ACI ファブリックのアクセス レイヤ 2 接続

この章の内容は、次のとおりです。

ネットワーク ドメイン

ファブリック管理者は、ポート、プロトコル、VLAN プール、およびカプセル化を設定するドメイン ポリシーを作成します。これらのポリシーは、単一テナント専用にすることも、共有することもできます。ファブリック管理者が ACI ファブリック内にドメインを設定すると、テナント管理者はテナント エンドポイント グループ（EPG）をドメインに関連付けることができます。

以下のネットワーク ドメイン プロファイルを設定できます。

- VMM ドメイン プロファイル（`vmmDomP`）は、仮想マシンのハイパーバイザ統合のために必要です。
- 物理ドメイン プロファイル（`physDomP`）は、ベア メタル サーバ接続と管理アクセスに使用します。

- ブリッジド外部ネットワーク ドメイン プロファイル（l2extDomP）は通常、ACI ファブリックのリーフ スイッチにブリッジド外部ネットワーク トランク スイッチを接続するために使用されます。
- ルーテッド外部ネットワーク ドメイン プロファイル（l3extDomP）は、ACI ファブリックのリーフ スイッチにルータを接続するために使用されます。

ドメインは VLAN プールに関連付けられるように設定されます。その後、EPG は、ドメインに関連付けられている VLAN を使用するように設定されます。

（注） EPG ポートと VLAN の設定は、EPG が関連付けられているドメイン インフラストラクチャ設定で指定されている設定に一致する必要があります。一致しない場合、APIC でエラーが発生します。そのようなエラーが発生した場合は、ドメインインフラストラクチャ設定が EPG ポートと VLAN の設定に一致していることを確認してください。

接続可能エンティティ プロファイル

ACI ファブリックにより、リーフ ポートを通してベア メタル サーバ、仮想サーバ、ハイパーバイザ、レイヤ 2 スイッチ（たとえば、Cisco UCS ファブリック インターコネクト）、またはレイヤ 3 ルータ（たとえば、Cisco Nexus 7000 シリーズ スイッチ）などのさまざまな外部エンティティに接続する複数の接続ポイントが提供されます。これらの接続ポイントは、リーフ スイッチ上の物理ポート、FEX ポート、ポート チャネル、またはバーチャル ポート チャネル（vPC）にすることができます。

接続可能エンティティ プロファイル（AEP）は、同様のインフラストラクチャ ポリシー要件を持つ外部エンティティのグループを表します。インフラストラクチャ ポリシーは、Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、最大伝送単位（MTU）、Link Aggregation Control Protocol（LACP）などのさまざまなプロトコル オプションを設定する物理インターフェイス ポリシーで構成されます。

AEP は、リーフ スイッチで VLAN プールを展開するのに必要です。カプセル化ブロック（および関連 VLAN）は、リーフ スイッチで再利用可能です。AEP は、VLAN プールの範囲を物理インフラストラクチャに暗黙的に提供します。

次の AEP の要件と依存関係は、さまざまな設定シナリオ（ネットワーク接続や VMM ドメインなど）でも考慮する必要があります。

- AEP は許容される VLAN の範囲を定義しますが、それらのプロビジョニングは行いません。EPG がポートに展開されていない限り、トラフィックは流れません。AEP で VLAN プールを定義しないと、EPG がプロビジョニングされても VLAN はリーフ ポートでイネーブルになりません。
- リーフ ポートで静的にバインディングしている EPG イベントに基づいて、または VMware vCenter や Microsoft Azure Service Center Virtual Machine Manager（SCVMM）などの外部コントローラからの VM イベントに基づいて、特定の VLAN がリーフ ポート上でプロビジョニングされるかイネーブルになります。

Virtual Machine Manager（VMM）ドメインは、AEP のインターフェイス ポリシー グループから物理インターフェイス ポリシーを自動的に取得します。

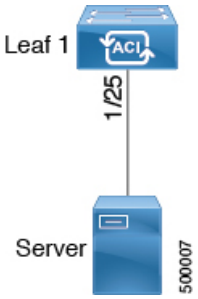
AEP のオーバーライド ポリシーを VMM ドメイン用の別の物理インターフェイス ポリシーを指定するために使用できます。このポリシーは、VM コントローラが中間レイヤ 2 ノードを介してリーフ スイッチに接続され、異なるポリシーがリーフ スイッチおよび VM コントローラの物理ポートで要求される場合に役立ちます。たとえば、リーフ スイッチとレイヤ 2 ノード間で LACP を設定できます。同時に、AEP オーバーライド ポリシーで LACP をディセーブルにすることで、VM コントローラとレイヤ 2 スイッチ間の LACP をディセーブルにできます。

ベア メタル サーバの ACI リーフ スイッチ インターフェイス設定

次の手順では、クイック スタート ウィザードを使用します。

（注） この手順では、ACI リーフ スイッチ インターフェイスにサーバを接続する手順を示します。手順は、ACI リーフ スイッチ インターフェイスに他の種類のデバイスを接続する場合と同じになります。

図 *1*：ベア メタル サーバのスイッチ インターフェイス設定



はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。

- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。

ステップ 1 APIC メニュー バーで、[Fabric] > [Access Policies] > [Quick Start] に移動し、[Configure an interface, PC, and VPC] をクリックします。

ステップ 2 [Select Switches To Configure Interfaces] 作業領域で、大きい [+] をクリックして、設定するスイッチを選択します。[Switches] セクションで、[Switches] をクリックして、使用可能なスイッチ ID のドロップダウン リストからスイッチ ID を追加し、[Update] をクリックします。

ステップ 3 大きい [+] をクリックして、スイッチ インターフェイスを設定します。
インターフェイス ポリシー グループは、選択したスイッチのインターフェイスに適用するインターフェイス ポリシーのグループを指定する名前付きポリシーです。インターフェイス ポリシーの例は、リンク レベル ポリシー（たとえば、1 gbit ポート速度）、ストーム制御インターフェイス ポリシーなどです。

（注） [Attached Dervice Type] ドメインは、スイッチ プロファイルで指定されているインターフェイスを EPG が使用できるようにするために必要です。

a) 使用するインターフェイス タイプとして [individual] を指定します。
b) 使用するインターフェイス ID を指定します。
c) 使用するインターフェイス ポリシーを指定します。
d) 使用する接続デバイス タイプを指定します。ベア メタル サーバに接続する場合、[Bare Metal] を選択します。ベア メタルでは、phys ドメイン タイプを使用します。
e) [Save] をクリックしてポリシーの詳細を更新し、[Submit] をクリックしてスイッチプロファイルを APIC に送信します。
APIC が、インターフェイス、セレクタ、および接続デバイス タイプの各ポリシーとともに、スイッチ プロファイルを作成します。

確認：スイッチインターフェイスが適切に設定されていることを確認するには、サーバが接続されているスイッチに対して CLI コマンド **show int** を使用します。

次の作業

これで、基本リーフ インターフェイスの設定手順は完了しました。

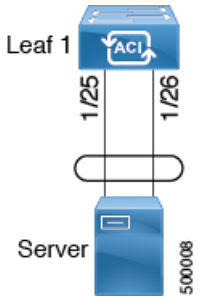
（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

ACI リーフ スイッチ ポート チャネル設定

次の手順では、クイック スタート ウィザードを使用します。

（注） この手順では、ACI リーフ スイッチ インターフェイスにサーバを接続する手順を示します。手順は、ACI リーフ スイッチ インターフェイスに他の種類のデバイスを接続する場合と同じになります。

図 *2*：スイッチ ポート チャネル設定



はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。

ステップ 1 APIC メニュー バーで、[Fabric] > [Access Policies] > [Quick Start] に移動し、[Configure an interface, PC, and VPC] をクリックします。

ステップ 2 [Select Switches To Configure Interfaces] 作業領域で、大きい [+] をクリックして、設定するスイッチを選択します。[Switches] セクションで、[Switches] をクリックして、使用可能なスイッチ ID のドロップダウン リストからスイッチ ID を追加し、[Update] をクリックします。

ステップ 3 大きい [+] をクリックして、スイッチ インターフェイスを設定します。
インターフェイス ポリシー グループは、選択したスイッチのインターフェイスに適用するインターフェイス ポリシーのグループを指定する名前付きポリシーです。インターフェイス ポリシーの例は、リンク レベル ポリシー（たとえば、1 gbit ポート速度）、ストーム制御インターフェイス ポリシーなどです。

（注） [Attached Dervice Type] は、スイッチ プロファイルで指定されているインターフェイスを EPG が使用できるようにするために必要です。

a) 使用するインターフェイス タイプとして [pc] を指定します。
b) 使用するインターフェイス ID を指定します。
c) 使用するインターフェイス ポリシーを指定します。

d) 使用する接続デバイス タイプを指定します。ベア メタル サーバに接続する場合、[Bare Metal] を選択します。ベア メタルでは、phys ドメイン タイプを使用します。

e) [Save] をクリックしてポリシーの詳細を更新し、[Submit] をクリックしてスイッチプロファイルを APIC に送信します。
APIC が、インターフェイス、セレクタ、および接続デバイス タイプの各ポリシーとともに、スイッチ プロファイルを作成します。

確認：スイッチインターフェイスが適切に設定されていることを確認するには、サーバが接続されているスイッチに対して CLI コマンド **show int** を使用します。

次の作業

これで、ポート チャネルの設定手順は完了しました。

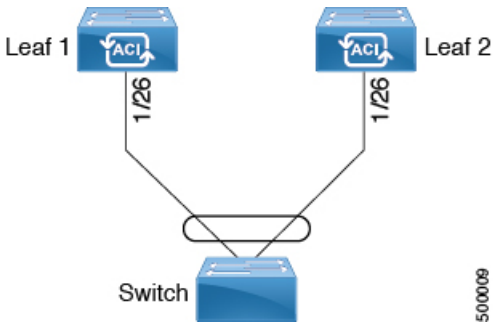
（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

ACI リーフ スイッチ バーチャル ポート チャネル設定

次の手順では、クイック スタート ウィザードを使用します。

（注） この手順では、ACI リーフ スイッチ バーチャル ポート チャネルにトランキング スイッチを接続する手順を示します。手順は、ACI リーフ スイッチ インターフェイスに他の種類のデバイスを接続する場合と同じになります。

図 *3*：スイッチ バーチャル ポート チャネル設定



はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。

ステップ 1 APIC メニュー バーで、[Fabric] > [Access Policies] > [Quick Start] に移動し、[Configure an interface, PC, and VPC] をクリックします。

ステップ 2 [Configure an interface, PC, and VPC] 作業領域で、大きい [+] をクリックして、スイッチを選択します。[Select Switches To Configure Interfaces] 作業領域が表示されます。

ステップ 3 ドロップダウン リストからスイッチ ID を選択し、プロファイルに名前を付け、[Save] をクリックします。保存したポリシーが [Configured Switch Interfaces] リストに表示されます。

ステップ 4 バーチャル ポート チャネルが選択したスイッチに対して使用する [Interface Policy Group] と [Attached Device Type] を設定します。
インターフェイス ポリシー グループは、選択したスイッチのインターフェイスに適用するインターフェイス ポリシーのグループを指定する名前付きポリシーです。インターフェイス ポリシーの例は、リンク レベル ポリシー（たとえば、1 gbit ポート速度）、ストーム制御インターフェイス ポリシーなどです。

（注） [Attached Dervice Type] ドメインは、スイッチ プロファイルで指定されているインターフェイスを EPG が使用できるようにするために必要です。

a) 使用するインターフェイス タイプ（individual、pc、または vpc）として [vpc] を指定します。
b) 使用するインターフェイス ID を指定します。
c) 使用するインターフェイス ポリシーを指定します。
d) 使用する接続デバイス タイプを指定します。スイッチの接続用に [External Bridged Devices] を選択します。
e) [Domain] および [VLAN Range] を指定します。
f) [Save] をクリックしてポリシーの詳細を更新し、[Submit] をクリックしてスイッチ プロファイルを APIC に送信します。
APIC が、インターフェイス、セレクタ、および接続デバイス タイプの各ポリシーとともに、スイッチ プロファイルを作成します。

確認：vpc が適切に設定されていることを確認するには、外部スイッチが接続されているリーフ スイッチに対して CLI コマンド **show int** を使用します。

次の作業

これで、スイッチ バーチャル ポート チャネルの設定手順は完了しました。

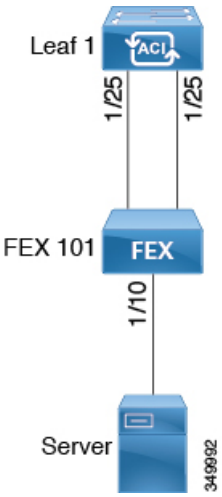
（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

基本的な FEX 設定

次の手順では、FEX導入に必要ないくつかのポリシーを自動的に作成するクイック スタート ウィザードを使用します。主な手順は次のとおりです。

1. 自動生成された FEX プロファイルを含むスイッチ プロファイルを設定します。
2. サーバを単一 FEX ポートに接続できるようにするために、自動生成された FEX プロファイルをカスタマイズします。

図 *4*：基本的な *FEX* 設定



（注） この手順では、FEX にサーバを接続する手順を示します。手順は、ACI が接続された FEX にデバイスを接続する場合と同じになります。

はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。

- ターゲット リーフ スイッチ、インターフェイス、およびプロトコルが設定されており、使用可能であること。
- FEX に電源が入っていて、ターゲット リーフ インターフェイスに接続されていること。

ステップ 1 APIC で、[Fabric] > [Access Policies] > [Quick Start] の [Configure Interface, PC, And VPC] ウィザードを使用して、スイッチ プロファイルを作成します。

a) APIC メニュー バーで、[Fabric] > [Access Policies] > [Quick Start] に移動します。
b) [Quick Start] ページで、[Configure an interface, PC, and VPC] オプションをクリックして [Configure Interface, PC And VPC] ウィンドウを開きます。
c) [Configure an interface, PC, and VPC] 作業領域で、[+] をクリックして、新しいスイッチ プロファイルを追加します。
d) [Select Switches To Configure Interfaces] 作業領域で、[Advanced] オプション ボタンをクリックします。
e) 使用可能なスイッチ ID のドロップダウン リストからスイッチを選択します。

トラブルシューティングのヒント
この手順では、1 つのスイッチがプロファイルに含まれています。複数のスイッチを選択すると、同じプロファイルを複数のスイッチで使用できます。

f) [Switch Profile Name] フィールドで名前を指定します。
g) [Fexes] リストの上にある [+] をクリックして、FEX ID およびスイッチ プロファイルへの接続に使用するスイッチ ポートを追加します。
h) [Save] をクリックして変更を保存します。[Submit] をクリックして、スイッチ プロファイルを APIC に送信します。
APIC が、必要な FEX プロファイル（*<switch policy name>_FexP<FEX ID>*）およびセレクタ（*<switch policy name>_ifselctor*）を自動的に生成します。

確認：FEX がオンラインであることを確認するには、FEX が接続されているスイッチに対して CLI コマンド **show fex** を使用します。

ステップ 2 サーバを単一 FEX ポートに接続できるようにするために、自動生成された FEX プロファイルをカスタマイズします。

a) [Navigation] ペインで、ポリシー リストで作成したスイッチ ポリシーを見つけます。また、自動生成された FEX、*<switch policy name>_FexP<FEX ID>* プロファイルもあります。
b) *<switch policy name>_FexP<FEX ID>* プロファイルの作業ペインで、[+] をクリックして *Interface Selectors For FEX* リストに新しいエントリを追加します。
[Create Access Port Selector] ダイアログが開きます。
c) セレクタの名前を指定します。
d) 使用する FEX インターフェイス ID を指定します。
e) リストから既存のインターフェイス ポリシー グループを選択するか、アクセス ポート ポリシー グループを作成します。
アクセス ポート ポリシー グループは、選択した FEX のインターフェイスに適用するインターフェイス ポリシーのグループを指定する名前付きポリシーです。インターフェイス ポリシーの例は、リンク

レベル ポリシー（たとえば、1 gbit ポート速度）、接続エンティティ プロファイル、ストーム制御インターフェイス ポリシーなどです。

（注） インターフェイス ポリシー グループ内で、FEX ポート セレクタで指定されているインターフェイスを EPG が使用できるようにするために、[Attached Entity Profile] は必須です。

f) [Submit] をクリックして FEX プロファイルを APIC に送信します。
APIC が FEX プロファイルを更新します。

確認：FEXインターフェイスが適切に設定されていることを確認するには、FEXが接続されているスイッチに対して CLI コマンド **show int** を使用します。

次の作業

これで、基本 FEX の設定手順は完了しました。

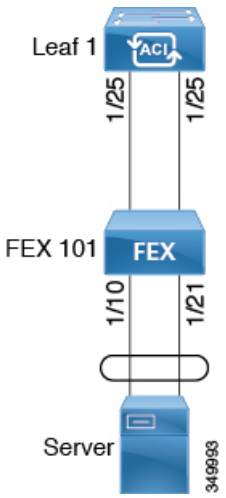
（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

FEX ポート チャネル設定

主な手順は次のとおりです。

1. ポート チャネルの形成に FEX ポートを使用するように FEX プロファイルを設定します。
2. サーバに接続できるようにポート チャネルを設定します。

図 *5*：*FEX* ポート チャネル



（注） この手順では、FEX ポート チャネルにサーバを接続する手順を示します。手順は、ACI が接続された FEX にデバイスを接続する場合と同じになります。

はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチ、インターフェイス、およびプロトコルが設定されており、使用可能であること。
- FEX が設定されており、電源が入っていて、ターゲット リーフ インターフェイスに接続されていること。

ステップ 1 APIC で、FEX プロファイルにポート チャネルを追加します。

a) APIC メニュー バーで、[Fabric] > [Access Policies] > [Switch Policies] > [Profiles] に移動します。

b) [Navigation] ペインで、FEX プロファイルを選択します。
APIC で自動生成された FEX プロファイル名の形式は、*<switch policy name>_FexP<FEX ID>* です。

c) [FEX Profile] 作業領域で、[+] をクリックして、[Interface Selectors For FEX] リストに新しいエントリを追加します。
[Create Access Port Selector] ダイアログが開きます。

ステップ 2 FEX ポート チャネルにサーバを接続できるように、[Create Access Port Selector] をカスタマイズします。

a) セレクタの名前を指定します。

b) 使用する FEX インターフェイス ID を指定します。

c) リストから既存のインターフェイス ポリシー グループを選択するか、PC インターフェイス プロファイル グループを作成します。
ポート チャネル インターフェイス ポリシー グループは、選択した FEX のインターフェイスに適用するポリシーのグループを指定します。インターフェイス ポリシーの例は、リンク レベル ポリシー（たとえば、1 gbit ポート速度）、接続エンティティ プロファイル、ストーム制御インターフェイス ポリシーなどです。

（注） インターフェイス ポリシー グループ内で、FEX ポート セレクタで指定されているインターフェイスを EPG が使用できるようにするために、[Attached Entity Profile] は必須です。

d) [Port Channel Policy] オプションで、設定の要件に従って静的 LDAP または動的 LDAP を選択します。

e) [Submit] をクリックして、更新された FEX プロファイルを APIC に送信します。
APIC が FEX プロファイルを更新します。

確認：ポート チャネルが適切に設定されていることを確認するには、FEX が接続されているスイッチに対して CLI コマンド **show port-channel summary** を使用します。

次の作業

これで、FEX ポート チャネルの設定手順は完了しました。

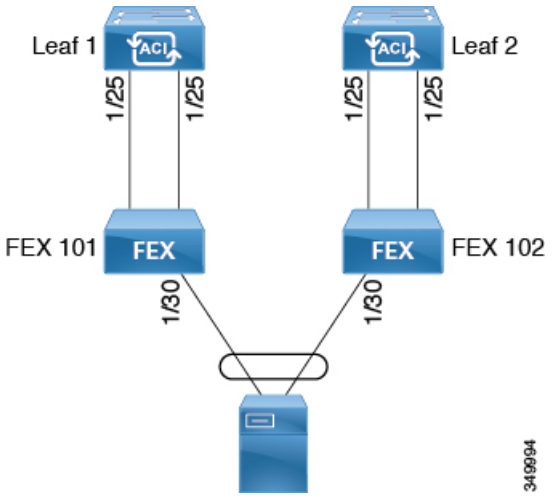
（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

FEX バーチャル ポート チャネル設定

主な手順は次のとおりです。

1. バーチャル ポート チャネルを形成するように、2 つの既存 FEX プロファイルを設定します。
2. FEX ポート チャネルにサーバを接続できるように、バーチャル ポート チャネルを設定します。

図 *6* : *FEX* バーチャル ポート チャネル



（注） この手順では、FEX バーチャル ポート チャネルにサーバを接続する手順を示します。手順は、ACI が接続された FEX にデバイスを接続する場合と同じになります。

はじめる前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチ、インターフェイス、およびプロトコルが設定されており、使用可能であること。
- FEX が設定されており、電源が入っていて、ターゲット リーフ インターフェイスに接続されていること。

ステップ 1 APIC で、2 つの FEX プロファイルにバーチャル ポート チャネルを追加します。

a) APIC メニュー バーで、[Fabric] > [Access Policies] > [Switch Policies] > [Profiles] に移動します。

b) [Navigation] ペインで、最初の FEX プロファイルを選択します。
APIC で自動生成された FEX プロファイル名の形式は、<*switch policy name*>_*FexP*<*FEX ID*> です。

c) [FEX Profile] 作業領域で、[+] をクリックして、[Interface Selectors For FEX] リストに新しいエントリを追加します。
[Create Access Port Selector] ダイアログが開きます。

ステップ 2 FEX バーチャル ポート チャネルにサーバを接続できるように、[Create Access Port Selector] をカスタマイズします。

a) セレクタの名前を指定します。

b) 使用する FEX インターフェイス ID を指定します。
通常、各 FEX に同じインターフェイス ID を使用してバーチャル ポート チャネルを形成します。

c) リストから既存のインターフェイス ポリシー グループを選択するか、VPC インターフェイス プロファイル グループを作成します。
バーチャル ポート チャネル インターフェイス ポリシー グループは、選択した FEX のインターフェイスに適用するポリシーのグループを指定します。インターフェイス ポリシーの例は、リンク レベル ポリシー（たとえば、1 gbit ポート速度）、接続エンティティ プロファイル、ストーム制御インターフェイス ポリシーなどです。

（注） インターフェイス ポリシー グループ内で、FEX ポート セレクタで指定されているインターフェイスを EPG が使用できるようにするために、[Attached Entity Profile] は必須です。

d) [Port Channel Policy] オプションで、設定の要件に従って静的 LDAP または動的 LDAP を選択します。

e) [Submit] をクリックして、更新された FEX プロファイルを APIC に送信します。
APIC が FEX プロファイルを更新します。

確認：ポート チャネルが適切に設定されていることを確認するには、FEX が接続されているスイッチに対して CLI コマンド **show port-channel summary** を使用します。

ステップ 3 最初の FEX に指定したものと同じインターフェイス ポリシー グループを使用するように 2 番目の FEX を設定します。

a) 2 番目の FEX プロファイルの [FEX Profile] 作業領域で、[+] をクリックして、[Interface Selectors For FEX] リストに新しいエントリを追加します。
[Create Access Port Selector] ダイアログが開きます。
b) セレクタの名前を指定します。
c) 使用する FEX インターフェイス ID を指定します。
通常、各 FEX に同じインターフェイス ID を使用してバーチャル ポート チャネルを形成します。
d) ドロップダウン リストから、最初の FEX プロファイルで使用したものと同じバーチャル ポート チャネル インターフェイス ポリシー グループを選択します。
バーチャル ポート チャネル インターフェイス ポリシー グループは、選択した FEX のインターフェイスに適用するポリシーのグループを指定します。インターフェイス ポリシーの例は、リンクレベル ポリシー（たとえば、1 gbit ポート速度）、接続エンティティ プロファイル、ストーム制御インターフェイス ポリシーなどです。

（注） インターフェイス ポリシー グループ内で、FEX ポート セレクタで指定されているインターフェイスを EPG が使用できるようにするために、[Attached Entity Profile] は必須です。

e) [Submit] をクリックして、更新された FEX プロファイルを APIC に送信します。
APIC が FEX プロファイルを更新します。

確認：バーチャル ポート チャネルが適切に設定されていることを確認するには、いずれかの FEX が接続されているスイッチに対して CLI コマンド **show vpc extended** を使用します。

次の作業

これで、FEX バーチャル ポート チャネルの設定手順は完了しました。

（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

トラフィック ストーム制御について

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御ポリシーを使用すると、物理インターフェイス上におけるブロードキャスト、未知のマルチキャスト、または未知のユニキャストのトラフィック ストームによって、レイヤ 2 ポート経由の通信が妨害されるのを防ぐことができます。

デフォルトでは、ストーム制御は ACI ファブリックでは有効になっていません。ACI ブリッジ ドメイン（BD）レイヤ 2 の未知のユニキャストのフラッディングは BD 内でデフォルトで有効になっていますが、管理者が無効にすることができます。その場合、ストーム制御ポリシーはブロードキャストと未知のマルチキャストのトラフィックにのみ適用されます。レイヤ 2 の未知のユニキャストのフラッディングが BD で有効になっている場合、ストーム制御ポリシーは、ブロード

キャストと未知のマルチキャストのトラフィックに加えて、レイヤ 2 の未知のユニキャストのフラッディングに適用されます。

トラフィック ストーム制御（トラフィック抑制ともいいます）を使用すると、着信するブロードキャスト、マルチキャスト、未知のユニキャストのトラフィックのレベルを 1 秒間隔でモニタできます。この間に、トラフィック レベル（ポートで使用可能な合計帯域幅のパーセンテージ、または特定のポートで許可される 1 秒あたりの最大パケット数として表されます）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。管理者は、ストーム制御しきい値を超えたときにエラーを発生させるようにモニタリング ポリシーを設定できます。

ストーム制御のガイドライン

以下のガイドラインと制約事項に従って、トラフィック ストーム制御レベルを設定してください。

- 通常、ファブリック管理者は以下のインターフェイスのファブリック アクセス ポリシーでストーム制御を設定します。
  - 標準トランク インターフェイス。
  - 単一リーフ スイッチ上のダイレクト ポート チャネル。
  - バーチャル ポート チャネル（2 つのリーフ スイッチ上のポート チャネル）。
- ポート チャネルおよびバーチャル ポート チャネルでは、ストーム制御値（1 秒あたりのパケット数またはパーセンテージ）はポート チャネルのすべての個別メンバーに適用されます。ポート チャネルのメンバーであるインターフェイスには、ストーム制御を設定しないでください。
- 使用可能な帯域幅のパーセンテージで設定する場合、値 100 はトラフィック ストーム制御を行わないことを意味し、値 0.01 はすべてのトラフィックを抑制します。
- ハードウェアの制限およびさまざまなサイズのパケットのカウント方式が原因で、レベルのパーセンテージは概数になります。着信トラフィックを構成するフレームのサイズに応じて、実際に適用されるパーセンテージ レベルと設定したパーセンテージ レベルの間には、数パーセントの誤差がある可能性があります。1 秒あたりのパケット数（PPS）の値は、256 バイトに基づいてパーセンテージに変換されます。
- 最大バーストは、通過するトラフィックがないときに許可されるレートの最大累積です。トラフィックが開始されると、最初の間隔では累積レートまでのすべてのトラフィックが許可されます。後続の間隔では、トラフィックは設定されたレートまでのみ許可されます。サポートされる最大数は 65535 KB です。設定されたレートがこの値を超えると、PPS とパーセンテージの両方についてこの値で制限されます。
- 累積可能な最大バーストは 512 MB です。
- 最適化されたマルチキャスト フラッディング（OMF）モードの出力リーフ スイッチでは、トラフィック ストーム制御は適用されません。

- OMF モードではない出力リーフ スイッチでは、トラフィック ストーム制御が適用されます。
- FEX のリーフ スイッチでは、ホスト側インターフェイスにはトラフィック ストーム制御を使用できません。

GUI を使用したトラフィック ストーム制御ポリシーの設定

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、[Access Policies] をクリックします。

ステップ 3 [Navigation] ペインで、[Interface Policies] を展開します。

ステップ 4 [Policies] を展開します。

ステップ 5 [Storm Control] を右クリックし、[Create Storm Control Interface Policy] を選択します。

ステップ 6 [Create Storm Control Interface Policy] ダイアログボックスで、[Name] フィールドにポリシーの名前を入力します。

ステップ 7 [Specify Policy In] フィールドで、[Percentage] または [Packets Per Second] いずれかのオプション ボタンをクリックします。

ステップ 8 [Percentage] を選択した場合は、次の手順を実行します。

a) [Rate] フィールドに、トラフィック レートのパーセンテージを入力します。
ポートで使用可能な合計帯域幅のパーセンテージを指定する 0 ～ 100 の数値を入力します。1 秒の間隔中に入力トラフィックがこのレベルに達すると、トラフィック ストーム制御により、その間隔の残りのトラフィックはドロップされます。値 100 は、トラフィック ストーム制御を行わないことを意味します。値 0 の場合、すべてのトラフィックが抑制されます。

b) [Max Burst Rate] フィールドに、バースト トラフィック レートのパーセンテージを入力します。
ポートで使用可能な合計帯域幅のパーセンテージを指定する 0 ～ 100 の数値を入力します。入力トラフィックがこのレベルに達すると、ストーム制御がトラフィックをドロップし始めます。

ステップ 9 [Packets Per Second] を選択した場合は、次の手順を実行します。

a) [Rate] フィールドに、トラフィック レートを 1 秒あたりのパケット数で入力します。
この間、トラフィック レベル（1 秒あたりにポートを通過するパケット数として表される）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

b) [Max Burst Rate] フィールドに、バースト トラフィック レートを 1 秒あたりのパケット数で入力します。
この間、トラフィック レベル（1 秒あたりにポートを通過するパケット数として表される）が、設定したバースト トラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

ステップ 10 [Submit] をクリックします。

ステップ 11 ストーム制御インターフェイス ポリシーをインターフェイス ポートに適用します。

a) メニュー バーで、[Fabric] をクリックします。
b) サブメニュー バーで、[Access Policies] をクリックします。
c) [Navigation] ペインで、[Interface Policies] を展開します。
d) [Policy Groups] を展開します。
e) [Policy Group] を選択します。
f) [Work] ペインで、[Storm Control Interface Policy] のドロップダウンをクリックし、作成したトラフィック ストーム制御ポリシーを選択します。
g) [Submit] をクリックします。

REST API を使用したトラフィック ストーム制御ポリシーの設定

トラフィック ストーム制御ポリシーを設定するには、希望するプロパティを使用して `stormctrl:IfPol` オブジェクトを作成します。

MyStormPolicy というポリシーを作成するには、次の HTTP POST メッセージを送信します。

```
POST https://192.0.20.123/api/mo/uni/infra/stormctrlifp-MyStormPolicy.json
```

使用可能な帯域幅のパーセンテージでポリシーを指定するには、POST メッセージの本文に次の JSON ペイロード構造を含めます。

```
{"stormctrlIfPol":
    {"attributes":
        {"dn":"uni/infra/stormctrlifp-MyStormPolicy",
        "name":"MyStormPolicy",
        "rate":"75",
        "burstRate":"85",
        "rn":"stormctrlifp-MyStormPolicy",
        "status":"created"
        },
        "children":[]
    }
}
```

1 秒あたりのパケット数でポリシーを指定するには、POST メッセージの本文に次の JSON ペイロード構造を含めます。

```
{"stormctrlIfPol":
    {"attributes":
        {"dn":"uni/infra/stormctrlifp-MyStormPolicy",
        "name":"MyStormPolicy",
        "ratePps":"12000",
        "burstPps":"15000",
        "rn":"stormctrlifp-MyStormPolicy",
        "status":"created"
        },
        "children":[]
    }
}
```

トラフィック ストーム制御インターフェイス ポリシーをインターフェイス ポートに適用します。

```
POST
http://192.0.20.123/api/node/mo/uni/infra/funcprof/accportgrp-InterfacePolicyGroup/rsstormctrlIfPol.json
```

ポリシーをインターフェイス ポリシー グループに適用するには、POST メッセージの本文に次の JSON ペイロード構造を含めます。

```
{"infraRsStormctrlIfPol":{"attributes":{"tnStormctrlIfPolName":"testStormControl"},"children":[]}}
```

CLI を使用したトラフィック ストーム制御ポリシーの設定

手順の概要

1. CLI で、ディレクトリを /storm-ctrl に変更します。
2. PPS ポリシーを作成するには、次の手順に従います。
3. パーセント ポリシーを作成するには、次の手順に従います。
4. CLI を使用して、トラフィック ストーム制御ポリシーを適用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	CLI で、ディレクトリを /storm-ctrl に変更します。 例： `cd aci/fabric/access-policies/interface-policies/policies/storm-ctrl/`	

ステップ 2	PPS ポリシーを作成するには、次の手順に従います。
	
	例：
	`> mocreate pps_10k_10k`
	`> cd pps_10k_10k/`
	`> moset rate-in-pps 10000`
	`> moset burst-rate-in-pps 10000`
	`> moconfig commit`	

ステップ 3	パーセント ポリシーを作成するには、次の手順に従います。
	
	例：
	`> cd /home/admin/aci/fabric/access-policies/interface-policies/policies/storm-ctrl`
	`> mocreate percent_50_60`
	`> cd percent_50_60/`
	`> moset rate-in-percentage 50`
	`> moset burst-rate-in-percentage 60`
	`> moconfig commit`	

ステップ 4	CLI を使用して、トラフィック ストーム制御ポリシーを適用します。
	
	例：
	`> cd`
	`/aci/fabric/access-policies/interface-policies/policy-groups/interface/InterfacePolicyGroup`	

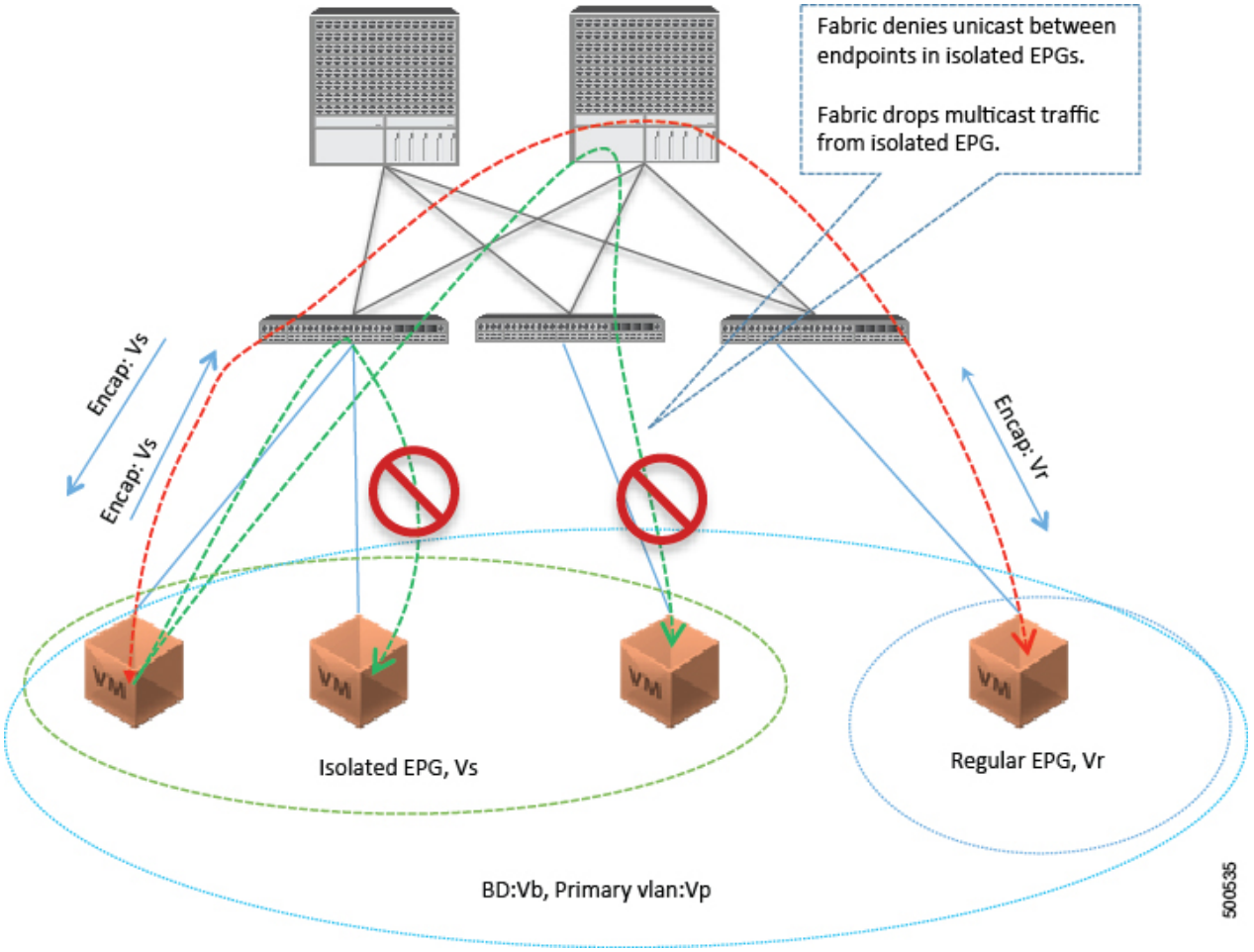
	コマンドまたはアクション	目的
	`> moset storm-control-policy MyStormPolicy` `> moconfig commit "`	

EPG 内拒否エンドポイントの分離

EPG 内拒否ポリシーにより、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。完全分離モードで稼働している EPG 内のエンドポイント間の通信は許可されません。分離モードの 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 カプセル化の数が削減されますが、相互通信は許可されません。EPG は、すべての ACI ネットワークドメインで分離されるか、またはどのドメインでも分離されません。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。

図 7: ベア メタル

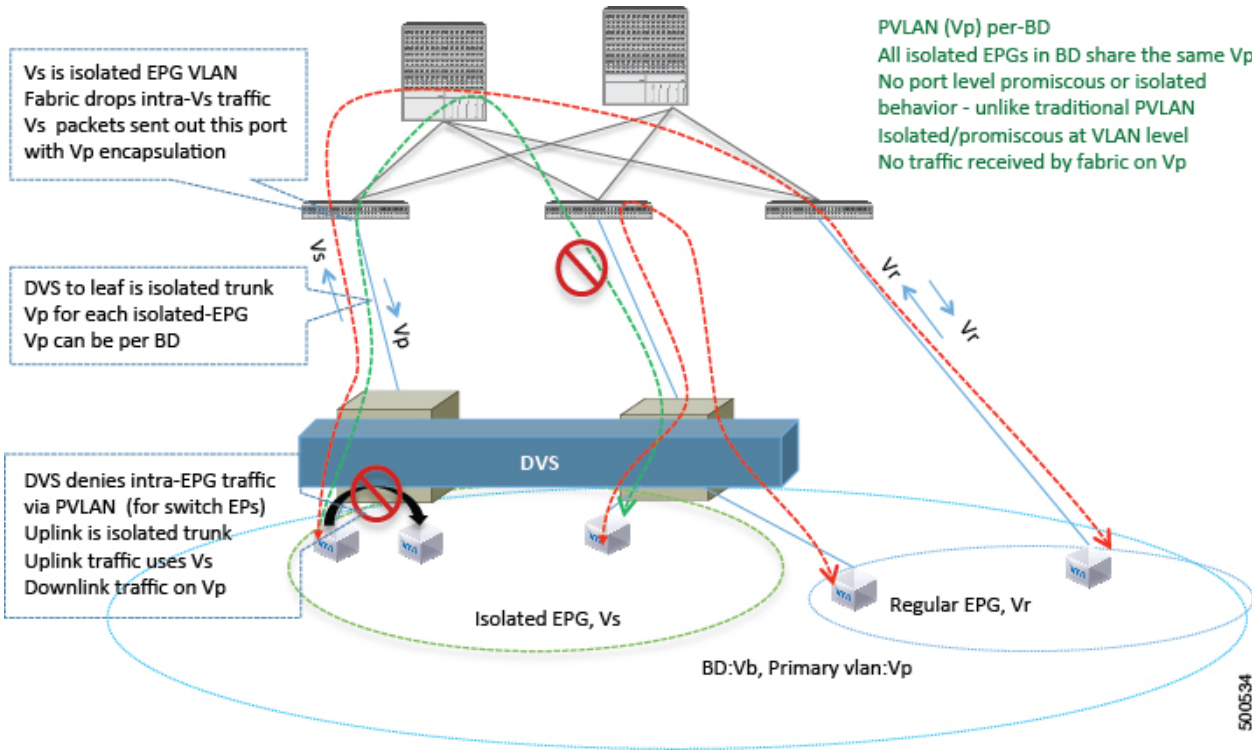


いくつかの使用例を次に示します。

- 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。

EPG 内拒否分離は、PVLAN タグに基づいて VMware Distributed Virtual Switch（DVS）導入環境に適用できます。

図 *8*：*VMware DVS*



ACI Virtual Machine Manager（VMM）ドメインは、EPG 内拒否が有効である EGP ごとに DVS に分離 PVLAN ポート グループを作成します。追加のプライマリ カプセル化を、管理者が提供するか、または EPG/VMM ドメイン間の関連付け時に動的に割り当てる必要があります。VMM は、分離されたセカンダリ（Vs）を持つプライマリ VLAN（Vp）を DVS に作成します。EPG 内拒否 EPG は、タイプを `PVLAN` に設定して Vs を使用します。ファブリックから DVS への通信では Vp が使用されます。DVS とファブリックは Vp/Vs カプセル化を交換します。Vp/Vs ペアは、EPG/ドメイン間の関連付け時に VMM ドメインごとに選択されます。ファブリック管理者が Vp と Vs の値を静的に選択するときに、VMM は、Vp と Vs がドメイン プール内の静的ブロックに含まれていること、およびそのドメイン内の他の EPG との衝突がないことを検証します。

（注） EPG 内エンドポイントの拒否分離を適用して EPG が設定されている場合、さらに 2 つの制限が適用されます。

- 分離された EPG 全体のすべてのレイヤ 2 エンドポイント通信は、ブリッジ ドメイン内にドロップされます。
- 分離された EPG 全体のすべてのレイヤ 3 エンドポイント通信は、同じサブネット内にドロップされます。

GUI を使用した EPG 内拒否 EPG の設定

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か、またはいずれかの VM マネージャ（VMM）に属している必要があります。

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. [Domains] ダイアログボックスで、次の操作を実行します。
3. [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) 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) [Step 2 for Specify the VM Domains] 領域で、[Associate VM Domain Profiles] を展開し、ドロップダウン リストから目的の VMM ドメインを選択します。[Update] をクリックし、[OK] をクリックします。

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

a) ベア メタルの場合、[Domain Profile] フィールドで、ドロップダウン リストからドメイン プロファイルを選択します（VMwarePVLAN）。

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（vlan-2005）を指定し、[Primary VLAN for Micro-Seg] フィールドで、プライマリ VLAN（vlan-2006）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。

b) VMware DVS の場合、[Domain Profile] フィールドで、ドロップダウン リストからドメイン プロファイルを選択します（VMwareDVS）。

c) [Next] をクリックします。

ステップ 3 [Leaves/Paths] ダイアログボックスで、次の操作を実行します。

a) ベア メタルの場合、[Path] セクションで、ドロップダウン リストからトランク モードでのパスを選択します（Node-107/eth1/16）。
セカンダリ VLAN の [Port Encap]（vlan-102）を指定します。

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

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

c) [Update] をクリックします。

d) [Finish] をクリックします。

NX-OS スタイルの CLI を使用した EPG 内拒否 EPG の設定

手順の概要

1. CLI で、EPG 内拒否 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	CLI で、EPG 内拒否 EPG を作成します。
	
	例：
	以下に、VMM ケースを示します。
	`ifav19-ifc1(config)# tenant SCVMMTenant`
	`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 SCVMMTenant`
	`  application PVLAN epg EPG1`	

	コマンドまたはアクション	目的

```
  tenant SCVMMTenant
     application PVLAN
      epg EPG1
        bridge-domain member VMM_BD
        contract consumer SCVMM-Ext
        contract consumer default
        contract provider Deny_EPG
        vmware-domain member PVLAN encap vlan-2002 primary-encap vlan-2001 push on-demand <---
Assigns static primary & secondary encap to EPG.
        vmware-domain member mininet  <--- If no static vlan assigned APIC assigns primary &
secondary encap for isolated EPG.
        isolation enforce   <---- This enables EPG into isolation mode.
        exit
    exit
exit
```

例：
スタティック バインディング EPG -> Tenant:Tenant_BareMetal -> Application: PVLAN -> Static を関連付けるには、次のようにします。

```
ifav19-ifc1(config)#
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 SCVMMTenant application
PVLAN epg StaticEPG primary-vlan 100
```

ステップ 2 設定を確認します。

例：

```
 show epg StaticEPG detail
Application EPg Data:
Tenant               : SCVMMTenant
Application          : PVLAN
AEPg                 : StaticEPG
BD                   : VMM_BD
uSeg EPG             : no
Intra EPG Isolation  : enforced
Vlan Domains         : phys
Consumed Contracts   : SCVMM-Ext
Provided Contracts   : default,Deny_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
 ----------  ------------------------------  ----------------  ------------------------------
```

	コマンドまたはアクション	目的
	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 EPG 内拒否 EPG の設定

はじめる前に

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か、またはいずれかの VM マネージャ（VMM）に属し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. ベア メタル展開では、POST メッセージの本文にこの XML 構造を含めます。
3. VMM 展開では、POST メッセージの本文にこの XML 構造を含めます。

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://192.0.20.123/api/mo/uni/tn-ExampleCorp.xml
```

ステップ 2 ベア メタル展開では、POST メッセージの本文にこの XML 構造を含めます。

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>
```

ステップ 3 VMM 展開では、POST メッセージの本文にこの XML 構造を含めます。

例：

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