Cisco Cloud Network Controller ポリシー モデル

CNC ポリシーモデルについて

CNC 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。

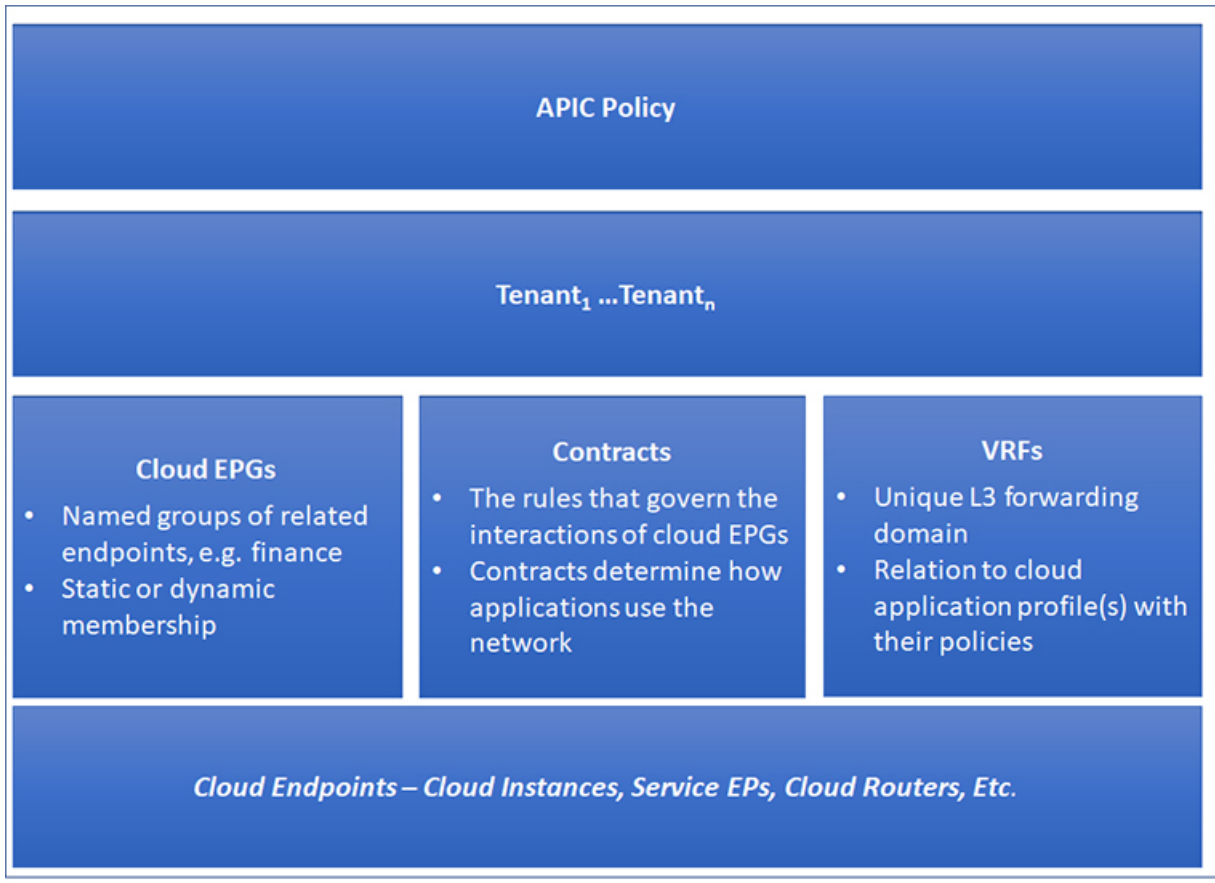
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシ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、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、CNC ポリシー モデルの論理構造の概要を示します。

図 *1 : CNC* 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。

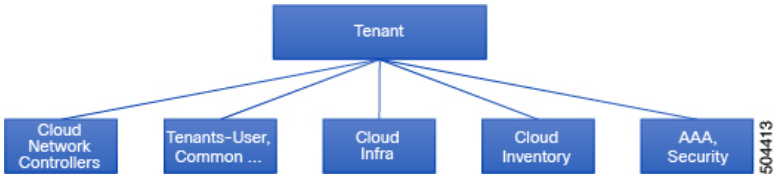
Cisco CNC ポリシー管理情報モデル

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 バリアントと同様に、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 CNC* 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。

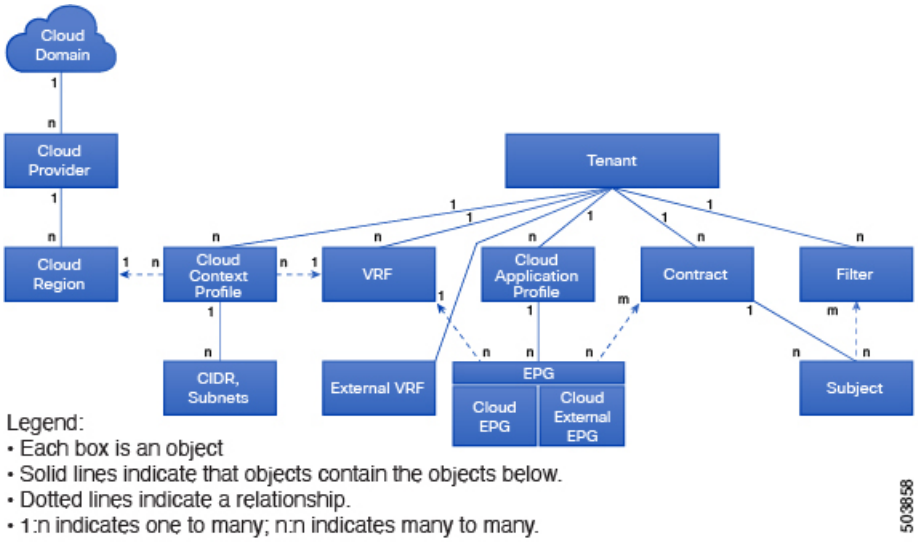
- テナントは、ポリシーのコンテナで、管理者はロールベースのアクセス コントロールを実行できます。システムにより、次の 4 種類のテナントが提供されます。
  - 管理者は、ユーザーのニーズに応じてユーザ テナントを定義します。アプリケーション、データベース、Web サーバ、ネットワークアタッチド ストレージ、仮想マシンなどのリソースの動作を管理するポリシーが含まれます。
  - システムは共通テナントを提供しますが、クラウドインフラストラクチャ管理者が設定できます。ファイアウォール、ロードバランサ、侵入検知アプライアンスなど、すべてのテナントにアクセス可能なリソースの動作を管理するポリシーが含まれます。
  - 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、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。
- アクセス、認証、およびアカウンティング（AAA）ポリシーは、Cisco Cloud ACI 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、Virtual Routing and Forwarding（VRF）インスタンス、Google Cloud プロバイダー構成、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。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 プロファイルに関連付けることができます。クラウド コンテキスト プロファイルは、VRF、テナント、およびリージョンとともに、Google Cloud のリソース グループを表します。VPC 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。CNC 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 構成のみをサポートします。

クラウド コンテキスト プロファイル

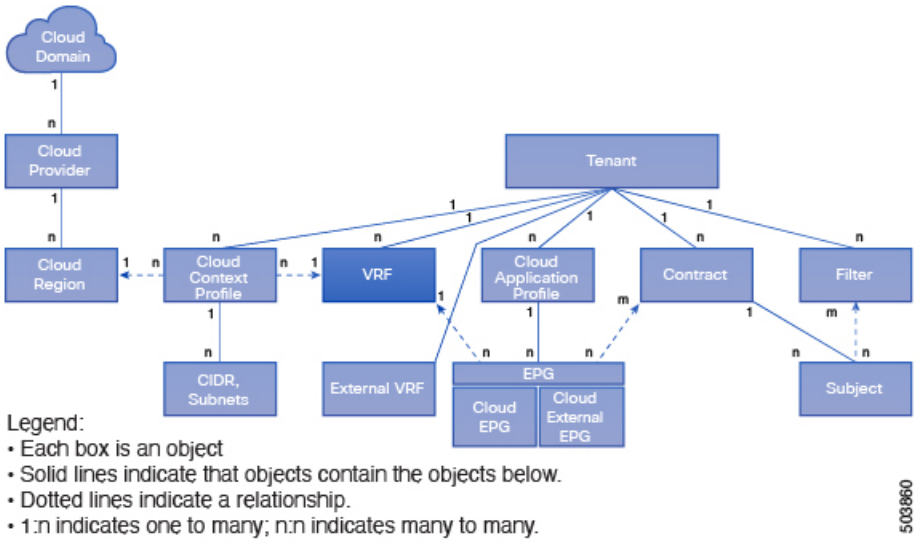
クラウド コンテキスト プロファイルには、以下の Cisco Cloud Network Cntroller コンポーネントに関する詳細が含まれます：

- CIDR
- VRF
- EPG
- [Regions]
- VPC
- 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 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。

外部 VRF

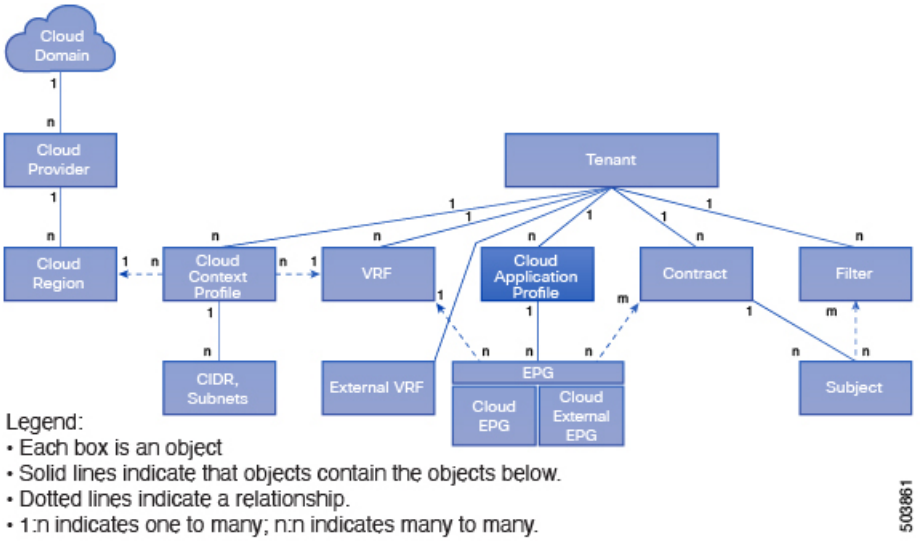
外部 VRFは、Cisco クラウド ネットワーク コントローラで使用可能な VRF のタイプです。外部 VRF はクラウドのプレゼンスをもたない固有の VRF です。このVRFは、 Cisco Cloud Network Controller によって使用されるクラウド コンテキスト プロファイルでは参照されません。

外部 VRFは、他のクラウドサイトまたはオンプレミスサイトに接続されている外部ネットワークを表します。複数のクラウド VRF は、外部 VRF にルートをリークしたり、外部 VRF からルートを取得したりできます。外部 VRFで外部ネットワークが作成されると、VRF 間ルーティングが設定され、外部ネットワークで受信およびアドバタイズされたルートが 外部 VRF で受信またはアドバタイズされます。 を参照してください。

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 (`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:* 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。

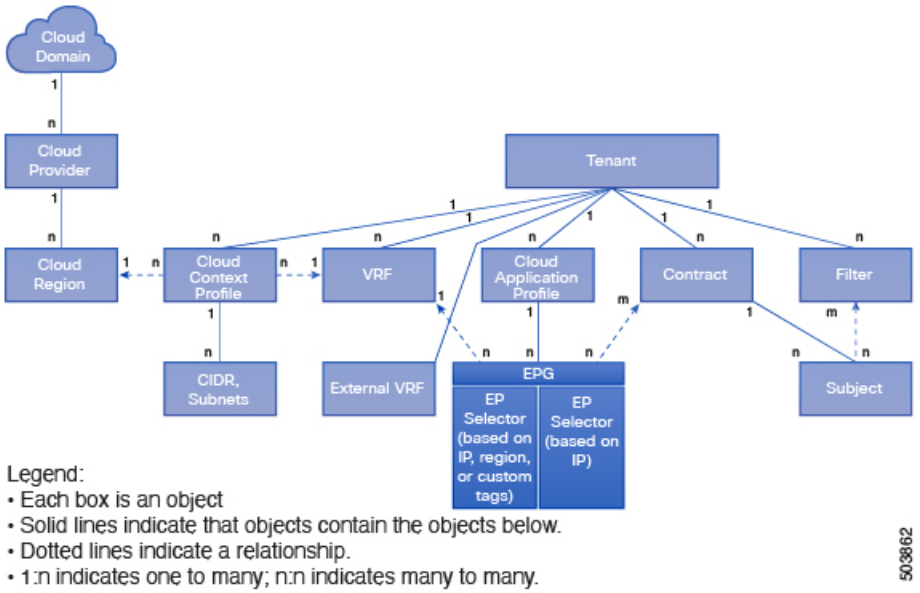
クラウド EPG は次のいずれかに従って組織化できます。

- 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。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。

CNC 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 EPG には、セキュリティ 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の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 CNC によって管理される Google Cloud VPC 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。

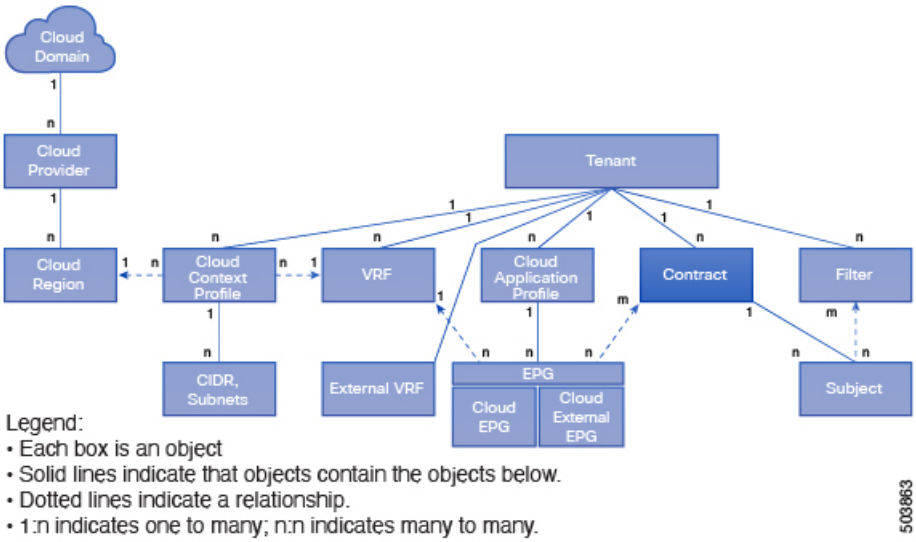


図 7: コントラクト

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なくても、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`）

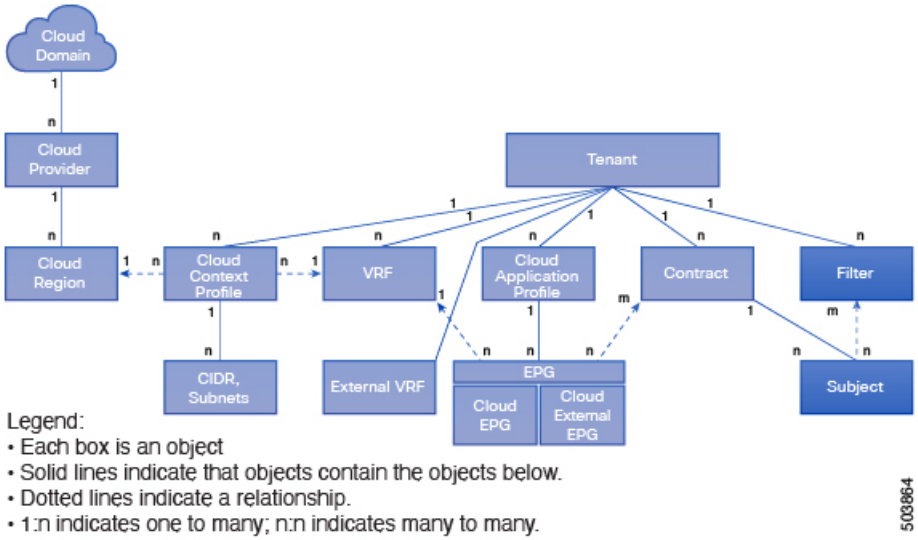
コントラクトは、プロバイダー、コンシューマ、またはその両方とラベル付されたクラウド EPG 間の通信を制御します。クラウド EPG とコントラクトの関係は、プロバイダーまたはコンシューマです。クラウド EPG がコントラクトを提供すると、そのクラウド EPG 内のクラウドエンドポイントとの通信は、通信が提供されたコントラクトに準拠している限り、他のクラウド EPG 内のクラウドエンドポイントから開始できます。クラウド EPG がコントラクトを使用すると、そのクラウド EPG のクラウドエンドポイントは、コントラクトを指定したクラウド EPG のクラウドエンドポイントと通信を開始できます。

（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。Google Cloud 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。

- Google Cloud構造体でレンダリングされるCNCコントラクト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、テンプレート入力の要素を追加、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。

Google Cloudネットワーク設定の中心的な機能の1つは、仮想プライベート クラウド（VPC）です。Google Cloudは世界中の多くの地域をサポートし、1つのVPCは1つの地域に固有です。

クラウドテンプレートは1つ以上のリージョン名を受け入れ、それらのリージョンのインフラVPCの設定全体を生成します。これらはインフラ VPC です。Google Cloud VPCに対応するCiscoクラウドネットワーク コントローラ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VPCの`cloudCtxProfile`MOは、クラウドテンプレートによって生成されます。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。

Google Cloud VPCの主要なプロパティはCIDRです。Cisco Cloud Network Controllerでは、ユーザーVPCでCIDRを選択して展開できます。インフラVPCのCIDRは、クラウドサイトの初期設定時に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Google Cloudに展開されます。

CIDRでは、`createdBy`というプロパティも使用できます。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。

インフラ VPC では複数の CIDR およびサブネット ブロックを設定できます。CIDR を作成し、インフラ VPC でサブネットを関連付けることができます。クラウド テンプレートのサブネットは、overlay-1 VRF にマッピングされます。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。

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*

MO	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。
`cloudtemplateIntNetwork`	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。
`cloudtemplateExtNetwork`	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。 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。 各リージョンは、`cloudRegionName`子 MO を介してキャプチャされます。

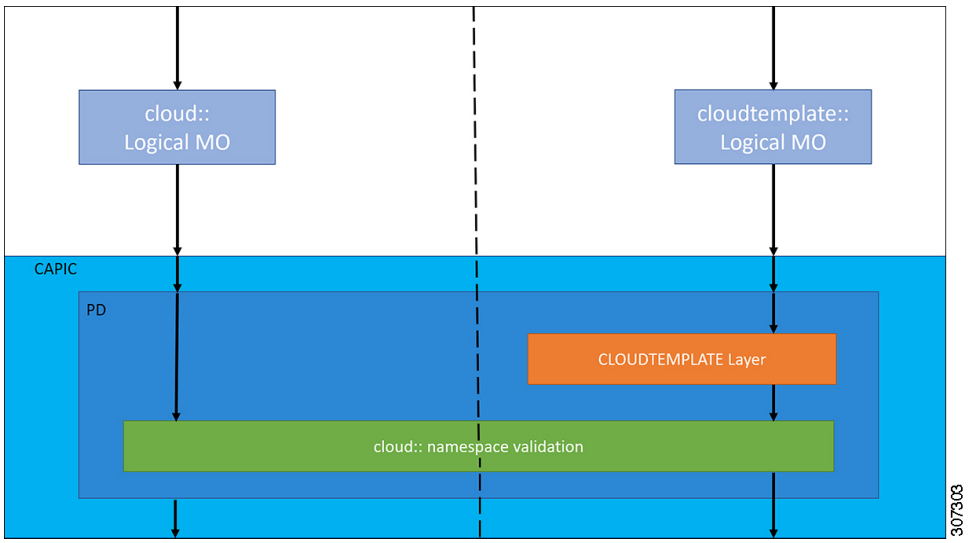
MO	目的
cloudtemplateIpSecTunnel	ACI オンプレミス サイトの IPSec ピアの IP アドレスをキャプチャします。

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。

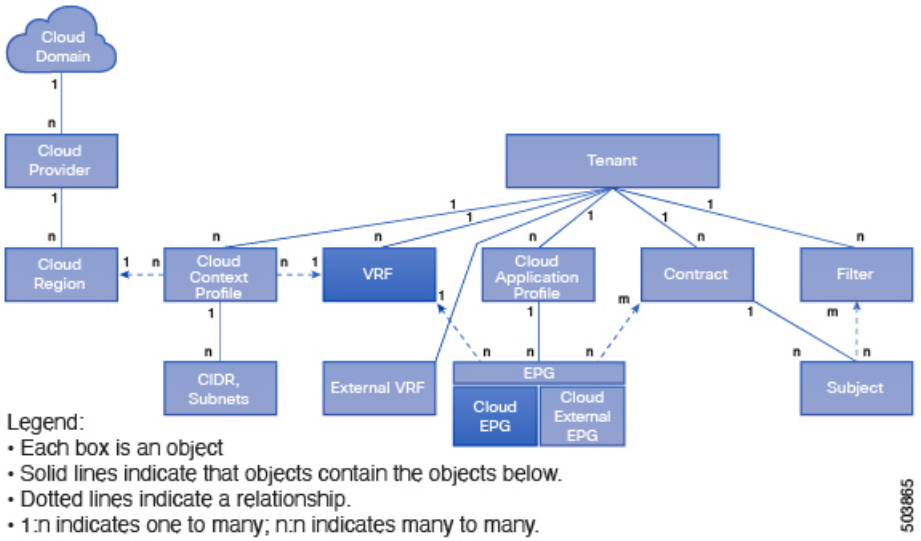
管理対象オブジェクトの関係とポリシー解決

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、CNC 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、CNC 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、CNC 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。

CNC 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。これらのデフォルト ポリシーの例は次のとおりです。

- Google Cloud プロバイダー（インフラ テナント用）
- モニタリング

（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。

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。