初期構成の完了

L3Out 接続の設定

この手順では、L3Out 接続を構成する方法について説明します。

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、ページの上部に「外部ネットワークをサポートするには、クラウド APIC セットアップで外部接続を有効にする必要があります」という警告が表示されます。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、セットアップ ウィザードを使用した Cisco Cloud APIC の設定 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 *1 : [*外部ネットワークの作成（***Create External Network***）*]* ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	外部ネットワーク名を入力します。
VRF	L3Out への接続に使用する VRF を選択するか、この目的で新しい VRF を作成します。 1. **[VRF の選択（Select VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。 [+ VRF の作成（+ Create VRF）] オプションを使用してVRFを作成することもできます。 3. [選択（Select）] をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。
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。 （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、セットアップ ウィザードを使用した Cisco Cloud APIC の設定 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。
設定	
地域	この L3Out 接続が存在するリージョンを選択します。 1. **[地域の追加（Add Region）]** をクリックします。 **[地域の選択（Select Regions）]** ダイアログボックスが表示されます。 • 初回セットアップの一部として選択した地域がここに表示されます。 • 複数の地域を選択して、複数の地域でクラウド ルータを起動できます。 2. **[地域の選択（Select Regions）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。

[プロパティ（Properties）]	説明
VPN ネットワーク	Cisco Cloud APIC によって使用される L3Out 接続は、IPSec VPN トンネル経由です。 VPN ネットワークの L3Out IPSec VPN 情報を追加します。 **1.** **[VPNネットワークの追加（Add VPN Network）]** をタップします。 **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスが表示されます。 **2.** **[名前（Name）]** フィールドに VPN ネットワークの名前を入力します。 **3.** **[+ IPSec ピアの追加（+ Add IPSec Peer）]** をクリックします。 IPSec ピア エントリごとに 2 つのトンネルが作成されます。 **4.** 追加する IPSec ピアの次のフィールドに値を入力します。 • **IPSec トンネル ピアの パブリック IP** • **事前共有キー** • **IKE Version**：IPSec トンネル接続用に **ikev1** または **ikev2** を選択します。 • **BGP ピア ASN** • **Subnet Pool Name**：**[サブネット プール名の選択（Select Subnet Pool Name）]** をクリックします。 **[サブネット プール名の選択（Select Subnet Pool Name）]** ダイアログボックスが表示されます。リストされている使用可能なサブネット プールのいずれかを選択し、**[選択（Select）]** をクリックします。 **5.** この IPSec トンネルを追加するには、チェックマークをクリックします。 別の IPSec トンネルを追加する場合は、**[+ IPSec トンネルの追加（+ Add IPSec Tunnel）]** をクリックします。 **6.** **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスで **[追加（Add）]** をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。

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

ステップ 5 L3Out 接続の設定を確認します。

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、**[Hybrid Connectivity]** > **[VPN]** > **[Cloud VPN Tunnels]** に移動します。

ステップ 6 L3Out 接続に必要な IAM アクセス許可を設定します。

a) Google Cloud GUIで、Cisco Cloud APIC のために作成したプロジェクトに移動します。
プロジェクトの**ダッシュボード**が表示されます。

b) 左側のナビゲーション バーで、**[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) 展開に適したサービス アカウントを見つけます。

[名前（Name）] 列に表示されているエントリ **[Google APIs Service Agent]** でサービス アカウントを探します（これも [メンバー（Member）] で *<project_number>*@cloudservices.gserviceaccount.com でリストされている）をクリックします。

このサービス アカウントは、Cisco Cloud APIC を起動し、クラウド ルータを展開したときに自動的に作成されます。このサービス アカウントが自動的に作成されていない場合は、次の手順に従って手動で作成します。

1. **[IAM]** ウィンドウで **[MEMBERS]** タブが選択されていることを確認します。
2. ウィンドウの上部にある **[追加（ADD）]** をクリックします。
3. **[新規メンバー（New Members）]** フィールドに、このサービス アカウントの名前を入力します。

   <service-acct-name>@*<project-name>*.iam.gserviceaccount.com
4. [保存（SAVE）] をクリックします。

d) 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 ネットワーク管理者
   - コンピューティング セキュリティ管理者
   - 管理者のログイン

- パブ/サブ管理者
- 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。

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使用してテナントを作成する方法について説明します。

Cloud APIC での Google Cloud の展開について （5 ページ） で説明したように、各 Cisco Cloud APIC 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。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 & Admin]** > **[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ー30 文字にする必要があります。
6. **[場所（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. [作成（CREATE）] をクリックします。

Cloud APIC での Google Cloud の展開について

Google Cloud は、ファイル システムに似た方法でリソースを編成します。

- 最上位の組織は複数のフォルダを持つことができます。
- すべてのフォルダには、他のフォルダを含めることも、すべてのプロジェクトに一意の ID があるプロジェクトを含めることもできます。

- クラウド リソース（VM、VPC、サブネットなど）はプロジェクトに含まれます。

組織とフォルダのレベルは、Google Cloud の観点から理解するのに有用な領域ですが、プロジェクトレベルは、Cloud APIC の観点から最も関連性があります。

各 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。

- Cloud APIC テナントは複数の Google Cloud プロジェクトにまたがることはできません
- Google Cloud プロジェクトに複数の Cloud APIC テナントを含めることはできません

Cloud APIC では、Google Cloud は **サービス アカウント**を使用してプロジェクトにアクセスできます。これらのアカウントは、Google Cloud サービスにアクセスする必要があるアプリケーション用です。これらを使用して、Cloud APIC と他のテナントのポリシーを実行および展開し、プッシュすることができます。Google Cloud 内部で実行されるアプリケーションで使用されるサービスアカウントにはクレデンシャルは必要ありませんが、事前に生成された秘密キーを必要とする Google Cloud の外部で実行されるアプリケーションにはクレデンシャルが必要です。サービス アカウントは1つの Google Cloud プロジェクトに存在しますが、他のプロジェクト（Cloud APIC の場合、他のテナント用）のポリシーを管理するためのアクセス権も付与されます。

次の項では、Google Cloud を使用して Cloud APICテナントを設定するさまざまな方法について詳しく説明します。

- 管理対象クレデンシャルを持つユーザ テナント （6 ページ）
- 管理対象外クレデンシャルを持つユーザ テナント （7 ページ）

管理対象クレデンシャルを持つユーザ テナント

このタイプのユーザ テナントには、次の特性があります。

- このテナント アカウントは Cisco Cloud APIC によって管理されます。
- このタイプのユーザ テナントのテナント設定プロセスの一環として、最初に Cisco Cloud APIC GUIで **[管理対象アイデンティティ（Managed Identity）]** を選択します。
- Cisco Cloud APIC で必要なパラメータを設定したら、Google Cloud でこのテナントに必要な権限を設定する必要があります。
  - 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 ネットワーク管理者
  - コンピューティング セキュリティ管理者
  - 管理者のログイン
  - パブ/サブ管理者
  - ストレージ管理者

このようなテナントの作成手順については、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 （13 ページ） を参照してください。

管理対象外クレデンシャルを持つユーザ テナント

このタイプのユーザ テナントには、次の特性があります。

- このテナント アカウントは Cisco Cloud APIC では管理されません。
- このタイプのテナントの Cisco Cloud APIC に必要なパラメータを設定する前に、まず、このテナントに関連付けられたサービス アカウントの Google Cloud から必要な秘密キー情報を含むJSONファイルをダウンロードする必要があります。
- 次に、このタイプのユーザ テナントのテナント設定プロセスの一環として、Cisco Cloud APIC GUI で **[管理対象外アイデンティティ（Unmanaged Identity）]** を選択します。Cisco Cloud APIC でこのタイプのテナントの設定プロセスの一環として、ダウンロードした JSON ファイルから次の情報を提供します。
  - キーID
  - RSA プライベート キー
  - クライアントID
  - E メール

このようなテナントの作成手順については、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 （7 ページ） を参照してください。

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 により管理されない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 （5 ページ） 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。必要に応じてこれらの手順については、テナントの作成 （5 ページ） を参照してください。

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

ステップ 3 左側のナビゲーション バーで、**[IAM & Admin]** をクリックし、**サービス アカウント** 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

[プロパティ（Properties）]	**説明**
名前（Name）	テナント名を入力します。
説明	テナントの説明を入力します。
設定	

[プロパティ（Properties）]	説明
セキュリティドメインの追加	テナントのセキュリティドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]** をクリックして、セキュリティドメインをテナントに追加します。
Google Cloud Project	
Google Cloud Project 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	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。 詳細については、Cloud APIC での Google Cloud の展開について （5 ページ）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。
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、次のように変更して入力します。 • キー文字列の先頭から次のテキストを削除します。 "—--BEGIN PRIVATE KEY------\n • キー文字列の末尾から次のテキストを削除します。 \n—--END PRIVATE KEY------\n"
クライアント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。

[プロパティ（Properties）]	説明
電子メール	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。 アカウントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[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。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。

ステップ 12 設定が終わったら [Save] をクリックします。

管理対象テナントの作成

次のセクションでは、管理対象テナントを作成するために必要な情報を提供します。

- 管理対象テナントの Google Cloud でプロジェクトを作成し、適切な権限とロールを割り当てます。
- Cisco Cloud APIC で管理対象テナントを作成する

管理対象テナント用の Google Cloud でのプロジェクトの作成

ステップ 1 Google Cloud で、この管理対象テナントに関連付けられたサービス アカウントで適切なサービス API を有効にします。

a) Google Cloud GUIで、この Cisco Cloud APIC 管理対象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。
プロジェクトの **ダッシュボード** が表示されます。

b) **ダッシュボード**の上部にある検索バーで、**「API & Services」** を検索し、その検索結果をクリックして**「API & Services」** ウィンドウにアクセスします。

c) **「API & Services」**ウィンドウで、**[+ ENABLE APIS AND SERVICES]** タブをクリックします。

[API ライブラリ（API Library）] ウィンドウが表示されます。

d) **[Search for APIs & Services]**フィールドで、必要なサービスを検索して有効にします。

次のリストの各サービスについて、

1. **[API とサービスの検索（Search for APIs & Services）]** フィールドで API またはサービスを検索します。
2. 検索結果をクリックすると、その API またはサービスのページが表示されます。
3. その API またはサービス ページで **[ENABLE]** ボタンをクリックします。

次に、検索して有効にする必要がある API とサービスを示します。

- コンピューティング エンジン
- Cloud Deployment Manager V2 API
- Cloud Pub / Sub API
- クラウド リソース マネージャ API
- Service Usage API
- Cloud Logging API

各 API またはサービスを有効にするには数分かかります。各APIまたはサービスを有効にした後、**[API とサービス（APIs & Services）]** ウィンドウに戻る必要があります。

上記のすべての API とサービスを有効にすると、次の追加の API とサービスが自動的に有効になります。

- Identity and Access Management（IAM）API
- IAM サービス アカウントの資格情報
- クラウド OS ログイン API
- クラウド DNS API
- レコメンダAPI

自動的に有効になっていない場合は、手動で有効にします。

ステップ 2 Google Cloud のこの管理対象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。
プロジェクトの **ダッシュボード** が表示されます。

b) 左側のナビゲーション バーで、**[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) 適切なサービス アカウントを見つけます。

d) 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 **[エディタ（Editor)]** 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。

   - エディタ（Editor）
   - ロール管理者
   - プロジェクト IAM 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。

ステップ 3 展開手順を実行したときに作成された **servacc-template** フォルダを見つけます。

この Google Cloud でのクラウド APIC の導入 手順では、`capic_deployment_pkg.tar` tar ファイルを展開した後に、**servacc-template** フォルダが作成されました。その **servacc-template** フォルダを見つけます。

ステップ 4 ディレクトリを **servacc-template** フォルダに変更し、必要なファイルがそのフォルダにあることを確認します。

次のファイルが **servacc-template** フォルダにあります。

- **capic_servacc.yaml**：ユーザ テナントロール権限展開スクリプト
- **capic_servacc.py.schema**：スキーマ定義パラメータ
- **capic_servacc.py**：リソース定義テンプレート

ステップ 5 テキスト エディタを使用して、infra テナント サービス アカウントで `capic_servacc.yaml` ファイルを編集します。

a) `capic_servacc.yaml` ファイルの情報を表示します。

`capic_servacc.yaml` ファイルの内容は次のようになります。

```
imports:
```

```
- path: capic_servacc.py
resources:
- name: capic-servacc-res
type: capic_servacc.py
properties:
serviceAccountEmail: capic-servacc@<infra_tenant_project_ID>.iam.gserviceaccount.com
```

b) `[serviceAccountEmail]` フィールドで、デフォルト エントリを Cisco Cloud APIC 展開の一部であるインフラ テナントのサービス アカウントに置き換えます。詳細については、インフラテナント用のプロジェクトの作成Google Cloudを参照してください。

c) `capic_servacc.yaml` ファイルを保存して終了します。

ステップ 6 Google Cloud のテナント プロジェクトで次のコマンドを実行します。

```
gcloud config set project <managed_tenenat_GCP_project_ID>
gcloud deployment-manager deployments create <deployment-name> --config capic_servacc.yaml
gcloud deployment-manager deployments list
```

ここで、

- 最初のコマンドについては、ユーザ テナント プロジェクトの下にいることを確認する必要があります。
- 2 番目のコマンドでは、インフラ テナント サービス アカウントをユーザ テナント サービス アカウントに展開します。
- 3 番目のコマンドで上記の展開を確認しています。

この時点で、Cisco Cloud APIC インフラ サービスアカウントは、管理対象テナントを管理するために必要なすべての権限を持ちます。

次のタスク

Cisco Cloud APIC GUI で管理対象テナントを設定する必要があります。「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 （13 ページ）」に進みます。

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 （5 ページ） 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。必要に応じてこれらの手順については、テナントの作成 （5 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 *3:* テナント ダイアログボックス フィールドの作成

[プロパティ（Properties）]	**説明**
名前（Name）	テナント名を入力します。
説明	テナントの説明を入力します。
設定	
セキュリティ ドメインの追加	テナントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。
Google Cloud Project	
Google Cloud Project 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	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。 詳細については、Cloud APIC での Google Cloud の展開について （5 ページ）を参照してください。

[プロパティ（Properties）]	説明
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。 アカウントのセキュリティ ドメインを追加するには、次の手順を実行します。 **1.** **[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。 **2.** セキュリティ ドメインをクリックして選択します。 **3.** **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。

ステップ 5 設定が終わったら [Save] をクリックします。

次のタスク

管理対象テナントの設定プロセスが完了しました。

何らかの理由で管理対象テナントを将来削除する場合は、次の指示に従って管理対象テナントを削除します。

1. Cisco Cloud APIC からテナント設定を削除します。
   1. 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。

      設定されたテナントが一覧表示されます。
   2. 削除するテナントの横にあるボックスをクリックし、**[アクション（Actions）]** >**[テナントの削除（Delete Tenant）]** をクリックします。
2. 管理対象テナントからインフラ サービス アカウントを削除するには、この Cisco Cloud APIC 管理対象テナントに関連付けられている Google Cloud プロジェクトで次のコマンドを入力します。

   ```
   gcloud deployment-manager deployments delete <deployment-name>
   ```

   次のコマンドを使用して、現在のユーザテナントプロジェクトを確認し、目的のプロジェクトでない場合はそのプロジェクトを設定する必要があることに注意してください。

   ```
   gcloud config set project <project-id>
   ```