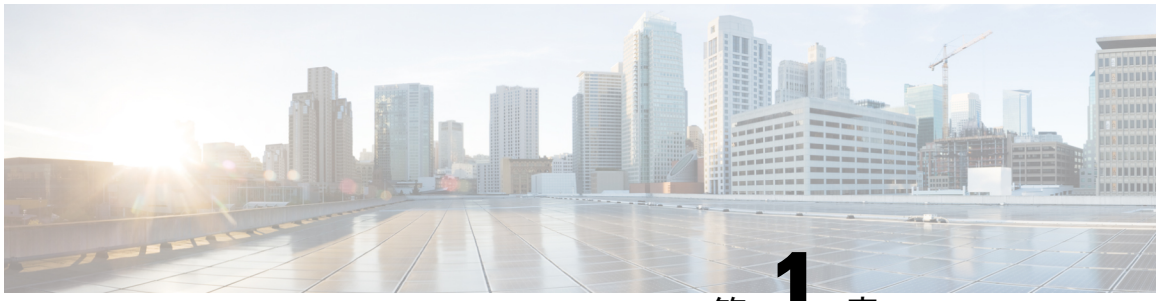
# Cisco ACI Virtual Edge リリース 2.0(2) コンフィギュレーションガイド

**初版**：2018 年 12 月 20 日

**シスコシステムズ合同会社**
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

# 目 次



第 1 章

# 新機能および変更された機能に関する情報

この章の内容は、次のとおりです。

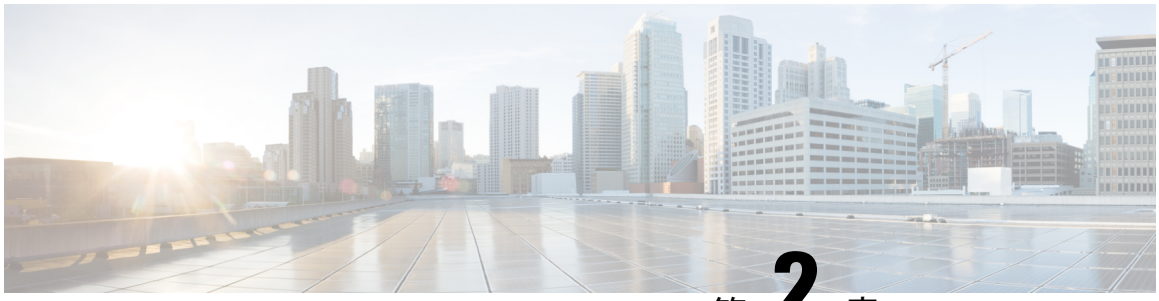


## 新機能および変更された機能に関する情報

次の表は、この Cisco Application Centric Infrastructure Virtual Edge の最新リリースまでにガイドに加えられた主な変更点の概要を示したものです。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

新機能および変更された機能に関する情報

| **Cisco Application Centric Infrastructure Virtual Edge** リリース | 機能 | 説明 | 参照先 |
|---|---|---|---|
| Cisco ACI Virtual Edge リリース 2.0(2)。 | Cisco Application Centric Infrastructure Virtual Edge（Cisco Application Centric Infrastructure (ACI) 仮想ポッド(vPod)の一部として）。<br>（注） Cisco ACI vPod は、Cisco APIC リリース 4.0(2) で一般に利用可能です。 | Cisco ACI vPod は、ベア メタル クラウドやその他のリモート ロケーションに Cisco ACI ファブリックを拡張できるようにする、ソフトウェアのみのソリューションです。<br>Cisco ACI vPod により、物理リーフがない場所で Cisco ACI Virtual Edge を使用できるようになります。Cisco ACI Virtual Edge を vCenter ドメインに展開する場合、Cisco ACI vPod の一部にするかどうかを VMware vCenter で指定する必要があります。 | • *Cisco ACI* 仮想ポッド リリース ノート<br>• *Cisco ACI* 仮想ポッドインストレーション ガイド<br>• *Cisco ACI* 仮想ポッド スタートアップ ガイド |



第 2 章

# Cisco ACI Virtual Edge の概要

この章の内容は、次のとおりです。



## About Cisco ACI Virtual Edge

Cisco APIC リリース 3.1(1) 以降では、シスコ アプリケーション セントリック インフラストラクチャは Cisco ACI 仮想エッジをサポートします。Cisco ACI 仮想エッジは、Cisco ACI 環境向けの次世代アプリケーション仮想スイッチ (AVS) です。Cisco ACI 仮想エッジはハイパーバイザに依存しない分散サービス VM で、ハイパーバイザに属しているネイティブな分散仮想スイッチを利用します。Cisco ACI Virtual Edge はユーザスペースで動作し、仮想リーフとして機能し、Cisco Application Policy Infrastructure Controller（APIC）によって管理されます。

Cisco AVS を使用する場合には、Cisco ACI Virtual Edge に移行することができます。VMware VDS を使用する場合には、その上で Cisco ACI Virtual Edge を実行できます。Cisco ACI Virtual Edge をカーネル スペースから分離したため、ソリューションはさまざまなハイパーバイザに適応できます。また、単純なアップグレードも容易になります。Cisco ACI Virtual Edge はハイパーバイザ アップグレードに関連付けられていないからです。Cisco ACI 仮想エッジでは、コントロールプレーンの通信に OpFlex プロトコルを実装しています。トラフィックの転送では、ローカルスイッチングおよびローカルスイッチングなしの 2 つのモードをサポートしています。

Cisco ACI Virtual Edge リリース 1.1(1a) は、VMware ハイパーバイザのみをサポートしています。これは、プライベート VLAN (PVLAN) モードで設定された vSphere 分散スイッチ (VDS) を活用します。

ネットワーク管理者が Cisco APIC 上で Cisco ACI Virtual Edge VMM ドメインを作成する場合には、ドメインを、DVS 上のポート グループの PVLAN ペア関連付けで使用される一定範囲の VLAN に関連付ける必要があります。サーバ管理者の場合は、PVLAN をvCenter のポート グループに関連付ける必要はありません。Cisco APIC が自動的に PVLAN ペアをエンドポイント グループ (EPG) に関連付けるからです。

（注） Cisco APIC の EPG は、vCenter のポート グループに相当します。

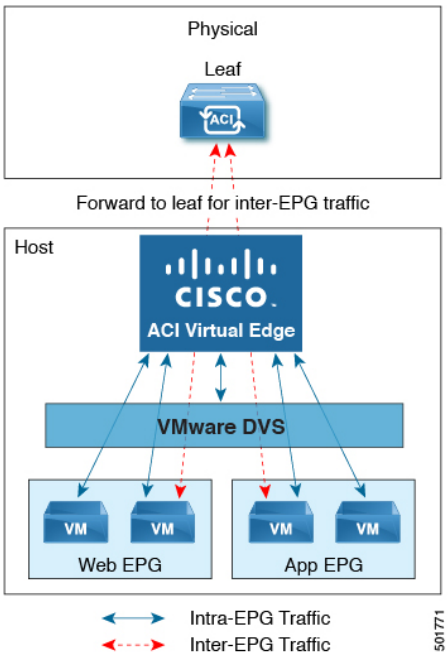
### ローカル スイッチング モード

ローカル スイッチング モードでは、Cisco ACI Virtual Edge は、EPG 内のすべてのトラフィックをリーフを経由せずローカルに転送します。すべての EPG 間トラフィックはリーフを通じて転送されます。このモードでは、Cisco ACI Virtual Edge は VLAN または VXLAN カプセル化、あるいはその両方を使用してトラフィックをリーフとバックに転送できます。カプセル化のタイプは、Cisco ACI Virtual Edge VMM ドメインの作成時に選択できます。

単一の VMM ドメインは、ローカル スイッチング モードで VLAN と VXLAN カプセル化を使用するように設定できます。

VLAN カプセル化を選択する場合は、一連の VLAN の範囲が Cisco ACI 仮想エッジによって使用可能である必要があります。これらの VLAN には、Cisco ACI Virtual Edge とリーフ間のレイヤ 2 ネットワーク内でのみ意味があるローカル スコープがあります。VXLAN カプセル化を選択する場合は、Cisco ACI Virtual Edge とリーフの間で使用できる必要があるのはインフラ VLAN のみです。これにより、設定が簡素化されます。Cisco ACI Virtual Edge と物理リーフ間に 1 つ以上のスイッチがある場合に推奨されるカプセル化タイプです。

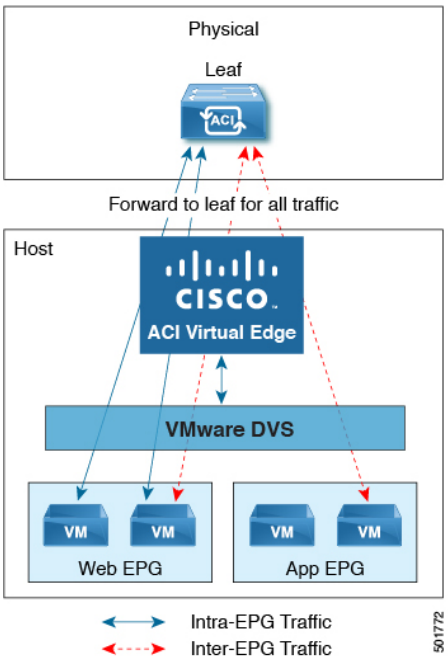
**図 *1*: ローカル スイッチング モードの *Cisco ACI Virtual Edge***




### ローカル スイッチング モードなし

ローカル スイッチング モードなしの場合、リーフはすべてのトラフィックを転送します。このモードでは、VXLAN が唯一許可されるカプセル化タイプです。

図 *2 :* ローカル スイッチングなしモードの *Cisco ACI Virtual Edge*




### Statistics Collection

Cisco ACI Virtual Edge での統計収集はデフォルトで有効になっています。Cisco APIC GUI 内では、VM リソースの使用に関連して Cisco ACI Virtual Edge の障害が出る場合があります。

これらの障害のトラブルシューティングは VMware vCenter で行ってください。Cisco ACI はこれらの障害を VMware vCenter から受信した情報だけに基づいて生成するからです。

# Cisco ACI Virtual Edge および VMware vCenter について

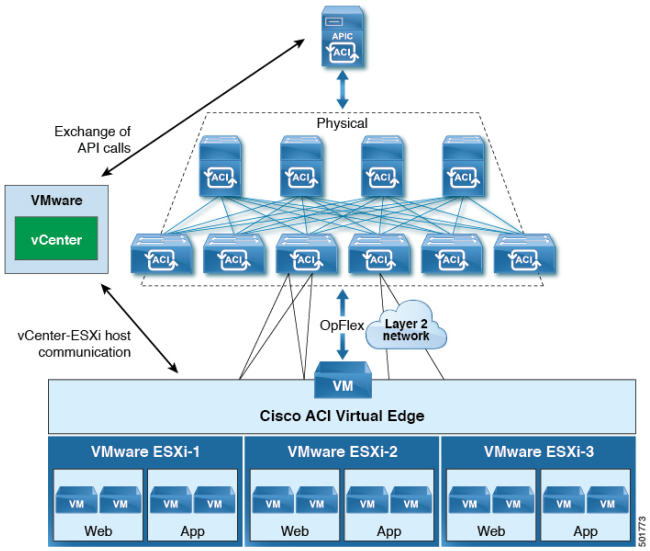
Cisco ACI Virtual Edge は、多数の仮想ホストにまたがって広がる分散仮想スイッチです。vCenter Server により定義されるデータセンターを管理します。

Cisco ACI Virtual Edge は、Cisco Nexus スイッチなどの、イーサネット標準準拠のアップストリーム物理アクセス レイヤ スイッチと互換性があります。Cisco ACI Virtual Edge は *VMware Hardware Compatibility List*（HCL）に記載されているすべてのサーバ ハードウェアと互換性があります。

Cisco ACI Virtual Edge は、VMware 仮想インフラストラクチャ内に完全に統合される、分散仮想スイッチ ソリューションです。このインフラストラクチャには、仮想化管理者のための VMware vCenter も含まれます。このソリューションにより、ネットワーク管理者は一貫したデータセンター ネットワーク ポリシーを確立するために仮想スイッチやポート グループを設定することができます。

次の図は、Cisco ACI Virtual Edge と Cisco APIC および VMware vCenter を含むトポロジを示しています。

図 *3 : Cisco ACI Virtual Edge* トポロジの例




（注） 1 つの Cisco ACI ファブリックに接続された複数の vCenters がある場合、デフォルトの OUI 割り当てではなく vCenters を展開する際には、複数の vCenters にわたる MAC アドレス割り当てスキーマにオーバーラップがないことを確認してください。オーバーラップがあると、重複した MAC アドレスが生成される可能性があります。詳細については、VMware のマニュアルを参照してください。

# マルチポッド環境での Cisco ACI Virtual Edge

Cisco ACI Virtual Edge はマルチポッド環境の一部である可能性があります。マルチポッド環境はすべてのポッドに単一の Cisco APIC クラスタを使用します。そのため、すべてのポッドが単一のファブリックとして機能します。

マルチポッド環境は、独立した制御プレーンプロトコルを有する複数のポッドで構成された、障害耐性の高いファブリックのプロビジョニングを可能にします。また、リーフスイッチとスパイン スイッチ間のフルメッシュケーブル配線にも柔軟性があります。

Cisco ACI Virtual Edge はマルチポッド環境で動作するための追加の設定を必要としません。

マルチコード環境の詳細については、Cisco.com の次のマニュアルを参照してください。

- 『*Cisco Application Centric Infrastructure Fundamentals*』
- 『*Cisco APIC Getting Started Guide*』
- 『*Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*』

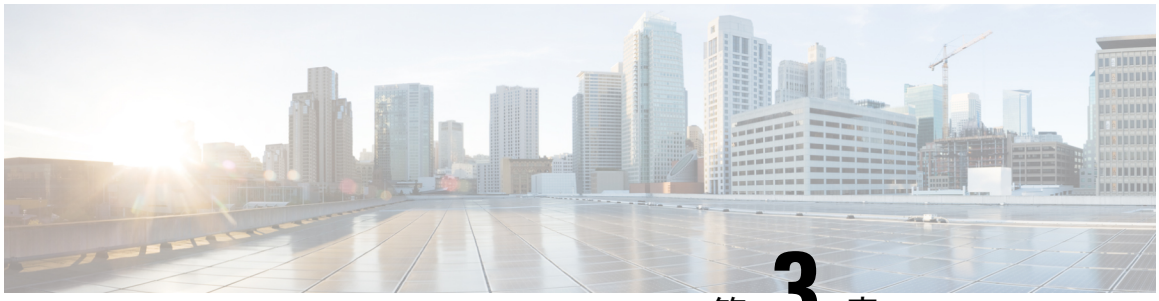
次の機能は、Cisco APIC リリース 3.1(1) ～ 4.0(1) のマルチポッドを使用した Cisco ACI Virtual Edge ではサポートされていません。

- L3 マルチキャスト
- 2 つの個別の POD に 2 つの個別の NFS を搭載したストレージ vMotion
- 異なる POD の ERSPAN 宛先
- 異なる POD の分散型ファイアウォール syslog サーバ

# 必要なソフトウェア

次の表に必要なソフトウェアのバージョンを示しています Cisco ACI Virtual Edge Cisco APIC、VMware vCenter と VMware ESXi ハイパーバイザで動作します。

| コンポーネント | 説明 |
|---|---|
| Cisco ACI Virtual Edge ソフトウェア | Cisco ACI Virtual Edge リリース 1.1(1) で始まるはサポートされています。 |
| Cisco APIC | Cisco ACI Virtual Edge Cisco APIC リリース 3.1 (1) 以降でサポートされます。 |
| VMware vCenter | Cisco ACI Virtual Edge は、VMware vCenter サーバのリリース 6.0 以降と互換性があります。 |
| VMware vSphere のベア メタル | Cisco ACI Virtual Edge は、VMware ESXi ハイパーバイザのリリース 6.0 以降で、Cisco APIC 用の vLeaf としてサポートされます。 |



第 3 章

# VXLAN ロード バランシング



# VXLAN ロード バランシング

仮想拡張 LAN（VXLAN）ロード バランシングにより、次の両方の状況で、Cisco Application Centric Infrastructure Virtual Edge とリーフ スイッチの間で複数のネットワーク インターフェイスを介してデータが効率的に移動することが保証されます。

- MAC 固定ポリシーを設定していて、VXLAN カプセル化を使用している場合
- Cisco Application Policy Infrastructure Controller（APIC）内の Cisco ACI Virtual Edge 仮想マシン マネージャ（VMM）ドメインで MAC 固定ポリシーと VXLAN カプセル化を有効にしている場合

この Cisco ACI Virtual Edge のリリース以降、VXLAN ロード バランシングはデフォルトで有効になっています。この Cisco ACI Virtual Edge のリリースでは、VXLAN ロード バランシングに対応し、全体的なパフォーマンスを向上させるためのインターフェイスが追加されています。

（注） Cisco ACI Virtual Edge が Cisco ACI 仮想ポッドの一部となっている場合（vPod モード）、Cisco ACI Virtual Edge では VXLAN ロード バランシングはサポートされません。

以前のリリースの Cisco ACI Virtual Edge には、管理用に 1 つ、内部用に 1 つ、外部用に 1 つという 3 つのインターフェイスがありました。VMware vCenter では、**internal** と **external** という 2 つのポート グループがありましたが、現在 Cisco ACI Virtual Edge では次のようになりました。

- 2 つの内部インターフェイス：仮想マシン（VM）からのデータ トラフィックを処理します。プライベート VLAN（PVLAN）からのトラフィックは、VMware vCenter の 2 つの新しい内部ポート グループである **ave-internal-1** と **ave-internal-2** の間で均等に分割されます。

- 2 つの外部 VXLAN インターフェイス：VXLAN トラフィックのロード バランシングを行います。VMware vCenter で、**ave-external-vxlan-1** と **ave-external-vxlan-2** の 2 つの新しいポート グループが、インターフェイスごとに 1 つずつあります。OpFlex で使用されるインフラ VLAN でも、これら 2 つの外部 VXLAN インターフェイスを使用します。
- 1 つの外部 VLAN インターフェイス：インフラ VLAN を除くすべての VLAN タグ付きトラフィックを処理します。**ave-external-vlan** という独自の VMware vCenter ポート グループがあります。このグループでは、VMM の構成に基づくすべての Cisco ACI ファブリック VLAN の使用が可能です。
- 管理インターフェイス：以前のリリースから変更されていません。
- 2 つの仮想トンネル エンドポイント（VTEP）（kni インターフェイス）が自動的に作成され、それぞれの external-vxlan インターフェイスに固定されます。

（注） 新しい VMware vCenter ポート グループの名前は自動的に割り当てられます。**ave-** で始まるこれらの新しいポート グループをテナント トラフィックで使用しないでください。

VMware vCenter には引き続き、**internal** および **external** のポート グループが存在しています。これらのポート グループは、Cisco ACI vPod に対応するため、およびアップグレードとダウングレードの互換性を保つために残されています。

# VXLAN ロード バランシングの確認

VXLAN ロードバランシングが有効になっていることを確認するには、Cisco Application Centric Infrastructure Virtual Edge が DHCP IP アドレスを受信したかどうか、および OpFlex が稼働しているかどうかを確認します。

Cisco ACI Virtual Edge が DHCP アドレスを受信したかどうかを確認するには、**ifconfig** コマンドを実行してカーネル NIC の情報を表示します。OpFlex が稼働しているかどうかを確認するには、**vemcmd opflex show** コマンドを実行します。

## カーネル NIC 情報の表示

カーネル NIC の情報を表示することができます。

**手順**

コマンド **ifconfig kni0** および **ifconfig kni2** を入力し、kni0 と kni2 に IP アドレスが割り当てられているかどうかを確認します。

**例**：

```
cisco-ave_198.51.100.62_AVE-FI:~$ ifconfig kni0
kni0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 198.51.100.111 netmask 255.255.0.0 broadcast 198.51.100.255
      inet6 fe80::250:56ff:feaf:807b prefixlen 64 scopeid 0x20<link>
```

```
      ether 00:50:56:af:80:7b txqueuelen 1000 (Ethernet)
      RX packets 528552 bytes 50610919 (48.2 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 285294 bytes 44487029 (42.4 MiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
cisco-ave_198.51.100.62_AVE-FI:~$ ifconfig kni2

kni2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 198.51.100.121 netmask 255.255.0.0 broadcast 198.51.100.255
      inet6 fe80::250:56ff:feaf:3dc9 prefixlen 64 scopeid 0x20<link>
      ether 00:50:56:af:3d:c9 txqueuelen 1000 (Ethernet)
      RX packets 285152 bytes 17116682 (16.3 MiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 10873 bytes 2921194 (2.7 MiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
cisco-ave_198.51.100.62_AVE-FI:~$
```

出力には、2 つの仮想 TEP の内部アップリンクに関する情報が表示されます。

（注） **ifconfig** コマンドを入力して、インターフェイスの詳細な情報を表示できます。たとえば、`ens160`、管理インターフェイス、`kni1`、vMotion の `ave-ctrl` インターフェイスに関する情報を表示できます。

## OpFlex 情報の表示

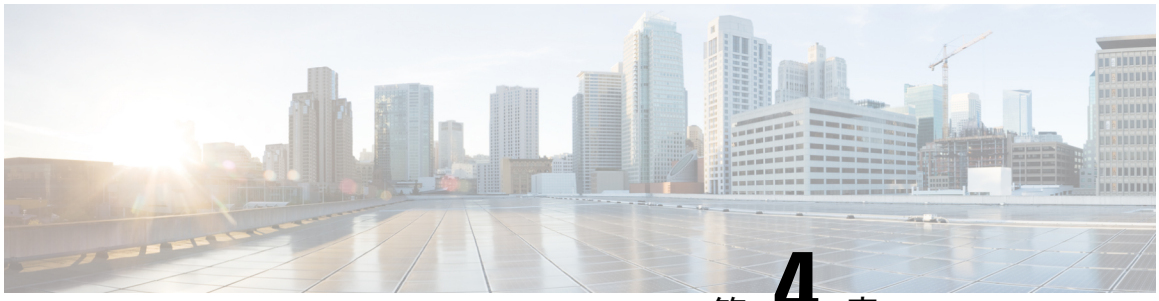
OpFlex がオンラインかどうかを確認し、そのランタイム ステータスを表示できます。

### 手順

コマンド **vemcmd show opflex** を入力します。

**例：**

```
cisco-ave_198.51.100.62_AVE-FI:~$ vemcmd show opflex
Status: 12 (Active)
Channel0: 12 (Active), Channel1: 12 (Active)
Dvs name: comp/prov-VMware/ctrlr-[AVE-FI]-vC-191/sw-dvs-413
Remote IP: 192.0.2.11 Port: 8000
Infra vlan: 5
FTEP IP: 192.0.2.20
Switching Mode: LS
Encap Type: VXLAN
NS GIPO: 225.10.10.1
cisco-ave_198.51.100.62_AVE-FI:~$
```



第 4 章

# 混合モードのカプセル化

この章の内容は、次のとおりです。



## 混合モードのカプセル化の設定

1 つの VMM ドメインで、VLAN と VXLAN のカプセル化を使用するように設定することができます。混合モードのカプセル化を使用すると、カプセル化モードに関係なく、すべての EPG に対応した単一のドメインを実現できます。これにより、EPG の追跡と管理が容易になります。

VMM ドメインを作成する際には、そのカプセル化モードとして、明示的に VLAN または VXLAN を選択することができます。

VMM ドメインのために新しい EPG を作成する際、ドメインの各 EPG は、デフォルトで VMM ドメインのカプセル化モードを使用します。ただし、新しい EPG を作成してそれをドメインに関連付ける場合には、EPG がドメインのカプセル化モードをオーバーライドし、別のモードを使用するように設定できます。

たとえば、VMM ドメインを作成する際に、VLAN の設定を選択することができます。ドメインのために新しい EPG を作成する際には、ドメインのモードして VLAN を使用するようを設定することができますし、または VXLAN を使用するように設定することもできます。

（注） 混合モードのカプセル化を使用するには、VXLAN プールと VLAN プールの両方を設定して VMM ドメインに割り当てる必要があります。

混合モードのカプセル化は、ローカル スイッチング モードの Cisco ACI Virtual Edge でのみ利用できます。

### カプセル化プールの組み合わせ

VMM ドメインに対して VLAN およびマルチキャスト プールの追加や削除を行えるかどうかは、そのドメインに EPG が関連付けられているかどうかに左右されます。

EPG が VMM ドメインに関連付けられていない場合は、VLAN とマルチキャスト プールの追加や削除が行えます。このことはこれは、VMM ドメインのデフォルトのカプセル化モードが VLAN と VXLAN のどちらであっても可能です。

EPG が VMM ドメインに関連付けられている場合は、既存の VLAN やマルチキャスト プールを削除することはできません。

- VLAN： VLAN およびマルチキャスト プールの両方を設定することができます。

  VLAN がドメインのデフォルトのカプセル化モードとなります。この VMM ドメイン用に新しく作成される EPG では、デフォルトで VLAN カプセル化が使用されます。VMM ドメインでマルチキャスト プールが設定されている場合、VXLAN カプセル化を使用するように EPG を設定することができます。

  （注） 内部スイッチングの VLAN プールで内部としてプライベート VLAN を設定します。内部スイッチング用に使用する VLAN プールは Cisco ACI Virtual Edge でのみ使用され、中継ネットワーク インターフェイスでの使用を許可する必要はありません。

- VXLAN： VLAN およびマルチキャスト プールの両方を設定することができます。VXLAN がドメインのデフォルトのカプセル化モードとなります。VMM ドメイン用に新しく作成される EPG では、デフォルトで VXLAN カプセル化が使用されます。VMM ドメインで VLAN プールが設定されている場合は、EPG を VLAN カプセル化を使用するように設定することができます。

# APIC GUI を使用した VMM ドメイン カプセル化モードの確認または変更

APIC GUI を使用して、VMM ドメイン カプセル化モードを確認または変更することができます。

（注） EPG が VMM ドメインに関連付けられている場合は、そのスイッチング モードを変更することはできません。ドメインで別のスイッチングモードを使用する必要がある場合には、いったん削除してから再作成してください。ただし、関連付けられている EPG がない場合は、VMM ドメインのスイッチング モードを変更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** **[Virtual Networking]** > **[Inventory]** > **[VMM Domains]** > **[VMware]** > ***[VMM domain]*** に移動します。

VMM ドメインの作業ウィンドウの [Properties] エリアでは、[Default Encapsulation Mode] フィールドの [VLAN] または [VXLAN] が青色でハイライトされています。

**ステップ 3** [Default Encapsulation Mode] で必要なモードをクリックして、モードを変更します。

**ステップ 4** 必要に応じて、作業ウィンドウで VLAN またはマルチキャスト プールを設定します。

デフォルトモードを [VLAN] に変更する場合には、VLANプールを設定する必要があります。デフォルトモードを [VXLAN] に変更する場合には、マルチキャストアドレスとマルチキャスト プールを設定する必要があります。

（注） VLAN と VXLAN のどちらでも、すでに行っていなければ、内部 VLAN プールをプライベート VLAN 用に設定します。これは内部スイッチングに使用されます。

**ステップ 5** [Submit] をクリックします。

# NX-OS CLI を使用して VMM ドメインのカプセル化モードを確認または変更する

NX-OS CLI を使用して、VMM ドメインのカプセル化モードを確認または変更できます。

（注） EPG が VMM ドメインに関連付けられている場合は、そのスイッチング モードを変更することはできません。ドメインで別のスイッチングモードを使用する必要がある場合には、いったん削除してから再作成してください。ただし、関連付けられている EPG がない場合は、VMM ドメインのスイッチング モードを変更することができます。

手順

ステップ 1 VMM ドメインのカプセル化モードを確認します。

例：

```
apic1(config-vmware-ave)# show run
# Command: show running-config vmware-domain mininet1 configure-ave
# Time: Tue Nov 21 07:07:58 2017
  vmware-domain mininet1
    configure-ave
      switching mode vlan
      multicast-address 230.1.2.3
      exit
    exit
apic1(config-vmware-ave)#
```

ステップ 2 VMM ドメインのカプセル化モードを変更します。

例：

```
apic1# configure
apic1(config)# vmware-domain mininet
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# switching mode ?
 vlan      VLAN/SW Mode
 vxlan     VXLAN/SW Mode
 vxlan-ns  VXLAN/HW Mode
```

# REST API を使用した VMM ドメインのカプセル化モードの確認または変更

REST API を使用して、VMM ドメインの検出と変更を行うことができます。

（注） EPG が VMM ドメインに関連付けられている場合は、そのスイッチング モードを変更することはできません。ドメインで別のスイッチング モードを使用する必要がある場合には、いったん削除してから再作成してください。ただし、関連付けられている EPG がない場合は、VMM ドメインのスイッチング モードを変更することができます。

手順

VMM ドメインのカプセル化モードの検出と変更

例：

```
<vmmProvP vendor="VMware">
    <vmmDomP name="mininet" enableAVE="true" enfPref="sw" mcastAddr="225.1.1.1"
```

```
encapMode="vxlan" prefEncapMode="vxlan">
</vmmProvP>
```

# APIC GUI を使用した EPG の VMM ドメイン カプセル化モードのオーバーライド

EPG を作成して VMM ドメインに関連付けた後、EPG のカプセル化モードを変更することができます。VMM ドメインとは別のカプセル化モードまたは同じカプセル化モードにできます。

### 始める前に

EPG がすでに作成されており、VMM ドメインに関連付けられている必要があります。

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** **[テナント]** > ***tenant*** > **[アプリケーション プロファイル]** > ***application profile*** > **[アプリケーション EPG]** > ***EPG*** > **[ドメイン（VM およびベア メタル]**.に進みます。

**ステップ 3** **[ドメイン（VM およびベア メタル）]** 作業ウィンドウで、ドメインをダブルクリックして、スイッチング モードが **[AVE]** になっていることを確認し、**[Encap モード]** ドロップダウン リストからモードを選択します。

次のいずれかのカプセル化モードを選択できます。

- **VXLAN**：これはドメインの VLAN 設定より優先され、EPG は VXLAN のカプセル化を使用することになります。ただし、ドメインでマルチキャスト プールが設定されていない場合は、EPG に対してエラーがトリガされます。
- **VLAN**：これはドメインのVXLAN 設定より優先され、EPG は VLAN のカプセル化を使用することになります。ただし、ドメインで VLAN プールが設定されていない場合は、EPG に対してエラーがトリガーされます。
- **Auto**1： EPG は、VMM ドメインと同じカプセル化モードを使用します。これはデフォルトの設定です。

**ステップ 4** [Update] をクリックします。

### 次のタスク

EPG カプセル化モードの EPG でエンドポイントをチェックして、設定を確認します。

# NX-OS スタイルの CLI を使用した EPG の VMM ドメイン カプセル化モードのオーバーライド

EPG を作成して VMM ドメインに関連付けた後 EPG のカプセル化モードを変更できるため、VMM ドメインカプセル化モードと同じ場合も、異なる場合もあります。

### 始める前に

EPG がすでに作成されており、VMM ドメインに関連付けられている必要があります。

### 手順

EPG のカプセル化モードを指定します。

例：

```
apic1(config)# tenant <tenant name>
apic1(config-tenant)# application <application name>
apic1(config-tenant-app)# epg <epg name>conf
apic1(config-tenant-app-epg)# vmware-domain member <vmm domain name>
apic1(config-tenant-app-epg-domain)# encap-mode auto | vlan | vxlan
apic1(config-tenant-app-epg-domain)# switching-mode AVE
```

次のいずれかのカプセル化モードを選択できます。

- **Auto** — EPG は、VMM ドメインと同じカプセル化モードを使用します。これはデフォルトの設定です。
- [VLAN]：これはドメインの VXLAN 設定より優先され、EPG は VLAN のカプセル化を使用することになります。ただし、ドメインで VLAN プールが設定されていない場合は、EPG に対してエラーがトリガーされます。
- [VXLAN]：これはドメインの VLAN 設定より優先され、EPG は VXLAN のカプセル化を使用することになります。ただし、ドメインでマルチキャストプールが設定されていない場合は、EPG に対してエラーがトリガーされます。

# REST API を使用した EPG の VMM ドメインカプセル化モードのオーバーライド

### 手順

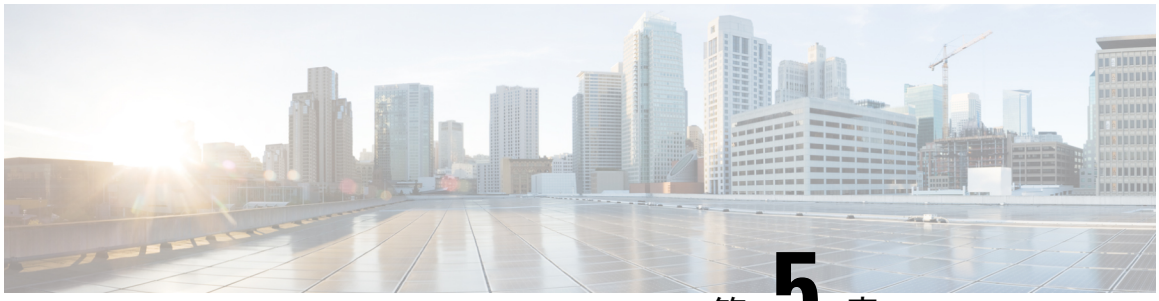
EPG の VMM ドメインのカプセル化モードをオーバーライドします。

例：

```
<polUni>
<fvTenant name="coke">
<fvAp name="sap">
<fvAEPg name="web1">
<fvRsDomAtt resImedcy="immediate"
tDn="uni/vmmp-VMware/dom-mininet"
switchingMode="AVE" encapMode="vxlan"/>
</fvAEPg>
</fvAp>
</fvTenant>
</polUni>
```

**encapMode=** では、次のいずれかを入力できます。

- **auto**—EPG は VMM ドメインと同じカプセル化モードを使用します。これはデフォルトの設定です。
- **Vlan**—ドメインの VXLAN 設定より優先され、EPG は VLAN のカプセル化を使用することになります。ただし、ドメインで VLAN プールが設定されていない場合は、EPG に対してエラーがトリガーされます。
- **Vxlan**—ドメインの VLAN 設定より優先され、EPG は VXLAN のカプセル化を使用することになります。ただし、ドメインでマルチキャスト プールが設定されていない場合は、EPG に対してエラーがトリガーされます。



第 5 章

# ポート チャネルと仮想ポート チャネルの構成

この章の内容は、次のとおりです。



## ポート チャネルまたは仮想ポート チャネルの設定

Cisco APIC GUI、NX-OS スタイル CLI、または REST APIを使用して、ポート チャネルまたは仮想ポート チャネルまたはポート チャネル ポリシーを設定することができます。

## GUI を使用したポート チャネルまたは仮想ポート チャネルの設定

ポート チャネルまたは仮想ポート チャネルを設定するには、Cisco APIC GUI を使用します。

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** [Fabric] > [Access Policies] を選択します。

**ステップ 3** **Interface** および **Leaf Interfaces** フォルダを展開します。

**ステップ 4** **Profiles** フォルダを右クリックし、**Create Leaf Interface Profile** を選択します。

**ステップ 5** **Create Leaf 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 6** **Interface Selectors** エリアで、+ をクリックして、アクセス ポート セレクタを追加します。

**ステップ 7** [Create Access Port Selector] ダイアログボックスで、次の手順を実行します。

a) [Name] フィールドにアクセス ポートの名前を入力します。

b) [Interface IDs] フィールドに、ホストが配置されているインターフェイス ID を入力します。

c) [Interface Policy Group] ドロップダウン リストから、[Create PC Interface Policy Group] または [Create VPC Interface Policy Group] を選択します。

**ステップ 8** **Create PC Interface Policy Group** ダイアログボックスまたは **reate VPC Interface Policy Group** 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、ポート チャネルの名前を入力します。

b) **Port Channel Policy** ドロップで、**Create Port Channel Policy** を選択します。

**ステップ 9** [Create Port Channel Policy] ダイアログボックスで、次のアクションを完了します。

a) [Name] フィールドにポリシーの名前を入力します。

b) [Mode] フィールドで、次のオプションのうちセットアップに適したものを 1 つ選択します。

- **Static Channel - Mode On**
- **LACP Active**
- **LACP Passive**
- **MAC Pinning**
- **MAC Pinning-Physical-NIC-load**

（注） LACP の Passive モードは、直接接続ホストではサポートされていません。LACP の Passive モードを使用するポートは、LACP ハンドシェイクを開始しません。常に、LACP Passive ではなく、 LACP Active を使用することを推奨します。LACP Passive は、Cisco ACI Virtual Edge /TOR ポリシー グループで、中間のレイヤ 2 デバイスが存在し、レイヤ 2 デバイス ポートが LACP の Active モードを使用している場合にのみ、使用できます。

（注） MAC Pinning-Physical-NIC-load モードは、Cisco ACI Virtual Edge ではサポートされていません。

c) **Submit** をクリックします。

**ステップ 10** **Create PC Interface Policy Group** または **Create VPC Interface Policy Group** ダイアログボックスで、**Attached Entity Profile** ドロップダウンリストからアタッチド エンティティ プロファイルを選択するか、作成して、**Submit** をクリックします。

**ステップ 11** [Create Access Port Selector] ダイアログボックスで、[OK] をクリックします。

**ステップ 12** **Create Leaf Interface Policy** ダイアログボックスで、**Submit** をクリックします。

# NX-OS スタイル CLI を使用したポート チャネル モードの設定

手順

ポート チャネル モードを設定します。

例：

```
apic1# conf t
apic1(config)# vmware-domain mininet
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# channel-mode ?
 active       Set channeling mode to ACTIVE
 mac-pinning  Set channeling mode to MAC-PINNING
 on           Set channeling mode to ON (static)
 passive      Set channeling mode to PASSIVE
apic1(config-vmware-ave)# channel-mode <mode>
```

# NX-OS スタイルの CLI を使用したポート チャネルの設定

手順

ポート チャネルを作成します。

例：

```
apic1# config
apic1(config)# template port-channel cli-pc1
apic1(config-if)# channel-mode active
apic1(config-if)# vlan-domain member cli-vdom1

apic1(config-if)# show running-config
# Command: show running-config interface port-channel cli-pc1
# Time: Thu Oct  1 10:38:30 2015
  interface port-channel cli-pc1
    vlan-domain member cli-vdom1
    channel-mode active
    exit
```

# NX-OS スタイル CLI を使用した設定例

NX-OS スタイル CLI を使用した仮想ポート チャネル（VPC）の設定は 2 つのタスクで構成されます。最初に VPC ドメインの設定し、次にスイッチ インターフェイスで VPC を設定します。

## NX-OS スタイルの CLI を使用した VPC ドメインの設定

**手順**

VPC ドメインを設定します。

**例：**

```
apic1# config
apic1(config)# vpc domain explicit 10 leaf 101 102

apic1(config-vpc)# show running-config
# Command: show running-config vpc domain explicit 10 leaf 101 102
# Time: Thu Oct  1 10:39:26 2015
  vpc domain explicit 10 leaf 101 102
    exit
```

## NX-OS スタイルの CLI を使用した、スイッチ インターフェイスでの VPC の構成

**手順**

スイッチ インターフェイスでの VPC の構成

**例：**

```
apic1# config
apic1(config)# leaf 101 - 102
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# channel-group cli-pc1 vpc

apic1(config-leaf-if)# show running-config
# Command: show running-config leaf 101 - 102 interface ethernet 1/3
# Time: Thu Oct  1 10:41:15 2015
  leaf 101
    interface ethernet 1/3
      channel-group cli-pc1 vpc
      exit
    exit
  leaf 102
    interface ethernet 1/3
      channel-group cli-pc1 vpc
```

```
  exit
exit
```

# ポート チャネル ポリシーの設定

Cisco ACI Virtual Edge 上には、複数のタイプのポート チャネル ポリシーのいずれかを設定できます:

- アクティブ モードのリンク アグリゲーション制御ポリシー （LACP）
- パッシブ モードのリンク アグリゲーション制御ポリシー （LACP）
- スタティック モード
- MAC ピニング

ポート チャネル ポリシーはCisco APIC GUI またはREST API によって設定できます。ただし、ポート チャネルのモードはNX-OS スタイル CLI を使用して設定できます。

（注） LACP ポリシーを VMM ドメインの vSwitch ポリシーとして適用した場合、LACP ポリシーは VMware vSphere 分散スイッチ（VDS）アップリンクにのみ適用されます。ただし、Cisco ACI Virtual Edge ポート チャネルには適用されません。これは想定されている動作です。Cisco ACI Virtual Edge では、自身のアップリンクで LACP がサポートされていません。これは、VDS の仮想イーサネット（vEth）インターフェイスでサポートされていないためです。そのため、VMM ポート チャネル ポリシーは VDS アップリンクに対してのみ適用されます。

## REST API を使用して LACP ポート チャネル ポリシーを設定する

**手順**

**ステップ 1** アクセス ポート プロファイルが関連付けられるリーフ ID を指定するノード プロファイルを作成します。

**例：**

```
<infraInfra dn="uni/infra">
    <infraNodeP name="bLeaf">
        <infraLeafS name="leafs" type="range">
            <infraNodeBlk name="nblk" from_="17" to_="17">
            </infraNodeBlk>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-shipping1"/>
        <infraRsAccPortP tDn="uni/infra/accportprof-shipping2"/>
    </infraNodeP>
```

**ステップ 2** アクセス バンドル グループに含まれるポートを指定するアクセス ポート プロファイルを作成します。

**例：**

```
<infraAccPortP name="shipping1">
    <infraHPortS name="pselc" type="range">
        <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="19" toPort="20"/>

        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-accountingLag1" />
    </infraHPortS>
  </infraAccPortP>
```

**ステップ 3** アクセス バンドル グループに含まれる 2 番目のポートを指定するアクセス ポート プロファイルを作成します。

**例：**

```
<infraAccPortP name="shipping2">
    <infraHPortS name="pselc" type="range">
        <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="21" toPort="22"/>

        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-accountingLag2" />
    </infraHPortS>
  </infraAccPortP>
```

**ステップ 4** ポート チャネル インターフェイス ポリシーを示すアクセス バンドル グループを作成します。

**例：**

```
<infraFuncP>
   <infraAccBndlGrp name="accountingLag1" lagT='link'>
        <infraRsLacpPol tnLacpLagPolName='accountingLacp1'/>
        <infraRsAttEntP tDn="uni/infra/attentp-default"/>
   </infraAccBndlGrp>
   <infraAccBndlGrp name="accountingLag2" lagT='link'>
         <infraRsLacpPol tnLacpLagPolName='accountingLacp2'/>
         <infraRsAttEntP tDn="uni/infra/attentp-default"/>
   </infraAccBndlGrp>
</infraFuncP>
```

**ステップ 5** ポート チャネル インターフェイス ポリシーを作成します。

**例：**

```
</infraFuncP>
<lacpLagPol name='accountingLacp1' ctrl='15' descr='accounting' maxLinks='14' minLinks='1'
mode='active' />
<lacpLagPol name='accountingLacp2' ctrl='15' descr='accounting' maxLinks='14' minLinks='1'
mode='active' />
```

`'active'` の代わりに `'passive'` にモードを設定できます。

**ステップ 6** アタッチ可能なエンティティ プロファイルに VMM ドメインを関連付けます。

**例：**

```
<infraAttEntityP name="default"> <infraRsDomP tDn="uni/vmmp-VMware/dom-mininet"/>
</infraAttEntityP>

</infraInfra>
```

# REST API を使用して MAC ピニング ポート チャネル ポリシーを設定する

手順

**ステップ 1** アクセス ポート プロファイルが関連付けられるリーフ ID を指定するノード プロファイルを作成します。

例：

```
<infraInfra dn="uni/infra">
    <infraNodeP name="bLeaf">
        <infraLeafS name="leafs" type="range">
            <infraNodeBlk name="nblk" from_="17" to_="17">
            </infraNodeBlk>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-shipping1"/>
        <infraRsAccPortP tDn="uni/infra/accportprof-shipping2"/>
    </infraNodeP>
```

**ステップ 2** アクセス バンドル グループに含まれるポートを指定するアクセス ポート プロファイルを作成します。

例：

```
<infraAccPortP name="shipping1">
    <infraHPortS name="pselc" type="range">
        <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="19" toPort="20"/>

        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-accountingLag1" />
    </infraHPortS>
  </infraAccPortP>
```

**ステップ 3** アクセス バンドル グループに含まれる 2 番目のポートを指定するアクセス ポート プロファイルを作成します。

例：

```
<infraAccPortP name="shipping2">
    <infraHPortS name="pselc" type="range">
        <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="21" toPort="22"/>

        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-accountingLag2" />
    </infraHPortS>
  </infraAccPortP>
```

**ステップ 4** ポート チャネル インターフェイス ポリシーを示すアクセス バンドル グループを作成します。

例：

```
<infraFuncP>
   <infraAccBndlGrp name="accountingLag1" lagT='link'>
        <infraRsLacpPol tnLacpLagPolName='accountingLacp1'/>
        <infraRsAttEntP tDn="uni/infra/attentp-default"/>
   </infraAccBndlGrp>
   <infraAccBndlGrp name="accountingLag2" lagT='link'>
         <infraRsLacpPol tnLacpLagPolName='accountingLacp2'/>
         <infraRsAttEntP tDn="uni/infra/attentp-default"/>
```

```
   </infraAccBndlGrp>
</infraFuncP>
```

**ステップ 5** ポート チャネル インターフェイス ポリシーを作成します。

**例：**

```
<lacpLagPol name='accountingLacp1' ctrl='15' descr='accounting' maxLinks='14' minLinks='1'
 mode='mac-pin' />
<lacpLagPol name='accountingLacp2' ctrl='15' descr='accounting' maxLinks='14' minLinks='1'
 mode='mac-pin' />
```

**ステップ 6** アタッチ可能なエンティティ プロファイルに VMM ドメインを関連付けます。

**例：**

```
<infraAttEntityP name="default"> <infraRsDomP tDn="uni/vmmp-VMware/dom-mininet"/>
</infraAttEntityP>

</infraInfra>
```

# REST API を使用して静的ポート チャネル ポリシーを設定する

**手順**

**ステップ 1** アクセス ポート プロファイルが関連付けられるリーフ ID を指定するノード プロファイルを作成します。

**例：**

```
<infraInfra dn="uni/infra">
    <infraNodeP name="bLeaf">
        <infraLeafS name="leafs" type="range">
            <infraNodeBlk name="nblk" from_="17" to_="17">
            </infraNodeBlk>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-shipping1"/>
        <infraRsAccPortP tDn="uni/infra/accportprof-shipping2"/>
    </infraNodeP>
```

**ステップ 2** アクセス バンドル グループに含まれるポートを指定するアクセス ポート プロファイルを作成します。

**例：**

```
<infraAccPortP name="shipping1">
    <infraHPortS name="pselc" type="range">
        <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="19" toPort="20"/>

        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-accountingLag1" />
    </infraHPortS>
  </infraAccPortP>
```

**ステップ 3** アクセス バンドル グループに含まれる 2 番目のポートを指定するアクセス ポート プロファイルを作成します。

例：

```
<infraAccPortP name="shipping2">
    <infraHPortS name="pselc" type="range">
        <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="21" toPort="22"/>

        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-accountingLag2" />
    </infraHPortS>
  </infraAccPortP>
```

**ステップ 4** ポート チャネル インターフェイス ポリシーを示すアクセス バンドル グループを作成します。

例：

```
<infraFuncP>
   <infraAccBndlGrp name="accountingLag1" lagT='link'>
        <infraRsLacpPol tnLacpLagPolName='accountingLacp1'/>
        <infraRsAttEntP tDn="uni/infra/attentp-default"/>
   </infraAccBndlGrp>
   <infraAccBndlGrp name="accountingLag2" lagT='link'>
         <infraRsLacpPol tnLacpLagPolName='accountingLacp2'/>
         <infraRsAttEntP tDn="uni/infra/attentp-default"/>
   </infraAccBndlGrp>
</infraFuncP>
```

**ステップ 5** ポート チャネル インターフェイス ポリシーを作成します。

例：

```
<lacpLagPol name='accountingLacp1' ctrl='15' descr='accounting' maxLinks='14' minLinks='1'
 mode='off' />
<lacpLagPol name='accountingLacp2' ctrl='15' descr='accounting' maxLinks='14' minLinks='1'
 mode='off' />
```

**ステップ 6** アタッチ可能なエンティティ プロファイルに VMM ドメインを関連付けます。

例：

```
<infraAttEntityP name="default"> <infraRsDomP tDn="uni/vmmp-VMware/dom-mininet"/>
</infraAttEntityP>

</infraInfra>
```

# Enhanced LACP ポリシーのサポート

Cisco Application Policy Infrastructure Controller（APIC）リリース 4.0(1) 以降では、さまざまな分散型仮想スイッチ（DVS）アップリンク ポート グループごとに異なる Link Aggregation Control Protocol（LACP）ポリシーを適用して、アップリンクのロードバランシングを向上させることができます。

Cisco APIC では VMware の Enhanced LACP がサポートされるようになりました。この機能は DVS 5.5 以降で使用できます。以前は、同じ LACP ポリシーをすべての DVS アップリンク ポート グループに適用していました。Cisco APIC リリース 4.0(1) では、Cisco APIC を使用して VMware のリンク集約グループ（LAG）を管理することができませんでした。

VMware vCenter 仮想マシン マネージャ（VMM）ドメインを Cisco Application Centric Infrastructure Virtual Edge または VMware VDS 用に作成する場合、最大 20 個のさまざまなロードバランシング アルゴリズムから選択することができます。アップリンク ポートグループごとに異なるポリシーを適用します。

8 つの DVS アップリンク ポートグループがあり、少なくとも 2 つのアップリンクを同じポリシーで設定する必要があります。したがって、DVS ごとに最大 4 つの異なる LACP ポリシーを設定できます。Enhanced LACP では、アクティブおよびパッシブの LACP モードのみがサポートされます。

（注） Cisco ACI Virtual Edge VXLAN モードでは、UDP ポートを持つロードバランシング アルゴリズムの使用が必須になります。アルゴリズム「**Source and Destination TCP/UDP Port**」の使用をお勧めします。VLXAN モードでは、トラフィックは常に VTEP 間で FTEP IP に送信されます。そのため、通信は常に 1 ペアの IP アドレス間で行われます。したがって、VXLAN トラフィックでは、UDP ポート番号を使用することがトラフィックを区別する唯一の方法になります。

以降のセクションでは、Cisco APIC GUI、NX-OS スタイル CLI、または REST API を使用して複数の LACP ポリシーを DVS アップリンク用に設定する手順について説明します。

# Enhanced LACP の制限事項

Enhanced Link Aggregation Control Protocol（LACP）ポリシーを使用する際は、次の制限事項に留意してください。

- Enhanced LACP へのアップグレード後に以前のバージョンの LACP に戻すことはできません。
- Enhanced LACP の設定を削除せずに、4.0（1）よりも前のバージョンの Cisco Application Policy Infrastructure Controller（APIC）にダウングレードすることはできません。このガイドの手順ダウングレード前の Enhanced LACP 設定の削除 （37 ページ）を参照してください。
- Cisco Application Centric Infrastructure Virtual Edgeの VXLAN モードのトラフィックでは、常に送信元 IP アドレスが TEP IP アドレスとして使用されます。適切なロードバランシングを確保するため、アルゴリズム「**Source and Destination TCP/UDP Port**」の使用をお勧めします。

# Cisco APIC GUI を使用した DVS アップリンク ポート用 LAG の作成

分散型仮想スイッチ（DVS）のアップリンク ポート グループをリンク集約グループ（LAG）に配置し、特定のロードバランシング アルゴリズムに関連付けることによって、ポート グループのロードバランシングを向上させます。Cisco Application Policy Infrastructure Controller（APIC）GUI を使用してこのタスクを実行することができます。

### 始める前に

- VMware VDS または Cisco Application Centric Infrastructure Virtual Edge 用に VMware vCenter 仮想マシン マネージャ（VMM）ドメインを作成する必要があります。
- VSwitch ポリシー コンテナが存在しない場合は、1 つ作成します。

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** **[Virtual Networking]** > **[Inventory]** > **[VMM Domains]** > **[VMware]** > ***[domain]*** に移動します。

**ステップ 3** 作業ペインで、**[Policy]** > **[VSwitch Policy]** を選択します。

**ステップ 4** [Properties] 領域でまだポリシーを選択していない場合は、選択します。

**ステップ 5** [Enhanced LAG Policy] 領域で、[+]（プラス記号）アイコンをクリックし、次の手順を実行します。

a) [Name] フィールドに、LAG の名前を入力します。
b) [Mode] ドロップダウン リストで、[LACP Active] または [LACP Passive] を選択します。
c) [Load Balancing Mode] ドロップダウン リストで、ロード バランシング方式を選択します。
d) [Number of Links] セレクターで、LAG に含める DVS アップリンク ポート グループの数を選択します。

2 ～ 8 個のアップリンク ポート グループを LAG に配置できます。

e) **Update** をクリックし、**Submit** をクリックします。

**ステップ 6** ステップ 5 を繰り返して、DVS 用の他の LAG を作成します。

### 次のタスク

VMware VDS を使用している場合は、Enhanced LACP ポリシーを設定しているドメインにエンドポイント グループ（EPG）を関連付けます。Cisco Application Centric Infrastructure Virtual Edge を使用している場合は、内部的に作成した内部および外部ポート グループを Enhanced LACP ポリシーに関連付けてから、EPG をポリシーとともにドメインに関連付けます。

# NX-OS スタイル CLI を使用した DVS アップリンク ポート用 LAG の作成

分散型仮想スイッチ（DVS）のアップリンク ポート グループをリンク集約グループ（LAG）に配置し、特定のロードバランシング アルゴリズムに関連付けることによって、ポート グループのロード バランシングを向上させます。NX-OS スタイル CLI を使用してこのタスクを実行することができます。

### 始める前に

VMware VDS または Cisco Application Centric Infrastructure Virtual Edge 用に VMware vCenter 仮想マシン マネージャ（VMM）ドメインを作成する必要があります。

### 手順

Enhanced LACP ポリシーを作成または削除します。

**例**：

```
apic1(config-vmware)# enhancedlacp  LAG name
apic1(config-vmware-enhancedlacp)# lbmode loadbalancing mode
apic1(config-vmware-enhancedlacp)# mode mode
apic1(config-vmware-enhancedlacp)# numlinks max number of uplinks
apic1(config-vmware)# no enhancedlacp LAG name to delete
```

### 次のタスク

VMware VDS を使用している場合は、Enhanced LACP ポリシーを設定しているドメインにエンドポイント グループ（EPG）を関連付けます。Cisco Application Centric Infrastructure Virtual Edge を使用している場合は、内部的に作成した内部および外部ポート グループを Enhanced LACP ポリシーに関連付けてから、EPG をポリシーとともにドメインに関連付けます。

# REST API を使用した DVS アップリンク ポート用 LAG の作成

分散型仮想スイッチ（DVS）のアップリンク ポート グループをリンク集約グループ（LAG）に配置し、特定のロードバランシング アルゴリズムに関連付けることによって、ポート グループのロード バランシングを向上させます。REST API を使用してこのタスクを実行することができます。

### 始める前に

VMware VDS または Cisco Application Centric Infrastructure Virtual Edge 用に VMware vCenter 仮想マシン マネージャ（VMM）ドメインを作成する必要があります。

### 手順

**ステップ 1** LAG を作成し、ロードバランシング アルゴリズムに関連付けます。

**例**：

```
<polUni>
<vmmProvP vendor="VMware">
    <vmmDomP name="mininetlacpavs">
        <vmmVSwitchPolicyCont>
            <lacpEnhancedLagPol name="lag2" mode="passive" lbmode="vlan" numLinks="4">
            </lacpEnhancedLagPol>
        </vmmVSwitchPolicyCont>
```

```
    </vmmDomP>
</vmmProvP>
</polUni>
```

**ステップ 2** 手順を繰り返して、DVS 用の他の LAG を作成します。

### 次のタスク

VMware VDS を使用している場合は、Enhanced LACP ポリシーを設定しているドメインにエンドポイント グループ（EPG）を関連付けます。Cisco Application Centric Infrastructure Virtual Edge を使用している場合は、内部的に作成した内部および外部ポート グループを Enhanced LACP ポリシーに関連付けてから、EPG をポリシーとともにドメインに関連付けます。

# Enhanced LACP ポリシーを持つ VMware vCenter ドメインへの内部ポート グループの関連付け（Cisco APIC GUI を使用する方法）

Cisco Application Centric Infrastructure Virtual Edge で内部的に作成した内部および外部ポート グループを、Enhanced LACP ポリシーを持つ VMware vCenter ドメインに関連付けます。Cisco Application Policy Infrastructure Controller（APIC）GUI を使用してこのタスクを実行することができます。

### 始める前に

分散型仮想スイッチ（DVS）のアップリンク ポート グループ用にリンク集約グループ（LAG）を作成し、ロードバランシング アルゴリズムを LAG に関連付けておく必要があります。

### 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]** > ***[domain]*** に移動します。

**ステップ 3** 作業ペインで、**[Policy]** > **[General]** を選択します。

**ステップ 4** [Enhanced LAG Policy] ドロップダウン リストで、ポリシーを選択します。

**ステップ 5** [Submit] をクリックします。

### 次のタスク

Enhanced LACP ポリシーが含まれている VMware vCenter ドメインに、エンドポイント グループ（EPG）を関連付けます。

# Enhanced LACP ポリシーを持つ VMware vCenter ドメインへの内部ポート グループの関連付け（NX-OS スタイル CLI を使用する方法）

Cisco Application Centric Infrastructure Virtual Edge で内部的に作成した内部および外部ポート グループを、Enhanced LACP ポリシーを持つ VMware vCenter ドメインに関連付けます。NX-OS スタイル CLI を使用してこのタスクを実行することができます。

### 始める前に

分散型仮想スイッチ（DVS）のアップリンク ポート グループ用にリンク集約グループ（LAG）を作成し、ロードバランシング アルゴリズムを LAG に関連付けておく必要があります。

### 手順

---

Enhanced LACP ポリシーを持つ VMM ドメインに、内部エンドポイント グループ（EPG）を関連付けます（または関連付けを解除します）。

**例**：

```
apic1(config-vmware)# lag-policy name of the policy to associate
apic1(config-vmware)#  no lag-policy name of the policy to deassociate
```

---

### 次のタスク

Enhanced LACP ポリシーが含まれている VMware vCenter ドメインに、EPG を関連付けます。

# Enhanced LACP ポリシーを持つ VMware vCenter ドメインへの内部ポート グループの関連付け（REST API を使用する方法）

Cisco Application Centric Infrastructure Virtual Edge で内部的に作成した内部および外部ポート グループを、Enhanced LACP ポリシーを持つ VMware vCenter ドメインに関連付けます。REST API を使用してこのタスクを実行することができます。

### 始める前に

分散型仮想スイッチ（DVS）のアップリンク ポートグループ用にリンク集約グループ（LAG）を作成し、ロードバランシング アルゴリズムを LAG に関連付けておく必要があります。

### 手順

---

**例**：

```
<vmmProvP vendor="VMware">
    <vmmDomP name="mininetlacpavs" enfPref="sw" mcastAddr="225.1.1.1" prefEncapMode="vlan"
 enableAVE="true">
```

```
        <vmmRsPrefEnhancedLagPol
tDn="uni/vmmp-VMware/dom-mininetlacpavs/vswitchpolcont/enlacplagp-lag2"/>
    </vmmDomP>
</vmmProvP>
```

### 次のタスク

Enhanced LACP ポリシーが含まれている VMware vCenter ドメインに、エンドポイント グループ（EPG）を関連付けます。

# EnhancedLACPポリシーを持つVMwarevCenterドメインへのアプリケーション EPG の関連付け（Cisco APIC GUI を使用する方法）

LAG とロードバランシング アルゴリズムを持つ VMware vCenter ドメインに、アプリケーション エンドポイント グループ（EPG）を関連付けます。Cisco Application Policy Infrastructure Controller（APIC）GUI を使用してこのタスクを実行することができます。

### 始める前に

分散型仮想スイッチ（DVS）のアップリンク ポート グループ用にリンク集約グループ（LAG）を作成し、ロードバランシング アルゴリズムを LAG に関連付けておく必要があります。

（注） この手順では、まだアプリケーション EPG を VMware vCenter ドメインに関連付けていないと仮定します。すでに関連付けを済ませている場合は、ドメインの関連付けを編集します。

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** **[Tenants]** > ***[tenant]*** > **[Application Profiles]** > ***[application_profile]*** > **[Application EPGs]** > ***[EPG]*** > **[Domains(VMs and Bare-Metals)]** に移動します。

**ステップ 3** **[ドメイン (VM およびベア メタル）]** を右クリックし **[VMM ドメインの関連付けの追加]** をクリックします。

**ステップ 4** [Add VMM Domain Association] ダイアログ ボックスで、次の手順を完了します。

a) [VMM Domain Profile] ドロップダウン リストで、EPG を関連付けるドメインを選択します。

b) [Enhanced Lag Policy] で、EPG に適用するドメイン用に設定したポリシーを選択します。

c) ドメインの関連付けについて残りの適切な値を追加し、[Submit] をクリックします。

**ステップ 5** 必要に応じて、テナント内の他のアプリケーション EPG についてステップ 2 ～ 4 を繰り返します。

# EnhancedLACPポリシーを持つVMwarevCenterドメインへのアプリケーション EPG の関連付け（NX-OS スタイル CLI を使用する方法）

LAG とロードバランシング アルゴリズムを持つ VMware vCenter ドメインに、アプリケーション エンドポイント グループ（EPG）を関連付けます。NX-OS スタイル CLI を使用してこのタスクを実行することができます。アプリケーション EPG とドメインとの関連付けを解除することもできます。

### 始める前に

分散型仮想スイッチ（DVS）のアップリンク ポート グループ用にリンク集約グループ（LAG）を作成し、ロードバランシング アルゴリズムを LAG に関連付けておく必要があります。

### 手順

**ステップ 1** アプリケーション EPG をドメインに関連付けるか、または関連付けを解除します。

**例**：

```
apic1(config-tenant-app-epg-domain)#  lag-policy name of the LAG policy to associate
apic1(config-tenant-app-epg-domain)# no  lag-policy name of the LAG policy to deassociate
```

**ステップ 2** 必要に応じて、テナント内の他のアプリケーション EPG についてステップ 1 を繰り返します。

# EnhancedLACPポリシーを持つVMwarevCenterドメインへのアプリケーション EPG の関連付け（REST API を使用する方法）

LAG とロードバランシング アルゴリズムを持つ VMware vCenter ドメインに、アプリケーション エンドポイント グループ（EPG）を関連付けます。REST API を使用してこのタスクを実行することができます。アプリケーション EPG とドメインとの関連付けを解除することもできます。

### 始める前に

分散型仮想スイッチ（DVS）のアップリンク ポート グループ用にリンク集約グループ（LAG）を作成し、ロードバランシング アルゴリズムを LAG に関連付けておく必要があります。

### 手順

**ステップ 1** EPG を VMware vCenter ドメインに関連付け、LAG をロードバランシング アルゴリズムに関連付けます。

**例**：

```
<polUni>
  <fvTenant
    dn="uni/tn-coke"
    name="coke">
    <fvCtx name="cokectx"/>
    <fvAp
      dn="uni/tn-coke/ap-sap"
      name="sap">
      <fvAEPg
        dn="uni/tn-coke/ap-sap/epg-web3"
        name="web3" >
          <fvRsBd tnFvBDName="cokeBD2" />
          <fvRsDomAtt resImedcy="immediate" switchingMode="native"
            tDn="uni/vmmp-VMware/dom-mininetlacpavs">
            <fvAEPgLagPolAtt >
              <fvRsVmmVSwitchEnhancedLagPol
tDn="uni/vmmp-VMware/dom-mininetlacpavs/vswitchpolcont/enlacplagp-lag2"/>
            </fvAEPgLagPolAtt>
          </fvRsDomAtt>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```

**ステップ 2** 必要に応じて、テナント内の他のアプリケーション EPG についてステップ 1 を繰り返します。

# ダウングレード前の Enhanced LACP 設定の削除

Cisco Application Policy Infrastructure Controller（APIC）を 4.0（1）よりも前のリリースにダウングレードする場合、事前に Enhanced LACP の設定を削除する必要があります。設定を削除するには、ここで説明している手順を実行します。

### 手順

**ステップ 1** すべての ESXi ホスト上のアップリンクを、リンク集約グループ（LAG）から通常のアップリンクに再割り当てします。

**ステップ 2** 分散型仮想スイッチ（DVS）に関連付けられているすべての EPG から、LAG との関連付けを削除します。

この手順の実行中はトラフィックの消失が予想されます。

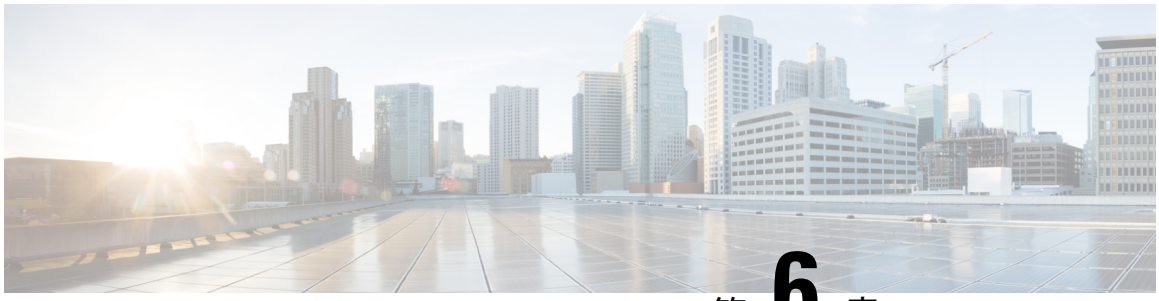
**ステップ 3** ポートチャネル設定を、スタティック チャネルまたは MAC 固定に変更します。これで、ポート チャネルが起動するとトラフィックが回復します。

**ステップ 4** 仮想マシン マネージャ（VMM）から LAG 関連の設定をすべて削除します。

**ステップ 5** VMware vCenter から、LAG 関連のすべてのポリシーが削除されたことを確認します。

### 次のタスク

4.0(1) よりも前のリリースの Cisco APIC にダウングレードします。



第 6 章

# SPAN の機能

この章の内容は、次のとおりです。



# SPAN 機能の設定について

Cisco ACI Virtual Edge は、ローカル SPAN およびカプセル化リモート SPAN（ERSPAN）を、含むスイッチド ポート アナライザ（SPAN）をサポートします。

SPANセッションの送信元または宛先として、Cisco ACI Virtual Edge内部または外部のインターフェイス アップリンクを使用することはできません。Cisco ACI Virtual Edge は DVS あたり 64 の SPAN セッション（ローカル SPAN および ERSPAN）をサポートします。送信元は最大 4 つの SPAN セッションのメンバーになることが可能です。

### SPAN を設定する際の注意事項

Cisco ACI Virtual Edge でローカル SPAN セッションを設定する場合は、次の注意事項に従ってください。

- セッションあたり 1 つの vLeaf のみ有することができます。
- セッションはクライアント エンド ポイント（CEP）によって定義されます。宛先としての EPG はサポートされていません。
- 宛先 CEP が定義された場合にセッションが vLeaf 上で展開されます。
- 通常のトラフィックは宛先 CEP を行き来することはできません。
- 無差別モードが有効になっている別の EPG は、LSPAN 宛先 CEP に作成される必要があります。

### ERSPAN を設定する際の注意事項

Cisco ACI Virtual Edge で ERSPAN セッションを設定する場合は、次の注意事項に従ってください。

- セッションは、その他のオプション パラメータの IP アドレスに基づいて定義されます。
- セッションは複数の vLeaf に展開できます。
- セッションは送信元 CEP またはエンドポイント グループ（EPG）が定義されている場合に vLeaf に展開されます。
- ERSPAN セッションの宛先は常に overlay-1 (infraVRF [virtual routing and forwarding]) である必要があります。宛先が Cisco ACI Virtual Edge の背後の VM である場合、インフラ EPG で前面に出します。

  ERSPAN 宛先は常にリモートである必要があります。Cisco ACI Virtual Edge から同じ Cisco ACI Virtual Edge の背後でホストされる宛先への ERSPAN はサポートされません。
- ERSPAN 宛先が VM の場合、VMotion がそこで無効になっていることを確認します。ERSPAN 宛先 VM が何らかの理由で別のホストに移動された場合、それに応じてスタティック CEP が設定されていることを確認します。セクション GUI を使用した SPAN 機能の構成 （41 ページ） のステップ 21 ～ 24 を参照してください。
- 宛先の IP アドレスは、DHCP（DHCP 中にオプション 61 が必要）またはスタティック設定を使用して取得できます。IP アドレスが overlay-1 (infra VRF) の他の VTEP と同じサブネット内にあることを確認してください。

（注） VM およびデバイスのすべてのオペレーティング システムは、DHCP オプション 61 をサポートします。その場合、スタティック IP アドレスをインフラ VLAN で使用します。インフラ VLAN で IP がリースされた DHCP IP と競合する可能性があるため、ERSPAN の IP アドレスを慎重に選択します。

### UCS B シリーズ サーバでの SPAN または ERSPAN の設定の注意事項

Cisco ACI Virtual Edge の SPAN または ERSPAN を設定し、Cisco ACI Virtual Edge ホストを UCS B シリーズ サーバで実行する場合、ファブリック インターコネクトに接続するインターフェイスに、MAC ピニングを持つポート チャネル（PC）インターフェイス ポリシー グループを設定する必要があります。これは、仮想送信元（vsource）と仮想宛先（vdestination）グループが PC ポリシー グループでのみ指定されているためです。

# GUI を使用した SPAN 機能の構成

### 始める前に

LSPAN を設定する場合で設定された新しい EPG を必須 **Promiscuous** を同じホスト上のローカル トラフィックをキャプチャするモード。この EPG は、トラフィックをキャプチャする VM で使用する必要があります。次の手順を実行します。

1. 新しい EPG を作成し、VMM ドメインに関連付けを選択すると **平均** スイッチング モードとしてと **自動** として、カプセル化モードに入ります。
2. 有効化 **Promiscuous** EPG のモード。

   Cisco APIC で EPG を展開し、をクリックして **ドメイン (Vm とベア metals)** 、EPG にすでに関連付けられている VMM を右クリックし、をクリックし、 **VMM ドメインの編集アソシエーション** 設定、 **承認を混合モードを許可する** 、] をクリックし、 **OK** 。

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** メニュー バーで、[Fabric] > [Access Policies] を選択します。

**ステップ 3** [Policies] ナビゲーション ペインで、[Policies] フォルダと [Troubleshooting] フォルダを開きます。

**ステップ 4** **[VSPAN]** フォルダを展開します。

**ステップ 5** **[VSPAN 宛先グループ]** フォルダを右クリックして、**[Create VSPAN 宛先グループの作成]** を選択します。

**ステップ 6** **[VSPAN 宛先グループ]** 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、名前を入力します

b) **[宛先の作成]** エリアで、**[+]** アイコンをクリックします。

**ステップ 7** **[VSPAN 宛先の作成]** ダイアログ ボックスで、次の手順を実行します。

a) **[宛先タイプ]** フィールドで、**[ERSPAN]** または **[LSPAN]** を選択します（ローカル SPAN）。

b) 次のいずれかの手順を実行します。

| 場合は、選択したステップ 7. | 結果 |
|---|---|
| ERSPAN | 次の値を入力します。<br>• [Name]：VSPAN宛先の名前を入力します（Destination1）。<br>• **[Description]**：（オプション）VSPAN宛先の説明を入力します。<br>• [Destination Type]：[ERSPAN] を選択します。<br>• [Destination IP]：宛先 IP アドレスを指定します。<br>• [Flow ID]：フロー ID 値を指定します。<br>• [TTL]：TTL 値（64）を指定します。<br>• [MTU]：MTU 値（1510）を指定します。<br>• **DSCP**：QoS の DSCP 値を入力します。 |
| LSPAN | 次の値を入力します。<br>• [Name]：VSPAN宛先の名前を入力します（Destination1）。<br>• **[Description]**：（オプション）VSPAN宛先の説明を入力します。<br>• [Destination Type]：[LSPAN] を選択します。<br>• **[宛先 CEP]**：（オプション）宛先に Tenant (1)、Application Profile (a1)、EPG (e1)、CEP MAC を選択します。<br>LSPAN にするための前提条件を満たす場合に、宛先CEP MACアドレスが表示されます。<br>（注） 宛先CEPを設定するときに、無差別モードを有効になっている状態で「開始する前に」のセクションで作成した EPG を選択します。 |

c) [OK] をクリックして、VSPAN 宛先を保存します。

**ステップ 8** [Create VSPAN Destination] ダイアログ ボックスで、[Submit] をクリックして VSPAN 宛先グループを保存します。

**ステップ 9** [Policies] ナビゲーション ペインで、[VSPAN Sessions] フォルダを右クリックし、[Create VSPAN Session] を右クリックします。

**ステップ 10** [Create VSPAN Session] ダイアログ ボックスの [Name] フィールドに、送信元グループの名前を入力します。

**ステップ 11** [Admin State] フィールドで、[Start] が選択されていることを確認します。

**ステップ 12** [Destination Group] ドロップダウン リストから、新しい宛先グループを選択します。

**ステップ 13** [Create Sources] エリアで、[+] アイコンをクリックします。

**ステップ 14** [Create VSPAN VSource] 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、送信元の名前を入力します。
b) [Direction] 領域で、送信元の方向を選択します（[Both]、[Incoming]、または**[Outgoing]**）
c) [Source type] 領域で、[EPG] または [CEP] を選択します。
d) [Source EPG] または [Source CEP] 領域で、ドロップダウン リストから、テナント、アプリケーション プロファイル、および EPG を選択します。
e) 送信元のタイプとして CEP を選択する場合は、ドロップダウン リストから [CEP] を選択します。
f) [Add Source Access Paths] エリアを無視します。
g) [OK] をクリックして、VSPAN 送信元を保存します。

**ステップ 15** [Submit] をクリックして VSPAN 送信元グループを保存します。

**ステップ 16** メニュー バーで、[Fabric] > [Access Policies] を選択します。

**ステップ 17** [Policies] ナビゲーション ウィンドウで、[Interfaces]、[Leaf Interfaces]、[Policy Groups] フォルダを展開します。

**ステップ 18** [VPC Interface] フォルダを展開して、接続する SPAN 送信元または宛先を介してポリシー グループをクリックします。

**ステップ 19** ポリシー グループの [PC/VPC Interface Policy Group] 作業ペインで、次の手順を実行します。

a) [Attached Entity Profile] ドロップダウン リストから接続済みのエンティティ プロファイルを選択または作成します。

手順については、このガイドの「GUI を使用したアタッチ可能エンティティ プロファイルの設定 （95 ページ）」を参照してください。

（注） 次の手順を完了するにはページの下にスクロールする必要があります。

b) [VSource Groups] 領域で、[+] アイコンをクリックし、目的の SPAN 送信元グループを選択し、[Update] をクリックします。

これは、ステップ 14.a で作成した送信元の名前です。

c) [VDestination Group] エリアで、SPAN 宛先グループを選択し、[Update] をクリックします。

これは、ステップ 7.b で作成した宛先の名前です。

d) [Submit] をクリックします。

これらの手順は、SPAN 送信元と SPAN 宛先グループを選択されたポリシー グループと関連付けます。

**ステップ 20** 設定を確認するには、Cisco ACI Virtual Edge で SSH セッションを開き、**vemcmd show span** コマンドを入力してアクティブな SPAN セッションを表示します。新しいセッションが実行されていることを検証します。

（注） ステップ 21 ～ 24 は、ERSPAN 専用です。

**ステップ 21** APIC GUI のメニュー バーで、[Tenants] > [infra] を選択します。

**ステップ 22** **[Tenant infra]** ナビゲーション ペインで、**[Application Profiles]** > **[access]** > **[Application FPGs]** > **[EPG default]** を展開します。

**ステップ 23** [Static EndPoint] フォルダを右クリックし、[Create Static EndPoint] を選択します。

**ステップ 24** [Create Static Endpoint] ダイアログボックスで、次の手順を実行します。

a) [MAC] フィールドに、MAC アドレスの ERSPAN 宛先を入力します。
b) [Type] 領域で、[tep] を選択します。
c) [Path Type] 領域で、適切なパス タイプを選択します。

パス タイプとしてポートを選択する場合は、[Node] ドロップダウン リストからノードを選択します。

パス タイプは、リーフが ERSPAN 宛先に接続される方法を決定します。リーフはポート、ダイレクト ポート チャネル、または仮想ポートチャネルによって接続できます。

d) [Path] フィールドに適切なパスを入力します。

パスは、ERSPAN 宛先がアタッチされるポリシー グループを決定します。

e) [IP Address] フィールドに ERSPAN 宛先 IP アドレスを入力します。
f) [Encap] フィールドで、適切な overlay-1 VLAN を入力します。
g) [Submit] をクリックします。
h) ERSPAN 宛先から overlay- IP アドレスを ping します。

この手順は、ファブリックが ERSPAN 宛先 IP アドレスについて学習することを確実にします。

# NX-OS CLI を使用した SPAN の設定

**手順**

**ステップ 1** SPAN を設定します。

**例：**

```
apic1(config)# monitor virtual session cli-vspan1
apic1(config-monitor-virtual)# source tenant cli-esx1 application cli-esx1 epg cli-vspan1
 mac <00:50:56:BA:BE:0F>
apic1(config-monitor-virtual-source)# direction both
apic1(config-monitor-virtual-source)# exit
apic1(config-monitor-virtual)# destination tenant cli-esx1 application cli-vspan1 epg
cli-esx1b mac <00:50:56:BA:F0:E0>

apic1(config)# vmware-domain cli-esx
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# monitor virtual session cli-vspan1
```

**ステップ 2** 設定を確認します。

**例**：

```
apic1(config-monitor-virtual)# show running-config
# Command: show running-config monitor virtual session cli-vspan1
# Time: Thu Oct  8 11:20:09 2015
  monitor virtual session cli-vspan1
    source tenant cli-esx1 application cli-esx1 epg cli-esx1 mac 00:50:56:BA:BE:0F
      exit
    destination tenant cli-esx1 application cli-esx1 epg cli-esx1b mac 00:50:56:BA:F0:E0

    exi
```

# REST API を使用した SPAN 機能の構成

## REST API を使用して CEP 送信元を持つローカル SPAN を構成する

**手順**

CEP 送信元を持つローカル SPAN を設定します。

**例**：

```
<polUni>
  <infraInfra>
    <spanVSrcGrp name="srcgrp2">
        <spanVSrc name="src1" dir="both" >
                          <spanRsSrcToVPort
tDn="uni/tn-t0/ap-a0/epg-g3/cep-00:50:56:B3:24:E1"/>
        </spanVSrc>
        <spanSpanLbl name="destgrp1">
        </spanSpanLbl>
    </spanVSrcGrp>
      <infraFuncP>
           <infraAccBndlGrp name="test-lvspan">
           <infraRsSpanVSrcGrp tnSpanVSrcGrpName="srcgrp1"/>
           <infraRsSpanVDestGrp tnSpanVDestGrpName="destgrp1"/>
           <infraRsAttEntP tDn="uni/infra/attentp-test-lvspan"/>
           </infraAccBndlGrp>
    </infraFuncP>
     <spanVDestGrp
```

```
                        name="destgrp2">
        <spanVDest name="dest1">
                           <spanRsDestToVPort
tDn="uni/tn-t0/ap-a0/Promiscuous-EPG/cep-00:50:56:B3:5F:AA"/>
        </spanVDest>
    </spanVDestGrp>
    <infraAttEntityP name="test-lvspan">
    <infraRsDomP tDn="uni/vmmp-VMware/dom-mininet"/>
 </infraAttEntityP>
 </infraInfra>
 </polUni>
```

# REST API を使用して EPG 送信元を持つローカル SPAN を設定する

**手順**

EPG 送信元を持つローカル SPAN を設定します。

**例**：

```
<polUni>
  <infraInfra>
  <spanVSrcGrp
                        name="srcgrp2" adminSt="start">
        <spanVSrc name="src2" dir="both">
                           <spanRsSrcToEpg  tDn="uni/tn-t0/ap-a0/epg-g11"/>
        </spanVSrc>
        <spanSpanLbl name="destgrp1">
          </spanSpanLbl>
    </spanVSrcGrp>
    <infraFuncP>
            <infraAccBndlGrp name="test-lvspan">
            <infraRsSpanVSrcGrp tnSpanVSrcGrpName="srcgrp2"/>
            <infraRsSpanVDestGrp tnSpanVDestGrpName="destgrp1"/>
            </infraAccBndlGrp>
    </infraFuncP>
  <spanVDestGrp
                        name="destgrp2">
        <spanVDest name="dest1">
                           <spanRsDestToVPort
tDn="uni/tn-t0/ap-a0/Promiscuous-EPG/cep-00:50:56:B3:5F:AA"/>
        </spanVDest>
    </spanVDestGrp>
    <infraAttEntityP name="test-lvspan">
    <infraRsDomP tDn="uni/vmmp-VMware/dom-mininet"/>
 </infraAttEntityP>
 </infraInfra>
 </polUni>
```

# REST API を使用して CEP 送信元を持つ ERSPAN を設定する

手順

CEP 送信元を持つ ERSPAN を設定します。

例：

```
<polUni>
  <infraInfra>
    <spanVSrcGrp name="srcgrp2">
        <spanVSrc name="src1" dir="both" >
                          <spanRsSrcToVPort
tDn="uni/tn-t0/ap-a0/epg-g3/cep-00:50:56:B3:24:E1"/>
        </spanVSrc>
        <spanSpanLbl name="destgrp1">
        </spanSpanLbl>
    </spanVSrcGrp>
      <infraFuncP>
           <infraAccBndlGrp name="test-lvspan">
           <infraRsSpanVSrcGrp tnSpanVSrcGrpName="srcgrp1"/>
           <infraRsSpanVDestGrp tnSpanVDestGrpName="destgrp1"/>
           <infraRsAttEntP tDn="uni/infra/attentp-test-lvspan"/>
           </infraAccBndlGrp>
    </infraFuncP>
          <spanVDestGrp
                       name="destgrp1">
        <spanVDest name="dest1">
           <spanVEpgSummary name="summ1" dstIp="10.30.13.195" ttl="50" mtu="1500"
dscp="2"/>
            </spanVDest>
    </spanVDestGrp>
   <infraAttEntityP name="test-lvspan">
    <infraRsDomP tDn="uni/vmmp-VMware/dom-mininet"/>
 </infraAttEntityP>
 </infraInfra>
 </polUni>
```

# REST API を使用して静的エンドポイントを持つ ERSPAN を設定する

手順

静的 CEP 送信元を持つ ERSPAN を設定します。

例：

```
<polUni>
 <fvTenant name="infra">
   <fvAp name="access">
     <fvAEPg name="default">
       <fvStCEp name="erspan-dest "
             type="tep"
             mac="00:50:56:B3:42:9C"
             ip="10.0.0.50"
```

```
            encap="vlan-4093">
          <fvRsStCEpToPathEp tDn="topology/pod-1/paths-110/pathep-[macpin-1]"/>
        </fvStCEp>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```

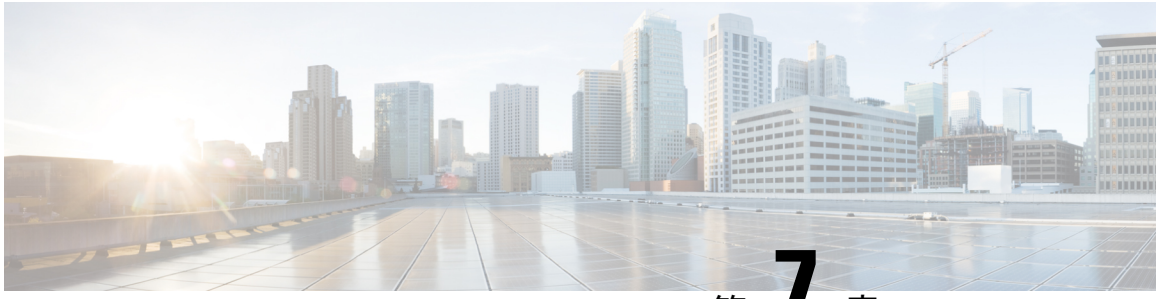
# REST API を使用して EPG 送信元を持つ ERSPAN を設定する

**手順**

EPG 送信元を持つ ERSPAN を設定します。

**例**：

```
<polUni>
  <infraInfra>
  <spanVSrcGrp
                        name="srcgrp2" adminSt="start">
        <spanVSrc name="src2" dir="both">
                           <spanRsSrcToEpg  tDn="uni/tn-t0/ap-a0/epg-g11"/>
        </spanVSrc>
        <spanSpanLbl name="destgrp1">
          </spanSpanLbl>
    </spanVSrcGrp>
    <infraFuncP>
            <infraAccBndlGrp name="test-lvspan">
            <infraRsSpanVSrcGrp tnSpanVSrcGrpName="srcgrp2"/>
            <infraRsSpanVDestGrp tnSpanVDestGrpName="destgrp1"/>
            </infraAccBndlGrp>
    </infraFuncP>
           <spanVDestGrp
                        name="destgrp1">
        <spanVDest name="dest1">
           <spanVEpgSummary name="summ1" dstIp="10.30.13.195" ttl="50" mtu="1500"
dscp="2"/>
             </spanVDest>
    </spanVDestGrp>
    <infraAttEntityP name="test-lvspan">
    <infraRsDomP tDn="uni/vmmp-VMware/dom-mininet"/>
 </infraAttEntityP>
 </infraInfra>
 </polUni>
```



第 7 章

# BPDU の機能

この章の内容は、次のとおりです。



## ブリッジ プロトコル データ ユニット機能の概要

この項では、Cisco APIC を備えた Cisco ACI Virtual Edge 上でサポートされるブリッジ プロトコル データ ユニット（BPDU）機能について説明します。BPDU ガードおよびBPDU フィルタリングはスイッチ全体の機能であり、VM 仮想イーサネット (vEth) ポートにのみ適用されます。

### BPDU ガード

BPDU ガードは、非トランキング ポートで BPDU が受信されたときにそのポートをエラー無効状態に移行させることにより、ループを防止します。スイッチでBPDUガードを有効にすると、インターフェイスが、BPDU の受信に関してブロッキング状態に移動されます。

BPDU ガードにより、管理者は手動でインターフェイスを再び動作させなければならないので、無効な設定に対する確実な対処が可能になります。インターフェイスをサービス状態に戻すには、VM ポートを切断し Cisco ACI Virtual Edge に再度接続するか、vCenter を介して EPG ポート グループに再接続します。

### BPDU フィルタリング

BPDU フィルタリングは、ポート上での BPDU の送受信を防止します。受信した BPDU は、フィルタ リングが有効になっているときに廃棄されます。BPDUフィルタリングは、デフォルトですべてのポート上で有効になっています。この機能を有効にすると Cisco ACI Virtual Edge アップリンク ポートで受信したすべての Bpdu をドロップします。

（注） 単一ポリシー インターフェイス グループで BPDU ポリシーを設定することをお勧めします。複数のポリシー インターフェイス グループで BPDU を設定すると、整合性のない動作につながります。

（注） L2 スイッチ拡張トポロジでは、添付されているエンティティ プロファイル vSwitch ポリシー オーバーライドを介して BPDU ポリシーを設定することをお勧めします。インターフェイス ポリシー グループの設定を使用すると、BPDU Guard またはフィルタが有効でリーフ ポート。これにより、これらのポートを error-disable L2 スイッチから BPDU パケットを受信するとします。

オーバーライド ポリシー経由で BPDU ポリシーの設定については、」の変更、インターフェイス ポリシー グループ vSwitch 側ポリシーをオーバーライドする」セクションを参照してください、 *Cisco* アプリケーション仮想エッジ *Installation guide* 』 。

# GUI を使用した BPDU 機能の設定

**手順**

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** メニュー バーで、[Fabric] > [Access Policies] を選択します。

**ステップ 3** **Policies** ナビゲーション ウィンドウで、 **Policies** および **Interface** フォルダを展開します。

**ステップ 4** [Spanning Tree Interface] フォルダを右クリックして、[Create Spanning Tree Interface Policy] を選択します。

**ステップ 5** **Create Spanning Tree Interface Policy** ダイアログで、次の手順に従います:

a) [Name] フィールドにポリシーの名前を入力します。
b) （任意）[Description] フィールドに、ポリシーの説明を入力します。
c) **Interface controls** エリアで、**BPDU Guard enabled** チェック ボックスまたは **BPDU filter enabled** チェック ボックスをオンにします。
d) **Submit** をクリックしてポリシーを保存します。

**ステップ 6** ステップ5で次の手順で作成したスパニングツリーインターフェイスポリシーを接続します。

a) 移動 **仮想ネットワーク** > **インベントリ** し、展開、 **VMM ドメイン** および **VMware** フォルダ。
b) ポリシーを接続する VMM ドメインをクリックします。
c) をクリックします **VSwitch ポリシー** 作業ウィンドウの右側にあるタブ。
d) **STP Policy** ドロップダウンリストから、ステップ 5 で作成したポリシーを選択します。
e) [Submit] をクリックします。

**ステップ 7** ESXi ハイパーバイザへの ESXi CLI セッションを開き、**vemcmd show card** コマンドを入力して、設定を確認します。

**例：**

```
cisco-ave# vemcmd show card
Global BPDU Guard: Enabled && Global BPDU Filter: Enabled
```

この出力は、BPDU フィルタリングおよびBPDU ガードが有効になっているかどうかを示します。

# NX-OS スタイル CLI を使用した BPDU 機能の設定

**手順**

**ステップ 1** vmware-domain モードに入ります。

**例：**

```
apic1# configure
apic1(config)# vmware-domain domain name
AVE-Vlan  AVE2-VXLAN  Test  Test2
```

**ステップ 2** スパニングツリー インターフェイス ポリシーを作成します。

**例：**

```
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# spanning-tree
              bpdu-filter  bpdu-guard
apic1(config-vmware-ave)# spanning-tree
              bpdu-filter  Configure BPDU filter override on AVE uplink ports
              bpdu-guard   Configure BPDU guard override on AVE uplink ports
```

**ステップ 3** BPDU フィルタを有効または無効にします。

**例：**

```
apic1(config-vmware-ave)# spanning-tree bpdu-filter
                 default  disable  enable
apic1(config-vmware-ave)# spanning-tree bpdu-filter
                 default  Remove BPDU filter/guard override policy
                 disable  Disable BPDU filter
                 enable   Enable BPDU filter
```

**ステップ 4** BPDU ガードを有効または無効にします。

```
apic1(config-vmware-ave)# spanning-tree bpdu-guard
               default  disable  enable
```

# REST API を使用した BPDU 機能の設定

手順

ステップ 1 BPDU ガードを設定します。

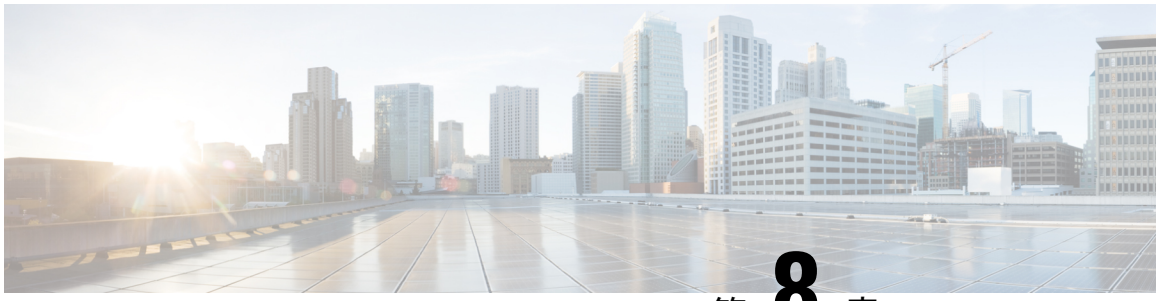
例：

```
<polUni>
  <infraInfra>
      <stpIfPol name="testStp5" ctrl="bpdu-guard"/>
      <infraFuncP>
        <infraAccBndlGrp name="test51">
        <infraRsStpIfPol tnStpIfPolName="testStp5"/>
        <infraRsAttEntP tDn="uni/infra/attentp-test-bpdu"/>
        </infraAccBndlGrp>
      </infraFuncP>
  </infraInfra>
</polUni>


<vmmProvP vendor="VMware">
     <vmmDomP name="mininet">
        <vmmVSwitchPolicyCont>
           <vmmRsVswitchOverrideStpPol tDn="uni/infra/ifPol-testStp5"/>
        </vmmVSwitchPolicyCont>
     </vmmDomP>
</vmmProvP
```

ステップ 2 BPDU フィルタリングを設定します。

例：

```
<polUni>
  <infraInfra>
      <stpIfPol name="testStp5" ctrl="bpdu-filter"/>
      <infraFuncP>
        <infraAccBndlGrp name="test51">
        <infraRsStpIfPol tnStpIfPolName="testStp5"/>
        <infraRsAttEntP tDn="uni/infra/attentp-test-bpdu"/>
        </infraAccBndlGrp>
      </infraFuncP>
 </infraInfra>
</polUni>

<vmmProvP vendor="VMware">
     <vmmDomP name="mininet">
        <vmmVSwitchPolicyCont>
           <vmmRsVswitchOverrideStpPol tDn="uni/infra/ifPol-testStp5"/>
        </vmmVSwitchPolicyCont>
     </vmmDomP>
</vmmProvP>
```



第 8 章

# IGMP クエリアとスヌーピング

この章の内容は、次のとおりです。



# IGMPスヌーピングおよびクエリアの設定に関するガイドラインおよび制約事項

設定に応じて、IGMP をレイヤ 2 スイッチ上、またはインフラ テナントまたは管理者作成のテナントブリッジドメイン上に設定する必要がある場合があります。このセクションでは、IGMP プロトコル スヌーピングおよびクエリアを設定する必要がある場合の 2 つの一般的なシナリオのガイドラインについて説明します。

（注） Cisco ACI Virtual Edgeは IGMP スヌーピングをサポートしていません。このセクションでの IGMP スヌーピングのガイドラインと制限事項および設定手順は、リーフ スイッチで IGMP スヌーピングを設定するためのものです。

### VXLAN カプセル化トラフィックのマルチ宛先フラッド

VXLAN でカプセル化されたトラフィックに対して Cisco ACI Virtual Edge でマルチ宛先フラッドを受信し、リーフと Cisco ACI Virtual Edge の間にレイヤ 2 デバイスがある場合、Cisco ACI Virtual Edge から発信され、終端するマルチキャスト フラッディング トラフィックを最小限に抑えるには、次を行います。

- IGMP スヌーピング ポリシーを適用し、Cisco APIC を介してインフラ テナント ブリッジ ドメイン サブネット上で IGMP クエリアをイネーブルにします。このガイドのGUI を使用した IGMP クエリアの設定 （54 ページ）セクションの手順を参照してください。
- リーフと Cisco ACI Virtual Edge 間の各レイヤ 2 デバイス上で IGMP スヌーピングを有効にします。デバイスに固有の手順に従ってください。たとえば、レイヤ 2 デバイスが Cisco Nexus 5000 シリーズ スイッチの場合、そのスイッチのコンフィギュレーション ガイドの手順を参照してください。

### 仮想マシンでのマルチキャスト ストリームの送信または受信

Cisco ACI Virtual Edge に接続された仮想マシンがあり、マルチキャスト ストリームを送信または受信する場合は、次の手順を実行します。

- IGMP スヌープ ポリシーを適用し、管理者が作成したテナント ブリッジ ドメインに対して IGMP クエリアを有効にします。管理者が作成したテナントブリッジドメインが複数ある場合は、IGMP スヌープ ポリシーを適用し、Cisco APIC を介して各管理者が作成したテナントブリッジ ドメインに IGMP クエリアを設定する必要があります。このガイドのGUI を使用した IGMP クエリアの設定 （54 ページ）セクションの手順を参照してください。
- リーフと Cisco ACI Virtual Edge 間の各レイヤ 2 デバイス上で IGMP スヌーピングをイネーブルにします。デバイスに固有の手順に従ってください。たとえば、レイヤ 2 デバイスが Cisco Nexus 5000 シリーズ スイッチの場合、そのスイッチのコンフィギュレーション ガイドの手順を参照してください。
- VM から開始または VM で終了するマルチキャスト トラフィックが VXLAN カプセル化される場合、この項および前の項のすべてのガイドラインに従ってください。

### 設定の順序

IGMP スヌーピングを設定する前に、IGMP クエリアを設定します。

# GUI を使用した IGMP クエリアの設定

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** テナントのタイプに応じて、次の一連の手順のいずれかを実行します。

| 次を有する場合： | 結果 |
| --- | --- |
| テナント インフラ | **1.** [Tenants] > [infra] を選択します。<br>**2.** ナビゲーション ウィンドウで次のフォルダを開きます。**[Networking]** > **[Bridge Domains]** > **[default]** > **[Subnets]**。<br>**3.** [Subnets] フォルダでサブネットを選択します。<br>**4.** [Properties] 作業ペインの [Subnet Control] エリアで、[Querier IP] チェックボックスがオンになっていることを確認します。<br>**5.** [Submit] をクリックします。 |
| 管理者が作成したテナント | **1.** [Tenants] を選択し、IGMP クエリアを設定するテナントを選択します。<br>**2.** テナント ナビゲーション ウィンドウで [Networking] フォルダ、[Bridge Domains] フォルダ、テナントに以前作成したブリッジ ドメインのフォルダを開きます。<br>選択したブリッジ ドメインにすでにゲートウェイの IP が紐づいたサブネットがある場合、それを使用して [Subnet Control] エリアで IGMP クエリアを有効にできます。または、残りの手順を実行して新しいサブネットを作成し、IGMP クエリアを有効にできます。<br>**3.** ブリッジ ドメイン フォルダ内の [Subnets] フォルダを右クリックし、[Create Subnet] を選択します。<br>**4.** [Create Subnet] ダイアログ ボックスで、次の手順を完了します。<br>**1.** ゲートウェイの IP アドレスを指定します。<br>（注） Cisco APIC ファブリック デバイスに対して予約されている 10.0.0.0/16 ネットワークからのものを除き、任意の IP アドレスを設定できます。<br>**2.** [Subnet Control] エリアで、[Querier IP] チェック ボックスがオンになっていることを確認します。<br>**3.** [Submit] をクリックします。 |

# NX-OS スタイル CLI を使用した IGMP クエリアの設定

**手順**

IGMP クエリアを設定します。

**例：**

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ip address <192.168.1.1/24> snooping-querier
 <CR>
multi-site  Set the address as multi-site address
scope       Scope of the address among ['public', 'private']
secondary   Set the address as secondary address
```

# REST API を使用して、ブリッジ ドメイン サブネット上の IGMP クエリアを有効にする

**手順**

ブリッジ ドメイン サブネット上で IGMP クエリアを有効にします。

**例：**

```
<fvTenant name="ms10">

<fvCtx name="msv10"/>

<fvBD name="msb10">
  <fvSubnet ctrl="querier" descr="" ip="1.1.9.1/24" name="" nameAlias=""
preferred="no" scope="private" virtual="no"/>
  <fvRsCtx tnFvCtxName="msv10"/>

</fvBD></fvTenant>
```

# GUI を使用して IGMP スヌーピングをすぐに有効にする

**手順**

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** 次のいずれかを実行します。

- インフラ テナントがある場合には、[Tenants] > [infra] を選択します。
- 管理者作成のテナントがある場合には、[Tenants] を選択し、IGMP スヌーピングを設定するテナントを選択します。

**ステップ 3** テナント ナビゲーション ウィンドウで次のアクションのいずれかを実行します:

- インフラ テナントがある場合には、[Networking] フォルダを開き、[Bridge Domains] フォルダを開き、[default] フォルダを選択します。
- 管理者作成のテナントがある場合には、[Networking] フォルダを開き、[Bridge Domains] フォルダを開き、テナントに対して前に作成したブリッジ ドメインを選択します。

**ステップ 4** [Properties] 作業ウィンドウで、[IGMP Snoop Policy] ドロップダウン リストから [Create IGMP Snoop Policy] を選択します。

**ステップ 5** [Create IGMP Snoop Policy] ダイアログボックスで、次の手順を実行します。

a) [Name] フィールドにポリシーの名前を入力します。
b) [Control] 領域で、[Enable querier] チェックボックスをオンにします。
c) （任意）他の関連する IGMP パラメータを設定します。
d) [Submit] をクリックします。

**ステップ 6** [Properties] ペインで [Submit] をクリックします。

# NX-OS スタイル CLI を使用してすぐに有効になるように IGMP スヌーピングを設定する

**手順**

すぐに有効になるように IGMP スヌーピングを設定する

**例：**

```
apic1# configure
apic1(config)# tenant t1
```

```
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ip igmp snooping querier
```

# GUIを使用してIGMPスヌーピングを後で有効になるように設定する

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** 次のいずれかを実行します。

- インフラ テナントがある場合には、[Tenants] > [infra] を選択します。
- 管理者作成のテナントがある場合には、[Tenants] を選択し、IGMP スヌーピングを設定するテナントを選択します。

**ステップ 3** テナント ナビゲーション ウィンドウで、[Policies] と [Protocol] フォルダを開きます。

**ステップ 4** [IGMP Snoop] フォルダを右クリックし、[Create IGMP Snoop Policy] を選択します。

**ステップ 5** [Create IGMP Snoop Policy] ダイアログボックスで、次の手順を実行します。

a) [Name] フィールドにポリシーの名前を入力します。
b) [Control] 領域で、[Enable querier] チェックボックスをオンにします。
c) （任意）他の関連する IGMP パラメータを設定します。
d) [Submit] をクリックします。

### 次のタスク

一度IGMPスヌーピングを設定すると、次の手順を完了することで、ブリッジドメインにいつでも適用できます。

1. 次のいずれかを実行します。
   - インフラ テナントがある場合には、[Tenants] > [infra] を選択します。
   - 管理者作成のテナントがある場合には、[Tenants] を選択し、IGMP スヌーピングを設定するテナントを選択します。
2. [Tenant] ナビゲーション ウィンドウで次のアクションのいずれかを実行します。
   - インフラテナントがある場合、[+]アイコンをクリックして[Networking]および[Bridge Domain] フォルダを開き、[default] フォルダを選択します。

- 管理者作成のテナントがある場合には、[Networking] および [Bridge Domain] フォルダを開き、テナントに対して前に作成したブリッジ ドメインを選択します。

3. [Properties] ペインの [IGMP Snoop Policy] ドロップダウン リストで、適用する IGMP スヌーピング ポリシーを選択します。
4. ブリッジ ドメインに対して有効になる IGMP ポリシーに対して [Submit] をクリックします。

# NX-OS スタイル CLI を使用して後ほど有効になるように IGMP スヌーピングを設定する

**手順**

後で有効になるように IGMP スヌーピングを設定します。

**例：**

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# template ip igmp snooping policy <foo_igmp>
apic1(config-tenant-template-ip-igmp-snooping)# ip igmp snooping querier
```

# REST API を使用したIGMP スヌーピング ポリシーの設定

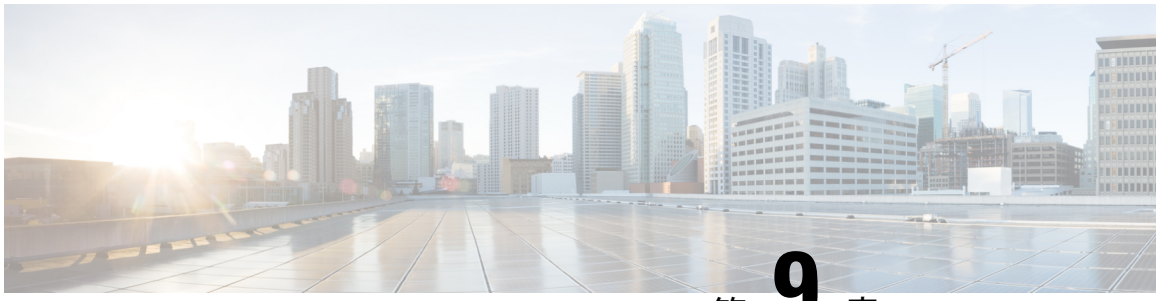
**手順**

IGMP スヌーピング ポリシーを作成し、ブリッジ ドメインに適用します。

**例：**

```
<igmpSnoopPol name="igmp_snp_bd_21"
              adminSt="enabled"
              ctrl="fast-leave,querier"
              lastMbrIntvl="1"
              queryIntvl="125"
              rspIntvl="10"
              startQueryCnt="2"
              startQueryIntvl="31"
              />
<fvCtx name="msv10"/>

<fvBD name="msb10">
  <fvRsCtx tnFvCtxName="msv10"/>
```

```
  <!-- Bind IGMP snooping to a BD -->
  <fvRsIgmpsn tnIgmpSnoopPolName="igmp_snp_bd_21"/>
</fvBD></fvTenant>
```



第 9 章

# Cisco ACI Virtual Edge での vMotion

この章の内容は、次のとおりです。



## Cisco ACI Virtual Edge で VMware vMotion を使用する際のガイドライン

Cisco ACI Virtual Edge VM を VMware vMotion で移動することはできませんが、同じホスト上のゲスト VM は vMotion で移動することができます。Cisco ACI Virtual Edge と同じホストを共有しているゲスト VM で vMotion を使用することに関する、このセクションのガイドラインに従ってください。

### vMotion の設定

ネイティブなスイッチング モードを使用していて、単独の EPG を有する個別の VMkernel NIC 上で vMotion を設定することを推奨します。

### クロス VMware vCenter vMotion のサポート

Cisco ACI Virtual Edge のための Cisco ACI によるマイクロセグメンテーションは、クロス VMware vCenter およびクロス VDS vMotion でサポートされます。

（注） エンドポイントに対して VMware vCenter vMotion を行うと、数秒間トラフィックが失われる可能性があります。

### クロス VMware vCenter および クロス VDS vMotion に関するガイドライン

• 送信元および宛先の VMware vCenter Server インスタンスと ESXi は 6.0 以降のバージョンを実行している必要があります。

- 送信元と宛先の vSphere Distributed Switch（VDS）のバージョンは同じである必要があります。
- クロス VDS および クロス VMware vCenter vMotion の前提条件については、VMware のマニュアルを参照してください。

### Cisco ACI Virtual Edge での vMotion のサポート

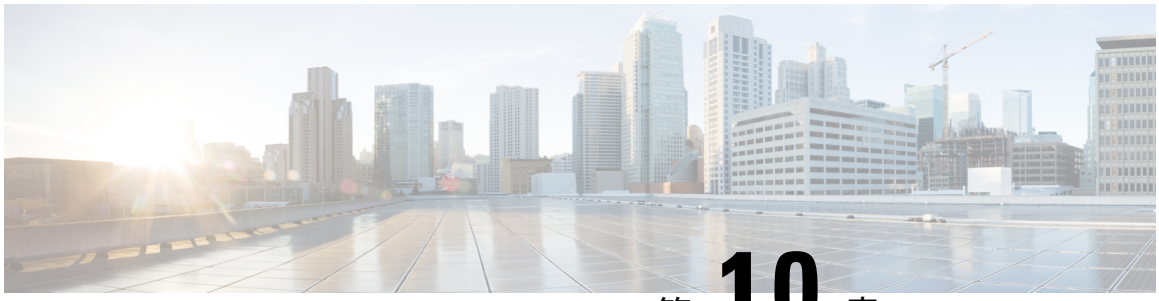
Cisco ACI Virtual Edge は、Cisco ACI Virtual Edge ドメインで分散ファイアウォールが有効になっていない場合に、クロス VMware vCenter および クロス DVS をサポートします。分散ファイアウォールが有効になっているときには、vMotion に対して次の制限がかかることに注意してください:

表 *1:* 分散ファイアウォールが有効になっている場合の *vMotion*

| vMotion のタイプ | VMM 内 (DVS 内) | VMM 間 (クロス DVS) |
|---|---|---|
| クロス vCenter | サポートあり | サポートあり |
| 単一 vCenter | サポートあり | サポートあり |
| クロス Cisco ACI マルチサイト | サポート対象外 | サポート対象外 |

### クロス データセンター VMware vMotion の後の古い VM エントリ

同じ VMware vCenter 内でクロス データセンター VMware vMotion を使用して VM を移行した場合、ソース側の DVS に古い VM エントリが残る場合があります。この古いエントリは、ホストの削除の失敗などの問題の原因となる可能性があります。この問題の回避策は、vNetwork DVS で「ポートの状態のモニタリングを開始」を有効にすることです。手順については、VMware の Web サイトの KB トピック、「Refreshing port state information for a vNetwork Distributed Virtual Switch」を参照してください。



第 10 章

# 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、EPG 内のエンドポイントを相互に分離することもできます。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 EPG 内のすべてのエンドポイントに分離を設定するか、どれにも設定しないことができます。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は設定しないことはできません。

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契約には影響しません。

（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。したがって、EPG 内分離が設定されている複数の EPG 間での、サブネット内の通信は、これらの Cisco ACI Virtual Edge EPG の間に契約が結ばれている場合でも不可能です。(VXLAN)。

• GUI を使用した Cisco ACI Virtual Edge の EPG 内分離の設定 （64 ページ）

# 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 [テナント] 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 （67 ページ） と 分離されたエンドポイントの統計情報を表示 Cisco ACI Virtual Edge [テナント] タブ （68 ページ） を参照してください。

# 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

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 アドレスのプールに、VXLAN に関連する設定に存在するかどうかを確認します。

### 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 [テナント] 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 （67 ページ） と 分離されたエンドポイントの統計情報を表示 Cisco ACI Virtual Edge [テナント] タブ （68 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 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** 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 [テナント] 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 （67 ページ） と 分離されたエンドポイントの統計情報を表示 Cisco ACI Virtual Edge [テナント] タブ （68 ページ） を参照してください。

# Cisco ACI 仮想エッジ上の分離エンドポイントの統計情報を選択する

# [テナント] 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** [Submit] をクリックします。

# [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** [Submit] をクリックします。

# Cisco ACI 仮想エッジ上の分離エンドポイントの統計情報を表示する

# 分離されたエンドポイントの統計情報を表示 Cisco ACI Virtual Edge [テナント] タブ

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 [テナント] 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 （67 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 [テナント] 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 （67 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。

第 11 章

# 分散ファイアウォール

この章の内容は、次のとおりです。



## 分散ファイアウォールについて

分散ファイアウォールは、ハードウェア支援によるファイアウォールです。これは、Cisco適応型セキュリティ仮想アプライアンス (ASAv) などの Cisco Application Centric Infrastructure (ACI) ファブリック、または Microsegmentation によって Cisco ACI Virtual Edge で作成されたセキュア ゾーンなどのセキュリティ機能を補完しますが、これに代わるものではありません。

分散ファイアウォールが機能するために他のソフトウェアは必要ありません。ただし、分散ファイアウォールを使用するように Cisco Application Policy Infrastructure Controller (APIC) にポリシーを設定する必要があります。

分散ファイアウォールはすべての仮想イーサネット (vEth) ポートでサポートされていますが、kni-opflex、kni-ave-ctrl dpdk インターフェイス、およびすべてのアップリンクポートでは無効です。

### 分散ファイアウォールの主な機能

| 機能 | 説明 |
|---|---|
| ダイナミック パケット フィルタリング (別名ステートフル インスペクション) を提供 | TCP 接続および FTP 接続の状態を追跡し、既知のアクティブ接続と一致しないパケットをブロックします。インターネットまたは内部ネットワークからのトラフィックは、APIC GUI で設定するポリシーに基づいてフィルタリングされます。 |

| 機能 | 説明 |
| --- | --- |
| 分散型 | vMotion を使用して仮想マシン (VM) を他のサーバーに移動した場合でも、接続を追跡します。 |
| SYN ACK 攻撃を阻止 | プロバイダー VM が SYN-ACK パケットを開始した場合、プロバイダー Cisco ACI Virtual Edge 上の分散ファイアウォールでは、対応するフロー (接続) が作成されていないためこれらのパケットをドロップします。 |
| TCP フロー エージングをサポート | ESTABLISHED 状態の接続は、ポート単位の制限が 75 % のしきい値に達しない限り 2 時間維持されます。このしきい値に達すると、新しい接続によって古い接続 (5 分間以上非アクティブ) が置き換えられる可能性が生じます。<br>ESTABLISHED TCP 以外の状態の接続は、アイドルまたは非アクティブの時間で 5 分間保持されます。 |
| レベル フローに実装される | TCP 接続上の VM 間のフローを有効にして、パケットごとに TCP/IP 接続を確立する必要性を排除します。 |
| 特定のトポロジや設定に依存しない | ローカル スイッチング モードとローカル スイッチングなしモードのいずれかで動作し、VLAN と VXLAN のいずれかを使用します。 |
| ハードウェア アシスト型 | ACI ファブリックでは、Cisco Nexus 9000 リーフ スイッチにポリシーが保存され、パフォーマンスへの影響が回避されます。 |
| 5 タプル値上の実装に基づく | 送信元と宛先の IP アドレス、送信元と宛先のポート、およびプロトコルを使用してポリシーを実装します。 |
| デフォルトで学習モード | アップグレードを容易にします。Cisco AVS のバージョンがリリース5.2 (1) SV3 (1.5) より前の場合、Cisco AVS から Cisco ACI Virtual Edge に移行する場合、分散ファイアウォールはラーニング モードになっている必要があります。これらのバージョンは、分散ファイアウォールをサポートしていません。 |

# 分散ファイアウォールの利点

ここでは、Cisco ACI ファブリックで分散ファイアウォールがハードウェアと連携してセキュリティを提供する方法の例を示します。

### 再帰 ACL のセキュリティ強化

管理者は、コンシューマ EPG とプロバイダー EPG 間の Cisco APIC で、サブジェクトとフィルタを使用して契約を作成し、Web トラフィックを許可します。管理者は Cisco APIC で、任意の送信元ポートから宛先ポート 80 へのトラフィックを許可するポリシーを作成します。

Cisco APIC でポリシーが設定されている場合、プロバイダーからコンシューマへの再帰アクセス コントロール リスト（ACL）エントリが、ACI ハードウェアで自動的にプログラムされます。この再帰 ACL は、接続が確立されている間のリバース トラフィックを可能にするために作成されます。リバース トラフィックをフローさせるには、この再帰 ACL エントリが必須です。

自動再帰 ACL の作成により、接続が確立された状態になっている場合、リーフ スイッチはプロバイダーの任意のクライアント ポートへの接続を許可します。しかし、一部のデータセンタでは、これが望ましくない場合があります。プロバイダー EPG のエンドポイントが、送信元ポート 80 を使って、コンシューマ EPG のエンドポイントに SYN 攻撃またはポート スキャンを開始する可能性があるためです。

ただし、分散ファイアウォールは物理ハードウェアを使用して、このような攻撃は許可しません。物理リーフ ハードウェアは、ハイパーバイザから受信したパケットをポリシー Ternary Content Addressable Memory（TCAM）エントリに照らして評価します。

### VM が vMotion によって移動される場合のデータの保護

送受信されるすべてのパケットは、Cisco ACI Virtual Edge および物理リーフの分散ファイアウォールのフローベース エントリに従います。フローは仮想マシン（VM）の仮想イーサネット（vEth）インターフェイスに直接接続されるため、VM が vMotion によって別のハイパーバイザ ホストに移動されても、フローとテーブル エントリはそれとともに新しいハイパーバイザに移動します。

この移動は、物理リーフにも報告されます。物理リーフは正当なフローの続行を許可し、発生した場合に攻撃を阻止します。したがって、VM が新しいホストに移動しても、VM は保護を失わずに通信し続けます。

### シームレスな FTP トラフィック処理

FTP プロトコルの動作およびインターワーキングは、他の TCP ベースのプロトコルとは異なります。このため、分散ファイアウォールでは特別な処理が必要です。FTP サーバ（プロバイダー）は制御ポート（TCP ポート 21）とデータ ポート（TCP ポート 20）でリッスンします。FTP クライアント（コンシューマ）とサーバ（プロバイダー）間で通信が開始されると、FTP クライアントとサーバ間で初期的に接続制御が設定されます。データ接続はオンデマンドで設定され（交換するデータがある場合のみ）、データ転送後にただちに破壊されます。

分散ファイアウォールは、アクティブFTPモードの処理のみをサポートします。パッシブFTPモードのデータ接続は追跡されません。

分散ファイアウォールは、制御接続ハンドシェイク中に受信したFTPクライアントIPおよびポート情報と一致する場合にのみ、FTPデータ接続を許可します。対応する接続制御がない場合、分散ファイアウォールはFTPデータ接続をブロックし、これによりFTP攻撃が阻止されます。

# 分散ファイアウォールの設定

3つのモードのいずれかに設定することで、分散ファイアウォールを設定します。

- 有効：分散ファイアウォールを適用します。
- 無効：分散ファイアウォールを適用しません。このモードは、分散ファイアウォールを使用しないときにのみ使用します。分散ファイアウォールを無効にすると、Cisco ACI Virtual Edgeのすべてのフロー情報が削除されます。
- 学習： Cisco ACI Virtual Edgeはすべての TCP 通信を監視し、フロー テーブルにフローを作成しますが、ファイアウォールは適用しません。学習がデフォルトのモードです。

分散ファイアウォールは、Cisco APICで作成されたポリシーに従って動作します。ポリシーを作成していないと、分散型ファイアウォールは効率的に作業することができません。

（注） 分散ファイアウォールを使用する際は、VMにvmxnet3アダプタを使用することが推奨されます。

重要 Cisco ACI Virtual Edge VMMドメインで分散ファイアウォールを有効にすると、vMotionは制限を受けます。詳細については、このガイドの Cisco ACI Virtual Edge で VMware vMotion を使用する際のガイドライン （61 ページ） に関する項を参照してください。

# 分散ファイアウォールの設定のワークフロー

このセクションでは、分散ファイアウォールを設定するために実行するタスクの概要を説明します。

1. インターフェイス ポリシー グループを作成して、Cisco APICでファイアウォール ポリシーを有効にします。または、インターフェイス ポリシー グループがすでに存在する場合は、ファイアウォール ポリシーが含まれていることを確認します。
2. 分散ファイアウォールのステートフル ポリシーを設定します。

このガイドの「GUI を使用した分散ファイアウォールのステートフル ポリシーの設定 （75 ページ）」のセクションの手順に従います。

3. 必要に応じて分散ファイアウォール モードを変更します。

   デフォルトでは、分散ファイアウォールは学習モードになっています。以前に分散ファイアウォールを有効にしていなかった場合には、このガイドでの手順を実行して、分散ファイアウォール モードを変更します。

4. Cisco ACI Virtual Edge は、分散ファイアウォールによって許可または拒否されたフローを、システム ログ（syslog）サーバに報告します。フローのパラメータを設定して、拒否されたフローを syslog サーバで確認できます。このガイドの「分散ファイアウォール フロー ロギング （80 ページ）」のセクションの手順を参照してください。

5. 表示する分散ファイアウォールのフロー数統計情報を選択します。

   Cisco ACI Virtual Edge は分散ファイアウォール フロー情報を収集しますが、それらを表示するには、必要な統計情報を選択する必要があります。手順については、このガイドの「分散ファイアウォール フローの数 （89 ページ）」のセクションを参照してください。

# GUI を使用した分散ファイアウォールのステートフル ポリシーの設定

分散ファイアウォールのポリシーを構成する前に、分散ファイアウォールのステートフルポリシーを設定します。

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** **[Tenants]** > ***[tenant]*** の順に選択します。

**ステップ 3** ナビゲーション ウィンドウでテナントのフォルダを展開します。

**ステップ 4** [Contracts] フォルダを右クリックして [Create Contract] を選択します。

**ステップ 5** [Create Contract] ダイアログボックスで、[Name] フィールドに、契約の名前を入力します。

**ステップ 6** [Subjects] 領域で、[+] アイコンをクリックします。

**ステップ 7** [Create Contract Subject] ダイアログボックスで、[Name] フィールドにサブジェクトの名前を入力します。

**ステップ 8** [Filter Chain] エリアで、[+] アイコンをクリックします。これは [Filters] の隣にあります。

**ステップ 9** 下向き矢印をクリックして [Name] ドロップダウン フィルタ リストを表示し、[Name] リスト上部の [+] アイコンをクリックします。

**ステップ 10** [Create Filter] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドにフィルタの名前を入力します。
b) [Entries] エリアで、[+] アイコンをクリックして、追加フィールドを表示します。
c) [Name] フィールドに、フィルタを詳しく説明する名前を入力します。
d) [Ether Type] ドロップダウン リストで、[IP] を選択します

e) [IP Protocol] フィールドで [tcp] を選択します。
f) [Stateful] チェックボックスをオンにします。
g) (オプション) [Source Port / Range] フィールドで、[To] および [From] のドロップダウン リストから、デフォルトである [Unspecified] を選択します。
h) [Destination Port / Range] フィールドで、[To] および [From] のドロップダウン リストから [http] を選択します。
i) [Update] をクリックし、 [Submit] をクリックします。

**ステップ 11** [Create Contract Subject] ダイアログ ボックスの [Filters] エリアで、[Update] をクリックし、[OK] をクリックします。

**ステップ 12** [Create Contract] ダイアログ ボックスで、[Submit] をクリックします。

### 次のタスク

分散ファイアウォール ポリシーを作成します。

# NX-OS スタイルの CLI を使用した分散ファイアウォールのステートフル ポリシーの設定

### 手順

Cisco APIC でステートフル ポリシーを設定します。

**例：**

```
apic1(config)# tenant Tenant1
apic1(config-tenant)# access-list TCP-511 apic1
apic1 (config-tenant-acl)# match icmp
apic1 (config-tenant-acl)# match raw TCP-511 dFromPort 443 dToPort 443 etherT ip prot 6
 stateful yes
apic1 (config-tenant-acl)# match raw tcp etherT ip prot 6 sFromPort 443 sToPort 443
stateful yes
apic1 (config-tenant-acl)# match raw tcp-22out dFromPort 22 dToPort 22 etherT ip prot 6
 stateful yes apic1(config-tenant-acl)# match raw tcp-all etherT ip prot 6 stateful yes

apic1(config-tenant-acl)# match raw tcp22-from etherT ip prot 6 sFromPort 22 sToPort 22
 stateful yes apic1(config-tenant-acl)# exit apic1(config-tenant)# contract TCP511
apic1(config-tenant-contract)# subject TCP-ICMP
apic1(config-tenant-contract-subj)# access-group TCP-511 both
apic1(config-tenant-contract-subj)# access-group arp both
apic1(config-tenant-contract-subj)#
```

### 次のタスク

分散ファイアウォール ポリシーを作成します。

# REST API を使用した分散ファイアウォールのステートフル ポリシーの設定

Cisco APIC でステートフル ポリシーを設定します。

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** https://*APIC-ip-address*/api/node/mo/.xml にポリシーをポストします。

**例**：

```
<polUni>
  <infraInfra>

    <nwsFwPol name="fwpol1" mode="enabled"/>    (enabled, disabled, learning)

    <infraFuncP>
        <infraAccBndlGrp name="fw-bundle">
            <infraRsFwPol tnNwsFwPolName="fwpol1"/>
            <infraRsAttEntP tDn="uni/infra/attentp-testfw2"/>
        </infraAccBndlGrp>
    </infraFuncP>

     <infraAttEntityP name="testfw2">
                <infraRsDomP tDn="uni/vmmp-VMware/dom-mininet"/>
     </infraAttEntityP>

  </infraInfra>

</polUni>
```

### 次のタスク

分散ファイアウォール ポリシーを作成します。

# GUI を使用した分散型ファイアウォール ポリシーの作成

分散ファイアウォール ポリシーは Cisco APIC GUI で作成できます。

### 始める前に

次のことは既に実行済みである必要があります:

- Cisco APIC に分散型ファイアウォール ポリシーを有効にするインターフェイス ポリシー グループを作成します。
- 分散ファイアウォールのステートフル ポリシーを作成します。

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** [Fabric] > [Access Policies] の順に移動します。

**ステップ 3** [Policies] ナビゲーション ウィンドウで、[Policies] と [Interface] フォルダを開きます。

**ステップ 4** [Firewall] フォルダを右クリックして [Create Firewall Policy] を選択します。

**ステップ 5** [Create Firewall 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 6** [Mode] 領域で、モードを選択します。

アップグレードを容易にするため、デフォルトのモードは [Learning] になっています。

Release 5.2(1)SV3(1.5) 以前の Cisco AVS から Cisco ACI Virtual Edge に移行する場合には、分散ファイアウォールを [Learning] モードにしておく必要があります。これらのバージョンでは分散ファイアウォールをサポートしていません。

それ以外の場合には、分散ファイアウォールを有効にします。

（注） モードは、[Disabled] から [Enabled] に直接変更しないでください。直接変更すると、トラフィックが損失することがあります。代わりに、[Disabled] モードから [Learning] モードに変更し、5 分待ってから [Enabled] モードへ変更します。[Create Firewall Policy] ダイアログ ボックスには [Syslog] エリアがあります。ここでは、syslog サーバに送信される送信元の分散ファイアウォール フロー情報を設定できます。手順については、このガイドの 分散ファイアウォール フロー ロギング （80 ページ）を参照してください。

**ステップ 7** [Submit] をクリックします。

**ステップ 8** 次の手順を実行して、新しいポリシーを VMM ドメインに関連付けます。

a) **[Virtual Networking]** > **[Inventory]** に移動します。

b) [Inventory] ナビゲーション ウィンドウで、[VMM Domains] フォルダと [VMware] フォルダを展開し、関連する VMM ドメインを選択します。

c) VMM ドメインの作業ウィンドウで、[VSwitch Policies] タブをクリックします。

d) [Properties] 作業ウィンドウで、[Firewall Policy] ドロップダウン リストから、作成したファイアウォール ポリシーを選択します。

e) [Submit] をクリックします。

### 次のタスク

次の手順を実行して、分散ファイアウォールポリシーが作成され、目的の状態であることを確認します。

1. [Fabric] > [Access Policies] の順に移動します。

2. [Policies] ナビゲーション ウィンドウで、[Policies]、 [Interface]、および [Firewall] フォルダを展開します。
3. ポリシーを選択します。
4. [Properties] 作業ウインドウで、ポリシーが表示されることと、モードが正しいことを確認します。

# GUI を使用して分散型ファイアウォール ポリシーのモードを変更する

分散ファイアウォールのモードを変更するには、次の手順を実行します。

（注） Cisco AVS から Cisco ACI Virtual Edge に移行し、Cisco AVS では分散ファイアウォールを有効にしていなかった場合には、分散ファイアウォールを有効にします。

### 始める前に

分散型ファイアウォール ポリシーが VMM ドメインに関連付けられてい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** [Fabric] > [Access Policies] の順に移動します。

**ステップ 3** [Policies] ナビゲーション ウィンドウで、[Policies]、 [Interface]、および [Firewall] フォルダを展開します。

**ステップ 4** 変更するポリシーをクリックします。

**ステップ 5** [Properties] 作業ウィンドウの [Mode] エリアで、モードを選択し、[Submit] をクリックします。

（注） モードは、[Disabled] から [Enabled] に直接変更しないでください。直接変更すると、トラフィックが損失することがあります。代わりに、[Disabled] モードから [Learning] モードに変更し、5 分待ってから [Enabled] モードへ変更します。[Learning] モードへ変更することで、 Cisco ACI Virtual Edge により既存フローのフロー テーブル エントリが追加されます。

（注） [Properties] 作業ウィンドウには、[Syslog] エリアが含まれます。ここでは、syslog サーバに送信される送信元の分散ファイアウォールフロー情報を設定できます。手順については、このガイドの 分散ファイアウォール フロー ロギング （80 ページ）を参照してください。

### 次のタスク

次の手順を実行して、分散ファイアウォールが目的の状態であることを確認します。

1. [Policies] ナビゲーション ウィンドウで、[Firewall] フォルダのポリシーを選択します。
2. [Properties] ダイアログボックスで、モードが正しいことを確認します。

# NX-OS スタイル CLI を使用して分散型ファイアウォールを有効にするかモードを変更する

NX-OS スタイル CLI を使用して、ファイアウォールの配信を有効にするか、モードを変更することができます。

### 手順

分散ファイアウォールを有効にしたり、モードを変更します。

例：

```
apic1# configure
apic1(config)# vmware-domain Direct-AVE2-VXLAN
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# firewall mode < any of below 3>
disabled  Disabled mode
enabled   Enabled mode
learning  Learning mode
```

# 分散ファイアウォール フロー ロギング

Cisco APIC と分散ファイアウォールのフロー情報を表示して、ネットワーク セキュリティの監査をサポートできます。

Cisco ACI Virtual Edge は、分散ファイアウォールによって拒否または許可されたフローを、システム ログ（syslog）サーバに報告します。分散ファイアウォールを有効にすると Cisco ACI Virtual Edge はデフォルトで TCP、UDP、および ICMP トラフィックをモニタします。これはまた、TCP トラフィックの追跡とログ記録、そしてパラメータの設定によっては、TCP トラフィックの許可と拒否も行います。拒否されたフローと許可されたフローは、syslog サーバ上で表示できます。

## 分散ファイアウォールのフロー情報のパラメータ設定

Cisco ACI Virtual Edge は、分散ファイアウォールで拒否または許可されたフロー、および UDP および ICMP フローを、システム ログ（syslog）サーバに報告します。

GUI でリモート接続先と呼ばれる最大 3 つの syslog サーバの設定と、syslog ポリシーの設定の 2 つのタスクで分散ファイアウォールロギングを設定します。次のパラメータを設定できます:

- syslog サーバのパラメータ
  - 有効/無効

    （注） 分散ファイアウォールのロギングは、デフォルトでは無効化されています。

  - 許可フロー、拒否フロー、またはその両方
  - ポーリング間隔

    フローのエクスポート間隔は、60 秒から 24 時間に設定できます。

    （注） 最大スケールでデータを送信するには、ポーリング間隔を 125 秒に設定することが必要です。少なくとも 150 秒のポーリング間隔になるよう syslog タイマーを設定することをお勧めします。

  - ログの重大度

    重大度レベルは、0 ～ 7 に設定できます。

- syslog ポリシーのパラメータ
  - IP アドレス
  - ポート
  - ログの重大度

    重大度レベルは、0 ～ 7 に設定できます。

  - ログのファシリティ

Cisco ACI Virtual Edge は、ポーリング間隔ごとに、最大 250,000 の拒否されたフローまたは許可されたフローを syslog サーバに報告します。拒否フローおよび許可フローのロギングを選択した場合、Cisco ACI Virtual Edge は最大 500,000 個のフローを報告します。また、Cisco ACI Virtual Edge は最大 100,000 個の短時間フロー（ポーリング間隔よりも短いフロー）も報告します。

syslog メッセージは、syslog の宛先ログの重大度が syslog ポリシーの同じログの重大度以下である場合にのみ送信されます。syslog サーバと syslog ポリシーの重大度レベルは、次のとおりです。

- 0：緊急

- 1：アラート
- 2：クリティカル
- 3：エラー
- 4：警告
- 5：通知
- 6：情報
- 7：デバッグ

# syslog サーバの設定に関するガイドライン

Cisco ACI Virtual Edge に syslog サーバを設定する際は、この項のガイドラインに従います。

- syslog サーバは、Cisco ACI Virtual Edge ホスト管理ネットワークまたは Cisco ACI Virtual Edge インフラ ポート グループ (テナント インフラの overlay-1 vrf) から常にアクセス可能でなければなりません。

  syslog サーバが Cisco ACI Virtual Edge の後ろにある場合、インフラ ポート グループに VM VNIC を起動します。

- syslog サーバは常に、Cisco ACI Virtual Edge とは違うホストに存在する必要があります。

  Cisco ACI Virtual Edge から同じ Cisco ACI Virtual Edge の背後でホストされる syslog サーバにログ メッセージを送信することはサポートされません。

- syslog サーバの宛先が VM の場合、vMotion が無効化されていることを確認してください。syslog サーバの宛先 VM が、何らかの理由で別のホストに移動した場合、静的クライアントエンドポイント (CEP) がそれに応じて設定されていることを確認してください。このガイドのGUI を使用した静的エンド ポイントの設定 （84 ページ）セクションを参照してください。

  syslog サーバの IP は、DHCP (DHCP 中にオプション 61 が必要) またはスタティック設定を使用して取得できます。IP アドレスがインフラ ポート グループ内の他の EP と同じサブネットにあることを確認してください (テナント インフラの overlay-1 vrf)。

# 分散ファイアウォール フローの syslog メッセージ

ここでは、分散ファイアウォール フローの syslog メッセージの形式と例を示します。

- 拒否されたフロー
  - 書式

```
<Syslog Server timestamp>  < PRI = Facility*8 + Severity > <syslog version>
<Host timestamp> <Host IP>  <Application name (ave-dfwlog)> - AVE IP: <AVEIP>
AVE Hostname <hostname> DFWLOG-DENY_FLOW - <Deny Reason> AVE UUID: <UUID>, Source
 IP: <Source IP address>, Destination IP: <Destination IP address> , Source Port:
```

```
 <Port number>, Destination Port: <Port Number>, Source Interface: <Interface
name>, Protocol: "TCP"(6), Hit-Count = <Number of Occurrences>, EPG Name: <EPG
Name>, EpP DN: <EpP DN>
```

- 例

```
Thu Apr 21 14:36:45 2016 10.197.139.205 <62>1 2017-12-06T18:58:30.835
10.197.139.205 ave-dfwlog - AVE IP: 10.197.139.205  AVE Hostname localhost,
DFWLOG-DENY_FLOW - SYN ACK ingress AVE UUID: 42094298-4996-60EF-CE86-E2B7FC70C2EC,
 Source IP: 54.0.0.5, Destination IP: 54.0.0.6, Source Port: 53535, Destination
 Port: 5555, Source Interface: 00:50:56:89:4d:3e, Protocol: "TCP"(6), Hit-Count
 = 1, EPG Name = Tenant1|AP-1|EPG-54, EpP DN:
uni/epp/fv-[uni/tn-Tenant1/ap-AP-1/epg-EPG-54]
```

- 許可されたフロー
  - 書式

```
<Syslog server timestamp> < PRI = Facility*8 + Severity> <syslog version> <Host
 timestamp> <Host IP>  <Application name (ave-dfwlog)> - AVE IP: <AVEIP> AVE
Hostname <hostname> DFWLOG-PERMIT_FLOW -<flow status>  AVE UUID: <UUID>, Source
 IP: <Source IP address>, Destination IP: <Destination IP address>, Source Port:
 <Port Number>, Destination Port: <Port Number>, Source Interface: <Interface
name>, Protocol: "TCP"(6), Age = <Age in seconds>, EPG Name: <EPG Name>, EpP DN:
 <EpP DN>
```

  - 例

```
Tue Apr 19 19:31:21 2016 10.197.139.205 <62>1 2017-12-06T18:45:13.458
10.197.139.205 ave-dfwlog - AVE IP: 10.197.139.205  AVE Hostname localhost,
DFWLOG-PERMIT_FLOW - ESTABLISHED AVE UUID: 42094298-4996-60EF-CE86-E2B7FC70C2EC,
 Source IP: 54.0.0.5, Destination IP: 54.0.0.6, Source Port: 59846, Destination
 Port: 5001, Source Interface: 00:50:56:89:4d:3e, Protocol: "TCP"(6), Age = 0,
EPG Name = Tenant1|AP-1|EPG-54, EpP DN:
uni/epp/fv-[uni/tn-Tenant1/ap-AP-1/epg-EPG-54]
```

- 短時間許可されたフロー
  - 書式

```
<Syslog Server timestamp>  < PRI = Facility*8 + Severity > <syslog version>
<Host timestamp> <Host IP>  <Application name (ave-dfwlog)> - AVE IP: <AVEIP>
AVE Hostname <hostname> DFWLOG-PERMIT_SHORT_LIVED - <State of flow> AVE UUID:
<UUID>, Source IP: <Source IP address>, Destination IP: <Destination IP address>,
 Source Port: <Port Number>, Destination Port: <Port Number>, Source Interface:
 <Interface Name>, Protocol: "TCP"(6), Timestamp = <Host Timestamp>, EPG Name:
<EPG Name>, EpP DN: <EpP DN>
```

  - 例

```
Thu Apr 21 14:46:38 2016 10.197.139.205 <62>1 2017-12-06T18:59:37.702
10.197.139.205 ave-dfwlog - AVE IP: 10.197.139.205  AVE Hostname localhost,
DFWLOG-PERMIT_SHORT_LIVED - CLOSED AVE UUID: 42094298-4996-60EF-CE86-E2B7FC70C2EC,
 Source IP: 54.0.0.5, Destination IP: 54.0.0.6, Source Port: 59847, Destination
 Port: 5001, Source Interface: 00:50:56:89:4d:3e, Protocol: "TCP"(6), Timestamp
 = 2017-12-06T18:59:37.702, EPG Name = Tenant1|AP-1|EPG-54, EpP DN:
uni/epp/fv-[uni/tn-Tenant1/ap-AP-1/epg-EPG-54]
```

- ICMP モニター フロー
  - 書式

```
<Syslog server timestamp> < PRI = Facility*8 + Severity> <syslog version> <Host
 timestamp> <Host IP> <Application name (ave-dfwlog)> - AVE IP: <AVEIP> AVE
Hostname <hostname>
DFWLOG-ICMP_TRACKING - AVE UUID: <UUID>, Source IP: <Source IP address>,
Destination IP: <Destination IP address>, Type:<ICMP type field>, Source
Interface:
<Interface name>, Protocol: "ICMP"(1), Timestamp= <Host time stamp>, Direction:
 <Egress/Ingress>, EPG Name:<EPG Name>, EpP DN: <EpP DN>
```

- 例

```
2016-11-28 11:02:43 News.Info 10.197.139.205 2017-12-06T19:01:05.061
10.197.139.205 ave-dfwlog - AVE IP: 10.197.139.205  AVE Hostname localhost,
DFWLOG-ICMP_TRACKING AVE UUID: 42094298-4996-60EF-CE86-E2B7FC70C2EC, Source IP:
 54.0.0.5, Destination IP: 54.0.0.6, Icmp type and code: Echo request (8,0)
Source Interface: 00:50:56:89:4d:3e, Protocol: "ICMP"(1), Timestamp =
2017-12-06T19:01:05.061, Direction: Ingress, EPG Name = Tenant1|AP-1|EPG-54, EpP
 DN: uni/epp/fv-[uni/tn-Tenant1/ap-AP-1/epg-EPG-54]
```

- UDP モニター フロー
  - 書式

```
UDP:
<Syslog server timestamp> < PRI = Facility*8 + Severity> <syslog version> <Host
 timestamp> <Host IP> <Application name (ave-dfwlog)> - AVE IP: <AVEIP> AVE
Hostname <hostname> DFWLOG-UDP_TRACKING - AVE UUID: <UUID>, Source IP: <Source
IP address>, Destination IP: <Destination IP address>, Source Port: <Port Number>,
 Destination Port: <Port Number>, Source Interface: <Interface name>, Protocol:
 "UDP"(17), Timestamp=<Host timestamp>, Direction: <Egress/Ingress>, EPG Name:
<EPG Name>
```

  - 例

```
2016-11-28 11:00:23 News.Info 10.197.139.205 1 2017-12-06T19:01:46.785
10.197.139.205 ave-dfwlog - AVE IP: 10.197.139.205  AVE Hostname localhost,
DFWLOG-UDP_TRACKING AVE UUID: 42094298-4996-60EF-CE86-E2B7FC70C2EC, Source IP:
55.0.0.253, Destination IP: 55.0.0.5, Source Port: 67, Destination Port: 68,
Source Interface: 00:50:56:00:55:05, Protocol: "UDP"(17), Timestamp =
2017-12-06T19:01:46.785, Direction: Egress, EPG Name = Tenant1|AP-1|EPG-55, EpP
 DN: uni/epp/fv-[uni/tn-Tenant1/ap-AP-1/epg-EPG-55]
```

# GUI を使用した静的エンド ポイントの設定

**手順**

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** [Tenant infra] ナビゲーション ウィンドウで、**[Application Profiles]** > **[access]** > **[Application EPGs]** > **[default]**を開きます。

**ステップ 3** [Static EndPoint] フォルダを右クリックし、[Create Static EndPoint] を選択します。

**ステップ 4** [Create Static Endpoint] ダイアログボックスで、次の手順を実行します。

a) [MAC] フィールドに、syslog サーバの宛先の MAC アドレスを入力します。

b) [Type] 領域で、[tep] を選択します。

c) [Path Type] 領域で、適切なパス タイプを選択します。

パス タイプにより、リーフが syslog サーバの宛先に接続される方法が決定されます。リーフはポート、ダイレクト ポート チャネル、または仮想ポート チャネルによって接続できます。

d) [Port] を [Path Type] として選択した場合には、[Node] ドロップダウンリストからノードを選択します。

e) [Path] フィールドに適切なパスを入力します。

パスにより、syslog サーバの宛先がアタッチされるポリシー グループが決定されます。

f) [IP Address] フィールドに、syslog サーバの宛先の IP アドレスを入力します。

g) [Encap] フィールドに、overlay-1 VLAN（vlan-xxix）を入力します。

h) [Submit] をクリックします。

**ステップ 5** syslog サーバの宛先から、10.0.0.30 などのオーバーレイ IP アドレスに ping します。

この手順によって、ファブリックは syslog サーバの宛先の IP アドレスを学習します。

# GUI を使用した、分散ファイアウォール フロー情報のパラメータの設定

パラメータを設定するには、まず syslog サーバのパラメータを設定し、次に syslog ポリシーのパラメータを設定します。GUI では、syslog サーバは *Remote Destination* と呼ばれます。

### 始める前に

分散ファイアウォールを有効にしておく必要があります。

### 手順

**ステップ 1** Cisco APIC にログインします。

**ステップ 2** **[Admin]** > **[External Data Collectors]** に移動します。

**ステップ 3** [External Data Collectors] ナビゲーション ウィンドウで [Monitoring Destinations] フォルダを展開し、[Syslog] フォルダを選択します。

**ステップ 4** [Syslog] 作業ウィンドウで [ACTIONS] の下向き矢印をクリックし、[Create Syslog Monitoring Destination Group] を選択します。

**ステップ 5** [Create Syslog Monitoring Destination Group STEP 1 > Profile] ダイアログボックスで、次の手順を実行します。

a) [Define Group Name and Profile] 領域で、[Name] フィールドに名前を入力します。

b) [Admin State] 領域で、ドロップダウン リストから [enabled] が選択されていることを確認します。

c) 残りのダイアログ ボックスではデフォルトを受け入れて、[Next] をクリックします。

**ステップ 6** [Create Syslog Monitoring Destination Group STEP 2 > Remote Destinations] ダイアログボックスで、[+] アイコンをクリックします。

**ステップ 7** [Create Syslog Remote Destination] ダイアログボックスで、次の手順を実行します。

a) [Host] フィールドに、ホストの IP アドレスを入力します。
b) [Name] フィールドにホスト名を入力します。
c) [Admin State] 領域で、[enabled] が選択されていることを確認します。
d) [Format] 領域で、[aci] が選択されていることを確認します。
e) [Severity] ドロップダウン リストから、重大度を選択します。
f) 他のポートを使用している場合を除き、[Port] ドロップダウン リストから標準ポートを受け入れます。
g) [Forwarding Facility] ドロップダウン リストから、ファシリティを選択します。
h) [Management EPG] ドロップダウン リストを無視して、[OK] をクリックします。

**ステップ 8** （オプション）[Create Syslog Monitoring Destination Group STEP 2 > Remote Destinations] ダイアログ ボックスで、最大 2 つの追加のリモート宛先を作成します。

**ステップ 9** [Create Syslog Monitoring Destination Group STEP 2 > Remote Destinations] ダイアログボックスで、[FINISH] をクリックします。
新しく作成された宛先が、[External Data Collectors] ナビゲーション ウィンドウの [Syslog] フォルダに表示されます。

**ステップ 10** **[Fabric]** > **[Access Policies]** の順に選択します。

**ステップ 11** [Policies] ナビゲーション ウィンドウで、[Polices] と [Interface] フォルダを開きます。

**ステップ 12** 次のいずれかの手順を実行します。

| 実行する操作 | 結果 |
|---|---|
| 新しい分散ファイアウォール ポリシーでの syslog ポリシーの設定 | **1.** [Firewall] フォルダを右クリックして [Create Firewall Policy] を選択します。<br>**2.** [Create Firewall Policy] ダイアログボックスの [Specify the Firewall Policy Properties] 領域で、[Name] フィールドにポリシーの名前を入力します。<br>**3.** [Mode] 領域で、モードを選択します。<br>Release 5.2(1)SV3(1.5) 以前の Cisco AVS から Cisco ACI Virtual Edge に移行する場合には、分散ファイアウォールを [Learning] モードにしておく必要があります。これらのバージョンでは分散ファイアウォールをサポートしていません。<br>**4.** [Syslog] 領域で、[Administrative State] ドロップダウン リストから [enabled] が選択されていることを確認します。<br>**5.** [Included Flows] 領域で、[Permitted flows]、[Denied flows]、またはその両方を選択します。 |

| 実行する操作 | 結果 |
| --- | --- |
| | **6.** [Polling Interval (seconds)] 領域で、60 秒から 24 時間の間隔を選択します。<br>**7.** [Log Level] ドロップダウン リストから、重大度レベルを選択します。<br>ロギング重大度レベルは、syslog サーバに定義された重大度レベルと同じか、それ以上である必要があります。重大度については、このガイドの分散ファイアウォールのフロー情報のパラメータ設定 （80 ページ）を参照してください。<br>**8.** [Dest Group] ドロップダウン リストから、作成したばかりの宛先グループを選択します。<br>**9.** [Submit] をクリックします。<br>**10.** [What To Do Next] セクションに移動し、VMM ドメインに新しい分散ファイアウォール ポリシーを関連付けます。 |
| 既存の分散ファイアウォール ポリシーでの syslog ポリシーの設定 | **1.** [Firewall] フォルダを展開し、変更する分散ファイアウォール ポリシーを選択します。<br>**2.** ポリシー作業ペインで、必要に応じて [Mode] を変更します。<br>Release 5.2(1)SV3(1.5) 以前の Cisco AVS から Cisco ACI Virtual Edge に移行する場合には、分散ファイアウォールを [Learning] モードにしておく必要があります。これらのバージョンでは分散ファイアウォールをサポートしていません。<br>**3.** [Syslog] 領域で、[Administrative State] ドロップダウン リストから [enabled] が選択されていることを確認します。<br>**4.** [Included Flows] 領域で、[Permitted flows]、[Denied flows]、またはその両方を選択します。<br>**5.** [Polling Interval (seconds)] 領域で、60 秒から 24 時間の間隔を選択します。<br>**6.** [Log Level] ドロップダウン リストから、重大度レベルを選択します。<br>ロギング重大度レベルは、syslog サーバに定義された重大度レベルと同じか、それ以上である必要があります。重大度については、このガイドの分散ファイアウォールのフロー情報のパラメータ設定 （80 ページ）を参照してください。<br>**7.** [Dest Group] ドロップダウン リストから、作成したばかりの宛先グループを選択します。<br>**8.** [Submit] をクリックします。 |

| 実行する操作 | 結果 |
| --- | --- |
| | 9. [Policy Usage Warning] ダイアログ ボックスが表示された場合は、[SUBMIT CHANGES] をクリックします。 |

### 次のタスク

新しい分散ファイアウォール ポリシーで syslog ポリシーを設定した場合、VMM ドメインにその分散ファイアウォール ポリシーを関連付ける必要があります。

1. Cisco APIC で、**[Virtual Networking]** > **[Inventory]** を選択します。
2. ナビゲーション ウィンドウで、[VMM Domains] フォルダと [VMware] フォルダを展開し、関連する VMM ドメインを選択します。
3. 作業ウィンドウで、[VSwitch Policy] タブ ([Policy] タブの下) をクリックします。
4. [Create VSwitch Policy Container] ダイアログボックスで、[Yes] をクリックします。
5. 作業ウィンドウで、[Firewall Policy] ドロップダウン リストから、ポリシーを選択します。
6. [Submit] をクリックします。
7. [Policy Usage Warning] ダイアログ ボックスが表示された場合は、[SUBMIT CHANGES] をクリックします。

# NX-OS スタイルの CLI を使用した分散ファイアウォールのフロー情報のパラメータの設定

### 手順

**ステップ 1** syslog サーバ（複数可）のパラメータを設定します。

**例**：

```
apic1# configure
apic1(config)# logging server-group group name
apic1(config-logging)# server IP address severity severity level facility facility
 name  port 1-65535 mgmtepg MgmtEpg
```

追加の syslog サーバのために最後のコマンドを繰り返すことができ、最大 3 つの syslog サーバを設定できます。

**ステップ 2** syslog 送信元のパラメータを設定します。

**例**：

```
apic1# configure
apic1(config)#  vmware-domain Direct-AVE
apic1(config-vmware)#  configure-ave
apic1(config-vmware-ave)# firewall mode enabled
apic1(config-vmware-ave)# firewall-logging server-group group name action-type
 permit, deny severity severity polling-interval 60-86400
```

（注） **firewall-logging** コマンドを入力する前に、**firewall mode enabled** コマンドを入力する必要があります。

（注） firewall-logging コマンドには、permit または deny のいずれかを入力できます。また、カンマで区切って両方を入力することもできます。

# REST API を使用した分散ファイアウォール フロー情報のパラメータの設定

手順

**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/node/mo/uni/fabric/slgroup-Syslog-Servers.xml
```

**ステップ 2** syslog サーバ（複数可）のパラメータを設定します。

例：

```
<syslogGroup descr="" dn="uni/fabric/slgroup-Syslog-Servers" format="aci"
name="Syslog-Servers" nameAlias="">
 <syslogRemoteDest adminState="enabled" descr="" format="aci" forwardingFacility="local7"
 host="10.197.139.216" name="10.197.139.216" nameAlias="" port="1514" severity="debugging">

  <fileRsARemoteHostToEpg tDn="uni/tn-mgmt/mgmtp-default/oob-default"/>
 </syslogRemoteDest>
 <syslogProf adminState="enabled" descr="" name="syslog" nameAlias=""/>
 <syslogFile adminState="disabled" descr="" format="aci" name="" nameAlias=""
severity="information"/>
 <syslogConsole adminState="disabled" descr="" format="aci" name="" nameAlias=""
severity="alerts"/>
</syslogGroup>
```

# 分散ファイアウォール フローの数

Cisco APIC で分散ファイアウォール フローの数を表示できます。

Cisco ACI Virtual Edge では分散ファイアウォール フロー情報が収集されますが、それらを表示するには、必要な統計情報を選択する必要があります。10秒から1年までのサンプリング間隔を選択できますが、デフォルトは 5 分です。

選択した統計情報は、Cisco APIC の 2 つの異なる場所で表示できます。**Virtual Networking** で始まるものと、**Tenants** で始まるものです。ただし、統計情報を選択および表示する手順は同じです。

Cisco APIC で統計情報を選択すると、さまざまなタイプの統計情報のリストが表示されますが、分散ファイアウォールに関連するのは 9 つだけです。

- 期限切れの接続（接続）
- 作成した接続（接続）
- 中断された接続（接続）
- 拒否されたグローバル入力接続（接続）
- ポート制限当たりの拒否された接続（接続）
- 無効な SYN ACK パケット（パケット）
- 無効な SYN パケット（パケット）
- 無効な接続パケット（パケット）
- 無効な ftp SYN パケット（パケット）

# 分散ファイアウォールについて表示する統計情報の選択

### 始める前に

分散ファイアウォールを有効にしておく必要があります。

### 手順

**ステップ 1** **[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 2** [Stats] タブをクリックします。

**ステップ 3** 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 4** [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 5** (オプション) サンプリング間隔を選択します。

**ステップ 6** [Submit] をクリックします。

# 分散ファイアウォールの統計情報の表示

分散ファイアウォールの統計情報を選択したら、それらを確認できます。

### 始める前に

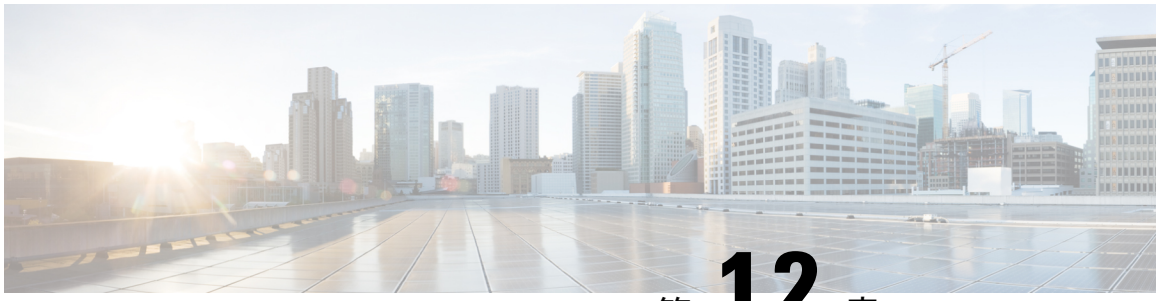
分散ファイアウォールについて表示する統計情報を選択しておく必要があります。

### 手順

**ステップ 1** **[Virtual Networking]** > **[Inventory]** > **[VMware]** > **[VMM Domains]** > ***[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 2** **[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。



第 12 章

# Cisco ACI でのマイクロセグメンテーション



## Cisco ACI でのマイクロセグメンテーション

Cisco APIC を使用すると、Cisco ACI でマイクロセグメンテーションを設定できます。マイクロセグメンテーションにより、さまざまな属性に基づいて、エンドポイントを特別なエンドポイント グループ、つまり EPG に割り当てることができます。これらの属性ベースの EPG がマイクロセグメントと呼ばれており、フィルタリングと転送ポリシーの適用を行えるので、論理的なセキュリティ ゾーンとして機能します。

マイクロセグメンテーションの使用と設定に関する情報については、『*Cisco ACI Virtualization Guide*』の「Microsegmentation with Cisco ACI」の章を参照してください。

Cisco ACI でのマイクロセグメンテーション

第 13 章

# 接続可能エンティティ プロファイルの設定

この章の内容は、次のとおりです。



## GUI を使用したアタッチ可能エンティティ プロファイルの設定

Cisco ACI ファブリックは、リーフ ポイントを通してベア メタル サーバ、仮想マシン ハイパーバイザ、レイヤ 2 スイッチ、またはレイヤ 3 ルータ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を提供します。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、または仮想ポート チャネル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、さまざまなプロトコルの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ています。

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。AEP についての詳細は、『Cisco ACI Fundamentals Guide』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** メニュー バーで、[Fabric] > [Access Polices] を選択します。

**ステップ 3** 左側の [Policies] ナビゲーション ウィンドウで、[Policies] および [Global] フォルダを展開します。

**ステップ 4** [Attachable Access Entity Profiles] フォルダを右クリックして [Create Attachable Access Entity Profile] を選択します。

**ステップ 5** [Create Attachable Access Entity Profile STEP 1 > Profile] ダイアログボックスで、次の手順に従います。

a) [Name] フィールドに、名前を入力します。
b) [Enable Infrastructure VLAN] チェック ボックスをオンにします。
c) [Domains (VMM, Physical or External) To Be Associated To Interfaces] エリアで、[+] アイコンをクリックします。
d) [Domain Profile] ドロップダウン リストで、ドメイン プロファイル (VMM ドメイン) を選択します。
e) [Update] をクリックしてドメインを更新します。
f) [Next] をクリックします。

**ステップ 6** [Create Attachable Access Entity Profile STEP 2 > Association To Interfaces] ダイアログボックスで、次の手順に従います:

a) ホストに対して作成したインターフェイス ポリシー グループを選択します。
b) 選択したインターフェイス ポリシー グループごとに、[All] または [Specific] を選択します。

[All] を選択した場合、アタッチしたエンティティは、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適用されます。[Specific] を選択した場合、インターフェイス ポリシー グループ リストの右側に表示される [Switch IDs] ドロップダウンリストからスイッチ ID を選択します。

c) [Finish] をクリックします。

第 14 章

# レイヤ 4 ～ レイヤ 7 サービス



# レイヤ 4 ～ レイヤ 7 サービス

Cisco Application Centric Infrastructure（ACI）では、アプリケーションのキーの一部としてサービスを扱います。必要とされるすべてのサービスが、Cisco Application Policy Infrastructure Controller（APIC）から ACI ファブリックでインスタンス化されるサービス グラフとして扱われます)。アプリケーションに対してサービスを定義し、サービス グラフはアプリケーションが必要とする一連のネットワークまたはサービス機能を識別します。

Cisco ACI Virtual Edge リリース 1.2(1) 以降、レイヤ 4 ～レイヤ 7 のサービス グラフが Cisco ACI Virtual Edge でサポートされます。

Cisco ACI Virtual Edge のレイヤ 4 ～レイヤ 7 のサービス グラフの設定に関する詳細は、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』を参照してください。ただし、最初にこの章の次のセクションにある注意事項に従い、制限事項を理解する必要があります。

『*Cisco APIC Layer 4 to Layer 7 ServicesDeployment Guide*』の手順に従う場合、VMware 分散型仮想スイッチ（DVS） VMM ドメイン上にサービスを設定する代わりに、スイッチング モードとして **AVE** を持つ Cisco ACI Virtual Edge VMM ドメイン上にサービスを設定してください。

# ガイドラインとレイヤ 7 構成のレイヤ 4 の制限事項

Cisco ACI Virtual Edge のレイヤ 4 からレイヤ 7 のサービス グラフを設定する準備をする場合は、このセクションのガイドラインに従ってください。

- レイヤ 4 からレイヤ 7 サービスは、初期リリースではルーテッド モードでのみサポートされています。透過モードはサポートされていません。

- HA のペアの両方のサービス VM を同じCisco ACI Virtual Edge の後ろにデプロイしないでください。

  配備後に HA ペアの両方のサービス VM が同じ Cisco ACI Virtual Edge の後ろで終わらないようにするには、VM ホスト類似性ルールを作成します。これにより、HA ペアの各サービス VM が異なるホスト上で動作することが可能になります。

  VM ホスト アフィニティルールを作成するときは、[Type] として、[Virtual Machines to Hosts] を選択し、[Must run on hosts in group] を選択します。VM ホスト アフィニティ ルールの作成の詳細については、対応する vSphere バージョンの Vmware のドキュメントを参照してください。

- 非サービス VM をサービス EPG に手動で関連付けしてはいけません。単一のホスト上の任意の時点で、各サービス EPG の 1 つのエンドポイントのみがサポートされます。

- Cisco ACI Virtual Edge にデプロイされたサービス VM インタフェースにはタグを付けません。 Cisco ACI Virtual Edge はトランク ポート グループをサポートしていません。

- Cisco ACI Virtual Edge は、仮想 MAC ベースのサービス VM のデプロイをサポートしていません。

  Cisco ACI Virtual Edge でサポートされているサービス VM デプロイ モードは、スタンドアロンおよび HA モード (アクティブ/スタンバイ) です。

- Cisco ACI Virtual Edge は、サービス VM の vMotion をサポートします。

  （注） Vmware 環境でのサービス VM の vMotion のサポートについては、対応するベンダーのドキュメントを参照してください。vMotion のサポートはベンダー固有のものであり、特定のガイドラインと制限事項があります。

- Cisco ACI Virtual Edge では、サービス グラフ ベースのデプロイメントのみがサポートされています。

- Cisco ACI Virtual Edge は、ルート ピアリング、トランキング ポート、および無作為モードをサポートしていません。

- Cisco Application Virtual Switch（AVS）ドメインに展開されているレイヤ 4 からレイヤ 7 のサービスを Cisco ACI Virtual Edge に移行することはできません。

  移行を進めるには、シスコの AVS 上のサービスの展開を解除してください。また、VMware VDS ドメインから Cisco ACI Virtual Edge に移行する際、コンシューマおよびプロバイダーの EPG を Cisco ACI Virtual Edge に移すことはできますが、レイヤ 4 からレイヤ 7 のサービスの EPG は VMware VDS に属します。詳細については、『*Cisco ACI Virtual Edge Installation Guide*』の「Migration from VMware VDS to CiscoACI Virtual Edge」の章を参照してください。

- サービス VM の管理インターフェイスと HA インターフェイスが VDS/vSwitch 上にあることを確認します。

- Cisco ACI Virtual Edge VMM ドメインを構成する場合は、VLAN プールをドメインに関連付けることが必須です。

  サービス VM は VLAN カプセル化モードで Cisco ACI Virtual Edge VMM ドメインにデプロイされるため、VLAN プールをドメインに関連付ける必要があります。VLAN プールの内部範囲と外部範囲の両方を設定します。詳細については、このガイドの混合モードのカプセル化 （13 ページ） 章を参照してください。

- Compute VM (プロバイダーとコンシューマー) は、VXLAN または VLAN カプセル化モードを使用して Cisco ACI Virtual Edge VMM ドメインに展開できます。

  どちらのモードでも VM の計算をサポートするには、混在モードのカプセル化を使用して Cisco ACI Virtual Edge VMM ドメインを構成します。詳細については、このガイドの混合モードのカプセル化 （13 ページ） 章を参照してください。

# 限定されるサービス デバイス

Cisco ACI Virtual Edge のためのサービス グラフ導入は、次のサービス デバイスに限定されます。

- Cisco 適応型セキュリティ仮想アプライアンス（ASAv）1 ファイアウォール バージョン 9.9(1)

  （注） Cisco ACI Virtual Edge VMM ドメインで ASAv を展開する前に、`externalIf` と `internalIf` のモニタリングを有効にします。CLI でモニタリングを有効にするには、ASAv で **monitor-interface externalIf** と **monitor-interface internalIf** コマンドを使用します。

- F5 ネットワーク BIG-IP ロード バランサ (アンマネージド モード) バージョン 13.1.0.3
- Citrix NetScaler VPX (アンマネージド モード) バージョン 11.0 ビルド 70.16

# サポートされる展開

Cisco ACI Virtual Edge は次の展開をサポートしています。

- ルーテッド モードの ASAv
- F5 ネットワーク BIG-IP ロード バランサ (アンマネージド モード)
  - ワンアーム モード
  - ツーアーム モード
- スタンドアロンおよび HA モード (アクティブ/スタンバイ)

- 1 ノードおよび 2 ノードの展開

# Cisco ASAV、Citrix NetScaler、F5 BIG-IP ADC のブリッジ ドメイン設定

Cisco ASAv、Citrix NetScaler、F5 BIG-IP ADC ブリッジ ドメインを設定するときは、次の場合を除き、一般的な設定を行うようにブリッジ ドメインを設定します。

| 設定 | アクション |
|---|---|
| **L2 不明のユニキャスト** | [Flood] を選択します。 |
| [ARP Flooding] チェックボックス | チェックボックスをオンにします。 |
| [Unicast Routing] チェックボックス | この設定は展開によって異なります。たとえば、Cisco ACI ファブリックをトラフィックにルートする場合、**[Unicast Routing]** チェックボックスをチェックします。さらに、内部のブリッジ ドメインを設定するときにエンドポイント接続を使用する場合、**[Unicast Routing]** を有効にします。 |

### 参照

Cisco ACI のブリッジ ドメイン設定の詳細については、『Cisco APIC Layer 2 Networking Configuration Guide』を参照してください。

サービス グラフ設計に関するブリッジ ドメインの設定についての全般情報は、『Service Graph Design with Cisco application Centric Infrastructure White Paper』を参照してください。