



スキーマ

- [Schema Design Considerations, on page 1](#)
- [設定の同時更新 \(6 ページ\)](#)
- [Creating Schemas and Templates, on page 8](#)
- [テンプレート オブジェクトの一括更新 \(27 ページ\)](#)
- [サイトへのテンプレートの割り当て \(30 ページ\)](#)
- [テンプレートのバージョンニング \(31 ページ\)](#)
- [テンプレートのレビューと承認 \(36 ページ\)](#)
- [テンプレートの展開 \(40 ページ\)](#)
- [テンプレートの展開解除 \(44 ページ\)](#)
- [サイトからのテンプレートの関連付け解除 \(45 ページ\)](#)
- [設定のばらつき \(46 ページ\)](#)
- [スキーマの複製 \(51 ページ\)](#)
- [テンプレートの複製 \(53 ページ\)](#)
- [テンプレート間でのオブジェクトの移行 \(54 ページ\)](#)
- [現在展開されている設定の表示 \(56 ページ\)](#)
- [スキーマの概要と展開ビジュアライザ \(57 ページ\)](#)
- [シャドウ オブジェクト \(60 ページ\)](#)

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。

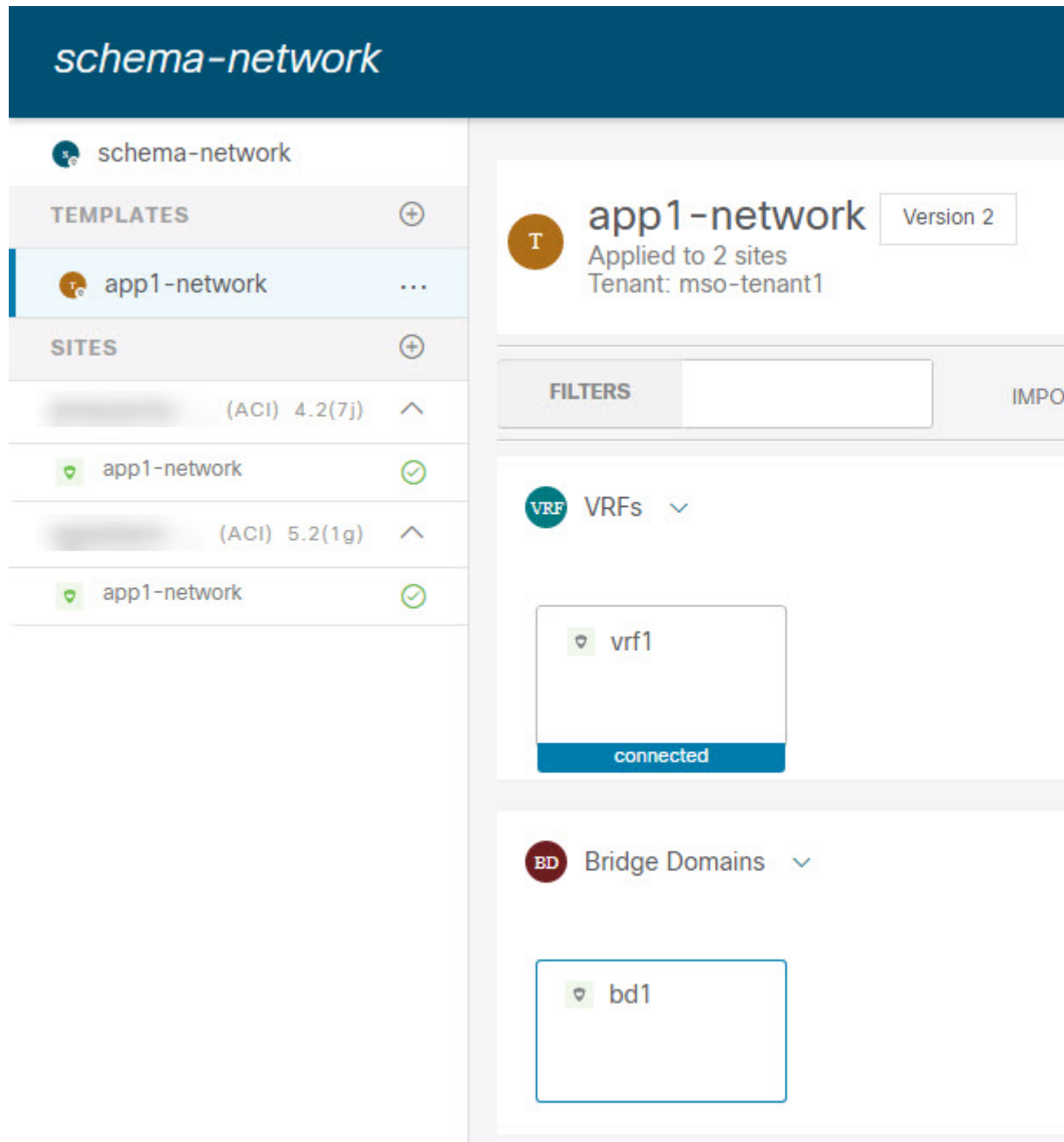
ネットワーク分離での複数スキーマ

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クングテンプレート設定を示しています。

図 1: 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ク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 2: ポリシー スキーマ

The screenshot displays the configuration page for a policy schema named 'schema-policy'. The interface is divided into a left sidebar and a main content area.

Left Sidebar:

- schema-policy (selected)
- TEMPLATES (+)
 - app1-policy
 - app2-policy
- SITES (+)
 - (ACI) 4.2(7j) ^
 - app1-policy ✓
 - (ACI) 5.2(1g) ^
 - app1-policy ... ✓
 - app2-policy ✓

Main Content Area:

- app1-policy (Tenant: mso-tenant1)
- FILTERS
- Application Profile app1 (AP)
- EPGs (EPG)
 - app1-db
 - app1-web
- Contracts (C)
 - app1-contrast (consumed)

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クキミ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

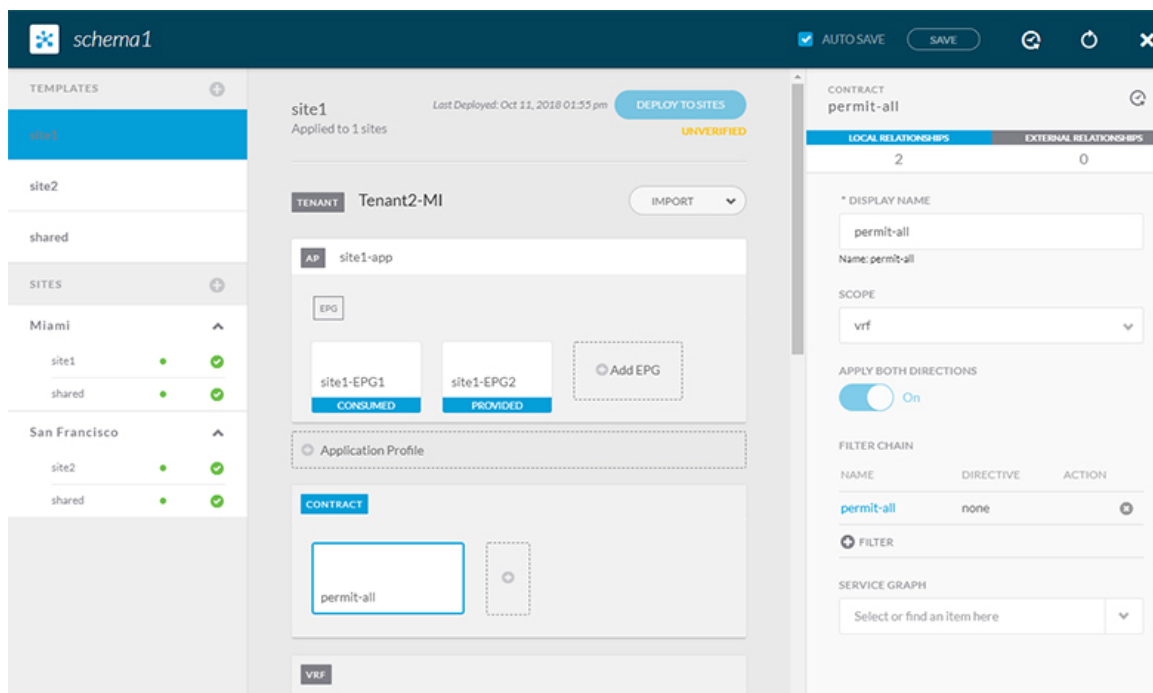
照を含むオブジェクトは、上のネットワークスキーマの図に示すように、リボンのアイコンでも示されます。

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 3: 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": "Templatel",
      "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": "Templatel",
      "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](#).

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.

- From the left navigation pane, choose **Application Management > Schemas**.
- On the Schemas page, click **Add Schema**.
- 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.

- In the left sidebar under **Templates**, click the + sign to add a new template.
- 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.

- In the right sidebar, specify the **Display Name**.
- (Optional) Provide a **Description**.
- 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](#).

- 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](#).

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.

- In the left pane, click the + icon next to Sites
- In the **Add Sites** window, check the checkbox next to the sites where you want to deploy the template.
- 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.

- 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 \(8 ページ\)](#) 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](#) 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](#) 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 \(8 ページ\)](#) 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 \(11 ページ\)](#) 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。

- 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。

- 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。
- (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。

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

- (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。
- (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かかわらず行われます。

- (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](#) を参照してください。

- (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せん。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ダプ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](#) 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 \(15 ページ\)](#) 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

次のものがが必要です。

- [ブリッジドメインの設定 \(12 ページ\)](#) 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](#) 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 \(8 ページ\)](#) 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。
- 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。
 - 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。
 - (任意) **[説明 (Description)]** を入力します。
- ステップ 3** EPG を作成します。
- 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。
 - 右側のペインで、EPG の **[表示名 (Display Name)]** を入力します。
 - (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 \(22 ページ\)](#) 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：
- [+ コントラクト (+ Contract)]** をクリックします。
 - [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。
 - [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 EPG 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](#)

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](#)

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 \(19 ページ\)](#) 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ものみ展開されます。

始める前に

次のものがが必要です。

- [アプリケーションプロファイルと EPG の設定 \(16 ページ\)](#) 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すべての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すべてのポートから送出されます。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](#).

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 \(8 ページ\)](#) 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 \(11 ページ\)](#) 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](#)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。

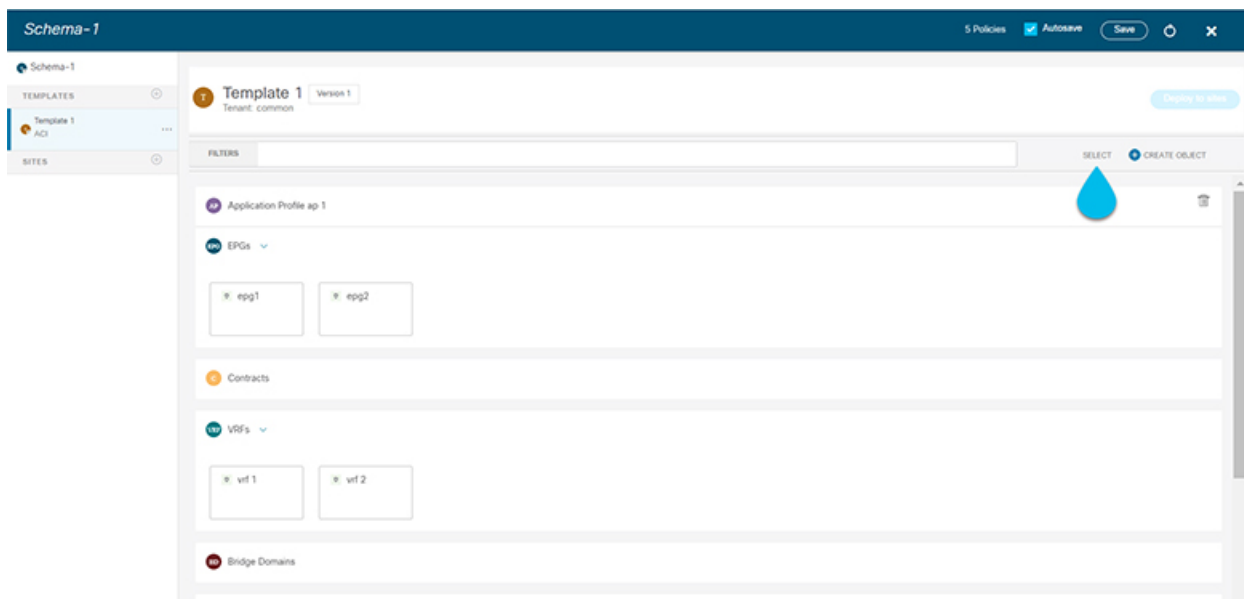
選択したオブジェクトにすでに別のプロパティ値が構成されている場合、更新により、それらのプロパティが指定した値で上書きされます。この機能により、オンプレミスのテンプレートレベルのオブジェクトプロパティを更新できます。サイトローカルプロパティとクラウドプロパティの更新はサポートされていません。



(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。

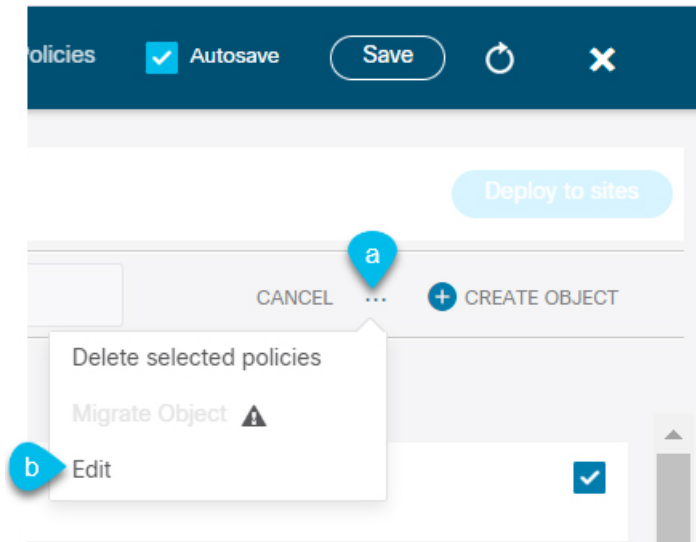
ステップ 2 右上のペインから、「選択」を選択します。同じタイプのオブジェクトを複数選択できます。



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。

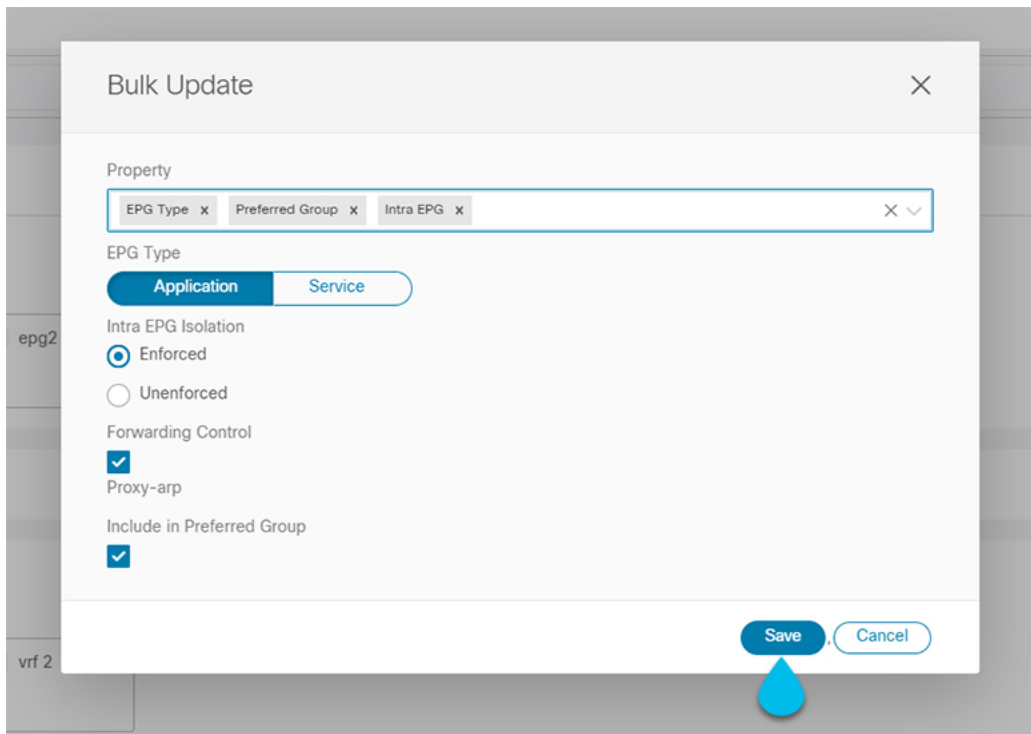


ステップ 4 [編集 (Edit)] を選択すると、ポップアップが表示されます。選択したオブジェクトのプロパティのサブセットが表示されます。

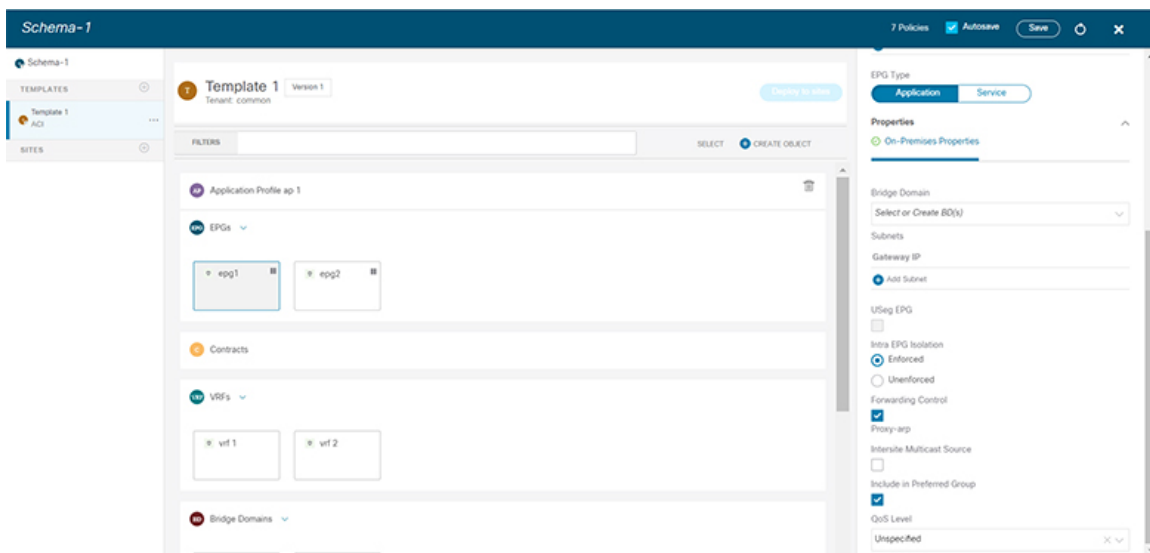
選択したオブジェクトのタイプに基づいて、次のプロパティを更新できます。

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グディング、IPv6 不明なマルチキャストフラグディング、複数宛先フラグディング、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ンング

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。

タグging 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。

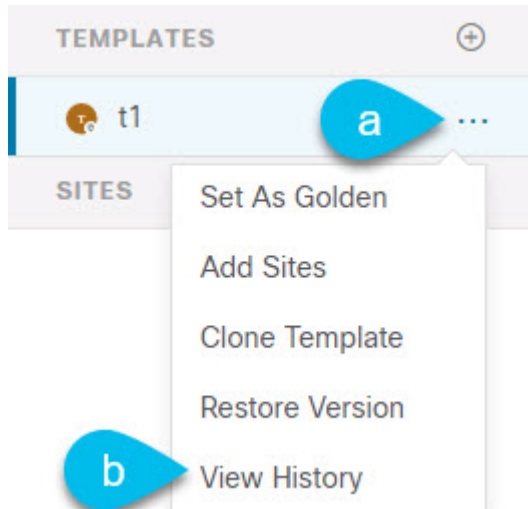
テンプレートがすでにタグ付けされている場合、オプションは [ゴールデンの削除 (Remove Golden)] に変更され、現在のバージョンからタグを削除できます。

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。

The screenshot shows the 'Version History' window for a schema. At the top, it displays 'General Information' with 'Schema versioning', 'Template t1', and 'Tenant mso-tenant1'. Below this is a 'Versions' section with a timeline of versions 1 through 4. Version 1 is marked as a 'Golden Version' (indicated by a blue circle 'a' and a checkbox). Version 2 is marked as a 'Deployed Version' (indicated by a blue circle 'b' and a checkbox). Version 4 is marked as the 'Current' version (indicated by a purple circle 'c'). A blue circle 'd' points to version 2 in the comparison panel below. The comparison panels show the JSON configuration for 'Version 2' (Selected) and 'Version 4' (Current). Version 2 has 1 policy and 0 sites, while Version 4 has 2 policies and 1 site. The JSON for Version 4 includes a 'siteDelta' object and a 'template' object with various configuration parameters.

- 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 \(32 ページ\)](#) 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（36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、[変更制御ワークフロー (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 37.

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 \(37 ページ\)](#) 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 \(37 ページ\)](#) 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に関連付ける必要もあります。

- 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。
- ユーザーが管理するテナントを選択します。
- 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。
- 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 \(37 ページ\)](#) 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 \(37 ページ\)](#) 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 \(38 ページ\)](#) 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ーが変更を行い、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 \(32 ページ\)](#) 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 \(56 ページ\)](#) 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 \(36 ページ\)](#) 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。

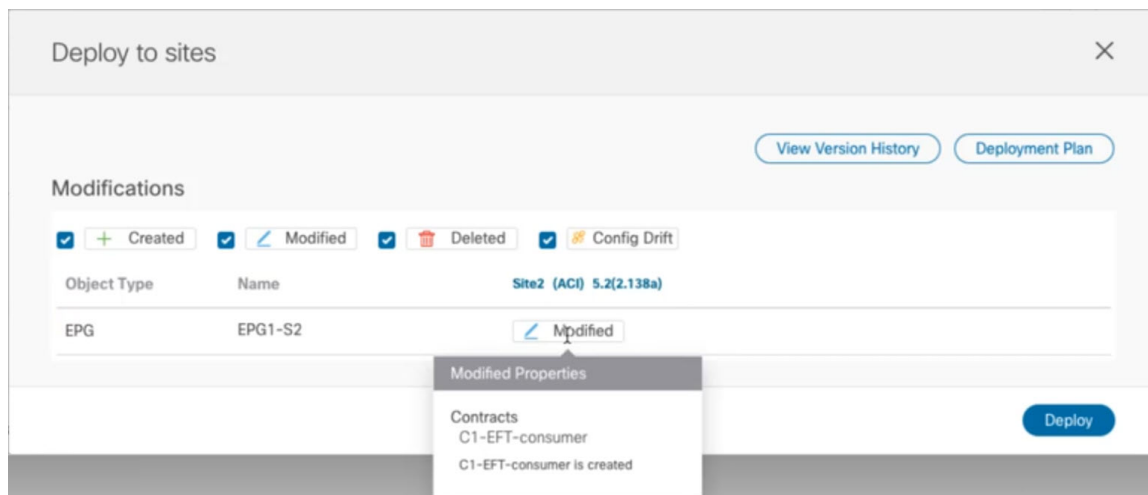
ステップ 3 テンプレート編集ビューの右上で、[展開 (Deploy)] をクリックします。

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 \(32 ページ\)](#) 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。

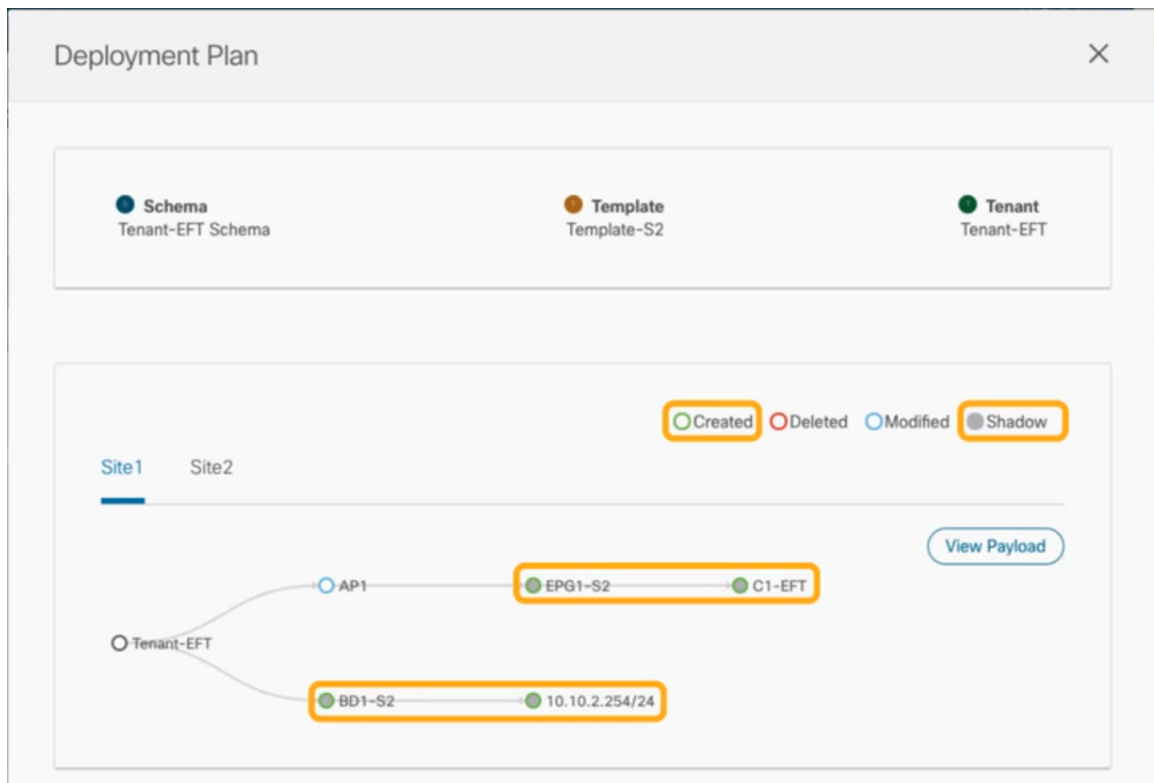
(注) テンプレートをデプロイする前に、このステップで説明されているように、デプロイメントプランを使用して変更を確認することをお勧めします。構成変更の視覚的な表現は、意図しない構成変更の展開による潜在的なエラーを減らすのに役立ちます。

- 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。。

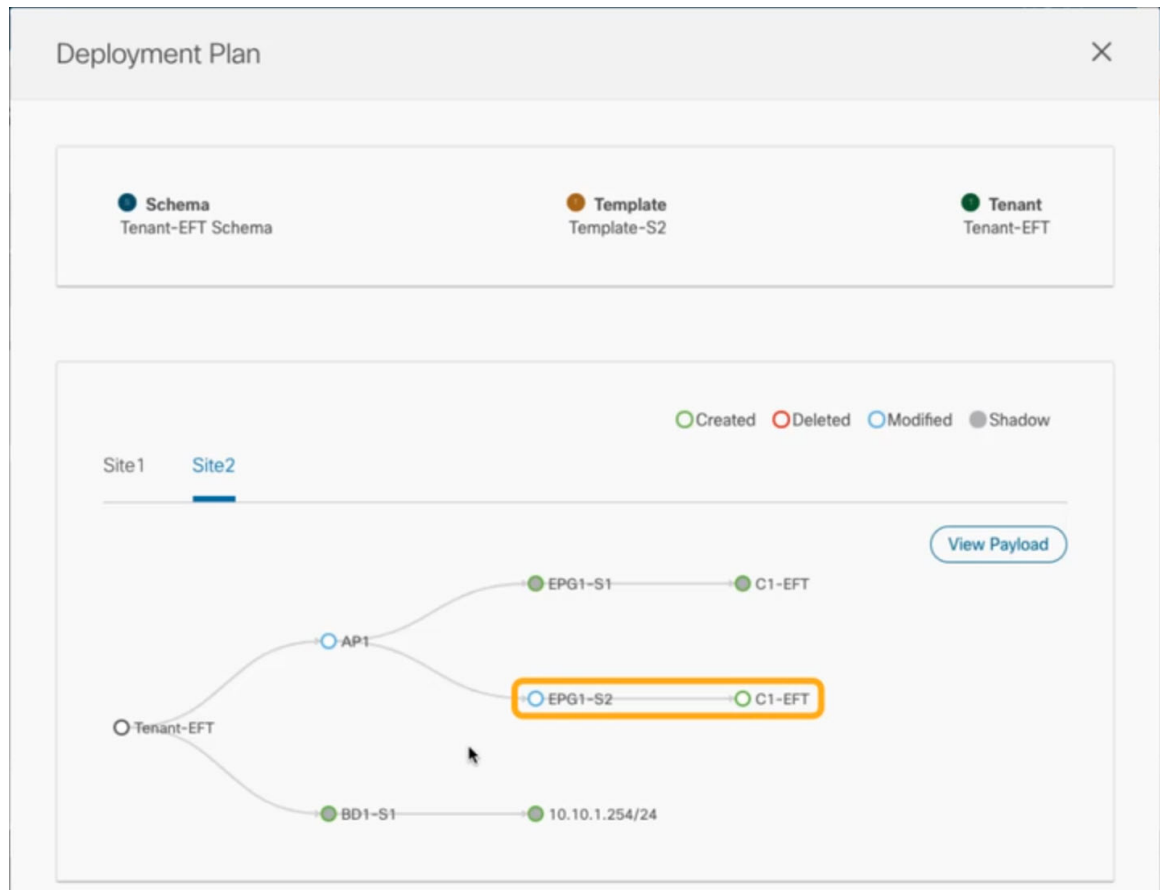
- 最初にリストされたサイトで変更を確認します。

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。

```

<polUni>
  <fvTenant name="Tenant-EFT" annotation="orchestrator:misc">
    <fvAp name="AP1" annotation="orchestrator:misc-shadow:no">
      <fvAEPg name="EPG1-S2" isAttrBasedEPg="no" pcEnfPref="unenforced" fwdCtrl="" prefGrMemb="exclude" hasMcastSource="no"
        prio="unspecified" annotation="orchestrator:misc-shadow:yes">
        <fvRsBd tnFvBDName="BD1-S2"/>
        <fvRsCons tnVzBrCPName="C1-EFT" annotation="orchestrator:misc">
        </fvRsCons>
        <fvSiteAssociated sitelid="1" name="misc-local">
        </fvSiteAssociated>
      </fvAEPg>
    </fvAp>
    <fvBD name="BD1-S2" arpFlood="yes" intersiteBumTrafficAllow="no" OptimizeWanBandwidth="no" unkMacUcastAct="proxy"
      intersiteL2Stretch="no" mcastAllow="no" hostBasedRouting="no" vmac="not-applicable" mac="00:22:BD:F8:19:FF"
      unkMcastAct="flood" v6unkMcastAct="flood" multiDstPktAct="bd-flood" unicastRoute="yes" annotation="orchestrator:misc-
      shadow:yes">
      <fvRsCtx tnFvCtxName="VRF1"/>
      <fvSubnet ip="10.10.2.254/24" scope="private" descr="" ctrl="no-default-gateway" virtual="no" preferred="no"
        annotation="orchestrator:misc-shadow:no">
      </fvSubnet>
      <fvSiteAssociated sitelid="1" name="misc-local">
      </fvSiteAssociated>
    </fvBD>
  </fvTenant>
</polUni>

```

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

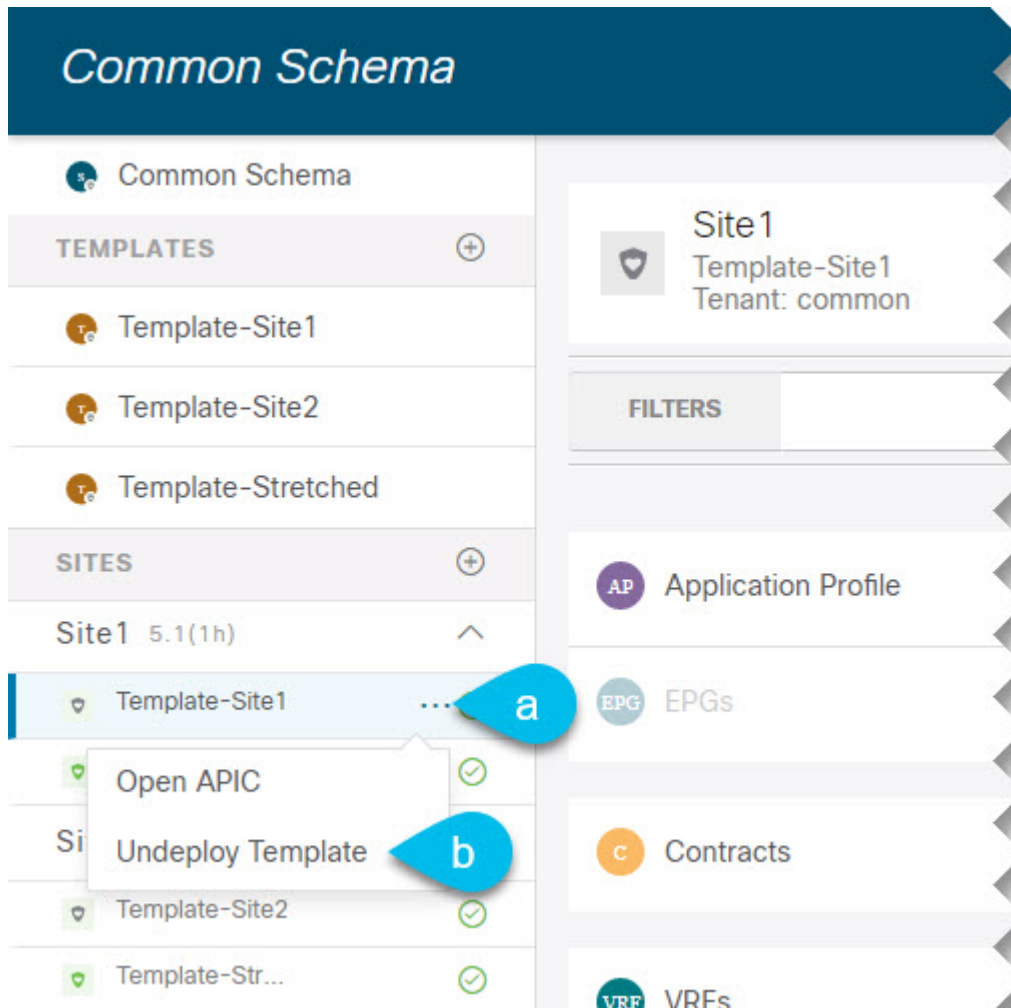
- テンプレートを最後に展開してから、テンプレートに変更を加えていないことを確認します。

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。

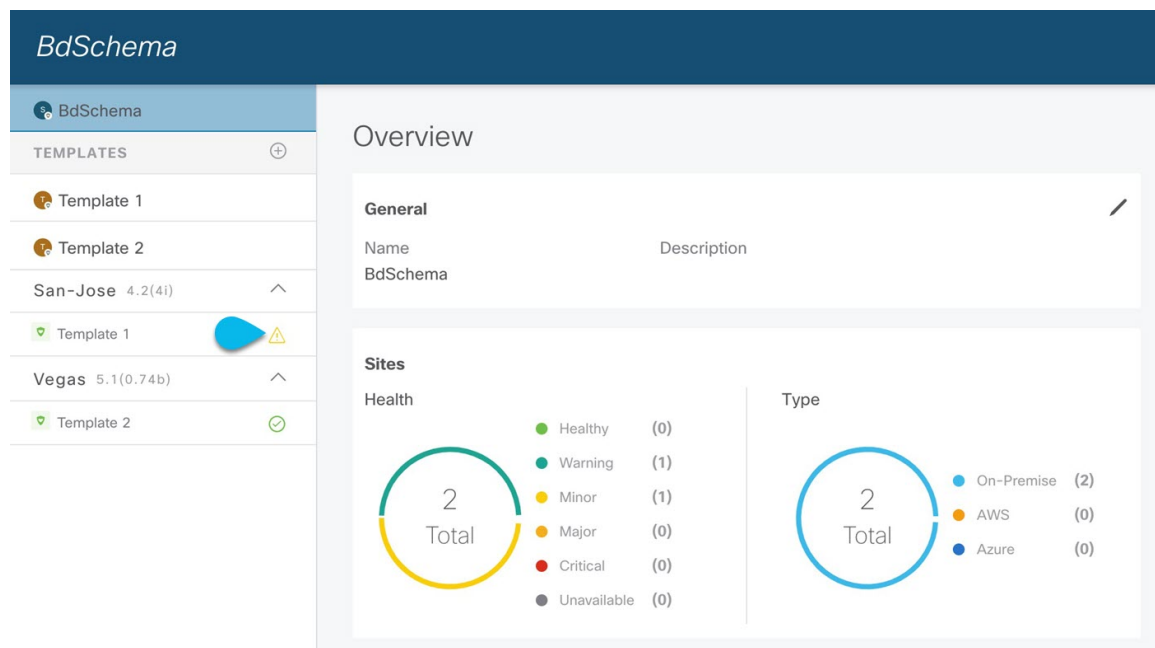
ステップ 5 [アクション (Actions)] メニューから [テンプレートの関連付け解除 (Disassociate Template)] を選択します。

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 4:



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

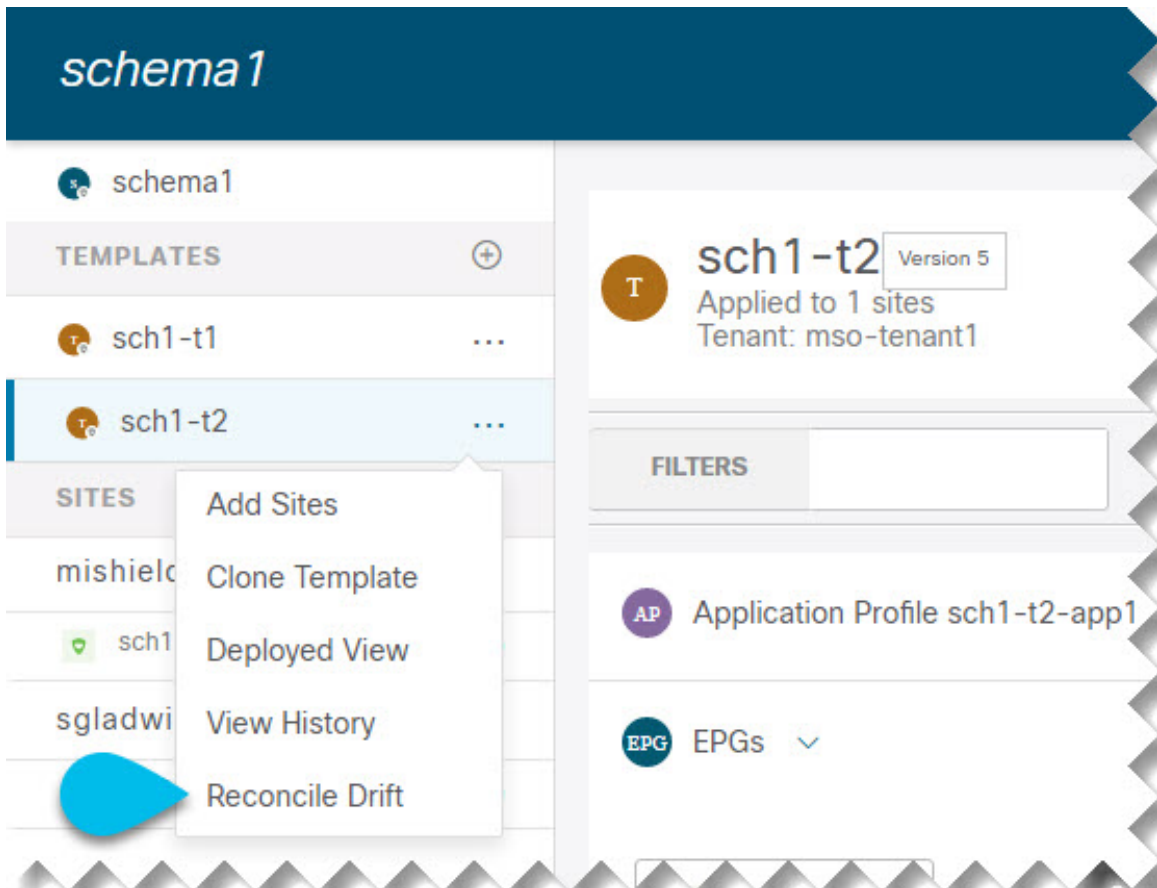
NDO リリース 3.6(1) では、Nexus Dashboard Orchestrator で定義されたテンプレート構成と、マルチサイトドメインのサイト部分の APIC コントローラーでレンダリングされた構成を比較するために実行できるばらつき調整ワークフローのサポートが導入されています。これにより、構成のばらつき（つまり、Nexus Dashboard Orchestrator または APIC で直接行われた変更）の原因をより明確に把握でき、以下の手順で説明するように、ばらつきを調整する方法をユーザーに選択させることができます。



(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。

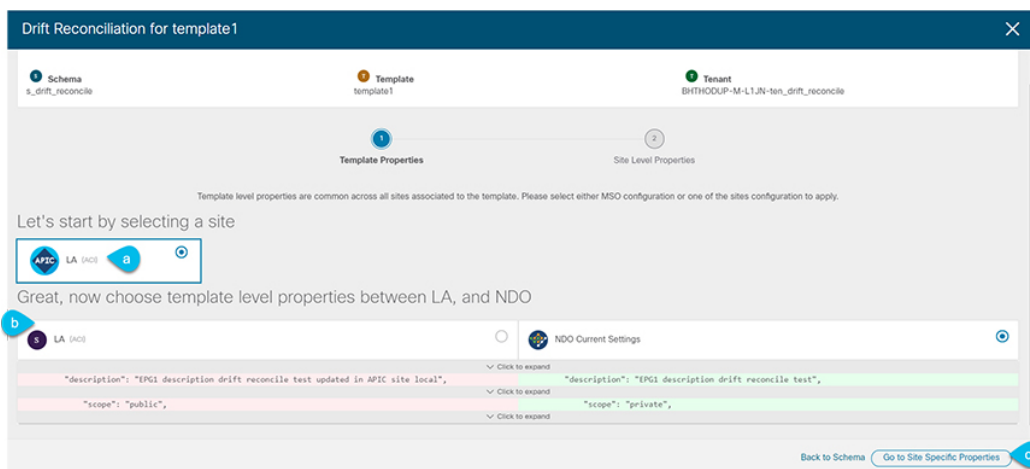
ステップ 1 設定のばらつきを確認するテンプレートを含むスキーマに移動します。

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。

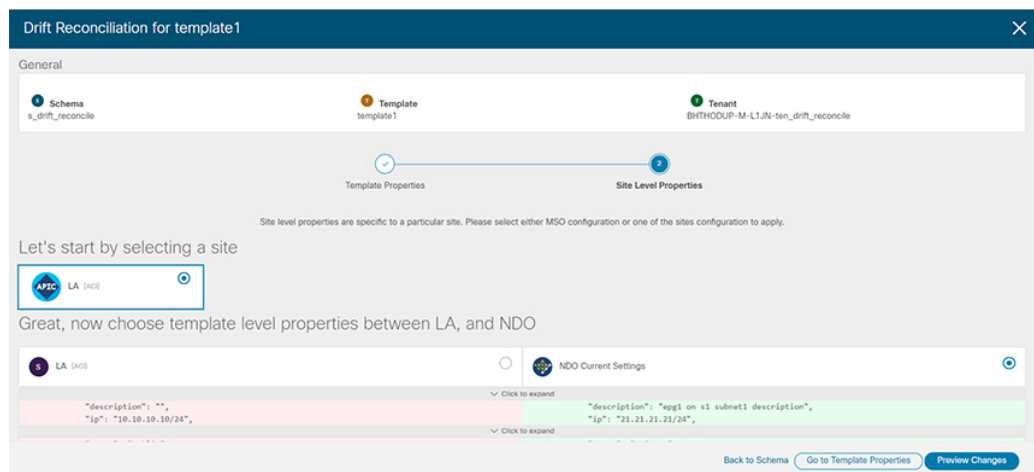


- (この特定のテンプレートに関連付けられているサイトのリストの中で) サイトを選択します。
- 保持するプロパティを選択します。

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 Dashboard 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があります（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。

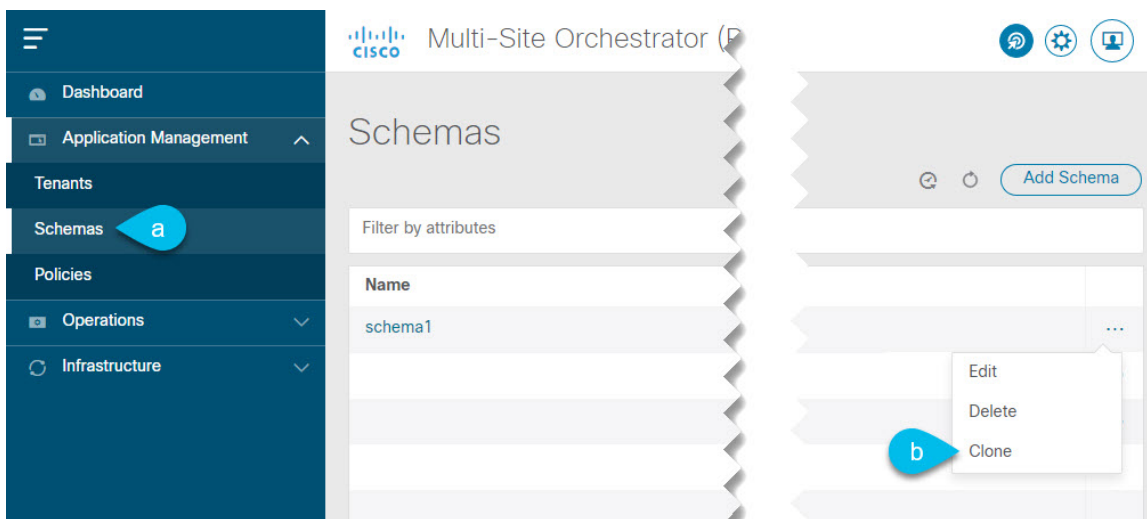
テンプレート設定は、[ばらつきの調整 (Diff Reconciliation)] ウィザードで選択したプロパティに基づいて調整されます。その後、[サイトに展開 (Deploy to site)] をクリックして設定を展開し、そのテンプレートのばらつきを調整できます。

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。

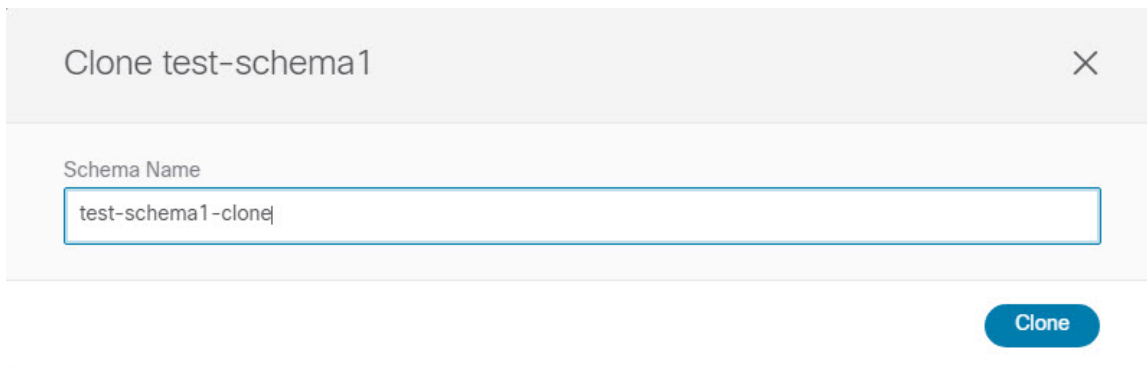
ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 複製するスキーマを選択します。

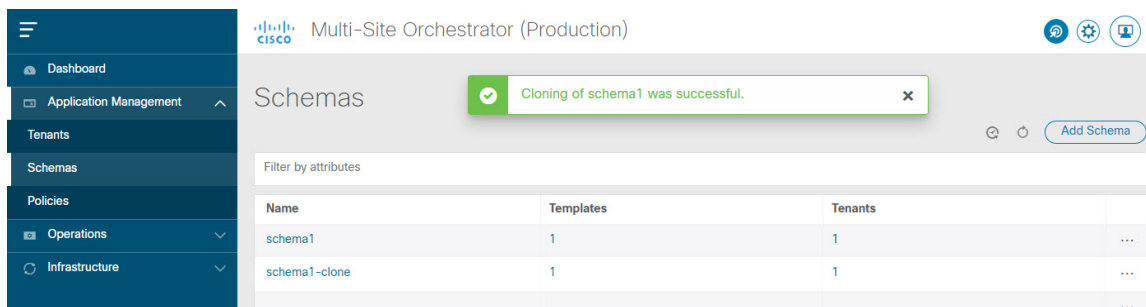


- 左側のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。
- 複製するスキーマ名の横にある [アクション (Actions)] メニューから、[スキーマの複製 (Clone Schema)] を選択します。

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。

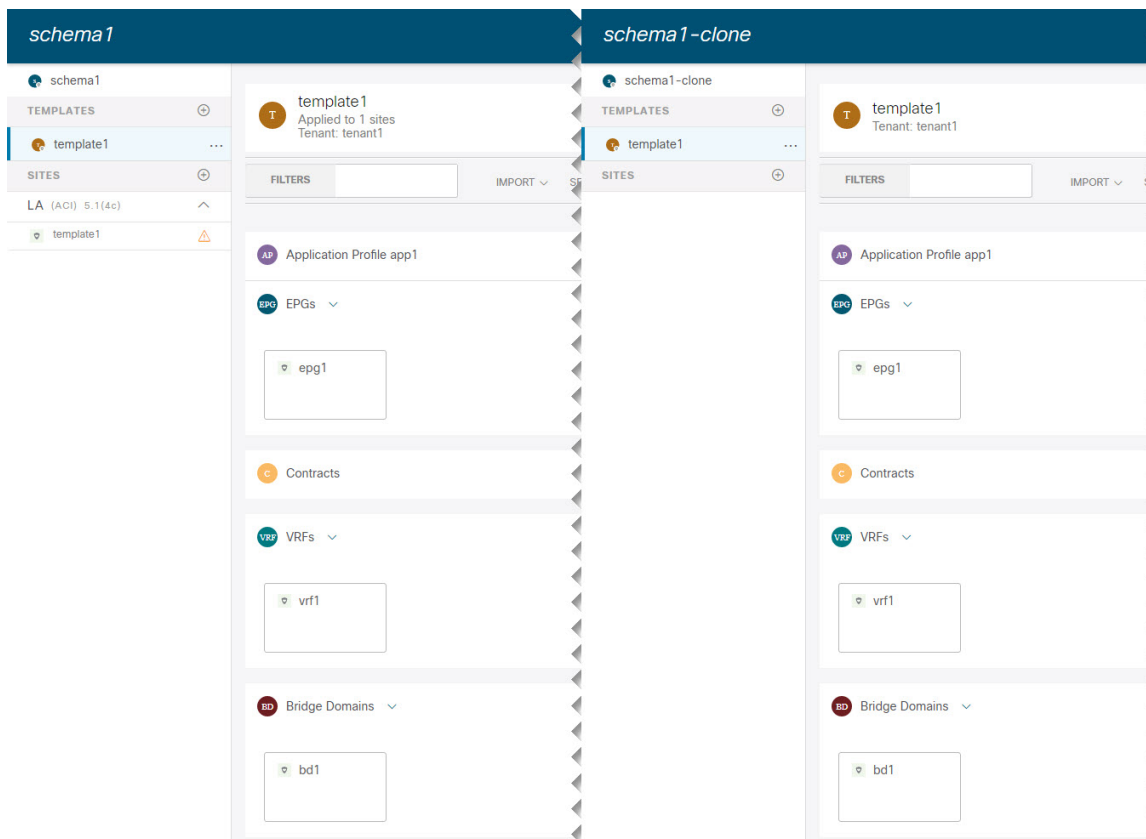


新しいスキーマは、元のスキーマとまったく同じテンプレート（およびそのテナントの関連付け）、オブジェクト、およびポリシー設定で作成されます。

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。

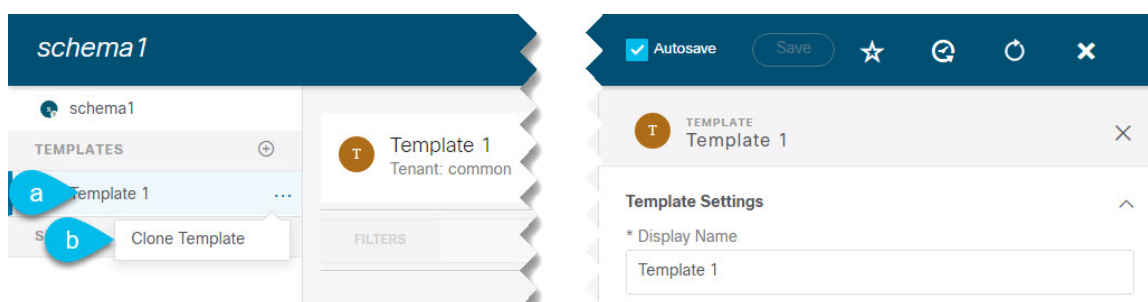
2つのスキーマを比較することで、操作が正常に完了したことを確認できます。



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。

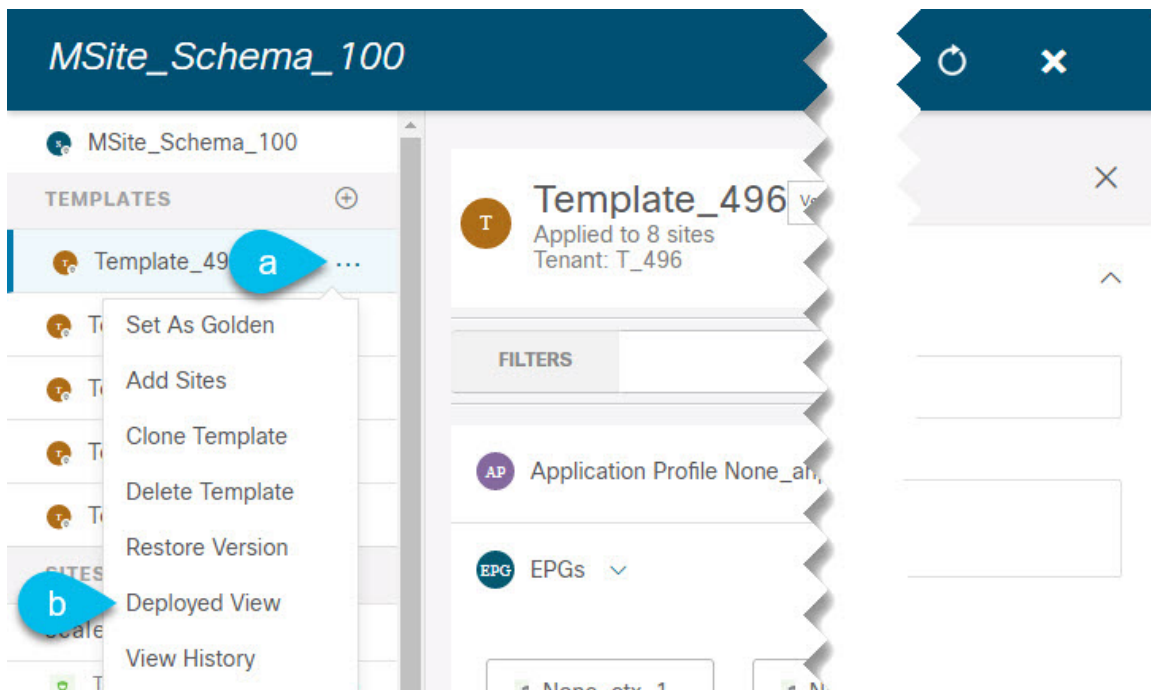
-
- ステップ 1** Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2** 左のナビゲーションメニューから **[スキーマ(Schemas)]** を選択します。
- ステップ 3** 移行するオブジェクトが含まれているスキーマをクリックします。
- ステップ 4** **[スキーマ (Schema)]** ビューで、移行するオブジェクトが含まれているテンプレートを選択します。
- ステップ 5** メインペインの右上にある **[選択 (Select)]** をクリックします。
これにより、移行する 1 つ以上のオブジ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。

```

<polUni>
  <fvTenant name='T_496' annotation='orchestrator:misc'>
    <fvAp name='None_anp_1' annotation='orchestrator:misc-shadow:no'>
      <fvAEPg name='None_ctx_2_bd_5_epg_1' isAttrBasedEPg='no' fwdCtrl=' prefGrMemb='exclude'
        hasMcastSource='no' prio='unspecified' annotation='orchestrator:misc-shadow:no'>
        <fvRsBd tnFvBDName='None_ctx_2_bd_5'>
        <fvRsProv tnVzBrCPName='tenant_ctr_None_ctx_2' annotation='orchestrator:misc'> </fvRsProv>
        <fvRsCons tnVzBrCPName='tenant_ctr_None_ctx_2' annotation='orchestrator:misc'>
        </fvRsCons>
    </fvAp>
  </fvTenant>

```

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

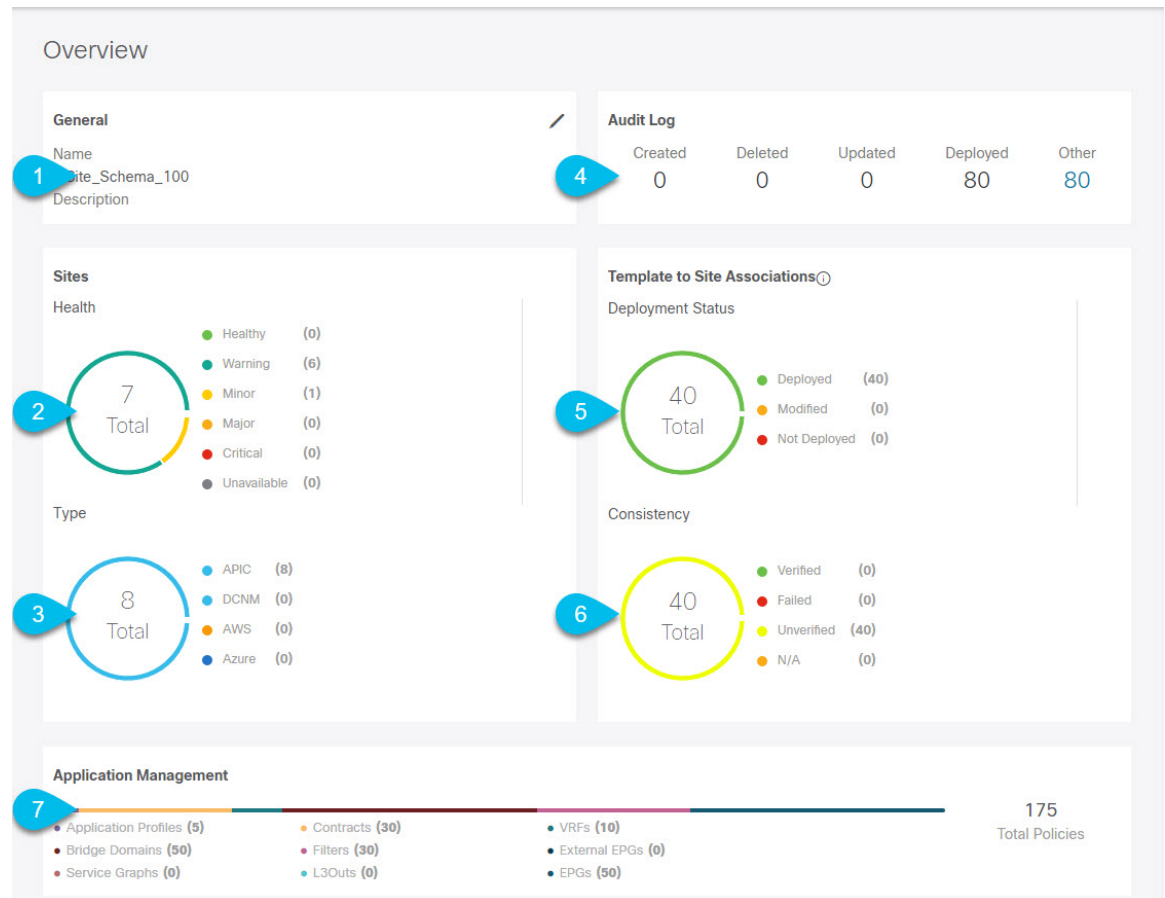
テンプレートの最新バージョンがすでに展開されている場合、ビューには色分けされたオブジェクトは含まれず、現在展開されている設定が表示されます。

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

スキーマの概要と展開ビジュアライザ

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

図 5: スキーマの概要



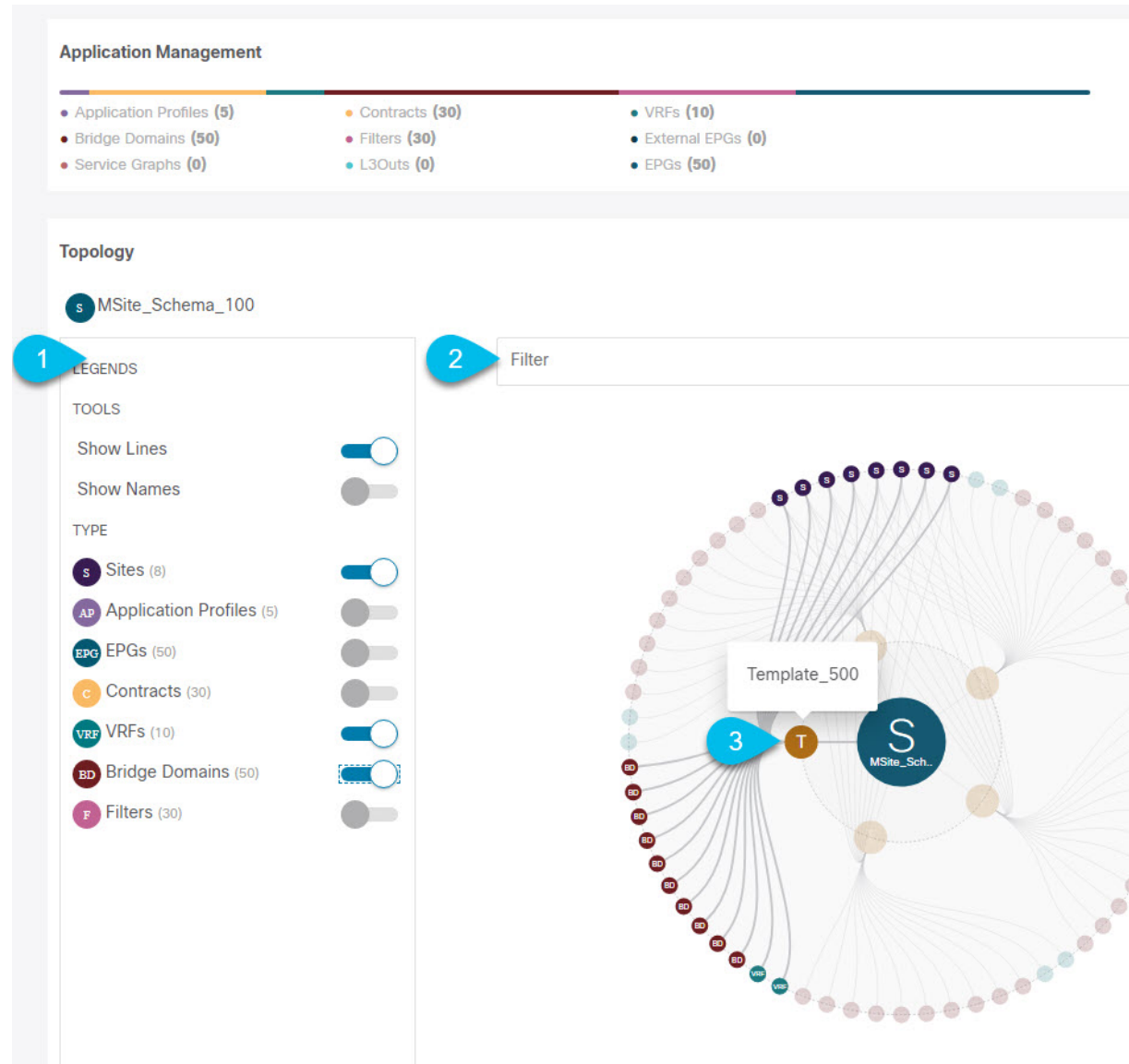
このページには、次の詳細が表示されます。

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

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

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

図 6: 展開ビジュアライザ



1. 凡例 (Legend) : 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

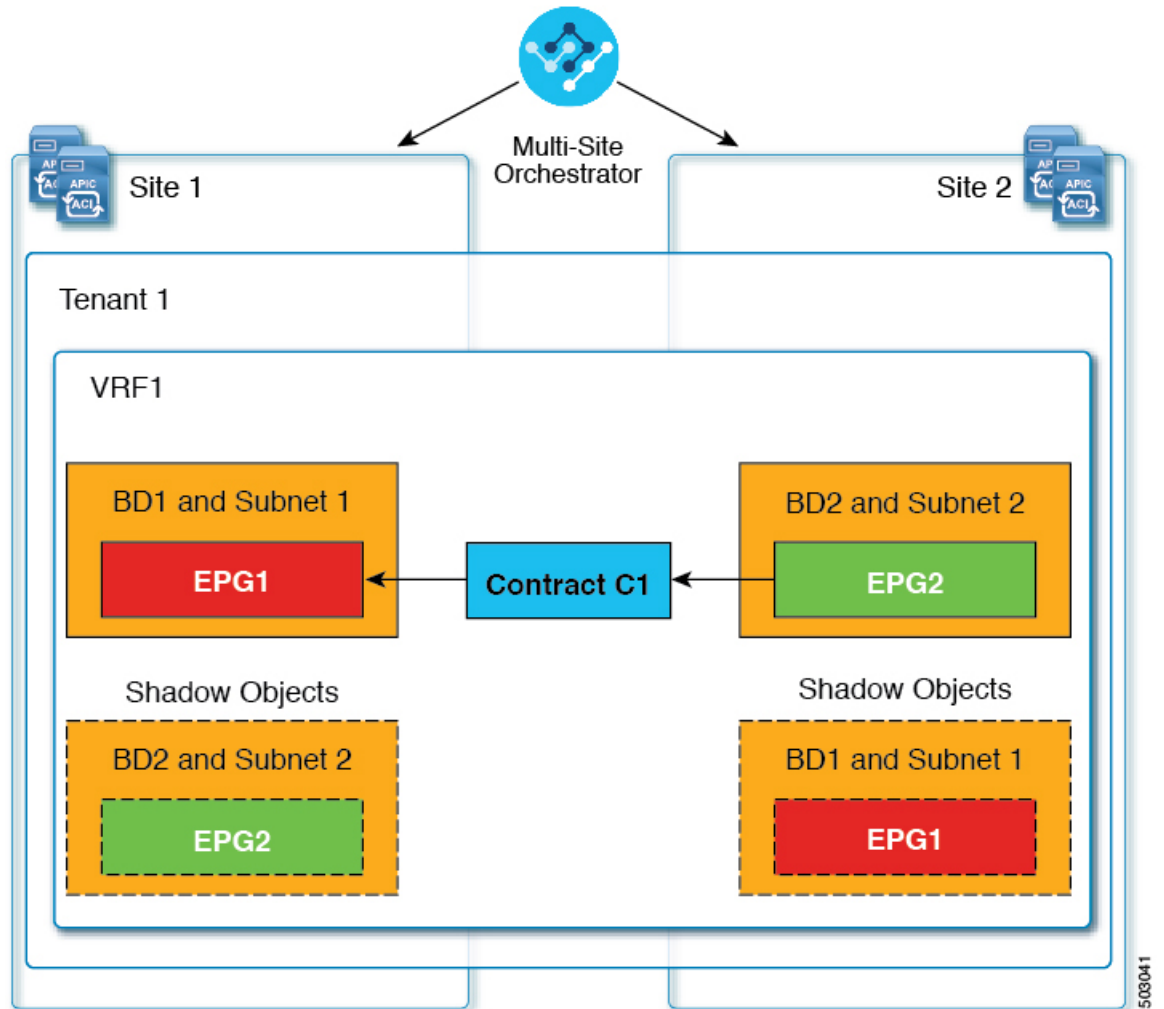
プロバイダとコンシューマーが異なる VRF にあり、テナント コントラクトを介して通信する拡張 VRF または共有サービスの使用例で、サイト ローカル EPG 間にコントラクトが存在する場合、EPG とブリッジドメイン (BD) はリモートサイトにミラーリングされます。ミラーされたオブジェクトは、これらのサイトのそれぞれの APIC で展開されているかのように表示される一方で、実際にはサイトの 1 つでだけ展開されています。これらのミラーされたオブジェクトは、「シャドウ」オブジェクトと呼ばれます。



(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 7: 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)

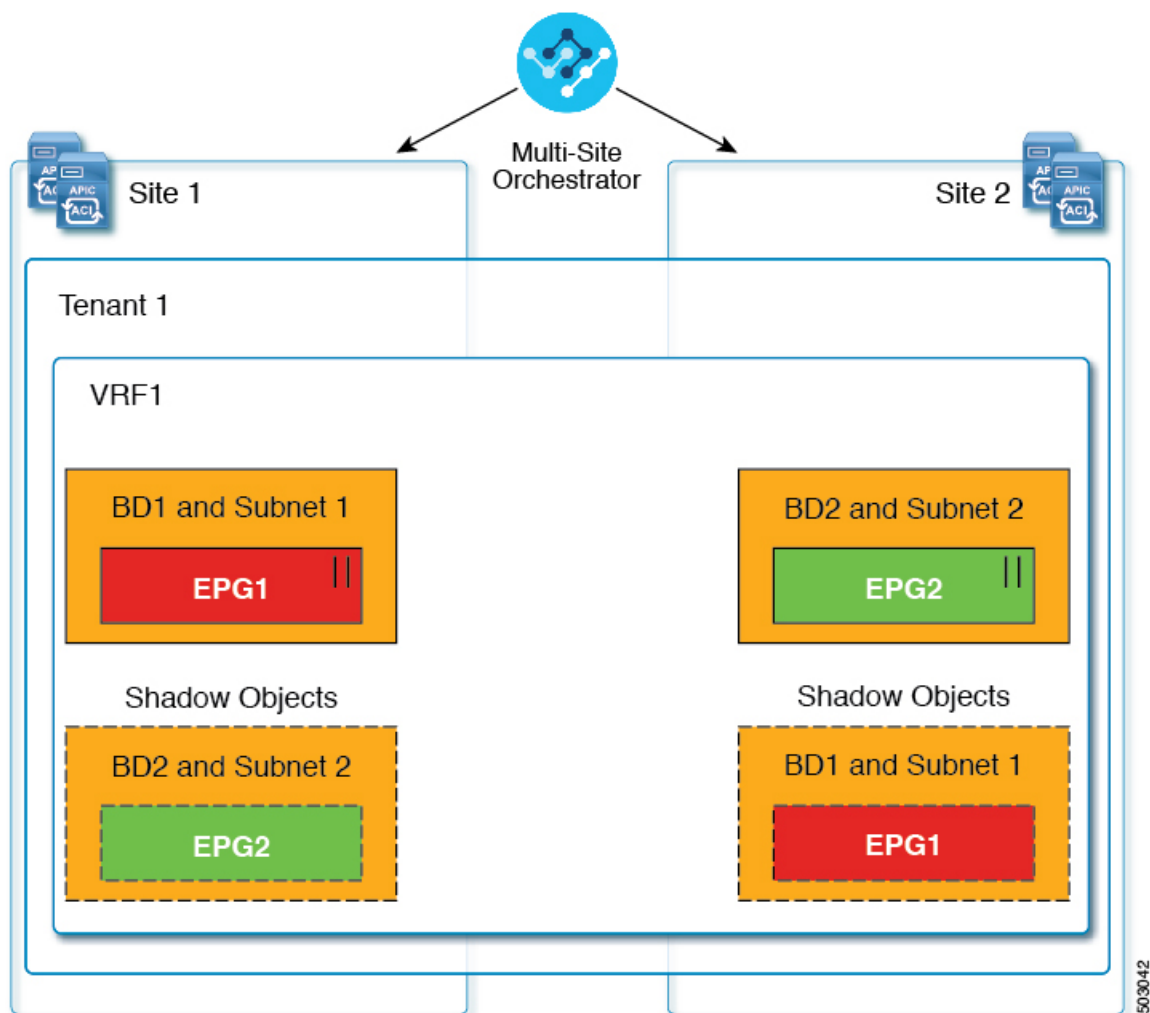
ファブリックが APIC リリース 5.0(2) 以降で実行されている場合、APIC GUI でシャドウ オブジェクトを選択すると、が表示されます。これはサイト間ポリシーをサポートするために、MSC からプッシュ

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 がないいぼずで、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。

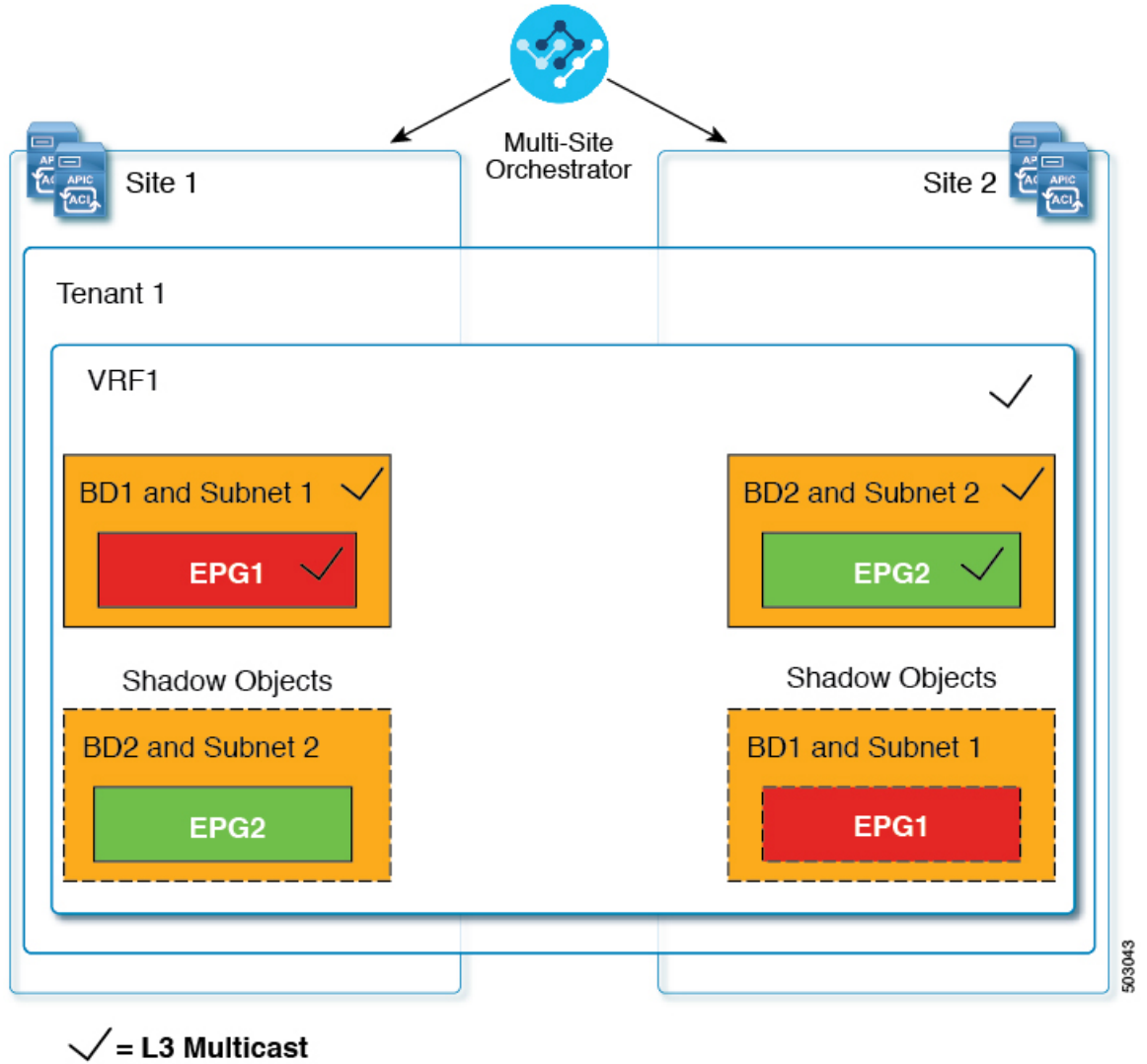
図 8: 優先グループ



|| = Preferred Group

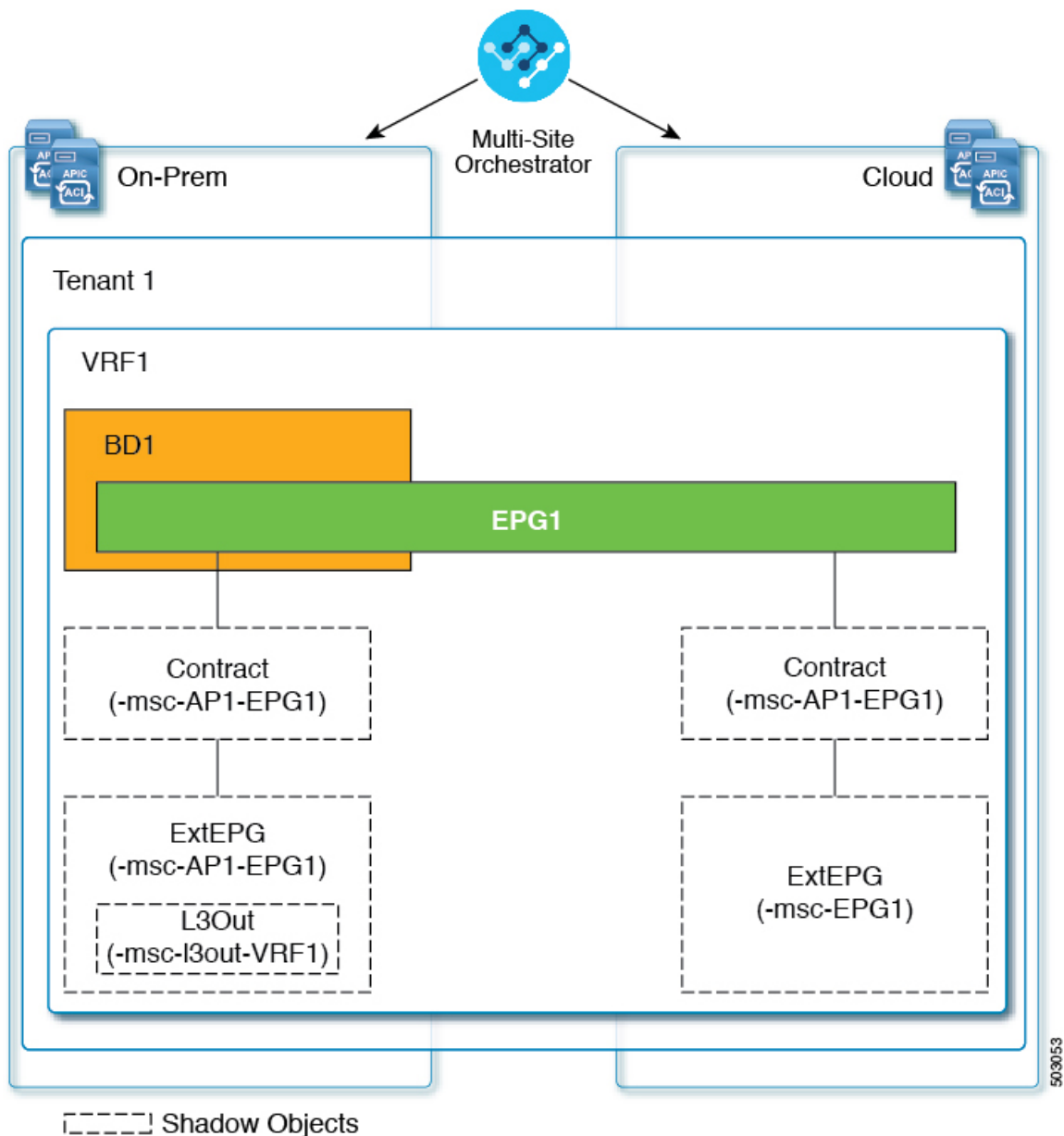
マルチキャストの場合、シャドウ オブジェクトは、マルチキャスト ソースが接続され、オプションが EPG レベルで明示的に設定されている EPG/BD に対してのみ作成されます。

図 9: 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 10: 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。
