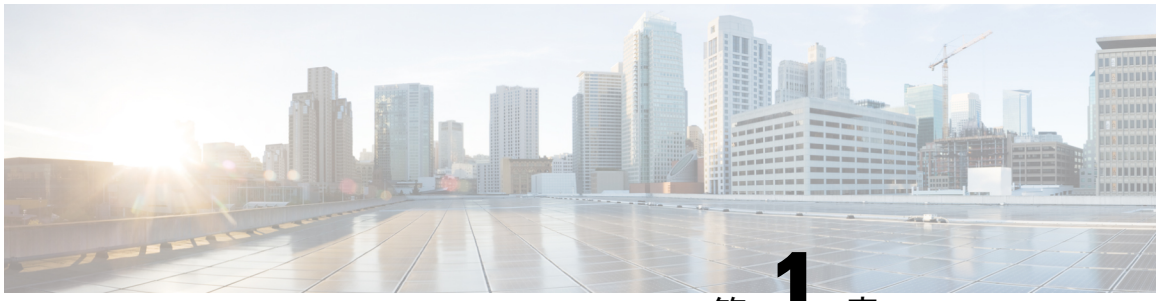
Cisco Cloud APIC for Google Cloud インストール ガイド、リリース 25.0(x)

初版：2021 年 9 月 20 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

Cisco Cloud APIC for Google Cloud インストール ガイド、リリース *25.0(x)* の入手

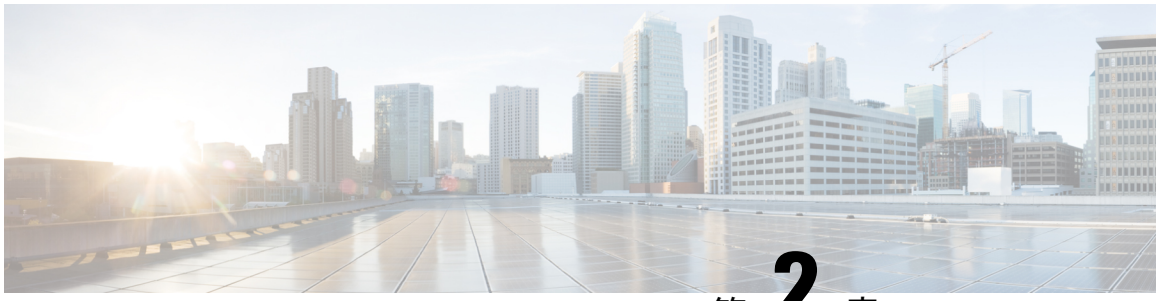
次の表は、現行リリースに至るまでにガイドの編成と特徴に加えられた主な変更点の概要を示しています。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco APIC for Cisco APIC Release 25.0(1)* の新機能と変更された動作

機能または変更	説明	参照先
Cisco Cloud APIC のリリース番号の変更	リリース 25.0(1) 以降では、Cisco Cloud APIC のリリース番号が変更されています。Cisco Cloud APIC のリリース順序は次のとおりです。 • 4.1(x)（AWS のみのサポート） • 4.2(x) • 5.0(x) • 5.1(x) • 5.2(x) • 25.0(x)（このリリース）	

新機能および変更された機能に関する情報

機能または変更	説明	参照先
Google Cloud の Cisco Cloud APIC によるサポート	リリース25.0(1) 以降、Cisco Cloud APIC で Google Cloud のサポートが利用可能になりました。	



第 2 章

概要

ポリシーの用語

Cisco Cloud APIC の主要な機能は、パブリック クラウドのネイティブ コンストラクトへの Cisco Application Centric Infrastructure（ACI）ポリシーの変換です。

次の表に、Google Cloud で Cisco ACI ポリシー用語との同等の用語を示します。

Cisco ACI	Google Cloud
テナント	プロジェクト（Project）
Virtual Routing and Forwarding（VRF）	VPC（仮想プライベート クラウド）
BD サブネット	サブネット
契約、フィルタ	ファイアウォールルール
EP から EPG へのマッピング	ルーティングおよびファイアウォール ルール
エンドポイント	VM インスタンスのネットワーク アダプタ

Cisco Cloud APIC ライセンシング

ここでは、使用するライセンシング要件Cisco Cloud Application Policy Infrastructure Controller（APIC）を示します。

Cisco Cloud APIC

シスコは、管理する各仮想マシン（VM）インスタンスごとにライセンス Cisco Cloud APIC を付与します。Cisco Cloud APICバイナリ イメージは Google Cloud ポータルで利用可能で、Bring Your Own License（BYOL）モデルをサポートしています。

Essentials Cloud 階層には、パブリック クラウド上の単一のポリシー ドメイン用または単一の Cisco Cloud APIC インスタンス用のライセンスが含まれています。の複数のインスタンスを展開する場合は、管理するVMインスタンスごとにAdvantage Cloudライセンスを購入します。Cisco Cloud APICCisco Cloud APIC

ライセンスの詳細は、『*Cisco Application Centric Infrastructure Ordering Guide*』を参照してください。

1 つ以上の Cisco Cloud APIC ライセンスを取得することに加えて、Cisco Smart Software Licensing に Cisco Cloud APIC を登録する必要があります。

シスコのスマート ライセンスは、複数のシスコ製品間でソフトウェア ライセンスを管理する統合ライセンス管理システムです。スマートソフトウェアライセンシングの詳細については、https：//www.cisco.com/go/smartlicensingを参照してください。

Cisco Cloud APIC を登録するためのステップは以下のとおりです。

1. 製品がインターネットにアクセスできること、またはネットワーク上にインストールされた Smart Software Manager サテライトにアクセスできることを確認してください。
2. スマートアカウントにログインします。
    1. Smart Software Manager : https://software.cisco.com/
    2. Smart Software Manager サテライト: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html
3. この製品インスタンスで使用するライセンスが含まれている仮想アカウントに移動します。
4. 製品インスタンス登録トークン(スマートアカウントを識別)の生成と、そのトークンのコピーまたは保存。

Cisco Cloud APIC 関連のマニュアル

さまざまなリソースから Cisco Cloud APIC と Google Cloud の情報を入手できます。

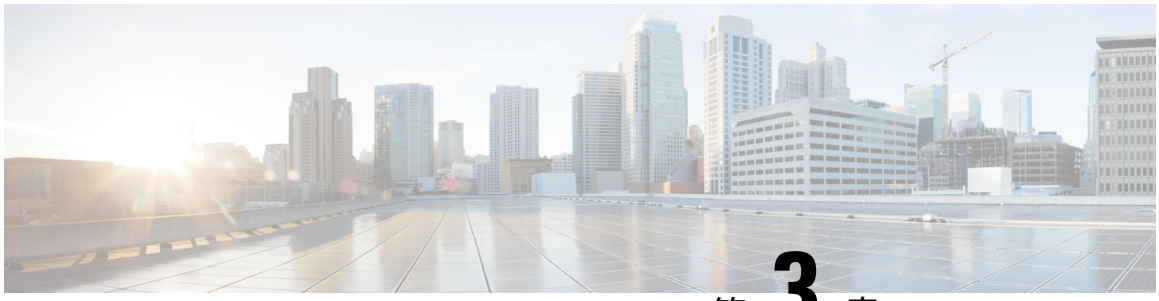
Cisco Cloud APICのマニュアル

Cisco.com で Cisco Cloud APIC のマニュアルを見つけることができます。

Cisco Cloud APIC ドキュメンテーション ライブラリ

Google Cloudのマニュアル

Google Cloud Web サイトで、ユーザ ガイド、FAQ、ケース スタディ、ホワイト ペーパーなどのドキュメントを検索できます。



第 3 章

Cisco Cloud APIC のインストールの準備

Google Cloud の導入要件

ここでは、Google Cloud での展開の要件を示します。

Cisco Cloud APIC リソース

展開中に次の Cisco Cloud APIC が作成されます。

- コンピューティング インスタンス
  - インスタンス タイプ：n2-standard-16
  - CPU：16 vCPU
  - メモリ：64 GB
  - ディスク：OS disk [300GB]、Data Disk – 100GB [empty]
- データ ディスク：
  - 空のデータ ディスク
  - サイズ：100GB
  - タイプ：標準 SSD
- VPCネットワーク：autoCreateSubnetworks が False に設定されている場合
- サブネット：Cisco Cloud APIC 管理 NIC がこのサブネットに接続されています。
- Google Cloud プロジェクト：2 つ以上の Google Cloud プロジェクト：
  - ACI インフラ用に 1 つ

- テナントごとに 1 つ

Cloud APIC 通信ポート

Cloud APIC 環境を設定する際は、下記のポートがネットワーク通信に必要であることに注意してください。

- Cloud APIC には、セットアップ ウィザードを使用した Cisco Cloud APIC の設定 （17 ページ） の開始時に Cloud APIC にログインするために使用するものと同じ Cloud APIC 管理IP アドレスを使用します。
- Google Cloud ファイアウォール ルールの場合：
  - WEB-Server：Ingress は 80、443 を許可します
  - SSH-Allow：Ingress は 22 を許可
- ライセンス登録の場合（`tools.cisco.com` へ）：ポート 443（アウトバウンド）が必要です。
- DNS の場合：UDP ポート 53 アウトバウンド
- NTP の場合：UDP ポート 123 アウトバウンド
- リモート認証（LDAP、Radius、TACACS+、SAML）を使用する場合は、適切なポートを開きます。
- 認証局を使用する場合は、適切なポートを開きます。

Cisco Cloud APIC のインストール ワークフロー

このセクションでは、Cisco Cloud APIC をインストールして展開するために必要なタスクの概要について説明します。インストール タスクは、Google Cloud 管理ポータルと Cloud APIC の初回セットアップ ウィザードを使用して実行します。

1. Google Cloud のサポートを Cisco Cloud APIC で準備するためのすべての前提条件を満たします。

   「Cisco Cloud APIC のインストールの準備 （7 ページ）」を参照してください。

2. Cisco Cloud APIC を Google Cloudで展開

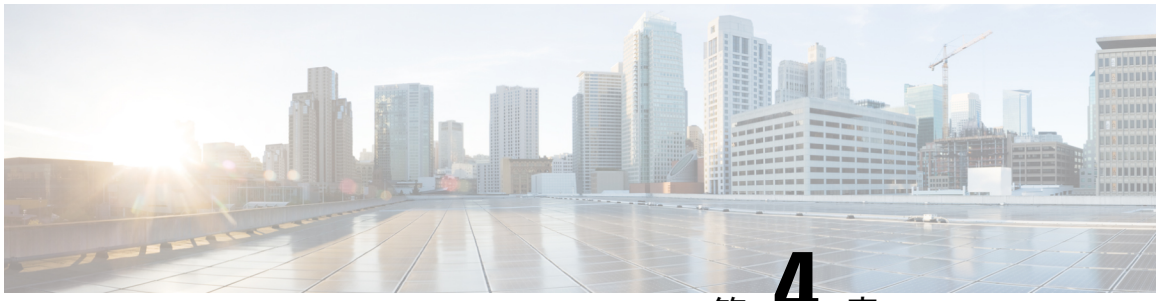
   セクション「Google Cloud でのクラウド APIC の展開 （11 ページ）」を参照してください。

3. 初回セットアップ ウィザードを使用して Cisco Cloud APIC を設定します。

セクション「セットアップ ウィザードを使用した Cisco Cloud APIC の設定 （17 ページ）」を参照してください。

4. Cisco Cloud APIC を通じて必要な設定変更を行います。

「Cisco Cloud APIC GUI の操作 （39 ページ）」および「Cisco Cloud APIC コンポーネントの設定 （40 ページ）」の項を参照してください。



第 4 章

Google Cloud でのクラウド APIC の展開

インフラテナント用のプロジェクトの作成Google Cloud

この手順では、Google Cloud でプロジェクトを作成し、プロジェクトで適切な API とサービスを有効にし、サービス アカウントに適切な権限を割り当てる方法について説明します。

これらの手順で作成されるテナントは、インフラ テナントと呼ばれます。

ステップ 1 Google Cloud アカウントにログインします。

ステップ 2 Cisco Cloud APIC に使用するプロジェクトを作成します。

これらの手順については、Google Cloud ドキュメントの「プロジェクトの作成と管理」を参照してください。

ステップ 3 プロジェクトで適切な API とサービスを有効にします。

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) **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 4 サービス アカウントに適切な権限を割り当てます。

サービス アカウントには次の 2 種類があります。

- **プロジェクトのサービス アカウント**：Cisco Cloud APIC のサービス アカウントを展開できます。
- **ユーザのサービス アカウント**：このサービス アカウントは API と通信します。このサービス アカウントは、ユーザ ログインまたはパスワードを使用する代わりに、プロジェクトに代わって機能し、リソースを作成します。

この手順では、プロジェクトのサービス アカウントに適切な権限を割り当てます。

a) Google Cloud GUIで、Cisco Cloud APIC プロジェクトの **[ダッシュボード（Dashboard）]** ウィンドウに戻ります。
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、前の手順で API を有効にしたときに自動的に作成されているはずです。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。

   `<project_number>@cloudservices.gserviceaccount.com`
4. [保存（SAVE）] をクリックします。

d) このサービス アカウントの権限が正しく設定されていることを確認します。

このサービス アカウントの [ロール（Role）] 列に **[所有者（Owner）]** が表示されます。

このサービス アカウントの [ロール（Role）] 列に **[所有者（Owner）]** が表示されない場合は、次の手順に従ってください。

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 **[所有者（Owner)]** を選択して、**[保存（Save）]** を選びます。

   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。

ステップ 5 プロジェクトがイメージにアクセスできることを確認します。

プロジェクトがイメージにアクセスできない場合は、Cisco TME にお問い合わせください。

Google Cloud でのクラウド APIC の導入

ステップ 1 展開用パッケージにアクセスします。

イメージが Google Cloud マーケットプレイスで入手可能になるまで、展開パッケージにアクセスするには、Cisco TME チームに連絡してください。

ステップ 2 次のコマンドを入力します。

```
# gsutil cp gs://cisco-capic-deployment-artifacts/capic_deployment_pkg.tar .
```

ステップ 3 次のコマンドを入力して、tar ファイルを展開します。

```
# tar -xvf capic_deployment_pkg.tar .
```

tar ファイルを展開すると、次のファイルが使用可能になります。

- **capic.yaml**：メイン導入テンプレート（パラメータ、リソース テンプレート、出力）

- **capic.py.schema**：スキーマ定義パラメータ
- capic.py：リソース定義テンプレート
- **capic_undeploy.sh**：すべてのリソースをクリーンアップするための展開解除スクリプト

これらのファイルは、インフラ テナントの展開に使用されます。

また、**vm-deployment** フォルダと **servacc-template** フォルダがこれらのファイルとともに表示されます。

ステップ 4 公開 SSH キーと秘密 SSH キーを生成します。

```
# ssh-keygen -t rsa -f ~/.ssh/gcp_capic_key -C admin
```

公開 SSH キーは次のとおりです。

```
# ~/.ssh/gcp_capic_key.pub
```

ステップ 5 テキスト エディタを使用して、`capic.yaml` ファイルを編集します。

- パラメータ領域を更新します。
  - **image**：Google Cloud のイメージへのパスを入力します。
  - **sshPubKey**：公開 ssh キー情報を次の形式で入力します。

    ```
    ssh-rsa <ssh-public-string> admin
    ```

- region/zone/CIDR およびその他の設定可能なパラメータも更新できます。

次のパラメータを変更しないでください。

- **machineType**: n2-standard-16
- **username**: admin

次に、`capic.yaml` ファイルの例を示します。太字の項目は、更新または変更する領域です。

```
imports:
  - path: capic.py

resources:
  - name: capic-res
    type: capic.py
    properties:
      region: us-central1
      infraVpcPool: 10.10.0.0/24
      zone: us-central1-a
      image:
https://www.googleapis.com/compute/v1/projects/gcp-ciscoacicapicgc-nprd-62814/global/images/aci-capic-2500-59-202108250542
      machineType: n2-standard-16
      extNw: 0.0.0.0/0
      password: abcd1234
      username: admin
      sshPubKey: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDleZsmW+ES/BtMFTU3qsg7VITjCq3S0qK6Ip7Z1j/CUUAwciekYhdQERLkvuHpAjXOJokcx1SGsGjctNbIsKnNLsfm1BP75eMp/XaqmV+q1fRfR+uojiBL6Twv
HW2ZRv5c4Myfsq1U9gXGEw3Narga4sf7lwR0U/xxxxxxxxxx7Ez/gA02yqBwLHa0H+74Pn1Q8vrkwn1dK0MWYtBg5aHpGIH8qUpNotPnMP6kxfaHIGUYZj4ARef1pk69w2dN/0QWrYWhyZhqjXdy2eIDkpH798rOqFe6g8hwWypagG
J6Md0sJcBNIZdyWbOrpbsI2MB+MFC69MNiQ43jivM6XdLIXvXYcIN8eTczTevKkWE7Cl5BL0nB9uy4pAX0EWRU1MtQ5nP794aWZtQZzdLjRn1Xi+OVC8SVHdkvpgi10umgeSOX4B+1jk3fYrK1hIRBYU/bEaqw/7+sERDq97IrH
5aAQ8e/lHW1JFo+xxxxxxxxxx= admin
```

```
outputs:
   - name: capic-management-ip
     value: $(ref.capic-vm.networkInterfaces[0].accessConfigs[0].natIP)
```

ステップ 6 編集した `capic.yaml` ファイルを保存して終了します。

ステップ 7 現在のGoogle Cloud プロジェクト情報を表示して、正しいプロジェクトで実行されていることを確認します。

```
# gcloud config list
```

ステップ 8 Cisco Cloud APIC を展開する前に、インフラ アカウントを展開するプロジェクトを設定します。

```
gcloud config set project <infra_tenenat_GCP_project_ID>
```

ステップ 9 次のコマンドを入力して、既存の展開があるかどうかを確認します。

```
# gcloud deployment-manager deployments list
```

（注） 削除する導入がリストされている場合は、ステップ 12 （15 ページ） の説明に従って必要なコマンドを入力し、ここに戻ります。

ステップ 10 Deployment Manager を使用して Cisco Cloud APIC ソリューションを展開します。

```
# gcloud deployment-manager deployments create <deployment-name> --config capic.yaml
...
 Create operation operation-1630191668544--5b89697e completed successfully.
 NAME                                TYPE                                STATE      ERRORS
 bind-iam-policy-capic-custom-role   iamMemberBinding                    COMPLETED  []
 capic-custom-role                   gcp-types/iam-v1:projects.roles COMPLETED  []
 capic-natip                         compute.v1.address                  COMPLETED  []
 capic-servacc                       iam.v1.serviceAccount               COMPLETED  []
 capic-vm                            compute.v1.instance                 COMPLETED  []
 firewall-ingress                    compute.v1.firewall                 COMPLETED  []
 overlay-1                           compute.v1.network                  COMPLETED  []
 overlay-1-subnet10-10-0-0x25        compute.v1.subnetwork               COMPLETED  []
 OUTPUTS              VALUE
 capic-management-ip  12.123.12.12
```

Deployment Manager からの出力の最後に表示される管理 IP アドレスを書き留めておいてください。この管理 IP アドレスを使用して Cisco Cloud APIC にログインします。

ステップ 11 次のコマンドを入力して、Cisco Cloud APIC 展開を一覧表示します。

```
# gcloud deployment-manager deployments list
```

ステップ 12 何らかの理由で Cisco Cloud APIC 展開を削除する場合は、次のコマンドを入力します。

```
# ./capic_undeploy.sh <project_ID> <region> <zone> <deployment_name>
```

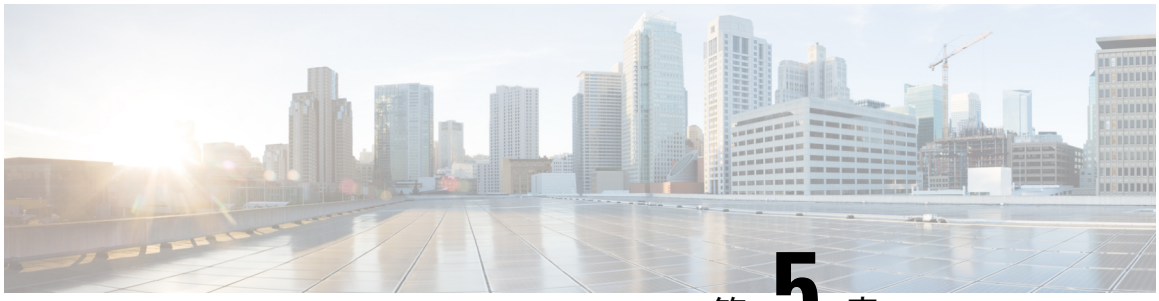
これにより、Cisco Cloud APIC 展開が削除され、Cisco Cloud APIC によって作成された内部リソースがクリーンアップされます。

この時点で、Cisco Cloud APIC カスタム IAM ロールは削除モードになっています。将来の展開に関する問題を回避するには、次のコマンドを入力して Cisco Cloud APIC カスタム IAM ロールの状態をクリーンアップします。

```
# gcloud iam roles undelete capic_custom_role --project=<project_ID>
```

次のタスク

これらの手順で作成したインフラ サービス アカウントは、インフラ プロジェクトとユーザ テナント プロジェクト間の通信を確立するために、各ユーザ テナント プロジェクト（管理対象テナント）に使用されます。次に、セットアップ ウィザードを使用した Cisco Cloud APIC の設定（17ページ）に進み、Cisco Cloud APIC のクラウドインフラストラクチャ設定をセットアップします。クラウドインフラストラクチャ設定では、Cisco Cloud APIC が必要な Google Cloud 構成を展開します。



第 5 章

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

Cloud APIC のクラウドインフラストラクチャ設定をセットアップするには、このトピックの手順に従います。Cloud APICは、必要な Google Cloud 構成を自動的に展開します。

始める前に

このタスクの前提条件は次のとおりです。

- 少なくとも 2 つの Google Cloud プロジェクトがあります。1 つは ACI インフラ用で、もう 1 つはテナントごとです。
- Google Cloud でのクラウド APIC の展開 （11 ページ） に記載されている手順を正常に完了しました。

ステップ 1 Cloud APIC の IP アドレスを検索します。

Google Cloud でのクラウド APIC の導入 （13 ページ） の Deployment Manager からの出力の最後に表示される管理 IP アドレス。

ステップ 2 ブラウザ ウィンドウを開き、セキュア バージョンの HTTP (`https://`) を使用して、URL フィールドに IP アドレスを貼り付け、Return を押してこの Cloud APIC にアクセスします。

たとえば、`https://192.168.0.0` と入力します。

[リスクを無視して証明書を受け入れる（Ignore Risk and Accept Certificate）] というメッセージが表示された場合は、証明書を受け入れて続行します。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

ステップ 3 Cloud APIC のログイン ページに次の情報を入力します。

- **ユーザ名**：このフィールドに **admin** と入力します。
- **パスワード**： Cloud APICにログインするために指定したパスワードを入力します。
- **ドメイン**：**[ドメイン（Domain）]**フィールドが表示された場合は、デフォルトの[ドメイン（Domain）]エントリをそのままにします。

ステップ 4 ページの下部にある **[ログイン]** をクリックします。

（注） ログインしようとしたときに、REST エンドポイントのユーザ認証データストアが初期化されていないなどのエラーメッセージが表示された場合は、このファブリック ノードのファブリック メンバーシップ ステータスを確認し、数分待ってから数分後に再試行してください。また、ログインするためにページを更新する必要があります。

[Cloud APIC へようこそ] セットアップ ウィザードのページが表示されます。

ステップ 5 **[セットアップの開始（Begin Set Up）]** をクリックします。

[基本設定（Let's Configure the Basics）] ページが表示され、次の領域が設定されます。

- **DNS サーバと NTP サーバ**
- **リージョン管理**
- **スマート ライセンス**

ステップ 6 **[DNS と NTP サーバ（DNS and NTP Servers）]** 行で、**[構成の編集（Edit Configuration）]** をクリックします。

[DNS と NTP サーバ（DNS and NTP Servers）] ページが表示されます。

ステップ 7 **[DNS と NTP サーバ（DNS and NTP Servers）]** ページで、必要に応じて DNS サーバと NTP サーバを追加します。

- DNS サーバはデフォルトですでに設定されています。特定の DNS サーバを使用する場合は、DNS サーバを追加します。
- NTP サーバはデフォルトでは設定されないため、NTP サーバを設定することを推奨します。NTP サーバを設定し、DNS サーバを設定しない場合は、7.d （18 ページ） に進みます。

a) 特定の DNS サーバを使用する場合は、**[DNS サーバ（DNS Servers）]** 領域で **[+ DNS プロバイダの追加（+ Add DNS Provider）]** をクリックします。
b) DNS サーバの IP アドレスを入力し、必要に応じて [優先 DNS プロバイダー（Preferred DNS Provider）] の横にあるボックスをオンにします。
c) DNS サーバの横にあるチェックマークをクリックし、追加する追加の DNS サーバについて繰り返します。
d) **[NTP サーバ（NTP Servers）]** 領域で、**[+ プロバイダの追加（+ Add Provider）]** をクリックします。
e) NTPサーバのIPアドレスを入力し、必要に応じて[優先NTPプロバイダー（Preferred NTP Provider）]の横にあるボックスをオンにします。

f) NTP サーバの横にあるチェックマークをクリックし、追加する NTP サーバを繰り返します。

ステップ 8 DNS サーバと NTP サーバの追加が完了したら、**[保存して続行（Save and Continue）]** をクリックします。

[Let's Configure the Basics] ページが再び表示されます。

ステップ 9 **[リージョン管理（Region Management）]** 行で、**[開始（Begin）]** をクリックします。

[地域管理（Region Management）] ページが表示されます。

ステップ 10 外部接続を設定するかどうかを決定します。

[有効（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 11 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。

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（すべてのリージョンが選択され、選択解除できません）、リージョン間接続が存在します。

ステップ 12 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 13 **[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。

次の制約事項に注意してください。

- Google Cloud でハブ 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 で 1 つのクラウド ルータのみが作成されます。

a) **[ハブ ネットワーク（Hub Network）]** 領域で、**[ハブ ネットワークの追加（Add Hub Network）]** をクリックします。

[ハブ ネットワークの追加（Add Hub Network）] ウィンドウが表示されます。

b) **[名前（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 は秘密 ASN である必要があります。各ハブネット ワークに 64512ー65534 または 4200000000ー4294967294 の値を入力します。

d) リージョンを追加するには、**[+ リージョンの追加（+ Add Region）]** をクリックします。

最大 4 つのリージョンを追加できます。

e) **[+ リージョンの追加（+ Add Region）]** ウィンドウに情報を入力したら、**[完了（Done）]** をクリックします。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

[一般接続（General Connectivity）] ページに戻ります。

f) デフォルトのエントリが **[VPN ルーター（VPN Router）]** フィールドに表示されます。

g) **[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。

ステップ 14 **[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 ツールの追加（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、デフォルトのサブネット プールを削除し、追加のサブネット 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 プールを入力したら、チェックマークをクリックします。

ステップ 15 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、L3Out 接続の設定 （23 ページ） にアクセスしてください。
- 外部ネットワークを作成しない場合は、**[ダッシュボードに移動（Go to Dashboard）]** をクリックします。

メインの **[ダッシュボード（Dashboard）]** ウィンドウに戻ります。

ステップ 16 **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 17 **[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 18 **[スマート ライセンシング]** 行で、**[登録]**をクリックします。

[スマート ライセンシング] ページが表示されます。

ステップ 19 **[スマート ライセンシング]** ページに必要な情報を入力します。

Cisco Smart Licensing は、複数のシスコ製品間でソフトウェア ライセンスを管理する統合ライセンス管理システムです。お使いの Cloud APIC を Cisco Smart Licensing に登録するには、以下のようにします。

- 製品がインターネットにアクセスできること、またはネットワーク上にインストールされた Smart Software Manager サテライトにアクセスできることを確認してください。
- スマート アカウントにログインします。
  - Smart Software Manager: https://software.cisco.com/
  - Smart Software Manager サテライト: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html
- この製品インスタンスで使用するライセンスが含まれている仮想アカウントに移動します。
- 製品インスタンス登録トークン(スマートアカウントを識別)の生成と、そのトークンのコピーまたは保存。

スマート ソフトウェア ライセンシングの詳細については、https://www.cisco.com/go/smartlicensing を参照してください。

ステップ 20 このページに必要なライセンス情報を入力した場合は、ページの下部にある **[登録（Register）]** をクリックします。評価モードで続行する場合は、**[評価モードで続行（Continue in Evaluation Mode）]** をクリックします。

[概要（Summary）] ページが表示されます。

ステップ 21 **[サマリ（Summary）]** ページで情報を確認し、**[完了（Finish）]** をクリックします。

この時点で、Cloud APIC の内部ネットワーク接続の設定は完了です。

Cloud APIC を初めて展開する場合は、このプロセスが正常に完了するまでにかなりの時間（30 分程度）がかかることがあります。

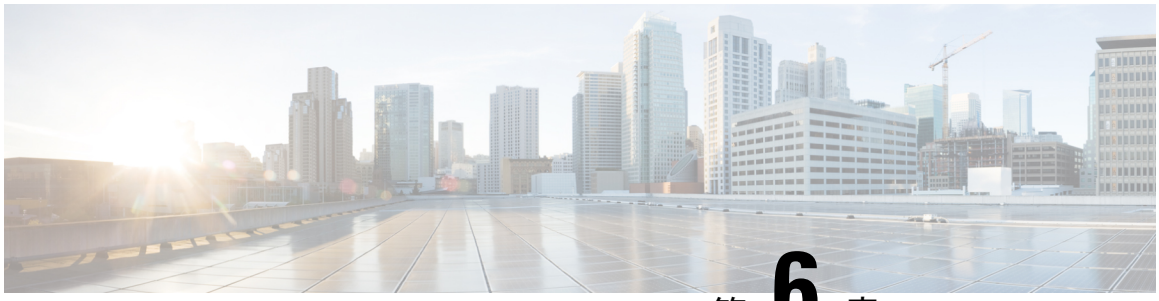
Cisco Cloud APIC セットアップ ウィザードの設定の確認

このトピックの手順を使用して、 Cloud APIC セットアップ ウィザードに入力した設定情報が正しく適用されていることを確認します。

Cisco Cloud APIC で、次の設定を確認します。

- **[クラウドリソース（Cloud Resources）]** で、**[リージョン（Regions）]** をクリックし、**[管理状態（Admin State）]** カラムにすべてのリージョンが管理対象として表示されていることを確認します。
- **[インフラストラクチャ（Infrastructure）]** で、**[外部接続（External Connectivity）]** をクリックし、この画面の情報が正しいことを確認します。

- **[ダッシュボード（Dashboard）]** をクリックし、外部接続ステータスを使用して、セットアップ ウィザードとトンネルの設定が正しく行われたことを確認します。



第 6 章

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 （17 ページ） 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 *2 : [*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 （17 ページ） 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 （27 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 （28 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 （29 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 （35 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 （29 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 （27 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 （27 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 *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	

[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 （27 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 （13 ページ） 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 （11 ページ）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 （35 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 （27 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 （27 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 *4:* 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 （27 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。

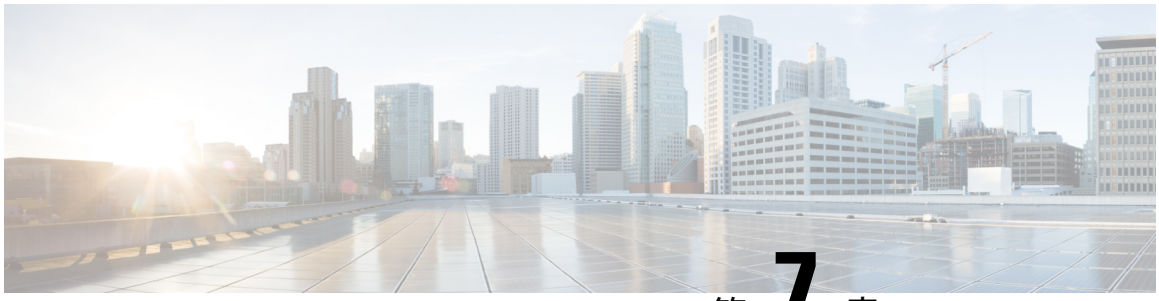
1. Cisco Cloud APIC からテナント設定を削除します。
   1. Cisco Cloud APIC GUI で **[アプリケーション管理（Application Management）]** > **[テナント（Tenants）]** に移動します。

      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>
   ```



第 7 章

Cisco Cloud APIC GUI について

Cisco Cloud APIC GUI の操作

Cisco Cloud APIC をインストール後、Cisco Application Centric Infrastructure（ACI）ポリシーを Google Cloud に拡張するために使用できます。これは Cisco Cloud APIC GUI を使用して行います。

Cisco Cloud APIC GUI では、テナントを作成し、アプリケーション プロファイル、エンドポイント グループ（EPG）、コントラクト、フィルタ、および VRF を設定できます。Cisco Cloud APIC トポロジ、設定、およびリソースを表示することもできます。

を使用して設定手順を実行します。**インテント**機能。**インテント**機能の使用方法については、Cisco Cloud APIC コンポーネントの設定 （40 ページ） を参照してください。『*Cisco Cloud APIC User Guide*』の「Understanding the Cisco Cloud APIC GUIアイコン」の項も参照してください。

Cisco Cloud APICの基本的なタスクを実行する手順は、通常のCisco APIC の手順とは異なります。ただし、テナントの機能、アプリケーションプロファイル、および Cisco APIC のその他の要素は同じです。詳細については、Cisco.com の『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

左側のナビゲーションペインで設定やその他の情報を表示します。**[Dashboard]**（デフォルトビュー）、**[Topology]**、**[Application Management]**、**[Cloud Resources]**、**[Operations]**、**[Infrastructure]**、および **[Administrative]** を選択できます。

アイコンの詳細については、Cisco.comの『*Cisco Cisco Cloud APIC User Guide*』の「Understanding the Cisco Cloud APICGUIアイコン」の項を参照してください。

Cisco Cloud APIC GUIを使用したテナントの作成

次の項では、Cisco Cloud APIC GUI 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。

Cisco Cloud APIC コンポーネントの設定

このセクションでは、テナント、アプリケーションプロファイル、およびエンドポイントグループ（EPG）の作成を含む、Cisco Cloud APIC で主要なタスクの実行の概要について説明します。

始める前に

Cisco Cloud APIC がインストールされている必要があります。このガイドの前のインストールの項を参照してください。

ステップ 1 Cisco Cloud APIC にログインします。

ステップ 2 **[ダッシュボード（Dashboard）]**ペインの右上で、ブルズアイを指す矢印の付いたアイコンをクリックします。

このアイコンは、**インテント** アイコンまたは機能と呼ばれることがあります。

ステップ 3 **[何をしますか]** ウィンドウに用語を入力して、オプションのリストを表示します。

たとえば、テナントを設定する場合は、検索ウィンドウにtenantと入力します。検索は、テナントの作成と設定に関連するタスクのリストを返します。

ステップ 4 タスクをクリックし、開いたウィンドウで設定手順を実行します。

次のタスク

左側のナビゲーションペインで設定を確認できます。[ダッシュボード（Dashboard）]ペインの左上にあるハンバーガーアイコンをクリックして、ペインを展開します。該当する見出しを展開して設定を表示します。

たとえば、テナントを設定した場合は、[アプリケーション管理（Application Management）]を展開し、[テナント（Tenants）]をクリックします。中央の作業ウィンドウにテナントに関する情報が表示されます。

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