



Cisco Cloud Network Controller ポリシー モデル

- [ACI ポリシー モデルの概要 \(1 ページ\)](#)
- [ポリシー モデルの主な特性 \(1 ページ\)](#)
- [論理構造 \(2 ページ\)](#)
- [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 \(17 ページ\)](#)
- [クラウド アプリケーション プロファイル \(18 ページ\)](#)
- [クラウド エンドポイント グループ \(19 ページ\)](#)
- [コントラクト \(20 ページ\)](#)
- [クラウド テンプレートの概要 \(23 ページ\)](#)
- [管理対象オブジェクトの関係とポリシー解決 \(26 ページ\)](#)
- [デフォルト ポリシー \(27 ページ\)](#)
- [共有サービス \(28 ページ\)](#)

ACI ポリシー モデルの概要

ACI ポリシー モデルにより、アプリケーション要件のポリシーの指定を有効化します。Cisco Cloud Network Controller は、クラウドインフラストラクチャにポリシーを自動的にレンダリングします。ユーザーまたはプロセスがクラウドインフラストラクチャ内のオブジェクトへの管理上の変更を開始すると、Cisco Cloud Network Controller は最初にポリシー モデルにその変更を適用します。このポリシーモデルの変更により、実際の管理対象項目への変更がトリガーされます。この方法を、モデル方式フレームワークといいます。

ポリシー モデルの主な特性

ポリシー モデルの主な特性には次のものがあります。

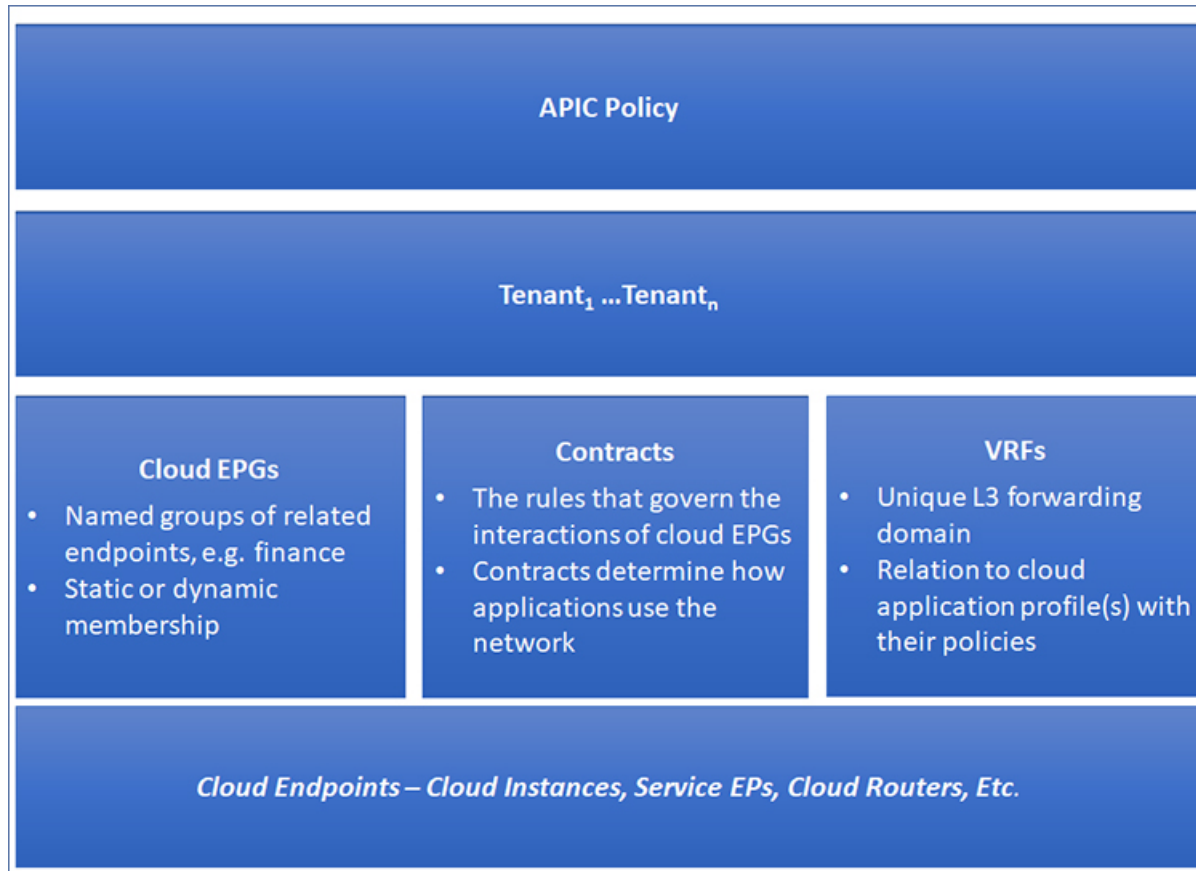
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシ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

モデル内の管理対象オブジェクトを操作することで、エンジニアは独立した個々のコンポーネントの構成を管理することから開放されます。これらの特性により、自動化と柔軟なワークロードのプロビジョニングが可能になり、インフラストラクチャ内のワークロードをどこでも検索できるようになります。ネットワーク接続されたサービスは簡単に展開でき、Cisco Cloud Network Controllerにより自動化フレームワークが提供され、それらのネットワーク接続されたサービスのライフサイクルを管理できます。

論理構造

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、ネットワークの動作を誘導する必要があり、その逆ではありません。

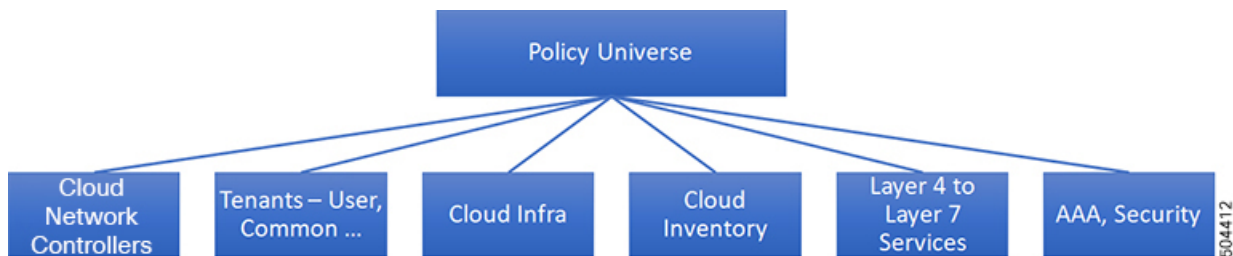
Cisco ACI ポリシー管理情報モデル

クラウドインフラストラクチャは、階層型管理情報ツリー（MIT）で表示できる管理情報モデル（MIM）に記録される論理コンポーネントから構成されます。Cisco Cloud Network Controller は、情報モデルを保存および管理するプロセスを実行します。OSI 共通管理情報プロトコル（CMIP）および他の X.500 バリエーションと同様に、Cisco Cloud Network Controller によって、MIT の階層構造内のオブジェクトの場所に応じて継承できるオブジェクトのプロパティとして管理可能な特性を示すことにより、管理対象リソースの制御が可能になります。

ツリーの各ノードは、管理対象オブジェクト（MO）またはオブジェクトのグループを表します。MO は、クラウドインフラストラクチャリソースの抽象化です。MO は、クラウドルー

ター、アダプターなどの具象オブジェクト、またはアプリケーションプロファイル、エンドポイントグループ、クラウドエンドポイントまたは障害などの論理オブジェクトを表すことができます。次の図は、MIT の概要について説明します。

図 2: Cisco ACI ポリシー管理情報モデルの概要



階層構造は、最上位（ルート）でポリシーユニバースから始まり、親と子ノードが含まれます。ツリー内の各ノードはMOで、クラウドインフラストラクチャ内の各オブジェクトには、オブジェクトを説明しツリー内の場所を検索する一意な識別名（DN）があります。

次の管理対象オブジェクトには、システムの動作を管理するポリシーが含まれます。

- テナントは、ポリシーのコンテナで、管理者はロールベースのアクセスコントロールを実行できます。システムにより、次の4種類のテナントが提供されます。
 - 管理者は、ユーザーのニーズに応じてユーザテナントを定義します。アプリケーション、データベース、Web サーバ、ネットワークアタッチドストレージ、仮想マシンなどのリソースの動作を管理するポリシーが含まれます。
 - システムは共通テナントを提供しますが、クラウドインフラストラクチャ管理者が設定できます。ファイアウォール、ロードバランサ、レイヤ4～レイヤ7サービス、侵入検知アプライアンスなど、すべてのテナントにアクセス可能なリソースの動作を管理するポリシーが含まれます。



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

- インフラストラクチャテナントは、システムによって提供されますが、クラウドインフラストラクチャの管理者が設定できます。インフラストラクチャリソースの動作を管理するポリシーが含まれます。また、ファブリックプロバイダーはリソースを1つ以上のユーザテナントに選択的に展開できます。インフラストラクチャテナントポリシーは、クラウドインフラストラクチャ管理者によって構成可能です。
- クラウドインフラポリシーを使用すると、Cisco Cloud Network Controller を設定するときに、オンプレミスおよびリージョン間接続を管理できます。詳細については、[Cisco Cloud Network Controller インストールガイド (Cisco Cloud Network Controller Installation Guide)] を参照してください。

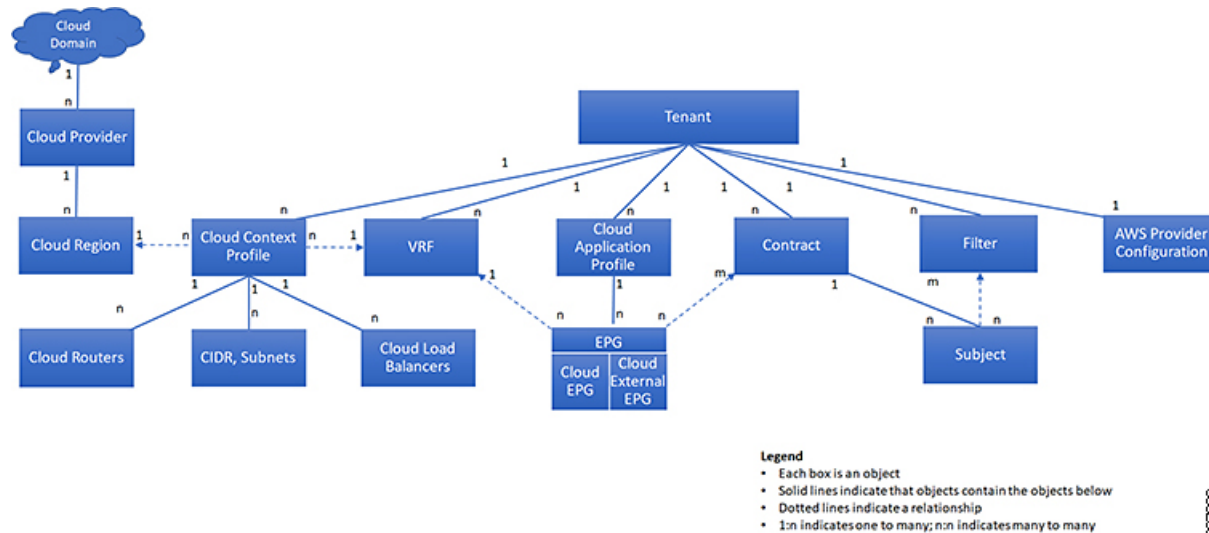
- クラウド インベントリは、GUI を使用してシステムのさまざまな側面を表示できるサービスです。たとえば、アプリケーションの側面から展開されたリージョンや、領域の側面から展開されたアプリケーションを表示できます。この情報は、クラウドリソースの計画とトラブルシューティングに使用できます。
- レイヤ4～レイヤ7のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムは動的に応答することができます。詳細については、[レイヤ4からレイヤ7サービスの展開](#)を参照してください。
- アクセス、認証、およびアカウントिंग（AAA）ポリシ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

階層型ポリシー モデルは、REST API インターフェイスとうまく適合します。呼び出されると、API は MIT 内のオブジェクトで読み取りまたは書き込みを行います。URL は、MIT 内のオブジェクトを識別する識別名に直接マッピングします。MIT 内のデータは、XML または JSON でエンコードされた自己完結型の構造化ツリーテキストドキュメントとして説明できます。

テナント

テナント (fvTenant) は、アプリケーションポリシーの論理コンテナで、管理者は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、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

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 Network Controller ソリューションには 2 つの CCR が必要です。

The **Cisco Catalyst 8000V** is used with the Cisco Cloud Network Controller. 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

以下は、Cisco Catalyst 8000V の更新情報です。

- [ライセンス \(7 ページ\)](#)

- [Throughput \(8 ページ\)](#)

ライセンス

Cisco Cloud Network Controller 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

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 Network Controller 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 Network Controller 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、ユーザーは 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支払うことができます。

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 Network Controller for AWS インストール ガイド \(Cisco Cloud Network Controller for AWS Installation Guide\)](#) の、「セットアップウィザードを使用した Cisco Cloud Network Controller 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 Network Controller 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

Cisco Cloud Network Controller 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

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 Network Controller でサポートされるデフォルトのスループットです。

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 Network Controller 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 コンピュート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 Network Controller 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

AWS EC2 インスタンス	CCR スループット	vCPU の数	メモリ
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
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

Private IP Address Support for Cisco Cloud Network Controller and CCR in AWS

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。To disable public IP to the Cisco Cloud Network Controller so that a private IP address is used for connectivity, see the *Deploying the Cisco Cloud Network Controller in AWS* procedure in the *Cisco Cloud Network Controller for AWS Installation Guide*.

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

- Cloud backbone for connecting to a Cisco Cloud Network Controller site of the same cloud provider, which is through AWS VPC Peering or Azure Vnet Peering

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

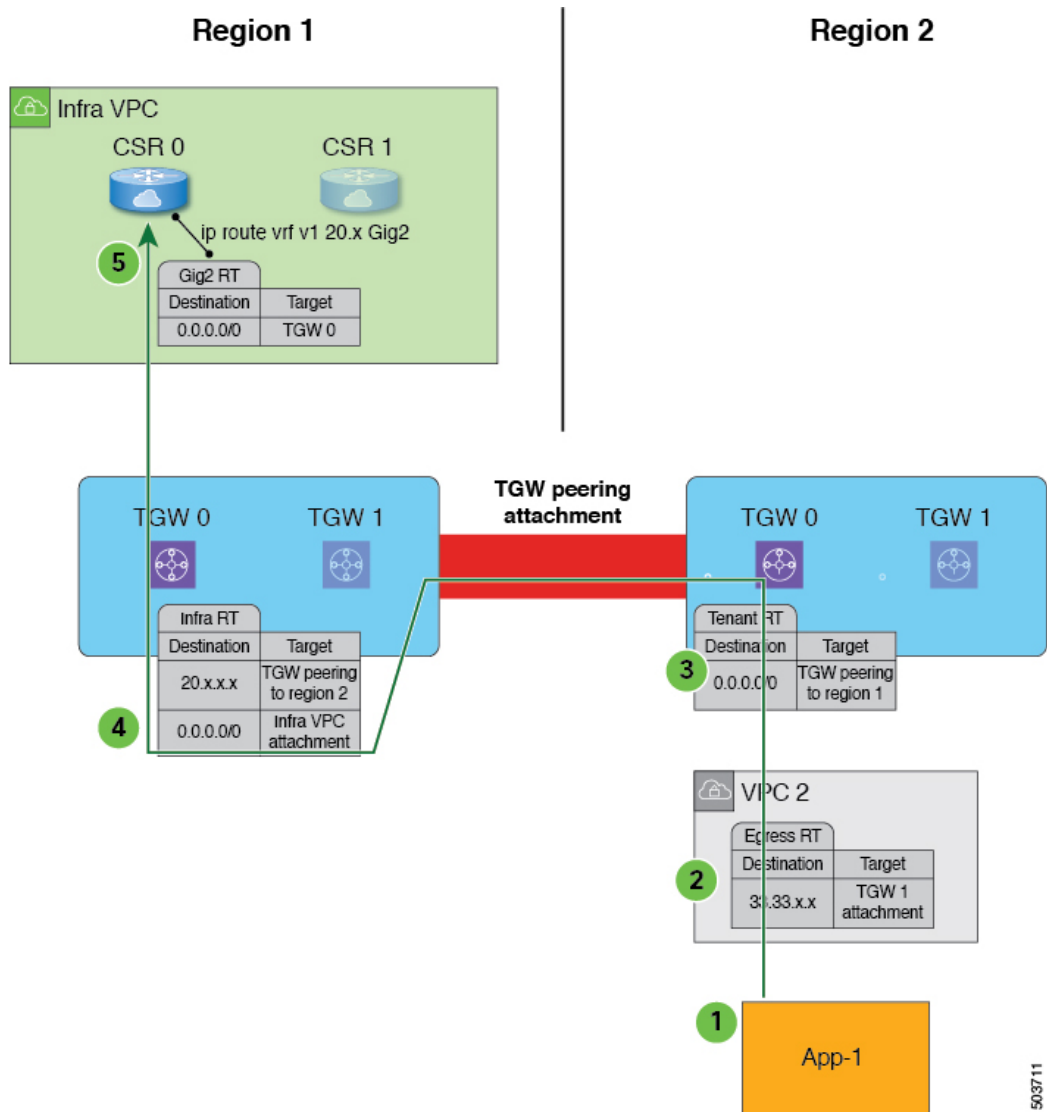
CCR のないリージョンからの外部サイトとの通信のサポートが利用可能です。This is accomplished by making use of the AWS Transit Gateway feature. When you enable the AWS Transit Gateway feature on Cisco Cloud Network Controller, you also enable peering between all managed regions on AWS. In this way, the AWS Transit Gateway peering feature allows the Cisco Cloud Network Controller to address the issue of communicating with external sites from regions without a CCR. 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、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。



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. 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. VPC2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

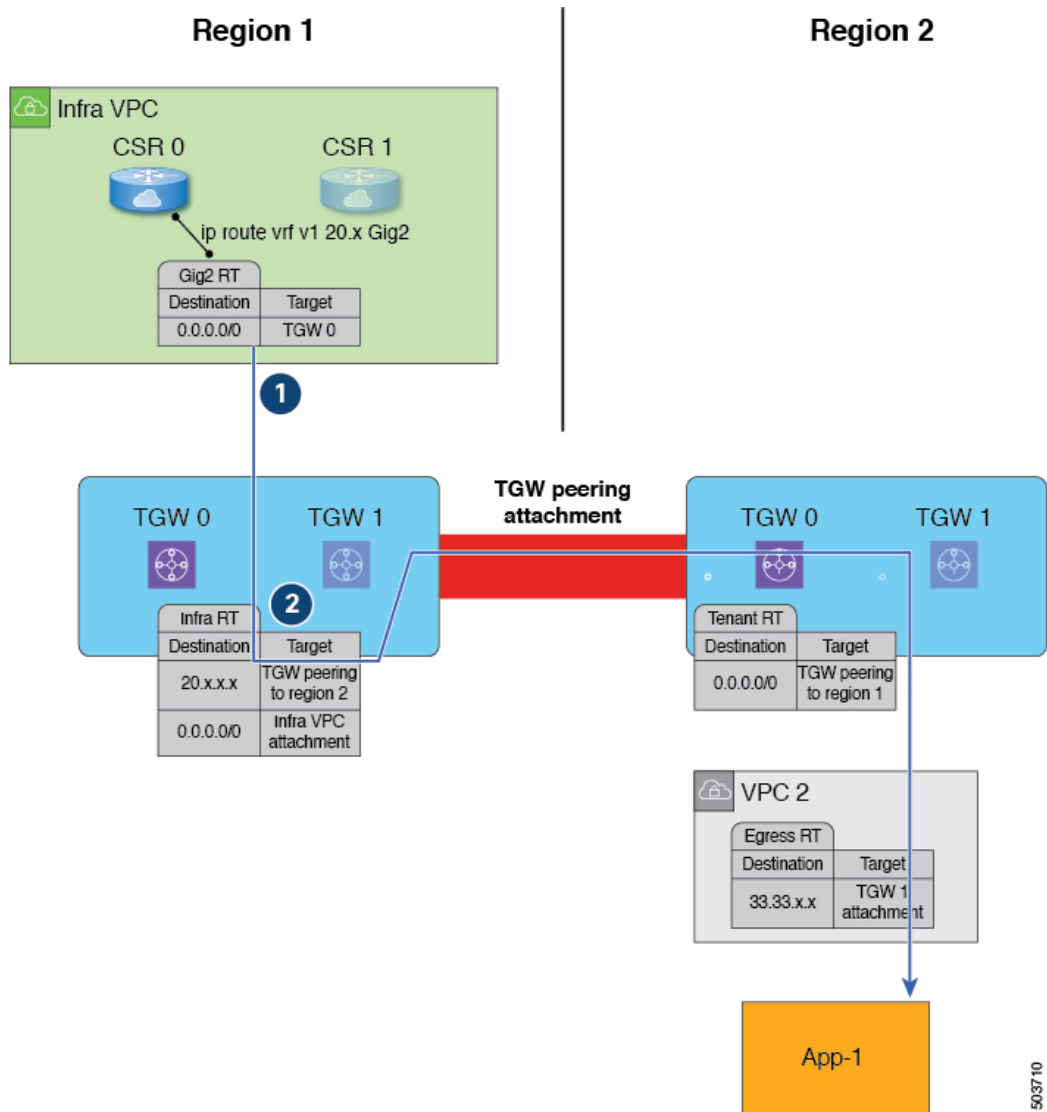
別のリージョン（例のシナリオではリージョン1）に移動します。使用される CCR のあるリージョンは、CCR がないリージョンへの地理的な近さに基づいて選択されます。

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。



503710

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. 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

Cisco Cloud Network Controller では、次の 2 種類のアベイラビリティ 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。

- **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。

The screenshot shows the 'Availability Zones' page with the 'Virtual Availability Zones' tab selected. The table below lists the virtual availability zones.

Name	Cloud Availability Zone	Application Management			Cloud Resources		
		Tenants	App. Profiles	EPGs	VPCs	Routers	Endpoints
af-south-1-1a region-af-south-1		N/A	N/A	N/A	N/A	0	N/A
af-south-1-1b region-af-south-1		N/A	N/A	N/A	N/A	0	N/A
ap-east-1-1a region-ap-east-1		N/A	N/A	N/A	N/A	0	N/A

- 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。

The screenshot shows the 'Availability Zones' page with the 'Cloud Availability Zones' tab selected. The table below lists the cloud availability zones.

Name	Tenants	Application Management			Cloud Resources		
		App. Profiles	EPGs	VPCs	Routers	Endpoints	
us-east-1a AWS > infra > us-east-1	N/A	N/A	N/A	N/A	0	N/A	
us-east-1b AWS > infra > us-east-1	N/A	N/A	N/A	N/A	0	N/A	
us-east-1c AWS > infra > us-east-1	N/A	N/A	N/A	N/A	0	N/A	

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

仮想アベイラビリティゾーンが構成されているデプロイがある場合は、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

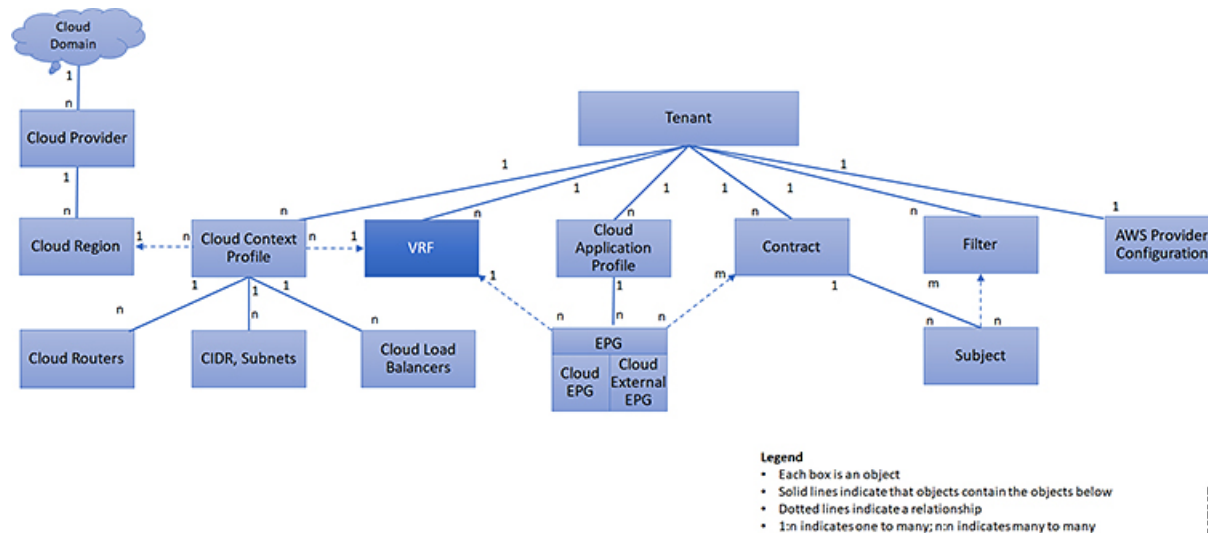
次に、複数のアベイラビリティゾーンをサポートに関するガイドラインと制限事項を示します。

- 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

A Virtual Routing and Forwarding (VRF) object (`f_vCtx`) or context is a tenant network (called a private network in the Cisco Cloud Network Controller GUI). 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

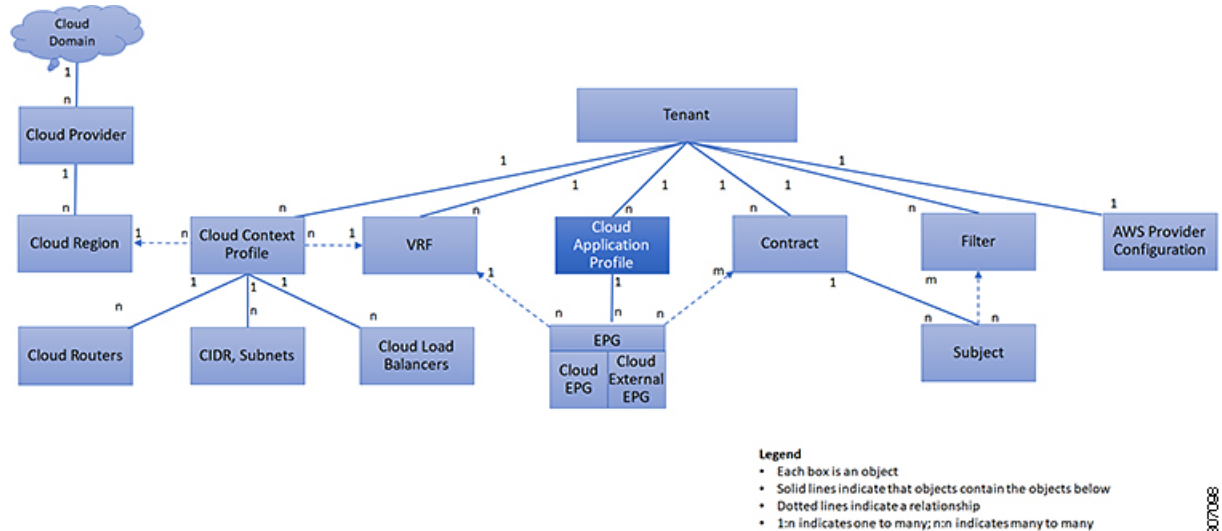


VRF は、レイヤ 3 のアドレスドメインを定義します。1つ以上のクラウドコンテキストプロファイルが VRF に関連付けられます。特定のリージョンの VRF に関連付けることができるクラウドコンテキストプロファイルは 1つだけです。レイヤ 3 ドメイン内のすべてのエンドポイントが一意の IP アドレスを持っている必要があります。なぜなら、ポリシーで許可されている場合にこれらのデバイス間でパケットを直接転送できるためです。テナントには、複数の VRF を含めることができます。管理者が論理デバイスを作成した後、管理者はデバイスクラスタの選択基準ポリシーを提供する論理デバイスの VRF を作成できま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

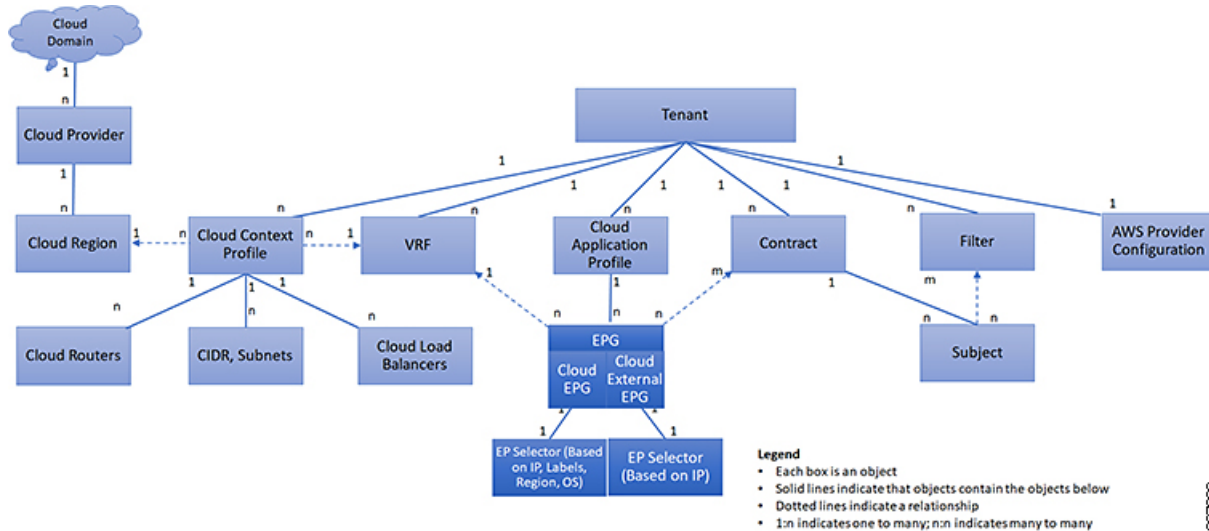
クラウド EPG は次のいずれかに従って組織化できます。

- 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によって、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、動的または静的にできます。

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。

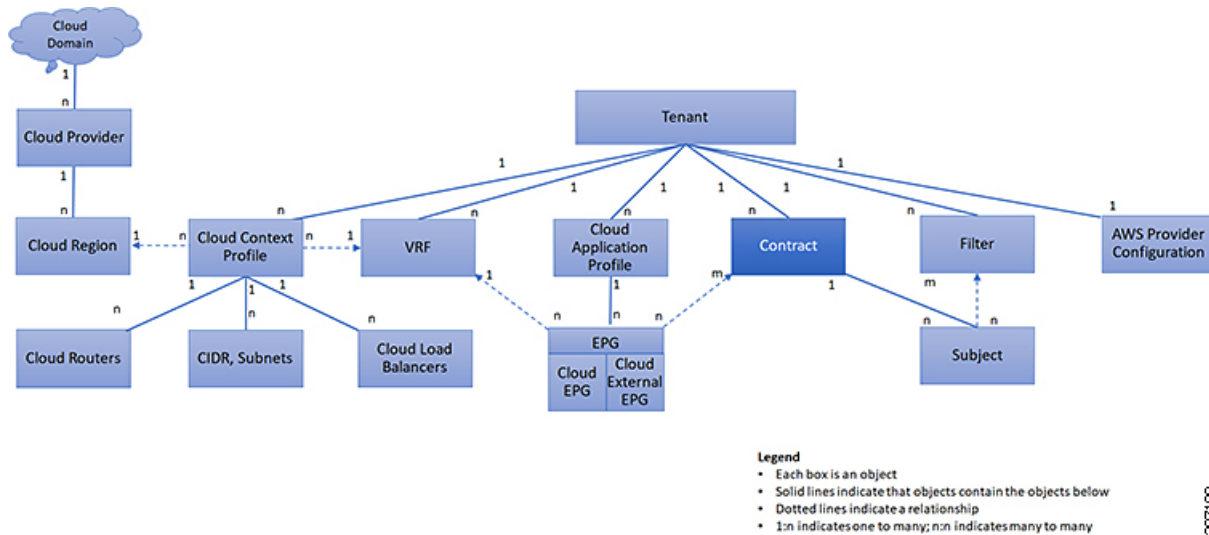
クラウド インフラストラクチャへの WAN ルータ接続は、スタティック クラウド EPG を使用する設定の 1 つの例です。クラウド インフラストラクチャへの WAN ルータ接続を設定するには、関連付けられている WAN サブネット内のエンドポイントを含む cloudExtEPg クラウド EPG を管理者が設定します。クラウド インフラストラクチャは、エンドポイントの接続ライフサイクルが経過する間に、検出プロセスを通してクラウド EPG のエンドポイントについて学習します。エンドポイントを学習すると、クラウド インフラストラクチャは、それに基づいて cloudExtEPg クラウド EPG 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 Network Controller はエンドポイントセレクタを使用して、エンドポイントをクラウド EPG に割り当てます。エンドポイントセレクタは、基本的に言って、Cisco ACI によって管理される 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。

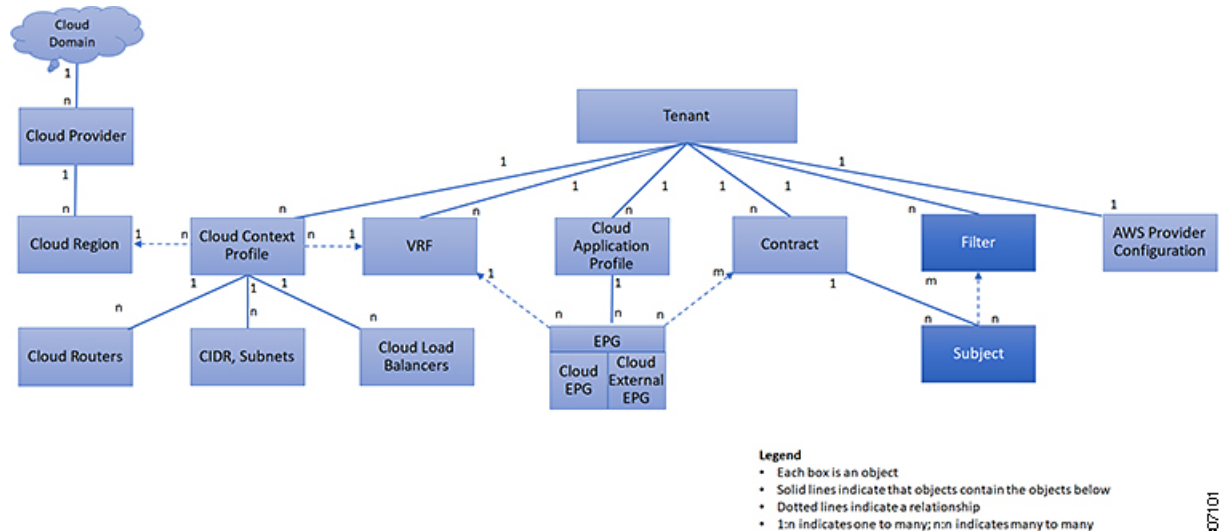


(注) 1つのクラウド EPG で同じコントラクトを指定および使用できます。クラウド EPG は複数のコントラクトを同時に指定および使用することもできます。

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 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 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に関連付け
- 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"> • routerUsername • routerPassword • routerThroughput • routerLicenseToken • routeDataInterfacePublicIP • routerMgmtInterfacePublicIP

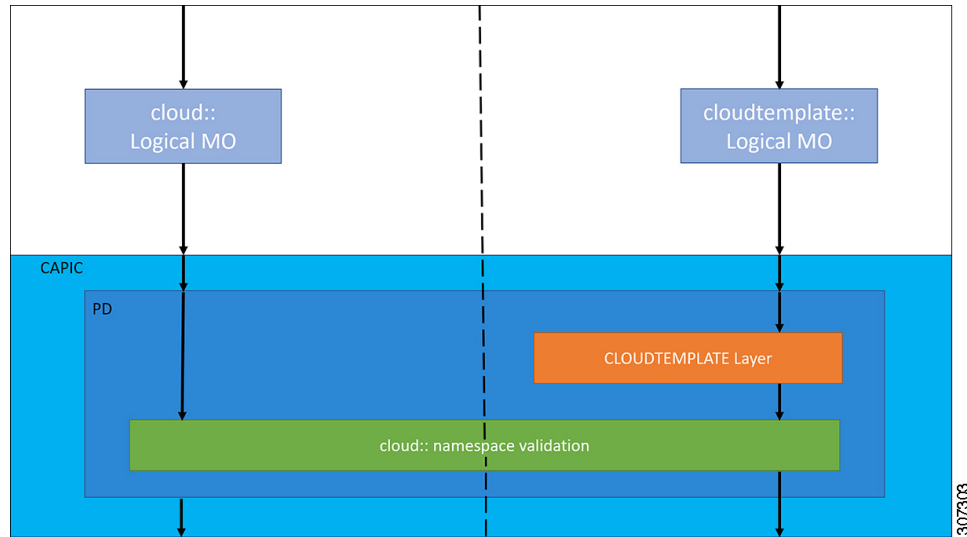
MO	目的
cloudtemplateIntNetwork	クラウドルータを展開する場所を指定するリージョンのリストが含まれます。各リージョンは、cloudRegionName子 MO を介してキャプチャされます。
cloudtemplateExtNetwork	クラウド外部のインフラ ネットワーク設定入力が含まれます。 クラウドルータが外部ネットワーキング用に設定されているリージョンのリストが含まれます。 各リージョンは、cloudRegionName子 MO を介してキャプチャされます。
cloudtemplateVpnNetwork	ACI オンプレミス サイトまたは別の Cisco Cloud 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。

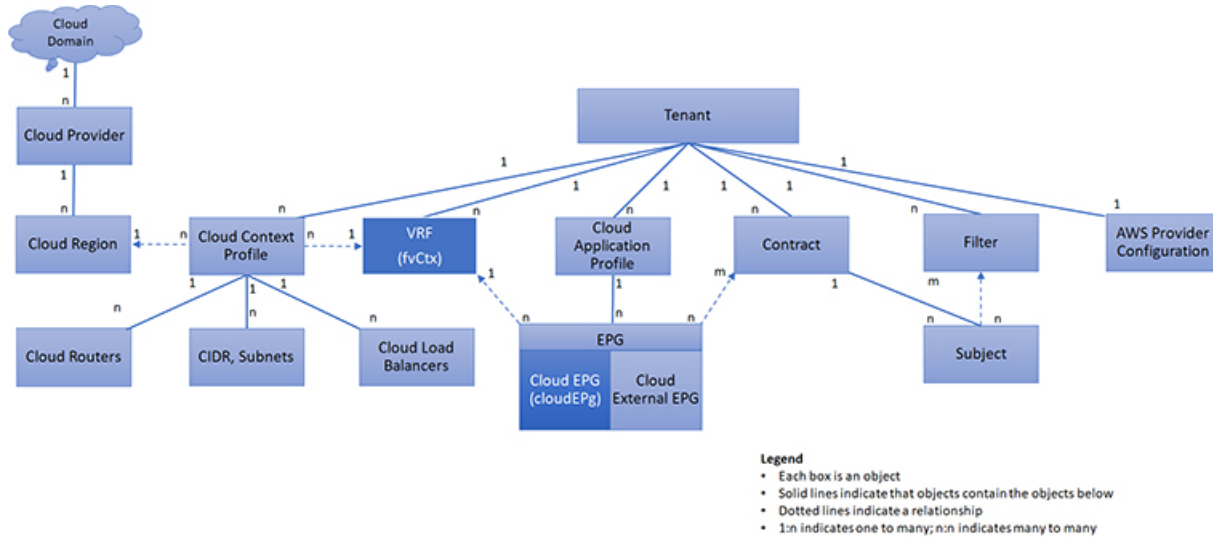
管理対象オブジェクトの関係とポリシー解決

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、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 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。