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。

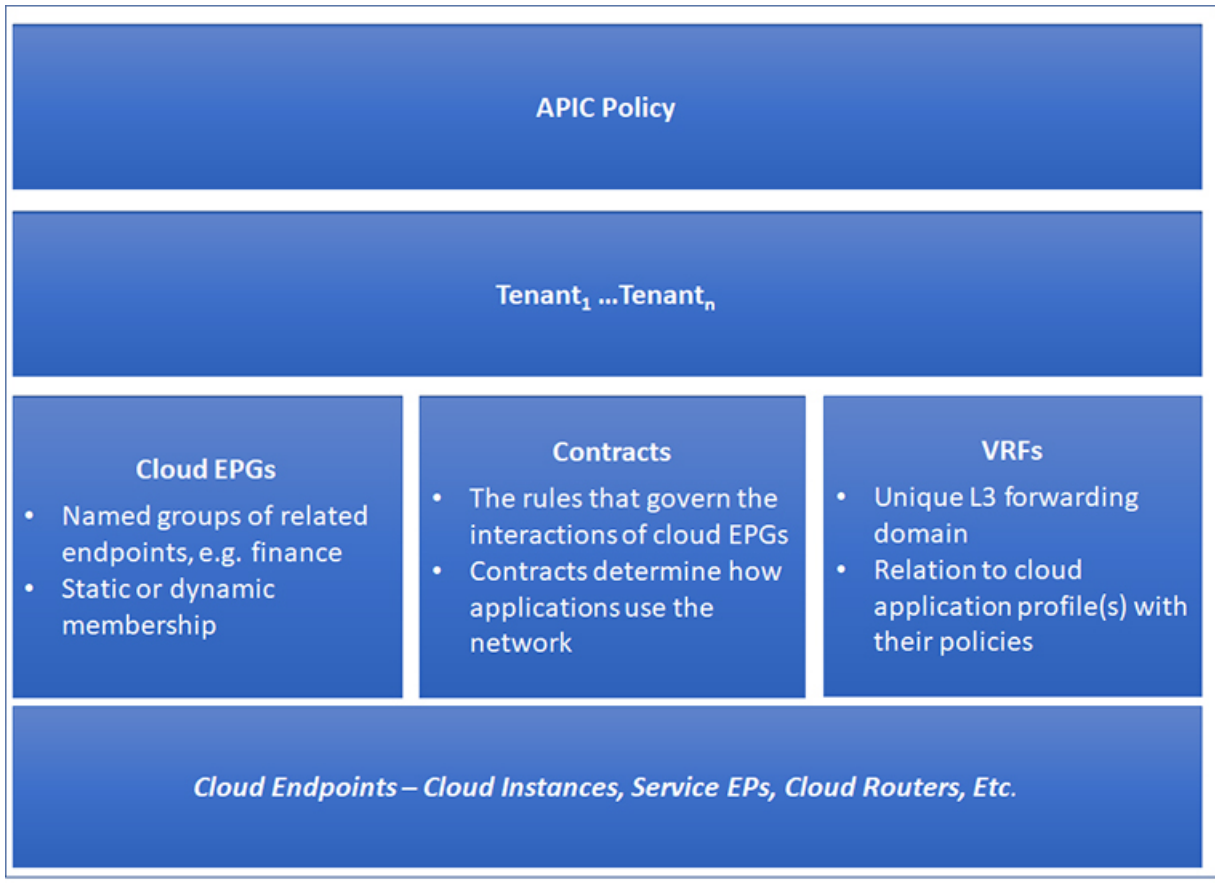
- モデル主導のアーキテクチャとして、ソフトウェアはシステム（モデル）の管理および動作状態の完全表記を維持します。モデルはクラウドインフラストラクチャ、サービス、システム動作、およびネットワークに接続された仮想デバイスに均一に適用されます。
- 論理ドメインと具象ドメインが区別されます。論理的な設定は、使用可能なリソースに関連するポリシーを適用することで具体的な設定にレンダリングされます。具体的なエンティティに対して構成は行われません。具象エンティティは、Cisco Cloud ポリシー モデルの変更の副作用として明示的に設定されます。
- システムは、新しいエンドポイントを含めるようにポリシ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

論理コンストラクト

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。

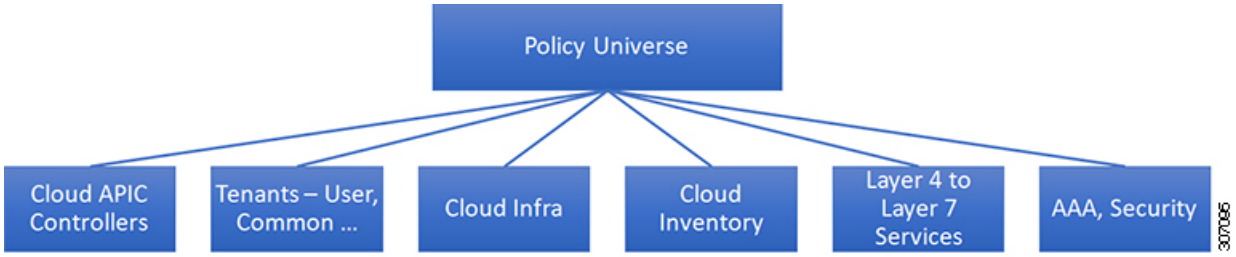
Cisco ACI ポリシー管理情報モデル

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。

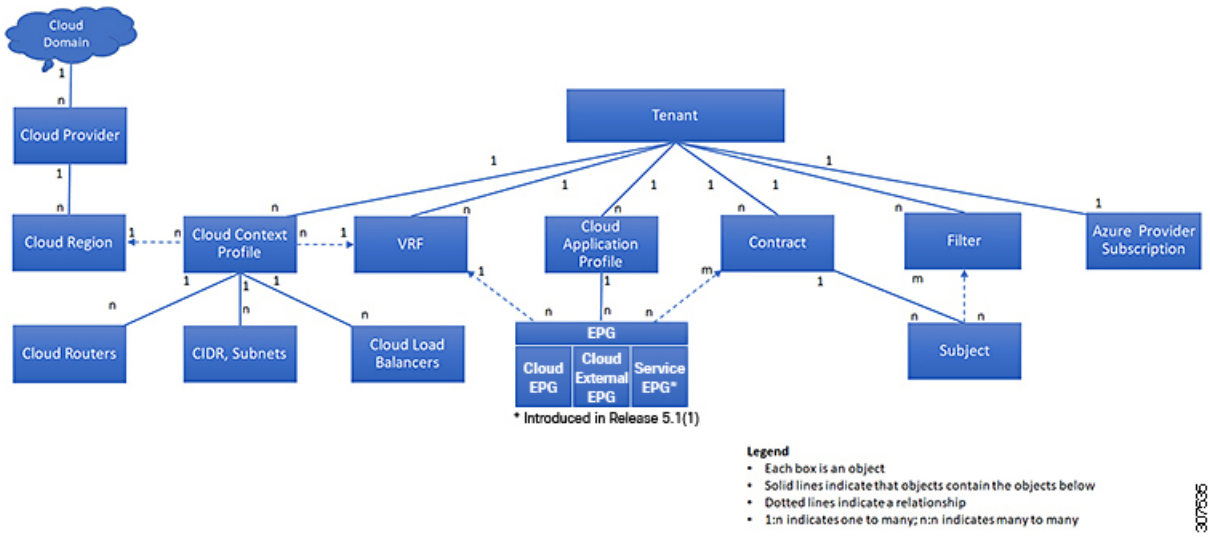
- クラウド インベントリは、GUI を使用してシステムのさまざまな側面を表示できるサービスです。たとえば、アプリケーションの側面から展開されたリージョンや、領域の側面から展開されたアプリケーションを表示できます。この情報は、クラウド リソースの計画とトラブルシューティングに使用できます。
- レイヤ 4 ～ レイヤ 7 のサービス統合ライフサイクルの自動化フレームワークにより、サービスがオンラインまたはオフラインになったときにシステムは動的に応答することができます。詳細については、レイヤ 4 から レイヤ 7 サービスの展開を参照してください。
- アクセス、認証、およびアカウンティング（AAA）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、仮想ルート転送（VRF）インスタンス、クラウド コンテキスト プロファイル、Azure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。クラウド コンテキスト プロファイルは、VRF、テナント、およびリージョンとともに、Azure のリソースグループを表します。VNET は、VRF 名に基づいてリソースグループ内に作成されます。

テナントはアプリケーション ポリシーの論理コンテナです。クラウド インフラストラクチャには、複数のテナントを含めることができます。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。

テナント、ID、およびサブスクリプションについて

AzureにはActive Directory構造があります。最上位レベルの構造は組織であり、その下にディレクトリ（Azureテナントとも呼ばれます）があります。ディレクトリ内には、1つ以上のAzureサブスクリプションを設定できます。

特定のAzureコンポーネント間の関係は次のとおりです。

テナントサブスクリプションリソースグループリソース ＞＞＞

それぞれの説明は次のとおりです。

- 1つのテナントは複数のサブスクリプションを持つことができますが、各サブスクリプションは1つのテナントにのみ属することができます。
- 1 つのサブスクリプションに複数のリソースグループを含めることができますが、各リソースグループは 1 つのサブスクリプションにのみ属することができます。
- 1 つのリソースグループは複数のリソースを持つことができますが、各リソースは 1 つのサブスクリプションにのみ属することができます。

次のセクションでは、これらのコンポーネントについて詳しく説明します。

- Azure とコンポーネントのマッピングCloud APIC （6 ページ）
- Azureサブスクリプションについて （7 ページ）
- テナントとアイデンティティについて （7 ページ）

Azure とコンポーネントのマッピングCloud APIC

Cloud APIC では、各 Azure リソース グループは 1 つのテナントにマッピングされ、1 つのテナントが複数の Azure リソースグループを持つことができます。Cloud APICCloud APIC

特定のコンポーネント間の関係は次のとおりです。Cloud APIC

テナントVRFリージョン ＞＞

でVRFを作成すると、新しいリソースグループもAzureに作成されます。Cloud APIC

Azureサブスクリプションについて

Azureサブスクリプションは、Azureクラウドサービスの支払いに使用されます。Azureサブスクリプションには、Azure Active Directory（Azure AD）との信頼関係があり、Azure ADを使用してユーザ、サービス、およびデバイスを認証します。複数のサブスクリプションは同じAzure ADを信頼できますが、各サブスクリプションは1つのAzure ADのみを信頼できます。

Azureでは、同じAzureサブスクリプションIDを複数のACIファブリックテナントに使用できます。これは、1つのAzureサブスクリプションを使用してインフラテナントを設定し、同じサブスクリプションで複数のユーザテナントを設定できることを意味します。ACIテナントはAzureサブスクリプションに関連付けられています。

テナントとアイデンティティについて

Azureおよびで使用できるさまざまなタイプのテナントとIDを次に示します。Cloud APIC

（注） リリース5.2（1）より前のリリースでは、管理対象アイデンティティのみがインフラテナントのアクセスタイプとしてサポートされ、管理対象アイデンティティとサービスプリンシパルの両方がユーザテナントのアクセスタイプとしてサポートされていました。

リリース5.2（1）以降、マネージドアイデンティティとサービスプリンシパルの両方が、インフラテナントとユーザテナントのアクセスタイプとしてサポートされるようになりました。

マネージドアイデンティティ

マネージドアイデンティティは、Azure AD認証をサポートするリソースに接続するときに使用するアプリケーションのアイデンティティを提供します。アプリケーションは管理対象IDを使用してAzure ADトークンを取得できます。たとえば、開発者が安全な方法でクレデンシャルを保存したり、ストレージアカウントにアクセスしたりするために、アプリケーションでマネージドアイデンティティを使用してAzure KeyVaultなどのリソースにアクセスできます。
https://docs.microsoft.com/en-us/azure/key-vault/general/overview

管理対象IDを使用する利点は次のとおりです。

- クレデンシャルにはアクセスできないため、クレデンシャルを管理する必要はありません。
- マネージドIDを使用して、独自のアプリケーションを含むAzure AD認証をサポートする任意のリソースを認証できます。
- マネージドIDは追加コストなしで使用できます。

Azureの管理対象アイデンティティの詳細については、以下を参照してください。

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

管理対象アイデンティティを使用してでテナントを設定する場合は、Azureポータルとで次の設定を行います。Cloud APICCloud APIC

1. Azureポータルで、仮想マシンのロール割り当てを追加します。このオプションは、Azureサブスクリプションが（同じ組織の）同じAzureディレクトリにある場合に使用します。

（注） Azureサブスクリプションが異なるディレクトリにあり、マネージドIDを使用してテナントを設定する場合は、Azureコンソールに移動し、各サブスクリプションをクリックして同じAzureディレクトリの下にサブスクリプションを移動できます。これは、（異なるサブスクリプションを含む）ディレクトリが同じ親組織の子である場合にのみ実行できます。

2. Cloud APIC では、Cloud APIC でテナントを構成するときに **[管理対象アイデンティティ（Managed Identity）]** オプションを選択します。

これらの構成の詳細については、Cisco Cloud APIC GUIを使用したテナントの作成 を参照してください。

サービス プリンシパル（Service Principal）

Azureサービスプリンシパルは、Azureリソースにアクセスするためのアプリケーション、ホステッドサービス、および自動化ツールで使用するために作成されたIDです。異なるサブスクリプションでテナントを設定する場合は、サービスプリンシパルIDを使用します。サブスクリプションが同じ組織内の異なる Azure ディレクトリ（Azure テナント）にあるか、サブスクリプションが異なる組織にある可能性があります。

サービスプリンシパルを使用してでテナントを設定する場合は、Azureポータルとで次の設定を行います。Cloud APICCloud APIC

1. Azureポータルで、**アプリケーション**のロール割り当てを追加します。この場合、クラウドリソースは特定のアプリケーションを介して管理されます。

2. では、テナントを設定するときに **[サービスプリンシパル（Service Principal）]** オプションを選択します。Cloud APICCloud APICこのページに入力するサブスクリプションは、同じ組織内の異なるAzureディレクトリ（Azureテナント）に配置することも、異なる組織に配置することもできます。

これらの構成の詳細については、Cisco Cloud APIC GUIを使用したテナントの作成 を参照してください。

共有テナント

Azureサブスクリプションを上記の2つの方法のいずれかにすでに関連付けており、そのサブスクリプションにさらにテナントを作成する場合は、このオプションを選択します。

でテナントを共有テナントとして設定する場合は、Azureポータルとで次の設定を行います。Cloud APICCloud APIC

1. 上記の2つの方法のいずれかでAzureサブスクリプションをすでに関連付けているため、Azureで共有テナント専用の設定を行う必要はありません。共有テナントでは、既存のサブスクリプションにさらにテナントを作成します。
2. では、テナントを設定するときに[共有（Shared）]オプションを選択します。Cloud APICCloud APIC

これらの構成の詳細については、Cisco Cloud APIC GUIを使用したテナントの作成 を参照してください。

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。

- CIDR
- VRF
- EPG
- [Regions]
- 仮想ネットワーク
- ルータ
- エンドポイント

CCR

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

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

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

Cisco Catalyst 8000V について

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

ライセンシング

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

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

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

BYOL ライセンス モデル

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

- ティアベースの Cisco Catalyst 8000V ライセンスの 1 つにサブスクライブする手順については、Cisco Catalyst 8000V Edge ソフトウェアを参照してください。
- 層に基づくさまざまなスループットの詳細については、スループット （11 ページ） を参照してください。

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

PAYGライセンス モデル

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

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

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

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

スループット

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

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

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

1. 所有ライセンス持ち込み（BYOL）

このモデルでは、Cisco Catalyst 8000V は、ティアベース（T0/T1/T2/T3）のスループット オプションをサポートしています。次の表に、シスコ クラウド サービス ルータ 8000v のさまざまなルータ スループット設定に必要な Azure VM のサイズを示します。

CCR スループット	Azure VMサイズ
T0（最大 15M のスループット）	DS3_v2
T1（最大 100M のスループット）	DS3_v2
T2（最大 1G のスループット）	DS3_v2
T3（最大 10G のスループット）	F16s_v2

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

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

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

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

2. ペイアズユーゴー（PAYG）ライセンス モデル

このモデル向けに、Cisco Cloud APIC は Cisco Catalyst 8000V 仮想ルータを使用し、クラウド ネットワーキングのニーズに合わせて Azuru 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、Azuru 上の Cisco Cloud APIC でサポートされているクラウド インスタンス タイプを示しています。

Azure 上の VmName	メモリ	vCPU の数	ネットワーク帯域
DS3V2	14GiB	4	最大 3 ギガビット
DS4V2	28GiB	8	最大 6 ギガビット
F16SV2	32GiB	16	最大 12.5 ギガビット
F32SV2	64GiB	32	最大 16 ギガビット

CCR の数を変更する

リリース 5.1(2) 以降、リージョンごとにサポートされる CCR の最大数は 4 から 8 に増加しました。これらの手順では、CCR の数を 4 より増やすか、必要に応じて CCR の数を 4 に戻す手順を示します。

次の点に注意してください。

- 2 ～ 4 CCR の範囲で CCR の数を増減する場合は、これらの手順を使用する必要はありません。これらの手順は、CCR の数を 4 以上に増やす場合、または 5 ～ 8 の範囲から CCR の数を 減らす場合にのみ使用してください。
- CCR の数を変更すると、最大 30 分間、トラフィックに影響を与える可能性があります。

ステップ 1 すべてのインフラ クラウド コンテキスト プロファイルで、ローカル レベルで Azure VNet ピアリングを無効にします。

a) **[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ページに移動します。

[アプリケーション管理（Application Management）]> > **[クラウド コンテキスト プロファイル（Cloud Context Profiles）]**

b) インフラ クラウド コンテキスト プロファイルの **[名前（Name）]** 列の下にあるリンクをクリックします。

このクラウドコンテキスト プロファイルの詳細を示すパネルが、ウィンドウの右側からスライドして表示されます。

c) [詳細（Details）] アイコンをクリックします（）。

このクラウド コンテキスト プロファイルの詳細情報を提供する別のウィンドウが表示されます。

d) ウィンドウの右上隅の鉛筆アイコンをクリックします。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

e) **[ハブ ネットワーク ピアリング（Hub Network Peering）]** フィールドのチェックを外します（無効にします）。

f) 設定が終わったら [Save] をクリックします。

これらの手順を繰り返して、すべてのインフラ クラウド コンテキスト プロファイルで Azure VNet ピアリングを無効にします。

ステップ 2 CCR の数を 4 より増やす場合は、必要に応じて、追加の CCR 用にサブネット プールを追加します。

CCR の数を 4 より大きくしようとするとエラー メッセージが表示され、システムは追加のサブネット プールが必要であると判断します。

a) Cloud APIC GUI で、インテント アイコン（）をクリックし、**[cAPIC セットアップ（cAPIC Setup）]** を選択します。

b) **[リージョン管理（Region Management）]** エリアで、**[設定の編集（Edit Configuration）]** をクリックします。

c) **[管理するリージョン（Regions to Manage）]** ウィンドウで、**[次へ（Next）]** をクリックします。

[一般接続（General Connectivity）] ウィンドウが表示されます。

d) **[全般（General）]** 領域の **[クラウド ルータのサブネット プール（Subnet Pools for Cloud Routers）]** フィールドで、CCR のサブネットを追加する場合は、**[クラウド ルータのサブネット プールの追加（Add Subnet Pool for Cloud Routers）]** をクリックします。

このサブネットプールのアドレスは、クラウドAPICで管理する必要がある追加のリージョンのリージョン間接続に使用されます。これはマスク /24 の有効な Ipv4 サブネットである必要があります。

ステップ 3 CCR の数を 4 より増やすか、CCR の数を 5 ～ 8 の範囲から減らします。

a) クラウド APIC GUI で、[インターネット（Intent）]アイコン（）をクリックし、**[cAPIC セットアップ（cAPIC Setup）]** を選択します。

b) **[リージョン管理（Region Management）]** エリアで、**[設定の編集（Edit Configuration）]** をクリックします。

[管理するリージョン（Regions to Manage）] ウィンドウが表示されます。

c) **[次へ（Next）]** をクリックして、以前に選択したリージョンと CCR をそのままにします。

[一般接続（General Connectivity）] ウィンドウが表示されます。

d) **[一般接続（General Connectivity）]** ウィンドウで **[CCR]** エリアを見つけ、**[リージョンごとのルータ数（Number of Routers Per Region）]** フィールドで、必要な変更を加えて CCR の数を増減します。

e) **[次へ（Next）]** をクリックし、次のページに必要な情報を入力して、**[保存して続行（Save and Continue）]** をクリックします。

CCR の追加または削除プロセスは、およそ 30 分ほどかかる場合があります。

ステップ 4 すべてのインフラ クラウド コンテキスト プロファイルで、ローカル レベルで Azure VNet ピアリングを再度有効にします。

a) **[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ページに移動します。

[アプリケーション管理（Application Management）]> > [クラウド コンテキスト プロファイル（Cloud Context Profiles）]

b) インフラ クラウド コンテキスト プロファイルの **[名前（Name）]** 列の下にあるリンクをクリックします。

このクラウド コンテキスト プロファイルの詳細を示すパネルが、ウィンドウの右側からスライドして表示されます。

c) [詳細（Details）] アイコンをクリックします（）。

このクラウド コンテキスト プロファイルの詳細情報を提供する別のウィンドウが表示されます。

d) ウィンドウの右上隅の鉛筆アイコンをクリックします。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

e) **[ハブ ネットワーク ピアリング（Hub Network Peering）]** フィールドをチェック（有効）します。

f) 設定が終わったら [Save] をクリックします。

これらの手順を繰り返して、すべてのインフラ クラウド コンテキスト プロファイルで Azure VNet ピアリングを有効にします。

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

リリース 5.1(2) 以前、Cisco Cloud Router (CCR) インターフェイスは、Cloud APIC によってパブリックおよびプライベート IP アドレス両方を割り当てられていました。リリース 5.1(2) 以降、

CCR インターフェイスはプライベート IP アドレスのみが割り当てられ、パブリック IP アドレスを CCR インターフェイスに割り当てることはオプションとなりました。プライベート IP アドレスは、常に CCR のすべてのインターフェイスに割り当てられます。CCR の GigabitEthernet1 のプライベート IP は、BGP および OSPF ルータ ID として使用されます。CCR にプライベート IP アドレスが割り当てられている場合、エクスプレス ルートを介したオンプレミスの ACI サイトを持つ Hcloud がサポートされます。CCR のプライベート IP を有効にするには、Cisco Cloud APIC GUI を使用したリージョンの管理（クラウド テンプレートの設定） の手順を参照してください。

リリース 5.1(2) 以前、クラウド APIC の管理インターフェイスは、パブリック IP アドレスおよびプライベート IP アドレスが割り当てられていました。リリース 5.1(2) 以降、プライベート IP アドレスは Cisco Cloud APIC 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。Cloud APIC のプライベート IP を有効にするには、『*Azure* 内での *Cisco Cloud APIC* 展開インストール ガイド』の「*Azure* 内での *Cloud APIC* の展開」手順を参照してください。

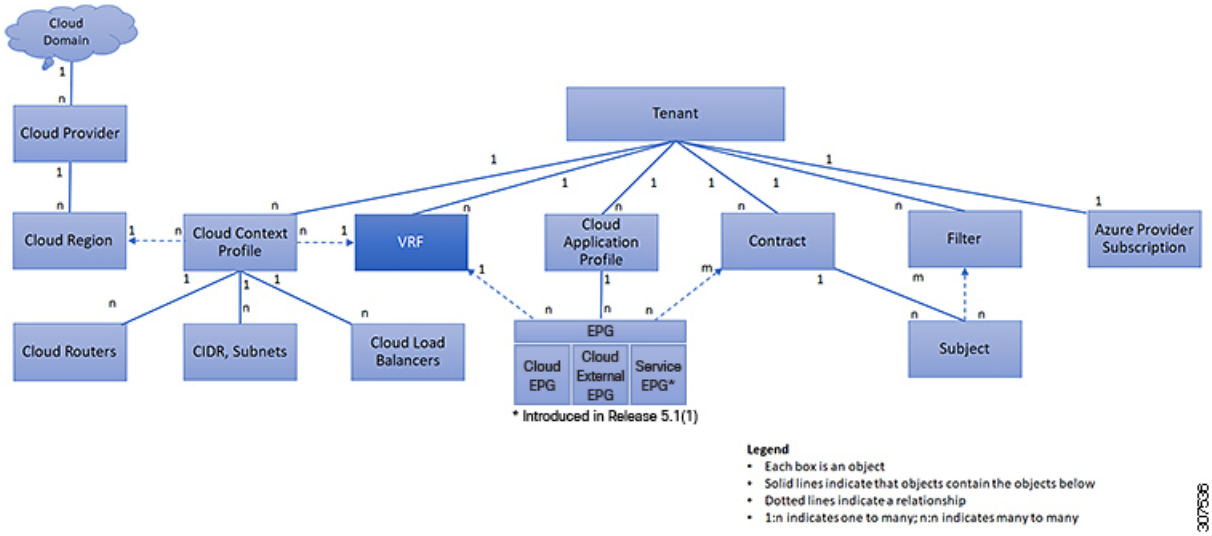
[プライベート IP アドレスを使用した CCR の制限（Restrictions for CCR with private IP address）] :

- サイト間通信には IPsec が必要なため、マルチクラウドの展開はサポートされていません。

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 ではVRF）と呼ばれます。テナントには、複数の VRF を含めることができます。VRF は、一意のレイヤ 3 フォワーディングおよびアプリケーション ポリシー ドメインです。次の図は、管理情報ツリー（MIT）内の VRF の場所とテナントの他のオブジェクトとの関係を示します。

図 *4 : VRF*



VRF は、レイヤ 3 のアドレス ドメインを定義します。1 つ以上のクラウド コンテキスト プロファイルが VRF に関連付けられます。特定のリージョンの VRF に関連付けることができるクラウド コンテキスト プロファイルは 1 つだけです。レイヤ 3 ドメイン内のすべてのエンドポイントが一意の IP アドレスを持っている必要があります。なぜなら、ポリシーで許可されている場合にこれらのデバイス間でパケットを直接転送できるためです。テナントには、複数の VRF が含まれる場合があります。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。

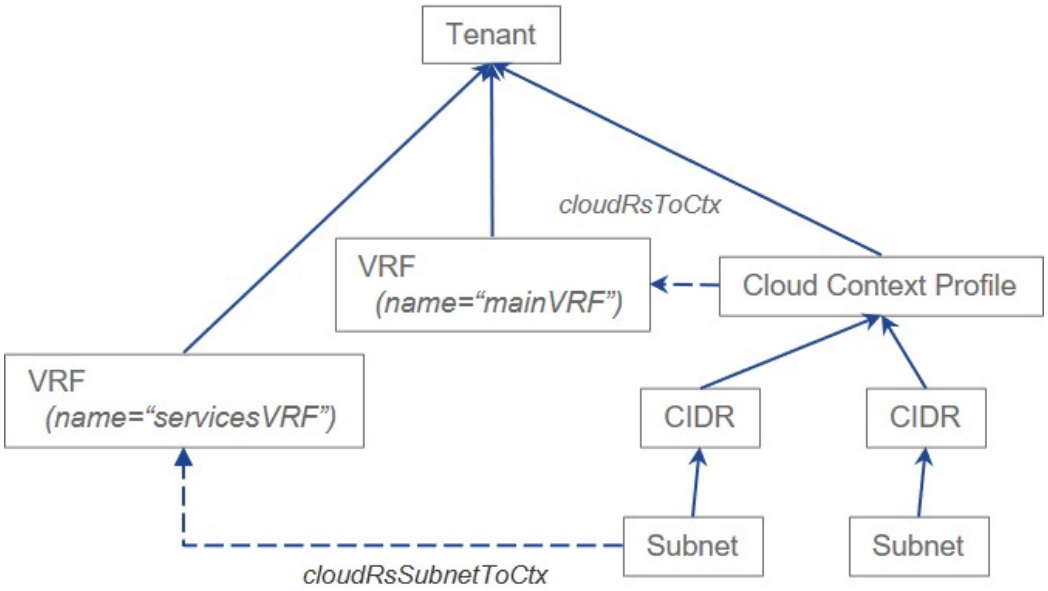
単一 VNet での複数の VRF のサポート

単一 VNet の下で複数の VRF がサポートされるようになりました。

複数の VRF に切り分けることができるインフラ（ハブ）VNet（インフラ テナントの `cloudCtxProfile`）を持つことができます。それぞれの VRF のすべてのサブネットは、VRF 分離のためにクラウド内に個別のルート テーブルを持ちます。

また、インフラ VNet を超えて複数の VRF を分割して、単一の VNet に複数の VRF が存在する場合、任意の VNet を同じテナントの下の複数の VRF に分割できるようにすることもできます。これは、クラウド サービス アクセスなど、特定の VNet 内に複数のネットワーク（VRF）を分割し、クラウドの VNet 内の各 VRF に固有のルート テーブルを用意することで個別のルーティングを行う必要がある場合に役立ちます。

次の図は、同じテナント（VNet）の下に複数の VRF がある管理対象オブジェクト（MO）関係ツリーの例を示しています。



この例では、同じテナント（VNet）の下に 2 つの VRF が存在します。

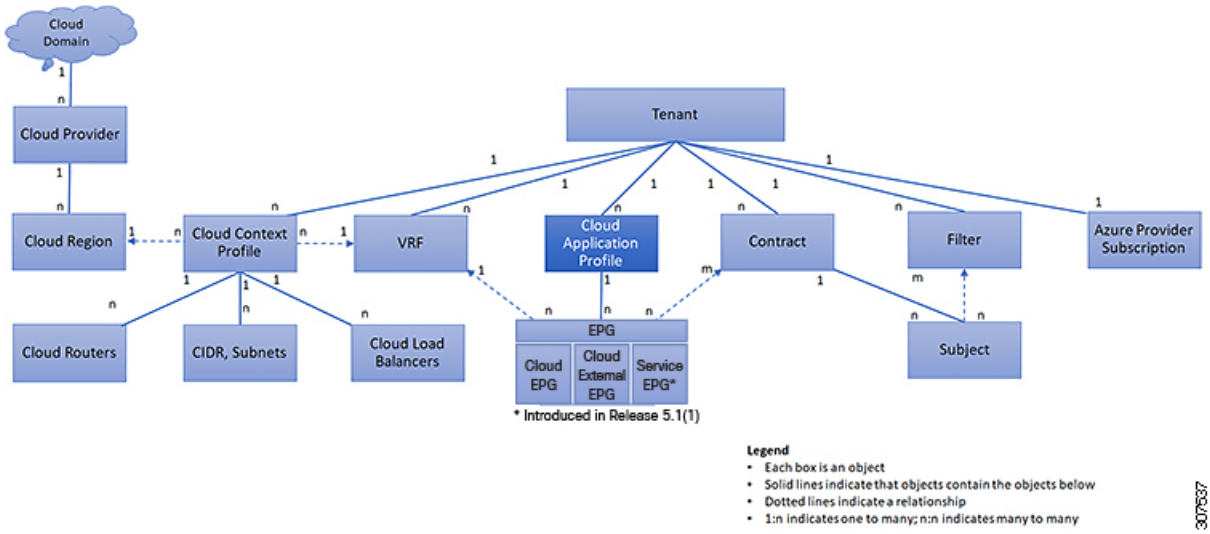
- `mainVRF` という名前のプライマリ VRF
- `servicesVRF` という名前のセカンダリ VRF

2 番目の CIDR ブロックとサブネットは、同じテナント（VNet）の下の同じクラウド コンテキスト プロファイルに存在しますが、その 2 番目の CIDR ブロックとサブネットは、その同じ VNet 内のセカンダリ VRF に関連付けられています。

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。

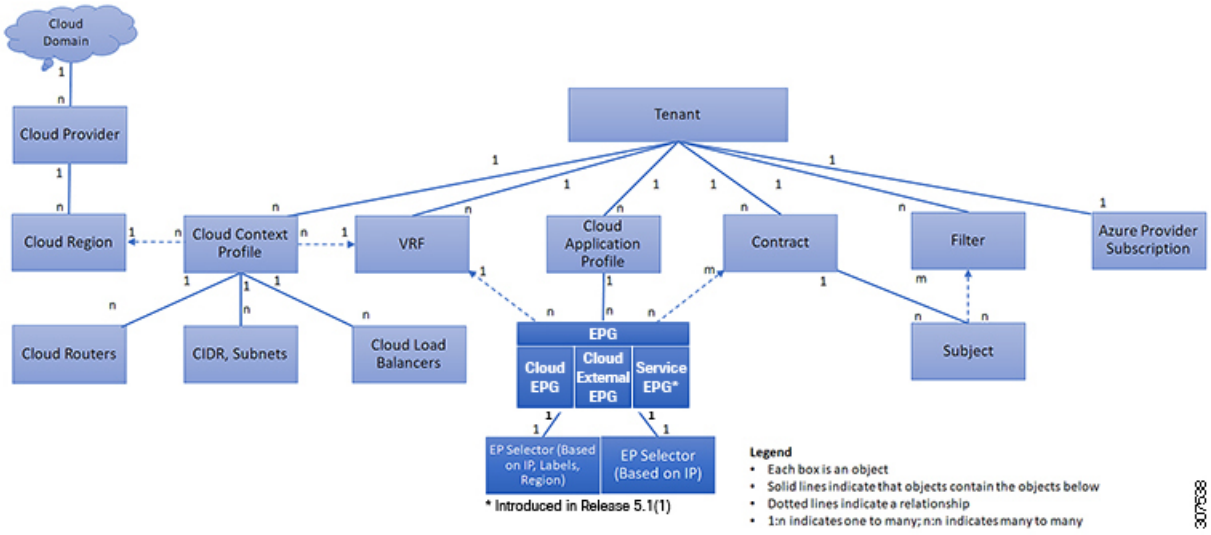
クラウド EPG は次のいずれかに従って組織化できます。

- 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 サービスエンドポイント グループ（`cloudSvcEPg`）：リリース 5.1(2) で導入されました。詳細については、「クラウド サービスエンドポイント グループ （19 ページ）」を参照してください。

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、`cloudEPg` クラウド EPG Web サーバとの通信が始まる前に、そのクライアント エンドポイントにポリシーを適用します。クライアント サーバ TCP セッションが終わり、クライアントとサーバの間の通信が終了すると、その WAN エンドポイントはもうクラウド インフラストラクチャ内に存在しません。

Cisco Cloud 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、Cisco ACI によって管理される Azure VNET 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。

クラウド サービスエンドポイント グループ

リリース 5.1(2) で導入されたクラウド サービス EPG は、クラウド ネイティブまたはサードパーティのサービスインスタンスまたはエンドポイントのコレクションを含む名前付き論理構成体である管理対象オブジェクトです。この場合、エンドポイントは特定のサービスインスタンスを指します。たとえば、SQL サーバーはエンドポイントと見なされ、SQL サーバーのコレクションはサービスエンドポイント グループを形成します。サービス EPG の他の例としては、ストレージ アカウントのコレクション、Key Vault のコレクションなどがあります。

サービス EPG には、いくつかの固有の属性があります。

- **サービス タイプ**：この属性は、グループ化されているクラウド サービスのタイプを示します。利用可能なサービスの種類の例には、**Azure SQL**、**Azure Containter Registery**、**Azure ApiManagement Services** などがあります。サービス タイプ **Custom**は、サードパーティ サービス EPG を構成するときに使用されます。
- **展開タイプ**：この属性は、サービスを展開する方法と場所を示します。 以下は使用可能な展開タイプです。
  - **クラウド ネイティブ**：このタイプの展開では、サービスはクラウドプロバイダーのネットワークでインスタンス化され、サービスを使用するユーザまたはアプリケーションはサービスを管理します。たとえば、Azure ストレージ アカウントが Azure 独

自の VNet 内に存在する場合があり、ストレージ コンテンツにアクセスするための URL があります。

- **クラウド ネイティブ管理対象**：このタイプの展開では、サービスは VNet またはサブネットでインスタンス化されます（Cisco Cloud APIC を介して作成されます）。たとえば、Azure Kubernetes cluster（AKS）は、Cisco Cloud APIC によって管理されるサブネットに展開できます。
- **サードパーティ**：これは、サードパーティ（Azure 以外）が市場を通じてサービスを提供している展開です。このサービスへのアクセスは、プライベートリンク機能を通じて提供されます。

- **アクセス タイプ**：サービスへのアクセス方法を示します。使用可能なアクセス タイプは次のとおりです。
  - **パブリック**：サービスには、割り当てられたパブリック IP アドレスを使用してアクセスできます。特定のサービスのパブリック IP アドレス範囲へのアクセスは、NSG ルールの Azure「サービスタグ」を使用して行います。
  - **プライベート**：割り当てられているプライベート IP アドレスを使用して、サービスにアクセスできます。この割り当ては、展開が **Cloud Native** および `Third Party` の場合、プライベートエンドポイントの作成を通して行われます。**Cloud Native Managed** 展開の場合、プライベート IP はサービスによってサブネット IP スペースから割り当てられます。

前の箇条書きで説明したように、特定の展開タイプ、および各展開タイプ内の特定のアクセスタイプのみが各サービスの種類でサポートされます。次の表は、各サービスの種類でサポートされている展開の種類とアクセスの種類の詳細を示しています。

サービスタイプ	プロバイダー	展開タイプ/アクセス タイプ		
		クラウドネイティブ	クラウドネイティブ管理対象	サードパーティ製の
Azure Storage Blob	Microsoft.Storage	プライベート	N/A	N/A
Azure SQL	Microsoft.Sql	• パブリック（Public） • プライベート（Private）	N/A	N/A
Azure Cosmos DB	Microsoft.DocumentDB	• パブリック（Public） • プライベート（Private）	N/A	N/A

サービスタイプ	プロバイダー	展開タイプ/アクセス タイプ		
		クラウドネイティブ	クラウドネイティブ管理対象	サードパーティ製の
Azure Databricks	Microsoft.Databricks	パブリック（Public）	• プライベート（Private） • パブリックとプライベート	N/A
Azure Storage	Microsoft.Storage	• パブリック（Public） • プライベート（Private）	N/A	N/A
Azure Storage ファイル	Microsoft.Storage	プライベート	N/A	N/A
Azure Storage キュー	Microsoft.Storage	プライベート	N/A	N/A
Azure Storage テーブル	Microsoft.Storage	プライベート	N/A	N/A
Azure Kubernetes Services（AKS）	Microsoft.ContainerService	プライベート	• プライベート • パブリックとプライベート	N/A
Azure Active Directory ドメイン サービス	Microsoft.AAD	パブリック（Public）	• プライベート（Private） • パブリックとプライベート	N/A
Azure Container レジストリ	Microsoft.ContainerRegistry	• パブリック（Public） • プライベート（Private）	N/A	N/A
Azure ApiManagement サービス	Microsoft.ApiManagement	パブリック（Public）	• プライベート（Private） • パブリックとプライベート	N/A

サービスタイプ	プロバイダー	展開タイプ/アクセス タイプ		
		クラウドネイティブ	クラウドネイティブ管理対象	サードパーティ製の
Azure Key Vault	Microsoft.KeyVault	• パブリック（Public） • プライベート（Private）	N/A	N/A
Redis キャッシュ	Microsoft.Cache	N/A	• プライベート • パブリックとプライベート	N/A
カスタムサービス		• パブリック（Public） • プライベート（Private）	N/A	プライベート

- **サービスエンドポイント セレクタ**： サービスエンドポイントは、既存のセレクタ（クラウド EPG 選択で使用される）と、以下にリストされている新しいタイプのセレクタを使用して選択できます。
  - **リソース名**：サービス リソースの名前
  - **リソース ID**：リソースのクラウドプロバイダーの ID
  - **URL**：サービスを識別するエイリアスまたは FQDN（プライベート リンク エイリアスは Azure で使用されます）

次の表に、各展開の種類でサポートされているエンドポイント セレクタの詳細を示します。

（注） クラウド ネイティブ（パブリック）展開タイプに関する情報は、次の表に記載されていません。展開タイプがエンドポイント セレクタをサポートしていないためです。

展開タイプ	タグ	地域	IP	リソース名	Resource ID	URL
クラウドネイティブ（プライベート）	Y	Y	N	Y	Y	N
クラウド ネイティブ管理対象	N	N	Y	N	N	N

展開タイプ	タグ	地域	IP	リソース名	Resource ID	URL
サードパーティ製の	N	N	N	N	N	Y（プライベート リンク接続にのみ適用）

クラウド サービス EPG の注意事項および制限事項

クラウド サービス EPG を構成している場合は、**サブネットごとの NSG** 構成を有効にする必要があります。詳細については、「セキュリティ グループ （28 ページ）」を参照してください。

サービス タイプについて

特定のサービス タイプに固有の追加情報を以下に示します。

Azure Storage

Azure Storage サービス タイプは、次の 4 つのサブタイプに分類できる一般的なサービス タイプです。

- BLOB
- ファイル
- テーブル
- キュー

一般的な Azure Storage サービス タイプを使用して、次の値でサービス EPG を構成する場合：

- **サービス タイプ**：`Azure Storage`
- **展開タイプ**：`Cloud Native`
- **アクセス タイプ**：`Private`

次に 4 つのプライベート エンドポイントが、上記の 4 つのサブタイプのそれぞれに対して 1 つ、このサービス EPG に対して自動的に構成されます。

ただし、より具体的な Azure Storage サービス タイプを使用して、次の値でサービス EPG を構成する場合は、次のようにします。

- **サービス タイプ**：これらのサービス タイプのうち 1 つ：
  - `Azure Storage Blob`
  - `Azure Storage File`
  - `Azure Storage Table`
  - `Azure Storage Queue`
- **展開タイプ**：`Cloud Native`
- **アクセス タイプ**：`Private`

次に、このサービス EPG のこの特定のサブタイプに対して、1 つのプライベート エンドポイントのみが自動的に構成されます。

展開タイプ `Cloud Native` でアクセス タイプ `Public` がある場合、特定の 4 つの Azure ストレージ サブタイプ（`Blob`、`File`、`Table`、`Queue`）は許可されないことに注意してください。これは、Azure サービス タグがストレージ サブタイプ固有ではないためです。

Azure ApiManagement サービス

Azure ApiManagement（APIM）サービス インスタンスを VNet に展開するには、他の多くの Azure サービスにアクセスできる必要があります。これを行うには、このアクセスを許可するセキュリティ グループ ルールをプログラムする必要があります。

Cisco Cloud APIC はこれを自動化し、ここにリストされているルールを構成します。

https://docs.microsoft.com/en-us/azure/api-management/api-management-using-with-vnet#-common-network-configuration-issues

Azure Databricks サービス

Azure Databricks には、次のものが必要です。

- 他のサービスへのアクセス
- サブネットが Microsoft に委任されている展開用の 2 つのサブネット

Azure Databricks の場合、次の構成を行います。

- サービス EPG を構成する前に、Azure Databricks サービス専用に 2 つのサブネットを構成する必要があります。
- サービス EPG を構成するときは、2 つのサービス サブネットを一致させるために使用される 2 つのサービスエンドポイント セレクタ作成する必要があります。

構成されたエンドポイント セレクタを介して Azure Databricks サービス EPG でサブネットが識別されると、Cisco Cloud APIC はサブネットを Azure に委任し、ここにリスト化されているルールを構成します。

https://docs.microsoft.com/en-us/azure/databricks/administration-guide/cloud-configurations/azure/vnet-inject

Azure Active Directory ドメイン サービス

Azure Active Directory ドメイン サービス（ADDS）には、次のものが必要です。

- 他のサービスへのアクセス
- サブネットが展開されているときに、ルーティング テーブルがサブネットにアタッチされていません

サブネットからルーティング テーブルの関連付けを解除するアクションは、サービス EPG を構成した後、ADDS を展開する前に、Azure ポータルを介して実行する必要があります。展開が完了したら、ルーティング テーブルをサブネットに接続できます。

Cisco Cloud APIC は、ここにリストされているルールのプログラミングを自動化します。

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/network-considerations

Azure Kubernetes サービス

Azure Kubernetes サービス（AKS）には、他のサービスへのアクセスが必要です。

Cisco Cloud APIC は、ここにリストされているルールのプログラミングを自動化します。

https://docs.microsoft.com/en-us/azure/aks/limit-egress-traffic#required-outbound-network-rules-and-fqdns-for-aks-clusters

AKS サービス EPG の構成例については、サービス EPG 構成例 を参照してください。

Azure Redis キャッシュ

Azure Redis キャッシュには、他のサービスへのアクセスが必要です。

Cisco Cloud APIC は、ここにリストされているルールのプログラミングを自動化します。

https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-how-to-premium-vnet#outbound-port-requirements

展開タイプについて

特定の展開タイプに固有の追加情報を以下に示します。

- クラウドネイティブ （25 ページ）
- クラウド ネイティブ管理対象 （27 ページ）

クラウドネイティブ

このタイプの展開では、サービスはクラウドプロバイダーのネットワークでインスタンス化され、サービスを使用するユーザまたはアプリケーションはサービスを管理します。たとえば、Azure ストレージ アカウントが Azure 独自の VNet 内に存在する場合があり、ストレージ コンテンツにアクセスするための URL があります。

次に、クラウド ネイティブ展開タイプのサービス EPG の例を示します。

- **サービス タイプ**：Azure SQL
- **展開タイプ**：クラウド ネイティブ
- **アクセス タイプ**：プライベート

このサンプル シナリオでは、この順番で次の構成を行います。

1. Cisco Cloud APIC GUI で、Azure SQL サービス EPG によって使用されるクラウド コンテキスト プロファイルにプライベート リンク ラベルを作成します。

   Cisco Cloud APIC GUI を使用したクラウド コンテキスト プロファイルの作成の手順を実行します。Azure SQL サービス EPG（`SQL-PLL` など）で使用されるプライベート リンク ラベルを構成します。

2. Cisco Cloud APIC GUI で、サービス タイプ Azure SQL のサービス EPG を作成します。

   次のパラメータを使用して、Cisco Cloud APIC GUI を使用したサービス EPG の作成 の手順に従います。

   - **サービス タイプ**：Azure SQL
   - **展開タイプ**：クラウド ネイティブ
   - **アクセス タイプ**：プライベート

   このタイプのサービス EPG を構成するプロセスの一部としてエンドポイント セレクタを構成する場合は、SQL サーバーの適切な値と一致するようにエンドポイント セレクタを構成します。

   たとえば、`ProdSqlServer` という名前の SQL サーバーを選択する場合は、次のように選択します。

   - **キー**：名前
   - **演算子**：equals
   - **値**：`ProdSqlServer`

   別の例として、クラウドプロバイダーのリソース ID `/subscriptions/{subscription-id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/ProdSqlServer` を使用して SQL サーバーを選択する場合は、次のように選択します。

   - **キー**：リソース ID
   - **演算子**：equals
   - **値**：`/subscriptions/{subscription-id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/ProdSqlServer`

3. Azure ポータルで、クラウド内の Azure SQL リソースを構成します。

クラウド ネイティブ管理対象

このタイプの展開では、サービスはVNetまたはサブネットでインスタンス化されます（Cisco Cloud APICを介して作成されます）。たとえば、Azure ApiManagement Servicesは、Cisco Cloud APICによって管理されるサブネットに展開できます。

次に、クラウド ネイティブ管理対象展開タイプのサービス EPG の例を示します。

- **サービス タイプ**：Azure ApiManagement Services
- **展開タイプ**：クラウド ネイティブ管理対象
- **アクセス タイプ**：プライベート

このサンプル シナリオでは、この順番で次の構成を行います。

1. Cisco Cloud APIC GUI で、Azure ApiManagement Services service EPG によって使用されるクラウド コンテキスト プロファイルにサブネットを作成します。

   Cisco Cloud APIC GUI を使用したクラウド コンテキスト プロファイルの作成の手順を実行します。Azure ApiManagement Services service EPG（たとえば、`10.50.0.0/16`）によって使用されるサブネットを構成します。

2. Cisco Cloud APIC GUI で、サービス タイプ Azure ApiManagement Services サービス EPG を作成します。

   次のパラメータを使用して、Cisco Cloud APIC GUI を使用したサービス EPG の作成 の手順に従います。

   - **サービス タイプ**：Azure ApiManagement Services
   - **展開タイプ**：クラウド ネイティブ管理対象
   - **アクセス タイプ**：プライベート

   このタイプのサービス EPG を構成するプロセスの一部としてエンドポイント セレクタを構成する場合は、最初の手順でクラウド コンテキスト プロファイルにサブネットを作成したときに使用したIPアドレスと一致するようにエンドポイント セレクタを構成します。

   たとえば、最初のステップで提供された例を使用して、このサービスEPGに対してこのエンドポイント セレクタを構成します。

   - **キー**：IP
   - **演算子**：equals
   - **値**：10.50.0.0/16

3. Azure ポータルで、クラウドの Azure ApiManagement Services リソースを構成します。

セキュリティ グループ

Azure では、2 種類のセキュリティ グループを使用して、仮想ネットワーク（VNet）内のネットワーク トラフィックを管理および制御します。

- **ネットワーク セキュリティ グループ**：ネットワーク セキュリティ グループ（NSG）は Azure で使用され、Azure リソースとの間のネットワーク トラフィックをフィルタ処理します。NSG は、受信および送信のセキュリティ ポリシーを定義するために使用され、いくつかの種類の Azure リソースへのインバウンド ネットワーク トラフィックまたはそこからのアウトバウンドネットワーク トラフィックを許可または拒否するセキュリティルールが含まれています。ルールごとに、送信元と送信先、ポート、およびプロトコルを指定できます。

  Cloud APIC では、NSG はコントラクトに基づいて自動的に構成されます。

- **アプリケーション セキュリティ グループ**：アプリケーション セキュリティ グループ（ASG）は Azure で使用され、仮想マシン（VM）NIC で実行されるアプリケーションに従って仮想マシン（VM）NIC をグループ化し、それらのグループに基づいてネットワーク セキュリティ ポリシーを定義します。ASG は NSG 内でこれらのセキュリティ ポリシーを定義し、ネットワーク セキュリティ ルールを特定のワークロードまたは仮想マシンのグループに適用するために使用されます。

  Cloud APIC では、ASG は各 EPG のエンドポイントの収集であり、NSG セキュリティポリシーの送信元または接続先として参照されます。

これらのセキュリティ グループの構成方法とマップ先は、リリースによって異なります。

- リリース 5.1(2) より前のリリース：EPG ごとの NSG 構成 （28 ページ）
- リリース 5.1(2) 以降：サブネットごとの NSG 構成 （29 ページ）
- リリース 5.1(2g) 以降：同じ VNet 内の VRF 間コントラクトの IP ベースのルール （29 ページ）

リリース 5.1(2) より前のリリース：EPG ごとの NSG 構成

リリース 5.1(2) より前のリリースでは、Azure の NSG と Cisco Cloud APIC の EPG との間に 1 対 1 のマッピングがあります（これらの構成は、このドキュメント全体で **EPG ごとの NSG** 構成とも呼ばれます）。Cloud APIC EPG のこれらの NSG には、EPG に関連付けられたコントラクトに基づいたセキュリティルールが構成されています。

リリース 5.1(2) より前のリリースでは、Cloud APIC で EPG を作成すると、次の Azure コンポーネントが作成されます。

- エンドポイント セレクタに基づいて各 EPG のすべてのエンドポイントまたは仮想マシン NIC をグループ化するために使用される ASG
- その ASG 内のすべての NIC に関連付けられ、その EPG のセキュリティ ポリシー定義を提供する NSG

リリース 5.1(2) 以降：サブネットごとの NSG 構成

リリース 5.1(2) 以降、以前に使用できた既存の EPG ごとの NSG 構成に加えて、Azure の NSG は Cloud APIC 上の EPG ではなくサブネットとの 1 対 1 のマッピングを持つこともできます（これらの構成は、このドキュメント全体で、**サブネットごとの NSG** 構成として呼ばれます）。デフォルトでは、NSG はリリース 5.1(2) 以降の EPG に対して作成されなくなり、NSG はその EPG の ASG 内のエンドポイントおよび VM NIC に関連付けられなくなりました。代わりに、各サブネットの NSG には、サブネットでエンドポイントが検出された ASG のコントラクトに基づくすべてのルールが含まれます。

サブネットごとの NSG 構成の場合、Cloud APIC で EPG を作成すると、次の Azure コンポーネントが作成されます。

- エンドポイント セレクタに基づいて各 EPG のすべてのエンドポイントまたは仮想マシン NIC をグループ化するために使用される ASG [リリース 5.1(2) より前のリリースからの ASG の動作は基本的に変更されません]
- その EPG のセキュリティ ポリシー定義を提供し続けるが、Cloud APIC が管理する VNet のサブネットに関連付けられるようになった NSG

別の視点から見た場合：

- Cloud APIC で管理された VNet 内のすべての EPG には、それに関連付けられた ASG があり、EPG 用に構成されたエンドポイント セレクタに基づいてすべてのエンドポイントがグループ化されます。
- Cloud APIC で管理された VNet 内のすべてのサブネットには、NSG が関連付けられています。

グリーンフィールドまたは新しい Cloud APIC 展開のデフォルト設定は、**サブネットごとの NSG** です。この構成を手動で設定する場合、前述のように新しい **サブネットごとの NSG** 構成またはリリース 5.1(2) 以降の古い **EPG ごとの NSG** 構成を選択できます。ただし、いくつかの理由から、新しい **サブネットごとの NSG構成**を選択することをお勧めします。

- **サブネットごとの NSG** 構成を使用すると、VNet 内の NSG の数が減り、共通の共有サービスにアクセスする多数のサブネットがある展開のルール数も減ります。これにより、個々の EPG または ASG にマッピングされた各 NSG ではなく、サブネットの 1 つの NSG ですべてのルールをチェックできるため、管理が容易になります。
- サービス EPG を構成している場合は、**サブネットごとの NSG 構成** を使用する必要があります。詳細については、「クラウド サービスエンドポイント グループ （19 ページ）」を参照してください。

EPG ごとの NSG またはサブネットごとの NSG 構成を有効または無効にする手順については、Cloud APIC GUI を使用したネットワーク セキュリティ グループの構成 を参照してください。

リリース 5.1(2g) 以降：同じ VNet 内の VRF 間コントラクトの IP ベースのルール

リリース 5.1(2g) より前では、2 つの EPG にコントラクトがあり、同じ VNet にあるが異なる VRF に属している場合、ASG ベースのルールが使用され、その VNet でホストされている VRF

間の通信を有効にしていました。Azure ではすべての NSG のルールで 100 ASG の制限があり、状況によっては（たとえばすべての共有サービスに対して 1 つの VNet がある場合）、この制限にすぐに達する可能性があります。

リリース 5.1(2g) 以降、2 つの EPG にコントラクトがあり同じ VNet にあるが、異なる VRF に属している場合、IP ベースのルールが使用され、その VNet でホストされている VRF 間の通信を有効にするようになりました。ルールで 4000 個の IP アドレスをサポートできるため推奨されます。これらの IP ベースのルールは、検出されたエンドポイントまたは EPG で使用されるサブネット セレクタに基づいています。

ASG および NSG の注意事項と制限事項

以下は、ASG および NSG の注意事項と制限事項です。

• 5.1(2) より前のリリースの注意事項と制限事項 （30 ページ）
• リリース 5.1(2) 以降の注意事項と制限事項 （30 ページ）

5.1(2) より前のリリースの注意事項と制限事項

リリース 5.1(2) より前のリリースでは、Cloud APIC の NSG から EPG へのマッピングのみがサポートされています。

リリース 5.1(2) 以降の注意事項と制限事項

- リリース 5.1(2) 以降、Cloud APIC の NSG からサブネットへのマッピングもサポートされています。ただし、新しいサブネットごとの NSG 構成または EPG ごとの NSG 構成のいずれかを使用できますが、同じ Cloud APIC システムに両方を含めることはできません。
- Cloud APIC で管理される VNET では、サブネットごとに 1 つの NSG を構成できます。サブネットのグループごとに 1 つの NSG を持つことは、現時点では Cloud APIC ではサポートされていません。
- 透過ファイアウォールなどのパススルー デバイスでは、NIC に NSG が接続されません。サブネットを共有する複数のパススルー デバイスがある場合、各デバイスのパススルー ルールはサブネット内のすべてのエンドポイントに適用されます。

セキュリティ ルール

NSG のセキュリティ ルールは、それらが EPG ごとの NSG 構成のルールであるか、サブネットごとの NSG 構成のルールであるかによって異なります。2 種類の構成のセキュリティ ルールの処理に関する主な違いは、ルールのインストールと削除のトリガーです。

• EPG ごとの NSG セキュリティ ルール （31 ページ）
• サブネットごとの NSG セキュリティ ルール （31 ページ）

EPG ごとの NSG セキュリティ ルール

- EPG とコントラクトが Cloud APIC で定義されると、NSG セキュリティ ルールで参照される ASG のエンドポイントが検出されるかどうかに関係なく、ASG を送信元および接続先として使用する NSG セキュリティ ルールが常にプログラムされます。
- VRF 間コントラクトの場合：
  - コンシューマまたはプロバイダー EPG のいずれかがサブネットに基づくエンドポイント セレクタを使用する場合、エンドポイントの検出に関係なく、EPG セレクタからのサブネットとして送信元または接続先を持つ NSG セキュリティ ルールが常にプログラムされます。
  - コンシューマまたはプロバイダーの EPG がサブネットに基づくエンドポイント セレクタを使用しない場合、エンドポイントの検出に応じて、エンドポイントの IP アドレスを送信元および接続先として使用する NSG セキュリティ ルールがプログラムされます。
- クラウド外部 EPG（`cloudExtEPg`）が関係するサイト間コントラクト用に作成されたルールも、エンドポイントが検出されることなく事前にプログラムされます。

サブネットごとの NSG セキュリティ ルール

EPG の NSG セキュリティ ルールは、EPG がそのサブネットで少なくとも 1 つのエンドポイントを検出するまで、サブネット ベースの NSG でプログラムされません。

ソフトウェア アップグレードまたはダウングレードによる NGS 動作

リリース 5.1(2) より前のリリースでは NSG ごとの EPG マッピングのみがサポートされており、NSG ごとのサブネット マッピングのサポートがリリース 5.1(2) 以降で使用可能になったため、特定の状況でソフトウェアをアップグレードまたはダウングレードした場合に、特定のシステム構成変更が行われる可能性があります。次のセクションでは、これらの状況と、これらのアップグレードまたはダウングレード操作中に発生する必要があることについて説明します。

- ソフトウェア アップグレードによる NSG の動作 （31 ページ）
- ソフトウェア ダウングレードによる NSG の動作 （32 ページ）

ソフトウェア アップグレードによる NSG の動作

リリース 5.1(2) より前のリリースからリリース 5.1(2) 以降への標準アップグレードを実行すると、リリース 5.1(2) より前のリリースでサポートされていた EPG ごとの NSG マッピングを使用して構成された NSG は、アップグレード後もそのまま残ります。これは、EPG ごとの NSG またはサブネットごとの NSG 構成のいずれかがリリース 5.1(2) 以降でサポートされているため、リリース 5.1(2) 以降への標準アップグレードを実行すると、古い EPG ごとの NSG 構成が自動的に保持されるためです。

ただし、サブネットごとのNSG構成には利点があるため、これらの利点を利用するには、EPGごとの NSG 構成をサブネットごとの NSG に変換することをお勧めします。さまざまな NSG 構成の詳細についてはセキュリティ グループ （28 ページ） を、EPG ごとの NSG またはサブネットごとの NSG 構成の有効化または無効化に関する指示についてはCloud APIC GUI を使用したネットワーク セキュリティ グループの構成 を参照してください。

アップグレード後は、古い EPG ごとの NSG 構成または新しいサブネットごとの NSG 構成のいずれかを使用できますが、同じ Cloud APIC システムで両方を使用することはできないことに注意してください。詳細については、「ASG および NSG の注意事項と制限事項 （30 ページ）」を参照してください。

ただし、Cisco Cloud APIC GUI を使用したバックアップ構成の作成 の手順を使用して既存のCloud APIC構成をバックアップし、アップグレードを実行し、アップグレード後にバックアップされた構成をインポートした場合、サブネットごとの NSG 構成は自動的にオンになり、古い EPG ごとの NSG 構成は新しいサブネットごとの NSG 構成に自動的に変換されます。

ソフトウェア ダウングレードによる NSG の動作

リリース 5.1(2) 以降からリリース 5.1(2) より前のリリースにダウングレードする場合は、サブネットごとの NSG 構成を、リリース 5.1(2) より前のリリースでサポートされていた EPG ごとの NSG 構成に手動で戻す必要があります。

ソフトウェアをダウングレードする前に、サブネットごとの NSG 構成から EPG ごとの NSG 構成に移行する一般的なプロセスを次に示します。

1. ソフトウェアをリリース 5.1(2) 以降から リリース 5.1(2) より前のリリースにダウングレードする前に、Cloud APIC GUI を使用したネットワーク セキュリティ グループの構成 で説明されている手順を使用して、サブネットごとの NSG 構成を無効にします。Cloud APIC ソフトウェアは、サブネットごとのNSGマッピングからEPGごとのNSGマッピングへの移行を開始します。

2. 移行が完了するまで待ちます。この場合、Cloud APIC ソフトウェアは、サブネットごとの NSG マッピング プロセスの一部として構成されたすべての NSG を削除し、EPG ごとの NSG マッピング構成用に新しい NSG を作成します。移行が完了する前にダウングレードを続行しようとすると、エラー メッセージが表示され、Cloud APIC ソフトウェアは、サブネット マッピングごとの NSG から EPG マッピングごとの NSG へのこの移行が完了するまで、ダウングレードを続行することを許可しません。

（注） GUI を使用してダウングレードするときに、移行が完了する前にソフトウェアのダウングレードを試みると、エラー メッセージが表示されます。ただし、REST API を使用してダウングレードするときに、ソフトウェアのダウングレードを早すぎてもエラー メッセージは表示されません。そのため、このような状況にある場合は、REST API を介してソフトウェアをダウングレードしないことをお勧めします。

REST API を使用してソフトウェアをダウングレードする場合は、次の MO を監視します。

`hcloudReconcileDone`

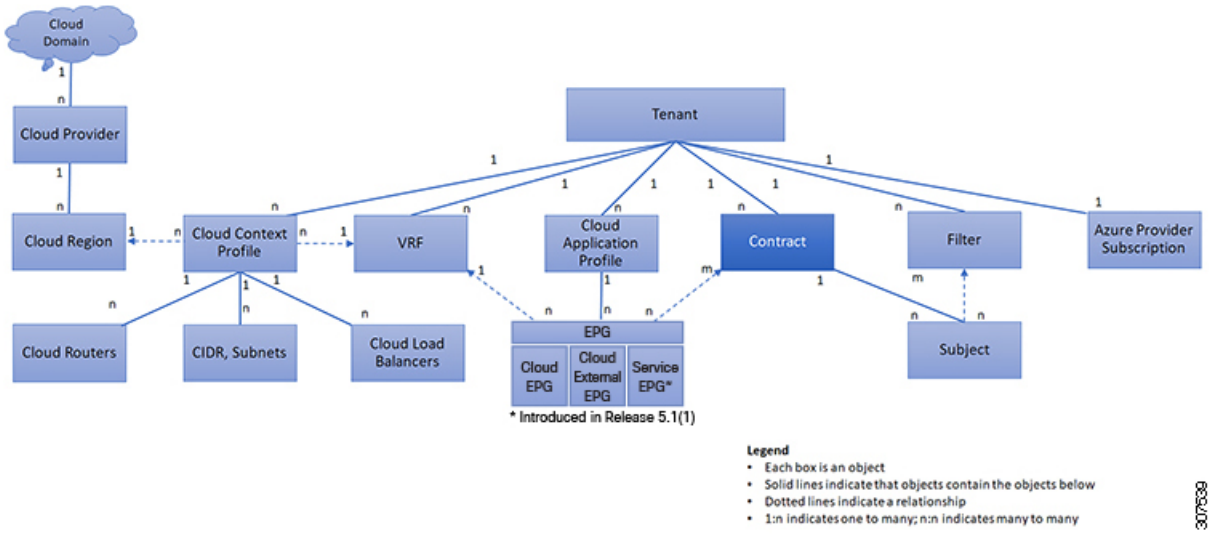
REST API を使用してダウングレードを続行する前に、プロパティ `sgForSubnetModeConverged` が `[yes]` に設定されていることを確認します。

3. システムが EPG ごとの NSG マッピングへの移行を正常に完了したことを確認したら、『*Cisco Cloud APIC for Azure* インストール ガイド』に記載されている手順を使用して、Cloud APIC ソフトウェアをダウングレードできます。

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。コントラクトがない場合、EPG 間通信はデフォルトで無効になります。EPG 内の通信に必要なコントラクトはありません。EPG 内の通信は常に暗黙的に許可されています。

コントラクトは、次のタイプのクラウド EPG 通信を管理します。

- クラウド EPG （`cloudEPg`）間のテナント内およびテナント間の両方

（注） 共有サービス モードの場合、コントラクトはテナント間通信に必要です。テナント VRF がポリシーを適用していなくても、コントラクトが VRF 間でスタティック ルートを指定するために使用されます。

- クラウド EPGとクラウド外部 EPG 間（`cloudExtEPg`）

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

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

コントラクト ルール統合のためのコンマ区切りフィルタのサポート

コントラクトが作成されると、コントラクトで定義されたルールの一部が統合され、特定の基準に基づいて Azure に表示されます。複数のポートと複数の IP アドレスと範囲を 1 つのわかりやすいルールに組み合わせることができます。ルールの統合の基準は次のとおりです。

- ルールは、コントラクト内でのみ統合されます。2 つの異なるコントラクトに起因する 2 つのルールは、Azure に統合されません。
- 送信元/宛先アドレス プレフィックスと宛て先ポートが統合されます。
- 複数のルールを NSG に統合するための条件は次のとおりです。
  - 同一コントラクト
  - 同じプロトコル（UDP、TCP、ICMP）
  - 同じ方向（インバウンド、アウトバウンド）

- 同型（SG、IP）

- 同一コントラクト内の同一プロトコル（TCP/UDP）の重複するポート範囲は1つに集約します。

  たとえば、TCP ポート 100 ～ 200、150 ～ 250 は 100 ～ 250 に統合されます。

- 1.2.3.4/32（任意のアドレスプレフィックス）が許可され、0.0.0.0/0 の拡張EPGが追加された場合、許可される送信元/宛先 IP は [1.2.3.4/32, 0.0.0.0/0] ではなく任意になります。

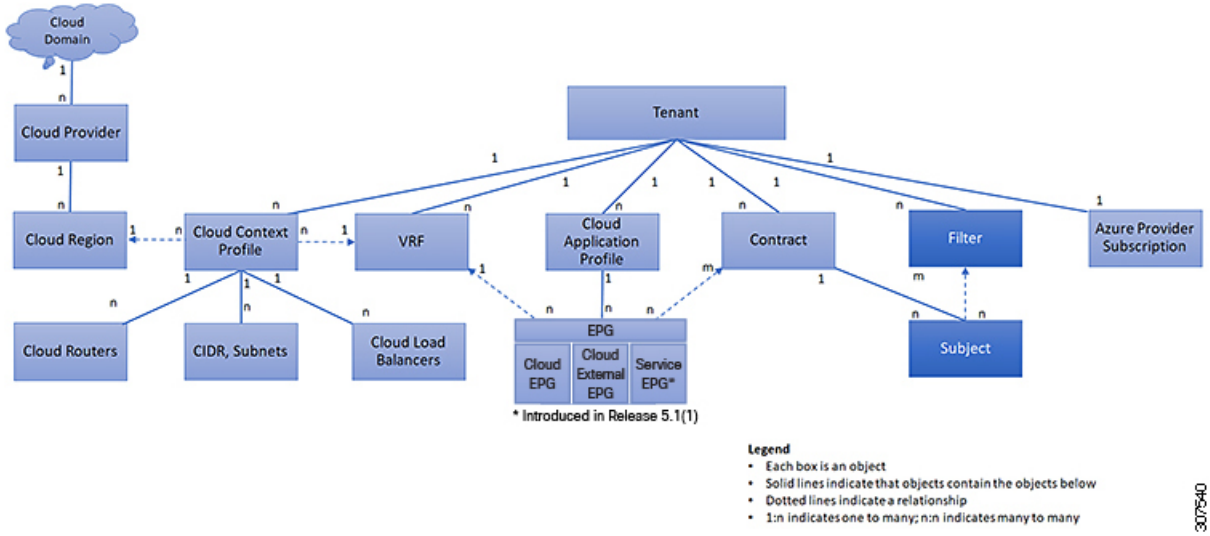
以下の例は、コントラクトC1およびC2に基づく、EPG1アウトバウンドルールと統合されたEPG1 アウトバウンド ルールを示しています。

```
Contract C1:
Consumer: EPG1 , Provider: EPG2
Filter: TCP  (ports 53)
Filter: UDP (port 53, 5000)

Contract C2:
Consumer: EPG1 , Provider: EPG2
Filter: TCP (ports 80, 8080)

EPG1 outbound rules:
EPG1 -> EPG2   TCP  80
EPG1 -> EPG2   TCP  8080
EPG1 -> EPG2        TCP        53
EPG1 -> EPG2   UDP  53
EPG1 -> EPG2   UDP  5000
EPG1 -> 1.1.1.1/32  TCP  80
EPG1 -> 1.1.1.1/32  TCP  8080
EPG1 -> 1.1.1.1/32  TCP  53
EPG1 -> 1.1.1.1/32  UDP  53
EPG1 -> 1.1.1.1/32  UDP 5000
EPG1 -> 2.2.2.2/32  TCP  80
EPG1 -> 2.2.2.2/32  TCP  8080
EPG1 -> 2.2.2.2/32  TCP       53
EPG1 -> 2.2.2.2/32  UDP  53
EPG1 -> 2.2.2.2/32  UDP  5000

Rules are consolidated by comma-separated filters (consolidated based on C1 and C2):
EPG1 -> EPG2     TCP  80,8080
EPG1 -> EPG2     UDP  53,5000
EPG1 -> EPG2     TCP  53
EPG1 -> 1.1.1.1/32, 2.2.2.2/32   TCP  80,8080
EPG1 -> 1.1.1.1/32, 2.2.2.2/32   UDP  53,5000
EPG1 -> 1.1.1.1/32, 2.2.2.2/32   TCP  53
```

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。Azure にインストールされているルールの場合、フィルタ エントリで指定された送信元ポートは考慮されません。

サブジェクトおよびフィルタは次のオプションに従ってクラウド EPG 通信を定義します。

- フィルタは、レイヤ 3 ～ レイヤ 4 フィールド、レイヤ 3 プロトコル タイプなどの TCP/IP ヘッダー フィールド、レイヤ 4 ポートなどです。関連するコントラクトに従って、クラウド EPG プロバイダーは、IN および OUT 両方の方向でプロトコルおよびポートを決定します。コントラクトのサブジェクトは、コントラクトを提供する側と消費する側のクラウド EPG の間に適用されるフィルタ（およびその方向）への関連付けが含まれています。
- サブジェクトはコントラクトに含まれています。コントラクト内のサブジェクトがフィルタを使用して、通信できるトラフィックのタイプと発生の仕方を指定します。たとえば、HTTPS メッセージの場合、サブジェクトはその方向と許可される IP アドレス タイプ（たとえば IPv4）、HTTP プロトコル、およびポートを指定するフィルタを指定します。サブジェクトは、フィルタを単方向にするか双方向にするかを決定します。単方向フィルタは 1 方向で使用されます。単方向フィルタは、IN または OUT の通信を定義しますが、両方に対して同じではありません。双方向フィルタは両方に対して同じで、IN および OUT の通信を定義します。
- Azure 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。

Azureネットワーク構成の中央のうちいずれかは、仮想プライベートクラウド（VNET）です。Azure 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 VNET 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承認し、それらのリージョンでインフラ VNET の構成全体を生成します。それらはインフラ VNET です。Azure VNET 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。インフラ VNet の `cloudCtxProfile` MO は、クラウド テンプレートにより生成されます。これは `ctxProfileOwner == SYSTEM` を伝送します。これは、この MO がシステムによって生成されることを意味します。非インフラストラクチャ ネットワークの場合、`cloudCtxProfile`を直接設定できます。この場合、`cloudCtxProfile` は `ctxProfileOwner == USER` を伝送します。

Azure VNet の主要なプロパティは CIDR です。Cisco Cloud APIC では、ユーザ VNet で CIDR を選択して展開できます。インフラ VNet の CIDR は、クラウド サイトの最初のセットアップ時にユーザによってクラウドテンプレートに提供され、クラウドテンプレートによってAzure クラウドに展開されます。

リリース 5.0(2) 以降、`createdBy` という新しいプロパティが CIDR に追加されています。この `createdBy` プロパティのデフォルト値は `USER` です。

- すべてのユーザー作成 CIDR について、`createdBy` プロパティの値は `USER` に設定されます。
- クラウド テンプレートで作成されたCIDRの場合、`createdBy` プロパティの値は `SYSTEM` に設定されます。

複数の CIDR ブロックとサブネット ブロックをインフラ VNet で構成できます。 CIDR を作成し、インフラストラクチャ VNet にサブネットを関連付けることができます。クラウドテンプレート サブネットは overlay-1 VRF にマッピングされますが、ユーザが作成したサブネットの場合、同じインフラ VNet 内のセカンダリ VRF へのサブネットから VRF へのマッピングを手動で構成する必要があります。それぞれの VRF のすべてのサブネットは、VRF 分離のためにクラウド内に個別のルート テーブルを持ちます。

インフラ テナントでクラウド EPG とクラウド外部 EPG を作成できます。すべてのクラウド EPG とクラウド外部 EPG は、インフラ テナントのセカンダリ VRF に関連付けられます。セカンダリ VRF 内のクラウド EPG は、セカンダリ VRF 内の他のクラウド EPG およびクラウド外

部 EPG と通信可能で、他のユーザ テナント VRF 内のクラウド EPG とも通信できます。既存の「クラウド インフラ」アプリケーション プロファイルを使用せず、代わりにインフラ テナントに新しいアプリケーション プロファイルを作成し、新しいアプリケーション プロファイルをセカンダリ VRF のクラウド EPG およびクラウド外部 EPG に関連付けることをお勧めします。

詳細については、Cisco Cloud APIC GUI を使用したアプリケーション EPG の作成を参照してください。

クラウド テンプレートは、`cloudCtxProfile` サブツリーに次のような多数の MO を生成して管理します。

- サブネット
- クラウド ルータ
- クラウド ルータ インターフェイスの IP アドレス割り当て
- トンネルの IP アドレスの割り当てと設定
- ループバックの IP アドレスの割り当てと設定

クラウド テンプレートがない場合は、これらの設定と管理を担当します。

Cisco Cloud Template MO テーブルには、クラウド テンプレートへの入力（MO）の概要が含まれています。

表 *1*: クラウド テンプレート *MO*

月	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。

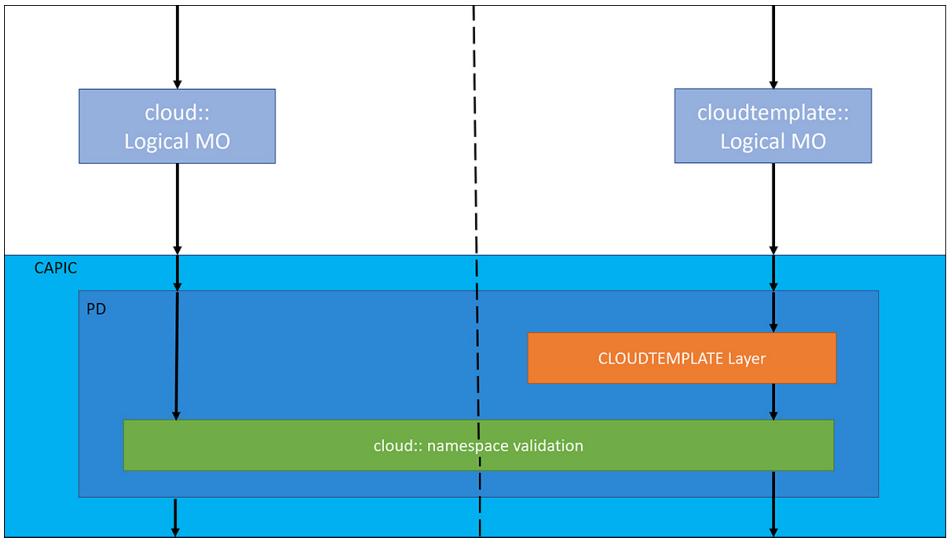
月	目的
cloudtemplateProfile	すべてのクラウドルータの設定プロファイル。次の属性が含まれます。 • routerUsername （注） • ユーザ名を「admin」にすることはできません。 • Azure からのユーザー名の制限が適用されます。 • routerPassword • routerThroughput • routerLicenseToken • routeDataInterfacePublicIP • routerMgmtInterfacePublicIP
cloudtemplateIntNetwork	クラウドルータを展開する場所を指定するリージョンの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。
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。

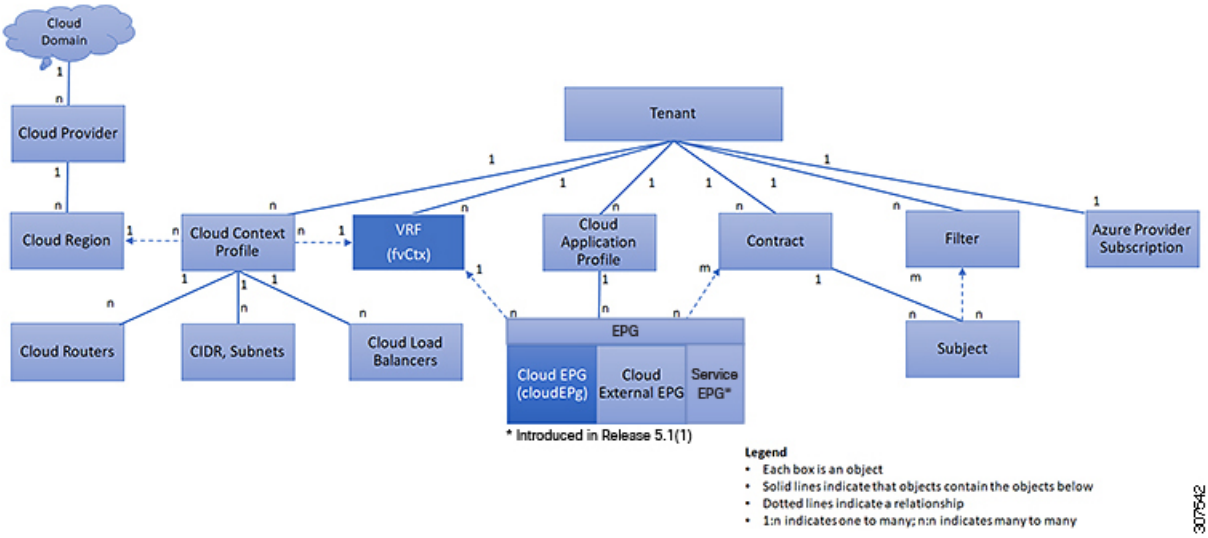
管理対象オブジェクトの関係とポリシー解決

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。

- `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 Azure 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。
  - テナント間コントラクトにはグローバル範囲が必要です。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。