Cisco Cloud Network Controller for Google Cloud インストール ガイド、リリース 25.0(5)

初版：2022 年 8 月 15 日

最終更新：2023 年 2 月 17 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/

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

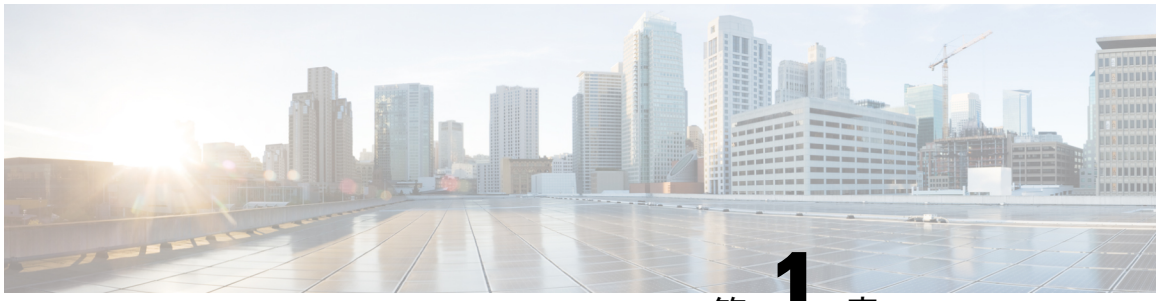
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Trademarks

目 次



第 1 章

新機能と変更情報

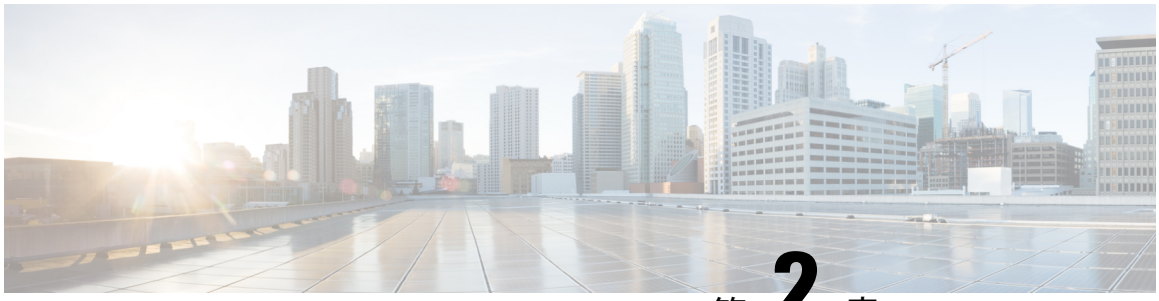
新機能と変更情報

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 Cloud Network Controller* リリース *25.0(5)* の新機能と変更された動作

機能または変更	説明	参照先
製品名の変更	リリース 25.0(5) 以降、Cisco Cloud APIC は Cisco Cloud Network Controller に名前が変更されました。	
サイト間接続のための BGP-EVPN 接続の構成のサポート	リリース 25.0(5) 以降、サイト間のユースケースでは、Google Cloud サイトと他のクラウド サイトまたは ACI オンプレミス サイトとの間のサイト間接続のための BGP-EVPN 接続の構成がサポートされています。 BGP-EVPN 接続には Cisco Catalyst 8000V が使用されます。	

新機能と変更情報



第 2 章

概要

ポリシーの用語

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

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 Network Controller のライセンシング

ここでは、Cisco Cloud Application Policy Infrastructure Controller（Cisco Cloud Network Controller）を使用するためのライセンス要件をリストします。

Cisco Cloud Network Controller

シスコは、管理する仮想マシン（VM）インスタンスごとに Cisco Cloud Network Controller をライセンスしています。Cisco Cloud Network Controller のバイナリ 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 Network Controller インスタンス用のライセンスが含まれています。Cisco Cloud Network Controller の複数のインスタンスを展開する場合は、Cisco Cloud Network Controller が管理する VM インスタンスごとに Advantage Cloud ライセンスを購入します。

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 Network Controller ライセンスを取得することに加えて、Cisco Smart Software Licensing に Cisco Cloud Network Controller 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 Network Controller を登録するには、次の手順を実行します。

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. 製品インスタンスの登録トークン（これによりスマートアカウントを識別）を生成し、そのトークンをコピーするか、または保存します。

Cisco Catalyst 8000V

Cisco Catalyst 8000V は、サブスクリプション ベースのライセンスをサポートしています。

- ティアベースの Cisco Catalyst 8000V ライセンスの 1 つにサブスクライブする手順については、Cisco Catalyst 8000V Edge ソフトウェアを参照してください。
- 層に基づくさまざまなスループットの詳細については、Google Cloud での Cisco Cloud Network Controller の展開に使用されるリソース （7 ページ） を参照してください。

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

Cisco Cloud Network Controller - 関連ドキュメント

Cisco Cloud Network Controller および Google Cloud の情報は、さまざまなリソースから見つけることができます。

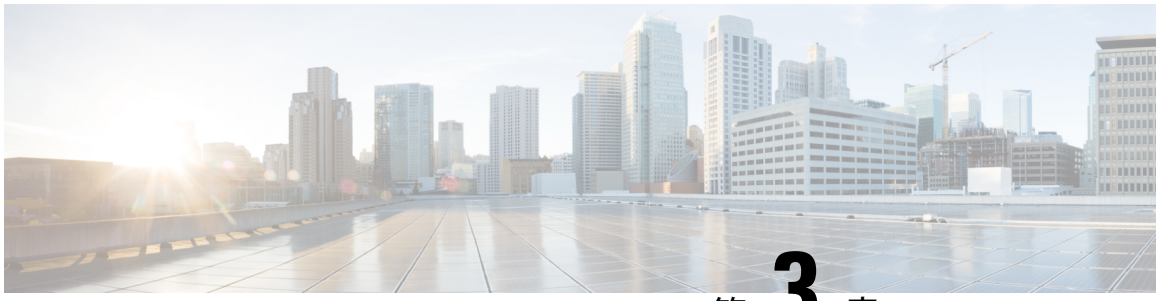
Cisco Cloud Network Controller の関連ドキュメント

Cisco Cloud Network Controller のドキュメントは Cisco.com で見つけることができます。

Cisco Cloud Network Controller ドキュメント 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 Network Controller のインストールの準備

Google Cloud での Cisco Cloud Network Controller の展開に使用されるリソース

ここでは、Google Cloud での Cisco Cloud Network Controller の展開の要件を示します。

Cisco Cloud Network Controller のリソース

Cisco Cloud Network Controller を Google Cloud に展開すると、Cisco Cloud Network Controller は次のインスタンス プロファイルを使用し、必要なリソースを作成します。

- 1 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 Network Controller の管理 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

（注） インフラ アカウントで実行できる Cloud Network Controller は 1 つだけです。同じインフラ アカウントで複数の Cloud Network Controller を実行することはサポートされていません。

Cisco Catalyst 8000V

Cisco Cloud Network Controller のセットアップ時に定義した帯域幅要件に応じて、適切なサイズで Cisco Catalyst 8000V を展開します。

ルータのスループットの値によって、展開する Cisco Catalyst 8000V インスタンスのサイズが決まります。スループットの値を大きくすると、それに応じた Google Cloud インスタンス タイプが展開されます。Cisco Catalyst 8000V ライセンスは、Cisco Cloud Network Controller のセットアップ プロセスの一部として設定したスループット構成に基づきます。コンプライアンスのために、Smartアカウントに同等以上のライセンスとAXフィーチャセットが必要です。

Cisco Catalyst 8000V は、ティアベース（T0/T1/T2/T3）のスループット オプションをサポートしています。次の表に、Cisco Catalyst 8000V のさまざまなルータ スループット設定に必要な Google Cloud インスタンス タイプを示します。

Cisco Catalyst 8000V のスループット	Google Cloud のインスタンス タイプ
T0（最大 15M のスループット）	n1-standard-2
T1（最大 100M のスループット）	n1-standard-4
T2（最大 1G のスループット）	n1-standard-4
T3（最大 10G のスループット）	n1-standard-8

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

Cisco Cloud Network Controller の通信ポート

Cisco Cloud Network Controller 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。

- Cisco Cloud Network Controller には、セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成 （29 ページ） の最初に Cisco Cloud Network Controller にログインするために使用するものと同じ Cisco Cloud Network Controller 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 Network Controller のインストール ワークフロー

このセクションでは、Cisco Cloud Network Controller 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 Cisco Cloud Network Controller 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 Network Controller で準備するためのすべての前提条件を満たします。

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

2. Google Cloud での Cisco Cloud Network Controller の展開

   Google Cloud での Cisco Cloud Network Controller の展開 （11 ページ）を参照してください。

3. First Time Setup Wizard を使用して Cisco Cloud Network Controller を構成します。

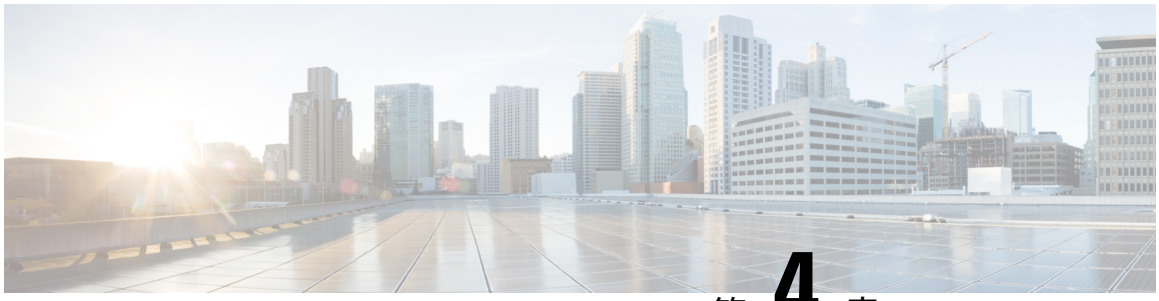
   セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成 （29 ページ）を参照してください。

4. Cisco Cloud Network Controller を介して必要な構成を行います。

   Cisco Cloud Network Controller GUI のナビゲート （57 ページ） およびCisco Cloud Network Controller コンポーネントの構成 （58 ページ） を参照してください。

5. 必要に応じて、展開を削除します。

「Google Cloud での Cisco Cloud Network Controller 展開の削除（Google Cloud ルーターを使用した外部接続） （22 ページ）」を参照してください。



第 4 章

Google Cloud での Cisco Cloud Network Controller 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 Network Controller で使用するプロジェクトを作成します。または既存のものを使用します。

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。

既存のプロジェクトを使用する場合は、このプロジェクトに以前の Cisco Cloud Network Controller 展開がないことを確認します。このプロジェクトに以前の Cisco Cloud Network Controller 展開がある場合は、Google Cloud での Cisco Cloud Network Controller 展開の削除（Google Cloud ルーターを使用した外部接続） （22 ページ） の手順に従って既存の展開を削除します。

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 Network Controller 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 Logging API
- Cloud Pub / Sub API
- クラウド リソース マネージャ API
- クラウド ランタイム構成 API
- Identity and Access Management（IAM）API
- Service Usage 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。

- 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
- 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**：このサービス アカウントで、Cisco Cloud Network Controller 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 Network Controller 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、**[Google APIs Service Agent]** というエントリを持つサービス アカウントを探し、クリックします（**[プリンシパル（Principal）]** 列にも、*<project_number>*@cloudservices.gserviceaccount.com という形式で表示されています）。

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 **[プリンシパル（PRINCIPALS）]** 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. **[新規プリンシパル（New Principals）]** 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 アカウントに必要なロール エントリを追加します。

このサービス アカウントの **[ロール（Role）]** 列には以下のエントリが表示されるはずです。

- エディタ（Editor）

また、このサービス アカウントに次のロールを追加する必要があります。

- プロジェクト IAM 管理者
- ロール管理者

このサービス アカウントに役割エントリを追加するには：

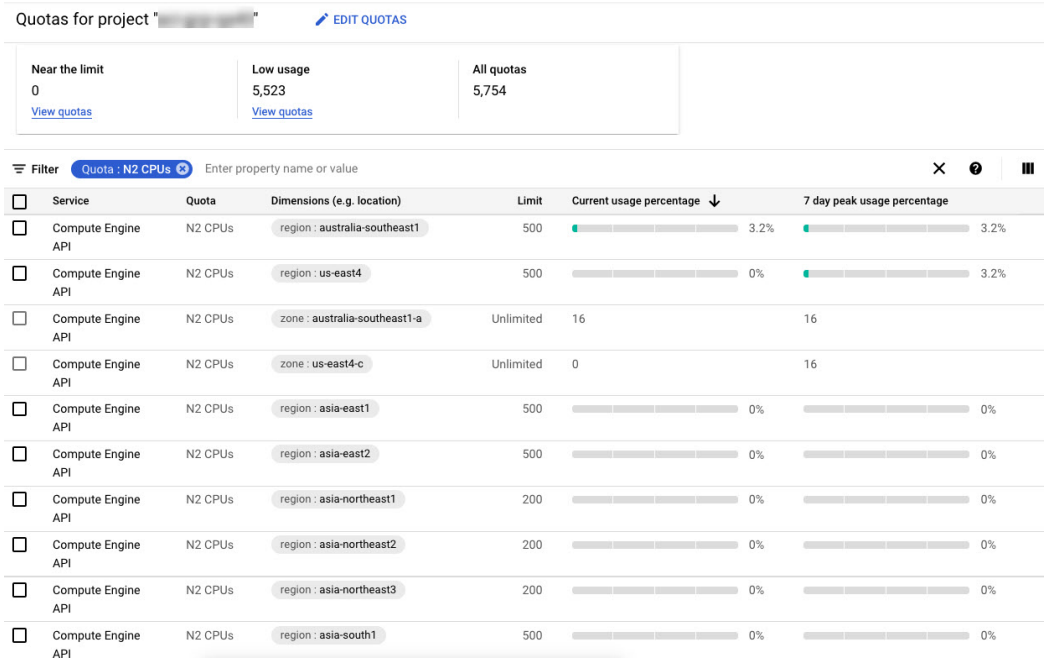
1. このサービス アカウントの行にある鉛筆アイコンをクリックします。

   [権限の編集（Edit Permissions）] ウィンドウが表示されます。
2. **[+別のロールを追加（+ ADD ANOTHER ROLE）]** をクリックし、Project IAM Admin ロール エントリを検索して選択します。
3. **[+別のロールを追加（+ ADD ANOTHER ROLE）]** を再度クリックし、Role Administrator ロール エントリを検索して選択します。
4. **[保存 (SAVE)]** をクリックします。

   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。

ステップ 5 Cisco Cloud Network Controller が展開されているリージョンで Google Cloud アカウントの N2 CPU クォータが少なくとも 16 に設定されていること、およびクォータが現在使用されていないことを確認します。

そうなっていない場合は、Google Cloud でケースを上げて、クォータ制限を増やします。



Linux または MacOS での SSH キー ペアの生成

次の手順では、Linux または MacOS で SSH 公開キーと秘密キーのペアを生成する方法について説明します。

ステップ 1 Linux 仮想マシンまたは Mac で、`ssh-keygen` を使用して公開キーと秘密キーのペアを作成し、出力をファイルに送信します。

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

ステップ 2 保存した公開キー ファイルを確認します。

公開キー ファイルは次のファイルに保存されます。

```
~/.ssh/cnc-ssh-key.pub
```

ステップ 3 公開キーファイルを開き、そのファイルから公開キー情報をコピーします。

公開キー情報は次の形式になります。

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

Google Cloud での Cisco Cloud Network Controller の展開

先頭の ssh-rsa テキストと末尾の admin テキストなど、必要なすべての公開キー情報をコピーしたことを確認します。

以下は、ファイルからコピーする公開キー情報の例です。

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABABABgQC+0Aom7Mblv+w7yWE7QOPytvpankAdOsNWd7keptT6nAnr
S2UjHP0c0KC0jABEo7fL0hwQpwKmLRfHi0poQ3FAy7Oof6XcFJx5aCcCayrGDhm96HPbcPoXjhhg0Fufr4QyL9cWpbsKn9K1k
OhnIw+KQyaxCQS1D1wMsgREKMDrkdk5MZazqZC8haThaaAO/h+i+OQ9juo6N6QPUogHRZ+E9ztyGU/buU1/0vnvzTTinvw8aq
mTnPUQxNI6wZ2FpMH8JHiDQ924wIboAEq0tvidnElemG5wsQrwUghD7r1D9uWjI1rsfGAJL8mSIkWbXZFo+AqNlbE69Oa1TIL
2DfmgYQm3M+qWdzaZPI6i+Ap/dMgGKyy8M4VGFN0o+wbkzi1XdEbMpSEBxyuDtoB5H9T4Kov2yuH/RdqPMSSt+ZgNgBZgcl6S
HXlpSA0GmwyHljYNizo70UMI2JDJDmUc4vCNMgVRxWkNraCWYEZD5iMjnAtIiZvQGmZKQwBH0GY3XIc= admin
```

次のタスク

Google Cloud での Cisco Cloud Network Controller の展開 （15 ページ） の手順に従って Google Cloud の構成プロセスを続行します。これには、Google Cloud 展開テンプレートへの公開キー情報の貼り付けが含まれます。

Google Cloud での Cisco Cloud Network Controller の展開

ステップ 1 Cisco Cloud Network Controller インフラ テナントの Google Cloud アカウントにログインします。

ステップ 2 Google Cloud マーケットプレイスに移動します。

ステップ 3 検索バーで、次を検索します：

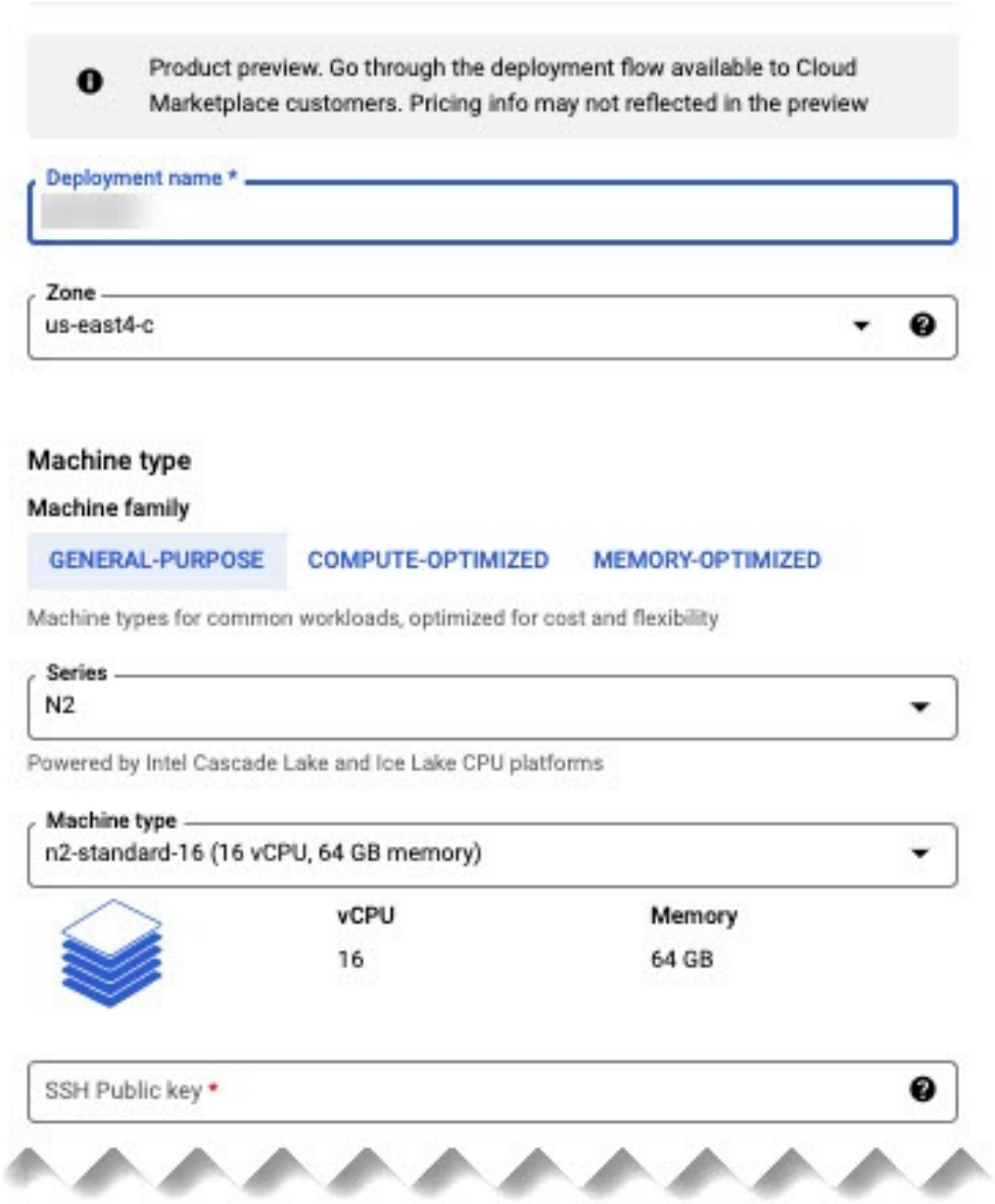
```
Cisco Cloud Network Controller
```

その検索結果を選択します。

ステップ 4 Google Cloud マーケットプレイスの **[Cisco Cloud Network Controller]** ウィンドウで、**[起動（LAUNCH）]** をクリックします。

[新しい Cisco Cloud Network Controller 展開（New Cisco Cloud Network Controller deployment）] ウィンドウが表示されます。

Google Cloud での Cisco Cloud Network Controller の展開



ステップ 5 **[新しい Cisco Cloud Network Controller 展開（New Cisco Cloud Network Controller deployment）]** ウィンドウで、次のフィールドに必要な情報を入力します。

- **[展開名（Deployment name）]** : この Cisco Cloud Network Controller 展開の一意の名前を入力します。
- **[ゾーン（Zone）]** : Cisco Cloud Network Controller が展開されるゾーンを選択します。

  Cisco Cloud Network Controller の展開は、次をサポートするすべてのゾーンでサポートされます。

  - **[汎用（GENERAL PURPOSE）]**（**[マシン ファミリー（Machine family）]**で）
  - **[n2-standard-16]**（**[マシン タイプ（Machine type）]**で）

詳細については、以下を参照してください。

https://cloud.google.com/compute/docs/general-purpose-machines#n2_machines

- **[Machine type（マシン タイプ）]** セクション：
  - **[Machine family（マシン ファミリー）]**：選択していない場合には**[汎用（GENERAL PURPOSE）]** タブを選択します。
  - **[シリーズ（Series）]**：デフォルトの **[N2]** のままにします。
  - **[マシン タイプ（Machine type）]**：このフィールドでは **[n2-standard-16]** オプションを選択することを推奨します。
  - **[SSH 公開キー（SSH Public key）]**：SSH 公開キーを入力して、Cisco Cloud Network Controller への SSH アクセスを有効にします。Cisco Cloud Network Controller には、この SSH キー ペアを使用してログインします。

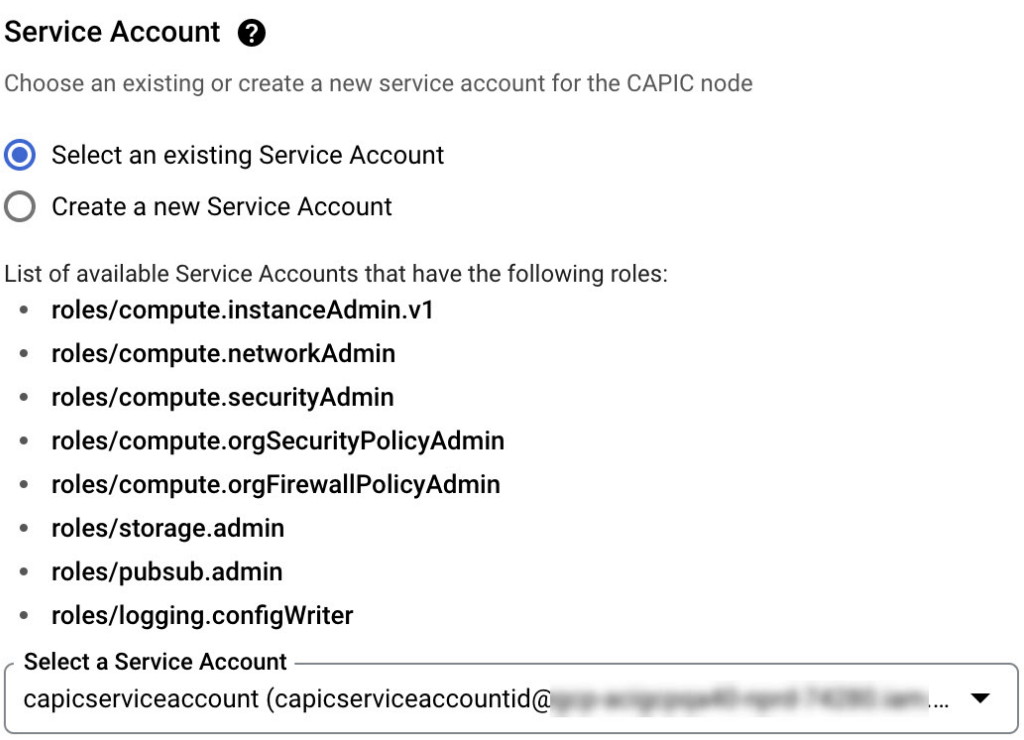
    Linux または MacOS での SSH キー ペアの生成 （14 ページ） の最後でコピーした公開キー情報を貼り付けます。ssh-rsa文字列は、このフィールドに貼り付ける公開キー文字列の先頭にある必要があります。この SSH 公開キーは、次の形式である必要があります。

    ```
    ssh-rsa <ssh-public-key-string> <user-info>
    ```

  - **[サービス アカウント（Service Account）]**：既存のサービス アカウントを選択するか、Cisco Cloud Network Controller 展開用の新しいサービス アカウントを作成します。
    - **[既存のサービス アカウントを選択（Select an existing Service Account）]**：Cisco Cloud Network Controller の展開に使用できる既存のサービス アカウントがある場合は、その既存のサービス アカウントを使用することをお勧めします。

      [既存のサービス アカウントを選択（Select an existing Service Account）] オプションをクリックします。
      - この Cisco Cloud Network Controller 展開に使用できる既存のサービス アカウントがある場合は、次のような画面が表示されます。

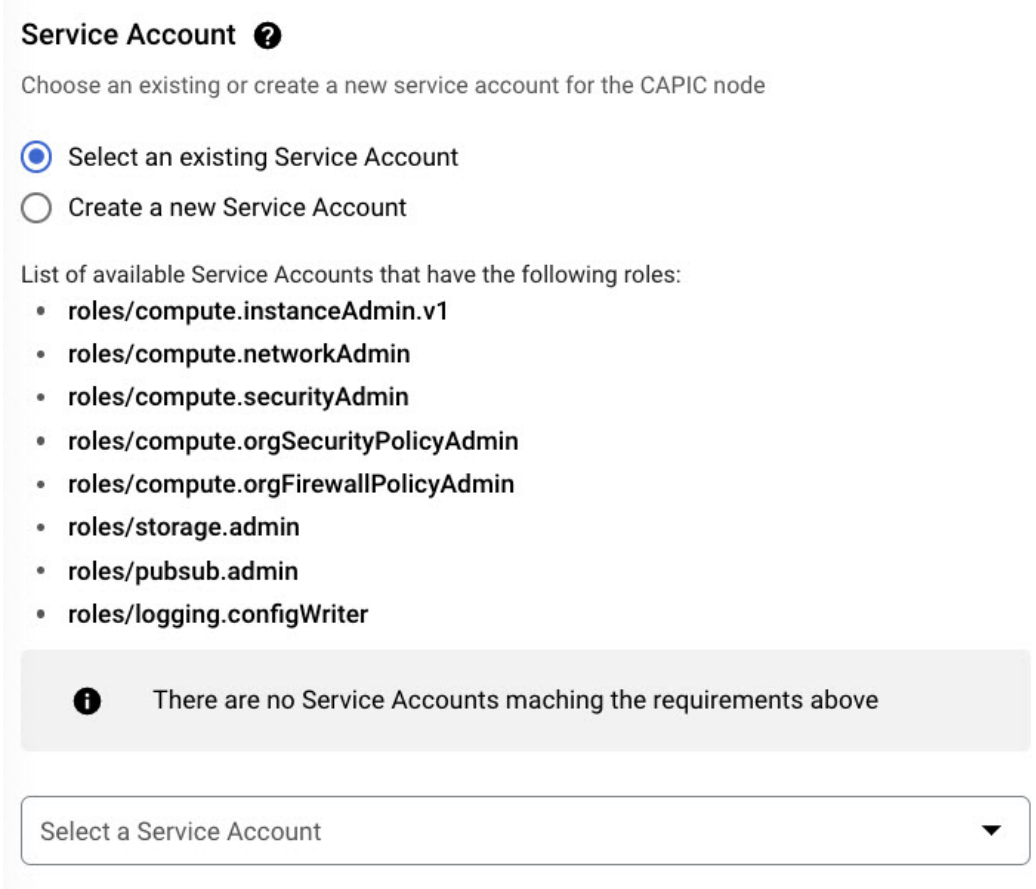
Google Cloud での Cisco Cloud Network Controller の展開



この場合、**[サービス アカウントの選択（Select a Service Account）]** フィールドでサービス アカウントを選択します。

- この Cisco Cloud Network Controller 展開に使用できる既存のサービス アカウントがない場合は、次のような画面が表示されます。

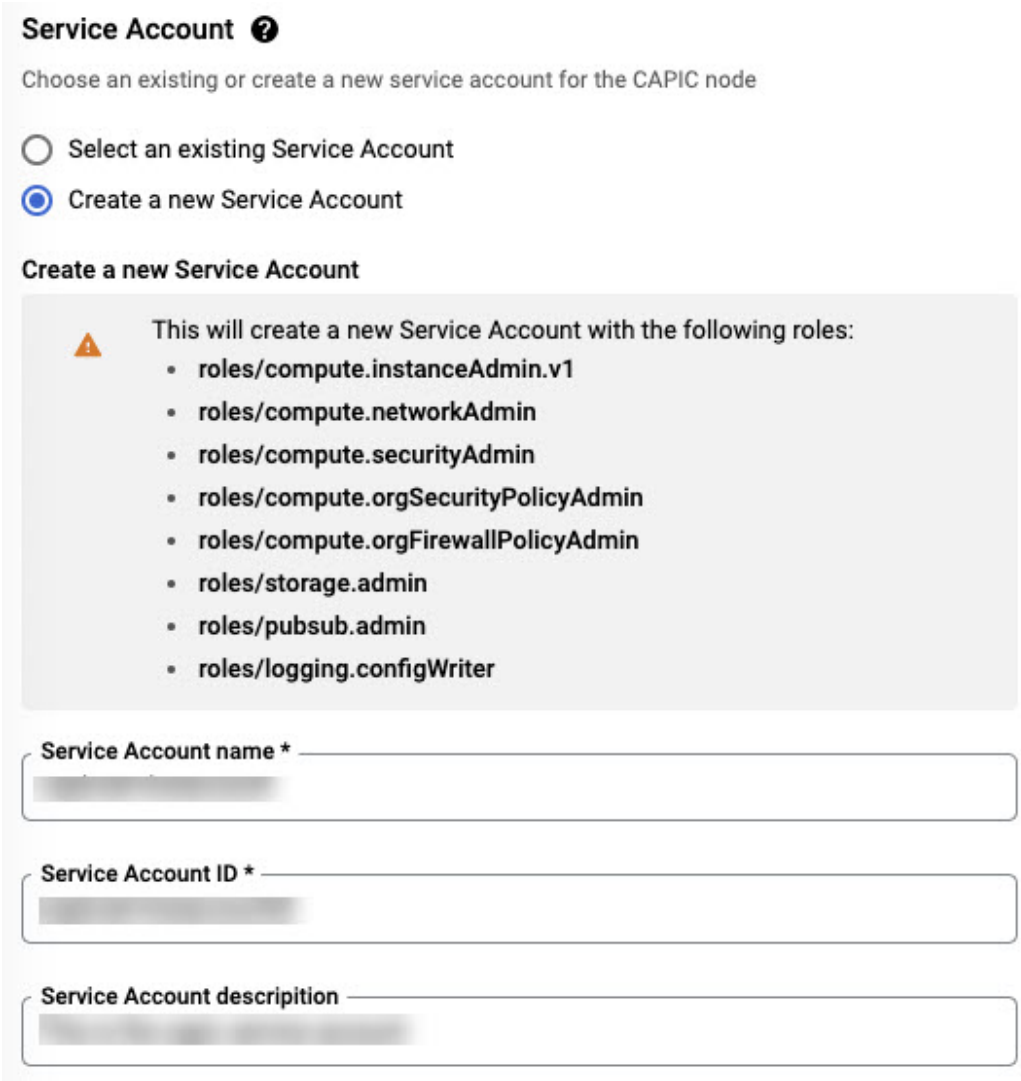
Google Cloud での Cisco Cloud Network Controller の展開



このメッセージが表示された場合は、この Cisco Cloud Network Controller 展開用に新しいサービス アカウントを作成する必要があります。これらの手順を実行する場合は、以下の **[新しいサービス アカウントの作成（Create a new Service Account）]** オプションに移動してください。

- **[新しいサービス アカウントの作成（Create a new Service Account）]**：Cisco Cloud Network Controller の展開に使用できる既存のサービス アカウントがない場合は、**[新しいサービス アカウントの作成（Create a new Service Account）]** オプションをクリックします。

Google Cloud での Cisco Cloud Network Controller の展開



次の情報を入力して、新しいサービス アカウントを作成します。

- **[サービス アカウント名（Service Account name）]**：このサービス アカウントの一意の名前を入力します。サービス アカウント名は 1 ～ 100 文字にする必要があります。
- **[サービス アカウント ID（Servide Account ID）]**：このサービス アカウントの一意の ID を入力します。サービス アカウント ID は 6 ～ 30 文字で、次のパターンに従っている必要があります。

  [a-z][a-z0-9]+[a-z0-9]

- **[サービス アカウントの説明（Service Account description）]**：このサービス アカウントの説明を入力します。

- **[VPC サブネット cidr（VPC subnet cidr）]**：サブネット CIDR を入力してサブネットを作成し、このサブネットから Cisco Cloud Network Controller を起動します。

Google Cloud での Cisco Cloud Network Controller の展開

これは、x.x.x.x/24 の形式の有効な CIDR である必要があります。サブネット マスクは /24 以上である必要があります。

- **[管理者ユーザー パスワード（Admin user password）**：Cisco Cloud Network Controller 管理者ユーザーのユーザー名を入力します。

  パスワードは次のルールに従う必要があります。

  - 8 文字以上
  - 1 つ以上の英字を含む
  - 1つ以上の数字
  - 1 つ以上の特殊文字

- **[リモート アクセス（Remote Access）]**：Cisco Cloud Network Controller へのアクセスが許可されている外部ネットワークを入力します。

  これは、x.x.x.x/xx の形式の有効な IP CIDR である必要があります。

ステップ 6 ページの下部にあるボックスをクリックして Google Cloud の条件に同意し、**[展開（DEPLOY）]** をクリックします。

[展開マネージャ（Deployment Manager）] ウィンドウが表示されます。Cisco Cloud Network Controller が展開中であることを示すメッセージが、約 5 ～ 10 分間表示されます。

- Cisco Cloud Network Controller の展開が完了したことを示すメッセージが表示されるのを待ちます。
- そのメッセージが表示されたら、システムが動作状態になるまでさらに約10分間待ちます。システムが動作状態になるまで、パスワードを使用して Cisco Cloud Network Controller にログインすることはできません。

（注） 何らかの理由で Google Cloud の Cisco Cloud Network Controller の展開を削除する場合は、Google Cloud での Cisco Cloud Network Controller 展開の削除 （22 ページ） の手順を参照してください。

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 Network Controller の構成 （29 ページ）に進み、Cisco Cloud Network Controller のクラウド インフラストラクチャ構成をセットアップします。クラウドインフラストラクチャ構成では、Cisco Cloud Network Controller は必要な Google Cloud コンストラクトを展開します。

Google Cloud での Cisco Cloud Network Controller 展開の削除

何らかの理由で Google Cloud の Cisco Cloud Network Controller 展開を削除する場合、その展開を削除する際に従う手順は、実行しているリリースと使用している展開のタイプによって異なります。

- リリース 25.0(5) より前のリリースで実行していて、Google Cloud ルータを使用して外部接続をセットアップしている場合、何らかの理由でその展開を削除するには、Google Cloud での Cisco Cloud Network Controller 展開の削除（Google Cloud ルーターを使用した外部接続） （22 ページ） の手順に従ってください。
- リリース 25.0(5) 以降で実行していて、
  - Google Cloud ルータを使用して外部接続をセットアップしている場合、何らかの理由でその展開を削除するには、Google Cloud での Cisco Cloud Network Controller 展開の削除（Google Cloud ルーターを使用した外部接続） （22 ページ） の手順に従ってください。
  - Cisco Catalyst 8000V を使用してサイト間接続をセットアップしている場合、何らかの理由でその展開を削除するには、Google Cloud での Cisco Cloud Network Controller 展開の削除（Cisco Catalyst 8000V を使用したサイト間接続） （24 ページ） の指示に従ってください。

Google Cloud での Cisco Cloud Network Controller 展開の削除（Google Cloud ルーターを使用した外部接続）

これらの手順は、Google Cloud での Cisco Cloud Network Controller の展開 （15 ページ） で提供されている手順を使用して Cisco Cloud Network Controller を Google Cloud にすでに展開していることを前提としています。ここでは、Google Cloud ルータを使用して外部接続を設定していたものの、Google Cloud での Cisco Cloud Network Controller 展開を削除する必要が生じたものとします。

何らかの理由で Cisco Cloud Network Controller 展開を削除する場合は、展開を削除する前に、以前に作成したすべてのリソースを削除する必要があります。次の手順に従って、このタイプの Cisco Cloud Network Controller 展開を削除します。

ステップ 1 Cisco Cloud Network Controller 用に Google Cloud に外部ネットワークが展開されている場合は、構成されている外部ネットワークを削除します。

Cisco Cloud Network Controller 用に Google Cloud に外部ネットワークが展開されていない場合は、ステップ 2 （23 ページ） に進んでください。

a) 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。
b) **[外部ネットワーク（External Networs）]** ウィンドウで、構成済みの外部ネットワークの横にあるボックスをクリックし、**[アクション（Actions）]**、>**[外部ネットワークの削除（Delete External Network）]** の順に選択します。

確認ウィンドウで **[OK]** をクリックして、外部ネットワークを削除します。

ステップ 2 いずれかのリージョンにクラウドルータが展開されている場合は、最初に外部接続を無効にします。

a) Cisco Cloud Network Controller GUI で、[インテント（Intent）] アイコン（）をクリックします。
b) **[ワークフロー（Workflows）]** 領域で、**[Cisco Cloud Network Controller のセットアップ（Cisco Cloud Network Controller Setup）]**をクリックします。
c) **[リージョン管理（Region Management）]** エリアで、**[構成の編集（Edit Configuration）]** をクリックします。

[地域管理（Region Management）] ページが表示されます。

d) **[リージョン管理（Region Management）]** ページで、**[Google Cloud Router を使用した外部接続（External Connectivity using Google Cloud Routers）]**の下のボックスにチェックが入っているリージョンを見つけます。

リージョンの **[Google Cloud Router を使用した外部接続（External Connectivity using Google Cloud Routers）]**チェックボックスがオンになっているということは、そのリージョンで外部接続が現在有効になっていることを示しています。

e) 外部ネットワーク接続を無効にする各リージョンで、**[Google Cloud Router を使用した外部接続（External Connectivity using Google Cloud Routers）]** 列のチェックボックスをクリックしてオフにします。

次のメッセージを含む確認ウィンドウが表示されます。

```
External Connectivity
Disabling External Connectivity will delete all Hub Networks and IPsec Tunnels, any Route
Leaks for External Networks will be disrupted.
```

f) 確認ウィンドウで **[確認（Confirm）]** をクリックして、外部接続を無効にします。
g) **[保存して続行（Save and Continue）]** をクリックして、**[完了（Done）]** をクリックします。
h) Google Cloud ポータルで、**[ハイブリッド接続（Hybrid Connectivity）]** > **[VPN]**をクリックして、以前に構成した VPN 接続が正常に削除されたことを確認します。

このウィンドウには、Cisco Cloud Network Controller に対して以前に構成した VPN 接続は表示されません。

ステップ 3 Google Cloud のファイアウォールルールを削除します。

a) ポータルで、[VPC ネットワーク ファイアウォール] をクリックします。Google Cloud >
b) **[名前（Name）]** の横のボックスをクリックして、このウィンドウに表示されているすべてのファイアウォール ルールを選択します。
c) **[削除（DELETE）]** をクリックします。

確認ウィンドウでもう一度 **[削除（DELETE）]** をクリックして、これらのファイアウォール ルールを削除します。

ステップ 4 Google Cloud の展開を削除します。

a) Google Cloudポータルで、**[クラウド展開マネージャ（Cloud Deployment Manage）]** ページに移動します。

b) **[クラウド展開マネージャ（Cloud Deployment Manage）]** をクリックします。

Google Cloud の展開項目が表示されます。

c) 削除する展開の隣にあるチェックボックスをオンにし、**[削除（DELETE）]** をクリックします。

確認ウィンドウで、デフォルト設定をそのままにして、展開と展開によって作成されたすべてのリソースを削除します。確認ウィンドウで **[すべて削除（DELETE ALL）]** をクリックして、展開を削除します。

削除に失敗すると、どのリソースがまだ存在しているため削除が失敗したかを示すメッセージが表示されます。その場合は、そのリソースを見つけて削除し、展開を削除する手順を繰り返します。

ステップ 5 再展開を試みる前に、現在の展開が完全に削除されていることを確認してください。

現在の展開を削除した後、約 10 分待ってから、Cisco Cloud Network Controller を再展開してください。

Google Cloud での Cisco Cloud Network Controller 展開の削除（Cisco Catalyst 8000V を使用したサイト間接続）

これらの手順は、Google Cloud での Cisco Cloud Network Controller の展開 （15 ページ） で提供されている手順を使用して Cisco Cloud Network Controller を Google Cloud にすでに展開していることを前提としています。ここでは、Cisco Catalyst 8000V を使用してサイト間接続を構成していたものの、Google Cloud での Cisco Cloud Network Controller 展開を削除する必要が生じたものとします。

何らかの理由で Cisco Cloud Network Controller 展開を削除する場合は、展開を削除する前に、以前に作成したすべてのリソースを削除する必要があります。次の手順に従って、このタイプの Cisco Cloud Network Controller 展開を削除します。

ステップ 1 Google Cloud の VM インスタンスを削除します。

a) Google Cloud ポータルで、**[仮想マシン（Virtual machines）]** > **[VM インスタンス（VM instances）]** に移動します。

b) **[ステータス（Status）]** の横にあるボックスをクリックして、このウィンドウに表示されているすべての VM インスタンスを選択します（Cisco Cloud Network Controller のインスタンスと Cisco Catalyst 8000V のインスタンス）。

c) **[削除（Delete）]** をクリックします。

（注） **[削除（DELETE）]** オプションを表示するには、縦の省略記号 (...) をクリックする必要がある場合があります。

確認ウィンドウでもう一度 **[削除（DELETE）]** をクリックして、これらの VM インスタンスを削除します。

ステップ 2 Google Cloud のサブネットを削除します。

a) Google Cloud ポータルで、**[VPC ネットワーク（VPC network）]** > **[VPC ネットワーク（VPC networks）]** に移動します。

Cisco Cloud Network Controller（[overlay-1] および [overlay-1-secondary] VPC ネットワーク）の 2 つの VPC ネットワークが表示されます。

b) overlay-1 VPC ネットワークをクリックしてから、**[サブネット（SUBNETS）]** タブをクリックします。

c) このタブに表示されているすべてのサブネットを選択するには、**[名前（Name）]** の横のボックスをクリックします。各サブネットを削除するには、各サブネットと同じ行にあるごみ箱アイコンをクリックします。

d) もう一度 VPC ネットワークに戻り、**[overlay-1-secondary VPC]** ネットワークをクリックしてから、その VPC ネットワークの **[サブネット（SUBNETS）]** タブをクリックします。

e) このタブに表示されているすべてのサブネットを選択するには、**[名前（Name）]** の横のボックスをクリックします。各サブネットを削除するには、各サブネットと同じ行にあるごみ箱アイコンをクリックします。

f) もう一度 **[VPC ネットワーク（VPC ネットワーク）]** に戻り、サブネットが各 VPC ネットワークに表示されていないことを確認します。

サブネットが削除されたことを確認するには、数秒待ってから **[更新（REFRESH）]** をクリックしなければならない場合があります。

ステップ 3 いずれかのリージョンにネイティブ クラウド ルータが展開されている場合は、外部接続を無効にして、VPN トンネル、VPN ゲートウェイ、およびネイティブ クラウド ルーターを削除します。

a) Cisco Cloud Network Controller GUI で、[インテント（Intent）] アイコン（  ）をクリックします。

b) **[ワークフロー（Workflows）]** 領域で、**[Cisco Cloud Network Controller のセットアップ（Cisco Cloud Network Controller Setup）]**をクリックします。

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

[地域管理（Region Management）] ページが表示されます。

d) **[リージョン管理（Region Management）]** ページで、**[Google Cloud Router を使用した外部接続（External Connectivity using Google Cloud Routers）]**の下のボックスにチェックが入っているリージョンを見つけます。

リージョンの **[Google Cloud Router を使用した外部接続（External Connectivity using Google Cloud Routers）]**チェックボックスがオンになっているということは、そのリージョンで外部接続が現在有効になっていることを示しています。

e) 外部ネットワーク接続を無効にする各リージョンで、**[Google Cloud Router を使用した外部接続（External Connectivity using Google Cloud Routers）]** 列のチェックボックスをクリックしてオフにします。

次のメッセージを含む確認ウィンドウが表示されます。

```
External Connectivity
Disabling External Connectivity will delete all Hub Networks and IPsec Tunnels, any Route
Leaks for External Networks will be disrupted.
```

f) 確認ウィンドウで **[確認（Confirm）]** をクリックして、外部接続を無効にします。
g) **[保存して続行（Save and Continue）]** をクリックして、**[完了（Done）]** をクリックします。
h) Google Cloud ポータルで、**[ハイブリッド接続（Hybrid Connectivity）]** > **[VPN]**をクリックして、以前に構成した VPN 接続が正常に削除されたことを確認します。

このウィンドウには、Cisco Cloud Network Controller に対して以前に構成した VPN 接続は表示されません。

ステップ 4 Google Cloud のファイアウォールルールを削除します。

a) Google Cloud ポータルで、**[VPC ネットワーク（VPC network）]** > **[ファイアウォール（Firewall）]**に移動します。
b) **[名前（Name）]** の横のボックスをクリックして、このウィンドウに表示されているすべてのファイアウォール ルールを選択します。
c) **[削除（DELETE）]** をクリックします。

確認ウィンドウでもう一度 **[削除（DELETE）]** をクリックして、これらのファイアウォール ルールを削除します。

ステップ 5 Google Cloud の VPC ピアリングを削除します。

a) Google Cloud ポータルで、**[VPC ネットワーク（VPC network）]** > **[VPC ネットワーク ピアリング（VPC network peering）]**に移動します。
b) **[名前（Name）]** の横のボックスをクリックして、このウィンドウに表示されているすべての VPC ネットワーク ピアリングを選択します。
c) **[削除（DELETE）]** をクリックします。

確認ウィンドウでもう一度 **[削除（DELETE）]** をクリックして、これらの VPC ネットワーク ピアリングを削除します。

ステップ 6 Google Cloud の VPC を削除します。

a) Google Cloud ポータルで、**[VPC ネットワーク（VPC network）]** > **[VPC ネットワーク（VPC networks）]** に移動します。

Cisco Cloud Network Controller（[overlay-1] および [overlay-1-secondary] VPC ネットワーク）の 2 つの VPC ネットワークが表示されます。

b) [overlay-1 VPC] ネットワークをクリックします。
c) **[VPC ネットワークの削除（DELETE VPC NETWORK）]** をクリックして、この VPC ネットワークを削除します。

確認ウィンドウでもう一度 **[削除（DELETE）]** をクリックして、この VPC ネットワーク ピアリングを削除します。

d) もう一度 **[VPC ネットワーク（VPC network）]** に戻り、[overlay-1-secondary] VPC ネットワークをクリックします。

e) **[VPC ネットワークの削除（DELETE VPC NETWORK）]** をクリックして、この VPC ネットワークを削除します。

確認ウィンドウでもう一度 **[削除（DELETE）]** をクリックして、この VPC ネットワークを削除します。

ステップ 7 Cisco Cloud Network Controller 用に Google Cloud に外部ネットワークが展開されている場合は、構成されている外部ネットワークを削除します。

a) 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。

b) **[外部ネットワーク（External Networs）]** ウィンドウで、構成済みの外部ネットワークの横にあるボックスをクリックし、**[アクション（Actions）]**、> **[外部ネットワークの削除（Delete External Network）]** の順に選択します。

確認ウィンドウで **[OK]** をクリックして、外部ネットワークを削除します。

ステップ 8 Google Cloud の展開を削除します。

a) Google Cloudポータルで、**[クラウド展開マネージャ（Cloud Deployment Manage）]** ページに移動します。

b) **[クラウド展開マネージャ（Cloud Deployment Manage）]** をクリックします。

Google Cloud の展開項目が表示されます。

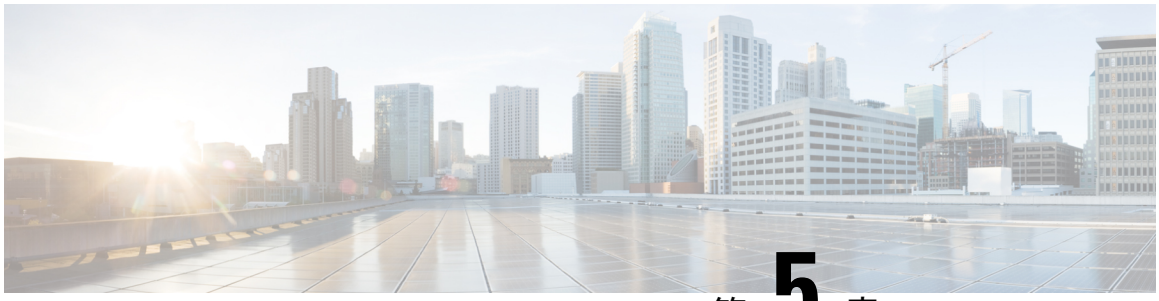
c) 削除する展開の隣にあるチェックボックスをオンにし、**[削除（DELETE）]** をクリックします。

確認ウィンドウで、デフォルト設定をそのままにして、展開と展開によって作成されたすべてのリソースを削除します。確認ウィンドウで **[すべて削除（DELETE ALL）]** をクリックして、展開を削除します。

削除に失敗すると、どのリソースがまだ存在しているため削除が失敗したかを示すメッセージが表示されます。その場合は、そのリソースを見つけて削除し、展開を削除する手順を繰り返します。

ステップ 9 再展開を試みる前に、現在の展開が完全に削除されていることを確認してください。

現在の展開を削除した後、約 10 分待ってから、Cisco Cloud Network Controller を再展開してください。



第 5 章

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

Cisco Cloud Network Controller のクラウドインフラストラクチャ構成をセットアップするには、このトピックの手順に従ってください。Cisco Cloud Network Controller は、必要な Google Cloud の構造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 Cisco Cloud Network Controller 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 Cisco Cloud Network Controller の IP アドレスを特定します。

管理 IP アドレスは、Google Cloud での Cisco Cloud Network Controller の展開 （15 ページ） の展開マネージャーからの出力の最後に表示される IP アドレスです。

[コンピューティング エンジン（Compute Engine）] > [VM インスタンス（VM instances）]に移動して、Cisco Cloud Network Controller の IP アドレスを見つけることもできます。[外部 IP] 列に表示される IP アドレスは、Cisco Cloud Network Controller の IP アドレスです。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

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 Cisco Cloud Network Controller 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。

ステップ 3 Cisco Cloud Network Controller 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（Password）]**：Cisco Cloud Network Controller 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。

[Cisco Cloud Network Controller へようこそ（Welcome to Cisco Cloud Network Controller）] 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**
- **詳細設定**
- **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 （31 ページ） に進みます。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

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 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 11 サイト間接続や外部接続を設定するかどうかを決定します。

- リリース 25.0(5) より前のリリースでは、**[有効化（Enabled）]** の横にあるボックスをクリックして、外部ネットワーク接続を有効にします。
- リリース 25.0(5) 以降では、サイト間接続または外部ネットワーク接続、あるいはその両方を設定するかどうかを決定します。
  - **[Catalyst 8000Vs]**：サイト間のユースケースで、サイト間の接続に Cisco Catalyst 8000V ルータを使用する場合には、リージョンのこのコラムのボックスをオンにします。これはリリース 25.0(5) で導入された機能であり、Cisco Catalyst 8000V ルータを使用して、Google Cloud サイトと他のクラウド サイトまたは ACI オンプレミス サイトとの間のサイト間接続で BGP-EVPN 接続を構成できるようにします。詳細については、*Cisco Cloud Network Controller for Google Cloud ユーザー ガイド*の「BGP-EVPN を使用したサイト間接続」を参照してください。
  - **[Google Cloud ルータを使用した外部接続（External Connectivity using Routers）]**：外部ネットワーク接続にGoogle Cloudルータを使用するリージョンのこの列のボックスをオンにします。これにより、Google Cloud サイトと非 Google Cloud サイトまたは外部デバイスとの間に IPv4 接続を構成でき、Google Cloud ルータと外部デバイスの間に VPN 接続が作成されます。詳細については、*Cisco Cloud Network Controller for Google Cloud ユーザー ガイド*の「外部ネットワーク接続」を参照してください。

ステップ 12 適切なボタンをクリックして、次のページに進みます。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

- **[リージョン管理（Region Management）]** ページでサイト間接続または外部ネットワーク接続を構成していなかった場合（**[リージョン管理（Region Management）]** ページでどのオプションもオンにしていなかった場合）**[保存して続行（Save and Continue）]** をクリックします。**[基本を構成しましょう（Let's Configure the Basics）]**ページに戻ります。「ステップ 20 （36 ページ）」に進みます。
- サイト間接続や外部ネットワーク接続を有効にした場合は、ページの下部にある **[次へ（Next）]** をクリックします。[General Connectivity]ページが表示されます。

ステップ 13 サイト間接続を構成した場合（**[リージョン管理（Region Management）]** ページで 1 つ以上のリージョンに対して **[Catalyst 8000Vs]** オプションを選択した場合）、**[クラウド ルータのサブネット プール（Subnet Pools for Cloud Routers）]**エリアに必要な情報を入力します。

最初のサブネットプールが自動的に入力されます（System Internalとして表示）。このサブネットプールのアドレスは、Cisco Cloud Network Controller で管理する必要がある追加のリージョンのリージョン間接続に使用されます。このフィールドに追加するサブネットプールは、マスク/24の有効なIPv4サブネットである必要があります。

[リージョン管理（Region Management）] ページで、追加のリージョンに Catalyst 8000V を展開するように選択した場合、2 ～ 4 台の Catalyst 8000V を展開する追加のリージョン（16.c （34 ページ） の **[リージョンごとのルータ数（Number of Routers Per Region）]** フィールドに、**2**、**3**、または **4** を入力したリージョン）ごとに、*1* つのサブネットを追加します。

ステップ 14 外部ネットワーク接続を構成した場合（**[リージョン管理（Region Management）]**ページで 1 つ以上のリージョンに対して **[Google Cloud Router を使用した外部接続（External Connectivity using Google Cloud Routers）]** オプションを選択した場合)、必要に応じて **[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。
- 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、前の **[リージョン管理（Region Management）]** ページで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。

前の **[リージョン管理（Region Management）]** ページでの設定ごとに、次のようにします。

- サイト間接続は有効にし（特定のリージョンで **[Catalyst 8000Vs]** 列のボックスをクリックし)、外部ネットワーク接続は有効にしなかった（どのリージョンでも、**[Google Cloud Router を使用した外部接続（External Connectivity using Google Cloud Routers）]** 列のボックスをクリックしなかった）場合、**[ハブ ネットワーク（Hub Network）]** エリアにはデフォルトで次のエントリが表示されますが、編集はできません。
  - **[名前（Name）]**：default

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

- **[BGP 自律システム番号（BGP Autonomous System Number）]**: 65534
- **[VPN ルータ（VPN Router）]** : default

- 外部ネットワーク接続を有効にした（いずれかのリージョンの **[Google Cloud Router を使用した外部接続（External Connectivity using Google Cloud Routers）]** 列で 1 つ以上のボックスをクリックした）場合、必要に応じて、**[BGP 自律システム番号（BGP Autonomous System Number）]** フィールドのデフォルト エントリを編集できます。

a) **[ハブ ネットワーク（Hub Network）]** 領域で、鉛筆アイコンをクリックして、**[ハブ ネットワーク（Hub Network）]** フィールドの情報を編集します。

[ネットワークの編集（Edit Network）] ウィンドウが表示されます。**[名前（Name）]** および **[VPN ルータ（VPN Router）]** フィールドのデフォルトエントリは編集できないことに注意してください。

b) 必要に応じて、**[BGP Autonomous System Number（BGP 自律システム番号）]** フィールドの値を変更します。

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。

c) **[ハブ ネットワークの編集（Editing Hub Network）]** 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。

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

ステップ 15 **[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 16 **[Catalyst 8000Vs]** 領域に必要な情報を入力します。

a) **[C8kVs の BGP 自律システム番号（BGP Autonomous System Number for C8kVs）]** フィールドで、固有の BGP 自立システム番号（ASN）を入力します。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

BGP自律システム番号は 1 ー 65535 の範囲で指定できます。

b) **[パブリック IP を C8kV インスタンスに割り当てる（Assign Public IP to C8kV Interface）]** フィールドで、パブリック IP アドレスを Catalyst 8000V インターフェイスに割り当てるかどうかを決定します。

プライベート IP アドレスは、デフォルトで Catalyst 8000V インターフェイスに割り当てられます。**[パブリック IP を C8kV インスタンスに割り当てる（Assign Public IP to C8kV Interface）]** オプションは、パブリック IP アドレスを Catalyst 8000V インターフェイスにも割り当てるかどうかを決定します。

Catalyst 8000V インターフェイス IP アドレスは次の目的で使用されます。

- Catalyst 8000V を管理すること、または Catalyst 8000V に直接 SSH で接続することができます。
- マルチクラウドおよびハイブリッドクラウド接続のために、サイト全体のインターフェイスをクロスプログラムできます。 Cisco Nexus Dashboard Orchestrator
- コントロール プレーン トラフィックとデータ プレーン トラフィックの両方の Catalyst 8000V の場合

デフォルトでは、この **[有効]** チェック ボックスはオンになっています。これは、Catalyst 8000V にパブリック IP アドレスを割り当てられることを意味します。

- *[パブリック（public）]* IP アドレスを Catalyst 8000V に割り当てる場合は、**[有効（Enabled）]** の横にあるチェックボックスをオンのままにします。
- プライベート IPアドレスのみをCatalyst 8000V に割り当てるには、オプションを無効化するために **[有効（Enabled）]** の横にあるチェックボックスをオフにします。

Catalyst 8000V 接続をプライベートからパブリック、またはその逆に変更すると、ネットワークが中断する可能性があることに注意してください。さらに、パブリック IP アドレスが Catalyst 8000V から削除された場合、Google Cloud サイトは Google Cloud 相互接続を介してプライベート IP アドレスを使用してオンプレミスの ACI サイトに接続します。Nexus Dashboard Orchestrator から Google Cloud サイトのプライベート サイト間接続を構成し、Google Cloud ポータルから Google Cloud 相互接続を構成する必要があります。

（注） Catalyst 8000V に割り当てられたパブリック IP アドレスとプライベート IP アドレスの両方が、**[クラウド リソース（Cloud Resources）]** 領域にルータの他の詳細とともに表示されます。Catalyst 8000V にパブリック IP アドレスが割り当てられていない場合は、プライベート IP アドレスだけが表示されます。

c) **[リージョンあたりのルータの数（Number of Routers Per Region）]** フィールドで、各リージョンで使用される Catalyst 8000Vs の数を選択します。

d) **[ユーザー名（Username）]** に、Catalyst 8000V のユーザー名を入力します。

e) **[パスワード（Password）]** フィールドに、Catalyst 8000V のパスワードを入力します。

[Confirm Password] フィールドに、もう一度パスワードを入力します。

f) **[ルータのスループット（Throughput of the routers）]** フィールドで、Catalyst 8000V のスループットを選択します。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

このフィールドの値を変更すると、展開されている Catalyst 8000V インスタンスのサイズが変更されます。スループットの値を高くすると、導入されるVMのサイズが大きくなります。

次の点に注意してください。

- Catalyst 8000V のライセンスは、この設定に基づいています。準拠するには、Smartアカウントに同等以上のライセンスが必要です。詳細については、「Google Cloud での Cisco Cloud Network Controller の展開に使用されるリソース （7 ページ）」を参照してください。
- クラウドルータは、ルータのスループットまたはログインクレデンシャルを変更する前に、すべてのリージョンから展開解除する必要があります。

  将来のある時点でこの値を変更することが必要になった場合は、Catalyst 8000V を削除してから、この章のプロセスを再度繰り返し、同じ**[ルータのスループット（Throughput of the routers）]**フィールドで新しい値を選択する必要があります。

g) 必要に応じて、[TCP MSS]フィールドに必要な情報を入力します。

[TCP MSS] オプションを使用すれば TCP 最大セグメントサイズ（MSS）を構成できます。この値は、データギガビットイーサネットインターフェイス、クラウドルータのIPSecトンネルインターフェイス、およびクラウド、オンプレミス、またはその他のクラウドサイトに対するVPNトンネルインターフェイスを含む、すべてのクラウドルータインターフェイスに適用されます。クラウドへのVPNトンネルの場合、クラウドプロバイダーのMSS値がこのフィールドに入力した値よりも小さい場合は、低い方の値が使用されます。それ以外の場合は、このフィールドに入力した値が使用されます。

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

h) **[ライセンス トークン（License Token）]** フィールドに、Catalyst 8000V のライセンス トークンを入力します。

これは、シスコスマートソフトウェアライセンシングアカウントからの製品インスタンス登録トークンです。このライセンストークンを取得するには、に移動し、[Smart Software Licensing Inventory Virtual Account]に移動して、製品インスタンス登録トークンを見つけます。http://software.cisco.com>>詳細については、「Cisco Cloud Network Controller のライセンシング （3 ページ）」を参照してください。

（注） プライベート IP アドレスを 16.b （34 ページ）の Catalyst 8000V に割り当てた場合、プライベート IP アドレスを使用して Catalyst 8000V のスマート ライセンスを登録するときにサポートされる唯一のオプションは、**[Cisco Smart Software Manager（CSSM）に直接接続（Direct connect to Cisco Smart Software Manager (CSSM)）]** です。この場合、エクスプレスルート経由でCSSMに到達可能性を提供する必要があります。

ステップ 17 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、外部ネットワークの構成 （39 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。

セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成

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 18 **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 19 **[ワークフロー（Workflows）]** 領域で、**[Cisco Cloud Network Controller の設定（Cisco Cloud Network Controller 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（DNS and NTP Servers）]**、**[詳細設定（Advanced Settings）]**、**[リージョン管理（Region Management）]**、**[スマート ライセンシング（Smart Licensing）]** の各オプションが示されます。

ステップ 20 **[詳細設定（Advanced Settings）]** 領域で、**[構成の編集（Edit Configuration）]** をクリックします。

ステップ 21 **[コントラクト ベースのルーティング（Contract Based Routing）]** フィールドで、**[はい（yes）]** の横のボックスをクリックしてコントラクト ベースのルーティングを有効にし、**[保存して続行（Save and Continue）]** をクリックします。

（注） Google Cloud サイトに移動し、**[サイト間接続（Inter-Site Connectivity）]** 領域の **[コントラクト ベースのルーティング（Contract Based Routing）]** オプションをクリックして、Nexus ダッシュボード オーケストレータを介してコントラクト ベースのルーティングを有効にすることもできます。

ステップ 22 **[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 23 **[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 Cisco Cloud Network Controller 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。
- 製品インスタンスの登録トークン（これによりスマート アカウントを識別）を生成し、そのトークンをコピーするか、または保存します。

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。

ステップ 24 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 25 **[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、Cisco Cloud Network Controller の内部ネットワーク接続の設定は完了です。

Cisco Cloud Network Controller 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。

次のタスク

必要に応じて、次のセクションまたはドキュメントのいずれかの手順を完了します。

- Cisco Cloud Network Controller セットアップ ウィザードの構成の確認 （37 ページ）
- 初期構成の完了 （39 ページ）
  - 外部ネットワークの構成 （39 ページ）
  - テナントの作成 （43 ページ）
  - Cisco Catalyst 8000V ルータを使用してサイト間接続用に BGP-EVPN 接続を構成した場合は、BGP-EVPN を使用したサイト間接続のための VPC ピアリングの構成 （54 ページ） の手順に従って、Google Cloud サイト内のユーザー VPC が他のクラウド サイトまたは ACI オンプレミス サイトの VPC と通信できるようにします。
- Cisco Cloud Network Controller サイトとともに追加のサイト (オンプレミス サイトまたはクラウド サイト) を管理している場合は、Nexus Dashboard Orchestrator を使用した Google Cloud サイトの管理ドキュメントを参照してください。
- Cisco Cloud Network Controller GUI を理解する （57 ページ）
- SSH を介した Cisco Cloud Network Controller へのログイン （59 ページ）

Cisco Cloud Network Controller セットアップ ウィザードの構成の確認

このトピックの手順に従って、Cisco Cloud Network Controller セットアップ ウィザードに入力した構成情報が正しく適用されていることを確認します。

ステップ 1 Cisco Cloud Network Controller 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。

ステップ 2 Catalyst 8000V を使用してサイト間接続用に BGP-EVPN 接続をセットアップする場合は、Google Cloud 側の VM インスタンスの数が、Cisco Cloud Network Controller でセットアップした Catalyst 8000V の数と一致することを確認します。

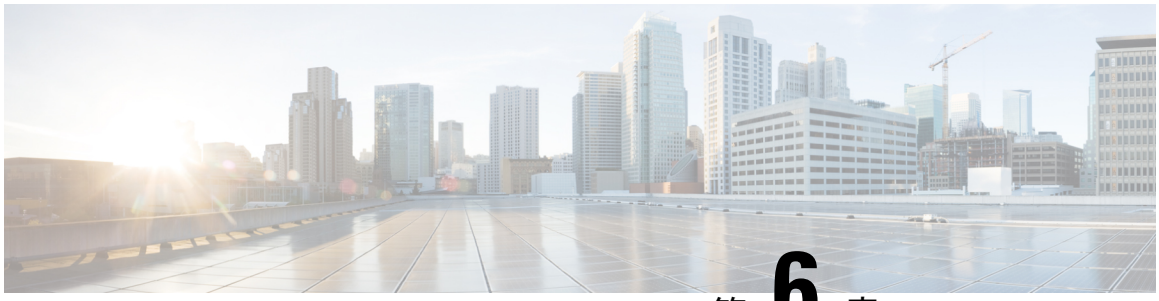
a) インフラ テナントに関連付けられた Google Cloud プロジェクトにログインします。
b) Google Cloud の **[コンピューティング エンジン（Compute Engine）]** > **[VM インスタンス（VM instances）]** に移動します。
c) **[インスタンス（Instances）]** タブに表示される VM インスタンスの数が、サイト間接続用の BGP-EVPN 接続に使用している Catalyst 8000V の総数と一致することを確認します。

たとえば、セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成 （29 ページ） の Cisco Cloud Network Controller にクラウド インフラストラクチャ構成をセットアップしているとして、2 つのリージョンを選択し、リージョンごとに 2 つの Catalyst 8000V を選択した場合、**[インスタンス（Instances）]** タブに 4 つの VM インスタンスが表示されます。

ステップ 3 Catalyst 8000V を使用してサイト間接続用に BGP-EVPN 接続をセットアップする場合は、Google Cloud の overlay-1 VPC および overlay-1 セカンダリ VPC 用に VPC ネットワークがセットアップされていることを確認してください。

詳細については、*Cisco Cloud Network Controller for Google Cloud ユーザー ガイド*の「BGP-EVPN を使用したサイト間接続」を参照してください。

a) Google Cloud の **[VPC ネットワーク（VPC network）]** > **[VPC ネットワーク（VPC networks）]**に移動します。
b) **[VPC ネットワーク（VPC networks）]** 画面に、overlay-1 VPC および overlay-1 セカンダリ VPC 用に設定された VPC ネットワークが表示されていることを確認します。



第 6 章

初期構成の完了

外部ネットワークの構成

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

始める前に

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

ステップ 1 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）] > [外部ネットワーク（External Networks）]** に移動します。
構成された外部ネットワークが表示されます。Cisco Cloud Network Controller 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 **[Cisco Cloud Network Controller 設定（Cisco Cloud Network Controller Setup）]** リンクをクリックし、ハブネットワークを作成して、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 Network Controller の構成（29 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	この 外部VRF は、オンプレミス CCR との外部接続に使用されます。この目的で複数の 外部VRF を作成できます。 この VRF は、VRF が次の 3 つの特性をすべて備えている場合に 外部VRF として識別されます。 • インフラ テナントの下で構成された • 外部ネットワークに関連付けられている • クラウド コンテキスト プロファイルに関連付けられていない 外部ネットワークに関連付けられているVRFはすべて 外部VRF になります。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。 外部VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。 **[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRFの選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択します。 [+ VRF の作成（+ Create VRF）] オプションを使用してVRFを作成することもできます。 3. **[選択（Select）]**をクリックします。 **[外部ネットワークの作成（Create External Network）]** ダイアログボックスに戻ります。
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に関する詳細は、Cisco Cloud Network Controller for Google Cloud インストール ガイド、リリース 25.0(x) 以降の、「セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成」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。
[設定（Settings）]	

[プロパティ（Properties）]	説明
地域	リージョンを選択するには: 1. **[地域の追加（Add Region）]** をクリックします。 **[地域の選択（Select Regions）]** ダイアログボックスが表示されます。 • 初回セットアップの一部として選択した地域がここに表示されます。 • 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	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。 VPN ネットワークを追加するには、次の手順を実行します。 **1.** **[VPNネットワークの追加（Add VPN Network）]** をタップします。 **[VPN ネットワークの追加（Add VPN Network）]** ダイアログボックスが表示されます。 **2.** **[名前（Name）]** フィールドに VPN ネットワークの名前を入力します。 **3.** **[+ IPSec ピアの追加（+ Add IPSec Peer）]** をクリックします。 IPSec ピア エントリごとに 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。

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。

テナントの作成

次のセクションでは、マネージド テナントまたはアンマネージド テナントを作成する方法。

Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する

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。

Google Cloud の観点から理解するのに有用な領域は、組織とフォルダのレベルですが、Cisco Cloud Network Controller の観点から最も関連性があるのは、プロジェクトのレベルです。

各 Cisco Cloud Network Controller 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 Network Controller 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 プロジェクト内に複数の Cisco Cloud Network Controller テナントを存在させることはできません。

Cisco Cloud Network Controller 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、Cisco Cloud Network Controller と他のテナントのポリシーを実行、展開し、また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（Cisco Cloud Network Controller 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 Cisco Cloud Network Controller テナントを構成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 （44 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 （44 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 Network Controller によって管理されます。
- このタイプのユーザーテナントのテナント構成プロセスの一環として、最初にCisco Cloud Network Controller GUIで **[マネージド ID（Managed Identity）]** を選択します。
- Cisco Cloud Network Controller で必要なパラメータを構成したら、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。Cisco Cloud Network Controller によって作成されたサービスアカウントを、次のルールを使用してIAMユーザーとして追加します。
  - 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、Cisco Cloud Network Controller GUI を使用した管理対象テナントの作成 （47 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 Network Controller によって管理されていません。
- このタイプのテナントの Cisco Cloud Network Controller に必要なパラメータを構成する前に、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。
- このタイプのユーザーテナントのテナント構成プロセスの一環として、Cisco Cloud Network Controller GUIで **[アンマネージド ID（Unmanaged Identity）]** を選択します。Cisco Cloud Network Controller でこのタイプのテナントの構成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、Cisco Cloud Network Controller GUI を使用したアンマネージド テナントの作成 （51 ページ） を参照してください。

ユーザー テナントの Google Cloud プロジェクトのセットアップ

このセクションの手順を実行して、ユーザー テナントの Google Cloud プロジェクトをセットアップします。そのユーザー テナントは、管理対象または管理対象外のテナントです。

ステップ 1 必要に応じて、ユーザー テナントの Google Cloud プロジェクトを作成します。

各ユーザー 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。ユーザー 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。

a) Google アカウントにログインします。
b) **[IAM & Admin]** > **[Manage resources]** に移動します。
c) 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。
d) **[+プロジェクトの作成（+ CREATE PROJECT）]** をクリックします。
e) 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。

f) **[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。

g) [作成（CREATE）] をクリックします。

ステップ 2 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、このユーザー 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 3 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、このユーザー 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。

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。

- Cisco Cloud Network Controller で管理対象テナントを作成する
- Google Cloud の管理対象テナントに必要な権限を設定します。

Cisco Cloud Network Controller 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 Network Controller で管理す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 ユーザーテナントの Google Cloud プロジェクトをセットアップします。

これらの手順については、ユーザー テナントの Google Cloud プロジェクトのセットアップ （45 ページ）を参照してください。

ステップ 2 Cisco Cloud Network Controller GUI で、**[アプリケーション管理（Application Management）]** > **[VRF]**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。正規表現の一致: `[az]（[-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。
説明	テナントの説明を入力します。
[設定（Settings）]	
セキュリティドメインの追加（Add Security Domain）	テナントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]** をクリックして、セキュリティ ドメインをテナントに追加します。
Google Cloud Project	
Google Cloud Project ID	この Cisco Cloud Network Controller テナントに関連付けられる Google Cloud プロジェクト ID を入力します。
アクセスタイプ	Cisco Cloud Network Controller で管理する予定のテナントの場合は、アクセス タイプとして **[管理対象 ID（Managed Identity）]** を選択します。 詳細については、Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する （43 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

Google Cloud で管理対象テナントに必要な構成を完了します。これらの手順については、マネージド テナント用に Google Cloud で必要な権限を設定する （49 ページ） にアクセスしてください。

マネージド テナント用に Google Cloud で必要な権限を設定する

マネージドテナントを作成している場合は、Google Cloud で必要なアクセス許可を設定する必要があります。

（注） アンマネージド テナントを作成している場合は、この手順に従う必要はありません。

ステップ 1 Google Cloud GUI で、このマネージド テナントに関連付けられる 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。

ステップ 2 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。

ステップ 3 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作成されたサービス アカウントを見つけます。

ステップ 4 サービス アカウント名をコピーします。

ステップ 5 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。

ステップ 6 このサービス アカウントの権限を設定します。

a) 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。

b) **[+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。

c) **[+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

d) 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。

アンマネージド テナントの作成

次のセクションでは、アンマネージド テナントを作成するために必要な情報を提供します。

- Google Cloud からアンマネージドテナントに必要な秘密鍵情報を生成してダウンロードします
- Cisco Cloud Network Controller にアンマネージド テナントを作成する

アンマネージド テナントの Google Cloud からの秘密キー情報の生成とダウンロード

アンマネージド テナントを作成する場合は、最初に Google Cloud から必要な秘密キー情報を生成してダウンロードする必要があります。

（注） マネージド テナントを作成している場合は、この手順の手順に従う必要はありません。

ステップ 1 Google Cloud で、まだ選択されていない場合、アンマネージド テナントに関連付けられる Google Cloud プロジェクトを選択します。

ステップ 2 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 3 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 4 **[キー（KEYS）]** タブをクリックします。

ステップ 5 **[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 6 **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 7 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。

Cisco Cloud Network Controller GUI を使用したアンマネージド テナントの作成

このセクションでは、GUI を使用して Cisco Cloud Network Controller GUI で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。

始める前に

このセクションの手順を使って続行する前に、アンマネージド テナントの Google Cloud からの秘密キー情報の生成とダウンロード （50 ページ） で説明されている手順を完了します。

ステップ 1 ユーザーテナントの Google Cloud プロジェクトをセットアップします。

これらの手順については、ユーザー テナントの Google Cloud プロジェクトのセットアップ （45 ページ）を参照してください。

ステップ 2 Cisco Cloud Network Controller GUI で、**[アプリケーション管理（Application Management）]** > **[VRF]**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。正規表現の一致: `[az]([-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。
説明	テナントの説明を入力します。
[設定（Settings）]	
セキュリティ ドメインの追加（Add Security Domain）	テナントのセキュリティ ドメインを追加するには、次の手順を実行します。 1. **[セキュリティ ドメインの追加（Add Security Domain）]**をクリックします。**[セキュリティ ドメインの選択（Select Security Domains）]** ダイアログが表示され、左側のペインにセキュリティ ドメインのリストが表示されます。 2. セキュリティ ドメインをクリックして選択します。 3. **[選択（Select）]**をクリックして、セキュリティ ドメインをテナントに追加します。
Google Cloud Project	

[プロパティ（Properties）]	説明
Google Cloud Project ID	この Cisco Cloud Network Controller テナントに関連付けられる Google Cloud プロジェクト ID を入力します。
アクセスタイプ	Cisco Cloud Network Controller で管理されていないテナントの場合は、アクセスタイプとして**[アンマネージド ID（Unmanaged Identity）]** を選択します。 詳細については、Cisco Cloud Network Controller を使用した Google Cloud の展開を理解する （43 ページ）を参照してください。
キーID	アンマネージドテナントの Google Cloud からの秘密キー情報の生成とダウンロード （50 ページ） でダウンロードした 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	アンマネージドテナントの Google Cloud からの秘密キー情報の生成とダウンロード （50 ページ） でダウンロードした JSON ファイルの `private_key` フィールドの情報を入力します。
クライアントID	アンマネージドテナントの Google Cloud からの秘密キー情報の生成とダウンロード （50 ページ） でダウンロードした JSON ファイルの `client_id` フィールドの情報を入力します。
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。

[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。

BGP-EVPN を使用したサイト間接続のための VPC ピアリングの構成

Cisco Catalyst 8000V ルーターを使用してサイト間接続用に BGP-EVPN 接続を構成した場合は、これらの手順に従って、Google Cloud サイト内のユーザー VPC が他のクラウド サイトまたは ACI オンプレミス サイトの VPC と通信できるようにします。詳細については、*Cisco Cloud Network Controller for Google Cloud ユーザー ガイド*の「BGP-EVPN を使用したサイト間接続」セクションの「VPC ピアリング」を参照してください。

通常、VRF を作成してから、その VRF の**ハブ ピアリング**を確認する Nexus ダッシュボード オーケストレータを介して BGP-EVPN を使用して、サイト間接続用に VPC ピアリングを構成します。これらの手順については、該当する Nexus Dashboard Orchestrator のドキュメントを参照してください。

Cisco Cloud Network Controller 側でこの構成を変更するには、次の手順を実行します。

ステップ 1 Cisco Cloud Network Controller GUI で、**[アプリケーション管理（Application Management）]** > **[クラウド コンテキスト プロファイル（Cloud Context Profiles）]** に移動します。

ステップ 2 **[名前（Name）]** 列で、オーバーレイ 1 VPC とピアリングする VPC に関連付けられているクラウド コンテキスト プロファイルの名前をダブルクリックします。

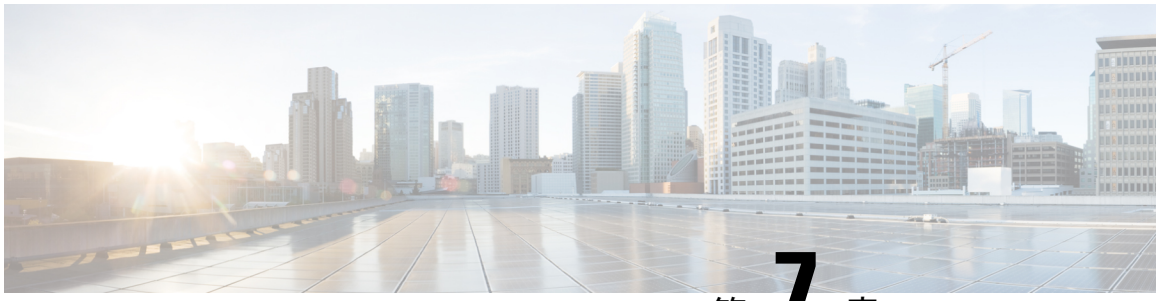
このクラウド コンテキスト プロファイルの詳細情報を提供する別のウィンドウが表示されます。

ステップ 3 **[アクション（Actions）]** > **[編集（Edit）]**をクリックします。

ステップ 4 **[VPC ハブ ピアリング（VPC Hub Peering）]** 領域で、**[有効化（Enable）]** の横にあるボックスをクリックして、この VPC の VPC ピアリングを有効にし、**[保存（Save）]** をクリックします。

ステップ 5 Google Cloud で、**[VPC ネットワーク（VPC network）]** > **[VPC ネットワーク ピアリング（VPC network peering）]**に移動します。

ステップ 6 Google Cloud サイトのユーザー VPC がオーバーレイ 1 VPC とピアリングしていることを確認します。



第 7 章

Cisco Cloud Network Controller GUI を理解する

Cisco Cloud Network Controller GUI のナビゲート

Cisco Cloud Network Controller は、インストール後に、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。これを行うには、Cisco Cloud Network Controller GUI を使用します。

Cisco Cloud Network Controller 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 Network Controller のトポロジ、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 Network Controller コンポーネントの構成 （58 ページ） を参照してください。*Cisco Cloud Network Controller* ユーザー ガイド の「Cisco Cloud Network Controller GUIのアイコンを理解する」の項も参照してください。

Cisco Cloud Network Controller 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 Cloud Network Controller User Guide* の「Understanding the Cisco Cloud Network Controller」の項を参照してください。

Cisco Cloud Network Controller GUI を使用したテナントの作成

次のセクションでは、Cisco Cloud Network Controller 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 Network Controller コンポーネントの構成

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 Network Controller での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 Network Controller をインストールしておく必要があります。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 Network Controller 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。

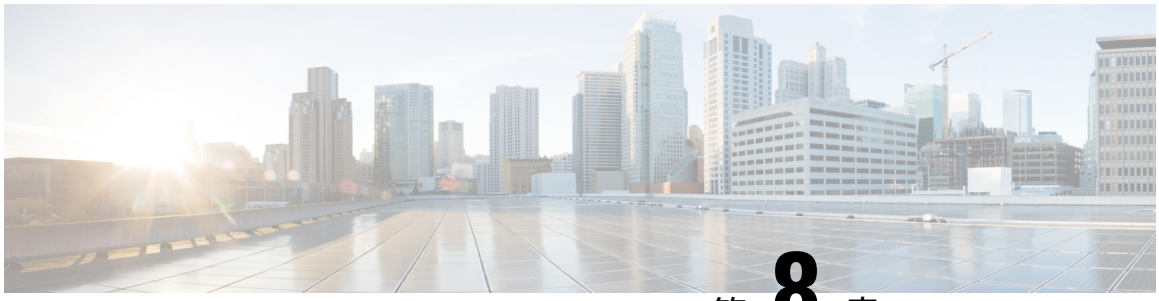
たとえば、テナントを設定する場合は、検索ウィンドウにtenantと入力します。検索は、テナントの作成と設定に関連するタスクのリストを返します。

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。



第 8 章

SSH を介した Cisco Cloud Network Controller へのログイン

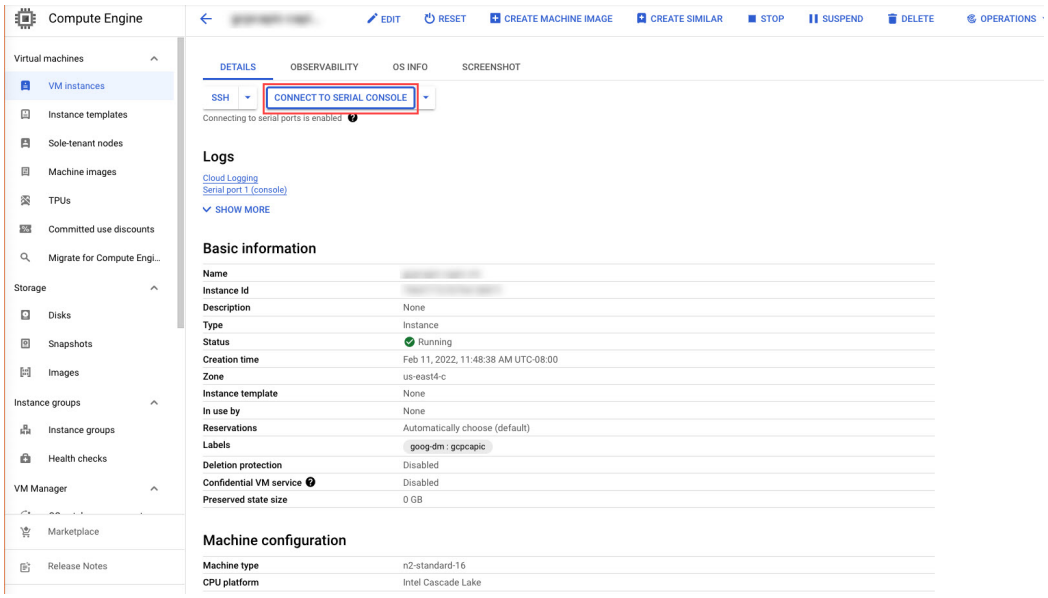
通常、セットアップ ウィザードを使用した Cisco Cloud Network Controller の構成 （29 ページ）で説明されているように、ブラウザを介して Cisco Cloud Network Controller にログインします。ただし、何らかの理由で SSH 経由で Cisco Cloud Network Controller にログインする必要がある場合のために、前のセクションで生成した SSH キーまたは SSH パスワード認証を使用して Cisco Cloud Network Controller にログインする方法について説明します。

Google Cloud を介したシリアル コンソールへの接続

次のように移動し、Google Cloud を介してシリアル コンソールに接続できます。

[仮想マシン（Virtual Machines）] > [VM インスタンス（VM instances）]

[VM インスタンス（VM instances）] ページで、**[インスタンス（Instances）]** タブをクリックし、Cisco Cloud Network Controller のインスタンスをクリックしてから、**[シリアル コンソールに接続（CONNECT TO SERIAL CONSOLE）]** をクリックします。



（注） この Google Cloud ページで許可されている操作は、シリアル コンソールへの接続のみです。たとえば、Google Cloud でこのページから Cisco Cloud Network Controller に SSH で接続することは許可されていません。SSH を介した Cisco Cloud Network Controller へのログイン （59 ページ） で説明されている他の方法を使用すれば、Cisco Cloud Network Controller に SSH で接続できます。

SSH キーを使用した Cisco Cloud Network Controller へのログイン

ステップ 1 Cisco Cloud Network Controller インフラ テナントの Google Cloud アカウントにログインします。

ステップ 2 Cisco Cloud Network Controller の IP アドレスを特定します。

Google Cloud での Cisco Cloud Network Controller の展開 （15 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。

[コンピューティング エンジン（Compute Engine）] > [VM インスタンス（VM instances）]に移動して、Cisco Cloud Network Controller の IP アドレスを見つけることもできます。[外部 IP] 列に表示される IP アドレスは、Cisco Cloud Network Controller の IP アドレスです。

ステップ 3 Linux システムの場合、以下を入力して、SSH キーを使用して Cisco Cloud Network Controller にログインします。

```
# ssh -i ~/.ssh/cnc-ssh-key admin@public-IP-address
```

次に例を示します。

```
# ssh -i ~/.ssh/cnc-ssh-key admin@192.0.2.1
```

公開キー ファイルの場所と形式の詳細については、Linux または MacOS での SSH キー ペアの生成 （14 ページ） を参照してください。

SSH パスワード認証を使用した Cisco Cloud Network Controller へのログイン

公開キーを使用するSSHとは異なり、SSHパスワード認証はデフォルトで無効になっています。ユーザー名とパスワードを使用して Cisco Cloud Network Controller に SSH 接続できるように、次の手順を使用して SSH パスワード認証を有効にします。

ステップ 1 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 Cisco Cloud Network Controller にアクセスします。

たとえば、`https://192.0.2.1`です。

ステップ 2 Cisco Cloud Network Controller のログイン ページに次の情報を入力します。

- [Username]：このフィールドにadminと入力します。
- **[パスワード（Password）]**：Cisco Cloud Network Controller 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（Domain）]：[ドメイン（Domain）]フィールドが表示される場合は、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 3 ページの下部にある **[ログイン]** をクリックします。

ステップ 4 [Infrastructure System Configuration]に移動し、[System Configuration]ページの[Management Access]タブをクリックします。 >

ステップ 5 SSH設定を編集するには、画面の右上隅にある鉛筆アイコンをクリックします。

SSH 用の設定ページが表示されます。

ステップ 6 [パスワード 認証ステータス（Password Authentication State] フィールドで、[有効（Enabled）] を選択します。

ステップ 7 **[Save]** をクリックします。

これで、公開キーファイルと秘密キーファイルにアクセスしなくても、Cisco Cloud Network Controller に SSH接続できます。

```
# ssh admin@192.0.2.1
```

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。