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

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

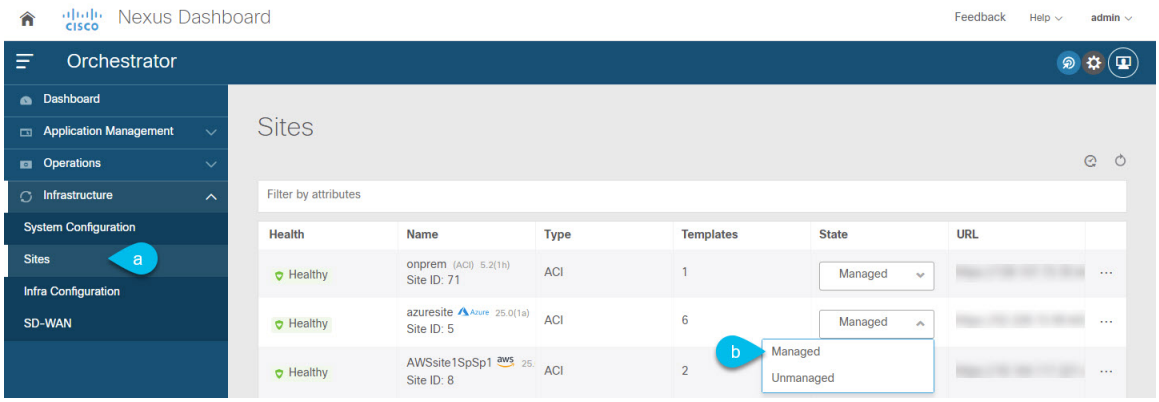
Google Cloud ユーザー テナントのインポート

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 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」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。

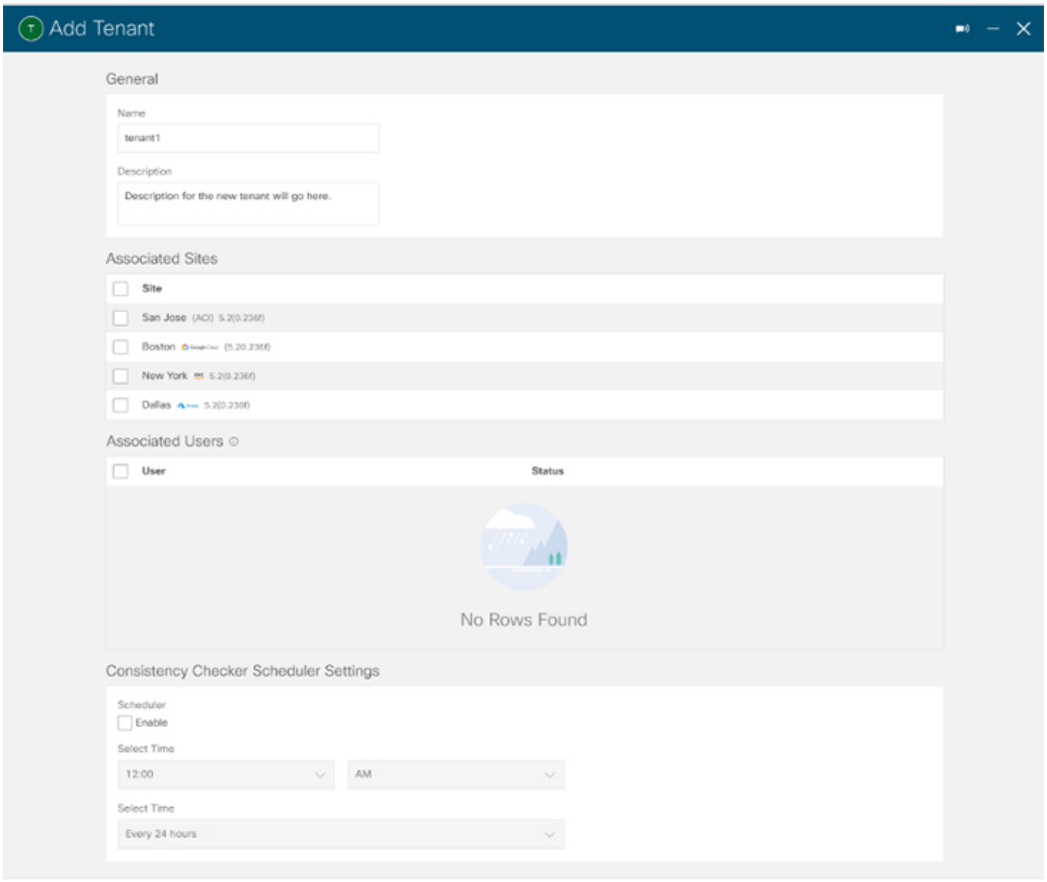
ステップ 4 **[全般（General）]** で、テナント名とオプションの説明を入力します。

テナント名は次のフォーマットにする必要があります：

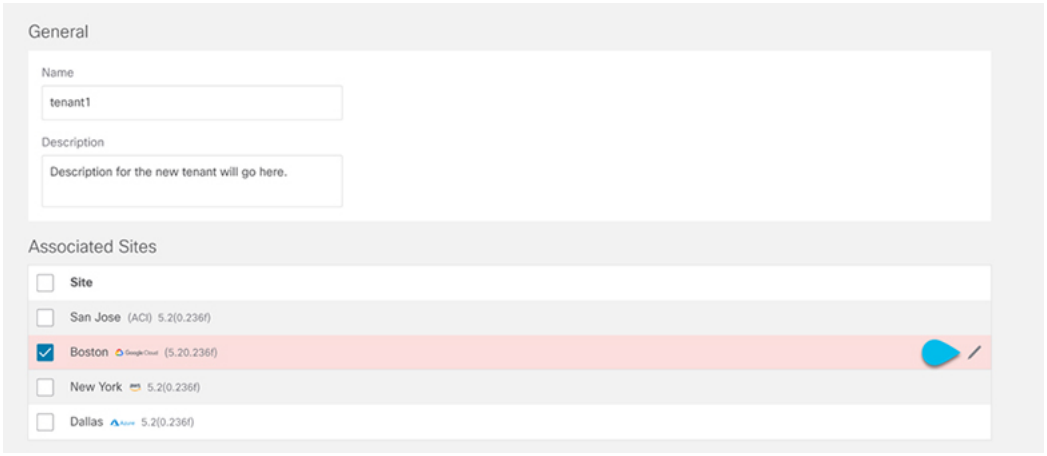
```
[az]（[-a-z0-9] * [a-z0-9]）?
```

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。

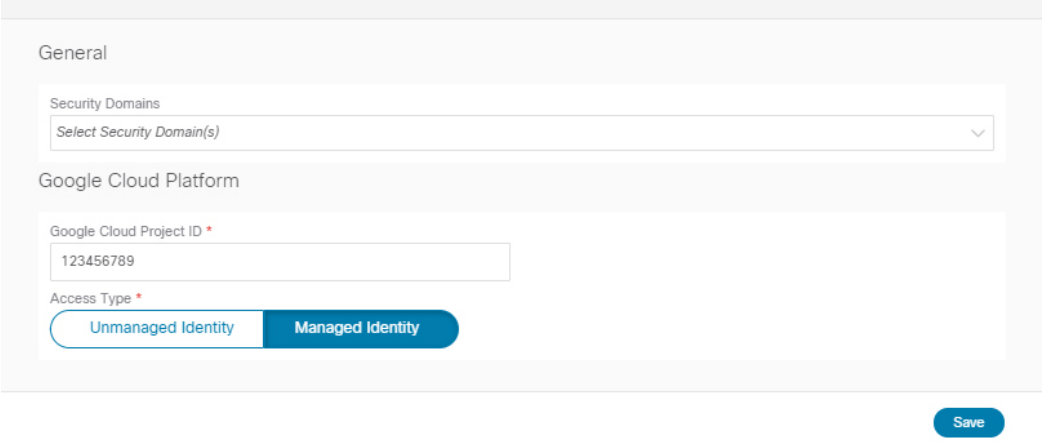
ステップ 5 **[Associated Sites（関連サイト）]** エリアから、テナントを作成する Google Cloud サイトを選択します。



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。



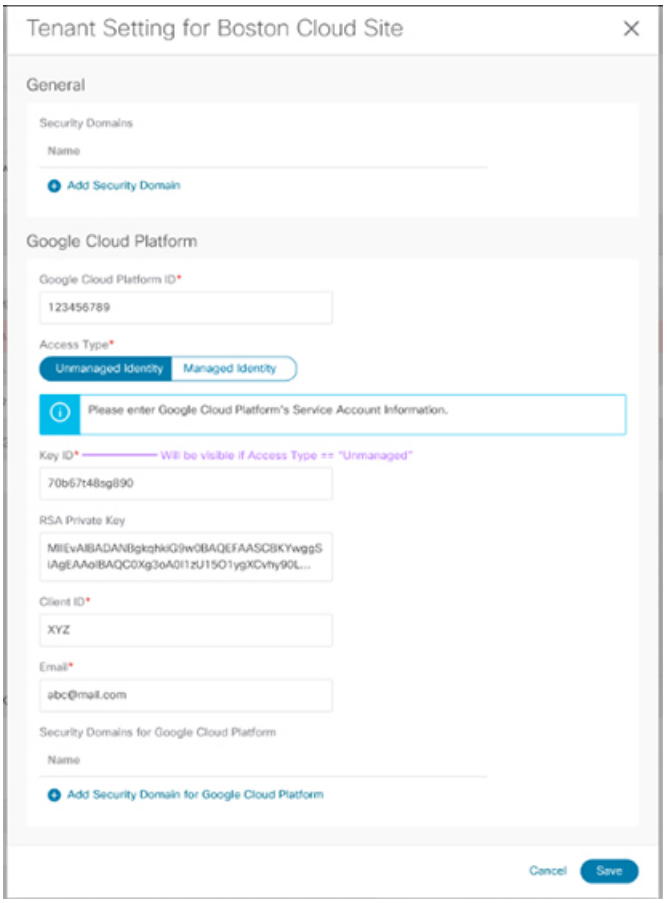
ステップ 7 必須情報をすべて入力します。



- **[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」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 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 または Google Cloud ユーザー テナントの作成 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 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 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。