



Cisco Cloud Network Controller ポリシー モデル

- [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 \(1 ページ\)](#)
- [論理コンストラクト \(2 ページ\)](#)
- [Cisco ACI ポリシー管理情報モデル \(3 ページ\)](#)
- [テナント \(5 ページ\)](#)
- [クラウド コンテキスト プロファイル \(6 ページ\)](#)
- [VRF \(7 ページ\)](#)
- [クラウド アプリケーション プロファイル \(8 ページ\)](#)
- [クラウド エンドポイント グループ \(9 ページ\)](#)
- [コントラクト \(11 ページ\)](#)
- [クラウド テンプレートの概要 \(14 ページ\)](#)
- [管理対象オブジェクトの関係とポリシー解決 \(17 ページ\)](#)
- [デフォルト ポリシー \(18 ページ\)](#)

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。Cisco Cloud Network Controller は、クラウド 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。ユーザーまたはプロセスがクラウド インフラストラクチャ内のオブジェクトへの管理上の変更を開始すると、Cisco Cloud Network Controller 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、実際の管理対象項目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。

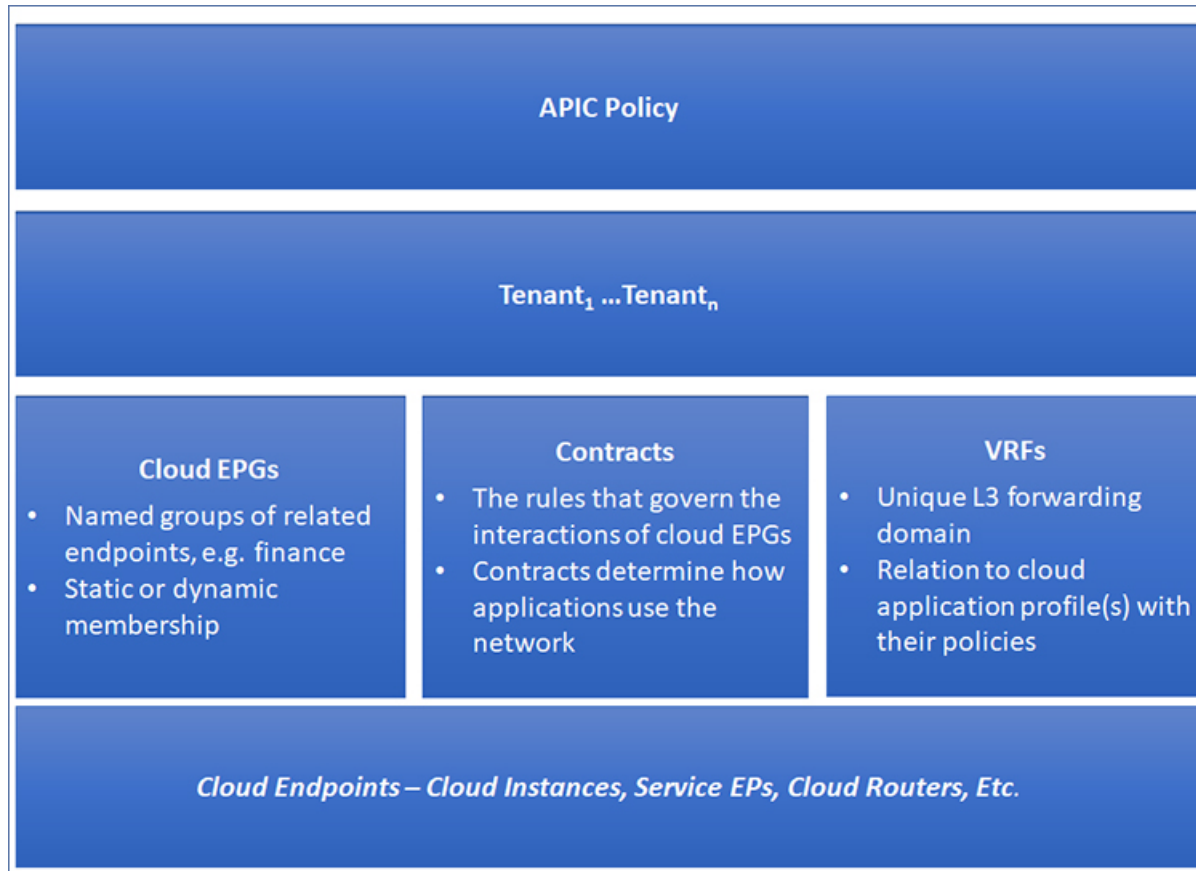
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシーモデルが更新されるまで、新たに接続されたエンドポイントとの通信を禁止します。
- ネットワーク管理者は、論理システムリソースを直接構成しません。代わりに、システム動作のさまざまな側面を制御する論理（ハードウェアに依存しない）構成とCisco Cloud Network Controller 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、Cisco Cloud Network Controller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。

論理コンストラクト

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、クラウドインフラストラクチャ全体を管理します。ポリシーモデルの論理構造は、クラウドインフラストラクチャの機能のニーズをクラウドインフラストラクチャ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



クラウドインフラストラクチャ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、ネットワークの動作を誘導する必要があり、その逆ではありません。

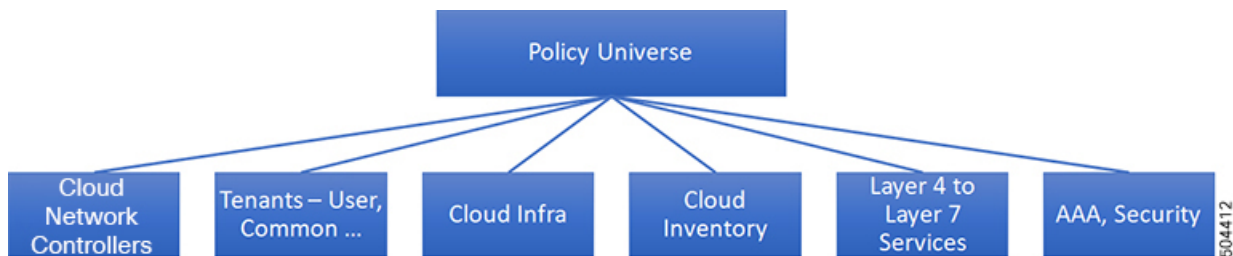
Cisco ACI ポリシー管理情報モデル

クラウドインフラストラクチャは、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）に記録される論理コンポーネントから構成されます。Cisco Cloud Network Controller は、情報モデルを保存および管理するプロセスを実行します。OSI 共通管理情報プロトコル（CMIP）および他の X.500 バリエーションと同様に、Cisco Cloud Network Controller 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、クラウドインフラストラクチャリソースの抽象化です。MO は、クラウドルー

ター、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、クラウドエンドポイント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、クラウドインフラストラクチャ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。

- テナントは、ポリシーのコンテナで、管理者はロール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。
 - 管理者は、ユーザーのニーズに応じてユーザテナントを定義します。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。
 - システムは共通テナントを提供しますが、クラウドインフラストラクチャ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。



(注) Cisco Cloud Network Controller は、レイヤ4からレイヤ7のサービスとしてロードバランサのみをサポートします。

- 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、クラウドインフラストラクチャの管理者が設定できます。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、クラウドインフラストラクチャ管理者によって構成可能です。
- クラウドインフラポリシーを使用すると、Cisco Cloud Network Controller を設定するときに、オンプレミスおよびリージョン間接続を管理できます。詳細については、[Cisco Cloud Network Controller インストールガイド (Cisco Cloud Network Controller Installation Guide)] を参照してください。

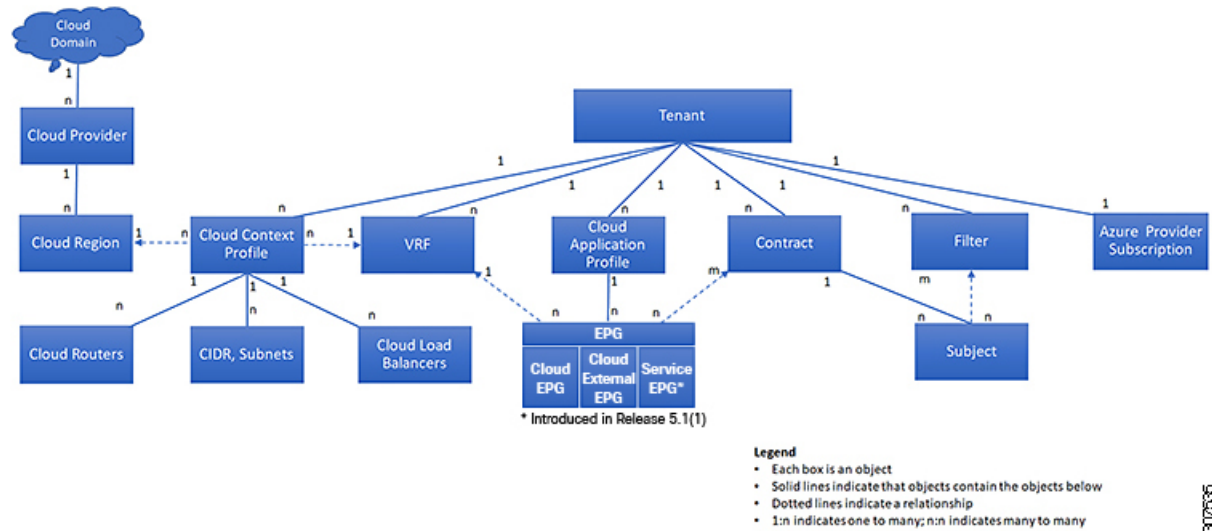
- クラウド インベントリは、GUI を使用してシステムのさまざまな側面を表示できるサービスです。たとえば、アプリケーションの側面から展開されたリージョンや、領域の側面から展開されたアプリケーションを表示できます。この情報は、クラウドリソースの計画とトラブルシューティングに使用できます。
- レイヤ4～レイヤ7のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムは動的に応答することができます。詳細については、[レイヤ4からレイヤ7サービスの展開](#)を参照してください。
- アクセス、認証、およびアカウントिंग（AAA）ポリシーは、Cisco Cloud Network Controller クラウドインフラストラクチャのユーザー権限、ロール、およびセキュリティドメインを管理します。詳細については、[Cisco Cloud Network Controller のセキュリティ](#)を参照してください。

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、管理者はデータ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、フィルタ、コントラクト、Virtual Routing and Forwarding (VRF) インスタンス、クラウドコンテキストプロフィール、Azure プロバイダ構成、およびエンドポイントグループ (EPG) を含むクラウドアプリケーションプロフィールが含まれるプライマリ要素です。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、それぞれを複数のクラウドコンテキストプロフィールに関連付けることができます。クラウドコンテキストプロフィールは、VRF、テナント、およびリージョンとともに、Azure のリソースグループを表します。VNET は、VRF 名に基づいてリソースグループ内に作成されます。

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。クラウドインフラストラクチャには、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 クラウドインフラストラクチャは、テナントネットワークに対して IPv4 およびデュアルスタック構成をサポートします。

クラウドコンテキストプロフィール

クラウドコンテキストプロフィールには、以下の Cisco Cloud Network Controller コンポーネントに関する詳細が含まれます：

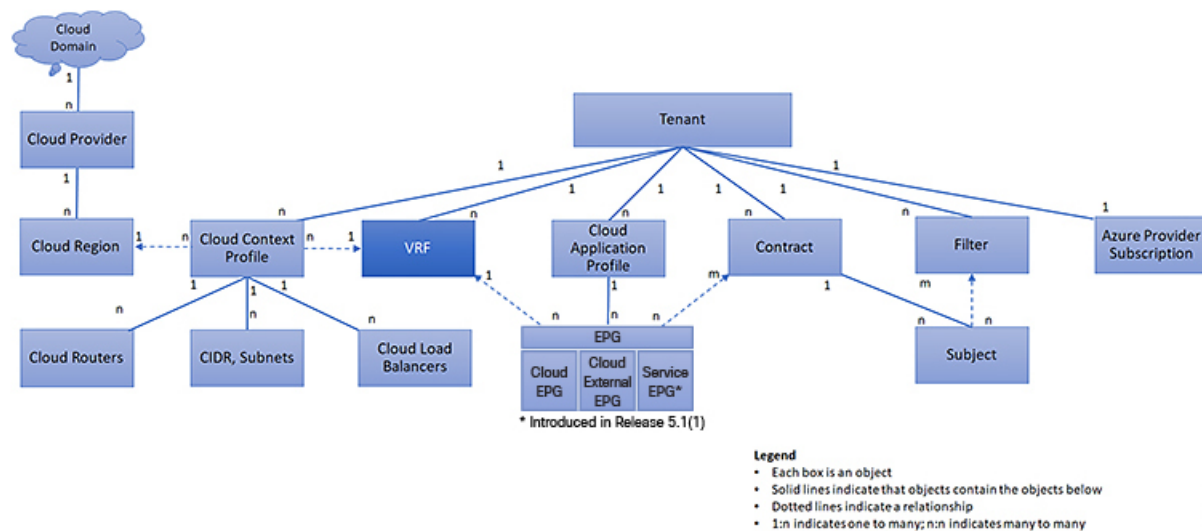
- CIDR
- VRF
- EPG
- [Regions]
- 仮想ネットワーク
- ルータ

- エンドポイント

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（Cisco Cloud Network Controller GUIではVRF）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。1つ以上のクラウドコンテキストプロファイルが VRF に関連付けられます。特定のリージョンの VRF に関連付けることができるクラウドコンテキストプロファイルは 1 つだけです。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 が含まれる場合があります。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。

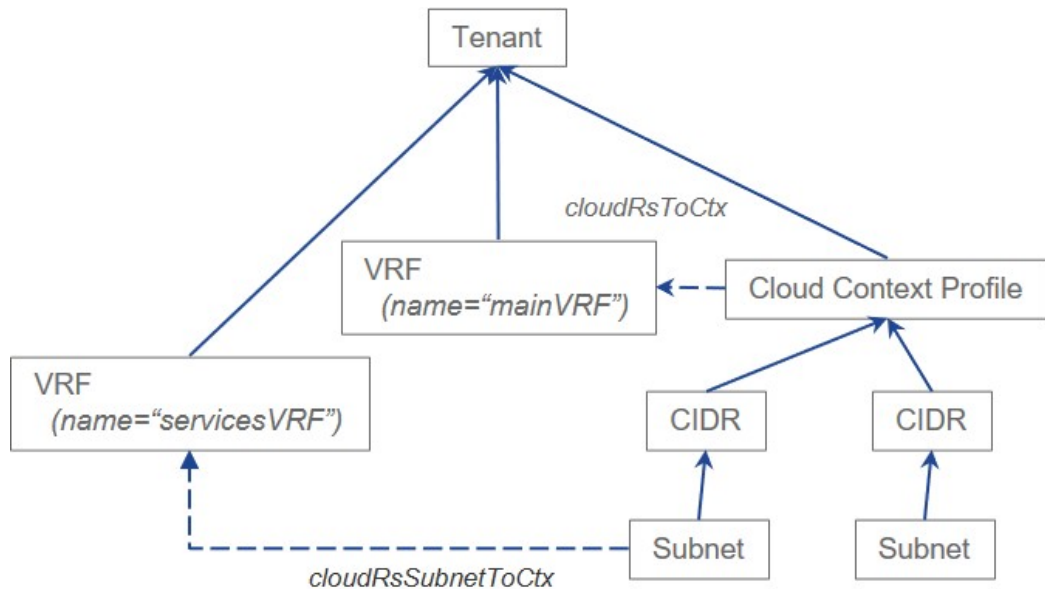
単一 VNet での複数の VRF のサポート

単一 VNet の下で複数の VRF がサポートされるようになりました。

複数の VRF に切り分けることができるインフラ（ハブ）VNet（インフラテナントの cloudCtxProfile）を持つことができます。それぞれの VRF のすべてのサブネットは、VRF 分離のためにクラウド内に個別のルートテーブルを持ちます。

また、インフラ VNet を超えて複数の VRF を分割して、単一の VNet に複数の VRF が存在する場合、任意の VNet を同じテナントの下に複数の VRF に分割できるようにすることもできます。これは、クラウドサービスアクセスなど、特定の VNet 内に複数のネットワーク (VRF) を分割し、クラウドの VNet 内の各 VRF に固有のルートテーブルを用意することで個別のルーティングを行う必要がある場合に役立ちます。

次の図は、同じテナント (VNet) の下に複数の VRF がある管理対象オブジェクト (MO) 関係ツリーの例を示しています。



この例では、同じテナント (VNet) の下に 2 つの VRF が存在します。

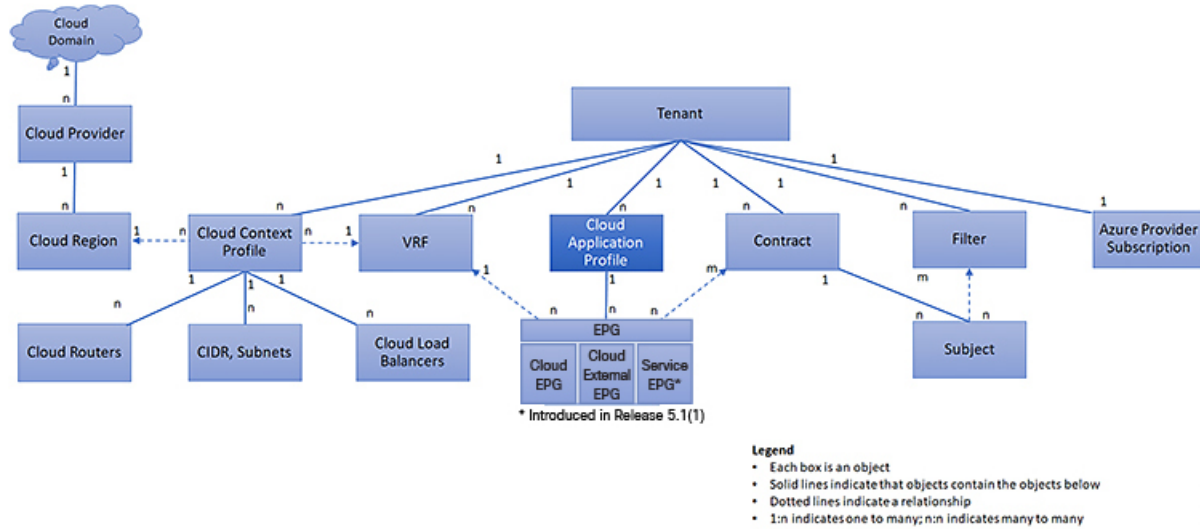
- mainVRF という名前のプライマリ VRF
- 名前が servicesVRF のセカンダリ VRF

2 番目の CIDR ブロックとサブネットは、同じテナント (VNet) の下の同じクラウドコンテキストプロフィールに存在しますが、その 2 番目の CIDR ブロックとサブネットは、その同じ VNet 内のセカンダリ VRF に関連付けられています。

クラウドアプリケーション プロファイル

クラウドアプリケーションプロフィール (cloudAp) は、ポリシー、サービスおよび EPG 間の関係を定義します。次の図は、管理情報ツリー (MIT) 内のクラウドアプリケーションプロフィールの場所と、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: クラウド アプリケーション プロファイル



クラウドアプリケーションプロファイルには、1つ以上のクラウド 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、ストレージサービス内にあるデータ、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。クラウド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）クラウド EPG が含まれます。

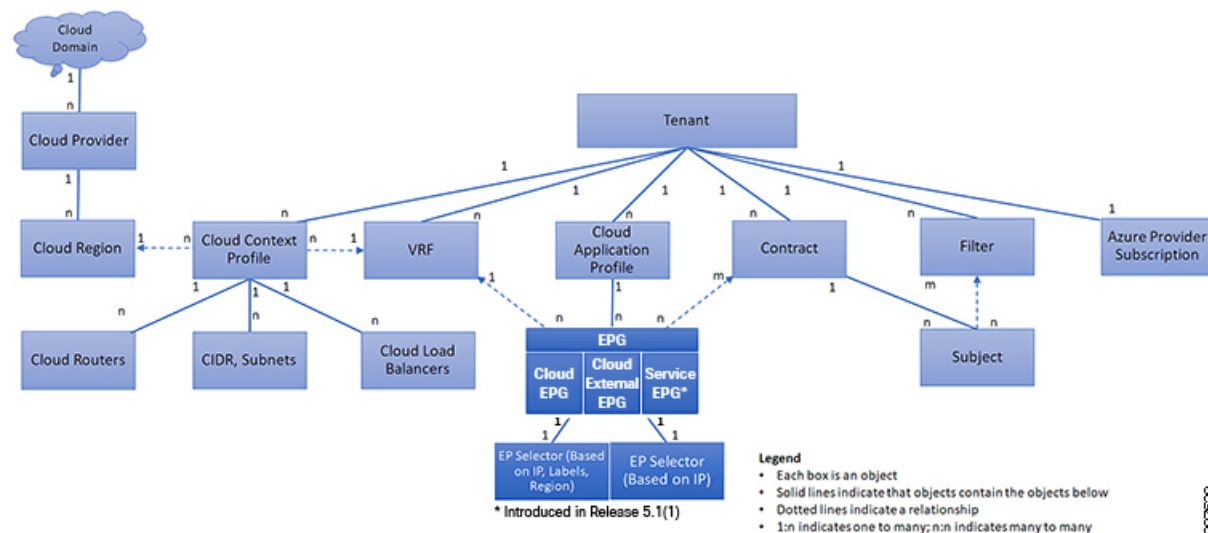
クラウド EPG は次のいずれかに従って組織化できます。

- 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）
- クラウドインフラストラクチャ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

クラウドエンドポイントグループ

クラウドエンドポイントグループ（クラウド 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クラウド 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: クラウドエンドポイントグループ



クラウド 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、ネットワークに接続されるデバイスです。エンドポイントは、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) を持ち、仮想です。エンドポイントのアドレスを知ること、他のすべての ID の詳細にアクセスすることもできます。クラウド 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、ストレージサービス、またはクライアントが含まれます。クラウド 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 クラウドインフラストラクチャには、次のタイプのクラウド EPG を含めることができます

- クラウド エンドポイント グループ (cloudEPg)
- クラウド外部エンドポイントグループ (cloudExtEPg)
- クラウドサービス エンドポイントグループ (cloudSvcEPg) : リリース 5.1(2) で導入されました。詳細については、「クラウドサービス エンドポイントグループ」を参照してください。

クラウド EPG には、セキュリティまたはレイヤ4からレイヤ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、クラウド EPG 内に配置され、グループとして管理されます。

ポリシーはクラウド 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。

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

クラウドインフラストラクチャへの WAN ルータ接続は、スタティッククラウド EPG を使用する設定の1つの例です。クラウドインフラストラクチャへの WAN ルータ接続を設定するに

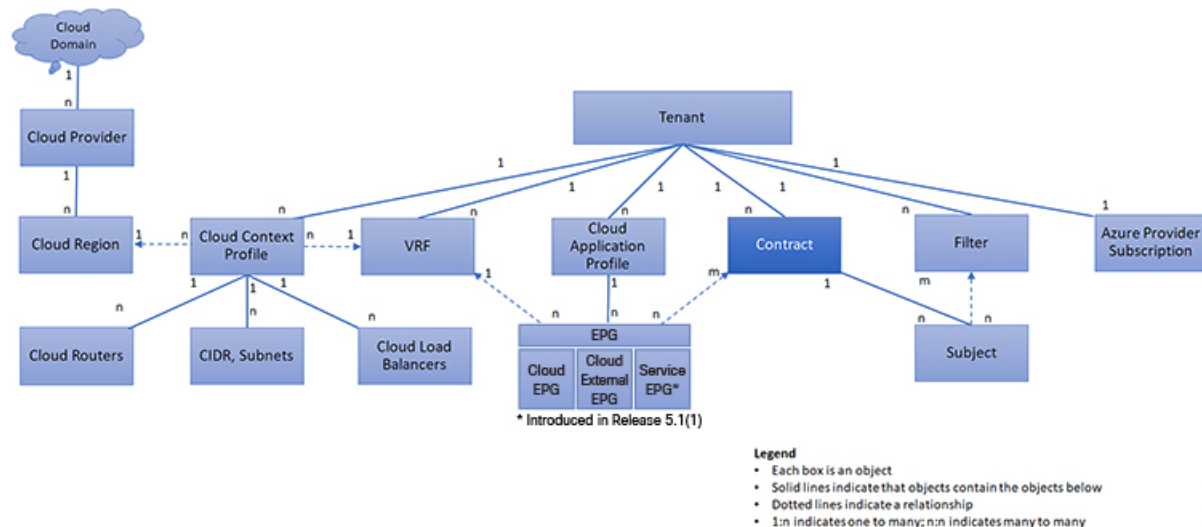
は、関連付けられている WAN サブネット内のエンドポイントを含む cloudExtEPg クラウド EPG を管理者が設定します。クラウドインフラストラクチャは、エンドポイントの接続ライフサイクルが経過する間に、検出プロセスを通してクラウド EPG のエンドポイントについて学習します。エンドポイントを学習すると、クラウドインフラストラクチャは、それに基づいて cloudExtEPg クラウド EPG ポリシーを適用します。たとえば、WAN 接続クライアントがアプリケーション (cloudEPg) クラウド EPG 内でサーバとの TCP セッションを開始すると、cloudExtEPg クラウド EPG は、cloudEPg クラウド 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間の通信が終了すると、その WAN エンドポイントはもうクラウドインフラストラクチャ内に存在しません。

Cisco Cloud Network Controller はエンドポイントセレクタを使用して、エンドポイントをクラウド EPG に割り当てます。エンドポイントセレクタは、基本的に言って、Cisco ACI によって管理される Azure VNET に割り当てられたクラウドインスタンスに対して実行される一連のルールです。エンドポイントインスタンスに一致するエンドポイントセレクタルールは、そのエンドポイントをクラウド EPG に割り当てます。エンドポイントセレクタは、Cisco ACI で使用可能な属性ベースのマイクロセグメンテーションに似ています。

コントラクト

クラウド 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。クラウド EPG が他のクラウド 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 7: 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1つまたは複数のタイプを選択します。コントラクトがない場合、EPG間通

信はデフォルトで無効になります。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、次のタイプのクラウド EPG 通信を管理します。

- クラウド EPG (cloudEPg) 間の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ても、コントラクトが VRF 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。

- クラウド EPG とクラウド外部 EPG 間 (cloudExtEPg)

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クラウド EPG 間の通信を制御します。クラウド 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。クラウド EPG がコントラクトを提供すると、そのクラウド EPG 内のクラウドエンドポイントとの通信は、通信が提供されたコントラクトに準拠している限り、他のクラウド EPG 内のクラウドエンドポイントから開始できます。クラウド EPG がコントラクトを使用すると、そのクラウド EPG のクラウドエンドポイントは、コントラクトを指定したクラウド EPG のクラウドエンドポイントと通信を開始できます。

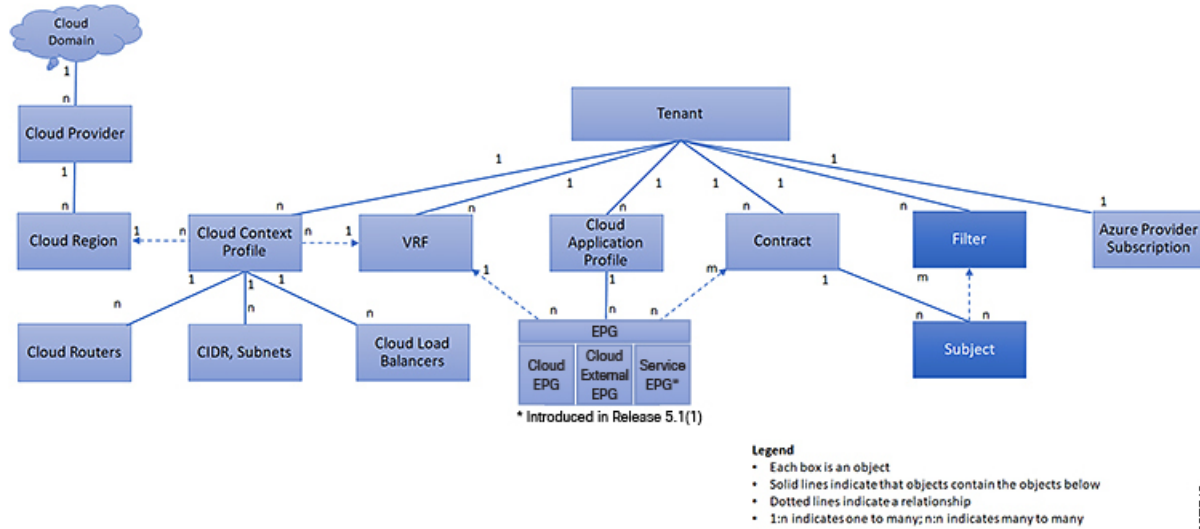


(注) 1 つのクラウド EPG で同じコントラクトを指定および使用できます。クラウド EPG は複数のコントラクトを同時に指定および使用することもできます。

クラウド EPG 通信を制御するフィルタおよびサブジェクト

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クラウド 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 8: 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、複数のクラウド EPG は複数のコントラクトを消費および提供できます。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。



(注) サブジェクトは Cisco Cloud Network Controller で非表示になり、設定できません。Azure にインストールされているルールの場合、フィルタ エントリで指定された送信元ポートは考慮されません。

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クラウド EPG 通信を定義します。

- フィルタは、レイヤ 3 ~ 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、クラウド 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。コントラクトのサブジェクトは、コントラクトを提供する側と消費する側のクラウド 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。
- 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。
- Azure 構造体でレンダリングされる ACI 契約は常にステートフルであり、リターントラフィックを許可します。

クラウドテンプレートの概要

クラウドテンプレートは、Cisco Cloud Network Controller インフラ ネットワークを設定および管理するテンプレートを提供します。テンプレートには、設定に最も重要な要素のみが必要です。これらの要素から、クラウドテンプレートはCisco Cloud Network Controller インフラ ネットワークのセットアップに必要な詳細設定を生成します。ただし、1 回限りの設定生成ではなく、テンプレート入力要素を追加、変更、または削除できます。クラウドテンプレートは、それに応じて結果の設定を更新します。

Azure ネットワーク構成の中央のうちいずれかは、仮想プライベートクラウド (VNET) です。Azure は世界中の多くのリージョンをサポートしており、1 つの VNET は 1 つのリージョンに固有です。

クラウドテンプレートは、1 つ以上のリージョン名を承認し、それらのリージョンでインフラ VNET の構成全体を生成します。それらはインフラ VNET です。Azure VNET に対応する Cisco Cloud Network Controller 管理対象オブジェクト (MO) は、cloudCtxProfile です。クラウドテンプレートで指定されたすべてのリージョンに対して、cloudCtxProfile 設定が生成されます。cloudCtxProfile は、リージョンに対応するすべての設定の最上位 MO です。その下には、特定の設定をキャプチャするためのツリーとして編成された他の多くの MO があります。インフラ VNet の cloudCtxProfile MO は、クラウドテンプレートにより生成されます。これは `ctxProfileOwner == SYSTEM` を伝送します。これは、この MO がシステムによって生成されることを意味します。非インフラストラクチャ ネットワークの場合、cloudCtxProfile を直接設定できます。この場合、cloudCtxProfile は `ctxProfileOwner == USER` を伝送します。

Azure VNet の主要なプロパティは CIDR です。Cisco Cloud Network Controller では、ユーザ VNet で CIDR を選択して展開できます。インフラ VNet の CIDR は、クラウドサイトの最初のセットアップ時にユーザーによってクラウドテンプレートに提供され、クラウドテンプレートによって Azure クラウドに展開されます。

リリース 5.0(2) 以降、createdBy という新しいプロパティが CIDR に追加されています。この createdBy プロパティのデフォルト値は USER です。

- すべてのユーザー作成 CIDR について、createdBy プロパティの値は USER に設定されます。
- クラウドテンプレートで作成された CIDR の場合、createdBy プロパティの値は SYSTEM に設定されます。

複数の CIDR ブロックとサブネットブロックをインフラ VNet で構成できます。CIDR を作成し、インフラストラクチャ VNet にサブネットを関連付けることができます。クラウドテンプレート サブネットは overlay-1 VRF にマッピングされますが、ユーザーが作成したサブネットの場合、同じインフラ VNet 内のセカンダリ VRF へのサブネットから VRF へのマッピングを手動で構成する必要があります。それぞれの VRF のすべてのサブネットは、VRF 分離のためにクラウド内に個別のルート テーブルを持ちます。

インフラ テナントでクラウド EPG とクラウド外部 EPG を作成できます。すべてのクラウド EPG とクラウド外部 EPG は、インフラ テナントのセカンダリ VRF に関連付けられます。セカンダリ VRF 内のクラウド EPG は、セカンダリ VRF 内の他のクラウド EPG およびクラウド外

部 EPG と通信可能で、他のユーザー テナント VRF 内のクラウド EPG とも通信できます。既存の「クラウド インフラ」アプリケーション プロファイルを使用せず、代わりにインフラ テナントに新しいアプリケーション プロファイルを作成し、新しいアプリケーション プロファイルをセカンダリ VRF のクラウド EPG およびクラウド外部 EPG に関連付けることをお勧めします。

詳細については、[Cisco Cloud Network Controller GUI を使用したアプリケーション EPG の作成](#)を参照してください。

クラウドテンプレートは、cloudCtxProfile サブツリーに次のような多数の MO を生成して管理します。

- サブネット
- クラウド ルータ
- クラウド ルータ インターフェイスの IP アドレス割り当て
- トンネルの IP アドレスの割り当てと設定
- ループバックの IP アドレスの割り当てと設定

クラウドテンプレートがない場合は、これらの設定と管理を担当します。

Cisco Cloud Template MO テーブルには、クラウドテンプレートへの入力 (MO) の概要が含まれています。

表 1:クラウドテンプレート MO

月	目的
cloudtemplateInfraNetwork	クラウドテンプレート設定のルート。次の属性が含まれます。 numRoutersPerRegion : cloudtemplateIntNetwork で指定された各 cloudRegionName のクラウド ルータの数。

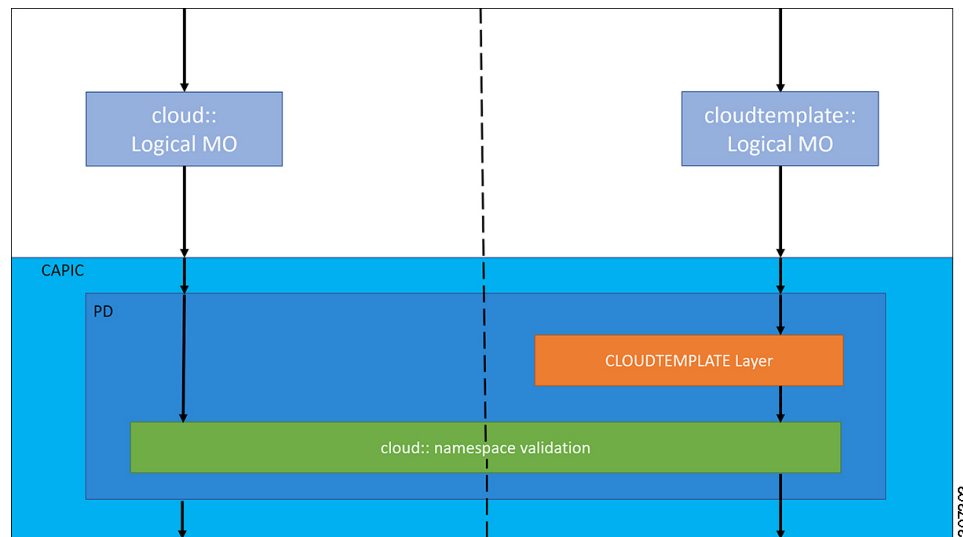
月	目的
cloudtemplateProfile	<p>すべてのクラウドルータの設定プロファイル。次の属性が含まれます。</p> <ul style="list-style-type: none"> routerUsername <p>(注)</p> <ul style="list-style-type: none"> ユーザ名を「admin」にすることはできません。 Azure からのユーザー名の制限が適用されます。 <ul style="list-style-type: none"> routerPassword routerThroughput routerLicenseToken routeDataInterfacePublicIP routerMgmtInterfacePublicIP
cloudtemplateIntNetwork	<p>クラウドルータを展開する場所を指定するリージョンのリストが含まれます。各リージョンは、cloudRegionName 子 MO を介してキャプチャされます。</p>
cloudtemplateExtNetwork	<p>クラウド外部のインフラ ネットワーク設定入力が含まれます。</p> <p>クラウドルータが外部ネットワーキング用に設定されているリージョンのリストが含まれます。</p> <p>各リージョンは、cloudRegionName 子 MO を介してキャプチャされます。</p>
cloudtemplateVpnNetwork	<p>ACI オンプレミス サイトまたは別の Cisco Cloud Network Controller サイトで VPN を設定するための情報が含まれています。</p>
cloudtemplateIpSecTunnel	<p>ACI オンプレミス サイトの IPSec ピアの IP アドレスをキャプチャします。</p>
cloudtemplateOspf	<p>VPN 接続に使用する OSPF エリアをキャプチャします。</p>
cloudtemplateBgpEvpn	<p>オンプレミス サイトとの BGP セッションを設定するために、ピア IP アドレス、ASN などをキャプチャします。</p>

Cisco Cloud Network Controller では、クラウドテンプレートにより、MO の階層化は通常の Cisco APIC とは若干異なります。通常の Cisco APIC では、2 つの変換レイヤを通過する論理 MO をポストします。

1. 論理 MO から解決済み MO へ
2. 解決済みの MO から具体的な MO

Cisco Cloud Network Controller には、インフラネットワーク用の追加の変換レイヤがあります。この追加レイヤでは、クラウドテンプレートが `cloudtemplate::` 名前空間の論理 MO をクラウド名前空間の論理 MO に変換します。インフラネットワーク外の設定では、クラウド名前空間に論理 MO をポストします。この場合、MO は通常の Cisco APIC と同様に通常の 2 層変換を実行します。

図 9: クラウドおよびクラウドテンプレート MO 変換



(注) クラウドテンプレートの設定については、[Cisco Cloud Network Controller コンポーネントの構成](#) を参照してください。

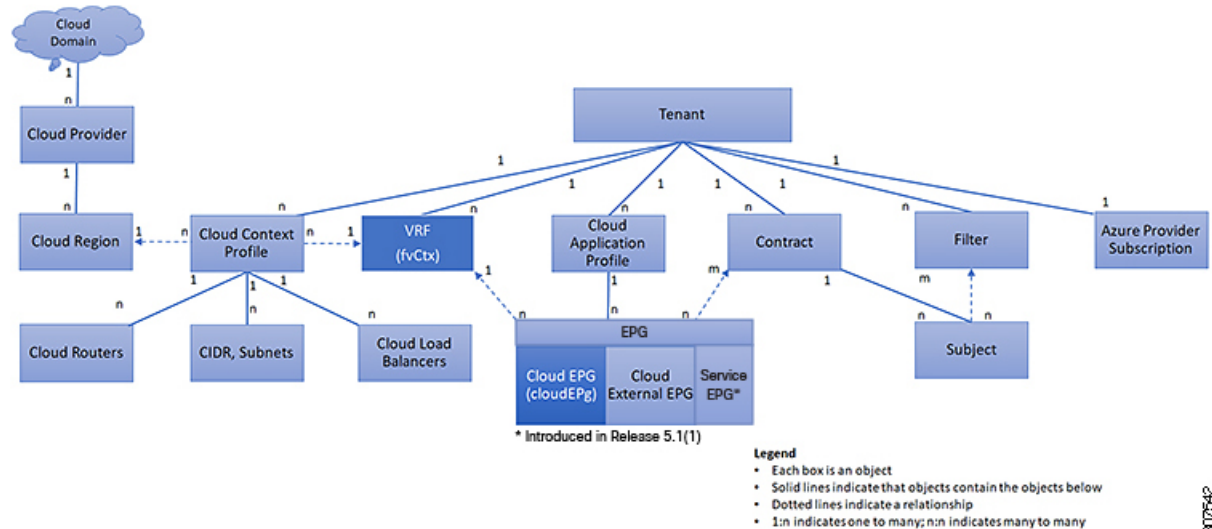
管理対象オブジェクトの関係とポリシー解決

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。

- `cloudRsCloudEPgCtx` などの明示的な関係は、ターゲット MO 識別名（DN）に基づく関係を定義します。
- 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 10: MO の関係



たとえば、クラウド EPG と VRF 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 (cloudEPg) には、ターゲットの VRF MO (fvCtx) の名前が付いた関係 MO (cloudRsCloudEPgCtx) が含まれます。たとえば、実稼働が VRF 名 (fvCtx.name=production) である場合、関係の名前は実稼働 (cloudRsCloudEPgCtx.tnFvCtxName=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 クラウドインフラストラクチャは共通のテナントで解決を試行します。たとえば、ユーザのテナントクラウド EPG がテナントに存在しない VRF 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 クラウドインフラストラクチャは、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 クラウドインフラストラクチャは共通のテナントでデフォルトポリシーを検索します。クラウドコンテキストプロファイル、VRF 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。

デフォルト ポリシー



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 クラウドインフラストラクチャは、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。

- Cloud Azure プロバイダ (インフラ テナント用)
- 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、現在または将来の設定がデフォルト 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。

デフォルト ポリシーは、次の複数の目的に使用されます。

- クラウド インフラストラクチャの管理者がモデル内のデフォルト値を上書きできます。
- 管理者が明示的なポリシーを提供しない場合、Cisco Cloud Network Controller はデフォルトのポリシーを適用します。管理者はデフォルトのポリシーを作成でき、管理者が明示的なポリシーを提供しない限り、Cisco Cloud Network Controller はそのポリシーを使用します。

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) 上記のシナリオは、テナントの VRF 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。

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を解決しようとします。クラウドコンテキスト プロファイルと VRF は、このルールの例外です。

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。