



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 \(1 ページ\)](#)
- [Cisco Cloud Network Controller セットアップウィザードの構成の確認 \(9 ページ\)](#)

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](#) 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](#) 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。

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 \(3 ページ\)](#) 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 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。

- **[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。

- **[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 (8 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 (6 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せん。

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

- [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 64512–65534 または 4200000000–4294967294 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。

BGP 自律システム番号は 1 – 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。

(注) 各リージョンで使用される Catalyst 8000V の数を増減させるためにフィールドの値変更する場合、またフィールドの値を変更する前にスマートライセンス サーバーの登録が正しく同期するようオペレーションが完了するまで待ちます。

- Catalyst 8000V の数を減らす場合、フィールドの値をまた変更する前にそれらの Catalyst 8000V が削除されるまで待ちます。
- Catalyst 8000V の数を増やす場合、フィールドの値をまた変更する前にそれらの Catalyst 8000V が展開されるまで待ちます。

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。

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](#)」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](#)」を参照してください。

- (注) プライベート IP アドレスを [16.b \(5 ページ\)](#) 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](#) 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 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)] の各オプションが表示されます。

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、以下のようになります。

- 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 \(9 ページ\)](#)
- [初期構成の完了](#)
 - [外部ネットワークの構成](#)
 - [テナントの作成](#)
 - 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](#) 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](#)
- [SSH を介した Cisco Cloud Network Controller へのログイン](#)

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 \(1 ページ\)](#) 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。

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。