ACI ファブリックの Nexus Dashboard Orchestrator スキーマとアプリケーション テンプレート、リリース 4.3.x

目次

シャドウ オブジェクト

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

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

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

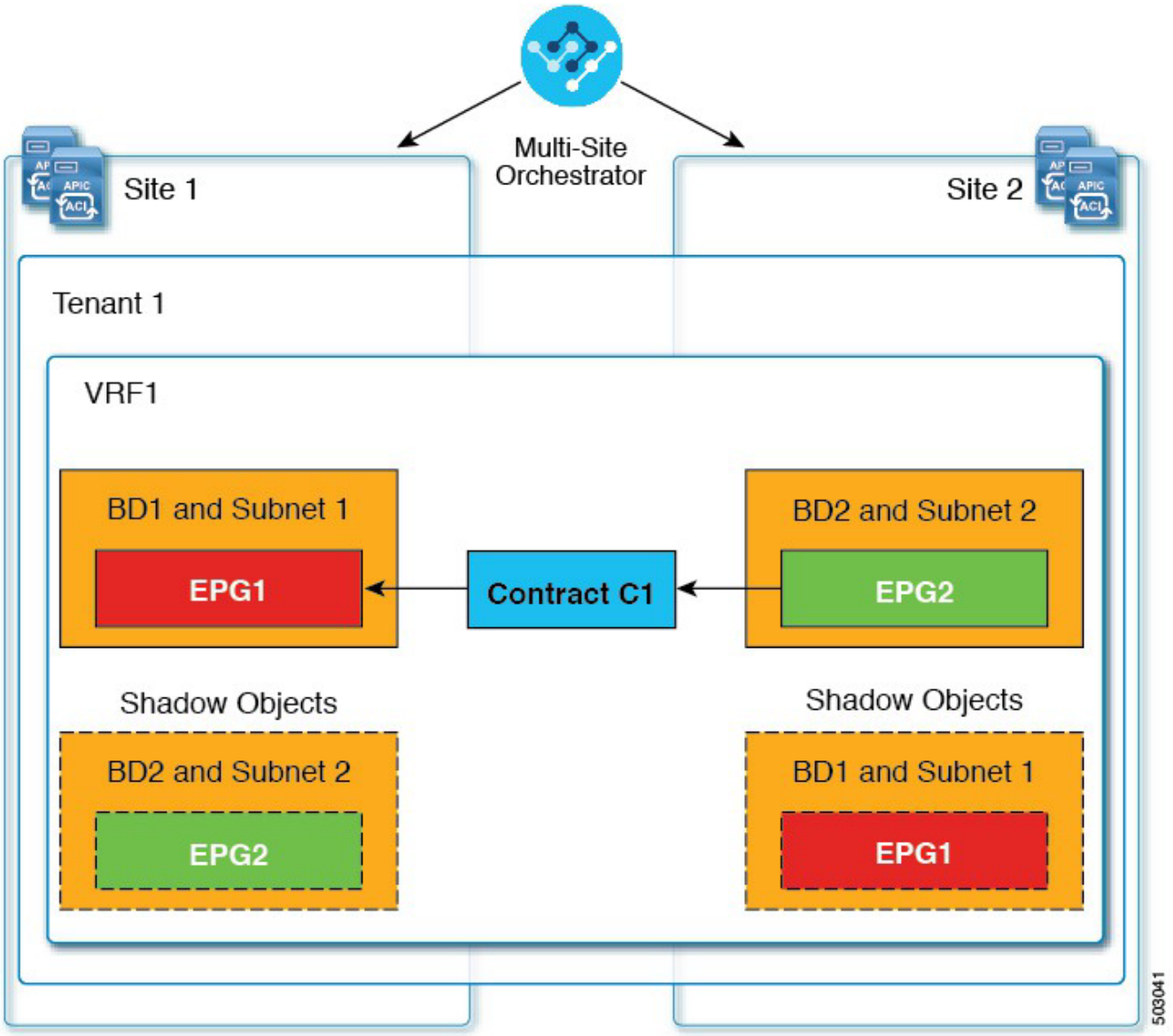

図 1. 基本的なシャドウ EPG

次のオブジェクトはシャドウ オブジェクトになる場合があります。

- VRF

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

ファブリックが APIC リリース 5.0(2) 以降で実行されている場合、APIC GUI でシャドウ オブジェクトを選択すると、 が表示されます。これはサイト間ポリシーをサポートするために、MSC からプッシュされたシャドウ オブジェクトです。このオブジェクトを変更または削除しないでください。メイン GUI ペイン上部の警告。さらに、VMM ドメインの一部ではないシャドウ EPG にはスタティック ポートがない一方で、シャドウ BD には、{FabricControllerShortName} GUI で **[**デフォルト **SVI** ゲートウェイなし（**No Default SVI Gateway**）**]** のオプションがあります。

シャドウ オブジェクトのその他の使用例

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

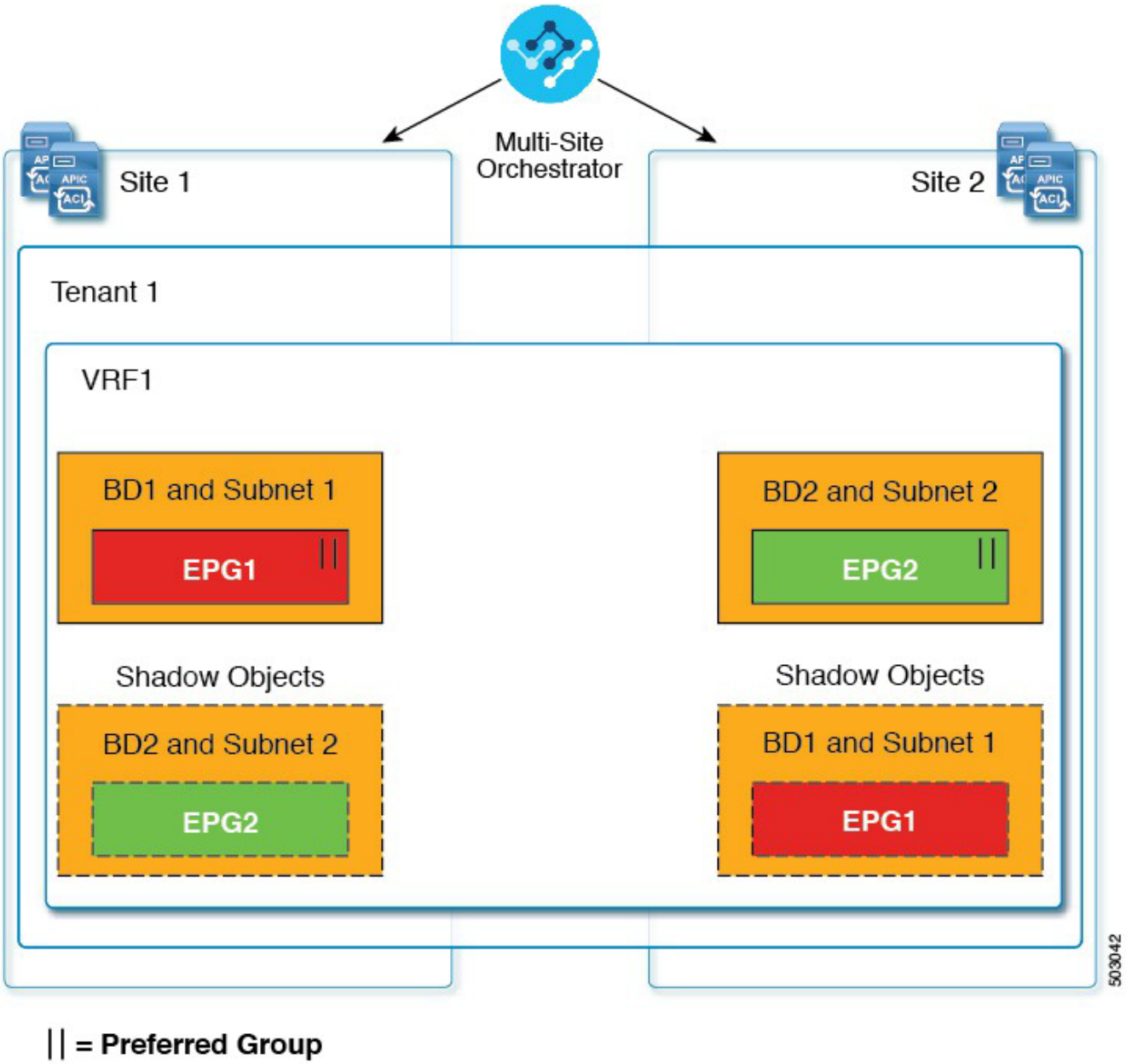

図 2 優先グループ

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

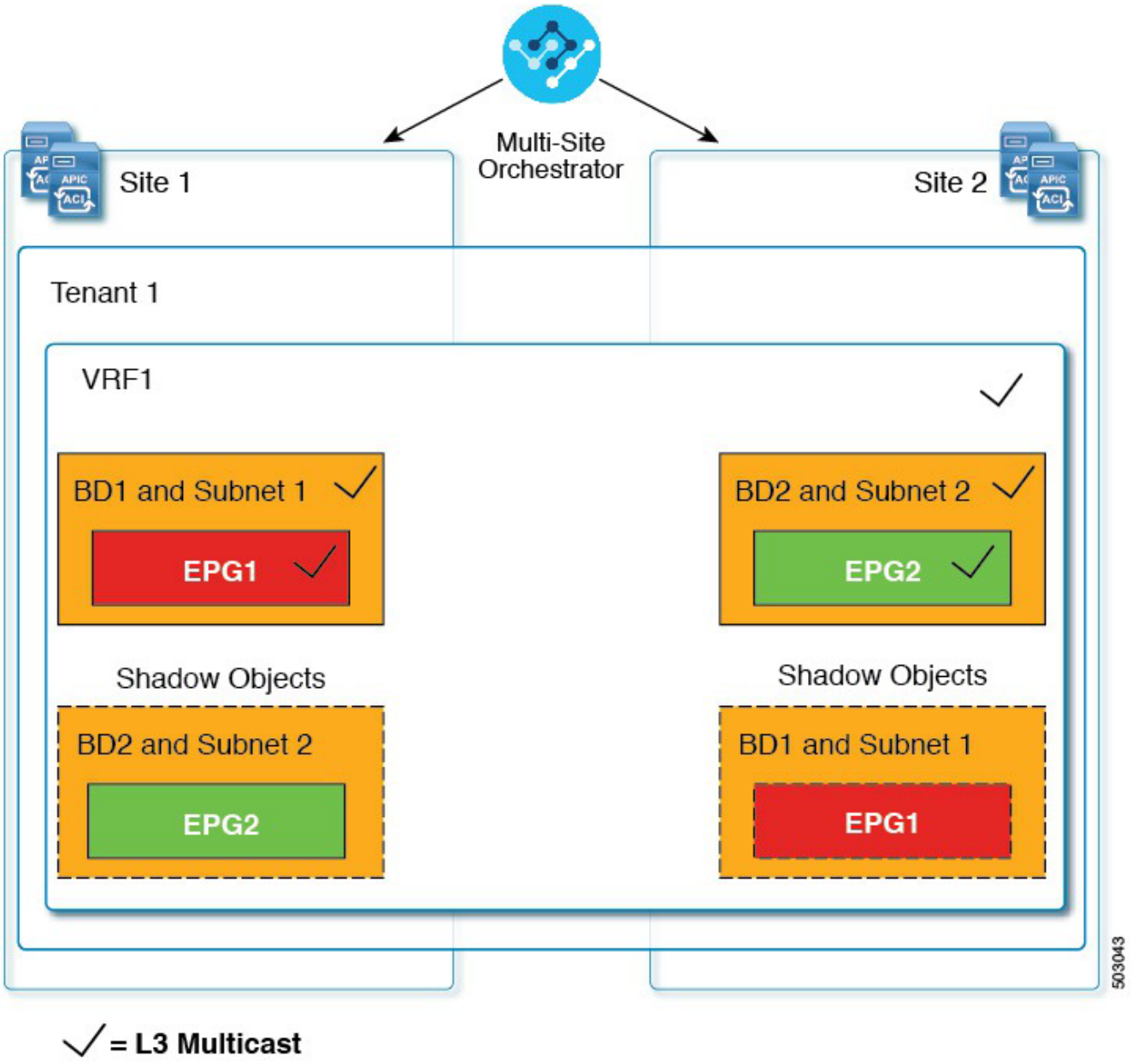

図 3. L3 マルチキャスト

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

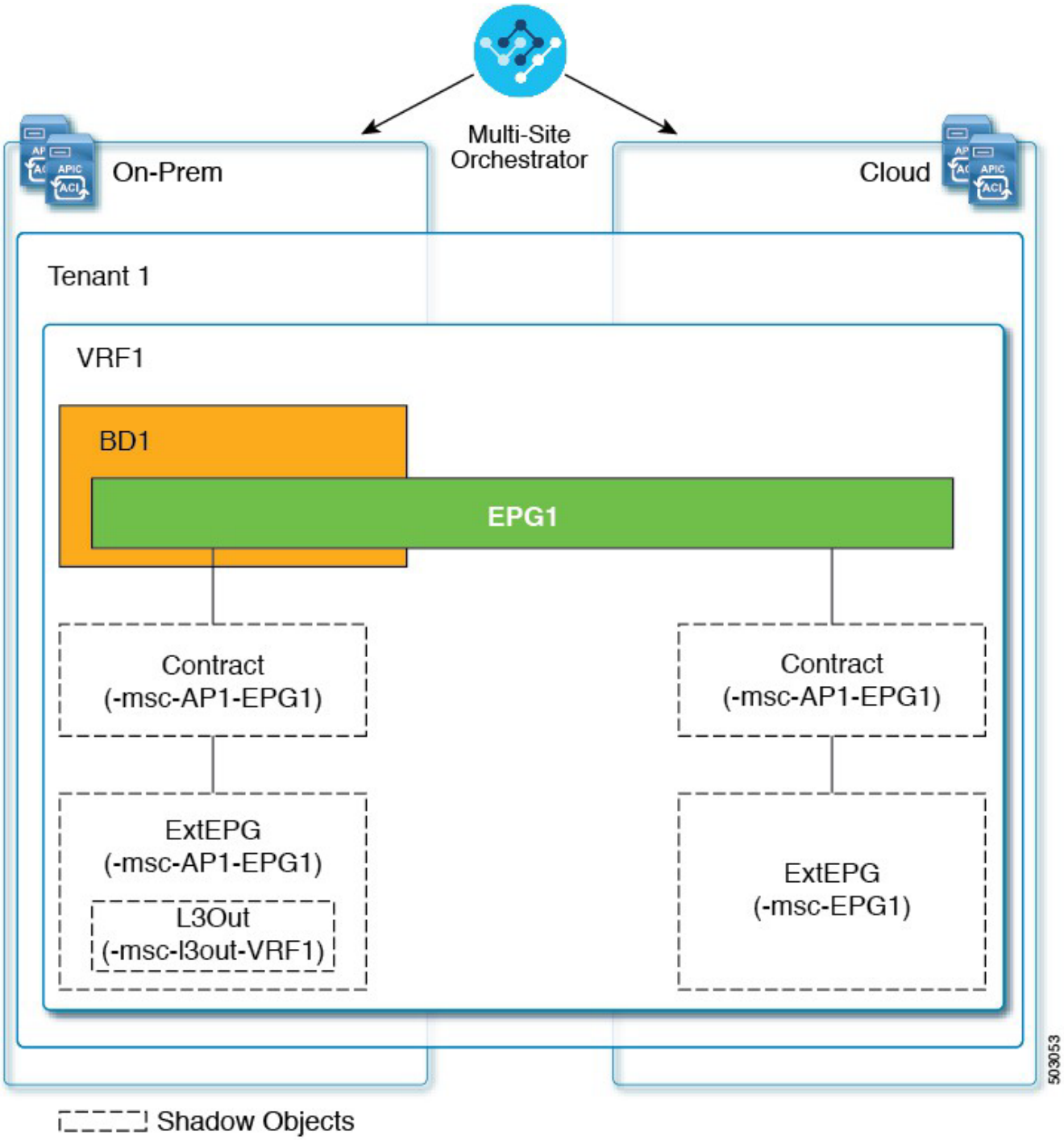

図 4 ハイブリッドクラウド

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

APIC GUI でのシャドウ オブジェクトを非表示にする

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

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

- このオプションは、Orchestrator からグローバルに設定することはできません。また、このセクションで説明するように、

各サイトの APIC で直接設定する必要があります。

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

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

    ファブリックの APIC の前に Orchestrator をアップグレードする場合、サイトのオブジェクトはタグ付けされず、フラグを設定するためにファブリックをアップグレードした後に構成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。
  1. サイトの APIC にログインします。
  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。
  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。
  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。

スキーマとテンプレートの作成

始める前に：

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

  は、「テナントとテナント ポリシー テンプレート」を参照してください。

1. Cisco Nexus Dashboard にログインし、Cisco Nexus Dashboard Orchestrator サービスを開きます。
2. スキーマを新規作成します。
   a. 左のナビゲーション ペインから、**[構成（Configure）] > [テナント テンプレート（Tenant Template）]** を選択します。
   b. [スキーマ（Schema）] ページで、**[スキーマの追加（Add Schema）]** をクリックします。
   c. スキーマ作成ダイアログで、スキーマの **[名前 (Name)]** と説明（オプション）を入力し、**[追加（Add）]** をクリックします。

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

3. テンプレートを作成します。
   a. スキーマのページで、**[新しいテンプレートの作成（Create New Template）]** をクリックします。
   b. **[テンプレート タイプの選択（Select a Template type）]** ウィンドウで、[ACI マルチクラウド（ACI Multi-Cloud）] を選択し、**[追加（Add）]** をクリックします。

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

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

          自律サイトは、定義により孤立したものであり、サイト間接続が一切ないので、サイト間にわたるシャドウ オブジェクト構成はありません。そしてサイト間トラフィック フローのスパイン スイッチ内で pctag またはVNID のクロスプログラムは行われません。

          自律テンプレートは、高い展開拡張を許可します。

        次のセクションでは、主にこのタイプのテンプレートに焦点を当てます。

      - **[NDFC]**：Cisco Nexus Dashboard Fabric Controller（以前のデータセンター ネットワーク マネージャ）サイト用に設計されたテンプレート。

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

Fabrics』を参照してください。

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

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

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

d. （任意）**[**説明 **(Description)]** を入力します。

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

   新しいスキーマを作成するために使用しているユーザ アカウントは、そのスキーマに追加しようとしているテナントに関連付けられている必要があることに注意してください。そうしないと、テナントはドロップダウン リストで使用できなくなります。ユーザー アカウントとテナントの関連付けについては、「テナントとテナント ポリシー テンプレート」に 説明されています。

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

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

g. この手順を繰り返して、追加のテンプレートを作成します。

   スキーマとテンプレートの設計の詳細については、「スキーマとテンプレートの設計の 考慮事項」を参照してください。

4. テンプレートをサイトに割り当てます。

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

   a. テンプレート ビュー ページで、**[**アクション（**Actions**）**]** をクリックして、**[**サイトの追加/削除（**Add/Remove Sites**）**]** を選択します。

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

次に行う作業：

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

APIC サイトからのスキーマ要素のインポート

始める前に：

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、[CiscoMSCShortName] 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。

（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。

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。
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（Template）]** を選択します。
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。
4. **[<site-name> からインポート（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。

   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。

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。

   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。

6. **[インポート（Import）]** をクリックします。

VRF の設定

始める前に：

「スキーマとテンプレートの作成」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、VRF の作成方法を説明します。

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。
2. VRF 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）] > [VRF]** を選択します。

      または、**[VRF（VRFs）]** エリアまでスクロールして、**[VRF の作成（Create VRF）]** をクリックします。

   b. プロパティ 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。
3. （オプション）1 つ以上の **[注釈（Annotations）]** を追加します。

   メタデータの任意の key:value ペアを注釈（tagAnnotation）としてオブジェクトに追加できます。注釈は、説明、個人スクリプトまたは API 呼び出しのマーカー、モニタリング ツールまたは Nexus Dashboard Orchestrator などのオーケストレーション アプリケーションのフラグなど、必要なカスタム目的のために提供されます。APIC はこれらの注釈を無視し、それらを他のオブジェクト データとともに格納するだけなので、APIC によって課される形式またはコンテンツの制限はありません。

4. VRF の **[オンプレミス プロパティ（On-Premises Properties）]** を構成します。
   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（enforce）] モードにロックされることに注意してください。

      ただし、これを使用して、インポート後、[非適用（unenforced）] 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（enforced）] 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 [適用（enforced）] モードに変換してサイト間でのストレッチ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（unenforced）] から [適用（enforced）] 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 **[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。

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。

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

詳細については、「EPG 優先グループの概要と制限事項」を参照してください。

f. （オプション）VRF の **[BD 適用ステータス（BD Enforcement Status）]** を有効にします。

特定のブリッジ ドメインの EPG からサーバをデフォルト設定することにより、別のブリッジ ドメインの SVI（サブネット）に ping を実行できます。ホストが属するブリッジ ドメインの SVI だけに ping を実行できるようにホストを制限する場合は、VRF でこの [BD 適用ステータス（BD Enforcement Status）] オプション構成を有効にできます。これは、サーバーが属するブリッジ ドメインとは異なるブリッジ ドメインのサブネット IP アドレスへの ICMP、TCP、および UDP トラフィックをブロックします。

ブリッジ ドメインの設定

始める前に：

- 「スキーマとテンプレートの作成」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 の構成」の説明に従って、VRF を作成しておく必要がありま

す。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。

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。
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、**[ブリッジ ドメインの作成（Create Bridge Domains）]** をクリックします。

   b. プロパティ 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。
3. （オプション）1 つ以上の **[注釈（Annotations）]** を追加します。

   メタデータの任意の key:value ペアを注釈（tagAnnotation）としてオブジェクトに追加できます。注釈は、説明、個人スクリプトまたは API 呼び出しのマーカー、モニタリング ツールまたは Nexus Dashboard Orchestrator などのオーケストレーション アプリケーションのフラグなど、必要なカスタム目的のために提供されます。APIC はこれらの注釈を無視し、それらを他のオブジェクト データとともに格納するだけなので、APIC によって課される形式またはコンテンツの制限はありません。

4. **[オンプレミス プロパティ（On-Premises Properties）]** を構成します。
   a. **[仮想ルーティングと転送（Virtual Routing & Forwarding）]** ドロップダウンから、ブリッジ ドメインを選択します。
   b. （オプション）**[L2 ストレッチ(L2 Stretch)]** を有効にします。
   c. （オプション）**[サイト間 BUM トラフィック許可 (Intersite BUM Traffic Allow)]** を有効にします。

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

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

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

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

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

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

Layer 3 マルチキャストの詳細については、「レイヤ 3 マルチキャスト」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 スイッチは、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。

L2 不明ユニキャスト設定を変更すると、このブリッジ ドメインに関連付けられた EPG に
接続されたデバイスへのインターフェイスで、トラフィックがバウンス（ダウン状態アップ状態）します。

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

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

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

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

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

- [フラッド（Flood）]（デフォルト）：不明な IPv6 マルチキャスト トラフィックは、このブリッジ ドメインに関連付けられた EPG に接続されたすべての前面パネル ポートでフラッディン

グされます。フラッディングは、ブリッジ ドメインの M ルータポートだけに制限されません。

- [最適化されたフラッド（Optimized Flood）]：ブリッジドメイン内の M ルータポートにのみデータを送信します。

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。

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 スイッチは、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 スイッチに直接転送するか（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。

仮想 MAC と仮想 IP サブネットは、個々のサイトを NDO 管理対象のマルチサイト 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。

5. BD の 1 つ以上の **[**サブネット （**Subnets**）**]** を追加します。

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

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

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

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

このオプションは、BD の [仮想 **MAC** アドレス（**Virtual MAC Address**）] とともに、個々の共通パーベイシブ ゲートウェイ構成から NDOに管理されるマルチサイト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）サブネットを構成する必要があり、その範囲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。

6. （オプション）**[EP 移動検出モード（EP Move Detection Mode）]**を有効にします。

   Gratuitous Address Resolution Protocol（GARP）パケットで受信した情報を使用して、以前に 1 つの MAC アドレス（mac-a）に関連付けられていた特定の IP アドレスが別の MAC アドレス（mac-b）に関連付けられたときに、エンドポイント テーブルを更新します。これは、同じインターフェイスで移動が発生する特定のシナリオに適用されます。

   Cisco ACI は、リーフ スイッチ ポート、リーフ スイッチ、ブリッジ ドメイン、および EPG の間での MAC および IP アドレスの移動を検出できますが、新しい MAC アドレスが古い MAC アドレスと同じインターフェイスおよび同じ EPG からのものである場合、その新しい MAC アドレスへの IP アドレスの移動を検出しません。

   GARP ベースの検出のオプションが有効になっている場合、同じインターフェイスおよび同じ EPG での移動が発生すると、Cisco ACI は GARP パケットに基づいてエンドポイントの移動をトリガします。GARP パケットが同じインターフェイスおよび同じ EPG から着信すると、ユニキャストルーティング、ARP フラッディング、および「GARP ベースの検出」のすべてがブリッジドメインで有効になっている場合にのみエンドポイント学習がトリガーされます。

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

   いくつかのテナント ポリシー テンプレートを構成し、ポリシー オブジェクトに関連付けることができます。詳細については、「テナント ポリシー テンプレートの作成」を参照してください。

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

   いくつかのテナント ポリシー テンプレートを構成し、ポリシー オブジェクトに関連付けることができます。詳細については、「テナント ポリシー テンプレートの作成」を参照してください。

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

   いくつかのテナント ポリシー テンプレートを構成し、ポリシー オブジェクトに関連付けることができます。詳細については、「テナント ポリシー テンプレートの作成」を参照してください。

10. （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、「linkhttps://www.cisco.com/c/dam/en/us/td/docs/dcn/ndo/4x/articles-431/nexus-dashboard- orchestrator-aci-dhcp-relay-431.html#_creating_dhcp_relay_policies[DHCP Relay」を参照してください。

11. 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。

    テンプレート レベルの構成に加えて、「ブリッジ ドメインのサイトローカル プロパティの構成」で説明しているように、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 プロパティの構成

始める前に：

次のものが必要です。

- 「ブリッジ ドメインの構成」 で説明されているように、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構成していること。
- 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。

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。

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。
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。
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 レベルで構成した値が表示されますが、ここでは編集できません。

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）] フラグを構成する必要もあります。詳細については、「使用 例：サイト間 L3Out」を参照してください。

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。

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。

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

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

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

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

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

      択します。これはサブネットのネッ

トワーク可視性です。

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

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

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

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

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

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

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

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

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

g. （オプション）**[プライマリ（Primary）]** オプションを有効にして、サ

ブネットをプライマリとして指定します。1 つのプライマリ IPv4 サブ

ネットと 1 つのプライマリ IPv6 サブネットが可能です。

h. **[保存（Save）]** をクリックします。

アプリケーション プロファイルと EPG の設定

始める前に：

「スキーマとテンプレートの作成」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、コントラクトとブリッジ ドメインが作成されていることも前

提としています。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。

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。
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、**[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。
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、**[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、**[EPG の作成（Create 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。
4. （オプション）EPG に 1 つ以上の **[注釈（Annotations）]** を追加します。
   メタデータの任意の key:value ペアを注釈（tagAnnotation）としてオブジェクトに追加できます。注釈は、説明、個人スクリプトまたは API 呼び出しのマーカー、モニタリング ツールまたは Nexus Dashboard Orchestrator などのオーケストレーション アプリケーションのフラグなど、必要なカスタム目的のために提供されます。APIC はこれらの注釈を無視し、それらを他のオブジェクト データとともに格納するだけなので、APIC によって課される形式またはコンテンツの制限はありません。
5. EPG に **[コントラクト（Contract）]** を追加します。

   コントラクトとフィルタの作成の詳細については、「コントラクトとフィルタの構成」で説明されています。コントラクトを作成済みの場合：

   a. [契約の追加（Add 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。
6. （オプション）EPG に **[EPG 内コントラクト（Intra-EPG Contract）]** を追加します。

   デフォルトでは、EPG ポリシー構成で EPG 内分離を有効にしない限り、EPG 内のエンドポイント間の通信はオープンです。

   EPG 内コントラクトでは、プロトコル、ポート、およびコントラクトのフィルタで指定されたその他のオプションに基づいて、EPG 内で許可されるトラフィックを指定できます。

   a. **[EPG 内コントラクト（Contract）]** エリアで、**[コントラクトの追加（Add 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。

7. **[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。

8. (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。

9. (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 [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。

10. (オプション) EPG 内分離を有効にします。

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

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

11. (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、「レイヤ 3 マルチキャスト」を参照してください:

12. (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、

「EPG 優先グループの概要と制限」を参照してください。

13. 必要に応じて、EPGのサイトローカル プロパティを構成します。

    テンプレート レベルの構成に加えて、「EPG のサイトローカル プロパティの構成」で説明しているように、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 プロパティの構成

始める前に：

次のものが必要です。

- 「アプリケーション プロファイルと EPG の構成」で説明されているように、アプリケーション プロファイルと EPG を作成し、テンプレート レベルのプロパティを構成していること。
- EPG 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。

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。

1. EPGでテンプレートを含むスキーマを開きます。
2. スキーマ ビューの **[概要を表示（View <Overview>）]** ドロップダウンから、EPG を含むテンプレートを選択します。
3. テンプレート ビューのメイン ペインで、**[<site-name>]** タブをクリックして、テンプレートのサイト固有のプロパティを選択します。
4. メイン ペインで、サイトローカル プロパティを更新する EPG をクリックします。

   これにより、EPG の [プロパティ（Properties）] ペインが開きます。ほとんどのフィールドでは、テンプレート レベルで構成した値が表示されますが、ここでは編集できません。

5. **[EPG 管理状態（EPG Admin State）]** を選択します。

   このフィールドは、EPG が infra または mgmt 以外のテナントに属している場合にのみ使用できます。

   EPG がシャットダウン モードの場合、EPG に関連する ACI ポリシー構成はサイトのすべてのスイッチから削除されます。EPG が ACI データ ストアに存在している間は、非アクティブ モードになります。

6. EPG に 1 つ以上の **[サブネット（Subnet）]** 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. 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 でサブネットを構成する必要があり、その範囲は外部にアドバタイズされ、VRF 間で共有されるように設定する必要があります。

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

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

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

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

f. **[OK]** をクリックして保存します。

7. 1 つ以上の **[スタティック ポート（Static ports）]** 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。

インターフェイス構成については、単一のリーフとパスを入力するオプションと、リーフの範囲（例：120 ~ 125）とパスの範囲（例：1/17 ~ 20）を入力するオプションがあります。また、**[リーフ（Leaf）]** の範囲を入力して単一の **[パス（Path）]** に関連付けるか、単一の **[リーフ（Leaf ）]** に **[パス（Path）]** 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 スイッチに送信され、リーフ スイッチ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）]：ポリシーがリーフ スイッチ ソフトウェアにダウンロードされたとき、ハードウェアポ リシー CAM で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 パスを構成することです。

- [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 ポートに組み込み 802.1p モードの EPG を 1 つ構成すると、そのパケットはタグなしの状態でポートを退出します。組み込み 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 ポートに構成すると、
  組み込み 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、組み込み 802.1p EPG は 1 つのみ許可されます。
- [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 スイッチを構成すると、パケットはタグなしの状態でスイッチを退出します。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。

8. 1 つ以上の **[スタティック リーフ（Static Leaf）]** 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。
9. 1 つ以上の **[ドメイン（Domains）]** 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
- ファイバ チャネル
- 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）]：ポリシーがリーフ スイッチ ソフトウェアにダウンロードされたとき、ハードウェアポ リシー CAM で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 にアタッチされる前でも、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。スイッチ上の構成がダウンロードにより事前プロビジョニングされます。

f. VMM ドメインの場合は、追加の設定を構成します。

リリース 4.2(1) 以降では、Cisco Nexus Dashboard Orchestrator から VMM ドメインのいくつかの追加プロパティを直接設定できます。

- [ポート バインディング（Port Bindings）]：次のいずれかのオプションを選択できます。
  - ダイナミック バインド
  - エフェメラル
  - デフォルト
  - 静的バインディング

  ポート バインドに関する詳細は、『*Cisco ACI 仮想化ガイド*』の「Cisco ACI と VMware VDS 統合」を参照してください。
- [NetFlow]：**VMM** ドメインの **NetFlow** を有効にするかどうかを選択します。
- **[**無差別モード（**Promiscuous Mode**）**]**：トランク ポート グループに接続された仮想マシン

の **MAC** アドレス宛てではないユニキャスト トラフィックを許可するか拒否するかを指定します。

- **[MACアドレスの変更（MAC Address Changes）]**：VM 内のネットワーク アダプタの MAC アドレスの変更を許可するか拒否するかを指定します。
- **[偽装送信（Forged Transmits）]**：偽装送信を許可するか拒否するかを指定します。

  偽装転送は、ネットワーク アダプタが偽装と識別したトラフィックの送信を開始した場合に行われます。このセキュリティ ポリシーでは、仮想ネットワーク アダプタの有効なアドレスと、仮想マシンによって生成された 802.3 イーサネット フレーム内の送信元アドレスを比較して、それらが一致することを確認します。

- **[カスタム EPG 名（Custom EPG Name）]**：この VMM ドメインに関連付けられている EPG のカスタム名を指定できます。

  EPG を VMM ドメインに関連付けると、APIC は VMware vCenter ポート グループまたは Microsoft VM ネットワークを自動的に作成します。EPG にカスタム名を付けるオプションがあるため、ポートグループまたは VM ネットワークの管理が容易になります。

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構成し、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 に関連付けられたコントラクトを通して、トラフィックをフィルタします。

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サイト 1 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、サイト 2 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 サイト 2 に作成します。
2. フィルタを作成します。
   a. メインペインで、**[+ オブジェクトの作成（+Create Object）] > [フィルタ（Filter）]** を選択します。

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

   b. 右側のペインで、フィルタの **[表示名（Display Name）]** を入力します。
   c. （任意）**[説明 (Description)]** を入力します。
3. （オプション）1 つ以上の **[注釈（Annotations）]** を追加します。

   メタデータの任意の key:value ペアを注釈（tagAnnotation）としてオブジェクトに追加できます。注釈は、説明、個人スクリプトまたは API 呼び出しのマーカー、モニタリング ツールまたは Nexus Dashboard Orchestrator などのオーケストレーション アプリケーションのフラグなど、必要なカスタム目的のために提供されます。APIC はこれらの注釈を無視し、それらを他のオブジェクト データとともに格納するだけなので、APIC によって課される形式またはコンテンツの制限はありません。
4. フィルタ エントリを作成します。
   a. 右側のペインで、**[+ エントリを追加（+ Add Entry）]** をクリックします。

      フィルタ エントリは、ネットワーク トラフィックの分類プロパティの組み合わせです。次の手順

の説明に従って、1 つ以上のオプションを指定できます。

b. フィルタの **[名前（Name）]** を指定します。

c. **[イーサー タイプ（Ether Type）]** を選択します。

たとえば [ip] です。

d. [IP プロトコル（IP Protocol）] を選択します。

たとえば [icmp] です。

e. **[接続先ポート範囲の開始（Destination Port Range From）]** と **[接続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。両方のフィールドに同じ値を指定すれば、単一のポートを定義できます。または、0 から 65535 の範囲内で、ポートの範囲を定義できます。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）]**（アドレス解決プロトコル）を指定します。

[ARP フラグ（APR Flag）] は、ARP に対する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。両方のフィールドに同じ値を指定すれば、単一のポートを定義できます。または、0 から 65535 の範囲内で、ポートの範囲を定義できます。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（TCP session rules）] 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（stateful）] ACL の動作を構成できます。

k. **[OK]** をクリックして、フィルタを保存します。

l. このフィルタの追加のフィルタ エントリを作成するには、この手順

を繰り返します。フィルタごとに複数のフィルタ エントリを作成し

て割り当てることができます。

5. コントラクトを作成します。
   a. メインペインで、**[+** オブジェクトの作成（**+Create Object**）**] > [**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（**Display Name**）**]** を指定します。
   c. （任意）**[**説明 **(Description)]** を入力します。
   d. （オプション）1 つ以上の **[**注釈（**Annotations**）**]** を追加します。

      メタデータの任意の key:value ペアを注釈（tagAnnotation）としてオブジェクトに追加できます。注釈は、説明、個人スクリプトまたは API 呼び出しのマーカー、モニタリング ツールまたは Nexus Dashboard Orchestrator などのオーケストレーション アプリケーションのフラグなど、必要なカスタム目的のために提供されます。APIC はこれらの注釈を無視し、それらを他のオブジェクト データとともに格納するだけなので、APIC によって課される形式またはコンテンツの制限はありません。

   e. 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。コントラクトは、プロバイダ EPG の範囲外のコンシューマ EPG には適用されません。

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

   f. コンシューマからプロバイダへの方向とプロバイダからコンシューマへの方向の両方に同じフィルタを適用する場合は、**[**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。

[両方向に適用（**Apply both directions**）] を有効にしてコントラクトを作成して展開した場合は、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。 変革後

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、オプションを使用してコントラクトを再作成する必要があります。
ファブリックの設定を正しく変更するために無効になっています。

g. （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。

h. （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。

6. コントラクトにフィルタを割り当てる

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

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

c. フィルタの [アクション（**Action**）] を選択します。

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

d. **[OK]** をクリックして、フィルタをコントラクトに追加します。

e. コントラクトで [両方向に適用（Apply both directions）] オプションを無効にした場合は、他のフィルタ チェーンに対してこの手順を繰り返します。

f. （オプション）複数のフィルタを作成して各コントラクトに割り当てる

ことができます。同じコントラクトに追加のフィルタを作成する場合：

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

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。Cisco 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。

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。

1. Cisco Nexus Dashboard Orchestrator の GUI にログインします。
2. 複製するスキーマを選択します。
   a. 左側のナビゲーション メニューから、**[**構成（**Configure**）**] > [**テナント テンプレート（**Tenant Template**）**]** を選択します。
   b. 複製するスキーマ名の横にある [アクション（Actions）] メニュー（**...**）から、[複製（Clone）] を選択します。
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。

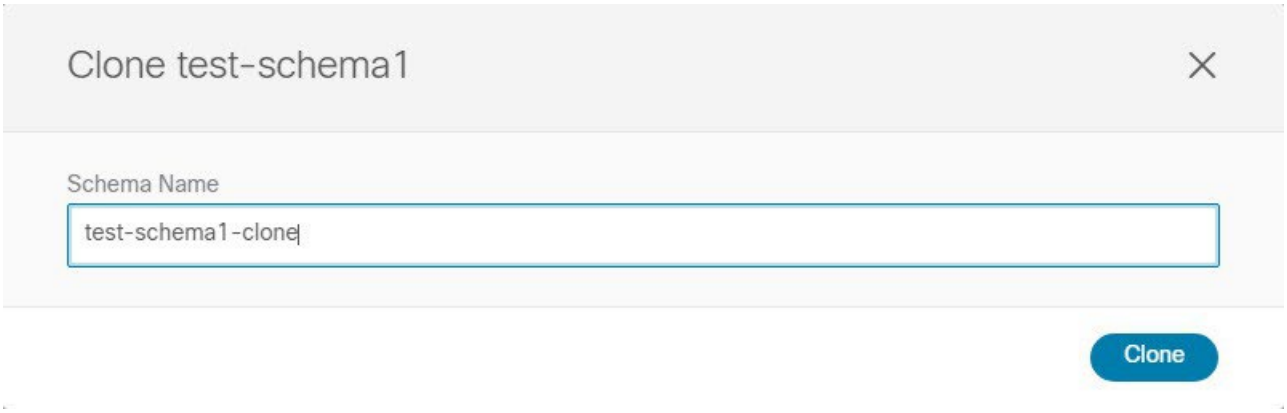

図 5 スキーマの複製

[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、および構成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。

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。

初版：2024 年 3 月 1 日
最終更新日：2024 年 3 月 1 日

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax：408 527-0883