Cisco Cloud APIC 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）
- クラウド コンテキスト プロファイル （6 ページ）
- VRF （18 ページ）
- クラウド アプリケーション プロファイル （19 ページ）
- クラウド エンドポイント グループ （20 ページ）
- コントラクト （21 ページ）
- クラウド テンプレートの概要 （24 ページ）
- 管理対象オブジェクトの関係とポリシー解決 （27 ページ）
- デフォルト ポリシー （28 ページ）
- 共有サービス （29 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 APIC 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 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。

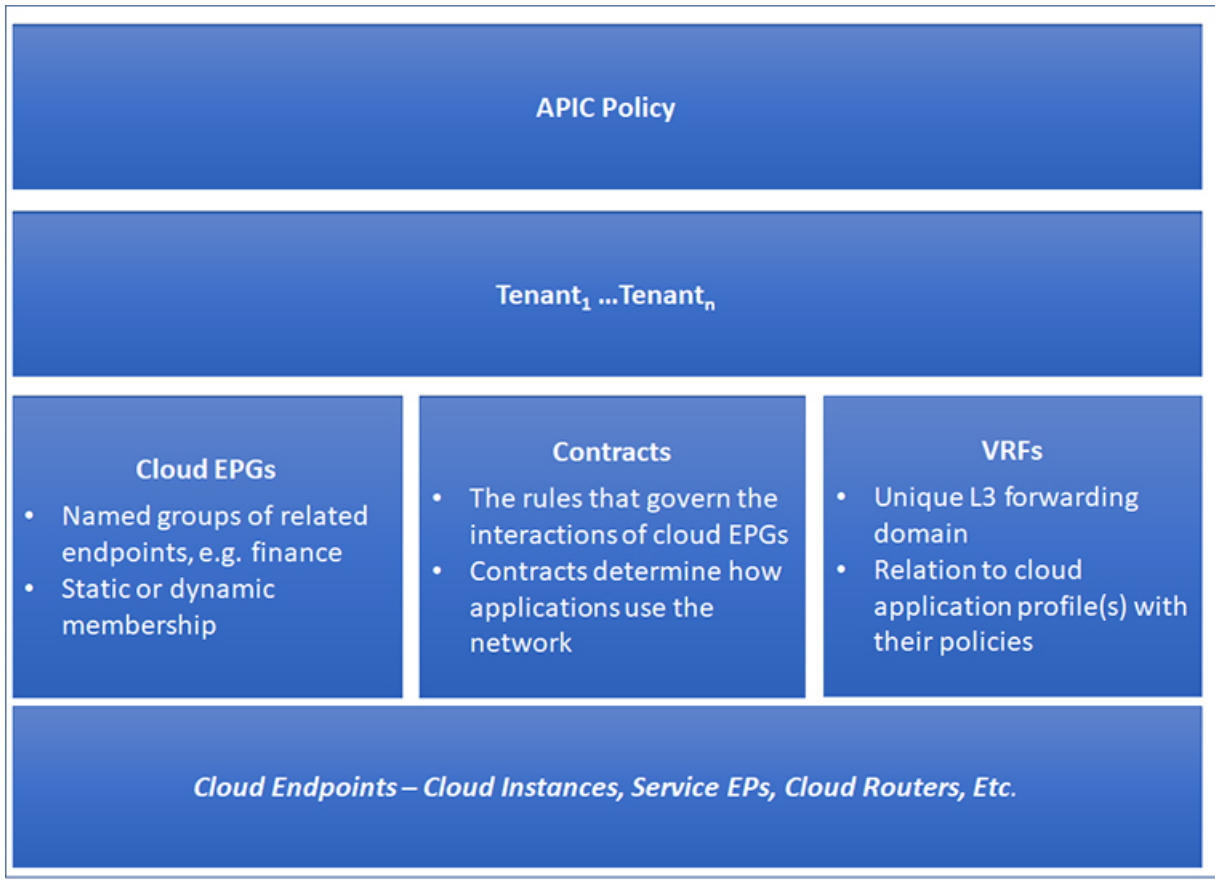
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシ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

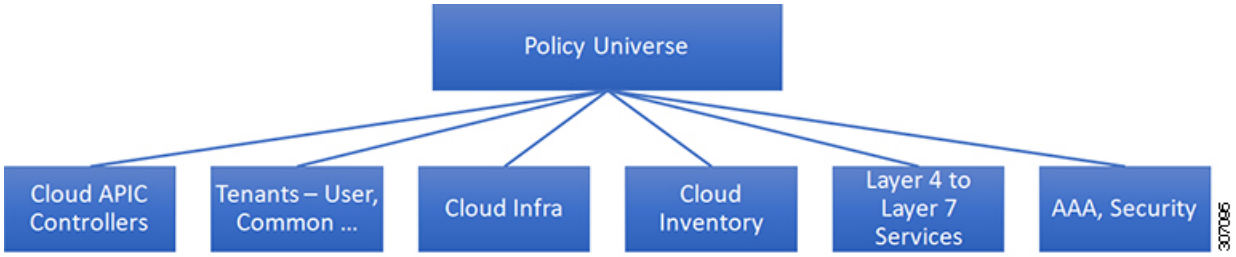
Cisco ACI ポリシー管理情報モデル

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 APIC 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 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、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 Application Policy Infrastructure Controller（APIC）リリース 4.1(1) の時点で、Cisco Cloud APIC 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ています。

  - 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 APIC 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 APIC Installation Guide*』を参照してください。

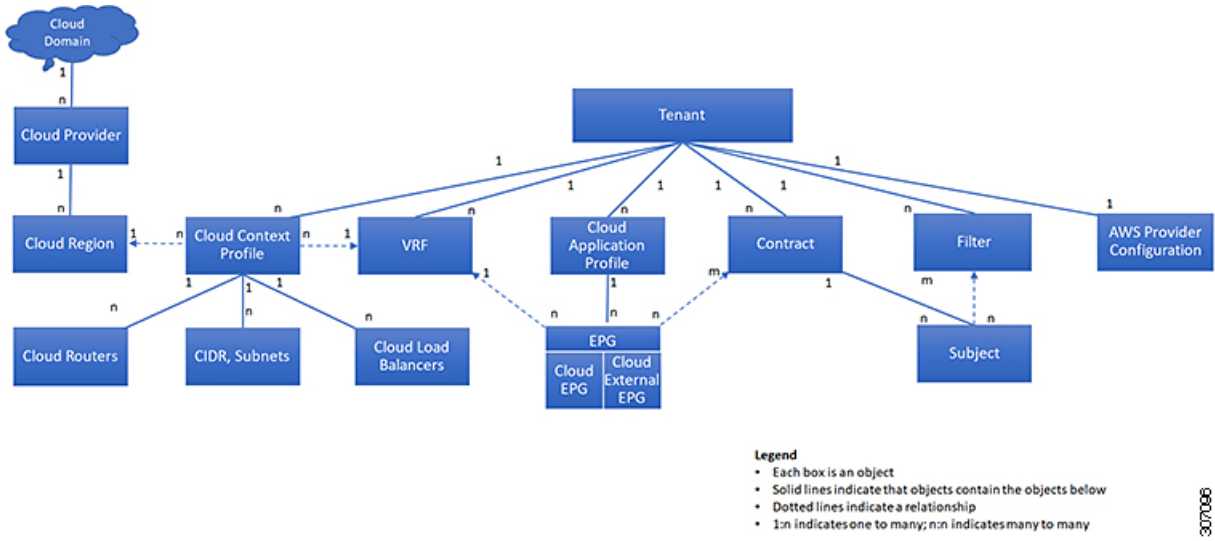
- クラウド インベントリは、GUI を使用してシステムのさまざまな側面を表示できるサービスです。たとえば、アプリケーションの側面から展開されたリージョンや、領域の側面から展開されたアプリケーションを表示できます。この情報は、クラウド リソースの計画とトラブルシューティングに使用できます。
- レイヤ 4 ～ レイヤ 7 のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムは動的に応答することができます。詳細については、レイヤ 4 から レイヤ 7 サービスの展開を参照してください。
- アクセス、認証、およびアカウンティング（AAA）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 APIC 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、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 プロファイル、AWS プロバイダー構成、およびエンドポイント グループ（EPG）を含むクラウド アプリケーション プロファイ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 プロファイルに関連付けることができます。VRF およびリージョンと組み合わせたクラウド コンテキスト プロファイルは、そのリージョンの AWS VPC を表します。

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 プロファイル

クラウドコンテキストプロファイルには、次の Cisco Cloud APIC コンポーネントに関する情報が含まれています。

- アベイラビリティ ゾーンおよびリージョン
- CIDR
- CCR
- エンドポイント
- EPG
- 仮想ネットワーク
- VRF

次のセクションでは、クラウド コンテキスト プロファイルの一部である一部のコンポーネントに関する追加情報を提供します。

CCR

CCR は、仮想およびクラウド環境で包括的な WAN ゲートウェイとネットワークサービスを提供します。CCR により、企業はWANをプロバイダーがホストするクラウドに拡張できます。Cisco Cloud APIC ソリューションには 2 つの CCR が必要です。

Cisco Cloud APIC で使用する CCR のタイプは、リリースによって異なります。

- リリース 25.2(3) よりも前のリリースでは、**Cisco Cloud Services Router 1000v** が Cisco Cloud APIC で使用されるCSRです。このタイプの CSR の詳細については、Cisco Cloud Services Router 1000v のドキュメントを参照してください。
- リリース 25.0(3) 以降、Cisco Cloud APIC では **Cisco Catalyst 8000V** が使用されます。この CCR のタイプに関する詳細は、『Cisco Catalyst 8000V Edge ソフトウェア マニュアル』を参照してください。

Cisco Catalyst 8000V について

リリース 25.0(3) 以降、Cisco Cloud APIC は、Cisco Cloud Services Router 1000v から Cisco Catalyst 8000V に移行します。以下は、Cisco Catalyst 8000V に固有の更新です。

- ライセンス （7 ページ）
- Throughput （8 ページ）

ライセンス

リリース 25.0(4) 以降、Cisco Cloud APIC 上の Cisco Catalyst 8000V は次のライセンス モデルをサポートしています。

1. **所有ライセンス持ち込み（BYOL）**ライセンス モデル
2. **ペイアズユーゴー（PAYG）**ライセンス モデル

（注） 25.0(4) より前のリリースの場合、Cisco Cloud APIC 上の Cisco Catalyst 8000V は、**所有ライセンス持ち込み（BYOL）**ライセンス モデルのみをサポートします。

BYOL ライセンス モデル

Cisco Catalyst 8000V の BYOL ライセンス モデルでは、Cisco から Catalyst 8000V Cisco DNA ライセンスを購入し、クラウドに展開する必要があります。

- ティアベースの Cisco Catalyst 8000V ライセンスの 1 つにサブスクライブする手順については、Cisco Catalyst 8000V Edge ソフトウェアを参照してください。
- 層に基づくさまざまなスループットの詳細については、Throughput （8 ページ） を参照してください。

Cisco Cloud APIC は「Cisco DNA Advantage」サブスクリプションを利用します。「Cisco DNA Advantage」サブスクリプションでサポートされる機能については、Cisco DNA ソフトウェア SD-WAN およびルーティング マトリックスを参照してください。

PAYGライセンス モデル

25.0(4) リリース以降、Cisco Cloud APIC は Cisco Catalyst 8000V でのペイアズユーゴー（PAYG）ライセンス モデルをサポートしています。これにより、ユーザは VM サイズに基づいてクラウドに Catalyst 8000V インスタンスを展開し、時間単位で使用料を購入できます。

スループットを得るために VM サイズに完全に依存しているため、PAYG ライセンス モデルを有効にするには、まず現在の Cisco Catalyst 8000V の展開を解除してから、新しい VM サイズでの初回セットアップを使用して再度展開します。詳細については、『*Cisco Cloud APIC for AWS 設置ガイド*』の「セットアップウィザードを使用した Cisco Cloud APIC の構成」の章を参照してください。

（注） 使用可能な 2 つのライセンス タイプを切り替える場合も、ライセンスを切り替える手順を使用できます。

（注） AWS マーケットプレイスでライセンスを使用するには、**Catalyst 8000V Cisco DNA Essentials** と **Catalyst 8000V Cisco DNA Advantage** の 2 つの PAYG オプションがあります。Cisco Cloud APIC は、**Catalyst 8000V Cisco DNA Advantage** を利用します。「Cisco DNA Advantage」サブスクリプションでサポートされる機能については、「Cisco DNA Software SD-WAN およびルーティング マトリックス」を参照してください。

Throughput

リリース 25.0(4) 以降、Cisco Cloud APIC 上の Cisco Catalyst 8000V は次のライセンス モデルをサポートしています。

1. **所有ライセンス持ち込み（BYOL）**ライセンス モデル
2. **ペイアズユーゴー（PAYG）**ライセンス モデル

（注） 25.0(4) より前のリリースの場合、Cisco Cloud APIC 上の Cisco Catalyst 8000V は、**所有ライセンス持ち込み（BYOL）**ライセンス モデルのみをサポートします。

1. 所有ライセンス持ち込み（BYOL）

このモデルでは、Cisco Catalyst 8000V は、ティアベース（T0/T1/T2/T3）のスループット オプションをサポートしています。次の表に、Cisco Catalyst 8000V 向けのさまざまなルータ スループット設定に使用される AWS EC2 インスタンスを示します。

CCR スループット	AWS EC2 インスタンス
T0（最大 15M のスループット）	c5.xlarge
T1（最大 100M のスループット）	c5.xlarge
T2（最大 1G のスループット）	c5.xlarge
T3（最大 10G のスループット）	c5.9xlarge

Tier2（T2）は、Cisco Cloud APIC でサポートされるデフォルトのスループットです。

次の表は、古い Cisco Cloud Services Router 1000v ルータから新しい Cisco Catalyst 8000V ルータへのスループットのマッピングを示しています。

Cisco クラウド サービス ルータ 1000v	Cisco Catalyst 8000V のスループット
10 M	T0 (最大 15M のスループット)
5,000 万人	T1（最大 100M のスループット）
1 億	T1 (最大 100M のスループット)
2 億 5000 万	T2 (最大 1G のスループット)
5 億	T2（最大 1G のスループット）
1G	T2 (最大 1G のスループット)
2.5G	T3 (最大 10G のスループット)
5G	T3 (最大 10G のスループット)
7.5G	T3（最大 10G のスループット）
10 G	T3 (最大 10G のスループット)

2. ペイアズユーゴー（PAYG）ライセンス モデル

このモデル向けに、Cisco Cloud APIC は Cisco Catalyst 8000V 仮想ルータを使用し、クラウド ネットワーキングのニーズに合わせて AWS EC2 インスタンスの範囲をサポートします。

以下の表は、AWS 上の Cisco Cloud APIC でサポートされているクラウド インスタンス タイプを示しています。

AWS EC2 インスタンス	CCR スループット	vCPU の数	メモリ
c5.xlarge	最大 5 ギガビット スループット	4	8 GiB
c5.2xlarge	最大 10 ギガビット スループット	8	16 GiB
c5.4xlarge	最大 10 ギガビット スループット	16	32 GiB
c5.9xlarge	最大 10 ギガビット スループット	36	72 GiB
c5n.xlarge	最大 25 ギガビット スループット	4	10.5 GiB
c5n.2xlarge	最大 25 ギガビット スループット	8	21 GiB

AWS EC2 インスタンス	CCR スループット	vCPU の数	メモリ
c5n.4xlarge	最大 25 ギガビット スループット	16	42 GiB
c5n.9xlarge	最大 50 ギガビット スループット	36	96 GiB

Cisco Cloud APIC および AWS の CCR 向けプライベート IP アドレス サポート

（注） Azure の場合、Cisco Cloud APIC および CCR のプライベート IP アドレスのサポートは、リリース 5.1(2) で利用可能になりました。AWS の場合、このサポートはリリース 5.2(1) 以降で利用できます。

AWS の場合、リリース 5.2(1) より前のリリースでは、Cisco Cloud Router（CCR）インターフェイスには Cisco Cloud APIC により、パブリックとプライベートの両方の IP アドレスが割り当てられていました。リリース 5.2(1) 以降、CCR インターフェイスはプライベート IP アドレスのみが割り当てられ、パブリック IP アドレスを CCR インターフェイスに割り当てることはオプションとなりました。プライベート IP アドレスは、常に CCR のすべてのインターフェイスに割り当てられます。CCR の GigabitEthernet1 のプライベート IP アドレスは、BGP および OSPF ルーター ID として使用されます。

CCR インターフェイスのパブリック IP アドレスを無効にするサイト間接続の CCR プライベート IP アドレスを有効にするには、Cisco Cloud APIC GUI を使用したリージョンの管理（クラウド テンプレートの設定） の手順を参照してください。

AWS の場合、リリース5.2（1）よりも前は、Cisco Cloud APIC の管理インターフェイスにパブリック IP アドレスとプライベート IP アドレスが割り当てられていました。リリース5.2（1）以降、プライベートIPアドレスはの管理インターフェイスに割り当てられ、パブリックIPアドレスの割り当てはオプションです。Cisco Cloud APICCisco Cloud APIC へのパブリック IP を無効にして、プライベート IP アドレスが接続に使用されるようにするには、*Cisco Cloud APIC for AWS Installation Guide*、Release 5.2(1) 以降の「*AWS での Cisco Cloud APIC*」手順を参照してください。

プライベート IP アドレスを使用した CCR の制限

パブリック IP が無効になっている場合、パブリック インターネットにはパブリック IP アドレスが必要なため、アンダーレイのサイト間接続をパブリック インターネットにすることはできません。アンダーレイのサイト間接続は、次のいずれかになります。

- AWS Direct Connect または Azure Express Route を介した、オンプレミスの ACI サイトに接続するためのプライベート接続
- AWS VPC ピアリングまたは Azure Vnet ピアリングを介して、同じクラウド プロバイダーのCisco Cloud APIC サイトに接続するためのクラウド バックボーン

CCR なしのリージョンからの外部サイトへのコミュニケーション

リリース 5.2(1) より前では、トラフィックが外部サイトに通過するには、トラフィックが通過するリージョンに CCR が展開されている必要があります。CCR は、そのリージョンにローカルな CIDR をアドバタイズします。リージョン内の EPG が外部サイトと契約している場合、そのリージョンには、その外部サイトと通信するために CCR が展開されている必要があります。

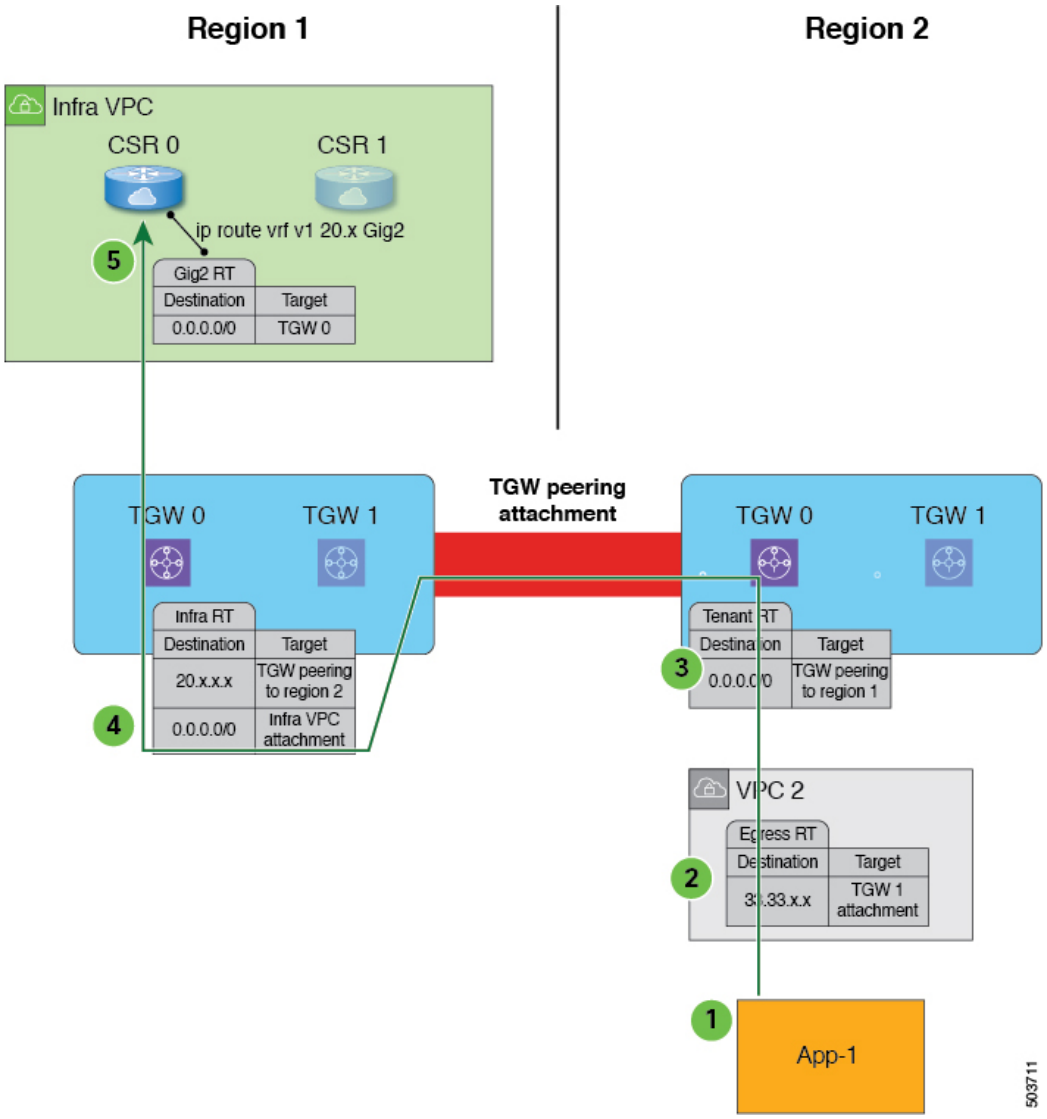
リリース 5.2(1) 以降、CCR のないリージョンから外部サイトと通信できるようになりました。これは、Cisco Cloud APIC リリース 5.0(1) で利用可能になった AWS Transit Gateway 機能を利用することによって実現されます。Cisco Cloud APIC で AWS Transit Gateway 機能を有効にすると、AWS のすべてのマネージド リージョン間のピアリングも有効になります。このようにして、Cisco Cloud APIC は AWS Transit Gateway のピアリング機能により、CCR なしでリージョンから外部サイトと通信する問題に対処できます。この問題は、トラフィックを CCR のあるリージョンに再ルーティングすることで解決します。

AWS Transit Gateway 機能を使用して、CCR のないリージョンからのトラフィックがサイトから出ようとすると、このトラフィックは CCR のある最も近いリージョンのインフラ VPC にルーティングされます。トラフィックがそのリージョンのインフラ VPC に再ルーティングされた後、その CCR はパケットの送信に使用されます。入力トラフィックの場合、外部サイトからのパケットは任意のリージョンの CCR に到達し、入力データ パスの AWS Transit Gateway ピアリングを使用して接続先リージョンにルーティングできます。

このような状況では、外部トラフィックが CCR のない領域を出入りしていることをシステムが認識すると、トラフィックは自動的に再ルーティングされます。ただし、システムがこの再ルーティング タスクを自動的に実行するには、次のコンポーネントを構成する必要があります。

- AWS Transit Gateway を設定する必要があります。詳細については、ドキュメント「AWS Transit Gateway を使用した VPC 間の帯域幅の増加」を参照してください。
- CCR は、少なくとも 1 つのリージョンに展開する必要があります。この拡張機能により、CCR を含まないリージョンから外部サイトと通信できるようになりますが、トラフィックが CCR のないリージョンから CCR のあるリージョンに再ルートできる CCR を含む別のリージョンが必要です。

次の図は、CCR のないリージョンから外部トラフィックが送信されていることをシステムが認識したときに、トラフィックが自動的に再ルーティングされるシナリオの例を示しています。



Cisco Cloud APIC がリージョン 2 に CCR がないことを認識しているが、トラフィックが外部サイトに出力されている場合、次のことが発生します（緑色の矢印と円で示されています）。

1. トラフィック フローは、リージョン 2 の App-1 の CIDR からリモート サイトへの出力を開始します。エンドポイントは、リモート サイトの CIDR を許可する適切なアウトバウンド ルールで構成されていることに注意してください。
2. VPC 2 出力ルート テーブルにはリモート サイト CIDR があり、次ホップとして AWS Transit Gateway があります。AWS Transit Gateway 情報は、設定されたコントラクトに基づいて自動的にプログラムされます。
3. 0.0.0.0/0 ルートが AWS Transit Gateway ルート テーブルに挿入されます。これは、基本的に、トラフィックが外部サイトに送信されているが、このリージョンに CCR がない場合に、AWS Transit Gateway ピアリング アタッチメントを取得するようにシステムに指示します。この状況では、AWS Transit Gateway ピアリングのアタッチメントは、CCR がある

別のリージョン（例のシナリオではリージョン1）に移動します。使用されるCCRのあるリージョンは、CCR がないリージョンへの地理的な近さに基づいて選択されます。

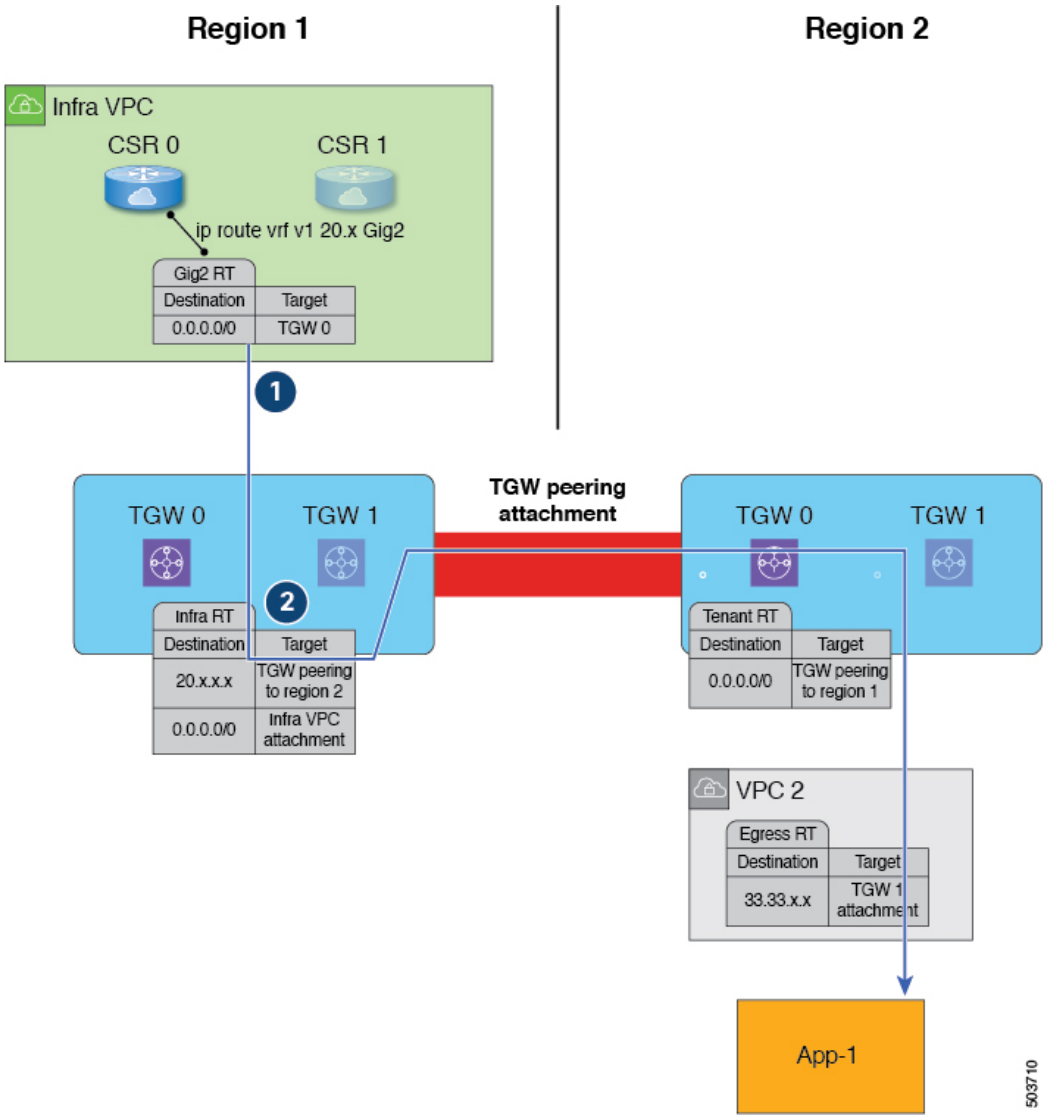
4. パケットは、最初にCCRを持つリージョン（リージョン1）のインフラVPCに転送され、次に適切なVRFグループに関連付けられているCCR上のギガビットイーサネットネットワーク インターフェイスに転送されます。

5. リージョン1のCCRのギガビット2インバウンドセキュリティ グループは、リモートリージョンVPCからのトラフィックを許可するように構成されています。

上記の出力の例では、次の点に注意してください。

- 手順1と2については、プレリリース5.2(1)の動作から変更はありません。
- ステップ3は、リリース5.2(1)のこの機能に固有の新しい動作であり、CCRのないリージョンからCCRのあるリージョンへのTGWピアリング接続にリダイレクトが発生します。さらに、ステップ3はAWSクラウドで発生します。
- ステップ4と5は、通常、リリース5.2(1)より前のリージョン2で発生しますが、リージョン2にCCRがある場合のみです。ただし、リージョン2にはCCRがないため、リリース5.2(1)のこの機能により、これらの手順はCCRが存在するリージョン1で実行されます。

次の図は、CCRのない領域に外部トラフィックが入っていることをシステムが認識したときに、トラフィックが自動的に再ルーティングされるシナリオの例を示しています。



Cisco Cloud APIC が、リージョン 2 に CCR がないことを認識しているが、トラフィックが外部サイトからリージョン 2 の App-1 の CIDR に進入している場合、以下が発生します（青い矢印と円で示されています）。

1. 通常、リージョン 1 の CCR は、そのリージョンにローカルな CIDR のみをアドバタイズします。ただし、リリース 5.2(1) の一部であるこの機能強化により、すべてのリージョンのすべての CCR がすべてのリモート リージョンからの CIDR をアドバタイズするようになりました。したがって、この例では、リージョン 1 の CCR は、リージョン 2 にある CIDR もアドバタイズします（AWS Transit Gateway ピアリングが両方のリージョン間で構成され、コントラクトが正しく構成されていると仮定します）。この状況では、トラフィックは外部サイトからリージョン 1 の CCR に進入し、リージョン 1 の CCR はリモート リージョン VPC CIDR の静的ルートをアドバタイズします。

2. インフラ ルート テーブル (リージョン 1 の AWS Transit Gateway ルート テーブル) には、リージョン 2 への AWS Transit Gateway ピアリング アタッチメントへのネクスト ホップがあります。

上記の入力の例では、次の点に注意してください。

- 上記の入力例の両方のステップ (ステップ 1 と 2) は、リリース 5.2(1) のこの機能に固有の新機能です。
- 入力例のステップ 1 は、CCR でプログラムされた構成を示しています。
- 入力例のステップ 2 は、AWS クラウドで発生します。

CCR のリモートサイトからの ECMP 転送のサポート

クラウド内の CCR は、通常、プレフィックスに対して複数のパスを受け取ります。リリース 5.2(1) より前は、CCR が複数のパスを受信する場合でも、均等コスト マルチパス（ECMP）を使用した CCR からのデータ転送はサポートされていませんでした。

リリース 5.2(1) 以降、CCR を使用した ECMP がサポートされるようになりました。CCR からのトラフィックは、接続先サイトから受信したすべての ECMP パスに転送されます。このサポートはリリース 5.2(1) で自動的に有効になり、このサポートを有効にするために手動で設定する必要はありません。

ローカル CIDR によるリージョンの CCR へのルートの基本設定

構成されているすべての CIDR は、特定のリージョンに対してローカルです。クラウド内に複数のリージョンがある場合、すべてのリージョンの CCR は冗長性のために CIDR をアドバタイズします。リリース 5.2(1) より前は、すべてのリージョンの CCR が同じ設定で CIDR がアドバタイズされました。これにより、リモートクラウドサイトまたはオンプレミスサイトが、CIDR がローカルではないリージョンを介して CIDR へのパスをインストールする可能性があります。これにより、パケットが必要以上に長い経路をたどる可能性があります。

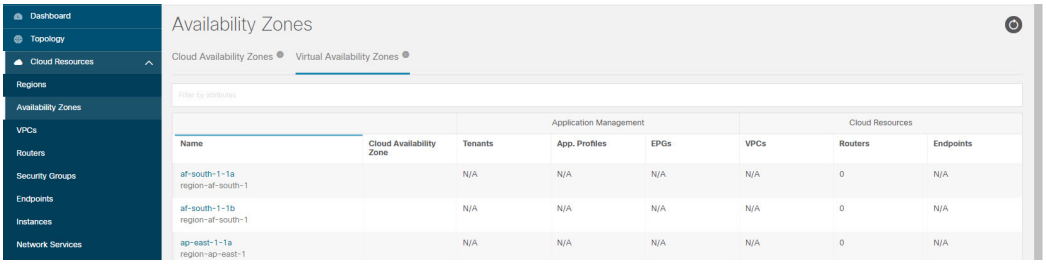
リリース 5.2(1) 以降、複数のリージョンからの CCR は引き続き CIDR をアドバタイズしますが、CIDR がローカルであるリージョンからの CCR は、より高い優先度でアドバタイズします。これにより、オンプレミス サイトまたはリモート クラウド サイトは、CIDR がローカルであるリージョンにトラフィックを直接送信します。ローカル リージョンの CCR に障害が発生した場合、他のリージョンからのパスをデータ転送に使用できます。

可用性ゾーン

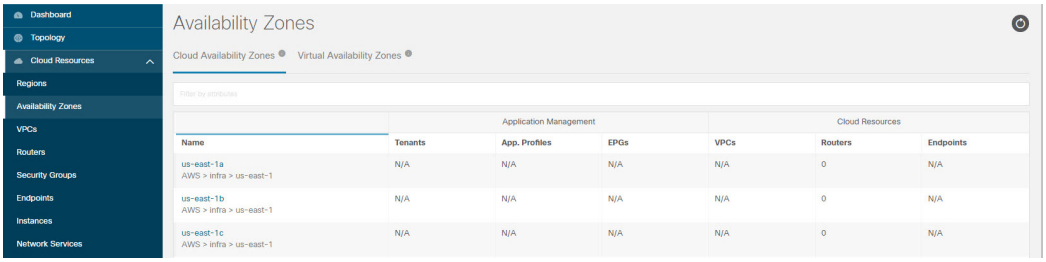
リリース 25.0(2) より前は、Cisco Cloud APIC は AWS のリージョンごとに 2 つのアベイラビリティ ゾーンのみをサポートします。その際に、Cisco Cloud APIC が <region-name>a と <region-name>b の形式を使用して、各リージョンに対して**仮想**アベイラビリティ ゾーンと呼ばれる 2 つのアベイラビリティ ゾーンを作成します。たとえば、`us-west-1` リージョンの下に、Cisco Cloud APIC は 2 つの仮想アベイラビリティ ゾーン `us-west-1a` と `us-west-1b` を作成します。

リリース 25.0(2) 以降、**クラウド** アベイラビリティ ゾーンがサポートされるようになり、各 AWS リージョンで Cisco Cloud APIC を使用して、複数のアベイラビリティ ゾーンが可能になりました。

- Cisco Cloud APIC の**仮想**アベイラビリティ ゾーンを表示するには、**[クラウド リソース]** > **[アベイラビリティ ゾーン]** に移動し、**[仮想アベイラビリティ ゾーン]** タブをクリックします。



- Cisco Cloud APIC の**クラウド** アベイラビリティ ゾーンを表示するには、**[クラウド リソース]** > **[アベイラビリティ ゾーン]** に移動し、**[クラウド アベイラビリティ ゾーン]** タブをクリックします。



仮想アベイラビリティ ゾーンからクラウド アベイラビリティ ゾーンへの移行

リリース 25.0(2) より前に構成したデプロイで、仮想アベイラビリティ ゾーンが構成されている場合、リリース 25.0(2) にアップグレードするときに、リリース 25.0(2) にアップグレードした後で、古い仮想アベイラビリティ ゾーンから新しいクラウド アベイラビリティ ゾーンに移行することをお勧めします。

- アベイラビリティーゾーンの移行の一部として、CIDR ブロック範囲内の個々のサブネットまたはすべてのサブネットを移行できます。
- 古い仮想アベイラビリティ ゾーンから新しいクラウド アベイラビリティ ゾーンに移行しても、AWS のクラウド リソースでトラフィックのドロップなどの機能への影響はありません。

（注） 次の手順では、クラウド コンテキスト プロファイルを使用して仮想アベイラビリティ ゾーンからクラウド アベイラビリティ ゾーンに移行する方法について説明しますが、インテント アイコン ( ) をクリックし、**[アベイラビリティ ゾーン構成の移行]** を選択して、アベイラビリティ ゾーンを移行することもできます。

仮想アベイラビリティーゾーンからクラウドアベイラビリティーゾーンに移行するには:

1. 以前の仮想アベイラビリティ ゾーンで以前に構成されたクラウド コンテキスト プロファイルに移動します。

   左側のナビゲーション ペインで、**[アプリケーション管理]** > **[クラウド コンテキスト プロファイル]** に移動し、以前の仮想アベイラビリティ ゾーンで以前に構成されたクラウド コンテキスト プロファイルを見つけます。

2. そのクラウド コンテキスト プロファイルをダブルクリックします。

   そのクラウドコンテキストプロファイルの詳細パネルが表示され、**[概要]** タブが自動的に選択されます。

   [概要] タブの **[アベイラビリティ ゾーン]** 列のエントリを表示して、このクラウド コンテキスト プロファイルに、クラウド アベイラビリティ ゾーンに移行できる仮想アベイラビリティ ゾーンがあるかどうかを判断します。

3. **[アクション]** > **[サブネット構成の移行]** の順にクリックします。

   [アベイラビリティ ゾーン構成の移行（Availability Zone Configuration Migration）] ウィンドウが表示されます。

4. クラウド アベイラビリティ ゾーンに移行する仮想アベイラビリティ ゾーンに関連付けられているサブネットを選択します。

   - このウィンドウに一覧表示され、仮想アベイラビリティゾーンに関連付けられているすべてのサブネットがデフォルトで選択されます。クラウド アベイラビリティ ゾーンに移行したくない仮想アベイラビリティゾーンに関連付けられているサブネットを手動で選択解除します。
   - クラウド アベイラビリティ ゾーンに移行される各仮想アベイラビリティ ゾーンについて、必要に応じて、[クラウド アベイラビリティ ゾーン] 列のエントリを書き留めて、そのサブネットの新しいアベイラビリティ ゾーン値を決定します。

5. **[サブネット構成の移行]** をクリックします。

   選択した仮想アベイラビリティ ゾーンがクラウド アベイラビリティ ゾーンに移行されます。

注意事項と制約事項

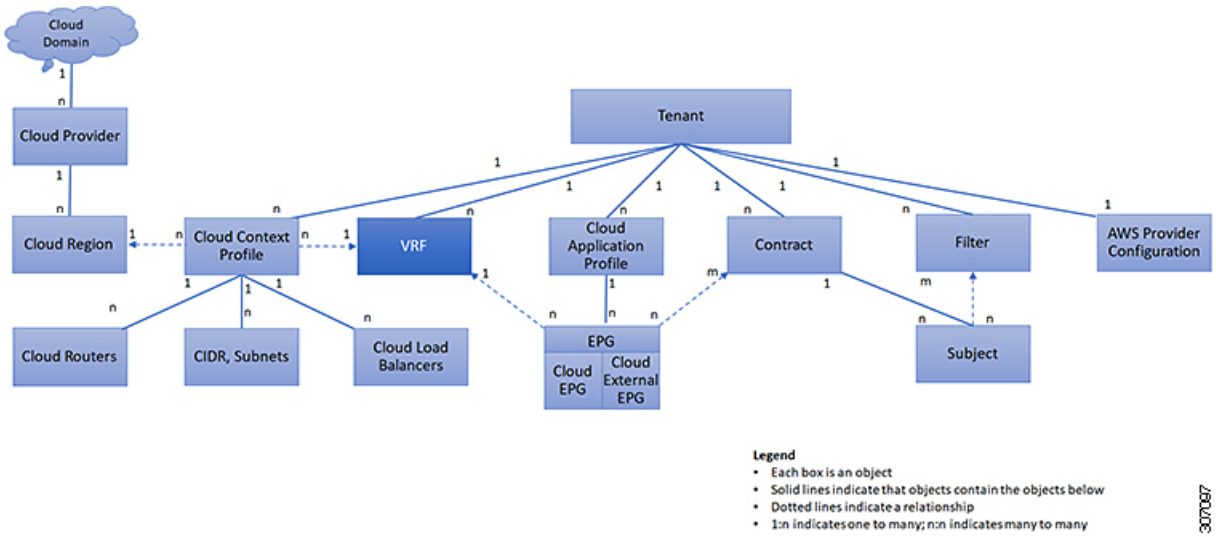
次に、複数のアベイラビリティ ゾーンのサポートに関するガイドラインと制限事項を示します。

- 3 つ以上のアベイラビリティ ゾーンを持つことができるクラウド アベイラビリティ ゾーンのサポートは、ユーザー テナントでのみ利用できます。インフラ テナントは、2 つのアベイラビリティ ゾーンの制限がある仮想アベイラビリティ ゾーンを引き続き使用します。

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（Cisco Cloud 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*

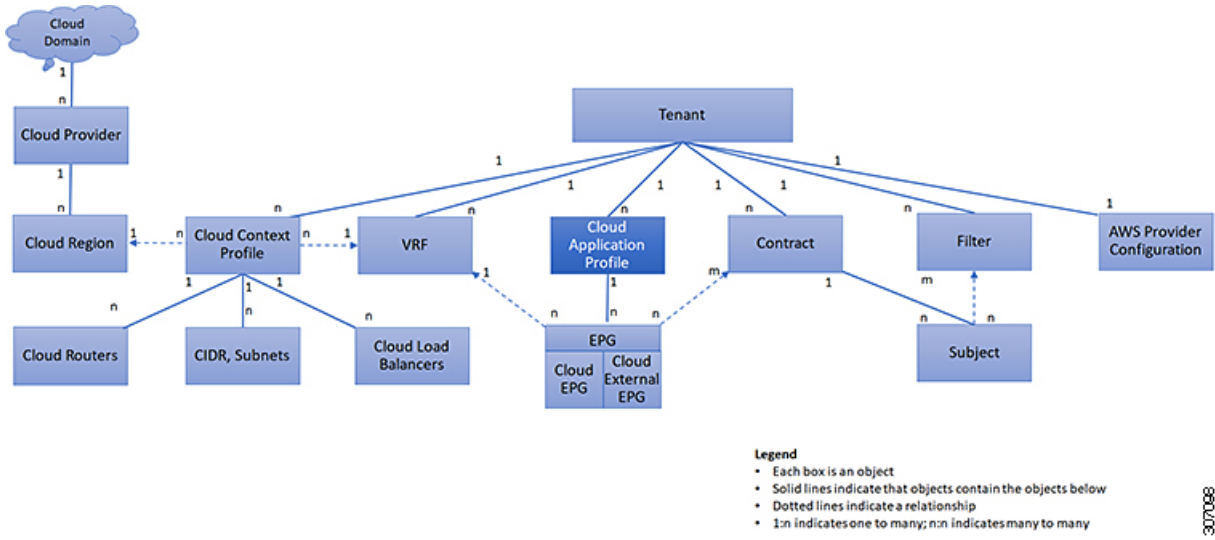


VRF は、レイヤ 3 のアドレス ドメインを定義します。1 つ以上のクラウド コンテキスト プロファイルが VRF に関連付けられます。特定のリージョンの VRF に関連付けることができるクラウド コンテキスト プロファイルは 1 つだけです。レイヤ 3 ドメイン内のすべてのエンドポイントが一意の IP アドレスを持っている必要があります。なぜなら、ポリシーで許可されている場合にこれらのデバイス間でパケットを直接転送できるためです。テナントには、複数の VRF を含めることができます。管理者が論理デバイスを作成した後、管理者はデバイス クラスタの選択基準ポリシーを提供する論理デバイスの VRF 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。

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。

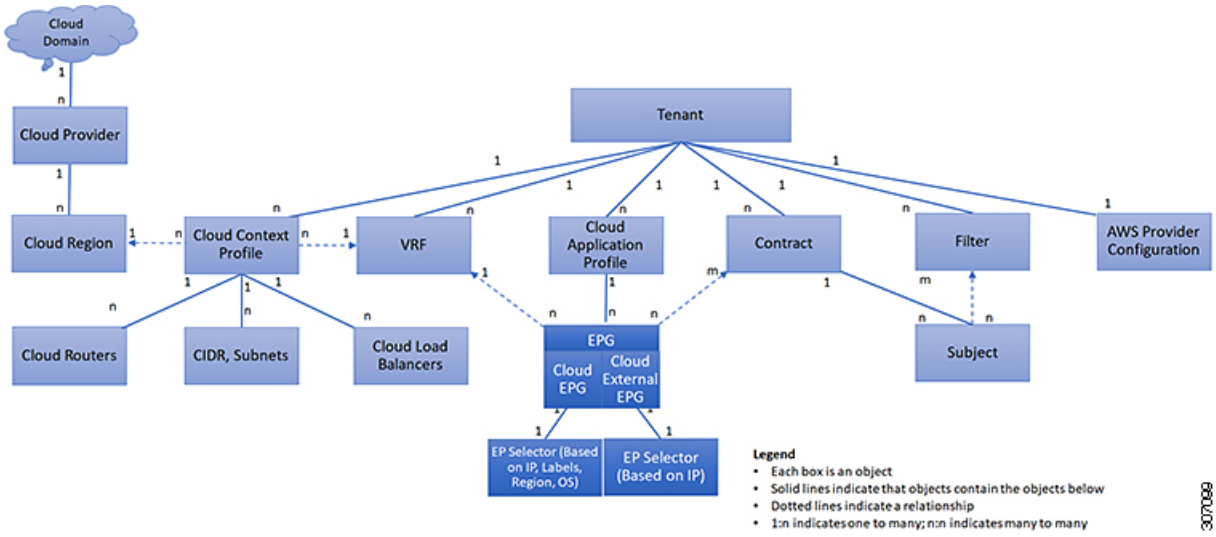
クラウド EPG は次のいずれかに従って組織化できます。

- 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。

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 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。

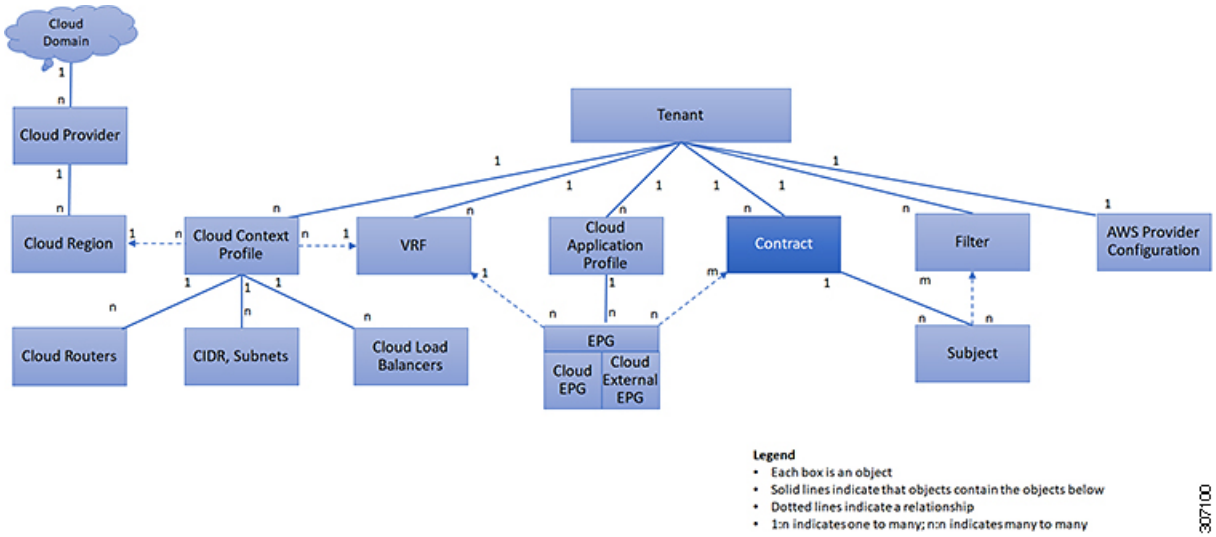
クラウド インフラストラクチャへの WAN ルータ接続は、スタティック クラウド EPG を使用する設定の 1 つの例です。クラウド インフラストラクチャへの WAN ルータ接続を設定するには、関連付けられている WAN サブネット内のエンドポイントを含む `cloudExtEPg` クラウド EPG を管理者が設定します。クラウド インフラストラクチャは、エンドポイントの接続ライフサイクルが経過する間に、検出プロセスを通してクラウド EPG のエンドポイントについて学習します。エンドポイントを学習すると、クラウドインフラストラクチャは、それに基づいて `cloudExtEPg` クラウド EPG 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、`cloudExtEPg` 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 APIC 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 AWS 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`）

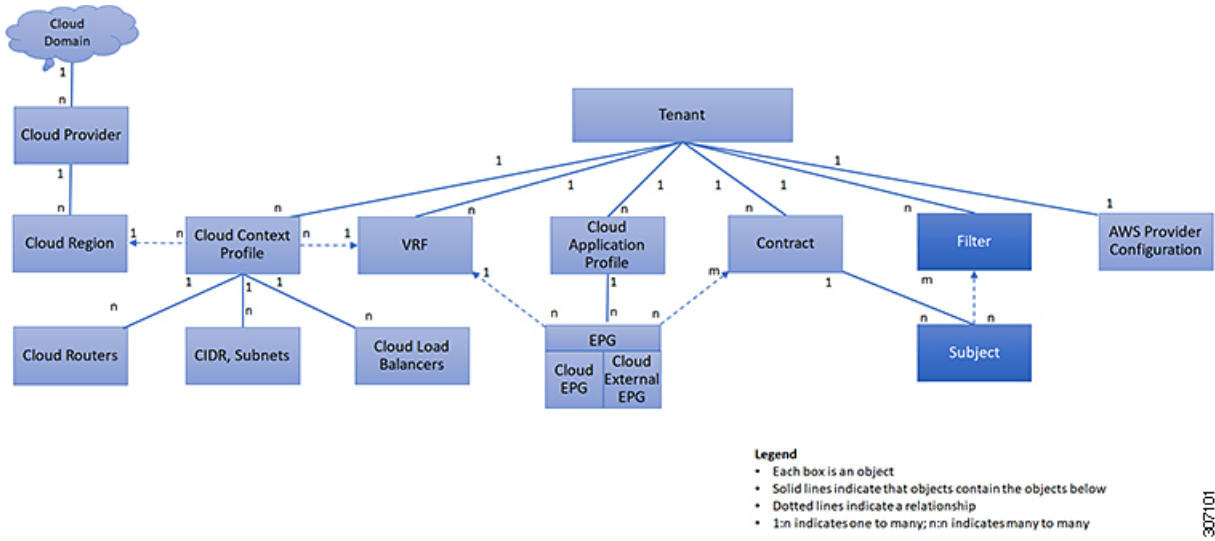
コントラクトは、プロバイダー、コンシューマ、またはその両方とラベル付されたクラウド EPG 間の通信を制御します。クラウド EPG とコントラクトの関係は、プロバイダーまたはコンシューマです。クラウド EPG がコントラクトを提供すると、通信が提供されたコントラクトに準拠している限り、そのクラウド EPG との通信は他のクラウド EPG から開始できます。クラウド EPG がコントラクトを使用すると、そのクラウド EPG のクラウド エンドポイントは、コントラクトを指定したクラウドEPGのクラウドエンドポイントと通信を開始できます。

（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 APIC で非表示になり、設定できません。AWS 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 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、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。

（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 のクラウド 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。

（注） AWS 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。

- AWS 構造体でレンダリングされる ACI 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 APIC 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 APIC 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。

AWS ネットワーク構成の中心的なものの 1 つは、仮想プライベート クラウド (VPC) です。AWS 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 VPC 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。AWS VPC に対応する Cisco Cloud APIC 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。クラウドテンプレートによって生成された `cloudCtxProfile MO` には、`ctxProfileOwner == SYSTEM` が含まれます。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。

AWS VPC の主要なプロパティは CIDR です。すべてのリージョンには、一意の CIDR が必要です。Cisco Cloud APIC では、インフラ VPC の CIDR を提供できます。最初の 2 つのリージョンの CIDR は、AWS に Cisco Cloud APIC AMI をデプロイする Cloud Formation Template (CFT) から取得されます。cloudApicSubnetPool MO は、追加リージョンの CIDR を Cisco Cloud APIC に直接提供します。Cisco Cloud APIC 構成では、cloudCtxProfile の子である cloudCidr MO が CIDR をモデル化します。

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
- サブネットと AWS アベイラビリティーゾーンの関連付け
- 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。
cloudtemplateProfile	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。 • routerUsername • routerPassword • routerThroughput • routerLicenseToken • routeDataInterfacePublicIP • routerMgmtInterfacePublicIP

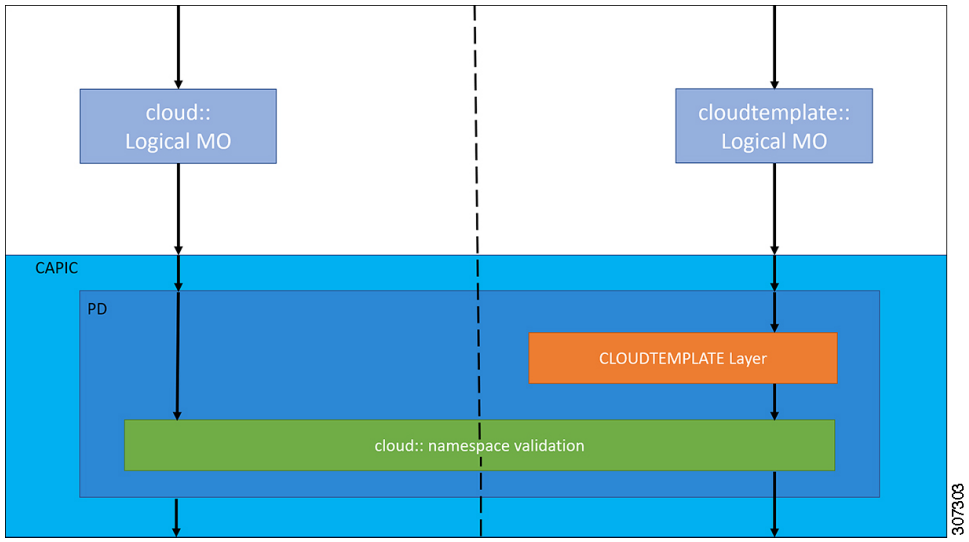
MO	目的
cloudtemplateIntNetwork	クラウドルータを展開する場所を指定するリージョンのリストが含まれます。各リージョンは、cloudRegionName子 MO を介してキャプチャされます。
cloudtemplateExtNetwork	クラウド外部のインフラ ネットワーク設定入力が含まれます。 クラウド ルータが外部ネットワーキング用に設定されているリージョンのリストが含まれます。 各リージョンは、cloudRegionName子 MO を介してキャプチャされます。
cloudtemplateVpnNetwork	ACI オンプレミス サイトまたは別の Cisco Cloud APIC サイトで VPN を設定するための情報が含まれています。
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。
cloudtemplateOspf	VPN接続に使用するOSPFエリアをキャプチャします。
cloudtemplateBgpEvpn	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。

Cisco Cloud APIC 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 APIC 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 APIC コンポーネントの設定 を参照してください。

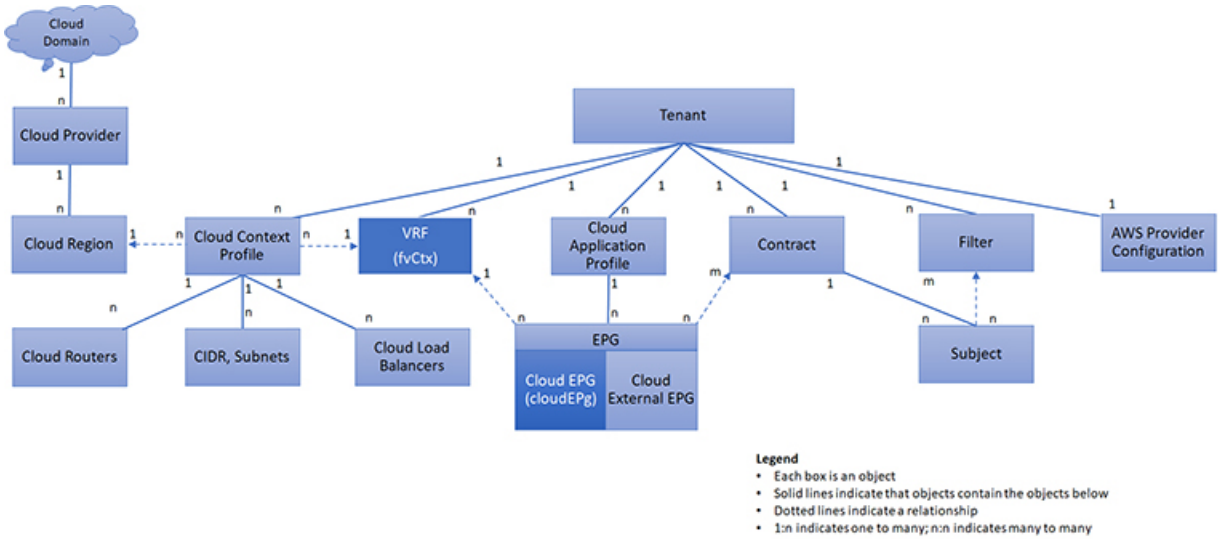
管理対象オブジェクトの関係とポリシー解決

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。

- `cloudRsZoneAttach` および `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 AWS プロバイダー（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 APIC 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 APIC 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、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。

共有サービス

あるテナントのクラウド 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クラウド EPG を伝達できます。同じテナント内で、ある VRF のクラウド EPG は、テナントで定義された契約を通じて、別の VRF の別のクラウド EPG と通信できま

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クラウド 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、クラウド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。

- 共有サービスは、重複しない CIDR サブネットのみでサポートされます。共有サービスの CIDR 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。
  - ある VRF から漏れた CIDR 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る CIDR 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。

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。