# 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） 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

## テナントの作成

次のセクションでは、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方法。

Cloud APIC での Google Cloud の展開について で説明したように、各 Cisco Cloud APIC テナントは Google Cloud プロジェクトに 1 対 1 でマッピングします。Cisco Cloud APIC テナント用の Google Cloud プロジェクトがまだ作成されていない場合は、次の手順に従って Google Cloud プロジェクトを作成します。

1. Google アカウントにログインします。
2. **[IAM と管理（IAM＆Admin）]** > **[リソースの管理（Manage resources）]**に移動します。

3. ページの上部にある **[組織の選択（Select Organization）]** ドロップダウン リストを使用して、プロジェクトを作成する組織を選択します。
4. **[+プロジェクトの作成（+ CREATE PROJECT）]** をクリックします。
5. 表示される **[新規プロジェクト（New Project）]** ウィンドウで、プロジェクト名を入力し、必要に応じて課金アカウントを選択します。

   プロジェクト名には、文字、数字、一重引用符、ハイフン、スペース、または感嘆符のみを含めることができ、4〜30 文字にする必要があります。
6. **[ロケーション（Location）]** フィールドに親組織またはフォルダを入力します。

   そのリソースは、新しいプロジェクトの階層的な親になります。
7. [CREATE] をクリックします。

## Google Cloud および Cisco Cloud APIC GUI を使用した管理対象テナントの作成

このセクションでは、GUIを使用して Cisco Cloud APIC により管理されるテナントを作成する方法について説明します。

**ステップ 1** 必要に応じて、この Cisco Cloud APIC テナントに関連付ける新しい Google Cloud プロジェクトを作成します。

Cloud APIC での Google Cloud の展開について で説明したように、各 Cisco Cloud APIC テナントは Google Cloud プロジェクトに 1 対 1 でマッピングされます。必要な場合は、これらの手順について テナントの作成 （1 ページ） を参照してください。

**ステップ 2** Cisco Cloud APIC GUI で **[アプリケーション管理（Application Management）]** > **[テナント（Tenants）]** に移動します。

すでに設定されているテナントのテーブルが表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックし、**[テナントの作成（Create Tenant）]**を選択します。

**[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

| Properties | 説明 |
|---|---|
| **[名前（Name）]** | テナント名を入力します。正規表現の一致:<br>`[a-z]([-a-z0-9]*[a-z0-9])?`<br>このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。 |

| Properties | 説明 |
|---|---|
| 説明 | テナントの説明を入力します。 |
| **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。<br>**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。<br>**2.** セキュリティ ドメインをクリックして選択します。<br>**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。 |
| **Google Cloud プロジェクト** | |
| **Google Cloud プロジェクト ID** | この Cisco Cloud APIC テナントに関連付けるGoogle Cloud プロジェクトIDを入力します。 |
| アクセス タイプ（**Access Type**） | Cisco Cloud APIC によって管理されるテナントの場合、アクセス タイプとして **[管理対象外 ID（Unmanaged Identity）]** を選択します。<br>詳細については、Cloud APIC での Google Cloud の展開についてを参照してください。 |
| **Google Cloud Project のセキュリティ ドメインを追加** | （注） テナントの作成時の Google Cloud のセキュリティ ドメインの追加はオプションです。<br>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。<br>**1.** **[Google Cloud Project のセキュリティ ドメインの追加（Add Security Domain for Google Cloud Project）]** 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。<br>**2.** セキュリティ ドメインをクリックして選択します。<br>**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 **[保存（Save）]** をクリックします。

**ステップ 6** アクセス タイプとして **[管理対象アイデンティティ（Managed Identity）]** を選択したため、次に Google Cloud でこのテナントに必要な権限を設定します。

a) Google Cloud GUIで、この Cisco Cloud APIC テナントに関連付けられている Google Cloud プロジェクトにログインします。
このプロジェクトの **ダッシュボード** が表示されます。
b) 左ナビゲーション バーで、**[IAM と管理（IAM & Admin）]** をクリックし、**[IAM]** を選択します。

**[IAM]** ウィンドウが表示され、いくつかのサービス アカウントが表示されます。

c) Cisco Cloud APIC インフラ アカウントに関連付けられているプロジェクトで Cisco Cloud APIC によって作成されたサービス アカウントを見つけます。
d) サービス アカウント名をコピーします。
e) このサービス アカウント名を、ユーザー テナント プロジェクトの IAM ユーザーとして追加します。
f) このサービス アカウントの権限を設定します。

1. このサービス アカウントの行にある鉛筆アイコンをクリックします。

   **[権限の編集（Edit Permissions）]** ウィンドウが表示されます。

2. **[+別のロールの追加（+ ADD ANOTHER ROLE）]** をクリックし、ロールとして **[クラウド機能サービス エージェント（Cloud Functions Service Agent）]** を選択します。

   サービス アカウントが表示された **[IAM]** ウィンドウに戻ります。

3. **[+別のロールの追加（+ ADD ANOTHER ROLE）]** を再度クリックし、このサービス アカウントに必要な残りのロールを追加します。

   以下は、このプロセスの最初のステップで追加したクラウド機能サービス エージェントを含む、このサービス アカウントに割り当てる必要があるロールの完全なリストです。

   - クラウド機能サービス エージェント
   - コンピューティング インスタンス管理（v1）
   - コンピューティング ネットワーク管理
   - コンピューティング セキュリティ管理
   - ログインしている管理
   - パブ/サブ管理
   - ストレージ管理者

4. 必要なすべてのロールを追加した後で、**[保存（Save）]** をクリックします。

   **IAM** ウィンドウに戻り、サービス アカウントが表示され、必要なロールがこのサービス アカウントに割り当てられます。

## Google Cloud および Cisco Cloud APIC GUI を使用した管理対象外テナントの作成

ここでは、GUI を使用して Cisco Cloud APIC の管理対象外のテナントを作成する方法について説明します。

**ステップ 1** 必要な場合は、この Cisco Cloud APIC と関連付けられる新しい Google Cloud プロジェクトを作成します。

Cloud APIC での Google Cloud の展開について で説明したように、各 Cisco Cloud APIC テナントは Google Cloud プロジェクトに 1 対 1 でマッピングします。必要な場合は、これらの手順について テナントの作成 （1 ページ） を参照してください。

**ステップ 2** Google Cloud で、Cisco Cloud APIC テナントに関連付けられている Google Cloudプロジェクトを選択します（まだ選択していない場合）。

**ステップ 3** 左ナビゲーション バーで、**[IAM および Admin]** をクリックして、**[サービス アカウント（Service Accounts）]** を選択します。

この Google Cloud プロジェクトのサービス アカウントが表示されます。

**ステップ 4** 既存のサービス アカウントを選択するか、**[+サービス アカウントの作成（+ CREATE SERVICE ACCOUNT）]** をクリックして新しいアカウントを作成します。

このサービス アカウントの情報が表示され、**[詳細（Details）]** タブがデフォルトで選択されています。

**ステップ 5** **[キー（KEYS）]** タブをクリックします。

**ステップ 6** **[ADD KEY（キーの作成）]** > **[新しいキーの作成（Create New Key）]**をクリックします。

このサービスアカウントの秘密キーを作成するためのオプションを提供するウィンドウが表示されます。

**ステップ 7** **JSON** キー タイプを選択したまま、**[作成（Create）]** をクリックします。

秘密キーがコンピュータに保存されたことを示すウィンドウが表示されます。

**ステップ 8** コンピュータにダウンロードした JSON ファイルを見つけて、コンピュータ上の安全な場所に移動します。

この JSON ファイルには、管理対象外テナントのフィールドに入力する必要があるキー情報が含まれています。


**ステップ 9** Cisco Cloud APIC GUI で **[アプリケーション管理（Application Management）]** > **[テナント（Tenants）]** に移動します。

すでに設定されているテナントのテーブルが表示されます。

**ステップ 10** **[アクション（Actions）]** をクリックし、**[テナントの作成（Create Tenant）]**を選択します。

**[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 11** 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 *2 :* テナント ダイアログボックス フィールドの作成

| Properties | 説明 |
|---|---|
| **[名前（Name）]** | テナント名を入力します。正規表現の一致:<br>`[a-z]([-a-z0-9]*[a-z0-9])?`<br>このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。 |
| **説明** | テナントの説明を入力します。 |
| **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。<br>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。<br>2. セキュリティ ドメインをクリックして選択します。<br>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。 |
| **Google Cloud プロジェクト** | |
| **Google Cloud プロジェクト ID** | この Cisco Cloud APIC テナントに関連付ける Google Cloud プロジェクト IDを入力します。 |
| **アクセス タイプ（Access Type）** | Cisco Cloud APIC によって管理されないテナントの場合は、アクセスタイプとして **[管理対象外 ID（Unmanaged Identity）]** を選択します。<br>詳細については、Cloud APIC での Google Cloud の展開についてを参照してください。 |
| **キー ID** | これらの手順の最初にダウンロードした JSON ファイルの `private_key_id` フィールドの情報を入力します。 |

| Properties | 説明 |
|---|---|
| **RSA プライベート キー** | これらの手順の最初にダウンロードしたJSONファイルの `private_key` フィールドの情報を入力します。 |
| **Client ID** | これらの手順の最初にダウンロードしたJSONファイルの `client_id` フィールドの情報を入力します。 |
| **Email** | Google Cloud プロジェクトに関連付けられている E メール アドレスを入力します。 |
| **Google Cloud Project のセキュリティドメインを追加** | （注） テナントの作成時の Google Cloud のセキュリティ ドメインの追加はオプションです。<br><br>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。<br>1. **[Google Cloud Project のセキュリティ ドメインの追加（Add Security Domain for Google Cloud Project）]** 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。<br>2. セキュリティ ドメインをクリックして選択します。<br>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 12　設定が終わったら **[保存（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** [Name] フィールドに名前を入力します。

次の制約事項に注意してください。

- 正規表現の一致:

  `[a-z]([-a-z0-9]*[a-z0-9])?`

  このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

- 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 を参照してください。

**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 **[保存（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。

（注）　外部 VRF を設定するには、下の **[テナント（Tenant）]** フィールドで [インフラ（infra）] を選択します。VRF は次の場合に 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
- 外部ネットワークに関連付けられています（Cisco Cloud APIC GUI を使用した外部ネットワークの作成 （10 ページ） を参照）。
- 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ません

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

| Properties | 説明 |
| --- | --- |
| **General** | |

<table>
<tr><th>Properties</th><th>説明</th></tr>
<tr><td>Name</td><td> [Name] フィールドに、VRF の表示名を入力します。 次の制約事項に注意してください。 <ul><li>正規表現の一致: <code>[az]（[-a-z0-9] * [a-z0-9]）?</code> このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。 </li><li>可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 を参照してください。</li></ul> 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。 </td></tr>
<tr><td>テナント</td><td> テナントを選択します。 <ol><li>[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。</li><li>[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。 </li></ol></td></tr>
<tr><td>説明</td><td>VRF の説明を入力します。</td></tr>
</table>

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 CSR 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。Cisco Cloud APIC は 1 つのハブ ネットワークのみをサポートするため、**[ハブ ネットワーク（Hub Network）]** 列には 1 つのハブ ネットワークのみが表示されます。

**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。

（注） ハブネットワークがまだ設定されていない場合は、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する必要があることを示す警告がページの上部に表示されます。メッセージ内の青い `[Cloud APIC のセットアップ（Cloud APIC Setup）]` リンクをクリックしてハブ ネットワークを作成し、ここに戻ります。ハブネットワークの作成の詳細については、『Cisco Cloud APIC for Google CloudInstallation Guide、Release 25.0(x)』の「Configuring Cisco Cloud APIC Using the Setup Wizard」の章を参照してください。

**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 *4 : [*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

| Properties | 説明 |
|---|---|
| **General** | |
| **Name** | 外部ネットワーク名を入力します。 |

| Properties | 説明 |
|---|---|
| **VRF** | この 外部 VRF は、オンプレミス CSR 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。<br><br>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。<br><br>• インフラ テナントの下で構成された<br>• 外部ネットワークに関連付けられている<br>• 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<br><br>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。この時点では、外部 VRF はインフラ テナント以外のテナントで作成することはできず、外部 VRF はクラウド 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。<br><br>外部 VRF を選択するには、次の手順を実行します。<br><br>1. **[VRF の選択（Select VRF）]** をクリックします。<br>**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。<br>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。<br>**[+ 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。<br>3. **[選択（Select）]** をクリックします。<br>**[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。 |
| **ハブ ネットワーク** | ハブ ネットワークは、初回セットアップで設定した後に自動的に表示されます。<br><br>（注） ハブ ネットワークがまだ設定されていない場合は、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する必要があります。ハブネットワークの作成の詳細については、『Cisco Cloud APIC for Google CloudInstallation Guide、Release 25.0(x)』の「Configuring Cisco Cloud APIC Using the Setup Wizard」の章を参照してください。 |
| **VPN ルータ** | このフィールドは編集できません。デフォルトの VPN ルータが自動的に選択されます。 |
| **Settings** | |

| Properties | 説明 |
| --- | --- |
| **[Regions]** | リージョンを選択するには:<br>1. **[リージョンの追加（Add Region）]** をクリックします。<br>**[リージョンの選択（Select Regions）]** ダイアログボックスが表示されます。<br>• 初回セットアップの一部として選択したリージョンがここに表示されます。<br>• 複数のリージョンを選択して、複数のリージョンでクラウドルータを起動できます。<br>2. **[リージョンの選択（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。<br>**[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。 |

<table>
<tr><th>Properties</th><th>説明</th></tr>
<tr><td>VPN ネットワーク</td><td>VPNネットワークエントリは、内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。<br><br>VPN ネットワークを追加するには、次の手順を実行します。<br><br>1. [VPNネットワークの追加（Add VPN Network）] をタップします。<br>[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。<br><br>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。<br><br>3. [+ IPSec ピアの追加（+ Add IPSec Peer）] をクリックします。<br>IPSec ピア エントリごとに 2 つのトンネルが作成されます。<br><br>4. 追加する IPSec ピアの次のフィールドに値を入力します。<br>• IPSec トンネル ピアの パブリック IP<br>• Pre-Shared Key; 事前共有キー<br>• IKE バージョン（IKE Version）：IPSec トンネル接続用に ikev1 または ikev2 を選択します。<br>• BGP ピア ASN<br>• サブネット プール名（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。<br>[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。<br><br>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。<br>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。<br><br>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。<br>[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。</td></tr>
</table>

**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 Google Cloud で構成されます。

Google Cloud でクラウドルータがで構成されていることを確認するには、インフラ VPC の Google Cloud アカウントで、**[ハイブリッド接続（Hybrid Connectivity）]** > **[クラウドルータ（Cloud Routers）]** に移動します。さまざまなリージョン用に作成されたクラウドルータが表示されます（新しく設定されたクラウドルータを表示するには、[更新（Refresh）]をクリックする必要があります）。

IPSec セッションを表示するには、**[ハイブリッド接続（Hybrid Connectivity）]** > **[VPN]** > **[クラウド VPN トンネル（Cloud VPN Tunnels）]** に移動します。

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

VRF 間ルートリークを使用すると、独立したルーティング ポリシーを設定して、次のタイプのサイト間のルーティングを設定するときに、VRF のペア間でリークするルートを指定できます。

- 2 つのクラウド サイト
- クラウド サイトと非 ACI オンプレミス サイト

（注） 詳細については、ルーティング ポリシーとセキュリティ ポリシーの個別の構成 を参照してください。

**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*）

| Properties | 説明 |
|---|---|
| **Source VRF** | 送信元 VRF を選択するには：<br>**1.** **[送信元 VRF の選択（Select Source VRF）]** をクリックします。<br>**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。<br>**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。<br>送信元VRFは、内部または外部（トランスポート）VRF であることに注意してください。<br>**3.** **[選択（Select）]** をクリックして、この送信元 VRF を選択します。<br>**[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。 |

| Properties | 説明 |
|---|---|
| **宛先 VRF** | 宛先 VRF を選択するには、次の手順を実行します。<br>1. **[宛先の選択（Select destination）]** をクリックします。<br>**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。<br>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。<br>3. **[選択（Select）]** をクリックして、この宛先 VRF を選択します。<br>**[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。 |
| **Type** | 構成するリーク ルートのタイプを選択します。<br>• **[すべてリーク（Leak All）]**：VRF 間でリークするすべてのルートを設定する場合に選択します。<br>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。<br>• **サブネット IP**：VRF 間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。<br>**[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。<br>VRF 間のリークのルートとして複数のサブネット IP アドレスを設定するには、異なるサブネットの追加エントリを入力します。 |

**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 **[別のルートの追加（Add Another 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 （15 ページ）ーステップ 5 （16 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 ルートの追加（Add Reverse 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 （15 ページ） ーステップ 5 （16 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 （15 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 （15 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。

# Google Cloud と外部デバイス間の接続の有効化

Google Cloud ルータと外部デバイス間の接続を手動で有効にするには、次の手順に従います。

## 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 **[接続（Connectivity）]** 領域の **[外部接続ステータス（External Connectivity Status）]** で、**[クラウド ルータ（Cloud Routers）]** エントリの上にある番号をクリックします。

**[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、Google Cloud ルーターと外部デバイス間の接続を有効にするため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。

## Google Cloud と外部デバイスの間の接続の有効化

### 始める前に

外部デバイス構成ファイルのダウンロード （17 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ます。

ステップ 1 Google Cloud と外部デバイスの間の接続を有効にするために必要な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 デバイスをクラウド ACI ファブリックに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 （17 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。

次に、vpn-connectivity 設定ページから **PRESHARED-KEY** を取得した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 54.215.245.58 5.500 for
hcextnwTunnIf.acct-[infra]/region-[us-west1]/hubCtx-[1]-id-[0]/ext-[extnwfoo_us-west1]/vpn-[vpnnwfoo]/rtr-default-peer-54.215.245.58/src-1-dest-[54.215.245.58]
! USER-DEFINED: please define rd: RD
! USER-DEFINED: please provide preshared-key: PRESHARED-KEY
! USER-DEFINED: please define router-id: ROUTER-ID
! USER-DEFINED: please define gig-number: GIG-NUMBER
! USER-DEFINED: please define gig-gateway: GIG-GATEWAY
! ikev: ikev2
! vrf-name: extv1
! user name: root
! tunnel counter: 5
! IPV4 address: 35.220.50.132
! tunnel interface destination: 54.215.245.58
! tunne id: 500
! BGP peer address: 169.254.10.6
! BGP peer neighbor address: 169.254.10.5
```

```
! BGP peer ASN: 64513
! hcloudHubCtx ASN: 64512

vrf definition extv1
    rd RD:1
    address-family ipv4
    exit-address-family
exit

interface Loopback0
    vrf forwarding extv1
    ip address 41.41.41.41 255.255.255.255
exit


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
exit

crypto ikev2 policy ikev2-1
    proposal ikev2-1
exit

crypto ikev2 keyring keyring-root-5
    peer peer-ikev2-keyring
        address 35.220.50.132
        pre-shared-key PRESHARED-KEY
    exit
exit

crypto ikev2 profile ikev-profile-root-5
    match address local interface GIG-NUMBER
    match identity remote address 35.220.50.132 255.255.255.255
    identity local address 54.215.245.58
    authentication remote pre-share
    authentication local pre-share
    keyring local keyring-root-5
    lifetime 3600
    dpd 10 5 periodic
exit

crypto ipsec transform-set ikev-transport-root-5 esp-gcm 256
    mode tunnel
exit

crypto ipsec profile ikev-profile-root-5
    set transform-set ikev-transport-root-5
    set pfs group14
    set ikev2-profile ikev-profile-root-5
exit

interface Tunnel500
    vrf forwarding extv1
    ip address 169.254.10.6 255.255.255.252
    ip mtu 1400
    ip tcp adjust-mss 1400
    tunnel source GIG-NUMBER
    tunnel mode ipsec ipv4
    tunnel destination 35.220.50.132
    tunnel protection ipsec profile ikev-profile-root-5
exit
```

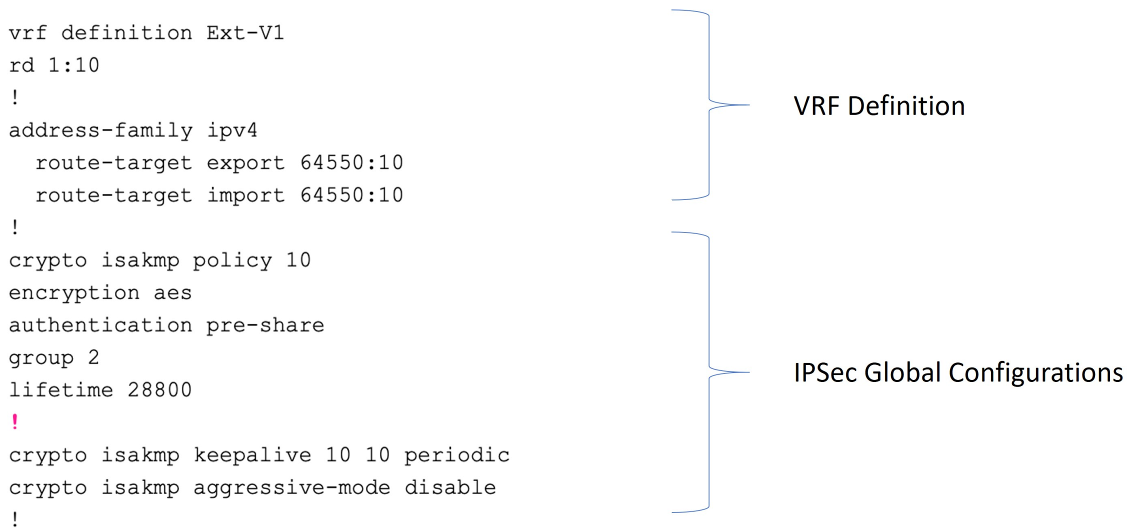
```
ip route 35.220.50.132 255.255.255.255 GIG-NUMBER GIG-GATEWAY

router bgp 64513
    bgp router-id ROUTER-ID
    bgp log-neighbor-changes

    address-family ipv4 vrf extv1
        network 41.41.41.41 mask 255.255.255.255
        neighbor 169.254.10.5 remote-as 64512
        neighbor 169.254.10.5 ebgp-multihop 255
        neighbor 169.254.10.5 activate
    exit-address-family
exit
```

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




- 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

# Cisco Cloud APIC GUI を使用した EPG の作成

アプリケーション EPG または外部 EPG を作成するには、このセクションの手順を使用します。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。

### 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

| Properties | 説明 |
|---|---|
| **General** | |

<table>
<tr><th>Properties</th><th>説明</th></tr>
<tr><td>Name</td><td>EPG の名前を入力します。<br>次の制約事項に注意してください。<br>• 正規表現の一致:<br><code>[a-z]([-a-z0-9]*[a-z0-9])?</code><br>このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。<br>• 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 を参照してください。</td></tr>
<tr><td>テナント</td><td>テナントを選択します。<br>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。<br>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。<br>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。</td></tr>
<tr><td>アプリケーション プロファイル</td><td>アプリケーション プロファイルを選択します。<br>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。<br>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。<br>（注）　インフラ テナントで EPG を作成している場合、オーバーレイ-1 VRF でそのアプリケーション プロファイルがしようされているため、<code>cloud-infra</code> アプリケーション プロファイルを選択しないことをお薦めします。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。<br>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。</td></tr>
<tr><td>説明</td><td>EPG の説明を入力します。</td></tr>
<tr><td colspan="2">Settings</td></tr>
</table>

| Properties | 説明 |
|---|---|
| **Type** | 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。<br>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。<br>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。<br>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。 |

| Properties | 説明 |
|---|---|
| エンドポイントセレクタ | |

<table>
<tr><th>Properties</th><th>説明</th></tr>
<tr><td></td><td>
（注）　エンドポイント セレクタ構成プロセスの一部として、Google Cloud の仮想マシンを構成する方法については、Google Cloud の仮想マシン セキュリティの設定（44 ページ）を参照してください。<br><br>
エンドポイント セレクタを追加するには：<br><br>
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。<br><br>
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。<br><br>
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。<br><br>
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。<br>
• 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。<br>
• エンドポイント セレクタに Google Cloud 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。<br>
• 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。<br>
（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）。<br><br>
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。<br>
• [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。<br>
• [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。<br>
• [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。<br>
• [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。<br>
• [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。<br>
• [キーを持たない（does not have key）]：キーを含まない式に使用されます。<br><br>
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
</td></tr>
</table>

| Properties | 説明 |
|---|---|
| | 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。<br>**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。<br>**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。<br>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。<br>• エンドポイント セレクタ 1、式 1:<br>• **[キー (Key):]** Region<br>• **演算子（Operator）**： equals<br>• **値**：us-west1<br>• エンドポイント セレクタ1、式 2:<br>• **[キー (Key):]** IP<br>• **演算子 (Operator)**： equals<br>• **[値 (Value):]** 192.0.2.1/24<br>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 us-west1 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。 |

<table>
<tr><th>Properties</th><th>説明</th></tr>
<tr><td></td><td>
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。
<ul><li>エンドポイント セレクタ 2、式 1:
<ul><li>[キー (Key):] Region</li>
<li>演算子： in</li>
<li>値：us-east1、us-central1</li></ul></li></ul>
その場合、次のようになります。
<ul><li>リージョンが us-west1 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) 場合<br>または</li>
<li>リージョンが us-east1 または us-central1 (エンドポイント セレクタ 2 の式) のいずれかである場合</li></ul>
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。
</td></tr>
</table>

**ステップ 5** 設定が終わったら **[保存（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。

### 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

| Properties | 説明 |
|---|---|
| **General** | |
| **Name** | EPG の名前を入力します。<br>次の制約事項に注意してください。<br>• 正規表現の一致:<br>`[a-z]([-a-z0-9]*[a-z0-9])?`<br>このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。<br>• 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 を参照してください。 |
| テナント | テナントを選択します。<br>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。<br>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。<br>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。 |

| 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。<br>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。<br>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。<br>（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。<br>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。 |
| **Settings** | |
| **Type** | 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。 |
| **VRF** | VRF を選択するには、次の手順を実行します。<br>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。<br>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。<br>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が自動的に選択されます（**Internet** または **外部サイト** のいずれか）。 |

<table>
<tr><th>Properties</th><th>説明</th></tr>
<tr><td>エンドポイントセレクタ</td><td>
（注） エンドポイントセレクタ設定プロセスの一部として Google Cloud で仮想マシンを設定する手順については、Google Cloud の仮想マシン セキュリティの設定 （44 ページ） を参照してください。<br><br>
エンドポイント セレクタを追加するには：<br><br>
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。<br>
2. [Name] フィールドに名前を入力します。<br>
3. サブネットにサブネットを入力します。<br>
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。<br>
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。<br><br>
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。<br><br>
• エンドポイントセレクタ 1：<br>
　• 名前：EP_Sel_1<br>
　• サブネット：192.1.1.1/24<br>
• エンドポイント セレクタ 2：<br>
　• 名前：EP_Sel_2<br>
　• サブネット：192.2.2.2/24<br><br>
その場合、次のようになります。<br><br>
• 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<br>
または<br>
• 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<br><br>
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。
</td></tr>
</table>

**ステップ 5** 設定が終わったら **[保存（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 *8 :* フィルタの作成ダイアログボックスのフィールド

| 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。 |
| テナント | テナントを選択します。<br>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。<br>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。 |

<table>
<tr><th>Properties</th><th>説明</th></tr>
<tr><td>Add Filter</td><td>フィルタを追加するには、次の手順を実行します。<br>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。<br>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。<br>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。<br>• IP<br>• [Unspecified]<br>（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。<br>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。<br>• ICMP<br>• [TCP]<br>• UDP<br>• [Unspecified]<br>（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。<br>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。<br>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。</td></tr>
</table>

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 9 : [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**

| Properties | 説明 |
| --- | --- |
| **[名前（Name）]** | 契約の名前を入力します。<br><br>次の制約事項に注意してください。<br><br>• 正規表現の一致:<br><br>`[a-z]([-a-z0-9]*[a-z0-9])?`<br><br>このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。<br><br>• Google Cloud ファイアウォール ルールによる制限のため、この名前には 14 文字以下を使用することをお勧めします。ファイアウォールルール名を構成する各 Cisco Cloud APIC コンポーネントに使用できる制限と文字数の合計については、Google Cloud ファイアウォール ルールによる命名の長さの制限 を参照してください。 |

| Properties | 説明 |
|---|---|
| テナント | テナントを選択します。<br>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。<br>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。<br>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。 |
| **Settings** | |
| 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。<br>（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。<br>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。<br>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。<br>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。<br>• **アプリケーション プロファイル**<br>• **VRF**<br>• **Global**<br>• **テナント** |
| **Add Filter** | フィルタを選択します。<br>1. [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。<br>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。<br>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。

# 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。

### 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 *10 : [*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

| Properties | 説明 |
|---|---|
| **[名前（Name）]** | 契約の名前を入力します。<br><br>これは Google Cloud のコントラクトの名前です。正規表現の一致:<br><br>`[az]（[-a-z0-9] * [a-z0-9]）？`<br><br>このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。 |
| テナント | テナントを選択します。<br><br>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。<br><br>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。<br><br>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。 |

| Properties | 説明 |
|---|---|
| 説明 | コントラクトの説明を入力してください。 |
| **Settings** | |
| スコープ | このスコープは、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 グループにコントラクトを制限します。<br>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。<br>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。 |
| **Add Filter** | フィルタを選択します。<br>**1.** [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。<br>**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。<br>**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（**[ア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。

# 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 ***11*** **:** 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

| 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。正規表現の一致:<br>`[a-z]([-a-z0-9]*[a-z0-9])?`<br>このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。 |
| テナント | テナントを選択します。<br>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。<br>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:<br>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。<br>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。 |

| Properties | 説明 |
|---|---|
| **VRF** | VRF を選択するには、次の手順を実行します。<br>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。<br>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。 |

<table>
<tr><th>Properties</th><th>説明</th></tr>
<tr><td>CIDR の追加（Add CIDR）</td><td>
（注）　プライマリおよびセカンダリ CIDR とサブネット グループラベルの詳細については、Google Cloud の下の VPC とサブネット、およびクラウド APIC でのクラウドコンテキストプロファイルについて を参照してください。<br><br>
CIDR を追加するには、次の手順を実行します。<br><br>
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。<br>
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。<br>
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。<br>
• クラウド コンテキスト プロファイルごとに少なくとも 1 つのプライマリ CIDR を追加する必要があります。<br>
• VPC のセカンダリ CIDR とサブネットを追加する場合は、[プライマリ（Primary）] ボックスをオフのままにします。<br>
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。<br>
• [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。<br>
• [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。<br>
• [サブネット グループ ラベル（Subnet Group Label）] フィールドで、次のいずれかを選択します。<br>
　• 既存のものを選択（Select Existing）：[サブネット グループ ラベルの選択（Select Subnet Group Label）] をクリックし、このサブネットに関連付ける既存のサブネット グループ ラベルを選択します。<br>
　• 新規作成（Create New）：このサブネットに関連付けるサブネットグループラベルの一意の名前を入力します。<br>
5. [VRF] フィールドで、必要に応じて選択します。<br>
• [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。<br>
• [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。<br>
6. 完了したら、[追加（Add）] をクリックします。
</td></tr>
</table>

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

# Google Cloud の仮想マシン セキュリティの設定

Cisco Cloud APIC のためのエンドポイント セレクタを設定するとき、Cisco Cloud APICを設定するエンドポイントセレクタに対応するGoogle Cloudで必要なインスタンスについても設定することが必要になります。

このトピックでは、Google Cloud で仮想マシンを設定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 セレクタを設定する前に、または後で、これらの要件を使用して Google Cloud のインスタンスを設定することができます。

たとえば、エンドポイントセレクタのタイプとして **[カスタム（Custom）]** を使用するとします（エンドポイントおよびエンドポイント セレクタを参照）。

- Google Cloud のアカウントに移動し、 Google Cloud でカスタムタグまたはラベルを使用してしてから、Cisco Cloud APIC 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もできます。
- 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、Google Cloud のアカウントに移動し、Google Cloud 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

Google Cloud 仮想マシンの設定プロセスの一環として、クラウド コンテキスト プロファイルを設定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 プロファイルを設定すると、VRF やリージョンの設定などの設定情報は、Google Cloud 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
- Google Cloud プロジェクト 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 Google Cloud インスタンス設定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。Google Cloud 仮想マシンを設定するときに、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 ユーザー テナントの Google Cloud 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 プロファイル設定から収集した情報を使用して Google Cloud VM の作成を開始します。

（注） Google Cloud ポータルで VM を作成する方法の詳細については、Google Cloud 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 *12 :* 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

| Properties | 説明 |
|---|---|
| **General** | |
| **Name** | バックアップ構成の名前を入力します。 |

| Properties | 説明 |
|---|---|
| 説明 | バックアップ構成の説明を入力します。 |
| **Settings** | |
| **Backup Destination** | バックアップ接続先を選択します。<br>• **Local**<br>• **[リモート（Remote）]** |

| **Properties** | 説明 |
| --- | --- |
| バックアップ オブジェクト | |

<table>
<tr><th>Properties</th><th>説明</th></tr>
<tr><td></td><td>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
<ul>
<li>ポリシー ユニバース</li>
<li>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。
<ol>
<li>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。
<ul>
<li>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。</li>
<li>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。</li>
<li>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。</li>
<li>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。</li>
<li>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。</li>
<li>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。</li>
<li>[クラウド コンテキスト プロファイル（Cloud Context Profile）]：これを選択すると、[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。</li>
</ul></li>
<li>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</li>
</ol></li>
</ul></td></tr>
</table>

| Properties | 説明 |
| --- | --- |
| | ます。<br>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。<br>（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。<br>• **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。<br>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。<br>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 | 次のいずれかを選択します。<br>• **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。<br>• **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 **[保存（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 *13 :* 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

| Properties | 説明 |
|---|---|
| **General** | |
| **Name** | 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。 |
| **Settings** | |

| Properties | 説明 |
|---|---|
| エクスポート先 | エクスポート先を選択します。<br>• コントローラ<br>• **[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。<br>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。<br>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。 |

**ステップ 5** 設定が終わったら **[保存（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 *14 :* スケジューラの作成ダイアログボックスのフィールド

| **Properties** | **説明** |
| --- | --- |
| **General** | |
| **Name** | 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。 |
| **Settings** | |

| Properties | 説明 |
|---|---|
| 繰り返しウィンドウ | |

<table>
<tr><th>Properties</th><th>説明</th></tr>
<tr><td></td><td>[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。<br><br>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。<br>• 毎日（Every Day）<br>• 偶数日（Even Days）<br>• 奇数日（Odd Days）<br>• [Monday]<br>• [Tuesday]<br>• [Wednesday]<br>• [Thursday]<br>• [Friday]<br>• [Saturday]<br>• [Sunday]<br><br>2. [開始時間（Start Time）] フィールドに、時間を入力します。<br><br>3. [最大同時タスク数（Maximum Concurrent Tasks）] フィールドで、次のいずれかを選択します。<br>• 無制限（Unlimited）：スケジューラ ウィンドウに適用できる同時タスクの最大数はありません。<br>• カスタム（Custom）：2番目の [最大同時タスク数（Maximum Concurrent Tasks）] フィールドに、同時に処理できるタスクの最大数を入力します。このフィールドに許容される最大値は 65535 レコードです。<br><br>4. [最大実行時間（Maximum Running Time）] フィールドで、次のいずれかを選択します。<br>• 無制限（Unlimited）：スケジューラ ウィンドウに適用される時間制限はありません。<br>• カスタム（Custom）：2 番目の[最大実行時</td></tr>
</table>

| Properties | 説明 |
|---|---|
| | 間（**Maximum Running Time**）**]** フィールドに、ウィンドウの最大継続時間を入力します。このフィールドで使用できる形式は `dd:hh:mm:ss` です。<br>**5.** 終了したら、[Add] をクリックします。 |
| 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。<br>**1.** **[開始時間（Start Time）]** フィールドに、時間を入力します。<br>**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。<br>**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。<br>**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 **[保存（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 *15*: 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

| **Properties** | 説明 |
| --- | --- |
| **General** | |
| **Name** | 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。 |
| **Settings** | |
| **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 |
| **Protocol** | プロトコルを選択します。<br>• **[FTP]**<br>• **SFTP**<br>• **SCP** |
| **Path** | リモート ロケーションのパスを入力します。 |
| **Port** | リモート ロケーションのポートを入力します。 |
| **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 | SFTP または SCP を使用する場合は、認証タイプを選択します。<br>• **Password**<br>• **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 **[保存（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 16 : 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**

| 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。<br>• **Local**<br>• **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。<br>• **RADIUS**：プロバイダーを追加する必要があります。<br>• **TACACS+**：プロバイダーの追加が必要です。<br>• **SAML**：プロバイダーの追加が必要です。 |

| 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。<br>**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。<br>**2.** クリックしてプロバイダーを選択します。<br>**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 | 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。<br>• **Cisco AV ペア**：（デフォルト）<br>• **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。 |

| Properties | 説明 |
|---|---|
| **LDAP グループ マップ ルール** | |

| 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。<br>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。<br>2. **[名前（Name）]** フィールドに、ルールの名前を入力します。<br>3. **[説明（Description）]** フィールドに、ルールの説明を入力します。<br>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。<br>5. セキュリティ ドメインの追加：<br>  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。<br>  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 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。<br>  3. セキュリティ ドメインをクリックして選択します。<br>  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。<br>  5. ユーザー ロールを追加する:<br>    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から、**[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で、左側のペインにロールのリストが表示されま |

| Properties | 説明 |
|---|---|
| | す。<br>2. クリックして、ロールを選択します。<br>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。<br>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。<br>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。<br>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 **[保存（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 **[タイプ（Type）]** フィールドで、セキュリティ ドメインのタイプを選択します。

- **制限なし（Unrestricted）**：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 ドメインで設定されたポリシー、プロファイル、またはユーザーを表示できます。
- **制限あり（Restricted）**：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 ドメインで設定されたポリシー、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 **[保存（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 *17 :* ロールの作成ダイアログボックスのフィールド

| Properties | 説明 |
|---|---|
| **General** | |
| **Name** | **[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。 |
| **Settings** | |

| Properties | 説明 |
| --- | --- |
| 特権 | |

| 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。<br>• **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。<br>• **access-connectivity**：インフラでのレイヤ1ー3の設定、テナントのL3Outでのスタティック ルート設定、管理インフラポリシー、およびテナント ERSPAN ポリシーに使用されます。<br>• **access-equipment**：アクセスポートの設定に使用されます。<br>• **access-protocol**：インフラストラクチャ、NTP、SNMP、DNS、およびイメージ管理用のファブリック全体のポリシー、およびクラスタ 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 ポリシーでレイヤ 1ー3 のプロトコル設定に使用されます。<br>• **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。<br>• **admin**：すべてへのアクセス（すべてのロールの組み合わせ）<br>• **config-manager**<br>• **custom-port-privilege**<br>• **custom-privilege-1 〜 custom-privilege-22**<br>• fabric-connectivity：ファブリック、ファームウェア、および導入ポリシーのレイヤ1ー3の設定に使用します。ポリシー導入の影響を推定するための警告、およびリーフスイッチと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を生成します。<br>• **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。<br>• **fabric-protocol**：ファブリックでのレイヤ 1ー3 のプロトコル設定、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、ERSPAN およびヘルス スコア ポリシー、および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。<br>• **none**：特権なし。<br>• **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。<br>• **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。<br>• **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。 |

| Properties | 説明 |
|---|---|
| | • **site-admin**<br>• **site-policy**<br>• **tenant-connectivity**：ブリッジ ドメイン、サブネット、および VRF を含むレイヤ1ー3 の接続変更に使用されます。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。テナントのインバンドおよびアウトオブバンド管理接続設定。アトミック カウンタやヘルススコアなどのデバッグ/モニタリング ポリシー。<br>• **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。<br>• **tenant-ext-connectivity**：書き込みアクセス ファームウェア ポリシーに使用されます。テナント L2Out および L3Out 設定の管理。デバッグ/モニタリング/オブザーバ ポリシー。<br>• **tenant-ext-protocol**：BGP、OSPF、PIM、IGMP などのテナント外部レイヤ1ー3 プロトコルの管理、およびtraceroute、ping、oam、eptrk などのデバッグ/モニタリング/オブザーバ ポリシーに使用されます。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。<br>• **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。<br>• **tenant-protocol**：テナント下のレイヤ 1ー3 プロトコルの設定、テナント traceroute ポリシー、およびファームウェア ポリシーの書き込みアクセスに使用されます。<br>• **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。<br>• **tenant-security**：テナントの契約関連の設定に使用されます。<br>• **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。 |

**ステップ 5** 設定が終わったら **[保存（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 *18 :* 証明書認証局の作成ダイアログボックスのフィールド

| **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。 |
| **用途** | 次のオプションから選択します。<br>• **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。<br>• **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。<br>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。<br>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。 |

| Properties | 説明 |
|---|---|
| **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。<br>（注） チェーンの証明書を次の順序で追加します。<br>**1.** CA<br>**2.** Sub-CA<br>**3.** サブサブCA<br>**4.** サーバー |

ステップ 5 設定が終わったら **[保存（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 ***19*** **:** キー リングの作成ダイアログボックスのフィールド

| Properties | 説明 |
|---|---|
| **[名前（Name）]** | キー リングの名前を入力します。 |

| Properties | 説明 |
|---|---|
| 説明 | キー リングの説明を入力します。 |
| 用途 | • **System**：キー リングはシステム用です。<br>• **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。 |
| テナントの選択 | テナントを選択します。<br>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。<br>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。 |
| **Settings** | |
| 認証局 | 認証局を選択するには：<br>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。<br>2. 左側の列で認証局をクリックして選択します。<br>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（**Private Key**） | 次のいずれかを選択します。<br>• **[新しいキーの生成（Generate New Key）]**：新しいキーを生成します。<br>• **[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。 |

| Properties | 説明 |
|---|---|
| 秘密キー（**Private Key**） | **[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）。 |
| **Modulus** | **[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。<br>• **MOD 512**<br>• **MOD 1024**<br>• **MOD 1536**<br>• **MOD 2048**：デフォルト |
| 証明書 | **[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 **[保存（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 ***20*** *:* 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

| Properties | 説明 |
|---|---|
| **Username** | 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。 |

| Properties | 説明 |
|---|---|
| 説明 | ローカル ユーザーの説明を入力します。 |
| **Settings** | |
| 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。<br>• **Active**：ローカル ユーザー アカウントをアクティブにします。<br>• **Blocked**：ローカルユーザーアカウントをブロックします。<br>• **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（First Name）]** | 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（**Email Address**） | ローカル ユーザーの E メール アドレスを入力します。 |
| **Phone Number** | ローカル ユーザーの 電話番号を入力します。 |

| Properties | 説明 |
| --- | --- |
| セキュリティ ドメイン | |

<table>
<tr><th>Properties</th><th>説明</th></tr>
<tr><td></td><td>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。<br><br>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。<br><br>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。<br><br>3. セキュリティ ドメインをクリックして選択します。<br><br>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。<br><br>5. ユーザー ロールを追加する:<br><br>    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。<br><br>    2. クリックしてロールを選択します。<br><br>    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。<br><br>    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。<br><br>    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</td></tr>
</table>

| Properties | 説明 |
|---|---|
| | クして、確認します。<br>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 *21 :* 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 |
|---|---|
| **Account Expires** | **[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。 |
| ユーザー証明書属性 | ユーザー証明書の属性。 |
| 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。<br>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。<br>2. [Name] フィールドに名前を入力します。<br>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。<br>4. [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。<br>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。<br>2. [Name] フィールドに名前を入力します。<br>3. **[キー（Key）]** テキストボックスに SSH キーを入力します。<br>4. [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 **[保存（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）

Google Cloud では、VPC リソースはすべての Google Cloud リージョンにまたがるグローバルリソースです。デフォルトでは、すべてのリージョンがGoogle Cloudによって管理され、リージョン間接続が存在します。Cloud APIC は、25 の Google Cloud リージョンすべてを管理します。

**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** **[ワークフロー（Workflows）]** 領域で、**[Cloud APIC の設定（Cloud APIC 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 3** **[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。
**[リージョン管理（Region Management）]** ウィンドウが表示されます。

**ステップ 4** 外部接続を構成するかどうかを決定します。

**[有効化（Enable）]** の横にあるボックスをクリックして、外部接続を有効にします。

**ステップ 5** ページ内のすべてのリージョンが選択されていることを確認します。

このページには、Google Cloud でサポートされているすべてのリージョンが表示されます。すべてのリージョンは Cloud APIC によって管理されます。

ステップ 6 ページの下部にある **[次へ（Next）]** をクリックします。

外部接続を有効にした場合は、**[一般接続（General Connectivity）]** ページが表示されます。

ステップ 7 **[ハブ ネットワーク（Hub Network）]** 領域に必要な情報を入力します。

ハブ ネットワーク管理は、特定の管理対象リージョンにクラウドルータを展開するために使用されます。クラウド サイトのファブリック インフラ接続を設定し、このエリアのクラウド サイトのクラウド ルータに使用する構成テンプレートを定義します。

次の制約事項に注意してください。

- Google Cloud のハブ ネットワークは 1 つだけ作成できます。
- ハブ ネットワークでは、Google Cloud に1 つのクラウドルータのみが作成されます。

a) [Hub Network] 領域で、[Add Hub Network] をクリックします。

**[Add Hub Network ]** ウィンドウが表示されます。

b) **[Name]** フィールドにハブ ネットワークの名前を入力します。

c) **[BGP 自律システム番号（BGP Autonomous System Number）]** フィールドに値を入力します。

BGP 自律システム番号（ASN）は、クラウドサイト内の BGP ピアリングと、他のサイトへの MP-BGP IPv4 ピアリングに使用されます。

ASN はプライベート ASN である必要があります。各ハブ ネットワークに 64512～65534 または 4200000000～4294967294 の値を入力し、フィールドの横にあるチェックマークをクリックします。

d) **[リージョン（Region）]** フィールドで、適切なリージョンを選択します。

このエリアには、最大 4 つのリージョンを追加してハブ ネットワークを展開できます。ハブ ネットワークは、選択した各リージョンに 1 つのクラウド ルータを作成します。

e) **[VPN ルータ（VPN Router）]** フィールドに VPN ルータの名前を入力します。

インフラ VPC は、クラウド ルータと VPN ゲートウェイを使用して、オンプレミス サイトまたはその他のクラウド サイトへの IPSec トンネルと BGP セッションを作成します。 スポーク VPC は、インフラ VPC とピアリングして、外部サイトへの VPN 接続を共有します。

ステップ 8 **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** 領域に必要な情報を入力します。

a) **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** 領域で、**[IPSec トンネル サブネット プールの追加（Add IPSec Tunnel Subnet Pools）]** をクリックします。

**[IPSec トンネル サブネット ツールの追加（Add IPSec Tunnel Subnet Pools）]** ウィンドウが表示されます。

b) 必要に応じて、IPSec トンネルに使用するサブネット プールを入力します。

デフォルトでは、`169.254.0.0/16`のサブネットプールが設定され、IPsec トンネルが作成されます。必要に応じて、既存のサブネット プールを削除し、サブネット プールを追加できます。

**IPSec トンネル サブネット プール エントリ**に使用されるサブネットは、`169.254.0.0/16` ブロックの共通 /30 CIDR である必要があります。たとえば、`169.254.7.0/24` と `169.254.8.0/24` は、このフィールドのサブネット プールの許容エントリです。

適切なサブネット プールに入力したら、チェック マークをクリックします。

**ステップ 9** このページに必要な情報をすべて入力したら、ページの下部にある [保存して続行（Save and Continue）] をクリックします。

必要に応じて、外部ネットワークを作成し、外部接続設定を完了するオプションが表示されます。これらの手順については、Cisco Cloud APIC GUI を使用した外部ネットワークの作成 （10 ページ） にアクセスしてください。

# 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

### 始める前に

このセクションの手順を実行する前に、Cloud APIC での Google Cloud の展開について に記載されている情報を確認してください。

**ステップ 1** 複数のテナント間で同じログイン情報を共有するには、次の POST を入力します。各テナントで `cloudCredentials` オブジェクトを複製し、同じ Google Cloud サービス アカウントを指定します。

次の点に注意してください。

- テナント `T1` は、サービス アカウントの秘密キーを保持する `cloudCredentials` オブジェクトを定義します。
- テナント `T1` と `T2` は両方とも、`cloudRsCredentials` リレーションを介してこの `cloudCredentials` オブジェクトを参照します。
- テナント `T1` によって定義されたサービス アカウントは、このシナリオの Google Cloud プロジェクト `project1` および`project2` のメンバーである必要があります。
- テナント T2 の POST で強調表示された領域は、最初のユーザー テナントと共有されるログイン情報を示します。

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

<fvTenant name="T1">
    <cloudAccount id="project1" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-T1/credentials-creds1" />
    </cloudAccount>
    <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
```

```
rsaPrivateKey="-----BEGIN .... -----END PRIVATE KEY-----\n" clientId="28763876"
email="capic-395@project2.iam.gserviceaccount.com"/>
    <fvRsCloudAccount tDn="uni/tn-T1/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
    <cloudAccount id="project2" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-T2/credentials-creds1" />
    </cloudAccount>
   <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
rsaPrivateKey="-----BEGIN .... -----END PRIVATE KEY-----\n" clientId="28763876"
email="capic-395@project2.iam.gserviceaccount.com"/>
    <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
</fvTenant>
```

**ステップ 2** Cloud APIC が Google Cloud（ログイン情報を持つインフラ テナント）の外部で実行されるユーザー テナントを作成するには、次の手順を実行します。

Google Cloudに追加された新しいプロパティは、以下で強調表示されていることに注意してください。

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

<fvTenant name="infra">
    <cloudAccount id="project1" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-infra/credentials-creds1" />
    </cloudAccount>
    <cloudCredentials name="creds1" keyId="de22a1bc-7872-4651-9d09-c5d820af7e1c"
rsaPrivateKey="-----BEGIN .... -----END PRIVATE KEY-----\n" clientId="28763876"
email="capic-395@project2.iam.gserviceaccount.com"/>
    <fvRsCloudAccount tDn="uni/tn-infra/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
    <cloudAccount id="project2" vendor="gcp" accessType="credentials" >
        <cloudRsCredentials tDn="uni/tn-infra/credentials-creds1" />
    </cloudAccount>
    <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
</fvTenant>
```

**ステップ 3** ユーザーが複数の Google Cloud プロジェクトでインフラサービス アカウントを共有する管理対象ユーザー テナントを作成するには、次の手順を実行します。

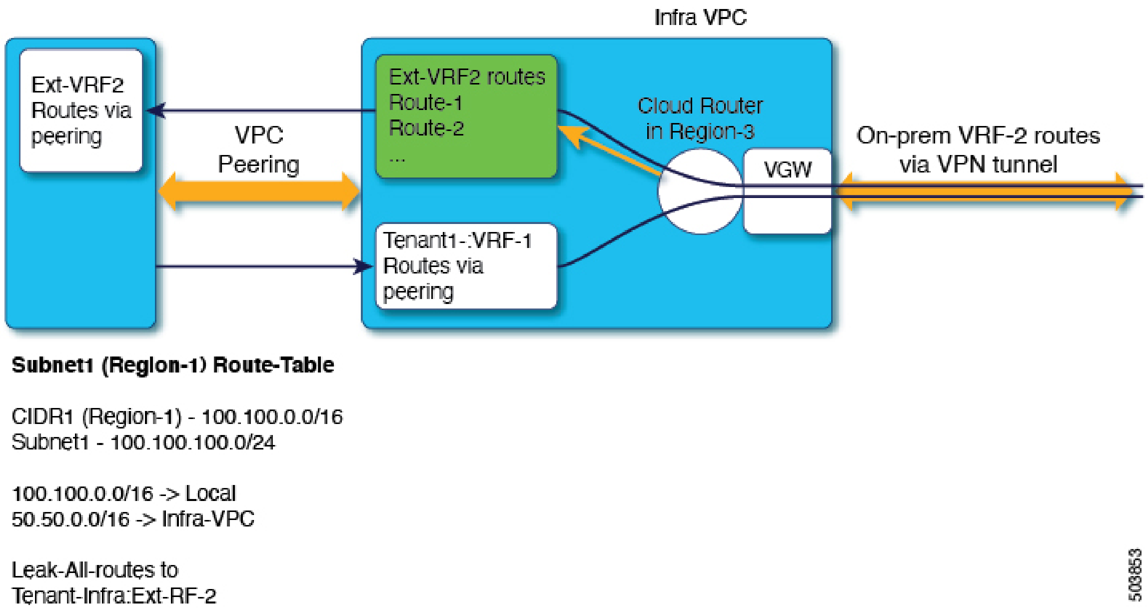
```
POST https://<cloud-apic-ip-address>/api/mo/uni.xml

<fvTenant name="infra">
    <cloudAccount id="project1" vendor="gcp" accessType="managed" />
    <fvRsCloudAccount tDn="uni/tn-infra/acct-[project1]-vendor-gcp"/>
</fvTenant>

<fvTenant name="T2">
    <cloudAccount id="project2" vendor="gcp" accessType="managed" />
    <fvRsCloudAccount tDn="uni/tn-T2/acct-[project2]-vendor-gcp"/>
</fvTenant>
```

# REST API を使用して VRF 間のルート リークの構成

この例では、REST API を使用した Cloud APIC のリーク ルートを構成する方法を示します。この例では、次の図に示すように、外部 VRF とクラウド VRF 間の VRF 間ルート リークを設定する方法を示します。




この例では、VRF 間ルート リークを設定します。

**例：**

```
<polUni>
    <fvTenant name="t1">
        <fvCtx name="VRF1">
            <leakRoutes>
                <leakInternalPrefix ip="0.0.0.0/0" status="">
                    <leakTo tenantName="infra" ctxName="Ext-VRF2" scope="public" status=""/>
                </leakInternalPrefix>
            </leakRoutes>
        </fvCtx>
        <cloudCtxProfile name="v1-us-west1" type="regular" vpcGroup="one" status="">
            <cloudRsToCtx tnFvCtxName="VRF1"/>
            <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1"/>
            <cloudCidr addr="100.100.0.0/16" primary="yes">
                <cloudSubnet ip="100.100.100.0/20" scope="public,shared" subnetGroup="one">
                   <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>

                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
    </fvTenant>
    <fvTenant name="infra" status="">
        <fvCtx name="Ext-VRF2">
            <leakRoutes>
                <leakExternalPrefix ip="0.0.0.0/0" status="">
                    <leakTo tenantName="t1" ctxName="VRF1" scope="public" status=""/>
```

```
                </leakInternalPrefix>
            </leakRoutes>
        </fvCtx>
    </fvTenant>
</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：

```
<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>
```

コントラクトの名前（`vzBrCP` エントリ）には次の制限があることに注意してください。

- 正規表現の一致:

  `[a-z]([-a-z0-9]*[a-z0-9])?`

  このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

- 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 を参照してください。

# 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="cProfilewest1151">
        <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1"/>
      <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-gcp/region-us-west1/zone-default"/>
```

```
        </cloudSubnet>
        <cloudSubnet ip="15.151.2.0/24" name="albsubnet" >
            <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
        </cloudSubnet>
          <cloudSubnet ip="15.151.3.0/24" name="subnet" usage="">
              <cloudRsZoneAttach tDn="uni/clouddomp/provp-gcp/region-us-west1/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-gcp/region-us-central1" 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-gcp/region-us-central1/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-gcp/region-us-central1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
    </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-[<gcp-id>]-vendor-gcp" />


        <fvCtx name="ctx151"/>

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

    </cloudApp>

  </fvTenant>
</polUni>
```

アプリケーション プロファイル名については、次の制約事項に注意してください。

- 正規表現の一致:

  `[a-z]([-a-z0-9]*[a-z0-9])?`

  このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

- 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 を参照してください。

# REST API を使用した EPG の作成

REST API を使用してアプリケーション EPG または外部 EPG を作成するには、このセクションの手順を使用します。

## 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。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
```

```
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<gcp-id>]-vendor-gcp" />


        <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>
```

次の制約事項に注意してください。

- 正規表現の一致:

  `[a-z]([-a-z0-9]*[a-z0-9])?`

  このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

- 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 を参照してください。

## 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。

外部 EPG の名前については、次の制約事項に注意してください。

- 正規表現の一致:

  `[a-z]([-a-z0-9]*[a-z0-9])?`

  このことは、最初の文字が小文字でなければならず、その後のすべての文字がハイフン、小文字、または数字でなければなりません。ただし、最後の文字にはハイフンを使用できません。

- 可能な場合、Google Cloud ファイアウォール ルールにより課される制限のために、この名前に対して 14 文字以下を使用することをお勧めします。ファイアウォール ルール名を構成する各 Cisco Cloud APIC コンポーネントの制約と許可される合計文字数については、Google Cloud ファイアウォール ルールによる命名の長さの制限 を参照してください。

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-[<gcp-id>]-vendor-gcp" />
        <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** の外部クラウド EPG、またはインフラ L3Out 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="infra">
        <cloudApp name="a1">
        <cloudExtEPg routeReachability="site-ext" name="extEpg-1">
            <fvRsCons tnVzBrCPName="extEpg-1"/>
            <cloudRsCloudEPgCtx tnFvCtxName="ctx152"/>
            <cloudExtEPSelector name="extSelector1" subnet="10.100.0.0/16"/>
       </cloudExtEPg>
    </cloudApp>
  </fvTenant>
</polUni>
```

# REST API を使用したクラウド ルータ、外部ネットワーク、および外部 VRF の作成

このセクションでは、REST API を使用してクラウド ルータ、外部ネットワーク、および外部 VRF を作成する方法を示します。

次の POST の例では、4 つのリージョンでクラウド ルータを起動し、各リージョンで外部 VRF を使用して外部ネットワークを追加する方法を示します。

```
<polUni>
    <fvTenant name="infra" status="">
        <fvCtx name="extv1" pcEnfPref="enforced" status=""/>
         <fvCtx name="extv2" pcEnfPref="enforced" status=""/>
          <fvCtx name="extv3" pcEnfPref="enforced" status=""/>

           <cloudtemplateInfraNetwork name="default" vrfName="overlay-1" hostRouterMode="manual"
status="">
            <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.7.0/24" poolname="pool1" />
             <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.8.0/24" poolname="pool2" />
             <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.10.0/24" poolname="pool3" />


            <cloudtemplateHubNetwork name="default" status="" >
                <cloudtemplateHubNetworkName name="foo1" asn="64514" status="">
                    <cloudRegionName provider="gcp" region="us-west4" status="" />
                    <cloudRegionName provider="gcp" region="us-west2" status="" />
                    <cloudRegionName provider="gcp" region="us-east1" status="" />
                      <cloudRegionName provider="gcp" region="us-west1" status=""/>
                </cloudtemplateHubNetworkName>
            </cloudtemplateHubNetwork>

            <cloudtemplateIntNetwork name="default">
                <cloudRegionName provider="gcp" region="us-west1">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
                <cloudRegionName provider="gcp" region="us-west2">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
                <cloudRegionName provider="gcp" region="us-east1">
                    <cloudtemplateVpnRouter name="default" status=""/>
                  </cloudRegionName>
                    <cloudRegionName provider="gcp" region="us-west4">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
            </cloudtemplateIntNetwork>

            <cloudtemplateExtNetwork name="default">
         </cloudtemplateExtNetwork>
               <cloudtemplateExtNetwork name="extnwfoo1" vrfName="extv1" hubNetworkName="foo1"
vpnRouterName="default" status="">
                    <cloudRegionName provider="gcp" region="us-west1" status=""/>
                       <cloudtemplateVpnNetwork name="onprem01" remoteSiteId="1" status="">
                 <cloudtemplateIpSecTunnel peeraddr="128.1.1.1" preSharedKey="abcd" poolname="pool1"
 status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
            </cloudtemplateExtNetwork>
            <cloudtemplateExtNetwork name="extnwfoo2" vrfName="extv2" hubNetworkName="foo1"
vpnRouterName="default" status="">
             <cloudRegionName provider="gcp" region="us-west2" status=""/>
                <cloudtemplateVpnNetwork name="onprem02" remoteSiteId="2" status="">
                       <cloudtemplateIpSecTunnel peeraddr="128.1.1.2" preSharedKey="def"
poolname="pool2" status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
            </cloudtemplateExtNetwork>
             <cloudtemplateExtNetwork name="extnwfoo3" vrfName="extv3" hubNetworkName="foo1"
vpnRouterName="default" status="">
                <cloudRegionName provider="gcp" region="us-east1" status=""/>
                   <cloudtemplateVpnNetwork name="onprem03" remoteSiteId="3" status="">
```

```
                        <cloudtemplateIpSecTunnel peeraddr="128.1.1.3" preSharedKey="abc"
poolname="pool3" status="">
                         <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529" status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
                  </cloudtemplateExtNetwork>
        </cloudtemplateInfraNetwork>
    </fvTenant>
</polUni>
```