



# Cisco Cloud Network Controller ポリシー モデル

---

- [CNC ポリシーモデルについて \(1 ページ\)](#)
- [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 CNC 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 \(15 ページ\)](#)
- [クラウド アプリケーション プロファイル \(16 ページ\)](#)
- [クラウド エンドポイント グループ \(17 ページ\)](#)
- [コントラクト \(19 ページ\)](#)
- [クラウド テンプレートの概要 \(22 ページ\)](#)
- [管理対象オブジェクトの関係とポリシー解決 \(25 ページ\)](#)
- [デフォルト ポリシー \(26 ページ\)](#)
- [共有サービス \(27 ページ\)](#)

## 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。

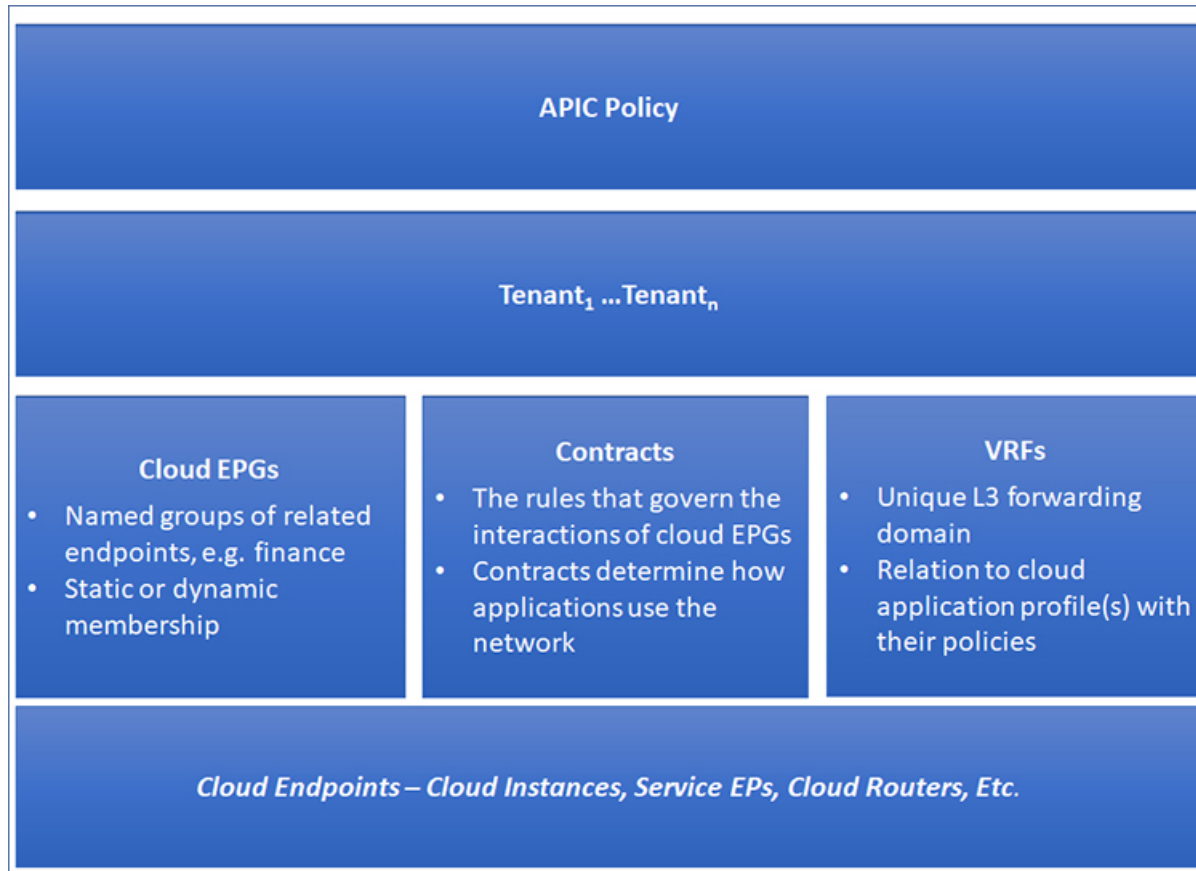
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシ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

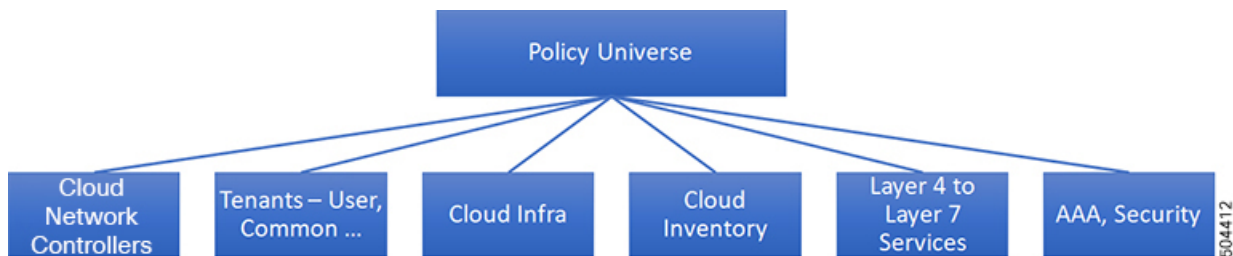
## Cisco CNC ポリシー管理情報モデル

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 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、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。

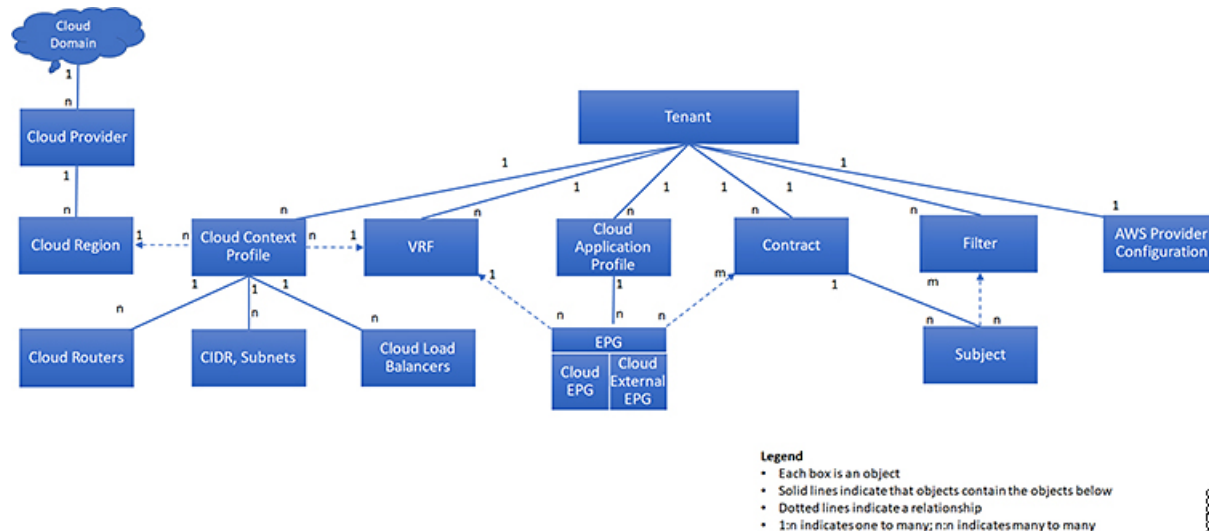
- クラウド インベントリは、GUI を使用してシステムのさまざまな側面を表示できるサービスです。たとえば、アプリケーションの側面から展開されたリージョンや、領域の側面から展開されたアプリケーションを表示できます。この情報は、クラウドリソースの計画とトラブルシューティングに使用できます。
- レイヤ4～レイヤ7のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムは動的に応答することができます。詳細については、[レイヤ4からレイヤ7サービスの展開](#)を参照してください。
- アクセス、認証、およびアカウントिंग（AAA）ポリシ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

- 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

The CCR is a virtual router that delivers comprehensive WAN gateway and network services into virtual and cloud environments. The CCR enables enterprises to extend their WANs into provider-hosted clouds. Two CCRs are required for Cisco Cloud Network Controller solution.

The **Cisco Catalyst 8000V** is used with the Cisco Cloud Network Controller. For more information on this type of CCR, see the [Cisco Catalyst 8000V Edge software documentation](#).

### About the Cisco Catalyst 8000V

Following are the updates for the Cisco Catalyst 8000V.

- [Licensing, on page 7](#)
- [Throughput, on page 7](#)

## Licensing

The Cisco Catalyst 8000V on Cisco Cloud Network Controller supports the following licensing models:

1. **Bring Your Own License (BYOL)** Licensing Model
2. **Pay As You Go (PAYG)** Licensing Model

### BYOL Licensing Model

The BYOL licensing model on Cisco Catalyst 8000V which requires you to purchase your Catalyst 8000V Cisco DNA license from Cisco and deploy it in the cloud.

- For instructions on subscribing to one of the tier-based Cisco Catalyst 8000V licenses, see [Cisco Catalyst 8000V Edge Software](#).
- For more information on different throughputs based on the tiers, see [Throughput, on page 7](#).

Cisco Cloud Network Controller makes use of the “Cisco DNA Advantage” subscription. For features supported by the “Cisco DNA Advantage” subscription, see [Cisco DNA Software SD-WAN and Routing Matrices](#).

### PAYG Licensing Model

Beginning with the 25.0(4) release, Cisco Cloud Network Controller supports Pay-As-You-Go (PAYG) Licensing Model on Cisco Catalyst 8000V which allows users to deploy a Catalyst 8000V instance in the cloud based on the VM size and purchase the usage on an hourly basis.

As you completely depend on the VM size to get the throughput, the PAYG licensing model can be enabled only by first un-deploying the current Cisco Catalyst 8000V and then re-deploying it using the First Time Set Up with the new VM size. For more information, see the chapter "Configuring Cisco Cloud Network Controller Using the Setup Wizard" in the [Cisco Cloud Network Controller for AWS Installation Guide](#)



---

**Note** The procedure for switching between licenses can also be used if you would like to switch between the two licensing types available.

---



---

**Note** There are two PAYG options for consuming licenses in the AWS marketplace: **Catalyst 8000V Cisco DNA Essentials** and **Catalyst 8000V Cisco DNA Advantage**. Cisco Cloud Network Controller will make use of **Catalyst 8000V Cisco DNA Advantage**. For features supported by the “Cisco DNA Advantage” subscription, see [Cisco DNA Software SD-WAN and Routing Matrices](#)

---

## Throughput

The Cisco Catalyst 8000V on Cisco Cloud Network Controller supports the following licensing models:

1. **Bring Your Own License (BYOL)** Licensing Model
2. **Pay As You Go (PAYG)** Licensing Model

### 1. Bring Your Own License (BYOL)

For this model, the Cisco Catalyst 8000V supports tier-based (T0/T1/T2/T3) throughput options. The following table lists what AWS EC2 instance is used for different router throughput settings for the Cisco Catalyst 8000V:

CCR Throughput	AWS EC2 Instance
T0 (up to 15M throughput)	c5.xlarge
T1 (up to 100M throughput)	c5.xlarge
T2 (up to 1G throughput)	c5.xlarge
T3 (up to 10G throughput)	c5.9xlarge

Tier2 (T2) is the default throughput supported by Cisco Cloud Network Controller.

## 2. Pay-As-You-Go Licensing Model

For this model, Cisco Cloud Network Controller supports a range of AWS EC2 instances for cloud networking needs powered by Cisco's Catalyst 8000V virtual router.

The table below shows the cloud instance type supported by Cisco Cloud Network Controller on AWS.-

AWS EC2 Instance	CCR Throughput	vCPUs	Memory
c5.xlarge	up to 5 Gigabit throughput	4	8 GiB
c5.2xlarge	up to 10 Gigabit throughput	8	16 GiB
c5.4xlarge	up to 10 Gigabit throughput	16	32 GiB
c5.9xlarge	up to 10 Gigabit throughput	36	72 GiB
c5n.xlarge	up to 25 Gigabit throughput	4	10.5 GiB
c5n.2xlarge	up to 25Gigabit throughput	8	21 GiB
c5n.4xlarge	up to 25 Gigabit throughput	16	42 GiB
c5n.9xlarge	up to 50 Gigabit throughput	36	96 GiB

## AWS の Cisco クラウド ネットワーク コントローラおよび CCR 向けプライベート IP アドレス サポート

デフォルトで 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 Network Controller GUI を使用したリージョンの管理 \(クラウドテンプレートの構成\)](#) の手順を参照してください。

デフォルトでプライベート IP アドレスは Cisco Cloud Network Controller 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。接続にプライベート IP アドレスが使用されるように Cisco Cloud Network Controller へのパブリック IP を無効にするには、[\[AWS インストール ガイド向け Cisco クラウド ネットワーク コントローラ \(Cisco Cloud Network Controller for AWS Installation Guide\) \]の\[AWS 内の Cisco クラウド ネットワーク コントローラを展開 \(Deploying the Cisco Cloud Network Controller in AWS\) \]](#)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 クラウド ネットワーク コントローラ サイトに接続するためのクラウドバックボーン

## Communicating to External Sites From Regions Without a CCR

Support is available for communication with an external site from regions without a CCR. This is accomplished by making use of the AWS Transit Gateway feature. When you enable the AWS Transit Gateway feature on Cisco Cloud Network Controller, you also enable peering between all managed regions on AWS. In this way, the AWS Transit Gateway peering feature allows the Cisco Cloud Network Controller to address the issue of communicating with external sites from regions without a CCR. It addresses this issue by having traffic rerouted to a region with a CCR.

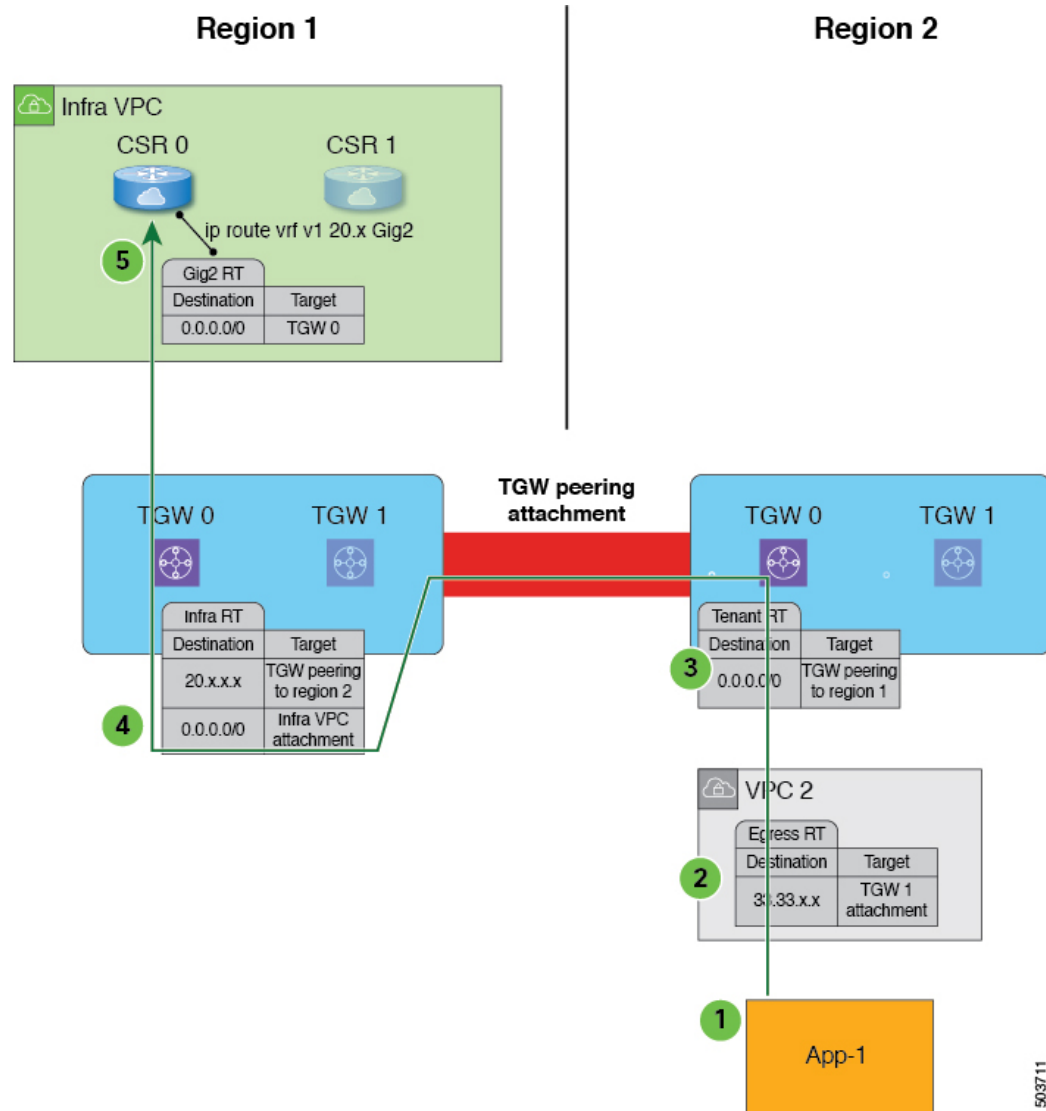
Using the AWS Transit Gateway feature, when traffic from a region without a CCR tries to egress out of a site, this traffic will be routed to the infra VPC for the closest region with a CCR. After the traffic is rerouted to that region's infra VPC, that CCR is used to egress out the packet. For ingress traffic, packets coming from an external site can reach any region's CCR and then be routed to the destination region using the AWS Transit Gateway peering in the ingress data path.

In these situations, traffic is rerouted automatically when the system recognizes that external traffic is egressing or ingressing through a region without a CCR. However, you must have the following components configured in order for the system to automatically perform this rerouting task:

- AWS Transit Gateway must be configured. If AWS Transit Gateway is not already configured, see [Increasing Bandwidth Between VPCs by Using AWS Transit Gateway](#) for those instructions.
- CCRs must be deployed in at least one region. Even though this enhancement allows you to communicate with an external site from a region that *does not* contain a CCR, in order to do this, you

must have another separate region that *does* contain a CCR so that traffic can be rerouted from the region without a CCR to the region with a CCR.

The following figure shows an example scenario where traffic is rerouted automatically when the system recognizes that external traffic is egressing from a region without a CCR.



503711

The following occurs when the Cisco Cloud Network Controller recognizes that Region 2 does not have a CCR, but traffic is egressing out to an external site (shown with the green arrow and circles):

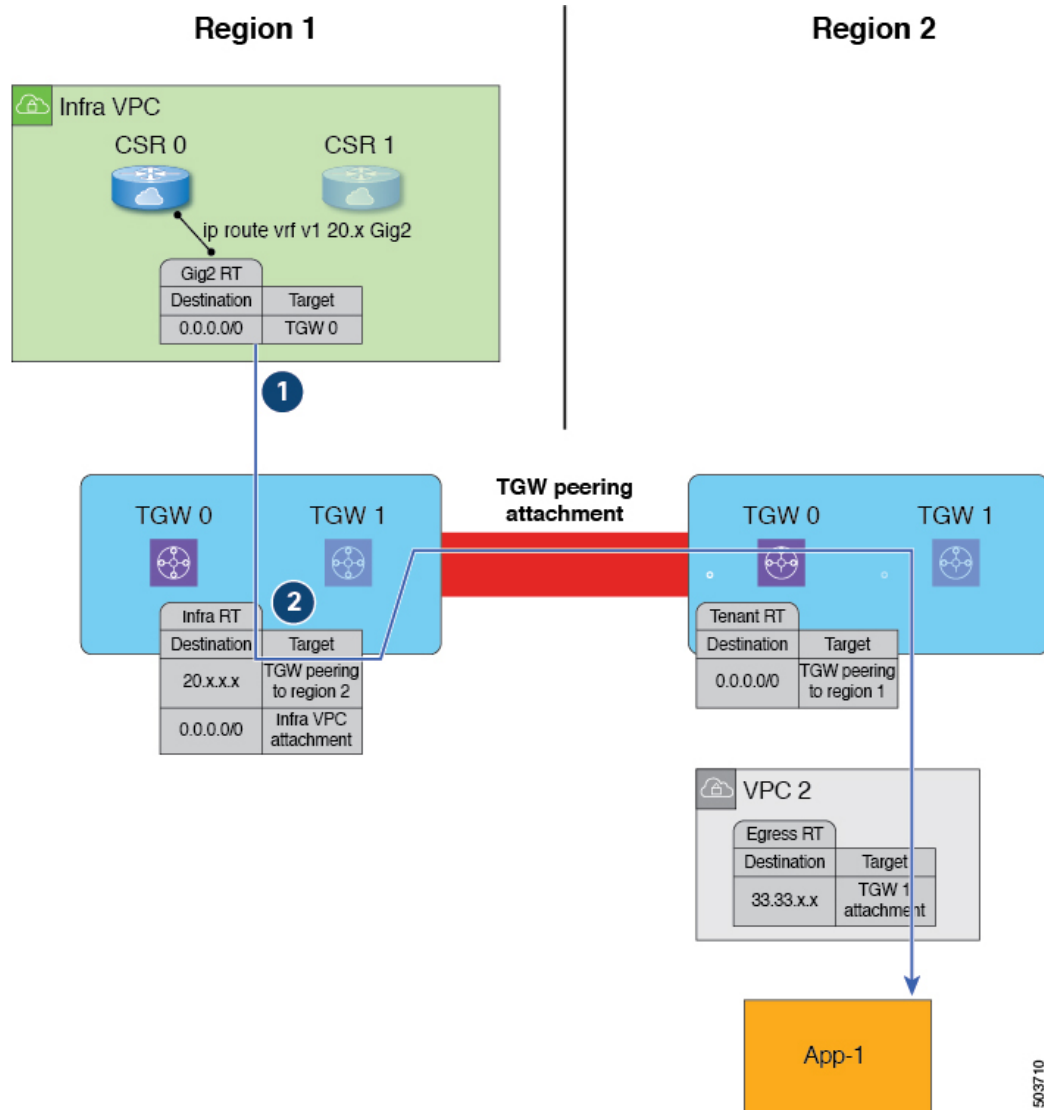
1. Traffic flow begins egressing out from the CIDR in App-1 in Region 2 to a remote site. Note that the endpoint is configured with the appropriate outbound rule to allow the remote site CIDR.
2. The VPC 2 egress route table has the remote site CIDR, which then has the AWS Transit Gateway as the next hop. The AWS Transit Gateway information is programmed automatically based on the configured contracts.

3. A 0.0.0.0/0 route is inserted in the AWS Transit Gateway route table, which essentially tells the system to take the AWS Transit Gateway peering attachment if traffic is egressing out to an external site but there is no CCR in this region. In this situation, the AWS Transit Gateway peering attachment goes to another region that does have a CCR (Region 1 in the example scenario). The region with a CCR that will be used is chosen based on geographical proximity to the region that does not have a CCR.
4. The packet is first forwarded to the infra VPC in the region with the CCR (Region 1), and is then forwarded to the gigabit ethernet network interface on the CCR that is associated with the appropriate VRF group.
5. The gigabit 2 inbound security group on the CCR in Region 1 is configured to allow traffic from the remote region VPC.

It's useful to note that in the egress example shown above:

- For steps 1 and 2, there is no change from pre-release 5.2(1) behavior.
- Step 3 is behavior that is new and unique to this feature in release 5.2(1), where the redirect occurs to the TGW peering attachment from the region without a CCR to the region with a CCR. In addition, step 3 occurs on the AWS cloud.
- Steps 4 and 5 would normally occur in Region 2 before release 5.2(1), but only if Region 2 had a CCR. However, because Region 2 does not have a CCR, with this feature in release 5.2(1), these steps are taking place in Region 1 where a CCR is present.

The following figure shows an example scenario where traffic is rerouted automatically when the system recognizes that external traffic is ingressing to a region without a CCR.



The following occurs when the Cisco Cloud Network Controller recognizes that Region 2 does not have a CCR, but traffic is ingressing in from an external site to a CIDR in App-1 in Region 2 (shown with the blue arrow and circles):

1. Normally, the CCR in Region 1 would only advertise the CIDRs that are local to that region. However, with this enhancement that is part of release 5.2(1), all CCRs in all regions now advertise CIDRs from all remote regions. Therefore, in this example, the CCR in Region 1 will also advertise the CIDRs that are in Region 2 (assuming AWS Transit Gateway peering is configured between both regions and the contracts are configured correctly). In this situation, the traffic ingresses in from an external site to the CCR in Region 1, where the CCR in Region 1 advertises the static route for the remote region VPC CIDRs.
2. The infra route table (the AWS Transit Gateway route table in Region 1) has the next hop to the AWS Transit Gateway peering attachment to Region 2.

It's useful to note that in the ingress example shown above:

- Both steps (steps 1 and 2) in the ingress example shown above are new and unique to this feature in release 5.2(1).
- Step 1 in the ingress example shows configurations programmed on the CCR.
- Step 2 in the ingress example occurs on the AWS cloud.

## CCR のリモートサイトからの ECMP 転送のサポート

CCR を使用した ECMP がサポートが利用可能です。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。このサポートは自動的に有効になり、有効にするために手動で構成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。ただし、すべてのリージョンの CCR が同じプリファレンスの CIDR をアドバタイズするのではなく、CIDR がローカルであるリージョンからより高いプリファレンスで CCR をアドバタイズするためのサポートを使用できます。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。

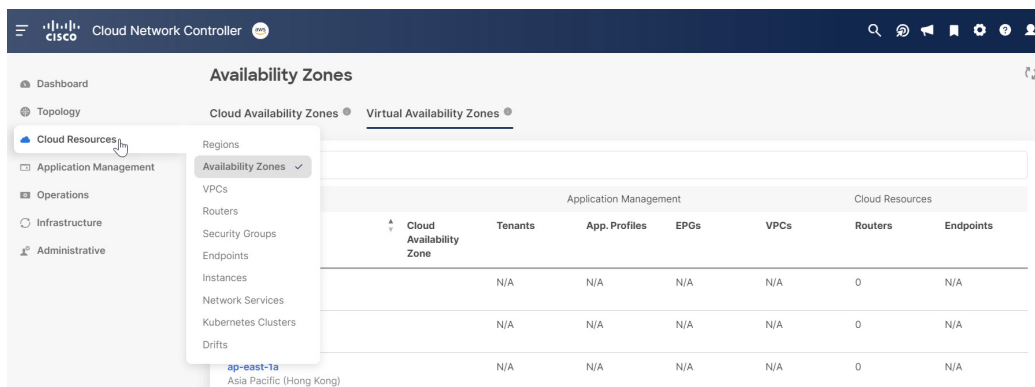
## 可用性ゾーン

Cisco クラウドネットワーク コントローラでは、次の 2 種類の可用性ゾーンがサポートされています。

- **仮想アベイラビリティ ゾーン** : Cisco Cloud Network Controller は、AWS のリージョンごとに 2 つの仮想アベイラビリティゾーンのみをサポートします。その際、Cisco Cloud Network Controller は、<リージョン名>a と <リージョン名>b という命名法により、リージョンごとに 2 つの仮想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 Network Controller 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。

Cisco Cloud Network Controller 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 (Cloud Resources)] > [アベイラビリティゾーン (Availability Zones)] に移動し、[仮想アベイラビリティゾーン (Virtual Availability Zones)] 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



- **クラウドアベイラビリティゾーン**：このタイプのアベイラビリティゾーンでは、Cisco Cloud Network Controller を使用して AWS リージョンごとに複数のアベイラビリティゾーンを使用できます。

Cisco Cloud Network Controller 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 (Cloud Resources)] > [アベイラビリティゾーン (Availability Zones)] に移動し、[クラウドアベイラビリティゾーン (Cloud Availability Zones)] 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

仮想可用性ゾーンが構成されている展開がある場合は、仮想可用性ゾーンからクラウド可用性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

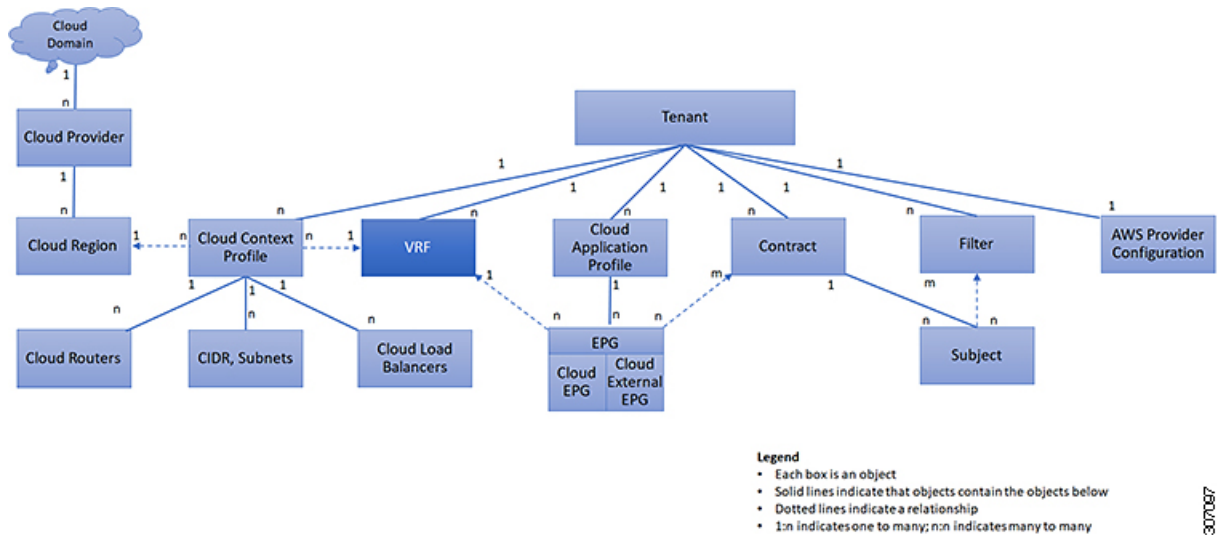
次に、複数のアベイラビリティ ゾーンのリソースに関するガイドラインと制限事項を示します。

- 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 ゾーンのリソースは、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 ゾーンのリソース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 クラウド ネットワーク コントローラ 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



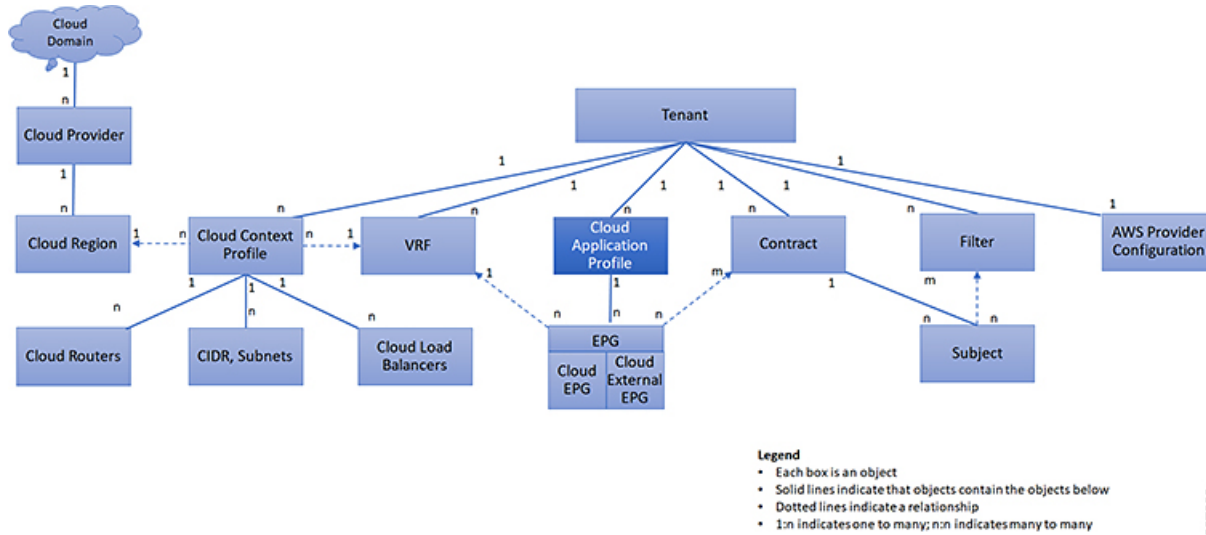
VRF は、レイヤ 3 のアドレス ドメインを定義します。1 つ以上のクラウド コンテキスト プロファイルが VRF に関連付けられます。特定のリージョンの VRF に関連付けることができるクラウド コンテキスト プロファイルは 1 つだけです。レイヤ 3 ドメイン内のすべてのエンドポイントが一意的 IP アドレスを持っている必要があります。なぜなら、ポリシーで許可されている場合にこれらのデバイス間でパケットを直接転送できるためです。テナントには、複数の VRF を含めることができます。管理者が論理デバイスを作成した後、管理者はデバイスクラスタの選択基準ポリシーを提供する論理デバイスの VRF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

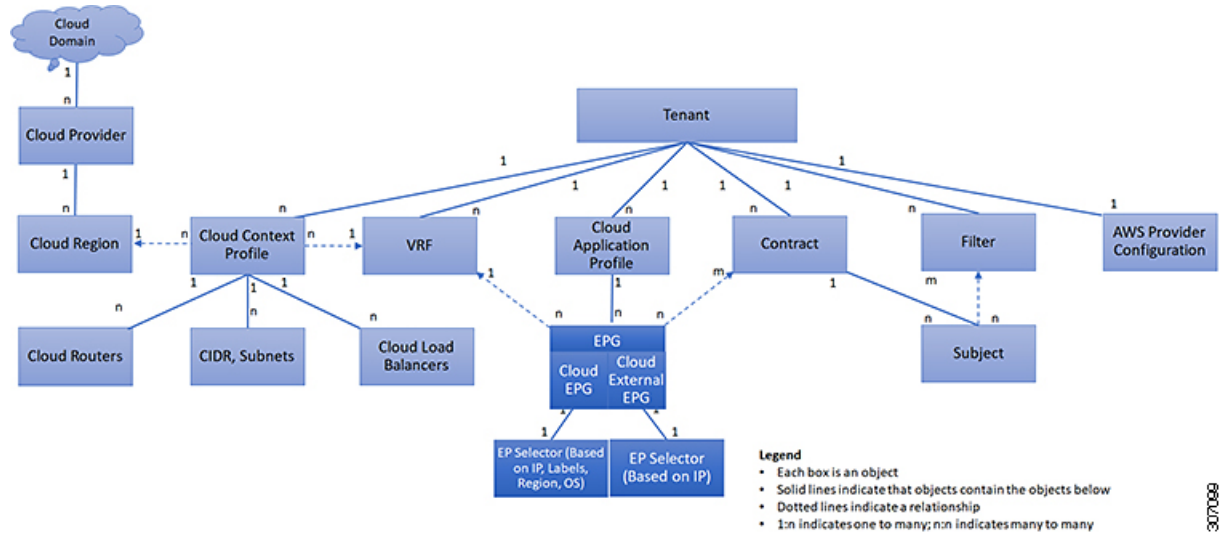
クラウド EPG は次のいずれかに従って組織化できます。

- 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、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

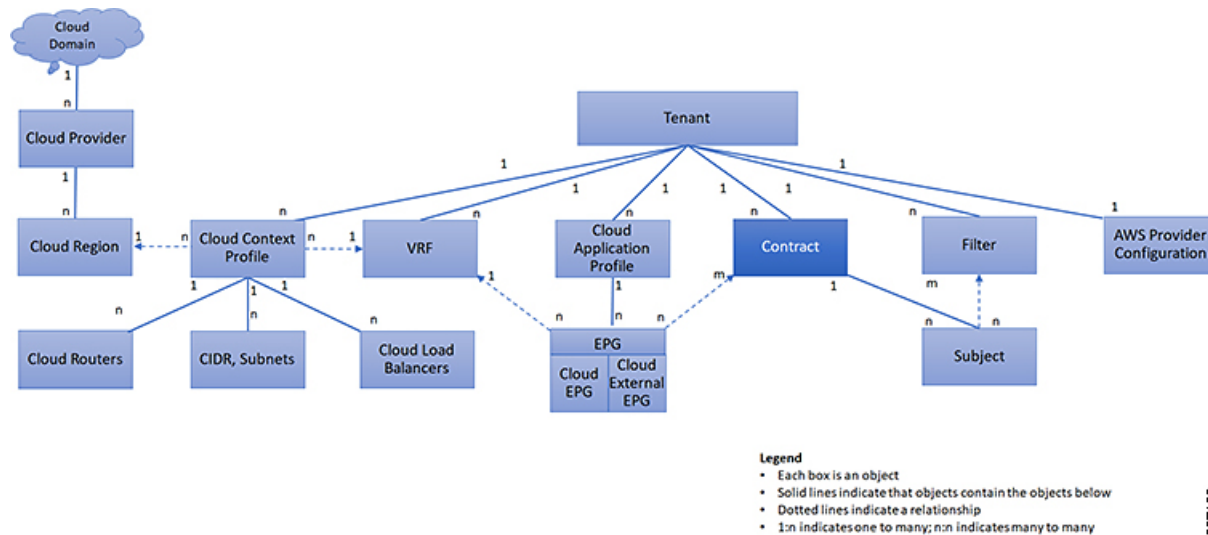
学習します。エンドポイントを学習すると、クラウドインフラストラクチャは、それに基づいて cloudExtEPg クラウド EPG ポリシーを適用します。たとえば、WAN 接続クライアントがアプリケーション (cloudEPg) クラウド EPG 内でサーバとの TCP セッションを開始すると、cloudExtEPg クラウド EPG は、cloudExtEPg クラウド EPG Web サーバとの通信が始まる前に、そのクライアント エンドポイントにポリシーを適用します。クライアントサーバ TCP セッションが終わり、クライアントとサーバの間の通信が終了すると、その WAN エンドポイントはもうクラウドインフラストラクチャ内に存在しません。

Cisco Cloud Network Controller はエンドポイントセクタを使用して、エンドポイントをクラウド EPG に割り当てます。エンドポイントセクタは、基本的に言って、Cisco CNC 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。

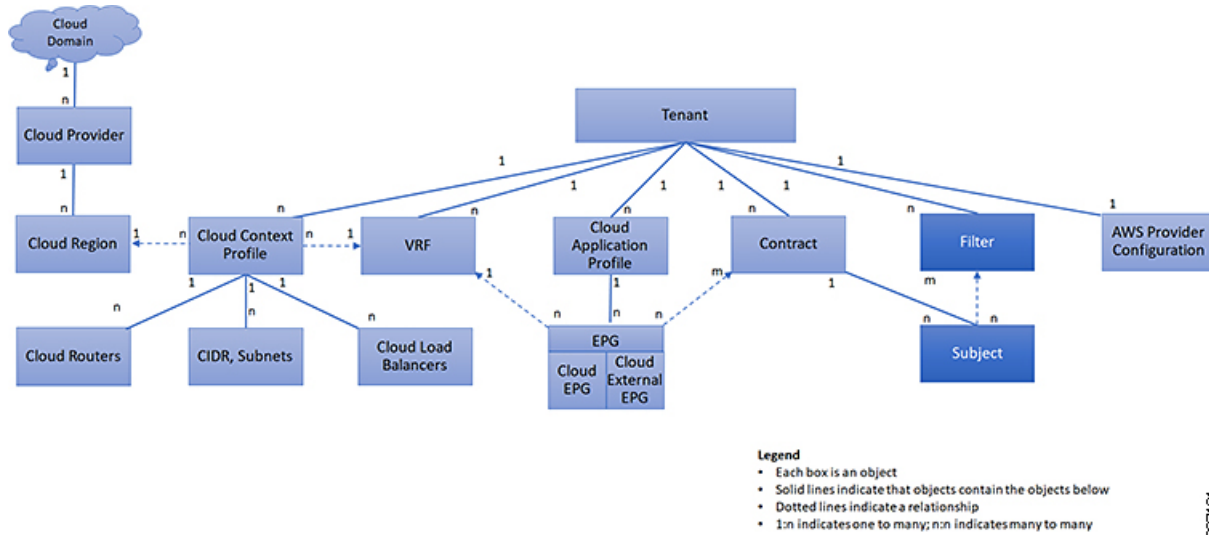


(注) 1 つのクラウド EPG で同じコントラクトを指定および使用できます。クラウド EPG は複数のコントラクトを同時に指定および使用することもできます。

## 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示し、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。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 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。

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 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。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 Network Controller 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 Network Controller AMI を展開する 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 Network Controller に直接提供します。Cisco Cloud Network Controller 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。 <ul style="list-style-type: none"> <li>• routerUsername</li> <li>• routerPassword</li> <li>• routerThroughput</li> <li>• routerLicenseToken</li> <li>• routeDataInterfacePublicIP</li> <li>• routerMgmtInterfacePublicIP</li> </ul>
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。

MO	目的
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 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。
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。

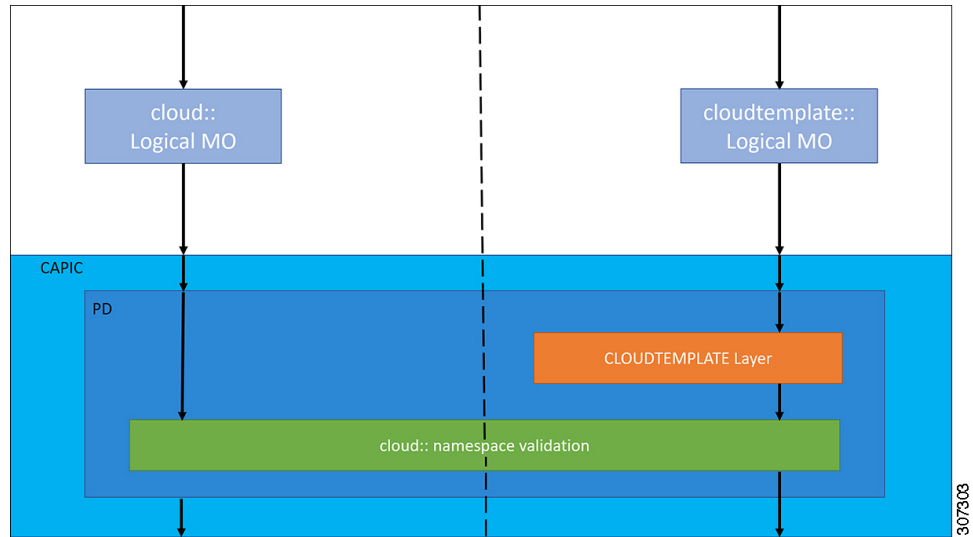
Cisco Cloud Network Controller では、クラウドテンプレートにより、MO の階層化は通常の Cisco APIC とは若干異なります。通常の Cisco APIC では、2つの変換レイヤを通過する論理 MO をポストします。

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。

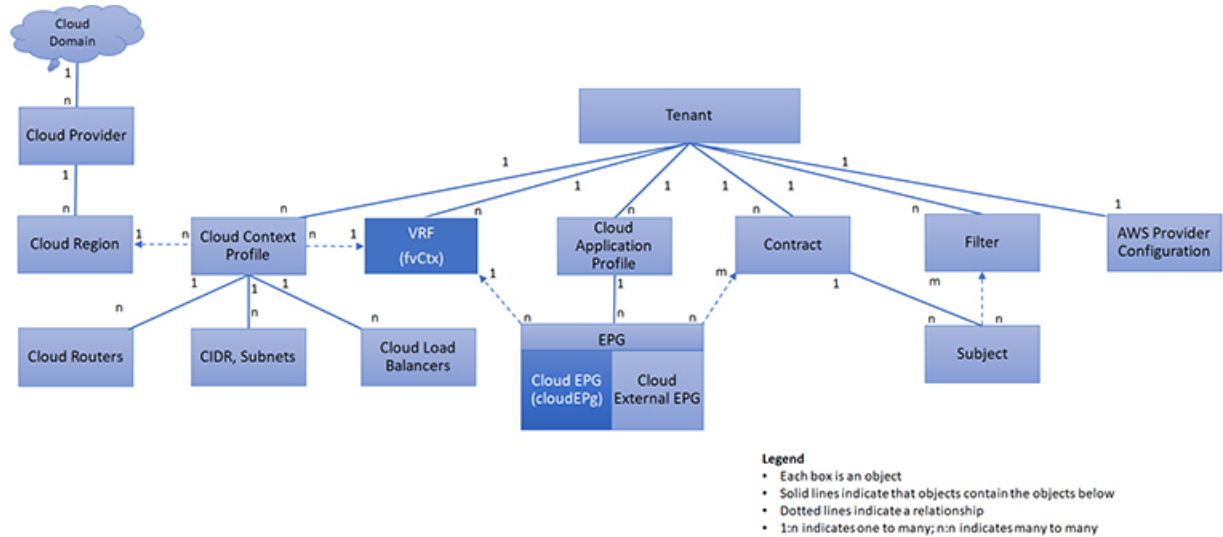
## 管理対象オブジェクトの関係とポリシー解決

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。

- `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、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 コンテキストプロヴァイル、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。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 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。

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。

## 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。