 (Add)] をクリックしてvManageドメインを保存します。vManage コントローラの情報を入力した後、既存の SLA ポリシーのリストがメイン ペインに表示されるまでに最大 1 分かかります。

次のタスク

グローバル DSCP ポリシーの設定 （328 ページ）の説明に従って、Nexus Dashboard Orchestrator でグローバル DSCP ポリシーを定義します。

グローバル DSCP ポリシーの設定

Cisco ACI ファブリック内でトラフィックが送受信される場合、VXLAN パケットの外部ヘッダーの CoS 値に基づいて決定される ACI QoS レベルに基づいて優先順位が付けられます。トラフィックがスパインスイッチからサイト間ネットワークへの ACI ファブリックを出ると、QoS レベルは VXLAN カプセル化パケットの外部ヘッダーに含まれる DSCP 値に変換されます。

ここでは、ACI ファブリックを出入りするトラフィックの DSCP 変換ポリシーを定義する方法について説明します。これは、トラフィックが非 ACI ネットワークを通過する必要がある場合（たとえば、Cisco APIC の管理下にないデバイスが通過するパケットの CoS 値を変更する可能性がある SD-WAN で区切られた複数のファブリック間）に必要です。

始める前に

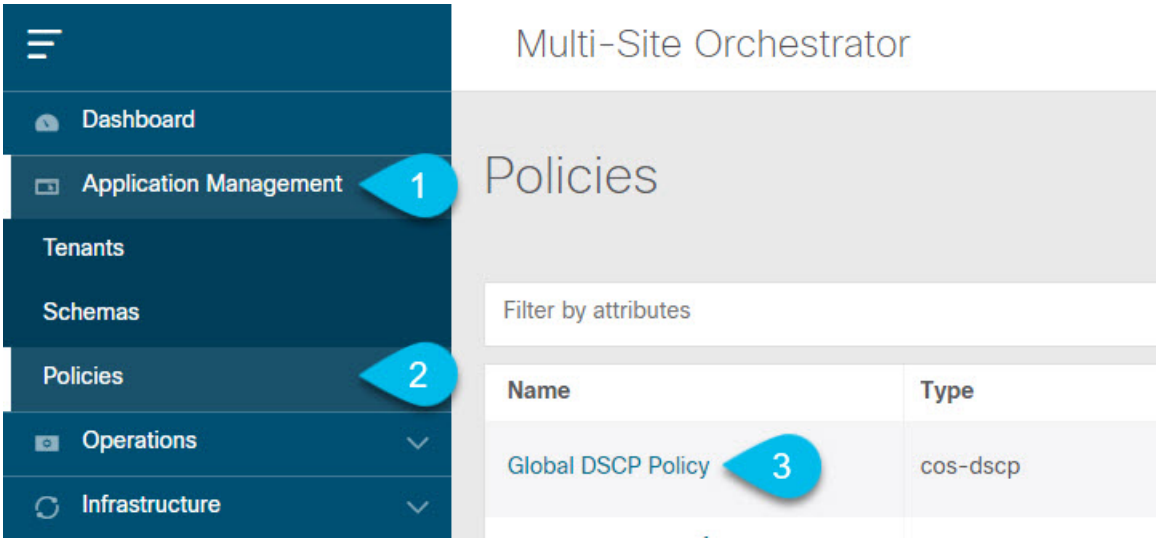
- vManage コントローラの追加 （327 ページ）の説明に従って、vManage コントローラを NDO に追加する必要があります。
- ACI ファブリック内の Quality of Service（QoS）機能に精通している必要があります。

  QoS の詳細については、*Cisco APIC and QoS* を参照してください。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 グローバル DSCP ポリシー設定画面を開きます。

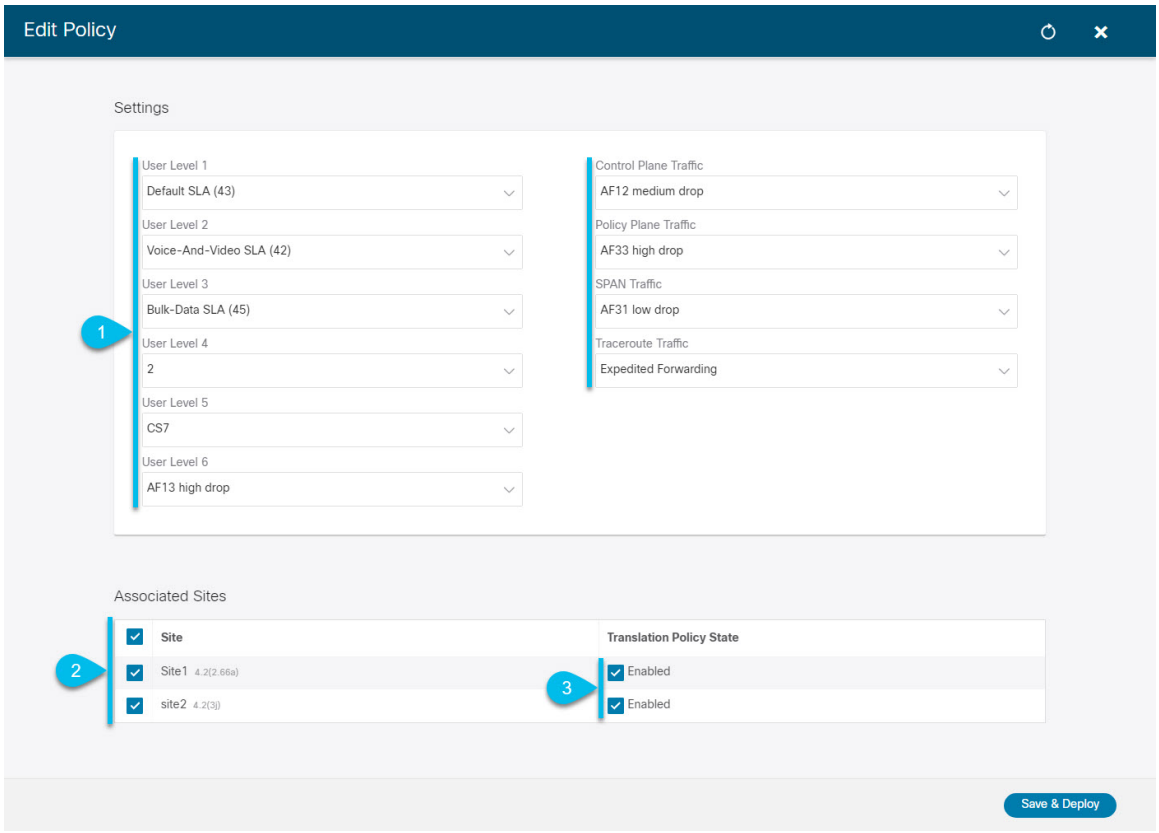


a) **[アプリケーション管理 (Application Management)[** > **[ポリシー (Policies)]** の順に移動します。

b) **[グローバル DSCP ポリシー名 (Global DSCP Policy name)]** をクリックします。

[ポリシーの編集 (Edit Policy)] ウィンドウが開きます。

ステップ 3 グローバル DSCP ポリシーを更新します。



a) 各 ACI QoS レベルの DSCP 値を選択します。

各ドロップダウンには、使用可能な DSCP 値のデフォルト リストと、vManage SLA ポリシーからインポートされた値（`Voice-And-Video SLA (42)` など）が含まれます。

b) ポリシーを展開するサイトを選択します。

エンドツーエンドの一貫した QoS 動作を実現するために、Multi-Site ドメインの一部であるすべてのサイトにポリシーを展開することを推奨します。

c) 各サイトの展開時にポリシーを有効にするかどうかを選択します。

d) [保存して展開（Save & Deploy）] をクリックします。

保存して展開すると、DSCP ポリシー設定が各サイトにプッシュされます。設定を確認するには、サイトの APIC にログインし、**[テナント (Tenants)]** > **[インフラ (infra)]** > **[ポリシー (Policies)]** > **[プロトコル (Protocol)]** > **[L3 トラフィックの DSCP クラス CoS 変換ポリシー (DSCP class-CoS translation policy for L3 traffic)]** に移動します。

次のタスク

グローバル DSCP ポリシーを定義した後、の説明に従って、ECI またはコントラクトに ACI QoS レベルを割り当てることができます。EPG およびコントラクトの QoS レベルの設定（331 ページ）

EPG およびコントラクトの QoS レベルの設定

ここでは、ファブリック内のトラフィックの ACI QoS レベルを選択する方法について説明します。個々のコントラクトまたは EPG 全体に対して QoS を指定できます。

始める前に

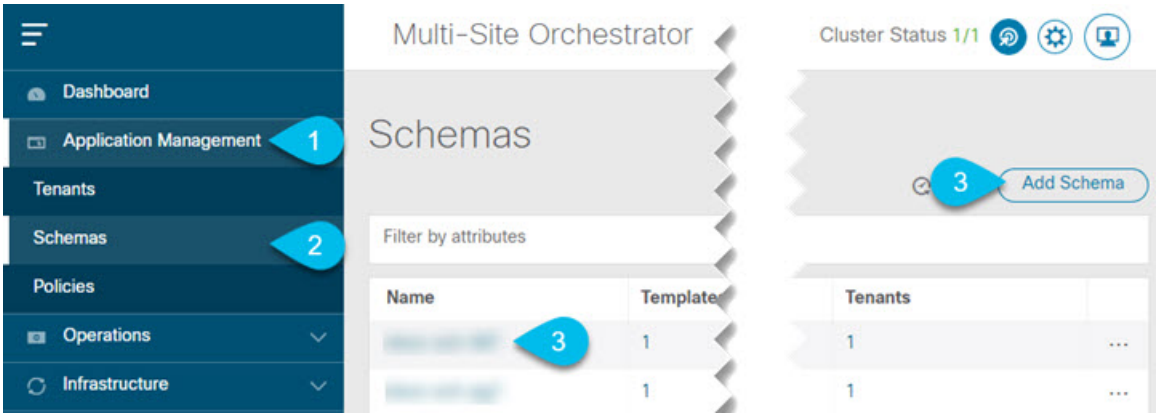
- vManage コントローラの追加 （327 ページ）の説明に従って、vManage コントローラを NDO に追加する必要があります。
- グローバル DSCP ポリシーの設定 （328 ページ）の説明に従って、グローバル DSCP ポリシーを定義しておく必要があります。
- ACI ファブリック内の Quality of Service（QoS）機能に精通している必要があります。

  QoS の詳細については、*Cisco APIC and QoS* を参照してください。

手順

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 編集するスキーマを選択します。

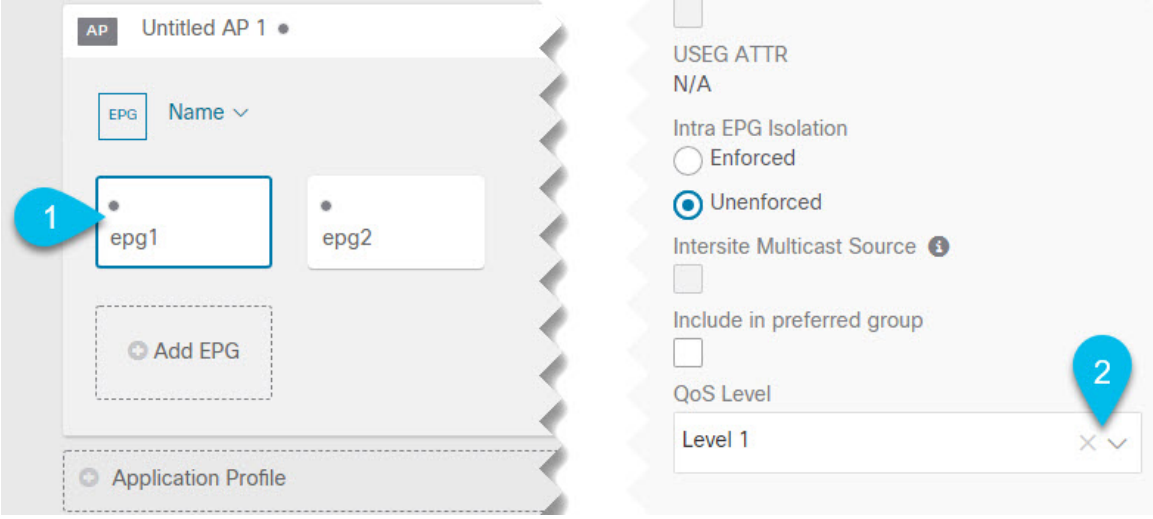


a) **[アプリケーション管理 (Application Management)[** > **[スキーマ (Schemas)]** > の順に移動します。

b) 編集するスキーマの名前をクリックするか、**[スキーマの追加 (Add Schema)]** をクリックして新しいスキーマを作成します。

[スキーマの編集 (Edit Schema)] ウィンドウが開きます。

ステップ 3 EPG の QoS レベルの選択

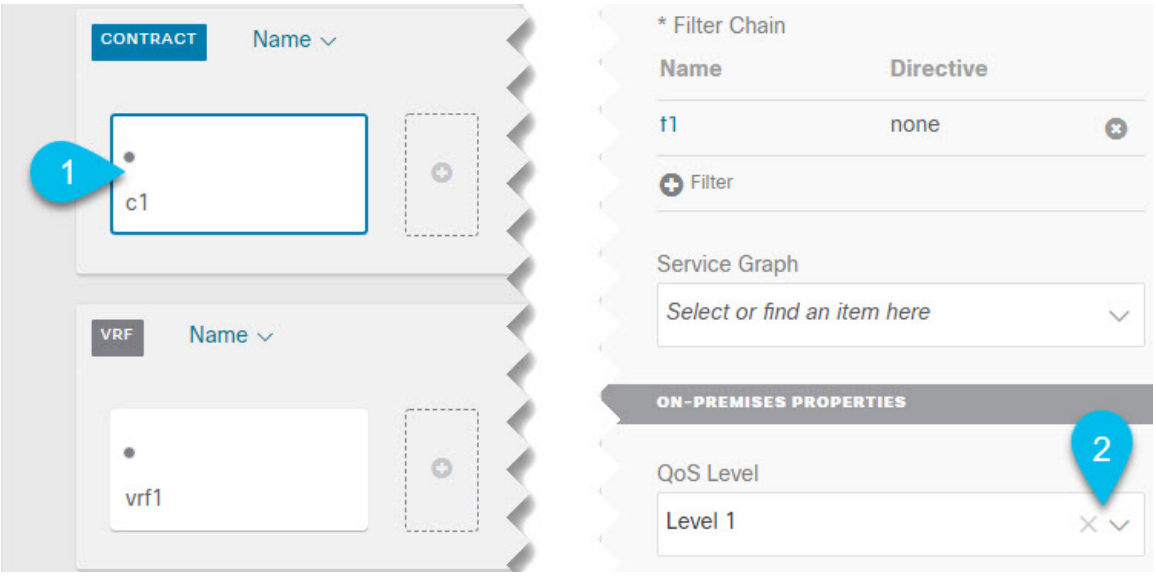


a) メインペインで、**[EPG]** エリアまでスクロールダウンして EPG を選択するか、**[EPG の追加 (Add EPG)]** をクリックして新しい EPG を作成します。

b) 右側のサイドバーで **[QoS レベル (QoS Level)]** ドロップダウンまでスクロールし、EPG に割り当てる QoS レベルを選択します。

EPGからのサイト間トラフィックがSD-WANネットワーク全体で目的のSLAで処理されるように、事前に設定されたグローバルDSCPポリシーに基づいてQoSレベルを選択する必要があります。

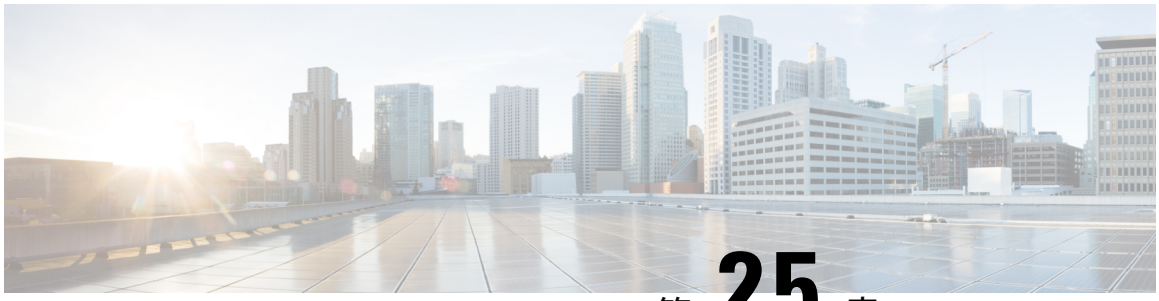
ステップ 4 EPG の QoS レベルの選択



a) メインペインで、**[コントラクト (Contract)]** 領域までスクロールダウンしてコントラクトを選択するか、**[+]** アイコンをクリックして新しいコントラクトを作成します。

b) 右側のサイドバーで、**[QoS レベル (QoS Level)]** ドロップダウンまでスクロールし、コントラクトに割り当てる QoS レベルを選択します。

2 つの EPG 間のサイト間トラフィックが SD-WAN ネットワーク全体で目的の SLA で処理されるように、事前に設定されたグローバル DSCP ポリシーに基づいて QoS レベルを選択する必要があります。



第 25 章

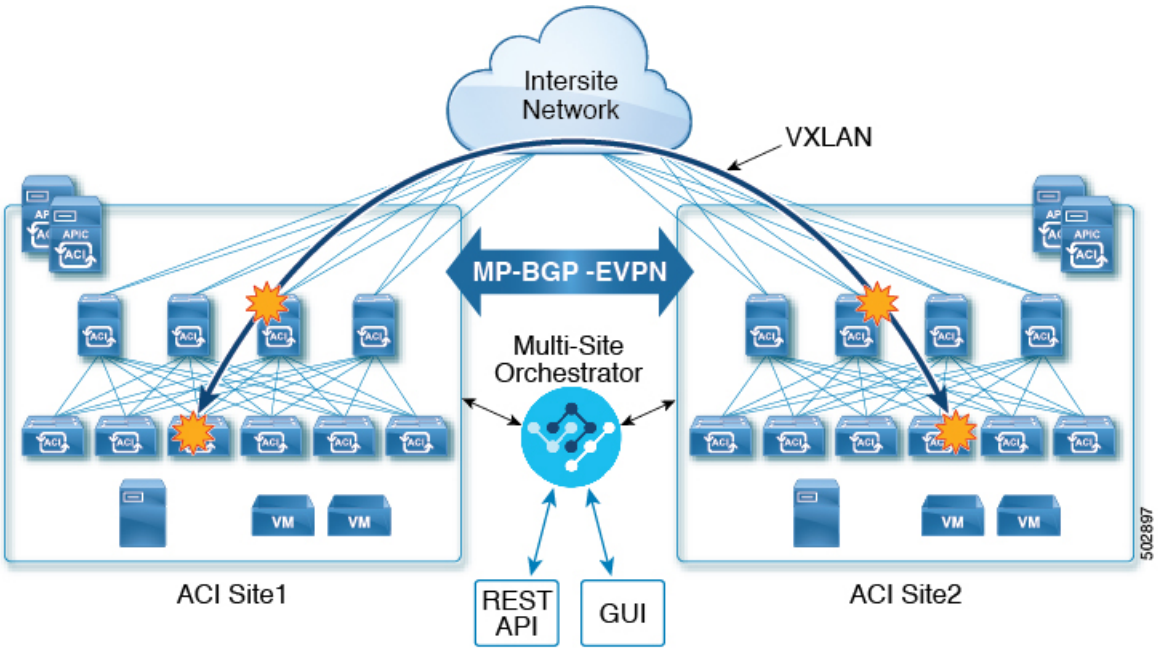
マルチサイトと SR-MPLS L3Out ハンドオフ

概要とユース ケース

Nexus Dashboard Orchestrator リリース 3.0（1）および APIC リリース 5.0（1）以降、マルチサイト アーキテクチャは、ACI ボーダー リーフ（BL）スイッチと SR-MPLS ネットワーク間のより優れたハンドオフ機能を提供します。

代表的な Multi-Site デプロイでは、サイト間トラフィックは、VXLAN カプセルかを介したサイト間ネットワーク（ISN）を通じて転送されます。

図 *32 : Multi-Site* と *ISN*

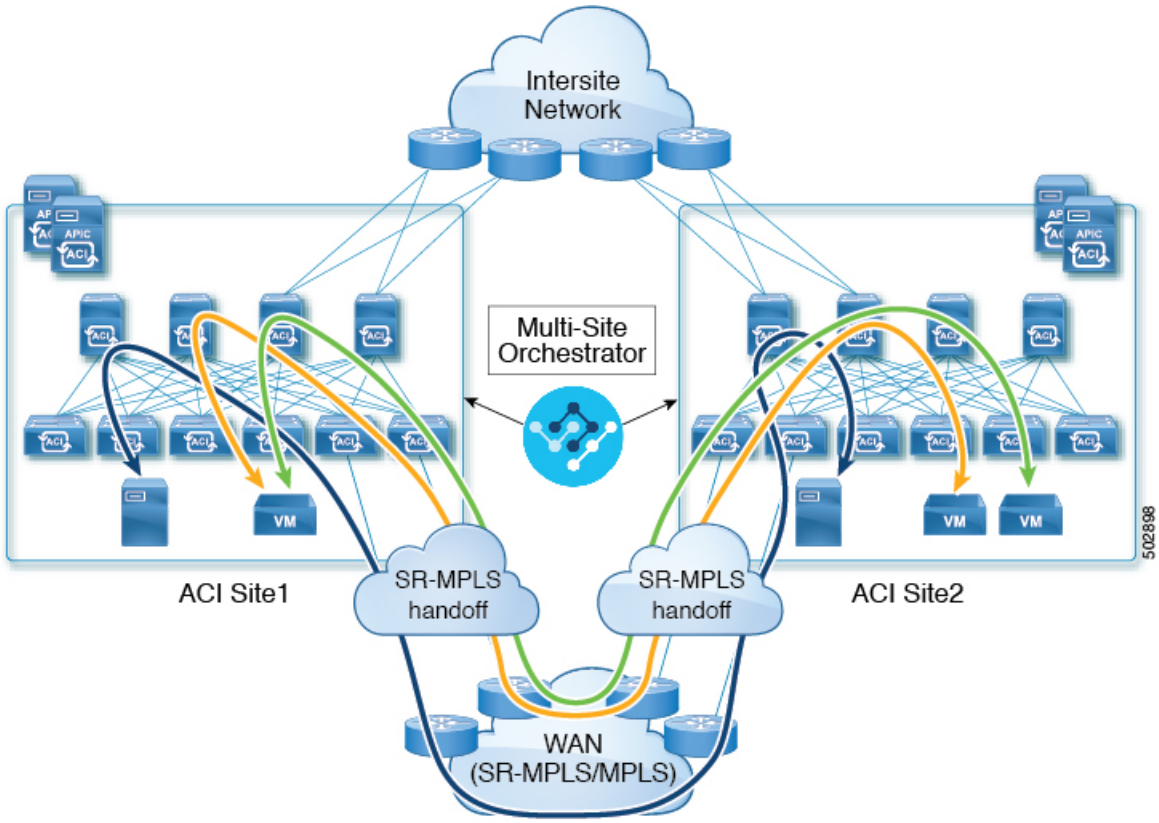


次の図に示されているようにリリース 3.0（1）で MPLS ネットワークは、WAN を介したサイト間通信を許可する ISN に加えて、またはその代わりに使用できます。East-West レイヤ 3 通信が SR-MPLS L3Out データ パス（ISN 全体の VXLAN データ パスではなく）に従うようにするために、この SR-MPLS ハンドオフのユース ケースにいくつかの制限を適用する必要がありました。

- SR-MPLS L3Out が属する VRF は、サイト間でストレッチしてはなりません。
- 上記の制限により、すべてのサイトは、定義されたサイトローカル VRF ごとに 1 つ（または複数）のローカル SR-MPLS L3Out を展開する必要があります。
- 異なる VRF に属するサイトローカル EPG 間で契約を適用してはなりません。

  これにより、通信は SR-MPLS L3Out データ パスに従うようになります。

図 *33 : Multi-Site* と *ISN*



リリース 4.0（2）以降の追加の使用例

リリース 4.0（2）より前では、SR-MPLS ユース ケースを展開する場合は、単一のサイトにのみ関連付けることができ、複数のサイトにまたがることはできない特別な「SR-MPLS」テンプレートを定義します。この場合、Nexus Dashboard Orchestrator によって管理され、SR-MPLS ネットワーク経由で接続された 2 つのサイトがあり、`[site1]` の EPG と `[site2]` の別の EPG 間の通信を確立したい場合、2 つの個別の VRF に関連付けられている 2 つの個別の SR-MPLS L3Out（各サイトに 1 つ）を展開する必要がありました。そして、各サイトの EPG とそのサイトの SR-MPLS L3Out（EPG 間で直接ではなく）との間でコントラクトを確立する必要もあります。つまり、EPG のトラフィックは、East-West トラフィック用の従来の Multi-Site データ プレーンと統合することなく、サイト間の EPG-to-EPG 通信でも常に SR-MPLS L3Out データ パスを使用します。

リリース 4.0（2）以降、SR-MPLS L3Out は従来の IP ベースの L3Out と同様に機能します。これにより、サイトと外部ネットワーク間の North-South 接続専用に SR-MPLS L3Out ハンドオフを使用できます。この間すべての East-West トラフィックは、ISN 全体で VXLAN でカプセル化されたデータ プレーンを使用して、従来のマルチサイト方式で処理されます。これは、SR-MPLS ハンドオフを従来の IP ベースのハンドオフとして扱うことができ、同じ VRF で IP と SR-MPLS L3Out の混合を展開できることを意味します。これらの変更により、次の特定のユース ケースのサポートが追加されます。

- 特定の VRF に属する SR-MPLS L3Out のサイトでの集中型展開。

  その VRF の一部である（同じサイトまたは異なるサイトに接続されている）エンドポイントからのすべてのトラフィックは、North-South 接続にその集中型 SR-MPLS L3Out を利用できます。これには、VRF をサイト間でストレッチする必要があることに注意してください。

- それぞれが独自のローカル SR-MPLS L3Outs を持つ複数のサイトの展開と、ローカル L3Out を使用する VRF 内トラフィック（使用可能な場合）または別のサイトからのリモート SR-MPLS-L3Out（サイト間 L3Out）。

  この場合、リモート SR-MPLS-L3Out を単純なバックアップとして使用したり、リモート SR-MPLS-L3Out で受信した一意の外部プレフィックスに到達したりできます。トラフィックはローカル EPG からローカル SR-MPLS L3Out に転送され、そのパスがダウンしているかルートが利用できない場合は、別のサイトのリモート SR-MPLS L3Out を使用できます。

- 同様の使用例が共有サービスでもサポートされており、1 つの VRF 内のアプリケーション EPG は、ローカル サイトまたはリモート サイトの別の VRF 内の SR-MPLS L3Out を使用できます。

  この場合、EPG は別のテナントにも配置できます。たとえば、Site1 の Tenant1 には、Site2 の Tenant2 で SR-MPLS L3Out を使用するアプリケーション EPG を含めることができます。

- IP ベースのハンドオフと SR-MPLS のハンドオフを組み合わせる機能。

- SR-MPLS ハンドオフを使用して、SR-MPLS コアネットワークの一部であるプロバイダー エッジ（PE）デバイスと、通常の MPLS ネットワークの一部である PE に接続できるようになりました。その際に、ハンドオフは単純な MPLS ハンドオフと見なされます。

（従来の IP ベースの L3Out の代わりに）SR-MPLS L3Out を使用すると、個別の BL ノード、BL 論理インターフェイス、および外部ネットワークに接続する必要のある各 VRF のルーティング ピアリングの作成を必要とする VRF-Lite 構成の必要性がなくなるため、より大規模な運用の簡素化が可能になります。SR-MPLS L3Out を使用すると、論理ノードと論理インターフェイスは、外部デバイスとの単一の MP-BGP EVPN ピアリングとともに、インフラ テナントで一度定義されます。このインフラ L3Out コンストラクトを使用して、複数のテナント VRF への外部接続を提供でき、すべての VRF のプレフィックスは、共通の MP-BGP EVPN コントロール プレーンを使用して交換されます。

次のセクションでは、Nexus Dashboard Orchestrator からサイトに展開されるスキーマを管理するためのガイドライン、制限事項、およびそれ特定の構成について説明します。MPLS ハンドオフ、サポートされている個々のサイトのトポロジ（リモート リーフ サポートなど）、ポリシー モデルは、『*Cisco APIC Layer 3 ネットワーキング構成ガイド*』で入手可能です。

構成ワークフロー

このドキュメントの他のセクションでは、必要な構成について詳しく説明しています。簡単に言えば、次のワークフローを実行します。

- SR-MPLS QoS ポリシーの作成

SR MPLS カスタム QoS ポリシーは、MPLS QoS 出力 ポリシーで定義された着信 MPLS EXP 値に基づいて、SR-MPLS ネットワークから送信されるパケットのプライオリティを定義します。これらのパケットは、ACI ファブリック内にあります。また、MPLS QoS 出力ポリシーで定義された IPv4 DSCP 値に基づく MPLS インターフェイスを介して ACI ファブリックから離れるパケットの CoS 値および MPLS EXP 値をマーキングします。

このステップはオプションであり、そしてカスタム出力ポリシーが定義されていない場合、デフォルトの Qos レベル（`Level3`）がファブリック内のパケットに割り当てられます。カスタム出力ポリシーが定義されていない場合、デフォルトの EXP 値（`0`）がファブリックから離れるパケットにマーキングされます。

- SR-MPLS インフラ L3Out を作成します。

  これにより、SR-MPLS ネットワークに接続されているサイトから出るトラフィックの L3Out が構成されます。

- SR-MPLS ルート マップ ポリシーを作成します。

  ルートマップは、テナントSR-MPLS L3Outからアドバタイズされるルートを指定できる `if-then` ルールのセットです。ルートマップでは、DC-PE ルータから受信したどのルートを BGP VPNv4 ACI コントロールプレーンに挿入するかを指定することもできます。

- リリース 4.0（2）より前のリリースと同様のユース ケースを展開する場合は、SR-MPLS ネットワーク経由で接続された各サイトに VRF、SR-MPLS L3Out、および SR-外部 EPG を作成し、各サイト内で契約を確立します。そのサイトのテナント EPG と SR-External EPG の間。

  この場合、1 つのサイトからのすべての通信は、North-South ルートをたどり、マルチサイト ドメインを出て、外部 SR-MPLS ネットワークに向かいます。トラフィックの宛先が、Orchestrator によって管理される別のサイトの EPG である場合、そのサイトの SR-MPLS L3Out を使用して、外部ネットワークから他のファブリックに入ります。

- North-South 通信専用の標準 IP ベースの L3Out と同じ方法で SR-MPLS L3Out を使用する場合は、既存のすべての EPG-to-EPG への通信の使用例に対して通常行うように、VRF、SR-MPLS L3Out、EPG、および契約を作成できます。

SR-MPLS インフラ要件とガイドライン

Nexus ダッシュボード オーケストレータを使用して、SR-MPLS ネットワークに接続された ACI ファブリックの SR-MPLS L3Out ハンドオフを管理する場合：

- ノードの更新など、トポロジーへの変更は、サイト接続性情報の更新（177 ページ） の説明に従ってサイトの構成が更新されるまで、Orchestrator 構成には反映されません。
- SR-MMPLS ネットワークを通じて接続あれているサイトに展開されているテナントは、SR-MPLS 設定に特別の固有の構成オプションのセットをもちます。テナント構成は、*Multi-Site* 構成ガイド、リリース *3.1(x)* の「テナント管理」の章で説明されています。

- リモート リーフ スイッチは、マルチサイト トラフィック フローの送信元または宛先としてサポートされていません。
- 優先グループの一部である SR-External EPG は、共有サービス（VRF 間）コントラクトのプロバイダになることはできません。
- 優先グループはサイト間 SR-MPLS L3Out をサポートしません。
- vzAny は共有サービスプロバイダーをサポートしません。
- 優先グループに対して有効になっている VRF は、vzAny コンシューマにすることはできません。
- 同じコントラクトを使用する他の構成オブジェクトとの循環依存を避けるために、専用テンプレートの下でテナント コントラクト オブジェクトを構成することをお勧めします
- SR L3Outs と外部 EPG を専用のテンプレートに保持することをお勧めします。

  これにより、インフラ SR L3Out がないサイトに他のオブジェクト（VRF、BD、EPG など）を拡張できます。
- 従来の IP ベースの L3Out の代わりに SR-MPLS L3Out を使用する場合：
  - ホストベースのルーティング アドバタイズメントは、サイト全体に広がるブリッジドメインではサポートされていません。
  - テナント ルーテッド マルチキャスト（TRM）は SR-MPLS L3Out でサポートされていないため、外部ネットワーク ドメインとのレイヤー3ユニキャスト通信を確立するためにのみ使用できます。

サポート対象ハードウェア

SR-MPLS ハンドオフは、以下のプラットフォームに対してサポートされています：

- **ボーダー リーフ スイッチ**：「FX」、「FX2」、および「GX」 スイッチ モデル。
- **スパイン スイッチ**:
  - ラインカード名の末尾に「LC-EX」、「LC-FX」、および「GX」が付いたモジュラ スパイン スイッチ モデル。
  - Cisco Nexus 9000 シリーズ N9K-C9364C および N9K-C9332C 固定スパイン スイッチ。
- DC-PEルータ：
  - Network Convergence System（NCS）5500 シリーズ
  - ASR 9000 シリーズ
  - NCS 540 または 560 ルータ

SR-MPLS インフラ L3Out

次のセクションの説明に従って、SR-MPLS ネットワークに接続されたファブリックの SR-MPLS Infra L3Out を作成する必要があります。SR-MPLS L3Out Infra を作成するときには、次の制約が適用されます。

- 各 SR-MPLS L3Out Infra L3Out には固有の名前が必要です。

  SR-MPLS インフラ L3Out を使用すると、ACI ボーダー リーフ スイッチと外部プロバイダー エッジ（PE）デバイスの間にコントロール プレーンとデータ プレーンの接続を確立できます。さまざまなテナント VRF に属する SR-MPLS L3Out は、そのインフラ L3Out 接続を利用して、外部ネットワーク ドメインとの通信を確立できます。

- 異なるルーティング ドメインに接続されているロケーションごとに複数の SR-MPLS Infra L3Out を持つこと、その際に同じボーダー リーフ スイッチは複数の L3Out にあること、各ルーティング ドメインに向かって VRF のルーティング ポリシーをエクスポートすることが可能です。

- ボーダー リーフ スイッチが複数の SR-MPLS Infra L3Out にあることができる場合でも、ボーダー リーフ スイッチ/プロバイダ エッジ ルーターの組み合わせは 1 つの SR-MPLS L3Out になければなりません。ユーザ VRF/ボーダー リーフ スイッチ/プロバイダ エッジ ルートの組み合わせに対して 1 つのルーティング ポリシーのみが存在できるからです。

- 複数のポッドおよびリモート ロケーションから SR-MPLS 接続を確立する必要がある場合は、SR-MPLS 接続を使用するポッドおよびリモート リーフ ロケーションのそれぞれに異なる SR-MPLS インフラ L3Out があることを確認します。

- ポッドの 1 つが SR-MPLS ネットワークに直接接続されていないマルチポッドまたはリモートリーフトポロジがある場合、SR-MPLS ネットワークを宛先とするそのポッドのトラフィックは、SR-MPLS L3Out を持つ別のポッドへの標準 IPN パスを使用します。その後、トラフィックは他のポッドの SR-MPLS L3Out を使用して、SR-MPLS ネットワーク全体の宛先に到達します。

- 複数の VRF からのルートは、1 つの SR-MPLS Infra L3Out から、この SR-MPLS Infra L3Out のノードに接続されているプロバイダ エッジ（PE）ルーターにアドバタイズできます。

  PE ルータは、ボーダー リーフに直接接続することも、他のプロバイダー（P）ルータを介して接続することもできます。

- アンダーレイ設定は、1 つのロケーションに対して複数の SR-MPLS Infra L3Out にわたって異なるか、同じ場合があります。

  たとえば、両方に対して別のプロバイダ ルーターに接続されたアンダーレイをもつ、ドメイン 1 の PE-1 とドメイン 2 の PE-2 に同じボーダー リーフ スイッチが接続されていると想定します。この場合、2 つの SR-MPLS Infra L3Out が作成されます。PE-1 に対して 1 つと PE-2 に対して 1 つです。しかしアンダーレイの場合、プロバイダ ルーターへの同じ BGP ピアになります。インポート/エクスポート ルートマップは、ユーザ VRF の対応するルート プロファイル設定に基づいて、PE-1 および PE-2 への EVPN セッションに設定されます。

MPLS カスタム QoS ポリシー

次に、MPLS QoS のデフォルトの動作を示します。

- 境界リーフ スイッチ上のすべての受信 MPLS トラフィックは QoS レベル 3（デフォルトの QoS レベル）に分類されます。
- 境界リーフ スイッチは、再マーキングなしで SR-MPLS からのトラフィックの元の DSCP 値を保持します。
- 境界リーフ スイッチは、デフォルトの MPLS EXP（0）のパケットを SR-MPLS ネットワークに転送します。

次に、MPLS カスタム QoS ポリシーを設定する際のガイドラインと制約事項を示します。

- データ プレーン ポリサー（DPP）は、SR-MPLS L3Out ではサポートされていません。
- レイヤ 2 DPP は、MPLS インターフェイスの入力方向で動作します。
- レイヤ 2 DPP は、出力カスタム MPLS QoS ポリシーがない場合、MPLS インターフェイスの出力方向で動作します。
- VRF レベルのポリシングはサポートされていません。

SR-MPLS テナントの要件と注意事項

Infra MPLS の設定と要件は Day-0 操作の章で説明されていますが、次の制約が SR-MPLS ネットワークに接続されているし後に展開するユーザ テナントに適用されます。

- ファブリックの 2 つの EPG 間のトラフィックが SR-MPLS ネットワークを通過する必要がある場合:
  - 各 EPG とローカル SR-MPLS L3Out で定義された SR-EPG の間に、コントラクトを割り当てる必要があります。
  - 両方の EPG が同じACI ファブリックの一部であるが、SR-MPLS ネットワークによって分離されている場合（たとえば、マルチポッドまたはリモートリーフの場合)、EPG が異なる VRF に属していること、その間にはコントラクトがないこと、ルートリーキングが設定されていないことが必要です。
  - EPG が異なるサイトにある場合、それらは同じ VRF に存在できますが、EPG と同じ VRF の一部の他のリモート EPGの間で直接構成されたコントラクトがあっては**なりません**。
- SR-MPLS L3Out のルート マップ ポリシーを設定する場合:
  - 各 L3Out は、単一のエクスポート ルート マップがなければなりません。オプションで、単一のインポート ルート マップももつことができます。

- SR-MPLS L3Out に関連付けられたルート マップは、SR-MPLS L3Out からアドバタイズする必要がある、ブリッジ ドメイン サブネットを含むすべてのルートを明示的に定義する必要があります。
- `0.0.0.0/0` プレフィックスを定義し、ルートをアグレゲートしないことにした場合、デフォルトのルートのみを許可します。

  しかし、ルート `0.0.0.0/0` プレフィックスにアグリゲートすることにした場合、VRF のすべてのトラフィックが許可されます。
- 任意のルーティング ポリシーを任意のテナント L3Out に関連付けることができます。

- Nexus Dashboard リリース 4.0（1）以降、SR-MPLS ネットワーク間のトランジット ルーティングは、Cisco APIC リリース 5.1（1）以降を実行しているファブリックに同じまたは異なる VRF を使用してサポートされます。

図 *34* : 単一の *VRF* を使用する移行ルーティング構成

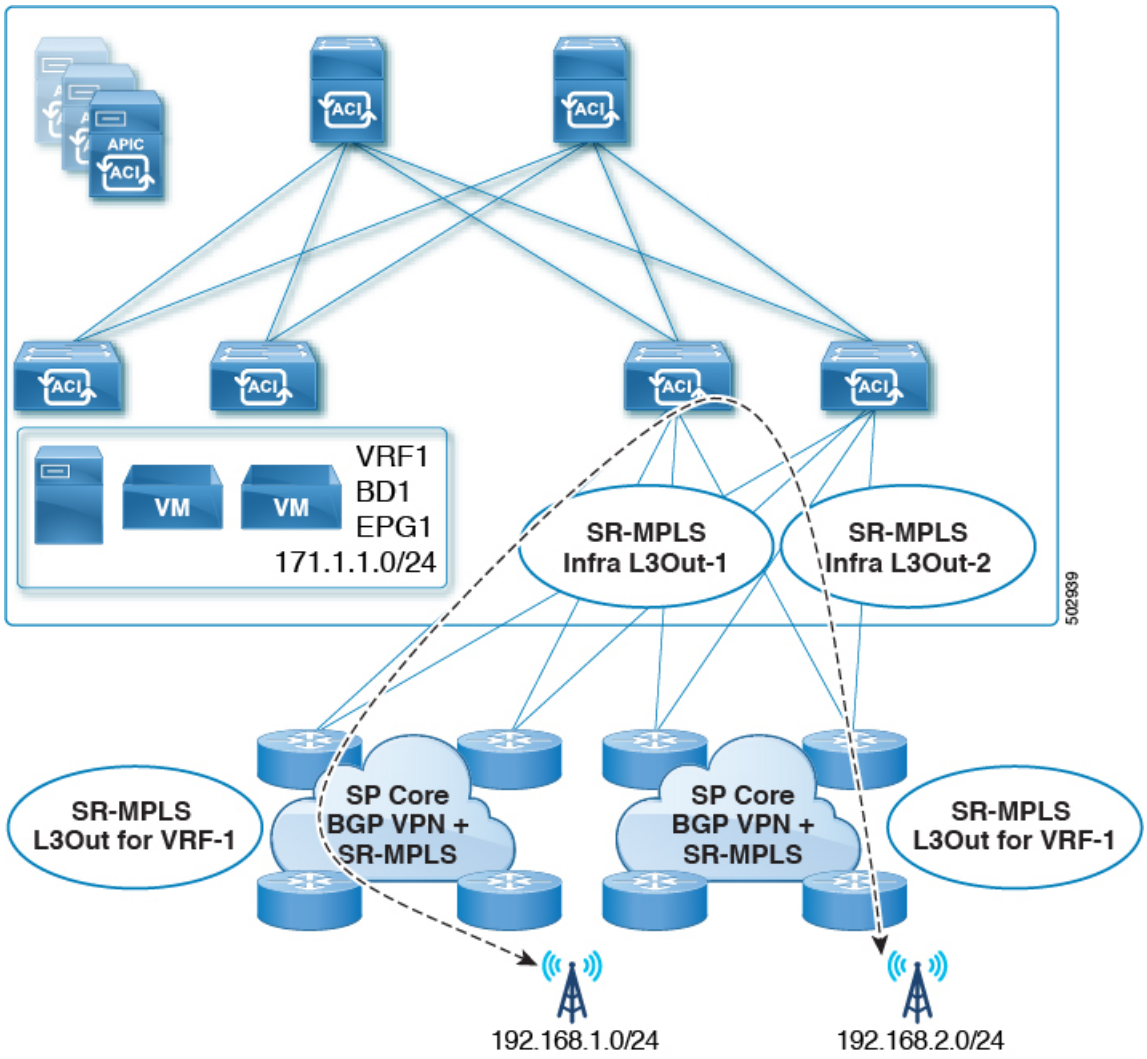
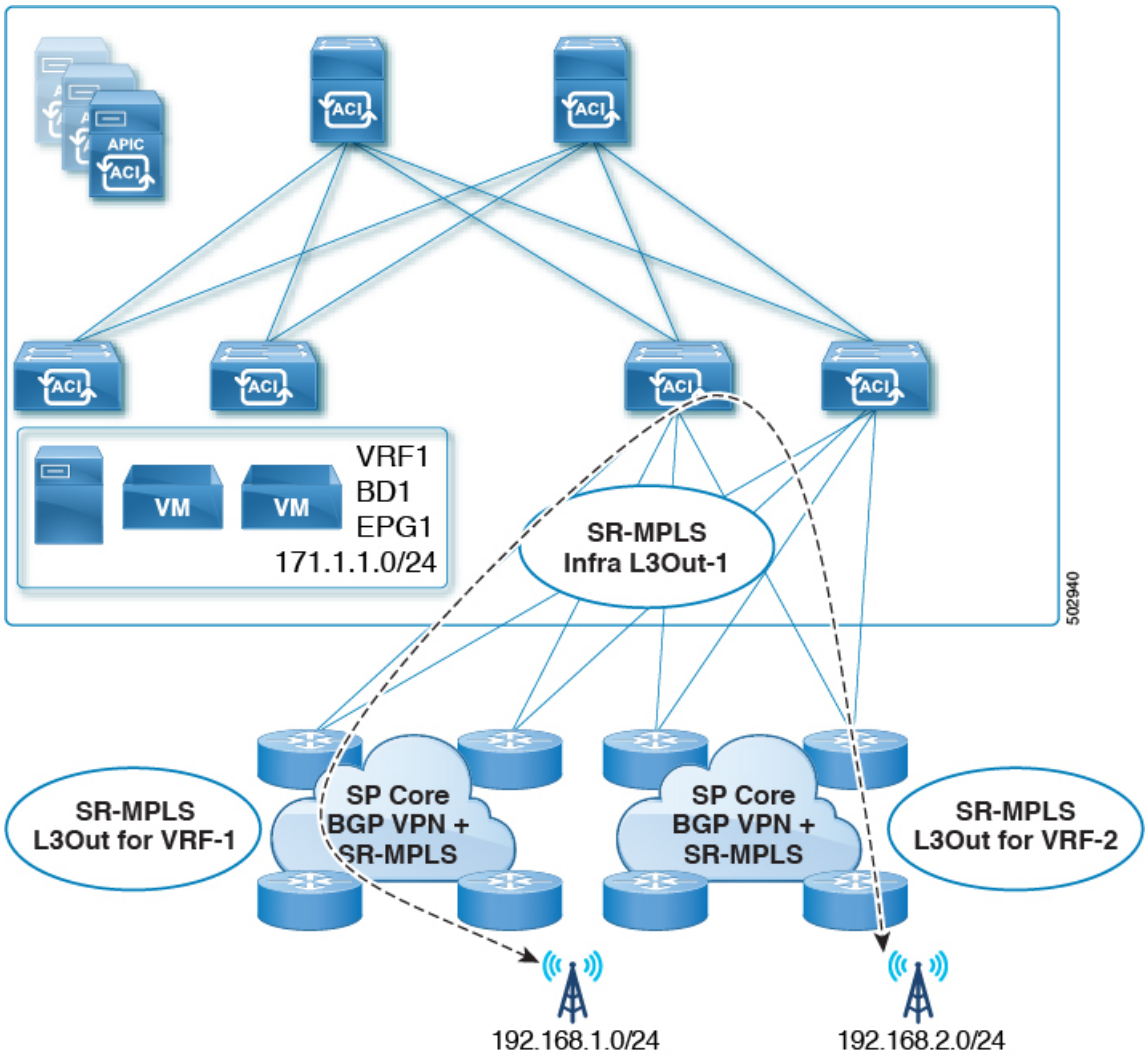


図 *35* : 異なる *VRF* を使用する移行ルーティング構成



以前のリリースでは、異なる VRF のみを使用したトランジット ルーティングがサポートされていました。

SR-MPLS のカスタム QoS ポリシー を作成

SR MPLS カスタム QoS ポリシーは、MPLS QoS 出力 ポリシーで定義された着信 MPLS EXP 値に基づいて、SR-MPLS ネットワークから送信されるパケットのプライオリティを定義します。これらのパケットは、ACI ファブリック内にあります。また、MPLS QoS 出力ポリシーで定義された IPv4 DSCP 値に基づく MPLS インターフェイスを介して ACI ファブリックから離れるパケットの CoS 値および MPLS EXP 値をマーキングします。

（注） カスタム QoS ポリシーの作成はオプションです。カスタム出力ポリシーが定義されていない場合、デフォルトの Qos レベル（Level3）がファブリック内のパケットに割り当てられます。カスタム出力ポリシーが定義されていない場合、デフォルトの EXP 値（0）がファブリックから離れるパケットにマーキングされます。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 新しいファブリック ポリシーを作成します。

a) 左側のナビゲーション メニューで、**[ファブリック管理（Fabric Management）]** > **[ファブリック ポリシー（Fabric Policies）]** を選択します。

b) **[ファブリック ポリシー テンプレート（Fabric Policy Template）]**ページ内で**[ファブリック ポリシー テンプレートを追加（Add Fabric Policy Template）]**をクリックします。

c) **[+オブジェクトを作成（+Create Object）** ドロップダウンから**QoS SR-MPLS**を作成します。

d) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。

e) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。

ステップ 3 入力 QoS 変換ルールを追加するには、**[入力ルールの追加 (Add Ingress Rule)]** をクリックします。

これらのルールは、MPLS ネットワークから ACI ファブリックをイングレスしているトラフィックに適用されます。そして、受信される EXP ビット（EXP）の値のパケットを ACI QoS レベルにマップするためとパケットがファブリックに接続されたエンドポイントに転送されるときに設定するべきだったDSCP および/または CoS の値の設定に使用されます。

値は、境界リーフでカスタム QoS 変換ポリシーを使用して取得されます。カスタム ポリシーが定義されていないか、一致していない場合、デフォルトのQoS レベル（Level3）が割り当てられます。

a) **[EXP 照合開始 (Match Exp From)]** と **[EXP 照合終了 (Match EXP To)]** フィールドで、照合する入力 MPLS パケットの EXP 範囲を指定します。

b) **[キューの優先順位 (Queuing Priority)]** ドロップダウンから、マッピングする ACI QoS レベルを選択します。

これは、ACI ファブリック内のトラフィックに割り当てる QoS レベルで、ACI はファブリック内のトラフィックのプライオリティを決めるために使用します。オプションの範囲は Level1 ー Level6 です。デフォルト値は Level3です。このフィールドで選択しない場合、トラフィックには自動的に Level3 の優先順位が割り当てられます。

c) **[DSCP を設定（Set DSCP）]** ドロップダウンから、カプセル化されていないパケットをファブリックに接続されたエンドポイントに送信するときに使用する DSCP 値を選択します。

指定された DSCP 値は、外部ネットワークから受信した元のトラフィックに設定されるため、トラフィックが宛先 ACI リーフ ノードで VXLAN カプセル化解除された場合にのみ再公開されます。

値を [未指定 (Unspecified)] に設定すると、パケットの元の DSCP 値が保持されます。

d) **[CoS を設定（Set CoS）]** ドロップダウンから、カプセル化されていないパケットをファブリックに接続されたエンドポイントに送信するときに使用する DSCP 値を選択します。

指定された CoS 値は、トラフィックが宛先 ACI リーフ ノードで VXLAN カプセル化解除された場合にのみ再公開されます。

値を [未指定（Unspecified）] に設定すると、パケットの元の CoS 値が保持されます。

上記のどちらの場合も、ファブリックで CoS 保存オプションを有効にする必要があります。CoS 保存の詳細については、「*Cisco APIC and QoS*」を参照してください。

e) チェックマーク アイコンをクリックして、ルールを保存します。

f) 追加の入力 QoS ポリシー ルールについて、この手順を繰り返します。

ステップ 4 出力 QoS 変換ルールを追加するには、**[出力ルールの追加 (Add Egress Add Rule)]** をクリックします。

これらのルールは、MPLS L3Out 経由で ACI ファブリックから発信されるトラフィックに適用され、パケットの IPv4 DSCP 値を MPLS パケットの EXP 値および内部イーサネットフレームの CoS 値にマッピングするために使用されます。

パケットの IPv4 DSCP 値の設定は、EPG および L3Out トラフィックに使用される既存のポリシーに基づいて非境界リーフ スイッチで行われます。カスタム ポリシーが定義されていないか、一致していない場合、デフォルトの EXP 値 0 がすべてのラベルでマークされます。EXP 値は、デフォルト ポリシー シナリオとカスタム ポリシー シナリオの両方でマークされ、パケット内のすべての MPLS ラベルで行われます。

カスタム MPLS 出力ポリシーは、既存の EPG、L3Out、および契約 QoS ポリシーをオーバーライドできます。

a) **[DSCP 照合開始 (MATCH DSCP From)]** と **[DSCP 照合終了 (MATCH DSCP To)]**] ドロップダウンを使用して、出力 MPLS パケットのプライオリティを割り当てるために一致させる ACI ファブリック パケットの DSCP 範囲を指定します。

b) **[MPLS EXP の設定 (SET MPLS EXP)]** ドロップダウンから、出力 MPLS パケットに割り当てる EXP 値を選択します。

c) **[CoS の設定(Set CoS)]** ドロップダウンから、出力 MPLS パケットに割り当てる CoS 値を選択します。

d) チェックマーク アイコンをクリックして、ルールを保存します。

e) 追加の出力 QoS ポリシー ルールについて、この手順を繰り返します。

ステップ 5 **[アクション（Actions）]** メニューから、**[サイトの関連付け（Sites Association）]** を選択し、このテンプレートを関連付ける SR-MPLS サイトを選択します。

ステップ 6 [保存（Save）] をクリックして、テンプレート ポリシーを保存します。

ステップ 7 **[展開する（Deploy）]** をクリックして、ファブリック ポリシーをサイトに展開します。

次のタスク

QoS ポリシーを作成したら、SR-MPLS インフラ L3Out の作成 （347 ページ） の説明に従って mpls 接続を有効にし、MPLS L3Out を設定します。

SR-MPLS インフラ L3Out の作成

このセクションでは、SR-MPLS ネットワーク経由で接続されているサイトの SR-MPLS インフラ L3Out を構成する方法について説明します。

- SR-MPLS インフラ L3Out は、境界リーフスイッチで設定され、SR-MPLS ハンドオフに必要なアンダーレイ BGP-LU およびオーバーレイ MP-BGP EVPN セッションを設定するために使用されます。
- SR-MPLS インフラ L3Out は、ポッドまたはリモート リーフ スイッチ サイトにスコープされます。
- 1 つの SR-MPLS インフラ L3Out 内の境界リーフ スイッチまたはリモート リーフ スイッチは、1 つ以上のルーティング ドメイン内の 1 つ以上のプロバイダー エッジ（PE）ルータに接続できます。
- ポッドまたはリモート リーフ スイッチ サイトには、1 つ以上の SR-MPLS インフラ L3Out を設定できます。

始める前に

次のものが必要です。

- Cisco ACI サイトの追加 （163 ページ） で説明しているように、MPLS ネットワークを経由して接続されているサイトを追加したこと。
- 必要に応じ、SR-MPLS の カスタム QoS ポリシー を作成 （344 ページ） で説明しているように、SR-MPLS QoS ポリシーを作成したこと。

手順

ステップ 1 サイトで SR-MPLS 接続が有効になっていることを確認します。

a) メイン ナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

b) **[サイト接続（Site Connectivity）]** ページで、**[構成（Configure）]** をクリックします。

c) 左のペインの **[サイト（Sites）]** の下、SR-MPLS で接続されている特定のサイトを選択します。

d) 右に **<*Site*>[設定（Settings）]** ペインで、**[SR-MPLS 接続（SR-MPLS Connectivity）]** を有効にして、SR-MPLS 情報を提供します。

- **セグメント ルーティング グローバル ブロック（SRGB）範囲**は、ラベル スイッチング データベース（LSD）でセグメント ルーティング（SR）用に予約されているラベル値の範囲です。セグメント識別子（SID）は、特定のセグメントの一意の識別子であり、MPLS トランスポート ループバック用に各ノードで構成されます。後にボーダー リーフ構成の一部として構成する SID 値は BGP-LU を使用してピア ルータにアドバタイズされ、ピア ルータは SID インデックスを使用してローカル ラベルを計算します。

デフォルトの範囲は 16000 ～ 23999 です。

- **ドメイン 識別子 ベース**は、BGP ドメイン パス機能を有効にします。詳細については、*Cisco APIC レイヤ 3 ネットワーキング 構成ガイド* を参照してください。

  このフィールドに値を指定してドメイン パス機能を有効にする場合は、マルチサイト ドメイン内の各 SR-MPLS サイトに一意の値を使用するようにしてください。これは、この ACI ファブリックに固有になります。

ステップ 2 メインのペインで、 ポッド内の**[+SR-MPLS L3Out の追加 (+Add SR-MPLS L3Out)]** をクリックします。

ステップ 3 右側の **[プロパティ (Properties)]** ペインで、SR-MPLS L3Out の名前を入力します。

ステップ 4 （任意）**[QoS ポリシー (QoS Policy)]** ドロップダウンで、MPLS トラフィックのために作成した QoS ポリシーを選択します。

SR-MPLS の カスタム QoS ポリシー を作成 （344 ページ）で作成した QoS ポリシーを選択します。

それ以外の場合、カスタムQoSポリシーを割り当てないと、次のデフォルト値が割り当てられます。

- 境界リーフ スイッチ上のすべての着信 MPLS トラフィックは、QoS レベル 3（デフォルトの QoS レベル）に分類されます。
- 境界リーフ スイッチは次の処理を実行します。
  - 再マーキングなしで SR-MPLS からのトラフィックの元の DSCP 値を保持します。
  - CoS 保存が有効な場合、テナント トラフィックの元の CoS 値を使用してパケットを MPLS ネットワークに転送します。
  - デフォルトの MPLS EXP 値 (0) のパケットを SR-MPLS ネットワークに転送します。
- また、境界リーフ スイッチは、SR ネットワークへの転送中に、アプリケーション サーバから着信するテナント トラフィックの元の DSCP 値を変更しません。

ステップ 5 **[L3 ドメイン (L3 Domain)]** ドロップダウンで、レイヤ 3 ドメインを選択します。

ステップ 6 境界リーフ スイッチと、SR-MPLS ネットワークに接続されているポートの設定を構成します。

境界リーフ スイッチについての情報、そして SR-MPLS ネットワークに接続されているインターフェイス ポートの情報を入力する必要があります。

a) **[+リーフの追加 (+Add Leaf)]** をクリックして、リーフ スイッチを追加します。

b) **[リーフの追加 (Add Leaf)]** ウィンドウで、**[リーフ名 (Leaf Name)]** ドロップダウンからリーフ スイッチを選択します。

c) **[SID 指数（SID Index）]** フィールド内で、有効なセグメント 識別子（SID）オフセットを入力します。

このセクションの後の部分で、インターフェイス ポートを設定する際には、セグメント ルーティングを有効にするかを選択できます。SID インデックスは、MPLS トランスポートループバックの各ノードで設定されます。SIDインデックス値はBGP-LUを使用してピア ルータにアドバタイズされ、ピア ルータはSIDインデックスを使用してローカル ラベルを計算します。セグメント ルーティングを使用する予定の場合には、この境界リーフのセグメント ID を指定する必要があります。

- 値は、先ほど設定した SRGB の範囲内である必要があります。
- この値は、サイト内のすべての SR-MPLS L3Out で選択したリーフスイッチで同じ必要があります。
- すべてのサイトの複数のリーフに同じ値を使用することはできません。
- 値を更新する必要がある場合は、まず、リーフ内のすべての SR-MPLS L3Out から値を削除し、設定を再展開する必要があります。その後、新しい値で更新し、新しい設定を再展開できます。

d) ローカルの **[ルータ ID (Router ID)]** を入力します。

ファブリック内で一意なルータ 識別子です。

e) **[BGP EVPN ループバック (BGP EVPN Loopback)]** アドレスを入力します。

BGP-EVPN ループバックが BGP-EVPN コントロール プレーン セッションに使用されます。このフィールドを使用して、境界リーフ スイッチの EVPN ループバックと DC-PE 間の MP-BGP EVPN セッションを設定し、オーバーレイ プレフィックスをアドバタイズします。MP-BGP EVPN セッションは、BGP -EVPN ループバックと BGP-EVPN リモート ピア アドレスの間で確立されます。このアドレスは、**[BGP-EVPN リモート IPv4 アドレス (BGP-EVPN Remote IPv4 Address)]** フィールドで設定します（前の **BGP 接続**のステップ）。

BGP-EVPN ループバックと MPLS トランスポート ループバックに異なる IP アドレスを使用できますが、ACI 境界リーフ スイッチの BGP-EVPN と MPLS トランスポート ループバックに同じループバックを使用することを推奨します。

f) **[MPLS トランスポート ループバック (MPLS Transport Loopback)]** アドレスを入力します。

MPLS トランスポート ループバックは、ACI 境界リーフ スイッチと DC-PE 間のデータ プレーン セッションを構築するために使用されます。MPLS トランスポート ループバックは、境界リーフ スイッチから DC-PE ルータにアドバタイズされるプレフィックスのネクスト ホップになります。

BGP-EVPN ループバックと MPLS トランスポート ループバックに異なる IP アドレスを使用できますが、ACI 境界リーフ スイッチの BGP-EVPN と MPLS トランスポート ループバックに同じループバックを使用することを推奨します。

g) **[インターフェイスの追加 (Add Interface)]** をクリックして、スイッチ インターフェイスの詳細を入力します。

[インターフェイスのタイプ (Interface Type)] ドロップダウンから、レイヤ 3 物理のインターフェイスなのか、それともポート チャネル インターフェイスなのかを選択します。ポート チャネル インターフェイスを使用する場合には、それ以前に APIC 上で作成しておく必要があります。

それからインターフェイス、その IP アドレス、および MTU サイズを入力します。サブインターフェイスを使用する場合には、サブインターフェイスの **[VLAN ID]** を入力します。それ以外の場合には [VLAN ID] フィールドはブランクのままにします。

[BGP ラベル ユニキャスト ピア IPv4 アドレス (BGP-Label Unicast Peer IPv4 Address)] および **[BGP ラベル ユニキャスト リモート AS 番号 (BGP-Label Unicast Remote AS Number)]** で、ネクスト ホップ デバイス（インターフェイスに直接接続されているデバイス）の BGP-LU ピア情報を指定します。

ネクスト ホップ アドレスは、インターフェイスで設定したサブネットの一部である必要があります。

MPLS または SR-MPLS ハンドオフを有効にするかどうかを選択します。

（任意）展開に基づいて追加の BGP オプションを有効にします。

最後に、**[インターフェイス タイプ (Interface Type)]** ドロップダウンの横にあるチェックマークをクリックして、、インターフェイス ポート情報を保存します。

h) MPLS ネットワークに接続されているスイッチのすべてのインターフェイスについて、前のサブステップを繰り返します。

i) **[保存 (Save)]** をクリックして、リーフ スイッチ情報を保存します。

j) MPLS ネットワークに接続されているすべてのリーフ スイッチについて、このステップを繰り返します。

ステップ 7 BGP 設定を構成します。

サイトの境界リーフ (BL) スイッチとプロバイダエッジ (PE) ルータ間の BGP EVPN 接続について、BGP 接続の詳細を指定する必要があります。

a) **[+BGP-EVPN 接続の追加（+Add BGP-EVPN Connectivity）]** をクリックします。

b) **[MPLS BGP-EVPN 接続の追加 (Add MPLS BGP-EVPN Connectivity)]** ウィンドウで詳細を入力します。

[MPLS BGP-EVPN ピア IPv4 アドレス (MPLS BGP-EVPN Peer IPv4 Address)] フィールドで、DC-PE ルータのループバック IP アドレスを入力します。このルータは必ずしも、境界リーフに直接接続されているデバイスとは限りません。

[リモート AS 番号 (Remote AS Number)] に、DC-PEのネイバー自律システムを一意に識別する番号を入力します。自律システム番号は 4 バイトで、1 ー 4294967295 のプレーン形式で指定します。ACIは `asplain` 形式のみをサポートし、`asdot` または `asdot+` 形式のAS番号はサポートしないことに注意してください。ASN形式の詳細については、『Explaining 4-Byte Autonomous System（AS）ASPLAIN and ASDOT Notation for Cisco IOS』を参照してください。

[TTL] フィールドで、境界リーフと DC-PE ルータ間の複数のホップ数を考慮に入れて、十分大きな値を指定します。たとえば `10` とします。許容範囲は `2 ー 255` ホップです。

（任意）展開に基づいて追加の BGP オプションを有効にします。

c) **[保存（Save）]** をクリックして BGP 設定を保存します。

d) 追加の BGP 接続があれば、このステップを繰り返します。

通常、2 つの DC-PE ルータに接続することになるので、両方の接続につてい BGP ピア情報を入力します。

ステップ 8 変更をサイトに展開します。

次のタスク

MPLS 接続を有効にして設定したら、SR-MPLS ルート マップ ポリシーの作成 （351 ページ）に説明されている方法で、テナント、ルートマップ、およびスキーマを作成し、管理することができます。

SR-MPLS ルート マップ ポリシーの作成

このセクションでは、ルートマップポリシーを作成する方法について説明します。ルートマップは、テナントSR-MPLS L3Outからアドバタイズされるルートを指定できる `if-then` ルールのセットです。ルートマップでは、DC-PE ルータから受信したどのルートを BGP VPNv4 ACI コントロールプレーンに挿入するかを指定することもできます。

SR-MPLS L3Out のサイト-ローカル設定を定義するときは、次のセクションで SR-MPLS ルート マップ ポリシーを使用します。

手順

ステップ 1 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 新しいテナント ポリシーを作成。

a) 左側のナビゲーション メニューで、**[アプリケーション管理（Application Management）]** > **[テナント ポリシー（Tenant Policies）]** を選択します。

b) **[テナント ポリシー テンプレート（Tenant Policy Template）]**ページ内で**[テナント ポリシー テンプレートを追加（Add Tenant Policy Template）]**をクリックします。

c) テナント ポリシー ページの右のプロパティ サイトバーにテナントの **[名前（Name）]** を入力します。

d) **[テナントの選択（Select a Tenant）]**ドロップダウンから、このテンプレートに関連付けるテナントを選択します。

次の手順で説明するようにテンプレートで作成したすべてのポリシーは、テンプレートを特定のサイトにプッシュすると、展開された選択したテナントに関連付けられます。

デフォルトでは、新しいテンプレートは空であるため、次のステップに従って 1 つ以上のテナント ポリシーを追加する必要があります。テンプレートで使用可能なすべてのポリシーを作成する必要はないことに注意してください。SR-MPLS のユース ケースに対して 1 つのルート マップ ポリシーだけでテンプレートを作成できます。

ステップ 3 ルート制御のルート マップ ポリシーを作成。

a) **[+オブジェクトの作成（+Create Object）]** ドロップダウンから、**[ルート コントロールのルート マップ ポリシー（Route Control Policy for Multicast）]** を選択します。

b) 右のプロパティのサイドバーでは、ポリシーの **[名前（Name）]** を指定します。

c) (オプション) **[説明を追加（Add Description）]** をクリックして、このポリシーの説明を入力します。

d) **[+エントリを追加（+Add Entry）]** をクリックして、ルート マップ情報を入力します。

ルート マップごとに、1 つ以上のコンテキスト エントリを作成する必要があります。次の情報によると各コンテキストは、1 つ以上の一致基準に基づいてアクションを定義するルールです：

- **コンテキストの順序** – コンテキストの順序は、コンテキストが評価される順序を決定するために使用されます。値は 0 ～ 9 の範囲内である必要があります。
- **コンテキスト アクション** – コンテキスト アクションは、一致が検出された場合に実行するアクションの 許可 または 拒否 を定義します。

コンテキストの順序とアクションを定義したら、コンテキストを一致させる方法を選択します。

- **[+ 属性の追加 (+Add Attibute)]** をクリックして、コンテキストが一致する必要があるアクションを指定します。

  次のアクションのうちの 1 つを選択できます。

  - コミュニティの設定
  - ルート タグの設定
  - ダンプニングを設定します
  - ウェイトの設定
  - ネクスト ホップの設定
  - プリファレンスの設定
  - メトリックの設定
  - メトリック タイプの設定
  - AS パス の設定
  - 追加のコミュニティを設定

  属性を構成したら、**[保存（Save）]**をクリックします。

- IP アドレスまたはプレフィックスに基づいてアクションを照合する場合は、**[IP アドレスの追加 (Add IP Address)]** をクリックします。

  [プレフィックス (prefix)] フィールドに、IP アドレス プレフィックスを入力します。IPv4 と IPv6 の両方のプレフィックスがサポートされています(例:2003:1:1a5:1a5::/64または205.205.0.0/16)。

  特定の範囲の IP を集約する場合は、**[集約 (aggregate)]** チェックボックスをオンにして、範囲を指定します。たとえば、0.0.0.0/0 プレフィックスを指定して任意の IP に一致させるか、10.0.0.0/8 プレフィックスを指定して任意の 10.xxx アドレスに一致させることができます。

- コミュニティリストに基づいてアクションを照合する場合は、**[コミュニティの追加 (Add community)]** をクリックします。

  [コミュニティ (Community)] フィールドに、コミュニティ文字列を入力します。たとえば、regular:as2-as2-nn2:200:300 などです。

次に、**[範囲（Scope）]**を選択します：推移性は、コミュニティがeBGPピアリング全体（自律システム（AS）全体）に伝播することを意味し、非推移性は、コミュニティが伝播しないことを意味します。

e) 前のサブステップを繰り返して、同じポリシーの追加のルート マップ エントリを作成します。
f) **[保存（Save）]** をクリックしてポリシーを保存し、テンプレート ページに戻ります。
g) この手順を繰り返して、ルート コントロール ポリシーの追加のルート マップを作成します。

ステップ 4 **[アクション（Actions）]** メニューから、**[サイトの関連付け（Sites Association）]** を選択し、このテンプレートを関連付ける SR-MPLS サイトを選択します。

ステップ 5 **[展開する（Deploy）]** をクリックして、テナント ポリシーをサイトに展開します。

EPG-to-External-EPG（North-South）通信を構成

このセクションでは、アプリケーションEPGと外部SR-MPLSネットワークとの間でNorth-South通信を確立する方法について説明します。また、このアプローチを使用して、SR-MPLS L3Outデータ パス（外部 SR-MPLS ネットワークを利用）を介したサイト間での EPG-to-EPG 通信を有効にすることもできます。

代わりに、リリース 4.0（2）からサポートされている ISN 全体の VXLAN データ プレーンを介して EPG から EPG へのサイト間接続を確立する場合は、EPG-to-EPG（East-West）通信の構成 の説明に従って、それらの EPG 間の契約関係を簡単に確立できます。

手順

ステップ 1 テンプレートを選択または、新しいのを作成します。

他の ACI ファブリックのユース ケースで通常行うように、テンプレートを選択できます。

a) メインのナビゲーション メニューで、**[Application Management (アプリケーション管理)]** > **[スキーマ (Schemas)]** を選択します。
b) 既存のスキーマを選択するか、新しいスキーマを作成します。
c) 既存のテンプレートを選択するか、**[新しいテンプレートの追加（Add New Template）]** をクリックして、テンプレート タイプとして `[ACI マルチクラウド（ACI Multi-Cloud）]` を選択します。
d) 新しいテンプレートのテナントを選択します。

テナントは SR-MPLS サイトに関連付けられている必要があります。

e) (オプション) このテンプレートを他のサイトへのサイト間接続を持たないサイトにのみ展開する予定の場合は、テンプレートの **[自律（Autonomous）]** オプションを有効にします。

ステップ 2 VRF を作成します。

a) **[+オブジェクトを作成（+Create Object）]** メニューから、**[VRF]** を選択します。
b) 右のプロパティのサイドバーでは、VRF の名前を指定します。

ステップ 3 SR-External EPG を作成します。

（注）
SR-External EPG を含むテンプレートを複数のサイトに割り当てると、EPG はそれらのすべてのサイトに拡張されます。この場合、各サイトにはローカル SR-MPLS L3Out が必要です。そうしないと、そのテンプレートを関連するすべてのサイトに展開できません。

a) **[+オブジェクトを作成（+Create Object）]** メニューから、**SR-External EPG** を選択します。
b) 右のプロパティのサイドバーでは、外部 EPG の名前を指定します。
c) [**仮想ルーティングと転送 (Virtual Routing & Forwarding)**] ドロップダウンから、前のステップで作成された VRF を選択します。

ステップ 4 SR-MPLS L3Out を作成します。

（注）
テナント SR-MPLS L3Out は、前の手順で作成した SR-External EPG と同じテンプレートで定義する必要があります。

a) **[+オブジェクトを作成（+Create Object）]** メニューから、**[SR-L3Out]** を選択します。
b) 右のプロパティのサイドバーでは、L3Out の名前を指定します。
c) [**仮想ルーティングと転送 (Virtual Routing & Forwarding)**] ドロップダウンから、前のステップの外部 EPG に対して選択した同じ VRF を選択します。
d) **[SR-External EPGs]** ドロップダウンから、前の手順で作成した SR-External EPG を選択します。

ステップ 5 構成する必要がある特定のユース ケースに応じて、テンプレートを 1 つのサイトまたは複数のサイトに割り当てます。

ステップ 6 構成しているテンプレートのサイトローカル設定を選択します。

次のいくつかの手順では、前の手順で作成した VRF および SR-External EPG および SR-MPLS L3Out のサイト ローカル設定を構成します。

ステップ 7 VRF のサイト ローカル設定を構成します。

SR-MPLS L3Out によって使用される VRF のための BGP ルート情報を設定する必要があります。

a) メインペインで **VRF** エリアにスクロールし、 前のステップで作成した VRF を選択します。
b) **[アドレス ファミリ (Address Family)]** ドロップダウンから、その IPv4 または IPv6 アドレスを選択します。
c) **[ルート ターゲット (Route Target)]** フィールドで、ルート文字列を設定します。

たとえば、`route-target:ipv4-nn2:1.1.1.1:1901` のようにします。

d) **[タイプ (Type)]** ドロップダウンで、ルートをインポートするのか、それともエクスポートするのかを選択します。
e) **[保存 (Save)]** をクリックして、ルート情報を保存します。
f) (オプション) このステップを繰り返して、その他の BGP ルート ターゲットを追加します。

ステップ 8 SR-MPLS L3Out のサイトローカル設定を構成します。

a) メインペインで、**[SR-Mpls L3Out]** エリアまで下にスクロールし、MPLS L3Out を選択します。

b) **[+ SR-MPLS Infra L3Out の追加（+Add SR-MPLS Infra L3Out）]** をクリックして、Infra SR-MPLS L3Out 情報を追加します。

c) **[SR-MPLS Infra L3Out の追加（Add SR-MPLS Infra L3Out）]** ウィンドウで、そのサイトのインフラを構成する際に作成した Infra SR-MPLS L3Out を選択します。

d) **[ルート マップ ポリシーの追加 (Add Route Map Policy)]** をクリックし、前のセクションで作成したルート マップ ポリシーをドロップダウンから選択し、ルートをインポートするかエクスポートをするかを指定します。

1 つのエクスポート ルート マップ ポリシーを設定する必要があります。オプションとして、追加のインポート ルート マップ ポリシーを設定することができます。

e) **[OK]**をクリックして、変更内容を保存します。

ステップ 9 通常のように、アプリケーション EPG を作成し構成します。

（注）
EPG は、同じまたは異なるテンプレートとスキーマにある可能性があります。

ステップ 10 アプリケーション EPG と SR-External EPG 間の契約を作成します。

ステップ 11 設定を展開する

a) [**スキーマ (Schemas)**] 表示のメイン ペインで、[**サイトに展開 (Deploy to Sites)**] をクリックします。

b) [**サイトに展開 (Deploy to Sites)**] ウィンドウで、サイトにプッシュされる変更を検証し、[**展開 (Deploy)**] をクリックします。

（注）
リリース 4.0（2）以降、従来の IP ベースの L3Out と同様に、North-South トラフィック（ACI ファブリックの外部の情報技術との通信）専用に EPG-to-SR-External-EPG コントラクトを使用できます。その場合、EPG 間の契約関係を作成するだけで、ISN 全体の VXLAN データ パスを介して EPG から EPG へのサイト間通信を有効にすることができます。

ただし、外部 SR-MPLS ネットワーク全体の異なるサイトにある EPG 間で EPG-to-EPG（East-West）通信を確立する場合は、次の手順で説明するように行うことができます。

ステップ 12 サイト間の EPG-to-EPG トラフィックに SR-MPLS L3Out データ パスを使用する場合（ISN 全体の VXLAN データ パスの代わりに SR-MPLS 外部ネットワークを利用）、各サイトローカル EPG 間で契約を確立できます。およびテナント SR-MPLS L3Out に関連付けられた SR-External EPG。

SR-External EPG は、各サイトのサイト ローカル オブジェクトとして、またはサイト全体のストレッチ オブジェクトとして展開できます。サイト間の EPG-to-EPG トラフィックに SR-MPLS L3out データ パスを使用できるのは、それらの EPG 間または各 EPG と他のリモート EPG 間に直接のコントラクト関係がない場合にのみ可能であることに注意してください。

a) 異なるサイトに関連付けられたテンプレートで通常行うように、2 つのアプリケーション EPG を作成します。

たとえば、`epg1` および `epg2` とします。

この EPG は、同じまたは異なる VRF またはテナントに含まれる場合があります。

b) 2 つの別個のサイトローカル SR-External EPG または単一の拡張 SR-External EPG を作成します。

個別の SR-External EPG を作成している場合、それらは、特定の展開シナリオに応じて、同じまたは異なる VRF またはテナントおよび同じテンプレートまたは異なるテンプレートにある可能性があります。

たとえば、 `mpls-extepg-1` および `mpls-extepg-2` とします。

c) 2 つの個別のサイトローカル テナント SR-MPLS L3Out または単一のストレッチ テナント SR-MPLS L3Out を設定します。

たとえば、`mpls-l3out-1` および `mpls-l3out-2` とします。

d) 各サイトのローカル EPG と SR-MPLS L3Out ローカル接続間のトラフィックを許可するために使用する契約を作成します。

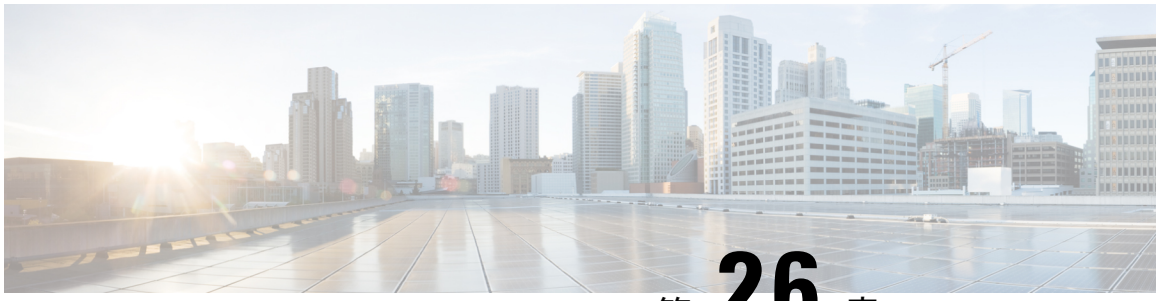
通常のように、コントラクトのためのフィルタを作成して定義する必要があります。

e) コントラクトを適切な EPG に割り当てます。

作成した 2 つのアプリケーション EPG 間のトラフィックを許可するため、実際にはコントラクトを 2 回割り当てる必要があります。`epg1` とその `mpls-extepg-1` の間、そして `epg2` とその `mpls-extepg-2` の間です。サイト間で拡張されている場合は、2 つの個別の EPG ではなく、同じ SR-External EPG を使用できることに注意してください。

例として、`epg1` が `epg2` にサービスを提供する場合、次のようにします。

- `epg1` にタイプ `consumer` でコントラクトを割り当てます。
- `mpls-l3out-1` にタイプ `consumer` でコントラクトを割り当てます。
- `epg2` にタイプ `consumer` でコントラクトを割り当てます。
- `mpls-extepg-2` にタイプ `consumer` でコントラクトを割り当てます。



第 26 章

vzAny コントラクト

vzAny および Multi-Site

vzAny管理対象オブジェクトは、各 EPG の個別のコントラクト関係を作成するのではなく、1 つまたは複数のコンテキストに仮想ルーティングと転送 (VRF) のすべてのエンドポイント グループ (EPG) を関連付ける便利な方法を提供します。

Cisco ACI ファブリックでは、コントラクトのルールにより、EPG は他の EPG としか通信できません。EPG とコントラクトの関係によって、EPG がコントラクトのルールに定義された通信を提供するのか、消費するのか、あるいは提供も消費も行うのかが指定されます。VRF 中のすべての EPG にコントラクトのルールを動的に適用することで、vzAny ではEPG とコントラクトとの関係を設定するプロセスが自動化されます。新しい EPG が VRF に追加されるたびに、vzAny コントラクト ルールが自動的に適用されます。vzAny と EPG の「1 対すべて」の関係は、コンテキスト中のすべての EPG にコントラクトのルールを適用するための最も効率的な方法です。

（注） L3Out に関連付けられ、VRF の一部である外部 EPG も vzAny 論理グループに含まれます。

利点

Cisco ACI のポリシー情報は、ファブリック スイッチの TCAM テーブルにプログラムされています。TCAMエントリは、一般的に、コントラクト経由で互いに通信することを許可する EPG

の各ペアに固有の特定のものです。このことは、同じコントラクトが再使用された場合でも、複数の TCAM エントリが EPG の各ペアに対して作成されることを意味します。

ポリシー TCAM テーブルのサイズは、使用しているスイッチの生成に応じて異なります。特定の大規模環境では、ポリシーTCAMの使用を考慮し、制限を超えないようにすることが重要です。

vzAny を使用すると、同じ VRF 内のすべての EPG を単一の「グループ」に結合し、単一の TCAM エントリのみを消費しながら、グループ内の個々の EPG ではなく、そのグループとのコントラクト関係を作成できます。これにより、TRF スペースだけでなく、VRF 内の個々の EPG の複数のコントラクト関係の作成に費やす時間を節約できます。

使用例

vzAny には次の 2 つの代表的な使用例があります。

- 自由な VRF 間通信 （363 ページ） に記載されているとおり、同じ VRF 内の EPG 間の自由な通信。
- 多対 1 の通信 （369 ページ） で詳細に説明するように、多 対 1 の通信により、同じ VRF 内のすべての EPG が単一の EPG から共有サービスを利用できるようになります。

vzAny およびマルチサイトのガイドラインと制限事項

vzAny を使用するときには、次の制約事項および使用上のガイドラインが適用されます。

- 特定の VRF の vzAny オブジェクトを有効にしてコントラクトを提供または消費することを計画している場合は、次の追加の制限が適用されます。
  - 特定の VRF の vzAny がコントラクト `c1` のコンシューマとして設定されている場合、他の VRF の vzAny オブジェクトを `c1` のプロバイダーとして設定してはなりません。
  - 特定の VRF の vzAny がコントラクト `c1` のプロバイダーとして設定されている場合、他の VRF の vzAny オブジェクトを `c1` のコンシューマとして設定してはなりません。
  - 特定の VRF の外部 EPG 部分がコントラクト `c1` を使用している場合、他の VRF の vzAny オブジェクトを `c1` のプロバイダーとして設定してはなりません。
  - 特定の VRF の EPG 部分がコントラクト `c1` を使用している場合、他の VRF の vzAny オブジェクトを `c1` のプロバイダーとして設定してはなりません。
  - 特定の VRF の vzAny が契約 `c1` のプロバイダーとして設定されている場合、EPG、外部 EPG、または他の VRF の vzAny オブジェクトを `c1` のコンシューマとして設定してはなりません。
- 特定の VRF の EPG および外部 EPG オブジェクトは、その VRF の vzAny がすでにコントラクトを使用または提供している場合、優先グループの一部として設定しないでください。

- 特定の VRF 内の EPG または外部 EPG オブジェクトがクラウド サイトに展開されている場合、その VRF の vzAny を設定してコントラクトを消費または提供することはできません。
- vzAny は、ファブリックが Cisco ACI 5.2(4) リリース以降を実行しているマルチサイト ドメインの一部である場合にのみ、VRF 間サイト間 L3Out 設定でサポートされます。
- vzAnyは、PBR でサービスグラフに関連付けられているコントラクトを、消費したり、または提供したりすることはできません。
- vzAnyは、VRF内通信を確立するためのコントラクトのプロバイダ、コンシューマ、または両方として設定できます。
- vzAnyは、共有サービスのコンシューマとしてのみサポートされていますが、プロバイダとしてはサポートされていません。
- VzAny VRF は、EPG とそれを使用する BD を導入する予定のすべてのサイトに拡張することをお勧めします。
- APIC から既存の vzAny 設定をインポートできます。

（注） 既存の問題 (CSCvt47568) が原因の特定の事例で、Nexus Dashboard Orchestrator から再展開する前にインポートされた設定を変更した場合、APIC で一部の変更が正しく更新されない場合があります。これを回避するには、インポート後すぐに設定を再展開してから、変更を加えます。変更されていない設定を再展開すると、通常どおりに更新できるようになります。

- vzAny プロバイダとコンシューマには、アプリケーション EPG、L3Outs に関連付けられた外部EPG、インバンドまたはアウトオブバンドアクセスのためのエンドポイントグループが含まれます。
- vzAny は、外部発信トラフィックの `0.0.0.0/0` 分類を暗黙に作成し、任意の外部 IP サブネットから発信されたすべてのトラフィックを許可します。VzAny が VRF に使用されている場合は、その VRF の L3Outs 部分に関連付けられた外部 EPG も含まれているため、VRF 自体で指定されたサブネットを含む L3external 分類を作成したことに相当します。
- VRF 内の EPG が別の VRF の EPG から共有サービス コントラクトを消費している場合、プロバイダ VRF の EPG からのトラフィックは、コンシューマー VRF 内でフィルタリングされます。vzAny は、送信元または宛先 EPG のワイルドカードに相当します。

  コンシューマ VRF の vzAny と別のプロバイダー VRF の EPG1 の間で共有サービス契約を設定する場合は注意してください。ポリシーの適用（フィルタリング）は常にコンシューマー VRF で実行されるため、プロバイダー VRF の一部である別の EPG2 に関連付けられたサブネットがコンシューマー VRF に漏洩した場合、EPG2 は、明示的にコントラクトを提供しなくても、VRF 全体でコンシューマー EPG との通信を開始します。このガイドラインに従わないと、VRF にわたる EPG 間での意図しないトラフィックが発生する可能性があります。

- 「Allow all」フィルタを使用して、コントラクトのプロバイダとコンシューマの両方として vzAny を使用した VRF を設定することは、非強制 VRF の設定と同じです。これは、その VRF 内のすべての EPG がコントラクトなしで相互に通信できることを意味します。
- コントラクトの範囲がアプリケーション プロファイルの場合、vzAny 設定は無視され、フィルタ ルールが拡張されます。CAM 使用率は、特定のコントラクトがコンシューマとプロバイダ EPG の各ペアの間に展開された場合と同じです。この場合、TCAM スペースの使用には利点がありません。
- 共有サービスの場合は、コンシューマ (vzAny) 側の宛先の分類 (`Pctag`) を適切に導出するために、EPG の下にプロバイダ EPG 共有サブネットを定義する必要があります。コンシューマとプロバイダの両方のサブネットがブリッジ ドメイン下で定義され、共有サービス コンシューマとして機能する vzAny に対して、BD から BD への共有サービス設定から移行する場合は、少なくとも共有フラグを使用してプロバイダ サブネットを EPG に追加する追加の設定手順を実行する必要があります。ただし、EPGの下のサブネットは接続に必要ではないため、常に `No default SVI gateway`フラグをチェックすることを推奨します。

  定義済みの BD サブネットの複製として EPG サブネットを追加する場合は、サブネットの両方の定義に同じフラグが定義されていることを確認してください。それをしない場合、エラーが発生する可能性があります。

コントラクトとフィルタの作成

vzAnyを使用するときは、基本的にコントラクト関係の単一のポイントを作成します。そのため、そのような関係とコントラクトのフィルタに使用する一般的なコントラクトが必要です。

このセクションでは、特別にこの目的の新しいコントラクトを作成する方法を説明します。代わりに、各 apic サイトで構成した既存のコントラクトのインポートを選択できます。

手順

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション ペインで、[**スキーマ (schema)**] を選択します。

ステップ 3 コントラクトを作成したいスキーマを選択します。

更新する既存のスキーマがある場合は、メイン ウィンドウペインでスキーマの名前をクリックするだけでかまいません。そうではない場合、新しいスキーマを作成する場合は、[**スキーマの追加 (Add Schema)**] ボタンをクリックして、いつも通り、名前やテナントなど、スキーマ情報を指定してください。

ステップ 4 フィルタを作成します。

a) **フィルタ** エリアまでスクロールし、+ をクリックしてフィルタを作成します。

b) コントラクトの名前を指定します。

c) **[+エントリ (+ Entry)]** をクリックし、フィルタ エントリを追加します。

d) [**エントリの追加 (Add Entry)**] ウィンドウでフィルタの詳細を入力します。

通常、許可するトラフィックの種類を定義する場合と同様に、フィルタの詳細を指定します。

e) **[保存 (SAVE)]** をクリックして、エントリを追加します。

f) (オプション) 必要な場合は、追加のフィルタ エントリを作成します。

ステップ 5 コントラクトを作成します。

a) **コントラクト** エリアまで下方へスクロールし、+ をクリックして新しいコントラクトを追加します。

b) コントラクトの名前を指定します。

例: `contract-vzany`。

c) コントラクトの範囲を選択します

使用例に適切な範囲を選択します。たとえば、クロステナント共有サービスを有効にする場合は、範囲を「`グローバル (Global)`」に設定します。

d) コントラクトが両方向に適用されるかどうかを選択します。

e) **[+フィルタ (+Filter)]** をクリックして、1 つ以上のコントラクト フィルタを追加します。

f) **[フィルタ チェーンの追加 (Add Filter Chain)]** ウィンドウで、前の手順で作成されたフィルタを選択します。

g) **[保存 (SAVE)]** をクリックして、フィルタを追加します。

h) (オプション) 必要な場合は、手順を繰り返してフィルタを追加します。

i) (オプション) **[両方向を適用 (Apply Both Directions)]** オプションを無効にする場合、コンシューマーとプロバイダの両方向にフィルタを提供します。

これで、次のセクションの vzAny で使用するコントラクトを作成しました。

コントラクトを消費または提供するための vzAny の設定

ここでは、vzAny VRF を作成する方法、または vzAny の既存の VRF を有効にする方法について説明します。

始める前に

次のものが必要です。

- コントラクトとフィルタの作成 （360 ページ）の説明に従って、vzAny で使用するコントラクトと1つ以上のフィルタを作成しました。

手順

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーション ペインで、[**スキーマ (schema)**] を選択します。

ステップ 3 VRF の定義を持つ特定のテンプレートを含むスキーマを選択します。

新しい設定の場合、[スキーマの追加（Add Schema）] ボタンを使用して新しいスキーマを作成し、VRF を設定できる新しいテンプレート（対象のテナントに関連付けられている）を定義できます。

ステップ 4 VRF を作成または選択します。

コントラクトを提供または消費するために vzAny を設定する既存の VRF がある場合は、メイン ウィンドウ ペインで [VRF] をクリックします。それ以外の場合は、新しい VRF を作成する場合、[**VRF**] エリアまで下にスクロールし、[+] 記号をクリックします。

ステップ 5 [vzAny] を選択します。

右側のサイドバーで、[**vzAny**] チェックボックスをオンにします。

ステップ 6 vzAny コントラクトを選択します。

[**+ Contract**] オプションは、[**vzAny**] チェックボックスを有効にすると使用可能になります。

a) [**+コントラクト (+Contract)**] をクリックし、新しいコントラクトを追加します。
b) コントラクトを選択します。

コントラクトとフィルタの作成 （360 ページ）で作成したコントラクトを選択します。

c) 契約タイプを選択します。

使用例に基づいて、契約のコンシューマまたはプロバイダのいずれかを選択できます。

vzAny VRF の一部として EPG を作成する

VzAny のユースケースには、新規作成するか、既存の EPG を使用するかを選択できます。EPG に明示的な vzAny 設定はなく、EPG が VRF の BD に関連付けられるとすぐに、EPG はその VRF（*vzAny* VRF）の vzAny 論理グループの一部になります。すでに作成され、構成されているすべての EPG に対して vzAny を有効にしているだけである場合は、このセクションをスキップすることができます。

始める前に

次のものが必要です。

- コントラクトとフィルタの作成 （360 ページ）の説明に従って、vzAny で使用するコントラクトと1つ以上のフィルタを作成しました。
- コントラクトを消費または提供するための vzAny の設定 （361 ページ） の説明に従って、vzAny VRF を作成してコントラクトに割り当てました。

手順

ステップ 1 vzAny VRF の一部として EPG を作成する場合

a) EPG に使用する BD を作成してください。
b) BD 構成サイドバーの [**Virtual Routing & Forwarding (仮想ルーティングと転送)**] ドロップダウンで、作成する vzAny VRF を選択します。
c) EPG を作成します。
d) EPG 設定サイドバーの [**Bridge Domain**(ブリッジ ドメイン)] ドロップダウンでは、作成する BD を選択します。

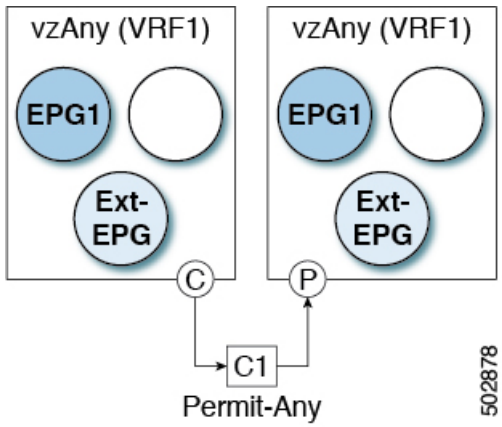
ステップ 2 vzAny VRF の一部として外部 EPG を作成する場合

a) 外部 EPG を作成します。
b) 外部 EPG 構成サイドバーの [**Virtual Routing & Forwarding (仮想ルーティングと転送)**] ドロップダウンで、作成する vzAny VRF を選択します。

自由な VRF 間通信

このセクションでは、制限の課されない VRF 間通信のための、様々なスキーマの例を示します。示されているすべてのシナリオにおいて、vzAnyは`permit any`フィルタを使用してコントラクトを提供し、消費します。これは基本的に、ポリシーを適用せずに ACI ファブリックをネットワーク接続に使用します。これは、*VRF* 非強制 オプションと同等です。

図 *36 :*



次のすべての使用例では、以下で要約されていものと同じ目的とポリシーを作成する必要があります。ただし、スキーマとテンプレート設計は、サイトの数だけではなく、拡大するオブジェクトに応じて異なります。以下の特定のセクションには、テンプレート レイアウトに関する推奨事項が含まれます。

手順

ステップ 1 スキーマを作成します。

ステップ 2 すべてのサイトにあるオブジェクトの構成を展開するために使用する共通のテンプレートを作成します（つまり *stretched objects*）。

ステップ 3 EPG が展開されるサイトのそれぞれの組み合わせに対して、追加のテンプレートを作成します。

1つのテンプレートをすべてのサイトに展開する場合は、この手順をスキップできます。このセクションの使用例のダイアグラムは、テンプレートの例を示します。

ステップ 4 共通テンプレート内で、vzAny によって消費/提供されるコントラクトとフィルタを作成します。

この特定の使用例では、コントラクトに 1 つの「permit-any」フィルタルールが必要です。

具体的な手順については、コントラクトとフィルタの作成 （360 ページ） を参照してください。

ステップ 5 共通テンプレート内で、VRF を作成し、「permit-any」ルールを使用して以前に定義されたコントラクトを消費して提供するように vzAny を設定します。

これにより、VRF 内の自由な通信を確立できるようになります。

具体的な手順については、コントラクトを消費または提供するための vzAny の設定 （361 ページ） を参照してください。

ステップ 6 各サイトのテンプレート内で、そのサイトにのみ展開される EPG を作成して設定します。

すべてのサイトに単一のテンプレートを展開する場合は、代わりに VRF と同じテンプレート内で EPG を作成します。このセクションの使用例のダイアグラムは、テンプレートの例を示します。

これについては、vzAny VRF の一部として EPG を作成する （362 ページ）で説明します。

ステップ 7 すべてのサイトに共通のテンプレートを割り当てます。

ステップ 8 各テンプレートを適切なサイトに割り当てます。

ステップ 9 テンプレートを展開します。

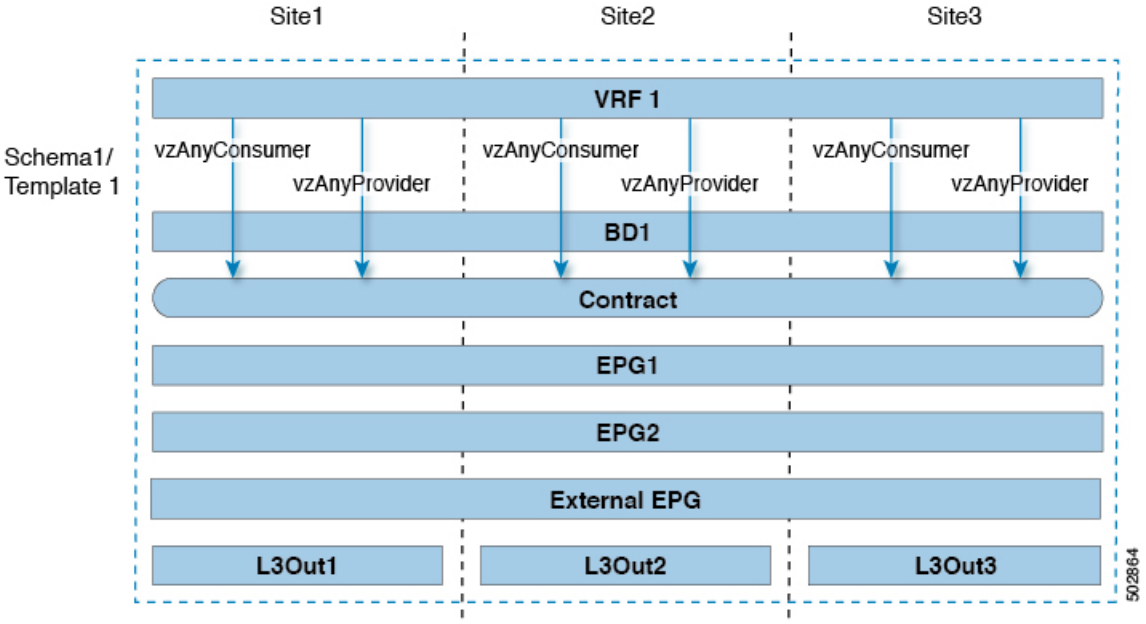
拡張された EPG

次の例は、EPG または外部 EPG の VRF 内通信を示し、それらのすべてはサイト間で拡張できます。この例では、EPG1 と EPG2 は同じ BD1 にマップされますが、両方の BD が VRF1 の一部である限り、それぞれが異なる BD の一部となる可能性があります。

このケースでは、同じテンプレート内のすべてのオブジェクトを作成し、テンプレートをすべてのサイトに展開できます。

（注） ベスト プラクティスとして、代わりに L3Out オブジェクトを Cisco APIC でのみ定義したままにするか、MSO でオンサイト ローカル テンプレートを設定することをお勧めします。

図 *37*:



サイトローカル EPG

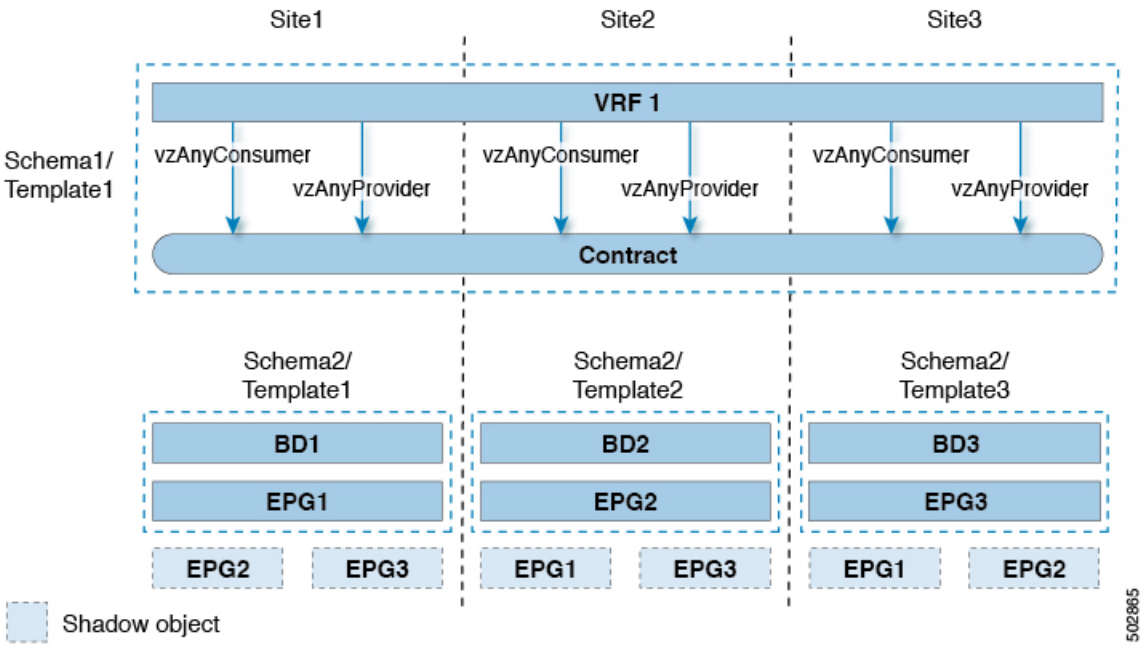
以下の例は、EPG または 外部 EPG 間の VRF 内通信を示しています。この場合、どの EPG も拡張されていませんが、vzAnyが「permit-any」コントラクトを消費して提供するため、相互に自由に通信できます。

この場合、複数のテンプレートを作成する必要があります。

- 各サイトに展開された共有オブジェクト (VRF、コントラクト) の単一のテンプレート。
- およびそのサイトに展開された EPG と BD を含むサイトごとの個別のテンプレート。

拡張されていないオブジェクトの場合は、シャドウ オブジェクトがほかのサイトで作成されます。

図 *38 :*



サイト ローカルおよび拡張 EPG の組み合わせ

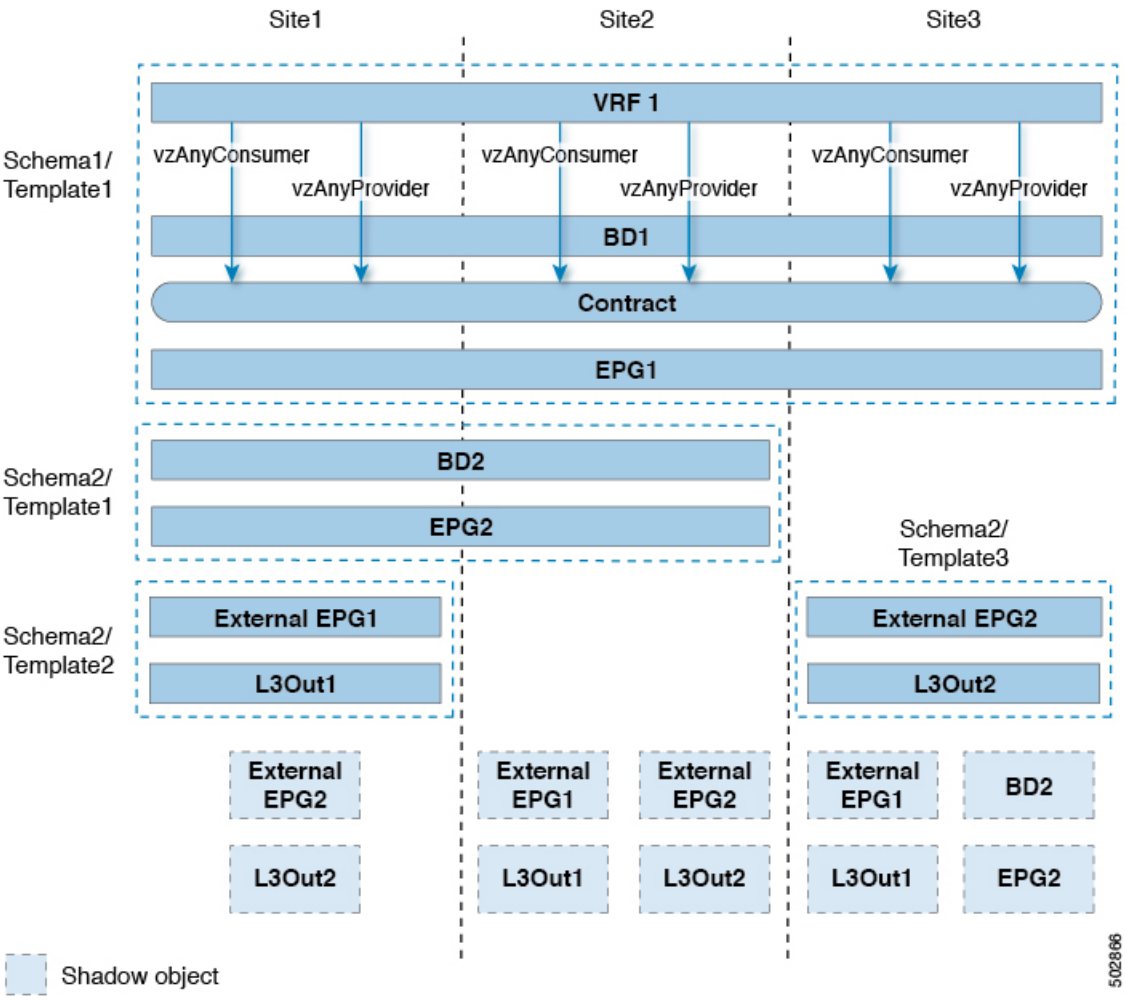
次の例は、EPG または 外部 EPG の間の VRF 内通信を示しています。一部の EPG は拡張されていますが、他のものは単一のサイトにのみ展開されます。それでも、すべての EPG は相互に自由に通信できます。vzAny は「すべて許可」のコントラクトを消費し、提供するからです。

この場合、複数のテンプレートを作成する必要があります。

- すべてのサイトに展開されている共有オブジェクト (VRF、コントラクト、BD) 用の単一のテンプレート。
- また、これらのサイトにのみ展開されたオブジェクトを含むサイトの組み合わせごとに個別のテンプレートがあります。

拡張されていないオブジェクトの場合は、シャドウオブジェクトがほかのサイトで作成されます。

図 *39 :*



VRF 内のサイト間 L3Out

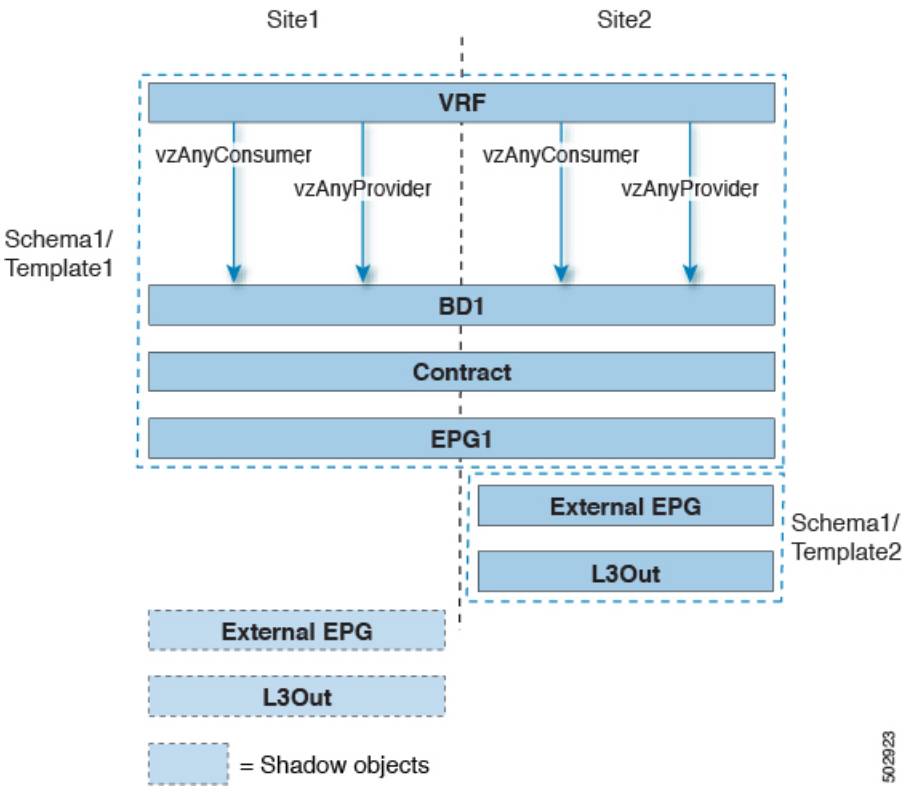
このユース ケースでは、1 つの vzAny VRF 内の複数の EPG 用に、サイト間 L3Out を設定できます。L3Out の外部 EPG が同じ VRF 内に存在する場合には、外部 EPG にプロバイダを明示的に追加する必要はありません。

この点を念頭に置くと、サイト間L3Outを設定する場合には、ポッドごとにルーティング可能な TEP を設定することが必要になります。追加のサイト間 L3Out の詳細と要件については、サイト間 L3Out の概要 （231 ページ） のセクションで説明されています。

この場合、次のように、複数のテンプレートを作成する必要があります。

- まず、1 つまたは複数のサイトに展開されている共有 vzAny オブジェクト (VRF、コントラクト、BD) 用の単一のテンプレートです。
- また、これらのサイトにのみ展開されたオブジェクトを含む、サイトの組み合わせごとの個別のテンプレートです。

図 *40 :*



上の図に示す構成に基づいて、拡張された EPG1 の一部であり、Site1 に接続されているエンドポイントは、Site2 に展開された L3Out 接続を介して外部ネットワーク ドメインと通信できます。同じことが、サイト 1 に展開されたサイトローカル EPG の一部であるエンドポイントにも当てはまります。

VRF 間 サイト間 L3Out

この使用例では、コンシューマー VRF と別のプロバイダー VRF の L3Out 外部 EPG との間の vzAny コントラクトを有効にすることができます。vzAny コンシューマー VRF の一部である複数の EPG は、提供 VRF で共有サービスを提供している単一の EPG と通信できます。 vzAny 契約は、VRF 内のすべての EPG の契約として機能します。参加している各 VRF および L3Out 外部 EPG は、サイト全体に拡張できます。

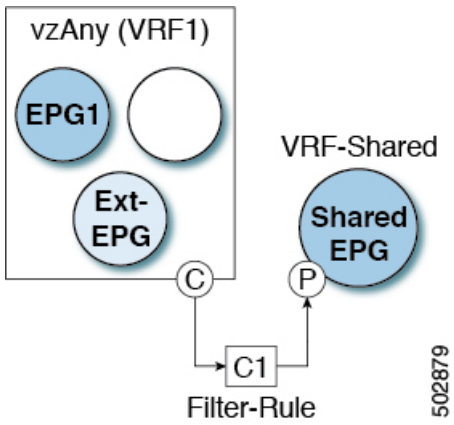
（注） VRF を vzAny プロバイダーにすることはできません。

多対 1 の通信

以下の 3 つのセクションでは、共有サービスを提供する単一の EPG との同じ vzAny VRF 通信の一部である、複数の EPG のスキーマの例を示します。この例では、1 つ以上のフィルタ ルールを指定できます。

共有サービスを提供する EPG は、個別の VRF 内のものであることも (下の図を参照)、vzAny VRF の一部であることも可能です。

図 *41 :*



次のすべての使用例では、以下で要約されていものと同じ目的とポリシーを作成する必要があります。ただし、スキーマとテンプレート設計は、サイトの数だけではなく、拡大するオブジェクトに応じて異なります。以下の特定のセクションには、テンプレート レイアウトに関する推奨事項が含まれます。

手順

ステップ 1 スキーマを作成します。

ステップ 2 すべてのサイトにあるオブジェクトの構成を展開するために使用する共通のテンプレートを作成します（つまり *stretched objects*）。

ステップ 3 EPG が展開されるサイトのそれぞれの組み合わせに対して、追加のテンプレートを作成します。

ステップ 4 共通テンプレート内で、vzAny によって消費され、共有サービスを提供する EPG によって提供される、コントラクトとフィルタを作成します。

これについては、コントラクトとフィルタの作成 （360 ページ）で説明します。

ステップ 5 共通テンプレート内で、VRF を作成し、前に定義したコントラクトを消費してするよう vzAny を設定します。

これについては、コントラクトを消費または提供するための vzAny の設定 （361 ページ）で説明します。

ステップ 6 各サイトのテンプレート内で、vzAny VRF の一部となる EPG を作成して設定します。

これについては、vzAny VRF の一部として EPG を作成する （362 ページ）で説明します。

ステップ 7 プロバイダ EPG を新規作成して設定するか、既存のプロバイダ EPG または外部 EPG を設定します。

プロバイダ EPG の新規作成と設定、既存のプロバイダ EPG または外部 EPG の設定は、通常どおりの方法で行います。

ステップ 8 プロバイダ EPG にコントラクトを割り当てます。

vzAny が消費するコントラクトの割り当てに加えて、同じコントラクトをプロバイダ EPG に割り当てることも必要になります。

VzAny VRF 内のプロバイダ EPG

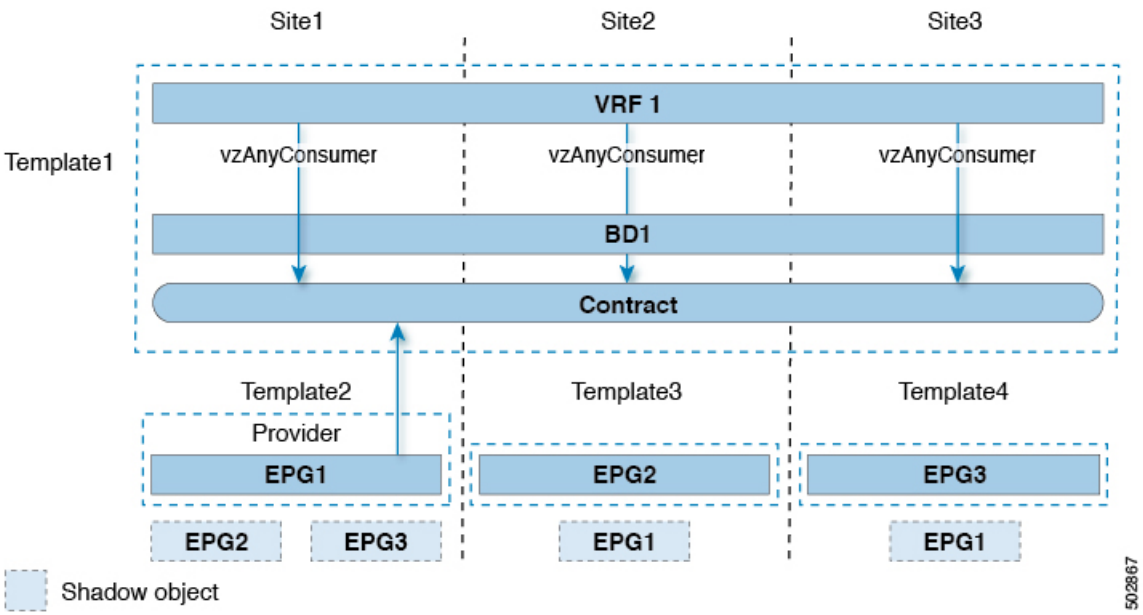
次の例は、単一のプロバイダ EPG (たとえば、共有サービス) と、同じ VRF 内の他のすべての EPG 間のサービスを消費する VRF 間の通信を示しています。

この場合、複数のテンプレートを作成する必要があります。

- すべてのサイトに展開されている共有オブジェクト (VRF、コントラクト、BD) 用の単一のテンプレート。
- また、これらのサイトにのみ展開されたオブジェクトを含むサイトの組み合わせごとに個別のテンプレートがあります。

次の図は、1つのストレッチ VRF/BD の設定を示しています。代わりに、EPG ごとに専用 BD を設定してマッピングすることもできます。その場合は、シャドウ BD がリモートサイトに展開されます。

図 *42 :*



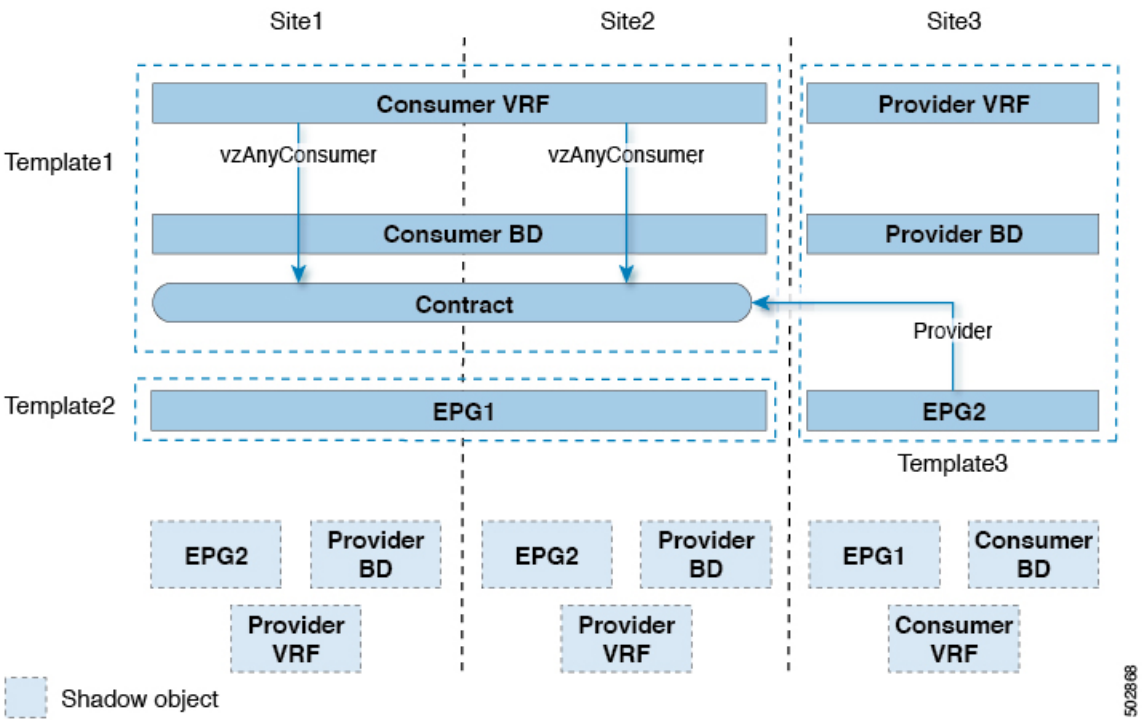
独自の VRF でのプロバイダ EPG

次の例は、独自の VRF 内の単一の EPG (たとえば、共有サービス プロバイダ) と、異なる vzAny VRF 内のすべての EPG との間の通信を示しています。プロバイダ EPG は、vzAny VRF のコンシューマ EPG と同じサイトまたは別のサイトに展開できます。

この場合、次のように、複数のテンプレートを作成する必要があります。

- まず、1 つまたは複数のサイトに展開されている共有 vzAny オブジェクト (VRF、コントラクト、BD) 用の単一のテンプレートです。
- また、これらのサイトにのみ展開されたオブジェクトを含む、サイトの組み合わせごとの個別のテンプレートです。

図 *43 :*


Site1
Site2
Site3
Consumer VRF
Provider VRF
Template1
vzAnyConsumer
vzAnyConsumer
Consumer BD
Provider BD
Contract
Provider
Template2
EPG1
EPG2
Template3
EPG2
Provider BD
EPG2
Provider BD
EPG1
Consumer BD
Provider VRF
Provider VRF
Consumer VRF
Shadow object
502868

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。