Nexus Dashboard Orchestrator を使用した Google Cloud サイトの管理

初版：2021 年 12 月 17 日

最終更新：2021 年 12 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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)

© 2021 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章 **新機能と更新情報 1**

新機能および変更された機能に関する情報 1

第 2 章 **概要 3**

Google Cloud の概要 3

Google Cloud プロジェクトの重要な情報の検索 3

Cloud APIC を使用した Google Cloud の展開について 4

BGP-EVPN を使用したサイト間接続 6

外部ネットワーク接続 8

ルーティング ポリシーとセキュリティ ポリシーの個別の構成 10

ルーティング ポリシーの設定 10

セキュリティ ポリシーの設定 11

第 3 章 **BGP-EVPN インターサイト接続を構成 17**

インフラの設定: 一般設定 17

クラウド サイト接続性情報の更新 21

インフラの構成：Google クラウド サイトの設定 22

第 4 章 **外部接続の構成 25**

Google Cloud サイト接続ワークフローの構成 25

インフラ テナントでの外部 VRF の作成 26

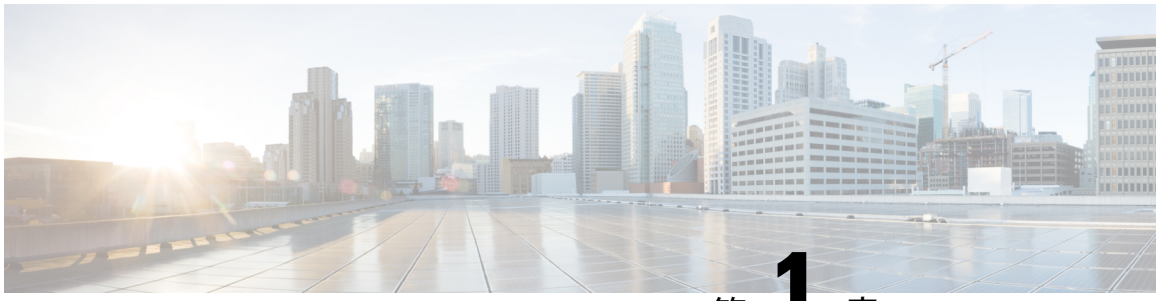
Google Cloud サイトとオンプレミス サイト間のサイト間接続を構成します。 27

外部デバイスの追加 27

Google Cloud サイトとオンプレミス サイト間のサイト間接続の確立 30

外部デバイスへの構成の展開 32
Google Cloud サイトと他のクラウド サイト間のサイト間接続の構成 34
インフラ設定の展開 38
外部 EPG の作成 39
Google Cloud ユーザー テナントのインポート 40
テナントの作成 41
ユーザー テナントの Google Cloud プロジェクトのセットアップ 41
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 44
Google Cloud ユーザー テナントの作成 45
管理対象テナント用に Google Cloud で必要な権限を設定する 48
Cloud EPG の作成 50
Google Cloud サイトのスキーマ、テンプレート、VRF の作成 51
アプリケーション プロファイルと EPG の構成 51
クラウド エンドポイント セレクタの追加 52
外部 EPG とクラウド EPG 間の契約の適用 53
Cloud VRF と外部 VRF 間のルート リークを構成 54

第 5 章 **Google Cloud ワークロードの内部接続を構成 59**
内部接続ワークフロー 59
Google Cloud ユーザー テナントのインポート 59
テナントの作成 61
ユーザー テナントの Google Cloud プロジェクトのセットアップ 61
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 63
Google Cloud ユーザー テナントの作成 64
管理対象テナント用に Google Cloud で必要な権限を設定する 67
Google Cloud サイトのスキーマ、テンプレート、VRF の作成 69
Cloud EPG の作成 70
クラウド EPG 間の契約の適用 71
2 つのクラウド VRF 間のルート リークの構成 71



第 1 章

新機能と更新情報

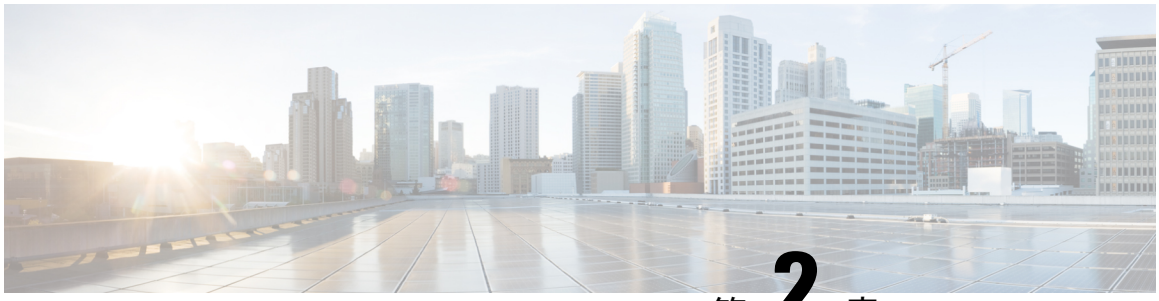
- 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

次の表に、このガイドの最初に発行されたリリースから現在のリリースまでに、このガイドの編成と機能に加えられた大幅な変更の概要を示します。テーブルは、ガイドに加えられたすべての変更のすべてを網羅したリストを提供しているわけではありません。

表 *1*: 最新のアップデート

リリース	新機能またはアップデート	参照先
2022 年 8 月 17 日	Google Cloud サイトの BGP-EVPN サイト間接続。	BGP-EVPN を使用したサイト間接続 （6 ページ）、BGP-EVPN インターサイト接続を構成 （17 ページ）
2021 年 12 月 18 日	このドキュメントの最初のリリース。	--



第 2 章

概要

- Google Cloud の概要 （3 ページ）
- BGP-EVPN を使用したサイト間接続 （6 ページ）
- 外部ネットワーク接続 （8 ページ）
- ルーティング ポリシーとセキュリティ ポリシーの個別の構成 （10 ページ）

Google Cloud の概要

次のセクションでは、Cisco Cloud APIC および Nexus Dashboard Orchestrator に関連する Google Cloud の概念の概要を簡単に説明します。Cloud APIC のデプロイと構成の詳細については、[Cloud APIC のドキュメント（Cloud APIC documentation）]を参照してください。

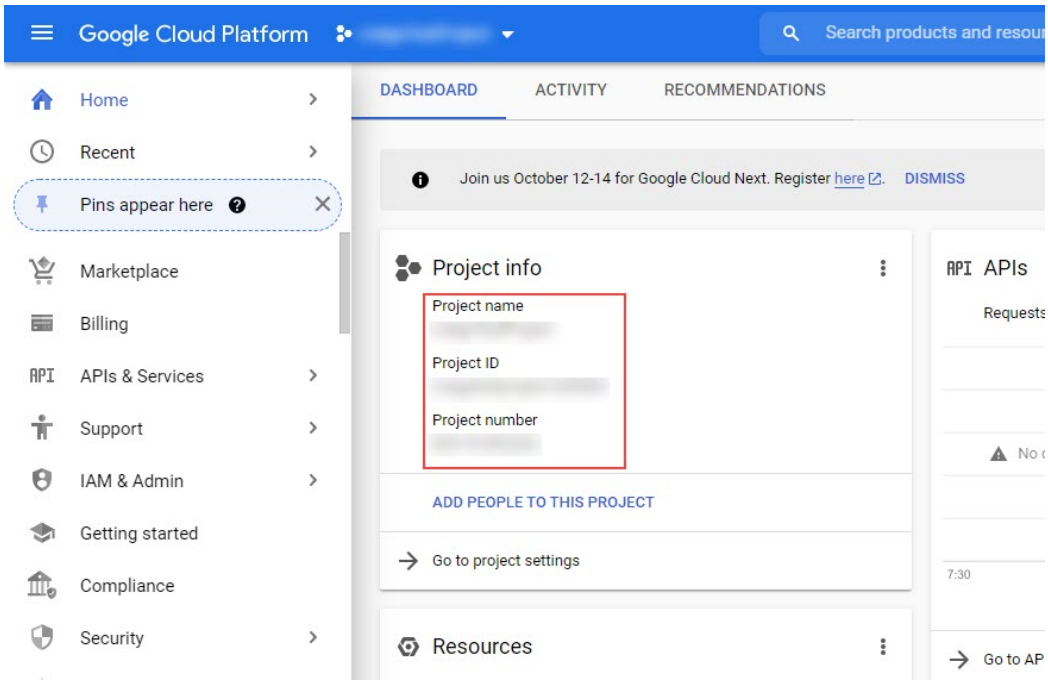
Google Cloud プロジェクトの重要な情報の検索

Google Cloud サイトに新しいテナントを作成する場合は、次の情報が必要です。既存のテナントのみをインポートする予定の場合は、このセクションをスキップできます。

Google Cloud プロジェクトを作成すると、そのプロジェクトには次の 3 つの固有の識別子が割り当てられます。

- プロジェクト名
- プロジェクト ID
- プロジェクト番号

Google Cloud 構成プロセスのさまざまな時点で、Google Cloud プロジェクトにこれら 3 つの識別子が必要になります。これらの Google Cloud プロジェクトIDを含む **[プロジェクト情報（Project Info）]** ペインを見つけるには、Google Cloud アカウントにログインし、**[プロジェクトの選択（Select a Project）]** ウィンドウで特定の Google Cloud プロジェクトを選択します。このプロジェクトの **[ダッシュボード（Dashboard）]** が表示され、[プロジェクト情報（Project Info）] ペインに Google Cloud プロジェクトのこれら3つの一意の識別子が表示されます。



Cloud APIC を使用した 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 テナントが存在することはできません

Cloud APIC を使用すると、Google Cloud は**[サービス アカウント（Service Accounts）]**を使用してプロジェクトへのアクセスを提供します。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、Google Cloud 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（Google Cloud 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。

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ー テナントのテナント設定プロセスの一環として、最初に Nexus Dashboard Orchestrator GUIで **[管理対象アイデンティティ（Managed Identity）]** を選択します。
- Nexus Dashboard Orchestrator で必要なパラメータを構成した後で、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 APIC 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

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。

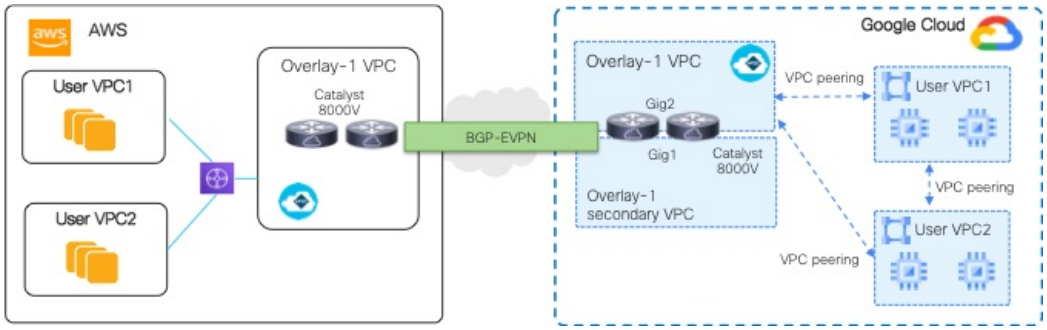
- このテナント アカウントは、Cisco Cloud APIC によって管理されません。
- このタイプのテナントの Cisco Cloud APIC に必要なパラメータを設定する前に、まず、このテナントに関連付けられたサービス アカウントの Google Cloud から必要な秘密キー情報を含む JSON ファイルをダウンロードする必要があります。
- 次に、このタイプのユーザー テナントのテナント設定プロセスの一環として、Nexus Dashboard Orchestrator GUI で **[管理対象外アイデンティティ（Unmanaged Identity）]** を選択します。Nexus Dashboard Orchestrator 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

BGP-EVPN を使用したサイト間接続

Cloud Network Controller リリース 25.0(5) 以降、次のシナリオでサイト間接続用の BGP-EVPN 接続を構成するためのサポートも利用できます。

- クラウド サイトからクラウド サイトへ：
  - Google Cloud サイトから Google Cloud サイトへ
  - Google Cloud サイトから AWS サイトへ
  - Google Cloud サイトから Azure サイトへ
- Google Cloud サイトから AWS サイトへ

これらの各シナリオでは、BGP-EVPN 接続に Cisco Catalyst 8000V が使用されます。



BGP-EVPN を使用したサイト間接続の特性

GCP の動作に基づいて、VM またはインスタンスの各ネットワーク インターフェイスを異なる VPC に関連付ける必要があります。Cisco Catalyst 8000V も VM であるため、これは、特定の Cisco Catalyst 8000V の各ネットワーク インターフェイスを異なる VPC に関連付ける必要があることを意味します。したがって、Cisco Catalyst 8000V の 2 つのギガビット ネットワーク インターフェイスは、次のように使用されます。

- gig1 インターフェイスは、overlay-1 セカンダリ VPC に関連付けられています。また、gig1 インターフェイスは管理インターフェイスとして使用されます。
- gig2 インターフェイスは、overlay-1 VPC に関連付けられています。また、ルーティング インターフェイスとしてgig2 インターフェイスを使用しています。

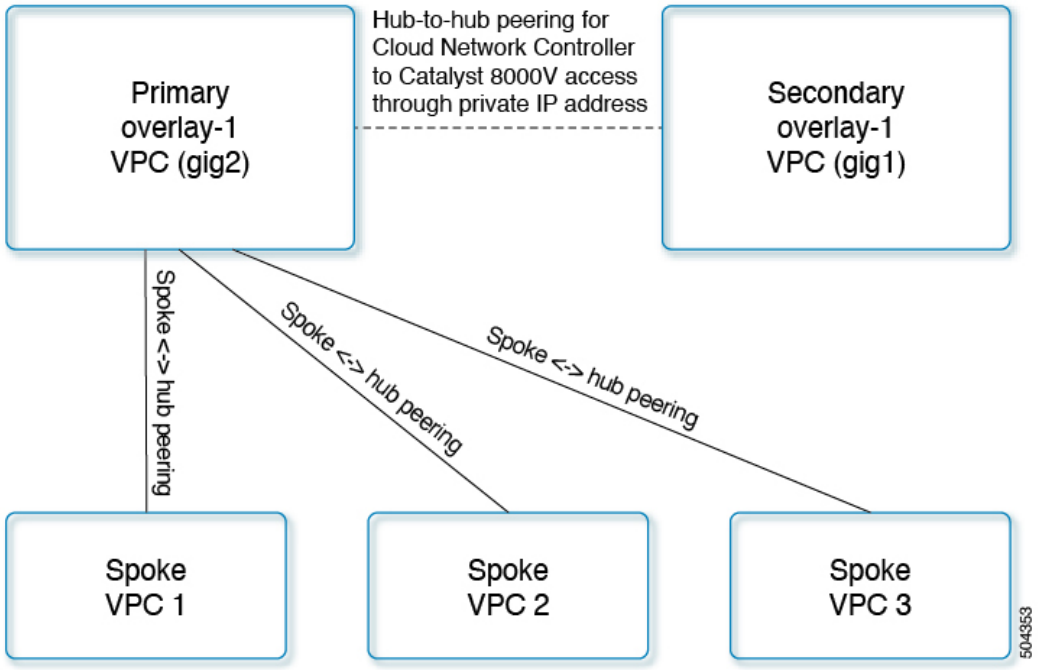
VPC ピアリング

スポーク VPC からオンプレミス ネットワークへの通信を行うには、スポーク VPC でハブ VPC へのピアリングが有効になっている必要があります。ピアリングは、Cisco Cloud Network Controller からの意図によって自動化されます。次の図に示すように、Google Cloud を使用した Cisco Cloud Network Controller の VPC ピアリングは、ハブスポーク トポロジを採用しています。

Google Cloud を備えた Cisco Cloud Network Controller は、次の 3 種類の VPC ピアリングを使用します。

- スポーク間 VPC ピアリング：これは、スポーク間のサイト内通信に使用されます。
- ハブツースポーク VPC ピアリング：これは、BGP-EVPN を使用して Cisco Catalyst 8000V ルーターを経由するサイト間通信に使用されます。
- ハブツーハブ VPC ピアリング：これは、overlay-1 VPC の Cisco Cloud Network Controller と overlay-1 セカンダリ VPC の Cisco Catalyst 8000V ルーター管理インターフェイスとの間の通信に使用されます。

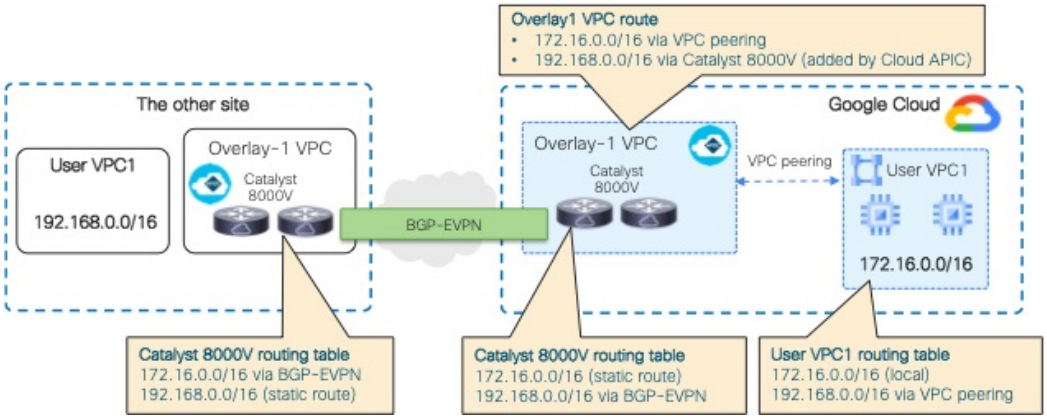
オーバーレイ 1 セカンダリ VPC は、スポーク間またはサイト間トラフィックのデータ パスに関与しないことに注意してください。



Cisco Cloud Network Controller は、次の状況でクラウド サイト間でルートを交換するための構成を自動化します。

- 同じサイト内の接続先へのオーバーレイ 1 VPC：オーバーレイ 1 VPC には、VPC ピアリングを介した同じサイト内のスポーク VPC へのルートがあります。
- 別のサイトの接続先への VPC のスポーク：他のサイトのサブネットのルートは、Cisco Cloud Network Controller によってオーバーレイ 1 VPC に追加され、ルートはスポーク VPC にエクスポートされます。このようにして、スポーク VPC には、他のサイトの接続先サブネットに到達するためのルートがあります。
- 異なるサイトの Cisco Catalyst 8000V 間：スポーク VPC CIDR の静的ルートは、同じサイトの Cisco Catalyst 8000V ルーターに追加されます。静的ルートは、BGP EVPN を介して他のサイトの Catalyst 8000V ルータに再配布されます。このようにして、Catalyst 8000V に

は、次の図に示すように、他のサイトの接続先サブネットに到達するためのルートがあります。



このシナリオでは、リモート CIDR への静的ルートがハブ VPC で、ネクスト ホップが Cisco Catalyst 8000V としてプログラムされています。これらのルートは、ピアリングを使用してスポーク VPC によって学習されます。

外部ネットワーク接続

サポートは、Google Cloudサイトと非 Google Cloud サイトまたは外部デバイス間の外部接続に使用できます。この IPv4 接続を確立するには、Google Cloud ルータと外部デバイス（CSR を含む）の間に VPN 接続を作成します。

次の項では、Cloud APIC リリース 25.0（2）以降で提供される新しい外部ネットワーク接続を可能にするコンポーネントの詳細について説明します。

外部VRF

[外部 VRF（external VRF）] は、クラウド内に存在しない一意の VRF です。このVRFは、Nexus Dashboard Orchestrator によって使用されるクラウド コンテキスト プロファイルでは参照されません。

外部 VRF は、他のクラウド サイトまたはオンプレミス サイトに接続されている外部ネットワークを表します。複数のクラウド VRF は、ルートを外部 VRF にリークしたり、外部 VRF からルートを取得したりする可能性があります。外部 VRF で外部ネットワークが作成されると、VRF 間ルーティングが設定され、外部ネットワークで受信およびアドバタイズされたルートが外部 VRF で受信またはアドバタイズされます。

クラウド ネイティブ ルータ

Google Cloud を使用して Cisco Cloud APIC を構成すると、インフラ VPC は Google Cloud ネイティブ ルータ（クラウド ルータおよびクラウド VPN ゲートウェイ）を使用して、オンプレミス サイト、他のクラウド サイト、または任意のリモート デバイスへの IPsec トンネルと BGP

セッションを作成します。BGP - IPv4 セッションが外部 VRF で作成されているクラウド ネイティブ ルータを使用したこのタイプの接続では、BGP - IPv4 接続のみがサポートされます。

Google Cloud は、スタティック ルートと BGP の両方で VPN 接続をサポートします。BGP との VPN 接続を作成するために、Cisco Cloud APIC はクラウド ルータと VPN ゲートウェイの両方が必要です。VPC は複数のクラウド ルータと VPN ゲートウェイを持つことができます。ただし、Google Cloud には、クラウド ルータと VPN ゲートウェイの両方が同じリージョンおよび同じ VPC に存在する必要があるという制限があります。さらに、Cisco Cloud APIC ではリージョンごとに 1 つのクラウド ルータと 1 つのクラウド VPN ゲートウェイのみがサポートされるという制限があります。

VPN 通信

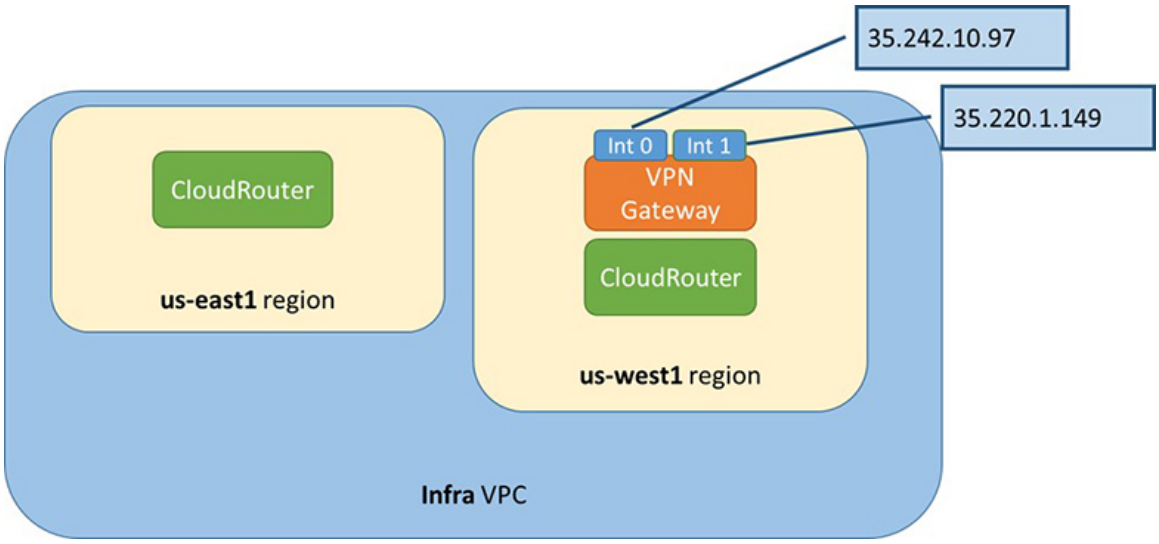
Cisco Cloud APIC を Google Cloud で構成する場合、インフラ VPC を使用して Cisco Cloud APIC をホストし、外部デバイスおよびサイトへの VPN 接続をホストします。ただし、インフラ VPC は、スポーク間通信を実装するための中継として使用されません。代わりに、Cisco Cloud APIC を Google Cloud と使用して構成すると、スポーク間通信はスポーク間 VPC ピアリングによって行われます。

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

- VPN 接続で受信したルートがスポーク VPC にリークされる
- スポーク VPC ルートが VPN 接続でアドバタイズされる

VRF 間ルーティングを使用すると、VPN 接続の外部 VRF とクラウド ローカル スポーク VRF 間でルートがリークされます。

VPN ゲートウェイには 2 つのインターフェイスがあり、Google Cloud は各インターフェイスにパブリック IP アドレスを割り当てます。Google Cloud VPN ゲートウェイは 1 つまたは 2 つのインターフェイスを持つことができますが、ハイアベイラビリティを実現するには 2 つのインターフェイスが必要であるため、Cisco Cloud APIC は 2 つのインターフェイスを持つ VPN ゲートウェイのみをサポートします。



ルーティングポリシーとセキュリティポリシーの個別の構成

異なるVRFの2つのエンドポイント間の通信を許可するには、ルーティングポリシーとセキュリティ ポリシーを別々に確立する必要があります。

- **ルーティング ポリシー**：トラフィック フローを確立するルートを定義するために使用されるポリシー
- **セキュリティ ポリシー**：ゾーン分割ルール、セキュリティ グループ ルール、ACL など、セキュリティ目的で使用されるルール

Google Cloudの場合、ルーティングはセキュリティとは無関係に構成する必要があります。つまり、Google Cloudの場合、「契約」はセキュリティのためだけに使用されます。ルーティングを構成するには、VRF ルート リークを構成する必要があります。

ルーティング ポリシーの設定

VRF 間ルーティングを使用すると、独立したルーティング ポリシーを設定して、VRF のペア間でリークするルートを指定できます。ルーティングを確立するには、VRFのペア間にルートマップを設定する必要があります。

ルート マップを使用して、VRF のペア間でリークするルートを設定できる状況では、VRF 間ルーティングに次のタイプの VRF が使用されます。

- **[外部 VRF（External VRF）]** は、1 つ以上の外部ネットワークに関連付けられている VRF です。

- **内部 VRF** は、1 つ以上のクラウド コンテキスト プロファイルまたはクラウド サブネットが関連付けられているVRFです。

次のタイプの VRF で VRF 間ルーティングを設定する場合：

- 内部 VRF のペア間では、常にすべてのルートをリークする必要があります。
- 内部 VRF から外部 VRF へ、特定のルートまたはすべてのルートをリークできます。
- 外部 VRF から内部 VRF に、すべてのルートをリークする必要があります。

注意事項および制約事項

VRF 間ルーティングを使用してルートマップを使用して VRF ペア間のルートをリークする場合は、次の注意事項が適用されます。

- ルートは常に 2 つの VRF 間で双方向にリークされます。あるテナント/VRF から別のテナント/VRF へのルート リーク エントリごとに、対応するルート リーク エントリが反対方向に存在する必要があります。

  たとえば、2 つのテナント（`t1`と`t2`）と 2 つの対応する VRF（`v1` と`v2`）があるとします。VRF `t2:v2` のすべてのルート リーク エントリ `t1:v1` に対して、VRF `t1:v1` の対応するルート リーク エントリ `t2:v2` が必要です。

- 外部 VRF を外部ネットワークに関連付けた後、外部 VRF を変更する場合は、外部ネットワークを削除してから、新しい外部 VRF で外部ネットワークを再作成する必要があります。
- 「より大きな」プレフィックスがすでにリークされている間に、「より小さな」プレフィックスをリークするように設定することはできません。たとえば、10.10.0.0/16 プレフィックスがすでにリークされるように設定されている場合、10.10.10.0/24 プレフィックスの設定は拒否されます。同様に、0.0.0.0/0（すべてリーク）プレフィックスを設定した場合、他のプレフィックスは設定できません。

セキュリティ ポリシーの設定

Cisco Cloud APIC の EPG は AWS と Azure のセキュリティ グループに対応しますが、EPGに対する Google Cloud の対応コンポーネントはありません。Google Cloud で最も近いものは、ファイアウォール ルールとネットワーク タグの組み合わせです。

Google Cloudのファイアウォール技術情報は、プロジェクト（テナント）に対してグローバルです。ファイアウォール ルールは単一の VPC に関連付けられ、その範囲は VPC 全体にグローバルに適用されます。ファイアウォール ルールの範囲は、Target パラメータによってさらに定義されます。つまり、ルールが適用されるインスタンスのセットは、次の 1 つ以上のターゲット タイプによって選択できます。

- **[ネットワーク タグ**：ネットワークタグは、Google Cloud の VM のファイアウォールとルーティング構成を制御するキー文字列です。インスタンス（VM など）は、一意の文字列でタグ付けできます。ファイアウォール ルールは、等しいタグを持つすべてのインスタンス

に適用されます。複数のタグ値は論理「or」演算子として機能し、少なくとも 1 つのタグが一致する限りファイアウォール ルールが適用されます。

- **ネットワーク内のすべてのインスタンス**：ファイアウォールルールは VPC 内のすべてのインスタンスに適用されます。

ファイアウォール ルールは、トラフィックの送信元と宛先も識別します。ルールが入力トラフィック（VM に向かう）または出力トラフィック（VM を離れる）のどちらであるかによって、送信元フィールドと宛先フィールドの値は異なります。次のリストに、これらの値の詳細を示します。

- **入力ルール**：
  - **ソース**：次を使用して識別できます。
    - ネットワーク タグ
    - IP アドレス
    - 論理「or」演算子を使用した IP アドレスとネットワーク タグの組み合わせ
  - **宛先**：Target パラメータは、宛先インスタンスを識別します。
- **出力ルール**：
  - **送信元**：Target パラメータは、送信元インスタンスを識別します。
  - **宛先**：IP アドレスのみを使用して識別できます（ネットワーク タグは使用できません）。

Cisco Cloud APIC が Google Cloud でファイアウォール ルールを実装する方法

次のリストは、Cisco Cloud APIC の Google Cloud を使用したファイアウォールルールの実装方法を示しています：

- **グローバル 技術情報（Global resources）**：Google Cloud の VPC とファイアウォールはグローバル リソースであるため、Cisco Cloud APIC は複数のリージョンにまたがるエンドポイントのファイアウォールルールをプログラムする必要はありません。エンドポイントが存在するすべてのリージョンに同じファイアウォール ルールが適用されます。
- **ファイアウォール出力ルールとネットワーク タグ**：ファイアウォール出力ルールは、宛先フィールドとしてネットワーク タグをサポートしていないため、エンドポイントの個々の IP アドレスをリストする必要があります。
- **ファイアウォール入力ルールおよびエイリアス IP 範囲の送信元タグ**：ファイアウォール入力ルールには、送信元フィールドで使用されるネットワークタグに一致する VM のエイリアス IP 範囲は含まれません。
- **ファイアウォール ルールの優先度フィールド（Priority fields in firewall rules）**：Google Cloud は優先度の値に従ってファイアウォール ルールを評価します。

Google Cloud ファイアウォール ルールが優先順位リストの後に続く場合、Cisco Cloud APIC は VPC の作成時に、低プライオリティの deny-all 入力ルールと出力ルールのペアを構成します。その後、Cisco Cloud APIC は EPG の優先度の高い契約に従ってトラフィックを開くルールを構成します。したがって、EPGコントラクトの結果として特定のトラフィックを許可する明示的なルールがない場合は、優先順位の低いルールが一致し、デフォルトの動作はdeny-allになります。

エンドポイントおよびエンドポイント セレクタ

Cisco Cloud APIC では、クラウド EPG は、同じセキュリティ ポリシーを共有するエンドポイントの集合です。クラウド EPG は、1 つまたは複数のサブネット内にエンドポイントを持つことができ、VRF に関連付けられます。

Cisco Cloud APIC には、エンドポイントをクラウド EPG に割り当てるために使用される、エンドポイント セレクタと呼ばれる機能があります。エンドポイント セレクタは、基本的に言って、Cisco ACI によって管理される Google Cloud VPC に割り当てられたクラウド インスタンスに対して実行される一連のルールです。エンドポイント インスタンスに一致するエンドポイント セレクタ ルールは、そのエンドポイントをクラウド EPG に割り当てます。エンドポイント セレクタは、 Cisco ACI で使用可能な属性ベースのマイクロ セグメンテーションに似ています。

次に、2 種類のクラウド EPG で使用可能なエンドポイント セレクタのタイプを示します。

- **アプリケーション EPG**：
  - **IP**): IP アドレスまたはサブネットによって選択するために使用されます。
  - **リージョン**: エンドポイントのリージョンで選択するために使用されます。
  - **カスタム**：カスタム タグまたはラベルで選択するために使用されます。たとえば、Google Cloud のロケーション タグを追加する場合、Google Cloud で以前に追加したロケーション タグと一致するこのフィールドにカスタム タグのロケーションを作成できます。
- **外部 EPG**：

  サブネット：サブネット セレクタはエンドポイント セレクタのタイプで、一致表現ではサブネットの IP アドレスが使用されるため、サブネット全体が EPG の一部として割り当てられます。基本的に、サブネット セレクタをエンドポイント セレクタとして使用する場合、そのサブネット内のすべてのエンドポイントは関連付けられたEPGに属します。

Google Cloud で Cisco Cloud APIC エンドポイント セレクタを使用する場合、Google Cloud の一致する VM に EPG を関連付けるネットワーク タグが適用されます。ネットワーク タグが VM で設定されると、Google Cloud は VM のトラフィックにファイアウォール ルールが適用されます。

Google Cloud 上の VM もラベルをサポートします。ラベルは、組織的なツールとなるキーと値のペアです。Cisco Cloud APIC のカスタムエンドポイントセレクタは、 Google Cloud の VM に割り当てられたラベルを認識します。

Cisco Cloud APIC は、EPG ごとに一意のネットワーク タグ文字列を予約します。Google Cloud では、この値が EPG 用に作成されたファイアウォール ルールのターゲット フィールドとして使用されます。新しい VM が EPG のエンドポイント セレクタに一致すると、Cisco Cloud APIC はこの値を既存の VM のネットワーク タグに追加します。さらに、EPG のネットワークタグは、Google Cloud ファイアウォール ルールの送信元フィールドで使用されます。

次の設定の VPC に 3 つのエンドポイントがあると仮定すると、Cisco Cloud APIC は次のネットワーク タグを構成します。Cisco Cloud APIC-configured ネットワーク タグは次のフォーマットです。

`capic-<app-profile-name>-<epg-name>`

エンドポイント	アプリケーション プロファイル	EPG	Primary IP	ラベル	クラウド APIC で設定されたネットワーク タグ
EP1	最初のアプリケーション プロファイル（app01）	最初の EPG（epg01）	10.0.0.1	server:web	capic-app01-epg01
EP2	2 番目のアプリケーション プロファイル（app02）	2 番目の EPG（epg02）	20.0.0.1	server:backend	capic-app02-epg02
EP3	2 番目のアプリケーション プロファイル（app02）	3 番目の EPG（epg03）	30.0.0.1	server:database	capic-app02-epg03

Cisco Cloud APIC がネットワーク タグを設定するには、VMに対する管理者権限が必要です。この権限は、コンピューティング インスタンス管理者ロールによって付与されます。

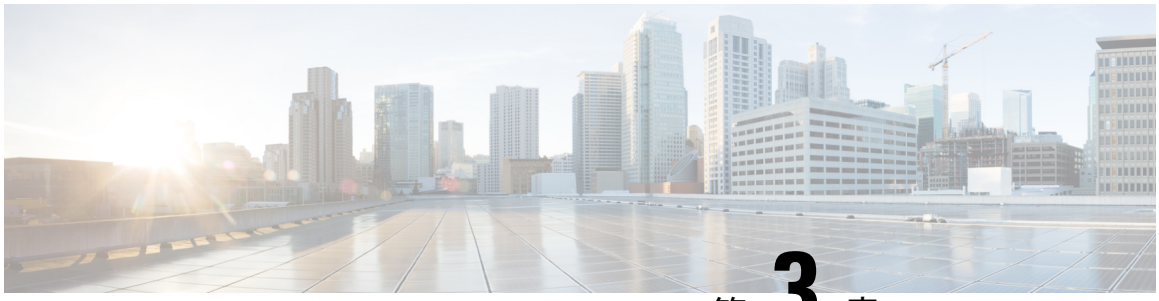
Cisco Cloud APIC にこの権限がなく、VM のタグを管理できない場合があります。これらのシナリオでは、最初にVMでネットワークタグを設定し、その後で Cisco Cloud APIC に適切なエンドポイント セレクタ設定を指定できます。

ファイアウォール ルールを確認するには：

- **Google Cloud の場合**： Google Cloud アカウントで、**[VPC ネットワーク（VPC Network）]** > **[ファイアウォール（Firewall）]**に移動します。
  - VM が EPG の一部である場合は、ファイアウォール ルールを展開し、**[フィルタ（Filters）]** 列に表示される複数のエントリを表示することで、エンドポイントを検索できます。
  - **[タイプ（Type）]** 列のエントリを使用して、特定のファイアウォール ルールが入力ファイアウォール ルールか出力ファイアウォール ルールかを判別します。

- ファイアウォールルールが入力タイプの場合、トラフィックはこれらのエンドポイントに送信されます。
- ファイアウォールルールが出力タイプの場合、これらのエントリはトラフィックを受信できる場所を示します。

- **Cisco Cloud APIC の場合**：ファイアウォール ルールは VPC に関連付けられているため、**[クラウド リソース（Cloud Resources）]** > **[VPC]**に移動し、VPC をダブルクリックして詳細画面を表示します。次に、**[クラウド リソース（Cloud Resources）]** タブをクリックします。入力ルールと出力ルールが表示されます。



第 3 章

BGP-EVPN インターサイト接続を構成

- インフラの設定: 一般設定 （17 ページ）
- クラウド サイト接続性情報の更新 （21 ページ）
- インフラの構成：Google クラウド サイトの設定 （22 ページ）

インフラの設定: 一般設定

ここでは、すべてのサイトの一般的なインフラ設定を構成する方法について説明します。

（注） 次の設定には、すべてのサイトに適用されるものと、特定のタイプのサイト（Cloud Network Controller サイトなど）に必要なものとがあります。各サイト固有のサイト ローカル設定に進む前に、インフラ一般設定で必要なすべての設定を完了していることを確認します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインにある **[構成（Configure）]** をクリックします。

ステップ 4 左側のサイドバーで、**[全般設定（General Settings）]**を選択します。

ステップ 5 **[コントロール プレーン設定（Control Plane Configuration）]** を指定します。

a) **[コントロール プレーン設定（Control Plane Configuration）]** タブを選択します。

b) **[BGP ピアリング タイプ（Bgp Peering Type）]** を選択します。

- `full-mesh`：各サイトのすべてのボーダー ゲートウェイ スイッチは、リモート サイトのボーダー ゲートウェイ スイッチとのピア接続を確立します。

  `full-mesh` 構成では、Nexus Dashboard Orchestrator は ACI 管理ファブリックのスパイン スイッチと NDFC 管理ファブリックのボーダー ゲートウェイを使用します。

- `[route-reflector]`：route-reflector オプションを使用すると、各サイトが MP-BGP EVPN セッションを確立する 1 つ以上のコントロール プレーン ノードを指定できます。ルート リフレクタ ノー

ドを使用すると、NDO によって管理されるすべてのサイト間で MP-BGP EVPN フル メッシュ隣接関係が作成されなくなります。

ACIファブリックの場合、`[route-reflector]` オプションは、同じ BGP ASN の一部であるファブリックに対してのみ有効です。

c) **[キープアライブ間隔 (秒) (Keepalive Interval (Seconds))]** フィールドに、キープアライブ間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

d) **[保留間隔 (秒) (Hold Interval (Seconds))]** フィールドに、保留間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

e) **[失効間隔 (秒) (Stale Interval (Seconds))]** フィールドに、失効間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

f) **[グレースフル ヘルパー (Graceful Helper)]** オプションをオンにするかどうかを選択します。

g) **[AS 上限（Maximum AS Limit）]**を入力します。

デフォルト値を維持することを推奨します。

h) **[ピア間のBGP TTL（BGP TTL Between Peers）]** を入力します。

デフォルト値を維持することを推奨します。

i) **[OSPF エリア ID (OSPF Area ID)]** を入力します。

Cloud Network Controller サイトがない場合、このフィールドは UI に表示されません。

これは、オンプレミス IPN ピアリングのためにクラウド サイトで使用される OSPF エリア ID です。

j) (オプション) CloudSec 暗号化の **[IANA 割り当てポート（IANA Assigned Port）]**を有効にします。

デフォルトでは、CloudSec は独自の UDP ポートを使用します。このオプションを使用すると、サイト間の CloudSec 暗号化に公式の IANA 予約ポート 8017 を使用するように CloudSec を構成できます。

（注） IANA 予約ポートは、リリース 5.2(4) 以降を実行している Cisco APIC サイトでサポートされています。

この設定を変更するには、すべてのサイトで CloudSec を無効にする必要があります。IANA 予約ポートを有効にしたいが、すでに 1 つ以上のサイトで CloudSec 暗号化を有効にしている場合は、すべてのサイトで CloudSec を無効にし、[IANA 予約 UDP ポート（IANA Reserve UDP Port）] オプションを有効にしてから、必要なサイトで CloudSec を再度有効にします。

CloudSec を構成するための詳細情報と手順については、*『ACI ファブリック用のNexus Dashboard Orchestrator 構成ガイド（Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics）』*の「CloudSec 暗号化」の章を参照してください。

ステップ 6 **[IPN デバイス情報]** を入力します。

オンプレミスとクラウドサイト間のサイト間接続を設定する予定がない場合は、この手順をスキップできます。

後のセクションで説明するように、オンプレミスとクラウドサイト間のサイトアンダーレイ接続を設定する場合は、クラウドCSRへの接続を確立するオンプレミスIPNデバイスを選択する必要があります。これらのIPNデバイスは、オンプレミスのサイト設定画面で使用可能になる前に、ここで定義する必要があります。

a) **[オンプレミス IPSec デバイス（On Premises IPSec Devices）]** タブを選択します。
b) **[+オンプレミス IPSec デバイスを追加（+Add On-Premises IPSec Device）]** をクリックします。
c) デバイスが**[管理対象外（Unmanaged）]**か**[管理対象（Managed）]**かを選択し、デバイス情報を提供します。

これは、デバイスがNDFCによって直接管理されるかどうかを定義します。

- **[管理対象（Managed）]** IPNデバイスにはシンプルにデバイスの**[名前（Name）]** と **[IP アドレス（IP Address）]** を入力してください。

  指定したIPアドレスは、IPNデバイスの管理IPアドレスではなく、クラウドCSRからのトンネル ピア アドレスとして使用されます。

- **[管理対象（Managed）]** IPNデバイスには、デバイスが入っているNDFC **[サイト（Site）]** を選択し、そのサイトの **[デバイス（Device）]** を選択します。

  次に、インターネットに接続しているデバイスの**[インターフェイス（Interface）]**を選択し、インターネットに接続しているゲートウェイのIPアドレスである**[ネクスト ホップ（Next Hop）]** IPアドレスを指定します。

d) チェック マーク アイコンをクリックして、デバイス情報を保存します。
e) 追加するIPNデバイスについて、この手順を繰り返します。

ステップ 7 **[外部 デバイス（External Devices）]** 情報を入力します。

Cloud Network Controllerサイトがない場合、このタブはUIに表示されません。

Multi-Site ドメインに Cloud Network Controller サイトがない場合、またはクラウド サイトとブランチ ルータまたはその他の外部デバイス間の接続を設定する予定がない場合は、この手順をスキップできます。

次の手順では、クラウドサイトからの接続を設定するブランチルータまたは外部デバイスに関する情報を指定する方法について説明します。

a) **[外部デバイス（External Devices）]** タブを選択します。

このタブは、Multi-Site ドメインに少なくとも 1 つのクラウドサイトがある場合にのみ使用できます。

b) **[外部デバイスの追加（Add External Device）]** をクリックします。

[外部デバイスの追加（Add External Device）] ダイアログが開きます。

c) デバイスの **[名前（Name）]**、**[IP アドレス（IP Address）]**、および **[BGP 自律システム番号（BGP Autonomous System Number）]** を入力します。

指定したIPアドレスは、デバイスの管理IPアドレスではなく、Cloud Network Controller の CSR からのトンネル ピア アドレスとして使用されます。接続は、IPSec を使用してパブリック インターネット経由で確立されます。

d) チェック マーク アイコンをクリックして、デバイス情報を保存します。

e) 追加する IPN デバイスについて、この手順を繰り返します。

すべての外部デバイスを追加したら、次の手順を完了して、IPSec トンネル サブネット プールにこれらのトンネルに割り当てられる内部 IP アドレスを指定します。

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

Cloud Network Controller サイトがない場合、このタブは UI に表示されません。

ここで指定できるサブネットプールには、次の 2 つのタイプがあります。

- **外部サブネット プール**：クラウド サイトの CSR と他のサイト（クラウドまたはオンプレミス）間の接続に使用されます。

  これらは、Nexus Dashboard Orchestrator によって管理される大規模なグローバル サブネット プールです。Orchestrator は、これらのプールからより小さなサブネットを作成し、サイト間 IPsec トンネルと外部接続 IPsec トンネルで使用するサイトに割り当てます。

  1 つ以上のクラウド サイトから外部接続を有効にする場合は、少なくとも 1 つの外部サブネット プールを提供する必要があります。

- **サイト固有のサブネット プール**：クラウド サイトの CSR と外部デバイス間の接続に使用されます。

  これらのサブネットは、外部接続 IPsec トンネルが特定の範囲内にあることが必要な場合に定義できます。たとえば、外部ルータに IP アドレスを割り当てるために特定のサブネットがすでに使用されており、それらのサブネットを NDO およびクラウド サイトの IPsec トンネルで引き続き使用する場合です。これらのサブネットは Orchestrator によって管理されず、各サブネットはサイト全体に割り当てられ、外部接続 IPsec トンネルにローカルで使用されます。

  名前付きサブネット プールを指定しない場合でも、クラウド サイトの CSR と外部デバイス間の接続を設定すると、外部サブネット プールが IP 割り当てに使用されます。.

（注） 両方のサブネット プールの最小マスク長は `/24` です。

1 つ以上の**外部サブネット プール**を追加するには：

a) **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** タブを選択します。
b) **[外部サブネット プール（External Subnet Pool）]** エリアで、**[+ IP アドレスの追加（+Add IP Address）]** をクリックして、1 つ以上の外部サブネット プールを追加します。

   このサブネットは、以前の Nexus Dashboard Orchestrator リリースでサイト間接続用に Cloud Network Controller で以前に設定した、オンプレミス接続に使用されるクラウド ルータの IPsec トンネル インターフェイスとループバックに対処するために使用されます。

   サブネットは、他のオンプレミス TEP プールと重複してはならず、`0.xxx` または `0.0.xx`で 始まってはならず、`/16` と `/24` の間のネットワーク マスク（`30.29.0.0/16` など）が必要です。

c) チェックマーク アイコンをクリックして、サブネット情報を保存します。
d) 追加するサブネット プールについて、これらのサブステップを繰り返します。

1 つ以上の **[サイト固有のサブネット プール（Site-Specific Subnet Pools）]** を追加するには：

a) **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** タブを選択します。

b) **[サイト固有のサブネット プール（Site-Specific Subnet Pools）]** エリアで、**[+ IP アドレスの追加（+Add IP Address）]** をクリックして、1 つ以上の外部サブネット プールを追加します。

[名前付きサブネットプールの追加（Add Named Subnet Pool）] ダイアログが開きます。

c) サブネットの **[名前（Name）]** を入力します。

後ほど、サブネットプールの名前を使用して、IP アドレスを割り当てるプールを選択できます。

d) **[+ IP アドレスの追加 (+ Add IP Address)]** をクリックして、1 つ以上のサブネット プールを追加します。

サブネットには `/16` と `/24` の間のネットワークが必要で、`0.x.x.x` または `0.0.x.x` で始めることはできません。たとえば、`30.29.0.0/16` のようにします。

e) チェックマーク アイコンをクリックして、サブネット情報を保存します。

同じ名前付きサブネット プールに複数のサブネットを追加する場合は、この手順を繰り返します。

f) **[保存（Save）]** をクリックして、名前付きサブネット プールを保存します。

g) 追加する名前付きサブネット プールについて、これらのサブステップを繰り返します。

次のタスク

全般的なインフラ設定を構成した後も、管理するサイトのタイプ（ACI、Cloud Network Controller、またはNDFC）に基づいて、サイト固有の設定に関する追加情報を指定する必要があります。次の項で説明する手順に従って、サイト固有のインフラストラクチャ設定を行います。

クラウド サイト接続性情報の更新

CSRやリージョンの追加や削除などのインフラストラクチャの変更には、Multi-Site ファブリック接続サイトの更新が必要です。このセクションでは、各サイトのコントローラから直接最新の接続性情報を取得する方法を説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]** を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のサイトを選択します。

ステップ 5 メインウィンドウで **[更新 (Refresh)]** ボタンをクリックして、新規または変更されたCSRおよびリージョンを検出します。

ステップ 6 最後に、**[はい (Yes)]** をクリックして確認し、接続情報をロードします。

これにより、新規または削除された CSR およびリージョンが検出されます。

ステップ 7 **[導入 (Deploy)]** をクリックして、クラウドサイトの変更を、接続している他のサイトに伝達します。

クラウドサイトの接続を更新し、CSR またはリージョンが追加または削除された後、インフラ設定を展開して、そのクラウドサイトへのアンダーレイ接続がある他のサイトが更新された設定を取得する必要があります。

インフラの構成：Google クラウド サイトの設定

ここでは、Cloud Network Controller サイト固有のインフラ設定を構成する方法について説明します。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインの右上にある **[構成（Configure）]** をクリックします。

ステップ 4 左側のペインの **[サイト (Sites)]** の下で、特定のクラウド サイトを選択します。

ステップ 5 **[サイト間接続（Inter-Site Connectivity）]** 情報を入力します。

a) 右側の ***[<Site>* 設定 (Settings)]** ペインで、**[サイト間接続 (Inter-Site Connectivity)]** タブを選択します。

b) **[マルチサイト（Multi-Site）]** ノブを有効にします。

これは、オーバーレイ接続がこのサイトと他のサイト間で確立されるかどうかを定義します。

オーバーレイ構成は、次の手順で説明するようにアンダーレイ サイト間接続が確立されていないサイトにはプッシュされないことに注意してください。

ステップ 6 サイト固有の **[サイト間接続 (Inter-Site Connectivity)]** 情報を入力します。

a) **[コントラクトベースのルーティング（Contract Based Routing）]** オプションを有効にする。

b) クラウド サイトの右側のプロパティ サイドバーで、**[サイトの追加（Add Site）]** をクリックします。

[サイトの追加（Add Site）] ウィンドウが表示されます。

c) [サイトへの接続（Connected to Site）] で、[サイトの選択（Select a Site）] をクリックし、構成しているサイト（たとえば、Site1）からの接続を確立するサイト（たとえば、Site2）を選択します。

リモート サイトを選択すると、[サイトの追加（Add Site）] ウィンドウが更新され、両方向の接続が反映されます：[サイト1（Site1）] > [サイト2（Site2）] および [サイト2（Site2）] > [サイト1（Site1）]。

d) [サイト1（Site1）] > [サイト2（Site2）] エリアで、[接続タイプ（Connection Type）] ドロップダウンから、サイト間の接続のタイプを選択します。

次のオプションを使用できます。

- `[パブリックインターネット (Public Internet)]`：2 つのサイト間の接続は、インターネットを介して確立されます。

  このタイプは、任意の 2 つのクラウド サイト間、またはクラウド サイトとオンプレミス サイト間でサポートされます。

- [プライベート接続 (Private Connection)]：2 つのサイト間のプライベート接続を使用して接続が確立されます。

  このタイプは、クラウド サイトとオンプレミス サイトの間でサポートされます。

- [クラウド バックボーン (Cloud Backbone)]：クラウドバックボーンを使用して接続が確立されます。

  このタイプは、Azure-to-Azure、AWS-to-AWS、GCP-to-GCP など同じタイプの 2 つのクラウド サイト間でサポートされます。

複数のタイプのサイト（オンプレミス、AWS、AzureとGCP）がある場合、サイトの異なるペアは異なる接続タイプを使用できます。

e) これら 2 つのサイト間の接続に使用する [プロトコル（Protocol）] を選択します。

このユース ケースでは、**BGP-EVPN** を使用します。オプションで **IPSec** を有効にして、使用するインターネット キー エクスチェンジ（IKE）プロトコルのバージョン（構成に応じて IKEv1（[バージョン 1（Version 1）]）または IKEv2（[バージョン 1（Version 1）]））を選択できます。

- パブリック インターネット接続の場合、IPsec は常に有効です。
- クラウド バックボーン接続の場合、IPsec は常に無効です。
- プライベート接続の場合、IPsec は有効または無効にすることができます。

代わりに [BGP-IPv4] 接続を使用する場合は、構成しているクラウドサイトからのルート リーク構成に使用される外部 VRF を提供する必要があります。

[サイト1（Site1）] > [サイト2（Site2）] の接続情報が提供された後、[サイト2（Site2）] > [サイト1（Site1）] 領域は、反対方向の接続情報を反映します。

f) **[保存 (Save)]** をクリックして、設定を保存します。

Site1 から Site2 への接続情報を保存すると、Site2 から Site1 へのリバース接続が自動的に作成されます。これは、他のサイトを選択し、右側のサイドバーにある **[サイト間接続（Inter-site Connectivity）]** 情報を選択することで確認できます。

g) 他のサイトのサイト間接続を追加するには、この手順を繰り返します。

Site1 から Site2 へのアンダーレイ接続を確立すると、リバース接続が自動的に行われます。

ただし、Site1 から Site3 へのサイト間接続も確立する場合は、そのサイトに対してもこの手順を繰り返す必要があります。

ステップ 7 **[外部接続 (External Connectivity)]** 情報を入力します。

NDOによって管理されていない外部サイトまたはデバイスへの接続を設定する予定がない場合は、この手順をスキップできます。

外部接続の使用例の詳細な説明は、『Nexus Dashboard Orchestrator を使用したクラウド CSR からの外部接続の構成』ドキュメントで入手できます。

a) 右側の ***[<Site> 設定 (Settings)]*** ペインで、**[外部接続 (External Connectivity)]** タブを選択します。
b) **[外部接続の追加 (Add External Connectivity)]** をクリックします。

[外部接続の追加 (Add External Connectivity)] ダイアログが開きます。

c) **[VRF]** ドロップダウンから、外部接続に使用する VRF を選択します。

これは、クラウド ルートをリークするために使用される VRF です。**[リージョン (Regions)]** セクションには、この設定を適用する CSR を含むクラウド リージョンが表示されます。

d) **[外部デバイス (External Devices)]** セクションの **[名前 (Name)]** ドロップダウンから、外部デバイスを選択します。

これは、一般的なインフラストラクチャ設定時に**[一般設定 (General Settings)]** > **[外部デバイス (External Devices)]** リストに追加した外部デバイスであり、インフラの設定: 一般設定 （17 ページ）の説明に従ってすでに定義されている必要があります。

e) **[トンネル IKE バージョン (Tunnel IKE Version)]** ドロップダウンから、クラウド サイトの CSR と外部デバイス間の IPSec トンネルの確立に使用する IKE バージョンを選択します。

f) （任意）**[トンネル サブネット プール (Tunnel Subnet Pool)]** ドロップダウンから、名前付きサブネット プールのいずれかを選択します。

名前付きサブネット プールは、クラウド サイトの CSR と外部デバイス間の IPSec トンネルに IP アドレスを割り当てるために使用されます。ここで**名前付き**サブネット プールを指定しない場合、**外部**サブネット プールが IP 割り当てに使用されます。

外部デバイス接続用の専用サブネット プールを提供することは、特定のサブネットがすでに外部ルータに IP アドレスを割り当てるために使用されており、それらのサブネットを NDO およびクラウド サイトのIPSecトンネルに引き続き使用する場合に役立ちます。

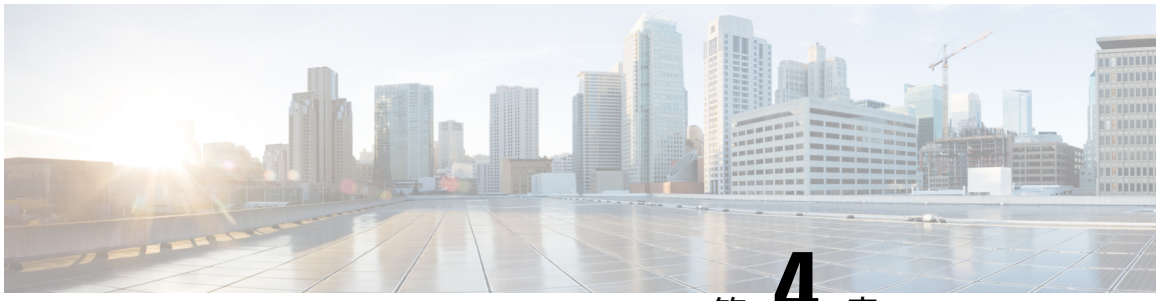
この接続に特定のサブネット プールを提供する場合は、インフラの設定: 一般設定 （17 ページ）の説明に従って作成済みである必要があります。

g) （オプション）**[事前共有キー (Pre-Shared Key)]** フィールドに、トンネルの確立に使用するカスタム キーを入力します。

h) 必要に応じて、同じ外部接続（同じ VRF ）に対して追加する外部デバイスについて、前のサブステップを繰り返します。

i) 必要に応じて、追加の外部接続（異なる VRF ）に対してこの手順を繰り返します。

CSR と外部デバイス間のトンネルエンドポイントには 1 対 1 の関係があるため、異なる VRF を使用して追加の外部接続を作成できますが、同じ外部デバイスに追加の接続を作成することはできません。



第 4 章

外部接続の構成

- Google Cloud サイト接続ワークフローの構成 （25 ページ）
- インフラ テナントでの外部 VRF の作成 （26 ページ）
- Google Cloud サイトとオンプレミス サイト間のサイト間接続を構成します。 （27 ページ）
- Google Cloud サイトと他のクラウド サイト間のサイト間接続の構成 （34 ページ）
- インフラ設定の展開 （38 ページ）
- 外部 EPG の作成 （39 ページ）
- Google Cloud ユーザー テナントのインポート （40 ページ）
- テナントの作成 （41 ページ）
- Cloud EPG の作成 （50 ページ）
- 外部 EPG とクラウド EPG 間の契約の適用 （53 ページ）
- Cloud VRF と外部 VRF 間のルート リークを構成 （54 ページ）

Google Cloud サイト接続ワークフローの構成

以下のセクションでは、GCP サイトのインフラストラクチャ、サイト間接続、および簡単な展開の使用例を構成する方法について説明します。ワークフローには次のものが含まれます。

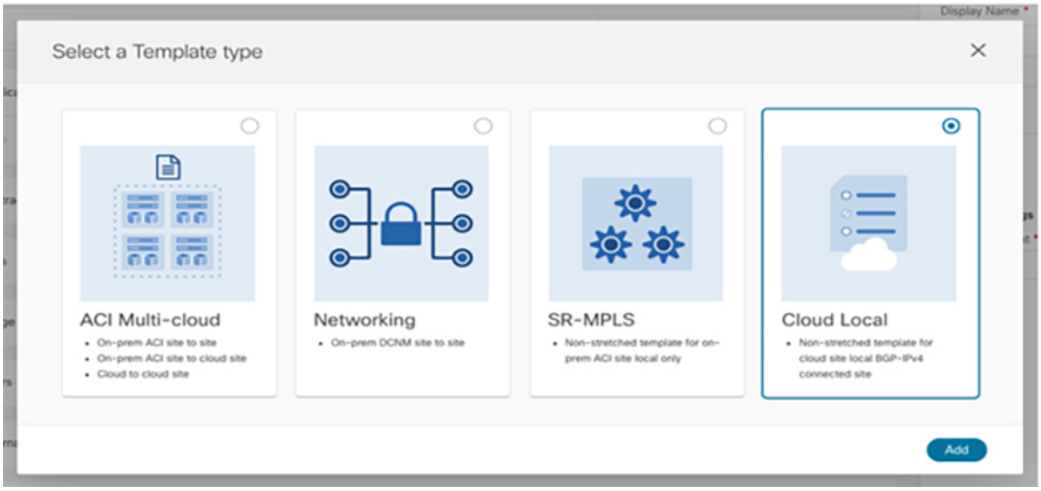
- オンプレミスの IPN デバイスを Nexus Dashboard Orchestrator で外部デバイスとして追加し、Google クラウド サイトからそれらのデバイスへの外部接続を確立するなど、一般的なインフラ設定を構成します。
- Google Cloud サイトのインフラ テナントでの外部 VRF の構成と展開
- Google Cloud サイトからオンプレミス サイトへのサイト間接続の構成とオンプレミス サイトから Google Cloud サイトへの接続の手動構成
- Google Cloud サイトと AWS/Azure などの他のクラウド サイト間のサイト間接続の構成
- サイト間のルーティングを有効にするための外部 VRF でのルート リークの構成
- ユーザー テナントと EPG の作成またはインポート、およびサイト間の通信を可能にするための契約の適用

インフラ テナントでの外部 VRF の作成

マルチサイト ドメイン内のすべてのクラウド サイトの外部 VRF を定義する単一のスキーマを作成できます。ただし、クラウド サイトごとに異なる VRF を展開する場合があるため、異なるクラウド サイト間でテンプレートを共有することはできないため、所有するクラウド サイトごとに個別のテンプレートを作成する必要があります。

次のセクションでは、新しいタイプのテンプレートを紹介し、外部 VRF を追加するプロセスについて説明します。スキーマで、Google Cloud サイトの新しいテンプレートを作成し、クラウドローカルテンプレートを使用して、テンプレートを Google Cloud サイトに割り当てます。

クラウド ローカルと呼ばれる新しいタイプのテンプレートを選択できます。



このタイプのテンプレートは、複数のサイトに拡張できません。すべてのタイプのクラウドサイトをサポートし、許可します。ただし、このテンプレートに添付できるサイトは1つだけです。このテンプレートには、VRF などのように、一部のオブジェクトがテナント内からのみである必要があるという別の制限があります。

次のセクションでは、外部デバイスのサブネットへの接続を確立するために使用される外部 VRF を作成する方法について説明します。指定されている手順に従って、外部 VRF をクラウド サイトにプロビジョニングできます。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 **メイン メニュー**で、**[Application Management (アプリケーション管理)]** > **[スキーマ (Schemas)]** を選択します。

ステップ 3 新しいスキーマとテンプレートを作成するか、外部 VRF 定義を含むインフラ テナントに関連付けられたテンプレートを展開する既存のスキーマを選択します。

このユース ケース専用の別個のスキーマを作成できます。ここでは、インフラ テナントに関連付けられ、外部デバイスへの接続を提供する外部 VRF を含むすべてのテンプレートを定義します。

外部 VRF テンプレートを作成する場合：

- さまざまなタイプのクラウド サイト（AWS、Azure、または Google Cloud）に個別のテンプレートを使用する必要があります。
- **Cloud Local** テンプレート タイプを選択する必要があります。
- テンプレートをインフラテナントにマッピングする必要があります。そうしないと、VRF は外部接続に使用できません。
- 両方のテンプレートで同じ VRF 名を使用できます。このドキュメントの例では、`extVrf1` を使用します。

ステップ 4 メインペインで、**[+ オブジェクトの作成 (+Create Object)]** > **[VRF]**を選択します。

ステップ 5 VRF の **[表示名（Display Name）]** を入力します。

他のすべてのオプションはデフォルト値のままにすることができます。

（注） VRF のサイト ローカル プロパティでは、この VRF をリージョンに付加しないでください。インフラ テナントで作成され、どのリージョンにも接続されていない VRF は、外部 VRF として扱われ、この使用例に使用できます。

ステップ 6 外部 VRF を含むテンプレートを、外部接続を確立する 1 つ以上のクラウド サイトに割り当てます。

テンプレートは、1 つのタイプのクラウドサイト（AWS、Azure、または Google Cloud）にのみ割り当てる必要があることに注意してください。

ステップ 7 テンプレートを展開して、クラウド サイトに外部 VRF を作成します。

Google Cloud サイトとオンプレミス サイト間のサイト間接続を構成します。

以下のセクションでは、GCP サイトとオンプレミス サイト間の接続を構成する方法について説明します。2 つのクラウド サイト間の接続を構成する場合は、Google Cloud サイトと他のクラウド サイト間のサイト間接続の構成 （34 ページ） を参照してください。

外部デバイスの追加

Google Cloud サイトとオンプレミス サイトの間にサイト間接続を確立する予定がない場合は、このセクションをスキップできます。このセクションでは、Orchestrator の **[サイトの接続（Site Connectivity）]** ページで、外部デバイスに関する情報を Nexus Dashboard Orchestrator に提供する方法について説明します。

（注） 次の手順では、この特定の使用例に必要な構成に焦点を当てています。すべてのインフラ構成設定に関する詳細情報は、『*Cisco Nexus Dashboard Orchestrator* 構成ガイド』で入手できます。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左のナビゲーションメニューから 、**[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**を選択します。

ステップ 3 メイン ペインにある **[構成（Configure）]** をクリックします。

ステップ 4 左側のサイドバーで、**[全般設定（General Settings）]**を選択します。

ステップ 5 **[外部 デバイス（External Devices）]** 情報を入力します。

この手順では、クラウドサイトからの接続を構成する外部デバイスに関する情報を提供する方法について説明します。このプロセスの詳細については、「一般的なインフラ設定の構成」を参照してください。

a) **[外部デバイス（External Devices）]** タブを選択します。

b) **[外部デバイスの追加（Add External Device）]** をクリックします。

[外部デバイスの追加（Add External Device）] ダイアログが開きます。

c) デバイスの **[名前（Name）]**、**[IP アドレス（IP Address）]**、および **[BGP 自律システム番号（BGP Autonomous System Number）]** を入力します。

指定した IP アドレスは、デバイスの管理 IP アドレスではなく、クラウド APIC の CSR または Google Cloud ネイティブ ルータの VPN ゲートウェイ のピア アドレスとして使用されます。接続は、IPSec を使用してパブリック インターネット経由で確立されます。

d) **[保存（Save）]** をクリックして、デバイス情報を保存します。

e) 加える追加の外部デバイスについて、この手順を繰り返します。

ステップ 6 **[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。

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Google クラウドとその他のクラウドサイト（AWS/Azure）の間に作成されます。必要に応じて、既存のサブネット プールを削除し、サブネットプールを追加できます。**IPSec トンネル サブネット プール** エントリに使用されるサブネットは、`169.254.0.0/16` ブロックの共通 /30 CIDR である必要があります。たとえば、`169.254.7.0/24` と `169.254.8.0/24` は、このフィールドのサブネットプールの許容エントリです。適切なサブネット プールを入力したら、チェックマークをクリックします。

次のサブネットは予約されており、どのトンネルにも使用できません。

- `169.254.0.0/30`
- `169.254.1.0/30`
- `169.254.2.0/30`
- `169.254.3.0/30`

- 169.254.4.0/30
- 169.254.5.0/30
- 169.254.112.0/24
- 169.254.113.0/24
- 169.254.114.0/24
- 169.254.169.252/30

ここで指定できるサブネットプールには、次の 2 つのタイプがあります。

- **外部サブネット プール**：クラウドサイトのルータと他のサイト（クラウドまたはオンプレミス）間の接続に使用されます。

  これらは、Nexus Dashboard Orchestrator によって管理される大規模なグローバル サブネット プールです。Orchestrator は、これらのプールからより小さなサブネットを作成し、サイト間 IPsec トンネルと外部接続 IPsec トンネルで使用するサイトに割り当てます。

  AWS/Azure の場合は、1 つ以上のクラウド サイトから外部接続を有効にするために、少なくとも 1 つの外部サブネット プールを提供する必要があります。ただし、GCP の場合、外部デバイスの接続を構成するときに、プール名を空白（未選択）のままにすることができます。この場合、Nexus Dashboard Orchestrator はサブネットから `/24169.254.0.0/16` を割り当てます (範囲の先頭から、つまり `169.254.255.0/24` などになります)。

- **サイト固有のサブネット プール**：クラウドサイトのルータと外部デバイス間の接続に使用されます。

  これらのサブネットは、外部接続 IPsec トンネルが特定の範囲内にあることが必要な場合に定義できます。たとえば、外部ルータに IP アドレスを割り当てるために特定のサブネットがすでに使用されており、それらのサブネットを Nexus Dashboard Orchestrator およびクラウド サイトの IPsec トンネルで引き続き使用する場合です。これらのサブネットは Orchestrator によって管理されず、各サブネットはサイト全体に割り当てられ、外部接続 IPsec トンネルにローカルで使用されます。

  サイト固有のサブネット プールに名前 (`169.254.0.0/24` など) を割り当て、外部デバイスの構成時に使用できるようにします。

  名前付きサブネット プールを指定しない場合でも、クラウド サイトのサイト ルータと外部デバイス間の接続を設定すると、外部サブネット プールがクラウド サイト ルータと外部デバイスの間で確立された IPsec トンネルに対する IP 割り当てに使用されます。

（注） 両方のサブネット プールの最小マスク長は `/24` です。

1 つ以上の**外部サブネット プール**を追加するには：

a) **[IPsec トンネル サブネット プール（IPsec Tunnel Subnet Pools）]** タブを選択します。
b) **[外部サブネット プール（External Subnet Pool）]** エリアで、**[+ IP アドレスの追加（+Add IP Address）]** をクリックして、1 つ以上の外部サブネット プールを追加します。

   このサブネットは、以前の Nexus Dashboard Orchestrator リリースでサイト間接続用にクラウド APIC で以前に設定した、オンプレミス接続に使用されるクラウド ルータの IPsec トンネル インターフェイスとループバックに対処するために使用されます。

サブネットは、他のオンプレミス TEP プールと重複してはならず、0.xxx または 0.0.xxで 始まってはならず、/16 と /24 の間のネットワーク マスク（10.12.0.0/16 など）が必要です。

c) チェックマーク アイコンをクリックして、サブネット情報を保存します。
d) 追加するサブネット プールについて、これらのサブステップを繰り返します。

1 つ以上の **[サイト固有のサブネット プール（Site-Specific Subnet Pools）]** を追加するには：

a) **[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** タブを選択します。
b) **[名前付きサブネット プール（Named Subnet Pool）]** エリアで、**[+ IP アドレスの追加（+Add IP Address）]** をクリックして、1 つ以上の外部サブネット プールを追加します。

[名前付きサブネットプールの追加（Add Named Subnet Pool）] ダイアログが開きます。

c) サブネットの **[名前（Name）]** を入力します。

後ほど、サブネットプールの名前を使用して、後で IP アドレスを割り当てるプールを選択できます。例： extSubPool1

d) **[+ IP アドレスの追加 (+ Add IP Address)]**をクリックして、1 つ以上のサブネット プールを追加します。

サブネットには /16 と /24 の間のネットワークが必要で、0.x.x.x または 0.0.x.x で始めることはできません。たとえば、10.181.0.0/16 のようにします。

e) チェックマーク アイコンをクリックして、サブネット情報を保存します。

同じ名前付きサブネット プールに複数のサブネットを追加する場合は、この手順を繰り返します。

f) **[保存（Save）]** をクリックして、名前付きサブネット プールを保存します。
g) 追加する名前付きサブネット プールについて、これらのサブステップを繰り返します。

Google Cloud サイトとオンプレミス サイト間のサイト間接続の確立

開始する前に、次のものが必要です。

- インフラ テナントでの外部 VRF の作成 （26 ページ） で説明されているように、Google Cloud サイトに外部 VRF を作成して展開します。
- 外部デバイスの追加 （27 ページ） で説明されているように、1 つまたは複数の外部デバイスを追加しました。

（注） 外部接続を構成する前に、Fabric Connectivity Infra ページのすべてのサイトを更新して展開し、AWS/AZure および Google Cloud サイトのクラウド ルータのすべての CSR が Nexus Dashboard Orchestrator に正しく反映されていることを確認できます。

始める前に

ここでは、クラウド APIC サイトにサイト固有のインフラ設定を構成する方法について説明します。開始する前に、次のことを確認してください。

- インフラ テナントでの外部 VRF の作成 （26 ページ） で説明されているように、Google Cloud サイトに外部 VRF を作成して展開します。
- 外部デバイスの追加 （27 ページ） で説明されているように、1 つまたは複数の外部デバイスを追加しました。

（注） 外部接続を構成する前に、Fabric Connectivity Infra ページのすべてのサイトを更新して展開し、AWS/AZure および Google Cloud サイトのクラウド ルータのすべての CSR が Nexus Dashboard Orchestrator に正しく反映されていることを確認できます。

ステップ 1 左側のペインの**Fabric Connectivity Infra**の **[サイト (Sites)]** の下で、特定のクラウド サイトを選択します。

これは、外部デバイスへの接続を確立するサイトです。

ステップ 2 **[外部接続 (External Connectivity)]** 情報を入力します。

このユース ケース構成の一部として外部デバイスに接続情報を提供するには、この手順を完了する必要があります。

a) 右側の ***[<Site> 設定 (Settings)]*** ペインで、**[外部接続 (External Connectivity)]** タブを選択します。

b) **[外部接続の追加 (Add External Connectivity)]** をクリックします。

[外部接続の追加 (Add External Connectivity)] ダイアログが開きます。

c) **[VRF]** ドロップダウンから、外部接続に使用する VRF を選択します。

これは、作成済みのクラウド ルートをリークするために使用される VRF（`extVrf1`）です。

d) **[+外部デバイスの追加（+Add External Device）]** をクリックします。

e) **[外部デバイス (External Devices)]** セクションの **[名前 (Name)]** ドロップダウンから、外部デバイスを選択します。

これは、一般的なインフラストラクチャ設定時に**[一般設定 (General Settings)]** > **[外部デバイス (External Devices)]** リストに追加した外部デバイスであり、すでに定義されている必要があります。

f) **[トンネル IKE バージョン（Tunnel IKE Version）]**は IKE-V2 を選択します。このリリースでは、IKE-V2 のみがサポートされています。

g) （任意）**[トンネル サブネット プール (Tunnel Subnet Pool)]** ドロップダウンから、サイト固有のサブネット プールのいずれかを選択します。

サイト固有のサブネット プールは、クラウド サイトのルータと外部デバイス間の IPsec トンネルに IP アドレスを割り当てるために使用されます。ここで**サイト固有**のサブネット プールを指定しない場合、**外部のサブネット プール** サブネット プールが IP 割り当てに使用されます。

外部デバイス接続用の専用サブネットプールを提供することは、特定のサブネットがすでに外部ルータに IP アドレスを割り当てるために使用されており、それらのサブネットを Nexus Dashboard Orchestrator およびクラウド サイトの IPsecトンネルに引き続き使用する場合に役立ちます。

h) （オプション）**[事前共有キー (Pre-Shared Key)]** フィールドに、トンネルの確立に使用するカスタム キーを入力します。

事前共有キーを提供しない場合、Cloud APIC はクラウド サイト ルータで自動的に生成します。

i) 必要に応じて、同じ外部接続（同じ外部 VRF ）に対して追加する外部デバイスについて、前のサブステップを繰り返します。

j) 必要に応じて、追加の外部接続（異なる外部 VRF ）に対してこの手順を繰り返します。

クラウド サイト ルータと外部デバイス間のトンネルエンドポイントには 1 対 1 の関係があるため、異なる外部 VRF を使用して追加の外部接続を作成できますが、同じ外部デバイスに追加の接続を作成することはできません。

外部デバイスへの構成の展開

前のセクションでは、クラウド サイトの Cloud APIC にインフラ構成を展開して、クラウド サイトから外部デバイスへの接続を有効にする方法について説明しましたが、このセクションでは、外部デバイスからクラウド サイトへの接続を有効にする方法について説明します。

ステップ 1 外部デバイスから接続をイネーブル化するために必要な情報を収集します。

手順の一部として、Nexus Dashboard Orchestrator の **[外部デバイス構成ファイルの展開とダウンロード（Deploy & Download External Device config files）]** オプションまたは **[外部デバイス構成ファイルのダウンロード（External Device config files）]** オプションを使用して、必要な構成の詳細を取得できます。

構成ファイルをダウンロードする場合：

- ファイルの数は、外部接続があるサイトの数と一致します。
- ファイル名の接尾辞はサイト識別子と一致します。

  たとえば、`<...> -2 .config` は、ファイルがサイト識別子 2 のサイト用であることを示します。サイト ID は、Nexus Dashboard Orchestrator GUI の各サイトの **[サイト接続（Site Connectivity）]** ページに表示されます。

ステップ 2 外部デバイスにログインします。

ステップ 3 外部デバイスからクラウド ルータへのトンネルと BGP を構成します。

外部デバイスを構成する場合：

- 特定の要件に応じて、外部サブネットはトンネル インターフェイスと同じ VRF にある場合とない場合があります。

  外部サブネットが異なる VRF にある場合は、外部デバイスで適切なルート リークを構成する必要があります。

  （注） Nexus Dashboard Orchestrator からダウンロードした構成では、IPsec および BGP 接続の確立のみが許可されることに注意してください。外部デバイス自体の内部のルート漏洩構成に関する情報は提供しません。

- 外部サブネットがクラウド サイト ルーターにアドバタイズされると、Nexus Dashboard Orchestrator はルート リーク構成をプロビジョニングして、ユーザー テナント VRF にインポートするサブネットを選択します。
- 次の例では、BGP 構成が外部 VRF（`extVrf1`）で行われ、外部サブネットと外部デバイスのトンネル インターフェイスが同じ VRF の一部であると想定しています。

次の例は、外部デバイス（この場合は ASR1K）から CSR への単一の IPsec トンネル（`Tunnel100`）を構成する方法を示しています。

例：

```
crypto ikev2 proposal ikev2-1
 encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
 integrity sha512 sha384 sha256 sha1
 group 24 21 20 19 16 15 14 2
!
crypto ikev2 policy ikev2-1
 proposal ikev2-1
!
crypto ikev2 keyring keyring-ifc-7
 peer peer-ikev2-keyring
  address 35.220.81.45
  pre-shared-key 163988519666274287497025544399329641924
 !
crypto ikev2 profile ikev-profile-ifc-7
 match address local interface GigabitEthernet1
 match identity remote address 35.220.81.45 255.255.255.255
 identity local address 20.92.217.94
 authentication remote pre-share
 authentication local pre-share
 keyring local keyring-ifc-7
 lifetime 3600
 dpd 10 5 periodic
 !
crypto ipsec transform-set ikev-transport-ifc-7 esp-gcm 256
 mode tunnel
 !
crypto ipsec profile ikev-profile-ifc-7
 set transform-set ikev-transport-ifc-7
 set pfs group14
 set ikev2-profile ikev-profile-ifc-7
 tunnel protection ipsec profile ikev-profile-ifc-7
 !
interface Tunnel100
 description To GCP VPN
 vrf forwarding wanVrf
 ip address 169.254.0.14 255.255.255.252
 ip mtu 1400
```

```
 ip tcp adjust-mss 1400
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 35.220.81.45
 tunnel protection ipsec profile ikev-profile-ifc-7
end
```

次に、BGPの構成例を以下に示します。

例：

```
router bgp 65320
 bgp router-id 172.16.1.1
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf wanVrf
  network 172.16.8.0 mask 255.255.255.0
  network 172.16.9.0 mask 255.255.255.0
  redistribute connected
  neighbor 169.254.0.9 remote-as 65092
  neighbor 169.254.0.9 ebgp-multihop 255
  neighbor 169.254.0.9 activate
  neighbor 169.254.0.13 remote-as 65092
  neighbor 169.254.0.13 ebgp-multihop 255
  neighbor 169.254.0.13 activate
 exit-address-family
!
```

ステップ 4 すべての外部デバイスについて、前の手順を繰り返します。

Google Cloud サイトと他のクラウド サイト間のサイト間接続の構成

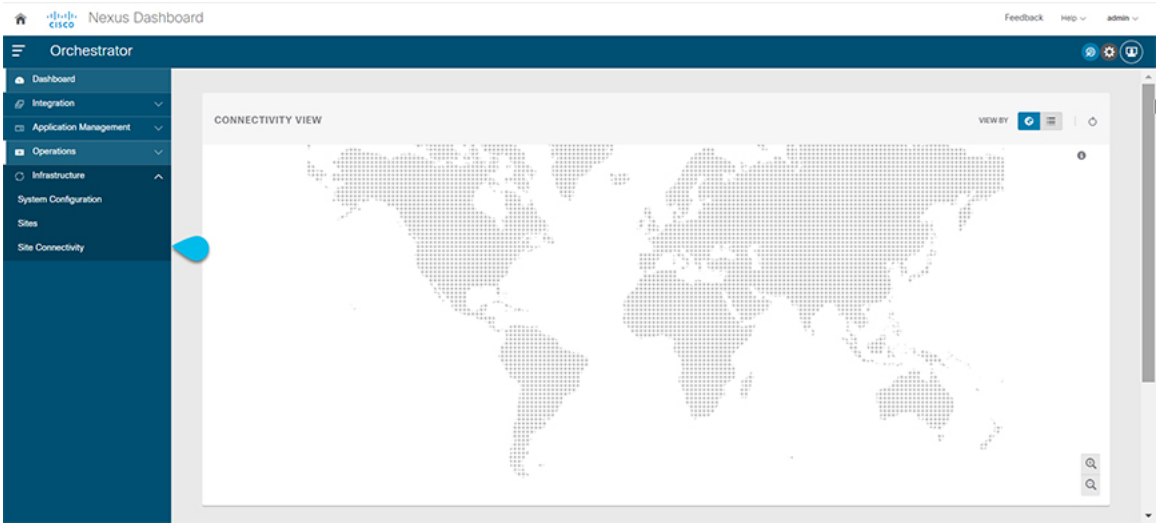
次のセクションでは、2 つのクラウド サイト間の接続を構成する方法について説明します。Google Cloud サイトとオンプレミス サイト間の接続を構成する場合は、Google Cloud サイトとオンプレミス サイト間のサイト間接続を構成します。 （27 ページ） を参照してください。

（注） Google Cloud は非 EVPN 接続のみをサポートするため、すべてのクラウド サイトは BGP-IPv4 である Google Cloud と同じ接続である必要があります。他のクラウド サイトが BGP-EVPN を使用している場合、Google Cloud は引き続き管理できますが、他のクラウド サイトへのサイト間接続はありません。

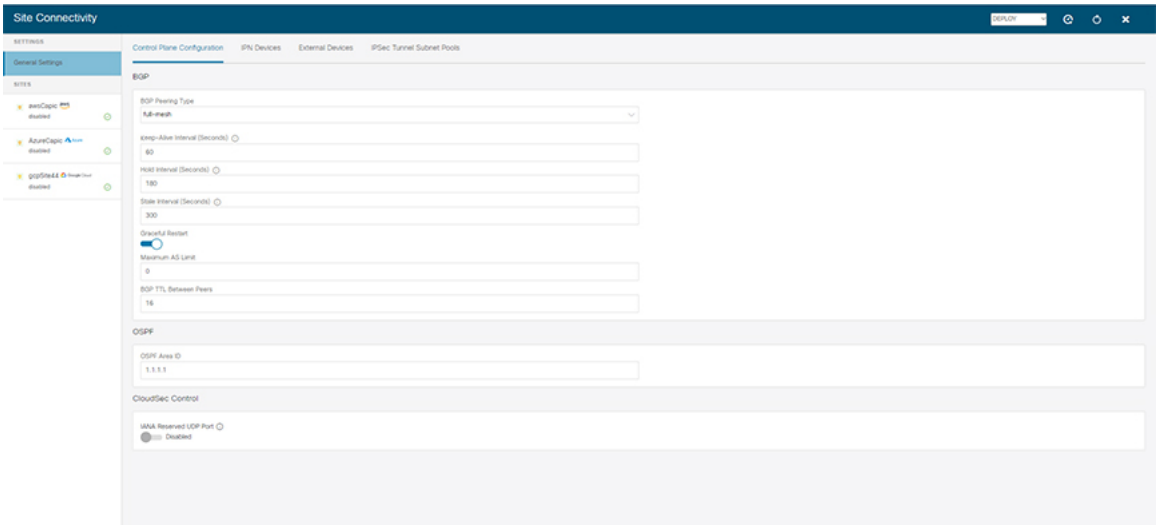
始める前に

ステップ 1 開始する前に、サイト間接続を確立するために、Cloud APIC に少なくとも 1 つのリージョン（サポートされる最大 4 つのリージョン）でハブ ネットワークが構成されていることを確認してください。

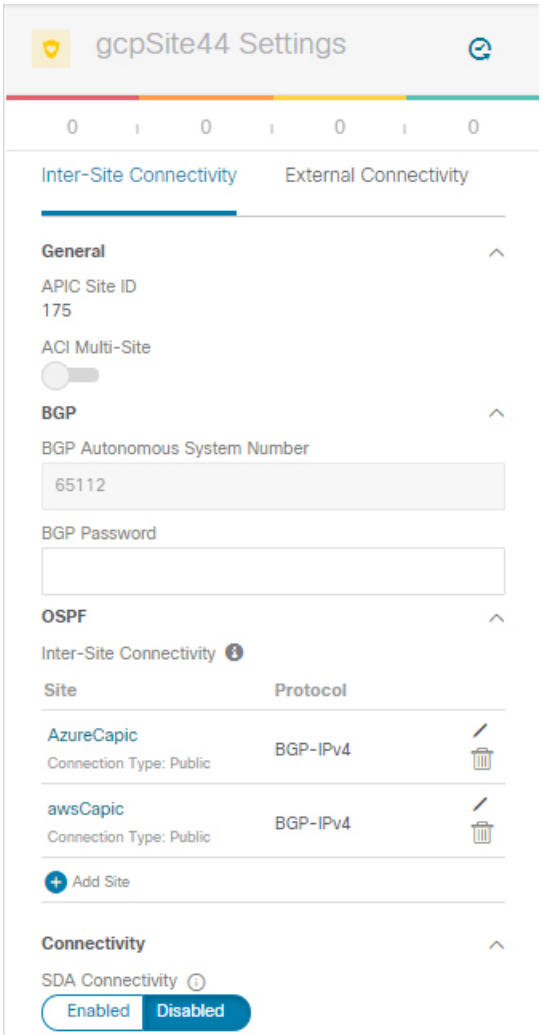
ステップ 2 **[サイト接続（Site Connectivity）]**に移動します。



ステップ 3 サイト間接続を作成するサイトを選択します。サイトを選択すると、右側のウィンドウにサイト間接続と外部接続が表示されます。

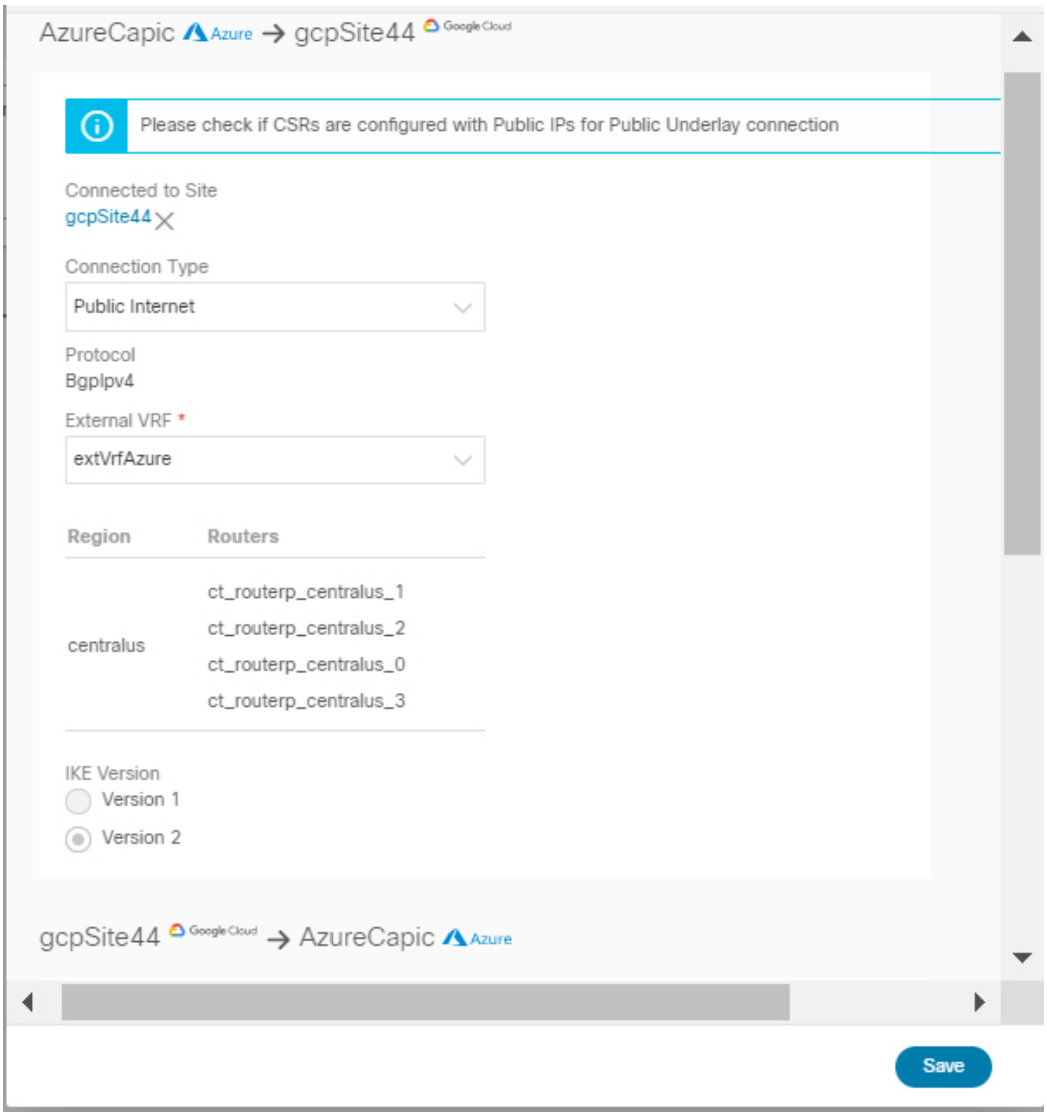


ステップ 4 サイト間接続で、**[サイトの追加（Add Site）]** を選択します。



ステップ 5 ダイアログ ウィンドウの **[Site に Connected（Connected to Site）]** で、クラウド APIC サイトを選択します。

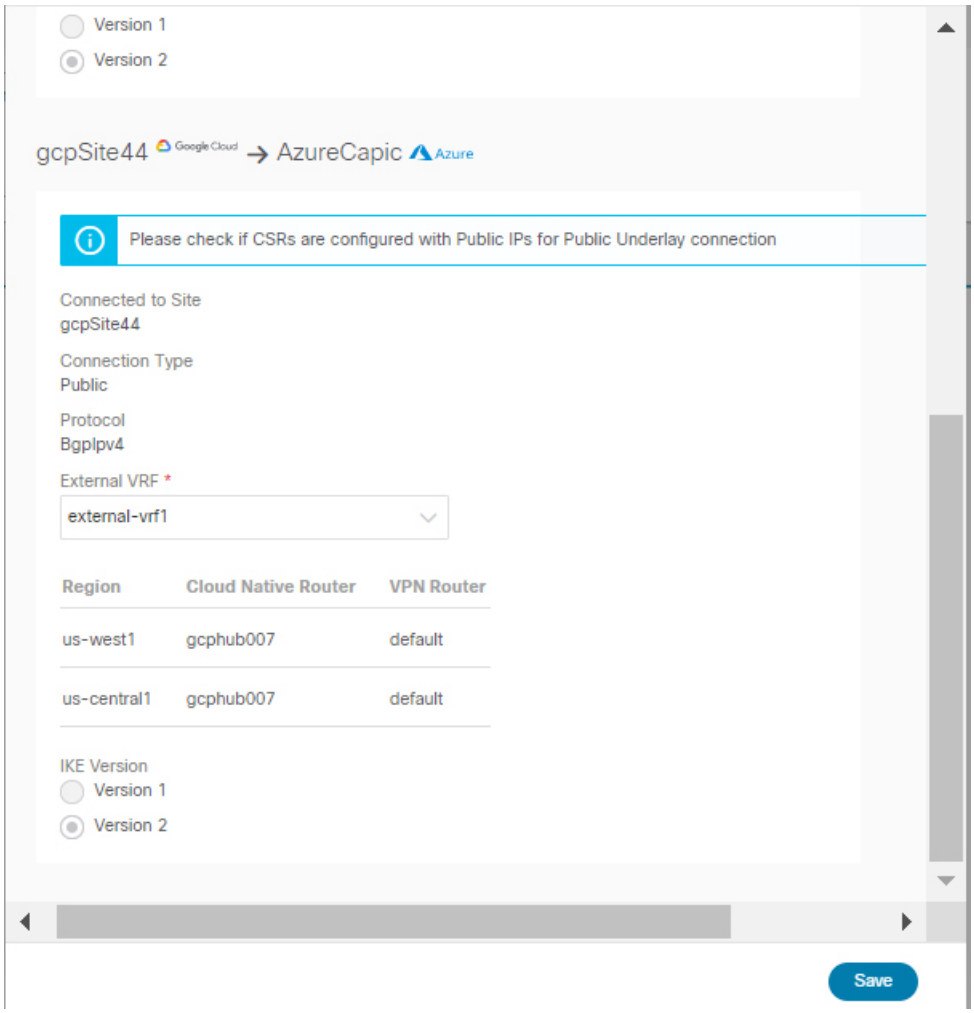
プロトコルの下には、接続タイプとして BGP-IPv4 のみが表示されます。これは、Google Cloud サイトを選択し、Google Cloud サイトが BGP-IPv4 接続のみをサポートしているためです。



ステップ 6 外部 VRF を選択します。

ステップ 7 **[外部 VRF（External VRF）]** ドロップダウンから、外部 VRF を選択します。

これは、インフラ テナントでの外部 VRF の作成 （26 ページ） に構成した外部 VRF です。



ステップ 8 **[保存 (Save)]** をクリックして、サイト間の接続構成を保存します。

インフラ設定の展開

このセクションでは、クラウドサイトからの外部接続用のインフラ構成を展開する方法について説明します。

ステップ 1 メインペインの右上で、**Deploy** > **Deploy & Download External Device Config files** を選択します。

[展開 & IPN デバイス設定ファイルをダウンロード（Deploy & Download IPN Device config files）] 両方のクラウド APIC サイトに構成をプッシュし、クラウドサイトと外部デバイス間のエンドツーエンドインターコネクトを有効にします。

さらに、このオプションでは、外部デバイスから、自分のクラウドサイトに展開された クラウド サイト ルータへ接続できるようにするための、構成情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

ステップ 2 確認ウィンドウで **[はい (Yes)]** をクリックします。

[展開が開始されました。個々のサイトの展開ステータスメッセージについては、左側のメニューを参照してください (Deployment started, refer to left menu for individual site deployment status)] というメッセージにより、インフラ構成の展開が開始されたことが示されます。左側のペインのサイト名の横に表示されるアイコンで、各サイトの進行状況を確認できます。展開が成功したら、Cloud APIC ダッシュボードから、クラウドサイト全体で作成されたトンネルと BGP セッションを確認できます。

外部 EPG の作成

このセクションでは、サブネット選択を使用してインフラ テンプレートに外部 EPG を作成する方法について説明します。この外部 EPG を使用して外部ネットワークを表し、外部 EPG とクラウドEPG間の契約を構成して適用し、クラウドサイトのエンドポイントと外部ネットワーク間の通信を許可します。

ステップ 1 **メイン メニュー**で、**[Application Management (アプリケーション管理)]** > **[スキーマ (Schemas)]** を選択します。

ステップ 2 外部 VRF を含むスキーマとテンプレートを選択します。

すべての（AWS、Azure、または Google Cloud）インフラ テンプレートに対して同様の構成を作成できますが、混乱を避けるために、次のステップで異なるアプリケーション プロファイル名を使用することをお勧めします。

ステップ 3 テンプレートで **[アプリケーション プロファイル]** を追加します。

作成する外部 EPG をアプリケーション プロファイルに関連付ける必要があります。

ステップ 4 **外部 EPG** を作成して構成します。

a) **[オブジェクトの作成]** > **[外部 EPG]** を選択します。
b) 外部 EPG のプロパティ サイドバーで、**サイト タイプ** に CLOUD を選択します。
c) **[アプリケーション プロファイル]** ドロップダウンから、前の手順で作成したプロファイルを選択します。
d) **[仮想ルーティングと転送（Virtual Routing & Forwarding）]** ドロップダウンから、先ほど作成した VRF を選択します。

ステップ 5 EPG のサイトローカル プロパティを構成します。

a) 左側のサイドバーで、割り当て先のサイトの下にあるテンプレートを選択します。
b) テンプレートのサイトローカル プロパティで、**ルート到達性（Route Reachability）** の [外部サイト（External-Site）] を選択します。

c) **[セレクタの追加（Add Selector）]** をクリックします。
d) **[新しいエンドポイント セレクターの追加]** ダイアログで、外部サブネットを指定します。

これは、前のセクションでルート リークを構成したクラウド サイトへの接続を必要とする外部サブネットです。たとえば、`172.16.8.0/24` です。

ステップ 6 テンプレートを展開して、クラウド サイトに外部 EPG を作成します。

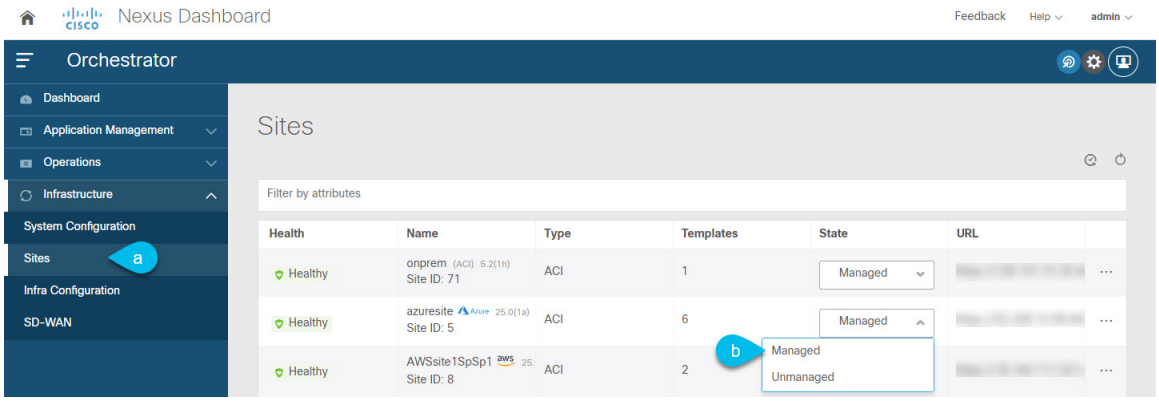
Google Cloud ユーザー テナントのインポート

既存のテナントをインポートする場合は、以下の手順に従ってください。新しいテナントを作成する場合は、この Google Cloud ユーザー テナントの作成 （45 ページ） セクションを参照してください。

ステップ 1 Nexus ダッシュボードの **[サービス カタログ (Service Catalog)]** から、Nexus Dashboard Orchestratorサービスを開きます。

Nexus ダッシュボード ユーザーのクレデンシャルを使用して自動的にログインします。

ステップ 2 Nexus Dashboard Orchestrator GUIで、サイトを管理します。



a) 左のナビゲーションメニューから、**[インフラストラクチャ (Infrastructure)]** > **[サイト (Sites)]**を選択します。
b) メインペインで、Nexus Dashboard Orchestrator で管理する各ファブリックの **[状態 (State)]** を `[非管理対象 (Unmanaged)]` から `[管理対象 (Managed)]` に変更します。

ステップ 3 既存のクラウドテナントをインポートします。

a) **[サイト（Sites）]** ページで、管理を有効にしたサイトの横にあるアクション **(...)** メニューをクリックし、**[テナントのインポート（Import Tenants）]** を選択します。
b) **[テナントのインポート（Import Tenants）]** ダイアログで、インポートするテナントを選択し、**OK** をクリックします。

ステップ 4 テナントの外部接続インフラ構成が正常にインポートされたことを確認します。

外部接続をインポートするには、ハブがインスタンス化されるすべてのリージョンで構成する必要があります。

a) **[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**ページに移動します。
b) [構成] をクリックします。
c) **[一般設定（General Settings）]** ページで、**[外部デバイス（External Devices）]** タブを選択します。

外部デバイスが存在することを確認します

d) **[一般設定（General Settings）]** ページで、**[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** タブを選択します。

外部接続サブネット プールが存在することを確認します。

e) 左側のサイドバーで、テナントをインポートしたサイトを選択します。

サイトの設定で、**[外部接続（External Connectivity）]** タブを選択し、外部ネットワークが存在することを確認します。

（注） 現時点では Nexus Dashboard からインフラ構成を展開せず、次のセクションに進んで外部 VRF をインポートしてください。

テナントの作成

次のセクションでは、管理対象テナントまたは非管理対象テナントを作成する方法について説明します。

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。

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、Google Cloudから最初に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） 管理対象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。

Google Cloud ユーザー テナントの作成

始める前に

Nexus Dashboard Orchestrator で Google Cloud ユーザー テナントを作成する前に、Google Cloud で特定の構成を行う必要があります。

- 管理されたテナントあるいは管理されていないテナントの場合、最初に Google Cloud でプロジェクトを設定する必要があります。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 （41 ページ）を参照してください。
- 管理されていないテナントの場合、必要な秘密キー情報を生成し、Google Cloud から JSON ファイルをダウンロードする必要があります。「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 （44 ページ）」を参照してください。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーションメニューで、「テナント」をクリックします。

ステップ 3 「テナント」を追加を選択します。

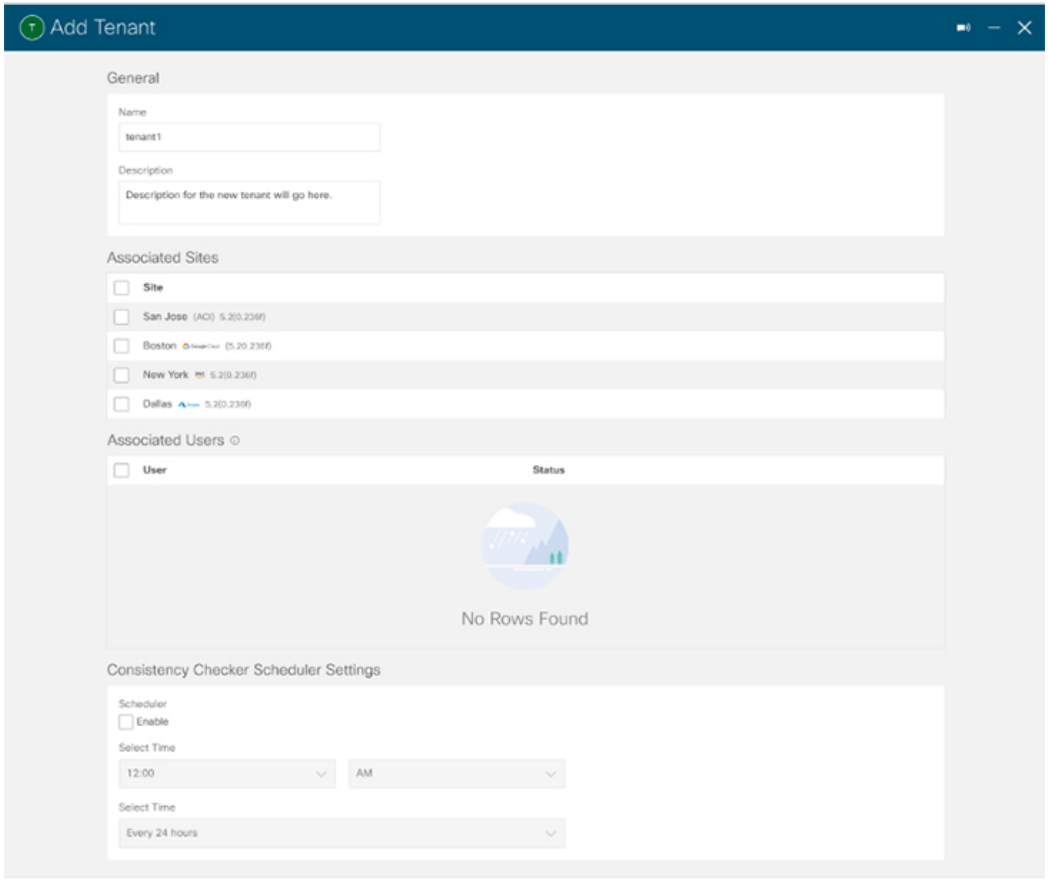
ステップ 4 **[全般（General）]** で、テナント名とオプションの説明を入力します。

テナント名は次のフォーマットにする必要があります：

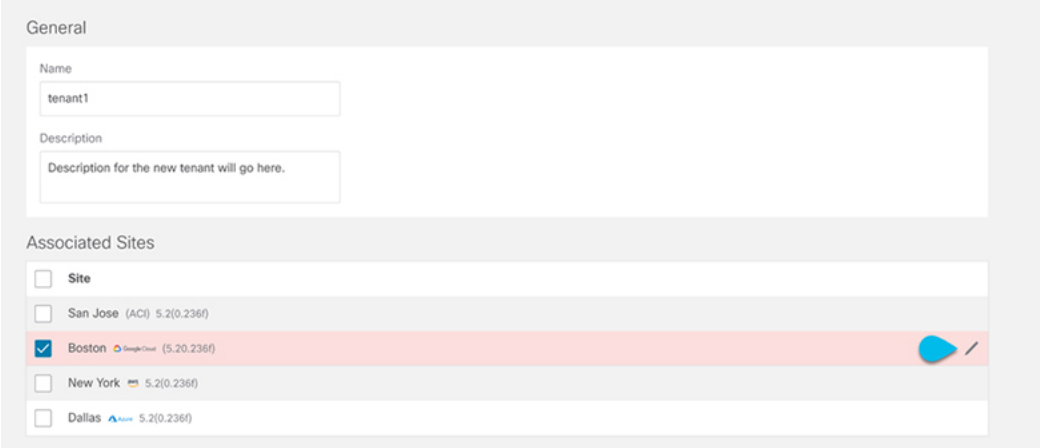
```
[az]([-a-z0-9] * [a-z0-9])?
```

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、または桁にできます。ただし、最後の文字にはハイフンを使用できません。

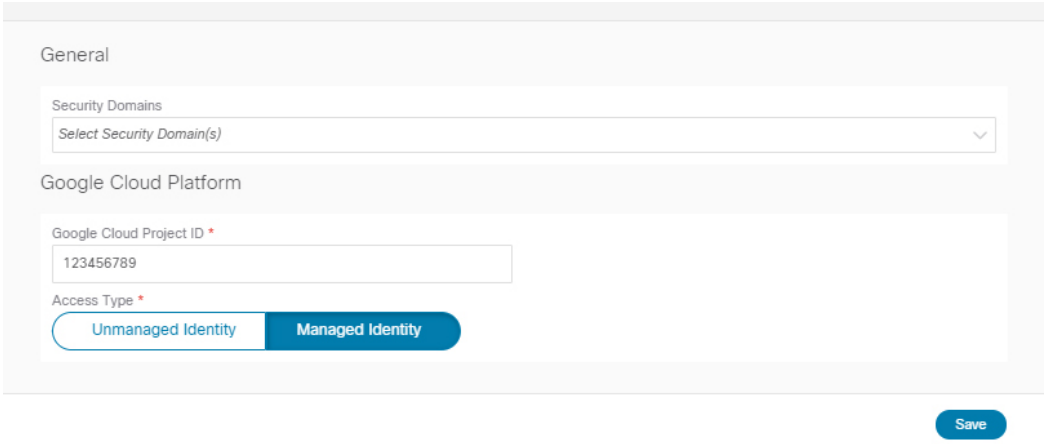
ステップ 5 **[Associated Sites（関連サイト）]** エリアから、テナントを作成する Google Cloud サイトを選択します。



ステップ 6 Google Cloud サイトを選択したら、編集アイコンをクリックしてアカウント情報を指定します。



ステップ 7 必須情報をすべて入力します。

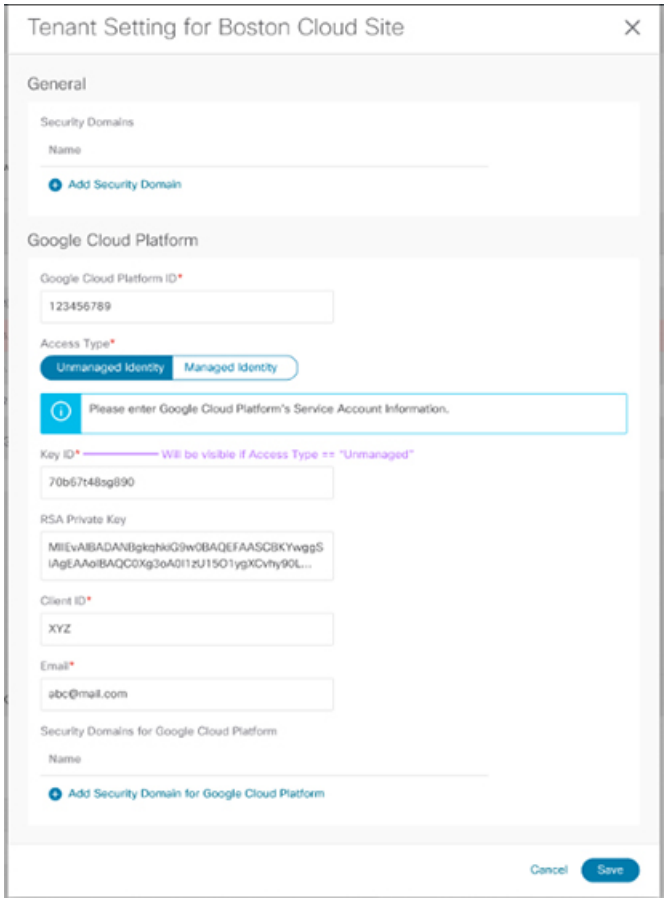


- **[Google Cloud Platform ID（Google Cloud Platform ID）]**：このテナント用に作成した Google Cloud ユーザー アカウントの 識別子 を指定します。
- **[アクセス タイプ（Access type）]**：アクセス タイプの下に 2 つのオプションがあります：
  - Cloud APIC VMがクラウドリソースを管理できるようにするには、**[管理対象アイデンティティ（Managed Identity）]** を選択します。

    管理されたテナントあるいは管理されていないテナントの場合、最初に Google Cloud でプロジェクトを設定する必要があります。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 （41 ページ）を参照してください。
  - 特定のアプリケーションを介してクラウドリソースを管理するには、**[管理されていないアイデンティティ（Unmanaged Identity）]** を選択します。この場合、アプリケーションのクレデンシャルも Cloud API に提供する必要があります。
    - 管理されたテナントあるいは管理されていないテナントの場合、最初に Google Cloud でプロジェクトを設定する必要があります。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 （41 ページ）を参照してください。
    - 管理されていないテナントの場合、必要な秘密キー情報を生成し、Google Cloud から JSON ファイルをダウンロードする必要があります。「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 （44 ページ）」を参照してください。

    アクセス タイプとして **[管理されていない識別子（Unmanaged Identity）]** を選択した場合は、**[キー ID（Key Id）]** と **[クライアント識別子（Client Id）]** フィールドが表示されます。
- **[キー 識別子（Key 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 （44 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。
- **[クライアント識別子（Client 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 （44 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。

- **[E メール（Email）]**：Google Cloud プロジェクトに関連付けられている E メール アドレスを入力します。



ステップ 8 Google Cloud の構成を入力したら、**[保存（Save）]** を選択します。

次のタスク

管理対象テナントを作成している場合は、管理されたテナントのGoogle Cloud で必要なアクセス許可を設定する必要があります。これらの手順については、管理対象テナント用に Google Cloud で必要な権限を設定する （48 ページ） にアクセスしてください。

管理対象テナント用に Google Cloud で必要な権限を設定する

管理対象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、この管理対象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。

Cloud EPG の作成

すでに行ったインフラ テナント設定（外部 VRF など）とは別のテンプレートとスキーマでクラウド オブジェクトを作成することをお勧めします。

次の手順を使用して、Cloud APIC サイトの新しいスキーマを作成します。この使用例では、1 つのスキーマと 1 つのテンプレートを構成します。

この手順全体では、Nexus Dashboard Orchestrator を使用しています。

ステップ 1 メイン メニューで **[スキーマ]** をクリックします。

ステップ 2 [スキーマ（Schema）] 画面で、**[スキーマの追加（Add Schema）]** ボタンをクリックします。

ステップ 3 [Untitled Schema] 画面で、ページの上部にあるテキスト `Untitled Schema`を、作成するスキーマの名前（たとえば、 `schema-1`）に置き換えます。

ステップ 4 テンプレートを作成します。

Google Cloud サイトに割り当てられたテンプレートは拡張できないため、クラウド ローカル テンプレートを作成します。

a) 左側のペインで、**Template 1** の上にマウスを移動し、[メモ] アイコンをクリックします。次に、テンプレートの名前を変更します（例: Google Cloud の場合、`template1-gcp`）。

b) 中央のペインで、**スキーマを作成するエリアをクリックしてテナントを選択してください** をクリックしてください。

c) 右側のペインで、**[テナントの選択（Select A Tenant）]** ダイアログ ボックスにアクセスし、必要なテナントを選択します。これは、インポートしたGoogle Cloud ユーザー テナントのインポート （40 ページ） または Google Cloud ユーザー テナントの作成 （45 ページ） で作成したテナントです。

ステップ 5 テナントを選択したら、テンプレートに**アプリケーション プロファイル**を作成します。

作成したクラウド EPG をアプリケーション プロファイルに関連付ける必要があります。

ステップ 6 **Cloud EPG** を作成して設定します。

a) **[オブジェクトの作成（Create Object）]** > **[Cloud EPG（Cloud EPGs）]** を選択します。

b) **[アプリケーション プロファイル（Application Profile）]** ドロップダウンから、前の手順で作成したプロファイルを選択します。

c) **[仮想ルーティングと転送（Virtual Routing & Forwarding）]** ドロップダウンから、作成したクラウド VRF を選択します。

d) 右側のプロパティ サイドバーで、この EPG 用に作成したクラウド VRF を選択します。

ステップ 7 先ほど作成したテンプレートを Google Cloud サイトに割り当てます。

ステップ 8 EPG のサイトローカル プロパティを構成します。

a) 左側のサイドバーで、割り当て先のサイトの下にあるテンプレートを選択します。

b) テンプレートのサイトローカルプロパティで、**ルート到達可能性**に対して`[クラウド サイト（Cloud Site）]` を選択します。

Google Cloud サイトのスキーマ、テンプレート、VRF の作成

ステップ 1 メイン メニューで **[スキーマ]** をクリックします。

ステップ 2 [スキーマ（Schema）] 画面で、**[スキーマの追加（Add Schema）]** ボタンをクリックします。

ステップ 3 [Untitled Schema] 画面で、ページの上部にあるテキスト `Untitled Schema`を、作成するスキーマの名前（たとえば、 `schema-1`）に置き換えます。

ステップ 4 最初のテンプレートを構成します。

クラウド ローカル テンプレートを選択します。

ステップ 5 左側のペインで、**テンプレート**の上にマウスを移動し、[メモ] アイコンをクリックします。次に、テンプレートの名前を変更します（例： `template1-gcp`）。

ステップ 6 クラウド テンプレートに移動します。

ステップ 7 VRF で **[VRFを追加（Add VRF）]** を選択し、VRF の表示名と説明を入力します。

ステップ 8 作成した VRF をクリックします。

テンプレート プロパティとサイト ローカル プロパティが画面の右側に表示されます。

ステップ 9 サイト レベルのプロパティで、**[リージョンの追加（Add Region）]** を選択します。

ポップアップで、目的の地域を選択します。

ステップ 10 リージョンを選択したら、**[CIDR の追加（Add CIDR）]** を選択します。

VRF の CIDR 情報を入力します。

- プライマリ CIDR を追加する場合は、**[プライマリ（Primary）]** を選択します。
- セカンダリ CIDR を追加する場合は、**[セカンダリ（Secondary）]** を選択します。

ステップ 11 サブネットとサブネット グループ ラベルを入力します。

サブネットを作成する場合、**Subnet Group Label**を使用して、特定のサブネット グループに一意のラベルを割り当てます。CIDR、サブネット、およびサブネット グループ ラベルの構成の詳細については、[Google Cloud 向け Cisco Cloud APIC ユーザー ガイド（Cisco Cloud APIC for Google Cloud User Guide）]の「Google Cloud の VPC とサブネットと Cloud APIC のクラウド コンテキスト プロファイルについて」を参照してください。

ステップ 12 [保存（Save）] を選択します。

アプリケーション プロファイルと EPG の構成

ステップ 1 中央のペインで、**[+ アプリケーション プロファイル (+ Application profile)]** をクリックします。

ステップ 2 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドにアプリケーション プロファイルの名前（app1 など）を入力します。

ステップ 3 中央のペインで、**[+ EPG の追加]** をクリックします。

ステップ 4 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドに EPG の名前を入力します。

ステップ 5 **[クラウドのプロパティ（Cloud Properties）]** 領域に、前のセクションで作成した VRF（`cloud-vrf` など）が表示されます。

クラウド エンドポイント セレクタの追加

Cloud APIC では、クラウド EPG は、同じセキュリティ ポリシーを共有するエンドポイントの集合です。クラウド EPG は、1 つまたは複数のサブネット内にエンドポイントを持つことができ、CIDR に関連付けられます。エンドポイント セレクタと呼ばれるオブジェクトを使用して、クラウド EPG のエンドポイントを定義します。エンドポイント セレクタは、Cisco ACI によって管理される AWS、Azure、Google Cloud に割り当てられたクラウド インスタンスに対して実行されるルールのセットです。エンドポイント インスタンスに一致するエンドポイント セレクタ ルールは、そのエンドポイントをクラウド EPG に割り当てます。エンドポイントが一度に 1 つの EPG にのみ属することができる従来のオンプレミス ACI ファブリックとは異なり、複数のクラウド EPG に一致するようにエンドポイント セレクタを構成することができます。これにより、同じインスタンスが複数の Cloud EPG に属することになります。ただし、各エンドポイントが単一の EPG のみに一致するようにエンドポイント セレクタを設定することをお勧めします。以下のセクションでは、エンド ポイント セレクタを追加するプロセスについて説明します。

ステップ 1 Nexus Dashboard Orchestrator で、前のセクションで作成した EPG を選択します。

ステップ 2 右側のペインの **[サイトのローカルのプロパティ（Site Local Properties）]** 領域で「セレクタ」見出しの下の **[+セレクタ（+Selector）]** をクリックします。

この EPG を拡張する予定がある場合は、代わりにテンプレート レベルでエンドポイント セレクタを追加することも選択できます。

ステップ 3 **[新しいエンドポイント セレクタの追加（Add New End Point Selector）]** ダイアログで、**[エンドポイント セレクタ名（End Point Selector Name）]** フィールドに、このエンドポイント セレクタで使用する分類に基づいて名前を入力します。

たとえば、IP サブネット分類のエンドポイント セレクタの場合は、`[IP-Subnet-EPSelector]`などの名前を使用できます。

ステップ 4 **[+ 式（+ Expression）]** をクリックし、3 つのフィールドを使用して、クラウドでエンドポイントを分類する方法に基づいてエンドポイント セレクタを構成します。

[タイプ（Type）] フィールドは、エンドポイント セレクタに使用する式を決定します。

- エンドポイント セレクタの個々の IP アドレスまたはサブネットを使用する場合は、**[IP アドレス]** を選択します。

- エンドポイントセレクタにクラウドリージョンを使用する場合は**[リージョン（Region）]**を選択し、使用する特定のリージョンを選択します。

  エンドポイント セレクタの [リージョン（Region）] を選択すると、そのリージョンで起動されるテナント内のすべてのインスタンスが、このクラウド EPG に割り当てられます。

- エンドポイント セレクタのカスタム タグまたはラベルを作成する場合は、**[カスタム タグまたはラベル（Custom tags or labels）]** を選択します。入力を開始してカスタム タグまたはラベルを入力し、新しいフィールドで **[作成（Create）]** をクリックして新しいカスタム タブまたはラベルを作成します。

[演算子（Operator）] フィールドは、タイプとその値の関係を決定します。

- **[等しい (Equals)]**：[値 (value)] フィールドに 1 つの値がある場合に使用します。
- **[等しくない (Not Equals)]**：値フィールドに 1 つの値がある場合に使用されます。
- **[含まれる (In)]**：[値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
- **[含まれない (Not In)]**：値フィールドに複数のカンマ区切り値がある場合に使用されます。
- **[キーを持つ (Has Key)]**：式にキーのみが含まれている場合に使用されます。
- **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用されます。

[値 (value)] フィールドで、2 つ前のフィールドに対して行った選択に基づいて、エンドポイント セレクタに使用する値を選択します。これは、単一の IP アドレス、サブネット、AWS リージョンまたはゾーン、またはカスタム タグ値にすることができます。

このユース ケースでは、IP サブネットに基づいてエンドポイントを割り当てるため、次の例の値を使用してエンドポイント セレクタを構成します。

- **[タイプ（Type）::** IP アドレス
- **[演算子（Operator）]**： 等しい
- **値**： 3.3.1.0/24

ステップ 5 新しいエンドポイント セレクタの横にあるチェックマークをクリックします。

ステップ 6 [新しいエンド ポイント セレクタの追加] フォームで **[保存（Save）]** をクリックします。

外部 EPG とクラウド EPG 間の契約の適用

このセクションでは、クラウドサイトのエンドポイントと外部ネットワーク間の通信を許可する契約を適用する方法について説明します。Google Cloud コントラクトに関して留意すべき 1 つのことは、コントラクトは双方向トラフィックに対して双方向に展開する必要があるということです。

始める前に

- クラウド サイトで 1 つ以上のクラウド EPG Cloud EPG の作成 （50 ページ） がすでに構成されている必要があります。
- 外部 EPG 外部 EPG の作成 （39 ページ）と外部 VRF インフラ テナントでの外部 VRF の作成 （26 ページ）がすでに構成されています。

ステップ 1 メイン メニューで、**[Application Management（アプリケーション管理）]**>**[スキーマ（Schemas）]** を選択します。

ステップ 2 コントラクトを作成し、クラウド EPG に割り当てます。

a) 既存のクラウド EPGを含むスキーマとテンプレートを選択します。

b) このユース ケースに使用する契約を作成します。

外部ネットワークとCloud EPG間の通信に適用する既存の契約がすでにある場合は、この手順をスキップできます。

それ以外の場合は、Cisco ACI ファブリックでの EPG 間通信で通常行うように、コントラクトと必要なフィルタ処理を作成します。

c) クラウド EPG にコントラクトを割り当てます。

特定のユース ケースに基づいて、2 つの EPG (クラウド EPG と外部 EPG) のどちらが[プロバイダ（provider）]になり、どちらが[コンシューマ（consumer）]になるかを決定できます。

ステップ 3 外部 EPG にコントラクトを割り当てます。

a) スキーマを選択し、外部 EPG を作成するテンプレートを選択します。

b) 外部 EPG にコントラクトを割り当てます。

クラウド EPG をプロバイダーとして構成した場合は、外部 EPG の[コンシューマ（consumer）]を選択します。それ以外の場合、クラウド EPG がコンシューマーである場合は、[プロバイダ（provider）] を選択します。

（注） 外部EPGとクラウドEPGの間でコントラクトを使用できるように、コントラクト範囲を「グローバル」に設定する必要があります。

ステップ 4 テンプレートを展開します。

Cloud VRF と外部 VRF 間のルート リークを構成

このユース ケースは、Google クラウド サイトと別のクラウドまたはオンプレミス サイトとの間のトラフィック フローを確立するために、Google クラウド VRF（ユーザー テナント内）と外部 VRF（インフラ内テナント）の間のルート リークに焦点を当てています。 2 つのクラウド VRF 間のルート リークを構成する方法については（たとえば、同じ Google Cloud サイト内

でトラフィック フローを有効にするなど）、2 つのクラウド VRF 間のルート リークの構成（71 ページ） を参照してください。

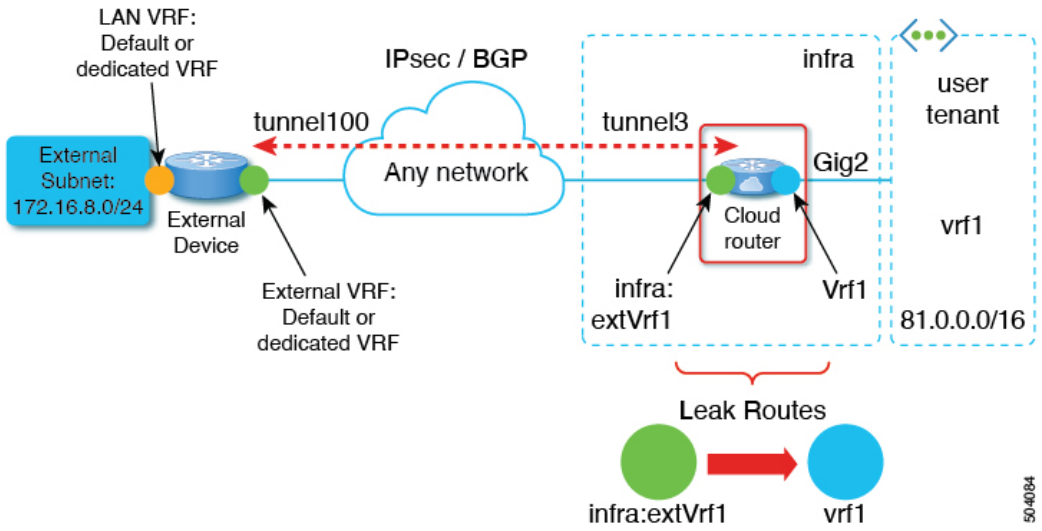
始める前に

クラウド サイトに 1 つ以上のクラウド VRF がすでに構成されている必要があります。外部 VRF から既存のクラウド VRF へのルート リークを構成します。

ステップ 1 **[メイン メニュー（Main menu）]**で、**[Application Management（アプリケーション管理）]** > **[スキーマ（Schemas）]** を選択します。

ステップ 2 外部 VRF からクラウド VRF へのルート リークを構成します。

次の手順は、次のルート リークを設定する方法を示しています。



a) 外部 VRF を含むインフラ テナント テンプレートを作成したスキーマを開きます。

b) **SITES** の下の左側のサイドバーで、クラウド サイトに関連付けられている特定のテンプレートを選択します。

c) サイトローカル プロパティで、テンプレートで定義されている外部 VRF を選択します。

これは、作成して 1 つ以上の外部デバイスに割り当てた VRF です。

d) VRF の右側のプロパティ サイドバーで、**[+リーク ルートの追加（+Add Leak Route）]** をクリックします。

[リーク ルートの追加] ダイアログが開きます。

e) [リーク ルートの追加] ダイアログの設定領域で、[VRF の選択] をクリックし、クラウド VRF を選択します。

この手順の目的は、外部 VRF からクラウド VRF にルートをリークすることであるため、プロパティを構成している外部 VRF からルートをリークするクラウド VRF を選択します。

f) **[リーク ルートの追加（Add Leak Routes）]** ダイアログで、**[すべてをリーク（Leak All）]** を選択するか、特定のサブネット IP に制限します。

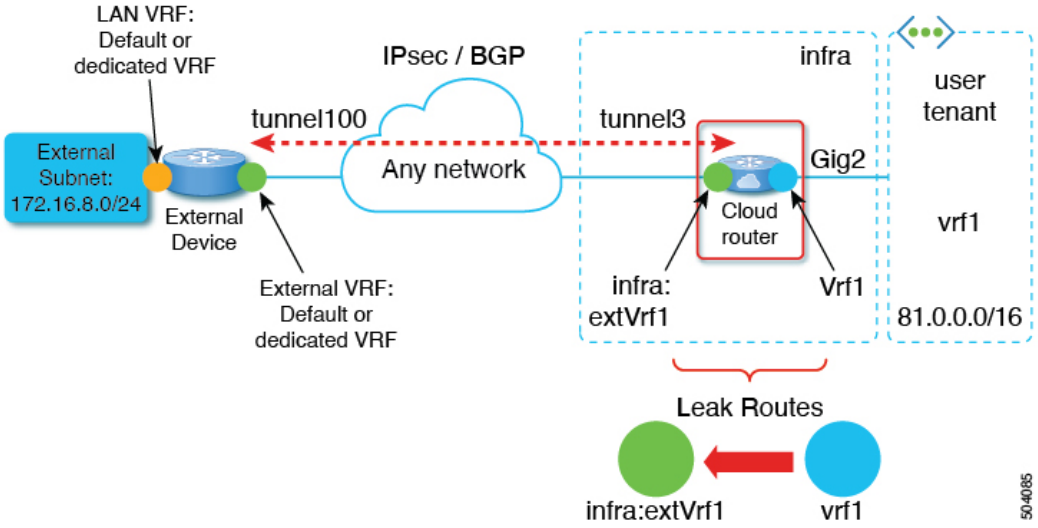
[すべてをリーク（Leak All）] を選択すると、サブネット IP に `0.0.0.0/0` が入力され、すべてのルートがリークされます。リークするルートを制限することを選択した場合は、[+サブネット IP の追加] をクリックし、外部ネットワークから到達可能にするクラウド VRF のサブネット（81.0.1.0/24 など）を指定します。チェックマーク アイコンをクリックして、サブネット情報を保存します。

g) **[保存（Save）]** をクリックして、ルーティング構成を保存します。

h) テンプレートを選択し、**[展開（Deploy）]** をクリックして構成を展開します。

ステップ 3 クラウド VRF から外部 VRF へのルート リークを構成します。

次の手順は、逆方向のルート リークを設定する方法を示しています。



a) クラウド VRF を定義するテンプレートを含むスキーマを開きます。

b) 左側のサイドバーの **SITES** の下で、特定のクラウド サイトを選択します。

c) サイトローカル プロパティで、クラウド VRF を選択します。

d) VRF の右側のプロパティ サイドバーで、**[+リーク ルートの追加（+Add Leak Route）]** をクリックします。

[リーク ルートの追加] ダイアログが開きます。

e) **[リーク ルートの追加]** ダイアログの設定領域で、**[VRF の選択]** をクリックし、外部 VRF を選択します。

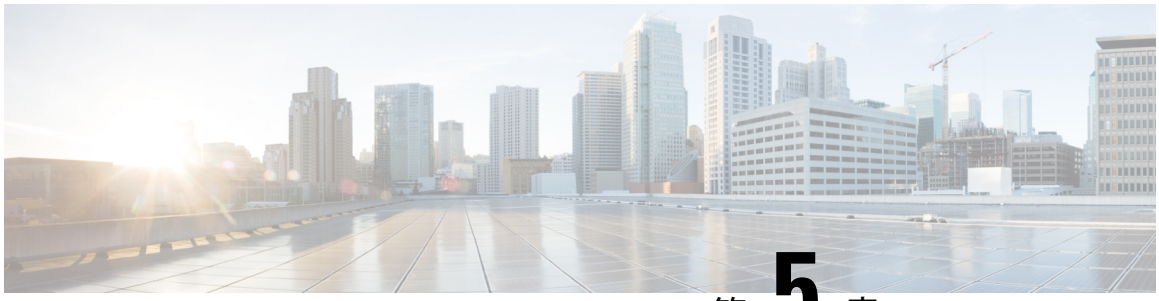
この手順の目的は、クラウド VRF から外部 VRF にルートをリークすることであるため、作成した外部 VRF を選択します。

f) **[リーク ルートの追加（Add Leak Routes）]** ダイアログで、**[すべてをリーク（Leak All）]** を選択したいかどうかもしくは、特定の**[サブネット IP（Subnet IP）]** に制限したいかどうかをを選択します。

[すべてをリーク（Leak All）] を選択すると、サブネット IP に `0.0.0.0/0` が入力され、すべてのルートがリークされます。

リークするルートを制限することを選択した場合は、**[+サブネット IP の追加（+Add Subnet IP）]**をクリックし、外部ネットワークから到達可能にするクラウド VRF のサブネット（`81.0.1.0/24` など）を指定します。チェックマーク アイコンをクリックして、サブネット情報を保存します。

g) **[保存（Save）]** をクリックして、ルーティング構成を保存します。
h) テンプレートを選択し、**[展開（Deploy）]** をクリックして構成を展開します。



第 5 章

Google Cloud ワークロードの内部接続を構成

- 内部接続ワークフロー （59 ページ）
- Google Cloud ユーザー テナントのインポート （59 ページ）
- テナントの作成 （61 ページ）
- Google Cloud サイトのスキーマ、テンプレート、VRF の作成 （69 ページ）
- Cloud EPG の作成 （70 ページ）
- クラウド EPG 間の契約の適用 （71 ページ）
- 2 つのクラウド VRF 間のルート リークの構成 （71 ページ）

内部接続ワークフロー

以下のセクションでは、GCP サイトのインフラストラクチャ、サイト間接続、および簡単な展開の使用例を構成する方法について説明します。ワークフローには次のものが含まれます。

- 前のセクションで作成した EPG を選択します
- クラウド VRF 間のルート リークの構成
- Google クラウド ユーザー テナントと EPG を作成またはインポートし、サイト間の通信を可能にするための契約を適用します

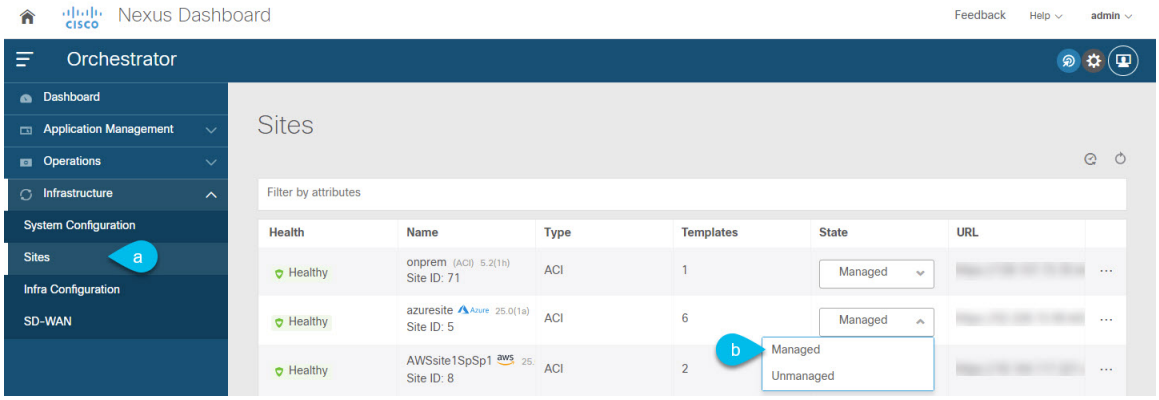
Google Cloud ユーザー テナントのインポート

既存のテナントをインポートする場合は、以下の手順に従ってください。新しいテナントを作成する場合は、この Google Cloud ユーザー テナントの作成 （45 ページ） セクションを参照してください。

ステップ 1 Nexus ダッシュボードの **[サービス カタログ (Service Catalog)]** から、Nexus Dashboard Orchestratorサービスを開きます。

Nexus ダッシュボード ユーザーのクレデンシャルを使用して自動的にログインします。

ステップ 2 Nexus Dashboard Orchestrator GUIで、サイトを管理します。



a) 左のナビゲーションメニューから、**[インフラストラクチャ (Infrastructure)]** > **[サイト (Sites)]**を選択します。

b) メインペインで、Nexus Dashboard Orchestrator で管理する各ファブリックの **[状態 (State)]** を［非管理対象 (Unmanaged)］から［管理対象 (Managed)］に変更します。

ステップ 3 既存のクラウド テナントをインポートします。

a) **[サイト（Sites）]** ページで、管理を有効にしたサイトの横にあるアクション **(...)** メニューをクリックし、**[テナントのインポート（Import Tenants）]** を選択します。

b) **[テナントのインポート（Import Tenants）]** ダイアログで、インポートするテナントを選択し、**OK** をクリックします。

ステップ 4 テナントの外部接続インフラ構成が正常にインポートされたことを確認します。

外部接続をインポートするには、ハブがインスタンス化されるすべてのリージョンで構成する必要があります。

a) **[インフラストラクチャ（Infrastructure）]** > **[サイト接続（Site Connectivity）]**ページに移動します。

b) [構成] をクリックします。

c) **[一般設定（General Settings）]** ページで、**[外部デバイス（External Devices）]** タブを選択します。

外部デバイスが存在することを確認します

d) **[一般設定（General Settings）]** ページで、**[IPSec トンネル サブネット プール（IPSec Tunnel Subnet Pools）]** タブを選択します。

外部接続サブネット プールが存在することを確認します。

e) 左側のサイドバーで、テナントをインポートしたサイトを選択します。

サイトの設定で、**[外部接続（External Connectivity）]** タブを選択し、外部ネットワークが存在することを確認します。

（注） 現時点では Nexus Dashboard からインフラ構成を展開せず、次のセクションに進んで外部 VRF をインポートしてください。

テナントの作成

次のセクションでは、管理対象テナントまたは非管理対象テナントを作成する方法について説明します。

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。

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、Google Cloudから最初に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） 管理対象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。

Google Cloud ユーザー テナントの作成

始める前に

Nexus Dashboard Orchestrator で Google Cloud ユーザー テナントを作成する前に、Google Cloud で特定の構成を行う必要があります。

- 管理されたテナントあるいは管理されていないテナントの場合、最初にGoogle Cloudでプロジェクトを設定する必要があります。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 （41 ページ）を参照してください。
- 管理されていないテナントの場合、必要な秘密キー情報を生成し、Google CloudからJSONファイルをダウンロードする必要があります。「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 （44 ページ）」を参照してください。

ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 左側のナビゲーションメニューで、「テナント」をクリックします。

ステップ 3 「テナント」を追加を選択します。

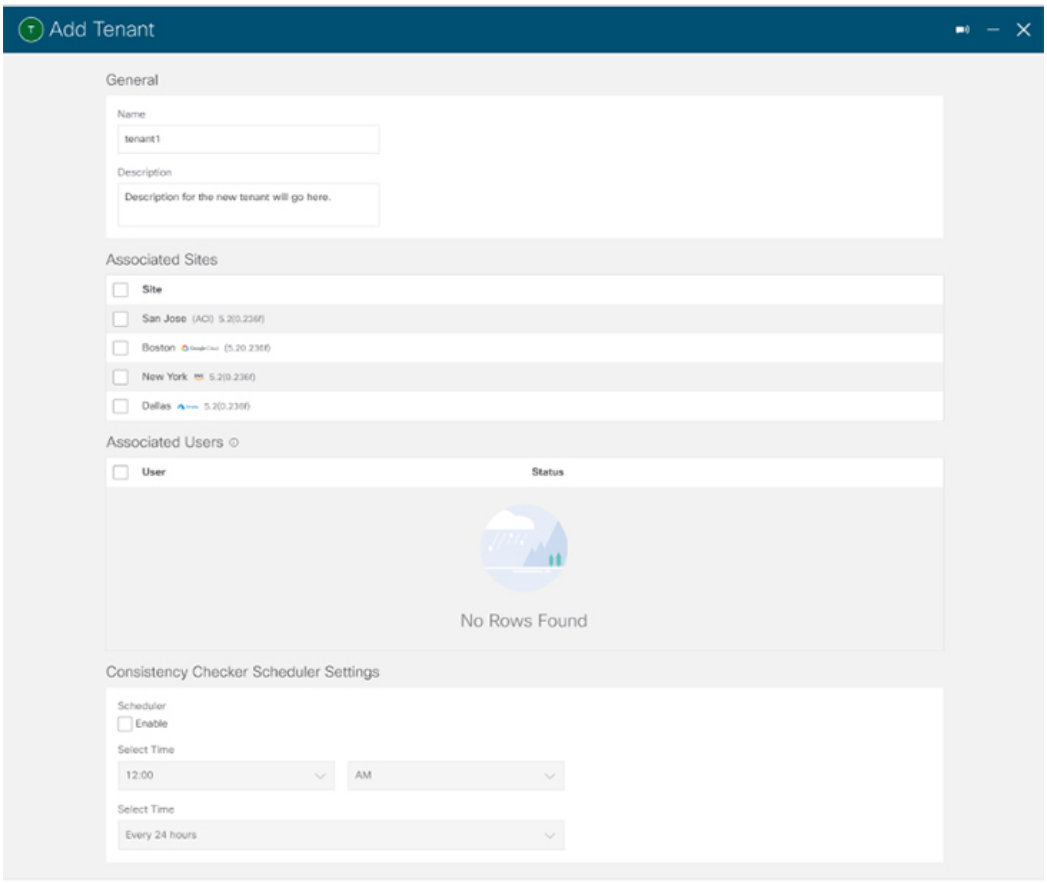
ステップ 4 **[全般（General）]** で、テナント名とオプションの説明を入力します。

テナント名は次のフォーマットにする必要があります：

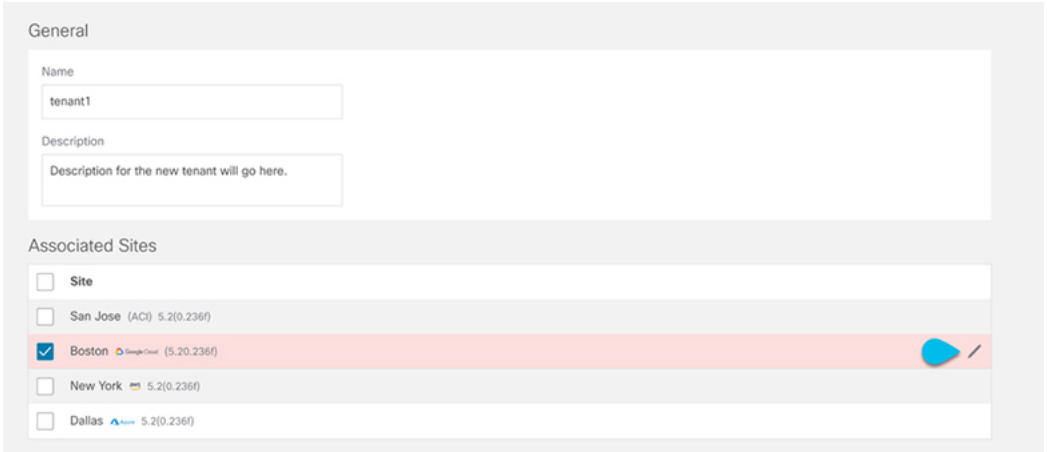
```
[az]([-a-z0-9] * [a-z0-9])?
```

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、または桁にできます。ただし、最後の文字にはハイフンを使用できません。

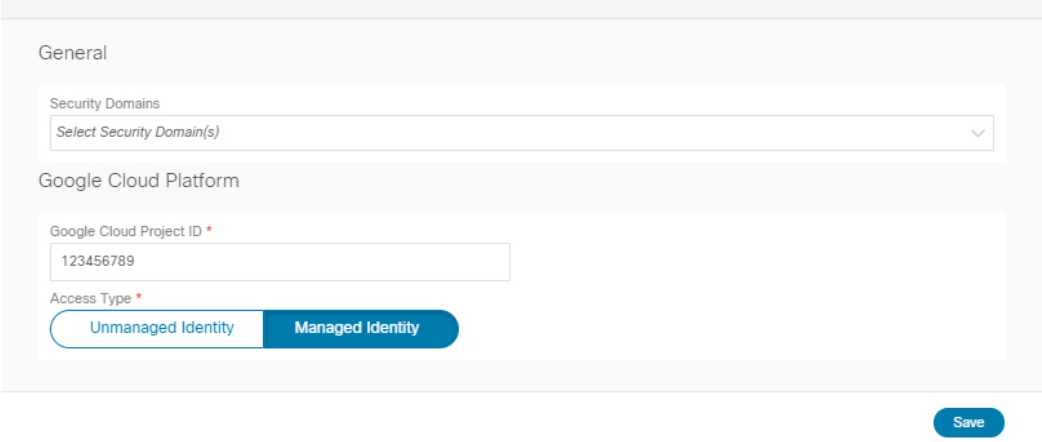
ステップ 5 **[Associated Sites（関連サイト）]** エリアから、テナントを作成する Google Cloud サイトを選択します。



ステップ 6 Google Cloud サイトを選択したら、編集アイコンをクリックしてアカウント情報を指定します。



ステップ 7 必須情報をすべて入力します。

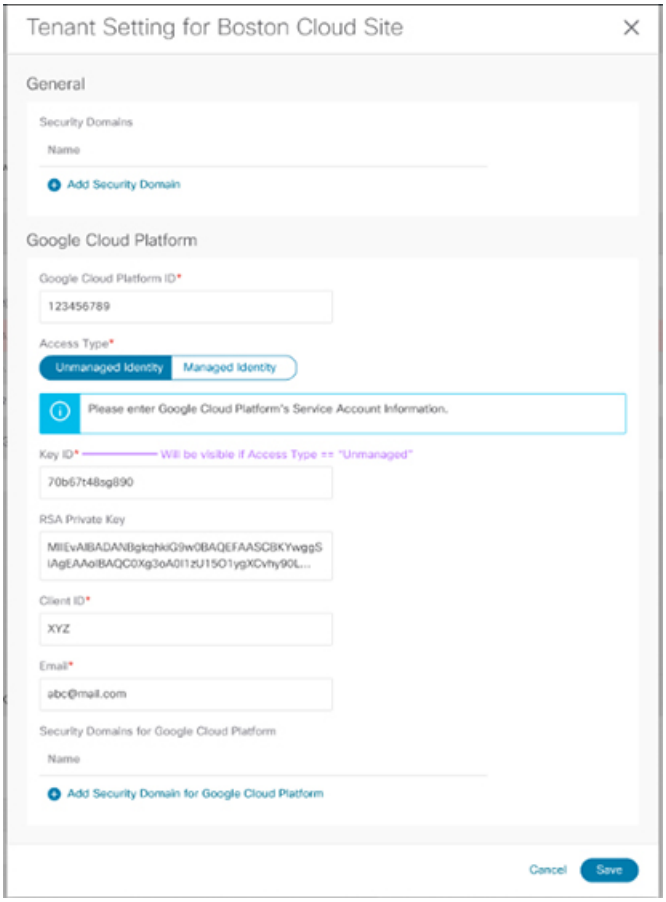


- **[Google Cloud Platform ID（Google Cloud Platform ID）]**：このテナント用に作成した Google Cloud ユーザー アカウントの 識別子 を指定します。
- **[アクセス タイプ（Access type）]**：アクセス タイプの下に 2 つのオプションがあります：
  - Cloud APIC VMがクラウドリソースを管理できるようにするには、**[管理対象アイデンティティ（Managed Identity）]** を選択します。

    管理されたテナントあるいは管理されていないテナントの場合、最初に Google Cloud でプロジェクトを設定する必要があります。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 （41 ページ）を参照してください。
  - 特定のアプリケーションを介してクラウドリソースを管理するには、**[管理されていないアイデンティティ（Unmanaged Identity）]** を選択します。この場合、アプリケーションのクレデンシャルも Cloud API に提供する必要があります。
    - 管理されたテナントあるいは管理されていないテナントの場合、最初に Google Cloud でプロジェクトを設定する必要があります。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 （41 ページ）を参照してください。
    - 管理されていないテナントの場合、必要な秘密キー情報を生成し、Google Cloud から JSON ファイルをダウンロードする必要があります。「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 （44 ページ）」を参照してください。

    アクセス タイプとして **[管理されていない識別子（Unmanaged Identity）]** を選択した場合は、**[キー ID（Key Id）]** と **[クライアント識別子（Client Id）]** フィールドが表示されます。
- **[キー 識別子（Key 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 （44 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。
- **[クライアント識別子（Client 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 （44 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。

- **[E メール（Email）]**：Google Cloud プロジェクトに関連付けられている E メール アドレスを入力します。



ステップ 8 Google Cloud の構成を入力したら、**[保存（Save）]** を選択します。

次のタスク

管理対象テナントを作成している場合は、管理されたテナントのGoogle Cloud で必要なアクセス許可を設定する必要があります。これらの手順については、管理対象テナント用に Google Cloud で必要な権限を設定する （48 ページ） にアクセスしてください。

管理対象テナント用に Google Cloud で必要な権限を設定する

管理対象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、この管理対象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。

Google Cloud サイトのスキーマ、テンプレート、VRF の作成

ステップ 1 メイン メニューで **[スキーマ]** をクリックします。

ステップ 2 [スキーマ（Schema）] 画面で、**[スキーマの追加（Add Schema）]** ボタンをクリックします。

ステップ 3 [Untitled Schema] 画面で、ページの上部にあるテキスト `Untitled Schema`を、作成するスキーマの名前（たとえば、 `schema-1`）に置き換えます。

ステップ 4 最初のテンプレートを構成します。

クラウド ローカル テンプレートを選択します。

ステップ 5 左側のペインで、**テンプレート**の上にマウスを移動し、[メモ] アイコンをクリックします。次に、テンプレートの名前を変更します（例： `template1-gcp`）。

ステップ 6 クラウド テンプレートに移動します。

ステップ 7 VRF で **[VRFを追加（Add VRF）]** を選択し、VRF の表示名と説明を入力します。

ステップ 8 作成した VRF をクリックします。

テンプレート プロパティとサイト ローカル プロパティが画面の右側に表示されます。

ステップ 9 サイト レベルのプロパティで、**[リージョンの追加（Add Region）]** を選択します。

ポップアップで、目的の地域を選択します。

ステップ 10 リージョンを選択したら、**[CIDR の追加（Add CIDR）]** を選択します。

VRF の CIDR 情報を入力します。

- プライマリ CIDR を追加する場合は、**[プライマリ（Primary）]** を選択します。
- セカンダリ CIDR を追加する場合は、**[セカンダリ（Secondary）]** を選択します。

ステップ 11 サブネットとサブネット グループ ラベルを入力します。

サブネットを作成する場合、**Subnet Group Label**を使用して、特定のサブネット グループに一意のラベルを割り当てます。CIDR、サブネット、およびサブネット グループ ラベルの構成の詳細については、[Google Cloud 向け Cisco Cloud APIC ユーザー ガイド（Cisco Cloud APIC for Google Cloud User Guide）]の「Google Cloud の VPC とサブネットと Cloud APIC のクラウド コンテキスト プロファイルについて」を参照してください。

ステップ 12 [保存（Save）] を選択します。

Cloud EPG の作成

すでに行ったインフラ テナント設定（外部 VRF など）とは別のテンプレートとスキーマでクラウド オブジェクトを作成することをお勧めします。

次の手順を使用して、Cloud APIC サイトの新しいスキーマを作成します。この使用例では、1 つのスキーマと 1 つのテンプレートを構成します。

この手順全体では、Nexus Dashboard Orchestrator を使用しています。

ステップ 1 メイン メニューで **[スキーマ]** をクリックします。

ステップ 2 [スキーマ（Schema）] 画面で、**[スキーマの追加（Add Schema）]** ボタンをクリックします。

ステップ 3 [Untitled Schema] 画面で、ページの上部にあるテキスト `Untitled Schema`を、作成するスキーマの名前（たとえば、 `schema-1`）に置き換えます。

ステップ 4 テンプレートを作成します。

Google Cloud サイトに割り当てられたテンプレートは拡張できないため、クラウド ローカル テンプレートを作成します。

a) 左側のペインで、**Template 1** の上にマウスを移動し、[メモ] アイコンをクリックします。次に、テンプレートの名前を変更します（例: Google Cloud の場合、`template1-gcp`）。

b) 中央のペインで、**スキーマを作成するエリアをクリックしてテナントを選択してください** をクリックしてください。

c) 右側のペインで、**[テナントの選択（Select A Tenant）]** ダイアログ ボックスにアクセスし、必要なテナントを選択します。これは、インポートしたGoogle Cloud ユーザー テナントのインポート （40 ページ） または Google Cloud ユーザー テナントの作成 （45 ページ） で作成したテナントです。

ステップ 5 テナントを選択したら、テンプレートに**アプリケーション プロファイル**を作成します。

作成したクラウド EPG をアプリケーション プロファイルに関連付ける必要があります。

ステップ 6 **Cloud EPG** を作成して設定します。

a) **[オブジェクトの作成（Create Object）]** > **[Cloud EPG（Cloud EPGs）]** を選択します。

b) **[アプリケーション プロファイル（Application Profile）]** ドロップダウンから、前の手順で作成したプロファイルを選択します。

c) **[仮想ルーティングと転送（Virtual Routing & Forwarding）]** ドロップダウンから、作成したクラウド VRF を選択します。

d) 右側のプロパティ サイドバーで、この EPG 用に作成したクラウド VRF を選択します。

ステップ 7 先ほど作成したテンプレートを Google Cloud サイトに割り当てます。

ステップ 8 EPG のサイトローカル プロパティを構成します。

a) 左側のサイドバーで、割り当て先のサイトの下にあるテンプレートを選択します。

b) テンプレートのサイトローカルプロパティで、**ルート到達可能性**に対して`[クラウド サイト（Cloud Site）]` を選択します。

クラウド EPG 間の契約の適用

このセクションでは、クラウドサイト内のエンドポイント間の通信を許可する契約を適用する方法について説明します。Google Cloud コントラクトに関して留意すべき 1 つのことは、コントラクトは双方向トラフィックに対して双方向に展開する必要があるということです。

始める前に

クラウド サイトに複数のクラウド EPG Cloud EPG の作成 （50 ページ） がすでに構成されている必要があります。

ステップ 1 メイン メニューで、**[Application Management（アプリケーション管理）]** > **[スキーマ（Schemas）]** を選択します。

ステップ 2 コントラクトを作成し、クラウド EPG に割り当てます。

a) 既存のクラウド EPGを含むスキーマとテンプレートを選択します。

b) このユース ケースに使用する契約を作成します。

Cloud EPG 間の通信に適用する既存の契約がすでにある場合は、この手順をスキップできます。

それ以外の場合は、Cisco ACI ファブリックでの EPG 間通信で通常行うように、コントラクトと必要なフィルタ処理を作成します。

c) クラウド EPG にコントラクトを割り当てます。

特定のユース ケースに基づいて、2 つの EPG のどちらを[プロバイダ（provider）]にし、どちらを[コンシューマ（consumer）]にするかを決定できます。

ステップ 3 別の EPG を選択します。

a) 右側のプロパティ サイド バーから、**[契約の追加（Add contract）]** を選択します。

b) 契約ウィンドウで、割り当てる契約を選択します。

c) 前のステップで割り当てたのと同じ契約を選択します。

d) [保存（Save）] をクリックします。

ステップ 4 テンプレートを展開します。

2 つのクラウド VRF 間のルート リークの構成

この使用例は、2 つの内部クラウド VRF 間のルート リークに焦点を当てています。クラウド サイトに複数のクラウド VRF がすでに設定されている必要があります。クラウド VRF と外部 VRF の間のルート リークを設定する場合（たとえば、Google Cloud サイトから別のサイトへの外部接続を有効にする場合）、Cloud VRF と外部 VRF 間のルート リークを構成 （54 ページ） を参照してください。

.

ステップ 1 メイン メニューで、**[Application Management（アプリケーション管理）]** > **[スキーマ（Schemas）]** を選択します。

ステップ 2 クラウド VRF-1 からクラウド VRF-2 へのルート リークを設定します。

次の手順は、次のルート リークを設定する方法を示しています。

a) 最初のクラウド VRF を含むインフラ テナント テンプレートを作成したスキーマを開きます。
b) **SITES** の下の左側のサイドバーで、クラウド サイトに関連付けられている特定のテンプレートを選択します。
c) サイトローカル プロパティで、テンプレートで定義されているクラウド VRF を選択します。
d) VRF の右側のプロパティ サイドバーで、**[+リーク ルートの追加（+Add Leak Route）]** をクリックします。

[リーク ルートの追加] ダイアログが開きます。

e) [リーク ルートの追加] ダイアログの設定領域で、[VRF の選択] をクリックし、クラウド VRF を選択します。
f) **[リーク ルートの追加]** ダイアログで、**[すべてのルートをリーク]** を選択します。

[すべてをリーク（Leak All）] を選択すると、サブネット IP に `0.0.0.0/0` が入力され、すべてのルートがリークされます。

g) **[保存（Save）]** をクリックして、ルーティング構成を保存します。
h) テンプレートを選択し、**[展開（Deploy）]** をクリックして構成を展開します。

ステップ 3 クラウド VRF-2 からクラウド VRF-1 へのルート リークを構成します。

a) クラウド VRF を定義するテンプレートを含むスキーマを開きます。
b) 左側のサイドバーの **SITES** の下で、特定のクラウド サイトを選択します。
c) サイトローカル プロパティで、クラウド VRF を選択します。
d) VRF の右側のプロパティ サイドバーで、**[+リーク ルートの追加（+Add Leak Route）]** をクリックします。

[リーク ルートの追加] ダイアログが開きます。

e) **[リーク ルートの追加]** ダイアログの設定領域で、**[VRF の選択]** をクリックし、内部 VRF を選択します。

このステップの目的は、クラウド VRF 間のルートをリークすることです。

f) **[リーク ルートの追加]** ダイアログで、**[すべてのルートをリーク]** を選択します。
g) **[保存（Save）]** をクリックして、ルーティング構成を保存します。
h) テンプレートを選択し、**[展開（Deploy）]** をクリックして構成を展開します。

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。