



EPG

この章は、次の内容で構成されています。

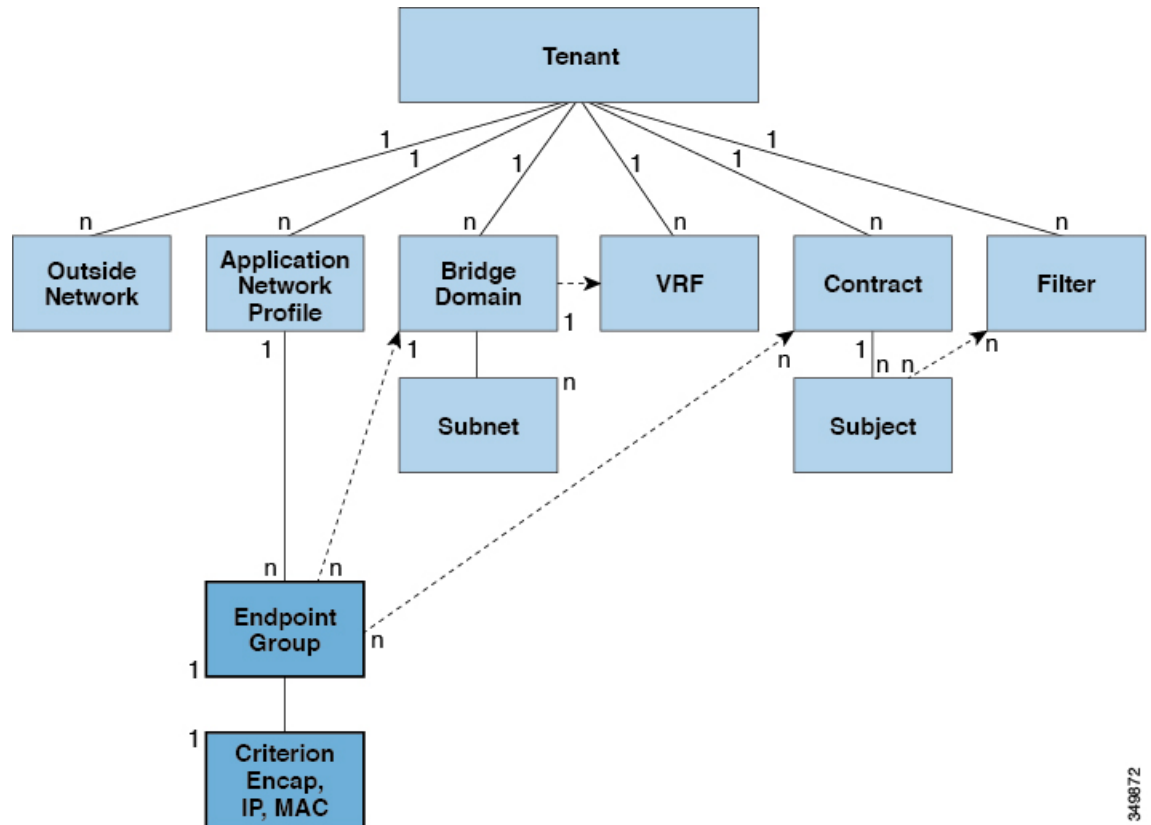
- [エンドポイントグループについて \(1 ページ\)](#)
- [特定のポートに EPG を導入する \(7 ページ\)](#)
- [特定のポートに EPG を導入するためのドメイン、接続エンティティプロファイル、および VLAN の作成 \(10 ページ\)](#)
- [添付されているエンティティプロファイルで複数のインターフェイスに EPG を導入する \(16 ページ\)](#)
- [EPG 内の分離 \(20 ページ\)](#)
- [Cisco ACI 仮想エッジの EPG 内分離の設定 \(34 ページ\)](#)

エンドポイントグループについて

エンドポイントグループ

エンドポイントグループ (EPG) は、ポリシーモデルの最も重要なオブジェクトです。次の図は、管理情報ツリー (MIT) 内のアプリケーション EPG の場所とテナント内の他のオブジェクトとの関係を示します。

図 1: エンドポイントグループ



349872

EPGは、エンドポイントの集合を含む名前付き論理エンティティである管理対象オブジェクトです。エンドポイントは、ネットワークに直接的または間接的に接続されるデバイスです。エンドポイントには、アドレス（ID）、ロケーション、属性（バージョンやパッチレベルなど）があり、物理または仮想にできます。エンドポイントのアドレスを知ることによって、他のすべてのIDの詳細にアクセスすることもできます。EPGは、物理および論理トポロジから完全に分離されます。エンドポイントの例には、インターネット上のサーバ、仮想マシン、ネットワーク接続ストレージ、またはクライアントが含まれます。EPG内のエンドポイントメンバシップは、ダイナミックまたはスタティックにできます。

ACI ファブリックには、次のタイプの EPG を含めることができます。

- アプリケーション エンドポイント グループ (fvAEPg)
- レイヤ 2 外部外側ネットワーク インスタンスのエンドポイント グループ (l2extInstP)
- レイヤ 3 外部外側ネットワーク インスタンスのエンドポイント グループ (l3extInstP)
- アウトオブバンド (mgmtOoB) またはインバンド (mgmtInB) アクセス用の管理エンドポイント グループ。

EPGには、セキュリティ、仮想マシンのモビリティ（VMM）、QoS、レイヤ4～レイヤ7サービスなどの共通のポリシー要件を持つエンドポイントが含まれます。エンドポイントは個別に設定および管理されるのではなく、EPG内に配置され、グループとして管理されます。

ポリシーはEPGに適用されます。個々のエンドポイントに適用されることは絶対にありません。EPGは、APICにおいて管理者により静的に設定されるか、vCenterまたはOpenStackなどの自動システムによって動的に設定されます。



- (注) EPGがスタティック バインディング パスを使用する場合、この EPG に関連付けられるカプセル化 VLAN はスタティック VLAN プールの一部である必要があります。IPv4/IPv6 デュアルスタック設定の場合、IP アドレスのプロパティは fvStCEp MO の fvStIp 子プロパティに含まれます。IPv4 および IPv6 アドレスをサポートする複数の fvStIp を 1 つの fvStCEp オブジェクト下に追加できます。ACI を、IPv4 のみのファームウェアから、IPv6 をサポートするバージョンのファームウェアにアップグレードすると、既存の IP プロパティが fvStIp MO にコピーされます。

EPG の設定内容にかかわらず、含まれるエンドポイントに EPG ポリシーが適用されます。

ファブリックへの WAN ルータ接続は、スタティック EPG を使用する設定の 1 つの例です。ファブリックへの WAN ルータ接続を設定するには、関連付けられている WAN サブネット内のエンドポイントを含む l3extInstP EPG を管理者が設定します。ファブリックは、エンドポイントの接続ライフサイクルが経過する間に、検出プロセスを通して EPG のエンドポイントについて学習します。エンドポイントを学習すると、ファブリックは、それに基づいて l3extInstP EPG ポリシーを適用します。たとえば、WAN 接続クライアントがアプリケーション (fvAEPg) EPG 内でサーバとの TCP セッションを開始すると、l3extInstP EPG は、fvAEPg EPG Web サーバとの通信が始まる前に、そのクライアントエンドポイントにポリシーを適用します。クライアントサーバ TCP セッションが終わり、クライアントとサーバの間の通信が終了すると、そのエンドポイントはもうファブリック内に存在しません。



- (注) リーフスイッチが EPG 下の *static binding (leaf switches)* 用に設定されている場合は、次の制限が適用されます。
- スタティック バインディングをスタティック パスで上書きすることはできません。
 - そのスイッチのインターフェイスをルーテッド外部ネットワーク (L3out) 設定に使用することはできません。
 - そのスイッチのインターフェイスに IP アドレスを割り当てることはできません。

VMware vCenter への仮想マシン管理接続は、ダイナミック EPG を使用する設定の 1 つの例です。ファブリックで仮想マシン管理ドメインが設定されると、vCenter は、必要に応じて仮想マシンエンドポイントを開始、移動、シャットダウンさせることのできる EPG の動的設定をトリガーします。

EPG シャットダウンでの ACI ポリシー設定

EPG がシャットダウン モードの場合、EPG に関連する ACI ポリシー設定はすべてのスイッチから削除されます。EPG はすべてのスイッチから削除されます。EPG が ACI データストアに存在している間は、非アクティブ モードになります。APIC GUI で、EPG をサービスから削除するチェックボックスをオンにすることができます。



(注) シャットダウン モードの EPG に接続されているホストは、EPG との間で送受信できません。

アクセス ポリシーによる VLAN から EPG への自動割り当て

テナント ネットワーク ポリシーがファブリックのアクセス ポリシーと別に設定される一方で、テナント ポリシーの基盤となるアクセス ポリシーが整わないとテナント ポリシーはアクティブ化されません。ファブリック アクセス外向きインターフェイスは、仮想マシン コントローラなどの外部デバイス、ハイパーバイザ、ホスト、ルータ、またはファブリック エクステンダ (FEX) と接続します。アクセス ポリシーにより、管理者はポート チャネルおよび仮想ポート チャネル、LLDP、CDP、LACP などのプロトコル、モニタリングや診断などの機能を設定することができます。

図 2: アクセス ポリシーとエンドポイントグループの関連付け



ポリシー モデルでは、vlan の Epg 緊密に結合されています。トラフィックが流れるようにするには、物理、VMM、L2out、L3out、またはファイバ チャネル ドメイン内に VLAN を持つ リーフ ポートに EPG を展開する必要があります。詳細については、[ネットワーク ドメイン](#)を参照してください。

ポリシー モデルでは、EPG に関連付けられているドメイン プロファイルには、VLAN インスタンス プロファイルが含まれています。ドメイン プロファイルには、両方の VLAN インスタンス プロファイル (VLAN プール) および `attacheable` アクセス エンティティ プロファイル (AEP) アプリケーション Epg に直接と関連付けられているが含まれています。AEP は、すべてのポートの [接続されている、および Vlan の割り当てのタスクを自動化するに] 関連付けられているアプリケーション Epg を展開します。大規模なデータセンター数千の Vlan の数百のプロビジョニング仮想マシンのアクティブなは簡単に、中に ACI ファブリックは VLAN プールから、VLAN Id を自動的に割り当てることができます。これは、膨大な従来データセンターで Vlan をトランキングと比較して、時間を節約できます。

VLAN の注意事項

EPG トラフィックがフローは、Vlan の設定には次のガイドラインを使用します。

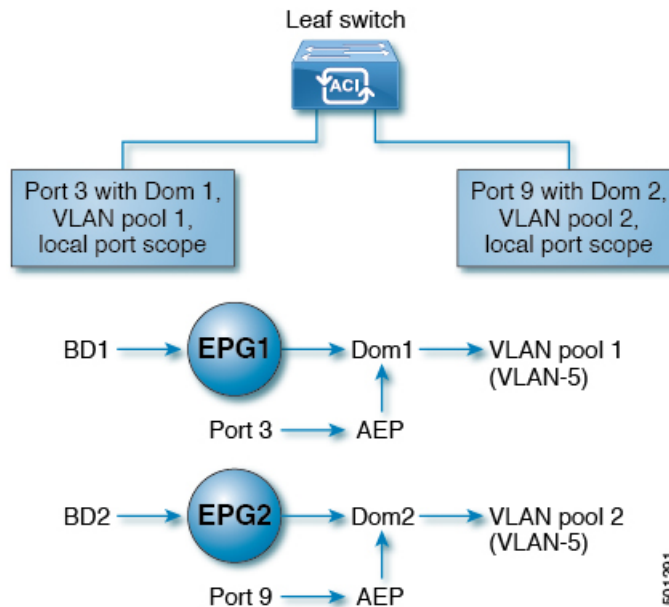
- 複数のドメインは、VLAN プールを共有できますが、1つのドメインは、1つの VLAN プールにのみ使用できます。

- 1つのリーフスイッチで同じ VLAN のカプセル化を複数の Epg を展開するを参照してください。 [ポート単位の VLAN \(5 ページ\)](#)。

ポート単位の VLAN

v1.1 リリースより前の ACI バージョンでは、特定の VLAN カプセル化はリーフスイッチ上の単一の EPG だけにマッピングされます。同じリーフスイッチ上に同じ VLAN カプセル化を持つ第 2 の EPG があると、ACI でエラーが発生します。

v1.1 リリース以降では、次の図と同様、ポート単位の VLAN 設定で、特定のリーフスイッチ (または FEX) 上に複数の EPG を同じ VLAN カプセル化で展開することができます。



単一のリーフスイッチ上で、同じカプセル化番号を使用する複数の EPG の展開を有効にするには、次の注意事項に従ってください。

- EPG は、さまざまなブリッジドメインに関連付けられている必要があります。
- EPG は、さまざまなポートに展開する必要があります。
- ポートと EPG の両方が、VLAN 番号が含まれている VLAN プールに関連付けられている同じドメインに関連付けられている必要があります。
- ポートは `portLocal VLAN` スコープで設定されている必要があります。

たとえば、上の図のポート 3 と 9 上に展開されている EPG のポート単位の VLAN で、両方が VLAN-5 を使用していれば、ポート 3 と EPG1 は Dom1 (プール 1) に、ポート 9 と EPG2 は Dom2 (プール 2) に関連付けられます。

ポート 3 からのトラフィックは EPG1 に関連付けられ、ポート 9 からのトラフィックは EPG2 に関連付けられます。

これは、外部レイヤ 3 外部接続用に設定されたポートには適用されません。

EPG に複数の物理ドメインがあり、VLAN プールが重複している場合は、EPG をポートに展開するために使用される AEP に複数のドメインを追加しないでください。これにより、トラフィック転送の問題が回避されます。

EPG に重複する VLAN プールを持つ物理ドメインが 1 つしかない場合、複数のドメインを単一の AEP に関連付けることができます。

入力および出力の両方向で個別の（ポート、VLAN）変換エントリの割り当てが可能なのは、vlanScope が portLocal に設定されているポートだけです。特定のポートで vlanScope が portGlobal（デフォルト）に設定されている場合には、EPG で使用される各 VLAN は、特定のリーフスイッチ上で一意のものである必要があります。



-
- (注) マルチスパンニングツリー (MST) で設定されているインターフェイス上では、ポート単位の VLAN はサポートされていません。このツリーでは、VLAN ID が 1 つのリーフスイッチ上で一意であること、そして VLAN の範囲がグローバルであることを必要とするからです。
-

同じリーフスイッチで EPG に使用されていた VLAN 番号の再利用

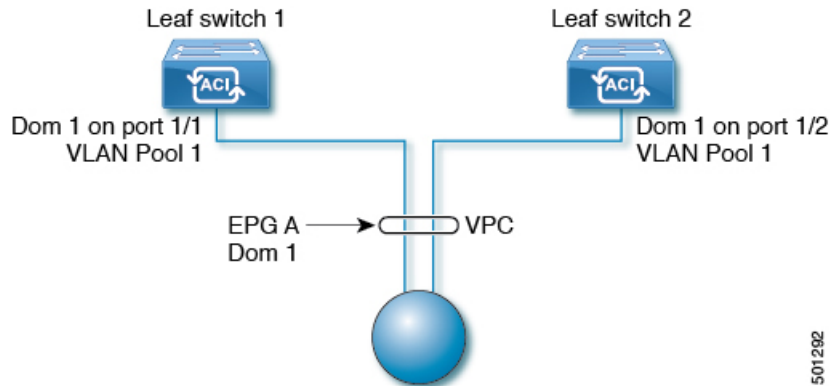
以前に、リーフスイッチのポートに展開されている EPG 用に VLAN を設定していて、同じ VLAN 番号を同じリーフスイッチの異なるポートの異なる EPG で再利用する場合には、中断なしでセットアップできるようにするため、次の例に示すようなプロセスに従ってください。

この例では、EPG は以前、9 ~ 100 の範囲の VLAN プールを含むドメインに関連付けられていたポートに展開されていました。ここで、9 ~ 20 からの VLAN カプセル化を使用する EPG を設定したいとします。

1. 異なるポート（たとえば、9 ~ 20 の範囲）で新しい VLAN プールを設定します。
2. ファイアウォールに接続されているリーフポートを含む新しい物理的なドメインを設定します。
3. ステップ 1 で設定した VLAN プールに物理的なドメインを関連付けます。
4. リーフポートの VLAN の範囲を portLocal として設定します。
5. 新しい EPG（この例ではファイアウォールが使用するもの）を、ステップ 2 で作成した物理ドメインに関連付けます。
6. リーフポートで EPG を展開します。

vPC に展開された EPG の VLAN ガイドライン

図 3: vPC の 2 つのレッグの VLAN



EPG を vPC に展開する場合は、vPC の 2 つのレッグのリーフ スイッチ ポートに割り当てられた同じドメイン（同じ VLAN プール）に関連付ける必要があります。

この図では、EPG A は、リーフ スイッチ 1 およびリーフ スイッチ 2 のポートに展開されている vPC に展開されています。2 本のリーフ スイッチ ポートおよび EPG は、すべて同じ VLAN プールが含まれている同じドメインに関連付けられています。

特定のポートに EPG を導入する

GUI を使用して特定のノードまたはポートへ EPG を導入する

始める前に

EPG を導入するテナントがすでに作成されていること。

特定のノードまたはノードの特定のポートで、EPG を作成することができます。

- ステップ 1 Cisco APIC にログインします。
- ステップ 2 [Tenants[> [tenant] を選択します。
- ステップ 3 左側のナビゲーション ウィンドウで、**tenant**、**Application Profiles**、および **application profile** を展開します。
- ステップ 4 **Application EPGs** を右クリックし、**Create Application EPG** を選択します。
- ステップ 5 **Create Application EPG STEP 1 > Identity** 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 の名前を入力します。
 - b) **Bridge Domain** ドロップダウンリストから、ブリッジ ドメインを選択します。
 - c) [Statically Link with Leaves/Paths] チェックボックスをオンにします。

このチェック ボックスを使用して、どのポートに EPG を導入するかを指定できます。

- d) [Next] をクリックします。
 e) [Path] ドロップダウンリストから、宛先 EPG への静的パスを選択します。

ステップ 6 **Create Application EPG STEP 2 > Leaves/Paths** ダイアログボックスで、**Physical Domain** ドロップダウンリストから物理ドメインを選択します。

ステップ 7 次のいずれかの手順を実行します。

オプション	説明
次のものに EPG を展開する場合、	次を実行します。
ノード	<ol style="list-style-type: none"> Leaves エリアを展開します。 [Node] ドロップダウンリストから、ノードを選択します。 Encap フィールドで、適切な VLAN を入力します。 (オプション)Deployment Immediacy ドロップダウンリストで、デフォルトの On Demand のままにするか、Immediate を選択します。 (オプション) [Mode] ドロップダウンリストで、デフォルトの [Trunk] のままにするか、別のモードを選択します。
ノード上のポート	<ol style="list-style-type: none"> Paths エリアを展開します。 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。 (オプション)Deployment Immediacy フィールドのドロップダウンリストで、デフォルトの On Demand のままにするか、Immediate を選択します。 (オプション) [Mode] ドロップダウンリストで、デフォルトの [Trunk] のままにするか、別のモードを選択します。 Port Encap フィールドに、導入するセカンダリ VLAN を入力します。 (オプション) Primary Encap フィールドで、展開するプライマリ VLAN を入力します。

ステップ 8 **Update** をクリックし、**Finish** をクリックします。

ステップ 9 左側のナビゲーション ウィンドウで、作成した EPG を展開します。

ステップ 10 次のいずれかの操作を実行します:

- ノードで EPG を作成した場合は、**Static Leafs** をクリックし、作業ウィンドウで、静的バインドパスの詳細を表示します。
- ノードのポートで EPG を作成した場合は、**Static Ports** をクリックし、作業ウィンドウで、静的バインドパスの詳細を表示します。

NX-OS スタイルの 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 VLAN ドメインを設定します。

例 :

```
apicl(config)# vlan-domain dom1
apicl(config-vlan)# vlan 10-100
```

ステップ 2 テナントを作成します。

例 :

```
apicl# configure
apicl(config)# tenant t1
```

ステップ 3 プライベート ネットワーク/VRF を作成します。

例 :

```
apicl(config-tenant)# vrf context ctx1
apicl(config-tenant-vrf)# exit
```

ステップ 4 ブリッジ ドメインを作成します。

例 :

```
apicl(config-tenant)# bridge-domain bd1
apicl(config-tenant-bd)# vrf member ctx1
apicl(config-tenant-bd)# exit
```

ステップ 5 アプリケーション プロファイルおよびアプリケーション EPG を作成します。

例 :

```
apicl(config-tenant)# application AP1
apicl(config-tenant-app)# epg EPG1
apicl(config-tenant-app-epg)# bridge-domain member bd1
apicl(config-tenant-app-epg)# exit
apicl(config-tenant-app)# exit
apicl(config-tenant)# exit
```

ステップ 6 EPG を特定のポートに関連付けます。

例 :

```
apicl(config)# leaf 1017
apicl(config-leaf)# interface ethernet 1/13
apicl(config-leaf-if)# vlan-domain member dom1
apicl(config-leaf-if)# switchport trunk allowed vlan 20 tenant t1 application AP1 epg EPG1
```

(注) 上の例に示した `vlan-domain` コマンドと `vlan-domain member` コマンドは、ポートに EPG を導入するための前提条件です。

REST API を使用した APIC の特定のポートへの EPG の導入

始める前に

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>
```

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

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。

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ます。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

APIC は、これらのドメインタイプのうち1つまたは複数に EPG が関連付けられているかどうかを確認します。EPG が関連付けられていない場合、システムは設定を受け入れますが、エラーが発生します。ドメインの関連付けが有効でない場合、導入された設定が正しく機能しない可能性があります。たとえば、VLAN のカプセル化を EPG で使用することが有効でない場合、導入された設定が正しく機能しない可能性があります。



- (注) スタティック バインディングを使用しない AEP との EPG アソシエーションは、一方のエンドポイントが同じ EPG の下でタグgingをサポートし、もう一方のエンドポイントが同じ EPG 内で VLAN タグgingをサポートしないような AEP の下では、EPG をトランクとして設定するシナリオで機能させることはできません。EPG で AEP を関連付ける際には、トランク、アクセス (タグ付き)、またはアクセス (タグなし) として設定できます。

GUI を使用して特定のポートに EPG を展開するためのドメインおよび VLAN の作成

始める前に

- 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、[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 (Navigation)] ペインで、[クイックスタート (Quick Start)] をクリックします。

ステップ 3 [作業 (Work)] ペインで、[インターフェイスの設定 (Configure Interfaces)] をクリックします。

ステップ 4 [インターフェイスの設定 (Configure Interfaces)] ダイアログで、以下のアクションを実行します。

- [ノードタイプ (Node Type)] で、[リーフ (Leaf)] をクリックします。
- [ポートタイプ (Port Type)] で、[アクセス (Access)] をクリックします。
- [インターフェイスタイプ (Interface Type)] で、目的のタイプを選択します。
- [インターフェイス集約タイプ (Interface Aggregation Type)] で、[個別 (Individual)] を選択します。
- [ノード (Node)] で、[ノードの選択 (Select Node)] をクリックし、目的のノードのボックスにチェックを入れて、[OK] をクリックします。複数のノードを選択できます。
- [すべてのスイッチのインターフェイス (Interfaces For All Switches)] で、目的のインターフェイスの範囲を入力します。
- [リーフアクセスポートポリシーグループ (Leaf Access Port Policy Group)] の場合は、[リーフアクセスポートポリシーグループの選択 (Select Leaf Access Port Policy Group)] をクリックします。

- h) [リーフアクセス ポート ポリシー グループの選択 (Select Leaf Access Port Policy Group)] ダイアログで、[リーフアクセス ポート ポリシー グループの作成 (Create Leaf Access Port Policy Group)] をクリックします。
- i) [リーフアクセス ポート ポリシー グループの作成 (Create Leaf Access Port Policy Group)] ダイアログの [リンク レベル ポリシー (Link Level Policy)] で、[リンク レベル ポリシーの選択 (Select Link Level Policy)] をクリックします。
- j) リンク レベル ポリシーを選択して [選択 (Select)] を選択するか、[リンク レベル ポリシーの作成 (Create Link Level Policy)] をクリックし、必要に応じてフィールドに入力して、[保存 (Save)] をクリックします。
- k) [保存 (Save)] をクリックします。

ステップ 5 以下のアクションを実行して、ドメインと VLAN プールを作成します。

- a) [ナビゲーション (Navigation)] ペインで、[物理ドメインと外部ドメイン (Physical and External Domains)] を展開します。
- b) [物理ドメイン (Physical Domains)] を右クリックし、適切な[物理ドメインの作成 (Create Physical Domain)] を選択します。
- c) [名前 (Name)] に、ドメインの名前を入力します。
- d) [VLAN プール (VLAN Pool)] で、[VLAN プールの作成 (Create VLAN Pool)] を選択し、必要に応じてフィールドに入力して、[送信 (Submit)] をクリックします。
- e) 目的に応じて、残りのフィールドに入力します。
- f) [送信 (Submit)] をクリックします。

ステップ 6 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 7 [作業 (Work)] ペインで、目的のテナントをダブルクリックします。

ステップ 8 [ナビゲーション (Navigation)] ペインで、テナント名 > [アプリケーション プロファイル (Application Profiles)] > プロファイル名 > [アプリケーション EPG (Application EPGs)] > EPG 名を展開し、以下の操作を実行します。

- a) [ドメイン (Domains) (VM またはベアメタル)] を右クリックし、[物理ドメインの関連付けの追加 (Add Physical Domain Association)] をクリックします。
- b) [物理ドメインの関連付けの追加 (Add Physical Domain Association)] ダイアログで、[物理ドメインのプロファイル (Physical Domain Profile)] ドロップダウン リストから、前に作成したドメインを選択します。
- c) [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。

NX-OS スタイルの 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

始める前に

- 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 VLAN ドメインを作成し、VLAN 範囲を割り当てます。

例 :

```
apicl(config)# vlan-domain domP
apicl(config-vlan)# vlan 10
apicl(config-vlan)# vlan 25
apicl(config-vlan)# vlan 50-60
apicl(config-vlan)# exit
```

ステップ 2 インターフェイスポリシーグループを作成し、そのポリシーグループにVLANドメインを割り当てます。

例 :

```
apicl(config)# template policy-group PortGroup
apicl(config-pol-grp-if)# vlan-domain member domP
```

ステップ 3 リーフ インターフェイス プロファイルを作成し、そのプロファイルにインターフェイス ポリシー グループを割り当てて、そのプロファイルを適用するインターフェイス ID を割り当てます。

例 :

```
apicl(config)# leaf-interface-profile InterfaceProfile1
apicl(config-leaf-if-profile)# leaf-interface-group range
apicl(config-leaf-if-group)# policy-group PortGroup
apicl(config-leaf-if-group)# interface ethernet 1/11-13
apicl(config-leaf-if-profile)# exit
```

ステップ 4 リーフ プロファイルを作成し、そのリーフ プロファイルにリーフ インターフェイス プロファイルを割り当てて、そのプロファイルを適用するリーフ ID を割り当てます。

例 :

```
apicl(config)# leaf-profile SwitchProfile-1019
apicl(config-leaf-profile)# leaf-interface-profile InterfaceProfile1
apicl(config-leaf-profile)# leaf-group range
apicl(config-leaf-group)# leaf 1019
apicl(config-leaf-group)#
```

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

始める前に

- 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>
```

重複する VLAN の検証

このグローバル機能は、単一の EPG での重複する VLAN プールの関連付けを防止します。APIC のいずれかの EPG で重複するプールが割り当てられている場合、この機能は有効にできません（有効にしようとするエラーが表示されます）。既存の重複プールが存在しない場合は、この機能を有効にできます。有効にすると、EPG にドメインを割り当てることを試行し、そのドメインに、EPG にすでに関連付けられている別のドメインと重複する VLAN プールが含まれていた場合、設定はブロックされます。

重複する VLAN プールが EPG の下に存在する場合、各スイッチによって EPG に割り当てられる FDVNID は非確定的になり、異なるスイッチが異なる VNID を割り当てる場合があります。これにより、vPC ドメイン内のリーフ間で EPM 同期が失敗する可能性が生じます（EPG 内のすべてのエンドポイントの接続が断続的になります）。また、ユーザーが EPG 間で STP を拡張している場合、FDVNID の不一致によりスイッチ間で BPDU がドロップされるため、ブリッジンググループが発生する可能性もあります。

GUI を使用した重複 VLAN の検証

この手順では、APIC GUI を使用して VLAN のオーバーラップの検証を設定する例を示します。

ステップ 1 メニューバーで、[システム (System)] > [システム設定 (System Settings)] を選択します。

ステップ 2 ナビゲーションペインで、[ファブリック ワイドの設定 (Fabric Wide Setting)] を選択します。

ステップ 3 作業ウィンドウで、[EPG VLAN 検証の適用 (Enforce EPG VLAN Validation)] を見つけてオンにします。

(注) 重複する VLAN プールがすでに存在し、このパラメータがオンになっている場合、システムはエラーを返します。この機能を選択する前に、EPG に重複しない VLAN プールを割り当てる必要があります。

このパラメータをオンにして、重複する VLAN プールを EPG に追加しようとする、エラーが返されます。

ステップ 4 [送信 (Submit)] をクリックします。

REST API を使用した重複 VLAN の検証

この手順では、REST API を使用して VLAN の重複の検証を設定する例を示します。

ステップ 1 XML API を使用して検証を有効にするには、この HTTP POST メッセージを送信します。

例 :

```
POST https://apic-ip-address/api/mo/infra/settings.xml
```

ステップ 2 次の XML 構造を POST メッセージの本文に含めます。

例 :

```
<?xml version="1.0" encoding="UTF-8"?>
<infraSetPol validateOverlappingVlans=yes />
```

(注) 重複する VLAN がすでに存在する場合、POST 中にエラーメッセージが表示され、重複する VLAN を持つ対応する EPG が示されます。

```
<?xml version="1.0" encoding="UTF-8"?><imdata totalCount="1">
<error code="100" text="Validation failed: Vlan ranges for an EPg cannot overlap
Dn0=uni/tn-ag/ap-app/epg-el,
"/></imdata>
```

添付されているエンティティプロファイルで複数のインターフェイスに EPG を導入する

AEP または インターフェイス ポリシー グループ を使用した アプリケーション EPG の複数のポートへの導入

APIC の拡張 GUI と REST API を使用して、接続エンティティプロファイルをアプリケーション EPG に直接関連付けることができます。これにより、単一の構成の接続エンティティプロファイルに関連付けられたすべてのポートに、関連付けられたアプリケーション EPG を導入します。

APIC REST API または NX-OS スタイルの CLI を使用し、インターフェイス ポリシー グループ を介して複数のポートにアプリケーション EPG を導入できます。

APIC GUI を使用した AEP による複数のインターフェイスへの EPG の導入

短時間でアプリケーションを接続エンティティプロファイルに関連付けて、その接続エンティティプロファイルに関連付けられたすべてのポートに EPG を迅速に導入することができます。

始める前に

- ターゲット アプリケーション EPG が作成されている。
- AEP での EPG 導入に使用する VLAN の範囲が含まれている VLAN プールが作成されている。
- 物理ドメインが作成され、VLAN プールと AEP にリンクされている。
- ターゲットの接続エンティティプロファイルが作成され、アプリケーション EPG を導入するポートに関連付けられている。

ステップ 1 ターゲットの接続エンティティプロファイルに移動します。

- 使用する接続エンティティプロファイルのページを開きます。[ファブリック (Fabric)] > [アクセスポリシー (Access Policies)] > [ポリシー (Policies)] > [グローバル (Global)] > [アタッチ可能なアクセスエンティティプロファイル (Attachable Access Entity Profiles)] に移動します。
- ターゲットの接続エンティティプロファイルをクリックして、[Attachable Access Entity Profile] ウィンドウを開きます。

ステップ 2 [Show Usage] ボタンをクリックして、この接続エンティティプロファイルに関連付けられたリーフスイッチとインターフェイスを表示します。

この接続エンティティプロファイルに関連付けられたアプリケーション EPG が、この接続エンティティプロファイルに関連付けられたすべてのスイッチ上のすべてのポートに導入されます。

ステップ 3 [Application EPGs] テーブルを使用して、この接続エンティティプロファイルにターゲットアプリケーション EPG を関連付けます。アプリケーション EPG エントリを追加するには、[+] をクリックします。各エントリに次のフィールドがあります。

フィールド	アクション
Application EPG	ドロップダウンを使用して、関連付けられたテナント、アプリケーションプロファイル、およびターゲットアプリケーション EPG を選択します。
Encap	ターゲットアプリケーション EPG の通信に使用される VLAN の名前を入力します。
Primary Encap	アプリケーション EPG にプライマリ VLAN が必要な場合は、プライマリ VLAN の名前を入力します。
モード	ドロップダウンを使用して、データを送信するモードを指定します。

フィールド	アクション
	<ul style="list-style-type: none"> • [Trunk] : ホストからのトラフィックに VLAN ID がタグ付けされている場合に選択します。 • [Access] : ホストからのトラフィックに 802.1p タグがタグ付けされている場合に選択します。 • [Access Untagged] : ホストからのトラフィックがタグ付けされていない場合に選択します。

ステップ 4 [Submit] をクリックします。

この接続エンティティ プロファイルに関連付けられたアプリケーション EPG が、この接続エンティティ プロファイルに関連付けられたすべてのスイッチ上のすべてのポートに導入されます。

NX-OS スタイルの CLI を使用したインターフェイス ポリシー グループによる複数のインターフェイスへの EPG の導入

NX-OS CLI では、接続エンティティ プロファイルを EPG に関連付けることによる迅速な導入が明示的に定義されていません。代わりにインターフェイス ポリシー グループが定義されてドメインが割り当てられます。このポリシー グループは、VLAN に関連付けられたすべてのポートに適用され、その VLAN を介して導入されるアプリケーション EPG を含むように設定されます。

始める前に

- ターゲット アプリケーション EPG が作成されている。
- AEP での EPG 導入に使用する VLAN の範囲が含まれている VLAN プールが作成されている。
- 物理ドメインが作成され、VLAN プールと AEP にリンクされている。
- ターゲットの接続エンティティ プロファイルが作成され、アプリケーション EPG を導入するポートに関連付けられている。

ステップ 1 ターゲット EPG をインターフェイス ポリシー グループに関連付けます。

このコマンドシーケンスの例では、VLAN ドメイン **domain1** と VLAN **1261** に関連付けられたインターフェイス ポリシー グループ **pg3** を指定します。このポリシー グループに関連付けられたすべてのインターフェイスに、アプリケーション EPG **epg47** が導入されます。

例 :

```
apic1# configure terminal
apic1(config)# template policy-group pg3
apic1(config-pol-grp-if)# vlan-domain member domain1
```

```
apic1(config-pol-grp-if)# switchport trunk allowed vlan 1261 tenant tn10 application pod1-AP
epg epg47
```

ステップ 2 ターゲット ポートで、アプリケーション EPG に関連付けられたインターフェイス ポリシー グループのポリシーが導入されたことを確認します。

次の **show** コマンドシーケンスの出力例は、ポリシー グループ **pg3** がリーフ スイッチ **1017** 上のイーサネット ポート **1/20** に導入されていることを示しています。

例 :

```
apic1# show run leaf 1017 int eth 1/20
# Command: show running-config leaf 1017 int eth 1/20
# Time: Mon Jun 27 22:12:10 2016
leaf 1017
  interface ethernet 1/20
    policy-group pg3
  exit
exit
ifav28-ifc1#
```

REST API を使用した AEP による複数のインターフェイスへの EPG の導入

AEP のインターフェイスセレクタを使用して、AEPg の複数のパスを設定できます。以下を選択できます。

1. ノードまたはノード グループ
2. インターフェイスまたはインターフェイス グループ
インターフェイスは、インターフェイス ポリシー グループ (および `infra:AttEntityP`) を使用します。
3. `infra:AttEntityP` を AEPg に関連付けることで、使用する VLAN を指定する。
`infra:AttEntityP` は、VLAN が異なる複数の AEPg に関連付けることができます。

3 のように `infra:AttEntityP` を AEPg に関連付けた場合、1 で選択したノード上の 2 のインターフェイスに、3 で指定した VLAN を使用して AEPg が導入されます。

この例では、AEPg `uni/tn-Coke/ap-AP/epg-EPG1` が、ノード 101 および 102 のインターフェイス 1/10、1/11、および 1/12 に `vlan-102` で導入されます。

始める前に

- ターゲット アプリケーション EPG (AEPg) を作成する。
- 接続エンティティ プロファイル (AEP) による EPG 導入に使用する VLAN の範囲が含まれている VLAN プールを作成する。
- 物理ドメインを作成して VLAN プールおよび AEP にリンクさせる。

選択したノードとインターフェイスに AEPg を導入するには、次の例のような XML を POST 送信します。

例：

```
<infraInfra dn="uni/infra">
  <infraNodeP name="NodeProfile">
    <infraLeafS name="NodeSelector" type="range">
      <infraNodeBlk name="NodeBlok" from_"101" to_"102"/>
      <infraRsAccPortP tDn="uni/infra/accportprof-InterfaceProfile"/>
    </infraLeafS>
  </infraNodeP>

  <infraAccPortP name="InterfaceProfile">
    <infraHPortS name="InterfaceSelector" type="range">
      <infraPortBlk name=" InterfaceBlock" fromCard="1" toCard="1" fromPort="10" toPort="12"/>
      <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-PortGrp" />
    </infraHPortS>
  </infraAccPortP>

  <infraFuncP>
    <infraAccPortGrp name="PortGrp">
      <infraRsAttEntP tDn="uni/infra/attentp-AttEntityProfile"/>
    </infraAccPortGrp>
  </infraFuncP>

  <infraAttEntityP name="AttEntityProfile" >
    <infraGeneric name="default" >
      <infraRsFuncToEpg tDn="uni/tn-Coke/ap-AP/epg-EPG1" encap="vlan-102"/>
    </infraGeneric>
  </infraAttEntityP>
</infraInfra>
```

EPG 内の分離

EPG 内エンドポイント分離

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

EPG の分離は、すべての Cisco Application Centric Infrastructure (ACI) ネットワーク ドメインに適用されるか、どれにも適用されないかの、どちらかになります。Cisco ACI ファブリックは接続エンドポイントに直接分離を実装しますが、ファブリックに接続されているスイッチはプライマリ VLAN (PVLAN) タグに従って分離規則を認識します。



- (注) EPG 内エンドポイント分離を適用して EPG を設定した場合は、次の制限が適用されます。
- 分離を適用した EPG 全体のすべてのレイヤ 2 エンドポイント通信がブリッジドメイン内にドロップされます。
 - 分離を適用した EPG 全体のすべてのレイヤ 3 エンドポイント通信が同じサブネット内にドロップされます。
 - トラフィックが、分離が適用されている EPG から分離が適用されていない EPG に流れている場合、QoS CoS の優先順位設定の保持はサポートされません。

BPDU は、EPG 内分離が有効になっている EPG を介して転送されません。したがって、Cisco ACI 上の独立した EPG にマッピングされている VLAN でスパンニング ツリーを実行する外部レイヤ 2 ネットワークを接続すると、Cisco ACI は外部ネットワークのスパンニング ツリーがレイヤ 2 ループを検出できなくなる可能性があります。この問題を回避するには、これらの VLAN 内の Cisco ACI と外部ネットワーク間に単一の論理リンクのみを設定します。

ベアメタルサーバの EPG 内分離

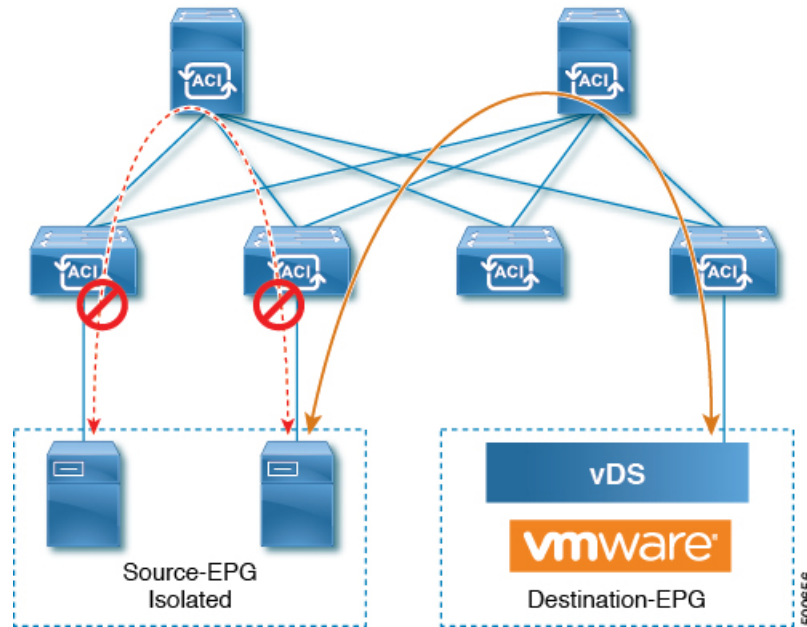
ベアメタルサーバの EPG 内分離

EPG 内エンドポイント分離のポリシーは、ベアメタルサーバなどの直接接続されているエンドポイントに適用できます。

次のような使用例があります。

- バックアップクライアントは、バックアップサービスにアクセスするための通信要件は同じですが、相互に通信する必要はありません。
- ロードバランサの背後にあるサーバの通信要件は同じですが、それらのサーバを相互に分離すると、不正アクセスや感染のあるサーバに対して保護されます。

図 4: ベア メタル サーバの EPG 内分離



ベア メタルの EPG 分離はリーフ スイッチで適用されます。ベア メタル サーバは VLAN カプセル化を使用します。ユニキャスト、マルチキャスト、およびブロードキャストのすべてのトラフィックが、分離が適用された EPG 内でドロップ（拒否）されます。ACI ブリッジ ドメインには、分離された EPG と通常の EPG を混在させることができます。分離された EPG それぞれには、VLAN 間トラフィックを拒否する複数の VLAN を指定できます。

GUI を使用したベア メタル サーバの EPG 内分離の設定

EPG が使用するポートは、リーフ スイッチにベア メタル サーバを直接接続するために使用する物理ドメイン内のベア メタル サーバと関連付ける必要があります。

手順の概要

1. テナントで、[Application Profile] を右クリックし、[Create Application EPG] ダイアログボックスを開いて次の操作を実行します。
2. [Leaves/Paths] ダイアログボックスで、次の操作を実行します。

手順の詳細

ステップ 1 テナントで、[Application Profile] を右クリックし、[Create Application EPG] ダイアログボックスを開いて次の操作を実行します。

- a) [Name] フィールドに、EPG の名前 (intra_EPG-deny) を追加します。
- b) [Intra EPG Isolation] で、[Enforced] をクリックします。
- c) [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。
- d) [Statically Link with Leaves/Paths] チェックボックスをオンにします。

e) [Next] をクリックします。

ステップ 2 [Leaves/Paths] ダイアログボックスで、次の操作を実行します。

a) [Path] セクションで、ドロップダウンリストからトランクモードでのパス (Node-107/eth1/16) を選択します。

セカンダリ VLAN の [Port Encap] (vlan-102) を指定します。

(注) ベアメタルサーバがリーフスイッチに直接接続されている場合、Port Encap のセカンダリ VLAN のみが指定されます。

プライマリ VLAN の [Primary Encap] (vlan-103) を指定します。

b) [Update] をクリックします。

c) [Finish] をクリックします。

NX-OS スタイルの CLI を使用したベアメタルサーバの EPG 内分離の設定

手順の概要

1. CLI で、EPG 内分離 EPG を作成します。
2. 設定を確認します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>CLI で、EPG 内分離 EPG を作成します。</p> <p>例：</p> <p>以下に、VMM ケースを示します。</p> <pre> ifav19-ifc1(config)# tenant Test_Isolation ifav19-ifc1(config-tenant)# application PVLAN ifav19-ifc1(config-tenant-app)# epg EPG1 ifav19-ifc1(config-tenant-app-epg)# show running-config # Command: show running-config tenant Test_Isolation application PVLAN epg EPG1 tenant Test_Isolation application PVLAN epg EPG1 bridge-domain member BD1 contract consumer bare-metal contract consumer default contract provider Isolate_EPG isolation enforce <---- This enables EPG isolation mode. exit exit ifav19-ifc1(config)# leaf ifav19-leaf3 ifav19-ifc1(config-leaf)# interface ethernet 1/16 ifav19-ifc1(config-leaf-if)# show running-config </pre>	

	コマンドまたはアクション	目的
	<pre> ifav19-ifc1(config-leaf-if)# switchport trunk native vlan 101 tenant Test_Isolation application PVLAN epg StaticEPG primary-vlan 100 exit </pre>	
ステップ 2	<p>設定を確認します。</p> <p>例 :</p> <pre> show epg StaticEPG detail Application EPg Data: Tenant : Test_Isolation Application : PVLAN AEPg : StaticEPG BD : BD1 uSeg EPG : no Intra EPG Isolation : enforced Vlan Domains : phys Consumed Contracts : bare-metal Provided Contracts : default,Isolate_EPG Denied Contracts : Qos Class : unspecified Tag List : VMM Domains: Domain Type Deployment Immediacy Resolution Immediacy State Encap Primary Encap ----- ----- DVS1 VMware On Demand immediate formed auto auto Static Leaves: Node Encap Deployment Immediacy Mode Modification Time ----- ----- Static Paths: Node Interface Encap Modification Time ----- ----- 1018 eth101/1/1 vlan-100 2016-02-11T18:39:02.337-08:00 1019 eth1/16 vlan-101 2016-02-11T18:39:02.337-08:00 Static Endpoints: Node Interface Encap End Point MAC End Point IP Address Modification Time ----- ----- </pre>	

	コマンドまたはアクション	目的
	----- ----- -----	

REST API を使用したベアメタルサーバのイントラ EPG 分離の設定

始める前に

EPG が使用するポートは、物理ドメイン内のベアメタルサーバインターフェイスに関連付けられている必要があります。

手順の概要

1. XML API を使用してアプリケーションを展開するには、次の HTTP POST メッセージを送信します。
2. 次の XML 構造を POST メッセージの本文に含めます。

手順の詳細

ステップ 1 XML API を使用してアプリケーションを展開するには、次の HTTP POST メッセージを送信します。

例：

```
POST https://apic-ip-address/api/mo/uni/tn-ExampleCorp.xml
```

ステップ 2 次の XML 構造を POST メッセージの本文に含めます。

例：

```
<fvTenant name="Tenant_BareMetal" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <fvRsBd tnFvBDName="bd" />
      <fvRsDomAtt tDn="uni/phys-Dom1" />
      <!-- PATH ASSOCIATION -->
      <fvRsPathAtt tDn="topology/pod-1/paths-1017/pathep-[eth1/2]" encap="vlan-51"
primaryEncap="vlan-100" instrImedcy='immediate' />
    </fvAEPg>
  </fvAp>
</fvTenant>
```

VMware vDS の EPG 内分離

VMware VDS または Microsoft Hyper-V 仮想スイッチの EPG 分離

EPG 内分離は、同じベース EPG またはマイクロセグメント (uSeg) EPG にある物理または仮想エンドポイントデバイスが相互に通信しないようにするオプションです。デフォルトでは、同じ EPG に含まれるエンドポイントデバイスは互いに通信することができます。しかし、EPG 内のエンドポイント デバイスの別のエンドポイント デバイスからの完全な分離が望ましい状況が存在します。たとえば、同じ EPG 内のエンドポイント VM が複数のテナントに属している場合、またはウイルスが広がるのを防ぐために、EPG 内の分離を実行することができます。

Cisco Application Centric Infrastructure (ACI) 仮想マシンマネージャ (VMM) ドメインは、EPG 内分離が有効になっている EPG ごとに、VMware VDS または Microsoft Hyper-V 仮想スイッチで分離 PVLAN ポート グループを作成します。ファブリック管理者がプライマリ カプセル化を指定するか、または EPG と VMM ドメインの関連付け時にファブリックが動的にプライマリ カプセル化を指定します。ファブリック管理者が VLAN pri 値と VLAN-sec 値を静的に選択すると、VMM ドメインによって VLAN-pri と VLAN-sec がドメインプール内のスタティックブロックの一部であることが検証されます。

プライマリ カプセル化は、EPG VLAN ごとに定義されます。EPG 内分離にプライマリ カプセル化を使用するには、次のいずれかの方法で展開する必要があります。

- プライマリ VLAN とセカンダリ VLAN で定義されたポートを異なるスイッチに分離します。EPG VLAN はスイッチごとに作成されます。ポートカプセル化があり、EPG のスイッチ上のスタティック ポートのみの場合、プライマリ カプセル化は関連付けられません。
- ポートカプセル化のみを使用するスタティックポートには別のカプセル化を使用します。これにより、プライマリカプセル化が関連付けられていない2番目の EPG VLAN が作成されます。

次の例では、プライマリ VLAN-1103 を持つ 2 つのインターフェイス (Eth1/1、Eth1/3) の出力トラフィックを考慮します。Eth1/1 ポートカプセル化が VLAN-1132 に (VLAN-1130 から) 変更されたため、Eth1/3 とセカンダリ VLAN を共有しません。

Port encap with VLAN-1130 on Eth1/1

```
Eth1/1: Port Encap only VLAN-1130
Eth1/6: Primary VLAN-1103 and Secondary VLAN-1130
```

```
fab2-leaf3# show vlan id 53 ext
```

VLAN Name	Encap	Ports
53 JT:jt-ap:EPG1-1	vlan-1130	Eth1/1, Eth1/3

```
module-1# show sys int eltmc info vlan access_encap_vlan 1130
```

```

vlan_id:          53  :::      isEpg:          1
bd_vlan_id:      52  :::      hwEpgId:       11278
srcpolicyincom:  0   :::      data_mode:     0
accencaptype:    0   :::      fabencaptype:  2
accencapval:     1130 :::      fabencapval:   12192
sclass:          49154 :::      sglabel:       12
sclassprio:      1   :::      floodmetptr:   13
maclearnen:      1   :::      iplearnen:     1
```

```

sclasslrnen:          1  :::  bypselfwdchk:          0
qosusetc:             0  :::  qosuseexp:            0
isolated:             1  :::  primary_encap:      1103
proxy_arp:            0  :::  qinq_core:            0
ivxlan_dl:            0  :::  dtag_mode:            0
is_service_epg:       0

```

Port encap changed to VLAN-1132 on Eth1/1

fab2-leaf3# show vlan id 62 ext

VLAN Name	Encap	Ports
62 JT:jt-ap:EPG1-1	vlan-1132	Eth1/1

module-1# show sys int eltmc info vlan access_encap_vlan 1132

```

[SDK Info]:
  vlan_id:             62  :::  isEpg:                1
  bd_vlan_id:          52  :::  hwEpgId:              11289
  srcpolicyincom:      0   :::  data_mode:            0
  accencaptype:        0   :::  fabencaptype:         2
  accencapval:        1132  :::  fabencapval:          11224
  sclass:              49154  :::  sglabel:              12
  sclassprio:          1   :::  floodmetptr:          13
  maclearnen:          1   :::  iplernen:             1
  sclasslrnen:         1   :::  bypselfwdchk:         0
  qosusetc:            0   :::  qosuseexp:            0
  isolated:            1   :::  primary_encap:      0
  proxy_arp:           0   :::  qinq_core:            0
  ivxlan_dl:           0   :::  dtag_mode:            0
  is_service_epg:      0

```

fab2-leaf3# show vlan id 53 ext

VLAN Name	Encap	Ports
53 JT:jt-ap:EPG1-1	vlan-1130	Eth1/3

module-1# show sys int eltmc info vlan access_encap_vlan 1130

```

[SDK Info]:
  vlan_id:             53  :::  isEpg:                1
  bd_vlan_id:          52  :::  hwEpgId:              11278
  srcpolicyincom:      0   :::  data_mode:            0
  accencaptype:        0   :::  fabencaptype:         2
  accencapval:        1130  :::  fabencapval:          12192
  sclass:              49154  :::  sglabel:              12
  sclassprio:          1   :::  floodmetptr:          13
  maclearnen:          1   :::  iplernen:             1
  sclasslrnen:         1   :::  bypselfwdchk:         0
  qosusetc:            0   :::  qosuseexp:            0
  isolated:            1   :::  primary_encap:      1103
  proxy_arp:           0   :::  qinq_core:            0
  ivxlan_dl:           0   :::  dtag_mode:            0

```



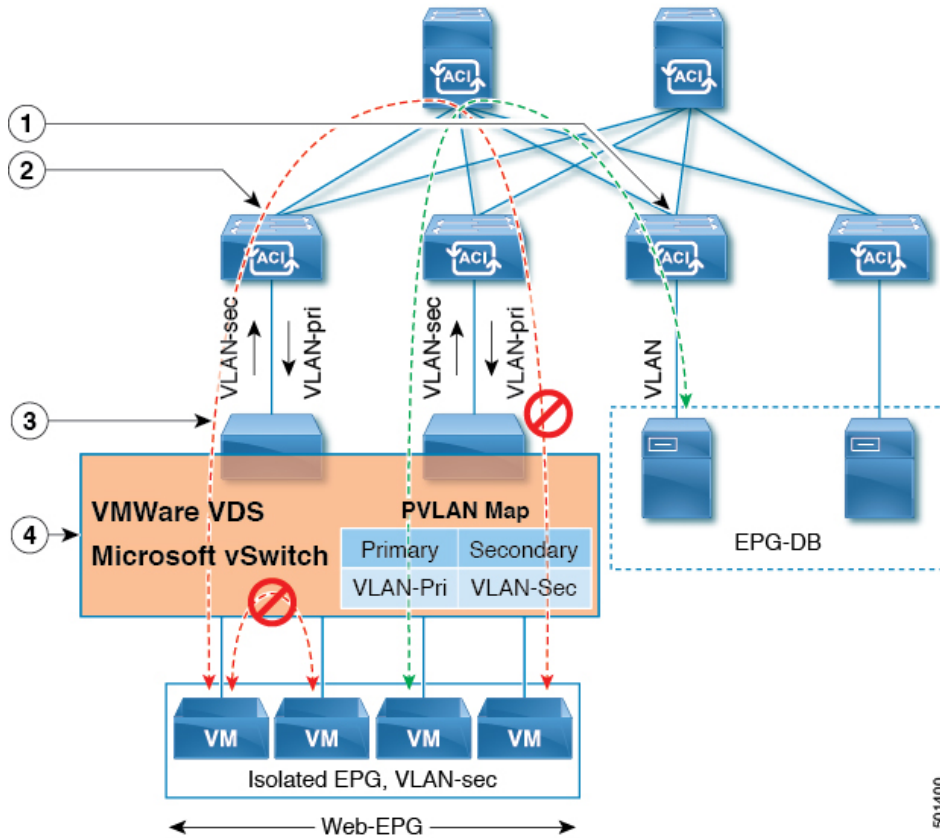
- (注)
- イントラ EPG 分離が強制されない場合、設定で指定されていても VLAN-pri 値は無視されます。
 - EDM UCSM 統合を使用した VMware 分散仮想スイッチ (DVS) ドメインが失敗することがあります。ドメインに接続されているエンドポイントグループ (EPG) で EPG 内分離を設定し、プライベート VLAN をサポートしない UCSM Mini 6324 を使用すると、ドメインに障害が発生します。

BPDU は、EPG 内分離が有効になっている EPG を介して転送されません。したがって、Cisco ACI 上の独立した EPG にマッピングされている VLAN でスパニング ツリーを実行する外部レイヤ 2 ネットワークを接続すると、Cisco ACI は外部ネットワークのスパニング ツリーがレイヤ 2 ループを検出できなくなる可能性があります。この問題を回避するには、これらの VLAN 内の Cisco ACI と外部ネットワーク間に単一の論理リンクのみを設定します。

VMware VDS または Microsoft Hyper-V 仮想スイッチの VLAN-pri/VLAN-sec ペアは、EPG とドメインの関連付け中に VMM ドメインごとに選択されます。EPG 内隔離 EPG に作成されたポートグループは `PVLAN` に設定されたタイプでタグ付けされた VLAN-sec を使用します。VMware VDS または Microsoft Hyper-V 仮想スイッチおよびファブリックは、VLAN-pri/VLAN-sec カプセル化をスワップします。

- Cisco ACI ファブリックから VMware VDS または Microsoft Hyper-V 仮想スイッチへの通信は VLAN-pri を使用します。
- VMware VDS または Microsoft Hyper-V 仮想スイッチから Cisco ACI ファブリックへの通信は VLAN-sec を使用します。

図 5: VMware VDS または Microsoft Hyper-V 仮想スイッチの EPG 分離



501400

この図に関する次の詳細に注意してください。

1. EPG-DB は Cisco ACI リーフスイッチに VLAN トラフィックを送信します。Cisco ACI 出力リーフスイッチは、プライマリ VLAN (PVLAN) タグを使用してトラフィックをカプセル化し、Web-EPG エンドポイントに転送します。
2. VMware VDS または Microsoft Hyper-V 仮想スイッチは、VLAN-sec を使用して Cisco ACI リーフスイッチにトラフィックを送信します。Web-EPG 内のすべての VLAN 内トラフィックに対して分離が適用されるため、Cisco ACI リーフスイッチはすべての EPG 内トラフィックをドロップします。
3. Cisco ACI リーフスイッチへの VMware VDS または Microsoft Hyper-V 仮想スイッチ VLAN-sec アップリンクが分離トランクモードです。Cisco ACI リーフスイッチは、VMware VDS または Microsoft Hyper-V 仮想スイッチへのダウンリンクトラフィックに VLAN-pri を使用します。
4. PVLAN マップは、VMware VDS または Microsoft Hyper-V 仮想スイッチおよび Cisco ACI リーフスイッチで設定されます。Web-EPG からの VM トラフィックは VLAN-sec 内でカプセル化されます。VMware VDS または Microsoft Hyper-V 仮想スイッチは PVLAN タグに従ってローカルの Web 内 EPG VM トラフィックを拒否します。すべての内部 ESXi ホストまたは Microsoft Hyper-V ホスト VM トラフィックは、VLAN-Sec を使用して Cisco ACI リーフスイッチに送信されます。

関連情報

Cisco ACI 仮想エッジ環境での EPG 内分離の設定については、[Cisco ACI Virtual Edge Configuration Guide](#) の「Intra-EPG Isolation Enforcement for Cisco ACI Virtual Edge」の章を参照してください。

GUI を使用した VMware VDS または Microsoft Hyper-V の EPG 内分離の設定

手順の概要

1. Cisco APIC にログインします。
2. **Tenants** > *tenant* を選択します。
3. 左側のナビゲーションウィンドウで、[アプリケーションプロファイル]フォルダと適切なアプリケーションプロファイルを展開します。
4. **Application EPGs** フォルダを右クリックし、**Create Application EPG** を選択します。
5. **Create Application EPG** ダイアログ ボックスで、次の手順を実行します:
6. **Update** をクリックし、**Finish** をクリックします。

手順の詳細

ステップ 1 Cisco APIC にログインします。

ステップ 2 **Tenants** > *tenant* を選択します。

ステップ 3 左側のナビゲーションウィンドウで、[アプリケーションプロファイル]フォルダと適切なアプリケーションプロファイルを展開します。

ステップ 4 **Application EPGs** フォルダを右クリックし、**Create Application EPG** を選択します。

ステップ 5 **Create Application EPG** 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 EPG 名を追加します。
- b) **Intra EPG Isolation** エリアで、**Enforced** をクリックします。
- c) **Bridge Domain** フィールドで、ドロップダウン リストからブリッジ ドメインを選択します。
- d) EPG をベア メタル/物理ドメイン インターフェイスまたは VM ドメインに関連付けます。
 - VM ドメインの場合、[Associate to VM Domain Profiles] チェックボックスをオンにします。
 - ベア メタルの場合、[Statically Link with Leaves/Paths] チェックボックスをオンにします。
- e) [Next] をクリックします。
- f) **Associated VM Domain Profiles** エリアで、+ アイコンをクリックします。
- g) **Domain Profile** プロファイルのドロップダウン リストから、適切な VMM ドメインを選択します。

スタティックの場合、**Port Encap (or Secondary VLAN for Micro-Seg)** フィールドでセカンダリ VLAN を指定し、**Primary VLAN for Micro-Seg** フィールドで、プライマリ VLAN を指定します。Encap フィールドを空白のままにすると、値が動的に割り当てられます。

(注) スタティックの場合、スタティック VLAN を VLAN プールで使用できる必要があります。

ステップ 6 **Update** をクリックし、**Finish** をクリックします。

NX-OS スタイル CLI を使用した VMware VDS または Microsoft Hyper-V の EPG 内分離の設定

手順の概要

1. CLI で、EPG 内分離 EPG を作成します。
2. 設定を確認します。

手順の詳細

ステップ 1 CLI で、EPG 内分離 EPG を作成します。

例：

次の例は VMware VDS の場合です：

```
apicl(config)# tenant Test_Isolation
apicl(config-tenant)# application PVLAN
apicl(config-tenant-app)# epg EPG1
apicl(config-tenant-app-epg)# show running-config
# Command: show running-config tenant Tenant_VMM application Web epg intraEPGDeny
tenant Tenant_VMM
  application Web
    epg intraEPGDeny
      bridge-domain member VMM_BD
      vmware-domain member PVLAN encap vlan-2001 primary-encap vlan-2002 push on-demand
      vmware-domain member mininet
    exit
  isolation enforce
  exit
exit
apicl(config-tenant-app-epg)#
```

例：

次の例は、Microsoft Hyper-V 仮想スイッチを示します。

```
apicl(config)# tenant Test_Isolation
apicl(config-tenant)# application PVLAN
apicl(config-tenant-app)# epg EPG1
apicl(config-tenant-app-epg)# show running-config
# Command: show running-config tenant Tenant_VMM application Web epg intraEPGDeny
tenant Tenant_VMM
  application Web
    epg intraEPGDeny
      bridge-domain member VMM_BD
      microsoft-domain member domain1 encap vlan-2003 primary-encap vlan-2004
      microsoft-domain member domain2
    exit
  isolation enforce
  exit
exit
apicl(config-tenant-app-epg)#
```

```
apic1(config-tenant-app-epg)#
```

ステップ2 設定を確認します。

例：

```
show epg StaticEPG detail
Application EPG Data:
Tenant           : Test_Isolation
Application       : PVLAN
AEPg             : StaticEPG
BD               : VMM_BD
uSeg EPG         : no
Intra EPG Isolation : enforced
Vlan Domains     : VMM
Consumed Contracts : VMware_vDS-Ext
Provided Contracts : default, Isolate_EPG
Denied Contracts  :
Qos Class        : unspecified
Tag List         :
VMM Domains:
Domain           Type      Deployment Immediacy Resolution Immediacy State      Encap
-----
Primary
Encap
-----
DVS1             VMware   On Demand           immediate    formed     auto
  auto
Static Leaves:
Node      Encap      Deployment Immediacy Mode      Modification Time
-----
Static Paths:
Node      Interface      Encap      Modification Time
-----
1018     eth101/1/1     vlan-100   2016-02-11T18:39:02.337-08:00
1019     eth1/16        vlan-101   2016-02-11T18:39:02.337-08:00
Static Endpoints:
Node      Interface      Encap      End Point MAC      End Point IP Address
Modification Time
-----
Dynamic Endpoints:
Encap: (P):Primary VLAN, (S):Secondary VLAN
Node      Interface      Encap      End Point MAC      End Point IP Address
Modification Time
-----
1017     eth1/3         vlan-943 (P)    00:50:56:B3:64:C4  ---
2016-02-17T18:35:32.224-08:00
vlan-944 (S)
```


REST API を使用した VMware VDS または Microsoft Hyper-V バーチャルスイッチの EPG 内の分離の設定

手順の概要

1. XML API を使用してアプリケーションを展開するには、次の HTTP POST メッセージを送信します。
2. VMware VDS または Microsoft Hyper-V 仮想スイッチデプロイメントの場合は、POST メッセージの本文に次の XML 構造のいずれかを含めます。

手順の詳細

ステップ 1 XML API を使用してアプリケーションを展開するには、次の HTTP POST メッセージを送信します。

例：

```
POST https://apic-ip-address/api/mo/uni/tn-ExampleCorp.xml
```

ステップ 2 VMware VDS または Microsoft Hyper-V 仮想スイッチデプロイメントの場合は、POST メッセージの本文に次の XML 構造のいずれかを含めます。

例：

次の例は、VMware VDS の場合です。

```
<fvTenant name="Tenant_VMM" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <fvRsBd tnFvBDName="bd" />
      <!-- STATIC ENCAP ASSOCIATION TO VMM DOMAIN-->
      <fvRsDomAtt encap="vlan-2001" instrImedcy="lazy" primaryEncap="vlan-2002"
resImedcy="immediate" tDn="uni/vmmp-VMware/dom-DVS1">
    </fvAEPg>
  </fvAp>
</fvTenant>
```

例：

次の例は、Microsoft Hyper-V の仮想スイッチの場合です。

```
<fvTenant name="Tenant_VMM" >
  <fvAp name="Web">
    <fvAEPg name="IntraEPGDeny" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <fvRsBd tnFvBDName="bd" />
      <!-- STATIC ENCAP ASSOCIATION TO VMM DOMAIN-->
      <fvRsDomAtt tDn="uni/vmmp-Microsoft/dom-domain1">
    <fvRsDomAtt encap="vlan-2004" instrImedcy="lazy" primaryEncap="vlan-2003"
resImedcy="immediate" tDn="uni/vmmp-Microsoft/dom-domain2">
    </fvAEPg>
  </fvAp>
</fvTenant>
```

Cisco ACI 仮想エッジの EPG 内分離の設定

Cisco ACI Virtual Edge での EPG 内分離の適用

デフォルトでは、EPGに属するエンドポイントは契約が設定されていなくても相互に通信できます。ただし、相互に、EPG内のエンドポイントを特定できます。たとえば、EPG内でウイルスや他の問題を持つVMがEPGの他のVMに影響を及ぼすことがないように、エンドポイント分離を適用するのが望ましい場合があります。

アプリケーション内のすべてのエンドポイントに分離を設定することも、いずれにも設定しないこともできます。一部のエンドポイントに分離を設定し、他のエンドポイントに設定しない方法は使用できません。

EPG内のエンドポイントを分離しても、エンドポイントが別のEPG内のエンドポイントと通信できるようにするコントラクトには影響しません。



(注) VLAN モードで Cisco ACI Virtual Edge ドメインと関連付けられている EPG での EPG 内分離の適用はサポートされていません。このような EPG で EPG 内の分離を適用しようとすると、エラーがトリガーされます。



(注) Cisco ACI Virtual Edge マイクロセグメント (uSeg) EPG で EPG 内分離を使用することは現在のところサポートされていません。



(注) VXLAN カプセル化を使用し、EPG 内分離が適用されている Cisco ACI Virtual Edge EPG では、プロキシ ARP はサポートされていません。従って、Cisco ACI Virtual Edge EPG 間で契約が設定されていても、EPG 内分離された EPG 間でサブネット間通信を行うことはできません。(VXLAN)。

GUI を使用した Cisco ACI Virtual Edge の EPG 内分離の設定

この手順に従って、EPG のエンドポイントが相互に分離されている EPG を作成します。

EPG が使用するポートは VM マネージャ (VMM) のいずれかに属している必要があります。



- (注) この手順は、EPG の作成時に EPG 内のエンドポイントを分離することを前提としていません。既存の EPG 内のエンドポイントを分離するには、Cisco APIC 内の EPG を選択し、[Properties] ペインの [Intra EPG Isolation] 領域で [Enforced] を選択して [SUBMIT] をクリックします。

始める前に

VXLAN 関連の設定が Cisco ACI Virtual Edge VMM ドメインに存在すること、特に Cisco ACI Virtual Edge ファブリック全体のマルチキャストアドレスとマルチキャストアドレスのプール (EPG ごとに 1 つ) が存在することを確認します。

ステップ 1 Cisco APIC にログインします。

ステップ 2 [Tenants] を選択してテナントのフォルダを展開し、[Application Profiles] フォルダを展開します。

ステップ 3 アプリケーション プロファイルを右クリックし、[Create Application EPG] を選択します。

ステップ 4 [Create Application EPG] 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 EPG 名を入力します。
- b) [Intra EPG Isolation] 領域で、[Enforced] をクリックします。
- c) [Bridge Domain] ドロップダウン リストから、ブリッジ ドメインを選択します。
- d) [Associate to VM Domain Profiles] チェックボックスをオンにします。
- e) [Next] をクリックします。
- f) **Associate VM Domain Profiles** エリアで、次の手順に従います:
 - +(プラス) アイコンをクリックし、**Domain Profile** ドロップダウンリストから、対象とする Cisco ACI Virtual Edge VMM ドメインを選択します。
 - **Switching Mode** ドロップダウンリストから、**AVE** を選択します。
 - **Encap Mode** ドロップダウンリストから **VXLAN** または **Auto** を選択します。

Auto を選択したら、Cisco ACI Virtual Edge VMM ドメインのカプセル化モードが **VXLAN** になっていることを確認します。

 - (オプション) セットアップに適した他の設定オプションを選択します。
- g) [Update] をクリックし、[Finish] をクリックします。

次のタスク

統計情報を選択して表示すると、エンドポイントが関与する問題の診断に役立ちます。このガイドの [Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する (36 ページ) と [Tenants] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する (36 ページ) を参照してください。

[Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する

[Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する

Cisco ACI Virtual Edge で EPG 内分離を設定した場合、拒否された接続数、受信パケット数、送信済みマルチキャストパケット数などのエンドポイントの統計情報を表示する前に、それらを選択する必要があります。その後、統計情報を表示できます。

- ステップ 1 Cisco APIC にログインします。
- ステップ 2 [Tenants] > [tenant] の順に選択します。
- ステップ 3 テナントのナビゲーション ウィンドウで、**Application Profiles**、*profile*、および **Application EPGs** フォルダを展開し、表示するエンドポイント統計情報を含む EPG を選択します。
- ステップ 4 EPG の [Properties] 作業ペインで、[Operational] タブをクリックして EPG 内のエンドポイントを表示します。
- ステップ 5 エンドポイントをダブルクリックします。
- ステップ 6 エンドポイントの [Properties] ダイアログボックスで、[Stats] タブをクリックし、チェック アイコンをクリックします。
- ステップ 7 **Select Stats** ダイアログボックスの **Available** ペインで、エンドポイントについて表示する統計情報を選択し、右向き矢印を使用してそれらの情報を **Selected** ペインに移動します。
- ステップ 8 [送信 (Submit)] をクリックします。

[Tenants] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する

Cisco ACI Virtual Edge で EPG 内分離を設定していた場合には、エンドポイントの統計情報を選択すると、確認することができるようになります。

始める前に

分離エンドポイントについて表示する統計情報を選択しておく必要があります。手順については、このガイドの [\[Tenants\] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する \(36 ページ\)](#) を参照してください。

- ステップ 1 Cisco APIC にログインします。
- ステップ 2 [Tenants] > [tenant] の順に選択します。
- ステップ 3 テナントのナビゲーション ウィンドウで、**Application Profiles**、*profile*、および **Application EPGs** フォルダを展開し、表示の必要な統計情報があるエンドポイントを含んでいる EPG を選択します。
- ステップ 4 EPG の [Properties] 作業ペインで、[Operational] タブをクリックして EPG 内のエンドポイントを表示します。
- ステップ 5 統計情報を表示するエンドポイントをダブルクリックします。
- ステップ 6 エンドポイントの **Properties** 作業ウィンドウで、**Stats** タブをクリックします。

作業ウィンドウに、先ほど選択した統計情報が表示されます。作業ウィンドウの左上で、テーブルビューアイコンやチャートビューアイコンをクリックして、ビューを変更できます。

[Virtual Networking] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する

Cisco ACI Virtual Edge で EPG 内分離を設定した場合、拒否された接続数、受信パケット数、送信済みマルチキャストパケット数などのエンドポイントの統計情報を表示する前に、それらを選択する必要があります。その後、統計情報を表示できます。

- ステップ 1 Cisco APIC にログインします。
- ステップ 2 **Virtual Networking > Inventory > VMM Domains > VMware > VMM domain > Controllers > controller instance name > DVS-VMM name > Portgroups > EPG name > Learned Point MAC address (node)** を選択します。
- ステップ 3 [Stats] タブをクリックします。
- ステップ 4 チェックマークが付いたタブをクリックします。
- ステップ 5 **Select Stats** ダイアログボックスで、表示する統計情報を **Available** ペインでクリックし、右向き矢印をクリックして、それらを **Selected** ペインに移動します。
- ステップ 6 (オプション) サンプル間隔を選択します。
- ステップ 7 [送信 (Submit)] をクリックします。

[Virtual Networking] タブで Cisco ACI Virtual Edge の分離エンドポイント統計情報を表示する

Cisco ACI Virtual Edge で EPG 内分離を設定していた場合には、エンドポイントの統計情報を選択すると、確認することができるようになります。

始める前に

分離エンドポイントについて表示する統計情報を選択しておく必要があります。手順については、このガイドの [Tenants] タブの下で、[Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する \(36 ページ\)](#) を参照してください。

- ステップ 1 Cisco APIC にログインします。
- ステップ 2 **Virtual Networking > Inventory > VMM Domains > VMware > VMM name > Controllers > controller instance name > DVS-VMM name > Portgroups > EPG name > Learned Point MAC address (node)** を選択します。
- ステップ 3 [Stats] タブをクリックします。

中央のウィンドウに、先ほど選択した統計情報を表示します。作業ウィンドウの左上で、テーブルビューアイコンやチャートビューアイコンをクリックして、ビューを変更できます。

NX-OS スタイルの CLI を使用した Cisco ACI Virtual Edge の EPG 内分離の設定

始める前に

VXLAN に関連する設定に存在するかどうかを確認します Cisco ACI Virtual Edge VMM ドメイン、特に、Cisco ACI Virtual Edge ファブリック全体のマルチキャストアドレスと (EPG ごとに 1 つ) のマルチキャストアドレスのプール。

CLI で、EPG 内分離 EPG を作成します。

例 :

```
# Command: show running-config tenant Tenant2 application AP-1 epg EPG-61
tenant Tenant2
  application AP-1
    epg EPG-61
      bridge-domain member BD-61
      vmware-domain member D-AVE-SITE-2-3
      switching-mode AVE
      encap-mode vxlan
    exit
  isolation enforce          # This enables EPG into isolation mode.
  exit
exit
exit
exit
```

次のタスク

統計情報を選択して表示すると、エンドポイントが関与する問題の診断に役立ちます。このガイドの [\[Tenants\] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する \(36 ページ\)](#) と [\[Tenants\] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する \(36 ページ\)](#) を参照してください。

REST API を使用した Cisco ACI Virtual Edge の EPG 内分離の設定

始める前に

VXLAN に関連する設定に存在するかどうかを確認します Cisco ACI Virtual Edge VMM ドメイン、特に、Cisco ACI Virtual Edge ファブリック全体のマルチキャストアドレスと (EPG ごとに 1 つ) のマルチキャストアドレスのプール。

ステップ 1 XML API を使用してアプリケーションを展開するには、次の HTTP POST メッセージを送信します。

例 :

```
POST
https://10.197.139.36/api/mo/uni/tn-Tenant2.xml
```

ステップ 2 VMM の導入では、POST メッセージの本文に次の例に示す XML 構造を含めます。

例 :

```
<fvTenant name="Tenant2" >
  <fvAp name="AP-1">
    <fvAEPg name="EPG-61" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <!-- pcEnfPref="unenforced" DISABLES ISOLATION-->
      <fvRsBd tnFvBDName="BD-61" />
      <fvRsDomAtt switchingMode="AVE" encapMode="vxlan" resImedcy="immediate"
tDn="uni/vmmp-VMware/dom-D-AVE-SITE-1-XXIII" >
        </fvRsDomAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

次のタスク

統計情報を選択して表示すると、エンドポイントが関与する問題の診断に役立ちます。このガイドの [\[Tenants\] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する \(36 ページ\)](#) と [\[Tenents\] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する \(36 ページ\)](#) を参照してください。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。