スキーマ管理

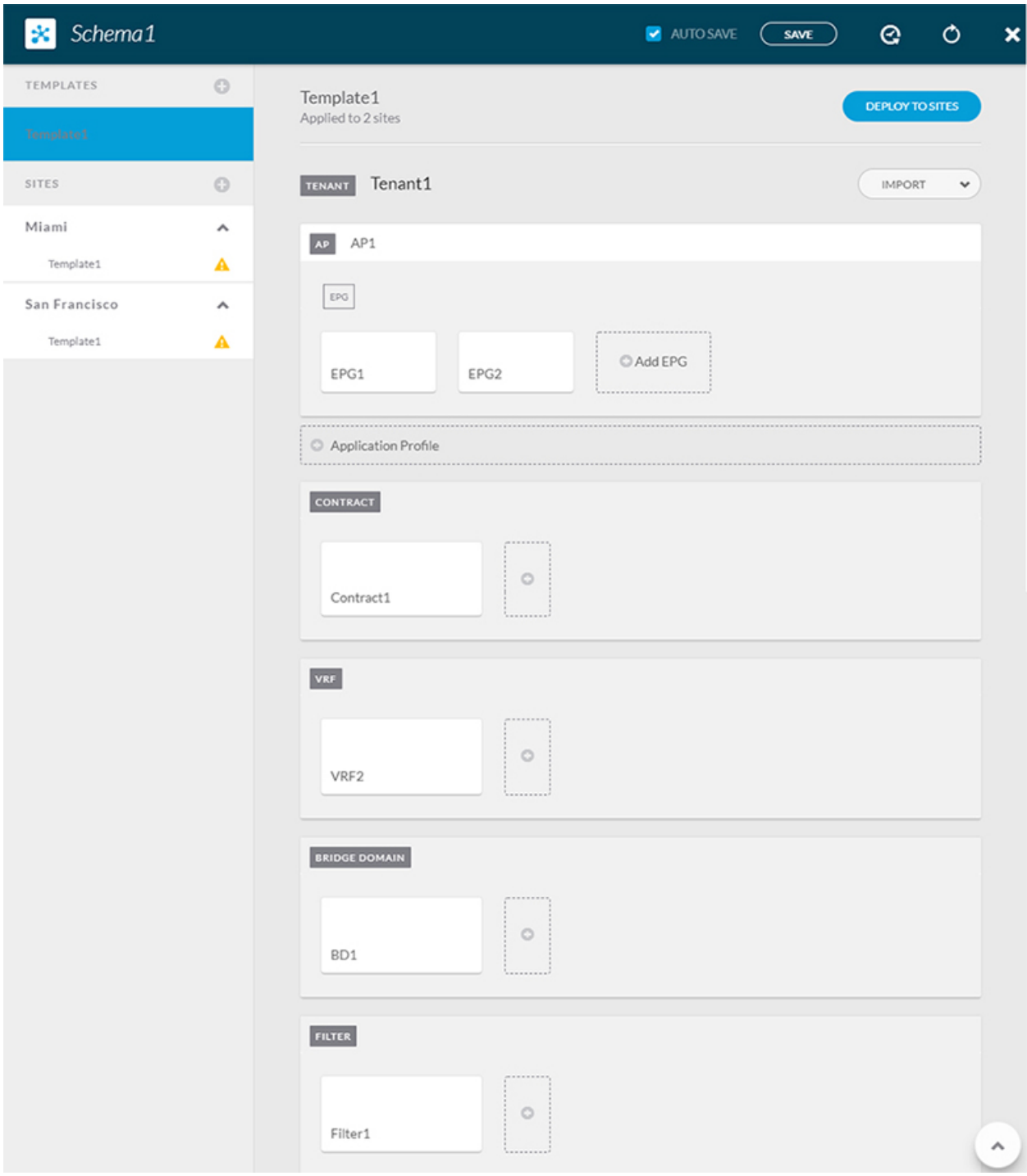
スキーマ設計上の考慮事項

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際には、スキーマの数、テンプレートの数、およびスキーマあたりのオブジェクト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、お使いのリリースに固有の*CISCO APIC、CISCO ACI Multi-Site、および Cisco Nexus 9000 シリーズ ACI モードのスイッチの検証済みスケーラビリティ ガイド*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、単一のテンプレートを展開することです。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することができます。その後、1 つのアプリケーションプロファイルまたは複数のアプリケーションプロファイルをテンプレート内に作成し、それを 1 つ以上のサイトに展開することができます。

図 *1*: 単一スキーマ



マルチサイトスキーマ作成に対するこの簡単なアプローチを上の図に示します。この場合、すべてのオブジェクトが同じスキーマ内で簡単に表示できるようになります。ただし、スキーマごとにサポートされているスキーマまたはテンプレートの数に制限があるため、このアプローチは、これらの制限を超える可能性があるような、大規模な展開には適していません。

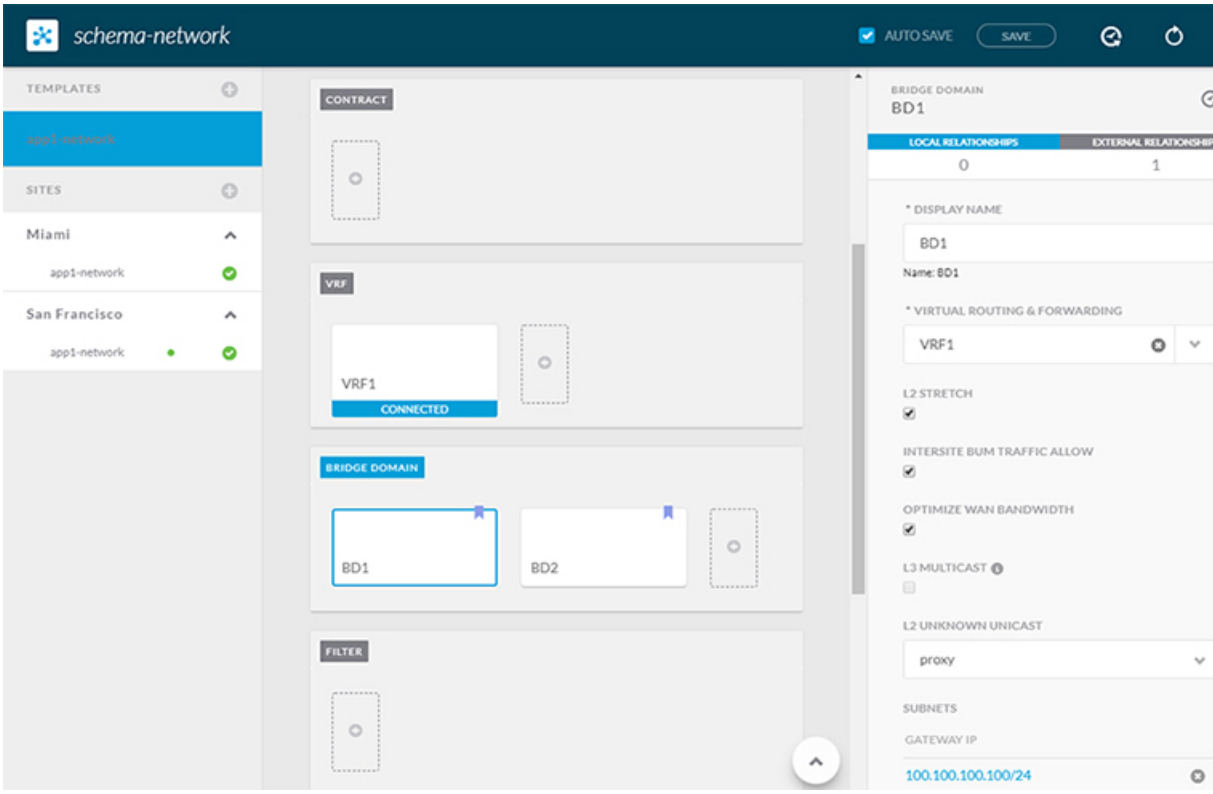
ネットワーク分離での複数スキーマ

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

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

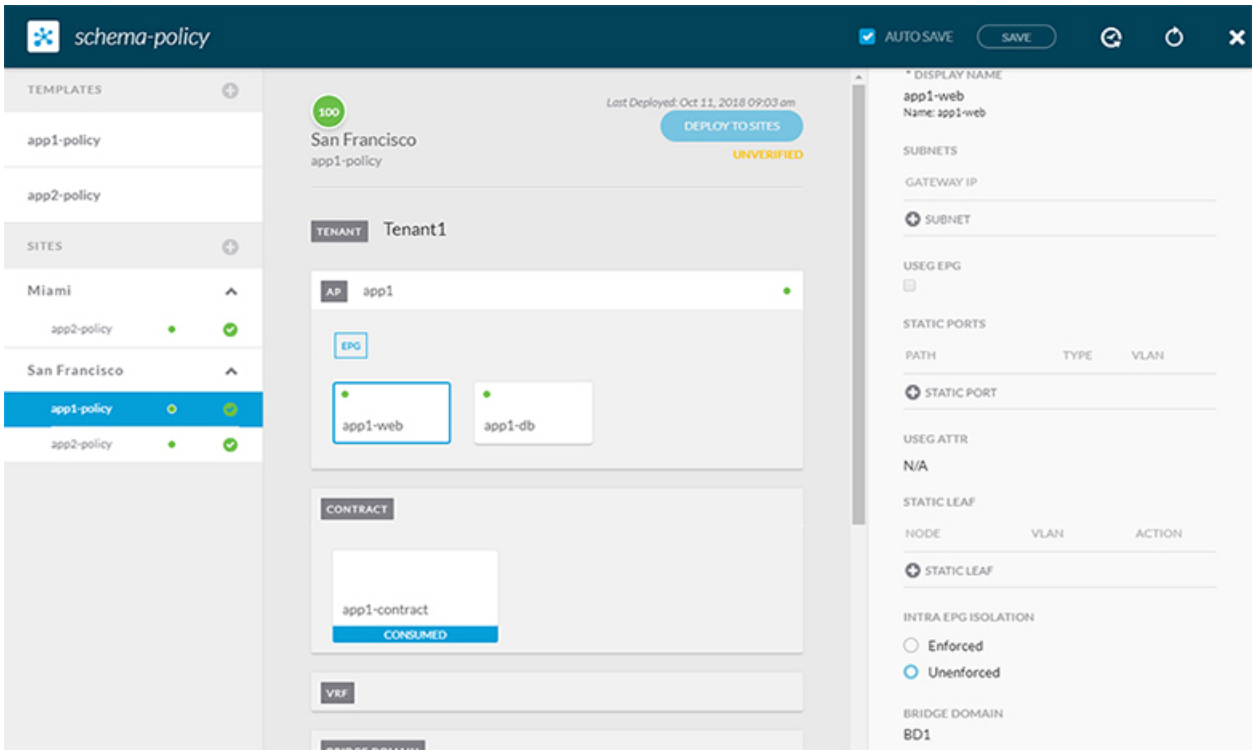
次の図は、VRF、BD、およびサブネットが設定され、2 つのサイトに展開されている単一のネットワーキング テンプレート設定を示しています。

図 *2:* ネットワーク スキーマ



その後、各アプリケーションのポリシーオブジェクトを含む、1つ以上の個別のスキーマを定義します。この新しいスキーマは、前のスキーマで定義されたブリッジドメインなどのネットワーク要素を参照できます。次の図に、2つのアプリケーションテンプレートを含むポリシースキーマを示します。これらのテンプレートの両方が外部スキーマのネットワーキング要素を参照しています。アプリケーションの一方は1つのサイトにローカルであり、他方は2つのサイト間で拡張されます。

図 *3:* ポリシー スキーマ



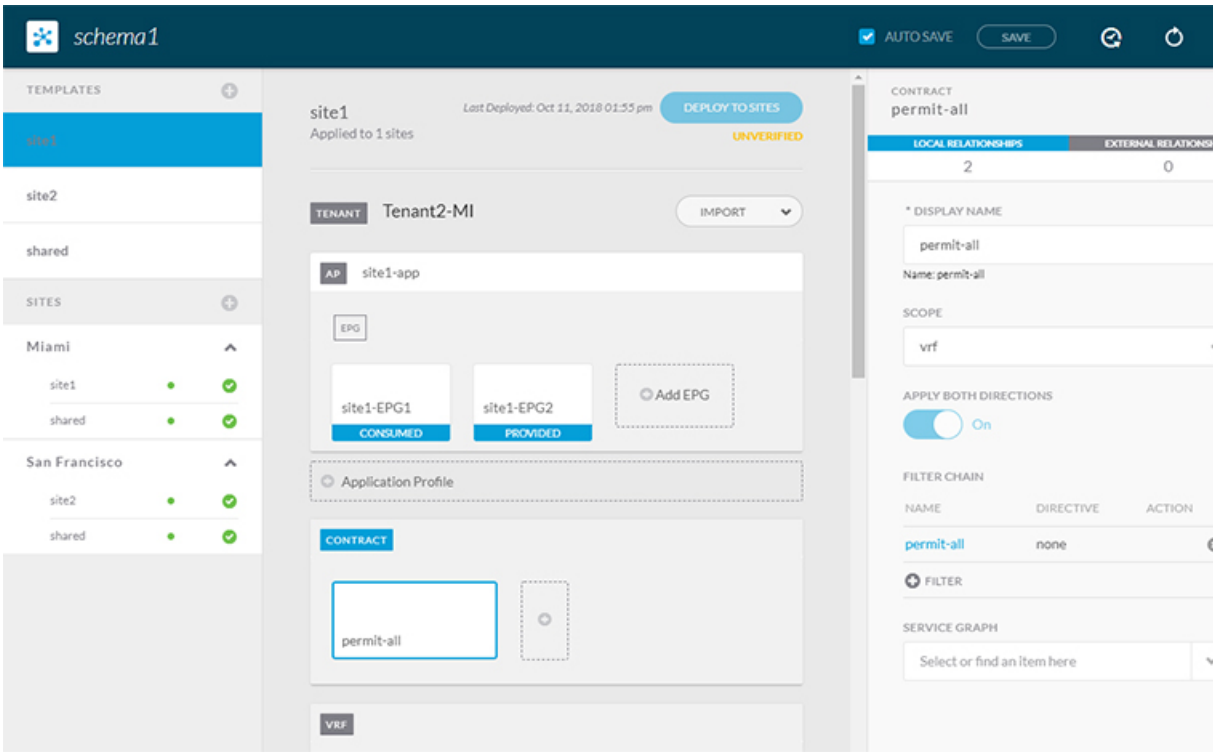
ポリシー スキーマとテンプレートを作成して展開すると、ネットワーク スキーマのネットワーキング オブジェクトに、ポリシー スキーマ要素による外部参照の数が表示されます。外部参照を含むオブジェクトは、上のネットワーク スキーマの図に示すように、リボンのアイコンでも示されます。

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

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 *4*: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に5つのテンプレートという制限を超えるため、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。

使用例のCisco Cloud APICスキーマ設計

Cisco ACI マルチサイトは、リリース 2.1(1) 以降の Amazon Web SERVICES (AWS) とリリース 2.2(1) 以降の Microsoft Azure にインストールされたインストールされた Cisco Cloud APIC をサポートしています。Each cloud deployment can be added to and managed by the マルチサイト Orchestrator as its own APIC site.

次のセクションでは、スキーマの作成と管理に必要な一般的な手順について概説していますが、クラウド APIC サイトでサポートされる特定の使用例のシナリオについては、次のクラウド APIC ドキュメントのランディングページ https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/tsd-products-support-series-home.html にある設定例で詳しく説明されています。

スキーマ 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。
- Cisco APIC テナント ユーザ 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 **[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。

ステップ 2 **[名称未設定のスキーマ (Untitled Schema)]** ページで、作成するスキーマの名前を入力します。

ステップ 3 **[テナントの選択 (Select A Tenant)]** ダイアログ ボックスにアクセスし、ドロップダウン メニューからテナントを選択します。

（注） 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。

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。

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ます。

ステップ 4 オブジェクトをインポートするサイトを選択します。

ステップ 5 [**インポート (Import)**] 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） マルチサイト Orchestrator 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。

アプリケーション プロファイルの設定

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。

ステップ 1 スキーマ編集ビューで、[**+ アプリケーション プロファイル (+ Application Profile)**] をクリックします。

ステップ 2 右側の [プロパティ (properties)] ペインで、アプリケーション プロファイル名を入力します。

ステップ 3 **[AP <名前>]** エリアで、**[+ EPG の追加 (+ Add EPG)]** をクリックして EPG を追加します。

ステップ 4 右側の [プロパティ (properties)] ペインで、EPG の名前を入力します。

ステップ 5 EPG のコントラクトを追加します。

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 6 **[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 7 (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 8 (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 9 (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。

ステップ 10 (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 （28 ページ）

ステップ 11 (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 （26 ページ）

テナントの VRF を設定する

このセクションでは、VRF の設定方法を説明します。

ステップ 1 [スキーマ編集 (Schema edit)] ビューで、**[VRF]** エリアまで下にスクロールし、+ をクリックします。

ステップ 2 右側の [プロパティ (properties)] ペインで、VRF の名前を入力します。

ステップ 3 (オプション) VRF 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 （28 ページ）

ブリッジ ドメインの設定

ステップ 1 [スキーマ編集 (Schema edit)] ビューで、**[ブリッジ ドメイン (Bridge Domain)]** エリアまで下にスクロールし、+ をクリックします。

ステップ 2 右側のプロパティ ペインで、以下のブリッジ ドメインの詳細を入力します。

- **[表示名 (Display Name)]** フィールドに BD 名。
- **[仮想ルーティングと転送 (Virtual Routing and Forwarding)]** フィールドに VRF。
- 必要に応じて、**[L2 ストレッチ (L2 STRETCH)]** チェックボックスをオンにします。
- **[L2 ストレッチ (L2 STRETCH)]** を有効にした場合は、**[サイト間 BUM トラフィックを許可 (INTERSITE BUM TRAFFIC ALLOW)]** も有効にできます。
- **[L2 ストレッチ (L2 STRETCH)]**を有効にしていない場合は、**[L2 不明なユニキャスト (L2 UNKNOWN UNICAST)]** フィールドの **[プロキシ (proxy)]** または **[フラッド (flood)]** を選択できます。

ステップ 3 (オプション) ブリッジ ドメインに 1 つまたは複数のサブネットの追加を選択できます。

a) **[+サブネット (+Subnet)]** をクリックします。

[サブネットの追加 (Add 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を入力します。

c) **[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)]** を選択します。

d) 必要に応じて、**[VRF 間で共有 (Shared Between VRFs)]** をオンにします。

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

f) 必要に応じて、**[クエリア(Querier)]** チェックボックスをオンにします。

g) **[保存 (SAVE)]** をクリックします。

コントラクトのフィルタの設定

ここでは、コントラクトのフィルタを設定す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 [スキーマ編集 (Schema edit)] ビューで、**[フィルタ (Filter)]** エリアまで下にスクロールし、**+** をクリックします。

ステップ 2 右側の [プロパティ (properties)] ペインで、フィルタの名前を入力します。

ステップ 3 **[+エントリ (+ Entry)]** をクリックし、フィルタ エントリを追加します。

開いた [エントリの追加 (Add Entry)] ウィンドウで、次の情報を入力します。

a) フィルタ エントリの名前。

b) (オプション) フィルタ エントリの説明。

c) EPG の通信のフィルタ処理を行うために、必要に応じて詳細を入力します。

たとえば、フィルタを通過する HTTPS トラフィックを許可するエントリを追加するには、次のように選択します。

- **EtherType**—`IP`
- **[IP プロトコル (IP Protocol)]**—`tcp`
- **宛先ポートの範囲 (先頭) (Destination Port Range From)**: `https`

  宛先ポートの範囲 (末尾) (Destination Port Range To): `https`

d) **[保存 (SAVE)]** をクリックします。

コントラクトの設定

このセクションでは、コントラクトの設定方法を説明します。

ステップ 1 [スキーマ編集 (Schema edit)] ビューで、**[コントラクト]** エリアまで下にスクロールし、**+** をクリックします。

ステップ 2 右側のプロパティ ペインで、コントラクトの名前を入力します。

ステップ 3 ドロップダウン メニューを使用して、**[範囲 (Scope)]** の値を選択します。

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`
- `tenant`

- global

ステップ 4 **[両方向の適用 (Apply Both Direction)]** トグル ボタンをクリックして、コントラクトで指定されたフィルタを一方向または両方向に適用します。

デフォルトの設定は **[ON]** です。

ステップ 5 コントラクト フィルタを追加します。

a) **[+フィルタ (+ Filter)]** をクリックします。

b) **[フィルタ チェーンの追加 (Add Filter Chain)]** ダイアログで、**[名前 (Name)]** フィールドをクリックして、フィルタを選択するか検索します。

c) (オプション) **[指令 (Directives)]** フィールドで、使用可能な指令を選択します。

d) **[保存]** をクリックします。

ステップ 6 **[両方向に適用 (Apply Both Direction)]** オプションを無効にした場合は、もう一方の方向に2番目のフィルタチェーンを追加します。

外部 EPG の設定

このセクションでは、外部 EPG を設定する方法について説明します。

始める前に

- テナントと VRF が拡大するすべてのサイト上の Cisco APIC 内で L3Out を作成します。
- 各 L3Out の VRF は、すべてのサイトで同じである必要があります。VRF の変更 APIC 外部 Epg を展開した後、L3Out をリセットし、再設定し、サイトの外部 EPG を再配置必要があります。

ステップ 1 [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、[+ をクリックします。

ステップ 2 右側の [プロパティ (properties)] ペインで、外部 EPG のタイプを選択し、名前を指定します。

クラウド外部 EPG の詳細については、Cisco Cloud APIC のマニュアルを参照してください。

ステップ 3 **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、この外部 EPG に関連付ける VRF を選択します。

ステップ 4 EPG が通信するために必要なコントラクトを追加します。

（注） 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 **[オンプレミスプロパティ (On-Prfem Properties)]** エリアで、この外部 EPG の L3Out を選択します。

L3Out の設定

このセクションでは、マルチサイトOrchestrator GUI を使用して L3Out 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 L3Out 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。VRF も Orchestrator で作成されるので、L3Out を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

ステップ 1 [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。

ステップ 2 右側の [プロパティ (properties)] ペインで、L3Out の表示名と、それに対応する仮想ルーティングおよび転送 (VRF) を入力します。

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。マルチサイト 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。

これらの マルチサイト Orchestrator GUI ページの機能の詳細については、Cisco ACI マルチサイトOrchestrator GUI の概要 を参照してください。

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異なるテンプレートとスキーマに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 マルチサイト Orchestrator 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、**[スキーマ (schema)]** 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。

シャドウ EPG と BD

拡張 VRF または共有サービスの使用例において、サイトローカル EPG 間にコントラクトが存在し、プロバイダとコンシューマが異なる VRF にあり、テナント コントラクトを通じて通信する場合、EPG とブリッジ ドメイン (BD) はリモート サイトでミラーリングされます。これらの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ますが、実際にはサイトの 1 つだけに展開されています。これらのミラーされたオブジェクトは、「シャドウ EPG または BD」と呼ばれます。

たとえば、プロバイダ サイト グループのテナントと VRF がサイト 1 とサイト 2 に拡張され、コンシューマ サイト グループのテナントと VRF がサイト 3 とサイト 4 に拡張されている場合、サイト 1、サイト 2、サイト 3、サイト 4 の APIC GUI では、両方のテナントとポリシーを表示できます。これらは、それぞれのサイトに直接展開されている場合と同じ名前で表示されます。

シャドウ オブジェクトはまた、優先グループ、vzAny、Layer 3 マルチキャスト使用例でも作成されます。

（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。

以下のオブジェクトは、サイト間で拡大するときにシャドウできます。

- 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

APIC GUI でシャドウ オブジェクトを選択する場合、 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 いよりプッシュされたシャドウ オブジェクトです。このオブジェクトは、変更を加えたり、削除したりしないでください。メイン GUI ペインの上部に の警告が表示されます。さらに、VMM ドメインの一部ではないシャドウ EPG にはスタティック ポートがないいぽプで、シャドウ BD は、APIC GUI で **[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)]**のオプションがあります。これらのオプションについては、次のように確認できます。

ステップ 1 同じ名前を持つ EPG のペアのうちのシャドウ EPG を識別するには、APIC GUI で、**[テナント (Tenants)]** > ***[<テナント名>]*** > **[アプリケーション プロファイル (Application Profiles)]** > ***[<アプリケーションプロファイル名>]*** > **[アプリケーション EPG (Application EPGs)]** > ***[<EPG 名>]*** > **[静的ポート (Static Ports)]** を選択します。

シャドウ EPG には、静的ポートへのパスはありません。

EPG に VM のみが含まれる VMM ドメイン インテグレーションでは、スタティック ポートもないため、この方法を使用してそれらをシャドウ EPG から区別できないことに注意してください。

ステップ 2 同じ名前を持つ BD のペアのうちのシャドウ BD を識別するには、APIC GUI で、 **Tenants** > ***tenant-name*** > **Networking** > **Bridge Domains** > ***bd-name*** > **Subnets** > ***subnet-name*** を選択します。

シャドウ BD のサブネットでは、**[デフォルト SVI ゲートウェイなし (No Default SVI Gateway)]** が有効になっています。

サイト内 L3Out

リリース 2.2(1) 以前、Multi-Site Orchestrator により管理される各サイトでは、トラフィックをファブリックの外にルートするために設定された固有のローカルL3Outが必要で、それによりしばしば 1 つのサイトのエンドポイントと別のサイトの L3Out に接続されたサービス (ファイアウォール、サーバロードバランサー、またはメインフレーム) の間のコミュニケーションの欠如を導くことがありました。

リリース 2.2(1) は、1 つのサイトにあるエンドポイントが、外部ネットワーク、メインフレーム、またはサービス ノードなどのリモート L3Out を通じて到達可能なエンティティとの接続を確立する多くのシナリオを有効にする機能を追加します。

このような要素として、次のものが挙げられます。

- サイト間の L3Out—別のサイトの L3Out を使用した 1 つのサイトのアプリケーション EPG のエンドポイント。

  L3Out とアプリケーション EPG は、同じまたは異なる VRF とテナントに存在することができます。

- サイト間の L3Out のトランジット—別のサイトの 外部 EPG のエンドポイントと通信する 1 つのサイトの外部 EPG のエンドポイント。

  外部 EPG は、同じまたは異なる VRF とテナントに存在することができます。

- サイト間L3Outの共有サービス—異なるVRFの間でのL3Outの共有またはトランジット。

サイト内 L3Out のガイドラインと制約事項

サイト間 L3Out を構成するときは、次のことを考慮する必要があります。

- サイト間 L3Out は IPv4 と IPv6 に対してサポートされています。
- リリース 2.2(1) 以前のリリースからアップグレードしている場合、サイト ローカル レベルの既存の外部 EPG から L3Out への関連付けは保持されます。さらに、Orchestrator は L3Out の作成とテンプレート レベルでの外部 EPG との関連付けをサポートするようになりました。

L3Out がスキーマ テンプレートで定義されている場合、既存の外部 EPG に対して使用できます。

- L3Out が APIC ですでに定義されている L3Out と**同じ名前**の場合、Orchestrator その L3Out の所有権を取得しますが、L3Out ノードプロファイル、インターフェースプロファイル、プロトコル設定、またはルート制御設定の構成を管理しません。

  次に、Orchestrator からこの L3Out を削除することにすると、それは Orchestrator により管理されなくなりますが、以前から存在する L3Out の構成は APIC に保存されます。

- L3Out が L3Out で定義された APIC とは **異なる名前** がある場合、外部 EPG は、APIC で定義された L3Out から削除され、Orchestrator で定義された L3Out に追加されます。これが APIC で定義された L3Out での唯一の外部 EPG である場合、これにより設定が境界リーフから削除され、トラフィックに影響を与える可能性があります。

- リリース 2.2(1) より前のリリースにダウングレードすることを選択した場合、Orchestrator MSO で作成された L3Out はテンプレートに存在しなくなるため、外部 EPG と L3Out 間のテンプレート レベルの関連付けは削除されます。この場合、サイト ローカル レベルで、外部 EPG と L3Out の関連付けを手動で再構成する必要があります。ダウングレード中、サイトローカルの関連付けは保持されます。

- これで、1 つのサイトのブリッジ ドメインを別のサイトの L3Out に関連付けることができますが、両方が同じテナントにある必要があります。

- サイト間 L3Out に関連付けられた VRF のポリシー制御施行方向は、デフォルトの入力モードで構成されたままにする必要があります。

- 次のシナリオは、サイト間 L3Out およびリモートリーフ (RL) ではサポートされていません。

  - 別々のサイトに関連付けられた RL ペアにデプロイされた L3Out 間のトランジット ルーティング

  - リモート サイトに関連付けられた RL ペアに展開された L3Out と通信するサイトに関連付けられた RL ペアに接続されたエンドポイント

  - リモート サイトに関連付けられた RL ペアに展開された L3Out と通信するローカル サイトに接続されたエンドポイント

  - リモート サイトに展開された L3Out と通信するサイトに関連付けられた RL ペアに接続されたエンドポイント

- 次の他の機能は、ACI マルチサイトのサイト間 L3Out ではサポートされていません。

  - 別のサイト L3Out を介して外部ソースからマルチキャストを受信するサイト内のマルチキャスト レシーバー。サイトで外部ソースから受信したマルチキャストが他のサイトに送信されることはありません。サイトのレシーバーが外部ソースからマルチキャストを受信する場合、ローカルの L3Out で受信する必要があります。

- PIM-SM Any Source Multicast (ASM) を使用して外部レシーバーにマルチキャストを送信する内部マルチキャスト ソース。内部マルチキャスト ソースは、ローカル L3Out から外部ランデブー ポイント (RP) に到達できる必要があります
- GOLF
- 外部 EPG の優先グループ

ルーティング可能な TEP アドレスの設定

サイト間 L3Out には、各ポッドの境界リーフ スイッチにルーティング可能な TEP アドレスが必要です。ルーティング可能な TEP プールがすでに設定されている場合 (たとえば、リモート リーフなどの別の機能のために) は、同じプールを使用できます。それ以外の場合は、この項で説明されているように、Orchestrator GUI で TEP プールを追加できます。新しい TEP プールを追加する場合は、ファブリック内の他の TEP プールと重複しないようにする必要があることに注意してください。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインで、**[スキーマ (schema)]** を選択します。

ステップ 3 メインペインの右上にある **[インフラの設定 (Configure Infra)]** をクリックします。

ステップ 4 左側のサイドバーで、設定するサイトを選択します。

ステップ 5 メイン ウィンドウで、サイト内のポッドをクリックします。

ステップ 6 右側のサイドバーで、**[+ TEP プールを追加 (+Add TEP Pool)]** をクリックします。

ステップ 7 **[TEP プールの追加 (Add TEP pool)]** ウィンドウで、そのサイトに対して設定するルーティング可能な TEP プールを指定します。

（注） 追加しようとしている TEP プールが他の TEP プールまたはファブリックアドレスと重複していないことを確認する必要があります。

ステップ 8 このプロセスを、サイト間の L3Outs を使用する予定のサイトおよびポッドごとに繰り返します。

サイト間 L3Out および VRF の作成またはインポート

ここでは、L3Out を作成し、それを Orchestrator GUI で VRF に関連付ける方法について説明します。これは APIC サイトにプッシュされるか、または APIC サイトの 1 つから既存の L3Out をインポートします。次に、この L3Out を外部 EPG に関連付け、その外部 EPG を使用して特定のサイト間 L3Out の使用例を設定します。

（注） L3Out に割り当てる VRF は、任意のテンプレートまたはスキーマにすることができますが、L3Out と同じテナントに存在する必要があります。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインで、**[スキーマ (schema)]** を選択します。

ステップ 3 [スキーマ (schema)] を選択し、VRF と L3Out を作成またはインポートするテンプレートを選択します。

複数のサイトに関連付けられているテンプレートで L3Out を作成すると、L3Out がそれらすべてのサイトに作成されます。1 つのサイトに関連付けられているテンプレートで L3Out を作成すると、そのサイトでのみ L3Out が作成されます。

ステップ 4 新しい VRF と L3Out を作成します。

既存の L3Out をインポートする場合は、この手順をスキップします。

（注） Orchestrator で L3Out オブジェクトを作成し、それを APIC にプッシュすることはできますが、L3Out の物理設定は APIC で実行する必要があります。

a) **[VRF]** エリアまで下にスクロールし、+ アイコンをクリックして新しい VRF を追加します。

右側のサイドバーで、VRF の名前を入力します (例: `vrf-l3out`)。

b) **[L3Out]** 領域まで下にスクロールし、+ アイコンをクリックして新しい L3Out を追加します。

右側のスライダで、必要な情報を入力します。

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

d) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、前のステップで作成された VRF を選択します。

ステップ 5 既存の L3Out をインポートします。

前の手順で新しい L3Out を作成した場合は、この手順をスキップします。

a) メイン テンプレート ビューの上部で、**[インポート (Import)]** をクリックします。

b) L3Out をインポートするサイトを選択します。

c) [インポート (Import)] ウィンドウの **[ポリシー タイプ(Policy Type)]** メニューで、[**L3Out**] を選択します。

d) インポートする L3Out をチェックします。

e) [Import] をクリックします。

サイト間 L3Out を使用するための外部 EPG の設定

このセクションでは、サイト間L3Outと関連付ける外部EPGの作成方法について説明します。その後、この外部 EPG とコントラクトを使用すれば、あるサイトのエンドポイント用の特定のユース ケースを設定し、別のサイトの L3Out を使用することができます。

始める前に

L3Out を作成し、サイト間 L3Out および VRF の作成またはインポート （17 ページ）に説明されている方法で VRF と関連付けます。

ステップ 1 左側のナビゲーション ペインで、**[スキーマ (schema)]** を選択します。

ステップ 2 [スキーマ (schema)] を選択し、外部 EPG を作成するテンプレートを選択します。

複数のサイトと関連付けられているテンプレート内で外部 EPG を作成した場合、その外部 EPG は、それらすべてのサイト上で作成されます。単一のサイトと関連付けられているテンプレート内で外部 EPG を作成した場合、その外部 EPG は、そのサイト内でのみ作成されます。

ステップ 3 **[外部 EPG (External EPG)]** エリアまで下方にスクロールして、+ アイコンをクリックして外部 EPG を追加します。

右側のスライダで、必要な情報を入力します。

a) 外部 EPG の名前を入力します。たとえば `[eepg-intersite-l3out]` のようにします。
b) **[仮想ルーティングと転送 (Virtual Routing & Forwarding)]** ドロップダウンから、先ほど作成した、L3Out 用の VRF を選択します。

ステップ 4 テンプレートレベルで L3Out を割り当てる場合...

外部 EPG 用の L3Out は、テンプレート レベルで選択し、設定できます。その場合、L3Out をサイトローカル レベルで設定することはできません。

a) スキーマ ビューの左サイドバーで、外部 EPG が置かれているテンプレートを選択します。
b) **[外部 EPG (External EPG)]** エリアまで下方にスクロールして、外部 EPG を選択します。
c) 右サイドバーで、**[L3Out]** ドロップダウンまで下方にスクロールして、作成したサイト間 L3Out を選択します。

ステップ 5 L3Out をサイトローカル レベルで割り当てるには...

代わりに、L3Out をサイトローカル レベルで外部 EPG に関連付けることもできます。

a) スキーマ ビューの左サイドバーで、外部 EPG が配置されているテンプレートを選択します。
b) **[外部 EPG (External EPG)]** エリアまで下方にスクロールして、外部 EPG を選択します。
c) 右サイドバーで、**[L3Out]** ドロップダウンまで下方にスクロールして、作成したサイト間 L3Out を選択します。

この場合、APIC で管理されている L3Out と、オーケストレーションで管理されている L3Out の両方が選択できます。前のセクションでこの目的のため特に作成した L3Out、またはサイトの APIC 内にすでにある L3Out のいずれかを選択します。

サイト間 L30ut のコントラクトの作成

ここでは、アプリケーション EPG とサイト間 L3Out を含む外部 EPG との間のトラフィック フローを有効にするために使用するフィルタとコントラクトを作成する方法について説明します。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインで、**[スキーマ (schema)]** を選択します。

ステップ 3 [スキーマ (schema)] 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。

L3Out、VRF、および外部 EPG を作成したのと同じスキーマとテンプレートを使用できます。または、別のスキーマとテンプレートを選択することもできます。

ステップ 4 コントラクトのフィルタを作成します。

a) **[Filter (フィルタ)]** エリアまでスクロールし、+ をクリックしてフィルタを作成します。
b) 右側のサイドバーで、フィルタの**[表示名 (Display Name)]**を入力します。
c) **[エントリ (Entry)]** で **[+エントリ (+ Entry)]** をクリックして、フィルタ エントリを入力します。
d) **[エントリの追加 (Add Entry)]** ウィンドウで詳細を入力します。

作成するフィルタは、展開と許可するトラフィックのタイプによって異なります。

e) **[保存 (Save)]** をクリックしてフィルタを保存します。

ステップ 5 コントラクトを作成します。

a) **[コントラクト (Contracts)]** エリアまで下方にスクロールし、+ をクリックして、コントラクトを作成します。
b) 右側のサイドバーで、コントラクトの**[表示名 (Display Name)]**を入力します。
c) **[範囲 (Scope)]** ドロップダウンから、適切な範囲を選択します。

サイト間 L3Out の別の VRF にある共有サービス エンドポイントを設定する場合にはは、その範囲の `テナント` を選択する必要があります。それ以外の場合、両方が同じ VRF 内にある場合は、範囲を `vrf` に設定できます。

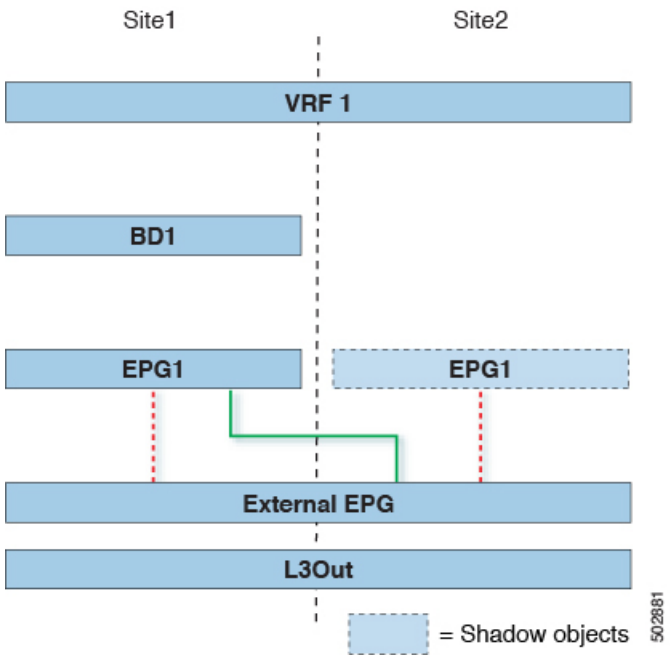
d) **[両方向に適用 (Apply Both Directions)]** ノブをオンのままにします。
e) **[+フィルタ (+ Filter)]** をクリックします。
f) **[名前 (Name)]** ドロップダウン メニューから、前の手順で作成したフィルタを選択します。
g) **[保存 (Save)]** をクリックして、フィルタをコントラクトに追加します。

アプリケーション EPG のサイト間 L30ut の設定

このセクションでは、別のサイトで L3Out を使用するようにアプリケーション EPG を設定する方法について説明します。

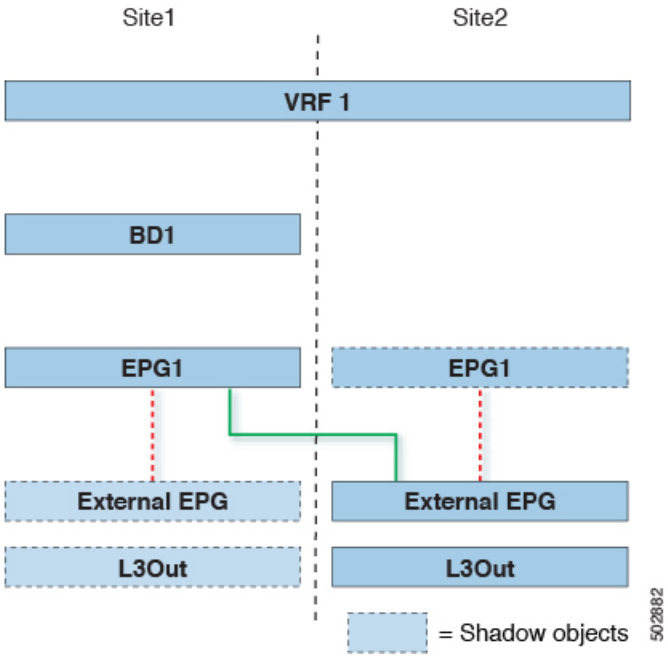
下の図に、拡大された外部 EPG と、両方のサイトで作成される関連づけられた L3Out を示します。アプリケーション EPG (epg1) はサイト 1 で作成され、外部 EPG とのコントラクトがあります。

図 *5*: 拡張された外部 *EPG*



次の 2 番目の図は、同様の使用例を示していますが、外部 EPG は物理 L3Out が配置されているサイトだけに導入されています。アプリケーション EPG とコントラクトは、1 つのサイトの EPG と他方の物理 L3Out 間のトラフィックフローを可能にするのと全く同じ方法で設定します。

図 *6*: 拡張されていない (サイトローカルの) 外部 *EPG*



L3Out を含む外部 EPG を拡張するかどうかにかかわらず、アプリケーション EPG と外部 EPG 間の通信はコントラクトによって有効になります。次の手順では、アプリケーション EPG を作成し、以前に設定した L3Out 外部 EPG との間でコントラクトを設定する方法について説明します。

始める前に

次のものがすでに設定されている必要があります。

- サイト間 L3Out を使用するための外部 EPG の設定 （18 ページ） で説明されているように、サイト間 L3Out の外部 EPG。
- サイト間 L3Out のコントラクトの作成 （20 ページ） で説明されているように、アプリケーション EPG と L3Out 外部 EPG の間で使用するコントラクト。
- サイト間 L3Out を使用するアプリケーション EPG。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインで、**[スキーマ (schema)]** を選択します。

ステップ 3 アプリケーション EPG のスキーマを選択します。

ステップ 4 アプリケーション EPG とそのブリッジ ドメインを設定します。

サイト間 L3Out を使用する EPG がすでにある場合は、この手順をスキップできます。

通常のように、EPG およびブリッジ ドメインを新規に作成するか、既存のものをインポートします。

ステップ 5 アプリケーション EPG にコントラクトを割り当てます。

a) EPG を選択します。
b) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
c) 前のセクションで作成したコントラクトとそのタイプを選択します。

ステップ 6 サイト間 L3Out を含む外部 EPG にコントラクトを割り当てます。

a) 外部 EPG が配置されているテンプレートを参照します。
b) 外部 EPG を選択します。
c) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
d) 前のセクションで作成したコントラクトとそのタイプを選択します。

ステップ 7 適切なサイトにテンプレートを割り当てます。

外部 EPG が拡張されている最初の図に示されている使用例を設定する場合は、外部 EPG のテンプレートをすべてのサイトに割り当て、アプリケーション EPG を 1 つのサイトに割り当てます。

外部 EPG とアプリケーション EPG がサイトに対してローカルである 2 番目の図に示されている使用例を設定する場合は、外部 EPG のテンプレートを 1 つのサイトに割り当て、アプリケーション EPG のテンプレートを別のサイトに割り当てます。

ステップ 8 アプリケーション EPG のブリッジ ドメインを L3Out に関連付けます。

a) 左側のサイドバーの **[サイト (Sites)]** の下で、アプリケーション EPG のテンプレートを選択します。
b) アプリケーション EPG に関連付けられたブリッジ ドメインを選択します。
c) 右側のサイドバーで、**[+ L3Out]** をクリックします。
d) 作成したサイト間 L3Out を選択します。

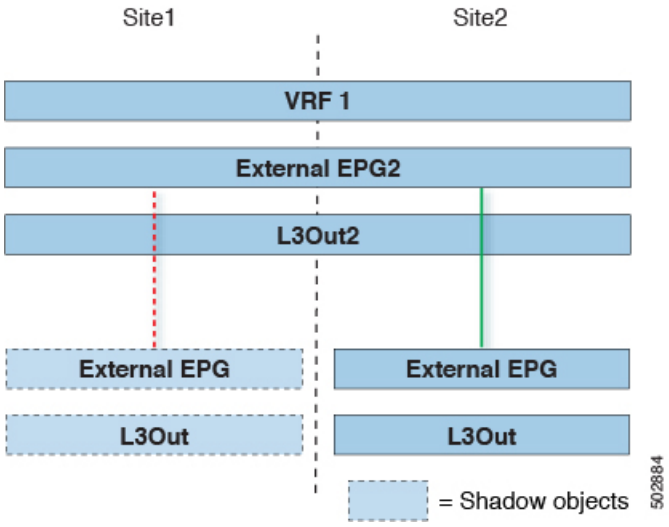
ステップ 9 スキーマを展開します。

サイト間での中継 L3Out の設定

このセクションでは、1 つのサイトの L3Out の背後にあるエンドポイントと、別のサイトの L3Out の背後にあるエンドポイント間の通信を設定する方法について説明します。

次の図は、異なるサイトに設定されている2つの L3Outs (`l3out1`と`l3out2`) を示しています。各 L3Out はそれぞれの外部 EPG (`ExtEPG1`および`ExtEPG2`) に関連付けられています。2つの外部 EPG 間のコントラクトにより、2 つの異なるサイトの 2 つの異なる L3Outs の背後にあるエンドポイント間の通信が可能になります。

図 *7:* 中継 *L3Out*



この図は外部 EPG の 1 つを示していますが、もう一方はサイトローカルで、中継 L3Out は 3 つのすべての組み合わせをサポートしています。この場合、外部 EPG は拡大されず、どちらかが拡大されるか、または両方ともサイト間で拡大されます。

始める前に

次のものがすでに設定されている必要があります。

- 異なるサイトにある2つの異なる L3Outs 用の 2 つの異なる外部 EPG。サイト間 L3Out を使用するための外部 EPG の設定 （18 ページ） の説明に従って、同じ手順を使用して両方の外部 EPG を作成できます。
- サイト間 L3Out のコントラクトの作成 （20 ページ） で説明されているように、アプリケーション EPG と L3Out 外部 EPG の間で使用するコントラクト。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインで、**[スキーマ (schema)]** を選択します。

ステップ 3 いずれかの外部 EPG にコントラクトを割り当てます。

a) 外部 EPG が配置されているスキーマとテンプレートを選択します。
b) 外部 EPG を選択します。
c) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
d) 前のセクションで作成したコントラクトとそのタイプを選択します。

次を選択することができます

ステップ 4 他の外部 EPG にコントラクトを割り当てます。

a) 外部 EPG が配置されているスキーマとテンプレートを選択します。
b) 外部 EPG が配置されているテンプレートを参照します。

c) 外部 EPG を選択します。
d) 右側のサイドバーで、**[+コントラクト (+Contract)]** をクリックします。
e) 前のセクションで作成したコントラクトとそのタイプを選択します。

ステップ 5 適切なサイトにテンプレートを展開します。

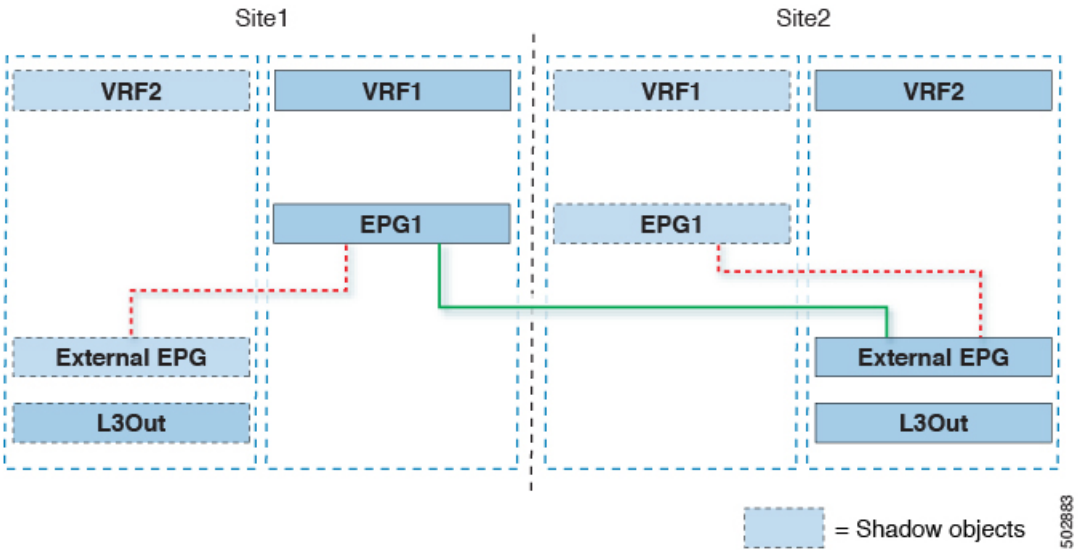
外部 EPG を1つのサイトまたは複数のサイトに展開することを選択できます。上の図は、1 つの外部 EPG が 1 つのサイトのみに展開されている間に 1 つの外部を拡大する例を示していますが、外部 EPG に対してストレッチまたはサイト ローカルを任意に組み合わせて選択することもできます。L3Outs は異なるサイトにあるため、トラフィックはサイト間で ACI ファブリックを通過します。

サイト間 L3Out による共有サービス

共有または中継サイト間 L3Out のための共有サービスの設定は、アプリケーション EPG のサイト間 L3Out の設定 （20 ページ） および サイト間での中継 L3Out の設定 （23 ページ） で説明している設定と類似していますが、下のように、いくつかの重要な相違点があります..

VRF 間の共有 L3Out

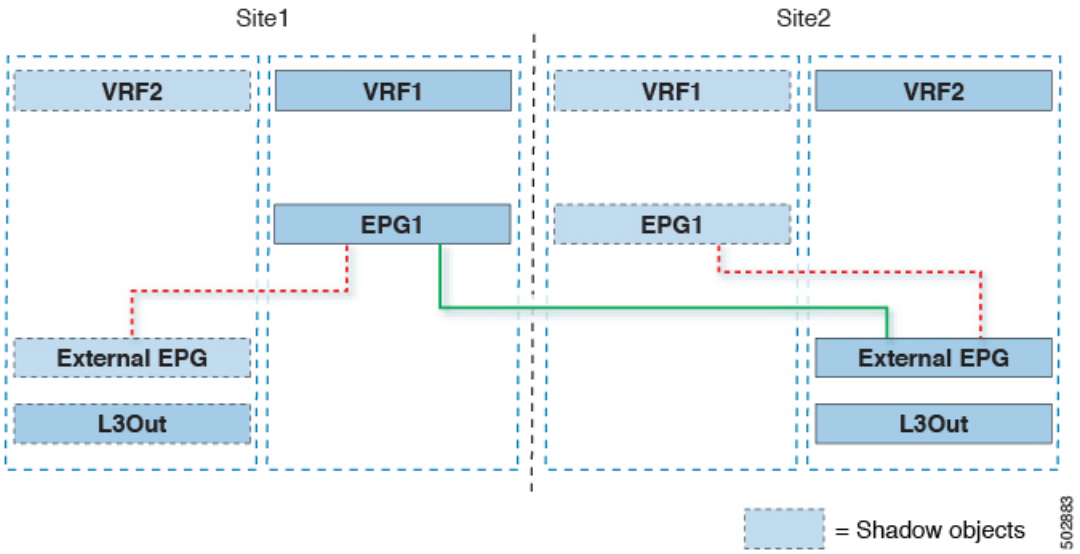
下の図はVRF 間の共有 L3Out シナリオの例を示しています。ここで、アプリケーション EPG (`epg-1`) は `site1` 内にあり、`vrf-1` は `site2` の L3Out を使用していますが、これは `vrf-2` 内にあります。



この VRF 間ユース ケースを設定する際には、アプリケーション EPG のブリッジ ドメインを設定するときに、**[外部にアドバタイズ (Advertised Externally)]** と **[VRF 間で共有 (Shared Between VRF)]** フラグを有効にする必要があります。

VRF 間の中継 L3Out

そして、下の図は、VRF 間の中継 L3Out シナリオの例を示しています。ここで、異なる VRF 内に位置する、2 つの異なる L3Out を持つ 2 つの外部 EPG は、コントラクトで設定されています。



この VRF 間ユース ケースを設定する際には、外部 EPG のサブネットを設定するときに、**[共有ルート制御サブネット (Shared Route Control Subnet)]**、**[共有セキュリティ インポート サブネット (Shared Security Import Subnet)]**、および **[共有ルートを集約 (Aggregate Shared Routes)]** フラグを有効にする必要があります。

EPG 優先グループ

デフォルトでは、マルチサイト アーキテクチャは EPG 間でコントラクトが設定されている場合のみ、EPG 間の通信を許可します。EPG 間にコントラクトがない場合は、EPG 間の通信は明示的に無効になります。優先グループ機能を使用すると、同じ VRF の一部である複数の EPG を指定して、コントラクトを作成する必要なく、それらの間の完全な通信を可能にすることができます。

優先グループ 対 コントラクト

コントラクト優先グループが設定されている VRF で、EPG に利用可能なポリシー施行には 2 種類あります。

- **EPG を含む** – 優先グループのメンバーである EPG は、コントラクトなしでグループ内の他のすべての EPG と自由に通信できます。通信は、`source-any-destination-any-permit` のデフォルト ルールと適切な マルチサイト 変換に基づいています。
- **EPG を除外** - 優先グループのメンバーではない EPG は、相互に通信するためにコントラクトが必要です。そうしない場合、デフォルトの `source-any-destination-any-deny` ルールが適用されます。

コントラクト優先グループ機能を使用すると、拡張 VRF コンテキストのサイト間での EPG 間の通信をより詳細に制御し、設定を容易にすることができます。拡張 VRF の 2 つ以上の EPG がオープン通信を要求する一方で、他は制限された通信しかもてない場合、コントラクト優先グループとフィルタ付きのコントラクトの組み合わせを設定し、EPG内の通信を正確に制御できます。優先グループから除外されている EPG は、`source-any-destination-any-deny`デフォルト ルールを上書きするコントラクトがある場合にのみ、他の EPG と通信できます。

拡張 対 シャドウ

複数のサイトの EPG が同じコントラクト優先グループの一部になるように構成されている場合、Multi-Site Orchestrator は他のサイトに各サイトの EPG のシャドウを作成して、EPG からサイト間接続を正しく変換およびプログラムします。次に、コントラクト優先グループポリシーコンストラクトが、EPG 間通信の実際の EPG とシャドウ EPG の間の各サイトに適用されます。

たとえば、Site1 のウェブサービス EPG1 と Site2 のアプリサービス EPG2 がコントラクト優先グループに追加される場合を考察します。次に、EPG1 が EPG2 にアクセスする場合は、最初にサイト 2 のシャドウ EPG1 に変換され、次にコントラクト優先グループを使用して EPG2 と通信できるようになります。適切な BD は、その下の EPG がコントラクト優先グループの一部である場合、拡張されるか、シャドウされます。

制限事項

優先グループはサイト間 L3Out 拡張外部 EPG でサポートされますが、サイト ローカル L3Out 外部 EPG ではサポートされません。

優先グループに対する EPG の設定

始める前に

スキーマ テンプレートに 1 つ以上の EPG を追加する必要があります。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のナビゲーション ペインで、**[スキーマ (schema)]** を選択します。

ステップ 3 変更するスキーマをクリックします。

ステップ 4 優先グループの一部として、スキーマで 1 つ以上の EPG を設定します。

（注） APICのいずれかに既存の優先グループがあり、その優先グループから マルチサイト Orchestrator にEPGをインポートすることを計画している場合は、グループ内のすべてのEPGをインポートする必要があります。一部の EPG が マルチサイト Orchestrator によって管理され、一部がローカル APIC によって管理される優先グループを設定することはできません。

単一の EPG を追加または削除するには:

a) EPGを選択します。

b) 右側のプロパティ バーで、**[優先グループに含める]** チェックボックスをオンまたはオフにします。

c) メイン ウィンドウの右上の隅にある **[保存]** をクリックします。

複数の EPG を一度に追加または削除するには:

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

次のタスク

VRF を選択し、右側のプロパティサイドバーで **PREFERRED GROUP EPGS** リストを確認すると、優先グループの一部として構成されている EPG の完全なリストを表示できます。

レイヤ3マルチキャスト

Cisco マルチキャスト レイヤ 3 マルチキャストは、VRF、ブリッジ ドメイン (BD)、およびマルチキャスト ソースが存在している任意の EPG という、3 つのレベルで有効または無効にできます。

トップ レベルでは、マルチキャスト ルーティングは、任意のマルチキャストが有効な BD を持つ VRF で有効にする必要があります。マルチキャストが有効な VRF では、マルチキャストが有効な BD と、マルチキャスト ルーティングが無効な BD の組み合わせにすることができます。Cisco マルチサイト Orchestrator GUI で VRF のマルチキャスト ルーティングを有効にすると、VRF が拡張されている APIC サイトで有効になります。

いったんマルチキャストで VRF を有効にすると、VRF の下の個別の BD では、マルチキャスト ルーティングを有効にすることができます。BD でレイヤ 3 マルチキャストを設定すると、その BD 上では、プロトコル独立ルーティング (PIM) が有効になります。デフォルトでは、マルチキャストはすべての BD で無効になっています。

EPG が、拡張されていないリモート サイトにマルチキャスト トラフィックを送信すると、マルチサイト Orchestrator は、このような EPG ごとに、リモート サイトにシャドウ EPG を作成します。これにより、サブネット ルートなどの設定変更がリモート トップオブラック (TOR) スイッチにプッシュされる可能性があります。この点を軽減するため、レイヤ3マルチキャストは、マルチキャストの送信元が存在する、個々の EPG 上でも有効にする必要があります。その場合、それらの EPG で必要な設定だけが、リモート サイトにプッシュされます。マルチキャストの受信者が存在する EPG では、レイヤ 3 マルチキャストを有効にする必要はありません。

マルチサイトは、以下のレイヤ 3 マルチキャスト送信元と受信者のすべての組み合わせをサポートしています。

- ACI ファブリック内のマルチキャスト送信元と受信者

- ACI ファブリック外のマルチキャスト送信元と受信者
- ACI ファブリック内のマルチキャスト送信元と外部受信者
- ACI ファブリック内のマルチキャスト受信者と外部送信元

レイヤ 3 マルチキャスト ルーティング

次に示すのは、サイト間レイヤ 3 マルチキャスト ルーティングの高レベルでの概要です。

- あるサイトで、マルチキャスト ソースをエンドポイント (EP) として ACI ファブリックにアタッチした場合、そのサイトのスパイン スイッチはマルチキャスト トラフィックを別のサイトの送信します。そこでは、ソースの VRF は、ヘッド エンド レプリケーション (HREP) を使用してインスタンス化されます。マルチキャスト トラフィックは VRF が拡張されている他のサイトに送り出され、マルチキャスト トラフィックは、グループ メンバシップに基づいて出力リーフ スイッチでプルーニング/転送されます。
- マルチキャスト ルーティング ソリューションは、ランデブー ポイント (RP) となる外部マルチキャスト ルータを必要とします。それぞれのサイトは、指定された拡張 VRF に対し、同じ RP アドレスをポイントしている必要があります。RP は、サイトローカルの L3Out を介して、各サイトに到達できる必要があります。
- 送信元がファブリックの外側、受信者が内側にある場合、受信者は、RP に対する PIM ジョインとしてのサイトローカルの L3Out を介してトラフィックをプルします。送信元は常にサイトローカルの L3Out を介して送信されます。
- 各サイトの受信者には、ファイブリック外部の送信元からのトラフィックを、サイトローカルの L3Out を介して取り込むことが期待されます。そのようなわけで、一方のサイトの L3Out を発するトラフィックは、別のサイトには送信されません。このことは、スパインにおいて、HREP トンネルへのレプリケーションからのマルチキャスト トラフィックをプルーニングすることによって行われます。
- 外部ルータから TOR の L3Out ブリッジ ドメインに入力されるマルチキャスト トラフィックでは、外部 VXLAN ヘッダの特別な DSCP 値で、再マーキングが行われます。スパインでは、そのDSCP 値のマッチングが行われ、HREP コピーを ISN ネットワークに複製して得られたすべてのマルチキャスト トラフィックはプルーニングされます。
- あるサイトから送信されたトラフィックは、任意のサイトの L3Out から送信できます。
- BD とマルチサイト Orchestrator からの EPG でマルチキャストが有効にされている場合、BD のすべてのサブネットは、境界リーフ (BL) を含めて、すべてのリーフ スイッチにインジェクトされます。これにより、リーフ スイッチにアタッチされた受信者は、送信側 BD がリーフ スイッチに存在しない場合に、マルチキャスト ソースの到達可能性を判定することができます。BL に対してポリシーが設定されていた場合、サブネットはアドバタイズされます。ホストベースのルーティングが BD で設定されている場合、/32 ホストルートがアドバタイズされます。L3Out ポシシーが、0/0 を含む大規模なサブネット範囲を許可しており、EPG でマルチキャストが有効になっていた場合、BD のサブネットとホストルートはアドバタイズされます。

マルチキャスト ルーティングについての詳細は、IP マルチキャストのセクションを参照してください。これは*Cisco APIC* レイヤ *3* ネットワーク コンフィギュレーション ガイドに記されています。

Layer 3 マルチキャストに関するガイドラインと制限事項

Cisco ACI マルチサイト Orchestrator は各サイトに必要なローカル ポリシーを作成できません。そのため、エンドツーエンドのソリューションを機能させるために、各 APIC サイトで IGMP 関連ポリシー、PIM 関連ポリシー、ルートマップ、RP、および L3Outs を個別に設定する必要があります。

また、すべてのファブリックの DSCP ポリシーが一貫して設定されていることを確認する必要があります。DSCP パケットヘッダー値は、サイト間で送信されるマルチキャスト トラフィックに対して一致する必要があります。

各サイトでこれらの設定を構成する方法の詳細については、*Cisco APIC* レイヤ *3* ネットワーク コンフィギュレーション ガイドを参照してください。

マルチキャスト フィルタ処理

マルチキャスト フィルタ処理を有効にすると、次の追加のガイドラインが適用されます。

- マルチキャスト フィルタ処理は、IPv4 でのみサポートされています。
- 同じブリッジドメインで、マルチキャスト送信元フィルタ処理または受信者フィルタ処理のいずれかまたは両方を有効にできます。
- ブリッジ ドメインにマルチキャスト フィルタを設定しない場合は、そのブリッジドメインで送信元フィルタまたは宛先フィルタ ルート マップを設定しないでください。

  デフォルトでは、ルートマップはブリッジ ドメインに関連付けられていません。これは、すべてのマルチキャスト トラフィックが許可されることを意味します。ルートマップがブリッジ ドメインに関連付けられている場合、そのルートマップ内の permit エントリだけが許可され、その他のすべてのマルチキャスト トラフィックはブロックされます。

  空のルートマップをブリッジ ドメインに接続すると、ルートマップはデフォルトで `deny all` を想定するため、すべての送信元とグループがそのブリッジ ドメインでブロックされます。
- マルチキャスト フィルタ処理は、同じブリッジ ドメイン (BD) 内の複数の EPG ではサポートされていません。

  マルチキャスト フィルタ処理はレイヤ 3 レベルで実行されるため、同じブリッジ ドメインに複数の EPGs を設定し、許可アクションを設定し、もう1つを [拒否 (Deny)] アクションとともに設定すると、レイヤ 3 マルチキャストはフィルタの対象を決定できなくなります。複数の EPG に対してマルチキャスト フィルタ処理を有効にする場合は、それらを個別の BD に設定する必要があります。
- マルチキャスト フィルタ処理は、任意の送信元マルチキャスト (ASM) 範囲にのみ使用することを目的としています。送信元固有のマルチキャスト (SSM) 範囲をサポートしている

場合は、IGMPv3 を使用した SSM join itself で送信元と結合をフィルタ処理することを推奨します。

マルチキャスト フィルタ処理機能の SSM 範囲を設定する場合は、次の制約事項が適用されます。

- **送信元フィルタ処理に対する影響**: SSM ルートはすでにハードウェアのドロップ エントリとしてプログラムされているため、ファースト ホップ ルータ (fhr) ではパントは受信されません。したがって、送信元フィルタ処理は SSM 範囲の影響を受けません。
- **受信者のフィルタ処理に適用**: 特定のブリッジ ドメインの最後のホップで受信した SSM join は、マルチキャスト RPF ルーティング情報ベース (MRIB) ルートでブロックされているように、そのグループの発信インターフェイス (OIF) リストを表示します。これは、最後のホップで IGMP のレポートポリシーを使用して実現することもできます。これにより、マルチキャスト ルーティング テーブルでの状態の作成が維持されます。

- 送信元フィルタ処理の場合、ルートマップエントリはエントリの指定された順序に基づいて照合され、最も小さい番号が最初に一致します。これは、より低い順序のエントリが、リスト内で最長一致でない場合でも、最初に一致することを意味し、より高い順序のエントリは考慮されません。

  たとえば、 `192.0.3.1/32` ソースに対して次のルートマップがあるとします。

順位	送信元 IP	操作
1	`192.0.0.0/16`	`Permit`
2	`192.0.3.0/24`	拒否（Deny）

  2番目のエントリ (`192.0.3.0/24`) が送信元 IP と一致する場合でも、最初のエントリ (`192.0.0.0/16`) は、下位の番号が原因で照合されます。

（注） マッチングの順序は、送信元のフィルタリングにのみ適用されます。受信者フィルタリングの場合、順序は重要ではなく、最長一致ルールが適用されます。

レイヤ 3 マルチキャストの有効化

以下の手順では、Cisco ACI マルチサイト Orchestrator GUI を使用して、VRF、BD、および EPG でレイヤ 3 マルチキャストを有効にする方法を説明しています。

始める前に

- Layer 3 マルチキャストに関するガイドラインと制限事項 （30 ページ） で説明されている情報を読んで、従っていることを確認してください。

ステップ 1 Cisco ACI マルチサイト Orchestrator にログインします。

ステップ 2 左側のサイドバーから、**[スキーマ (schema)]** ビューを選択します。

ステップ 3 変更するスキーマをクリックします。

ステップ 4 VRD でレイヤ 3 マルチキャストを有効にします。

まず、サイト間で拡張されている VRF でレイヤ 3 マルチキャストを有効にします。

a) レイヤ 3 マルチキャストを有効にする VRF を選択します。
b) 右のプロパティサイドバーで、**[L3 マルチキャスト (L3 Multicast)]** チェックボックスをオンにします。

ステップ 5 BD でレイヤ 3 マルチキャストを有効にします。

いったん ＶＲＦ で L3 マルチキャストを有効にすると、L3 マルチキャストをブリッジ ドメイン (BD) レベルで有効にすることができます。

a) レイヤ 3 マルチキャストを有効にする BD を選択します。
b) 右のプロパティサイドバーで、**[L3 マルチキャスト (L3 Multicast)]** チェックボックスをオンにします。

ステップ 6 最後に、EPG でマルチキャストを有効にします。

いったん BD で L3 マルチキャストを有効にすると、マルチキャスト送信元を持つ EPG を選択できるようになります。これは、EPG がマルチ客ストを有効にした BD または VRF の一部である場合にのみ行えます。

a) レイヤ 3 マルチキャストを有効にする EPG を選択します。
b) 右側のサイドバーで、**[サイト間マルチキャスト送信元 (Intersite Multicast Source)]** チェックボックスをオンにします。