Google Cloud Platform Virtual Edge デプロイ ガイド

VMware SD-WAN 3.4

最新の技術ドキュメントは、 VMware の Web サイト （https://docs.vmware.com/jp/）

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

Google Cloud Platform Virtual Edge デプロイ ガイド

1

このドキュメントでは、Google Cloud Platform (GCP) で仮想 VMware SD-WAN Edge をデプロイする手順について説明します。

この章には、次のトピックが含まれています。

Google Cloud Virtual Edge のデプロイの概要

多くのユーザーがワークロードをパブリック クラウド インフラストラクチャに移行し、SD-WAN をリモート サイトからパブリック クラウドに拡張して SLA（サービス レベル アグリーメント）を保証しようと取り組んでいます。VMware には複数のオプションが用意されています。分散 VMware SD-WAN Gateways を活用して、パブリック クラウドのプライベート ネットワークのための IPsec を確立したり、Virtual Edge を Google Cloud Platform (GCP) に直接デプロイしたりすることができます。

1G 未満のスループットを必要とする小規模なブランチの場合は、単一の Virtual Edge をプライベート GCP ネットワークにデプロイできます。数ギガビットのスループットを必要とする大規模なデータセンター環境の場合は、Hub クラスタリングをデプロイできます。

注： VMware SD-WAN Hub クラスタリング設計では、レイヤー 3 インスタンスを LAN 側で利用して、クラスタ内の Hub とレイヤー 3 インスタンスとの間で BGP を実行し、LAN でルートを分散します。GCP ルーターは動的ルーティング プロトコルをサポートしていないため、GCP インフラストラクチャにはサードパーティ製の仮想ルーターが必要です。

このドキュメントでは、基本的なトポロジと、GCP に仮想 SD-WAN Edge (vVCE) をデプロイするための概要レベルのワークフローについて説明します。GCP での Virtual Edge のデプロイを参照してください。

前提条件

- GCP アカウントとログイン情報。
- GCP ネットワークに関する十分な知識。詳細については、https://cloud.google.com/vpc/docs/overview を参照してください。
- SD-WAN Orchestrator のターゲットおよびログインのための管理者アカウント。

GCP マシン タイプ

VMware SD-WAN Virtual Edge のサイズを設定するときには、帯域幅のスループットとネットワーク インターフェイスの数を考慮する必要があります。必要なネットワーク インターフェイスの最小数は 3 です（GE1、GE2、GE3）。

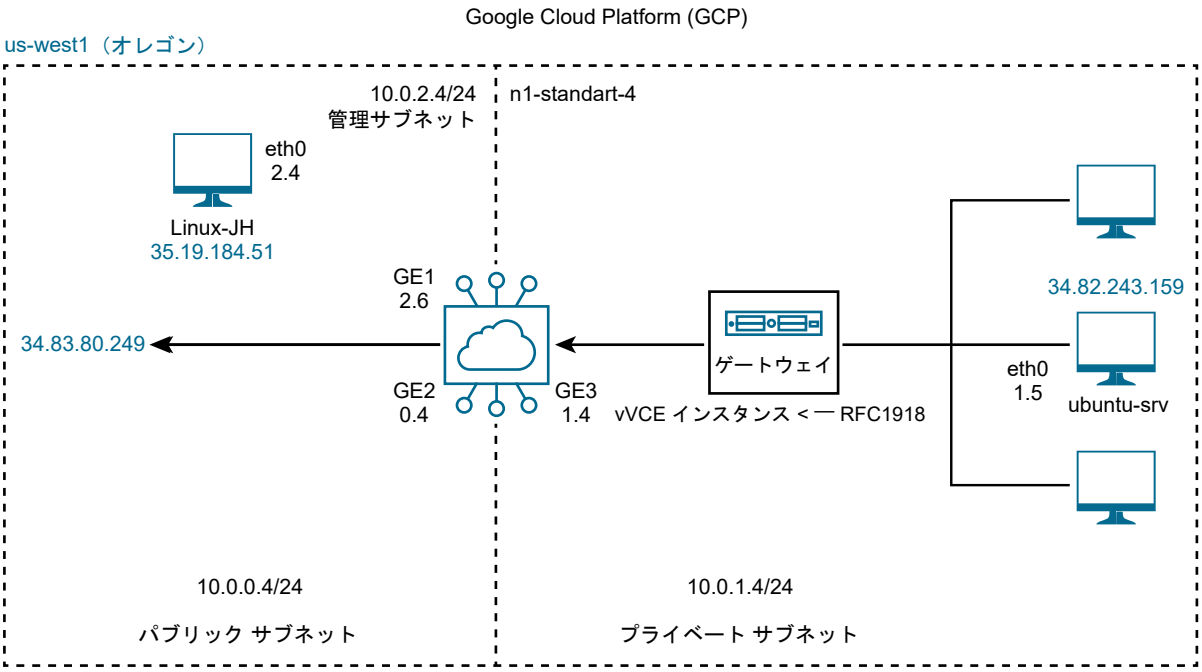
スループット	30 Mbps	50 Mbps	100 Mbps	200 Mbps	400 Mbps	1 Gbps
vCPU	2	2	2	2	4	4
メモリ	4 GB	4 GB	4 GB	8 GB	8 GB	8 GB

マシン タイプ	vCPU 数	メモリ (Gb)	最大 NIC 数
n1-standard-4	4	15	4
n1-standard-8	8	30	8

GCP での Virtual Edge のデプロイ

次のトポロジ図に示すように、管理 VPC (10.0.2.x/24)、パブリック VPC (10.0.0.x/24)、およびプライベート VPC (10.0.1.x/24) の 3 つの VPC ネットワーク（Edge に接続されたサブネットごとに 1 つ）がある Google Cloud Virtual Private Cloud (VPC) 上での Virtual Edge のデプロイについて説明します。

基本的なトポロジ



Virtual Edge は、2 つのサブネット間でルーティングされます。パブリック VPC ルートは、すべてのオフネット トラフィックをインターネット ゲートウェイに転送します。プライベート サブネット内のゲートウェイ ルーターは、Virtual Edge (GE3) 上の LAN に接続するインターフェイスにすべてのトラフィックを転送します。この例では、デフォルト ルートを使用して、ワークロードから「すべて」のトラフィックを転送していますが、必須ではありません。RFC1918 集約または特定のブランチ/ハブ プリフィックスを使用して、Virtual Edge に送信されるトラフィックを絞り込むことができます。たとえば、プライベート サブネット内のワークロードにパブリック送信元 IP アドレスから SSH 接続でアクセスできるようにする必要がある場合は、デフォルト ルート (0.0.0.0/0) がインターネット ゲートウェイを指すように、また、RFC1918 集約が Virtual Edge を指すように VPC ルーターを構成することもできます。

ワークフローの概要

VMware SD-WAN Virtual Edge を Google Cloud Platform にデプロイするには、次の手順を実行します。

1 GCP 環境の準備：

a 3 つの Virtual Private Cloud (VPC) ネットワーク（管理 VPC ネットワーク、パブリック VPC ネットワーク、プライベート VPC ネットワーク）を作成し、トポロジ図に示すように、それぞれを Edge (n1-standard-4) に接続するサブネットに使用します。

- 管理インターフェイス GE1 を介した Edge へのコンソール/管理アクセスのための管理サブネット。
- WAN 側インターフェイス GE2 を介した Edge からのインターネット アクセスのためのパブリック サブネット。
- LAN 側インターフェイス GE3 を介した LAN 側のデバイス アクセスのためのプライベート サブネット。

手順については、VPC ネットワークの作成を参照してください。

b VPC ネットワーク（管理、プライベート、パブリック）の受信ファイアウォール ルールを作成します。手順については、受信ファイアウォール ルールの作成を参照してください。

c Edge を指すプライベート VPC ネットワークのルート テーブルに、Edge の GE3 インターフェイスの IP アドレスとしてネクスト ホップ IP アドレスを指定して、新しいデフォルト ルート (0.0.0.0/0) エントリを追加します。

手順については、VPC ネットワークでのルートの作成を参照してください。

2 次のように、VMware SD-WAN Orchestrator で SD-WAN Edge をプロビジョニングします。

a [Virtual Edge] タイプの Edge を作成します。

b GE1 インターフェイスを [スイッチ (Switched)] から [ルーティング (Routed)] に変更し、[WAN オーバーレイ (WAN Overlay)] と [NAT ダイレクト トラフィック (NAT Direct Traffic)] を無効にします。

c GE2 インターフェイスを [スイッチ (Switched)] から [ルーティング (Routed)] に変更し、[WAN オーバーレイ (WAN Overlay)] と [NAT ダイレクト トラフィック (NAT Direct Traffic)] を有効にします。

d GE3 インターフェイスについては、[WAN オーバーレイ (WAN Overlay)] と [NAT ダイレクト トラフィック (NAT Direct Traffic)] を無効にします。このインターフェイスは、プライベート サブネット（LAN デバイス）に接続されているデバイスのネクスト ホップになります。

詳細については、SD-WAN Orchestrator での Edge のプロビジョニングを参照してください。

3 Virtual Edge をデプロイします。次のいずれかの方法を使用して、Virtual Edge をデプロイできます。

- GCP マーケットプレイスからの Virtual Edge のデプロイ
- GCP Deployment Manager を使用した Virtual Edge のデプロイ

4 SD-WAN Orchestrator で Virtual Edge が稼動しているかどうかを確認します。

GCP 環境の準備

Google Cloud Platform (GCP) に Virtual Edge をデプロイする前に、次の手順を実行して GCP 環境を準備する必要があります。

- VPC ネットワークの作成
- 受信ファイアウォール ルールの作成
- VPC ネットワークでのルートの作成

VPC ネットワークの作成

自動モードまたはカスタム モードを選択して Virtual Private Cloud (VPC) ネットワークを作成できます。自動モードのネットワークでは、ネットワークの作成時に、Google Cloud リージョンごとに 1 つのサブネットが自動的に作成されます。カスタム モードの VPC ネットワークの場合は、ネットワークを作成してから、必要なサブネットをリージョン内に作成する必要があります。ネットワークの作成時にサブネットを作成することも、後でサブネットを追加することもできますが、サブネットが定義されていないリージョンにインスタンスを作成することはできません。

前提条件

Google Cloud Platform (GCP) コンソールに対する Google アカウントとアクセス/ログイン情報があることを確認します。

手順

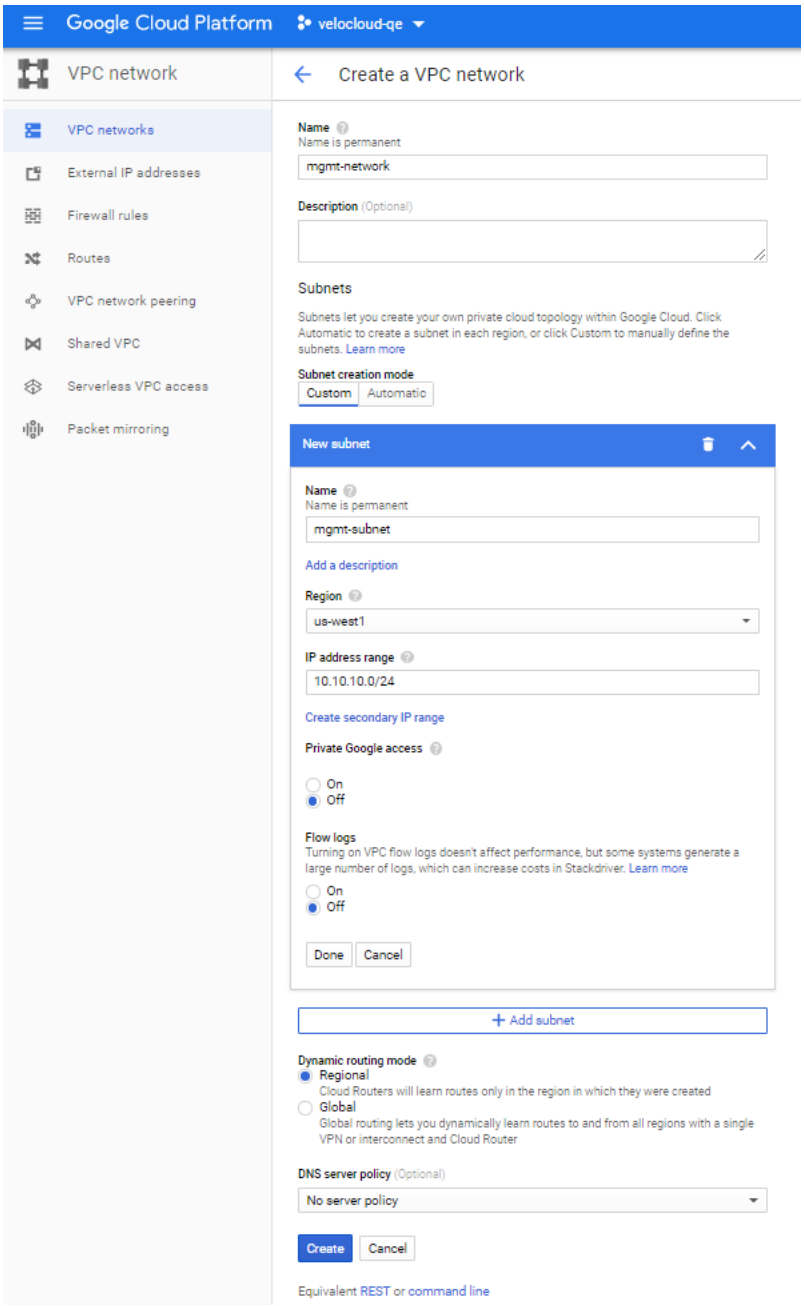
1 GCP コンソールにログインします。

2 [VPC ネットワーク (VPC Networks)] をクリックします。

[VPC ネットワーク (VPC Networks)] ページが表示されます。

3 [VPC ネットワークの作成 (Create VPC network)] をクリックします。

[VPC ネットワークの作成 (Create a VPC network)] ページが表示されます。



4 [名前 (Name)] テキスト ボックスに、VPC ネットワークの一意の名前を入力します。

5 [サブネット (Subnets)] で、[サブネットの作成モード (Subnet creation mode)] として [カスタム (Custom)] または [自動 (Automatic)] を選択します。[カスタム (Custom)] を選択した場合は、[新規サブネット (New subnet)] 領域で、サブネットの次の構成パラメータを指定します。

a [名前 (Name)] テキスト ボックスに、サブネットの一意の名前を入力します。

b [リージョン (Region)] ドロップダウン メニューから、サブネットのリージョンを選択します。

c [IP アドレス範囲 (IP address range)] テキスト ボックスに、IP アドレスの範囲を入力します。

d サブネットのセカンダリ IP アドレス範囲を定義するには、[セカンダリ IP アドレス範囲の作成 (Create secondary IP range)] をクリックします。

e [プライベート Google アクセス (Private Google access)]：サブネットのプライベート Google アクセスをサブネットの作成時に有効にするか、後で編集して有効にするかを選択します。

f [フロー ログ (Flow logs)]：サブネットの VPC フロー ログをサブネットの作成時に有効にするか、後で編集して有効にするかを選択します。

g [完了 (Done)] をクリックします。

6 サブネットをさらに追加するには、[サブネットの追加 (Add subnet)] をクリックして、手順 5 の操作を繰り返します。ネットワークの作成後にさらにサブネットをネットワークに追加することもできます。

7 VPC ネットワークの [動的ルーティング モード (Dynamic routing mode)] を選択します。

8 [作成 (Create)] をクリックします。

結果

VPC ネットワークとサブネットが作成されます。

次のステップ

受信ファイアウォール ルールの作成

受信ファイアウォール ルールの作成

ファイアウォール ルールはネットワーク レベルで定義され、作成先のネットワークにのみ適用されます。VPC ネットワークの受信ファイアウォール ルールを作成するには、次の手順を実行します。

前提条件

- Google Cloud Platform (GCP) コンソールに対する Google アカウントとアクセス/ログイン情報があることを確認します。
- VPC ネットワークが作成されていることを確認します。
- ファイアウォール ルールのコンポーネントを確認し、Google Cloud で使用されるファイアウォール構成コンポーネントについて理解しておきます。

手順

1 GCP コンソールにログインします。

2 [VPC ネットワーク (VPC Networks)] をクリックします。

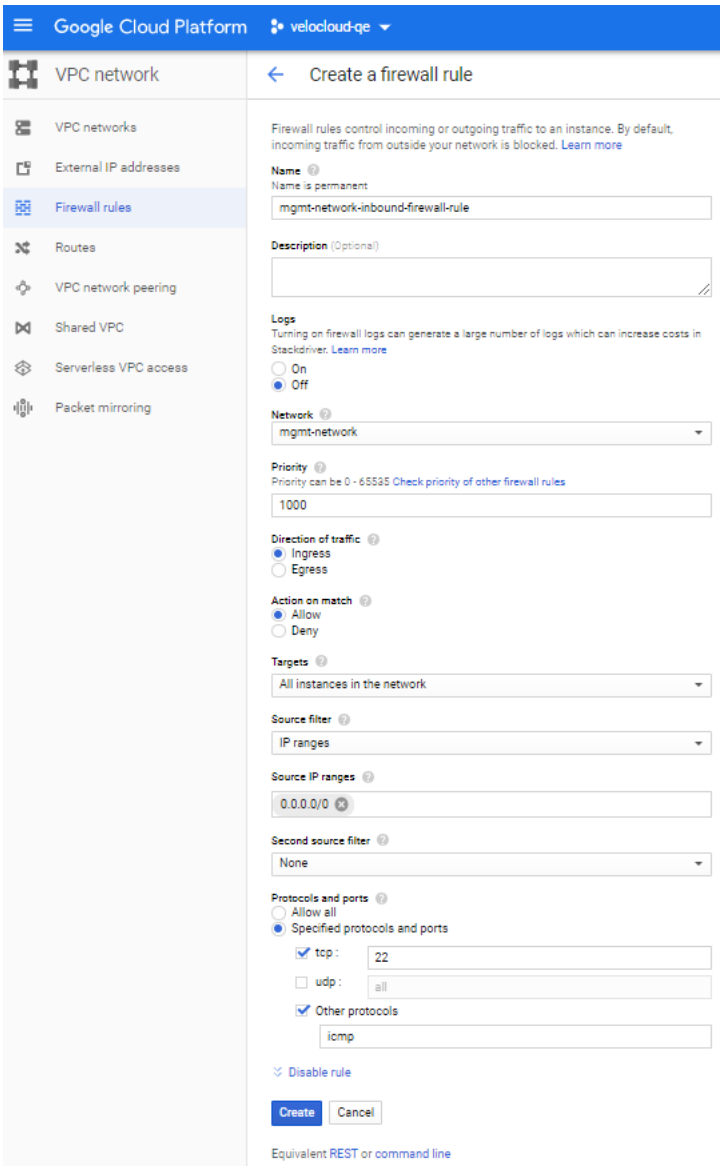
[VPC ネットワーク (VPC Networks)] ページが表示されます。

3 ファイアウォール ルールを追加する VPC ネットワークをクリックします。

選択した VPC ネットワークの [VPC ネットワークの詳細 (VPC network details)] ページが表示されます。

4 [ファイアウォール ルール (Firewall rules)] タブに移動して、[ファイアウォール ルールの追加 (Add firewall rule)] をクリックします。

[ファイアウォール ルールの作成 (Create a firewall rule)] ページが表示されます。



5 [名前 (Name)] テキスト ボックスに、ファイアウォール ルールの一意の名前を入力します。

6 必要な場合は、[ログ (Logs)] の下の [オン (On)] をクリックして、ファイアウォール ログを有効にすることができます。デフォルトでは、ファイアウォール ログは無効になっています。

7 [トラフィックの方向 (Direction of traffic)] で、[入力方向 (Ingress)] を選択します。

8 [一致した場合のアクション (Action on match)] で、[許可 (Allow)] または [拒否 (Deny)] を選択します。

9 [ターゲット (Targets)] ドロップダウン メニューから、ルールのターゲットを選択します。

- ネットワーク内のすべてのインスタンスにルールを適用する場合は、[ネットワーク内のすべてのインスタンス (All instances in the network)] を選択します。

- ネットワーク（ターゲット）タグを使用して特定のインスタンスにルールを適用する場合は、[指定されたターゲット タグ (Specified target tag)] を選択してから、ルールを適用するタグを [ターゲット タグ (Target tags)] テキスト ボックスに入力します。
- 関連付けられたサービス アカウントを使用して特定のインスタンスにルールを適用する場合は、[指定されたサービス アカウント (Specified service account)] を選択し、[サービス アカウントの範囲 (Service account scope)] で、サービス アカウントが現在のプロジェクトに含まれているか、別のプロジェクトのものであるかを指定します。それから、[ターゲット サービス アカウント (Target service account)] フィールドで、サービス アカウント名を選択するか入力します。

10 [送信元フィルタ (Source filter)] ドロップダウン メニューから、[IP アドレス範囲 (IP ranges)] を選択します。

11 [送信元 IP アドレス範囲 (Source IP ranges)] テキスト ボックスに CIDR ブロックを入力して、IP アドレス範囲で受信トラフィックの送信元を定義します。任意のネットワークからの送信元の場合、`0.0.0.0/0` を使用します。

12 ルールが適用される [プロトコルとポート (Protocols and ports)] を定義します。

- すべてのプロトコルとポートにルールを適用するには、アクションに応じて [すべて許可 (Allow all)] または [すべて拒否 (Deny all)] を選択します。
- 特定のプロトコルとポートを定義します。
  - TCP プロトコルとポートを含めるには、[tcp] を選択します。`all` と入力するか、`20–22, 80, 8080` のようにポートのカンマ区切りリストを入力します。
  - UDP プロトコルとポートを含めるには、[udp] を選択します。`all` と入力するか、`67–69, 123` のようにポートのカンマ区切りリストを入力します。
  - 必要に応じて、[その他のプロトコル (Other protocols)] を選択して、ICMP、VCMP、SNMP などのプロトコルを含めます。

13 （オプション）適用状態を無効に設定して、ファイアウォール ルールを適用せずに作成することもできます。[ルールの無効化 (Disable rule)] をクリックしてから、[無効 (Disabled)] を選択します。

14 [作成 (Create)] をクリックします。

結果

選択した VPC ネットワークのファイアウォール ルールが作成されます。

次のステップ

- VPC ネットワークでのルートの作成

VPC ネットワークでのルートの作成

トポロジ図に示すように、Edge を指すプライベート Virtual Private Cloud (VPC) ネットワークに新しいデフォルト ルートを追加する方法について説明します。

前提条件

- Google Cloud Platform (GCP) コンソールに対する Google アカウントとアクセス/ログイン情報があることを確認します。
- VPC ネットワークが作成されていることを確認します。

手順

1 GCP コンソールにログインします。

2 [VPC ネットワーク (VPC Networks)] をクリックします。

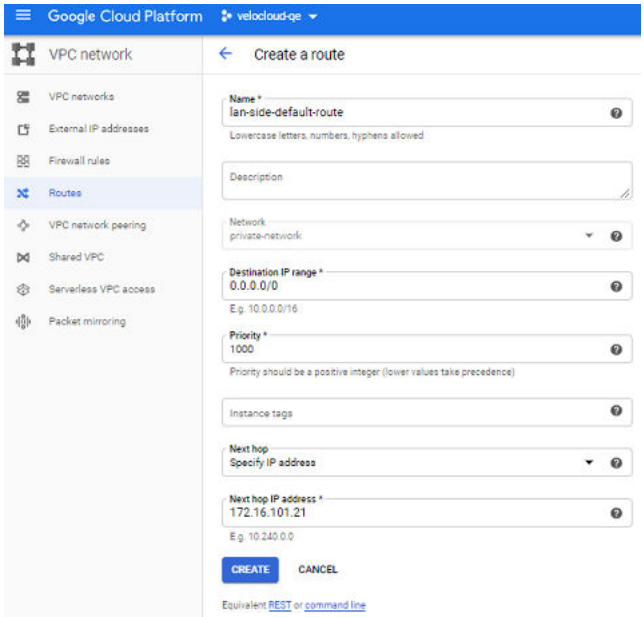
[VPC ネットワーク (VPC Networks)] ページが表示されます。

3 新しいデフォルト ルートを追加する VPC ネットワーク（プライベート VPC ネットワーク）をクリックします。

[VPC ネットワークの詳細 (VPC network details)] ページが表示されます。

4 [ルート (Routes)] タブに移動し、VPC ネットワークの作成中に作成されたデフォルト ルートを削除します。

5 [ルートの追加 (Add route)] をクリックします。[ルートの作成 (Create a route)] ページが表示されます。



a [名前 (Name)] テキスト ボックスに、ルート エントリの一意の名前を入力します。

b [宛先 IP アドレス範囲 (Destination IP range)] テキスト ボックスに、新しいデフォルト ルート（たとえば 0.0.0.0/0）を指定します。

c [優先度 (Priority)] テキスト ボックスで、ルートの優先順位を指定します。優先順位は、ルートの宛先が同等の場合にルーティングの順序を決定するためにのみ使用されます。

d [ネクスト ホップ (Next hop)] ドロップダウン メニューで、[IP アドレスの指定 (Specify IP address)] を選択します。

e [ネクスト ホップの IP アドレス (Next hop IP address)] テキスト ボックスに、選択した VPC ネットワークの Edge インターフェイスの IP アドレスを入力します。

f [作成 (Create)] をクリックします。

結果

ルート エントリが選択した VPC ネットワークのルート テーブルに追加されます。

VPC ネットワークでのブランチ間ルートの追加

シングルアーム トポロジに示すように Edge を指すパブリック Virtual Private Cloud (VPC) ネットワークにブランチ間ルートを追加する方法について説明します。

前提条件

- Google Cloud Platform (GCP) コンソールに対する Google アカウントとアクセス/ログイン情報があることを確認します。
- VPC ネットワークが作成されていることを確認します。

手順

1 GCP コンソールにログインします。

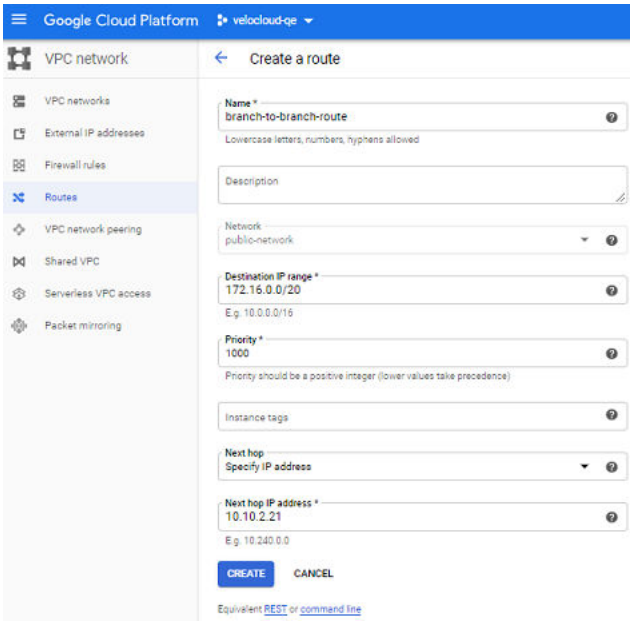
2 [VPC ネットワーク (VPC Networks)] をクリックします。

[VPC ネットワーク (VPC Networks)] ページが表示されます。

3 ブランチ間ルートを追加する VPC ネットワーク（パブリック VPC ネットワーク）をクリックします。

[VPC ネットワークの詳細 (VPC network details)] ページが表示されます。

4 [ルート (Routes)] タブに移動して、[ルートの追加 (Add route)] をクリックします。[ルートの作成 (Create a route)] ページが表示されます。



a [名前 (Name)] テキスト ボックスに、ルート エントリの一意の名前を入力します。

b [宛先 IP アドレス範囲 (Destination IP range)] テキスト ボックスで、エンタープライズ ネットワーク内のブランチの IP アドレス（たとえば 172.16.0.0/20）を指定します。

c [優先度 (Priority)] テキスト ボックスで、ルートの優先順位を指定します。優先順位は、ルートの宛先が同等の場合にルーティングの順序を決定するためにのみ使用されます。

d [ネクスト ホップ (Next hop)] ドロップダウン メニューで、[IP アドレスの指定 (Specify IP address)] を選択します。

e [ネクスト ホップの IP アドレス (Next hop IP address)] テキスト ボックスに、選択した VPC ネットワークの Edge インターフェイスの IP アドレスを入力します。

f [作成 (Create)] をクリックします。

結果

ルート エントリが選択した VPC ネットワークのルート テーブルに追加されます。

SD-WAN Orchestrator での Edge のプロビジョニング

SD-WAN Edge をプロビジョニングするには、次の手順を実行します。

前提条件

ログインするための SD-WAN Orchestrator ホスト名と管理者アカウントがあることを確認します。

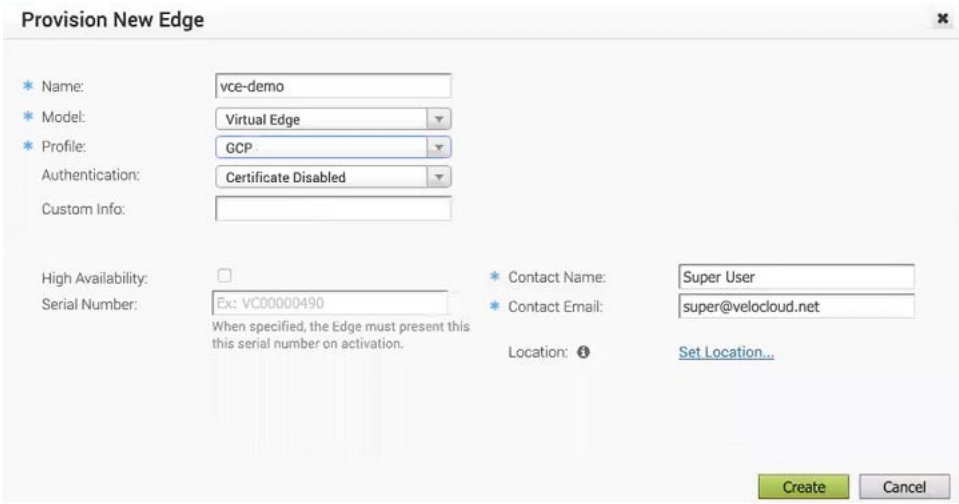
手順

1 ログイン認証情報を使用して、SD-WAN Orchestrator アプリケーションに管理者ユーザーとしてログインします。

2 [構成 (Configure)] > [Edge (Edges)] に移動します。

3 [新規 Edge (New Edge)] をクリックします。

[新規 Edge のプロビジョニング (Provision New Edge)] ダイアログ ボックスが表示されます。



4 [名前 (Name)] テキスト ボックスに、Edge の一意の名前を入力します。

5 [モデル (Model)] ドロップダウン メニューから、[Virtual Edge] を選択します。

6 [プロファイル (Profile)] ドロップダウン メニューから、[クイック スタート プロファイル (Quick Start Profile)] を選択し、[作成 (Create)] をクリックします。

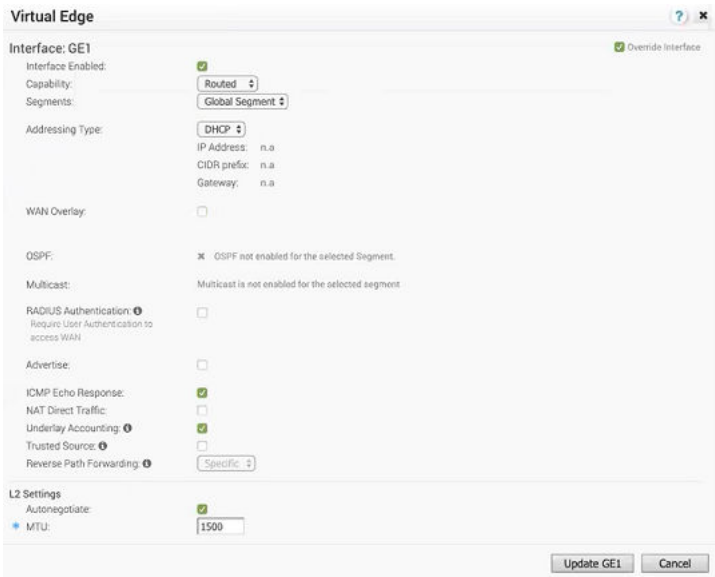
Edge がプロビジョニングされ、アクティベーション キーがページの上部に表示されます。Google Cloud Platform (GCP) コンソールから Edge を起動するときに必要となるため、アクティベーション キーをメモしておきます。

7 Virtual Edge インターフェイスを構成します。次の手順の説明では、GCP での Virtual Edge のデプロイを想定しています。

a [デバイス (Device)] タブをクリックし、[インターフェイス設定 (Interface Settings)] 領域に移動します。

b 次のようにして、インターフェイスに対応する [編集 (Edit)] をクリックし、[インターフェイスのオーバーライド (Override Interface)] チェックボックスをオンにして、Virtual Edge インターフェイス（[GE1 インターフェイス]、[GE2 インターフェイス]、[GE3 インターフェイス]）の構成を更新します。

- [GE1] インターフェイスの機能を [ルーティング (Routed)] に変更し、[WAN オーバーレイ (WAN Overlay)] と [NAT ダイレクト トラフィック (NAT Direct Traffic)] を無効にします。
- [GE2] インターフェイスの機能を [ルーティング (Routed)] に変更し、[WAN オーバーレイ (WAN Overlay)] と [NAT ダイレクト トラフィック (NAT Direct Traffic)] が有効になっていることを確認します。
- [GE3] インターフェイスについては、[WAN オーバーレイ (WAN Overlay)] と [NAT ダイレクト トラフィック (NAT Direct Traffic)] を無効にします。このインターフェイスは、プライベート VPC サブネット（LAN デバイス）に接続されているデバイスのネクスト ホップになります。



結果

Virtual Edge は SD-WAN Orchestrator にプロビジョニングされます。

次のステップ

GCP に Virtual Edge をデプロイします。次のいずれかの方法を使用して、Virtual Edge をデプロイできます。

- GCP マーケットプレイスからの Virtual Edge のデプロイ
- GCP Deployment Manager を使用した Virtual Edge のデプロイ

GCP マーケットプレイスからの Virtual Edge のデプロイ

Google Cloud コンソールで、起動ディスク イメージ、起動ディスク スナップショット、またはコンテナ イメージを使用して、仮想マシン (VM) インスタンスを作成およびデプロイできます。起動ディスク イメージを使用して仮想マシン (VM) インスタンスを作成およびデプロイするには、次の手順を実行します。

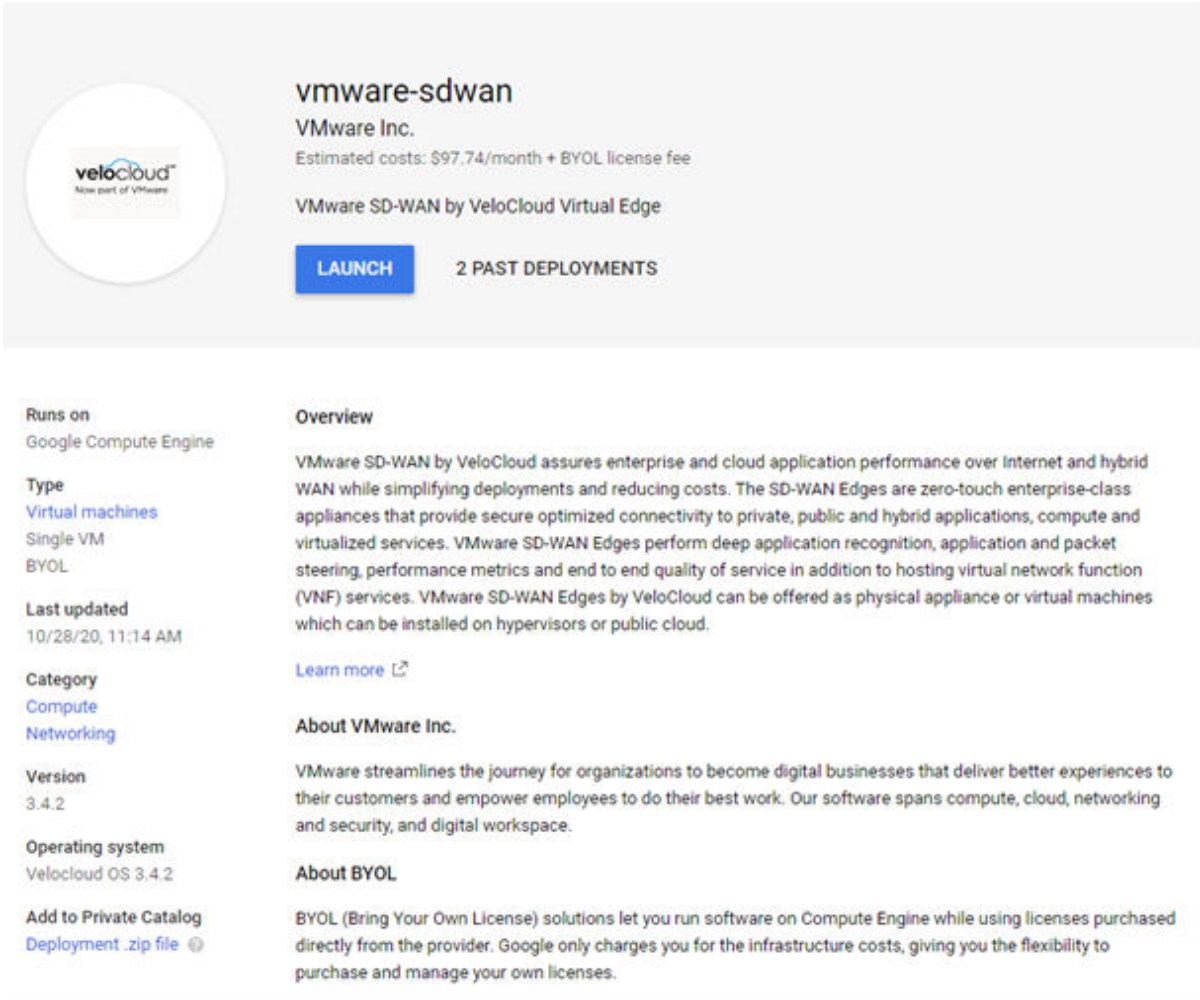
前提条件

Google Cloud Platform (GCP) コンソールに対する Google アカウントとアクセス/ログイン情報があることを確認します。

手順

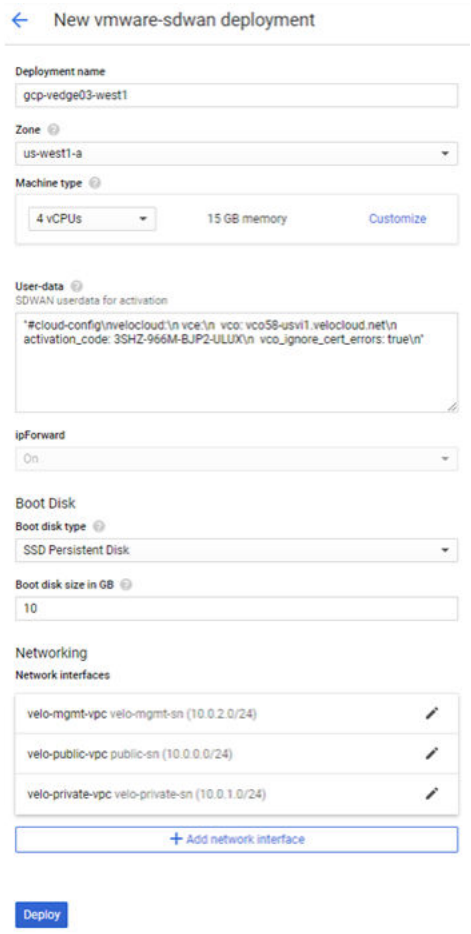
1 GCP コンソールにログインします。

2 VMware SD-WAN は GCP マーケットプレイスで利用できるようになりました。マーケットプレイスで VMware SD-WAN を検索して開始してください。



3 [運用開始 (LAUNCH)] をクリックします。

[インスタンスの作成 (Create an instance)] ページが表示されます。



4 [デプロイ名 (Deployment name)] テキスト ボックスに、インスタンスの一意の名前を入力します。

5 [ゾーン (Zone)] ドロップダウン メニューから、VPC ネットワークを作成するリージョンを選択します。

6 インスタンスのマシン構成を選択します。[マシン タイプ (Machine type)] ドロップダウン メニューから、構成されているトポロジに基づいてオプションを選択します。

7 [ユーザーデータ (User-data)] フィールドで、ターゲット VMware SD-WAN Orchestrator に対して Virtual Edge を有効にするために次のサンプル形式で cloud-init 情報を指定します。

cloud-init ユーザーデータのサンプル

```
"#cloud-config\nvelocloud:\n vce:\n  vco: vco58-usvi1.velocloud.net\n  activation_code: 3SHZ-966M-BJP2-ULUX\n  vco_ignore_cert_errors: false\n"
```

処理を成功させるには正しい形式であることが非常に重要です。形式が正しくないと、アクティベーションはサイレントに失敗します（Orchestrator でエラー イベントが発生しません）。

`#cloud-config` は引用符で囲む必要があります。そうしないと、起動時に GCP がエラーをスローします。引用符は、[ユーザーデータ (User-data)] フィールドにすでに含まれています。引用符の間に cloud-config を挿入するか、サンプルの cloud-init ユーザーデータを切り取って貼り付け、[ユーザーデータ (User-data)] フィールドのすべてのテキストを置換することができます。

注： 解析を機能させるには、改行 (\n) 文字とスペースが正確である必要があります。上記のサンプルを切り取ってメモ帳に貼り付け、スペースを変更せずに必要に応じて値を置き換えることをお勧めします。

SSH キーはプロジェクト レベルで管理されます。https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys を参照してください。

8 IP アドレス転送により、Virtual Edge 上のインターフェイスは、ローカル インターフェイスの MAC アドレス宛てではないパケットを処理できます。IP アドレス転送はデフォルトで有効になっています。これは適切なルーティングが機能するために必要であり、変更することはできません。

9 [起動ディスク (Boot disk)] 領域で、ブート イメージのディスク タイプとサイズはデフォルト値（SSD パーシステント ディスクと 10 GB）のままにする必要があります。

10 [ネットワーク (Networking)] 領域で、次のようにして、構成した VPC ネットワークのインターフェイスを追加します。

a [ネットワーク インターフェイス (Network interfaces)] で、[+ ネットワーク インターフェイスの追加 (+ Add Network Interface)] アイコンをクリックします。

b [ネットワーク (Network)] ドロップダウン メニューから、インターフェイスを追加するネットワークを選択します。

c 外部 IP アドレスを次のように構成します。

- 管理ネットワークの場合：[外部 IP アドレス (External IP)] について [なし (None)] を選択します。
- パブリック ネットワークの場合：このインターフェイスをパブリック インターネット IP アドレスにマッピングする必要があるため、[外部 IP アドレス：短期 (External IP: Ephemeral)] を選択します。
- プライベート ネットワークの場合 - [外部 IP アドレス (External IP)] について [なし (None)] を選択します。

d [完了 (Done)] をクリックします。

e 別のインターフェイスを追加するには、[ネットワーク インターフェイスの追加 (Add network interface)] をクリックし、上記の手順 b から d を繰り返します。

11 [デプロイ (Deploy)] をクリックします。

結果

Virtual Edge インスタンスが作成され、作成後にコンピューティング エンジンによって自動的に開始されます。

次のステップ

Edge のアクティベーションの確認

GCP Deployment Manager を使用した Virtual Edge のデプロイ

Deployment Manager を使用して VMware SD-WAN Virtual Edge を Google Cloud Platform にデプロイするには、次の手順を実行します。

1 GCP で Cloud Deployment Manager API を有効にします。手順については、Deployment Manager の有効化を参照してください。

2 次のように、SD-WAN Orchestrator で SD-WAN Edge をプロビジョニングします。

   a タイプが [Virtual Edge] の Edge を作成し、Edge のプロビジョニング後に画面の上部に表示されるアクティベーション キーをメモしておきます。

   b Edge の VLAN IP アドレス (169.254.0.1/24 を使用) を設定します。[アドバタイズ (Advertise)] および [DHCP] を有効にしないでください。

   c 次のようにして、Virtual Edge インターフェイスを構成します。

      - GE2 インターフェイスの機能を [スイッチ (Switched)] から [ルーティング (Routed)] に変更し、[WAN オーバーレイ (WAN Overlay)] と [DHCP アドレス指定 (DHCP Addressing)] を有効にします。
      - GE3 インターフェイスについては、LAN 側ゲートウェイに使用するため、[WAN オーバーレイ (WAN Overlay)] と [NAT ダイレクト トラフィック (NAT Direct Traffic)] を無効にします。

   詳細については、SD-WAN Orchestrator での Edge のプロビジョニングを参照してください。

   注： SD-WAN Orchestrator では、Edge のアクティベーションの前にデバイス設定を構成する必要があります。このステップを実行しない場合、Virtual Edge はアクティベーションされますが、数分後にオフラインになります。

3 最初に VPC ネットワークを作成してから、各インターフェイスの相対参照を含む DM テンプレートをデプロイするという方法で、GCP イメージをデプロイします。また、vEdge の SD-WAN Orchestrator ターゲットとアクティベーション キーを指定するため、cloud-init もテンプレートで使用します。

   a 3 つの Virtual Private Cloud (VPC) ネットワーク（管理 VPC ネットワーク、パブリック VPC ネットワーク、プライベート VPC ネットワーク）を作成し、トポロジ図に示すように、それぞれを Edge (n1-standard-4) に接続するサブネットに使用します。

      - 管理インターフェイス GE1 を介した Edge へのコンソール/管理アクセスのための管理サブネット。
      - WAN 側インターフェイス GE2 を介した Edge からのインターネット アクセスのためのパブリック サブネット。
      - LAN 側インターフェイス GE3 を介した LAN 側のデバイス アクセスのためのプライベート サブネット。

      VPC ネットワークを作成する手順については、VPC ネットワークの作成を参照してください。

   b Deployment Manager (DM) テンプレートを編集します。以下に、YAML DM テンプレートのサンプルを示します。このテンプレートを利用することができますが、必ず、ご使用の環境に応じて必要な変更を加えてください。YAML DM テンプレートでは、目的の環境に合わせて次の項目を変更する必要があります。

      - プロジェクト名

- リージョンとゾーン
- VPC 名とサブネット
- VMware SD-WAN Orchestrator の IP アドレスまたは FQDN
- アクティベーション コード（形式：xxxx-xxxx-xxxx-xxxx）
- VMware SD-WAN Orchestrator の「Ignore Cert Errors」：true または false

```
# "VMware SD-WAN by VeloCloud GCP Deployment Manager Template (34220201029)"
# gcloud deployment-manager deployments create velocloud-vce --config gcp_dm.yaml
# gcloud deployment-manager deployments delete velocloud-vce

resources:
- type: compute.v1.instance
  name: dm-gcp-vce-01
  properties:
    zone: us-west1-a
    machineType: https://www.googleapis.com/compute/v1/projects/gcp-nsx-sdwan/zones/us-west1-
a/machineTypes/n1-standard-4
    canIpForward: true
    disks:
    - deviceName: boot
      type: PERSISTENT
      boot: true
      autoDelete: true
      initializeParams:
        sourceImage: https://www.googleapis.com/compute/v1/projects/vmware-sdwan-public/
global/images/vce-342-102-r342-20200610-ga-3f5ad3b9e2
networkInterfaces:
      - network: https://www.googleapis.com/compute/v1/projects/gcp-nsx-sdwan/global/networks/
velo-mgmt-vpc
        subnetwork: projects/gcp-nsx-sdwan/regions/us-west1/subnetworks/velo-mgmt-sn
      - network: https://www.googleapis.com/compute/v1/projects/gcp-nsx-sdwan/global/networks/
velo-public-vpc
        subnetwork: projects/gcp-nsx-sdwan/regions/us-west1/subnetworks/public-sn
        accessConfigs:
          - name: External NAT
            type: ONE_TO_ONE_NAT
      - network: https://www.googleapis.com/compute/v1/projects/gcp-nsx-sdwan/global/networks/
velo-private-vpc
        subnetwork: projects/gcp-nsx-sdwan/regions/us-west1/subnetworks/velo-private-sn
    metadata:
      items:
      - key: user-data
        value: |
           #cloud-config
           velocloud:
            vce:
             vco: vco58-usvi1.velocloud.net
             activation_code: YPTF-PN33-THTX-28V5
             vco_ignore_cert_errors: false
```

gcloud CLI の詳細については、https://cloud.google.com/sdk/gcloud/を参照してください。

4 Virtual Edge が SD-WAN Orchestrator でアクティベーションされているかどうかを確認します。

インスタンスが GCP で実行されており、指定されたすべての情報が正しければ、Virtual Edge はアクティベーション キーを使用して SD-WAN Orchestrator に到達し、アクティベーションになり、必要な場合はソフトウェアの更新を実行します (そして、アップグレードが実行された場合は再起動されます)。デプロイにかかる時間は、通常は 3 ～ 4 分です。

Deployment Manager の有効化

Deployment Manager は、Google Cloud リソースの作成と管理を自動化するインフラストラクチャ デプロイ サービスです。Deployment Manager は、各 Google Cloud サービスの基盤となる API を利用してリソースをデプロイします。

Google Cloud Deployment Manager V2 API は、クラウド リソースのデプロイを指定するテンプレートを使用して、Google Cloud サービスと API を構成、デプロイ、および表示するためのサービスを提供します。Cloud Deployment Manager V2 API を有効にして認証情報を作成するには、次の手順を実行します。

前提条件

- GCP アカウントとログイン情報。
- GCP Deployment Manager でサポートされるリソース タイプに関する十分な知識。詳細については、https://cloud.google.com/deployment-manager/docs/configuration/supported-resource-types を参照してください。

手順

1 GCP コンソールにログインします。

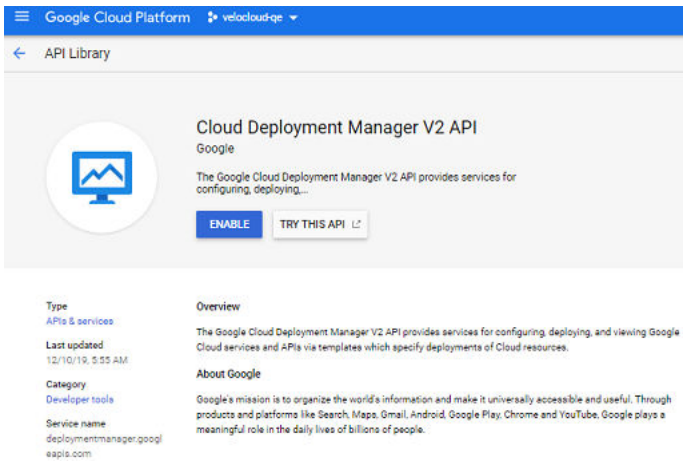
2 [API とサービス (APIs & Services)] > [ダッシュボード (Dashboard)] に移動します。

[API とサービス (APIs & Services)] ページが表示されます。

3 [API とサービスの有効化 (Enable APIS AND SERVICES)] をクリックします。

4 [検索 (Search)] テキスト ボックスを使用して、Deployment Manager API を検索します。

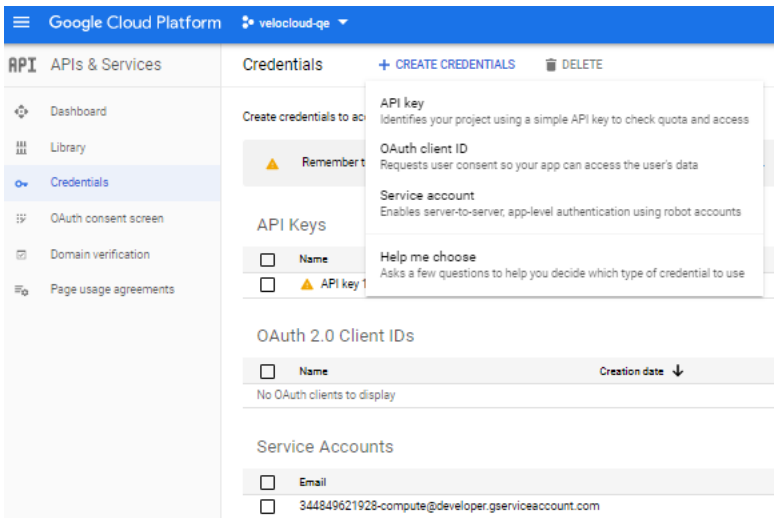
5 [Cloud Deployment Manager V2 API] をクリックしてから、[有効化 (Enable)] をクリックします。



Cloud Deployment Manager API が有効になります。この API を使用するには、認証情報の作成する必要があります。

6 [認証情報 (Credentials)] > [認証情報の作成 (CREATE CREDENTIALS)] をクリックし、次のいずれかのオプションを選択して認証情報を作成します。

- API キー (API key)
- OAuth クライアント ID (OAuth client ID)
- サービス アカウント (Service account)
- 選択に関するヘルプ (Help me choose)



7 [API キー (API key)] をクリックすると API キーが作成されます。このキーをアプリケーションで使用できます。

8 本番環境での不正使用を防ぐためにキーを制限する場合は、API キーが作成されたことを通知するポップアップ ウィンドウで [キーを制限する (RESTRICT KEY)] をクリックし、それ以外の場合は [閉じる (CLOSE)] をクリックします。

結果

Deployment Manager と Compute Engine API が有効になり、API を使用して Virtual Edge リソースをデプロイできるようになります。

次のステップ

Deployment Manager を使用して Virtual Edge をデプロイすることができます。詳細な手順については、GCP Deployment Manager を使用した Virtual Edge のデプロイを参照してください。

Edge のアクティベーションの確認

SD-WAN Orchestrator で Virtual Edge のアクティベーションを確認する方法について説明します。

1 SD-WAN Orchestrator にログインします。

2 [監視 (Monitor)] > [Edge (Edges)] の順に移動します。

3 [VeloCloud Edge (VeloCloud Edges)] 画面で、Virtual Edge が正常にアクティベーションされているかどうかを確認できます。