EPG 内分離の適用と Cisco ACI

この章は、次の内容で構成されています。

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   :::   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
          sclassprio:               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）

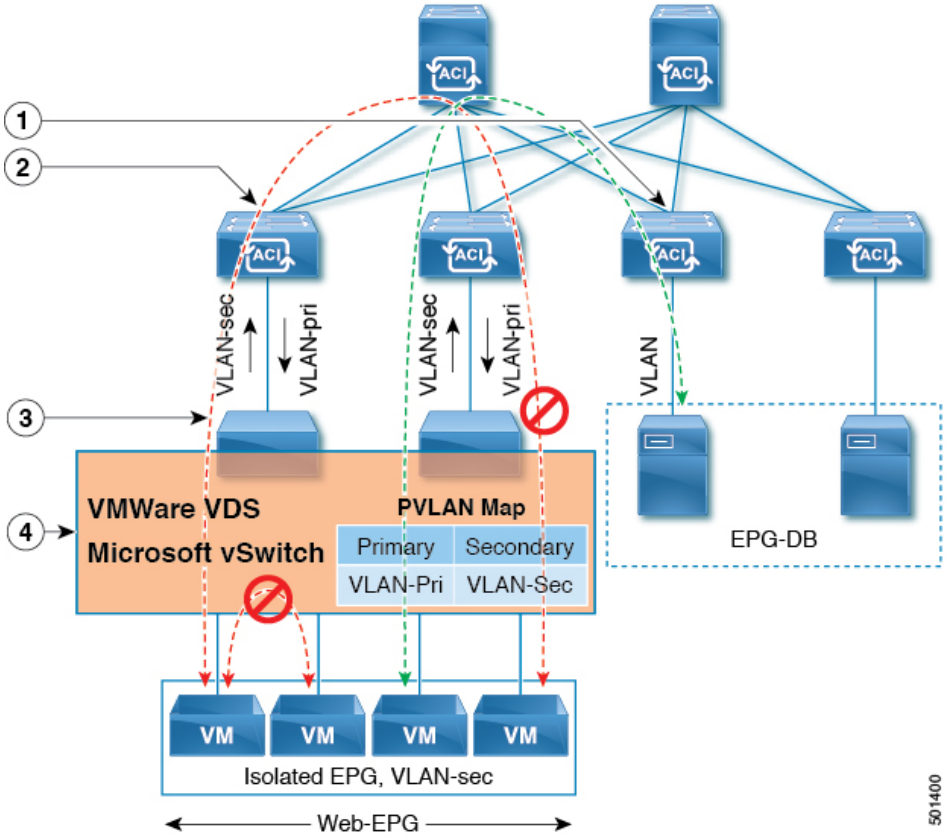
- イントラ EPG 隔離が強制されない場合、設定で指定されていても VLAN-pri 値は無視されます。
- EDM UCSM 統合を使用した VMware 分散仮想スイッチ（DVS）ドメインが失敗することがあります。ドメインに接続されているエンドポイントグループ（EPG）でEPG内分離を設定し、プライベート VLAN をサポートしない UCSM Mini 6324 を使用すると、ドメインに障害が発生します。

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 *1 : 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。

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

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。

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。