Cisco Cloud APIC コンポーネントの設定

Cisco クラウド APIC の設定について

Cisco Cloud APIC GUI または REST API を使用して Cisco Cloud APIC コンポーネントを作成します。ここでは、設定、アプリケーション管理、運用、および管理コンポーネントの作成方法について説明します。

（注）

- ロードバランサとサービス グラフの設定については、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。
- ナビゲーションや構成可能なコンポーネントのリストなどの GUI については、Cisco Cloud APIC GUI の概要 を参照してください。

GUI を使用した Cisco Cloud Cisco APIC の設定

Cisco Cloud APIC GUIを使用したテナントの作成

このセクションでは、Cisco Cloud APIC GUI を使用したテナントの作成方法について説明します。

始める前に

- Cisco Cloud APIC によって管理されるテナント、または管理されていないテナントを作成できます。管理対象テナントを確立するには、最初に Azure ポータルから Azure サブスクリプション ID を取得する必要があります。テナントの作成時に、Cisco Cloud APIC の適

切なフィールドにサブスクリプション ID を入力します。管理対象テナントを使用する前に、サブスクリプションを管理するためのアクセス許可を Cisco Cloud APIC に明示的に付与する必要があります。これを行うための手順は、テナントの作成中に Cisco Cloud APIC GUI に表示されます。ただし、インフラ テナントの手順は、インフラ テナントの詳細ビューに表示されます。

1. **[ナビゲーション（Navigation）]** メニュー > **[アプリケーション管理（Application Management）]** サブタブをクリックします。
2. インフラ テナントをダブルクリックします。
3. **[Azure ロールの割り当てコマンドの表示（View Azure Role Assignment Command）]** をクリックします。サブスクリプションを管理するためのアクセス許可を Cisco Cloud APIC に付与する手順が表示されます。

（注） Azure サブスクリプション ID の取得については、Microsoft Azure のドキュメントを参照してください。

- 非管理対象テナントを作成するには、エンタープライズアプリケーションからディレクトリ（Azure テナント）ID、Azure エンタープライズ アプリケーション ID、およびクライアントシークレットを取得する必要があります。詳細については、Microsoft Azure のマニュアルを参照してください。

（注） Cloud APIC は、他のアプリケーションまたはユーザによって作成された Azure リソースを妨害しません。自身で作成した Azure リソースのみを管理します。

- 特定のサブスクリプションを管理するための許可を Cisco Cloud APIC に明示的に付与するために必要な手順は、Cisco Cloud APIC GUI にあります。テナントを作成する場合、クライアントシークレットを入力した後に手順が表示されます。
- Cloud APIC は所有権チェックを適用して、意図的にまたは誤って行われた同じテナントとリージョンの組み合わせでポリシーが展開されないようにします。たとえば、リージョン R1 の Azure サブスクリプション IA1 に Cloud APIC が展開されているとします。ここで、リージョン R2 にテナント TA1 を展開します。このテナント展開（TA1-R2 のアカウントとリージョンの組み合わせ）は、IA1-R1 によって所有されています。別の Cloud APIC が将来のある時点で同じテナントとリージョンの組み合わせを管理しようとした場合（たとえば、CAPIC2 がリージョン R3 の Azure サブスクリプション IA2 に導入されている場合）、これは展開 TA1-R2 の所有者が現在、IA1-R1 であるため許可されません。つまり、1 つの Cloud APIC で管理できるのは 1 つのリージョン内の 1 つのアカウントのみです。以下の例は、いくつかの有効な展開の組み合わせと間違った展開の組み合わせを示しています。

```
Capic1:
IA1-R1: TA1-R1 - ok
```

```
        TA1-R2 - ok

Capic2:
IA1-R2: TA1-R1 - not allowed
        TA1-R3 - ok

Capic3:
IA2-R1: TA1-R1 - not allowed
        TA1-R4 - ok
        TA2-R4 - ok
```

- 所有権の強制は、Azure リソースグループを使用して行われます。リージョン R2 のサブスクリプション TA1 の新しいテナントが Cloud APIC によって管理される場合、リソースグループ CAPIC_TA1_R2（例：CAPIC_123456789012__eastus2）がサブスクリプションに作成されます。このリソースグループには、値が IA1_R1_TA1_R2 のリソース タグ AciOwnerTag があります（サブスクリプション IA1 の Cloud APIC によって管理され、リージョン R1 に展開されていると想定）。AciOwnerTag の不一致が発生した場合、テナントとリージョンの管理は中止されます。

  AciOwnerTag の不一致ケースの概要は次のとおりです。

  - 最初に Cloud APIC がサブスクリプションにインストールされ、次に削除され、Cloud APIC が別のサブスクリプションにインストールされます。既存のすべてのテナント リージョンの展開が失敗します。
  - 別の TA1-R2 が同じテナント リージョンを管理しています。

  所有権が一致しない場合、**再試行** (テナント リージョンの再セットアップ) は現在サポートされていません。回避策として、他の CloudAPIC が同じテナントとリージョンの組み合わせを管理していないことが確実な場合は、テナントの Azure サブスクリプションにログオンし、影響を受けるリソースグループ（例：CAPIC_123456789012__eastus2 など）を手動で削除します。次に、Cloud APIC をリロードするか、テナントを再度削除して追加します。

- リリース 5.2(1) より前は、テナントのタイプに応じて、Azure リソースへのアクセスに使用できる方法のサポートが異なりました。
  - **インフラ テナント**：リリース 5.2(1) より前では、認証または資格情報を処理するときに、管理対象 ID のみがサポートされていました。
  - **ユーザ テナント**：認証または資格情報を処理するときに、管理対象 ID と非管理対象 ID/サービス プリンシパルの両方をサポートできます。

  リリース 5.2(1) 以降、インフラ テナントおよびユーザ テナント両方で、認証または資格情報を処理するとき、管理対象 ID と非管理対象 ID/サービス プリンシパルの両方をサポートできるようになりました。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）]オプションのリストが**[インテント（Intent）]**メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[テナントの作成（Create Tenant）]** をクリックします。**[テナントの作成（Create Tenant）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[*テナント ダイアログボックス フィールドの作成（*Create Tenant Dialog Box Field*）*]* の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *1:* テナント ダイアログボックス フィールドの作成

[プロパティ（Properties）]	説明
名前（Name）	テナント名を入力します。
説明	テナントの説明を入力します。
[設定（Settings）]	
セキュリティ ドメインの追加（Add Security Domain）	テナントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]**をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]**をクリックして、セキュリティ ドメインをテナントに追加します。
Azure サブスクリプション	
モード（Mode）	アカウント タイプを選択します。 • **[固有作成（Create Own）]**：新しいテナントを作成するには、このオプションを選択します。 • **[共有を選択（Select Shared）]**：このオプションを選択して、既存のテナントから管理対象または非管理対象の設定を継承します。
Azure サブスクリプション ID	Azure サブスクリプション ID を入力します。

[プロパティ（Properties）]	説明
アクセスタイプ	アクセス タイプを選択します。 • **[サービス プリンシパル（Service Principal）]** または **[非管理対象 ID（Unmanaged Identity）]**：テナント サブスクリプションが Cisco Cloud APIC によって管理されていない場合は、このオプションを選択します。 • **[管理対象 ID（Managed Identity）]**：テナント サブスクリプションが Cisco Cloud APIC によって管理されている場合は、このオプションを選択します。 （注） リリース 5.2(1) より前は、インフラストラクチャ テナントにのみ**[管理対象 ID（Managed Identity）]** を割り当てることができました。リリース 5.2(1) 以降では、インフラテナントに **[サービス プリンシパル（Service Principal）]** または **[管理対象 ID（Managed Identity）]** を割り当てることができるようになりました。 詳細については、テナント、ID、およびサブスクリプションについて を参照してください。
アプリケーションID	（注） このフィールドは、**[サービス プリンシパル（Service Principal）]** または **[非管理対象 ID（Unmanaged Identity）]** アクセス タイプに対してのみ有効です。 アプリケーション ID を入力します。 （注） アプリケーション ID の取得については、Azure のドキュメントまたはサポートを参照してください。

[プロパティ（Properties）]	説明
クライアントのシークレット（Client Secret）	（注） このフィールドは、**[サービス プリンシパル（Service Principal）]** または **[非管理対象 ID（Unmanaged Identity）]** アクセス タイプに対してのみ有効です。 クライアントシークレットを入力します。 （注） • クライアントシークレットの作成については、Azure のドキュメントまたはサポートを参照してください。 • 特定のサブスクリプションを管理するには、Cloud APIC のアクセス許可を明示的に付与する必要があります。Azure ポータルに移動して、次の手順に従います。 1. クラウド シェルをオープンします。 2. 「バッシュ」を選択 3. Cisco Cloud APIC GUI に表示されるコマンドをコピーして貼り付けます。
Active Directory ID	（注） このフィールドは、**[サービス プリンシパル（Service Principal）]** または **[非管理対象 ID（Unmanaged Identity）]** アクセス タイプに対してのみ有効です。 ディレクトリ ID を入力します。 （注） Active Directory ID の取得については、Azure のドキュメントまたはサポートを参照してください。

[プロパティ（Properties）]	説明
セキュリティドメインの追加（Add Security Domain）	アカウントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したアプリケーション プロファイルの作成

このセクションでは、Cisco Cloud APIC GUI を使用したアプリケーション プロファイルの作成方法を説明します。

始める前に

テナントを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[アプリケーション プロファイルの作成（Create Application Profile）]** をクリックします。**[アプリケーション プロファイルの作成（Create Application Profile）]** ダイアログ ボックスが表示されます。

ステップ 4 [名前（Name）] フィールドに名前を入力します。

ステップ 5 テナントを選択します。

a) **[テナントの選択（Select Tenant）]** をクリックします。

[テナントの選択（Select Tenant）] ダイアログボックスが表示されます。

b) **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。

[アプリケーションプロファイルの作成（Create Application Profile）] ダイアログボックスで、次の手順を実行します。

ステップ 6 **[説明（Description）]** フィールドに説明を入力します。

ステップ 7 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用した VRF の作成

このセクションでは、Cisco Cloud APIC GUI を使用した VRF の作成方法について説明します。

始める前に

テナントを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[VRF の作成（Create VRF）]** をクリックします。**[VRF の作成（Create VRF）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[VRF* ダイアログボックスの作成（*Create VRF*）*]* ダイアログボックスのフィールドの表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *2 : [VRF* の作成（*Create VRF*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	**[Name]** フィールドに、VRF の表示名を入力します。 すべての VRF に *vrfEncoded* 値が割り当てられます。テナントと VRF 名の組み合わせが 32 文字を超える場合、VRF 名（テナント名も含む）は *vrfEncoded* 値を使用してクラウド ルータで識別されます。*vrfEncoded* 値を表示するには、**[Application Management]** > **[VRFs]** サブタブに移動します。右側のペインで VRF をクリックし、クラウド ルータで *[Encoded VRF Name]* を探します。

[プロパティ（Properties）]	説明
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[VRF の作成（Create VRF）]** ダイアログボックスに戻ります。
説明	VRF の説明を入力します。

ステップ 5 作業が完了したら、[保存（Save）] をクリックします。

Cisco Cloud APIC GUI を使用した外部ネットワークの作成

この手順は、外部ポリシーの作成方法を示しています。オンプレミス サイトの複数のルータに接続できる単一の外部ネットワーク、または CCR への接続に使用できる複数の VRF を持つ複数の外部ネットワークを設定できます。

始める前に

外部ネットワークを作成する前に、ハブ ネットワークを作成しておく必要があります。

ステップ 1 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）]** > **[外部ネットワーク（External Networks）]**に移動します。
構成された外部ネットワークが表示されます。

ステップ 2 **[アクション（Actions）]** をクリックし、**[外部ネットワークの作成（Create External Network）]** を選択します。
[外部ネットワークの作成（Create External Network）] ウィンドウが表示されます。

ステップ 3 次の *[外部ネットワークの作成ダイアログボックスのフィールド（Create External Network Dialog Box Fields）]* の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *3 : [外部ネットワークの作成（Create External Network）] ダイアログボックスのフィールド*

[プロパティ（Properties）]	説明
全般	
名前	外部ネットワーク名を入力します。

[プロパティ（Properties）]	説明
VRF	この 外部 VRF は、外部の非 ACI デバイスとの外部接続に使用されます。この目的で複数の外部 VRF を作成できます。 この VRF は、VRF が次の 3 つの特性をすべて備えている場合に 外部 VRF として識別されます。 • インフラ テナントの下で構成された • 外部ネットワークに関連付けられている • クラウド コンテキスト プロファイルに関連付けられていない 外部ネットワークに関連付けられているVRFはすべて 外部 VRF になります。外部 VRF をクラウド コンテキスト プロファイルまたはサブネットに関連付けることはできません。 外部 VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。 [+ VRF の作成（+ Create VRF）] オプションを使用してVRFを作成することもできます。 3. **[選択（Select）]**をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。
ホスト ルーター名	このフィールドは編集できません。デフォルトのホスト ルータが自動的に選択されます。
[設定（Settings）]	
地域	リージョンを選択するには: 1. **[地域の追加（Add Region）]** をクリックします。 **[地域の選択（Select Regions）]** ダイアログボックスが表示されます。 初回セットアップの一部として選択した地域がここに表示されます。 2. **[地域の選択（Select Regions）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。

[プロパティ（**Properties**）]	説明
VPN ネットワーク	

[プロパティ（Properties）]	説明
	VPN ネットワーク エントリは、外部接続に使用されます。設定されたすべてのVPNネットワークが、選択したすべてのリージョンに適用されます。 VPN ネットワークを追加するには、次の手順を実行します。 **1.** **[VPNネットワークの追加（Add VPN Network）]** をタップします。 **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスが表示されます。 **2.** **[名前（Name）]** フィールドに VPN ネットワークの名前を入力します。 **3.** **[+ IPSec ピアの追加（+ Add IPSec Peer）]** をクリックします。 IPSec ピア エントリごとにトンネルが作成されます。 **4.** 追加する IPSec トンネルの次のフィールドに値を入力します。 • **IPSec トンネル ピアの パブリック IP** • **事前共有キー** • **IKE Version**：IPSec トンネル接続用に **ikev1** または **ikev2** を選択します。 • **BGP ピア ASN** • **Subnet Pool Name**：**[サブネット プール名の選択（Select Subnet Pool Name）]** をクリックします。 **[サブネット プール名の選択（Select Subnet Pool Name）]** ダイアログボックスが表示されます。リストされている使用可能なサブネット プールのいずれかを選択し、**[選択（Select）]** をクリックします。 （注） 必要に応じて、追加の IPsec トンネル サブネット プールを [外部ネットワーク] ページに追加するか、Cloud APIC の初回セットアップを介して追加できます。For more information on adding additional subnet pools through the Cloud APIC First Time Set Up, see the chapter "Configuring Cisco Cloud APIC Using the Setup Wizard" in the *Cisco Cloud APIC for Azure Installation Guide*, Release 25.0(1)-25.0(4) and later. サブネット プールのサイズは、作成される IPsec トンネルの数に対応できる十分な大きさにする必要があります。 • **IPsec トンネル ソース インターフェイス**: このフィールドのエントリを使用して、Cisco Cloud APIC は、選択された各ソース インターフェイスから接続先 IP アドレスへの 1 つの IPsec トンネルを作成します。 （注） **ikev2** は、このフィールドのデフォルト オプションです。IPsec トンネル ソース インターフェイス機能は、IKEv2 構成でのみサポートされます。 **gig3** は、デフォルトで選択されます。次の中から1つまたは複数のインターフェイスを選択します • **gig2**: GigabitEthernet2 インターフェイス

[プロパティ（Properties）]	説明
	• **gig3**: GigabitEthernet3 インターフェイス • **gig4**: GigabitEthernet4 インターフェイス （注） この外部ネットワークで IPsec トンネル ソース インターフェイスを構成した後、ルーティング ポリシー: リリース 25.0(2)で説明されているように、同じ接続先へのトンネルを形成できる追加のネットワークで IPsec トンネル ソース インターフェイスを構成できます。 **5.** この IPSec トンネルを追加するには、チェックマークをクリックします。 別の IPSec トンネルを追加する場合は、**[+ IPSec トンネルの追加（+ Add IPSec Tunnel）]** をクリックします。 **6.** **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスで **[追加（Add）]** をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。

ステップ 4 外部ネットワークの作成が完了したら、**[保存（Save）]** をクリックします。
[外部ネットワークの作成（Create External Network）] ウィンドウで **[保存（Save）]** をクリックすると、クラウド ルータが AWS で構成されます。

グローバル VRF 間ルート リーク ポリシーの構成

グローバル VRF 間ルート リーク ポリシー機能は、リリース 25.0(2) で導入されました。

始める前に

[クラウド APIC セットアップ（Cloud APIC Setup）] ウィンドウの **[コントラクト ベース ルーティング（Contract Based Routing）]** 領域で変更を行う前に、 内部 VRF 間のルート リークで提供された情報を確認してください。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[構成（Configuration）]** を選択します。

オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]**メニューの**[構成（Configuration）]**リストで、**[クラウド APIC セットアップ（Cloud APIC Setup）]** をクリックします。
[セットアップ - 概要] ダイアログ ボックスが表示されます。

ステップ 4 **[コントラクト ベースのルーティング]** 領域で、**[コントラクト ベースのルーティング]** フィールドの現在の設定を書き留めます。

[コントラクト ベースのルーティング] 設定は、現在の内部 VRF ルート リーク ポリシーを反映しています。これは、インフラ テナントの下のグローバル ポリシーであり、ブール フラグを使用して、コントラクトがルート マップがない場合にルートを駆動できるかどうかを示します。

- **オフ**: デフォルト設定。ルートがコントラクトに基づいてリークされておらず、代わりにルート マップに基づいてリークされていることを示します。
- **オン（On）**: ルート マップが存在しない場合に、契約に基づいてルートが漏洩していることを示します。有効に設定されている場合、ルート マップが構成されていないときに、ドライブ回送を契約します。ルート マップが存在するときに、ルート マップは常にドライブ回送です。

ステップ 5 **[コントラクト ベースのルーティング]** フィールドの現在の設定を変更するかどうかを決定します。

ある設定から別の設定に切り替える場合は、次の手順に従います。

- **オン設定からオフへの切り替え (コントラクト ベースのルーティングを無効にする)**: この状況では、現在、コントラクトベースのルーティングが構成されており、ルートマップベースのルーティングに切り替えることが想定されています。コントラクトベースのルーティングからルート マップベースのルーティングに切り替える前にマップ ベースのルーティングが構成されていない場合、これは混乱を招く可能性があります。

  この状況で**オン**設定から**オフ**設定に切り替える前に、次の変更を行います。

  1. 既存のコントラクトを持つ VRF のすべてのペア間で、ルート マップ ベースのルート リークを有効にします。

     Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定 （15 ページ） の手順を実行します。

  2. グローバル ポリシーでコントラクト ベースのルート ポリシーを無効にします。

     [コントラクト ベースのルーティング] フィールドのスイッチを **[オン]** 設定から **[オフ]** 設定に切り替えて、契約ベースのルーティングからルート マップ ベースのルーティングに切り替えます。

  3. 有効にした新しいルート マップ ベースのルーティングに基づいて必要な粒度を反映するようにルーティングを変更します。

- **オフ設定からオンへの切り替え（コントラクトベースのルーティングを有効にする）**：この状況では、現在マップ ベースのルーティングが構成されており、コントラクトベースのルーティングに切り替えることが想定されています。コントラクトとルート マップの両方を VRF のペア間で有効にできるため、これは中断を伴う操作ではなく、付加的な操作です。このような状況では、ルーティングを有効にするときに、コントラクトよりもルートマップが優先されます。マップ ベースのルーティングが有効になっている場合、コントラクト ベースのルーティングを追加しても中断は発生しません。

  そのため、この状況では、**オフ**設定から**オン**設定に切り替える前に変更を行う必要はありません。ただし、VRF のペア間でコントラクトとルート マップの両方を有効にせず、完全にコントラクト ベース ルーティングに移行する場合は、VRF 間のコントラクトを完全に設定し、**[コントラクト ベースの**

ルーティング] フィールドで **[オン]** 設定に切り替える前に VRF 間のルート マップを削除する必要があります。

ステップ 6 **[コントラクト ベースのルーティング]** 領域の現在の設定を変更する場合は、必要なルーティングのタイプに基づいて設定を切り替えます。

ステップ 7 **Cloud APIC セットアップ**の構成が完了したら、**[完了]** をクリックします。

Cisco Cloud APIC GUI を使用したリーク ルートの構成

Cisco Cloud APIC GUI を使用してリーク ルートを設定する手順は、リリースによって若干異なります。

- 25.0(2) より前のリリースでは、独立したルーティング ポリシーを設定して、外部接続機能を使用して ACI クラウド サイトと外部宛先の間のルーティングを設定するときに、内部 VRF と外部 VRF の間でリークするルートを指定できます。これらの手順については、Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定 （15 ページ） を参照してください。
- リリース 25.0(2) 以降では、内部 VRF のペア間のルート マップベースのルート リークがサポートされています。これらの手順については、Cisco Cloud APIC GUI を使用した内部 VRF のリーク ルートの構成 （18 ページ） を参照してください。

Cisco Cloud APIC GUI を使用した VRF間 ルート リークの設定

リーク ルートの設定は、ルーティング ポリシーとセキュリティ ポリシーが別々に設定されるリリース 25.0(1) アップデートの一部です。VRF 間ルーティングを使用すると、独立したルーティング ポリシーを設定して、外部接続機能を使用して ACI クラウド サイトと外部宛先との間のルーティングを設定するときに、内部 VRF と外部 VRF の間でリークするルートを指定できます。詳細については、「サポートされているルーティングとセキュリティ ポリシーの概要」を参照してください。

外部宛先は、Azure サイトから外部デバイスへの接続を有効にする （21 ページ） 手順を使用して手動で構成する必要があります。外部の接続先は、別のクラウドサイト、ACI オンプレミス サイト、または分散拠点である可能性があります。

（注）
- これら手順を使用して、セキュリティポリシーとは無関係に、内部と 外部 VRF の間でのみルーティング ポリシーを構成します。
- これらの手順を使用して、内部 VRF のペア間のルーティングを設定しないでください。その場合、リリース 25.0(1) より前の通常どおりにコントラクトを使用します。

ステップ 1 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）]** > **[VRF]**に移動します。
設定された VRF が表示されます。

ステップ 2 **[リーク ルート（Leak Routes）]** タブをクリックします。
すでに構成されているリーク ルートが表示されます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[リーク ルートの作成（Create Leak Route）]** を選択します。
[リーク ルートの作成（Create a Leak Route）] ウィンドウが表示されます。

ステップ 4 次の *[リーク ルートの作成ダイアログボックスのフィールド（Leak Routes Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *4*: リーク ルートの作成ダイアログボックスのフィールド（*Leak Routes Dailog Box Fields*）

[プロパティ（Properties）]	説明
送信元VRF	送信元 VRF を選択するには： 1. **[送信元 VRF の選択（Select Source VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、送信元 VRF に使用するために左側の列の VRF をクリックして選択してます。 送信元 VRF は、内部または 外部 VRF であることに注意してください。 3. **[選択（Select）]** をクリックして、この送信元 VRF を選択します。 **[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。
宛先 VRF	宛先 VRF を選択するには、次の手順を実行します。 1. **[宛先の選択（Select destination）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、宛先 VRF に使用するために左側の列の VRF をクリックして選択してます。 送信元 VRF も内部 VRF である場合、接続先 VRF を内部 VRF にすることはできないことに注意してください。 3. **[選択（Select）]** をクリックして、この宛先 VRF を選択します。 **[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
タイプ	構成するリーク ルートのタイプを選択します。 • **すべてをリーク**: 接続元 VRF から接続先 VRF にリークするために、すべてのルートを構成することを選択します。 この場合、デフォルトでは、エントリ `0.0.0.0/0` がサブネット IP エリアに自動的に入力されます。 • **サブネット IP**：接続元VRFから接続先VRFまでのリークのルートとして特定のサブネット IP アドレスを設定する場合に選択します。**[サブネット IP（Subnet IP）]** ダイアログ ボックスが表示されます。 **[サブネット IP（Subnet IP）]** ボックスに、VRF 間のリークのルートとしてサブネット IP アドレスを入力します。

ステップ 5 作業が完了したら、[保存（Save）] をクリックします。
[成功（Success）] ウィンドウが表示されます。

ステップ 6 追加の VRF 間ルート リークを設定するかどうかを決定します。

- VRF のペア間でリークする別のルートを追加する場合は、**[成功（Success）]** ウィンドウで **[別のリーク ルートの追加（Add Another Leak Route）]** オプションをクリックします。

  [リーク ルートの追加（Add Leak Route）] ウィンドウに戻ります。VRF のペア間でリークする別のルートを設定するには、ステップ 4 （16 ページ）ーステップ 5 （17 ページ） を繰り返します。

- リバース ルートを追加する場合は、次のようにします。
  - 以前の設定の宛先 VRF が送信元 VRF になり、
  - 以前の設定の送信元 VRF が宛先 VRF になります。

  次に、**[成功（Success）]** ウィンドウで **[リバース リーク ルートの追加（Add Reverse Leak Route）]** オプションをクリックします。

  [リーク ルートの追加（Add Leak Route）] ウィンドウに戻ります。ステップ 4 （16 ページ）ーステップ 5 （17 ページ） を繰り返して別のルートを設定しますが、今度は次のようになります。
  - **[送信元 VRF（Source VRF）]** フィールドで、前の設定で宛先 VRF として選択したVRF を選択します。
  - **[宛先 VRF（Destination VRF）]** フィールドで、前の設定で送信元 VRF として選択した VRF を選択します。

ステップ 7 リーク ルートの設定が完了したら、**[完了（Done）]** をクリックします。

メイン **VRF** ページの **[リーク ルート（Leak Routes）]**タブが再び表示され、新しく設定されたリーク ルートが表示されます。

ステップ 8 送信元または宛先VRFの詳細情報を取得したり、構成済みのリークルートを変更したりするには、メイン **[VRF]** ページの**[リーク ルート（Leak Routes）]** タブで [VRF] をダブルクリックします。
そのルート テーブルの **[概要（Overview）]** ページが表示されます。

ステップ 9 [VRF] ページの上部にある **[アプリケーション管理（Application Management）]** タブをクリックし、左側のナビゲーションバーで**[リーク ルート（Leak Routes）]**タブをクリックします。
この特定の VRF に関連付けられているリーク ルートが表示されます。

ステップ 10 必要に応じて、この VRF に関連付けられた追加のリーク ルートを設定します。

- このVRFからリークルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> からリーク ルートを追加（Add Leak Route from <VRF_name>）]**を選択します。

  [リーク ルートの追加（Add Leak Router）] ウィンドウが表示されます。ステップ 4 （16 ページ）の情報を使用して、必要な情報を入力します。**送信元VRF**のエントリは事前に選択されており、この状況では変更できないことに注意してください。

- この VRF にリークルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> にリーク ルートを追加（Add Leak Route to <VRF_name>）]**を選択します。

  [リーク ルートの追加（Add Leak Router）] ウィンドウが表示されます。ステップ 4 （16 ページ）の情報を使用して、必要な情報を入力します。**宛先VRF**のエントリは事前に選択されており、この状況では変更できないことに注意してください。

次のタスク

これでルーティング ポリシーが構成されました。ルーティング ポリシーとセキュリティ ポリシーは別であるため、セキュリティ ポリシーを別個に構成する必要があります。

- Cisco Cloud APIC GUI を使用した外部 EPG の作成 （31 ページ）: 次の手順を使用して、外部 EPG を作成します。
- Cisco Cloud APIC GUI を使用したコントラクトの作成 （55 ページ）: これらの手順を使用して、外部 EPG とクラウド EPG 間のコントラクトを作成します。

Cisco Cloud APIC GUI を使用した内部 VRF のリーク ルートの構成

リリース 25.0(2) 以降、内部 VRF 間のルート リーク で説明されているように、内部 VRF のペア間のルートマップベースのルートリークがサポートされます。この機能は、リリース25.0(1)で提供されたルーティングとセキュリティの分割更新を拡張したもので、ルーティングとセキュリティ ポリシーが別々に設定されています。

ステップ 1 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）]** > **[VRF]**に移動します。
設定された VRF が表示されます。

ステップ 2 **[リーク ルート（Leak Routes）]** タブをクリックします。
すでに構成されているリーク ルートが表示されます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[リーク ルートの作成（Create Leak Route）]** を選択します。**[リーク ルートの作成（Create a Leak Route）]** ウィンドウが表示されます。

ステップ 4 次の *[リーク ルートの作成ダイアログボックスのフィールド（Leak Routes Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *5:* リーク ルートの作成ダイアログボックスのフィールド（*Leak Routes Dailog Box Fields*）

[プロパティ（Properties）]	**説明**
送信元VRF	送信元 VRF を選択するには： **1.** **[送信元 VRF の選択（Select Source VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 **2.** **[VRFの選択（Select VRF）]** ダイアログで、送信元 VRF に使用するために左側の列の VRF をクリックして選択してます。 この手順は、内部 VRF のペア間のルート マップ ベースのルート リークのためのものであるため、接続元 VRF には内部 VRF を選択します。 **3.** **[選択（Select）]** をクリックして、この送信元 VRF を選択します。 **[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。
宛先 VRF	宛先 VRF を選択するには、次の手順を実行します。 **1.** **[宛先の選択（Select destination）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 **2.** **[VRFの選択（Select VRF）]** ダイアログで、宛先 VRF に使用するために左側の列の VRF をクリックして選択してます。 この手順は、内部 VRF のペア間のルート マップ ベースのルート リークのためのものであるため、接続先 VRF には内部 VRF を選択します。 **3.** **[選択（Select）]** をクリックして、この宛先 VRF を選択します。 **[リーク ルートの作成（Create Leak Route）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
タイプ	構成するリーク ルートのタイプを選択します。 • **すべてをリーク**: 接続元 VRF から接続先 VRF にリークするために、すべてのルートを構成することを選択します。 この場合、デフォルトでは、エントリ `0.0.0.0/0` がサブネット IP エリアに自動的に入力されます。 • **サブネット IP**：接続元VRFから接続先VRFまでのリークのルートとして特定のサブネット IP アドレスを設定する場合に選択します。**[サブネット IP（Subnet IP）]** ダイアログ ボックスが表示されます。 **[サブネット IP（Subnet IP）]** ボックスに、VRF 間のリークのルートとしてサブネット IP アドレスを入力します。

ステップ 5 作業が完了したら、[保存（Save）] をクリックします。
[成功（Success）] ウィンドウが表示されます。

ステップ 6 追加の VRF 間ルート リークを設定するかどうかを決定します。

- VRF のペア間でリークする別のルートを追加する場合は、**[成功（Success）]** ウィンドウで **[別のリーク ルートの追加（Add Another Leak Route）]** オプションをクリックします。

  [リーク ルートの追加（Add Leak Route）] ウィンドウに戻ります。VRF のペア間でリークする別のルートを設定するには、ステップ 4 （19 ページ）ーステップ 5 （20 ページ） を繰り返します。

- リバース ルートを追加する場合は、次のようにします。
  - 以前の設定の宛先 VRF が送信元 VRF になり、
  - 以前の設定の送信元 VRF が宛先 VRF になります。

  次に、**[成功（Success）]** ウィンドウで **[リバース リーク ルートの追加（Add Reverse Leak Route）]** オプションをクリックします。

  [リーク ルートの追加（Add Leak Route）] ウィンドウに戻ります。ステップ 4 （19 ページ）ーステップ 5 （20 ページ） を繰り返して別のルートを設定しますが、今度は次のようになります。
  - **[送信元 VRF（Source VRF）]** フィールドで、前の設定で宛先 VRF として選択したVRF を選択します。
  - **[宛先 VRF（Destination VRF）]** フィールドで、前の設定で送信元 VRF として選択した VRF を選択します。

ステップ 7 リーク ルートの設定が完了したら、**[完了（Done）]** をクリックします。

メイン **VRF** ページの **[リーク ルート（Leak Routes）]**タブが再び表示され、新しく設定されたリーク ルートが表示されます。

ステップ 8 送信元または宛先VRFの詳細情報を取得したり、構成済みのリークルートを変更したりするには、メイン **[VRF]** ページの**[リーク ルート（Leak Routes）]** タブで [VRF] をダブルクリックします。
そのルート テーブルの **[概要（Overview）]** ページが表示されます。

ステップ 9 [VRF] ページの上部にある **[アプリケーション管理（Application Management）]** タブをクリックし、左側のナビゲーションバーで**[リーク ルート（Leak Routes）]**タブをクリックします。
この特定の VRF に関連付けられているリーク ルートが表示されます。

ステップ 10 必要に応じて、この VRF に関連付けられた追加のリーク ルートを設定します。

- この VRF からリーク ルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> からリーク ルートを追加（Add Leak Route from <VRF_name>）]**を選択します。

  [リーク ルートの追加（Add Leak Router）] ウィンドウが表示されます。ステップ 4 （19 ページ）の情報を使用して、必要な情報を入力します。**送信元 VRF** のエントリは事前に選択されており、この状況では変更できないことに注意してください。

- この VRF にリークルートを追加するには、**[アクション（Actions）]** をクリックし、**[<VRF_name> にリーク ルートを追加（Add Leak Route to <VRF_name>）]**を選択します。

  [リーク ルートの追加（Add Leak Router）] ウィンドウが表示されます。ステップ 4 （19 ページ）の情報を使用して、必要な情報を入力します。**宛先 VRF** のエントリは事前に選択されており、この状況では変更できないことに注意してください。

Azure サイトから外部デバイスへの接続を有効にする

次の手順に従って、インフラ VNet CCR から IPSec/BGP を使用して任意の外部デバイスへの IPv4 接続を手動で有効にします。

外部デバイス構成ファイルのダウンロード

ステップ 1 Cisco Cloud APIC GUI で、**[ダッシュボード（Dashboard）]** をクリックします。
Cisco Cloud APIC の**ダッシュボード**が表示されます。

ステップ 2 **[インフラストラクチャ]** > **[外部接続]**に移動します。
[外部接続（External Connectivity）] ウィンドウが表示されます。

ステップ 3 **[アクション（Actions）]** > **[外部デバイス構成ファイルのダウンロード（Download External Device Configuration Files）]** をクリックします。
[外部デバイス構成ファイルのダウンロード（Download External Device Configuration Files）] ポップアップが表示されます。

ステップ 4 ダウンロードする外部デバイス構成ファイルを選択し、**[ダウンロード（Download）]** をクリックします。
このアクションにより、CCR への IPv4 接続のための外部デバイスの手動構成に使用する構成情報を含む zip ファイルがダウンロードされます。

Azure サイトから外部デバイスへの接続を有効にする

ステップ 1 インフラ VNet CCR から EVPN を使用しない外部デバイスへの IPv4 接続を手動で有効にするために必要な情報を収集します。

ステップ 2 外部デバイスにログインします。

ステップ 3 外部ネットワーキング デバイスを接続するための構成情報を入力します。

外部デバイス構成ファイルのダウンロード （21 ページ） の手順を使用して外部デバイス構成ファイルをダウンロードした場合、最初のトンネルの構成情報を見つけて、その構成情報を入力します。

最初のトンネルの外部デバイス設定ファイルの例を示します。

```
! The following file contains configuration recommendation to connect an external networking device
 with the cloud ACI Fabric
! The configurations here are provided for an IOS-XE based device. The user is expected to understand
 the configs and make any necessary amends before using them
! on the external device. Cisco does not assume any responsibility for the correctness of the config.

! Tunnel to 128.107.72.122 1.100 [ikev2] for
hctunnIf.acct-[infra]/region-[westus]/context-[overlay-1]-addr-[10.115.9.128/25]/csr-[ct_routerp_westus_0:0]/tunn-34
! USER-DEFINED: please define gig-gateway: GIG-GATEWAY
! USER-DEFINED: please define GigabitEthernet2 if required
! USER-DEFINED: please define tunnel-id: 100 if required
! USER-DEFINED: please define vrf-name: infra:externalvrf1 if required
! USER-DEFINED: please define gig3-public-ip: 13.88.168.176 if 0.0.0.0 ip still not provided by AWS.
! Device:             128.107.72.122
! Tunnel ID:          100
! Tunnel counter:     1
! Tunnel address:     5.16.1.9
! Tunnel Dn:
acct-[infra]/region-[westus]/context-[overlay-1]-addr-[10.115.9.128/25]/csr-[ct_routerp_westus_0:0]/tunn-34
! VRF name:           infra:externalvrf1
! ikev:               ikev2
! Bgp Peer addr:      5.16.1.10
! Bgp Peer asn:       65015
! Gig3 Public ip:     13.88.168.176
! PreShared key:      device1azure
! ikev profile name: ikev2-100

vrf definition infra:externalvrf1
    rd 1:1

    address-family ipv4
        route-target export 64550:1
        route-target import 64550:1
    exit-address-family
exit

crypto ikev2 proposal ikev2-infra:externalvrf1
    encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
    integrity sha512 sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-infra:externalvrf1
    proposal ikev2-infra:externalvrf1
exit

crypto ikev2 keyring keyring-ikev2-100
```

```
    peer peer-ikev2-keyring
        address 13.88.168.176
        pre-shared-key device1azure
    exit
exit

crypto ikev2 profile ikev2-100
    match address local interface GigabitEthernet2
    match identity remote address 13.88.168.176 255.255.255.255
    identity local address 128.107.72.122
    authentication remote pre-share
    authentication local pre-share
    keyring local keyring-ikev2-100
    lifetime 3600
    dpd 10 5 on-demand
exit

crypto ipsec transform-set ikev2-100 esp-gcm 256
    mode tunnel
exit

crypto ipsec profile ikev2-100
    set transform-set ikev2-100
    set pfs group14
    set ikev2-profile ikev2-100
exit

interface Tunnel100
    vrf forwarding infra:externalvrf1
    ip address 5.16.1.10 255.255.255.252
    ip mtu 1400
    ip tcp adjust-mss 1400
    tunnel source GigabitEthernet2
    tunnel mode ipsec ipv4
    tunnel destination 13.88.168.176
    tunnel protection ipsec profile ikev2-100
exit

ip route 13.88.168.176 255.255.255.255 GigabitEthernet2 GIG-GATEWAY

router bgp 65015

address-family ipv4 vrf infra:externalvrf1
    redistribute connected
    maximum-paths eibgp 32

    neighbor 5.16.1.9 remote-as 65008
    neighbor 5.16.1.9 ebgp-multihop 255
    neighbor 5.16.1.9 activate
    neighbor 5.16.1.9 send-community both

    distance bgp 20 200 20
exit-address-family
```

次の図に、外部デバイス構成ファイルで使用される各フィールド セットの詳細を示します。

- 次の図に示すフィールドは、これらの領域の構成に使用されます。
  - vrf definition
  - IPSec global configurations

```
vrf definition Ext-V1
rd 1:10
!
address-family ipv4
  route-target export 64550:10
  route-target import 64550:10
!
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2
lifetime 28800
!
crypto isakmp keepalive 10 10 periodic
crypto isakmp aggressive-mode disable
!
```

VRF Definition

IPSec Global Configurations

- 次の図に示すフィールドは、これらの領域の構成に使用されます。
  - トンネルごとの IPSec および ikev1 構成
  - VRF ネイバーの BGP 設定

```
!
crypto keyring Ext-V1-1000-ike
  pre-shared-key address <50.18.55.126>[cAPIC CSR Gig3 public IP] key <abcdefg12345>
!
crypto isakmp profile Ext-V1-1000-ike
   keyring Ext-V1-1000-ike
   match identity address <50.18.55.126>[cAPIC CSR1 gig3 Public IP] 255.255.255.255
!
crypto ipsec transform-set Ext-V1-1000-ike esp-aes esp-sha-hmac
mode tunnel
!
crypto ipsec profile Ext-V1-1000-ike
set security-association lifetime kilobytes disable
set security-association replay window-size 512
set transform-set Ext-V1-1000-ike
set pfs group14
!
interface Tunnel1000
vrf forwarding Ext-V1
ip address 50.50.0.2[cAPIC CSR BGP Peer Addr] 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1400
tunnel source GigabitEthernet2
tunnel mode ipsec ipv4
tunnel destination <50.18.55.126>[cAPIC CSR1 gig3 Public IP]
tunnel protection ipsec profile Ext-V1-1000-ike
!
router bgp 64550
!
address-family ipv4 vrf Ext-V1
  redistribute connected
  neighbor <50.50.0.1>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
  neighbor 50.50.0.1 ebgp-multihop 255
  neighbor 50.50.0.1 activate
  neighbor 50.50.0.1 send-community both
  neighbor <50.50.0.5>[cAPIC CSR1 Tunnel Inner IP Addr] remote-as 1234
  neighbor 50.50.0.5 ebgp-multihop 255
  neighbor 50.50.0.5 activate
  neighbor 50.50.0.5 send-community both
  distance bgp 20 200 20
!
ip route 50.18.55.126[cAPIC CSR1 gig3 Public IP] 255.255.255.255 GigabitEthernet2 10.10.0.103
```

IPSec and Ikev1
Per Tunnel Configurations

BGP Configurations for VRF Neighbor

- 次の図に示すフィールドは、これらの領域の構成に使用されます。
  - グローバル構成
  - トンネルごとの IPSec および ikev2 の構成

```
crypto ikev2 proposal ikev2-1
 encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
 integrity sha512 sha384 sha256 sha1
 group 24 21 20 19 16 15 14 2
!
crypto ikev2 policy ikev2-1
 proposal ikev2-1
!
crypto ikev2 keyring keyring-ikev2-2000
 peer peer-ikev2-keyring
  address 35.81.94.248 [cAPIC CSR1 gig3 Public IP]
  pre-shared-key abcdefg12345
!
crypto ikev2 profile ikev2-2000
 match address local interface GigabitEthernet3
 match identity remote address 35.81.94.248[cAPIC CSR1 gig3 Public IP] 255.255.255.255
 identity local address 52.53.49.193 [Local Device tunnel source interface Public IP (Gig3 public IP)]
 authentication remote pre-share
 authentication local pre-share
 keyring local keyring-ikev2-2000
 lifetime 3600
 dpd 10 5 on-demand
!
crypto ipsec transform-set ikev2-2000 esp-gcm 256
 mode tunnel
!
crypto ipsec profile ikev2-2000
 set transform-set ikev2-2000
 set pfs group14
 set ikev2-profile ikev2-2000
!
interface Tunnel2000
 vrf forwarding Ext-V1
 ip address 50.50.0.14 [cAPIC CSR1 BGP Peer Addr] 255.255.255.252
 ip mtu 1400
 ip tcp adjust-mss 1400
 tunnel source GigabitEthernet3
 tunnel mode ipsec ipv4
 tunnel destination 35.81.94.248[cAPIC CSR1 gig3 Public IP]
 tunnel protection ipsec profile ikev2-2000
```

Ikev2 Global Configurations

IPSec and Ikev2
Per Tunnel Configurations

ステップ 4 前の手順を繰り返して、追加のトンネルを構成します。

Cisco Cloud APIC GUI を使用した EPG の作成

このセクションの手順を使用して、アプリケーション EPG、外部 EPG、サービス EPG を作成します。使用可能な構成オプションは、作成する EPG のタイプによって異なります。

Cisco Cloud APIC GUI を使用したアプリケーション EPG の作成

このセクションでは、Cisco Cloud APIC GUI を使用したアプリケーション EPG の作成方法を説明します。各サービスは、少なくとも 1 つのコンシューマー EPG と 1 つのプロバイダー EPG を必要とします。

（注） 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。

始める前に

アプリケーション プロファイルと VRF を作成します。

ステップ 1 **インテント** アイコンをクリックします。

[インテント（Intent）] メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[EPG の作成（Create EPG）]** をクリックします。

[EPG の作成（Create EPG）] ダイアログ ボックスが表示されます。

ステップ 4 次の *[EPG* 作成ダイアログボックスのフィールド（*Create EPG Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *6 : [EPG* の作成（*Create EPG***）*]* ダイアログボックスのフィールド**

[プロパティ（Properties）]	説明
全般	
名前	EPG の名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択します。 リリース 5.0(2) 以降では、このセクションで前述したように、インフラ テナントを選択し、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。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
アプリケーション プロファイル	アプリケーション プロファイルを選択します。 1. **[アプリケーション プロファイルの選択（Select Application Profile）]**をクリックします。**[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログ ボックスが表示されます。 2. **[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログで、左側の列のアプリケーション プロファイルをクリックして選択します。 （注） インフラ テナントで EPG を作成する場合、アプリケーション プロファイルはオーバーレイ-1 VRF の EPG で使用されるため、クラウド インフラ アプリケーション プロファイルを選択しないことを推奨します。異なるアプリケーション プロファイルを選択するか、**[アプリケーション プロファイルの作成（Create Application Profile）]** を選択して、新しいプロファイルを作成します。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
説明	EPG の説明を入力します。
[設定（Settings）]	
タイプ	これはアプリケーション EPG であるため、EPG タイプとして **[アプリケーション（Application）]** を選択します。
VRF	VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログ ボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。 インフラ テナントで EPG を作成している場合は、この手順でセカンダリ VRF を選択します。セカンダリ VRF のクラウド EPG は、他のクラウド EPG およびセカンダリ VRF のクラウド外部 EPG と通信でき、他のユーザ テナント VRF のクラウド EPG とも通信できます。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。

[プロパティ（**Properties**）]	説明
エンドポイントセレクタ	

[プロパティ（Properties）]	説明
	（注） エンドポイント セレクタ構成プロセスの一部として Azure で仮想マシンを構成する手順については、Azure での仮想マシンの構成 （72 ページ） を参照してください。 エンドポイント セレクタを追加するには： 1. **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックして、**[エンドポイント セレクタの追加]** ダイアログを開きます。 2. **[エンドポイント セレクタの追加（Add Endpoint Selector）]** ダイアログの **[Name（名前）]** フィールドに名前を入力します。 3. **[セレクタ式（Selector Expression）]** をクリックします。**[キー（Key）]**、**[演算子（Operator）]**、および **[値（Value）]** フィールドが有効になります。 4. **[キー（Key）]** ドロップダウン リストをクリックしてキーを選択します。次のオプションがあります。 • エンドポイント セレクタに IP アドレスまたはサブネットを使用する場合は、**[IP]** を選択します。 （注） IPv6はAzureではサポートされていません。Cisco Cloud APICこのフィールドには有効なIPv4アドレスを使用する必要があります。 • エンドポイント セレクタに Azure リージョンを使用する場合は、**[リージョン（Region）]** を選択します。 • エンドポイント セレクタのカスタム キーを作成する場合は、**[カスタム（Custom）]** を選択します。 （注） **[カスタム（Custom）]** オプションを選択すると、ドロップダウン リストがテキスト ボックスになります。**custom:** の後にスペースのキーの名前を入力する必要があります（例：**custom: Location**）。 5. **[演算子（Operator）]** ドロップダウン リストから演算子を選択します。次のオプションがあります。 • **[等しい (Equals）]**: 値フィールドに 1 つの値がある場合に使用します。 • **[等しくない（Not Equals）]**: 値フィールドに 1 つの値がある場合に使用されます。 • **[の中にある（In）]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。 • **[の中にない（Not In）]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。 • **[キーを持つ（Has Key）]**: 式にキーのみが含まれている場合に使用されます。 • **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用され

[プロパティ（Properties）]	説明
	ます。 **6.** **[値（Value）]** フィールドに値を入力し、チェックマークをクリックしてエントリを検証します。入力する値は、**[キー（Key）]** フィールドと **[演算子（Operator）]** フィールドで選択した内容によって異なります。たとえば、**[キー（Key）]** フィールドが **[IP]** に設定され、**[演算子（Operator）]** フィールドが **[等しい（equals）]** に設定されている場合、**[値（Value）]** フィールドは IP アドレスまたはサブネットでなければなりません。ただし、**[演算子（Operator）]** フィールドが **[キー（keys）]** に設定されている場合、**[値（Value）]** フィールドは無効になります。 **7.** 完了したら、チェックマークをクリックしてセレクタ式を検証します。 **8.** エンドポイント セレクタに追加のエンドポイント セレクタ式を作成するかどうかを決定します。単一のエンドポイント セレクタで複数の式を作成した場合、それらの式の間には論理 AND があるものとみなされます。 たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。 • エンドポイント セレクタ 1、式 1: • **[キー (Key):]** Region • **演算子（Operator）** : equals • 値：westus • エンドポイント セレクタ1、式 2: • **[キー (Key):]** IP • **演算子 (Operator）** : equals • **[値 (Value):]** 192.0.2.1/24 この場合、これらの式の両方が真になる場合（リージョンが westus で、IP アドレスがサブネット 192.0.2.1/24 に属している場合）に、そのエンドポイントはクラウド EPG に割り当てられます。

[プロパティ（Properties）]	説明
	9. このエンドポイント セレクタで作成するすべての式を追加した後で、 チェックマークをクリックし、終了したら、**[追加（Add）]** をクリックします。 EPG の下で複数のエンドポイント セレクタを作成した場合は、それらのエンドポイント セレクタの間には論理 OR があるものとみなされます。たとえば、前のステップで説明したようにエンドポイント セレクタ 1 を作成し、次に、次に示すように 2 番目のエンドポイント セレクタを作成したとします。 • エンドポイント セレクタ 2、式 1: • **[キー (Key):]** Region • **演算子**： in • **値**： eastus、centralus その場合、次のようになります。 • リージョンが westus で、IP アドレスが 192.0.2.1/24 サブネットに属している（エンドポイント セレクタ 1 の式） または • リージョンが eastus または centralus のどちらかである場合（エンドポイント セレクタ 2 式） その場合、エンドポイントがクラウド EPG に割り当てられます。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用した外部 EPG の作成

このセクションでは、Cisco Cloud APIC GUI を使用したアプリケーション EPG の作成方法を説明します。各サービスには、少なくとも 1 つのコンシューマ EPG と 1 つのプロバイダー EPG が必要です。

（注） 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。

始める前に

アプリケーション プロファイルと VRF を作成します。

ステップ 1 **インテント** アイコンをクリックします。

[インテント（Intent）] メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[EPG の作成（Create EPG）]** をクリックします。

[EPG の作成（Create EPG）] ダイアログ ボックスが表示されます。

ステップ 4 次の *[EPG* 作成ダイアログボックスのフィールド（*Create EPG Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *7: [EPG* の作成（***Create EPG***）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	EPG の名前を入力します。

[プロパティ（Properties）]	説明
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択します。 リリース 5.0(2) 以降では、このセクションで前述したように、インフラ テナントを選択し、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。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
アプリケーション プロファイル	アプリケーション プロファイルを選択します。 1. **[アプリケーション プロファイルの選択（Select Application Profile）]**をクリックします。**[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログ ボックスが表示されます。 2. **[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログで、左側の列のアプリケーション プロファイルをクリックして選択します。 （注） インフラ テナントで EPG を作成する場合、アプリケーション プロファイルはオーバーレイ-1 VRF の EPG で使用されるため、クラウド インフラ アプリケーション プロファイルを選択しないことを推奨します。異なるアプリケーション プロファイルを選択するか、**[アプリケーション プロファイルの作成（Create Application Profile）]** を選択して、新しいプロファイルを作成します。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
説明	EPG の説明を入力します。
[設定（Settings）]	
タイプ	これは外部 EPG であるため、EPG タイプとして **[外部（External）]** を選択します。

[プロパティ（Properties）]	説明
VRF	VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。 インフラ テナントで EPG を作成している場合は、この手順でセカンダリ VRF を選択します。セカンダリ VRF のクラウド EPG は、他のクラウド EPG およびセカンダリ VRF のクラウド外部 EPG と通信でき、他のユーザ テナント VRF のクラウド EPG とも通信できます。 3. **[選択（Select）]** をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
ルート到達可能性	外部 EPG のルート到達可能性のタイプを選択します。次のオプションがあります。 • **インターネット** • **外部サイト**

[プロパティ（Properties）]	説明
エンドポイントセレクタ	（注） エンドポイント セレクタ構成プロセスの一部として Azure で仮想マシンを構成する手順については、Azure での仮想マシンの構成 （72 ページ） を参照してください。 エンドポイント セレクタを追加するには： 1. **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックして、エンドポイント セレクタを追加します。 2. [名前（Name）] フィールドに名前を入力します。 3. **サブネット**にサブネットを入力します。 （注） IPv6はAzureではサポートされていません。Cisco Cloud APICこのフィールドには有効なIPv4アドレスを使用する必要があります。 4. 終了したら、チェックマークをクリックしてエンドポイント セレクタを検証します。 5. 追加のエンドポイント セレクタを作成するかどうかを決定します。 EPG の下で複数のエンドポイント セレクタを作成した場合は、それらのエンドポイント セレクタの間には論理 OR があるものとみなされます。たとえば、2 つのエンドポイント セレクタを作成したとします。 • エンドポイントセレクタ 1： • **名前**：EP_Sel_1 • **サブネット**：192.1.1.1/24 • エンドポイント セレクタ 2： • **名前**：EP_Sel_2 • **サブネット**：192.2.2.2/24 その場合、次のようになります。 • IP アドレスが 192.1.1.1/24 サブネット（エンドポイント セレクタ 1）に属する場合 または • IPアドレスが 192.2.2.2/24 サブネット（エンドポイント セレクタ 2）に属する場合 その場合、エンドポイントがクラウド EPG に割り当てられます。

ステップ 5 設定が終わったら [Save] をクリックします。

サービス EPG の作成

次のセクションの手順を使用して、サービス EPG を作成します。

サービス EPG を構成する前に実行するタスク

サービス EPG を構成する前に、事前に実行する必要がある特定のタスクがあります。サービス EPG でサブネットまたはプライベート リンク ラベルを使用している場合は、最初にサービス EPG の外部にサブネットまたはプライベート リンク ラベルを構成する必要があります。

ステップ 1 必要に応じて VRF を作成します。

a) **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

b) **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

c) **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[VRF の作成（Create VRF）]** をクリックします。**[VRF の作成（Create VRF）]** ダイアログ ボックスが表示されます。

d) 次のように選択します。

- **[名前（Name）]** : VRF の名前を入力します。
- **[テナント（Tenant）]** : テナントを選択します。

e) [保存（Save）] をクリックします。

ステップ 2 クラウド コンテキスト プロファイルを構成します。

a) **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

b) **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

c) **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[クラウド コントラクト プロファイルの作成（Create Cloud Context Profile）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログ ボックスが表示されます。

ステップ 3 次の *[クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド（Create Cloud Context Profile Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *8:* クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（**Name**）	クラウド コンテキスト プロファイルの名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスで、次の手順を実行します。
説明	クラウド コンテキスト プロファイルの説明を入力します。
Settings	
リージョン（**Region**）	リージョンを選択するには: 1. **[リージョンの選択（Select Region）]** をクリックします。**[リージョンの選択（Select Region）]** ダイアログボックスが表示されます。 2. **[リージョンの選択（Select Region）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスで、次の手順を実行します。
VRF	VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRF の選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
CIDR の追加（Add CIDR）	

[プロパティ（Properties）]	説明
	（注） VNet ピアリングが有効になっている場合、CIDR を追加、削除、または編集することはできません。CIDR を追加、削除、または編集する前に、VNet ピアリングを無効にする必要があります。VNet ピアリングを無効にするには： • インフラ テナントの場合は、クラウド コンテキスト プロファイルの **[ハブ ネットワーク ピアリング（Hub Network Peering）]** オプションを無効にします。 • ユーザ（非インフラ）テナントの場合、クラウド コンテキスト プロファイルの **[VNet ピアリング（VNet Peering）]** オプションを無効にします。 CIDR 構成を変更したら、VNet ピアリングを再度有効にします。 次の機能はリリースによってサポートされます。 • インフラ VNet の追加のセカンダリ CIDR およびサブネットを追加することもできます（クラウド テンプレートで作成された `cloudCtxProfiles`）。プライマリ CIDR を追加したり、クラウド テンプレートによって作成された既存の CIDR を変更したりすることはできません。ユーザが作成した CIDR の下にサブネットが作成されると、サブネットは暗黙的にセカンダリ VRF にマッピングされます。 • インフラ VNet 以外の VNet のセカンダリ CIDR とサブネットを追加することもできます。 詳細については、「単一 VNet での複数の VRF のサポート」を参照してください。 CIDR を追加するには、次の手順を実行します。 1. **[CIDR の追加（Add CIDR）]** をクリックします。**[CIDR の追加（Add CIDR）]** ダイアログボックスが表示されます。 2. **[CIDR ブロック範囲（CIDR Block Range）]** フィールドにアドレスを入力します。 3. **[プライマリ（Primary）]** チェックボックスをオン（有効）またはオフ（無効）にします。 追加のセカンダリ CIDR および VNet のサブネットを追加している場合、**[プライマリ（Primary）]** ボックスのチェックを外します。 4. **[サブネットの追加（Add Subnet）]** をクリックして、次の情報を入力します。 • **[アドレス（Address）]** フィールドに、サブネット アドレスを入力します。 • [名前（Name）] フィールドに、このサブネットの名前を入力します。 • **[プライベート リンク ラベル（Private Link Label）]** フィールドで、**[新規作成（Create New）]** を選択し、プライベート リンク ラベルの固有の名前を入力し、このサブネットに関連付けます。 5. **[VRF]** フィールドで、必要に応じて選択します。 • **[プライマリ（Primary）]** フィールドの横にあるボックスをオンにすると、この CIDR は自動的にプライマリ VRF に関連付けられます。

[プロパティ（Properties）]	説明
	• **[プライマリ（Primary）]**フィールドの横にあるチェックボックスをオンにしなかった場合は、この CIDR をセカンダリ VRF に関連付けることができます。VRFの横にある **[X]** をクリックし、**[VRF の選択（Select VRF）]** をクリックして、この CIDR に関連付けるセカンダリ VRF を選択します。 **6.** 完了したら、**[追加（Add）]** をクリックします。
[VNet ゲートウェイ ルータ（VNet Gateway Router）]	クリックして**[VNet ゲートウェイ ルータ（VNet Gateway Router）]**チェックボックスをチェック（有効）またはチェックを外します（無効）。
VNET ピアリング	クリックして、Azure VNet ピアリング機能をオン（有効）またはオフ（無効）にします。 VNetピアリング機能の詳細については、Cisco Cloud APICドキュメンテーションページの「Configuring VNet Peering for Cloud APIC for Azure」を参照してください。https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/series.html#Configuration

ステップ 4 [保存（Save）] をクリックします。

Cisco Cloud APIC GUI を使用したサービス EPG の作成

このセクションでは、Cisco Cloud APIC GUI を使用したサービス EPG の作成方法を説明します。各サービスには、少なくとも 1 つのコンシューマ EPG と 1 つのプロバイダー EPG が必要です。

始める前に

- クラウド サービスエンドポイント グループの情報を確認してください。
- **サブネットごとの NSG** 構成が有効になっていることを確認します。

  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」を参照してください。
- アプリケーション プロファイルと VRF を作成します。

ステップ 1 **インテント** アイコンをクリックします。

[インテント（Intent）] メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[EPG の作成（Create EPG）]** をクリックします。

[EPG の作成（Create EPG）] ダイアログ ボックスが表示されます。

ステップ 4 次の *[EPG* 作成ダイアログボックスのフィールド（*Create EPG Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *9 : [EPG* の作成（*Create EPG*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
全般	
名前	EPG の名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択します。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
アプリケーションプロファイル	アプリケーション プロファイルを選択します。 1. **[アプリケーション プロファイルの選択（Select Application Profile）]**をクリックします。**[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログ ボックスが表示されます。 2. **[アプリケーション プロファイルの選択（Select Application Profile）]** ダイアログで、左側の列のアプリケーション プロファイルをクリックして選択します。 （注） インフラテナントでサービスEPGを作成する場合、アプリケーションプロファイルはオーバーレイ-1 VRF の EPG で使用されるため、`cloud-infra` アプリケーションプロファイルを選択しないことを推奨します。異なるアプリケーションプロファイルを選択するか、**[アプリケーション プロファイルの作成（Create Application Profile）]** を選択して、新しいプロファイルを作成します。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
説明	EPG の説明を入力します。

[プロパティ（Properties）]	説明
[設定（Settings）]	
タイプ	これはサービス EPG であるため、EPG タイプとして **[サービス（Service）]** を選択します。
VRF	VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。 3. **[選択（Select）]**をクリックします。**[EPG の作成（Create EPG）]** ダイアログボックスに戻ります。
導入タイプ	EPG 展開タイプを選択します。 サービスは展開モードによって異なります。 • **[クラウドネイティブ（Cloud Native）]**：プロバイダーネットワークに展開されたクラウド ネイティブ サービス • **[クラウドネイティブ管理対象（Cloud Native Managed）]**：ネットワークに展開されたクラウド ネイティブ サービス • **[サードパーティ（Cloud Native Managed）]**：市場からのサードパーティ サービス

[プロパティ（Properties）]	説明
アクセスタイプ	EPG 展開のアクセス タイプを選択します。アクセス タイプは、他のサービスまたは VM がサービスに接続する方法を示します。 選択肢は、**[展開タイプ（Deployment Type）]** フィールドで行った選択によって異なります。 • **[クラウド ネイティブ（Cloud Native）]** 展開タイプ： • **[パブリック（Public）]**：サービスのパブリック IP にアクセスします。 • **[プライベート（Private）]**：プライベート リンクとプライベート エンドポイントを使用してサービスにアクセスします。 • **[クラウド ネイティブ管理対象（Cloud Native Managed）]**展開タイプ： • **[プライベート（Private）]**：管理対象サブネットに展開されたサービスにプライベート IP アドレスのみがある場合は、このタイプを選択します。 • **[パブリックおよびプライベート（Public and Private）]**：パブリック エンドポイントとプライベートエンドポイントを使用してサービスにアクセスします。これは、Cisco Cloud APIC で管理されたサブネットに展開されたときにパブリック IP アドレスも公開するサービスに使用されます。 • **[サードパーティ（Third-Party）]**展開タイプ：**[プライベート（Private）]**は、アクセス タイプとして使用できる唯一のオプションです。これは、サービスが提供する場合、サービスへのプライベート エンドポイントのみを使用することを意味します。

[プロパティ（Properties）]	説明
サービスの種類	Azure サービス タイプを選択します。 特定のサービス タイプは、ある特定の展開タイプでのみサポートされます。特定の展開タイプでサポートされるサービス タイプの詳細については、クラウド サービス エンドポイント グループ を参照してください。 次のオプションがあります。 • **[Azure Storage Blob]**（Azure Storage を参照） • **[Azure SQL]** • **Azure Cosmos DB** • **[Azure Databricks]**（Azure Databricks サービス を参照） • **[Azure Storage]**（Azure Storage を参照） • **[Azure Storage ファイル（Azure Storage File）]**（Azure Storage を参照） • **[Azure Storage キュー（Azure Storage Queue）]**（Azure Storage を参照） • **[Azure Storage テーブル（Azure Storage Table）]**（Azure Storage を参照） • **[Azure Kubernetes サービス（AKS）（Azure Kubernetes Services （AKS）]**（Azure Kubernetes サービス を参照） • **[Azure Active Directory ドメイン サービス（Azure Active Directory Domain Services）]**（Azure Active Directory ドメイン サービス を参照） • **[Azure コンテナ レジストリ（Azure Container Registry）]** • **[Azure ApiManagement サービス（Azure ApiManagement Services）]**（Azure ApiManagement サービスを参照） • **Azure Key Vault** • **[Redis キャッシュ（Redis Cache）]**（Azure Redis キャッシュ を参照） • **[カスタム サービス（Custom Service）]**（**[展開タイプ（Deployment Type）]**として **[サードパーティ（Third-Party）]** を選択した場合に使用します。）

ステップ 5 **[展開タイプ（Deployment Type）]** フィールドで選択した内容に応じて、**[エンドポイント セレクタ（Endpoint Selector）]** エリアに必要な情報を入力します。

- 展開タイプとして **[クラウド ネイティブ（Cloud Native）]** を選択した場合は、展開タイプとしてクラウド ネイティブを構成する （45 ページ） に進みます。
- 展開タイプとして **[クラウド ネイティブ管理対象（Cloud Native Managed）]** を選択した場合は、展開タイプとしてクラウド ネイティブ管理対象を構成する （48 ページ） に進みます。

- 展開タイプとして **[サードパーティ（Third-Party）]** を選択した場合は、展開の種類としてサードパーティを構成する （50 ページ） に進みます。

展開タイプとしてクラウド ネイティブを構成する

このセクションの手順を使用して、サービス EPG の展開タイプとして **[クラウド ネイティブ（Cloud Native）]** を構成します。

始める前に

クラウドネイティブに記載されている情報を確認して、これらの手順を使用する前に実行する必要があるタスクを理解してください。

ステップ 1 これらの手順を開始する前に、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （40 ページ） の手順を完了していることを確認します。

これらの手順は、これらのの手順で展開タイプを構成する前に、`Azure SQL` などのサービス タイプを設定する Cisco Cloud APIC GUI を使用したサービス EPG の作成 （40 ページ） で提供される手順の続きです。

ステップ 2 アクセス タイプとして **[プライベート（Private）]** を選択した場合、**[プライベート リンク ラベルの選択（Select Private Link Label）]** オプションが使用可能になります。

プライベート リンク ラベルは、サブネットをサービス EPG に関連付けるために使用されます。

ステップ 3 **[プライベート リンク ラベルの選択（Select Private Link Label）]** をクリックします。

[プライベート リンク ラベルの選択（Select Private Link Label）] ウィンドウが表示されます。

ステップ 4 適切なプライベート リンク ラベルを検索します。

サービス EPG を構成する前に実行するタスク （36 ページ） で提供されている手順を使用して作成したプライベート リンク ラベルを検索します。

ステップ 5 **[プライベート リンク ラベルの選択（Select Private Link Label）]** ウィンドウで、適切なプライベート リンク ラベルを選択します。

[EPG の作成（Create EPG）] ウィンドウに戻ります。

次に、**[エンドポイント セレクタ（Endpoint Selectors）]** フィールドにエンドポイント セレクタを追加します。

ステップ 6 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックします。

[エンドポイント セレクタの追加（Add Endpoint Selector）] ウィンドウが表示されます。

ステップ 7 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** ウィンドウの **[Name（名前）]** フィールドに名前を入力します。

ステップ 8 **[キー（Key）]** ドロップダウン リストをクリックしてキーを選択します。

次のオプションがあります。

- カスタム エンドポイント セレクタを作成する場合は、**[カスタム（Custom）]** を選択します。
- エンドポイント セレクタに Azure リージョンを使用する場合は、**[リージョン（Region）]** を選択します。
- エンドポイント セレクタにサービス リソースの名前を使用する場合、**[名前（Name）]** を選択します。

  たとえば、`ProdSqlServer` という名前の SQL サーバーを選択するには、これらの手順の後半で、**[キー（Key）]** フィールドで **[名前（Name）]** を選択し、**[値（Value）]** フィールドに `ProdSqlServer` と入力します。
- エンドポイント セレクタにクラウドプロバイダーの ID を使用する場合、**[リソース ID（Resource ID）]** を選択します。

  たとえば、クラウドプロバイダーのリソース ID を使用して SQL サーバーを選択するには、これらの手順の後に **[キー]** フィールドで **[リソース ID（Resouce ID）]** を選択し、セレクタの値（`/subscriptions/{subscription-id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Sql/servers/ProdSqlServer` など）を **[値（Value）]** フィールド入力します。

ステップ 9 **[演算子（Operator）]** ドロップダウン リストから演算子を選択します。

次のオプションがあります。

- **[等しい (Equals）]**: 値フィールドに 1 つの値がある場合に使用します。
- **[等しくない（Not Equals）]**: 値フィールドに 1 つの値がある場合に使用されます。
- **[の中にある（In）]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
- **[の中にない（Not In）]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。
- **[キーを持つ（Has Key）]**: 式にキーのみが含まれている場合に使用されます。
- **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用されます。

ステップ 10 **[値（Value）]** フィールドに値を入力し、チェックマークをクリックしてエントリを検証します。

入力する値は、**[キー（Key）]** フィールドと **[演算子（Operator）]** フィールドで選択した内容によって異なります。

たとえば、**[キー（Key）]** フィールドが **[IP]** に設定され、**[演算子（Operator）]** フィールドが **[等しい（equals）]** に設定されている場合、**[値（Value）]** フィールドは IP アドレスまたはサブネットでなければなりません。ただし、**[演算子（Operator）]** フィールドが **[キー（keys）]** に設定されている場合、**[値（Value）]** フィールドは無効になります。

ステップ 11 完了したら、チェックマークをクリックしてセレクタ式を検証します。

ステップ 12 エンドポイント セレクタに追加のエンドポイント セレクタ式を作成するかどうかを決定します。

単一のエンドポイント セレクタで複数の式を作成した場合、それらの式の間には論理 AND があるものとみなされます。

たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。

- エンドポイント セレクタ 1、式 1:
  - **[キー (Key):]** Region
  - **演算子（Operator）** : equals
  - **値**：`westus`
- エンドポイント セレクタ1、式 2:
  - **キー**： Name
  - **演算子 (Operator）** : equals
  - **値**：`ProdSqlServer`

このケースでは、これらの式の両方が true の場合（リージョンが `westus` であり、リソースに関連付けられた名前が `ProdSqlServer` である場合）、そのエンドポイントはサービス EPG に割り当てられます。

ステップ 13 このエンドポイントセレクタで作成するすべての式を追加した後で、チェックマークをクリックし、終了したら、**[追加（Add）]** をクリックします。

[EPG の作成（Create EPG）] 画面に戻り、新しいエンドポイントセレクタと構成された式が表示されます。

ステップ 14 追加のエンドポイント セレクタを作成する場合は、**[エンドポイント セレクタの追加（Add Endpoint Selector）]** を再度クリックし、これらの手順を繰り返して追加のエンドポイント セレクタを作成します。

EPGの下で複数のエンドポイントセレクタを作成した場合は、それらのエンドポイントセレクタの間には論理 OR があるものとみなされます。たとえば、前のステップで説明したようにエンドポイント セレクタ 1 を作成し、次に、次に示すように 2 番目のエンドポイント セレクタを作成したとします。

- エンドポイント セレクタ 2、式 1:
  - **[キー (Key):]** Region
  - **演算子**： in
  - **値**： `eastus`、`centralus`

その場合、次のようになります。

- リージョンが `westus` であり、リソースに付けられた名前が `ProdSqlServer` である場合（エンドポイント セレクタ 1 式）

  または

- リージョンが `eastus` または `centralus` のどちらかである場合（エンドポイント セレクタ 2 式）

その場合、エンドポイントがサービス EPG に割り当てられます。

ステップ 15 設定が終わったら [Save] をクリックします。

展開タイプとしてクラウド ネイティブ管理対象を構成する

このセクションの手順を使用して、サービス EPG の展開タイプとして **[クラウド ネイティブ管理（Cloud Native Managed）]** を構成します。

始める前に

クラウド ネイティブ管理対象 に記載されている情報を確認して、これらの手順を使用する前に実行する必要があるタスクを理解してください。

ステップ 1 これらの手順を開始する前に、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （40 ページ） の手順を完了していることを確認します。

これらの手順は、これらの手順で展開タイプを構成する前に、`Azure ApiManagement Services` などのサービス タイプを設定する Cisco Cloud APIC GUI を使用したサービス EPG の作成 （40 ページ） で提供される手順の続きです。

ステップ 2 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックします。

[エンドポイント セレクタの追加（Add Endpoint Selector）] ウィンドウが表示されます。

ステップ 3 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** ウィンドウの **[Name（名前）]** フィールドに名前を入力します。

ステップ 4 **[キー（Key）]** ドロップダウン リストをクリックしてキーを選択します。

現時点では、このアクセス タイプのキーとして使用できるオプションは **[IP]** のみです。

（注） IPv6はAzureではサポートされていません。Cisco Cloud APICこのフィールドには有効なIPv4アドレスを使用する必要があります。

ステップ 5 **[演算子（Operator）]** ドロップダウン リストから演算子を選択します。

次のオプションがあります。

- **[等しい (Equals）]**: 値フィールドに 1 つの値がある場合に使用します。
- **[等しくない（Not Equals）]**: 値フィールドに 1 つの値がある場合に使用されます。
- **[の中にある（In）]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
- **[の中にない（Not In）]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。
- **[キーを持つ（Has Key）]**: 式にキーのみが含まれている場合に使用されます。
- **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用されます。

ステップ 6 **[値（Value）]** フィールドに適切な IP アドレスまたはサブネットを入力し、チェックマークをオンにしてエントリを検証します。

サービス EPG を構成する前に実行するタスク （36 ページ） で提供されている手順を使用して作成した IP アドレスまたはサブネットを入力します。

ステップ 7 完了したら、チェックマークをクリックしてセレクタ式を検証します。

ステップ 8 エンドポイント セレクタに追加のエンドポイント セレクタ式を作成するかどうかを決定します。

単一のエンドポイント セレクタで複数の式を作成した場合、それらの式の間には論理 AND があるものとみなされます。

たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。

- エンドポイント セレクタ 1、式 1:
  - **[キー (Key):]** IP
  - **演算子 (Operator）** ： equals
  - **値** ：192.1.1.1/24
- エンドポイント セレクタ1、式 2:
  - **[キー (Key):]** IP
  - **演算子** ： not equals
  - **値** ：192.1.1.2

この場合、これらの式の両方が true の場合（IP アドレスがサブネット 192.1.1.1/24 に属し、IP アドレスが 192.1.1.2 でない場合）、そのエンドポイントはサービス EPG に割り当てられます。

ステップ 9 このエンドポイントセレクタで作成するすべての式を追加した後で、チェックマークをクリックし、終了したら、**[追加（Add）]** をクリックします。

[EPG の作成（Create EPG）] 画面に戻り、新しいエンドポイント セレクタと構成された式が表示されます。

ステップ 10 追加のエンドポイント セレクタを作成する場合は、**[エンドポイント セレクタの追加（Add Endpoint Selector）]** を再度クリックし、これらの手順を繰り返して追加のエンドポイント セレクタを作成します。

EPG の下で複数のエンドポイントセレクタを作成した場合は、それらのエンドポイントセレクタの間には論理 OR があるものとみなされます。たとえば、前のステップで説明したようにエンドポイント セレクタ 1 を作成し、次に、次に示すように 2 番目のエンドポイント セレクタを作成したとします。

- エンドポイント セレクタ 2、式 1:
  - **[キー (Key):]** IP
  - **演算子 (Operator）** ： equals
  - **値** ：192.2.2.2/24

その場合、次のようになります。

- IP アドレスがサブネット 192.1.1.1/24 に属し、IP アドレスが 192.1.1.2 でない場合（エンドポイントセレクタ 1 式）

  または

- IPアドレスがサブネット 192.2.2.2/24 に属する場合

その場合、エンドポイントがサービス EPG に割り当てられます。

ステップ 11 設定が終わったら [Save] をクリックします。

展開の種類としてサードパーティを構成する

このセクションの手順を使用して、サービス EPG の展開タイプとして **[サードパーティ（Third-Party ）]** を構成します。

（注） **[展開タイプ（Deployment Type）]**として **[サードパーティ（Third-Party）]** を選択した場合は、**[サービス タイプ（Service Type）]** として **[カスタム（Custom）]** を選択する必要があります。

ステップ 1 これらの手順を開始する前に、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （40 ページ） の手順を完了していることを確認します。

これらの手順は、Cisco Cloud APIC GUI を使用したサービス EPG の作成 （40 ページ） で提供されている手順の続きであり、これらの手順で展開タイプを構成する前にサービス タイプを `[カスタム サービス（Custom Service）]`として設定します。

ステップ 2 **[サードパーティ（Third-Party）]** の展開タイプのアクセス タイプに必要な選択を行います。

[プライベート（Private）]は、アクセス タイプとして使用できる唯一のオプションです。これは、サービスが提供する場合、サービスへのプライベート エンドポイントのみを使用することを意味します。

[プライベート リンク ラベルの選択（Select Private Link Label）] オプションは、このアクセス タイプで使用できるようになります。プライベート リンク ラベルは、サブネットをサービス EPG に関連付けるために使用されます。

ステップ 3 適切なプライベート リンク ラベルを検索します。

サービス EPG を構成する前に実行するタスク （36 ページ） で提供されている手順を使用して作成したプライベート リンク ラベルを検索します。

ステップ 4 **[プライベート リンク ラベルの選択（Select Private Link Label）]** ウィンドウで、適切なプライベート リンク ラベルを選択します。

[EPG の作成（Create EPG）] ウィンドウに戻ります。

次に、**[エンドポイント セレクタ（Endpoint Selectors）]** フィールドにエンドポイント セレクタを追加します。

ステップ 5 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** をクリックします。

[エンドポイント セレクタの追加（Add Endpoint Selector）] ウィンドウが表示されます。

ステップ 6 **[エンドポイント セレクタの追加（Add Endpoint Selector）]** ウィンドウの **[Name（名前）]** フィールドに名前を入力します。

ステップ 7 **[キー（Key）]** ドロップダウン リストをクリックしてキーを選択します。

現時点では、このアクセス タイプのキーとして使用できるオプションは **[URL]** のみであり、エンドポイント セレクタのサービスを識別するエイリアスまたは完全修飾ドメイン名（FQDN）を使用します。

ステップ 8 **[演算子（Operator）]** ドロップダウン リストから演算子を選択します。

次のオプションがあります。

- **[等しい (Equals）]**: 値フィールドに 1 つの値がある場合に使用します。
- **[等しくない（Not Equals）]**: 値フィールドに 1 つの値がある場合に使用されます。
- **[の中にある（In）]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
- **[の中にない（Not In）]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。
- **[キーを持つ（Has Key）]**: 式にキーのみが含まれている場合に使用されます。
- **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用されます。

ステップ 9 **[値（Value）]** フィールドに有効な URL を入力し、チェックマークをクリックしてエントリを検証します。

ステップ 10 完了したら、チェックマークをクリックしてセレクタ式を検証し、**[追加（Add）]** をクリックします。

[EPG の作成（Create EPG）] 画面に戻り、新しいエンドポイント セレクタと構成された式が表示されます。

ステップ 11 追加のエンドポイント セレクタを作成する場合は、**[エンドポイント セレクタの追加（Add Endpoint Selector）]** を再度クリックし、これらの手順を繰り返して追加のエンドポイント セレクタを作成します。

EPG の下で複数のエンドポイント セレクタを作成した場合は、それらのエンドポイント セレクタの間には論理 OR があるものとみなされます。

たとえば、下で説明しているように 2 つのエンドポイント セレクタを作成したとします。

- エンドポイントセレクタ 1：
  - **キー**： URL
  - **演算子 (Operator）**： equals
  - **値**： `www.acme1.com`
- エンドポイント セレクタ 2：
  - **キー**： URL

- **演算子 (Operator）** ： equals
- **値**： `www.acme2.com`

その場合、次のようになります。

- URL が `www.acme1.com` の場合

  または

- URL が `www.acme2.com` の場合

その場合、エンドポイントがサービス EPG に割り当てられます。

ステップ 12 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したフィルタの作成

このセクションでは、クラウド APIC GUI を使用したフィルタの作成方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[フィルタの作成（Create Fileter）]** をクリックします。**[フィルタの作成（Create Filter）]** ダイアログボックスが表示されます。

ステップ 4 次の *[フィルタの作成ダイアログボックスのフィールド（Create Filter Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *10 :* フィルタの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	**[名前（Name）]** フィールドにハードウェア フィルタの名前を入力します。

[プロパティ（**Properties**）]	説明
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[フィルタの作成（Create ）]** ダイアログボックスに戻ります。
説明	フィルタの説明を入力します。

[プロパティ（Properties）]	説明
フィルタの追加	フィルタを追加するには、次の手順を実行します。 1. **[フィルタ エントリの追加（Add Filter Entry）]** をクリックします。**[フィルタの追加（Add Filter）]** ダイアログボックスが表示されます。 2. **[名前（Name）]** フィールドにフィルタエントリの名前を入力します。 3. **[イーサネット タイプ（Ethernet Type）]** ドロップダウン リストをクリックして、イーサネットタイプを選択します。次のオプションがあります。 • **IP** • **[Unspecified]** （注） **[指定なし（Unspecified）]** を選択すると、IP を含むすべてのトラフィックタイプが許可され、残りのフィールドは無効になります。 4. **[IP プロトコル（IP Protocol）]** ドロップダウンメニューをクリックして、プロトコルを選択します。次のオプションがあります。 • **tcp** • **udp** • **[Unspecified]** （注） 残りのフィールドは、**tcp** または **udp** が選択されている場合にのみ有効になります。 5. **[宛て先ポート（Destination Port）]** フィールドに適切なポート範囲情報を入力します。 6. フィルタエントリ情報の入力が完了したら、**[追加（Add）]** をクリックします。**[フィルタの作成（Create Filter）]** ダイアログボックスに戻り、別のフィルタエントリを追加する手順を繰り返すことができます。

ステップ 5 作業が完了したら、[保存（Save）] をクリックします。

Cisco Cloud APIC GUI を使用したコントラクトの作成

このセクションでは、Cisco Cloud APIC GUI を使用したコントラクトの作成方法について説明します。

始める前に

フィルタを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが**[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[コントラクトの作成（Create Contract）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[*コントラクト ダイアログ ボックス フィールドの作成（*Create Contract Dialog Box Fields*）*]* テーブルにリストされているように、各フィールドに適切な値を入力して続行します。

表 *11 : [*コントラクトの作成（*Create Contract*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	契約の名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択します。 （注） リリース 5.0(2) 以降、インフラテナントでコントラクトを作成できます。共有サービスの使用例では、インフラテナントからコントラクトをエクスポートしたり、インフラテナントにコントラクトをインポートしたりすることもできます。 3. **[選択（Select）]**をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。
説明	コントラクトの説明を入力してください。
[設定（Settings）]	

[プロパティ（Properties）]	説明
スコープ	スコープは、同じアプリケーション プロファイル内、同じ VRF インスタンス内、ファブリック全体（グローバル）、または同じテナント内のエンドポイント グループに契約を制限します。 （注） 共有サービスにより、異なるテナントの EPG 間および異なる VRF の EPG 間の通信が可能になります。 1 つのテナントの EPG が別のテナントの EPG と通信できるようにするには、**[グローバル（Global）]** スコープを選択します。 1 つの VRF の EPG が別の VRF の別の EPG と通信できるようにするには、**[グローバル（Global）]** または **[テナント（Tenant）]** スコープを選択します。 共有サービスの詳細については、共有サービス を参照してください。 ドロップダウン矢印をクリックして、次のスコープ オプションから選択します。 • **アプリケーション プロファイル** • **VRF** • **グローバル** • **テナント**
フィルタの追加	フィルタを選択します。 1. [フィルタの追加（Add Filter）] をクリックします。フィルタ行が表示され、**[フィルタの選択（Select Filter）]** オプションが表示されます。 2. **[フィルタの選択（Select Filter）]** をクリックします。**[フィルタの選択（Select Filter）]** ダイアログボックスが表示されます。 3. **[フィルタの選択（Select Filter）]** ダイアログで、左側の列のフィルタをクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したテナント間コントラクトの作成

このセクションでは、Cisco Cloud APIC GUI を使用したテナント間コントラクトの作成方法について説明します。テナント間コントラクトの作成が必要になる状況の詳細については、共有サービス を参照してください。

始める前に

フィルタを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが**[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[コントラクトの作成（Create Contract）]** をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[*コントラクト ダイアログ ボックス フィールドの作成（*Create Contract Dialog Box Fields*）*]* テーブルにリストされているように、各フィールドに適切な値を入力して続行します。

表 *12 : [*コントラクトの作成（*Create Contract*）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	契約の名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択します。 （注） リリース 5.0(2) 以降、インフラテナントでコントラクトを作成できます。共有サービスの使用例では、インフラテナントからコントラクトをエクスポートしたり、インフラテナントにコントラクトをインポートしたりすることもできます。 3. **[選択（Select）]**をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。
説明	コントラクトの説明を入力してください。
[設定（Settings）]	

[プロパティ（Properties）]	説明
スコープ	スコープは、同じアプリケーション プロファイル内、同じ VRF インスタンス内、ファブリック全体（グローバル）、または同じテナント内のエンドポイント グループに契約を制限します。 テナント間通信の場合は、まずテナントの1つ（**tenant1** など）の**グローバル**スコープとの契約を作成します。このテナントのEPGは、常にこの契約のプロバイダーになります。 このコントラクトは、他のテナント（**tenant2**など）にエクスポートされます。この契約をインポートする他のテナントでは、そのEPGがインポートされた契約のコンシューマになります。**tenant2** の EPG をプロバイダー、tenant1 の EPG をコンシューマにするには、tenant2 でコントラクトを作成し、**tenant1** にエクスポートします。
フィルタの追加	フィルタを選択します。 **1.** [フィルタの追加（Add Filter）] をクリックします。フィルタ行が表示され、**[フィルタの選択（Select Filter）]** オプションが表示されます。 **2.** **[フィルタの選択（Select Filter）]** をクリックします。**[フィルタの選択（Select Filter）]** ダイアログボックスが表示されます。 **3.** **[フィルタの選択（Select Filter）]** ダイアログで、左側の列のフィルタをクリックして選択し、**[選択（Select）]**をクリックします。**[コントラクトの作成（Create Contract）]** ダイアログボックスに戻ります。

ステップ 5 設定が終わったら **[保存（Save）]** をクリックします。

ステップ 6 作成したコントラクトを別のテナントにエクスポートします。

たとえば、次のようなケースがあるとします。

- 上記の手順で作成したコントラクトの名前は、tenant **tenant1** の **contract1** です。
- エクスポートするコントラクトは、**exported_contract1** という名前で、テナント **tenant2** にエクスポートします。

a) [コントラクト（Contracts）] ページ（**[あプリケーション管理（Application Management）]** > **[コントラクト（Contracts）]**）に移動します。

設定されたコントラクトがリストされます。

b) 作成したばかりのコントラクトを選択します。

たとえば、コントラクト **contract1** が表示されるまでリストをスクロールし、その横にあるボックスをクリックして選択します。

c) **[アクション（Actions）]** > **[コントラクトのエクスポート（Export Contract）]**に移動します。

[[コントラクトのエクスポート（Export Contract）] ウィンドウが表示されます。

d) **[テナントの選択（Select Tenant）]** をクリックします。

[テナントの選択（Select Tenant）] ウィンドウが表示されます。

e) 契約をエクスポートするテナントを選択し、**[保存（Save）]** をクリックします。

たとえば、**tenant2** です。**[コントラクトのエクスポート（Export Contract）]** ウィンドウに戻ります。

f) **[名前（Name）]** フィールドに、エクスポートされたコントラクトの名前を入力します。

たとえば、**exported_contract1** です。

g) **[説明（Description）]** フィールドに、コントラクトの説明を入力します。

h) [**保存（Save**）] をクリックします。

コントラクトのリストが再び表示されます。

ステップ 7 最初のテナントの EPG をプロバイダー EPG として設定し、EPG 通信設定の最初の部分として元のコントラクトを設定します。

a) **[インテント（Intent）]** ボタンをクリックし、**[EPG 通信（EPG Communication）]** を選択します。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

b) **[では始めましょう（Let's Get Started）]** をクリックします。

c) **[コントラクト（Contract）]** 領域で、**[コントラクトの選択（Select Contract）]** をクリックします。

[選択（Select）] ウィンドウが表示されます。

d) これらの手順の最初に作成したコントラクトを見つけて選択します。

この例では、**contract1** を見つけて選択します。

e) **[選択（Select）]** をクリックします。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

f) **[プロバイダー EPG（Provider EPGs）]** 領域で、**[プロバイダー EPG の追加（Add Provider EPGs）]** をクリックします。

[プロバイダー EPG の選択（Select Provider EPGs）] ウィンドウが表示されます。

g) **[選択した項目を保持（Keep selected Items）]**チェックボックスをオンのままにして、最初のテナント（**tenant1**）の EPG を選択します。

h) **[選択（Select）]** をクリックします。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

i) [**保存（Save**）] をクリックします。

ステップ 8 2 番目のテナントの EPG をコンシューマ EPG として構成し、エクスポートされたコントラクトを EPG 通信構成の 2 番目の部分として設定します。

a) **[インテント（Intent）]** ボタンをクリックし、**[EPG 通信（EPG Communication）]** を選択します。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

b) **[では始めましょう（Let's Get Started）]** をクリックします。

c) **[コントラクト（Contract）]** 領域で、**[コントラクトの選択（Select Contract）]** をクリックします。

[選択（Select）] ウィンドウが表示されます。

d) これらの手順の最初に作成したコントラクトを見つけて選択します。

この例では、**exported_contract1** を見つけて選択します。

e) **[選択（Select）]** をクリックします。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

f) **[コンシューマー EPG（Consumer EPGs）]** 領域で、**[コンシューマー EPG の追加（Add Consumer EPGs）]** をクリックします。

[コンシューマー EPG の選択（Select Consumer EPGs）] ウィンドウが表示されます。

g) **[選択した項目を保持（Keep selected Items）]** チェックボックスをオンのままにして、2 番目のテナント（**tenant2**）の EPG を選択します。

h) **[選択（Select）]** をクリックします。

[EPG 通信（EPG Communication）] ウィンドウが表示されます。

i) [保存（Save）] をクリックします。

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

セキュリティ グループ で説明されているように、ネットワーク セキュリティ グループの構成方法は、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）。
- 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 Cisco 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）。

（注） Cisco Cloud APIC では、新しい **サブネットごとの NSG** 構成 または 古い **EPG ごとの NSG** 構成を使用できます。同じ Cisco Cloud APIC システムで両方の構成を使用することはできません。

これらの手順では、リリース 5.1(2) 以降の Cisco Cloud APIC に対して、新しい **サブネットごとの NSG** 構成または古い **EPG ごとの NSG** 構成のいずれかを選択する方法について説明します。

始める前に

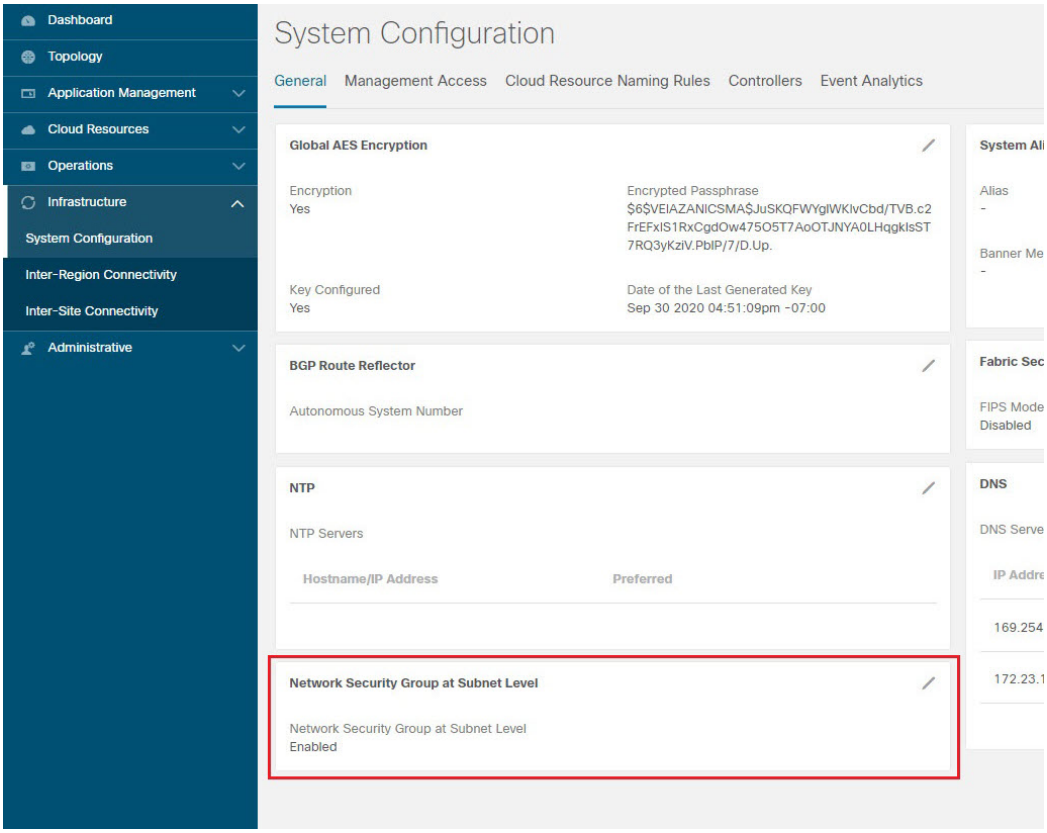
セキュリティ グループ で提供されている情報を確認して、リリースに応じてセキュリティ グループがどのように構成されているかを理解し、セキュリティ グループのガイドラインと制限を理解してください。

ステップ 1 まだログインしていない場合は、Cloud APIC にログインします。

ステップ 2 左のナビゲーション バーで、**[インフラストラクチャ（Infrastructure）]**> > **[システム構成（System Configuration）]**に移動します。

デフォルトでは **[全般（General）]** タブが表示されます。

ステップ 3 **[システム構成（System Configuration）]** ウィンドウの **[全般（General）]** エリアで、**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドを見つけます。



ステップ 4 **[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの現在の構成を確認します。

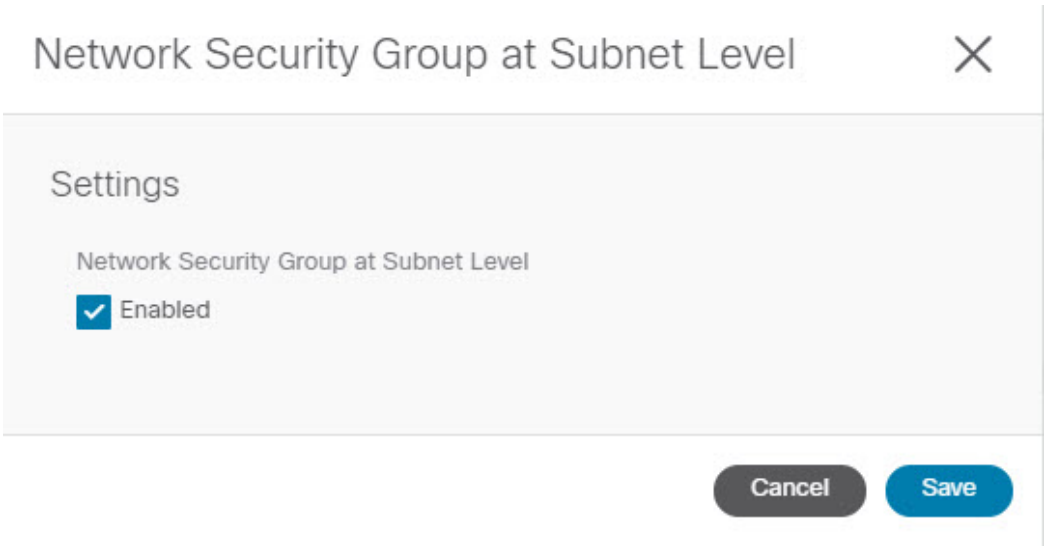
- このフィールドの値として **[有効（Enabled）]** が表示されている場合は、 Cisco Cloud APIC の新しい **サブネットごとの NSG** 構成があることを意味します。
- このフィールドの値として **[無効（Disabled）]** が表示されている場合は、Cisco Cloud APIC に古い **EPG ごとの NSG** 構成があることを意味します。

ステップ 5 **[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの設定を変更するか、そのままにするかを決定します。

必要な構成	既存の構成	アクション
Cisco Cloud APIC の新しい **サブネットごとの NSG** 構成が必要な場合、次のようにします：	**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの値として **[有効（Enabled）]** が表示されている場合は、次のようにします。	Cisco Cloud APIC は、必要な**サブネットごとのNSG**構成ですでにセットアップされています。変更を加える必要はありません。
	[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）] フィールドの値として **[無効（Disabled）]** が表示されている場合は、次のようにします。	**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの設定を変更する必要があります。「ステップ 6（62 ページ）」に進みます。
Cisco Cloud APIC に古い **EPG ごとの NSG** 構成を使用する場合、次のようにします：	**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの値として **[有効（Enabled）]** が表示されている場合は、次のようにします。	**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの設定を変更する必要があります。「ステップ 6（62 ページ）」に進みます。
	[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）] フィールドの値として **[無効（Disabled）]** が表示されている場合は、次のようにします。	Cisco Cloud APIC は、必要な **EPG ごとの NSG** 構成ですでにセットアップされています。変更を加える必要はありません。

ステップ 6 **[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの設定を変更する必要がある場合は、フィールドの右上隅にある鉛筆アイコンをクリックします。

[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）] の **[設定（Settings）]** ウィンドウが表示されます。



ステップ 7 ウィンドウで必要な変更を行います。

（注） ネットワーク セキュリティ グループの設定を変更すると、トラフィックが失われます。ネットワーク セキュリティ グループの設定を変更する必要がある場合は、メンテナンス期間中に変更を行うことをお勧めします。

- Cisco Cloud APIC の新しい**サブネットごとの NSG** 構成が必要で、このウィンドウの **[有効（Enabled）]** フィールドの横にあるボックスにチェックが入っていない場合は、ボックスをクリックしてチェックマークを追加します。これにより、Cisco Cloud APIC の新しい **サブネットごとの NSG** 構成を有効にすることができます。
- Cisco Cloud APIC に古い **EPG ごとの NSG** 構成を使用する必要があり、このウィンドウの **[有効（Enabled）]** フィールドの横にあるボックスにチェックが入っている場合は、ボックスをクリックしてチェック マークを外します。これにより、Cisco Cloud APIC に対して、新しい **サブネットごとの NSG** 構成を無効にし、古い **EPG ごとの NSG** 構成を有効にすることができます。

  次の点に注意してください。

  - 新しい **サブネットごとの NSG** から古い **EPG ごとの NSG** 構成に設定を変更することはお勧めしません。**サブネットごとの NSG** 設定を無効にすると、サービス EPG 構成のサポートが失われ、トラフィックが失われます。
  - サービス EPG またはプライベート リンク ラベルが構成されている場合、**サブネットごとの NSG** 構成を無効にすることはできません。**サブネットごとの NSG** 構成を無効にする前に、構成されたサービス EPG またはプライベート リンク ラベルを無効にする必要があります。
    - 設定されたサービス EPG を無効にするには：
      1. **[アプリケーション管理]**>>**[EPG s]** の順に移動します。
      2. **[タイプ（Type）]** 列に表示されている **[サービス（Service）]** を含む EPG を見つけます。
      3. 削除するサービス EPG を選択し、**[アクション（Actions）]**>>**[EPG の削除（Delete EPG）]** をクリックします。

- 構成されたプライベート リンク ラベルを無効にするには：

1. **[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）]**に移動します。
2. 必要なクラウド コンテキスト プロファイルを見つけて、そのプロファイルをクリックします。

   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。
3. [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。**[CIDR]** エリアの **[サブネット（Subnets）]** 列に、テキスト **Private Link Labels** が表示されます。
4. 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。
5. **[設定（Settings）]** エリアで、もう一度 **[CIDR]** エリアを見つけて、その行の鉛筆アイコンをクリックします。

   [CIDR の編集（Edit CIDR）] ウィンドウが表示されます。
6. **[サブネット（Subnets）]** エリアで、**[プライベート リンク ラベル（Private Link Label）]** 列にエントリがある行を見つけ、そのサブネットの行の鉛筆アイコンをクリックします。

   このサブネット行のエントリが編集可能になります。
7. そのサブネット行の **[プライベート リンク ラベル（Private Link Label）]** 列のエントリの横にある **[X]** をクリックします。

   これにより、プライベート リンク ラベルが削除されます。

ステップ 8 **[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** ウィンドウで必要な変更を行った後、**[保存（Save）]** をクリックします。

[システム構成（System Configuration）] ウィンドウの **[全般（General）]** エリアが再び表示され、**[サブネット レベルのネットワーク セキュリティ グループ（Network Security Group at Subnet Level）]** フィールドの設定に、前の手順で行った変更が反映されます。

セキュリティ グループの詳細の表示

ステップ 1 まだログインしていない場合は、Cisco Cloud APIC GUI にログインします。

ステップ 2 **[クラウド リソース（Cloud Resources）]**> > **[セキュリティ グループ（Security Groups）]**に移動します。

[セキュリティ グループ（Security Groups）] ウィンドウが表示されます。

ステップ 3 詳細を取得するセキュリティ グループのタイプに応じて、**[ネットワーク セキュリティ グループ（Network Security Groups）]**（NSG）タブまたは **[アプリケーション セキュリティ グループ（Application Security Groups）]** ASG タブをクリックします。

各タブには、次の情報が表示されます。

- **[ネットワーク セキュリティ グループ（Network Security Groups）]** タブ：
  - **名前**：ネットワーク セキュリティ グループの名前。
  - **クラウドプロバイダー ID**：ネットワーク セキュリティ グループに関連付けられているクラウドプロバイダー ID。

    [名前（Name）] および **[クラウドプロバイダー ID（Cloud Provider ID）]** フィールドに入力されている値は、NSG が新しいサブネットごとの NSG 構成（**[クラウド プロバイダ ID（Cloud Provider ID）]** の **[subnet-]** として表示）で構成されているか、古い EPG ごとの NSG 構成（**[クラウドプロバイダー ID（Cloud Provider ID）]** 列の **[epg-]**）で構成されているかを示します。ソフトウェア リリースに応じて使用できるさまざまなタイプの NSG 構成の詳細については、セキュリティ グループ を参照してください。
  - **EPG**：以前の EPG ごとの NSG 構成を使用している場合、ネットワーク セキュリティ グループに関連付けられている EPG。
  - **仮想マシン**：ネットワーク セキュリティ グループに関連付けられている仮想マシン。
  - **エンドポイント**：ネットワーク セキュリティ グループに関連付けられているエンドポイント。
  - **サブネット**：新しいサブネットごとの NSG 構成を使用している場合、ネットワーク セキュリティ グループに関連付けられているサブネット。
- **[アプリケーション セキュリティ グループ（Application Security Groups）]** タブ：
  - **正常性**：アプリケーション セキュリティ グループの正常性ステータス。
  - **名前**：アプリケーション セキュリティ グループの名前。
  - **クラウドプロバイダー ID**：アプリケーション セキュリティ グループに関連付けられているクラウドプロバイダー ID。
  - **EPG**：アプリケーション セキュリティ グループに関連付けられている EPG。
  - **仮想マシン**：アプリケーション セキュリティ グループに関連付けられている仮想マシン。
  - **エンドポイント**：アプリケーション セキュリティ グループに関連付けられているエンドポイント。

ステップ 4 いずれかの列の値をクリックして、詳細情報を取得します。

たとえば、**[ネットワーク セキュリティ グループ（Network Security Groups）]** タブの **[名前（Name）]** 列の値をクリックすると、その特定のネットワーク セキュリティ グループに関する詳細情報が表示されます。

このウィンドウで [詳細（Details）] アイコン（）をクリックすると、別のウィンドウが表示され、入力ルールと出力ルールを含むクラウドリソース情報など、このセキュリティ グループの詳細情報が表示されます。

Cisco Cloud APIC を使用したコンシューマおよびプロバイダー EPG の指定

ここでは、EPG をコンシューマまたはプロバイダーとして指定する方法について説明します。

始める前に

- コントラクトを設定できます。
- EPG が設定済みです。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウンをクリックし、**[構成（Configuration）]** を選択します。

[インテント（Intent）] の [構成（Configuration）] オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]**メニューの **[構成（Configuration）]** リストで、**[EPG Communication]** をクリックします。**[EPG通信（EPG Communication）]** ダイアログボックスに、**コンシューマ EPG**、**コントラクト**、および**プロバイダー EPG**の情報が表示されます。

ステップ 4 コントラクトを選択します。

a) **[コントラクトの選択（Select Contract）]** をクリックします。**[コントラクトの選択（Select Contract）]** ダイアログ ボックスが表示されます。

b) **[コントラクトの選択（Select Contract）]** ダイアログの左側のペインで、契約をクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの選択（Select Contract）]** ダイアログ ボックスが閉じます。

ステップ 5 コンシューマ EPG を追加するには、次の手順を実行します。

a) **[コンシューマ EPG の追加（Add Consumer EPGs）]** をクリックします。**[コンシューマー EPG の選択（Select Consumer EPGs）]** ダイアログが表示されます。

（注） テナント内（契約が作成される）の EPG が表示されます。

b) **[コンシューマー EPG の選択（Select Consumer EPGs）]** ダイアログの左側のペインで、チェックボックスをオンにして EPG を選択します。

ステップ 6 プロバイダー EPG を追加するには、次の手順を実行します。

a) **[プロバイダー EPG の追加（Add Provider EPGs）]** をクリックします。**[プロバイダー EPG の選択（Select Provider EPGs）]** ダイアログが表示されます。

（注） テナント内（契約が作成される）の EPG が表示されます。

b) **[プロバイダーEPGの選択（Select Provider EPGs）]** ダイアログの左側のペインで、チェックボックスをオンにしてプロバイダー EPG を選択します。

（注） 選択したコントラクトがインポート済みコントラクトの場合、プロバイダー EPG の選択は無効になります。

c) 完了したら、**[選択（Select）]** をクリックします。**[プロバイダーEPGの選択（Select Provider EPGs）]** ダイアログボックスが閉じ、**[EPS コミュニケーション構成（EPG Communication Configuration）]** ウィンドウに戻ります。

d) [保存（Save）] をクリックします。

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

このセクションでは、Cisco Cloud APIC GUI を使用したロールの作成方法について説明します。

始める前に

VRF を作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[クラウド コントラクト プロファイルの作成（Create Cloud Context Profile）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド（Create Cloud Context Profile Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *13* : クラウド コントラクト プロファイルの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（Name）	クラウド コンテキスト プロファイルの名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスで、次の手順を実行します。
説明	クラウド コンテキスト プロファイルの説明を入力します。
Settings	
リージョン（Region）	リージョンを選択するには: 1. **[リージョンの選択（Select Region）]** をクリックします。**[リージョンの選択（Select Region）]** ダイアログボックスが表示されます。 2. **[リージョンの選択（Select Region）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスで、次の手順を実行します。
VRF	VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRF の選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択し、**[選択（Select）]** をクリックします。**[クラウド コンテキスト プロファイルの作成（Create Cloud Context Profile）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
CIDR の追加（Add CIDR）	

[プロパティ（Properties）]	説明
	（注） 次のサブネットは予約されているため、この **[CIDR の追加（Add CIDR）]** フィールドでは使用しないでください。 192.168.100.0/24（□ブリッジ ドメイン インターフェイス用に CCR によって予約済み） （注） VNet ピアリングが有効になっている場合、CIDR を追加、削除、または編集することはできません。CIDR を追加、削除、または編集する前に、VNet ピアリングを無効にする必要があります。VNet ピアリングを無効にするには： • インフラ テナントの場合は、クラウド コンテキスト プロファイルの **[ハブ ネットワーク ピアリング（Hub Network Peering）]** オプションを無効にします。 • ユーザ（非インフラ）テナントの場合、クラウド コンテキスト プロファイルの **[VNet ピアリング（VNet Peering）]** オプションを無効にします。 CIDR 構成を変更したら、VNet ピアリングを再度有効にします。 次の機能はリリースによってサポートされます。 • インフラ VNet の追加のセカンダリ CIDR およびサブネットを追加することもできます（クラウド テンプレートで作成された `cloudCtxProfiles`）。プライマリ CIDR を追加したり、クラウド テンプレートによって作成された既存の CIDR を変更したりすることはできません。ユーザが作成した CIDR の下にサブネットが作成されると、サブネットは暗黙的にセカンダリ VRF にマッピングされます。 • インフラ VNet 以外の VNet のセカンダリ CIDR とサブネットを追加することもできます。 詳細については、「単一 VNet での複数の VRF のサポート」を参照してください。 CIDR を追加するには、次の手順を実行します。 1. **[CIDR の追加（Add CIDR）]** をクリックします。**[CIDR の追加（Add CIDR）]** ダイアログボックスが表示されます。 2. **[CIDR ブロック範囲（CIDR Block Range）]** フィールドにアドレスを入力します。 3. **[プライマリ（Primary）]** チェックボックスをオン（有効）またはオフ（無効）にします。 追加のセカンダリ CIDR および VNet のサブネットを追加している場合、**[プライマリ（Primary）]** ボックスのチェックを外します。

[プロパティ（Properties）]	説明
	4. **[サブネットの追加（Add Subnet）]** をクリックして、次の情報を入力します。 • **[アドレス（Address）]** フィールドに、サブネット アドレスを入力します。 • [名前（Name）] フィールドに、このサブネットの名前を入力します。 • **[プライベート リンク ラベル（Private Link Label）]** フィールドで、次のいずれかを選択します。 • **[既存のものを選択（Select Existing）]**：**[プライベート リンク ラベルの選択（Select Private Link Label）]** をクリックし、このサブネットに関連付ける既存のプライベート リンク ラベルを選択します。 • **[新規作成（Create New）]**：このサブネットに関連付けるプライベート リンク ラベルの一意の名前を入力します。 5. **[VRF]** フィールドで、必要に応じて選択します。 • **[プライマリ（Primary）]** フィールドの横にあるボックスをオンにすると、この CIDR は自動的にプライマリ VRF に関連付けられます。 • **[プライマリ（Primary）]** フィールドの横にあるチェックボックスをオンにしなかった場合は、この CIDR をセカンダリ VRF に関連付けることができます。VRFの横にある **[X]** をクリックし、**[VRF の選択（Select VRF）]** をクリックして、この CIDR に関連付けるセカンダリ VRF を選択します。 6. 完了したら、**[追加（Add）]** をクリックします。
[VNet ゲートウェイ ルータ（VNet Gateway Router）]	クリックして **[VNet ゲートウェイ ルータ（VNet Gateway Router）]** チェックボックスをチェック（有効）またはチェックを外します（無効）。
VNET ピアリング	クリックして、Azure VNet ピアリング機能をオン（有効）またはオフ（無効）にします。 VNetピアリング機能の詳細については、Cisco Cloud APICドキュメンテーションページの「Configuring VNet Peering for Cloud APIC for Azure」を参照してください。 https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/series.html#Configuration

ステップ 5 設定が終わったら [Save] をクリックします。

Azure での仮想マシンの構成

Cisco Cloud APIC のためのエンドポイント セレクタを構成するとき、Cisco Cloud APIC を構成するエンドポイントセレクタに対応するAzureで必要な仮想マシンの構成も必要になります。

このトピックでは、Azureで仮想マシンを構成するための要件について説明します。Cisco Cloud APICのエンドポイントセレクタを構成する前に、または後で、これらの要件を使用してAzureの仮想マシンを構成することができます。たとえば、先にAzureのアカウントに移動し、Azureのカスタム タグまたはラベルを作成してから、Cisco Cloud APIC以降のカスタム タグまたはラベルを使用して、エンドポイント セレクタを作成することができます。または、Cisco Cloud APICでカスタムタグまたはラベルを使用してエンドポイントセレクタを作成してから、Azureのアカウントに移動し、Azure以降のカスタム タグまたはラベルを作成することもできます。

始める前に

Azure仮想マシンの構成プロセスの一環として、クラウドコンテキストプロファイルを構成する必要があります。GUI を使用してクラウド コンテキスト プロファイルを構成すると、VRF やリージョンの設定などの構成情報は、Azure にプッシュされます。

ステップ 1 クラウド コンテキスト プロファイル設定を確認して、次の情報を取得します。

- VRF 名
- サブネット情報
- サブスクリプション ID
- クラウド コンテキスト プロファイルが展開されている場所に対応するリソース グループ。

（注） 上記の情報に加えて、タグベースのEPGを使用している場合は、タグ名も知っている必要があります。タグ名は、クラウド コンテキスト プロファイル設定では使用できません。

クラウド コンテキスト プロファイル設定情報を取得するには、次の手順を実行します。

a) **[ナビゲーション (Navigation)]** メニューで、**[アプリケーション管理 (Application Management)]** タブを選択します。

[アプリケーション管理 (Application Management)] タブを展開すると、サブタブ オプションのリストが表示されます。

b) **[クラウド コンテキスト プロファイル (Cloud Context Profiles)]** サブタブ オプションを選択します。

Cisco Cloud APIC 用に作成したクラウド コンテキスト プロファイルのリストが表示されます。

c) この Azure 仮想マシン構成プロセスの一部として使用するクラウド コンテキスト プロファイルを選択します。

リージョン、VRF、IPアドレス、サブネットなど、このクラウドコンテキストプロファイルのさまざまな設定パラメータが表示されます。Azure仮想マシンを構成するときに、このウィンドウに表示される情報を使用します。

ステップ 2 Cisco Cloud APICユーザ テナントの Azure ポータル アカウントにログインし、クラウド コンテキスト プロファイル構成から収集した情報を使用して Azure VM の作成を開始します。

（注） Azure ポータルで VM を作成する方法の詳細については、Microsoft Azure のマニュアルを参照してください。

Cisco Cloud APIC GUI を使用したバックアップ構成の作成

ここでは、バックアップ構成を作成する方法を説明します。

始める前に

必要に応じて、リモート ロケーションとスケジューラを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[操作（Operations）]** を選択します。

[インテント（Intent）] の **[操作（Operations）]** オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** の **[操作（Operations）]** リストから、**[バックアップ構成の作成（Create Backup Configuration）]** をクリックします。**[バックアップ構成の作成（Create Backup Configuration）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[*バックアップ構成の作成ダイアログボックスのフィールド（*Create Backup Configuration Dialog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *14 :* バックアップ構成の作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	バックアップ構成の名前を入力します。
説明	バックアップ構成の説明を入力します。
[設定（Settings）]	
Backup Destination	バックアップ接続先を選択します。 • ローカル • リモート

[プロパティ（**Properties**）]	説明
バックアップ オブジェクト	

[プロパティ（Properties）]	説明
	バックアップで考慮するルート階層コンテンツを選択します • ポリシーユニバース • セレクタオブジェクト（Selector Object）：これを選択すると、[オブジェクトタイプ（Object Type）] ドロップダウンリストと [オブジェクト DN（Object DN）] フィールドが追加されます。 1. オブジェクトタイプ（Object Type）ドロップダウン リストで、次のオプションから選択します。 • テナント（Tenant）：選択すると、[テナントの選択（Select Tenant）] オプションが表示されます。 • アプリケーション プロファイル（Application Profile）：選択すると、[アプリケーション プロファイルの選択（Select Application Profile）] オプションが表示されます。 • EPG：これを選択すると [EPG の選択（Select EPG）] オプションが表示されます。 • コントラクト（Contract）：これを選択すると、[コントラクトの選択（Select Contract）] オプションが表示されます。 • フィルタ（Filter）：これを選択すると、[フィルタの選択（Select Filter）] オプションが表示されます。 • VRF：これを選択すると、[VRFの選択（Select VRF）] オプションが表示されます。 • デバイス：[SelectfvcloudLBCtx] プションが表示されます。 • サービス グラフ：選択すると、[Select Service Graph] オプションが表示されます。 • [クラウド コンテキスト プロファイル（Cloud Context Profile）]：これを選

[プロパティ（Properties）]	説明
	択すると、**[クラウド コンテキスト プロファイルの選択**（Select Cloud Context Profile）]オプションが表示されます。 2. **Select <object_name>** をクリックjします。**Select <object_name>** ダイアログが表示されます。 3. **Select <object_name>** ダイアログから左側の列のオプションからクリックして選んで、**[選択（Select）]** をクリックします。**[バックアップ構成の作成（Create Backup Configuration）]** ダイアログ ボックスに戻ります。 （注） **[オブジェクトDN（Object DN）]** フィールドには、バックアップするオブジェクトツリーのルートとして使用するオブジェクトの DN が自動的に入力されます。 • **DN の入力（Enter DN）**：このオプションを選択すると、**[オブジェクト DN（Object DN）]** フィールドが表示されます。 1. **[オブジェクトDN（Object DN）]** フィールドに、バックアップするオブジェクト ツリーのルートとして使用する特定のオブジェクトの DN を入力します。
スケジューラ	1. **[スケジューラの選択（Select Scheduler）]** をクリックして **[スケジューラの選択（Select Scheduler）]** ダイアログを開き、左側の列からスケジューラを選択します。 2. 終了したら、右下隅にある **[選択（Select）]** ボタンをクリックします。
作成後のバックアップのトリガー	次のいずれかを実行します。 • **はい（Yes）**：（デフォルト）バックアップ設定の作成後にバックアップをトリガーします。 • **いいえ（No）**：バックアップ設定の作成後にバックアップをトリガーしません。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したテクニカル サポート ポリシーの作成

このセクションでは、テクニカル サポート ポリシーを作成する方法について説明します。

始める前に

リモート ロケーションのテクニカル サポート ポリシーを作成する場合は、まずリモート ロケーションを作成する必要があります。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[操作（Operations）]** を選択します。

[インテント（Intent）] の **[操作（Operations）]** オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** の **[操作（Operations）]** リストから、**[テクニカル サポートの作成（Create Tech Support）]** をクリックします。**[テクニカル サポートの作成（Create Tech Support）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[テクニカル サポートの作成ダイアログボックスのフィールド（Create Tech Support Dialog Box Fields）]* のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

表 *15* : テクニカル サポートの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
全般	
名前	テクニカル サポート ポリシーの名前を入力します。
説明	テクニカル サポートの説明を入力します。
[設定（Settings）]	

[プロパティ（Properties）]	説明
エクスポート先	エクスポート先を選択します。 • コントローラ • [リモート ロケーション（Remote Location）]：選択すると、[リモート ロケーションの選択（Select Remote Location）] オプションが表示されます。 1. [リモート ロケーションの選択（Select Remote Location）] をクリックします。[リモート ロケーションの選択（Select Remote Location）] ダイアログボックスが表示されます。 2. [[リモート ロケーションの選択（Select Remote Location）] ダイアログで、左側の列のリモート ロケーションをクリックして選択し、[選択（Select）] をクリックします。[テクニカル サポートの作成（Create Tech Support）] ダイアログボックスに戻ります。
アップグレード前のログを含める	テクニカル サポート ポリシーにアップグレード前のログを含める場合は、[有効（Enabled）] チェックボックスをオンにします。
作成後のトリガー	ポリシーの作成後にテクニカル サポート ポリシーを作成する場合は、[有効] (デフォルト) チェックボックスをクリックしてオンにします。無効にするには、チェックボックスをオフにします。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したスケジューラの作成

このセクションでは、ユーザー ラップトップブ ラウザのローカル時間で、Cisco Cloud APIC のデフォルト UTC 時間に変換されるスケジューラを作成する方法について説明します。

ステップ 1 インテント アイコンをクリックします。[インテント（Intent）] メニューが表示されます。

ステップ 2 [インテント（Intent）] 検索ボックスの下のドロップダウン□をクリックし、[操作（Operations）] を選択します。

[インテント（Intent）] の **[操作（Operations）]** オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** の **[操作（Operations）]** リストから、**[スケジューラの作成（Create Scheduler）]** をクリックします。**[スケジューラの作成（Create Scheduler）]** ダイアログボックスが表示されます。

ステップ 4 次の *[*スケジューラの作成ダイアログボックスのフィールド（*Create Scheduler Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *16 :* スケジューラの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	トリガー スケジューラ ポリシーの名前を入力します。
説明	トリガーの説明を入力します。
[設定（Settings）]	

[プロパティ（Properties）]	説明
繰り返しウィンドウ	**[繰り返しウィンドウの追加（Add Recurring Window）]** をクリックします。**[繰り返しウィンドウの追加（Add Recurring Window）]** ダイアログウィンドウが表示されます。 1. **[スケジュール（Schedule）]** ドロップダウンリストから、次のいずれかを選択します。 • 毎日 • 月曜日 • 火曜日 • 水曜日 • 木曜日 • 金曜日 • 土曜日 • 日曜日 • 奇数日 • 偶数日 2. **[開始時間（Start Time）]** フィールドに、時間を入力します。 3. **[最大同時タスク数（Maximum Concurrent Tasks）]** フィールドから数値を入力するか、フィールドを空白のままにして無制限を指定します。 4. **[最大実行時間（Maximum Running Time）]** で、**[無制限（Unlimited）]** または **[カスタム（Custom）]** をクリックして選択します。 5. 終了したら、[Add] をクリックします。

[プロパティ（Properties）]	説明
ワンタイム ウィンドウの追加	**[ワンタイムウィンドウの追加（Add One Time Window）]** をクリックします。**[ワンタイムウィンドウの追加（Add One Time Window）]** ダイアログが表示されます。 1. **[開始時間（Start Time）]** フィールドに、時間を入力します。 2. **[最大同時タスク数（Maximum Concurrent Tasks）]** フィールドに数値を入力するか、フィールドを空白のままにして無制限を指定します。 3. **[最大実行時間（Maximum Running Time）]** で、**[無制限（Unlimited）]** または **[カスタム（Custom）]** をクリックして選択します。 4. 終了したら、[Add] をクリックします。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したリモート ロケーションの作成

このセクションでは、Cisco Cloud APIC を使用したリモート ロケーションの作成方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[操作（Operations）]** を選択します。

[インテント（Intent）] の **[操作（Operations）]** オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[操作（Operations）]** リストで、**[リモート ロケーションの作成（Create Remote Location）]** をクリックします。**[リモート ロケーションの作成（Create Remote Location）]** ダイアログボックスが表示されます。

ステップ 4 次の *[リモート ロケーションの作成ダイアログボックスのフィールド（Create Remote Location Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *17 :* リモート ロケーションの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	

[プロパティ（Properties）]	説明
名前	リモート ロケーション ポリシーの名前を入力します。
説明	リモート ロケーション ポリシーの説明を入力します。
[設定（Settings）]	
[ホスト名/IP アドレス（Hostname/IP Address）]	リモート ロケーションのホスト名または IP アドレスを入力します
プロトコル	プロトコルを選択します。 • FTP • SFTP • SCP
パス	リモート ロケーションのパスを入力します。
[ポート（Port）]	リモート ロケーションのポートを入力します。
ユーザ名（Username）	リモートロケーションのユーザー名を入力します。
認証タイプ（Authentication Type）	SFTP または SCP を使用する場合は、認証タイプを選択します。 • [Password] • SSH キー（SSH Key）
SSH キー コンテンツ	SSH キーのコンテンツを入力します。
SSH キー パスフレーズ	SSH キー パスフレーズ
Password	リモート ロケーションにアクセスするためのパスワードを入力します。
Confirm Password	リモート ロケーションにアクセスするためのパスワードを再入力します。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したローカル ドメインの作成

このセクションでは、クラウドAPIC GUIを使用したログイン ドメインの作成方法について説明します。

始める前に

非ローカルドメインを作成する前に、プロバイダーを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[ログイン ドメインの作成（Create Login Domain）]** をクリックします。**[ログイン ドメインの作成（Create Login Domains）]** ダイアログボックスが表示されます。

ステップ 4 次の *[ログイン ドメインダイアログボックスの作成のフィールド（Login Domains Dialog Box Fields）]* のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

表 *18 :* ログイン ドメインダイアログボックスの作成のフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	ログイン ドメインの名前を入力します。
説明	ログイン ドメインの説明を入力します。
レルム	レルムを選択します。 • **ローカル** • **LDAP**：プロバイダーを追加し、認証タイプを選択する必要があります。 • **RADIUS**：プロバイダーを追加する必要があります。 • **TACACS+**：プロバイダーの追加が必要です。 • **SAML**：プロバイダーの追加が必要です。

[プロパティ（Properties）]	説明
プロバイダ	プロバイダーを追加するには、次の手順を実行します。 1. **[プロバイダーの追加（Add Providers）]**をクリックします。**[プロバイダーの選択（Select Providers）]** ダイアログが表示され、左側のペインにプロバイダーのリストが表示されます。 2. クリックしてプロバイダーを選択します。 3. **[選択 (Select)]** をクリックして、プロバイダを追加します。
詳細設定	**[認証タイプ（Authentication Type）]** および **[LDAP グループ マップ ルール（LDAP Group Map Rules）]** フィールドを表示します。
認証タイプ（Authentication Type）	レルム オプションにLDAPを選択した場合は、次のいずれかの認証タイプを選択します。 • **Cisco AV ペア**：（デフォルト） • **LDAP グループ マップ ルール**：LDAP グループ マップ ルールを追加する必要があります。

[プロパティ（**Properties**）]	説明
LDAP グループ マップ ルール	

[プロパティ（Properties）]	説明
	LDAP グループ マップ ルールを追加するには、次の手順を実行します。 1. **[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** をクリックします。**[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** ダイアログが表示され、左側のペインにプロバイダーのリストが表示されます。 2. **[名前（Name）]** フィールドに、ルールの名前を入力します。 3. **[説明（Description）]** フィールドに、ルールの説明を入力します。 4. **[グループ DN（Group DN）]** フィールドにルールのグループ DN を入力します。 5. セキュリティ ドメインの追加： 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスが表示されます。 2. **[セキュリティ ドメインの選択（Select Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログボックスが表示され、左側のウィンドウにセキュリティ ドメインのリストが表示されます。 3. セキュリティ ドメインをクリックして選択します。 4. **[選択（Select）]** をクリックして、セキュリティ ドメインを追加します。**[セキュリティ ドメインの追加（Add Security Domain）] ダイアログボックスに戻ります。** 5. ユーザー ロールを追加する: 1. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスで、**[ロールの選択（Select Role）]** をクリックします。**[ロールの選択（Select Role）]** ダイアログボックスが表示され、左側のペインにロールのリストが表

[プロパティ（Properties）]	説明
	示されます。 2. クリックしてロールを選択します。 3. **[選択（Select）]** をクリックしてロールを追加します。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスに戻ります。 4. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスから、**[権限タイプ（Privilege Type）]** ドロップダウンリストをクリックして、**[読み取り権限（Read Privilege）]** または **[書き込み権限（Write Privilege）]** を選択します。 5. **[権限タイプ（Privilege Type）]** ドロップダウン リストの右側のチェックマークをクリックして、確認します。 6. 終了したら、[Add] をクリックします。**[LDAP グループ マップ ルールの追加（Add LDAP Group Map Rule）]** ダイアログボックスに戻り、別のセキュリティ ドメインを追加できます。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したセキュリティ ドメインの作成

セキュリティドメインは、追加するセキュリティドメインにテナントを制限します。セキュリティドメインを追加しない場合、すべてのセキュリティドメインがこのテナントにアクセスできます。このセクションでは、GUI を使用してセキュリティ ドメインを作成する方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの**[管理（Administrative）]** リストで、**[セキュリティ（Security）]** > **[セキュリティ ドメイン（Security Domains）]** > **[セキュリティ ドメインの作成（Create Security Domain）]** をクリックします。**[セキュリティ ドメインの作成（Create Security Domain）]** ダイアログ ボックスが表示されます。

ステップ 4 **[名前（Name）]** フィールドに、セキュリティ ドメインの名前を入力します。

ステップ 5 **[説明（Description）]** フィールドに、セキュリティ ドメインの説明を入力します。

ステップ 6 **[制限付きドメイン（Restricted Domain）]**制御を **[はい（Yes）]** または **[いいえ（No）]** に設定します。

セキュリティ ドメインが制限付きドメインとして構成されている場合（**[はい（Yes）]**）、このドメインに割り当てられているユーザーは、他のセキュリティ ドメインで構成されたポリシー、プロファイル、またはユーザーを表示できません。

ステップ 7 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したロールの作成

このセクションでは、クラウド APIC GUI を使用したロールの作成方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[Intent]** メニューの **[Administrative]** リストで、**[セキュリティ ドメインの作成（Create Security Domain）]** をクリックします。**[ロールの作成（Create Role）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[*ロールの作成ダイアログボックスのフィールド（*Create Role Dailog Box Fields*）*]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *19 :* ロールの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
全般	
名前	**[Name]** フィールドにロール名を入力します。
説明	ロールの説明を入力します。
[設定（Settings）]	

[プロパティ（**Properties**）]	説明
特権	

[プロパティ（Properties）]	説明
	クリックして、ユーザに割り当てる権限のチェックボックスをオンにします。権限は次のとおりです。 • **aaa**：認証、許可、アカウンティング、インポート/エクスポート ポリシーの設定に使用されます。 • **access-connectivity-l1** インフラの下のレイヤ 1 設定に使用されます。例：セレクタとポート レイヤ 1 のポリシー設定。 • **access-connectivity-l2** ：インフラの下のレイヤ 2 設定に使用されます。例：セレクタおよび接続可能なエンティティ設定をカプセル化します。 • **access-connectivity**：インフラでのレイヤ 3 の設定、テナントの L3Out でのスタティック ルート設定に使用されます。 • **access-connectivity-mgmt** ：管理インフラ ポリシーに使用されます。 • **access-connectivity-util** ：テナント ERSPAN ポリシーに使用されます。 • **access-equipment**：アクセスポートの設定に使用されます。 • **access-protocol-l1** ：インフラのレイヤ 1 プロトコル設定に使用されます。 • **access-protocol-l2** ：インフラのレイヤ 2 プロトコル設定に使用されます。 • **access-protocol-l3** ：インフラでのレイヤ 3 プロトコル設定に使用されます。 • **access-protocol-mgmt** ：NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシーに使用されます。 • **access-protocol-ops** ：クラスタ ポリシーやファームウェア ポリシーなどの操作関連のアクセス ポリシーに使用されます。 • **access-protocol-util** ：テナント ERSPAN ポリシーに使用されます。 • **access-qos**：CoPP および QoS に関連するポリシーの変更に使用されます。

[プロパティ（Properties）]	説明
	• **admin**：すべてへのアクセス（すべてのロールの組み合わせ） • **fabric-connectivity-l1** ：ファブリックの下のレイヤ 1 設定に使用されます。例：セレクタとポート レイヤ 1 ポリシーと VNET 保護。 • **fabric-connectivity-l2** ：ポリシー展開の影響を推定するための警告を生成するために、ファームウェアおよび展開ポリシーで使用されます。 • **fabric-connectivity-l3** ：ファブリックの下のレイヤ 3 設定に使用されます。例: ファブリック IPv4 および MAC 保護グループ。 • **fabric-connectivity-mgmt**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、および診断ポリシーに使用されます。 • **fabric-connectivity-util**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。 • **fabric-equipment**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。 • **fabric-protocol-l1** ：ファブリックの下のレイヤ 1 プロトコル設定に使用されます。 • **fabric-protocol-l2** ：ファブリックの下のレイヤ 2 プロトコル設定に使用されます。 • **fabric-protocol-l3** ：ファブリックの下のレイヤ 3 プロトコル設定に使用されます。 • **fabric-protocol-mgmt** ：NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシーに使用されます。 • **fabric-protocol-ops** ：ERSPAN およびヘルス スコア ポリシーに使用されます。 • **fabric-protocol-util** ：ファームウェア管理の traceroute およびエンドポイント トラッキング ポリシーに使用されます。 • **none**：特権なし。

[プロパティ（Properties）]	説明
	• **nw-svc-device** ：レイヤ 4 からレイヤ 7 のサービス デバイスを管理するために使用されます。 • **nw-svc-devshare** ：共有レイヤ 4 ～ レイヤ 7 サービス デバイスの管理に使用されます。 • **nw-svc-params**：レイヤ 4 ～ レイヤ 7 のサービス ポリシーの管理に使用されます。 • **nw-svc-policy**：レイヤ 4 ～ レイヤ 7 のネットワーク サービス オーケストレーションの管理に使用されます。 • **ops**：アトミック カウンタ、SPAN、TSW、技術サポート、トレースルート、分析、コア ポリシーなど、ポリシーのモニタリングとトラブルシューティングを含む動作ポリシーに使用されます。 • **tenant-connectivity-l1** ：ブリッジ ドメインやサブネットなど、レイヤ 1 接続の変更に使用されます。 • **tenant-connectivity-l2** ：ブリッジ ドメインやサブネットなど、レイヤ 2 接続の変更に使用されます。 • **tenant-connectivity-l3** ：VRF を含むレイヤ 3 接続の変更に使用されます。 • **tenant-connectivity-mgmt** ：テナントのインバンドおよびアウトオブバンドの管理接続構成、およびアトミック カウンターやヘルス スコアなどのポリシーのデバッグ/監視に使用されます。 • **tenant-connectivity-util**：リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。 • **tenant-epg**：エンドポイント グループ、VRF、ブリッジ ドメインの削除/作成など、テナント設定の管理に使用されます。 • **tenant-ext-connectivity-l2**：テナントの L2Out 構成を管理するために使用されます。 • **tenant-ext-connectivity-l3**：テナント L3Out 構成の管理に使用されます。

[プロパティ（Properties）]	説明
	• **tenant-ext-connectivity-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。 • **tenant-ext-connectivity-util** ： traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。 • **tenant-ext-protocol-l1**：テナントの外部レイヤ 1 プロトコルの管理に使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。 • **tenant-ext-protocol-l2** ：テナントの外部レイヤ 2 プロトコルの管理に使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。 • **tenant-ext-protocol-l3** ：BGP、OSPF、PIM、IGMP などのテナントの外部レイヤ 3 プロトコルを管理するために使用されます。 • **tenant-ext-protocol-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。 • **tenant-ext-protocol-util**：traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。 • **tenant-network-profile**：ネットワーク プロファイルの削除および作成、エンドポイント グループの削除および作成など、テナント設定の管理に使用されます。 • **tenant-protocol-l1** ：テナントの下でレイヤ 1 プロトコルの設定を管理するために使用されます。 • **tenant-protocol-l2** ：テナントの下でレイヤ 2 プロトコルの設定を管理するために使用されます。 • **tenant-protocol-l3** ：テナントの下でレイヤ 3 プロトコルの設定を管理するために使用されます。 • **tenant-protocol-mgmt**：ファームウェア ポリシーの書き込みアクセスとして使用されます。

[プロパティ（Properties）]	説明
	• **tenant-protocol-ops** ：テナント traceroute ポリシーに使用されます。 • **tenant-protocol-util** — traceroute、ping、oam、eptrk などのデバッグ/監視/観察ポリシーに使用されます。 • **tenant-qos**：ファームウェア ポリシーの書き込みアクセスとしてのみ使用されます。 • **tenant-security**：テナントの契約関連の設定に使用されます。 • **vmm-connectivity**：VM 接続に必要な APIC の VMM インベントリ内のすべてのオブジェクトを読み取るために使用されます。 • **vmm-ep**：APIC の VMM インベントリ内の VM およびハイパーバイザーエンドポイントを読み取るために使用されます。 • **vmm-policy**：VM ネットワーキングのポリシーの管理に使用されます。 • **vmm-protocol-ops**：VMM ポリシーでは使用されません。 • **vmm-security**：テナントの契約関連の設定に使用されます。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用した認証局の作成

ここでは、GUI を使用して認証局を作成する方法について説明します。

始める前に

- 証明書チェーン（certificate chain）を設定します。
- 認証局がテナント用の場合は、テナントを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。
ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[インテント（Intent）] メニューに**管理**オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[証明書認証局の作成（Create Certificate Authority）]** をクリックします。**[証明書認証局の作成（Create Certificate Authority）]** ダイアログボックスが表示されます。

ステップ 4 *[*証明書認証局の作成ダイアログボックスのフィールド（*Create Certificate Authority Dialog Box Fields*）*]* のテーブルにリストされた各フィールドに適切な値を入力して、続行します。

表 *20 :* 証明書認証局の作成ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	証明書認証局の名前を入力してください。
説明	証明書認証局の説明を入力してください。
コントローラ	次のオプションから選択します。 • **テナント（Tenant）**：認証局が特定のテナント用かどうかを選択します。選択すると、**[テナントの選択（Select Tenant）]** オプションがGUIに表示されます。 • **システム（System）**：認証局がシステム用である場合に選択します。
テナントの選択	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[証明書認証局の作成（Create Certificate Authority）]** ダイアログボックスが表示されます。
[証明書チェーン（Certificate Chain）]	**[証明書チェーン (Certificate Chain)]** フィールドに、証明書チェーンを入力します。 （注） チェーンの証明書を次の順序で追加します。 1. CA 2. Sub-CA 3. サブサブCA 4. サーバ

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したキー リングの作成

このセクションでは、Cisco Cloud APIC GUI を使用したキー リングの作成方法について説明します。

始める前に

- 認証局を作成します。
- 証明書を持っています。
- キー リングが特定のテナント用である場合は、テナントを作成します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[キー リングの作成（Create Key Ring）]** をクリックします。**[キー リングの作成（Create Key Ring）]** ダイアログ ボックスが表示されます。

ステップ 4 次の *[キー リングの作成ダイアログボックスのフィールド（Create Key Ring Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *21* : キー リングの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	**説明**
名前（Name）	キー リングの名前を入力します。
説明	キー リングの説明を入力します。
コントローラ	• **System**：キー リングはシステム用です。 • **Tenant**：キー リングは特定のテナント用です。テナントを指定する **[テナント（Tenant）]** フィールドを表示します。

[プロパティ（Properties）]	説明
テナントの選択	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログボックスが表示されます。 2. **[テナントの選択（Select Tenant）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。**[キー リングの作成（Create Key Ring）]** ダイアログボックスに戻ります。
[設定（Settings）]	
認証局	認証局を選択するには： 1. **[認証局の選択（Select Certificate Authority）]** をクリックします。**[認証局の選択（Select Certificate Authority）]** ダイアログが表示されます。 2. 左側の列で認証局をクリックして選択します。 3. **[選択（Select）]**をクリックします。**[キー リングの作成（Create Key Ring）]** ダイアログボックスに戻ります。
秘密キー	次のいずれかを実行します。 • **[新しいキーの生成（Generate New Key）]**：新しいキーを生成します。 • **[既存のキーのインポート（Import Existing Key）]**：**[秘密キー（Private Key）]** テキストボックスが表示され、既存のキーを使用できます。
秘密キー	**[秘密キー（Private Key）]** テキスト ボックスに既存のキーを入力します（**[既存のキーのインポート（Import Existing Key）]** オプションの場合）。

[プロパティ（Properties）]	説明
モジュラス	**[モジュール（Modulus）]** ドロップダウン リストをクリックし、次の項目の中から選択します。 • **MOD 512** • **MOD 1024** • **MOD 1536** • **MOD 2048**：デフォルト
認証	**[証明書（Certificate）]** テキスト ボックスに証明書情報を入力します。

ステップ 5 設定が終わったら [Save] をクリックします。

Cisco Cloud APIC GUI を使用したローカル ユーザーの作成

このセクションでは、クラウド APIC GUI を使用したローカル ユーザーの作成方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[Intent]メニューに管理オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストで、**[ローカル ユーザーの作成（Create Local User）]** をクリックします。**[ローカル ユーザーの作成（Create New User）]** ダイアログボックスが表示されます。

ステップ 4 次の *[ローカル ユーザーの作成ダイアログボックスのフィールド（Create Local User Dailog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *22 :* ローカル ユーザーの作成ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（Name）	ローカル ユーザーのユーザー名を入力します。
Password	ローカル ユーザーのパスワードを入力します。
Confirm Password	ローカル ユーザーのパスワードを再入力します。
説明	ローカル ユーザーの説明を入力します。
[設定（Settings）]	

[プロパティ（Properties）]	説明
アカウント ステータス	アカウント ステータスを選択するには、次の手順を実行します。 • **Active**：ローカル ユーザー アカウントをアクティブにします。 • **Inactive**：ローカル ユーザー アカウントを非アクティブにします。
名	ローカル ユーザーの名を入力します。
姓（Last Name）	ローカル ユーザーの姓を入力します。
電子メール アドレス	ローカル ユーザーの E メール アドレスを入力します。
電話番号（Phone Number）	ローカル ユーザーの 電話番号を入力します。

[プロパティ（**Properties**）]	説明
セキュリティ ドメイン	

[プロパティ（Properties）]	説明
	セキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスが表示されます。 2. **[セキュリティ ドメインの選択（Select Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログボックスが表示され、左側のウィンドウにセキュリティ ドメインのリストが表示されます。 3. セキュリティ ドメインをクリックして選択します。 4. **[選択（Select）]** をクリックして、セキュリティ ドメインを追加します。**[セキュリティ ドメインの追加（Add Security Domain）] ダイアログボックスに戻ります。** 5. ユーザー ロールを追加する: 1. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスで、**[ロールの選択（Select Role）]** をクリックします。**[ロールの選択（Select Role）]** ダイアログ ボックスが表示され、左側のペインにロールのリストが表示されます。 2. クリックしてロールを選択します。 3. **[選択（Select）]** をクリックしてロールを追加します。**[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログボックスに戻ります。 4. **[セキュリティ ドメインの追加（Add Security Domain）]** ダイアログ ボックスから、**[権限タイプ（Privilege Type）]** ドロップダウン リストをクリックして、**[読み取り権限（Read Privilege）]** または **[書き込み権限（Write Privilege）]** を選択します。 5. **[権限タイプ（Privilege Type）]** ドロップダウンリストの右側のチェックマークをクリッ

[プロパティ（Properties）]	説明
	クして、確認します。 6. 終了したら、[Add] をクリックします。**[ローカル ユーザーの作成（Create Local User）]** ダイアログボックスに戻り、別のセキュリティ ドメインを追加できます。

ステップ 5 **[高度な設定（Advanced Settings）]** をクリックして、*[ローカルユーザーの作成ダイアログボックスのフィールド：高度な設定（Create Local User Dailog Box Fields: Advanced Settings）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *23 :* ローカル ユーザーの作成ダイアログボックスのフィールド：高度な設定

プロパティ	説明
アカウント期限切れ	**[はい（Yes）]** を選択すると、アカウントは選択した時点で期限切れになるように設定されます。
パスワードの更新が必要です	**[はい（Yes）]** を選択した場合、ユーザーは次回ログイン時にパスワードを変更する必要があります。
OTP	ユーザーのワンタイム パスワード機能を有効にするには、チェックボックスをオンにします。
ユーザー証明書	ユーザー証明書を追加するには、次の手順を実行します。 1. **[X509 証明書の追加（Add X509 Certificate）]** をクリックします。**[X509 証明書の追加（Add X509 Certificate）]** ダイアログボックスが表示されます。 2. [名前（Name）] フィールドに名前を入力します。 3. **[ユーザー X509 証明書（User X509 Certificate）]** テキストボックスにX509証明書を入力します。 4. **[追加（Add）]** をクリックします。**[ユーザー X509 証明書の X509 証明書]** ダイアログボックスが閉じます。**[ローカル ユーザー]** ダイアログボックスに戻ります。

プロパティ	説明
SSH キー	SSH キーを追加するには、次の手順を実行します。 1. **[SSH キーを追加（Add SSG Key）]** をクリックします。**[SSH キーの追加（Add SSG Key）]** ダイアログボックスが表示されます。 2. [名前（Name）] フィールドに名前を入力します。 3. **[キー（Key）]** テキストボックスに SSH キーを入力します。 4. **[追加（Add）]** をクリックします。**[SSH キーの追加（Add SSG Key）]** ダイアログボックスが閉じます。**[ローカル ユーザー]** ダイアログボックスに戻ります。

ステップ 6 設定が終わったら [Save] をクリックします。

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）

リージョンは、初回セットアップ時に構成されます。構成時に、Cisco Cloud APIC によって管理されるリージョンと、そのリージョンのサイト間およびリージョン間の接続を指定します。このセクションでは、初期インストール後に Cisco Cloud APIC GUI を使用してクラウド テンプレートでリージョンを管理する方法について説明します。

クラウドテンプレートの詳細については、クラウドテンプレートの概要を参照してください。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[構成（Configuration）]** を選択します。

オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[構成（Configuration）]** リストから、**[cAPIC セットアップ（cAPIC Setup）]** をクリックします。
[設定-概要（Set up-Overview）] ダイアログボックスが表示され、**[DNS と NTPサーバ]**、**[リージョン管理]**、**[スマート ライセンシング]** のオプションが示されます。

ステップ 4 **[リージョン管理（Region Management）]** で、**[構成の編集（Edit Configuration）]** をクリックします。

[セットアップ - リージョン管理] ダイアログ ボックスが表示されます。**セットアップ - リージョン管理**の一連のステップの最初のステップ、**管理するリージョン**が表示され、管理対象リージョンのリストが表示されます。

ステップ 5 サイト間接続が必要な場合は、[サイト間接続（Inter-Site Connectivity）] 領域の [有効（Enabled）] ボックスをクリックしてオンにします。
このオプションを選択すると、ページ上部の**[セットアップ-リージョン管理（Setup-Region Management）]** の手順に**サイト間接続**の手順が追加されます。

ステップ 6 Cisco Cloud APIC で管理するリージョンを選択するには、そのリージョンのチェック ボックスをクリックしてチェック マークを付けます。

ステップ 7 クラウド ルータをこのリージョンにローカルに展開するには、そのリージョンの [Cloud Routers] チェック ボックスをオンにします。

ステップ 8 クラウド サイトのファブリック インフラ接続を構成するには、**[次へ]** をクリックします。
[セットアップ - リージョン管理（Setup - Region Management）] の一連の手順の次の手順である、**[一般的な接続（General Connectivity）]** が表示されます。

ステップ 9 CCR のサブネット プールを追加するには、**[クラウド ルータのサブネット プールを追加する（Add Subnet Pool for Cloud Router）]** をクリックし、テキスト ボックスにサブネットを入力します。

（注） クラウド APIC の導入時に提供される /24 サブネットは、最大 2 つのクラウド サイトに十分です。3 つ以上のクラウド サイトを管理する必要がある場合は、さらにサブネットを追加する必要があります。

ステップ 10 **[CCR向け BGP 自律システム番号（BGP Autonomous System Number for CCRs）]** フィールドに値を入力します。

BGP ASN の範囲は 1 ー 65534 です。

ステップ 11 **[Assign Public IP to CCR Interface（パブリック IP を CCR インターフェイスに割り当てる）]** フィールドで、CCR インターフェイスにパブリック IP アドレスまたはプライベート IP アドレスを割り当てるかどうかを決定します。

CCR では、サイト間通信のためにパブリック IP アドレスが必要であることに注意してください。

- 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には、**[有効（Enabled）]** チェック ボックスをオンのままにします。デフォルトでは、この **[有効]** チェック ボックスはオンになっています。
- プライベート IP アドレスを CCR インターフェイスに割り当てるには、**[有効（Enabled）]** チェック ボックスのチェックを外します。この場合、接続にはプライベート IP アドレスが使用されます。

（注） CCR アドレスをパブリック IP アドレスからプライベート IP アドレスに（またはその逆に）変更すると、中断が発生し、トラフィックが失われる可能性があります。

リリース 5.1(2) 以降では、CCRに割り当てられたパブリック IP アドレスとプライベート IP アドレスの両方が、[クラウド リソース（Cloud Resources）] 領域にルータの他の詳細とともに表示されます。パブリック IP が CSR に割り当てられていない場合は、プライベート IP だけが表示されます。

ステップ 12 リージョンごとのルータ数を選択するには、**[リージョンごとのルータ数（Number of Routers Per Region）]** ドロップダウン リストをクリックし、**[2]**、**[3]**、または **[4]**、**[6]**、 または **[8]** をクリックします。

ステップ 13 **[ユーザー名（Username）]** テキストボックスにユーザー名を入力します。

（注） Azure クラウド サイトに接続する場合は、CCR のユーザ名として admin を使用しないでください。

ステップ 14 **[パスワード（Password）]** テキスト ボックスと **[パスワードの確認（Confirm Password）]** テキスト ボックスに新しいパスワードを入力します。

ステップ 15 スループット値を選択するには、**[ルーターのスループット]** ドロップダウン リストをクリックします。

（注）
- クラウド ルータは、ルータのスループットまたはログイン情報を変更する前に、すべてのリージョンから展開解除する必要があります。
- 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。Cisco Catalyst 8000V のスループット値については、Cisco Catalyst 8000V について を参照してください。

ステップ 16 必要に応じて、[TCP MSS]フィールドに必要な情報を入力します。

リリース 4.2(4q) 以降では、TCP 最大セグメントサイズ（MSS）を構成するために **[TCP MSS]** オプションを使用できます。この値は、クラウドへの VPN トンネルとオンプレミス サイトまたは他のクラウド サイトへの外部トンネルを含む、すべてのクラウドルータ トンネルインターフェイスに適用されます。クラウドへのVPNトンネルの場合、クラウドプロバイダーのMSS値がこのフィールドに入力した値よりも小さい場合は、低い方の値が使用されます。それ以外の場合は、このフィールドに入力した値が使用されます。

MSS値はTCPトラフィックにのみ影響し、pingトラフィックなどの他のタイプのトラフィックには影響しません。

ステップ 17 (オプション) ライセンス トークンを指定するには、**[ライセンス トークン]** テキスト ボックスに製品インスタンスの登録トークンを入力します。

（注）
- 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。Cisco Catalyst 8000V のライセンス情報については、Cisco Catalyst 8000V について を参照してください。
- トークンが入力されていない場合、CCR は EVAL モードになります。
- プライベート IP アドレスを ステップ 11 （104 ページ） の CCR に割り当てた場合、プライベート IP アドレスを使用して CCR のスマート ライセンスを登録するときに、**Cisco Smart Software Manager（CSSM）**に直接接続できます（**[管理（Administrative）]> > [スマート ライセンス（Smart Licensing）]**）に移動して使用可能。この場合、エクスプレスルート経由でCSSMに到達可能性を提供する必要があります。

ステップ 18 [次へ（Next)] をクリックします。

- これらの手順の前半で **[サイト間接続]** 領域の **[有効]** ボックスにチェック マークを付けた場合、**サイト間接続**は、**セットアップ- リージョン管理**の一連のステップの次のステップとして表示されます。「ステップ 19 （106 ページ）」に進みます。
- これらの手順の前半で **[サイト間接続（Inter-Site Connectivity）]** エリアの **[有効（Enabled）]** ボックスにチェック マークを付けなかった場合、**[クラウド リソース命名規則（Cloud Resource Naming Rules）]**は、**[セットアップ - リージョン管理（Setup - Region Management）]**の一連の手順の次の手順として表示されます。「ステップ 23 （106 ページ）」に進みます。

ステップ 19 テキスト ボックスにオンプレミスの IPsec トンネル ピアのピア パブリック IP アドレスを入力するには、**[IPSec トンネル ピアのパブリック IP を追加]** をクリックします。

ステップ 20 **[エリア ID]** フィールドに OSPF エリア ID を入力します。

ステップ 21 外部サブネット プールを追加するには、**[外部サブネットの追加]** をクリックし、テキスト ボックスにサブネット プールを入力します。

ステップ 22 すべての接続オプションを設定したら、ページの下部にある[次へ（Next）]をクリックします。

[クラウド リソース 命名規則（Cloud Resource Naming Rules）] ページが表示されます。

ステップ 23 **[クラウド リソースの命名規則（Cloud Resource Naming Rules）]** ページで、必要に応じてクラウド リソースの命名規則を構成します。

クラウド リソースの命名規則については、クラウドリソースの命名 （107 ページ） セクションで詳しく説明します。命名規則を変更する必要がない場合は、このページをスキップできます。

ステップ 24 終了したら **[Save and Continue（保存して続行）]** ボタンをクリックします。

スマート ライセンスの設定

このタスクでは、Cisco Cloud APIC でスマート ライセンスを設定する方法を示します。

始める前に

製品インスタンス登録トークンが必要です。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[構成（Configuration）]** を選択します。

オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[構成（Configuration）]** リストから、**[cAPIC のセットアップ（Set Up cAPIC）]** をクリックします。**[設定-概要（Set up-Overview）]** ダイアログボックスが表示され、**[DNS サーバー（DNS Servers）]**、**[リージョン管理（Region Management）]**、**[スマート ライセンス（Smart Licensing）]** のオプションが示されます。

ステップ 4 Cloud APIC をシスコの統合ライセンス管理システムに登録するには、**[スマート ライセンス（Smart Licensing）]** から、**[登録（Register）]** をクリックします。**[スマート ライセンス（Smart Licensing）]** ダイアログが表示されます。

ステップ 5 トランスポート設定を選択してください。

- **Cisco Smart Software Manager（CSSM）に直接接続する**
- **トランスポートゲートウェイ/Smart Software Managerサテライト**
- **HTTP/HTTPS プロキシ（HTTP/HTTPS Proxy）**

（注） **HTTP/HTTPS プロキシ** を選択するときは、IP アドレスが必要です。

ステップ 6 指定されたテキスト ボックスで製品インスタンス登録トークンを入力します。

ステップ 7 完了したら **[登録（Register）]** をクリックします。

クラウドリソースの命名

クラウドAPICリリース5.0（2）より前では、AzureのクラウドAPICによって作成されたクラウドリソースには、ACIオブジェクトの名前から派生した名前が割り当てられていました。

- リソースグループは、テナント、VRF、およびリージョンに基づいて作成されました。たとえば、`CAPIC_<tenant>_<vrf>_<region>`。
- VNET名は、クラウドAPIC VRFの名前と一致しました。
- サブネット名はCIDRアドレス空間から取得されました。たとえば、10.10.10.0 / 24クラウドサブネットの場合はsubnet-10.10.10.0_24です。
- クラウドアプリケーション名は、EPG名とアプリケーションプロファイル名から取得されました。たとえば、`<epg-name>_cloudapp_<app-profile-name>`

このアプローチは、クラウドリソースの命名規則が厳格な導入には適していません。また、クラウドリソースの命名とタグ付けに関するAzureのベストプラクティスに従っていません。

クラウド APIC リリース 5.0（2）以降、クラウド APIC でグローバル ネーミング ポリシーを作成できます。これにより、クラウド APIC から Azure クラウドに展開されたすべてのオブジェクトのカスタム クラウド リソース命名規則を定義できます。クラウド APIC ARM テンプレートの導入に使用される**リソース グループ**名を除き、クラウド APIC の初回セットアップ ウィザードで、すべてのクラウドリソースのカスタム命名ルールを定義できます。テンプレートのリソース グループ名は、最初に展開したときに定義され、その後は変更できません。グローバル ポリシーに加えて、REST API を使用して各クラウド APIC オブジェクトから作成されたクラウド リソースの名前を明示的に定義することもできます。

クラウド APIC リリース 5.1（2）以降、レイヤ 4ーレイヤ 7 サービスの導入では、ネットワーク ロード バランサ、アプリケーション ロード バランサ、デバイス アプリケーション セキュリティグループなどのクラウドリソースにカスタム名を指定できます。

（注） カスタム ネーミング ポリシーを使用しても、クラウドリソースが作成されると、名前を変更できないことに注意してください。既存のクラウド リソースの名前を変更する場合は、構成したすべてのクラウド リソースを削除して再作成する必要があります。削除されるクラウドソースには、セカンダリ CIDR とサブネット、Cloud APIC によって展開された CCR が含まれ、したがって、CCR からすべてのリモートサイトへの IPSec トンネルが含まれます。

命名ルールに使用できる変数

クラウドリソースの命名ポリシーを作成する場合、次の変数を使用して、オブジェクトに基づいてクラウドリソースの名前を動的に定義できます。Cisco Cloud APIC

- $ {tenant} –リソースにはテナントの名前が含まれます
- $ {ctx} –リソースにはVRFの名前が含まれます。
- $ {ctxprofile}：リソースにはクラウドコンテキストプロファイルが含まれます。これは、特定のクラウド領域に導入されたVRFです。
- $ {subnet}：リソースには文字列subnetの後にサブネットIPアドレスが含まれます。
- $ {app}：リソースにはアプリケーションプロファイルの名前が含まれます。
- $ {epg}：リソースにはEPGの名前が含まれます。
- $ {contract} –リソースには契約の名前が含まれます
- $ {region} –リソースにはクラウドリージョンの名前が含まれます。
- $ {priority}：リソースにはネットワークセキュリティグループ（NSG）ルールの優先度が含まれます。この番号は、各NSGルール名が一意になるように自動的に割り当てられます。
- $ {serviceType}：リソースにはサービスタイプの省略形が含まれます（プライベートエンドポイントリソースにのみ有効）。
- $ {resourceName}：リソースにはターゲットリソースの名前が含まれます（プライベートエンドポイントリソースにのみ有効）。
- $ {device}：リソースにはレイヤ4ーレイヤ7デバイスの名前が含まれます。
- $ {interface}：リソースには、レイヤ4ーレイヤ7のデバイスインターフェイスの名前が含まれます。
- $ {deviceInterfaceDn}：リソースには、レイヤ7デバイスインターフェイスのDNが含まれます。

プライベートエンドポイントの場合、$ {app}-$ {svcepg}-$ {subnet}-$ {serviceType}-$ {resourceName}の組み合わせにより、プライベートエンドポイント名が一意になります。これ

らの変数のいずれかを削除すると、すでに存在するプライベートエンドポイントの名前になる場合があります。これにより、によって障害が発生します。Cisco Cloud APICまた、最大長の要件はAzureサービスによって異なります。

1つ以上の上記の変数を使用してグローバル名前付けポリシーを定義すると、はすべての必須変数が存在し、無効な文字列が指定されていないことを確認するために文字列を検証します。Cisco Cloud APIC

Azureには名前の最大長の制限があります。名前の長さがクラウドプロバイダーでサポートされている長さを超えると、設定が拒否され、リソースの作成に失敗したというエラーが発生します。Cisco Cloud APICその後、障害の詳細を確認し、命名規則を修正できます。リリース5.0（2）の時点での最大長の制限を以下に示します。最新の最新情報および長さ制限の変更については、Azureのドキュメントを参照してください。Cisco Cloud APIC

次の表に、上記の各命名変数をサポートするクラウドリソースの概要を示します。アスタリスク（*）で示されたセルは、そのタイプのクラウドリソースに必須の変数を示します。プラス記号（+）で示されるセルは、これらの変数の少なくとも1つがそのタイプのクラウドリソースに必須であることを示します。たとえば、VNETリソースの場合、${ctx}、${ctxprofile}、またはその両方を指定できます。

表 *24:* クラウドリソースでサポートされる変数

Azure のリソース	`${tenant}`	`${ctx}`	`${ctxprofile}`	`${subnet}`	`${app}`	`${epg}`	`${contract}`	`${region}`	`${priority}`
リソースグループ 最長：90	○*	○*						○*	
仮想ネットワーク(VNET) 最長：64	対応	はい+	Yes+					対応	
Subnet 最長：80	○	○	○	○*				はい	
アプリケーションセキュリティグループ（ASG） 最長：80	○				○*	○*		はい	

Azure のリソース	${tenant}	${ctx}	${ctxprofile}	${subnet}	${app}	${epg}	${contract}	${region}	${priority}
ネットワーク セキュリティ グループ（NSG） 最長：80	○				○*	○*		はい	
ネットワーク セキュリティ グループ ルール 最長：80	○						○		Yes *（自動）

表 *25 :* クラウドリソースでサポートされる変数（レイヤ*4*～レイヤ*7*デバイスサービス）

Azure のリソース	${tenant}	${region}	${ctxprofile}	${device}	${interface}	${deviceInterfaceDN}
インターネット ネットワーク ロード バランサ 最長：80	○	○	○	○*		
インターネット側のネットワークロードバランサ 最長：80	○	○	○	○*		
インターネット アプリケーション ロード バランサ 最長：80	○	○	○	○*		

Azure のリソース	${tenant}	${region}	${ctxprofile}	${device}	${interface}	${deviceInterfaceDN}
インターネット向けApplication Load Balancer 最長：80	○	○	○	○*		
デバイスASG 最長：80	○	○		○*	○*	○*

命名ルールのガイドラインと制限事項

クラウドリソースの命名にカスタムルールを設定する場合、次の制限が適用されます。

- クラウドAPICの初回セットアップ時に、次の2つの命名ルールセットを使用して、グローバル命名ポリシーを定義します。
  - **[ハブ リソース命名規則（Hub Resource Naming Rules）]**は、インフラ テナントのハブ リソースグループ、ハブ VNET、オーバーレイ 1 CIDR、セカンダリ 2 CIDR サブネットの名前、およびインフラテナントのシステムによって自動的に作成されるサブネットのサブネット プレフィックスを定義します。
  - クラウドリソース名前付けルールは、ネットワークセキュリティグループ（NSG）、アプリケーションセキュリティグループ（ASG）、ネットワークロードバランサ、アプリケーションロードバランサ、デバイスアプリケーションセキュリティグループ、およびインフラテナントで作成するサブネットの名前と名前を定義します。ユーザテナント内のすべてのリソース（リソースグループ、仮想ネットワーク、サブネット、NSG、ASG、ネットワークロードバランサ、アプリケーションロードバランサ）。

  命名規則を定義したら、それらを確認して確認する必要があります。クラウドリソースを展開する前に、命名規則を確認する必要があることに注意してください。
- クラウドリソースが作成されると、その名前は変更できず、GUIで命名ポリシーを更新できません。クラウドAPICをリリース5.0（2）にアップグレードし、一部のリソースがすでにAzureに導入されている場合は、グローバルカスタム命名ルールを変更することもできません。

  既存のクラウドリソースまたはポリシーの名前を変更する場合は、GUIでグローバル名前付けポリシーを更新する前に、展開されたリソースを削除する必要があります。

  このような場合、REST APIを使用して、作成する新しいリソースにカスタム名を明示的に割り当てることができます。
- REST APIを使用してクラウドリソースの命名を更新する場合は、同時に設定をインポートしないことを推奨します。

最初に命名規則を定義することをお勧めします。それからテナント設定も行ってください。

テナント設定の展開後は、命名ポリシーを変更しないことをお勧めします。

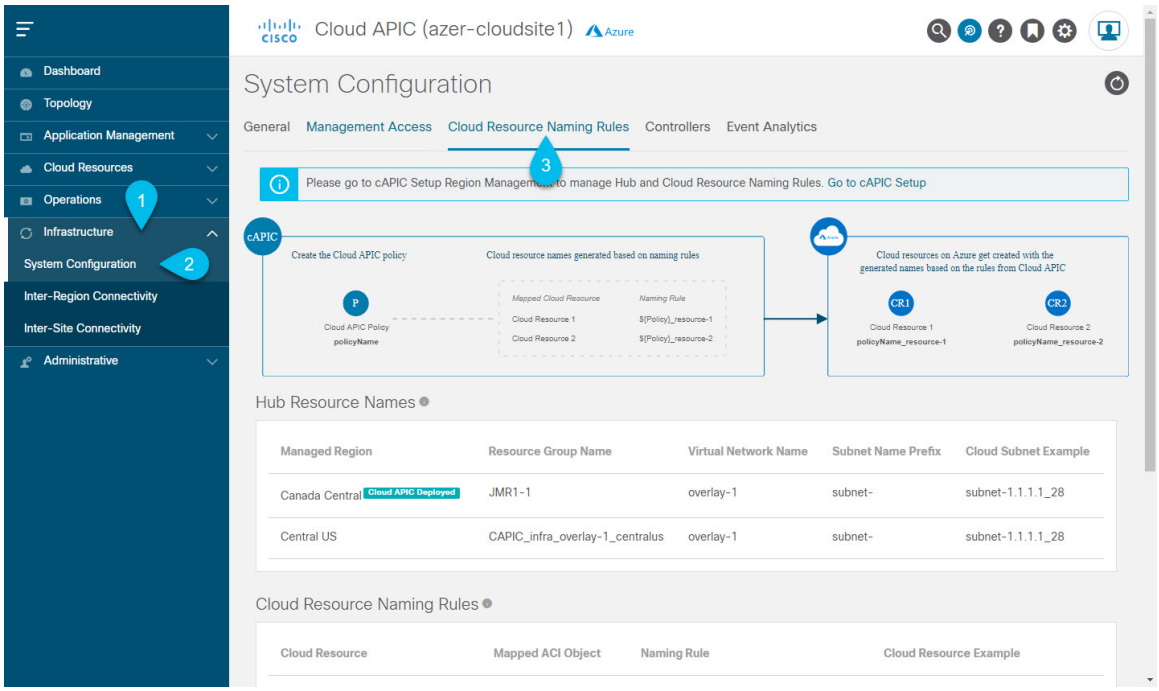
クラウド リソースの命名規則の表示

最初に、Cloud APIC を展開するときに、初回セットアップウィザードのリージョン管理部分でクラウド リソースの命名規則を定義します。これについては、『*Cisco Cloud APIC* 設置ガイド』で説明されています。初期セットアップの後、このセクションで説明されているように、Cloud APIC GUI の **[システム構成（System Configuration）]** 画面で構成した規則を表示できます。

この画面の情報は読み取り専用ビューで表示されます。最初の展開後に規則を変更する場合は、最初のセットアップウィザードを再実行する必要があります。

ステップ 1 Cloud APIC GUI にログインします。

ステップ 2 **[クラウド リソースの命名規則（Cloud Resource Naming Rules）]** 画面に移動します。



a) **[ナビゲーション（Navigation）]** サイドバーで、**[インフラストラクチャ（Infrastructure）]** カテゴリを展開します。

b) **[インフラストラクチャ（Infrastructure）]** カテゴリから、**[システム構成（System Configuration）]** を選択します。

c) **[システム構成（System Configuration）]** 画面で、**[クラウド リソースの命名規則（Cloud Resource Naming Rules）]** タブを選択します。

[クラウド リソースの命名規則（Cloud Resource Naming Rules）] タブでは、Cloud APIC からクラウドサイトに展開するリソースの名前に対して現在構成されている規則の概要を確認できます。

以前にカスタム命名規則を構成していない場合は、クラウドリソースの Cloud APIC オブジェクト名を使用するデフォルトの規則がここにリストされます。

最初のセットアップ時に定義した命名規則を受け入れなかった場合は、画面の上部に警告バナーが表示されます。

（注） クラウドリソースを展開する前に、命名規則を確認する必要があることに注意してください。

REST API を使用した Cisco Cloud APIC の構成

REST API を使用したテナントの作成

サブスクリプションには次の 2 つのタイプがあります：独自および共有。各サブスクリプション タイプにはプライマリ テナントがあります。新しい管理対象テナントまたは非管理対象テナントを作成するときに、独自のサブスクリプションを選択します。既存のプライマリ テナントの管理対象または管理対象外の設定を継承するテナントを作成するときに、共有サブスクリプションを選択します。このセクションでは、独自のタイプのサブスクリプションを使用して管理対象テナントと非管理対象テナントを作成する方法と、共有サブスクリプションを作成する方法を示します。

このセクションでは、Postman の本文からのサンプル POST 要求を使用して、REST API を使用してテナントを作成する方法を示します。

ステップ 1 独自サブスクリプションの作成。

a) クライアントシークレットを使用して非管理対象テナントを作成するには：

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="{{primary-tenant-name}}">
    <cloudAccount id="{{user-tenant-subscription-id}}" vendor="azure" accessType="credentials"
 status="">
       <cloudRsCredentials tDn="uni/tn-{{primary-tenant-name }}/credentials-{{ primary-tenant-name
 }}"/>
    </cloudAccount>
    <cloudCredentials name="{{ primary-tenant-name }}" keyId="{{application_key_id}}"
key="{{client_secret_key}}">
        <cloudRsAD tDn="uni/tn-{{ primary-tenant-name }}/ad-{{active_directory_id}}"/>
    </cloudCredentials>
    <cloudAD name="{{active_directory_name}}" id="{{active_directory_id}}" />
   <fvRsCloudAccount tDn="uni/tn-{{ primary-tenant-name }}/act-[{{ user-tenant-subscription-id
 }}]-vendor-azure" status=""/>
</fvTenant>
```

b) 管理対象テナントを作成するには：

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="{{ primary-tenant-name }}">
    <cloudAccount id="{{ user-tenant-subscription-id }}" vendor="azure" accessType="managed"
status="" />
    <fvRsCloudAccount tDn="uni/tn-{{ primary-tenant-name }}/act-[{{ user-tenant-subscription-id
 }}]-vendor-azure" status=""/>
</fvTenant>
```

ステップ 2 共有サブスクリプションの作成：

```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="{{ primary-tenant-name }}">
    <fvRsCloudAccount tDn="uni/tn-{{ primary-tenant-name }}/act-[{{ user-tenant-subscription-id
}}]-vendor-azure" status=""/>
</fvTenant>
```

REST API を使用したコントラクトの作成

この例では、REST API を使用して Cisco Cloud APIC のコントラクトを作成する方法を示します。

始める前に

フィルタを作成します。

コントラクトを作成するには：

例：

```
<polUni>
  <fvTenant name="t2" status="">
    <vzFilter descr="" name="http-family-destination" ownerKey="" ownerTag="">
      <vzEntry name="http" prot="tcp" etherT="ip" dFromPort="http" dToPort="http"/>
      <vzEntry name="https" prot="tcp" etherT="ip" dFromPort="https" dToPort="https"/>
    </vzFilter>
    <vzBrCP name="httpFamily">
      <vzSubj name="default" revFltPorts="yes" targetDscp="unspecified">
        <vzRsSubjFiltAtt action="permit" directives="" tnVzFilterName="http-family-destination"/>
      </vzSubj>
    </vzBrCP>
  </fvTenant>
</polUni>
```

REST API を使用したクラウド コンテキスト プロファイルの作成

このセクションでは、クラウド コンテキスト プロファイルを作成する方法を示します。

始める前に

VRF を作成します。

ステップ 1 基本的なクラウド コンテキスト プロファイルを作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
    <cloudCtxProfile name="cProfilewestus151">
        <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus"/>
      <cloudRsToCtx tnFvCtxName="ctx151"/>
    <cloudCidr addr="15.151.0.0/16" primary="true" status="">
          <cloudSubnet ip="15.151.1.0/24" name="GatewaySubnet" usage="gateway">
              <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="15.151.2.0/24" name="albsubnet" >
            <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
          <cloudSubnet ip="15.151.3.0/24" name="subnet" usage="">
              <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
        </cloudSubnet>
    </cloudCidr>
    </cloudCtxProfile>
  </fvTenant>
</polUni>
```

ステップ 2 VNet のセカンダリ VRF、CIDR、およびサブネットを追加するクラウド コンテキスト プロファイルを作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tenant1" status="">
        <fvCtx name="VRF1" />
        <fvCtx name="VRF2" />
        <cloudCtxProfile name="vpc1" status="">
           <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-centralus" status=""/>

            <cloudRsToCtx tnFvCtxName="VRF1" />
            <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
            <cloudCidr name="cidr1" addr="192.0.2.0/16" primary="yes" status="">
                <cloudSubnet ip="192.0.3.0/24" usage="gateway" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-centralus/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
            <cloudCidr name="cidr1" addr="193.0.2.0/16" primary="no" status="">
                <cloudSubnet ip="193.0.3.0/24" usage="" status="">
                    <cloudRsSubnetToCtx tnFvCtxName="VRF2"/>
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-centralus/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
    </fvTenant>
```

```
</polUni>
```

REST API を使用したクラウド リージョンの管理

このセクションでは、REST API を使用してクラウド リージョンを管理する方法を示します。

クラウド リージョンを作成するには:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <cloudDomP name="default">
       <cloudProvP vendor="azure">
          <cloudRegion adminSt="managed" name="eastus"><cloudZone name="default"/></cloudRegion>
          <cloudRegion adminSt="managed" name="eastus2"><cloudZone name="default"/></cloudRegion>
          <cloudRegion adminSt="managed" name="westus"><cloudZone name="default"/></cloudRegion>
        </cloudProvP>
    </cloudDomP>
</polUni>
```

REST API を使用したフィルタの作成

このセクションでは、REST API を使用してフィルタを作成する方法を示します。

フィルタを作成するには、次の手順を実行します。

```
https://<IP_Address>/api/node/mo/.xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="t15">
    <vzFilter name="rule1">
      <vzEntry etherT="ip" dToPort="22" prot="tcp" dFromPort="22" name="ssh"/>
      <vzEntry etherT="ip" prot="unspecified" name="any"/>
    </vzFilter>
    <vzFilter name="rule2">
      <vzEntry etherT="ip" dToPort="http" prot="tcp" dFromPort="http" name="http"/>
    </vzFilter>
    <vzFilter name="rule3">
      <vzEntry etherT="ip" dToPort="22" prot="tcp" dFromPort="22" name="ssh"/>
    </vzFilter>
    <vzFilter name='all_rule'>
        <vzEntry etherT="ip" prot="unspecified" name="any"/>
  </vzFilter>

    <vzBrCP name="c1">
        <vzSubj name="c1">
            <vzRsSubjFiltAtt tnVzFilterName="rule2"/>
            <vzRsSubjGraphAtt tnVnsAbsGraphName="c13_g1"/>
```

```
            <vzRsSubjFiltAtt tnVzFilterName="rule3"/>
            <vzRsSubjFiltAtt tnVzFilterName="all_rule"/>
      </vzSubj>
    </vzBrCP>

  </fvTenant>
</polUni>
```

REST API を使用したアプリケーション プロファイルの作成

このセクションでは、REST API を使用してアプリケーション プロファイルを作成する方法を示します。

始める前に

テナントを作成します。

アプリケーション プロファイルを作成する方法：

```
https://<IP_Address>/api/node/mo/.xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />


        <fvCtx name="ctx151"/>

        <cloudVpnGwPol name="VgwPol1"/>
        <cloudApp name="a1">

    </cloudApp>

  </fvTenant>
</polUni>
```

REST API を使用したネットワーク セキュリティ グループの構成

この例は、REST API を使用して、Cisco Cloud APIC の新しい **サブネットごとの NSG** 構成を設定する方法を示しています。

始める前に

セキュリティ グループに記載の情報について、確認してください。

Cisco Cloud APIC のサブネットごとの NSG 構成を設定するには、次の手順を実行します。

例：

```
<polUni>
    <cloudDomP status="">
        <cloudProvP vendor="azure">
            <cloudProvResPolCont><cloudProvSGForSubnetP enableSGForSubnet="true"
status=""/></cloudProvResPolCont>
        </cloudProvP>
    </cloudDomP>
</polUni>
```

REST API を使用した EPG の作成

このセクションの手順を使用して、REST API を使用したアプリケーション EPG、外部 EPG、サービス EPG を作成します。

REST API を使用したクラウド EPG の作成

この例では、REST API を使用してクラウド EPG を作成する方法を示します。

始める前に

アプリケーション プロファイルと VRF を作成します。

クラウド EPG を作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />


        <fvCtx name="ctx151"/>

        <cloudVpnGwPol name="VgwPol1"/>
        <cloudApp name="a1">


        <cloudEPg name="epg1">
            <cloudRsCloudEPgCtx tnFvCtxName="ctx151"/>
            <cloudEPSelector matchExpression="custom:tag1=='value1'" name="selector-1"/>
        </cloudEPg>


    </cloudApp>
```

```
  </fvTenant>
</polUni>
```

REST API を使用した外部クラウド EPG の作成

この例では、REST API を使用して外部クラウド EPG を作成する方法を示します。

始める前に

アプリケーション プロファイルと VRF を作成します。

ステップ 1 外部クラウド EPG を作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />
        <fvCtx name="ctx151"/>
        <cloudVpnGwPol name="VgwPol1"/>
        <cloudApp name="a1">
        <cloudExtEPg routeReachability="internet" name="extEpg-1">
            <fvRsCons tnVzBrCPName="extEpg-1"/>
            <cloudRsCloudEPgCtx tnFvCtxName="ctx151"/>
            <cloudExtEPSelector name="extSelector1" subnet="0.0.0.0/0"/>
       </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

ステップ 2 タイプ **site-external** で外部クラウド EPG を作成するには：

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="infra">
        <cloudApp name="a1">
        <cloudExtEPg routeReachability="site-ext" name="extEpg-1">
            <fvRsCons tnVzBrCPName="extEpg-1"/>
            <cloudRsCloudEPgCtx tnFvCtxName="overlay-2"/>
            <cloudExtEPSelector name="extSelector1" subnet="10.100.0.0/16"/>
       </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

REST API を使用したサービス EPG の作成

この例では、REST API を使用してサービス EPG を作成する方法を示します。

始める前に

- クラウド サービスエンドポイント グループの情報を確認してください。
- アプリケーション プロファイルと VRF を作成します。

ステップ 1 クラウド ネイティブの展開タイプでサービス EPG を作成するには、次の手順を実行します。

例：

```
<cloudSvcEPg name="Storage" type="Azure-Storage" accessType="Private" deploymentType="CloudNative">

    <cloudPrivateLinkLabel name="ProductionSubnets"/>
    <cloudRsCloudEPgCtx tnFvCtxName="HUB-SERVICES-VRF"/>
    <cloudSvcEPSelector matchExpression="ResourceName=='StorageAcct1'" name="selector-1"/>
    <cloudSvcEPSelector matchExpression="custom:Tag=='ProdStorage'" name="selector-2"/>
</cloudSvcEPg>
```

ステップ 2 クラウド ネイティブ管理対象の展開タイプでサービス EPG を作成するには、次の手順を実行します。

例：

```
<cloudSvcEPg name="APIM" type="Azure-ApiManagement" accessType="Private"
deploymentType="CloudNativeManaged" status="">
    <cloudRsCloudEPgCtx tnFvCtxName="infra-SvcCtx" />
    <fvRsCons tnVzBrCPName="infra-APIM-Mock"/>
    <fvRsProv tnVzBrCPName="infra-managedAPIM" status=""/>
    <cloudSvcEPSelector matchExpression="IP=='10.21.52.0/28'" name="sel1" status=""/>
</cloudSvcEPg>
```

ステップ 3 サードパーティの展開タイプでサービス EPG を作成するには：

例：

```
<cloudSvcEPg name="SaaS-Hub" type="Custom"  accessType="Private" deploymentType="Third-party"
status="">
    <cloudRsCloudEPgCtx tnFvCtxName="infra-SvcCtx" status=""/>
    <cloudSvcEPSelector
matchExpression="URL=='saassvcepg.286b0377-a9b7-40d7-a94f-67abe03ce5f4.centralus.azure.privatelinkservice'"
 name="s1" status=""/>
    <cloudPrivateLinkLabel name="saas-hub" status=""/>
    <fvRsProv tnVzBrCPName="SaaS-Hub" status=""/>
</cloudSvcEPg>
```

REST API を使用したクラウド テンプレートの作成

このセクションでは、REST API を使用してクラウド テンプレートを作成する方法を示します。クラウド テンプレートの詳細については、クラウド テンプレートの概要 を参照してください。

REST API は、選択したライセンス モデルのタイプによって異なります。Cisco Catalyst 8000V のライセンス タイプは、`cloudtemplateProfile` 管理対象オブジェクトの `routerThroughput` プロパティによって取得されます。

routerThroughput 値が **T0/T1/T2/T3** に属している場合、**BYOL** Cisco Catalyst 8000V が Cisco Cloud APIC に展開されます。routerThroughput 値が **PAYG** の場合、**PAYG** Cisco Catalyst 8000V が Cisco Cloud APIC に展開されます。

始める前に

ステップ 1 **BYOL** Cisco Catalyst 8000V を展開するためのクラウド テンプレート ポストを作成するには、次の手順を実行します。

```
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" numRemoteSiteSubnetPool="2" numRoutersPerRegion="2"
status="" vrfName="overlay-1">
         <cloudtemplateProfile name="default" routerPassword="cisco123" routerUsername="cisco"
routerThroughput="250M" routerLicenseToken="thisismycsrtoken" />
              </cloudtemplateProfile>
      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>

      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="azure" region="westus"/>
        <cloudRegionName provider="azure" region="westus2"/>
      </cloudtemplateIntNetwork>

      <cloudtemplateExtNetwork name="default">
        <cloudRegionName provider="azure" region="westus2"/>

        <cloudtemplateVpnNetwork name="default">

          <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />

          <cloudtemplateOspf area="0.0.0.1"/>

        </cloudtemplateVpnNetwork>

      </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

ステップ 2 **PAYG** Cisco Catalyst 8000V を展開するためのクラウド テンプレート ポストを作成するには、次の手順を実行します。

```
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" numRemoteSiteSubnetPool="2" numRoutersPerRegion="2"
status="" vrfName="overlay-1">
         <cloudtemplateProfile name="default" routerPassword="cisco123" routerUsername="cisco"
routerThroughput="PAYG" vmType="DS2V2" />
              </cloudtemplateProfile>
cloudtemplateProfile name="default" routerPassword="cisco123" routerUsername="cisco"
routerThroughput="250M" routerLicenseToken="thisismycsrtoken" />
              </cloudtemplateProfile>
      <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>

      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="azure" region="westus"/>
        <cloudRegionName provider="azure" region="westus2"/>
```

```
      </cloudtemplateIntNetwork>

      <cloudtemplateExtNetwork name="default">
        <cloudRegionName provider="azure" region="westus2"/>

        <cloudtemplateVpnNetwork name="default">

          <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
          <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />

          <cloudtemplateOspf area="0.0.0.1"/>

        </cloudtemplateVpnNetwork>

      </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

PAYG スループットを選択する場合、ユーザは、Cloud APIC によって作成され、管理対象オブジェクト `vmName` によって表される vmNames のリストから **VmType** も選択する必要があります。

次の表に、`cloudtemplateProfile` のプロパティ `vmType` によって示される vmNames タイプを示します。

Azure 上の VmName	メモリ	vCPU の数	ネットワーク帯域
DS2V2	7GiB	2	最大 1.5 ギガビット
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

REST API を使用して VRF リーク ルートの構成

始める前に

このセクションの手順を実行する前に、内部 VRF 間のルート リーク と グローバルな Inter-VRF ルート リーク ポリシー に記載されている情報を確認してください。

ステップ 1 次のような投稿を入力して、契約ベースのルーティングを有効または無効にします。

```
<fvTenant name="infra">
    <cloudVrfRouteLeakPol name="default" allowContractBasedRouting="true"/>
</fvTenant>
```

`allowContractBasedRouting` フィールドには、次のいずれかの設定があります。

- **true** : ルート マップがない場合、契約に基づいてルートが漏洩していることを示します。有効に設定されている場合、ルートマップが構成されていないときに、ドライブ回送を契約します。ルートマップが存在するときに、ルート マップは常にドライブ回送です。
- **false**: デフォルト設定です。ルートが契約に基づいてリークされておらず、代わりにルート マップに基づいてリークされていることを示します。

ステップ 2 次のような投稿を入力して、leakInternalPrefix フィールドを使用して、VRF に関連付けられたすべてのクラウド CIDR のルート リークを設定します。

```
<fvTenant name=”t1”>
  <fvCtx name="v1">
    <leakRoutes>
      <leakInternalPrefix ip="0.0.0.0/0" le="32">
        <leakTo tenantName="t2" ctxName="v2" scope="public"/>
      </leakInternalPrefix>
    </leakRoutes>
  </fvCtx>
</fvTenant>

<fvTenant name=”t2”>
  <fvCtx name="v2">
    <leakRoutes>
      <leakInternalPrefix ip="0.0.0.0/0" le="32">
        <leakTo tenantName="t1" ctxName="v1" scope="public"/>
      </leakInternalPrefix>
    </leakRoutes>
  </fvCtx>
</fvTenant>
```

ステップ 3 次のような投稿を入力して、leakInternalSubnet フィールドを使用して、VRF のペア間の特定のルートをリークします。

```
<fvTenant name=”anyTenant" status="">
    <fvCtx name="VRF1" >
        <leakRoutes status="">
            <leakInternalSubnet ip="110.110.1.0/24" >
                <leakTo ctxName=”VRF2" scope="public" tenantName=" anyTenant " />
            </leakInternalSubnet>
        </leakRoutes>
    </fvCtx>
    <fvCtx name="VRF2" status="" >
        <leakRoutes status="">
            <leakInternalSubnet ip="110.110.2.0/24" >
                <leakTo ctxName=”VRF1" scope="public" tenantName=" anyTenant " />
            </leakInternalSubnet>
        </leakRoutes>
    </fvCtx>
</fvTenant>
```

REST API を使用したトンネルのソース インターフェイス選択の構成

始める前に

このセクションの手順を実行する前に、トンネルのソース インターフェイスの選択 に記載されている情報を確認してください。

次のような投稿を入力して、トンネルの送信元インターフェイスの選択を構成します。

```
<cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
  <cloudtemplateProfile name="defaultxyz" routerUsername="james" routerPassword="bond@@7" />

  <cloudtemplateIpSecTunnelSubnetPool subnetpool="10.20.0.0/16" poolname="pool1" />

  <cloudtemplateIntNetwork name="default">
    <cloudRegionName provider="aws" region="us-west-1"/>
    <cloudRegionName provider="aws" region="us-west-2"/>
  </cloudtemplateIntNetwork>

  <cloudtemplateExtNetwork name="something" vrfName="xyz" >
    <cloudRegionName provider="aws" region="us-west-2"/>
    <cloudtemplateVpnNetwork name="default">
      <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" poolname="" presharedkey="abcd"
ikeVersion="v1|v2">
          <cloudtemplateIpSecTunnelSourceInterface sourceInterfaceId="2" />
      </cloudtemplateIpSecTunnel>
    </cloudtemplateVpnNetwork>
  </cloudtemplateExtNetwork>
</cloudtemplateInfraNetwork>
```

グローバルクラウドリソースの命名規則の定義または特定のオブジェクトの名前のオーバーライド

このセクションでは、クラウド リソースに名前を付けるためのグローバル ポリシーを構成したり、特定のクラウド リソースの名前をオーバーライドしたりするために使用できる REST API POST の例を示します。

（注） カスタム命名規則を確実にサポートできるようにするために、クラウド リソース名をオブジェクトごとに定義できます。これらの明示的な名前のオーバーライドは Cloud APIC GUI では使用できず、REST API を使用してのみ実行できます。名前を定義するには、グローバル クラウド リソースの名前付けポリシーを使用することをお勧めします。明示的な名前のオーバーライドは、グローバルな名前付けポリシーを使用して名前付け要件を満たすことができない場合にのみ使用する必要があります。

ステップ 1 ハブ リソースの命名規則を作成するには：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" numRemoteSiteSubnetPool="2"
    numRoutersPerRegion="2" status="" vrfName="overlay-1">
      <cloudtemplateIntNetwork name="default">
        <cloudRegionName provider="azure" region="west's" status="">
          <cloudtemplateRegionNameCustomization ctxProfileName="infra-vnet"
          resourceGroupName="infra-rh" subnetNamePrefix="snet-" />
        </cloudRegionName>
      </cloudtemplateIntNetwork>
    </cloudtemplateInfraNetwork>
  </fvTenant>
</polUni>
```

ステップ 2 クラウド リソースの命名規則を作成するには：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <cloudDomP name="default">
    <cloudNaming
    azResourceGroup="${tenant}-network-${ctx}-${region}-rg"
    azVirtualNetwork="${tenant}-${ctxprofile}-vnet"
    azSubnet="${tenant}-${ctxprofile}-snet-${subnet}"
    azNetworkSecurityGroup="${app}-${epg}-nsg"
    azApplicationSecurityGroup="${app}-${epg}-asg"
    azNetworkSecurityGroupRule="${contract}--${priority}"
    internetApplicationBalancer="agw-e-${device}"
    internalApplicationBalancer="agw-i-${device}"
    internetNetworkBalancer="lbe-${device}"
    internalNetworkBalancer="lbi-${device}"
    l4L7DeviceApplicationSecurityGroup="${deviceInterfaceDn}"
   reviewed="yes" />
  </cloudDomP>
</polUni>
```

ステップ 3 特定の Cloud APIC オブジェクトに対応する Azure クラウド リソース名をオーバーライドするには:

API を使用してカスタム名を指定するときに、同じ変数）たとえば、 `${tenant}` ）を使用できます。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<fvTenant name="ExampleCorp" status="">
  <fvRsCloudAccount status="" tDn="uni/tn-infra/act-[<infra-subscription>]-vendor-azure"/>
  <fvCtx name="VRF1"/>
  <cloudApp name="App1">
   <cloudEPg name="Db" azNetworkSecurityGroup="db-nsg" azApplicationSecurityGroup="db-asg-${region}">

     <cloudRsCloudEPgCtx tnFvCtxName="VRF1"/>
     <cloudEPSelector matchExpression="custom:EPG=='db'" name="100"/>
   </cloudEPg>
  </cloudApp>
  <cloudCtxProfile name="c02" azResourceGroup="custom-tc-rg1" azVirtualNetwork="vnet1">
    <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus"/>
    <cloudRsToCtx tnFvCtxName="VRF1"/>
    <cloudCidr addr="10.20.20.0/24" name="cidr1" primary="yes" status="">
      <cloudSubnet ip="10.20.20.0/24" name="subnet1" azSubnet="s1" status="">
        <cloudRsZoneAttach status="" tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
```

```
      </cloudSubnet>
    </cloudCidr>
  </cloudCtxProfile>
</fvTenant>
```

ステップ 4 特定の Cloud APIC オブジェクトに対応するレイヤ 4 からレイヤ 7 の Azure クラウド リソース名をオーバーライドするには：

API を使用してカスタム名を指定するときに、同じ変数（たとえば、`${tenant}` ）を使用できます。

ロード バランサのポリシーを上書きします。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
 <fvTenant>
 <cloudLB name="ALB" type="application" scheme="internet" size="small" instanceCount="2" status=""
 nativeLBName=”ALB” >
                <cloudRsLDevToCloudSubnet
tDn="uni/tn-{{tenantName}}/ctxprofile-c1/cidr-[31.10.0.0/16]/subnet-[31.10.80.0/24]" status="" />
        </cloudLB>
 </fvTenant>
```

デバイス ASG のオーバーライド ポリシー：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
 <fvTenant>
 <cloudLDev name="{{FWName}}" status="" l4L7DeviceApplicationSecurityGroup="Group1" >
            <cloudRsLDevToCtx tDn="uni/tn-{{tenantName}}/ctx-VRF1" status=""/>
            </cloudLIf>
        </cloudLDev>
 <fvTenant>
```

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。