Cisco ACI の VMware VDS との統合

この章の内容は、次のとおりです。

- 仮想マシン ネットワーキング ポリシーの設定 （1 ページ）
- VMM ドメイン プロファイルの作成 （5 ページ）
- VDS アップリンク ポート グループの作成 （12 ページ）
- トランク ポート グループの作成 （13 ページ）
- GUI を使用した トランク ポート グループの作成 （13 ページ）
- NX-OS スタイルの CLI を使用したトランク ポート グループの作成 （14 ページ）
- REST API を使用した トランク ポート グループの作成 （16 ページ）
- ブレード サーバの使用 （17 ページ）
- Cisco ACI と VMware VMM システム統合のトラブルシューティング （20 ページ）
- 追加参考セクション （20 ページ）

仮想マシン ネットワーキング ポリシーの設定

Cisco APIC は、Cisco ACI の利点を仮想インフラストラクチャに拡張するために、サードパーティの VM マネージャ (VMM) (たとえば VMware vCenter) と統合するようになっています。Cisco APIC は、VMM システム内の CIsco ACI ポリシーを有効にして、管理者が使用できるようにします。

Cisco ACI と VMware の VMM 統合では以下のモードがサポートされます。

- VMware VDS：Cisco ACI と統合するときに、VMware vSphere Distributed Switch（VDS）によって、ACI ファブリックの VM ネットワーキングが設定できるようになります。
- Cisco ACI Virtual Edge: Cisco ACI Virtual Edge をインストールして設定する方法の詳細については、 *Cisco ACI Virtual Edge*『インストレーション ガイド』および *Cisco ACI Virtual Edge*『構成ガイド』を参照してください。Cisco.com からアクセスできます。
- Cisco Application Virtual Switch (AVS): Cisco AVS を Cisco ACI とともにインストールして構成する方法については、Cisco AVS のマニュアルを参照してください。Cisco.com からアクセスできます。

APIC でサポートされる VMware VDS バージョン

VMware VDS は、Cisco APIC 3.2(2) での Release 6.7 を含む、VMware vSphere 5.1 以降でサポートされます。

（注） VMware vSphere Distributed Switch（VDS）を使用した VMM ドメインに VMware ESXi ホストを追加するときは、ESXi ホストのバージョンが、vCenter にすでに導入されている Distributed Virtual Switch（DVS）バージョンと互換性があることを確認してください。ESXi ホストに関する VMware VDS 互換性要件の詳細については、VMware のマニュアルを参照してください。

ESXi ホスト バージョンに既存の DVS との互換性がない場合、vCenter はその ESXi ホストを DVS に追加することはできず、非互換性エラーが発生します。Cisco APIC から既存の DVS バージョン設定を変更することはできません。vCenter で DVS バージョンを低くするには、VMM ドメイン設定を削除してから、低くした設定で再適用する必要があります。

重要 VIC カードで UCS B シリーズまたは C シリーズ サーバを実行している ESXi 6.5 ホストがある場合には、一部の VMNIC が、リンク フラップや TOR リロードなどのポート状態イベントの際にダウンすることがあります。この問題を防ぐため、デフォルトの eNIC ドライバを使用せず、VMware Web サイト、https://my.vmware.com/web/vmware/details?downloadGroup=DT-ESXI65-CISCO-NENIC-1020&productId=614 からのものをインストールしてください。

5.X から 6.x への VMware DVS のアップグレードと VMM 統合に関するガイドライン

ここでは、VMware 分散仮想スイッチ（DVS）の 5.x から 6.x へのアップグレードおよび VMM 統合のガイドラインを説明します。

- DVS のバージョニングは VMware DVS にのみ適用され、Cisco Application Virtual Switch（AVS）には適用されません。DVS のアップグレードは、ACI からではなく VMware vCenter または関連するオーケストレーション ツールから開始されます。vCenter 内の AVS スイッチの場合、 **Upgrade Version** オプションはグレー表示になります。
- DVS を 5.x から 6.x にアップグレードする場合、vCenter Server をバージョン 6.0 に、および分散スイッチに接続されているすべてのホストを ESXi 6.0 にアップグレードする必要があります。vCenter およびハイパーバイザ ホストのアップグレードの詳細については、VMware のアップグレード マニュアルを参照してください。DVS をアップグレードするには、Web クライアントに移動します（**[Home]** > **[Networking]** > **[DatacenterX]** > **[DVS-X]** > **[Actions Menu]** > **[Upgrade Distributed Switch]**）。
- vCenter に表示される DVS バージョンが APIC で設定された VMM ドメインの DVS バージョンと一致しない場合でも、DVS の機能、能力、パフォーマンス、スケールへの機能上

の影響はありません。APIC および VMM ドメインの DVS バージョンは、初期導入にのみ使用されます。

VMware VDS 統合のためのガイドライン

VMware vSphere 分散スイッチ (VDS) を Cisco Application Centric Infrastructure (ACI) に統合するときには、このセクションのガイドラインに従う必要があります。

- VMM 統合用に設定された VMware VDS では次の設定を変更しないでください:
  - VMware vCenter のホスト名 (DNS を使用している場合)。
  - VMware vCenter IP アドレス (IP を使用している場合)。
  - Cisco APIC が使用している VMware vCenter のクレデンシャル。
  - データセンター名
  - フォルダ、VDS、またはポート グループの名前。
  - VMware VDS が含まれているフォルダ構造。

    たとえば、フォルダを別のフォルダに入れるようなことはしないでください。
  - LACP/ポート チャネル、LLDP、CDP などの設定を含む、アップリンク ポート チャネル設定
  - ポートグループの VLAN
  - Cisco APIC がプッシュするポート グループのアクティブなアップリンク。
  - Cisco APIC がプッシュするポートグループのセキュリティ パラメータ (無差別モード、MAC アドレスの変更、偽造送信)。
- 実行している Cisco ACI のバージョンでサポートされている VMware vCenter/vSphere のバージョンを使用します。
- いずれかのポートグループを追加または削除する場合は、Cisco APIC または VMware vCenter の Cisco ACI vCenter プラグインを使用します。
- Cisco APIC は、VMware vCenter で行われた変更の一部を上書きする可能性があることに注意してください。

  たとえば、Cisco APIC がポートグループを更新すると、ポート バインディング、無差別モード、およびロード バランシングが上書きされることがあります。

ACI と VMware の構造のマッピング

表 *1: ACI* と *VMware* の構造のマッピング

Cisco APIC 用語	VMware 用語
VM コントローラ	vCenter (データセンター)
Virtual Machine Manager（VMM） ドメイン	vSphere Distributed Switch（VDS）
エンドポイント グループ（EPG）	ポート グループ

APIC によって管理される VMware VDS パラメータ

APIC によって管理される VDS パラメータ

VMware VDS	デフォルト値	APIC ポリシーを使用して設定可能か
名前	VMM ドメイン名	はい（ドメインから派生）
説明	"APIC Virtual Switch"	いいえ
フォルダ名	VMM ドメイン名	はい（ドメインから派生）
バージョン	vCenter でサポートされる最新	はい
Discovery プロトコル	LLDP	はい
アップリンク ポートおよびアップリンク名	8	いいえ
アップリンク名プレフィックス	uplink	いいえ
最大 MTU	9000	はい
LACP ポリシー	disabled	はい
ポートのミラーリング	0 セッション。	はい
アラーム	フォルダ レベルに 2 アラーム追加	いいえ

APIC によって管理される VDS ポート グループ パラメータ

VMware VDS ポート グループ	デフォルト値	APIC ポリシーを使用して設定可能か
名前	テナント名|アプリケーション プロファイル名|EPG 名	はい（EPG から導出）
ポート バインディング	スタティック バインディング	いいえ
VLAN	VLAN プールから選択	はい
ロードバランシング アルゴリズム	APIC のポート チャネル ポリシーに基づいて派生	はい
無差別モード	ディセーブル	はい
偽装された転送	Disabled	はい
MAC 変更	Disabled	はい
すべてのポートをブロック	False	いいえ

VMM ドメイン プロファイルの作成

VMM ドメイン プロファイルは、仮想マシン コントローラを Cisco ACI ファブリックに接続させる接続ポリシーを指定します。同様のネットワーキング ポリシー要件を持つ VM コントローラをグループ化します。たとえば、VM コントローラは VLAN プールとアプリケーション エンドポイント グループ（EPG）を共有できます。Cisco APIC はコントローラと通信して、仮想ワークロードに適用するポート グループなどのネットワーク設定をパブリッシュします。詳細については、 Cisco.com の『Cisco Application Centric Infrastructure Fundamentals』を参照してください。 on Cisco.com.

Cisco APIC リリース 3.1(1) 以降では、読み取り専用の VMM ドメインを作成することもできます。読み取り専用 VMM ドメインを使用すればと、Cisco APIC が管理していない VMware vCenter での VDS のインベントリ情報を表示できます。読み取り専用 VMM ドメインを設定する手順は、他の VMM ドメインを作成する手順とは若干異なります。ただし、同じワークフローと前提条件が適用されます。

（注） このセクションでの VMM ドメインの例は、vCenter ドメインです。

GUI タスク

ここでは、GUI を使用してタスクを実行する方法を示します。

- REST API タスクのリファレンスについては、REST API タスク （23 ページ）を参照してください。
- NX-OS スタイルの CLI のタスクのリファレンスについては、NX-OS スタイルの CLI のタスク （30 ページ）を参照してください。

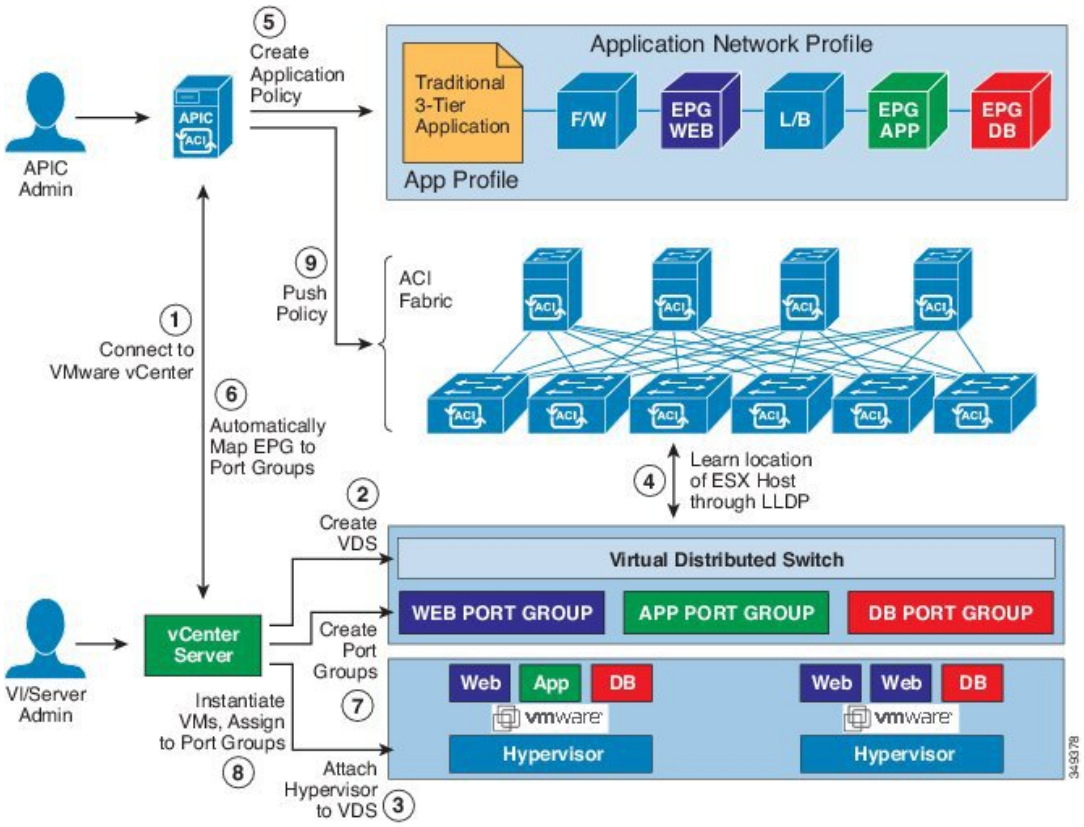
VMM ドメイン プロファイルを作成するための前提条件

VMM ドメイン プロファイルを設定するには、次の前提条件を満たす必要があります。

- すべてのファブリック ノードが検出され、設定されている。
- インバンド（inb）またはアウトオブバンド（oob）管理が APIC 上で設定されている。
- Virtual Machine Manager（VMM）がインストールされ、設定されて、inb/oob 管理ネットワーク（たとえば、vCenter）経由で到達可能である。

vCenter ドメイン運用ワークフロー

図 *1 : vCenter* ドメイン運用ワークフロー順の説明



APIC管理者は、APIC の vCenter ドメイン ポリシーを設定します。APIC 管理者は、次の vCenter 接続情報を提供します。

- vCenter IP アドレス、vCenter クレデンシャル、VMM ドメイン ポリシー、VMM ドメイン SPAN
- ポリシー（VLAN プール、VMware VDS などのドメイン タイプ、Cisco Nexus 1000V スイッチ）
- 物理リーフ インターフェイスへの接続性（接続エンティティ プロファイルを使用）

1. APIC が自動的に vCenter に接続します。
2. APICVDS の作成: すでに作成されている場合は、既存の VDS を使用または: VMM ドメインの名前に一致します。

（注） 既存の VDS を使用する場合、同じ名前でフォルダ内に VDS 必要があります。

（注） VCenter から既存の VDS を表示する場合は、これを行う指定することにより、 **読み取り専用モード** で、 **アクセス モード** エリア Cisco APIC を使用して vCenter で VDS と同じ名前の VMM ドメインを作成する際にします。この VMM で **読み取り専用モード** APIC で管理されていません。VCenter のユーザ クレデンシャルと vCenter IP アドレスを除くこの VMM ドメインの任意のプロパティを変更することはできません。

3. vCenter の管理者やコンピューティングの管理ツールは、APIC VDS に ESX ホストまたはハイパーバイザを追加し、APIC VDS 上にアップリンクとして ESX ホスト ハイパーバイザ ポートを割り当てます。これらのアップリンクは ACI リーフ スイッチを接続する必要があります。
4. APIC がハイパーバイザの LLDP または CDP 情報を使用して、リーフ接続へのハイパーバイザ ホストの場所を学習します。
5. APIC 管理者がアプリケーション EPG ポリシーを作成して関連付けます。
6. APIC 管理者が VMM ドメインに EPG ポリシーを関連付けます。
7. APIC は、VDS 下の VMware vCenter でポート グループを自動的に作成します。このプロセスは VMware vCenter でネットワーク ポリシーをプロビジョニングします。

（注）
- ポート グループ名は、テナント名、アプリケーション プロファイル名および EPG 名を連結したものです。
- ポート グループは、VDS 下で作成され、APIC によって以前に作成されたものです。

8. vCenter の管理者やコンピューティングの管理ツールは、VM をインスタンス化しポートグループに割り当てます。
9. APIC は、vCenter イベントに基づいて VM の配置について学習します。APIC は、アプリケーション EPG および関連するポリシー（たとえば、コントラクトやフィルタ）を ACI ファブリックに自動的にプッシュします。

GUI を使用した vCenter ドメイン プロファイルの作成

vCenter ドメインの作成時に行う作業の概要は次のとおりです（詳細は下のステップで説明します）。

- スイッチ プロファイルの作成/選択
- インターフェイス プロファイルの作成/選択
- インターフェイス ポリシー グループの作成/選択
- VLAN プールの作成/選択
- vCenter ドメインの作成
- vCenter クレデンシャルの作成

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順にクリックします。

ステップ 2 ナビゲーション ウィンドウで、[Quick Start] をクリックし、中央ペインで [Configure an interface, PC, and VPC] をクリックします。

ステップ 3 [Configure an interface, PC, and VPC] ダイアログ ボックスで、次のアクションを実行します。

a) [Configured Switch Interfaces] を展開します。
b) [+] アイコンをクリックします。
c) [Quick] オプション ボタンが選択されていることを確認します。
d) [Switches] ドロップダウン リストから、適切なリーフ ID を選択します。

[Switch Profile Name] フィールドに、スイッチプロファイル名が自動的に入力されます。

e) スイッチ インターフェイスを設定するために [+] アイコンをクリックします。
f) [Interface Type] エリアで、適切なラジオ ボタンをオンにします。
g) [Interfaces] フィールドに、目的のインターフェイス範囲を入力します。
h) [Interface Selector Name] フィールドに、セレクタ名が自動的に入力されます。
i) [Interface Policy Group] 領域で、[Create One] オプション ボタンを選択します。
j) [Link Level Policy] ドロップダウン リストから、目的のリンク レベル ポリシーを選択します。
k) [CDP Policy] ドロップダウン リストから、目的の CDP ポリシーを選択します。

（注） 同様に、利用可能なポリシーエリアから目的のインターフェイスポリシーを選択します。

l) [Attached Device Type] エリアで、[ESX Hosts] を選択します。
m) [Domain] エリアで、[Create One] ラジオ ボタンが選択されていることを確認します。
n) [Domain Name] フィールドに、ドメイン名を入力します
o) [VLAN] エリアで、[Create One] ラジオ ボタンが選択されていることを確認します。
p) [VLAN Range] フィールドに、必要に応じて VLAN の範囲を入力します。

（注） 少なくとも 200 の VLAN 番号の範囲を推奨します。（VLAN 4）、この VLAN ID を含む範囲を定義しないでください。

q) [vCenter Login Name] フィールドに、ログイン名を入力します。
r) （任意） [Security Domains] ドロップダウン リストから、適切なセキュリティ ドメインを選択します。
s) [Password] フィールドに、パスワードを入力します。
t) [Confirm Password] フィールドにパスワードを再入力します。
u) **vCenter** を展開します。

ステップ 4 [Create vCenter Controller] ダイアログボックスに適切な情報を入力し、[OK] をクリックします。

ステップ 5 [Configure Interface, PC, And VPC] ダイアログボックスで、次の操作を実行します。

[Port Channel Mode] および [vSwitch Policy] エリアでポリシーを指定しなかった場合、この手順の前の部分で設定したのと同じポリシーが vSwitch でも有効になります。

a) [Port Channel Mode] ドロップダウンリストからモードを選択します。
b) [vSwitch Policy] エリアで、必要なラジオボタンをクリックして CDP または LLDP をクリックします。
c) [NetFlow Exporter Policy] ドロップダウンリストで、ポリシーを選択するか、作成します。

NetFlow エクスポータ ポリシーは、外部コレクタの到達可能性を設定します。

d) [Active Flow Time0ut]、 [Idle Flow Timeout]、および [Sampling Rate] ドロップダウンリストから値を選択します。
e) [SAVE] を 2 回クリックしてから [SUBMIT] をクリックします。

ステップ 6 次の手順に従って、新しいドメインとプロファイルを確認します。

a) メニュー バーで、**[Virtual Networking]** > **[Inventory]** を選択します。
b) [Navigation] ウィンドウで、 **[VMM Domains]** > **[VMware]** > ***[Domain_name]*** > **[vCenter_name]** を展開します。

[Work] ペインの [Properties] に VMM ドメイン名を表示して、コントローラがオンラインであることを確認します。[Work] ペインに、vCenter のプロパティが動作ステータスとともに表示されます。表示される情報によって、APIC コントローラから vCenter Server への接続が確立され、インベントリが使用できることを確認します。

読み取り専用 VMM ドメインの作成

Cisco APIC リリース 3.1 (1) 以降では、読み取り専用 VMM ドメインを作成することができます。これにより、Cisco APIC は管理されませんする VMware vCenter での VDS のインベントリの情報を表示します。

読み取り専用 VMM ドメインを作成したら、通常の VMM ドメインと同じように、ハイパーバイザ、VM、NIC のステータス、およびその他のインベントリ情報を表示できます。EPG を VMM ドメインに関連付けて、そのためのポリシーを構成できます。ただし、読み取り専用 VMM ドメインから VDS にポリシーがプッシュされることはありません。また、読み取り専用 VMM ドメインでは障害は発生しません。

Cisco APIC GUI、NX-OS スタイルの CLI、または REST API を使用して、読み取り専用 VMM ドメインを作成することができます。手順については、このガイドの次のセクションを参照してください。

- Cisco APIC GUI を使用した読み取り専用 VMM ドメインの作成 （10 ページ）
- REST API を使用した読み取り専用 VMM ドメインの作成 （25 ページ）
- NX-OS スタイルの CLI を使用した 読み取り専用 VMM ドメインの作成 （32 ページ）

Cisco APIC GUI を使用した読み取り専用 VMM ドメインの作成

読み取り専用 VMM ドメインを作成するため、[Virtual Networking] タブの [Create vCenter Domain] ダイアログ ボックスでドメインを作成します。ドメインを作成するためにセクション「GUI を使用した vCenter ドメイン プロファイルの作成 （8 ページ） 」の手順に従わないでください。その手順では、VMM ドメインのアクセス モードを設定できません。

これを作成した後に VMM ドメインのアクセス モードを変更することはできません。変更しようとすると、エラー メッセージが表示されます。

始める前に

- セクション「VMM ドメイン プロファイルを作成するための前提条件 （6 ページ） 」の前提条件を満たします。
- VMware vCenter の [Networking] タブの下で、フォルダに VDS が含まれていることを確認します。

  また、フォルダと VDS の名前が、作成する読み取り専用 VMM ドメインと正確に一致し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 **[Virtual Networking]** > **[Inventory]** を選択し、[VMM Domains] フォルダを展開します。

ステップ 3 [VMM Domains] フォルダを右クリックし、[Create vCenter Domain] を選択します。

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

a) [Virtual Switch Name] フィールドで、 ドメインの名前を入力します。

（注） 読み取り専用のドメインの名前は、VDS と VMware vCenter が含まれているフォルダの名前と同じにする必要があります。

b) [Virtual Switch] エリアで、[VMware vSphere Distributed Switch] を選択します。

c) [Access Mode] エリアで、[Read Only Mode] を選択します。

d) [vCenter Credentials] エリアで、[+]（プラス）アイコンをクリックし、ドメインの VMware vCenter クレデンシャルを作成します。

e) [VCenter] エリアで、[+]（プラス）アイコンをクリックし、ドメインの vCenter コントローラを追加します。

f) [Submit] をクリックします。

次のタスク

読み取り専用 VMM ドメインを EPG にアタッチし、そのポリシーを設定できます。ただし、これらのポリシーは、VMware vCenter で VD へプッシュされません。

エンドポイント保持の設定

vCenter ドメインを作成した後は、エンドポイントの保持を設定できます。この機能では、エンドポイントの削除の遅延を有効にして、トラフィックがドロップされる可能性を小さくすることができます。

エンドポイントの保持は、APIC GUI、NX-OS スタイル CLI または REST API を使用して設定できます。詳細については、該当するガイドの次のセクションを参照してください:

- GUI を使用したエンドポイント保持の設定 （11 ページ）
- NX-OS スタイルの CLI を使用したエンドポイント保持の設定 （12 ページ）
- REST API を使用したエンドポイント保持の設定 （28 ページ）

GUI を使用したエンドポイント保持の設定

始める前に

vCenter ドメインを作成し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 **VM Networking** > **Inventory** を選択します。

ステップ 3 左側のナビゲーション ウィンドウで、**VMware** フォルダを展開し、以前に作成した vCenter ドメインをクリックします。

ステップ 4 中央の **Domain** 作業ウィンドウで、**Policy** および **General** タブが選択されていることを確認します。

ステップ 5 **End Point Retention Time (seconds)** カウンタで、エンドポイントを解除するまで保持する時間の秒数を選択します。

0 ～ 600 秒を選択できます。デフォルトは 0 です。

ステップ 6 [送信（Submit）] をクリックします。

NX-OS スタイルの CLI を使用したエンドポイント保持の設定

始める前に

vCenter ドメインを作成している必要があります。

手順

ステップ 1 CLI で、コンフィギュレーション モードに入ります:

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 デタッチされたエンドポイントの保持時間を設定するには、次の手順に従います:

遅延は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 です。

例：

```
apic1(config)# vmware-domain <domainName>

apic1(config-vmware)# ep-retention-time <value>
```

VDS アップリンク ポート グループの作成

各 VMM ドメインは vSphere Distributed Switch（VDS）として vCenter に表示されます。仮想化管理者は、APIC によって作成された VDS にホストを関連付け、特定の VDS に使用する vmnic を選択します。VDS アップリンクの設定は、APIC コントローラから VMM ドメインに関連付けられている接続エンティティ プロファイル（AEP）の vSwitch 設定を変更することによって行います。AEP は、[Fabric Access Policies] 設定領域の APIC の GUI に含まれています。

（注） ACI と vSphere VMM の統合を使用するときは、リンク集約グループ（LAG）は、APIC によって作成された分散スイッチでインターフェイス チームを作成するための方法としてはサポートされません。APIC は、インターフェイス ポリシー グループや AEP vSwitch ポリシーの設定に基づいて、必要なインターフェイス チーミングの設定をプッシュします。vCenter のインターフェイス チームはサポートされません。つまり、手動で作成する必要があります。

トランク ポート グループの作成

GUI を使用した トランク ポート グループの作成

ここでは、GUI を使用してトランク ポート グループを作成する方法を説明します。

始める前に

- トランク ポート グループはテナントから独立している必要があります。

手順

ステップ 1 APIC GUI にログインします。

ステップ 2 メニュー バーで、[Virtual Networking] を選択します。

ステップ 3 ナビゲーション ウィンドウで、**VMM Domains** > **VMware** > **Domain_name** > **Trunk Port Groups** を選択し、**Create Trunk Port Group** を右クリックします。

ステップ 4 [Create Trunk Port Group] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに EPG 名を入力します。

b) **Promiscuous Mode** ボタンについては、**Disabled** または **Enabled** のいずれかをクリックします。デフォルトは **Disabled** です。

c) **Trunk Portgroup Immediacy** ボタンについては、**Immediate** または **On Demand** のいずれかをクリックします。デフォルトは **On Demand** です。

d) **MAC changes** ボタンについては、**Disabled** または **Enabled** のいずれかをクリックします。デフォルトは [Enabled] です。

e) **Forged transmits** ボタンについては、**Disabled** または **Enabled** のいずれかをクリックします。デフォルトは [Enabled] です。

f) **VLAN Ranges** フィールドで、+ アイコンを選択して、 VLAN の範囲 (vlan-100 vlan-200) を入力します。

（注） VLAN の範囲を指定しない場合、VLAN のリストはドメインの VLAN の名前空間から取られます。

g) **Update** をクリックします。

ステップ 5 [送信（Submit）] をクリックします。

NX-OS スタイルの CLI を使用したトランク ポート グループの作成

ここでは、NX-OS スタイルの CLI を使用してトランク ポート グループを作成する方法を説明します。

始める前に

- トランク ポート グループはテナントから独立している必要があります。

手順

ステップ 1 Vmware-domain コンテキストに移動し、次のコマンドを入力します。

例：

```
apic1(config-vmware)# vmware-domain ifav2-vcenter1
```

ステップ 2 トランク ポート グループを作成するには、次のコマンドを入力します。

例：

```
apic1(config-vmware)# trunk-portgroup trunkpg1
```

ステップ 3 VLAN の範囲を入力します。

例：

```
apic1(config-vmware-trunk)# vlan-range 2800-2820, 2830-2850
```

（注） VLAN の範囲を指定しない場合、VLAN リストはドメインの VLAN ネームスペースから取得されます。

ステップ 4 mac の変更はデフォルトで受け入れられます。mac の変更を受け入れないことを選択した場合は、次のコマンドを入力します。

例：

```
apic1(config-vmware-trunk)# no mac-changes accept
```

ステップ 5 forged transmit はデフォルトで受け入れられます。forged transmit を受け入れないことを選択した場合は、次のコマンドを入力します。

例：

```
apic1(config-vmware-trunk)# no forged-transmit accept
```

ステップ 6 無差別モードは、デフォルトでは無効になっています。トランク ポート グループでプロミスキャス モードをイネーブルにする場合は、次のように入力します。

例：

```
apic1(config-vmware-trunk)# allow-promiscuous enable
```

ステップ 7 トランク ポート グループの即時性は、デフォルトでオンデマンドに設定されます。即時即時性をイネーブルにするには、次のコマンドを入力します。

例：

```
apic1(config-vmware-trunk)# immediacy-immediate enable
```

ステップ 8 VMware ドメインを表示します。

例：

```
apic1(config-vmware)# show vmware domain name mininet
Domain Name                          : mininet
Virtual Switch Mode                  : VMware Distributed Switch
Switching Encap Mode                 : vlan
Vlan Domain                          : mininet (2800-2850, 2860-2900)
Physical Interfaces                  :
Number of EPGs                       : 2
Faults by Severity                   : 0, 2, 4, 0
LLDP override                        : no
CDP override                         : no
Channel Mode override                : no

vCenters:
Faults: Grouped by severity (Critical, Major, Minor, Warning)
 vCenter               Type      Datacenter            Status    ESXs   VMs    Faults

 --------------------  --------  --------------------  --------  -----  -----
---------------
 172.22.136.195        vCenter   mininet               online    2      57     0,0,4,0


Trunk Portgroups:
 Name                                          VLANs

 ----------------------------------------------
----------------------------------------------
 epgtr1                                        280-285

 epgtr2                                        280-285

 epgtr3                                        2800-2850


apic1(config-vmware)# show vmware domain name mininet trunk-portgroup

 Name                           Aggregated EPG
 -----------------------------  ---------------------------------------------
 epgtr1                         test|wwwtestcom3|test830
 epgtr2
 epgtr3                         test|wwwtestcom3|test830
                                test|wwwtestcom3|test833


apic1(config-vmware)# )# show vmware domain name ifav2-vcenter1 trunk-portgroup name
trunkpg1
Name                           Aggregated EPG                 Encap
 -----------------------------  -----------------------------  ------------
 trunkpg1                       LoadBalance|ap1|epg1           vlan-318
                                LoadBalance|ap1|epg2           vlan-317
```

```
LoadBalance|ap1|failover-epg    vlan-362
SH:l3I:common:ASAv-HA:test-     vlan-711
rhi|rhiExt|rhiExtInstP
SH:l3I:common:ASAv-HA:test-     vlan-712
rhi|rhiInt|rhiIntInstP
test-dyn-ep|ASA_FWctxctx1bd-    vlan-366
inside|int
test-dyn-ep|ASA_FWctxctx1bd-    vlan-888
inside1|int
test-dyn-ep|ASA_FWctxctx1bd-    vlan-365
outside|ext
test-dyn-ep|ASA_FWctxctx1bd-    vlan-887
outside1|ext
test-inb|FW-Inbctxtrans-        vlan-886
vrfinside-bd|int
test-inb|FW-Inbctxtrans-        vlan-882
vrfoutside-bd|ext
test-inb|inb-ap|inb-epg         vlan-883
test-pbr|pbr-ap|pbr-cons-epg    vlan-451
test-pbr|pbr-ap|pbr-prov-epg    vlan-452
test1|ap1|epg1                  vlan-453
test1|ap1|epg2                  vlan-485
test1|ap1|epg3                  vlan-454
test2-scale|ASA-                vlan-496
Trunkctxctx1bd-inside1|int
test2-scale|ASA-                vlan-811
Trunkctxctx1bd-inside10|int
```

```
apic1(config-vmware)# show running-config vmware-domain mininet
# Command: show running-config vmware-domain mininet
# Time: Wed May 25 21:09:13 2016
  vmware-domain mininet
    vlan-domain member mininet type vmware
    vcenter 172.22.136.195 datacenter mininet
      exit
    configure-dvs
      exit
    trunk-portgroup epgtr1 vlan 280-285
    trunk-portgroup epgtr2 vlan 280-285
    trunk-portgroup epgtr3 vlan 2800-2850
    exit
```

REST API を使用した トランク ポート グループの作成

ここでは、REST API を使用してトランク ポート グループを作成する方法を説明します。

始める前に

- トランク ポート グループはテナントから独立している必要があります。

手順

トランク ポート グループを作成します。

例：

```
<vmmProvP vendor="VMware">
 <vmmDomP name=”DVS1">
  <vmmUsrAggr name="EPGAggr_1">
   <fvnsEncapBlk name="blk0" from="vlan-100” to="vlan-200"/>
  </vmmUsrAggr>
 </vmmDomP>
</vmmProvP>
```

ブレード サーバの使用

Cisco UCS B シリーズ サーバに関するガイドライン

ブレード サーバ システムを VMM 統合の目的で Cisco ACI に統合するとき（たとえば Cisco UCS ブレード サーバまたは他のシスコ以外のブレード サーバを統合するとき）は、次のガイドラインを検討する必要があります。

（注） この例では、Cisco UCS ブレード サーバを統合するためにポート チャネル アクセス ポリシーを設定する方法を示します。同様の手順は、Cisco UCS ブレード サーバ アップリンクをファブリックに接続する方法に応じて、バーチャル ポート チャネルまたは個別のリンク アクセス ポリシーの設定に使用できます。UCS ブレード サーバ アップリンクの APIC で明示的にポート チャネルを設定しない場合、デフォルトの動作は MAC Pinning になります。

- VM エンドポイントの学習は、CDP または LLDP プロトコルに依存します。CDP がサポートされる場合は、ブレード スイッチ経由のリーフ スイッチ ポートからブレード アダプタまで、すべてを有効にする必要があります。
- 管理アドレスのタイプ、長さ、および値（TLV）がブレード スイッチ（CDP プロトコルまたは LLDP プロトコル）上で有効になっていて、サーバとファブリック スイッチに対してアドバタイズされることを確認します。管理 TLV アドレスの設定がブレード スイッチの CDP プロトコルと LLDP プロトコルで一貫している必要があります。
- APIC はファブリック インターコネクトとブレード サーバを管理しません。そのため、CDP やポート チャネル ポリシーなどの UCS 固有のポリシーは、UCS Manager で設定する必要があります。
- APIC の接続可能アクセス エンティティ プロファイルで使用される VLAN プールで定義される VLAN も、UCS で手動で作成し、ファブリックに接続する適切なアップリンクで許可する必要があります。これには、該当する場合は、インフラストラクチャ VLAN を

含める必要もあります。詳細については、『*Cisco UCS Manager GUI Configuration Guide*』を参照してください。

- Cisco UCS B シリーズ サーバを使用し、APIC ポリシーを使用している場合は、Link Layer Discovery Protocol（LLDP）はサポートされません。
- Cisco Discovery Protocol （CDP） は、Cisco UCS Manager ではデフォルトで無効にされています。Cisco UCS Manager では、ネットワーク コントロール ポリシーを作成して、CDP を有効にする必要があります。
- UCS サーバ サービス プロファイルでアダプタのファブリック フェールオーバーを有効にしないでください。シスコは、トラフィックのロードバランシングが適切に行われるように、ハイパーバイザが仮想スイッチ レイヤでフェールオーバーを処理できるようにすることを推奨します。

（注） 症状：ブレード スイッチやファブリック インターコネクトのようなアンマネージド ノードの管理 IP の変更は VMware vCenter で更新されますが、VMware vCenter はイベントを APIC に送信しません。

状況：これにより、VMware vCenter と APIC との同期外れが発生します。

回避策：アンマネージド ノードの背後の ESX サーバを管理する VMware vCenter コントローラのインベントリ プルをトリガーする必要があります。

GUI を使用した、ブレード サーバのアクセス ポリシーのセットアップ

始める前に

Cisco APIC と動作するには、Cisco UCS ファブリック インターコネクトは少なくともバージョン 2.2(1c) である必要があります。BIOS、CIMC およびアダプタなどのすべてのコンポーネントは、バージョン 2.2(1c) 以降である必要があります。その他の詳細については、『*Cisco UCS Manager CLI Configuration Guide*』を参照してください。

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** を選択します。

ステップ 2 ナビゲーション ウィンドウで、**Quick Start** クリックします。

ステップ 3 中央ペインで、**Configure an interface, PC, and VPC** をクリックします。

ステップ 4 [Configure Interface, PC, and VPC] ダイアログボックスで、スイッチを選択するために、[+] アイコンをクリックします。

ステップ 5 [Switches] フィールドで、ドロップダウリストから必要なスイッチ ID を選択します。

ステップ 6 スイッチ インターフェイスを設定するために [+] アイコンをクリックします。

ステップ 7 [Interface Type] フィールドで、[VPC] オプション ボタンをクリックします。

ステップ 8 [Interfaces] フィールドに、ブレード サーバに接続された適切なインターフェイスまたはインターフェイス範囲を入力します。

ステップ 9 [Interface Selector Name] フィールドに名前を入力します。

ステップ 10 [CDP Policy] ドロップダウン リストから、デフォルトを選択します。

デフォルトの CDP ポリシーは無効に設定されています。（リーフ スイッチとブレード サーバ間では、CDP を無効にする必要があります。）

ステップ 11 [LLDP Policy] ドロップダウン リストから、デフォルトを選択します。

デフォルトのLLDPポリシーは、受信および送信状態に対して有効に設定されています。（リーフ スイッチとブレード サーバ間では、LLDP を有効にする必要があります。）

ステップ 12 [LACP Policy] ドロップダウン リストから、[Create LACP Policy] を選択します。

リーフ スイッチとブレード サーバ間では、LACP ポリシーをアクティブにする必要があります。

ステップ 13 [Create LACP Policy] ダイアログボックスで、次のアクションを実行します。

a) [Name] フィールドにポリシーの名前を入力します。
b) [Mode] フィールドで [Active] オプション ボタンをオンにします。
c) 残りのデフォルト値はそのままにして、[Submit] をクリックします。

ステップ 14 [Attached Device Type] フィールドのドロップダウン リストで、[ESX Hosts] を選択します。

ステップ 15 [Domain Name] フィールドに、適宜名前を入力します。

ステップ 16 [VLAN Range] フィールドに、範囲を入力します。

ステップ 17 [vCenter Login Name] フィールドに、ログイン名を入力します。

ステップ 18 [Password] フィールドおよび [Confirm Password] フィールドに、パスワードを入力します。

ステップ 19 **vCenter** フィールドを展開し、**Create vCenter Controller** ダイアログボックスで必要な情報を入力して **OK** をクリックします。

ステップ 20 [vSwitch Policy] フィールドで、次の操作を実行します。

ブレード サーバと ESX ハイパーバイザ間では、CDP を有効にし、LLDP を無効にし、LACP を無効にして、MAC ピニングを設定する必要があります。

a) [MAC Pinning] チェックボックスをオンにします。
b) [CDP] チェックボックスをオンにします。
c) LLDP は無効のままにする必要があるため、[LLDP] チェックボックスはオフのままにします。

ステップ 21 **[Save]** をクリックし、**[Save]** をもう一度クリックします。[Submit] をクリックします。
アクセス ポリシーが設定されます。

Cisco ACI と VMware VMM システム統合のトラブルシューティング

トラブルシューティングの詳細については、次のリンクを参照してください。

- Cisco APIC Troubleshooting Guide
- ACI Troubleshooting Book

追加参考セクション

最小 VMware vCenter 権限を持つカスタム ユーザ アカウント

これにより、APIC は vCenter に VMware API コマンドを送信して、DVS/AVS の作成、VMK インターフェイス（AVS）の作成、ポート グループの発行および必要なすべてのアラートのリレーを行うことができます。

To configure the vCenter from Cisco APIC, your credentials must allow the following minimum set of privileges within the vCenter:

- **アラーム**

  APIC ではフォルダに 2 つのアラームを作成します。DVS に 1 個、ポート グループのもう 1 個。EPG またはドメイン ポリシーが APIC で削除されるとアラームが発生しますが、ポート グループまたは DVS については、VM が接続されているため削除できません。

- **分散スイッチ**
- **dvPort グループ**
- **フォルダ**
- **ネットワーク**

  ポートグループの追加または削除、ホスト/DVS MTU, LLDP/CDP, LACP の設定など APIC でネットワーク設定を管理します。

- **Host**

  上記に加えて AVS を使用する場合、APIC が DVS を作成するデータ センタで、ホスト権限が必要です。

  - **Host.Configuration.Advanced settings**
  - **Host.Local operations.Reconfigure virtual machine**
  - **Host.Configuration.Network configuration**

これは、仮想レイヤ 4 ～ レイヤ 7 サービスの VM の AVS と自動配置機能に必要です。AVS については、APIC が VMK インターフェイスを作成し、'OpFlex に使用される 「vtep」 ポート グループに配置します。

- 仮想マシン

  上記に加えてサービス グラフを使用する場合、サービス グラフに使用される仮想アプライアンスに仮想マシン権限が必要です。

  - 仮想マシン.構成.デバイス設定の変更
  - 仮想マシン.構成.設定

検疫ポート グループ

検疫ポート グループ機能は、ポート グループの割り当てを特定の状況下でクリアする手段を提供します。VMware vCenter で、VMware vSphere Distributed Switch（VDS）を作成すると、検疫ポート グループが VDS にデフォルトで作成されます。検疫ポート グループのデフォルト ポリシーは、すべてのポートをブロックします。

ロード バランサやファイアウォールなどの Layer 4 to Layer 7 仮想サービス アプライアンス統合の一環として Application Policy Infrastructure Controller（APIC） は、サービスのスティッチングのために vCenter でサービス ポート グループを作成し、サービス グラフ レンダリング機能の一部としてこれらのサービス ポート グループ内でサービス仮想マシン（VM）などの仮想アプライアンスの配置を調整します。サービス グラフを削除すると、サービス VM は検疫ポート グループに自動的に移動されます。削除時の検疫ポート グループへの自動転送は、APIC によって調整されたサービス VM についてのみ実行されます。

必要に応じて、検疫ポート グループのポートについて詳細なアクションを実行できます。たとえば、検疫ポート グループから VM ネットワークなどの別のポート グループにすべてのポートを移行できます。

検疫ポート グループの機能は通常のテナント エンドポイント グループ（EPG）および関連付けられたポート グループとテナント VM には適用されません。したがって、テナント EPG を削除すると、関連付けられたポート グループに存在するすべてのテナント VM はそのまま残り、検疫ポート グループに移動されません。テナント ポート グループへのテナント VM の配置は APIC レルムの外部になります。

オンデマンド VMM インベントリの更新

Triggered Inventory provides a manual trigger option to pull and resynchronize inventory between a virtual machine manager (VMM) controller and the APIC. トリガード インベントリは同期外れシナリオからの迅速なリカバリを実現します。トリガード インベントリは vCenter VMM コントローラのみに適用できます。通常のシナリオには必要ありません。インベントリ同期は VMM コントローラに負荷がかかる操作であるため、裁量で使用する必要があります。

The APIC initiates vCenter inventory pull. ホスト、VM、DVS、アップリンク ポート グループ、NIC などは最初の VMM コントローラ作成作業の一環として、取得されます。以降の vCenter

の変更はイベント サブスクリプション メカニズムを介して学習されます。This enables the APIC VMM manager to send endpoint attach/detach updates to the APIC policy manager which downloads updated policies to leaf switches accordingly.

When there is a process restart, leadership change, or background periodic 24 hour inventory audit, the APIC does inventory pull to keep VMM inventory synchronized between VMM controllers and the APIC. When heavily loaded, the vCenter fails to provide the APIC an appropriate inventory event notification. In this case, triggered inventory helps to keep the APIC in synchronization with the vCenter.

ACI インバンド VLAN に vCenter ハイパーバイザ VMK0 を移行するためのガイドライン

ACI のインバンド ポートにバインドされた接続からデフォルトの vCenter ハイパーバイザ VMK0 を移行するためには、以下のガイドラインに従います。ACI ファブリック インフラストラクチャ管理者が必要なポリシーを使用して APIC を設定した後、vCenter 管理者が適切な ACI ポート グループに VMK0 を移行します。

APIC での必要な管理 EPG ポリシーの作成

ACI ファブリック インフラストラクチャ管理者として、管理テナントおよび VMM ドメイン ポリシーの作成時に、次のガイドラインを使用します。

- ESX 管理に使用する VLAN を選択します。
- ESX 管理用に選択した VLAN をターゲット VMM ドメインに関連付けられている VLAN プールの範囲（または Encap ブロック）に追加します。この VLAN を追加する範囲は、割り当てモードをスタティック割り当てにする必要があります。
- ACI 管理テナント（mgmt）で管理 EPG を作成します。
- 管理 EPG に関連付けられているブリッジ ドメインがプライベート ネットワーク（inb）にも関連付けられていることを確認します。
- 次のようにターゲット VMM ドメインに管理 EPG を関連付けます。
  - 事前プロビジョニングとして解決の緊急度を使用します。
  - VM ドメイン プロファイル関連付けの [Port Encap] フィールドで管理 VLAN を指定します。

その結果、APIC によって vCenter の下にユーザが指定する VLAN を使用してポート グループが作成されます。APIC は、自動的に VMM ドメインと接続エンティティ プロファイル（AEP）に関連付けられたリーフ スイッチにポリシーをプッシュします。

インバンド ACI VLAN への VMK0 の移行

デフォルトでは、vCenter はハイパーバイザ管理インターフェイスでデフォルト VMK0 を設定します。上述のように作成した ACI ポリシーによって、vCenter 管理者はこのデフォルトの

VMK0 を APIC によって作成されたポート グループに移行できるようになります。そうすることで、ハイパーバイザ管理ポートが解放されます。

REST API タスク

ここでは、REST API を使用してタスクを実行する方法を示します。

- GUI タスクのリファレンスについては、VMM ドメイン プロファイルの作成 （5 ページ）とGUI を使用した、ブレード サーバのアクセス ポリシーのセットアップ （18 ページ）の項を参照してください。
- NX-OS スタイルの CLI のタスクのリファレンスについては、NX-OS スタイルの CLI のタスク （30 ページ）を参照してください。

REST API を使用した vCenter ドメイン プロファイルの作成

手順

ステップ 1 VMM ドメイン名、コントローラおよびユーザ クレデンシャルを設定します。

例：

```
 POST URL: https://<api-ip>/api/node/mo/.xml

<polUni>
<vmmProvP vendor="VMware">
<!-- VMM Domain -->
<vmmDomP name="productionDC">
<!-- Association to VLAN Namespace -->
<infraRsVlanNs tDn="uni/infra/vlanns-VlanRange-dynamic"/>
<!-- Credentials for vCenter -->
<vmmUsrAccP name="admin" usr="administrator" pwd="admin" />
<!-- vCenter IP address -->
<vmmCtrlrP name="vcenter1" hostOrIp="<vcenter ip address>" rootContName="<Datacenter
Name in vCenter>">
<vmmRsAcc tDn="uni/vmmp-VMware/dom-productionDC/usracc-admin"/>
</vmmCtrlrP>
</vmmDomP>
</vmmProvP>
```

例：

```
<polUni>
<vmmProvP vendor="VMware">
    <vmmDomP name="mininet" delimiter="@" >
   </vmmDomP>
</vmmProvP>
</polUni>
```

ステップ 2 VLAN ネームスペースの導入用の接続可能エンティティ プロファイルを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<infraInfra>
<infraAttEntityP name="profile1">
<infraRsDomP tDn="uni/vmmp-VMware/dom-productionDC"/>
</infraAttEntityP>
</infraInfra>
```

ステップ 3 インターフェイス ポリシー グループおよびセレクタを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraAccPortP name="swprofile1ifselector">
        <infraHPortS name="selector1" type="range">
            <infraPortBlk name="blk"
             fromCard="1" toCard="1" fromPort="1" toPort="3">
            </infraPortBlk>
     <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-group1" />
        </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
        <infraAccPortGrp name="group1">
            <infraRsAttEntP tDn="uni/infra/attentp-profile1" />
        </infraAccPortGrp>
    </infraFuncP>
</infraInfra>
```

ステップ 4 スイッチ プロファイルを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraNodeP name="swprofile1">
        <infraLeafS name="selectorswprofile11718" type="range">
            <infraNodeBlk name="single0" from_="101" to_="101"/>
            <infraNodeBlk name="single1" from_="102" to_="102"/>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-swprofile1ifselector"/>
    </infraNodeP>
</infraInfra>
```

ステップ 5 VLAN プールを設定します。

例：

```
 POST URL: https://<apic-ip>/api/node/mo/.xml

<polUni>
<infraInfra>
<fvnsVlanInstP name="VlanRange" allocMode="dynamic">
   <fvnsEncapBlk name="encap" from="vlan-100" to="vlan-400"/>
</fvnsVlanInstP>
</infraInfra>
</polUni>
```

ステップ 6 設定されたすべてのコントローラとそれらの動作状態を検索します。

例：

```
GET:
https://<apic-ip>/api/node/class/compCtrlr.xml?
<imdata>
<compCtrlr apiVer="5.1" ctrlrPKey="uni/vmmp-VMware/dom-productionDC/ctrlr-vcenter1"
deployIssues="" descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1" domName="
productionDC"
hostOrIp="esx1" mode="default" model="VMware vCenter Server 5.1.0 build-756313"
name="vcenter1" operSt="online" port="0" pwd="" remoteOperIssues="" scope="vm"
usr="administrator" vendor="VMware, Inc." ... />
</imdata>
```

ステップ 7 「ProductionDC」という VMM ドメイン下の「vcenter1」という名前の vCenter をハイパーバイザと VM で検索します。

例：

```
GET:
https://<apic-ip>/api/node/mo/comp/prov-VMware/ctrlr-productionDC-vcenter1.xml?query-target=children

<imdata>
<compHv descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/hv-host-4832" name="esx1"
state="poweredOn" type="hv" ... />
<compVm descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/vm-vm-5531" name="AppVM1"
state="poweredOff" type="virt" .../>
<hvsLNode dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/sw-dvs-5646" lacpEnable="yes"
lacpMode="passive" ldpConfigOperation="both" ldpConfigProtocol="lldp" maxMtu="1500"
mode="default" name="apicVswitch" .../>
</imdata>
```

ステップ 8 （オプション）分離されたエンドポイントの保持時間を設定します。

遅延は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 秒です。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<vmmProvP vendor="VMware" >
<vmmDomP name="mininetavs" mode="n1kv" enfPref="sw" epRetTime=”60”>
<infraRsVlanNs tDn="uni/infra/vlanns-inst-dynamic"/>
<vmmUsrAccP
name="defaultAccP"
usr="administrator"
pwd="admin"
/>
</vmmDomP>
</vmmProvP>
```

REST API を使用した読み取り専用 VMM ドメインの作成

読み取り専用 VMM ドメインは、REST API を使用して作成することができます。作成した後で VMM ドメインのアクセス モードを変更することはできません。変更しようとすると、エラー メッセージが表示されます。

始める前に

- セクション「 VMM ドメイン プロファイルを作成するための前提条件 （6 ページ） 」の前提条件を満たします。
- VMware vCenter の [Networking] タブの下で、フォルダに VDS が含まれていることを確認します。

  また、フォルダと VDS の名前が、作成する読み取り専用 VMM ドメインと正確に一致していることを確認します。

手順

ステップ 1 VMM ドメイン名、コントローラおよびユーザ クレデンシャルを設定します。

例：

```
POST URL: https://<api-ip>/api/node/mo/.xml
<polUni>
<vmmProvP vendor="VMware">
<!-- VMM Domain -->
<vmmDomP name="productionDC" accessMode="read-only">
<!-- Association to VLAN Namespace -->
<infraRsVlanNs tDn="uni/infra/vlanns-VlanRange-dynamic"/>
<!-- Credentials for vCenter -->
<vmmUsrAccP name="admin" usr="administrator" pwd="admin" />
<!-- vCenter IP address -->
<vmmCtrlrP name="vcenter1" hostOrIp="<vcenter ip address>" rootContName="<Datacenter
Name in vCenter>">
<vmmRsAcc tDn="uni/vmmp-VMware/dom-productionDC/usracc-admin"/>
</vmmCtrlrP>
</vmmDomP>
</vmmProvP>
```

例：

```
<polUni>
<vmmProvP vendor="VMware">
    <vmmDomP name="mininet" delimiter="@" >
   </vmmDomP>
</vmmProvP>
</polUni>
```

ステップ 2 VLAN ネームスペースの導入用の接続可能エンティティ プロファイルを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<infraInfra>
<infraAttEntityP name="profile1">
<infraRsDomP tDn="uni/vmmp-VMware/dom-productionDC"/>
</infraAttEntityP>
</infraInfra>
```

ステップ 3 インターフェイス ポリシー グループおよびセレクタを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraAccPortP name="swprofile1ifselector">
        <infraHPortS name="selector1" type="range">
            <infraPortBlk name="blk"
             fromCard="1" toCard="1" fromPort="1" toPort="3">
            </infraPortBlk>
     <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-group1" />
        </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
        <infraAccPortGrp name="group1">
            <infraRsAttEntP tDn="uni/infra/attentp-profile1" />
        </infraAccPortGrp>
    </infraFuncP>
</infraInfra>
```

ステップ 4 スイッチ プロファイルを作成します。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml

<infraInfra>
    <infraNodeP name="swprofile1">
        <infraLeafS name="selectorswprofile11718" type="range">
            <infraNodeBlk name="single0" from_="101" to_="101"/>
            <infraNodeBlk name="single1" from_="102" to_="102"/>
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-swprofile1ifselector"/>
    </infraNodeP>
</infraInfra>
```

ステップ 5 VLAN プールを設定します。

例：

```
 POST URL: https://<apic-ip>/api/node/mo/.xml

<polUni>
<infraInfra>
<fvnsVlanInstP name="VlanRange" allocMode="dynamic">
   <fvnsEncapBlk name="encap" from="vlan-100" to="vlan-400"/>
</fvnsVlanInstP>
</infraInfra>
</polUni>
```

ステップ 6 設定されたすべてのコントローラとそれらの動作状態を検索します。

例：

```
GET:
https://<apic-ip>/api/node/class/compCtrlr.xml?
<imdata>
<compCtrlr apiVer="5.1" ctrlrPKey="uni/vmmp-VMware/dom-productionDC/ctrlr-vcenter1"
deployIssues="" descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1" domName="
productionDC"
hostOrIp="esx1" mode="default" model="VMware vCenter Server 5.1.0 build-756313"
name="vcenter1" operSt="online" port="0" pwd="" remoteOperIssues="" scope="vm"
usr="administrator" vendor="VMware, Inc." ... />
```

```
</imdata>
```

ステップ 7 「ProductionDC」という VMM ドメイン下の「vcenter1」という名前の vCenter をハイパーバイザと VM で検索します。

例：

```
GET:
https://<apic-ip>/api/node/mo/comp/prov-VMware/ctrlr-productionDC-vcenter1.xml?query-target=children

<imdata>
<compHv descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/hv-host-4832" name="esx1"
state="poweredOn" type="hv" ... />
<compVm descr="" dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/vm-vm-5531" name="AppVM1"
state="poweredOff" type="virt" .../>
<hvsLNode dn="comp/prov-VMware/ctrlr-productionDC-vcenter1/sw-dvs-5646" lacpEnable="yes"
lacpMode="passive" ldpConfigOperation="both" ldpConfigProtocol="lldp" maxMtu="1500"
mode="default" name="apicVswitch" .../>
</imdata>
```

ステップ 8 （オプション）分離されたエンドポイントの保持時間を設定します。

遅延は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 秒です。

例：

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<vmmProvP vendor="VMware" >
<vmmDomP name="mininetavs" mode="n1kv" enfPref="sw" epRetTime=”60”>
<infraRsVlanNs tDn="uni/infra/vlanns-inst-dynamic"/>
<vmmUsrAccP
name="defaultAccP"
usr="administrator"
pwd="admin"
/>
</vmmDomP>
</vmmProvP>
```

次のタスク

読み取り専用 VMM ドメインを EPG にアタッチし、そのポリシーを設定できます。ただし、これらのポリシーは、VMware vCenter で VD へプッシュされません。

REST API を使用したエンドポイント保持の設定

始める前に

vCenter ドメインを設定済みである必要があります。

手順

デタッチされたエンドポイントの保持時間を設定するには、次の手順に従います:

遅延は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 秒です。

```
POST URL: https://<apic-ip>/api/policymgr/mo/uni.xml
<vmmProvP vendor="VMware" >

<vmmDomP name="mininetavs" epRetTime=”60”>
</vmmDomP>
</vmmProvP>
```

REST API を使用した、ブレード サーバのアクセス ポリシーのセットアップ

手順

ブレード サーバのアクセス ポリシーをセットアップします。

例：

```
POST: https://<ip or hostname APIC>/api/node/mo/uni.xml

<polUni>
                <infraInfra>
                <!-- Define LLDP CDP and LACP policies -->
                <lldpIfPol name="enable_lldp" adminRxSt="enabled" adminTxSt="enabled"/>
              <lldpIfPol name="disable_lldp" adminRxSt="disabled" adminTxSt="disabled"/>

                <cdpIfPol name="enable_cdp" adminSt="enabled"/>
                <cdpIfPol name="disable_cdp" adminSt="disabled"/>
<lacpLagPol name='enable_lacp' ctrl='15' descr='LACP' maxLinks='16' minLinks='1'
mode='active'/>
                <lacpLagPol name='disable_lacp' mode='mac-pin'/>


        <!-- List of nodes. Contains leaf selectors. Each leaf selector contains list
of node blocks -->
        <infraNodeP name="leaf1">
                <infraLeafS name="leaf1" type="range">
                <infraNodeBlk name="leaf1" from_="1017" to_="1017"/>
            </infraLeafS>
            <infraRsAccPortP tDn="uni/infra/accportprof-portselector"/>
        </infraNodeP>


        <!-- PortP contains port selectors. Each port selector contains list of ports.
It also has association to port group policies -->
        <infraAccPortP name="portselector">
                <infraHPortS name="pselc" type="range">
              <infraPortBlk name="blk" fromCard="1" toCard="1" fromPort="39" toPort="40">

                </infraPortBlk>
                <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-leaf1_PC"/>
            </infraHPortS>
        </infraAccPortP>

        <!-- FuncP contains access bundle group policies -->
        <infraFuncP>
                <!-- Access bundle group has relation to PC, LDP policies and to attach
 entity profile -->
            <infraAccBndlGrp name="leaf1_PC" lagT='link'>
```

```
            <infraRsLldpIfPol tnLldpIfPolName="enable_lldp"/>
            <infraRsLacpPol tnLacpLagPolName='enable_lacp'/>
            <infraRsAttEntP tDn="uni/infra/attentp-vmm-FI2"/>
        </infraAccBndlGrp>
    </infraFuncP>

    <!-- AttEntityP has relation to VMM domain -->
    <infraAttEntityP name="vmm-FI2">
            <infraRsDomP tDn="uni/vmmp-VMware/dom-productionDC"/>
        <!-- Functions -->
        <infraProvAcc name="provfunc"/>
        <!-- Policy overrides for VMM -->
        <infraAttPolicyGroup name="attpolicy">
            <!-- RELATION TO POLICIES GO HERE -->
            <infraRsOverrideCdpIfPol tnCdpIfPolName="enable_cdp"/>
            <infraRsOverrideLldpIfPol tnLldpIfPolName="disable_lldp"/>
            <infraRsOverrideLacpPol tnLacpLagPolName="disable_lacp"/>
        </infraAttPolicyGroup/>
    </infraAttEntityP>

    </infraInfra>
</polUni>

OUTPUT:
<?xml version="1.0" encoding="UTF-8"?>
<imdata></imdata>
```

NX-OS スタイルの CLI のタスク

ここでは、NX-OS スタイルの CLI を使用してタスクを実行する方法を示します。

- GUI タスクのリファレンスについては、VMM ドメイン プロファイルの作成 （5 ページ）とGUI を使用した、ブレード サーバのアクセス ポリシーのセットアップ （18 ページ）の項を参照してください。
- REST API タスクのリファレンスについては、REST API タスク （23 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 vCenter ドメイン プロファイルの作成

始める前に

ここでは、NX-OS スタイルの CLI を使用して vCenter ドメイン プロファイルを作成する方法を説明します。

手順

ステップ 1 CLI で、コンフィギュレーション モードに入ります。

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 VLAN ドメインを設定します。

例：

```
apic1(config)# vlan-domain dom1 dynamic
apic1(config-vlan)# vlan 150-200 dynamic
apic1(config-vlan)# exit
apic1(config)#
```

ステップ 3 この VLAN ドメインにインターフェイスを追加します。これらは VMware ハイパーバイザのアップリンク ポートに接続されるインターフェイスです。

例：

```
apic1(config)# leaf 101-102
apic1(config-leaf)# interface ethernet 1/2-3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 4 VMware ドメインを作成して VLAN ドメイン メンバーシップを追加します。

例：

```
apic1(config)# vmware-domain vmmdom1
apic1(config-vmware)# vlan-domain member dom1
apic1(config-vmware)#
```

特定のデリミタを使用してドメインを作成します。

例：

```
apic1(config)# vmware-domain vmmdom1 delimiter @
```

ステップ 5 DVS にドメイン タイプを設定します。

例：

```
apic1(config-vmware)# configure-dvs
apic1(config-vmware-dvs)# exit
apic1(config-vmware)#
```

ステップ 6 （オプション）分離されたエンドポイントの保持時間を設定します。

遅延時間は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 です。

例：

```
apic1(config)# vmware-domain <domainName>

apic1(config-vmware)# ep-retention-time <value>
```

ステップ 7 ドメインのコントローラを設定します。

例：

```
apic1(config-vmware)# vcenter 192.168.66.2 datacenter prodDC
apic1(config-vmware-vc)# username administrator
Password:
Retype password:
apic1(config-vmware-vc)# exit
apic1(config-vmware)# exit
apic1(config)# exit
```

（注） パスワードを設定する際には、Bash シェルが間違えて解釈することを避けるために、「$」または「!」などの特殊文字の前にバックスラッシュを付ける必要があります（「\$」）。エスケープのバックスラッシュは、パスワードを設定するときにだけ必要です。実際のパスワードにはバックスラッシュは表示されません。

ステップ 8 設定を確認します。

例：

```
apic1# show running-config vmware-domain vmmdom1
# Command: show running-config vmware-domain vmmdom1
# Time: Wed Sep  2 22:14:33 2015
  vmware-domain vmmdom1
    vlan-domain member dom1
    vcenter 192.168.66.2 datacenter prodDC
      username administrator password *****
    configure-dvs
      exit
    exit
```

NX-OS スタイルの CLI を使用した 読み取り専用 VMM ドメインの作成

NX-OS スタイルの CLI を使用すれば、読み取り専用VMM ドメインを作成できます。

VMM ドメインのアクセスモードは、これを作成した後に変更することはできません。変更しようとすると、エラー メッセージが表示されます。

始める前に

- セクション「VMM ドメイン プロファイルを作成するための前提条件 （6 ページ）」の前提条件を満たします。
- VMware vCenter の [Networking] タブの下で、フォルダに VDS が含まれていることを確認します。

  また、フォルダと VDS の名前が、作成する読み取り専用 VMM ドメインと正確に一致していることを確認します。

手順

ステップ 1 CLI で、コンフィギュレーション モードに入ります。

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 VLAN ドメインを設定します。

例：

```
apic1(config)# vlan-domain dom1 dynamic
apic1(config-vlan)# vlan 150-200 dynamic
apic1(config-vlan)# exit
apic1(config)#
```

ステップ 3 この VLAN ドメインにインターフェイスを追加します。これらは VMware ハイパーバイザのアップリンク ポートに接続されるインターフェイスです。

例：

```
apic1(config)# leaf 101-102
apic1(config-leaf)# interface ethernet 1/2-3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 4 VMware ドメインを作成して VLAN ドメイン メンバーシップを追加します。

例：

```
apic1(config)# vmware-domain vmmdom1 access-mode readonly
apic1(config-vmware)# vlan-domain member dom1
apic1(config-vmware)#
```

特定のデリミタを使用してドメインを作成します。

例：

```
apic1(config)# vmware-domain vmmdom1 delimiter @
```

ステップ 5 DVS にドメイン タイプを設定します。

例：

```
apic1(config-vmware)# configure-dvs
apic1(config-vmware-dvs)# exit
apic1(config-vmware)#
```

ステップ 6 （オプション）分離されたエンドポイントの保持時間を設定します。

遅延時間は 0 ～ 600 秒の範囲で選択できます。デフォルトは 0 です。

例：

```
apic1(config)# vmware-domain <domainName>

apic1(config-vmware)# ep-retention-time <value>
```

ステップ 7 ドメインのコントローラを設定します。

例：

```
apic1(config-vmware)# vcenter 192.168.66.2 datacenter prodDC
apic1(config-vmware-vc)# username administrator
Password:
Retype password:
apic1(config-vmware-vc)# exit
apic1(config-vmware)# exit
apic1(config)# exit
```

（注） パスワードを設定する際には、Bashシェルが間違えて解釈することを避けるために、「$」または「!」などの特殊文字の前にバックスラッシュを付ける必要があります（「\$」）。エスケープのバックスラッシュは、パスワードを設定するときにだけ必要です。実際のパスワードにはバックスラッシュは表示されません。

ステップ 8 設定を確認します。

例：

```
apic1# show running-config vmware-domain vmmdom1
# Command: show running-config vmware-domain vmmdom1
# Time: Wed Sep  2 22:14:33 2015
  vmware-domain vmmdom1
    vlan-domain member dom1
    vcenter 192.168.66.2 datacenter prodDC
      username administrator password *****
    configure-dvs
      exit
    exit
```

次のタスク

読み取り専用 VMM ドメインを EPG にアタッチし、そのポリシーを設定できます。ただし、これらのポリシーは、VMware vCenter で VD へプッシュされません。