EPG

この章は、次の内容で構成されています。

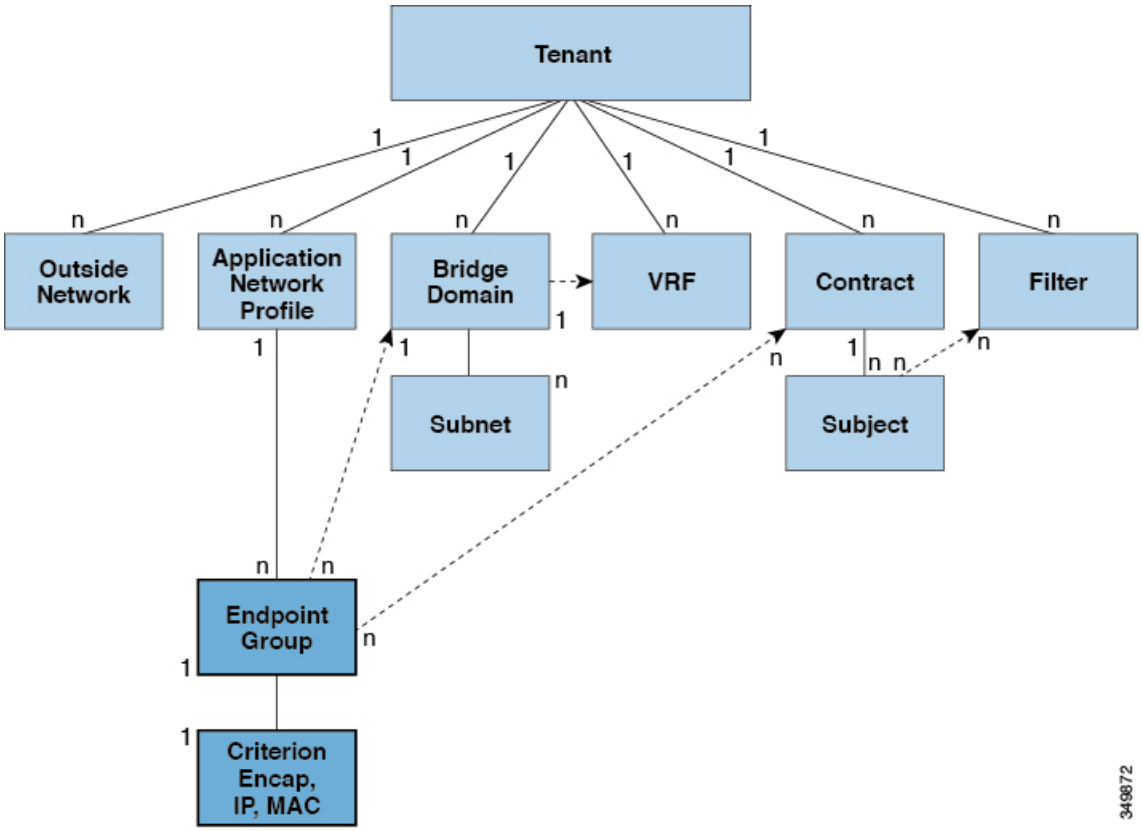
- エンドポイント グループについて （1 ページ）
- 特定のポートに EPG を導入する （7 ページ）
- 特定のポートに EPG を導入するためのドメイン、接続可能アクセス エンティティ プロファイル、および VLAN の作成 （10 ページ）
- 添付されているエンティティ プロファイルで複数のインターフェイスに EPG を導入する （15 ページ）
- EPG 内の分離 （17 ページ）
- Cisco ACI 仮想エッジの EPG 内分離の設定 （29 ページ）
- トラブルシューティング （34 ページ）
- エンドポイント接続のトラブルシューティング （34 ページ）
- IP bエース EPG 構成の確認 （39 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



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で、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

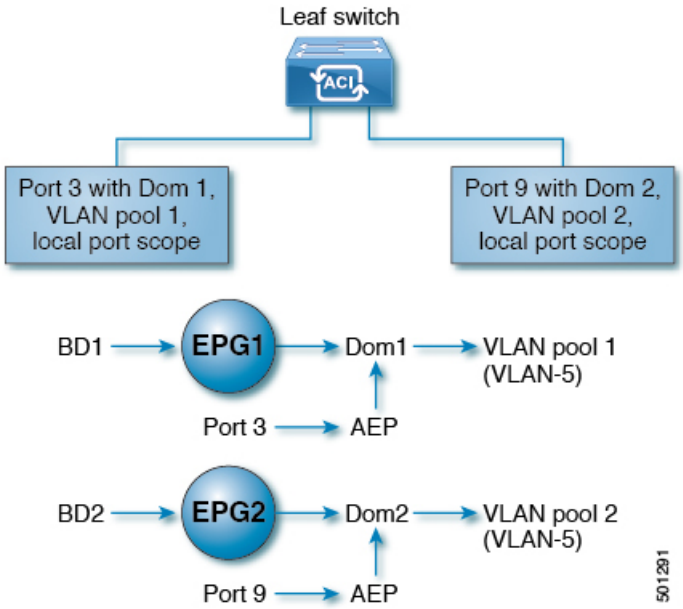
EPG トラフィックがフローは、Vlan の設定には次のガイドラインを使用します。

- 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

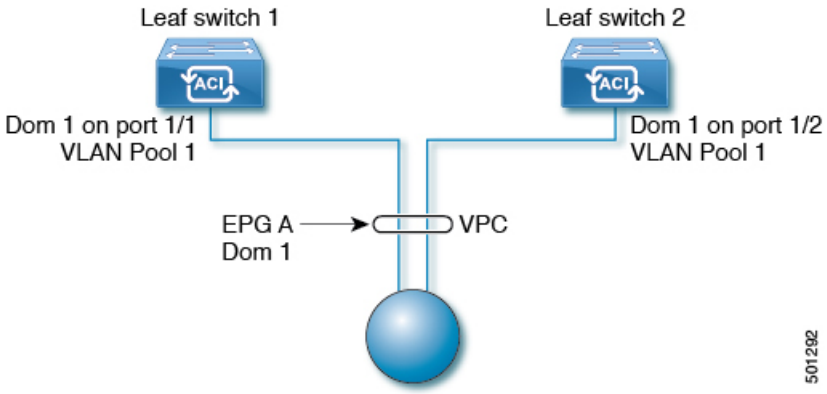
以前に、リーフ スイッチのポートに展開されている EPG 用に VLAN を設定していて、同じ VLAN 番号を同じリーフ スイッチの異なるポートの異なる EPG で再利用する場合には、中断なしでセットアップできるようにするため、次の例に示すようなプロセスに従ってください。

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。

手順

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	**1.** **Leaves** エリアを展開します。 **2.** [Node] ドロップダウン リストから、ノードを選択します。 **3.** **Encap** フィールドで、適切な VLAN を入力します。 **4.** (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。 **5.** (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	**1.** **Paths** エリアを展開します。 **2.** **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。 **3.** (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。 **4.** (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。 **5.** **Port Encap** フィールドに、導入するセカンダリ VLAN を入力します。 **6.** (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

この手順では、NX-OS スタイルの CLI を使用し、Cisco Application Policy Infrastructure Controller（APIC）の特定のポートに EPG を展開します。

（注） Cisco APIC でインターフェイスごとの設定を行う際に、GUI と CLI を混在させないでください。GUI で実行した設定が、NX-OS スタイルの CLI では部分的にしか扱えない場合があります。

手順

ステップ 1 VLAN ドメインを設定します。

例：

```
apic1(config)# vlan-domain dom1
apic1(config-vlan)# vlan 10-100
```

ステップ 2 テナントを作成します。

例：

```
apic1# configure
apic1(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：

```
apic1(config-tenant)# vrf context ctx1
apic1(config-tenant-vrf)# exit
```

ステップ 4 ブリッジ ドメインを作成します。

例：

```
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# vrf member ctx1
apic1(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：

```
apic1(config-tenant)# application AP1
apic1(config-tenant-app)# epg EPG1
apic1(config-tenant-app-epg)# bridge-domain member bd1
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
```

ステップ 6 EPG を特定のポートに関連付けます。

例：

```
apic1(config)# leaf 1017
apic1(config-leaf)# interface ethernet 1/13
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# switchport trunk allowed vlan 20 tenant t1 application AP1 epg EPG1
```

（注）
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。

特定のポートに EPG を導入するためのドメイン、接続可能アクセス 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、接続可能アクセス 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、接続可能アクセス 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 グループを接続可能アクセス 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

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 の下でタギングをサポートし、もう一方のエンド ポイントが同じ EPG 内で VLAN タギング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。

手順

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。

a) **[ノード タイプ（Node Type）]** で、**[リーフ（Leaf）]** をクリックします。

b) **[ポート タイプ（Port Type）]** で、**[アクセス（Access）]** をクリックします。

c) **[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。

d) **[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。

e) **[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。

f) **[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。

g) **[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。

手順

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：

```
apic1(config)# vlan-domain domP
apic1(config-vlan)# vlan 10
apic1(config-vlan)# vlan 25
apic1(config-vlan)# vlan 50-60
apic1(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：

```
apic1(config)# template policy-group PortGroup
apic1(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：

```
apic1(config)# leaf-interface-profile InterfaceProfile1
apic1(config-leaf-if-profile)# leaf-interface-group range
apic1(config-leaf-if-group)# policy-group PortGroup
apic1(config-leaf-if-group)# interface ethernet 1/11-13
apic1(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：

```
apic1(config)# leaf-profile SwitchProfile-1019
apic1(config-leaf-profile)# leaf-interface-profile InterfaceProfile1
apic1(config-leaf-profile)# leaf-group range
apic1(config-leaf-group)# leaf 1019
apic1(config-leaf-group)#
```

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と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 FD VNID 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 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。

手順

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と、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。

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 を使用してアプリケーション EPG を複数のポートに展開する

APIC GUI と REST API を使用して、接続可能エンティティ 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、単一の構成の接続可能エンティティ 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 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

アプリケーション EPG を接続可能アクセス エンティティ プロファイルに関連付けて、その接続可能アクセス 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。
- ターゲットの接続可能アクセス 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。
- Cisco APIC 6.1(3) よりも前は、アクセス ポリシー階層を介してのみ、アプリケーションを接続可能アクセスエンティティプロファイルに関連付けることができました。Cisco APIC 6.1(3) 以降は、テナント階層またはアクセス ポリシー階層を介して、アプリケーションを接続可能アクセス エンティティ プロファイルに関連付けることができるようになりました。

（注） これらの特定の階層のいずれかを使用して AEP アタッチメントを作成する場合は、後続の変更操作も、作成された階層でのみ実行する必要があります。操作に重複がある場合、Cisco APIC はこの設定を拒否します。

手順

ステップ 1 次のいずれかの方法を使用して、アプリケーション EPG を接続可能アクセス エンティティ プロファイルに関連付けることができます。

a) 使用するアプリケーション EPG のページを開きます。GUI で、**[テナント（Tenant）]** > **[tenant_name]** > **[アプリケーション プロファイル（Application Profiles）]** > **[epg_name]** > **[静的 AAEP（Static AAEP）]** をクリックします。

b) **[静的 AAEP（Static AAEP）]** ウィンドウで、ターゲット接続可能アクセス エンティティ プロファイルをアプリケーション EPG に関連付けます。

フィールド	アクション（Action）
名前	AEP の名前を選択します。
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 ID を入力します。
Primary Encap	（オプション）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 ID を入力します。
展開の緊急性	**[直ちに展開（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 **[オンデマンド（On Demand）]** のままにするか、**[即座（Immediate）]** を選択します。
モード（Mode）	データを送信するモードを指定します： • **[トランク（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。 • **[トランク（ネイティブ）（Trunk（Native））]**：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。 • **[アクセス（タグなし）（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 2 または、この方法を使用して、アプリケーション EPG を接続エンティティ プロファイルに関連付けます。

a) 使用する接続可能アクセス 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）]** > **[接続可能アクセス エンティティ プロファイル（Attachable Access Entity Profiles）]** に移動します。

b) 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、[接続可能アクセス エンティティ プロファイル（Attachable Access Entity Profiles）] ウィンドウを開きます。

c) **[使用方法を表示（Show Usage）]** ボタンをクリックして、この接続可能アクセス 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展開されます。

d) **[アプリケーション EPG（Application EPGs）]** テーブルに基づき、この接続可能アクセス 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（**Action**）
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 ID の名前を入力します。
Primary Encap	（オプション）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 ID 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。 • [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。 • **[トランク（ネイティブ）（Trunk（Native））]**：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。 • **[アクセス（タグなし）（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 3 [送信（Submit）] をクリックします。
この接続可能アクセス 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、この接続可能アクセス 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展開されます。

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 EGP 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。

ベア メタル サーバの EPG 内分離

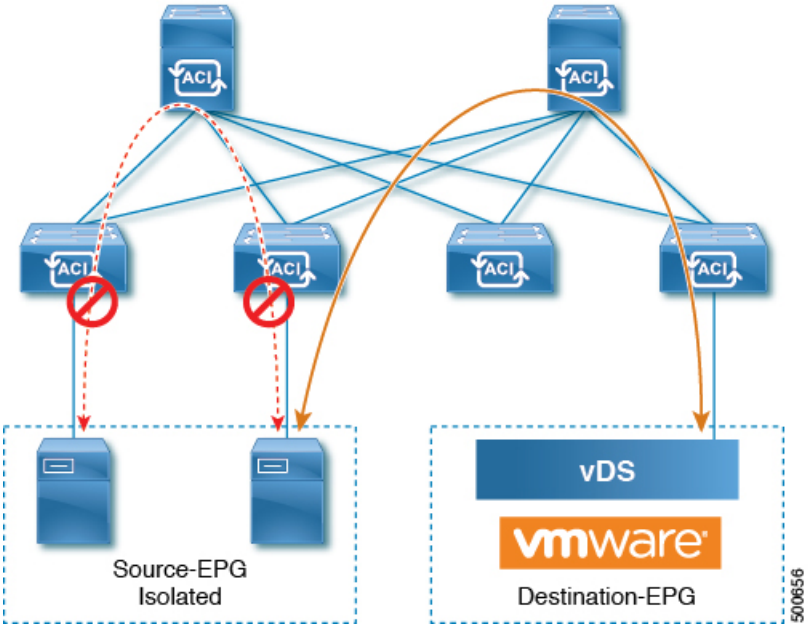
ベア メタル サーバの EPG 内分離

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

手順

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) **[完了（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

手順

	コマンドまたはアクション	目的

ステップ 1	CLI で、EPG 内分離 EPG を作成します。
	例：
	以下に、VMM ケースを示します。
	`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`	

	コマンドまたはアクション	目的

	`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`
	
	`ifav19-ifc1(config-leaf-if)# switchport trunk native vlan 101 tenant Test_Isolation application PVLAN epg StaticEPG primary-vlan 100`
	`exit`	

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 : 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`	

	コマンドまたはアクション	目的
	vlan-101 2016-02-11T18:39:02.337-08:00 Static Endpoints: Node Interface Encap End Point MAC End Point IP Address Modification Time ---------- ---------- ---------- ---------- ---------- ----------	

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
          classprio:              1   :::     floodmetptr:             13
          maclearnen:             1   :::       iplearnen:              1
         sclasslrnen:             1   :::   bypselffwdchk:              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
          classprio:              1   :::     floodmetptr:             13
          maclearnen:             1   :::       iplearnen:              1
         sclasslrnen:             1   :::   bypselffwdchk:              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   :::       iplearnen:              1
sclasslrnen:              1   :::   bypselffwdchk:              0
   qosusetc:              0   :::       qosuseexp:              0
   isolated:              1   :::   primary_encap:           1103
  proxy_arp:              0   :::       qinq core:              0
  ivxlan_dl:              0   :::       dtag_mode:              0
```

（注）

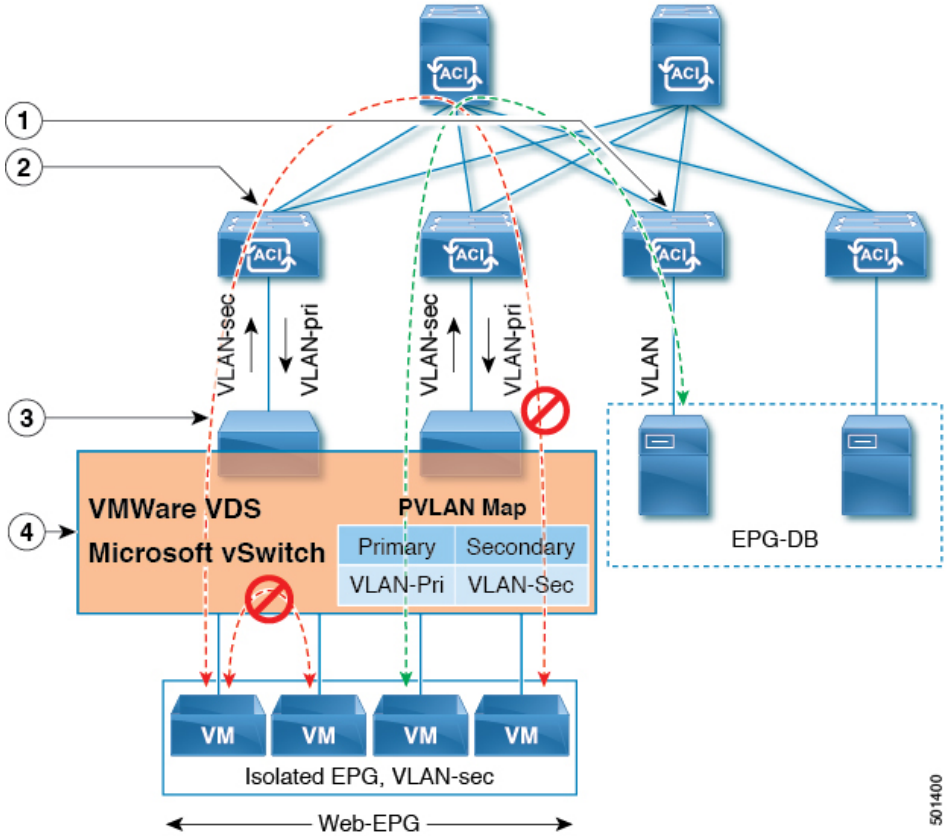
- イントラ EPG 隔離が強制されない場合、設定で指定されていても VLAN-pri 値は無視されます。
- EDM UCSM 統合を使用した VMware 分散仮想スイッチ（DVS）ドメインが失敗することがあります。ドメインに接続されているエンドポイント グループ（EPG）で EPG 内分離を設定し、プライベート VLAN をサポートしない UCSM Mini 6324 を使用すると、ドメインに障害が発生します。

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



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。

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

手順

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

手順

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:

```
apic1(config)# tenant Test_Isolation
apic1(config-tenant)# application PVLAN
apic1(config-tenant-app)# epg EPG1
apic1(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
    exit
apic1(config-tenant-app-epg)#
```

例：

次の例は、Microsoft Hyper-V 仮想スイッチを示します。

```
apic1(config)# tenant Test_Isolation
apic1(config-tenant)# application PVLAN
apic1(config-tenant-app)# epg EPG1
apic1(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
    exit
```

```
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)
```

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す。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。

手順

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 （31 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 （31 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

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。

手順

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。

[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

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 （31 ページ） を参照してください。

手順

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。

手順

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)サンプリング間隔を選択します。

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 （31 ページ） を参照してください。

手順

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。

手順

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
```

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 （31 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 （31 ページ） を参照してください。

トラブルシューティング

エンドポイント接続のトラブルシューティング

手順

ステップ 1 各エンドポイントの動作ステータスを調べます。

動作ステータスにはエンドポイントのエラーや設定ミスが示されます。詳細は、

エンドポイント ステータスの検査 （35 ページ） を

ステップ 2 トンネル インターフェイスのステータスを調べます。

動作ステータスにはトンネルのエラーや設定ミスが示されます。「トンネル インターフェイス ステータスの検査 （35 ページ）」を参照してください。

ステップ 3 エンドポイント グループ（EPG）間で traceroute を実行します。

トレースルートでは、スパイン ノードなどの中間ノード、およびエンドポイント間の問題が明らかになります。「エンドポイント 間での traceroute の実行 （36 ページ）」を参照してください。

ステップ 4 エンドポイントのアトミック カウンタを構成します。

アトミック カウンタは、発信元エンドポイントがパケットを送信しているか、また送信先エンドポイントがパケットを受信しているか、そして受信されたパケット数が送信されたパケット数に等しいかどうかを確認します。「アトミック カウンタの構成 （37 ページ）」を参照してください。

ステップ 5 各 EPG でコントラクトを調べます。

各 EPG でのコントラクトを調べ、EPG 間でのトラフィックの流れが許可されているかを確認します。テストとして一時的にコントラクトを開き、無制限のトラフィックを許可することができます。

ステップ 6 発信元パケットをモニタリング ノードに転送するようにスパン ポリシーを構成します。

モニタリング ノードのパケット アナライザが誤ったアドレスやプロトコルなどのパケットの問題を示します。「Cisco APIC GUI を使用したテナント SPAN セッションの設定 （38 ページ）」を参照してください。

エンドポイント ステータスの検査

手順

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 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 **[ナビゲーション（Navigation）]**ペインでテナントを拡張し、**[アプリケーション プロファイル（Application Profiles）]** を拡張して、エンドポイントが含まれるアプリケーション プロファイルを拡張します。

ステップ 4 **[アプリケーション EPG（Application EPGs）]** を展開し、確認する EPG をクリックします。

ステップ 5 **[作業（Work）]** ペインで、**[エンドポイント（Endpoint）]** テーブルのエンドポイントのリストから送信元エンドポイントをダブルクリックし、**[クライアント エンド ポイント（Client End Point）]** ダイアログボックスを開きます。

ステップ 6 **[クライアント エンド ポイント（Client End Point）]** ダイアログボックスで、エンドポイントのプロパティを確認し、**[操作性（Operational）]** タブをクリックします。

ステップ 7 **[操作性（Operational）]** タブで、健全性、ステータスおよび障害情報を表示します。

[ステータス（Status）]テーブルで、変更、イベント、またはエラーなどのエントリがある項目をクリックします。

ステップ 8 **[クライアント エンド ポイント（Client End Point）]** ダイアログボックスを閉じます。

ステップ 9 **[エンドポイント（Endpoint）]** テーブルでエンドポイントの **[インターフェイス（Interface）]** エントリを表示し、ノードとトンネル ID をメモに記録します。

ステップ 10 送信先エンドポイントでこの手順を繰り返します。

（注）
ファブリック内の 2 つのリーフ スイッチの背後に展開された 2 つのマイクロセグメント EPG の IP アドレス間で、双方向のトラフィックが中断されることがあります。これは、マイクロセグメント EPG からベース EPG への構成変更により、IP アドレスが移行しているときに発生する可能性があります。または逆に、双方向トラフィックの実行中に2つの異なるリーフ スイッチで同時に発生する可能性があります。この場合、各リモート エンドポイントのポリシー タグは引き続き以前の EPG を指します。

回避策：スイッチのリモートエンドポイントを手動でクリアするか、リモートエンドポイントが期限切れになるのを待ちます。エンドポイントをクリアするには、各スイッチの CLI にログオンし、適切なオプションを指定して **clear system internal epm endpoint** コマンドを入力します。たとえば、エンドポイントが IP アドレスに基づいている場合は、**clear system internal epm endpoint key vrf** *vrf_name***{ip | ipv6}** *ip-address* と入力します。その後、エンドポイントは正しいポリシー タグで再学習されます。

トンネル インターフェイス ステータスの検査

この手順では、トンネル インターフェイスの動作ステータスを調べる方法を示します。

手順

ステップ 1 メニュー バーで、[Fabric] をクリックします。

ステップ 2 サブメニュー バーで、[Inventory] をクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインでポッドを拡張し、発信元エンドポイント インターフェイスのノード ID を拡張します。

ステップ 4 ノードの下で **[インターフェイス（Interfaces）]** を拡張し、**[トンネル インターフェイス（Tunnel Interfaces）]** を拡張して、発信元エンドポイント インターフェイス のトンネル ID をクリックします。

ステップ 5 **[作業（Work）]** ペインで、トンネル インターフェイスのプロパティを確認し、**[操作（Operational）]** タブをクリックします。

ステップ 6 **[操作性（Operational）]** タブで、健全性、ステータスおよび障害情報を表示します。

[ステータス（Status）] テーブルで、変更、イベント、またはエラーなどのエントリがある項目をクリックします。

ステップ 7 送信先エンドポイント インターフェイスでこの手順を繰り返します。

エンドポイント 間での traceroute の実行

手順

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 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 **[ナビゲーション]** ペインでテナントを展開し、**[ポリシー]** > **[トラブルシューティング]** を展開します。

ステップ 4 [Troubleshoot] で次のトレースルート ポリシーのいずれかを右クリックします。

- [Endpoint-to-Endpoint Traceroute Policies] を右クリックして [Create Endpoint-to-Endpoint Traceroute Policy] を選択する
- [Endpoint-to-External-IP Traceroute Policies] を右クリックして [Create Endpoint-to-External-IP Traceroute Policy] を選択する
- [External-IP-to-Endpoint Traceroute Policies] を右クリックして [Create External-IP-to-Endpoint Traceroute Policy] を選択する
- [External-IP-to-External-IP Traceroute Policies] を右クリックして [Create External-IP-to-External-IP Traceroute Policy] を選択する

ステップ 5 ダイアログボックスのフィールドに適切な値を入力し、[Submit] をクリックします。

（注）

フィールドの説明については、ダイアログボックスの右上隅にあるヘルプアイコン（[?]）をクリックしてください。

ステップ 6 **[Navigation]** ペインまたは **[Traceroute Policies]** テーブルで、traceroute ポリシーをクリックします。

トレースルート ポリシーが [Work] ペインに表示されます。

ステップ 7 [Work] ペインで [Operational] タブをクリックし、[Source Endpoints] タブ、[Results] タブの順にクリックします。

ステップ 8 **[Traceroute Results]** テーブルで、追跡に使用された単数または複数のパスを確認します。

（注）

- 複数のパスが、送信元ノードから宛先ノードへの移動に使用されている場合があります。
- **[Name]** 列など、1 つまたは複数の列の幅を広げると確認しやすくなります。

アトミック カウンタの構成

手順

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 サブメニュー バーで、必要なテナントをクリックします。

ステップ 3 **Navigation** ウィンドウで、テナントを展開し、**Policies** を展開し、それから **Troubleshoot** を展開します。

ステップ 4 **Troubleshoot** の下で、**Atomic Counter Policy** を展開し、トラフィック トポロジを選択します。

エンドポイントの組み合わせ、エンドポイント グループ、外部インターフェイスおよびIPアドレス間のトラフィックを測定できます。

ステップ 5 必要なトポロジを右クリックして、**Add** *topology* **Policy** を選択し、**Add Policy** ダイアログボックスを開きます。

ステップ 6 [Add Policy] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドにポリシーの名前を入力します。

b) トラフィックの送信元の識別情報を選択するか、入力します。

必要な識別情報のソース（エンドポイント、エンドポイントのグループ、外部インターフェイス、または IP アドレス）によって異なります。

c) トラフィックの宛先の識別情報を選択するか、入力します。

d) （任意）（任意）[Filters] テーブルで +アイコンをクリックし、カウントするトラフィックのフィルタリングを指定します。

表示される [Create Atomic Counter Filter] ダイアログボックスで、IP プロトコル番号（たとえば TCP=6）によるフィルタリング、および送信元と宛先の IP ポート番号によるフィルタリングを指定できます。

e) [Submit] をクリックし、アトミック カウンタ ポリシーを保存します。

ステップ 7 [Navigation] ペインで、選択したトポロジの下の新しいアトミック カウンタ ポリシーを選択します。
ポリシー設定が [Work] ペインに表示されます。

ステップ 8 [Work] ペインで [Operational] タブをクリックし、[Traffic] サブタブをクリックして、アトミック カウンタの統計情報を表示します。

Cisco APIC GUI を使用したテナント SPAN セッションの設定

SPAN は、スイッチまたはテナントで設定できます。このセクションでは、Cisco APIC GUI を使用して、複製された送信元パケットをリモート トラフィック アナライザに転送するようにテナントの SPAN ポリシーを設定する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。フィールドを理解し、有効な値を決定するには、ダイアログ ボックスの右上隅にあるヘルプアイコン（**?**）をクリックしてヘルプ ファイルを表示します。

手順

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 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインでテナントを展開し、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > を展開して、**[SPAN]** を展開します。

[SPAN] に表示される 2 つのノード：**[SPAN 宛先グループ（SPAN Destination Groups）]** と **[SPAN 送信元グループ（SPAN Source Groups）]**。

ステップ 4 **[ナビゲーション（Navigation）]** の下で **[SPAN 送信元グループ（SPAN Source Groups）]** を右クリックし、**[SPAN 送信元グループの作成（Create SPAN Source Group）]** を選択します。
[Create SPAN Source Group] ダイアログが表示されます。

ステップ 5 **[SPAN 送信元グループの作成（Create SPAN Source Group）]** ダイアログ ボックスの必須フィールドに適切な値を入力します。

ステップ 6 **[送信元の作成（Create Sources）]** テーブルを展開し、**[SPAN 送信元の作成]** ダイアログ ボックスを開きます。

ステップ 7 **[SPAN 送信元の作成（Create SPAN Source）]** ダイアログ ボックスのフィールドに適切な値を入力します。

ステップ 8 SPAN送信元の作成が完了したら、**[OK]** をクリックします。

[SPAN 送信元グループの作成（Create VRF）] ダイアログ ボックスに戻ります。

ステップ 9 **[リモート場所の作成（Create Remote Location）]** ダイアログのフィールドに値を入力したら、**[送信（Submit）]** をクリックします。

次のタスク

SPAN 送信先のトラフィック アナライザを使用して、SPAN 送信元 EPGからのデータ パケットを観察し、パケット形式、アドレス、プロトコルおよびその他の情報を確認できます。

IP bエース EPG 構成の確認

作成できるエンドポイント グループ（EPG）には、アプリケーション EPG と IP ベースの EPG の 2 種類があります。IP ベースの EPG は、マイクロセグメント EPG であるという点で通常のアプリケーション EPG とは異なります。この章では、GUI またはスイッチ コマンドを使用して、IP ベースの EPG 構成が IP ベースとして正しく分類されていることを確認する方法について説明します。

この章は、次の項で構成されています。

GUI を使用した IP ベースの EPG 構成の確認

この手順では、GUI および Visore ツールを使用して IP ベースの EPG が正しく構成されていることを確認する方法について説明します。

手順

ステップ 1 作成した IP ベースの EPG が GUI の **uSeg EPGs** フォルダーの下に表示されていることを確認します（次のスクリーン キャプチャを参照）。
REST API を使用して作成された「IP」という名前の uSeg EPG の下にリストされている 1 つの IP ベースの EPG があることに注意してください。

ステップ 2 各 EPG IP（IP ベースの EPG）の EPG - IP プロパティ画面（右側のウィンドウ ペイン）で情報が正しいことを確認します。
画面の下部に表示される IP ベースの EPG と IP アドレスのリストに注意してください。

ステップ 3 Web ブラウザから、APIC の IP アドレスに続けて「/visore.html」を入力します。Visore は、EPG など、システム内のすべてのオブジェクトを表示できるツールです。Visore を使用して、IP ベースの EPG が正しく構成されていることを確認できます。Visore の詳細については、『アプリケーション ポリシー インフラストラクチャ コントローラ *Visore* ツールの紹介』を参照してください。

ステップ 4 ユーザー名とパスワードを入力し、**[ログイン（Login）]** をクリックします。

ステップ 5 **クラスまたは DN** の隣のフィールド（たとえば、「fvAEPg」）にクラスの名前を入力して、GUI で確認した IP ベースの EPG のクエリを実行します。

（注）
これは、APIC の観点からのビューです。上記の「示されるオブジェクトの総数（Total objects shown）」が「3」であることがわかります。これは、スイッチにダウンロードされた 3 つの EPG があることを意味します。以前 GUI に「IP」としてリストされていた IP ベースの EPG が、「dn」の隣に表示されていることがわかります。また、「isAttrBasedEPg」の横に「yes」と表示されていることにも注意してください。これは、これが IP ベースの EPG として適切に構成されたことを意味します。アプリケーション EPG と IP

ベースの EPG の両方を含む、すべてのオブジェクトが Visore を使用して正常に設定されていることを確認できます。

ステップ 6 スイッチ側から見た図です。スイッチで、fvEpP クラスのクエリを実行して EPG を表示し、「crtrnEnabled」属性を確認できます。IP ベースの EPG の場合は「yes」に設定されます。
この EPG の下で、EPG の子が IP アドレスとともに表示されていることを確認して、適切な構成を確保します。構成された IP アドレスごとに、スイッチがトラフィックの分類に使用する 1 つのオブジェクト（「l3IpCktEp」という名前）があります。構成が完了すると、パケットが到着すると、スイッチはこれらのオブジェクトを使用して分類します。

ステップ 7 構成したすべてのエンドポイントと IP アドレスの pcTag が一致することを確認します。すべての EPG には pcTag があります。構成した IP アドレスと一致するすべてのエンドポイントは、この pcTag に分類されます。すべてのエンドポイントには、クラスクエリを実行できる IP アドレスがあります。トラブルシューティングを行うときは、これらのエンドポイント（サーバー）がこの IP ベースの EPG に正しく分類されているかどうかを確認する必要があります。（pcTags は IP ベースの EPG に一致する必要があります。）

スイッチ コマンドを使用した IP-EPG 構成の確認

この手順では、スイッチ コマンドを使用して IP-EPG (「IpCkt」)構成定を確認する方法について説明します。

手順

ステップ 1 リーフにログインします。

ステップ 2 /mit/sys ディレクトリに移動します。

ステップ 3 /mit/sys ディレクトリで、ctx（vrf コンテキスト ディレクトリ）を見つけます。

ステップ 4 VRF cts ディレクトリで、IpCkt が構成されている特定の BD ディレクトリに移動します。
IpCkt が表示されます。

（注）
「IpCkt」と「IP-EPG」は、このドキュメントでは同じ意味で使用されます。

ステップ 5 ディレクトリに移動すると、「猫の概要」に IpCkt に関する情報が表示されます。

ステップ 6 サマリーの「operSt」に「サポートされていない」と表示されていないことを確認してください。

ステップ 7 IpCkt が構成されている BD に対応する VLAN ID を見つけます。

（注）
VLAN ID は、**show vlan internal bd-info** コマンドのいずれか、または **show system internal epm vlan all** コマンドで見つけることができます。

ステップ 8 BD の VLAN ID を見つけたら、**show system internal epm <vlan-id> detail** を発行します。
ここで、特定の sclass で構成されたすべての IpCkts を表示できるはずです。（/mit/sys ディレクトリに表示されるものと一致する必要があります。）

ステップ 9 vsh で実行した手順を vsh_lc に対して繰り返します。

ステップ 10 BD の IpCtk に一致する IP を使用して、**show system internal epm endp ip <a.b.c.d>** を介してトラフィックを送信します。学習した IP に「sclass」の IP フラグと特定の sclass 値があることを確認できます。

ステップ 11 vsh で実行した手順を vsh_lc に対して繰り返します。

この手順で使用するスイッチ トラブルシューティング コマンドのリスト:

```
Cd /mits/sys/ctx-vxlan…/bd-vxlan…
     - cat summary
Vsh -c “show system internal epm vlan all” or
Vsh -c “show vlan internal bd-info”
Vsh -c “show system internal epm vlan <vlan-id> detail”
Vsh -c “show system internal epm endp ip <a.b.c.d>"
Vsh_lc -c “show system internal epm vlan all” or
Vsh_lc -c “show vlan internal bd-info”
Vsh_lc -c “show system internal epm vlan <vlan-id> detail”
vsh_lc -c “show system internal epm endp ip <a.b.c.d>”
vsh_lc -c “show system internal epm epg”
```

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。