ファブリック接続

ファブリック ポリシーの概要

これまでに、ACMEにACIファブリックをプロビジョニングし、リーフとスパインスイッチ、アクセス権限、および基本的な管理ポリシー間にインフラストラクチャ領域を設定しました。次に、ACIファブリック内で接続ポリシーの作成を開始します。APIC GUIの[Fabric]タブを使用して、デバイスディスカバリとインベントリ管理、診断ツール、ドメインの設定、スイッチとポートの動作など、システムレベルの機能を設定します。[Fabric]ペインは3つのセクション（[inventory]、[fabric policies]、[access policies]）に分かれています。ファブリック ポリシーとアクセス ポリシーによってファブリックを設定する方法を理解することは、ACMEのネットワーク チームにとって重要です。このチームは、ファブリックのリーフ ノード間の内部接続や、サーバ、ネットワーク機器、ストレージアレイなどの外部エンティティへの接続のために、これらのポリシーを保持する必要があるからです。サーバ チームなどの他のチームも、ネットワーク チームと協力して作業する上で（特に、キャパシティを追加するビルド プロセスにおいて）、これらの概念を理解する必要があります。

この章では、[Fabric]タブの[access policies]サブセクションの主要オブジェクト（その多くが再利用可能）をレビューし、スイッチの追加および事前プロビジョニング方法について説明します。また、ACIファブリックを効果的に運用するために新しいデバイスをファブリックに追加する場合に必要な、手順とオブジェクトについても概説します。多くのポリシーは再利用可能ですが、ACIファブリックでのポリシーの削除による影響を理解することも重要です。

[access policies]サブセクションは複数のフォルダに分割されており、ファブリックの動作に影響するさまざまなタイプのポリシーとオブジェクトが分類されています。たとえば、インターフェイス ポリシーのフォルダにはポートの動作が設定されています（ポートの速度、リーフ

スイッチ インターフェイスで LACP などのプロトコルを実行するかどうかなど）。[access policies] ビューではドメインと AEP も作成されます。また、ファブリックにおけるリーフ スイッチのアクセス ポートの基本設定は、ファブリック アクセス ポリシーによって行われます。

[Fabric] - [Access Policies]

ドメイン

ACI では、エンドポイント グループは 「who」、コントラクトは「what/when/why」に該当します。また、AEPは「where」、ドメインはファブリックの「how」と見なすことができます。デバイスがリーフ スイッチに接続している方法に応じて、さまざまなドメイン タイプが作成されます。4 つのドメイン タイプ（物理ドメイン、外部ブリッジ ドメイン、外部ルーテッド ドメイン、VMMドメイン）があります。

- 物理ドメインは、通常、ベアメタルサーバ、またはハイパーバイザの統合がオプションでないサーバに対して使用されます。
- 外部ブリッジ ドメインはレイヤ 2 接続に使用されます。たとえば、外部ブリッジ ドメインを使用して、トランクアップされている既存のスイッチをリーフ スイッチに接続できます。
- 外部ルーテッド ドメインはレイヤ 3 接続に使用されます。たとえば、外部ルーテッド ドメインを使用して、WAN ルータをリーフ スイッチに接続することができます。
- ドメインは、[Fabric] タブで行われたポリシー モデルの設定と [Tenant] ペインにあるエンドポイント グループの設定を結びつける役割を果たします。ドメインはファブリック オペレータによって作成され、テナント管理者によってエンドポイント グループに関連付けられます。

理想的には、ポリシーを 1 回だけ作成して、ファブリックに新しいデバイスを接続するときにそれを再利用します。ポリシーとオブジェクトを最大限に再利用すると、日常業務が飛躍的に速くなり、大規模な変更が容易になります。これらのポリシーの使用状況は、 Application Policy Infrastructure Controller (APIC) GUI で **[Show Usage]** ボタンをクリックして表示できます。これを使用して、特定のポリシーをどのオブジェクトが使用しているかを判別することで、変更を行った場合の影響を把握することができます。

ドメインの詳細については、https://www.youtube.com/watch?v=_iQvoC9zQ_A にあるビデオ「How Devices Connect to the Fabric: Understanding Cisco ACI Domains」をご覧ください。

VLAN プール

VLAN プールにはドメインが関連付けられる EPG によって使用される VLAN が含まれています。ドメインは 1 つの VLAN プールに関連付けられます。VXLAN やマルチキャスト アドレス プールも設定できます。VLAN は、AEP の設定に基づいてリーフ スイッチでインスタンス化されます。許可/拒否の決定は、サブネットや VLAN ではなく、コントラクトとポリシー モデルに基づきます。

接続可能アクセス エンティティ プロファイル

接続可能アクセス エンティティ プロファイル（AEP）は、ファブリック設定の「where」に該当し、類似の要件を持つドメインのグループ化に使用されます。AEP はインターフェイス ポリシー グループに関連付けられます。1 つ以上のドメインを AEP に追加できます。ドメインを AEP にグループ化して関連付けることによって、ファブリックはドメイン内のさまざまなデバイスの場所を把握し、Application Policy Infrastructure Controller (APIC) は必要とする場所に VLAN やポリシーをプッシュできます。AEP は [Global Policies] セクションで設定されます。

ポリシー タイプ

大部分のポリシー フォルダにはサブフォルダがあります。たとえば、[interface policies] フォルダには、[policies]、[policy groups]、[profiles] という設定用のフォルダがあります。

スイッチ ポリシー

また、スイッチ用のポリシーもあります。たとえば、Application Policy Infrastructure Controller (APIC) GUI および vPC ポリシーで明示的 vPC 保護グループと呼ばれる、vPC ドメインを設定したりします。理想的には、ポリシーを 1 回だけ作成して、ファブリックに新しいデバイスを接続するときにそれを再利用します。ポリシーとオブジェクトを最大限に再利用すると、日常業務が飛躍的に速くなり、大規模な変更が容易になります。

スイッチ ポリシー グループ

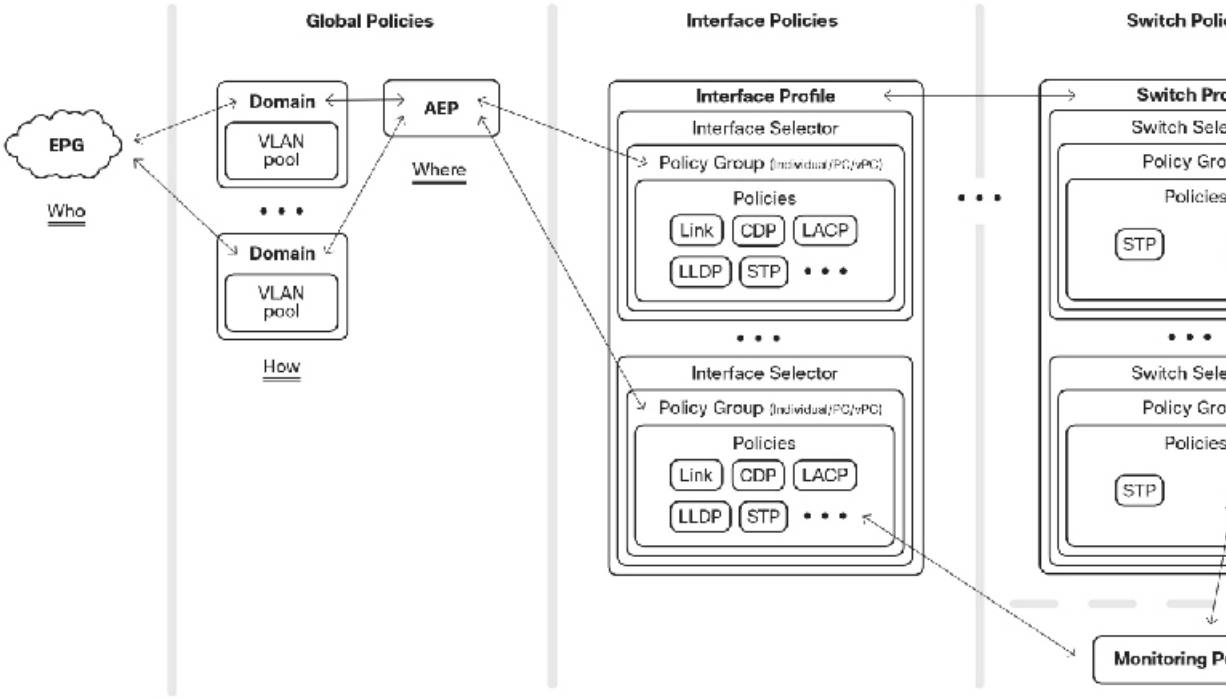
スイッチ ポリシー グループを使用すると、スパニングツリー ポリシーやモニタリング ポリシーなど、既存のスイッチ ポリシーを活用できます。

スイッチ プロファイル

スイッチプロファイルを使用すると、1 つ以上のリーフ スイッチを選択してインターフェイス プロファイルを関連付け、特定のノードにポートを設定できます。この関連付けによって、インターフェイスに設定がプッシュされ、インターフェイス ポリシーで設定されている場合は、ポート チャネルまたは vPC が作成されます。

次の図は、さまざまなグローバル ポリシー、スイッチ ポリシー、インターフェイス ポリシー間の関係を示しています。

図 *1: EPG* に物理インターフェイスまたはインターフェイスを接続できる関係



インターフェイス ポリシー

インターフェイス ポリシーはインターフェイスの動作を指示し、その後、インターフェイス ポリシー グループに関連付けられます。たとえば、CDP の無効化を指示するポリシーと CDP の有効化を指示するポリシーがある場合、リーフ スイッチに新しいデバイスが接続されたときにこれらを再利用できます。

インターフェイス ポリシー グループ

インターフェイス ポリシー グループはポートの動作を指示するテンプレートであり、AEP に関連付けられます。インターフェイス ポリシー グループは、前の段落で説明したポリシーを使用して、リンクの動作方法を指定します。また、同じポート設定が必要な多数のデバイスがポートに接続していることがよくあるので、再利用可能なオブジェクトもあります。リンクのタイプに応じて、3 つのインターフェイス ポリシー グループ（アクセス ポート、ポート チャネル、vPC）があります。

リーフ スイッチのポートはデフォルトで 10 GE に設定されるので、その速度で接続するデバイスに対しては 1 GE リンク レベルのポリシーを作成する必要があります。ポート チャネルと vPC については、ポリシー グループごとにスイッチ上の単一の論理インターフェイスが指定されます。10 個の PC/vPC を作成する場合、10 のポリシー グループを作成する必要があります。アクセス ポートのポリシー グループはインターフェイス間で再利用することができます。ポリシー グループは、プロトコルやポート動作を実装する where（対象）を実際には指定しませ

ん。以降で説明するように、「where（対象）」は、スイッチ プロファイルに 1 つ以上のインターフェイス プロファイルを関連付けることによって生じます。

インターフェイス プロファイル

インターフェイスプロファイルは部分を結合するのに役立ちます。インターフェイスプロファイルはポートインターフェイス セレクタのブロックを含んでおり、前述のように、インターフェイス ポリシー グループに関連付けられます。また、これは単なる任意ポート（e1/1 など）なので、ポートを設定するには、プロファイルを特定のスイッチプロファイルに関連付ける必要があります。

レイヤ 2 インターフェイス ポリシー

Cisco APIC リリース 1.1 では設定可能なインターフェイス ポリシーが追加され、ポート単位の VLAN シグニフィカンスが可能になりました。

Cisco Application Centric Infrastructure (Cisco ACI) ファブリックにデバイスを接続するために、タグなしトラフィック、802.1Q タグ付きトラフィック、または VXLAN カプセル化を使用できます。ポート単位の VLAN を使用すると、トラフィックが別のポートに着信される場合、同じ VLAN を異なるエンドポイント グループに使用できます。リリース 1.1 より前は、VLAN はリーフ スイッチごとに 1 つのエンドポイント グループのみを関連付けることができました。

従来のネットワークでは、ネットワーク デバイス内の VLAN 数が 4096 までに限定されているため、VLAN カプセル化に関する制限の 1 つとして、拡張性と再利用可能性が制限されています。

Cisco ACI のデフォルト設定（グローバル）では、EPG が個別のスイッチにバインドされ、異なる VLAN プールにバインドされている異なる物理ドメインを使用している限り、同じ VLAN カプセル化で EPG を使用できます。これによって、テナント間の通信を許可しなくても、テナントはファブリックを介して VLAN カプセル化 ID を再使用できます。ただし、グローバル設定では、テナントがリーフ スイッチを共有しておらず、したがって、同じリーフ スイッチ内に重複する VLAN がないと想定しています。

ポート単位の VLAN に関する制限事項と考慮事項

- ポート単位の VLAN を使用する場合は、VLAN カプセル化 ID の代わりに、ポートと VLAN のペア（P、V）が内部に登録されます。これによって、スイッチ レベルごとのハードウェア リソース消費量が増加します。
- 1 つのブリッジ ドメインに属している 2 つの EPG は、リーフ スイッチで同じカプセル化 ID を共有できません。
- グローバルとローカル間のレイヤ 2 インターフェイス ポリシーが変更されると、ポートがフラップすることが想定されます。つまり、トラフィックに影響します。

DWDM-SFP10G-C 光インターフェイス ポリシー

Cisco APIC リリース 3.1 (1) は DWDM-SFP10G-C 光ファイバのサポートを追加し、光ファイバのインターフェイス ポリシーを含みます。DWDM-SFP10G-C ポートが挿入されるとき、デフォルトでポートにはチャンネル番号 32 があります。DWDM-SFP10G-C 光インターフェイス ポリ

シーでは、1～96の番号にチャネル番号を変更でき、それで光ファイバを対応する波長に調整します。

表 *1:* チャネルごとの *DWDM-SFP10G-C* ポート波長

チャネル番号	周波数（THz）	波長（nm）
1	191.35	1566.72
2	191.40	1566.31
3	191.45	1565.90
4	191.50	1565.50
5	191.55	1565.09
6	191.60	1564.68
7	191.65	1564.27
8	191.70	1563.86
9	191.75	1563.45
10	191.80	1563.05
11	191.85	1562.64
12	191.90	1562.23
13	191.95	1561.83
14	192.00	1561.42
15	192.05	1561.01
16	192.10	1560.61
17	192.15	1560.20
18	192.20	1559.79
19	192.25	1559.39
20	192.30	1558.98
21	192.35	1558.58
22	192.40	1558.17
23	192.45	1557.77
24	192.50	1557.36
25	192.55	1556.96
26	192.60	1556.55
27	192.65	1556.15
28	192.70	1555.75
29	192.75	1555.34

チャネル番号	周波数（THz）	波長（nm）
30	192.80	1554.94
31	192.85	1554.54
32	192.90	1554.13
33	192.95	1553.73
34	193.00	1553.33
35	193.05	1552.93
36	193.10	1552.52
37	193.15	1552.12
38	193.20	1551.72
39	193.25	1551.32
40	193.30	1550.92
41	193.35	1550.52
42	193.40	1550.12
43	193.45	1549.72
44	193.50	1549.32
45	193.55	1548.91
46	193.60	1548.51
47	193.65	1548.11
48	193.70	1547.72
49	193.75	1547.32
50	193.80	1546.92
51	193.85	1546.52
52	193.90	1546.12
53	193.95	1545.72
54	194.00	1545.32
55	194.05	1544.92
56	194.10	1544.53
57	194.15	1544.13
58	194.20	1543.73
59	194.25	1543.33
60	194.30	1542.94
61	194.35	1542.54

チャネル番号	周波数（THz）	波長（nm）
62	194.40	1542.14
63	194.45	1541.75
64	194.50	1541.35
65	194.55	1540.95
66	194.60	1540.56
67	194.65	1540.16
68	194.70	1539.77
69	194.75	1539.37
70	194.80	1538.98
71	194.85	1538.58
72	194.90	1538.19
73	194.95	1537.79
74	195.00	1537.40
75	195.05	1537.00
76	195.10	1536.61
77	195.15	1536.22
78	195.20	1535.82
79	195.25	1535.43
80	195.30	1535.04
81	195.35	1534.64
82	195.40	1534.25
83	195.45	1533.86
84	195.50	1533.47
85	195.55	1533.07
86	195.60	1532.68
87	195.65	1532.29
88	195.70	1531.90
89	195.75	1531.51
90	195.80	1531.12
91	195.85	1530.72
92	195.90	1530.33
93	195.95	1529.94

チャネル番号	周波数（THz）	波長（nm）
94	196.00	1529.55
95	196.05	1529.16
96	196.10	1528.77

ベスト プラクティス

シスコは、ファブリック設定のベストプラクティスを策定しました。これらは必須条件ではなく、すべての環境やアプリケーションに適しているわけでもありませんが、Cisco Application Centric Infrastructure (ACI) ファブリックの日常の運用を簡素化する上で役立ちます。

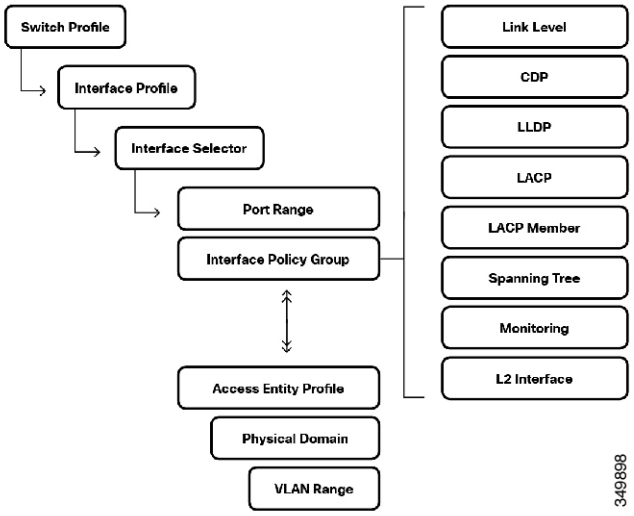
- ポリシー
  - 可能な限りポリシーを再利用します。たとえば、LACPの場合は、アクティブ/パッシブ/オフ、ポート速度 1GE、ポート速度 10GE を指定するポリシーがあります。
  - ポリシーに名前を付ける場合は、設定が伝わりやすい名前を使用します。たとえば、アクティブ モードで LACP を有効にするポリシーに、「LACP-Active」という名前を付けたりします。「デフォルト」と名付けられたポリシーが多数あります。しかし、すべてのデフォルトを覚えておくのは大変です。ですから、新しいデバイスをファブリックに追加する際にミスを防ぐためにも、わかりやすい名前を指定する必要があります。
  - 各リーフ スイッチごとにスイッチ プロファイルを個別に作成し、さらに、（vPC を使用している場合は）各 vPC ペアごとにスイッチ プロファイルを作成します。
- ドメイン
  - 同様の処理が必要なハイパーバイザを統合せずに、ベア メタル サーバまたはサーバ用に、テナントごとに 1 つの物理ドメインを構築します。
  - 外部接続用にテナントごとに 1 つの物理ドメインを構築します。
  - 複数のテナント間で VMM ドメインを活用する必要がある場合は、1 つの VMM ドメインを作成して、VMware ESXi サーバが接続しているすべてのリーフ ポートに関連付けることができます。
- AEP
  - 簡素化するために、複数のドメインを 1 つの AEP に関連付けることができます。場合によっては、重複 VLAN プールなどのインフラストラクチャ VLAN を有効にしたり、ファブリック全体での VLAN の範囲を制限するために、複数の AEP の設定が必要なこともあります。

ファブリックへの新しいデバイスの追加

ここでは、日常のファブリック運用を簡素化し、ファブリック アクセス ポリシーを再利用するためのACIの設定方法を示します。また、ファブリック全体でプロファイルを再利用する方法に焦点を当て、プロファイルの設定について最初から説明します。前の項で概説したよう

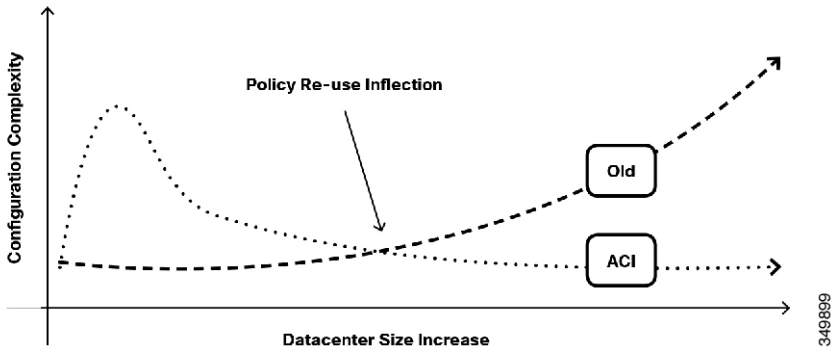
に、これらのさまざまなプロファイルは互いにリンクして依存関係を築いています。次の図は、オブジェクトの関係を示しています。

図 *2:* オブジェクトの関係



スイッチの従来のコマンドラインインターフェイスは、一般的にポート単位の設定を必要としますが、ACIでは再利用可能なポリシーとオブジェクトを定義することができます。ポリシーの再利用によって、スイッチの設定を非常に簡単に複製することができます。次の図は、この再利用によってファブリックの運用が簡素化される仕組みを時系列で示しています。

図 *3:* ポリシーの再利用



どのデータセンターでも、少数のスイッチを設定する場合には多数のプロセスや自動化は必要ありません。自動化は事業運営コストに直接影響するため、データセンターの規模の拡大に伴い、自動化はますます重要になります。従来のネットワークでは、多数のデバイスに影響を及ぼす変更を行う必要が生じた場合、オペレータはそれらのデバイスを管理するプロセスの設計コストに直面します。それらはネットワーク管理ツール、スクリプト、または専用アプリケーションかもしれません。Cisco ACI ポリシー モデルを活用すると、オペレータはプロファイル

を使用して、デバイスの追加や管理に関する操作を合理化できます。このことは、上記の図でポリシー再利用の変曲点として示されています。

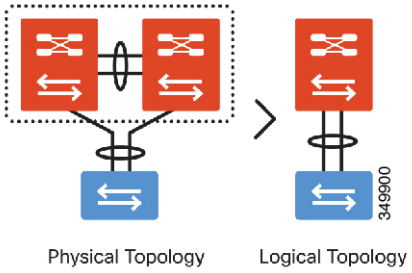
設定例

以降の項では、接続デバイス、ポートチャネル接続デバイス、vPC接続デバイスの個々の設定例を、設定されたオブジェクトのレビューも含めて、検討していきます。これらは、新しいデバイスがリーフ スイッチに接続されたときに、リーフ スイッチのアクセス ポートのスイッチポート設定が適切であることを確認するために、APIC GUI で実行されるステップであり、また、設定の正しさを確認するための検証ステップでもあります。次のステップは、リーフ スイッチに接続された新しいベアメタル サーバを追加する場合の使用例です。

一般的なサーバ接続方法である vPC の設定を行う前に、vPC について理解し、vPC と従来のサーバ接続方法との相違を理解することが重要です。ここでは、vPC とは何か、vPC によるメリット、および NX-OS ソフトウェア が稼働している Cisco Nexusスイッチに展開された vPC と ACI ファブリック内の vPC との相違について概要を説明します。

大まかに言えば、vPC は 2 つの個別の物理スイッチにリンク集約を拡張します。

図 *4 : vPC* トポロジ



上の図では、冗長性のために、1 つのサーバが 2 つの異なるスイッチにデュアルホーム接続されています。vPC を使用しない場合、サーバはアクティブ/スタンバイ設定を使用するか、アルゴリズムによってトラフィックをインテリジェントにロードバランスできる、NIC ドライバまたはカーネルの特別な設定を使用します。

当社では、2つの異なるスイッチに同じポートチャネルとしてポートを設定し、スイッチ間メッセージング チャネル（左側の緑色のボックスにあるスイッチ間ポート チャネルなど）を使用して冗長性に対処することにより、サーバのプロビジョニングと管理を大幅に簡素化する論理トポロジを実現しています。

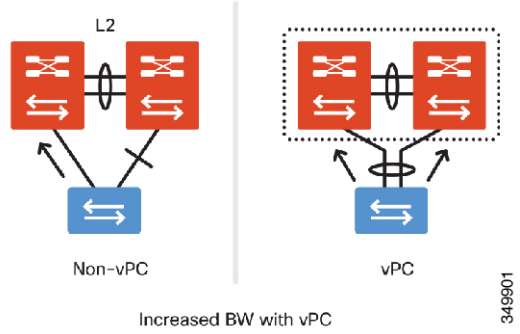
これにより、サーバ展開の観点から見て重要な次のメリットがもたらされます。

- リンク集約に基づく復元力のある レイヤ 2 トポロジを作成できます。
- STP は必要ありません。
- すべてのリンクがアクティブに転送されるため、帯域幅が増加します。
- 設定は単なるポートチャネルとして示され、特別なソフトウェアが不要なので、ドライバやカーネルの調整の観点から見て、サーバの設定が簡素化されます。

また、vPC を使用して他のダウンストリーム デバイス（Cisco UCS ファブリック インターコネクトなど）を接続すると、同様のメリットを実現できます。

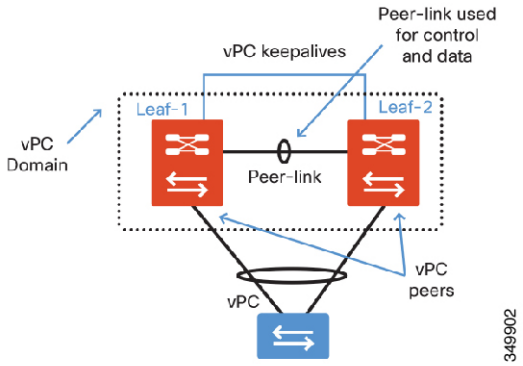
下記の図は、vPC 対応の Ciscoスイッチ ペアに接続された従来の単一のレイヤ 2 スイッチを示しています。

図 *5: vPC* と従来の接続の比較



従来の vPC ドメインのコンポーネントは、次の図のとおりです。

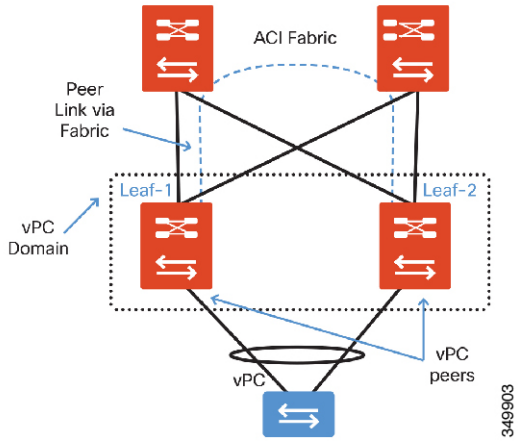
図 *6:* 従来の *vPC* トポロジ



上記の図に示すように、NX-OS ソフトウェアを実行している Cisco スイッチ製品では、vPC の設定はオペレータが手動で行う必要があり、設定にはピアリンクという専用の「スイッチ間」リンク ペアが必要です。また、アウトオブバンド管理ポートには、通常、ピアキープアライブ リンクがあり、これを使用してピアの状態を調べ、vPC ピア スイッチのフォールトを検出します。このような状況で、コンフィギュレーション同期機能を有効にせずに、設定を変更すると、vPC のプライマリとセカンダリ スイッチ間で vPC パラメータの不一致が生じ、タイプ 1 の不整合が検出された場合は、変更時に部分的な接続損失が発生する可能性があります。

ACI ファブリックは VPC の設定を大幅に簡素化します。

図 *7 : ACI* の *vPC* トポロジ



従来のvPC設計と比較した場合、注意すべき重要な相違点は、vPCピアリンクの設定に対して要件がないということです。また、管理ポートには送信するキープアライブがありません。ファブリック自体がピアリンクとして動作します。ファブリック ノード間の優れた相互接続によって、ピアがピア間のアクティブ パスを持つ可能性は低くなります。

注意点として、2つのリーフ スイッチ間でケーブル接続を試みると、GUIで「配線の不一致」フォールトが発生し、ポートは手動での復旧が必要なポートとしてブラックリストに入れられます。

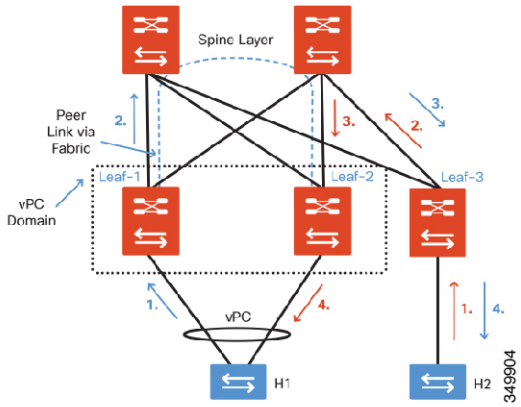
以下に、vPC を ACI ファブリックに適用する際に vPC に対して行われるその他の重要な動作変更を、従来の vPC と対比して示します。オペレータはこれらをよく理解する必要があります。

- ACI ファブリックの全設定を集中管理する APIC によるエラーのない設定を回避するために、設定は自動的に同期されます。
- 従来の vPC ソリューションでは、MCT がダウンした場合、スレーブ スイッチはその vPC リンクをすべて停止させます。
- ACI ファブリックでは、vPC ピア間のすべての冗長パスが同時に機能しなくなることはほとんどありません。したがって、ピア スイッチが到達不能になった場合、そのスイッチはクラッシュしたと見なされます。スレーブ スイッチは vPCリンク を停止しません。
- ロールの選択は引き続き発生し、ピアはマスター/スレーブの役割を担います。
- ロールは、vPC タイプ 1 の整合性エラー時に使用されます。スレーブ スイッチは vPC ポートをすべて停止します。次に示すタイプ 1 パラメータは、ACI ファブリック固有の vPC ドメインの整合性をチェックするために使用されます。
- グローバル タイプ 1 パラメータ：
  - STP
- インターフェイス タイプ 1 パラメータ：
  - STP：BPDU Guard のみ設定可能
  - EthPM

- ポート速度
- デュプレックス モード
- ポート モード
- MTU
- ネイティブ VLAN
  - PCM：チャネル モード、static と lacp
  - LACP：Lag ID

次の図は、ファブリック内の vPC ドメインと非 vPC 接続ホスト間で、ACI ファブリックによってトラフィックが転送される仕組みを示しています。

図 *8 : vPC* 転送



ユニキャスト パケット フロー H2 -> H1

1. H2 が、S3 へのリンクを介して H1 にパケットを送信します。
2. S3 が、vPC 仮想 IP（VIP）を使ってテーブルを検索し、ルーティングします。
3. スパイン スイッチは、VIP の複数のルートを調べ、そのいずれかを選択します（この例では S2）。
4. S2 が、ローカル接続されたホスト H1 にパケットを配信します。

H1 -> H2

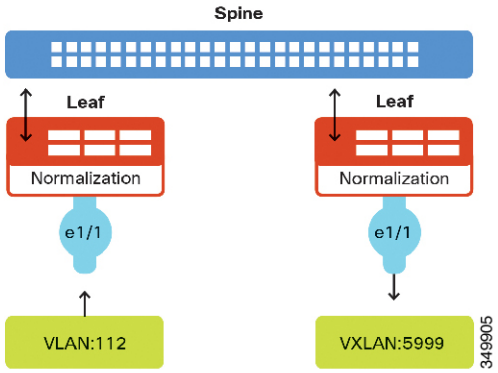
1. H1 が、PC リンクのいずれか（この例では S1）を介して H2 にパケットを送信します。
2. S1 が、S3 の IP を使ってテーブルを検索し、ルーティングします。
3. スパイン スイッチが S3 にルーティングします。
4. S3 が、ローカル接続されたホスト H2 にパケットを配信します。

VLAN プールの作成

この例では、新たに接続されたベアメタルサーバを設定するために、最初に物理ドメインを作成し、次に VLAN プールへのドメインのアソシエーションを作成する必要があります。前の項で説明したように、VLAN プールは EPG で使用される VLAN ID の範囲を定義します。

サーバはファブリックの2つの異なるリーフ ノードに接続されています。各サーバは、802.1Q または VXLAN カプセル化を使用してタギングされます。この設定例で使用される VLAN の範囲は 100 ～ 199 です。次の図に示すように、ACI ファブリックは、タグなしトラフィック、802.1Q VLAN タグ、VXLAN VNID、NVGRE タグなど、異なるカプセル化タイプ間のゲートウェイとしても動作することができます。リーフ スイッチは、タグを除去して、必要なタグをファブリック出力に再適用することで、トラフィックを正規化します。ACI では、VLAN はリーフ スイッチのポートに関係するため、VLAN の定義は識別用にのみ使用されることを理解する必要があります。ファブリックのリーフ スイッチの入り口にパケットが到達したときに、VLAN、VXLAN、NVGRE、物理ポート ID、仮想ポート ID などの識別子を使用してさまざまな EPG にパケットを分類する方法を、ACI が事前に知っている必要があります。

図 *9*: カプセル化の正規化



GUI を使用した VLAN プールの作成

この手順では、GUI を使用して、VLAN プールを作成します。

手順

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

ステップ 2 [Navigation] ペインで、**[Pools]** > **[VLAN]** の順に選択します。

ステップ 3 [Work] ペインで、**[Actions]** > **[Create VLAN Pool]** の順に選択します。

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

a) VLAN プールの名前を入力します。

b) （任意） VLAN プールの説明を入力します。

c) 割り当てモードを選択します。

- **Dynamic Allocation**： Application Policy Infrastructure Controller (APIC) はプールから VLAN を動的に選択します。これは、ポリシーが EPG 自体に適用されるため、実際の VLAN ID は重要ではない、VMM 統合モードで共通です。
- Static Allocation：これは通常、ベアメタル サーバで使用するために、スタティック ソース（EPG のスタティック パス バインディングなど）のプールが参照される場合に使用されます。

d) 1 つ以上のカプセル化ブロックを追加します。

カプセル化ブロックはVLANプールのVLAN範囲を定義します。1つのプールに複数の範囲を追加できます。カプセル化の各ブロックの割り当てのモードを選択します。

- **Dynamic Allocation**： Application Policy Infrastructure Controller (APIC) はプールからVLANを動的に選択します。これは、ポリシーがEPG自体に適用されるため、実際のVLAN ID は重要ではない、VMM 統合モードで共通です。
- Inherit Allocation Mode from parent：カプセル化ブロックはVLANプールに基づいてモードを継承します。
- Static Allocation：これは通常、ベアメタル サーバで使用するために、スタティック ソース（EPG のスタティック パス バインディングなど）のプールが参照される場合に使用されます。

ステップ 5 [送信（Submit）] をクリックします。

REST API を使用した VLAN プールの作成

次の REST 要求は VLAN プールを作成します。

```
<fvnsVlanInstP allocMode="static" childAction="" configIssues="" descr=""
  dn="uni/infra/vlanns-[bsprint-vlan-pool]-static" lcOwn="local"
modTs="2015-02-23T15:58:33.538-08:00"
  monPolDn="uni/fabric/monfab-default" name="bsprint-vlan-pool"
  ownerKey="" ownerTag="" status="" uid="8131">
    <fvnsRtVlanNs childAction="" lcOwn="local" modTs="2015-02-25T11:35:33.365-08:00"
      rn="rtinfraVlanNs-[uni/l2dom-JC-L2-Domain]" status="" tCl="l2extDomP"
tDn="uni/l2dom-JC-L2-Domain"/>
    <fvnsRtVlanNs childAction="" lcOwn="local" modTs="2015-02-23T16:13:22.007-08:00"
      rn="rtinfraVlanNs-[uni/phys-bsprint-PHY]" status="" tCl="physDomP"
tDn="uni/physbsprint-PHY"/>
    <fvnsEncapBlk childAction="" descr="" from="vlan-100" lcOwn="local"
modTs="2015-02-23T15:58:33.538-08:00"
      name="" rn="from-[vlan-100]-to-[vlan-199]" status="" to="vlan-199" uid="8131"/>
</fvnsVlanInstP>
```

物理ドメインの作成

物理ドメインは、VLANプールとアクセス エンティティ プロファイル（AEP）間のリンクとして動作します。ドメインはファブリックの設定をテナントの設定に結びつけます。ドメインをEPGに関連付けるのはテナント管理者であり、ドメインが作成されるのは[Fabric]タブだからです。この順序で設定すると、プロファイル名とVLANプールのみが設定されます。AEPとアソシエーションの作成については、この項の後半で説明します。

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Physical and External Domains] > [Physical Domains] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Physical Domain] の順に選択します。
4. [Create Physical Domain] ダイアログボックスで、次の操作を実行します。

1. プロファイルのわかりやすい名前を定義します。
2. 作成した VLAN プールを選択します。

XML オブジェクト

```
<physDomP childAction="" configIssues="" dn="uni/phys-bsprint-PHY" lcOwn="local"
modTs="2015-02-23T16:13:21.906-08:00" monPolDn="uni/fabric/monfab-default"
name="bsprint-PHY" ownerKey="" ownerTag="" status="" uid="8131">
<infraRsVlanNs childAction="" forceResolve="no" lcOwn="local" modTs="2015-02-
23T16:13:22.065-08:00" monPolDn="uni/fabric/monfab-default" rType="mo" rn="rsvlanNs"
state="formed" stateQual="none" status="" tCl="fvnsVlanInstP" tDn="uni/infra/vlanns-
[bsprint-vlan-pool]-static" tType="mo" uid="8131"/>
<infraRsVlanNsDef childAction="" forceResolve="no" lcOwn="local" modTs="2015-02-
23T16:13:22.065-08:00" rType="mo" rn="rsvlanNsDef" state="formed" stateQual="none"
status="" tCl="fvnsAInstP" tDn="uni/infra/vlanns-[bsprint-vlan-pool]-static"
tType="mo"/>
<infraRtDomP childAction="" lcOwn="local" modTs="2015-02-23T16:13:52.945-08:00"
rn="rtdomP-[uni/infra/attentp-bsprint-AEP]" status="" tCl="infraAttEntityP"
tDn="uni/infra/attentp-bsprint-AEP"/>
</physDomP>
```

GUI を使用した接続可能アクセス エンティティ プロファイルの作成

この手順では、GUI を使用して接続可能なアクセス エンティティ プロファイル（AEP）が作成されます。

手順

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

ステップ 2 [Navigation] ペインで、**[Global Policies]** > **[Attached Acess Entity Profle]** の順に選択します。

ステップ 3 [Work] ペインで、**[Actions]** > **[Create Attached Entity Profile]** の順に選択します。

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

a) AEP の名前を入力します。
b) （任意） AEP の説明を入力します。
c) インフラストラクチャ VLAN がこの AEP に関連付けられたリンクを通過するようにするには、[Enable Infrastructure VLAN] チェックボックスにチェックマークを付けてください。
d) [+] をクリックして、ドメインを AEP に関連付けます。
e) 先ほど設定した物理ドメインを選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 [送信（Submit）] をクリックします。

REST API を使用した接続可能アクセス エンティティ プロファイルの作成

次の REST 要求は接続可能アクセス エンティティ プロファイル（AEP）を作成します。

```
<infraAttEntityP childAction="" configIssues="" descr="" dn="uni/infra/attentpbsprint-AEP"
```

```
  lcOwn="local" modTs="2015-02-23T16:13:52.874-08:00" monPolDn="uni/fabric/monfab-default"

  name="bsprint-AEP" ownerKey="" ownerTag="" status="" uid="8131">
    <infraContDomP childAction="" lcOwn="local" modTs="2015-02-23T16:13:52.874-08:00"
      rn="dompcont" status="">
        <infraAssocDomP childAction="" dompDn="uni/phys-bsprint-PHY" lcOwn="local"
          modTs="2015-02-23T16:13:52.961-08:00" rn="assocdomp-[uni/phys-bsprint-PHY]"
status=""/>
        <infraAssocDomP childAction="" dompDn="uni/l2dom-JC-L2-Domain" lcOwn="local"
          modTs="2015-02-25T11:35:33.570-08:00" rn="assocdomp-[uni/l2dom-JC-L2-Domain]"
          status=""/>
    </infraContDomP>
    <infraContNS childAction="" lcOwn="local" modTs="2015-02-23T16:13:52.874-08:00"
      monPolDn="uni/fabric/monfab-default" rn="nscont" status="">
        <infraRsToEncapInstDef childAction="" deplSt="" forceResolve="no" lcOwn="local"
          modTs="2015-02-23T16:13:52.961-08:00" monPolDn="uni/fabric/monfabdefault"
          rType="mo" rn="rstoEncapInstDef-[allocencap-[uni/infra]/encapnsdef-
         [uni/infra/vlanns-[bsprint-vlan-pool]-static]]" state="formed" stateQual="none"

          status="" tCl="stpEncapInstDef" tDn="allocencap-[uni/infra]/encapnsdef-
          [uni/infra/vlanns-[bsprint-vlan-pool]-static]" tType="mo">
            <fabricCreatedBy childAction="" creatorDn="uni/l2dom-JC-L2-Domain"
              deplSt="" domainDn="uni/l2dom-JC-L2-Domain" lcOwn="local" modTs="2015-02-
              25T11:35:33.570-08:00" monPolDn="uni/fabric/monfab-default" profileDn=""
              rn="source-[uni/l2dom-JC-L2-Domain]" status=""/>
            <fabricCreatedBy childAction="" creatorDn="uni/phys-bsprint-PHY" deplSt=""
              domainDn="uni/phys-bsprint-PHY" lcOwn="local"
modTs="2015-02-23T16:13:52.961-08:00"
              monPolDn="uni/fabric/monfab-default" profileDn=""
rn="source-[uni/phys-bsprint-PHY]"
              status=""/>
        </infraRsToEncapInstDef>
    </infraContNS>
    <infraRtAttEntP childAction="" lcOwn="local" modTs="2015-02-24T11:59:37.980-08:00"
      rn="rtattEntP-[uni/infra/funcprof/accportgrp-bsprint-AccessPort]" status=""
      tCl="infraAccPortGrp" tDn="uni/infra/funcprof/accportgrp-bsprint-AccessPort"/>
    <infraRsDomP childAction="" forceResolve="no" lcOwn="local" modTs="2015-02-
      25T11:35:33.570-08:00" monPolDn="uni/fabric/monfab-default" rType="mo"
      rn="rsdomP-[uni/l2dom-JC-L2-Domain]" state="formed" stateQual="none" status=""
      tCl="l2extDomP" tDn="uni/l2dom-JC-L2-Domain" tType="mo" uid="8754"/>
    <infraRsDomP childAction="" forceResolve="no" lcOwn="local"
     modTs="2015-02-23T16:13:52.961-08:00" monPolDn="uni/fabric/monfab-default" rType="mo"

      rn="rsdomP-[uni/phys-bsprint-PHY]" state="formed" stateQual="none" status=""
tCl="physDomP"
      tDn="uni/phys-bsprint-PHY" tType="mo" uid="8131"/>
</infraAttEntityP>
```

インターフェイス ポリシーの作成

次に、インターフェイスプロファイルを定義し、ファブリック ポリシーの再利用を示します。インターフェイス ポリシーは、さまざまなインターフェイス プロファイル定義の要件によって、必要に応じて再利用できます。ここでは、新しいプロファイルの作成について説明しますが、簡単に選択できるポリシーが既に存在していれば理想的です。

リンク レベル ポリシーの作成

リンク レベル ポリシーは、ポートの速度などの設定を行います。

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Policies] > [Link Level] の順に選択します。

3. [Work] ペインで、[Actions] > [Create Link Level Policy] の順に選択します。
4. [Create Link Level Policy] ダイアログボックスで、次の操作を実行します。
    1. ポリシーのわかりやすい名前を定義します。
    2. （任意）ポリシーの説明を入力します。
    3. インターフェイスに対してオート ネゴシエーション モードを選択します。
    4. インターフェイスの速度を選択します。リーフ スイッチ ポートはデフォルトで 10 GE になります。
    5. 必要に応じて、デバウンス間隔を変更します。
5. [Submit] をクリックします。`

XML オブジェクト

```
<fabricHIfPol autoNeg="on" childAction="" descr="" dn="uni/infra/hintfpol-1G-Auto"
lcOwn="local" linkDebounce="100" modTs="2015-01-14T06:47:15.693-08:00" name="1G-Auto"
ownerKey="" ownerTag="" speed="1G" status="" uid="15374">
<fabricRtHIfPol childAction="" lcOwn="local" modTs="2015-01-14T06:48:48.081-
08:00" rn="rtinfraHIfPol-[uni/infra/funcprof/accportgrp-UCS-1G-PG]" status=""
tCl="infraAccPortGrp" tDn="uni/infra/funcprof/accportgrp-UCS-1G-PG"/>
<fabricRtHIfPol childAction="" lcOwn="local" modTs="2015-02-25T11:48:11.331-
08:00" rn="rtinfraHIfPol-[uni/infra/funcprof/accportgrp-L3-Example]" status=""
tCl="infraAccPortGrp" tDn="uni/infra/funcprof/accportgrp-L3-Example"/>
</fabricHIfPol>
```

CDP インターフェイス ポリシーの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Policies] > [CDP Interface] の順に選択します。
3. [Work] ペインで、[Actions] > [Create CDP Interface Policy] の順に選択します。
4. [Create CDP Interface Policy] ダイアログボックスで、次の操作を実行します。
    1. ポリシーのわかりやすい名前を定義します（「CDP-Enable」など）。
    2. （任意）ポリシーの説明を入力します。
    3. 管理状態として [enabled] または [disabled] を選択します。
5. [Submit] をクリックします。`

XML オブジェクト

```
<cdpIfPol adminSt="enabled" childAction="" descr="" dn="uni/infra/cdpIfP-CDP-Enable"
lcOwn="local" modTs="2015-01-14T06:47:25.470-08:00" name="CDP-Enable" ownerKey=""
ownerTag="" status="" uid="15374">
<cdpRtCdpIfPol childAction="" lcOwn="local" modTs="2015-01-14T07:23:54.957-
08:00" rn="rtinfraCdpIfPol-[uni/infra/funcprof/accportgrp-UCS-10G-PG]" status=""
tCl="infraAccPortGrp" tDn="uni/infra/funcprof/accportgrp-UCS-10G-PG"/>
<cdpRtCdpIfPol childAction="" lcOwn="local" modTs="2015-02-24T14:59:11.154-
08:00" rn="rtinfraCdpIfPol-[uni/infra/funcprof/accbundle-ACI-VPC-IPG]" status=""
tCl="infraAccBndlGrp" tDn="uni/infra/funcprof/accbundle-ACI-VPC-IPG"/>
<cdpRtCdpIfPol childAction="" lcOwn="local" modTs="2015-01-14T06:48:48.081-
08:00" rn="rtinfraCdpIfPol-[uni/infra/funcprof/accportgrp-UCS-1G-PG]" status=""
tCl="infraAccPortGrp" tDn="uni/infra/funcprof/accportgrp-UCS-1G-PG"/>
<cdpRtCdpIfPol childAction="" lcOwn="local" modTs="2015-02-24T11:59:37.980-
08:00" rn="rtinfraCdpIfPol-[uni/infra/funcprof/accportgrp-bsprint-AccessPort]"
status="" tCl="infraAccPortGrp" tDn="uni/infra/funcprof/accportgrp-bsprint-
```

```
AccessPort"/>
<cdpRtCdpIfPol childAction="" lcOwn="local" modTs="2015-02-25T11:48:11.331-
08:00" rn="rtinfraCdpIfPol-[uni/infra/funcprof/accportgrp-L3-Example]" status=""
tCl="infraAccPortGrp" tDn="uni/infra/funcprof/accportgrp-L3-Example"/>
</cdpIfPol>
```

LLDP インターフェイス ポリシーの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. ナビゲーション ウィンドウで、**[Interface Policies] > [Policies] > [LLDP Interface]** の順に選択します。
3. [Work] ペインで、[Actions] > [Create LLDP Interface Policy] の順に選択します。
4. [Create LLDP Interface Policy] ダイアログボックスで、次の操作を実行します。
    1. ポリシーのわかりやすい名前を定義します。
    2. （任意）ポリシーの説明を入力します。
    3. 受信状態を選択します。
    4. 送信状態を選択します。
5. [Submit] をクリックします。`

XML オブジェクト

```
<lldpIfPol adminRxSt="enabled" adminTxSt="enabled" childAction=""
descr=""
dn="uni/infra/lldpIfP-LLDP-Enable" lcOwn="local" modTs="2015-02-11T07:40:35.664-08:00"
name="LLDP-Enable" ownerKey="" ownerTag="" status="" uid="15374">
<lldpRtLldpIfPol childAction="" lcOwn="local" modTs="2015-02-24T14:59:11.154-
08:00" rn="rtinfraLldpIfPol-[uni/infra/funcprof/accbundle-ACI-VPC-IPG]"
status=""
tCl="infraAccBndlGrp" tDn="uni/infra/funcprof/accbundle-ACI-VPC-IPG"
/>
<lldpRtLldpIfPol childAction="" lcOwn="local" modTs="2015-02-25T11:48:11.331-
08:00" rn="rtinfraLldpIfPol-[uni/infra/funcprof/accportgrp-L3-Example]"
status=""
tCl="infraAccPortGrp" tDn="uni/infra/funcprof/accportgrp-L3-Example"
/>
</lldpIfPol>
```

GUI を使用したポート チャネル ポリシーの作成

この手順では、GUI を使用して、ポート チャネルのポリシーを作成します。

手順

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

ステップ 2 [Navigation] ペインで、**[Interface Policies]** > **[Policies]** > **[Port Channel Policies]** の順に選択します。

ステップ 3 [Work] ペインで、**[Actions]** > **[Create Port Channel Policy]** の順に選択します。

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

a) ポート チャネル ポリシーの名前を入力します。

b) （任意） ポート チャネル ポリシーの説明を入力します。
c) サーバに必要な LACP モードを選択します。

リーフ スイッチでLACPが有効になっている場合は、サーバまたは他の接続デバイスでもLACP を有効にする必要があります。

d) （任意） コントロール状態を選択します。
e) （任意） ポート チャネルのリンクの最小数と最大数を指定します。

（注） 右上隅にあるアイコン **i** を **ポート チャネル ポリシーの作成** ダイアログボックスでクリックして、 **Cisco APIC Online Help** ファイルにアクセスして、オプションの完全なリストを表示します。

ステップ 5 [送信（Submit）] をクリックします。

REST API を使用したポート チャネル ポリシーの作成

次の REST 要求はポート チャネル ポリシーを作成します。

```
<lacpLagPol childAction="" ctrl="fast-sel-hot-stdby,graceful-conv,susp-individual"
  descr="" dn="uni/infra/lacplagp-LACP-Active" lcOwn="local" maxLinks="16" minLinks="1"
  modTs="2015-02-24T11:58:36.547-08:00" mode="active" name="LACP-Active" ownerKey=""
  ownerTag="" status="" uid="8131">
    <lacpRtLacpPol childAction="" lcOwn="local" modTs="2015-02-24T14:59:11.154-08:00"
      rn="rtinfraLacpPol-[uni/infra/funcprof/accbundle-ACI-VPC-IPG]" status=""
      tCl="infraAccBndlGrp" tDn="uni/infra/funcprof/accbundle-ACI-VPC-IPG"/>
</lacpLagPol>
```

（注）

- 対称ハッシュを有効にするために、 `ctrl =「対称ハッシュ」` を REST 要求に追加します。
- 対称ハッシュは、次のスイッチではサポートされていません。
  - Cisco Nexus 93128TX
  - Cisco Nexus 9372PX
  - Cisco Nexus 9372PX-E
  - Cisco Nexus 9372TX
  - Cisco Nexus 9372TX-E
  - Cisco Nexus 9396PX
  - Cisco Nexus 9396TX

GUI を使用したポート チャネル メンバ プロファイルの作成（任意）

この手順では、GUI を使用して、ポート チャネルのメンバ プロファイルを作成します。

手順

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

ステップ 2 [Navigation] ペインで、**[Interface Policies]** > **[Policies]** > **[Port Channel Member Policies]** の順に選択します。

ステップ 3 [Work] ペインで、**[Actions]** > **[Create Port Channel Member Policy]** の順に選択します。

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

a) ポリシーの名前を入力します。
b) （任意） ポリシーの説明を入力します。
c) 必要に応じて、プライオリティを変更します。
d) 必要に応じて、送信レートを変更します。

ステップ 5 [送信（Submit）] をクリックします。

GUI を使用したスパニング ツリー インターフェイス ポリシーの作成（任意）

スパニング ツリー ポリシーは、サウスバウンド リーフ ポートのスパニング ツリー機能の動作を指定します。一般的なベスト プラクティスは、サーバに接続しているインターフェイスで BPDU ガードを有効にすることです。

（注） ACIは、リーフとスパイン間のファブリックでスパニング ツリーを実行しません。スパニング ツリー インターフェイス ポリシーは、ポートの動作を定義するだけです。

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Policies] > [Spanning Tree Interface] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Spanning Tree Interface Policy] の順に選択します。
4. [Create Spanning Tree Interface Policy] ダイアログボックスで、次の操作を実行します。
    1. ポリシーのわかりやすい名前を定義します。
    2. （任意）ポリシーの説明を入力します。
    3. BPDU フィルタと BPDU ガード（またはどちらか一方）を有効にします。
5. [送信（Submit）] をクリックします。

GUI を使用したストーム制御ポリシーの作成（任意）

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能を使用すると、物理インターフェイス上のブロードキャスト、マルチキャス

ト、またはユニキャスト トラフィック ストームによって、ポート経由の通信が中断されるのを防ぐことができます。

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Policies] > [Storm Control] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Storm Control Policy] の順に選択します。
4. [Create Storm Control Policy] ダイアログボックスで、次の操作を実行します。
    1. ポリシーのわかりやすい名前を定義します。
    2. （任意）ポリシーの説明を入力します。
    3. 制御ポリシーの適用方法を指定します（データセンターの要件に一致する合計帯域幅の割合、またはパケット/秒定義として適用）。
5. [送信（Submit）] をクリックします。

GUI を使用した誤配線プロトコル インターフェイス ポリシーの作成（任意）

誤配線プロトコル（MCP）は、Link Layer Discovery Protocol（LLDP）、スパニング ツリー プロトコル（STP）が検出できない設定ミスを処理するために設計されました。MCPには、それを使用するレイヤ 2 パケットがあり、MCP はファブリック内のループを形成するポートを無効にします。Cisco Application Centric Infrastructure (ACI) ファブリック リーフはスパニング ツリープロトコル（STP）に参加せず、STP に関してハブとして動作します。タグ付けされていない MCP パケットが送信され、ファブリックはパケットが戻ったことを確認し、ループが存在することを認識した場合、ファブリックはそのイベントに基づいてアクションを実行します。これが発生するとエラーとイベントが生成されます。MCP は、グローバルに、およびインターフェイスごとに有効にできます。デフォルトでは、MCP がグローバルに無効にされ、各ポートで有効になっています。MCP が機能するには、インターフェイス単位の設定に関係なく、グローバルに有効にする必要があります。

次の手順では、GUI を使用して MPC インターフェイス ポリシーを作成します。

手順

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

ステップ 2 [Navigation] ペインで、**[Interface Policies]** > **[Policies]** > **[MCP Interface]** の順に選択します。

ステップ 3 [Work] ペインで、**[Actions]** > **[Create Mis-cabling Protocol Interface Policy]** の順に選択します。

ステップ 4 [Create Mis-cabling Protocol Interface Policy] ダイアログボックスで、次の操作を実行します。

a) ポリシーの名前を入力します。
b) （任意） ポリシーの説明を入力します。
c) [Admin State] に対して、ポリシーを有効にするには [Enable] を選択し、ポリシーを無効にするには [Disable] を選択します。

ステップ 5 [送信（Submit）] をクリックします。

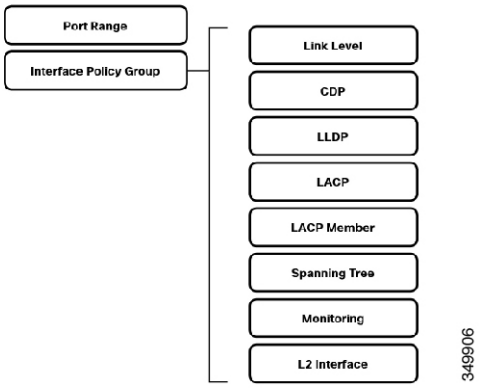
GUI を使用したポート単位 VLAN を有効にするレイヤ 2 インターフェイス ポリシーの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Policies] > [L2 Interface] の順に選択します。
3. [Work] ペインで、[Actions] > [Create L2 Interface Policy] の順に選択します。
4. [Create L2 Interface Policy] ダイアログボックスで、次の操作を実行します。
   1. L2 インターフェイスの名前、および説明（任意）を入力します。
   2. ポート単位の VLAN を有効にするため、VLAN Scope で Port Local scope を選択します。

インターフェイス ポリシー グループの作成

インターフェイスポリシーグループは複数のインターフェイスポリシーから構成されており、機能グループとしてインターフェイスに関連付けられます。次の図は、これまでに作成した項目がポリシー グループの下にグループ化されている事を示しています。

図 *10 :* ポリシー グループに含まれているポリシー



すべてのインターフェイスポリシーを定義したら、個々のポリシーを統合してポリシーグループを形成し、インターフェイス プロファイルにリンクすることができます。ポリシー グループは、次のいずれかのマスター定義から定義されます。

- アクセス ポリシー グループ
- ポート チャネル ポリシーグループ
- vPC ポリシー グループ

GUI を使用したアクセス ポート ポリシー グループの作成

アクセス ポート ポリシーは、個々のリンク（非ポート チャネルまたは vPC）に対して定義されます。

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Policy Groups] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Access Policy Group] の順に選択します。
4. [Create Access Policy Group] ダイアログボックスで、次の操作を実行します。
   1. ポリシー グループのわかりやすい名前を定義します。
   2. （任意）ポリシー グループの説明を入力します。
   3. 前に作成した、このポリシー グループに関連するプロファイルを使用します。
5. [送信（Submit）] をクリックします。

GUI を使用したポート チャネル インターフェイス ポリシー グループの作成

ポートチャネルは、チャネル グループのメンバーである物理インターフェイス間のトラフィックをロード バランシングします。ポート チャネルに設定する必要があるインターフェイス グループごとに、異なるポリシー グループを作成する必要があります。このポリシー グループは動作を定義します。たとえば、あるポート チャネルにポート 1/1-4 を設定し、別のポート チャネルにポート 1/5-8 を設定する場合は、これらの各グループに対して個別にポリシー グループを作成する必要があります。

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Policy Groups] の順に選択します。
3. [Work] ペインで、[Actions] > [Create PC Interface Policy Group] の順に選択します。
4. [Create PC Interface Policy Group] ダイアログボックスで、次の操作を実行します。
   1. ポリシー グループのわかりやすい名前を定義します。
   2. （任意）ポリシー グループの説明を入力します。
   3. 前に作成した、この PC ポリシー グループに関連するプロファイルを選択します。
5. [送信（Submit）] をクリックします。

VPC インターフェイス ポリシー グループの作成

（注） このオブジェクトは、作成される各 vPC に対して一意である必要があります。

仮想ポート チャネル（vPC）は、2 つの異なるデバイスに物理的に接続されたリンクを、その他のデバイスから単一のポート チャネルとして見えるようにします。ACI では、ダウンストリーム デバイスがアクティブ-アクティブでデュアルホーム接続できるように、リーフ スイッチ ペアが vPC ドメインに設定される場合があります。

vPC に設定する各インターフェイス グループごとに、異なるインターフェイス ポリシー グループを作成する必要があります。vPC ポリシー グループには、ポート チャネルの動作の定義、および ID の両方が含まれています。たとえば、2 つのスイッチ間のひとつの vPC にポート 1/1-4 を設定し、別の vPC にポート 1/5-8 を設定する場合は、これらの各グループに対して個別にポリシー グループを作成する必要があります。

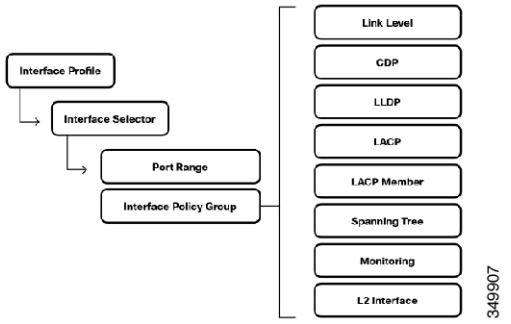
（注） vPC の場合は、2 つのペア スイッチ間に一意の vPC ドメイン定義が必要です。詳細については後述します。

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Policy Groups] の順に選択します。
3. [Work] ペインで、[Actions] > [Create vPC Interface Policy Group] の順に選択します。
4. [Create vPC Interface Policy Group] ダイアログボックスで、次の操作を実行します。
    1. ポリシー グループのわかりやすい名前を定義します。
    2. （任意）ポリシー グループの説明を入力します。
    3. 前に作成した、この vPC ポリシー グループに関連するプロファイルを選択します。
5. [送信（Submit）] をクリックします。

インターフェイス プロファイル

ACI 内のインターフェイス プロファイルは、インターフェイスの動作を定義するポリシー グループをインターフェイスにリンクします。ポリシーグループは特定のポートを纏めるインターフェースセレクタに割り当てます。次に、インターフェイス プロファイルがスイッチ プロファイルに関連付けられ、設定するリーフ スイッチ上のポートが指定されます。引き続きポートプロファイルを定義していきますが、さまざまなプロファイルが設定されているこのオブジェクト ツリーを見ると、その下位から作業を積み上げてきた様子を確認できます。相互に関連しているこれらの各ポリシーの目的は、ポリシーの再利用を最大化することです。

図 *11*:インターフェイス セレクタとインターフェイス ポリシー グループにリンクしているインターフェイス プロファイル



ポリシーはインターフェイス プロファイルで定義され、インターフェイス セレクタとアクセス ポート ポリシー グループによってポートに割り当てられます。前の項の図は、そのようなポリシーをグループ化することによって何を実現できるかを視覚的に示しています。

インターフェイス プロファイルの作成

インターフェイス プロファイルは次の 2 つのプライマリ オブジェクトから構成されます。インターフェイス セレクタとアクセス ポート ポリシー グループ。インターフェイス セレクタは、どのインターフェイスがアクセス ポート ポリシーを適用するかを定義します。同じ属性を共有するポートは、同じインターフェイスプロファイルにグループ化できます。

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Profiles] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Interface Profile] の順に選択します。
4. [Create Interface Profile] ダイアログボックスで、次の操作を実行します。
    1. プロファイルのわかりやすい名前を定義します。
    2. （任意）プロファイルの説明を入力します。
5. [送信（Submit）] をクリックします。

GUI を使用したインターフェイス セレクタの作成

この手順では、GUI を使用してインターフェイス セレクタを作成します。

手順

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

ステップ 2 [Navigation] ペインで、**[Interface Policies]** > **[Profiles]** > ***[Name_of_Interface_Profile]*** の順に選択します。

ステップ 3 [Work] ペインで、**[Actions]** > **[Create Access Port Selector]** の順に選択します。

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

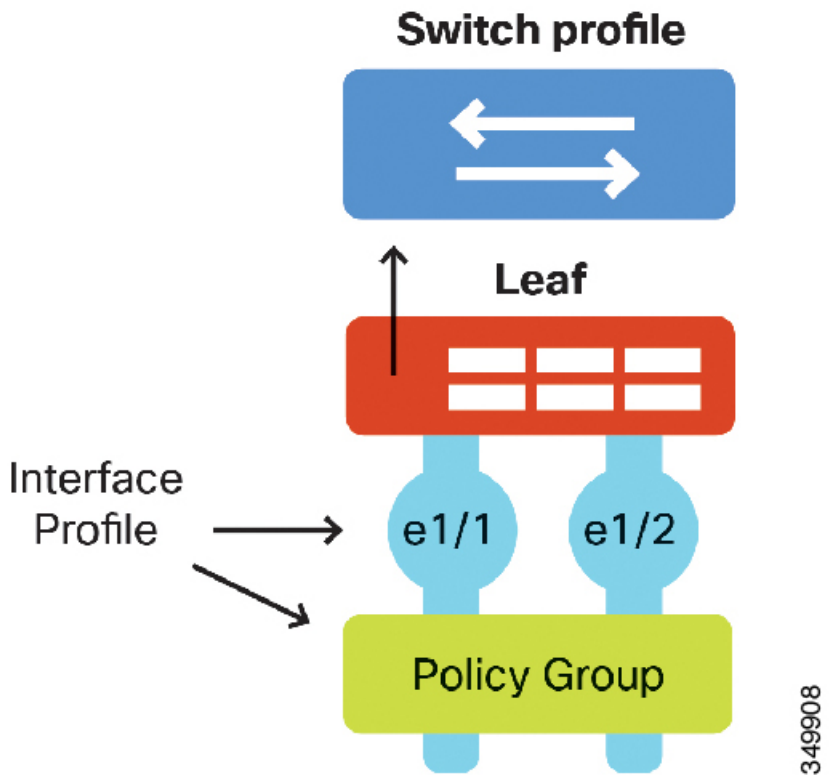
a) プロファイル名を入力します。
b) （任意） プロファイルの説明を入力します。
c) インターフェイス ID を入力します。
d) ポートが FEX に接続されたら、[Connected to FEX] ボックスにチェックマークを付けてください。
e) ポートに関連付けるインターフェイス ポリシー グループを選択します。

ステップ 5 [送信（Submit）] をクリックします。

GUI を使用したポート チャネルのインターフェイス プロファイルの作成

サーバにリーフ スイッチへの複数のアップリンクがある場合は、復元性と負荷分散が有効になるように、それらのリンクを 1 つのポート チャネルにバンドルできます。ACI にこれを設定するには、`Port Channel` タイプのインターフェイス ポリシー グループを作成して、インターフェイスにバンドルします。異なるポート チャネルには異なるポリシー グループが必要です。

図 *12 :* ポート チャネル ポリシーグループ



この手順では、GUI を使用して、ポート チャネルのインターフェイス プロファイルを作成します。

手順

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

ステップ 2 [Navigation] ペインで、**[Interface Policies]** > **[Profiles]** の順に選択します。

ステップ 3 [Work] ペインで、**[Actions]** > **[Create Interface Profile]** の順に選択します。

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

a) プロファイル名を入力します。
b) （任意） プロファイルの説明を入力します。

ステップ 5 [Submit] をクリックします。`

次に、インターフェイス ポート セレクタを作成します。ポート チャネルを設定するため、オペレータは、ポート チャネル インターフェイスで必要なインターフェイスをすべて追加します。この例では、インターフェイスのイーサネット 1/1-2 を 1 つのポート チャネルに設定し、インターフェイスのイーサネット 1/3-4 を別のポート チャネルに設定します。

ステップ 6 メニュー バーで、**[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 7 [Navigation] ペインで、**[Interface Policies]** > **[Profiles]** > ***[Name_of_Interface_Profile]*** の順に選択します。

ステップ 8 [Work] ペインで、**[Actions]** > **[Create Access Port Selector]** の順に選択します。

ステップ 9 [Create Access Port Selector] ダイアログボックスで、次の操作を実行します。

a) プロファイル名を入力します。
b) （任意） プロファイルの説明を入力します。
c) 1 番目のポート チャネルのインターフェイス ID を入力します。
d) インターフェイス ポリシー グループを選択します。

ステップ 10 [Submit] をクリックします。`

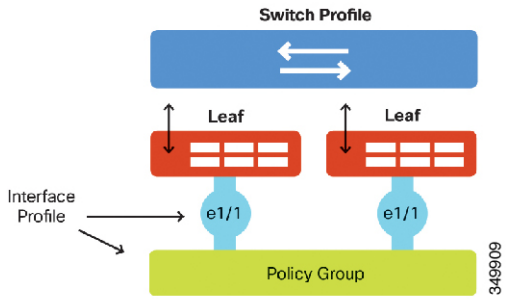
ステップ 11 別のポート チャネルを追加するには、ステップ 8 から 10 を繰り返します。

仮想ポート チャネルのインターフェイス プロファイルの作成

vPC ドメインは、常に 2 つのリーフ スイッチから構成され、リーフ スイッチは 1 つの vPC ドメインのメンバーにのみなることができます。つまり、ACI では、ポリシーの定義は 2 つのスイッチ間で重要になります。2 つのスイッチ間で同じポリシーを再利用し、vPC ドメインを介してペアを定義できます。ファームウェア メンテナンス グループを設定する際は、vPC スイッチ ドメインのメンバーを考慮する必要があります。このことに留意して、ファームウェアのアップグレードによって両方の vPC スイッチ ピアが同時に影響を受けないようにします。この詳細については、「ファームウェアのアップグレードとダウングレード」の項を参照してください。

したがって、2 つの個別のスイッチ ID を示すスイッチ プロファイルを作成する必要があります。同じポリシー グループ内の2つのポートとこれらのスイッチとの関係は、インターフェイス プロファイルによって定義されます。

図 *13 : vPC* ポリシー グループ



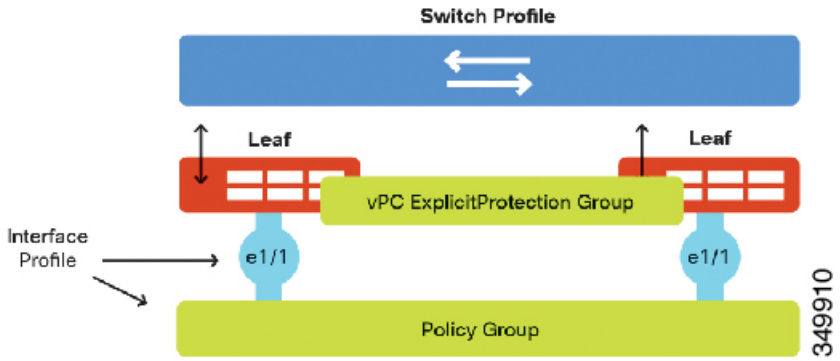
vPC のメンバーになる各側のグループ化されたインターフェイスに対して、同じ手順を繰り返す必要があります。

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Profiles] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Interface Profile] の順に選択します。
4. [Create Interface Profile] ダイアログボックスで、次の操作を実行します。
    1. プロファイルのわかりやすい名前を定義します。
    2. （任意）プロファイルの説明を入力します。
5. [Submit] をクリックします。`
6. ナビゲーション ウィンドウで、**[Interface Policies] > [Profiles] > *[Name_of_Interface_Profile_Created]*** の順に選択します。
7. [Work] ペインで、[Actions] > [Create Access Port Selector] の順に選択します。
8. [Create Access Port Selector] ダイアログボックスで、次の操作を実行します。
    1. プロファイルのわかりやすい名前を定義します。
    2. （任意）プロファイルの説明を入力します。
    3. インターフェイスの ID を入力します。
    4. vPC ポートの動作に関連付けるインターフェイス ポリシー グループを選択します。
9. [送信（Submit）] をクリックします。

仮想ポート チャネル用の vPC ドメインの作成

vPC を設定する場合は、さらに別のステップを実行して、同じ vPC ドメインに 2 つのリーフ スイッチを配置します。

図 *14 : vPC* ドメインの作成



1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Switch Policies] > [vPC Domain] > [Virual Port Channel default]> の順に選択します。
3. [Work] ペインで、[Actions] > [Create Explicit vPC Protection Group] の順に選択します。
4. [Create Explicit vPC Protection Group] ダイアログボックスで、次の操作を実行します。
   1. vPC ドメインのわかりやすい名前を定義します。
   2. vPC ドメインを表す一意の ID を入力します。
   3. vPC ドメインに組み込む 1 番目のスイッチを選択します。
   4. vPC ドメインに組み込む 2 番目のスイッチを選択します。
5. [送信（Submit）] をクリックします。

スイッチ プロファイル

スイッチ プロファイルは、個々のスイッチ ポートの動作を定義するすべてのインターフェイス プロファイルをグループ化します。スイッチプロファイルは、1 つのスイッチの定義である場合と、複数のスイッチの定義である場合があります。ベストプラクティスとして、各リーフ スイッチ用のスイッチ プロファイルと、リーフ スイッチの各 vPC ドメイン ペア用の別のスイッチ プロファイルが必要です。

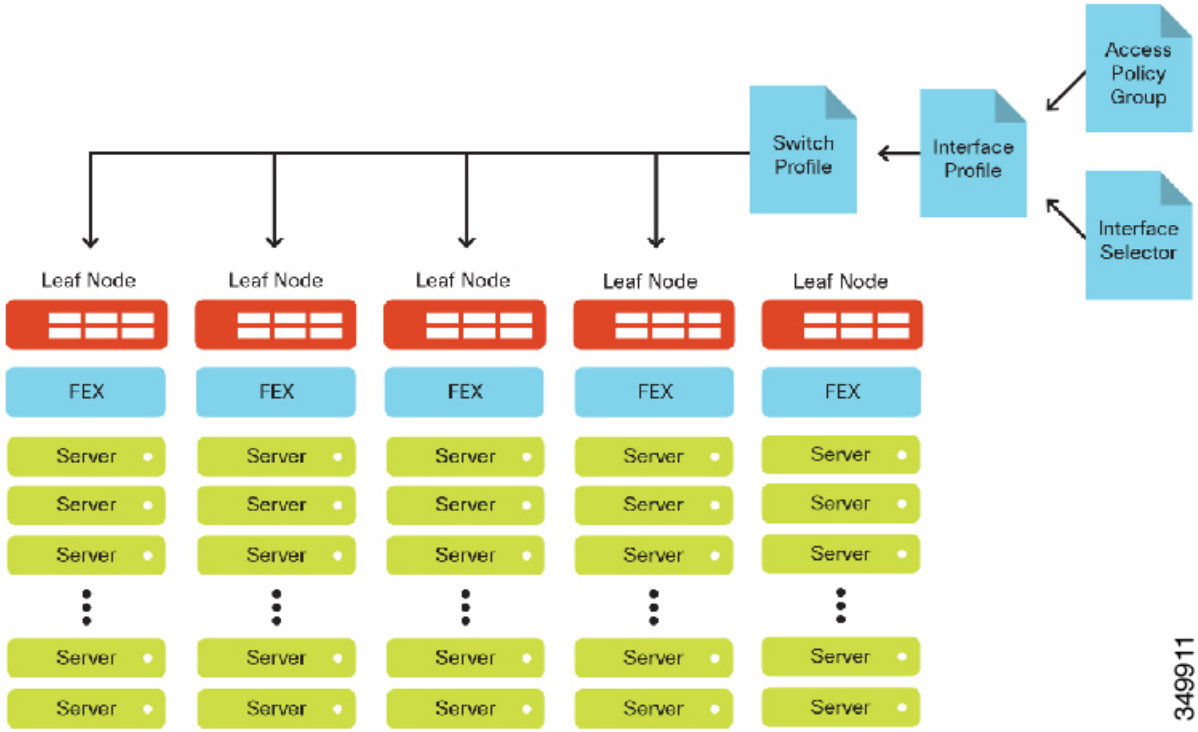
ユーザが作成したインターフェイスプロファイルは、1 つのスイッチプロファイルによってスイッチに関連付けることができます。または、さまざまなスイッチプロファイルによって関連付けることができます。同じ方法で設定されたインターフェイス ポートが複数のスイッチにあ

る場合は、同じスイッチプロファイルを使用すると役立ちます。これによって、各スイッチを個々に設定することなく、運用中に多数のスイッチの設定を変更できます。

再利用

運用面から再度強調しますが、ポリシーの再利用機能は重要です。たとえば、速度1GBのポートを設定するプロファイルが定義されている場合、そのプロファイルを多数のインターフェイス ポリシー グループに対して再利用できます。スイッチの設定全体に目を通すことで、プロファイルの再利用を拡張して、データセンターの運用を簡素化し、コンプライアンスを確保できます。次の図は、スイッチのラック間でのプロファイルの再利用を示しています。

図 *15*：大規模なポリシーの再利用



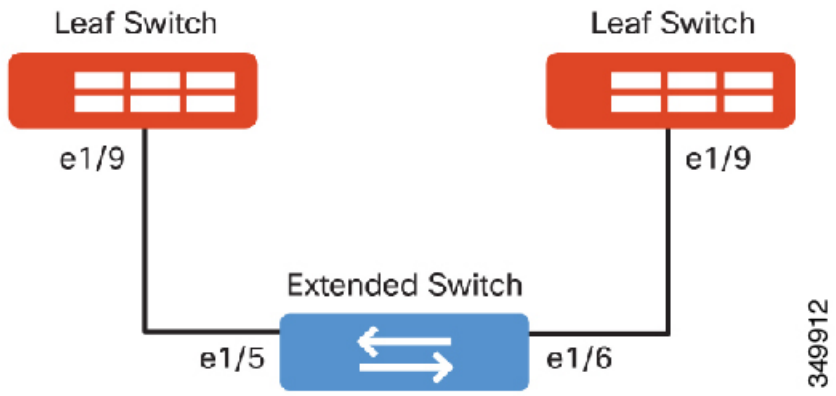
上記の図では、トップオブ ラック スイッチが同じスイッチ プロファイルに基づいています。これらのラックがすべて同じ方法で設定されている場合（つまり、同じ方法で配線されている場合）は、スイッチを同じスイッチプロファイルに割り当てるだけで同じポリシーを再利用できます。これにより、スイッチはプロファイルツリーを継承し、他のラックとまったく同じように設定されます。

また、プロファイルの削除による影響を確認することも重要です。複数のデバイス間でプロファイルが再使用されている場合は、プロファイルやポリシーを削除する前に、それが使用中かどうかを確認してください。

vPC の作成例

以下の手順は、vPC のブリングアップの様子、および vPC の API POST 設定評価を示しています。次のトポロジを設定します。

図 *16*：トポロジの例



VLAN プールの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Pools] > [VLAN] の順に選択します。
3. [Work] ペインで、[Actions] > [Create VLAN Pool] の順に選択します。
4. [Create VLAN Pool] ダイアログボックスで、次の操作を実行します。
    1. プールのわかりやすい名前を定義します。
    2. （任意）プールの説明を入力します。
    3. 割り当てモードに対して [Static Allocation] をクリックします。**注**：この例では、プールは VLAN 100 ～ VLAN 199 になります。

```
REST :: /api/node/class/fvnsVlanInstP.xml
```

物理ドメインの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Physical and External Domains] > [Physical Domains] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Physical Domain] の順に選択します。
4. [Create Physical Domain] ダイアログボックスで、次の操作を実行します。
    1. ドメインのわかりやすい名前を定義します。
    2. 前に作成した VLAN プールを選択します。

```
REST :: /api/node/class/physDomP.xml
```

アクセス エンティティ プロファイルの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Global Policies] > [Attachable Access Entity Profles] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Attached Entity Profile] の順に選択します。
4. [Create Attached Entity Profile] ダイアログボックスで、次の操作を実行します。
    1. AEP のわかりやすい名前を定義します。
    2. AEP を表す一意の ID を入力します。
    3. [Enable Infrastructure VLAN] チェックボックスはオフのままにします。
    4. [+] をクリックし、インターフェイスに関連付けるドメインを追加します。
    5. 前に作成した物理ドメインを選択します。
5. [Next] をクリックします。
6. [Submit] をクリックします。`

```
REST :: /api/node/class/infraAttEntityP.xml
```

リンク レベル ポリシーの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Policies] > [Link Level] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Link Level Policy] の順に選択します。
4. [Create Link Level Policy] ダイアログボックスで、次の操作を実行します。
    1. プールのわかりやすい名前を定義します。
    2. （任意）ポリシーの説明を入力します。
    3. インターフェイスに対してオートネゴシエーションを選択します。
    4. インターフェイス要件に合致する速度を選択します。
5. [Submit] をクリックします。`

```
REST :: /api/node/class/fabricHIfPol.xml
```

ポート チャネル ポリシーの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Policies] > [Port Channel] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Port Channel Policy] の順に選択します。
4. [Create Port Channel Policy] ダイアログボックスで、次の操作を実行します。
    1. ポリシーのわかりやすい名前を定義します。
    2. （任意）プールの説明を入力します。
    3. モードで [Active] をクリックします。
5. [Submit] をクリックします。`

```
REST :: /api/node/class/lacpLagPol.xml
```

vPC インターフェイス ポリシー グループの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Policy Groups] の順に選択します。
3. [Work] ペインで、[Actions] > [Create vPC Interface Policy Group] の順に選択します。
4. [Create vPC Interface Policy Group] ダイアログボックスで、次の操作を実行します。
    1. ポリシー グループのわかりやすい名前を定義します。
    2. （任意）ポリシー グループの説明を入力します。
    3. リンク レベル ポリシーを選択します。
    4. ポート チャネル ポリシーを選択します。

（注） vPC の場合は LACP をお勧めします。ただし、リーフ スイッチに接続しているデバイス上に LACP が設定されていることを確認してください。

    5. ポリシー グループに関連付ける AEP を選択します。
5. [Submit] をクリックします。`

```
REST :: /api/node/class/infraAccBndlGrp.xml
```

インターフェイス プロファイルの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Interface Policies] > [Profiles] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Interface Profile] の順に選択します。
4. [Create Interface Profile] ダイアログボックスで、次の操作を実行します。
    1. ポリシー グループのわかりやすい名前を定義します。
    2. （任意）ポリシー グループの説明を入力します。
5. [Submit] をクリックします。`
6. [Navigation] ペインで、[Interface Policies] > [Profiles] > [Profiles] > [ACI-VPC-int-profile] の順に選択します。
7. [Work] ペインで、[Actions] > [Create Access Port Selector] の順に選択します。
8. [Create Access Port Selector] ダイアログボックスで、次の操作を実行します。
    1. プロファイルのわかりやすい名前を定義します。
    2. （任意）説明を入力します。
    3. 適切なインターフェイスを選択します。
    4. インターフェイス ポリシー グループを選択します。
9. [Submit] をクリックします。`

```
REST :: /api/node/class/infraAccPortP.xml
```

スイッチ プロファイルの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Switch Policies] > [Profiles] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Switch Profile] の順に選択します。
4. [Create Switch Profile] ダイアログボックスで、次の操作を実行します。
    1. プロファイルのわかりやすい名前を定義します。
    2. （任意）プロファイルの説明を入力します。
    3. スイッチ セレクタで、[+] 記号をクリックします。
        1. Name：103 - 104（ノード番号を名前にした例）。
        2. Blocks：スイッチ 103 と スイッチ 104 を選択します。
5. [Next] をクリックします。
6. 前に作成したインターフェイス セレクタを選択します。
7. [Finish] をクリックします。

```
REST :: /api/node/class/infraNodeP.xml
```

vPC ドメインの作成

1. メニュー バーで、[Fabric] > [Access Policies] の順に選択します。
2. [Navigation] ペインで、[Switch Policies] > [Policies] > [Virual Port Channel default]> の順に選択します。
3. [Work] ペインで、[Actions] > [Create Explicit vPC Protection Group] の順に選択します。
    1. [Create Explicit vPC Protection Group] ダイアログボックスで、次の操作を実行します。
    2. [Explicit vPC Protection Groups] セクションで、[+] をクリックして vPC 保護グループを作成します。
    3. vPC ドメインのわかりやすい名前を定義します。
    4. vPC ドメインの一意の ID を入力します。
    5. この vPC ペアの 1 番目のスイッチの ID（103）を選択します。
    6. この vPC ペアの 2 番目のスイッチの ID（104）を選択します。
4. [Submit] をクリックします。`

```
REST :: /api/node/class/fabricExplicitGEp.xml
```

GUI を使用した設定済み vPC の動作の検証

1. メニュー バーで、[Fabric] > [Inventory] の順に選択します。
2. [Navigation] ペインで、[POD 1] > [Node_Name] > [Interfaces] > [vPC Interfaces] の順に選択します。
3. [Work] ペインに、vPC インターフェイスのステータスを示すテーブルが表示されます。適切に設定されている場合は、ステータスが表示され、vPC ドメインが正常に設定されたことが示されます。

CLI を使用した設定済み vPC の動作の検証

スイッチの CLI から直接、vPC の動作を検証することができます。コンソールまたはリーフノードのアウトオブバンド管理インターフェイスに接続している場合は、showvpcコマンドを使ってステータスを表示できます。

```
Leaf-3# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 100
Peer status : peer adjacency formed ok
vPC keep-alive status : Disabled
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : primary
Number of vPCs configured : 1
Peer Gateway : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Enabled (timeout = 240 seconds)
Operational Layer3 Peer : Disabled
vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 up -
vPC status
----------------------------------------------------------------------------
id Port Status Consistency Reason Active vlans
-- ---- ------ ----------- ------ ------------
1 Po1 up success success
```

次の REST API 呼び出しを使用して、vPC を構築し、スタティック ポート バインディングに vPC を接続できます。

```
URL: https://{{apic-ip}}/api/policymgr/mo/.xml
<polUni>
<infraInfra>
<!-- Switch Selector -->
<infraNodeP name="switchProfileforVPC_201">
<infraLeafS name="switchProfileforVPC_201" type="range">
<infraNodeBlk name="nodeBlk" from_="201" to_="201"/>
</infraLeafS>
<infraRsAccPortP tDn="uni/infra/accportprof-intProfileforVPC_201"/>
</infraNodeP>
<infraNodeP name="switchProfileforVPC_202">
<infraLeafS name="switchProfileforVPC_202" type="range">
<infraNodeBlk name="nodeBlk" from_="202" to_="202"/>
</infraLeafS>
<infraRsAccPortP tDn="uni/infra/accportprof-intProfileforVPC_202"/>
</infraNodeP>
<!-- Interface Profile -->
<infraAccPortP name="intProfileforVPC_201">
<infraHPortS name="vpc201-202" type="range">
<infraPortBlk name="vpcPort1-15" fromCard="1" toCard="1" fromPort="15"
toPort="15"/>
<infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-intPolicyGroupforVPC"/>
</infraHPortS>
</infraAccPortP>
<infraAccPortP name="intProfileforVPC_202">
<infraHPortS name="vpc201-202" type="range">
```

```
<infraPortBlk name="vpcPort1-1" fromCard="1" toCard="1" fromPort="1"
toPort="1"/>
<infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-intPolicyGroupforVPC"/>
</infraHPortS>
</infraAccPortP>
<!-- Interface Policy Group -->
<infraFuncP>
<infraAccBndlGrp name="intPolicyGroupforVPC" lagT="node">
<infraRsAttEntP tDn="uni/infra/attentp-AttEntityProfileforCisco"/>
<infraRsCdpIfPol tnCdpIfPolName="CDP_ON" />
<infraRsLacpPol tnLacpLagPolName="LACP_ACTIVE" />
<infraRsHIfPol tnFabricHIfPolName="10GigAuto" />
</infraAccBndlGrp>
</infraFuncP>
</infraInfra>
</polUni>
https://{{hostName}}/api/node/mo/uni.xml
<polUni>
<fvTenant descr="" dn="uni/tn-Cisco" name="Cisco" ownerKey="" ownerTag="">
<fvAp descr="" name="CCO" ownerKey="" ownerTag="" prio="unspecified">
<fvAEPg descr="" matchT="AtleastOne" name="Web" prio="unspecified">
<fvRsPathAtt encap="vlan-1201" instrImedcy="immediate" mode="native"
tDn="topology/pod-1/protpaths-201-202/pathep-[vpc201-202]” />
</fvAEPg>
<fvAEPg descr="" matchT="AtleastOne" name="App" prio="unspecified">
<fvRsPathAtt encap="vlan-1202" instrImedcy="immediate" mode="native"
tDn="topology/pod-1/protpaths-201-202/pathep-[vpc201-202]” />
</fvAEPg>
</fvAp>
</fvTenant>
</polUni>
```

サーバ接続

サーバ接続は、 Cisco Application Centric Infrastructure (ACI) ファブリックで、すべてのアプリケーション ワークロードが適切に機能するために必要です。サーバ インフラストラクチャで指定されたファブリック接続要件を注意深く検討する必要があります。Cisco Unified Computing System（UCS）の場合は、これらの条件に一致するように、ファブリック アクセス ポリシーをプロビジョニングする必要があります。これらのポリシーはすべて、インターフェイス ポリシー グループによって管理されます。ACME 社には、データセンター内に複数の異なるサーバ モデルがあります。たとえば、Cisco UCS B シリーズおよび Cシリーズ、ACI ファブリックに接続する必要があるサード パーティ製サーバなどです。

シスコ UCS B シリーズ サーバ

UCS を ACI ファブリックに接続するときに、ポート側のファブリック インターコネクトで必要とされるレイヤ2接続のタイプを最初に決定する必要があります。ベストプラクティスは、仮想ポート チャネル（vPC）を使用して UCS 環境に接続することで、マルチシャーシ EtherChannel を作成することです。このシナリオでは、個々のリンクとファブリック スイッチのフォールトが軽減され、高いアップタイムが期待されます。

UCS へのリンクを vPC または従来のポート チャネルとして設定するプロセスの詳細については、「ファブリックへの新しいデバイスの追加」の項を参照してください。

スタンドアロン ラック マウント サーバまたはシスコ以外のサーバ

UCS 以外のサーバ アーキテクチャも、ACI ファブリックや Cisco Nexus 2000 ファブリック エクステンダ（FEX）に直接接続できます。ACI ファブリックに接続する場合は、サーバ リンクからの予想されるトラフィックのタイプを調べる必要があります。ワークロードがベアメタル サーバである場合は、トラフィックをポート単位で分類し、タグありまたはタグなしのトラフィックと一致するように、関連する AEP と EPG を適切にマッピングできます。サポートされているハイパーバイザ—を使用する場合は、Virtual Machine Manager（VMM）ドメインを適切に設定し、EPG と AEP のマッピングを介したハイパーバイザとして、ファブリックの対応するポートに関連付ける必要があります。重要なことは、予想されるトラフィックの分類をサーバ インフラストラクチャに接続しているポートにマッピングすることです。

FEX の使用は、ACI ファブリックにホストデバイスを接続する別の方法です。非ホスト側ポートはサポート対象外という、NX-OSモードに関する制限は引き続き有効です。ポートはホストにのみ接続する必要があり、他のネットワーク デバイスへの接続は正常に動作しません。FEX を使用すると、すべてのホスト側ポートは、ACI ファブリックに直接接続しているかのように扱われます。

仮想マシン ネットワーキング

ACI の VM ネットワーキングの概要

シスコ アプリケーション セントリック インフラストラクチ（ACI）の最も一般的な使用方法の 1 つは、仮想環境でのアプリケーションの管理と展開を支援することです。ACI を使用すると、同じポリシーセットで仮想と物理の両方のエンドポイントを管理できます。この章では、日常の運用において実行されるさまざまな操作タスクについて説明します。

次のリストは、Virtual Machine Manager（VMM）システムの用語を示しています。

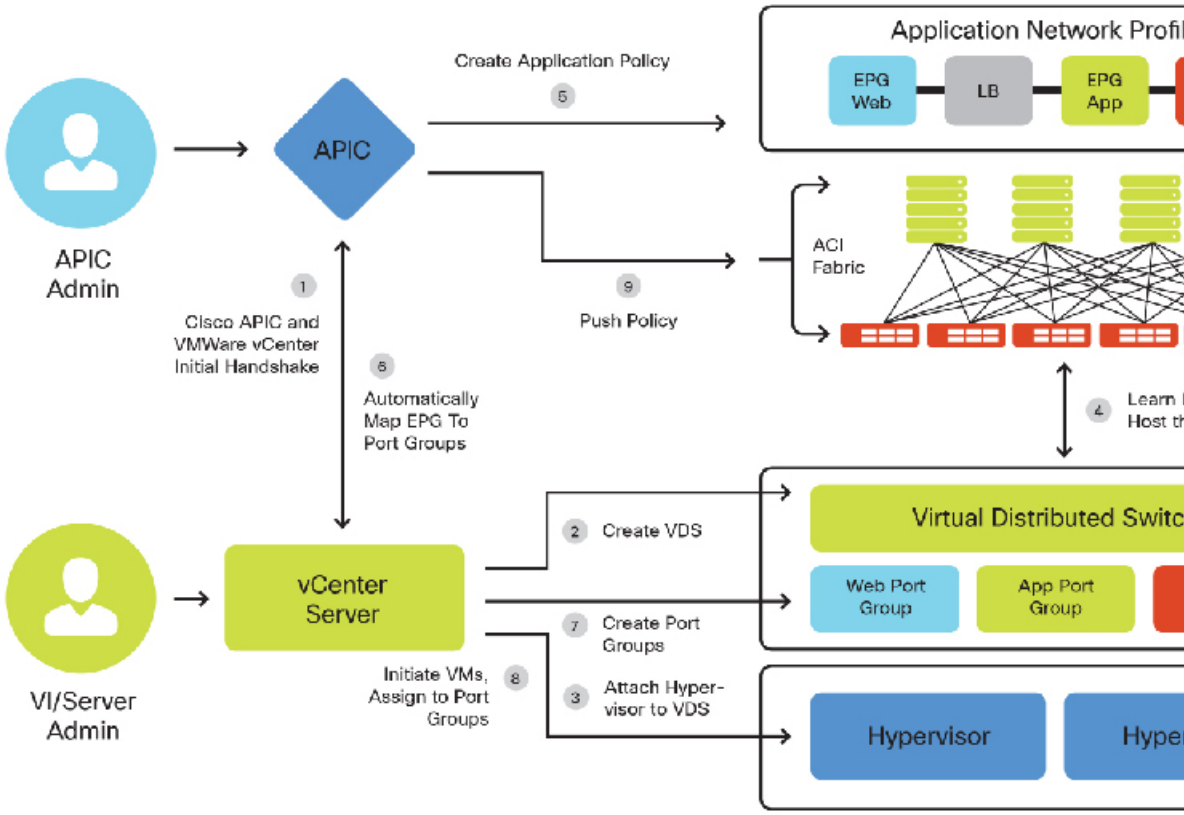
- 仮想マシン コントローラは外部 VMM エンティティです。たとえば、VMware vCenter、VMware vShield、Microsoft Systems Center Virtual Machine Manager（SCVMM）などが該当します。Application Policy Infrastructure Controller（APIC）は、VMM と通信し、仮想ワークロードに適用されるネットワーク ポリシーを公開します。仮想マシン コントローラの管理者は、APIC 管理者に仮想マシン コントローラの認証クレデンシャルを提供します。同じタイプの複数のコントローラが同じクレデンシャルを使用できます。
- クレデンシャルとは、仮想マシン コントローラと通信するための認証情報を指しています。複数のコントローラが同じクレデンシャルを使用できます。
- プールは、VLAN、VXLAN ID、マルチキャスト アドレスなどの、トラフィックのカプセル化 ID の範囲を表します。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。重複 VLAN プールのそれぞれを、同じ接続可能エンティティ プロファイル（AEP）に関連付けることはできません。
- VLAN ベースのポートには、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。VMware 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。これは、VMM 統合に必要なプール タイプです。
- スタティック プール：EPG はドメインと関係があり、ドメインはプールと関係があります。プールには、さまざまなカプセル化された VLAN および VXLAN が含まれます。スタティック EPG 導入環境の場合、ユーザはインターフェイスとカプセル化を定義します。カプセル化は、EPG が関連付けられているドメインに関連付けられたプールの範囲内である必要があります。

VMM 統合のダイナミック VLAN プールを作成する場合は、中間デバイス（従来のスイッチやブレードスイッチなど）で VLAN 範囲を作成する必要があります。これには、Unified Computing System（UCS）での VLAN の作成が含まれます。

ACI VM 統合のワーク フロー

図 *17 : ACI VM* 統合のワーク フロー



Application Policy Infrastructure Controller (APIC)Application Policy Infrastructure Controller (APIC) による VMware vSphere Distributed Virtual Switch の展開方法については、『*Cisco APIC Getting Started Guide*』を参照してください。

Microsoft SCVMM と Cisco Application Centric Infrastructure (ACI) を統合をイネーブルにする方法の詳細とワークフローについては、『*Cisco ACI with Microsoft SCVMM Workflow*』を参照してください。

VMware の統合

Cisco Application Centric Infrastructure (ACI) を VMware インフラストラクチャに統合する場合は、ネットワークの展開に対して 2 つのオプションがあります。VMware ドメインは、VMware vSphere Distributed Virtual Switch（DVS）または Cisco Application Virtual Switch（AVS）を利用して展開できます。どちらも同様の基本的な仮想ネットワーク機能を備えていますが、AVS には、VXLAN やマイクロセグメントのサポートなど、特別な機能が追加されています。ACME 社は AVS の特別機能を活用することにしました。VMware の標準 DVS を使用することに関心がある組織の方は、次のドキュメント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/getting-started/video/cisco_apic_create_vcenter_domain_profile_using_gui.html

ACI 1.2 リリースは vCenter 6.0 および DVS のみに対する次の機能をサポートします。

- データセンターでの DVS 間の vMotion
- 同じ vCenter 内のデータセンター間の vMotion
- vCenter 間の vMotion
- vSphere 5.1 および 5.5 を使用した vSphere 6.0 への ACI 展開のアップグレード
- vSphere 6.0 での vShield 5.5
- vSphere 6.0 での NSX Manager 6.1

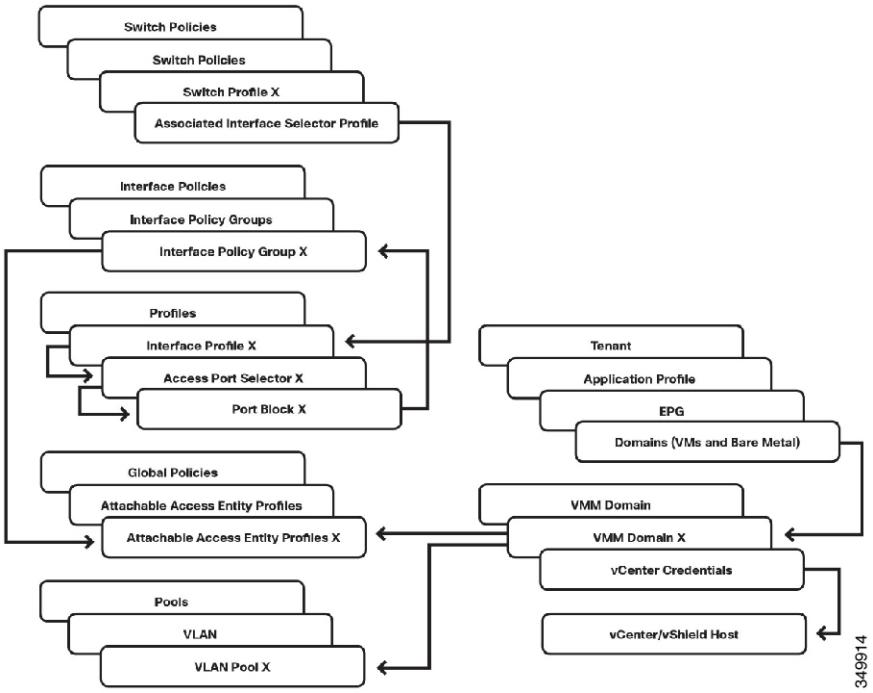
次の機能はサポートされていません。

- 長距離 vMotion

VMM ポリシー モデルの連携

下記は、VM 統合の設定に関連するさまざまな ACI ポリシーの一部を示しています。これは、さまざまなポリシーを相互に関連付ける上で参考になります。

図 *18 : VMM* ポリシー モデルの連携



VMM ドメインへの EPGS のパブリッシュ

ここでは、Virtual Machine Manager（VMM）ドメインに既存のエンドポイント グループ（EPG）をパブリッシュする方法について説明します。EPG の作成方法の詳細については、「テナント」の項を参照してください。

VMM ドメインに EPG をプッシュする場合は、テナントの EPG 内でドメインのバインディングを作成する必要があります。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. [Navigation] ペインで、 ***Tenant_Name*** **> Application Profiles >** ***Application_Profile_Name*** **> Application EPGs >** ***Application_EPG_Name*** **> Domains (VMs and Bare-Metals)** の順に選択します。
4. [Work] ペインで、[Actions] > [Add VM Domain Association] の順に選択します。
5. [Add VM Domain Association] ダイアログボックスで、前に作成した VMM ドメイン プロファイルを選択します。
    1. [Deployment and Resolution Immediacy] に対しては、デフォルトの [On Demand] オプションを使用することをお勧めます。これによって、この EPG に割り当てられたエンドポイントを接続するときに、リーフ ノードにポリシーを展開するだけで、ファブリックで最適なリソース使用を実現できます。このデフォルトを選択したままにしておくと、通信の遅延やトラフィック損失が発生しません。

6. [Submit] をクリックします。` これで、VMM のポート グループとして EPG を 使用できます。

vCenter のエンドポイント グループ ポート グループへの仮想マシンの接続

1. VI クライアントを使用して vCenter に接続します。
2. [Host and Clusters] ビューで、仮想マシンを右クリックし、[Edit Settings] を選択します。
3. [Network Adapter] をクリックし、[Network Connection] ドロップダウン ボックスで EPG に対応するポート グループを選択します。データは次の形式で表示されます。**[*TENANT* | *APPLICATION_PROFILE* | *EPG* | *VMM_DOMAIN_PROFILE*]**

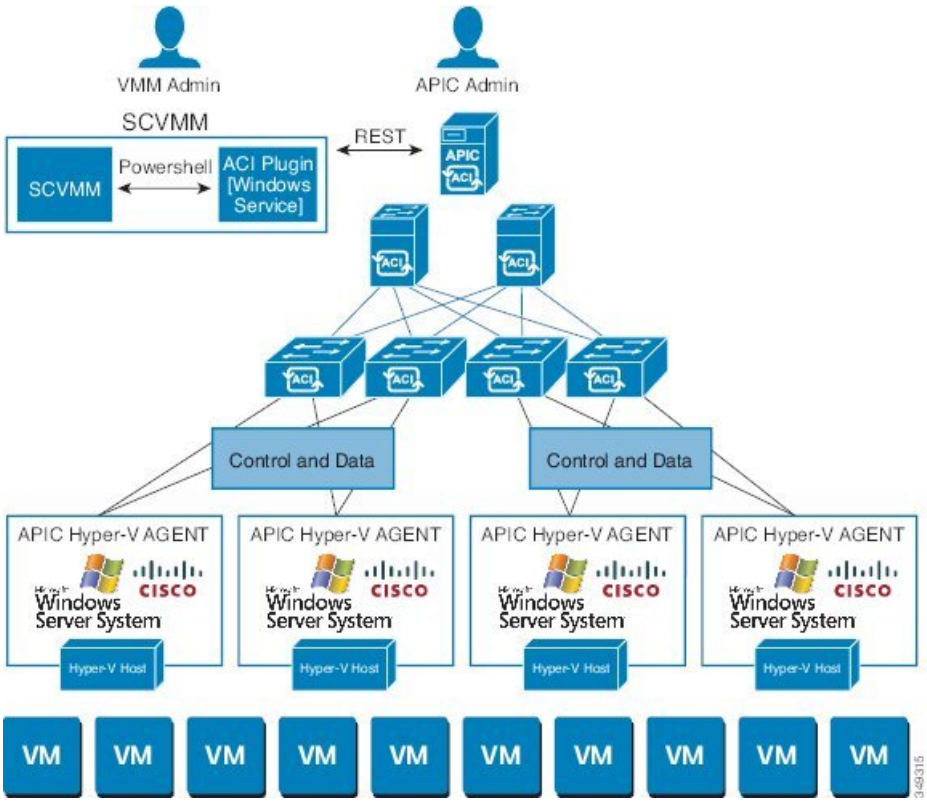
[Network Connection] リストに自分の Cisco Application Centric Infrastructure (ACI) EPG が表示されない場合は、次のいずれかを意味しています。

- Application Policy Infrastructure Controller (APIC) が管理する分散スイッチに接続されていないホストで、VM が実行されています。
- APIC と vCenter 間で、OOB または INB 管理ネットワークを介しての通信に問題がある可能性があります。

Microsoft SCVMM の統合

次の図は、Cisco Application Centric Infrastructure (ACI) との System Center Virtual Machine Manager（SCVMM）導入の典型的なトポロジを示しています。SCVMM 仮想マシンと Application Policy Infrastructure Controller (APIC) 間の Hyper-V クラスタリング接続を管理ネットワークで実行することができます。

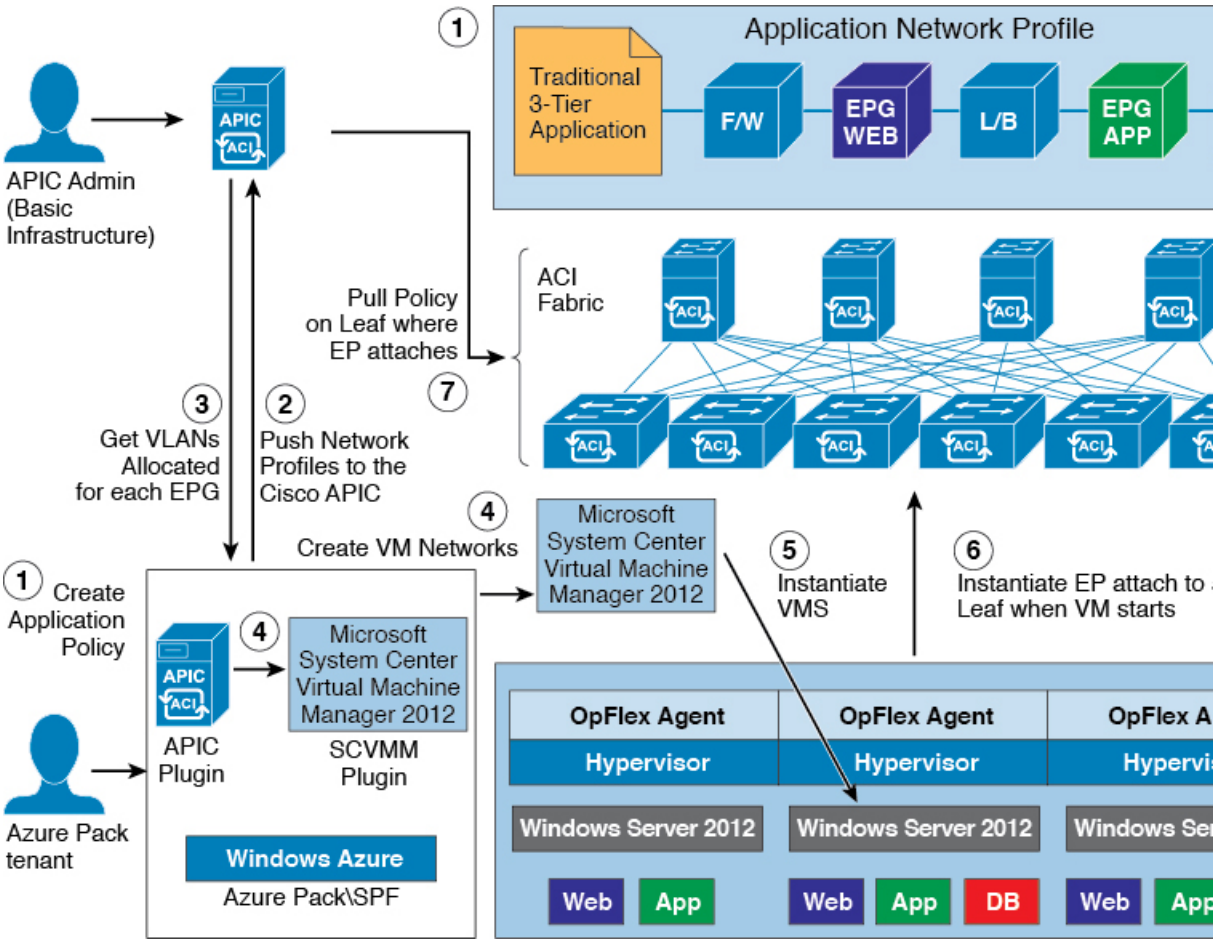
図 *19* : 次の *SCVMM* 導入のトポロジ *ACI*



ACI SCVMM のワークフロー

次の図に、Microsoft SCVMM と Cisco Application Centric Infrastructure (ACI) とを統合するためのワークフローを示します。

図 *20 : ACI SCVMM* のワークフロー

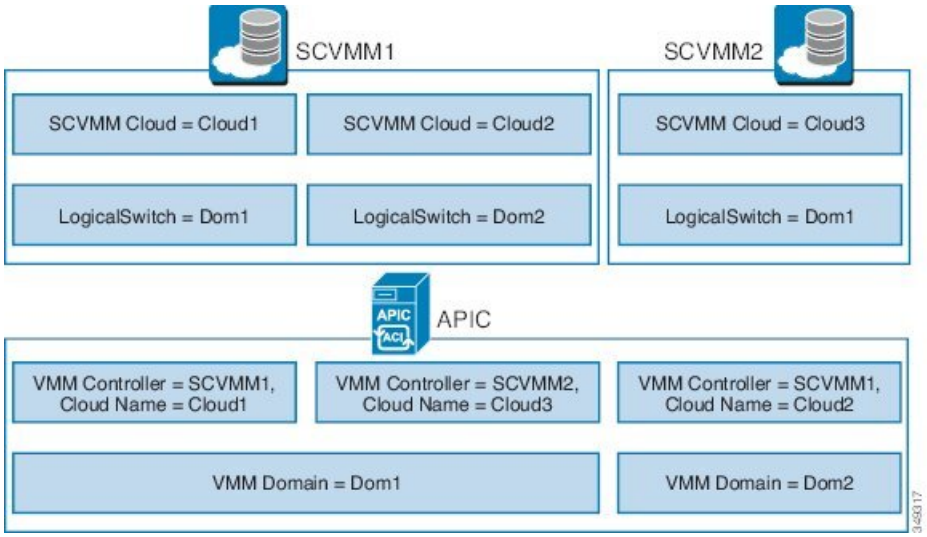


Microsoft SCVMM と ACI の統合のワークフローの詳細については、『*Cisco ACI with Microsoft SCVMM Workflow*』を参照してください。

ACI および SCVMM コントラクトのマッピング

次の図に、Cisco Application Centric Infrastructure (ACI) および SCVMM コントラクト（SCVMM コントローラ、クラウド、論理スイッチ）のマッピングを示します。

図 *21 : ACI* および *SCVMM* コンストラクト



1 つの VMM ドメインを、同じ SCVMM に複数回マッピングすることはできません。Application Policy Infrastructure Controller (APIC) コントローラは、最大 5 つの SCVMM コントローラに関連付けることができます。その他の制限の詳細については、『*Verified Scalability Guide for Cisco ACI*』 を参照してください。

APIC コントローラへの複数の SCVMM のマッピング

複数の SCVMM が Application Policy Infrastructure Controller (APIC) コントローラに関連付けられている場合、必要に応じて、第 1 の SCVMM のコントローラの Opflex 証明書を第 2 のコントローラやその他のコントローラにコピーする必要があります。ローカル SCVMM コントローラで **certlm.msc** コマンドを使用して、証明書を次の場所にインポートします。

```
Certificates - Local Computer > Personal > Certificates
```

この SCVMM コントローラが管理する Hyper-V サーバ上に同一の Opflex 証明書が導入されます。Hyper-V サーバに証明書をインストールするには、**mmc** コマンドを使用します。

OpFlex 証明書が SCVMM から APIC への接続のために展開されていることの確認

OpFlex 証明書が SCVMM から Application Policy Infrastructure Controller (APIC) への接続に対して展開されていることを、`C:\Program Files (x86)\ApicVMMService\Logs\` ディレクトリにある、`Cisco_APIC_SCVMM_Service` ログ ファイルを表示することで確認できます。ファイルでは、次のことを確認してください。

- 正しい証明書が使用されている
- 次へのログインに成功しました. APIC

次のサンプル ログ ファイルは、これらを示しています。

```
2/22/2016 1:14:07 PM-1044-13||UpdateCredentials|| AdminSettingsController:
UpdateCredentials.
2/22/2016 1:14:07 PM-1044-13||UpdateCredentials|| new: EndpointAddress:
Called_from_SCVMMM_PS,
```

```
  Username ApicAddresses 192.168.1.47;192.168.1.48;192.168.1.49 CertName: OpflexAgent
2/22/2016 1:14:07 PM-1044-13||UpdateCredentials|| ########
2/22/2016 1:14:07 PM-1044-13||UpdateCredentials|| oldreg_apicAddresses is
2/22/2016 1:14:07 PM-1044-13||UpdateCredentials|| Verifying APIC address 192.168.1.47
2/22/2016 1:14:07 PM-1044-13||GetInfoFromApic|| Querying URL
https://192.168.1.47/api/node/class/infraWiNode.xml
2/22/2016 1:14:07 PM-1044-13||GetInfoFromApic|| HostAddr 192.168.1.47
2/22/2016 1:14:07 PM-1044-13||PopulateCertsAndCookies|| URL:/api/node/class/infraWiNode.xml
2/22/2016 1:14:07 PM-1044-13||PopulateCertsAndCookies|| Searching Cached Store Name: My
2/22/2016 1:14:07 PM-1044-13||PopulateCertsAndCookies|| Using Certificate CN=OpflexAgent,
 C=USA, S=CA, O=TS,
  E=sj_aci_sol@lab.local in Cached Store Name:My
2/22/2016 1:14:07 PM-1044-13||PopulateCertsAndCookies|| Using the following CertDN:
  uni/userext/user-admin/usercert-OpFlexAgent
2/22/2016 1:14:07 PM-1044-13||GetInfoFromApic|| IFC returned OK to deployment query
2/22/2016 1:14:07 PM-1044-13||GetInfoFromApic|| Successfully deserialize deployment query
 response
2/22/2016 1:14:07 PM-1044-13||UpdateCredentials|| ApicClient.Login(addr 192.168.1.47)
Success.
```

APIC から SCVMM への VMM の展開の確認

C:\Program Files (x86)\ApicHyperAgent\Logs ディレクトリにあるログ ファイルを表示することで、OpFlex 証明書が Hyper-V サーバに展開されたことを確認できます。ファイルでは、次のことを確認してください。

- 正しい証明書が使用されている。
- ファブリック リーフで Hyper-V サーバとの接続が確立されている。

SCVMM では、次のことを確認してください。

- **[ファブリック（Fabric）] > [論理スイッチ（Logical Switches）]** の下で、SCVMM から「apicVswitch_VMMdomainName」が Application Policy Infrastructure Controller (APIC) から SCVMM に展開されていることを確認します。
- **[Fabric] > [Logical Networks]** の下で、「apicLogicalNetwork_VMMdomainName」が APICconrefAPICから SCVMM に展開されていることを確認します。
- **[Fabric] > [Port Profiles]** の下で、「apicUplinkPortProfile_VMMdomainName」が展開されていることを確認します。そうでない場合、[Servers]の下のホストに移動し、ホストを右クリックして [Properties] を選択します。[Virtual Switches] に移動し、物理アダプタが仮想スイッチに接続されていることを確認します。
- VTEP 仮想ネットワーク アダプタが、仮想スイッチに追加され、IP アドレスが VTEP のアダプタに割り当てられます。

（注） APIC GUI では、SCVMM の最初の 3 つの箇条書き項目が満たされるまで、Hyper-V サーバと仮想マシンは、Microsoft SCVMM のインベントリの下に表示されません。

VMM 展開を確認するためのその他のトラブルシューティングのヒント

- APIC_SCVMM_Service エージェントおよび APIC_Hyper-V エージェントのログは、それぞれ、C:\Program Files(x86)\ApicVMMService および C:\Program Files(x86)\ApicHypervAgent ディレクトリにあります。
- これらのサービスに対するサポート スクリプトがあります。サポート スクリプトをデバッグ モードで実行し、それぞれ SCVMM コントローラまたは Hyper-V サーバのサービス ステータスおよび設定をより詳細に把握することができます。

  サポート スクリプトを使用するには、次の手順を実行します。

  1. スクリプトを右クリックします。
  2. [Edit] を選択します。[Power Shell ISE] ウィンドウが開きます。
  3. 上部のバーにある [Debug] をクリックして、スクリプトを実行します。
  4. 問題に対するスクリプトの出力を確認します。

仮想エンドポイント ラーニングの確認

VM を適切なポート グループ/EPG に接続したら、APIC が仮想エンドポイントを学習したことを確認する必要があります。

APIC の VM エンドポイント ラーニングの GUI による確認

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Application Profiles] > [Application_Profile_Name] > [Application EPGs] > [Application_EPG_Name] の順に選択します。
4. [Work] ペインで、[Operational] タブをクリックします。**注**：現在のタブにクライアント エンドポイントが表示されます。すべてのエンドポイント（仮想または物理）が表示されます。ここで、[Learning Source] カラムをフィルタリングして、値「Learned VMM」を持つ行を表示すると、自分の仮想マシンを見つけることができます。

APIC の VM エンドポイント ラーニングの CLI による確認

「moquery」（管理対象オブジェクト クエリー）コマンドを使用し、2 つのフィルタを追加することで、CLI から上記と同じ情報を確認できます。1 つは EPG の識別名（DN）用、もう 1 つは「fvCEp」（ファブリック ベクトル クライアント エンドポイント）のクラス名用です。

```
moquery -c fvCEp --dn uni/tn-<TENANT_NAME>/ap-<APP_PROFILE_NAME>/epg-<EPG_NAME>
```

GUI で EPG を右クリックし、[Save As] を選択して XML オブジェクトを表示することで、EPG の DN を確認できます。このファイルで、特定の EPG の DN エントリを調べます。

```
<imdata totalCount="1"><fvAEPg uid="15374" triggerSt="triggerable" status=""
scope="2588672" prio="unspecified" pcTag="49159" name="epg-od"
monPolDn="uni/tn-common/monepg-default" modTs="2015-02-06T06:46:24.729+11:00"
```

```
matchT="AtleastOne" lcOwn="local" dn="uni/tn-mb-tennant1/ap-mb-app-pro/epg-epg-od"
descr="" configSt="applied" configIssues="" childAction=""/></imdata>
```

次に、この DN を moquery コマンドで使用すると、EPG のクライアント エンドポイントのリストが返されます。

```
admin@apic1:~> moquery -c fvCEp --dn uni/tn-mb-tennant1/ap-mb-app-pro/epg-epg-od
Total Objects shown: 1
# fv.CEp
name : 00:50:56:BB:8C:6A
childAction :
dn : uni/tn-mb-tennant1/ap-mb-app-pro/epg-epg-od/cep-00:50:56:BB:8C:6A
encap : vlan-211
id : 0
idepdn :
ip : 10.10.10.10
lcC : learned,vmm
lcOwn : local
mac : 00:50:56:BB:8C:6A
mcastAddr : not-applicable
modTs : 2015-02-06T06:48:52.229+11:00
rn : cep-00:50:56:BB:8C:6A
status :
uid : 0
uuid :
```

VMware 統合の使用例

ACME の VMware 管理者は、VLAN セットを ESX ホストにトランキングして、DVS スイッチへの接続を確保することをネットワーク チームに依頼しました。ネットワーク チームは、サーバごとに VLAN をトランキングするのではなく、より俊敏な新しい方法を利用すること、必要な時と場所に応じたリソースのオンデマンド プロビジョニングを活用すること、および、ACI ファブリック内の全 VM ホストに無制限のレイヤ 2 モビリティを提供することを決めました。

これを実行するために、ネットワーク管理者は VMware 管理者と協力し、APIC によって ESX ホストに動的に提供する VLAN の範囲を決定しました。また、未使用の VLAN 範囲（600 ～ 800）も決定しました。これは、ダイナミック VLAN プールです。範囲を決定した後、APIC 管理者は、APIC に vCenter クレデンシャルを許可して、APIC GUI で VMM 統合を設定します。APIC はすべての EPG を動的にプロビジョニングして、ポート グループとして ESX ホストで使用できるようにします。

注：APIC は VMNIC をポート グループに自動的に移動しません。これにより、VMware 管理者は、仮想 NIC を制御してポート グループにオンデマンドで移動きるようになります。

VMware 管理者が ESX ホストをプロビジョニングして、VM に適したポート グループを選択すると、APIC は vCenter と動的に通信して、ポート グループから EPG を使用できるようにします。また、APIC は、必要に応じて、リーフ スイッチに VLAN ID を設定します。

vMotion イベント中、APIC は、VM の移動について自動通知を受けると、エンドポイント トラッキング テーブルを更新してシームレスに通信できるようにします。VM は、vCenter による制限以外の制限を受けることなく、ACI ファブリック内の任意の個所に移動できます。

重要な点は、ACME は、引き続き、ポート単位で EPG を静的にプロビジョニングして、VMware DVS スイッチに従来の VLAN トランキングを展開することを選択可能であり、柔軟なレイヤ 2 ACI ファブリックのメリットを享受できることです。しかし、ACME は最適な展開モデルと

して VMM 統合を選択しました。VMM 統合は、組織の課題の克服、オンデマンドのリソース割り当て、および仮想と物理の両環境における可視化とテレメトリの向上を実現する最も効果的な方法であるからです。

アプリケーション仮想スイッチの展開

Cisco Application Virtual Switch の展開に関する前提条件

- すべてのスイッチ ノードがファブリックによって検出されている。
- INB または OOB 管理接続が設定されている。
- VMware vCenter がインストール済みで設定されており、使用可能である。
- 1 つ以上の vSphere ホストを AVS への展開に使用できる。
- （任意）DNS サーバ ポリシーが設定されており、ホスト名を使用して VMM に接続できる。
- ダイナミック VLAN プールが作成済みで十分な VLAN ID を備えており、各 VMM ドメインへの展開を計画している EPG ごとに 1 つの VLAN を収容できる。

使用する前に

AVS ソフトウェアは、APIC ソフトウェア バージョンから独立して動作するように設計されています。これにより、デバイスを個別にアップグレードできます。常に AVS リリース ノートを参照して、特別な考慮事項があるかどうかを確認してください。

他のソフトウェアと同様、AVS の新バージョンのリリースには新しい機能と機能強化が含まれています。最初にリリースされた AVS ソフトウェア バージョン 4.2.1 の後にバージョン 5.2.1 がリリースされました。『*ACI Ecosystem Compatibility List* 』マニュアルを参照して、必要な AVS のバージョンが、実行されている APIC および vSphere のバージョンと互換性があることを確認してください。

どちらのバージョンの AVS パッケージにも、vSphere Installation Bundle （VIB）が含まれています。AVS ソフトウェアの各バージョンには、すべてのサポートされている vSphere バージョン用の VIB ファイルが含まれています。本書の発行時点では、vSphere バージョン 5.1 と 5.5 に対応する 2 つの VIB があります（vSphere 5.0 はサポートされていません）。これらは、次の場所の CCO からダウンロードできます。

[Downloads Home] > [Products] > [Switches] > [Virtual Networking] > [Application Virtual Switch]

```
AVS 4.2.1 Bundle
cross_cisco-vem-v165-4.2.1.2.2.3.0-3.1.1.vib  5.1 VIB
cross_cisco-vem-v165-4.2.1.2.2.3.0-3.2.1.vib  5.5 VIB

AVS 5.2.1 Bundle
cross_cisco-vem-v172-5.2.1.3.1.3.0-3.1.1.vib
cross_cisco-vem-v172-5.2.1.3.1.3.0-3.2.1.vib
```

AVS VIB のインストール

APIC で AVS を設定する前に、仮想イーサネット モジュール（VEM）と呼ばれる AVS ソフトウェアを vSphere にインストールする必要があります。これはさまざまな方法で実行でき、すべての方法が『*Cisco Application Virtual Switch Installation Guide*』で説明されています。ホストが少数の場合は、この作業を手動で簡単に実行できますが、10+ホストの場合は、Virtual Switch Update Manager（VSUM）を利用するとインストール プロセスを自動化できるので、より簡単に実行できます。

手動インストール

1. ホストを [Maintenance] モードにします。
2. ホストに VIB ファイルをコピーします。ホストに VIB をコピーする最も簡単な方法は、[Host] > [Configuration] > [Storage] > [Datastore_X] に移動し、VMware VI クライアントを利用することです。目的のデータストアを右クリックし、[Browse Datastore] を選択します。ここから、ホストのデータストアに VIB を直接アップロードできます。
3. AVS VIB をインストールする vSphere ホストに SSH 接続します。SSH が有効でない場合は、**[Host Configuration]** > **[Security Profile]** > **[SSH]** で有効化できます。
4. **esxcli** コマンドを使用して、VIB をインストールまたはアップグレードします。

   AVS VIB をインストールする場合：

   ```
   esxcli software vib install -v /<path>/<vibname> --maintenance-mode --no-sig-check
   ```

   既存の AVS VIB をアップグレードする場合：

   ```
   esxcli software vib update -v /<path>/<vibname> --maintenance-mode --no-sig-check
   ```

   出力例は次のとおりです。

   ```
   # esxcli software vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v172-
   5.2.1.3.1.3.0-3.2 .1.vib --maintenance-mode --no-sig-check
   Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: Cisco_bootbank_cisco-vem-v172-5.2.1.3.1.3.0-3.2.1
   VIBs Removed:
   VIBs Skipped:
   /vmfs/volumes/53cab6da-55209af3-0ef2-24e9b391de3e # vem version
   Running esx version -1623387 x86_64
   VEM Version: 5.2.1.3.1.3.0-3.2.1
   VSM Version:
   System Version: VMware ESXi 5.5.0 Releasebuild-1623387
   ```

5. VEM がロードされ、実行されていることを確認します。

   ```
   # vem status
   VEM modules are loaded
   Switch Name   Num Ports   Used Ports   Configured Ports   MTU   Uplinks
   vSwitch0      3072        6            128                1500  VMNIC0
   VEM Agent (vemdpa) is running
   ```

接続可能アクセス エンティティ プロファイル（AEP）と AVS

AVS で使用される重要なコンポーネントの 1 つとして、接続可能エンティティ プロファイル（AEP）があげられます。既存の AEP を使用するか、新しい AEP を作成するかに関係なく、AEP ポリシーに対して [Enable Infrastructure VLAN] チェックボックスをオンにする必要があります。これによって、対象トラフィック（DHCP 要求/オファーなど）またはデータ パケットがインフラストラクチャ VLAN から AVS に確実に流れるようになります。AEP は、ホスト側インターフェイスで許可する VLAN を定義します。ドメインがエンドポイント グループにマップされると、AEP では、VLAN が特定のインターフェイスに導入可能なことを確認します。「VM ネットワーキングの概要」の章の「VMM ポリシー モデルの連携」の図に戻って説明すると、AEP とは vSphere ホストが接続されている物理インターフェイスに VMM ドメインを結び付けるものです。AEP は VMM ドメインの作成時にオンザフライで作成できますが、本書では、まず AEP を個別に作成する方法について説明します。

新しい AEP の作成

1. メニュー バーで、[Fabric] > [Access Policies] を選択します。
2. [Navigation] ペインで、[Global Policies] > [Attachable Access Entity Profile] の順に選択します。
3. [Work] ペインで、[Actions] > [Create Attachable Access Entity Profile] の順に選択します。
4. [Create Attachable Access Entity Profile] ダイアログボックスで、次の操作を実行します。
    1. AEP ウィザードに情報を入力し、[Next] をクリックします。
        1. Name：AEP を識別する名前を入力します（「AVS-AEP」など）。
        2. Enable Infrastructure VLAN：このチェックボックスをオンにします。
        3. Domains (VMs or Baremetal)：空白のままにします。これについては、後ほど「***VMM* ドメインへの *EPG* のパブリッシュ**」の章で説明します。
    2. ウィザードの次のページで、AEP に関連付ける [Interface Policy Group] を選択します。この手順では、インターフェイス ポリシー グループが作成済みであることを前提としています。目的のインターフェイス ポリシー グループの [All Interfaces] オプション ボタンをクリックします。

（注） インターフェイス ポリシー グループの作成は、本書の他の項で説明されています。基本的に、インターフェイス ポリシー グループは、インターフェイス セレクタとプロパティ（速度/ネゴシエーション、LLDP、CDP など）を定義するインターフェイス ポリシーの集合です。インターフェイス ポリシー グループとインターフェイス プロファイルの作成の詳細については、「ファブリックへの新しいデバイスの追加」の章を参照してください。

既存の AEP の変更

1. メニュー バーで、[Fabric] > [Access Policies] を選択します。
2. [Navigation] ペインで、[Global Policies] > [Attachable Access Entity Profile] の順に選択します。
    1. ナビゲーション ウィンドウで、既存の AEP を選択します。
    2. [Work] ペインで、[Enable Infrastructure VLAN] チェックボックスをオンにします。

注：この章の前半で説明したように、OpenFlex 制御チャネルを使用して AVS からファブリックと通信するために、インフラストラクチャ VLAN が必要です。

vCenter の VMM ドメイン

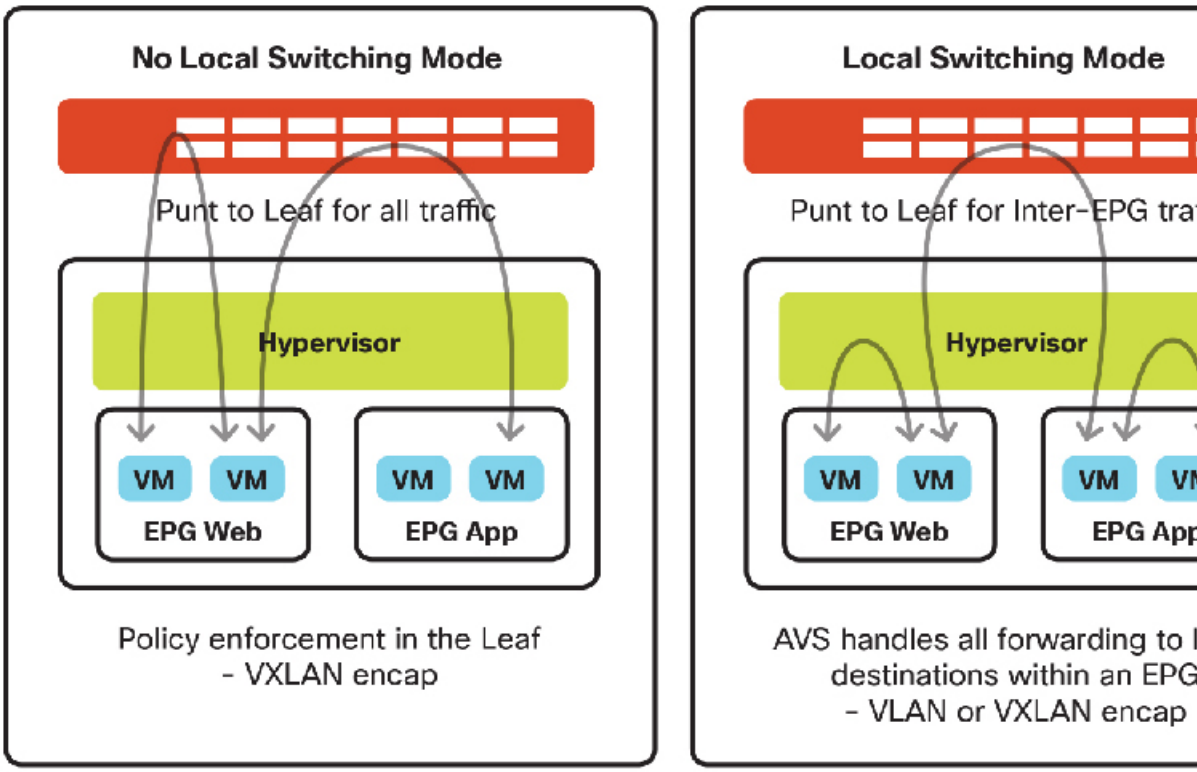
Virtual Machine Manager（VMM）ドメインは、ACI に統合する仮想インフラストラクチャを定義します。これにより、物理エンドポイントに適用するのと同じポリシーを仮想エンドポイントに適用できます。vCenter VMM ドメインは VMware DVS または Cisco AVS を使用して作成されます。一方から他方を変更することはできません。新しい VMM ドメインは AVS 導入をサポートするために一から作成されます。

AVS スイッチング モード

AVS は次のスイッチング モードで実行できます。

- Local Switching：VXLAN カプセル化または VLAN カプセル化をサポートします。
    - このスイッチング モードでは、EPG 間のトラフィックを AVS にローカルに切り替えることができます。
- No Local Switch：VLAN カプセル化のみをサポートします。
    - このスイッチング モードは、すべてのトラフィック（EPG 間トラフィックを含む）をリーフ スイッチに送信します。

図 *22 : AVS* スイッチング モード : ローカル スイッチなしとローカル スイッチング モード



使用するカプセル化（VLAN または VXLAN）の決定には、ファブリック外部の別の VLAN 拡張要件が必要です。VXLAN カプセル化を使用する場合は、インフラストラクチャ VLAN のみを AVS ホストに拡張する必要があります。AVS アップリンクと ACI ファブリック間のすべてのトラフィックは、VXLAN によりカプセル化され、インフラストラクチャ VLAN を使用して転送されます。

VLAN カプセル化を使用する場合は、VM ドメインの VLAN プール内のすべての VLAN をファブリックと AVS ホスト間に拡張する必要があります。これには、中間デバイス（UCS、AVS vSphere ホスト用の vNIC など）における VLAN の作成などが含まれます。

AVS の VMM ドメインの作成

これまでに、DHCP サーバポリシーを作成し、AEP を作成または変更しました。この時点で、AVS の VMM ドメインを作成できます。

1. メニュー バーで、[VM NETWORKING] を選択します。
2. [Navigation] ペインで、[Policies] タブを選択します。
3. [Work] ペインで、[Actions] > [Create VCenter Domain] の順に選択します。
4. [Create vCenter Domain] ダイアログボックスで、次の操作を実行します。

1. Name：この値は、vCenter で表示される AVS の「スイッチ名」として使用されます。
2. Virtual Switch：Cisco AVS
3. **Switching Preference**：**[Local Switching] または [No Local Switching] を選択します。**
   - [No Local Switching] モードの場合：
     - Multicast Address：AVS を表すマルチキャスト アドレスを割り当てます。
     - Multicast Address Pool：各 AVS vSphere ホストを収容できる十分な大きさのマルチキャスト アドレス プールを作成します。
   - [Local Switching] モードの場合：
     - Encapsulation：設定に基づいて [VLAN] または [VXLAN] を選択します。
       - [VLAN] カプセル化の場合：
         - VLAN Pool：VLAN プールを選択または作成します。
       - [VXLAN] カプセル化の場合：
         - Multicast Address：AVS を表すマルチキャスト アドレスを割り当てます。
         - Multicast Address Pool：各 AVS vSphere ホストを収容できる十分な大きさのマルチキャスト アドレス プールを作成します。
4. Attachable Access Entity Profile ：前に作成/変更した AEP を選択します。
5. vCenter Credentials：vCenter に対する管理者権限/ルート アクセス権限があるクレデンシャルを作成します。
6. vCenter ：vCenter の詳細を追加します。
   - Name：この vCenter のわかりやすい名前。
   - Hostname/IP Address：vCenter の DNS または IP アドレス。
   - DVS Version：vCenter のデフォルト。
   - Datacenter：vCenter で表示する正確なデータセンター名を入力します。
   - Management EPG：管理 EPG への OOB または INB を設定します。
   - Associated Credentials：前に作成したクレデンシャル設定を選択します。
   - [OK] をクリックし、vCenter の作成を完了します。
5. [送信（Submit）] をクリックします。

vCenter 上の AVS 展開の確認

1. vCenter クライアントで、[HOME] > [INVENTORY] > [NETWORKING] の順に移動し、新しい Distributed Virtual Switch フォルダが作成されたことを確認します。
2. このフォルダを展開し、AVS と、**uplink** および **vtep** を含むいくつかのデフォルトのポート グループを検索します。

AVS への vSphere ホストの追加

vCenter で AVS が作成されたら、それにホストを接続する必要があります。これを実行するには、少なくとも 1 つの未使用の物理インターフェイス（VMNIC）を各ホストのアップリンクとして動作させる必要があります。AVS アップリンクは 既存の vSwitch や vDS で共有できません。

1. vCenter クライアントで、[Home] > [Inventory] > [Networking] の順に移動します。
2. 新しく作成された（フォルダでなく）AVS スイッチを右クリックし、**[Add Host]** を選択します。.
3. [Add Host] ダイアログボックスで、vSphere ホストを選択して AVS に追加し、割り当てられていない VMNIC アップリンクを選択します。
4. ウィザードが完了するまで [Next] をクリックし、現時点では、仮想アダプタまたは仮想マシン ネットワーキングの移行をスキップします。

   注：UCS などのブレード スイッチ システムの場合は、使用する VMNIC インターフェイスに使用可能な必須 VLAN がすべて含まれている必要があります。UCS の条件として、サービス プロファイル内の vNIC にすべての関連 VLAN が含まれ、それらがアクティブになっている必要があります。
5. vCenter内の分散スイッチ上に作成され、「vtep」ポート グループに割り当てられた新しい vmk インターフェイスが表示されます。この VMK が、仮想トンネル エンドポイント（VTEP）インターフェイスとなります。VTEP は、TEP サブネットの APIC から DHCP アドレスを取得しているはずです。下記のスクリーンショットに示すように、VMkernel ポートは APIC から IP アドレスを受信済みです。APIC は、APIC のセットアップ時に作成されたのと同じ 10.0.0.0/16 プ ールを使用して、IPアドレスをプロビジョニングします。これは、AVS と APIC 間の Opflex 通信の準備ができていることを示しています。

```
~ # esxcfg-VMKNIC -l
 Interface  Port Group/DVPort   IP Family  IP Address     Netmask        Broadcast
 vmk0       Management Network  IPv4       172.16.176.54  255.255.255.0  172.16.176.255

 vmk1       vmotion             IPv4       192.168.99.54  255.255.255.0  192.168.99.255

 vmk2       9                   IPv4       10.0.16.95     255.255.0.0    10.0.255.255


 MAC Address       MTU   TSO MSS  Enabled Type
 00:25:b5:00:00:29 1500  65535    true    STATIC
 00:50:56:61:1c:92 1500  65535    true    STATIC
 00:50:56:65:3d:b3 1500  65535    true    DHCP
```

ESX 上の AVS の確認

ESX のコマンドラインで、「**vemcmd show openflex**」コマンドを実行します。

「**status: 12 (Active)**」と表示されること、およびスイッチング モードであることを確認します。また、GIPO アドレスが、VMM ドメインの作成中に使用されたマルチキャスト アドレスと同じであることを確認します。

```
~ # vemcmd show openflex
Status: 12 (Active)
Dvs name: comp/prov-VMware/ctrlr-[AVS-TEST]-VC/sw-dvs-87
Remote IP: 10.0.0.30 Port: 8000
Infra vlan: 4093
FTEP IP: 10.0.0.32
Switching Mode: LS
NS GIPO: 225.127.1.1
```

AVS ホストで、ホストに展開された各 EPG ごとに 1 つのマルチキャスト グループが存在することを確認します。下記の出力例では、異なる EPG に接続されている 3 種類の仮想マシンがあります。

```
~ # vemcmd show epp multicast
Number of Group Additions 3
Number of Group Deletions 0
Multicast Address EPP Ref Count
225.0.0.58        1
225.0.0.76        1
225.0.0.92        1
```

これらのマルチキャスト アドレスは APIC GUI に表示される EPG の詳細と対応しています。EPG の詳細は、[Tenants] > [TenantX] > [Application Profiles] > [ApplicationProfileX] > [End Point Groups] > [EndPointGroupX] で、[Operational] タブの [Client End Points] をクリックすると表示されます。

VXLAN ロード バランシング

VXLAN ロード バランシングは、複数の VMKNIC が Cisco AVS に接続されるとただちに自動的に有効になります。各 VMKNIC は 1 つのアップリンク ポートしか使用できません。VMKNIC とアップリンクは同じ数が必要です。最大 8 個の VMKNIC を Cisco AVS スイッチに接続できます。作成した VMKNIC にはそれぞれ固有のソフトウェア ベースの MAC アドレスがあります。VXLAN ロード バランシングでは、VMKNIC によってデータ パケットに一意の MAC アドレスが付与され、これによって、データ パケットが特定の物理 NIC（VMNIC）を使用するように指定できます。

ホストと同じ数の VMKNIC を持つ必要があります（最大 8 つまで）。たとえば、ホストに 5 つの VMNIC がある場合は、4 つの VMKNIC を追加して VXLAN ロード バランシングを有効にする必要があります。残りの 1 つは、ホストを分散仮想スイッチ（DVS）に追加したときに、Cisco Application Policy Infrastructure Controller（APIC）によって作成済みです。

VMware vSphere Client で、各 AVS アップリンク用の追加の仮想アダプタ（VMK）を作成する必要があります。AVS 用に作成した各 vmk インターフェイスは、vtep ポート グループに接続して、DHCP 用に設定する必要があります。追加された各 VMK インターフェイスに、ファブリック TEP プールから一意の DHCP アドレスが割り当てられます。

AVS の IGMP スヌーピング ポリシー

AVS 展開における Cisco UCS B シリーズの考慮事項

ここでは、Cisco UCS B シリーズから AVS を有効にする必要手順について重点的に説明します。

USC-B FI では、デフォルトで IGMP スヌーピングが有効になります。そのため、APIC に IGMP クエリア ポリシーを設定する必要があります。IGMP スヌーピング ポリシーは、インフラストラクチャ テナントで有効にする必要があります。

UCS または他の中間ブレード スイッチで IGMP スヌーピングを無効にした場合、ブレード スイッチはすべての関連するポートにマルチキャスト トラフィックをフラッディングするので、IGMP ポリシーは必要ありません。

AVS の IGMP スヌーピング ポリシーの作成

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[infra] を選択します。
3. [Navigation] ペインで、[infra] > [Networking] > [Bridge Domain] > [default] の順に選択します。
    1. [IGMP Snoop Policy] ドロップダウン リストで、[Create IGMP Snooping Policy] を選択します
    2. ポリシーの名前を入力します（「IGMP_Infra」など）。
    3. [Fast Leave] チェックボックスをクリックします。
    4. [Enable Querier] チェックボックスをクリックします。
4. [Submit] をクリックします。`

（注） IGMP スヌーピング クエリアが UCS ファブリック インターコネクトに表示されているかどうかを確認します。この例では、VLAN 4093 はインフラストラクチャ VLAN であり、192.168.0.30 はインフラストラクチャ ブリッジ ドメインのブリッジ ドメイン サブネットです。

```
ucsb-A(nxos)# show ip igmp snooping querier vlan 4093
Vlan   IP Address      Version   Expires     Port
4093  192.168.0.30     v3        00:03:46    port-channel1
```

vSphere ホスト CLI で **vemcmd show epp multicast** コマンドを使用することにより、IGMP スヌーピングが正常に動作しているかどうかを確認できます。他には、UCS 上に IGMP ポリシーを作成して IGMP スヌーピングを無効にする方法があります。この方法では、すべてのエンドポイントにマルチキャスト トラフィックのフラッディングを引き起こす可能性があります。

Cisco Application Virtual Switch によるマイクロセグメンテーション

Cisco Application Virtual Switch（AVS）によるマイクロセグメンテーション（uSeg）は、さまざまな属性に基づいて自動的にエンドポイントをエンドポイント グループに割り当てる機能を提供します。Cisco AVS によるマイクロセグメンテーションは、Cisco AVS リリース 5.2(1)SV3(1.5) で導入されました。この機能は、Cisco Application Centric Infrastructure (ACI) で Cisco AVS についてのみ使用可能です。VMware Distributed Virtual Switch（DVS）には使用できません。エンドポイント グループは現在、アプリケーション エンドポイント グループと uSeg エンドポイント グループの 2 つのカテゴリに分類されます。アプリケーション エンドポイント グループは、vCenter などの VMM に出現するもので、ネットワーク ポート グループとして仮想マシンに割り当てられます。uSegエンドポイントグループは、同じテナントおよびVMMドメイン内のすべての仮想マシンに、属性の一致を保留して、暗黙的に適用されます。

Cisco AVS で使用されるマイクロセグメンテーション ポリシーは、Application Policy Infrastructure Controller (APIC) により集約的に管理されてファブリックによって適用されます。uSeg エンドポイント グループは vCenter には出現しません。仮想マシンのネットワーク バインディングを変更すると、[uSeg EPG] は、ポート グループのバインディング オプションとして表示されません。ただし、仮想マシンは、ファブリック内の通常のエンドポイント アプリケーション グループに割り当てられたままになります。

表 *2 : uSeg* エンドポイント グループの自動割り当てに使用可能な属性

属性	Attribute Type
VM Name	VM
VM ID	VM
VNIC ID	VM
ハイパーバイザ	VM
DVS ポート グループ	VM
DVS 名	VM
MAC 設定	ネットワーク
IP 設定	ネットワーク

外部接続

外部レイヤ 2 への ACI の拡張

本書の概要で説明したように、ACME 社は複数のデータセンターを持つ多国籍企業です。したがって、ACME 社はいくつかの レイヤ 2 接続を設定する必要があります。この設定は、デー

タセンター相互接続（DCI）プラットフォームにレイヤ2接続を拡張し、さらにリモートデータセンターに接続を拡張するか、またはファブリック外部にレイヤ2ドメインを拡張してACI以外のファブリックの既存のレイヤ2ネットワークに接続するために必要です。

ACI ファブリック外部へのエンドポイント グループの拡張

ACIファブリック外部にエンドポイントグループ（EPG）を拡張する最も簡単な方法は、既存のエンドポイントグループに静的にリーフポートとVLAN IDを割り当てることです。割り当てると、VLAN IDが設定されているリーフポートで受信されたすべてのトラフィックがEPGにマッピングされ、このEPGの設定ポリシーが適用されます。トラフィックの分類はポートで受信されたカプセル化に基づくため、エンドポイントを直接ACIリーフに接続する必要はありません。

ACI リーフ ポートのレイヤ 2 接続を静的に EPG に 割り当てる手順：

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. In the Navigation pane, choose ***Tenant_Name*** **> Application Profiles >** ***App_Profile_Name*** **> Application EPGs >** ***EPG_Name*** **> Static Bindings (Paths)**.
4. [Work] ペインで、[Actions] > [Deploy Static EPG on PC, vPC or Interface] の順に選択します。
    1. [Path] フィールドで、ポートと VLAN ID を指定します。
    2. [Deployment Immediacy] オプション ボタン のいずれかをクリックします。実際の設定がリーフスイッチハードウェアに適用されるタイミングは、展開の緊急度によって決まります。また、このEPGの関連コントラクトをサポートするためのVLANリソースやポリシー連想メモリ（CAM）など、ハードウェア リソースがリーフ スイッチで使用されるタイミングも緊急度によって決まります。[Immediate] オプションを選択すると、EPGの設定とそれに関連するポリシー設定がハードウェアでただちにプログラムされます。[On Demand] オプションを選択した場合、リーフ スイッチは、ポリシーと一致するトラフィックがEPGで受信された場合にのみ、EPGとその関連ポリシーをハードウェアでプログラムします。
    3. 次のいずれかの [Mode] オプション ボタンをクリックします。モード オプションは、着信トラフィックへのVLAN IDのタグ付けについて、ACIリーフがどのように想定するかを指定するために使用します。
        1. Tagged - リーフ ノードは、事前に確立された特定のVLAN IDが着信トラフィックにタグ付けされているものと想定します。これはデフォルトの展開モードです。ホストからのトラフィックにVLAN IDがタグ付けされている場合は、このモードを選択します。カプセル化VLAN/VXLAN IDが一意である限り、複数のEPGを同じインターフェイスに静的にバインドできます。
        2. [Untagged] ：リーフは、トラフィックにVLAN IDがタグ付けされていないものと想定します。**switchport access vlan** ***vlan_ID*** コマンドと同様、このオプションを使用する場合は、1つのEPGにのみインターフェイスを割り当てることができます。このオプションを使用すると、通常はタグなしトラフィックを生成するネットワーク インターフェイス カード（NIC）を備えるベアメタルサーバにリーフ ポートを

接続できます。ポートには、1 つのタグなしの EPG のみを静的にバインドできます。

3. 802.1P - 802.1P ヘッダーがタグ付けされているトラフィックを参照します。802.1P モードは、（**switchport trunk native vlan *vlan_ID*** コマンドと同様に）インターフェイスにタグ付けされていない 1 つの EPG のトラフィックを処理する場合に役立ちます。ただし、（タグなしモードとは異なり）802.1P を使用すると、他の「タグ付き」EPG を同じインターフェイスに静的にバインドできます。このモード分類のリンクで受信されたトラフィックには、次の条件が適用されます。

4. 物理ドメインとそれに関連付ける VLAN プール作成します。
5. 該当する EPG に物理ドメインを関連付けます。
6. 接続可能アクセスエンティティプロファイル（AEP）を作成し、インターフェイスとポリシーを一緒にマッピングします。

AEP と物理ドメインの設定方法については、「ファブリックへの新しいデバイスの追加」の項を参照してください。

ファブリック外部への ACI ブリッジ ドメインの拡張

レイヤ 2 外部接続はブリッジ ドメインに関連付けられ、ブリッジ ドメインの個々の EPG ではなく、ブリッジ ドメイン全体を外部ネットワークに拡張するように設計されています。

ブリッジ ドメインの外部への拡張を実現するには、ブリッジ ドメイン用にレイヤ 2 外部接続を作成する必要があります。そのプロセスで、外部トラフィックを分類するための新しい外部 EPG を作成します。この新しい EPG は既存のブリッジ ドメインの一部になります。外部接続またはエンドポイントを新しい外部 EPG に分類します。また、2 つの EPG を使用する場合は、その間を通過させるトラフィックを選択する必要があります。既存の EPG にエンドポイントを追加する前述の例と同様、この方式では、エンドポイントが同じサブネットとデフォルトゲートウェイを共有できます。

外部 レイヤ 2 ドメインを作成する手順：

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、 ***[Tenant_Name]*** を選択します。
3. [Navigation] ペインで、 ***[Tenant_Name]*** **> [Networking] > [External Bridged Network]** の順に選択します。
4. [Work] ペインで、[Action] > [Create Bridged Outside] の順に選択します。
5. [Create Bridged Outside] ダイアログボックスで、次の操作を実行します。
    1. レイヤ 2 外部接続にブリッジ ドメインと VLAN ID を関連付けます。この VLAN は、外部レイヤ 2 ネットワークで設定する必要があります。レイヤ 2 外部接続は、この VLAN と ACI ファブリックのブリッジ ドメインを同じレイヤ 2 ドメインに配置しま

す。この VLAN ID は、レイヤ 2 外部接続に使用される VLAN プールの範囲内でなければなりません。

1. レイヤ 2 ドメインをまだ作成していない場合は、[External Bridged Domain] リストでそれを作成します。
2. レイヤ2 ドメインの作成時に、VLANプールが未作成の場合は、それを作成して、レイヤ 2 外部接続の VLAN に関連付けます。この操作で、レイヤ 2 外部接続の作成に使用される VLAN ID の範囲を指定します。これにより、EPG 用の VLAN とレイヤ 2 外部接続用の VLAN 間で VLAN 範囲が重複するのを回避できます。

2. レイヤ 2 境界リーフ ノード、およびレイヤ 2 外部接続用のレイヤ 2 インターフェイスを追加します。
3. レイヤ2境界リーフとレイヤ2インターフェイスを追加したら、[Next] をクリックし、レイヤ 2 EPG の作成を開始します。レイヤ 2 EPG の名前を入力します。指定された VLAN（ステップ 1 で指定した VLAN ID）が付いたトラフィックは、ACI ファブリックに入ると、すべてこのレイヤ 2 EPG に分類されます。
4. 既存の EPG 内の既存のエンドポイントと新しい外部レイヤ 2 EPG との間の通信を許可するコントラクトを設定します。[Navigation] ペインで、[External Bridged Networks] > [Networks] を選択し、このポリシーを制御するコントラクトを使用コントラクトとして指定します。このコントラクトを内部EPGのコントラクトとして指定すると、外部レイヤ 2 EPG と既存の内部 EPG 間で通信できるようになります。
5. AEP を作成します。これは、選択したポートで特定のカプセル化（VLAN）を許可するように APIC に指示するポリシー オブジェクトです。接続可能アクセス エンティティ プロファイルの作成方法については、「ファブリックへの新しいデバイスの追加」の項を参照してください。

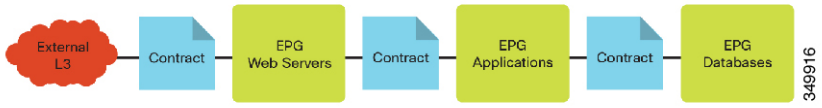
これで、内部と外部のレイヤ 2 セグメント間に必要な到達可能性を確保できました。

外部レイヤ 3 への ACI の拡張

どのアプリケーションにおいても、最も重要なコンポーネントはユーザまたはカスタマーです。これらは、通常ファブリックに直接接続していないため、外部ネットワークに接続する必要があります。ACME は、社内バックボーンに加えて、モバイル アプリケーションへのアクセス用としてインターネットにも接続できなければなりません。この統合は、テナント ポリシー レベルでシスコ 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）を使用することにより実現できます。ルータなどのデバイスへのレイヤ3接続は**外部ルーテッド ネットワーク**と呼ばれ、テナントのプライベート ネットワークと外部 IP ネットワーク間に IP 接続を提供します。各レイヤ 3 外部接続は 1 つのテナント プライベート ネットワークに関連付けられます。レイヤ 3 外部ネットワークの要件は、アプリケーション プロファイルのデバイス グループがACIファブリック外部のネットワークへのレイヤ3接続を必要とする場合にのみ必要です。

アプリケーション プロファイルによって、オペレータはアプリケーションのさまざまなコンポーネントや階層をエンドポイント グループ（EPG）にグループ化できます。これらのアプリケーション コンポーネントには、外部からの接続に対して要件がある場合があります。次の図は、ファブリックの一部を簡略化して示しています。

図 *23*：階層間にコントラクトがある *3* 層アプリケーションのアプリケーション プロファイルの例



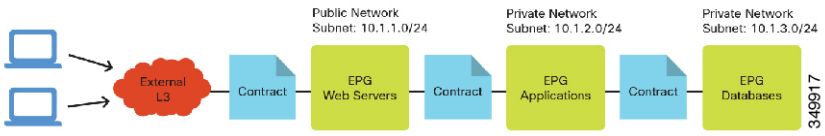
たとえば、Web サーバでは、ユーザが外部に到達するための接続が必要です。ACI では、定義されている外部レイヤ 3 エンドポイント グループとのコントラクトによって接続が定義されます。ファブリックのオペレータが指定することにより、テナント管理者は、テナントのアプリケーション プロファイルに対して一意に定義されたレイヤ 3 コンストラクトを使用するか、共有インフラストラクチャを使用して、さまざまな方法で外部レイヤ 3 接続とインターフェイスをとることができます。

外部レイヤ 3 接続は通常、ACI の境界リーフ コンストラクトで確立されます。ACI リーフは境界リーフになることができます。大規模な ACI 設計では、境界リーフとして専用の ACI リーフを設定すると生産性が向上することがあります。スパイン ノードが外部ルータに接続できないことに注意することが重要です。境界リーフとは、レイヤ 3 デバイスに接続することになるリーフを意味します。サーバなどの他のデバイスは、引き続き境界リーフに接続できます。ACI ファブリックでは、外部レイヤ 3 接続は次のタイプのいずれかです。

1. 物理層 3 インターフェイス
2. 8021.Q タギングがあるサブインターフェイス
3. スイッチ仮想インターフェイス（SVI）

次の図は、パブリックおよびプライベート ネットワークのロジックを示しています。

図 *24*：外部コンシューマ、パブリックおよびプライベート ネットワークに関する注釈付きのアプリケーション プロファイル



外部レイヤ 3 接続を介して接続するデバイスの場合、外部ネットワークは内部 ACI ネットワーク 10.1.1.0/24 を学習しており、これがレイヤ 3 外部接続を介して隣接ルータにアドバタイズされます。プライベート ネットワークの場合、ACI はルーティング プロトコルによってネットワークをレイヤ 3 隣接ルータにアドバタイズせず、ネットワークはファブリックの外部デバイスに到達できません。

Cisco Application Policy Infrastructure Controller（APIC）バージョン 1.1 以前のリリースでは、ファブリックは、関連するブリッジ ドメインでパブリックとしてマークされたサブネットだけをアドバタイズします。ファブリックの外部から学習されたルートは、他のポートを介してア

ドバタイズされません。この動作は、非トランジットファブリックと呼ばれます。バージョン1.1 以降のリリースでは、ACI は中継ネットワークとして機能し、ファブリックのルートだけではなく、外部のレイヤ 3 接続から学習したルートを別の外部レイヤ 3 接続にアドバタイズできます。

ネットワーク チームは、テナントに外部レイヤ 3 接続を提供します。一般的な方式の 1 つは、ルータのサブインターフェイスを使用して、異なるレイヤ 3 ドメインを作成することです。これは、各テナントに独自の外部ルータがない可能性があるからです。

サポートされるルーティング プロトコル

書き込み時には次のルーティング プロトコルがサポートされます。

- スタティック ルート：スタティック ルートを外部に定義することができます。スタティック ルートを使用すると、リーフ ノードのルーティング テーブルのサイズと複雑さを軽減できますが、管理者の負担が増加します。スタティック ルートを使用する場合は、外部から戻るための到達可能な内部ネットワークのスタティック パスを設定する必要があります。
- OSPF NSSA：Not-So-Stubby Area（NSSA）を使用して、Open Shortest Path First（OSPF）データベースのサイズを削減し、大きいルート テーブルを持つルーティング プロトコルのオーバーヘッドの保守を軽減します。OSPF NSSA の場合、ルータは、ファブリックからのデフォルト パスを含めて、ルートの集約のみを学習します。OSPF NSSA は、外部レイヤ 3 の内部パブリック サブネット部分を隣接ルータにアドバタイズします。
- iBGP ピアリング リーフと外部ルータ：内部ボーダー ゲートウェイ プロトコル（iBGP）では、ACI は、内部マルチプロトコル ボーダー ゲートウェイ プロトコル（MP-BGP）ルート リフレクタで使用される番号と一致する、1 つの自律システム（AS）番号のみをサポートします。MP-BGP がない場合、レイヤ 3 外部接続の外部ルート（スタティック、OSPF、または BGP）はファブリック内に伝播されず、境界リーフに含まれていない ACI リーフは外部ネットワークに IP 接続できません。両方のケースに対して同じ AS 番号を使用する場合、ユーザは、ACI 境界リーフの接続先ルータの AS 番号を検索し、その番号を ACI ファブリックの BGP AS 番号として使用する必要があります。

MP-BGP スパイン ルート リフレクタの設定

ACI ファブリックのルート リフレクタは、マルチプロトコル ボーダー ゲートウェイ プロトコル（MP-BGP）を使用してファブリック内に外部ルートを配布するので、フル メッシュ BGP トポロジは必要ありません。ACI ファブリックでルート リフレクタを有効にするには、ファブリック管理者が、ルート リフレクタとなる 1 つ以上のスパイン スイッチを選択し、ファブリックに自律システム（AS）番号を指定する必要があります。ルート リフレクタを設定すると、管理者は外部ネットワークへの接続を設定できます。

ACI ファブリックに外部レイヤ 3 デバイスを接続するには、ファブリック インフラストラクチャのオペレータが、ルート リフレクタ ポリシーを設定し、ルート リフレクタとして動作するスパインを指定する必要があります。冗長性のために、ルータ リフレクタ ノードとして複数のスパインを設定します。

テナントでレイヤ 3 接続が必要な場合、インフラストラクチャ オペレータは、WAN ルータが接続されているリーフノードを境界リーフ ノードとして設定する必要があります。これによって、境界リーフ ノードに BGP ピアとして 1 つのルート リフレクタ ノードが組み合わされます。ルート リフレクタを設定すると、それらによってファブリックのルートをアドバタイズできます。

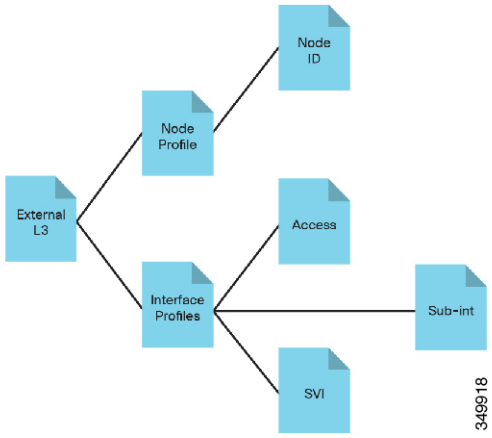
各リーフ ノードには書き込み時に 4000 ルートを格納できます。4000 以上のルートをアドバタイズする必要がある場合、WAN ルータは複数のリーフ ノードを使ってピアします。インフラストラクチャ オペレータは、ノードがアドバタイズできるルート（またはルート プレフィクス）をペア リーフ ノードのそれぞれに設定します。

ルート リフレクタ ポリシーを設定する手順：

1. メニュー バーで、[Fabric] > [Fabric Policies] を選択します。
2. [Navigation] ペインで、[Pod Policies] > [Policies] > [BGP Route Deflector default] の順に選択します。
3. [Work] ペインで、次の操作を実行します。
    1. ネットワークに必要な番号と一致するように、[Autonomous System Number] を変更します。
    2. このリフレクタ ポリシーのメンバーとなる 2 つのスパイン ノードを追加します。
    3. [Submit] をクリックします。`
4. [Navigation] ペインで、[Pod Policies] を選択します。
5. [Work] ペインで、[Actions] > [Create Pod Policy Group] の順に選択します。
6. [Create Pod Policy Group] ダイアログボックスで、次の操作を実行します。
    1. [BGP Route Reflector Policy] ドロップダウン リストから [default] を選択します。
    2. [Navigation] ペインで、[Pod Policies] > [Profiles] > [default] の順に選択します。
    3. [Work] ペインで、[Fabric Policy Group] ドロップダウン リストから [Create Pod Policy Group] を選択します。
    4. [Create Pod Policy Group] ダイアログボックスで、[Date Time Policy] ドロップダウン リストから [default] を選択します。
    5. [BGP Route Reflector Policy] ドロップダウン リストから [default] を選択します。
    6. 設定に応じて、ダイアログボックスの残りの設定を完了させます。
7. [Submit] をクリックします。`

次の図は、外部レイヤ 3 接続のオブジェクトとその関係を示しています。

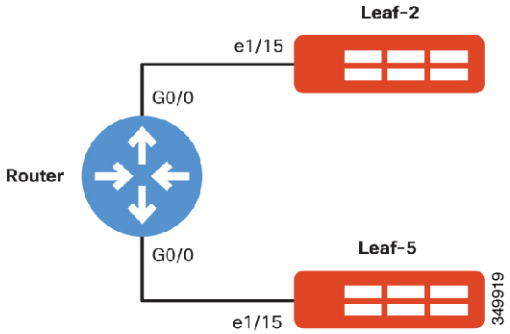
図 *25 :* レイヤ *3* 外部オブジェクトの関係



OSPF NSSA によるマルチテナント ネットワーク経由のレイヤ 3 の統合

次の図は、OSPF を使用して ACI に外部レイヤ 3 を統合する仕組みを簡略化して示しています。

図 *26 : 2* つの境界リーフと通信する外部 *OSPF* ルータの論理トポロジ



このセットアップには、リーフ スイッチに接続する 2 つのインターフェイスを持つ 1 つのルータが含まれています。

注：ルータに接続しているリーフのインターフェイスに対してアクセス ポリシーを設定するには、「ファブリックへの新しいデバイスの追加」の項を参照してください。

OSPF/NSSA によってマルチテナント ネットワーク経由でレイヤ 3 を統合する手順：

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインでテナントを選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** **> [Networking] > [External Routed Networks]** を選択します。

4. [Work] ペインで、[Actions] > [Create Routed Outside] の順に選択します。
5. [Create Routed Outside] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、プロファイルの名前を入力します。
    2. [Private Network] ドロップダウン リストから、テナントのプライベート ネットワークを選択します。
    3. [OSPF] チェックボックスをオンにします。
    4. [OSPF Area ID] フィールドに、OSPF エリア ID を入力します（「1」など）。
    5. [OSPF Area Control] セクションで、[Send redistributed LSAs into NSSA area] チェックボックスをクリックします。
    6. [OSPF Area Type] セクションで、[NSSA Area] オプション ボタンをクリックします。
    7. [Nodes and Interfaces Protocol Profiles] セクションで、[+] をクリックしてプロファイルを追加します。
    8. [Create Node Profile] ダイアログボックスで、次の操作を実行します。
        1. [Name] フィールドに、プロファイルの名前を入力します。
        2. [Nodes] セクションで、[+] をクリックしてノードを追加します。
        3. [Select Node] ダイアログボックスで、次の操作を実行します。
            1. [Node ID] ドロップダウン リストで、ノードを選択します（[Leaf-1] など）。
            2. [Router ID] フィールドに、ID としてルータの IP アドレスを入力します（「10.0.1.1」など）。
            3. [Router ID as Loopback Address] チェックボックスをオフにします。
            4. [Loopback Addresses] セクションで、[+] をクリックしてループバック アドレスを追加します。
            5. ループバック アドレス（「10.254.254.1」など）を入力し、[Update] をクリックします。
            6. [OK] をクリックします。
        4. [OSPF Interface Profiles] セクションで、[+] をクリックし、OSPF インターフェイス プロファイルを作成します。
        5. [Create Interface Profile] ダイアログボックスで、次の操作を実行します。
            1. [Name] フィールドに、プロファイルの名前を入力します。
            2. [OSPF Policy] ドロップダウン リストで、[Create OSPF Interface Policy] を選択します。別の OSPF ルータとの相互作用を定義する場合は、ポリシーの相互作用を指定する必要があります。本書では、さまざまな OSPF パラメータについては説明しません。

3. [Create OSPF Interface Policy] ダイアログボックスで、次の操作を実行します。

Ordered List Number 5	[Name] フィールドに、OSPF ポリシーの名前を入力します（「OSPF- Point2Point」など）。
Ordered List Number 5	[Network Type] セクションで、隣接ルータと一致するオプションボタン（[Point to Point] など）をクリックします。
Ordered List Number 5	設定に応じて、ダイアログボックスの残りの設定を完了させます。
Ordered List Number 5	[Submit] をクリックします。`

4. [Interfaces] セクションで、[Routed Intefaces] タブをクリックします。
5. [+] をクリックし、ルーテッド インターフェイスを選択します。
6. [Select Routed Interface] ダイアログボックスで、次の操作を実行します。

Ordered List Number 5	[Path] ドロップダウン リストから、リーフのインターフェイスを選択します（e1/9 on Leaf-1 など）。
Ordered List Number 5	[IP Address] フィールドに、レイヤ 3 外部プロファイルに関連付けられているパスの IP アドレス（「10.0.1.1/24」など）を入力します。
Ordered List Number 5	[MTU (bytes)] フィールドに、外部ネットワークの最大 MTU を入力します（例のピアルータに一致する「1500」など）。
Ordered List Number 5	設定に応じて、ダイアログボックスの残りの設定を完了させ、[OK] をクリックします

7. [OK] をクリックします。

6. [OK] をクリックします。

9. [次へ（Next）] をクリックします。

10. [External EPG Networks] セクションで、[+] をクリックし、外部ネットワークを作成します。
11. [Create External Network] ダイアログボックスで、次の操作を実行します。
    1. [IP Address] フィールドに、「0.0.0.0/0」を入力してサブネットの学習を許可し、[OK] をクリックします。
12. [Finish] をクリックします。次に、外部ネットワーク EPG を設定する必要があります。

複数テナントの 外部レイヤ 3

ACI では、さまざまな機能を使用して、複数のテナントに対して同じ外部レイヤ 3 ルータを再利用できます。隣接ルータがレイヤ 2 トランク インターフェイスを備えた Cisco Nexus シリーズ スイッチの場合は、SVI を介してルーティングするように外部レイヤ 3 接続を設定できます。サブインターフェイスを使用可能なルータの場合は、それらを使用して、複数の VRF やテナントに複数の外部レイヤ 3 接続を提供できます。ファブリック オペレータは、サブインターフェイスまたは SVI を使用して、複数の外部レイヤ 3 接続を設定し、それを各テナントに提供できます。

アプリケーションの移行の使用例

ACI ファブリックを運用しているときに、ACI ファブリックの外部からワークロード、サーバ、または仮想ホストを移行しなければならない場合があります。一般的な例として、従来のデータセンター構成から ACI を使用するポリシー主導型データセンターに移行する場合などがあげられます。ACME がさらに多くのデータセンターで ACI の使用を開始するには、これらの移行を実行する必要があります。この例では、ACME はスイッチ仮想インターフェイス（SVI）の移行を管理することに加えて、トラフィックがレイヤ 2 外部ネットワークを通じて ACI ファブリックに到達できるように、ポリシーを管理する必要があります。

おおまかに説明すると、まず、レイヤ 2 外部ネットワークを設定し、ソース VLAN からのトラフィックが ACI ファブリックの同じ VLAN と通信できるようにする必要があります。また、SVI 移行後の完全接続に備えて、ファブリックから既存のレイヤ 3 ネットワークへのレイヤ 3 接続を設定する必要があります。

ポリシーを含めたレイヤ 2 とレイヤ 3 接続の詳細および作成手順については、本書の「ファブリック接続」の章を参照してください。

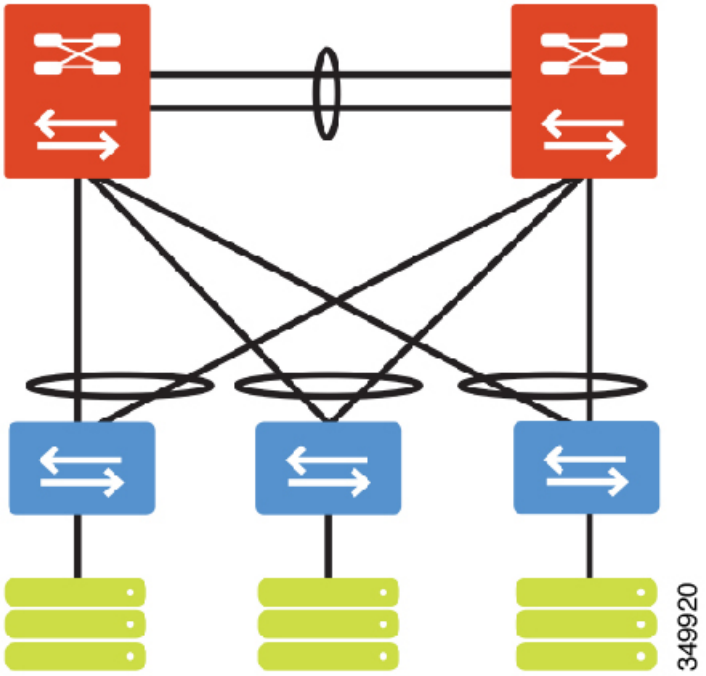
外部レイヤ 2 ネットワーク（これを介して、ワークロードやホストが到達）と既存の内部ファブリック EPG 間の接続が正常に確立されたら、移行プロセスを開始して、ファブリックにアプリケーション ワークロードを移動できます。考慮すべき重要事項の 1 つとして、既存の環境から ACI ファブリックに SVI インターフェイスをスイッチ オーバーするタイミングと、SVI ネットワークにルートをアドバタイズするタイミングがあげられます。SVI が外部レイヤ 2 ネットワーク上に存在する場合は、ホストの大部分を移行してから、SVI を ACI ファブリックに移動することをお勧めします。

ACI へのネットワークの拡張

ACME は、サイトの 1 つをレガシー データセンター アーキテクチャから次世代の Cisco Application Centric Infrastructure (ACI) ファブリックに移行することを希望しています。必要に応じて ACI の革新的技術を活用すると同時に、最小限のサービス中断でサイトを移行する必要があります。ACME はいくつかの段階を踏んで移行を実行したいと考えています。

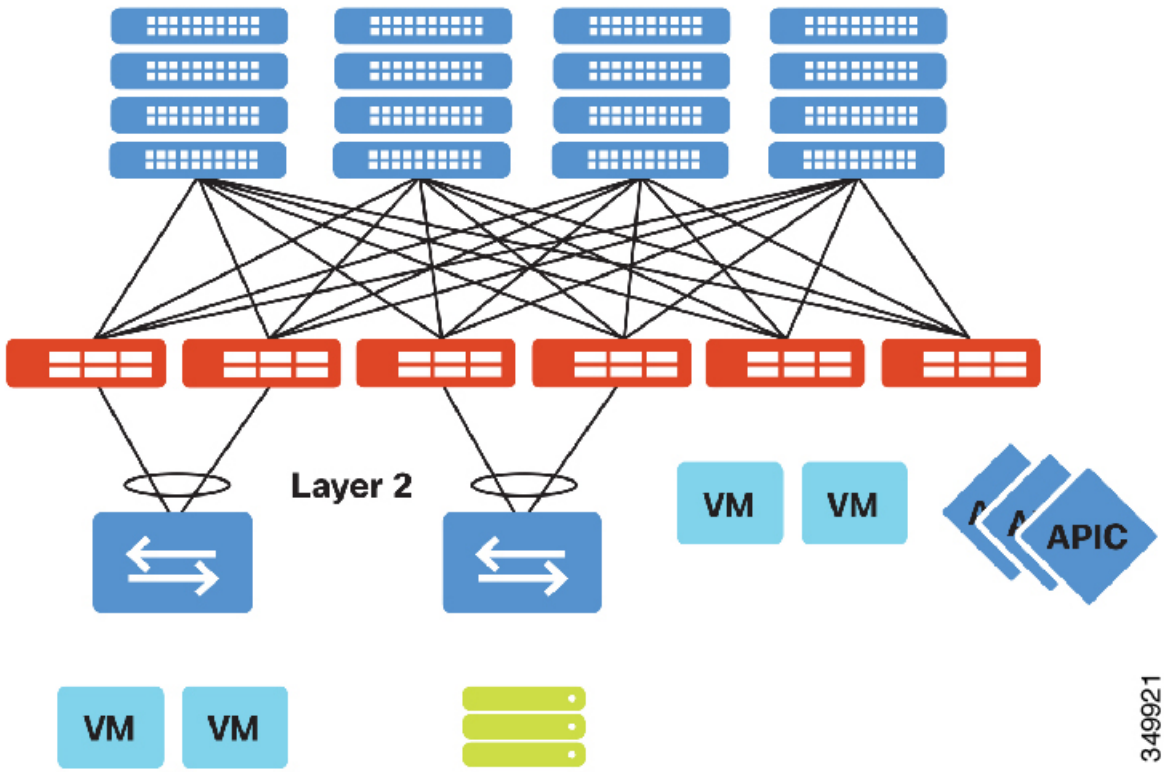
移行前のレガシー データセンター：

図 *27*：移行前の従来のデータセンター



移行後の ACI データセンター：

図 *28* : 移行後の *ACI* ベースのデータセンター トポロジ



第 1 段階として、レガシー データセンターから ACI ファブリックへの接続を確立します。この状態で、VLAN=EPG を論理的にマッピングします。レガシー ネットワークから ACI ファブリックへの相互接続は、標準のレイヤ 2 拡張（VLAN/VXLAN）によって実現されます。

既存のアグリゲーション レイヤから ACI 境界リーフへの物理的な接続を確立します。この接続は、仮想ポート チャネル、ポート チャネル、または 1 つのインターフェイスの形式で実現されます。

1. アグリゲーション スイッチ #1 から ACI 境界リーフ #1 への物理的接続を確立します。
2. アグリゲーション スイッチ #1 から ACI 境界リーフ #2 への物理的接続を確立します。

注：ファブリックへの外部物理接続を確立する前に、DCI で使用するアクセス ポートのファブリック アクセス ポリシーを設定する必要があります。アクセス ポリシーの設定の詳細については、本書の「ファブリック接続」の項を参照してください。

アグリゲーション リンクをレイヤ 2 トランクとして設定します。

1. ホスト接続を表すVLANをトランキングします。これにより、ホストVLANをファブリックに拡張できます。

Application Policy Infrastructure Controller (APIC) で、1 つのテナントを設定します。作成したテナントは、ACI ファブリック内でレガシー データセンターを表します。

1. メニュー バーで [Tenants] > [Add Tenant] の順に選択します。
2. [Create Tenant] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドにテナントの名前を入力します。
    2. [次へ（Next）] をクリックします。
3. [完了（Finish）] をクリックします。

1 つのプライベート ネットワークを設定します。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Private Networks] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Private Network] の順に選択します。
5. [Create Private Network] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、プライベート ネットワークの名前を入力します。
    2. [Next] をクリックします。
    3. [Name] フィールドに、ブリッジ ドメインの名前を入力します。
    4. [Forwarding] ドロップダウン リストから [Custom] を選択します。
    5. [Layer 2 Unknown Unicast] オプション ボタンで、[Flood] をクリックします。
    6. [Multi Destination Flooding] オプション ボタンで、[Flood in BD] をクリックします。
    7. [ARP Flooing] チェックボックスをクリックします。
6. [Finish] をクリックします。

注：ファブリック内の不明なユニキャストと arp をフラッディングするのは、レガシー データセンターのレイヤ2セマンティックスを ACI ファブリックに拡張できるようにするためです。レガシー データセンターのホストが ARP 要求を送ったり、不明なユニキャスト フレームをフラッディングすると、ブリッジ ドメインは ACI ファブリックでその動作を模倣します。デフォルトでは、BPDU フレームは EPG内にフラッディングされます。

1 つのアプリケーション プロファイルを設定します。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Application Profiles] を選択します。
4. [Work] ペインで、[Actions] > [Create Application Profile] の順に選択します。
5. [Create Application Profile] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、アプリケーション プロファイルの名前を入力します。
    2. [Submit] をクリックします。`

1 つのエンドポイント グループを設定します。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。

3. [Navigation] ペインで、[Tenant_Name] > [Application Profiles] > [Application_Profile_Name] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Application EPG] の順に選択します。
5. [Create Application EPG] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドにエンドポイント グループの名前を入力します。
    2. [Bridge Domain] で、適切なブリッジ ドメインを選択します。
    3. [Finish] をクリックします。

注：ファブリック内の EPG はレガシー データセンター内の 1 つの VLAN にマッピングします。ファブリックの革新的技術を導入すると同時に、EPG ごとに 1 つの VLAN を使用して、ネットワーク中心型の移行による影響を最小化するパスを指定します。

レガシー データセンターに接続するための VPC を設定します。「ファブリック接続」の項を参照してください。次に、エンドポイント グループ AcmeOutSide で VPC を使用して、スタティック トランクのバインディングを設定します。カプセル化 VLAN が、定義されているレガシー データセンターの VLAN 定義と一致する必要があります。

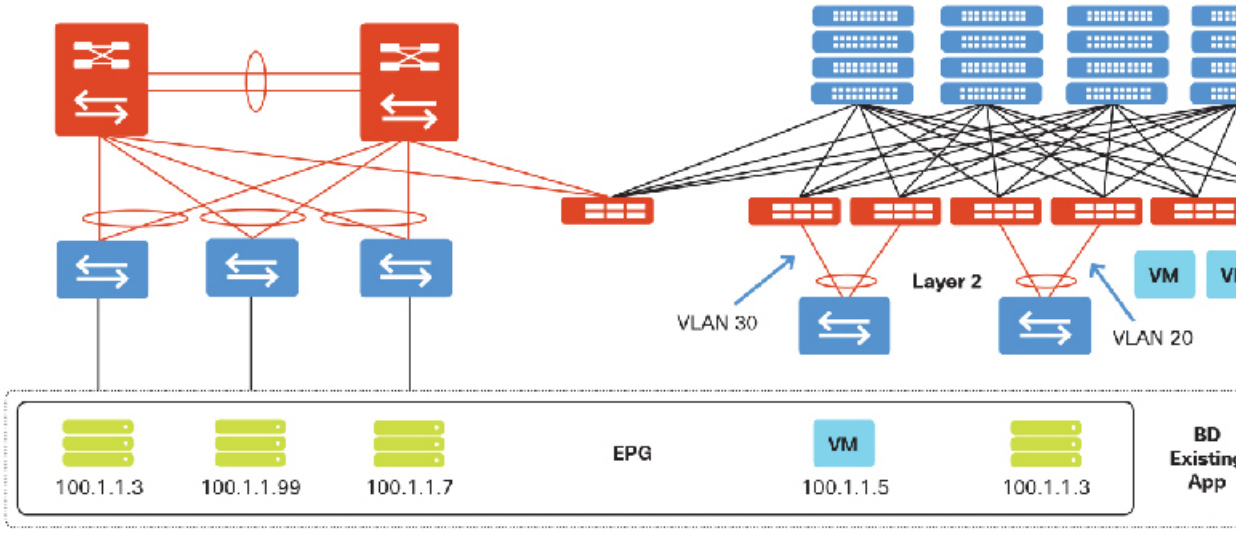
1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、**[Tenant_Name]** > **[Application Profiles]** > **[Application_Profile_Name]** > **[Application EPGs]** > **[EPG_Name]** > **[Domains VMs and Bare-Metals]** の順に選択します。
4. [Work] ペインで、[Actions] > [Add Physical Domain Association] の順に選択します。
5. [Add Physical Domain Association] ダイアログボックスで、次の操作を実行します。
    1. レガシー データ センターのインターフェイスに関連付ける [Physical Domain Profile] を選択します。
    2. [Deploy Immediacy] を選択します。
    3. [Resolution Immediacy] を選択します。
    4. [Submit] をクリックします。`
6. [Navigation] ペインで、[Tenant_Name] > [Application Profiles] > [Application_Profile_Name] > [Application EPGs] > [EPG_Name] > [Static Bindings (Paths)] の順に選択します。
7. [Work] ペインで、[Actions] > [Deploy Static EPG on PC, VPC or Interface] の順に選択します。
8. [Deploy Static EPG on PC, VPC or Interface] ダイアログボックスで、次の操作を実行します。
    1. [Path Type] を選択します。
    2. [Path] を選択します。
    3. カプセル化 VLAN を入力します。
    4. [Submit] をクリックします。`

移行の第 1 段階が完了すると、レガシー ホスト VLAN が ACIファブリックに拡張され、ファブリックの観点から、すべてのホストが EPG AcmeOutSide に含まれます。ローカル VLAN 番号は、レガシー データセンター向けの VPC でタグ付き VLAN にマップされるため、ACIファ

ブリックにとってローカルVLAN番号は重要ではありません。これは正規化と呼ばれ、ACIはタグ付き VLAN を使用して、外部レイヤ 2 接続を ACI エンドポイント グループにマップします。

以下に示す接続は BD=EPG=VLAN を表しています。ACI ファブリックおよびレガシー データセンターのレイヤ 3 ゲートウェイは、レガシー データセンターによって提供されます。

図 *29 : VLAN* データセンター展開としての *EPG*



移行の第 2 段階では、ファブリック ポリシー モデルを利用して、さらにアプリケーションのモデル化を定義します。この段階では、到達性を定義する APIC コントラクトによって複数の EPG が作成されます。次のリストは、実行する必要があるステップの概要を示しています。

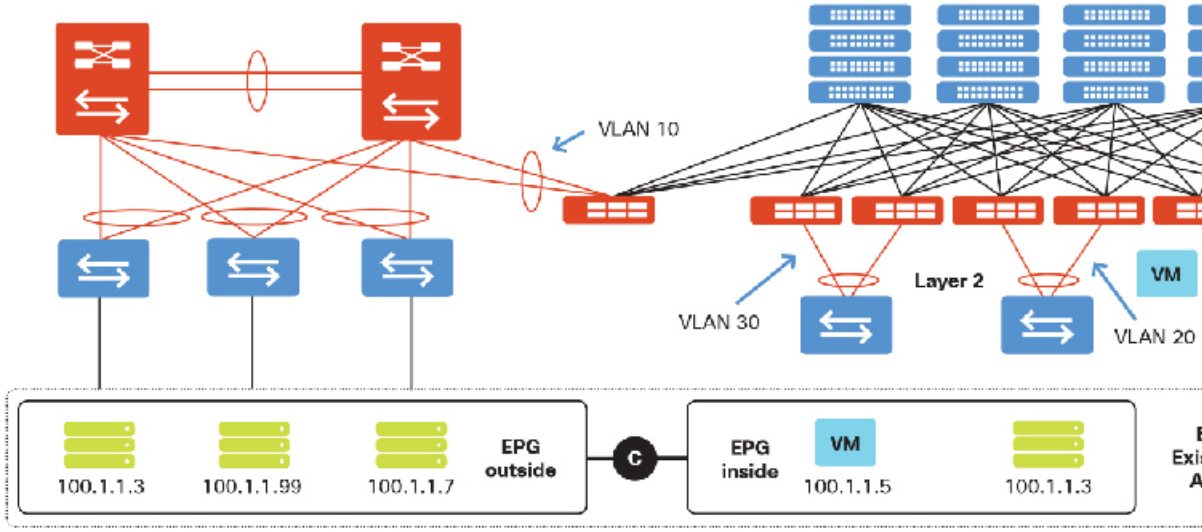
1. APIC で次の手順を実行します。
    1. （任意）追加のテナントを設定します。
    2. （任意）追加のプライベート ネットワークを設定します。
    3. （任意）追加のブリッジ ドメインを設定します。
    4. （任意）追加のアプリケーション プロファイルを設定します。
    5. 追加のエンドポイント グループを設定します。
        1. エンドポイント グループ「AcmeInSide」を作成します。
    6. EPG 間通信のコントラクトを設定します。
        1. [Scope] ドロップダウン リストから [Tenant] を選択します。
        2. [Allow] ドロップダウン リストから [Any-Any] を選択します。
2. ファブリックの EPG「AcmeInSide」へのホストの移行を開始します。
    1. 移行する各物理ホストのスタティック バインディングを作成します。
    2. （任意）VMM ドメインを作成して、ACI ファブリック内にホストを展開します。

注：接続、VLAN プール、物理ドメインまたは VMM ドメイン、AEP、およびスイッチまたはインターフェイスのプロファイルをサポートする、適切なリソースが作成されていることを確認します。詳細については、「ファブリック接続」の項を参照してください。

移行の第 2 段階が完了すると、レガシー データセンターと ACI ファブリックの両方にわたるホスト接続が、APIC ポリシー（コントラクト）によって管理されるようになります。

注：ACI ファブリックおよびレガシー データセンターのレイヤ 3 ゲートウェイは、レガシー データセンターによって提供されます。

図 *30*：既存の *DC* によって提供されるレイヤ *3* と *ACI* データセンターに拡張されたレイヤ *2* によるデータセンターの移行



移行の第 3 段階では、従来のデータセンターから ACI ファブリックにレイヤ 3 ゲートウェイを移動します。次のリストは、実行する必要があるステップの概要を示しています。

1. APIC で、以下を実行します。
    1. レイヤ 3 出力を設定します。
    2. レガシー データセンターからファブリックにゲートウェイを移行します。
        1. [Bridge Domain] ドロップダウン リストから [AcmeBD] を選択します。
        2. [Flood Layer 2] ドロップダウン リストから [Unknown Unicast] を選択します。
        3. [ARP] ドロップダウン リストから [Flooding] を選択します。
        4. [Unicast] ドロップダウン リストから [Routing] を選択します。

注：ブリッジ ドメイン内のユニキャスト ルーティングのコンセプトによって、ファブリック全体にわたる広範なゲートウェイの設定が可能になります。ACI ファブリックおよびレガシー データセンターのレイヤ 3 ゲートウェイは、ACI ファブリックによって提供されます。