ACI ポリシー モデル

この章の内容は、次のとおりです。

ACI ポリシー モデルについて

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行えます。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。

- モデル駆動型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。論理的な設定は、使用可能な物理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設定にレンダリングされます。 具象エンティティに対して設定は行われません。 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設定されます。 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設定しませんが、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）論理的な設定と APIC ポリシーを定義します。

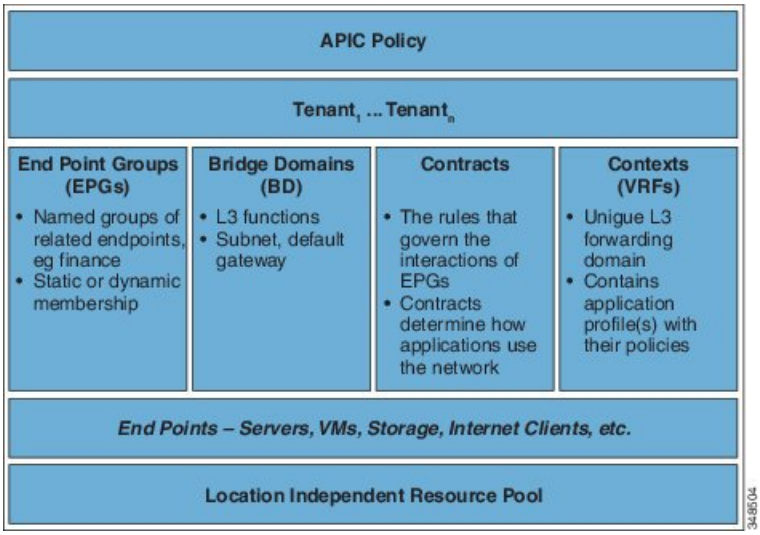
モデル内の管理対象オブジェクトを操作することで、エンジニアは独立した個々のコンポーネントの設定を管理することから開放されます。 これらの特性により、自動化と柔軟なワークロードのプロビジョニングが可能になり、インフラストラクチャ内のワークロードをどこでも検索できるようになります。 ネットワーク接続されたサービスは簡単に展開でき、APIC により自動化フレームワークが提供され、それらのネットワーク接続されたサービスのライフサイクルを管理できます。

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。

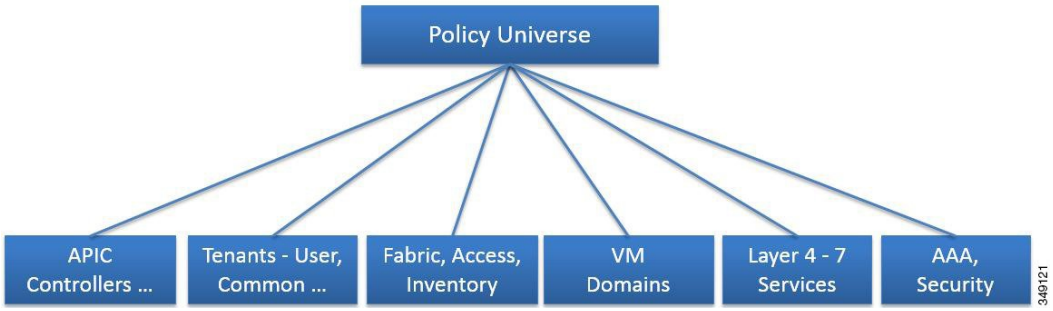
管理情報モデル

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*：管理情報ツリーの概要



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 コントロールを実行できます。 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、ネットワーク接続ストレージ、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設定できます。 ファイアウォール、ロード バランサ、レイヤ 4 ～ レイヤ 7 のサービス、侵入検知アプライアンスなどの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設定できます。 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設定できます。
  - 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設定できます。 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設定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（ブリッジドおよびルーテッド）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設定以外のインターフェイス設定を必要とする場合、管理者はアクセス ポリシーを設定して、リーフ スイッチのアクセス ポートでそのような設定を有効にする必要があります。
- ファブリック ポリシーは、ネットワーク タイムプロトコル（NTP）のサーバ同期、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）の領域およびアプリケーション エンドポイント グループ（EPG）を共有できます。 APIC は VM コントローラと通信し、のちに仮想ワークロードに適用されるポート グループなどのネットワーク設定を公開します。
- 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動的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。

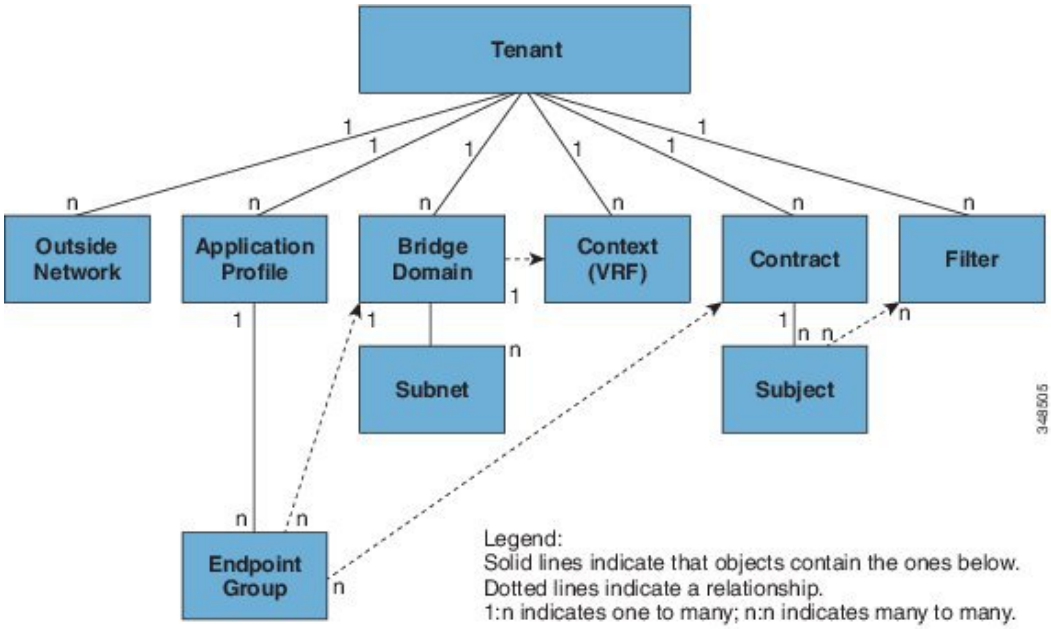
階層型ポリシー モデルは、RESTful API インターフェイスとうまく適合します。 呼び出されると、API は MIT 内のオブジェクトで読み取りまたは書き込みを行います。 URL は、MIT 内のオブジェクトを識別する識別名に直接マッピングします。 MIT 内のデータは、XML または JSON でエンコードされた自己完結型の構造化ツリー テキスト ドキュメントとして説明できます。

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



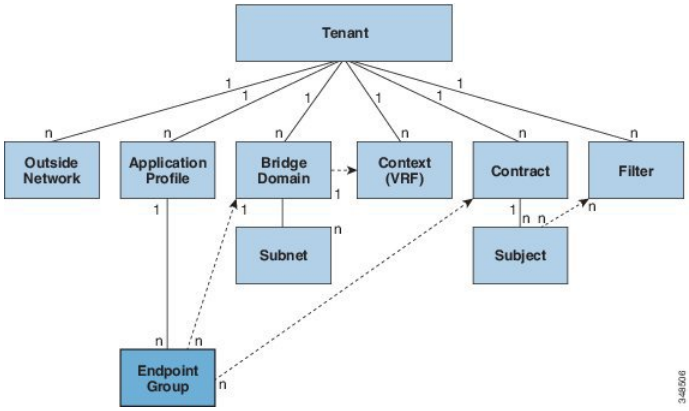
テナントは相互に分離することも、リソースを共有することもできます。 テナントが含む主要な要素は、フィルタ、コントラクト、外部ネットワーク、ブリッジ ドメイン、コンテキスト、およびエンドポイント グループ（EPG）を含むアプリケーション プロファイルです。テナントのエンティティはそのポリシーを継承します。 テナントには、1 つ以上の仮想ルーティングおよび転送（VRF）インスタンスまたはコンテキストを含めることができます。各コンテキストは、複数のブリッジ ドメインに関連付けることができます。

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。

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 *4*：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。

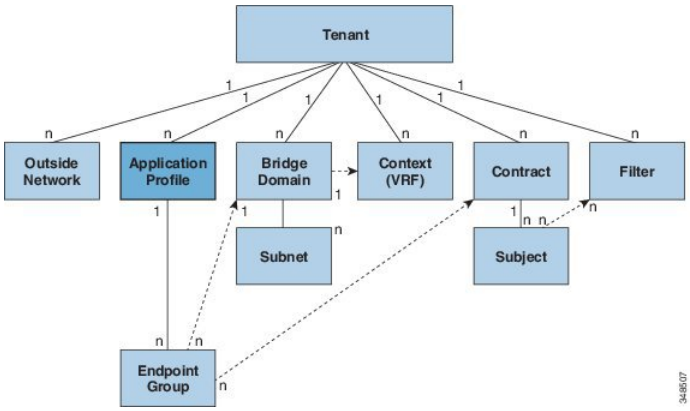
EPG には、セキュリティ、QoS、レイヤ 4 ～ レイヤ 7 サービスなどの共通のポリシー要件を持つエンドポイントが含まれます。 エンドポイントは個別に設定および管理されるのではなく、EPG 内に配置され、グループとして管理されます。 ACI ファブリックには、次のタイプの EPG を含めることができます。

- 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。

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、アプリケーション要件をモデル化します。 アプリケーションプロファイルは、EPGをグループ化する便利な論理コンテナです。 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。

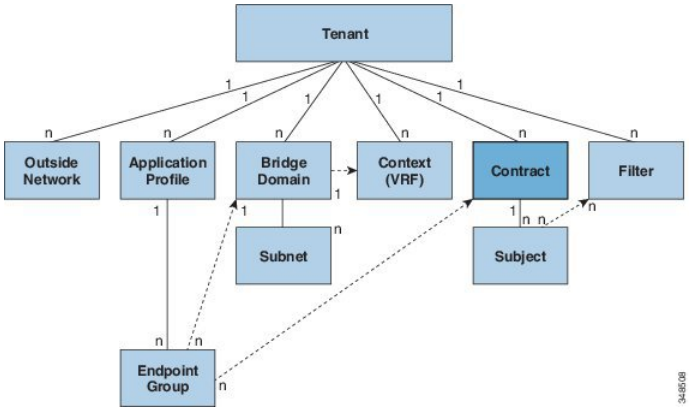
EPG は次のいずれかに従って組織化できます。

- 提供するアプリケーション（付録 A の例にある sap など）
- 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

コントラクト

EPG に加えて、コントラクト（vzBrCP）はポリシー モデルの主要オブジェクトです。 EPG は唯一、コントラクトのルールに従って他のEPGと通信できます。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 *6*：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るプロトコルやポートを含むEPG間を通過できるトラフィックのタイプを選択します。 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。

コントラクトは、次のタイプのエンドポイント グループ通信を管理します。

- 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 コンテキストがポリシーを適用していなくても、コントラクトがコンテキスト間でスタティック 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 アウトオブバンドまたはインバンド管理 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

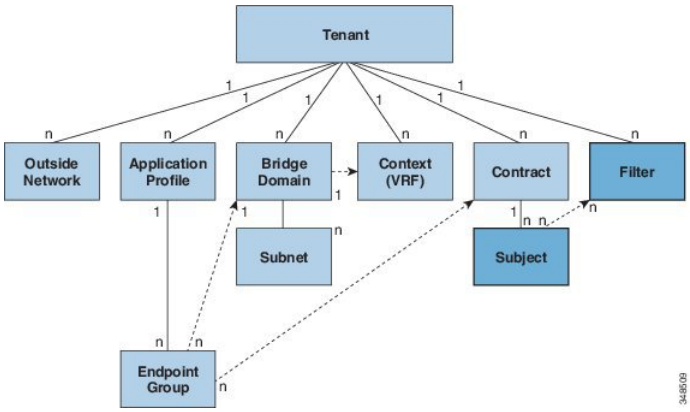
ラクトを提供すると、通信が提供されたコントラクトに準拠している限り、そのEPGとの通信は他のEPGから開始できます。 EPGがコントラクトを消費すると、消費するEPGのエンドポイントが、そのコントラクトを提供しているEPGの任意のエンドポイントとの通信を開始する場合があります。

（注） EPGは同じコントラクトを提供および消費できます。 EPGは複数のコントラクトを同時に提供および消費することもできます。

EPG通信を制御するラベル、フィルタ、およびサブジェクト

ラベル、サブジェクト、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 7: ラベル、サブジェクトおよびフィルタ



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現でき、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、付録Aのサンプル ポリシーでは、HTTPまたはHTTPSが必要な異なるEPG間でどのように通信が発生するかを識別するために、同一のコントラクトがどのようにラベル、サブジェクトおよびフィルタを使用するかが示されています。

ラベル、サブジェクト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。 付録 B は、すべてのラベルの一致タイプとその結果のシンプルな例を示します。

（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。

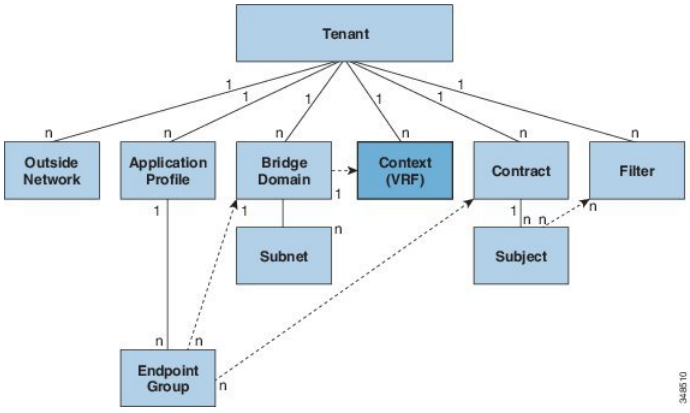
- EPG に適用されるサブジェクト ラベル。 サブジェクト ラベルの一致により、EPG はコントラクト内のサブジェクトのサブセットを選択することができます。
- EPG に適用されるプロバイダー/コンシューマ ラベル。 プロバイダー/コンシューマのラベルの一致により、コンシューマ EPG はプロバイダー EPG を選択でき、その逆も可能です。

- 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 タイプなどの TCP/IP ヘッダー フィールド、レイヤ 4 ポートなどです。 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 サブジェクトには、コントラクトを作成して消費する EPG 間で適用されるフィルタ（およびその方向）へのアソシエーションが含まれます。
- サブジェクトはコントラクトに含まれています。 コントラクト内の 1 つ以上のサブジェクト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。

コンテキスト

コンテキスト（fvCtx）は、一意なレイヤ 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）内のコンテキス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 *8*：コンテキスト



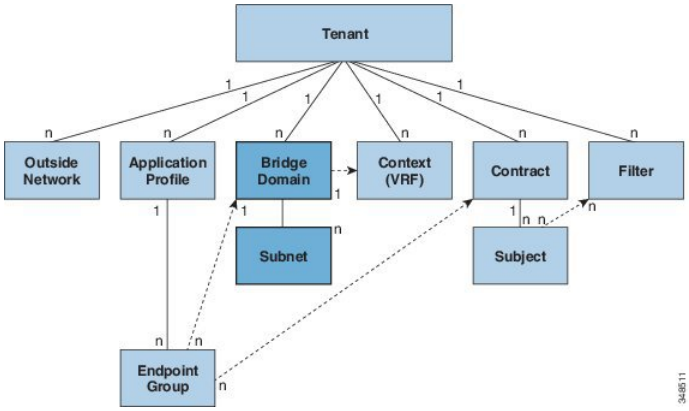
コンテキストは、レイヤ 3 のアドレス ドメインを定義します。 1 つ以上のブリッジ ドメインがコンテキストに関連付けられます。 レイヤ 3 ドメイン内のすべてのエンドポイントが一意の IP アドレスを持っている必要があります。なぜなら、ポリシーで許可されている場合にこれらのデバイス間でパケットを直接転送できるためです。 テナントには、複数のコンテキストを含めることができます。 管理者が論理デバイスを作成した後、管理者はデバイス クラスタの選択基準ポリシーを提供する論理デバイス コンテキストを作成できます。 論理デバイスは、コントラクト名、グラフ名、またはグラフ内の関数ノード名に基づいて選択で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

（注） コンテキストは、ネットワーキング ワールドの仮想ルーティングおよび転送（VRF）インスタンスに相当します。

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（L2）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 *9*：ブリッジ ドメイン



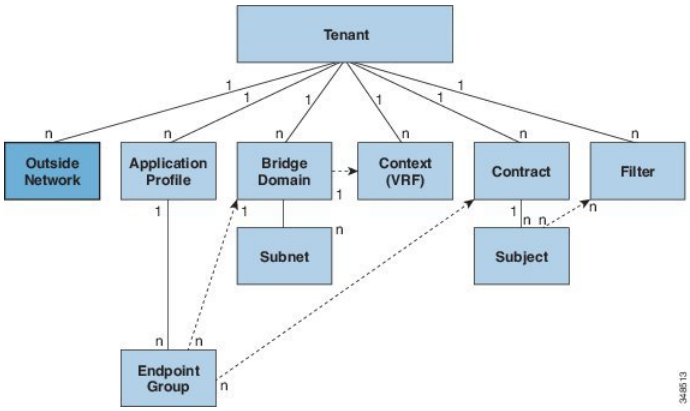
ブリッジ ドメインは、コンテキストにリンクされ、それに関連付けられた少なくとも 1 個のサブネット（fvSubnet）が必要です。 ブリッジ ドメインは、このようなフラッディングがイネーブルの場合に、一意のレイヤ 2 MAC アドレス空間およびレイヤ 2 フラッド ドメインを定義します。 コンテキストが一意の IP アドレス空間を定義する一方で、そのアドレス空間は複数のサブネットで構成できます。 それらのサブネットは、対応するコンテキストを参照する 1 つ以上のブリッジ ドメインで定義されます。

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。 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。

外部ネットワーク

外部ネットワークのオブジェクトポリシーは、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 *10*：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、ボーダー リーフとして知られています。 外部デバイスに接続するボーダー 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設定できます。ルーテッドインターフェイスの場合、スタティックまたはダイナミック ルーティングを使用できます。 ボーダー 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。

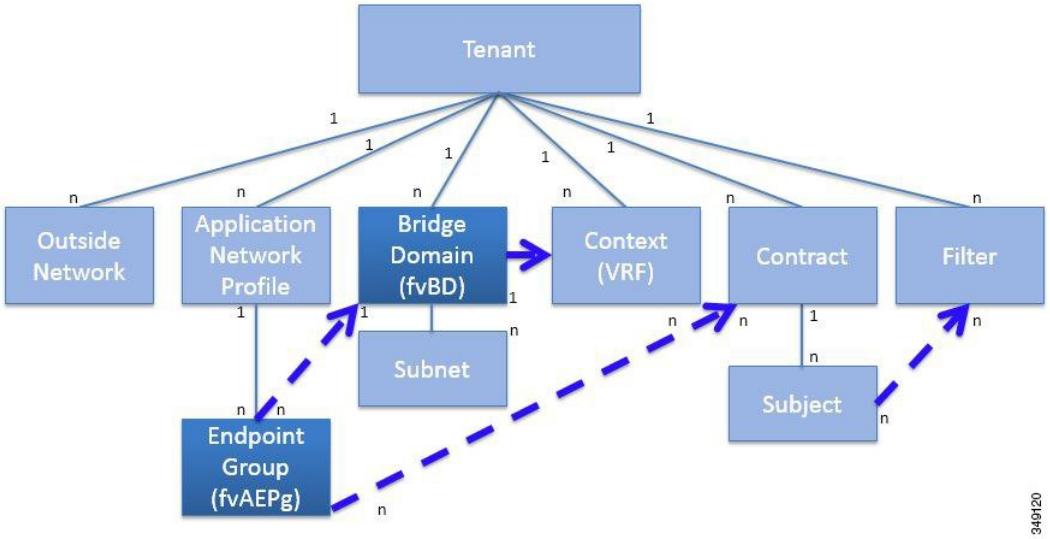
管理対象オブジェクトの関係とポリシー解決

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 のドメイン名（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 *11*：*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（fvDB）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。

名前付き関係に基づくポリシー解決の場合は、一致する名前を持つターゲット MO が現在のテナントに見つからない場合、ACI ファブリックは共通のテナントで解決を試行します。 たとえば、ユーザのテナント EPG がテナントに存在しないブリッジ ドメインを対象とした関係 MO を含んでいた場合、システムは共通の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。 存在しない場合、ACI ファブリックは共通のテナントでデフォルト ポリシーを検索します。 ブリッジドメイン、コンテキストおよびコントラクト（セキュリティ ポリシー）の名前付き関係はデフォルトに解決されません。

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サブジェクトを消費します。 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、サブジェクト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。

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 サーバの EPG への簡易な検索可能アクセスをイネーブルにするには、このようなすべての 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。