Virtual Machine Manager のドメイン

この章の内容は、次のとおりです。

Virtual Machine Manager のドメイン

APIC は、アクセス ポリシーおよびレイヤ 4 ～ レイヤ 7 サービスを含むすべての仮想および物理ワークロードに対するネットワーキング全体を自動化する一括管理コントローラです。 VMware vCenter の場合、分散仮想スイッチ（VDS）およびポート グループのすべてのネットワーキング機能は APIC を使用して実行されます。 vCenter の管理者が vCenter で実行する必要がある唯一の機能は、vNIC を APIC により作成された適切なグループに配置することです。

VM コントローラ：VMware vCenter、VMware vShield、Microsoft System Center Virtual Machine Manager（SCVMM）などの外部仮想マシンの管理システムを表します。

Virtual Machine Manager（VMM）のドメイン：VM コントローラを同様のネットワーキング ポリシー要件でグループ化します。 たとえば、VM コントローラは、VLAN または Virtual Extensible Local Area Network（VXLAN）の領域およびアプリケーション 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。

（注） 単一の VMM ドメインには、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、同じベンダーから取得する必要があります（たとえば VMware や Microsoft から）。

VMM ドメインでの EPG のプロビジョニング：次のように VMM ドメインにアプリケーション プロファイル EPG を関連付けます。

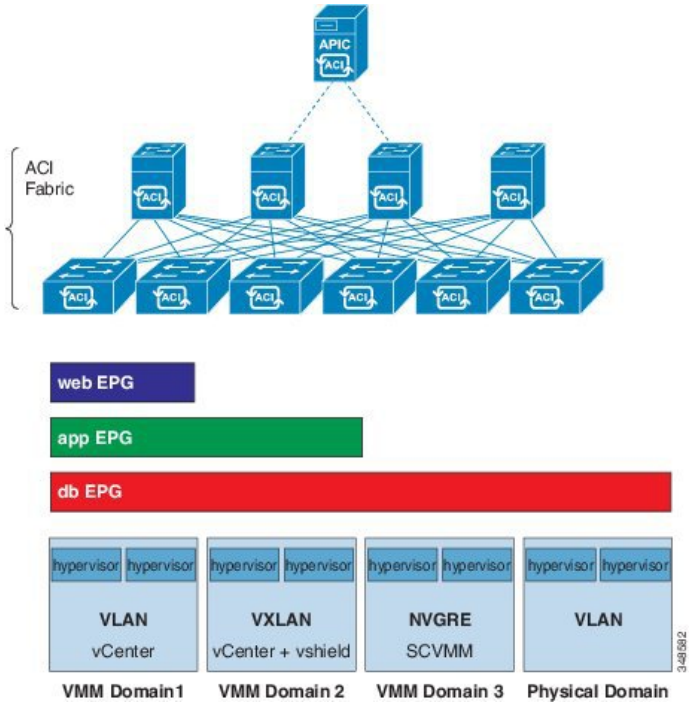
- APIC は、これらの EPG をポート グループとして VM コントローラにプッシュします。 次にコンピューティングの管理者がこれらのポート グループに vNIC を配置します。
- 1 つの EPG は、複数の VMM ドメインをカバーでき、1 つの VMM ドメインには複数の EPG を含めることができます。

ファブリックの EPG スケーラビリティ：EPG は複数の VMM ドメインを使用して次を行うことができます。

- VMM ドメイン内の EPG は、APIC によって自動的に管理されるカプセル化識別子を使用して識別されます。 たとえば、VLAN、仮想ネットワーク ID（VXLAN 用の VNID）、または仮想サブネット ID（NVGRE 用の VSID）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、VNID、VSID ID のカプセル化を使用できます。
- 入力リーフ スイッチは、パケットからファブリックのローカル VXLAN VNID（セグメント ID）へのカプセル化（VLAN/VNID/VSID）を正常化し変換します。これにより、EPG のカプセル化がリーフ スイッチにローカライズされます。
- 異なるリーフ スイッチ間でカプセル化 ID を再利用することができます。 たとえば、VLAN ベースのカプセル化では VMM ドメイン内の EPG の数が 4096 に制限されます。 複数の VMM ドメインを作成して EPG を増やし、複数の VMM ドメイン間で同じ EPG を関連付けることができます。

（注） 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。 次の図を参照してください。 同様に、同じリーフ スイッチ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。

図 *1*：ファブリック内の複数の *VMM* ドメインと *EPG* の増大



接続エンティティ 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 baremetal 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）、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、ポート チャネル、または仮想ポート チャネル（vPC）にすることができます。

接続可能エンティティ プロファイル（AEP）は、同様のインフラストラクチャ ポリシー要件を持つ外部エンティティのグループを表します。 インフラストラクチャ ポリシーは、物理インターフェイス ポリシーで構成され、たとえば Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、最大伝送単位（MTU）、Link Aggregation Control Protocol（LACP）などがあります。

VM 管理（VMM）ドメインは、AEP に関連付けられたインターフェイス 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 でオーバーライド 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、ハイパーバイザが中間レイヤ 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 スイッチおよびハイパーバイザ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、ハイパーバイザとレイヤ 2 スイッチ間の LACP をディセーブルにできます。

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。 異なるリーフ スイッチ間でカプセル化プール（たとえば VLAN）を再利用することができます。 AEP は、（VMM ドメインに関連付けられた）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。

（注）

- AEP は、リーフ上で VLAN プール（および関連 VLAN）をプロビジョニングします。 VLAN はポートでは実際にイネーブルになっていません。 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 を使用して VLAN プールを展開しないと、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 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。
- リーフ スイッチは、重複した VLAN プールをサポートしていません。 異なる重複した VLAN プールを同一の AEP に関連付けることはできません。

Pools

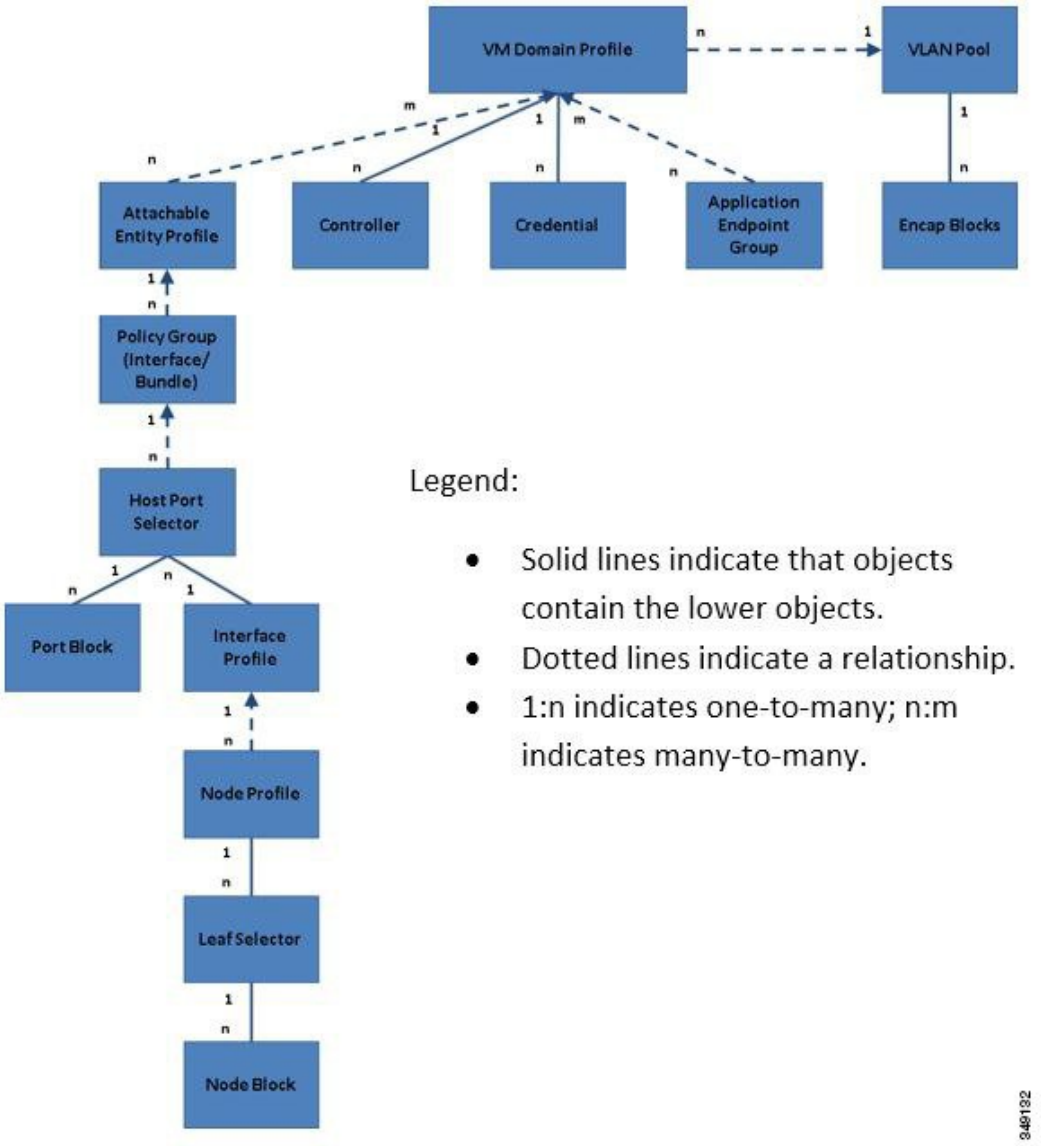
プールは、トラフィックのカプセル化 ID の範囲を表します（たとえば、VLAN ID、VNID、マルチキャスト アドレスなど）。 プールは共有リソースで、VMM などの複数のドメインおよびレイヤ 4 ～ レイヤ 7 のサービスで消費できます。 リーフ スイッチは、重複した VLAN プールをサポートしていません。 異なる重複した VLAN プールを同一の接続可能エンティティ プロファイル（AEP）と関連付けることはできません。 VLAN ベースのプールには、次の 2 種類があります。

- ダイナミック プール：APIC によって内部的に管理され、エンドポイント グループ（EPG）の VLAN を割り当てます。 vCenter ドメインはダイナミック プールのみに関連付けることができます。
- スタティック プール：1 つ以上の EPG がドメインに関連付けられ、そのドメインは VLAN のスタティック範囲に関連付けられます。 VLAN のその範囲内に静的に展開された EPG を設定する必要があります。

VMM ポリシー モデル

ACI ファブリック VM ネットワーキングにより、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することができます。 次の図は、VM ネットワーキング ポリシー モデルのオブジェクトと VM ドメイン プロファイル内の他のオブジェクトとの関連を示します。

図 *2* : ***VMM*** ポリシー モデル



VM ドメイン プロファイルには、次の MO が含まれます。

- **クレデンシャル**：ユーザを VM ドメインに関連付けます。

- **コントローラ**：含む側のポリシー適用ドメインの一部である VMM 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 VM ドメインの一部である VMware vCenter への接続を指定します。
- **アプリケーション EPG**：アプリケーション エンドポイント グループは、ポリシーの範囲内でエンドポイント間の接続性と可視性を調整するポリシーです。
- **接続可能エンティティ プロファイル**：リーフ ポートの大規模セットでハイパーバイザ ポリシーを展開するためのテンプレートを提供し、VM ドメインと物理ネットワーク インフラストラクチャの関連付けも提供します。 接続可能エンティティ プロファイルには次が含まれます。
  - 使用するインターフェイス ポリシーを指定するポリシー グループ。
  - 設定するポートとそれらのポートを設定する方法を指定するホスト ポート セレクタ。
  - インターフェイスの範囲を指定するポート ブロック。
  - インターフェイス設定を指定するインターフェイス プロファイル。
  - ノード設定を指定するノード プロファイル。
  - どのリーフ ノードを設定するかを指定するリーフ セレクタ。
  - ノードの範囲を指定するノード ブロック。
- **VLAN プール**：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アドレスを指定します。

vCenter ドメイン設定のワークフロー

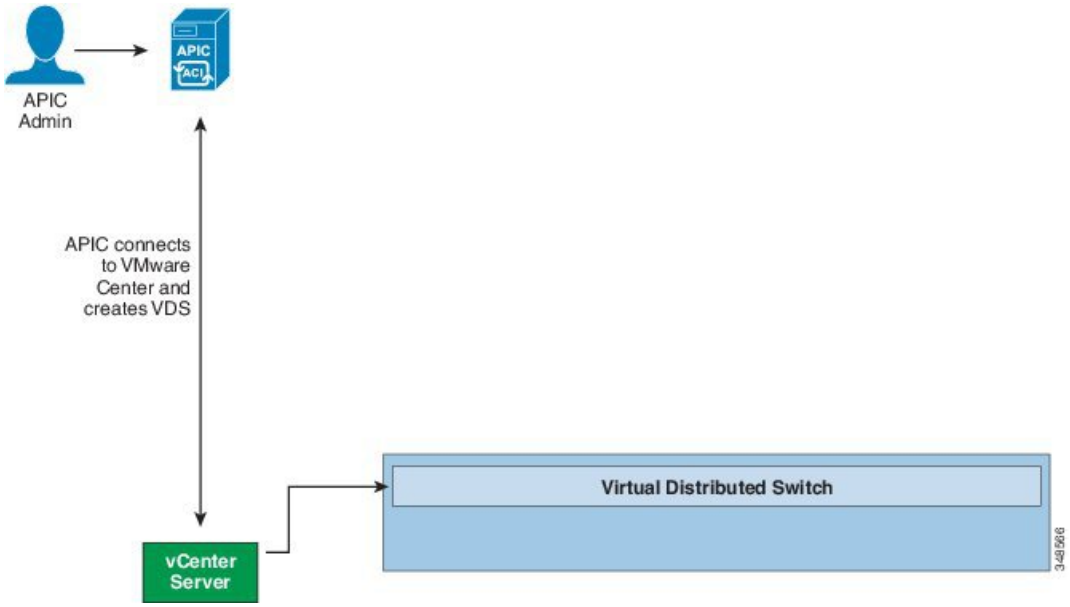
1. APIC 管理者は、vCenter ドメイン ポリシーを APIC で設定します。 次の図を参照してください。 APIC 管理者は、次の vCenter 接続情報を提供します。
   - vCenter IP アドレス、vCenter クレデンシャル、VMM ドメイン ポリシー、VMM ドメイン SPAN
   - ポリシー（VLAN プール、VMware VDS などのドメイン タイプ、Cisco Nexus 1000V スイッチ）
   - 物理リーフ インターフェイスへの接続性（接続エンティティ プロファイルを使用）

図 *3*： *APIC* 管理者による *vCenter* ドメイン ポリシーの設定

APIC は、vCenter に自動的に接続し、vCenter 下で VDS を作成します。 次の図を参照してください。

（注） VDS 名は、VMM ドメイン名とデータセンター名を連結したものです。

図 *4*： ***vCenter*** での ***VDS*** の作成



2 APIC 管理者は、アプリケーション EPG を作成し、VMM ドメインにそれを関連付けます。

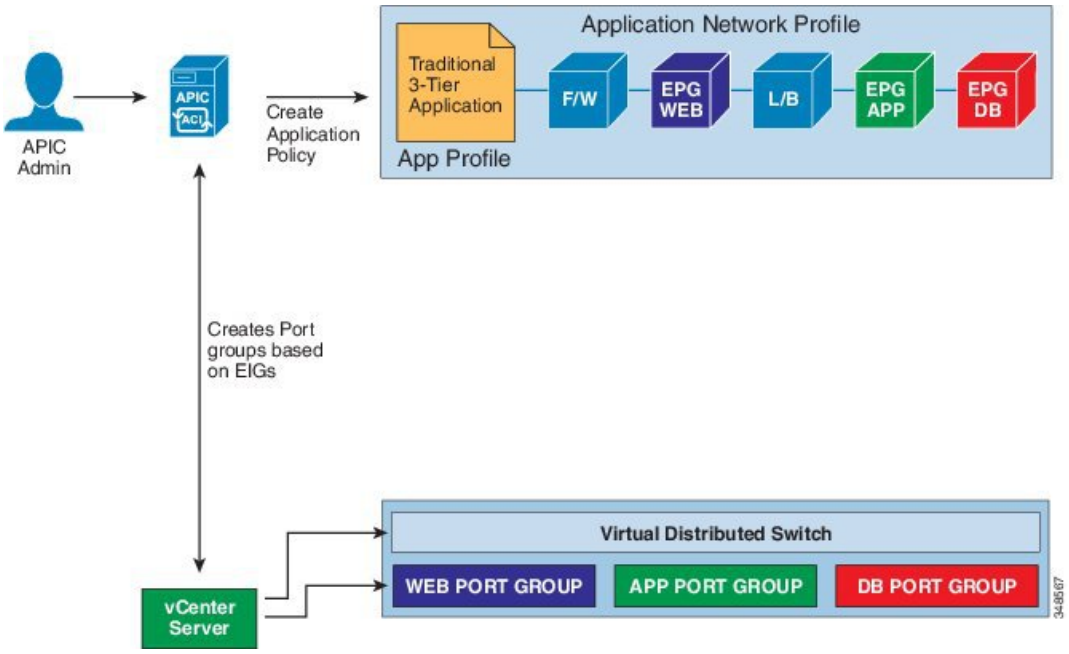
- APIC は、VDS 下の VMware vCenter でポート グループを自動的に作成します。
- このプロセスは VMware vCenter でネットワーク ポリシーをプロビジョニングします。

次の図を参照してください。

（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。

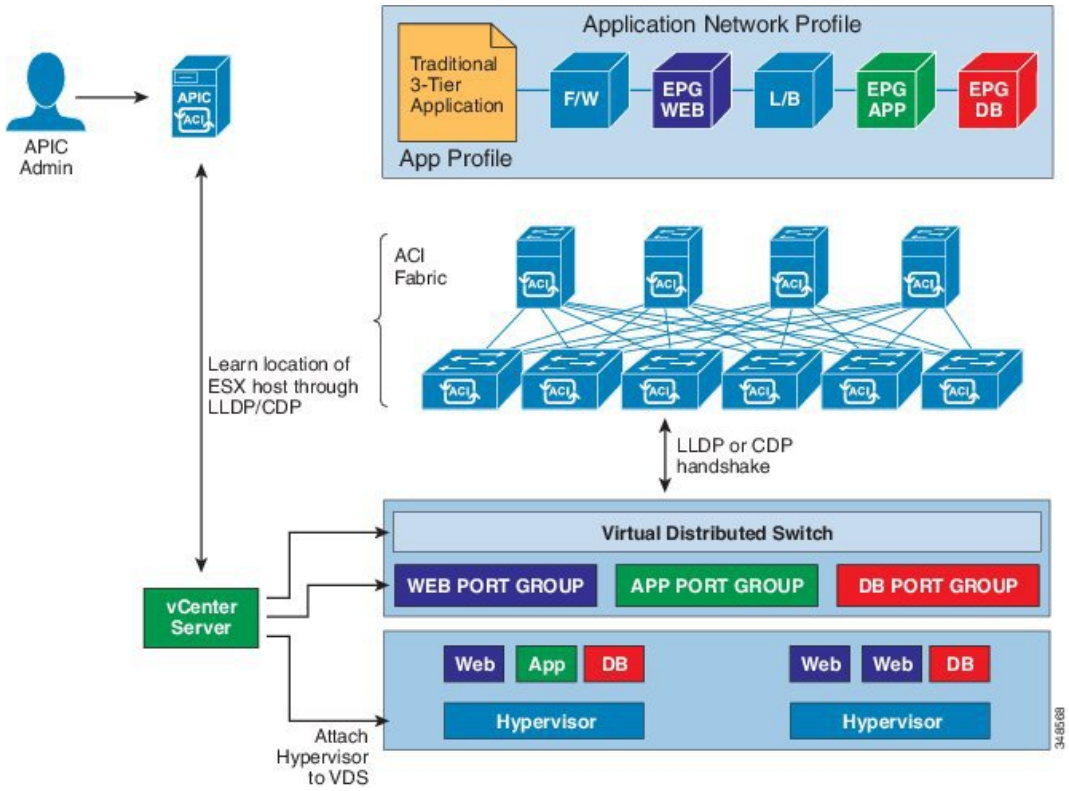
図 *5*：*VMM* ドメインへのアプリケーション *EPG* の関連付け



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。

- APIC は、次の図に示すように、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。

図 *6* : 管理ツールを使用した *VDS* へのハイパーバイザの接続

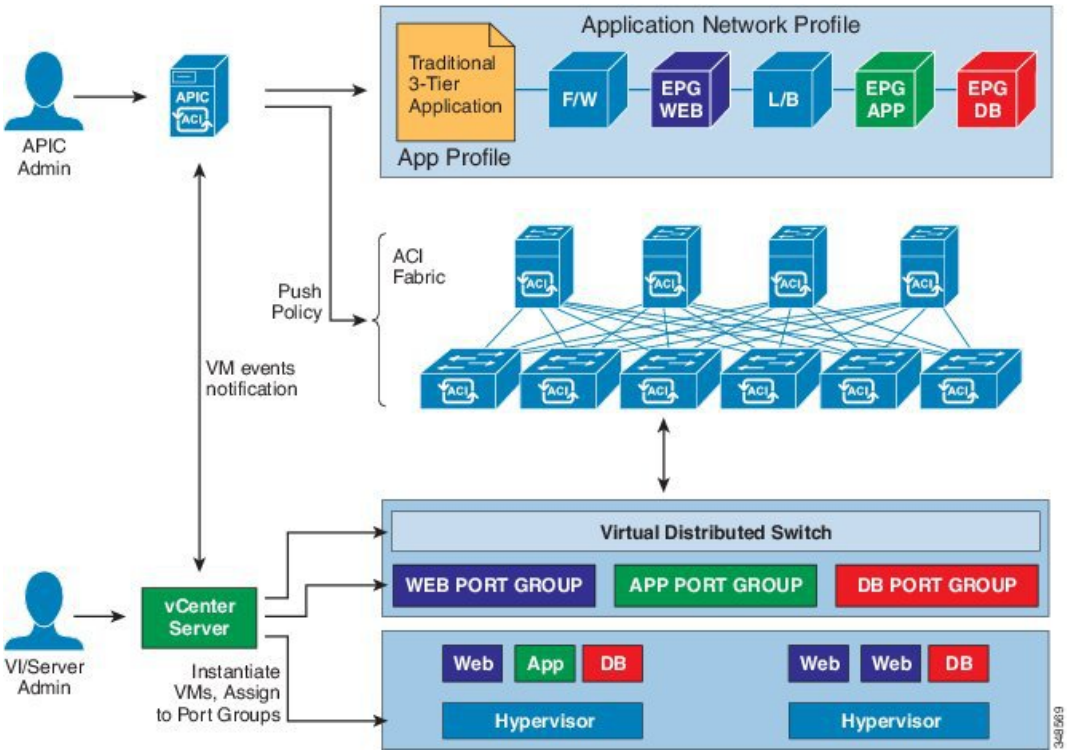


4 vCenter の管理者やコンピューティングの管理ツールは、VM をインスタンス化しポート グループに割り当てます。

- 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。 次の図を参照してください。

図 *7* : ***ACI*** ファブリックへのポリシーのプッシュ



vCenter および vShield ドメイン設定のワークフロー

このワークフローでは、VMware で提供されるハイパーバイザ VXLAN 機能を使用するために APIC がどのように vShield Manager と統合するかを示します。

（注） APIC は vShield Manager で VXLAN 全体の準備と導入を制御および自動化するので、ユーザは vShield Manager で操作を実行する必要がありません。

設定を開始する前に、次の前提条件を満たす必要があります。

- vCenter Server の IP アドレスは vShield Manager で設定する必要があります。
- **ファブリック インフラストラクチャ VLAN** はハイパーバイザ ポートに拡張する必要があります。 ファブリック インフラストラクチャ VLAN は、VXLAN データ パケットのイーサネット ヘッダーで外部 VLAN として使用されます。 VXLAN 用に APIC VDS を準備するときに、

APIC はファブリック インフラストラクチャ VLAN を vShield Manager に自動的にプッシュします。

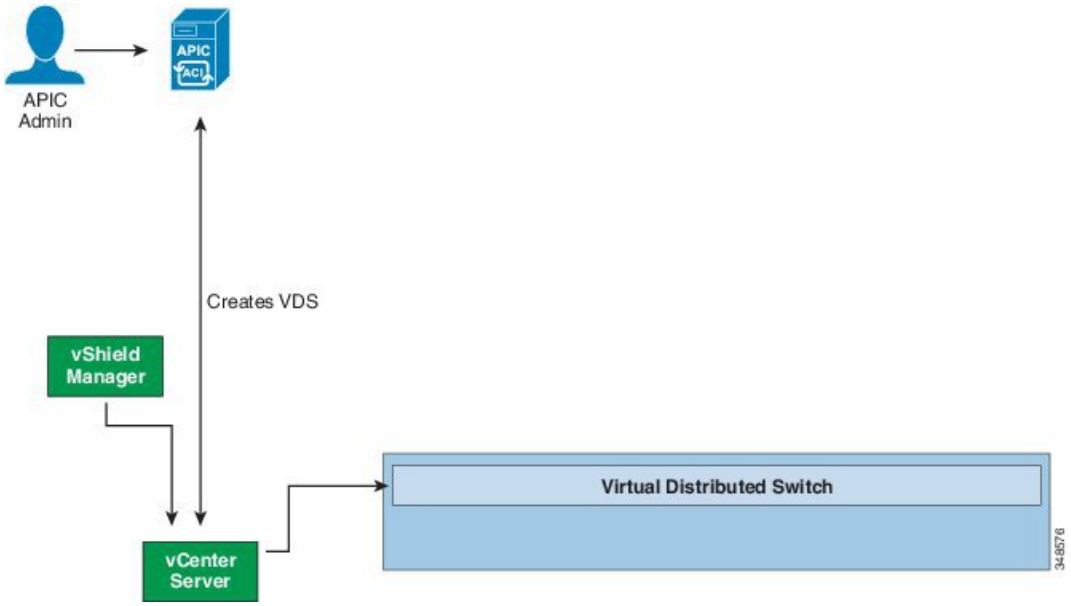
- データ パスが機能するようにするには、ファブリック インフラストラクチャ VLAN をハイパーバイザ ポートに拡張する必要があります。
  - リーフ スイッチのテナント向きのポートでは、インフラストラクチャ VLAN は APIC で接続エンティティ プロファイルを作成することでプロビジョニングできます。（接続エンティティ プロファイルの作成については、『*APIC Getting Started Guide*』を参照してください）
  - 中間レイヤ2スイッチがハイパーバイザとリーフスイッチの間にある場合、ネットワーク管理者は中間レイヤ 2 ノードでインフラストラクチャ VLAN を手動でプロビジョニングする必要があります。

1 APIC 管理者は、vCenter および vShield のドメイン ポリシーを APIC で設定します。

（注）
- APIC 管理者は、APIC で vShield Manager と vCenter Server 間のアソシエーションを提供する必要があります。
- APIC 管理者は、セグメント ID および VXLAN に必要なマルチキャスト アドレス プールを提供する必要があります。 vShield Manager のセグメント ID プールは、APIC で設定された他の vShield Manager のプールと重複してはなりません。

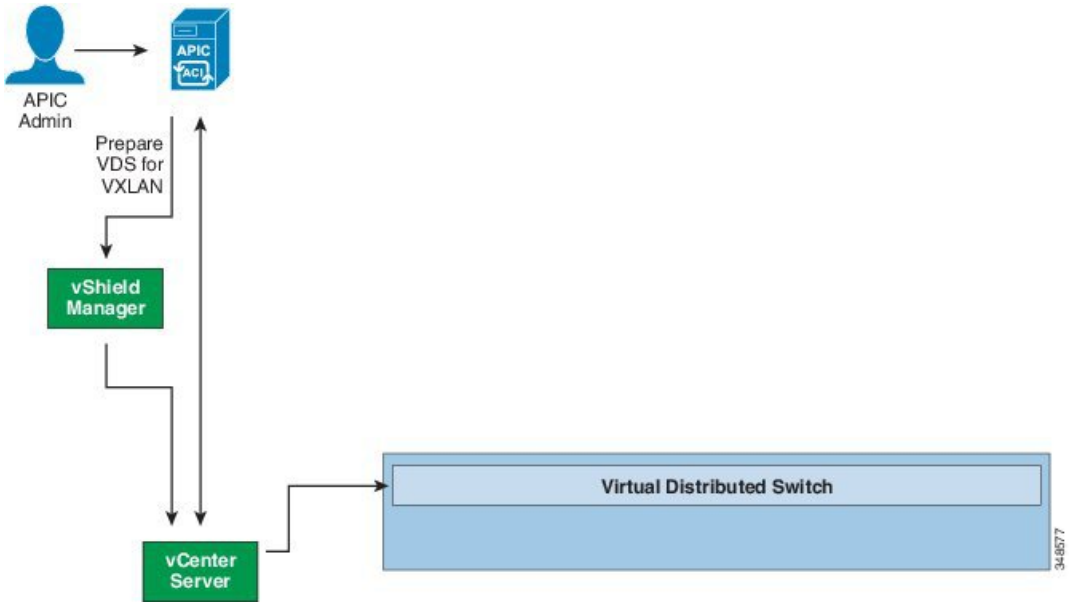
a APIC は、vCenter に接続し、VDS を作成します。 次の図を参照してください。

図 *8*： *vCenter* への接続と *VDS* の作成



b APIC は、vShield Manager に接続し、セグメント ID とマルチキャスト アドレス プールをプッシュし、VXLAN 用の VDS を準備します。 次の図を参照してください。

図 *9* : ***vShield Manager*** への接続と ***VXLAN*** 用の ***VDS*** の準備

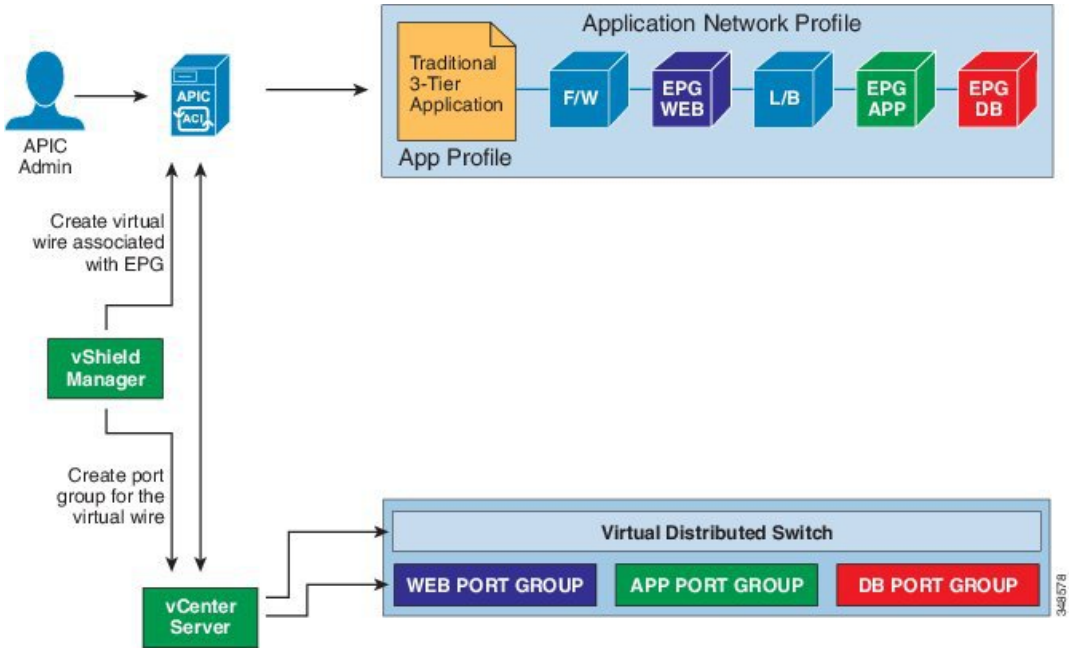


2 APIC 管理者は、アプリケーション プロファイルと EPG を作成し、それらを VMM ドメインに関連付けます。 次の図を参照してください。

- APIC は、VDS 下の vShield Manager で仮想ワイヤを自動的に作成します。
- APIC は、vShield Manager から送信される VXLAN 仮想ワイヤからセグメント ID とマルチキャスト アドレスを読み込みます。
- vShield Manager は、VDS 下で vCenter Server のポート グループとして仮想ワイヤをプッシュします。

（注） 仮想ワイヤ名は、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。

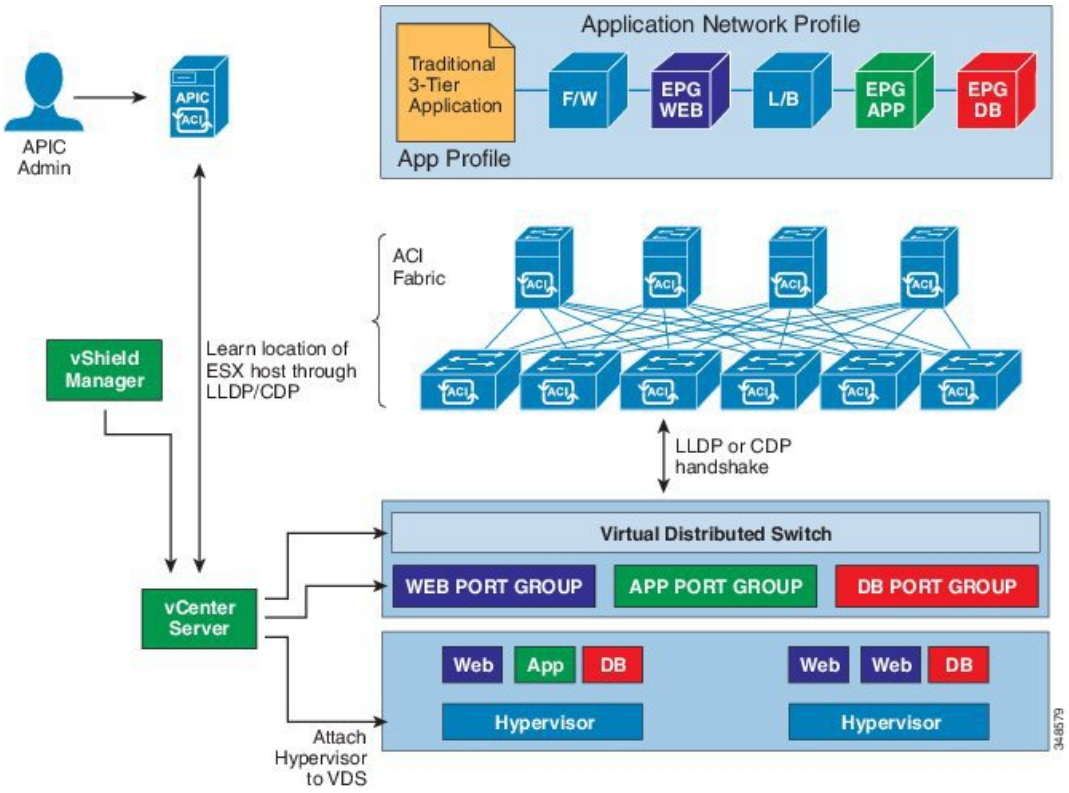
図 *10*：アプリケーション プロファイルと *EPG* の作成



3 vCenter の管理者やコンピューティングの管理ツールは、VDS にハイパーバイザを接続します。次の図を参照してください。

- APIC は、ハイパーバイザからの 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。

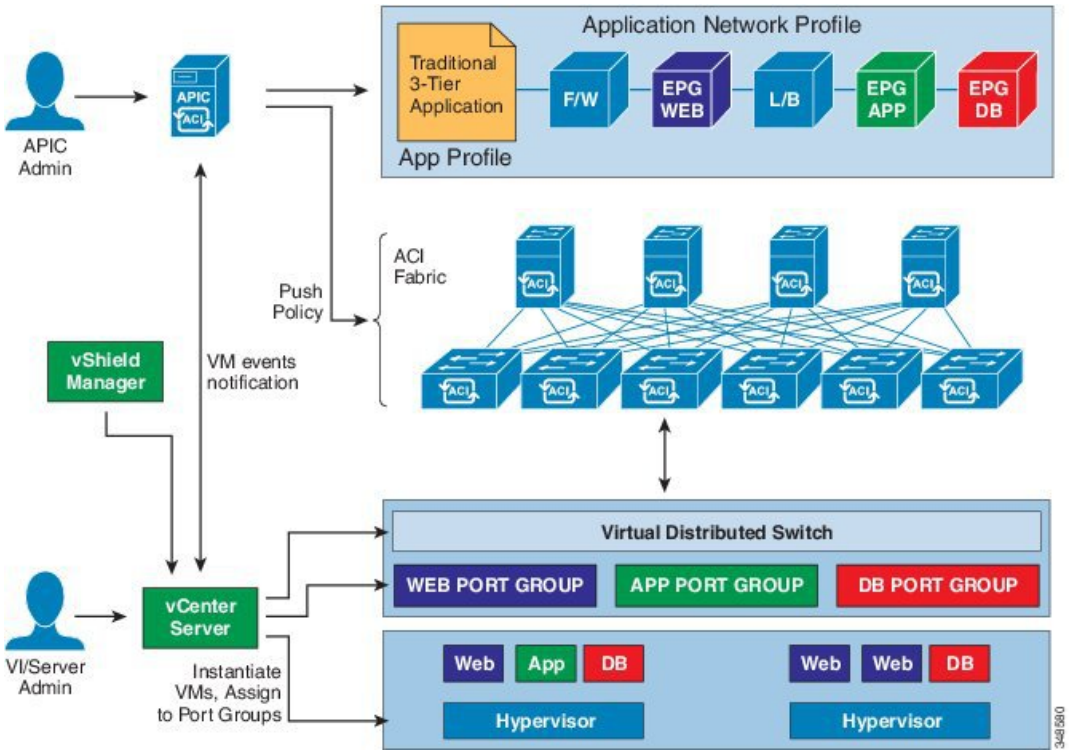
図 *11* : ***VDS*** へのハイパーバイザの接続



4 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。

APIC は、ACI ファブリックにポリシーを自動的にプッシュします。 次の図を参照してください。

図 *12* : *ACI* ファブリックへのポリシーのプッシュ



アプリケーション EPG のポリシー解決の作成と展開の緊急性

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、ポリシーをいつプッシュするかを指定できます。

解決の緊急性

- [Immediate]：ハイパーバイザが VDS 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。 LLDP または OpFlex 権限は、ハイパーバイザ/リーフ ノード接続を解決するために使用されます。
- [On Demand]：pNIC がハイパーバイザ コネクタに接続し、VM がポート グループ（EPG）に配置される場合にのみ、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。

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、ポリシーがハードウェアのポリシー CAM にプッシュされるときに、インストルメンテーションの緊急性が指定できます。

- [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。