Cisco Cloud APIC ポリシー モデル

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。

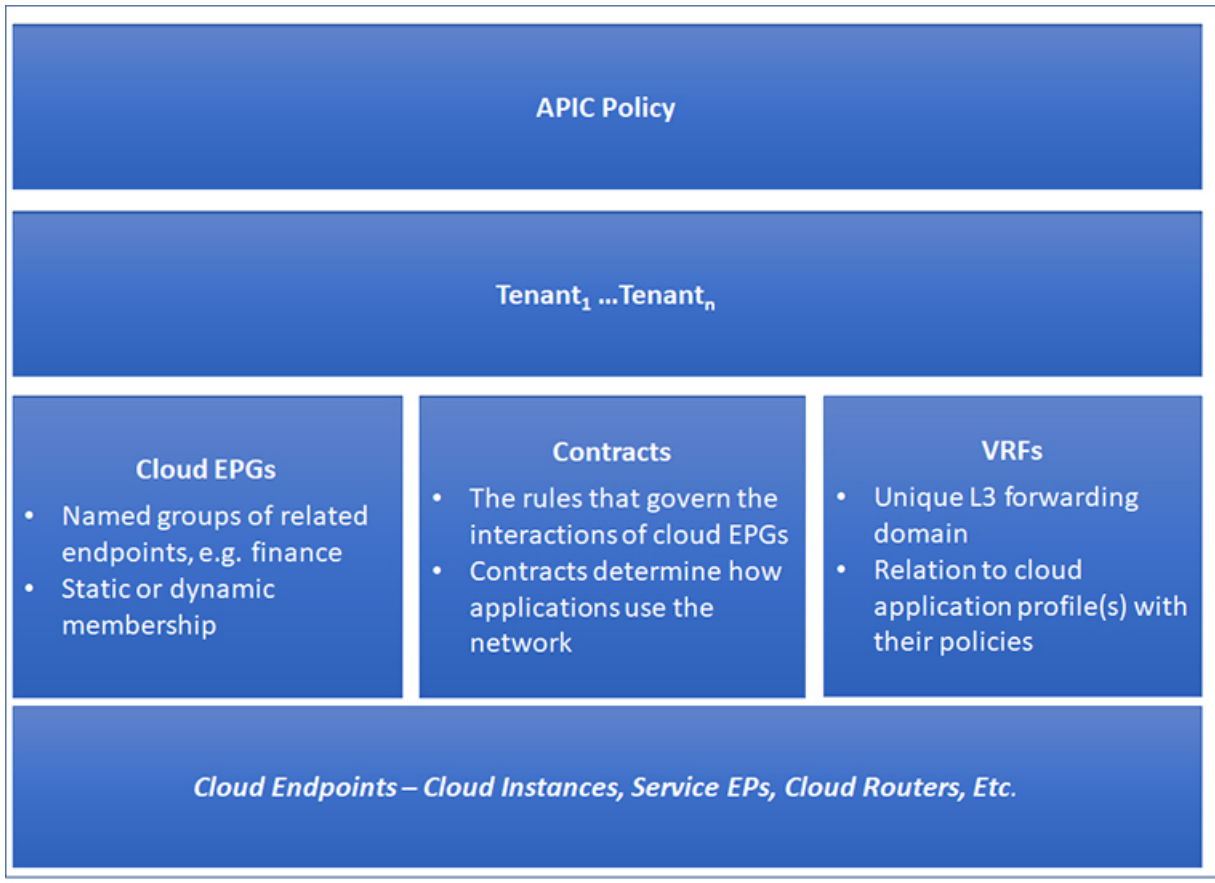
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシ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

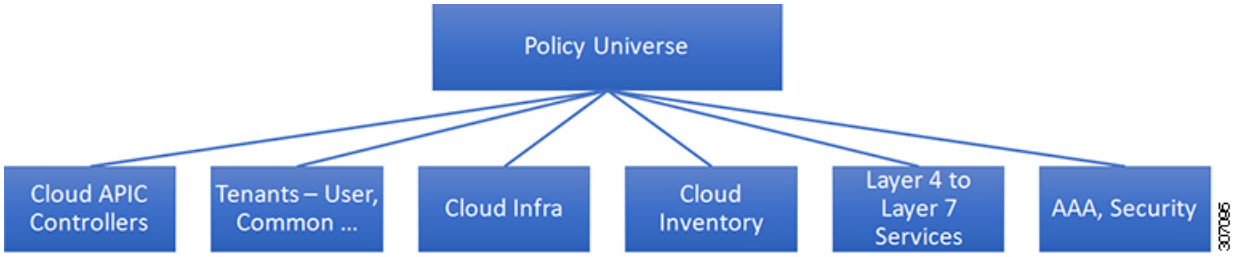
Cisco ACI ポリシー管理情報モデル

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。

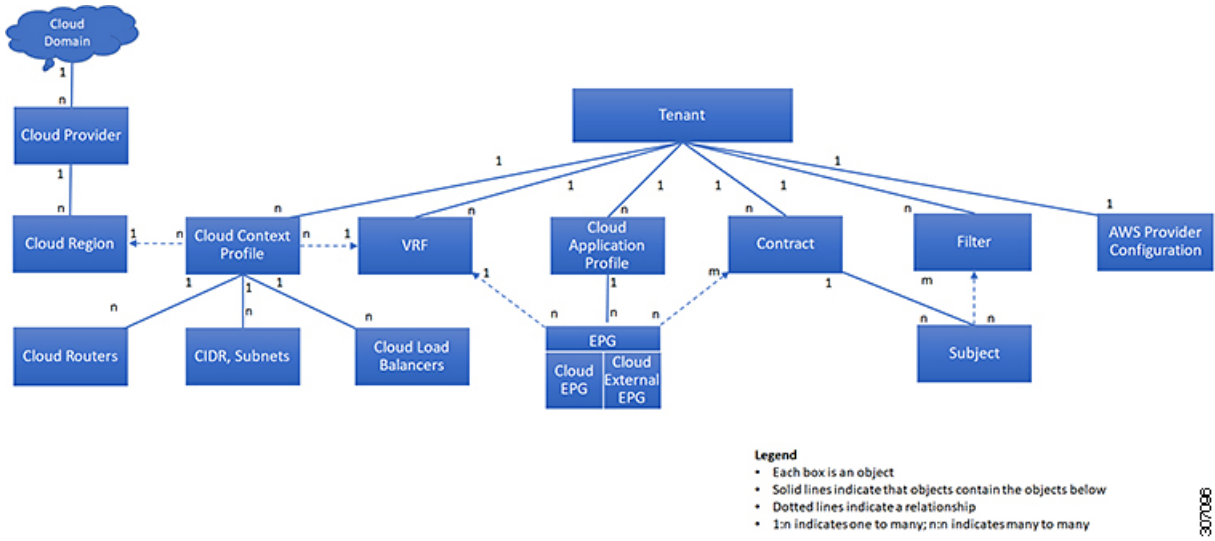
- クラウド インベントリは、GUI を使用してシステムのさまざまな側面を表示できるサービスです。たとえば、アプリケーションの側面から展開されたリージョンや、領域の側面から展開されたアプリケーションを表示できます。この情報は、クラウド リソースの計画とトラブルシューティングに使用できます。
- レイヤ 4 ～ レイヤ 7 のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムは動的に応答することができます。詳細については、レイヤ 4 から レイヤ 7 サービスの展開 を参照してください。
- アクセス、認証、およびアカウンティング（AAA）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

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 APIC solution.

The type of CCR used with the Cisco Cloud APIC varies depending on the release:

- For releases prior to release 25.0(3), the **Cisco Cloud Services Router 1000v** is used with the Cisco Cloud APIC. For more information on this type of CSR, see the Cisco Cloud Services Router 1000v documentation.
- For release 25.0(3) and later, the **Cisco Catalyst 8000V** is used with the Cisco Cloud APIC. For more information on this type of CCR, see the Cisco Catalyst 8000V Edge software documentation.

About the Cisco Catalyst 8000V

Beginning with release 25.0(3), Cisco Cloud APIC moves from the Cisco Cloud Services Router 1000v to the Cisco Catalyst 8000V. Following are updates that are specific to the Cisco Catalyst 8000V.

- #unique_31 unique_31_Connect_42_section_wrv_w2n_vsb
- #unique_31 unique_31_Connect_42_section_r2n_w2n_vsb

Licensing

The Cisco Catalyst 8000V supports subscription-based licensing.

- 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 #unique_31 unique_31_Connect_42_section_wrv_w2n_vsb.

Cisco Cloud APIC 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.

Throughput

For the BYOL Licensing 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 APIC.

The following table shows the mapping of throughput from the older Cisco Cloud Services Router 1000v routers to the newer Cisco Catalyst 8000V routers:

Throughput on Cisco Cloud Services Router 1000v	Throughput on Cisco Catalyst 8000V
10M	T0 (up to 15M throughput)
50M	T1 (up to 100M throughput)
100M	T1 (up to 100M throughput)
250M	T2 (up to 1G throughput)
500M	T2 (up to 1G throughput)
1G	T2 (up to 1G throughput)

Throughput on Cisco Cloud Services Router 1000v	Throughput on Cisco Catalyst 8000V
2.5G	T3 (up to 10G throughput)
5G	T3 (up to 10G throughput)
7.5G	T3 (up to 10G throughput)
10G	T3 (up to 10G throughput)

Private IP Address Support for Cisco Cloud APIC and CCR in AWS

（注） For Azure, support for private IP addresses for Cisco Cloud APIC and CCRs became available in release 5.1(2). 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。

For AWS, prior to release 5.2(1), Cisco Cloud Router (CCR) interfaces were assigned both public and private IP address by Cisco Cloud APIC. Beginning with release 5.2(1), CCR interfaces are assigned private IP addresses only and assignment of public IP addresses to CCR interfaces is optional. Private IP addresses are always assigned to all the interfaces of a CCR. The private IP address of GigabitEthernet1 of a CCR is used as BGP and OSPF router IDs.

To enable CCR private IP addresses for inter-site connectivity, where you are disabling public IP addresses for the CCR interfaces, see the 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） procedure.

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。

Restrictions for CCR with Private IP Address

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

Communicating to External Sites From Regions Without a CCR

Prior to release 5.2(1), for traffic to pass through to an external site, the region where the traffic is passing through must have a CCR deployed. The CCR advertises the CIDRs that are local to that region. If an

EPG in a region has a contract with an external site, then that region must have a CCR deployed in order to communicate with that external site.

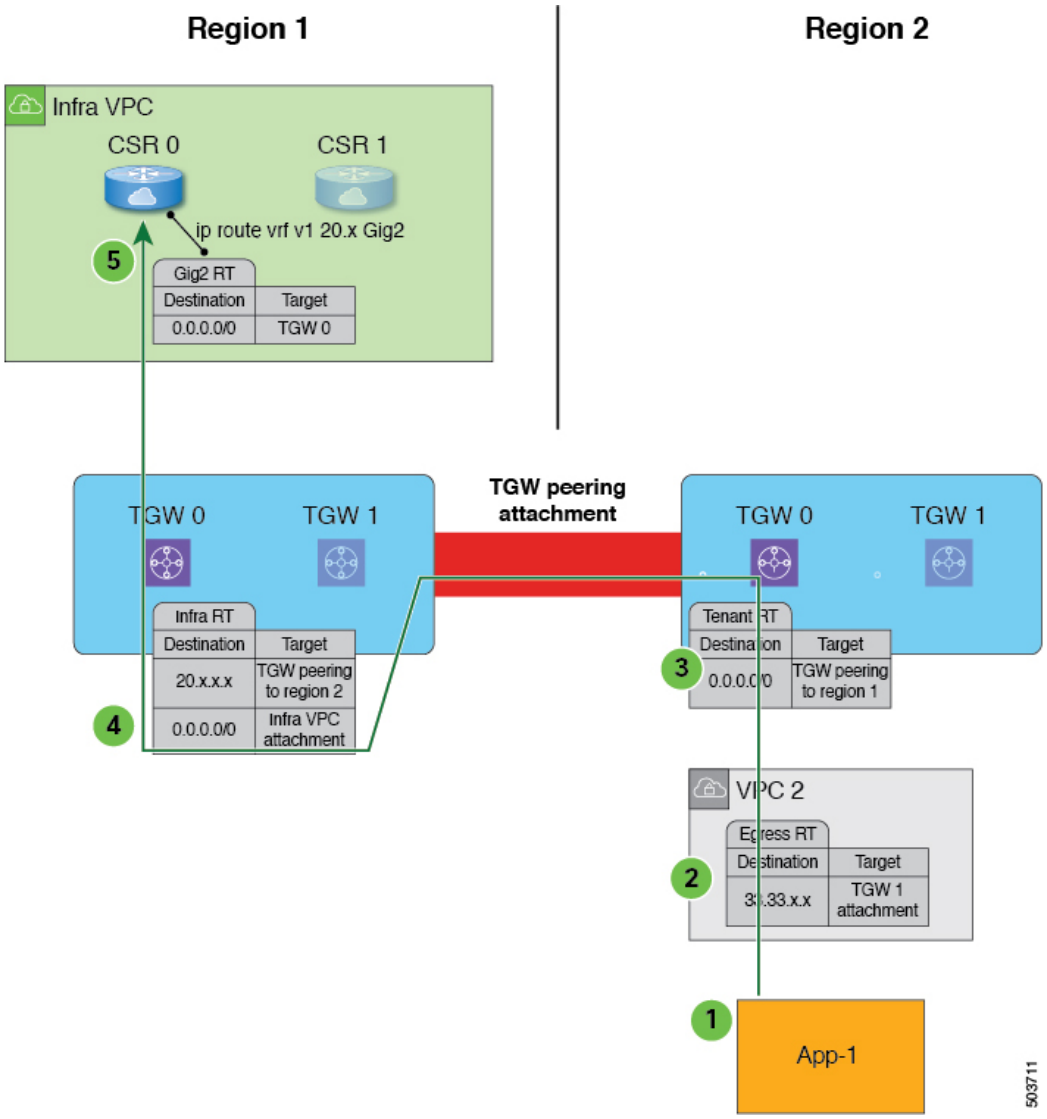
Beginning with release 5.2(1), you can now have communication with an external site from regions without a CCR. This is accomplished by making use of the AWS Transit Gateway feature, which became available for Cisco Cloud APIC in release 5.0(1). When you enable the AWS Transit Gateway feature on Cisco Cloud APIC, you also enable peering between all managed regions on AWS. In this way, the AWS Transit Gateway peering feature allows the Cisco Cloud APIC 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.



The following occurs when the Cisco Cloud APIC 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):

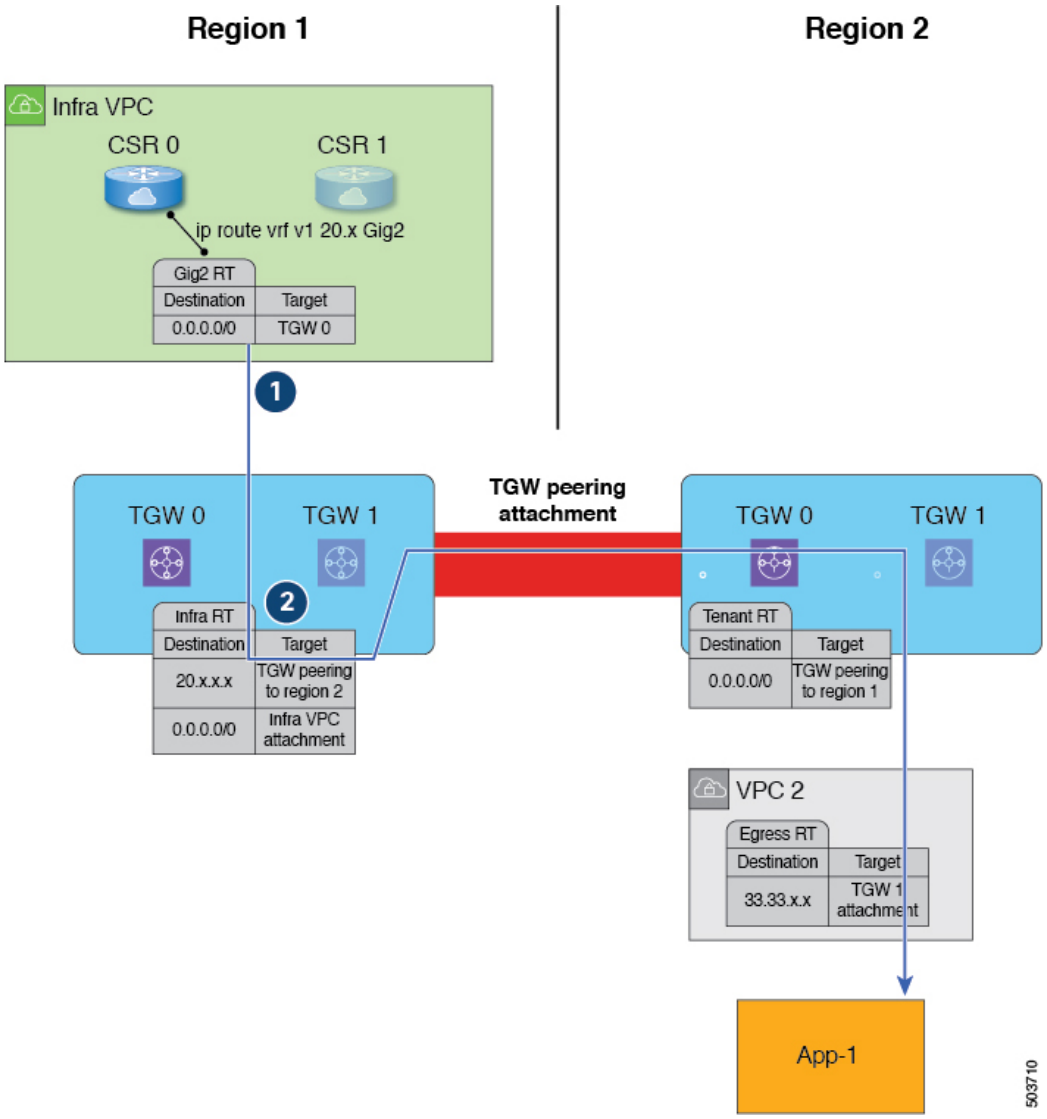
1. Traffic flow begins egressing out from the CIDR in App-1 in Region 2 to a remote site. Note that the endpoint is configured with the appropriate outbound rule to allow the remote site CIDR.
2. The VPC 2 egress route table has the remote site CIDR, which then has the AWS Transit Gateway as the next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

Support for ECMP Forwarding from Remote Sites for CCRs

CCRs in a cloud will typically receive more than one path for a prefix. Prior to release 5.2(1), there was no support for data forwarding from CCRs using Equal Cost Multiple Path (ECMP), even though the CCR receives multiple paths.

Beginning with release 5.2(1), support is now available for ECMP with CCRs, where traffic from CCRs will be forwarded to all ECMP paths received from a destination site. 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。

Preference For Routes to CCRs in Regions with Local CIDRs

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。With multiple regions in a cloud, CCRs from all regions advertise the CIDRs for redundancy. Prior to release 5.2(1), CCRs from all regions advertised the CIDRs with the same preference. 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。

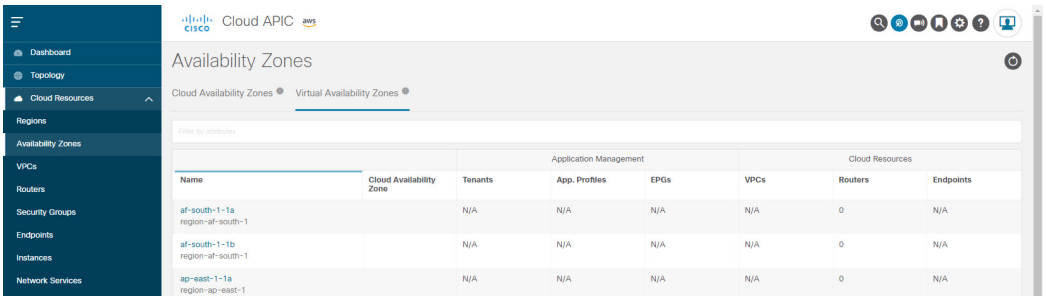
Beginning with release 5.2(1), CCRs from multiple regions will continue to advertise the CIDRs, but CCRs from the region where the CIDR is local will advertise with a higher preference. これにより、オンプレミス サイトまたはリモート クラウド サイトは、CIDR がローカルであるリージョンにトラフィックを直接送信します。If the CCRs in the local region fail, the paths from the other regions can be used for data forwarding.

可用性ゾーン

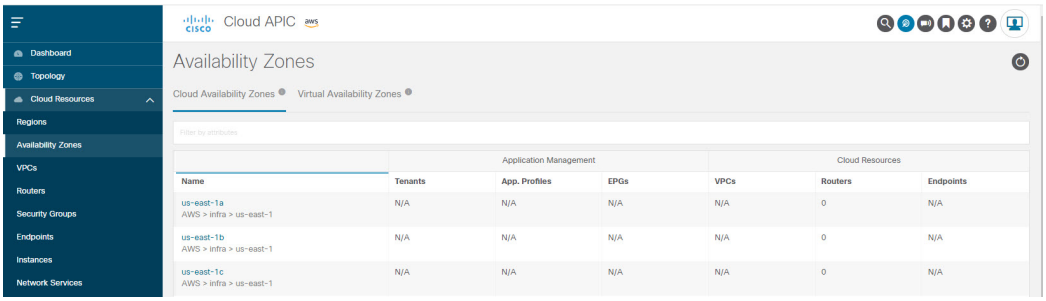
リリース 25.0(2) より前は、Cisco Cloud APIC は AWS のリージョンごとに 2 つのアベイラビリティ ゾーンのみをサポートします。その際に、Cisco Cloud APIC が <region-name>a と <region-name>b の形式を使用して、各リージョンに対して**仮想**アベイラビリティ ゾーンと呼ばれる 2 つのアベイラビリティ ゾーンを作成します。たとえば、`us-west-1` リージョンの下に、Cisco Cloud APIC は 2 つの仮想アベイラビリティ ゾーン `us-west-1a` と `us-west-1b` を作成します。

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。

ガイドラインと制約事項

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。

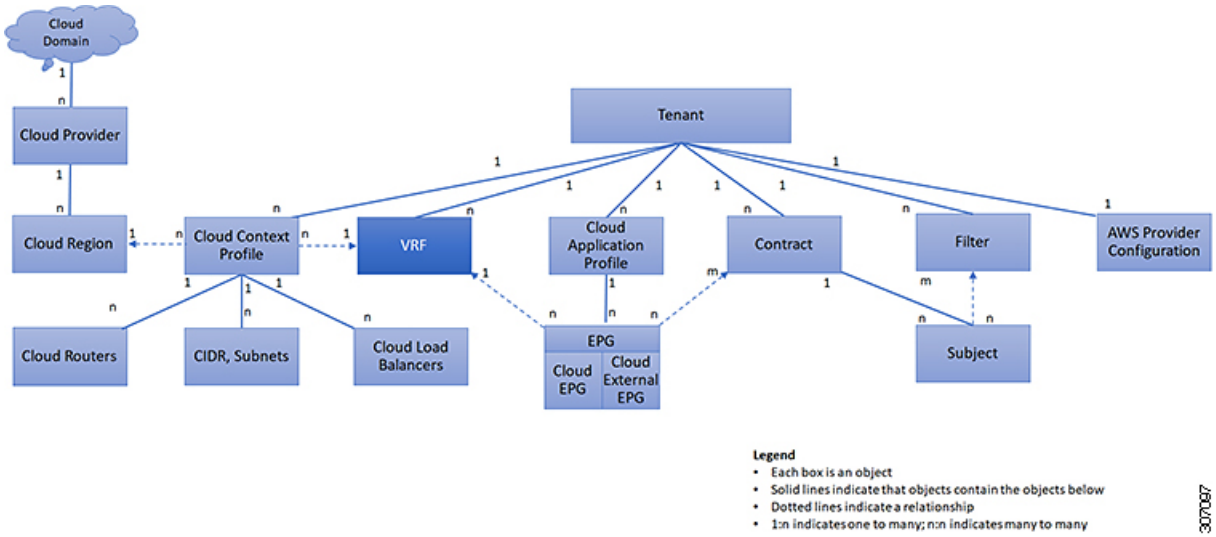
- 3 つ以上のアベイラビリティ ゾーンを持つことができるクラウド アベイラビリティ ゾーンのサポートは、ユーザーテナントでのみ利用できます。インフラテナントは、2つのアベイラビリティ ゾーンの制限がある仮想アベイラビリティ ゾーンを引き続き使用します。

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*

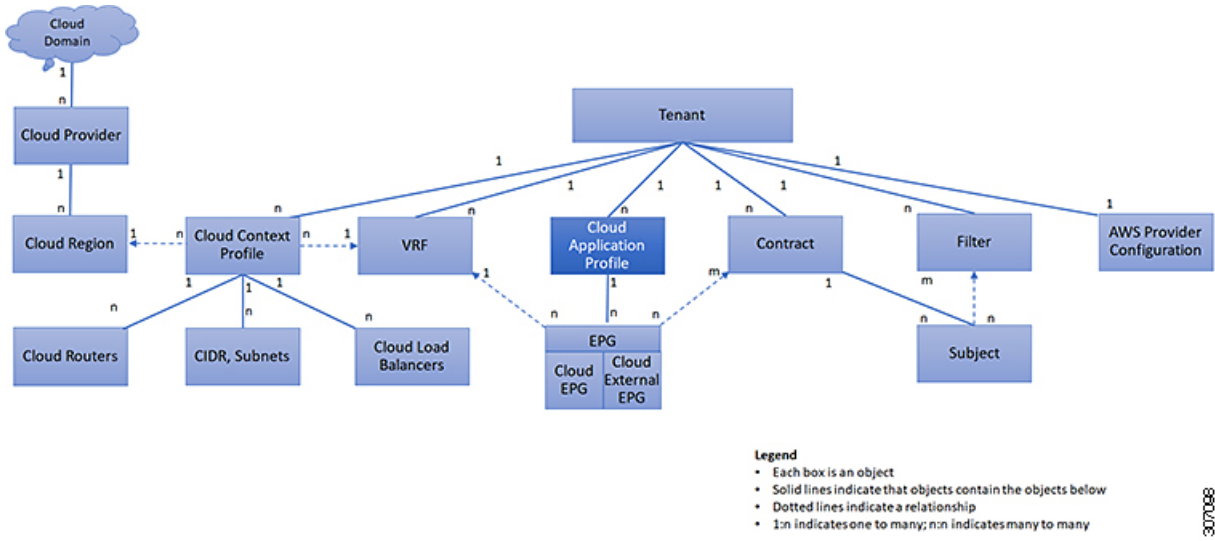


VRF は、レイヤ 3 のアドレス ドメインを定義します。1 つ以上のクラウド コンテキスト プロファイルが VRF に関連付けられます。特定のリージョンの VRF に関連付けることができるクラウド コンテキスト プロファイルは 1 つだけです。レイヤ 3 ドメイン内のすべてのエンドポイントが一意の IP アドレスを持っている必要があります。なぜなら、ポリシーで許可されている場合にこれらのデバイス間でパケットを直接転送できるためです。テナントには、複数の VRF を含めることができます。管理者が論理デバイスを作成した後、管理者はデバイス クラスタの選択基準ポリシーを提供する論理デバイスの VRF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

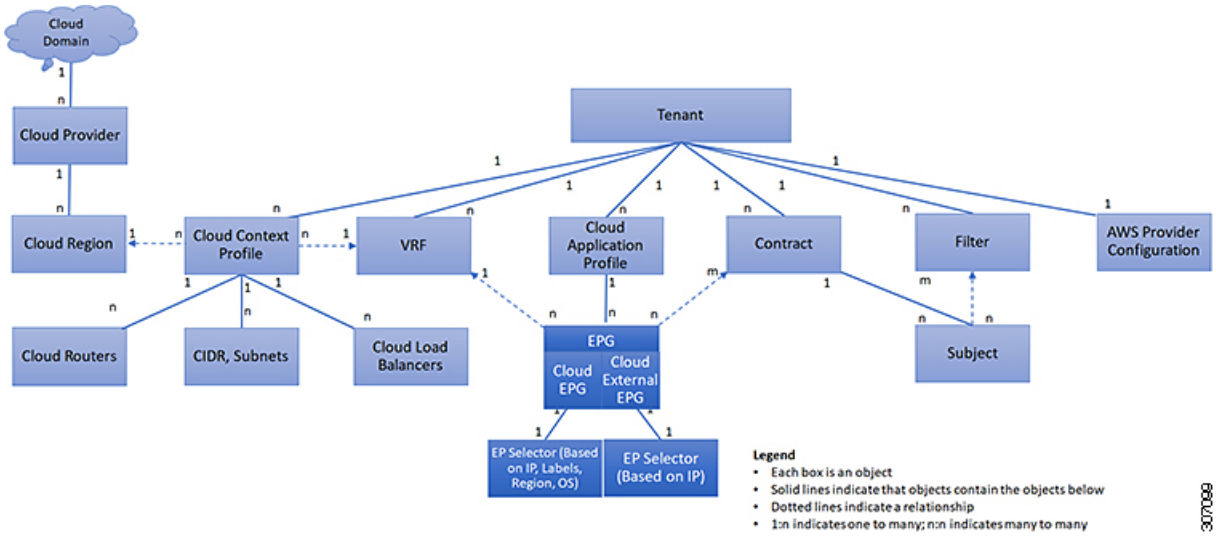
クラウド EPG は次のいずれかに従って組織化できます。

- 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

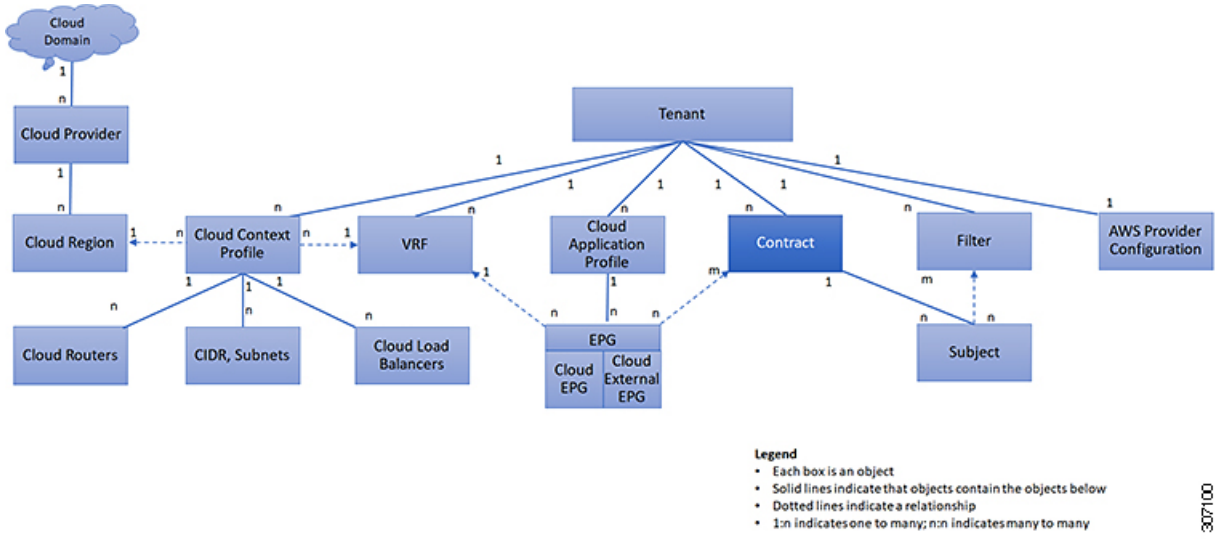
学習します。エンドポイントを学習すると、クラウドインフラストラクチャは、それに基づいて cloudExtEPg クラウド EPG ポリシーを適用します。たとえば、WAN 接続クライアントがアプリケーション（cloudEPg）クラウド EPG 内でサーバとの TCP セッションを開始すると、cloudExtEPg クラウドEPG は、cloudExtEPg クラウド EPG Web サーバとの通信が始まる前に、そのクライアント エンドポイントにポリシーを適用します。クライアント サーバ TCP セッションが終わり、クライアントとサーバの間の通信が終了すると、その WAN エンドポイントはもうクラ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

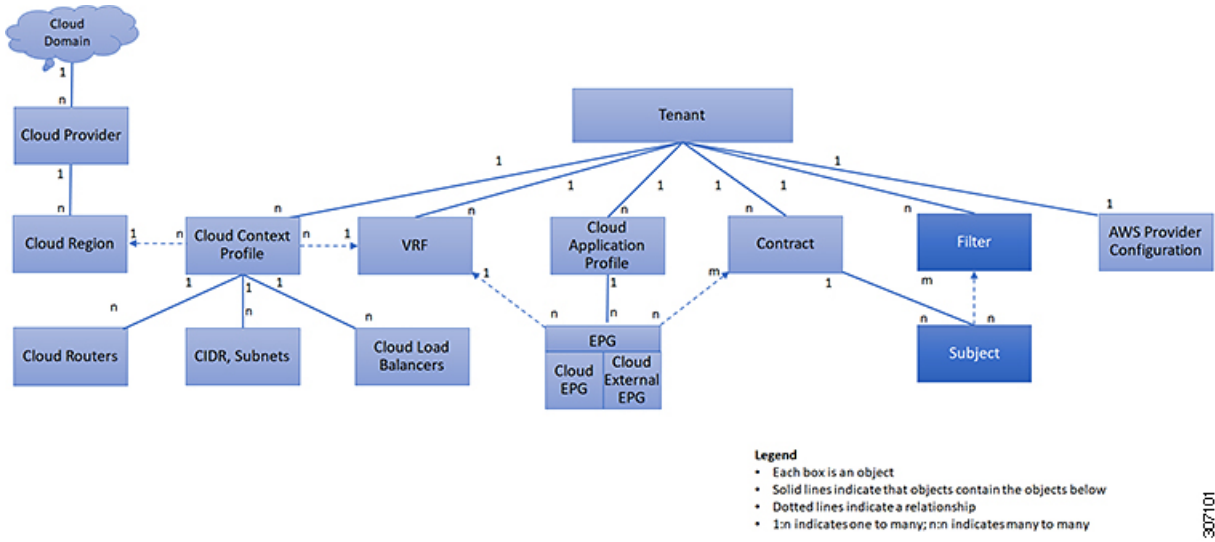
コントラクトは、プロバイダー、コンシューマ、またはその両方とラベル付されたクラウド EPG 間の通信を制御します。クラウド EPG とコントラクトの関係は、プロバイダーまたはコンシューマです。クラウド EPG がコントラクトを提供すると、通信が提供されたコントラクトに準拠している限り、そのクラウド EPG との通信は他のクラウド EPG から開始できます。クラウド EPG がコントラクトを使用すると、そのクラウド EPG のクラウド エンドポイントは、コントラクトを指定したクラウドEPGのクラウドエンドポイントと通信を開始できます。

（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`
`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。

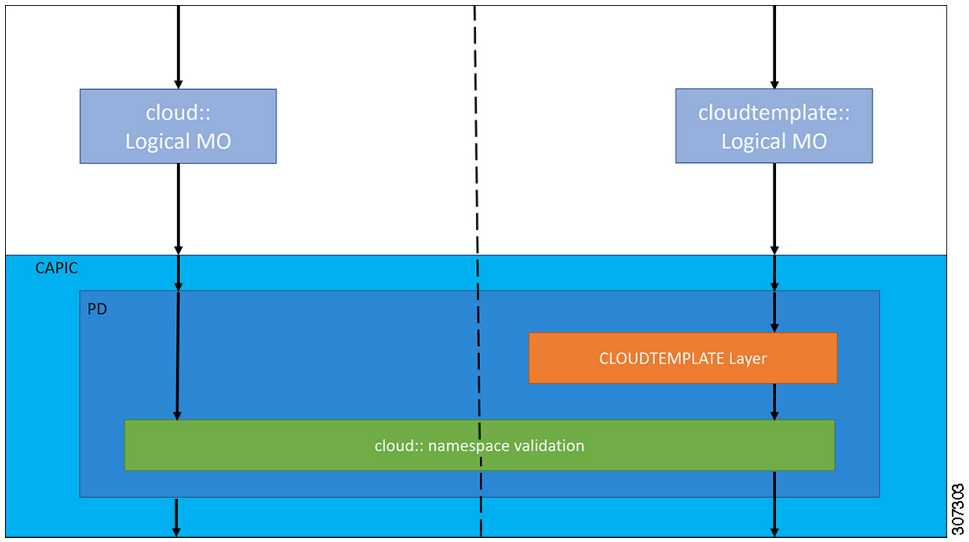
MO	目的
cloudtemplateExtNetwork	クラウド外部のインフラ ネットワーク設定入力が含まれます。 クラウド ルータが外部ネットワーキング用に設定されているリージョンのリストが含まれます。 各リージョンは、cloudRegionName子 MO を介してキャプチャされます。
cloudtemplateVpnNetwork	ACI オンプレミス サイトまたは別の Cisco Cloud APIC サイトで VPN を設定するための情報が含まれています。
cloudtemplateIpSecTunnel	ACI オンプレミス サイトの IPSec ピアの IP アドレスをキャプチャします。
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。

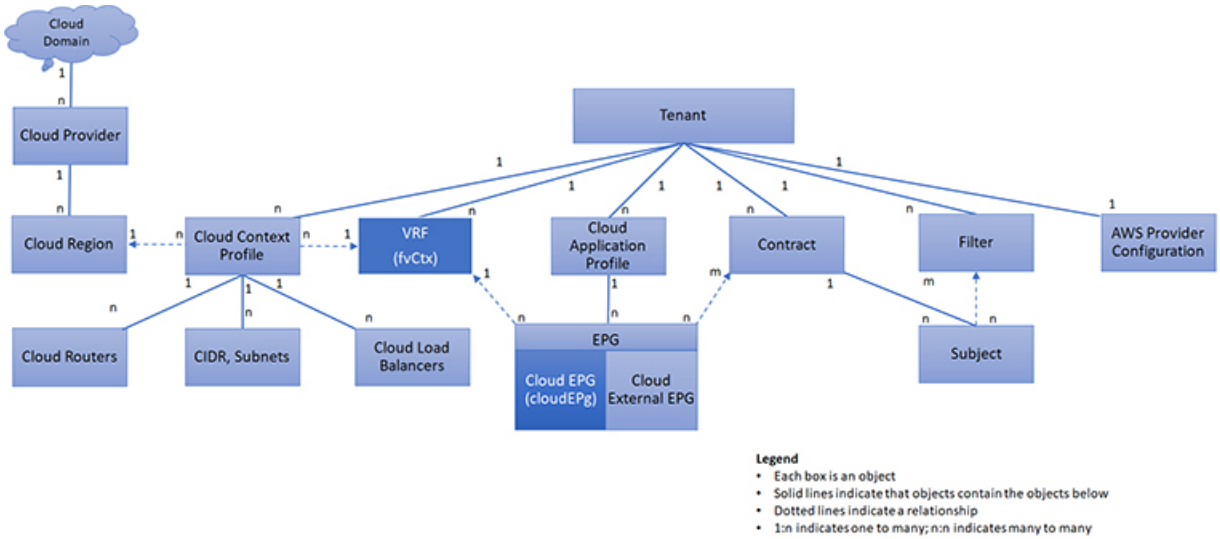
管理対象オブジェクトの関係とポリシー解決

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。