Cisco ACI の仮想マシン ネットワーキング

この章の内容は、次のとおりです。

- Cisco ACI の VM ネットワーキングによる Virtual Machine Manager のサポート （1 ページ）
- Virtual Machine Manager ドメインの主要コンポーネント （3 ページ）
- Virtual Machine Manager のドメイン （4 ページ）
- VMM ドメイン VLAN プールの関連付け （5 ページ）
- VMM ドメイン EPG の関連付け （5 ページ）
- トランク ポート グループについて （8 ページ）
- 接続可能エンティティ プロファイル （9 ページ）
- EPG ポリシーの解決および展開の緊急度 （10 ページ）
- VMM ドメインを削除するためのガイドライン （12 ページ）
- NetFlow と仮想マシン ネットワーキング （12 ページ）
- VMM 接続のトラブルシューティング （21 ページ）

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 ACI 仮想マシン（VM） ネットワーキングは、複数のベンダーからのハイパーバイザをサポートしています。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 ファブリックのオーケストレーションと仮想マシン統合できます。Cisco ACI VM ネットワーキングにより、複数のベンダーのハイパーバイザで管理される仮想ワークロードと物理ワークロードの両方にわたって一貫してポリシーを適用できます。

接続可能エンティティ プロファイルにより、VM モビリティと Cisco ACI ファブリック内の任意の場所のワークロードの配置を簡単に実現できます。Cisco Application Policy Infrastructure Controller (APIC) は、一元化されたトラブルシューティング、アプリケーションのヘルス スコア、および仮想化の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 の自動化は、手動による構成の必要性と人的エラーの発生を抑えるか、さらには排除します。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ベンダー

Cisco ACI では、次の製品とベンダーからの仮想マシン マネージャ (VMM) をサポートしています。

- Cisco Application Centric Infrastructure (ACI) Virtual Pod (vPod)

  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。

  （注） 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。

- Cisco Application Centric Infrastructure Virtual Edge

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

- Cisco Application Virtual Switch（AVS）

  詳細については、Cisco.com の『Cisco ACI 仮想化ガイド』の「Cisco AVS での Cisco ACI」の章と Cisco AVS のマニュアルを参照してください。

- クラウド ファンドリー

  Cisco ACI とクラウド ファンドリーの統合は、Cisco APIC リリース 3.1(2) 以降でサポートされます。

- 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 ACI 仮想化ガイド』の「Cisco ACI と Microsoft SCVMM」および「Cisco ACI と Microsoft Windows Azure Pack」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）。

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）。

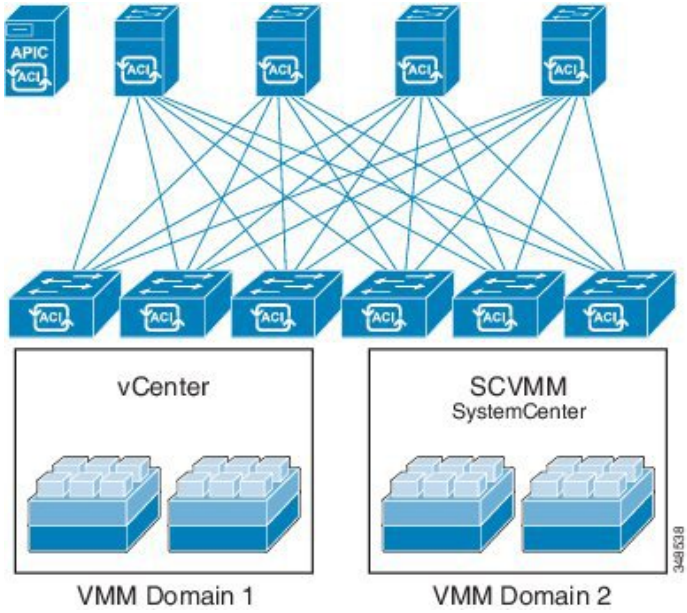
- **EPG の関連付け**：エンドポイント グループにより、エンドポイント間の接続と可視性が VMM ドメイン ポリシーの範囲内に規制されます。VMM ドメイン EPG は次のように動作します。
  - APIC は、これらの EPG をポート グループとして VM コントローラにプッシュします。
  - 1 つの EPG は、複数の VMM ドメインをカバーでき、1 つの VMM ドメインには複数の EPG を含めることができます。

- **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。

図 *1: ACI VMM* ドメイン *VM* コントローラの統合



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 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。

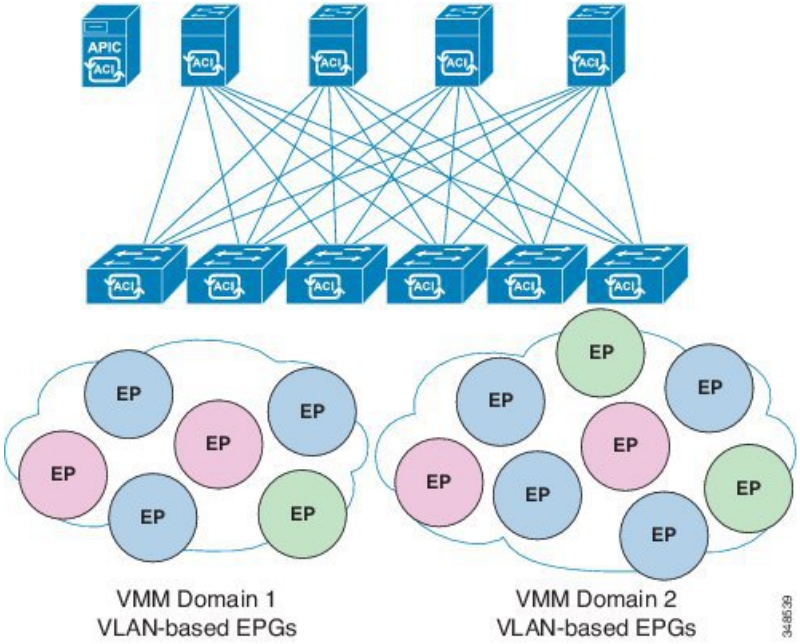
VMM ドメインは、1 つの動的 VLAN プールにのみ関連付けることができます。デフォルトでは、VMM ドメインに関連付けられた EPG への VLAN ID の割り当ては、APIC によって動的に行われます。動的割り当てがデフォルトであり、推奨設定ですが、管理者は代わりに EPG に静的に VLAN ID を割り当てることができます。この場合、使用する ID は VMM ドメインに関連付けられている VLAN プールのカプセル化ブロックから選択し、その割り当てタイプを静的に変更する必要があります。

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）。

VMM ドメイン EPG の関連付け

ACI ファブリックは、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、またはその設定を作成する APIC 管理者によって、VMM ドメインにテナント アプリケーション プロファイル EPG を関連付けます。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。

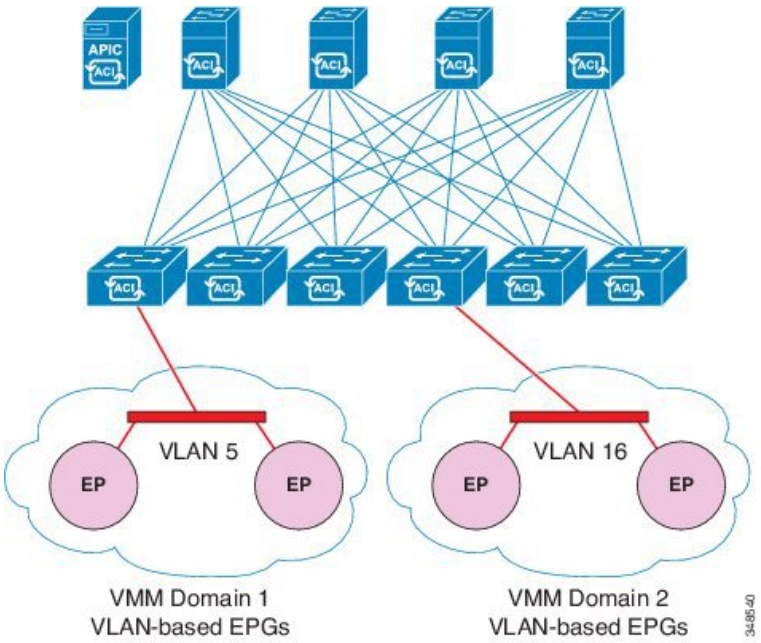
図 *2 : VMM* ドメイン *EPG* の関連付け



上の図では、同じ色のエンド ポイント（EP）は同じエンド ポイント グループに属しています。たとえば、緑色のすべての EP は 2 つの異なる VMM ドメインに含まれていますが同じ EPG に属しています。

仮想ネットワークと VMM ドメイン EPG 機能の情報については、Cisco ACI ドキュメントの最新の『Verified Scalability Guide』を参照してください。

図 *3 : 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ていない場合は、同じ VLAN プールを異なるドメイン間で使用できます。

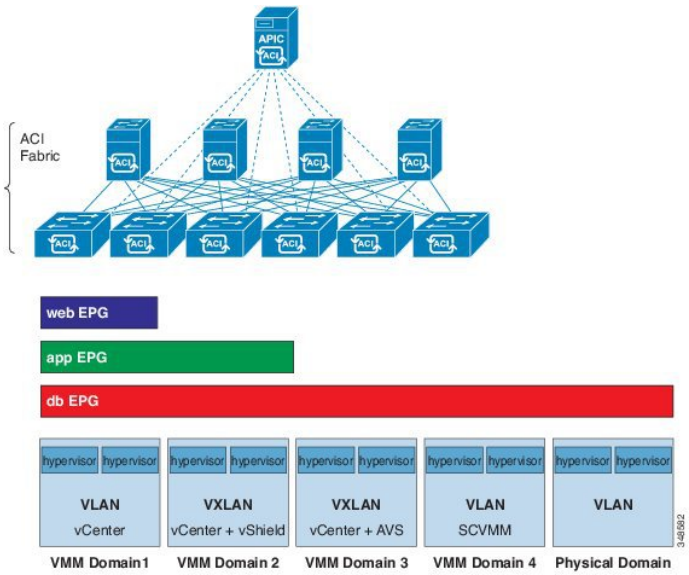
EPG は複数の VMM ドメインを次のように使用できます。

- VMM ドメイン内の EPG は、APIC によって自動的に管理されるか管理者によって固定で選択されたカプセル化識別子を使用して識別されます。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、APIC は動的に EPG の VLAN の割り当てを管理します。VMware DVS 管理者は、EPG に対して特定の VLAN を設定できます。その場合は、VLAN は VMM ドメインに関連付けられたプール内のスタティック割り当てブロックから選択します。

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 *4:* 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。

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EPGのトラフィックを集約します。現時点では、VMwareドメインのみでサポートされます。トランク ポート グループの名前付けスキームが EPG の T|A|E形式に従っていません。トランク ポート グループはテナントに対応しないため、名前には任意の ASCII 文字列を使用できます。

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、常に集約が再評価され、EGP を集約するかどうかが決まります。トランク ポート グループは、ベース EPG と uSeg EPG の両方を含む、集約される EPG に割り当てられた VLAN などのネットワーク リソースのリーフでの導入を制御しますuSeg EPG の場合、トランク ポート グループの VLAN の範囲には、プライマリ VLAN とセカンダリ VLAN の両方を含める必要があります。

（注） ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した multipod 接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています（結果として、最大パケット サイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます）。ただし、IOS XR などの他のプラットフォームは、パケット ヘッダーのを除く MTU 値を設定します（結果として最大パケット サイズは 8986 バイトになります）。

各プラットフォームの適切なMTU値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

注意 ファブリックのリーフ スイッチとスパイン スイッチの間に 1 ギガビット イーサネット (GE) または 10GE リンクを設置すると、帯域幅が不十分なために、パケットが転送されずにドロップされる可能性があります。これを避けるためには、リーフ スイッチとスパイン スイッチの間で 40GE または 100GE リンクを使用してください。

（注） ポート VLAN ごとの機能 (localPort 範囲に同じ VLAN ID を使用してリーフ スイッチで複数の EPG を設定する) で設定されたインターフェイスでは、マルチ スパニング ツリー (MST) はサポートされません。

（注） この Cisco APIC クラスタ/ファブリックで Cisco ACI マルチサイト を使用している場合、ナビゲーション バーのオブジェクト名のクラウド アイコンを検索します。これは、情報が マルチサイト から派生したことを示します。マルチサイト GUI からのみ変更を加えることをお勧めします。ここで変更を行い前に、マルチサイト ドキュメンテーションを確認してください。

（注） イベント レコードの Cisco APIC REST API クエリについて、APIC システムでは最大 500,000 イベント レコードへの応答に制限しています。応答が 500,000 イベント以上の場合は、エラーが返されます。クエリを絞り込むためにフィルタを使用します。詳細については、クエリー フィルタ式の作成を参照してください。

詳細については、次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

EPGがVMMドメインに関連付けられるたびに、管理者は解決と展開の優先順位を選択して、ポリシーをいつリーフ スイッチにプッシュするかを指定できます。

解決の緊急性

- [Pre-provision] — VM コントローラが仮想スイッチ（たとえば、VMware VDS など）に接続される前でもポリシー（たとえば、VLAN、VXLAN バインディング、コントラクト、

フィルタなど）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。

これは、ハイパーバイザ/VM コントローラの管理トラフィックも APIC VMM ドメイン (VMM スイッチ) に関連付けられている仮想スイッチを使用しているような状況で役に立ちます。

VLAN などの VMM ポリシーを ACI リーフ スイッチ上に展開するには、 APIC が、VM コントローラ経由のハイパーバイザと ACI リーフ スイッチの両方から、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 がそのハイパーバイザ、さらには APICと通信するのに同じ VMM ポリシー (VMM スイッチ) を使用することになっている場合には、ハイパーバイザの CDP/LLDP 情報を収集できません。VM コントローラ/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展開されていないからです。

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、ACI リーフ スイッチにダウンロードされます。これは、VMM スイッチに接続されたハイパーバイザ ホストがない場合もです。

- [Immediate]—ESXi ホストが DVS に接続すると、EPG ポリシー（コントラクトおよびフィルタを含む）が、関連付けられているリーフ スイッチ ソフトウェアにダウンロードされるよう指定します。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。

- [On Demand] — ESXi ホストがDVSに接続され、VM がポート グループ（EPG）に配置されている場合にのみ、ポリシー（たとえば、VLAN、VXLAN バインディング、コントラクト、フィルタ）がリーフ ノードにプッシュされるよう指定します。

  ホストが VMM スイッチに追加され、仮想マシンをポート グループ（EPG）に配置する必要がある場合、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。

  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。

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。

- [Immediate] — ポリシーがリーフ ソフトウェアでダウンロードされるとすぐにポリシーがハードウェアのポリシー CAM でプログラムされるよう指定します。

- [On Demand]—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 でプログラムされるよう指定します。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。

Cisco Application Virtual Switch でサポートされている NetFlow

Cisco Application Virtual Switch（AV）は、次の注意事項と NetFlow がサポートされています。

- 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 NetFlow を有効または無効にして、収集されるトラフィックの方向を指定できます。
- Cisco AV 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。

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 [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 [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 ドメイン関連付けの追加]** 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]** では **[有効]** を選択します。

b) （Cisco AVS のみ）**[NetFlow 方向]** を選択し、モニタおよび収集する必要があるフローの **[入力]**、**[出力]**、**[両方]** 選択します。

ステップ 6 [Submit] をクリックします。

NX OS スタイル CLI を使用した仮想マシン ネットワーキングの NetFlow エクスポータ ポリシーの設定

次の手順の例では、NX OS スタイル CLI を使用して、仮想マシン 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 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 エクスポータ ポリシーを設定します。

例：

```
apic1(config)# flow vm-exporter vmExporter1 destination address 2.2.2.2 transport udp
1234
apic1(config-flow-vm-exporter)# source address 4.4.4.4
apic1(config-flow-vm-exporter)# exit
apic1(config)# exit
```

VMware VDS の NX-OS スタイル CLI を使用して VMM ドメインで NetFlow エクスポータ ポリシーを利用する

次の手順では、VMM ドメインで NetFlow エクスポータ ポリシーを消費するために、NX OS スタイル CLI を使用します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 NetFlow エクスポータ ポリシーを消費します。

例：

```
apic1(config)# vmware-domain mininet
apic1(config-vmware)# configure-dvs
apic1(config-vmware-dvs)# flow exporter vmExporter1
apic1(config-vmware-dvs-flow-exporter)# active-flow-timeout 62
apic1(config-vmware-dvs-flow-exporter)# idle-flow-timeout 16
apic1(config-vmware-dvs-flow-exporter)# sampling-rate 1
apic1(config-vmware-dvs-flow-exporter)# exit
apic1(config-vmware-dvs)# exit
apic1(config-vmware)# exit
apic1(config)# exit
```

Cisco AVS の NX-OS スタイル CLI を使用して、VMM ドメイン下の NetFlow エクスポータ ポリシーを利用する

次の手順では、VMM ドメインで NetFlow エクスポータ ポリシーを消費するために、NX OS スタイル CLI を使用します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 NetFlow エクスポータ ポリシーを消費します。

例：

```
apic1(config)# vmware-domain mininet
apic1(config-vmware)# configure-avs
apic1(config-vmware-dvs)# flow exporter vmExporter1
apic1(config-vmware-dvs-flow-exporter)# active-flow-timeout 62
apic1(config-vmware-dvs-flow-exporter)# idle-flow-timeout 16
apic1(config-vmware-dvs-flow-exporter)# exit
apic1(config-vmware-dvs)# exit
apic1(config-vmware)# exit
apic1(config)# exit
```

VMware 用 NX OS スタイル CLI を使用したエンドポイント グループ上の NetFlow の有効化または無効化

次の手順では、NX OS スタイル CLI を使用してエンドポイント グループ上で NetFlow を有効または無効にします。

手順

ステップ 1 NetFlow の有効化：

例：

```
apic1# config
apic1(config)# tenant tn1
apic1(config-tenant)# application app1
apic1(config-tenant-app)# epg epg1
apic1(config-tenant-app-epg)# vmware-domain member mininet
apic1(config-tenant-app-epg-domain)# flow monitor enable
apic1(config-tenant-app-epg-domain)# exit
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
apic1(config)# exit
```

ステップ 2 （任意） NetFlow を使用しない場合は、この機能を無効にします。

例：

```
apic1(config-tenant-app-epg-domain)# no flow monitor enable
```

Cisco AVS の NX-OS スタイルの CLI を使用して、エンドポイント グループ上の NetFlow を有効または無効にする

NX-OS スタイルの CLI を使用して、エンドポイント グループでの NetFlow を有効または無効にするには、次の手順を実行します。

手順

ステップ 1 NetFlow の有効化：

例：

```
apic1# config
apic1(config)# tenant tn1
apic1(config-tenant)# application app1
apic1(config-tenant-app)# epg epg1
apic1(config-tenant-app-epg)# vmware-domain member mininet
apic1(config-tenant-app-epg-domain)# flow monitor enable
apic1(config-tenant-app-epg-domain)#flow direction {ingress | egress | both}
```

```
apic1(config-tenant-app-epg-domain)# exit
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
apic1(config)# exit
```

ステップ 2 （任意） NetFlow を使用しない場合は、この機能を無効にします。

例：

```
apic1(config-tenant-app-epg-domain)# no flow monitor enable
```

REST API 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

XML の次の例では、REST API を使用して VM ネットワー キングの NetFlow エクスポータ ポリシーを設定する方法を示します。

```
<polUni>
    <infraInfra>
        <netflowVmmExporterPol name="vmExporter1" dstAddr="2.2.2.2" dstPort="1234"
srcAddr="4.4.4.4"/>
    </infraInfra>
</polUni>
```

VMware VDS に REST API を使用して VMM ドメインで NetFlow エクスポータ ポリシーを使用する

次に示すのは、REST API を使用して VMM ドメインで NetFlow エクスポータ ポリシーを利用する方法を示す XML の例です:

```
<polUni>
    <vmmProvP vendor="VMware">
        <vmmDomP name="mininet">
            <vmmVSwitchPolicyCont>
                <vmmRsVswitchExporterPol tDn="uni/infra/vmmexporterpol-vmExporter1"
activeFlowTimeOut="62" idleFlowTimeOut="16" samplingRate="1"/>
            </vmmVSwitchPolicyCont>
        </vmmDomP>
    </vmmProvP>
</polUni>
```

Cisco AVS 用の REST API を使用して VMM ドメイン下で NetFlow エクスポータ ポリシーを使用する

手順

VMM ドメインで NetFlow エクスポータ ポリシーを消費するには、次の例のように POST メッセージを送信します。

例：

```
<polUni>
    <vmmProvP vendor="VMware">
        <vmmDomP name="mininet">
            <vmmVSwitchPolicyCont>
                <vmmRsVswitchExporterPol tDn="uni/infra/vmmexporterpol-vmExporter1"
activeFlowTimeOut="62" idleFlowTimeOut="16"/>
            </vmmVSwitchPolicyCont>
        </vmmDomP>
    </vmmProvP>
</polUni>
```

VMware VDS の VMM ドメイン アソシエーションのエンドポイント グループ上で NetFlow を有効にする

次の XML の例では、REST API を使用して、VMM ドメイン アソシエーションのためのエンドポイント グループ上で NetFlow を有効化する方法を示しています:

```
<polUni>
    <fvTenant name="t1">
        <fvAp name="a1">
            <fvAEPg name="EPG1">
                <fvRsDomAtt tDn="uni/vmmp-VMware/dom-mininet" netflowPref="enabled" />
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
```

Cisco AVS の VMM ドメイン アソシエーションのエンドポイント グループで NetFlow を有効にする

手順

次の例のような POST メッセージの送信によって、VMM ドメイン アソシエーションのために、エンドポイント グループの NetFlow を有効にします。

例：

（注） この例では、NetFlowの方向を「入力」にしています。また、「出力」または「両方」を選択できます。

```
<polUni>
    <fvTenant name="t1">
        <fvAp name="a1">
            <fvAEPg name="EPG1">
                <fvRsDomAtt tDn="uni/vmmp-VMware/dom-mininet" netflowPref="enabled"
netflowDir="ingress"/>
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
```

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。