



スキーマ

- スキーマ設計上の考慮事項 (1 ページ)
- 設定の同時更新 (6 ページ)
- スキーマとテンプレートの作成 (8 ページ)
- サイトへのテンプレートの割り当て (28 ページ)
- テンプレートのバージョンニング (29 ページ)
- テンプレートのレビューと承認 (34 ページ)
- テンプレートの展開 (37 ページ)
- テンプレートの展開解除 (38 ページ)
- サイトからのテンプレートの関連付け解除 (39 ページ)
- 設定のばらつき (40 ページ)
- スキーマの複製 (42 ページ)
- テンプレートの複製 (44 ページ)
- テンプレート間でのオブジェクトの移行 (46 ページ)
- 現在展開されている設定の表示 (47 ページ)
- スキーマの概要と展開ビジュアライザ (49 ページ)
- シャドウ オブジェクト (52 ページ)

スキーマ設計上の考慮事項

スキーマは、ポリシーの定義に使用されるテンプレートの集合であり、各テンプレートは特定のテナントに割り当てられます。展開の使用例に固有のスキーマとテンプレートの設定を作成する際に、複数のアプローチを実行できます。ここでは、マルチサイト環境でスキーマ、テンプレート、およびポリシーを定義する方法を決定する際に実行できる、いくつかの簡単な設計方針について説明します。

スキーマを設計するには、スキーマ、テンプレート、およびスキーマあたりのオブジェクトの数に対してサポートされているスケーラビリティ制限を考慮する必要があることに注意してください。検証済みスケーラビリティ制限の詳細については、お使いのリリースの『[Cisco Multi-Site Verified Scalability Guides](#)』を参照してください。

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。

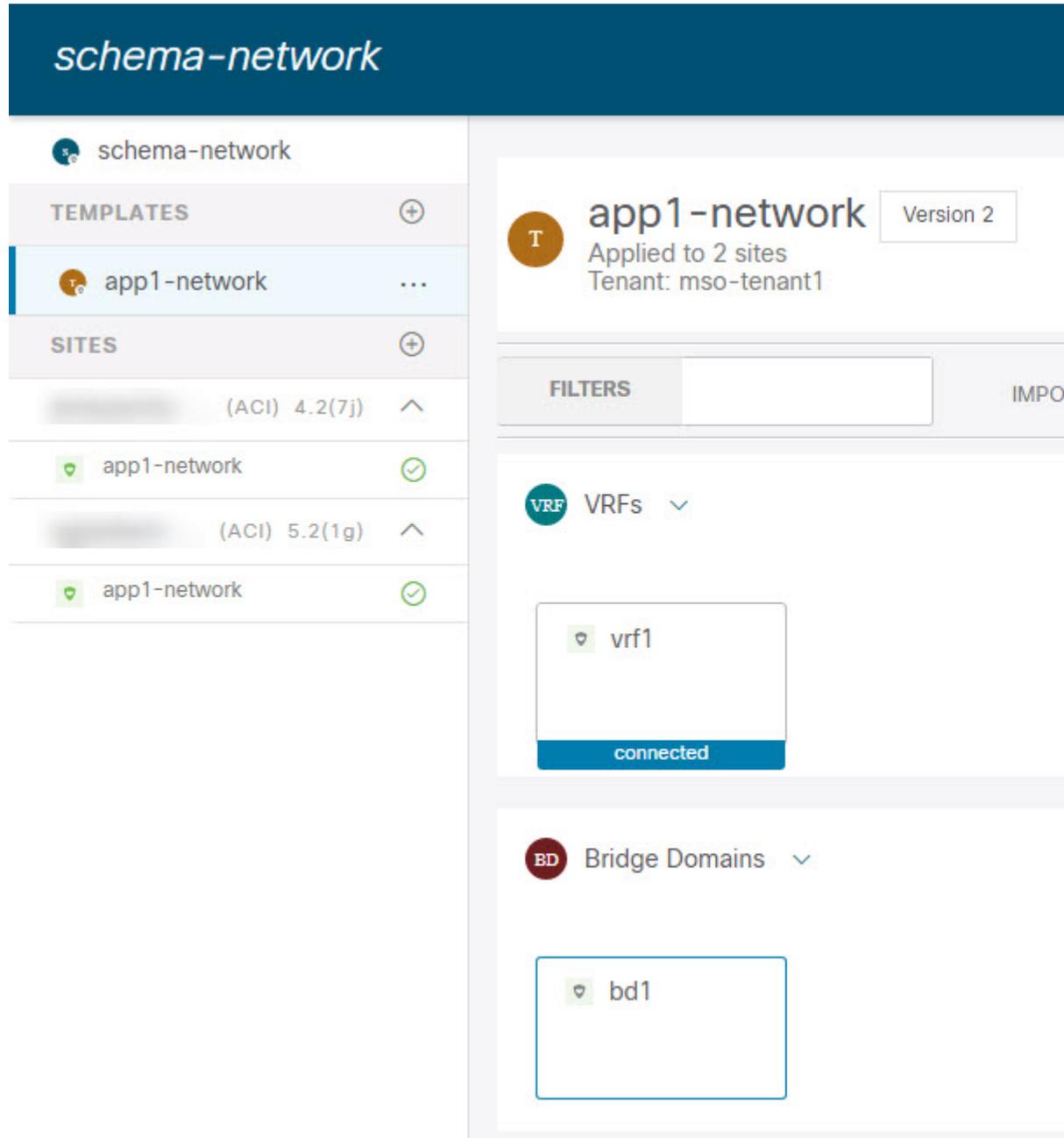
ネットワーク分離での複数スキーマ

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

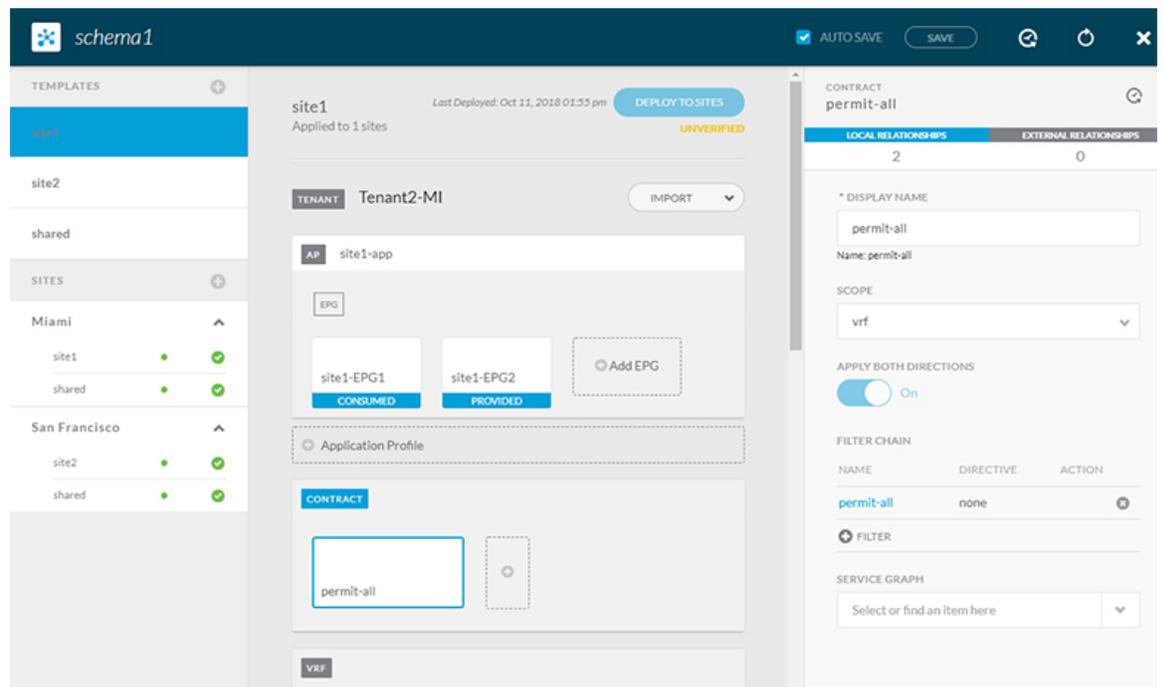
照を含むオブジェクトは、上のネットワークスキーマの図に示すように、リボンのアイコンでも示されます。

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。

オブジェクトの関係性に基づく複数スキーマ

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

図 3: サイトごとに1つのテンプレート



上の図の **site1** テンプレートには、Site1 に対してローカルなオブジェクトのみが含まれています。このテンプレートは、Miami サイトにのみ展開されます。同様に、**site2** テンプレートには Site2 に関連するオブジェクトのみが含まれており、San Francisco サイトに展開されます。これらのテンプレートのいずれかのオブジェクトに変更を加えても、他のテンプレートのオブジェクトには影響しません。共有テンプレートには、サイト間で共有されるオブジェクトが含まれています。

このシナリオは、次のテンプレートレイアウトを持つ追加サイトに拡張できます。

- サイト 1 テンプレート

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

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

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

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ー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。



Update failed, object version in the DB has changed,
refresh your client and retry



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



(注) この機能を有効にする場合は、次の点に注意してください。

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

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

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

例

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

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

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

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



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

- PUT API を使用して、更新されるスキーマ全体ペイロードとします。

```
PUT /v1/schemas/601acfed38000070a4ee9ec0?enableVersionCheck=true
{
  "id": "601acfed38000070a4ee9ec0",
```

```

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

```

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

```

PATCH /v1/schemas/601acfed38000070a4ee9ec0?enableVersionCheck=true
[
  {
    "op": "replace",
    "path": "/templates/Template1/displayName",
    "value": "new name",
    "_updateVersion": 12
  }
]

```

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

```

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

```

スキーマとテンプレートの作成

始める前に

- 管理者ユーザ アカウント (完全な読み取り/書き込み権限を持つ) が必要です。
- テナント アカウント (テナント ポリシーの読み取り/書き込み権限を持つ) が必要です。
Cisco APIC Basic Configuration Guide の *User Access, Authentication, and Accounting* を参照してください。
- サイトに組み込むには、少なくとも 1 つの使用可能なテナントが必要です。
詳細については、[テナントの追加](#) を参照してください。

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

ステップ2 スキーマを新規作成します。

- a) 左側のナビゲーションメニューで、[アプリケーション管理 (Application Management)] > [スキーマ (Schemas)] を選択します。
- b) [スキーマ (Schema)] ページで、[スキーマの追加 (Add Schema)] をクリックします。
- c) スキーマ作成ダイアログで、スキーマの [名前 (Name)] と説明 (オプション) を入力します。
デフォルトでは、新しいスキーマは空であるため、1 つ以上のテンプレートを追加する必要があります。

ステップ3 テンプレートを作成します。

- a) 左側のサイドバーの [テンプレート (Templates)] で、[+] 記号をクリックして新しいテンプレートを追加します。
- b) 右側のサイドバーで、[表示名 (Display name)] を指定します。
- c) (任意) [説明 (Description)] を入力します。
- d) SR-MPLSテンプレートを設定する場合は、**SR-MPLS** ノブを有効にします。
SR-MPLSテンプレートの詳細については、[SR-MPLS 経由で接続されたサイト](#)を参照してください。
- e) [テナントの選択 (Select a Tenant)] ドロップダウンから、このテンプレートのテナントを選択します。
新しいスキーマを作成するために使用しているユーザアカウントは、そのスキーマに追加しようとしているテナントに関連付けられている必要があることに注意してください。そうしないと、テナントはドロップダウンメニューで使用できなくなります。ユーザアカウントとテナントの関連付けについては、[テナントの追加](#)を参照してください。

ステップ4 テンプレートをサイトに割り当てます。

一度に1つのテンプレートを展開するため、設定を展開する少なくとも1つのサイトにテンプレートを関連付ける必要があります。

- a) 左側のペインで、サイトの横にある [+] 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の横のチェックボックスをオンにします。
- c) 各サイトの横にある [テンプレートに割り当て (Assign to Template)] ドロップダウンから、1 つ以上のテンプレートを選択します。
テンプレートの展開は、関連付けられているすべてのサイトに一度に1つずつ行いますが、サイトへの関連付けは、一度に複数のテンプレートで行えます。
- d) [保存 (Save)] をクリックします。

APIC サイトからのスキーマ要素のインポート

新しいオブジェクトを作成し、1 つまたは複数のサイトに公開できます。または、サイトローカルの既存のオブジェクトをインポートし、マルチサイト Orchestrator を使用して管理できま

す。ここでは、1つ以上の既存のオブジェクトをインポートする方法について説明します。このドキュメントでは、新しいオブジェクトを作成する方法について説明します。

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

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

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

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

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

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

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

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

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

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

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

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

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

VRF の設定

このセクションでは、VRF の設定方法を説明します。

始める前に

[スキーマとテンプレートの作成 \(8 ページ\)](#) 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

- [スキーマとテンプレートの作成 \(8 ページ\)](#) 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。

- 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かかわらず行われません。

- 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](#) 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](#) 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 (16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、SVIMAC 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

[スキーマとテンプレートの作成 \(8 ページ\)](#) 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。

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

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

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

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

- c) (任意) **[説明 (Description)]** を入力します。

ステップ 3 EPG を作成します。

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

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

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

- c) (任意) **[説明 (Description)]** を入力します。

ステップ 4 EPG のコントラクトを追加します。

コントラクトとフィルタの作成については、[コントラクトとフィルタの設定 \(22 ページ\)](#) 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：

- 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 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 \(17 ページ\)](#) 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。

- [+ スタティック ポートの追加 (+Static Port)]** をクリックします。
- [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。
- 物理インターフェイスを設定する場合は、インターフェイスの **ポッド** と **リーフ 1** を選択します。
- インターフェイスの **[パス (Path)]** を指定します。
- [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路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。

コントラクトとフィルタの設定

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

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

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

ステップ2 フィルタを作成します。

- a) メインペインで、**[+ オブジェクトの作成 (+Create Object)]** > **[フィルタ (Filter)]** を選択します。
または、**[フィルタ (Filters)]** エリアまでスクロールダウンし、タイトルの上にマウスを移動して、**[フィルタの追加 (Add Filter)]** をクリックします。
- b) 右側のペインで、フィルタの **[表示名 (Display Name)]** を入力します。
- c) (任意) **[説明 (Description)]** を入力します。

ステップ3 フィルタ エントリを作成します。

- a) 右側のペインで、**[+ エントリ (+ Entry)]** をクリックします。
フィルタ エントリは、ネットワーク トラフィックの分類プロパティの組み合わせです。次の手順の説明に従って、1つ以上のオプションを指定できます。
- b) フィルタの **[名前 (Name)]** を指定します。
- c) **[イーサー タイプ (Ether Type)]** を選択します。
たとえば [ip] です。
- d) **[IP プロトコル (IP Protocol)]** を選択します。
たとえば [icmp] です。
- e) **[宛先ポート範囲の開始 (Destination Port Range From)]** と **[宛先ポート範囲の終了 (Destination Port Range To)]** を選択します。
宛先ポート範囲の開始と終了です。開始フィールドと終了フィールドに同じ値を指定すれば、単一のポートの指定になります。または、0 から 65535 の範囲内で、ポートの範囲を定義することもできます。また、特定のポート番号 (http など) の代わりに、いずれかのサーバタイプを指定することもできます。
- f) **[フラグメントのみの一致 (Match only fragment)]** オプションを有効にします。
有効の場合、オフセットが 0 より大きいすべての IP フラグメント (最初のフラグメントを除くすべての IP フラグメント) にこのルールが適用されます。無効の場合、TCP/UDP ポート情報は最初のフラグメントでしかチェックできないため、オフセットが 0 より大きい IP フラグメントにルールは適用されません。
- g) **[ステートフル (Stateful)]** オプションを有効にします。
このオプションを有効にする場合には、プロバイダーからコンシューマに戻るすべてのトラフィックは、常にパケットに ACK ビットが設定されている必要があります。そうでないと、パケットはドロップされます。
- h) **[ARP フラグ (ARP flag)]** : (Address Resolution Protocol) を指定します。
ARPフラグは、ARPの特定のフィルタを作成するときに使用され、ARP要求またはARP応答を指定できます。
- i) **[送信元ポート範囲の開始 (Source Port Range From)]** と **[送信元ポート範囲の終了 (Source Port Range To)]** を指定します。

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

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

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

- k) **[保存 (Save)]** をクリックしてフィルタを保存します。
 l) このフィルタの追加のフィルタ エントリを作成するには、この手順を繰り返します。
 フィルタごとに複数のフィルタ エントリを作成して割り当てることができます。

ステップ4 コントラクトの作成

- a) メインペインで、**[+ オブジェクトの作成 (+Create Object)]** > **[コントラクト (Contract)]** を選択します。
 または、**[コントラクト (Contract)]** エリアまでスクロールダウンし、タイルの上にマウスを移動して、**[コントラクトの追加 (Add Contract)]** をクリックします。
 b) 右側のペインで、コントラクトの**表示名**を指定します。
 c) (任意) **[説明 (Description)]** を入力します。
 d) コントラクトの適切な**[範囲 (Scope)]** を選択します。

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

- アプリケーションプロファイル
- vrf
- テナント
- global

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

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

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

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

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

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

ステップ 5 コントラクトにフィルタを割り当てる

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

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

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

同じコントラクトに追加のフィルタを作成する場合：

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

オンプレミス外部接続の設定

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

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

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

始める前に

- [スキーマとテンプレートの作成 \(8 ページ\)](#) 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。

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 左側のペインで、サイトの横にある [+] のアイコンをクリックします。

ステップ3 [**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。

ステップ4 各サイトの横にある [**テンプレートに割り当て (Assign to Template)**] ドロップダウンから、1つ以上のテンプレートを選択します。

テンプレートの展開は、関連付けられているすべてのサイトに一度に1つずつ行いますが、サイトへの関連付けは、一度に複数のテンプレートで行えます。

ステップ5 [**保存 (Save)**] をクリックします。

ステップ 6 他のサイトに対して上記の手順を繰り返します。

一度に1つのテンプレートを展開するため、設定を展開する少なくとも1つのサイトにテンプレートを関連付ける必要があります。

テンプレートのバージョンニング

リリース 3.4(1) では、テンプレートのバージョン管理のサポートが追加されています。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。

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。

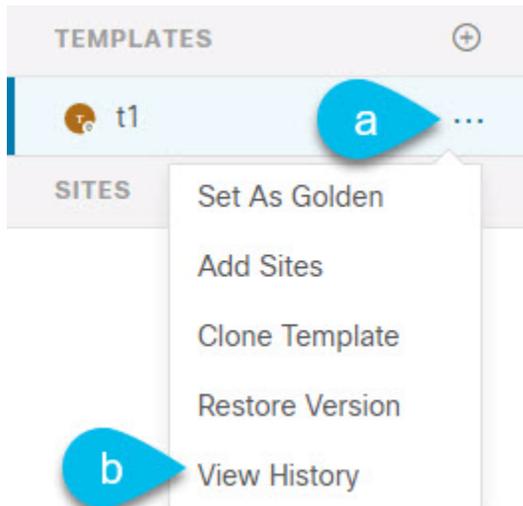
ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

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。

The screenshot displays the 'Version History' window for a schema. It shows a sequence of versions from 1 to 4. Version 2 is marked as a 'Golden Version' and is currently selected. Version 4 is the 'Current' version. The interface allows filtering versions as 'Golden' or 'Deployed'. Below the timeline, the JSON configuration for Version 2 and Version 4 is shown for comparison.

```

Version 2 (Selected)
1 policies | 0 sites
1. {
2.   "siteDelta": {},
3. }
4.   "anps": [],
5.   "bds": [],
34. }

Version 4 (Current)
2 policies | 1 sites
1. {
2.   "siteDelta": {
3.     "ø": {
4.       "anps": [],
5.       "bds": [],
6.       "contracts": [],
7.       "externalEggs": [],
8.       "intersitel3outs": [],
9.       "networks": [],
10.      "serviceGraphs": [],
11.      "siteId": "61042fa61a7b8c0a62a1a0c4",
12.      "templateName": "t1",
13.      "vrfs": []
14.    }
15.  },
16.  "template": {
17.    "anps": [],
18.    "bds": [
19.      {
20.        "arpFlood": true,
21.        "bdRef":
22.        "/schemas/610450571f0000a5030540af/templates/t1/bds/bd1",
23.        "dhcpLabels": [],
24.        "displayName": "bd1",
25.        "intersiteBumTrafficAllow": true,
26.        "l3Stretch": true

```

- 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 \(29 ページ\)](#) 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。

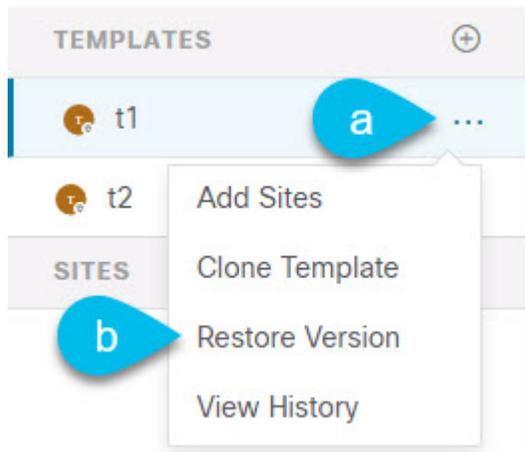
ステップ1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

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、[バージョンの復元 (Restore Version)] を選択します。



ステップ6 [バージョンの復元 (Restore Version)] 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 \(34ページ\)](#) 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。

必要なロールを持つユーザの作成

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

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

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

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

ステップ 3 必要なユーザーを作成します。

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

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

承認者ロールを持つ別個のユーザーが、[テンプレート承認要件の有効化 \(34 ページ\)](#) で設定した承認の最小数と同数以上必要です。

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

テンプレートのレビューと承認の要求

ここでは、テンプレートのレビューと承認を要求する方法について説明します。

始める前に

次のものがが必要です。

- 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 \(34 ページ\)](#) 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ーを作成または更新した ([必要なロールを持つユーザの作成 \(35 ページ\)](#) 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 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 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 \(34 ページ\)](#) を参照)。
- 承認者ロールと展開者ロールを使用してNexusダッシュボードでユーザを作成または更新した ([必要なロールを持つユーザの作成 \(35 ページ\)](#) 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 \(35 ページ\)](#) 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 \(29 ページ\)](#) 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 \(47 ページ\)](#) 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 \(34 ページ\)](#) 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。

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

ステップ 4 [展開 (Deploy)] をクリックして、新しいテンプレートを展開します。

- このテンプレートを初めて展開する場合、または以前に展開したテンプレートに変更を加えた場合は、**[展開 (Deploy)]** の概要に、サイトに展開される設定の違いが表示されます。

[バージョン履歴の表示 (View Version History)] をクリックして、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します。バージョン履歴の詳細については、[履歴の表示と以前のバージョンの比較 \(29 ページ\)](#) 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 を表示します。[**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 \(47 ページ\)](#) 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。

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。

- 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。

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

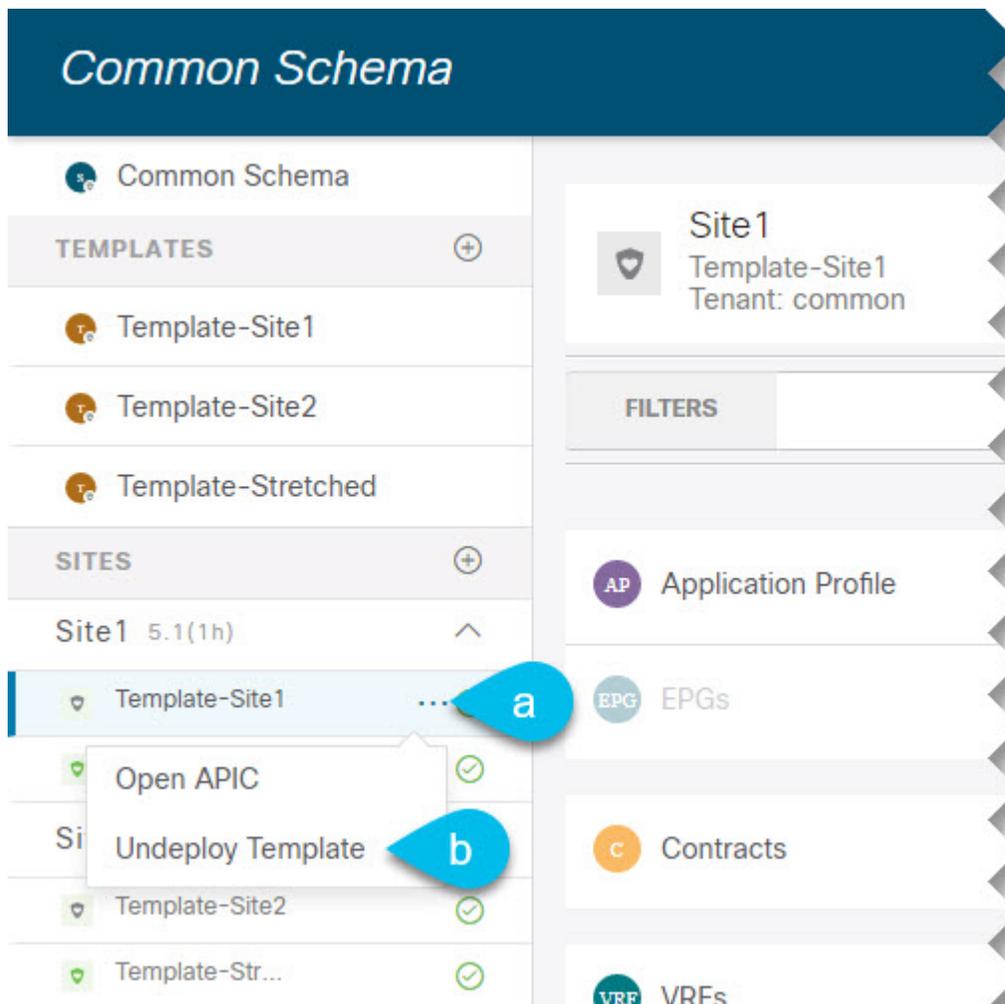
- テンプレートを最後に展開してから、テンプレートに変更を加えていないことを確認します。

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。

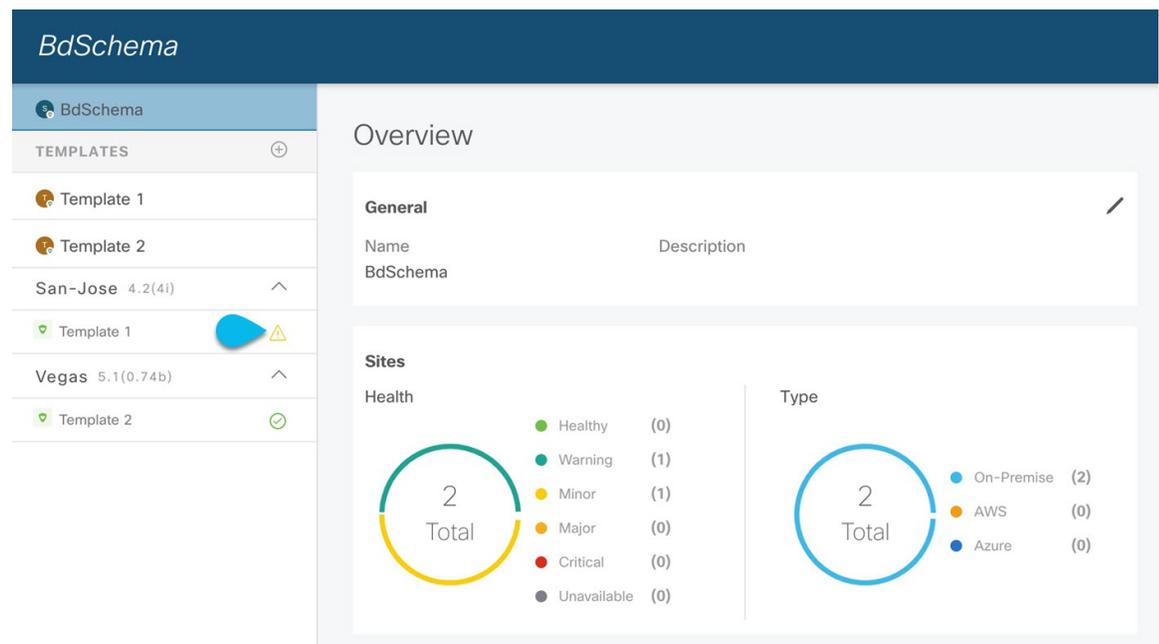
ステップ5 [アクション (Actions)] メニューから [テンプレートの関連付け解除 (Disassociate Template)] を選択します。

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。これらの設定の不一致は、**設定のばらつき**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感嘆符で示されます。

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。設定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。
 - ローカルの変更を取り消す場合は、NDO からテンプレートを再展開して、サイトレベルで行われた手動の変更を上書きします。
 - ローカルの変更を保持する場合は、変更したオブジェクトをサイトから NDO テンプレートにインポートし、スキーマを保存して、サイトに再展開します。
- **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設定に変更が加えられた場合、バックアップを復元すると設定がずれる可能性があります。
 - バックアップ以降の変更を保存する場合は、設定の復元後に変更したオブジェクトをサイトから NDO テンプレートにインポートし、スキーマを保存して、サイトに再展開します。
 - 変更を保持しない場合は、NDO からテンプレートを再展開して、サイトレベルで設定の不一致を上書きします。
これにより、NDO から管理できるオブジェクトおよびオブジェクトのプロパティの設定を上書きできることに注意してください。APIC レベルで設定され、NDO から直接管理できない追加のオブジェクトとプロパティは削除されません。
- **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 で新しいプロパティが変更され、値がデフォルトと異なる場合に発生します。
 - オブジェクトのプロパティをデフォルト値にリセットする場合は、テンプレートを再展開します。
 - 新しくサポートされたオブジェクトプロパティにすでに設定されているカスタム値を保持する場合は、変更したオブジェクトをサイトから NDO テンプレートにインポートし、スキーマを保存して、テンプレートをサイトに再展開します。

- **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。
 - オブジェクトのプロパティをデフォルト値にリセットする場合は、テンプレートを再展開します。
 - 新しくサポートされたオブジェクトプロパティにすでに設定されているカスタム値を保持する場合は、変更したオブジェクトをサイトから NDO テンプレートにインポートし、スキーマを保存して、テンプレートをサイトに再展開します。

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。

Clone test-schema1

Schema Name

Clone

[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。

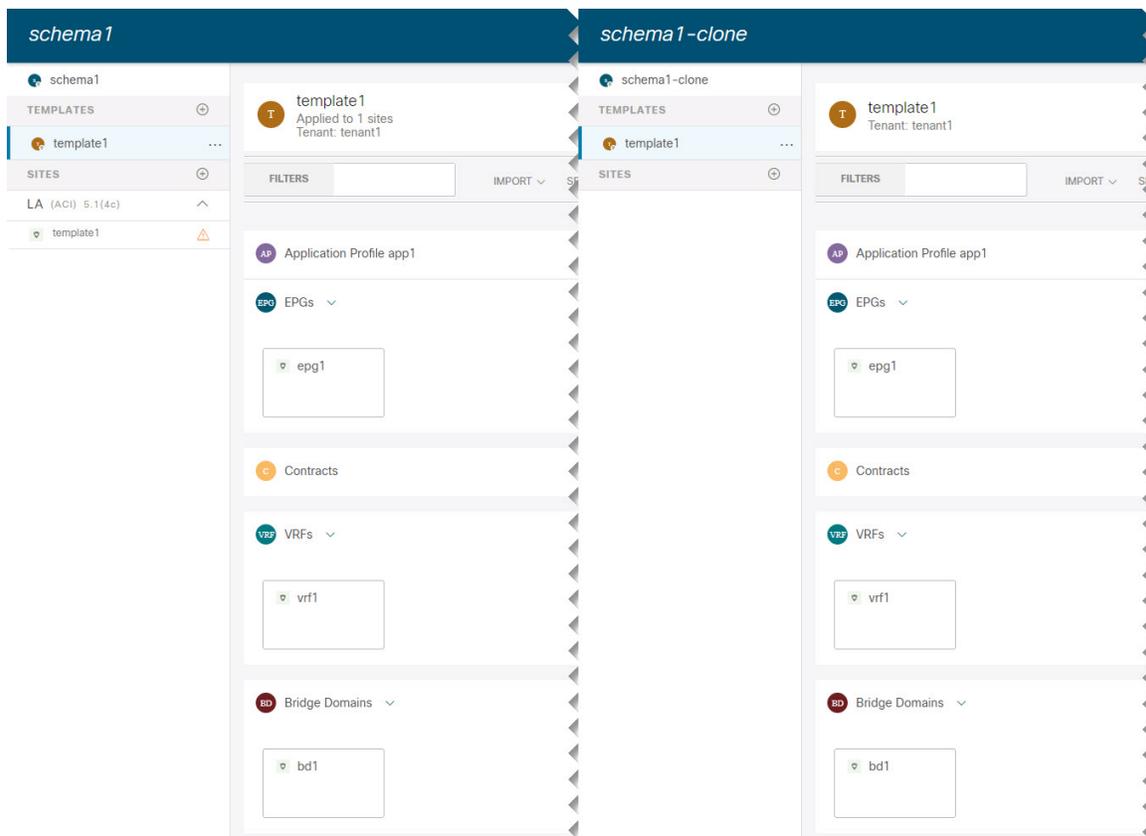
Name	Templates	Tenants	
schema1	1	1	...
schema1-clone	1	1	...

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。

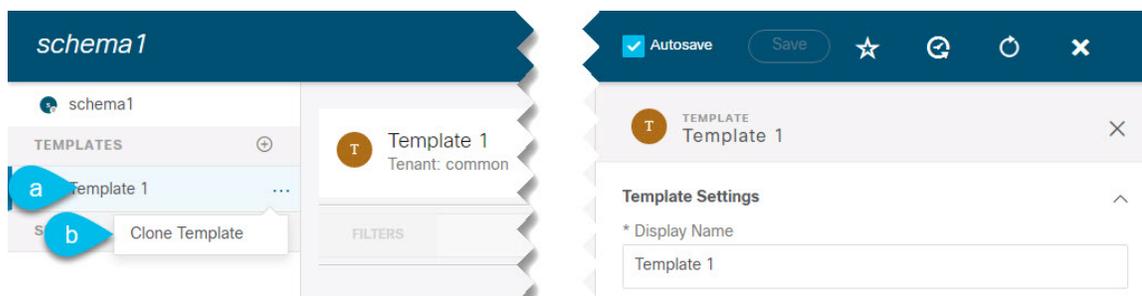
2 つのスキーマを比較することで、操作が正常に完了したことを確認できます。



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。

Clone Template 1
✕

Destination Tenant

Destination Schema

Cloned Template Name

- 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する必要があります。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。

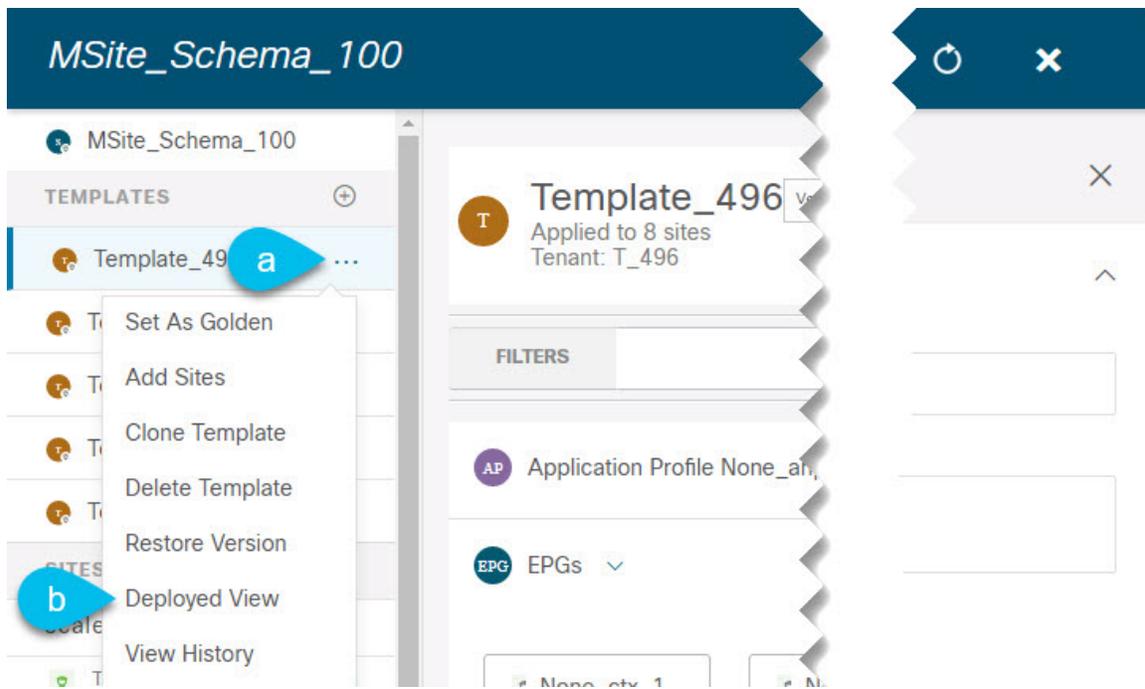
この情報は Orchestrator データベースから取得されるため、サイトのコントローラで直接行われた変更によって発生する可能性のある設定の変動は考慮されません。

- 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。

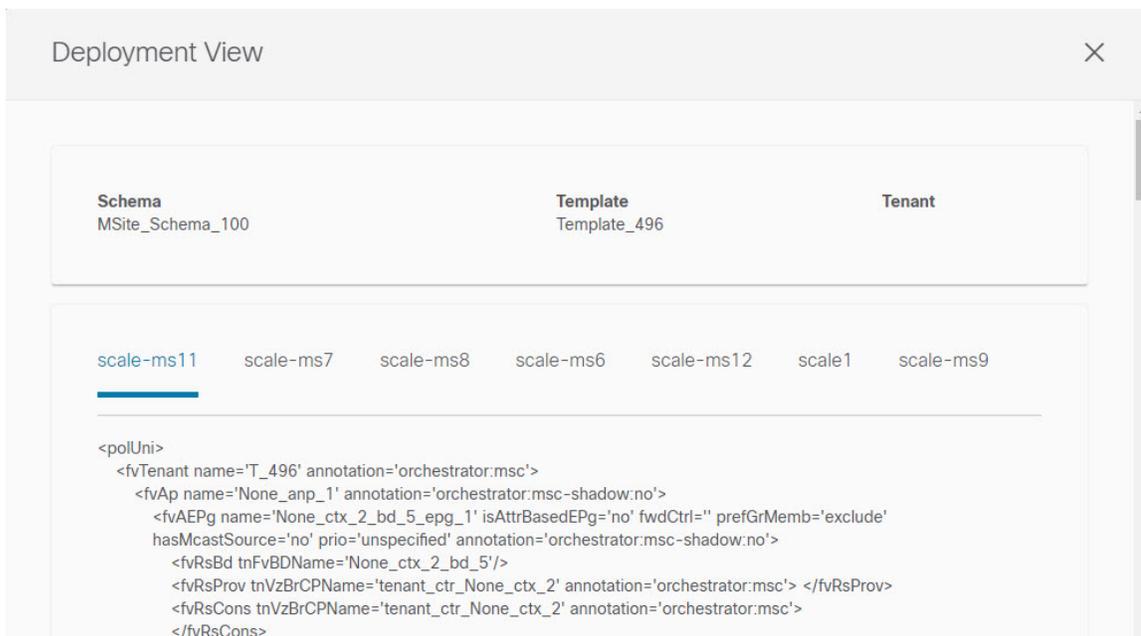


a) テンプレートの名前の横にある [アクション (Actions)] メニューをクリックします。

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。

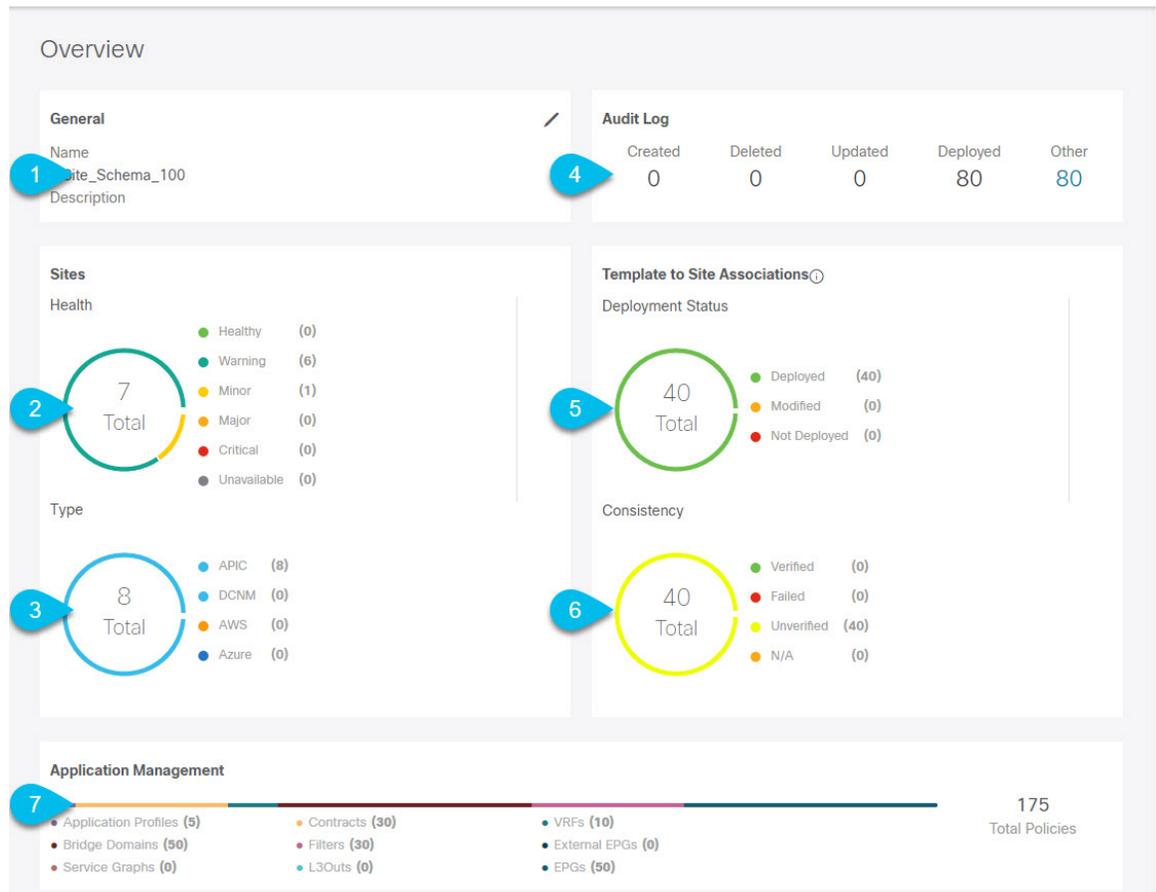


- 色分けされた凡例は、この時点でテンプレートを展開する場合に作成、削除、または変更されるオブジェクトを示します。
テンプレートの最新バージョンがすでに展開されている場合、ビューには色分けされたオブジェクトは含まれず、現在展開されている設定が表示されます。
- サイト名をクリックすると、その特定のサイトの設定を表示できます。
- [XML/JSON表示 (View XML/JSON)]** をクリックすると、選択したサイトに展開されているすべてのオブジェクトの XML 設定が表示されます。

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



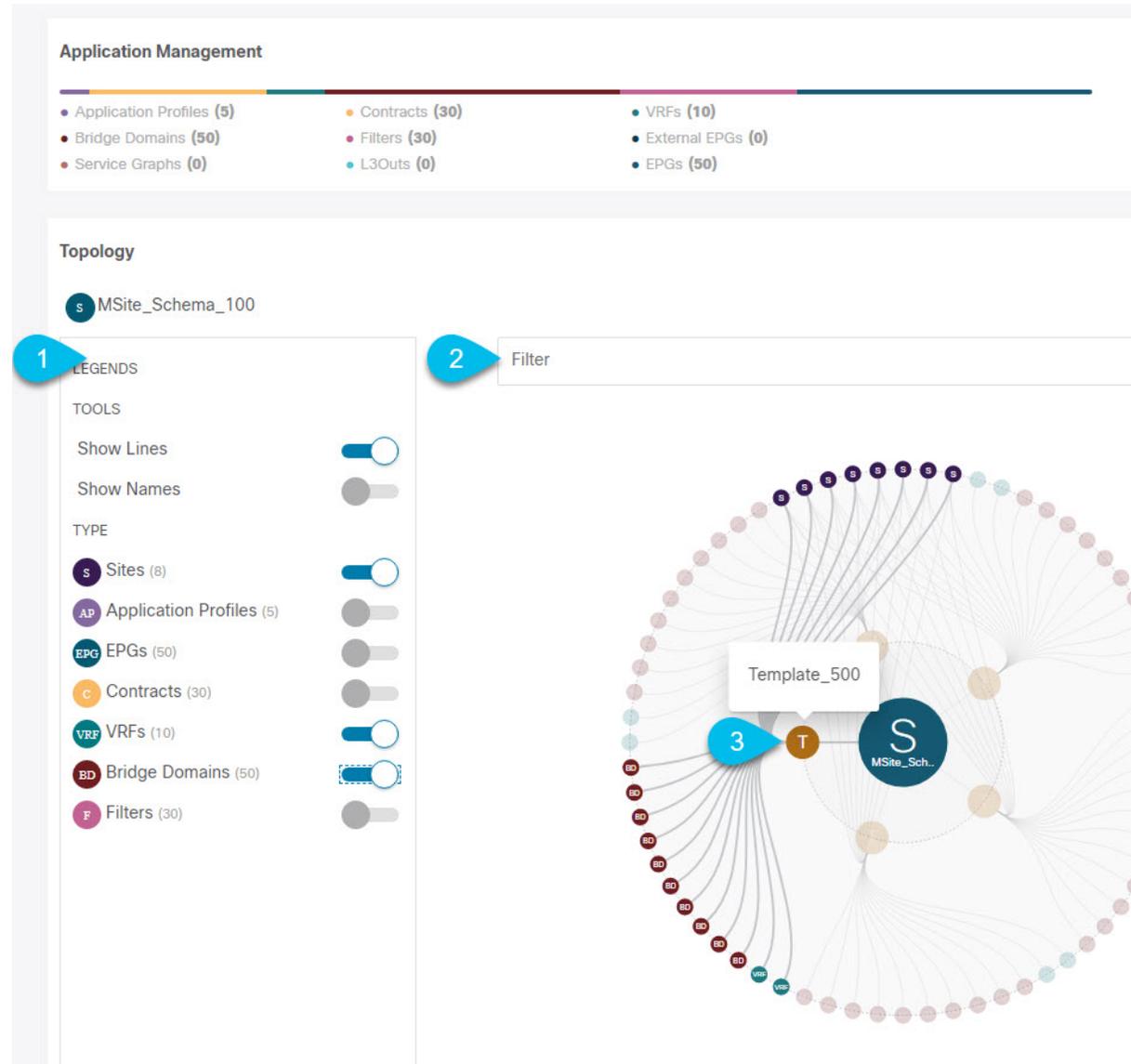
このページには、次の詳細が表示されます。

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

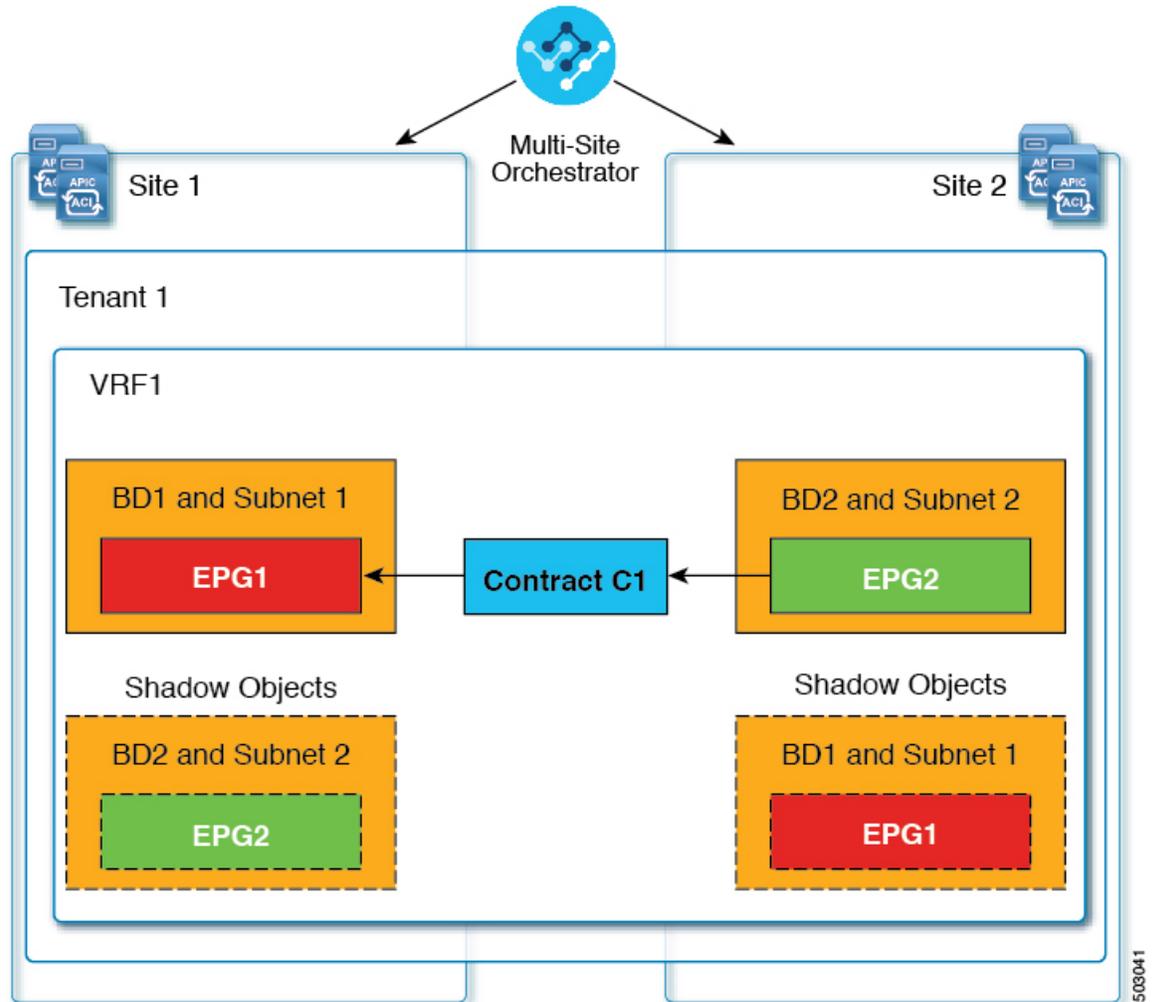
プロバイダとコンシューマーが異なる VRF にあり、テナント コントラクトを介して通信する拡張 VRF または共有サービスの使用例で、サイト ローカル EPG 間にコントラクトが存在する場合、EPG とブリッジドメイン (BD) はリモートサイトにミラーリングされます。ミラーされたオブジェクトは、これらのサイトのそれぞれの APIC で展開されているかのように表示される一方で、実際にはサイトの 1 つでだけ展開されています。これらのミラーされたオブジェクトは、「シャドウ」オブジェクトと呼ばれます。



(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)

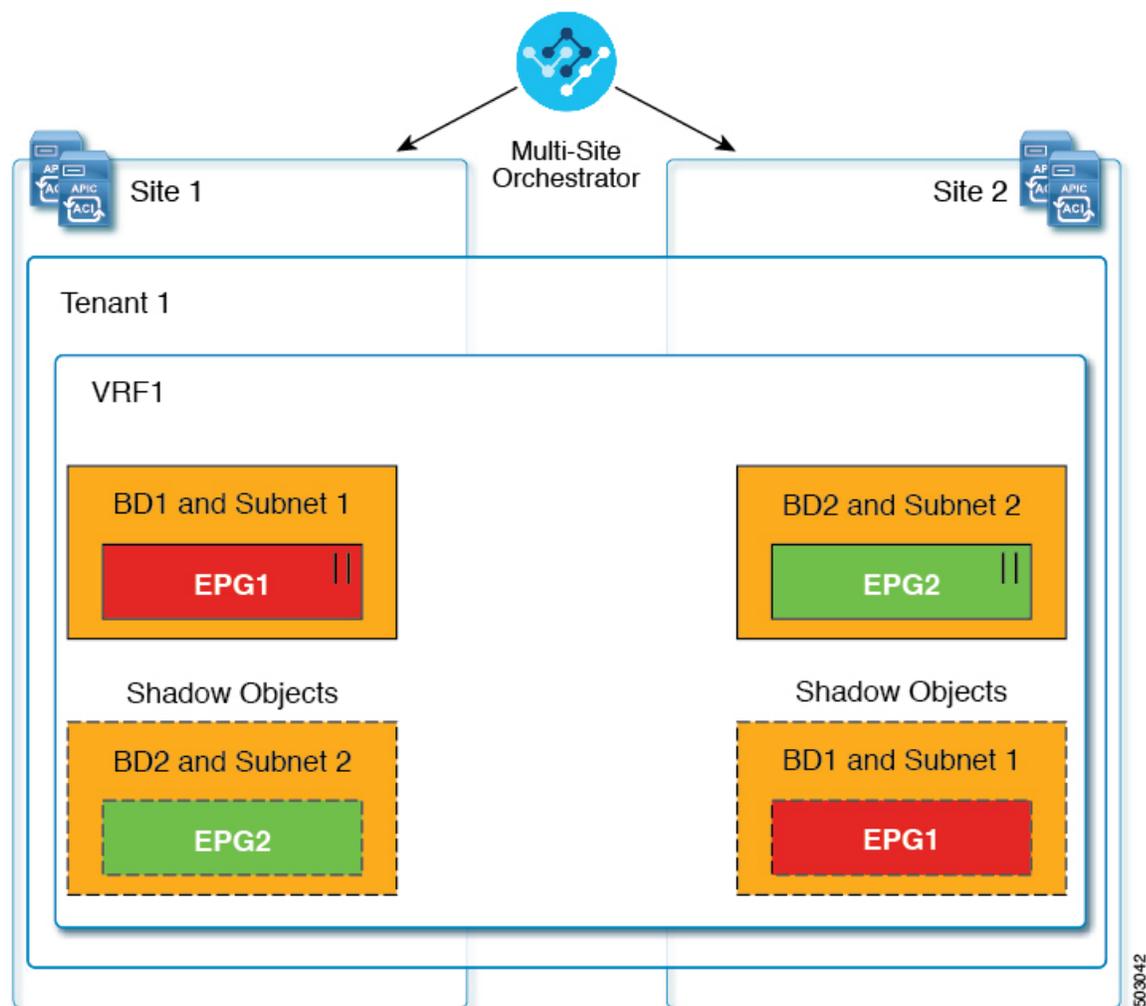
ファブリックが APIC リリース 5.0(2) 以降で実行されている場合、APIC GUI でシャドウ オブジェクトを選択すると、が表示されます。これはサイト間ポリシーをサポートするために、MSC からプッシュ

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。

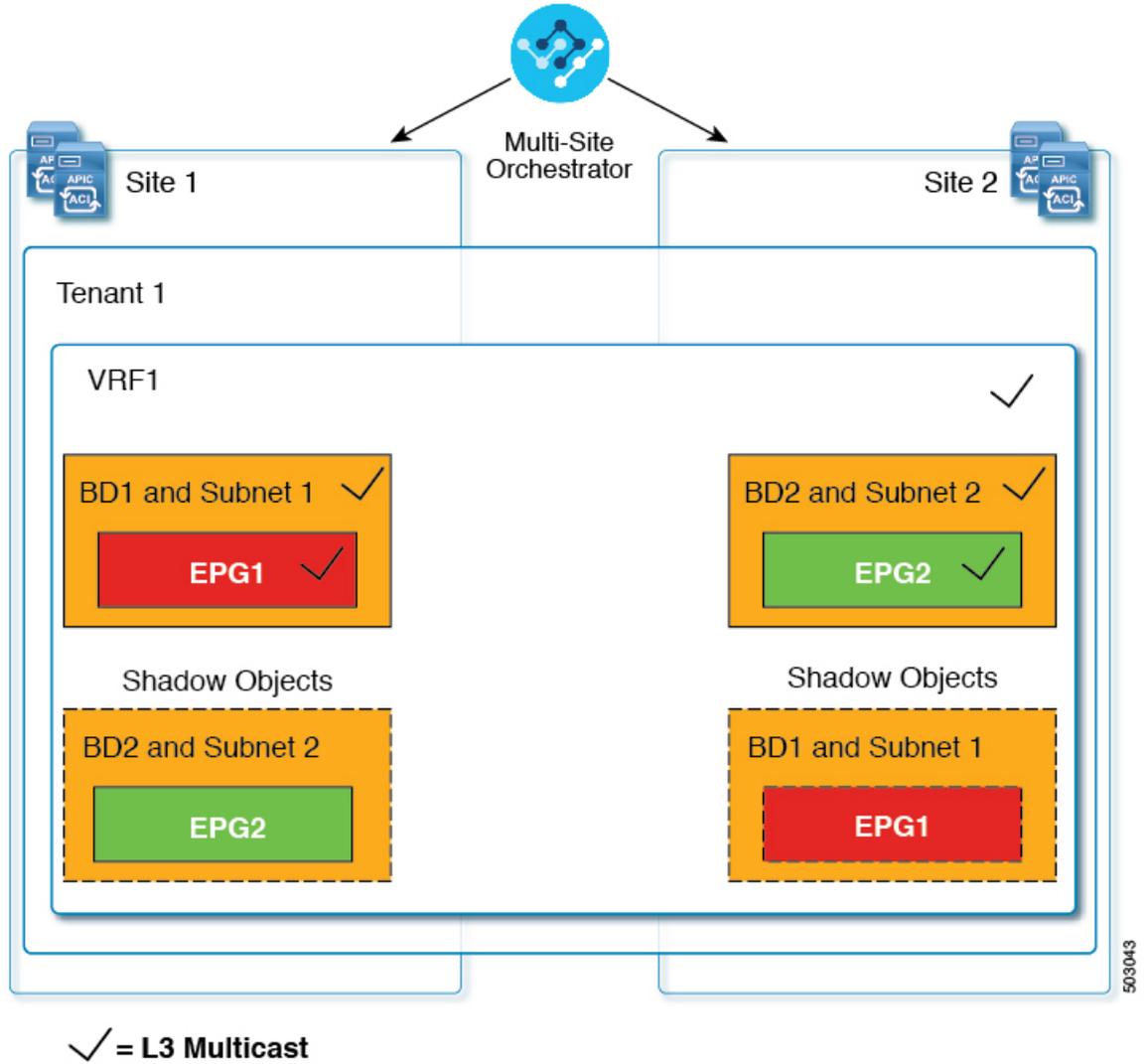
図 8: 優先グループ



|| = Preferred Group

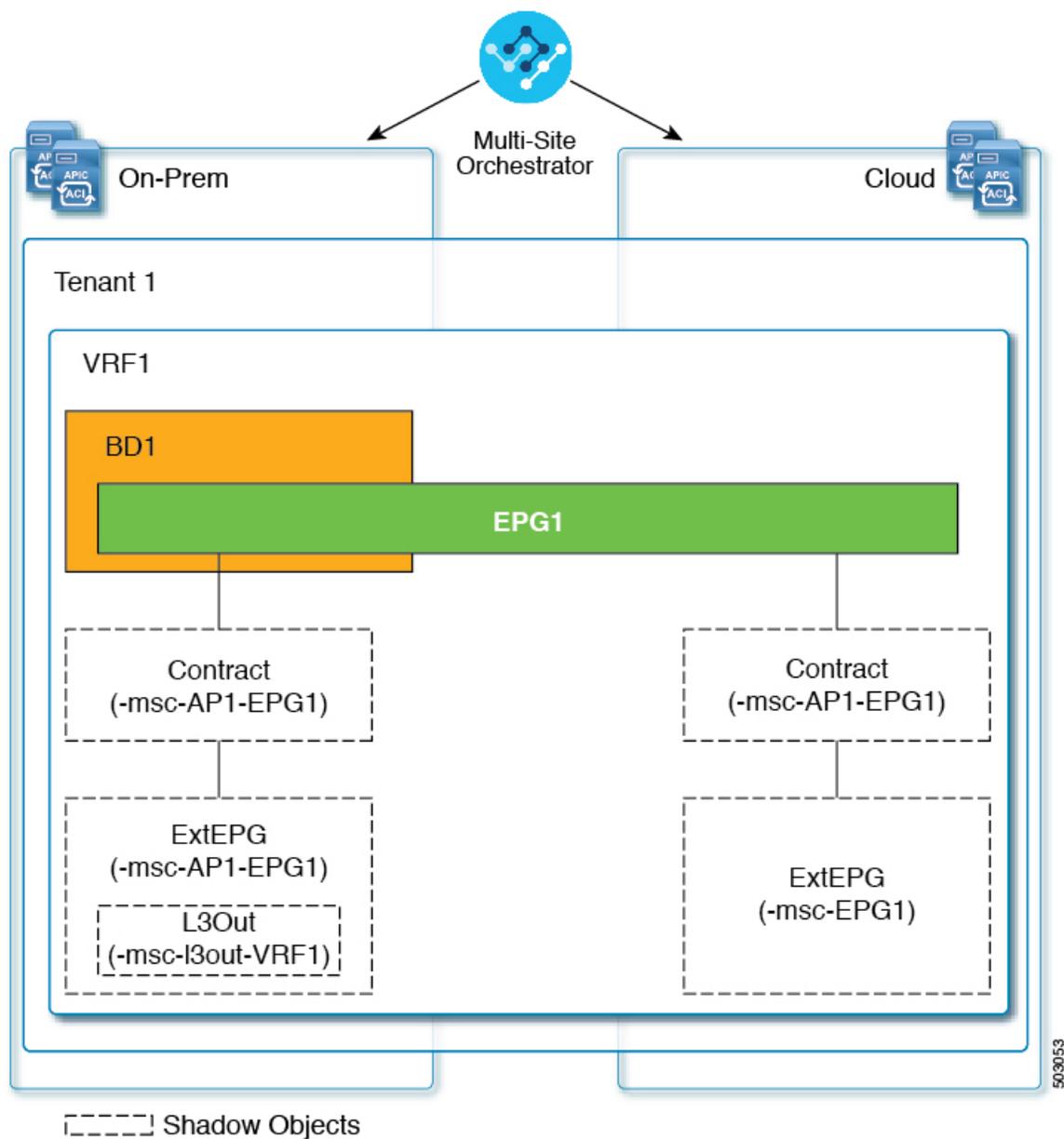
マルチキャストの場合、シャドウ オブジェクトは、マルチキャスト ソースが接続され、オプションが EPG レベルで明示的に設定されている EPG/BD に対してのみ作成されます。

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



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。
