Cisco ACI の VMware VDS との統合

この章は、次の内容で構成されています。

仮想マシン ネットワーキング ポリシーの設定

Cisco Application Policy Infrastructure Controller（APIC）は、VMware vCenter などのサードパーティの VM マネージャ（VMM）と統合して、Cisco Application Centric Infrastructure（ACI）の利点を仮想化インフラストラクチャに拡張します。Cisco APIC では管理者が VMM システム内で Cisco ACI ポリシーを使用できるようにします。

次のモードの Cisco ACI および VMware VMM 統合がサポートされています。

- VMware VDS：Cisco ACI と統合するとき、VMware vSphere 分散スイッチ（VDS）では Cisco ACI ファブリック内に VM ネットワークを構成できます。
- Cisco ACI Virtual Edge：Cisco ACI Virtual Edge のインストールおよび設定の方法については、*Cisco.com* の『*Cisco ACI Virtual Edge*インストール 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 Application Virtual Switch（AVS）：Cisco ACI を搭載した Cisco AVS をインストールおよび設定する方法については、Cisco.com で Cisco AVS のドキュメントを参照してください。

（注） Cisco APIC が多くのフォルダを持つ VMware vCenter に接続されている場合、新しいポート グループを Cisco APIC から VMWare vCenter にプッシュするときに遅延が発生することがあります。

Cisco APIC でサポートされる VMware VDS バージョン

VMware vSphere Distributed Switch（DVS）の異なるバージョンは、異なるバージョンの Cisco Cisco Application Policy Infrastructure Controller（APIC）をサポートします。Cisco APIC と VMware コンポーネントとの互換性については、『Cisco ACI 仮想互換性マトリクス』を参照してください。

VMware vSphere

サポートされているリリースバージョンについては、『ACI 仮想化互換性マトリクス』を参照してください。

ESXi ホストの考慮事項の追加

VMware vSphere Distributed Switch（VDS）を使用して仮想マシン マネージャ（VMM）ドメインに追加の VMware ESXi ホストを追加する場合は、ESXi ホストのバージョンが vCenter に既に展開されている分散仮想スイッチ（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。

VIC カードと UCS サーバを備えた ESXi 6.5 ホスト

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。

VMware vCenter ハイ アベイラビリティ

VMware vSphere 6.5 で導入された VMware vCenter High Availability（VCHA）は、VMware vCenter の単一障害点を排除します。

VCHA では VMware vCenter アクティブ ノードに障害が発生すると、パッシブ ノードが引き継ぎます。パッシブ ノードには、アクティブ ノードと同じ IP アドレス、資格情報、およびその他の情報があります。VCHA を利用するために、新しい VMM 構成は必要ありません。パッシブ ノードが引き継ぎ到達可能になると、Cisco APIC では自動的に再接続します。

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。**[ホーム（Home）] > [ネットワーキング（Networking）] > [DatacenterX] > [DVS-X] > [アクション メニュー（Actions Menu）] > [アップグレード分散スイッチ（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。

- DVS モードの VMM 統合により、APIC からリーフ スイッチ ポートと ESXi ハイパーバイザ ポート間のポート チャネルを構成できます。LACP は、ポート チャネルの拡張モードまたは基本モードのいずれかでサポートされます。ACI および VMware 側のサポートのマトリクスは次のとおりです。

表 *1 : LACP* サポート

	3.2.7 より前の **ACI** リリース	**3.2.7** 以降の **ACI** リリース	**6.6** より前の **VMware DVS** リリース	**6.6** 以降の **VMware DVS** リリース
基本 LACP	はい	はい	はい	いいえ
Enhanced LACP	いいえ	はい	はい	はい

VMware 側の DVS をバージョン 6.6 以降にアップグレードする場合、LACP を基本モードから拡張モードに再構成する必要があります。以前のバージョンの DVS（6.6 より前）で

拡張 LACP（eLACP）をすでに構成している場合は、DVS 6.6 にアップグレードするときに eLACP を再構成する必要はありません。

（注） DVS バージョン 6.6 以降、基本的な LACP はサポートされていません。

LACP を基本から拡張に移行すると、トラフィックが失われる可能性があります。メンテナンス期間中に移行を実行します。詳細な移行手順については、基本 LACP から拡張 LACP への移行 （20 ページ） を参照してください。

eLACP の詳細、および eLACP を VMM ドメインに追加するには、この章で後述する「拡張 *LACP* ポリシー サポート」セクションを参照してください。

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。

Cisco ACI と VMware コンストラクトのマッピング

表 *2 : Cisco Application Centric Infrastructure（ACI）と VMware* コンストラクトのマッピング

Cisco ACI に関する用語	**VMware** 用語
エンドポイント グループ（EPG）	ポート グループ
LACP Active	• IP ハッシュに基づくルート（ダウンリンク ポート グループ） • LACP 有効/アクティブ（アップリンク ポート グループ）
LACP Passive	• IP ハッシュに基づくルート（ダウンリンク ポート グループ） • LACP 有効/アクティブ（アップリンク ポート グループ）
MAC ピニング	• 発信元仮想ポートに基づくルート • LACP 無効
MAC Pinning-Physical-NIC-Load	• 物理 NIC ロードに基づくルート • LACP 無効
静的チャネル - モード オン	• IP ハッシュに基づくルート（ダウンリンク ポート グループ） • LACP 無効
Virtual Machine Manager（VMM）ドメイン	vSphere Distributed Switch（VDS）
VM コントローラ	vCenter (データセンター)

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

対応する Cisco ACI と VMware コンストラクトのマッピング（ACI）および VMware 用語の表については、このガイドのセクション Cisco Application Centric Infrastructure を参照してください。

VMware VDS	デフォルト値	Cisco APIC ポリシーを使用して構成できますか?
名前	VMM ドメイン名	はい（ドメインから派生）
説明	APIC 仮想スイッチ	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	はい（Cisco APIC リリース 4.2(1) から）
アップリンク名プレフィックス	uplink	はい（Cisco APIC リリース 4.2(1) から）
最大 MTU	9000	はい
LACP ポリシー	disabled	対応
アラーム	フォルダ レベルに 2 アラーム追加	いいえ

（注） Cisco APIC ではポート ミラーリングを管理しません。ポート ミラーリングは、VMware vCenter から直接構成できます。Cisco APIC では構成を上書きしません。Cisco APIC が構成を管理している場合、Cisco APIC では障害が発生します。Cisco APIC が構成を管理しない場合、Cisco APIC では障害は発生しません。

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）

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
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	無効	はい
偽装された転送	無効	はい
MAC 変更	無効	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 コントローラが Cisco Application Centric Infrastructure（ACI）ファブリックに接続できるようにす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 Application Policy Infrastructure Controller（APIC）はコントローラと通信し、のちに仮想ワークロードに適用されるポート グループなどのネットワーク設定を公開します。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.

（注） この項での VMM ドメインの例は、vCenter ドメインです。

削除後の VMM ドメインのプッシュ

Cisco APICで作成した VMware 分散仮想スイッチ（DVS）を VMware vCenter から誤って削除する可能性があります。その場合、Cisco APIC ポリシーは VMware vCenter に再度プッシュされません。

VMM ドメインを VMware vCenter に再度プッシュするには、Cisco APIC VMware vCenter 接続を切断します。これにより、再接続後に Cisco APIC により VMM ドメインが VMware vCenter に再度プッシュされ、DVS が VMware vCenter で再作成されます。

読み取り専用 VMM ドメイン

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。

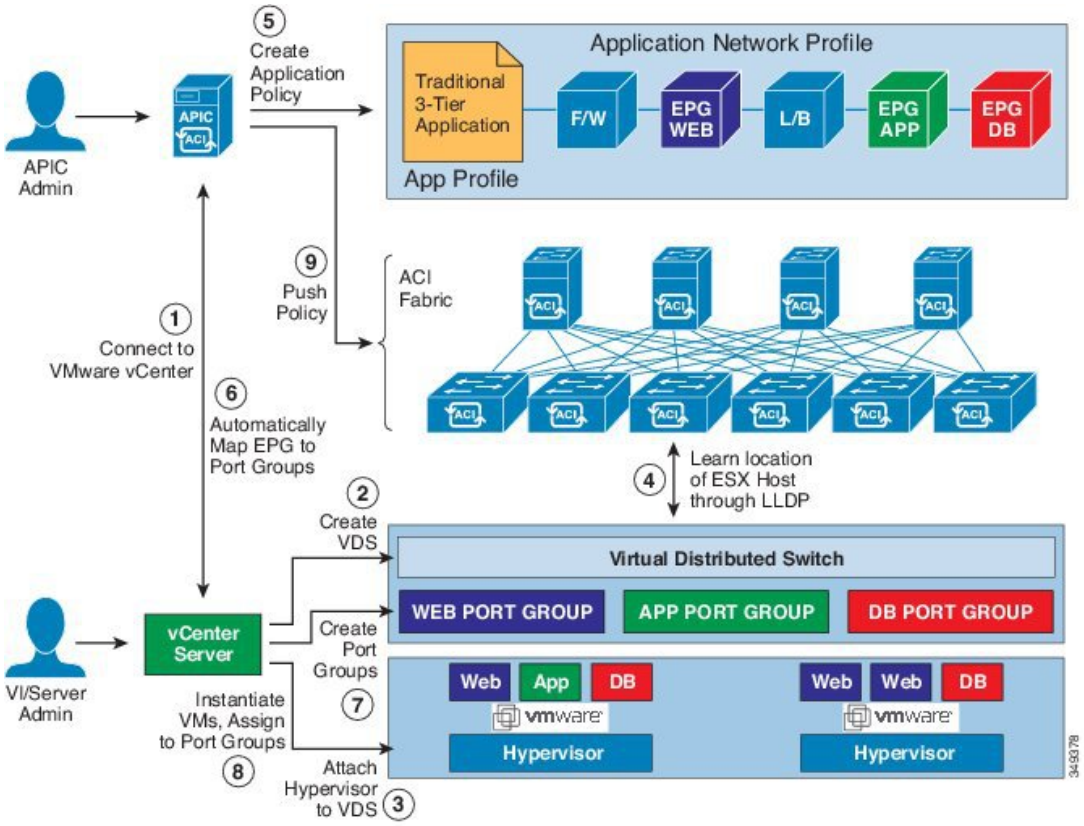
VMM ドメイン プロファイルを作成するための前提条件

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 プロファイルを作成または選択します。
- インターフェイス プロファイルを作成または選択します。
- インターフェイス ポリシー グループを作成または選択します。
- VLAN プールを作成または選択します。
- vCenter ドメインを作成します。
- vCenter クレデンシャルを作成します。

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。手動で割り当てたインフラ VLAN を含む範囲を定義しないでください。そのような定義をした場合、Cisco Application Policy Infrastructure Controller（APIC）のバージョンによっては障害が発生することがあります。インフラ VLAN を OpFlex 統合の一部として拡張する必要がある場合は、特定の使用例やオプションを設定します。

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。

作業ペインの [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 （12 ページ）
- REST API 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 を使用した 読み取り専用 VMM ドメインの作成

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 （10 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。

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 （8 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。

読み取り専用 VMM ドメインを読み取り/書き込みに昇格させる

Cisco APIC リリース 4.0(1) 以降では、既存の読み取り専用 VMM ドメインを、完全管理の読み取り/書き込み VMM ドメインに昇格させることができます。これにより、VMware vCenter での VDS のインベントリの情報を表示できるだけでなく、Cisco APIC を利用して管理することができます。

読み取り専用の VMM ドメインの作成方法は 読み取り専用 VMM ドメインの作成 （12 ページ） で説明されています。

既存の読み取り専用 VMM ドメインを昇格する前に、読み取り専用 VMM ドメインの昇格に関する注意事項 （13 ページ） で説明されているガイドラインと制限を慎重に検討してください。

VMM ドメインを読み取り専用から読み取り/書き込みに昇格させることで、APIC が VMM ドメインを監視および管理できるだけでなく、EPG をポート グループとして関連付けできるようになります。Cisco APIC GUI、NX-OS style CLI, または REST API を使用して読み取り専用 VMM ドメインを促進できます。Cisco APIC GUI の手順については、このセクションを参照してください。手順NX-OS スタイルの CLI を使用した、読み取り専用 VMM ドメインのプロモート および REST API を使用して読み取り専用 VMM ドメインに昇格させる については付録を参照してください。

読み取り専用 VMM ドメインの昇格に関する注意事項

読み取り専用 VMM ドメインを読み取り/書き込みに昇格させる際は、次の点に注意してください。

- 読み取り専用のドメインを昇格させるには、vCenter サーバ上のドメインの VDS のための、特定のネットワーク フォルダ構造が必要です。既存の VDS がフォルダに収められておらず、データセンターの直下に置かれている場合には、VDS と同じ名前のフォルダを作

成し、VDS をそのフォルダに入れてから、ドメインを読み取り/書き込みに昇格させてください。これは、APIC が適切に管理できるようにするためです。VDS がデータセンターの直下に設定されているドメインを昇格させると、APIC は、新しいフォルダの内部に新しい VDS を作成します。

- フル マネージドに昇格する予定の読み取り専用 VMM ドメイン用に vCenter でポート グループを作成するときは、 *<tenant-name>|<application-name>|<EPG-name>* 形式で名前を付けることをお勧めします。

  VMM ドメインを完全管理に昇格させて、ドメインに EPG を関連付けるときに、この標準形式の名前が付いているポート-グループはすべて、自動的に EPG に追加されます。

  ポート グループ名の別の形式を選択した場合は、ドメインの昇格後に、既存のポート グループから、APIC によって EPG 用に作成された新しいポート グループに、すべての VM を手動で再割り当てする必要があります。

  - EPG を作成して VMM ドメインに関連付けます。

    VMM ドメインで、ポート グループの EPG ポリシーを見つけられないと障害が発生します。

  - 既存のポート グループから仮想マシン（VM）を削除し、EPG に接続します。

（注） このプロセスの実行時にトラフィックが消失する場合があります。

  - VM がポート グループから分離されたら、古いポート グループを vCenter から削除します。

    すべての VM をポート グループから分離する必要があります。そうしないとポート グループを削除できません。

- ドメインを読み取り専用から読み取り/書き込みに移行する際は、移行プロセス時に使用可能な VLAN が使い果たされる可能性を避けるために、一意で、かつ物理ドメイン範囲から独立している VLAN 範囲を使用することをお勧めします。
- 複数の VMM および VMware vCenter で同じ EPG を使用する必要がある場合は、ドメインと同じ名前の Link Aggregation Group（LAG）ポリシーを設定します。EPG は 1 つの LAG ポリシーにのみ接続できます。異なる LAG ポリシーを使用する場合は、それぞれの LAG ポリシーを異なる EPG に関連付ける必要があります。

  詳細については、このガイドの Enhanced LACP ポリシーのサポート （16 ページ） に関する項を参照してください。

Cisco APIC GUI を使用して読み取り専用 VMM ドメインを昇格させる

Cisco APIC GUI を使用して、読み取り専用 VMM ドメインを昇格させることができます。

始める前に

管理対象のドメインに読み取り専用VMMドメインを昇格するための手順では、次の前提条件を満たすことを前提にしています。

- 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 （8 ページ）の前提条件を満たす
- 読み取り専用 VMM ドメインの作成 （12 ページ）に記載されているとおりに、読み取り専用を構成する
- VMware vCenter の [Networking] タブで、昇格しようとしている読み取り専用 VMM ドメインと全く同じ名前のネットワーク フォルダに VDS が含ま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 アクセスエンティティ プロファイル（AEP）を読み取り専用VMMドメインに関連付けます。

a) **[Fabric]** > **[Access Policies]** > **[Policies]** > **[Global]** > **[Attachable Access Entity Profiles]** に移動します。

b) AEP を選択し、完全管理に昇格させる読み取り専用 VMM ドメインに関連付けます。

ステップ 3 VMM ドメインを昇格させます。

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

b) **[VMM Domains]** > **[Vmware]** フォルダーを展開します。

c) 昇格する読み取り専用 VMM ドメインを選択します。

d) [Access Mode] の設定を [Read Write Mode] に変更します。

e) ドロップダウンメニューから [VLAN Pool] を選択し、VLAN プールをドメインに関連付けます。

f) [Submit] をクリックして変更を保存します。

ステップ 4 新しい Link Aggregation Group（LAG）ポリシーを作成します。

vCenter バージョン 5.5 以降を使用している場合は、「Cisco APIC GUI を使用して DVS アップリンク ポート グループの LAG を作成する （18 ページ）」の説明に従って、ドメインで Enhanced LACP 機能を使用するために LAG ポリシーを作成する必要があります。

それ以外の場合は、このステップを省略できます。

ステップ 5 LAG ポリシーを適切な EPG に関連付けます。

vCenter バージョン 5.5 以降を使用している場合は、「Cisco APIC GUI を使用したアプリケーション EPG を拡張 LACP ポリシーを備えた VMware vCenter ドメインに関連付ける （19 ページ）」の説明に従って、Enhanced LACP 機能を使用するために LAG ポリシーを EPG に関連付ける必要があります。

それ以外の場合は、このステップを省略できます。

次のタスク

これで、VMM ドメインに接続したすべての EPG と、設定したすべてのポリシーが、VMware vCenter で VDS にプッシュされます。

Enhanced LACP ポリシーのサポート

（APIC）リリース 3.2(7) では、さまざまな Link Aggregation Control Protocol（LACP）ポリシーをさまざまな分散仮想スイッチ（DVS）アップリンク ポート グループに適用することにより、アップリンク ロードバランシングを改善できます。Cisco Application Policy Infrastructure Controller

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、すべての DVS アップリンク ポート グループに同じ LACP ポリシーが適用されていました。Cisco APIC リリース 3.2(7) より前は、Cisco APIC を備えた VMware リンク集約グループ（LAG）を管理することはできませんでした。

ACI 側で拡張 LACP ポリシーを有効にすると、設定が DVS にプッシュされます。後で、ACI 側でポリシーを削除しても、拡張LACPポリシーを有効にした後は元に戻すことができないため、DVS 側で引き続き拡張 LACP を使用できます。

（注） 拡張 LACP は、ACI 側または DVS 側のいずれかで有効にできます。

VMware vCenter 仮想マシン マネージャ（VMM）ドメインを Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 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。

Cisco APIC リリース 5.2(1) 以降、拡張 LACP ポリシーは、サービス グラフで使用されるレイヤ 4 ～ レイヤ 7 サービス デバイスのインターフェイスでサポートされます。『*Cisco APIC* レイヤ*4*～ レイヤ*7*サービス展開ガイド』にある「論理デバイスの定義」セクションを参照してください。

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。
- 拡張 LACP 設定を削除せずに、3.2(7) より前のバージョンの 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に拡張 LACP 構成を削除する （21 ページ）を参照してください。
- Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge の場合、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**」をお勧めします。
- 拡張 LACP を介して Cisco ACI Virtual Edge ドメインにトラフィックが存在し、アップリンクの数を増減すると、5 秒または 10 秒のトラフィック損失が発生します。
- 拡張 LACP LAG ポリシー名が以前の拡張 LACP リンク集約グループ（LAG）ポリシー アップリンクの名前と競合すると、トラフィックが中断されます。DVS ドメインの ELACP-DVS という名前の拡張 LACP LAG ポリシーがある場合、ポリシーで構成されたアップリンク番号に応じて、自動的に ELACP-DVS-1、ELACP-DVS-2、ELACP-DVS-3 などの名前が付けられます。

  以前のポリシー アップリンク名と競合する名前で別の拡張 LAG ポリシーを構成または追加しようとすると、トラフィックの損失が発生します。この問題を解決するには、LAG ポリシーを削除し、別の名前で再作成します。
- レイヤ 4 ～レイヤ 7 サービス デバイスのインターフェイスは、Cisco APIC リリース 5.2(1) の LAG ポリシーをサポートします。ただし、VMM ドメインにレイヤ 4 ～ レイヤ 7 のサービス デバイスがある場合、その VMM ドメイン全体で拡張 LAG を使用することはできません（5.2(1) より前のリリースに適用されます）。これは、レイヤ 4 ～ レイヤ 7 のサービス デバイスのインターフェイスが LAG を使用していない場合、拡張 LAG にアップリンクを接続できないためです。

  リリース 5.2(1) からのダウングレード

インストールするリリース	使用される LAG	必須のアクション
5.2(1) より前のリリース	EPG	操作は不要です。

インストールするリリース	使用される LAG	必須のアクション
5.2(1) より前のリリース	レイヤ 4 ～ レイヤ 7 サービス デバイスの EPG およびインターフェイス	VMM ドメイン全体から LAG を削除します。
3.2(7) より前のリリース	レイヤ 4 からレイヤ 7 サービス デバイスの EPG および/またはインターフェイス	VMM ドメイン全体から LAG を削除します。

- 拡張 LACP 構成は、スイッチング モードが ネイティブに設定されている *VMware vDS VMM* ドメインおよび *AVE VMM* ドメインでのみ使用できます。

  AVE VMM ドメインのスイッチング モードが *AVE* に設定されている場合、GUI は論理デバイス構成中にクラスタ インターフェイスで拡張 LACP ポリシーを構成することをサポートしません。これは、AVE スイッチング モードが ネイティブに設定されている場合、ポート グループが *AVE VM* に接続されるためです。 そのポート グループからのトラフィックは、最初に AVE に送られ、次に AVE が送信します。したがって、AVE モードのこれらのポート グループでは、アップリンクが有効になっていません。AVE スイッチング モードが ネイティブ に設定されている場合、そのポート グループからのトラフィックは AVE VM をバイパスし、DVS 経由で直接物理ポートに移動します。

Cisco APIC GUI を使用して DVS アップリンク ポート グループの LAG を作成する

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 Link Aggregation Group（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 アプリケーション セントリック インフラストラクチャ (ACI) 仮想 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。

（注） 拡張 LAG ポリシーを作成する前に、ポート チャネル ポリシーを設定する必要があります。vCenter ドメイン プロファイルを作成するときに、ポート チャネル ポリシーを作成できます。

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]** > ***[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 アプリケーション セントリック インフラストラクチャ (ACI) 仮想 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。

Cisco APIC GUI を使用したアプリケーション EPG を拡張 LACP ポリシーを備えた VMware vCenter ドメインに関連付ける

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 [Domains (VMs and Bare-Metals)] を右クリックし [Add VMM Domain Association] 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) （オプション）**[デリミタ（Delimiter）]** フィールドで次のうちいずれかを入力します。**|**, **~**, **!**, **@**, **^**, **+**, or **=**。

記号を入力しなかった場合、ポリシーにシステムのデフォルトのデリミタの **|** が表示されます。

d) 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。

基本 LACP から拡張 LACP への移行

この手順を使用して、既存の VMware vCenter ドメイン VDS で基本 LACP を拡張 LACP に移行します。

前のセクション「*Cisco APIC GUI* を使用して *DVS* アップリンク ポート グループの *LAG* を作成する」、「*Cisco APIC GUI* を使用して拡張 *LACP* ポリシーを使用してアプリケーション *EPG* を *VMware vCenter* ドメインに関連付ける」で説明したように、拡張 LACP 構成には次の重要な手順が含まれます。

- VMware VMM ドメインの VSwitch ポリシーで拡張ラグ ポリシーを構成します。
- EPG ごとに VMware VMM ドメインの関連付けで拡張 LAG ポリシーを選択します。

上記の両方の手順を実行しないと、トラフィックは適切に転送されません。2 番目のステップでは、各 EPG のポート グループのチーミングとフェールオーバーでアクティブなアップリンク設定を処理します。これは、VMware VMM ドメインを使用するすべての EPG に対して実行する必要があります。

LACP を基本から拡張に移行すると、自動化されていてもトラフィックが失われる可能性があるため、メンテナンス期間中に移行を実行することをお勧めします。この手順は、メンテナンス期間に移行が実行された場合でも、トラフィックの損失を最小限に抑えるためのものです。

手順

ステップ 1 DVS を VMware vCenter 上の拡張 LACP にアップグレードします（APIC 経由ではありません）。次の手順を実行します。

a) **[メニュー（Menu）** から **[ネットワーキング（Networking）]** を選択し、DVS を見つけます。

b) DVS を右クリックし、表示されるポップアップ画面で、**[アップグレード（Upgrade）]** > **[LACP サポートの強化（Enhance LACP Support）]** を選択します。

この手順では、LACP 構成、*ELAG* を作成し、*ELAG* グループを使用するようにポート グループのアクティブなアップリンク構成を自動的に更新します。物理ネットワーク アダプタの構成が更新されるため、この手順の実行中にトラフィックの損失が予想される可能性があります。APIC は障害 F3290 を発生させます。

c) VDS で更新された LACP 設定を確認します。

確認するには、**[DVS]** > **[構成（Configure）]** > **[設定（Settings）]** > **[LACP]** を選択します。

ステップ 2 既存の VMware VMM ドメインの vSwitch ポリシーに同じ拡張 LAG ポリシー (*ELAG*) を作成してください。LAG ポリシーの作成の詳細については、「*Cisco APIC GUI* を使用した *DVS* アップリンク ポート グループの *LAG* の作成手順」を参照してください。

障害 F3290 がクリアされます。

ステップ 3 EPG ごとに VMware VMM ドメインの関連付けで拡張ラグ ポリシーを選択します。詳細については、「*Cisco APIC GUI* を使用してアプリケーション *EPG* を拡張 *LACP* ポリシーを備えた *VMware vCenter* ドメインに関連付ける」を参照してください。

ステップ 4 転送が正常に機能しているかどうかを確認します。

ダウングレード前に拡張 LACP 構成を削除する

3.2(7) より前のリリースに Cisco Application Policy Infrastructure Controller（APIC）をダウングレードする前に、拡張LACP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。

（注） ダウングレードする前に、LAG サポートに基づいて必要なアクションの Enhanced LACP の制限事項 （17 ページ） セクションを参照してください。

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 分散仮想スイッチ（DVS）に関連付けられている、サービス グラフで使用される L4～L7 サービス デバイスのすべての EPG およびインターフェイスから LAG の関連付けを削除します。

この手順を実行している間、トラフィックの損失が予想されます。

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

3.2(7) より前の Cisco APIC リリースにダウングレードします。

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 （22 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構成
- REST API を使用したエンドポイント保持の設定

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。

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

トランク ポート グループ

トランク ポート グループを使用して、VMware virtual machine manager (VMM) ドメインのエンドポイント グループ (EPG) のトラフィックを集約します。

トランク ポート グループの詳細については、 トランク ポート グループについて を参照してください。

トランク ポート グループを作成する手順については、次のセクションを参照してください。

- GUI を使用した トランク ポート グループの作成 （24 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
- REST API を使用した 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 グループがテナントに依存していないことを確認してください。

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 ペインで、**[VMM ドメイン（VMM Domains）] > [VMware] > [ドメイン（domain）] > [トランク ポート グループ（Trunk Port Groups）]** を選択し、**[トランク ポート グループの作成（Create Trunk Port Group）]** を選択します。

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。。

トランク ポート グループに接続された仮想マシンは、MAC アドレス宛ではないユニキャスト トラフィックを受信します。次のオプションがあります。

- **有効**
- **無効（Disabled）**（デフォルト）

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。

フィールドは、ポリシーがすぐに解決されるか、リーフ スイッチで必要なのはいつかを指定します。次のオプションがあります。

- **即時**
- **オンデマンド**（デフォルト）

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。

このフィールドでは、VM 内のネットワーク アダプターの新しい MAC アドレスを定義できます。次のオプションがあります。

- **有効**（デフォルト）
- **無効**

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。

フィールドは、偽装転送を許可するかどうかを指定します。偽装転送は、ネットワーク アダプタが偽装と識別したトラフィックの送信を開始した場合に行われます。このセキュリティ ポリシーでは、仮想ネットワーク アダプタの有効なアドレスと、仮想マシンによって生成された 802.3 イーサネット フレーム内の送信元アドレスを比較して、それらが一致することを確認します。次のオプションがあります。

- **有効**（デフォルト）
- **無効**

f) **[拡張ラグ ポリシー（Enhanced Lag Policy）]** ドロップダウン リストから、適用するリンク集約制御プロトコル（LACP）ポリシーを持つアップリンクを選択します。

ポリシーは、リンク集約グループ（LAG）で構成され、ロードバランシング アルゴリズムに関連付けられている分散仮想スイッチ（DVS）アップリンク ポート グループで構成されています。LACP ポリシーを含む少なくとも 1 つのアップリンクを DVS アップリンク ポート グループに適用しておく必要があります。これにより、アップリンク ロード バランシングを改善できます。

拡張 LACP の詳細については、このガイドのセクション Enhanced LACP ポリシーのサポート （16 ページ） を参照してください。

g) **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。

h) **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。

VMware vSphere vMotion の使用

VMware vSphere vMotion を使用すると、サービスを中断することなく、異なる物理ホスト間で仮想マシン (VM)を移動できます。

ドキュメントを含む VMware vSphere vMotion の詳細については、VMware の Web サイトを参照してください。

VMware vMotion を使用して VM を VMware 分散仮想スイッチ（DVS）の背後に移動すると、トラフィックが数秒から数分中断されます。中断は、デフォルトのローカルエンドポイント保持間隔である最大 15 分間続くことがあります。中断は、次の 2 つのケースの両方が当てはまる場合に発生します。

- 仮想スイッチが逆アドレス解決プロトコル（RARP）のみを使用して VM の移動を示す場合
- ブリッジ ドメインが、IP インスペクションが有効になっている First Hop Security (FHS) ポリシーに関連付けられている場合

この問題を回避するには、ブリッジ ドメインから FHS ポリシーの関連付けを解除するか、ポリシーを IP インスペクションが無効になっているポリシーに変更します。

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

VMM 統合の目的でブレード サーバ システムを Cisco ACI Cisco Application Centric Infrastructure に統合する場合（たとえば、Cisco Unified Computing System（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場合）、次の注意事項を考慮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 サーバー アップリンクの Cisco Application Policy Infrastructure Controller（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、Cisco Discovery Protocol（CDP）または Link Layer Discovery Protocol（LLDP）のいずれかに依存しています。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。
- Cisco APIC はファブリック インターコネクトとブレード サーバーを管理しません。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。
- Cisco 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 サーバを使用している場合、UCSM 2.2.4b 以降、CDP と LLDP の両方がサポートされます。UCS B シリーズ サーバが以前のファームウェアを使用している場合、LLDP はサポートされません。
- Cisco UCS Manager では、CDP はデフォルトで無効になっています。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 Cisco APIC に送信しません。

状況：これにより、VMware vCenter と Cisco 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。[送信（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

VMware vCenter 権限を設定すると、Cisco Application Policy Infrastructure Controller（APIC）は、DVS を作成するために VMware API コマンドを VMware vCenter に送信できます。権限を設定し、Cisco APIC によりポート グループを公開し、必要なすべてのアラートをリレーできるようになます。

Cisco APIC から vCenter を設定するには、VMware vCenter で次の最小権限セットが許可されるクレデンシャルである必要があります。

- アラーム

  Cisco APIC は 2 つのアラームをフォルダに作成します。1 つは DVS 用で、もう 1 つはポートグループ用です。Cisco APIC でEPG またはドメイン ポリシーが削除されると、アラームが発生します。ただし、関連付けられている仮想マシン（VM）があるため、DVS またはポートグループのアラームを削除することはできません。

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

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

- Host
  - Host.Configuration.Advanced settings
  - Host.Local operations.Reconfigure virtual machine
  - Host.Configuration.Network configuration
- 仮想マシン

前述の権限に加えてサービス 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

サービスVMのオーケストレーション機能を使用してサービスVMを展開する場合は、前述の権限に加えて次の権限を有効にします。

これらの機能の詳細については、『*Cisco APIC* レイヤ *4* ～ レイヤ *7* サービス導入ガイド』の「Service VM Orchestration」の章を参照してください。

- データストア
  - 領域の割り当て
  - データストアの参照
  - 低レベルのファイル操作
  - ファイルの削除
- **Host**
  - **Local operations.Delete virtual machine**
  - **Local operations.Reconfigure virtual machine**
- **Resource**
  - **Assign virtual machine to resource pool**
- 仮想マシン
  - **Inventory.Create new**
  - **Inventory.Create from existing**
  - **Inventory.Remove**
  - **Configuration.Add new disk**
  - **Provisioning.Deploy template**
  - **Provisioning.Clone template**
  - **Provisioning.Clone virtual machine**
  - **Provisioning.Customize**
  - **Interaction**（**all**）
- グローバル
  - 顧客属性の管理
  - カスタム属性の設定

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

トリガされたインベントリには、virtual machine manager（VMM）コントローラから Cisco Application Policy Infrastructure Controller（APIC）インベントリをプルおよび更新するための手動トリガ オプションが用意されています。これは通常のシナリオでは必要ありません。エラーが発生した場合にのみ慎重に使用してください。

プロセスの再起動、リーダーシップの変更、バックグラウンドでの定期的な 24 時間インベントリ監査が生じた場合、Cisco APIC はインベントリのプルを行って、VMM インベントリと VMM コントローラ インベントリ間の適合性を維持します。場合によっては、VMware vCenter API でエラーが発生し、Cisco APIC では再試行しても VMware vCenter からインベントリを完全にダウンロードできないことがあります。Cisco APIC は、ユーザーに見える障害のあるこの状態を示します。この場合、トリガされたインベントリにより、Cisco APIC VMM から VMware vCenter へのインベントリのプルを開始できます。

Cisco APIC VMM 構成と VMware vCenter VDS 構成間の同期を維持しません。VMware vCenter から VDS 設定を直接変更する場合、Cisco APIC ではユーザー設定（PVLAN 構成以外）を上書きしません。

ESXi ホストの物理的な移行

ESXi ホストを物理的に移行するには、この手順のタスクを実行します。

手順

ステップ 1 ホストをメンテナンス モードにするか、別の方法で仮想マシン（VM）のワークロードを退避させます。

ステップ 2 VMware VDS、Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge、または Cisco Application Virtual Switch から ESXi ホストを削除します。

ステップ 3 新しいリーフ スイッチまたはリーフ スイッチのペアに ESXi ホストを物理的に配線し直します。

ステップ 4 VMware VDS、Cisco アプリケーション セントリック インフラストラクチャ (ACI) 仮想 Edge、または Cisco Application Virtual Switch に ESXi ホストを再び追加します。

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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。