ACI ポリシー モデル

この章は、次の内容で構成されています。

- ACI ポリシー モデルの概要 （1 ページ）
- ポリシー モデルの主な特性 （2 ページ）
- 論理構造 （2 ページ）
- Cisco ACI ポリシー管理情報モデル （3 ページ）
- テナント （5 ページ）
- VRF （6 ページ）
- アプリケーション プロファイル （7 ページ）
- エンドポイント グループ （8 ページ）
- ブリッジ ドメインとサブネット （13 ページ）
- 接続可能エンティティ プロファイル （19 ページ）
- VLAN と EPG （20 ページ）
- コントラクト （32 ページ）
- 外部ネットワーク （45 ページ）
- 管理対象オブジェクトの関係とポリシー解決 （46 ページ）
- デフォルト ポリシー （47 ページ）
- トランス テナント EPG 通信 （49 ページ）
- タグ （50 ページ）
- APIC クォータ管理の構成について （51 ページ）

ACI ポリシー モデルの概要

ACI ポリシー モデルにより、アプリケーション要件のポリシーの指定を有効化します。APIC は、ファブリック インフラストラクチャにポリシーを自動的にレンダリングします。ユーザまたはプロセスがファブリック内のオブジェクトへの管理上の変更を開始すると、APIC は最初にポリシー モデルにその変更を適用します。このポリシー モデルの変更により、実際の管理対象エンドポイントへの変更がトリガーされます。この方法を、モデル方式フレームワークといいます。

ポリシー モデルの主な特性

ポリシー モデルの主な特性には次のものがあります。

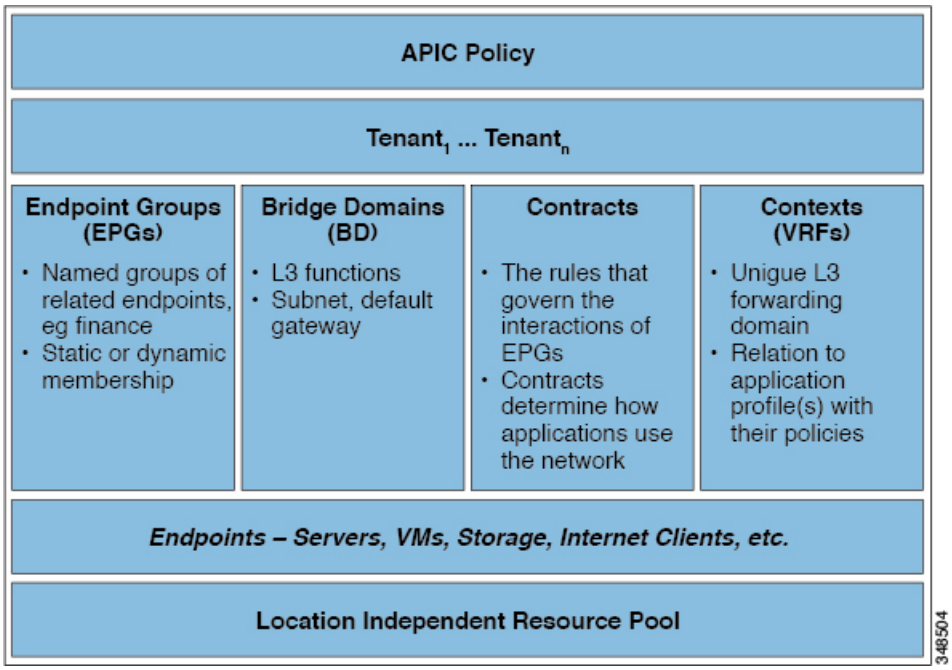
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはファブリック、サービス、システム動作、およびネットワークに接続された仮想および物理デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な構成は、使用可能なリソースに関連するポリシーを適用することで具体的な構成にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、APIC ポリシー モデルの変更の副作用として明示的に構成されます。具象エンティティは、（仮想マシンまたはVLANなど）物理的にすることができますが、そうする必要はありません。
- システムは、新しいデバイスを含めるようにポリシーモデルが更新されるまで、新たに接続されたデバイスとの通信を禁止します。
- ネットワーク管理者は、論理的および物理的なシステムリソースを直接構成しませんが、システム動作のさまざまな面を制御する（ハードウェアに依存しない）論理的な構成とAPIC ポリシーを定義します。

モデル内の管理対象オブジェクトを操作することで、エンジニアは独立した個々のコンポーネントの構成を管理することから開放されます。これらの特性により、自動化と柔軟なワークロードのプロビジョニングが可能になり、インフラストラクチャ内のワークロードをどこでも検索できるようになります。ネットワーク接続されたサービスは簡単に展開でき、APIC により自動化フレームワークが提供され、それらのネットワーク接続されたサービスのライフサイクルを管理できます。

論理構造

ポリシーモデルは、インフラストラクチャ、認証、セキュリティ、サービス、アプリケーション、診断など、ファブリック全体を管理します。ポリシーモデルの論理構造は、ファブリックの機能のニーズをファブリックがどのように満たすかを定義します。次の図は、ACI ポリシーモデルの論理構造の概要を示します。

図 *1 : ACI* ポリシー モデルの論理構造の概要



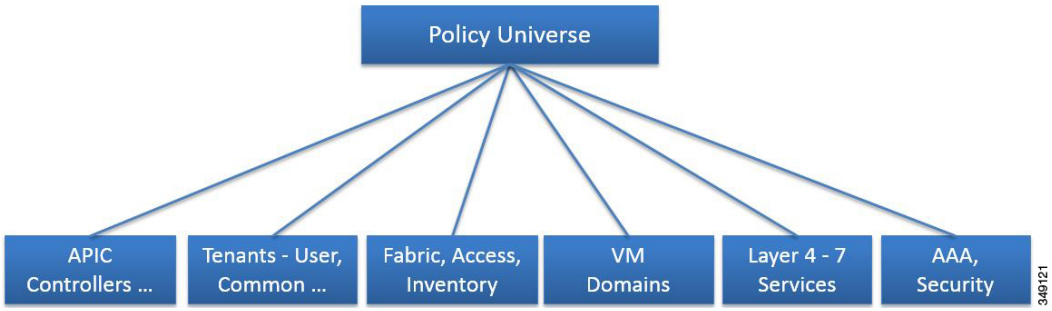
ファブリック全体またはテナントの管理者は、アプリケーションまたは共有リソースの要件を含む事前定義されたポリシーを作成します。これらのポリシーは、アプリケーション、ネットワーク接続サービス、セキュリティ ポリシー、およびテナント サブネットのプロビジョニングを自動化し、管理者をインフラストラクチャの構成要素ではなくアプリケーションの観点から、リソースプールにアプローチするポジションにします。アプリケーションは、ネットワーキングの動作を誘導する必要があり、その逆ではありません。

Cisco ACI ポリシー管理情報モデル

ファブリックは、階層型管理情報ツリー（MIT）で表示できる管理情報モデル（MIM）に記録される物理および論理コンポーネントから構成されます。情報モデルは、APIC で実行するプロセスによって保存され管理されます。OSI 共通管理情報プロトコル（CMIP）および他の X.500 バリアントと同様に、APIC によって、MIT の階層構造内のオブジェクトの場所に応じて継承できるオブジェクトのプロパティとして管理可能な特性を示すことにより、管理対象リソースの制御が可能になります。

ツリーの各ノードは、管理対象オブジェクト（MO）またはオブジェクトのグループを表します。MO はファブリック リソースの抽象化です。MO は、スイッチ、アダプターなどの具象オブジェクト、またはアプリケーション プロファイル、エンドポイント グループ、または障害などの論理オブジェクトを表すことができます。次の図は、MIT の概要について説明します。

図 *2 : Cisco ACI* ポリシー管理情報モデルの概要



階層構造は、最上位（ルート）でポリシー ユニバースから始まり、親と子ノードが含まれます。ツリー内の各ノードはMOで、ファブリック内の各オブジェクトには、オブジェクトを説明しツリー内の場所を検索する一意な識別名（DN）があります。

次の管理対象オブジェクトには、システムの動作を管理するポリシーが含まれます。

- APIC コントローラは、マルチテナント ファブリックの管理、ポリシー プログラミング、アプリケーション展開、およびヘルスモニタリングを提供する複製同期されたクラスタ化コントローラを構成します。
- テナントはポリシーのコンテナで、管理者はドメインベースのアクセス制御を実行できます。システムにより、次の 4 種類のテナントが提供されます。
  - ユーザ テナントは、ユーザのニーズに応じて管理者によって定義されます。アプリケーション、データベース、Web サーバ、ネットワークアタッチド ストレージ、仮想マシンなどのリソースの動作を管理するポリシーが含まれます。
  - 共通テナントは、システムによって提供されますが、ファブリックの管理者が構成できます。ファイアウォール、ロードバランサ、レイヤ4～レイヤ7サービス、侵入検知アプライアンスなど、すべてのテナントにアクセス可能なリソースの動作を管理するポリシーが含まれます。
  - インフラストラクチャテナントは、システムによって提供されますが、ファブリックの管理者が構成できます。ファブリック VXLAN オーバーレイなどのインフラストラクチャ リソースの動作を管理するポリシーが含まれます。また、ファブリック プロバイダーはリソースを1つ以上のユーザテナントに選択的に展開できます。インフラストラクチャ テナント ポリシーは、ファブリックの管理者が構成できます。
  - 管理テナントは、システムによって提供されますが、ファブリックの管理者が構成できます。ファブリック ノードのインバンドおよびアウトオブバンドの構成に使用するファブリック管理機能の動作を管理するポリシーが含まれます。管理テナントには、スイッチの管理ポートを介したアクセスを提供するファブリック データ パスの外部にある APIC/fabric 内部通信用のプライベートなアウトオブバウンド アドレス空間が含まれます。管理テナントにより、仮想マシン コントローラとの通信の検出と自動化が可能になります。
- アクセスポリシーは、ストレージ、コンピューティング、レイヤ2およびレイヤ3（ブリッジおよびルーテッド）接続、仮想マシン ハイパーバイザ、レイヤ 4 ～ レイヤ 7 のデバイ

スなどのリソースへの接続を提供するスイッチ アクセス ポートの動作を管理します。テナントが Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、Link Aggregation Control Protocol（LACP）、またはスパニングツリーなどのデフォルトのリンクで提供される構成以外のインターフェイス構成を必要とする場合、管理者はアクセスポリシーを構成して、リーフスイッチのアクセス ポートでそのような構成を有効にする必要があります。

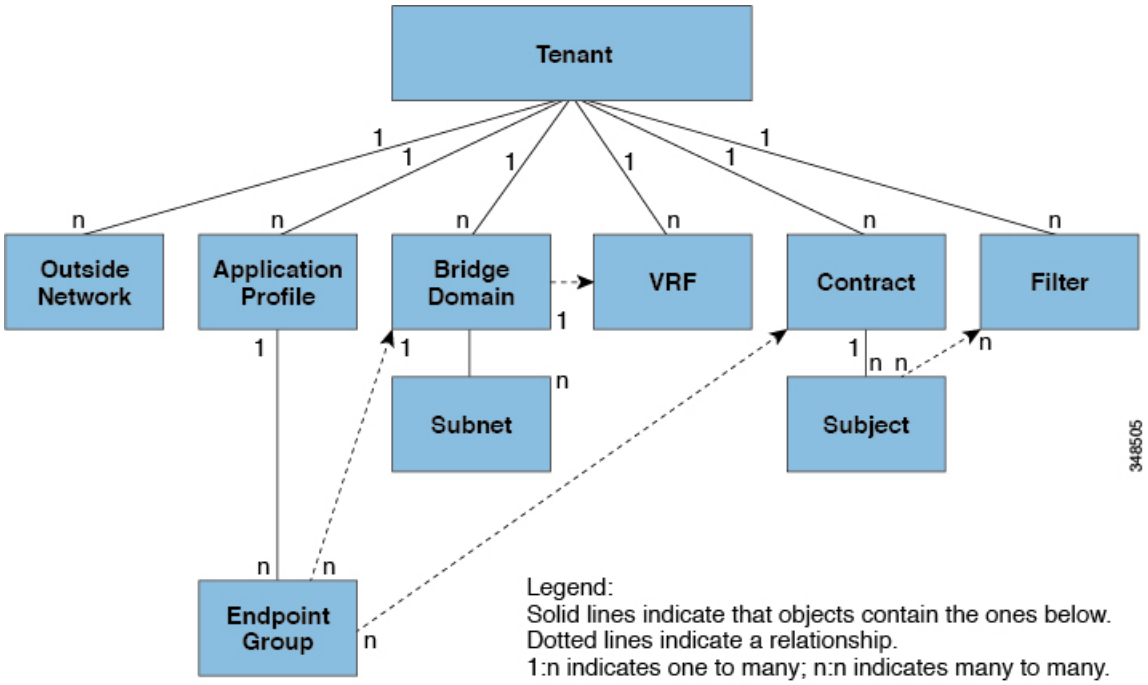
- ファブリック ポリシーは、Network Time Protocol（NTP）のサーバー同期、Intermediate System-to-Intermediate System Protocol（IS-IS）、ボーダーゲートウェイ プロトコル（BGP）のルートリフレクタ、ドメインネームシステム（DNS）などの機能を含む、スイッチファブリック ポートの動作を管理します。ファブリック MO には、電源、ファン、シャーシなどのオブジェクトが含まれます。
- 仮想マシン（VM）ドメインは、同様のネットワーキング ポリシー要件を持つ VM コントローラをグループ化します。VM コントローラは、VLAN または Virtual Extensible Local Area Network（VXLAN）のエリアおよびアプリケーションエンドポイント グループ（EPG）を共有できます。APIC はコントローラと通信し、のちに仮想ワークロードに適用されるポート グループなどのネットワーク構成を公開します。
- レイヤ 4 ～ レイヤ 7 のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムはダイナミックに応答することができます。ポリシーは、サービス デバイス パッケージとインベントリ管理機能を提供します。
- アクセス、認証、およびアカウンティング（AAA）ポリシーは、Cisco ACI ファブリックのユーザ権限、ロール、およびセキュリティ ドメインを管理します。

階層型ポリシー モデルは、REST API インターフェイスとうまく適合します。呼び出されると、API は MIT 内のオブジェクトで読み取りまたは書き込みを行います。URL は、MIT 内のオブジェクトを識別する識別名に直接マッピングします。MIT 内のデータは、XML または JSON でエンコードされた自己完結型の構造化ツリーテキスト ドキュメントとして説明できます。

テナント

テナント (`fvTenant`) は、アプリケーション ポリシーの論理コンテナで、管理者はドメインベースのアクセス コントロールを実行できます。テナントはポリシーの観点から分離の単位を表しますが、プライベート ネットワークは表しません。テナントは、サービス プロバイダーの環境ではお客様を、企業の環境では組織またはドメインを、または単にポリシーの便利なグループ化を表すことができます。次の図は、管理情報ツリー (MIT) のテナント部分の概要を示します。

図 *3:* テナント



テナントは相互に分離することも、リソースを共有することもできます。テナントに含まれる主要な要素は、フィルタ、コントラクト、外部ネットワーク、ブリッジ ドメイン、仮想ルーティングおよび転送 (VRF) インスタンス、エンドポイント グループ (EPG) を含むアプリケーション プロファイルです。テナントのエンティティはそのポリシーを継承します。VRF はコンテキストとも呼ばれ、それぞれを複数のブリッジ ドメインに関連付けることができます。

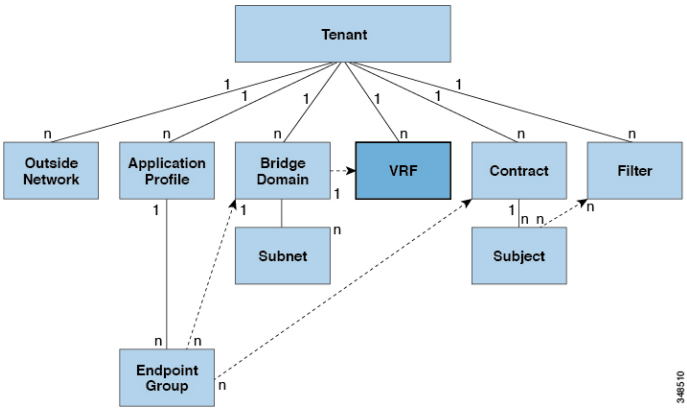
（注） APIC GUI のテナント ナビゲーション パスでは、VRF (コンテキスト) はプライベート ネットワークと呼ばれます。

テナントはアプリケーション ポリシーの論理コンテナです。ファブリックには複数のテナントを含めることができます。レイヤ 4 ～ 7 のサービスを展開する前に、テナントを設定する必要があります。ACI ファブリックは、テナント ネットワークに対して IPv4、IPv6、およびデュアル スタック構成をサポートします。

VRF

仮想ルーティングおよび転送（VRF）オブジェクト（`fvCtx`）またはコンテキストは、テナント ネットワーク（ APIC GUI のプライベート ネットワーク）と呼ばれます。テナントには、複数の VRF を含めることができます。VRF は、一意のレイヤ 3 フォワーディングおよびアプリケーション ポリシー ドメインです。次の図は、管理情報ツリー（MIT）内の VRF の場所とテナントの他のオブジェクトとの関係を示します。

図 *4 : VRF*



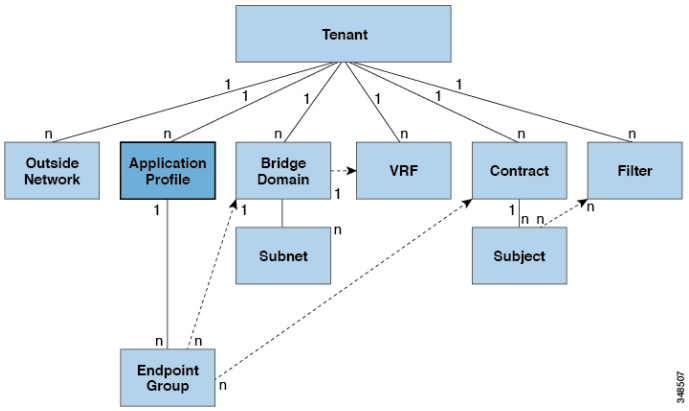
VRF は、レイヤ 3 のアドレス ドメインを定義します。VRF には 1 つ以上のブリッジ ドメインが関連付けられます。レイヤ 3 ドメイン内のすべてのエンドポイントが一意の IP アドレスを持っている必要があります。なぜなら、ポリシーで許可されている場合にこれらのデバイス間でパケットを直接転送できるためです。テナントには、複数の VRF を含めることができます。管理者が論理デバイスを作成した後、管理者はデバイス クラスタの選択基準ポリシーを提供する論理デバイスの VRF を作成できます。論理デバイスは、コントラクト名、グラフ名、またはグラフ内の関数ノード名に基づいて選択できます。

（注） APIC GUI では、VRF（`fvCtx`）は「コンテキスト」または「プライベートネットワーク」とも呼ばれます。

アプリケーション プロファイル

アプリケーション プロファイル（`fvAp`）は、ポリシー、サービス、およびエンドポイント グループ（EPG）間の関係を定義します。次の図は、管理情報ツリー（MIT）内のアプリケーション プロファイルの場所と、テナント内の他のオブジェクトとの関係を示します。

図 *5:* アプリケーション プロファイル



アプリケーション プロファイルには、1 つ以上の EPG が含まれます。最新のアプリケーションには、複数のコンポーネントが含まれます。たとえば、e-コマースアプリケーションには、Web サーバ、データベース サーバ、ストレージ エリア ネットワーク内にあるデータ、および金融取引を可能にする外部リソースへのアクセスが必要となる場合があります。アプリケーションプロファイルには、アプリケーションの機能の提供に論理的に関連する必要な数の（またはそれ以下の）EPG が含まれます。

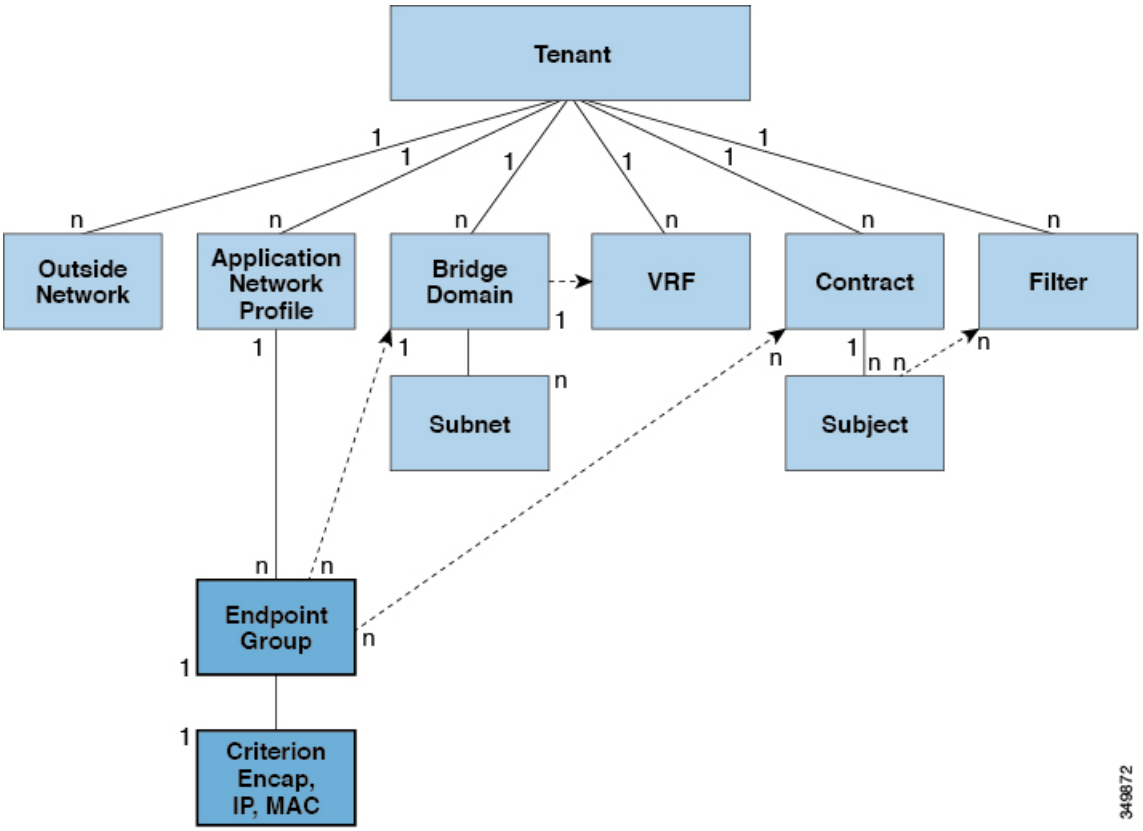
EPG は次のいずれかに従って組織化できます。

- 提供するアプリケーション（DNS サーバや SAP アプリケーションなど）（『*Cisco APIC REST API Configuration Guide*』の「*Tenant Policy Example*」を参照）。
- 提供する機能（インフラストラクチャなど）
- データセンターの構造内の場所（DMZ など）
- ファブリックまたはテナントの管理者が使用することを選択した組織化の原則

エンドポイント グループ

エンドポイント グループ（EPG）は、ポリシー モデルの最も重要なオブジェクトです。次の図は、管理情報ツリー（MIT）内のアプリケーション EPG の場所とテナント内の他のオブジェクトとの関係を示します。

図 *6 :* エンドポイント グループ



EPGは、エンドポイントの集合を含む名前付き論理エンティティである管理対象オブジェクトです。エンドポイントは、ネットワークに直接的または間接的に接続されるデバイスです。エンドポイントには、アドレス（ID）、ロケーション、属性（バージョンやパッチ レベルなど）があり、物理または仮想にできます。エンドポイントのアドレスを知ることで、他のすべての ID の詳細にアクセスすることもできます。EPG は、物理および論理トポロジから完全に分離されます。エンドポイントの例には、インターネット上のサーバ、仮想マシン、ネットワーク接続ストレージ、またはクライアントが含まれます。EPG 内のエンドポイント メンバシップは、ダイナミックまたはスタティックにできます。

ACI ファブリックには、次のタイプの EPG を含めることができます。

- アプリケーション エンドポイント グループ（`fvAEPg`）
- レイヤ 2 外部外側ネットワーク インスタンスのエンドポイント グループ（`l2extInstP`）
- レイヤ 3 外部外側ネットワーク インスタンスのエンドポイント グループ（`l3extInstP`）
- アウトオブバンド（`mgmtOoB`）またはインバンド（`mgmtInB`）アクセス用の管理エンドポイント グループ。

EPGには、セキュリティ、仮想マシンのモビリティ（VMM）、QoS、レイヤ4～レイヤ7サービスなどの共通のポリシー要件を持つエンドポイントが含まれます。エンドポイントは個別に設定および管理されるのではなく、EPG 内に配置され、グループとして管理されます。

ポリシーは EPG に適用されます。個々のエンドポイントに適用されることは絶対にありません。EPG は、APIC において管理者により静的に設定されるか、vCenter または OpenStack などの自動システムによって動的に設定されます。

（注） EPG がスタティック バインディング パスを使用する場合、この EPG に関連付けられるカプセル化 VLAN はスタティック VLAN プールの一部である必要があります。IPv4/IPv6 デュアルスタック設定の場合、IP アドレスのプロパティは `fvStCEp` MO の `fvStIp` 子プロパティに含まれます。IPv4 および IPv6 アドレスをサポートする複数の `fvStIp` を 1 つの `fvStCEp` オブジェクト下に追加できます。ACI を、IPv4 のみのファームウェアから、IPv6 をサポートするバージョンのファームウェアにアップグレードすると、既存の IP プロパティが `fvStIp` MO にコピーされます。

EPG の設定内容にかかわらず、含まれるエンドポイントに EPG ポリシーが適用されます。

ファブリックへの WAN ルータ接続は、スタティック EPG を使用する設定の 1 つの例です。ファブリックへの WAN ルータ接続を設定するには、関連付けられている WAN サブネット内のエンドポイントを含む `l3extInstP` EPG を管理者が設定します。ファブリックは、エンドポイントの接続ライフサイクルが経過する間に、検出プロセスを通して EPG のエンドポイントについて学習します。エンドポイントを学習すると、ファブリックは、それに基づいて `l3extInstP` EPG ポリシーを適用します。たとえば、WAN 接続クライアントがアプリケーション（`fvAEPg`）EPG 内でサーバとの TCP セッションを開始すると、`l3extInstP` EPG は、`fvAEPg` EPG Web サーバとの通信が始まる前に、そのクライアント エンドポイントにポリシーを適用します。クライアント サーバ TCP セッションが終わり、クライアントとサーバの間の通信が終了すると、そのエンドポイントはもうファブリック内に存在しません。

（注） リーフ スイッチが EPG 下の *static binding (leaf switches)* 用に設定されている場合は、次の制限が適用されます。

- スタティック バインディングをスタティック パスで上書きすることはできません。
- そのスイッチのインターフェイスをルーテッド外部ネットワーク（L3out）設定に使用することはできません。
- そのスイッチのインターフェイスに IP アドレスを割り当てることはできません。

VMware vCenter への仮想マシン管理接続は、ダイナミック EPG を使用する設定の 1 つの例です。ファブリックで仮想マシン管理ドメインが設定されると、vCenter は、必要に応じて仮想マシン エンドポイントを開始、移動、シャットダウンさせることのできる EPG の動的設定をトリガーします。

IP ベース EPG

カプセル化ベースの EPG が一般的に使用されますが、IP ベース EPG は、最長プレフィックス一致（LPM）分類ではサポートできない多数の EPG が必要なネットワークに適しています。IP ベース EPG では、LPM 分類とは異なり、EPG ごとにネットワーク/マスク範囲を割り当てる必要はありません。また、IP ベース EPG ごとに一意のブリッジドメインは必要ありません。IP ベースの EPG の構成手順は、Cisco AVS vCenter 構成で使用される仮想 IP ベースの EPG を構成する手順に似ています。

次に示す IP ベース EPG のガイドラインおよび制限事項に従ってください。

- IP ベース EPG は、APIC 1.1(2x) および ACI スイッチ 11.1(2x) リリース以降、次の Cisco Nexus N9K スイッチでサポートされています。
  - スイッチ名の末尾に「E」が付いているスイッチ（N9K-C9372PX-E など）。
  - スイッチ名の末尾に「EX」が付いているスイッチ（N9K-93108TC-EX など）。

  IP ベース EPG をサポートしていない古いスイッチに展開しようとすると、APIC で障害が発生します。
- IP ベース EPG は、特定の IP アドレスまたはサブネットに対して構成できますが、IP アドレスの範囲には構成できません。
- IP ベース EPG は、次のシナリオではサポートされていません。
  - 静的 EP 構成と組み合わせて使用します。
  - 外部のインフラストラクチャテナント（インフラ）構成はブロックされませんが、この場合はレイヤ 3 学習がないため、有効になりません。
  - レイヤ 2 のみのブリッジドメインでは、ルーティングされたトラフィックがないため、IP ベースの EPG は有効になりません。レイヤ 3 ブリッジドメインでプロキシ ARP が有効になっている場合、エンドポイントが同じサブネットにある場合でも、トラフィックはルーティングされます。したがって、この場合は IP ベース EPG が機能します。
  - 共有サービスと IP ベース EPG の両方に使用されるプレフィックスを持つ構成。

マイクロセグメンテーション

マイクロセグメンテーションでは、仮想マシンの属性、IP アドレス、または MAC アドレスに従って、複数の EPG のエンドポイントが、マイクロセグメント化された EPG に関連付けられます。仮想マシン属性には、VNic ドメイン名、VM 識別子、VM 名、ハイパーバイザ識別子、VMM ドメイン、データセンター、オペレーティングシステム、またはカスタム属性が含まれます。

マイクロセグメンテーションには、次のような利点があります。

- ライン レートを適用するステートレス ホワイト リスト ネットワーク アクセスセキュリティ。
- マイクロセグメントごとの粒度セキュリティ自動化により、ダイナミック レイヤー 4 ～ レイヤー 7 サービスの挿入と連鎖が可能。
- 幅広い仮想スイッチ環境でのハイパーバイザに依存しないマイクロセグメンテーション。
- 問題のある VM を検疫セキュリティ ゾーンに簡単に移動させる ACI ポリシー。
- ベアメタルおよび VM エンドポイントの EPG 内分離と組み合わせると、マイクロセグメンテーションは、アプリケーション階層内でポリシー駆動型の自動化された完全なエンドポイント分離を提供できます。

どの EPG についても、ACI ファブリック入力リーフスイッチは、入力ポートに関連付けられたポリシーに従って、パケットを EPG に分類します。マイクロセグメント化された EPG は、マイクロセグメント化された EPG ポリシーで指定された VM 属性、MAC アドレス、または IP アドレスに基づいて派生した個々の仮想または物理エンドポイントにポリシーを適用します。

EPG 内エンドポイント分離

EPG内エンドポイント分離ポリシーにより、仮想エンドポイントまたは物理エンドポイントが完全に分離されます。分離を適用した状態で稼働している EPG 内のエンドポイント間の通信は許可されません。分離を適用した EGP では、多くのクライアントが共通サービスにアクセスするときに必要な EPG カプセル化の数は低減しますが、相互間の通信は許可されません。

EPG の分離は、すべての Cisco Application Centric Infrastructure（ACI）ネットワーク ドメインに適用されるか、どれにも適用されないかの、どちらかになります。Cisco ACI ファブリックは接続エンドポイントに直接分離を実装しますが、ファブリックに接続されているスイッチはプライマリ VLAN（PVLAN）タグに従って分離規則を認識します。

（注） EPG 内エンドポイント分離を適用して EPG を設定した場合は、次の制限が適用されます。

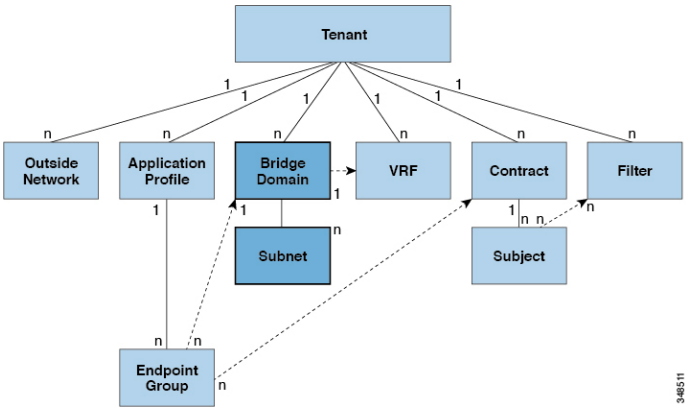
- 分離を適用した EPG 全体のすべてのレイヤ 2 エンドポイント通信がブリッジ ドメイン内にドロップされます。
- 分離を適用した EPG 全体のすべてのレイヤ 3 エンドポイント通信が同じサブネット内にドロップされます。
- トラフィックが、分離が適用されている EPG から分離が適用されていない EPG に流れている場合、QoS CoS の優先順位設定の保持はサポートされません。

BPDU は、EPG 内分離が有効になっている EPG を介して転送されません。したがって、Cisco ACI 上の独立した EPG にマッピングされている VLAN でスパニング ツリーを実行する外部レイヤ 2 ネットワークを接続すると、Cisco ACI は外部ネットワークのスパニング ツリーがレイヤ 2 ループを検出できなくなる可能性があります。この問題を回避するには、これらの VLAN 内の Cisco ACI と外部ネットワーク間に単一の論理リンクのみを設定します。

ブリッジ ドメインとサブネット

ブリッジ ドメイン（fvBD）は、ファブリック内のレイヤ 2 フォワーディングの構造を表します。次の図は、管理情報ツリー（MIT）内のブリッジ ドメインの場所とテナントの他のオブジェクトとの関係を示します。

図 7: ブリッジ ドメイン



ブリッジ ドメインは、VRF インスタンス（コンテキストまたはプライベート ネットワークとも呼ばれる）にリンクする必要があります。レイヤ 2 VLAN を除いて、少なくとも 1 つのサブネット（fvSubnet）が関連付けられている必要があります。フラッディングが有効な場合、ブリッジ ドメインは、一意のレイヤ 2 MAC アドレス空間とレイヤ 2 フラッド ドメインを定義します。VRF インスタンスが一意の IP アドレス空間を定義する一方で、そのアドレス空間は複数のサブネットで構成できます。これらのサブネットは、対応する VRF インスタンスを参照する 1 つ以上のブリッジ ドメインで定義されます。

ブリッジ ドメインまたは EPG の下のサブネットのオプションは次のとおりです。

- パブリック（*Public*）：サブネットをルーテッド接続にエクスポートできます。
- プライベート（*Private*）：サブネットはテナント内にのみ適用されます。
- 共有（*Shared*）：共有サービスの一部として、同じテナントまたは他のテナントにわたる複数の VRF インスタンスに対してサブネットの共有やエクスポートを行うことができます。共有サービスの例としては、異なるテナントの別の VRF インスタンスに存在する EPG へのルーテッド接続などがあります。これにより、トラフィックが VRF インスタンス間で双方向に移動することが可能になります。共有サービスを提供する EPG は、その EPG の下で（ブリッジ ドメインの下ではなく）サブネットを設定する必要があり、そのスコープは外部にアドバタイズするように設定し、VRF インスタンス間で共有する必要があります。

（注） 共有サブネットは、通信に含まれるVRFインスタンス全体で一意でなければなりません。EPG下のサブネットがレイヤ3外部ネットワーク共有サービスを提供する場合、このようなサブネットは、Cisco Application Centric Infrastructure（ACI）ファブリック内全体でグローバルに一意である必要があります。

ブリッジ ドメイン パケットの動作は次の方法で制御できます。

パケット タイプ	モード
ARP	**ARP フラッディング**は有効または無効にできます。フラッディングを行わない場合、ARPパケットはユニキャストで送信されます。 （注） `limitIpLearnToSubnets` を `fvBD` で設定すると、ブリッジ ドメインの構成済みサブネット内または共有サービス プロバイダーである EPG サブネット内にIPアドレスが存在する場合のみ、エンドポイントの学習がブリッジ ドメインに限定されます。
未知のユニキャスト	**L2 Unknown Unicast** は、**Flood** または **Hardware Proxy** になり得ます。 （注） ブリッジ ドメインが **L2 Unknown Unicast** を持っており、それが **Flood** に設定されている場合、エンドポイントが削除されると、システムはそれを両方のローカル リーフ スイッチから削除します。そして、**Clear Remote MAC Entries** を選択すると、ブリッジ ドメインが展開されているリモートのリーフ スイッチからも削除されます。この機能を使用しない場合、リモート リーフは、タイマーが時間切れになるまで、学習したこのエンドポイントの情報を保持します。 **L2 Unknown Unicast** の設定を変更すると、このブリッジ ドメインに関連付けられたEPGにアタッチされているデバイスのインターフェイス上で、トラフィックがバウンスします(アップ ダウンします)。

パケット タイプ	モード
未知の IP マルチキャスト	**L3 の不明なマルチキャスト フラッディング** **フラッド（Flood）**：パケットは入力および境界リーフ スイッチ ノードでのみフラッディングされます。N9K-93180YC-EX では、パケットは、ブリッジ ドメインが導入されているすべてのノードでフラッディングされます。 **最適化（Optimized）**：1 リーフあたり 50 のブリッジ ドメインのみサポートされます。この制限は N9K-93180YC-EX には該当しません。
L2 マルチキャスト、ブロードキャスト、ユニキャスト	**マルチ宛先フラッディング**、次のいずれかになり得ます。 • **BD でフラッド（Flood in BD）**：ブリッジ ドメインにフラッドします。 • **カプセル化でフラッド（Flood in Encapsulation）**：カプセル化でフラッドします。 • **ドロップ（Drop）**：パケットをドロップします。

（注） Cisco APIC リリース 3.1(1) 以降では、Cisco Nexus 9000 シリーズ スイッチで (EX と FX で終わる名前を持つものとそれ以降)、次のプロトコルのカプセル化のフラッディングまたはブリッジ ドメインにフラッディングが可能です：OSPF/OSPFv3、BGP、EIGRP、LACP、ISIS、IGMP、PIM、ST-BPDU、ARP/GARP、RARP、および ND。

ブリッジ ドメインは複数のスイッチにまたがることができます。ブリッジ ドメインには複数のサブネットを含めることができますが、サブネットは単一のブリッジ ドメイン内に含まれます。ブリッジ ドメイン（fvBD）の `limitIPLearnToSubnets` プロパティが `yes` に設定されていると、ブリッジ ドメインの設定済みサブネットのいずれかの中に IP アドレスがあるとき、または EPG が共有サービス プロバイダーである場合には EPG サブネット内に IP アドレスがあるときのみ、ブリッジ ドメイン内でエンドポイントの学習が行われます。サブネットは複数の EPG にまたがることができ、1 つ以上の EPG を 1 つのブリッジ ドメインまたはサブネットに関連付けることができます。ハードウェアのプロキシ モードでは、異なるブリッジ ドメインのエンドポイントがレイヤ 3 のルックアップ動作の一部として学習されると、そのエンドポイントに ARP トラフィックが転送されます。

ブリッジ ドメイン オプション

ブリッジ ドメインは、不明なユニキャスト フレームのフラッド モードで、またはこれらのフレームのフラッディングを排除する最適化されたモードで動作するように設定できます。フラッディング モードで使用する場合、レイヤ 2 の不明なユニキャスト トラフィックはブリッジ ドメイン（GIP）のマルチキャスト ツリーでフラッディングされます。最適化されたモードでブリッジ ドメインを動作するようにするには、ハードウェア プロキシに設定する必要があります。この状況では、レイヤ 2 の不明なユニキャスト フレームはスパイン プロキシ エニーキャスト VTEP アドレスに送信されます。

注意 不明なユニキャスト フラッディング モードから hw プロキシ モードに変更すると、ブリッジ ドメイン内のトラフィックが停止します。

ブリッジ ドメインで IP ルーティングが有効になっている場合、マッピング データベースは、MAC アドレスだけでなく、エンドポイントの IP アドレスを学習します。

レイヤ 3 の設定 ブリッジ ドメイン ()] パネルのタブには次のパラメータを設定するには、管理者が使用できます。

- **ユニキャスト ルーティング** ：この設定が有効になっているサブネット アドレスが設定されている場合は、ファブリックはデフォルト ゲートウェイの機能を提供して、トラフィックをルーティングします。ユニキャストルーティングを有効にすると、マッピングデータベースがこのブリッジドメインのエンドポイントに付与された IP アドレスと VTEP の対応関係を学習します。IP学習は、ブリッジドメイン内にサブネットが構成されているかどうかに左右されません。
- **サブネット アドレス** ：このオプションは、ブリッジ ドメインの SVI IP アドレス (デフォルト ゲートウェイ) を設定します。
- **制限のサブネット IP ラーニング** ：このオプションは、ユニキャスト リバース転送パス チェックに似ています。このオプションを選択すると、ファブリックはブリッジ ドメインに設定されている 1 以外のサブネットから IP アドレスを学習されません。

注意 有効化 **サブネットに制限 IP ラーニング** がブリッジ ドメイン内のトラフィックを停止します。

拡張 L2 専用モード：レガシーモード

Cisco Application Centric Infrastructure（ACI）では、VLAN が異なるリーフ ノードに展開されている限り、任意の目的で同じ VLAN ID を再利用できます。これにより、Cisco ACI ファブリックは、ファブリックとしての VLAN の理論上の最大数、4094 を超えることができます。ただし、これを実現するため、および基盤となる VxLAN 実装の複雑さを隠すために、個々のリーフノードに含めることのできる VLAN の数は少なくなります。このことは、リーフノードあたりの VLAN の密度が必要な場合に問題の原因となる可能性があります。このようなシナリオでは、ブリッジ ドメインで以前はレガシーモードと呼ばれていた、拡張 L2 専用モードを有効

にできます。拡張 L2 専用モードのブリッジドメインでは、リーフノードごとに多数の VLAN を使用できます。ただし、このようなブリッジ ドメインにはいくつかの制限があります。

拡張 L2 専用モードとそれ以外のモードで、リーフ ノードごとにサポートされる VLAN またはブリッジ ドメインの数については、ご使用のリリースの Verified Scalability Guideを参照してください。

拡張 L2 専用モードの制限事項

レガシー モードまたは拡張 L2 専用モードの制限は次のとおりです。

- ブリッジ ドメインには、1 つの EPG と 1 つの VLAN のみを含めることができます。
- ユニキャスト ルーティングはサポートされていません。
- コントラクトはサポートされていません。
- VMM 統合のダイナミック VLAN 割り当てはサポートされていません。
- サービス グラフはサポートされていません。
- QoS ポリシーはサポートされていません。
- ブリッジ ドメインは、スタンドアロン Cisco NX-OS では基本的に VLAN として動作します。

拡張 L2 専用モードの設定

次に、拡張 L2 専用 モードでブリッジ ドメインを設定する際の考慮事項を示します。

- VLAN ID はブリッジドメインで設定されます。
- EPG で設定された VLAN ID は上書きされます。
- 既存のブリッジ ドメインで拡張 L2 専用モードの有効と無効を切り替えると、サービスに影響します。

  VLAN ID が変更前に使用されていたものと異なる場合、Cisco Application Policy Infrastructure Controller（APIC）は自動的にブリッジ ドメインの展開解除と再展開を行います。

  モード変更の前後で同じ VLAN ID が使用された場合、Cisco APIC はブリッジ ドメインの自動的な展開解除と再展開は行いません。手動でブリッジ ドメインを展開解除して再展開する必要があります。これは、 EPG で静的ポート設定を削除して再作成することで実行できます。
- 拡張 L2 専用モードの VLAN ID を変更する場合は、まずモードを無効にしてから、新しい VLAN ID で拡張 L2 専用モードを有効にする必要があります。

ブリッジ ドメインごとの IP 学習の無効化

ブリッジ ドメインの IP データプレーン学習は無効にできます。MAC 学習は引き続きハードウェアで行われますが、IP 学習は ARP/GARP/ND プロセスからのみ行われます。この機能は、

Cisco APIC 3.1 リリースで主にサービス グラフ ポリシーベース リダイレクト（PBR）展開用に導入されましたが、VRF インスタンスごと（Cisco APIC リリース 4.0）ブリッジ ドメインサブネットごと、（Cisco APIC リリース 5.2）、および EPG ごと（Cisco APIC リリース 5.2）に IP データプレーン学習を無効にする機能に置き換えられました。ブリッジ ドメインごとに IP ラーニングを無効にすることは推奨されません。また、PBR で使用する場合を除き、サポートされません。

ブリッジ ドメインごとに IP 学習を無効化するには、次の注意事項と制限事項を参照してください。

- リモート リーフ スイッチで送信元 IP アドレスが S,G 情報を入力するように学習していないため、レイヤ 3 マルチキャストはサポートされていません。
- DL ビットが iVXLAN ヘッダーで設定されているため、MAC アドレスはリモート リーフ スイッチのデータ パスから学習されません。そのため、ブリッジ ドメインが展開されているファブリックで、リモート リーフ スイッチからすべてのリーフ スイッチに、不明なユニキャスト トラフィックがフラッディングされることになります。エンドポイントデータプレーン学習が無効になっている場合は、この状況への対策として、プロキシモードでブリッジ ドメインを構成することをお勧めします。
- ARP がフラッド モードであり、GARP ベースの検出を有効にする必要があります。
- IP 学習を無効にすると、対応する VRF インスタンスでレイヤ 3 エンドポイントがフラッシュされません。同じリーフ スイッチを恒久的に指すエンドポイントになる可能性があります。この問題を解決するには、すべてのリーフ スイッチで、 この VRF 内のすべてのリモート IP エンドポイントをフラッシュします。

ブリッジ ドメインの構成を変更して、データプレーン学習を無効にしても、以前にローカルに学習したエンドポイントはフラッシュされません。これにより、既存のトラフィック フロー中断の影響は限られます。Cisco ACI リーフ スイッチが特定の送信元 MAC を持つトラフィックをエンド ポイント保持ポリシーよりも長く見ない場合、MAC が学習したエンドポイントは通常どおりエージングします。

（注） IP データプレーン学習を無効にすると、トラフィック転送の結果としてエンドポイントの IP 情報が更新されることはなくなりますが、Cisco ACI は ARP/ND を使用してエンドポイント IP 情報を更新できます。つまり、ローカルエンドポイントのエージング（設定変更前に学習されたか、設定変更後に学習されたか）は、通常のエージングとは若干異なり、`[システム (System)] > [システム設定 (System Settings)] > [エンドポイント制御 (Endpoint Controls)] > [IPエージング (IP Aging)]` にも依存します。

`IP エージング`が無効の場合、すでに学習されたエンドポイント MAC と一致する送信元 MAC からのトラフィックは、エンドポイントテーブルの MAC アドレス情報を更新し、その結果、IP 情報も更新します（これは IP データプレーンの学習が有効になっている場合と同じです）。

`IP エージング`が有効の場合、Cisco ACI はエンドポイント IP アドレスを個別にエージング アウトします（これは IP データプレーン学習が有効になっている場合と同じです）が、すでに学習したエンドポイントとマッチする既知の送信元 MAC および IP からのトラフィックにより、エンドポイントテーブルの MAC アドレス情報は更新されるのに対し、IP 情報は更新されないという点で、IP データプレーン学習を有効にした構成とは異なります。

接続可能エンティティ プロファイル

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

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

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

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

接続可能エンティティ プロファイル（AEP）は、同様のインフラストラクチャ ポリシー要件を持つ外部エンティティのグループを表します。インフラストラクチャ ポリシーは、Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、Link Aggregation Control

Protocol（LACP）などのさまざまなプロトコル オプションを設定する物理インターフェイス ポリシーで構成されます。

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

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

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

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

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

VLAN と EPG

アクセス ポリシーによる VLAN から EPG への自動割り当て

テナント ネットワーク ポリシーがファブリックのアクセス ポリシーと別に設定される一方で、テナント ポリシーの基盤となるアクセス ポリシーが整わないとテナント ポリシーはアクティブ化されません。ファブリック アクセス外向きインターフェイスは、仮想マシン コントローラなどの外部デバイス、ハイパーバイザ、ホスト、ルータ、またはファブリック エクステンダ (FEX) と接続します。アクセス ポリシーにより、管理者はポート チャネルおよび仮想ポート

チャネル、LLDP、CDP、LACP などのプロトコル、モニタリングや診断などの機能を設定することができます。

図 *8*: アクセス ポリシーとエンドポイント グループの関連付け

ポリシー モデルでは、vlan の Epg 緊密に結合されています。トラフィックが流れるようにするには、物理、VMM、L2out、L3out、またはファイバ チャネル ドメイン内に VLAN を持つリーフ ポートに EPG を展開する必要があります。詳細については、ネットワーク ドメインを参照してください。

ポリシー モデルでは、EPG に関連付けられているドメイン プロファイルには、VLAN インスタンス プロファイルが含まれています。ドメイン プロファイルには、両方の VLAN インスタンス プロファイル (VLAN プール) および attacheable アクセス エンティティ プロファイル (AEP) アプリケーション Epg に直接と関連付けられているが含まれています。AEP は、すべてのポートの [接続されている、および Vlan の割り当てのタスクを自動化するに関連付けられているアプリケーション Epg を展開します。大規模なデータセンター数千の Vlan の数百のプロビジョニング仮想マシンのアクティブなは簡単に、中に ACI ファブリックは VLAN プールから、VLAN Id を自動的に割り当てることができます。これは、膨大な従来データセンターで Vlan をトランキングと比較して、時間を節約できます。

VLAN の注意事項

EPG トラフィックがフローは、Vlan の設定には次のガイドラインを使用します。

- 複数のドメインは、VLAN プールを共有できますが、1 つのドメインは、1 つの VLAN プールにのみ使用できます。
- 1 つのリーフ スイッチで同じ VLAN のカプセル化を複数の Epg を展開するを参照してください。 ポート単位の VLAN （24 ページ） 。

インターフェイス上のネイティブ 802.1p およびタグ付き EPG

アクセス（802.1p またはタグなし）モードを割り当てるときは、次のガイドラインに従って、タグなしまたは 802.1p パケットを必要とするデバイスが ACI リーフスイッチのアクセス ポートに接続されたときに想定通りに動作するようにします。

これらのガイドラインは、単一のリーフスイッチのポートに展開された EPG に適用されます。EPG が異なるスイッチに展開されている場合、これらの制限は適用されません。

- APIC GUI では、ポートの VLAN を EPG に割り当てるときに、**[トランク（Trunk）]**、**[アクセス（802.1p）（Access（802.1p））]**、または **アクセス（タグなし）（Access（Untagged））]** のいずれかの VLAN モードを割り当てることができます。
- 1 つのポートで許可される 802.1p VLAN またはタグなし VLAN は 1 つだけです。どちらか一方の場合もありますが、両方の場合はありません。

- 第 1 世代スイッチの場合、リーフスイッチのいずれかのポートに展開された EPG がアクセス（タグなし）モードで構成されている場合、EPG によって使用されるすべてのポートは、同じリーフスイッチとその VPC ピア（存在する場合）でタグ付けされていない必要があります。 第 2 世代スイッチ（-EX、-FX、または -FX2 サフィックス付き）では、タグなしポートとタグ付きポートを組み合わせて使用できます。
- **[アクセス（タグなし）（Access（Untagged））]** モードのポートに展開された EPG を使用して、同じポートの **[トランク（Trunk）]** モードで（タグ付き）VLAN 番号を使用して異なる EPG を展開できます。

リーフスイッチ ポートが **[アクセス（802.1p）（Access（802.1p））]** または **[アクセス（タグなし）（Access（Untagged））]** モードとして構成されている単一の EPG に関連付けられている場合、スイッチに応じて、トラフィック処理にいくつかの違いがあります。

第 1 世代スイッチ

- ポートが **アクセス（802.1p）** モードで構成されている場合：
  - 出力時に、アクセス VLAN がポートに展開された唯一の VLAN である場合、トラフィックはタグ付けされません。
  - 出力で、ポートにタグなしの EPG とともに展開された他の（タグ付き）VLAN がある場合、その EPG からのトラフィックはタグ付きゼロです。
  - 出力では、ポートに構成されている 1 つ以上の VLAN タグに関係なく、すべての FEX ポートのトラフィックはタグ付けされていません。
  - ポートは、タグなし、タグ付き、または 802.1p モードの入力トラフィックを受け入れます。
- ポートが **アクセス（タグなし）** モードで構成されている場合：
  - 出力では、EPG からのトラフィックはタグなしです。
  - ポートは、タグなし、タグ付き、または 802.1p の入力トラフィックを受け入れます。

第 2 世代スイッチ

第 2 世代以降のスイッチは、**[アクセス（タグなし）（Access（Untagged））]** モードと **[アクセス（802.1p）（Access（802.1p））]** モードを区別しません。EPG がタグなしまたは 802.1p モードで構成された第 2 世代ポートに展開されている場合：

- 出力では、トラフィックはこれが展開されているノードで常にタグなしです。
- ポートは、タグなし、タグ付き、または 802.1p モードの入力トラフィックを受け入れます。

ポートでの VLAN モードの組み合わせ：3.2(3i) 以前の Cisco APIC リリースを実行する第 1 世代および第 2 世代のハードウェア

1 つの EPG でサポートされる VLAN モードの組み合わせ

VLAN モードで、ポート 1 上の EPG 1 の場合：	異なるポートの EPG 1 では、次の VLAN モードが許可されます。
トランク	トランクまたは 802.1p
タグなし	タグなし
802.1p	トランクまたは 802.1p

複数の EPG でサポートされる VLAN モードの組み合わせ

VLAN モードで、ポート 1 上の EPG 1 の場合：	ポート 2 の EPG 1 では、次のモードが許可されます。	ポート 1 の EPG 2 では、次のモードが許可されます。
タグなし	タグなし	トランク
802.1p	トランクまたは 802.1p	トランク
トランク	802.1p またはトランク	トランクまたは 802.1p またはタグなし

ポートでの VLAN モードの組み合わせ：Cisco APIC リリース 3.2(3i) 以降を実行する第 2 世代ハードウェア

1 つの EPG でサポートされる VLAN モードの組み合わせ

VLAN モードで、ポート 1 上の EPG 1 の場合：	異なるポートの EPG 1 では、次の VLAN モードが許可されます。
トランク	トランク（タグ付き）、タグなし、または 802.1p
タグなし	タグなし、または 802.1p またはトランク（タグ付き）
802.1p	トランク（タグ付き）または 802.1p またはタグなし

複数の EPG でサポートされる VLAN モードの組み合わせ

VLAN モードで、ポート 1 上の EPG 1 の場合：	ポート 2 の EPG 1 では、次のモードが許可されます。	ポート 1 の EPG 2 では、次のモードが許可されます。
タグなし	タグなし、または 802.1p またはトランク（タグ付き）	トランク（タグ付き）

VLAN モードで、ポート 1 上の EPG 1 の場合：	ポート 2 の EPG 1 では、次のモードが許可されます。	ポート 1 の EPG 2 では、次のモードが許可されます。
802.1p	トランク（タグ付き）または 802.1p またはタグなし	トランク（タグ付き）
トランク	802.1p またはトランク（タグ付き）またはタグなし	トランク（タグ付き）または 802.1p またはタグなし

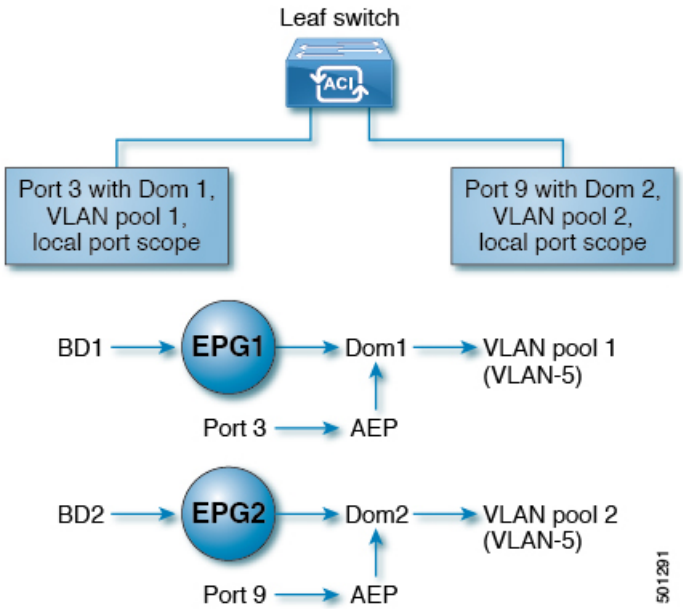
（注） タグなしのネイティブ VLAN でトラフィックを送信する特定の古いネットワーク インターフェイス カード（NIC）は、VLAN 0 としてタグ付けされたリターン トラフィックをドロップします。これは通常、トランク ポートとして構成されたインターフェイスでのみ問題になります。ただし、アクセス ポートのアタッチ可能エンティティ プロファイル（AEP）がインフラ VLAN を伝送するように構成されている場合、アクセス ポートとして構成されていても、トランク ポートとして扱われます。このような状況では、ネットワーク フロー エンジン（NFE）カードを備えたスイッチからネイティブ VLAN で送信されたパケットは VLAN 0 としてタグ付けされ、古いスイッチの NIC はパケットをドロップする可能性があります。この問題に対処するオプションは次のとおりです。

- AEP からインフラ VLAN を削除します。
- ポートで「ポート ローカル スコープ」を構成します。これにより、ポートごとの VLAN 定義が可能になり、NFE を搭載したスイッチがネイティブ VLAN 上でタグなしでパケットを送信できるようになります。

ポート単位の VLAN

v1.1 リリースより前の ACI バージョンでは、特定の VLAN カプセル化はリーフ スイッチ上の単一の EPG だけにマッピングされます。同じリーフ スイッチ上に同じ VLAN カプセル化を持つ第 2 の EPG があると、ACI でエラーが発生します。

v1.1 リリース以降では、次の図と同様、ポート単位の VLAN 設定で、特定のリーフ スイッチ (または FEX) 上に複数の EPG を同じ VLAN カプセル化で展開することができます。



単一のリーフ スイッチ上で、同じカプセル化番号を使用する複数の EPG の展開を有効にするには、次の注意事項に従ってください。

- EPG は、さまざまなブリッジ ドメインに関連付けられている必要があります。
- EPG は、さまざまなポートに展開する必要があります。
- ポートと EPG の両方が、VLAN 番号が含まれている VLAN プールに関連付けられている同じドメインに関連付けられている必要があります。
- ポートは `portLocal` VLAN スコープで設定されている必要があります。

たとえば、上の図の ポート 3 と 9 上に展開されている EPG のポート単位の VLAN で、両方が VLAN-5 を使用していれば、ポート 3 と EPG1 は Dom1 (プール 1) に、ポート 9 と EPG2 は Dom2 (プール 2) に関連付けられます。

ポート 3 からのトラフィックは EPG1 に関連付けられ、ポート 9 からのトラフィックは EPG2 に関連付けられます。

これは、外部レイヤ 3 外部接続用に設定されたポートには適用されません。

EPG に複数の物理ドメインがあり、VLAN プールが重複している場合は、EPG をポートに展開するために使用される AEP に複数のドメインを追加しないでください。これにより、トラフィック転送の問題が回避されます。

EPG に重複する VLAN プールを持つ物理ドメインが 1 つしかない場合、複数のドメインを単一の AEP に関連付けることができます。

入力および出力の両方向で個別の（ポート、VLAN）変換エントリの割り当てが可能なのは、`vlanScope` が `portlocal` に設定されているポートだけです。特定のポートで `vlanScope` が `portGlobal` (デフォルト) に設定されている場合には、EPG で使用される各 VLAN は、特定のリーフ スイッチ上で一意のものである必要があります。

（注） マルチ スパニング ツリー (MST) で設定されているインターフェイス上では、ポート単位の VLAN はサポートされていません。このツリーでは、VLAN ID が 1 つのリーフ スイッチ上で一意であること、そして VLAN の範囲がグローバルであることを必要とするからです。

同じリーフ スイッチで EPG に使用されていた VLAN 番号の再利用

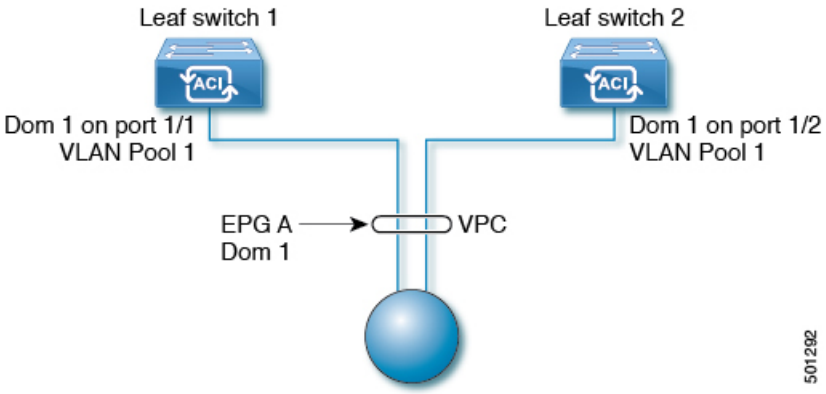
以前に、リーフ スイッチのポートに展開されている EPG 用に VLAN を設定していて、同じ VLAN 番号を同じリーフ スイッチの異なるポートの異なる EPG で再利用する場合には、中断なしでセットアップできるようにするため、次の例に示すようなプロセスに従ってください。

この例では、EPGは以前、9 ～ 100 の範囲の VLAN プールを含むドメインに関連付けられていたポートに展開されていました。ここで、9 ～ 20 からの VLAN カプセル化を使用する EPG を設定したいとします。

1. 異なるポート (たとえば、9 ～ 20 の範囲) で新しい VLAN プールを設定します。
2. ファイアウォールに接続されているリーフ ポートを含む新しい物理的なドメインを設定します。
3. ステップ 1 で設定した VLAN プールに物理的なドメインを関連付けます。
4. リーフ ポートの VLAN の範囲を `portLocal` として設定します。
5. 新しい EPG (この例ではファイアウォールが使用するもの) を、ステップ 2 で作成した物理ドメインに関連付けます。
6. リーフ ポートで EPG を展開します。

vPC に展開された EPG の VLAN ガイドライン

図 9 : vPC の 2 つのレッグの VLAN



EPG を vPC に展開する場合は、vPC の 2 つのレッグのリーフ スイッチ ポートに割り当てられた同じドメイン（同じ VLAN プール）に関連付ける必要があります。

この図では、EPG A は、リーフ スイッチ 1 およびリーフ スイッチ 2 のポートに展開されている vPC に展開されています。2 本のリーフ スイッチ ポートおよび EPG は、すべて同じ VLAN プールが含まれている同じドメインに関連付けられています。

カプセル化によるすべてのプロトコルおよびプロキシARPのカプセル化のフラッディングを設定する

Cisco Application Centric Infrastructure（ACI）は、ブリッジ ドメインをレイヤ 2 ブロードキャスト境界として使用します。各ブリッジ ドメインには複数のエンドポイント グループ（EPG）を含めることができ、各 EPG は複数の仮想ドメインまたは物理ドメインにマッピングできます。各 EPG は、ドメインごとに異なる VLAN カプセル化プールを使用することもできます。各 EPG は、ドメインごとに異なる VLAN または VXLAN カプセル化プールを使用することもできます。

通常、ブリッジ ドメイン内に複数の EPG を配置すると、ブロードキャスト フラッディングはブリッジ ドメイン内のすべての EPG にトラフィックを送信します。EPG はエンドポイントをグループ化し、特定の機能を実行するためにトラフィックを管理するために使用されるものなので、ブリッジ ドメイン内のすべての EPG に同じトラフィックを送信することは必ずしも実用的ではありません。

カプセル化でのフラッディングは、ネットワーク内のブリッジ ドメインを統合するのに役立ちます。この機能は、EPG が関連付けられている仮想ドメインまたは物理ドメインのカプセル化に基づいて、ブリッジ ドメイン内のエンドポイントへのブロードキャスト フラッディングを制御できるようにするからです。

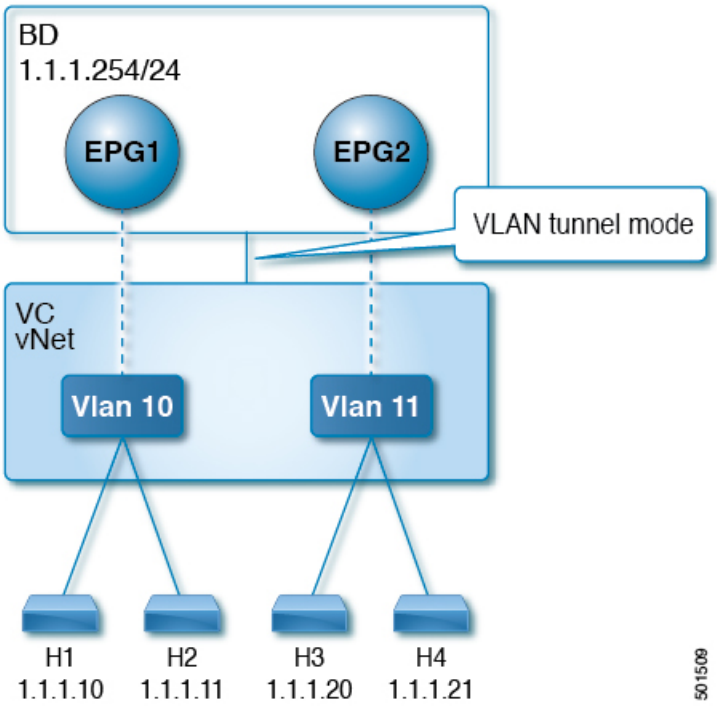
カプセル化でのフラッディングでは、同じブリッジ ドメインにおける異なる EPG のエンドポイント間の通信を許可するために、ブリッジ ドメインにサブネットと IP ルーティングを構成する必要があり、Cisco ACI がプロキシ ARP の役割を果たします。

VLAN カプセル化を使用したカプセル化でのフラッディングの使用例

カプセル化のフラッディングは、外部デバイスが VLAN に依存しない MAC 学習のために vNet ごとに 1 つの MAC アドレスが維持される仮想接続 トンネル モードを使用している場合によく用いられます。

トンネル モードで複数の VLAN を使用すると、いくつかの課題を導入できます。次の図に示すように、単一のトンネルでCisco ACIを使用する一般的な導入では、1 つのブリッジ ドメインの下に複数の EPG があります。この場合、特定のトラフィックがブリッジ ドメイン内（つまりすべての EPG 内）でフラッディングし、MACがあいまいになって転送エラーが発生するリスクがあります。

図 *10 : VLAN*トンネルモードの*Cisco ACI*の課題



このトポロジでは、ブレードスイッチ（この例では仮想接続）に、1つのアップリンクを使用してCisco ACIリーフノードに接続する単一のトンネルネットワークが定義されています。このリンクでは、2 人のユーザの VLAN、VLAN 10 と VLAN 11 が行われます。サーバーのゲートウェイがCisco ACIクラウドの外部にあるため、ブリッジ ドメインはフラッディング モードに設定されます。次のプロセスで ARP 交渉が発生します。

- サーバは、VLAN 10 ネットワーク経由で 1 つの ARP ブロードキャスト要求を送信します。
- ARP パケットは、外部のサーバに向かってトンネル ネットワークを通過し、そのダウンリンクから学習した送信元 MAC アドレスを記録します。
- その後、サーバーはアップリンクからCisco ACIリーフスイッチにパケットを転送します。
- Cisco ACIファブリックは、アクセスポート VLAN 10に着信する ARP ブロードキャスト パケットを確認し、EPG1 にマッピングします。
- ブリッジ ドメインは ARP パケットをフラッディングするように設定されているため、パケットはブリッジ ドメイン内でフラッディングされます。したがって、両方の EPG が同じブリッジ ドメイン内にあるため、これらのポートにフラッディングされます。
- 同じ ARP ブロードキャスト パケットは、同じアップリンクで復帰します。
- ブレード スイッチは、このアップリンクからの元の送信元 MAC アドレスを認識します。

結果：ブレード スイッチは、単一の MAC 転送テーブル内のダウンリンク ポートとアップリンク ポートの両方から学習した同じMACアドレスを持ち、トラフィックが中断します。

推奨される解決策

カプセル化オプションのフラッディングは、ブリッジドメイン内のフラッディング トラフィックを単一のカプセル化に制限するために使用されます。EPG1/VLAN X and EPG2/VLAN Y が同じブリッジドメインを共有し、カプセル化でのフラッディングが有効になっている時、カプセル化フラッディング トラフィックは他の EPG/VLAN に到達しません。

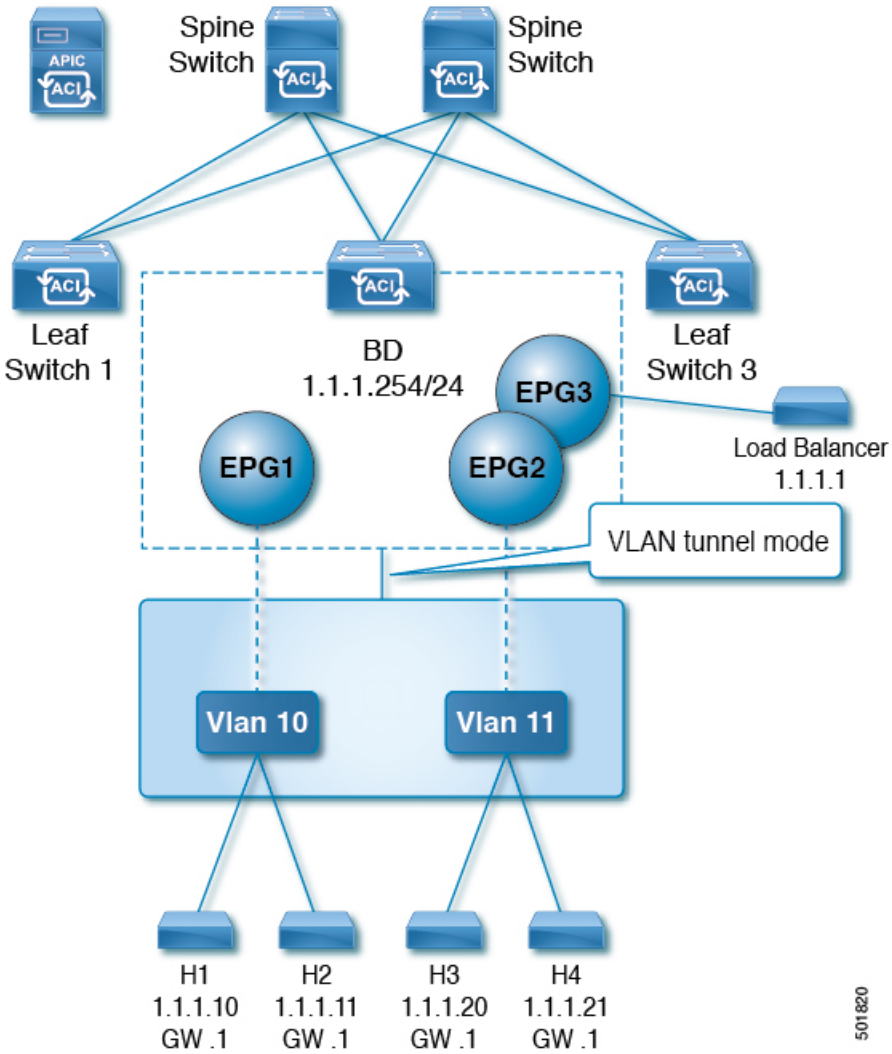
Cisco Application Policy Infrastructure Controller（APIC）リリース 3.1(1) 以降、Cisco Nexus 9000 シリーズスイッチ（名前の末尾が EX および FX 以降）では、すべてのプロトコルがカプセル化されます。また、VLAN 間のトラフィックのブリッジ ドメインでフラッディングが有効になっている場合、プロキシ ARP は MAC フラップの問題が発生しないようにします。また、すべてのフラッディング（ARP、GARP、およびBUM）をカプセル化に制限します。この制限は、有効になっているブリッジ ドメイン下のすべての EPG に適用されます。

（注） Cisco APIC APIC リリース 3.1 (1) より前のリリースでは、これらの機能はサポートされていません（カプセル内でフラッディングするとき含まれるプロキシ ARP およびすべてのプロトコル）。以前の Cisco APIC リリースまたは以前の世代のスイッチ（名前に EX または FX がない）では、カプセル化でフラッディングを有効にしても機能しません。情報障害は生成されませんが、Cisco APIC はヘルス スコアを 1 減らします。

（注） Cisco APIC リリース 3.2(5) 以降では、VXLAN カプセル化に関連付けられた EPG のカプセル化でフラッディングを設定できます。以前は、VLAN のみが仮想ドメインのカプセル化でのフラッディングでサポートされていました。ブリッジ ドメインまたは EPG を作成または変更するときに、カプセル化でのフラッディングを設定します。

推奨される解決策は、外部スイッチを追加して、1 つのブリッジ ドメインで複数の EPG をサポートすることです。外部のスイッチがある 1 つのブリッジ ドメイン下で複数の EPG を持つこの設計は、次の図に示されています。

図 *11*：外部のスイッチがある *1* つのブリッジ ドメイン下で複数の *EPG* を持つ設計



同じブリッジ ドメイン内では、一部の EPG をサービス ノードにすることができ、他の EPG にはカプセル化でのフラッディングを設定できます。ロード バランサは別の EPG に存在します。ロード バランサは EPG からパケットを受信し、その他の EPG に送信します（プロキシ ARP はなく、カプセル内のフラッディングは発生しません）。

マルチ宛先プロトコル トラフィック

EPG/ブリッジ ドメイン レベルのブロードキャスト セグメンテーションは、次のネットワーク制御プロトコルでサポートされます。

- OSPF
- EIGRP
- LACP
- IS-IS

- BGP
- IGMP
- PIM
- STP BPDU（EPG 内フラッディング）
- ARP/GARP（ARP プロキシによって制御）
- ND

カプセル化でのフラッディングの制限事項

すべてのプロトコルのカプセル化でのフラッディングには、次の制限が適用されます。

- カプセルのフラッディングは、ARP ユニキャスト モードでは機能しません。
- このリリースでは、ネイバー送信要求（プロキシ NS/ND）はサポートされていません。
- プロキシアドレス解決プロトコル（ARP）は暗黙的に有効にされるため、ARP トラフィックは異なるカプセル化間の通信のために CPU に送信できます。

  ARP トラフィックを処理するために異なるポートに均等に配信されるようにするには、ポート単位のコントロール プレーン ポリシング（CoPP）を有効にします。
- カプセル化でのフラッディングは、フラッド モードのブリッジ ドメインおよびフラッド モードの ARP でのみサポートされます。ブリッジ ドメイン スパイン プロキシ モードはサポートされていません。
- IPv4 レイヤ 3 マルチキャストはサポートされていません。
- カプセル化でのフラッディングが有効な場合でも、IPv6 NS/NDプロキシはサポートされません。その結果、同じ IPv6 サブネット下にあっても、カプセル化が異なる EPG に存在する 2 つのエンドポイント間の接続は、機能しないことがあります。
- 別の VLAN への仮想マシンの移行には、時間的な問題（60 秒）があります。別の VLAN または VXLAN への仮想マシンの移行には、時間的な問題（60 秒）があります。
- 仮想マシンの IP アドレスが、ファイアウォールの IP アドレスではなく、ゲートウェイの IP アドレスに変更された場合、ファイアウォールはバイパスされるため、ファイアウォールをゲートウェイにする仮想マシン間の通信セットアップは推奨されません。
- 以前のリリースではサポートされていません（以前と現在のリリース間の相互運用もサポートされていません）。
- 古い世代アプリケーション リーフ エンジン（ALE）とアプリケーション スパイン エンジン（ASE）を使用した混合モード トポロジは推奨されません。また、カプセル化でのフラッディングではサポートされません。同時に有効にすると、QoS の優先順位が適用されるのを防ぐことができます。
- 同じマルチサイト ドメインの一部であるCisco ACIファブリック全体に拡張された EPG とブリッジドメインでは、カプセル化でのフラッディングはサポートされません。ただし、

Cisco ACIファブリックでローカルに定義された EPG とブリッジ ドメインでは、カプセル化でのフラッディングは引き続き機能し、完全にサポートされています。Cisco ACIファブリックと、そのファブリックに関連付けられたリモート リーフ スイッチ間でストレッチされる EPG またはブリッジ ドメインにも、同じ考慮事項が適用されます。

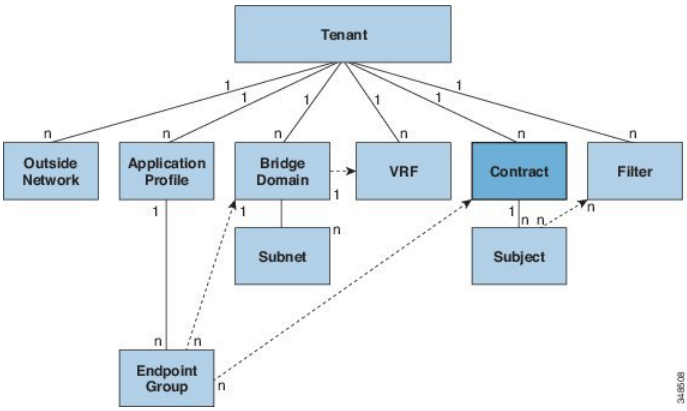
- マイクロセグメンテーションがいずれかの形式で構成されている EPG では、カプセル化でのフラッディングはサポートされません。これには、EPG 内分離、VMM ドメインでの「マイクロセグメンテーションを許可する」、マイクロセグメンテーション EPG、EPG 内コントラクトが含まれます。
- 共通パーベイシブ ゲートウェイでは、カプセル化でのフラッディングはサポートされていません。Cisco APIC Layer 3 Networking Configuration Guide の「Common Pervasive Gateway」の章を参照してください。
- ブリッジ ドメインのすべてのEPGでカプセル化でのフラッディングを設定する場合は、ブリッジ ドメインでもカプセル化でのフラッディングを設定してください。
- IGMP スヌーピングは、カプセル化でのフラッディングではサポートされません。
- Cisco ACIにおいては、カプセル化でのフラッディングのために設定された EPG で受信されるパケットのフラッディングを、（カプセル化ではなく）ブリッジ ドメインで生じさせる条件が存在します。これは、管理者がカプセル化でのフラッディングを EPG で直接設定したか、ブリッジ ドメインで設定したかに関係なく発生します。この転送動作の条件は、入力リーフ ノードに宛先MACアドレスのリモートエンドポイントがあり、出力リーフ ノードに対応するローカル エンドポイントがない場合です。これは、インターフェイスのフラッピング、STP TCNによるエンドポイント フラッシュ、過剰な移動のためにブリッジ ドメインで学習が無効になっているなどの理由で発生する可能性があります。

  4.2(6o) 以降の 4.2(6)リリース、4.2(7m) 以降の 4.2(7) リリース、および 5.2(1g) 以降のリリースでは、この動作が拡張されました。管理者が（EPG ではなく）ブリッジ ドメインでカプセル化のフラッディングを有効にした場合、Cisco ACI は非入力（出力および中継）リーフ ノード上の外部デバイスに面したダウンリンクからのカプセル化で、このようなパケットを送信しません。この新しい動作により、パケットが予期しないカプセル化に漏洩することが防止されます。カプセル化でのフラッディングが EPG レベルでのみ有効になっている場合、非入力リーフ ノードは、カプセル化ではなくブリッジ ドメインでパケットをフラッディングする可能性があります。詳細については、拡張バグ CSCvx83364 を参照してください。
- レイヤ 3 ゲートウェイは Cisco ACI ファブリック内にある必要があります。

コントラクト

EPG に加えて、コントラクト（`vzBrCP`）はポリシー モデルのキー オブジェクトです。EPG が他の EPG と通信するには、コントラクトのルールに従う必要があります。次の図は、管理情報ツリー（MIT）内のコントラクトの場所とテナントの他のオブジェクトとの関係を示します。

図 *12 :* コントラクト



管理者はコントラクトを使用して、許可されているプロトコルとポートを含む ESG 間をパス可能なトラフィックの種類を選択します。コントラクトがなければ、EPG 間通信はデフォルトでディセーブルになります。EPG 内の通信に必要なコントラクトはありません。EPG 内の通信は常に暗黙的に許可されています。

また、コントラクト優先グループを構成して、VRF で EPG 間のより高度な通信の制御も可能です。VRF の EPG のほとんどはオープン通信ですが、一部には他の EPG との制限がある場合、コントラクト優先グループとフィルタ付きのコントラクトの組み合わせを構成し、通信を正確に制御できます。

コントラクトは、次のタイプのエンドポイント グループの通信を管理します。

- ACI ファブリック アプリケーション EPG （`fvAEPg`）間、テナント内およびテナント間の両方

（注） 共有サービスモードの場合、コントラクトはテナント間通信に必要です。テナント VRF がポリシーを適用していなくても、コントラクトが VRF 間で静的ルートを指定するために使用されます。

- ACI ファブリック アプリケーション EPG とレイヤ 2 外部外側ネットワークのインスタンス EPG （`l2extInstP`）間
- ACI ファブリック アプリケーション EPG とレイヤ 3 外部外側ネットワークのインスタンス EPG （`l3extInstP`）間
- ACI ファブリック アウトオブバンド（`mgmtOoB`）またはインバンド（`mgmtInB`）管理 EPG 間

コントラクトは、プロバイダー、コンシューマ、またはその両方とラベル付された EPG 間の通信を制御します。EPG プロバイダーは、コンシューマ EPG が従う必要のあるコントラクトを公開します。EPG とコントラクトの関係は、プロバイダーまたはコンシューマです。EPG がコントラクトを提供すると、通信が提供されたコントラクトに準拠している限り、その EPG

との通信は他の EPG から開始できます。EPG がコントラクトを使用すると、その EPG のエンドポイントは、コントラクトを指定した EPG のエンドポイントと通信を開始できます。

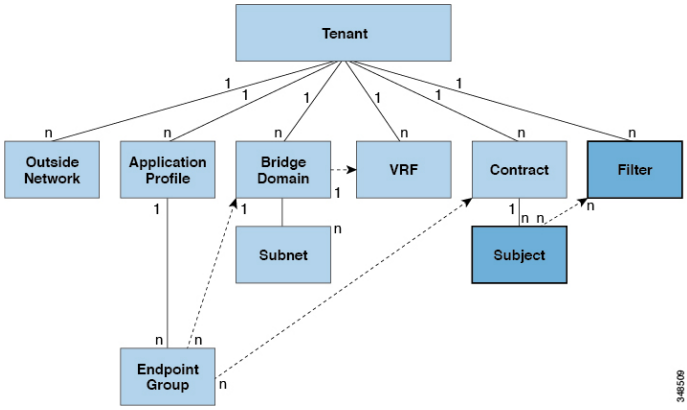
（注） 1 つの EPG で同じコントラクトを指定および使用できます。EPG は複数のコントラクトを同時に指定および使用することもできます。

（注） ユーザーテナントから common テナントにエクスポートされたコントラクトは、他のユーザーテナントで自動的に使用できるようにはなりません。複数のユーザーテナントと common テナント間でコントラクトを共有するには、コントラクトを common テナントで定義するか、目的の各テナントに個別にエクスポートする必要があります。

EPG 通信を制御するラベル、フィルタ、エイリアス、および情報カテゴリ

ラベル、情報カテゴリ、エイリアス、およびフィルタの管理対象オブジェクトにより、さまざまなアプリケーションまたはサービスの提供要件を満たすための EPG とコントラクト間の混合と照合が可能になります。次の図は、管理情報ツリー（MIT）内のアプリケーション サブジェクトおよびフィルタの場所と、テナント内の他のオブジェクトとの関係を示します。

図 *13*：ラベル、情報カテゴリ、およびフィルタ



コントラクトには、複数の通信ルールを含めることができ、複数の EPG は複数のコントラクトを消費および提供できます。ラベルは、EPG の特定のペア間で通信が行われるときにどのルールが適用されるかを管理します。ポリシーの設計者は、複雑な通信ポリシーを簡潔に表し、アプリケーションの複数のインスタンス間でこれらのポリシーを再利用できます。たとえば、*Cisco Application Centric Infrastructure Fundamentals* の「Contract Scope Examples」の章のサンプルポリシーは、同じコントラクトがラベル、情報カテゴリ、およびフィルタを使用して、HTTP または HTTPS を必要とするさまざまな EPG 間で通信がどのように発生するかを区別する方法を示しています。

ラベル、情報カテゴリ、およびフィルタは次のオプションに従って EPG 通信を定義します。

- ラベルは、プロパティ（名前）を 1 つだけ持つ管理対象オブジェクトです。ラベルにより、互いに通信できるオブジェクトとできないオブジェクトを分類できます。ラベルの一致は最初に行われます。ラベルが一致しない場合、他のコントラクトまたはフィルタ情報は処理されません。ラベルの一致属性は、次の値のいずれかになります。At Least One（デフォルト）、All、None または Exactly One。*Cisco Application Centric Infrastructure Fundamentals* の「Label Matching」の章では、すべてのラベル マッチ タイプとその結果の簡単な例を示しています。

（注） ラベルは、EPG、コントラクト、ブリッジ ドメイン、DHCP リレー ポリシー、および DNS ポリシーなどのさまざまなプロバイダーおよびコンシューマの管理対象オブジェクトに適用できます。ラベルはオブジェクトタイプ間では適用されません。アプリケーション EPG のラベルは、ブリッジドメインのラベルと関連がありません。

ラベルは、互いに通信できる EPG コンシューマと EPG プロバイダーを決定します。ラベルの一致により、コントラクトのどのサブジェクトがそのコントラクトの所定の EPG プロバイダーまたは EPG コンシューマに使用できるかが決定されます。

ラベルには次の 2 つのタイプがあります。

- 情報カテゴリのラベルは EPG に適用されます。サブジェクト ラベルの一致により、EPG はコントラクト内のサブジェクトのサブセットを選択することができます。
- EPG に適用されるプロバイダー/コンシューマ ラベル。プロバイダー/コンシューマのラベルの一致により、コンシューマ EPG はプロバイダー EPG を選択できます。その逆も可能です。

- エイリアスは、オブジェクトに適用できる代替名であり、名前とは異なり、変更できます。
- フィルタは、レイヤ 2 ～ レイヤ 4 フィールド、レイヤ 3 プロトコル タイプ、レイヤ 4 ポートなどの TCP/IP ヘッダー フィールドなどです。関連するコントラクトに従って、EPG プロバイダーは、IN および OUT 両方の方向でプロトコルおよびポートを決定します。コントラクトの情報カテゴリは、コントラクトを提供する側と消費する側の EPG の間に適用されるフィルタ（およびその方向）への関連付けが含まれています。

（注） コントラクト フィルタの一致タイプが `すべて（All）` の場合、ベスト プラクティスは VRF 非強制モードを使用することです。特定の状況下では、これらのガイドラインに従わないと、コントラクトで VRF の EPG 間のトラフィックが許可されなくなります。

- 情報カテゴリはコントラクトに含まれています。コントラクト内の1つ以上の情報カテゴリがフィルタを使用して、通信できるトラフィックのタイプと発生の仕方を指定します。たとえば、HTTPS メッセージの場合、サブジェクトはその方向と許可される IP アドレスタイプ（たとえば IPv4）、HTTP プロトコル、およびポートを指定するフィルタを指定します。サブジェクトは、フィルタを単方向にするか双方向にするかを決定します。単方向フィルタは 1 方向で使用されます。単方向フィルタは、IN または OUT の通信を定義しますが、両方に対して同じではありません。双方向フィルタは両方に対して同じで、IN および OUT の通信を定義します。

コントラクトまたはコントラクトの件名の例外の設定

Cisco APIC リリース 3.2(1) では、EPG 間のコントラクトが拡張され、コントラクトに参加しているコントラクトプロバイダまたはコンシューマのサブネットを拒否できます。インター EPG コントラクトおよびい内部 EPG コントラクトは、この機能でサポートされます。

プロバイダ EPG の件名を有効にして、件名またがコントラクトの例外で一致基準が設定されているものを除くすべてのコンシューマ EPG との通信が可能になります。たとえば、サブセットを除く、テナントのすべての EPG にサービスを提供するために EPG を有効にする場合、これら EPG を除外できます。これを設定するには、コントラクトまたはそのコントラクトの件名のいずれかで例外を作成します。サブセットがコントラクトの提供または消費のアクセスを拒否します。

ラベル、カウンタ、許可および拒否ログは、コントラクトおよび件名の例外でサポートされています。

コントラクトのすべての件名に例外を適用するには、コントラクトに例外を追加します。コントラクトの単一の件名にのみ例外を適用する場合、件名に例外を追加します。

件名にフィルタを追加する場合、フィルタのアクションを設定できます（フィルタ条件に一致するオブジェクトを許可または拒否する）。また、**[拒否]** フィルタについては、フィルタの優先順位を設定することができます。**[許可]** フィルタは常にデフォルトの優先順位があります。自動拒否の件名-フィルタ関係をマーキングすると、件名に一致している場合、各 EPG のペアに適用されます。コントラクトと件名には、複数の件名-フィルタ関係を含むことができます。これは、フィルタに一致するオブジェクトを許可または拒否するように独自に設定できます。

例外タイプ

コントラクトと件名の例外は次のタイプに基づき、* ワイルドカードなどの正規表現を含むことができます。

例外の条件は、[コンシューマ正規表現] および [プロバイダ正規表現]のフィールドで定義されているように、これらのオブジェクトを除外します。	例	説明
テナント	<vzException consRegex= “common” field= “Tenant” name= “excep03” provRegex= “t1” />	この例では、common テナントを使用して、 EPG が t1 テナントにより提供されるコントラクトを消費しないように除外します。
VRF	<vzException consRegex= “ctx1” field= “Ctx” name= “excep05” provRegex= “ctx1” />	この例では、ctx1 のメンバーが同じ VRF から提供されるサービスを使用しないように除外します。
EPG	<vzException consRegex= “EPgPa.*” field= “EPg” name= “excep03” provRegex= “EPg03” />	この例では、名前が EPGPa から始まる複数の EPG が存在すると仮定し、EPg03 により提供されているコントラクトのコンシューマとしてすべて拒否される必要があります。
Dn	<vzException consRegex= “uni/tn-t36/ap-customer/epg-epg193” field= “Dn” name=“excep04” provRegex= “uni/tn-t36/ap-customer/epg-epg200” />	この例では、epg193 が epg200 により提供されたコントラクトを消費しないように除外します。
タグ	<vzException consRegex= “red” field= “Tag” name= “excep01” provRegex= “green” />	例では、red タグでマークされているオブジェクトが消費することと、green タグでマークされているオブジェクトがコントラクトに参加しないように除外します。

タブー

セキュリティを確保する通常のプロセスも適用されますが、ACI ポリシーモデルは、どのようなセキュリティ プラクティスが採用されても完全性を確保するのに役立ちます。ACI ポリシーモデルのアプローチでは、すべての通信がこれらの条件に準拠する必要があります。

- 通信は、モデルの管理対象オブジェクトであるコントラクトに基づいてのみ許可されます。コントラクトがなければ、EPG 間通信はデフォルトでディセーブルになります。

- ハードウェアへのダイレクト アクセスはなく、すべてのインタラクションはポリシー モデルを通じて管理されます。

禁止コントラクトは特定のトラフィックを拒否するために使用できます。そうしないと、コントラクトによって許可されます。ドロップされるトラフィックは、パターンと一致しています（すべての EPG、特定の EPG、フィルタに一致するトラフィックなど）。禁止ルールは単方向で、コントラクトを提供する EPG に対して一致するトラフィックを拒否します。

Cisco APIC リリース 3.2(x) および名前が EX または FX で終わるスイッチでは、標準コントラクトで代わりに件名 [拒否] アクションまたは [コントラクトまたは件名の除外] を使用して、指定のパターンを持つトラフィックをブロックできます。

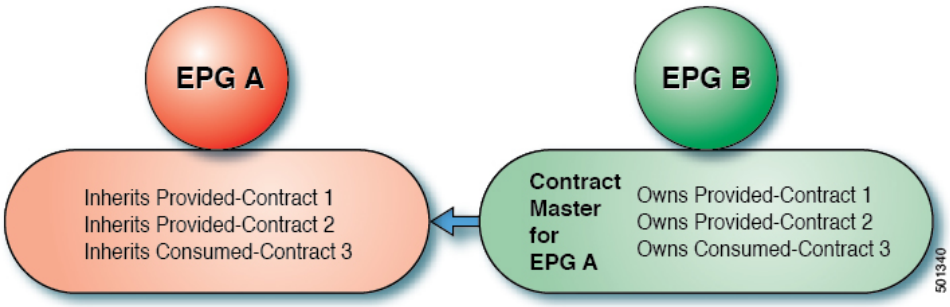
コントラクト継承について

関連する契約を新しい EPG に統合するため、EPG を有効にして同じテナントの別の EPG に直接関連する契約すべて（提供済み/消費済み）を継承できます。コントラクトの継承は、アプリケーション EPG、マイクロセグメント EPG、L2Out EPG、および L3Out EPG に設定できます。

リリース 3.x では、EPG 間の提供済み/消費済みの両方の契約に、契約を継承する設定も可能です。EPG 間契約が、モデル名や後発のモデルの最後に EX または EX が付く、Cisco Nexus 9000 シリーズ スイッチでサポートされています。

EPG を有効にし、APIC GUI、NX-OS スタイル CLI、REST API を使用して、別の EPG に直接関連する契約すべてを継承できます。

図 *14*：コントラクトの継承



上の図で、EPG A は EPG B から（EPG A の契約マスター）提供済みの契約 1 および 2、消費済みの契約 3 を継承するように設定されています。

コントラクト継承を設定する際は、次のガイドラインに従ってください。

- コントラクト継承は、アプリケーション EPG、マイクロセグメント（uSeg）EPG、外部 L2Out EPG、および外部 L3Out EPG 用に設定できます。コントラクト関係は同じタイプの EPG 間で確立する必要があります。
- 関係が確立されると、提供するコントラクトと消費するコントラクトの両方がコントラクト マスターから継承されます。

- コントラクト マスターとコントラクトを継承する EPG は同じテナント内にある必要があります。
- マスター契約への変更は、すべての継承に伝播されます。新しい契約がマスターに追加される場合、継承先にも追加されます。
- EPG は、複数のコントラクト マスターからコントラクトを継承することができます。
- コントラクト継承は単一のレベルでのみサポートされ（連結できない）、コントラクトマスターがコントラクトを継承することはできません。
- コントラクト継承のラベルがサポートされます。EPG A が EPG B からコントラクトを継承するとき、EPG A と EPG B で異なるサブジェクト ラベルが設定されている場合、APIC は EPG B から継承されたコントラクトの EPG B で設定されたラベルを使用します。 APIC は EPG A が直接関与するコントラクトに対し、EPG A の下で設定されたラベルを使用します。
- EPG が契約に直接関連付けられている、または契約を継承しているかどうかに関わらず、TCAM 内のエントリが消費されます。したがって契約スケール ガイドラインが引き続き適用されます。詳細については、お使いのリリースの「検証されたスケーラビリティ ガイド」を参照してください。
- vzAny セキュリティ コントラクトとタブー コントラクはサポートされません。
- Cisco APIC リリース 5.0(1) および 4.2(6) 以降、コントラクトと EPG が同じテナントにある場合、サービス グラフによるコントラクトの継承がサポートされます。

契約の継承設定および継承済みおよびスタンドアロン契約を表示することに関する詳細は、「*Cisco APIC* の基本設定ガイドを参照してください。

契約優先グループについて

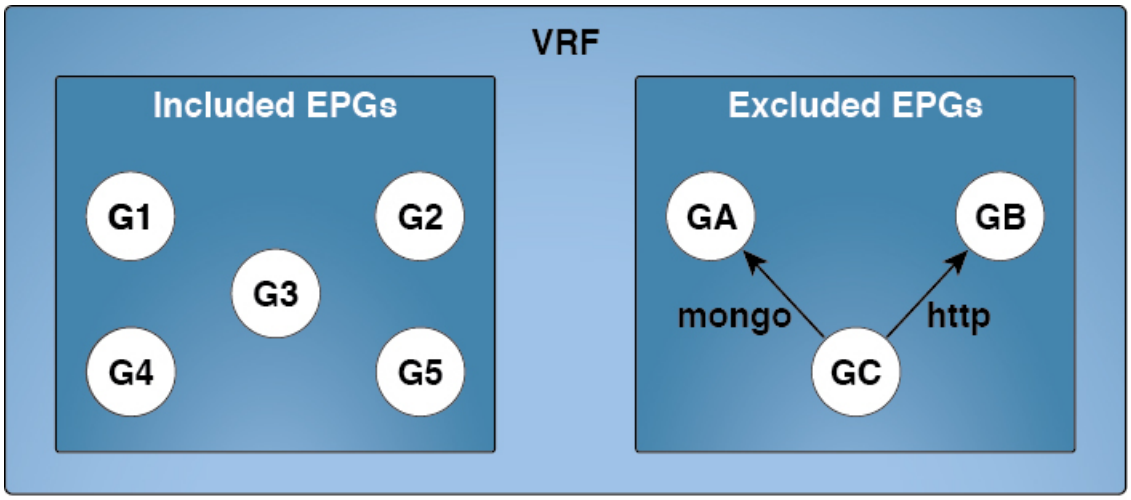
契約優先グループが設定されている VRF で、EPG に利用可能なポリシー適用には 2 種類あります。

- EPG を含む：EPG が契約優先グループのメンバーシップを持っている場合、EPG は契約をせずにお互いに自由に通信できます。これは、source-any-destination-any-permit デフォルト ルールに基づくものです。
- EPG を除外：優先グループのメンバーではない EPG は、相互に通信するために契約が必要です。そうしない場合、デフォルトの source-any-destination-any-deny ルールが適用されます。

契約優先グループ機能では、VRF で EPG 間のより高度な通信の制御が可能です。VRF の EPG のほとんどはオープン通信ですが、一部には他の EPG との制限がある場合、契約優先グループとフィルタ付きの契約の組み合わせを設定し、EPG 内の通信を正確に制御できます。

優先グループから除外されている EPG は、source-any-destination-any-deny デフォルト ルールを上書きする契約がある場合にのみ、他 EPG と通信できます。

図 *15*：契約優先グループの概要



Source	Destination	Filter	Action
any	any	implicit	permit
GA	any	implicit	deny
any	GA	implicit	deny
GB	any	implicit	deny
any	GB	implicit	deny
GC	any	implicit	deny
any	GC	implicit	deny

Source	Destination	Filter	Action
GC	GA	mongo	permit
GA	GC	mongo	permit
GC	GB	http	permit
GB	GC	http	permit

501168

サービス グラフ サポート

APIC リリース 4.0(1) 以降では、サービス グラフによって作成された EPG を優先契約グループに含めることができます。優先グループ メンバーシップのタイプ（include または exclude）を定義する新しいポリシー（サービス EPG ポリシー）が使用可能です。設定後は、デバイス選択ポリシーまたはサービス グラフ テンプレートのアプリケーションを通じて適用できます。

また、シャドウ EPG を優先グループに含めるか、優先グループから除外するかも設定できるようになりました。

制限事項

以下の制限が契約優先グループに適用されます。

- L3Out およびアプリケーション EPG が契約優先グループで設定されており、EPG が VPC でのみ展開されているトポロジで、VPC の 1 つのリーフ スイッチのみに L3Out のプレフィックス エントリがあることがわかります。この場合、VPC の他のリーフ スイッチにはエントリがなく、そのためトラフィックをドロップします。

  この問題を回避するには、次のいずれかを行います。

  - VRF の契約グループを無効および再度有効にします。

- L3Out EPG のプレフィックス エントリを削除し再度作成します。

- また、サービス グラフ契約のプロバイダまたはコンシューマ EPG が契約グループに含まれる場合、シャドウ EPG は契約グループから除外できません。シャドウ EPG は契約グループで許可されますが、シャドウ EPG が展開されているノードで契約グループ ポリシーの展開をトリガしません。ノードに契約グループ ポリシーをダウンロードするには、契約グループ内にダミー EPG を展開します。
- CSCvm63145 により、コントラクト優先グループの EPG は共有サービス コントラクトを使用できますが、L3Out EPG をコンシューマとして使用する共有サービス コントラクトのプロバイダになることはできません。

契約のパフォーマンスの最適化

Cisco APIC、リリース 3.2 で始まるより効率的なハードウェア契約データの TCAM ストレージをサポートしている双方向契約を設定できます。最適化を有効になっている、両方向の統計情報を契約は統合します。

TCAM 最適化は、第 2 世代 Cisco Nexus 9000 シリーズのトップオブラック（TOR）スイッチでサポートされます。これは、EX、FX、および FX2 以降のサフィックスが付いたものです（たとえば、N9K-C93180LC-EX または N9K-C93180YC-FX ）。

TCAM 契約の効率的なデータ ストレージを設定するには、次のオプションが有効にします。

- プロバイダとコンシューマの間で両方向に適用されるコントラクトをマークします。
- IP TCP または UDP プロトコルを使用するフィルタの場合は、リバース ポート オプションを有効にします。
- コントラクト サブジェクトを設定する場合は、**[ポリシー圧縮の有効化（Enable Policy Compression）]** ディレクティブを選択します。これにより、`actrl : Rule` 管理対象オブジェクトのアクション属性に `no_stats` オプションが追加されます。

制限事項

[ポリシー圧縮の有効化（Enable Policy Compression）]（`no_stats`）オプションを選択すると、ルールごとの統計情報が失われます。ただし、両方の方向の複合ルール統計情報は、ハードウェア統計情報に存在します。

Cisco APIC 3.2(1) にアップグレードした後、`no_stats` オプションをアップグレード前のコントラクト サブジェクト（フィルタまたはフィルタ エントリを含む）に追加するには、コントラクト サブジェクトを削除し、**Enable Policy Compression** ディレクティブで再設定する必要があります。そうしないと、圧縮は行われません。

双方向サブジェクト フィルタを使用するコントラクトごとに、Cisco NX-OS は 2 つのルールを作成します。

- `sPcTag` および `dPcTag` が含まれ、`direction=bi-dir` とマークされているルール。これはハードウェアでプログラミングされます。

- プログラミングされていない direction=uni-dir-ignore でマークされたルール

次の設定とルールは圧縮されません。

- ルールの優先順位を持つ fully_qual
- ルールの反対側 (双 dir および uni dir 無視 マーク) と同一ではないプロパティは、次のように **アクション** を含む **統制** 、 **prio**、**qos** または **markDscp**
- ルール 暗黙的 または implarp フィルタ
- ルール アクションで Deny 、 Redir 、 コピー 、または Deny ログ

次の月クエリ出力は、圧縮のと見なされる、契約の 2 つのルールを示します。

```
apic1# moquery -c actrlRule
Total Objects shown: 2

# actrl.Rule
scopeId            : 2588677
sPcTag             : 16388
dPcTag             : 49156
fltId              : 67
action             : no_stats,permit
actrlCfgFailedBmp  :
actrlCfgFailedTs   : 00:00:00:00.000
actrlCfgState      : 0
childAction        :
ctrctName          :
descr              :
direction          : bi-dir
dn                 : sys/actrl/scope-2588677/rule-2588677-s-16388-d-49156-f-67
id                 : 4112
lcOwn              : implicit
markDscp           : unspecified
modTs              : 2019-04-27T09:01:33.152-07:00
monPolDn           : uni/tn-common/monepg-default
name               :
nameAlias          :
operSt             : enabled
operStQual         :
prio               : fully_qual
qosGrp             : unspecified
rn                 : rule-2588677-s-16388-d-49156-f-67
status             :
type               : tenant


# actrl.Rule
scopeId            : 2588677
sPcTag             : 49156
dPcTag             : 16388
fltId              : 64
action             : no_stats,permit
actrlCfgFailedBmp  :
actrlCfgFailedTs   : 00:00:00:00.000
actrlCfgState      : 0
childAction        :
ctrctName          :
descr              :
direction          : uni-dir-ignore
```

```
dn                  : sys/actrl/scope-2588677/rule-2588677-s-49156-d-16388-f-64
id                  : 4126
lcOwn               : implicit
markDscp            : unspecified
modTs               : 2019-04-27T09:01:33.152-07:00
monPolDn            : uni/tn-common/monepg-default
name                :
nameAlias           :
operSt              : enabled
operStQual          :
prio                : fully_qual
qosGrp              : unspecified
rn                  : rule-2588677-s-49156-d-16388-f-64
status              :
type                : tenant
```

表 *1*: 圧縮マトリクス

リバース フィルタ ポートが有効	TCP または UDP 発信元ポート	TCP または UCP 宛先ポート	圧縮
はい	ポート A	ポート B	はい
○	未指定	ポート B	はい
○	ポート A	未指定	はい
○	未指定	未指定	はい
非対応	ポート A	ポート B	いいえ
非対応	未指定	ポート B	いいえ
非対応	ポート A	未指定	いいえ
非対応	未指定	未指定	はい

vzAny とは

vzAny 管理対象オブジェクトは、各 EPG の個別のコントラクト関係を作成するのではなく、1 つまたは複数のコントラクト（vzBrCP）に仮想ルーティングと転送（VRF）のすべてのエンドポイント グループ（EPG）を関連付ける便利な方法を提供します。

Cisco ACI ファブリックでは、コントラクトのルールにより、EPG は他の EPG としか通信できません。EPG とコントラクトの関係によって、EPG がコントラクトのルールに定義された通信を提供するのか、消費するのか、あるいは提供も消費も行うのかが指定されます。VRF 中のすべての EPG にコントラクトのルールを動的に適用することで、vzAny ではEPG とコントラクトとの関係を構成するプロセスが自動化されます。新しい EPG が VRF に追加されるたびに、vzAny コントラクト ルールが自動的に適用されます。vzAny と EPG の「1 対すべて」の関係は、コンテキスト中のすべての EPG にコントラクトのルールを適用するための最も効率的な方法です。

（注） テナントの APIC GUI では、VRF はプライベートネットワーク（テナント内のネットワーク）またはコンテキストとも呼ばれます。

共有サービスの場合は、コンシューマ（vzAny）側の接続先の pcTag（分類）を適切に導出するために、EPG の下にプロバイダ EPG 共有サブネットを定義する必要があります。コンシューマとプロバイダの両方のサブネットがブリッジ ドメイン下で定義され、共有サービス コンシューマとして機能する vzAny に対して、BD から BD への共有サービス設定から移行する場合は、少なくとも共有フラグを使用してプロバイダ サブネットを EPG に追加する追加の設定手順を実行する必要があります。

（注） 定義済みの BD サブネットの複製として EPG サブネットを追加する場合は、サブネットの両方の定義に同じフラグが定義されていることを確認してください。そうしないと、予期しないファブリック転送の動作が発生する可能性があります。

vzAny を使用するには、**[テナント（Tenants）]**> > **[*tenant-name*]** > > **[ネットワーキング（Networking）]** > > **[VRFs]**> > **[*vrf-name*]**> > **[VRF 向けの EPG 収集（EPG Collection for VRF）]** の順に移動します。

コピー サービスについて

すべてのトラフィックを複製する SPAN とは異なり、 Cisco Application Centric Infrastructure (ACI) のコピー サービス機能は、契約での仕様に従って、エンドポイント グループ間のトラフィックのうちコピーの部分だけを選択的に有効にします。ブロードキャスト、不明なユニキャストとマルチキャスト (BUM)、および契約の対象外であるコントロール プレーン トラフィックは、コピーされません。対照的に、SPAN は、エンドポイント グループ、アクセス ポートまたはアップリンク ポートから発するすべてのトラフィックをコピーします。SPAN とは異なり、コピーサービスは、コピーされたトラフィックにヘッダーを追加しません。コピーサービスのトラフィックは、通常のトラフィックの転送への影響を最小限に抑えるため、スイッチ内で内部的に管理されます。

コピー サービスは、コピーされるトラフィックの宛先としてコピー クラスタを指定する、レイヤ 4 ～ レイヤ 7 サービス グラフ テンプレートの一部として構成されます。コピー サービスはサービス グラフ内の異なるホップにタップすることができます。たとえば、コピー サービスは、コンシューマ エンドポイント グループとファイアウォール プロバイダ エンドポイントの間のトラフィック、またはサーバのロードバランサとファイアウォールの間のトラフィックを選択することができます。コピー クラスタは、テナント間で共有することができます。

コピー サービスを使用するには、以下のタスクを実施する必要があります:

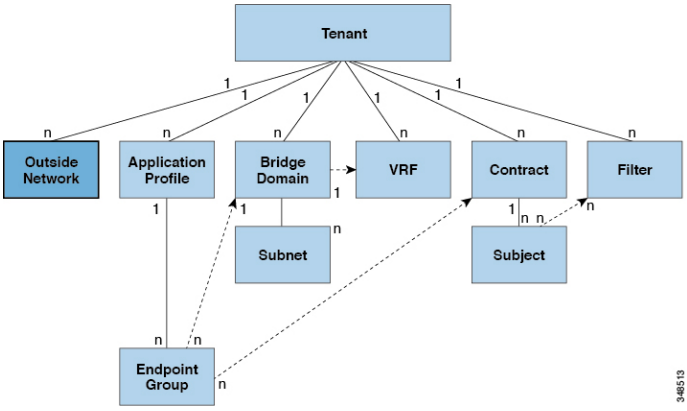
- 送信元と宛先エンドポイント グループを特定します。
- 情報カテゴリ、および契約フィルタで許可されている内容に従って、コピー対象を指定する契約を構成します。

- ターゲット デバイスを特定するレイヤ 4 ～ レイヤ 7 のコピー デバイスを構成し、それらが接続するポートを指定します。
- コピー サービスをレイヤ 4 ～ レイヤ 7 サービス グラフ テンプレートの一部として使用します。
- どのデバイスがサービス グラフからのトラフィックを受信するかを指定する、デバイス選択ポリシーを構成します。デバイス選択ポリシーを構成する際には、契約、サービス グラフ、コピー クラスタ、およびコピー デバイス内のクラスタ論理インターフェイスを指定します。

外部ネットワーク

外部ネットワーク ポリシーは、外部への接続を制御します。テナントには、複数の外部ネットワーク オブジェクトを含めることができます。次の図は、管理情報ツリー（MIT）内の外部ネットワークの場所とテナントの他のオブジェクトとの関係を示します。

図 *16 :* 外部ネットワーク



外部ネットワーク ポリシーは、外部のパブリック/プライベート ネットワークと ACI ファブリック間の通信を制御する関連するレイヤ 2（`l2extOut`）またはレイヤ 3（`l3extOut`）プロパティを指定します。WAN およびエンタープライズ コアに接続するルータや既存のレイヤ 2 スイッチなどの外部デバイスは、リーフスイッチの前面パネルのインターフェイスに接続します。このような接続を提供するリーフスイッチは、境界リーフとして知られています。外部デバイスに接続する境界リーフスイッチ インターフェイスは、ブリッジドまたはルーテッド インターフェイスとして構成できます。ルーテッドインターフェイスの場合、静的またはダイナミック ルーティングを使用できます。境界リーフスイッチは、標準のリーフスイッチのすべての機能を実行することもできます。

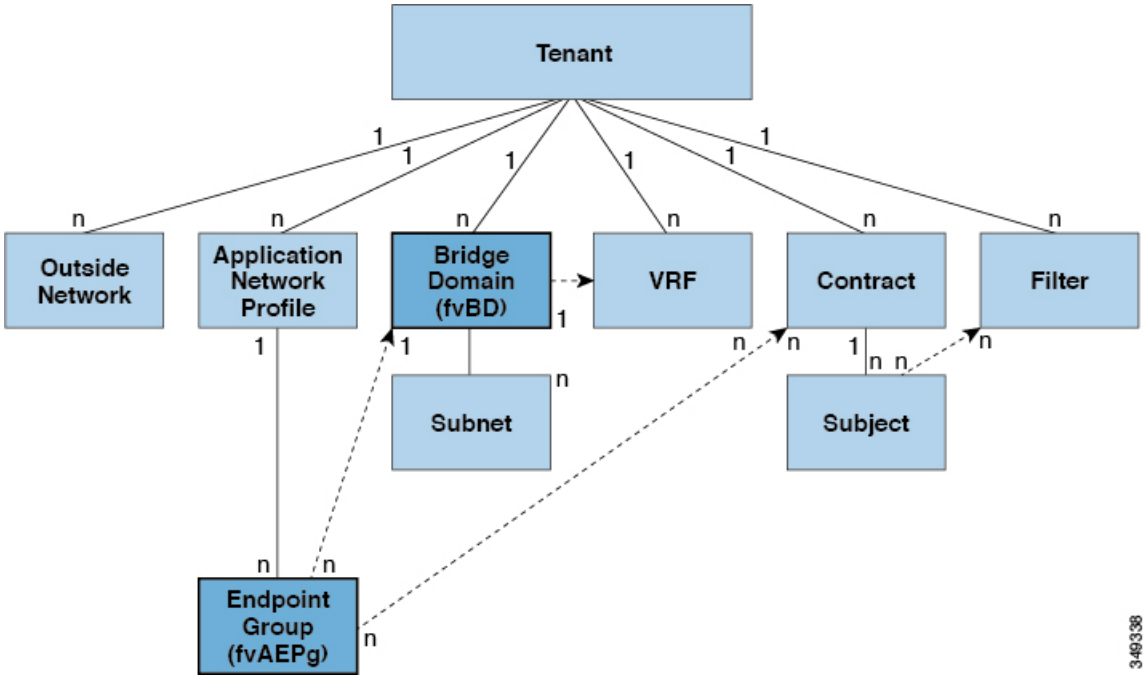
管理対象オブジェクトの関係とポリシー解決

関係管理対象オブジェクトは、抑制（親/子）の関係を共有しない管理対象オブジェクトのインスタンス間の関係を表します。MO の関係は、次の 2 つの方法のいずれかでソース MO とターゲット MO の間に確立されます。

- 明示的な関係（`fvRsPathAtt`）は、ターゲット MO の識別名（DN）に基づいて関係を定義します。
- 名前付きの関係は、ターゲット MO の名前に基づいて関係を定義します。

次の図の点線は、いくつかの一般的な MO の関係を示します。

図 *17 : MO* の関係



たとえば、EPG とブリッジドメイン間の点線は、これら 2 つの MO 間の関係を定義します。この図では、EPG（`fvAEPg`）には、ターゲットのブリッジドメイン MO（`fvBD`）の名前が付いた関係 MO（`fvRsBD`）が含まれます。たとえば、実稼働がブリッジドメイン名（`tnFvBDName=production`）である場合、関係の名前は実稼働（`fvRsBdName=production`）になります。

「命名された関係に基づくポリシー解決では、一致する名前を持つ対象の MO が現在のテナントで見つからない場合、ACI ファブリックが共通テナントで解決を試みます。たとえばユーザーのテナント EPG に、存在しないブリッジドメインを対象とした関係 MO が含まれていた場合、システムは共通テナントでその関係の解決を試行します。名前付き関係が現在のテナントまたは共通のテナントで解決できない場合、ACI ファブリックは、デフォルト ポリシーに解決を試行します。デフォルト ポリシーが現在のテナントに存在する場合、それが使用されま

す。デフォルトポリシーが存在しない場合は、ACI ファブリックが共通テナント内のデフォルトポリシーを検索します。ブリッジドメイン、VRF、コントラクト（セキュリティポリシー）の命名済み関係はデフォルト値に解決されません。

デフォルト ポリシー

APIC デフォルト ポリシー値の初期値は、スイッチにロードされる具象モデルから取得されます。ファブリックの管理者は、デフォルト ポリシーを変更できます。

警告 デフォルト ポリシーは、変更または削除できません。デフォルト ポリシーを削除すると、ポリシー解決プロセスが異常終了する可能性があります。

ACI ファブリックは、そのコア機能の多くにデフォルトのポリシーを含んでいます。デフォルト ポリシーの例には、次のものがあります。

- ブリッジドメイン（common テナント内）
- レイヤ 2 およびレイヤ 3 プロトコル
- ファブリックの初期化、デバイスの検出、およびケーブル接続の検出
- ストーム制御とフラッディング
- 仮想ポートチャネル
- スイッチバッファ内の学習済みエンドポイントのキャッシングとエージングのためのエンドポイント保持
- ループ検出
- モニタリングと統計情報

（注） デフォルトポリシーを使用する構成を実装する際の混乱を避けるために、デフォルトポリシーに加えられた変更を文書化します。デフォルトポリシーを削除する前に、現在または将来の構成がデフォルトポリシーに依存していないことを確認してください。たとえば、デフォルトのファームウェアの更新ポリシーを削除すると、将来のファームウェアの更新に問題が生じる可能性があります。

（注） デフォルトの VRF またはブリッジ ドメインがユーザー テナントに存在し、VRF またはブリッジ ドメインの関連付けがブリッジ ドメイン/EPG で空の場合、インストゥルメンテーション ポリシーが必要です。

ACI ファブリックをアップグレードした場合、デフォルト値が新しいリリースで変更されても既存のポリシーのデフォルト値が保持されます。ノードが APIC に初めて接続されると、ノードはそれ自体をすべてのデフォルト ポリシーをノードにプッシュする APIC に登録します。デフォルト ポリシーでのすべての変更がノードにプッシュされます。

デフォルト ポリシーは、次の複数の目的に使用されます。

- ファブリックの管理者がモデル内のデフォルト値を上書きできます。
- 管理者が明示ポリシーを提供しない場合、APIC はデフォルト ポリシーを適用します。管理者はデフォルト ポリシーを作成でき、管理者が明示ポリシーを提供しない限り、APIC はそのポリシーを使用します。

たとえば、管理者が行うアクションまたは行わないアクションに応じて、APIC は次を実行します。

- 管理者が選択したポートに対して LLDP ポリシーを指定しないため、APIC はポート セレクタに指定されたポートに対しデフォルトの LLDP インターフェイス ポリシーを適用します。
- 管理者がポート セレクタからポートを削除すると、APIC はそのポートにデフォルト ポリシーを適用します。この例では、管理者がポート 1/15 をポート セレクタから削除すると、そのポートはポート チャネルの一部ではなくなり、APIC はそのポートにすべてのデフォルト ポリシーを適用します。

次のシナリオでは、一般的なポリシー解決の動作について説明します。

- 構成は、デフォルト ポリシーを明示的に参照します。現在のテナントにデフォルト ポリシーが存在する場合は、それが使用されます。それ以外の場合は、テナント**共通の**デフォルト ポリシーが使用されます。
- 構成は、現在のテナントまたはテナント共通に存在しない名前付きポリシー (デフォルトではない) を参照します。現在のテナントにデフォルト ポリシーがある場合は、それが使用されます。それ以外の場合は、テナント**共通の**デフォルト ポリシーが使用されます。

（注） これは、テナント内のブリッジドメインまたは VRF（プライベートネットワーク）には適用されません。

- 構成はポリシー名を参照しません。現在のテナントにデフォルト ポリシーが存在する場合、それが使用されます。それ以外の場合は、テナント**共通の**デフォルト ポリシーが使用されます。

（注） ブリッジドメインと VRF の場合、これは、**common** テナントの接続計測ポリシー（`fvConnInstrPol`）に適切なブリッジドメインまたはVRFフラグが設定されている場合にのみ適用されます。これにより、意図しない EPG がテナント **common** サブネットに展開されるのを防ぎます。

ポリシー モデルは、オブジェクトが自身の下に関係管理対象オブジェクト（MO）を持つことによって別のポリシーを使用していることや、関係 MO が名前によってターゲット ポリシーを参照することを指定します。この関係が、名前による明示的なポリシー参照を行わない場合には、システムは、デフォルトと呼ばれるポリシーの解決を試みます。ブリッジドメイン（BD）と VRF（Ctx）は、このルールの例外です。

エンドポイント グループ（EPG）には、`tnFvBDName` というプロパティを持つ BD（`fvRsBd`）との関係があります。これが設定されていない場合（`tnVfBDName=""` ）、接続計測ポリシー（`fvConnInstrPol`）がこの場合の動作を派生させます。このポリシーは、すべての EPG ケース（VMM、ベアメタル、l2ext、l3ext）に適用されます。計測ポリシーは、`bdctrl` プロパティを使用してデフォルトの BD ポリシーを使用するかどうかを制御し、`ctxCtrl` プロパティを使用してデフォルトの VRF（Ctx）ポリシーを使用するかどうかを制御します。次のオプションは両方で同じです。

- *do not instrument*：リーフスイッチはデフォルト ポリシーを使用しません。
- *Instruments-and-no-route*：ポリシーを計測し、ルーティングを有効にしません。
- *Instruments-and-route*：ポリシーを計測し、ルーティングを有効にします。

トランス テナント EPG 通信

あるテナントの EPG は、共有テナントに含まれるコントラクト インターフェイスを介して他のテナントの EPG を伝達できます。コントラクト インターフェイスは、異なるテナントに含まれる EPG によってコントラクト消費インターフェイスとして使用できる MO です。インターフェイスへの関連付けによって、EPG は共有テナントに含まれるコントラクトへのインターフェイスによって表される情報カテゴリを消費します。テナントは第 3 位で定義された単一のコントラクトに参加できます。より厳しいセキュリティ要件は、テナントが互いに完全に独立したままになるようにテナント、コントラクト、情報カテゴリおよびフィルタの方向を定義することで満たすことができます。

共有サービス コントラクトの設定時は、次のガイドラインに従ってください。

- インバンド EPG とアウトオブバンド EPG の間でコントラクトが構成されている場合、次の制限が適用されます。
  - 両方の EPG が同じ VRF（コンテキスト）にある必要があります。
  - フィルタは、着信方向にのみ適用されます。

- レイヤ 2 フィルタはサポートされません。
- QoS は、インバンド レイヤ 4 ～ レイヤ 7 のサービスには適用されません。
  - 管理統計は利用できません。
  - CPU 宛てトラフィックの共有サービスはサポートされません。

- プライベートネットワークを適用しない場合、コントラクトがブリッジ間ドメインのトラフィックに必要です。
- プレフィクスベースの EPG はサポートされません。共有サービスはレイヤ 3 外部外側ネットワークではサポートされません。レイヤ 3 外部外側ネットワークによって提供または消費されるコントラクトは、同じレイヤ 3 VRF を共有する EPG により消費または提供される必要があります。
- 共有サービスは、重複しないサブネットのみでサポートされます。共有サービスのサブネットを構成するときは、次のガイドラインに従ってください。
  - 共有サービスプロバイダーのサブネットは、ブリッジドメイン下ではなく EPG 下で構成します。
  - 同じ VRF を共有する EPG で構成されたサブネットは、統合および重複してはなりません。
  - ある VRF からリークされたサブネットは、切り離されている必要があり、重複してはなりません。
  - 複数のコンシューマー ネットワークから VRF に、またはその逆にアドバタイズされたサブネットは、切り離されている必要があり、重複してはなりません。

（注） 2 人のコンシューマーが誤って同じサブネットに構成されている場合は、両方のサブネットの構成を削除してこの状態からリカバリし、その後サブネットを正しく再構成します。

- プロバイダー VRF で共有サービスを `AnyToProv` で構成しないでください。APIC はこの構成を拒否し、障害が発生します。
- 共有サービスを提供している間は、プロバイダーのプライベートネットワークは非強制モードにできません。

タグ

オブジェクト タグにより、API 操作が簡素化されます。API 操作では、識別名（DN）の代わりにタグ名でオブジェクトまたはオブジェクトのグループを参照できます。タグは、タグ付けするアイテムの子オブジェクトです。名前以外に他のプロパティはありません。

オブジェクトのグループに記述名を割り当てる際にタグを使用します。同じタグ名を複数のオブジェクトに割り当てることができます。複数のタグ名を1つのオブジェクトに割り当てることができます。たとえば、すべての Web サーバ EPG へのアクセスを簡単に検索できるようにするには、該当するすべての EPG に Web サーバ タグを割り当てます。ファブリック全体の Web サーバ EPG は、Web サーバ タグを参照することで検索できます。

APIC クォータ管理の構成について

Cisco Application Policy Infrastructure Controller（APIC）リリース 2.3(1) 以降から、テナント管理者が構成できるオブジェクトの数に制限が設けられました。これにより管理者は、特定のテナントの下に、またはテナント全体でグローバルに追加できる管理対象オブジェクトを制限できます。

この機能は、テナントまたはテナントのグループが、リーフごと、またはファブリックごとの ACI の最大数を超えないようにする点で、または利用可能なリソースの大部分を不当に消費して、同じファブリックの他のテナントに影響を及ぼすことがないようにする点で役立ちます。

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