『Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics、Release 3.6（x）』

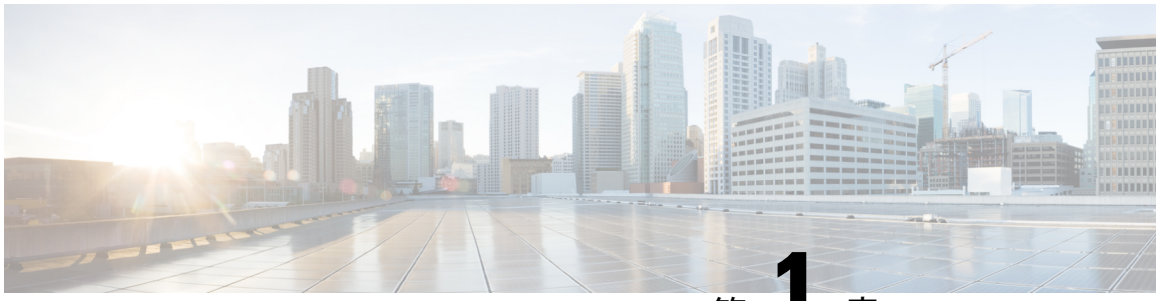
初版：2021 年 10 月 3 日

最終更新：2022 年 3 月 21 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

新機能および変更された機能に関する情報

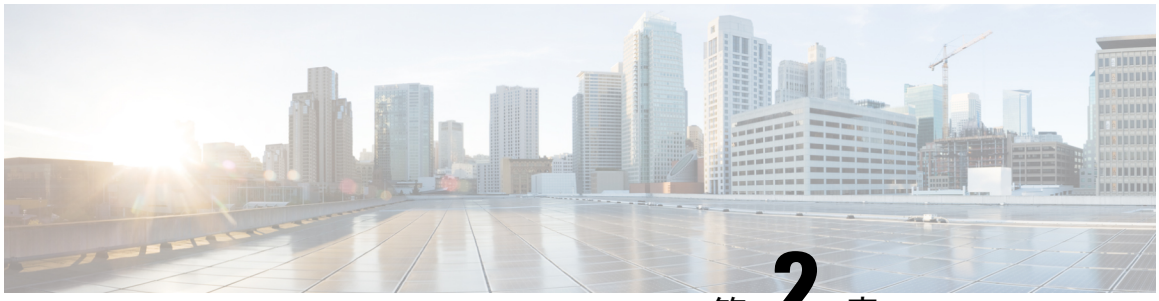
新機能および変更された機能に関する情報

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
3.6(1)	Cisco Data Center Network Manager（DCNM）は、リリース 12.0.1a 以降、Cisco Nexus Dashboard Fabric Controller（NDFC）に名前が変更されました。	--
3.6(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 2 章

GUI の概要

概要

Nexus Dashboard Orchestrator (NDO) GUI はブラウザ ベースのグラフィカル インターフェイスで、Cisco APIC、クラウド APIC、およびDCNM の展開を設定し、監視できます。

GUI は、機能に応じて配置されています。たとえば、**[ダッシュボード (Dashboard)]** ページには、ファブリックとそのヘルスの概要が表示されます。**[サイト (sites)]** ページでは、各サイトに関する情報が提供され、サイトを追加できます。**[スキーマ (schema)]** ページでは、スキーマの作成と設定を行うことができます。各 NDO GUI ページの機能については、次のセクションで説明されています。

各ページの上部には、動作しているコントローラの数を示すコントローラ ステータス、および **[開始 (Get Started)]** メニュー アイコン、**[設定]** アイコン、**[ユーザ]** アイコンが示されます。

[開始 (Get Started)] メニューは、サイトまたはスキーマの追加、特定のポリシーの設定、管理タスクの実行など、実行する可能性のある多数の一般的なタスクへの簡単なアクセスを提供します。

[設定 (Settings)] アイコンを使用すると、現在実行中のバージョン、現在のリリースの最新情報、API ドキュメント、システム ステータスなど、Nexus Dashboard Orchestrator の概要情報にアクセスできます。

- **[NDOについて (About NDO)]** リンクには、現在インストールされている Nexus Dashboard Orchestrator のバージョンに関する情報が表示されます。

- **[このリリースの最新情報 (What's New in This Release)]** リンクをクリックすると、お使いのリリースの新機能の概要や、Nexus Dashboard Orchestrator の他のドキュメントへのリンクが表示されす。
- **[API ドキュメント (API Docs)]** リンクをクリックすると、一連の Swagger API オブジェクトとメソッドの参照にアクセスできます。Swagger API の使用の詳細については、『*Cisco ACI Multi-Site REST API* 設定ガイド』を参照してください。
- **[システム ステータス (System Status)]**リンクは、NDOで使用されているすべての実行中のサービスのステータスと正常性を提供します。

[ユーザー (User)] アイコンを使用すると、設定やブックマークなど、現在ログインしているユーザーに関する情報を表示できます。また、Orchestrator GUI からログアウトすることもできます。

（注） リリース3.2（1）以降、ユーザ管理は、NDOサービスが実行されているNexusダッシュボードの共通ユーザおよび認証管理に移動しました。

- **[設定 (Preferences)]**リンクを使用すると、いくつかの GUI オプションを変更できます。
- **[ブックマーク (Bookmarks)]** リンクをクリックすると、Orchestrator の使用中に保存したすべてのブックマークされたスキーマのリストが開きます。スキーマを表示または編集する際に、画面の右上隅にあるブックマークアイコンをクリックして、スキーマをブックマークすることができます。

ファブリックオブジェクトを使用すると、オブジェクトが表示されるたびに、Orchestrator の GUI 全体で **[表示名 (Display Name)]** フィールドが使用されます。オブジェクトの作成時に表示名を指定できますが、サイトコントローラ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ます。結果として得られた**内部名**が、オブジェクトをサイトに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、通常、**[表示名 (Display Name)]** テキストボックスの下に表示されます。

ダッシュボード

Nexus Dashboard Orchestrato ダッシュ ボードには、現在の機能と健全性だけでなく、サイトの実装のすべてのリストが表示されます。

ダッシュボードには次の機能領域があります:

- **サイトのステータス**: サイトのステータスのテーブルには、名前と場所に従ってサイトの一覧が表示されます。このテーブルには、わかりやすいカラーコードによって、実装の現在の健全性も表示されます。
  - [Controller State] カラムには、使用可能および実行中のコントローラの数が表示されます。複数サイトの実装では、最大で 3 つのコントローラを設定できます。たとえば、3 つのコントローラのうち 1 つがダウンしている場合には、2/3 として表示されます。

- [Connectivity] カラムには、BGP セッションの動作ステータスとデータプレーン ユニキャスト、およびダッシュボードの各サイトでピア サイトに接続されているマルチキャスト トンネルが示されます。

  1 つ以上の BGP セッションまたはトンネル確立に失敗した場合、 Multi-Site は、BGP セッションまたはトンネル確立に失敗したのがどのローカル スパインとリモート スパインであるかについての情報を提供します。Multi-Site は、インフラストラクチャ構成内のサイトを有効にします。ピア サイトへの BGP セッションとデータプレーン ユニキャストおよびマルチキャスト トンネルが確立されるようにするためです。

  BGP セッション

  - BGP ピアリングタイプが **Infra**-> **General Settings** でフル メッシュになっている場合、BGP ピアリングを有効にしたサイトのスパイン ノードは、すべてのピア サイト内で BGP ピアリングが有効にされているすべてのスパイン ノードに対して BGP セッションを確立します。
  - BGP ピアリングタイプが **Infra**-> **General Settings**, でルート リフレクタになっている場合、BGP ピアリングとルート リフレクタの両方を有効にしたサイトのスパイン ノードは、すべてのピア サイト内で BGP ピアリングが有効にされているすべてのスパイン ノードに対して BGP セッションを確立します。ルート リフレクタ モードでは、少なくともローカル スパイン ノードまたはリモート スパイン ノードまたはその両方で、ルートリフレクタを有効にする必要があります。そうしないと、それらの間で BGP セッションは確立されません。
  - ローカルおよびリモート ASN が異なる場合は、eBGP になります。したがって、それらのサイト間のセッションは、BGP ピアリング タイプとルート リフレクタの構成に関係なく、常にフル メッシュとなります。

  ユニキャストおよびマルチキャスト トンネル: ISN に接続し、インフラストラクチャ構成を持つサイトのスパイン ノードは、ピア サイトで ISN に接続しているすべてのスパイン ノードに対してトンネルを確立します。

  カラー コードは、次の条件を示します。

  - **重大** (赤色)
  - **メジャー** (オレンジ色)
  - **マイナー** (黄色)
  - **警告** (緑色)

  色インジケータ カラムの番号は、サイトごとの障害の数を示しています。

- **Schema Health**: ロケールと健全性のスキーマの一覧を提供します。
  - 対象のスキーマを検索するには、虫めがねアイコンをクリックし、スキーマ名を入力します。
  - **[+]** 記号をクリックして、サイトへの新しいスキーマの追加を開始できます。

- スキーマの詳細とテンプレートのステータスを表示するには、**[スキーマ正常性(Schema Health)]** テーブルのサイト ロケールをクリックします。

  Schema Health テーブルはヒート マップタイプの表示になっています。対象としているスキーマの健全性が、色に従って表示されます。2 つのカラム (つまり、ロケール) にまたがっているスキーマは、拡大状態であることを示しています。

  - 色によって強調表示されたセルをクリックすると、対象とするスキーマにどのようなポリシーが組み込まれているかをより詳細に確認できます。スキーマの詳細ページでは、矢印をクリックしてスキーマ ビルダーに移動し、対象とするスキーマのポリシーの詳細を更新できます。
  - 色分けスライダーを使用すると、健全性をさらにレビューすることが必要なスキーマを、範囲を選択して識別できます。たとえば、スライダーの値を80～100の間に調整することができます。その後、指定した範囲に含まれるスキーマの実装を、付随する [Schema Health] テーブルで表示できます。

[アプリケーション管理 (Application Management)] > [テナント (Tenants)] ページ

Multi-Site **Tenants** ページには、実装を構成しているすべてのテナントが一覧表示されます。

Tenants ページのテーブルには、以下の項目が表示されます:

- テナント名
- 割り当て先サイト
- 割り当て先ユーザ
- 割り当て先スキーマ
- アクション

このページの特徴と機能としては、次のものがあります:

- **Name**: テナント名をクリックすると、**Tenant Details** の設定にアクセスできます。**Tenant Details** ページでは、次のセクションの編集や更新を行えます:
  - **General Settings**: 必要に応じて、表示名と説明を変更します。
  - **Associated Sites**: 対象のテナントと関連付けられているサイトを表示します。
  - **Associated Users**: 対象のテナントと関連付けられているユーザを表示します。ユーザ名の隣にあるボックスをオンにすれば、ユーザを対象のテナントと関連付けることができます。

- **Associated Schemas**: **Associated Schema** の一覧をクリックすると、対象のテナントに関連付けられたスキーマが表示されます。
- **Actions**: **Actions** の一覧をクリックすると、対象テナントの詳細サイトの編集や、新しいネットワーク マッピングの作成を行えます。

（注） **Delete** を **Actions** ドロップダウン メニューから選択すれば、テナントを削除することができます。

- **Add Tenant: Add Tenant** ボタンをクリックすると、実装内容に既存のテナントを追加できます。それから [Tenant Details] ページでは、テナント名、説明、セキュリティ ドメイン、および関連付けられているユーザを追加できます。

監査ログ

をクリックして、 **監査ログ** にアイコン、 **スキーマの追加** スキーマ ページのログの詳細を一覧表示するには、タブ。**[監査ログ：テナント リスト (Audit Logs: Tenants List)]** ページが表示されます。

ページの表には、次の詳細情報が表示されます：

- **日付**
- **アクション**
- **詳細**
- **ユーザ**

[最新 (Most Recent)] タブをクリックすると、特定の期間の監査ログを選択できます。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。

[**フィルタ (Filter)**] アイコン ([**最新 (Most Recent)**] タブの隣) をクリックすれば、次のような基準に基づいてログの詳細のフィルタ処理を行うことができます:

- [**ユーザ (User)**]:あるユーザまたはすべてのユーザを選択して [**適用 (Apply)**] をクリックすると、ユーザ名に基づいてログの詳細のフィルタ処理を行えます。
- [**アクション (Action)**]: アクションを選択します。たとえば作成、更新または削除を行って [**適用 (Apply)**] をクリックすると、そのアクションに従ってログの詳細のフィルタ処理を行えます。

詳細については、テナント （13 ページ）の章を参照してください。

[アプリケーション管理(ApplicationManagement)]>-[スキーマ (Schemas)] ページ

[スキーマ (Schemas)] ページでは、すべての実装に関連付けられているスキーマを一覧表示します。

特定のスキーマを検索するには、虫めがねと関連付けられているフィールドを使用します。スキーマを設定に使用するか、VRF、EPG を持つアプリケーション プロファイル、フィルタおよびコントラクト、ブリッジ ドメイン、外部 EPG を含むテナント ポリシーをインポートします。

スキーマの表では、次の情報が表示されます。

- **名前**: スキーマ名をクリックすると、件名スキーマの設定を表示または更新します。
- **テンプレート**: スキーマに使用されるテンプレートの名前が表示されます。テンプレートは、グループ ポリシーである ACI コンテキストのプロファイルと同様です。ストレッチ オブジェクトまたは特有のオブジェクトのテンプレートを作成することができます。
- **テナント**: 件名スキーマに使用されるテナントの名前が表示されます。
- **アクション**: 関連付けられるスキーマを持つ **[アクション]** フィールドをクリックして、件名スキーマを編集または削除します。

[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追加できます。これについては、このドキュメントの後のセクションで詳しく説明します。

監査ログ

をクリックして、 **監査ログ** にアイコン、 **スキーマの追加** スキーマ ページのログの詳細を一覧表示するには、タブ。[**監査ログ**：**スキーマ リスト**] ページが表示されます。

ページの表には、次の詳細情報が表示されます：

- **日付**
- **アクション**
- **詳細**
- **ユーザ**

[最新 (Most Recent)] タブをクリックすると、特定の期間の監査ログを選択できます。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。

[**フィルタ (Filter)**] アイコン ([**最新 (Most Recent)**] タブの隣) をクリックすれば、次のような基準に基づいてログの詳細のフィルタ処理を行うことができます:

- [**ユーザ (User)**]:あるユーザまたはすべてのユーザを選択して [**適用 (Apply)**] をクリックすると、ユーザ名に基づいてログの詳細のフィルタ処理を行えます。
- [**アクション (Action)**]: アクションを選択します。たとえば作成、更新または削除を行って [**適用 (Apply)**] をクリックすると、そのアクションに従ってログの詳細のフィルタ処理を行えます。

[アプリケーション管理 (Application Management)] > [ポリシー (Policies)] ページ

Nexus Dashboard Orchestrator の **[ポリシー (Policies)]** ページには、ファブリック用に設定したすべてのポリシーが表示されます。

[ポリシー (Policies)] ページには、すべてのポリシーのテーブルとともに、それらのタイプの概要、関連付けられているテナント、説明、および使用方法が表示されます。このページを使用して、新しいポリシーを追加したり、既存のポリシーを編集したりすることができます。

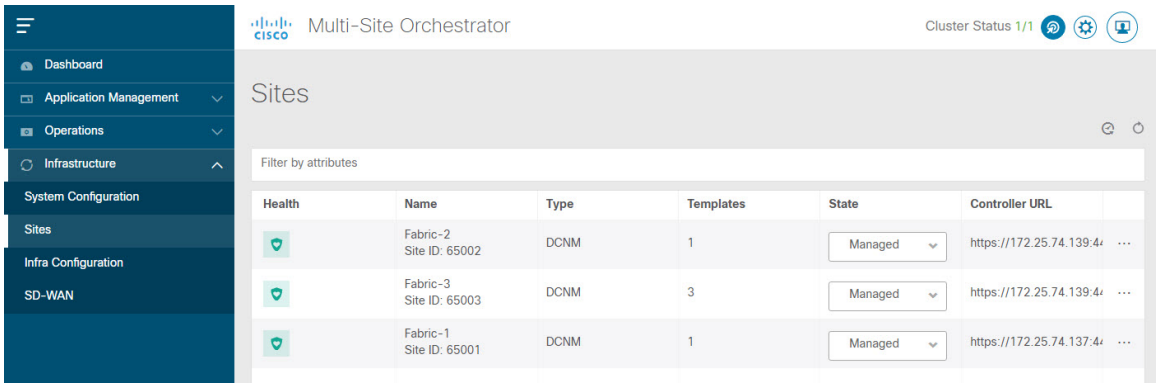
以下のポリシーを設定できます。

- DHCPポリシー（DHCPリレー （187 ページ）章で説明）。
- MPLS QoSポリシー（SR-MPLS 経由で接続されたサイト （299 ページ）章で説明）。
- ルート マップ ポリシー（SR-MPLS 経由で接続されたサイト （299 ページ）章で説明）。
- マルチキャスト ルート マップ ポリシー（レイヤ 3 マルチキャスト （251 ページ）章で説明）。

[インフラストラクチャ (Infrastructure)] > [サイト (Sites)] ページ

NDO の**[インフラストラクチャ (Infrastructure)]** > **[サイト (Sites)]** ページには、実装されているすべてのサイトが表示されます。次のようなものがあります。

図 *1:* マルチサイトの *[Sites]* ページ



[サイト (Sites)] ページには、次の情報が含まれます。

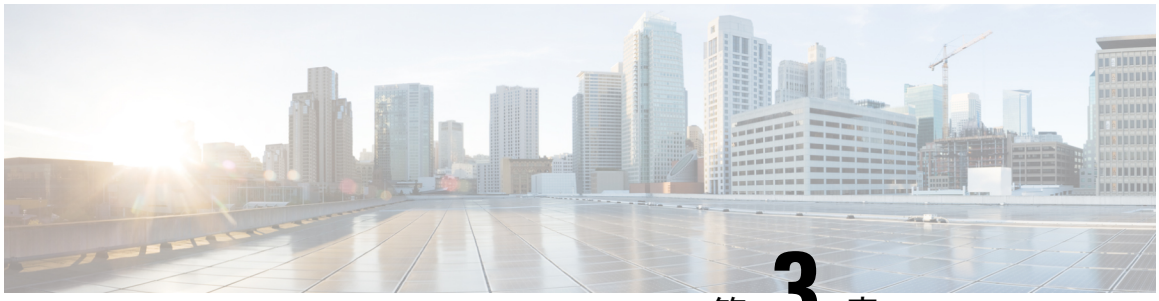
- **[サイトの正常性 (Site Health)]** は、次の色分けされた識別子に従って、サイトの全体的な正常性のステータスを示します。
  - **重大** (赤色)
  - **メジャー** (オレンジ色)
  - **マイナー** (黄色)
  - **警告** (緑色)
- **[サイト名 (Site Name)]** には、サイトの追加時に定義したサイトの表示名が表示されます。
- **[サイトのタイプ (Site Type)]** には、ACI や DCNM などのファブリック タイプが表示されます。
- **[テンプレート (Templates)]** 列には、サイトに関連付けられているテンプレートの数が表示されます。
- **[状態 (State)]** 列は、この特定のファブリックがNDOによって管理されているかどうかを示します。

  Nexus Dashboard GUI でサイトとそのプロパティを追加し、管理します。NDO の **[サイト (Sites)]** ページには、Nexus Dashboard GUI で使用可能なすべてのサイトが表示され、NDO で管理する特定のサイトを定義できます。
- **[コントローラ URL (Controller URL)]** 列には、サイトのコントローラのインバンド IP アドレスが表示されます。
- アクション メニュー（**...**）では、サイトのテナント（ACIファブリックのみ）をインポートしたり、サイトのコントローラ UI を開いたりできます。

特定のサイトをクリックすると、右側の **[プロパティ (Properties)]** サイドバーが開き、サイトに関する追加情報を表示できます。

第 I 部

アプリケーション管理およびファブリックリソース



第 3 章

テナント

テナント

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。

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。

次の 3 つの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 DCNM 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 DCNM ファブリックを管理する場合は、事前に設定されているデフォルトの `dcnm-default-tn` を使用し、次のオブジェクトを作成および管理できます。

- VRF

- ネットワーク

テナントの追加

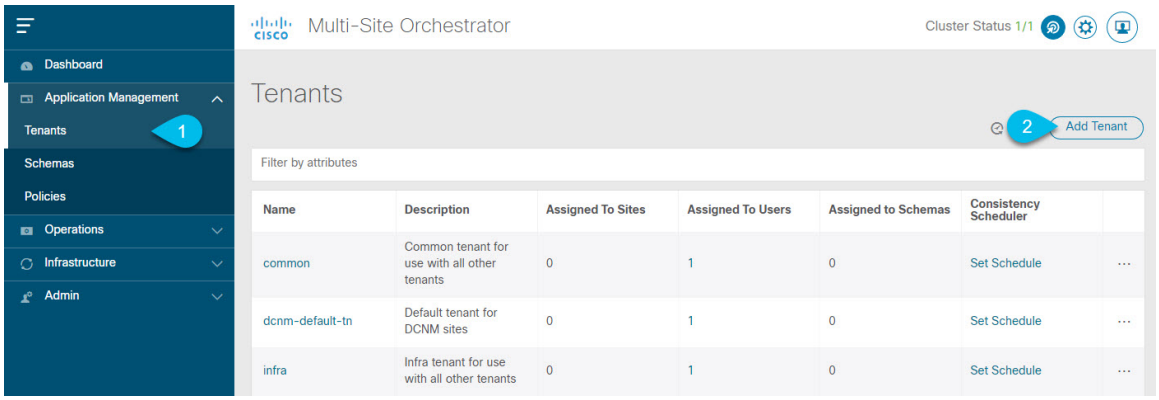
このセクションでは、Nexus Dashboard Orchestrator GUI を使用してテナントを追加する方法について説明します。

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。

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

ステップ 2 テナントを追加します。



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)]** > **[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。

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と、使用する **[セキュリティドメイン (Security Domain)]** 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。

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。

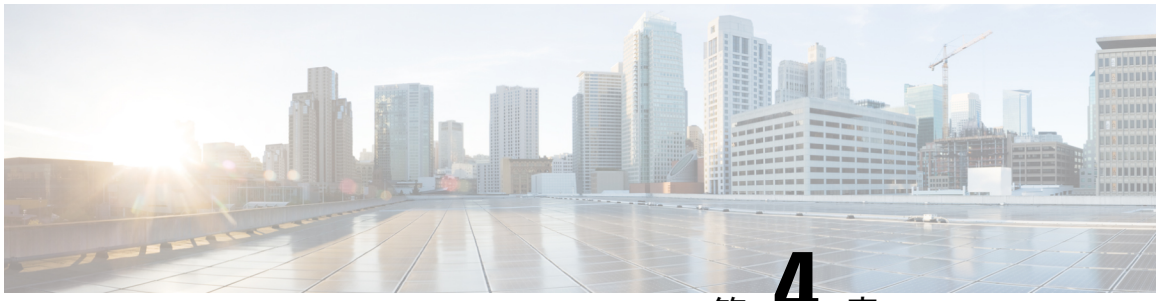
c) **[関連付けられたユーザー (Associated Users)]** セクションで、テナントへのアクセスが許可されているNexus Dashboard Orchestratorユーザーを選択します。

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。

d) (オプション) 整合性チェッカ スケジューラを有効にします。

これにより、定期的な整合性チェックを有効にできます。整合性チェッカ機能の詳細については、*Cisco Multi-Site Troubleshooting Guide* を参照してください。

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。



第 4 章

スキーマ

Schema Design Considerations

A schema is a collection of templates, which are used for defining policies, with each template assigned to a specific tenant. There are multiple approaches you can take when it comes to creating schema and template configurations specific to your deployment use case. The following sections describe a few simple design directions you can take when deciding how to define the schemas, templates, and policies in your Multi-Site environment.

Keep in mind that when designing schemas, you must consider the supported scalability limits for the number of schemas, templates, and objects per schema. Detailed information on verified scalability limits is available in the *Cisco Multi-Site Verified Scalability Guides* for your release.

単一スキーマの展開

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。

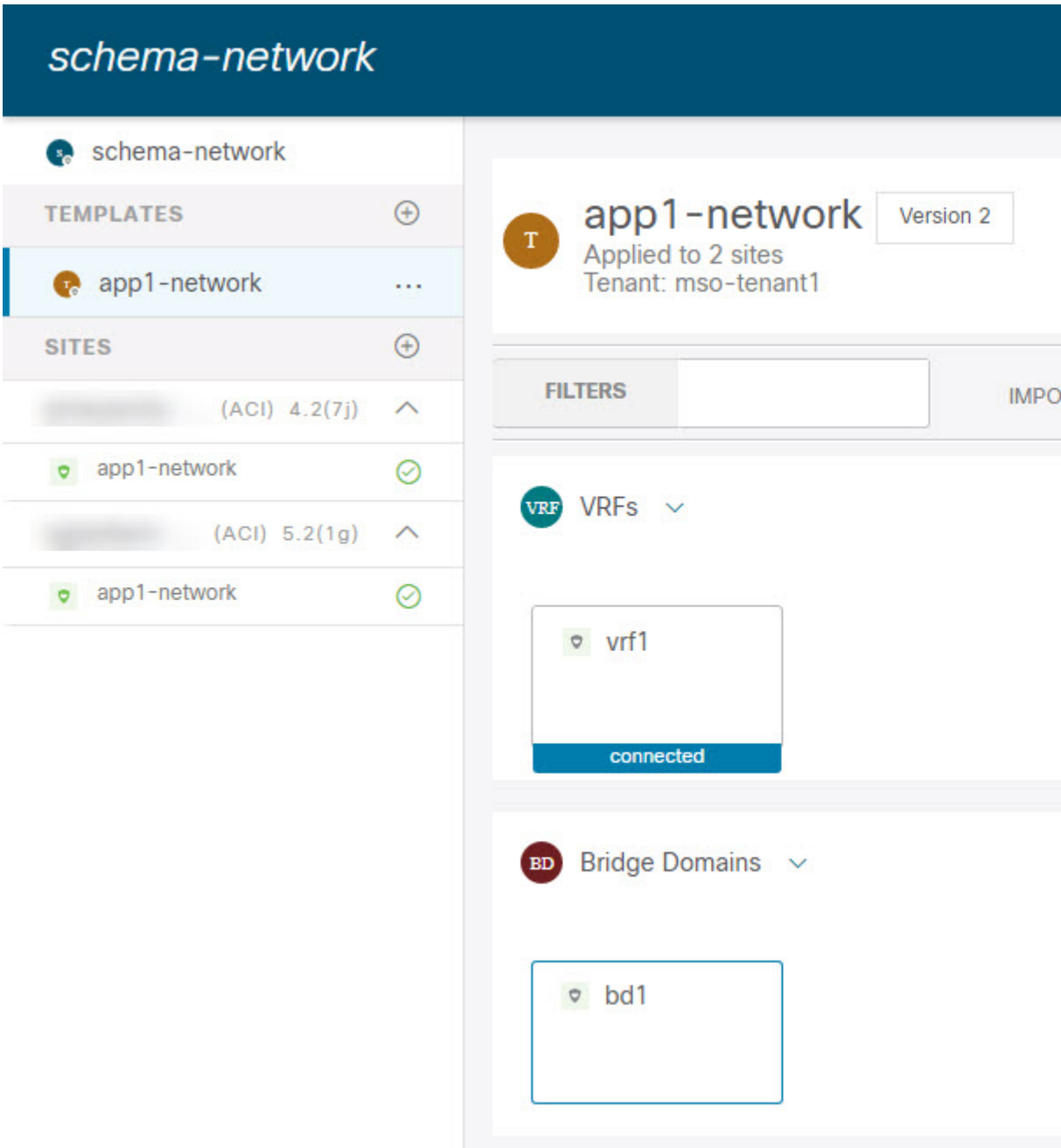
ネットワーク分離での複数スキーマ

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。

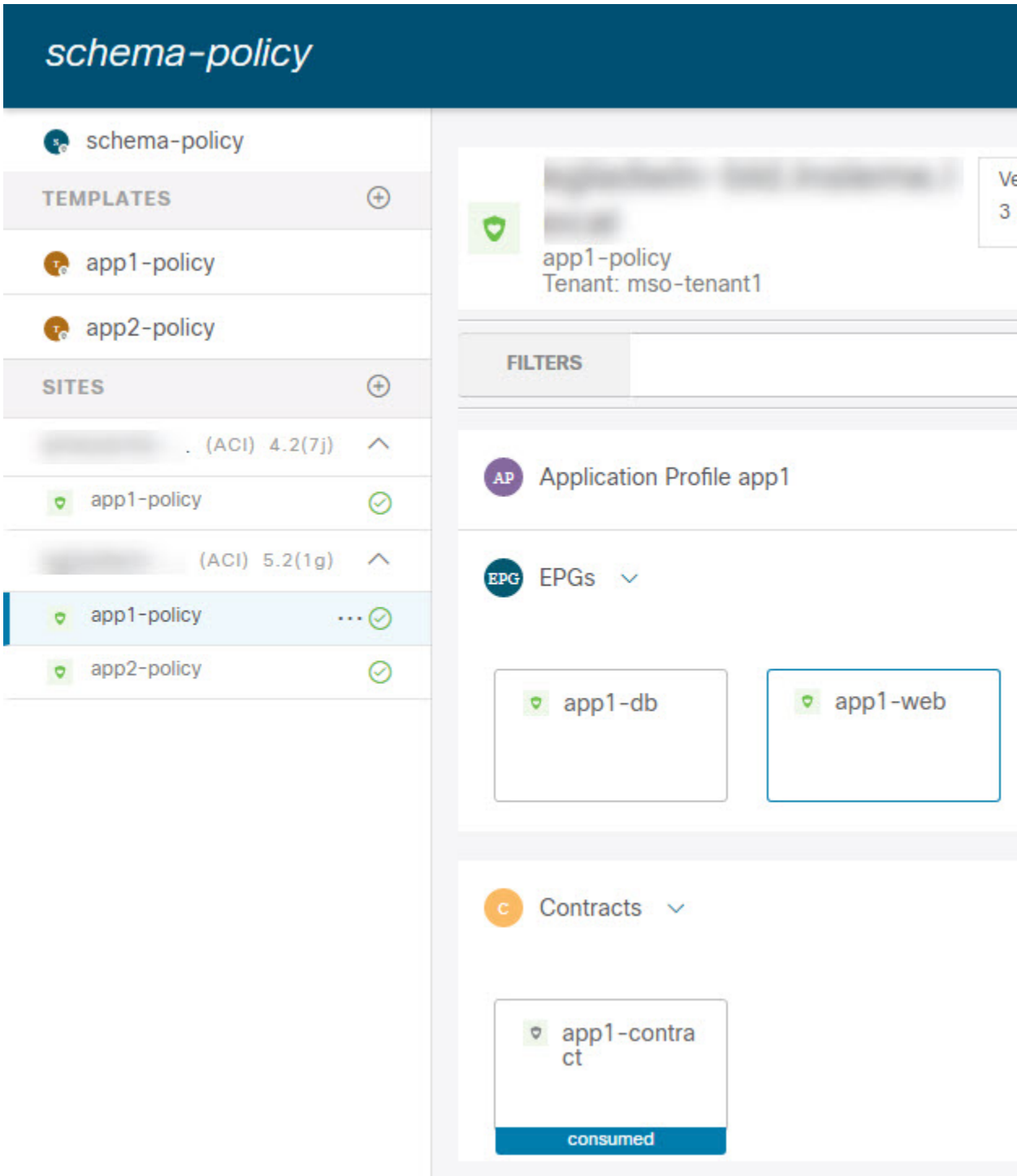
次の図は、VRF、BD、およびサブネットが設定され、2 つのサイトに展開されている単一のネットワーキング テンプレート設定を示しています。

図 *2*: ネットワーク スキーマ



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。次の図に、2つのアプリケーションテンプレートを含むポリシースキーマを示します。これらのテンプレートの両方が外部スキーマのネットワーキング要素を参照しています。アプリケーションの一方は1つのサイトにローカルであり、他方は2つのサイト間で拡張されます。

図 *3:* ポリシー スキーマ



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

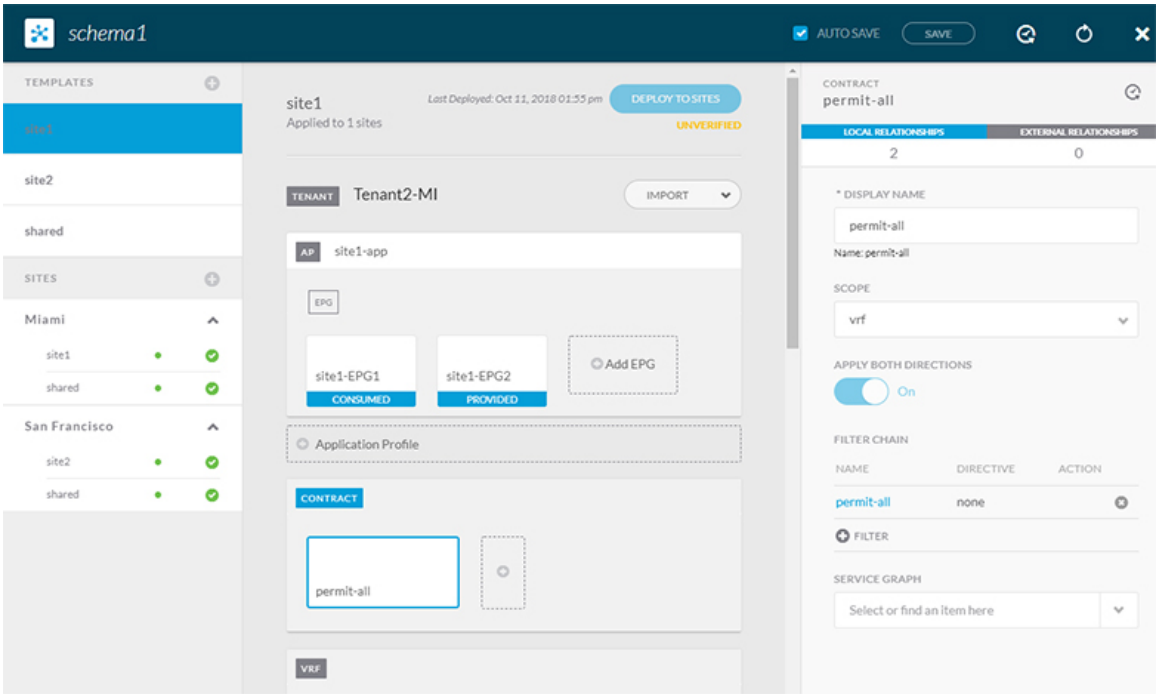
照を含むオブジェクトは、上のネットワーク スキーマの図に示すように、リボンのアイコンでも示されます。

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。

Multiple Schemas Based On Object Relationships

When configuring multiple schemas with shared object references, it is important to be careful when making changes to those objects. For instance, making changes to or deleting a shared networking object can impact applications in one or more sites. Because of that, you may choose to create a template around each individual site that contains only the objects used by that site and its applications, including the VRFs, BDs, EPGs, Contracts, and Filters. And create different templates containing the shared objects.

Figure 4: One Template per Site



The **site1** template in the above figure contains only the objects that are local to Site1 and the template is deployed to only the Miami site. Similarly, the **site2** template contains only the object relevant to site2 and is deployed to the San Francisco site. Any change made to any object in either of these templates has no effect on the other one. The **shared** template contains objects that are shared between the sites.

You can extend this scenario for an additional site with the following template layout:

- Site 1 template
- Site 2 template
- Site 3 template
- Site 1 and 2 shared template

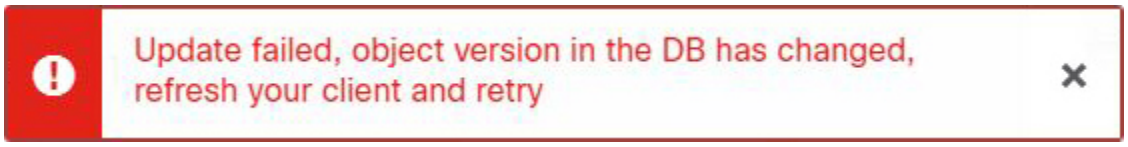
- Site 1 and 3 shared template
- Site 2 and 3 shared template
- All shared template

Similarly, rather than separating objects based on which site they are deployed to, you can also choose to create schemas and templates based on individual applications instead. This would allow you to easily identify each application profile and map them to schemas and sites as well as easily configure each application as local or stretched across sites.

However, as this could quickly exceed the templates per schema limit (listed in the Verified Scalability Guide for your release), you would have to create additional schemas to accommodate the multiple combinations. While this creates additional complexity with multiple additional schemas and templates, it provides true separation of objects based on site or application.

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"
}
```

Creating Schemas and Templates

Before you begin

- You must have an administrative user account with full read/write privileges.
- You must have a user account with read/write tenant policy privileges.

  For more information, see the *User Access, Authentication, and Accounting* chapter in the *Cisco APIC Basic Configuration Guide*.
- You must have at least one available tenant that you want to incorporate into your site.

  For more information, refer to テナントの追加, on page 14.

ステップ 1 Log in to your Nexus Dashboard and open the Nexus Dashboard Orchestrator service.

ステップ 2 Create a new schema.

a) From the left navigation pane, choose **Application Management** > **Schemas**.
b) On the Schemas page, click **Add Schema**.
c) In the schema creation dialog, provide the **Name** and optional description for the schema.

   By default, the new schema is empty, so you need to add one or more templates.

ステップ 3 Create a template.

a) In the left sidebar under **Templates**, click the + sign to add a new template.
b) In the **Select a Template type** window, choose **ACI Multi-Cloud** for the template type.

   - **ACI Multi-Cloud**—Templates used for Cisco ACI on-premises and cloud sites, which allow template and object stretching between multiple sites.

     The following sections focus primarily on this type of template.

- **Networking**—Templates designed for Cisco Nexus Dashboard Fabric Controller (formerly Data Center Network Manager) sites.

  This guide described Nexus Dashboard Orchestrator configurations for Cisco ACI and cloud ACI sites. For information on working with Cisco NDFC sites, see the *Cisco Nexus Dashboard Orchestrator Configuration Guide for DCNM Fabrics* instead.

- **SR-MPLS**—Template designed for SR-MPLS integration.

  For detailed information on the SR-MPLS use case, see "SD-WAN Integration" chapter of this guide.

- **Cloud Local**—Templates designed for specific Cisco Cloud ACI use cases, such as Google Cloud site connectivity, and cannot be stretched between multiple sites.

c) In the right sidebar, specify the **Display Name**.
d) (Optional) Provide a **Description**.
e) If you are configuring an SR-MPLS template, enable the **SR-MPLS** knob.

   For detailed information on SR-MPLS templates, see SR-MPLS 経由で接続されたサイト, on page 299.

f) From the **Select a Tenant** dropdown, select the Tenant for this template.

   Keep in mind, the user account you're using to create a new schema must be associated with the tenant you are trying to add to it, otherwise the tenant will not be available in the drop-down menu. Associating a user account with a tenant is described in テナントの追加, on page 14.

ステップ 4 Assign the templates to sites.

You deploy one template at a time, so you need to associate the template with at least one site where you want to deploy the configuration.

a) In the left pane, click the + icon next to Sites
b) In the **Add Sites** window, check the checkbox next to the sites where you want to deploy the template.
c) From the **Assign to Template** dropdown next to each site, select one or more templates.

   While you deploy one template at a time to every site with which it is associated, you can associate multiple templates to a site at once.

d) Click **Save**.

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、Multi-Site 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。

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

Creating Schemas and Templates （24 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。

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 （251 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 （319 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

- Creating Schemas and Templates （24 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 （27 ページ）の説明に従って VRF を作成する必要があります。

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。

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 （251 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。
- [フラッドの最適化 (Optimize 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。
- [フラッドの最適化 (Optimize 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 ゲートウェイ設定から NDO 統合 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）**[DHCP ポリシー (DHCP Policy)]** を追加します。

詳細については、DHCPリレー （187 ページ） を参照してください。

ステップ 6 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（32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 （28 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。

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、サイト内 L3Out （201 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。

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

Creating Schemas and Templates （24 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。

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、Configuring Contracts and Filters （38 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 （251 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 優先グループ （197 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 （35 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 （33 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。

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) **[保存（Save）]** をクリックします。

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。

Configuring Contracts and Filters

This section describes how to configure a contract, a filter, and assign the filter to the contract. A filter is similar to an Access Control List (ACL), it is used to filter traffic through contracts associated to EPGs.

ステップ 1 Select the schema and template where you want to create contract and filter.

You can create the contract in the same or different template as the objects (EPGs and external EPGs) to which you will apply it. If the objects that will use the contract are deployed to different sites, we recommend defining the contract in a template associated to multiple sites. However, this is not strictly required and even if the contract and filters are defined only as local objects in Site1, NDO will create those objects in a remote Site2 when a local EPG or external EPG in Site2 needs to consume or provide that contract.

ステップ 2 Create a filter.

a) In the main pane, select **+Create Object** > **Filter**.

Alternatively, you can scroll down to the **Filters** area, mouse over the tile, and click **Add Filter**.

b) In the right pane, provide the **Display Name** for the filter.
c) (Optional) Provide a **Description**.

ステップ 3 Create a filter entry.

a) In the right pane, click **+ Entry**.

The filter entry is a combination of network traffic classification properties. You can specify one or more options as described in the following step.

b) Provide the **Name** for the filter.
c) Choose the **Ether Type**.

For example, `ip`.

d) Choose the **IP Protocol**.

For example, `icmp`.

e) Choose the **Destination Port Range From** and **Destination Port Range To**.

The start and end of the destination ports range. You can define a single port by specifying the same value in both fields or you can define a range of ports from `0` to `65535`. You can also choose to specify one of the server types instead of specific port numbers, for example `http`.

f) Enable **Match only fragments** option.

When enabled, the rule applies to any IP fragment with an offset that is greater than `0` (all IP fragments except the first). When disabled, the rule will not apply to IP fragments with an offset greater than `0` because TCP/UDP port information can only be checked in initial fragments.

g) Enable **Stateful** option.

When this option is enabled, any traffic coming from the provider back to the consumer will always have to have the `ACK` bit set in the packet or else the packets will be dropped.

h) Specify **ARP flag** (Address Resolution Protocol).

The **ARP Flag** is used when creating a specific filter for ARP and allows you to specify ARP request or ARP reply.

i) Choose the **Source Port Range From** and **Source Port Range To**.

The start and end of the source ports range. You can define a single port by specifying the same value in both fields or you can define a range of ports from `0` to `65535`. You can also choose to specify one of the server types instead of specific port numbers, for example `http`.

j) Specify **TCP session rules**.

TCP session rules are used when creating a filter for TCP traffic and allow you to configure `stateful` ACL behavior.

k) Click **Save** to save the filter.
l) Repeat this step to create any additional filter entries for this filter.

You can create and assign multiple filter entries for each filter.

ステップ 4 Create a contract

a) In the main pane, select **+Create Object** > **Contract**.

Alternatively, you can scroll down to the **Contract** area, mouse over the tile, and click **Add Contract**.

b) In the right pane, provide the **Display Name** for the contract.
c) (Optional) Provide a **Description**.
d) Select the appropriate **Scope** for the contract.

Contract scope limits the contract's accessibility; the contract will not be applied to any consumer EPG outside the scope of the provider EPG:

- `application-profile`
- `vrf`
- `tenant`
- `global`

e) Toggle the **Apply both directions** knob if you want the same filter to apply for both consumer-to-provider and provider-to-consumer directions.

If you enable this option, you will need to provide the filters only once and they will apply for traffic in both directions. If you leave this option disabled, you will need to provide two sets of filter chains, one for each direction.

Note If you create and deploy a contract with **Apply both directions** enabled, you cannot simply disable the option and re-deploy for the change to apply. To disable this option on an already deployed contract, you must delete the contract, deploy the template, then re-create the contract with the option disabled to correctly change the setting in your fabrics.

f) (Optional) From the **Service Graph** dropdown, select a service graph for this contract.
g) (Optional) From the **QoS Level** dropdown, select a value for this contract.

This value specifies the ACI QoS Level that will be assigned to the traffic using this contract. For more information, see IPN 全体での QoS の保持, on page 263.

If you leave this at `Unspecified`, the default QoS Level 3 is applied to the traffic.

ステップ 5 Assign the filters to the contract

a) In the right pane, scroll down to the **Filter Chain** area and click **+ Filter** to add a filter to the contract.
b) In the **Add Filter Chain** window that opens, select the filter you added in previous step from the **Name** dropdown menu.
c) Select the **Action** for the filter.

When adding filters, you can choose whether to permit or deny traffic that matches the filter criteria. For `deny` filters, you can set the priority of the filter to one of four levels: `default`, `low`, `medium`, or `high`; the `permit` filters always have the default priority. For more information on ACI contracts and filters, see *Cisco ACI Contract Guide*.

d) Click **Save** to add the filter to the contract.
e) If you disabled the `Apply both directions` option on the contract, repeat this step for the other filter chain.
f) (Optional) You can create and assign multiple Filters to each Contract.

If you want to create additional filter for the same contract:

- Repeat Step 2 and Step 3 to create another filter along with its filter entries.

• Then repeat this step to assign the new filter to this Contract.

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

- Creating Schemas and Templates （24 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 （27 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。

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。

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。

c) **[+ コントラクト (+ 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 優先グループ （197 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

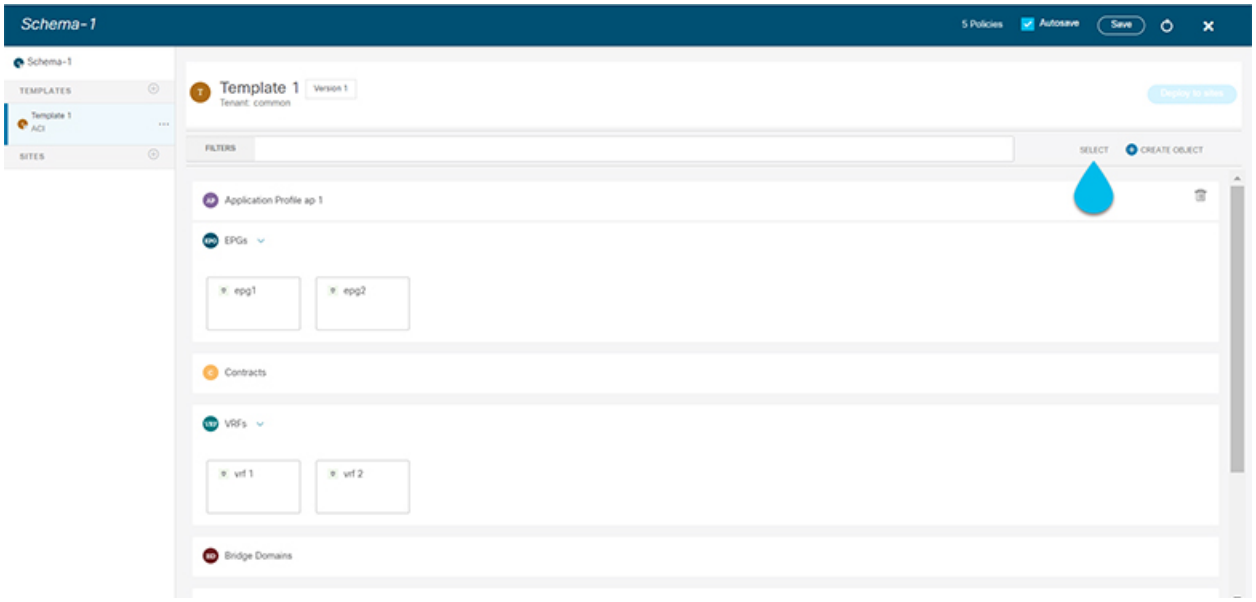
一括更新機能を使用すると、テンプレート内の同じタイプの複数の異なるオブジェクトの複数のプロパティを一度に更新できます。たとえば、各オブジェクトを個別に変更する代わりに、同時に 2 つ以上の EPG にインフラ EPG 分離を適用できます。このワークフローを使用する場合、選択したすべてのオブジェクトは同じタイプである必要があります。たとえば、EPG と BD を同時に更新することはできません。

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 DCNM ファブリックでのみサポートされています。 Cisco Cloud APIC サイトではサポートされていません。

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に移行します。

ステップ 2 右上のペインから、「選択」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。

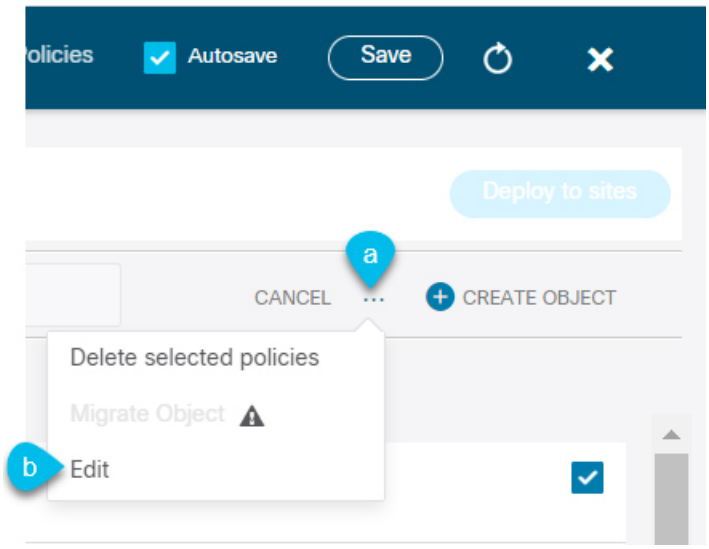


ステップ 3 更新するすべてのオブジェクトを選択した後。

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」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。

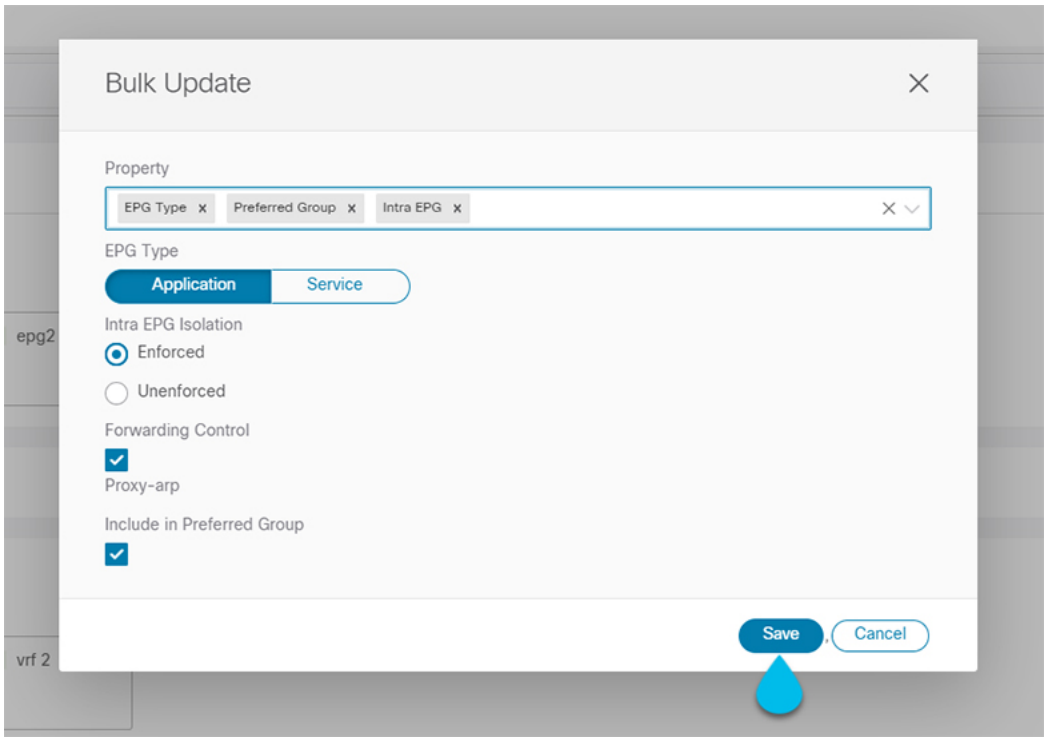


ステップ 4 [編集（Edit）] を選択すると、ポップアップが表示されます。選択したオブジェクトのプロパティのサブセットが表示されます。

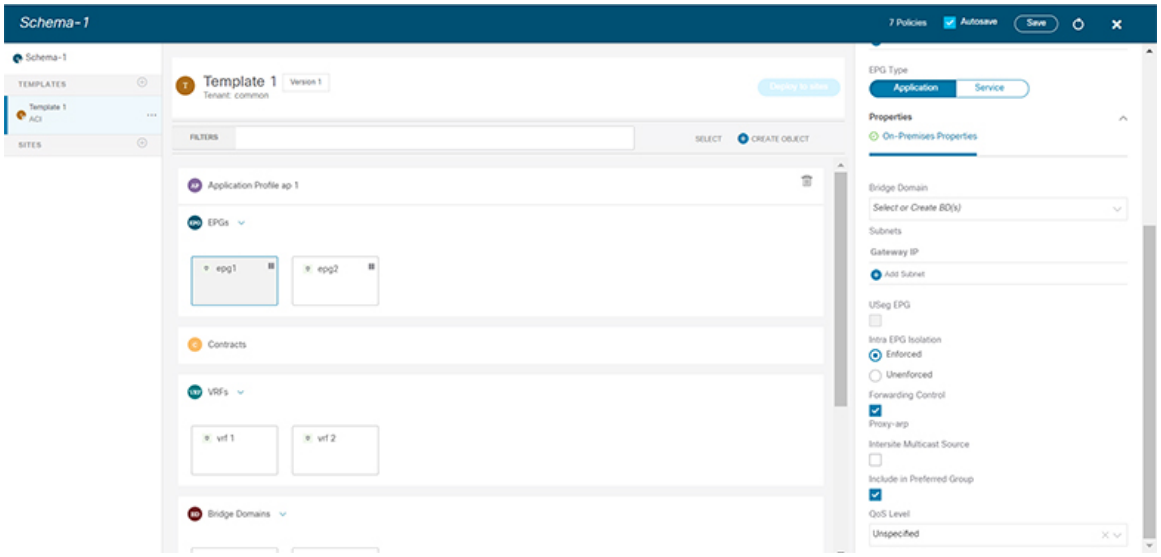
選択したオブジェクトのタイプに基づいて、次のプロパティを更新できます。

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。

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 テンプレートの名前の横にある **[アクション (Actions)]** メニュー **(...)** をクリックし、**[サイトの追加（Add Sites）]** を選択します。

[<template-name> へのサイトの追加] ウィンドウが開きます。

ステップ 4 **[サイトの追加（Add 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 **[Save（保存）]** 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。

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。
- テンプレートごとに無制限のバージョンをサポートしていた以前のリリースから最初にアップグレードする場合、既存のすべてのバージョンはそのまま残ります。

  テンプレートが変更されて保存または展開されると、20 Deployed および 20 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。

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。

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、**[ゴールデンとして設定 (Set as Golden)]** 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 **[ゴールデンの削除 (Remove Golden)]** 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。

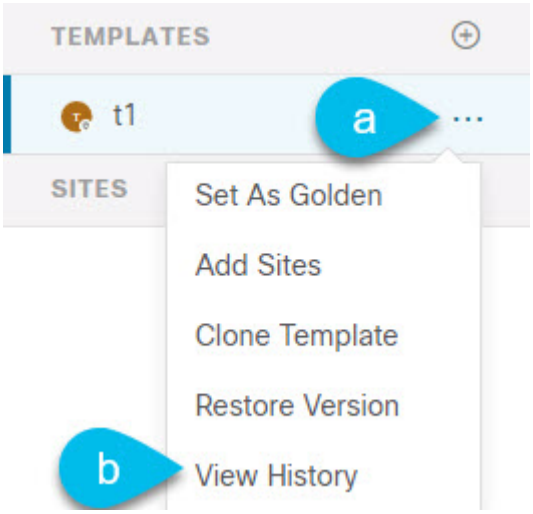
ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

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。

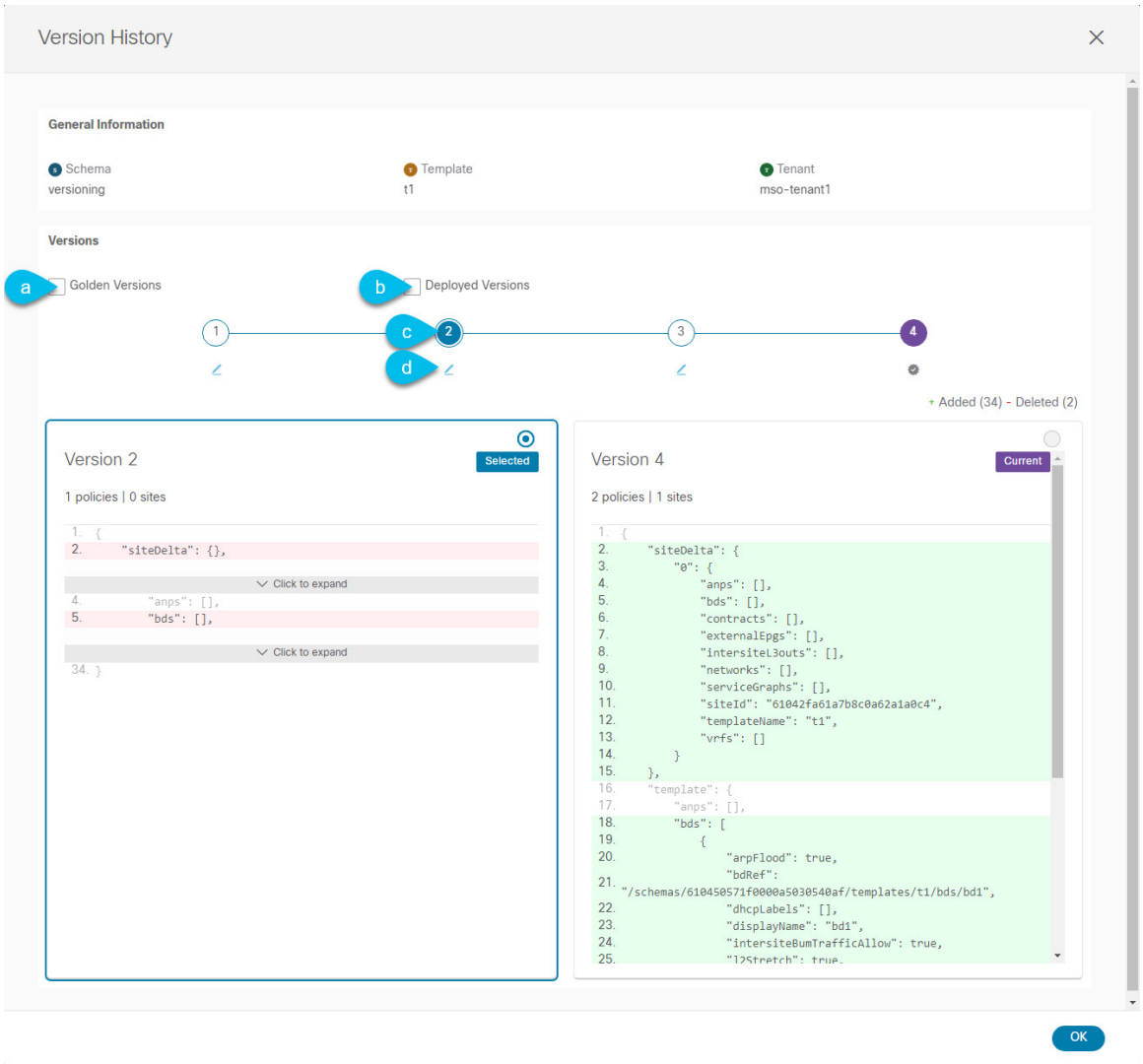
ステップ 3 表示するテンプレートを含むスキーマをクリックします。

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、**[履歴の表示 (View 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 （48 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。

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（52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

リリース 3.4(1) では、テンプレートのレビューと承認（変更管理）のワークフローのサポートが追加されます。これにより、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。

（注） レビューと承認のワークフローは、Nexus Dashboard で定義されたユーザ ロールに依存するため、この機能を使用するには、Nexus Dashboard リリース2.1(1) 以降を実行する必要があります。Nexus Dashboard リリース 2.0.2 で Nexus Dashboard Orchestrator を展開した場合、プラットフォームをアップグレードするまで、確認と承認の機能は無効になります。

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。

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 **[変更制御 (Change Control)]** ウィンドウで、**[変更制御ワークフー (Change Control Workflow)]** チェックボックスをオンに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。

Create Users with Required Roles

Before you can use the review and approval workflow for template configuration and deployment, you must create the users with the necessary privileges in the Nexus Dashboard where the NDO service is deployed.

ステップ 1 Log in to your Nexus Dashboard GUI.

Users cannot be created or edited in the NDO GUI, you must log in directly to the Nexus Dashboard cluster where the service is deployed.

ステップ 2 From the left navigation menu, select **Administrative** > **Users**.

ステップ 3 Create the required users.

The workflow depends on three distinct user roles: template designer, approver, and deployer. You can assign each role to a different user or combine the roles for the same user; users with `admin` privileges can perform all 3 actions.

There is no `Designer` role predefined on Nexus Dashboard, so the designer duties are assigned to any `Tenant Manager` or `Site Manager` user with write privileges, in addition to the default `Admin` user role:

- `Tenant Manager` should be used when the designer needs to make changes to templates associated only to a specific tenant (or a subset of tenants). In this case, the user should be mapped to the specific tenants.
- `Site Manager` should be used when the designer needs to make changes to templates that belong to different tenants.

In contrast to `Designer` role, there are pre-defined `Approver` and `Deployer` roles on the Nexus Dashboard that can be associated to the users. `Approver` and `Deployer` roles are not bound to specific tenant(s) by design. However, when creating a user role with both designer and approver (or designer and deployer) rights, follow the same guidelines as listed above.

Detailed information about configuring users and their privileges for local or remote Nexus Dashboard users is described in the Nexus Dashboard User Guide.

You must have at least as many unique users with `Approver` role as the minimum number of approvals required, which you configured in テンプレート承認要件の有効化, on page 53.

Note If you disable the **Change Control Workflow** feature, any `Approver` and `Deployer` users will have read-only access to the Nexus Dashboard Orchestrator.

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 （53 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（Create Users with Required Roles （53 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。

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 （53 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（Create Users with Required Roles （53 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 （54 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。

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 （48 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（72 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。

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が必要です。

テンプレートのレビューと承認 （52 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 左側のサイドバーで、展開するテンプレートを選択します。

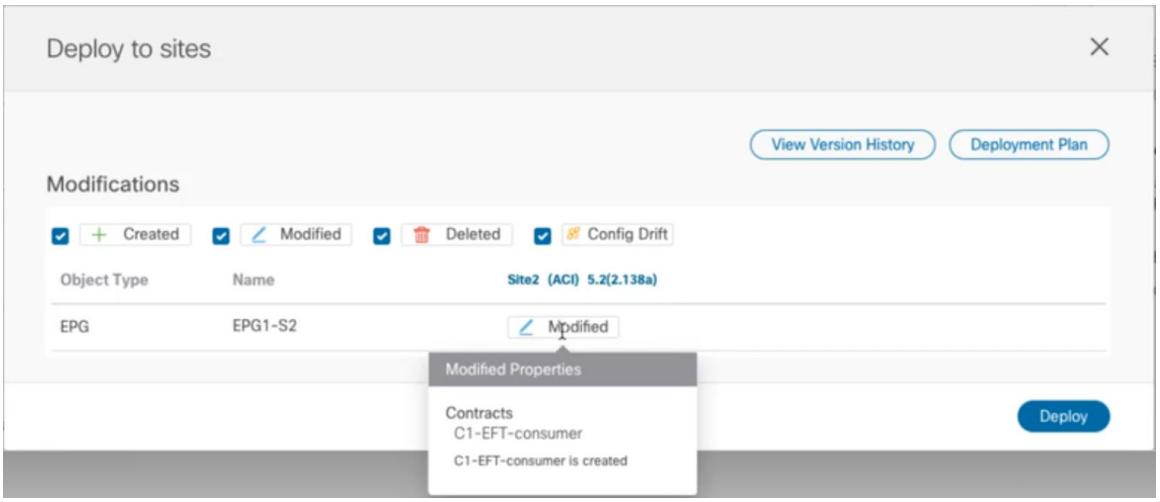
ステップ 3 テンプレート編集ビューの右上で、[展開（Deploy）]をクリックします。

The **Deploy to sites** window opens that shows the summary of the objects to be deployed.

ステップ 4 テンプレートに変更を加えた場合は、展開計画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。In this case, you can skip this step.

[サイトに展開] 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、Site2 の既存の EPG (EPG1-S2) に消費者契約を追加する簡単な例を示しています。



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。

- **View Version History**, which shows the complete version history and incremental changes made between versions. 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 （48 ページ）を参照してください。
- Check the **Deployment Plan** to see a visualization and an XML payload of the configuration that will be deployed from this template.

  この機能により、テンプレートに変更を加えて 1 つ以上のサイトにデプロイした後に、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よく可視化できます。

  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 Multi-Site Orchestrator の以前のリリースとは異なり、展開計画では、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。

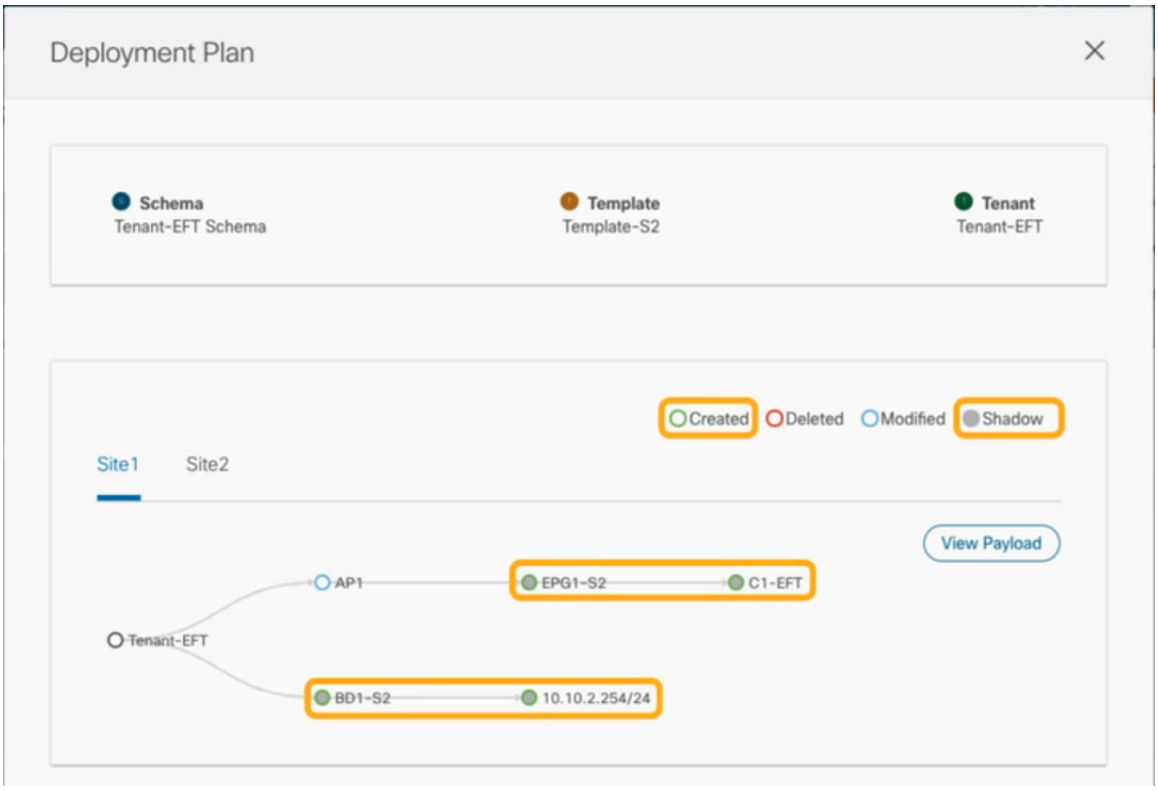
  （注） テンプレートをデプロイする前に、このステップで説明されているように、デプロイメント プランを使用して変更を確認することをお勧めします。構成変更の視覚的な表現は、意図しない構成変更の展開による潜在的なエラーを減らすのに役立ちます。

a) Click the **Deployment Plan** button.

   前のステップで示したのと同じ例を続けると、消費者契約がサイト 2 の既存の EPG に追加されました。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。 。

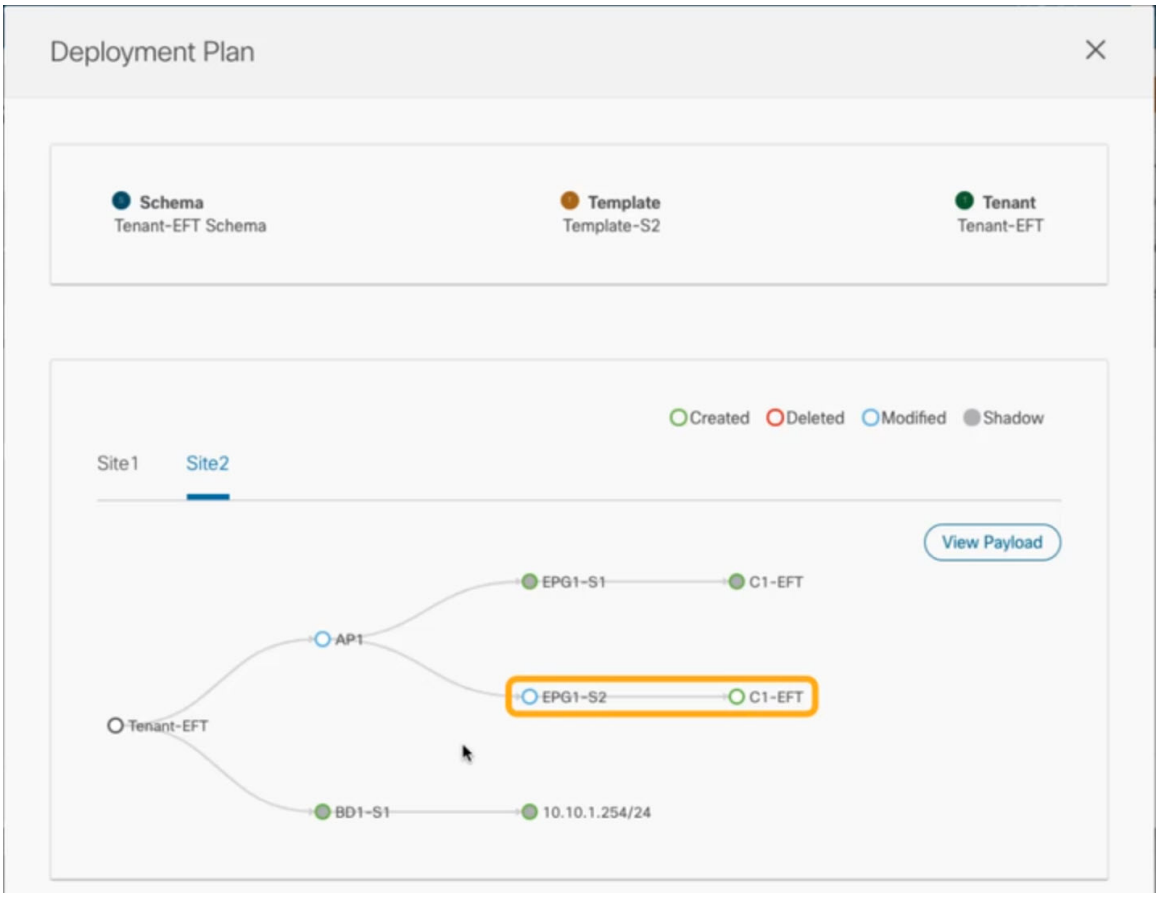
b) 最初にリストされたサイトで変更を確認します。

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。



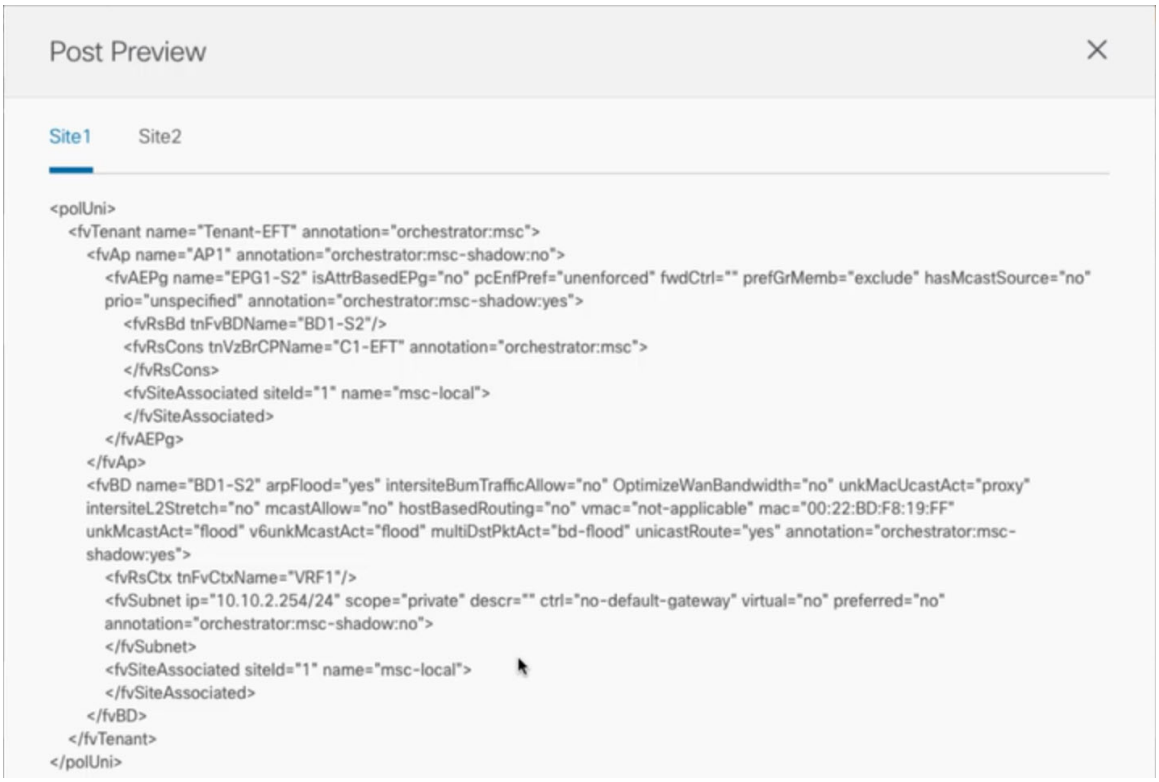
c) Repeat the previous substep to verify the changes in other sites

ここでは、契約 (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、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。 、その契約を提供しています。



d) (オプション) [ペイロードの表示] をクリックして、各サイトの XML ペイロードを表示します。

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、各サイトの変更のペイロードの表示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 [Deployment Plan] 画面を閉じます。

ステップ 5 [サイトにデプロイ] ウィンドウで、[デプロイ] をクリックしてテンプレートをデプロイします。

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

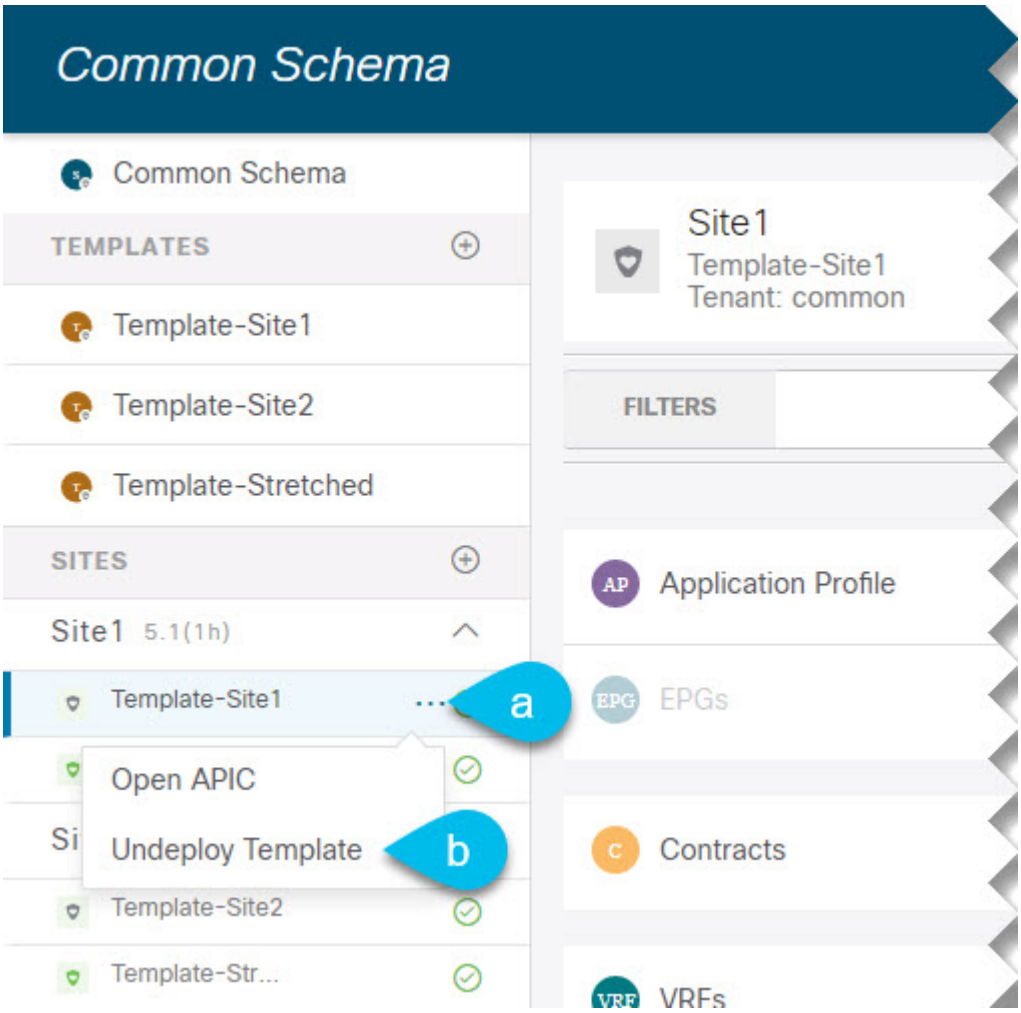
- テンプレートを最後に展開してから、テンプレートに変更を加えていないことを確認します。

  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。

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 **[サイト (SITES)]** の下の左側のサイドバーで、展開を解除するテンプレートを選択します。

ステップ 3 テンプレートを展開解除します。



a) テンプレートの横にある **[その他のオプション (More options) (. . .)]** メニューをクリックします。
b) **[テンプレートの展開解除 (Undeploy Template)]** をクリックします。

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。

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。

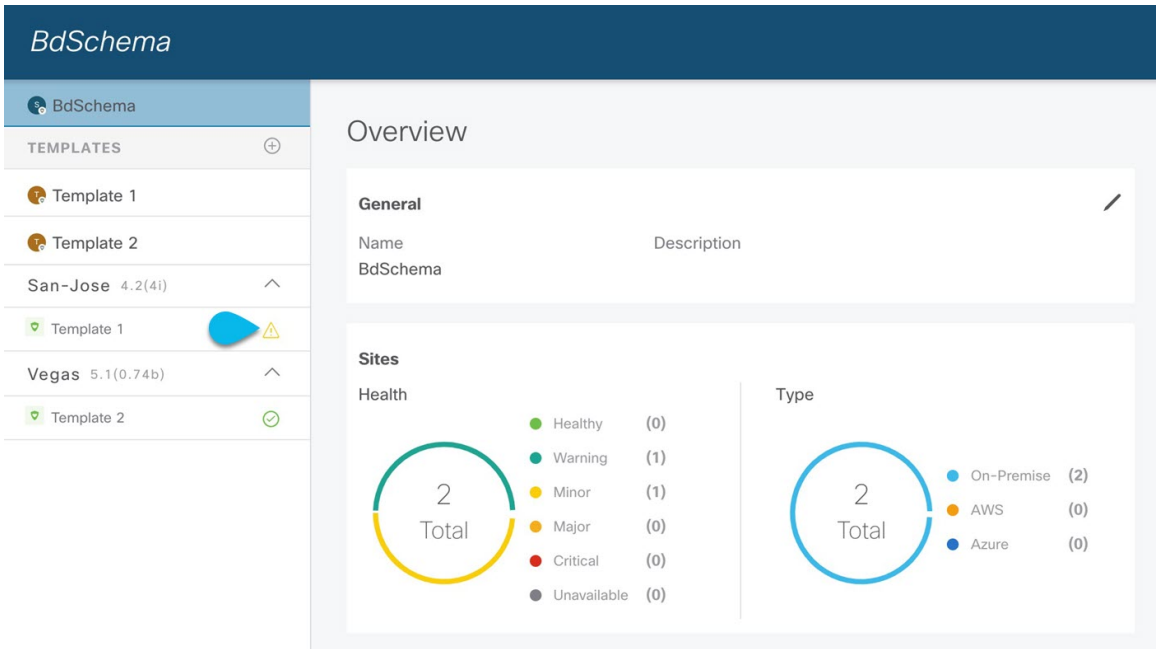
ステップ 5 **[アクション (Actions)]** メニューから **[テンプレートの関連付け解除 (Disassociate Template)]** を選択します。

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。

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、スキーマ ビューのテンプレート名の横に黄色の注意サインで示されます。

図 *5:*



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。

  NDO リリース 3.6(1) 以降、テンプレートに対して「ばらつきの調整」ワークフローを実行して、ばらつきの原因をより詳細に把握し、ばらつきを調整できるようにすることをお

勧めします。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。NDO 3.6 の新しいばらつきの調整ワークフローの詳細については、以下の「構成のばらつきの調整」セクションを参照してください。

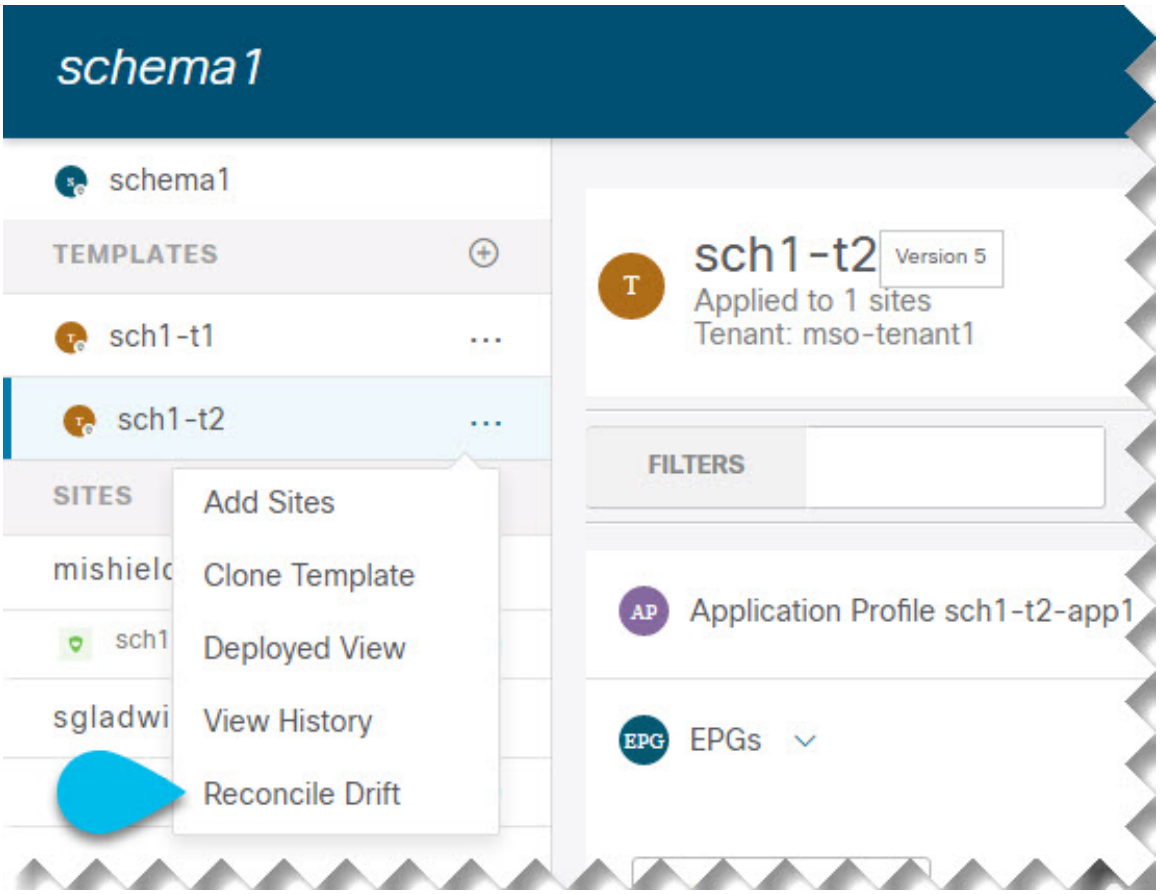
設定のばらつきの調整

NDO リリース 3.6(1) では、Nexus Dashboard Orchestrator で定義されたテンプレート構成と、マルチサイト ドメインのサイト部分の APIC コントローラーでレンダリングされた構成を比較するために実行できるばらつき調整ワークフローのサポートが導入されています。これにより、構成のばらつき（つまり、Nexus Dashbaord Orchestrator または APIC で直接行われた変更）の原因をより明確に把握でき、以下の手順で説明するように、ばらつきを調整する方法をユーザーに選択させることができます。

（注） 選択した構成が必要ない場合は、スキーマを閉じて再度開くことができます。これにより、元の構成が表示されます。必要に応じて、「Reconcile Drift」フローを再度トリガーできます。[保存（Save）] または [展開（Deploy）] ボタンを選択した後にのみ、スキーマが保存されます。

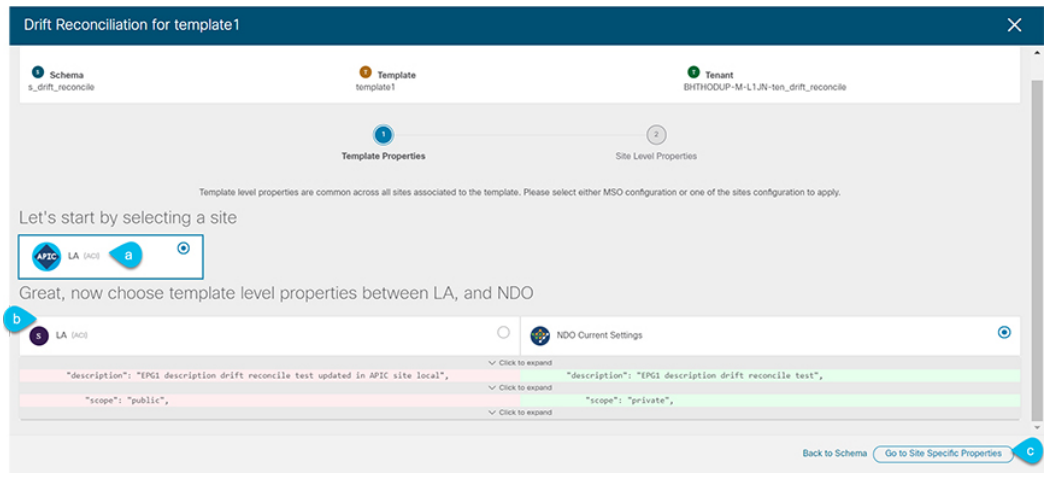
ステップ 1 設定のばらつきを確認するテンプレートを含むスキーマに移動します。

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 **[テンプレートのプロパティ (Template Properties)]** 画面で、各サイトのテンプレートレベルの設定を比較し、必要な設定を選択します。



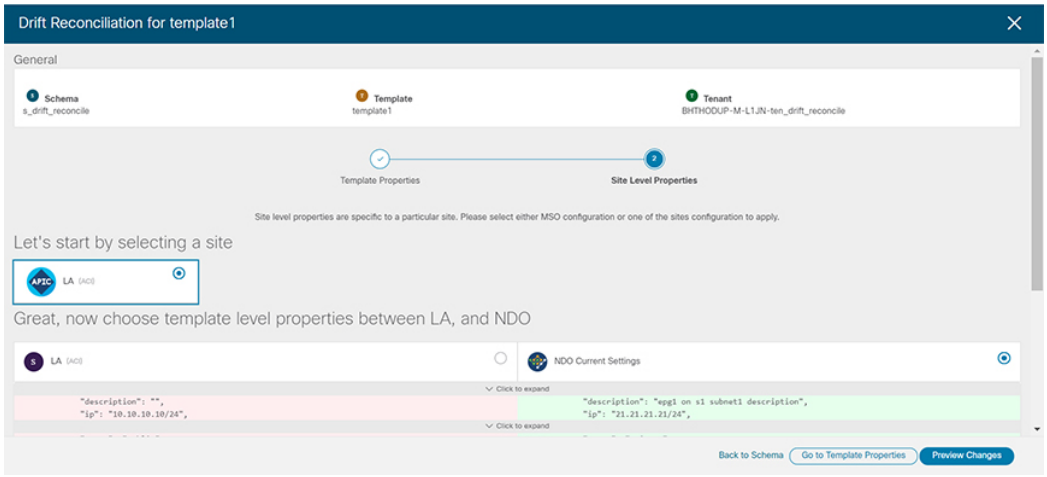
a) （この特定のテンプレートに関連付けられているサイトのリストの中で）サイトを選択します。

b) 保持するプロパティを選択します。

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で共通であることに注意してください。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。サイト構成を選択すると、既存の Nexus Dashboard Orchestrator テンプレート内のこれらのプロパティが変更されますが、Nexus Dashboard Orchestrator 構成を選択すると、既存の Nexus Dashbaord Orchestrator テンプレート構成がそのまま保持されます。

c) 「サイト固有のプロパティに移動」を選択します。

ステップ 4 特定のサイトのプロパティとの比較対象にするサイトを選択できます。テンプレートに関連付けられた各サイトを選択し、Nexus Dashboard Orchestrator から定義された構成を維持するか、サイトに現在存在する構成を維持するかを選択します。



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。

また、ユーザーが「テンプレート プロパティ」レベルで APIC 設定を選択し、「サイト ローカル プロパティ」レベルで Nexus Dashboard Orchestrator サイト レベル設定を選択する場合もあります（またはその逆）。ウィザードは、そのレベルの柔軟性を提供するように設計されていますが、ほとんどのシナリオでは、テンプレート レベルとサイト レベルの構成の両方で一貫して選択が行われる可能性があります。

ステップ 5 **[プレビュー（Preview）]** をクリックして変更を確認します。

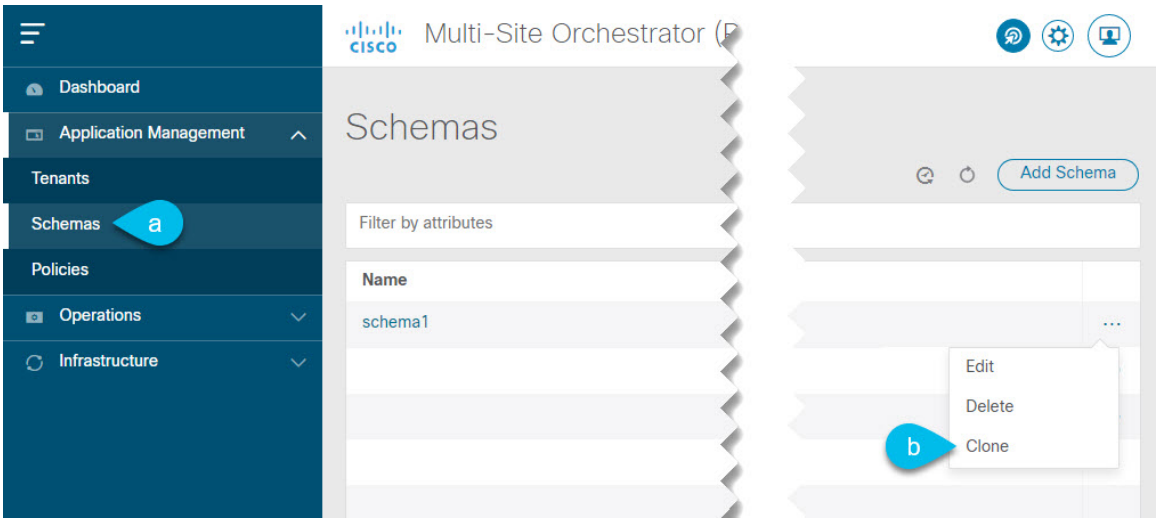
テンプレート設定は、**[ばらつきの調整 (Dift Reconciliation)]** ウィザードで選択したプロパティに基づいて調整されます。その後、**[サイトに展開 (Deploy to site)]** をクリックして設定を展開し、そのテンプレートのばらつきを調整できます。

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。

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

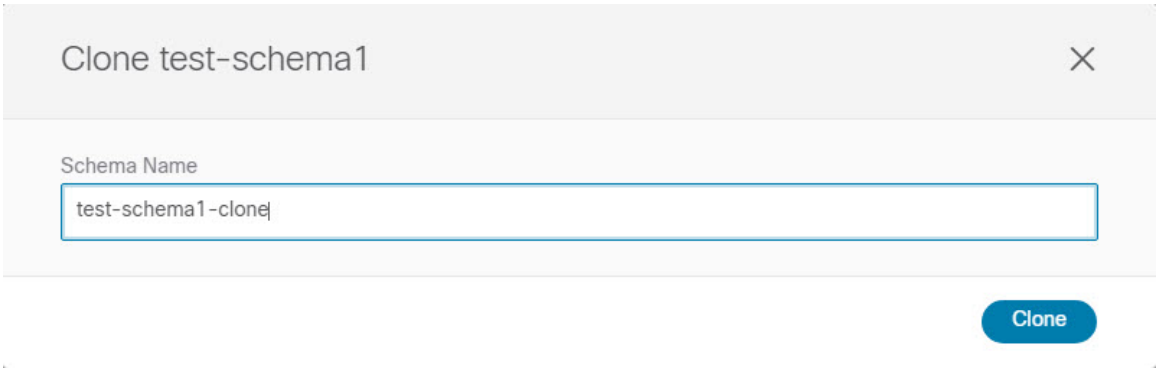
ステップ 2 複製するスキーマを選択します。



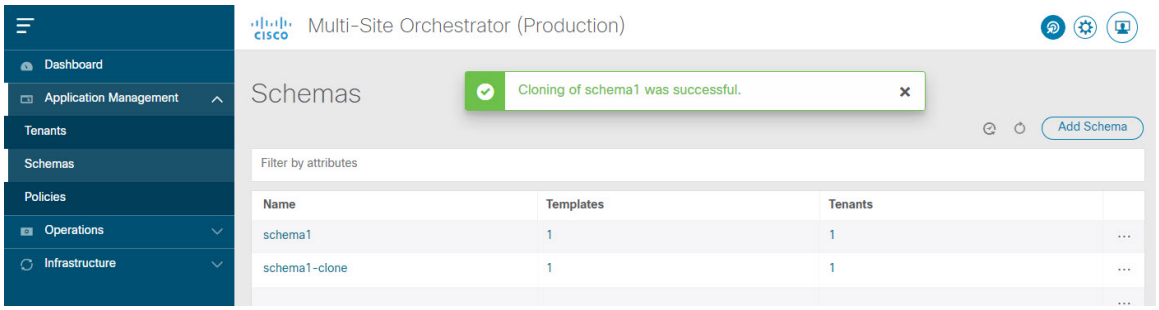
a) 左型のナビゲーション メニューで、**[アプリケーション管理 (Application Management)]** > **[スキーマ (Schemas)]** を選択します。

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、**[スキーマの複製 (Clone Schema)]** 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。

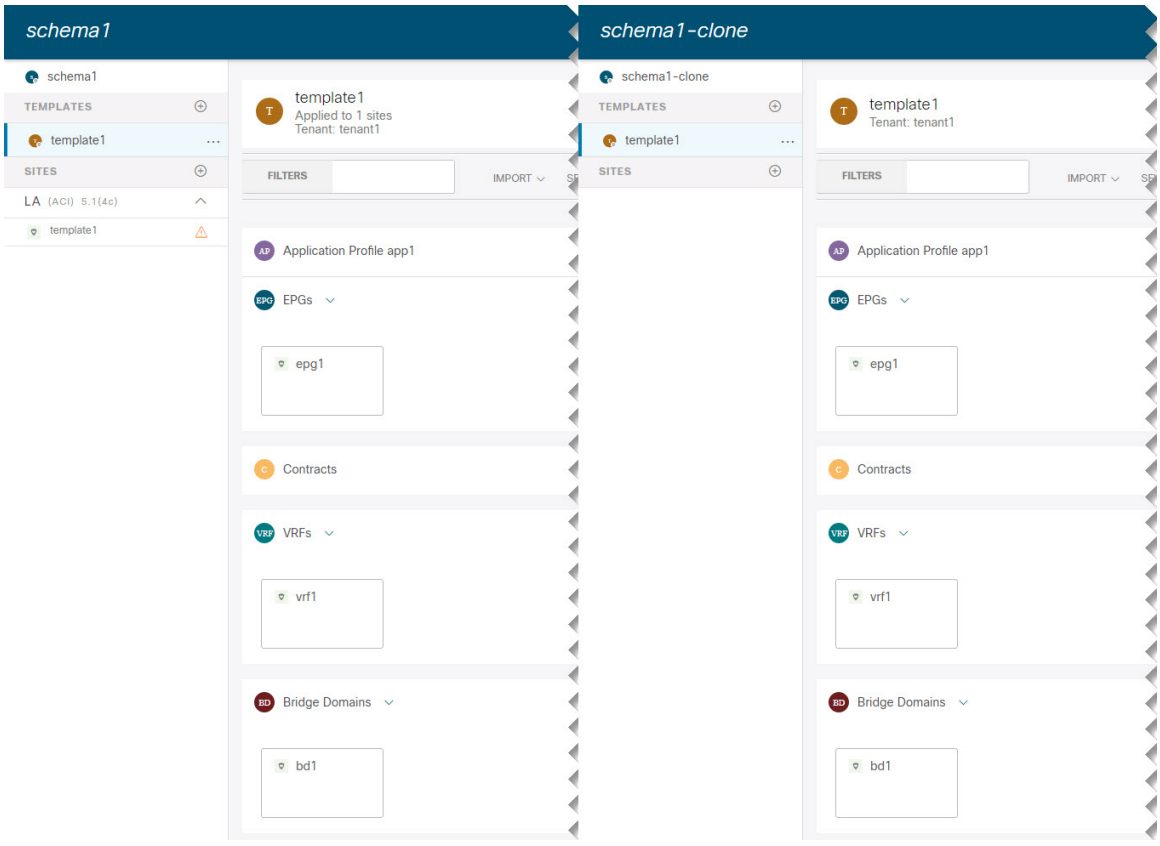


新しいスキーマは、元のスキーマとまったく同じテンプレート（およびそのテナントの関連付け）、オブジェクト、およびポリシー設定で作成されます。

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

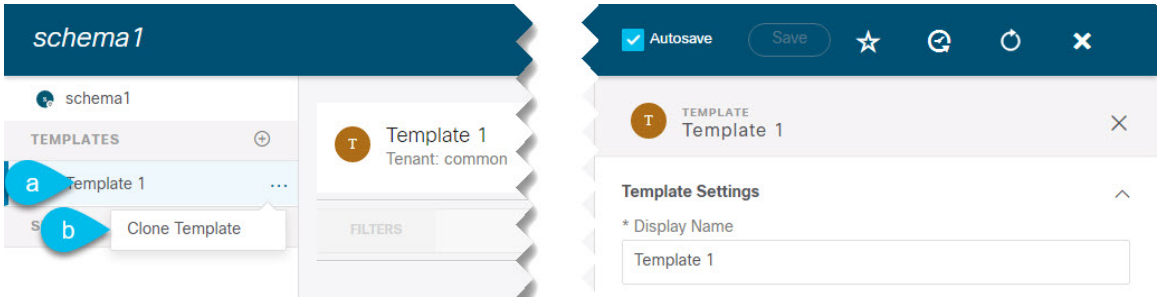
ここでは、スキーマ ビューで [テンプレートの複製 (Clone Template)]機能を使用して既存のテンプレートのコピーを作成する方法について説明します。

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 [スキーマ (Schema)] ビューで、**[テンプレートのクローン (Clone Template)]** ダイアログを開きます。



a) 複製するテンプレートを選択します。

b) **[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 5 クローンの複製先の詳細を入力します。

a) **[複製先テナント (Destination Tenant)]** ドロップダウンから、ターゲット テナントを選択します。

デフォルトでは、現在のテンプレートのテナントが選択されています。テナントを変更すると、代わりに新しいテンプレートが選択したテナントに割り当てられます。

複製先テナントはすでに存在している必要があります。テンプレートを複製して新しいテナントに割り当てる場合は、まず**[テナント (Tenants)]**ページでテンプレートを作成してから、テンプレートに戻って複製する必要があります。

（注） 異なるテナント間で複製する場合、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テンプレートに含めることはできません。

b) **[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。

c) [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。
d) **[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 APIC 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。

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。

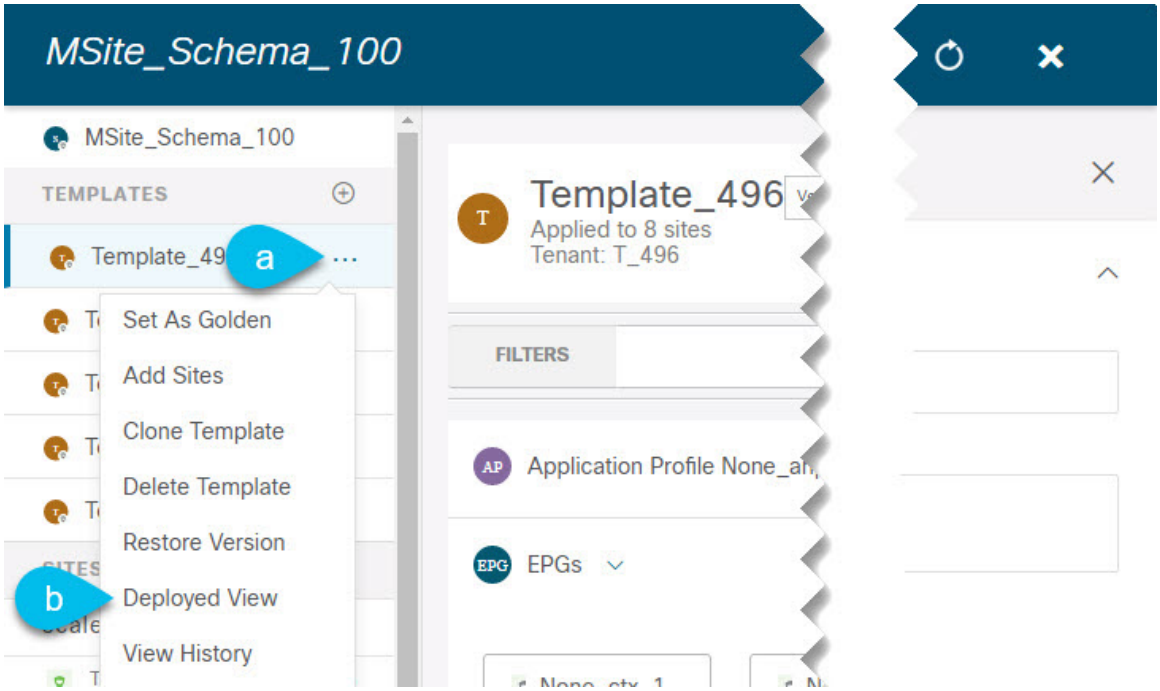
ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

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。

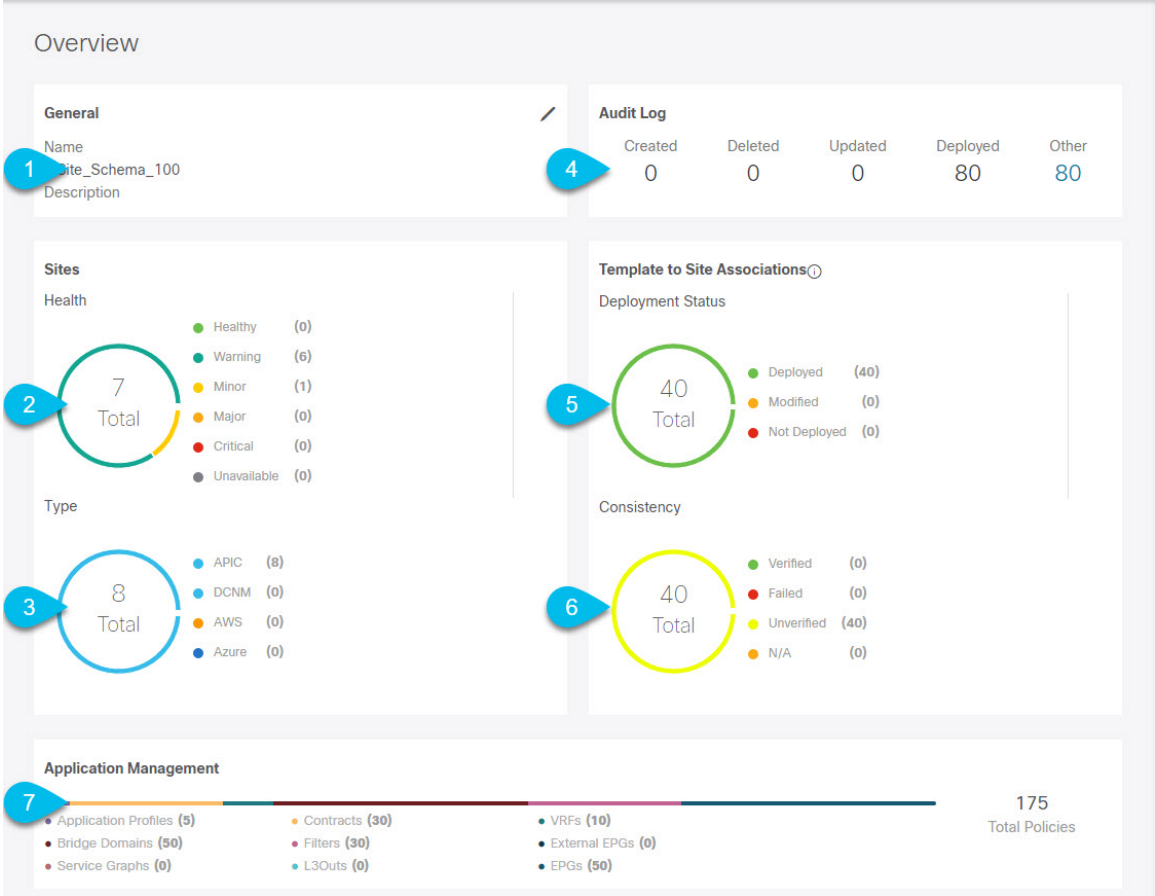
b) サイト名をクリックすると、その特定のサイトの設定を表示できます。

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 *6*: スキーマの概要



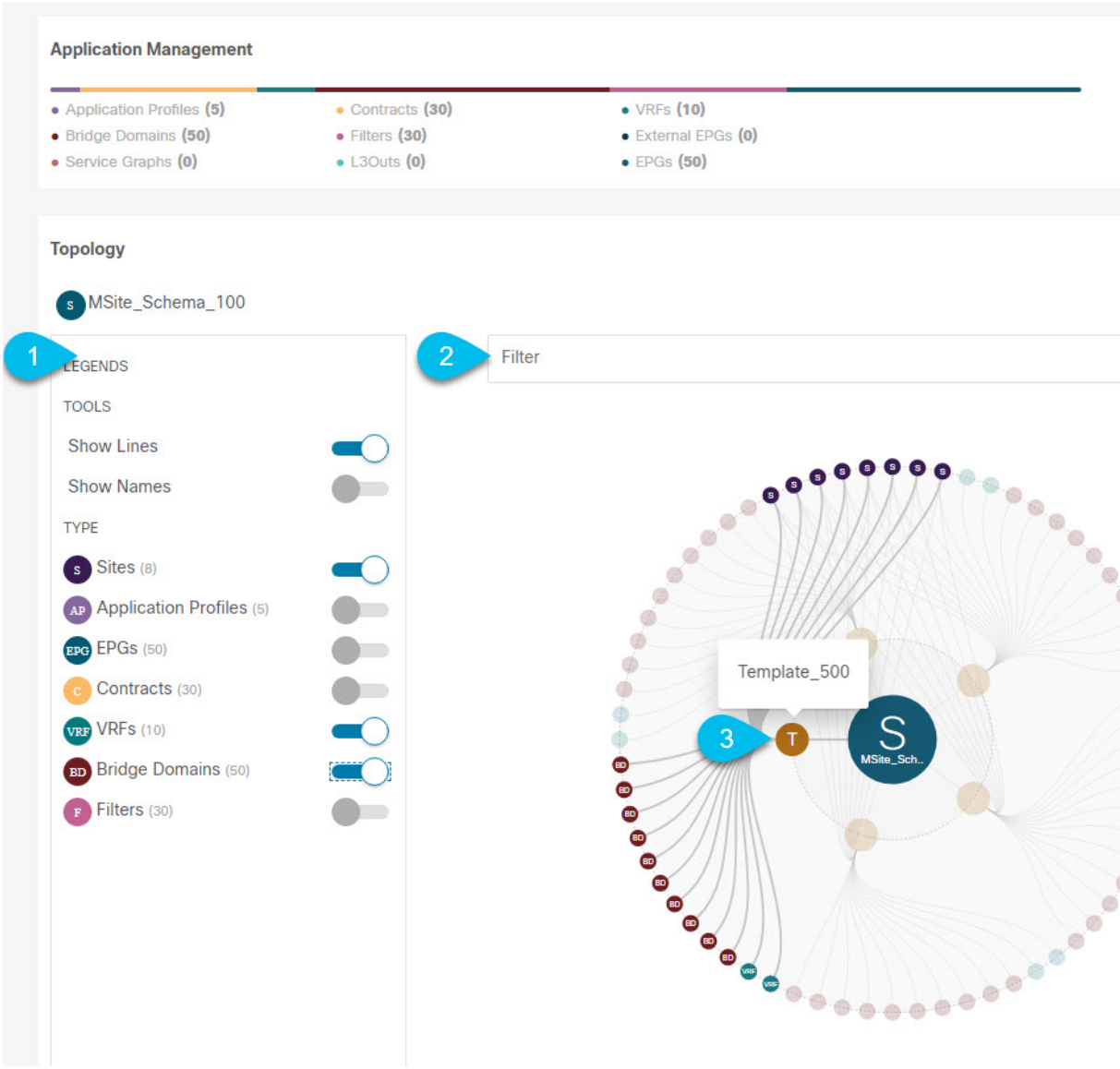
このページには、次の詳細が表示されます。

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 7: 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。

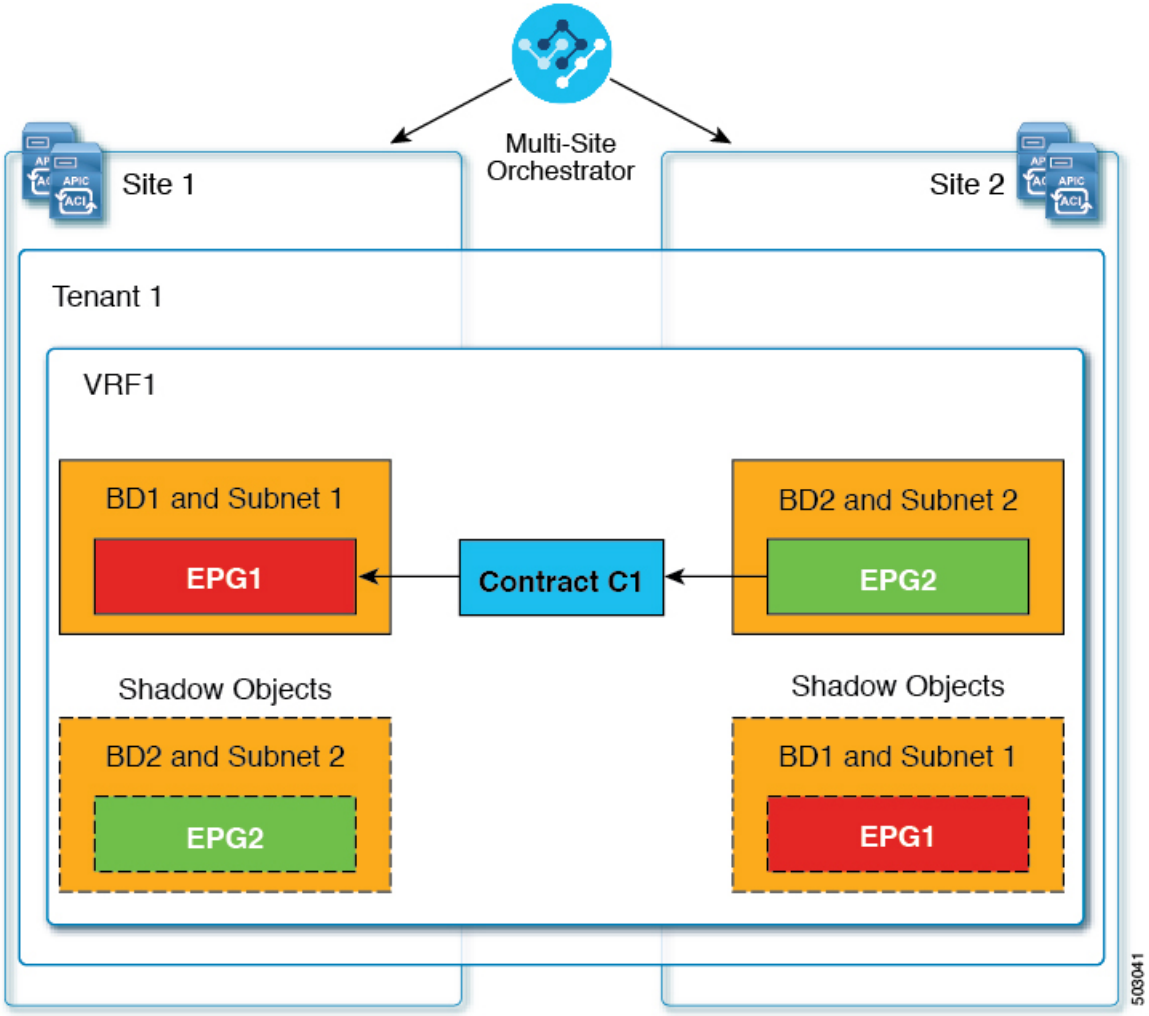
シャドウ オブジェクト

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 APIC 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 *8* : 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）

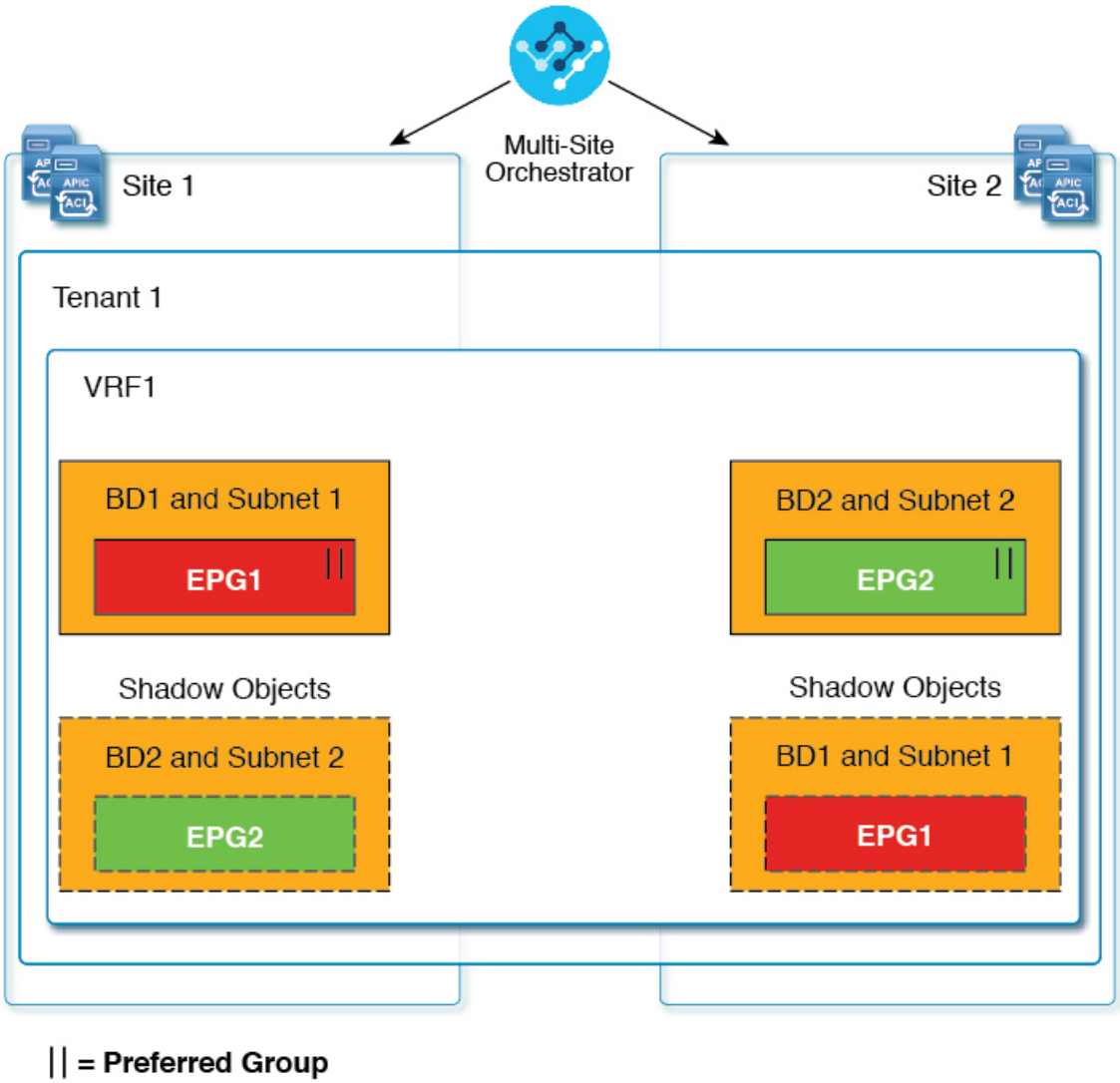
ファブリックが APIC リリース 5.0(2) 以降で実行されている場合、APIC GUI でシャドウ オブジェクトを選択すると、 が表示されます。これはサイト間ポリシーをサポートするために、MSC からプッシュ

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

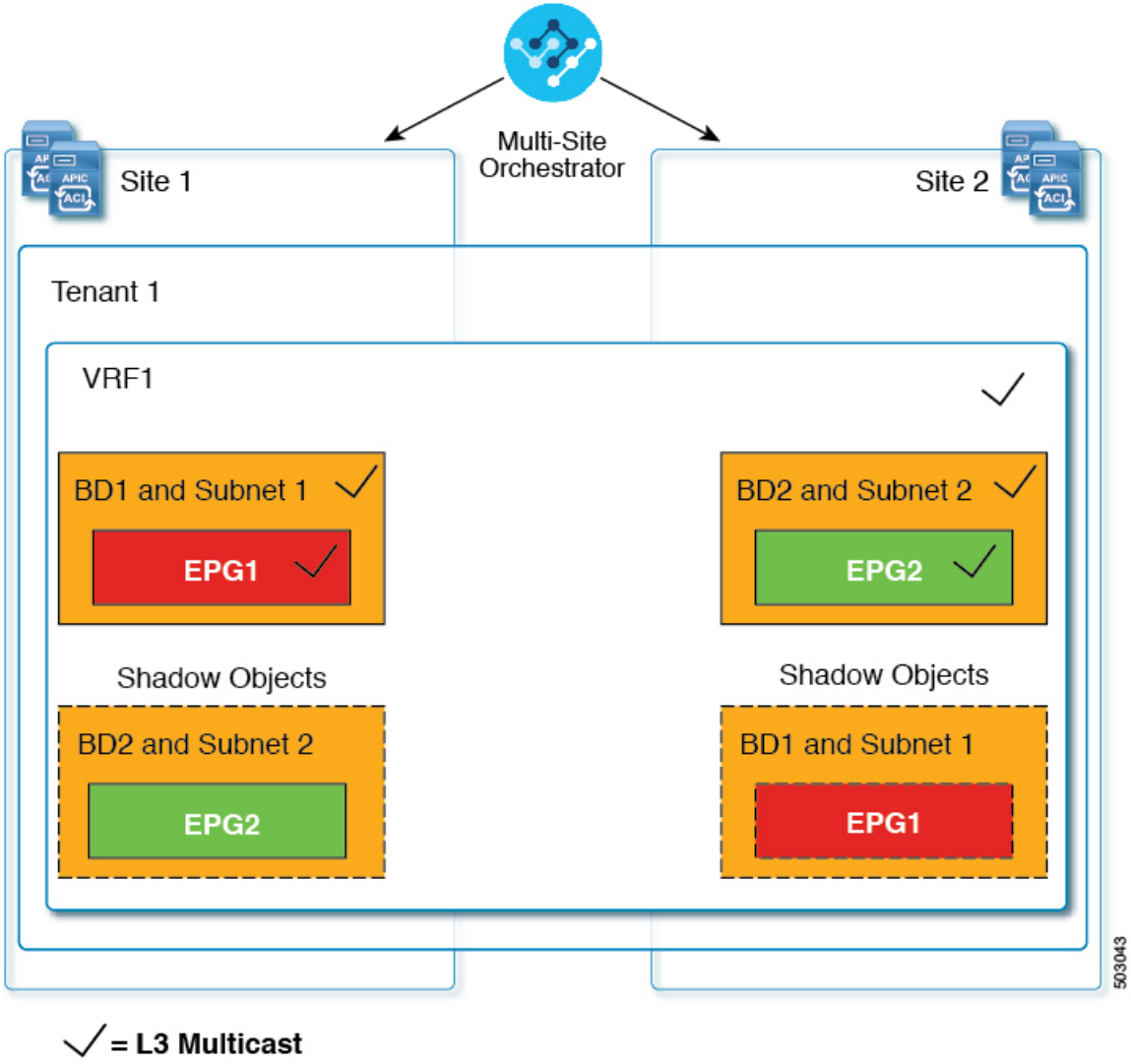
シャドウ オブジェクトは、次の図に示すように、[優先グループ (Preferred Group)]、[vzAny]、[レイヤ3マルチキャスト (Layer 3 Multicast)]、およびハイブリッド クラウドなど、さまざまな使用例でも作成されます。

図 *9:* 優先グループ



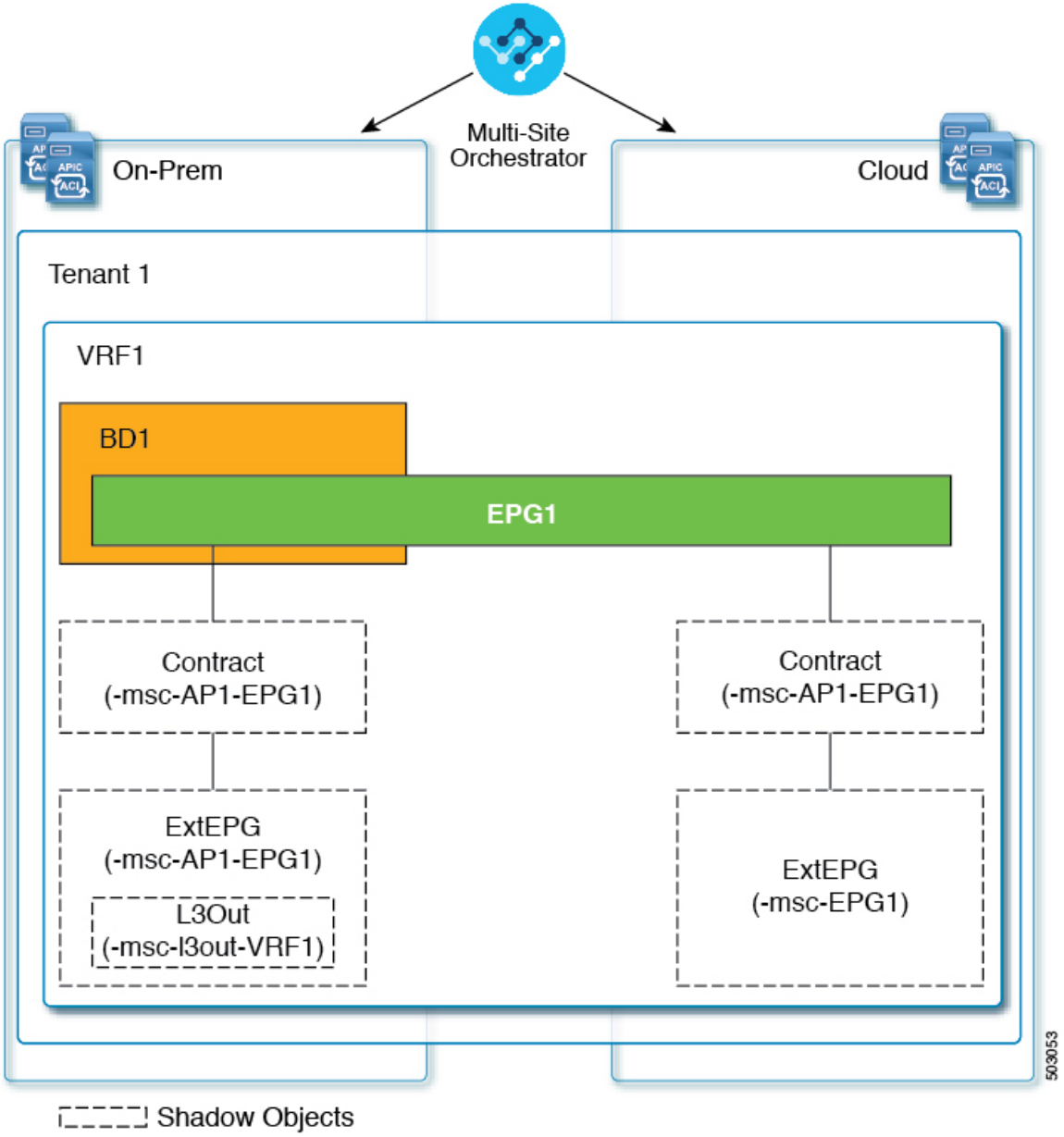
マルチキャストの場合、シャドウ オブジェクトは、マルチキャスト ソースが接続され、オプションが EPG レベルで明示的に設定されている EPG/BDに対してのみ作成されます。

図 *10 : 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 *11* : 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 APIC 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。

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。

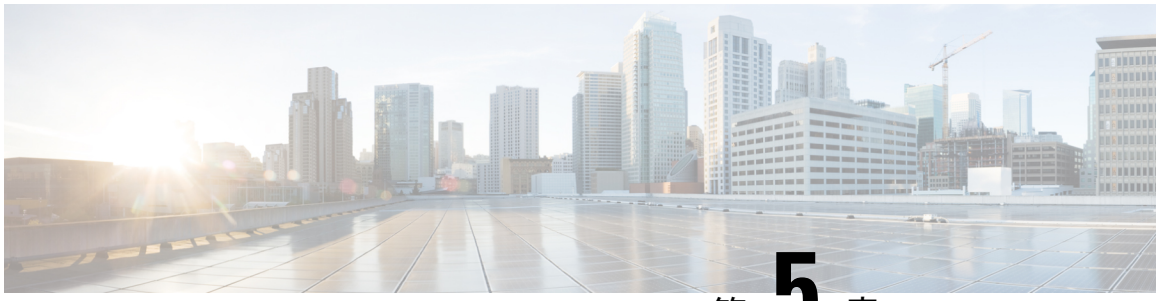
ステップ 3 **[アプリケーション設定 (Application Settings)]** ウィンドウで、**[非表示のポリシーを表示 (Show Hidden Policies)]** チェックボックスをオンまたはオフにします。

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。

第 II 部

操作



第 5 章

監査ログ

監査ログ

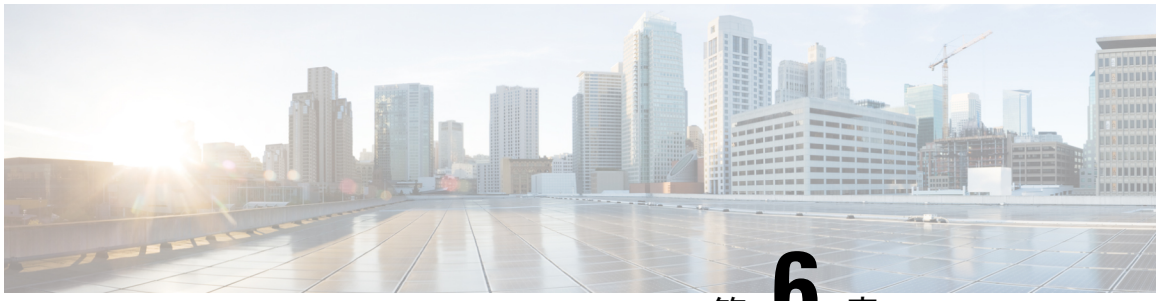
Nexus Dashboard Orchestrator のシステム ロギングは、最初に Orchestrator クラスタをデプロイしたときに自動的に有効になり、環境内で発生したイベントと障害をキャプチャします。

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

設定のバックアップと復元

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。

バックアップと復元に関するガイドライン

設定のバックアップを保存および復元する際には、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 3.2(1) より前のリリースで作成された設定バックアップの復元は、Nexus Dashboard へのクラスタ移行中のワンタイム ステップとしてサポートされます。

VMware ESX または Application Services Engine 展開で、 Multi-Site Orchestrator リリースからバックアップしていた場合、その後の復元はサポートされていません。

- 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 アクションを復元すると、Nexus Dashboard Orchestrator でのデータベースは復元されますが、各サイトのコントローラ（APIC、Cloud APIC、または DCNM など）データベースは変更されません。したがって、Nexus Dashboard Orchestrator と 各サイトのコントローラ間のポリシーが食い違う可能性を避けるため、Nexus Dashboard Orchestrator データベースを復元した後には、既存のスキーマを再展開する必要があります。
- バックアップはリモート ロケーションで作成する必要があります。

  リリース 3.4(1) よりも前のリリースでは、クラスタを最初に展開したとき、作成していたバックアップは、各ノードのローカルディスク上のデフォルトの場所に保存され、さらに Orchestrator クラスタ外のリモート ロケーションを設定して、そこにバックアップを再配置するオプションがありました。

  リリース 3.4(1) 以降では、ローカルディスク オプションは廃止されたので、すべてのバックアップは Nexus ダッシュボード クラスタ外のリモート ロケーションに作成する必要があります。次のセクションの説明に従って、NDO GUI を使用してリモート SCP または SFTP ロケーションを設定し、そこにバックアップ ファイルをエクスポートできます。

  リリース 3.3(1) 以前からリリース 3.4(1) 以降に初めてアップグレードする場合は、古いローカル バックアップのダウンロードとインポート （89 ページ） の説明に従って、以前に作成したローカルバックアップをダウンロードできます。その後、リモートロケーションを経由して、これらのバックアップを Nexus Dashboard Orchestrator に再インポートできます。

  （注） ローカル バックアップは復元できません。

- 設定のバックアップを作成してリモートサーバにエクスポートするときには、ファイルは最初に Orchestrators ローカル ドライブに作成され、その後リモートの場所にアップロードされ、最後にローカル 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 3.4(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取得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。

バックアップ以降の設定変更はありません

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 （93 ページ） の説明に従って設定を復元するだけです。

バックアップ以降に作成、変更、または削除されたサイト、オブジェクトまたはポリシー

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。古い設定を回避するには、バックアップを復元した後に手動でこれらを削除する必要があります。

  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 （93 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、設定を各サイトに適切にプッシュするには、それを再展開して、Nexus Dashboard Orchestrator の設定をサイトと同期させる必要があります。

- 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。

古いローカル バックアップのダウンロードとインポート

3.4(1) より前のリリースでは、オーケストレータのローカルディスクでの設定バックアップの作成がサポートされていました。リリース 3.4(1) 以降にアップグレードする前に、ローカル バックアップをダウンロードしておくことを推奨します。ただし、ローカル バックアップはアップグレード後も引き続きダウンロードできます。

アップグレード後に古いバックアップをダウンロードすることはできますが、UI で直接バックアップを復元することはできません。このセクションでは、このようなバックアップを Orchestrator GUI からローカルマシンにダウンロードし、今度はリモートロケーションを使用して Nexus Dashboard Orchestrator GUI に再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。

- リリース 3.3(1) 以前からリリース 3.4(1) 以降にアップグレードされていること。新しいリリースでは、ローカルバックアップはサポートされなくなりました。
- バックアップのリモート ロケーションの設定 （90 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。

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、バックアップファイルがシステムにダウンロードされます。

ステップ 4 Nexus Dashboard Orchestrator GUIでダウンロードしたバックアップを削除します。

以前のバージョンから既存のローカルバックアップを削除せずにバックアップを再インポートしようとすると、同じ名前のバックアップファイルがすでに存在するため、アップロードが失敗します。

ダウンロードしたバックアップを削除するには、バックアップの横にあるアクション（**...**）メニューをクリックし、**[削除 (Delete)]** を選択します。

ステップ 5 バックアップをリモートの場所にインポートします。

バックアップのアップロード （91 ページ）に記載されているように、リモート ロケーションを使用してダウンロードしたバックアップ ファイルを Nexus Dashboard Orchestrator に再アップロードします。

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。

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)]** > **[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。

バックアップのアップロード

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 （92 ページ） および バックアップのダウンロード （94 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 （90 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。

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 （90 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。

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

ステップ 2 バックアップを新規作成します。

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。

ステップ 3 バックアップ情報を指定します。

a) バックアップの **[名前 (Name)]** とオプションの **[メモ (Notes)]** を指定します。

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。

b) **[リモート ロケーション (Remote location)]** ドロップダウンから、バックアップ用に設定したリモート ロケーションを選択します。
c) **[リモートパス (Remote Path)]** では、デフォルトのターゲット ディレクトリのままにするか、またはパスにサブディレクトリを追加することができます。

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 サーバーで作成されている必要があることに注意してください。

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 アクションを復元すると、Nexus Dashboard Orchestrator でのデータベースは復元されますが、各サイトのコントローラデータベースは変更されません。したがって、Nexus Dashboard Orchestrator と 各サイトのポリシーが食い違う可能性を避けるため、Nexus Dashboard Orchestrator データベースを復元した後には、既存のスキーマを再展開する必要があります。

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、バックアップと復元に関するガイドライン （87 ページ）を参照してください。

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、バックアップと復元に関するガイドライン （87 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 必要に応じて、設定を再展開します。

復元された設定を APIC サイトと同期する際には、この手順を実行することをお勧めします。追加のコンテキストは、バックアップと復元に関するガイドライン （87 ページ） にあります。

バックアップのダウンロード

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

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 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 （90 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。

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。

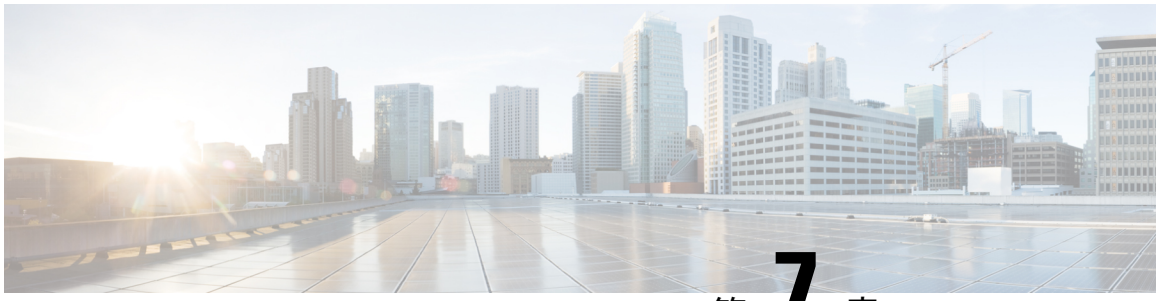
f) （オプション）**[リモート パス (Remote Path)]** フィールドで、バックアップが保存されるリモート ロケーションのパスを更新します。

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 Cloud APIC または Cisco DCNM ファブリックではサポートされません。

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。

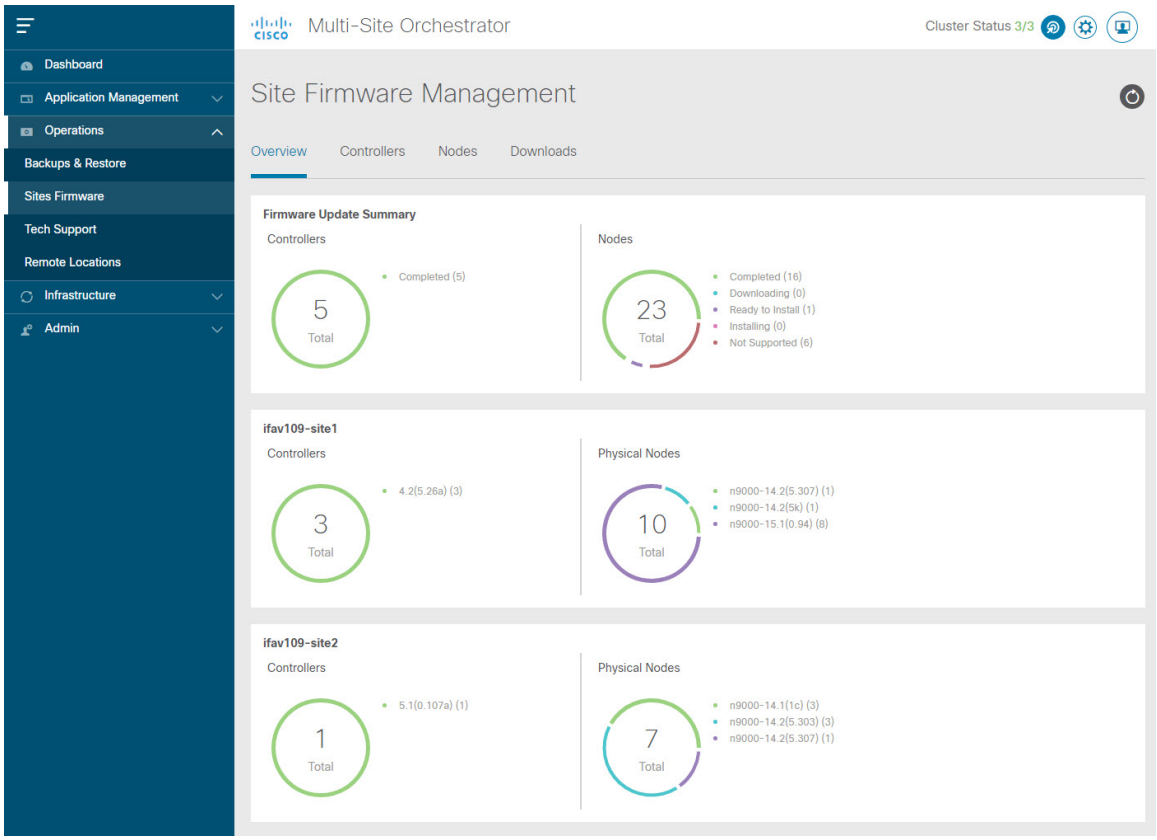
リリース 3.1(1) 以降、Cisco Nexus Dashboard Orchestrator は、すべてのサイトのソフトウェア アップグレードを単一のポイントから管理できるワークフローを提供します。複数のサイト管理者がソフトウェア アップグレードを手動で調整する必要がなく、アップグレードに影響する可能性のある、潜在的な問題を把握できます。

[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 *12*：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。

Guidelines and Limitations

When performing fabric upgrades from the Nexus Dashboard Orchestrator, the following restrictions apply:

- You must review and follow the guidelines, recommendations, and limitations specific to the Cisco APIC upgrade process described in the Upgrading and Downgrading the Cisco APIC and Switch Software of the *Cisco APIC Installation, Upgrade, and Downgrade Guide*.
- Your Nexus Dashboard Orchestrator must be deployed in Cisco Nexus Dashboard.

  The site upgrade feature is not available for NDO deployments in VMware ESX and you need to follow the standard upgrade procedures described in *Cisco APIC Installation, Upgrade, and Downgrade Guide*
- The fabrics must be running Cisco APIC, Release 4.2(5) or later.

  Fabrics running earlier APIC releases will not be available for selection during the upgrade workflow. Follow the standard upgrade procedures described in *Cisco APIC Installation, Upgrade, and Downgrade Guide*.
- We recommend coordinating the site upgrades with the site administrators managing those fabrics. You may need access to the controllers or switch nodes to troubleshoot any potential issues should they arise.
- If a fabric switch node goes into an `inactive` state in the middle of the upgrade process, for example due to hardware or power failure, the process will be unable to complete. You will not be able to remove or modify the node upgrade policy from NDO during this time as NDO is unable to differentiate whether the node went down or is simply in the middle of a reboot for the upgrade.

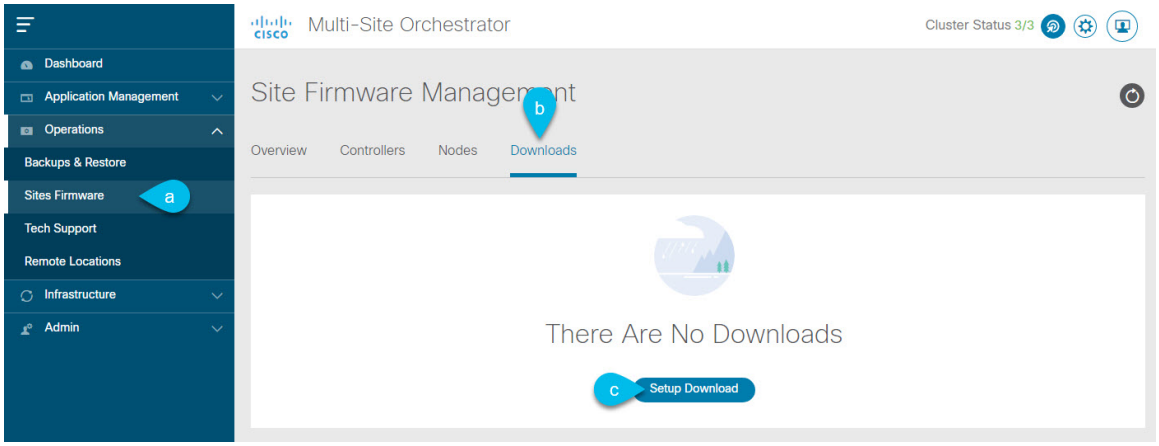
  To resolve this issue, you must manually decommission the inactive node from the APIC, at which point the NDO upgrade policy will recognize the change and return a `failed` status. Then you can update the upgrade policy on the NDO to remove the switch and re-run the upgrade.

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。

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。

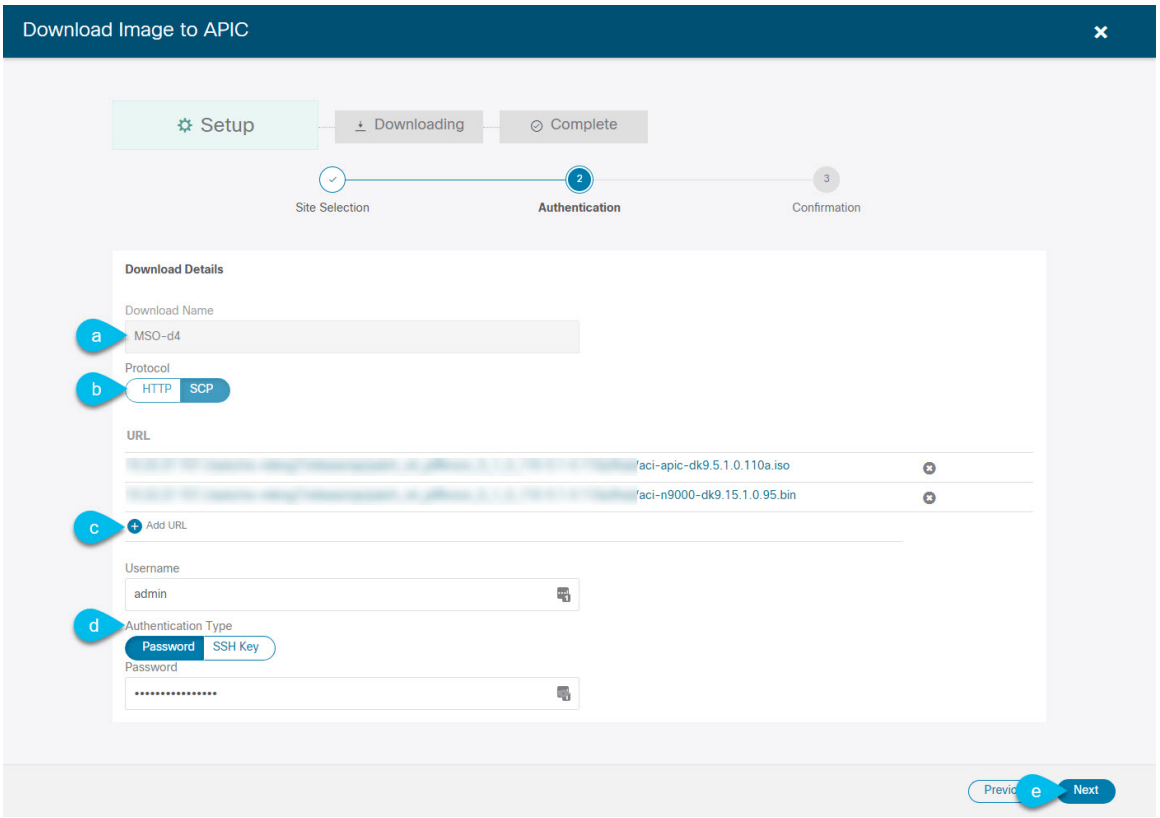
ここで選択したすべてのサイトの Cisco APIC にイメージがダウンロードされます。

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。

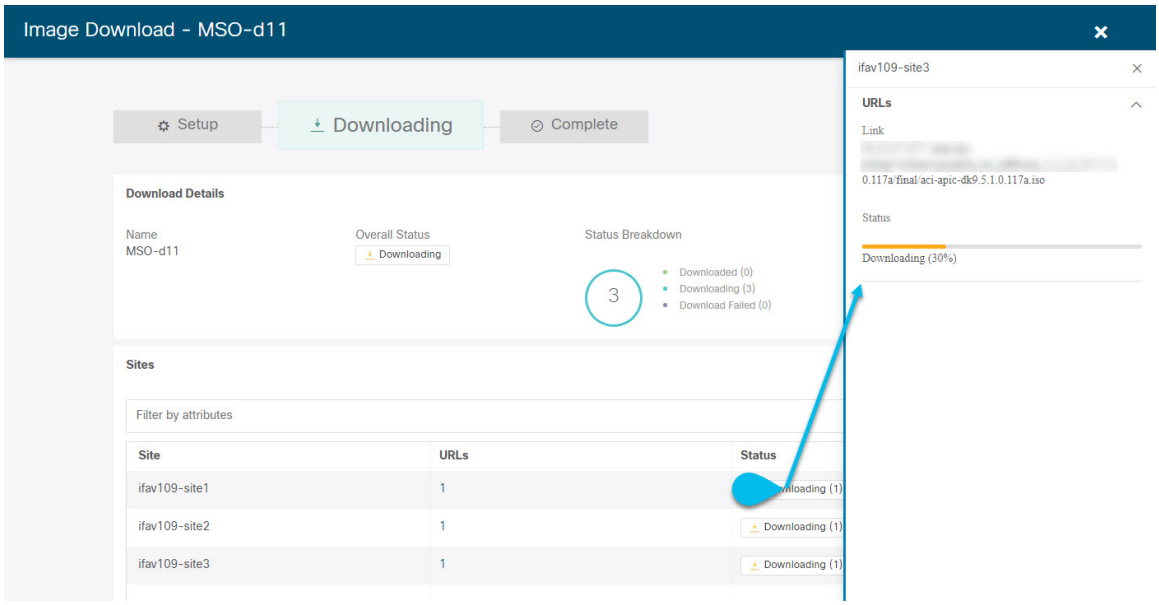
- **パスワード認証**の場合は、前に指定したユーザ名のパスワードを入力します。
- **SSH キー**認証の場合は、**SSH キー**と **SSH キー パスフレーズ**を入力する必要があります。

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。



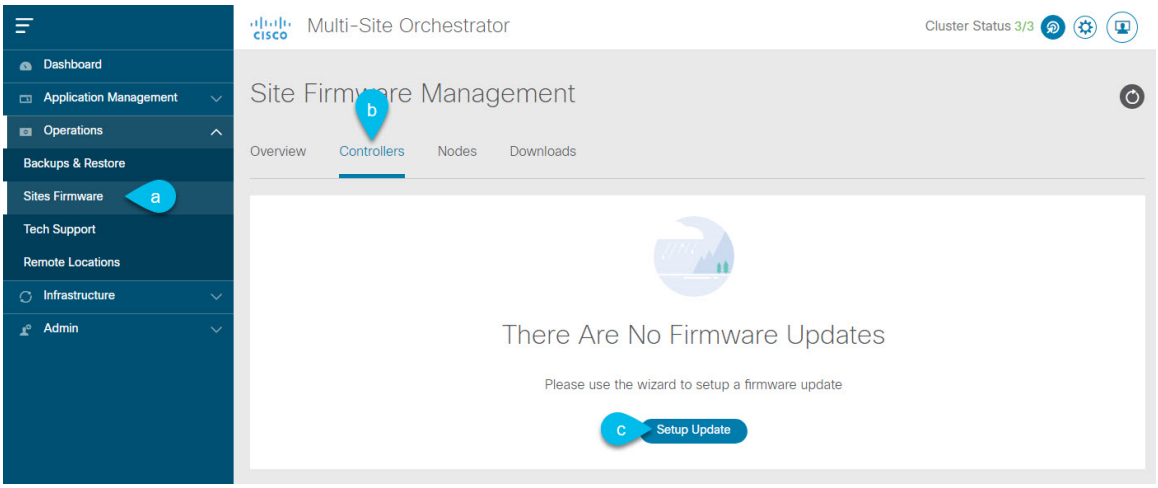
すべてのダウンロードが完了すると、**[完了 (Completed)]** 画面に移行します。**[ダウンロード (Downloading)]** 画面で待機する必要はありません。前の手順で指定したダウンロード名をクリックすると、**[ダウンロード (Downloads)]** タブからいつでも戻ることができます。

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。

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。

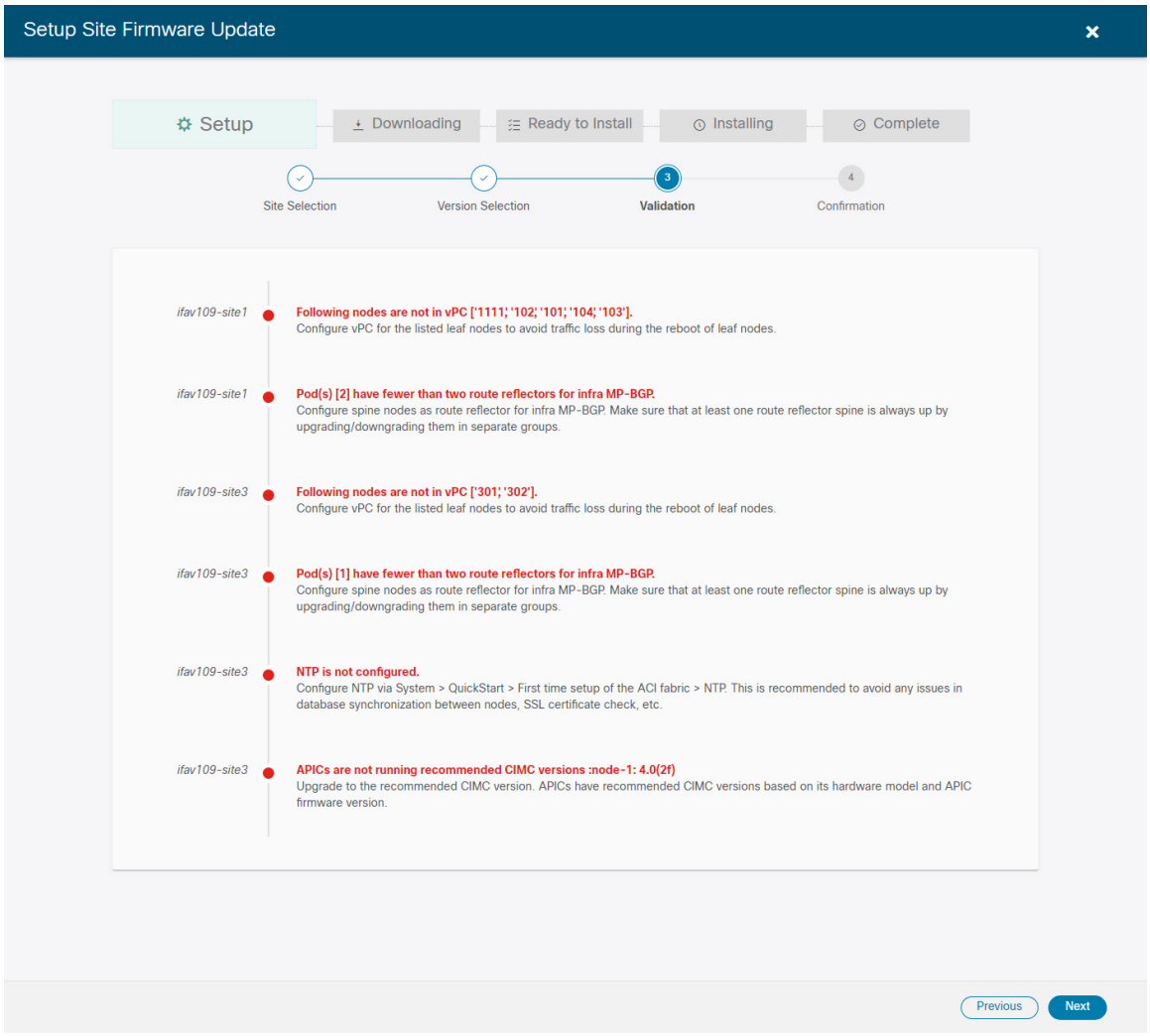
d) [次へ（Next）] をクリックして続行します。

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。

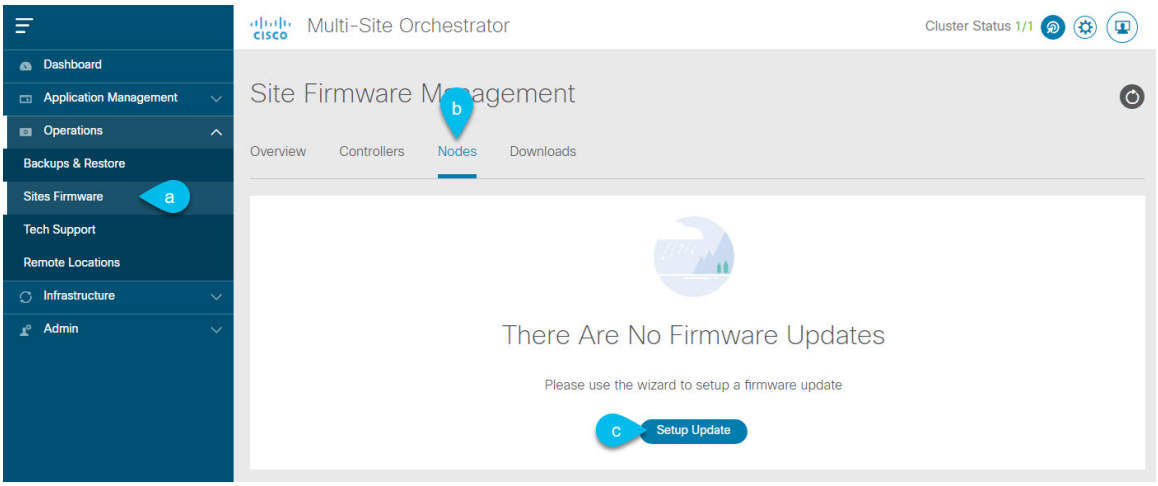
アップグレード プロセス中に NDO からサイトへの接続が失われると、GUI には、接続が失われる前の、アップグレードの最新の既知ステータスが表示されます。接続が再確立されると、アップグレードのステータスが更新されます。接続が失われた後、メインペインの右上にある **[更新 (Refresh)]** ボタンをクリックすると、手動で更新できます。

Upgrading Nodes

This section describes how to set up a software upgrade for your sites' switch nodes.

ステップ 1 Log in to your Nexus Dashboard Orchestrator.

ステップ 2 Set up switch nodes upgrade.



a) From the left navigation pane, select **Operations** > **Sites Firmware**.
b) In the main window, select the **Nodes** tab.
c) Click **Setup Update** tab.

If you have previously set up one or more updates, click the **Setup Update** button in the top right of the main pane instead.

The **Setup Node Firmware Update** screen opens.

ステップ 3 Provide the upgrade details.

a) Provide the **Name**.

This is the upgrade policy name you will be able to use to track the upgrade progress at any time.

b) Click **Select Nodes**.

The **Select Nodes** window opens.

c) Select a site, then select the switch nodes in that site and click **Add and Close**.

You can add switch nodes from a single site at a time. You will repeat this step if you want to add switches from other sites.

d) Repeat the previous substep for nodes in other sites
e) Click **Next** to proceed.

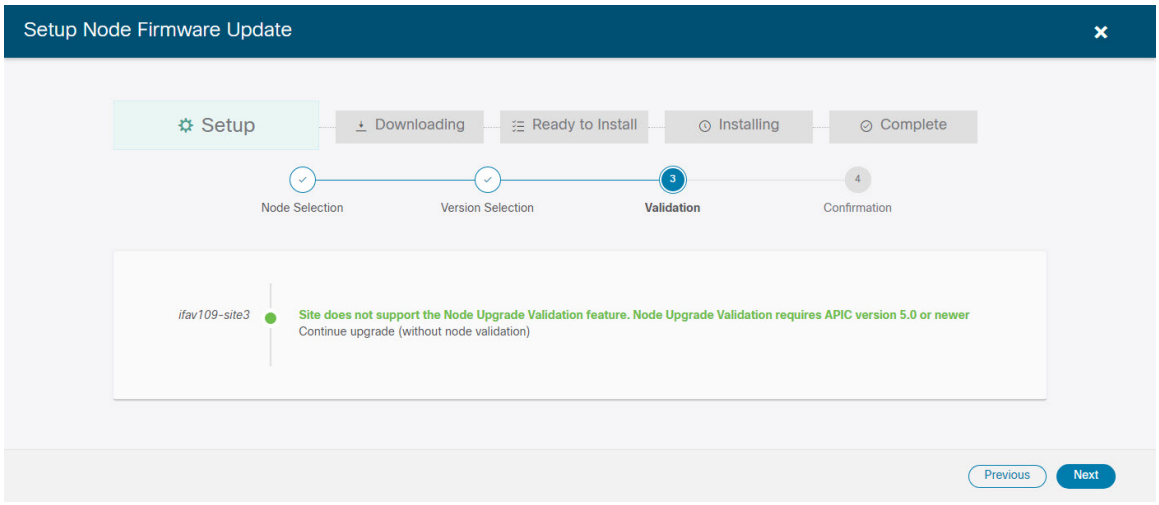
ステップ 4 In the **Version Selection** screen, select the firmware version and click **Next**.

The firmware must be downloaded to the sites before it becomes available here. If the download you set up in previous section has completed successfully but the image is still not available here, close the **Setup Site Firmware Update** screen, navigate back to **Operations** > **Sites Firmware** > **Nodes** tab, and click the **Refresh** button to reload the latest information available for the sites; then restart the upgrade steps.

ステップ 5 In the **Validation** screen, ensure that there are no faults raised, then click **Next**.

Ensure that there are no faults and review any additional information that may affect your upgrade:

Note Sites running releases prior to Release 5.0(1) do not support node validation, so we recommend checking for any switch node faults in the site's APIC prior to starting the upgrade from NDO.



ステップ 6 In the **Confirmation** screen, review the information and click **Submit**.

This will trigger image to be pre-downloaded to all the nodes you have selected. After the download completes, the screen will transition to **Ready to Install** and you can proceed to the next step.

ステップ 7 (Optional) Change **Advanced Settings**.

Note Review the guidelines, recommendations, and limitations for the Cisco APIC upgrade process described in the Upgrading and Downgrading the Cisco APIC and Switch Software of the *Cisco APIC Installation, Upgrade, and Downgrade Guide* before making changes to the advanced options.

In the **Ready to Install** screen, you can open the **Advanced Settings** menu for additional options:

- **Ignore Compatibility Check**—by default, the option is set to `No` and compatibility check is enabled and verifies if an upgrade path from the currently-running version of the system to a specified newer version is supported.

  If you choose to ignore the compatibility check feature, you run the risk of making an unsupported upgrade to your system, which could result in your system going to an unavailable state.

- **Graceful Check**—by default, the option is set to `No` and the upgrade process will not put any of the switches into Graceful Insertion and Removal (GIR) mode before performing the upgrade.

  You can choose to enable this option to bring down the node gracefully (using GIR) while performing the upgrade so that the upgrade will have reduced traffic loss.

- **Run Mode**—by default, the option is set to `Continue on Failure` and if a node upgrade fails, the process proceeds to the next node. Alternatively, you can set this option to `Pause on Failure` to halt upgrade process if any one of the node upgrades fails.

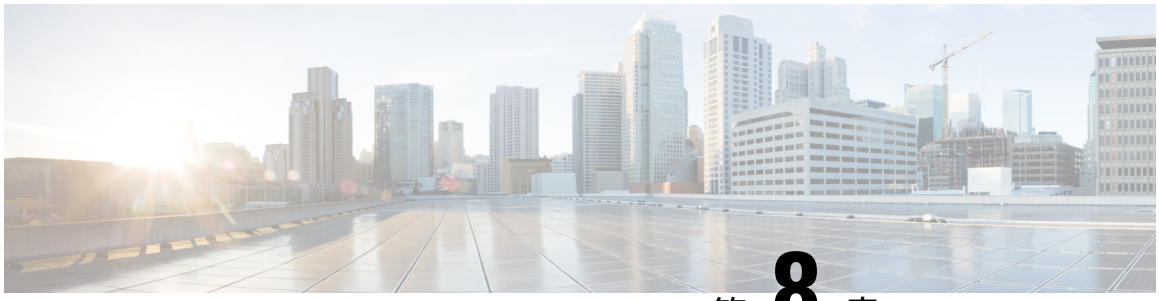
ステップ 8 Remove any nodes marked as `Failed` from the upgrade.

The upgrade cannot proceed if the upgrade policy contains one or more nodes that failed to download the firmware. You can mouse over the `Failed` status for more information and reason for failure.

To remove the nodes from the upgrade, click **Edit Update Details** link in the **Ready to Install** screen.

ステップ 9 Click **Install** to start the upgrade.

If NDO to site connectivity is lost during the upgrade process, the GUI will display the last known status of the upgrade prior to loss of connectivity. Once connectivity is re-established, the upgrade status will be refreshed. You can perform a manual refresh after connectivity loss by clicking the **Refresh** button in the top right of the main pane.



第 8 章

テクニカル サポート

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
```

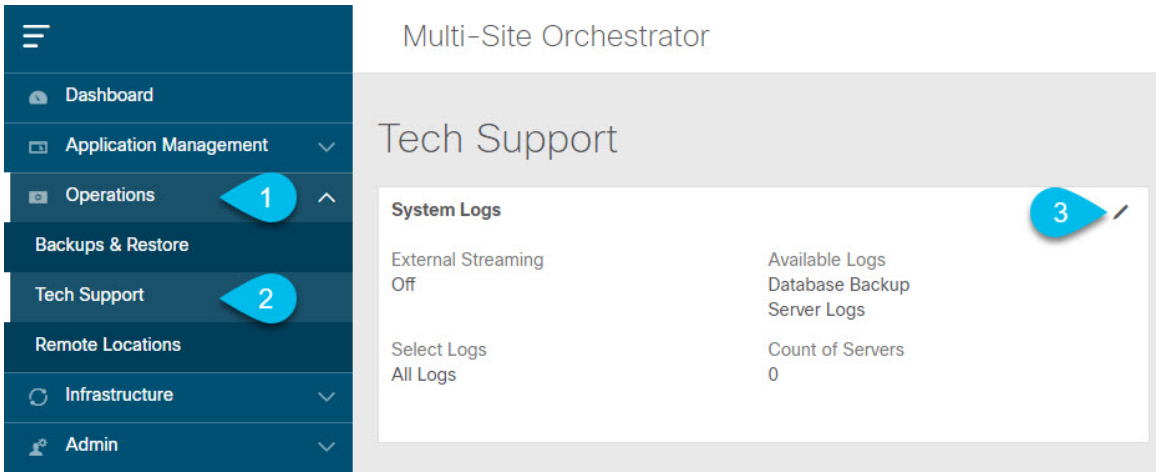
```
msc_consistency.json
...
```

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。

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

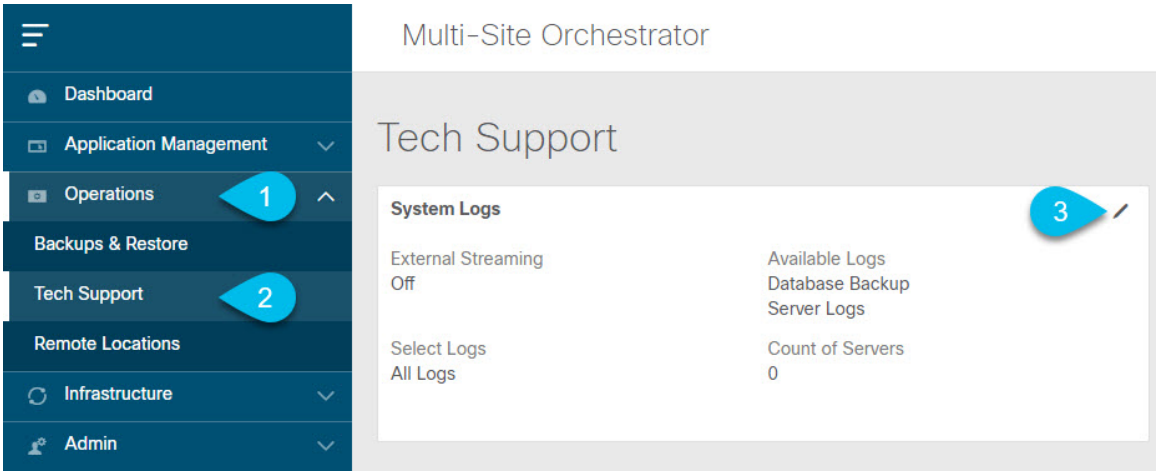
- このリリースでは、外部ログ アナライザーとして Splunk と `syslog` のみがサポートされています。
- このリリースでは、Application Services Engine 展開で Nexus Dashboard Orchestrator の `syslog` のみがサポートされます。
- このリリースは、最大 5 台の外部サーバをサポートします。
- Splunk を使用する場合は、ログ アナライザー サービス プロバイダをセットアップして構成します。

  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。

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。

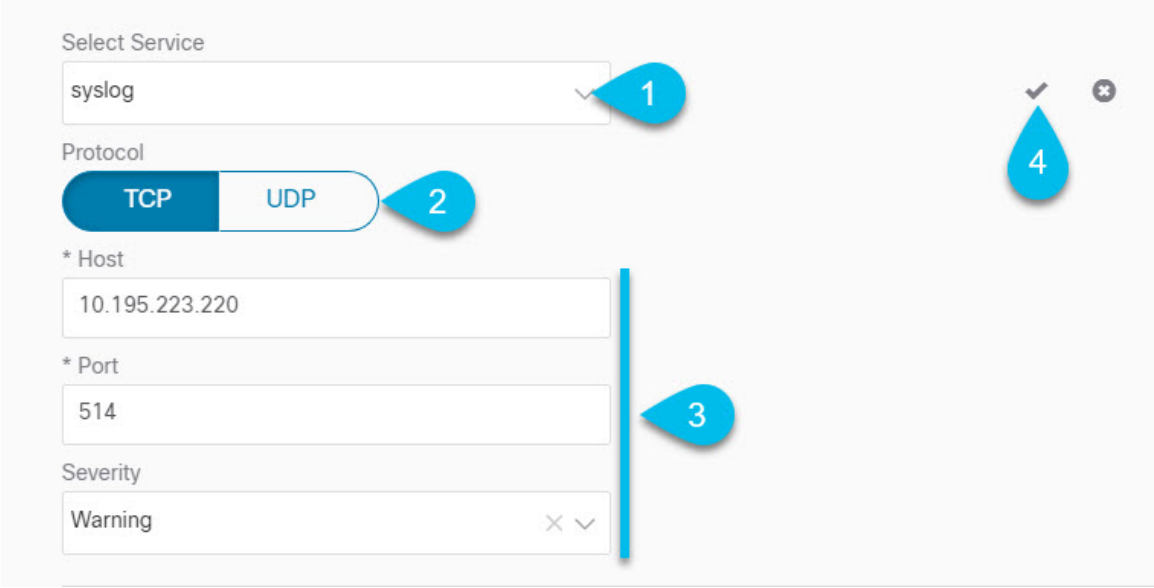
c) Splunk サービスから取得したサーバ名または IP アドレス、ポート、および認証トークンを入力します。

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。

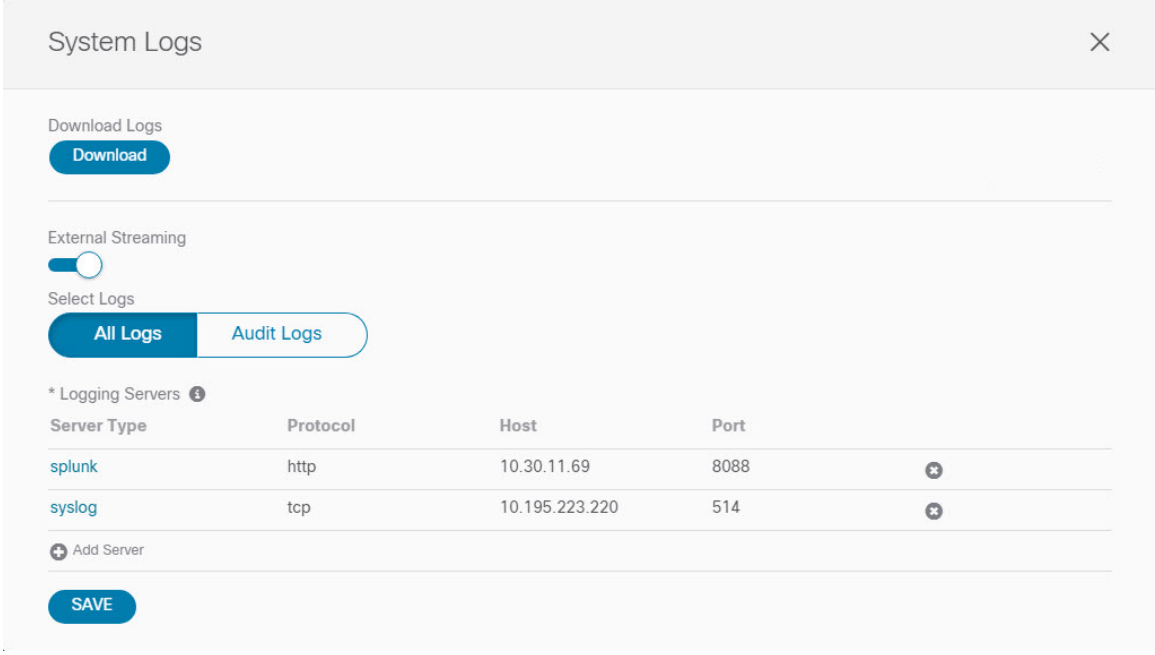
c) サーバー名またはIPアドレス、ポート番号、およびストリーミングするログ メッセージの重大度を指定します。

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。

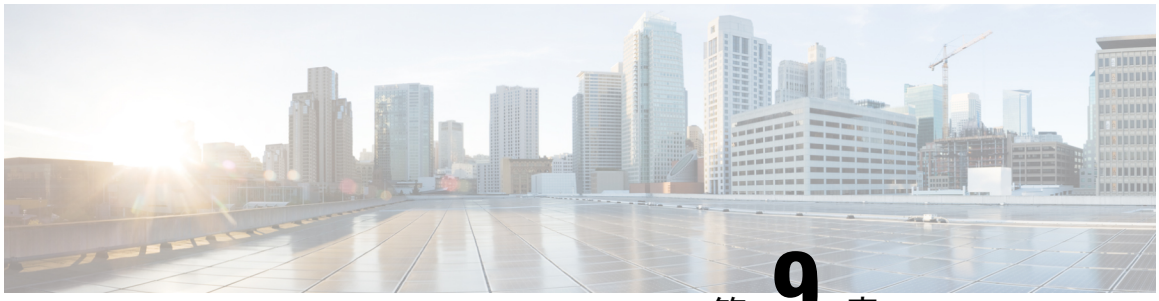
このリリースは、最大 5 台の外部サーバ0をサポートします。

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

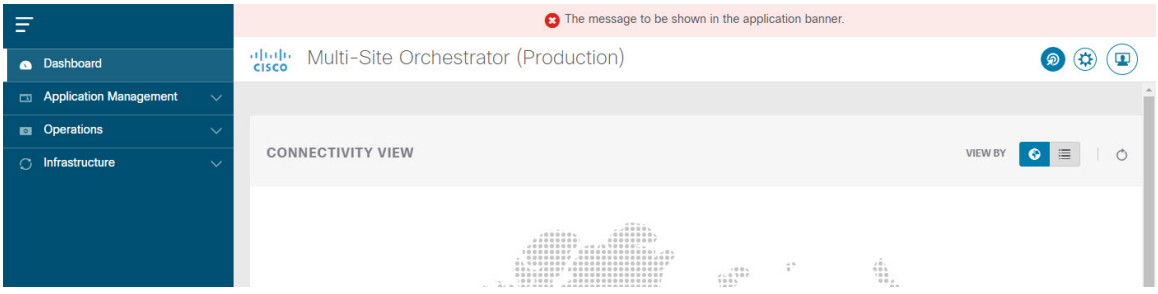
システム設定

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 *13* : システム バナーの表示



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。

ログイン試行回数とロックアウト時間

Orchestratorがログイン試行を連続して失敗したことが検出されると、そのユーザは、不正アクセスを防ぐために、システムからロックアウトされます。ログイン試行が失敗した場合の処理方法は設定できます。たとえば、何回失敗するとロックアウトされるか、およびロックアウトの長さなどがあります。

（注） この機能は、リリース 2.2(1) 以降を最初にインストールしたとき、アップグレードしたときにデフォルトで有効になります。

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 **[試行の失敗&ロックアウト時間 (Fail Attempts & Lockout Time)]**エリアの右側にある **[編集 (Edit)]** アイコンをクリックします。

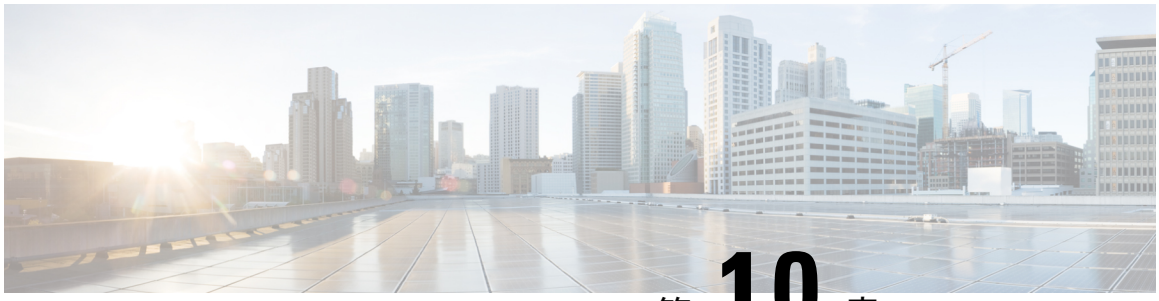
これにより、**[試行の失敗&ロックアウト時間 (Fail Attempts & Lockout Time)]** 設定ウィンドウが表示されます。

ステップ 4 **[試行の失敗の設定 (Fail Attempts Settings)]** ドロップダウンから、ユーザが何回試行に失敗するとロックアウトされるかを選択します。

ステップ 5 **[ロックアウト時間 (分) (Lockout Time (Minutes)]** ドロップダウンから、ロックアウトの長さを選択します。

これは、トリガーされた後の、基本的なロックアウト期間を指定します。このタイマーは、さらにログイン試行が連続して失敗するたびに、3 ずつ延長されます。

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。



第 10 章

NDO サービスのアップグレードまたはダウングレード

Overview

The following sections describe how to upgrade or downgrade Cisco Nexus Dashboard Orchestrator, Release 3.2(1) or later that is deployed in Cisco Nexus Dashboard.

If you are running an earlier release deployed in VMware ESX VMs or Cisco Application Services Engine, you must deploy a brand new cluster and then transfer the configuration from your existing cluster, as described in the "Migrating Existing Cluster to Nexus Dashboard" chapter of the *Nexus Dashboard Orchestrator Deployment Guide*.

Prerequisites and Guidelines

Before you upgrade or downgrade your Cisco Nexus Dashboard Orchestrator cluster:

- Stateful upgrades from releases prior to Release 3.2(1) are not supported.

  If you are upgrading from an earlier release, skip the rest of this chapter and follow the instructions described in the "Migrating Existing Cluster to Nexus Dashboard" section of the *Nexus Dashboard Orchestrator Deployment Guide*.

- Ensure that your current Nexus Dashboard cluster is healthy.

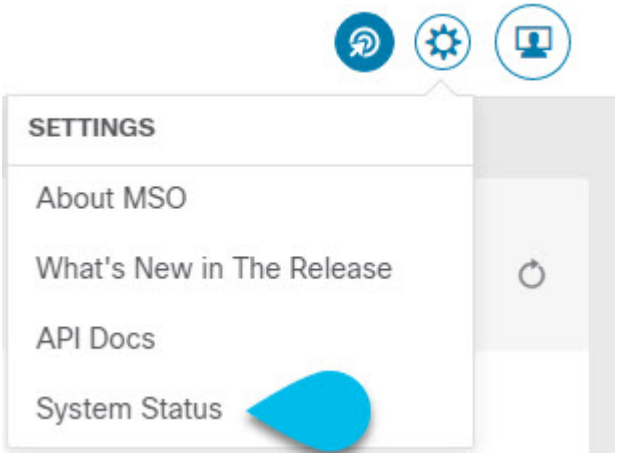
  You can check the Nexus Dashboard cluster health in one of two ways:

  - By logging into your Nexus Dashboard GUI and verifying system status in the **System Overview** page.
  - By logging into any one of the nodes directly as `rescue-user` and running the following command:

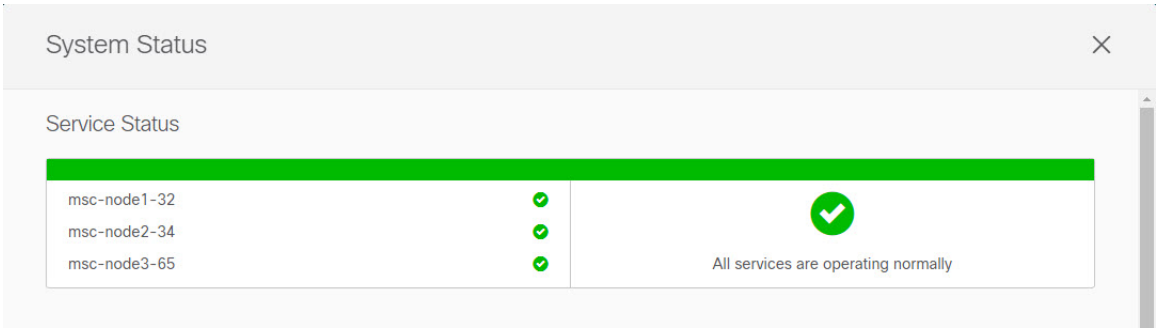
```
# acs health
All components are healthy
```

- Ensure that your current Cisco Nexus Dashboard Orchestrator is running properly.

  You can check the status of you Nexus Dashboard Orchestrator service by navigating to **Settings** > **System Status**:



  Then ensure that the status of all nodes and services is healthy:



- You can upgrade the NDO service in one of two ways:
  - Using the Nexus Dashboard's App Store, as described in Upgrading NDO Service Using Cisco App Store, on page 121.

    In this case, the Cisco DC App Center must be reachable from the Nexus Dashboard via the Management Network directly or using a proxy configuration. Nexus Dashboard proxy configuration is described in the *Nexus Dashboard User Guide*.

Note The App Store allows you to upgrade to the latest available version of the service only. In other words, if release 3.4(1) is available, you cannot use the App Store to upgrade to release 3.3(1) and must use the manual upgrade process as described below.

  - By manually uploading the new app image, as described in NDO サービスの手動アップグレード, on page 123.

You can use this approach if you are unable to establish the connection to the DC App Center or if you want to upgrade to a version of the application that is not the latest available release.

- If you plan to add and manage new Cloud APIC sites after you upgrade your Nexus Dashboard Orchestrator to release 3.3(1) or later, you must ensure that they are running Cloud APIC release 5.2(1) or later.

  On-boarding and managing Cloud APIC sites running earlier releases is not support in Nexus Dashboard Orchestrator 3.3(1).

- Downgrading to releases prior to release 3.3(1) is not supported.

  If you want to downgrade to an earlier release, you must deploy a new Nexus Dashboard Orchestrator cluster on a platform supported by the earlier release, then restore the older configuration backup. Restoring backups created on Release 3.3(1) or later to an older NDO cluster is not supported.

  If you downgrade to an earlier release of Nexus Dashboard Orchestrator, you must also downgrade all Cloud APIC sites to a release prior to Release 5.2(1).

Upgrading NDO Service Using Cisco App Store

This section describes how to upgrade Cisco Nexus Dashboard Orchestrator, Release 3.2(1) or later.

Before you begin

- Ensure that you have completed the prerequisites described in Prerequisites and Guidelines, on page 119.
- Ensure that Cisco DC App Center is reachable from the Nexus Dashboard via the Management Network directly or using a proxy configuration.

  Nexus Dashboard proxy configuration is described in the *Nexus Dashboard User Guide*

ステップ 1 Log in to your Nexus Dashboard..

ステップ 2 From the left navigation menu, select **Service Catalog**.

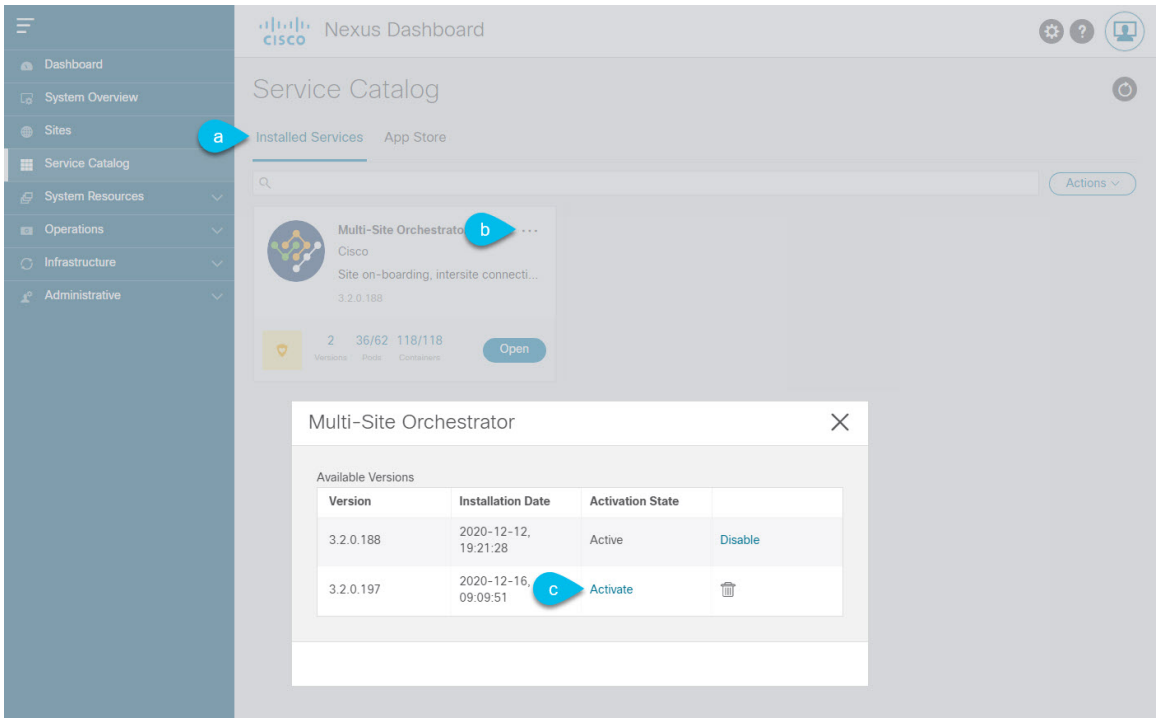
ステップ 3 Upgrade the application using the App Store.

a) In the **Service Catalog** screen, select the **App Store** tab.
b) In the **Nexus Dashboard Orchestrator** tile, click **Upgrade**.
c) In the License Agreement window that opens, click **Agree and Download**.

ステップ 4 Wait for the new image to initialize.

It may take up to 20 minutes for the new application image to become available.

ステップ 5 Activate the new image.



a) In the **Service Catalog** screen, select the **Installed Services** tab.
b) In the top right of the Nexus Dashboard Orchestrator tile, click the menu (. . .) and choose **Available Versions**.
c) In the available versions window, click **Activate** next to the new image.

Note Do not **Disable** the currently running image before activating the new image. The image activation process will recognize the currently running image and perform the upgrade workflows necessary for the currently running app version.

It may take up to 20 additional minutes for all the application services to start and the GUI to become available. The page will automatically reload when the process is completed.

ステップ 6 (Optional) Delete the old application image.

You can choose to retain the old application version in case you ever want to downgrade. Or you can delete it as described in this step.

a) In the **Service Catalog** screen, select the **Installed Services** tab.
b) In the top right of the Nexus Dashboard Orchestrator tile, click the menu (. . .) and choose **Available Versions**.
c) In the available versions window, click the delete icon next to the image you want to delete.

ステップ 7 Launch the app.

To launch the app, simply click **Open** on the application tile in the Nexus Dashboard's **Service Catalog** page.

The single sign-on (SSO) feature allows you to log in to the application using the same credentials as you used for the Nexus Dashboard.

NDO サービスの手動アップグレード

ここでは、Cisco Nexus Dashboard Orchestrator リリース 3.2(1) 以降をアップグレードする方法について説明します。

始める前に

- Prerequisites and Guidelines （119 ページ） で説明している前提条件をすべて満たしていることを確認します。

ステップ 1 ターゲットのリリース イメージをダウンロードします。

a) DC App Center で Nexus Dashboard Orchestrator ページを参照します。
https://dcappcenter.cisco.com/nexus-dashboard-orchestrator.html

b) **[バージョン (Version)]** ドロップダウンから、インストールするバージョンを選択し、**[ダウンロード (Download)]** をクリックします。

c) **[同意してダウンロード (Agree and download)]** をクリックしてライセンス契約に同意し、イメージをダウンロードします。

ステップ 2 Nexus Dashboard にログインします。

ステップ 3 Nexus ダッシュボードにイメージをアップロードします。

a) 左のナビゲーションメニューから **[サービス カタログ (Service Catalog)]** を選択します。

b) Nexus ダッシュボードの **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。

c) メインペインの右上にある **[アクション (Actions)]** メニューから、**[アプリケーションのアップロード (Upload App)]** を選択します。

d) **[アプリケーションのアップロード (Upload App)]** ウィンドウで、イメージの場所を選択します。

アプリケーション イメージをシステムにダウンロードした場合は、**[ローカル (Local)]** を選択します。

サーバでイメージをホストしている場合は、**[リモート (Remote)]** を選択します。

e) ファイルを選択します。

前のサブステップで **[ローカル (Local)]** を選択した場合は、**[ファイルの選択 (Select File)]** をクリックし、ダウンロードしたアプリケーションイメージを選択します。

[リモート（Remote）] を選択した場合は、イメージ ファイルのフル URL を指定します。たとえば、`http://<ip-address>:<port>/<full-path>/cisco-mso-<version>.nap` のようになります。

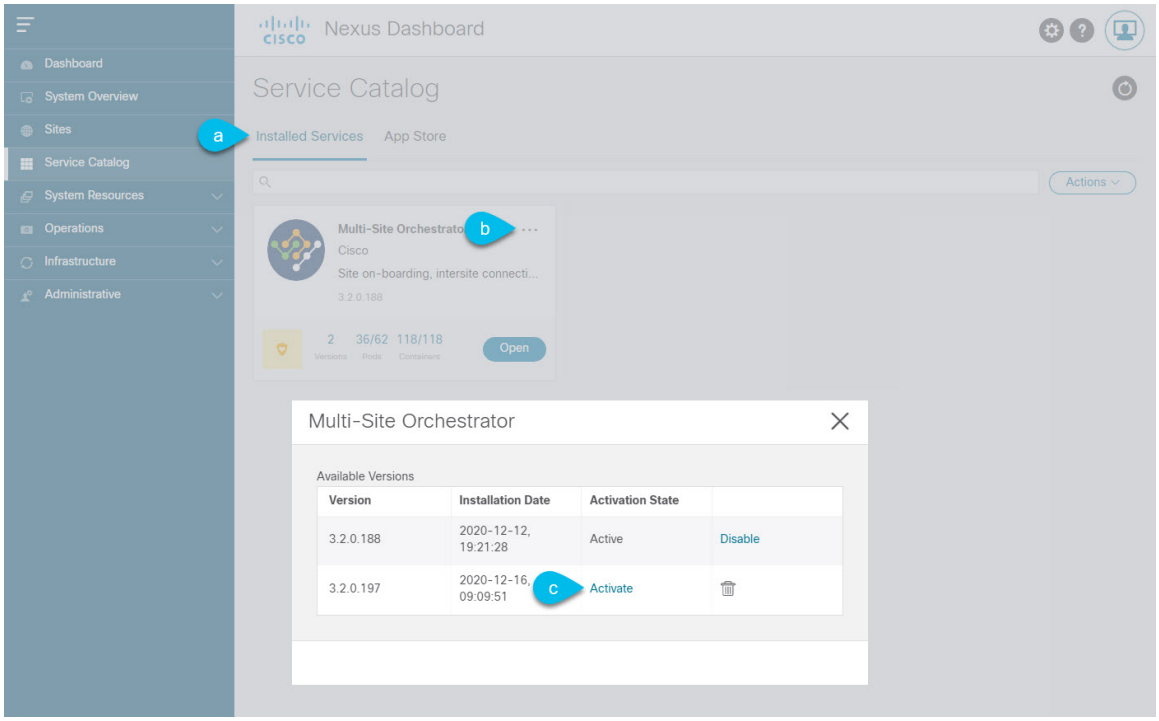
f) **[アップロード (Upload)]** をクリックして、アプリケーションをクラスタに追加します。

アップロードの進行状況バーとともに新しいタイルが表示されます。イメージのアップロードが完了すると、Nexus ダッシュボードは新しいイメージを既存のアプリケーションとして認識し、新しいバージョンとして追加します。

ステップ 4 新しいイメージが初期化されるまで待ちます。

新しいアプリケーションイメージが使用可能になるまでに最大 20 分かかることがあります。

ステップ 5 新しい画像をアクティブにします。



a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。

b) [Nexus Dashboard Orchestrator]タイルの右上にあるメニュー（...）をクリックし、**[利用可能なバージョン (Available Versions)]** を選択します。

c) [Available Versions]ウィンドウで、新しいイメージの横にある **[アクティベート (Activate)]** をクリックします。

（注） 新しいイメージをアクティブにする前に、現在実行中のイメージを**無効にしないでください**。イメージアクティベーション プロセスは、現在実行中のイメージを認識し、現在実行中のアプリケーション バージョンに必要なアップグレード ワークフローを実行します。

すべてのアプリケーション サービスが起動し、GUI が使用可能になるまでに、さらに最大 20 分かかる場合があります。このページは、プロセスが完了した時点で自動的に再ロードされます。

ステップ 6 （任意）古いアプリケーション イメージを削除します。

ダウングレードする場合に備えて、古いアプリケーション バージョンを保持しておくこともできます。または、この手順の説明に従って削除することもできます。

a) **[サービス カタログ (Service Catalog)]** 画面で、**[インストール済みサービス (Installed Services)]** タブを選択します。

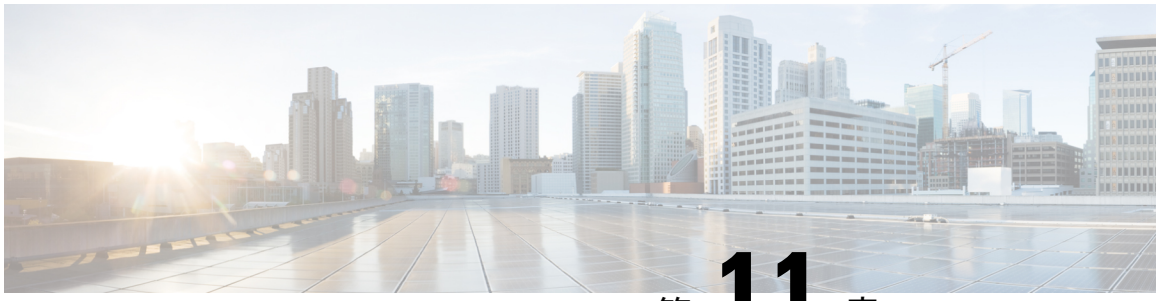
b) [Nexus Dashboard Orchestrator]タイルの右上にあるメニュー（...）をクリックし、**[利用可能なバージョン (Available Versions)]** を選択します。

c) 使用可能なバージョンのウィンドウで、削除するイメージの横にある削除アイコンをクリックします。

ステップ 7 アプリを起動します。

アプリケーションを起動するには、Nexus ダッシュボードの **[サービスカタログ (Service Catalog)]** ページのアプリケーションタイルで **[開く (Open)]** をクリックします。

シングルサインオン（SSO）機能を使用すると、Nexus ダッシュボードで使用したものと同じクレデンシャルを使用してアプリケーションにログインできます。



第 11 章

Cisco ACI サイトの設定

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。

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。

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 （129 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 （128 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。

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。

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。

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。

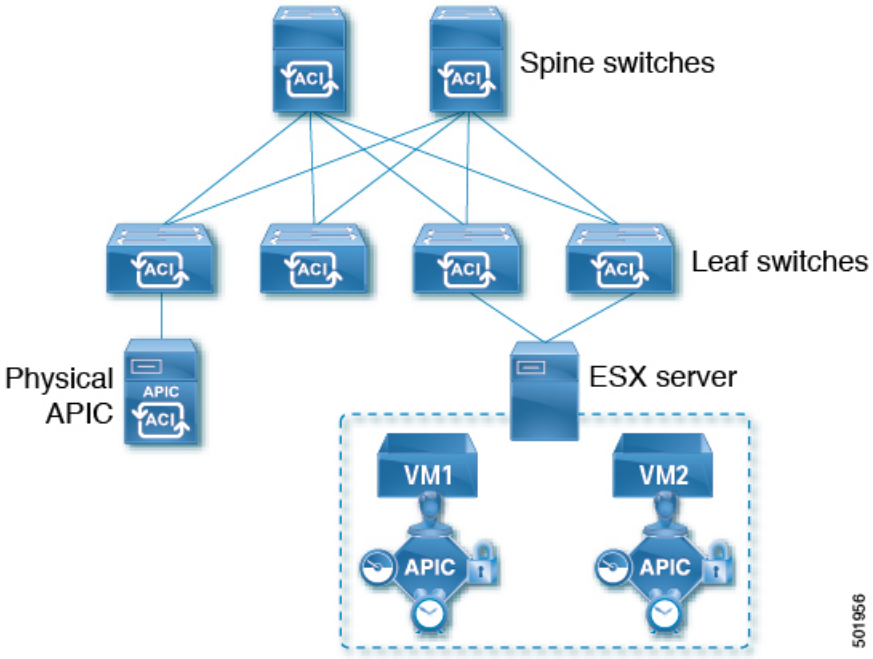
Cisco Mini ACI Fabrics

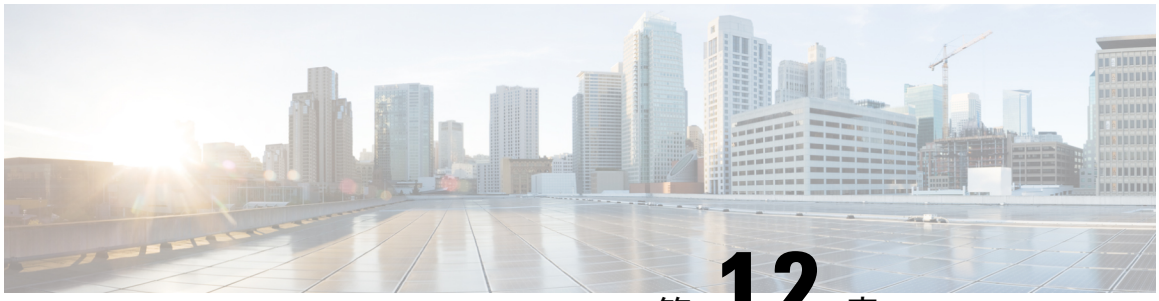
Cisco Multi-Site supports Cisco Mini ACI fabrics as typical on-premises sites without requiring any additional configuration. This section provides a brief overview of Mini ACI fabrics, detailed info on deploying and configuring this type of fabrics is available in *Cisco Mini ACI Fabric and Virtual APICs*.

Cisco ACI, Release 4.0(1) introduced Mini ACI Fabric for small scale deployment. Mini ACI fabric works with Cisco APIC cluster consisting of one physical APIC and two virtual APICs (vAPIC) running in virtual machines. This reduces the physical footprint and cost of the APIC cluster, allowing ACI fabric to be deployed in scenarios with limited rack space or initial budget, such as a colocation facility or a single-room data center, where a full-scale ACI installations may not be practical due to physical footprint or initial cost.

The following diagram shows an example of a mini Cisco ACI fabric with a physical APIC and two virtual APICs (vAPICs):

Figure 14: Cisco Mini ACI Fabric





第 12 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)

Adding Cisco ACI Sites

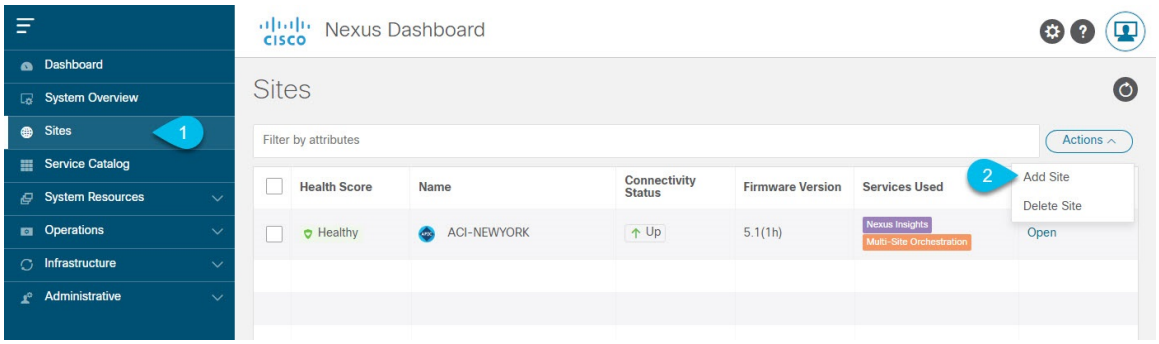
This section describes how to add a Cisco APIC or Cloud APIC site using the Nexus Dashboard GUI and then enable that site to be managed by Nexus Dashboard Orchestrator.

Before you begin

- If you are adding on-premises ACI site, you must have completed the site-specific configurations in each site's APIC, as described in previous sections in this chapter.
- You must ensure that the site(s) you are adding are running Release 4.2(4) or later.

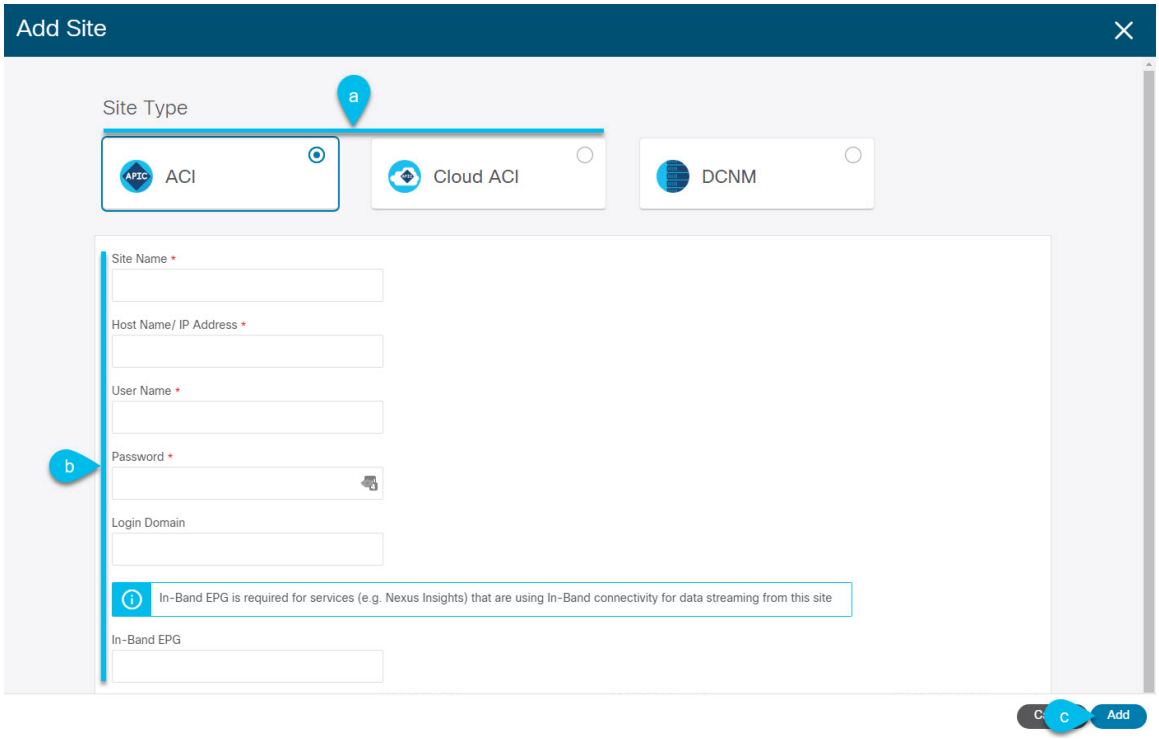
ステップ 1 Log in to the Nexus Dashboard GUI

ステップ 2 Add a new site.



a) From the left navigation menu, select **Sites**.
b) In the top right of the main pane, select **Actions** > **Add Site**.

ステップ 3 Provide site information.



a) For **Site Type**, select **ACI** or **Cloud ACI** depending on the type of ACI fabric you are adding.
b) Provide the controller information.

- You need to provide the **Host Name/IP Address**, **User Name**, and **Password.** for the APIC controller currently managing your ACI fabrics.

  Note For APIC fabrics, if you will use the site with Nexus Dashboard Orchestrator service only, you can provide either the in-band or out-of-band IP address of the APIC. If you will use the site with Nexus Dashboard Insights as well, you must provide the in-band IP address.

- For on-premises ACI sites managed by Cisco APIC, if you plan to use this site with Day-2 Operations applications such as Nexus Insights, you must also provide the **In-Band EPG** name used to connect the Nexus Dashboard to the fabric you are adding. Otherwise, if you will use this site with Nexus Dashboard Orchestrator only, you can leave this field blank.

- For cloud ACI sites, **Enable Proxy** if your cloud site is reachable via a proxy.

  Proxy must be already configured in your Nexus Dashboard's cluster settings. If the proxy is reachable via management network, a static management network route must also be added for the proxy IP address. For more information about proxy and route configuration, see Nexus Dashboard User Guide for your release.

c) Click **Add** to finish adding the site.

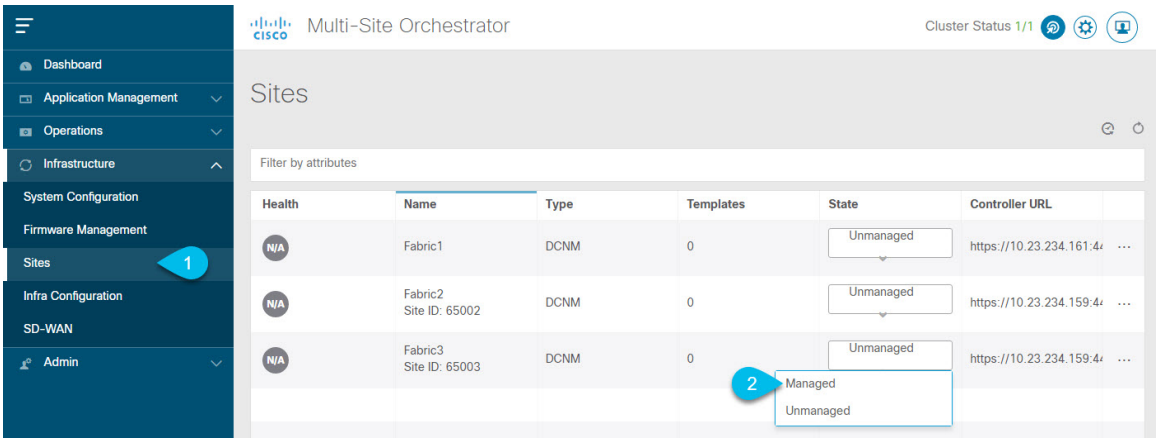
At this time, the sites will be available in the Nexus Dashboard, but you still need to enable them for Nexus Dashboard Orchestrator management as described in the following steps.

ステップ 4 Repeat the previous steps for any additional ACI sites.

ステップ 5 From the Nexus Dashboard's **Service Catalog**, open the Nexus Dashboard Orchestrator service.

You will be automatically logged in using the Nexus Dashboard user's credentials.

ステップ 6 In the Nexus Dashboard Orchestrator GUI, manage the sites.



a) From the left navigation menu, select **Infrastructure** > **Sites**.

b) In the main pane, change the **State** from `Unmanaged` to `Managed` for each fabric that you want the NDO to manage.

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。

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 サイトのアンダーレイ設定を削除します。

a) 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）]**>**[インフラの設定（Infra Configuration）]**を選択します。
b) メイン ペインにある **[インフラの設定（Configure Infra）]** 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) 右側のバーの **[オーバレイの設定 (Overlay Configuration)]** タブで、**[Multi-Site]** ノブを無効にします。
e) 右側のサイドバーで、**[アンダーレイ設定 (Underlay Configuration)]** タブを選択します。
f) サイトからすべてのアンダーレイ設定を削除します。
g) **[展開 (Deploy)]** をクリックして、アンダーレイとオーバーレイの設定変更をサイトに展開します。

ステップ 3 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、NDOで管理する各ファブリックの **[状態 (State)]** を `[管理対象 (Managed)]` から `[非管理対象 (Unmanaged)]` に変更します。

（注） 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 4 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アプリケーション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) 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。
b) 削除するサイトを1つ以上選択します。
c) 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。
d) 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。

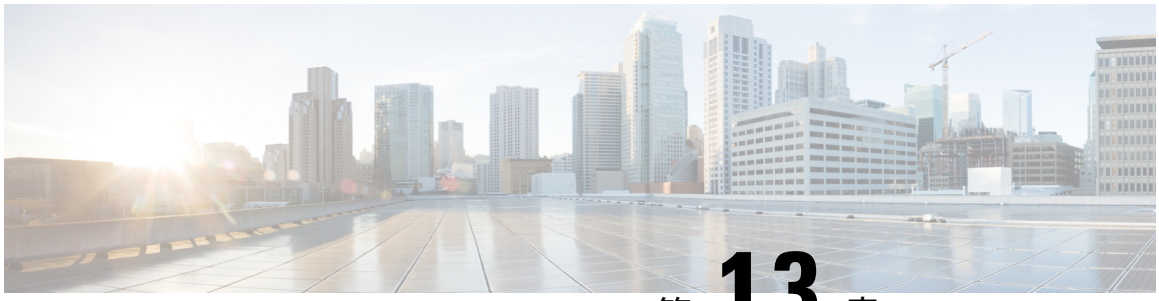
ファブリック コントローラへの相互起動

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。



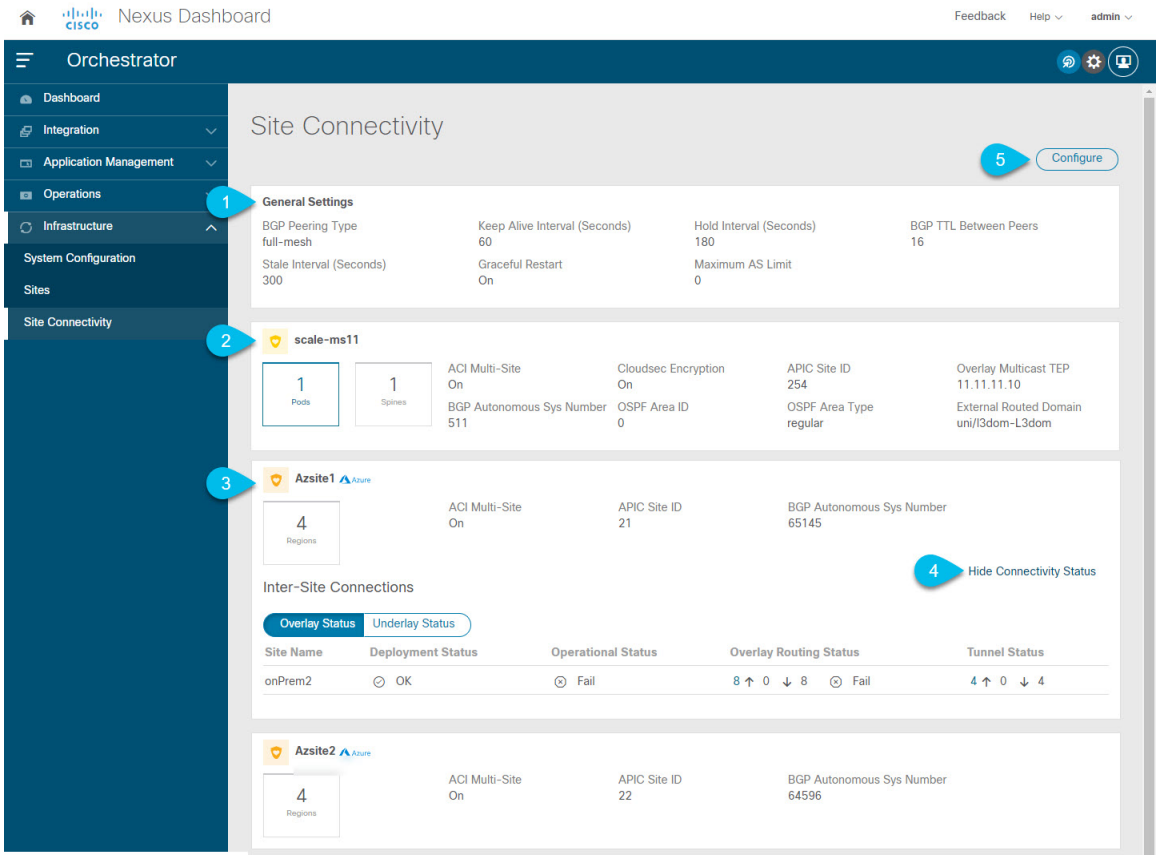
第 13 章

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 *15:* 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 （151 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 APIC サイトのインフラの設定 （159 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（151 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 APIC 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（クラウド APIC 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。

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。

  `[フルメッシュ]` 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 DCNM 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。

クラウド APIC 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、以前の Nexus Dashboard Orchestrator リリースでサイト間接続用にクラウド APIC で以前に設定した、オンプレミス IPN ピアリング用のクラウドサイトで使用される OSPF エリア ID です。

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Configuring Infra: On-Premises Site Settings （152 ページ）を参照してください。

a) **[デバイス (Devices)]** タブを選択します。

b) **[IPN デバイスの追加 (Add IPN Device)]** をクリックします。

c) IPN デバイスの **[名前（Name）]** と **[IPアドレス（IP Address）]** を入力します。

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 APIC の CSR からのトンネル ピア アドレスとして使用されます。

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。

ステップ 7 **[外部 デバイス（External Devices）]** 情報を入力します。

クラウド APIC サイトがない場合、このタブは UI に表示されません。

Multi-Site ドメインにクラウド APIC 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、クラウド APIC 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。

クラウド APIC 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クラウド APIC 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。

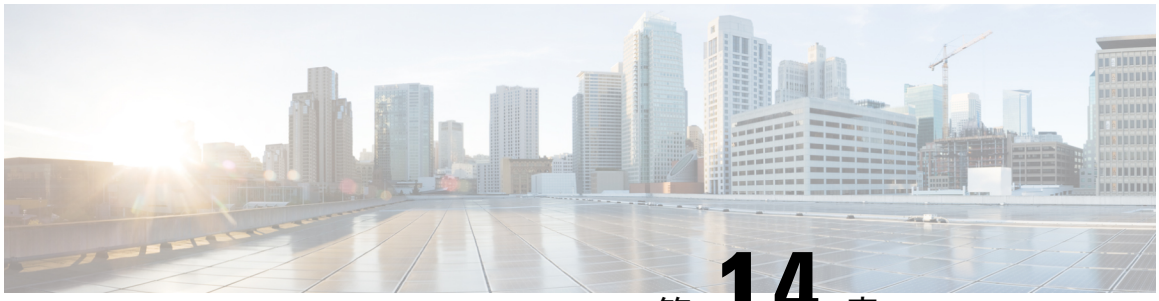
e) チェックマーク アイコンをクリックして、サブネット情報を保存します。

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（オンプレミス ACI、クラウド ACI、またはオンプレミス ファブリック）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 14 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。

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。

Configuring Infra: On-Premises Site Settings

This section describes how to configure site-specific Infra settings for on-premises sites.

ステップ 1 Log in to the Cisco Nexus Dashboard Orchestrator GUI.

ステップ 2 In the left navigation menu, select **Infrastructure** > **Site Connectivity**.

ステップ 3 In the top right of the main pane, click **Configure**.

ステップ 4 In the left pane, under **Sites**, select a specific on-premises site.

ステップ 5 Provide the **Inter-Site Connectivity** information.

a) In the right **<*Site*> Settings** pane, enable the **Multi-Site** knob.

This defines whether the overlay connectivity is established between this site and other sites.

b) (Optional) Enable the **CloudSec Encryption** knob encryption for the site.

CloudSec Encryption provides inter-site traffic encryption. The "Infrastructure Management" chapter in the *Cisco Multi-Site Configuration Guide* covers this feature in detail.

c) Specify the **Overlay Multicast TEP**.

This address is used for the inter-site L2 BUM and L3 multicast traffic. This IP address is deployed on all spine switches that are part of the same fabric, regardless of whether it is a single pod or Multi-Pod fabric.

This address should not be taken from the address space of the original fabric's `Infra` TEP pool or from the `0.x.x.x` range.

d) Specify the **BGP Autonomous System Number**.

e) (Optional) Specify the **BGP Password**.

f) Provide the **OSPF Area ID**.

The following settings are required if you are using OSPF protocol for underlay connectivity between the site and the IPN. If you plan to use BGP instead, you can skip this step. BGP underlay configuration is done at the port level, as described in インフラの設定: スパイン スイッチ, on page 155.

g) Select the **OSPF Area Type** from the dropdown menu.

The following settings are required if you are using OSPF protocol for underlay connectivity between the site and the IPN. If you plan to use BGP instead, you can skip this step. BGP underlay configuration is done at the port level, as described in インフラの設定: スパイン スイッチ, on page 155.

The OSPF area type can be one of the following:

- `nssa`
- `regular`

h) Configure OSPF policies for the site.

The following settings are required if you are using OSPF protocol for underlay connectivity between the site and the IPN. If you plan to use BGP instead, you can skip this step. BGP underlay configuration is done at the port level, as described in インフラの設定: スパイン スイッチ, on page 155.

You can either click an existing policy (for example, `msc-ospf-policy-default`) to modify it or click **+Add Policy** to add a new OSPF policy. Then in the **Add/Update Policy** window, specify the following:

- In the **Policy Name** field, enter the policy name.
- In the **Network Type** field, choose either `broadcast`, `point-to-point`, or `unspecified`.

  The default is `broadcast`.
- In the **Priority** field, enter the priority number.

  The default is `1`.
- In the **Cost of Interface** field, enter the cost of interface.

  The default is `0`.
- From the **Interface Controls** dropdown menu, choose one of the following:
  - **advertise-subnet**
  - **bfd**
  - **mtu-ignore**
  - **passive-participation**
- In the **Hello Interval (Seconds)** field, enter the hello interval in seconds.

  The default is `10`.
- In the **Dead Interval (Seconds)** field, enter the dead interval in seconds.

  The default is `40`.
- In the **Retransmit Interval (Seconds)** field, enter the retransmit interval in seconds.

  The default is `5`.
- In the **Transmit Delay (Seconds)** field, enter the transmit delay in seconds.

  The default is `1`.

i) (Optional) From the **External Routed Domain** dropdown, select the domain you want to use.

Choose an external router domain that you have created in the Cisco APIC GUI. For more information, see the *Cisco APIC Layer 3 Networking Configuration Guide* specific to your APIC release.

j) (Optional) Enable **SDA Connectivity** for the site.

If the site is connected to an SDA network, enable the **SDA Connectivity** knob and provide the **External Routed Domain**, **VLAN Pool**, and **VRF Lite IP Pool Range** information.

If you enable SDA connectivity for the site, you will need to configure additional settings as described in the SDA use case chapter of the *Cisco Multi-Site Configuration Guide for ACI Fabrics*.

k) (Optional) Enable **SR-MPLS Connectivity** for the site.

If the site is connected via an MPLS network, enable the **SR-MPLS Connectivity** knob and provide the Segment Routing global block (SRGB) range.

The Segment Routing Global Block (SRGB) is the range of label values reserved for Segment Routing (SR) in the Label Switching Database (LSD). These values are assigned as segment identifiers (SIDs) to SR-enabled nodes and have global significance throughout the domain.

The default range is `16000-23999`.

If you enable MPLS connectivity for the site, you will need to configure additional settings as described in the "Sites Connected via SR-MPLS" chapter of the *Cisco Multi-Site Configuration Guide for ACI Fabrics*.

ステップ 6 Configure inter-site connectivity between on-premises and cloud sites.

If you do not need to create inter-site connectivity between on-premises and cloud sites, for example if your deployment contains only cloud or only on-premises sites, skip this step.

When you configure underlay connectivity between on-premises and cloud sites, you need to provide an IPN device IP address to which the Cloud APIC's CSRs establish a tunnel and then configure the cloud site's infra settings.

a) Click **+Add IPN Device** to specify an IPN device.
b) From the dropdown, select one of the IPN devices you defined previously.

The IPN devices must be already defined in the **General Settings** > **IPN Devices** list, as described in インフラの設定: 一般設定, on page 146

c) Configure inter-site connectivity for cloud sites.

Any previously configured connectivity from the cloud sites to this on-premises site will be displayed here, but any additional configuration must be done from the cloud site's side as described in Cisco Cloud APIC サイトのインフラの設定, on page 159.

What to do next

While you have configured all the required inter-site connectivity information, it has not been pushed to the sites yet. You need to deploy the configuration as described in インフラ設定の展開, on page 163

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。

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、CiscoMulti-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。

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 ～ 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、Configuring Infra: On-Premises Site Settings （152 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 APIC 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。

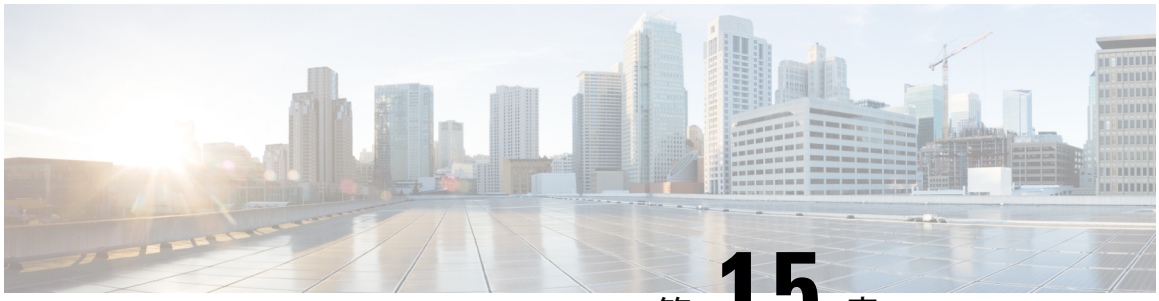
- **[BGP パスワード (BGP Password)]** フィールドに、BGP ピア パスワードを入力します。

- 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 15 章

Cisco Cloud APIC サイトのインフラの設定

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。

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。

Configuring Infra: Cloud Site Settings

This section describes how to configure site-specific Infra settings for Cloud APIC sites.

ステップ 1 Log in to the Cisco Nexus Dashboard Orchestrator GUI.

ステップ 2 In the left navigation menu, select **Infrastructure** > **Site Connectivity**.

ステップ 3 In the top right of the main pane, click **Configure**.

ステップ 4 In the left pane, under **Sites**, select a specific cloud site.

ステップ 5 Provide the general **Inter-Site Connectivity** information.

a) In the right **<*Site*> Settings** pane, select the **Inter-Site Connectivity** tab.

b) Enable the **Multi-Site** knob.

This defines whether the overlay connectivity is established between this site and other sites.

Note that the overlay configuration will not be pushed to sites which do not have the underlay intersite connectivity established as desrcibed in the next step.

c) (Optional) Specify the **BGP Password**.

ステップ 6 Provide site-specific **Inter-Site Connectivity** information.

a) In the right properties sidebar for the cloud site, click **Add Site**.

The **Add Site** window opens.

b) Under **Connected to Site**, click **Select a Site** and select the site (for example, `Site2`) to which you want to establish connectivity from the site you are configuring (for example, `Site1`) .

Once you select the remote site, the **Add Site** window will update to reflect both directions of connectivity: **Site1 > Site2** and **Site2 > Site1**.

c) In the **Site1 > Site2** area, from the **Connection Type** dropdown, choose the type of connection between the sites.

The following options are available:

- `Public Internet`—connectivity between the two sites is established via the Internet.

  This type is supported between any two cloud sites or between a cloud site and an on-premises site.

- `Private Connection`—connectivity is established using a private connection between the two sites.

  This type is supported between a cloud site and an on-premises site.

- `Cloud Backbone`—connectivity is established using cloud backbone.

  This type is supported between two cloud sites of the same type, such as Azure-to-Azure or AWS-to-AWS.

If you have multiple types of sites (on-premises, AWS, and Azure), different pairs of site can use different connection type.

d) Choose the **Protocol** that you want to use for connectivity between these two sites.

If using **BGP-EVPN** connectivity, you can optionally enable **IPSec** and choose which version of the Internet Key Exchange (IKE) protocol to use: IKEv1 (`Version 1`) or IKEv2 (`Version 1`) depending on your configuration.

- For `Public Internet` connectivity, IPsec is always enabled.
- For `Cloud Backbone` connectivity, IPsec is always disabled.
- For `Private Connection`, you can choose to enable or disable IPsec.

If using **BGP-IPv4** connectivity instead, you must provide an external VRF which will be used for route leaking configuration from the cloud site you are configuring.

After **Site1** > **Site2** connectivity information is provided, the **Site2** > **Site1** area will reflect the connectivity information in the opposite direction.

e) Click **Save** to save the inter-site connectivity configuration.

When you save connectivity information from `Site1` to `Site2`, the reverse connectivity is automatically created from `Site2` to `Site1`, which you can see by selecting the other site and checking the **Inter-site Connectivity** information in the right sidebar.

f) Repeat this step to add inter-site connectivity for other sites.

When you establish underlay connectivity from `Site1` to `Site2`, the reverse connectivity is done automatically for you.

However, if you also want to establish inter-site connectivity from `Site1` to `Site3`, you must repeat this step for that site as well.

ステップ 7 Provide **External Connectivity** information.

If you do not plan to configure connectivity to external sites or devices that are not managed by NDO, you can skip this step.

Detailed description of an external connectivity use case is available in the *Configuring External Connectivity from Cloud CSRs Using Nexus Dashboard Orchestrator* document.

a) In the right **<*Site*> Settings** pane, select the **External Connectivity** tab.

b) Click **Add External Connection**.

The **Add External Connectivity** dialog will open.

c) From the **VRF** dropdown, select the VRF you want to use for external connectivity.

This is the VRF which will be used to leak the cloud routes. The **Regions** section will display the cloud regions that contain the CSRs to which this configuration be applied.

d) From the **Name** dropdown in the **External Devices** section, select the external device.

This is the external device you added in the **General Settings** > **External Devices** list during general infra configuration and must already be defined as described in インフラの設定: 一般設定, on page 146.

e) From the **Tunnel IKE Version** dropdown, pick the IKE version that will be used to establish the IPSec tunnel between the cloud site's CSRs and the external device.

f) (Optional) From the **Tunnel Subnet Pool** dropdown, choose one of the named subnet pools.

Named subnet pool are used to allocate IP addresses for IPSec tunnels between cloud site CSRs and external devices. If you do not provide any **named** subnet pools here, the **external** subnet pool will be used for IP allocation.

Providing a dedicated subnet pool for external device connectivity is useful for cases where a specific subnet is already being used to allocate IP addresses to the external router and you want to continue to use those subnets for IPSec tunnels for NDO and cloud sites.

If you want to provide a specific subnet pool for this connectivity, it must already be created as described in インフラの設定: 一般設定, on page 146.

g) (Optional) In the **Pre-Shared Key** field, provide the custom keys you want to use to establish the tunnel.

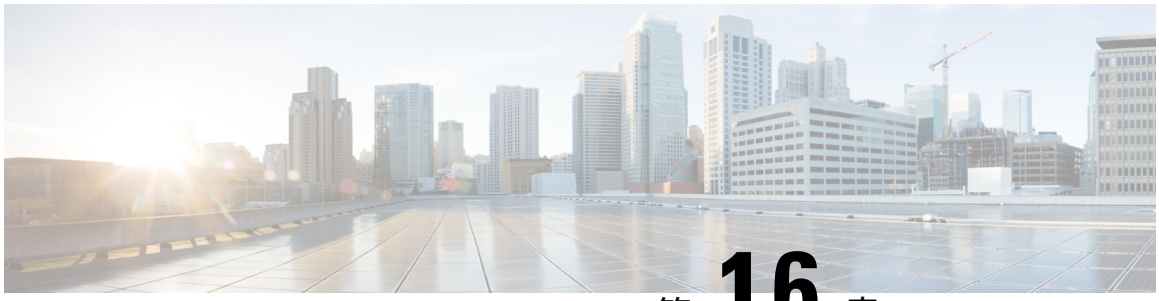
h) If necessary, repeat the previous substeps for any additional external devices you want to add for the same external connection (same VRF).

i) If necessary, repeat this step for any additional external connections (different VRFs).

Note that there's a one-to-one relationship for tunnel endpoints between CSRs and external devices, so while you can create additional external connectivity using different VRFs, you cannot create additional connectivity to the same external devices.

What to do next

While you have configured all the required inter-site connectivity information, it has not been pushed to the sites yet. You need to deploy the configuration as described in インフラ設定の展開, on page 163



第 16 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。

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 クラウド APIC 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):]** 両方のクラウド APIC 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 （151 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 サイトとクラウド APIC 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 APIC 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。

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 （163 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*>：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*>：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*> インターフェイスの IP アドレスです。
- <*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 APIC 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
```

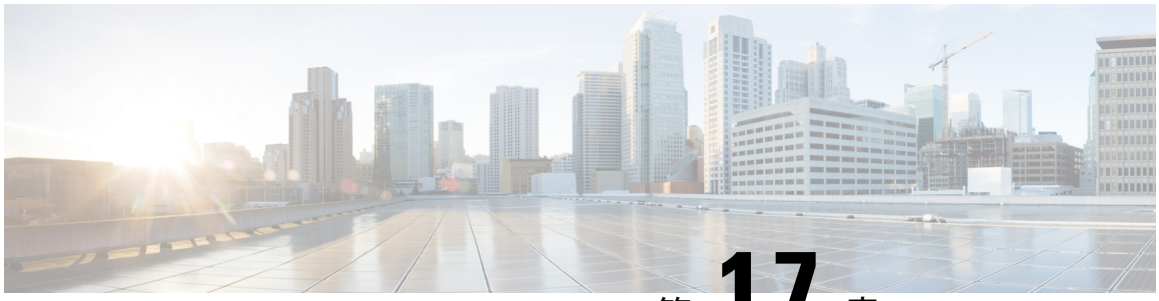
```
    set pfs group14
    set ikev2-profile ikev2-infra:overlay-1-2001
    set transform-set infra:overlay-1-2001
exit

! 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 17 章

CloudSec 暗号化

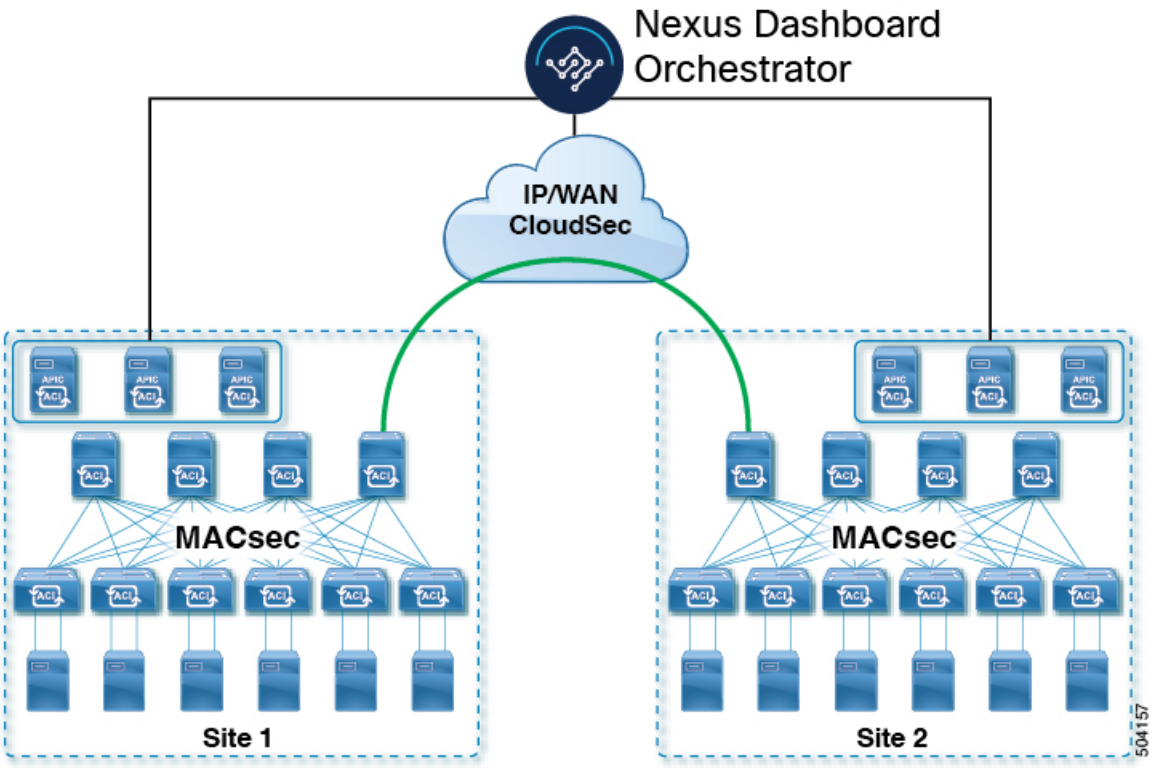
Cisco ACI CloudSec 暗号化

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 *16 : CloudSec* 暗号化



Requirements and Guidelines

When configuring CloudSec encryption, the following guidelines apply:

- CloudSec has been validated using a Nexus 9000 Inter-Site Network (ISN) infrastructure. If your ISN infrastructure is made up of different devices, or the devices are unknown (such as in the case of circuits purchased from a service provider), it is required that an ASR1K router is the first hop device directly connected to the ACI spine (with a separate pair of ASR1K devices deployed in each site), or the Nexus 9000 ISN network. The ASR1K router with padding-fixup enabled allows the CloudSec traffic to traverse any IP network between the sites.

  To configure an ASR1K router:

  1. Log in to the device.
  2. Configure the UDP ports.

     ```
     ASR1K(config)# platform cloudsec padding-fixup dst-udp-port 9999
     ```

  3. Verify the configuration.

     ```
     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
```

- If one or more spine switches are down when you attempt to disable CloudSec encryption, the disable process will not complete on those switches until the switches are up. This may result in packet drops on the switches when they come back up.

  We recommend you ensure that all spine switches in the fabric are up or completely decommissioned before enabling or disabling CloudSec encryption.

- The CloudSec Encryption feature is not supported with the following features:
  - Precision Time Protocol (PTP)
  - Remote Leaf Direct
  - Virtual Pod (vPOD)
  - SDA
  - Intersite L3Out, if the sites are running Cisco APIC releases prior to 5.2(4).

    CloudSec is supported with intersite L3Out for APIC sites running release 5.2(4) or later.
  - Other routable TEP configurations

Requirements

The CloudSec encryption capability requires the following:

- Cisco ACI spine-leaf architecture with a Cisco APIC cluster for each site
- Cisco Nexus Dashboard Orchestrator to manage each site
- One **Advantage** or **Premier** license per each device (leaf only) in the fabric
- An add-on license **ACI-SEC-XF** per device for encryption if the device is a fixed spine
- An add-on license **ACI-SEC-XM** per device for encryption if the device is a modular spine

The following table provides the hardware platforms and the port ranges that are capable of CloudSec encryption.

Hardware Platform	Port Range
N9K-C9364C spine switches	Ports 49-64
N9K-C9332C spine switches	Ports 25-32
N9K-X9736C-FX line cards	Ports 29-36

If CloudSec is enabled for a site, but the encryption is not supported by the ports, a fault is raised with `unsupported-interface` error message.

CloudSec encryption's packet encapsulation is supported if Cisco QSFP-to-SFP Adapters (QSA), such as CVR-QSFP-SFP10G, is used with a supported optic. The full list of supported optics is available from the following link: https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html.

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。

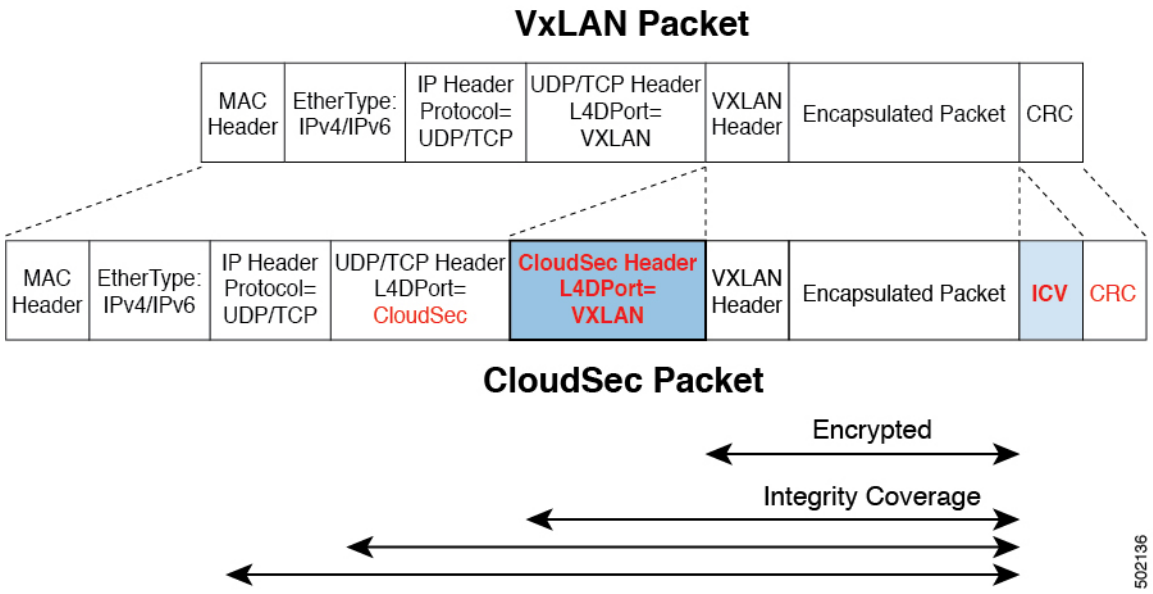
- 事前共有キー （PSK） – CloudSec TX および RX キーを生成するためのランダム シードとして使用するには、Cisco APIC GUI で 1 つ以上のキーを設定する必要があります。複数の PSK が設定される場合、各キーの再生成プロセスはインデックスの順序で次の PSK を使用します。さらに高いインデックスの PSK がない場合、最下位のインデックスの PSK が使用されます。各 PSK は、64文字の長さの16進数ストリングでなければなりません。Cisco APIC は最大256の事前共有キーをサポートします。

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 *17 : 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 ヘッダーとレイヤ 4 宛先ポート情報を使用してフィルタ処理され、一致する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。
- 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シスコ独自のレイヤ 4 ポート番号（ポート `9999`）で上書きされます。
- [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。

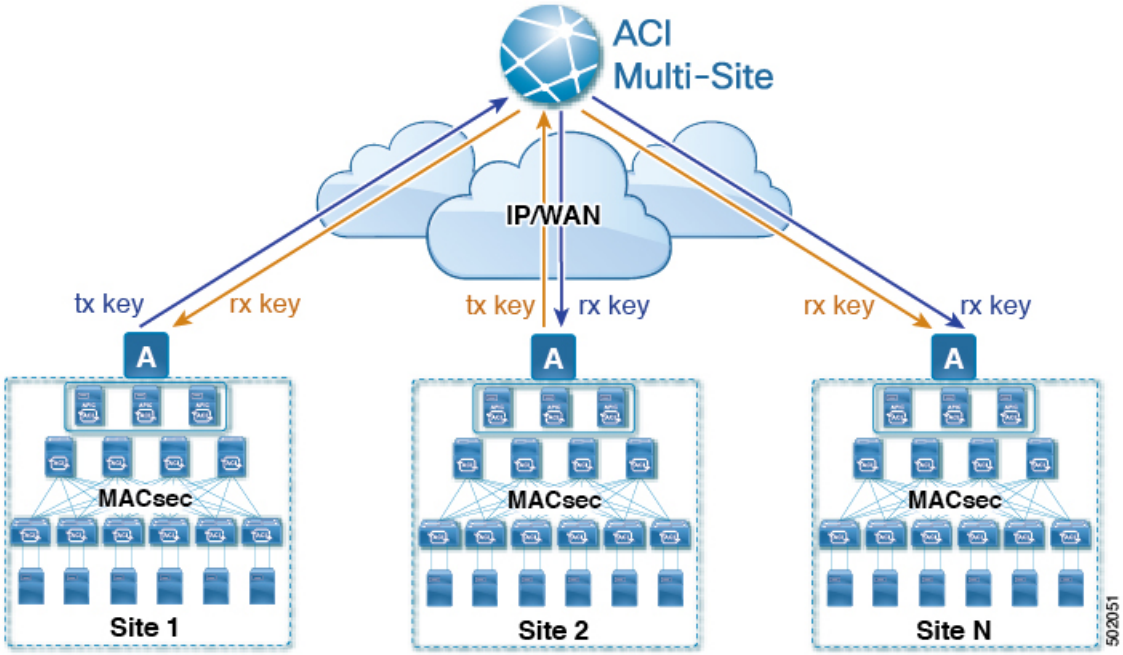
- 受信したパケットが CloudSec パケットである場合は、暗号解読され、ICV が検証されます。

  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。
- キー ストアが2つ以上の可能な暗号解読キーを返す場合、CloudSec ヘッダーの Association Number (AN) フィールドを使用して、使用するキーを選択します。
- 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 *18 : 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。

- 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 （182 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 （178 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 （179 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 （180 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。

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。

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。

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 GUI を使用した 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。

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 （182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 （182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、CiscoAPIC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。

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。

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>
```

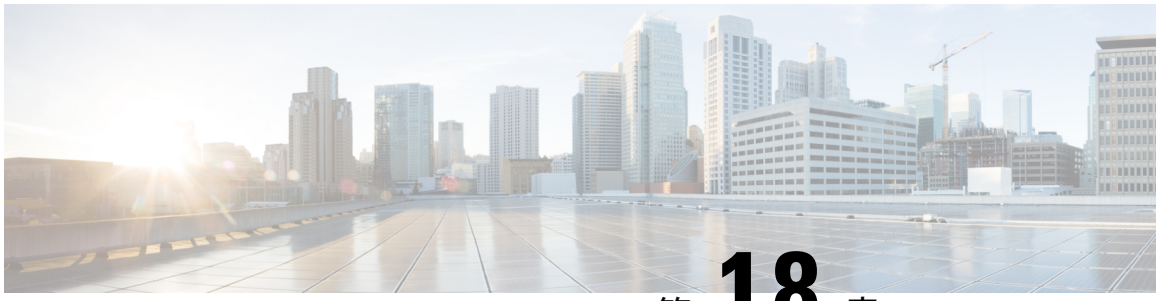
ステップ 2 キー再生成プロセスは、次のXML メッセージを使用して有効にすることができます。

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 18 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。

ガイドラインと制約事項

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 の背後にある DHCP リレー クライアント。

- 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。

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)]** > **[ポリシー (Policies)]** を選択します。

ステップ 3 メインペインの右上で**[ポリシー追加（Add Policy）]** > **[DHCP ポリシーの作成（Creating DHCP Policy）]** を選択します。

これは、**[DHCP の追加]** 設定画面を開きます。

ステップ 4 **[名前 (Name)]** フィールドにポリシーの名前を入力します。

ステップ 5 **[テナントの選択]** ドロップダウンから、DHCP サーバを含むテナントを選択します。

ステップ 6 (オプション) **[説明]** フィールドに、このポリシーの説明を入力します。

ステップ 7 **タイプ** に対して、リレー を選択します。

ステップ 8 **[+プロバイダ]** をクリックします。

ステップ 9 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—エンドポイントとして追加する DHCP サーバを含む特定のアプリケーション EPG を指定します。
- L3 外部ネットワーク—DHCP サーバー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。

ステップ 10 ドロップダウン メニューから、EPG または外部 EPG を選択します。

ステップ 11 **[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。

ステップ 12 **[保存 (Save)]** をクリックして、プロバイダを追加します。

ステップ 13 (オプション) 追加プロバイダがあれば、それを加えます。

追加のそれぞれの DHCP サーバに対して手順 9 ~ 12 を繰り返します。

ステップ 14 **[保存 (Save)]** をクリックして DHCP リレー ポリシーを保存します。

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 （189 ページ） の説明に従って作成された DHCP リレー ポリシー。

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)]** > **[ポリシー (Policies)]** を選択します。

ステップ 3 メイン ペインの右上で**[ポリシー追加 (Add Policy)]** > > **[DHCP ポリシーの作成 (Creating DHCP Policy)]** を選択します。

これは、**[DHCP の追加]** 設定画面を開きます。

ステップ 4 **[名前 (Name)]** フィールドにポリシーの名前を入力します。

これは、作成しているポリシーの名前であり、特定の DHCP オプションの名前ではありません。各ポリシーには、複数の DHCP オプションが含まれる場合があります。

ステップ 5 **[テナントの選択]** ドロップダウンから、DHCP サーバを含むテナントを選択します。

ステップ 6 (オプション) **[説明]** フィールドに、このポリシーの説明を入力します。

ステップ 7 **[タイプ]** に対して [オプション] を選択します。

ステップ 8 **[+オプション (+Options)]** をクリックします。

ステップ 9 オプションの名前を指定します。

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。

ステップ 10 オプションの ID を指定します。

RFC 2132 にリストされているとおり、オプション コードを提供する必要があります。

たとえば、ネーム サーバ オプションに対して 5 が挙げられます。

ステップ 11 オプションのデータを指定します。

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。

ステップ 12 **[データ]** フィールドの隣のチェックマークをクリックして、オプションを保存します。

ステップ 13 (オプション) 追加オプションを加えるための手順を繰り返します。

ステップ 14 **[保存 (Save)]** をクリックして DHCP オプション ポリシーを保存します。

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 （189 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 （190 ページ） の説明に従って、DHCP オプション ポリシー。
- Creating Schemas and Templates （24 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。

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 （190 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 （189 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 （190 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 （191 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。

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。

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

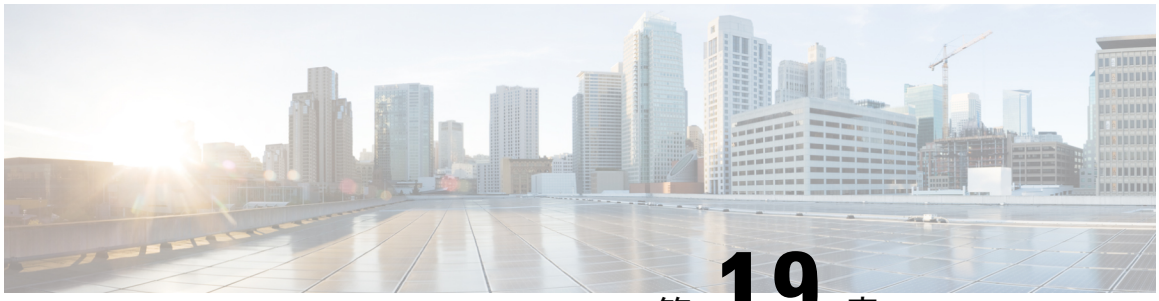
このセクションでは、DHCP リレーまたはオプション ポリシーを編集または削除する方法について説明します。

（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。

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 19 章

EPG 優先グループ

EPG 優先グループ

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。

一方、Nexus Dashboard Orchestrator 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

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。

優先グループに対する EPG の設定

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。

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、**[スキーマ (schema)]** 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 優先グループの一部として、スキーマで 1 つ以上の EPG を設定します。

（注） 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。一部の EPG が Nexus Dashboard Orchestrator によって管理され、一部がローカル APIC によって管理される優先グループを設定することはできません。

単一の EPG を追加または削除するには:

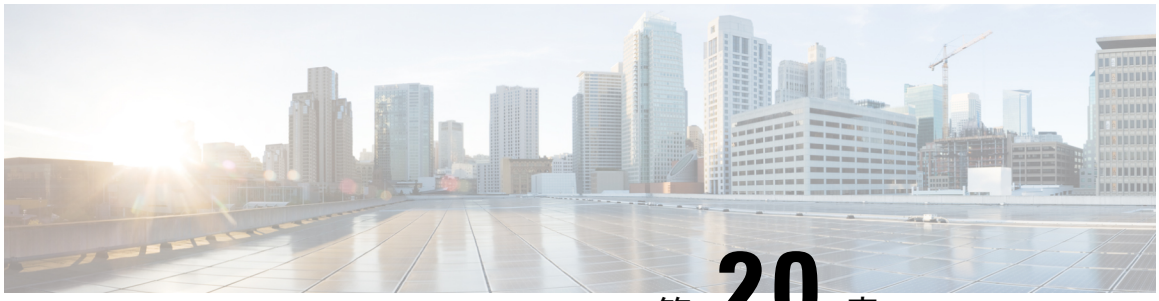
a) EPGを選択します。
b) 右側のプロパティ バーで、**[優先グループに含める]** チェックボックスをオンまたはオフにします。
c) メイン ウィンドウの右上の隅にある **[保存]** をクリックします。

複数の EPG を一度に追加または削除するには:

a) **[アプリケーション プロファイル]** タブの右上隅の **SELECT** をクリックします。
b) 1 つまたは複数のEPGをクリックして選択するか、**[すべて選択]**をクリックしてすべてのEPGを選択します。
c) **[アプリケーション プロファイル (Application Profile)]** タブの右上隅の **...** をクリックして、**[優先グループへの EPG の追加]** または **[優先グループからの EPG の削除]** を選択します。
d) メイン ウィンドウの右上の隅にある **[保存]** をクリックします。

次のタスク

VRF を選択し、右側のプロパティサイドバーで **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 20 章

サイト内 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。
- You can now associate a bridge domain in one site with the L3Out in another site, however they must both be in the same VRF.

  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。

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。

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`。

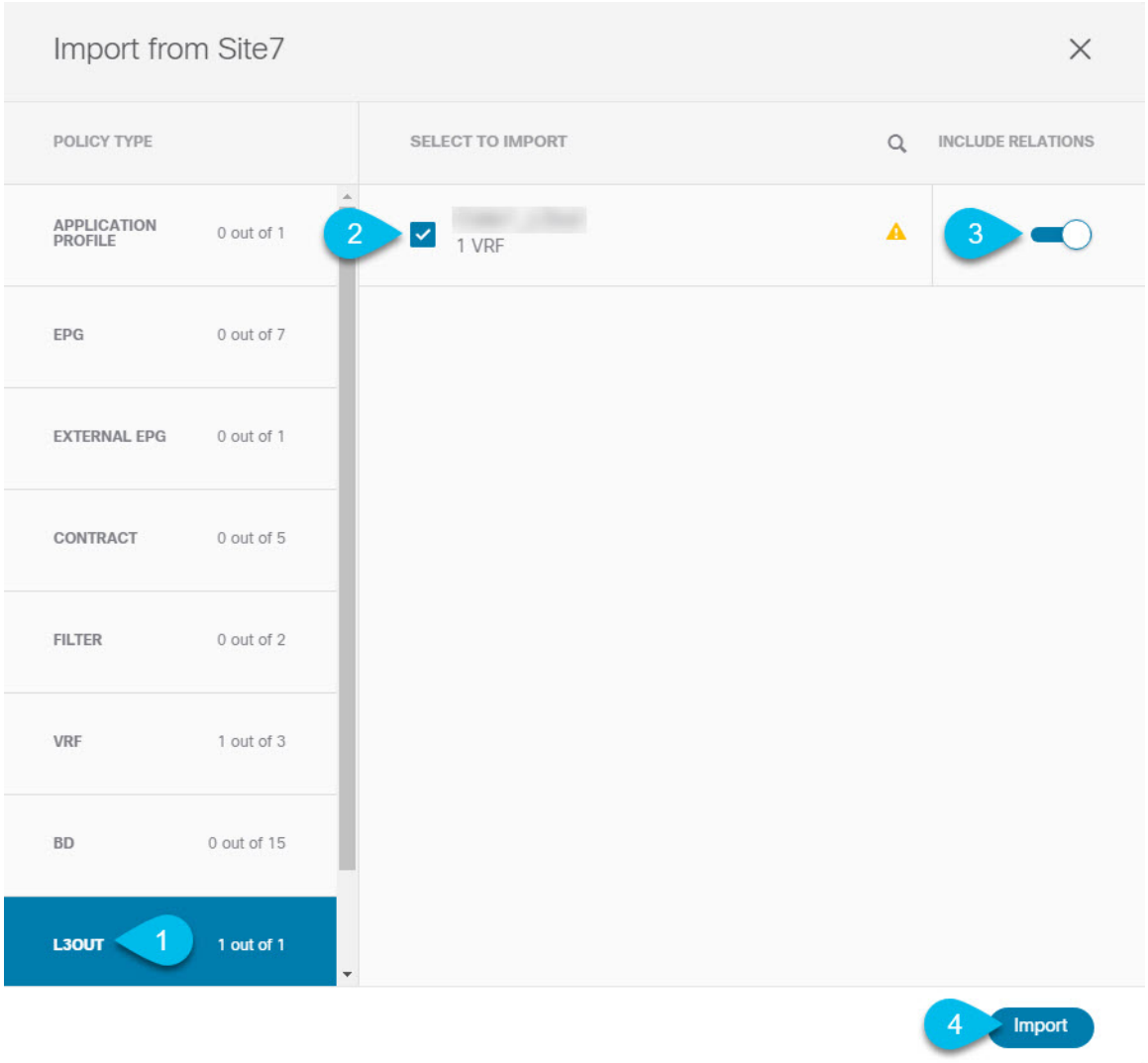
d) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、VRF を選択します。

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 （204ページ）に説明されている方法で VRF と関連付けます。

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。

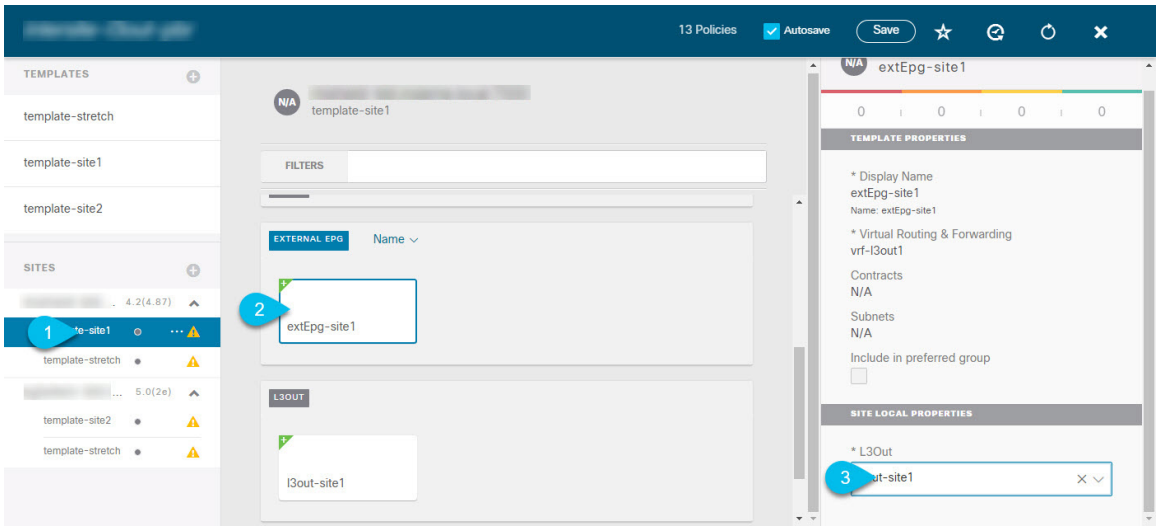
右側のスライダで、必要な情報を入力します。

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。

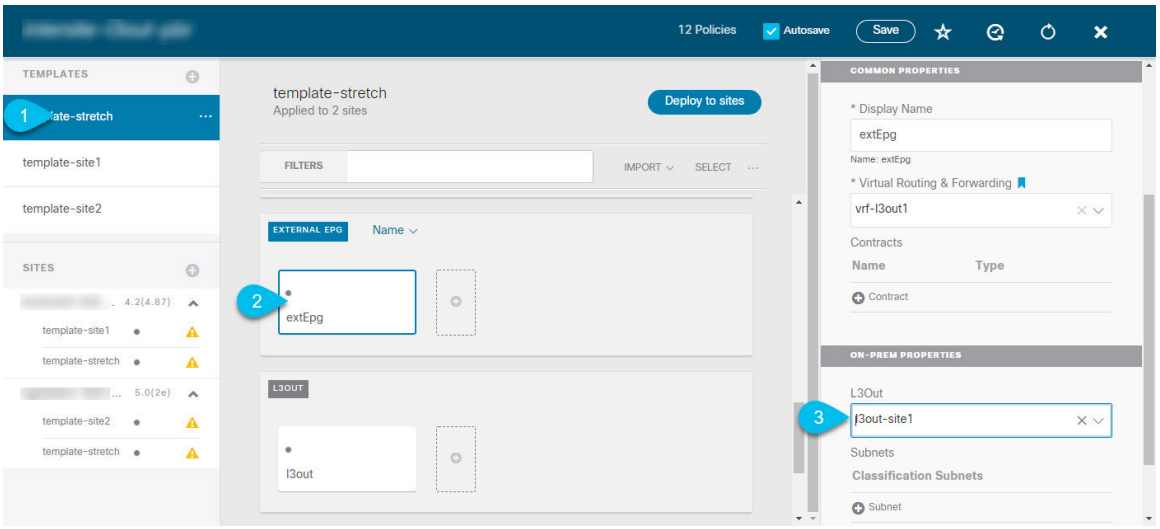
b) **[外部 EPG (External EPG)]** エリアまで下方にスクロールして、外部 EPG を選択します。

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

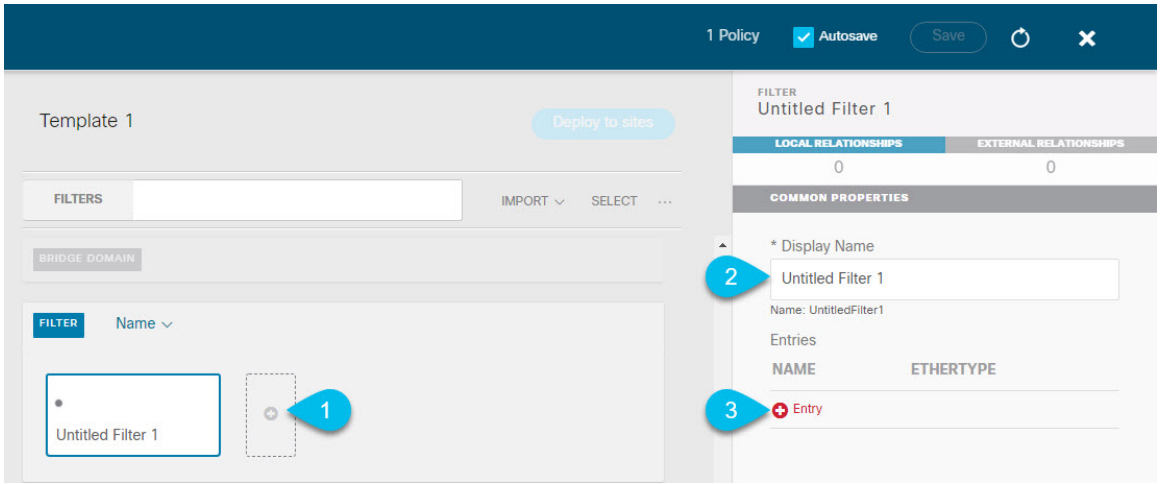
ここでは、サイトに展開されたアプリケーション EPG と、別のサイトの L3Out に関連付けられた外部 EPG（サイト間 L3Out 機能）との間の通信を可能にするために使用するフィルタとコントラクトを作成する方法について説明します。

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。

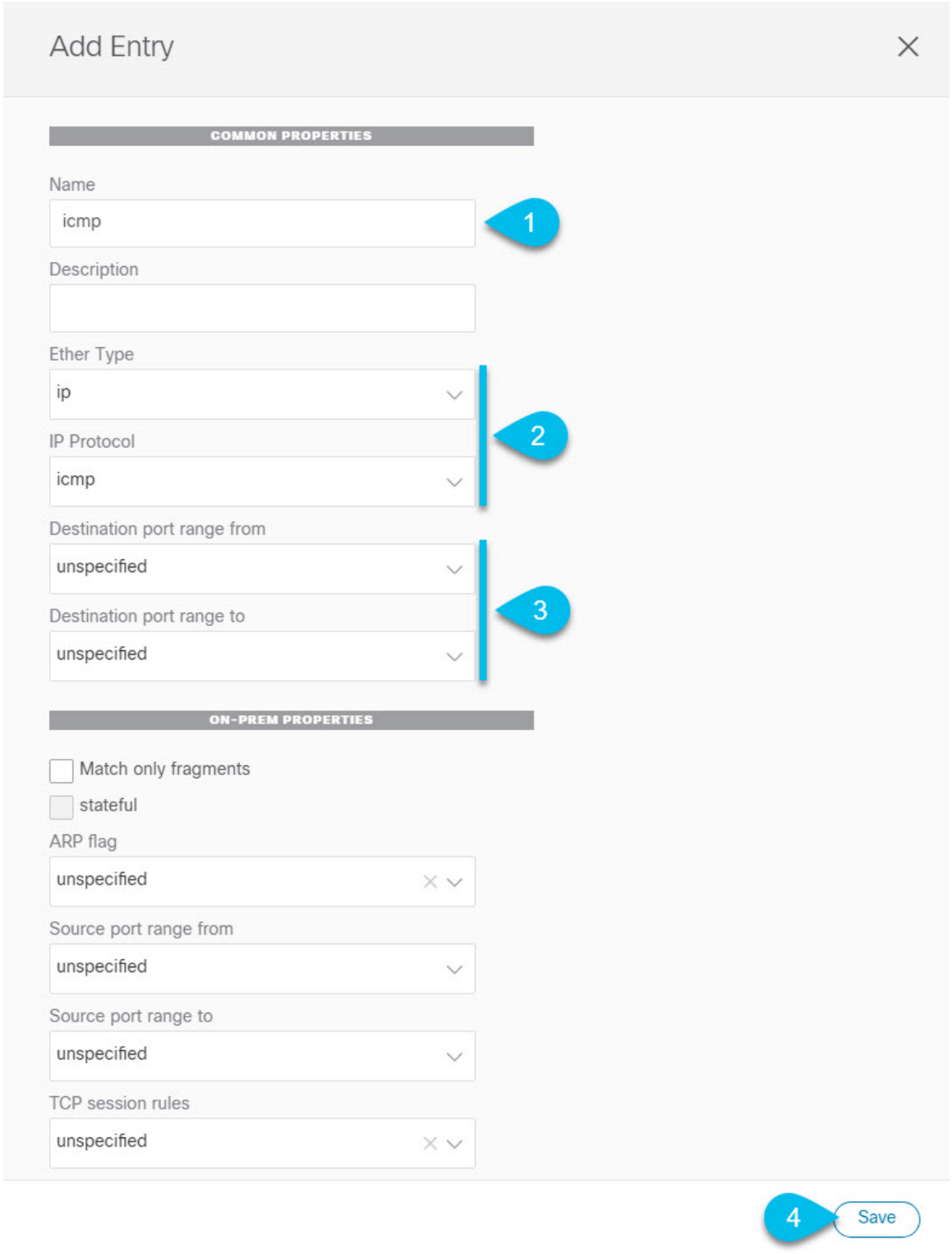
コントラクトは異なるサイトに展開されたオブジェクト（EPG および外部 EPG）に適用されるため、複数のサイトに関連付けられたテンプレートで定義することを推奨します。ただし、これは必須ではありません。コントラクトとフィルタが Site1 のローカル オブジェクトとしてのみ定義されている場合でも、 Site2 のローカル EPG または外部 EPG がそのコントラクトを消費または提供する必要がある場合、NDO はリモート Site2 に対応するシャドウ オブジェクトを作成します。 。

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。

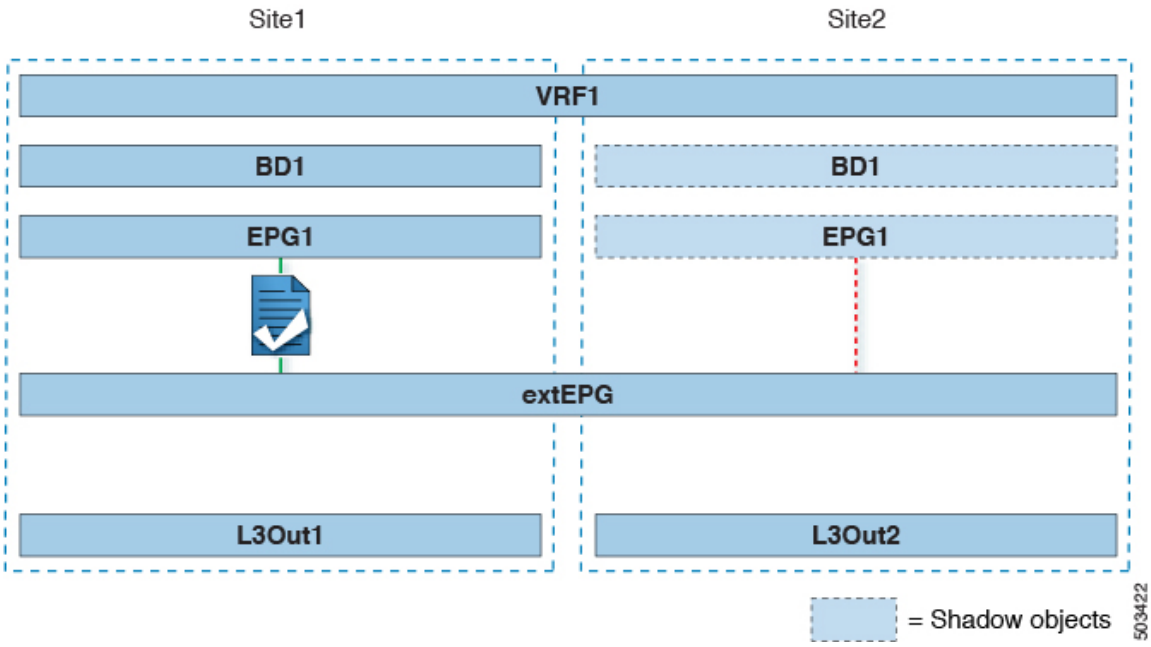
使用例

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。

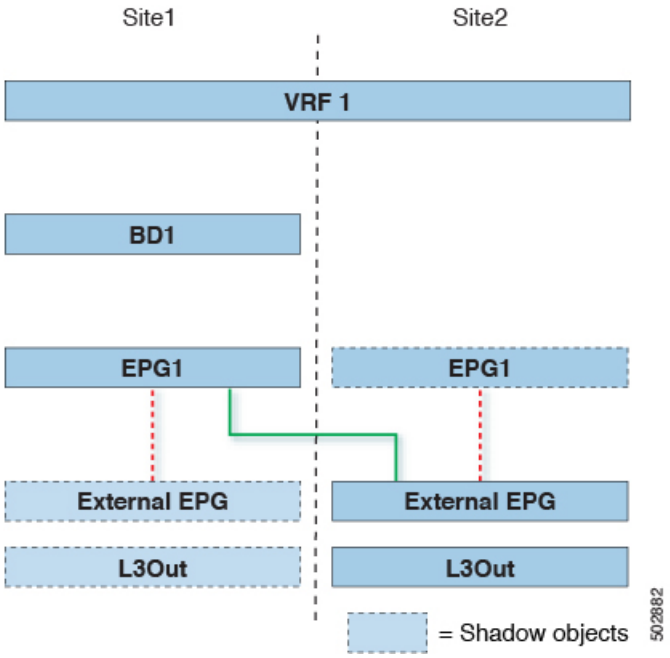
最初の図は、拡大された外部 EPG と、両方のサイトで作成される関連づけられた L3Out を示しています。アプリケーション EPG (EPG1) はサイト 1 で作成され、外部 EPG とのコントラクトがあります。この使用例は、別のサイトの L3Out が外部リソースの共通セットへのアクセスを提供する場合に推奨されます。ポリシー定義と外部トラフィック分類が簡素化され、独立した APIC ドメインの各 L3Out に個別にルートマップポリシーを適用できます。

図 *19*：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 *20* : 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 （204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 （207 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 （210 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。

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。

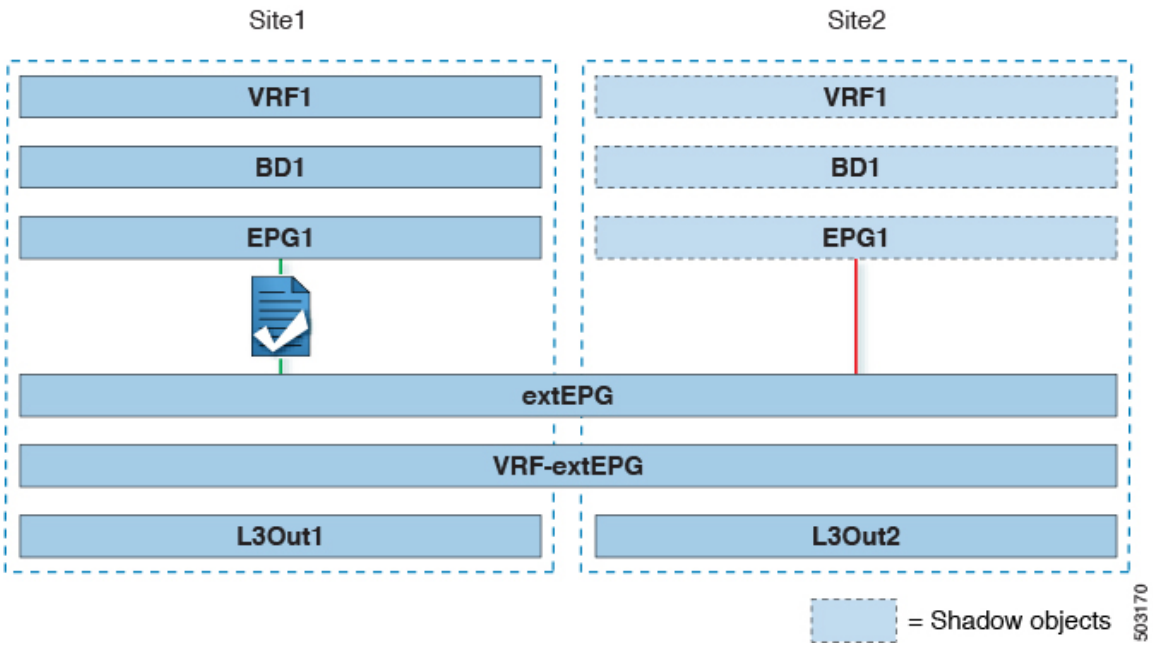
ステップ 8 スキーマを展開します。

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 *21* : 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。



The following steps describe the configuration required to implement the use case shown in Figure 3.

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 （204 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 （207 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 （210 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。

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。

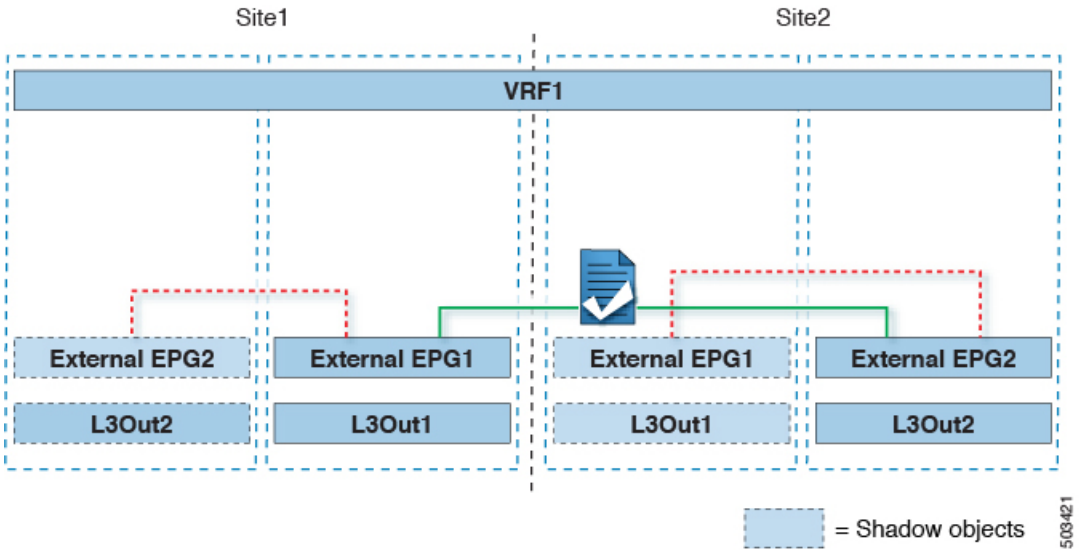
サイト間中継ルーティング

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

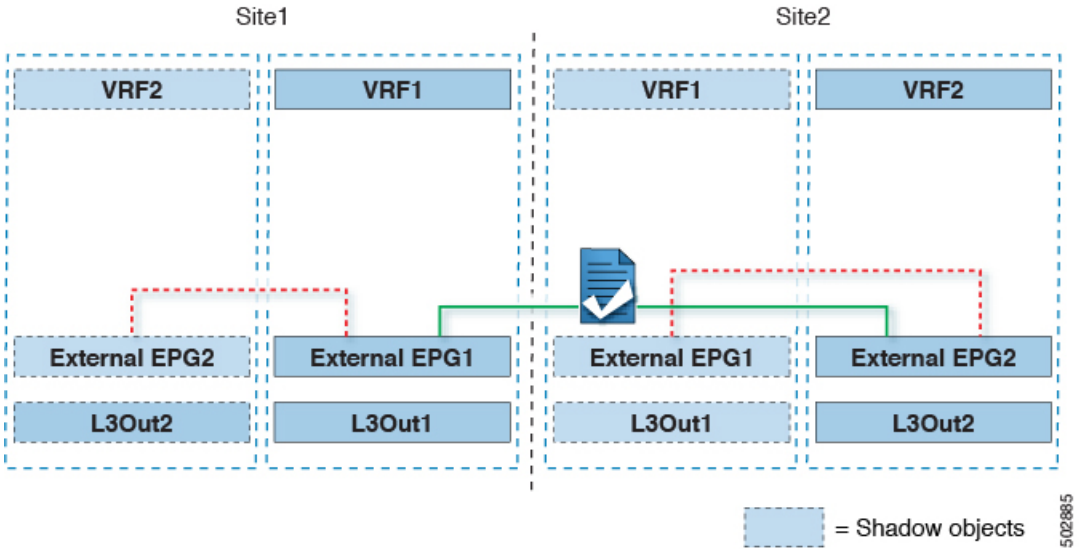
EPG 間のコントラクトにより、2 つの異なるサイトの 2 つの異なる L3Outs の背後にあるエンドポイント間の通信が可能になります。

図 *22 : 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 *23 : 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 （204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 （207 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（210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。

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。

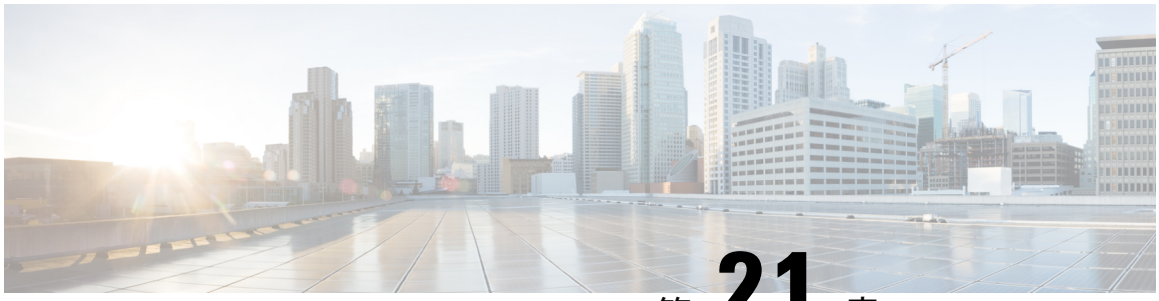
コンシューマまたはプロバイダを選択します。

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 21 章

PBR を使用したサイト間 L3Out

Intersite L3Out with PBR

Cisco Application Centric Infrastructure (ACI) policy-based redirect (PBR) enables traffic redirection for service appliances, such as firewalls or load balancers, and intrusion prevention system (IPS). Typical use cases include provisioning service appliances that can be pooled, tailored to application profiles, scaled easily, and have reduced exposure to service outages. PBR simplifies the insertion of service appliances by using contract between the consumer and provider endpoint groups even if they are all in the same virtual routing and forwarding (VRF) instance.

PBR deployment consists of configuring a route redirect policy and a cluster redirect policy, and creating a service graph template that uses these policies. After the service graph template is deployed, you can attach it to a contract between EPGs so that all traffic following that contract is redirected to the service graph devices based on the PBR policies you have created. Effectively, this allows you to choose which type of traffic between the same two EPGs is redirected to the L4-L7 device, and which is allowed directly.

More in-depth information specific to services graphs and PBR is available in the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*

PBR Support in Multi-Site Deployments

Cisco Multi-Site has supported EPG-to-EPG (east-west) and L3Out-to-EPG (north-south) contracts with PBR since Cisco APIC, Release 3.2(1). However, the L3Out-to-EPG across sites (traffic from an external endpoint in `site1` to an endpoint in `site2`) case was supported only if both sites had local L3Outs. The intersite L3Out use cases were limited to the examples and configurations described in the サイト内

L3Out, on page 201 chapter. Similarly, the Service Graph integration with PBR but no intersite L3Out is described in great detail in the *Cisco Multi-Site and Service Node Integration White Paper*.

Starting with Cisco APIC, Release 4.2(5), the L3Out-to-EPG with PBR across sites (intersite L3Out) use case has been extended to support cases where the application EPG has no local L3Out or the local L3Out is down.

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 （230 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 （234 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 （235 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 （237 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 （244 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 （246 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 （207 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 *24 :* インバウンド トラフィック

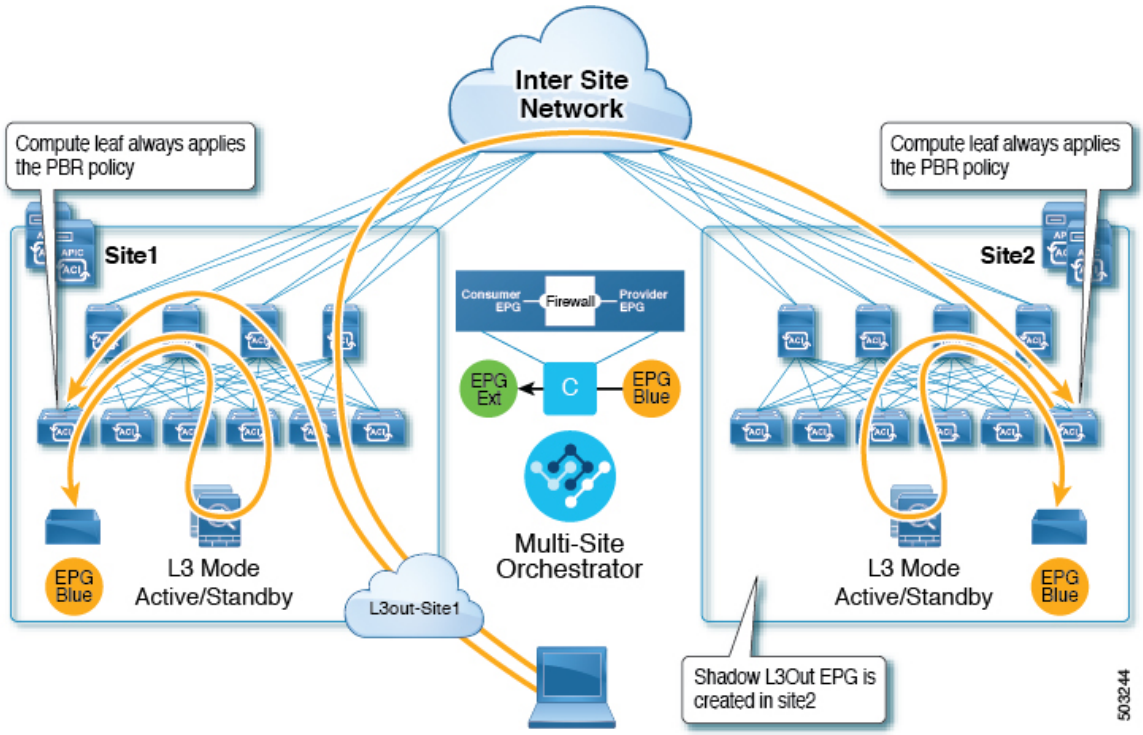
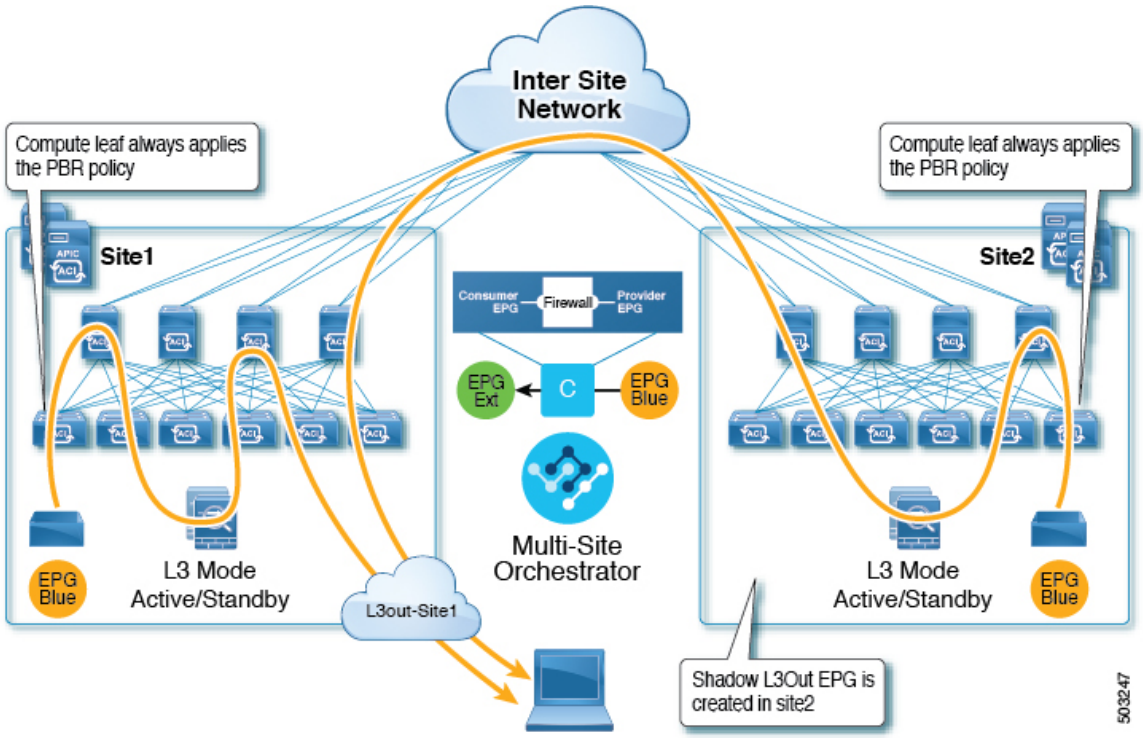


図 *25 :* アウトバウンド トラフィック



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 *26* : インバウンド トラフィック

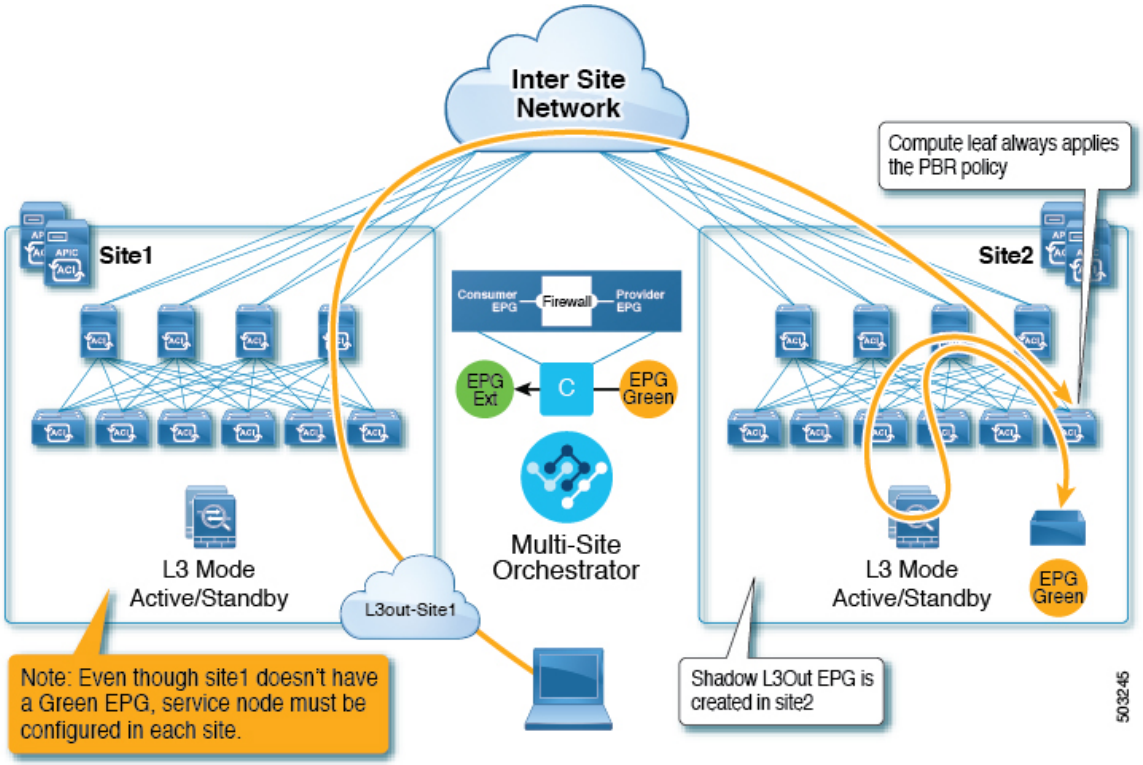
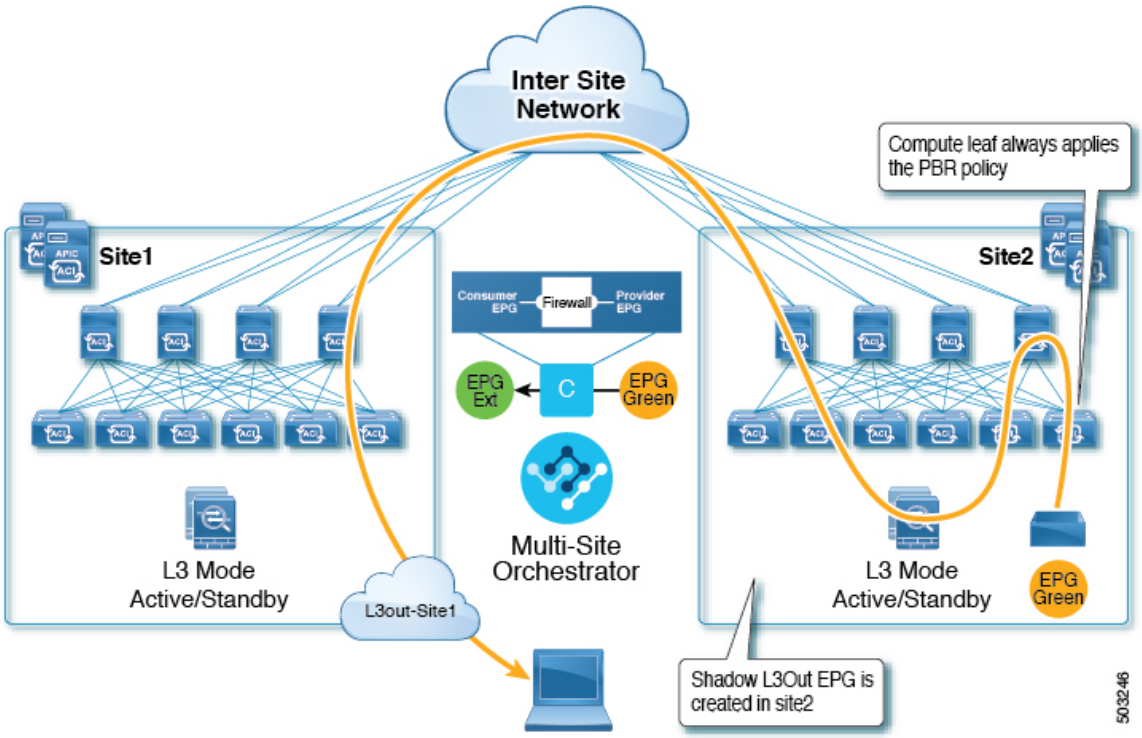


図 *27:* アウトバウンド トラフィック



ガイドラインと制約事項

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。

- PBR を使用しないサイト間 L3Out の使用例については、サイト内 L3Out （201 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。

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。

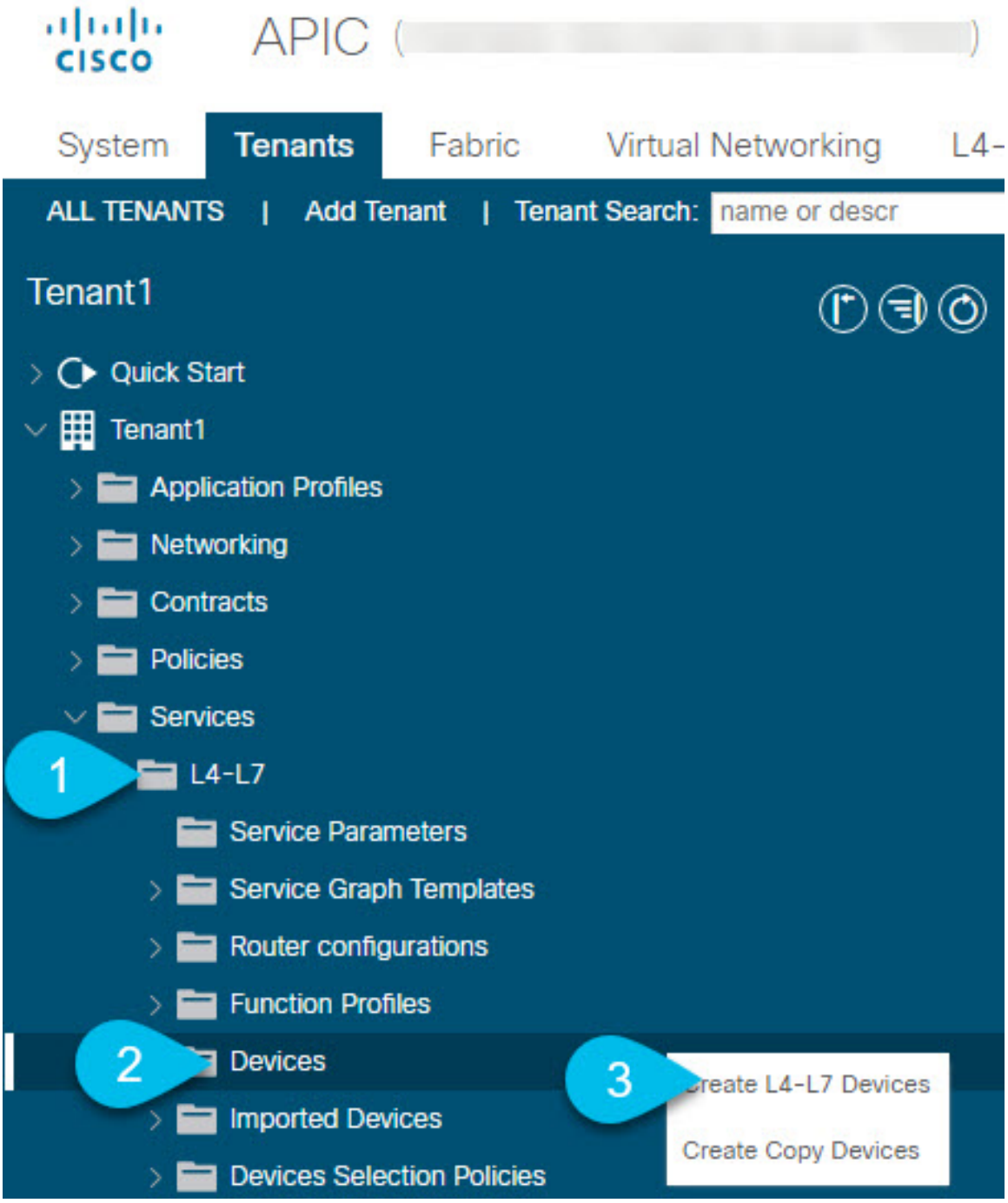
L4-L7 デバイスおよび PBR ポリシーの作成と設定

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。

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。

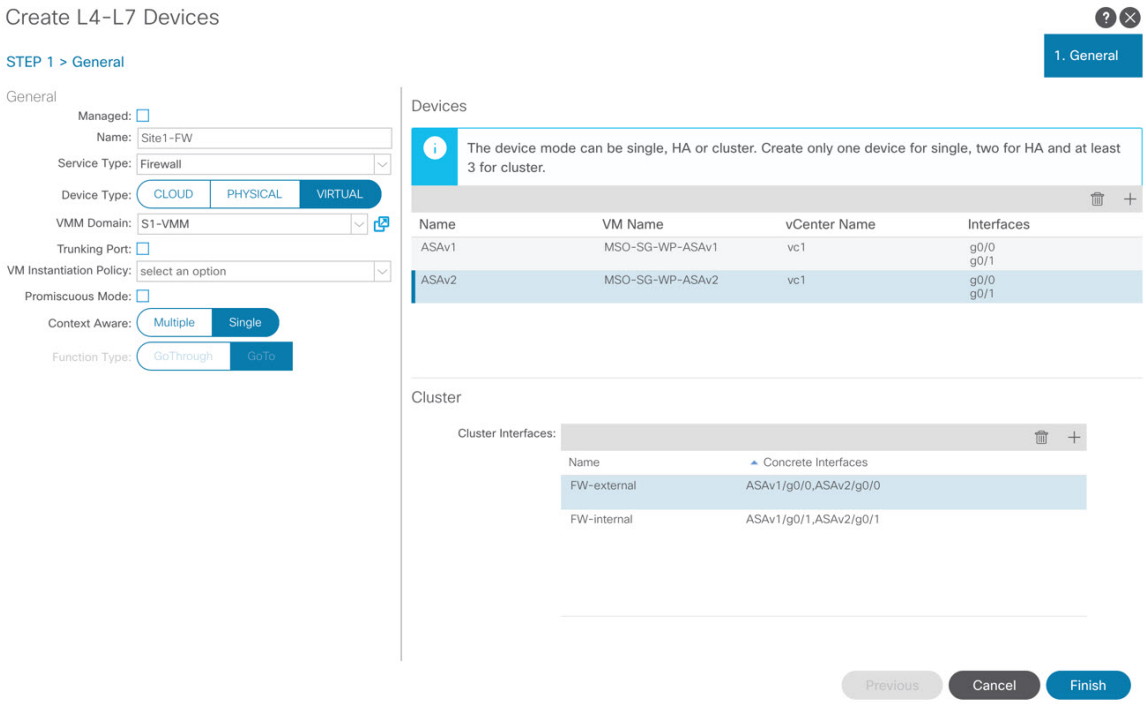


a) 左側のサイドバーで、**<tenant-name>** > **[サービス (Services)]** > **[L4-L7]** カテゴリを展開します。
b) **[デバイス (Devices)]** カテゴリを右クリックします。
c) **[L4-L7 デバイスの作成 (Create L4-L7 Devices)]** を選択します。

[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。

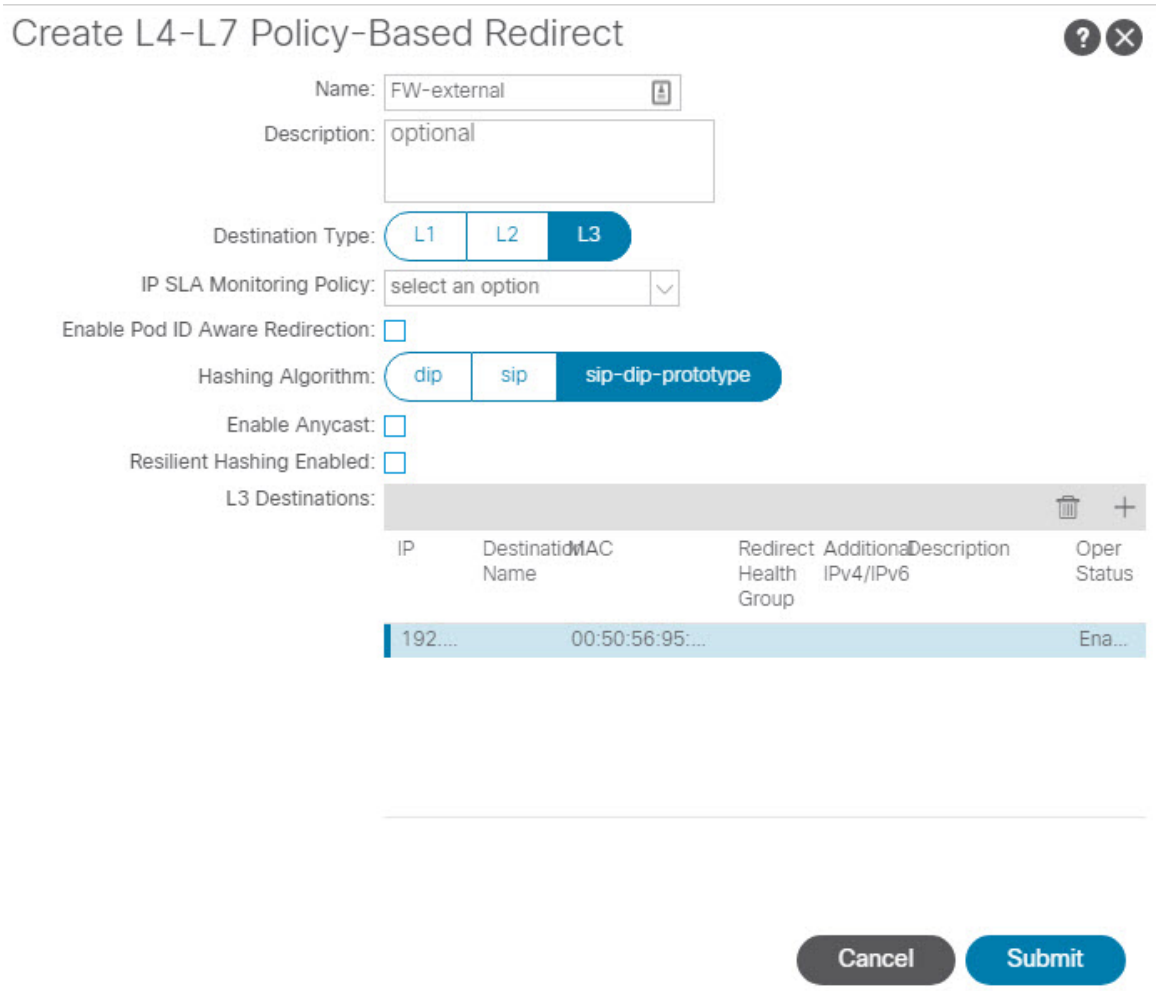
a) 左側のサイドバーで、**<tenant-name>** > **[ポリシー(Policies)]** > **[プロトコル (Protocol)]** カテゴリを展開します。
b) **[L4-L7 ポリシーベース リダイレクト (L4-L7 Policy-Based Redirect)]** カテゴリを右クリックします。
c) **[L4-L7 ポリシーベース リダイレクトの作成 (Create L4-L7 Policy-Based Redirect)]** を選択します。

[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。

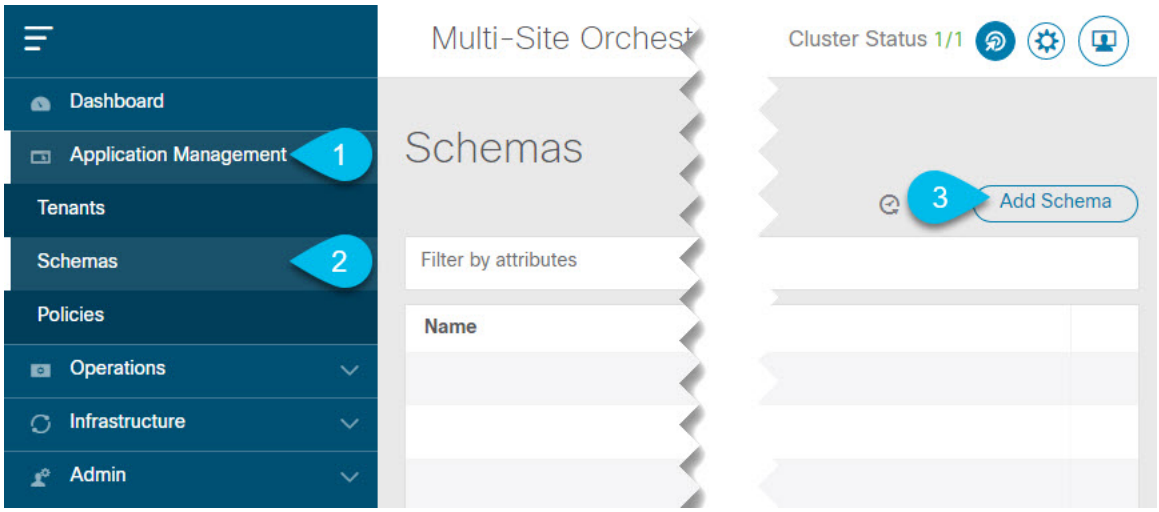
始める前に

次のものが必要です。

- ガイドラインと制約事項 （228 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 （204 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 （230 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。

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。



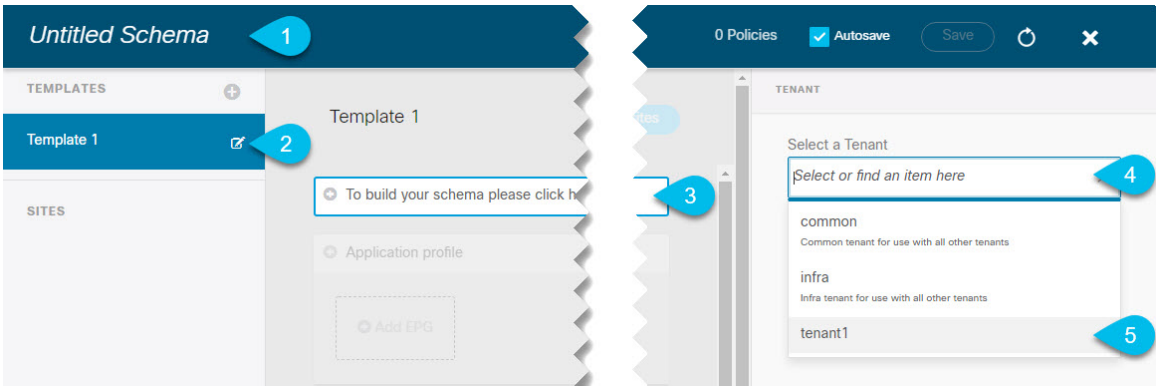
a) 左側のナビゲーションサイドバーで、**[アプリケーション管理 (Application Management)]** カテゴリを展開します。

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。

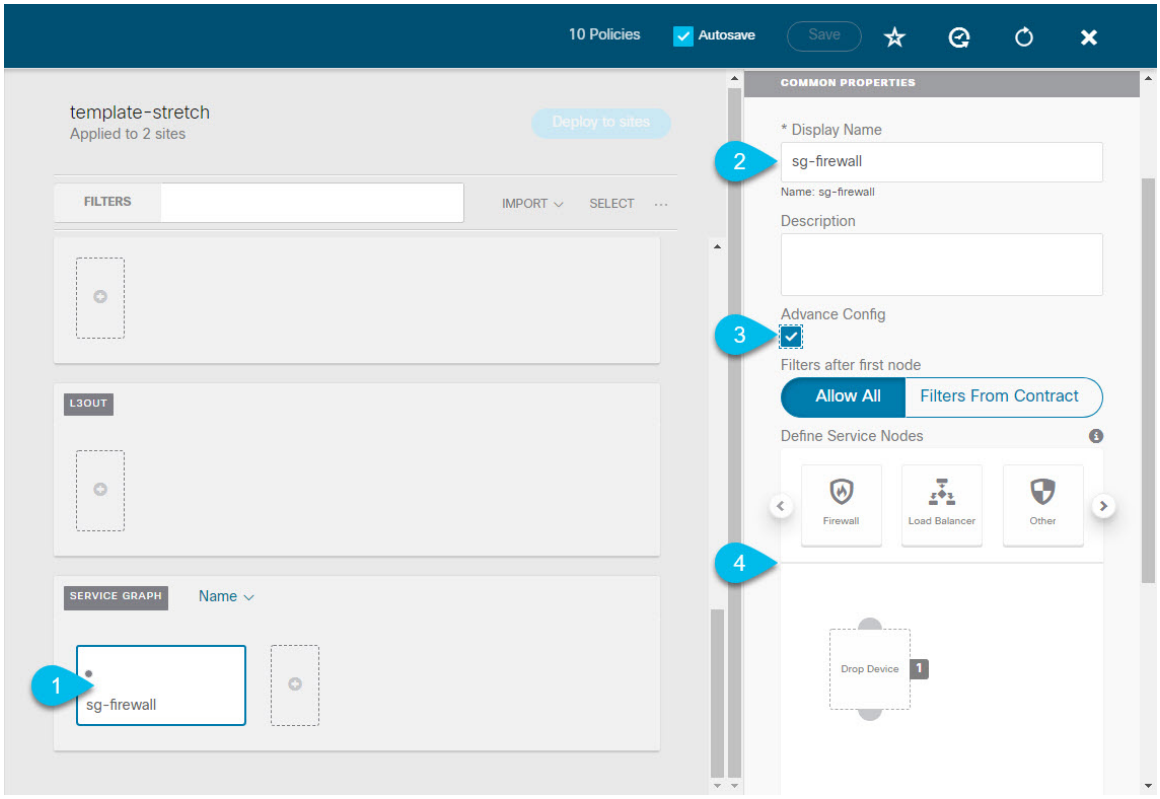
- L4-L7 デバイスおよび PBR ポリシーの作成と設定 （230 ページ）の説明に従い、サイトの APIC ごとに直接作成された L4-L7 デバイス。
- テンプレートの作成 （234 ページ）の説明に従って作成された、これらのオブジェクトを作成するためのテンプレート。

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。

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。

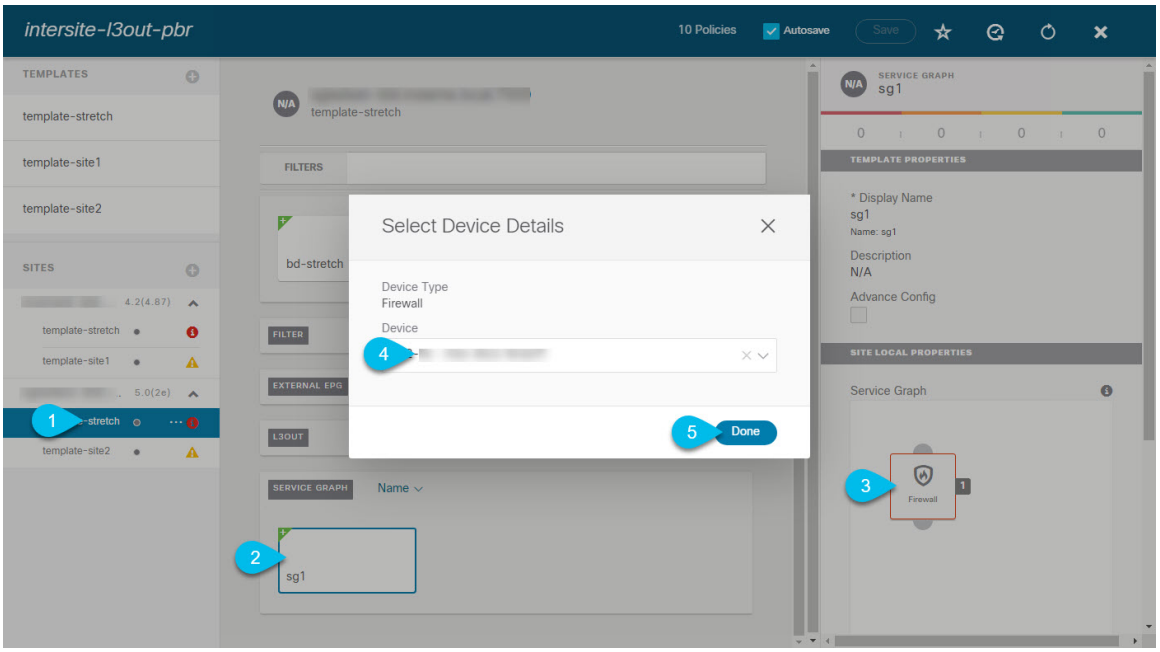
- **[契約からのフィルタ (Filters From Contract)]**：コントラクトの件名から特定のフィルタを使用します。

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。

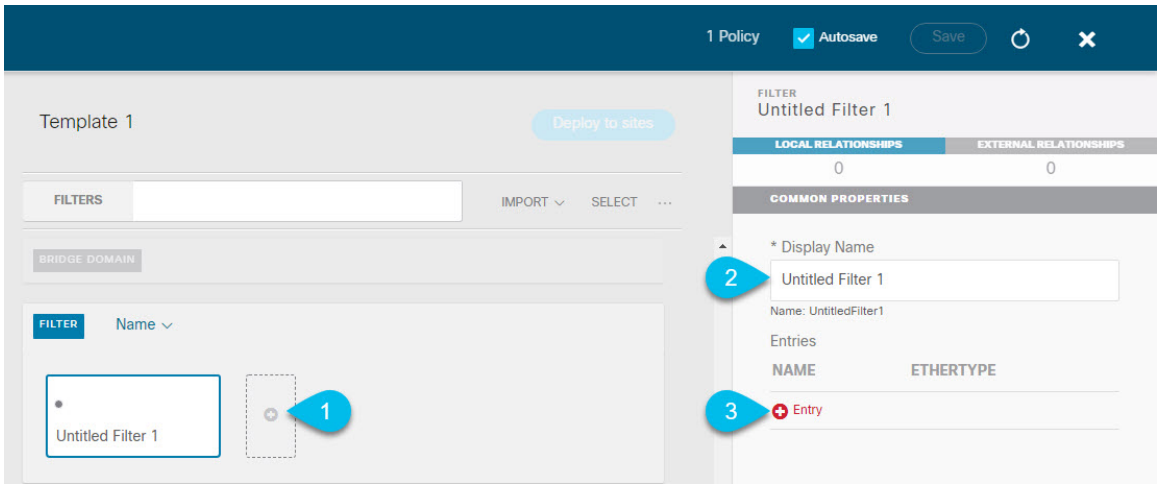
コントラクトのフィルタの作成

次のものが必要です。

- テンプレートの作成 （234 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。

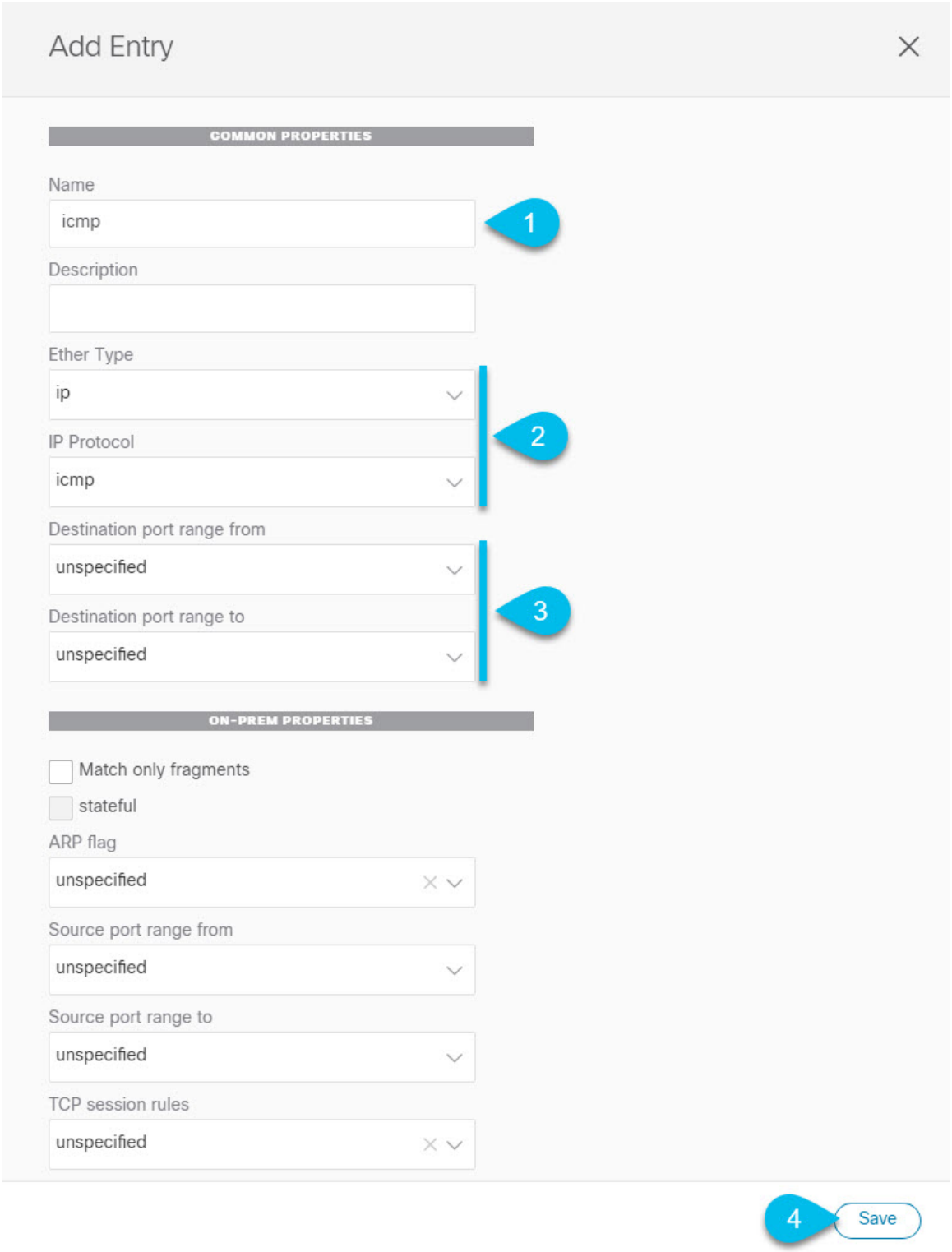
このセクションでは、サービスグラフを介してアプリケーションEPGとL3Out間のトラフィックに使用されるコントラクトとフィルタの作成方法について説明します。

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。

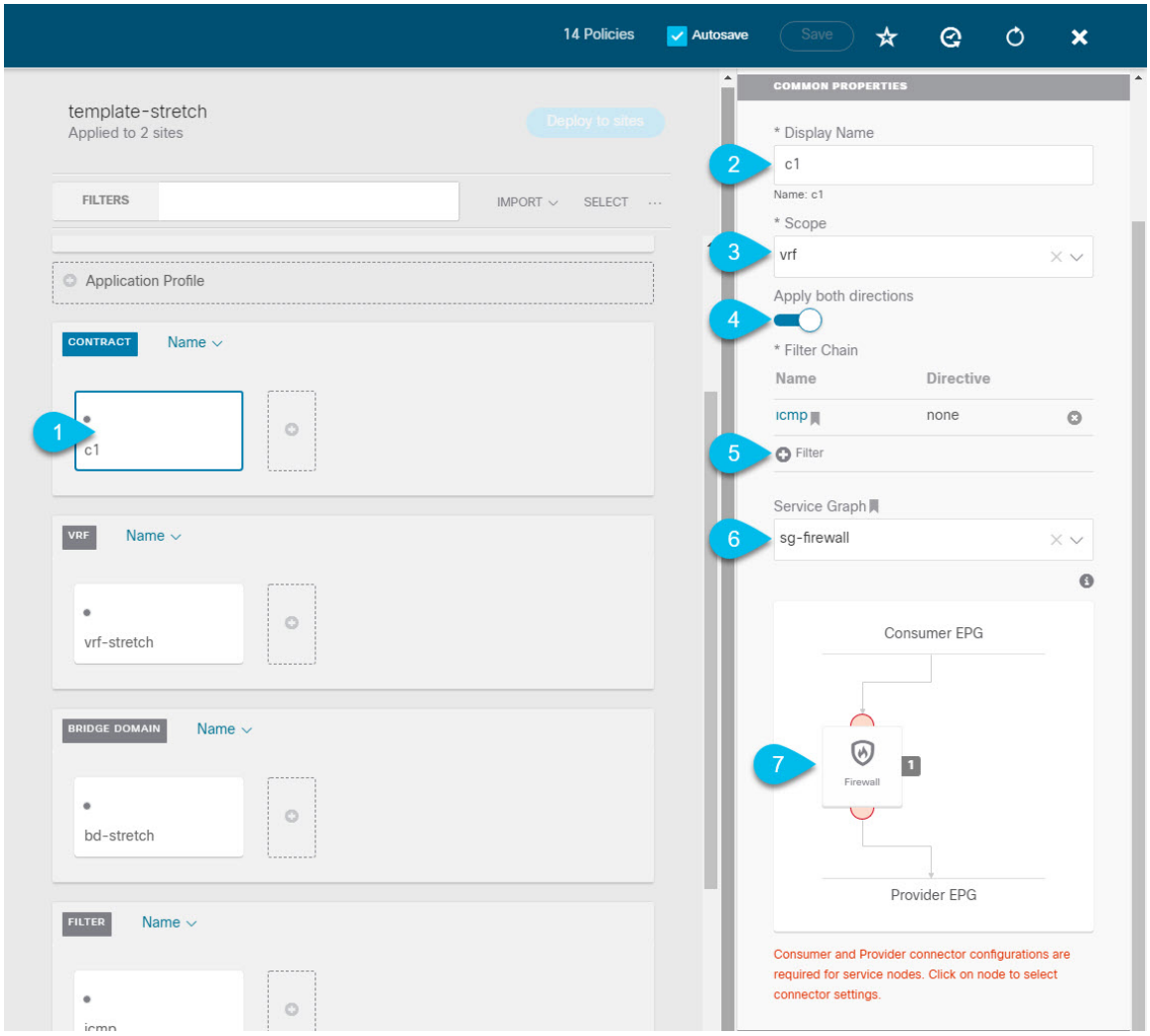
b) **[イーサー タイプ (Ether Type)]** と **[IP プロトコル (IP Protocol)]** を選択します。

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。

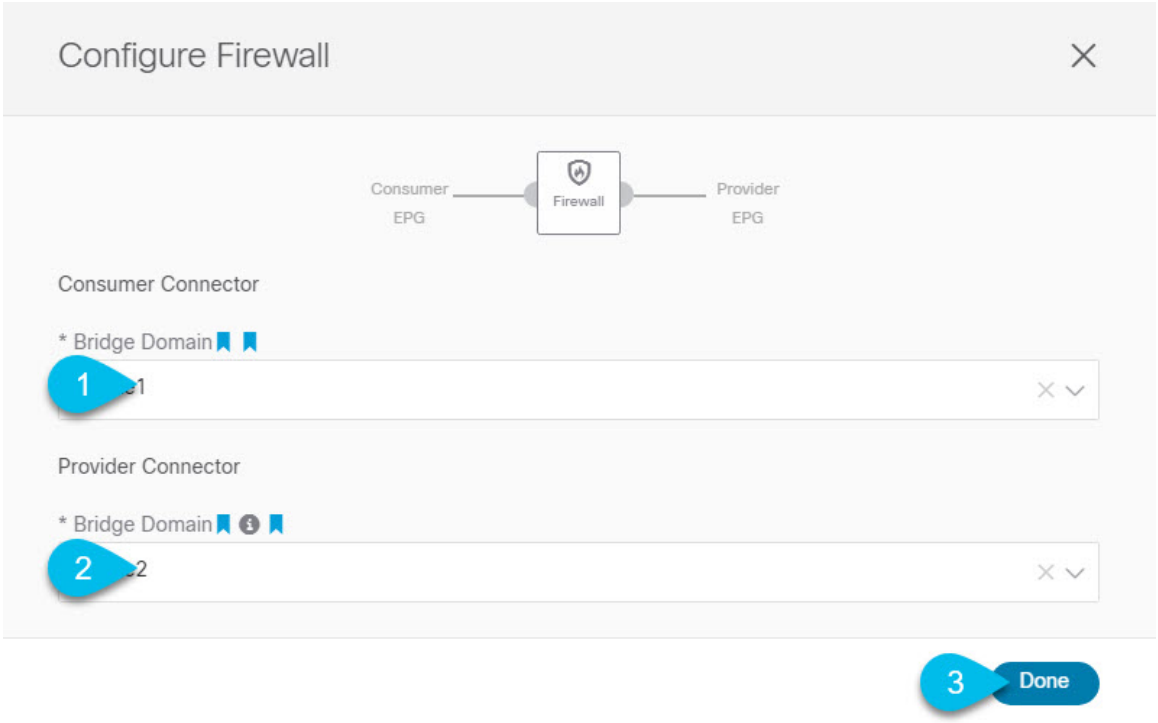
表示される **[フィルタ チェーンの追加 (Add Filter Chain)]** ウィンドウで、**[名前 (Name)]** ドロップダウン メニューから前のセクションで追加したフィルタを選択します。

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。

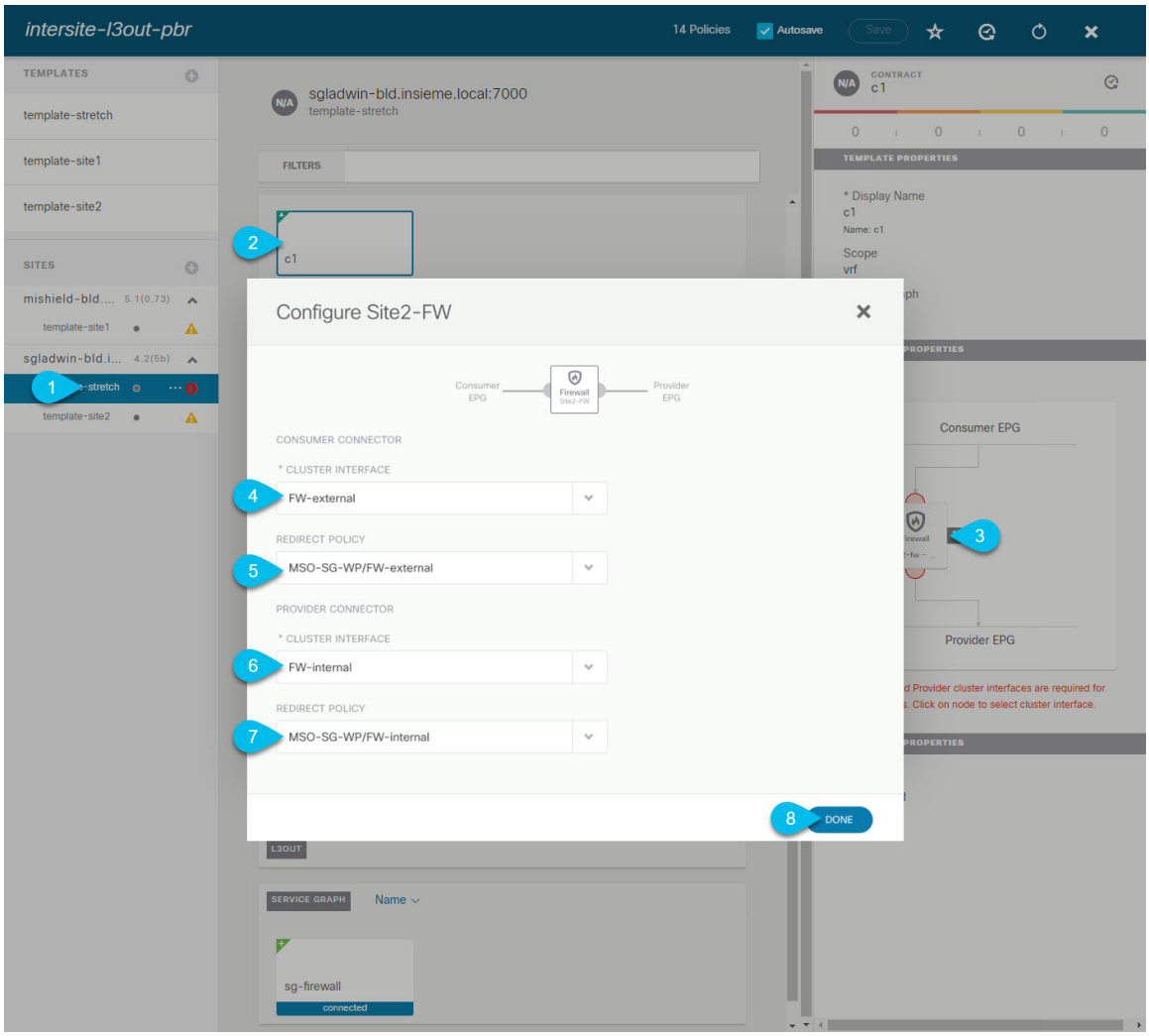


a) **[コンシューマ コネクタ (Consumer Connector)]** ブリッジ ドメインを指定します。

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

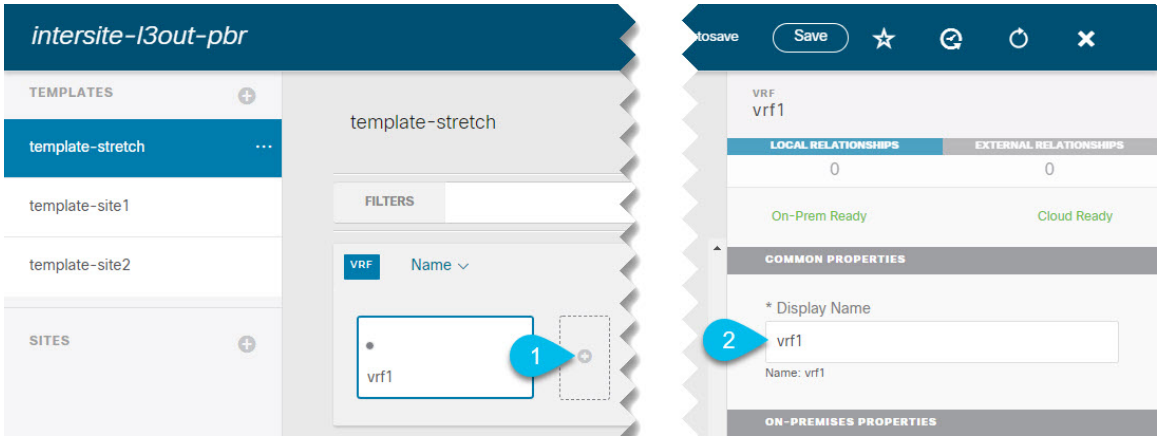
次のものが必要です。

- テンプレートの作成 （234 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。

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。

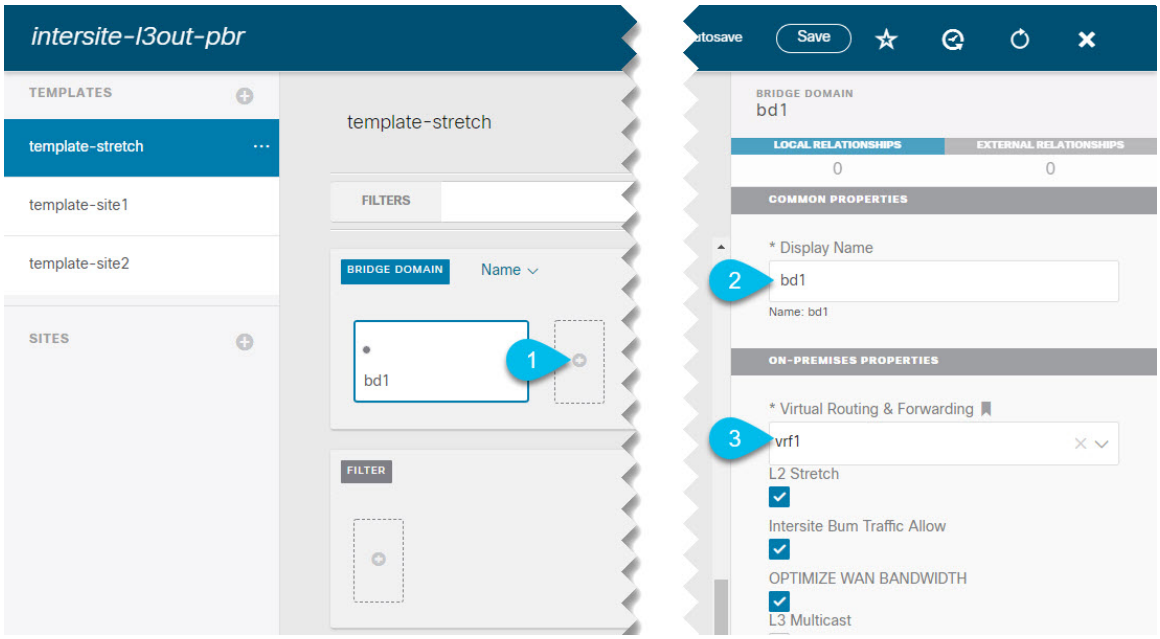


a) メイン ペインの **[VRF]** 領域で、プラス (+) 記号をクリックして VRF を追加します。

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

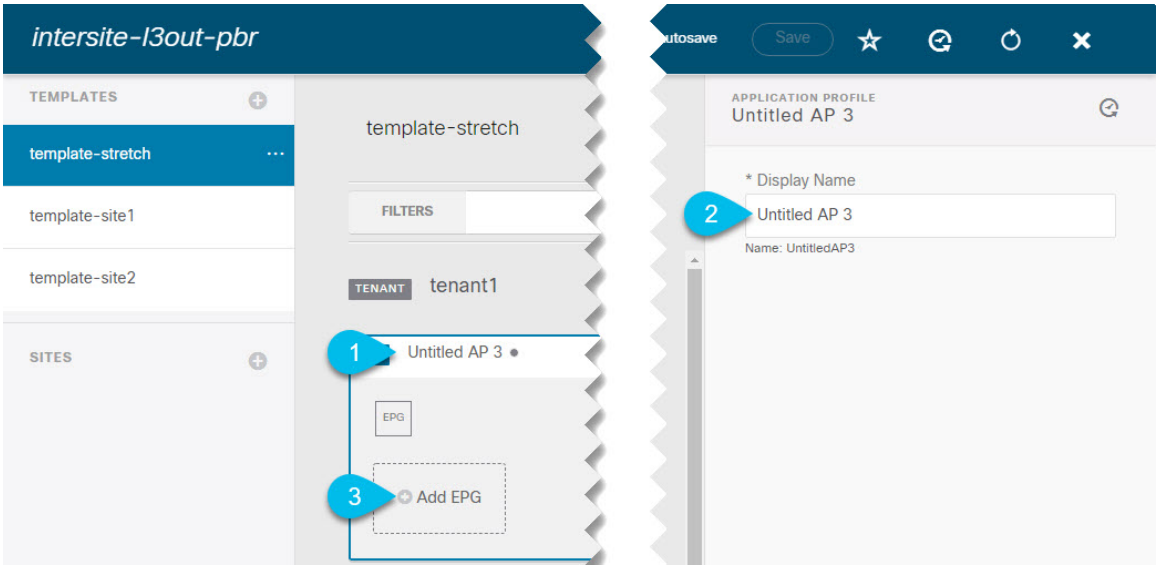
次のものが必要です。

- テンプレートの作成 （234 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 （237 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 （243 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

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。

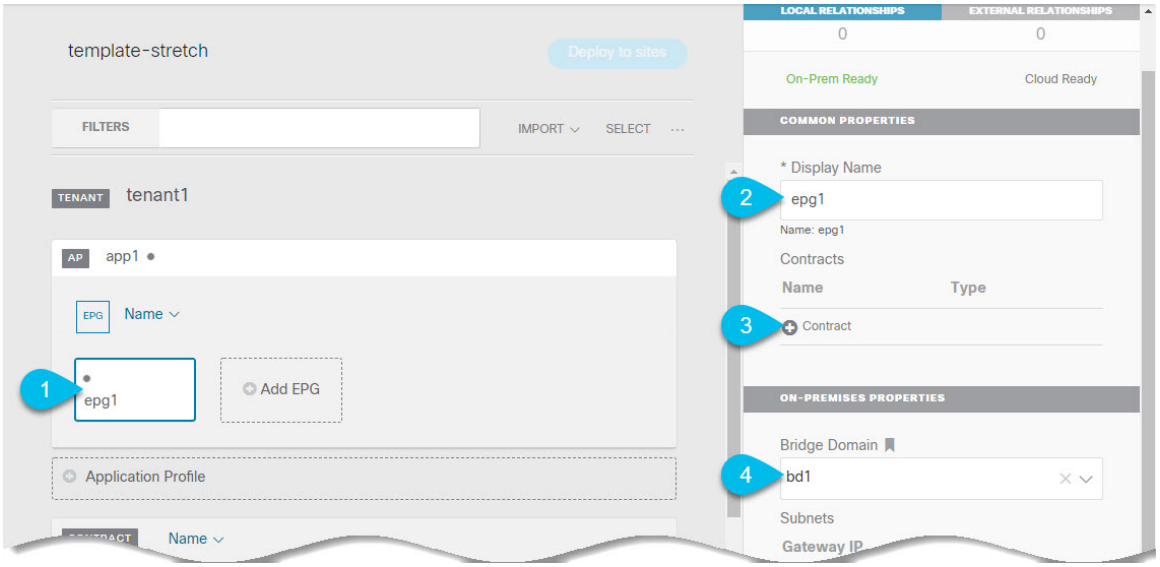
アプリケーション EPG を拡張する場合は、拡張テンプレートで作成します。アプリケーション EPG をサイトローカルにする場合は、サイト固有のテンプレートで作成します。

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 （234 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。

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。

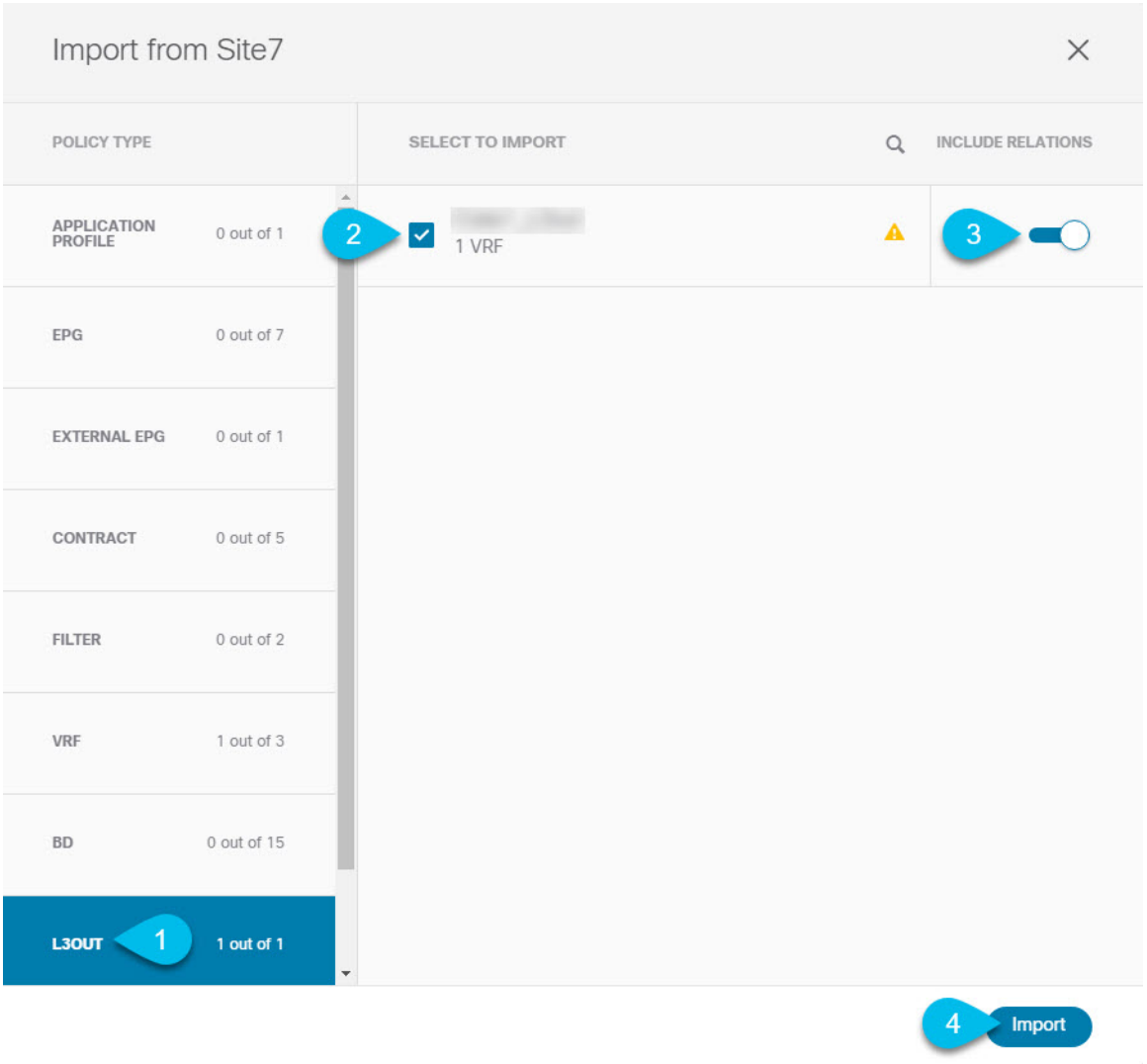
c) L3Out の名前を指定します (例: `l3out-intersite`。

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) [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 （234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 （246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。

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。

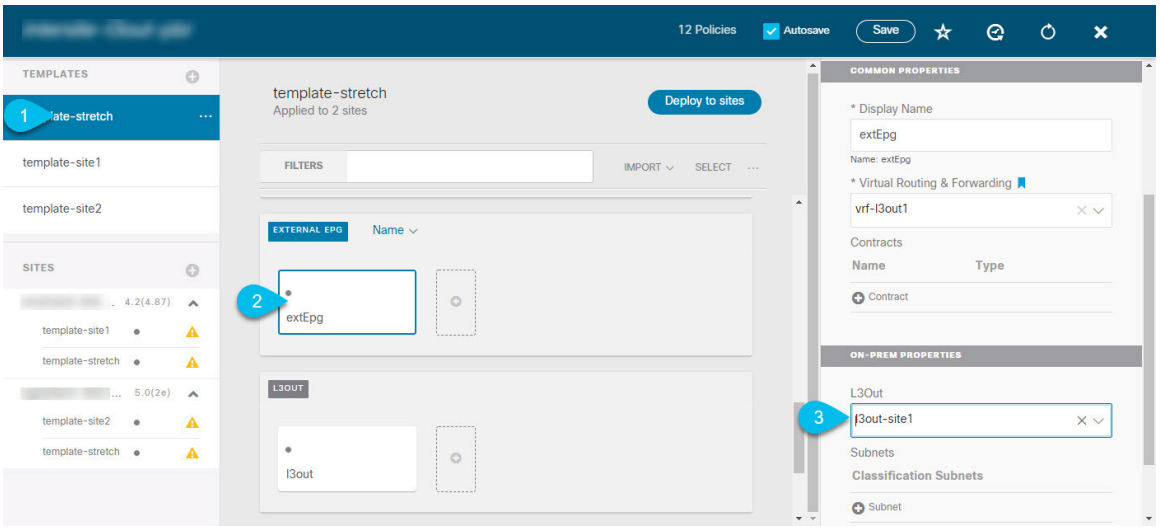
a) 外部 EPG の名前を入力します。たとえば `extEpg` のようにします。
b) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、先ほど作成した、L3Out 用の VRF を選択します。
c) **[+コントラクト (+Contract)]** をクリックし、コントラクトを選択します。

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。



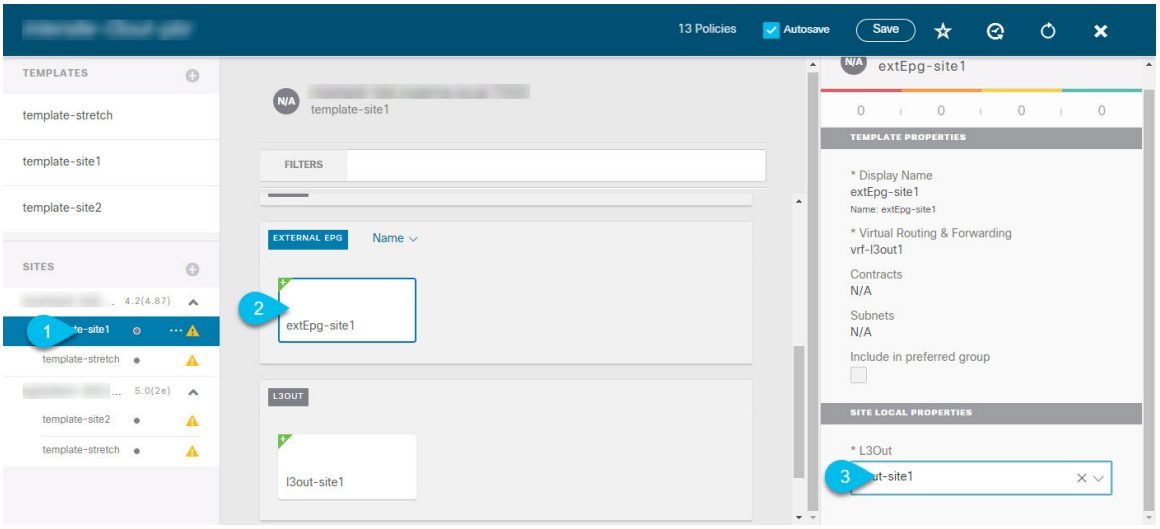
a) スキーマ ビューの左サイドバーで、外部 EPG が置かれているテンプレートを選択します。

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。

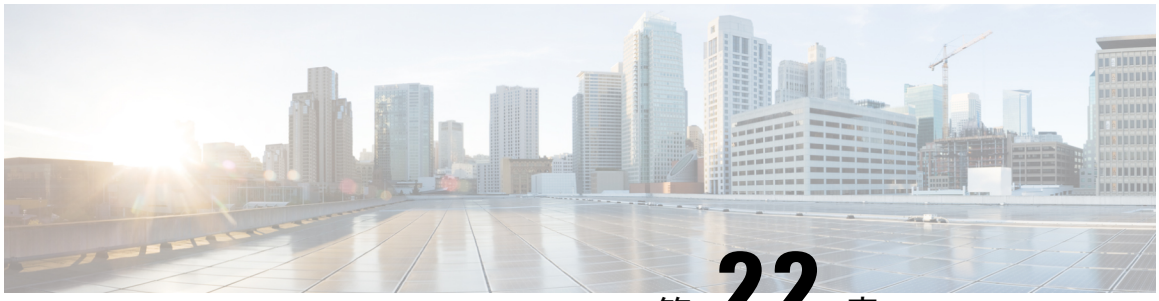


a) スキーマ ビューの左サイドバーで、外部 EPG が配置されているテンプレートを選択します。

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 22 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

Layer 3 Multicast Routing

The following is a high level overview of the Layer 3 multicast routing across sites:

- When the multicast source is attached to the ACI fabric as an endpoint (EP) at one site and starts streaming a multicast flow, the specific site's spine switch that is elected as designated forwarder for the source VRF will forward the multicast traffic to all the remote sites where the source's VRF is stretched using Head End Replication (HREP). If there are no receivers in a specific remote site for that specific group. the traffic gets dropped on the receiving spine node. If there is at least a receiver, the traffic is forwarded into the site and reaches all the leaf nodes where the VRF is deployed and at that point is pruned/forwarded based on the group membership information.
- Prior to Cisco ACI Release 5.0(1), the multicast routing solution required external multicast routers to be the Rendezvous Points (RPs) for PIM-SM any-source multicast (ASM) deployments. Each site must point to the same RP address for a given stretched VRF. The RP must be reachable on each site via the site's local L3Out.
- When the source is outside and the receiver is within a fabric, the receiver will pull traffic via site's local L3Out as PIM joins toward RP and source are always sent via site local L3Out.
- Receivers in each site are expected to draw traffic from an external source via the site's local L3Out. As such, traffic received on the L3Out on one site should not be sent to other sites. This is achieved on the spine by pruning multicast traffic from being replicated into HREP tunnels.

  In order to be able to do so, all multicast traffic originated from an external source and received on a local L3Out is remarked with a special DSCP value in the outer VXLAN header. The spines can hence match that specific DSCP value preventing the traffic from being replicated toward the remote sites.
- Traffic originated from a source connected to a site can be sent toward external receivers via a local L3Out or via L3Outs deployed in remote sites. The specific L3Out that is used for this solely depends on which site received the PIM Join for that specific multicast group from the external network.
- When multicast is enabled on a BD and an EPG on the Nexus Dashboard Orchestrator, all of the BD's subnets are programmed in the routing tables of all the leaf switches, including the border leaf nodes (BLs). This enables receivers attached to the leaf switches to determine the reachability of the multicast source in cases where the source BD is not present on the leaf switches. The subnet is advertised to the external network if there is a proper policy configured on the BLs. The `/32` host routes are advertised if host-based routing is configured on the BD.

For additional information about multicast routing, see the IP Multicast section of the *Cisco APIC Layer 3 Networking Configuration Guide*.

Rendezvous Points

Multicast traffic sources send packets to a multicast address group, with anyone joining that group able to receive the packets. Receivers that want to receive traffic from one or more groups can request to join the group, typically using Internet Group Management Protocol (IGMP). Whenever a receiver joins a group, a multicast distribution tree is created for that group. A Rendezvous Point (RP) is a router in a PIM-SM multicast domain that acts as a shared root for a multicast shared tree.

The typical way to provide a redundant RP function in a network consists in deploying a functionality called Anycast RP, which allows two or more RPs in the network to share the same anycast IP address. This provides for redundancy and load balancing. Should one RP device fails, the other RP can take over without service interruption. Multicast routers can also join the multicast shared tree by connecting to any of the anycast RPs in the network, with PIM `join` requests being forwarded to the closest RP.

Two types of RP configurations are supported from Nexus Dashboard Orchestrator:

- **Static RP**—If your RP is outside the ACI fabric.
- **Fabric RP**—If the border leaf switches in the ACI fabric will function as the anycast RPs.

Any number of routers can be configured to work as RPs and they can be configured to cover different group ranges. When defining the RP inside the ACI fabric, you can configure which groups the RP covers by creating a route-map policy that contains the list of groups and attaching this policy to the RP when adding it to the VRF. Creating a route map is described in マルチキャスト ルート マップ ポリシーの作成, on page 256, while VRF configuration is described in Enabling Any-Source Multicast (ASM) Multicast, on page 257.

Both static and fabric RPs require PIM-enabled border leaf switches in the VRF where multicast routing is enabled. L3Out configuration is currently configured locally from the APIC at each site including enabling PIM for the L3Out. Please refer to the *Cisco APIC Layer 3 Networking Configuration Guide* for details on configuration PIM on L3Outs

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 Multicast Guidelines and Limitations

Up to the current software release, Cisco Nexus Dashboard Orchestrator cannot be used to deploy specific multicast control plane filtering policies, such as IGMP or PIM related policies, on each site. As such you must configure any additional policies required for your use case on each APIC site individually for end-to-end solution to work. For specific information on how to configure those settings on each site, see the *Cisco APIC Layer 3 Networking Configuration Guide*.

You must also ensure that QoS DSCP translation policies in all fabrics are configured consistently. When you create custom QoS policies in ACI fabrics, you can create a mapping between the ACI QoS Levels and the packet header DSCP values for packets ingressing or egressing the fabric. The same ACI QoS Levels must be mapped to the same DSCP values on all sites for the multicast traffic to transit between those sites. For specific information on how to configure those settings on each site, see the *Cisco APIC and QoS*

Multicast Filtering

The following additional guidelines apply if you enable the multicast filtering:

- Multicast filtering is supported only for IPv4.
- You can enable either the multicast source filtering, or the receiver filtering, or both on the same bridge domain.
- If you do not want to have multicast filters on a bridge domain, do not configure a source filter or destination filter route maps on that bridge domain.

  By default, no route maps are associated with a bridge domain, which means that all multicast traffic is allowed. If a route map is associated with a bridge domain, only the permit entries in that route map will be allowed, while all other multicast traffic will be blocked.

  If you attach an empty route map to a bridge domain, route maps assume a `deny-all` by default, so all sources and groups will be blocked on that bridge domain.
- Multicast filtering is done at the BD level and apply to all EPGs within the BD. As such you cannot configure different filtering policies for different EPGs within the same BD. If you need to apply filtering more granularly at the EPG level, you must configure the EPGs in separate BDs.
- Multicast filtering is intended to be used for Any-Source Multicast (ASM) ranges only. Source-Specific Multicast (SSM) is not supported for source filtering and is supported only for receiver filtering.

- For both, source and receiver filtering, the route map entries are matched based on the specified `order` of the entry, with lowest number matched first. This means that lower order entries will match first, even if they are not the longest match in the list, and higher order entries will not be considered.

  For example, if you have the following route map for the `192.0.3.1/32` source:

Order	Source IP	Action
1	192.0.0.0/16	Permit
2	192.0.3.0/24	Deny

  Even though the second entry (`192.0.3.0/24`) is a longer match as a source IP, the first entry (`192.0.0.0/16`) will be matched because of the lower order number.

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。

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

ステップ 2 **[メイン メニュー (Main menu)]** で、**[アプリケーション管理 (Application Management)]** > **[ポリシー (Policies)]** を選択します。

ステップ 3 メイン ペインで、**[ポリシーの追加 (Add Policy)]** > **[マルチキャスト ルート マップ ポリシーの作成 (Create Multicast Route-Map Policy)]** を選択します。

ステップ 4 **[マルチキャスト ルート マップ ポリシーの追加 (Add Multicast Route-Map Policy)]** 画面で、テナントを選択し、ポリシーの名前を指定します。

ステップ 5 ルート マップ エントリを追加するには、**[ルート マップ エントリの順序 (Route-Map Entry Order)]**の下の **[ルートマップ エントリの追加 (Add Route-Map Entry)]** をクリックします。

a) **[順序 (Order)]** と **[アクション(Action)]**を指定します。

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。

[アクション(Action)]は、一致が検出された場合に実行するアクション(許可（permit）または拒否（deny）)を定義します。

b) 必要に応じて、**[グループ IP (Group IP)]**、**[ソース IP (Source IP)]**、および **[RP IP]** 情報を指定します。

このセクションの初めで説明したように、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 ポイントの設定をマルチキャスト 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 /8 ～ /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 /8 ～ /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。

c) エントリを保存するには、**[保存（Save）]** をクリックします。

ステップ 6 (オプション) 同じルート ポリシーに複数のエントリを追加する場合は、前の手順を繰り返します。

ステップ 7 **[保存 (Save)]** をクリックして、ルート マップ ポリシーを保存します。

Enabling Any-Source Multicast (ASM) Multicast

The following procedure describes how to enable ASM multicast on VRF, BD, and EPG using the Nexus Dashboard Orchestrator GUI. If you want to enable SSM multicast, follow the steps in Enabling Source-Specific Multicast (SSM), on page 259 instead.

Before you begin

- Ensure you have read and followed the information described in Layer 3 Multicast Guidelines and Limitations, on page 255.
- If you plan to enable multicast filtering, create the required multicast route maps, as described in マルチキャスト ルート マップ ポリシーの作成, on page 256.

- Note that the site-local L3Outs must have PIM enabled in the VRF when fabric RP is enabled.

  This is described in Step 6 of the following procedure. Additional information about PIM configuration on an L3Out is available in the *Cisco APIC Layer 3 Networking Configuration Guide*.

ステップ 1 Log in to your Nexus Dashboard Orchestrator.

ステップ 2 From the left-hand sidebar, select the **Application Management** > **Schemas** view.

ステップ 3 Click on the Schema you want to change.

ステップ 4 Enable Layer 3 multicast on a VRF.

First, you enable Layer 3 multicast on a VRF that is stretched between sites.

a) Select the VRF for which you want to enable Layer 3 multicast.
b) In the right properties sidebar, check the **L3 Multicast** checkbox.

ステップ 5 Add one or more Rendezvous Points (RP).

a) Select the VRF.
b) In the right properties sidebar, click **Add Rendezvous Points**.
c) With the VRF still selected, click **Add Rendezvous Points** in the right sidebar.
d) In the **Add Rendezvous Points** window, provide the IP address of the RP.
e) Choose the type of the RP.

- **Static RP**—If your RP is outside the ACI fabric.
- **Fabric RP**—If your RP is inside the ACI fabric.

f) (Optional) From the **Multicast Route-Map Policy** dropdown, select the route-map policy you configured previously.

By default, the RP IP you provide applies to all multicast groups in the fabric. If you want to restrict the RP to only a specific set of multicast groups, define those groups in a route map policy and select that policy here.

ステップ 6 Enable PIM on the L3Out.

Both static and fabric RPs require PIM-enabled border leaf switches where multicast routing is enabled. L3Out configuration currently cannot be done from the Nexus Dashboard Orchestrator, so you must ensure that PIM is enabled directly in the site's APIC. Additional information about PIM configuration on an L3Out is available in the *Cisco APIC Layer 3 Networking Configuration Guide*.

a) Log in to your site's Cisco APIC.
b) In the top menu, click **Tenants** and select the tenant that contains the L3Out.
c) In the left navigation menu, select **Networking** > **L3Outs** > ***<l3out-name>***.
d) In the main pane, choose the **Policy** tab.
e) Check the **PIM** options.

Multi-Site supports IPv4 multicast only.

ステップ 7 Enable Layer 3 multicast on a BD.

Once you have enabled L3 Multicast on a VRF, you can enable L3 multicast on a Bridge Domain (BD) level.

a) Select the BD for which you want to enable Layer 3 multicast.
b) In the right properties sidebar, check the **L3 Multicast** checkbox.

ステップ 8 (Optional) If you want to configure multicast filtering, provide the route-maps for source and destination filtering.

a) Select the BD.

b) In the right properties sidebar, select a **Route-Map Source Filter** and **Route-Map Destination Filter**.

You can choose to enable either the multicast source filtering, or the receiver filtering, or both.

Keep in mind, if you do not select a route map, the default action is to allow all multicast traffic on the bridge domain; however, if you select a route map the default action changes to deny any traffic not explicitly matched to a filter entry in the route map.

ステップ 9 If your multicast source is in one site and is not stretched to the other sites, enable intersite multicast source option on the EPG.

Once you have enabled L3 Multicast on the BD, you must also enable multicast on the EPGs (part of multicast-enabled BDs) where multicast sources are connected.

a) Select the EPG for which you want to enable Layer 3 multicast.

b) In the right-hand sidebar, check the **Intersite Multicast Source** checkbox.

Enabling Source-Specific Multicast (SSM)

The following procedure describes how to enable SSM multicast on VRF, BD, and EPG using the Nexus Dashboard Orchestrator GUI. If you want to enable ASM multicast, follow the steps in Enabling Any-Source Multicast (ASM) Multicast, on page 257 instead.

Before you begin

- Ensure you have read and followed the information described in Layer 3 Multicast Guidelines and Limitations, on page 255.
- If you plan to enable multicast filtering, create the required multicast route maps, as described in マルチキャスト ルート マップ ポリシーの作成, on page 256.
- Note that you need to configure IGMPv3 interface policy for the multicast-enabled BDs at the site-local level.

  This is described in Step 8 of the following procedure. Additional information is available in the *Cisco APIC Layer 3 Networking Configuration Guide*.

ステップ 1 Log in to your Nexus Dashboard Orchestrator.

ステップ 2 From the left-hand sidebar, select the **Application Management** > **Schemas** view.

ステップ 3 Click on the Schema you want to change.

ステップ 4 Enable Layer 3 multicast on a VRF.

First, you enable Layer 3 multicast on a VRF that is stretched between sites.

a) Select the VRF for which you want to enable Layer 3 multicast.

b) In the right properties sidebar, check the **L3 Multicast** checkbox.

ステップ 5 (Optional) Configure a custom range for SSM listeners.

The default SSM range is `232.0.0.0/8`, which is automatically configured on the switches in your fabric. If you are using SSM, we recommend configuring your listeners to join groups in this range, in which case you can skip this step.

If for any reason you do not want to change your listener configuration, you can add additional SSM ranges under the VRF settings by creating a route-map with up to 4 additional ranges. Keep in mind that if you add a new range it will become an SSM range and cannot be used for ASM at the same time.

Custom SSM range configuration must be done directly in the site's APIC:

a) Log in to your site's Cisco APIC.
b) In the top menu, click **Tenants** and select the tenant that contains the VRF.
c) In the left navigation menu, select **Networking** > **VRFs** > **<*VRF-name*>** > **Multicast**.
d) In the main pane, choose the **Pattern Policy** tab.
e) From the **Route Map** dropdown in the **Source Specific Multicast (SSM)** area, choose an existing route map or click **Create Route Map Policy for Multicast** option to create a new one.

If you select an existing route map, click the icon next to the dropdown to view the route map's details.

In the route map details window or the **Create Route Map Policy for Multicast** window that opens, click **+** to add an entry. Then configure the Group IP; you need to provide only the group IP address to define the new range.

ステップ 6 (Optional) Enable PIM on the site's L3Out.

If you connect multicast sources and/or receivers to the external network domain, you must also enable PIM on the site's L3Out. L3Out configuration currently cannot be done from the Nexus Dashboard Orchestrator, so you must ensure that PIM is enabled directly in the site's APIC. Additional information about PIM configuration on an L3Out is available in the *Cisco APIC Layer 3 Networking Configuration Guide*.

a) Log in to your site's Cisco APIC.
b) In the top menu, click **Tenants** and select the tenant that contains the L3Out.
c) In the left navigation menu, select **Networking** > **L3Outs** > **<*l3out-name*>**.
d) In the main pane, choose the **Policy** tab.
e) Check the **PIM** options.

Multi-Site supports IPv4 multicast only.

ステップ 7 Enable Layer 3 multicast on a BD.

Once you have enabled L3 Multicast on a VRF, you can enable L3 multicast on a Bridge Domain (BD) level.

a) Select the BD for which you want to enable Layer 3 multicast.
b) In the right properties sidebar, check the **L3 Multicast** checkbox.

ステップ 8 Enabled IGMPv3 interface policy on the bridge domains where receivers are connected.

Because you are configuring SSM, you must also assign an IGMPv3 interface policy to the BD. By default, when PIM is enabled, IGMP is also automatically enabled on the SVI but the default version is set to IGMPv2. You must explicitly set the IGMP interface policy to IGMPv3. This must be done at the site-local level:

a) Log in to your site's Cisco APIC.
b) In the top menu, click **Tenants** and select the tenant that contains the BD.
c) In the left navigation menu, select **Networking** > **Bridge Domains** > **<*BD-name*>**.
d) In the main pane, choose the **Policy** tab.

e) From the **IGMP Policy** dropdown, select the IGMP policy or click **Create IGMP Interface Policy** to create a new one.

If you select an existing policy, click the icon next to the dropdown to view the policy details.

In the policy details window or the **Create Route Map Policy for Multicast** window that opens, ensure that the **Version** field is set to `Version 3`.

ステップ 9 (Optional) If you want to configure multicast filtering, provide the route-maps for source and destination filtering.

a) Select the BD.
b) In the right properties sidebar, select a **Route-Map Source Filter** and **Route-Map Destination Filter**.

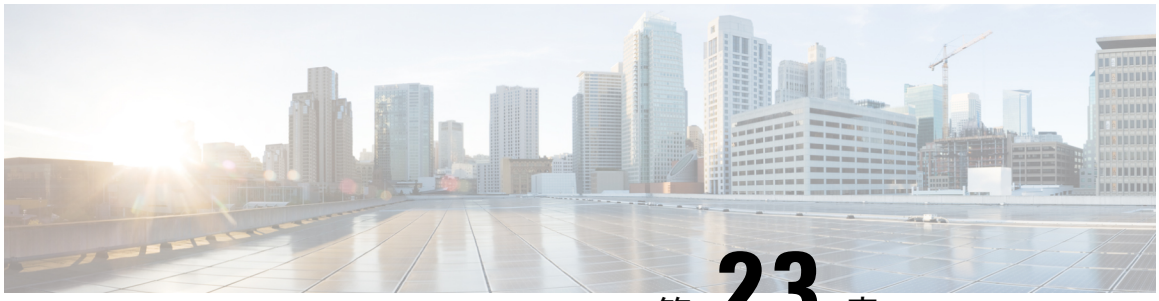
You can choose to enable either the multicast source filtering, or the receiver filtering, or both.

Keep in mind, if you do not select a route map, the default action is to allow all multicast traffic on the bridge domain; however, if you select a route map the default action changes to deny any traffic not explicitly matched to a filter entry in the route map.

ステップ 10 If your multicast source is in one site and is not stretched to the other sites, enable intersite multicast source option on the EPG.

Once you have enabled L3 Multicast on the BD, you must also enable multicast on the EPGs (part of multicast-enabled BDs) where multicast sources are connected.

a) Select the EPG for which you want to enable Layer 3 multicast.
b) In the right-hand sidebar, check the **Intersite Multicast Source** checkbox.



第 23 章

IPN 全体での QoS の保持

QoS and Global DSCP Policy

Cisco ACI Quality of Service (QoS) feature allows you to classify the network traffic in your fabric and then to prioritize and police the traffic flow to help avoid congestion in your network. When traffic is classified within the fabric, it is assigned a QoS Priority Level, which is then used throughout the fabric to provide the most desirable flow of packets through the network.

This release of Nexus Dashboard Orchestrator supports configuration of QoS level based on source EPG or a specific Contract. Additional options are available in each fabric directly. You can find detailed information on ACI QoS in *Cisco APIC and QoS*.

When traffic is sent and received within the Cisco ACI fabric, the QoS Level is determined based on the CoS value of the VXLAN packet's outer header. In certain use cases, such as multi-pod or remote leaf topologies, the traffic must transit an intersite network, where devices that are not under Cisco APIC's management may modify the CoS values in the packets. In these cases you can preserve the ACI QoS Level between parts of the same fabric or different fabrics by creating a mapping between the Cisco ACI QoS level and the DSCP value within the packet.

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 （291 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。

Configuring Global DSCP Policy

When traffic is sent and received within a Cisco ACI fabric, it is prioritized based on the ACI QoS Level, which is determined based on the CoS value of the VXLAN packet's outer header. When traffic exits the ACI fabric towards an intersite network, for example in multi-pod and remote leaf topologies, the QoS level is translated into a DSCP value which is included in the outer header of the VXLAN-encapsulated packet.

This section describes how to define the DSCP translation policy for traffic entering or exiting ACI fabric. This is required when traffic must transit through non-ACI networks, where devices that are not under Cisco APIC's management may modify the CoS values in the transiting packets.

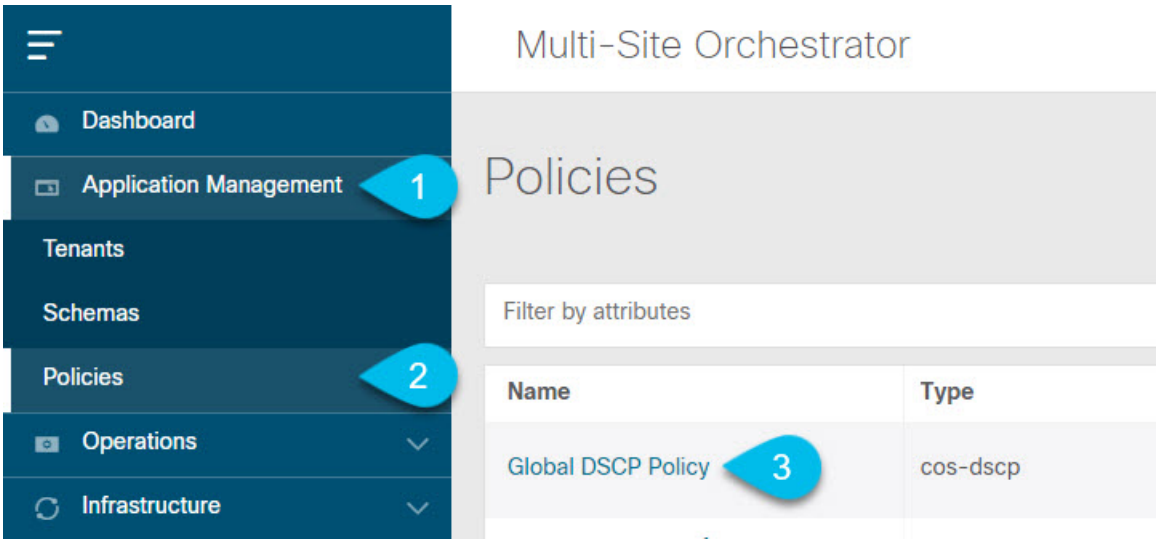
Before you begin

- You should be familiar with Quality of Service (QoS) functionality within ACI fabrics.

  QoS is described in more detail in *Cisco APIC and QoS*.

ステップ 1 Log in to your Cisco Nexus Dashboard Orchestrator GUI.

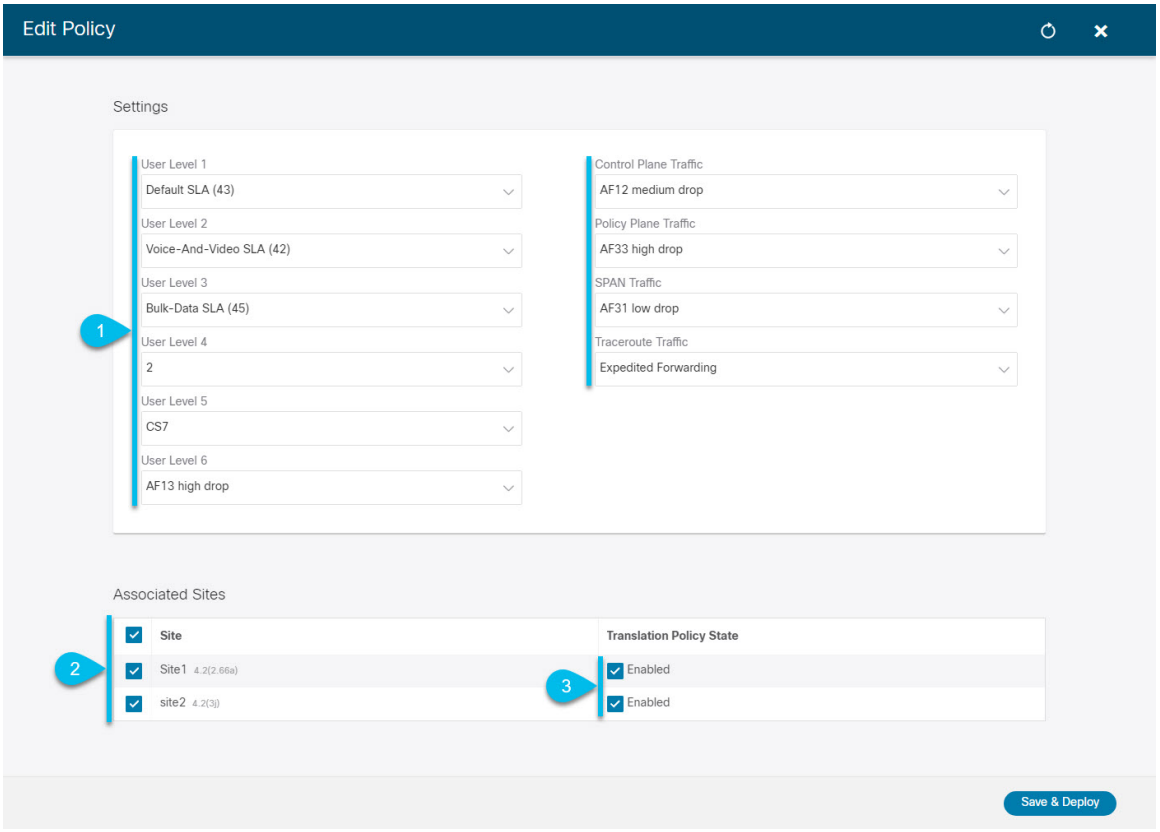
ステップ 2 Open the global DSCP policy configuration screen.



a) Navigate to **Application Management** > **Policies**.
b) Click **Global DSCP Policy** name.

The **Edit Policy** window will open.

ステップ 3 Update the global DSCP policy.



a) Choose the DSCP value for each ACI QoS level.

Each dropdown contains the default list of available DSCP values. You must choose a unique DSCP value for each level.

b) Choose the sites where you want to deploy the policy.

We recommend deploying the policy to all sites that are part of the Multi-Site domain in order to achieve a consistent end-to-end QoS behavior.

c) Choose whether you want to enable the policy on each site when it is deployed.

d) Click **Save & Deploy**.

After you save and deploy, the DSCP policy settings will be pushed to each site. You can verify the configuration by logging in to the site's APIC and navigating to **Tenants** > **infra** > **Policies** > **Protocol** > **DSCP class-CoS translation policy for L3 traffic**.

What to do next

After you have defined the global DSCP policy, you can assign the ACI QoS Levels to EPGs or Contracts as described in Set QoS Level for EPGs and Contracts, on page 266.

Set QoS Level for EPGs and Contracts

This section describes how to choose an ACI QoS level for traffic in your fabrics. You can choose to specify QoS for individual Contracts or entire EPGs.

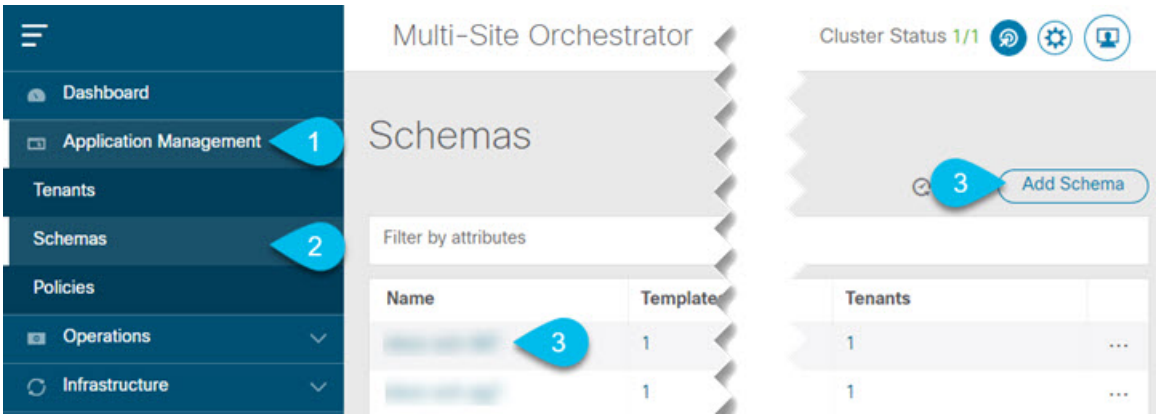
Before you begin

- You must have defined the global DSCP policy, as described in Configuring Global DSCP Policy, on page 264.
- You should be familiar with Quality of Service (QoS) functionality within ACI fabrics.

  QoS is described in more detail in *Cisco APIC and QoS*.

ステップ 1 Log in to your Cisco Nexus Dashboard Orchestrator GUI.

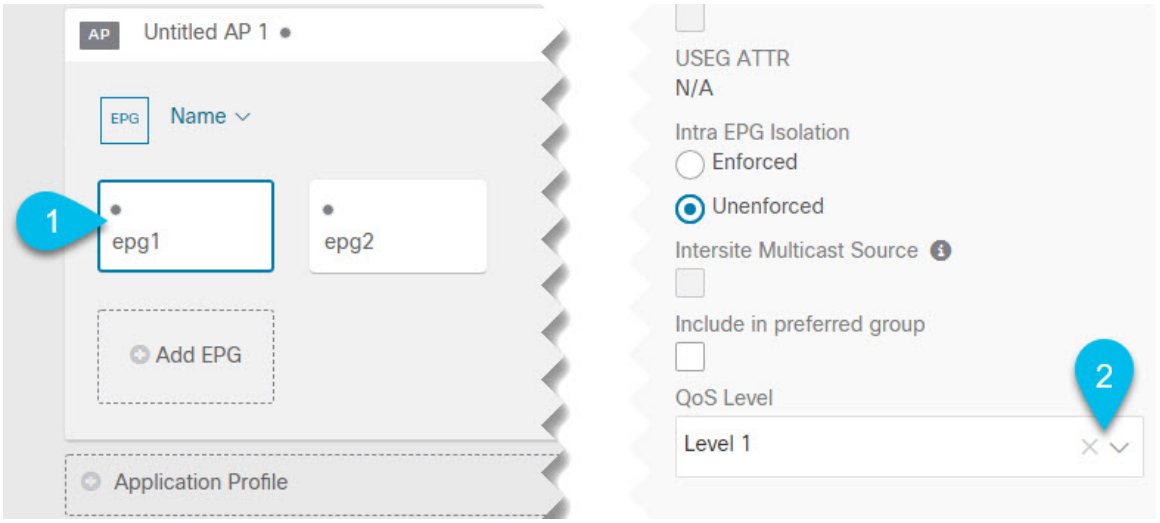
ステップ 2 Choose the Schema you want to edit.



a) Navigate to **Application Management** > **Schemas** > **.**
b) Click the name of the schema you want to edit or **Add Schema** to create a new one.

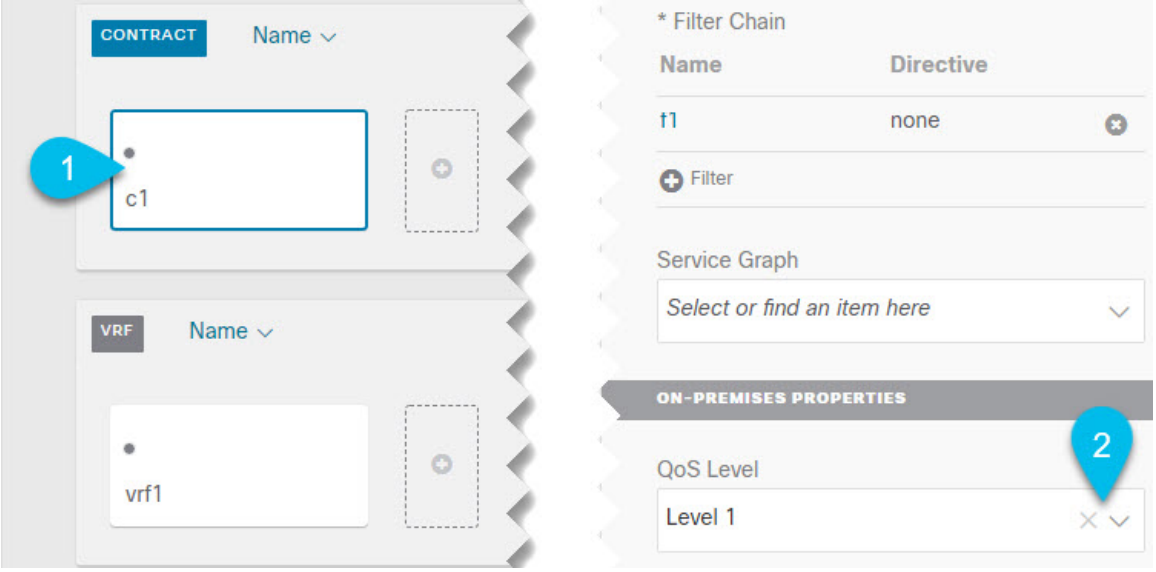
The **Edit Policy** window will open.

ステップ 3 Pick a QoS Level for an EPG

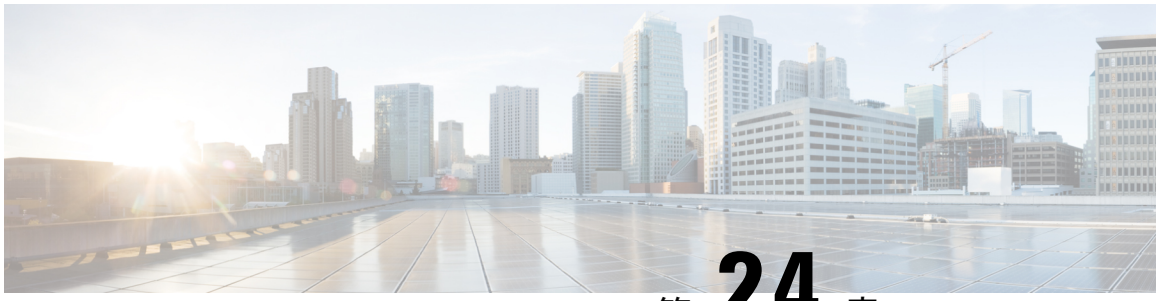


a) In the main pane, scroll down to the **EPG** area and select an EPG or click **Add EPG** to create a new one.
b) In the right sidebar, scroll down to the **QoS Level** dropdown and choose the QoS Level you want to assign to the EPG.

ステップ 4 Pick a QoS Level for an EPG



a) In the main pane, scroll down to the **Contract** area and select a Contract or click the + icon to create a new one.
b) In the right sidebar, scroll down to the **QoS Level** dropdown and choose the QoS Level you want to assign to the Contract.



第 24 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 Intent-Based Networking (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、および保証によってビジネス 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無線ネットワーク ファブリックを定義します。Cisco Digital Network Architecture Controller（DNAC）は、Cisco Identity Services Engine（ISE）と組み合わせて、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 3.6(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 3.6(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

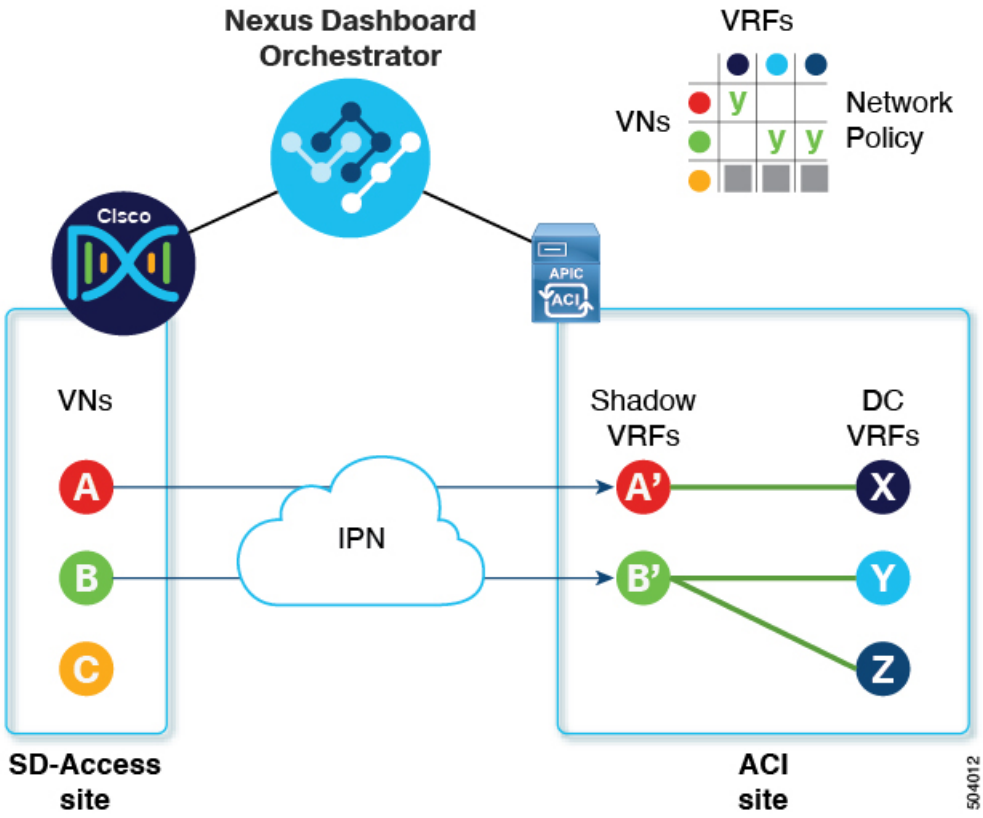
Cisco Nexus Dashboard Orchestrator（NDO）の Cisco SD-Access および Cisco ACI の統合機能により、ACI ドメインと SD-Access ドメイン間のネットワーク要素のマクロ セグメンテーションが可能になります。

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。SD-Access 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。VN 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 SD-Access 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。2 つのドメイン、ACI および SD-Access 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。Cisco Nexus ダッシュボード オーケストレータ Cisco SD-Access と Cisco ACI の統合により、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 と Cisco ACI の統合ワークフローは、次の図を参照する次の手順で構成されます。

図 *28 : 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。SD-AccessDNAC 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、Cisco SD-Access と Cisco ACI の統合のために特別な変更は加えられていないことに注意してください。
- 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 Cisco SD-Access 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。図 28 :

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（271 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 が設定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 統合ガイドライン

- 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設定を提供します。
- 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。)。
  - ACI 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 統合のスケーラビリティ （274 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。
- SD-Access と ACI 統合のスケーラビリティ （274 ページ） で説明されている制限内で、SD-Access 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。
- 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 **[統合] > [DNAC] > [仮想ネットワーク]** テーブルの **[ステータス]** 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（285 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 統合のスケーラビリティ

- SD-Access の 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。
- 単一の DNAC で管理されている場合、複数の SD-Access (キャンパス) サイトがサポートされます。
- SD-Access のピアリングでは、最大 2 つの ACI サイトがサポートされます。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。
- SD-Access 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。

ソフトウェアの互換性

SD-Access の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。

製品	サポート対象の製品バージョン
NDO	3.6 以降のリリース
ACI	4.2 以降のリリース
DNAC	2.3.2 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

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) [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 Cisco SD-Access の 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。ACI ファブリックごとに、Cisco SD-Access ドメインへの接続を提供する境界リーフ 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。

始める前に

DNA センターに登録している必要があります。

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]** で、接続する ACI サイトを選択します。

[サイト接続] ウィンドウが右側に表示されます。

ステップ 6 **[サイト接続]** ウィンドウで、**SDA 接続**コントロールまで下にスクロールし、**[有効]** に設定します。

SDA 接続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、SD-Access 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]** をクリックします。

[Select a Leaf（リーフの選択）] 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) **[Select a Leaf（リーフの選択）]** ペインの **[リーフノード（Leaf Node）]** ドロップダウン リストから、SD-Accessドメインに接続する境界リーフ スイッチを選択します。
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] で、**[インターフェースの追加]** 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。

SD-Access 接続する ACI 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。

SD-Access 接続への ACI 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) **[Save（保存）]** 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、設定はまだ 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。

SD-Access to ACI 統合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 SD-Access サイトの数とタイプ。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 DCNM 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、SD-Access 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。VN 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。ステータス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 の最新ステータスの読み取り。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。
[RouteLeakNone]	赤 (失敗)	VN サブネットはまだ DC 境界リーフ 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 マップされた 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 Sites）]** : 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 デバイス構成] の下にある [詳細を表示] をクリックして、このサイトに接続されている IPN デバイスのサンプル構成を表示します。

- **[…（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。

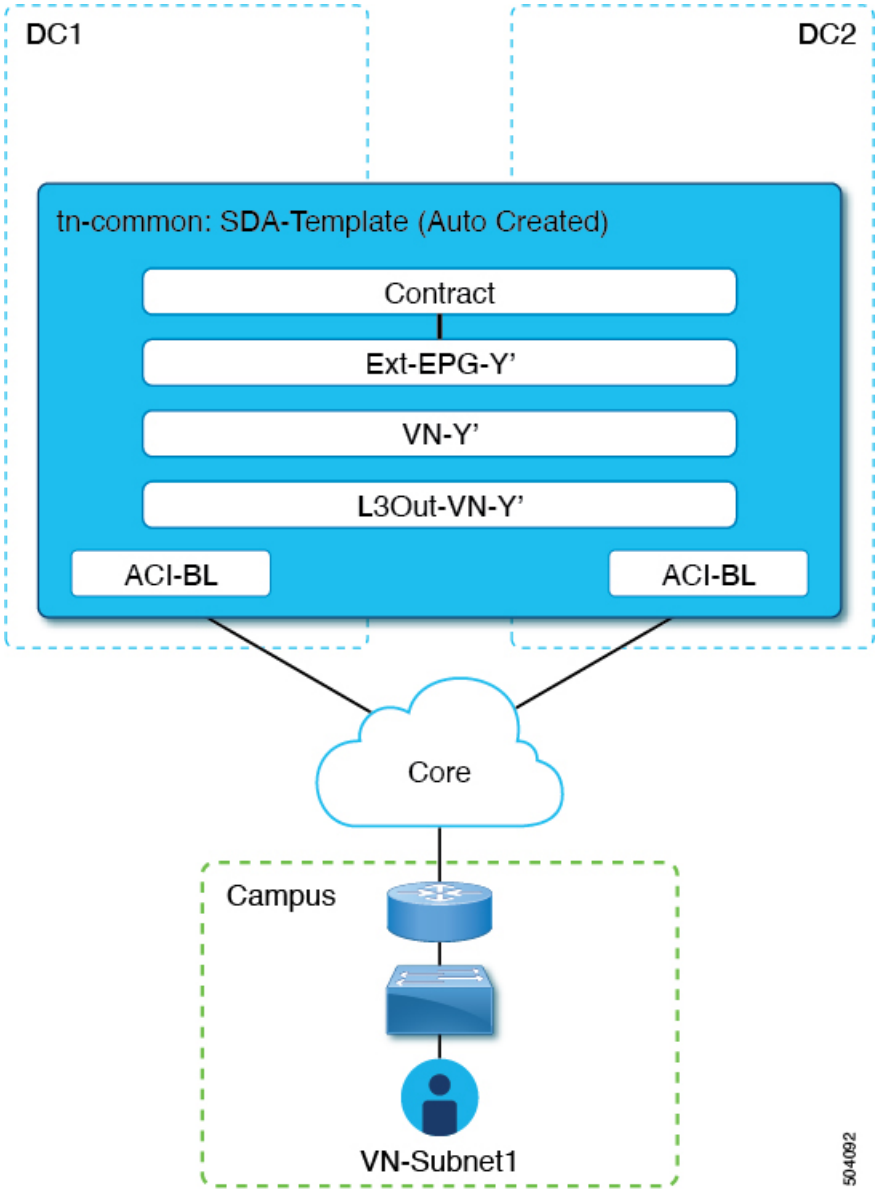
  - VN の拡張 / 拡張解除
  - DC VRF のマッピング / マッピング解除
  - トランジット ルートの有効化 / 無効化

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 29 : VN の拡張 （280 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 *29 : 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SD-Accessドメインへの接続を構成しておく必要があります。

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、SD-Access 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。

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 （275 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、SD-Access 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。

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。

- SD-Access 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。**[インテグレーション（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**[インテグレーション（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

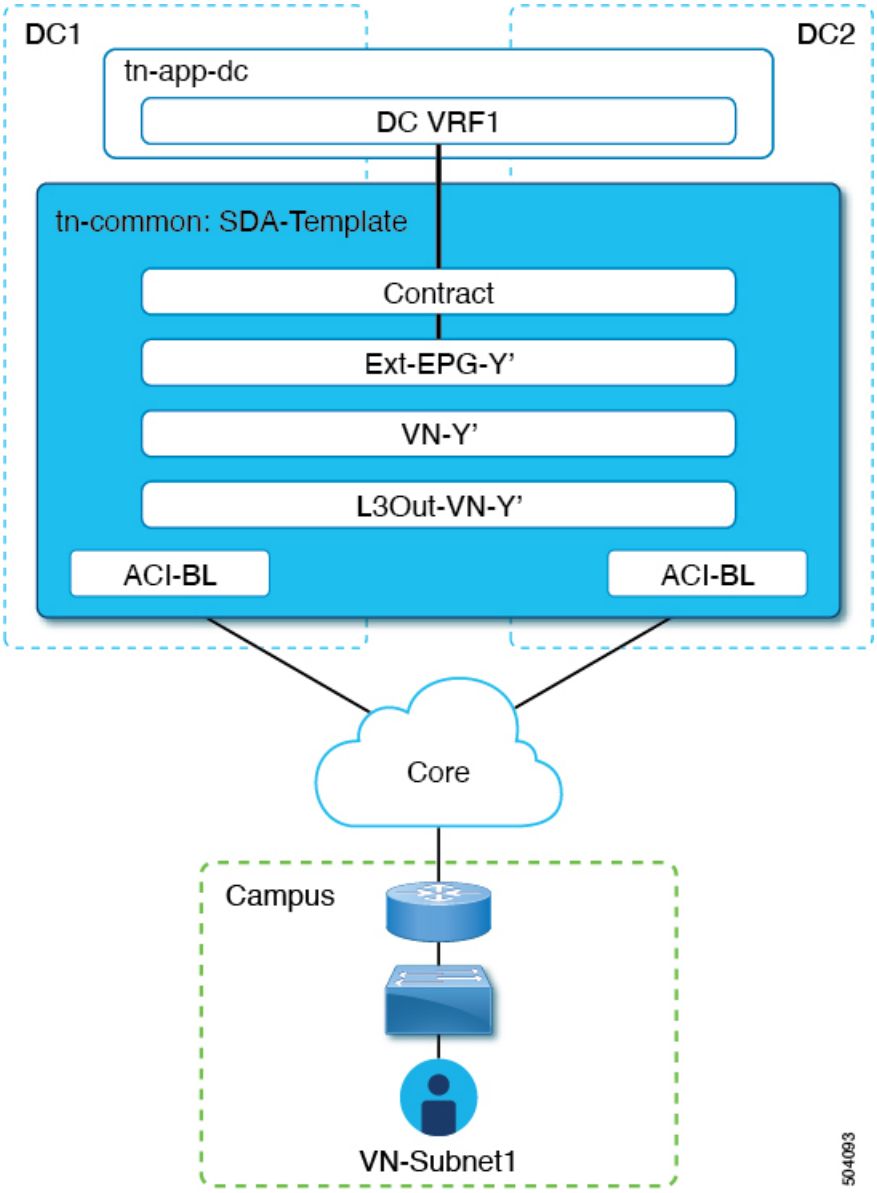
ら、境界リーフ インターフェイスの BGP ピアリング ステータスが「アップ」を示していることを確認します。

VN の VRF へのマッピングまたはマッピング解除 （282 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 30 : VRF へのマッピング （283 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 *30 : 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。

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、SD-Access 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。

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]** 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。

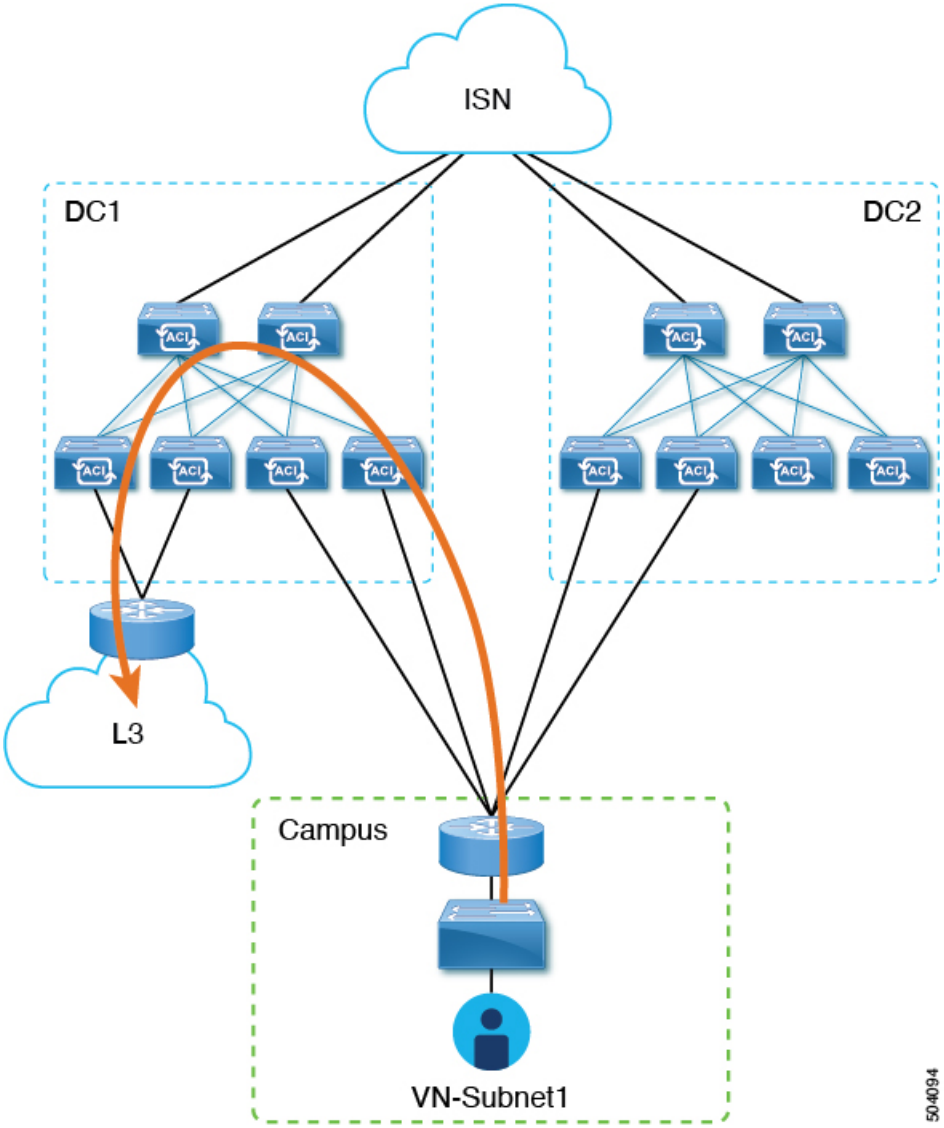
トランジット ルーティングの設定

拡張 SD-Access (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 SD-Access ドメインに向けてアドバタイズされます。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。

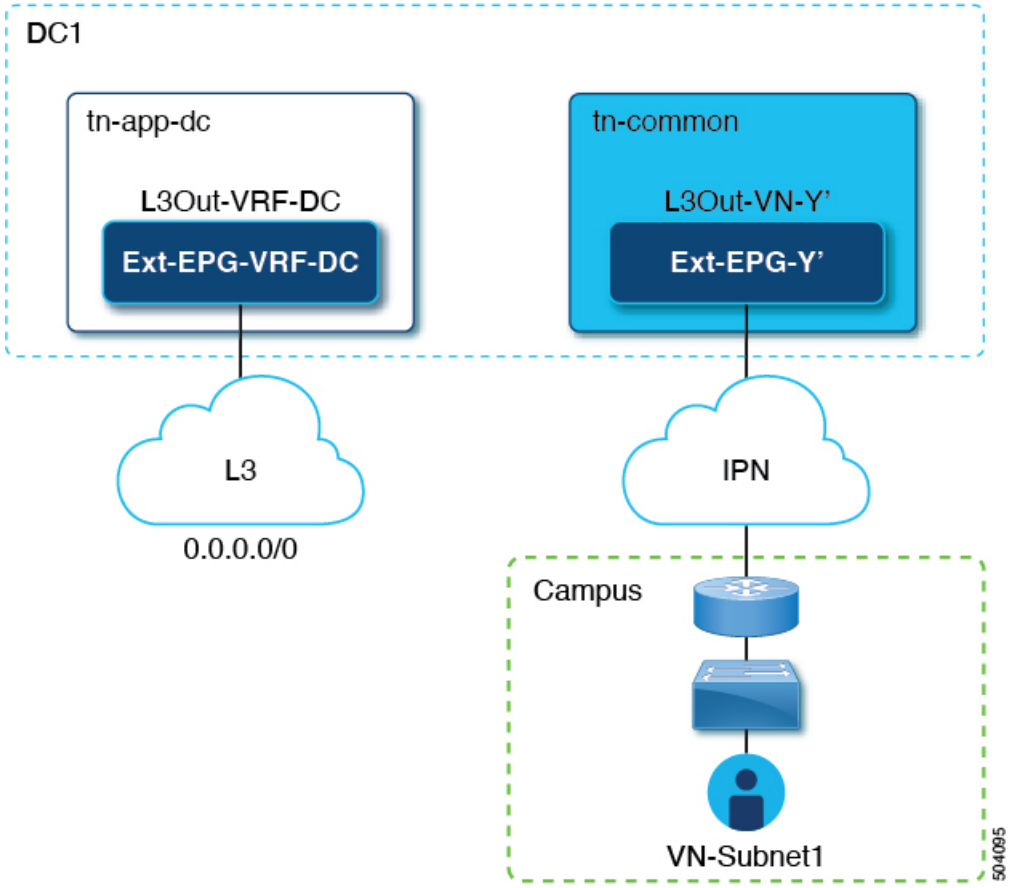
これらの BD サブネットのアドバタイズに加えて、キャンパス ユーザーが ACI ドメインをトランジットとして使用して外部 L3 ネットワーク ドメインにアクセスする必要がある場合があります (図 31 : トランジットとしての ACI ドメイン （286 ページ）)。

図 *31* : 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 32 : L3Out 接続（287 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 *32 : 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。

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

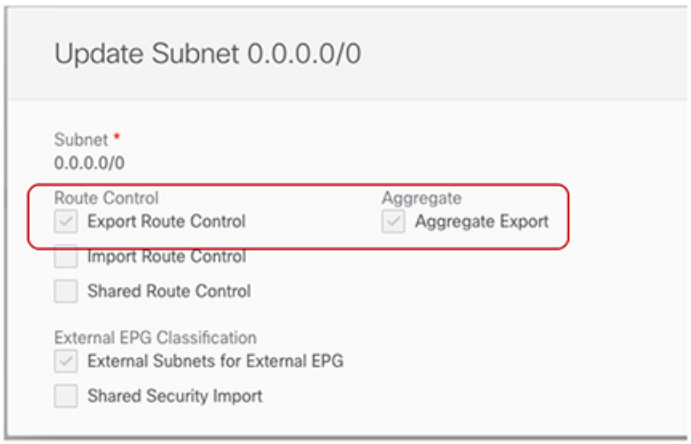
ステップ 2 左側のナビゲーション ペインで、**[インテグレーション（Integrations）] > [DNAC]** を選択します。

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 マッピングに成功したキャンパス 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]** を選択します。

この構成 (図 33 : エクスポート ルート制御 （288 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 *33* : エクスポート ルート制御



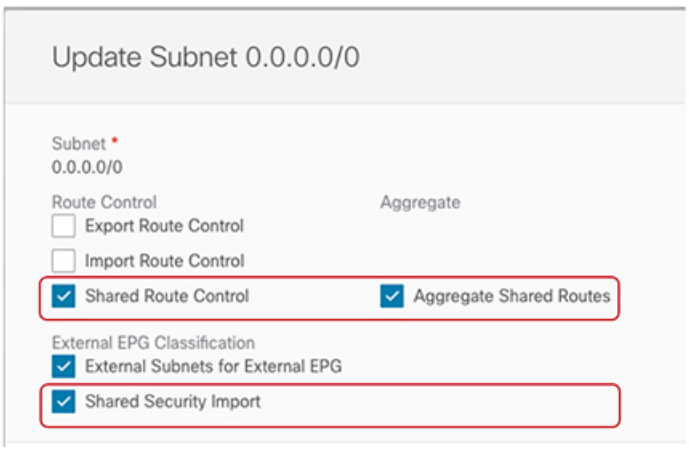
トランジット ルーティングを無効にするには、アクション メニュー（[...]）をクリックし、**[トランジット ルートを無効にする（Disable Transit Route）]** を選択します。

（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]** > [スキーマ] 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 34 : 共有ルート コントロール （288 ページ）)。

図 *34* : 共有ルート コントロール

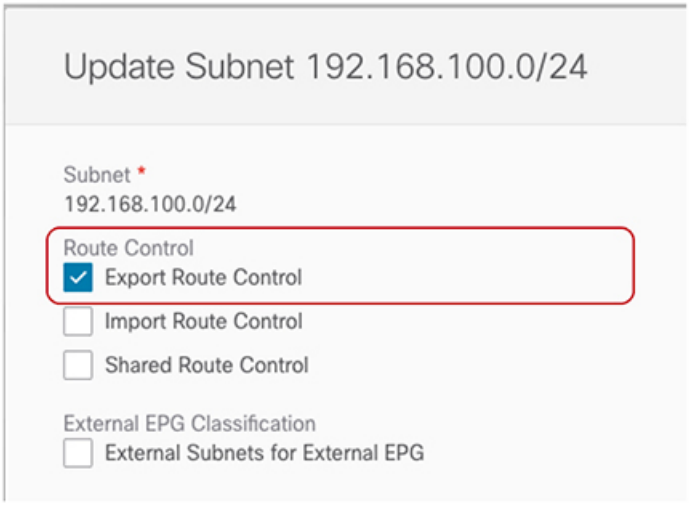


（注） 示されている設定により、L3Out-VRF-DC で受信されたすべての外部プレフィックスが tm-common にリークされるため、キャンパス ドメインに向けてアドバタイズされます。この設定により、L3 ドメインから受信した場合、0.0.0.0/0 デフォルト ルートのリークも許可されます。必要に応じて、外部プレフィックスのサブセットのみを tn-common にリークできる、より詳細な構成を適用できます。これは、プレフィックスのこれらのサブセットに一致する特定のエントリを作成し、それらのエントリに「ここに」示されているのと同じフラグ構成を適用することによって実現されます。

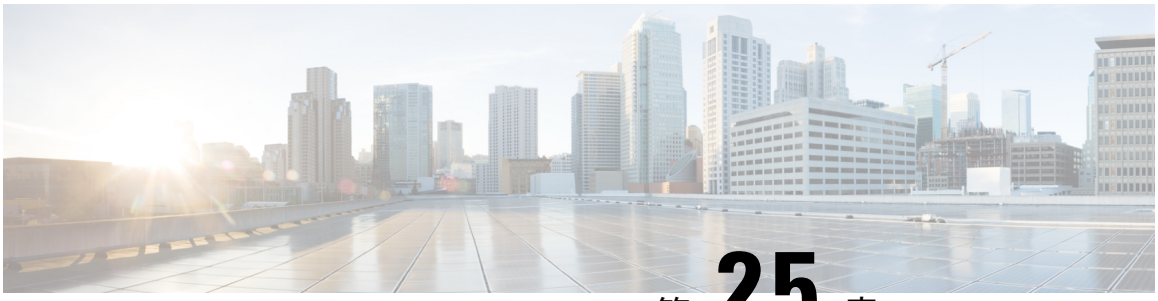
ステップ 7 データセンター テナント アプリケーション テンプレートで、外部 L3 ドメインに向けてアドバタイズされるキャンパス VN サブネット（またはサブネットのセット）に一致する Ext-EPG-VRF-DC の下に特定のプレフィックスを定義します。

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 35 : サブネットの更新 （289 ページ）

図 *35 :* 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 25 章

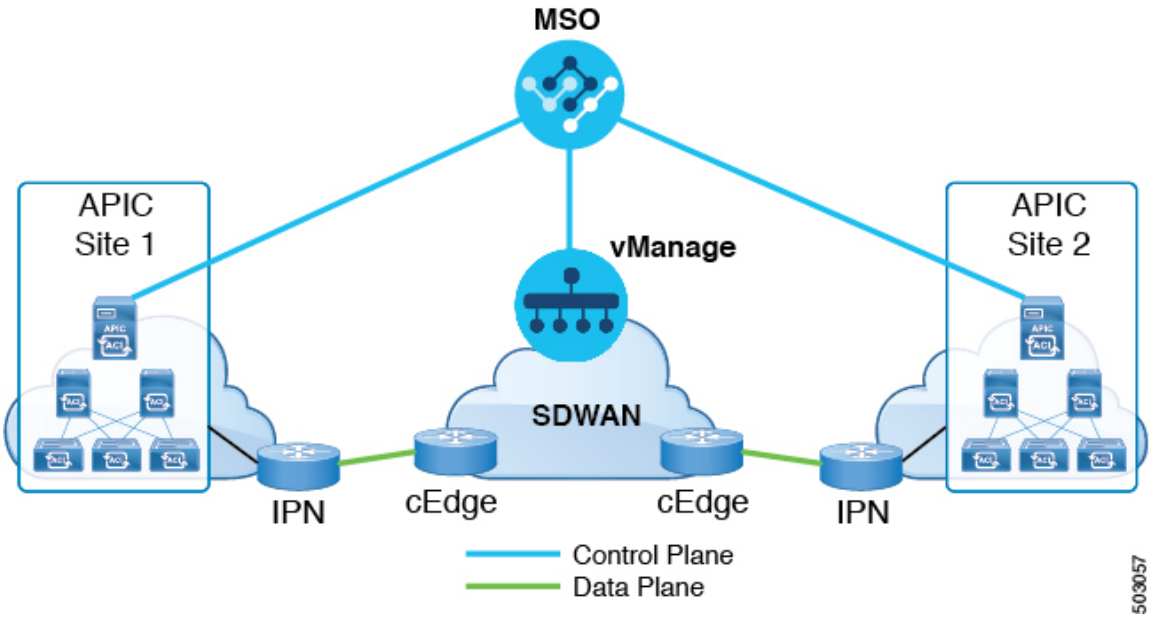
SD-WAN の統合

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 *36 : 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 Integration Guidelines and Limitations

When enabling Multi-Site and SD-WAN integration, the following guidelines apply.

- To enable uniform user QoS Level and DSCP translation for east-west traffic across sites with Muilti-Site SD-WAN integration, the spine switches in each fabric must be connected to the SD-WAN edge devices, either directly or via multiple hops.

This is in contrast with the existing implementation of APIC SD-WAN integration for north-south traffic where the leaf switches must be connected to the SD-WAN edge devices.

- Global DSCP policy is supported for on-premises sites only.
- SD-WAN integration is supported for Nexus Dashboard Orchestrator deployments in Cisco Application Services Engine only.

  For more information, see the Deployment Overview chapter in the *Cisco Nexus Dashboard Orchestrator Installation and Upgrade Guide*.
- When defining the global DSCP policy, you must pick a unique value for each QoS Level.
- In addition to existing DSCP policy values, you can import up to four SLA policies from vManage with one of the following values: 41, 42, 43, 45, 47 and 49.
- SLA policies must be already defined in your Cisco vManage.
- When assigning QoS level, you can choose to assign it to a specific Contract or an entire EPG.

  If multiple QoS levels could apply for any given traffic, only one is applied using the following precedence:
  - Contract QoS level: If QoS is enabled in the Contract, the QoS level specified in the contract is used.
  - Source EPG QoS level: If QoS level is not specified for the Contract, the QoS level set for the source EPG is used.
  - Default QoS level: If no QoS level is specified, the traffic is assigned Level 3 QoS class by default.

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。

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

Configuring Global DSCP Policy （294 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。

Configuring Global DSCP Policy

When traffic is sent and received within a Cisco ACI fabric, it is prioritized based on the ACI QoS Level, which is determined based on the CoS value of the VXLAN packet's outer header. When traffic exits the ACI fabric from a spine switch towards an intersite network, the QoS level is translated into a DSCP value which is included in the outer header of the VXLAN-encapsulated packet.

This section describes how to define the DSCP translation policy for traffic entering or exiting ACI fabric. This is required when traffic must transit through non-ACI networks, such as between multiple fabrics separated by SD-WAN, where devices that are not under Cisco APIC's management may modify the CoS values in the transiting packets.

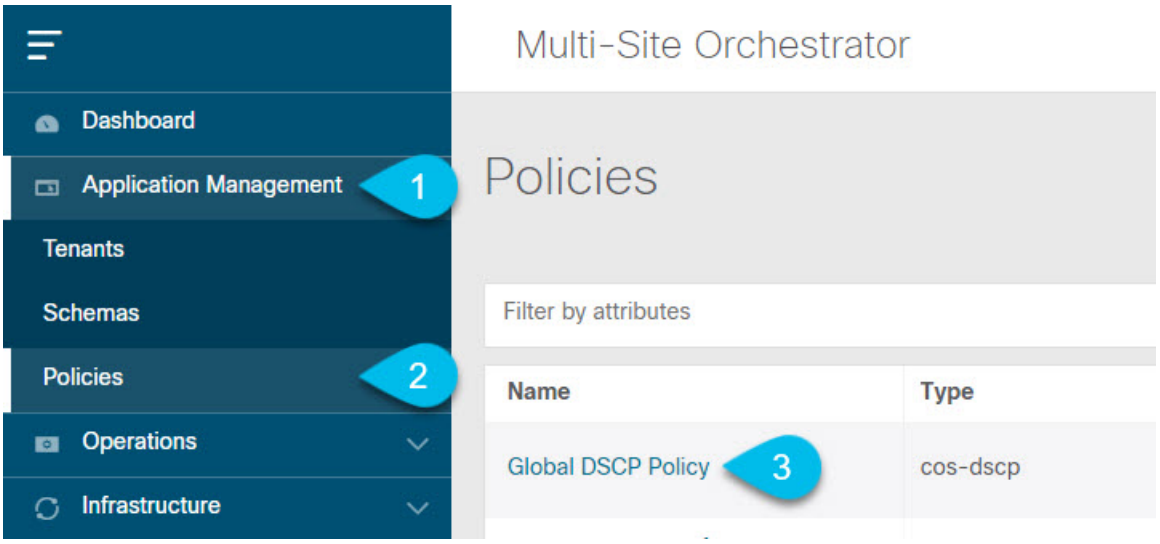
Before you begin

- You must have added a vManage controller to your NDO, as described in vManage コントローラの追加, on page 293.
- You should be familiar with Quality of Service (QoS) functionality within ACI fabrics.

  QoS is described in more detail in *Cisco APIC and QoS*.

ステップ 1 Log in to your Cisco Nexus Dashboard Orchestrator GUI.

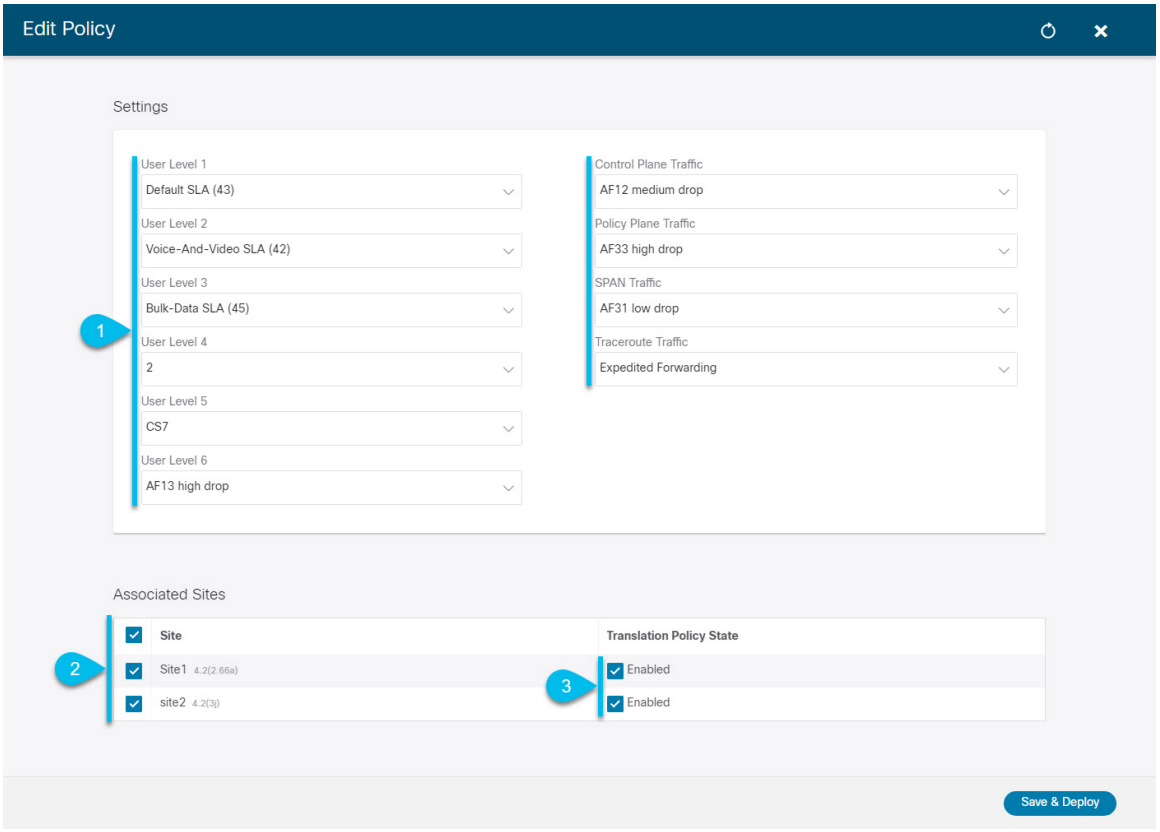
ステップ 2 Open the global DSCP policy configuration screen.



a) Navigate to **Application Management** > **Policies**.
b) Click **Global DSCP Policy** name.

The **Edit Policy** window will open.

ステップ 3 Update the global DSCP policy.



a) Choose the DSCP value for each ACI QoS level.

Each dropdown contains the default list of available DSCP values as well as any values imported from the vManage SLA policies, for example `Voice-And-Video SLA (42)`.

b) Choose the sites where you want to deploy the policy.

We recommend deploying the policy to all sites that are part of the Multi-Site domain in order to achieve a consistent end-to-end QoS behavior.

c) Choose whether you want to enable the policy on each site when it is deployed.

d) Click **Save & Deploy**.

After you save and deploy, the DSCP policy settings will be pushed to each site. You can verify the configuration by logging in to the site's APIC and navigating to **Tenants** > **infra** > **Policies** > **Protocol** > **DSCP class-CoS translation policy for L3 traffic**.

What to do next

After you have defined the global DSCP policy, you can assign the ACI QoS Levels to EPGs or Contracts as described in Set QoS Level for EPGs and Contracts, on page 296

Set QoS Level for EPGs and Contracts

This section describes how to choose an ACI QoS level for traffic in your fabrics. You can choose to specify QoS for individual Contracts or entire EPGs.

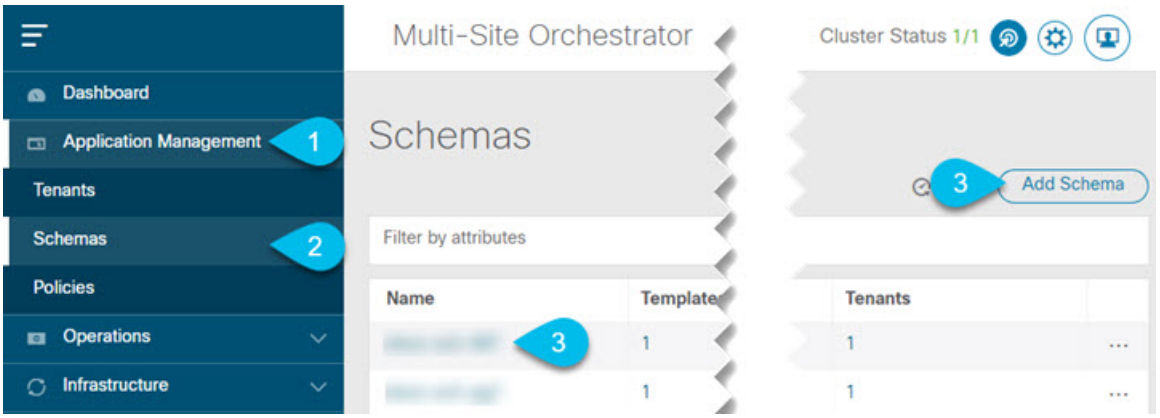
Before you begin

- You must have added a vManage controller to your NDO, as described in vManage コントローラの追加, on page 293.
- You must have defined the global DSCP policy, as described in Configuring Global DSCP Policy, on page 294.
- You should be familiar with Quality of Service (QoS) functionality within ACI fabrics.

  QoS is described in more detail in *Cisco APIC and QoS*.

ステップ 1 Log in to your Cisco Nexus Dashboard Orchestrator GUI.

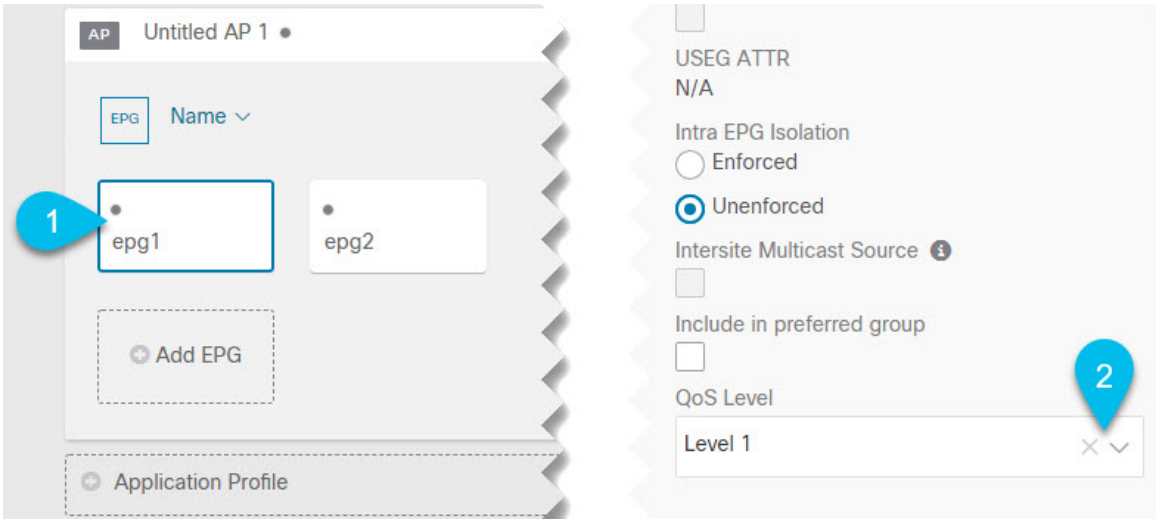
ステップ 2 Choose the Schema you want to edit.



a) Navigate to **Application Management** > **Schemas** > **.**
b) Click the name of the schema you want to edit or **Add Schema** to create a new one.

The **Edit Schema** window will open.

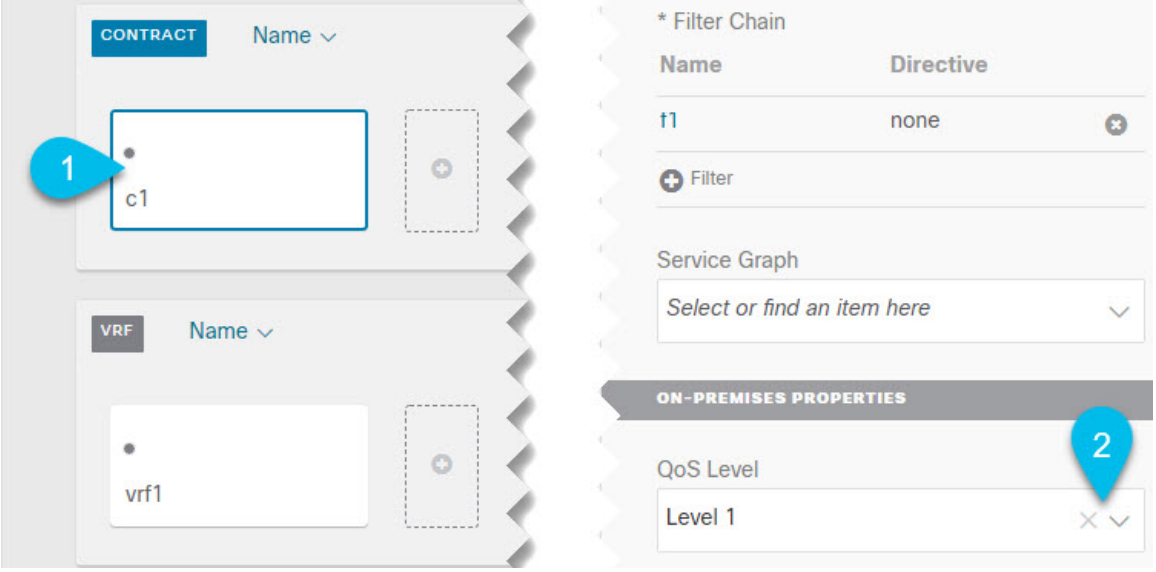
ステップ 3 Pick a QoS Level for an EPG



a) In the main pane, scroll down to the **EPG** area and select an EPG or click **Add EPG** to create a new one.
b) In the right sidebar, scroll down to the **QoS Level** dropdown and choose the QoS Level you want to assign to the EPG.

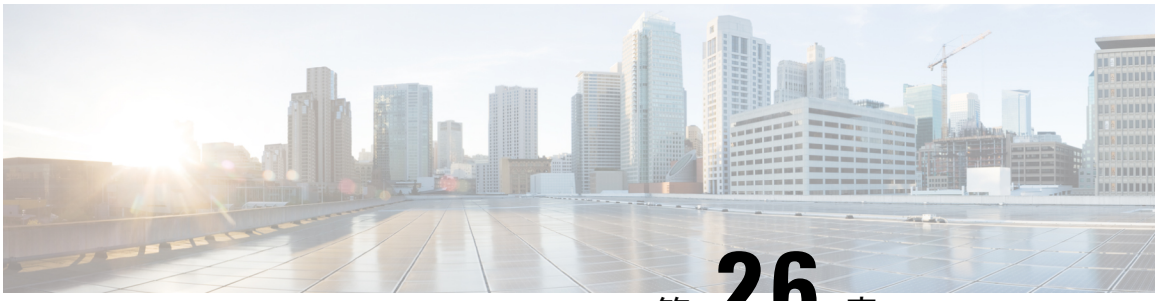
You must choose the QoS level based on the previously configured Global DSCP policy to ensure that intersite traffic from the EPG is treated with the desired SLA across the SD-WAN network.

ステップ 4 Pick a QoS Level for an EPG



a) In the main pane, scroll down to the **Contract** area and select a Contract or click the + icon to create a new one.
b) In the right sidebar, scroll down to the **QoS Level** dropdown and choose the QoS Level you want to assign to the Contract.

   You must choose the QoS level based on the previously configured Global DSCP policy to ensure that intersite traffic between two EPGs is treated with the desired SLA across the SD-WAN network.



第 26 章

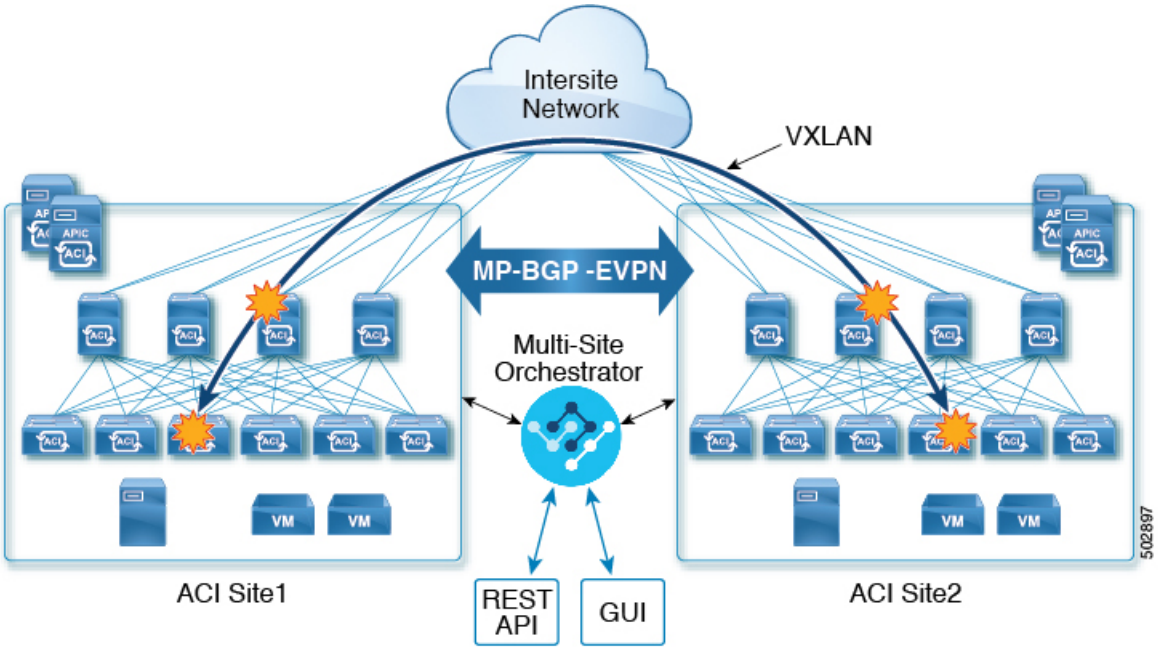
SR-MPLS 経由で接続されたサイト

SR-MPLS and Multi-Site

Starting with Nexus Dashboard Orchestrator, Release 3.0(1) and APIC Release 5.0(1), the Multi-Site architecture supports APIC sites connected via MPLS networks.

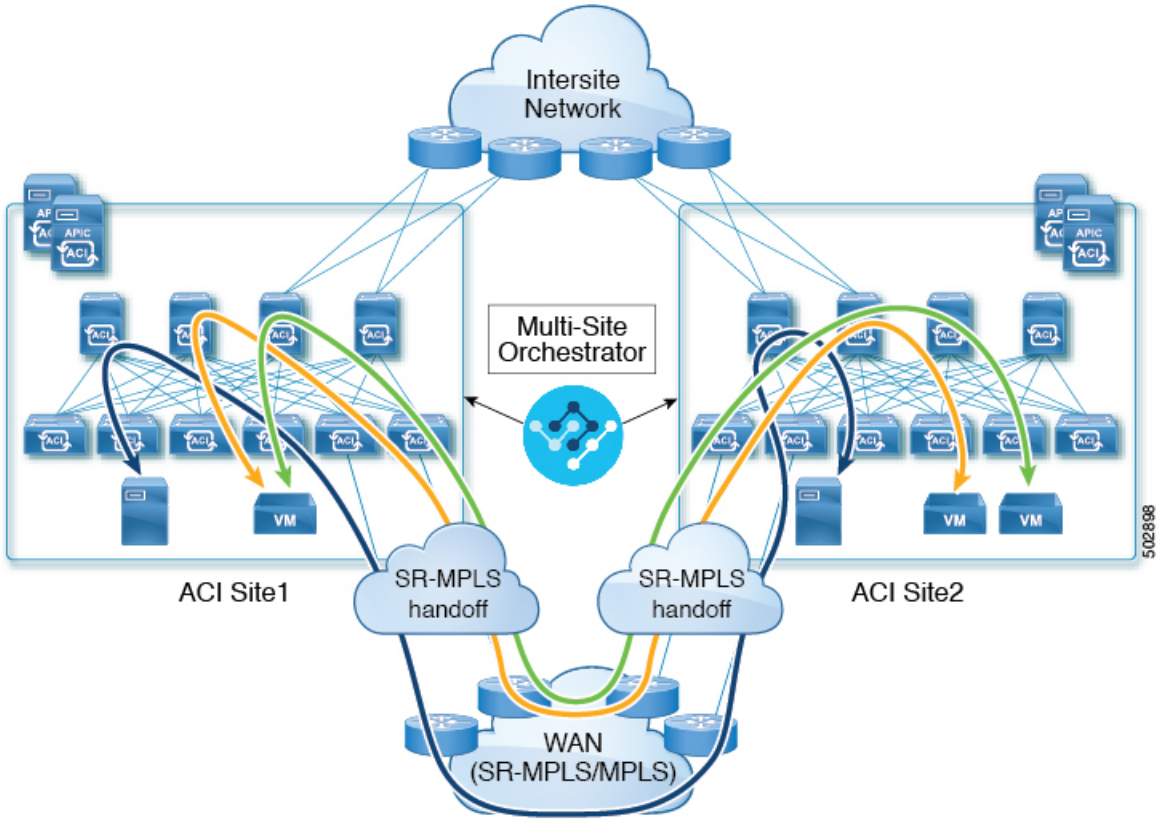
In a typical Multi-Site deployment, traffic between sites is forwarded over an intersite network (ISN) via VXLAN encapsulation:

Figure 37: Multi-Site and ISN



With Release 3.0(1), MPLS network can be used in addition to or instead of the ISN allowing inter-site communication via WAN:

Figure 38: Multi-Site and MPLS



The following sections describe guidelines, limitations, and configurations specific to managing Schemas that are deployed to these sites from the Nexus Dashboard Orchestrator. Detailed information about MPLS hand off, supported individual site topologies (such as remote leaf support), and policy model is available in the *Cisco APIC Layer 3 Networking Configuration Guide*.

インフラの設定

SR-MPLS Infra Guidelines and Limitations

If you want to add an APIC site that is connected to an SR-MPLS network to be managed by the Nexus Dashboard Orchestrator, keep the following in mind:

- Any changes to the topology, such as node updates, are not reflected in the Orchestrator configuration until site configuration is refreshed, as described in サイト接続性情報の更新, on page 151.
- Objects and policies deployed to a site that is connected to an SR-MPLS network cannot be stretched to other sites.

  When you create a template and specify a Tenant, you will need to enable the `SR-MPLS` option on the tenant. You will then be able to map that template only to a single ACI site.

- Tenants deployed to a site that is connected via an SR-MPLS network will have a set of unique configuration options specifically for SR-MPLS configuration. Tenant configuration is described in the "Tenants Management" chapter of the *Multi-Site Configuration Guide, Release 3.1(x)*

Supported Hardware

The SR-MPLS connectivity is supported for the following platforms:

- **Border Leaf switches**: The "FX", "FX2", and "GX" switch models.
- **Spine switches**:
  - Modular spine switch models with "LC-EX", "LC-FX", and "GX" at the end of the linecard names.
  - The Cisco Nexus 9000 series N9K-C9332C and N9K-C9364C fixed spine switches.
- **DC-PE routers**:
  - Network Convergence System (NCS) 5500 Series
  - ASR 9000 Series
  - NCS 540 or 560 routers

SR-MPLS Infra L3Out

You will need to create an SR-MPLS Infra L3Out for the fabrics connected to SR-MPLS networks as described in the following sections. When creating an SR-MPLS Infra L3Out, the following restrictions apply:

- Each SR-MPLS Infra L3Out must have a unique name.
- You can have multiple SR-MPLS infra L3Outs connecting to different routing domains, where the same border leaf switch can be in more than one L3Out, and you can have different import and export routing policies for the VRFs toward each routing domain.
- Even though a border leaf switch can be in multiple SR-MPLS infra L3Outs, a border leaf switch/provider edge router combination can only be in one SR-MPLS infra L3Out as there can be only one routing policy for a user VRF/border leaf switch/DC-PE combination.
- If there is a requirement to have SR-MPLS connectivity from multiple pods and remote locations, ensure that you have a different SR-MPLS infra L3Out in each of those pods and remote leaf locations with SR-MPLS connectivity.
- If you have a multi-pod or remote leaf topology where one of the pods is not connected directly to the SR-MPLS network, that pod's traffic destined for the SR-MPLS network will use standard IPN path to another pod, which has an SR-MPLS L3Out. Then the traffic will use the other pod's SR-MPLS L3Out to reach its destination across SR-MPLS network.
- Routes from multiple VRFs can be advertised from one SR-MPLS Infra L3Out to provider edge (PE) routers connected to the nodes in this SR-MPLS Infra L3Out.

  PE routers can be connected to the border leaf directly or through other provider (P) routers.

- The underlay configuration can be different or can be the same across multiple SR-MPLS Infra L3Outs for one location.

  For example, assume the same border leaf switch connects to PE-1 in domain 1 and PE-2 in domain 2, with the underlay connected to another provider router for both. In this case, two SR-MPLS Infra L3Outs will be created: one for PE-1 and one for PE-2. But for the underlay, it's the same BGP peer to the provider router. Import/export route-maps will be set for EVPN session to PE-1 and PE-2 based on the corresponding route profile configuration in the user VRF.

Guidelines and Limitations for MPLS Custom QoS Policies

Following is the default MPLS QoS behavior:

- All incoming MPLS traffic on the border leaf switch is classified into QoS Level 3 (the default QoS level).
- The border leaf switch will retain the original DSCP values for traffic coming from SR-MPLS without any remarking.
- The border leaf switch will forward packets with the default MPLS EXP (0) to the SR-MPLS network.

Following are the guidelines and limitations for configuring MPLS Custom QoS policies:

- Data Plane Policers (DPP) are not supported at the SR-MPLS L3Out.
- Layer 2 DPP works in the ingress direction on the MPLS interface.
- Layer 2 DPP works in the egress direction on the MPLS interface in the absence of an egress custom MPLS QoS policy.
- VRF level policing is not supported.

Creating SR-MPLS QoS Policy

This section describes how to configure SR-MPLS QoS policy for a site that is connected via an MPLS network. If you have no such sites, you can skip this section.

SR-MPLS Custom QoS policy defines the priority of the packets coming from an SR-MPLS network while they are inside the ACI fabric based on the incoming MPLS EXP values defined in the MPLS QoS ingress policy. It also marks the CoS and MPLS EXP values of the packets leaving the ACI fabric through an MPLS interface based on IPv4 DSCP values defined in MPLS QoS egress policy.

If no custom ingress policy is defined, the default QoS Level (`Level3`) is assigned to packets inside the fabric. If no custom egress policy is defined, the default EXP value of `0` will be marked on packets leaving the fabric.

ステップ 1 Log in to the Nexus Dashboard Orchestrator GUI.

ステップ 2 In the **Main menu**, select **Application Management** > **Policies**.

ステップ 3 In the main pane, select **Add Policy** > **Create QoS Policy**.

ステップ 4 In the **Add QoS Policy** screen, provide the name for the policy.

ステップ 5 Click **Add Ingress Rule** to add an ingress QoS translation rule.

These rules are applied for traffic that is ingressing the ACI fabric from an MPLS network and are used to map incoming packet's experimental bits (EXP) values to ACI QoS levels, as well as to set differentiated services code point (DSCP) values in the VXLAN header for the packet while it's inside the ACI fabric.

The values are derived at the border leaf using a custom QoS translation policy. The original DSCP values for traffic coming from SR-MPLS without any remarking. If a custom policy is not defined or not matched, default QoS Level (`Level3`) is assigned

a) In the **Match EXP From** and **Match EXP To** fields, specify the EXP range of the ingressing MPLS packet you want to match.
b) From the **Queuing Priority** dropdown, select the ACI QoS Level to map.

   This is the QoS Level you want to assign for the traffic within ACI fabric, which ACI uses to prioritize the traffic within the fabric.. The options range from Level1 to Level6. The default value is `Level3`. If you do not make a selection in this field, the traffic will automatically be assigned a `Level3` priority.

c) From the **Set DSCP** dropdown, select the DSCP value to assign to the packet when it's inside the ACI fabric.

   The DSCP value specified is set in the original traffic received from the external network, so it will be re-exposed only when the traffic is VXLAN decapsulated on the destination ACI leaf node.

   If you set the value to `Unspecified`, the original DSCP value of the packet will be retained.

d) From the **Set CoS** dropdown, select the CoS value to assign to the packet when it's inside the ACI fabric.

   The CoS value specified is set in the original traffic received from the external network, so it will be re-exposed only when the traffic is VXLAN decapsulated on the destination ACI leaf node.

   If you set the value to `Unspecified`, the original CoS value of the packet will be retained, but only if the CoS preservation option is enabled in the fabric. For more information about CoS preservation, see *Cisco APIC and QoS*.

e) Click the checkmark icon to save the rule.
f) Repeat this step for any additional ingress QoS policy rules.

ステップ 6 Click **Add Egress Rule** to add an egress QoS translation rule.

These rules are applied for the traffic that is leaving the ACI fabric via an MPLS L3Out and are used to map the packet's IPv4 DSCP value to the MPLS packet's EXP value as well as the internal ethernet frame's CoS value.

Classification is done at the non-border leaf switch based on existing policies used for EPG and L3Out traffic. If a custom policy is not defined or not matched, the default EXP value of `0` is marked on all labels. EXP values are marked in both, default and custom policy scenarios, and are done on all MPLS labels in the packet.

Custom MPLS egress policy can override existing EPG, L3out, and Contract QoS policies

a) Using the **Match DSCP From** and **Match DSCP To** dropdowns, specify the DSCP range of the ACI fabric packet you want to match for assigning the egressing MPLS packet's priority.
b) From the **Set MPLS EXP** dropdown, select the EXP value you want to assign to the egressing MPLS packet.
c) From the **Set CoS** dropdown, select the CoS value you want to assign to the egressing MPLS packet.
d) Click the checkmark icon to save the rule.
e) Repeat this step for any additional egress QoS policy rules.

ステップ 7 Click **Save** to save the QoS policy.

What to do next

After you have created the QoS policy, enable MPLS connectivity and configure MPLS L3Out as described in #unique_202.

Creating SR-MPLS Infra L3Out

This section describes how to configure SR-MPLS L3Out settings for a site that is connected to an SR-MPLS network.

- The SR-MPLS infra L3Out is configured on the border leaf switch, which is used to set up the underlay BGP-LU and overlay MP-BGP EVPN sessions that are needed for the SR-MPLS handoff.
- An SR-MPLS infra L3Out will be scoped to a pod or a remote leaf switch site.
- Border leaf switches or remote leaf switches in one SR-MPLS infra L3Out can connect to one or more provider edge (PE) routers in one or more routing domains.
- A pod or remote leaf switch site can have one or more SR-MPLS infra L3Outs.

Before you begin

You must have:

- Added a site that is connected via SR-MPLS network as described in Adding Cisco ACI Sites, on page 137.
- If necessary, created SR-MPLS QoS policy as described in Creating SR-MPLS QoS Policy, on page 303.

ステップ 1 Log in to the Cisco Nexus Dashboard Orchestrator GUI.

ステップ 2 Ensure that SR-MPLS Connectivity is enabled for the site.

a) In the main navigation menu, select **Infrastructure** > **Infra Configuration**.
b) In the **Infra Configuration** view, click **Configure Infra**.
c) In the left pane, under **Sites**, select a specific site.
d) In the right ***<Site>*** **Settings** pane, enable the **SR-MPLS Connectivity** knob and provide the Segment Routing global block (SRGB) range

The SID index is configured on each node for the MPLS transport loopback. The SID index value is advertised using BGP-LU to the peer router, and the peer router uses the SID index to calculate the local label.

The Segment Routing Global Block (SRGB) is the range of label values reserved for Segment Routing (SR) in the Label Switching Database (LSD). The SID index is configured on each node for the MPLS transport loopback. The SID index value is advertised using BGP-LU to the peer router, and the peer router uses the SID index to calculate the local label.

The default range is `16000-23999`.

ステップ 3 In the main pane, click **+Add SR-MPLS L3Out** within a pod.

ステップ 4 In the right **Properties** pane, provide a name for the SR-MPLS L3Out.

ステップ 5 (Optional) From the **QoS Policy** dropdown, select a QoS Policy you created for SR-MPLS traffic.

Select the QoS policy you created in Creating SR-MPLS QoS Policy, on page 303.

Otherwise, if you do not assign a custom QoS policy, the following default values are assigned:

- All incoming MPLS traffic on the border leaf switch is classified into QoS Level 3 (the default QoS level).
- The border leaf switch does the following:
  - Retains the original DSCP values for traffic coming from SR-MPLS without any remarking.
  - Forwards packets to the MPLS network with the original CoS value of the tenant traffic if the CoS preservation is enabled.
  - Forwards packets with the default MPLS EXP value (`0`) to the SR-MPLS network.
- In addition, the border leaf switch does not change the original DSCP values of the tenant traffic coming from the application server while forwarding to the SR network.

ステップ 6 From the **L3 Domain** dropdown, select the Layer 3 domain.

ステップ 7 Configure BGP settings.

You must provide BGP connectivity details for the BGP EVPN connection between the site's border leaf (BL) switches and the provider edge (PE) router.

a) Click **+Add BGP Connectivity**.

b) In the **Add BGP Connectivity** window, provide the details.

For the **MPLS BGP-EVPN Peer IPv4 Address** field, provide the loopback IP address of the DC-PE router, which is not necessarily the device connected directly to the border leaf.

For the **Remote AS Number**, enter a number that uniquely identifies the neighbor autonomous system of the DC-PE. the Autonomous System Number can be in 4-byte as plain format from 1 to 4294967295. Keep in mind, ACI supports only `asplain` format and not `asdot` or `asdot+` format AS numbers. For more information on ASN formats, see Explaining 4-Byte Autonomous System (AS) ASPLAIN and ASDOT Notation for Cisco IOS document.

For the **TTL** field, specify a number large enough to account for multiple hops between the border leaf and the DC-PE router, for example `10`. The allowed range `2-255` hops.

(Optional) Choose to enable the additional BGP options based on your deployment.

c) Click **Save** to save BGP settings.

d) Repeat this step to for any additional BGP connections.

Typically, you would be connecting to two DC-PE routers, so provide BGP peer information for both connections.

ステップ 8 Configure settings for border leaf switches and ports connected to the SR-MPLS network.

You need to provide information about the border leaf switches as well as the interface ports which connect to the SR-MPLS network.

a) Click **+Add Leaf** to add a leaf switch.

b) In the **Add Leaf** window, select the leaf switch from the **Leaf Name** dropdown.

c) Provide a valid segment ID (SID) offset.

When configuring the interface ports later in this section, you will be able to choose whether you want to enable segment routing. The SID index is configured on each node for the MPLS transport loopback. The SID index value is advertised using BGP-LU to the peer router, and the peer router uses the SID index to calculate the local label. If you plan to enable segment routing, you must specify the segment ID for this border leaf.

- The value must be within the SRGB range you configured earlier.
- The value must be the same for the selected leaf switch across all SR-MPLS L3Outs in the site.
- The same value cannot be used for more than one leaf across all sites.
- If you need to update the value, you must first delete it from all SR-MPLS L3Outs in the leaf and re-deploy the configuration. Then you can update it with the new value, followed by re-deploying the new configuration.

d) Provide the local **Router ID**.

Unique router identifier within the fabric.

e) Provide the **BGP EVPN Loopback** address.

The BGP-EVPN loopback is used for the BGP-EVPN control plane session. Use this field to configure the MP-BGP EVPN session between the EVPN loopbacks of the border leaf switch and the DC-PE to advertise the overlay prefixes. The MP-BGP EVPN sessions are established between the BP-EVPN loopback and the BGP-EVPN remote peer address (configured in the **MPLS BGP-EVPN Peer IPv4 Address** field in the **BGP Connectivity** step before).

While you can use a different IP address for the BGP-EVPN loopback and the MPLS transport loopback, we recommend that you use the same loopback for the BGP-EVPN and the MPLS transport loopback on the ACI border leaf switch.

f) Provide the **MPLS Transport Loopback** address.

The MPLS transport loopback is used to build the data plane session between the ACI border leaf switch and the DC-PE, where the MPLS transport loopback becomes the next-hop for the prefixes advertised from the border leaf switches to the DC-PE routers.

While you can use a different IP address for the BGP-EVPN loopback and the MPLS transport loopback, we recommend that you use the same loopback for the BGP-EVPN and the MPLS transport loopback on the ACI border leaf switch.

g) Click **Add Interface** to provide switch interface details.

From the **Interface Type** dropdown, select whether it is a typical interface or a port channel. If you choose to use a port channel interface, it must have been already created on the APIC.

Then provide the interface, its IP address, and MTU size. If you want to use a subinterface, provide the **VLAN ID** for the sub-interface, otherwise leave the VLAN ID field blank.

In the **BGP-Label Unicast Peer IPv4 Address** and **BGP-Label Unicast Remote AS Number**, specify the BGP-LU peer information of the next hop device, which is the device connected directly to the interface. The next hop address must be part of the subnet configured for the interface.

Choose whether you want to enable segment routing (SR) MPLS.

(Optional) Choose to enable the additional BGP options based on your deployment.

Finally, click the checkmark to the right of the **Interface Type** dropdown to save interface port information.

h) Repeat the previous sub-step for all interfaces on the switch that connect to the MPLS network.

i) Click **Save** to save the leaf switch information.

ステップ 9 Repeat the previous step for all leaf switches connected to MPLS networks.

What to do next

After you have enabled and configured MPLS connectivity, you can create and manage Tenants, route maps, and schemas as described in the *Multi-SiteConfiguration Guide, Release 3.0(x)*.

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。

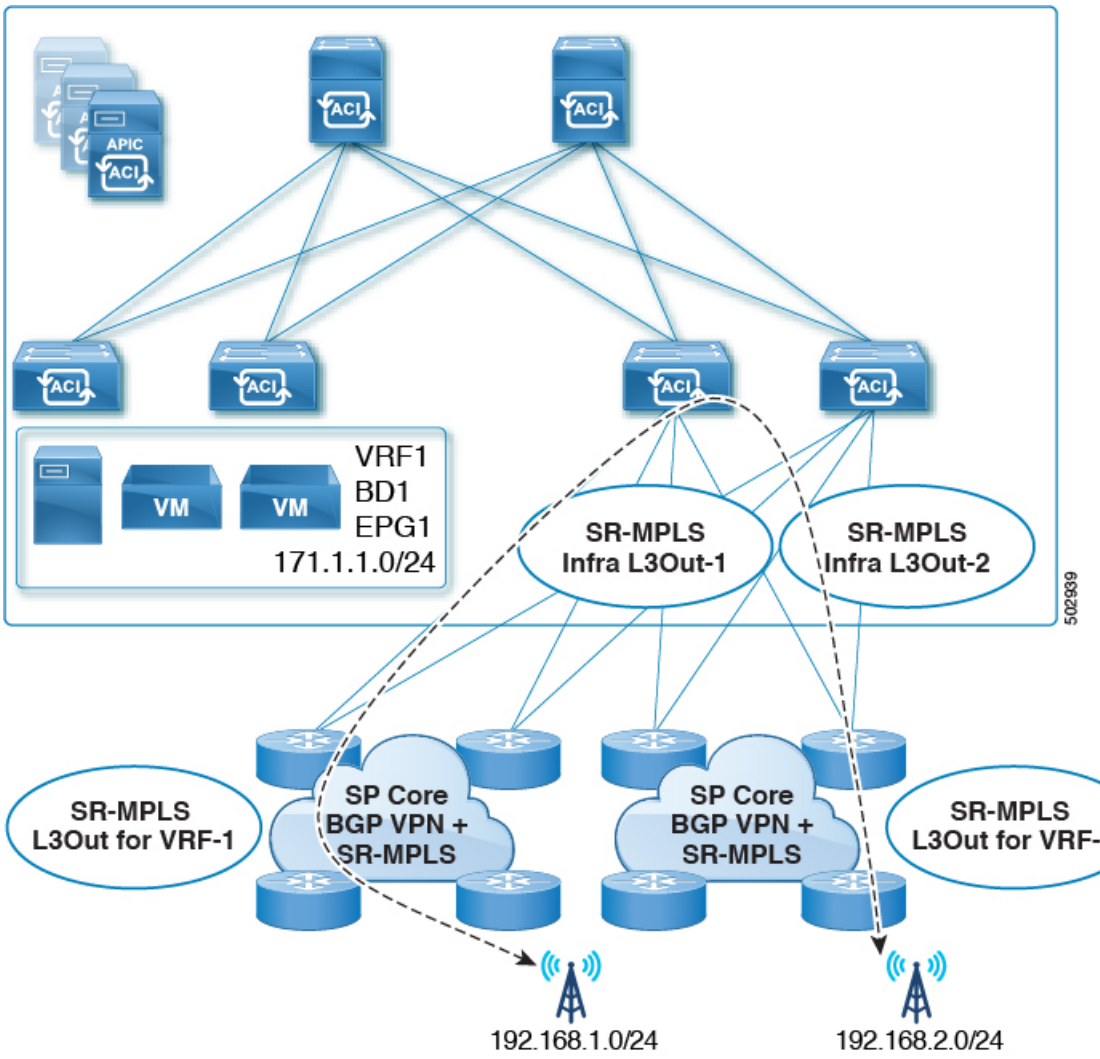
- Day-0 操作の章で説明されているとおり、QoS ポリシーを含む SR-MPLS Infra L3Outs を作成し、設定します。
- ファブリックの 2 つの EPG 間のトラフィックが SR-MPLS ネットワークを通過する必要がある場合:
  - 各 EPG とローカル SR-MPLS L3Out で定義された外部EPGの間に、コントラクトを割り当てる必要があります。
  - 両方の EPG が同じACI ファブリックの一部であるが、SR-MPLS ネットワークによって分離されている場合（たとえば、マルチポッドまたはリモートリーフの場合)、EPG が異なる VRF に属していること、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、それらの間で直接設定されたコントラクトがあっては**なりません**。

    EPGが異なるサイトにある場合、各EPGは単一サイトにのみ展開する必要があることにご留意ください。サイト間の EPG の拡張は、SR-MPLS L3Outs を使用するときはサポートされていません。
- 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` ～ `32` を `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。
- 移行ルーティングがサポートされますが、一部の制約があります。

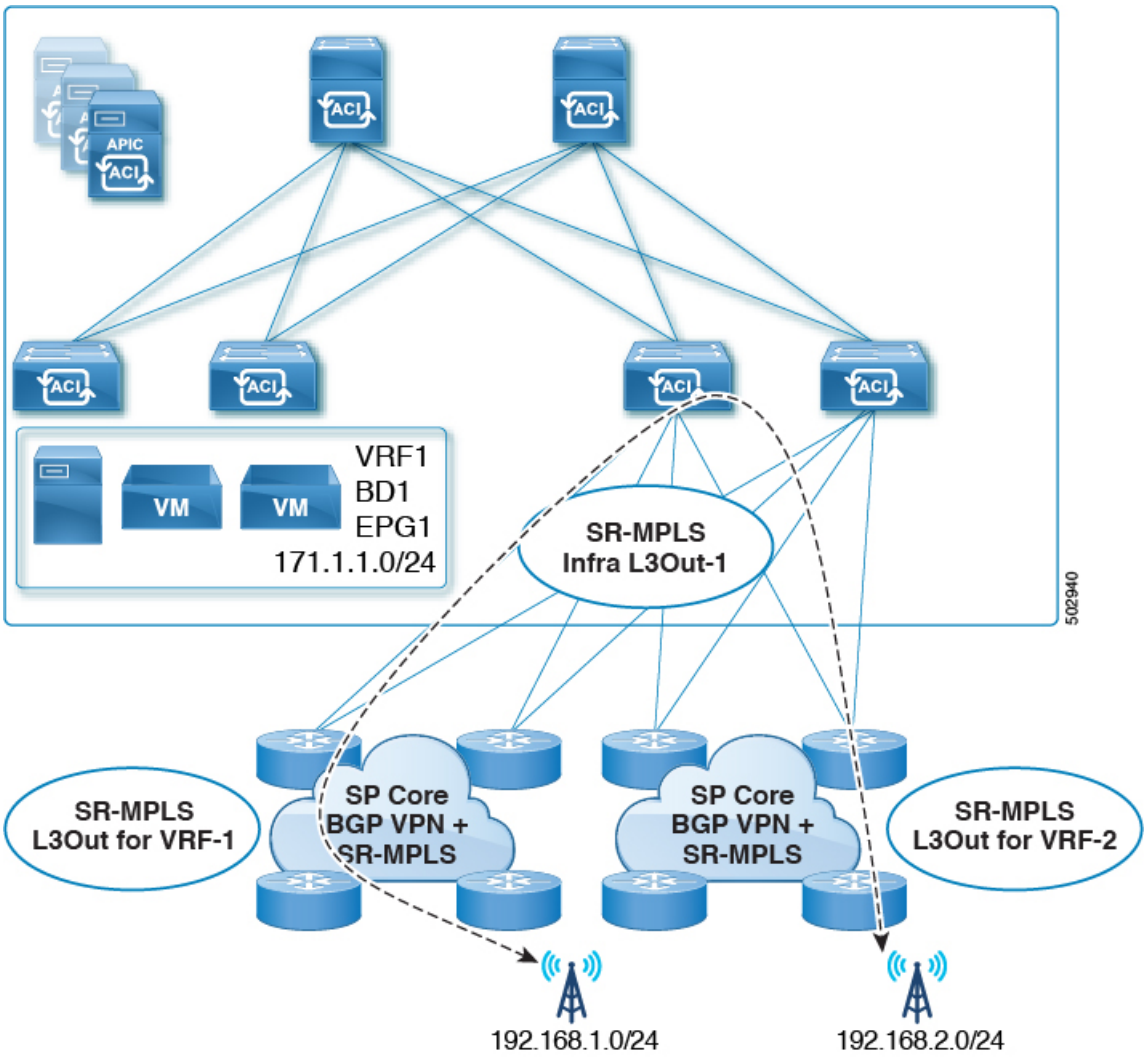
- **同じ VRF を使用する** 2 つの SR-MPLS ネットワーク間の移行ルーティングはサポートされていません。次の図は、サポートされていない設定の例を示します。

図 *39*：単一の *VRF* を使用するサポートされていない移行ルーティング設定



- **異なる VRF を使用する** 2 つの SR-MPLS ネットワーク間の移行ルーティングはサポートされています。次の図は、サポートされている設定の例を示します。

図 *40* : 異なる *VRF* を使用するサポートされている移行ルーティング設定



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。

MPLS ネットワークに接続されているサイトがない場合は、このセクションをスキップできます。

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

ステップ 2 **[メイン メニュー (Main menu)]** で、**[アプリケーション管理 (Application Management)]** > **[ポリシー (Policies)]** を選択します。

ステップ 3 メイン ペインで、**[ポリシーの追加 (Add Policy)]** > **[ルート マップ ポリシーの作成 (Create Route Map Policy)]** を選択します。

ステップ 4 **[ルート マップ ポリシーの追加 (Add Route Map Policy)]** 画面で、テナントを選択し、ポリシーの名前を指定します。

ステップ 5 ルート マップ エントリを追加するには、**[ルート マップ エントリの順序 (Route-Map Entry Order)]**の下の **[エントリの追加 (add Entry)]** をクリックします。

a) **[コンテキストの順序 (Contrext Order)]** と **[コンテキスト アクション(Context Action)]**を指定します。

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。

[アクション(Action)] は、一致が検出された場合に実行するアクション(`許可 (permit)` または `拒否 (deny)`)を定義します。

b) 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、ルート `0 ～ 32` を集約するよう選択できます。

c) 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。

d) **[+ アクションの追加 (+Add Action)]** 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
- 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

アクションを設定したら、チェックマーク アイコンをクリックしてアクションを保存します。

e) (オプション) 前のサブステップを繰り返して、同じコンテキスト エントリ内で複数の一致基準とアクションを指定できます。

f) **[保存 (save)]** をクリックして、コンテキスト エントリを保存します。

ステップ 6 (オプション) 同じルート ポリシーに複数のエントリを追加する場合は、前の手順を繰り返します。

ステップ 7 **[保存 (Save)]** をクリックして、ルート マップ ポリシーを保存します。

SR-MPLS 設定のテンプレートの有効化

MPLS を介して接続されたサイトに展開する際に固有のテンプレート構成設定がいくつかあります。テナントの SR MPLS を有効にすると、MPLS サイトで使用できない特定の設定を制限およびフィルタ処理し、そのようなサイトでのみ使用可能な追加の設定を行うことができます。

MPLS 固有の設定を更新する前に、テンプレートのテナント プロパティで **SR-MPLS** ノブを有効にする必要があります。

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

ステップ 2 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。

ステップ 3 新規作成するか、または SR-MPLS テナントを設定する既存のスキーマを選択します。

ステップ 4 テナントを選択します。

新しいスキーマを作成した場合は、通常と同じようにテナントを選択します。それ以外の場合は、左側のサイドバーで既存のテンプレートをクリックします。

ステップ 5 右側のサイドバーの **テンプレート** のプロパティで、 **SR MPLS** ノブを有効にします。

VRF および SR-MPLS L3Out の作成

このセクションでは、MPLS ネットワークで区切られるアプリケーション EPG 間の通信を設定するために使用する VRF、テナント SR-MPLS L3Out、および External EPG を作成する方法を説明します。

始める前に

次のことが必要です。

- SR-MPLS 設定のテンプレートの有効化 （312 ページ） で説明しているように、テンプレートを作成して、そのテナントで SR-MPLS を有効にしていること。

ステップ 1 テンプレートを選択します。

ステップ 2 VRF を作成します。

a) メインペインで、**VRF** エリアまで下方にスクロールして、+ 記号をクリックして VRF を追加します。

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-MPLS L3Out を作成します。

a) メイン ペインで、**SR-MPLS L3Out** エリアまで下方にスクロールして、+ 記号をクリックして L3Out を追加します。

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。

ステップ 4 外部 EPG を作成します。

a) メイン ペインで、**[外部 EPG (External EPG)]** エリアまで下方にスクロールし、+ 記号をクリックして外部 EPG を追加します。

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。

サイトローカル VRF 設定の構成

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。

始める前に

次のことが必要です。

- SR-MPLS 設定のテンプレートの有効化（312 ページ） で説明しているように、テンプレートを作成して、そのテナントで SR-MPLS を有効にしていること。
- VRF および SR-MPLS L3Out の作成（312 ページ） で説明しているように、VRF と SR-MPLS L3Out を作成していること。
- MPLS サイトにテンプレートを追加していること。

ステップ 1 テンプレートを含むスキーマを選択します。

ステップ 2 スキーマ ビューの左サイドバーの **[サイト (Sites)]** の下で、サイトローカル プロパティを編集するためにテンプレートを選択します。

ステップ 3 メインペインで、**[VRF]** エリアまで下にスクロールし、VRF を選択します。

ステップ 4 右プロパティ サイドバーで、**[+ BGP ルート ターゲット アドレスを追加 (+Add BGP Route Target Address)]** をクリックします。

ステップ 5 BGP 設定を構成します。

a) **[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。

b) **[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。

c) **[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。

d) **[保存 (Save)]** をクリックして、ルート情報を保存します。

ステップ 6 (オプション) 上記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。

サイトローカル SR-MPLS L3Out 設定の構成

通常の外部 EPG のサイトローカル L3Out プロパティを設定する場合と同じように、MPLS で接続されているサイトに展開される外部 EPG の SR-MPLS L3Out の詳細を設定する必要があります。

始める前に

次のことが必要です。

- SR-MPLS 設定のテンプレートの有効化 （312 ページ） で説明しているように、テンプレートを作成して、そのテナントで SR-MPLS を有効にしていること。
- VRF および SR-MPLS L3Out の作成 （312 ページ） で説明しているように、VRF と SR-MPLS L3Out を作成していること。
- サイトローカル VRF 設定の構成 （313 ページ） で説明しているように、VRF のサイトローカル プロパティを設定していること。
- MPLS サイトにテンプレートを追加していること。

ステップ 1 テンプレートを含むスキーマを選択します。

ステップ 2 スキーマ ビューの左サイドバーの **[サイト (Sites)]** の下で、サイトローカル プロパティを編集するためにテンプレートを選択します。

ステップ 3 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。

ステップ 4 右のプロパティ サイドバーで、**[+ SR-MPLS ロケーションの追加 (+Add SR-MPLS Location)]** をクリックします。

ステップ 5 SR-MPLS のロケーションの設定を構成します。

a) **[SR-MPLS のロケーション (SR-MPLS Location)]** ドロップダウンで、そのサイトのインフラを設定する際に作成したインフラ SR-MPLS L3Out を選択します。

b) **[外部 EPG (External EPGs)]** セクションで、ドロップダウンから外部 EPG を選択し、チェックlマークのアイコンをクリックして追加します。

外部 EPG は複数追加できます。

c) **[ルート マップ ポリシー (Route Map Policy)]** セクションの下で、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てから、チェックマークのアイコンをクリックして追加します。

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。

d) **[保存 (Save)]** をクリックして、ロケーションを MPLS L3Out に追加します。

ステップ 6 (オプション) 前のステップを繰り返して、その他の SR-MPLS ロケーションを SR-MPLS L3Out に追加します。

MPLS ネットワークにより区切られた EPG 間の通信

通常、2 つの EPG 間の通信を確立するには、1 つの EPG をプロバイダに、もう1つをコンシューマとし、両方の EPG に同じコントラクトを割り当てるだけです。

しかし、2 つの EPG が MPLS ネットワークで区切られている場合には、トラフィックはそれぞれの EPG の MPLS L3Out を通らなければならないので、コントラクトは、それぞれの EPG と、その MPLS L3Out の間に確立します。この動作は、EPG が異なるファブリックに展開されている場合でも、マルチポッドまたはリモートリーフの場合のように、同じサイトに展開されていて、SR-MPLS ネットワークで区切られている場合でも同じです。

始める前に

次のことが必要です。

- MPLS ネットワークに接続されている 1 つ以上のサイトを Orchestrator に追加していること。
- インフラ MPLS の設定を、「ゼロデイ オペレーション」の章で説明しているように構成していること。
- SR-MPLS 設定のテンプレートの有効化 （312 ページ） で説明されているとおり、スキーマを作成し、テナントを追加し、SR-MPLS に対してテナントを有効にしていること。

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

ステップ 2 通常のように、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。

ステップ 3 2 つの独立した外部 EPG を作成します。

これらの EPG は、特定の導入シナリオに応じて、同じテンプレートに含めることも、異なるテンプレートに含めることもできます。

たとえば、 `mpls-extepg-1` および `mpls-extepg-2` とします。

ステップ 4 2 つの個別のテナント 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。

各テナント SR-MPLS L3Out について、サイトローカル VRF 設定の構成 （313 ページ） および サイトローカル SR-MPLS L3Out 設定の構成 （314 ページ） の説明に従って、VRF、ルート マップ ポリシー、および外部 EPG を設定します。

ステップ 5 ステップ 2 で作成した、2 つのアプリケーション EPG の間のトラフィックを許可するために使用するコントラクトを作成します。

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。

ステップ 6 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-l3out-1` の間、そして `epg2` とその `mpls-l3out-2` の間です。

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。

a) `epg1` にタイプ `consumer` でコントラクトを割り当てます。
b) `mpls-l3out-1` にタイプ `consumer` でコントラクトを割り当てます。
c) `epg2` にタイプ `consumer` でコントラクトを割り当てます。
d) `mpls-l3out-1` にタイプ `consumer` でコントラクトを割り当てます。

設定の展開

1 つの例外を除いて、構成テンプレートを通常どおり MPLS サイトに展開できます。MPLS サイトと別のサイトの間でオブジェクトとポリシーを拡張することはできないため、テンプレートを展開するときに選択できるサイトは 1 つだけです。

ステップ 1 テンプレートを展開するサイトを追加します。

a) [**スキーマ (Schema)**] 表示の左側のサイドバーで、[**サイト (Sites)**] の下の + アイコンをクリックします。
b) [**サイトの追加 (Add Sites)**] ウィンドウで、テンプレートを展開するサイトを選択します。

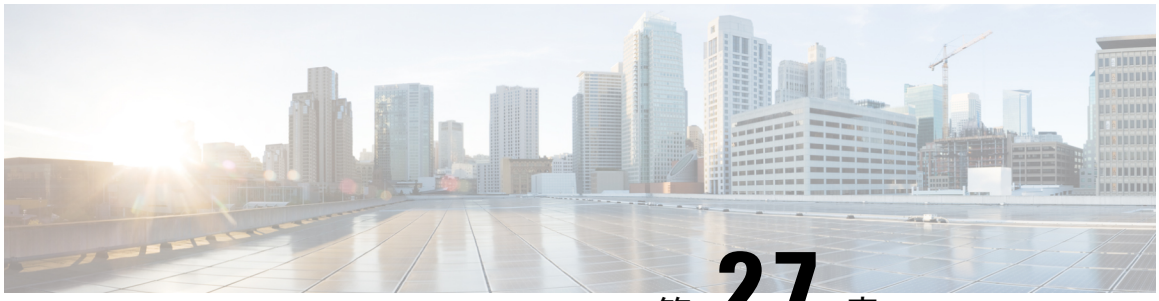
テンプレートが MPLS 対応の場合、単一サイトのみを選択できます。

c) [**テンプレートへの割り当て (Assign to Template)**] ドロップダウンからスキーマを作成した 1 つ以上のテンプレートを選択します。
d) [**保存 (Save)**] をクリックして、サイトを追加します。

ステップ 2 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。



第 27 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 （325 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 （331 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契約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 が契約 `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 が契約 `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、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、Multi-Site 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。

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 （322 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。

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 （322 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 （322 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 （323 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。

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

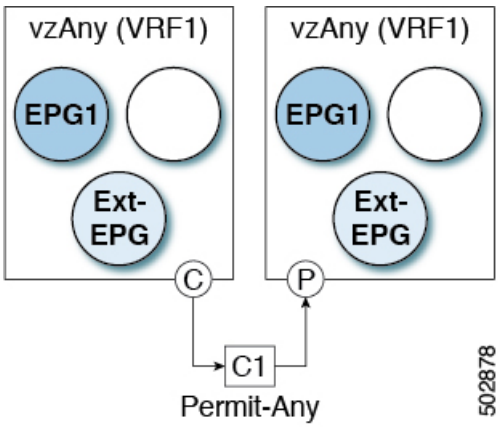
a) 外部 EPG を作成します。

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のみ使用します。これは、*VRF* 非強制 オプションと同等です。

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。

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 （322 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 （323 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 （324 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。

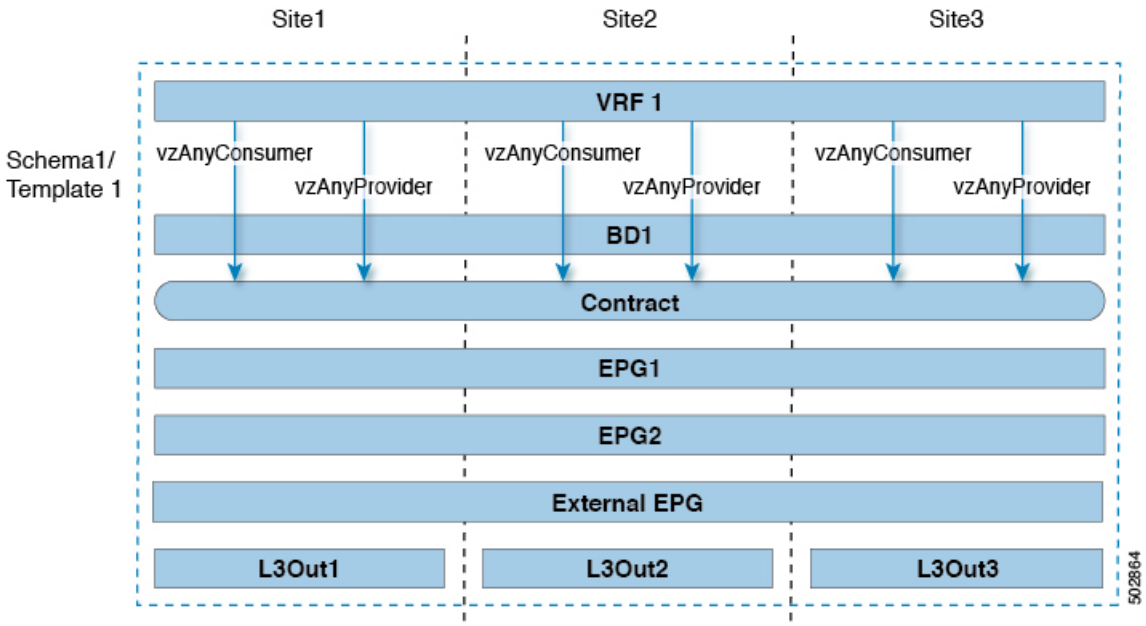
拡張された EPG

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 *42 :*



サイトローカル EPG

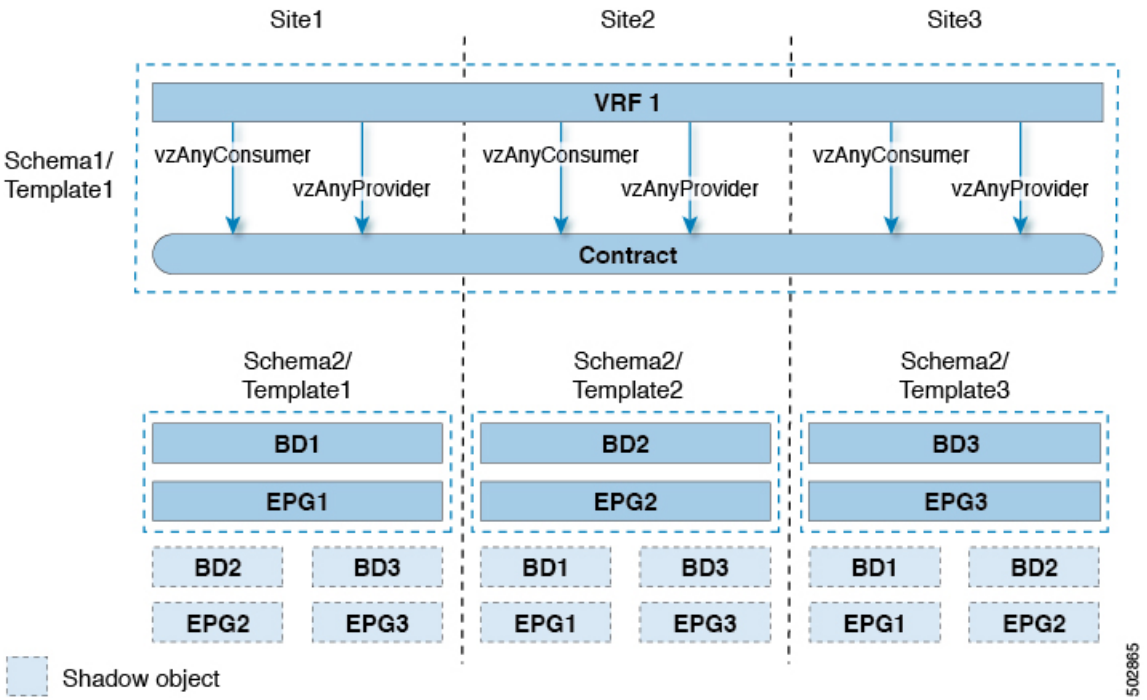
以下の例は、EPG または 外部 EPG 間の VRF 内通信を示しています。この場合、どの EPG も拡張されていませんが、vzAnyが「permit-any」コントラクトを消費して提供するため、相互に自由に通信できます。

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 *43 :*



サイト ローカルおよび拡張 EPG の組み合わせ

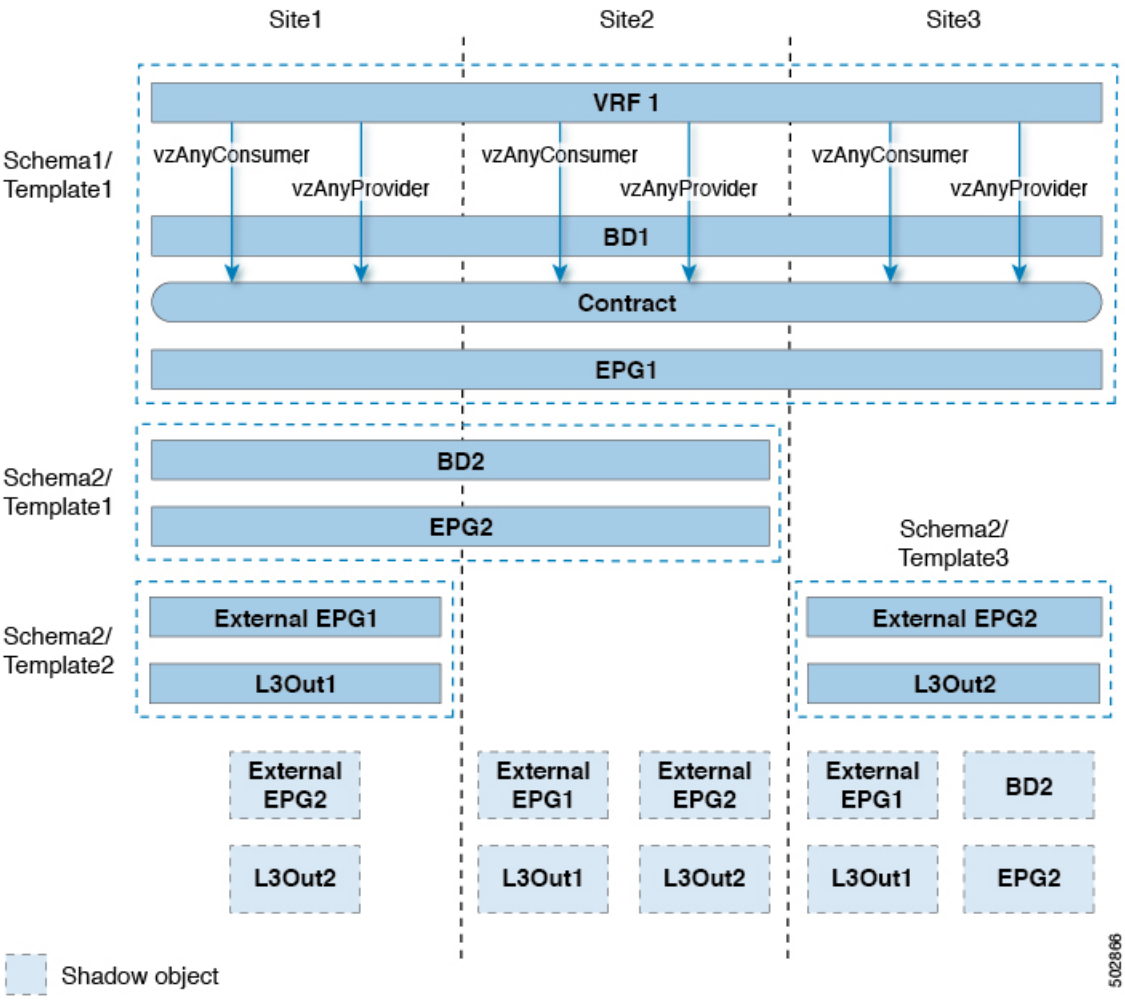
次の例は、EPG または 外部 EPG の間の VRF 内通信を示しています。一部の EPG は拡張されていますが、他のものは単一のサイトにのみ展開されます。それでも、すべての EPG は相互に自由に通信できます。vzAny は「すべて許可」のコントラクトを消費し、提供するからです。

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 *44 :*



VRF 内のサイト間 L3Out

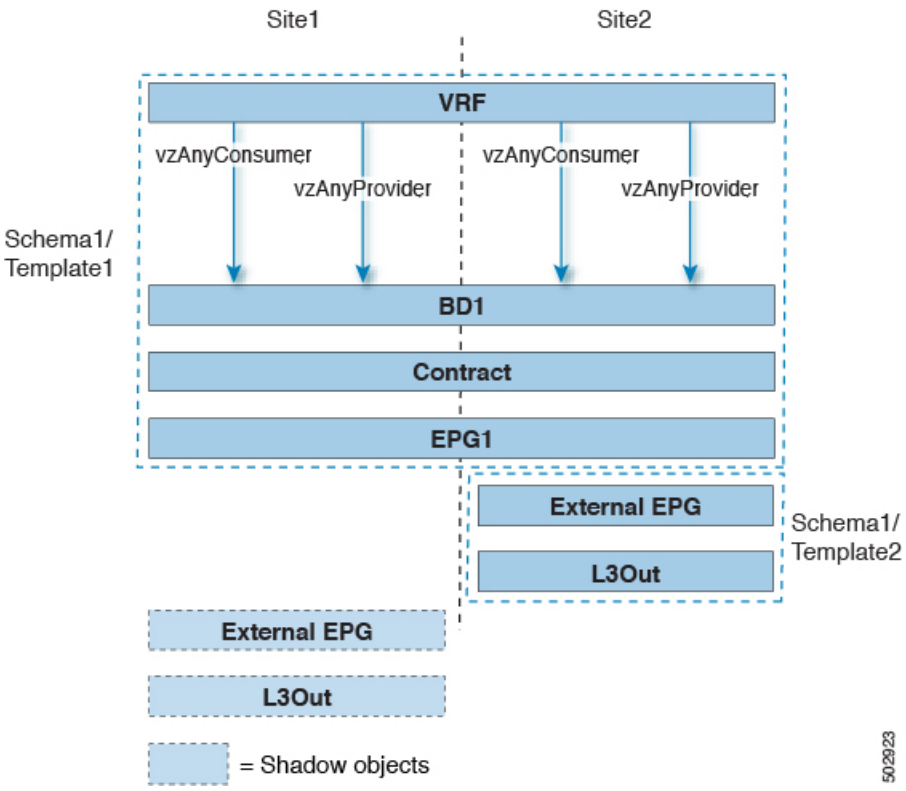
このユース ケースでは、1 つの vzAny VRF 内の複数の EPG 用に、サイト間 L3Out を設定できます。L3Out の外部 EPG が同じ VRF 内に存在する場合には、外部 EPG にプロバイダを明示的に追加する必要はありません。

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 （201 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 *45 :*



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。

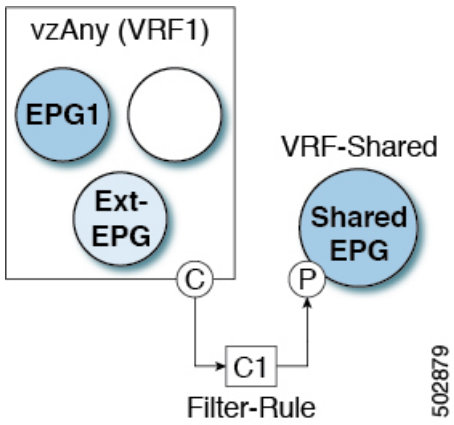
（注） VRF を vzAny プロバイダーにすることはできません。

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 *46 :*



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。

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 （322 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 （323 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 （324 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

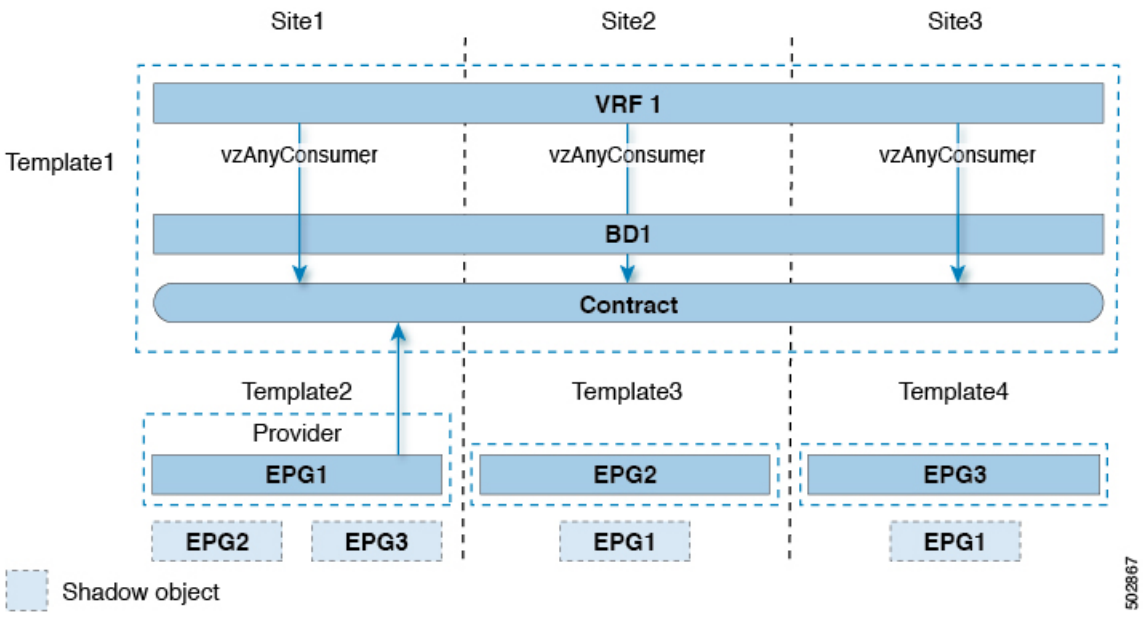
次の例は、単一のプロバイダ EPG (たとえば、共有サービス) と、同じ VRF 内の他のすべての EPG 間のサービスを消費する VRF 間の通信を示しています。

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 *47*:



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 *48 :*