



ACI ファブリックの PBR を使用する Nexus Dashboard Orchestrator ファブ リック間 L3Out、リリース 4.4.1

目次

- PBR を使用したファブリック間 L3Out..... 1
 - 構成ワークフロー 1
 - サポートされる使用例..... 2
 - VRF 内と VRF 間..... 2
 - ストレッチ EPG への L3Out..... 2
 - ファブリックローカル EPG への L3Out..... 3
- 注意事項と制約事項..... 6
- サービス デバイス テンプレートの作成..... 7
- コントラクトへのサービス チェーンの追加 9

PBR を使用したファブリック間 L3Out

Cisco Application Centric Infrastructure (ACI) ポリシーベース リダイレクト (PBR) は、ファイアウォールやロード バランサなどのサービス アプライアンス、および侵入防御システム (IPS) のトラフィック リダイレクションを可能にします。一般的な使用例としては、プールしてアプリケーション プロファイルに合わせて調整すること、また容易にスケーリングすることができ、サービス停止の問題が少ないサービス アプライアンスのプロビジョニングがあります。PBR により、コンシューマとプロバイダ エンドポイントの間のコントラクトに基づくサービス アプライアンスの挿入は簡素化されます。このことは、それらすべてが同じ仮想ルーティングおよびフォワーディング (VRF) インスタンスに存在する場合でも成り立ちます。

PBR の展開には、ルート リダイレクト ポリシーおよびクラスタのリダイレクト ポリシーの設定と、これらのポリシーを使用するサービス グラフ テンプレートの作成が含まれます。サービスグラフ テンプレートを展開した後、EPG 間のコントラクトにアタッチして、そのコントラクトに従うすべてのトラフィックが、作成した PBR ポリシーに基づいてサービス グラフ デバイスにリダイレクトされるようにすることができます。これにより、同じ 2 つの EPG 間のどのタイプのトラフィックを L4 ~ L7 デバイスにリダイレクトし、どれがファブリック レベルで適用されるセキュリティ ポリシーの対象となるかを選択できます。

サービス グラフおよび PBR に固有の詳細情報については、[『Cisco APIC レイヤ 4 ~ レイヤ 7 サービス 展開ガイド』](#) を参照してください。

構成ワークフロー

次のセクションで説明する使用例は、基本的なファブリック間 L3Out (PBR なし) の使用例の拡張であり、言い換えると、各ファブリックの基本的な外部接続 (L3Out) 構成の拡張です。サポートされるユース ケースを構成するワークフローは同じであり、オブジェクトを同じ VRF で作成するか、異なる VRF で作成するか (VRF 内と VRF 間)、およびオブジェクトを展開する場所 (ストレッチか非ストレッチか) のみが異なります。

1. 各ファブリックの基本的な外部接続 (L3Out) を構成します。

以下のセクションで説明される PBR 構成を持つファブリック間 L3Out は、各ファブリックの既存の外部接続 (L3Out) の上部で構築されます。L3Out を構成していない場合、次のセクションに進む前に、[\[外部接続 \(L3Out\) \(External Connectivity \(L3Out\)\)\]](#) の章で説明されている方法で 1 つ作成し、展開します。

2. PBR を使用しないファブリック間 L3Out の使用例を構成します。

サービス チェーンを追加する前に、ポリシーベースのリダイレクションを使用しない単純なファブリック間 L3Out の使用例を構成することをお勧めします。これについては、「[ファブリック間 L3Out](#)」の章で詳しく説明します。

3. 以下のセクションに説明されるように、L3Out コントラクトにサービス チェーンを追加します。これには、以下が含まれます。

- ファブリック間 L3Out が展開されている各ファブリックの各ポッドに外部 TEP プールを追加します。
- サービス デバイス テンプレートを作成し、ファブリックに割り当てます。

サービス デバイス テンプレートは、他の構成オブジェクトを含む L3Out およびアプリケーション テンプレートと同じファブリックに割り当てする必要があります。

- サービス デバイス テンプレートにファブリックレベル構成を提供します。

各ファブリックは、異なる高可用性モデル（アクティブ/アクティブ、アクティブ/スタンバイ、独立サービス ノードなど）を含む独自のサービス デバイス構成を持つことができます。

- 定義したサービス デバイスを、前の手順で展開した基本的なファブリック間 L3Out の使用例で使用するコントラクトに関連付けます。

サポートされる使用例

次の図は、アプリケーション EPG の ACI 内部エンドポイントと、サポートされているファブリック間 L3Out with PBR 使用例の別のファブリックの L3Out を経由する外部エンドポイント間のトラフィック フローを示しています。

VRF 内と VRF 間

アプリケーション EPG と外部 EPG を作成および構成する場合、アプリケーション EPG のブリッジドメインと L3Out に VRF を提供する必要があります。同じ VRF (intra-VRF) を使用するか、異なる VRF (inter-VRF) を使用するかを選択できます。

EPG 間のコントラクトを確立する場合は、1 つの EPG をプロバイダとして指定し、もう 1 つの EPG をコンシューマとして指定する必要があります。

- ・ 両方の EPG が同じ VRF にある場合、どちらか一方がコンシューマまたはプロバイダになることができます。
- ・ EPG が異なる VRF にある場合は、外部 EPG がプロバイダーであり、アプリケーション EPG がコンシューマである必要があります。

ストレッチ EPG への L3Out

この使用例は、2 つのファブリック間で拡張される単一のアプリケーション EPG と、1 つのファブリックでのみ作成される単一の L3Out を示しています。アプリケーション EPG のエンドポイントが L3Out と同じファブリックにあるか、他のファブリックにあるかに関係なく、トラフィックは同じ L3Out を通過します。ただし North-South トラフィックの場合、PBR ポリシーは常にコンピューティング リーフ ノードにのみ適用されるため（ボーダー リーフ ノードには適用されない）、トラフィックは常にエンドポイントのファブリックに対してローカルなサービス ノードを通過します。



外部 EPG が拡張され、各ファブリックに独自の L3Out がありますが、トラフィック の発信元または宛先ファブリックの L3Out がダウンしている場合に、同じフローが適用されます。

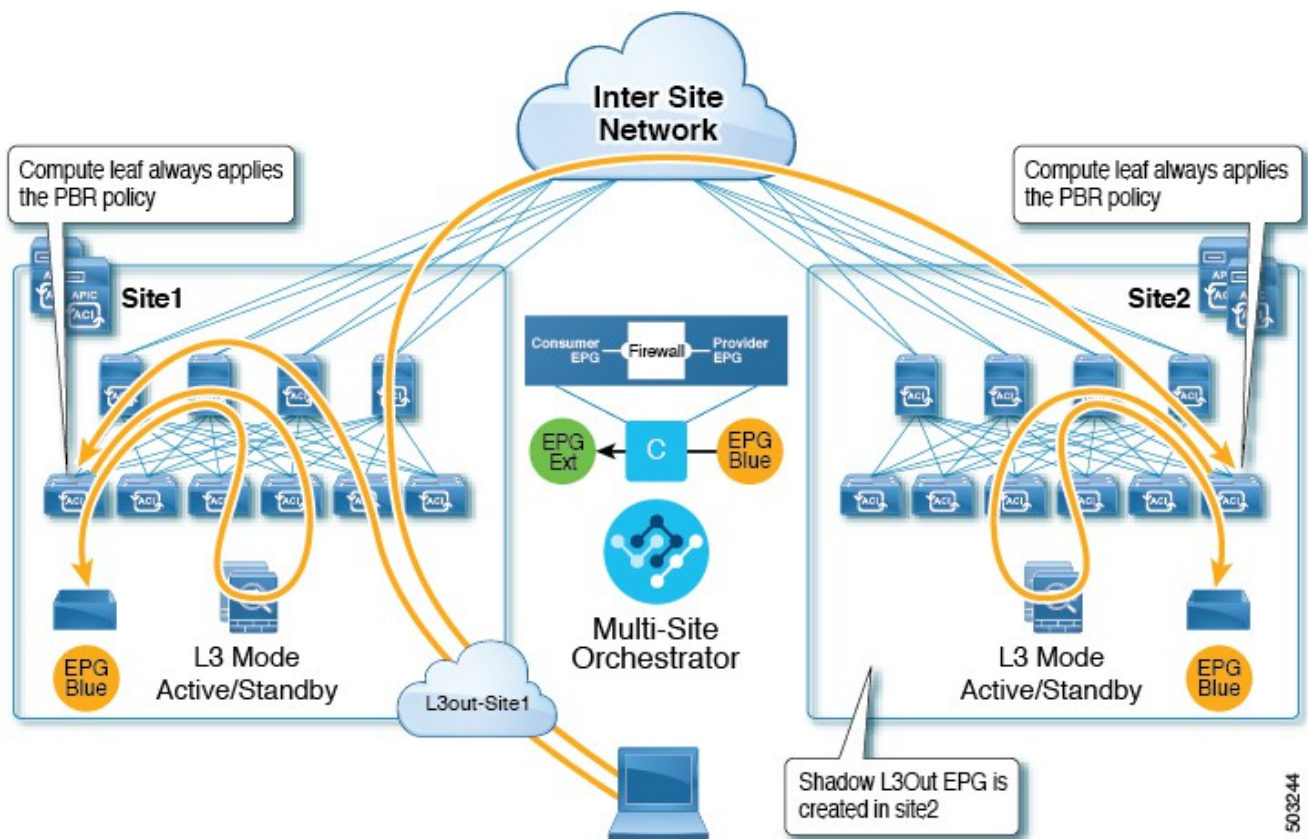


図 1. インバウンド トラフィック

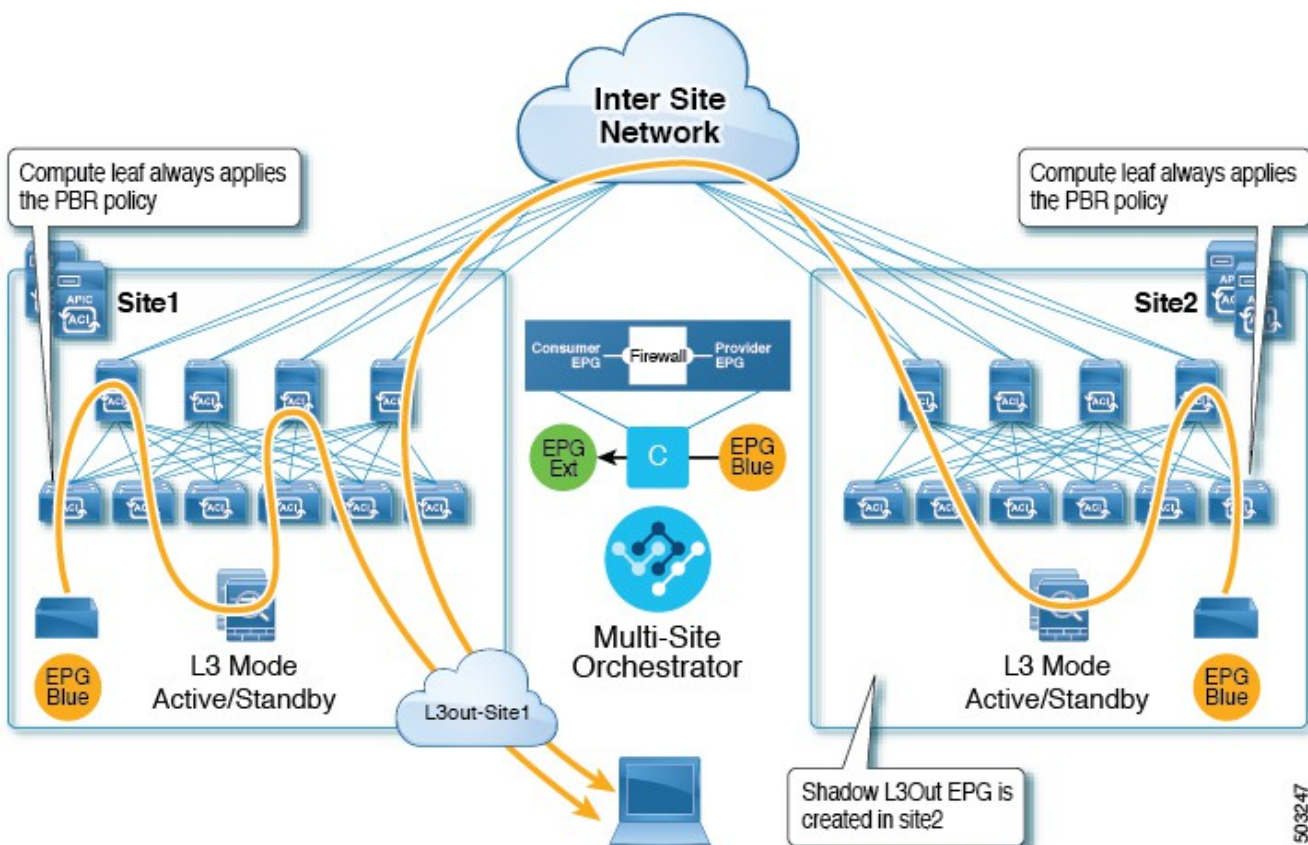


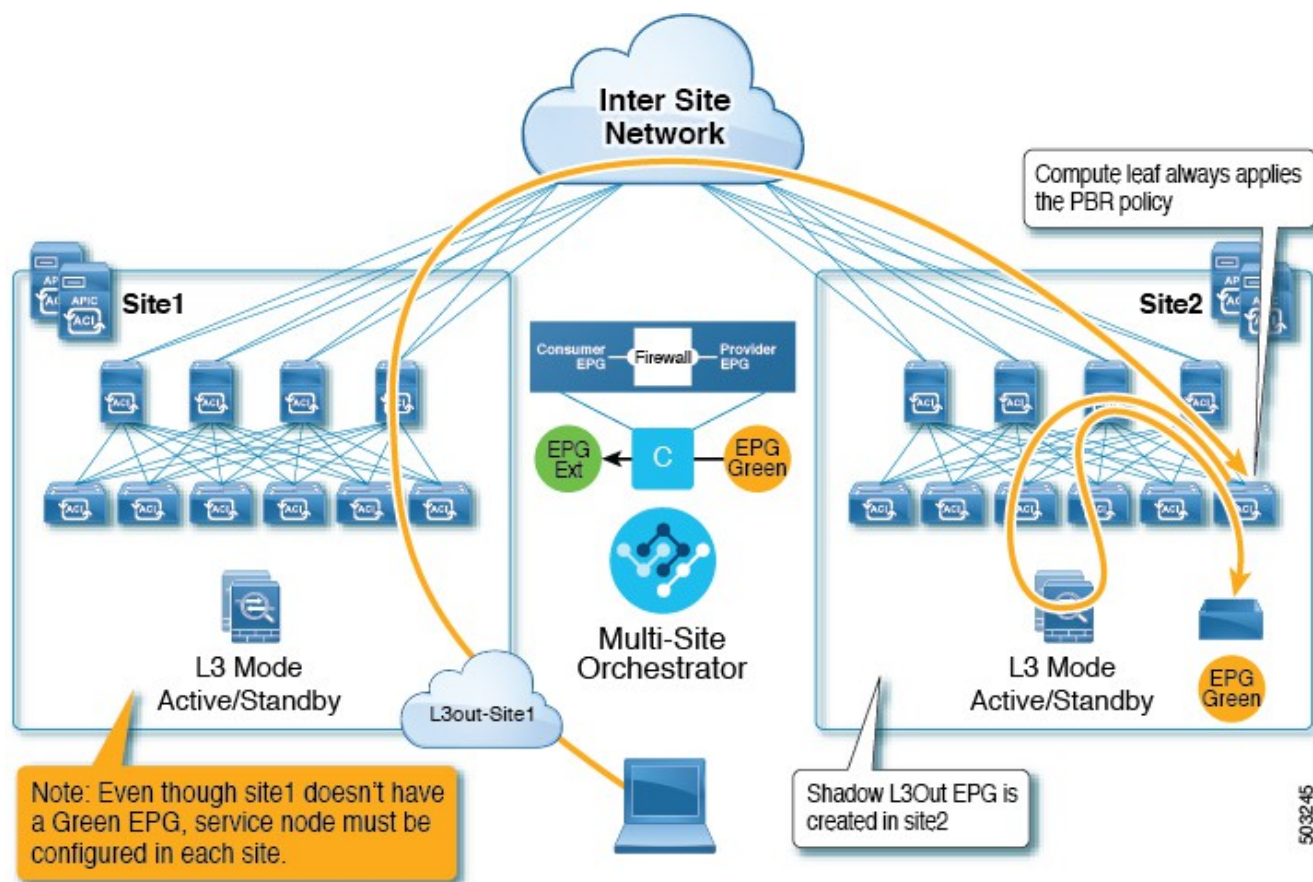
図 2 アウトバウンド トラフィック

ファブリックローカル EPG への L3Out

この使用例は、North-South トラフィックに他のファブリックの L3Out を使用するサイトローカル アプリケーション EPG を示しています。前の例と同様に、すべてのトラフィックは EPG のファブリック ローカル サービス グラフ デバイスを使用します。

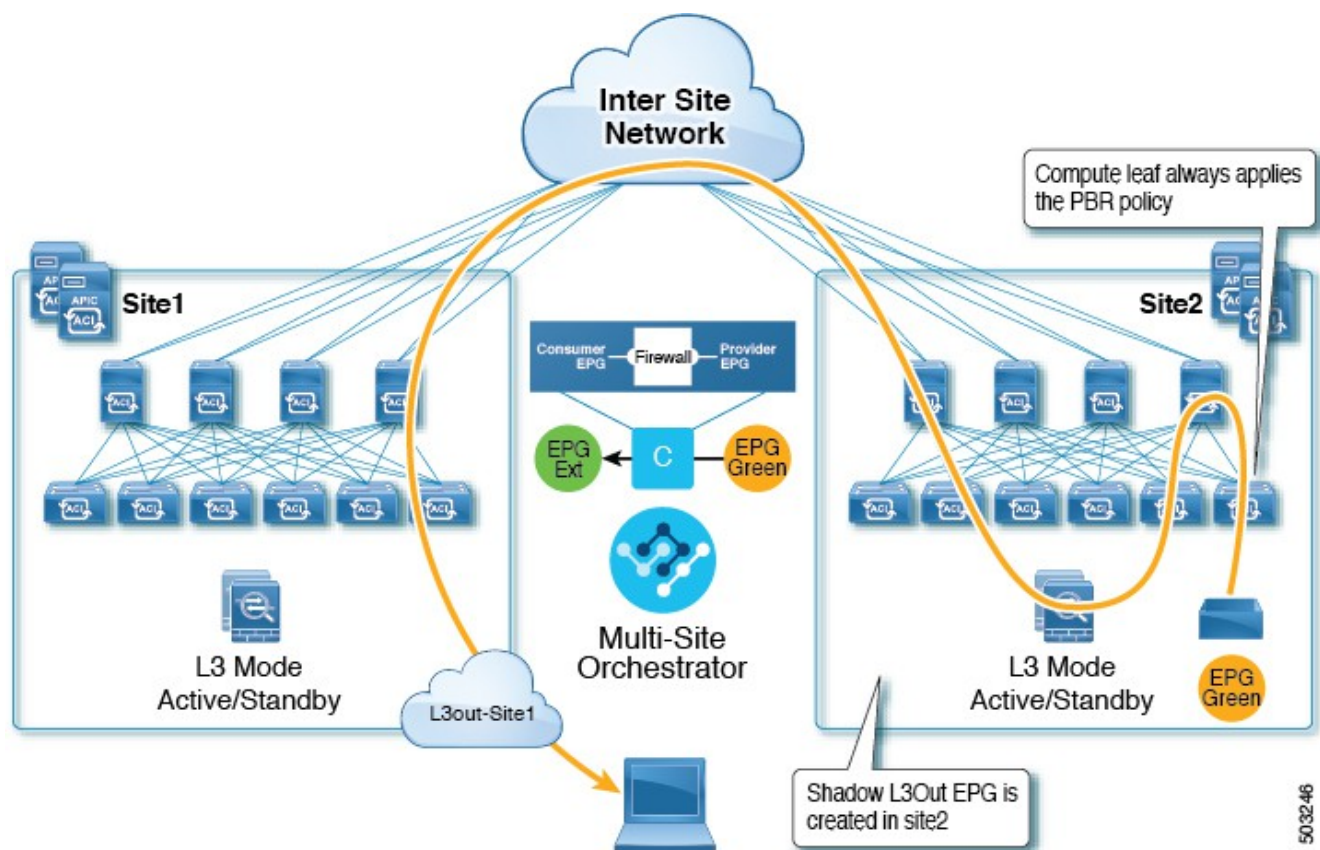


部 EPG が拡張され、各ファブリックに独自の L3Out があり、EPG のローカル L3Out がダウンしている場合も、同じフローが適用されます。



503245

図 3. インバウンド トラフィック



503246

図 4 アウトバウンド トラフィック

注意事項と制約事項

ファブリック間 L3Out を構成する際には次の制約事項が適用されます。

- ・ エンドポイント グループ (EPG) 間で MultiSite ポリシーベース リダイレクト (PBR) を設定する場合、次の機能は特定の IP エンドポイントまたはホスト プレフィックス (IPv4 の場合は /32、IPv6 の場合は /128) ではサポートされません。
 - ブリッジ ドメインのスタティック ルート (NH 到達可能性)
 - Microsoft ネットワーク ロード バランシング
 - エニーキャストMAC
- ・ PBR を使用したファブリック間 L3Out では、次の使用例がサポートされています。
 - アプリケーション EPG を **コンシューマ**とする Inter-VRF ファブリック間 L3Out。

VRF 間コントラクトの場合、L3Out へ関連付けられている外部 EPG が **プロバイダ**である必要があります。

この使用例は、Cisco APIC リリース 4.2(5) 以降またはリリース 5.1(x) を実行しているファブリックでサポートされていますが、APIC リリース 5.0(x) ではサポートされていません。

- アプリケーション EPG が **プロバイダ**または **コンシューマ**のいずれかである VRF 内ファブリック間 L3Out

この使用例は、Cisco APIC リリース 4.2(5) 以降またはリリース 5.1(x) を実行しているファブリックでサポートされていますが、APIC リリース 5.0(x) ではサポートされていません。

- ・ EPG-to-L3Out の使用例では、アプリケーション EPG をストレッチまたはファブリック」ローカルにすることができます。
- ・ EPG-to-L3Out のユース ケース では、ワンアームとツアームの両方の導入モデルがサポートされています。L3Out-to-L3Out の使用例では、ワンアーム ファイアウォール デバイスのみがサポートされます。

ワンアーム展開では、サービス グラフの内部インターフェイスと外部インターフェイスの両方が同じブリッジ ドメインに接続されます。ツアーム展開では、サービス グラフ インターフェイスは個別の BD に接続されます。

- ・ EPG-to-L3Out 使用例については、PBR を使用してロード バランサを構成する場合、ロード バランサと仮想 IP (VIP) の実サーバは同じファブリックに存在する必要があります。PBR が無効の場合、ロードバランサと実サーバは異なるファブリックに存在できます。

L3Out-to-L3Out の場合は、ロードバランサをサポートしていません。

- ・ 1 つのファブリックの L3Out と別のサイトの EPG 間、または異なるファブリックの 2 つの L3Out 間ですでに構成されているコントラクトでサービス チェーンを有効にして、サービス デバイスを挿入する前に、サイト間 L3Out の基本的な使用例を構成しておく必要があります。

PBR を使用しないファブリック間 L3Out の展開に関する詳細な手順については、「[ファブリック間 L3Out](#)」の章を参照してください。

サービス デバイス テンプレートの作成

- ・「[注意事項および 制限事項](#)」で説明されているように、要件を読んで満たしていることを確認します。

ここでは、サービスグラフの1つ以上のデバイスを設定する方法について説明します。

1. Nexus Dashboard Orchestrator の GUI にログインします。
2. 左のナビゲーション ペインから、**[テナント テンプレートの構成 (Configure Tenant Template)]** を選択します。
3. **[サービス デバイス (Service Device)]** タブを選択します。
4. サービス デバイス テンプレートを作成し、ファブリックに関連付けます。
 - a. **[構成 (Configure)]** > **[テナント テンプレート (Tenant Templates)]** から、**[サービス デバイス (Service Device)]** タブを選択します。
 - b. **[サービス デバイス テンプレートの作成 (Create Service Device Template)]** をクリックします。
 - c. 開くテンプレート プロパティ サイドバーで、テンプレートの **[名前 (Name)]** を入力し、**[テナントの選択 (Select a Tenant)]** を選択します。
 - d. **[テンプレート プロパティ (Template Properties)]** ページで、**[アクション (Actions)]** > **[ファブリックの追加/削除 (Add/Remove Fabrics)]** を選択し、両方のファブリックにテンプレートを関連付けます。
 - e. **[保存 (Save)]** をクリックして、テンプレートを保存します。
5. デバイス クラスタを作成して構成します。
 - a. **[テンプレート プロパティ (Template Properties)]** ページ (テンプレートレベルの構成) で、**[オブジェクトの作成 (Create Object)]** > **[サービス デバイス クラスタ (Service Device Cluster)]** を選択します。

デバイス クラスタは、トラフィックのリダイレクト先であるサービスを定義します。

- b. **[<cluster-name>]** サイドバーで、クラスタの **[名前 (Name)]** を入力します。

[デバイスの場所 (Device Location)] と **[デバイス モード (Device Mode)]** は、現在サポートされている使用例に基づいて事前に入力されています。

- c. **[デバイス タイプ (Device Type)]** を選択します。
- d. **[デバイス モード (Device Mode)]** では、**[L3]** を選択します。
- e. **[接続モード (Connectivity Mode)]** を選択します。



L3Out-to-L3Out の使用例を構成する場合は、**[One Arm]** を使用する必要があります

- f. **[インターフェイス名 (Interface Name)]** を入力します。
- g. **[インターフェイス タイプ (Interface Type)]** で、**[BD]** を選択します。

vzAny の使用例の場合、このリリースでは、ブリッジ ドメインへのサービス デバイスの接続のみがサポートされます。

- h. **[BD の選択 (Select BD)]** をクリックして、このデバイスを接続するサービス ブリッジ ドメインを選択します。

これは、前のセクションで作成したストレッチ サービス BD です (例: **[FW 外部]**) 。

- i. [リダイレクト (Redirect)] オプションで、[はい (Yes)] を選択します。

PBR の使用例では、リダイレクトの有効化を選択する必要があります。[はい (Yes)] を選択すると、[IP SLA モニタリング ポリシー (IP SLA Monitoring Policy)] オプションが使用可能になります。

- j. (オプション) [IP SLA モニタリング ポリシーの選択 (Select IP SLA Monitoring Policy)] をクリックし、作成した IP SLA ポリシーを選択します。
- k. (オプション) サービス クラスタの追加設定を指定する場合は、[詳細設定 (Advanced Settings)] エリアで [有効 (Enable)] を選択します。

次の詳細設定を構成できます。

- [QoS ポリシー (QoS Policy)] : リダイレクトされたトラフィックに ACI ファブリック内で特定の QoS レベルを割り当てることができます。
- [優先グループ (Preferred Group)] : このサービス クラスタが優先グループの一部であるかどうかを指定します。
- [ロード バランシング ハッシュ (Load Balancing Hashing)] : PBR ロード バランシングのハッシュ アルゴリズムを指定できます。

詳細については、 [「ACI ポリシーベースのリダイレクト サービス グラフの設計」](#) を参照してください。

- [ポッド対応リダイレクション (Pod Aware Redirection)] : 優先 PBR ノードを指定する場合は、マルチポッド構成で構成できます。ポッド対応リダイレクションを有効にすると、ポッド ID を指定でき、リダイレクトは指定されたポッドにあるリーフ スイッチでのみプログラムされます。
- [送信元 MAC の書き換え (Rewrite Source MAC)] : PBR ノードが IP ベースの転送ではなく「送信元 MAC ベースの転送」を使用している場合に、送信元 MAC アドレスを更新します。

詳細については、 [「ACI ポリシーベースのリダイレクト サービス グラフの設計」](#) を参照してください。

- [高度なトラッキング オプション (Advanced Tracking Options)] : サービス ノード トラッキングのさまざまな詳細設定を構成できます。詳細については、 [「サービスノードをトラッキングするための ポリシーベースリダイレクトとしきい値の設定」](#) を参照してください。

- l. [OK] をクリックして保存します。

サービス デバイス クラスタを作成すると、[テンプレート プロパティ (Template Properties)] (テンプレート レベルの構成) ページで赤色で強調表示されることに注意してください。この時点で、ファイアウォール サービスへのリダイレクトを定義しましたが、やはりファブリックローカルレベルで使用するファイアウォール情報とリダイレクト ポリシーを指定する必要があります。

コントラクトへのサービス チェーンの追加

基本のファブリック間 L3Out 使用例とサービス デバイス テンプレートを展開した後、L3Out とアプリケーション EPG または別の L3Out の間で作成したコントラクトにサービス チェーンを追加することで、ポリシーベースのリダイレクションを追加できます。

1. コントラクトを定義したアプリケーション テンプレートに戻ります。
2. コントラクトを選択します。
3. [サービス チェーン (Service Chaining)] エリアで、[+ サービス チェーン (+Service Chaining)] をクリックします。
4. [デバイス タイプ (Device Type)] を選択します。



L3Out-to-L3Out のユース ケースは、ワンアームの **[ファイアウォール (Firewall)]** デバイスのみをサポートします。PBR を使用した他のファブリック間 L3Out の使用例では、複数のデバイスをチェーンできます。

5. [デバイス (Device)] ドロップダウンから、前の手順で作成した FW デバイス クラスタを選択します。
6. [コンシューマ コネクタ タイプのリダイレクト (Consumer Connector Type Redirect)] が有効になっていることを確認します。
7. [プロバイダ コネクタ タイプのリダイレクト (Provider Connector Type Redirect)] が有効になっていることを確認します。
8. [追加 (Add)] をクリックして続行します。
9. [保存 (Save)] をクリックして、テンプレートを保存します。
10. [テンプレートの展開 (Deploy Template)] をクリックして、再展開します。

初版：2024 年 3 月 1 日

最終更新日：2024 年 7 月 26 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