基本ユーザ テナント設定

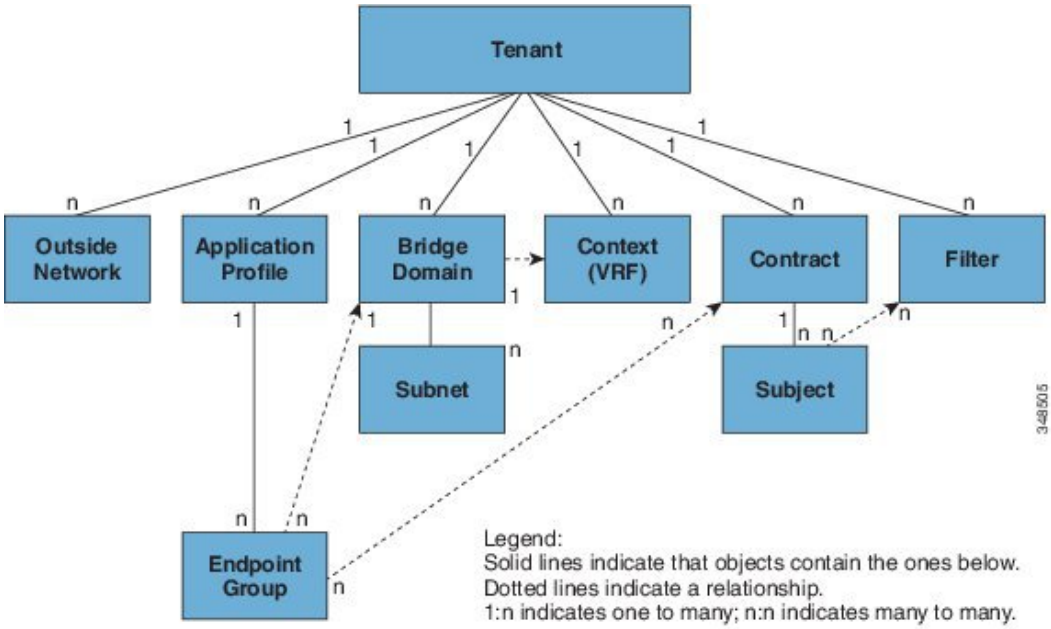
この章の内容は、次のとおりです。

テナント

テナント（fvTenant）は、アプリケーション ポリシーの論理コンテナで、管理者はドメインベースのアクセス コントロールを実行できます。テナントはポリシーの観点から分離の単位を表しますが、プライベート ネットワークは表しません。テナントは、サービス プロバイダーの環境では

お客様を、企業の環境では組織またはドメインを、または単にポリシーの便利なグループ化を表すことができます。次の図は、管理情報ツリー（MIT）のテナント部分の概要を示します。

図 *1*：テナント



テナントは相互に分離することも、リソースを共有することもできます。テナントが含む主要な要素は、フィルタ、コントラクト、外部ネットワーク、ブリッジ ドメイン、コンテキスト、およびエンドポイント グループ（EPG）を含むアプリケーション プロファイルです。テナントのエンティティはそのポリシーを継承します。テナントには、1 つ以上の仮想ルーティングおよび転送（VRF）インスタンスまたはコンテキストを含めることができます。各コンテキストは、複数のブリッジ ドメインに関連付けることができます。

（注） テナント ナビゲーション パス の下の APIC GUI では、コンテキスト（VRF）はプライベート ネットワークと呼ばれます。

テナントはアプリケーション ポリシーの論理コンテナです。ファブリックには複数のテナントを含めることができます。レイヤ 4 ～ 7 のサービスを展開する前に、テナントを設定する必要があります。ACI ファブリックは、テナント ネットワークに対して IPv4、IPv6、およびデュアル スタック構成をサポートします。

テナント内のルーティング

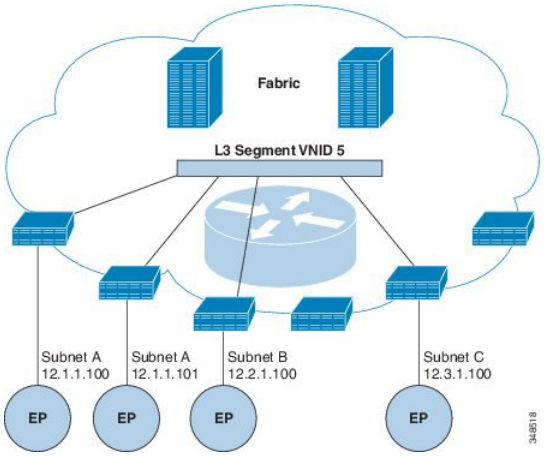
アプリケーション セントリック インフラストラクチャ（ACI）のファブリックでは、テナントのデフォルト ゲートウェイ機能が提供され、ファブリックの Virtual Extensible Local Area（VXLAN）

ネットワーク間のルーティングが行えます。各テナントについて、APIC でサブネットが作成されるたびに、ファブリックは仮想デフォルト ゲートウェイまたはスイッチ仮想インターフェイス（SVI）を提供します。これは、そのテナント サブネットの接続エンドポイントがあるすべてのスイッチにわたります。各入力インターフェイスはデフォルトのゲートウェイ インターフェイスをサポートし、ファブリック全体のすべての入力インターフェイスは任意のテナント サブネットに対する同一のルータの IP アドレスと MAC アドレスを共有します。

Intersubnet のテナント トラフィックを転送するために使用されるレイヤ 3 VNID

ACI モデルでは、ACI ファブリックのデフォルト ゲートウェイに送信されるファブリックのイングレスに到達するトラフィックは、レイヤ 3 VNID として知られる仮想ネットワーク セグメントにルーティングされます。単一のレイヤ 3 VNID が、各テナント コンテキストに割り当てられます。次の図は、テナント内のルーティングがどのように行われるかを示します。

図 *2*：*Intersubnet* のテナント トラフィックを転送するレイヤ *3 VNID*



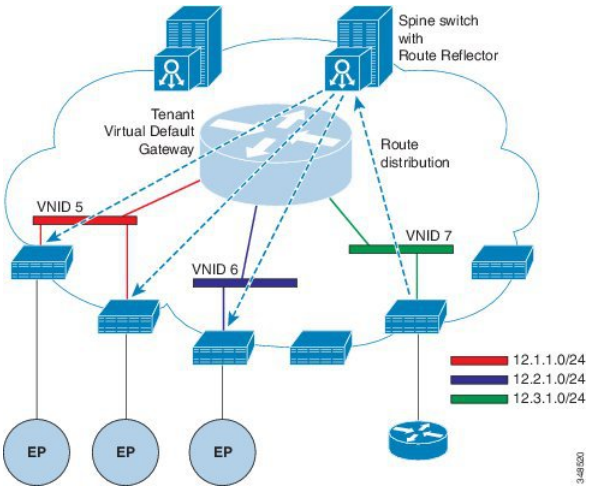
レイヤ 3 VNID は、APIC によって割り当てられます。ファブリックを経由するトラフィックは、レイヤ 3 セグメントの VNID を使用して転送されます。出力リーフ スイッチでは、パケットはレイヤ 3 セグメントの VNID から出力サブネットの VNID にルーティングされます。

ACI モデルでは、テナント内でルーティングされるトラフィックのファブリックで非常に効率的な転送が提供されます。たとえば、同じ物理ホストの同じテナントに属するがサブネットは異なる 2 つの仮想マシン（VM）間のトラフィックでは、（最小パス コストを使用して）正しい宛先にルーティングされる前の移動先は入力スイッチのみです。現在の VM 環境では、トラフィックは正しい宛先にルーティングされる前に、（異なる物理サーバ上にあると思われる）エッジ VM に伝送されます。

ルータ ピアリングおよびルート配布

次の図に示すように、ルーティング ピア モデルを使用すると、リーフ スイッチ インターフェイスが外部ルータのルーティング プロトコルとピアリングするように静的に設定されます。

図 *3*：ルータのピアリング

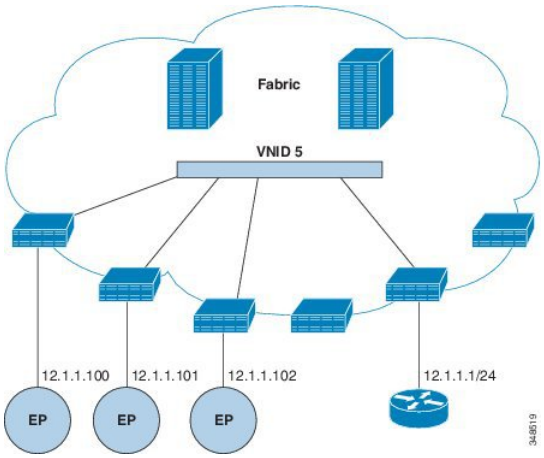


ピアリングによって学習されるルートは、スパイン スイッチに送信されます。スパイン スイッチはルート リフレクタとして動作し、外部ルートを同じテナントに属するインターフェイスを持つすべてのリーフ スイッチに配布します。これらのルートは、最長プレフィクス照合（LPM）により集約されたアドレスで、外部ルータが接続されているリモートのリーフ スイッチの VTEP IP アドレスが含まれるリーフ スイッチの転送テーブルに配置されます。WAN ルートには転送プロキシはありません。WAN ルートがリーフ スイッチの転送テーブルに適合しない場合、トラフィックはドロップされます。外部ルータがデフォルト ゲートウェイではないため、テナントのエンドポイント（EP）からのパケットはACI ファブリックのデフォルト ゲートウェイに送信されます。

外部ルータへのブリッジド インターフェイス

次の図に示すように、リーフ スイッチのインターフェイスがブリッジドインターフェイスとして設定されている場合、テナント VNID のデフォルト ゲートウェイが外部ルータとなります。

図 *4*：ブリッジド外部ルータ



ACI ファブリックは、外部ルータの存在を認識せず、APIC はリーフ スイッチのインターフェイスを EPG に静的に割り当てます。

ルート リフレクタの設定

ACI ファブリックのルート リフレクタは、マルチプロトコル BGP（MP-BGP）を使用してファブリック内に外部ルートを配布します。ACI ファブリックでルート リフレクタをイネーブルにするには、ファブリックの管理者がルートリフレクタになるスパインスイッチを選択して、自律システム（AS）番号を提供する必要があります。ルート リフレクタが ACI ファブリックでイネーブルになると、管理者は次の項で説明するように、外部ネットワークへの接続を設定できます。

ACI ファブリックに外部ルータを接続するには、ファブリック インフラストラクチャの管理者がボーダー ゲートウェイ プロトコル（BGP）のルート リフレクタとしてスパイン ノードを設定します。冗長性のために、複数のスパインがルータ リフレクタ ノードとして設定されます（1 台のプライマリ リフレクタと 1 台のセカンダリ リフレクタ）。

テナントが ACI ファブリックに WAN ルータを接続する必要がある場合は、インフラストラクチャの管理者が WAN ルータが WAN のトップ オブ ラック（ToR）として接続されるリーフ ノードを（以下の通りに）設定し、この WAN ToR を BGP ピアとしてルート リフレクタ ノードの 1 つと組み合わせます。ルート リフレクタが WAN ToR に設定されていると、ファブリックにテナント ルートをアドバタイズできます。

各リーフ ノードには最大 4000 のルートを保存できます。WAN ルータが 4000 を超えるルートをアドバタイズしなければならない場合、複数のリーフ ノードとピアリングする必要があります。

インフラストラクチャの管理者は、ペアになったリーフ ノードそれぞれをアドバタイズできるルート（またはルート プレフィクス）で設定します。

インフラストラクチャの管理者は、次のようにファブリックに接続されている外部 WAN ルータを設定する必要があります。

1. ルート リフレクタとして最大 2 つのスパイン ノードを設定します。冗長性のために、プライマリおよびセカンダリ ルート リフレクタを設定します。
2. WAN ToR で、プライマリおよびセカンダリ ルート リフレクタのノードを設定します。
3. WAN ToR で、ToR がアドバタイズを担当するルートを設定します。これは任意で、テナント ルータが 4000 を超えるルートをアドバタイズすることがわかっている場合にのみ行う必要があります。

テナントの外部接続の設定

スタティック ルートをアプリケーション セントリック インフラストラクチャ（ACI）ファブリック上の他のリーフ スイッチに配布する前に、マルチプロトコル BGP（MP-BGP）プロセスが最初に動作していて、スパイン スイッチが BGP ルート リフレクタとして設定されている必要があります。

ACI ファブリックを外部ルーテッド ネットワークに統合するために、管理テナントのレイヤ 3 接続に対し Open Shortest Path First（OSPF）を設定できます。

拡張 GUI を使用した MP-BGP ルート リフレクタの設定

（注） このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。

ステップ 1 メニュー バーで、[FABRIC] > [Fabric Policies] を選択します。

ステップ 2 [Navigation] ペインで、[Pod Policies] > [Policies] > [BGP Route Reflector default] を展開し、[BGP Route Reflector default] を右クリックし、[Create Route Reflector Node Policy EP] をクリックします。

ステップ 3 [Create Route Reflector Node Policy EP] ダイアログボックスで、[Spine Node] ドロップダウン リストから、適切なスパイン ノードを選択します。[Submit] をクリックします。

（注） 必要に応じてスパイン ノードを追加するには、上記の手順を繰り返してください。

スパイン スイッチがルート リフレクタ ノードとしてマークされます。

ステップ 4 [BGP Route Reflector default] プロパティ領域で、[Autonomous System Number] フィールドで、適切な番号を選択します。[Submit] をクリックします。

（注） 自律システム番号は、Border Gateway Protocol（BGP）がルータに設定されている場合は、リーフが接続されたルータ設定に一致する必要があります。スタティックまたは Open Shortest Path First（OSPF）を使用して学習されたルートを使用している場合は、自律システム番号値を任意の有効な値にできます。

ステップ 5 [Navigation] ペインで、[Policy Groups] を展開して右クリックし、[Create POD Policy Group] をクリックします。

ステップ 6 [Create POD Policy Group] ダイアログボックスで、[Name] フィールドに、ポッド ポリシー グループの名前を入力します。

ステップ 7 [BGP Route Reflector Policy] ドロップダウン リストで、適切なポリシー（デフォルト）を選択します。[Submit] をクリックします。
BGP ルート リフレクタのポリシーは、ルート リフレクタのポッド ポリシー グループに関連付けられ、BGP プロセスはリーフ スイッチでイネーブルになります。

ステップ 8 [Navigation] ペインで、[Pod Policies] > [Profiles] > [default] の順に選択します。[Work] ペインで、[Fabric Policy Group] ドロップダウン リストから、前に作成されたポッド ポリシーを選択します。[Submit] をクリックします。
ポッド ポリシー グループが、ファブリック ポリシー グループに適用されました。

拡張 GUI を使用した管理テナントの OSPF 外部ルーテッド ネットワークの作成

- ルータ ID と論理インターフェイス プロファイルの IP アドレスが異なっていて重複していないことを確認します。
- 次の手順は、管理テナントの OSPF 外部ルーテッド ネットワークを作成するためのものです。テナントの OSPF 外部ルーテッド ネットワークを作成するには、テナントを選択し、テナント用の VRF を作成する必要があります。
- 詳細については、トランジット ルーティングに関する KB 記事も参照してください。

（注） このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。

ステップ 1 メニュー バーで、[TENANTS] > [mgmt] を選択します。

ステップ 2 [Navigation] ペインで、[Networking] > [External Routed Networks] を展開します。

ステップ 3 [External Routed Networks] を右クリックし、[Create Routed Outside] をクリックします。

ステップ 4 [Create Routed Outside] 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、名前（RtdOut）を入力します。

b) [OSPF] チェックボックスをオンにします。

c) [OSPF Area ID] フィールドに、エリア ID を入力します。
d) [OSPF Area Control] フィールドで、適切なチェックボックスをオンにします。
e) [OSPF Area Type] フィールドで、適切なエリア タイプを選択します。
f) [OSPF Area Cost] フィールドで、適切な値を選択します。
g) [VRF] フィールドのドロップダウン リストから、VRF（inb）を選択します。
（注） このステップでは、ルーテッド Outside をインバンド VRF に関連付けます。
h) [External Routed Domain] ドロップダウン リストから、適切なドメインを選択します。
i) [Nodes and Interfaces Protocol Profiles] 領域の [+] アイコンをクリックします。

ステップ 5 [Create Node Profile] 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、ノード プロファイルの名前を入力します（borderLeaf）。
b) [Nodes] フィールドで、[+] アイコンをクリックして [Select Node] ダイアログボックスを表示します。
c) [Node ID] フィールドで、ドロップダウン リストから、最初のノードを選択します（leaf1）。
d) [Router ID] フィールドに、一意のルータ ID を入力します。
e) [Use Router ID as Loopback Address] フィールドをオフにします。
（注） デフォルトでは、ルータ ID がループバック アドレスとして使用されます。これらが異なるようにする場合は、[Use Router ID as Loopback Address] チェックボックスをオフにします。
f) [Loopback Addresses] を展開し、[IP] フィールドに IP アドレスを入力します。[Update] をクリックし、[OK] をクリックします。
希望する IPv4 または IPv6 の IP アドレスを入力します。
g) [Nodes] フィールドで、[+] アイコンを展開して [Select Node] ダイアログボックスを表示します。
（注） 2 つ目のノード ID を追加します。
h) [Node ID] フィールドで、ドロップダウン リストから、次のノードを選択します（leaf2）。
i) [Router ID] フィールドに、一意のルータ ID を入力します。
j) [Use Router ID as Loopback Address] フィールドをオフにします。
（注） デフォルトでは、ルータ ID がループバック アドレスとして使用されます。これらが異なるようにする場合は、[Use Router ID as Loopback Address] チェックボックスをオフにします。
k) [Loopback Addresses] を展開し、[IP] フィールドに IP アドレスを入力します。[Update] をクリックし、[OK] をクリックします。[OK] をクリックします。
希望する IPv4 または IPv6 の IP アドレスを入力します。

ステップ 6 [Create Node Profile] ダイアログボックスで、[OSPF Interface Profiles] 領域の [+] アイコンをクリックします。

ステップ 7 [Create Interface Profile] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、プロファイルの名前（portProf）を入力します。
b) [Interfaces] 領域で、[Routed Interfaces] タブをクリックし、[+] アイコンをクリックします。
c) [Select Routed Interfaces] ダイアログボックスの [Path] フィールドで、ドロップダウン リストから、最初のポート（leaf1、ポート 1/40）を選択します。
d) [IP Address] フィールドに、IP アドレスとマスクを入力します。[OK] をクリックします。

e) [Interfaces] 領域で、[Routed Interfaces] タブをクリックし、[+] アイコンをクリックします。
f) [Select Routed Interfaces] ダイアログボックスの [Path] フィールドで、ドロップダウン リストから、2 つ目のポート（leaf2、ポート 1/40）を選択します。
g) [IP Address] フィールドに、IP アドレスとマスクを入力します。[OK] をクリックします。
（注） この IP アドレスは、前に leaf1 に入力した IP アドレスと異なっている必要があります。
h) [Create Interface Profile] ダイアログボックスで、[OK] をクリックします。

インターフェイスが OSPF インターフェイスとともに設定されます。

ステップ 8 [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 9 [Create Routed Outside] ダイアログボックスで、[Next] をクリックします。
[Step 2 External EPG Networks] 領域が表示されます。

ステップ 10 [External EPG Networks] 領域で、[+] アイコンをクリックします。

ステップ 11 [Create External Network] 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、外部ネットワークの名前（extMgmt）を入力します。
b) [Subnet] を展開し、[Create Subnet] ダイアログボックスの [IP address] フィールドに、サブネットの IP アドレスとマスクを入力します。
c) [Scope] フィールドで、目的のチェックボックスをオンにします。[OK] をクリックします。
d) [Create External Network] ダイアログボックスで、[OK] をクリックします。
e) [Create Routed Outside] ダイアログボックスで、[Finish] をクリックします。
（注） [Work] ペインで、[External Routed Networks] 領域に、外部ルーテッド ネットワークのアイコン（RtdOut）が表示されるようになりました。

REST API を使用した MP-BGP ルート リフレクタの設定

ステップ 1 スパイン スイッチをルート リフレクタとしてマークします。

例：

```
POST URL: https://apic-ip/api/policymgr/mo/uni/fabric.xml

<bgpInstPol name="default">
  <bgpAsP asn="1" />
  <bgpRRP>
     <bgpRRNodePEp id="<spine_id1>"/>
     <bgpRRNodePEp id="<spine_id2>"/>
  </bgpRRP>
</bgpInstPol>
```

ステップ 2 次のポストを使用してポッド セレクタをセットアップします。

例：

FuncP セットアップの場合：

```
POST URL:
https://APIC-IP/api/policymgr/mo/uni.xml

<fabricFuncP>
  <fabricPodPGrp name="bgpRRPodGrp”>
    <fabricRsPodPGrpBGPRRP tnBgpInstPolName="default" />
  </fabricPodPGrp>
</fabricFuncP>
```

例：
PodP セットアップの場合：

```
POST URL:
https://APIC-IP/api/policymgr/mo/uni.xml

<fabricPodP name="default">
  <fabricPodS name="default" type="ALL">
    <fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-bgpRRPodGrp"/>
  </fabricPodS>
</fabricPodP>
```

MP-BGP ルート リフレクタ設定の確認

ステップ 1 次の操作を実行して、設定を確認します。

a) セキュア シェル（SSH）を使用して、必要に応じて各リーフ スイッチへの管理者としてログインします。

b) **show processes | grep bgp** コマンドを入力して、状態が S であることを確認します。
状態が NR（実行していない）である場合は、設定が正常に行われませんでした。

ステップ 2 次の操作を実行して、自律システム番号がスパイン スイッチで設定されていることを確認します。

a) SSH を使用して、必要に応じて各スパイン スイッチへの管理者としてログインします。

b) シェル ウィンドウから次のコマンドを実行します。

例：
cd /mit/sys/bgp/inst

例：
grep asn summary

設定した自律システム番号が表示される必要があります。自律システム番号の値が 0 と表示される場合は、設定が正常に行われませんでした。

テナント、VRF、およびブリッジ ドメインの作成

テナントの概要

- テナントには、承認されたユーザのドメインベースのアクセス コントロールをイネーブルにするポリシーが含まれます。承認されたユーザは、テナント管理やネットワーキング管理などの権限にアクセスできます。
- ユーザは、ドメイン内のポリシーにアクセスしたりポリシーを設定するには読み取り/書き込み権限が必要です。テナント ユーザは、1 つ以上のドメインに特定の権限を持つことができます。
- マルチテナント環境では、リソースがそれぞれ分離されるように、テナントによりグループ ユーザのアクセス権限が提供されます（エンドポイント グループやネットワーキングなどのため）。これらの権限では、異なるユーザが異なるテナントを管理することもできます。

テナントの作成

テナントには、最初にテナントを作成した後に作成できるフィルタ、契約、ブリッジ ドメイン、およびアプリケーション プロファイルなどのプライマリ要素が含まれます。

VRF およびブリッジ ドメイン

テナントの VRF およびブリッジ ドメインを作成および指定できます。定義されたブリッジ ドメイン要素のサブネットは、対応するレイヤ 3 コンテキストを参照します。

IPv6 ネイバー探索の有効化の詳細については、関連 KB 記事、「*KB: Creating a Tenant, VRF, and Bridge Domain with IPv6 Neighbor Discovery*」を参照してください。

拡張 GUI を使用したテナント、VRF、およびブリッジ ドメインの作成

- このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。
- 外部ルーテッドを設定するときにパブリック サブネットがある場合は、ブリッジ ドメインを外部設定と関連付ける必要があります。

手順の概要

1. メニュー バーで、[TENANT] > [Add Tenant] の順にクリックします。
2. [Create Tenant] ダイアログボックスで、次のタスクを実行します。
3. [Navigation] ペインで、[Tenant-name] > [Networking] の順に展開し、[Work] ペインで、[VRF] アイコンをキャンバスにドラッグして [Create VRF] ダイアログボックスを開き、次のタスクを実行します。
4. [Networking] ペインで、[BD] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Bridge Domain] ダイアログボックスが表示されたら、次のタスクを実行します。
5. [Networks] ペインで、[L3] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Routed Outside] ダイアログボックスが表示されたら、次のタスクを実行します。

手順の詳細

ステップ 1 メニュー バーで、[TENANT] > [Add Tenant] の順にクリックします。

ステップ 2 [Create Tenant] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) [Security Domains +] アイコンをクリックして [Create Security Domain] ダイアログボックスを開きます。
c) [Name] フィールドに、セキュリティ ドメインの名前を入力します。[Submit] をクリックします。
d) [Create Tenant] ダイアログボックスで、作成したセキュリティ ドメインのチェックボックスをオンにし、[Submit] をクリックします。

ステップ 3 [Navigation] ペインで、[Tenant-name] > [Networking] の順に展開し、[Work] ペインで、[VRF] アイコンをキャンバスにドラッグして [Create VRF] ダイアログボックスを開き、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) [Submit] をクリックして VRF の設定を完了します。

ステップ 4 [Networking] ペインで、[BD] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Bridge Domain] ダイアログボックスが表示されたら、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) [L3 Configurations] タブをクリックします。
c) [Subnets] を展開して [Create Subnet] ダイアログボックスを開き、[Gateway IP] フィールドにサブネット マスクを入力し、[OK] をクリックします。
d) [Submit] をクリックしてブリッジ ドメインの設定を完了します。

ステップ 5 [Networks] ペインで、[L3] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Routed Outside] ダイアログボックスが表示されたら、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) [Nodes And Interfaces Protocol Profiles] を展開して [Create Node Profile] ダイアログボックスを開きます。
c) [Name] フィールドに、名前を入力します。
d) [Nodes] を展開して [Select Node] ダイアログボックスを開きます。

e) [Node ID] フィールドで、ドロップダウン リストからノードを選択します。
f) [Router ID] フィールドに、ルータ ID を入力します。
g) [Static Routes] を展開して [Create Static Route] ダイアログボックスを開きます。
h) [Prefix] フィールドに、IPv4 アドレスまたは IPv6 アドレスを入力します。
i) [Next Hop Addresses] を展開し、[Next Hop IP] フィールドに IPv4 アドレスまたは IPv6 アドレスを入力します。
j) [Preference] フィールドに数値を入力し、[UPDATE] をクリックしてから [OK] をクリックします。
k) [Select Node] ダイアログボックスで、[OK] をクリックします。
l) [Create Node Profile] ダイアログボックスで、[OK] をクリックします。
m) 必要に応じてチェックボックス [BGP]、[OSPF]、または [EIGRP] をオンにし、[NEXT] をクリックします。[OK] をクリックしてレイヤ 3 の設定を完了します。

L3 設定を確認するには、[Navigation] ペインで、[Networking] > [VRFs] の順に展開します。

アプリケーション ポリシーの展開

セキュリティ ポリシーの適用

トラフィックは前面パネルのインターフェイスからリーフ スイッチに入り、パケットは送信元 EPG の EPG でマーキングされます。リーフ スイッチはその後、テナント エリア内のパケットの宛先IPアドレスでフォワーディングルックアップを実行します。ヒットすると、次のシナリオのいずれかが発生する可能性があります。

1. ユニキャスト（/32）ヒットでは、宛先エンドポイントの EPG と宛先エンドポイントが存在するローカル インターフェイスまたはリモート リーフ スイッチの VTEP IP アドレスが提供されます。
2. サブネット プレフィクス（/32 以外）のユニキャスト ヒットでは、宛先サブネット プレフィクスの EPG と宛先サブネット プレフィクスが存在するローカル インターフェイスまたはリモート リーフ スイッチの VTEP IP アドレスが提供されます。
3. マルチキャスト ヒットでは、ファブリック全体の VXLAN カプセル化とマルチキャスト グループの EPG で使用するローカル レシーバのローカル インターフェイスと外側の宛先 IP アドレスが提供されます。

（注） マルチキャストと外部ルータのサブネットは、入力リーフ スイッチでのヒットを常にもたらします。セキュリティ ポリシーの適用は、宛先 EPG が入力リーフ スイッチによって認識されるとすぐに発生します。

転送テーブルの誤りにより、パケットがスパイン スイッチの転送プロキシに送信されます。転送プロキシはその後、転送テーブル検索を実行します。これが誤りである場合、パケットはドロップされます。これがヒットの場合、パケットは宛先エンドポイントを含む出力リーフ スイッチに送信されます。出力リーフ スイッチが宛先の EPG を認識するため、セキュリティ ポリシーの適用が実行されます。出力リーフ スイッチは、パケット送信元の EPG を認識する必要があります。ファブリック ヘッダーは、入力リーフ スイッチから出力リーフ スイッチに EPG を伝送するため、このプロセスをイネーブルにします。スパイン スイッチは、転送プロキシ機能を実行するときに、パケット内の元の EPG を保存します。

出力リーフ スイッチでは、送信元 IP アドレス、送信元 VTEP、および送信元 EPG 情報は、学習によってローカルの転送テーブルに保存されます。ほとんどのフローが双方向であるため、応答パケットがフローの両側で転送テーブルに入力し、トラフィックが両方向で入力フィルタリングされます。

セキュリティ ポリシー仕様を含むコントラクト

ACI セキュリティ モデルでは、コントラクトに EPG 間の通信を管理するポリシーが含まれます。コントラクトは通信内容を指定し、EPG は通信の送信元と宛先を指定します。コントラクトは次のように EPG をリンクします。

EPG 1 ---------- コントラクト ---------- EPG 2

コントラクトで許可されていれば、EPG 1 のエンドポイントは EPG 2 のエンドポイントと通信でき、またその逆も可能です。このポリシーの構造には非常に柔軟性があります。たとえば、EPG 1 と EPG 2 間には多くのコントラクトが存在でき、1 つのコントラクトを使用する EPG が 3 つ以上存在でき、コントラクトは複数の EPG のセットで再利用できます。

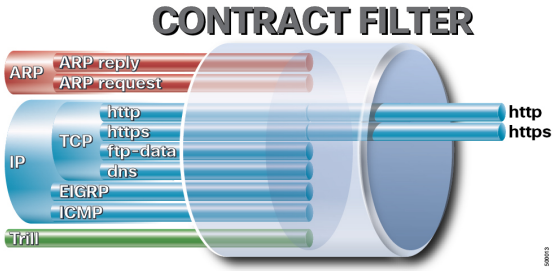
また EPG とコントラクトの関係には方向性があります。EPG はコントラクトを提供または消費できます。コントラクトを提供する EPG は通常、一連のクライアントデバイスにサービスを提供する一連のエンドポイントです。そのサービスによって使用されるプロトコルはコントラクトで定義されます。コントラクトを消費する EPG は通常、そのサービスのクライアントである一連のエンドポイントです。クライアントエンドポイント（コンシューマ）がサーバエンドポイント（プロバイダー）に接続しようとすると、コントラクトはその接続が許可されるかどうかを確認します。特に指定のない限り、そのコントラクトは、サーバがクライアントへの接続を開始することを許可しません。ただし、EPG 間の別のコントラクトが、その方向の接続を簡単に許可する場合があります。

この提供/消費の関係は通常、EPG とコントラクト間を矢印を使って図で表されます。次に示す矢印の方向に注目してください。

EPG 1 <------- 消費 -------- コントラクト <------- 提供 -------- EPG 2

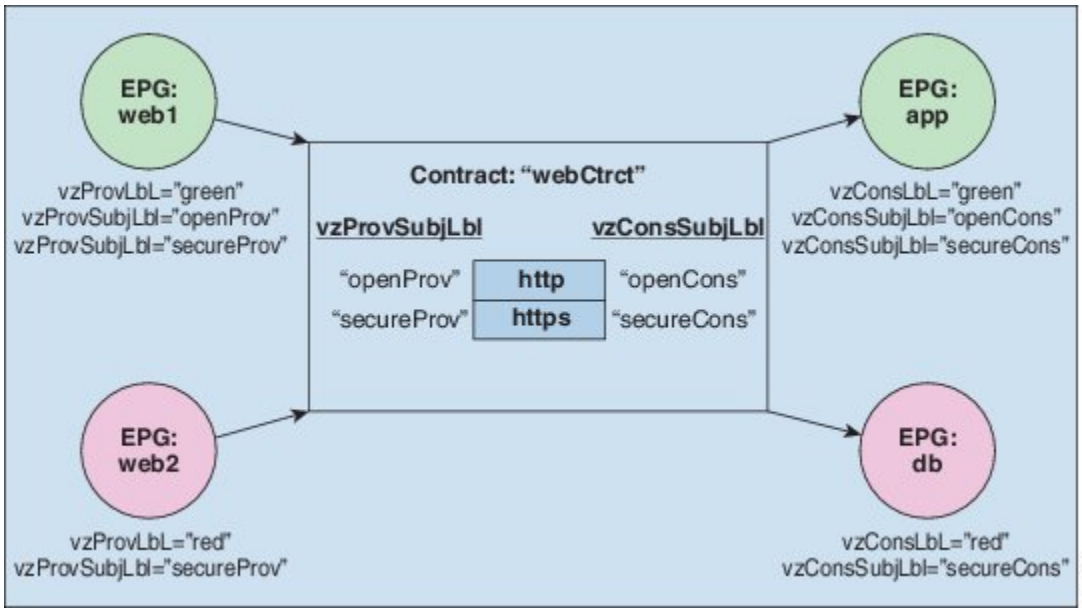
コントラクトは階層的に構築されます。1 つ以上のサブジェクトで構成され、各サブジェクトには 1 つ以上のフィルタが含まれ、各フィルタは 1 つ以上のプロトコルを定義できます。

図 *5*：コントラクト フィルタ



次の図は、コントラクトが EPG の通信をどのように管理するかを示します。

図 *6*：*EPG/EPG* 通信を決定するコントラクト



たとえば、TCP ポート 80 とポート 8080 を指定する HTTP と呼ばれるフィルタと、TCP ポート 443 を指定する HTTPS と呼ばれる別のフィルタを定義できます。その後、2 セットのサブジェクトを持つ webCtrct と呼ばれるコントラクトを作成できます。openProv と openCons are は HTTP フィルタが含まれるサブジェクトです。secureProv と secureCons は HTTPS フィルタが含まれるサブジェクトです。この webCtrct コントラクトは、Web サービスを提供する EPG とそのサービスを消費するエンドポイントを含む EPG 間のセキュアな Web トラフィックと非セキュアな Web トラフィックの両方を可能にするために使用できます。

これらの同じ構造は、仮想マシンのハイパーバイザを管理するポリシーにも適用されます。EPG が Virtual Machine Manager（VMM）のドメイン内に配置されると、APIC は EPG に関連付けられたすべてのポリシーを VMM ドメインに接続するインターフェイスを持つリーフ スイッチにダウ

ンロードします。VMM ドメインの完全な説明については、『ACI の基本』マニュアルの「Virtual Machine Manager のドメイン」の章を参照してください。このポリシーが作成されると、APIC は EPG のエンドポイントへの接続を可能にするスイッチを指定する VMM ドメインにそれをプッシュ（あらかじめ入力）します。VMM ドメインは、EPG 内のエンドポイントが接続できるスイッチとポートのセットを定義します。エンドポイントがオンラインになると、適切な EPG に関連付けられます。パケットが送信されると、送信元 EPG および宛先 EPG がパケットから取得され、対応するコントラクトで定義されたポリシーでパケットが許可されたかどうかが確認されます。許可された場合は、パケットが転送されます。許可されない場合は、パケットはドロップされます。

コントラクトは、許可や拒否よりも複雑なアクションも許可します。コントラクトは、所定のサブジェクトに一致するトラフィックをサービスにリダイレクトしたり、コピーしたり、その QoS レベルを変更したりできることを指定可能です。具象モデルでアクセス ポリシーをあらかじめ入力すると、APIC がオフラインまたはアクセスできない場合でも、エンドポイントは移動でき、新しいエンドポイントをオンラインにでき、通信を行うことができます。APIC は、ネットワークの単一の障害発生時点から除外されます。ACI ファブリックにパケットが入力されると同時に、セキュリティ ポリシーがスイッチで実行している具象モデルによって適用されます。

Three-Tier アプリケーションの展開

フィルタは、フィルタを含む契約により許可または拒否されるデータ プロトコルを指定します。契約には、複数のサブジェクトを含めることができます。サブジェクトは、単方向または双方向のフィルタを実現するために使用できます。単方向フィルタは、コンシューマからプロバイダー（IN）のフィルタまたはプロバイダーからコンシューマ（OUT）のフィルタのどちらか一方向に使用されるフィルタです。双方向フィルタは、両方の方向で使用される同一フィルタです。これは、再帰的ではありません。

契約は、エンドポイント グループ間（EPG 間）の通信をイネーブルにするポリシーです。これらのポリシーは、アプリケーション層間の通信を指定するルールです。契約が EPG に付属していない場合、EPG 間の通信はデフォルトでディセーブルになります。EPG 内の通信は常に許可されているので、EPG 内の通信には契約は必要ありません。

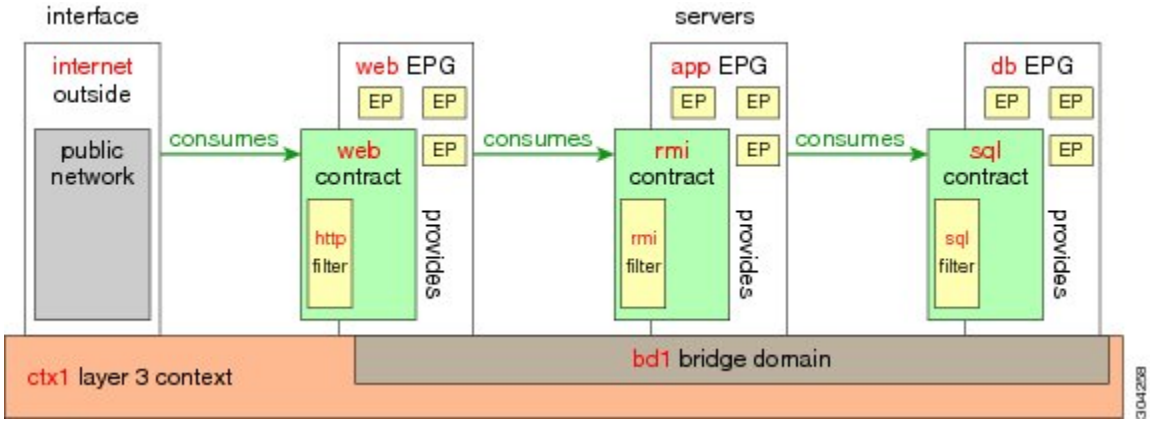
アプリケーション プロファイルでは、APIC がその後ネットワークおよびデータセンターのインフラストラクチャで自動的にレンダリングするアプリケーション要件をモデル化することができます。アプリケーション プロファイルでは、管理者がインフラストラクチャの構成要素ではなくアプリケーションの観点から、リソース プールにアプローチすることができます。アプリケーション プロファイルは、互いに論理的に関連する EPG を保持するコンテナです。EPG は同じアプリケーション プロファイル内の他の EPG および他のアプリケーション プロファイル内の EPG と通信できます。

アプリケーションポリシーを展開するには、必要なアプリケーションプロファイル、フィルタ、および契約を作成する必要があります。通常、APIC ファブリックは、テナント ネットワーク内の Three-Tier アプリケーションをホストします。この例では、アプリケーションは 3 台のサーバ（Web サーバ、アプリケーション サーバ、およびデータベース サーバ）を使用して実行されます。Three-Tier アプリケーションの例については、次の図を参照してください。

Web サーバには HTTP フィルタがあり、アプリケーション サーバには Remote Method Invocation（RMI）フィルタがあり、データベース サーバには Structured Query Language（SQL）フィルタが

あります。アプリケーション サーバは、SQL 契約を消費してデータベース サーバと通信します。Web サーバは、RMI 契約を消費して、アプリケーション サーバと通信します。トラフィックは Web サーバから入り、アプリケーション サーバと通信します。アプリケーション サーバはその後、データベース サーバと通信し、トラフィックは外部に通信することもできます。

図 *7*：*Three-Tier* アプリケーションの図



http 用のフィルタを作成するパラメータ

この例での http 用のフィルタを作成するパラメータは次のとおりです。

パラメータ名	http のフィルタ
名前	http
エントリの数	2
エントリ名	Dport-80 Dport-443
Ethertype	IP
プロトコル	tcp tcp
宛先ポート	http https

rmi および sql 用のフィルタを作成するパラメータ

この例での rmi および sql 用のフィルタを作成するパラメータは次のとおりです。

パラメータ名	rmi のフィルタ	sql のフィルタ
名前	rmi	sql
エントリの数	1	1
エントリ名	Dport-1099	Dport-1521
Ethertype	IP	IP
プロトコル	tcp	tcp
宛先ポート	1099	1521

アプリケーション プロファイル データベースの例

この例のアプリケーション プロファイル データベースは次のとおりです。

EPG	提供される契約	消費される契約
Web	Web	rmi
app	rmi	sql
db	sql	--

GUI を使用したアプリケーション ポリシーの展開

GUI を使用したフィルタの作成

3 つの個別のフィルタを作成します。この例では、HTTP、RMI、SQL です。このタスクでは、HTTP フィルタを作成する方法を示します。このタスクは、他のフィルタを作成するタスクと同じです。

はじめる前に

テナント、ネットワーク、およびブリッジ ドメインが作成されていることを確認します。

手順の概要

1. メニュー バーで、[TENANTS] を選択します。[Navigation] ペインで、[tenant] > [Security Policies] を展開し、[Filters] を右クリックして、[Create Filter] をクリックします。
2. [Create Filter] ダイアログボックスで、次の操作を実行します。
3. [Name] フィールドの [Entries] を展開します。同じプロセスを実行して、別のエントリを宛先ポートとして HTTPS で追加し、[Update] をクリックします。
4. さらに 2 つのフィルタ（rmi および sql）を作成し、rmi および sql 用のフィルタを作成するパラメータ，（18 ページ）に示すパラメータを使用するには、上記手順の同じプロセスを実行します。

手順の詳細

ステップ 1 メニュー バーで、[TENANTS] を選択します。[Navigation] ペインで、[tenant] > [Security Policies] を展開し、[Filters] を右クリックして、[Create Filter] をクリックします。

（注） [Navigation] ペインで、フィルタを追加するテナントを展開します。

ステップ 2 [Create Filter] 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、フィルタ名（http）を入力します。
b) [Entries] を展開し、[Name] フィールドに、名前（Dport-80）を入力します。
c) [EtherType] ドロップダウン リストから、EtherType（IP）を選択します。
d) [IP Protocol] ドロップダウン リストから、プロトコル（tcp）を選択します。
e) [Destination Port/Range] ドロップダウン リストから、[From] フィールドと [To] フィールドで、[http] を選択します。（http）
f) [Update] をクリックし、[Submit] をクリックします。
新しく追加されたフィルタが、[Navigation] ペインと [Work] ペインに表示されます。

ステップ 3 [Name] フィールドの [Entries] を展開します。同じプロセスを実行して、別のエントリを宛先ポートとして HTTPS で追加し、[Update] をクリックします。
この新しいフィルタ ルールが追加されます。

ステップ 4 さらに 2 つのフィルタ（rmi および sql）を作成し、rmi および sql 用のフィルタを作成するパラメータ，（18 ページ）に示すパラメータを使用するには、上記手順の同じプロセスを実行します。

GUI を使用した契約の作成

手順の概要

1. メニュー バーで、[TENANTS] と実行するテナント名を選択します。[Navigation] ペインで、[tenant] > [Security Policies] を展開します。
2. [Contracts] > [Create Contract] を右クリックします。
3. [Create Contract] ダイアログボックスで、次のタスクを実行します。
4. [Create Contract Subject] ダイアログボックスで、[OK] をクリックします。
5. この手順と同じステップに従って、rmi と sql 用の契約をさらに 2 つ作成します。rmi 契約の場合は rmi サブジェクトを選択し、sql の場合は sql サブジェクトを選択します。

手順の詳細

ステップ 1 メニュー バーで、[TENANTS] と実行するテナント名を選択します。[Navigation] ペインで、[tenant] > [Security Policies] を展開します。

ステップ 2 [Contracts] > [Create Contract] を右クリックします。

ステップ 3 [Create Contract] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、契約名（web）を入力します。

b) [Subjects] の横の [+] 記号をクリックし、新しいサブジェクトを追加します。

c) [Create Contract Subject] ダイアログボックスで、[Name] フィールドにサブジェクト名を入力します。（web）

d) （注） この手順では、契約のサブジェクトで前に作成されたフィルタを関連付けます。

[Filter Chain] 領域で、[Filters] の横の [+] 記号をクリックします。

e) ダイアログボックスで、ドロップダウンメニューから、フィルタ名（http）を選択し、[Update] をクリックします。

ステップ 4 [Create Contract Subject] ダイアログボックスで、[OK] をクリックします。

ステップ 5 この手順と同じステップに従って、rmi と sql 用の契約をさらに 2 つ作成します。rmi 契約の場合は rmi サブジェクトを選択し、sql の場合は sql サブジェクトを選択します。

GUI を使用したアプリケーション プロファイルの作成

手順の概要

1. メニュー バーで、[TENANTS] を選択します。[Navigation] ペインで、テナントを展開し、[Application Profiles] を右クリックし、[Create Application Profile] をクリックします。
2. [Create Application Profile] ダイアログボックスで、[Name] フィールドに、アプリケーション プロファイル名（OnlineStore）を追加します。

手順の詳細

ステップ 1 メニュー バーで、[TENANTS] を選択します。[Navigation] ペインで、テナントを展開し、[Application Profiles] を右クリックし、[Create Application Profile] をクリックします。

ステップ 2 [Create Application Profile] ダイアログボックスで、[Name] フィールドに、アプリケーション プロファイル名（OnlineStore）を追加します。

GUI を使用した EPG の作成

EPG が使用するポートは、VM マネージャ（VMM）ドメインまたは EPG に関連付けられた物理ドメインのいずれか 1 つに属している必要があります。

手順の概要

1. [EPGs] を展開します。[Create Application EPG] ダイアログボックスで、次の操作を実行します。
2. [Create Application Profile] ダイアログボックスで、EPG をさらに 2 つ作成します。3 つの EPG は、同じブリッジ ドメインおよびデータセンター内の db、app、および web である必要があります。

手順の詳細

ステップ 1 [EPGs] を展開します。[Create Application EPG] 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、EPG の名前（db）を追加します。
b) [Bridge Domain] フィールドで、ドロップダウン リストからブリッジ ドメイン（bd1）を選択します。
c) [Associate to VM Domain Profiles] チェックボックスをオンにします。[Next] をクリックします。

d) [Step 2 for Specify the VM Domains] 領域で、[Associate VM Domain Profiles] を展開し、ドロップダウン リストから目的の VMM ドメインを選択します。[Update] をクリックし、[OK] をクリックします。

ステップ 2 [Create Application Profile] ダイアログボックスで、EPG をさらに 2 つ作成します。3 つの EPG は、同じブリッジ ドメインおよびデータセンター内の db、app、および web である必要があります。

GUI を使用した契約の消費と提供

EPG 間のポリシー関係を作成するために、前に作成した契約を関連付けることができます。

提供するコントラクトと使用するコントラクトに名前を付けるときは、提供するコントラクトと使用するコントラクトの両方に同じ名前を付けてください。

手順の概要

1. APIC GUI ウィンドウをクリックして db EPG から app EPG にドラッグします。
2. [Name] フィールドで、ドロップダウン リストから、sql 契約を選択します。[OK] をクリックします。
3. APIC GUI 画面 をクリックして、app ePG から web EPG にドラッグします。
4. [Name] フィールドで、ドロップダウン リストから、rmi 契約を選択します。[OK] をクリックします。
5. web EPG のアイコンをクリックし、[Provided Contracts] 領域の [+] 記号をクリックします。
6. [Name] フィールドで、ドロップダウン リストから、web 契約を選択します。[OK] をクリックします。[Submit] をクリックします。
7. 確認するには、[Navigation] ペインで、[Application Profiles] 下の [OnlineStore] に移動してクリックします。
8. [Work] ペインで、[Operational] > [Contracts] を選択します。

手順の詳細

ステップ 1 （注） db、app、および web EPG は、アイコンで表示されます。
APIC GUI ウィンドウをクリックして db EPG から app EPG にドラッグします。
[Add Consumed Contract] ダイアログボックスが表示されます。

ステップ 2 [Name] フィールドで、ドロップダウン リストから、sql 契約を選択します。[OK] をクリックします。
この手順により、db EPG は sql 契約を提供でき、app EPG は sql 契約を消費することができます。

ステップ 3 APIC GUI 画面 をクリックして、app ePG から web EPG にドラッグします。
[Add Consumed Contract] ダイアログボックスが表示されます。

ステップ 4 [Name] フィールドで、ドロップダウン リストから、rmi 契約を選択します。[OK] をクリックします。

この手順により、app EPG は rmi 契約を提供でき、web EPG は rmi 契約を消費することができます。

ステップ 5 web EPG のアイコンをクリックし、[Provided Contracts] 領域の [+] 記号をクリックします。
[Add Provided Contract] ダイアログボックスが表示されます。

ステップ 6 [Name] フィールドで、ドロップダウン リストから、web 契約を選択します。[OK] をクリックします。
[Submit] をクリックします。
OnlineStore と呼ばれる 3 層アプリケーション プロファイルが作成されました。

ステップ 7 確認するには、[Navigation] ペインで、[Application Profiles] 下の [OnlineStore] に移動してクリックします。
[Work] ペインで、3 つの EPG app、db および web が表示されていることを確認できます。

ステップ 8 [Work] ペインで、[Operational] > [Contracts] を選択します。
消費/提供される順番で表示された EPG と契約を確認できます。

特定のポートへの EPG の静的な導入

このトピックでは、Cisco APIC を使用しているときに特定のポートに EPG を静的に導入する方法の典型的な例を示します。

GUI を使用した APIC の特定のポートへの EPG の導入

はじめる前に

EPG を導入するテナントがすでに作成されていること。

ステップ 1 メニュー バーで、[TENANTS] をクリックします。

ステップ 2 [with APIC] ペインで、*[Tenant_name]* > [Application Profiles] の順に適切に展開します。

ステップ 3 [Application Profiles] を右クリックし、[Create Application Profile] をクリックします。

ステップ 4 [Create Application Profile] 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、アプリケーション プロファイルの名前を入力します。

b) [EPGs] を展開します。

c) [Create Application EPG] ダイアログボックスで、[Name] フィールドに、EPG 名を入力します。

d) [Statically Link with Leaves/Paths] フィールドで、[Statically Link with Leaves/Paths] のチェックボックスをオンにします（これは、EPG を導入する必要があるポートを指定するために選択します）。[Next] をクリックします。

e) [Leaves/Paths] 領域で、[Paths] を展開します。
この例では、EPGをノードのポートに導入します。または、EPGをノードに導入することもできます。

f) [Path] ドロップダウン リストから、適切なノードおよびポートを選択します。

g) [Encap] フィールドに、導入先の VLAN を入力します。

h) [Deployment Immediacy] フィールドのドロップダウン リストで、希望する導入時間を選択します。
i) [Mode] フィールドで、適切なモードを選択します。
j) [OK] をクリックし、[Submit] をクリックします。

ステップ 5 [Navigation] ペインで、[Application Profiles] を展開して、新しいアプリケーション プロファイルを表示します。

ステップ 6 [Application EPGs] を展開して、新しい EPG を表示します。

ステップ 7 EPG を展開して [Static Bindings (Paths)] をクリックし、[Work] ペインで、確立されたスタティック バインディング パスの詳細を表示します。

REST API を使用した APIC の特定のポートへの EPG の導入

はじめる前に

EPG を導入するテナントが作成されていること。

特定のポート上に EPG を導入します。

例：

```
<fvTenant name="<tenant_name>" dn="uni/tn-test1" >
    <fvCtx name="<network_name>" pcEnfPref="enforced" knwMcastAct="permit"/>
    <fvBD name="<bridge_domain_name>" unkMcastAct="flood" >
        <fvRsCtx tnFvCtxName="<network_name>"/>
    </fvBD>
    <fvAp name="<application_profile>" >
        <fvAEPg name="<epg_name>" >
            <fvRsPathAtt tDn="topology/pod-1/paths-1017/pathep-[eth1/13]" mode="regular"
instrImedcy="immediate" encap="vlan-20"/>
        </fvAEPg>
    </fvAp>
</fvTenant>
```

CLI を使用した APIC の特定のポートへの EPG の導入

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 テナントを作成します。

例：

```
# tenant
admin@apic1:~> cd '/aci/tenants'
admin@apic1:tenants> mocreate 'test1'
admin@apic1:tenants> moconfig commit
```

ステップ 3 ブリッジ ドメインを作成します。

例：

```
# bridge-domain
admin@apic1:tenants> cd '/aci/tenants/test1/networking/bridge-domains'
admin@apic1:bridge-domains> mocreate 'bd1'
admin@apic1:bridge-domains> cd 'bd1'
admin@apic1:bd1> moset network 'ctx1'
admin@apic1:bd1> moconfig commit
```

ステップ 4 プライベート ネットワークを作成します。

例：

```
# private-network
admin@apic1:bd1> cd '/aci/tenants/test1/networking/private-networks'
admin@apic1:private-networks> mocreate 'ctx1'
admin@apic1:private-networks> moconfig commit
```

ステップ 5 アプリケーション プロファイルを作成します。

例：

```
# application-profile
admin@apic1:private-networks> cd '/aci/tenants/test1/application-profiles'
admin@apic1:application-profiles> mocreate 'AP1'
admin@apic1:application-profiles> moconfig commit
```

ステップ 6 アプリケーション EPG を作成します。

例：

```
# application-epg
admin@apic1:application-profiles> cd '/aci/tenants/test1/application-profiles/AP1/application-epgs'
admin@apic1:application-epgs> mocreate 'EPG1'
admin@apic1:application-epgs> moconfig commit
```

ステップ 7 EPG を特定のポートに関連付けます。

例：

```
# fv-rspathatt
admin@apic1:application-epgs> cd
'/aci/tenants/test1/application-profiles/AP1/application-epgs/EPG1/static-bindings-paths'
admin@apic1:static-bindings-paths> mocreate 'topology/pod-1/paths-1017/pathep-[eth1/13]'
admin@apic1:static-bindings-paths> cd '[topology--pod-1--paths-1017--pathep-[eth1--13]]'
admin@apic1:[topology--pod-1--paths-1017--pathep-[eth1--13]]> moset encap 'vlan-20'
admin@apic1:[topology--pod-1--paths-1017--pathep-[eth1--13]]> moset deployment-immediacy 'immediate'
admin@apic1:[topology--pod-1--paths-1017--pathep-[eth1--13]]> moconfig commit
```

特定のポートに EPG を導入するためのドメイン、接続エンティティ プロファイル、および VLAN の作成

このトピックでは、特定のポートに EPG を導入する場合に必須である物理ドメイン、接続エンティティ プロファイル（AEP）、および VLAN を作成する方法の典型的な例を示します。

（注） すべてのエンドポイント グループ（EPG）にドメインが必要です。また、インターフェイス ポリシー グループを接続エンティティ プロファイル（AEP）に関連付ける必要があり、AEP と EPG が同じドメインに存在する必要がある場合は、AEP をドメインに関連付ける必要があります。EPG とドメイン、およびインターフェイス ポリシー グループとドメインの関連付けに基づいて、EPG が使用するポートと VLAN が検証されます。以下のドメイン タイプが EPG に関連付けられます。

- アプリケーション EPG
- レイヤ 3 Outside 外部ネットワーク インスタンス EPG
- レイヤ 2 Outside 外部ネットワーク インスタンス EPG
- アウトオブバンドおよびインバンド アクセスの管理 EPG

GUI を使用した、EPG を特定のポートに導入するためのドメインおよび VLAN の作成

はじめる前に

- EPG を導入するテナントがすでに作成されていること。
- EPG は特定のポートに静的に導入されます。

ステップ 1 メニュー バーで、[FABRIC] > [Access Policies] をクリックします。

ステップ 2 [Navigation] ペインで、[Quick Start] をクリックします。

ステップ 3 [Work] ペインで、[Configure an interface, PC, and vPC] をクリックします。

ステップ 4 [Configure Interface, PC, and vPC] ダイアログボックスで、[+] アイコンをクリックしてスイッチを選択し、次の操作を実行します。

a) [Switches] ドロップダウン リストで、目的のスイッチのチェックボックスをオンにします。

b) [Switch Profile Name] フィールドに、スイッチ名が自動的に入力されます。

（注） 任意で、変更した名前を入力することができます。

c) スイッチ インターフェイスを設定するために [+] アイコンをクリックします。
d) [Interface Type] フィールドで、[Individual] オプション ボタンをクリックします。
e) [Interfaces] フィールドに、目的のインターフェイスの範囲を入力します。
f) [Interface Selector Name] フィールドに、インターフェイス名が自動的に入力されます。
（注） 任意で、変更した名前を入力することができます。
g) [Interface Policy Group] フィールドで、[Create One] オプション ボタンを選択します。
h) [Link Level Policy] ドロップダウン リストで、適切なリンク レベル ポリシーを選択します。
（注） 必要に応じて追加のポリシーを作成します。または、デフォルトのポリシー設定を使用できます。
i) [Attached Device Type] フィールドから、適切なデバイス タイプを選択します。
j) [Domain] フィールドで、[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] フィールドで、[Create One] オプション ボタンをクリックします。
m) [VLAN Range] フィールドに、目的の VLAN 範囲を入力します。[Save] をクリックし、[Save] をもう一度クリックします。
n) [Submit] をクリックします。

ステップ 5 メニュー バーで、[TENANTS] をクリックします。[Navigation] ペインで、*[Tenant_name]* > [Application Profiles] > [Domains (VMs and Bare-Metals)] > *[EPG_name]* の順に適切に展開し、次の操作を実行します。

a) [Domains (VMs and Bare-Metals)] を右クリックし、[Add Physical Domain Association] をクリックします。
b) [Add Physical Domain Association] ダイアログボックスで、[Physical Domain Profile] ドロップダウン リストから、適切なドメインを選択します。
c) [Deploy Immediacy] フィールドで、目的のオプション ボタンをクリックします。
d) [Resolution Immediacy] フィールドで、目的のオプション ボタンをクリックします。[Submit] をクリックします。
AEP は、ノード上の特定のポート、およびドメインに関連付けられます。物理ドメインは VLAN プールに関連付けられ、テナントはこの物理ドメインに関連付けられます。

スイッチ プロファイルとインターフェイス プロファイルが作成されます。インターフェイス プロファイルのポート ブロックにポリシー グループが作成されます。AEP が自動的に作成され、ポート ブロックおよびドメインに関連付けられます。ドメインはVLANプールに関連付けられ、テナントはドメインに関連付けられます。

REST API を使用した、EPG を特定のポートに導入するための AEP、ドメイン、および VLAN の作成

はじめる前に

- EPG を導入するテナントがすでに作成されていること。

- EPG は特定のポートに静的に導入されます。

ステップ 1 インターフェイスプロファイル、スイッチプロファイル、および接続エンティティプロファイル（AEP）を作成します。

例：

```
   <infraInfra>

      <infraNodeP  name="<switch_profile_name>" dn="uni/infra/nprof-<switch_profile_name>" >
           <infraLeafS  name="SwitchSeletor" descr="" type="range">
                <infraNodeBlk name="nodeBlk1" descr="" to_="1019" from_="1019"/>
           </infraLeafS>
          <infraRsAccPortP tDn="uni/infra/accportprof-<interface_profile_name>"/>
      </infraNodeP>

      <infraAccPortP name="<interface_profile_name>"
dn="uni/infra/accportprof-<interface_profile_name>" >
           <infraHPortS  name="portSelector"  type="range">
              <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-<port_group_name>" fexId="101"/>

                <infraPortBlk name="block2"  toPort="13" toCard="1" fromPort="11" fromCard="1"/>
          </infraHPortS>
     </infraAccPortP>

   <infraAccPortGrp  name="<port_group_name>" dn="uni/infra/funcprof/accportgrp-<port_group_name>"
 >
          <infraRsAttEntP tDn="uni/infra/attentp-<attach_entity_profile_name>"/>
          <infraRsHIfPol tnFabricHIfPolName="1GHifPol"/>
    </infraAccPortGrp>

    <infraAttEntityP  name="<attach_entity_profile_name>"
dn="uni/infra/attentp-<attach_entity_profile_name>" >
         <infraRsDomP tDn="uni/phys-<physical_domain_name>"/>
    </infraAttEntityP>

<infraInfra>
```

ステップ 2 ドメインを作成する。

例：

```
<physDomP  name="<physical_domain_name>" dn="uni/phys-<physical_domain_name>">
    <infraRsVlanNs tDn="uni/infra/vlanns-[<vlan_pool_name>]-static"/>
</physDomP>
```

ステップ 3 VLAN 範囲を作成します。

例：

```
<fvnsVlanInstP  name="<vlan_pool_name>" dn="uni/infra/vlanns-[<vlan_pool_name>]-static"
allocMode="static">
    <fvnsEncapBlk name="" descr="" to="vlan-25" from="vlan-10"/>
</fvnsVlanInstP>
```

ステップ 4 ドメインに EPG を関連付けます。

例：

```
<fvTenant  name="<tenant_name>" dn="uni/tn-" >
    <fvAEPg prio="unspecified" name="<epg_name>" matchT="AtleastOne"
dn="uni/tn-test1/ap-AP1/epg-<epg_name>" descr="">
        <fvRsDomAtt tDn="uni/phys-<physical_domain_name>" instrImedcy="immediate"
resImedcy="immediate"/>
```

```
    </fvAEPg>
</fvTenant>
```

CLI を使用した、EPG を特定のポートに導入するための AEP、ドメイン、および VLAN の作成

はじめる前に

- EPG を導入するテナントがすでに作成されていること。
- EPG は特定のポートに静的に導入されます。

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 インターフェイス プロファイルを作成します。

例：

```
# interface-profile
admin@apic1:~> cd '/aci/fabric/access-policies/interface-policies/profiles/interfaces'
admin@apic1:interfaces> mocreate 'InterfaceProfile1'
admin@apic1:interfaces> moconfig commit

# access-port-selector
admin@apic1:interfaces> cd
'/aci/fabric/access-policies/interface-policies/profiles/interfaces/InterfaceProfile1'
admin@apic1:InterfaceProfile1> mocreate 'portSelector' 'range'
admin@apic1:InterfaceProfile1> cd 'portSelector-range'
admin@apic1:portSelector-range> moset policy-group
'fabric/access-policies/interface-policies/policy-groups/interface/PortGroup'
admin@apic1:portSelector-range> moconfig commit

# access-port-block
admin@apic1:portSelector-range> cd
'/aci/fabric/access-policies/interface-policies/profiles/interfaces/InterfaceProfile1/portSelector-range'
admin@apic1:portSelector-range> mocreate 'block2'
admin@apic1:portSelector-range> cd 'block2'
admin@apic1:block2> moset from-port '11'
admin@apic1:block2> moset to-port '13'
admin@apic1:block2> moconfig commit

# access-port-policy-group
admin@apic1:block2> cd '/aci/fabric/access-policies/interface-policies/policy-groups/interface'
admin@apic1:interface> mocreate 'PortGroup'
admin@apic1:PortGroup> cd 'PortGroup'
admin@apic1:PortGroup> moset link-level-policy '1GHifPol'
admin@apic1:PortGroup> moset attached-entity-profile
'fabric/access-policies/global-policies/attachable-entity-profile/IntfAttEntityP'
admin@apic1:PortGroup> moconfig commit
```

ステップ 3 スイッチ プロファイルを作成します。

例：

```
# switch-profile
admin@apic1:PortGroup> cd '/aci/fabric/access-policies/switch-policies/profiles'
admin@apic1:profiles> mocreate 'SwitchProfile-1019'
admin@apic1:profiles> moconfig commit

# infra-rsaccportp
admin@apic1:profiles> cd
'/aci/fabric/access-policies/switch-policies/profiles/SwitchProfile-1019/associated-interface-selector-profiles'
admin@apic1:associated-interface-selector-profiles> mocreate
'fabric/access-policies/interface-policies/profiles/interfaces/InterfaceProfile1'
admin@apic1:associated-interface-selector-profiles> moconfig commit

# leaf-selector
admin@apic1:associated-interface-selector-profiles> cd
'/aci/fabric/access-policies/switch-policies/profiles/SwitchProfile-1019/switch-selectors'
admin@apic1:switch-selectors> mocreate 'SwitchSeletor' 'range'
admin@apic1:switch-selectors> moconfig commit

# node-block
admin@apic1:switch-selectors> cd
'/aci/fabric/access-policies/switch-policies/profiles/SwitchProfile-1019/switch-selectors/SwitchSeletor-range'
admin@apic1:SwitchSeletor-range> mocreate 'eeac466a56b66898'
admin@apic1:SwitchSeletor-range> cd 'eeac466a56b66898'
admin@apic1:eeac466a56b66898> moset from '1019'
admin@apic1:eeac466a56b66898> moset to '1019'
admin@apic1:eeac466a56b66898> moconfig commit
```

ステップ 4 接続エンティティ プロファイル（AEP）を作成します。

例：

```
# attachable-access-entity-profile
admin@apic1:~> cd '/aci/fabric/access-policies/global-policies/attachable-entity-profile'
admin@apic1:attachable-entity-profile> mocreate 'IntfAttEntityP'
admin@apic1:attachable-entity-profile> moconfig commit

# infra-rsdomp
admin@apic1:attachable-entity-profile> cd
'/aci/fabric/access-policies/global-policies/attachable-entity-profile/IntfAttEntityP/domains-associated-to-interfaces'
admin@apic1:domains-associated-to-interfaces> mocreate
'fabric/access-policies/physical-and-external-domains/physical-domains/domP'
admin@apic1:domains-associated-to-interfaces> moconfig commit
```

ステップ 5 ドメインを作成します。

例：

```
# physical-domain
admin@apic1:~> cd '/aci/fabric/access-policies/physical-and-external-domains/physical-domains'
admin@apic1:physical-domains> mocreate 'domP'
admin@apic1:physical-domains> cd 'domP'
admin@apic1:domP> moset vlan-pools 'fabric/access-policies/pools/vlan/vlanPool1-static-allocation'
admin@apic1:domP> moconfig commit
```

ステップ 6 VLAN プールを作成します。

例：

```
# vlan-pool
admin@apic1:~> cd '/aci/fabric/access-policies/pools/vlan'
admin@apic1:vlan> mocreate 'vlanPool1' 'static-allocation'
admin@apic1:vlan> moconfig commit

# fvns-encapblk
admin@apic1:vlan> cd '/aci/fabric/access-policies/pools/vlan/vlanPool1-static-allocation/encap-blocks'
```

```
admin@apic1:encap-blocks> mocreate 'vlan-10' 'vlan-25'
admin@apic1:encap-blocks> moconfig commit
```

ステップ 7 ドメインに EPG を関連付けます。

例：

```
admin@apic1:~> cd
'/aci/tenants/test1/application-profiles/AP1/application-epgs/EPG1/domains-vms-and-bare-metals'
admin@apic1:domains-vms-and-bare-metals> mocreate
'fabric/access-policies/physical-and-external-domains/physical-domains/domP'
admin@apic1:domains-vms-and-bare-metals> cd
'[fabric--access-policies--physical-and-external-domains--physical-domains--domP]'
admin@apic1:[fabric--access-policies--physical-and-external-domains--physical-domains--domP]> moset
 deployment-immediacy 'immediate'
admin@apic1:[fabric--access-policies--physical-and-external-domains--physical-domains--domP]> moset
 resolution-immediacy 'immediate'
admin@apic1:[fabric--access-policies--physical-and-external-domains--physical-domains--domP]> moset
 name 'domP'
admin@apic1:[fabric--access-policies--physical-and-external-domains--physical-domains--domP]>
moconfig commit
```