Cisco APIC レイヤ 4 ～ レイヤ 7 サービス導入ガイド、リリース 5.2 (x)

初版：2021 年 6 月 4 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

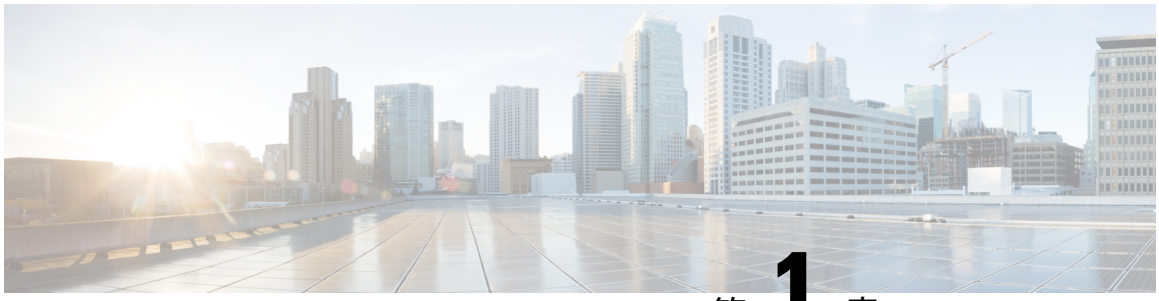
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Trademarks

目 次



第 1 章

新規および変更情報

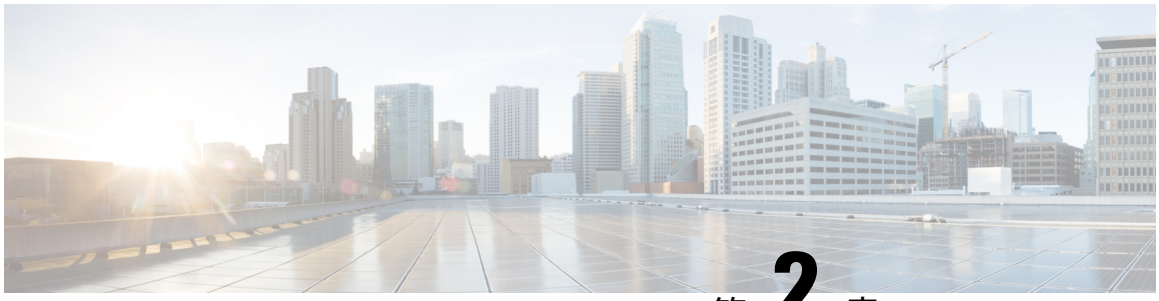
新規および変更情報

次の表に、本リリースに関するこのガイドでの重要な変更点の概要を示します。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco APIC* リリース *6.0(1)* の新機能と動作変更

特長	説明	参照先
重みベースの対称ポリシーベースリダイレクト (PBR)	重みベースの対称 PBR では、管理者によってサービスノードのキャパシティに基づいて PBR 接続先（サービスノード）の重みを設定でき、設定された重みに基づいてトラフィックを負荷分散できます。	重みベースの対称ポリシーベースのリダイレクトについて （103 ページ）

新規および変更情報



第 2 章

概要

アプリケーションセントリックインフラストラクチャのレイヤ 4 ～ 7 サービスの導入について

従来の方法を使用する場合、サービスをネットワークに挿入すると、手間がかかって複雑な VLAN（レイヤ 2）または仮想ルーティングおよび転送（VRF）インスタンス（レイヤ 3）スティッチングを、ネットワーク要素およびサービス アプライアンスの間で実行する必要があります。この従来のモデルでは、アプリケーションに対する新規サービスを配備するのに数日から数週間かかります。サービスには柔軟性が少なく、操作エラーはより頻繁に発生し、トラブルシューティングはより困難です。アプリケーションが使用されなくなる場合、ファイアウォール ルールなどのサービス デバイス設定の削除は困難になります。ロードに基づいたサービスのスケール アウト/スケール ダウンを実行することもできません。

VLAN および仮想ルーティングおよび転送（VRF）スティッチングは従来のサービス挿入モデルによってサポートされますが、Application Policy Infrastructure Controller（APIC）はポリシー制御の中心点として機能する一方でサービス挿入を自動化できます。Cisco APIC ポリシーは、ネットワーク ファブリックとサービス アプライアンスの両方を管理します。Cisco APIC は、トラフィックがサービスを通って流れるように、ネットワークを自動的に設定できます。Cisco APIC は、アプリケーション要件に従ってサービスを自動的に設定することもでき、それにより組織はサービス挿入を自動化し、従来のサービス挿入の複雑な技術の管理に伴う課題を排除できます。

開始する前に次の Cisco APIC オブジェクトを設定する必要があります。

- レイヤ 4 ～ 7 サービスを提供/消費するテナント
- テナントのネットワーク外部のレイヤ 3

- 最低でも 1 個のブリッジ ドメイン
- アプリケーション プロファイル
- 物理ドメインまたは VMM ドメイン

  VMM ドメインについて、VMM ドメインのクレデンシャルを設定し、vCenter/vShield コントローラ プロファイルを設定します。
- カプセル化ブロック範囲を持つ VLAN プール
- 最低でも 1 個の契約
- 最低でも 1 個の EPG

次のタスクを実行し、レイヤ 4 ～ 7 サービスを展開します。

1. デバイスおよび論理インターフェイスを登録します。

   このタスクでは、具象デバイスと具象インターフェイスも登録します。
2. **論理デバイス** を作成します。
3. オプション。ASA ファイアウォールサービスを設定している場合は、デバイスでトランキングを有効にします。
4. **デバイス選択ポリシー** を設定します。
5. **サービス グラフ テンプレート** を設定します。
6. 契約のサービス グラフ テンプレートを添付します。

（注） 仮想アプライアンスは、VLAN を使用して VMware ESX サーバとリーフ ノード間にトランスポートとして導入できますが、ハイパーバイザとして導入する場合は VMware ESX のみが使用できます。

レイヤ 4 ～ レイヤ 7 サービスデバイスについて

レイヤ 4 ～ レイヤ 7 サービスデバイスは、ファイアウォール、侵入防止システム (IPS)、ロードバランサなどのファブリックに接続される機能コンポーネントです。

サービス グラフ テンプレートについて

Cisco Application Centric Infrastructure（ACI）では、特定のタイプのファイアウォールとそれに続く特定のモデルおよびバージョンのロードバランサといった一連のメタデバイスを定義できます。これはサービスグラフテンプレートと呼ばれ、抽象グラフとも呼ばれます。抽象サービス グラフ テンプレートがコントラクトによって参照されると、サービス グラフ テンプレート

はファブリック内に存在するファイアウォールやロードバランサなどの具象デバイスにマッピングすることでインスタンス化されます。マッピングはコンテキストの概念で発生します。デバイスコンテキストは、Cisco ACI がどのファイアウォールとロードバランサを抽象グラフにマッピングできるかを識別可能にするマッピング設定です。もう 1 つの重要な概念は、具象デバイスのクラスタを表す論理デバイス、つまりデバイスクラスタです。サービス グラフ テンプレートのレンダリングは、コントラクトによって定義されるパスに挿入可能な適切な論理デバイスの識別に基づいています。

Cisco ACI はサービスをアプリケーションの重要部分として見なします。必要なサービスは、Cisco Application Policy Infrastructure Controller (APIC) から Cisco ACI ファブリックにインスタンス化されたサービスグラフとして見なします。ユーザは、アプリケーションに対してサービスを定義し、サービス グラフテンプレートはアプリケーションが必要とする一連のネットワークまたはサービス機能を識別します。グラフを Cisco APIC に設定すると、Cisco APIC はサービス グラフ テンプレートで指定されたサービス機能要件に基づいてサービスを自動的に設定します。さらに Cisco APIC は、サービス グラフ テンプレートで指定されたサービス機能のニーズに応じてネットワークを自動的に設定しますが、これによってサービスデバイスでの変更が必要になることはありません。

GUI を使用したレイヤ 4 ～ レイヤ 7 サービスの設定

次のリストは、GUI を使用してレイヤ 4 ～ レイヤ 7 サービスを構成する方法の概要を示しています。

1. デバイスを構成します。

   GUI を使用したレイヤ 4 ～ レイヤ 7 サービスデバイスの設定 （10 ページ）を参照してください。

   （オプション）デバイスを変更します。

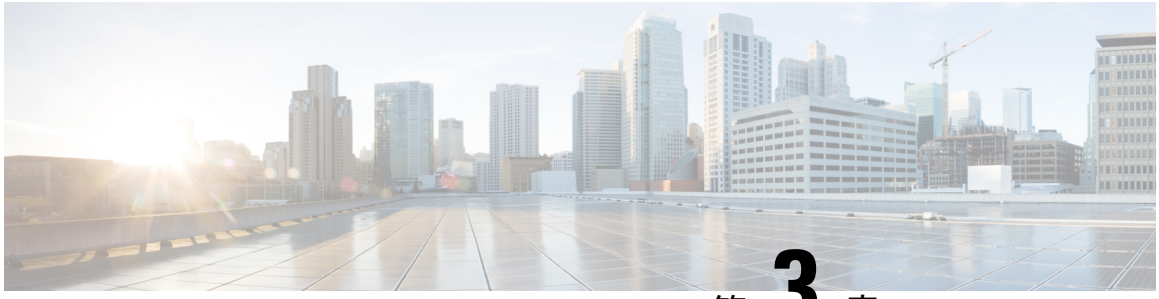
   GUI を使用したデバイスの変更 （22 ページ）を参照してください。

2. サービスグラフテンプレートを設定します。

   GUI でサービスグラフテンプレートを構成する （51 ページ）を参照してください。

3. エンドポイント グループ（EGP）にサービス グラフ テンプレートを適用します。

   「GUI を使用したエンドポイント グループへのサービス グラフ テンプレートの適用 （53 ページ）」を参照してください。



第 3 章

論理デバイスの定義

デバイス クラスタについて

デバイス クラスタ（別名論理デバイス）は、単一のデバイスとして機能する 1 つ以上の具象デバイスです。デバイス クラスタには、そのデバイス クラスタのインターフェイス情報を説明するクラスタ（論理）インターフェイスがあります。サービス グラフ テンプレートのレンダリング時に、機能ノード コネクタはクラスタ（論理）インターフェイスに関連付けられます。Application Policy Infrastructure Controller（APIC）は、サービス グラフ テンプレートのインスタンス化およびレンダリング時に機能ノード コネクタにネットワーク リソース（VLAN または Virtual Extensible Local Area Network（VXLAN））を割り当て、クラスタ（論理）インターフェイスにネットワーク リソースをプログラミングします。

Cisco APICでは、グラフのインスタンス化時にサービスグラフに対してネットワークリソースのみを割り当てて、ファブリック側のみをプログラミングできます。この動作は、既存のオーケストレータまたはデバイスクラスタ内のデバイスをプログラムするdev-opツールがすでにある環境では有効です。

Cisco APICはデバイス クラスタおよびデバイスのトポロジ情報（論理インターフェイスと具象インターフェイス）を把握する必要があります。この情報により、Cisco APICはリーフスイッチの適切なポートをプログラミングできます。また、Cisco APICではこの情報をトラブルシューティング ウィザードの目的で使用できます。さらに、Cisco APICはカプセル化の割り当てに使用するDomPとの関係も把握する必要があります。

次の設定は必要ありません。

- 論理デバイス（vnsLDevViP）およびデバイス（CDev）の接続情報：管理IPアドレス、ログイン情報、インバンド接続情報
- サポートする機能タイプ（go-through、go-to、L1、L2）に関する情報
- コンテキスト認識に関する情報（シングル コンテキストかマルチコンテキスト）

サービス グラフ テンプレートは、管理者が定義するデバイス選択ポリシー（論理デバイス コンテキストと呼ばれます）に基づく特定のデバイスを使用します。

管理者は、アクティブ/スタンバイ モードで最大2つの具象デバイスをセットアップできます。

デバイス クラスタをセットアップするには、次のタスクを実行する必要があります。

1. ファブリックに具象デバイスを接続します。
2. デバイス クラスタに管理 IP アドレスを割り当てます。
3. デバイス クラスタを Cisco APIC に登録します。

（注） Cisco APICは、2つのデバイスのクラスタにIPアドレスが重複して割り当てられているかどうかを検証しません。Cisco APICは、2つのデバイスのクラスタが同じ管理IPアドレスを持っている場合、不適切なデバイスのクラスタをプロビジョニングすることがあります。デバイスクラスタでIPアドレスが重複している場合には、いずれかのデバイスのIPアドレスの設定を削除し、管理IPアドレスの設定のためにプロビジョニングされたIPアドレスが重複していないことを確認してください。

具象デバイスについて

具象デバイスとしては、物理デバイスまたはバーチャル デバイスがあり得ますl。具象デバイスには、具象インターフェイスがあります。具象デバイスが論理デバイスに追加されると、具象インターフェイスが論理インターフェイスにマッピングされます。サービス グラフ テンプレートのインスタンス化時に、VLANおよびVXLANは、論理インターフェイスとの関連付けに基づいた具象インターフェイス上でプログラミングされます。

トランキングの概要

レイヤ 4 ～ レイヤ 7 仮想 ASA デバイスのトランキングを有効にでき、これはトランク ポート グループを使用してエンドポイント グループのトラフィックを集約します。トランキングを使用せず、仮想サービス デバイスには各インターフェイスに 1 個の VLAN のみ所有し、最大 10 個のサービス グラフを所有できます。トランキングが有効にしている状態では、仮想サービス デバイスはサービス グラフの数を無制限に設定できます。

トランク ポート グループについての詳細は、『*Cisco ACI Virtualization Guide*』を参照してください。

レイヤ 4 ～ レイヤ 7 サービスのエンドポイント グループについて

Application Policy Infrastructure Controller (APIC) を使用すると、グラフのインスタンス化中にグラフコネクタに使用するエンドポイントグループを指定できます。これにより、グラフ導入のトラブルシューティングが容易になります。APIC は、指定されたレイヤ 4 ～レイヤ 7 サービスエンドポイント グループを使用してリーフスイッチにカプセル化情報をダウンロードします。また、APIC はこのエンドポイント グループを使用して仮想デバイスの分散仮想スイッチにポート グループを作成します。さらに、レイヤ 4 ～ レイヤ 7 サービスのエンドポイント グループを使用して、グラフ コネクタのエラー情報や統計情報も集約します。

導入されたグラフ リソースへの可視性の向上に加えて、レイヤ 4 ～ レイヤ 7 サービスのエンドポイント グループも使用して、特定のグラフ インスタンスに使用する静的なカプセル化を指定することもできます。このカプセル化は、複数のグラフ インスタンス間でレイヤ 4 ～ レイヤ 7 サービスのエンドポイント グループを共有することによって、複数のグラフ インスタンス間で共有することもできます。

グラフ コネクタと共に レイヤ 4 ～ レイヤ 7 サービスのエンドポイントをどのように使用できるかを示す XML コードの例については、レイヤ 4 ～ レイヤ 7 サービスのエンドポイント グループとコネクタを関連付ける XML の例 （21 ページ）を参照してください。

グラフ コネクタに対する静的なカプセル化の使用

Application Policy Infrastructure Controller（APIC）は、処理中にさまざまなサービス グラフにカプセル化を割り当てます。一部の使用例では、サービス グラフ内の特定のコネクタに使用するカプセル化を明示的に指定できます。これは静的なカプセル化と呼ばれます。静的なカプセル化は、物理サービスを持つサービス デバイス クラスタがあるサービス グラフ コネクタについてのみサポートされます。仮想サービス デバイスがあるサービス デバイス クラスタは、そのサービス デバイス クラスタに関連付けられた VMware ドメインから動的に割り当てられた VLAN を使用します。

静的なカプセル化は、レイヤ 4 ～ レイヤ 7 サービスのエンドポイント グループの一部としてカプセル化値を指定することによってグラフ コネクタで使用できます。レイヤ 4 ～ レイヤ 7 サービスのエンドポイントで静的なカプセル化の使用方法を示すXML コードの例については、レイヤ 4 ～ レイヤ 7 サービスのエンドポイント グループで静的なカプセル化を使用する XML の例 （22 ページ）を参照してください。

GUI を使用したレイヤ 4 ～ レイヤ 7 サービスデバイスの設定

レイヤ4～レイヤ7サービスデバイスを作成すると、物理デバイスまたは仮想マシンのいずれかに接続できます。接続先のタイプによって、フィールドが若干異なります。物理デバイスに接続する場合は、物理インターフェイスを指定します。仮想マシンに接続する場合は、VMM ドメイン、仮想マシン、および仮想インターフェイスを指定します。さらに、不明モデルを選択することで、接続を手動で設定することもできます。

（注） ロードバランサであるレイヤ4～レイヤ7サービスデバイスを構成する場合、コンテキスト認識パラメータは使用されません。context aware パラメータには `single context` というデフォルト値がありますが、これは無視されます。

始める前に

- テナントを作成しておく必要があります。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ウィンドウで、**Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Devices** を選択します。

ステップ 4 作業ウィンドウで、 **Actions** > **Create L4-L7 Devices** を選択します。

ステップ 5 [Create L4-L7 Devices] ダイアログボックスで、[General] セクションの次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	デバイスの名前を入力します。

名前	説明
[Service Type] ドロップダウン リスト	サービス タイプを選択します。タイプは次のとおりです。 • ADC • ファイアウォール • その他 （注） レイヤ 1/レイヤ 2 ファイアウォール設定の場合は、[**その他（Other**）] を選択します。
[Device Type] ボタン	デバイス タイプを選択します。
[Physical Domain] ドロップダウン リストまたは [VMM Domain] ドロップダウン リスト	物理ドメインまたは VMM ドメインを選択します。
スイッチング モード （Cisco ACI Virtual Edgeのみ）	Cisco ACI Virtual Edge仮想ドメインでは、次のモードのいずれかを選択します: • **AVE**：トラフィックは Cisco ACI Virtual Edge を介して切り替えられます。 • **native**：トラフィックは VMware DVS を介して切り替えられます。
View ラジオボタンを表示します。	デバイスのビューを選択します。ビューとしては、次のものがあり得ます: • **単一ノード**：1 つのノードのみ • **HA ノード**：ハイアベイラビリティノード（2 ノード） • **クラスタ**：3 ノード以上

名前	説明
コンテキスト認識	デバイスのコンテキスト認識。認識は次のとおりです。 • **単一（Single）**：プロバイダーネットワークでホストされる特定のタイプの複数のテナントでは、デバイスクラスタを共有できません。特定のユーザーの特定のテナントにデバイスクラスタを提供する必要があります。 • **複数（Multiple）**：プロバイダーネットワークでホストされる特定のタイプの複数のテナント全体でデバイスクラスタを共有できます。たとえば、同じデバイスを共有する 2 つのホスティング会社が存在する可能性があります。 デフォルトは**単一（Single）**です。 （注） ロードバランサであるレイヤ 4 ～ レイヤ 7 サービスデバイスを作成する場合、**コンテキスト認識パラメータ**は使用されないため無視できます。
機能タイプ	機能種別は次のとおりです。 • **GoThrough**：透過モード • **GoTo**：ルーテッドモード • **L1**：レイヤ 1 ファイアウォールモード • **L2**：レイヤ 2 ファイアウォールモード デフォルトは **GoTo** です。 （注） レイヤ 1 またはレイヤ 2 モードの場合、チェックボックスをオンにしてアクティブ/アクティブモードを有効にします。有効にすると、レイヤ 1/レイヤ 2 PBR デバイスのアクティブ/アクティブ展開/ECMP パスがサポートされます。

ステップ 6 [Device 1] セクションで、次のフィールドに入力します。

名前	説明
[VM] ドロップダウン リスト	（仮想デバイス タイプの場合のみ）仮想マシンを選択します。

ステップ 7 [Device Interfaces] テーブルで、[+] ボタンをクリックしてインターフェイスを追加し、次のフィールドに入力します。

名前	説明
[Name] ドロップダウン リスト	インターフェイス名を選択します。

名前	説明
[VNIC] ドロップダウン リスト	（仮想デバイス タイプの場合のみ）vNIC を選択します。
[Path] ドロップダウン リスト	（物理デバイスタイプまたはL3Outのインターフェイスの場合み）インターフェイスが接続されるポート、ポートチャネル、仮想ポートチャネルを選択します。

ステップ 8 [Update] をクリックします。

ステップ 9 （HA クラスタの場合のみ）各デバイスのフィールドに入力します。

ステップ 10 [**クラスタインターフェイス（Cluster Interfaces**）] セクションのフィールドに入力します。

[+] をクリックしてクラスタインターフェイスを追加し、次の詳細を入力します。

名前	説明
[Name] ドロップダウン リスト	クラスタ インターフェイスの名前を入力します。
Concrete Interfaces ドロップダウンリスト	具象インターフェイスを選択します。ドロップダウンリストのインターフェイスは、手順7で作成したデバイスインターフェイスに基づいています。
[**拡張 LAG ポリシー（Enhanced Lag Policy**）] ドロップダウンリスト	（オプション）デバイスのVMMドメインに構成されている LAG ポリシーを選択します。 このオプションは、[**デバイスタイプ（Device Type**）] (手順 5 で説明) を [**Virtual（仮想**）] に選択した場合にのみ使用できます。

HA クラスタでは、クラスタのインターフェイスが、クラスタ内の両方の具体デバイスにある対応するインターフェイスにマッピングされていることを確認してください。

ステップ 11 [Finish] をクリックします。

NX OS スタイル CLI を使用したレイヤ 4 ～ レイヤ 7 の作成

レイヤ4～レイヤ7デバイスを作成するときに、物理デバイスまたは仮想マシンのいずれかに接続できます。物理デバイスに接続する場合は、物理インターフェイスを指定します。仮想マシンに接続する場合は、VMM ドメイン、仮想マシン、および仮想インターフェイスを指定します。

（注） ロード バランサであるレイヤ 4 ～ レイヤ 7 デバイスを設定する場合、[コンテキスト認識] パラメータは使用されません。[コンテキスト認識] パラメータには、無視可能な シングル コンテキスト のデフォルト値があります。

始める前に

- テナントを作成しておく必要があります。

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 テナントのコンフィギュレーション モードを開始します。

```
tenant tenant_name
```

例：

```
apic1(config)# tenant t1
```

ステップ 3 レイヤ 4 ～ レイヤ 7 デバイス クラスタを追加します。

```
l4l7 cluster name cluster_name type cluster_type vlan-domain domain_name
  [function function_type] [service service_type]
```

パラメータ	説明
名前	デバイス クラスタの名前。
type	デバイス クラスタのタイプ。値は次のとおりです。 • virtual • physical
vlan-domain	VLANの割り当てに使用するドメイン。このドメインは、仮想デバイスの場合はVMMドメイン、物理デバイスの場合は物理ドメインである必要があります。
switching-mode （Cisco ACI Virtual Edgeのみ）	（オプション）次のいずれかのモードを選択します。 • **AVE**：Cisco ACI Virtual Edge を通過するトラフィックのスイッチ。 • **ネイティブ**：VMware DVS を通過するトラフィックのスイッチ。これはデフォルト値です。

パラメータ	説明
機能	（任意）機能タイプ。値は次のとおりです。 • go-to • go-through • L1 • L2
service	（任意）サービス タイプ。ADC 固有またはファイアウォール固有のアイコンおよび GUI を表示するために GUI で使用します。値は次のとおりです。 • ADC • FW • OTHERS

例：

物理デバイスの場合は、次のように入力します。

```
apic1(config-tenant)# l4l7 cluster name D1 type physical vlan-domain phys
  function go-through service ADC
```

仮想デバイスの場合は、次のように入力します。

```
apic1(config-tenant)# l4l7 cluster name ADCCluster1 type virtual vlan-domain mininet
```

ステップ 4 1 つ以上のクラスタ デバイスをデバイス クラスタに追加します。

```
cluster-device device_name [vcenter vcenter_name] [vm vm_name]
```

パラメータ	説明
vcenter	（仮想デバイスの場合のみ）仮想デバイスの仮想マシンをホストする VCenter の名前。
vm	（仮想デバイスの場合のみ）仮想デバイスの仮想マシンの名前。

例：

物理デバイスの場合は、次のように入力します。

```
apic1(config-cluster)# cluster-device C1
apic1(config-cluster)# cluster-device C2
```

仮想デバイスの場合は、次のように入力します。

```
apic1(config-cluster)# cluster-device C1 vcenter vcenter1 vm VM1
apic1(config-cluster)# cluster-device C2 vcenter vcenter1 vm VM2
```

ステップ 5 1 つ以上のクラスタ インターフェイスをデバイス クラスタに追加します。

```
cluster-interface interface_name [vlan static_encap]
```

パラメータ	説明
vlan	（仮想デバイスの場合のみ）クラスタ インターフェイスのスタティックなカプセル化。VLAN の値は、1 ～ 4094 とする必要があります。

例：

物理デバイスの場合は、次のように入力します。

```
apic1(config-cluster)# cluster-interface consumer vlan 1001
```

仮想デバイスの場合は、次のように入力します。

```
apic1(config-cluster)# cluster-interface consumer
```

ステップ 6 1 つ以上のメンバーをクラスタ インターフェイスに追加します。

```
member device device_name device-interface interface_name
```

パラメータ	説明
デバイス	**cluster-device** コマンドを使用して、このデバイスにすでに追加されている必要があるクラスタ デバイスの名前。
device-interface	クラスタ デバイス上のインターフェイスの名前。

例：

```
apic1(config-cluster-interface)# member device C1 device-interface 1.1
```

ステップ 7 メンバーにインターフェイスを追加します。

```
interface {ethernet ethernet_port | port-channel port_channel_name [fex fex_ID] |
  vpc vpc_name [fex fex_ID]} leaf leaf_ID
```

インターフェイスではなく vNIC を追加する場合は、このステップをスキップします。

パラメータ	説明
ethernet	（イーサネットまたは FEX イーサネット インターフェイスの場合のみ）クラスタ デバイスがCisco Application Centric Infrastructure（ACI）ファブリックに接続されるリーフ上のイーサネット ポート。FEX イーサネット メンバーを追加する場合は、FEX IDと FEX ポートの両方を次の形式で指定します。 *FEX_ID/FEX_port* 次に例を示します。 101/1/23 FEX ID は、クラスタ デバイスがファブリック エクステンダにどこで接続するかを指定します。
port-channel	（ポート チャネルまたは FEX ポート チャネル インターフェイスの場合のみ）クラスタ デバイスが ACI ファブリックに接続されるポート チャネル名。

パラメータ	説明
vpc	（バーチャル ポート チャネルまたはFEXバーチャル ポート チャネル インターフェイスの場合のみ）クラスタ デバイスがACIファブリックに接続されるバーチャル ポート チャネル名。
fex	（ポート チャネル、FEX ポート チャネル、バーチャル ポート チャネル、またはFEX バーチャル ポートの場合のみ）ポート チャネルまたはバーチャル ポート チャネルの形成に使用するスペース区切りリスト形式の FEX ID。
leaf	クラスタ デバイスがどこで接続するかのスペース区切りリスト内のリーフ ID。

例：

イーサネット インターフェイスの場合は、次のように入力します。

```
apic1(config-member)# interface ethernet 1/23 leaf 101
apic1(config-member)# exit
```

FEX イーサネット インターフェイスの場合は、次のように入力します。

```
apic1(config-member)# interface ethernet 101/1/23 leaf 101
apic1(config-member)# exit
```

ポート チャネル インターフェイスの場合は、次のように入力します。

```
apic1(config-member)# interface port-channel pc1 leaf 101
apic1(config-member)# exit
```

FEX ポート チャネル インターフェイスの場合は、次のように入力します。

```
apic1(config-member)# interface port-channel pc1 leaf 101 fex 101
apic1(config-member)# exit
```

バーチャル ポート チャネル インターフェイスの場合は、次のように入力します。

```
apic1(config-member)# interface vpc vpc1 leaf 101 102
apic1(config-member)# exit
```

FEX バーチャル ポート チャネル インターフェイスの場合は、次のように入力します。

```
apic1(config-member)# interface vpc vpc1 leaf 101 102 fex 101 102
apic1(config-member)# exit
```

ステップ 8 メンバーに vNIC を追加します。

```
vnic "vnic_name"
```

vNIC の代わりにインターフェイスを追加する場合は、前のステップを参照してください。

パラメータ	説明
vnic	クラスタ デバイスの仮想マシンの vNIC アダプタの名前。名前を二重引用符で囲みます。

例：

```
apic1(config-member)# vnic "Network adapter 2"
apic1(config-member)# exit
```

ステップ 9 デバイスの作成が完了したら、コンフィギュレーション モードを終了します。

例：

```
apic1(config-cluster-interface)# exit
apic1(config-cluster)# exit
apic1(config-tenant)# exit
apic1(config)# exit
```

NX-OS スタイルの CLI を使用したハイ アベイラビリティ クラスタの作成

次に、NX-OS スタイルの CLI を使用してハイ アベイラビリティ クラスタを作成する手順の例を示します。

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 テナントのコンフィギュレーション モードを開始します。

```
tenant tenant_name
```

例：

```
apic1(config)# tenant t1
```

ステップ 3 クラスタを作成します。

例：

```
apic1(config-tenant)# l4l7 cluster name ifav108-asa type physical vlan-domain phyDom5 servicetype
FW
```

ステップ 4 クラスタ デバイスを追加します。

例：

```
apic1(config-cluster)# cluster-device C1
apic1(config-cluster)# cluster-device C2
```

ステップ 5 プロバイダー クラスタ インターフェイスを追加します。

例：

```
apic1(config-cluster)# cluster-interface provider vlan 101
```

ステップ 6 インターフェイスにメンバー デバイスを追加します。

例：

```
apic1(config-cluster-interface)# member device C1 device-interface Po1
apic1(config-member)# interface vpc VPCPolASA leaf 103 104
apic1(config-member)# exit
```

```
apic1(config-cluster-interface)# exit
apic1(config-cluster-interface)# member device C2 device-interface Po2
apic1(config-member)# interface vpc VPCPolASA-2 leaf 103 104
apic1(config-member)# exit
apic1(config-cluster-interface)# exit
```

ステップ 7 別のプロバイダー クラスタ インターフェイスを追加します。

例：

```
apic1(config-cluster)# cluster-interface provider vlan 102
```

ステップ 8 最初のインターフェイスからこの新しいインターフェイスに同じメンバー デバイスを追加します。

例：

```
apic1(config-cluster-interface)# member device C1 device-interface Po1
apic1(config-member)# interface vpc VPCPolASA leaf 103 104
apic1(config-member)# exit
apic1(config-cluster-interface)# exit
apic1(config-cluster-interface)# member device C2 device-interface Po2
apic1(config-member)# interface vpc VPCPolASA-2 leaf 103 104
apic1(config-member)# exit
apic1(config-cluster-interface)# exit
```

ステップ 9 クラスタ作成モードを終了します。

例：

```
apic1(config-cluster)# exit
```

NX-OS スタイルの CLI を使用した仮想デバイスの作成

次に、NX-OS スタイルの CLI を使用して仮想デバイスを作成する手順の例を示します。

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 テナントのコンフィギュレーション モードを開始します。

```
tenant tenant_name
```

例：

```
apic1(config)# tenant t1
```

ステップ 3 クラスタを作成します。

例：

```
apic1(config-tenant)# l4l7 cluster name ifav108-citrix type virtual vlan-domain ACIVswitch servicetype
 ADC
```

ステップ 4 クラスタ デバイスを追加します。

例：

```
apic1(config-cluster)# cluster-device D1 vcenter ifav108-vcenter vm NSVPX-ESX
```

ステップ 5 コンシューマ クラスタ インターフェイスを追加します。

例：

```
apic1(config-cluster)# cluster-interface consumer
```

ステップ 6 コンシューマ インターフェイスにメンバー デバイスを追加します。

例：

```
apic1(config-cluster-interface)# member device D1 device-interface 1_1
apic1(config-member)# interface ethernet 1/45 leaf 102
ifav108-apic1(config-member)# vnic "Network adapter 2"
apic1(config-member)# exit
apic1(config-cluster-interface)# exit
```

ステップ 7 プロバイダー クラスタ インターフェイスを追加します。

例：

```
apic1(config-cluster)# cluster-interface provider
```

ステップ 8 プロバイダー インターフェイスに同じメンバー デバイスを追加します。

例：

```
apic1(config-cluster-interface)# member device D1 device-interface 1_1
apic1(config-member)# interface ethernet 1/45 leaf 102
ifav108-apic1(config-member)# vnic "Network adapter 2"
apic1(config-member)# exit
apic1(config-cluster-interface)# exit
```

ステップ 9 クラスタ作成モードを終了します。

例：

```
apic1(config-cluster)# exit
```

論理デバイスを作成する XML の例

LDevVip オブジェクトを作成する XML の例

次の XML の例では、`LDevVip` オブジェクトを作成します。

```
<polUni>
    <fvTenant name="HA_Tenant1">
        <vnsLDevVip name="ADCCluster1" devtype="VIRTUAL" managed="no">
            <vnsRsALDevToDomP tDn="uni/vmmp-VMware/dom-mininet"/>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

Cisco ACI Virtual Edge の場合、次の XML の例では、スイッチングモードが ave である Cisco ACI Virtual Edge VMM ドメインに関連付けられた LDevVip オブジェクトが作成されます。

```
<polUni>
    <fvTenant name="HA_Tenant1">
        <vnsLDevVip name="ADCCluster1" devtype="VIRTUAL" managed="no">
          <vnsRsALDevToDomP switchingMode="AVE" tDn="uni/vmmp-VMware/dom-mininet_ave"/>

        </vnsLDevVip>
    </fvTenant>
</polUni>
```

AbsNode オブジェクトを作成する XML の例

次の XML の例では、AbsNode オブジェクトを作成します。

```
<fvTenant name="HA_Tenant1">
    <vnsAbsGraph name="g1">
        <vnsAbsTermNodeProv name="Input1">
            <vnsAbsTermConn name="C1">
            </vnsAbsTermConn>
        </vnsAbsTermNodeProv>

        <!-- Node1 provides a service function -->
        <vnsAbsNode name="Node1" managed="no">
            <vnsAbsFuncConn name="outside" >
            </vnsAbsFuncConn>
            <vnsAbsFuncConn name="inside" >
            </vnsAbsFuncConn>
        </vnsAbsNode>

        <vnsAbsTermNodeCon name="Output1">
            <vnsAbsTermConn name="C6">
            </vnsAbsTermConn>
        </vnsAbsTermNodeCon>

        <vnsAbsConnection name="CON2" >
            <vnsRsAbsConnectionConns
              tDn="uni/tn-HA_Tenant1/AbsGraph-g1/AbsTermNodeCon-Output1/AbsTConn"/>
            <vnsRsAbsConnectionConns
              tDn="uni/tn-HA_Tenant1/AbsGraph-g1/AbsNode-Node1/AbsFConn-outside"/>
        </vnsAbsConnection>

        <vnsAbsConnection name="CON1" >
            <vnsRsAbsConnectionConns
              tDn="uni/tn-HA_Tenant1/AbsGraph-g1/AbsNode-Node1/AbsFConn-inside"/>
            <vnsRsAbsConnectionConns
              tDn="uni/tn-HA_Tenant1/AbsGraph-g1/AbsTermNodeProv-Input1/AbsTConn"/>
        </vnsAbsConnection>
    </vnsAbsGraph>
</fvTenant>
```

レイヤ 4 ～ レイヤ 7 サービスのエンドポイント グループとコネクタを関連付ける XML の例

次に、レイヤ 4 ～ レイヤ 7 サービスのエンドポイント グループとコネクタを関連付ける XML の例を示します。

```
<fvTenant name="HA_Tenant1">
    <vnsLDevCtx ctrctNameOrLbl="any" descr=""
dn="uni/tn-HA_Tenant1/ldevCtx-c-any-g-any-n-any"
      graphNameOrLbl="any" name="" nodeNameOrLbl="any">
        <vnsRsLDevCtxToLDev tDn="uni/tn-HA_Tenant1/lDevVip-ADCCluster1"/>
        <vnsLIfCtx connNameOrLbl="inside" descr="" name="inside">
            <vnsRsLIfCtxToSvcEPg tDn="uni/tn-HA_Tenant1/ap-sap/SvcEPg-EPG1"/>
            <vnsRsLIfCtxToBD tDn="uni/tn-HA_Tenant1/BD-provBD1"/>
            <vnsRsLIfCtxToLIf tDn="uni/tn-HA_Tenant1/lDevVip-ADCCluster1/lIf-inside"/>
        </vnsLIfCtx>
        <vnsLIfCtx connNameOrLbl="outside" descr="" name="outside">
            <vnsRsLIfCtxToSvcEPg tDn="uni/tn-HA_Tenant1/ap-sap/SvcEPg-EPG2"/>
            <vnsRsLIfCtxToBD tDn="uni/tn-HA_Tenant1/BD-consBD1"/>
            <vnsRsLIfCtxToLIf tDn="uni/tn-HA_Tenant1/lDevVip-ADCCluster1/lIf-outside"/>
        </vnsLIfCtx>
    </vnsLDevCtx>
</fvTenant>
```

レイヤ 4 ～ レイヤ 7 サービスのエンドポイント グループで静的なカプセル化を使用する XML の例

次の XML の例では、レイヤ 4 ～ レイヤ 7 サービスエンドポイント グループで静的カプセル化を使用しています。

```
<polUni>
    <fvTenant name="HA_Tenant1">
        <fvAp name="sap">
            <vnsSvcEPg name="EPG1" encap="vlan-3510">
            </vnsSvcEPg>
        </fvAp>
    </fvTenant>
</polUni>
```

GUI を使用したデバイスの変更

デバイスを作成した後で、そのデバイスを変更することができます。

（注） デバイスを作成するか、または既存のクラスタにデバイスを追加するには、「デバイスの作成」の手順を使用する必要があります。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ウィンドウで、**Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Devices** > ***device_name*** を選択します。
[Work] ウィンドウにデバイスに関する情報が表示されます。

ステップ 4 **General** セクションではいくつかのパラメータを変更するコ音ができます。

Device 1 セクションでは、インターフェイスの追加、または既存のインターフェイスのパスの変更を行えます。インターフェイスを追加するには、**+** ボタンをクリックします。パスを変更するには、変更するパスをダブルクリックします。

ステップ 5 パラメータを変更した後、**Submit** をクリックします。

GUI を使用してレイヤ 7 仮想 ASA デバイスにレイヤ 4 でのトランキングを有効化

次の手順では、GUI を使用したレイヤ 7 仮想 ASA デバイスにレイヤ 4 でのトランキングが有効にします。

始める前に

- ASA デバイスの仮想レイヤ 7 にレイヤ 4 に設定した必須。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。
ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。
ステップ 3 [Navigation] ウィンドウで、**Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Devices** > ***device_name*** を選択します。
ステップ 4 [Work] ウィンドウで、**Trunking Port** チェック ボックスをオンにします。
ステップ 5 [送信（Submit）] をクリックします。

REST Api を使用してレイヤ 7 仮想 ASA デバイスにレイヤ 4 でのトランキングを有効化

次の手順では、REST Api を使用して、レイヤ 7 仮想の ASA デバイスにレイヤ 4 でのトランキングを有効にする例を示します。

始める前に

- ASA デバイスの仮想レイヤ 7 にレイヤ 4 に設定した必須。

名前付きレイヤ 7 デバイスにレイヤ 4 でのトランキングを有効にする `InsiemeCluster` ：

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="InsiemeCluster" devtype=“VIRTUAL” trunking=“yes">
            ...
```

```
        ...
      </vnsLDevVip>
    </fvTenant>
</polUni>
```

REST API とともにインポートされたデバイスの使用

次の REST API ではインポートされたデバイスを使用します。

```
<polUni>
  <fvTenant dn="uni/tn-tenant1" name="tenant1">
    <vnsLDevIf ldev="uni/tn-mgmt/lDevVip-ADCCluster1"/>
    <vnsLDevCtx ctrctNameOrLbl="any" graphNameOrLbl="any" nodeNameOrLbl="any">
     <vnsRsLDevCtxToLDev tDn="uni/tn-tenant1/lDevIf-[uni/tn-mgmt/lDevVip-ADCCluster1]"/>

      <vnsLIfCtx connNameOrLbl="inside">
        <vnsRsLIfCtxToLIf
tDn="uni/tn-tenant1/lDevIf-[uni/tn-mgmt/lDevVip-ADCCluster1]/lDevIfLIf-inside"/>
        <fvSubnet ip="10.10.10.10/24"/>
        <vnsRsLIfCtxToBD tDn="uni/tn-tenant1/BD-tenant1BD1"/>
      </vnsLIfCtx>
      <vnsLIfCtx connNameOrLbl="outside">
        <vnsRsLIfCtxToLIf
tDn="uni/tn-tenant1/lDevIf-[uni/tn-mgmt/lDevVip-ADCCluster1]/lDevIfLIf-outside"/>
        <fvSubnet ip="70.70.70.70/24"/>
        <vnsRsLIfCtxToBD tDn="uni/tn-tenant1/BD-tenant1BD4"/>
      </vnsLIfCtx>
    </vnsLDevCtx>
  </fvTenant>
</polUni>
```

NX-OS スタイルの CLI を使用した別のテナントからのデバイスの作成

共有サービスのシナリオでは、別のテナントからデバイスをインポートできます。

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 テナントのコンフィギュレーション モードを開始します。

```
tenant tenant_name
```

例：

```
apic1(config)# tenant t1
```

ステップ 3 デバイスをインポートします。

```
l4l7 cluster import-from tenant_name device-cluster device_name
```

パラメータ	説明
import-from	デバイスのインポート元のテナントの名前。
device-cluster	指定したテナントからインポートするデバイス クラスタの名前。

例：

```
apic1(config-tenant)# l4l7 cluster import-from common device-cluster d1
apic1(config-import-from)# end
```

GUI を使用したデバイスのインポートの確認

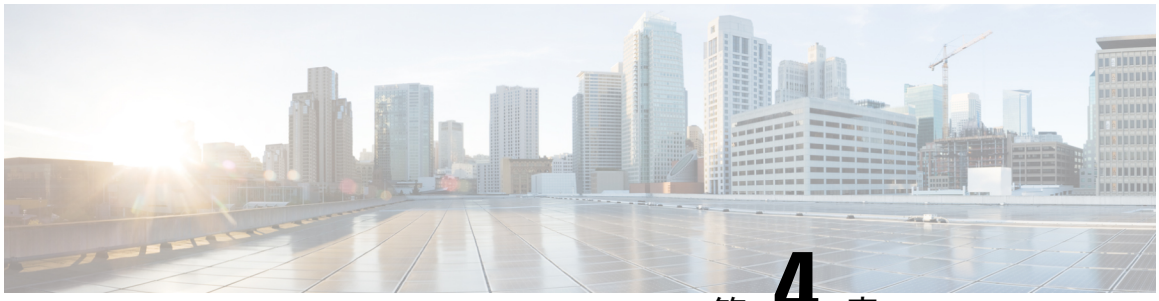
GUI を使用して、デバイスが正常にインポートされたことを確認することができます。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ウィンドウで、**Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Imported Devices** > ***device_name*** を選択します。

デバイス情報が [Work] ペインに表示されます。



第 4 章

サービス VM オーケストレーション

サービス VM オーケストレーション

サービス仮想マシン（VM）オーケストレーションは、Cisco Application Policy Infrastructure Controller（APIC）でのサービス VM の作成と管理を容易にするポリシーベースの機能です。サービス VM オーケストレーションは、Cisco APIC 4.0(1) の VMware vCenter 環境向けの新機能です。

以前は、VMware vCenter でサービス VM を作成し、そのサービス VM が属していたデータセンターを定義してデータストアに関連付ける必要がありました。また、管理ネットワークの設定および Cisco APIC への接続も必要でした。ところが、サービス VM オーケストレーションを使用すると、これらのタスクをすべて Cisco APIC で実行できます。

サービス VM オーケストレーションは、具象デバイス（CDev）とも呼ばれるサービス VM の設定プロセスを合理化します。CDev は、論理デバイス（LDev）とも呼ばれるデバイスクラスタにグループ化されます。LDev に適用される設定とポリシーは、LDev に含まれている各 CDev に適用されます。

サービス VM オーケストレーションを使用するには、コンフィギュレーション ファイルを作成してアップロードします。次に VM インスタンス化ポリシーを設定してレイヤ 4 ～レイヤ 7 LDev を作成し、LDev に関連付ける CDev を作成します。サービス VM オーケストレーションを設定する前に、サービス VM オーケストレーションの注意事項と制約事項 （28 ページ）を読んで理解してください。

サービス VM オーケストレーション タスクは、Cisco APIC GUI、NX-OS スタイル CLI、または REST API を使用して実行できます。説明については、次の項を参照してください。

- Cisco APIC GUI を使用したサービス VM オーケストレーションの設定 （29 ページ）

• NX-OS スタイル CLI を使用したサービス VM オーケストレーションの設定 （35 ページ）
• REST API を使用したサービス VM オーケストレーションの設定 （36 ページ）

サービス VM オーケストレーションの注意事項と制約事項

サービス VM オーケストレーションを使用する場合は、次の注意事項と制約事項に留意してください。

- サービス VM オーケストレーションは Cisco 適応型セキュリティ仮想アプライアンス（ASAv）および Palo Alto Networks デバイスでのみサポートされます。
- サービス VM オーケストレーションを使用したハイ アベイラビリティ（HA）仮想マシン（VM）の導入は、共有ストレージでのみサポートされます。ローカルデータ ストアではサポートされません。
- 単一サービス VM または HA サービス VM の導入では、Dynamic Host Configuration Protocol（DHCP）IP アドレッシングはサポートされません。
- VMware vCenter で作成されたポート グループまたは VM テンプレートについては、サービス VM オーケストレーションを使用する前に、Cisco Application Policy Infrastructure Controller（APIC）でインベントリを手動で同期する必要があります。設定に関するドキュメントでインベントリの同期をトリガーする方法を確認してください。
- Palo Alto の導入は、デフォルトのユーザー名 **admin** とパスワード **admin** でのみ動作します。
- Palo Alto デバイスを導入すると、「`Script error: force config push is required`」と表示されて Cisco APIC で 10 分間の障害が発生します。このメッセージの原因は Palo Alto デバイスで実行されている内部プロセスです。設定が正常にプッシュされてデバイスが安定すると、障害は解消されます。
- Cisco APIC は、削除および再導入後に Cisco 適応型セキュリティ仮想アプライアンス（ASAv）デバイスに到達できません。この問題は、上流に位置するスイッチで古い MAC アドレスがクリアされていないために発生します。上流に位置するスイッチでサービス VM に使用される IP アドレスの MAC エントリをクリアし、サービス VM オーケストレーションを使用してサービス VM を再導入してください。
- 既存のポリシーを複製する場合は、複製が完了するまで、論理デバイスに関連付けられている VM インスタンス化ポリシーを変更しないでください。
- サービス VM オーケストレーションを使用してサービス VM を導入するには、追加の VMware vCenter 権限を有効にします。『*Cisco ACI Virtualization Guide*』で「Cisco ACI with VMware VDS Integration」の章の「Custom User Account with Minimum VMware vCenter Privileges」を参照してください。

Cisco APIC GUI を使用したサービス VM オーケストレーションの設定

Cisco Application Policy Infrastructure Controller（APIC）GUI でいくつかのタスクを実行してサービス VM オーケストレーションを設定できます。

Cisco APIC GUI を使用した VM インスタンス化ポリシーの作成

仮想マシン（VM）インスタンス化ファイルの作成は、サービス仮想マシン（VM）オーケストレーションを使用して Cisco Application Policy Infrastructure Controller でサービス VM を導入および管理するプロセスの最初のタスクです。デバイス クラスタまたは論理デバイス（LDev）用に作成されたポリシーが、LDev に属する具象デバイス（CDev）に適用されます。

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[Tenants]** > テナント > **[Policies]** > **[VMM]** > **[VM Instantiation Policies]** に移動します。

ステップ 3 作業ウィンドウの右上隅にあるハンマーとレンチのアイコンをクリックし、[Create VM Instantiation Policy] を選択します。

ステップ 4 [Create VM Instantiation Policy] ダイアログボックスで、次の手順を実行します。

a) [Name] フィールドにポリシーの名前を入力します。

b) [Controller] ドロップダウンリストからコントローラを選択します。

c) [VM Template] ドロップダウンリストで、作成するサービス VM のテンプレートを選択します。

ドロップダウンリストには、コントローラに関連付けられている VM テンプレートが表示されます。

（注） VMware vCenter で作成した VM テンプレートが表示されない場合は、次の手順を実行します。

1. [Controller] ドロップダウンリストの横にある青色のアイコンをクリックします。
2. [Controller Instance] ダイアログボックスの右側にあるレンチとハンマーのアイコンをクリックし、[Trigger Inventory Sync]、[Yes] の順にクリックして同期をトリガーします。
3. [Controller Instance] ダイアログボックスを閉じて [Create VM Instantiation Policy] ダイアログボックスに戻ります。

d) [Host Name] ドロップダウンリストで、サービス VM を導入するホストを選択します。

VMware vSphere 分散リソース スケジューラ（DRS）クラスタまたは個々のホストを選択できます。

e) [Data Store] ドロップダウンリストで、VM ディスクを配置するデータ ストアを選択します。

f) [Submit] をクリックします。
作業ウィンドウに VM インスタンス化ポリシーが表示されます。

GUI を使用してレイヤ 4 ～ レイヤ 7 サービスデバイスを作成して VM インスタンス化ポリシーに関連付ける

この手順では、レイヤ 4 ～ レイヤ 7 サービスデバイスを作成し、事前に作成した仮想マシン（VM）インスタンス化ポリシーに関連付けます。

レイヤ 4 ～ レイヤ 7 サービスデバイスを作成すると、物理デバイスまたは仮想マシンのいずれかに接続できます。接続先のタイプによって、フィールドが若干異なります。物理デバイスに接続する場合は、物理インターフェイスを指定します。仮想マシンに接続する場合は、VMM ドメイン、仮想マシン、および仮想インターフェイスを指定します。また、不明モデルを選択して接続を手動で設定することもできます。

VM インスタンス化ポリシーに関連付けるレイヤ 4 ～ レイヤ 7 のサービスデバイスを作成する場合は、ポリシーを指定して新しいサービス VM を作成することもできます。

（注） ロードバランサであるレイヤ 4 ～ レイヤ 7 サービスデバイスを構成する場合、コンテキスト認識パラメータは使用されません。context aware パラメータのデフォルト値は single context コンテキストです。無視することができます。

始める前に

- テナントを作成しておく必要があります。
- VM インスタンス化ポリシーを作成済みである必要があります。Cisco APIC GUI を使用した VM インスタンス化ポリシーの作成 （29 ページ）の項を参照してください。

ステップ 1 Cisco Application Policy Infrastructure Controller（APIC）にログインします。

ステップ 2 **[Tenants]** > テナント > **[Services]** > **[L4-L7]** > **[Devices]** に移動します。

ステップ 3 [Devices] を右クリックして [Create L4-L7 Devices] を選択します。

または、作業ウィンドウの右上にあるアクションアイコン（交差したハンマーとレンチ）をクリックし、[Create L4-L7 Devices] を選択することもできます。

ステップ 4 [Create L4-L7 Devices] ダイアログボックスで、[General] セクションの次のフィールドに入力します。

名前	説明
名前（**Name**）	レイヤ 4 ～ レイヤ 7 サービスデバイスの名前を入力します。

名前	説明
サービス タイプ	ドロップダウンリストからサービスの種類を選択します。次のいずれかの種類を選択できます。 • [ADC]（アプリケーション配信コントローラ） [ADC] は、デフォルトのサービスの種類です。 • [Firewall]：ルーテッドまたはトランスペアレント展開モードを選択します。 • [Other]：その他のモード。 （注） ポリシーベース リダイレクト設定では、サービスの種類として [Firewall] または [ADC] を選択します。
Device Type	[**仮想**（**Virtual**）]（仮想レイヤ 4 ～ レイヤ 7 サービスデバイス）を選択します。
VMM ドメイン	ドロップダウンリストから VMM ドメインを選択します。
VM Instantiation Policy	ドロップダウンリストで、前に作成した VM インスタンス化ポリシーを選択します。 ポリシーを選択すると、新しいレイヤ 4 ～ レイヤ 7 サービスデバイスに関連付けられます。VMware vCenter で自動的に VM を作成することもできます。
無差別モード	サービスグラフの展開後に生成される Cisco Application Centric Infrastructure (ACI) で管理されるポートグループで無差別モードを有効にするには、チェックボックスをオンにします。 無差別モードを有効にすると、ポート グループのすべてのトラフィックが無差別ポートに接続されている VM に到達できます。

名前	説明
コンテキスト認識	[Single]（デフォルト）または [Multiple] を選択します。 [Single] を選択した場合、プロバイダー ネットワーク上でホストされた特定のタイプの複数のテナントでデバイス クラスタを共有することはできません。特定のユーザーの特定のテナントにデバイス クラスタを提供する必要があります。 [Multiple] を選択した場合は、プロバイダー ネットワーク上でホストする特定のタイプの複数のテナントでデバイス クラスタを共有できます。たとえば、同じデバイスを共有する 2 つのホスティング会社が存在する可能性があります。
機能タイプ	次のオプションを選択できます。 • [GoThrough]（トランスペアレント モード） • [GoTo]（ルーテッド モード）

ステップ 5 [Devices] セクションでプラス アイコンをクリックします。

ステップ 6 **[デバイスの作成手順 1 （Create Device STEP 1）] > [デバイス（Device）]** ダイアログボックスで、次のフィールドに入力して具象デバイス (CDev) を構成し、レイヤ 4 ～ レイヤ 7 サービスデバイスに関連付けます。

名前	説明
Gateway IP	新しいサービス VM のゲートウェイ IP アドレスを入力します。
[Subnet Mask]	新しいサービス VM のサブネットマスクを入力します。
Management vNIC	ドロップダウンリストから新しいサービス VM の管理 vNIC を選択します。
VM	VMware vCenter に表示される新しいサービス VM の VM 名を入力します。

名前	説明
Host （任意）	ドロップダウンリストから新しいサービス VM のホストを選択します。ホストを選択しない場合は、VMインスタンス化ポリシーで選択されているホストが使用されます。 ポリシーベース リダイレクト（PBR）およびDirect Server Return（DSR）機能の場合は、トポロジに基づいて特定のホストを選択する必要があります。その場合は正しいホストを選択してください。 DSR と PDR の場合は、コンピューティング VM とサービス VM を同じトップオブラック（ToR）スイッチ ペアに置くことはできません。したがって PBR または DSR トポロジのサービス VM を導入するためのホストを選択する必要があります。選択しないと、機能によってサービス VM がコンピューティング VM と同じホストに導入される可能性があります。 Cisco アプリケーションセントリック インフラストラクチャ (ACI) 仮想 Edge で接続するデバイスの場合、同じホストにハイアベイラビリティのレイヤ4 ～ レイヤ 7 サービスデバイスを展開することはできません。したがって、プライマリ VM とセカンダリ VM に異なるホストを選択します。
Port Group Name （任意）	ドロップダウンリストで、新しいサービス VM を導入するポート グループを選択します。選択しない場合は、VMテンプレートで使用されているポート グループが使用されます。
HA EPG （任意）	新しいサービス VM のハイ アベイラビリティ（HA）通信用に、HA エンドポイント グループ（EPG）か、vSwitch または分散型仮想スイッチ（DVS）ポート グループをドロップダウンリストから選択します。
HA Network Adapter （任意）	ドロップダウンリストから新しいサービス VM 用の HA ネットワーク アダプタを選択します。
Username	新しいサービス VM のユーザー名を入力します。
Password	新しいサービス VM のパスワードを入力します。
Confirm Password	パスワードを再入力します。

ステップ 7 [次へ] をクリックします。

ステップ 8 [Create Device STEP 2] > [Interfaces] ダイアログボックスの [Interfaces] セクションで、プラス アイコンをクリックします。

ステップ 9 ダイアログボックスで次のフィールドに入力し、CDev のインターフェイスを設定します。

名前	説明
名前（Name）	ドロップダウンリストからレイヤ 4 ～ レイヤ 7 サービス デバイス インターフェイスの名前を選択します。
vNIC （仮想デバイス タイプのみ）	ドロップダウンリストから VM ネットワーク アダプタの名前を選択します。
Path （レイヤ 4 ～ レイヤ 7 サービスデバイスが仮想デバイスの場合はオプション）	インターフェイスを接続するポート、ポート チャネル（PC）、またはバーチャル ポート チャネル（VPC）を選択します。

ステップ 10 [Interfaces] セクションでプラス アイコンをもう一度クリックし、別のインターフェイスを設定します。

ステップ 11 [Update] をクリックします。

ステップ 12

ステップ 13 レイヤ 4 ～ レイヤ 7 サービスデバイスにサービス VM をさらに追加するには、手順 8 ～手順 13 を繰り返します。

ステップ 14 複数のサービス VM を使用する場合は、[Create Device STEP 1] > [Device] ダイアログボックスの [Cluster] セクションで、デバイスごとに次のフィールドに入力します。

HA クラスタでは、クラスタのインターフェイスが、クラスタ内の両方の具体デバイスにある対応するインターフェイスにマッピングされていることを確認してください。

名前	説明
[Cluster Interfaces] 領域	次のフィールドに入力して、レイヤ 4 ～ レイヤ 7 サービスデバイスの外部接続を設定します。 • [Type] ドロップダウンリストからクラスタ インターフェイス タイプを選択します。タイプは次のとおりです。 • **failover_link** • **ユーティリティ** • **consumer** • **provider** • **mgmt** • **cluster_ctrl_lk** • **failover-lan** • **consumer and provider** • [Name] ドロップダウンリストからクラスタ インターフェイス名を選択します。 • [Concrete Interfaces] ドロップダウンリストで、関連付けられている具象インターフェイスを選択します。

ステップ 15 [Finish] をクリックします。

次のタスク

[Recent Tasks] で、VMware vCenter での新しいサービス VM の作成を確認できます。表示されるまでにしばらく時間がかかることがあります。

NX-OS スタイル CLI を使用したサービス VM オーケストレーションの設定

NX-OS スタイル CLI を使用して、仮想マシン（VM）インスタンス化ポリシーとレイヤ 4 ～レイヤ 7 具象デバイスを作成し、デバイスをインスタンス化ポリシーにマッピングできます。その後、内部および外部インターフェイスを VM ネットワーク アダプタにマッピングできます。

ステップ 1 VM インスタンス化ポリシーを作成します。

例：

```
APIC1(config-tenant)# inst-pol VMPolName VMMname VcentercontrollerName VMtemplateName ClusterName
datastorename
```

ステップ 2 レイヤ 4 ～レイヤ 7 具象デバイスを作成して VM インスタンス化ポリシーに関連付けます。

例：

```
APIC1(config)# tenant T0
APIC1(config-tenant)# l4l7 cluster name ASA-Single type virtual vlan-domain ASAVMM switching-mode
AVE vm-instantiation-policy ASA-Template-Pol  service FW function go-to context single trunking
disable
```

ステップ 3 内部および外部インターフェイスを VM ネットワーク アダプタにマッピングします。

例：

```
APIC1(config-cluster)# cluster-interface external
APIC1(config-cluster-interface)# member device ASA-Cdev device-interface GigabitEthernet0/0
APIC1(config-member)# vnic "Network adapter 2"
APIC1(config-member)# exit
APIC1(config-cluster)# cluster-interface internal
APIC1(config-cluster-interface)# member device ASA-Cdev device-interface GigabitEthernet0/1
APIC1(config-member)# vnic "Network adapter 3"
APIC1(config-member)# exit
APIC1(config-cluster-interface)# exit
APIC1(config-cluster)#
```

REST API を使用したサービス VM オーケストレーションの設定

REST API を使用してサービス VM オーケストレーションを設定できます。

サービス VM オーケストレーションを設定します。

例：

```
<vnsLDevVip contextAware="single-Context" devtype="VIRTUAL"
  dn="uni/tn-T0/lDevVip-NEW-HA-LDEV-20" funcType="GoTo" isCopy="no" mode="legacy-Mode"
  name="NEW-HA-LDEV-20" promMode="no" svcType="FW" trunking="no">
    <vnsLIf encap="unknown" name="client">
        <vnsRsMetaIf isConAndProv="no"
          tDn="uni/infra/mDev-CISCO-ASA-1.3/mIfLbl-external"/>
        <vnsRsCIfAttN
          tDn="uni/tn-T0/lDevVip-NEW-HA-LDEV-20/cDev-CDEV-HA-S1-NEW/cIf-[GigabitEthernet0/0]"/>
        <vnsRsCIfAttN
          tDn="uni/tn-T0/lDevVip-NEW-HA-LDEV-20/cDev-CDEV-HA-P1-NEW/cIf-[GigabitEthernet0/0]"/>
    </vnsLIf>
    <vnsLIf encap="unknown" name="server">
        <vnsRsMetaIf isConAndProv="no" tDn="uni/infra/mDev-CISCO-ASA-1.3/mIfLbl-internal"/>
        <vnsRsCIfAttN
```

```
      tDn="uni/tn-T0/lDevVip-NEW-HA-LDEV-20/cDev-CDEV-HA-S1-NEW/cIf-[GigabitEthernet0/1]"/>
    <vnsRsCIfAttN
      tDn="uni/tn-T0/lDevVip-NEW-HA-LDEV-20/cDev-CDEV-HA-P1-NEW/cIf-[GigabitEthernet0/1]"/>
</vnsLIf>
<vnsRsLDevVipToInstPol tDn="uni/tn-T0/svcCont/instPol-HA-POL"/>
<vnsRsALDevToDomP switchingMode="AVE" tDn="uni/vmmp-VMware/dom-mininet"/>
<vnsCDev cloneCount="0" host="10.197.146.188" isCloneOperation="no" isTemplate="no"
  name="CDEV-HA-S1-NEW" vcenterName="orionin103-vcenter1" vmName="ASA-S1-VM-20">
    <vnsHAPortGroup portGroupName="10.197.146.188 | VLAN2500-172-25"
      vnicName="Network adapter 10"/>
    <vnsDevFolder key="FailoverConfig" name="FailoverConfig">
        <vnsDevParam key="lan_unit" name="lan_unit" value="secondary"/>
        <vnsDevParam key="failover" name="failover" value="enable"/>
        <vnsDevFolder key="mgmt_standby_ip" name="mgmt_standby_ip">
            <vnsDevParam key="standby_ip" name="standby_ip" value="10.197.146.178"/>
        </vnsDevFolder>
        <vnsDevFolder key="polltime" name="polltime">
            <vnsDevParam key="interval_value" name="interval_value" value="1"/>
            <vnsDevParam key="interval_unit" name="interval_unit" value="second"/>
            <vnsDevParam key="holdtime_value" name="holdtime_value" value="3"/>
        </vnsDevFolder>
        <vnsDevFolder key="failover_link_interface" name="failover_link_interface">
            <vnsDevParam key="use_lan" name="use_lan" value="fover"/>
            <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
            <vnsDevParam key="interface" name="interface" value="GigabitEthernet0/8"/>
        </vnsDevFolder>
        <vnsDevFolder key="failover_ip" name="failover_ip">
            <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
            <vnsDevParam key="active_ip" name="active_ip" value="172.25.0.178"/>
            <vnsDevParam key="netmask" name="netmask" value="255.255.0.0"/>
            <vnsDevParam key="standby_ip" name="standby_ip" value="172.25.0.179"/>
        </vnsDevFolder>
        <vnsDevFolder key="failover_lan_interface" name="failover_lan_interface">
            <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
            <vnsDevParam key="interface" name="interface" value="GigabitEthernet0/8"/>
        </vnsDevFolder>
    </vnsDevFolder>
    <vnsCIf name="GigabitEthernet0/1" vnicName="Network adapter 3"/>
    <vnsCIf name="GigabitEthernet0/0" vnicName="Network adapter 2"/>
</vnsCDev>
<vnsCDev cloneCount="0" host="10.197.146.187" isCloneOperation="no" isTemplate="no"
  name="CDEV-HA-P1-NEW" vcenterName="orionin103-vcenter1" vmName="ASA-P1-VM-20">
    <vnsHAPortGroup portGroupName="10.197.146.187 | VLAN2500-172-25"
      vnicName="Network adapter 10"/>
    <vnsDevFolder key="FailoverConfig" name="FailoverConfig">
        <vnsDevParam key="lan_unit" name="lan_unit" value="primary"/>
        <vnsDevParam key="failover" name="failover" value="enable"/>
        <vnsDevFolder key="failover_ip" name="failover_ip">
            <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
            <vnsDevParam key="standby_ip" name="standby_ip" value="172.25.0.179"/>
            <vnsDevParam key="netmask" name="netmask" value="255.255.0.0"/>
            <vnsDevParam key="active_ip" name="active_ip" value="172.25.0.178"/>
        </vnsDevFolder>
        <vnsDevFolder key="failover_lan_interface" name="failover_lan_interface">
            <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
            <vnsDevParam key="interface" name="interface" value="GigabitEthernet0/8"/>
        </vnsDevFolder>
        <vnsDevFolder key="mgmt_standby_ip" name="mgmt_standby_ip">
            <vnsDevParam key="standby_ip" name="standby_ip" value="10.197.146.179"/>
        </vnsDevFolder>
        <vnsDevFolder key="failover_link_interface" name="failover_link_interface">
            <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
            <vnsDevParam key="use_lan" name="use_lan" value="fover"/>
            <vnsDevParam key="interface" name="interface" value="GigabitEthernet0/8"/>
```

```
            </vnsDevFolder>
            <vnsDevFolder key="polltime" name="polltime">
                <vnsDevParam key="holdtime_value" name="holdtime_value" value="3"/>
                <vnsDevParam key="interval_unit" name="interval_unit" value="second"/>
                <vnsDevParam key="interval_value" name="interval_value" value="1"/>
            </vnsDevFolder>
        </vnsDevFolder>
        <vnsCIf name="GigabitEthernet0/1" vnicName="Network adapter 3"/>
        <vnsCIf name="GigabitEthernet0/0" vnicName="Network adapter 2"/>
    </vnsCDev>
    <vnsRsMDevAtt tDn="uni/infra/mDev-CISCO-ASA-1.3"/>
</vnsLDevVip>
```

サービスVMオーケストレーションのトラブルシューティング

ここでは、サービスVMオーケストレーションの既知の問題と制限事項、および問題が発生した場合のトラブルシューティング手順について説明します。

サービス VM テンプレートが VM インスタンス化ポリシーに表示されない

VMware vCenter で作成したサービス VM テンプレートが VM インスタンス化ポリシーに表示されない場合は、次の手順を実行します。

ステップ 1 **vnsInstPol** を使用して Visore を確認し、`vmTemplate` を探します。

vnsInstPol フィールドの値がない場合、または値が null の場合は、次の手順に進みます。

ステップ 2 インベントリの同期をトリガーします。

a) Cisco Application Policy Infrastructure Controller（APIC）で **[Virtual Networking]** > **[Inventory]** に移動し、[VMM Domains] および [VMware] フォルダを展開します。
b) VMM ドメインをクリックします。
c) 中央のペインでコントローラをダブルクリックします。
d) [VMM Controller] ダイアログボックスでハンマーとレンチのドロップダウンリストから [Trigger Inventory Sync] を選択し、プロンプトが表示されたら [Yes] をクリックします。

ステップ 3 仮想マシン（VM）インスタンス化ポリシーを確認します（VMM ドメインにマッピングされているコントローラを選択し、VM テンプレートが存在するかどうかを確認してください）。

VMware vCenter で作成したポート グループが CDev に表示されない

VMware vCenter で作成したポート グループが具象デバイス（CDev）に表示されない場合は、次の手順を実行します。

ステップ 1 インベントリの同期をトリガーします。

a) Cisco Application Policy Infrastructure Controller（APIC）で **[Virtual Networking]** > **[Inventory]** に移動し、[VMM Domains] および [VMware] フォルダを展開します。
b) VMM ドメインをクリックします。
c) 中央のペインでコントローラをダブルクリックします。
d) [VMM Controller] ダイアログボックスでハンマーとレンチのドロップダウンリストから [Trigger Inventory Sync] を選択し、プロンプトが表示されたら [Yes] をクリックします。

ステップ 2 ポート グループが表示されるかどうかを確認します。

a) **[Tenants]** > **テナント** > **[Services]** > **[L4-L7]** > **[Devices]** > **デバイス**に移動し、デバイスをクリックします。

ステップ 3 [Concrete Device] 作業ウィンドウで、[Port Group Name] ドロップダウンリストにポート グループが表示されるかどうかを確認します。

サービス VM の IP アドレスに到達できない

サービス仮想マシン（VM）の導入後にサービス仮想マシン（VM）の IP アドレスに到達できない場合は、次の手順を実行します。

ステップ 1 Cisco Application Policy Infrastructure Controller（APIC）でサービス VM の接続性を確認します。

Cisco APIC は、削除および再導入後に Cisco 適応型セキュリティ仮想アプライアンス（ASAv）デバイスに到達できません。この問題は、上流に位置するスイッチで古い MAC アドレスがクリアされていないために発生します。サービス VM に使用される IP アドレスの MAC エントリをクリアしてサービス VM を再導入してください。

ステップ 2 デバイス管理で vSwitch ポート グループを使用している場合は、Cisco APIC と VMware vCenter の間にあるすべての中間スイッチおよびデバイスで、VLAN およびルートの存在を確認します。

Cisco APIC は、サービス VM が正常に導入されたかどうかを確認するために、デバイスの IP アドレスに ping を実行できる必要があります。

ステップ 3 具象デバイス（CDev）の管理インターフェイスに対して、適切なポート グループまたは EPG が選択されていることを確認します。

ステップ 4 サービス VM がアップストリーム ゲートウェイに到達できるように接続性を確認します。

デバイスの状態が Init と表示される

デバイスの状態が init と表示される場合は、次の手順を実行します。

ステップ 1 NX-OS スタイル CLI から、サービス デバイスの到達可能性を確認する ping を実行します。

ステップ 2 サービスデバイスへのログインクレデンシャルがデバイス設定で指定されたユーザ名とパスワードに一致することを確認します。

ステップ 3 サービス デバイスの仮想 IP アドレスおよびポートが開いていることを確認します。

ステップ 4 Cisco Application Policy Infrastructure Controller（APIC）設定でユーザー名とパスワードが正しいことを確認します。

LIF 設定が無効である

論理デバイスの `lif-invalid-Clf` が原因で論理インターフェイス（LIF）の設定が無効になる F0772 障害が発生した場合は、次の手順を実行します。

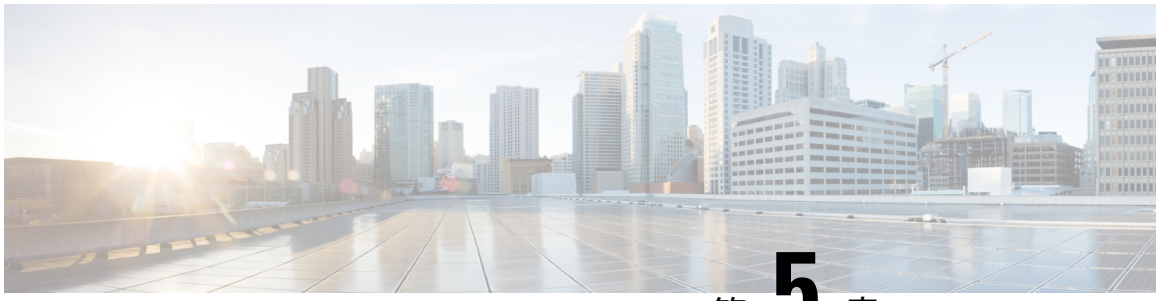
ステップ 1 LIF および具象インターフェイス（ClF）と呼ばれる項目を特定します。

この特定の障害において、LIF は正しくレンダリングされていない要素です。これは、機能ノードが LIF を実際のインターフェイスまたは具象インターフェイスにマッピングして関係を形成する場合に発生します。

F0772 は、次のいずれかの問題を意味します。

- LIF が作成されてない。
- LIF が正しい具象インターフェイスにマッピングされていない。

ステップ 2 レイヤ 4 ～ レイヤ 7 デバイスの状態に関するその他の問題については、このマニュアルのトラブルシューティングの情報を参照してください。



第 5 章

グラフをレンダリングするレイヤ 4 ～ レイヤ 7 デバイスの選択

デバイス選択ポリシーについて

デバイスは、コントラクト名、グラフ名、またはグラフ内の機能ノード名に基づいて選択できます。デバイスを作成した後は、デバイスに選択条件ポリシーを提供するデバイス コンテキストを作成できます。

デバイス選択ポリシー（デバイス コンテキストとも呼ばれる）は、サービス グラフ テンプレートのデバイスを選択するためのポリシーを指定します。これにより、管理者は複数のデバイスを持つことができ、それらを異なるサービス グラフ テンプレートに対して使用することができます。たとえば、管理者は、高いパフォーマンス ADC アプライアンスがあるデバイスと、パフォーマンスが低い ADC アプライアンスがある別のデバイスを持つことができます。高いパフォーマンスの ADC デバイス用と低いパフォーマンスの ADC デバイス用の 2 つの異なるデバイス選択ポリシーを使用して、管理者は高いパフォーマンスが必要となるアプリケーションには高いパフォーマンスの ADC デバイスを選択し、低いパフォーマンスが必要なアプリケーションには低いパフォーマンスの ADC デバイスを選択することができます。

GUI を使用したデバイス選択ポリシーの作成

Apply L4-L7 Service Graph Template To EPGs ウィザードを使用せずにサービス グラフ テンプレートを適用した場合には、デバイス選択ポリシー(論理デバイス コンテキストとも呼ばれる)を設定することが必要になる可能性があります。デバイス選択ポリシーは Cisco Application Centric Infrastructure (ACI) に対し、グラフのレンダリングのためにどのファイアウォールやロード バランサを使用するかを指定します。

Apply L4-L7 Service Graph Template To EPGs ウィザードを使用してサービス グラフ テンプレートを適用した場合には、デバイス選択ポリシーは自動的に設定されるので、手動での設定を行う必要はありません。

デバイスクラスタ インターフェイスを intra-vrf および inter-vrf コントラクトに使用する場合は、デバイス選択ポリシーのコンテキスト名を設定する必要があります。コンテキスト名は、個別の展開されたグラフインスタンスによって共有される同じデバイスに対して同一である必要があります。

たとえば、intra-vrf 用の contract1 と inter-vrf トラフィック用の contract2 がある場合、両方のコントラクトにサービスグラフがあり、同じデバイスクラスタ インターフェイスを使用する場合は、デバイス選択ポリシーに同じコンテキスト名を設定する必要があります。

（注） NX OS スタイルの CLI を使用すると、デバイス選択ポリシーは自動的に設定されますが、同等の NX-OS スタイルの CLI コマンドはありません。

すでに導入されているサービス グラフ テンプレートにコピー デバイスを追加する場合には、コピー サービスのために使用するデバイス選択ポリシーを作成する必要があります。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ウィンドウで、**Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Devices Selection Policies**.

ステップ 4 [Work] ペインで、**[Actions]** > **[Create Logical Device Context]** の順に選択します。

ステップ 5 [Create Logical Device Context] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [Contract Name] ドロップダウンリストで、デバイス選択ポリシーの契約を選択します。デバイスを使用する条件の一部として契約名を使用しない場合は、**any** を選択します。

b) **Graph Name** ドロップダウンリストで、デバイス選択ポリシーのためのグラフを選択します。デバイスを使用する条件の一部としてグラフ名を使用しない場合は、**any** を選択します。

c) **Node Name** ドロップダウンリストで、デバイス選択ポリシーのためのノードを選択します。デバイスを使用する条件の一部としてグノード名を使用しない場合は、[any] を選択します。

ステップ 6 [Cluster Interface Contexts] セクションの [+] をクリックしてクラスタ インターフェイス コンテキストを追加します。

ステップ 7 [Create A Cluster Interface Context] ダイアログボックスで次のプロパティを設定します。

プロパティ	説明
Connector Name	コネクタの名前または論理インターフェイス コンテキストのラベルです。デフォルトは **Any** です。
Cluster Interface	ターゲット インターフェイスの一意の名前。このフィールドは必須です。

プロパティ	説明
関連付けられたネットワーク	関連付けられたネットワークタイプを選択します。選択可能なタイプは次のとおりです。 • **ブリッジドメイン**：サービスグラフの展開中に、インターフェイスに対してサービスEPGが新規に作成されます。 • **L3Out**：既存の L3Out EPG がインターフェイスに使用されます。
ブリッジ ドメイン	対象のインターフェイスに関連付けられたネットワークのブリッジドメインを選択します。このドロップダウンリストは、**関連付けられたネットワーク**に**ブリッジドメイン**を選択した場合にのみ表示されます。 エニーキャストの場合は、ノードに使用するブリッジ ドメインと同じである必要があります。
L3Out	対象のインターフェイスに関連付けられたネットワークのL3Out EPGを選択します。このドロップダウンリストは、**関連付けられたネットワーク**に**L3Out**を選択した場合にのみ表示されます。
L3 Destination (VIP)	この論理インターフェイスによって、サービスチェーン内のレイヤ 3 トラフィックが終端されているかどうかを示します。 このパラメータのデフォルトは有効（オン）です。ただし、論理インターフェイスコンテキストにポリシーベースリダイレクトポリシーが設定されている場合、この設定は考慮されません。 （注） マルチノードPBRでは、この論理インターフェイスが仮想 IP 外部ネットワークで終端されるロードバランサのコンシューマー構成の場合、このボックスにチェックを入れ、次のフィールド（**L4 ～ L7 ポリシーベースリダイレクト**）のリダイレクトポリシーと関連するものをすべて削除します。 この論理インターフェイスがロード バランサのプロバイダー構築で、かつSNATを実行している場合は、このボックスをオンにして、次のフィールド（[L4-L7 Policy Based Redirect]）でリダイレクト ポリシーへの関連付けを削除します。

プロパティ	説明
L4-L7 Policy Based Redirect	オプション。ポリシーベースリダイレクトポリシーを選択するか、**L4 ～ L7 ポリシーベースリダイレクトを作成します**。 （注） マルチノードPBRでは、この論理インターフェイスが仮想IPアドレス外部ネットワークで終端されるロードバランサのコンシューマー構成の場合、リダイレクトポリシー（入力されている場合）への関連付けを削除して、[**L3 Destination (VIP)**] ボックスをオンにします。
L4 ～ L7 サービス EPG ポリシー	優先グループのインターフェイスのサービスEPGを含めるか除外するかを選択します。デフォルトでは、サービス EPG は除外されています。
Custom QoS Policy	オプション。カスタムQoSポリシーまたはデフォルトポリシーを指定するか、[Create Custom QoS Policy] を選択します。このドロップダウンリストは、**関連付けられたネットワーク**に**ブリッジドメイン**を選択した場合にのみ表示されます。
Preferred Contract Group	優先グループポリシーの適用タイプ。有効なタイプは次のとおりです。 • [Include]：このポリシー オプションで設定されたEPGまたはインターフェイスはサブグループに含まれ、サブグループ内で契約なしで通信できます。 • [Exclude]：このポリシー オプションで設定されたEPGまたはインターフェイスはサブグループに含まれず、サブグループ内で契約なしで通信することはできません。
Permit Logging	インターフェイス コンテキストの許可ロギングを有効にするには、ボックスにチェックを入れます。デフォルトではディセーブルになっています。
Subnets	[+] をクリックしてサブネットを追加します。 ゲートウェイアドレス、サブネットのネットワーク可視性（範囲）、プライマリ IPアドレス（優先サブネット）、およびサブネット制御の状態を設定します。

プロパティ	説明
仮想 IP アドレス	このサブネットがレイヤ 3 仮想接続先に使用されている場合（**L3 接続先 (VIP)** のチェックボックスがオンになっている）は、[+] をクリックして仮想 IP アドレス (VIP) を追加します。

ステップ 8 [OK] をクリックします。

ステップ 9 [送信（Submit）] をクリックします。

REST API を使用したデバイス選択ポリシーの設定

REST API を使用してデバイス選択ポリシーを設定することができます。

REST API を使用してデバイス選択ポリシーの作成

次の REST API ではデバイス選択ポリシーを作成します。

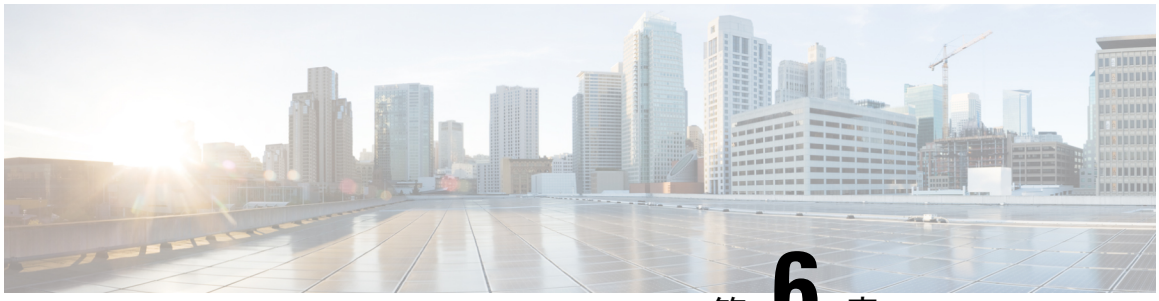
```
<polUni>
    <fvTenant dn="uni/tn-acme" name="acme">
       <vnsLDevCtx ctrctNameOrLbl="webCtrct" graphNameOrLbl="G1" nodeNameOrLbl="Node1">

            <vnsRsLDevCtxToLDev tDn="uni/tn-acme/lDevVip-ADCCluster1"/>

             <!-- The connector name C4, C5, etc.. should match the
                  Function connector name used in the service graph template -->

             <vnsLIfCtx connNameOrLbl="C4">
                <vnsRsLIfCtxToLIf tDn="uni/tn-acme/lDevVip-ADCCluster1/LIf-ext"/>
            </vnsLIfCtx>
            <vnsLIfCtx connNameOrLbl="C5">
                <vnsRsLIfCtxToLIf tDn="uni/tn-acme/lDevVip-ADCCluster1/LIf-int"/>
            </vnsLIfCtx>
        </vnsLDevCtx>
    </fvTenant>
</polUni>
```

REST API を使用したデバイスでの論理インターフェイスの追加

次の REST API はデバイス内に論理インターフェイスを追加します。

```
<polUni>
    <fvTenant dn="uni/tn-acme" name="acme">
        <vnsLDevVip name="ADCCluster1">

            <!-- The LIF name defined here (such as e.g., ext, or int) should match the

                 vnsRsLIfCtxToLIf 'tDn' defined in LifCtx  -->

            <vnsLIf name="ext">

                <vnsRsMetaIf tDn="uni/infra/mDev-Acme-ADC-1.0/mIfLbl-outside"/>
```

```
                    <vnsRsCIfAtt tDn="uni/tn-acme/lDevVip-ADCCluster1/cDev-ADC1/cIf-ext"/>
                </vnsLIf>
                <vnsLIf name="int">
                    <vnsRsMetaIf tDn="uni/infra/mDev-Acme-ADC-1.0/mIfLbl-inside"/>
                    <vnsRsCIfAtt tDn="uni/tn-acme/lDevVip-ADCCluster1/cDev-ADC1/cIf-int"/>
                </vnsLIf>
            </vnsLDevVip>
        </fvTenant>
    </polUni>
```



第 6 章

サービス グラフの設定

サービス グラフについて

Cisco Application Centric Infrastructure（ACI）はアプリケーションの重要部分としてサービスを見なします。必要なサービスは、Cisco Application Policy Infrastructure Controller（APIC）からの Cisco ACI ファブリックでインスタンス化されたサービス グラフとして処理されます。ユーザは、アプリケーションに対してサービスを定義し、サービス グラフはアプリケーションが必要とする一連のネットワークまたはサービス機能を識別します。

サービス グラフは、次の要素を使ってネットワークを表します。

- 機能ノード：機能ノードは、トランスフォーム（SSL ターミネーション、VPN ゲートウェイ）、フィルタ（ファイアウォール）、または端末（侵入検知システム）など、トラフィックに適用される機能を表します。サービス グラフ内の 1 つの機能は 1 つ以上のパラメータを必要とし、1 つまたは複数のコネクタを持っている場合があります。
- 端末ノード：端末ノードはサービスグラフからの入出力を有効にします。
- コネクタ：コネクタはノードからの入出力を有効にします。

- 接続：接続によって、ネットワーク経由でトラフィックを転送する方法が決定されます。

グラフが Cisco APIC に設定されると、Cisco APIC はサービス グラフに明記されたサービス機能の要件に従って、サービスを自動的に設定します。Cisco APIC はまた、サービス グラフで指定されるサービス機能のニーズに応じてネットワークを自動的に設定しますが、これによってサービス デバイスでの変更は要求されません。

サービス グラフは、アプリケーションの複数の階層として表され、適切なサービス機能が間に挿入されます。

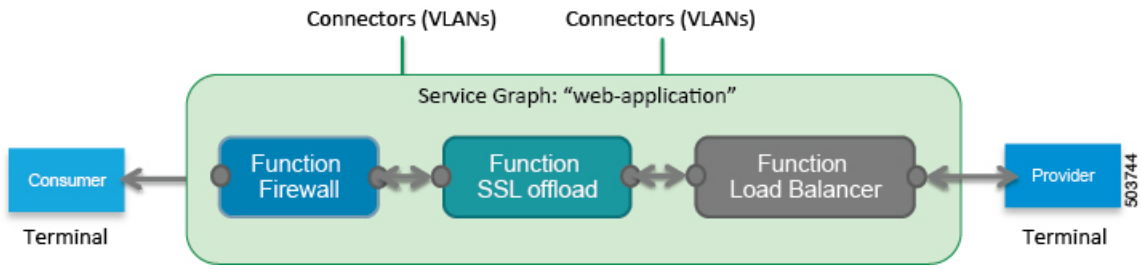
サービス アプライアンス（デバイス）は、グラフ内でサービス機能を実行します。1 つ以上のサービス アプライアンスが、グラフに必要なサービスをレンダリングするために必要になることがあります。1 つ以上のサービス機能が単一のサービス デバイスで実行できます。

サービス グラフおよびサービス機能には、次の特性があります。

- エンドポイント グループで送受信されたトラフィックはポリシーに基づいてフィルタリングでき、トラフィックのサブセットはグラフ内の異なるエッジにリダイレクトできます。
- サービス グラフのエッジには方向性があります。
- タップ（ハードウェア ベースのパケット コピー サービス）は、サービス グラフの異なるポイントに接続できます。
- 論理機能は、ポリシーに基づいて適切な（物理または仮想）デバイスでレンダリングできます。
- サービス グラフでは、エッジの分割と結合がサポートされ、管理者は線形サービス チェーンに制限されません。
- トラフィックは、サービス アプライアンスが発信した後にネットワーク内で再度分類できます。
- 論理サービス機能は、要件に応じて、拡張や縮小が可能で、クラスタ モードまたは 1:1 アクティブ/スタンバイ ハイアベイラビリティ モードで展開できます。

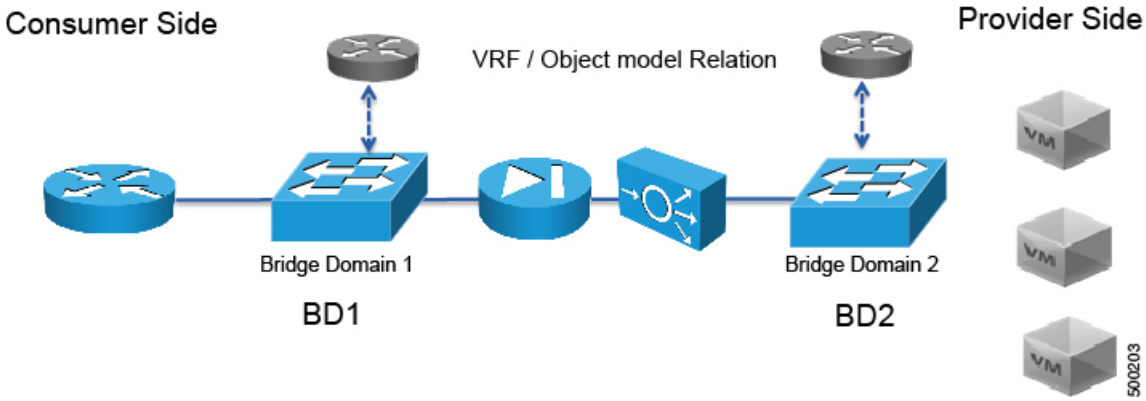
次の図は、サービスグラフの導入の例を示しています:

図 *1:* サービス グラフの展開の例



サービスグラフを展開するには、次の図に示すようにブリッジドメインと VRF インスタンスが必要です。

図 *2:* サービスグラフのブリッジドメインと *VRF* インスタンス



（注） 使用すると、その他のテナント内のエンドポイント グループに関連付けられているサービス グラフの脚の一部があるかどうか、 **グラフ テンプレートの関連のオブジェクトを削除** GUI で、機能、 Cisco APIC 以外のテナントからインポートされた契約は削除されませんサービス グラフが存在します。Cisco APICもサービス グラフよりも異なるテナントにあるエンドポイント グループ契約のクリーニングはありません。手動で異なるテナントではこれらのオブジェクトを削除する必要があります。

機能ノードについて

機能ノードは、単一のサービス機能を表します。機能ノードには、サービス機能のネットワーク要件を表す機能ノード コネクタがあります。

Cisco Application Policy Infrastructure Controller (APIC) は、ネットワークリソースを割り当てて、ファブリック側で VLAN/VXLAN のプログラミングのみを実行します。

次の設定は必要ありません。

- `MFunc` の関係
- サポートされる機能タイプ（go-through、go-to）に関する情報

Cisco APIC は、機能ノードのネットワーク情報（LIF、CIF）を把握する必要があります。この情報は、Cisco APIC がリーフスイッチでネットワークを適切にプログラムするためと、Cisco APIC がこの情報をトラブルシューティング ウィザードの目的で使用するために必要です。

さらに、次の設定が必要です。

- グラフ インスタンス化時に `LDevVip` の選択を可能にする `LDevCtx`
- グラフ インスタンス化時に `LIf` の選択を可能にする `LIfCtx`
- `LIfCtx` 内のブリッジ ドメイン

- LIfCtx でのルート ピアリング
- LIfCtx 内のサブネット

（注） Cisco ACI マルチサイト 構成の場合、サービスグラフに最大 2 つのノードを展開できます。非 Cisco ACI マルチサイト 構成の場合、サービスグラフに最大 5 つのノードを展開できます。

機能ノード コネクタについて

機能ノード コネクタは、サービス グラフに機能ノードを接続し、グラフのコネクタ サブネットに基づいて適切なブリッジ ドメインと接続と関連付けられます。各コネクタは、VLAN または Virtual Extensible LAN（VXLAN）に関連付けられます。コネクタの両側がエンドポイント グループ（EPG）として扱われ、ホワイトリストがスイッチにダウンロードされ、2 つの機能ノード間の通信がイネーブルになります。

サービス グラフ接続について

サービス グラフ接続は、1 つの機能ノードを別の機能ノードに接続します。

端末ノードについて

端末ノードはサービス グラフとコントラクトを接続します。コントラクトに端末ノードを接続することにより、2台のアプリケーションエンドポイントグループ（EPG）間のトラフィックにサービス グラフを挿入できます。接続されると、コントラクトのコンシューマ EPG とプロバイダー EPG 間のトラフィックはサービス グラフにリダイレクトされます。

サービスの注意事項と制限事項

サービスグラフの設定に関する注意事項と制限事項を以下に示します。

- 以下のようなサービスグラフ関連の構成
  - ブリッジドメイン（サービスグラフで使用する場合）およびサービスグラフテンプレートには、その名前の一部に文字列「C-」を含めることができません。
  - 論理デバイスは、その名前の一部に文字列「N-」を含めることができません。

GUI でサービスグラフテンプレートを構成する

サービスグラフテンプレートは、レイヤ 4 ～ レイヤ 7 サービス機能、レイヤ 4 ～ レイヤ 7 サービスデバイス、またはコピーデバイスとそれらに関連する一連の設定です。サービスグラフテンプレートは、レイヤ 4 ～ レイヤ 7 サービスデバイスまたはコピーデバイス、およびファブリック上で「レンダリング済み（rendered）」または設定されるコントラクトに関連付けられている必要があります。

始める前に

テナントを作成しておく必要があります。

ステップ 1 メニュー バーで、[テナント（Tenants）] > [すべてのテナント（ALL Tenants）] の順に選択します。 >

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーションウィンドウで、**[テナント（Tenant）]** ***[テナント名（tenant_name）]*** > **[サービス（Services）]** > **[L4-L7]** > **[サービスグラフテンプレート（Service Graph Templates）]** の順に選択します。

ステップ 4 ナビゲーション ウィンドウで、**Service Graph Templates** を右クリックして、**Create a L4-L7 Service Graph Template** を選択します。

Create L4-L7 Service Graph Template ダイアログボックスが表示されます。

ステップ 5 必要に応じて、1 つまたは複数のレイヤ 4 ～ レイヤ 7 サービスデバイスまたはコピーデバイスを作成します。

a) **Device Clusters** ペイン (**Create L4-L7 Service Graph Template** ダイアログボックス) でドロップダウン矢印をクリックして、**Create L4-L7 Devices** または **Create Copy Devices** を選択します。
対応するダイアログボックスが表示されます。

b) ダイアログボックスに従い、ダイアログボックスに表示される適切な値を入力して **Next** をクリックし、完了するまで続けます。

（注） ダイアログボックス内のフィールドの説明については、右上隅のヘルプ アイコンをクリックして、ヘルプ ファイルを表示してください。

c) 完了したら、**Finish** をクリックします。

Create L4-L7 Service Graph Template ダイアログボックスに戻ります。

ステップ 6 **Create L4-L7 Service Graph Template** ダイアログボックスに適切な値を入力します。

（注） ダイアログボックス内のフィールドの説明については、右上隅のヘルプ アイコンをクリックして、ヘルプ ファイルを表示してください。

ステップ 7 （任意） (既存のサービス グラフ テンプレートを複製場合のみ) 複製したサービス グラフ テンプレートからノードを削除する場合は、ノードを右クリックして、**Remove Node** を選択します。

ステップ 8 サービスノードを作成するには、レイヤ 4 ～ レイヤ 7 サービスデバイスを [**デバイスクラスタ（Device Clusters**）]セクションからドラッグし、コンシューマーエンドポイントグループとプロバイダーエンド

ポイントグループの間にドロップします。コピー ノードを作成するには、コピーデバイスをドラッグ アンド ドロップします。既存のサービス グラフ テンプレートを複製し、それにサービス グラフ テンプレートに使用するすべてのノードが含まれている場合には、この手順はオプションです。

複数のデバイスをドラッグ アンド ドロップして、複数のノードを作成することができます。サービス ノードの最大数は 3 ですが、他のデバイスはそれ以上ドラッグ アンド ドロップできます。

コピーデバイスをドロップした場所が、データ フローの中で、コピーデバイスがトラフィックをコピーする場所になります。

ステップ 9 1 つまたは複数のサービスノードを作成した場合は、各レイヤ 4 ～ レイヤ 7 サービスデバイスの **[デバイス名（*device_name*）情報]** セクションで、フィールドに入力します。フィールドは、デバイスのタイプによって異なります。

（注） フィールドの説明については、右上隅のヘルプ アイコンをクリックして、ヘルプ ファイルを表示してください。

ステップ 10 完了したら、**Submit** をクリックします。

ステップ 11 （任意） **Navigation** ウィンドウで、サービス グラフ テンプレートをクリックします。
作業ウィンドウには、そのサービス グラフ テンプレートのグラフィック トポロジが表示されます。

REST API を使用したサービス グラフ テンプレートの設定

次の REST API を使用してサービス グラフ テンプレートを設定できます。

```
<polUni>
  <fvTenant name="acme">
    <vnsAbsGraph name="G1">
      <vnsAbsTermNodeCon name="Input1">
        <vnsAbsTermConn name="C1">
            </vnsAbsTermConn>
      </vnsAbsTermNodeCon>
      <vnsAbsNode name="Node" funcType="GoTo">
        <vnsRsDefaultScopeToTerm
          tDn="uni/tn-acme/AbsGraph-G1/AbsTermNodeProv-Output1/outtmnl"/>
        <vnsAbsFuncConn name="inside">
          <vnsRsMConnAtt
            tDn="uni/infra/mDev-Insieme-Generic-1.0/mFunc-SubnetFunc/mConn-external"/>
        </vnsAbsFuncConn>
        <vnsAbsFuncConn name="outside">
          <vnsRsMConnAtt
            tDn="uni/infra/mDev-Insieme-Generic-1.0/mFunc-SubnetFunc/mConn-internal"/>
        </vnsAbsFuncConn>
        <vnsAbsDevCfg>
          <vnsAbsFolder key="oneFolder" name="f1">
            <vnsAbsParam key="oneParam" name="p1" value="v1"/>
          </vnsAbsFolder>
        </vnsAbsDevCfg>
        <vnsAbsFuncCfg>
          <vnsAbsFolder key="folder" name="folder1" devCtxLbl="C1">
            <vnsAbsParam key="param" name="param" value="value"/>
          </vnsAbsFolder>
          <vnsAbsFolder key="folder" name="folder2" devCtxLbl="C2">
```

```
            <vnsAbsParam key="param" name="param" value="value"/>
          </vnsAbsFolder>
        </vnsAbsFuncCfg>
        <vnsRsNodeToMFunc tDn="uni/infra/mDev-Insieme-Generic-1.0/mFunc-SubnetFunc"/>
      </vnsAbsNode>
      <vnsAbsTermNodeProv name="Output1">
        <vnsAbsTermConn name="C6">
            </vnsAbsTermConn>
      </vnsAbsTermNodeProv>
      <vnsAbsConnection name="CON1">
        <vnsRsAbsConnectionConns
          tDn="uni/tn-acme/AbsGraph-G1/AbsTermNodeCon-Input1/AbsTConn"/>
        <vnsRsAbsConnectionConns
tDn="uni/tn-acme/AbsGraph-G1/AbsNode-Node/AbsFConn-inside"/>
      </vnsAbsConnection>
      <vnsAbsConnection name="CON3">
        <vnsRsAbsConnectionConns
tDn="uni/tn-acme/AbsGraph-G1/AbsNode-Node/AbsFConn-outside"/>
        <vnsRsAbsConnectionConns
          tDn="uni/tn-acme/AbsGraph-G1/AbsTermNodeProv-Output1/AbsTConn"/>
      </vnsAbsConnection>
    </vnsAbsGraph>
  </fvTenant>
</polUni>
```

GUI を使用したエンドポイント グループへのサービス グラフ テンプレートの適用

次の手順で、エンドポイント グループへのサービス グラフ テンプレートの適用法を説明します。

始める前に

次を作成しておく必要があります。

- アプリケーション エンドポイント グループ
- サービス グラフ テンプレート

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ウィンドウで、**Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Service Graph Templates** > ***template_name*** を選択します。

ステップ 4 [Navigation] ウィンドウで、EPG を適用する ***template_name*** を右クリックし、**Apply L4-L7 Service Graph Template** を選択します。

Apply L4-L7 Service Graph Template To EPGs ダイアログボックスが表示されます。レイヤ 4 ～ レイヤ 7 サービス グラフ テンプレートをコンシューマ エンドポイント グループとプロバイダー エンドポイント グループに関連付けます。

ステップ 5 [Apply L4-L7 Service Graph Template To EPGS STEP 1] > [Contract] ダイアログボックスで、適切な値を入力して契約を設定します。

a) EPG 内契約を設定する場合は、[Configure an Intra-EPG Contract] チェックボックスをオンにして、[EPG / Network] ドロップダウンリストから EPG とネットワークの組み合わせを選択します。
b) 標準契約を設定する場合は、該当するドロップダウンリストでコンシューマ/プロバイダーEPGとネットワークの組み合わせを選択します。
c) [Contract] フィールドで適切なオプションボタンをクリックして、新しい契約を作成するか既存の契約を選択します。[Create A New Contract] を選択した場合、フィルタを設定するには、[No Filter (Allow All Traffic)] チェックボックスをオフにします。[+] をクリックしてフィルタ エントリを追加し、完了したら [Update] をクリックします。

（注） コピーサービスグラフの場合、L3Out EPG に適用される場合に限りコントラクトを複数回使用できます。内部 EPG には非共有コントラクトが必要です。

ステップ 6 [次へ] をクリックします。
[STEP 2] > [Graph] ダイアログが表示されます。

ステップ 7 [*device_name* Information] セクションで、赤色のボックスで示された必須フィールドを設定します。

（注） 優先グループ（契約なしのエンドポイント間通信）にコネクタを含めるには、[Service EPG Policy] ドロップダウンリストから設定済みポリシーを選択します。

ステップ 8 [次へ] をクリックします。
[STEP 3] > [device_name Information] ダイアログが表示されます。

ステップ 9 [Finish] をクリックします。
サービス グラフ テンプレートがアクティブになりました。

GUI を使用したエンドポイントセキュリティ グループへのサービスグラフテンプレートの適用

次の手順では、サービスグラフテンプレートをエンドポイントセキュリティ グループ (ESG) に適用する方法について説明します。

始める前に

次を作成しておく必要があります。

- ESG
- サービス グラフ テンプレート

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > **[すべてのテナント（ALL Tenants）]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーションウィンドウで、**[テナント（Tenant）]** ***[テナント名（tenant_name）]*** > **[サービス（Services）]** > **[L4-L7]** > **[サービスグラフテンプレート（Service Graph Templates）** > **テンプレート名（*template_name*）]** の順に選択します。

ステップ 4 [Navigation] ウィンドウで、EPG を適用する ***template_name*** を右クリックし、**Apply L4-L7 Service Graph Template** を選択します。

Apply L4-L7 Service Graph Template To EPGs ダイアログボックスが表示されます。レイヤ 4 ～ レイヤ 7 サービスグラフテンプレートを、コンシューマーおよびプロバイダーのエンドポイントセキュリティ グループに関連付けます。

ステップ 5 [Apply L4-L7 Service Graph Template To EPGS STEP 1] > [Contract] ダイアログボックスで、適切な値を入力して契約を設定します。

a) エンドポイントセキュリティ グループタイプとして、[**エンドポイントセキュリティ グループ（Endpoint Security Group**）] を選択します。

b) 標準コントラクトを構成する場合、適切なドロップダウンリストでコンシューマー/プロバイダー ESG とネットワークの組み合わせを選択します。

c) [Contract] フィールドで適切なオプション ボタンをクリックして、新しい契約を作成するか既存の契約を選択します。[Create A New Contract] を選択した場合、フィルタを設定するには、[No Filter (Allow All Traffic)] チェックボックスをオフにします。[+] をクリックしてフィルタ エントリを追加し、完了したら [Update] をクリックします。

ステップ 6 [次へ] をクリックします。

[STEP 2] > [Graph] ダイアログが表示されます。

ステップ 7 [*device_name* Information] セクションで、赤色のボックスで示された必須フィールドを設定します。

ステップ 8 [次へ] をクリックします。

[STEP 3] > [device_name Information] ダイアログが表示されます。

ステップ 9 [Finish] をクリックします。
サービス グラフ テンプレートがアクティブになりました。

NX-OS スタイルの CLI を使用したコントラクトによるサービスグラフテンプレートの適用

次の手順では、NX-OS スタイルの CLI を使用して、コントラクトでサービスグラフテンプレートを適用します。

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 テナントのコンフィギュレーション モードを開始します。

```
tenant tenant_name
```

例：

```
apic1(config)# tenant t1
```

ステップ 3 サービス グラフを追加します。

```
l4l7 graph graph_name [contract contract_name]
```

パラメータ	説明
グラフ	サービス グラフの名前。
contract	このサービス グラフ インスタンスに関連付けられたコントラクトの名前。サービス グラフ インスタンスを作成する場合にのみ、コントラクトを指定します。インスタンス化せずに（サービス グラフ テンプレートと同様に）簡単にサービス グラフを設定できます。

例：

```
apic1(config-tenant)# l4l7 graph G2 contract C2
```

ステップ 4 サービス グラフにノード（サービス）を追加します。

```
service node_name [device-cluster-tenant tenant_name] [device-cluster device_name] [mode
deployment_mode]
```

パラメータ	説明
service	追加するサービス ノードの名前。
device-cluster-tenant	デバイス クラスタのインポート元のテナント。これは、デバイスクラスタが、グラフが構成されているテナントと異なる場合にのみ指定します。
device-cluster	このサービス ノードに使用するデバイス クラスタの名前。
mode	導入モード。値は次のとおりです。 • ADC_ONE_ARM：ワンアームモードを指定します。 • ADC_TWO_ARM：ツーアームモードを指定します。 • FW_ROUTED：ルーテッド（GoTo）モードを指定します • FW_TRANS：トランスペアレント (GoThrough) モードを指定します。 • OTHERS：その他の展開モードを指定します。 モードを指定しないと、導入モードは使用されません。

例：

次に、ノード N1 をテナント t1 からデバイス クラスタ D4 に追加する例を示します。

```
apic1(config-graph)# service N1 device-cluster-tenant t1 device-cluster D4
```

次に、ノード N1 をテナント t1 からデバイス クラスタ D4 に追加し、ルーテッド導入モードを使用する例を示します。

```
apic1(config-graph)# service N1 device-cluster-tenant t1 device-cluster D4 mode FW_ROUTED
```

ステップ 5 コンシューマ コネクタを追加します。

```
connector connector_type [cluster-interface interface_type]
```

パラメータ	説明
コネクタ	サービス グラフ内のコネクタのタイプ。値は次のとおりです。 • provider • consumer
cluster-interface	デバイス クラスタ インターフェイスのタイプ。値は次のとおりです。 • provider • consumer テナント Common 内のサービス グラフ テンプレートの場合は、このパラメータを指定しないでください。

例：

```
apic1(config-service)# connector consumer cluster-interface consumer
```

ステップ 6 サービスインターフェイスがブリッジドメインにある場合は、次のサブステップを実行します。

a) ブリッジ ドメイン情報と、そのブリッジ ドメインが存在するテナントを指定し、コネクタにブリッジ ドメインを設定します。

```
bridge-domain tenant tenant_name name bridge_domain_name
```

パラメータ	説明
tenant	ブリッジ ドメインを所有するテナント。同じテナントまたはテナント Common からのみ、ブリッジを指定できます。たとえば、テナント t1 の場合、テナント t2 からのブリッジ ドメインは指定できません。
name	ブリッジ ドメインの名前。

例：

```
apic1(config-connector)# bridge-domain tenant t1 name bd2
```

b) コネクタの Direct Server Return（DSR）仮想 IP アドレス（VIP）を設定します。

```
dsr-vip ip_address
```

DSR VIP を指定した場合、Application Policy Infrastructure Controller（APIC）は VIP を取得しません。

パラメータ	説明
dsr-vip	コネクタの DSR の仮想 IP アドレス。

例：

```
apic1(config-connector)# dsr-vip 192.168.10.100
```

ステップ 7 サービスインターフェイスが L3Out にある場合は、次のサブステップを実行します。

a) テナントをコネクタに関連付け、コネクタ コンフィギュレーション モードを終了します。

```
l4l7-peer tenant tenant_name out L3OutExternal epg epg_name
  redistribute redistribute_property
exit
```

パラメータ	説明
tenant	コネクタに関連付けるテナントの名前。
out	レイヤ 3 Outside の名前。
epg	エンドポイント グループの名前。
redistribute	再配布プロトコルのプロパティ。

例：

```
apic1(config-connector)# l4l7-peer tenant t1 out L3OutExternal epg L3ExtNet
  redistribute connected,ospf
apic1(config-connector)# exit
```

b) プロバイダーに対して手順 5 と 7a を繰り返します。

例：

```
apic1(config-service)# connector provider cluster-interface provider
apic1(config-connector)# l4l7-peer tenant t1 out L3OutInternal epg L3IntNet
  redistribute connected,ospf
apic1(config-connector)# exit
```

c) （任意）ルータを追加し、ノード コンフィギュレーション モードを終了します。

```
rtr-cfg router_ID
exit
```

パラメータ	説明
rtr-cfg	ルータの ID。

テナント Common でサービス グラフ テンプレートを作成する場合は、この手順をスキップします。

例：

```
apic1(config-service)# rtr-cfg router-id1
apic1(config-service)# exit
```

ステップ 8 コンシューマとプロバイダーに対する接続を設定して、サービス グラフ コンフィギュレーション モードを終了します。

```
connection connection_name {terminal terminal_type service node_name connector connector_type} |
  {intra_service service1 node_name connector1 connector_type service2 node_name connector2
connector_type}
exit
```

パラメータ	説明
connection	接続の名前。
terminal	サービス ノードを端末に接続します。端末のタイプを指定します。値は次のとおりです。 • provider • consumer
service service1 service2	追加するサービスノード名です。service は terminal でのみ使用します。service1 と service2 は、intra_service でのみ使用します。
コネクタ connector1 connector2	コネクタのタイプ。値は次のとおりです。 • provider • consumer connector は terminal でのみ使用し、connector1 と connector2 は intra_service でのみ使用します。
intra_service	別のノードにサービス ノードを接続します。

例：

次に、単一ノード グラフの接続を設定する例を示します。

```
apic1(config-graph)# connection CON1 terminal consumer service N1 connector consumer
apic1(config-graph)# connection CON2 terminal provider service N2 connector provider
apic1(config-graph)# exit
```

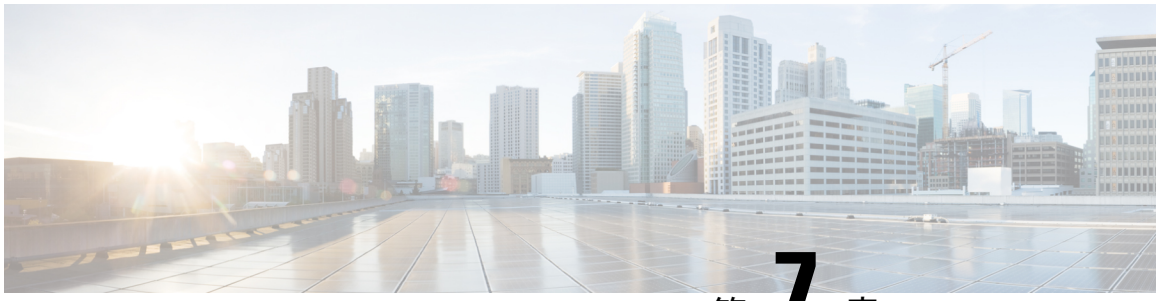
次に、2 ノード グラフの接続を設定する例を示します。

```
apic1(config-graph)# connection CON1 terminal consumer service N1 connector consumer
apic1(config-graph)# connection CON2 intra_service service1 N1 connector1 provider service2 N2
connector2 consumer
apic1(config-graph)# connection CON3 terminal provider service N2 connector provider
apic1(config-graph)# exit
```

ステップ 9 コンフィギュレーション モードを終了します。

例：

```
apic1(config-tenant)# exit
apic1(config)# exit
```



第 7 章

ルート ピアリングの設定

ルート ピアリングについて

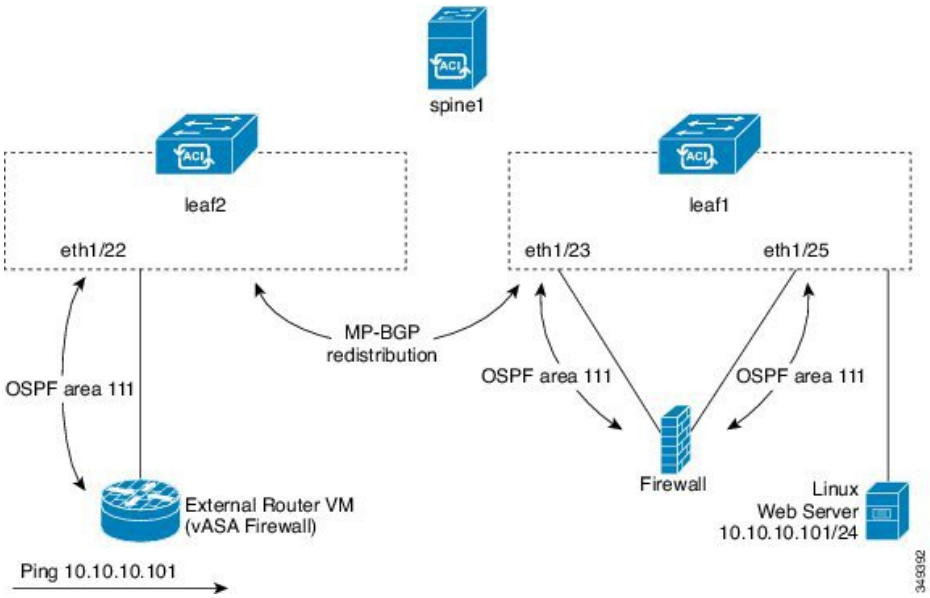
ルート ピアリングは、トランジットの使用例としてより一般的なCisco Application Centric Infrastructure（ACI）ファブリックの特殊ケースで、ルート ピアリングによってACI ファブリックが Open Shortest Path First（OSPF）プロトコルまたは Border Gateway Protocol（BGP）プロトコルのトランジット ドメインとして機能できるようになります。ルート ピアリングの一般的な使用例はルート ヘルス インジェクションであり、サーバのロード バランシング仮想 IP が OSPF または内部 BGP（iBGP）を使用して、ACI ファブリック外にあるクライアントにアドバタイズされます。デバイスが接続されている ACI リーフ スイッチとピアリングしたり、ルートを交換したりできるように、ルート ピアリングを使用して OSPF ピアリングや BGP ピアリングをサーバ デバイス上に設定したりすることができます。

次のプロトコルは、ルート ピアリングをサポートしています。

- OSPF
- OSPFv3
- iBGPv4
- iBGPv6
- スタティック ルート

次の図に、ルート ピアリングの一般的な導入方法を示します。

図 *3:* 一般的なルート ピアリング トポロジ



図に示すように、ルート ピアリングを設定してサービス グラフを導入することによって、Web サーバのパブリック IP アドレスがファイアウォールを介して外部ルータにアドバタイズされます。ファイアウォールの各レッグに OSPF ルーティング ポリシーを導入する必要があります。通常、これを行うには、`l3extOut` ポリシーを導入します。これにより、Web サーバの到達可能性情報がファイアウォールを介してボーダー リーフ スイッチと外部ルータに OSPF でアドバタイズされるようになります。

ファブリック内のリーフ スイッチ間のルート配布は Multi-Protocol Border Gateway Protocol（MP-BGP）により内部的に実行されます。

ルート ピアリング トポロジのより詳しい例については、ルート ピアリングのエンドツーエンド フロー （70 ページ） を参照してください。

`l3extOut` ポリシーの設定の詳細については、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

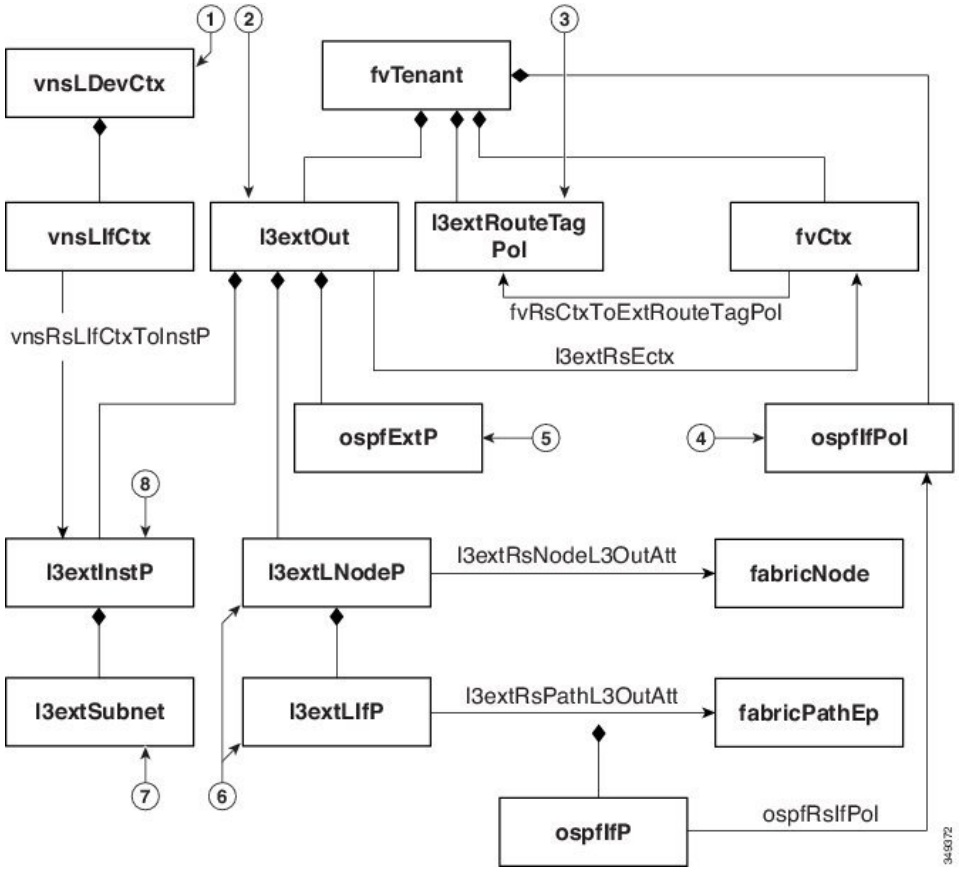
（注） ポイントツーポイントの非ブロードキャスト モードは、Adaptive Security Appliance （ASA）ではサポートされていません。Application Policy Infrastructure Controller（APIC）からポイントツーポイントの非ブロードキャスト モード設定を削除する必要があります（存在する場合）。

Open Shortest Path First ポリシー

ルート ピアリングを設定するには、最初に 1 つ以上の `l3extOut` ポリシーを作成し、サービス デバイスを接続するファブリック リーフ ノードに導入します。これらの `l3extOut` ポリシー

で、ファブリック リーフで有効にする必要がある Open Shortest Path First（OSPF）のパラメータを指定します。これらのポリシーは外部通信に使用される `l3extOut` ポリシーとよく似ています。次の図に、ルート ピアリング オブジェクトの関係を示します。

図 *4 : OSPF* ルート ピアリング オブジェクトの関係



1. `vnsLDevCtx`：デバイス選択ポリシー。
2. `l3extOut`：1 つのエリアのすべての OSPF ポリシーが含まれます。
3. `l3extRouteTagPol`：ルート ピアリングで必要な各コンテキストには OSPF ループを回避するための一意のルート タグが必要です。1 つのレッグから取得される OSPF ルートは、ルート タグが異なっていない限り、他のレッグでは取得されません。
4. `ospfIfPol`：インターフェイスごとの OSPF ポリシー。
5. `ospfExtP`：エリア ポリシーごとの OSPF。
6. `l3extLNodeP/l3extLIfP`：この `l3extOut` を導入するノードまたはポート。
7. `l3extSubnet`：ファブリックに対してエクスポートまたはインポートするサブネット。
8. `l3extInstP`：プレフィックス ベースの EPG。

次に、l3extOut の 2 つの 例（OspfExternal と OspfInternal）を示します。これらのポリシーは、図 3 : 一般的なルート ピアリング トポロジ （62 ページ） のファイアウォール デバイスの外部レッグと内部レッグに導入されます。l3extOut ポリシーは、ファブリック リーフがトラフィックを分類する方法と、サービスデバイスに対してルートをインポートまたはエクスポートする方法も制御する 1 つ以上のプレフィックス ベースの EPG（l3extInstP）を指定します。l3extOut ポリシーには、そのポリシーの下で指定される OSPF のエリアごとのポリシー（ospfExtP）と 1 つ以上の OSPF インターフェイス ポリシー（ospfIfPol）が含まれています。

次に、値「100」で設定される area-Id を持つ OSPF エリアの例を示します。

```
<ospfExtP areaId="100" areaType="regular" areaCtrl="redistribute"/>
```

エリア タイプは「regular」に設定し、エリア制御属性は「redistribute」に設定します。

OSPF インターフェイス ポリシーで、1 つ以上の OSPF インターフェイス タイマーを指定します。

```
<ospfIfPol name="ospfIfPol" ctrl="mtu-ignore" nwT="bcast" xmitDelay="1" helloIntvl="10"
  deadIntvl="40" status="created,modified"/>
```

デフォルト タイマーが正常であれば、このポリシーを指定する必要はありません。このポリシーでは、特定のタイマーをデフォルト値から変更し、次の関係を使用することによって、1 つ以上のインターフェイスに関連付けることができます。

```
<l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]" ifInstT="ext-svi"
  encap="vlan-3844" addr="30.30.30.100/28" mtu="1500"/>
```

l3extRsPathL3OutAtt の関係の属性は次のとおりです。

- ifInstT：論理インターフェイス タイプ。通常は「ext-svi」。
- encap：このインターフェイスを作成するときは VLAN カプセル化を指定する必要があります。カプセル化はサービス デバイスにプッシュされます。
- addr：この l3extOut を導入するファブリック リーフで作成された SVI インターフェイスの IP アドレス。

次のポリシーで、l3extOut ポリシーをどこに導入するかを制御します。

```
<l3extNodeP name="bLeaf-101">
  <l3extRsNodeL30utAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.11"/>
  <l3extLIfP name="portIf">
    <l3extRsPathL30utAtt tDn="topology/pod-1/paths-101/pathep-teth1/251"
      ifInstT="ext-svi" encap="vlan-3844" addr="30.30.30.100/28" mtu="1500"/>
    <ospfIfP authKey="tecom" authType="md5" authKeyId='1'>
      <ospfRslfPol tnOspfIfPolName="ospfIfPol"/>
    </ospflfP>
  </l3extLIfP>
</l3extLNodeP>
```

l3extOut ポリシーは、サービス デバイスが接続されているリーフ ポートと同じものに導入する必要があります。

scope=import-security 属性は次を実行します。

- データ プレーン内のトラフィックのフローを制御する
- このルートをアドバタイズする外部デバイスへのディレクティブとして機能する

（注） ルート ピアリングを正しく動作させるには、l3extRsPathL3OutAtt の関係が、デバイスを表す vnsCDev の下の RsCIfPathAtt の関係と同じファブリックの宛先を指している必要があります。

OspfExternal ポリシー

OspfInternal ポリシー

仮想サービス

```
<polUni>
  <fvTenant name="common">
    <fvCtx name="commonctx">
      <fvRsCtxToExtRouteTagPol tnL3extRouteTagPolName="myTagPol"/>
    </fvCtx>
    <l3extRouteTagPol tag="212" name="myTagPol"/>
    <l3extOut name="OspfExternal" status="created,modified">
      <l3extLNodeP name="bLeaf-101">
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.8/28"/>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"
            ifInstT="ext-svi" encap="vlan-3843" addr="40.40.40.100/28" mtu="1500"/>
          <ospfIfP authKey="tecom" authType="md5" authKeyId='1'>
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
          </ospfIfP>
        </l3extLIfP>
      </l3extLNodeP>
      <ospfExtP areaId="100" areaType="regular" areaCtrl="redistribute"/>
      <l3extInstP name="ExtInstP">
        <l3extSubnet ip="40.40.40.100/28" scope="import-security"/>
        <l3extSubnet ip="10.10.10.0/24" scope="import-security"/>
      </l3extInstP>
      <l3extRsEctx tnFvCtxName="commonctx"/>
    </l3extOut>
   <ospfIfPol name="ospfIfPol" ctrl="mtu-ignore" nwT="bcast" xmitDelay="1" helloIntvl="10"

      deadIntvl="40" status="created,modified"/>
  </fvTenant>
</polUni>
```

```
<polUni>
  <fvTenant name="tenant1">
    <l3extRouteTagPol tag="213" name="myTagPol"/>
    <fvCtx name="tenant1ctx1">
      <fvRsCtxToExtRouteTagPol tnL3extRouteTagPolName="myTagPol"/>
    </fvCtx>
    <l3extOut name="OspfInternal" status="created,modified">
      <l3extLNodeP name="bLeaf-101">
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.11"/>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]"
            ifInstT="ext-svi" encap="vlan-3844" addr="30.30.30.100/28" mtu="1500"/>
          <ospfIfP authKey="tecom" authType="md5" authKeyId='1'>
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
          </ospfIfP>
        </l3extLIfP>
      </l3extLNodeP>
      <ospfExtP areaId="100" areaType="regular" areaCtrl="redistribute"/>
```

```
      <l3extInstP name="IntInstP">
        <l3extSubnet ip="30.30.30.100/28" scope="import-security"/>
        <l3extSubnet ip="20.20.20.0/24" scope="import-security"/>
      </l3extInstP>
      <l3extRsEctx tnFvCtxName="tenant1ctx1"/>
    </l3extOut>
   <ospfIfPol name="ospfIfPol" ctrl="mtu-ignore" nwT="bcast" xmitDelay="1" helloIntvl="10"

      deadIntvl="40" status="created,modified"/>
  </fvTenant>
</polUni>
```

`OspfExternalInstP` ポリシーは、プレフィクスの 40.40.40.100/28 と 10.10.10.0/24 をプレフィクス ベースのエンドポイントのアソシエーションに使用する必要があることを指定します。また、このポリシーは、プレフィックスの 20.20.20.0/24 をサービス デバイスにエクスポートするようにファブリックに指示します。

```
      <l3extInstP name="OspfExternalInstP">
        <l3extSubnet ip="40.40.40.100/28" scope="import-security"/>
        <l3extSubnet ip="10.10.10.0/24" scope="import-security"/>
        <l3extSubnet ip="20.20.20.0/24" scope="export"/>
      </l3extInstP>
```

`bleaf-101` ポリシーは、この `l3extOut` ポリシーを導入する場所を制御します。

```
      <l3extLNodeP name="bLeaf-101">
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.8/28"/>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"
            ifInstT="ext-svi" encap="vlan-3843" addr="40.40.40.100/28" mtu="1500"/>
          <!-- <ospfIfP authKey="tecom" authType="md5" authKeyId='1'> -->
          <ospfIfP>
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
          </ospfIfP>
        </l3extLIfP>
      </l3extLNodeP>
```

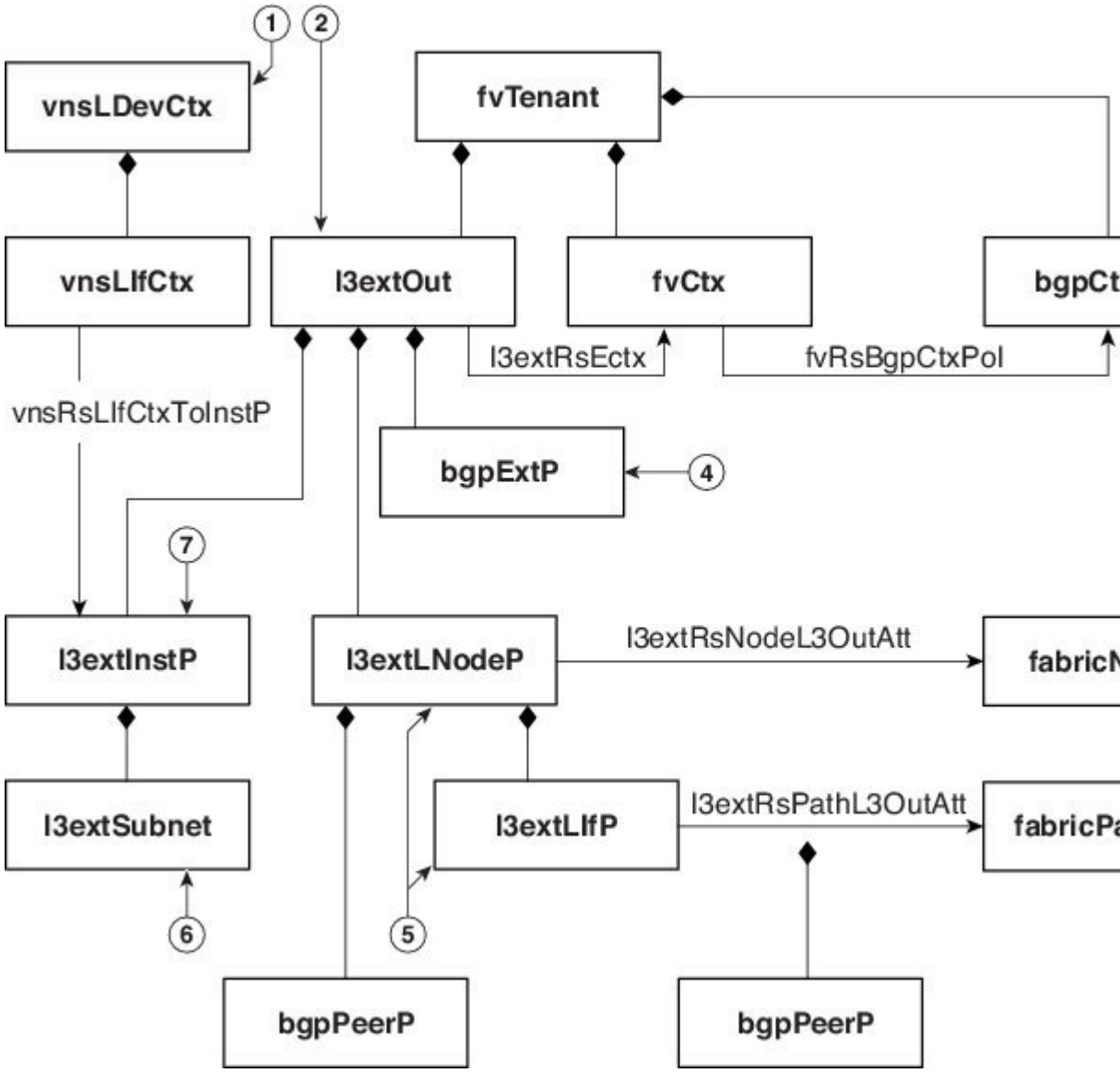
仮想サービスはルート ピアリングとともに導入できますが、`vnsCIf` オブジェクトでの `l3extRsPathL3OutAtt` 検証は実行されません。このデータ パスは、`l3extOut` オブジェクトが仮想サービス データが接続されている正しいリーフに導入されている場合にのみ動作します。

Border Gateway Protocol ポリシー

内部 Border Gateway Protocol（iBGP）を使用してデバイスの外部インターフェイスにルート ピアリングを設定し、内部インターフェイスに静的ルートを設定できます。追加設定なしにデバイス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に iBGP を設定することはできません。これは、インターフェイスが異なる自律システムに存在する必要があり、相互自律システム再配布ポリシーをプッシュ ダウンしないためです。

次の図に、ルート ピアリング オブジェクトの関係を示します。

図 *5 : iBGP* ルート ピアリング オブジェクトの関係



1. `vnsLDevCtx`：デバイス選択ポリシー。
2. `l3extOut`：単一の自律システム用のすべての BGP ポリシーが含まれます。
3. `bgpCtxPol`：コンテキスト単位の BGP タイマー。
4. `bgpExtP`：ASN ポリシー単位の BGP。
5. `l3extLIfP/l3extLNodeP`：これらのエンドポイント グループ（EPG）を導入するノードまたはポートを制御します。
6. `l3extSubnet`：ファブリックからのエクスポートするサブネットとファブリックにインポートするサブネット。

7. `l3extInstP`：プレフィックス ベースの EPG。

次のポリシーは、外部インターフェイスに iBGPv4/v6 を設定します。

```
<polUni>
  <fvTenant name="common">
    <fvCtx name="commonctx">
      <fvRsBgpCtxPol tnBgpCtxPolName="timer-3-9"/>
      <fvRsCtxToExtRouteTagPol tnL3extRouteTagPolName="myTagPol"/>
    </fvCtx>
    <l3extRouteTagPol tag="212" name="myTagPol"/>
   <bgpCtxPol grCtrl="helper" holdIntvl="9" kaIntvl="3" name="timer-3-9" staleIntvl="30"/>

    <l3extOut name="BgpExternal" status="created,modified">
      <l3extLNodeP name="bLeaf-101">
        <!-- <bgpPeerP addr="40.40.40.102/32 "ctrl="send-com"/> -->
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.8/28>"
          <l3extLoopBackIfP addr="50.50.50.100/32"/>
        </l3extRsNodeL3OutAtt>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"
            ifInstT="ext-svi" encap="vlan-3843" addr="40.40.40.100/28 "mtu="1500">
            <bgpPeerP addr="40.40.40.102/32 "ctrl="send-com"/>
          </l3extRsPathL3OutAtt>
        </l3extLIfP>
      </l3extLNodeP>
      <bgpExtP/>
      <l3extInstP name="ExtInstP">
        <l3extSubnet ip="40.40.40.100/28 "scope="import-security"/>
        <l3extSubnet ip="10.10.10.0/24 "scope="import-security"/>
        <l3extSubnet ip="20.20.20.0/24 "scope="export-rtctrl"/>
      </l3extInstP>
      <l3extRsEctx tnFvCtxName="commonctx"/>
    </l3extOut>
  </fvTenant>
</polUni>
```

iBGP ピアは、物理インターフェイス レベルまたはループバック レベルで設定できます。次に、物理インターフェイス レベルで設定された iBGP ピアの例を示します。

```
<l3extLIfP name="portIf">
    <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"
      ifInstT="ext-svi" encap="vlan-3843" addr="40.40.40.100/28 "mtu="1500">
        <bgpPeerP addr="40.40.40.102/32 "ctrl="send-com"/>
    </l3extRsPathL3OutAtt>
</l3extLIfP>
```

この場合、ファブリック上で実行する iBGP プロセスはスイッチ仮想インターフェイス（SVI）IP アドレス 40.40.40.100/28 を使用して、ネイバーとピアリングします。ネイバーは、IP アドレス 40.40.40.102/32 のサービス デバイスです。

次に、iBGP ピアの定義が論理ノード レベル（`l3extLNodeP` の下）に移動され、ループバック インターフェイスが作成されている例を示します。

```
      <l3extLNodeP name="bLeaf-101">
        <bgpPeerP addr="40.40.40.102/32 "ctrl="send-com"/>
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.8/28>"
          <l3extLoopBackIfP addr="50.50.50.100/32"/>
        </l3extRsNodeL3OutAtt>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"
            ifInstT="ext-svi" encap="vlan-3843" addr="40.40.40.100/28 "mtu="1500">
```

```
          </l3extRsPathL3OutAtt>
        </l3extLIfP>
      </l3extLNodeP>
```

この例では、iBGPプロセスはループバックアドレスを使用してネイバーとピアリングします。ループバックが設定されていない場合は、ファブリックは rtrId で指定された IP アドレスを使用してネイバーとピアリングします。

次に、デバイスの内部インターフェイス用にファブリック上で静的ルートを設定する例を示します。

```
<polUni>
  <fvTenant name="tenant11">
    <l3extOut name="StaticInternal" status="created,modified">
      <l3extLNodeP name="bLeaf-201">
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.11>"
          <ipRouteP ip="20.20.20.0/24>"
            <ipNexthopP nhAddr="30.30.30.102/32"/>
          </ipRouteP>
        </l3extRsNodeL3OutAtt>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]"
            ifInstT="ext-svi" encap="vlan-3844" addr="30.30.30.100/28 "mtu="1500"/>
        </l3extLIfP>
      </l3extLNodeP>
      <l3extInstP name="IntInstP">
        <l3extSubnet ip="20.20.20.0/24 "scope="import-security"/>
      </l3extInstP>
      <l3extRsEctx tnFvCtxName="tenant1ctx1"/>
    </l3extOut>
  </fvTenant>
</polUni>
```

クラスタ用の L3extOut ポリシーの選択

特定の l3extOut ポリシーを、選択ポリシー vnsLIfCtx を使用して論理デバイスのインターフェイスに関連付けることができます。次に、これを実現する例を示します。

```
<vnsLDevCtx ctrctNameOrLbl="webCtrct1" graphNameOrLbl="WebGraph" nodeNameOrLbl="FW">
    <vnsRsLDevCtxToLDev tDn="uni/tn-tenant1/lDevVip-Firewall"/>
    <vnsLIfCtx connNameOrLbl="internal">
        <vnsRsLIfCtxToInstP tDn="uni/tn-tenant1/out-OspfInternal/instP-IntInstP"
          status="created,modified"/>
        <vnsRsLIfCtxToLIf tDn="uni/tn-tenant1/lDevVip-Firewall/lIf-internal"/>
    </vnsLIfCtx>
    <vnsLIfCtx connNameOrLbl="external">
        <vnsRsLIfCtxToInstP tDn="uni/tn-common/out-OspfExternal/instP-ExtInstP"
          status="created,modified"/>
        <vnsRsLIfCtxToLIf tDn="uni/tn-tenant1/lDevVip-Firewall/lIf-external"/>
    </vnsLIfCtx>
</vnsLDevCtx>
```

vnsRsLIfCtxToInstP の関係を使用して、サービスデバイスのこのレッグと関連付ける特定のプレフィックスベースの EPG（l3extInstP）を選択します。この関係に、redistribute プロトコル再配布プロパティを指定できます。redistribute プロパティのデフォルト値は「ospf,bgp」です。redistribute をデフォルト値のままにすると、各レッグで設定されているルーティングプロトコルが Application Policy Infrastructure Controller（APIC）によって自動検出され、適切な

再配布設定にプッシュされます。自動設定は、常にInterior Gateway Protocol（OSPF）から外部ゲートウェイ プロトコル（BGP）に再配布します。

静的または接続済みといった特定の再配布設定を使用する場合は、それらの設定をこの関係に追加します。たとえば、`redistribute="ospf,bgp,static"` は、自動検出設定と `redistribute-static` をサービス デバイスにプッシュします。

このプロパティをデフォルト値を含まない特定の値（たとえば、`redistribute="ospf,static,connected"`）に設定すると、それらの設定がそのままサービス デバイスにプッシュされます。これは、APICによって選択されたデフォルト値を上書きする場合に役に立ちます。

（注） この関係は `l3extOut` 自体でなく、EPG（`l3extInstP`）を指します。これは、`l3extOut` ポリシーにはこのようなEPGが複数存在する可能性があり、別のデバイス選択ポリシーがそれらのEPGを指していることがあるためです。これにより、さまざまなサービス グラフによってインポートまたはエクスポートされるプレフィックスを細かく制御できます。

関連付けられた具象デバイスには `vnsRsCIfPathAtt` オブジェクトが必要です。このオブジェクトでは、デバイスを同じファブリック リーフに導入します（下記参照）。

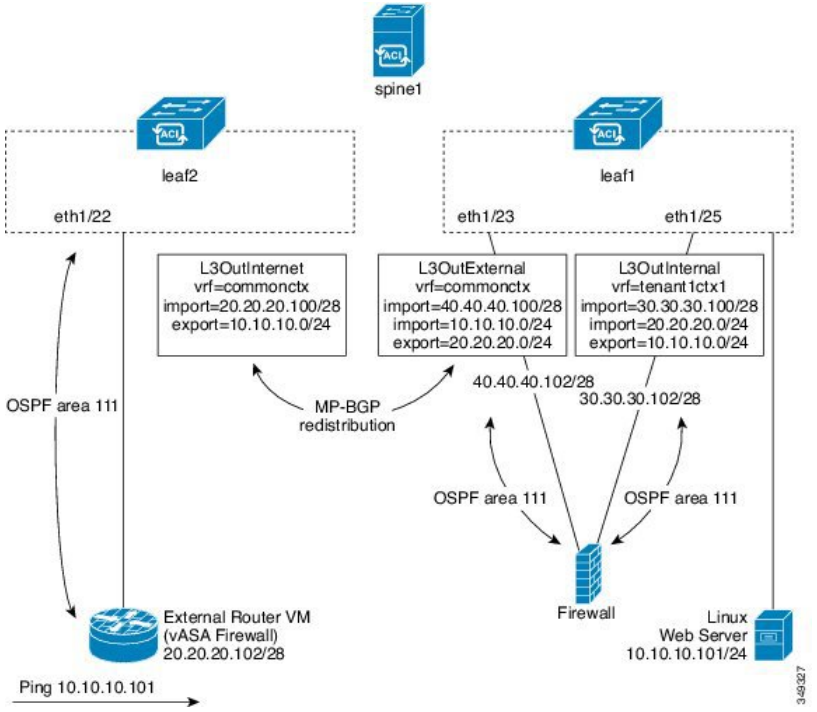
```
<vnsCDev name="ASA">
    <vnsCIf name="Gig0/0">
      <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"/>
    </vnsCIf>
    <vnsCIf name="Gig0/1">
      <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]"/>
    </vnsCIf>
</vnsCDev>
```

（注） ルート ピアリングを設定した場合は、`vnsLIfCtx` セレクタにブリッジ ドメインを設定する必要がありません。ブリッジ ドメインの関係（`vnsRsLIfCtxToBD`）と `l3extInstP` の関係（`vnsRsLIfCtxToInstP`）の両方を設定しようとすると、エラーになります。

ルート ピアリングのエンドツーエンド フロー

次の図に、ルート ピアリングがエンドツーエンドでどのように動作するかを示します。

図 *6 :* ルート ピアリングのエンドツーエンド フロー



この図には、ルート ピアリングを使用して Linux Web サーバの IP アドレスが外部ルータにアドバタイズされる、単一スパイン スイッチ トポロジである 2 台のリーフ スイッチの例が示されています。Linux Web サーバは IP アドレス 10.10.10.101 にあり、`leaf1` に接続する ESX サーバ上でホストされています。通常のブリッジドメインベースのエンドポイント グループ（EPG）が導入されており、Web サーバから発信されるトラフィックを表しています。

2 アームのルーティング可能なファイアウォールから構成され、両方のアームを `leaf1` に接続したサービス グラフを導入します。ファイアウォール デバイスでは、Virtual Routing and Forwarding (VRF) 分割が行われています。つまり、ファイアウォールの各アームが異なる VRF のリーフ（コンテキスト）に接続されています。VRF 分割は、トラフィックがリーフ スイッチによって短絡されるのではなく、サービスデバイスを通じて確実にルーティングされるようにするために必要です。外部トラフィックは `leaf2` に導入されている `l3extOut`（`L3OutInternet`）で表されます。このシナリオでは、`leaf2` をファブリックの境界リーフ スイッチと見なすことができます。`L3OutInternet` と Web サーバ EPG 間にコントラクトを導入できます。このコントラクトは、ファイアウォール デバイスを含むサービス グラフに関連付けられます。

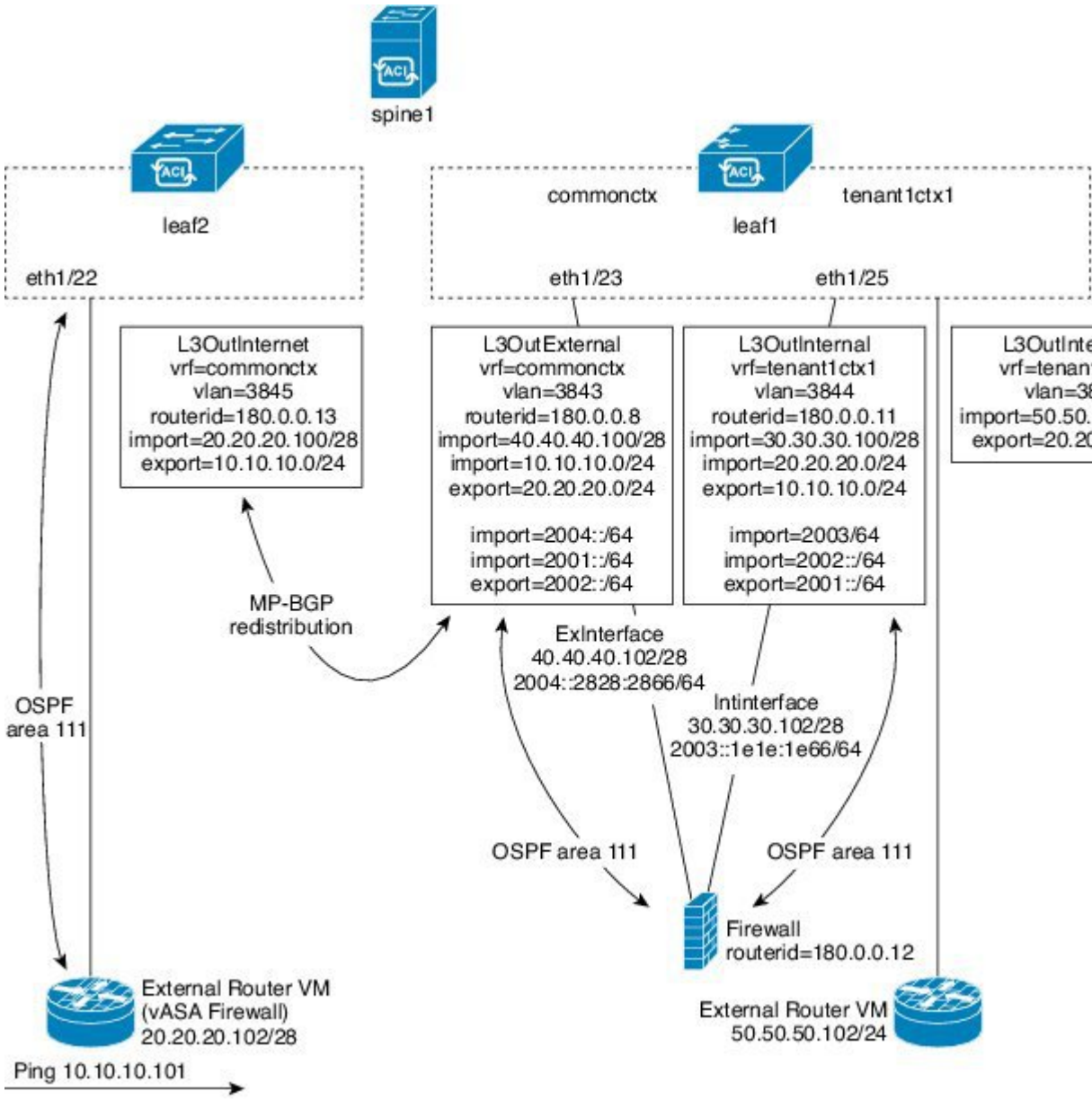
Web サーバ ルートを外部にパブリッシュするには、2 つの `l3extOut`（`L3OutExternal` と `L3OutInternal`）を、サービス デバイスを接続するリーフ スイッチ ポートに展開します。その結果、Open Shortest Path First (OSPF) ピアリング セッションが、両方のコンテキスト（`commonctx` と `tenant1ctx1`）のリーフ スイッチとファイアウォール間で確立されます。これらの `l3extOut` の export 属性が境界リーフ スイッチへのルーティング情報のアドバタイズ方法を制御します。ルートはマルチプロトコル Border Gateway Protocol (MP-BGP) の再配布を使用して、ファブリック リーフ スイッチの間で内部的に交換されます。

最終的に、別の OSPF セッションを使用して Web サーバ ルートが外部ルータ（IP アドレス 20.20.20.102）にアドバタイズされます。これにより、静的ルートを手動で設定することなく、外部ルータから Web サーバを ping できるようになります。

Cisco Application Centric Infrastructure トランジット ルーティング ドメインとして機能するファブリック

Cisco Application Centric Infrastructure（ACI）ファブリックをトランジット ルーティング ドメインとして導入できるので、ACI の受渡しポイント（POD）が他の POD 間のトランジット ルーティング ドメインとして機能している場合に便利です。次の図に、2 つの境界リーフ スイッチへの 2 つの 外部 `l3extOut`（`L3OutInternet` と `L3OutInternet2`）の展開を示します。これらの `3extOut` 間には関連付けられているコントラクトがあり、そのコントラクトはファイアウォール サービス デバイスを含む単一ノードのサービス グラフに適用されています。

図 *7*: *ACI* トランジット ルーティング ドメインとして機能するファブリック



2 つの追加 `l3extOut` は、ファイアウォール デバイスの外部レッグと内部レッグに導入され、それらの間に Open Shortest Path First（OSPF）ピアリング セッションを確立します。インポート セキュリティ制御（`import-security` 属性）を適切に設定することで、境界リーフ スイッチへの ACI ファブリックの通過を許可するルートを制御できます。

GUI を使用したルート ピアリングの設定

ルート ピアリングを設定するには、次のタスクを実行する必要があります。

1. デバイスとCisco Application Centric Infrastructure（ACI）ファブリック間のカプセル化VLANに使用するスタティック VLAN プールを作成します。

   GUI を使用したスタティック VLAN プールの作成 （74 ページ）を参照してください。

2. デバイスの場所（リーフ ノード/パス）と VLAN プールを結びつける外部ルーテッド ドメインを作成します。

   GUI を使用した外部ルーテッド ドメインの作成 （74 ページ）を参照してください。

3. ルート ピアリングで ACI ファブリックのルーティング設定を指定するために使用する外部ルーテッド ネットワークを作成します。

   GUI を使用した外部ルーテッド ネットワークの作成 （75 ページ）を参照してください。

4. デバイスで使用するルータ ID を指定する新しいルータ設定を作成します。

   GUI を使用したルータ設定の作成 （78 ページ）を参照してください。

5. サービス グラフのアソシエーションを作成します。これには、外部ルーテッドネットワーク ポリシーおよびルータ設定とデバイス選択ポリシーの関連付けが含まれます。

   「GUI を使用したサービス グラフ アソシエーションの作成 （78 ページ）」を参照してください。

GUI を使用したスタティック VLAN プールの作成

外部ルーテッド ネットワーク設定を作成する前に、デバイスとファブリック間のカプセル化 VLAN に使用するスタティック VLAN プールを作成する必要があります。

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 2 [Navigation] ペインで、**[Pools]** > **[VLAN]** の順に選択します。

ステップ 3 [Work] ペインで、**[Actions]** > **[Create VLAN Pool]** の順に選択します。

ステップ 4 **[Create VLAN Pool]** ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) **[Allocation Mode]** オプション ボタンでは **[Static Allocation]** を選択します。

b) **[Encap Blocks]** セクションでは、**[+]** をクリックします。

ステップ 5 **[Create Ranges]** ダイアログボックスで、一意の VLAN 範囲を入力し、**[OK]** をクリックします。

ステップ 6 **[Create VLAN Pool]** ダイアログボックスで、**[Submit]** をクリックします。

GUI を使用した外部ルーテッド ドメインの作成

デバイスの場所 (リーフ ノード/パス) とルート ピアリング用に作成するスタティック VLAN プールを結びつける外部ルーテッド ドメインを作成する必要があります。

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）] > [アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 ナビゲーションウィンドウで、[**スイッチポリシー（Switch Policies**）] を右クリックして、[**インターフェイス、PC、VPC の設定（Configure Interface, PC, and VPC**）]を選択します。

ステップ 3 **[Configure Interface, PC, and VPC]** ダイアログボックスで、Application Policy Infrastructure Controller (APIC) に接続されるスイッチ ポートを設定し、次の操作を実行します。

a) スイッチ図の横にある大きい **[+]** アイコンをクリックし、新しいプロファイルを作成して VLAN を APIC 用に設定します。

b) **[Switches]** フィールドのドロップダウン リストから、APIC を接続するスイッチのチェックボックスをオンにします

c) **[Switch Profile Name]** フィールドに、プロファイルの名前を入力します。

d) **[+]** アイコンをクリックして、ポートを設定します。

e) **[Interface Type]** 領域で、**[Individual]** オプション ボタンが選択されていることを確認します。

f) **[Interfaces]** フィールドで、APIC が接続されるポートを入力します。

g) **[Interface Selector Name]** フィールドに、ポート プロファイルの名前を入力します。

h) **[Interface Policy Group]** フィールドで、**[Create One]** オプション ボタンをクリックします。

i) **[Attached Device Type]** ドロップダウン リストで、**[External Routed Devices]** を選択します。

j) **[Domain]** オプション ボタンでは、**[Create One]** オプション ボタンをクリックします。

k) **[Domain Name]** フィールドに、ドメイン名を入力します

l) VLAN プールを前に作成していた場合は、**[VLAN]** オプション ボタンとして、**[Choose One]** オプション ボタンをクリックします。その他の場合は、**[Create One]** オプション ボタンをクリックします。

既存の VLAN プールを選択する場合は、**[VLAN Pool]** ドロップダウン リストで、VLAN プールを選択します。

VLAN プールを作成する場合は、**[VLAN Range]** フィールドに VLAN 範囲を入力します。

m) **[Save]** をクリックし、**[Save]** をもう一度クリックします。

n) [送信（Submit）] をクリックします。

GUI を使用した外部ルーテッド ネットワークの作成

外部ルーテッド ネットワークは、ルート ピアリングでCisco Application Centric Infrastructure（ACI）ファブリックのルーティング設定を指定します。

ステップ 1 メニュー バーで、**[Tenants] > [All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ペインで、***[tenant_name]*** > **[Networking]** > **[External Routed Networks]** を選択します。

ステップ 4 [Work] ペインで、**[Actions] > [Create Routed Outside]** を選択します。

ステップ 5 [Create Routed Outside] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) ダイナミック ルーティングの場合は、[BGP] チェックボックスまたは [OSPF] チェックボックスをオンにします。

Open Shortest Path Firs （OSPF ）の場合は、追加の OSPF 固有のフィールドに入力します。

b) [Private Network] ドロップダウン リストで、デバイスがルートを交換するプライベート ネットワークを選択します。

c) [External Routed Domain] ドロップダウン リストで、ルート ピアリング用に作成した外部ルーテッド ドメインを選択します。

d) [Nodes and Interfaces Protocol Profiles] セクションで、[+] をクリックします。

ステップ 6 [Create Node Profile] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [Nodes] セクションで、[+] をクリックします。

ステップ 7 [Select Node] ダイアログボックスで、下記に指定している項目を除き、必要に応じてフィールドに入力します。

a) [Node ID] ドロップダウン リストで、デバイスを接続するノード ID を選択します。

- 物理デバイスの場合は、物理デバイスをファブリックに接続するノードの ID にする必要があります。
- 仮想デバイスの場合は、仮想マシンをホストしているサーバが接続するノードの ID にする必要があります。

b) [Router ID] フィールドに、ACI ファブリックがルーティング プロトコル プロセスで使用するルータ ID を入力します。

c) ACI ファブリックとデバイスの間でスタティック ルーティングを使用する場合は、[Static Routes] セクションで [+] をクリックします。それ以外の場合は、ステップ 10 （76 ページ） に進みます。

ステップ 8 [Create Static Route] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [Prefix] セクションには、静的ルートのプレフィックスを入力します。

b) [Next Hop Addresses] セクションでは、[+] をクリックします。

c) 静的ルートのネクスト ホップ IP アドレスを入力します。

d) [Update] をクリックします。

ステップ 9 **OK** をクリックします。

ステップ 10 [Select Node] ダイアログボックスで、[OK] をクリックします。

ステップ 11 ダイナミック ルーティング プロトコルとしてデバイスで BGP を使用する場合は、[BGP Peer Connectivity Profiles] セクションで、[+] をクリックします。それ以外の場合は、ステップ 14 （77 ページ） に進みます。

ステップ 12 [Create Peer Connectivity Profile] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [Peer Address] フィールドで、BGP セッションを確立するデバイスの IP アドレスであるピア アドレスを入力します。

ステップ 13 [Create Peer Connectivity Profile] ダイアログボックスで、[OK] をクリックします。

ステップ 14 [Interface Profiles] セクションで、[+] をクリックします。

ステップ 15 [Create Interface Profile] ダイアログボックスで、必要に応じてフィールドに入力します。

a) ダイナミック ルーティング プロトコルとして OSPF を使用する場合は、OSPF プロファイル情報を入力します。

ステップ 16 [Interface] セクションでは、[SVI] タブを選択します。

ステップ 17 [Interface] セクションで、[+] をクリックします。

ステップ 18 [Select SVI Interface] ダイアログボックスで、下記に指定している項目を除き、必要に応じてフィールドに入力します。

a) [Path Type] オプション ボタンでは、デバイスのファブリックへの接続方法と一致するタイプを選択します。

b) [Path] ドロップダウン リストで、デバイスをファブリックに接続するパスを選択します。

- 物理デバイスの場合は、物理デバイスをファブリックに接続するパスです。
- 仮想デバイスの場合は、仮想マシンをホストしているサーバを接続するパスです。

c) [Encap] フィールドで、カプセル化 VLAN を指定します。

d) [IP Address] フィールドで、ファブリック SVI インターフェイスで使用する IP アドレスを指定します。

e) [MTU (bytes)] フィールドで、最大伝送ユニット サイズをバイト単位で指定します。

デフォルト値の「inherit」の場合、ACI ではデフォルト値の「9000」が使用され、リモート デバイスでは通常はデフォルト値の「1500」が使用されます。異なる MTU 値を指定すると、ACI とリモート デバイス間のピアリングで問題が発生する可能性があります。リモート デバイスの MTU 値を「1500」に設定した場合は、リモート デバイスの `L3Out` オブジェクトの MTU 値を「9000」に設定して ACI の MTU 値と一致させます。

ステップ 19 [OK] をクリックします。

ステップ 20 [Create Interface Profile] ダイアログボックスで、[OK] をクリックします。

ステップ 21 [Create Node Profile] ダイアログボックスで、[OK] をクリックします。

ステップ 22 [Create Routed Outside] ダイアログボックスで、[Next] をクリックします。

ステップ 23 [External EPG Networks] セクションで、[+] をクリックします。

ステップ 24 [Create External Network] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [Subnet] セクションで、[+] をクリックします。

ステップ 25 [Create Subnet] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [IP Address] フィールドに IP アドレスまたはサブネット マスクを入力します。

サブネットマスクは、従来のルーティングプロトコル設定で定義するネットワーク ステートメントと同等です。

ステップ 26 [OK] をクリックします。

ステップ 27 （任意） 必要に応じて、さらにサブネットを作成します。

ステップ 28 **[Create External Network]** ダイアログボックスで、**[OK]** をクリックします。

ステップ 29 **[Create Routed Outside]** ダイアログボックスで、**[Finish]** をクリックします。

GUI を使用したルータ設定の作成

ルーティング プロトコル設定の一部として、デバイスで使用するルータ ID を指定する必要があります。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ペインで、**テナント名** > **[Services]** > **[L4-L7]** > **[Router configurations]** を選択します。

ステップ 4 [Work] ペインの [Router Configurations] テーブルで、[+] をクリックします。

ステップ 5 デバイスでルータ ID として使用する IP アドレスを入力します。

ステップ 6 [更新（Update）] をクリックします。

GUI を使用したサービス グラフ アソシエーションの作成

サービス グラフのアソシエーションを作成する必要があります。これには、外部ルーテッド ネットワーク ポリシーおよびルータ設定とデバイス選択ポリシーの関連付けが含まれます。

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > **[すべてのテナント（ALL Tenants）]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーションウィンドウで、**[テナント（Tenant）]*[テナント名（tenant_name）]*** > **[サービス（Services）]** > **[L4-L7]** > **[デバイス選択ポリシー（Device Selection Policies）]** > ***[デバイス選択ポリシー（device_selection_policy）]*** の順に選択します。

ステップ 4 ナビゲーションウィンドウで、***[テナント名（tenant_name）]*** > **[L4 ～ L7 サービス（L4-L7 Services）]** > **[デバイス選択ポリシー（Device Selection Policies）]** > ***[デバイス選択ポリシー（device_selection_policy）]*** の順に選択します。*[デバイス選択ポリシー（device_selection_policy）]* は、Cisco Application Centric Infrastructure（ACI）ファブリックでルートピアリングを実行する際に使用するデバイス選択ポリシーです。

ステップ 5 [Work] ペインの [properties] セクションにある **[Router Config]** ドロップダウン リストで、ルーティング ピアリング用に作成したルータ設定を選択します。

ステップ 6 [Navigation] ペインで、選択したデバイス選択ポリシーを展開し、ACI ファブリックとピアリングするインターフェイスを選択します。

ステップ 7 [Work] ペインの [properties] セクションにある [Associated Network] オプション ボタンで、[L3 External Network] を選択します。

ステップ 8 **[L3 External Network]** ドロップダウン リストで、ルート ピアリング用に作成した外部ルーテッド ネットワークを選択します。

次のように変更されます。

- 外部ルーテッド ネットワークと関連付けたインターフェイスのカプセル化 VLAN が、外部ルーテッド ネットワーク インターフェイス プロファイルの一部として設定した VLAN と一致するようにプログラミングされる
- 外部ルーテッド ネットワーク インターフェイスとルーティング プロトコル設定がルーフ スイッチにプッシュされる
- ルーティングプロトコル設定がデバイスにプッシュされます

NX-OS スタイルの CLI を使用したルート ピアリングの設定

ここでは、ルート ピアリングを設定する NX OS スタイルの CLI のコマンドの例を示します。

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 テナントのコンフィギュレーション モードを開始します。

例：

```
apic1(config)# tenant 101
```

ステップ 3 サービス グラフを追加し、それをコントラクトと関連付けます。

例：

```
apic1(config-tenant)# l4l7 graph g1 contract c1
```

ステップ 4 デバイス クラスタに関連付けるノード（サービス）を追加します。

例：

```
apic1(config-graph)# service ASA_FW device-cluster-tenant 101 device-cluster ASA_FW1
```

ステップ 5 サービス機能で、コンシューマ コネクタとプロバイダー クラスタ インターフェイスを設定します。

例：

```
apic1(config-service)# connector consumer cluster-interface provider
```

ステップ 6 クラスタ インターフェイスで、サービス デバイスでのルート ピアリングで使用するレイヤ 3 Outside（l3extOut）とエンドポイント グループ（l3extInstP）を指定し、コネクタのコンフィギュレーション モードを終了します。

例：

```
apic1(config-connector)# l4l7-peer tenant 101 out l101 epg e101 redistribute bgp
apic1(config-connector)# exit
```

ステップ 7 プロバイダー コネクタとコンシューマのクラスタ インターフェイスにステップ 5 とステップ 6 を繰り返します。

例：

```
apic1(config-service)# connector provider cluster-interface consumer
apic1(config-connector)# l4l7-peer tenant 101 out l101 epg e101 redistribute bgp
apic1(config-connector)# exit
```

ステップ 8 （任意） コネクタからエンドポイント グループの関連付けを解除する場合は、**no l4l7-peer** コマンドを使用します。

例：

```
apic1(config-connector)# no l4l7-peer tenant 101 out l101 epg e101 redistribute bgp
```

ステップ 9 ルータ設定ポリシーをテナントに作成し、ピア レイヤ 4 ～ レイヤ 7 デバイスにルータ ID を指定し、コンフィギュレーション モードに戻ります。

例：

```
apic1(config)# tenant 102
apic1(config-tenant)# rtr-cfg bgp1
apic1(config-router)# router-id 1.2.3.5
apic1(config-router)# exit
```

ステップ 10 ルータ設定ポリシーを特定のサービス デバイスに関連付け、テナント コンフィギュレーション モードに戻ります。

例：

```
apic1(config-tenant)# l4l7 graph g2 contract c2 subject http
apic1(config-graph)# service ASA_FW device-cluster-tenant 102 device-cluster ASA_FW2
apic1(config-service)# rtr-cfg bgp1
apic1(config-service)# exit
apic1(config-graph)# exit
```

ステップ 11 レイヤ 3 Outside をリーフ インターフェイスおよび VRF に関連付けます。

例：

```
apic1(config-tenant)# external-l3 epg e101 l3out l101
apic1(config-tenant-l3ext-epg)# vrf member v101
apic1(config-tenant-l3ext-epg)# match ip 101.101.1.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant 101 vrf v101 l3out l101
apic1(config-leaf-vrf)# ip route 101.101.1.0/24 99.1.1.2
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/10
apic1(config-leaf-if)# vrf member tenant 101 vrf v101 l3out l101
apic1(config-leaf-if)# vlan-domain member dom101
```

```
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# ip address 99.1.1.1/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ルーティング プロトコル（BGP、OSPF）やルート マップなど、名前付きモードを使用したレイヤ 3 外部接続（レイヤ 3 Outside）の詳細な設定については、『*Cisco APIC NX-OS Style CLI Command Reference*』ドキュメントを参照してください。

（注） CLI での外部レイヤ3設定は、2つのモード（基本モードと名前付きモード）で使用できます。特定のテナントまたは VRF では、すべての外部レイヤ 3 設定にこれらのモードの 1 つのみを使用します。ルート ピアリングは名前付きモードでのみサポートされています。

ルート ピアリングのトラブルシューティング

Cisco Application Centric Infrastructure（ACI）ファブリックにルート ピアリングまたはデータ トラフィックの問題がある場合に、その問題をトラブルシーティングするために ACI ファブリック リーフ スイッチ上で実行できるコマンドがいくつかあります。

次の表に、ファブリック リーフ スイッチのスイッチ シェルで実行できるトラブルシューティング コマンドを示しますスイッチ。

コマンド	説明
show ip route vrf all	動的に取得したルートを含む特定のコンテキストのすべてのルートを表示します。
show ip ospf neighbor vrf all	隣接デバイスとの Open Shortest Path First（OSPF）ピアリング セッションを表示します。
show ip ospf vrf all	各コンテキスト内のランタイム OSPF 設定を表示します。
show ip ospf traffic vrf all	Virtual Routing and Forwarding（VRF）の各コンテキストの OSPF トラフィックを確認します。
show system internal policymgr stats	特定のリーフ スイッチのコントラクト フィルタ ルールを表示し、ルールのパケット ヒット カウントを確認します。

次の表に、**vsh_lc** シェルで実行できるトラブルシューティング コマンドを示します。

コマンド	説明
show system internal aclqos prefix	特定のリーフ スイッチの IPv4 プレフィックス アソシエーション ルールとルールのトラフィック ヒット カウントを確認します。

シェル コマンドに加えて、トラブルシューティングに役立つ次の点を確認できます。

- デバイスの健全性カウント
- 特定のテナントの下のすべてのエラーと `NwIssues`

CLI を使用したリーフ スイッチのルート ピアリング機能の確認

ファブリック リーフ上でスイッチ シェル コマンドを使用して、リーフ スイッチ設定とルート ピアリング機能を確認することができます。

ステップ 1 デバイスが接続されているファブリック リーフ スイッチで、SVI インターフェイスが設定されていることを確認します。

```
fab2-leaf3# show ip interface vrf user1:global
IP Interface Status for VRF "user1:global"
vlan30, Interface status: protocol-up/link-up/admin-up, iod: 134,
  IP address: 1.1.1.1, IP subnet: 1.1.1.0/30
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 1, tag: 0
lo3, Interface status: protocol-up/link-up/admin-up, iod: 133,
  IP address: 10.10.10.1, IP subnet: 10.10.10.1/32
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 1, tag: 0

fab2-leaf3#
```

インターフェイス vlan30 には SVI インターフェイス設定が含まれており、インターフェイス lo3 には外部ルーテッド ネットワーク設定に指定されているルータ ID が含まれています。

ステップ 2 ファブリック リーフ スイッチの Open Shortest Path First（OSPF）の設定を確認します。

```
fab2-leaf3# show ip ospf vrf user1:global

 Routing Process default with ID 10.10.10.1 VRF user1:global
 Stateful High Availability enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Table-map using route-map exp-ctx-2949120-deny-external-tag
 Redistributing External Routes from
   static route-map exp-ctx-st-2949120
   bgp route-map exp-ctx-proto-2949120
   eigrp route-map exp-ctx-proto-2949120
 Maximum number of non self-generated LSA allowed 100000
    (feature configured but inactive)
    Current number of non self-generated LSA 1
    Threshold for warning message 75%
    Ignore-time 5 minutes, reset-time 10 minutes
    Ignore-count allowed 5, current ignore-count 0
 Administrative distance 110
```

```
 Reference Bandwidth is 40000 Mbps
 SPF throttling delay time of 200.000 msecs,
   SPF throttling hold time of 1000.000 msecs,
   SPF throttling maximum wait time of 5000.000 msecs
 LSA throttling start time of 0.000 msecs,
   LSA throttling hold interval of 5000.000 msecs,
   LSA throttling maximum wait time of 5000.000 msecs
 Minimum LSA arrival 1000.000 msec
 LSA group pacing timer 10 secs
 Maximum paths to destination 8
 Number of external LSAs 0, checksum sum 0x0
 Number of opaque AS LSAs 0, checksum sum 0x0
 Number of areas is 1, 1 normal, 0 stub, 0 nssa
 Number of active areas is 1, 1 normal, 0 stub, 0 nssa
   Area (0.0.0.200)
        Area has existed for 00:17:55
        Interfaces in this area: 1 Active interfaces: 1
        Passive interfaces: 0  Loopback interfaces: 0
        SPF calculation has run 4 times
         Last SPF ran for 0.000273s
        Area ranges are
        Area-filter in 'exp-ctx-proto-2949120'
        Number of LSAs: 3, checksum sum 0x0
fab2-leaf3#
```

ステップ 3 ファブリック リーフ スイッチの OSPF ネイバーの関係を確認します。

```
fab2-leaf3# show ip ospf neighbors vrf user1:global
 OSPF Process ID default VRF user1:global
 Total number of neighbors: 1
 Neighbor ID     Pri State            Up Time  Address         Interface
 10.10.10.2        1 FULL/BDR         00:03:02 1.1.1.2         Vlan30
fab2-leaf3#
```

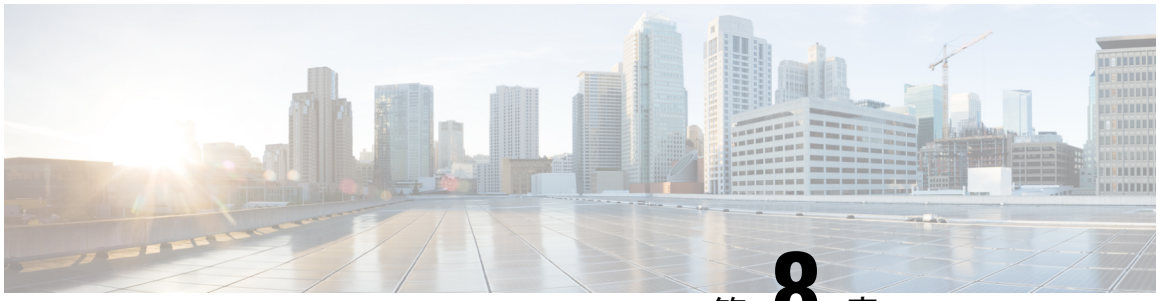
ステップ 4 ルートがファブリック リーフ スイッチによって取得されることを確認します。

```
fab2-leaf3# show ip route vrf user1:global
IP Route Table for VRF "user1:global"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

1.1.1.0/30, ubest/mbest: 1/0, attached, direct
    *via 1.1.1.1, vlan30, [1/0], 00:26:50, direct
1.1.1.1/32, ubest/mbest: 1/0, attached
    *via 1.1.1.1, vlan30, [1/0], 00:26:50, local, local
2.2.2.0/24, ubest/mbest: 1/0
    *via 1.1.1.2, vlan30, [110/20], 00:06:19, ospf-default, type-2
10.10.10.1/32, ubest/mbest: 2/0, attached, direct
    *via 10.10.10.1, lo3, [1/0], 00:26:50, local, local
    *via 10.10.10.1, lo3, [1/0], 00:26:50, direct
10.122.254.0/24, ubest/mbest: 1/0
    *via 1.1.1.2, vlan30, [110/20], 00:06:19, ospf-default, type-2
fab2-leaf3#
```

ステップ 5 OSPF がデバイス（この例では Cisco ASAv）に設定されていることを確認します。

```
ciscoasa# show running-config
: Saved
:
: Serial Number: 9AGRM5NBEXG
: Hardware:   ASAv, 2048 MB RAM, CPU Xeon 5500 series 2133 MHz
:
```

```
ASA Version 9.3(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif internalIf
 security-level 100
 ip address 2.2.2.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif externalIf
 security-level 50
 ip address 1.1.1.2 255.255.255.252
!
<<..>>
router ospf 1
 router-id 10.10.10.2
 network 1.1.1.0 255.255.255.252 area 200
 area 200
 log-adj-changes
 redistribute connected
 redistribute static
!
```



第 8 章

ポリシー ベース リダイレクトの設定

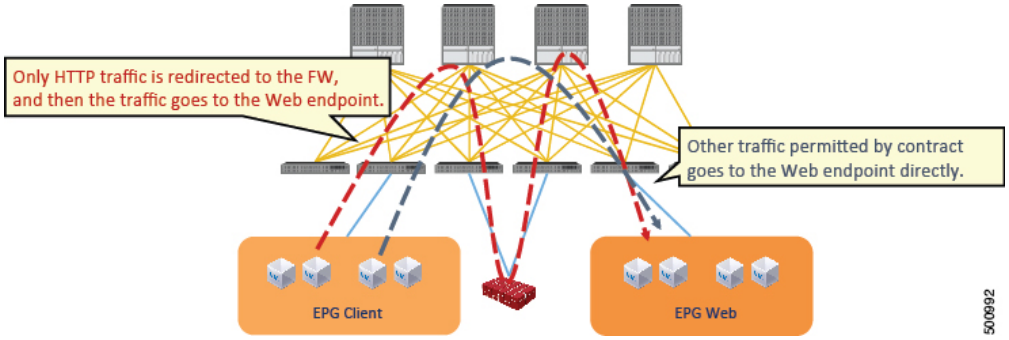
ポリシーベースのリダイレクトについて

Cisco Application Centric Infrastructure (ACI) ポリシーベースリダイレクト (PBR) により、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をプロビジョニングできます。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、プロビジョニングするコンシューマおよびプロバイダー エンドポイント グループをすべて同じ仮想ルーティングおよび転送（VRF）インスタンスに含めることで、サービス アプライアンスの展開をシンプル化できます。PBR の導入は、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、ルーティングとクラスタ リダイレクト 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から構成されます。サービス グラフ テンプレートを展開した後は、サービス グラフ プロバイ

ダーのエンドポイント グループを利用するためにエンドポイント グループを有効にすることにより、サービス アプライアンスを使用します。これは、vzAny を使用することにより、さらに簡素化し、自動化できます。パフォーマンスの要件が、専用のサービス アプライアンスをプロビジョニングするかどうかを決定するものとなるのに対し、PBR を使用すれば、仮想サービス アプライアンスの展開も容易になります。

次の図は、ファイアウォールへのトラフィックに固有の、リダイレクトの使用例を示しています:

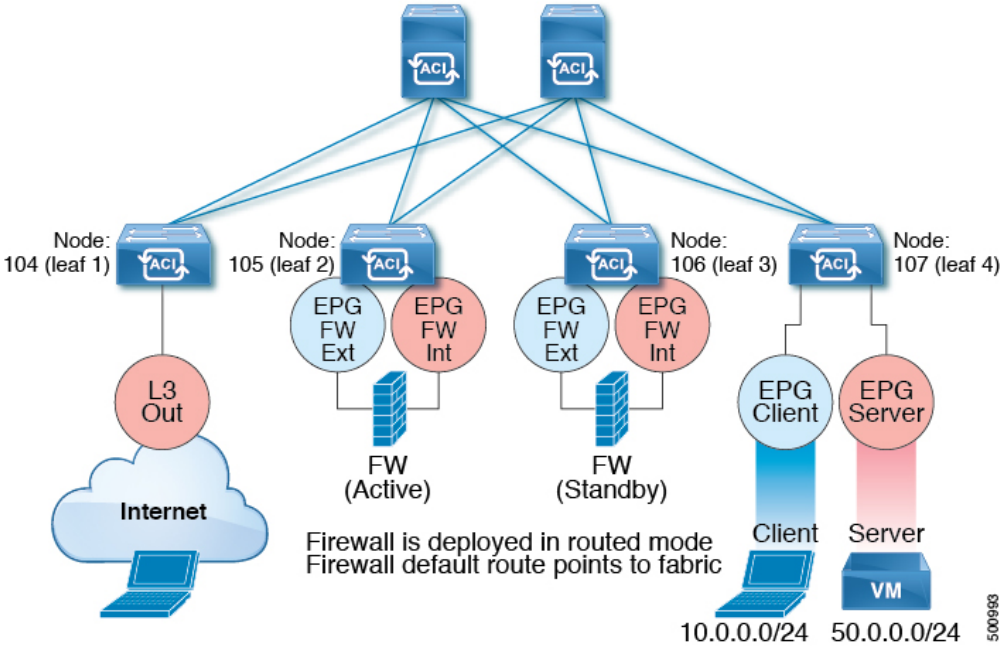
図 *8*: 使用例: ファイアウォール特有のトラフィックのリダイレクト



この使用例では、2つの情報カテゴリを作成する必要があります。最初の情報カテゴリはHTTPトラフィックを許可します。その後このトラフィックはファイアウォールにリダイレクトされます。トラフィックはファイアウォールを通過してから、Webエンドポイントに送られます。2 番目の情報カテゴリはすべてのトラフィックを許可します。これは最初の情報カテゴリではリダイレクトされなかったトラフィックをキャプチャします。トラフィックはそのまま Web エンドポイントに送られます。

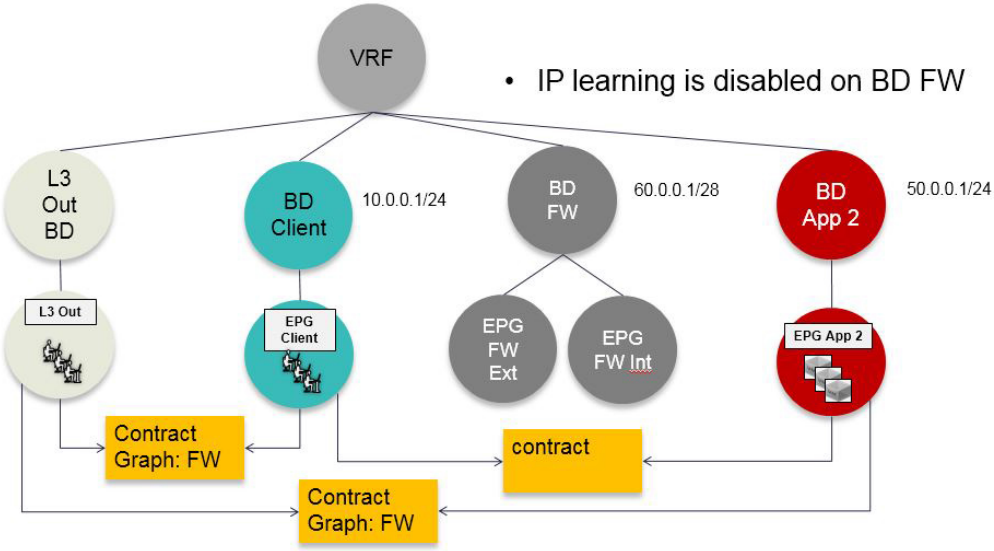
次の図は、ACI PBR 物理トポロジのサンプルを示しています:

図 *9* : サンプルの *ACI PBR* 物理トポロジ



次の図は、ACI PBR 論理トポロジのサンプルを示しています:

図 *10* : サンプルの *ACI PBR* 論理トポロジ



これらの例はシンプルな導入ですが、 ACI PBR は、ファイアウォールやサーバのロード バランサなどのような、複数のサービスのために物理および仮想サービス アプライアンスの両方を混在させたものにスケールアップすることを可能にします。

ポリシーベースのリダイレクトを設定する際の注意事項と制約事項

ポリシーベースリダイレクト(PBR)サービスノードを計画するときは、次の注意事項と制限事項に従ってください。

- ファブリック内の PBR でパケットをルーティングする必要があるため、パケットの送信元 MAC アドレスが書き換えられる可能性があります。IP アドレスヘッダーの存続可能時間(TTL)フィールドは、ファブリック内でパケットがルーティングされる回数だけ減少します。
- 両方のサービスレッグに同じアクションを選択します。つまり、内部サービスレッグの拒否アクションを選択した場合は、外部サービスレッグの拒否アクションも選択する必要があります。
- L3Out EPG と通常の EPG は、コンシューマー EPG またはプロバイダー EPG にできます。
- L2Out EPG は、コンシューマー EPG またはプロバイダー EPG にすることはできません。
- Cold Standby のアクティブ/スタンバイ導入では、サービス ノードにアクティブな導入の MAC アドレスを設定します。Cold Standby のアクティブ/スタンバイ導入では、アクティブ ノードがダウンすると、スタンバイ ノードがアクティブ ノードの MAC アドレスを引き継ぎます。
- ネクストホップ サービスノードの IP アドレスを指定する必要があります。
- 5.2(1) より前のリリースでは、仮想 MAC アドレスを指定する必要があります。5.2(1) 以降のリリースでは、オプションで仮想MACアドレスを提供せず、代わりにCisco Application Policy Infrastructure Controller (Cisco APIC) にアドレスを動的に検出できます。
- 別のブリッジ ドメイン サービスにアプライアンスをプロビジョニングします。Cisco APIC 3.1(1)以降のリリースでは、サービスアプライアンスを別のブリッジドメインにプロビジョニングすることは必須ではありません。そのためには、Cisco Nexus 9300-EX と 9300-FX プラットフォームのリーフ スイッチが必要です。
- Cisco APIC リリース 3.1 からダウングレードする場合、ポリシーベースのリダイレクトブリッジドメインが同じブリッジドメインをコンシューマーまたはプロバイダーとして使用しているかどうかを内部コードで確認します。その場合にはダウングレード中にエラーが出されます。そのような設定は Cisco APIC の以前のバージョンではサポートされないからです。
- 5.2(1) 以降のリリースから 5.2(1) より前のリリースにダウングレードする場合は、5.2 リリースからの PBR 関連の機能を含むすべての PBR 関連の設定を削除し、関連するサービスグラフを削除する必要があります。次に例を示します。
  - L3Out で PBR 接続先を使用するデバイス選択ポリシーを削除します。
  - 拡張 LAG ポリシーを使用するレイヤ 4 ～ レイヤ 7 サービスデバイスを削除します。
  - HTTP SLA タイプを使用する IP SLA モニタリングポリシーを削除します。
  - 接続先 MAC アドレスが設定されていない PBR 接続先を削除します。

- サービスアプライアンス、ソース、ブリッジドメインは、同じ VRF インスタンスに配置できます。
- Cisco N9K-93128TX、N9K-9396PX、N9K-9396TX、N9K-9372PX、および N9K-9372TX スイッチでは、サービスアプライアンスを、送信元または宛先のいずれかのエンドポイントグループと同じリーフ スイッチに配置することはできません。Cisco N9K-C93180YC-EX および N9K-93108TC-EX スイッチでは、サービス アプライアンスを、送信元または宛先のいずれかのエンドポイント グループと同じリーフ スイッチに配置することができます。
- PBR ノードインターフェイスは、FEX ホストインターフェイスではサポートされていません。PBR ノードインターフェイスは、FEX ホストインターフェイスではなく、リーフ ダウンリンク インターフェイスの下に接続する必要があります。コンシューマーとプロバイダーのエンドポイントは、FEX ホストインターフェイスで接続できます。
- サービスアプライアンスは、ブリッジドメインにのみ存在できます。
- サービス アプライアンスのプロバイダーのエンドポイント グループによって提供される契約は `allow-all` に設定できますが、トラフィックを Cisco Application Centric Infrastructure (Cisco ACI) ファブリックでルーティングすることはできません。
- Cisco APIC リリース 3.1(1) 以降のリリースでは、Cisco Nexus 9300-EX および 9300-FX プラットフォーム リーフ スイッチを使用する場合、ポリシーベースのリダイレクト ブリッジドメインでエンドポイントデータプレーン学習を無効にする必要はありません。サービス グラフの導入時には、ポリシーベースのリダイレクト ノード EPG の場合にのみ、エンドポイント データプレーンの学習は自動的に無効にされます。非 EX および非 FX プラットフォーム リーフ スイッチを使用する場合は、ポリシー ベースのリダイレクト ブリッジドメインでエンドポイントデータプレーンの学習を無効にする必要があります。ポリシーベースのリダイレクト ブリッジ ドメインでは、エンドポイント データプレーンの学習を無効にする必要があります。
- Cisco APIC リリース 4.0(1) 以降のリリースでは、PBR を使用してサービスグラフをコントラクト対象に付加できます。サービスグラフとの EPG 内コントラクトは、EPG 間コントラクトとして同時に使用することはできません。リダイレクトが有効になっているサービスグラフで使用する場合は、EPG 間および EPG 内の通信に別々のコントラクトを使用する必要があります。
- Cisco APIC リリース 4.2(3) 以降のリリースでは、サービスグラフテンプレートでコントラクトからのフィルタ（filters-from-contract）オプションが利用可能になり、ソースまたは接続先にコンシューマー EPG クラス ID を含まないゾーニングルールに対して、デフォルトのフィルタの代わりにサービスグラフが付加されているコントラクト対象の特定のフィルタを使用できるようになりました。ソースまたは接続先としてコンシューマー EPG クラス ID を持つゾーニングルールでは、オプションに関係なく特定のフィルタを使用します。
- マルチノードポリシーベースのリダイレクト（マルチノード PBR）：
  - ポリシーベースリダイレクト用に構成できるサービスグラフで最大 5 つの機能ノードをサポートします。

- マルチノード PBR サービスチェーンを使用する場合、すべてのサービスデバイスはローカルリーフスイッチにあるか、リモートリーフスイッチに接続されている必要がありますが、両方に分散することはできません。
  - サポートされるトポロジ：

    このトポロジでは、*RL* はリモートリーフスイッチを意味し、*LL* はリモートリーフスイッチの下ではなく、メインロケーションの下にあるローカルリーフスイッチを意味します。

    - N1(LL)--N2(LL)--N3(LL)：すべてのデバイスは、メインロケーションとリモートリーフスイッチに分散されていないローカルリーフスイッチに接続されています。
    - N1(RL)-N2(RL)--N3(RL)：すべてのデバイスがリモートリーフスイッチに接続されています。

  - サポートされていないトポロジ：
    - N1(LL)--N2(RL)--N3(LL)：サービスデバイスは、ローカルリーフスイッチとリモートリーフスイッチに分かれます。

- ロードバランサ向けのマルチノード PBR レイヤ 3 接続先ガイドライン：
  - レイヤ 3 接続先アップグレード：レイヤ 3 接続先 (VIP) パラメータは、アップグレード後にデフォルトで有効になります。特定のサービスノードでPBRポリシーが設定されていない場合（3.2(1) より前のリリース）、ノードコネクタはレイヤ 3 の接続先として扱われ、新しい Cisco APIC リリースでも引き続き使用されるため、このことによる問題は発生しません。
  - トラフィックは、必ずしもコンシューマー/プロバイダーのみが接続先である必要はありません。
  - 転送方向では、トラフィックはロードバランサのVIPアドレスに送信されます。
  - 逆方向では、SNAT が有効になっている場合、トラフィックはロードバランサの内部レッグに送信されます。
  - 両方向で、論理インターフェイス コンテキストでレイヤ 3 接続先 (VIP) を有効（チェック）します。
  - 両方向でレイヤ 3 接続先 (VIP) を有効（チェック）し、内部側で PBR ポリシーを構成することにより、ロードバランサ内部で SNAT から No-SNAT に切り替えられるようにします。
  - SNAT が無効の場合:
    - 逆方向のトラフィックはコンシューマーに送られますが、ロードバランサの内部レッグには送られません（内部レッグで PBR ポリシーを有効にします）。

- この場合はPBRポリシーが適用されるため、レイヤ3接続先(VIP)は適用されません。

- マルチキャストおよびブロードキャスト トラフィック リダイレクションはサポートされていません。
- リダイレクト ポリシーの宛先を別のグループに変更した場合、Cisco APICは変更に対してエラーを発生し、ポリシーの動作状態は無効になります。ポリシーを再度有効にするには、エラーをクリアする必要があります。
- PBRを使用するEPG内または外部内のEPGコントラクトは、EPG間コントラクトには使用できません。
- 非PBR EPGからPBR EPGにエンドポイントを移行する場合、接続先リーフスイッチのリモートエンドポイントは、古い非PBR EPGのsclassの詳細を持つリモートエンドポイントをクリアしません。この問題は、リモートエンドポイントを持つ接続先リーフスイッチが、製品IDに-EX、-FX、または-GXサフィックスが付いているスイッチの場合に発生します。この問題は、製品IDに-FX2、-GX2、またはそれ以降のサフィックスが付いているスイッチでは発生しません。

  この問題が発生した場合、次のCLIコマンドを使用して、リモートエンドポイントを手動でクリアできます。

  ```
  vsh -c "clear system internal epm endpoint key vrf vrf_name ip ip_name"
  ```

- サポートされているポリシーベースのリダイレクト設定には、次のものがあります。

図 *11* : 同じ *VRF* インスタンスのポリシーベースリダイレクト

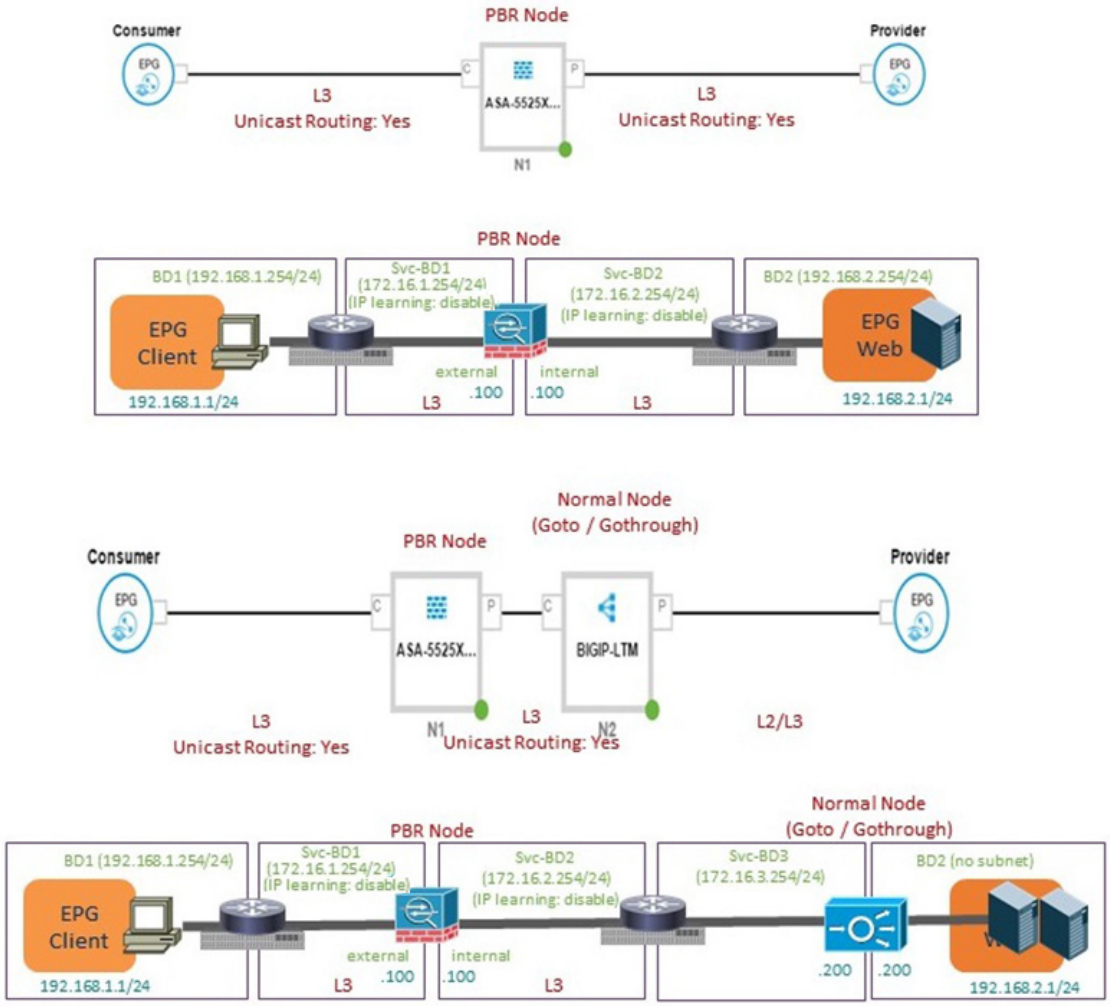


図 *12* : 異なる *VRF* インスタンスのポリシーベースリダイレクト

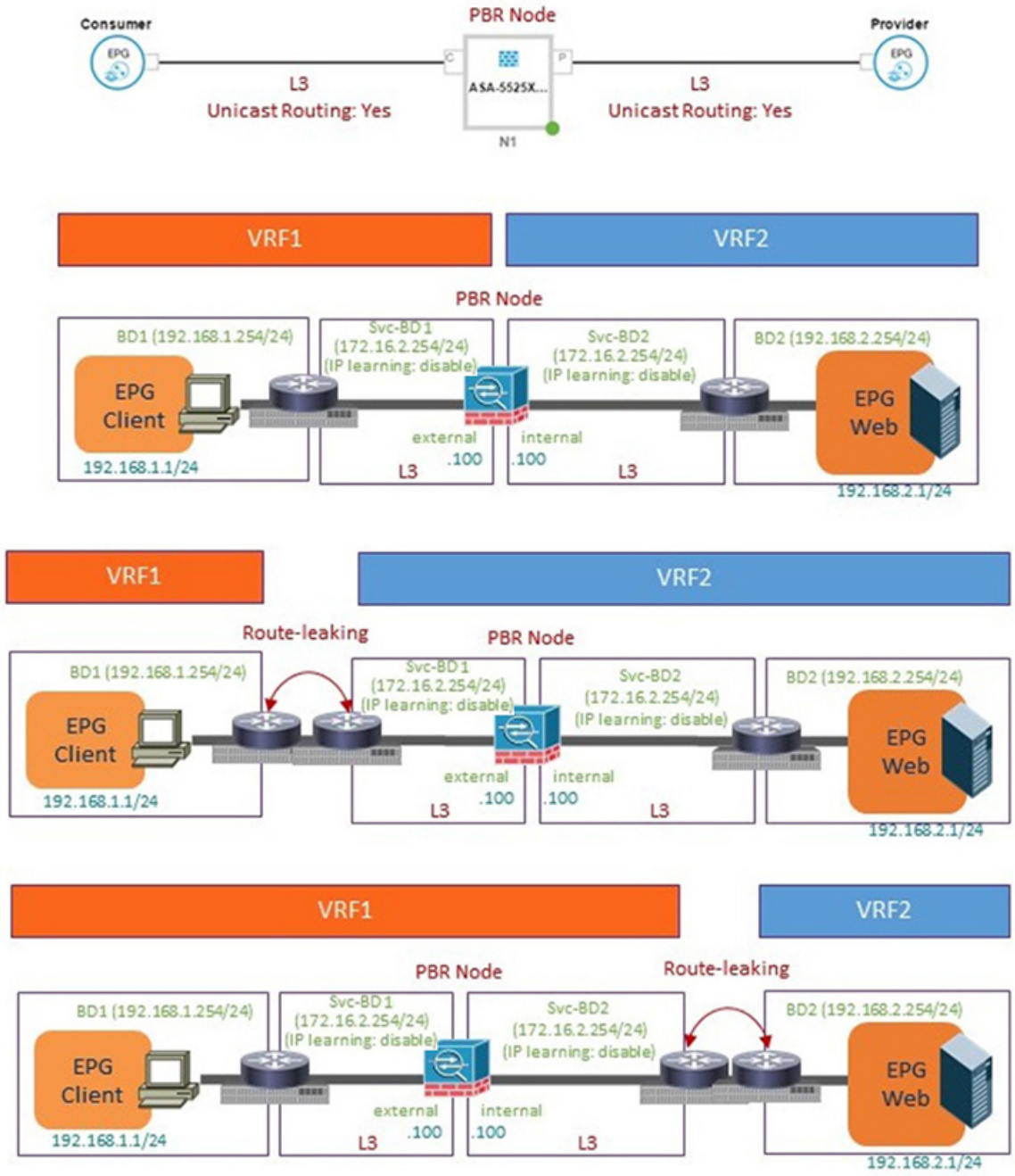
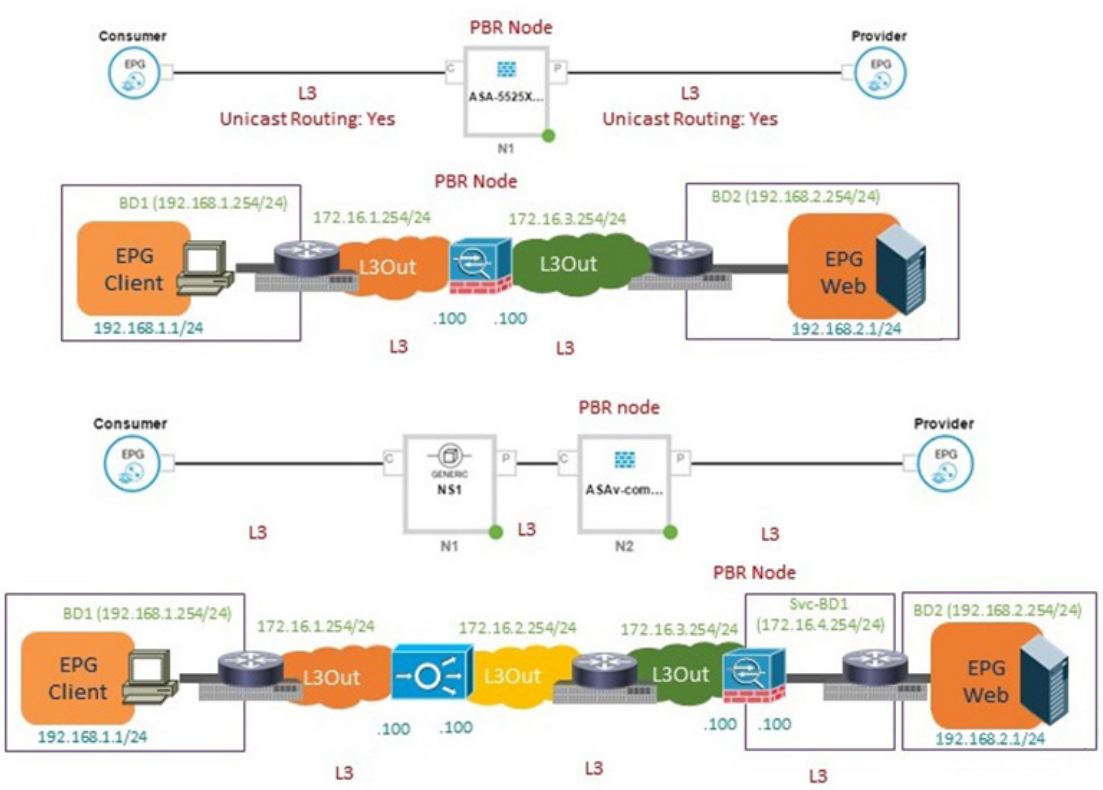
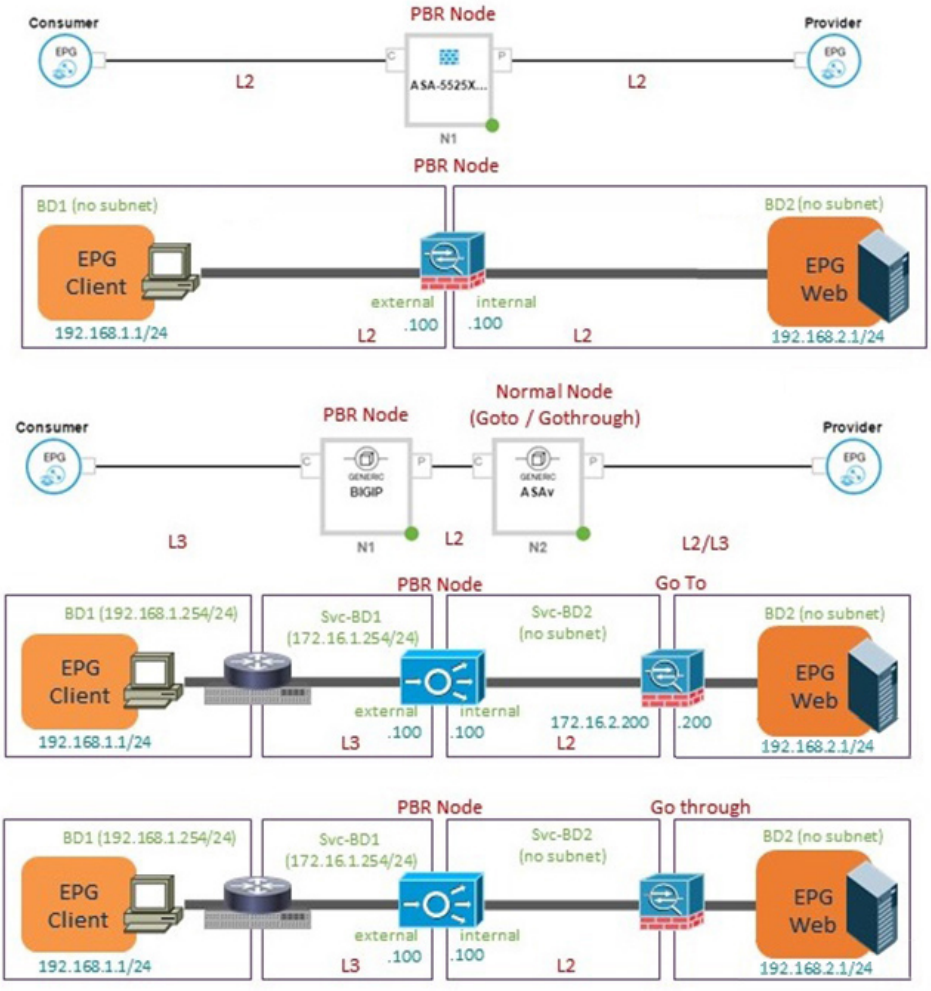


図 *13 : L3Out* 接続先を使用したポリシーベースリダイレクト



- サポートされていないポリシー ベースのリダイレクト設定は次のとおりです:

図 *14* : サポートされていないポリシー ベースのリダイレクト設定



GUI を使用したポリシー ベース リダイレクトの設定

次の手順では、GUI を使用してポリシー ベース リダイレクト (PBR) を設定します。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ウィンドウで、**Tenant *tenant_name*** > **Services** > **L4-L7** > **Devices** を選択します。

ステップ 4 作業ウィンドウで、 **Actions** > **Create L4-L7 Devices** を選択します。

ステップ 5 **Create L4-L7 Devices** ダイアログボックスで、必要に応じてフィールドに入力します。

[全般（**General**）] セクションでは、[**サービスタイプ**（**Service Type**）] には [**ファイアウォール**（**Firewall**）]、[**ADC**]、[その他（Other）] を選択できます。

（注） レイヤ 1/レイヤ 2 PBR 設定の場合、レイヤ 4 ～ レイヤ 7 サービスデバイスを作成し、次の手順を実行します。

1. [**その他（Other）**] として、[**サービスタイプ**] を選択します。
2. [**デバイスタイプ（Device Type）**] には、[**物理（Physical）**] を選択します（クラウド/仮想はサポートされていません）。
3. 物理ドメインを選択します。
4. 必要に応じて、[**機能タイプ（Function Type）**] [**L1**] または [**L2**] を選択します。
5. 外部および内部の具象インターフェイスを作成し、対応するリーフにポート接続を作成します。
6. 事前に作成した具象インターフェイスを選択し、クラスタインターフェイスを作成します。このインターフェイスを作成するときは VLAN カプセル化を指定する必要があります。カプセル化はサービス デバイスにプッシュされます。

   （注） 静的VLAN構成の場合、外部レッグと内部レッグがレイヤ2に対して異なるVLANを持つことを確認します。それ以外は、レイヤ1に対して同じVLANになります。

ステップ 6 ナビゲーション ウィンドウで、**Tenant** *tenant_name* > **Services** > **L4-L7** > **Service Graph Templates** を選択します。

ステップ 7 作業ウィンドウで、**Action** > **Create L4-L7 Service Graph Template** を選択します。

ステップ 8 **Create L4-L7 Service Graph Template** ダイアログボックスで、次の操作を実行します:

a) **Graph Name** フィール小渡に、サービス グラフ テンプレートの名前を入力します。
b) **Graph Type** ラジオ ボタンで、**Create A New Graph** をクリックします。
c) **Device Clusters** ペインで作成したデバイスを、コンシューマ エンドポイント グループとプロバイダ エンドポイント グループの間にドラッグ アンド ドロップします。これで、サービス ノードが作成されます。

   Cisco Application Policy Infrastructure Controller (APIC) リリース 4.2(1) 以降のリリースでは、オプションで手順 c を繰り返すことで、最大で 5 つのサービスノードを含めることができます。

d) デバイスのサービスの種類に基づいて、以下を選択します:

   ファイアウォールの場合には、**Routed** を選択して、次の手順を続けます。

   ADC の場合には、**One-Arm** または **Two-Arm** を選択して、次の手順を続けます。

e) **Route Redirect** チェックボックスをオンにします。
f) [Submit] をクリックします。

新しいサービスグラフテンプレートが [**サービスグラフテンプレート（Service Graph Templates**）] テーブルに表示されます。

ステップ 9 ナビゲーション ウィンドウで、**Tenant** *tenant_name* > **Policies** > **Protocol** > **L4-L7 Policy Based Redirect** を選択します。

ステップ 10 作業ウィンドウで、**Action** > **Create L4-L7 Policy Based Redirect** を選択します。

ステップ 11 **Create L4-L7 Policy Based Redirect** ダイアログボックスで、必要に応じてフィールドに入力します。このポリシーベースのリダイレクト ポリシーは、コンシューマ コネクタ用のものです。

ステップ 12 プロバイダ コネクタ用には、別のポリシー ベースのリダイレクト ポリシーを作成します。

ステップ 13 ナビゲーション ウィンドウで、**Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Service Graph Templates** > ***service_graph_template_name*** を選択します。

作成したサービス グラフ テンプレートを選択します。

ステップ 14 サービス グラフ テンプレートを右クリックして、**Apply L4-L7 Service Graph Template** を選択します。

ステップ 15 **Apply L4-L7 Service Graph Template to EPGs** ダイアログボックスで、次の操作を実行します:

a) **Consumer EPG/External Network** ドロップダウンリストで、コンシューマ エンドポイント グループを選択します。

b) **Provider EPG/External Network** ドロップダウンリストで、プロバイダ エンドポイント グループを選択します。

c) **Contract** オプション ボタンの **Create A New Contract** をクリックします。

d) **Contract Name** フィールドに、契約の名前を入力します。

e) **No Filter (Allow All Traffic)** チェック ボックスはオンにしないでください。

f) **Filter Entries** テーブルで **+** をクリックしてエントリを追加します。

g) 新しいフィルタ エントリで、名前として [IP] を入力し、**IP** を **Ether Type** として選択して、**Update** をクリックします。

h) **Next** をクリックします。

i) コンシューマ コネクタの **Redirect Policy** ドロップダウンリストで、コンシューマ コネクタ用に作成したリダイレクト ポリシーを選択します。

j) コンシューマ コネクタの **Cluster Interface** ドロップダウンリストで、コンシューマ クラスタ インターフェイスを選択します。

k) プロバイダ コネクタの **Redirect Policy** ドロップダウンリストで、プロバイダ コネクタ用に作成したリダイレクト ポリシーを選択します。

l) プロバイダ コネクタの **Cluster Interface** ドロップダウンリストで、プロバイダ クラスタ インターフェイスを選択します。

m) **Finish** をクリックします。

NX-OS スタイルの CLI を使用したポリシー ベース リダイレクトの設定

この手順のコマンド例にはには、ルート リダイレクト、クラスタのリダイレクト、およびグラフの導入が含まれます。デバイスはテナント T1 の下に作成されます。

ステップ 1 デバイス クラスタを作成します。

例：

```
l4l7 cluster name ifav-asa-vm-ha type virtual vlan-domain ACIVswitch service FW function go-to
    cluster-device Device2 vcenter ifav108-vcenter vm "ASAv_HA1"
    cluster-device Device1 vcenter ifav108-vcenter vm "ASAv_HA"
    cluster-interface provider
```

```
      member device Device1 device-interface GigabitEthernet0/1
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 3"
        exit
      member device Device2 device-interface GigabitEthernet0/1
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 3"
        exit
      exit
    cluster-interface failover_link
      member device Device1 device-interface GigabitEthernet0/8
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 10"
        exit
      member device Device2 device-interface GigabitEthernet0/8
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 10"
        exit
      exit
    cluster-interface consumer
      member device Device1 device-interface GigabitEthernet0/0
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 2"
        exit
      member device Device2 device-interface GigabitEthernet0/0
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 2"
        exit
      exit
    exit
exit
```

ステップ 2 テナント PBRv6_ASA_HA_Mode の下に、PBR サービス グラフ インスタンスを展開します。

例：

```
tenant PBRv6_ASA_HA_Mode
  access-list Contract_PBRv6_ASA_HA_Mode_Filter
    match ip
    exit
```

ステップ 3 フィルタが IP プロトコルに一致する PBR 用の契約を作成します。情報カテゴリの下で、レイヤ 4 ～ レイヤ 7 サービス グラフ名を指定します。

サービス アプライアンスのプロバイダ エンドポイント グループによって提供される契約は、`allow-all` 設定では構成できません。

例：

```
  contract Contract_PBRv6_ASA_HA_Mode
    scope tenant
    subject Subject
      access-group Contract_PBRv6_ASA_HA_Mode_Filter both
      l4l7 graph PBRv6_ASA_HA_Mode_Graph
      exit
    exit
  vrf context CTX1
    exit
  vrf context CTX2
    exit
```

ステップ 4 クライアントとサーバのエンドポイント グループ用にブリッジ ドメインを作成します。クライアントとサーバの両方が同じ VRF インスタンスに属します。

例：

```
bridge-domain BD1
  arp flooding
  l2-unknown-unicast flood
  vrf member CTX1
  exit
bridge-domain BD2
  arp flooding
  l2-unknown-unicast flood
  vrf member CTX1
  exit
```

ステップ 5 ファイアウォールの内部および外部レッグ用には、別のブリッジ ドメインを作成します。

PBR では、リモート リーフ スイッチの送信元 VTEP の学習が無効になっている必要があります。これは、**no ip learning** コマンドで行います。

例：

```
bridge-domain External-BD3
  arp flooding
  no ip learning
  l2-unknown-unicast flood
  vrf member CTX1
  exit
bridge-domain Internal-BD4
  arp flooding
  no ip learning
  l2-unknown-unicast flood
  vrf member CTX1
  exit
```

ステップ 6 アプリケーションプロファイルを作成し、エンドポイント グループを指定します。

例：

```
application AP1
  epg ClientEPG
    bridge-domain member BD1
    contract consumer Contract_PBRv6_ASA_HA_Mode
    exit
  epg ServerEPG
    bridge-domain member BD2
    contract provider Contract_PBRv6_ASA_HA_Mode
    exit
  exit
```

ステップ 7 ブリッジ ドメインのデフォルト ゲートウェイを指定します。

例：

```
interface bridge-domain BD1
  ipv6 address 89:1:1:1::64/64
  exit
interface bridge-domain BD2
  ipv6 address 99:1:1:1::64/64
  exit

interface bridge-domain External-BD3
  ipv6 address 10:1:1:1::64/64
  exit
interface bridge-domain Internal-BD4
  ipv6 address 20:1:1:1::64/64
  exit
```

ステップ 8 テナント T1 からデバイスをインポートします。

例：

```
l417 cluster import-from T1 device-cluster ifav-asa-vm-ha
```

ステップ 9 サービス リダイレクト ポリシーを使用してサービス グラフを作成します。

例：

```
l417 graph PBRv6_ASA_HA_Mode_Graph contract Contract_PBRv6_ASA_HA_Mode
      service N2 device-cluster-tenant T1 device-cluster ifav-asa-vm-ha mode FW_ROUTED svcredir
enable
      connector consumer cluster-interface consumer_PBRv6
          bridge-domain tenant PBRv6_ASA_HA_Mode name External-BD3
          svcredir-pol tenant PBRv6_ASA_HA_Mode name External_leg
          exit
      connector provider cluster-interface provider_PBRv6
          bridge-domain tenant PBRv6_ASA_HA_Mode name Internal-BD4
          svcredir-pol tenant PBRv6_ASA_HA_Mode name Internal_leg
          exit
        exit
    connection C1 terminal consumer service N2 connector consumer
    connection C2 terminal provider service N2 connector provider
    exit
```

ステップ 10 外部および内部レッグのサービス リダイレクトのポリシーを作成します。IPv6 アドレスは次の例で使用されます。同じコマンドを使用して IPv4 アドレスを指定することもできます。

例：

```
svcredir-pol Internal_leg
    redir-dest 20:1:1:1::1 00:00:AB:CD:00:11
    exit
svcredir-pol External_leg
    redir-dest 10:1:1:1::1 00:00:AB:CD:00:09
    exit
exit
```

NX-OS スタイルの CLI を使用したポリシー ベースのリダイレクト設定を確認する

ポリシー ベースのリダイレクトを設定した後は、NX-OS スタイル CLI を使用して設定を確認できます。

ステップ 1 テナントの実行設定を表示します。

例：

```
apic1# show running-config tenant PBRv6_ASA_HA_Mode svcredir-pol
# Command: show running-config tenant PBRv6_ASA_HA_Mode svcredir-pol
# Time: Wed May 25 00:57:22 2016
  tenant PBRv6_ASA_HA_Mode
    svcredir-pol Internal_leg
      redir-dest 20:1:1:1::1/32 00:00:AB:CD:00:11
      exit
    svcredir-pol External_leg
```

```
      redir-dest 10:1:1:1::1/32 00:00:AB:CD:00:09
      exit
    exit
```

ステップ 2 テナントとそのサービス グラフの実行設定を表示します。

例：

```
apic1# show running-config tenant PBRv6_ASA_HA_Mode l4l7 graph PBRv6_ASA_HA_Mode_Graph
# Command: show running-config tenant PBRv6_ASA_HA_Mode l4l7 graph PBRv6_ASA_HA_Mode_Graph
# Time: Wed May 25 00:55:09 2016
  tenant PBRv6_ASA_HA_Mode
    l4l7 graph PBRv6_ASA_HA_Mode_Graph contract Contract_PBRv6_ASA_HA_Mode
      service N2 device-cluster-tenant T1 device-cluster ifav-asa-vm-ha mode FW_ROUTED svcredir
enable
        connector consumer cluster-interface consumer_PBRv6

          bridge-domain tenant PBRv6_ASA_HA_Mode name External-BD3

          svcredir-pol tenant PBRv6_ASA_HA_Mode name External_leg

          exit

        connector provider cluster-interface provider_PBRv6

          bridge-domain tenant PBRv6_ASA_HA_Mode name Internal-BD4
          svcredir-pol tenant PBRv6_ASA_HA_Mode name Internal_leg
          exit
        exit
      connection C1 terminal consumer service N2 connector consumer
      connection C2 terminal provider service N2 connector provider
      exit
    exit
```

ステップ 3 サービス グラフ設定を表示します。

例：

```
apic1# show l4l7-graph graph PBRv6_ASA_HA_Mode_Graph
Graph           : PBRv6_ASA_HA_Mode-PBRv6_ASA_HA_Mode_Graph
Graph Instances : 1

Consumer EPg     : PBRv6_ASA_HA_Mode-ClientEPG
Provider EPg     : PBRv6_ASA_HA_Mode-ServerEPG
Contract Name    : PBRv6_ASA_HA_Mode-Contract_PBRv6_ASA_HA_Mode
Config status    : applied
Service Redirect : enabled

Function Node Name : N2
 Connector   Encap       Bridge-Domain  Device Interface      Service Redirect Policy
 ----------  ----------  ----------     --------------------  -----------------------
 consumer    vlan-241    PBRv6_ASA_HA_  consumer_PBRv6        External_leg
                         Mode-
                         External-BD3
 provider    vlan-105    PBRv6_ASA_HA_  provider_PBRv6        Internal_leg
                         Mode-
                         Internal-BD4
```

複数ノード ポリシー ベースのリダイレクトについて

マルチノード ポリシーベースリダイレクトは、サービスグラフで最大 5 つの機能ノードをサポートすることで PBR を強化します。どのサービス ノードのコネクタがトラフィックの終端になるかは設定することができ、この設定に基づいて、サービス チェーンの送信元および宛先クラス ID が決定されます。複数のノード PBR 機能では、ポリシー ベースのリダイレクトはサービス ノード コネクタのコンシューマ側、プロバイダ側、またはその両方で有効にすることができます。これは、転送方向にも、または逆方向にも設定できます。サービス ノードのコネクタで PBR ポリシーを設定した場合、そのコネクタがトラフィックを終端することはありません。

対称ポリシー ベースのリダイレクトについて

対称ポリシーベースリダイレクト(PBR)構成により、サービスノードのプールをプロビジョニングできるため、ポリシーに基づき、コンシューマーとプロバイダーのエンドポイントグループ間のトラフィックを負荷分散できます。トラフィックは、送信元および宛先 IP 等価コストマルチパス ルーティング(ECMP)プレフィックス ハッシュに応じて、プール内のサービス ノードの 1 つにリダイレクトされます。

（注） 対称 PBR 構成には、9300-EX 以降のハードウェアが必要です。

対称 PBR REST のサンプルの例を以下に示します。

```
Under fvTenant svcCont

<vnsSvcRedirectPol name="LoadBalancer_pool">
          <vnsRedirectDest name="lb1" ip="1.1.1.1" mac="00:00:11:22:33:44"/>
          <vnsRedirectDest name="lb2" ip="2.2.2.2" mac="00:de:ad:be:ef:01"/>
          <vnsRedirectDest name="lb3" ip="3.3.3.3" mac="00:de:ad:be:ef:02"/>
</vnsSvcRedirectPol>

<vnsLIfCtx name="external">
          <vnsRsSvcRedirectPol tnVnsSvcRedirectPolName="LoadBalancer_pool"/>
          <vnsRsLIfCtxToBD tDn="uni/tn-solar/bd-fwBD">
</vnsLIfCtx>

<vnsAbsNode name="FW" routingMode="redirect">
```

対称 PBR NX-OS スタイルの CLI コマンドの例を次に示します。

テナント スコープの下の次のコマンドは、サービス リダイレクト ポリシーを作成します。

```
apic1(config-tenant)# svcredir-pol fw-external
apic1(svcredir-pol)# redir-dest 2.2.2.2 00:11:22:33:44:56
```

次のコマンドは PBR を有効にします。

```
apic1(config-tenant)# l4l7 graph FWOnly contract default
apic1(config-graph)# service FW svcredir enable
```

次のコマンドは、デバイス選択ポリシーコネクタの下にリダイレクトポリシーを設定します。

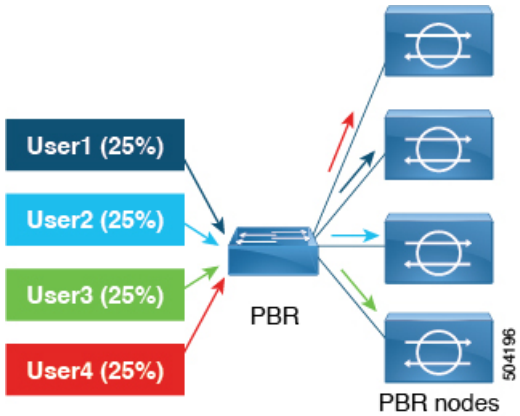
```
apic1(config-service)# connector external
apic1(config-connector)# svcredir-pol tenant solar name fw-external
```

重みベースの対称ポリシーベースのリダイレクトについて

Cisco APIC リリース 6.0(1) より前のリリースでは、各 PBR 接続先の重みを指定するオプションはありませんでした。PBR 接続先（サービスノード）のキャパシティは考慮されておらず、各接続先の重みは同じでデフォルト値の 1 です。次の例では、4 つの接続先を考えます。トラフィックのロードバランスの重みが同じであるため、各接続先では約 25% とほぼ同じ量のトラフィックを受信できます。

表 *2 : PBR* 接続先へのトラフィック（デフォルト設定の対称 *PBR*、重みは「*1*」）

Destination	重量	**Traffic %-age** （おおよその）
接続先 1	1	25
接続先 2	1	25
接続先 3	1	25
接続先 4	1	25

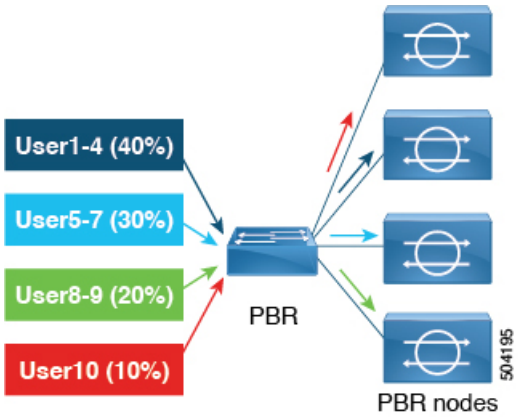


Cisco APIC リリース 6.0(1) 以降のリリースでは、トラフィックをより効率的に処理する重みベースの対称 PBR がサポートされています。重みベースの対称 PBR では、管理者はサービスノードのキャパシティに基づいて PBR 接続先の重みを設定し、設定された重みに基づいて負荷分散できます。1つのサービスノードは複数のポリシーに属することができ、異なるポリシーで異なる重みを持てます。

容量の異なる 4 つの PBR 接続先について考察します。すべての接続先に同じ量のトラフィックは送信されず、接続先の PBR 設定は重みベースです。1 から 10 までの重みを付けることができます。重みが付いてない場合、デフォルト値は1です。重みによって、接続先に送信されるトラフィックが決まります。トラフィックの重みベースの分散の例を以下に示します。

表 *3 : PBR* 接続先へのトラフィック（重みベースの対称 *PBR*）

Destination	重量	**Traffic %-age** （おおよその）
接続先 1	4	40
接続先 2	3	30
接続先 3	2	20
接続先 4	1	10



（注） 上記に示すトラフィックのパーセンテージ（25%、30%、10% など）の数値は示唆的なものであり、明確なものではありません。

サービス付加の対称 PBR を維持するには、各サービスノードがコンシューマーコネクタとプロバイダーコネクタの2つのインターフェイスを持ち、両方向、つまりコンシューマーからプロバイダーおよびプロバイダーからコンシューマーに同じ重みを設定するようにします。

重みベースの PBR の制限事項

ブリッジドメインの PBR 接続先では、PBR ポリシーごとの最大の重みは 128 です。L3Out の PBR 接続先の場合、PBR ポリシーごとの最大の重みは 64 です。

システム障害は、次の条件下で発生します。

- プライマリとバックアップの接続先の重みの合計が 128（または L3Out の場合は 64）を超える場合の動作障害。

- プライマリ接続先の重みの合計が 128（または L3Out の場合は 64）を超える場合の設定障害。
- バックアップ接続の重みの合計が 128（または L3Out の場合は 64）を超える場合の設定障害。

ポリシーベースのリダイレクトとハッシュアルゴリズム

（注） この機能は、APIC リリース 2.2(3x) リリースおよび APIC リリース 3.1 (1) で使用できます。APIC リリース 3.0(x) ではサポートされていません。

Cisco APIC、リリース 2.2(3x) では、ポリシー ベースのリダイレクト機能 (PBR) は、次のハッシュ アルゴリズムをサポートします。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元 IP アドレス、接続先 IP アドレス、プロトコル番号（デフォルト構成）。

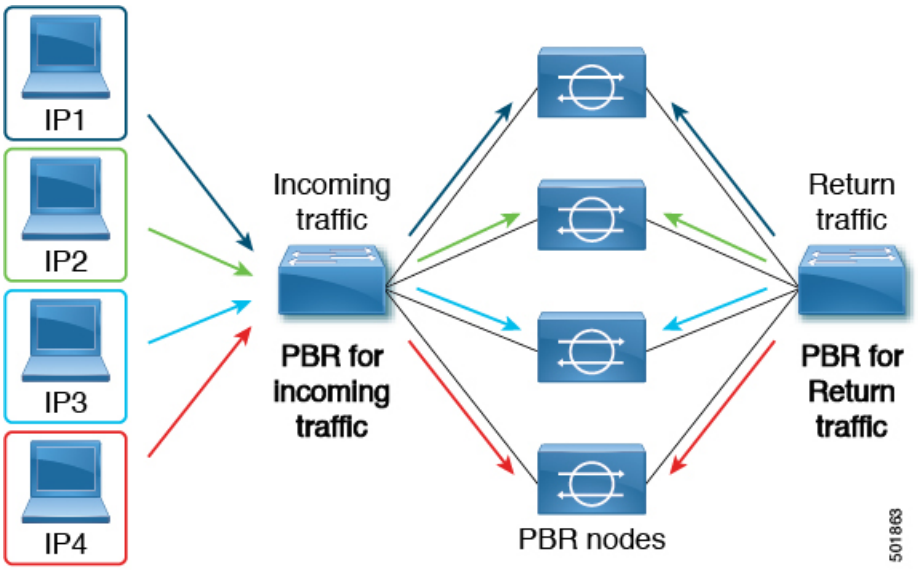
ポリシーベースのリダイレクトの修復性のあるハッシュ

対称 PBR では、着信と戻りユーザ トラフィックは、ECMP グループで同じ PBR ノードを使用します。ただし、PBR ノードのいずれかがダウンするか、障害を起こした場合には、既存のトラフィック フローは別のノードに送られて再ハッシュされます。これは、機能しているノードの既存のトラフィックが、現在の接続情報を持っていない他の PBR ノードに負荷分散のために送られるといったような問題の原因となります。トラフィックがステートフルファイアウォールを通過する場合には、接続がリセットされることにもつながります。

修復性のあるハッシュは、トラフィック フローを物理ノードへマッピングするプロセスで、障害の発生したノードからのフロー以外のトラフィックが再ハッシュされるのを避けられるようにします。障害を起こしたノードからのトラフィックは、「バックアップ」ノードに再マッピングされます。「バックアップ」ノード上の既存のトラフィックは移動できません。

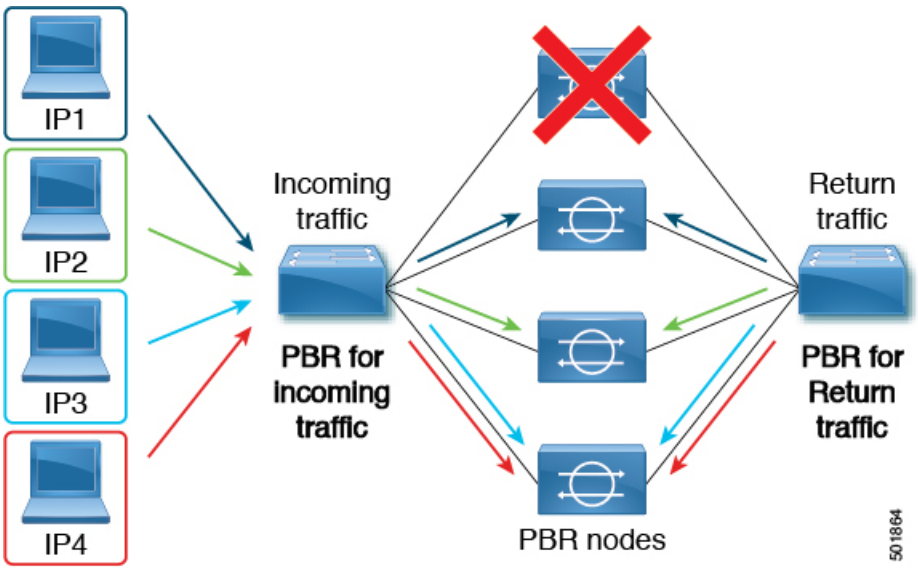
次の図は、着信と戻りユーザ トラフィックが同じ PBR ノードを使用している、対称 PBR の基本的な機能を示しています。

図 *15* : 対称 *PBR*



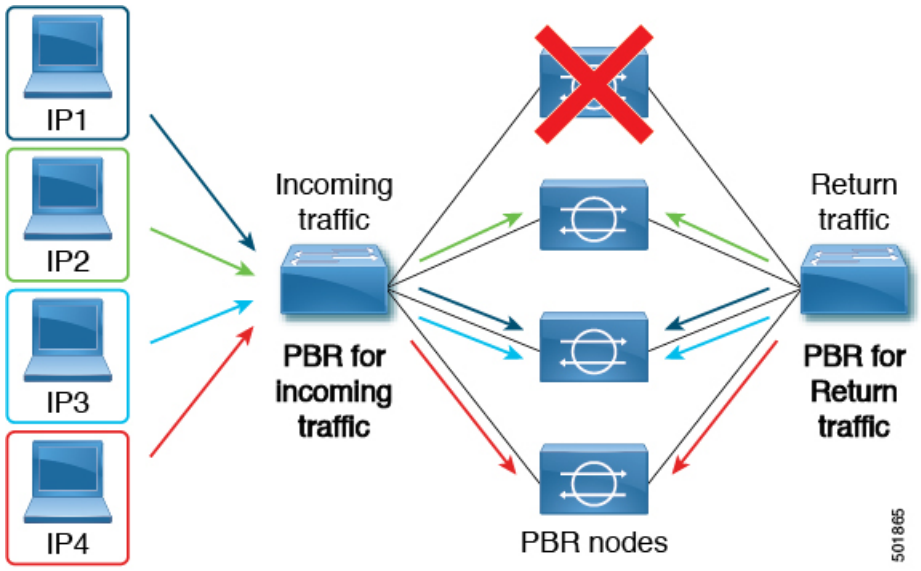
次の画像は、PBR ノードのいずれかが無効か、障害が発生したときに何が生じるかを示しています。IP1 のトラフィックは隣のノードへ再ハッシュされ、IP2 および IP3 のトラフィックがもう 1 つの PBR ノードに負荷分散されます。このことは、前述のように、他の PBR ノードが IP2 および IP3 トラフィックの現在の接続情報を持っていない場合、接続の中断や遅延という問題につながることがあり得ます。

図 *16* : 修復性のあるハッシュがない場合の無効化された/障害の発生した *PBR* ノード



最後の図は、修復性のあるハッシュが有効になっている場合に、この同じ使用例がどのように対処されるかを示しています。無効化された/障害の発生したノードからのユーザ トラフィックだけが移動されます。その他のすべてのユーザ トラフィックは、それぞれの PBR ノードに残ります。

図 *17* : 修復性のあるハッシュがある場合の無効化された/障害の発生した *PBR* ノード



ノードがサービス可能状態に戻ると、障害の発生したノードからアクティブなノードに再ハッシュされたトラフィック フローは、再度アクティブ化されたノードに戻ります。

（注） ECMP グループの PBR ノードを追加または削除すると、すべてのトラフィック フローが再ハッシュされる原因となることがあります。

L4 ～ L7 のポリシー ベース リダイレクトで復元力のあるハッシュを有効にする

始める前に

このタスクでは、L4-7 ポリシー ベースのリダイレクト ポリシーが作成されたことを前提としています。

ステップ 1 メニュー バーで、**Tenants** > **All Tenants** の順に選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ウィンドウで、**Tenant** ***tenant_name*** > **Policies** > **Protocol** > **L4-L7 Policy Based Redirect** > ***L4-L7_PBR_policy_name*** を選択します。

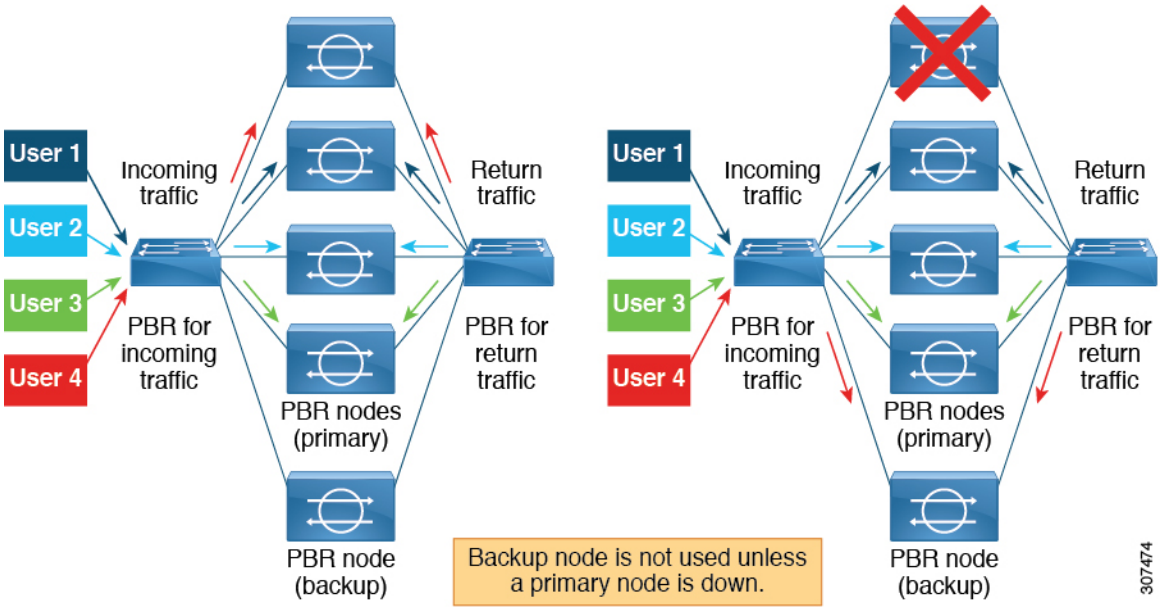
ステップ 4 Work ペインで、**Resilient Hashing Enabled** チェック ボックスをオンにします。

ステップ 5 [送信（Submit）] をクリックします。

PBR バックアップポリシーについて

Cisco APIC リリース 4.2(1) より前のリリースでは、PBR ポリシー内のすべてのポリシーベースリダイレクト (PBR) 接続先は、PBR 接続先が機能している限り使用されます。PBR ノードの 1 つで障害が発生すると、既存のトラフィックフローが再ハッシュされます。これにより、たとえば、データパスがステートフルファイアウォールを通過している場合に、接続がリセットされる可能性があります。復元力のあるハッシュの PBR では、障害が発生したノードを通過したトラフィックのみが使用可能なノードの 1 つに転送されるため、新しく共有されるノードのトラフィックが過負荷になる可能性があります。使用可能なノードの 1 つを共有する代わりに、グループ内のバックアップノードを構成して使用して、トラフィックの負荷を吸収することができます。PBR バックアップポリシーごとに複数のバックアップ PBR 接続先を構成できます。

Cisco APIC リリース 4.2(1) 以降のリリースでは、新しい PBR バックアップポリシー オプションが利用できます。



復元力のあるハッシュでは、障害が発生したノードを通過したトラフィックのみが、使用可能なノードの 1 つに再ルーティングされます。復元力のあるハッシュと PBR バックアップポリシーを使用すると、障害が発生したプライマリノードを通過したトラフィックは、使用可能なバックアップノードの 1 つに再ルーティングされます。

バックアップポリシーの注意事項と制限事項

PBR バックアップポリシー オプションについては、次の注意事項と制限事項に従ってください。

- PBR バックアップポリシー オプションは、新世代リーフスイッチでのみサポートされます。これらのスイッチモデルでは、スイッチ名の最後に「-EX」、「-FX」、「-FX2」が付きます。
- 復元力のあるハッシュを有効にする必要があります。
- Cisco APIC リリース 5.0(1) 以降のリリースでは、レイヤ 1/レイヤ 2 PBR もバックアップポリシーをサポートしています。
- 接続先は、PBR 接続先またはバックアップ PBR 接続先として使用できますが、両方は使用できません（同じまたは異なる PBR ポリシーでは、プライマリ PBR 接続先を PBR ポリシーでバックアップ PBR 接続先としては使用できません）。
- 1 つのバックアップ PBR ポリシーは、1 つの PBR ポリシーでのみ使用できます。PBR ポリシーに 2 番目のバックアップポリシーを追加しようとすると、構成が拒否されます。

  複数の PBR ポリシーに同じバックアップ PBR 接続先を使用する場合は、同じバックアップ PBR 接続先を使用して 2 つの異なるバックアップ PBR ポリシーを作成します。これらの両方のポリシーの接続先には、同じヘルスグループが構成されている必要があります。
- Cisco APIC リリース 6.0(1) 以降のリリースでは、バックアップノードで重みベースの PBR を設定できます。プライマリノードがダウンしている場合、（障害が発生した）プライマリノードと同等またはそれ以上の重みを持つバックアップが使用されます。たとえば、プライマリノードの重みを 5 と考えると、プライマリノードの障害後に有効なバックアップノードの重みは 5 以上である必要があります。
- 復元力のあるハッシュと PBR バックアップ ポリシーの使用：
  - 障害が発生したノードを通過したトラフィックは、IP アドレスが小さい順に、PBR バックアップポリシーのバックアップノードに送信されます。複数のプライマリノードに障害が発生し、すべてのバックアップノードが使用されている場合、障害が発生したノードを通過したトラフィックは、プライマリノードとバックアップノードを含む使用可能なノードの 1 つに、IP アドレスの低い順にルーティングされます。たとえば、4 つのプライマリノード（192.168.1.1 ～ 192.168.1.4）と 2 つのバックアップノード（192.168.1.5 および 192.168.1.6）があるとします。
    - IP アドレス 192.168.1.1 のプライマリノードに障害が発生した場合、このノードを通過したトラフィックは、最小の IP アドレス 192.168.1.5 で使用できるバックアップノードにルーティングされます。
    - IP アドレス 192.168.1.1 と 192.168.1.2 の 2 つのプライマリノードに障害が発生した場合、192.168.1.1 を通過したトラフィックはバックアップノード 192.168.1.5 に、192.168.1.2 を通過したトラフィックはバックアップノード 192.168.1.6 にルーティングされます。
    - IP アドレス 192.168.1.1、198.168.1.2、192.168.1.3 の 3 つのプライマリノードに障害が発生し、192.168.1.5 のバックアップ ノードが 1 つだけ使用可能な場合、最初に障害が発生したノード 192.168.1.1 を通過したトラフィックは、バックアップノード 192.168.1.5 にルーティングされます。

- 2 番目に障害が発生したプライマリノード 192.168.1.2 の場合、バックアップノードが使用されている IP アドレス 192.168.1.1 と使用可能なプライマリノード 192.168.1.4 の IP アドレスを比較すると、192.168.1.1 は、最初に使用可能なプライマリノード 192.168.1.4 より小さいため、障害ノード 192.168.1.2 を通過したトラフィックは、バックアップノード 192.168.1.5 に再ルーティングされます。
- 3 番目に障害が発生したノード 192.168.1.3 では、バックアップノードがすでに使用されているため、3 番目に障害が発生したノードを通過したトラフィックは、使用可能なプライマリノード 192.168.1.4 にルーティングされます。

- ポッド認識 PBR が有効な場合、障害が発生したプライマリノードでは、障害が発生したノードを通過したトラフィックは、最初に使用可能なローカルバックアップノードに送られます。バックアップノードが使用できない場合は、ローカルプライマリノードが優先されます。すべてのローカルプライマリノードとローカルバックアップノードに障害が発生し、ローカルノードを使用できない場合、障害が発生したノードを通過したトラフィックは、リモートプライマリノードから、リモートバックアップノードに送られます。次に例を示します。
  - プライマリノードとバックアップノードの両方が同じポッドにあり、ポッド認識 PBR が有効な場合、ローカルポッドのプライマリノードで障害が発生すると、障害が発生したノードを通過したトラフィックは同じローカル Pod のバックアップノードに送られます。
  - ローカルプライマリノードとローカルバックアップノードがあり、ポッド認識 PBR が有効な場合、ローカルプライマリノードおよびローカルバックアップノードで障害が発生すると、障害が発生したノードを通過したトラフィックは、別のポッド内の異なるプライマリノードに移動します。

PBR バックアップポリシーの作成

ステップ 1 メニュー バーで、**Tenants** > **All Tenants** の順に選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーションウィンドウで、**[テナント（Tenant）]** > ***[テナント名（tenant_name）]*** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[L4 ～ L7 ポリシーベースリダイレクト バックアップ（L4-L7 Policy Based Redirect Backup）]** の順に選択します。

ステップ 4 [**L4 ～ L7 ポリシーベースリダイレクト バックアップ（L4-L7 Policy Based Redirect Backup**）] を右クリックし、[**L4 ～ L7 ポリシーベースリダイレクト バックアップの作成（Create L4-L7 Policy Based Redirect Backup**）] を選択します。

[**PBR バックアップポリシーの作成（Create PBR Backup Policy**）] ダイアログが表示されます。

ステップ 5 [**名前（Name**）] フィールドに、バックアップポリシーの一意の名前を入力します。

ステップ 6 [**L3 接続先（L3 Destinations**）] テーブルで、[+] をクリックします。

[**リダイレクトされたトラフィックの接続先の作成（Create Destination of Redirected Traffic**）] ダイアログが表示されます。

a) [**IP**] フィールドに、レイヤ 3 接続先ノードの IP アドレスを入力します。
b) [**MAC**] フィールドに、レイヤ 3 接続先ノードの MAC アドレスを入力します。
c) オプション：[**追加の IPv4/IPv6**] フィールドに、レイヤ 3 接続先ノードのセカンダリ IP アドレスを入力します。
d) [**ポッド ID（Pod ID**）] フィールドに値を入力します。デフォルト値は 1 です。
e) [**重み（Weight**）] フィールドに値を入力します。デフォルト値は 1 です。指定できる範囲は 1 ～ 10 です。

プライマリノードに障害が発生すると、重みに基づいてバックアップノードが割り当てられます。

f) [**リダイレクトヘルスグループ（Redirect Health Group**）] フィールドで、既存のヘルスグループを選択するか、新しいヘルスグループを作成します。

新しいリダイレクトヘルスグループ作成の詳細については、「GUI を使用したリダイレクトヘルスグループの設定 （142 ページ）」を参照してください。

g) [OK] をクリックします。

オプション：手順 a から手順 e を繰り返して、さらにレイヤ 3 接続先を追加します。

ステップ 7 [送信（Submit）] をクリックします。

PBR バックアップポリシーの有効化

始める前に

このタスクは、レイヤ 4 ～ レイヤ 7 ポリシーベースリダイレクト (PBR) ポリシーが作成されていることを前提としています。

ステップ 1 メニュー バーで、**Tenants** > **All Tenants** の順に選択します。
ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。
ステップ 3 ナビゲーションウィンドウで、**[テナント（Tenant）]** > ***[テナント名（tenant_name）]*** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[L4 ～ L7 ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）]** > ***[L4 ～ L7 PBR ポリシー名（L4-L7_PBR_policy_name）]*** の順に選択します。
ステップ 4 [**接続先タイプ（Destination Type**）] フィールドで、[**L3**] を選択します。
ステップ 5 [**IP SLA モニタリングポリシー（IP SLA Monitoring Policy**）] フィールドで、既存のポリシーを選択するか、モニタリング中に使用されるプローブを定義する新しい IP SLA モニタリング ポリシーを作成します。

新しい IP SLA モニタリングポリシーの作成の詳細については、「*Cisco APIC Layer 3* ネットワーキング設定ガイド」を参照してください。

ステップ 6 [**復元力のあるハッシュの有効化（Resilient Hashing Enabled**）] チェックボックスをオンにします。

ステップ 7 [**バックアップポリシー（Backup Policy**）] フィールドで、既存のポリシーを選択するか、新しいバックアップポリシーを作成します。

新しいバックアップポリシー作成の詳細については、「PBR バックアップポリシーの作成（110 ページ）」を参照してください。

ステップ 8 **L3 接続先**または **L1/L2 接続先**テーブルに少なくとも 1 つのアクティブな PBR 接続先が表示され、リダイレクトヘルスグループで構成されていることを確認します。

新しいリダイレクトヘルスグループ作成の詳細については、「GUI を使用したリダイレクトヘルスグループの設定 （142 ページ）」を参照してください。

ステップ 9 [送信（Submit）] をクリックします。

バイパスアクションについて

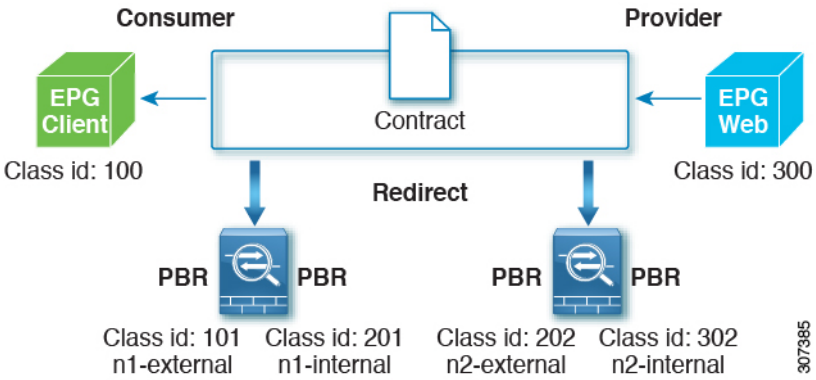
Cisco Application Policy Infrastructure Controller (APIC) リリース 4.1(2) より前のリリースでは、レイヤ 4 ～ レイヤ 7 サービスのポリシーベースリダイレクトを作成する場合にしきい値の有効化を選択すると、**拒否アクション**または**許可アクション**の 2 つのオプションしか使用できませんでした。

これらの 2 つのオプションを使用すると、マルチノード ポリシーベースリダイレクト グラフで、1 つのノードがしきい値の下限を下回ると、選択した 2 つのオプションに応じて、次のアクションが発生します。

- **拒否アクション**：このノードでのトラフィックがドロップされます。
- **許可アクション**：トラフィックは接続先に直接送信され、残りのサービスチェーンはスキップされます。

Cisco APIC リリース 4.1(2) 以降のリリースでは、新しい**バイパスアクション** オプションが利用可能になりました。このオプションを使用すると、マルチノードポリシーベースリダイレクトグラフで、1 つのノードがしきい値下限を下回っても、トラフィックは稼働しているかバイパスできない残りのサービスチェーンを介して通過できます。

次のセクションでは、この 2 ノードのポリシーベースリダイレクト グラフの例を使用して、これら 3 つのオプションによってトラフィックを処理する方法をそれぞれ説明します。



両方のノードが稼働している場合、この2ノードのポリシーベースリダイレクトは次のように動作します。

送信元 EPG	宛先 EPG	Action
100	300	PBR から n1-external
201	300	PBR から n2-external
302	300	permit
300	100	PBR から n2-internal
202	100	PBR から n1-internal
101	100	permit

次のセクションでは、[**しきい値ダウンアクション（Threshold Down Action）**]フィールドで選択したオプションに基づいて、最初のノードがダウンしたときに2ノードのポリシーベースリダイレクトがどのように動作するかについて説明します。

拒否(deny action)

上記の設定例で、[**しきい値ダウンアクション（Threshold Down Action）**]フィールドで**拒否アクション**を選択し、最初のノードがダウンすると、次の表のように最初のノードを使用するPBR ポリシーが「ドロップ（Drop）」に更新され、クライアント EPG と Web EPG 間の通信がドロップします。

送信元 EPG	宛先 EPG	Action
100	300	**削除（Drop）**
201	300	PBR から n2-external
302	300	permit
300	100	PBR から n2-internal
202	100	**削除（Drop）**

送信元 EPG	宛先 EPG	Action
101	100	permit

許可(permit action）

上記の設定例で、[**しきい値ダウンアクション（Threshold Down Action**）] フィールドで **許可** アクションを選択し、最初のノードがダウンすると、最初のノードを使用する PBR ポリシーが「許可」に更新されます。クライアント EPG から Web EPG（100 から 300）へのトラフィックは、サービスノードを介さずに直接通過します。Web EPG からクライアント EPG（300 から 100）へのリターントラフィックは、次の表に示すように、n2-internal にリダイレクトされます。ただし、非対称フローであるため、2 番目のノードはパケットがドロップされる可能性があります。

送信元 EPG	宛先 EPG	Action
100	300	**Permit**
201	300	PBR から n2-external
302	300	permit
300	100	PBR から n2-internal
202	100	**Permit**
101	100	permit

バイパス（bypass action）

Cisco APIC リリース 4.1(2) 以降のリリースでは、[**しきい値ダウンアクション（Threshold Down Action**）] フィールドで新しい**バイパスアクション** オプションを選択し、最初のノードがダウンすると、最初のノードを使用する PBR ポリシーが「PBR から次のデバイス（PBR to next device）」に更新されます。この場合、次のようになります。

- クライアント EPG から Web EPG（100 から 300）へのトラフィックは、n2-external にリダイレクトされます。
- Web EPG からクライアント EPG（300 から 100）へのリターントラフィックは、n2-internal にリダイレクトされます。
- n2-external からコンシューマーへのリターントラフィックは「許可」に設定されます。

送信元 EPG	宛先 EPG	Action
100	300	**PBR から n2-external**
201	300	PBR から n2-external
302	300	permit

送信元 EPG	宛先 EPG	Action
300	100	PBR から n2-internal
202	100	**Permit**
101	100	permit

ガイドラインと制約事項

バイパスアクション オプションの注意事項と制限事項は次のとおりです。

- **バイパスアクション** オプションは、新世代 ToR スイッチでのみサポートされます。これらのスイッチモデルでは、スイッチ名の最後に「EX」、「FX」、「FX2」が付きます。
- **バイパスアクション**オプションは、1 ノードサービスグラフでは必要ありません。この場合、バイパスが設定されていれば転送アクションは許可アクションと同じになります。
- L3Out EPG と通常の EPG は、コンシューマー EPG またはプロバイダー EPG にできます。
- NAT が有効のサービスノードは、トラフィックフローが中断するためバイパスできません。
- 5.0(1) 以降のリリースでは、レイヤ 1/レイヤ 2 PBR はバイパスアクションをサポートしています。
- 次の場合、**バイパスアクション** オプションはサポートされません。
  - ワンアームモードのレイヤ 4 ～ レイヤ 7 デバイス。
  - リモートリーフスイッチ。
- バイパスアクションが有効の場合は、複数のサービスグラフで同じ PBR ポリシーを使用しないでください。Cisco APIC では、バイパスアクションを持つ同じ PBR ポリシーが複数のサービスグラフで使用されている場合、設定は拒否されます。これを回避するには、同じ PBR 接続先 IP アドレス、MAC アドレス、ヘルスグループを使用する異なる PBR ポリシーを設定します。

ポリシーベースリダイレクトでのしきい値ダウンアクションの設定

始める前に

このタスクは、レイヤ 4 ～ レイヤ 7 サービス ポリシーベースリダイレクト (PBR) ポリシーが作成されていることを前提としています。

ステップ 1 メニュー バーで、**Tenants** > **All Tenants** の順に選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーションウィンドウで、**[テナント（Tenant）]** > ***[テナント名（tenant_name）]*** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[L4 ～ L7 ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）]** > ***[L4 ～ L7 PBR ポリシー名（L4-L7_PBR_policy_name）]*** の順に選択します。

ステップ 4 **[接続先タイプ（Destination Type）]** フィールドで、**[L3]** を選択します。

ステップ 5 **[IP SLA モニタリングポリシー（IP SLA Monitoring Policy）]** フィールドで、既存のポリシーを選択するか、モニタリング中に使用されるプローブを定義する新しい IP SLA モニタリング ポリシーを作成します。

新しい IP SLA モニタリングポリシーの作成の詳細については、「*Cisco APIC Layer 3* ネットワーキング設定ガイド」を参照してください。

ステップ 6 **[しきい値有効（Threshold Enable）]** チェックボックスをオンにします。

次のフィールドが表示されます。

- 最小しきい値のパーセンテージ (%)
- 最大しきい値のパーセンテージ (%)
- しきい値ダウン時のアクション

ステップ 7 最小しきい値および最大しきい値をパーセンテージ (%) で指定します。

最小しきい値と最大しきい値の詳細については、「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 （139 ページ）」を参照してください。

ステップ 8 **[しきい値ダウン時のアクション（Threshold Down Action）]** エリアで、しきい値ダウン時のアクションを選択します。

次のオプションがあります。

- **バイパス（bypass action）**
- **拒否(deny action）**
- **許可(permit action）**

ステップ 9 [送信（Submit）] をクリックします。

L3Out によるポリシーベースリダイレクト

Cisco Application Policy Infrastructure Controller (APIC) リリース 4.1(2) 以降のリリースでは、L3Out を使用して、サービスグラフの一部であるレイヤ 4 ～ レイヤ 7 サービスデバイスに接続できます。ポリシーベースリダイレクト (PBR) サービスグラフの一部として L3Out を使用するには、複数の方法があります。

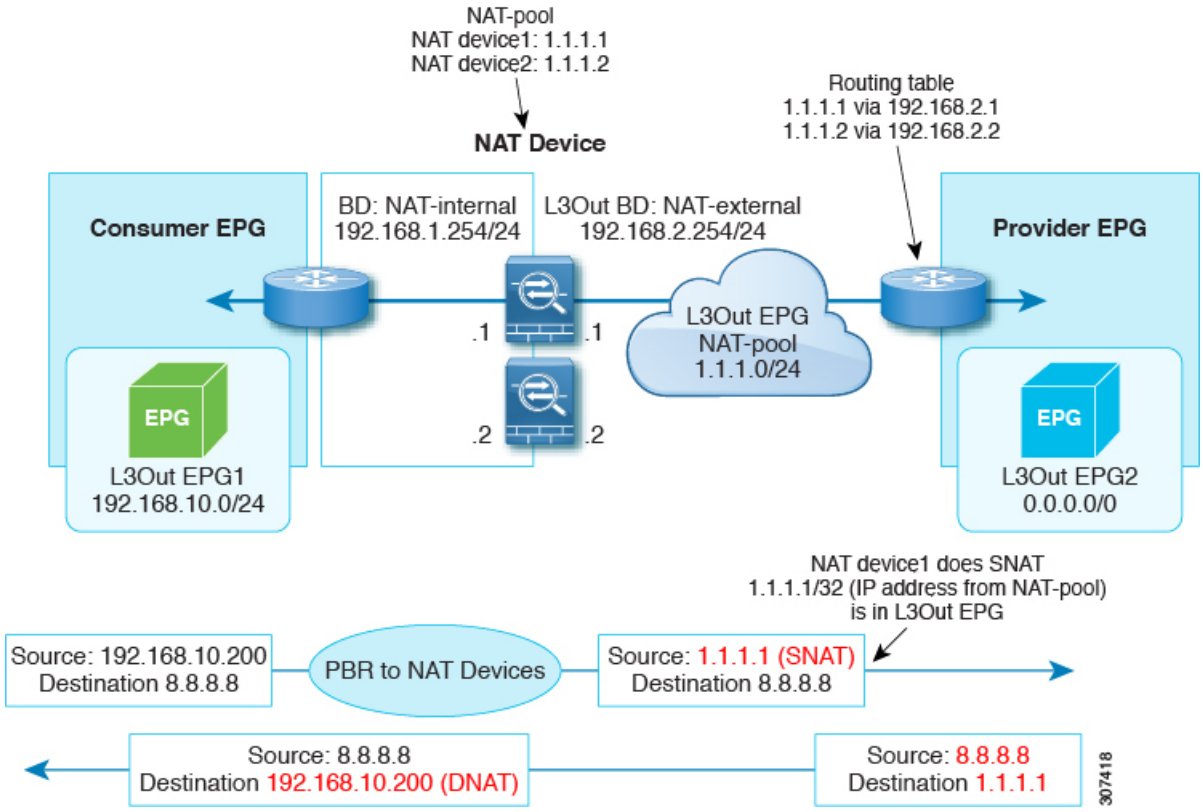
- PBR を使用すると、レイヤ 4 ～ レイヤ 7 サービスデバイスのコンシューマーインターフェイスのみにリダイレクトし、レイヤ 4 ～ レイヤ 7 サービスデバイスのプロバイダー インターフェイスは L3Out に接続します。これは、PBR がトラフィックの一方向に対してのみ

実行されるため、「単方向」PBR と呼ばれます。このオプションは Cisco APIC リリース 4.1(2) で導入されました。

- PBR を使用すると、レイヤ 4 ～ レイヤ 7 サービスデバイスのプロバイダー インターフェイスのみにリダイレクトし、レイヤ 4 ～ レイヤ 7 サービスデバイスのコンシューマー インターフェイスは L3Out に接続します。このオプションは Cisco APIC リリース 5.0(1) で導入されました。これも単方向 PBR 設計であり、前に箇条書きで説明したものの対称設計です。
- PBR を使用して、L3Out に接続されているレイヤ 4 ～ レイヤ 7 サービスデバイス インターフェイスにリダイレクトします。このオプションは Cisco APIC リリース 5.2(1) で導入されました。

これらのユースケースについては、以下のテキストで詳しく説明されています。

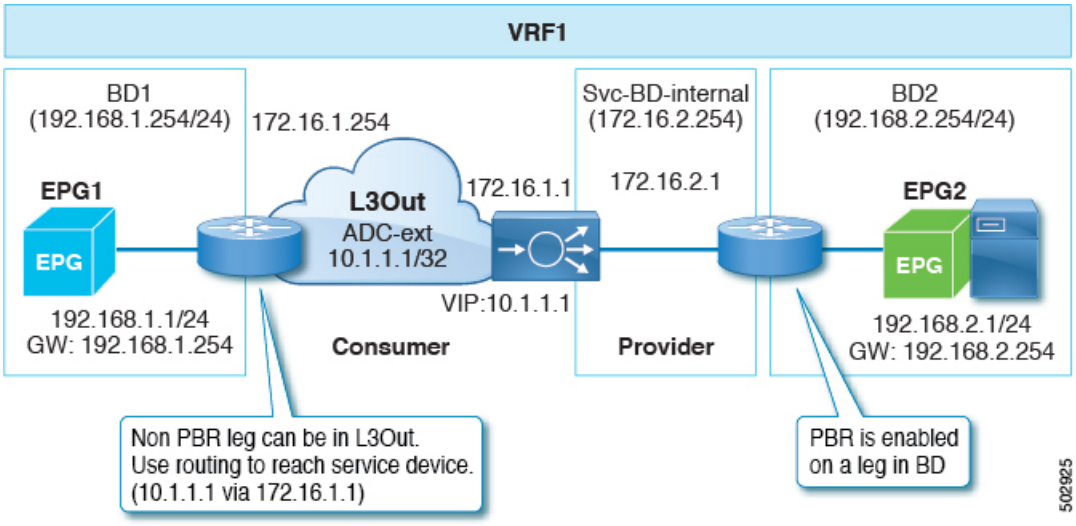
最初の箇条書きで述べたように、Cisco APIC リリース 4.1(2) 以降のリリースでは、次の図に示すように、コンシューマー インターフェイスに単方向 PBR を設定し、プロバイダー インターフェイスを L3Out に接続できます。



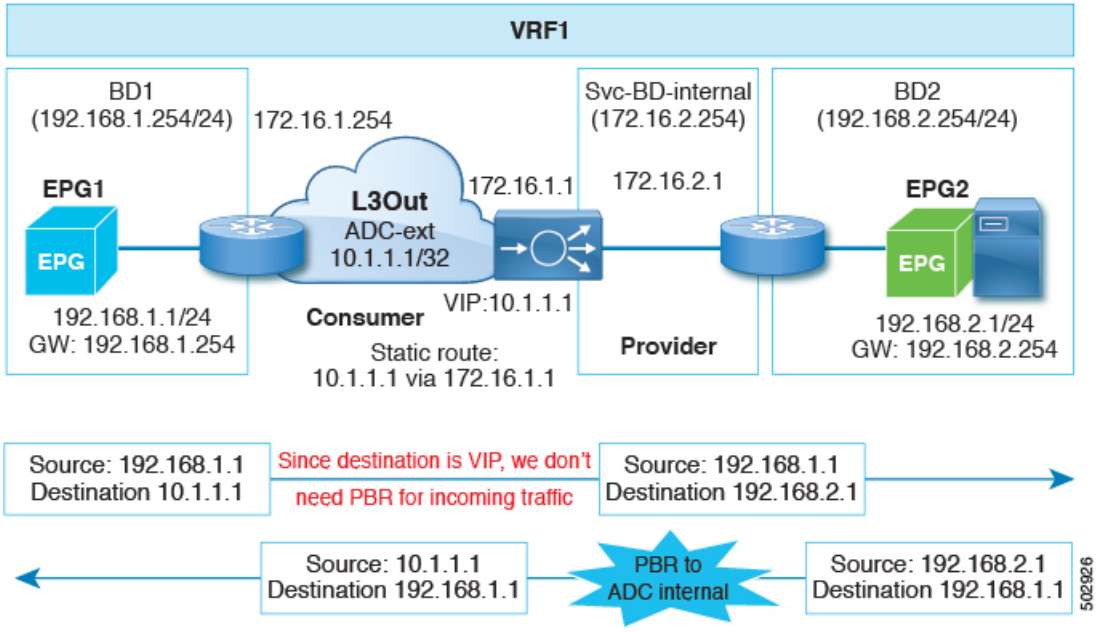
この例では、ブリッジドメインのコンシューマーコネクタで PBR が有効になっていますが、L3Out のプロバイダーコネクタでは PBR が有効になっていません。この設計は、L3Out が最後のサービスノードのプロバイダーコネクタである場合にのみサポートされます。Cisco APIC 4.1(2) より前のリリースでは、トラフィックをサービスグラフのノードにリダイレクトするように PBR が設定されていると、単方向 PBR の場合でもレイヤ 4 ～ レイヤ 7 サービスデバイス

のコンシューマーコネクタとプロバイダーコネクタの両方がブリッジドメインに存在する必要がありました。

Cisco APIC リリース 5.0(1) 以降のリリースでは、L3Out がプロバイダーコネクタまたはコンシューマーコネクタであるかどうか、L3Out が最後のノードであるかどうかにかかわらず、単方向 PBR は L3Out 内の他のコネクタでサポートされます。これには、次の図に示すようにロードバランサがサービスノードのコンシューマー側のローカルサブネットの外部に VIP アドレスを持っている場合も含まれます。

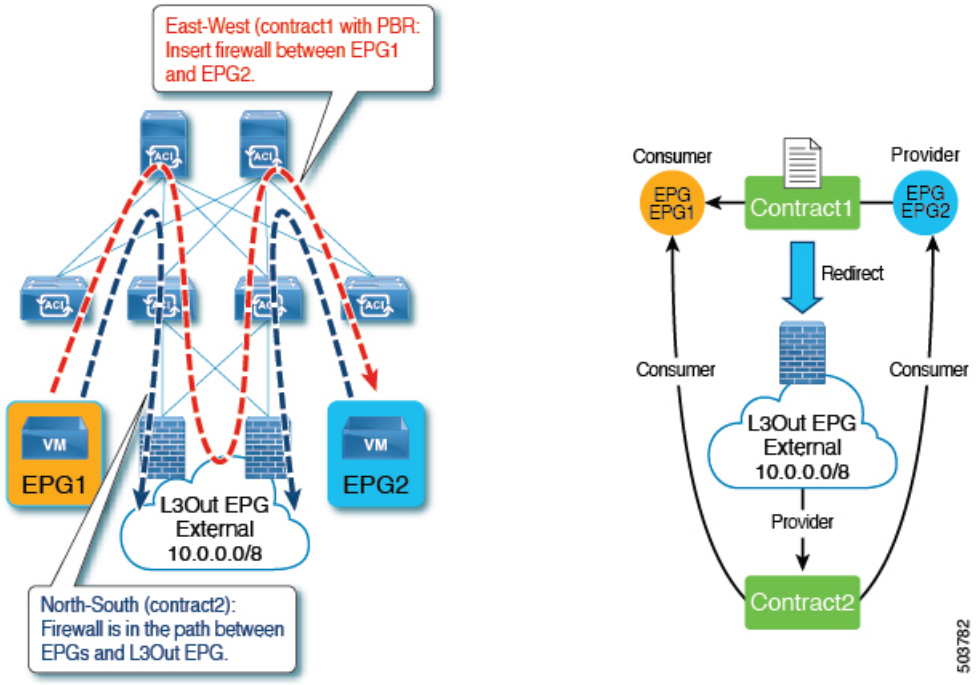


次の図の例では、コンシューマーエンドポイントから VIP アドレスへの着信トラフィックは、ルーティングテーブルに基づいて、L3Out に接続されているロードバランサに転送されます。次に、トラフィックはプロバイダーのエンドポイントに転送されます。プロバイダーエンドポイントからコンシューマーエンドポイントへのリターントラフィックは、PBR により、サービスノードのプロバイダー側にリダイレクトされます。

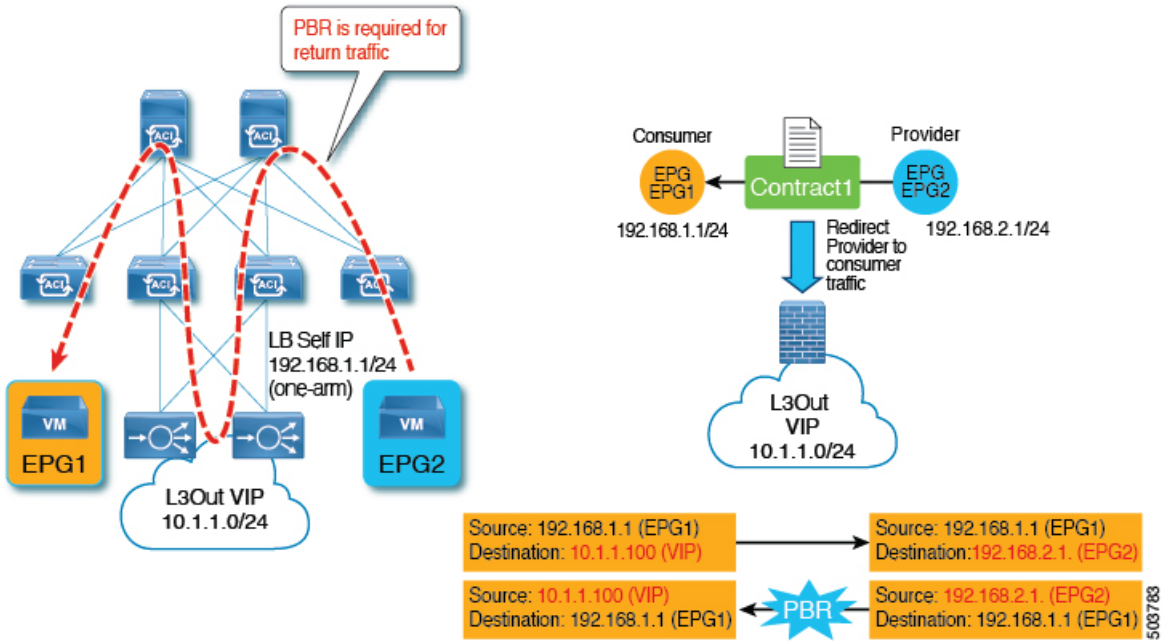


Cisco APIC リリース 5.2(1) 以降のリリースでは、PBR ポリシーの接続先として使用されるレイヤ 4 ～ レイヤ 7 サービスデバイスは、L3Out にインターフェイスを持つことができます。これより前のリリースでは、PBR ポリシーの接続先インターフェイスはブリッジドメインのみにありました。一般的な導入例には次のものもあります。

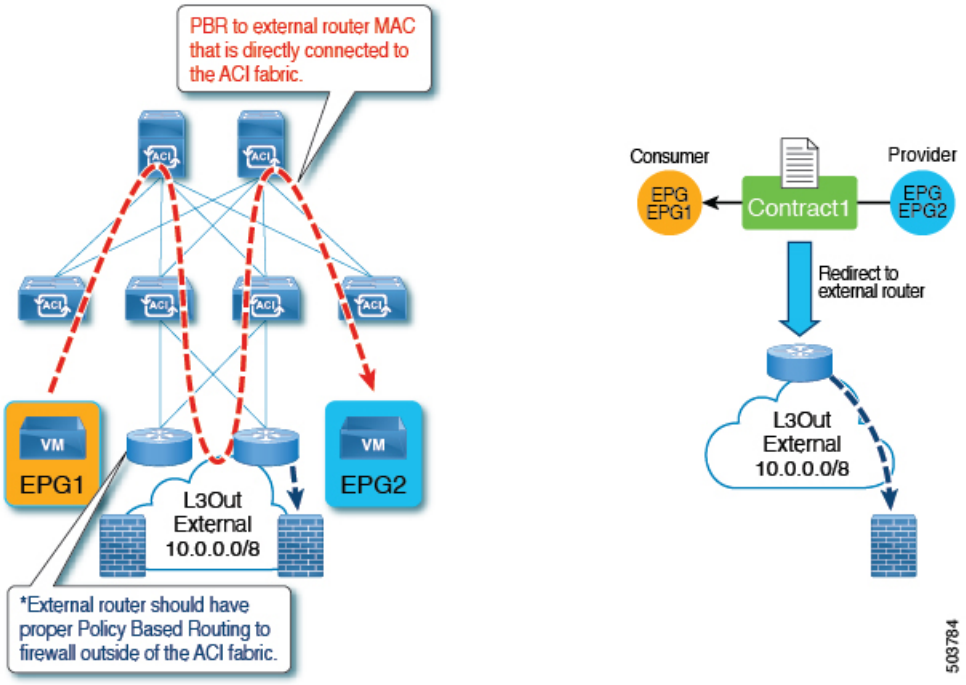
- 水平方向のトラフィックと垂直方向のトラフィックの両方に同じファイアウォールを使用できます。この場合、ファイアウォールの内部レッグは Cisco Application Centric Infrastructure (ACI) ファブリックに接続されていますが、ファイアウォールの外部レッグは Cisco ACI ファブリックの外部にあります。



- ローカルサブネットの外部にある VIP アドレスを持つワンアームロードバランサを持てます。この場合、VIP アドレスは、ロードバランサのセルフ IP アドレスサブネットの外部にあります。ロードバランサはソースネットワークアドレス変換 (SNAT) を実行しないため、リターントラフィックには PBR が必要です。



- 外部ファイアウォールなど、Cisco ACI に直接接続されていないデバイスにトラフィックを再ルーティングできます。



L3Out によるポリシーベースリダイレクトの注意事項と制限事項

次の注意事項と制限事項は、L3Out を使用したポリシーベースリダイレクト (PBR) に関するものです。

- ワンアームモードとツーアームモードの両方がサポートされています。
- ブリッジドメインの PBR とサービスグラフの同じ機能ノードの L3Out の PBR を混在させることはできません。次に例を示します。
  - N1 のコンシューマーコネクタを BD1（PBR は有効）に構成し、N1 のプロバイダーコネクタを L3Out1（PBR は有効）に構成することはできません。
  - ただし、N1 のコンシューマーコネクタを BD1（PBR は無効）に構成し、N1 のプロバイダーコネクタを L3Out1（PBR は無効）に構成できます。
- スイッチ仮想インターフェイス (SVI)、ルーテッド サブインターフェイス、またはルーテッドインターフェイスを使用した L3Out がサポートされています。
- PBR 接続先にフローティング SVI を使用するインフラ L3Out、GOLF L3Out、SDA L3Out、L3Out を使用することはできません。
- 同じ VRF インスタンスに他の L3Out EPG がある場合は、特定の L3Out EPG サブネットを使用します。そうしないと、他の L3Out が誤って EPG の分類に使用される可能性があります。

- 0.0.0.0/0 または 0::0 の L3Out EPG は、PBR 接続先の L3Out EPG には使用できません。これは、水平方向のトラフィックを自動的に作成されたサービス EPG で分類する必要があるためです。したがって、L3Out EPG が 0.0.0.0/0 で設定されている場合、水平方向のトラフィックは外部からのトラフィックとして分類されます。
- サービスデバイスが ツーアームモードで、サービスデバイスコネクタの L3Out の 1 つが 0.0.0.0/0 または 0::0 を学習する場合、両方のアームを同じリーフスイッチまたは同じ vPC ペアに接続する必要があります。
- コンシューマー/プロバイダー EPG が L3Out EPG の場合、PBR 接続先の L3Out が存在するサービスリーフスイッチの下に配置することはできません。これはハードウェアの制限です。
  - リーフスイッチは、特定の L3Out EPG サブネットを使用している場合でも、パケットがコンシューマー/プロバイダー L3Out EPG からのものか、サービスデバイスから戻ったものなのかを判断できません。

    コンシューマー/プロバイダー EPG が L3Out EPG ではなく通常の EPG の場合、コンシューマー、プロバイダー、サービスデバイスの L3Out は同じリーフスイッチの下に配置できます。
- L3Out の背後のサービスデバイスを使用してツーアームモードで PBR を展開し、ネクストホップ接続に OSPF または EIGRP プロトコルを使用する場合、両方のアームを同じサービスリーフスイッチに展開することはサポートされていません。各アームを異なるサービスリーフスイッチに展開することができます。
- ツーアームモードで PBR を展開し、OSPF、EIGRP、BGP プロトコルを使用してサービスノード L3Out を展開する場合、各アームでサービスデバイスのネクストホップを適切に制御する必要があります。
- 次の表に、サポートされるコンシューマー/プロバイダー EPG タイプの組み合わせまとめます。

表 *4*：サポートされるコンシューマー/プロバイダー *EPG* タイプの組み合わせ

コンシューマー/プロバイダー	EPG	L3Out	ESG
EPG	サポート対象	サポート対象	サポート対象外[1]
L3Out	サポート対象	サポート対象	サポート対象
ESG	非対応	サポートあり	サポート対象

[1] EPG 間のコントラクトは、サービスグラフがなくてもサポートされません。

- PBR を使用した EPG/ESG/L3Out EPG 内コントラクトがサポートされています。
  - リリース 5.2(1) 以降のリリースでは、L3Out EPG 内コントラクトがサポートされています。

- ブリッジドメインで PBR でサービスグラフを使用する場合、Cisco ACI ではサービス *EPG* と呼ばれる非表示の EPG が自動的に作成されます。Cisco ACI は、サービス EPG とユーザーが作成した EPG の間のコントラクトを設定して、サービスグラフによって定義されたトラフィックパスを許可します。レイヤ 4 ～レイヤ 7 サービスデバイスインターフェイスを L3Out に接続し、このインターフェイスをサービスグラフの PBR 接続先として使用すると、Cisco ACI によってサービス EPG が自動的に作成されますが、管理者はサービス EPG に加えて L3Out EPG も作成する必要があります。一部のトラフィックは PBR を使用してレイヤ 4 ～ レイヤ 7 インターフェイスに転送されますが、ロードバランサによるキープアライブなどの他のトラフィックは、通常のトラフィック転送（ルーティング）を使用して送信する必要があります。ロードバランサのキープアライブの場合に必要なように、レイヤ 4 ～ レイヤ 7 サービスデバイスで使用される L3Out EPG とエンドポイントがある EPG 間の通信を有効にするには、**ダイレクトコネクト**を設定し、L3Out EPG とサーバーがある EPG 間のコントラクトも設定する必要があります。

- コンバージェンスを向上させるため、L3Out の PBR 接続先にはトラッキングが必須です。

- ブリッジドメインの PBR 接続先にも適用できるワンアームモードでは、バイパス機能はサポートされていません。

- マルチノード PBR がサポートされています。

- アクティブ/アクティブ対称 PBR がサポートされています。

- トラッキング、しきい値ダウンアクションがサポートされています。

- 復元力のあるハッシュがサポートされています。

- N+M 冗長性がサポートされています。

- 単一のポッド、Cisco ACI マルチポッド、リモートリーフスイッチがサポートされています。

- Cisco ACI マルチサイト はサポートされていません。

- エンドポイントセキュリティ グループ (ESG) のない VRF 間コントラクトで、PBR L3Out の接続先がプロバイダー VRF インスタンスにある場合：

  - サービスデバイスによって使用される L3Out EPG サブネットをコンシューマー VRF インスタンスにリークする必要があります。そうしないと、コンシューマー VRF インスタンスには PBR 接続先へのルートがなく、プロバイダー VRF インスタンスにはプロバイダー VRF インスタンスの PBR 接続先からコンシューマー EPG へのトラフィックに対する許可ルールがありません。PBR 接続先がブリッジドメインにある場合、PBR 接続先のサービスブリッジドメインをコンシューマー VRF インスタンスにリークする必要はありません。

- PBR の有無による ESG から L3Out、ESG 間に対する ESG による VRF 内コントラクト：

  - コンシューマー ESG または L3Out サブネットをプロバイダー VRF インスタンスにリークし、プロバイダー ESG または L3Out サブネットをコンシューマー VRF インスタンスにリークする必要があります。さらに、PBR を使用している場合：

- PBR 接続先がブリッジドメインにある場合、サービスデバイスサブネットをリークする必要はありません。
- L3Out の PBR 接続先が L3Out EPG がコンシューマーまたはプロバイダー VRF インスタンスにあるかどうかにかかわらず、サービスデバイスが使用する L3Out EPG サブネットを他の VRF インスタンスにリークする必要があります。

- L3Out EPG サブネットをリークするには、サブネットのプロパティを変更し、**共有ルート制御サブネット**と**共有セキュリティ インポートサブネット**を有効にします。また、必要に応じて**集約共有ルート**を有効にします。
- 内部 VRF インスタンスは、PBR 接続先への L3Out を持つボーダーリーフスイッチ上に作成されます（VRF は同じテナントの下に作成されます）。内部 VRF インスタンスは、PBR ポリシーの PBR 接続先ごとに作成されます。
  - たとえば、PBR-policy1 に 3 つの接続先がある場合、PBR ポリシーに 3 つの VRF インスタンスが 作成されます。複数のコントラクトで PBR-policy1 を再利用する場合、3 つの VRF インスタンスのみが作成されます。
  - コンシューマー/プロバイダーのリーフスイッチには VRF スケールの影響はありません。
- L3Out がコンシューマーまたはプロバイダーのいずれかの VRF インスタンスに属していることを確認します。

GUI を使用した L3Out によるポリシーベースリダイレクトの設定

L3Out を使用したポリシーベースリダイレクト (PBR) の構成手順は、一部の相違点を除き、通常のポリシーベースリダイレクト構成とほとんど同じです。

始める前に

必要なテナント、VRF インスタンス、EPG、EPG のブリッジドメイン、サービスブリッジドメインを作成します。

ステップ 1 レイヤ 4 ～ レイヤ 7 デバイスの作成PBR の接続先が L3Out にある場合、具象インターフェイスの場合、パスは L3Out 論理インターフェイスで使用されるパスと一致する必要があります。

「GUI を使用したレイヤ 4 ～ レイヤ 7 サービスデバイスの設定 （10 ページ）」を参照してください。

L3Out とピアリングするレイヤ 4 ～レイヤ 7 のサービス仮想アプライアンスと組み合わせて L3Out で PBR を使用する場合、具体的なデバイス構成の一部として仮想化ホストインターフェイスのパスを構成する必要があります。レイヤ 4 ～ レイヤ 7 サービスの具象デバイス設定で使用されるパスと、L3Out 設定で使用されるパスは一致する必要があります。これは、フローティング L3Out 機能がまだサービスグラフに統合されていないためです。したがって、Cisco Application Centric Infrastructure (ACI) にはパス情報を設定する必要があります。

ステップ 2 サービス グラフ テンプレートを作成します。

GUI でサービスグラフテンプレートを構成する （51 ページ）を参照してください。

ステップ 3 IP SLA モニタリング ポリシーの設定

次のサイトで、「*Cisco APIC Layer 3* ネットワーキング設定ガイド」 の IP SLA に関する章を参照してください。

https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

ステップ 4 PBR ポリシーを作成します。

「GUI を使用したポリシー ベース リダイレクトの設定 （95 ページ）」を参照してください。

トラッキングを有効にするには、リダイレクトヘルスグループを設定する必要があります。「GUI を使用したリダイレクトヘルスグループの設定 （142 ページ）」を参照してください。

ステップ 5 L3Out と L3Out EPG（または外部 EPG）を作成します。

0.0.0.0/0 は使用せず、ファイアウォールまたはロードバランサのサブネットアドレスと、外部トラフィックのサブネットを必ず含めてください。

次のサイトで、「*Cisco APIC Layer 3* ネットワーキング設定ガイド」を参照してください。

https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

ステップ 6 デバイス選択ポリシーを作成します。

「GUI を使用したデバイス選択ポリシーの作成 （41 ページ）」を参照してください。

手順に従って、次のサブステップを必要に応じて置き換えます。

a) [**関連付けられたネットワーク（Associated Network）**]ボタンで、[**ブリッジドメイン（Bridge Domain）**] または [**L3Out**] を選択します。

PBR ポリシーの接続先が L3Out のインターフェイスである場合は、[**L3Out**] を選択する必要があります。

b) [**ブリッジドメイン（Bridge Domain）**] を選択した場合は、[**ブリッジドメイン（Bridge Domain）**] ドロップダウンリストで、ターゲットインターフェイスのブリッジドメインを選択します。[**L3Out**] を選択した場合は、[**L3Out**] ドロップダウンリストで、ターゲットインターフェイスの L3Out EPG を選択します。

c) 必要に応じて、[**L4 ～ L7 ポリシーベースリダイレクト（L4-L7 Policy-Based Redirect）**] ドロップダウンリストで、適切な PBR ポリシーを選択します。

PBR ポリシーの接続先が L3Out のインターフェイスである場合は、PBR ポリシーを選択する必要があります。

d) 必要に応じて、デバイス選択ポリシーの残りの部分を設定します。

ステップ 7 サービスグラフをコントラクトに付加したサービスグラフを適用します。

「GUI を使用したエンドポイント グループへのサービス グラフ テンプレートの適用 （53 ページ）」を参照してください。

コンシューマとプロバイダ ブリッジ ドメイン内のサービス ノードへの PBR によるサポート

Cisco APIC 3.1(1) リリース以降、コンシューマやプロバイダを含むブリッジ ドメイン (BD) は、サービス ノードもサポートするようになりました。したがって今後は、別の PBR ブリッジ ドメインをプロビジョニングする必要はありません。

Cisco Nexus 9300-EX と 9300-FX プラットフォームのリーフ スイッチは、この機能をサポートします。

レイヤ 1/レイヤ 2 ポリシーベースリダイレクトについて

レイヤ 1 デバイスの使用は、通常、インラインモードまたは有線モードと呼ばれ、サービスデバイスがレイヤ 2 またはレイヤ 3 転送に関与していないセキュリティ機能を実行することが予想される場合、ファイアウォールと侵入防御システム (IPS) に使用されます。

レイヤ2デバイスの使用は、通常、透過モードまたはブリッジモードと呼ばれ、ファイアウォールおよび IPS に使用されます。

レイヤ3デバイスの使用は、通常、ルーテッドモードと呼ばれ、ルータファイアウォールおよびロードバランサに使用されます。

Cisco Application Policy Infrastructure Controller (APIC) リリース 4.1 より前のリリースでは、PBR は、レイヤ 3 デバイス (Go-To) モードでのみ設定されたレイヤ 4 ～ レイヤ 7 サービスデバイスにトラフィックをリダイレクトするように設定できました。レイヤ 4 ～ レイヤ 7 サービスデバイスが、透過ファイアウォールなどのレイヤ 1 またはレイヤ 2 デバイスである場合、PBR は使用できませんでした。サービスグラフを使用し、レイヤ 4 ～ レイヤ 7 サービスデバイスを**透過（Go-Through）**モードで定義することで、レイヤ 1 またはレイヤ 2 モードで動作するレイヤ 4 ～ レイヤ 7 サービスデバイスのみを展開できました。

Cisco APIC リリース 4.1 以降のリリースでは、レイヤ 1/レイヤ 2 デバイスモードで設定されたレイヤ 4 ～ レイヤ 7 サービスデバイスにトラフィックをリダイレクトするように PBR を設定することもできます。PBR は、ルーテッドモードのファイアウォールに加えて、インライン IPS または透過ファイアウォールで使用できます。

レイヤ 1/レイヤ 2 PBR 機能の一部として、Cisco APIC は、リンクレイヤをトラッキングするためにレイヤ 2 ping パケットを使用してレイヤ 4 ～ レイヤ 7 サービスデバイスがトラフィックを転送しているかどうかを確認できます。

非 IP アドレストラフィックも転送できる **透過（Go-Through）** モードとは異なり、レイヤ 1/レイヤ 2 PBR は IP アドレストラフィックにのみ適用されます。

レイヤ 1/レイヤ 2 PBR 設定の概要

次のリストは、主要なレイヤ 1/レイヤ 2 PBR 設定の概念の一部をまとめたものです。

- デバイスレイヤ 1/レイヤ 2 PBR でレイヤ 4 ～ レイヤ 7 サービスデバイスを展開する場合、コンシューマー側とプロバイダー側の 2 つのブリッジドメインを設定する必要がありますが、通常の PBR とは異なり、これらのブリッジドメインはエンドポイント（コンシューマーまたはプロバイダー）に設定されているブリッジドメインと同じにできません。
- サービスブリッジドメインは、ユニキャストルーティングが有効になっている必要があります。
- 物理レイヤ 4 ～ レイヤ 7 サービスデバイスは、個々のリンクまたは VPC を使用してリーフスイッチに接続できます。
- レイヤ 1 デバイスでは、コンシューマー側の VLAN とプロバイダー側の VLAN は同じですが、ブリッジドメインが異なります。したがって、レイヤ 4 ～ レイヤ 7 サービスデバイスのコンシューマー側とプロバイダー側は、異なる物理リーフに接続する必要があります。
- レイヤ 4 ～ レイヤ 7 サービスデバイスがレイヤ 1 またはレイヤ 2 デバイスとして設定されている場合、トラフィックを送受信するインターフェイスに IP アドレスがないため、接続先のリーフ/ポートおよび VLAN を入力することによってリダイレクトポリシーを定義します。
- リダイレクトポリシーの設定には、リーフ/ポートと VLAN の定義のみが必要で、MAC アドレスの入力はオプションです。MAC フィールドが空白の場合、Cisco Application Centric Infrastructure (ACI) は動的に 1 つの MAC アドレスを生成します。この MAC アドレスは、サービスブリッジドメイン上のレイヤ 4 ～ レイヤ 7 サービスデバイスに送信する際に、接続先 MAC アドレスを書き換えるために使用されます。これらの MAC アドレスは、レイヤ 4 ～ レイヤ 7 サービスデバイスの MAC アドレスではありません。これらは、Cisco ACI がトラフィックの接続先 MAC アドレスを書き換えるために使用する仮想 MAC アドレスです。
- レイヤ 4 ～ レイヤ 7 サービスデバイスがレイヤ 2 モードで展開されている場合、PBR がトラフィックを転送するために使用する MAC アドレスを、レイヤ 4 ～ レイヤ 7 サービスデバイスに転送するように静的に設定する必要があります。1 つの MAC アドレスは、サービスブリッジドメインで使用されるコンシューマーからプロバイダーへの接続先 MAC アドレスを識別し、もう 1 つの MAC アドレスは、他のサービスブリッジドメインで使用されるプロバイダーからコンシューマーへの接続先 MAC アドレスを定義します。

  これらの MAC アドレスは、リダイレクトポリシー定義の一部としてユーザーが APIC に手動で入力するか、フィールドが空のままの場合は自動生成されます。管理者は、これらの MAC アドレスをレイヤ 4 ～ レイヤ 7 サービスデバイスの MAC アドレステーブルに追加し、コンシューマーからプロバイダーへの方向で使用される MAC アドレスのプロバイダー側のポートと、プロバイダーからコンシューマーへの方向で使用されるコンシューマー側のポートに関連付ける必要があります。

- 中間スイッチがリーフと、レイヤ 1/レイヤ 2 モードで展開されたレイヤ 4 ～ レイヤ 7 サービスデバイスの間にある場合、中間スイッチは、書き換えられた接続先 MAC 宛てのトラフィックを転送する必要もあります。
- レイヤ 1/レイヤ 2 PBR は、リーフ/ポート/VLAN への転送に基づいているため、VMM ドメインではなく、物理ドメインでのみ展開できます。仮想アプライアンスでレイヤ 1/レイヤ 2 PBR を展開する必要がある場合は、物理ドメインで構成する必要があります。
- ハイアベイラビリティの観点から、レイヤ 4 ～ レイヤ 7 サービスデバイスはアクティブ/スタンバイ モードで展開され、Cisco ACI では、どのパス（リーフ/ポート）がアクティブか、スタンバイかを確認するためにトラッキングを実行する必要があります。トラッキングは、レイヤ 4 ～レイヤ 7 サービス論理デバイスクラスタ内の複数のサービスデバイスに必須です。
- レイヤ 1/レイヤ 2 PBR トラッキングには、レイヤ 2 ping が使用されます。IP SLA タイプはレイヤ 2 ping です。
- レイヤ 2 ping の `ethertype 0x0721` は、サービスデバイスを通過するリーフノード間で交換されます。したがって、レイヤ 1/レイヤ 2 デバイスでは `ethertype 0x0721` を許可する必要があります。
- レイヤ 1/レイヤ 2 ポリシーベースリダイレクトは、CLI ではサポートされていません。
- レイヤ 1/レイヤ 2 PBR アクティブ/アクティブ PBR 接続先は、カプセル化のフラッディングがリモートリーフスイッチでサポートされていないため、リモートリーフスイッチには接続できません。プロバイダーおよびコンシューマーのサービスノードは、引き続きリモートリーフスイッチに接続できます。
- アクティブ/スタンバイモード（ハイアベイラビリティ）で構成されたレイヤ 1/レイヤ 2 対称 PBR の場合、重みベースの対称 PBR はサポートされません。アクティブおよびスタンバイ PBR の接続先には重みを設定しないことをお勧めします。
- アクティブ/アクティブモードで設定されたレイヤ 1/レイヤ 2 対称 PBR の場合、重みベースの対称 PBR がサポートされます。
- 動的な VLAN 割り当てはサポートされていません。

アクティブ/スタンバイ レイヤ 1/レイヤ 2 PBR 設計の概要

Cisco Application Policy Infrastructure Controller (APIC) リリース 4.1 以降のリリースでは、レイヤ 1/レイヤ 2 ポリシーベースリダイレクト (PBR) およびアクティブ/スタンバイ PBR 設計がトラッキングでサポートされています。

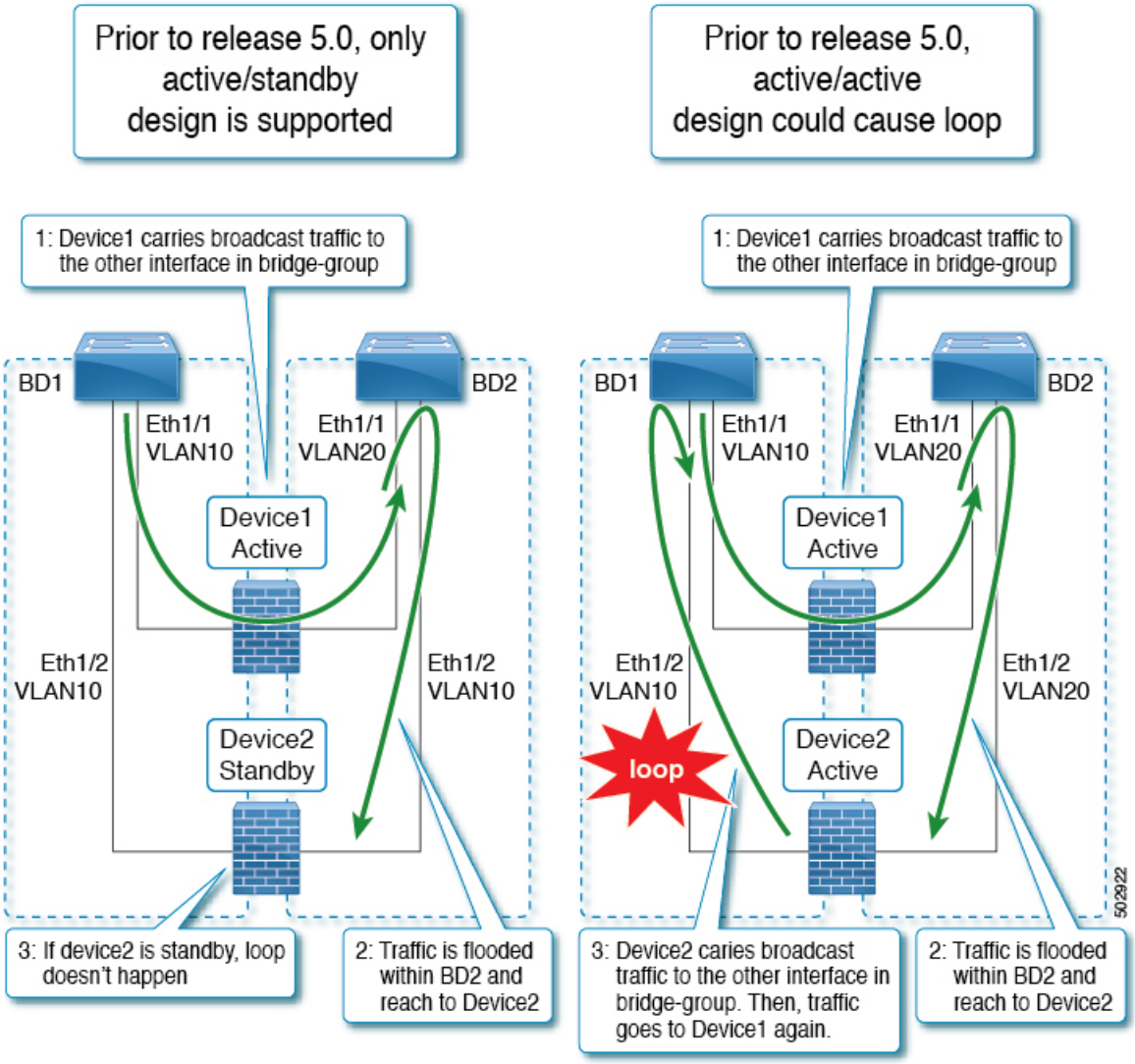
レイヤ 1/レイヤ 2 PBR の場合、レイヤ 2 ping の送信元および接続先 MAC アドレスは PBR 接続先 MAC アドレスです。PBR ノードが稼働してトラフィックを伝送している場合、レイヤ 2 ping は正常に Cisco Application Centric Infrastructure (ACI) ファブリックに戻ることになります。その後、Cisco ACI ファブリックは PBR 接続先が使用可能であることを認識します。レイヤ 1/レイヤ 2 PBR を使用して挿入するアクティブおよびスタンバイのハイアベイラビリティ レイヤ 1/レイヤ 2 サービスノードがあり、トラッキングが有効になっている 2 つの PBR 接続先が

ある場合、スタンバイデバイスはトラフィックを転送しないため、アクティブノードに接続されているパスの 1 つのみが稼働することになります。その結果、トラフィックはアクティブノードに接続されているインターフェイスにリダイレクトされます。

フェールオーバーが発生し、スタンバイがアクティブロールを引き継ぐ場合、トラッキングステータスが変化し、トラフィックは新しいアクティブノードに接続されているインターフェイスにリダイレクトされます。

Cisco APIC リリース 5.0(1) より前のリリースでは、次の図に示すように、同一のサービスブリッジ ドメインペアに複数のレイヤ 1/レイヤ 2 デバイスがアクティブ/スタンバイ設計で存在する場合、ブリッジドメイン内でトラフィックがフラッディングされ、トラフィックが 2 番目のレイヤ 4 ～ 7 サービスデバイスに到達しても、この 2 番目のレイヤ 4 ～ 7 サービスデバイスがスタンバイモードであるため、ループは発生しません。

Cisco APIC リリース 5.0(1) より前のリリースでアクティブ/アクティブ設計がサポートされない理由は、アクティブ/アクティブ設計で、同じサービスブリッジ ドメインペアに複数のレイヤ 1/レイヤ 2 デバイスがある場合、2 番目のデバイスがレイヤ 4 ～ レイヤ 7 サービスデバイスはトラフィックを他のブリッジドメインの他のインターフェイスに転送し、トラフィックは最初のデバイスに到達してループが発生するためです。



アクティブ/アクティブ レイヤ 1/レイヤ 2 対称 PBR 設計の概要

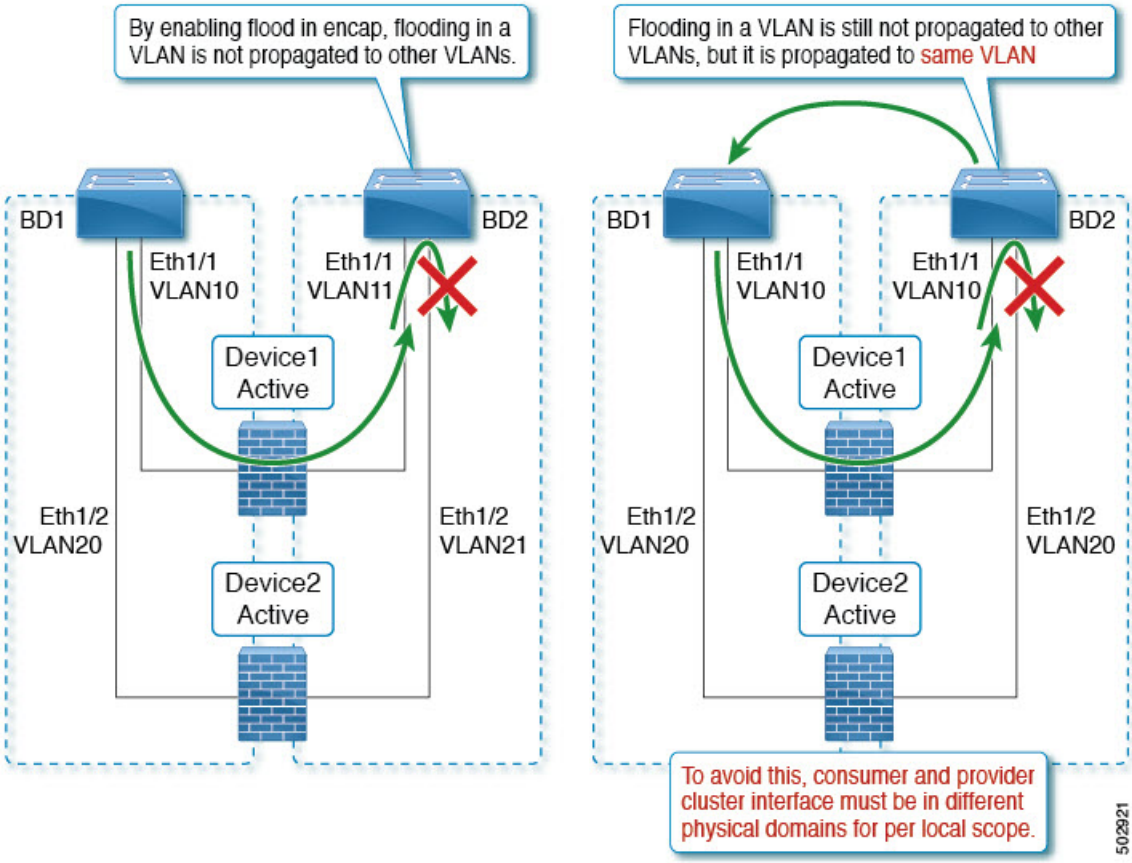
Cisco APIC リリース 5.0(1) 以降のリリースでは、サービス チェーン内のレイヤ 1/レイヤ 2 デバイスは、アクティブ/アクティブの対称 PBR 設計で動作できます。対称 PBR は、ハッシュに基づいて個々のデバイスへのトラフィックを負荷分散するために使用されます。

このモードでは、トラフィックフローのハイアベイラビリティと効率的な分散が実現できます。APIC リリース 5.0(1) では、対称 PBR 関連機能として、しきい値、ダウンアクション、バックアップ PBR ポリシー（N+M ハイアベイラビリティ）などがサポートされています。レイヤ 1 PBR アクティブ/アクティブモードの場合、コンシューマーコネクタとプロバイダーコネクタは異なる物理ドメインにある必要があります。

レイヤ 1/レイヤ 2 のアクティブ/アクティブ設計を展開するには、レイヤ 4 ～ レイヤ 7 論理デバイス クラスタでアクティブ/アクティブモードを有効にする必要があります。クラスタ内の具象デバイスインターフェイスごとにカプセル化する必要があります。

例：同じブリッジドメインペアで、カプセル化が有効なフラッディングを使用すると、フラッディングは VLAN 内で伝達され、他の VLAN には伝達されません。そのため、同じブリッジドメイン内の複数のアクティブデバイスを接続できます。

レイヤ 1 アクティブ/アクティブモードの場合、外部コネクタと内部コネクタは同じカプセル化を持っています。アクティブノードごとに異なる VLAN を使用する場合、カプセル化が有効なフラッディングだけでは、ループを防止するには不十分です。この問題を回避するには、デバイスの両レッグを異なる物理ドメインと異なる VLAN 名前空間に関連付ける必要があります（実際の VLAN の範囲はそのままにできます）。これにより、レッグごとに異なる `fabEncap` が生成され、トラフィックループを防止します。



GUI を使用したレイヤ 1/レイヤ 2 デバイスの設定

始める前に

- Cisco APIC GUI を使用してレイヤ 1/レイヤ 2 デバイスを作成し、具象デバイスインターフェイスを作成します。

ステップ 1 メニュー バーで、[テナント（Tenants）] > [すべてのテナント（ALL Tenants）] の順に選択します。 >

ステップ 2 ナビゲーションウィンドウで、**[テナント（Tenant）]** *[テナント名（tenant_name）]* > **[サービス（Services）]** > **[L4-L7]** の順に選択します。

ステップ 3 右クリックで、[**デバイス（Devices**）] > [**L4 ～ L7 デバイスの作成（Create L4-L7 Devices**）] の順に選択します。

ステップ 4 [**L4 ～ L7 デバイスの作成（Create L4-L7 Devices**）] ダイアログボックスに、次のフィールドを入力にします。

a) [**名前（Name**）] フィールドで、レイヤ 4 ～ レイヤ 7 デバイスクラスタの名前を指定します。
b) [**サービスタイプ（Service Type**）] 領域で、[**Other（その他**）] を選択します。
c) [**デバイスタイプ（Device Type**）] で [**物理（Physical**）] を選択します。
d) [**物理ドメイン（Physical Domain**）] で、[物理ドメイン名（physical domain name）] を選択します。
e) [**コンテキスト認識（Context Aware**）] で [**単一（Single**）] を選択します。
f) [**機能タイプ（Function Type**）] で、[**L1**] または [**L2**] を選択します。
g) チェックボックスをオンにして、**アクティブ/アクティブモード**を有効にします。

ステップ 5 具象デバイスインターフェイスを作成します。レイヤ 1 またはレイヤ 2 の**アクティブ/アクティブモード**の場合は、右側の作業ペインの [**デバイス（Devices**）] モードで [+] をクリックします。[**具象デバイスの作成（Create Concrete Device**）] ダイアログボックスが表示されます。

a) [**名前（Name**）] フィールドに、デバイス名を入力します。
b) [+] をクリックして、具象デバイスインターフェイスにカプセル化を作成します。名前と具象インターフェイス名を入力します。

   レイヤ 1/レイヤ 2 PBR はツーアーム設計のみをサポートするため、[+] をもう一度クリックして、別の具象インターフェイスを作成します。名前、インターフェイスパス、カプセル化を入力します。[**更新（Update**）] > [**OK**] の順にクリックします。

   アクティブデバイスをさらに追加するには、手順 5a と手順 5b を繰り返します。

c) クラスタで、[+] をクリックしてコンシューマークラスタインターフェイスを作成し、コンシューマー具象インターフェイスを選択します。レイヤ 1 モードの場合、物理ドメインを選択します。

   [+] をもう一度クリックしてプロバイダークラスタインターフェイスを作成し、プロバイダー具象インターフェイスを選択します。レイヤ 1 モードの場合は、別の物理ドメインを選択します。

   （注） レイヤ 1 アクティブ/アクティブデバイスの場合、2 つの異なる VLAN プールにマッピングされた 2 つの物理ドメインを作成しますが、同じ VLAN 範囲を維持します。レイヤ 2 アクティブ/アクティブデバイスの場合、物理ドメインは手順 4e で選択されます。

ステップ 6 [Finish] をクリックします。

APIC GUI を使用したレイヤ 1/レイヤ 2 PBR の設定

始める前に

- レイヤ 1/レイヤ 2 機能タイプを使用して、L4 ～ L7 デバイスおよびサービスグラフを作成します。詳細は、「*GUI* を使用したポリシーベースリダイレクトの設定の設定手順」を参照してください。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 ナビゲーション ウィンドウで、**Tenant** *tenant_name* > **Policies** > **Protocol** > **L4-L7 Policy Based Redirect** を選択します。

ステップ 3 作業ウィンドウで、**Action** > **Create L4-L7 Policy Based Redirect** を選択します。

ステップ 4 [**L4 ～ L7 ポリシーベースリダイレクトの作成（Create L4-L7 Policy Based Redirect**）] ダイアログボックスで、次のフィールドを入力します。

a) [**名前（Name**）] フィールドに、名前を入力します。

b) [**接続先タイプ（Destination Type**）] フィールドで、[**L1**] または [**L2**] を選択します。

c) **IP SLA モニタリングポリシー**で、L2 ping モニタリングポリシーを作成します。

- [**名前（Name**）] フィールドに、名前を入力します。
- [**SLA タイプ（SLA Type**）] で、[**L2Ping**] を選択します。

  [**SLA 頻度（SLA Frequency**）] はオプションです。

d) [**L1 ～ L2 接続先（L1-L2 Destination**）] で、[+] をクリックして接続先を追加します。

名前、リダイレクトヘルスグループ、具象インターフェイスを入力します。MACアドレスの構成はオプションです。

e) [OK] をクリックします。

（注） 実際のインターフェイスの MAC アドレスは入力しないでください。APIC が自動的に MAC を生成するように空白のままにするか、外部 PBR ポリシー MAC A および内部 PBR ポリシー MAC B にダミーの MAC アドレスを入力します。これらの MAC アドレスはファイアウォール設定で使用されることに注意してください。

ステップ 5 [送信（Submit）] をクリックします。

ステップ 6 ナビゲーションウィンドウで、[**サービス（Services**）] > [**L4 ～ L7（L4-L7**）] > [**デバイス選択ポリシー（Device Selection Policies**）] > [論理デバイスコンテキスト名（*Logical Device Context_name*）] の順に選択します。

ステップ 7 論理デバイスを展開し、コンシューマーまたはプロバイダーの [**L4 ～ L7 ポリシーベースリダイレクト（L4-L7 Policy-Based Redirect**）] フィールドにレイヤ 1/レイヤ 2 PBR ポリシーを適用します。

ステップ 8 [送信（Submit）] をクリックします。

CLI を使用したレイヤ 1/レイヤ 2 PBR の ASA の設定

始める前に

- 一般的な構成の場合、サービスデバイスはレイヤ 2 ping トラッキングパケットを転送できる必要があります。

  レイヤ 2 ping、`ethertype 0x0721` がトラッキングに使用されます。レイヤ 2 ping は、サービスデバイスを通過するリーフノード間で交換されます。したがって、レイヤ 1/レイヤ 2 デバイスでは `ethertype 0x0721` を許可する必要があります。

- 静的 MAC 構成が必要です。
- 次に、ASA がレイヤ 2 モードで L4 ～ L7 デバイスとして使用される ASA 設定の例を示します。

ステップ 1 ASA インターフェイス（サービスレッグ）は、同じブリッジグループで設定する必要があります。

例：

```
interface GigabitEthernet0/0
nameif externalIf
brdige-group 1

interface GigabitEthernet0/1
nameif internalIf
bridge-group 1
```

ステップ 2 ASA は、レイヤ 2 ping トラフィックの送信元 MAC アドレスを学習します。レイヤ 2 ping トラフィックは同じ送信元 MAC を使用してコンシューマーとプロバイダーの方向をトラッキングするため、ASA で作成されるエントリが競合するのを避けるために、MAC 学習を無効にすることをお勧めします。

次の例では、**externalIf** は、レイヤ 1/レイヤ 2 サービスノードのコンシューマーコネクタとして使用される ASA のインターフェイス名で、**internalIf** は、レイヤ 1/レイヤ 2 サービスノードのプロバイダーコネクタとして使用される ASA のインターフェイス名です。**externalIf** および **internalIf** で MAC 学習を無効にします。L2 ping は、外部レッグと内部レッグの両方をトラッキングする場合に同じソース MAC を使用します。

レイヤ 2 ping が同じ送信元 MAC を使用して外部と内部をトラッキングするため、ASA で競合するエントリが作成されるのを避けるために、MAC 学習は無効になっています。

例：

```
mac-learn externalIf disable
mac-learn internalIf disable
```

ステップ 3 L2 ping カスタム EtherType を許可するように ASA ルールを設定します。

例：

```
access-list Permit-Eth ethertype permit any
access-group Permit-Eth in interface externalIf
access-group Permit-Eth in interface internalIf
```

ステップ 4 リダイレクトされたトラフィックとレイヤ 2（Layer2）ping パケットは PBR 接続先 MAC を使用し、ASA はコンシューマー インターフェイスとプロバイダー インターフェイスをブリッジします。ASA 透過モードは、一般に不明な接続先 MAC をフラッディングしますが、L2 PBR では、PBR 接続先 MAC が実際にはネットワークに存在しないため、この方法は使用できません。したがって、レイヤ 2 ping および PBR トラフィックが ASA によってすべてのケースで適切にブリッジされるように静的 MAC エントリを使用することを勧めします。

例：

```
mac-address-table static externalIf (MAC B)
mac-address-table static internalIf (MAC A)
```

（注） ASA などのサービスデバイスの設定とは別に、リーフとサービスデバイスの間に中間スイッチがある場合、中間スイッチによってトラフィックを伝送できるようにする必要があります。中間スイッチで静的 MAC 構成または無差別モード構成が必要になる場合があります。

CLI を使用したリーフのレイヤ 1/レイヤ 2 PBR ポリシーの確認

この手順のコマンド例では、レイヤ 1 およびレイヤ 2 のポリシーベースリダイレクト ノードを設定します。

ステップ 1 スイッチに PBR グループと接続先情報が設定されているかを確認します。

例：

```
sdk74-leaf4# show service redir info
GrpID Name                           destination                                   operSt
===== ====                           ===========                                   ======
1     destgrp-1                      dest-[50.50.50.1]-[vxlan-2719744]]            enabled
2     destgrp-2                      dest-[20.20.20.1]-[vxlan-2719744]]            enabled
Name                                 bdVnid          ip              vMac                 vrf
      vrfEncap        operSt
====                                 ======          ==              ====                 ===
       =
dest-[20.20.20.1]-[vxlan-2719744]   vxlan-16514958  20.20.20.1     00:00:14:00:00:01    coke1:cokectx1
  vxlan-2719744   enabled
dest-[50.50.50.1]-[vxlan-2719744]   vxlan-16711542  50.50.50.1     00:00:3C:00:00:01    coke1:cokectx1
  vxlan-2719744   enabled
```

ステップ 2 正しいアクションとグループ情報でゾーニングルールが構成されているかを確認します。

例：

```
sdk74-leaf4# show zoning-rule | grep redir
4103            49155           49154           18              enabled         2719744
redir(destgrp-2)      fully_qual(6)
4106            49154           49155           17              enabled         2719744
redir(destgrp-1)      fully_qual(6)
```

ステップ 3 PBR の Aclqos サブコマンド：

例：

```
module-1# show system internal aclqos services redir ?
  <CR>
```

```
  dest   Dest related info
  group  Group related info

module-1# show system internal aclqos services redir group 1

 Flag Legend :
 0x1: In SDK
 0x10: In local DB
 0x20: Delete pending
 0x40: Dummy adj

******* Service key redir-group(1) *******
 Service flags: 0x11
 Num of reference: 0x1
 Num of path: 1
 path 0 key: redir-dest-ipv4(vrf vnid vxlan-2719744 prefix-50.50.50.1)

module-1# show system internal aclqos services redir dest 2719744 50.50.50.1
 Flag Legend :
 0x1: In SDK
 0x10: In local DB
 0x20: Delete pending
 0x40: Dummy adj
******* Service key redir-dest-ipv4(vrf vnid vxlan-2719744 prefix-50.50.50.1) *******
 Service flags: 0x10
 Num of reference: 0x1
 Num of path: 1
 Ifindx: 0x18010007
 Bd_vnid: 16711542
 Vmac: 00:00:3c:00:00:01
```

ステップ 4 ゾーニングルールコマンド：

例：

```
module-1# show system internal aclqos zoning-rules 4106
 ASIC type is Sug
==============================================================
Rule ID: 4106 Scope 3 Src EPG: 49154 Dst EPG: 49155 Filter 17
  Redir group: 1

  Curr TCAM resource:
  ============================
    unit_id: 0
    === Region priority: 1539 (rule prio: 6 entry: 3)===
        sw_index = 44 | hw_index = 44
    === SDK Info ===
        Result/Stats Idx: 81876
        30
        Tcam Total Entries: 1
        HW Stats: 0
```

REST API を使用したレイヤ 1/レイヤ 2 PBR の設定

レイヤ 1/レイヤ 2 ポリシーベースリダイレクト構成：

例：

```
<polUni>
    <fvTenant name="coke" >

        <!—If L1/L2 device in active-active mode -- >
        <vnsLDevVip name="N1"  activeActive="yes" funcType="L1" managed="no">
        </vnsLDevVip>
        <!—If L1/L2 device in active-standby mode -- >
        <vnsLDevVip name="N1"  activeActive="no" funcType="L1" managed="no">
        </vnsLDevVip>

        <vnsAbsGraph descr="" dn="uni/tn-coke/AbsGraph-WebGraph" name="WebGraph" ownerKey=""
ownerTag="" uiTemplateType="UNSPECIFIED">

        <!—For L2 device -- >
       <vnsAbsNode descr="" funcTemplateType="OTHER" funcType="L2" isCopy="no" managed="no" name="N1"
 ownerKey="" ownerTag="" routingMode="Redirect" sequenceNumber="0" shareEncap="no">
    </vnsAbsNode>

       <!—For L1 device -- >
     <vnsAbsNode descr="" funcTemplateType="OTHER" funcType="L1" isCopy="no" managed="no" name="N1"
 ownerKey="" ownerTag="" routingMode="Redirect" sequenceNumber="0" shareEncap="no">
    </vnsAbsNode>

    </vnsAbsGraph>

    <fvIPSLAMonitoringPol name="Pol2" slaType="l2ping"/>
<vnsSvcCont>
<vnsRedirectHealthGroup name="2" />
             <vnsSvcRedirectPol name="N1Ext"  destType="L2">
                   <vnsRsIPSLAMonitoringPol tDn="uni/tn-coke/ipslaMonitoringPol-Pol2"/>
     <vnsL1L2RedirectDest destName="1">
                <vnsRsL1L2RedirectHealthGroup tDn="uni/tn-coke/svcCont/redirectHealthGroup-2"/>
            <vnsRsToCIf tDn="uni/tn-coke/lDevVip-N1/cDev-ASA1/cIf-[Gig0/0]"/>
  </vnsL1L2RedirectDest>
             </vnsSvcRedirectPol>

             <vnsSvcRedirectPol name="N1Int" destType="L2">
                   <vnsRsIPSLAMonitoringPol tDn="uni/tn-coke/ipslaMonitoringPol-Pol2"/>
      <vnsL1L2RedirectDest destName="2">
                <vnsRsL1L2RedirectHealthGroup tDn="uni/tn-coke/svcCont/redirectHealthGroup-2"/>
           <vnsRsToCIf tDn="uni/tn-coke/lDevVip-N1/cDev-ASA1/cIf-[Gig0/1]"/>
     </vnsL1L2RedirectDest>
          </vnsSvcRedirectPol>
        </vnsSvcCont>
</fvTenant>
</polUni>
```

ポリシーベースリダイレクトとサービスノードのトラッキング

Cisco Application Policy Infrastructure Controller (APIC) 2.2(3) および 3.1(1) リリース (ただし、3.0 リリースを除く) 以降のリリースでは、ポリシーベースリダイレクト機能 (PBR) は、サービスノードをトラッキングする機能をサポートしています。トラッキングにより、ダウンしているサービスノードへのトラフィックのリダイレクトを防ぐことができます。サービスノード（PBR 接続先）がダウンした場合、PBR ハッシュはポリシーで使用可能な PBR 接続先の選択を開始

できます。この機能を使うには、Cisco Nexus 9300-EX、-FX、またはそれ以降のプラットフォーム リーフスイッチが必要です。

サービスノードは、デュアル IP アドレススタッキングをサポートできます。したがって、この機能には、IPv4 アドレスと IPv6 アドレスの両方を同時にトラッキングできます。IPv4 アドレスと IPv6 アドレスの両方が「up（動作中）」の場合、PBR 接続先は「up（動作中）」とマークされます。

スイッチでは、Cisco IP SLA モニタリング機能を内部的に使用して、PBR トラッキングをサポートします。トラッキング機能では、サービスノードに到達できない場合、リダイレクト接続先ノードを「ダウン（down）」としてマークします。トラッキング機能では、サービスノードが接続を再開すると、リダイレクト先をノード「動作中（up）」としてマークします。サービスノードが「ダウン（down）」とマークされている場合、そのノードはトラフィックの送信またはハッシュに使用されません。代わりに、トラフィックはリダイレクト先ノードのクラスタ内の別のサービスノードに送信またはハッシュされます。

一方向のトラフィックのブラックホール化を避けるために、サービスノードの入力および出力のリダイレクト接続先ノードをリダイレクトヘルスポリシーに関連付けることができます。そうすることで、入力または出力のリダイレクト接続先ノードがダウンした場合、もう一方のリダイレクト接続先ノードも「ダウン（down）」としてマークされます。したがって、入力トラフィックと出力トラフィックの両方が、リダイレクト先ノードのクラスタ内の異なるサービスノードにハッシュされます。

トラッキングには次のプロトコルを使用できます。

- ICMP（レイヤ 3 PBR の場合）
- TCP（レイヤ 3 PBR の場合）
- L2ping（レイヤ 1/2 PBR の場合）
- HTTP URI（レイヤ 3 PBR の場合、5.2(1) 以降のリリース）

ポリシーベースリダイレクトとヘルスグループによるサービスノードのトラッキング

ポリシーベースリダイレクト(PBR)サービスノードトラッキングを使用すると、障害が発生したPBRノードへのトラフィックのリダイレクトを防止できます。PBRノードのコンシューマーコネクタまたはプロバイダーコネクタがダウンした場合、障害が発生したノードを通過したトラフィックがブラックホールになる可能性があります。トラフィックがブラックホール化されるのを防ぐために、Cisco Application Centric Infrastructure (ACI) では両方向のトラフィックにPBRノードを使用しないようにします。レイヤ4からレイヤへのサービスデバイスには、別のインターフェイスがダウンした場合にインターフェイスを停止できるものもあります。これを使用して、トラフィックのブラックホール化を防ぐことができます。PBRノードにこの機能がない場合、コンシューマーコネクタまたはプロバイダーコネクタのいずれかがダウンしている場合は、ヘルスグループ機能を使用してノードの PBR を無効にする必要があります。

各 PBR 接続先 IP と MAC アドレスは、ヘルスグループに含めることができます。たとえば、2 つの PBR ノードの接続先があるとします。1 つは、Health-group1 にあり、コンシューマーコネクタとして 172.16.1.1 を持ち、プロバイダーコネクタとして 172.16.2.1 を持っています。もう 1 つは、Health-group2 にあり、コンシューマーコネクタとして 172.16.1.2 を持ち、プロバイダーコネクタとして 172.16.2.2 を持っています。同じヘルスグループ内の PBR 接続先のいずれかがダウンしている場合、そのノードは PBR に使用されません。

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

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(PBR)ポリシーを構成する場合、次のしきい値設定を使用できます。

- しきい値の有効化または無効化：しきい値が有効になっているとき、最小および最大のしきい値のパーセンテージを指定します。リダイレクト先グループを完全に無効にして、リダイレクトを防止したい場合は、有効になっているしきい値は必須です。リダイレクトがないときに、トラフィックがコンシューマとプロバイダ間で直接送信されます。
- 最小しきい値：指定した最小しきい値のパーセンテージ。トラフィックが最小パーセンテージを下回る場合、パケットはリダイレクトされずに許可されます。デフォルト値は 0 です
- 最大しきい値：指定された最大しきい値のパーセンテージ。最小しきい値に達すると、操作状態に戻すため最大パーセンテージに最初に到達する必要があります。デフォルト値は 0 です

例として、ポリシーに 3 つのリダイレクト先があると仮定してみましょう。最小しきい値が 70% に指定されており、最大しきい値が 80% に指定されています。3 つのリダイレクト先ポリシーの 1 つがダウンすると、アベイラビリティのパーセンテージは 3 つのうちの 1 つ（または 33%）が低下し、最小しきい値を下回ります。その結果、リダイレクト先グループの最小しきい値のパーセンテージがダウンし、トラフィックがリダイレクトではなく許可の取得を開始します。同じ例で、最大しきい値が 80% の場合、リダイレクトポリシーの接続先グループを動作状態に戻すには、最大しきい値のパーセンテージよりも大きいパーセンテージにする必要があります。

重みベースの PBR の場合、しきい値は使用可能な PBR 接続先のすべての重みの合計を、設定された PBR 接続先のすべての重みの合計で割った値になります。以下の例では、すべての接続先が稼働している場合、しきい値は 100% になります。接続先 1 がダウン（重み 4）で、しきい値が 60% であるとします。

Destination	**重量**	**Traffic %-age** **（おおよその）**
接続先 1	4	40
接続先 2	3	30

Destination	重量	Traffic %-age （おおよその）
接続先 3	2	20
接続先 4	1	10

ポリシーベースリダイレクトとトラッキングサービスノードについての注意事項と制限事項

サービスノードでポリシーベースリダイレクト(PBR)トラッキングを使用する場合は、次の注意事項と制限事項に従ってください。

- 接続先を共有する接続先グループには、同じヘルスグループと IP SLA モニタリングポリシーが設定されている必要があります。
- リリース 4.0(1) 以降のリリースでは、リモートリーフスイッチ設定は PBR トラッキングをサポートしますが、システムレベルのグローバル GIPo が有効になっている場合に限ります。「*GUI* を使用してリモート リーフのグローバル *GIPo* を構成する」を参照してください。
- リリース 4.0(1) 以降のリリースでは、リモートリーフスイッチ設定は PBR の復元力のあるハッシュをサポートします。
- Cisco ACI マルチポッド ファブリック セットアップがサポートされています。
- Cisco ACI マルチサイト セットアップはサポートされていますが、PBR の接続先を別のサイトにすることはできません。
- L3Out は、コンシューマー EPG およびプロバイダー EPG でサポートされています。
- PBR は、リーフスイッチで最大 100 のトラッキング可能な IP アドレスをサポートし、Cisco Application Centric Infrastructure (ACI) ファブリックで 400 のトラッキング可能な IP アドレスをサポートします。
- Cisco ACI ファブリック内のサービスグラフインスタンスの最大数については、お客様がお使いのリリース向けの『Cisco APIC 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。
- デバイスごとのサービスグラフインスタンスの最大数については、お客様がお使いのリリース向けの『Cisco APIC 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。
- PBR ポリシーごとに最大 40 のサービスノードを設定できます。
- サービスチェーンごとに最大 3 つのサービスノードを設定できます。
- PBR トラッキングでは、共有サービスがサポートされています。
- 次のしきい値ダウン時のアクションがサポートされています。

- バイパス（bypass action）
- 拒否(deny action）
- 許可(permit action）

- 複数の PBR ポリシーが同じ VRF インスタンスに同じ PBR 接続先 IP アドレスを持つ場合、そのポリシーは PBR 接続先に対して同じ IP SLA ポリシーとヘルスグループを使用する必要があります。

PBR を設定し、GUI を使用してサービス ノードのトラッキング

ステップ 1 メニュー バーで [Tenant] > **テナント名**をクリックします。ナビゲーションウィンドウで、**[ポリシー（Policies）] > [プロトコル（Protocol）] > [L4 ～ L7 ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）]** の順に選択します。

ステップ 2 右クリックして **L4 ~ L7 ポリシー ベースのリダイレクト** をクリックします **作成 L4 ~ L7 ポリシー ベースのリダイレクト** 。

ステップ 3 **Create L4–L7 Policy Based Redirect** ダイアログボックスで、次の操作を実行します:

a) [**名前（Name**）] フィールドに、ポリシーベースリダイレクト (PBR) ポリシーの名前を入力します。

b) ダイアログボックスで、ハッシュアルゴリズム、IP SLA モニタリングポリシー、およびその他の必要な値を適切に設定します。

（注） 接続先を共有する接続先グループには、同じ IP SLA モニタリングポリシーが設定されている必要があります。

c) しきい値の設定フィールドでは、必要に応じて設定を指定し、必要な場合。

d) [**L3 接続先（L3 Destinations**）]の場合は、[+] をクリックして、[**リダイレクトされたトラフィックの接続先の作成（Create Destination of Redirected Traffic**）] を表示します。

e) [**リダイレクトされたトラフィックの接続先の作成（Create Destination of Redirected Traffic**）] ダイアログボックスに、適切な値を入力します。

[**IP**] および [**追加の IPv4/IPv6（Additional IPv4/IPv6**）] フィールドが提供され、IPv4 または IPv6 アドレスを指定できます。

（注） [**追加の IPv4/IPv6（Additional IPv4/IPv6**）] フィールドは必須ではありません。レイヤ 4 ～ レイヤ 7 サービスデバイスに複数の IP アドレスがあり、 Cisco Application Centric Infrastructure(ACI) でそれらの両方を確認する場合は、このフィールドを使用します。

[**IP**] と [**追加の IPv4/IPv6（Additional IPv4/IPv6**）] パラメータの両方が設定されている場合、PBR 接続先を「稼働中」としてマークするには、両方が稼働している必要があります。

f) **[リダイレクト ヘルス グループ]** フィールドで、既存のヘルス グループに関連付けるか、適切であれば、新しいヘルス グループを作成します。[OK] をクリックします。

（注） 接続先を共有する接続先グループには、同じヘルスグループが設定されている必要があります。

g) **Create L4–L7 Policy Based Redirect** ダイアログボックスで **Submit** をクリックします。

レイヤ 4 ～レイヤ 7 PBR とサービスノードのトラッキングは、リダイレクト ヘルスグループポリシーを PBR ポリシーにバインドし、リダイレクト接続先グループをトラッキングする設定を有効にした後で行います。

GUI を使用したリダイレクトヘルスグループの設定

ステップ 1 メニューバーで、**[テナント（Tenant）]**>**[テナント名（Tenant_name）]**をクリックします。ナビゲーションウィンドウで、**[ポリシー（Policies）]**>**[プロトコル（Protocol）]**>**[L4 ～ L7 リダイレクトヘルスグループ（L4-L7 Redirect Health Groups）]** の順に選択します。

ステップ 2 [**L4 ～ L7 リダイレクトヘルスグループ（L4-L7 Redirect Health Groups**）] を右クリックし、[**L4 ～ L7 リダイレクトヘルスグループの作成（Create L4-L7 Redirect Health Group**）] を選択します。

ステップ 3 **Create L4–L7 Redirect Health Group** ダイアログボックスで、次の操作を実行します。

a) **Name** フィールドに、 リダイレクト正常性ポリシーの名前を入力します。

b) 適切であれば、**Description** フィールドに追加の情報を入力し、**Submit** をクリックします。

レイヤ 4 ～ レイヤ 7 サービスのリダイレクトヘルスポリシーが設定されています。

GUI を使用してリモート リーフのグローバル GIPo を構成する

このタスクを実行すると、リモート リーフ設定で PBR トラッキングを機能させることができます。

（注） リモート リーフで PBR トラッキングを機能させるには、この設定を行う必要があります。この設定を行わないと、メイン データセンターが到達可能でも、リモート リーフで PBR トラッキングは機能しません。

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。

ステップ 2 [System Settings] ナビゲーション ウィンドウで [System Global GIPo] をクリックします。

ステップ 3 [System Global GIPo Policy] 作業ウィンドウで [Enabled] をクリックします。

ステップ 4 [Policy Usage Warning] ダイアログで、GIPo ポリシーを使用する可能性があるノードとポリシーを確認し、必要に応じて [Submit Changes] をクリックします。

REST API を使用したサービス ノードのトラッキングのサポートをする PBR の設定

トラッキング サービス ノードをサポートする PBR を設定します。

例：

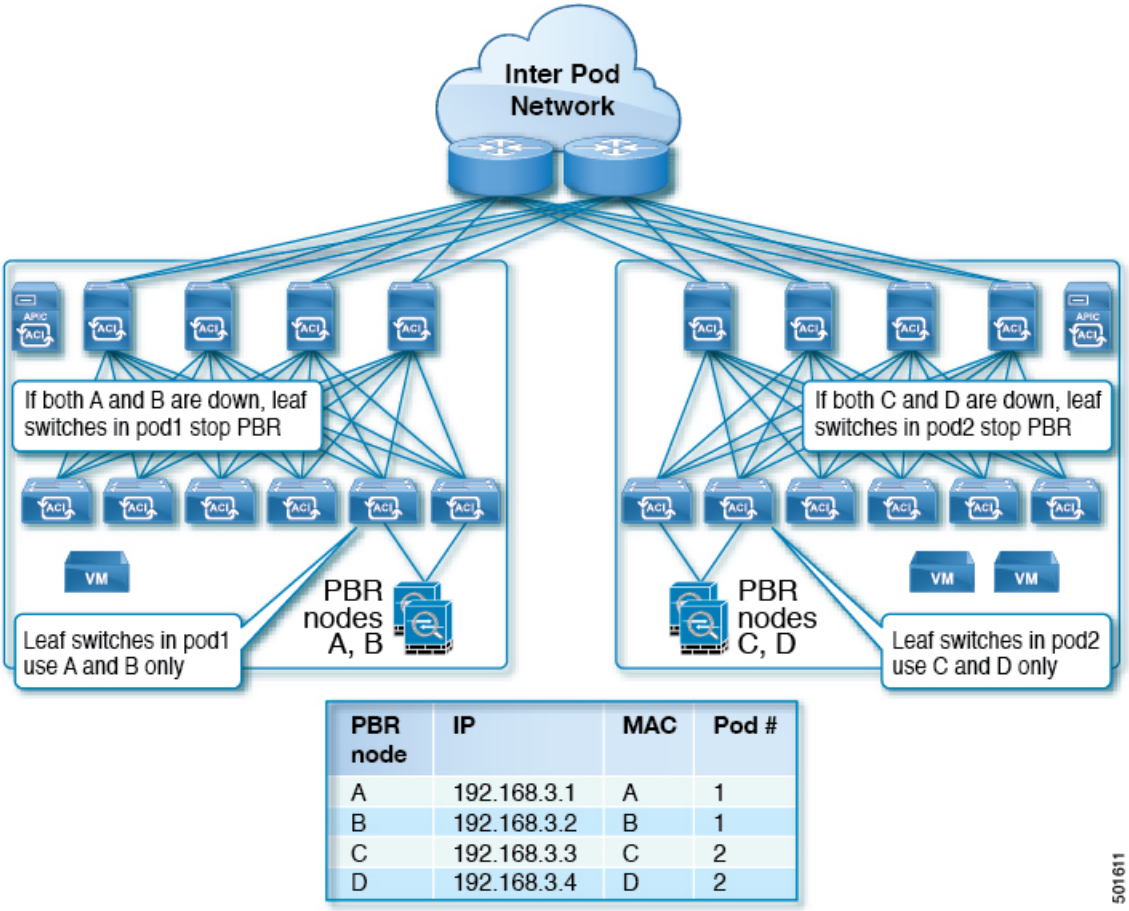
```
<polUni>
    <fvTenant name="t1" >
    <fvIPSLAMonitoringPol name="tcp_Freq60_Pol1" slaType="tcp" slaFrequency="60" slaPort="2222" />
    <vnsSvcCont>
        <vnsRedirectHealthGroup name="fwService1"/>
          <vnsSvcRedirectPol name="fwExt" hashingAlgorithm="sip" thresholdEnable="yes"
            minThresholdPercent="20" maxThresholdPercent="80">
            <vnsRedirectDest ip="40.40.40.100" mac="00:00:00:00:00:01">
               <vnsRsRedirectHealthGroup tDn="uni/tn-t1/svcCont/redirectHealthGroup-fwService1"/>
            </vnsRedirectDest>
            <vnsRsIPSLAMonitoringPol tDn="uni/tn-t1/ipslaMonitoringPol-tcp_Freq60_Pol1"/>
          </vnsSvcRedirectPol>
         <vnsSvcRedirectPol name="fwInt" hashingAlgorithm="sip" thresholdEnable="yes"
           minThresholdPercent="20" maxThresholdPercent="80">
             <vnsRedirectDest ip="30.30.30.100" mac="00:00:00:00:00:02">
                <vnsRsRedirectHealthGroup tDn="uni/tn-t1/svcCont/redirectHealthGroup-fwService1"/>
             </vnsRedirectDest>
             <vnsRsIPSLAMonitoringPol tDn="uni/tn-t1/ipslaMonitoringPol-tcp_Freq60_Pol1"/>
          </vnsSvcRedirectPol>
        </vnsSvcCont>
    </fvTenant>
</polUni>
```

ベース リダイレクトの場所に対応したポリシーについて

ロケーション対応ポリシー ベースのリダイレクト (PBR) はサポートされています。この機能は、multipod 設定シナリオに役立ちます。ここでは、ポッド認識サポートされ、優先ローカル PBR ノードを指定できます。ロケーション対応のリダイレクトを有効にすると、ポッド Id が指定されて、レイヤ 4 ~ レイヤ 7 PBR ポリシー内のすべてのリダイレクト宛先はポッド認識必要があります。リダイレクト宛先は、特定の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。

次の図は、2 個のポッドの例を表示します。ポッド 1 で PBR ノード A と B、C と D PBR ノードがポッド 2 では。ポッド 1 のリーフ スイッチが A、B、PBR ノードを使用する prefer し、ポッド 2 のリーフ スイッチ C と D で PBR ノードの使用場所に対応した PBR 設定を有効にするとPBR ノード A と B ポッド 1 では、ダウンは、[ポッド 1 のリーフ スイッチと開始 PBR ノード C と D を使用するには同様に、PBR ノード C と D ポッド 2 では、ダウンが、ポッド 2 のリーフ スイッチと開始 PBR ノード A および B を使用するには

図 *18 : 2* 個のポッドのロケーション対応 *PBR* 設定の例



PBR node	IP	MAC	Pod #
A	192.168.3.1	A	1
B	192.168.3.2	B	1
C	192.168.3.3	C	2
D	192.168.3.4	D	2

ロケーション認識型 PBR の注意事項

ロケーション認識 PBR を使用する場合は、次の注意事項に従ってください。

- Cisco Nexus 9300（Cisco Nexus 9300 EX および 9300 FX を除く）プラットフォーム スイッチは、ロケーション認識型 PBR 機能をサポートしていません。
- GOLF ホストアドバタイズメントと北南ファイアウォール連携にロケーション認識型 PBR を使用します。

  外部 EPG から EPG へのトラフィックの VRF 内コントラクトや、EPG 間のトラフィックの VRF 内コントラクトなど、着信トラフィックとリターントラフィックが同じリーフノードに適用されるコントラクトには、ロケーション認識 PBR を使用します。それ以外の場合では、トラフィックの対称性が失われる可能性があります。
- 複数の PBR ポリシーで同じ VRF に同じ PBR 接続先 IP アドレスを持つ場合、すべてのポリシーでポッド ID 認識リダイレクトを有効にするか、ポッド ID 認識リダイレクトを無効にする必要があります。同じ（VRF、IP アドレス）ペアは、有効の Pod ID 認識リダイレ

クト ポリシーと無効の Pod ID 認識リダイレクトポリシーで同時に使用することはできません。たとえば、次の構成はサポートされていません。

- PBR-policy1 には、VRF A の PBR 接続先 192.168.1.1 があり、Pod ID 認識リダイレクションが有効で、POD 1 に 192.168.1.1 が設定されています。
- PBR-policy2 では、VRF A に PBR 接続先 192.168.1.1 があり、Pod ID 認識リダイレクションが無効になっています。

GUI を使用したロケーション認識型 PBR の設定

この機能を有効にするための 2 つの項目をプログラムする必要があります。ポッド ID 認識リダイレクトを有効にし、特定のポッドにあるリーフ スイッチで、リダイレクト宛先をプログラムして、優先 PBR ノードにポッド ID を関連付けます。

ステップ 1 メニュー バーで [Tenant] > **テナント名**をクリックします。[Navigation] ペインで、[Policies] > [Protocol] > [L4-L7 Policy Based Redirect] をクリックします。

ステップ 2 右クリックして **L4 ~ L7 ポリシー ベースのリダイレクト** をクリックします **作成 L4 ~ L7 ポリシー ベースのリダイレクト** 。

ステップ 3 **Create L4–L7 Policy Based Redirect** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに PBR ポリシーの名前を入力します。

b) **[ポッド ID 認識リダイレクトの有効化]** チェック ボックスをオンにします。

c) ダイアログ ボックスでハッシュ アルゴリズム、IP SLA モニタリング ポリシー、およびその他の必要な値を構成するため、適切な設定を選択します。

d) しきい値の設定フィールドでは、必要に応じて設定を指定し、必要な場合。

e) [Destinations] を展開して [Create Destination of Redirected Traffic] を表示します。

f) **リダイレクト トラフィックの宛先の作成** ダイアログボックスなどの適切な詳細を入力します **IP** アドレス、および **MAC アドレス** フィールド。

IP アドレスと 2 番目の IP アドレスのフィールドでは、IPv4 アドレスと IPv6 あれドレスを指定できます。

g) **[ポッド ID]** フィールドに、ポッド ID 値を入力します。

h) [**重み**（**Weight**）] フィールドに値を入力します。デフォルト値は 1 です。指定できる範囲は 1 ～ 10 です。

このフィールドは、[**ポッド ID 認識リダイレクトを有効にする**（**Enable Pod ID Aware Redirection**）] チェックボックスがオンになっている場合にのみ表示されます。

i) **[リダイレクト ヘルス グループ]** フィールドで、既存のヘルス グループに関連付けるか、適切であれば、新しいヘルス グループを作成します。[OK] をクリックします。

必要に応じて別のポッド ID にリダイレクトされたトラフィックの他の宛先を作成します。

j) **Create L4–L7 Policy Based Redirect** ダイアログボックスで **Submit** をクリックします。

L4-L7 ロケーション認識型 PBR が設定されています。

REST API を使用して設定の場所に対応した PBR

2 つ設定する必要があります項目の場所に対応した PBR を有効にして、プログラムが特定のポッドにあるリーフ スイッチ内の送信先をリダイレクトします。次の例の場所に対応した PBR を有効にするよう設定されている属性が: programLocalPodOnly と podId 。

ロケーション対応 PBR を設定します。

例：

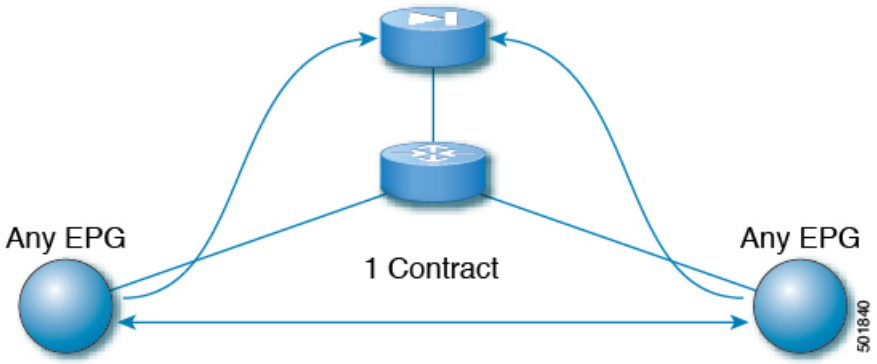
```
<polUni>
    <fvTenant name="coke" >
    <fvIPSLAMonitoringPol name="icmp_Freq60_Pol1" slaType="icmp" slaFrequency="60"/>
    <vnsSvcCont>
        <vnsRedirectHealthGroup name="fwService1"/>
          <vnsSvcRedirectPol name="fwExt" hashingAlgorithm="sip" thresholdEnable="yes"
minThresholdPercent="20" maxThresholdPercent="80" programLocalPodOnly="yes">
            <vnsRedirectDest ip="40.40.40.100" mac="00:00:00:00:00:01" podId="2">
              <vnsRsRedirectHealthGroup tDn="uni/tn-coke/svcCont/redirectHealthGroup-fwService1"/>

            </vnsRedirectDest>
            <vnsRsIPSLAMonitoringPol tDn="uni/tn-coke/ipslaMonitoringPol-icmp_Freq60_Pol1"/>
          </vnsSvcRedirectPol>
          <vnsSvcRedirectPol name="fwInt" hashingAlgorithm="dip" thresholdEnable="yes"
minThresholdPercent="20" maxThresholdPercent="80">
            <vnsRedirectDest ip="30.30.30.100" mac="00:00:00:00:00:02">
              <vnsRsRedirectHealthGroup tDn="uni/tn-coke/svcCont/redirectHealthGroup-fwService1"/>

            </vnsRedirectDest>
            <vnsRsIPSLAMonitoringPol tDn="uni/tn-coke/ipslaMonitoringPol-icmp_Freq60_Pol1"/>
          </vnsSvcRedirectPol>
        </vnsSvcCont>
    </fvTenant>
</polUni>
```

同じVRFインスタンス内のすべてのEPG-EPGにトラフィックをリダイレクトするには、ポリシーベースのリダイレクトとサービス グラフ

設定できる Cisco Application Centric Infrastructure (Cisco ACI) サービス グラフ リダイレクト vzAny と vzAny の設定によって、デバイスはすべてのエンドポイントを表す構築をレイヤ 7 にレイヤ 4 で同じ:VRF インスタンス内の他のエンドポイント グループをすべてのエンドポイン

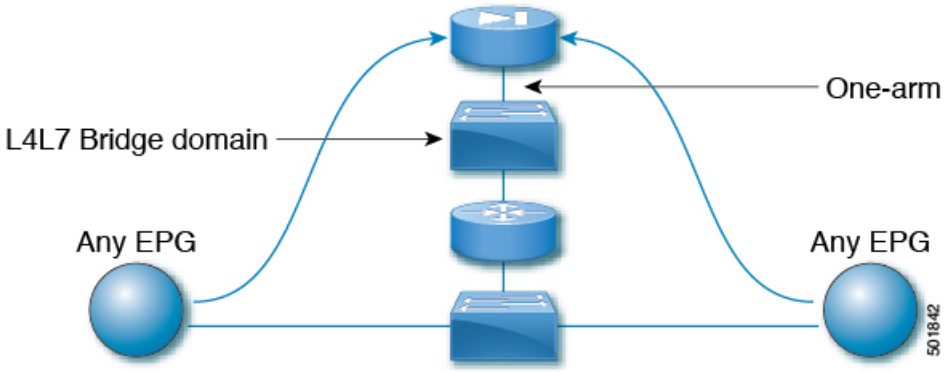
トグループからのすべてのトラフィックを転送するには。同じVRFインスタンスでグループ。vzAny は「any EPG」と呼ばれることがあります。

図 *19 : vzAny* トポロジ



同じ VRF インスタンスの下にある任意のエンドポイント グループ ペア間のトラフィックは、ファイアウォールなどのレイヤ 4 からレイヤ 7 デバイスにリダイレクトできます。また、同じブリッジ ドメイン内のトラフィックをファイアウォールにリダイレクトすることもできます。ファイアウォールは、次の図に示すように、任意の一対のエンドポイント グループ間のトラフィックをフィルタリングできます。

図 *20 :* 任意の *EPG* ペア間のトラフィックをフィルタリングするファイアウォール



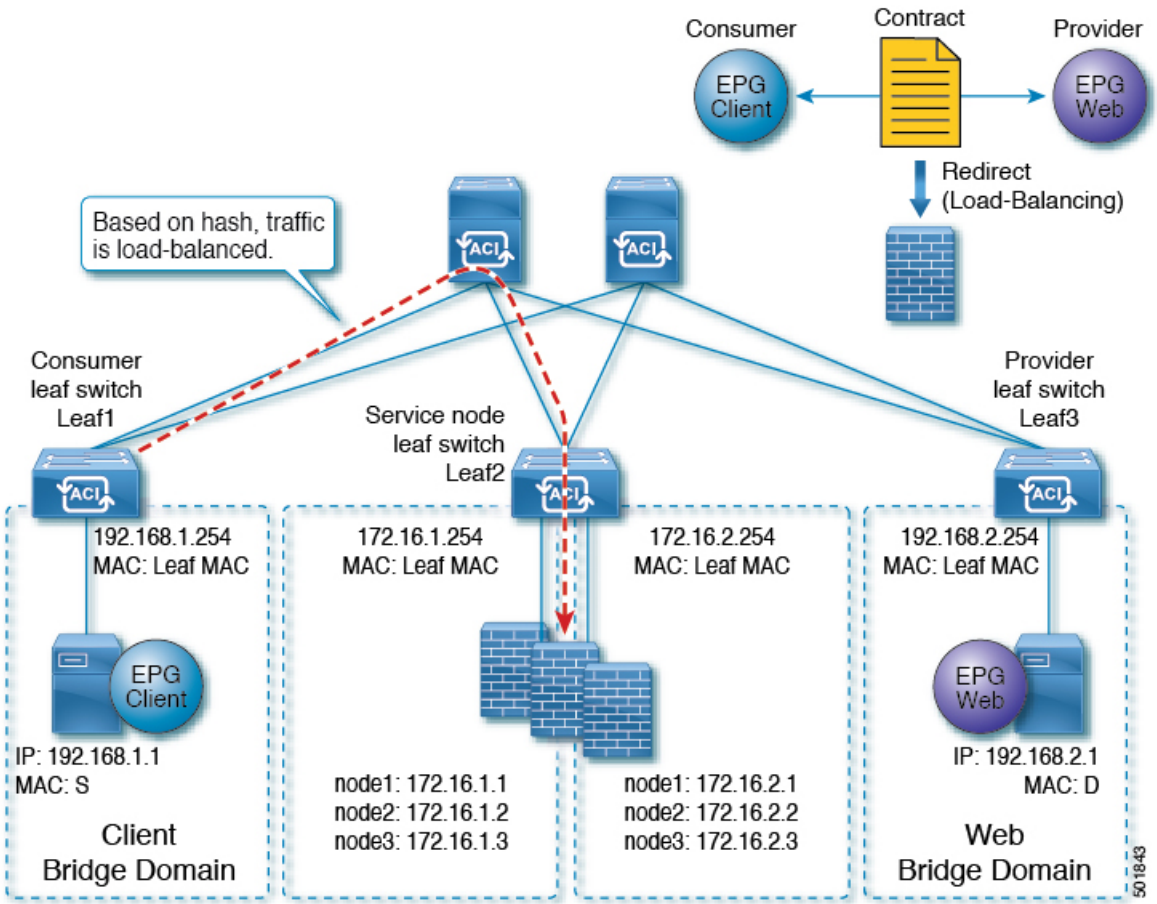
この機能の 1 つの使用例は、Cisco ACI をデフォルト ゲートウェイとして使用することですが、ファイアウォールを通るトラフィックをフィルタリングすることもそうです。vzAny とポリシー ベースのリダイレクト ポリシーにより、セキュリティ管理者は ACL ルールを管理し、ネットワーク管理者はルーティングとスイッチングを管理します。この設定の利点には、エンドポイント トラッキング、ARP インスペクションによるファースト ホップ セキュリティ、IP アドレス ソース ガードなどの Cisco Application Policy Infrastructure Controller (Cisco APIC) ツールを使用できることが含まれます。

ポリシー ベースのリダイレクト ポリシーを使用してサービス グラフを適用すると、次の機能も有効になります。

- ファイアウォール クラスタリング

- ファイアウォールの健全性追跡
- 位置認識リダイレクション

図 *21 :* ファイアウォール クラスタリング



Cisco APIC 3.2 のリリースより前に、vzAny を契約のコンシューマとして使用することができました。Cisco APIC 3.2 のリリースから、vzAny を契約のプロバイダとして使用することもできます。この拡張により、以下の構成が可能になります。

- プロバイダとしての vzAny、コンシューマとしての vzAny (ワンアームのみのポリシーベースのリダイレクト)
- プロバイダとしての vzAny、およびコンシューマとしての通常のエンドポイント グループ (ポリシーベースのリダイレクトおよび非ポリシーベースのリダイレクトの場合)

vzAny を使用してトラフィックをリダイレクトするポリシー ベースのリダイレクト ポリシーを使用してサービス グラフを適用した後、2 つのサーバ間のデータ バックアップ トラフィックなどのトラフィックがファイアウォールをバイパスするようにする場合には、エンドポイント グループ間でより具体的な契約を作成することができます。たとえば、2つのエンドポイン

トグループは、特定のポート上でトラフィックを相互に直接送信できます。より具体的なルールは、「任意のEPGから任意のEPGへ」リダイレクト ルールに優先します。

同じ VRF インターフェイス内のすべての EPG 間トラフィックをリダイレクトするために、ポリシーベースのリダイレクトポリシーをサービス グラフとともに設定する際の注意事項と制約事項

次の注意事項と制約事項は、同じ VRF インターフェイス内のすべての EPG 間トラフィックをリダイレクトするために、ポリシーベースのリダイレクト ポリシーをサービス グラフとともに設定する際に適用されます。

- レイヤ 4 ～ レイヤ 7 サービスデバイスと vzAny は、同じ VRF インスタンスに属している必要があります。
- レイヤ 4 ～ レイヤ 7 サービスデバイスは、ワンアームモードで展開する必要があります。
- 一般的な場合、多くの EPG が同じコントラクトを消費して提供する代わりに、vzAny コントラクトを使用して、多くの EPG から多くの EPG トラフィックへの PBR を有効にすることをお勧めします。ただし、同じ EPG で、コンシューマーコントラクトとプロバイダーコントラクトの両方としてサービスグラフが付加されているコントラクトを持たないでください。

  この推奨事項は、多くのプロバイダーおよびコンシューマー EPG を持つコントラクトの設定変更に影響を与える可能性があるために設けられています。Cisco Application Policy Infrastructure Controller (APIC) の 1 つの構成変更が同時に複数のゾーニングルール変更に関連する場合、Cisco APIC では、特定のリーフノードのハードウェアのプログラミングを完了するのに時間が必要です。
- 複数ノードのサービス グラフで設定された vzAny も機能する可能性はありますが、この設定は試験されておらず、サポートされません。自身のリスクにおいて使用してください。
- VRF リーキングと組み合わせた使用は、実装されていません。VRF インスタンスの vzAny に、他の VRF インスタンスの vzAny の契約の提供または利用を行わせることはできません。
- 異なるテナントのエンドポイント グループと vzAny の間で契約を設定することは、 VRF インスタンスがテナント **Common** にある場合のように、同じ VRF に属している限りにおいて可能です。
- マルチポッド環境では、 vzAny をプロバイダおよびコンシューマとして使用できます。
- Cisco ACI マルチサイト 環境では、サイト間で vzAny をプロバイダーおよびコンシューマーとして使用することはできません。

同じ VRF インターフェイス内のすべての EPG 間トラフィックをリダイレクトするために、ポリシーベースのリダイレクトポリシーをサービス グラフとともに設定する

次の手順では、同じ VRF インスタンス内のすべての EPG-EPG にトラフィックをリダイレクトするサービス グラフでポリシー ベースのリダイレクト ポリシーで設定します。

ステップ 1 レイヤ 4 レイヤ 7 デバイスへの接続を割り当てるはサービス ブリッジ ドメインを作成します。

ブリッジ ドメインの作成については、*Cisco APIC* ベーシック コンフィギュレーション ガイド を参照してください。

ステップ 1 > メイン 画面。

a) **VRF** ドロップダウンリスト、エンドポイントのグループが含まれている:VRF インスタンスを選択します。
b) **転送** ドロップダウンリスト、選択した場合 **カスタム** 、次に、 **L2 不明なユニキャスト** ドロップダウンリストを選択できます **フラッド** 必要かどうか。

ステップ 2 > L3 設定 画面。

a) チェックがあることを確認します **ユニキャスト ルーティング** チェック ボックス。
b) **サブネット** テーブルで、サブネットを作成します。

ゲートウェイ IP アドレスは、レイヤ 7 デバイス インターフェイスをレイヤ 4 に与えるは IP アドレスと同じサブネット内にする必要があります。

c) チェックを外し、 **エンドポイント データ ラーニング** チェック ボックス。

ステップ 2 リダイレクト ポリシーを作成します。

a) **ナビゲーション**ウィンドウで、**[テナント（Tenant）][テナント名（tenant_name）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4 ～ L7 ポリシーベースリダイレクト（L4-L7 Policy Based Redirect）]** の順に選択します。
b) 右クリックして **L4 L7 ポリシー ベースのリダイレクト**] を選択します **作成 L4 L7 ポリシー ベースのリダイレクト** 。
c) [Name] フィールドにポリシーの名前を入力します。
d) [**L3 接続先（L3 Destinations**）] テーブルで、[+] をクリックします。
e) **リダイレクト トラフィックの宛先の作成** ダイアログ ボックスで、次の情報を入力します。

- **IP** : IP アドレスを入力レイヤ 7 デバイスにレイヤ 4 に割り当てるされます。ブリッジ ドメインに支えられている IP アドレスと同じサブネットの IP アドレスがあります。
- **MAC**（オプション）。レイヤ 4 ～ レイヤ 7 デバイスに割り当てる MAC アドレスを入力します。レイヤ 7 デバイスにレイヤ 4 のフェールオーバー時にも有効な MAC アドレスを使用する必要があります。たとえば、ASA ファイアウォールの場合、これは仮想 *MAC* と呼ばれます。MAC アドレスを指定しない場合、アドレスは動的に検出されます。

f) その他の適切な値を入力し、クリックして **OK** 。
g) **作成 L4 L7 ポリシー ベースのリダイレクト** ダイアログ ボックスで、他の適切な値を入力し、クリックして **Submit** 。

ステップ 3 1 つの具体的なインターフェイスを 1 つの論理インターフェイス レイヤ 7 デバイスにレイヤ 4 を作成します。

レイヤ 7 デバイスにレイヤ 4 の作成についてを参照してください。GUI を使用したレイヤ 4 ～ レイヤ 7 サービスデバイスの設定 （10 ページ） 。

ステップ 4 ルート リダイレクトを有効になっていると、サービス グラフ テンプレートを作成します。

a) **Navigation** ウィンドウで、**Tenant tenant_name** > **Services** > **L4-L7** > **Service Graph Template** を選択します。
b) 右クリックして **サービス グラフ テンプレート**] を選択します **サービス グラフ テンプレートの作成** します。
c) **Name** フィールドに、サービス グラフの名前を入力します。
d) 以前を作成していないレイヤ 7 デバイスにレイヤ 4 の場合、 **デバイス クラスタ**] ペインで、デバイスを作成します。
e) ドラッグ アンド ドロップ レイヤ 4 からレイヤ 7 デバイス、 **デバイス クラスタ** され、中間 EPG コンシューマとプロバイダー EPG にウィンドウ。
f) **L4L7** ラジオ ボタンをクリックします **ルーテッド** 。
g) チェック マークを残します、 **リダイレクト ルーティング** チェック ボックス。
h) [Submit] をクリックします。

ステップ 5 サービス グラフ vzAny (AnyEPG) エンドポイント グループに適用されます。

ステップ 1 > 契約 画面。

a) **Navigation** ウィンドウで、**Tenant tenant_name** > **Services** > **L4-L7** > **Service Graph Template** > ***service_graph_name*** を選択します。

service_graph_name は、作成したサービス グラフ テンプレートです。

b) サービス グラフ テンプレートを右クリックし、選択 **L4 L7 サービス グラフ テンプレートの適用** 。
c) **コンシューマ EPG/外部ネットワーク** ドロップダウンリスト、選択、 **AnyEPG** テナントに対応するリスト項目とのこれを使用する VRF インスタンス使用例。

たとえば、テナントは、「tenant1」:VRF インスタンスは「vrf1」で、選択 **tenant1/vrf1/AnyEPG** .

d) **プロバイダー EPG 内部ネットワーク/** ドロップダウンリスト、同じ選択 **AnyEPG** コンシューマ EPG 用に選択したリスト項目。
e) **Contract Name** フィールドに、契約の名前を入力します。
f) [Next] をクリックします。

ステップ 2 > グラフ 画面。

a) 両方の **BD**] ドロップダウン リスト、ステップ 1 で作成したレイヤ 7 サービス ブリッジ ドメインをレイヤ 4 を選択します。
b) 両方の **リダイレクト ポリシー**] ドロップ ダウン リストでは、この使用例用に作成したリダイレクト ポリシーを選択します。

c) コンシューマ コネクタの **クラスタ インターフェイス** ドロップダウンリスト、ステップ 3 で作成したクラスタ インターフェイス (論理インターフェイス) を選択します。
d) プロバイダー コネクタの **クラスタ インターフェイス** ドロップダウンリスト、ステップ 3 で作成した同じクラスタ インターフェイス (論理インターフェイス) を選択します。
e) [Finish] をクリックします。

レイヤ3ポリシーベースリダイレクト先の動的MACアドレス検出

Cisco Application Policy Infrastructure Controller (APIC) 5.2(1) 以降のリリースでは、MAC アドレスを指定せずにレイヤ 3 ポリシーベースリダイレクト (PBR) の接続先を設定できます。PBR 接続先の一例として、サービスグラフの一部であるレイヤ 4 ～ レイヤ 7 デバイスがあります。この機能を設定することで、リーフスイッチは Address Resolution Protocol（ARP）を使用して、PBR ネクストホップの MAC アドレスを決定します。これにより、各 PBR 接続先の MAC アドレスを確認する必要がなく、アクティブ/スタンバイ HA ペアでフローティング MAC アドレスを使用する必要がないという利点があります。

レイヤ3ポリシーベースリダイレクト先の動的MACアドレス検出の注意事項と制限事項

レイヤ 3 ポリシーベースリダイレクト (PBR) 接続先の動的 MAC アドレス検出を設定するための注意事項と制限事項を次に示します。

- MAC アドレスを指定しなかった接続先に対しては、トラッキングを有効にする必要があります。
- すべてのレイヤ 3 PBR Equal Cost Multipath（ECMP：等コストマルチパス）機能と、IPv4 および IPv6 の接続先を使用できます。
- 同じ PBR ポリシーで、MAC アドレスを設定した接続先と MAC アドレスを設定していない接続先を一緒に持つことができます。
- MAC アドレスが変更された場合、トラッキング間隔によっては、新しい MAC アドレスを検出して、コンシューマーおよびプロバイダーのリーフスイッチで PBR 接続先 MAC アドレスを更新するのに時間がかかります。
- リーフスイッチごとに 100 の接続先、ファブリックごとに 1,500 の接続先を持つことができます。

GUI を使用したレイヤ 3 ポリシーベースリダイレクト先の動的 MAC アドレス検出の設定

次の手順では、レイヤ 3 ポリシーベースリダイレクト (PBR) 接続先の動的 MAC アドレス検出を設定します。

ステップ 1 メニュー バーで、**[テナント（Tenants）] > [すべてのテナント（ALL Tenants）]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーションウィンドウで、**[テナント（Tenant）] *[テナント名（tenant_name）]* > [ポリシー（Policies）] > [プロトコル（Protocol）] > [L4 ～ L7 ポリシーベースリダイレクト（L4-L7 Policy-Based Redirect）]** の順に選択します。

ステップ 4 [**L4 ～ L7 ポリシーベースリダイレクト（L4-L7 Policy-Based Redirect**）] を右クリックし、[**L4 ～ L7 ポリシーベースリダイレクトの作成（Create L4-L7 Policy-Based Redirect**）] を選択します。

ステップ 5 [**L4 ～ L7 ポリシーベースリダイレクトの作成（Create L4-L7 Policy-Based Redirect**）] ダイアログボックスで、必要に応じてフィールドに入力します（次に指定されているものは除く）。

a) [**接続先タイプ（Destination Type**）] で、まだ選択されていない場合は [**L3**] を選択します。

b) [**IP SLA モニタリング ポリシー（IP SLA Monitoring Policy**）] ドロップダウンリストで、既存の IP SLA モニタリングポリシーを選択するか、新しいポリシーを作成します。

c) [**L3 接続先（L3 Destinations**）] セクションで、[+] をクリックします。

d) [**リダイレクトされたトラフィックの接続先の作成（Create Destination of redirected traffic**）] ダイアログボックスの [**MAC**] フィールドに、`00:00:00:00:00:00` と入力するか、値を空のままにします。

どちらの方法でも、動的MACアドレス検出が有効になります。値を空のままにした場合、ポリシーの作成が完了すると値は `00:00:00:00:00:00` になります。

e) [**リダイレクトヘルスグループ（Redirect Health Group**）] で、必要に応じて、既存のヘルスグループを選択するか、新しいヘルスグループを作成します。

f) 必要に応じて、残りのフィールドに値を入力します。

g) [OK] をクリックします。

h) [送信（Submit）] をクリックします。

REST API を使用したレイヤ 3 ポリシーベースリダイレクト先の動的 MAC アドレス検出の設定

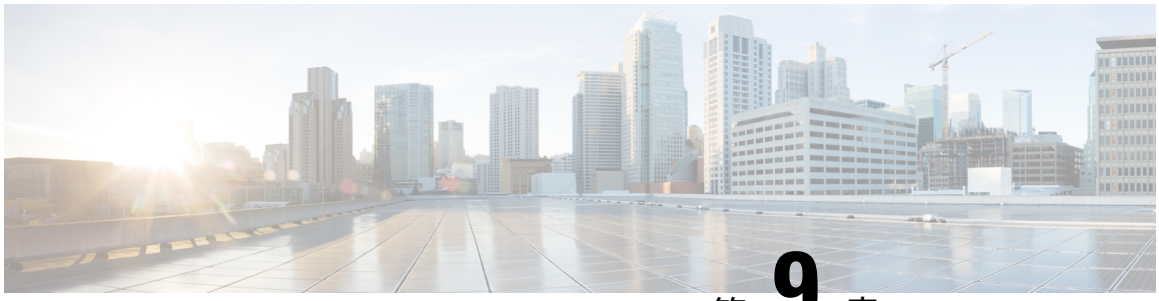
次の REST API の例では、MAC アドレスに `00:00:00:00:00:00` を指定することで、レイヤ 3 ポリシーベースリダイレクト先の動的 MAC アドレス検出を有効にします。

```
<vnsSvcRedirectPol AnycastEnabled="no" destType="L3"
  dn="uni/tn-t0/svcCont/svcRedirectPol-TEST-PBR-POL" hashingAlgorithm="sip-dip-prototype"

  maxThresholdPercent="0" minThresholdPercent="0" name="TEST-PBR-POL"
  programLocalPodOnly="no" resilientHashEnabled="no" srcMacRewriteEnabled="no"
```

```
  thresholdDownAction="permit" thresholdEnable="no" userdom=":all:common:">
    <vnsRsIPSLAMonitoringPol tDn="uni/tn-t0/ipslaMonitoringPol-l3ping"
      userdom=":all:common:"/>
    <vnsRedirectDest ip="11.2.2.100" ip2="0.0.0.0" mac="00:00:00:00:00:00" podId="1"
      userdom=":all:common:">
        <vnsRsRedirectHealthGroup tDn="uni/tn-t0/svcCont/redirectHealthGroup-Test-HG"
          userdom=":all:common:"/>
    </vnsRedirectDest>
</vnsSvcRedirectPol>
```

または、mac に空の値を指定できます。

```
   <vnsRedirectDest ip="11.2.2.100" ip2="0.0.0.0" mac="" podId="1" userdom=":all:common:">
```



第 9 章

Direct Server Return の設定

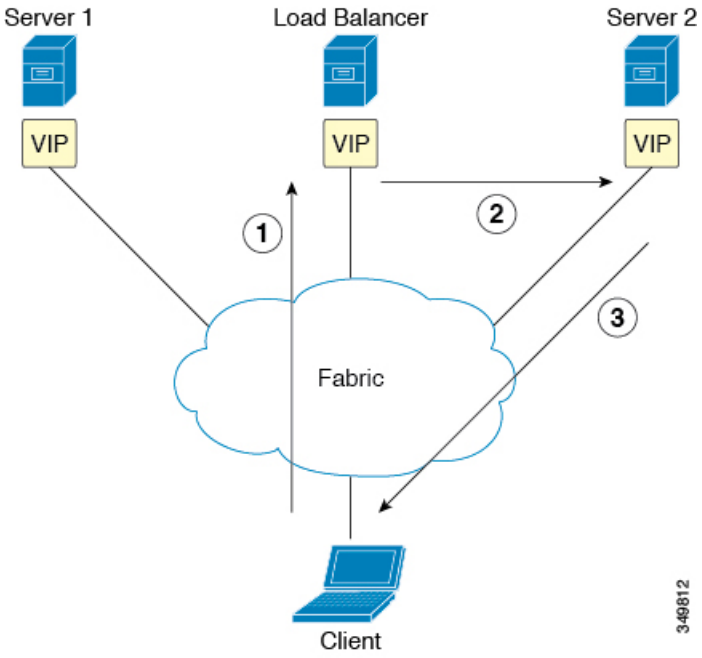
Direct Server Return について

Didrect Server Return 機能により、サーバはロード バランサを通過する必要なく、クライアントに直接応答できます。これにより、サーバからクライアントへのパスにおけるボトルネックが解消されます。従来のロードバランサの導入では、ロードバランサは、クライアントとサーバとの通信のパス（クライアントからサーバへの要求パスとサーバからクライアントへの応答パスの両方）に存在します。クライアントからサーバ方向の要求内のデータの量は比較的少ないものの、サーバからクライアントへの応答トラフィックはかなり大きく、クライアントからサーバへの要求データの約10倍になります。この大量の応答トラフィックがあるパス内のロード バランサがボトルネックになり、通信に悪影響を及ぼします。

Direct Server Return の導入では、ロード バランサとサーバとで仮想 IP アドレスが共有されます。クライアントは、ロード バランサに到達することを目的とした仮想 IP アドレスに常に要求を送信し、また、サーバからクライアントへの直接応答ではこの仮想 IP アドレスを送信元アドレスとして使用します。IP 送信元アドレスのデータパスの取得が有効になっているCisco Application Centric Infrastructure（ACI）は、サーバーからクライアントへのトラフィックの仮想 IP アドレスを取得する際に問題を引き起こし、クライアントからロード バランサへの要求トラフィックを途絶させることになります。Direct Server Return の導入を適切に動作させるには、ACI ファブリックは通信中のエンドポイント間の要求と応答のトラフィックを目的の宛先に正しく配信されるようにする必要があります。これには、リーフ上でのデータパス IP アドレスの取得を、クライアントからロードバランサへのトラフィック、ロードバランサからサーバへのトラフィック、およびサーバからクライアントへのトラフィックに割り込みを生じさせないように制御することが必要です。

次の図に、Direct Server Return の導入のデータ パスを示します。

図 *22 : Direct Server Return* の全体的なフロー



1. ロード バランサとすべてのバックエンド サーバが仮想 IP アドレスで設定されています。ロード バランサのみが、この仮想 IP アドレス宛の Address Resolution Protocol（ARP）要求に応答します。クライアント要求のロード バランシング後に、ロード バランサはパケット内の宛先 MAC アドレスを書き換えて、その MAC アドレスをバックエンド サーバの 1 つに転送します。
2. 仮想 IP アドレスはバックエンド サーバ上に設定されますが、ARP が無効になっているため、この仮想 IP アドレス宛の ARP 要求にバックエンド サーバは応答できません。
3. サーバはリターン トラフィックをクライアントに直接送信してロード バランサをバイパスします。

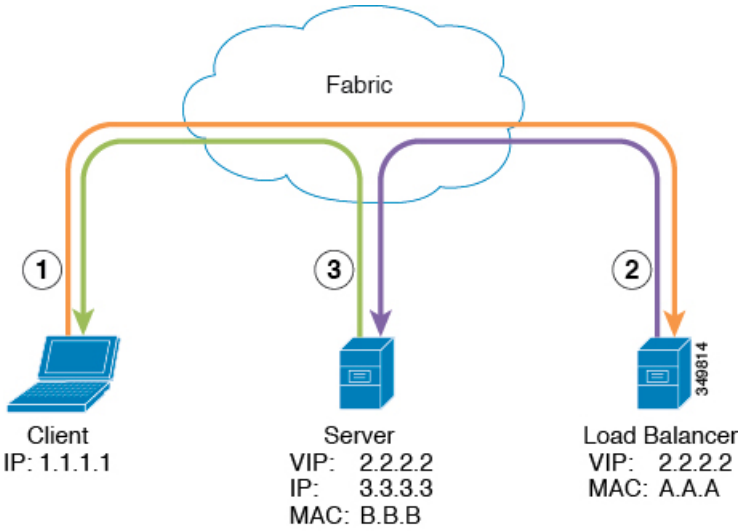
レイヤ 2 の Direct Server Return

レイヤ 2 の Direct Server Return は一般的な導入または従来型の導入であり、ダイレクト ルーティング、SwitchBack、または nPath とも呼ばれます。この導入では、ロード バランサとサーバで仮想 IP アドレスが共有されます。ロード バランサとサーバはレイヤ 2 隣接である必要があります。レイヤ 2 の Direct Server Return の導入には、次の制限があります。

- サーバ配置の柔軟性が失われる
- クライアントの仮想 IP アドレス要求への Address Resolution Protocol（ARP）応答を抑制するために、追加のサーバ設定が必要になる
- ポート選択はレイヤ 3 で行われ、プロトコルに依存する。ポート選択はレイヤ 2（サーバ通信に対するロード バランサ）で行われない

レイヤ 2 の Direct Server Return の導入には、次のトラフィック フローがあります。

図 *23* : レイヤ *2* の *Direct Server Return* のトラフィック フロー



1. クライアントからロード バランサへ

Source IP Address	1.1.1.1
Destination IP Address	2.2.2.2
宛先 MAC アドレス	A.A.A

2. ロード バランサからサーバへ

Source IP Address	1.1.1.1
Destination IP Address	2.2.2.2
宛先 MAC アドレス	B.B.B

3. サーバからクライアントへ

Source IP Address	2.2.2.2
Destination IP Address	1.1.1.1
宛先 MAC アドレス	デフォルト ゲートウェイの MAC アドレス

でのレイヤ2DirectServerReturnの導入についてCiscoApplicationCentric Infrastructure

次の情報は、Cisco Application Centric Infrastructure（ACI）でのレイヤ 2 Direct Server Return の導入に当てはまります。

- 仮想 IP アドレス（2.2.2.2）は ACI ファブリック内を移動する
  - 同じ送信元仮想 IP アドレス（2.2.2.2）を持つロード バランサからサーバおよびサーバからクライアントへのトラフィック
  - サーバからクライアントへのトラフィックはルーティングされ、トラフィックはファブリック内のゲートウェイ MAC アドレス宛になる
  - サーバからの送信元 IP アドレスのデータ パスの取得はファブリック内の仮想 IP アドレスに移動する
- 異なる送信元から表示されるクライアント IP アドレス（1.1.1.1）についての問題はない
  - クライアント IP アドレスはファブリック内のクライアントとロード バランサの両方からの送信元 IP アドレスとして表示される
  - ロード バランサとサーバは、レイヤ 2 隣接であり、ロード バランサからサーバへのトラフィックはレイヤ 2 に転送される
  - ファブリック内のレイヤ 2 転送トラフィックからのデータパス IP アドレスの取得はない
  - クライアント IP アドレスがファブリック内のロード バランサからの送信元 IP アドレスとして表示された場合も、クライアント IP アドレスは取得されない

Direct Server Return の設定に関する注意事項と制約事項

Direct Server Return を展開する際には、次の注意事項と制約事項に従ってください:

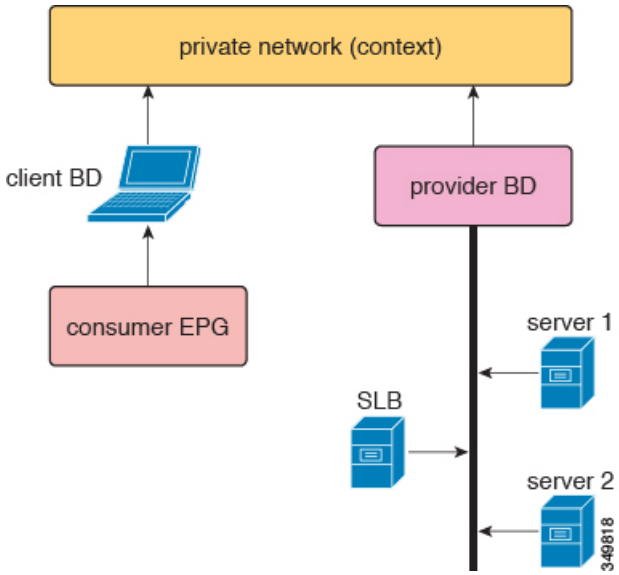
- VIP が展開される VRF は、「強制（enforced）」モードに設定する必要があります。
- VRF は「入力（ingress）」適用に設定する必要があります。
- 共有サービスは、この構成ではサポートされていません。
- EP 移動検出モード：ブリッジドメインに対して GARP ベースの検出を有効にする必要があります。
- ブリッジ ドメインに対してユニキャストルーティングを有効にする必要があります。
- VIP がある EPG には、それに関連付けられている契約が必要です (契約はハードウェアの設定を進めます)。

- レイヤ 4 ～ レイヤ 7 VIP オプションは、EPG でのみ設定できますが、VRF（vzAny とも呼ばれる）の EPG コレクションでは設定できません。
- クライアントから VIP へのトラフィックは、常にプロキシスパインを通過する必要があります。
- ロードバランサは、ワンアームモードである必要があります。
- サーバとロード バランサ EPG を同じデバイス上に配置するか、ロード バランサ EPG をすべてのサーバ EPG ToR に展開する必要があります。
- サーバー EPG とロードバランサ EPG は、同じブリッジドメインにある必要があります。
- マイクロセグメント化された EPG または対応するベース EPG でのレイヤ 4 ～レイヤ 7 の仮想 IP (VIP) アドレスの設定はサポートされていません。

サポートされている Direct Server Return の設定

次の図に、サポートされている Direct Server Return の設定を示します。

図 *24* : サポートされている *Direct Server Return* の設定



サポートされている設定に次の情報が適用されます。

- サーバ ロード バランサとサーバは同じサブネットとブリッジ ドメインにある
- サーバ ロード バランサは 1 ARM モードで動作する必要があり、サーバ ロード バランサの内部レッグと外部レッグは同じブリッジ ドメインを指している必要がある
- コンシューマ エンドポイント グループとプロバイダー エンドポイント グループは、同じプライベート ネットワークの下にある必要がある。共有サービス設定はサポートされていない

静的なサービス導入のための Direct Server Return の XML POST の例

次の XML POST は、ダイレクトサーバーリターン (DSR) の静的サービス展開の例です。

```
<fvAp name="dev">
      <fvAEPg name="loadbalancer">
        <fvRsDomAtt tDn="uni/phys-{{tenantName}}"/>
        <fvRsBd tnFvBDName="lab"/>
        <fvVip addr="121.0.0.{{net}}" />
        <fvRsPathAtt tDn="topology/pod-1/paths-104/pathep-[eth1/1]" encap="vlan-33" />
        <fvRsProv tnVzBrCPName="loadBalancer"/>
        <fvRsCons tnVzBrCPName="webServer"/>
      </fvAEPg>
        <fvAEPg name="webServer">
          <fvRsDomAtt tDn="uni/phys-{{tenantName}}"/>
            <fvRsBd tnFvBDName="lab"/>
          <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/1]" encap="vlan-34"/>

            <fvRsProv tnVzBrCPName="webServer"/>
        </fvAEPg>
      <fvAEPg name="client">
        <fvRsDomAtt tDn="uni/phys-{{tenantName}}"/>
        <fvRsBd tnFvBDName="lab"/>
        <fvRsPathAtt tDn="topology/pod-1/paths-103/pathep-[eth1/4]" encap="vlan-1114"/>
        <fvRsCons tnVzBrCPName="loadBalancer"/>
      </fvAEPg>
</fvAp>
```

DSR 設定は、レイヤ 4 ～ レイヤ 7 の仮想 IP アドレスが展開されている EPG を持つすべてのトップオブラックスイッチ (ToR)、またはレイヤ 4 ～レイヤ 7 の仮想 IP が展開されている EPG とコントラクトしている EPG に、コントラクトの方向に関係なくダウンロードされます。この例では、DSR 仮想 IP アドレス構成が ToR ノード 101、103、104 にダウンロードされます。ノード 104 には、レイヤ 4 ～ レイヤ 7 の仮想 IP アドレスが設定されたロードバランサ EPG があります。ノード 101 および 103 には、ロードバランサ EPG とのコントラクトを持つ Web サーバーまたはクライアント EPG があります。

DSR 構成をダウンロードしたすべての ToR は、データパスからレイヤ 4 ～ レイヤ 7 の仮想 IP アドレスを学習しません。また、このような ToR は、他の EPG からレイヤ 4 ～ レイヤ 7 の仮想 IP アドレスを学習しません。これは、Address Resolution Protocol（ARP）、Gratuitous Address Resolution Protocol (GARP)、または IPv6 ネイバー探索 (ND) を使用する場合も同様です。たとえば、ToR は、コントロールプレーン経由でロードバランサ EPG からレイヤ 4 ～ レイヤ 7 の仮想 IP アドレスのみを学習します。この制限は、Web サーバーで ARP を抑制し忘れた場合などに、Web サーバー EPG からのレイヤ 4 ～ レイヤ 7 の仮想 IP アドレスを誤って学習することを防止するのに有効です。

静的なサービス導入のための Direct Server Return

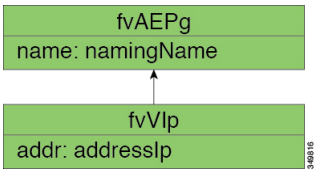
静的なサービス導入モードでは、適切なアプリケーション エンドポイント グループとコントラクトをホップごとに作成することによって、サービス フローを設定します。

静的なサービス導入の論理モデル用の Direct Server Return

アプリケーション エンドポイント グループ（fvAEPg）の下に fvVip オブジェクトを使用することによって、ロード バランサが使用する仮想 IP アドレスを設定できます。

次の図に、静的なサービス導入の論理モデルを示します。

図 *25 :* 静的なサービス導入の論理モデル



サービス グラフを挿入するための Direct Server Return

Cisco Application Centric Infrastructure（ACI）は、サービスグラフを使用してサービスの挿入を自動化します。このモードでは、サービスデバイスレッグ用に作成されるエンドポイントグループ（内部および外部エンドポイントグループなど） は、 Cisco ACI によってオペレータを構成することなく作成されます。

サービス グラフの挿入では、次の XML POST の例に示すように、サービス デバイスの適切な論理インターフェイス コンテキストの下に仮想 IP アドレスを設定する必要があります。

```
<vnsLDevCtx ctrctNameOrLbl="webCtrct"
  graphNameOrLbl="G1"
  nodeNameOrLbl="SLB">
    <vnsRsLDevCtxToLDev tDn="uni/tn-t1/lDevVip-InsiemeCluster"/>
    <vnsLIfCtx connNameOrLbl="inside">
        <vnsRsLIfCtxToBD tDn="uni/tn-t1/BD-t1BD1"/>
        <vnsRsLIfCtxToLIf tDn="uni/tn-t1/lDevVip-InsiemeCluster/lIf-inside"/>
    </vnsLIfCtx>
    <vnsLIfCtx connNameOrLbl="outside">
        <vnsRsLIfCtxToBD tDn="uni/tn-t1/BD-t1BD1"/>
        <vnsRsLIfCtxToLIf tDn="uni/tn-t1/lDevVip-InsiemeCluster/lIf-outside"/>
        <vnsSvcVip addr="9.9.9.9" />
        <vnsSvcVip addr="11.11.11.11" />
    </vnsLIfCtx>
</vnsLDevCtx>
```

この要求の例では、2 つの仮想 IP アドレス（9.9.9.9 と 11.11.11.11）をサーバ ロード バランサの外部レッグ上に設定します。仮想 IP アドレスの定義は、静的な Direct Server Return 設定と同様に、エンドポイント グループの下ではなく、LIfCtx の下になります。これは、静的サービスの導入の場合とは異なり、サービス グラフの場合は、オペレータにデバイス レッグのエンドポイント グループへの直接アクセス権がないためです。

Direct Server Return 共有レイヤ 4 ～ レイヤ 7 サービスの設定

サービスデバイスを共通のテナントまたは管理テナントに設定した場合、暗黙モデルには若干の違いがあります。vnsEPpInfo の代わりに、サービス仮想 IP アドレスの更新管理対象オブジェ

クトが vnsREPpInfo の子として作成されます。1 つの vnsSvcEpgCont の管理対象オブジェクトが vnsRsEPpInfo ごとに作成されて複数のテナント間で共有 SvcVip を追跡します。

Direct Server Return 用の Citrix サーバ ロード バランサの設定

次に、Direct Server Return 用に Citrix サーバ ロード バランサを設定する方法の概要を示した手順を説明します。

ステップ 1 バックエンド サーバがパケットを受け入れるようにバックエンド サーバのループバックに仮想 IP アドレスを設定します。

ステップ 2 バックエンド サーバの仮想 IP アドレスに対する Address Resolution Protocol（ARP）応答を無効にします。

ステップ 3 必要に応じて、ロードバランシング仮想サーバにバインドされたサービスのプロキシ ポートを無効にします。プロキシ ポートはデフォルトで無効になっています。

ステップ 4 ロード バランシング仮想サーバの m パラメータを「MAC」に設定します。

ステップ 5 グローバルか、またはサービスごとに USIP モードを有効にします。

ステップ 6 「L3」モード、「USNIP」モード、および「MBF」モードを有効にします。

ステップ 7 バックエンド サーバのルートを直接インターネットに到達できるように設定します。

Direct Server Return 用の Linux サーバの設定

次に、Direct Server Return 用に Linux サーバを設定する方法の概要を示した手順を説明します。

ステップ 1 次のコンテンツを使用し、Centos 内に /etc/sysconfig/network-scripts/ifcfg-lo ファイルを作成して、ループバック インターフェイス上に仮想 IP アドレスを設定します。

```
DEVICE=lo:1
IPADDRESS=10.10.10.99
NETMASK=255.255.255.255
NETWORK=10.10.10.99
BROADCAST=10.10.10.99
ONBOOT=yes
NAME=loopback
```

この例では、10.10.10.99 が仮想 IP アドレスです。

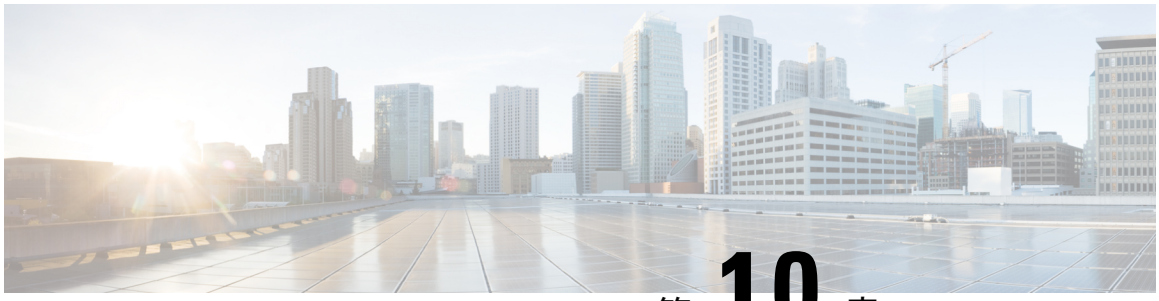
ステップ 2 クライアント要求への応答に使用するサーバ インターフェイスの arp_ignore と arp_announce の値を設定します。

```
echo 1 > /proc/sys/net/ipv4/conf/eth1/arp_ignore
echo 2 > /proc/sys/net/ipv4/conf/eth1/arp_announce
```

この例では、eth1 がクライアント要求への応答に使用するサーバ インターフェイスです。

ARP の設定の詳細については、次の Linux 仮想サーバの Wiki ページを参照してください。

http://kb.linuxvirtualserver.org/wiki/Using_arp_announce/arp_ignore_to_disable_ARP



第 10 章

コピー サービスの設定

コピー サービスについて

すべてのトラフィックを複製する SPAN とは異なり、 Cisco Application Centric Infrastructure (ACI) のコピー サービス機能は、契約での仕様に従って、エンドポイント グループ間のトラフィックのうちコピーの部分だけを選択的に有効にします。ブロードキャスト、不明なユニキャストとマルチキャスト (BUM)、および契約の対象外であるコントロール プレーン トラフィックは、コピーされません。対照的に、SPAN は、エンドポイント グループ、アクセス ポートまたはアップリンク ポートから発するすべてのトラフィックをコピーします。SPAN とは異なり、コピーサービスは、コピーされたトラフィックにヘッダーを追加しません。コピーサービスのトラフィックは、通常のトラフィックの転送への影響を最小限に抑えるため、スイッチ内で内部的に管理されます。

コピー サービスは、コピーされるトラフィックの宛先としてコピー クラスタを指定する、レイヤ 4 ～ レイヤ 7 サービス グラフ テンプレートの一部として構成されます。コピー サービスはサービス グラフ内の異なるホップにタップすることができます。たとえば、コピー サービスは、コンシューマ エンドポイント グループとファイアウォール プロバイダ エンドポイントの間のトラフィック、またはサーバのロードバランサとファイアウォールの間のトラフィックを選択することができます。コピー クラスタは、テナント間で共有することができます。

コピー サービスを使用するには、以下のタスクを実施する必要があります:

- 送信元と宛先エンドポイント グループを特定します。
- 情報カテゴリ、および契約フィルタで許可されている内容に従って、コピー対象を指定する契約を構成します。
- ターゲット デバイスを特定するレイヤ 4 ～ レイヤ 7 のコピー デバイスを構成し、それらが接続するポートを指定します。

- コピー サービスをレイヤ 4 ～ レイヤ 7 サービス グラフ テンプレートの一部として使用します。
- どのデバイスがサービス グラフからのトラフィックを受信するかを指定する、デバイス選択ポリシーを構成します。デバイス選択ポリシーを構成する際には、契約、サービス グラフ、コピー クラスタ、およびコピー デバイス内のクラスタ論理インターフェイスを指定します。

コピー サービスの制限

コピー サービス機能を使用する場合、次の制限が適用されます:

- コピー サービスは、N9K-9300-EX と -FX リーフ スイッチでのみサポートされます。
- ローカルおよびリモートのアナライザ ポートにコピーされるデータ パス トラフィックについては、コピーされたトラフィックではサービス クラス (CoS) および差別化サービス コード ポイント (DSCP) の値が保持されません。これは、コピー アクションの契約が、実際の COS または DSCP 値の変更の前後に、入力または出力 TOR のいずれかで問題となる可能性があるからです。

  特定のエンドポイント入力方向での、データ パスのトラフィックにポリシーを適用する際、トラフィックは、実際の着信トラフィックにポリシーが適用される前にコピーされます。これは、N9K-93108TC-EX および N9K-93180YC-EX スイッチでの ASIC の制限のためです。
- コピー サービスは、コピー クラスタごとに 1 つのデバイスだけをサポートします。
- コピー クラスタは、1 つの論理インターフェイスだけをサポートします。
- コンシューマ エンドポイントまたはプロバイダー エンドポイントでのコピー アナライザは、N9K-93108TC-EX および N9K-93180YC-EX スイッチでのみ設定できます。N9K-93128TX、N9K-9396PX、または N9K-9396TX スイッチでコピー アナライザを設定すると、エラーが発生します。
- `tn-common/ctx-copy` VRF インスタンスは、コピー VRF インスタンスとも呼ばれ、コピー サービスのためのシステム予約コンテキストです。コピー VRF インスタンスは、ブートアップ シーケンス中に、システムにより自動設定されます。コピー VRF インスタンスをユーザが設定または削除することはできません。
- vzAny 契約でのコピー サービスはサポートされていません。
- フローの各方向に別々のコピーデバイスを使用する場合は、2 つの異なる単方向フィルタが必要です。

GUI を使用したコピー サービスの設定

この手順では、GUI を使用して、コピー サービスを設定します。

（注） コピー デバイスを設定すると、context aware パラメータは使用されません。context aware パラメータには `single context` というデフォルト値がありますが、これは無視されます。

ステップ 1 1 つ以上の コピー デバイスを作成します。

コピー デバイスの作成についての詳細は、GUI を使用したコピーデバイスの作成 （167 ページ）を参照してください。

ステップ 2 コピー サービスで使用するサービス グラフ テンプレートを作成します。

サービス グラフ テンプレートの作成についての詳細は、GUI でサービスグラフテンプレートを構成する（51 ページ）を参照してください。

a) 1 つ以上のサービス ノードを作成する場合は、**Device Clusters** セクションから、レイヤ 4 ～ レイヤ 7 サービス デバイスを、コンシューマ エンドポイント グループとプロバイダー エンドポイント グループの間にドラッグします。

b) **Device Clusters** セクションから、コピー デバイスを、任意の 2 つのオブジェクトの間にドラッグして 1 つ以上のコピー ノードを作成します。

コピーデバイスをドロップした場所が、コピーデバイスがトラフィックをコピーする、データ フロー内のポイントとなります。

ステップ 3 レイヤ 4 ～ レイヤ 7 サービス グラフ テンプレートを適用します。

サービス グラフ テンプレートを適用する方法の詳細については、GUI を使用したエンドポイント グループへのサービス グラフ テンプレートの適用 （53 ページ）を参照してください。

GUI を使用したコピーデバイスの作成

コピー デバイスは、copy ノードを作成するコピー サービス機能の一部として使用されます。コピーのノードは、トラフィックをコピーするエンドポイント グループ間のデータ フローのどの時点を指定します。

この手順では、コピー デバイスの作成のみを行います。コピー サービス機能を使用するために必要なその他の設定は行いません。コピー サービスの設定の詳細については、GUI を使用したコピー サービスの設定 （166 ページ）を参照してください。

始める前に

テナントを作成しておく必要があります。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ウィンドウで、**Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Devices** を選択します。

ステップ 4 [Work] ウィンドウで、**Actions** > **Create Copy Devices** を選択します。

ステップ 5 **Create Copy Devices** ダイアログボックスの **General** セクションで、次のフィールドを設定します:

名前	説明
[名前（Name）] フィールド	コピーデバイスの名前を入力します。
Device Type ボタン	デバイス タイプです。コピー デバイスは、物理デバイスに限られます。
Physical Domain ドロップダウンリスト	デバイスの物理ドメインを選択します。

ステップ 6 **Device 1** セクションで、**+** をクリックしてデバイス インターフェイスを追加し、以下のフィールドを設定して、 **Update** をクリックします:

名前	説明
[名前（Name）] フィールド	デバイス インターフェイスの名前を入力します。
Path ドロップダウン リスト	使用するデバイス インターフェイスのポート、ポート チャネル、または仮想ポートチャネルを選択します。コピーデバイスは、そのポート、ポート チャネルまたは仮想ポート チャネルに接続し、そこからトラフィックをコピーします。

ステップ 7 **Cluster** セクションで、**+** をクリックしてクラスタ インターフェイスを追加し、以下のフィールドを設定して、**Update** をクリックします:

名前	説明
[名前（Name）] フィールド	クラスタ インターフェイスの名前を入力します。
Concrete Interfaces ドロップダウンリスト	使用するクラスタ インターフェイスの、1 つ以上の具体的なインターフェイスを選択します。

Encap フィールド	カプセル化で使用する VLAN を入力します。VLAN 名の書式は次のとおりです:
	`vlan-#`
	# は VLAN の ID です。次に例を示します:
	`vlan-12`

ステップ 8 [送信（Submit）] をクリックします。

NX-OS スタイルの CLI を使用したコピー サービスの設定

この手順では、CLI を使用してコピー サービスを設定する例を提供します。

（注） コピー デバイスを設定すると、context aware パラメータは使用されません。context aware パラメータには `single context` というデフォルト値がありますが、これは無視されます。

ステップ 1 コピー クラスタを作成します。

例：

```
l4l7 cluster name Copy_1 type physical vlan-domain phys_scale_copy service COPY function none
  cluster-device Copy_1_Device_1
  cluster-interface Tap_copy vlan 3644
    member device Copy_1_Device_1 device-interface int1
      interface ethernet 1/15 leaf 104
      exit
    member device Copy_1_Device_1 device-interface int2
      interface ethernet 1/15 leaf 105
      exit
    member device Copy_1_Device_1 device-interface int3
      interface ethernet 1/20 leaf 105
      exit
    exit
  exit
```

ステップ 2 抽象グラフとデバイスのコンテキストを作成し、グラフを適用します。

例：

```
l4l7 graph g5 contract c5
  service CP1 device-cluster-tenant t1 device-cluster Copy_1 mode OTHER service COPY
    connector copy cluster-interface Tap_copy
      exit
    exit
  connection C1 terminal consumer terminal provider copyservice CP1 connector copy
  Exit
```

ステップ 3 グラフを契約を接続します。

例：

```
contract c5
  scope tenant
  subject Subject
    access-group default both
    l4l7 graph g5
    exit
  Exit
```

ステップ 4 契約をエンドポイント グループを接続します。

例：

```
  epg epg2210
    bridge-domain member bd5
```

```
  contract consumer c5
  exit
epg epg2211
  bridge-domain member bd5
  contract provider c5
  Exit
```

例

次の例では、両側でコピー デバイスとファイアウォール サービス グラフを作成します。

```
  tenant tenant_cmd_line
    l4l7 graph graph_fire contract fire
     service Fire device-cluster-tenant tenant_cmd_line device-cluster Fire mode FW_ROUTED

        connector consumer cluster-interface Outside_cmdline
          bridge-domain tenant tenant_cmd_line name Consumer_BD_1
          exit
        connector provider cluster-interface Inside_cmdline
          bridge-domain tenant tenant_cmd_line name Provider_BD1
          exit
        exit
      service CP2 device-cluster-tenant tenant_cmd_line device-cluster copy1 mode OTHER
       service COPY
        connector copy cluster-interface int1
          exit
        exit
      service CP3 device-cluster-tenant tenant_cmd_line device-cluster copy1 mode OTHER
       service COPY
        connector copy cluster-interface int1
          exit
        exit
      connection C1 terminal consumer service Fire connector consumer copyservice CP2
       connector copy
      connection C2 terminal provider service Fire connector provider copyservice CP3
       connector copy
      exit
    Exit
```

次の例では、すべてのリンクで接続されているコピーデバイスでワンアームモードでファイアウォールとロード バランスを作成します。

```
    l4l7 graph Graph_LB_Firewall contract c1_firewall
      service Fire device-cluster-tenant Tenant_Firewall_LB device-cluster Firewall_1
mode
       FW_ROUTED
        connector consumer cluster-interface Outside_Firewall
          bridge-domain tenant Tenant_Firewall_LB name BD1_Consumer
          exit
        connector provider cluster-interface Inside_Firewall
          bridge-domain tenant Tenant_Firewall_LB name BD2_Provider
          exit
        exit
      service LB device-cluster-tenant Tenant_Firewall_LB device-cluster LB_1 mode
ADC_ONE_ARM
        connector consumer cluster-interface LB_Inside
          bridge-domain tenant Tenant_Firewall_LB name BD2_Provider
          exit
        connector provider cluster-interface LB_Inside
```

```
      bridge-domain tenant Tenant_Firewall_LB name BD2_Provider
      exit
    Exit
 service CP6 device-cluster-tenant Tenant_Pass2 device-cluster Copy_pass2 mode OTHER

   service-type COPY
    connector copy cluster-interface tap_copy
      exit
    Exit
 service CP7 device-cluster-tenant Tenant_Pass2 device-cluster Copy_pass2 mode OTHER

   service-type COPY
    connector copy cluster-interface tap_copy
      exit
    Exit
 service CP8 device-cluster-tenant Tenant_Pass2 device-cluster Copy_pass2 mode OTHER

   service-type COPY
    connector copy cluster-interface tap_copy
      exit
    exit
  connection C1 terminal consumer service Fire connector consumer copyservice CP6
   connector copy
 connection C2 intra-service service1 Fire connector1 provider service2 LB connector2

   consumer copyservice CP7 connector copy
  connection C3 terminal provider service LB connector provider copyservice CP8
   connector copy
  exit
exit
```

REST API を使用してコピー サービスの設定

コピー デバイスは、copy ノードを作成するコピー サービス機能の一部として使用されます。コピーのノードは、トラフィックをコピーするエンドポイント グループ間のデータ フローのどの時点を指定します。

この手順では、REST API を使用してコピー サービスを設定する例を提供します。

（注） コピー デバイスを設定すると、context aware パラメータは使用されません。context aware パラメータには `single context` というデフォルト値がありますが、これは無視されます。

始める前に

テナントを作成しておく必要があります。

ステップ 1 コピー デバイスを作成します。

例：

```
<vnsLDevVip contextAware="single-Context" devtype="PHYSICAL" funcType="None" isCopy="yes"
  managed="no" mode="legacy-Mode" name="copy0" svcType="COPY" trunking="no">
    <vnsRsALDevToPhysDomP tDn="uni/phys-phys_scale_copy"/>
```

```
    <vnsCDev devCtxLbl="" name="copy_Dyn_Device_0" vcenterName="" vmName="">
        <vnsCIf name="int1" vnicName="">
            <vnsRsCIfPathAtt tDn="topology/pod-1/paths-104/pathep-[eth1/15]"/>
        </vnsCIf>
        <vnsCIf name="int2" vnicName="">
            <vnsRsCIfPathAtt tDn="topology/pod-1/paths-105/pathep-[eth1/15]"/>
        </vnsCIf>
    </vnsCDev>
    <vnsLIf encap="vlan-3540" name="TAP">
        <vnsRsCIfAttN tDn="uni/tn-t22/lDevVip-copy0/cDev-copy_Dyn_Device_0/cIf-[int2]"/>
        <vnsRsCIfAttN tDn="uni/tn-t22/lDevVip-copy0/cDev-copy_Dyn_Device_0/cIf-[int1]"/>
    </vnsLIf>
</vnsLDevVip>
```

ステップ 2 論理デバイス コンテキスト (デバイス選択ポリシーとも呼ばれる) を作成します。

例：

```
<vnsLDevCtx ctrctNameOrLbl="c0" descr="" graphNameOrLbl="g0" name="" nodeNameOrLbl="CP1">
    <vnsRsLDevCtxToLDev tDn="uni/tn-t22/lDevVip-copy0"/>
    <vnsLIfCtx connNameOrLbl="copy" descr="" name="">
        <vnsRsLIfCtxToLIf tDn="uni/tn-t22/lDevVip-copy0/lIf-TAP"/>
    </vnsLIfCtx>
</vnsLDevCtx>
```

ステップ 3 作成し、コピーするグラフ テンプレートを適用します。

例：

```
<vnsAbsGraph descr="" name="g0" ownerKey="" ownerTag="" uiTemplateType="UNSPECIFIED">
    <vnsAbsTermNodeCon descr="" name="T1" ownerKey="" ownerTag="">
        <vnsAbsTermConn attNotify="no" descr="" name="1" ownerKey="" ownerTag=""/>
        <vnsInTerm descr="" name=""/>
        <vnsOutTerm descr="" name=""/>
    </vnsAbsTermNodeCon>
    <vnsAbsTermNodeProv descr="" name="T2" ownerKey="" ownerTag="">
        <vnsAbsTermConn attNotify="no" descr="" name="1" ownerKey="" ownerTag=""/>
        <vnsInTerm descr="" name=""/>
        <vnsOutTerm descr="" name=""/>
    </vnsAbsTermNodeProv>
    <vnsAbsConnection adjType="L2" connDir="provider" connType="external" descr="" name="C1"
      ownerKey="" ownerTag="" unicastRoute="yes">
        <vnsRsAbsConnectionConns tDn="uni/tn-t22/AbsGraph-g0/AbsTermNodeCon-T1/AbsTConn"/>
        <vnsRsAbsConnectionConns tDn="uni/tn-t22/AbsGraph-g0/AbsTermNodeProv-T2/AbsTConn"/>
        <vnsRsAbsCopyConnection tDn="uni/tn-t22/AbsGraph-g0/AbsNode-CP1/AbsFConn-copy"/>
    </vnsAbsConnection>
    <vnsAbsNode descr="" funcTemplateType="OTHER" funcType="None" isCopy="yes" managed="no"
      name="CP1" ownerKey="" ownerTag="" routingMode="unspecified" sequenceNumber="0"
      shareEncap="no">
        <vnsAbsFuncConn attNotify="no" descr="" name="copy" ownerKey="" ownerTag=""/>
        <vnsRsNodeToLDev tDn="uni/tn-t22/lDevVip-copy0"/>
    </vnsAbsNode>
</vnsAbsGraph>
```

ステップ 4 エンドポイントのグループに関連付けられている契約でコピー グラフに関係を定義します。

例：

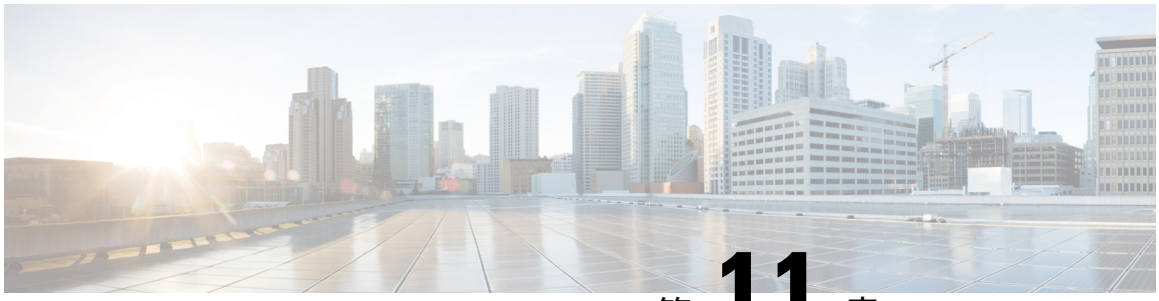
```
<vzBrCP descr="" name="c0" ownerKey="" ownerTag="" prio="unspecified" scope="tenant"
  targetDscp="unspecified">
    <vzSubj consMatchT="AtleastOne" descr="" name="Subject" prio="unspecified"
      provMatchT="AtleastOne" revFltPorts="yes" targetDscp="unspecified">
        <vzRsSubjFiltAtt directives="" tnVzFilterName="default"/>
        <vzRsSubjGraphAtt directives="" tnVnsAbsGraphName="g0"/>
```

```
    </vzSubj>
</vzBrCP>
```

ステップ 5 エンドポイント グループを契約を接続します。

例：

```
<fvAEPg name="epg2860">
    <fvRsCons tnVzBrCPName="c0"/>
    <fvRsBd tnFvBDName="bd0"/>
    <fvRsDomAtt tDn="uni/phys-phys_scale_SB"/>
    <fvRsPathAtt tDn="topology/pod-1/paths-104/pathep-[PC_int2_g1]" encap="vlan-2860"
      instrImedcy="immediate"/>
</fvAEPg>
<fvAEPg name="epg2861">
    <fvRsProv tnVzBrCPName="c0"/>
    <fvRsBd tnFvBDName="bd0"/>
    <fvRsDomAtt tDn="uni/phys-phys_scale_SB"/>
    <fvRsPathAtt tDn="topology/pod-1/paths-105/pathep-[PC_policy]" encap="vlan-2861"
      instrImedcy="immediate"/>
</fvAEPg>
```



第 11 章

レイヤ 4 ～ レイヤ 7 リソース プールの設定

レイヤ 4 ～ レイヤ 7 リソース プールについて

レイヤ 4 ～ レイヤ 7 リソース プールは、レイヤ 4 ～ レイヤ 7 サービス デバイスの展開に関し、関係する設定をまとめます。関連する設定がパッケージとしてまとめられるので、レイヤ 4 ～ レイヤ 7 サービス デバイスを展開するための Cisco Application Centric Infrastructure (Cisco ACI) Windows Azure パック統合などのような、オーケストレーション レイヤで使用することができます。

外部およびパブリック IP アドレス プールについて

Cisco APIC リリース 3.0(x) 以前で作成されたレイヤ 4 ～ レイヤ 7 リソース プールの場合、パブリック IP アドレス プールと外部 IP アドレス プールは全く同じものであり、単に外部としてマークされているだけです。Cisco APIC リリース 3.1(x) 以降で作成されたレイヤ 4 ～ レイヤ 7 リソース プールの場合、これら 2 つのタイプのアドレス プールは分けられており、区別されます。外部 IP アドレス プールは、レイヤ 4 ～ レイヤ 7 デバイスの外部インタフェースおよび L3Out SVI の IP 割り当てのために使用されます。VPC を通してファブリックに接続するレイヤ 4 ～ レイヤ 7 デバイスの場合、 L3Out の設定のために 3 つの IP アドレス (サイド A のプライマリ IP アドレス、サイド B のプライマリ IP アドレス、およびセカンダリ IP アドレス) が消費されます。一方、ポート チャネルとシングル インターフェイス接続の場合、2 つの IP アドレス (プライマリ IP アドレスおよびセカンダリ IP アドレス) を消費します。

パブリック IP アドレス プールは、ダイナミック NAT の IP アドレスの割り当て (テナント VRF ごとに 1 つ)、ロード バランサ、仮想 IP アドレス (テナント EPG ごとに 1)、およびその他のパブリック NAT IP アドレスを割り当てるために用いられます。

2 つの IP アドレスのタイプを分けることにより、Cisco APIC 管理者は、次のことを行えます。

- IP プールの中でパブリックとマークされている IP アドレスだけをエクスポートします。デバイスレベルのインターフェイス IP アドレスを隠すことができます。
- パブリック IP アドレス プールの IP アドレスのさまざまなブロックに対し、アドレスを取得して、共通のテナント L3Out で利用可能になったときに段階的に追加を行えます。

外部レイヤ 3 ルーテッド ドメインおよび関連付けられた VLAN プールについて

外部 L3Out ルーテッド ドメインは、レイヤ 4 ～ レイヤ 7 デバイスの内部および外部コネクタの両方に L3Out をプロビジョニングするために使用されます。これらの L3Out は、トラフィックが Cisco Application Centric Infrastructure (Cisco ACI) ファブリックの外部から発信すること、および Cisco ACI ファブリック内部のリソースに到達することを可能にします。また、L3Outs は、トラフィックが Cisco ACI ファブリックの内部から発信すること、および Cisco ACI ファブリックの外部に到達することも可能にします。L3Out ルーテッド ドメインに関連付けられる VLAN プール内の VLANは、レイヤ 4 ～ レイヤ 7 サービス デバイスが接続されている特定のリーフまたは VPC リーフスイッチ ペアに対して一意のものである必要があります。レイヤ 4 ～ レイヤ 7 サービス デバイスが複数のリーフまたは VPC リーフスイッチ ペアにわたるものである場合、この制限はそれらのリーフまたは VPC リーフスイッチ ペアにも及びます。

（注） いったんレイヤ 4 ～ レイヤ 7 リソース プールが使用されたら、VLAN ブロックを再設定したり、VLANプールから削除したりするべきではありません。拡張が必要な場合は、現在の VLAN ブロックに VLAN ブロックを追加できます。

VLAN プールのサイズについては、次の考慮点が:

- 外部 IP アドレス プールごとに、1 つの VLAN がダイナミックに割り当てられます。
- レイヤ 4 ～ レイヤ 7 リソース プールにアクセスする、テナント仮想フォワーディングおよびルーティング (VRF) ごとに、1 つの VLAN がダイナミックに割り当てられます。
- 外部ルーテッド ドメインおよび関連付けられている VLAN プールは、レイヤ 4 ～ レイヤ 7 リソース プール全体にわたって使用できます。

OSPF 外部ルーテッド ネットワークの概要

外部ルーテッド ネットワークの設定についての情報は、次の URL の テナントネットワークの外部の *Cisco APIC* レイヤ *3* を参照してください。

http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

GUI を使用してレイヤ 4 ～ レイヤ 7 リソース プールのための IP アドレス プールを作成する

次の手順では、いずれかの GUI モードを使用して、レイヤ 4 ～ レイヤ 7 リソース プールのための IP アドレス プールを作成します。

ステップ 1 メニュー バーで、**Tenants** > **Common** を選択します。

ステップ 2 **Navigation** ウィンドウで、**Tenant Common** > **IP Address Pools** を選択します。

ステップ 3 **Work** ウィンドウで、**Actions** > **Create IP Address Pool** を選択します。

ステップ 4 **Create IP Address Pool** ダイアログボックスで、必要に応じてフィールドに入力します。

Address Ranges には、ゲートウェイ アドレスを含めないでください。ゲートウェイ アドレスは、レイヤ 4 ～ レイヤ 7 デバイスの外部 L3Out のセカンダリ IP アドレスとして使用されます。これはパーベイシブ ゲートウェイになります。

例：

- **Name**—`ExtIPPool1`
- **Gateway Address**— `132.121.101.1/24`
- **Address Block**
  - **From**—`132.121.101.2`
  - **To**—`132.121.101.200`

ステップ 5 [送信（Submit）] をクリックします。

GUI を使用したレイヤ 4 ～ 7 リソース プールのダイナミック VLAN プールの作成

次の手順では、GUI モードを使用して、レイヤ 4 ～ レイヤ 7 のリソース プールのためにダイナミック VLAN プールを作成します。

ステップ 1 メニューバーで、**[Fabric]** > **[Access Policies]** を作成します。

ステップ 2 [Navigation] ウィンドウで、 **[Pools]** > **[VLAN]** の順に選択します。

ステップ 3 [Work] ウィンドウで、**[Actions]** > **[Create VLAN Pool]** の順に選択します。

ステップ 4 [Create VLAN Pool] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [Allocation Mode] ボタンでは、[Dynamic Allocation] をクリックします。

b) [Encap Blocks] テーブルで、[+] をクリックします。

c) [Create Ranges] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します:

- [Range] フィールドに、目的の VLAN 範囲を入力します。
- [Allocation Mode] ボタンでは、[Inherit alloc mode from parent] をクリックします。

d) [OK] をクリックします。

ステップ 5 [Create VLAN Pool] ダイアログボックスで、[Submit] をクリックします。

GUI を使用して、レイヤ 4 ～ レイヤ 7 のリソース プールのために外部ルーテッド ドメインを作成する

次の手順では、GUI モードを使用して、レイヤ 4 ～ レイヤ 7 のリソース プールのためにダイナミック VLAN プールを作成します。

ステップ 1 メニューバーで、**[Fabric]** > **[Access Policies]** を作成します。

ステップ 2 [Navigation] ウィンドウで、 **[Physical and External Domains]** > **[External Routed Domains]** を選択します。

ステップ 3 [Work] ウィンドウで、**[Actions]** > **[Create Layer 3 Domain]** を選択します。

ステップ 4 [Create Layer 3 Domain] ダイアログ ボックスで、次に指定されている点を除き、必要に応じてフィールドに入力します。

a) [Associated Attachable Entity Profile] ドロップダウンリストでは、すべてのレイヤ 4 ～ レイヤ 7 サービス デバイスの接続先となっている、アタッチ可能なエンティティのプロファイルを選択します。

b) [VLAN Pool] ドロップダウンリストでは、レイヤ 4 ～ レイヤ 7 リソース プールのために作成したダイナミック VLAN プールを選択します。

c) [Security Domains] テーブルで、必要なセキュリティ ドメインを追加します。

ステップ 5 [送信（Submit）] をクリックします。

レイヤ 4 ～ レイヤ 7 リソース プールで使用するレイヤ 4 ～ レイヤ 7 デバイスの準備

レイヤ 4 ～ レイヤ 7 デバイスの物理接続を設定するには、デバイス内のポート チャネルまたは VPC 設定に関して、各デバイスごとに適切な設定ガイドを参照してください。

（注） コンテキスト認識である ASA55xx ファイアウォール デバイスについて、パス設定は特定の物理 ASA55xx のすべての ASA コンテキストの間で整合性がある必要があります。異なるインターフェイスを使用して ASA コンテキストを設定することは、この設定では許可されていません。

レイヤ 4 ～ レイヤ 7 リソース プールで使用するレイヤ 4 ～ レイヤ 7 デバイスの APIC 設定の検証

次の手順では、レイヤ 4 ～ レイヤ 7 リソースプールで使用するレイヤ 4 ～ レイヤ 7 サービス デバイスの Cisco Application Policy Infrastructure Controller (Cisco APIC) 設定を、GUI モードを使用して検証します。

ステップ 1 メニュー バーで、 **Tenants** > **Common** を選択します。

ステップ 2 [Navigation] ウィンドウで、**Tenant** ***tenant_name*** > **Services** > **L4-L7** > **Devices** > ***ASA_or_NetScaler_logical_device_name*** > ***concrete_device_name*** を選択します。

ステップ 3 **Work** ウィンドウで、**Policy** タブを選択します。

ステップ 4 [インターフェイス（**Interfaces**）] テーブルで、少なくとも 2 つのインターフェイスがあり、それぞれがファブリック内の検証パス（ポート、ポートチャネル、vPC）にマッピングされていることを確認します。

ステップ 5 ASA または NetScaler ごとに、**Cluster > consumer** インターフェイスと **Cluster > provider** インターフェイスの両方が定義されていることを確認します。NetScalers が内部のロード バランシングで使用される場合

でも、そのような設定は、テナントがプライベートおよびパブリック両方の IP アドレス ロード バランシングで NetScaler を使用ことを許可するようにします。

ステップ 6 HA 設定では、クラスタ インターフェイスごとに 2 つの具体的なインターフェイスがあることを確認します。これにより、各ポート、ポートチャネル、vPC が正しく設定されます。

デバイス管理ネットワークとルートの構成

レイヤ 4 ～ レイヤ 7 デバイス上で管理ルートを構成し、直接アウト オブ バンドとなっているデフォルトのルートを削除する必要があります。

次の例では、 Cisco Application Policy Infrastructure Controller (Cisco APIC) の NX-OS スタイル CLI を使用して、ASA ファイアウォールの管理ルートを構成します:

```
apic1(config)# route management 10.24.24.0 255.255.255.0 172.0.0.1
```

次の例では、 Cisco APIC の NX-OS スタイル CLI を使用して、デフォルトのルートを削除します。

```
apic1(config)# no route 0.0.0.0 0.0.0.0 172.0.0.1
```

次の例では、Citrix NetScaler CLI を使用して、NetScaler アプリケーション配信コントローラ (ADC) のロード バランサの管理ルートを構成します:

```
> add route 10.24.24.0 255.255.255.0 172.0.0.1
```

次の例では、Citrix NetScaler CLI を使用して、デフォルト ルートを削除します:

```
> rm route 0.0.0.0 0.0.0.0 172.0.0.1
```

レイヤ 4 ～ レイヤ 7 リソース プールの作成

GUI を使用したレイヤ 4 ～ レイヤ 7 リソース プールの作成

次の手順では、GUI モードを使用してレイヤ 4 ～ レイヤ 7 リソース プールを作成します。いったんリソース プールに、テナントで使用するためのさまざまなコンポーネントを割り当てると、その後でリソース プールを変更することはできません。IP アドレス ブロックの追加、VLAN ブロックを追加して、ASA ファイアウォールまたは Citrix NetScaler などの論理デバイスの追加などの、メンテナンス タスクは実行できます。

ステップ 1 メニュー バーで、**[Tenants]** > **[Common]** を選択します。

ステップ 2 [Navigation] ペインで、 **[Tenant Common]** > **[Services]** > **[L4-L7]** > **[L4-L7 Resource Pools]** を選択します。

ステップ 3 **Work** ウィンドウで、**Actions** > **Create L4-L7 Resource Pool** を選択します。

ステップ 4 **Create L4-L7 Resource Pool** ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します:

a) **Private IP Address Subnet** フィールドで、内部デバイス インターフェイスの IP アドレス、内部 VIP アドレス、および内部 L3Out IP アドレスに使用されるサブネットを入力します。

b) **External IP Address Pool** ドロップダウンリストで、サービス グラフとデバイス全体で使用される IP アドレスの動的な割り当てに使用される IP アドレス プールを選択します。必要に応じて新しいIP アドレス プールを作成できます。**Connect Type** では、 **L3 External Network**を選択します。

c) **Public IP Address Pool** テーブルで、NAT IP アドレッシングと VIP アドレッシングで使用される IP アドレスの動的な割り当てに使用される IP アドレス プールを選択します。必要に応じて新しいIP アドレス プールを作成できます。**Connect Type** では、 **L3 External Network**を選択します。

d) **External Routed Domain** ドロップダウンリストで、このレイヤ 4 ～ 7 リソース プールで使用するために作成した外部ルーテッド ドメインを選択します。必要に応じて新しい外部ルーテッド ドメインを作成できます。

e) **外部ルーテッド ネットワーク** テーブルで、テナントが利用できる外部ルーテッド ネットワークを追加します。

最初の外部ルーテッド ネットワークは自動的に `Default` とマークされます。現時点では、デフォルトのルーテッド ネットワークのみが使用されます。

f) **L4-L7 Devices** テーブルに、このレイヤ 4 ～ レイヤ 7 リソース プールの一部となるレイヤ 4 ～ レイヤ 7 デバイスを追加します。

ステップ 5 [送信（Submit）] をクリックします。

NX-OS スタイル CLI を使用したレイヤ 4 ～ レイヤ 7 リソース プールの作成

このセクションでは、NX OS スタイルの CLI を使用してレイヤ 4 ～ レイヤ 7 リソース プールを設定するコマンドの例を示します。

ステップ 1 コンフィギュレーション モードを開始します。

```
apic1# configure
```

ステップ 2 テナント共通の設定モードを開始します。

```
apic1(config)# tenant common
```

ステップ 3 レイヤ 4 ～ レイヤ 7 リソース プールを指定します。

```
apic1(config)# l4l7 resource-pool <resource pool name>
```

ステップ 4 リソース プール バージョンを設定します。

```
apic1(config-resource-pool)# version normalized
```

（注） バージョンは次のとおりです。

- **クラシック**：Cisco Application Policy Infrastructure Controller (APIC) リリース 3.1(1) より前に作成されたリソースプールの場合。
- **正規化**：Cisco APIC リリース 3.1(1) 以降に作成されたリソースプールの場合。

ステップ 5 リソース プールにレイヤ 4 ～ レイヤ 7 デバイスを関連付けます。

```
apic1(config-resource-pool)# l4l7-cluster Dev-ASA-4
apic1(config-resource-pool)# l4l7-cluster Dev-MPX-4
```

ステップ 6 リソース プールに外部 IP アドレス プールとして IP アドレス プールを関連付けます。

```
apic1(config-resource-pool)# address-pool mininetExtPoolL3Ext l3-external
```

ステップ 7 (正規リソース プール）リソース プールにパブリック IP アドレス プールと IP アドレス プールを関連付けます。

```
apic1(config-resource-pool)# public-address-pool mininetPubPoolL3Ext l3-external
```

ステップ 8 外部ルーテッド ドメインに関連付けます。

```
apic1(config-resource-pool)# external-routed-domain L3ServicesDom
```

ステップ 9 リソー スプールのプライベート IP アドレスのサブネットを設定します。

```
apic1(config-resource-pool)# subnet 192.168.254.1/24
```

ステップ 10 共通テナントで L3Out EPG に関連付けます。

```
apic1(config-resource-pool)# l3out vpcDefaultInstP default
```

GUI を使用したレイヤ 4 ～ レイヤ 7 リソース プールの設定

リソース プール内のレイヤ 4 ～ レイヤ 7 リソース デバイスの設定

レイヤ 4 ～ レイヤ 7 デバイスをレイヤ 4 ～ レイヤ 7 リソース プールに追加する

（注） 専用 VLAN は、L3Out がテナントのため、そのプライベート VRF 内で作成されるたびに消費されます。レイヤ 3 ドメインに関連付けられているダイナミック VLAN プールは、リソース プールに追加されるデバイスに適合できるように、付加的な VLAN の追加を必要とする場合があります。

新しいレイヤ4～レイヤ7デバイスは、いつでもリソースプールに追加することができます。

ステップ 1 メニュー バーで、**[Tenants]** > **[Common]** を選択します。

ステップ 2 [Navigation] ペインで、 **[Tenant Common]** > **[Services]** > **[L4-L7]** > **[L4-L7 Resource Pools]** を選択します。

リソースプ - ルは、[Navigation] ウィンドウに、[L4-L7 Resource Pools] の下のドロップダウンリストとして表示されます。

ステップ 3 デバイスを追加するレイヤ 4 ～ レイヤ 7 リソース プーをクリックします。

ステップ 4 [Work] ウィンドウの **L4-L7 Devices** タブをクリックします。

ステップ 5 **L4-L7 Devices** テーブルで、プラスのアイコン (+) をクリックします。

Create An L4-L7 Device ダイアログが表示されます。

ステップ 6 **Device** ドロップダウン矢印をクリックして、レイヤ 4 ～ レイヤ 7 デバイスを選択します。

ステップ 7 [送信（Submit）] をクリックします。

レイヤ 4 ～ レイヤ 7 デバイスをレイヤ 4 ～ レイヤ 7 リソース プールから削除する

リソース プールは、設定されたレイヤ 4 ～ レイヤ 7 デバイスが利用可能出ない限り、どのテナントも使用できません。レイヤ4～レイヤ7デバイスが割り当てられておらず、どのテナントにもエクスポートされていない場合には、次の手順を実行します:

ステップ 1 メニュー バーで、**[Tenants]** > **[Common]** を選択します。

ステップ 2 [Navigation] ペインで、 **[Tenant Common]** > **[Services]** > **[L4-L7]** > **[L4-L7 Resource Pools]** を選択します。

リソースプ - ルは、[Navigation] ウィンドウに、[L4-L7 Resource Pools] の下のドロップダウンリストとして表示されます。

ステップ 3 削除するデバイスが含まれているレイヤ 4 ～ 7 リソース プールをクリックします。

ステップ 4 作業ウィンドウで、**L4-L7 Devices** タブをクリックします。

ステップ 5 削除するレイヤ 4 ～ レイヤ 7 デバイスをハイライトして、**trashcan** のアイコンをクリックします。

確認用のダイアログが表示されます。

ステップ 6 **[はい (Yes)]** をクリックして削除を確認します。

リソー スプールの外部 IP アドレス プールの設定

レイヤ 7 リソース プールにレイヤ 4 への外部 IP アドレス プールの追加

リソース プールが使用中の場合には、外部 IP アドレス プールもテナントで使用されているので、削除や更新は行わないでください。

ステップ 1 メニュー バーで、**[Tenants]** > **[Common]** を選択します。

ステップ 2 [Navigation] ペインで、 **[Tenant Common]** > **[Services]** > **[L4-L7]** > **[L4-L7 Resource Pools]** を選択します。

リソース プ - ルは、[Navigation] ウィンドウに、[L4-L7 Resource Pools] の下のドロップダウンリストとして表示されます。

ステップ 3 外部の IP アドレス プールを追加するレイヤ 7 リソース プールにレイヤ 4 をクリックします。

ステップ 4 [Work] ウィンドウの **Basic** タブをクリックします。

ステップ 5 **外部 IP アドレス プール** テーブルで、プラス記号アイコンをクリックします (+)。

外部 IP アドレス プール フィールドが表示されます。

ステップ 6 **Connect Type** ドロップダウン矢印をクリックして **L3 External Network** を選択し、その他の **External IP Address Pool** フィールドに適切な値を入力します。

（注） フィールドの説明については、右上隅のヘルプアイコン ([?]) をクリックしてください。

ステップ 7 [更新（Update）] をクリックします。

外部 IP アドレス プールをレイヤ 4 ～ レイヤ 7 リソース プールから削除する

（注）
- リソース プールが使用中の場合には、外部 IP アドレス プールもテナントで使用されているので、削除や更新は行わないでください。
- IP アドレス プールの枯渇に対応するために外部 IP アドレス プールの削除、追加、または更新を行う場合には、大規模な IP アドレス プールの追加や削除は行わないでください。これらの状況では、レイヤ 3 ドメインや L3Out と似た構成の、新しい外部 IP アドレス プールを伴うレイヤ 4 ～ レイヤ 7 リソース プールを作成します。
- 外部 IP アドレス プールが設定されていないと、テナントはリソース プールを使用できません。

ステップ 1 メニュー バーで、**[Tenants]** > **[Common]** を選択します。

ステップ 2 [Navigation] ペインで、 **[Tenant Common]** > **[Services]** > **[L4-L7]** > **[L4-L7 Resource Pools]** を選択します。

リソース プ - ルは、[Navigation] ウィンドウに、[L4-L7 Resource Pools] の下のドロップダウンリストとして表示されます。

ステップ 3 削除する外部 IP アドレス プールを持つレイヤ 4 ～ レイヤ 7 リソース プールをクリックします。

ステップ 4 作業ウィンドウで、**Basic** タブをクリックします。

ステップ 5 **External IP Address Pool** テーブルで、削除する外部 IP アドレス プールをクリックしてハイライトし、**trashcan** アイコンをクリックします。

確認用のダイアログが表示されます。

ステップ 6 **[はい (Yes)]** をクリックして削除を確認します。

リソー スプールのパブリック IP アドレス プールの設定

パブリック IP アドレス プールをレイヤ 4 ～ レイヤ 7 リソース プールに追加する

（注）
- Cisco APIC Release 3.0(x) 以前で作成されたレイヤ 4 ～ 7 リソース プールの場合、外部 IP アドレス プールがパブリック IP アドレス プールとして使用されます。いったんテナントで使用されたら、変更してはなりません。
- Cisco APIC リリース 3.1(x) 以降で作成されたレイヤ 4 ～ レイヤ 7 リソース プールの場合、いつでも新しいパブリック IP アドレス プールをリソース プールに追加できます。
- パブリック IP アドレス プールが設定されていないと、テナントはリソース プールを使用できません。

ステップ 1 メニュー バーで、**[Tenants]** > **[Common]** を選択します。

ステップ 2 [Navigation] ペインで、 **[Tenant Common]** > **[Services]** > **[L4-L7]** > **[L4-L7 Resource Pools]** を選択します。

リソース プ - ルは、[Navigation] ウィンドウに、[L4-L7 Resource Pools] の下のドロップダウンリストとして表示されます。

ステップ 3 パブリック IP アドレス プールに追加するレイヤ 4 ～ レイヤ 7 リソース プールをクリックします。

ステップ 4 作業ウィンドウで、**Basic** タブをクリックします。

ステップ 5 **Public IP Address Pool** テーブルで、プラスのアイコン (+) をクリックします。

Public IP Address Pool フィールドが表示されます。

ステップ 6 **Connect Type** ドロップダウン矢印をクリックして **L3 External Network** を選択し、その他の **External IP Address Pool** フィールドに適切な値を入力します。

（注） フィールドの説明については、右上隅のヘルプアイコン ([?]) をクリックしてください。

ステップ 7 [更新（Update）] をクリックします。

パブリック IP アドレス プールをレイヤ 4 ～ 7 リソース プールから削除する

（注）
- Cisco APIC Release 3.0(x) 以前で作成されたレイヤ 4 ～ 7 リソース プールの場合、外部 IP アドレス プールがパブリック IP アドレス プールとして使用されます。いったんテナントで使用されたら、変更してはなりません。
- Cisco APIC Release 3.1(x) 以降で作成されたレイヤ 4 ～ 7 リソース プールの場合、いずれかのテナントが現在 IP アドレス プールを利用している場合、リソース プールから IP アドレス プールを削除してはなりません。
- パブリック IP アドレスが設定されていない場合、リソース プールはどのテナントからも利用できません。

ステップ 1 メニュー バーで、**[Tenants]** > **[Common]** を選択します。

ステップ 2 [Navigation] ペインで、 **[Tenant Common]** > **[Services]** > **[L4-L7]** > **[L4-L7 Resource Pools]** を選択します。

リソース プ - ルは、[Navigation] ウィンドウに、[L4-L7 Resource Pools] の下のドロップダウンリストとして表示されます。

ステップ 3 削除するパブリック IP アドレス プールが含まれているレイヤ 4 ～ 7 リソース プールをクリックします。

ステップ 4 [Work] ウィンドウで、[Basic] タブをクリックします。

ステップ 5 **[Public IP Address Pool]** テーブルで、削除するパブリック VIP アドレス プールをクリックしてハイライトし、[trashcan] のアイコンをクリックします。

確認用のダイアログが表示されます。

ステップ 6 **[はい (Yes)]** をクリックして削除を確認します。

レイヤ 4 ～ レイヤ 7 リソース プールの外部ルーテッド ドメインの更新

外部ルーテッド ドメインが設定されていないと、テナントはリソース プールを使用できません。

ステップ 1 メニュー バーで、**[Tenants]** > **[Common]** を選択します。

ステップ 2 [Navigation] ペインで、 **[Tenant Common]** > **[Services]** > **[L4-L7]** > **[L4-L7 Resource Pools]** を選択します。

リソース プ - ルは、[Navigation] ウィンドウに、[L4-L7 Resource Pools] の下のドロップダウンリストとして表示されます。

ステップ 3 更新する外部ルーテッド ドメインのあるレイヤ 4 ～ レイヤ 7 リソース プールをクリックします。

ステップ 4 [Work] ウィンドウで、[External] タブをクリックします。

ステップ 5 [External Routed Domain] ドロップダウン矢印をクリックして、レイヤ 3 ドメインを選択します。

ステップ 6 [送信（Submit）] をクリックします。

レイヤ 4 からレイヤ 7 リソースプールの外部ルーテッド ネットワークの更新

外部ルーテッド ネットワークが設定されていない場合、リソース プールはどのテナントでも使用できません。

ステップ 1 メニュー バーで、**[Tenants]** > **[Common]** を選択します。

ステップ 2 [Navigation] ペインで、 **[Tenant Common]** > **[Services]** > **[L4-L7]** > **[L4-L7 Resource Pools]** を選択します。

リソース プ - ルは、[Navigation] ウィンドウに、[L4-L7 Resource Pools] の下のドロップダウンリストとして表示されます。

ステップ 3 更新する外部ルーテッド ネットワークがあるレイヤ 4 からレイヤ 7 のリソース プールをクリックします。

ステップ 4 [Work] ウィンドウで、[External] タブをクリックします。

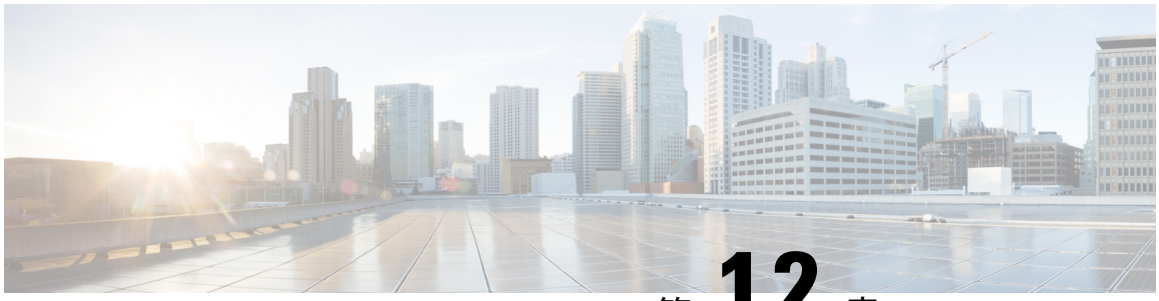
ステップ 5 [External Routed Networks] テーブルから、プラスアイコン ([+]) をクリックします。

[External Routed Networks] フィールドが表示されます。

ステップ 6 [External Routed Networks] フィールドに適切な値を入力します。

（注） フィールドの説明については、右上隅のヘルプアイコン ([?]) をクリックしてください。

ステップ 7 [更新（Update）] をクリックします。



第 12 章

サービス グラフのモニタリング

GUI を使用したサービス グラフ インスタンスのモニタリング

サービス グラフ テンプレートを設定し、エンドポイント グループ（EPG）およびコントラクトにグラフをアタッチした後は、サービス グラフ インスタンスをモニタできます。モニタリングには、グラフ インスタンスの状態、グラフ インスタンスの機能、機能に割り当てられたリソース、および機能に指定されたパラメータの表示が含まれます。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、サービス グラフをモニタするテナントの名前をダブルクリックします。

ステップ 3 **[Navigation]** ペインで、**[Tenant]** ***tenant_name*** > **[Services]** > **[L4-L7]** > **[Deployed Graph Instances]** の順で選択します。[Work] ペインは、アクティブなサービス グラフ インスタンスに関する次の情報を表示します。

名前	説明
[Service Graph] カラム	サービス グラフ テンプレートの名前。
[Contract] カラム	サービス グラフ テンプレートに表示されるコントラクトの名前。
[Contained By] カラム	サービス グラフ テンプレートを含むネットワークの名前。

名前	説明
[State] カラム	サービス グラフ テンプレートの状態。[applied] の状態は、グラフが適用され、グラフ ポリシーがファブリックおよびサービス デバイス内でアクティブであることを意味します。
[Description] カラム	サービス グラフの説明

ステップ 4 [Deployed Service Graphs] ブランチを展開します。アクティブなサービス グラフ インスタンスがブランチの下にリストされます。

ステップ 5 サービス グラフ インスタンスをクリックして、[Work] ペインにそのインスタンスに関する追加情報を表示します。デフォルト ビューはグラフのトポロジです。[Work] ペインのタブのいずれかをクリックして、そのグラフのビューを変更できます。

ステップ 6 グラフ インスタンスのいずれかのブランチを展開します。グラフ インスタンスの機能は、インスタンスの下に表示されます。

ステップ 7 機能をクリックして、[Work] ペインにその機能に関する追加情報を表示します。デフォルト ビューはその機能のポリシーです。[Work] ペインのタブのいずれかをクリックして、その機能のビューを変更できます。[Work] ペインには、ポリシーに関する次の情報が表示されます。

名前	説明
[POLICY] タブ	機能のプロパティ、機能に割り当てられたリソース、および機能のパラメータ。
[FAULTS] タブ	機能ノードで生じている問題。
[HISTORY] タブ	機能ノードで発生したイベントの履歴。

ステップ 8 [Navigation] ペインで、[Deployed Device] をクリックします。[Work] ペインにデバイスのインスタンスに関する情報が表示されます。

GUI を使用したサービス グラフ エラーのモニタリング

サービス グラフ テンプレートを設定し、エンドポイント グループ（EPG）およびコントラクトにグラフをアタッチした後は、サービス グラフ テンプレートのエラーをモニタできます。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、サービス グラフをモニタするテナントの名前をダブルクリックします。

ステップ 3 [Navigation] ウィンドウで、**Tenant *tenant_name*** > **Services** > **L4-L7** > **Deployed Graph Instances** を選択します。

ステップ 4 エラーを表示するグラフ インスタンスのブランチを展開します。グラフ インスタンスの機能は、インスタンスの下に表示されます。

ステップ 5 機能のいずれかをクリックします。デフォルトで、[Work] ペインはその機能のポリシーを示します。

ステップ 6 [Work] ペインの [FAULTS] タブをクリックします。[Work] ペインが機能ノードのエラーを表示します。

サービス グラフ エラーの解決

1 つ以上のサービス グラフ テンプレート エラーを発見した場合、問題の解決はエラーによって異なります。次の表は、エラーの説明とエラーを解決する方法を説明しています。

表 *5 :* コネクタのエラー

Fault	CLI ラベル	説明と解決法
missing-connection	connection associated with a connector not found	グラフ コネクタの設定が無効です。コネクタに関連付けられた接続が見つかりませんでした。
missing-nodeinst	NodeInst associated with a connector not found	グラフ コネクタの設定が無効です。コネクタに関連付けられた NodeInst が見つかりませんでした。
conn-nonrenderable	Graph connector could not be rendered.	グラフ コネクタの設定が無効です。グラフをレンダリングできませんでした。
invalid-bd	BD associated with a connector is not valid	グラフ コネクタの設定が無効です。コネクタの関連ブリッジ ドメインが無効です。
invalid-ctx	Ctx associated with a connector is not valid.	グラフ コネクタの設定が無効です。コネクタの関連する Ctx が無効です。
missing-peer-conn	Peer connector associated with a connector not found.	グラフ コネクタの設定が無効です。接続のピア コネクタが見つかりませんでした。

表 *6 : AbsGraph* および *GraphInst* エラー

Fault	CLI ラベル	説明と解決法
invalid-abstract-graph-config	invalid abstract graph config	抽象グラフ設定が無効です。
epp-download-failure	epp download failure	グラフ ポリシーがスイッチのダウンロードに失敗しました。

Fault	CLI ラベル	説明と解決法
param-duplicate-name-failure	duplicate param name	同じ名前のパラメータの複数の同一コピーが検出されました。
id-allocation-failure	id allocation failure	一意のネットワーク リソース（VLAN VXLAN）を割り当てることができませんでした。
missing-ldev	No cluster found	クラスタが見つかりませんでした。
context-cardinality-violation-failure	invalid cluster context cardinality	クラスタは必要なテナント機能（マルチテナントまたはシングル テナント）をサポートしていません。
function-type-mismatch-failure	invalid function type	機能タイプが選択したデバイスでサポートされていません。AbsNode 機能タイプと解決された LDevVip 機能タイプが一致するか確認します。
missing-mparam	No parameter definition found	必要なパラメータ定義が見つかりませんでした。
missing-abs-graph	no abs graph found	抽象グラフ設定がグラフ インスタンスにありません。
invalid-param-config	invalid param config	パラメータ設定が無効です。
invalid-param-scope	invalid parameter scope	パラメータ スコープが無効です。AbsGraph の vnsRsScopeToTerm パラメータが正しいかどうか確認します。
invalid-ldev	Invalid cluster	クラスタ設定が無効です。解決した LDevVip のステータスを確認して、エラーを解決します。
missing-tenant	no tenant found	グラフに対してテナントが見つかりませんでした。
internal-error	internal error	内部エラーがグラフ処理中に発生しました。
resource-allocation-failure	resource allocation failure	グラフ処理中に必要なリソースを割り当てることができませんでした。

Fault	CLI ラベル	説明と解決法
missing-abs-function	no abstract function found	抽象機能の定義が見つかりません。
missing-mconn	No connector found	必要なコネクタが見つかりませんでした。
invalid-graphinst	invalid graphinst config	グラフ インスタンスが無効です。
missing-interface	no interface found	インターフェイスが見つかりませんでした。
missing-bd	no bd found	ブリッジ ドメインが見つかりませんでした。
missing-terminal	Terminal node is missing a terminal	端末ノードに端末がありません。端末ノードの設定を確認してください。
missing-namespace	no vlan/vxlan namespace found	VLAN または VXLAN の割り当てに必要なネームスペースが見つかりません。解決された fvnsVlanInstp と関係がある phyDomp パラメータまたは vmmDompパラメータが解決された vnsLDevVip に設定されていることを確認します。
missing-lif	no cluster interface found	必要なクラスタ インターフェイスが見つかりませんでした。vnsLDevVip の vnsLIf パラメータが正しく設定されていることを確認します。
missing-cdev	No device found	具象デバイスがクラスタ内に見つかりませんでした。有効な vnsCDev が解決された vnsLDevVip の下に存在することを確認してください。
insufficient-devctx	Folder must have one value for each associated CDev	フォルダは具象デバイスに固有です。フォルダは、各具象デバイスに対して少なくとも 1 つの値を持つ必要があります。
cdev-missing-cif	No interface defined	具象デバイスには少なくとも 1つのインターフェイスを定義する必要があります。

Fault	CLI ラベル	説明と解決法
cdev-missing-pathinfo	Missing path for interface	物理サービス アプライアンスでは、インターフェイスがどのリーフ ポートに接続されているかを把握する必要があります。vnsCifPathAtt パラメータが、解決された vnsCDev の下のすべての vnsCIf に存在することを確認します。
missing-cif	Device interfaces does not match cluster	デバイス インターフェイスは、クラスタに設定されているインターフェイスに一致させる必要があります。vnsCIf パラメータおよび vnsLIf パラメータが、解決された vnsLDevVip の下に存在することを確認します。
lif-invalid-CIf	LIf has an invalid CIf	LIf に含まれる CIf がありません。具象デバイスおよび CIf の設定を確認します。
missing-function-node	Abstract graph missing function node	抽象グラフには、少なくとも 1 つの機能ノードが存在する必要があります。
graph-loop-detected	Abstract graph config has a loop	抽象グラフ設定が無効です。設定にループがあります。
gothrough-routing-enabled-both	Both the legs of go through node has routing enabled	通過ノードの両方のレッグでルーティングが有効になっています。
invalid-terminal-nodes	Abstract graph has invalid number of terminal nodes	抽象グラフは少なくとも 2 つの端末ノードを持つ必要があります。
missing-ldev-ctx	No device context found for LDev	デバイスのデバイス コンテキストが見つかりませんでした。vnsLDevCtx にコントラクト、グラフおよびノードに一致する値があることを確認します。
arp-flood-enabled	ARP flood is enabled on the management end point group	ARP フラッディングは管理エンドポイントのグループに対して無効です。

Fault	CLI ラベル	説明と解決法
folderinst-validation-failed	FolderInst has key, that is not found in MFolder	FolderInst のキーおよび値は MFolder 仕様を尊重する必要があります。
paraminst-validation-failed	ParamInst has key and/or value, that are not found in MParam	ParamInst のキーおよび値は MParam 仕様を尊重する必要があります。
invalid-mfolder	FolderInst points to an invalid MFolder	FolderInst は有効な MFolder をポイントする必要があります。
invalid-mparam	ParamInst points to an invalid MParam	ParamInst は有効な MParam をポイントする必要があります。
devfolder-validation-failed	DevFolder has key, that is not found in MFolder	DevFolders のキーおよび値は MFolder 仕様を尊重する必要があります。
devparam-validation-failed	DevParam has key and/or value, that are not found in MParam	DevParam のキーおよび値は MParam 仕様を尊重する必要があります。
cdev-missing-virtual-info	Virtual Object Info is missing in CDev	LDevVip のタイプが Virtual の場合は仮想オブジェクト情報を指定する必要があります。
invalid-rsmconnatt	Relationship to metaconnector is invalid	メタコネクタの DN を修正し、正しい MDev 階層にバインドすることを確認します。

GUI を使用した仮想デバイスのモニタリング

サービス グラフ テンプレートを設定し、エンドポイント グループ（EPG）およびコントラクトにグラフをアタッチした後は、テナントの仮想デバイスをモニタできます。仮想デバイスをモニタリングすると、どのデバイスが使用中か、どの VLAN がデバイス用に設定されているかや、デバイスに渡されるパラメータ、デバイスの統計、およびデバイスの健全性を確認できます。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、サービス グラフをモニタするテナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ペインで、次のように選択します。 **テナント *tenant_name*** > **サービス** > **L4 L7** > **デバイスの導入** 。

ステップ 4 導入されたデバイスのいずれかをクリックします。デフォルトでは、[Work] ペインに導入済みのデバイスのポリシーが表示されます。ビューを変更するには、[Work] ペインのタブをクリックします。タブは、仮想デバイスに関する以下の情報を表示します。

タブ	説明
[POLICY] タブ	使用中のデバイス、デバイス内で設定されたVLAN、およびデバイスに渡されたパラメータ。
[OPERATIONAL] タブ	さまざまなデバイスから受信する統計情報。
[HEALTH] タブ	デバイスの状態。

NX-OSスタイルのCLIを使用したデバイス クラスタとサービス グラフ ステータスのモニタリング

この項のコマンドで、NX-OS スタイルの CLI を使用してデバイス クラスタとサービス グラフ ステータスをモニタする例を示します。

デバイス クラスタの動作情報の表示

次に、デバイス クラスタの動作情報を表示するコマンドを示します。

```
show l4l7-cluster tenant tenant_name cluster device_cluster_name
```

例：

```
apic1# show l4l7-cluster tenant HA_Tenant1 cluster Firewall
tenant-graph : HA_Tenant1-g2,HA_Tenant1-g1


Device Cluster    : Firewall
Cluster Interface : consumer1
Encap             : vlan-501
Pctag             : 32773
Devices           : FW2(int),FW1(int)
Graphs            : HA_Tenant1-g1
Contracts         : HA_Tenant1-c1


Device Cluster    : Firewall
Cluster Interface : provider1
Encap             : vlan-502
Pctag             : 32774
Devices           : FW2(ext),FW1(ext)
Graphs            : HA_Tenant1-g1
Contracts         : HA_Tenant1-c1
```

デバイス クラスタの動作ステータスの表示

次に、デバイス クラスタの動作ステータスを表示するコマンドを示します。

```
apic1# show l4l7-graph tenant tenant_name [graph graph_name]
```

例：

次に、HA_Tenant1 テナントのステータスの高レベル出力を提供する例を示します。

```
apic1# show l4l7-graph tenant HA_Tenant1
Graph           : g1
Total Instances : 1
Encaps Used     : vlan-501,vlan-502,vlan-503,vlan-504
Device Used     : uni/tn-HA_Tenant1/lDevVip-Firewall

Graph           : g2
Total Instances : 1
Encaps Used     : vlan-501,vlan-502,vlan-503,vlan-504
Device Used     : uni/tn-HA_Tenant1/lDevVip-Firewall
```

次に、HA_Tenant1 に関連付けられた g1 サービス グラフの詳細出力を提供する例を示します。

```
apic1# show l4l7-graph tenant HA_Tenant1 graph g1
Graph           : HA_Tenant1-g1
Graph Instances : 1

Consumer EPg  : HA_Tenant1-consEPG1
Provider EPg  : HA_Tenant1-provEPG1
Contract Name : HA_Tenant1-c1
Config status : applied

Function Node Name : Node1
 Connector   Encap       Bridge-Domain  Device Interface
 ----------  ----------  -----------    ---------------------
 consumer    vlan-3001   provBD1        consumer
 provider    vlan-3335   consBD1        provider
```

デバイス クラスタのエラーの表示

次に、デバイス クラスタのエラーを表示するコマンドを示します。

```
show faults l4l7-cluster
```

例：

```
apic1# show faults l4l7-cluster
Code            : F0772
Severity        : minor
Last Transition : 2015-09-01T01:41:13.767+00:00
Lifecycle       : soaking-clearing
Affected object : uni/tn-ts1/lDevVip-d1/lIf-ext/fault-F0772
Description     : LIf configuration ext for L4-L7 Devices d1 for tenant ts1
                  is invalid.

Code            : F1085
Severity        : cleared
Last Transition : 2015-09-01T01:39:04.696+00:00
Lifecycle       : retaining
Affected object : uni/tn-ts1/lDevVip-d1/rsmDevAtt/fault-F1085
Description     : Failed to form relation to MO uni/infra/mDev-CiscoInternal-
                  NetworkOnly-1.0 of class vnsMDev

Code            : F1690
Severity        : minor
Last Transition : 2015-09-01T01:39:04.676+00:00
Lifecycle       : soaking
Affected object : uni/tn-ts1/lDevVip-d1/vnsConfIssue-missing-
```

```
                namespace/fault-F1690
Description     : Configuration is invalid due to no vlan/vxlan namespace
                found
```

サービス グラフのエラーの表示

次に、サービス グラフのエラーを表示するコマンドを示します。

```
show faults l4l7-graph
```

例：

```
apic1# show faults l4l7-graph
Code            : F1690
Severity        : minor
Last Transition : 2015-11-25T20:07:33.635+00:00
Lifecycle       : raised
DN              : uni/tn-HA_Tenant1/AbsGraph-WebGraph/vnsConfIssue-invalid-
                  abstract-graph-config-param/fault-F1690
Description     : Configuration is invalid due to invalid abstract graph
                  config param
```

デバイス クラスタの実行コンフィギュレーションの表示

次に、デバイス クラスタの実行コンフィギュレーションを表示するコマンドを示します。

```
show running-config tenant tenant_name l4l7 cluster
```

例：

```
apic1# show running-config tenant common l4l7 cluster
# Command: show running-config tenant common l4l7 cluster
# Time: Thu Nov 26 00:35:59 2015
  tenant common
    l4l7 cluster name ifav108-asa type physical vlan-domain phyDom5 service FW function
 go-through
      cluster-device C1
      cluster-interface consumer_1
        member device C1 device-interface port-channel1
          interface vpc VPCPolASA leaf 103 104
          exit
        exit
      cluster-interface provider_1
        member device C1 device-interface port-channel1
          interface vpc VPCPolASA leaf 103 104
          exit
        exit
      exit
```

サービス グラフの実行コンフィギュレーションの表示

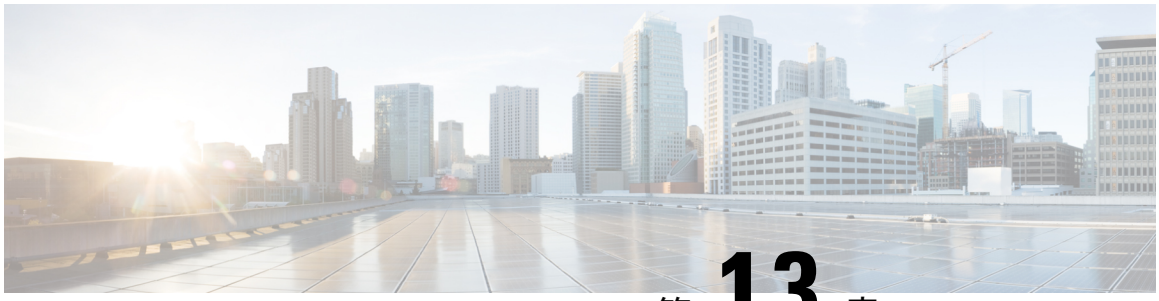
次に、サービス グラフの実行コンフィギュレーションを表示するコマンドを示します。

```
show running-config tenant tenant_name l4l7 graph
```

例：

```
apic1# show running-config tenant common l4l7 graph
# Command: show running-config tenant common l4l7 graph
# Time: Thu Nov 26 00:35:59 2015
  tenant T1
    l4l7 graph Graph-Citrix contract Contract-Citrix
      service N1 device-cluster-tenant common device-cluster ifav108-citrix mode
```

```
ADC_ONE_ARM
        connector provider cluster-interface pro
          bridge-domain tenant common name BD4-Common
          exit
        connector consumer cluster-interface pro
          bridge-domain tenant common name BD4-Common
          exit
        exit
      connection C1 terminal consumer service N1 connector consumer
      connection C2 terminal provider service N1 connector provider
      exit
```



第 13 章

多層アプリケーションとサービス グラフの設定

多層アプリケーションとサービス グラフについて

[Multi-Tier Application with Service Graph Quick Start] ダイアログは、ブリッジ ドメイン、EPG、VRF、サービス、契約など、サービス グラフのコンポーネントを構成するための、統一された方法を提供します。Cisco APIC の別々の場所で各オブジェクトを設定しなくても、[Quick Start] ダイアログは、必要な設定を収集し、それらをシンプルで組織的なステップバイ ステップのプロセスにまとめます。

GUI を使用した多階層アプリケーション プロファイルの作成

始める前に

手順を実行中に、使用可能な場合または前に、次のオブジェクトを設定します。

- **テナント:** 手順を実行する前に少なくとも 1 つのテナントを設定します。
- **VMM ドメイン プロファイル:** デバイス仮想サービスを使用すると、レイヤ 7 デバイスのクラスタ (デバイスがホストされる) をレイヤ 4 で、Virtual Machine Manager (VMM) ドメイン プロファイルと、VM を設定します。
- **外部ルーテッド ネットワーク:** 外部ルーテッド ネットワークにサービス デバイスを接続する場合は、(L3Out) ネットワークの外部レイヤ 3 を設定します。

ステップ 1 [Quick Start] の [Multi-Tier Application] ダイアログにアクセスします。

a) メニュー バーで、[Tenant] > [All Tenants] の順にクリックします。
b) [All Tenants] 作業ペインで、テナントの名前をダブルクリックします。
c) [Navigation] ペインで、[Tenant *tenant_name*] > [Quick Start] > [Multi-tier Application] を選択します。
d) [Work] ペインで、[Configure Multi-tier Application] をクリックします。
[Create Application Profile] ダイアログが表示されます。
e) [Start] をクリックします。

ステップ 2 [STEP 2 > EPGs] ダイアログ ボックスで、プロファイルの基本を設定し、ブリッジ ドメインと EPG を設計します。

a) [Application Profile] フィールドで、プロファイルの一意の名前を入力します。
b) （オプション）このプロファイルで 1 個以上のデバイスが仮想である場合は、[VMM Domain Profile] ドロップダウンリストから仮想マシン マネージャ（VMM）ドメイン プロファイルを選択します。

（注） [VMM Domain Profile] ドロップダウン リストで表示および選択されるように、この手順を実行する前に VMM ドメイン プロファイルを作成する必要があります（[Virtual Networking] > [VMM Domains]）。

c) （オプション）コンシューマまたはプロバイダー EPG が外部ルーテッド ネットワークに属している場合は、[Consumer L3 Outside] および [Provider L3 Outside] フィールド（またはいずれか）のドロップダウンリストからネットワークを選択します。

（注） 外部ルーテッド ネットワークが [L3 Outside] ドロップダウンリストに表示されて選択できるように、この手順を実行する前に外部ルーテッド ネットワークを作成する必要があります（[Tenants] > テナント > [Networking] > [External Routed Networks]）。

d) ブリッジ ドメイン ボタンについて、EPG ゲートウェイ IP アドレスが単一の共有サブネットか、 EPG ごとに設定されるかを決定します。

[Shared] を選択した場合、[Shared Gateway IP] フィールドが表示されます。[Per EPG] を選択した場合、手順 f に進みます。

e) [Bridge Domain] ボタンから [Shared] ボタンを選択した場合、[Shared Gateway IP] フィールドの EPG で共有されるゲートウェイの IPv4 アドレスを入力します。
f) アプリケーション階層（EPG）の [Name] フィールドに EPG の名前を入力します。
g) [Bridge Domain] ボタンから [Per EPG] を選択した場合、EPG で使用されるゲートウェイの IPv4アドレスを入力します。[Bridge Domain] ボタンから [Shared] を選択した場合、[Shared Gateway IP] フィールドに入力した IP アドレスが表示されます。
h) （オプション）[+] をクリックし、手順 g に従い別の EPG を追加して EPG を設定します。3 つの EPG が必要な場合はこの手順を繰り返します。
i) [Next] をクリックします。

ステップ 3 [STEP 3 > Services] ダイアログで、必要に応じて、EPG の近隣にあるサービスに含まれるものを設定します。

a) (オプション）[Share same device] ボックスのチェックをオンにして、すべての EPG でファイアウォール ロード バランサを共有します。

b) （オプション）各 EPG の間で、このプロファイルに含むファイアウォール（**FW**）またはロード バランサ（**ADC**）を選択します。
c) （オプション）EPG 間で複数のデバイスを追加する場合は、**< Toggle >** をクリックしてデバイスを再配置します。
d) [Next] をクリックします。

ステップ 4 （ファイアウォールとロードバランサ）**[STEP 4 >]** ダイアログとファイアウォールまたはロードバランサの設定セクションで、サービス デバイスを設定します。

a) **[デバイス タイプ]** ボタンでは、**[物理]** または **[仮想]** を選択します。
b) **[デバイス タイプ]** に **[物理]** を選択した場合、**[物理ドメイン]** ドロップダウン リストからドメインを選択します。**[デバイス タイプ]** に **[仮想]** を選択した場合、**[VMM ドメイン]** ドロップダウン リストおよび **[デバイス 1 VM]** ドロップダウン リストからホストされたデバイスの仮想マシン（VM）からドメインを選択します。
c) **[ノード タイプ]** ボタンでは、**[One-Arm]** または **[Two-Arm]** を選択します。デバイスがコンシューマ コネクタ（one-arm）のみを有するか、コンシューマとプロバイダ（two-arm）を有するか決定します。
d) **[ビュー]** ボタンでは、**[単一ノード]** または **[HA ノード]** を選択します。**[HA ノード]** を選択した場合、2 番目のインターフェイス（物理デバイス）または 2 番目の VNIC（仮想デバイス）がコネクタの設定に含まれており、仮想デバイスでは 2 番目の仮想マシンを選択する必要があります。

ステップ 5 （ファイアウォールのみ）**[STEP 4 >]** ダイアログおよびコンシューマとプロバイダーセクションで、ファイアウォール コンシューマとプロバイダー コネクタを設定します。

a) **[IP]** フィールドの物理デバイスでは、ファイアウォール デバイスのレイヤ 4 ～ レイヤ 7 ポリシー ベースのリダイレクト ポリシーにコンシューマ/プロバイダー インターフェイス IP アドレスを入力します。仮想デバイスでは、コンシューマ/プロバイダー インターフェイスの IP アドレスを入力します。
b) **[MAC]** フィールドで、ファイアウォール デバイスのレイヤ 4 ～ レイヤ 7 ポリシー ベースのリダイレクト ポリシーの MAC アドレスを入力します。
c) **[ゲートウェイ IP]** フィールドで、ルート ゲートウェイ IP アドレスを入力します。
d) 物理デバイスでは、**[デバイス 1 インターフェイス]** ドロップダウン リストで、インターフェイスを選択します。仮想デバイスでは、**[デバイス 1 VNIC]** ドロップダウン リストで vNIC を選択します。**[ビュー]** ボタンから **[HA]** ノードを選択した場合、**[デバイス 2 VNIC]** ドロップダウン リストで 2 番目の vNIC を選択する必要があります。
e) （物理デバイスのみ）**[Encap]** フィールドで、インターフェイスのポート カプセル化を入力します。

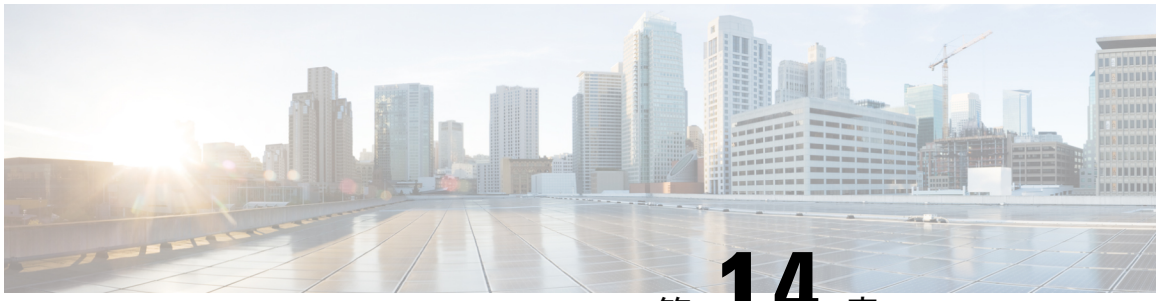
ステップ 6 (ロード バランサのみ)**[手順 4 >]** ダイアログおよびコンシューマとプロバイダー セクションで、ロード バランサ コンシューマおよびプロバイダー コネクタを設定します。

a) **[ゲートウェイ IP]** フィールドで、ルート ゲートウェイ IP アドレスを入力します。
b) 物理デバイスでは、**[デバイス 1 インターフェイス]** ドロップダウン リストで、インターフェイスを選択します。仮想デバイスでは、**[デバイス 1 VNIC]** ドロップダウン リストで vNIC を選択します。**[ビュー]** ボタンから **[HA]** ノードを選択した場合、**[デバイス 2 VNIC]** ドロップダウン リストで 2 番目の vNIC を選択する必要があります。
c) （物理デバイスのみ）**[Encap]** フィールドで、インターフェイスのポート カプセル化を入力します。
d) コネクタで L3 トラフィックを終端させるには、[L3 Destination (VIP)] ボックスをオンのままにします。コネクタが L3 宛先ではない場合はオフにします。

（注） このパラメータのデフォルトは有効（オン）です。ただし、ポリシーベース リダイレクトがインターフェイスで設定されている場合、この設定は考慮されません。

ステップ 7 追加でデバイスを設定する場合は、[Next] をクリックし、各デバイスごとに手順 4 ～ 6 を繰り返します。

ステップ 8 [Finish] をクリックします。



第 14 章

サービス コンフィギュレーションの管理に対する管理ロールの設定

権限について

Application Policy Infrastructure Controller（APIC）で設定したロールに権限を付与できます。権限は、ロールが実行できるタスクを決定します。管理者ロールには次の特権を付与できます。

特権	説明
nw-svc-policy	ネットワーク サービス ポリシー権限では次を実行できます。 • サービス グラフ テンプレートの作成 • アプリケーション エンドポイント グループ（EPG）およびコントラクトへのサービス グラフ テンプレートのアタッチ • サービス グラフのモニタ
nw-svc-device	ネットワーク サービス デバイス権限では次を実行できます。 • デバイスの作成 • 具象デバイスの作成 • デバイス コンテキストの作成

デバイス管理のロールの設定

デバイスを管理するためのロールを有効化するには、そのロールに次の特権を付与する必要があります。

- nw-svc-device

サービス グラフ テンプレート管理のロールの設定

サービス グラフ テンプレートを管理するためのロールを有効化するには、そのロールに次の特権を付与する必要があります。

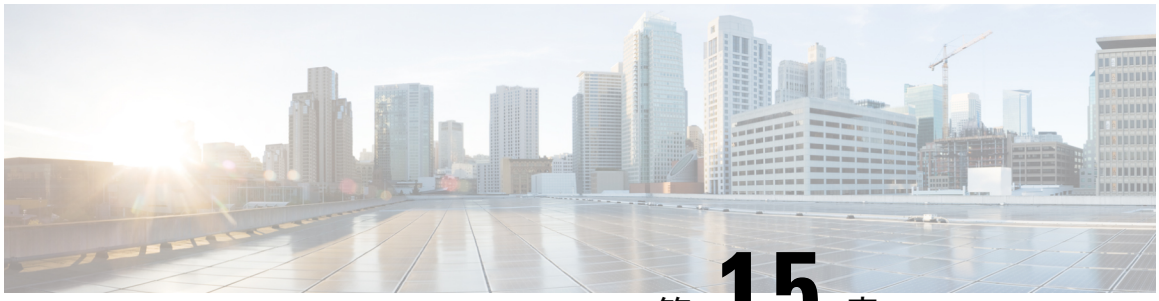
- nw-svc-policy

デバイスをエクスポートするためのロールの設定

デバイスをエクスポートして、テナント間でデバイスを共有することができます。**nw-device** ロールを持つテナントはデバイスを作成できます。デバイスを所有するテナントがこれらを別のテナントと共有する場合、共有には **nw-svc-devshare** 特権が必要です。

nw-svc-devshare 特権を使用すると、テナントはデバイスをエクスポートできます。

（注） インポートされたデバイスを使用できるようにするには、インポートされたデバイスを持つ他のテナントが **nw-svc-policy** 特権を持つ必要があります。



第 15 章

自動化の開発

REST API について

自動化は、Application Policy Infrastructure Controller（APIC）のノースバウンド Representational State Transfer （REST）API を使用します。また、Cisco APIC GUI で実行可能なものは、ノースバウンド API を使用した XML ベースの REST POST で実行できます。たとえば、これらの API 経由でのイベントのモニタ、EPG のダイナミックな有効化、およびポリシーの追加などを実行できます。

また、ノースバウンド REST API を使用して、デバイスがオンボードになったことの通知や、エラーをモニタできます。両方のケースで特定のアクションをトリガするイベントをモニタできます。たとえば、特定のアプリケーション層で発生したエラーを検出し、接続の切断がありリーフ ノードがダウンした場合、これらのアプリケーションを他の場所に再展開するアクションをトリガーできます。パケット ドロップが検出された特定のコントラクトがある場合、これらのコントラクトの複数のコピーを特定のアプリケーション上で有効化できます。また、レポートされた問題に基づいて特定のカウンタをモニタできる統計モニタリング ポリシーを使用できます。

『*Cisco APIC Management Information Model Reference*』で定義されている次の Python API はノースバウンド API を使用した REST POST コールのサブミットに使用できます。

- `vns:LDevVip`：デバイス クラスタをアップロードします
- `vns:CDev`：デバイスをアップロードします
- `vns:LIf`：論理インターフェイスを作成します
- `vns:AbsGraph`：グラフを作成します
- `vz:BrCP`：コントラクトにグラフを追加します

（注） エンドポイントセキュリティ グループ (ESG) の場合、エンドポイントグループと同じサービスグラフ展開 REST API を使用できます。ただし、コントラクトと ESG を関連付ける必要があります。

REST API を使用した自動化の例

ここでは、REST API を使用してタスクを自動化する例を示します。

次の REST 要求は、ブロードキャスト ドメインを持つテナント、レイヤ 3 ネットワーク、アプリケーション エンドポイント グループ、およびアプリケーション プロファイルを作成します。

```
<polUni>
    <fvTenant dn="uni/tn-acme" name="acme">

        <!—L3 Network-->
        <fvCtx name="MyNetwork"/>

        <!-- Bridge Domain for MySrvr EPG -->
        <fvBD name="MySrvrBD">
            <fvRsCtx tnFvCtxName="MyNetwork"/>
            <fvSubnet ip="10.10.10.10/24">
            </fvSubnet>
        </fvBD>

        <!-- Bridge Domain for MyClnt EPG -->
        <fvBD name="MyClntBD">
            <fvRsCtx tnFvCtxName="MyNetwork"/>
            <fvSubnet ip="20.20.20.20/24">
            </fvSubnet>
        </fvBD>

        <fvAp dn="uni/tn-acme/ap-MyAP" name="MyAP">

            <fvAEPg dn="uni/tn-acme/ap-MyAP/epg-MyClnt" name="MyClnt">
                <fvRsBd tnFvBDName="MySrvrBD"/>
                <fvRsDomAtt tDn="uni/vmmp-Vendor1/dom-MyVMs"/>
                <fvRsProv tnVzBrCPName="webCtrct"> </fvRsProv>
                <fvRsPathAtt tDn="topology/pod-1/paths-17/pathep-[eth1/21]"
                  encap="vlan-202"/>
                <fvRsPathAtt tDn="topology/pod-1/paths-18/pathep-[eth1/21]"
                  encap="vlan-202"/>
           </fvAEPg>

            <fvAEPg dn="uni/tn-acme/ap-MyAP/epg-MySRVR" name="MySRVR">
                <fvRsBd tnFvBDName="MyClntBD"/>
                <fvRsDomAtt tDn="uni/vmmp-Vendor1/dom-MyVMs"/>
                <fvRsCons tnVzBrCPName="webCtrct"> </fvRsCons>
                <fvRsPathAtt tDn="topology/pod-1/paths-17/pathep-[eth1/21]"
                  encap="vlan-203"/>
                <fvRsPathAtt tDn="topology/pod-1/paths-18/pathep-[eth1/21]"
                  encap="vlan-203"/>
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
```

次の REST 要求は VLAN ネームスペースを作成します。

```
<polUni>
    <infraInfra>
        <fvnsVlanInstP name="MyNS" allocMode="dynamic">
            <fvnsEncapBlk name="encap" from="vlan-201" to="vlan-300"/>
        </fvnsVlanInstP>
    </infraInfra>
</polUni>
```

次の REST 要求は VMM ドメインを作成します。

```
<polUni>
    <vmmProvP vendor="Vendor1">
        <vmmDomP name="MyVMs">
            <infraRsVlanNs tDn="uni/infra/vlanns-MyNS-dynamic"/>
            <vmmUsrAccP name="admin" usr="administrator" pwd="in$1eme"/>
            <vmmCtrlrP name="vcenter1" hostOrIp="192.168.64.186">
                <vmmRsAcc tDn="uni/vmmp-Vendor1/dom-MyVMs/usracc-admin"/>
            </vmmCtrlrP>
        </vmmDomP>
    </vmmProvP>
</polUni>
```

次の REST 要求は物理ドメインを作成します。

```
<polUni>
    <physDomP name="phys">
        <infraRsVlanNs tDn="uni/infra/vlanns-MyNS-dynamic"/>
    </physDomP>
</polUni>
```

次の REST 要求はデバイスクラスタを作成します。

```
<polUni>
    <fvTenant name="HA_Tenant1">

        <vnsLDevVip name="ADCCluster1" devtype="VIRTUAL" managed="no">
            <vnsRsALDevToDomP tDn="uni/vmmp-VMware/dom-mininet"/>
        </vnsLDevVip>

    </fvTenant>
</polUni>
```

次の REST 要求はデバイス クラスタ コンテキストを作成します。

```
<polUni>
    <fvTenant dn="uni/tn-acme" name="acme">
       <vnsLDevCtx ctrctNameOrLbl="webCtrct" graphNameOrLbl="G1" nodeNameOrLbl="Node1">

            <vnsRsLDevCtxToLDev tDn="uni/tn-acme/lDevVip-ADCCluster1"/>
            <vnsLIfCtx connNameOrLbl="ssl-inside">
                <vnsRsLIfCtxToLIf tDn="uni/tn-acme/lDevVip-ADCCluster1/lIf-int"/>
            </vnsLIfCtx>
            <vnsLIfCtx connNameOrLbl="any">
                <vnsRsLIfCtxToLIf tDn="uni/tn-acme/lDevVip-ADCCluster1/lIf-ext"/>
            </vnsLIfCtx>
        </vnsLDevCtx>
    </fvTenant>
</polUni>
```

次の要求は、ルーティング ピアリングに使用されるデバイス クラスタ コンテキストを作成します。

```
<polUni>
    <fvTenant dn="uni/tn-coke{{tenantId}}" name="coke{{tenantId}}">
        <vnsLDevCtx ctrctNameOrLbl="webCtrct1" graphNameOrLbl="WebGraph"
          nodeNameOrLbl="FW">
            <vnsRsLDevCtxToLDev tDn="uni/tn-tenant1/lDevVip-Firewall"/>
            <vnsLIfCtx connNameOrLbl="internal">
               <vnsRsLIfCtxToInstP tDn="uni/tn-tenant1/out-OspfInternal/instP-IntInstP"

                  status="created,modified"/>
                <vnsRsLIfCtxToLIf tDn="uni/tn-tenant1/lDevVip-Firewall/lIf-internal"/>
            </vnsLIfCtx>
            <vnsLIfCtx connNameOrLbl="external">
                <vnsRsLIfCtxToInstP tDn="uni/tn-common/out-OspfExternal/instP-ExtInstP"
                  status="created,modified"/>
                <vnsRsLIfCtxToLIf tDn="uni/tn-tenant1/lDevVip-Firewall/lIf-external"/>
            </vnsLIfCtx>
        </vnsLDevCtx>
    </fvTenant>
</polUni>
```

（注） テナント（レイヤ3 Outside）の外部接続の設定については、『*Cisco APIC* ベーシック コンフィギュレーション ガイド』を参照してください。

次の REST 要求はデバイス クラスタの論理インターフェイスを追加します。

```
<polUni>
    <fvTenant dn="uni/tn-acme" name="acme">
        <vnsLDevVip name="ADCCluster1">
            <vnsLIf name="C5">
                <vnsRsMetaIf tDn="uni/infra/mDev-Acme-ADC-1.0/mIfLbl-outside"/>
                <vnsRsCIfAtt tDn="uni/tn-acme/lDevVip-ADCCluster1/cDev-ADC1/cIf-int"/>
            </vnsLIf>
            <vnsLIf name="C4">
                <vnsRsMetaIf tDn="uni/infra/mDev-Acme-ADC-1.0/mIfLbl-inside"/>
                <vnsRsCIfAtt tDn="uni/tn-acme/lDevVip-ADCCluster1/cDev-ADC1/cIf-ext"/>
            </vnsLIf>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

次の REST 要求は物理デバイス クラスタの具象デバイスを追加します。

```
<polUni>
    <fvTenant dn="uni/tn-acme" name="acme">
        <vnsLDevVip name="ADCCluster1">
            <vnsCDev name="ADC1" devCtxLbl="C1">
                <vnsCIf name="int">
                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-17/pathep-[eth1/22]"/>
                </vnsCIf>
                <vnsCIf name="ext">
                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-17/pathep-[eth1/21]"/>
                </vnsCIf>
                <vnsCIf name="mgmt">
                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-17/pathep-[eth1/20]"/>
                </vnsCIf>
            </vnsCDev>
            <vnsCDev name="ADC2" devCtxLbl="C2">
                <vnsCIf name="int">
                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-17/pathep-[eth1/23]"/>
                </vnsCIf>
                <vnsCIf name="ext">
```

```
                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-17/pathep-[eth1/24]"/>
                </vnsCIf>
                <vnsCIf name="mgmt">
                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-17/pathep-[eth1/30]"/>
                </vnsCIf>
            </vnsCDev>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

次の REST 要求は仮想デバイス クラスタの具象デバイスを追加します。

```
<polUni>
    <fvTenant dn="uni/tn-coke5" name="coke5">
        <vnsLDevVip name="Firewall5" devtype="VIRTUAL">
            <vnsCDev name="ASA5" vcenterName="vcenter1" vmName="ifav16-ASAv-scale-05">
                <vnsCIf name="Gig0/0" vnicName="Network adapter 2"/>
                <vnsCIf name="Gig0/1" vnicName="Network adapter 3"/>
                <vnsCIf name="Gig0/2" vnicName="Network adapter 4"/>
                <vnsCIf name="Gig0/3" vnicName="Network adapter 5"/>
                <vnsCIf name="Gig0/4" vnicName="Network adapter 6"/>
                <vnsCIf name="Gig0/5" vnicName="Network adapter 7"/>
                <vnsCIf name="Gig0/6" vnicName="Network adapter 8"/>
                <vnsCIf name="Gig0/7" vnicName="Network adapter 9"/>
            </vnsCDev>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

次の REST 要求はサービスグラフを作成します。

```
<polUni>
    <fvTenant name="HA_Tenant1">
        <vnsAbsGraph name="g1">

            <vnsAbsTermNodeProv name="Input1">
                <vnsAbsTermConn name="C1">
                </vnsAbsTermConn>
            </vnsAbsTermNodeProv>

            <!-- Node1 Provides LoadBalancing functionality -->
            <vnsAbsNode name="Node1" managed="no">
                <vnsRsDefaultScopeToTerm
                  tDn="uni/tn-HA_Tenant1/AbsGraph-g1/AbsTermNodeProv-Input1/outtmnl"/>
                <vnsAbsFuncConn name="outside" attNotify="true">
                </vnsAbsFuncConn>
                <vnsAbsFuncConn name="inside" attNotify="true">
                </vnsAbsFuncConn>
            </vnsAbsNode>

            <vnsAbsTermNodeCon name="Output1">
                <vnsAbsTermConn name="C6">
                </vnsAbsTermConn>
            </vnsAbsTermNodeCon>

            <vnsAbsConnection name="CON2" adjType="L3" unicastRoute="yes">
                <vnsRsAbsConnectionConns
                  tDn="uni/tn-HA_Tenant1/AbsGraph-g1/AbsTermNodeCon-Output1/AbsTConn"/>
                <vnsRsAbsConnectionConns
                  tDn="uni/tn-HA_Tenant1/AbsGraph-g1/AbsNode-Node1/AbsFConn-outside"/>
            </vnsAbsConnection>

            <vnsAbsConnection name="CON1" adjType="L2" unicastRoute="no">
                <vnsRsAbsConnectionConns
                  tDn="uni/tn-HA_Tenant1/AbsGraph-g1/AbsNode-Node1/AbsFConn-inside"/>
```

```
                <vnsRsAbsConnectionConns
                  tDn="uni/tn-HA_Tenant1/AbsGraph-g1/AbsTermNodeProv-Input1/AbsTConn"/>
            </vnsAbsConnection>

        </vnsAbsGraph>
    </fvTenant>
</polUni>
```

次の REST 要求はフィルタ処理とセキュリティポリシー（コントラクト）を作成します。

```
<polUni>
    <fvTenant dn="uni/tn-acme" name="acme">
        <vzFilter name="HttpIn">
            <vzEntry name="e1" prot="6" dToPort="80"/>
        </vzFilter>

        <vzBrCP name="webCtrct">
            <vzSubj name="http">
                <vzRsSubjFiltAtt tnVzFilterName="HttpIn"/>
            </vzSubj>
        </vzBrCP>
    </fvTenant>
</polUni>
```

次の REST 要求はコントラクトにサービス グラフをアタッチします。

```
<polUni>
    <fvTenant name="acme">
        <vzBrCP name="webCtrct">
            <vzSubj name="http">
                <vzRsSubjGraphAtt graphName="G1" termNodeName="Input1"/>
            </vzSubj>
        </vzBrCP>
    </fvTenant>
</polUni>
```