Cisco ACI の仮想マシン ネットワーキング

この章は、次の内容で構成されています。

Cisco ACI の VM ネットワーキングによる Virtual Machine Manager のサポート

ACI VM ネットワー キングの利点

Cisco Application Centric Infrastructure（ACI）稼働マシン（VM）ネットワーキングは、複数のベンダーからハイパーバイザをサポートします。ハイパーバイザに対し、高パフォーマンスでスケーラブルな仮想データセンターインフラストラクチャへのプログラム可能で自動化されたアクセスを提供します。

プログラム可能性と自動化は、スケーラブルなデータ センター仮想化インフラストラクチャにおける重要な機能です。Cisco ACI オープン REST API により、ポリシー モデル ベースの Cisco ACI ファブリックとの仮想マシンの統合およびオーケストレーションが可能になります。Cisco

ACI VM ネットワーキングでは、複数のベンダーからハイパーバイザにより管理されている仮想および物理ワークロードの両方でのポリシーの一貫した適用を可能にします。

接続可能なエンティティ プロファイルにより、VM のモビリティと、Cisco ACI ファブリック内の任意の場所にワークロードを簡単に配置できます。Cisco Application Policy Infrastructure Controller（APIC）は、一元化されたトラブルシューティング、アプリケーション ヘルス スコア、および仮想化モニタリングを提供します。Cisco ACI マルチハイパーバイザ VM 自動化により、手動構成と手動エラーが削減または排除されます。これにより、仮想化データセンターが多数の VM を信頼性が高く、コスト効率の優れた方法でサポートすることが可能になります。

サポートされている製品とベンダー

Cisco ACI は、次の製品およびベンダーの virtual machine managers（VMM）をサポートします。

- **Cisco Unified Computing System Manager（UCSM）**

  Cisco UCSM の統合は、Cisco Cisco APIC リリース 4.1(1) 以降でサポートされています。詳細については、『*Cisco ACI 仮想化ガイド、リリース 4.1(1)*』の「Cisco ACI と Cisco UCSM の統合」の章を参照してください。

- **Cisco Application Centric Infrastructure (ACI) 仮想ポッド (vPod)**

  Cisco ACI vPod は、Cisco APIC リリース 4.0(2) 以降で一般に利用可能です。詳細については、Cisco.com で Cisco ACI vPod のマニュアルを参照してください。

- **Cloud Foundry**

  Cloud Foundry と Cisco ACI との統合は、Cisco APIC リリース 3.1(2) 以降でサポートされています。詳細については、Cisco.com のナレッジ ベース記事「Cisco ACI と Cloud Found 統合」を参照してください。

- **Kubernetes**

  詳細については、Cisco.com の ナレッジ ベースの記事、 『Cisco ACI と Kubernetes の統合』を参照してください。

- **Microsoft System Center Virtual Machine Manager（SCVMM）**

  詳細については、Cisco.com の『*Cisco ACI 仮想化ガイド*』の「Microsoft SCVMM を搭載した Cisco ACI」および「Microsoft Windows Azure Pack を搭載した Cisco ACI」の章を参照してください。

- **OpenShift**

  詳細については、Cisco.com の OpenShift のマニュアルを参照してください。

- **Openstack**

  詳細については、Cisco.com の OpenStack のマニュアルを参照してください。

- **Red Hat 仮想化 (RHV)**

  詳細については、Cisco.com のナレッジ ベースの記事、 『Cisco ACI および Red Hat の統合』を参照してください。

- **VMware 仮想分散スイッチ（VDS）**

  詳細については、『Cisco ACI 仮想化ガイド』の「Cisco "ACI と VMware VDSの統合」の章を参照してください。

検証済みの相互運用可能な製品の最新のリストについては、『Cisco ACI Virtualization Compatibility Matrix』を参照してください）。

Cisco ACI と VMware コンストラクトのマッピング

Cisco Application Centric Infrastructure（ACI）と VMware は、同じ構造を説明するために異なる用語を使用します。このセクションでは、Cisco ACI および VMware の用語のマッピング表を示します。この情報は VMware vSphere 分散スイッチ（VDS）に関連しています。

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、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	VDS
VM コントローラ	vCenter (データセンター)

Virtual Machine Manager ドメインの主要コンポーネント

ACI ファブリック Virtual Machine Manager（VMM）ドメインにより、管理者は仮想マシン コントローラの接続ポリシーを設定できます。ACI VMM ドメイン ポリシーの基本的なコンポーネントは次のとおりです。

- **Virtual Machine Manager ドメイン プロファイル**：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。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。VMM ドメイン プロファイルには、次の基本コンポーネントが含まれます。
  - **クレデンシャル**：有効な VM コントローラ ユーザ クレデンシャルを APIC VMM ドメインと関連付けます。
  - **コントローラ**：ポリシーの適用ドメインの一部である VM コントローラへの接続方法を指定します。たとえば、コントローラは VMM ドメインの一部である VMware vCenter への接続を指定します。

（注） 1 つのドメインに VM コントローラの複数のインスタンスを含めることができますが、それらは同じベンダーのものである必要があります（VMware または Microsoft など）。

- **EPG の関連付け**：エンドポイント グループにより、エンドポイント間の接続と可視性が VMM ドメイン ポリシーの範囲内に規制されます。VMM ドメイン EPG は次のように動作します。
  - APIC は、これらの EPG をポート グループとして VM コントローラにプッシュします。
  - 1 つの EPG は、複数の VMM ドメインをカバーでき、1 つの VMM ドメインには複数の EPG を含めることができます。
- **接続可能エンティティ プロファイルの関連付け**：VMM ドメインを物理ネットワーク インフラストラクチャと関連付けます。接続可能エンティティ プロファイル（AEP）は、多数のリーフ スイッチ ポートで VM コントローラ ポリシーを展開するための、ネットワーク インターフェイス テンプレートです。AEP は、使用できるスイッチやポートおよびその設定方法を指定します。
- **VLAN プールの関連付け**：VLAN プールは、VMM ドメインが消費する VLAN カプセル化に使用する VLAN ID または範囲を指定します。

Virtual Machine Manager のドメイン

APIC VMM ドメイン プロファイルは、VMM ドメインを定義するポリシーです。VMM ドメイン ポリシーは APIC で作成され、リーフ スイッチにプッシュされます。

VMM ドメインは以下を提供します。

- 複数の VM コントローラ プラットフォームに対してスケーラブルな耐障害性サポートを可能にする、ACI ファブリックの共通レイヤ
- ACI ファブリック内の複数のテナントに対する VMM サポート

VMM ドメインには、VMware vCenter や Microsoft SCVMM Manager などの VM コントローラと、VM コントローラと対話するための ACI API に必要なクレデンシャルが含まれます。VMM ドメインはドメイン内の VM モビリティを実現できますが、ドメイン間は実現できません。単一の VMM ドメイン コントローラに VM コントローラの複数のインスタンスを含めることはできますが、同じタイプである必要があります。たとえば、1 つの VMM ドメインに、それぞれが複数の VM を実行する複数のコントローラを管理する多くの VMware vCenter を含めることができますが、SCVMM Manager も含めることはできません。VMM ドメインはコントローラ要素（pNIC、vNIC、VM 名など）をインベントリに含め、コントローラにポリシーをプッシュして、ポート グループなどの必要な要素を作成します。ACI VMM ドメインは VM モビリティなどのコントローラ イベントを監視し、状況に応じて応答します。

VMM ドメイン VLAN プールの関連付け

VLAN プールは、トラフィック VLAN ID のブロックを表します。VLAN プールは共有リソースで、VMM ドメインおよびレイヤ 4 ～レイヤ 7 のサービスなど、複数のドメインで使用できます。

各プールには、作成時に定義された割り当てタイプ（静的または動的）があります。割り当てタイプによって、含まれる ID が Cisco APIC で自動割り当てに使用されるか（動的）、管理者によって明示的に設定されるか（静的）が決まります。デフォルトでは、VLAN プールに含まれるすべてのブロックの割り当てタイプはプールと同じですが、ユーザは動的プールに含まれるカプセル化ブロックの割り当てタイプを静的に変更できます。これを行うと、動的割り当てからそれらが除外されます。

VMM ドメインは、1 つの動的 VLAN プールにのみ関連付けることができます。デフォルトでは、VMM ドメインに関連付けられた EPG への VLAN ID の割り当ては、Cisco APIC によって動的に行われます。動的割り当てはデフォルトの推奨設定ですが、管理者は代わりにエンドポイント グループ（EPG）に VLAN 識別子を静的に割り当てることができます。この場合、使用する ID は VMM ドメインに関連付けられている VLAN プールのカプセル化ブロックから選択し、その割り当てタイプを静的に変更する必要があります。

Cisco APIC は、リーフ ポート上の VMM ドメイン VLAN を EPG イベントに基づいてプロビジョニングします（リーフ ポート上の静的バインドまたは VMware vCenter や Microsoft SCVMM などのコントローラからの VM イベントに基づいて）。

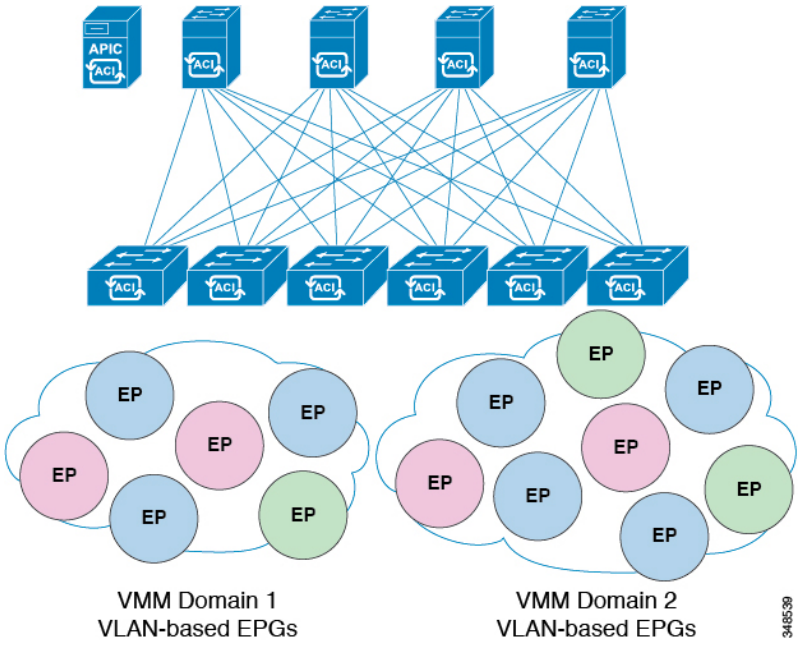
（注） 動的 VLAN プールでは、VLAN と EPG の関連付けが解除されると、5 分以内に自動的に EPG に再関連付けされます。

（注） 動的 VLAN 関連付けは構成ロールバックの一部ではありません。つまり、EPG またはテナントが最初に削除され、バックアップから復元された場合、動的VLANプールから新しいVLANが自動的に割り当てられます。

VMM ドメイン EPG の関連付け

Cisco Application Centric Infrastructure（ACI）ファブリックは、テナント アプリケーション プロファイルエンドポイント グループ（EPG）を仮想マシン マネージャ（VMM）ドメインに関連付けます。Cisco ACI では、Microsoft Azure などのオーケストレーション コンポーネントによって自動的に、またはそのような構成を作成する Cisco Application Policy Infrastructure Controller（APIC）管理者によって行われます。1 つの EPG は、複数の VMM ドメインをカバーでき、1 つの VMM ドメインには複数の EPG を含めることができます。

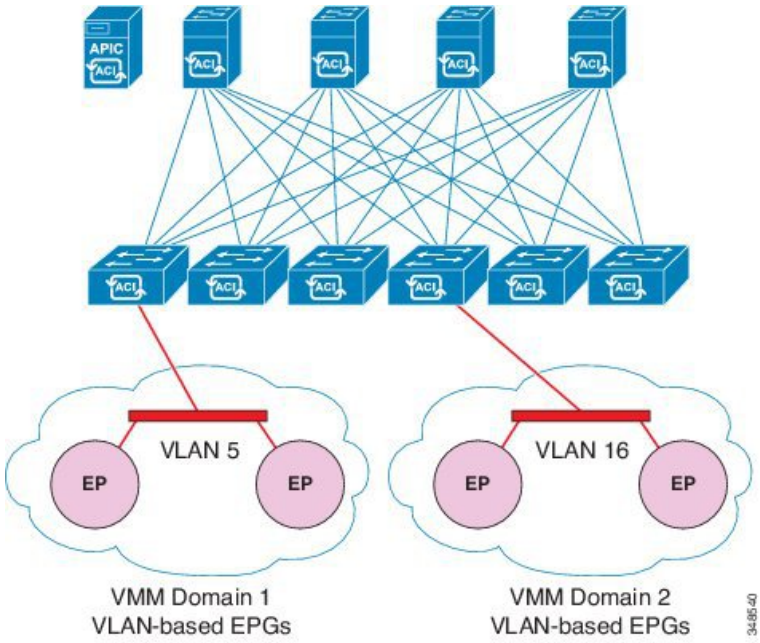
図 *1 : VMM* ドメイン *EPG* の関連付け



前の図では、同じ色のエンド ポイント（EP）が同じ EPG の一部です。たとえば、2 つの異なる VMM ドメインにあるにもかかわらず、すべての緑の EP は同じ EPG にあります。

仮想ネットワークおよび VMM ドメイン EPG の容量情報については、最新の『*Cisco ACI* の検証済みスケーラビリティ ガイド』を参照してください。

図 *2 : VMM* ドメイン *EPG VLAN* の消費



（注） 同じポートに重複する VLAN プールがない場合は、複数の VMM ドメインを同じリーフ スイッチに接続できます。同様に、リーフ スイッチの同じポートを使用しない場合、異なるドメインで同じ VLAN プールを使用できます。

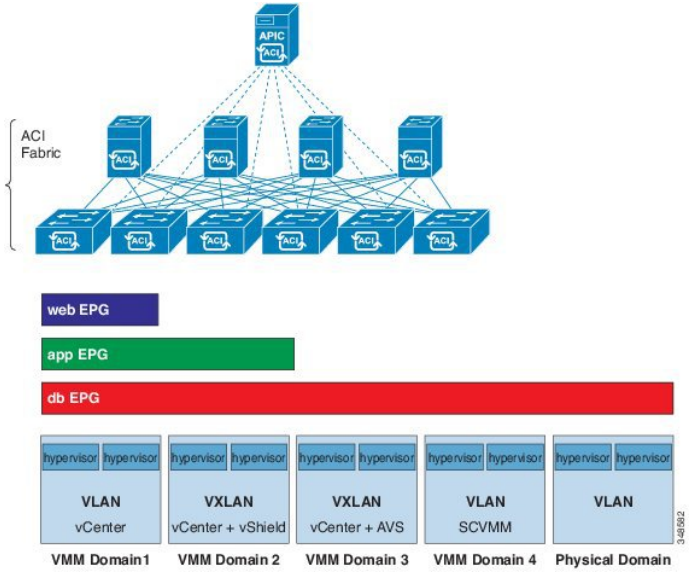
EPG は複数の VMM ドメインを次のように使用できます。

- カプセル化 ID を使用して VMM ドメイン内の EPG が識別されます。Cisco APIC は自動的に ID を管理したり、管理者が静的に選択したりできます。一例は、VLAN、仮想ネットワーク ID（VNID）です。
- EPG は複数の物理ドメイン（baremetal サーバの場合）または仮想ドメインにマッピングできます。各ドメインで異なる VLAN または VNID カプセル化を使用できます。

（注） デフォルトでは、Cisco APIC は EPG の VLAN の割り当てを動的に管理します。VMware DVS 管理者は、EPG に対して特定の VLAN を設定できます。その場合、VLAN は、VMM ドメインに関連付けられているプール内の静的割り当てブロックから選択されます。

アプリケーションは、複数の VMM ドメインに導入できます。

図 *3:* ファブリック内の複数の *VMM* ドメインと *EPG* の増大



VMM ドメイン内の VM のライブ マイグレーションがサポートされていても、VMM ドメイン間の VM のライブ マイグレーションはサポートされません。

（注） VMM ドメインが関連付けられている EPG にリンクされているブリッジ ドメインで VRF を変更すると、ポート グループが削除され、vCenter に再び追加されます。これにより、EPG が VMM ドメインから展開解除されます。これは想定されている動作です。

トランク ポート グループについて

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。Cisco Application Policy Infrastructure Controller (APIC) GUI の [テナント (Tenant)] タブで設定されている通常のポート グループとは異なり、[VM ネットワーキング (VM Networking)] タブでトランク ポート グループが設定されます。通常のポート グループは、EPG 名の *T*|*A*|*E* 形式に従います。

同じドメインの EPG の集約は、トランク ポート グループに含まれるカプセル化ブロックとして指定された VLAN の範囲に基づきます。EPG のカプセル化を変更するか、またはトランク ポート グループのカプセル化ブロックを変更した場合は、EGP を集約する必要があるかどうかを判別するために、集約が再評価されます。

トランク ポート グループは、集約される EPG に割り当てられた VLAN などのネットワーク リソースのリーフ展開を制御します。EPG には、ベース EPG とマイクロセグメント (uSeg) EPG の両方が含まれています。uSeg EPG の場合、トランク ポート グループの VLAN 範囲は、プライマリおよびセカンダリ VLAN の両方を含む必要があります。

詳細については、次の手順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
- 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

接続可能エンティティ プロファイル

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

（注） 2 つのリーフ スイッチ間での VPC ドメインを作成するとき、同じスイッチの生成を次のいずれかのどちらのスイッチも必要があります。

- 1: なしで Cisco Nexus N9K スイッチの生成」EX」または「FX」、スイッチ名前末尾にたとえば、N9K 9312TX
- 2: Cisco Nexus N9K スイッチ間での生成」EX」または「FX」スイッチ モデルの名前の末尾にたとえば、N9K-93108TC-EX

スイッチなど、これらの 2 つが互換性のある VPC ピアではありません。代わりに、同じ世代のスイッチを使用します。

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

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

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

- AEP は許容される VLAN の範囲を定義しますが、それらのプロビジョニングは行いません。EPG がポートに展開されていない限り、トラフィックは流れません。AEP で VLAN プールを定義しないと、EPG がプロビジョニングされても VLAN はリーフ ポートでイネーブルになりません。

- リーフ ポートで静的にバインディングしている EPG イベントに基づいて、または VMware vCenter や Microsoft Azure Service Center Virtual Machine Manager（SCVMM）などの外部コントローラからの VM イベントに基づいて、特定の VLAN がリーフ ポート上でプロビジョニングされるかイネーブルになります。
- 添付されているエンティティ プロファイルに関連付けられているすべてのポートに関連付けられているアプリケーション Epg を導入するアプリケーション Epg に直接と関連付けることができますプロファイルのエンティティが添付されています。AEP では、アタッチ可能なエンティティ プロファイルに関連付けられているセレクタの一部であるすべてのインターフェイスで導入されている EPG (infraRsFuncToEpg) との関係が含まれている設定可能な一般的な機能 (infraGeneric) があります。

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

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

EPG ポリシーの解決および展開の緊急度

エンドポイント グループ（EPG）が virtual machine manager（VMM）ドメインに関連付けられるときは常に、管理者は解像度と展開設定を選択して、ポリシーをリーフ スイッチにプッシュするタイミングを指定できます。

解決の緊急性 (Resolution Immediacy)

- 事前プロビジョニング：VM コントローラが仮想スイッチ（例：VMware vSphere 分散スイッチ（VDS））に接続される前でも、ポリシー（例：VLAN、VXLAN バインディング、契約、またはフィルタ）をリーフ スイッチにダウンロードすることを指定します。これにより、スイッチ上の設定が事前プロビジョニングされます。

  「この設定は、ハイパーバイザまたは VM コントローラ用の管理トラフィックに対して、Cisco Application Policy Infrastructure Controller（APIC）VMM ドメインに関連付けられた仮想スイッチ（VMM スイッチ）を使用している状況で役立ちます」

  Cisco Application Centric Infrastructure（ACI）リーフ スイッチで VLAN など VMM ポリシーを展開する場合、Cisco APIC により、VM コントローラおよび Cisco ACI リーフ スイッチを介して両方のハイパーバイザから CDP/LLDP 情報を収集する必要があります。ただし、VM コントローラが同じ VMM ポリシー（VMM スイッチ）を使用してハイパーバイザまたは Cisco APIC と通信することが想定されている場合は、VM コントローラまたはハイパーバイザの管理トラフィックに必要なポリシーがまだ導入されていないため、ハイパーバイザの CDP または LLDP の情報を収集することは絶対にできません。

事前プロビジョニングを直ちに使用する場合、ポリシーは、CDP/LLDP のネイバーシップには関係なく、Cisco ACI リーフ スイッチにダウンロードされます。VMM スイッチに接続されているハイパーバイザ ホストがない場合でも可能です。

- 即時：EPG ポリシー（契約およびフィルタを含む）が、DVS への ESXi ホスト接続時に関連するリーフ スイッチ ソフトウェアにダウンロードされることを指定します。VM コントローラ/リーフ ノード接続を解決するために LLDP または OpFlex 権限が使用されます。

  VMM スイッチにホストを追加すると、ポリシーがリーフにダウンロードされます。ホストからリーフへの CDP または LLDP のネイバーシップが必要です。

- オンデマンド：ESXi ホストが DVS に接続され、VM がポート グループに配置されるときにのみ、ポリシー（例：VLAN, VXLAN バインディング、契約、またはフィルタ）がリーフ ノードにプッシュされることを指定します。

  VMM スイッチにホストが追加されると、ポリシーがリーフにダウンロードされます。VM はポート グループ（EPG）に配置する必要があります。ホストからリーフへの CDP または LLDP のネイバーシップが必要です。

  即時とオンデマンドの両方において、ホストおよびリーフが LLDP または CDP のネイバーシップを失うと、ポリシーは削除されます。

（注） OpFlex ベースの VMM ドメインでは、ハイパーバイザの OpFlex エージェントが、EPG への VM/EP 仮想ネットワーク インターフェイス カード（vNIC）の接続をリーフ OpFlex プロセスに報告します。オンデマンド即時解決を使用する場合、次の条件に当てはまる場合、EPG VLAN/VXLAN は**すべて**のリーフ ポート チャネル ポート、仮想ポート チャネル ポート、またはその両方でプログラムされます。

- ハイパーバイザは、直接またはブレードスイッチを介して接続されたポート チャネルまたは仮想ポート チャネルのリーフに接続されます。
- VM またはインスタンス vNIC が EPG に接続されています。
- ハイパーバイザは、EPG または VMM ドメインの一部として接続されます。

Opflex ベースの VMM ドメインは、Microsoft Security Center Virtual Machine Manager（SCVMM）と HyperV、および Cisco Application Virtual Switch（AVS）です。

展開の緊急性

ポリシーがリーフ ソフトウェアにダウンロードされると、展開の緊急度によってポリシーをいつハードウェア ポリシーの Content-Addressable Memory (CAM) にプッシュするかを指定できます。

- 即時：リーフ ソフトウェアにダウンロードされたポリシーがハードウェアのポリシー CAM ですぐにプログラミングされるように指定します。
- オンデマンド：最初のパケットがデータ パス経由で受信された場合にのみポリシーがハードウェアのポリシー CAM でプログラミングされるように指定します。このプロセスは、ハードウェアの領域を最適化するのに役立ちます。

（注） オン デマンドの緊急性指定と MAC 固定の VPC の両方を使用する場合、 最初のエンドポイントがリーフごとの EPG を学習するまでは、EPG コントラクトはリーフの三重 Content-Addressable Memory (TCAM) にプッシュされません。このような場合、VPC ピア間での TCAM 使用率が不均一になる可能性があります。(通常、コントラクトは両方の両方のピアにプッシュされます)。

VMM ドメインを削除するためのガイドライン

次の手順に従って、VMM ドメインを自動的に削除する APIC リクエストによって関連する VM コントローラ（VMware vCenter または Microsoft SCVMM）がトリガーされ、プロセスが正常に完了すること、および ACI ファブリックに孤立した EPG が残されないことを確認します。

1. VM 管理者は、APIC によって作成されたすべての VM を、ポート グループ（VMware vCenter の場合）または VM ネットワーク（SCVMM の場合）からデタッチする必要があります。

   Cisco AVS の場合、VM 管理者は Cisco AVS に関連付けられている vmk インターフェイスも削除する必要があります。

2. ACI 管理者は、APIC で VMM ドメインを削除します。APIC は、VMware VDS または Cisco AVS または SCVMM 論理スイッチおよび関連するオブジェクトの削除をトリガーします。

（注） VM 管理者が仮想スイッチまたは関連オブジェクト（ポート グループまたは VM ネットワークなど）を削除することはできません。上記のステップ 2 の完了時に、APIC に仮想スイッチの削除を許可します。VMM ドメインが APIC で削除される前に VM 管理者が VM コントローラから仮想スイッチを削除した場合、EPG は APIC で孤立する可能性があります。

このシーケンスに従わない場合、VM コントローラは APIC VMM ドメインに関連付けられている仮想スイッチを削除します。このシナリオでは、VM 管理者は VM コントローラから VM および vtep アソシエーションを手動で削除してから、以前に APIC VMM ドメインに関連付けられていた仮想スイッチを削除します。

NetFlow と仮想マシン ネットワーキング

NetFlow と仮想マシン ネットワーキングについて

NetFlowテクノロジは、ネットワーク トラフィック アカウンティング、従量制のネットワーク課金、ネットワーク プランニング、そしてサービス拒絶に対する監視機能、ネットワーク監視、社外マーケティング、およびサービス プロバイダと企業顧客向け両方のデータ マイニングなど、主要な一連のアプリケーションの計測基盤を効果的にします。Cisco は NetFlow エクスポート データの収集、データ量削減、ポスト プロセッシングを行う一連の NetFlow アプリケーションを提供し、エンド ユーザー アプリケーションが NetFlow データへ簡単にアクセスできるようにします。この機能により、同じレベルを介したトラフィックのモニタリングを実行する、NetFlowがデータ センターを通過するトラフィックのモニタリングを有効にすると、Cisco Application Centric Infrastructure (Cisco ACI) ファブリック。

ハードウェアがレコードからコレクタに直接エクスポートする代わりに、レコードはスーパーバイザ エンジンで処理され、必要な形式で標準の NetFlow コレクタにエクスポートされます。

NetFlow の詳細については、*Cisco APIC* と *NetFlow* ナレッジ ベース記事を参照してください。

仮想マシンのネットワーキングの NetFlow エクスポータ ポリシーについて

仮想マシン manager エクスポータ ポリシー (netflowVmmExporterPol) では、レポートのサーバまたはNetFlow コレクタに送信されたフローの収集されたデータに関する情報について説明します。NetFlow コレクタは、外部、標準の NetFlow プロトコルをサポートし、パケットを受け入れているエンティティが付いている NetFlow ヘッダーが無効です。

エクスポータ ポリシーには、次のプロパティがあります。

- VmmExporterPol.dstAddr]: この必須プロパティは、NetFlow フロー パケットを受信する NetFlow コレクタの IPv4 または IPv6 アドレスを指定します。このホストの形式である必要があります (つまり、「/32」または「/128」)。IPv6 アドレスは、vSphere 分散スイッチ (vDS) バージョン 6.0 でサポートされている以降です。
- VmmExporterPol.dstPort]: この必須プロパティは着信接続を受け入れるコレクタを有効に NetFlow コレクタ アプリケーションでリッスンするポートを指定します。
- VmmExporterPol.srcAddr]: このオプションのプロパティは、エクスポートされた NetFlow フロー パケットで発信元アドレスとして使用される IPv4アドレスを指定します。

VMware vSphere 分散スイッチでの NetFlow サポート

VMware vSphere 分散スイッチ (VDS) では、次の注意事項と NetFlow をサポートしています。

- 外部のコレクタは、ESX 経由で到達可能である必要があります。ESX は、仮想ルーティングおよび一般（VRF）をサポートしていません。
- ポート グループでは、有効にしたり、NetFlow を無効にすることができます。
- VDS は、フロー レベルのフィルタ リングをサポートしていません。

VMware vCenter で、次の VDS パラメータを設定します。

- コレクタの IP アドレスとポート。IPv6は、 VDS バージョン 6.0 以降でサポートされています。これらは必須です。
- 発信元の IP アドレス。これは任意です。
- アクティブなフロー タイムアウト、フローのアイドル タイムアウト、およびサンプリング レート。これらは任意です。

GUI を使用した、VM ネットワーキングのための NetFlow エクスポータ ポリシーの設定

次の手順では、VM のネットワー キングの NetFlow エクスポータ ポリシーを設定します。

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、[展開 **ポリシー** > **インターフェイス** > **NetFlow** 。

ステップ 3 右クリックして **VM Networking 社で働いて NetFlow エクスポータ**] を選択します **VM Networking 社で働いて NetFlow エクスポータを作成** します。

ステップ 4 **Create NetFlow Exporter for VM Networking** ダイアログボックスで、必要に応じてフィールドに入力します。

ステップ 5 [送信（Submit）] をクリックします。

GUI を使用した VMM ドメイン下での NetFlow エクスポータ ポリシーの利用

次の手順では、GUI を使用して VMM ドメイン下で NetFlow エクスポータ ポリシーを利用します。

手順

ステップ 1 メニュー バーで、 **[Virtual Networking]** > **[Inventory]** を選択します。

ステップ 2 **Navigation** ウィンドウで **VMM Domains** フォルダを展開し **VMware** を右クリックし、**Create vCenter Domain** を選択します。

ステップ 3 **Create vCenter Domain** ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します:

a) **NetFlow Exporter Policy** ドロップダウンリストで、目的のエクスポータ ポリシーを選択します。 または、新しいポリシーを作成します。

b) **Active Flow Timeout** フィールドで、秒単位で目的のアクティブなフロータイムアウトを入力します。

Active Flow Timeout パラメータでは、アクティブなフローが開始してから NetFlow が待機する遅延を指定します。その後で、NetFlow は集したデータを送信します。範囲は 60 ～ 3600 です。デフォルト値は 60 です。

c) **Idle Flow Timeout** フィールドで、目的のアイドル フロー タイムアウトを秒単位で入力します。

Idle Flow Timeout パラメータでは、アイドルなフローが開始してから NetFlow が待機する遅延を指定します。その後で、NetFlow は集したデータを送信します。範囲は 10 ～ 300 です。デフォルト値は 15 です。

d) (VDS のみ) **Sampling Rate** フィールドに、目的のサンプリング レートを入力します。

Sampling Rate パラメータでは、毎回収集したパケットの後で、NetFlow がいくつのパケットをドロップするかを指定します。0 の値を指定した場合、NetFlow はパケットをドロップしません。範囲は 0 ～ 1000 です。デフォルト値は 0 です

ステップ 4 [送信（Submit）] をクリックします。

GUI を使用してエンドポイント グループ上の NetFlow から VMM ドメインへの関連付けを有効化する

次の手順により、エンドポイント グループ上の NetFlow と VMM ドメインの関連付けを有効にします。

始める前に

次を設定する必要があります。

- アプリケーション プロファイル
- アプリケーション エンドポイント グループ

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 **[作業]** ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 左側の [ナビゲーション] ウィンドウで、***tenant_name*** > **[アプリケーション プロファイル]** > ***application_profile_name*** > **[アプリケーション EPG]** > ***application_EPG_name*** を展開します。

ステップ 4 [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 5 **[VMM ドメインの関連付けの追加（Add VMM Domain Association）]** ダイアログボックスで、必要に応じてフィールドに記入します。ただし、**[NetFlow]** 領域で **[有効（Enable）]** を選択します。

ステップ 6 [送信（Submit）] をクリックします。

VMM 接続のトラブルシューティング

次の手順では、VMM 接続の問題を解決します。

手順

ステップ 1 Application Policy Infrastructure Controller（APIC）でインベントリの再同期をトリガします。

APIC で、インベントリの再同期をトリガする方法の詳細については、次のナレッジ ベース記事を参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_VMM_OnDemand_Inventory_in_APIC.html

ステップ 2 手順 1 で、影響を受ける EPG の問題が解決しない場合は、VMM ドメインの事前プロビジョニングを使用して解決の緊急性を設定します。

「事前プロビジョニング」は、ネイバー隣接関係または OpFlex 許可、その後の VMM ドメイン VLAN プログラミングのダイナミック特性の必要性がありません。解決の緊急度に関する詳細は、次の EPG ポリシーの解決および展開の緊急度を参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/aci-fundamentals/b_ACI-Fundamentals/b_ACI-Fundamentals_chapter_01011.html#concept_EF87ADDAD4EF47BDA741EC6EFDAECBBD

ステップ 3 手順 1 と 2 では問題が解決せず、すべての VM に問題が見られる場合は、VM コントローラ ポリシーを削除し、ポリシーを再度追加します。

（注） そのコントローラ ポリシーを削除すると、コントローラ上のすべての VM のトラフィックに影響があります。

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。