

# Google Cloud Platform 虛 擬 Edge 部署指南

VMware SD-WAN 4.1

您可以在 VMware 網站上找到最新的技術文件，網址如下：

<https://docs.vmware.com/tw/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2020 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

# 目錄

<b>1</b>	<b>Google Cloud Platform 虛擬 Edge 部署指南</b>	<b>4</b>
	Google Cloud 虛擬 Edge 部署概觀	4
	GCP 上的虛擬 Edge 部署	5
	準備 GCP 環境	7
	建立 VPC 網路	7
	建立輸入防火牆規則	9
	在 VPC 網路中建立路由	11
	在 SD-WAN Orchestrator 上佈建 Edge	14
	從 GCP Marketplace 部署虛擬 Edge	15
	使用 GCP Deployment Manager 部署虛擬 Edge	18
	啟用 Deployment Manager	20
	驗證 Edge 啟用	22

# Google Cloud Platform 虛擬 Edge 部署指南

# 1

此文件提供在 Google Cloud Platform (GCP) 上部署虛擬 VMware SD-WAN Edge 的相關指示。

本章節討論下列主題：

- [Google Cloud 虛擬 Edge 部署概觀](#)
- [GCP 上的虛擬 Edge 部署](#)
- [準備 GCP 環境](#)
- [在 SD-WAN Orchestrator 上佈建 Edge](#)
- [從 GCP Marketplace 部署虛擬 Edge](#)
- [使用 GCP Deployment Manager 部署虛擬 Edge](#)
- [驗證 Edge 啟用](#)

## Google Cloud 虛擬 Edge 部署概觀

越來越多客戶將工作負載移至公有雲基礎結構，並預期將 SD-WAN 從遠端站台延伸至公有雲，以保證 SLA。VMware 提供多種選項，可利用分散式 VMware SD-WAN Gateways 建立面向公有雲私人網路的 IPsec，或在 Google Cloud Platform (GCP) 上直接部署虛擬 Edge。

對於總流量需求低於 1G 的小型分支部署，在私人 GCP 網路中部署單一虛擬 Edge 即可。對於需要數 GB 總流量的較大資料中心部署，則可以部署 Hub 叢集。

---

**備註** 在 VMware SD-WAN Hub 叢集設計中，LAN 端利用第 3 層執行個體在叢集的 Hub 之間執行 BGP，並利用第 3 層執行個體在 LAN 中分配路由。由於 GCP 路由器不支援動態路由通訊協定，因此 GCP 基礎結構中需要使用第三方虛擬路由器。

---

本文件說明在 GCP 上部署虛擬 SD-WAN Edge (vVCE) 的基本拓撲和高階工作流程。請參閱 [GCP 上的虛擬 Edge 部署](#)。

### 必要條件

- GCP 帳戶和登入資訊。
- 熟悉 GCP 網路概念。如需詳細資訊，請參閱 <https://cloud.google.com/vpc/docs/overview>。
- SD-WAN Orchestrator 目標和登入的管理員帳戶。

## GCP 機器類型

調整 VMware SD-WAN 虛擬 Edge 的大小時，需要考慮頻寬總流量和網路介面數目。所需網路介面的最小數目為三個 (GE1、GE2、GE3)。

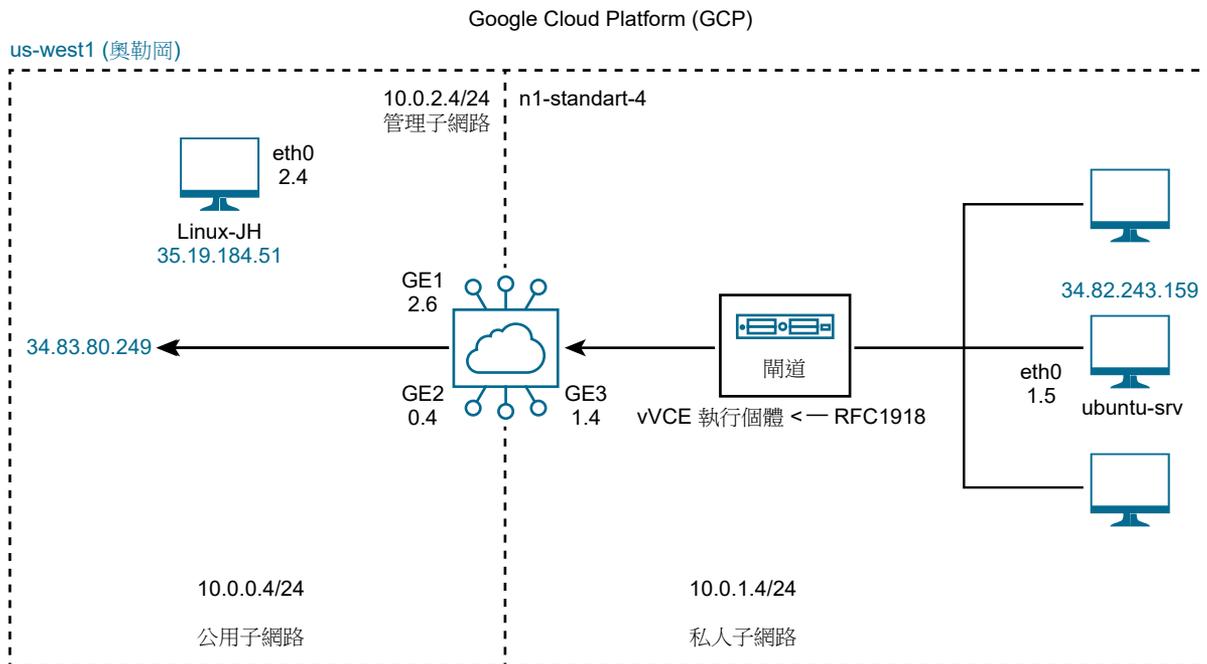
總流量	30 Mbps	50 Mbps	100 Mbps	200 Mbps	400 Mbps	1 Gbps
vCPU	2	2	2	2	4	4
記憶體	4 GB	4 GB	4 GB	8 GB	8 GB	8 GB

機器類型	vCPU	記憶體 (Gb)	NIC 數目上限
n1-standard-4	4	15	4
n1-standard-8	8	30	8

## GCP 上的虛擬 Edge 部署

說明在 Google Cloud Virtual Private Cloud (VPC) 上部署虛擬 Edge，其中包含三個 VPC 網路：管理 VPC (10.0.2.x/24)、公用 VPC (10.0.0.x/24) 和私人 VPC (10.0.1.x/24)，各代表連線至 Edge 的一個子網路，如下列拓撲圖所示。

### 基本拓撲



虛擬 Edge 會在兩個子網路之間路由。公用 VPC 路由會將所有網域離線流量轉送至網際網路閘道。私人子網路中的閘道路由器會將所有流量轉送至虛擬 Edge 上面向 LAN 的介面 (GE3)。在此範例中，預設路由用於轉送來自工作負載的「全部」流量，但非必要。RFC1918 摘要或特定分支/Hub 首碼可用來限縮傳送至虛擬 Edge 的項目。例如，如果仍需要從公開來源 IP 透過 SSH 存取私人子網路中的工作負載，則可設定 VPC 路由器將預設路由 (0.0.0.0/0) 指向網際網路閘道，並將 RFC1918 摘要指向虛擬 Edge。

## 高階工作流程

若要在 [Google Cloud Platform](#) 上部署 VMware SD-WAN 虛擬 Edge，請執行下列步驟：

### 1 準備 GCP 環境：

- a 建立三個 Virtual Private Cloud (VPC) 網路 (管理 VPC 網路、公用 VPC 網路和私人 VPC 網路)，各代表連線至 Edge (n1-standard-4) 的一個子網路，如拓撲圖所示。
  - 管理子網路，用於透過管理介面 GE1 對 Edge 進行主控台/管理存取。
  - 公用子網路，用於透過 WAN 端介面 GE2 從 Edge 存取網際網路。
  - 私人子網路，用於透過 LAN 端介面 GE3 存取 LAN 端裝置。

如需相關步驟，請參閱[建立 VPC 網路](#)。

- b 建立 VPC 網路的輸入防火牆規則：管理、私人 and 公用。如需相關步驟，請參閱[建立輸入防火牆規則](#)。
- c 在指向 Edge 之私人 VPC 網路的路由表中新增預設路由 (0.0.0.0/0) 項目，並以下一個躍點 IP 位址作為 Edge 的 GE3 介面 IP。

如需相關步驟，請參閱[在 VPC 網路中建立路由](#)。

### 2 在 VMware SD-WAN Orchestrator 上佈建 SD-WAN Edge，如下所示：

- a 建立**虛擬 Edge (Virtual Edge)** 類型的 Edge。
- b 將 GE1 介面從已交換 (Switched) 變更為已路由 (Routed)，並停用 **WAN 覆疊 (WAN Overlay)** 和 **NAT 直接流量 (NAT Direct Traffic)**。
- c 將 GE2 介面從已交換 (Switched) 變更為已路由 (Routed)，並啟用 **WAN 覆疊 (WAN Overlay)** 和 **NAT 直接流量 (NAT Direct Traffic)**。
- d 針對 GE3 介面，停用 **WAN 覆疊 (WAN Overlay)** 和 **NAT 直接流量 (NAT Direct Traffic)**，這將成為連線至私人子網路的裝置 (LAN 裝置) 的下一個躍點。

如需詳細資訊，請參閱[在 SD-WAN Orchestrator 上佈建 Edge](#)。

### 3 部署虛擬 Edge。您可以使用下列其中一種方法來部署虛擬 Edge：

- 從 [GCP Marketplace](#) 部署虛擬 Edge
- 使用 [GCP Deployment Manager](#) 部署虛擬 Edge

### 4 確認 SD-WAN Orchestrator 中是否已啟動虛擬 Edge。

## 準備 GCP 環境

在 Google Cloud Platform (GCP) 上部署虛擬 Edge 之前，您必須先透過完成下列步驟來準備 GCP 環境：

- [建立 VPC 網路](#)
- [建立輸入防火牆規則](#)
- [在 VPC 網路中建立路由](#)

### 建立 VPC 網路

您可以選擇建立自動模式或自訂模式的 Virtual Private Cloud (VPC) 網路。當您建立網路時，自動模式網路會自動在每個 Google Cloud 區域中建立一個子網路。對於自訂模式 VPC 網路，您必須建立網路，然後在區域內建立所需的子網路。您可以在建立網路時建立子網路，也可以稍後新增子網路，但無法在未定義子網路的區域中建立執行個體。

#### 必要條件

請確定您擁有 Google 帳戶和 Google Cloud Platform (GCP) 主控台的存取/登入資訊。

#### 程序

- 1 登入 [GCP 主控台](#)。
- 2 按一下 **VPC 網路 (VPC Networks)**。

此時會顯示 **VPC 網路 (VPC Networks)** 頁面。

### 3 按一下**建立 VPC 網路 (Create VPC network)**。

此時會顯示**建立 VPC 網路 (Create a VPC network)** 頁面。

The screenshot shows the Google Cloud Platform console interface for creating a VPC network. The main form includes the following fields and options:

- Name:** mgmt-network
- Description:** (Optional)
- Subnets:** Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. [Learn more](#)
- Subnet creation mode:** Custom (selected) | Automatic
- New subnet modal:**
  - Name:** mgmt-subnet
  - Region:** us-west1
  - IP address range:** 10.10.10.0/24
  - Create secondary IP range:** (Optional)
  - Private Google access:** Off (selected)
  - Flow logs:** Off (selected)
- Dynamic routing mode:** Regional (selected)
  - Cloud Routers will learn routes only in the region in which they were created
  - Global: Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router
- DNS server policy (Optional):** No server policy

4 在**名稱 (Name)** 文字方塊中，輸入 VPC 網路的唯一名稱。

5 在**子網路 (Subnets)** 下，選擇**自訂 (Custom)** 或**自動 (Automatic)** 作為**子網路建立模式 (Subnet creation mode)**。如果您選擇**自訂 (Custom)**，請在**新增子網路 (New subnet)** 區域中，為子網路指定下列組態參數：

- 在**名稱 (Name)** 文字方塊中，輸入子網路的唯一名稱。
- 從**區域 (Region)** 下拉式功能表中，選取子網路的區域。

- c 在 **IP 位址範圍 (IP address range)** 文字方塊中，輸入 IP 位址範圍。
  - d 若要定義子網路的次要 IP 範圍，請按一下 **建立次要 IP 範圍 (Create secondary IP range)**。
  - e **私人 Google 存取 (Private Google access)**：在建立子網路或稍後編輯子網路時，選擇是否啟用私人 Google 存取。
  - f **流量記錄 (Flow logs)**：在建立子網路或稍後編輯子網路時，選擇是否啟用 VPC 流量記錄。
  - g 按一下 **完成 (Done)**。
- 6 若要新增更多子網路，請按一下 **新增子網路 (Add subnet)**，然後重複步驟 5 中的步驟。您也可以在建網後將更多子網新增至網路。
  - 7 為 VPC 網路選擇 **動態路由模式 (Dynamic routing mode)**。
  - 8 按一下 **建立 (Create)**。

#### 結果

隨即建立 VPC 網路和子網路。

#### 後續步驟

[建立輸入防火牆規則](#)

## 建立輸入防火牆規則

防火牆規則會在網路層級定義，且僅套用至其建立所在的網路。若要建立 VPC 網路的輸入防火牆規則，請執行此程序中的步驟。

#### 必要條件

- 請確定您擁有 Google 帳戶和 Google Cloud Platform (GCP) 主控台的存取/登入資訊。
- 請確定您已建立 VPC 網路。
- 請檢閱防火牆規則元件，務必熟悉 Google Cloud 中使用的防火牆組態元件。

#### 程序

- 1 登入 [GCP 主控台](#)。
- 2 按一下 **VPC 網路 (VPC Networks)**。  
此時會顯示 **VPC 網路 (VPC Networks)** 頁面。
- 3 按一下您要新增防火牆規則的 VPC 網路。  
此時會顯示所選 VPC 網路的 **VPC 網路詳細資料 (VPC network details)** 頁面。

- 4 移至**防火牆規則 (Firewall rules)** 索引標籤，然後按一下**新增防火牆規則 (Add firewall rule)**。此時會顯示**建立防火牆規則 (Create a firewall rule)** 頁面。

The screenshot shows the 'Create a firewall rule' page in the Google Cloud Platform console. The left sidebar contains navigation options: VPC networks, External IP addresses, Firewall rules (selected), Routes, VPC network peering, Shared VPC, Serverless VPC access, and Packet mirroring. The main content area is titled 'Create a firewall rule' and includes the following fields and options:

- Name:** mgmt-network-inbound-firewall-rule
- Description (Optional):** (Empty text box)
- Logs:** Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. **Off** (selected)
- Network:** mgmt-network
- Priority:** 1000
- Direction of traffic:** **Ingress** (selected)
- Action on match:** **Allow** (selected)
- Targets:** All instances in the network
- Source filter:** IP ranges
- Source IP ranges:** 0.0.0.0/0
- Second source filter:** None
- Protocols and ports:** **Specified protocols and ports** (selected)
  - tcp: 22
  - udp: all
  - Other protocols: icmp
- Disable rule:** (checked)
- Buttons:** Create, Cancel
- Footer:** Equivalent REST or command line

- 5 在**名稱 (Name)** 文字方塊中，輸入防火牆規則的唯一名稱。
- 6 選擇性按一下**記錄 (Logs)** 下方的**開啟 (On)**，以啟用防火牆記錄。依預設系統會停用防火牆記錄。
- 7 針對**流量方向 (Direction of traffic)**，選擇入口 (**ingress**)。
- 8 針對符合時的動作 (**Action on match**)，選擇允許 (**Allow**) 或拒絕 (**Deny**)。
- 9 從**目標 (Targets)** 下拉式功能表中，選取規則的目標：
  - 如果要將規則套用至網路中的所有執行個體，請選擇**網路中的所有執行個體 (All instances in the network)**。

- 如果要將規則套用至依網路 (目標) 標籤選取的執行個體，請選擇**指定的目標標籤 (Specified target tags)**，然後在**目標標籤 (Target tags)** 文字方塊中，輸入應套用規則的標籤。
  - 如果要將規則套用至依相關聯服務帳戶選取的執行個體，請選擇**指定的服務帳戶 (Specified service account)**，在**服務帳戶範圍 (Service account scope)** 下方指出服務帳戶位於目前專案或其他專案中，然後在**目標服務帳戶 (Target service account)** 欄位中，選擇或輸入服務帳戶名稱。
- 10 從**來源 (Source)** 篩選器下拉式功能表中，選取 **IP 範圍 (IP ranges)**。
- 11 在 [來源 IP 範圍] (Source IP ranges) 文字方塊中，輸入 CIDR 區塊，依 IP 位址範圍定義傳入流量的來源。使用 `0.0.0.0/0` 以表示來自任何網路的來源。
- 12 定義將套用規則的**通訊協定和連接埠 (Protocols and ports)**：
- 視動作而定，選取**全部允許 (Allow all)** 或**全部拒絕 (Deny all)**，將規則套用至所有通訊協定和連接埠。
  - 定義特定通訊協定和連接埠：
    - 選取 **tcp** 以包含 TCP 通訊協定和連接埠。輸入 `all` 或以逗號分隔的連接埠清單，例如 `20-22, 80, 8080`。
    - 選取 **udp** 以包含 UDP 通訊協定和連接埠。輸入 `all` 或以逗號分隔的連接埠清單，例如 `67-69, 123`。
    - 選取**其他通訊協定 (Other protocols)**，以根據需求包含 ICMP、VCMP、SNMP 等通訊協定。
- 13 (選用) 您可以建立防火牆規則，但將其強制執行狀態設定為已停用時，便不會強制執行防火牆規則。按一下**停用規則 (Disable rule)**，然後選取**已停用 (Disabled)**。
- 14 按一下**建立 (Create)**。

## 結果

隨即為選取的 VPC 網路建立防火牆規則。

## 後續步驟

- [在 VPC 網路中建立路由](#)

## 在 VPC 網路中建立路由

說明如何在指向 Edge 的私人 Virtual Private Cloud (VPC) 網路中新增預設路由，如拓撲圖中所示。

### 必要條件

- 請確定您擁有 Google 帳戶和 Google Cloud Platform (GCP) 主控台的存取/登入資訊。
- 請確定您已建立 VPC 網路。

### 程序

- 1 登入 [GCP 主控台](#)。

## 2 按一下 **VPC 網路 (VPC Networks)**。

此時會顯示 **VPC 網路 (VPC Networks)** 頁面。

## 3 按一下您想要新增預設路由的 VPC 網路 (私人 VPC 網路)。

此時會顯示 **VPC 網路詳細資料 (VPC network details)** 頁面。

## 4 移至**路由 (Routes)** 索引標籤，然後刪除在 VPC 網路建立期間建立的預設路由。

## 5 按一下 **新增路由 (Add route)**。此時會顯示**建立路由 (Create a route)** 頁面。

The screenshot shows the 'Create a route' form in the Google Cloud Platform console. The form is titled 'Create a route' and is part of the 'VPC network' configuration. The left sidebar shows the navigation menu with 'Routes' selected. The main form area contains the following fields:

- Name \***: lan-side-default-route (Lowercase letters, numbers, hyphens allowed)
- Description**: (Empty text field)
- Network**: private-network (Dropdown menu)
- Destination IP range \***: 0.0.0.0/0 (E.g. 10.0.0.0/16)
- Priority \***: 1000 (Priority should be a positive integer (lower values take precedence))
- Instance tags**: (Empty text field)
- Next hop**: Specify IP address (Dropdown menu)
- Next hop IP address \***: 172.16.101.21 (E.g. 10.240.0.0)

At the bottom of the form, there are two buttons: 'CREATE' and 'CANCEL'. Below the buttons, there is a link: 'Equivalent REST or command line'.

- 在**名稱 (Name)** 文字方塊中，輸入路由項目的唯一名稱。
- 在目的地 **IP 範圍 (Destination IP range)** 文字方塊中，指定新的預設路由 (例如 0.0.0.0/0)。
- 在**優先順序 (Priority)** 文字方塊中，指定路由的優先順序。只在路由具有同等目的地時，才會使用優先順序決定路由順序。
- 從**下一個躍點 (Next hop)** 下拉式功能表中，選取 **指定 IP 位址 (Specify IP address)**。
- 在**下一個躍點 IP 位址 (Next hop IP address)** 文字方塊中，輸入所選 VPC 網路中 Edge 介面的 IP 位址。
- 按一下**建立 (Create)**。

### 結果

路由項目會新增至所選 VPC 網路的路由表中。

## 在 VPC 網路中新增分支至分支路由

說明如何在指向 Edge 的公用 Virtual Private Cloud (VPC) 網路中新增分支至分支路由，如「單臂拓撲」中所示。

## 必要條件

- 請確定您擁有 Google 帳戶和 Google Cloud Platform (GCP) 主控台的存取/登入資訊。
- 請確定您已建立 VPC 網路。

## 程序

- 1 登入 [GCP 主控台](#)。
- 2 按一下 **VPC 網路 (VPC Networks)**。  
此時會顯示 **VPC 網路 (VPC Networks)** 頁面。
- 3 按一下您想要新增路由由至路由的 VPC 網路 (公用 VPC 網路)。  
此時會顯示 **VPC 網路詳細資料 (VPC network details)** 頁面。
- 4 移至 **路由 (Routes)** 索引標籤，然後按一下 **新增路由 (Add route)**。此時會顯示 **建立路由 (Create a route)** 頁面。

- a 在 **名稱 (Name)** 文字方塊中，輸入路由項目的唯一名稱。
- b 在 **目的地 IP 範圍 (Destination IP range)** 文字方塊中，指定企業網路中的分支 IP 位址，例如 172.16.0.0/20。
- c 在 **優先順序 (Priority)** 文字方塊中，指定路由的優先順序。只在路由具有同等目的地時，才會使用優先順序決定路由順序。
- d 從 **下一個躍點 (Next hop)** 下拉式功能表中，選取 **指定 IP 位址 (Specify IP address)**。
- e 在 **下一個躍點 IP 位址 (Next hop IP address)** 文字方塊中，輸入所選 VPC 網路中 Edge 介面的 IP 位址。
- f 按一下 **建立 (Create)**。

## 結果

路由項目會新增至所選 VPC 網路的路由表中。

## 在 SD-WAN Orchestrator 上佈建 Edge

若要佈建 SD-WAN Edge，請執行此程序中的步驟。

### 必要條件

請確定您擁有 SD-WAN Orchestrator 的主機名稱和管理員帳戶可供登入。

### 程序

- 1 使用您的登入認證，以 Admin 使用者身分登入 SD-WAN Orchestrator 應用程式。
- 2 移至**設定 (Configure) > Edge**。
- 3 按一下**新增 Edge (New Edge)**。

此時會顯示**佈建新的 Edge (Provision New Edge)** 對話方塊。

The screenshot shows the 'Provision New Edge' dialog box with the following fields and values:

- Name:** vce-demo
- Model:** Virtual Edge
- Profile:** GCP
- Authentication:** Certificate Disabled
- Custom Info:** (empty)
- High Availability:** (checkbox unchecked)
- Serial Number:** Ex: VC00000490
- Contact Name:** Super User
- Contact Email:** super@velocloud.net
- Location:** (info icon) [Set Location...](#)

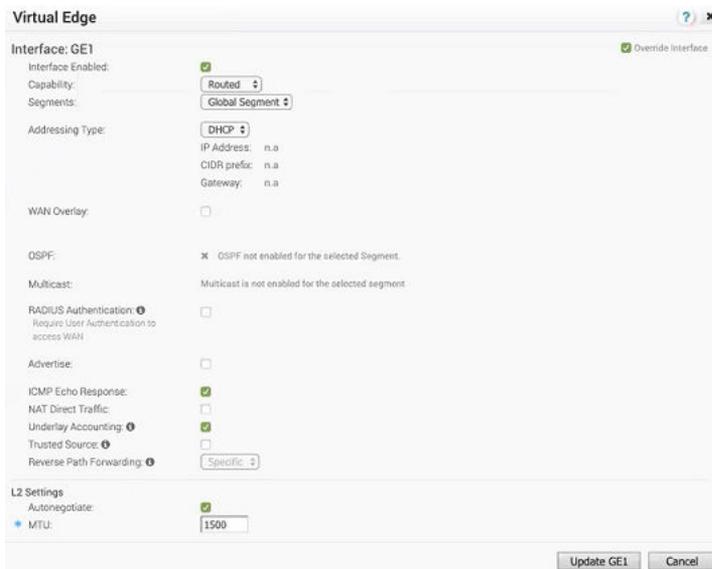
Buttons: Create (green), Cancel (grey)

- 4 在**名稱 (Name)** 文字方塊中，輸入 Edge 的唯一名稱。
- 5 從**模式 (Model)** 下拉式功能表中，選取**虛擬 Edge (Virtual Edge)**。
- 6 從**設定檔 (Profile)** 下拉式功能表中，選取**快速入門設定檔 (Quick Start Profile)**，然後按一下**建立 (Create)**。

隨即佈建 Edge，頁面頂端會顯示啟用金鑰。請記下啟用金鑰，並用於從 Google Cloud Platform (GCP) 主控台啟動 Edge。

7 設定虛擬 Edge 介面。考慮 [GCP 上的虛擬 Edge 部署](#) 時會說明下列步驟。

- a 按一下 **裝置 (Device)** 索引標籤，然後移至介面設定 (**Interface Settings**) 區域。
- b 按一下對應於介面的 **編輯 (Edit)**，然後選取 **覆寫介面 (Override Interface)** 核取方塊，以更新虛擬 Edge 介面 (**GE1 介面**、**GE2 介面** 和 **GE3 介面**) 的組態，如下所示：
  - 將 **GE1 介面** 功能變更為 **已路由 (Routed)**，並停用 **WAN 覆疊 (WAN Overlay)** 和 **NAT 直接流量 (NAT Direct Traffic)**。
  - 將 **GE2 介面** 功能變更為 **已路由 (Routed)**，並確保 **WAN 覆疊 (WAN Overlay)** 和 **NAT 直接流量 (NAT Direct Traffic)** 已啟用。
  - 針對 **GE3 介面**，停用 **WAN 覆疊 (WAN Overlay)** 和 **NAT 直接流量 (NAT Direct Traffic)**，這將成為連線至私人 VPC 子網路之裝置 (LAN 裝置) 的下一個躍點。



## 結果

虛擬 Edge 會在 SD-WAN Orchestrator 上進行佈建。

## 後續步驟

在 GCP 上部署虛擬 Edge。您可以使用下列其中一種方法來部署虛擬 Edge：

- [從 GCP Marketplace 部署虛擬 Edge](#)
- [使用 GCP Deployment Manager 部署虛擬 Edge](#)

## 從 GCP Marketplace 部署虛擬 Edge

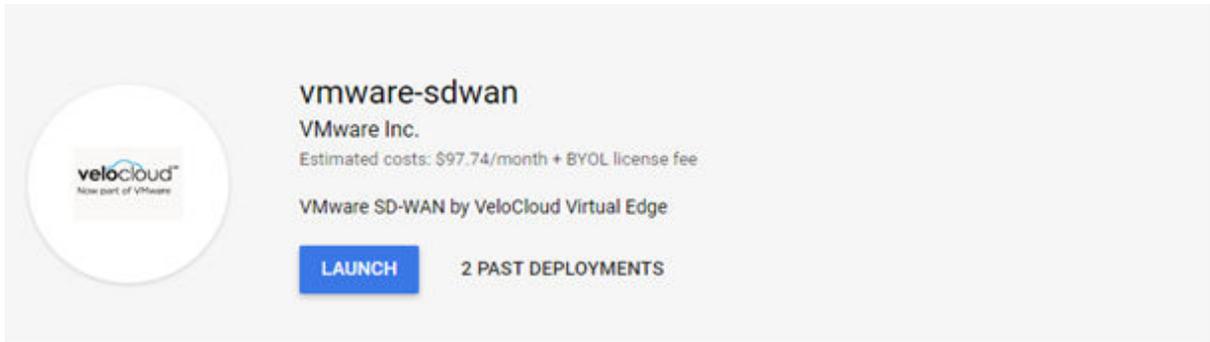
在 Google Cloud 主控台，您可以使用開機磁碟映像、開機磁碟快照或容器映像，以建立和部署虛擬機器 (VM) 執行個體。若要使用開機磁碟映像建立和部署虛擬機器 (VM) 執行個體，請執行此程序中的步驟。

## 必要條件

請確定您擁有 Google 帳戶和 Google Cloud Platform (GCP) 主控台的存取/登入資訊。

## 程序

- 1 登入 [GCP 主控台](#)。
- 2 VMware SD-WAN 現在可於 GCP Marketplace 中取得。請在 Marketplace 中搜尋 VMware SD-WAN 即可開始使用。



**Runs on**  
Google Compute Engine

**Type**  
[Virtual machines](#)  
Single VM  
BYOL

**Last updated**  
10/28/20, 11:14 AM

**Category**  
[Compute](#)  
[Networking](#)

**Version**  
3.4.2

**Operating system**  
VeloCloud OS 3.4.2

**Add to Private Catalog**  
[Deployment .zip file](#)

### Overview

VMware SD-WAN by VeloCloud assures enterprise and cloud application performance over Internet and hybrid WAN while simplifying deployments and reducing costs. The SD-WAN Edges are zero-touch enterprise-class appliances that provide secure optimized connectivity to private, public and hybrid applications, compute and virtualized services. VMware SD-WAN Edges perform deep application recognition, application and packet steering, performance metrics and end to end quality of service in addition to hosting virtual network function (VNF) services. VMware SD-WAN Edges by VeloCloud can be offered as physical appliance or virtual machines which can be installed on hypervisors or public cloud.

[Learn more](#)

### About VMware Inc.

VMware streamlines the journey for organizations to become digital businesses that deliver better experiences to their customers and empower employees to do their best work. Our software spans compute, cloud, networking and security, and digital workspace.

### About BYOL

BYOL (Bring Your Own License) solutions let you run software on Compute Engine while using licenses purchased directly from the provider. Google only charges you for the infrastructure costs, giving you the flexibility to purchase and manage your own licenses.

### 3 按一下啟動 (LAUNCH)。

此時會顯示**建立執行個體 (Create an instance)** 頁面。

The screenshot shows the 'New vmware-sdwan deployment' configuration page. The settings are as follows:

- Deployment name:** gcp-vedge03-west1
- Zone:** us-west1-a
- Machine type:** 4 vCPUs, 15 GB memory
- User-data:** Sdwan userdata for activation: `"#cloud-config\nvelocloud:\n vce:\n vco: vco58-usv11.velocloud.net\n activation_code: 3SHZ-966M-BJP2-ULUX\n vco_ignore_cert_errors: true\n"`
- ipForward:** On
- Boot Disk:** SSD Persistent Disk
- Boot disk size in GB:** 10
- Networking:**
  - velo-mgmt-vpc velo-mgmt-sn (10.0.2.0/24)
  - velo-public-vpc public-sn (10.0.0.0/24)
  - velo-private-vpc velo-private-sn (10.0.1.0/24)

At the bottom, there is a 'Deploy' button.

- 4 在**部署名稱 (Deployment name)** 文字方塊中，輸入執行個體的唯一名稱。
- 5 從**區域 (Zone)** 下拉式功能表中，選取要建立 VPC 網路的區域。
- 6 選取執行個體的機器組態。從**機器類型 (Machine type)** 下拉式功能表中，根據已設定的拓撲選取選項。
- 7 在**使用者資料 (User-data)** 欄位中，以下列範例格式提供 cloud-init 資訊，以針對目標 VMware SD-WAN Orchestrator 啟用虛擬 Edge。

Cloud-init 使用者資料範例

```
"#cloud-config\nvelocloud:\n vce:\n vco: vco58-usv11.velocloud.net\n activation_code: 3SHZ-966M-BJP2-ULUX\n vco_ignore_cert_errors: false\n"
```

請務必檢查格式正確無誤以確保其會經過處理，否則啟用會以無訊息方式失敗 (即 Orchestrator 中沒有錯誤事件)。

#cloud-config 需要使用引號加以封裝，否則 GCP 會在啟動期間擲回錯誤。引號已包含在**使用者資料 (User-data)** 欄位中。您只需在引號之間插入 cloud-config 即可，或者，也可以剪下並貼上範例 cloud-init 使用者資料，並取代**使用者資料 (User-data)** 欄位中的所有文字。

**備註** 換行 (\n) 字元和間距必須正確無誤，剖析才能運作。最佳做法是將上面的範例剪下並貼到記事本中，並只視需要取代值，而不修改間距。

SSH 金鑰會在專案層級進行管理。請參閱 <https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys>。

- 8 IP 轉送可讓虛擬 Edge 上的介面處理目的地不是本機介面 MAC 位址的封包。依預設會啟用 IP 轉送，必須啟用此設定才能讓路由正確運作，且您無法變更此設定。
- 9 在**開機磁碟 (Boot disk)** 區域中，開機映像的磁碟類型和大小應保留為預設值：分別是 SSD 持續性磁碟和 10 GB。
- 10 在**網路 (Networking)** 區域中，對已設定的 VPC 網路新增介面，如下所示。
  - a 在**網路介面 (Network interfaces)** 下，按一下 **+ 新增網路介面 (+ Add Network Interface)** 圖示。
  - b 從**網路 (Network)** 下拉式功能表中，選取您要新增介面的網路。
  - c 設定外部 IP，如下所示：
    - 針對管理網路 - 針對**外部 IP (External IP)** 選取**無 (None)**。
    - 針對公用網路 - 選取**外部 IP：暫時 (External IP: Ephemeral)**，因為此介面需要對應至公用國際網路 IP。
    - 針對私人網路 - 針對**外部 IP (External IP)** 選取**無 (None)**。
  - d 按一下**完成 (Done)**。
  - e 若要新增其他介面，請按一下**新增網路介面 (Add network interface)**，然後重複上述 b 到 d 的步驟。
- 11 按一下**部署 (Deploy)**。

#### 結果

建立虛擬 Edge 執行個體後，計算引擎會自動啟動 Edge 執行個體。

#### 後續步驟

驗證 [Edge 啟用](#)

## 使用 GCP Deployment Manager 部署虛擬 Edge

若要使用 Deployment Manager 在 [Google Cloud Platform](#) 上部署 VMware SD-WAN 虛擬 Edge，請執行下列步驟：

- 1 在 GCP 中啟用 Cloud Deployment Manager API。如需相關步驟，請參閱[啟用 Deployment Manager](#)。

- 2 在 SD-WAN Orchestrator 上佈建 SD-WAN Edge，如下所示：
  - a 建立**虛擬 Edge (Virtual Edge)**類型的 Edge，並記下啟用金鑰 (佈建 Edge 後會顯示在畫面頂端)。
  - b 為 Edge 設定 VLAN IP 位址 (使用 169.254.0.1/24)。請勿啟用**通告 (Advertise)**和 **DHCP**。
  - c 設定虛擬 Edge 介面，如下所示：
    - 將 GE2 介面功能從已**交換 (Switched)**變更為已**路由 (Routed)**，並啟用 **WAN 覆蓋 (WAN Overlay)**和 **DHCPAddressing**。
    - 針對 GE3 介面，停用 **WAN 覆蓋 (WAN Overlay)**和 **NAT 直接流量 (NAT Direct Traffic)**，因為此介面將用於 LAN 端閘道。

如需詳細資訊，請參閱[在 SD-WAN Orchestrator 上佈建 Edge](#)。

---

**備註** SD-WAN Orchestrator 需要在 Edge 啟動之前進行「裝置設定」。如果遺漏此步驟，則虛擬 Edge 會啟動，但幾分鐘後就進入離線狀態。

---

- 3 先建立 VPC 網路，然後以每個介面的相對參考來部署 DM 範本，以部署 GCP 映像。範本中也會使用 CLOUD-INIT，以提供 SD-WAN Orchestrator 目標和啟用金鑰給 vEdge。
  - a 建立三個 Virtual Private Cloud (VPC) 網路 (管理 VPC 網路、公用 VPC 網路和私人 VPC 網路)，各代表連線至 Edge (n1-standard-4) 的一個子網路，如拓撲圖所示。
    - 管理子網路，用於透過管理介面 GE1 對 Edge 進行主控台/管理存取。
    - 公用子網路，用於透過 WAN 端介面 GE2 從 Edge 存取網際網路。
    - 私人子網路，用於透過 LAN 端介面 GE3 存取 LAN 端裝置。

如需有關如何建立 VPC 網路的步驟，請參閱[建立 VPC 網路](#)。
  - b 修改 Deployment Manager (DM) 範本。以下是範例 YAML DM 範本。您可以使用此範本，但務必根據您的環境進行必要的變更。YAML DM 範本將需要修改下列項目以符合預期的環境：
    - 專案名稱
    - 區域 (Region) 和區域 (Zone)
    - VPC 名稱和子網路
    - VMware SD-WAN Orchestrator IP 或 FQDN
    - 啟用代碼 (格式：xxxx-xxxx-xxxx-xxxx)
    - VMware SD-WAN Orchestrator 忽略憑證錯誤：true 或 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

```

如需 GCloud CLI 的相關資訊，請參閱 <https://cloud.google.com/sdk/gcloud/>。

#### 4 確認 SD-WAN Orchestrator 中是否已啟動虛擬 Edge。

一旦執行個體在 GCP 中執行，且提供的所有資訊都正確，虛擬 Edge 將使用啟用金鑰向外連接至 SD-WAN Orchestrator，並視需要啟動和執行軟體更新（升級後會重新開機）。部署時間通常為 3 到 4 分鐘。

## 啟用 Deployment Manager

Deployment Manager 是基礎結構部署服務，可自動建立和管理 Google Cloud 資源。Deployment Manager 會使用每個 Google Cloud 服務的基礎 API 來部署資源。

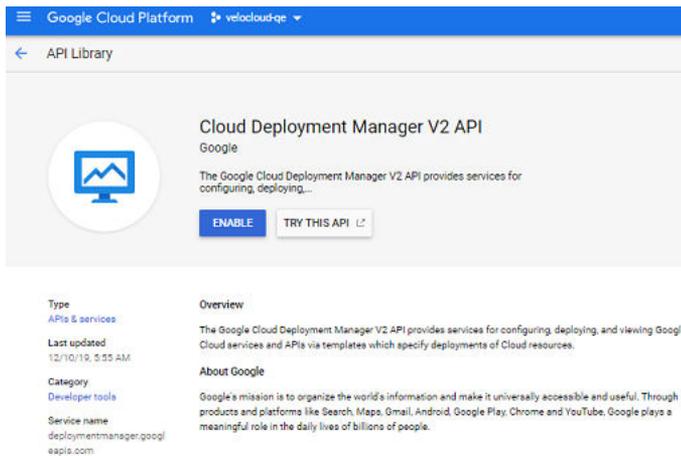
Google Cloud Deployment Manager V2 API 提供各種服務，可讓您透過範本指定雲端資源的部署，以設定、部署和檢視 Google Cloud 服務和 API。若要啟用 Cloud Deployment Manager V2 API 並建立認證，請執行下列步驟。

## 必要條件

- GCP 帳戶和登入資訊。
- 熟悉 GCP Deployment Manager 支援的資源類型。如需詳細資訊，請參閱 <https://cloud.google.com/deployment-manager/docs/configuration/supported-resource-types>。

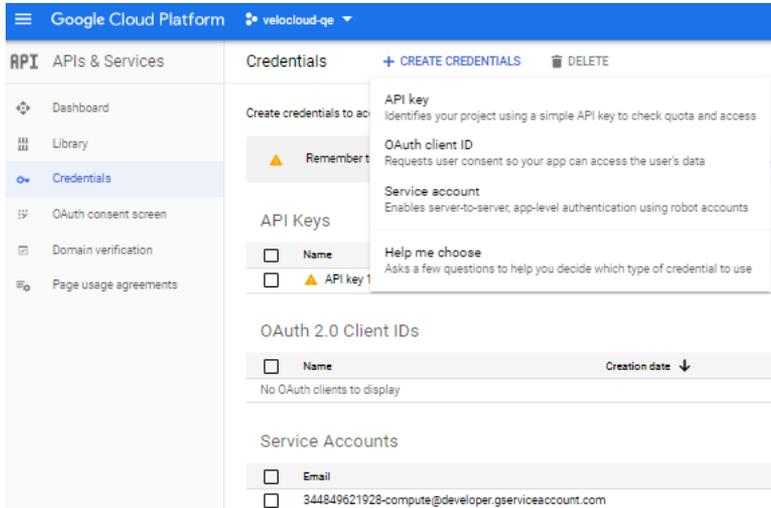
## 程序

- 1 登入 [GCP 主控台](#)。
- 2 移至 **API 和服務 (APIs & Services) > 儀表板 (Dashboard)**。  
此時會顯示 **API 和服務 (APIs & Services)** 頁面。
- 3 按一下**啟用 API 和服務 (Enable APIs AND SERVICES)**。
- 4 使用**搜尋 (Search)** 文字方塊，尋找 Deployment Manager API。
- 5 按一下 **Cloud Deployment Manager V2 API**，然後按一下**啟用 (Enable)**。



將啟用 Cloud Deployment Manager API。若要使用此 API，您必須建立認證。

- 6 按一下**認證 (Credentials) > 建立認證 (CREATE CREDENTIALS)**，然後選取下列其中一個選項來建立認證：
  - API 金鑰 (API key)
  - OAuth 用戶端識別碼 (OAuth client ID)
  - 服務帳戶 (Service account)
  - 協助我選擇 (Help me choose)



- 7 按一下 **API 金鑰 (API key)** 將建立 API 金鑰，供您在應用程式中使用。
- 8 在已建立 API 金鑰快顯視窗中，如果您想要限制金鑰以防止在生產環境中未經授權使用，請按一下**限制金鑰 (RESTRICT KEY)**，否則按一下**關閉 (CLOSE)**。

**結果**

Deployment Manager 和 Compute Engine API 已啟用，您可以使用 API 來部署虛擬 Edge 資源。

**後續步驟**

您可以使用 Deployment Manager 來部署虛擬 Edge。如需完整步驟，請參閱[使用 GCP Deployment Manager 部署虛擬 Edge](#)。

## 驗證 Edge 啟用

說明如何在 SD-WAN Orchestrator 中確認虛擬 Edge 啟用。

- 1 登入 SD-WAN Orchestrator。
- 2 移至**監控 (Monitor) > Edge**。
- 3 在 **VeloCloud Edge** 畫面中，您可以確認是否已成功啟用虛擬 Edge。

The screenshot displays the 'VeloCloud Edges' management console. On the left is a navigation sidebar with sections: Monitor (Network Overview, Edges, Network Services, Routing, Alerts, Events, Reports), Configure, Test & Troubleshoot, and Administration. The main area features a world map with various countries labeled. Below the map is a toolbar with a dropdown menu set to 'GCP-1', and buttons for 'Cols', 'Reset View', 'Refresh', and 'CSV'. A table below the toolbar shows one edge node:

Edge	Status	HA	Links	VM Status	VNF	Gateways	Profile	Operator Profile
1 GCP-1	<span style="color: green;">●</span>		<span style="color: green;">↔ 1</span>			<a href="#">View</a>	GCP	R340-20200208-QA-