

AWS 虛擬 Edge 部署指南

2020

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

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

目錄

1	AWS 虛擬 Edge 部署指南	4
	AWS 虛擬 Edge 部署概觀	4
	使用 CloudFormation 部署虛擬 Edge	7
	EC2 執行個體類型	15
	確認 VMware SD-WAN Orchestrator 中是否已啟動虛擬 Edge。	16

AWS 虛擬 Edge 部署指南

1

本文件提供《AWS 虛擬 Edge 部署指南》的逐步指示。

本章節討論下列主題：

- [AWS 虛擬 Edge 部署概觀](#)
- [使用 CloudFormation 部署虛擬 Edge](#)
- [EC2 執行個體類型](#)
- [確認 VMware SD-WAN Orchestrator 中是否已啟動虛擬 Edge。](#)

AWS 虛擬 Edge 部署概觀

此 AWS 虛擬 Edge 部署指南的概觀提供了一般概觀、CloudFormation 範本概觀和 CloudFormation 下載 (綠地 VPC 範本和棕地範本)。

一般概觀

在過去幾年中，多雲端或混合雲部署已變得越來越普遍，企業客戶在將其工作負載移至公有雲基礎結構時，會預期將 SD-WAN 從遠端分支延伸至公有雲，以保證 SLA。根據下列使用案例，VMware 提供了兩個主要選項：利用分散式 VCG 建立指向公有雲的 IPsec，或在公有雲虛擬私人網路中直接部署虛擬 Edge。本文件說明如何在 AWS 中部署虛擬 Edge。

對於總流量需求低於 1 G 的小型分支部署，在私人網路 (AWS VPC) 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，由於 AWS VPC 路由器不支援動態路由通訊協定，因此 AWS 基礎結構中需要協力廠商 L3 虛擬路由器，才能在叢集的 Hub 之間執行 BGP，並利用第 3 層路由器在 LAN 中分配路由。在此解決方案中，我們已使用備援 Cisco 服務路由器 (CSR) 1000v 進行驗證，但支援 HA 和 BGP 的其他虛擬路由器也應正常運作。

CloudFormation 範本概觀

有兩個 CloudFormation 預設範本：「新增 - 綠地 VPC」和「現有 - 棕地 VPC」；兩者皆代表 AWS 內的一般部署，如標題為[基本拓撲](#)的一節中的拓撲圖中所示。這兩個 CloudFormation 預設範本會建立必要資源、收集 SD-WAN Orchestrator 目標，以及收集啟動金鑰以透過 CLOUD-INIT 推送。

注意：無論您選擇哪個範本，在部署之前，請務必先檢閱並瞭解範本。這兩個 CloudFormation 範本皆用作參考，且可能需要變更以容納您的特定環境。

CloudFormation 範本值

以下列出了 CloudFormation 範本中包含的值：

- 將介面連結至 VMware 執行個體 (GE1 – eth0 / GE2 – eth1 / GE3 – eth2)
- 配置彈性 IP 並連結至 GE2
- 建立 LAN 端和 WAN 端安全群組 – 允許的連接埠：
 - WAN: GE1 和 GE2: UDP 2426 – VMware 多重路徑通訊協定
 - WAN: GE1 和 GE2: TCP 22 – SSH 存取 (適用於支援存取)
 - WAN: GE1 和 GE2: UDP 161 – SNMP
 - LAN: GE3 – 僅限 ICMP (部署後新增其他通訊協定，或視需要修改範本)
- 公用路由表 (VPC 路由器): 0.0.0.0/0 至網際網路閘道
- 私人路由表 (VPC 路由器): 0.0.0.0/0 至 ENI (SD-WAN Edge GE3)
- 在所有介面上停用來源/目的地檢查

CloudFormation 範本下載

有兩個可用的範本可供您選擇以部署虛擬 Edge (即新增 - 綠地 VPC 或現有 - 棕地 VPC)。雖然這些範本會啟用虛擬 Edge，但拓撲的簡化並不會容納所有環境。因此，您必須據以編輯您的環境。若要更深入瞭解 CloudFormation 範本結構和語法，請參閱：<https://aws.amazon.com/cloudformation/aws-cloudformation-templates/>。如需有關這些範本的詳細資訊，請參閱以下區段。

新增 – 綠地 VPC 範本

如果您想要建立新的 VPC，請使用綠地範本。在此下載新增 - 綠地範本：[新增 - 綠地範本](#)

Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

ActivationKey
Edge Activation Key

AvailabilityZone
Availability zone to deploy in

EC2InstanceType
Throughput and number of NICs dictate instance type

IgnoreCertificateValidation
Set to true if using private or self signed certificate on the VCO

PrivateCidrBlockValue
CIDR block for the LAN side of the Edge

PublicCidrBlockValue
CIDR block for the WAN side of the Edge

ResourcePrefix
Prefix used for naming all resources created by this template

SoftwareVersion
VeloCloud Virtual Edge Software Version

VCO
Orchestrator IP address or hostname (fqdn)

VeloCloudEdgeName
Name of Edge to be deployed

VeloCloudKeyPairName
Public/Private Key Name of Edge to be deployed

VpcCidrBlockValue
CIDR block for the VPC

現有 – 棕地範本

如果您使用現有 – 棕地範本，將不會建立 VPC、子網路和路由表。現有 – 棕地範本將顯示已填入現有 VPC 的下拉式功能表，以及可用於該區域的子網路。在此下載現有 – 棕地範本：[現有 – 棕地範本](#)。

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

ActivationKey
Edge Activation Key

EC2InstanceType
Throughput and number of NICs dictate instance type

c4.large

ExistingPrivateSubnet
Existing Subnet ID for the LAN side

ExistingPublicSubnet
Existing Subnet ID for the WAN side

ExistingVpc
Existing VPC ID

IgnoreCertificateValidation
Set to true if using private or self signed certificate on the VCO

false

ResourcePrefix
Prefix used for naming all resources created by this template

velocloud

SoftwareVersion
VeloCloud Virtual Edge Software Version

322

VCO
Orchestrator IP address or hostname (fqdn)

VeloCloudEdgeName
Name of Edge to be deployed

VeloCloudKeyPairName
Public/Private Key Name of Edge to be deployed

使用 CloudFormation 部署虛擬 Edge

以下說明如何使用 CloudFormation 範本部署虛擬 Edge 的指示。但是，在部署之前，請務必遵循必要條件需求。

必要條件

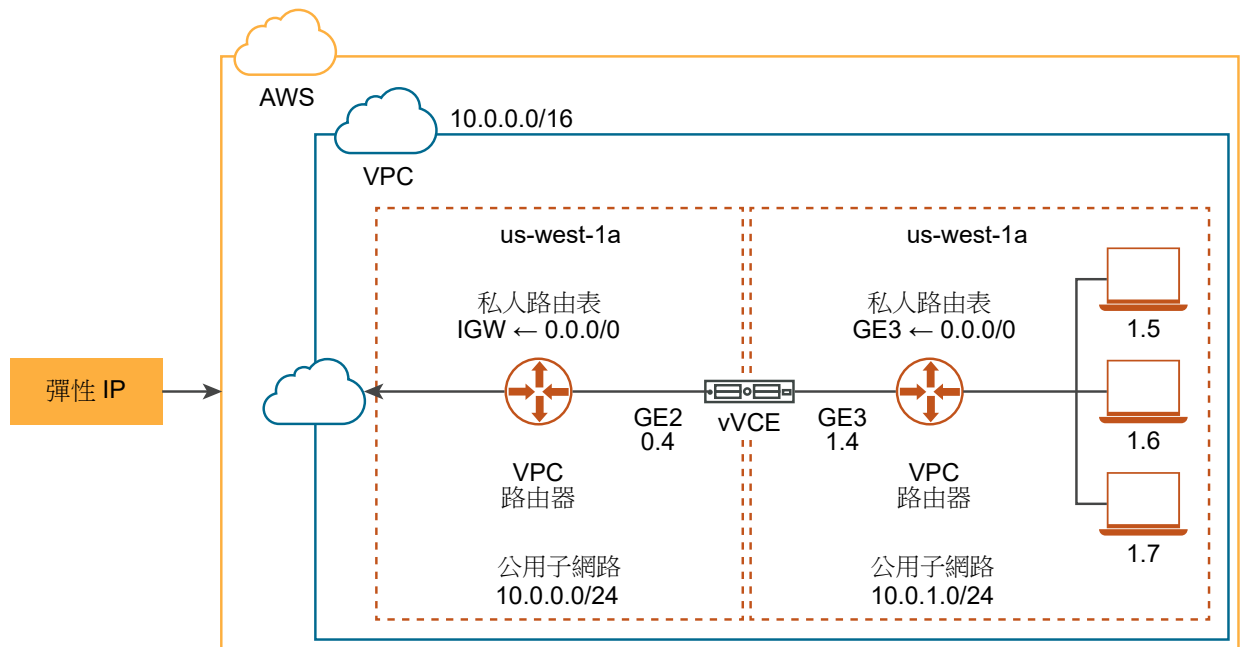
使用 CloudFormation 範本開始部署虛擬 Edge 之前，需要下列項目：

- AWS 帳戶和登入資訊
- 熟悉 AWS 網路概念 (請參閱：https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Networking.html)
- RSA 公開金鑰 (請參閱：<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>)

- VMware CloudFormation 範本 (下列其中一項):
 - 綠地部署 (在此處下載)
 - 棕地部署 (在此處下載)
- SD-WAN Orchestrator 目標和登入的管理員帳戶

基本拓撲

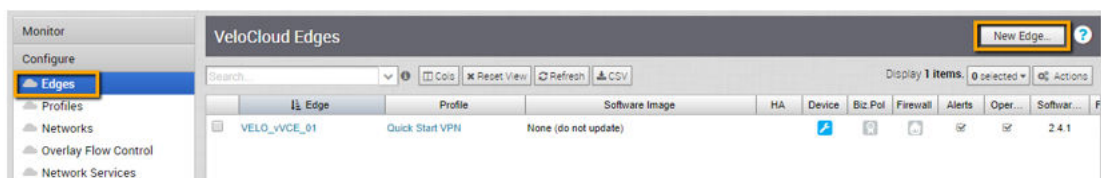
在基本拓撲範例中，AWS VPC (10.0.0.0/16) 分為一個公用子網路 (10.0.0.0/24) 和一個私人子網路 (10.0.1.0/24)。虛擬 Edge 會在兩個子網路之間路由。公用 VPC 路由會將所有網域離線流量轉送至網際網路閘道。私人子網路中的 VPC 路由器會將所有流量轉送至虛擬 Edge 上面向 LAN 的介面 (GE3 的 ENI)。在此範例中，預設路由用於轉送來自工作負載的「全部」流量，但非必要。RFC1918 摘要或特定分支/Hub 首碼可用來限縮傳送至虛擬 Edge 的項目。例如，如果需要從公開來源 IP 透過 SSH 存取私人子網路中的工作負載，則可設定 VPC 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。



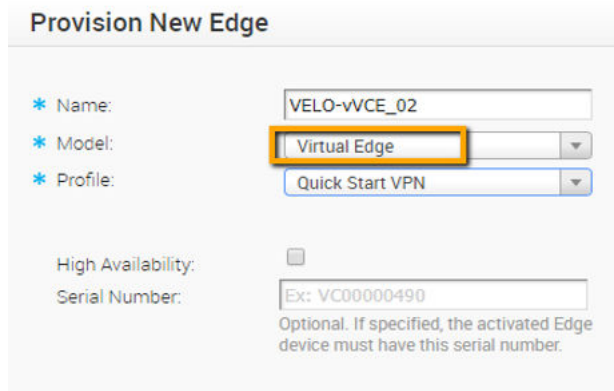
程序：

步驟 1: 透過 SD-WAN Orchestrator 將虛擬 Edge 新增至企業

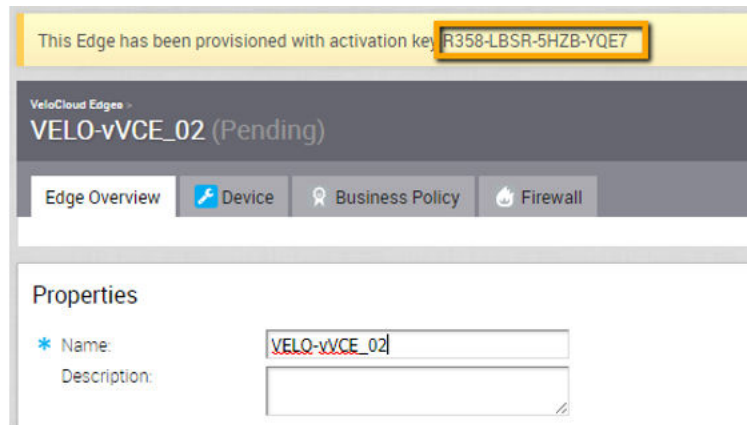
- 1 登入 SD-WAN Orchestrator。
- 2 移至導覽面板中的設定 (Configure) > Edge，然後按一下新增 Edge (New Edge) 按鈕。



隨即顯示佈建新的 Edge (Provision New Edge) 對話方塊。



- 3 在佈建新的 Edge (Provision New Edge) 對話方塊中：
 - a 在名稱 (Name) 文字方塊中輸入虛擬 Edge 的名稱。
 - b 在模式 (Model) 下拉式功能表中，選擇虛擬 Edge (Virtual Edge)。
 - c 在設定檔 (Profile) 下拉式功能表中，選擇虛擬 Edge 的設定檔。
 - d 將高可用性 (High Availability) 核取方塊保留取消勾選，因為其不適用。
 - e 將 [序號 (Serial Number)] 文字方塊保留空白。
 - f 按一下儲存 (Save)。
- 4 虛擬 Edge 會使用啟用金鑰進行佈建。記下啟動金鑰，因為在您部署 CloudFormation 範本時會用到。



步驟 2：新增 VLAN IP

必須已指派 IP 位址給 VLAN 組態，才能儲存裝置設定，但不會使用 IP 位址。例如，使用 IP 位址 169.254.0.1。請遵循下列步驟來新增 VLAN IP 位址。

- 1 對於剛建立的虛擬 Edge，按一下 SD-WAN Orchestrator 上的裝置 (Device) 索引標籤。
- 2 向下滑動至設定 VLAN (Configure VLAN) 區段，然後按一下新增 VLAN (Add VLAN) 按鈕。
VLAN 對話方塊隨即顯示。

The screenshot shows the 'VLAN' configuration window with the following details:

- Segment:** Global Segment (dropdown)
- VLAN Name:** Corporate
- VLAN Id:** 1
- Assign Overlapping Subnets:** unchecked
- Edge LAN IP Address:** 169.254.0.1
- Cidr Prefix:** 24
- Network:** 169.254.0.0
- Advertise:** unchecked
- Multicast:** Multicast is not enabled for the selected segment
- Fixed IPs:** Table with columns MAC Address, IP, and Description. Example: aa:bb:cc:dd:ee:ff, Ex: 10.0.2.5, Description (optional)
- LAN Interfaces:** GE1, GE2
- SSID:** There are no Wi-Fi SSIDs configured on this VLAN.
- DHCP Type:** Enabled, Relay, Disabled (selected)
- OSPF:** Enabled. Note: OSPF not enabled for the selected Segment.
- Buttons:** Update VLAN, Cancel

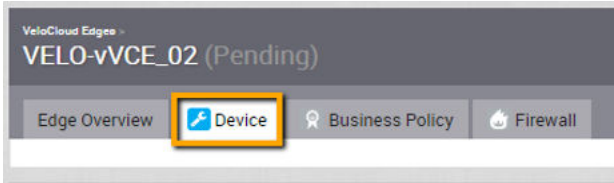
3 在 **VLAN** 對話方塊中，完成下列項目：

- a 如有必要，請勾選 **Edge 覆寫 (Edge Override)** 核取方塊來啟用 Edge 覆寫。
- b 在**區段 (Segment)** 下拉式功能表中選擇區段。
- c **VLAN 名稱 (VLAN Name)** 會顯示預設名稱，且可加以忽略。
- d **VLAN 識別碼 (VLAN ID)** 會顯示預設值，且可加以忽略。
- e 依預設會停用**指派重疊的子網路 (Assign Overlapping Subnets)**。
- f 在 **Edge LAN IP 位址 (Edge LAN IP Address)** 文字方塊中輸入 169.254.0.1。
- g 在 **Cidr 首碼 (Cidr Prefix)** 文字方塊中輸入 24。
- h **網路 (Network)** 值將根據 Cidr 首碼 (Cidr Prefix) 進行設定。
- i 將**通告 (Advertise)** 核取方塊取消勾選。
- j 重新命名欄位 (多點傳播、固定 IP、LAN 介面和 SSID) 可以保留其預設設定。
- k 如有必要，請勾選 **Edge 覆寫 (Edge Override)** 核取方塊來啟用 SD-WAN Edge 覆寫，以停用 DHCP。
- l 對於 **DHCP 類型 (DHCP Type)**，按一下已停用 (**Disabled**)。
- m 可以忽略 **OSPF** 區域。

步驟 3：設定虛擬 Edge 介面

警告： 在 SD-WAN Edge 啟動之前，必須先在 SD-WAN Orchestrator 中設定裝置設定 (**Device Settings**)。如果您略過此步驟，虛擬 Edge 將會啟動，但會在幾分鐘後進入離線狀態。

- 1 導覽至虛擬 Edge 的裝置設定 (設定 (**Configure**) > **Edge** > 裝置 (**Device**) 索引標籤)。



- 2 向下捲動至介面設定 (**Interface Settings**) 區段。

The screenshot shows the 'Interface Settings' table with columns for 'Interface', 'Mode', 'VLANs', 'Addressing', and 'WAN Overlay'. The GE2 interface is highlighted with a yellow box, and a red arrow points to the 'Auto Detect' option in the 'WAN Overlay' column.

Actions		Interface	Mode	VLANs	Addressing	WAN Overlay
Edit	<input checked="" type="checkbox"/>	GE1	Access	1 - Corporate		
Edit	<input checked="" type="checkbox"/>	GE2			DHCP	Auto Detect
Edit	<input checked="" type="checkbox"/>	GE3			DHCP	disabled
Edit	<input type="checkbox"/>	GE4			DHCP	Auto Detect
Edit	<input type="checkbox"/>	GE5			DHCP	Auto Detect
Edit	<input type="checkbox"/>	GE6			DHCP	Auto Detect
Edit	<input type="checkbox"/>	GE7			DHCP	Auto Detect
Edit	<input type="checkbox"/>	GE8			DHCP	Auto Detect

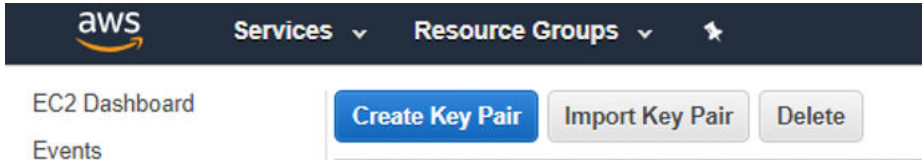
- 3 按一下 GE2 介面的編輯 (**Edit**) 連結，以變更介面設定。
隨即顯示 GE2 介面設定的對話方塊。
- 4 在 GE2 介面設定 (**Interface Settings**) 對話方塊中，按一下覆寫介面 (**Override Interface**) 核取方塊，然後完成下列步驟：
 - a 在功能 (**Capability**) 下拉式功能表中，將 GE2 介面功能從已交換 (**Switched**) 變更為已路由 (**Routed**)。
 - b 從定址類型 (**Addressing Type**) 下拉式功能表中選擇 DHCP。
 - c 勾選 **WAN 覆疊 (WAN Overlay)** 核取方塊來啟用 WAN 覆疊。
- 5 按一下 GE3 介面的編輯 (**Edit**) 連結，以變更介面設定。
隨即顯示 GE3 介面設定的對話方塊。
- 6 在 GE3 介面設定對話方塊中，按一下覆寫介面 (**Override Interface**) 核取方塊，然後完成下列步驟：
 - a 取消勾選 **WAN 覆疊 (WAN Overlay)** 核取方塊來停用 WAN 覆疊，因為此介面將用於 LAN 端閘道。
 - b 取消勾選 **NAT 直接流量 (NAT Direct Traffic)** 核取方塊，以停用 NAT 直接流量。

步驟 4：透過 CloudFormation 啟動虛擬 Edge

附註： 如果這是第一次部署虛擬 Edge，則在從 CloudFormation 範本部署之前，您可能需要先「訂閱」AWS Marketplace 中的 Edge 版本。

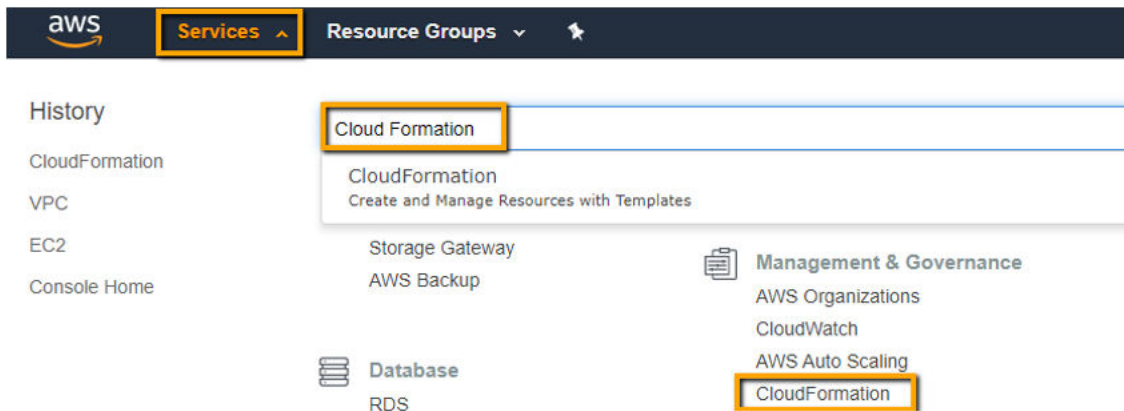
備註 如需如何設定 AWS 特定元件的其他資訊，請參閱 AWS 說明文件。

- 1 登入 AWS 主控台。
- 2 建立或匯入金鑰配對 (Key Pair)。

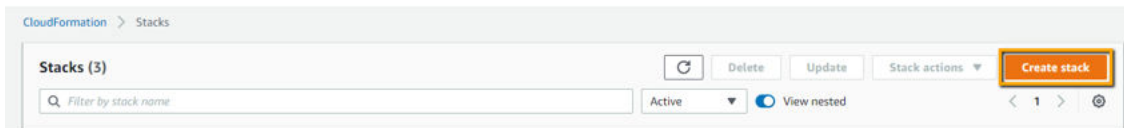


附註： 如需其他有關 AWS EC2 執行個體金鑰的資訊，請參閱：<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>

- 3 導覽至 CloudFormation。



- 4 建立 CloudFormation 堆疊。



- 5 上傳 CloudFormation 範本。

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Template is ready Use a sample template Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL Upload a template file

Upload a template file
 `Velocloud%20AWS%20CloudFormation%20Green%20Field%20%2820190708%29.json`
JSON or YAML formatted file

S3 URL: `https://s3-us-west-1.amazonaws.com/cf-templates-orh6oevth7h-us-west-1/2019288jEm-Velocloud%20AWS%20CloudFormation%20Green%20Field%20%2820190708%29.json`

6 指定堆疊詳細資料，如下圖所示。

Specify stack details

Stack name

Stack name

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

ActivationKey
Edge Activation Key

AvailabilityZone
Availability zone to deploy in

EC2InstanceType
Throughput and number of NICs dictate instance type

IgnoreCertificateValidation
Set to true if using private or self signed certificate on the VCO

PrivateCidrBlockValue
CIDR block for the LAN side of the Edge

PublicCidrBlockValue
CIDR block for the WAN side of the Edge

ResourcePrefix
Prefix used for naming all resources created by this template

SoftwareVersion
VeloCloud Virtual Edge Software Version

VCO
Orchestrator IP address or hostname (fqdn)

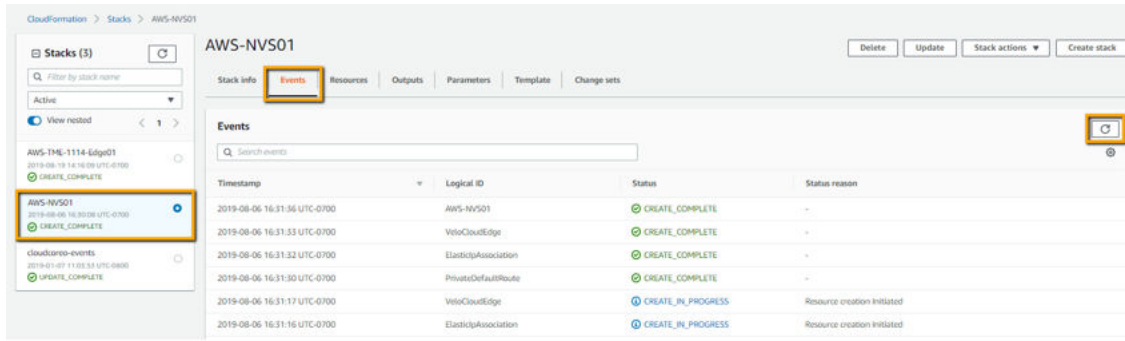
VeloCloudEdgeName
Name of Edge to be deployed

VeloCloudKeyPairName
Public/Private Key Name of Edge to be deployed

VpcCidrBlockValue
CIDR block for the VPC

對於幾個剩餘的畫面，除非您有特定需要變更，否則您可以將這些參數、欄位或文字方塊保留為預設設定。最後一個步驟是建立堆疊。

- 7 檢閱並建立堆疊。
- 8 監控您的部署進度。



EC2 執行個體類型

調整 VMware 虛擬 Edge 的大小時，必須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 和 GE3)。

授權和頻寬階層

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

計算最佳化

執行個體類型	vCPU	記憶體 (Gb)	NIC 數目上限
C4.large	2	3.75	3
C4.xlarge	4	7.5	4
C4.2xlarge	8	15	4
C4.4xlarge	16	30	8
C5.large	2	4	3
C5.xlarge	4	8	4
C5.2xlarge	8	16	4
C5.4xlarge	16	32	8

Amazon EC2 C5 執行個體是下一代的 Amazon EC2 Compute 最佳化執行個體系列。如果需要 C5 執行個體類型 (例如，若要支援類似巴黎區域的特定區域)，則需要 VMware 軟體版本 3.3.1 或更新版本。

執行個體類型	區域	代碼 (Code)	支援的
C5	巴黎	3.3.1	是
C5	巴黎	3.2.2	否
C4	巴黎	3.3.1	否
C5	俄亥俄州	3.3.1	是

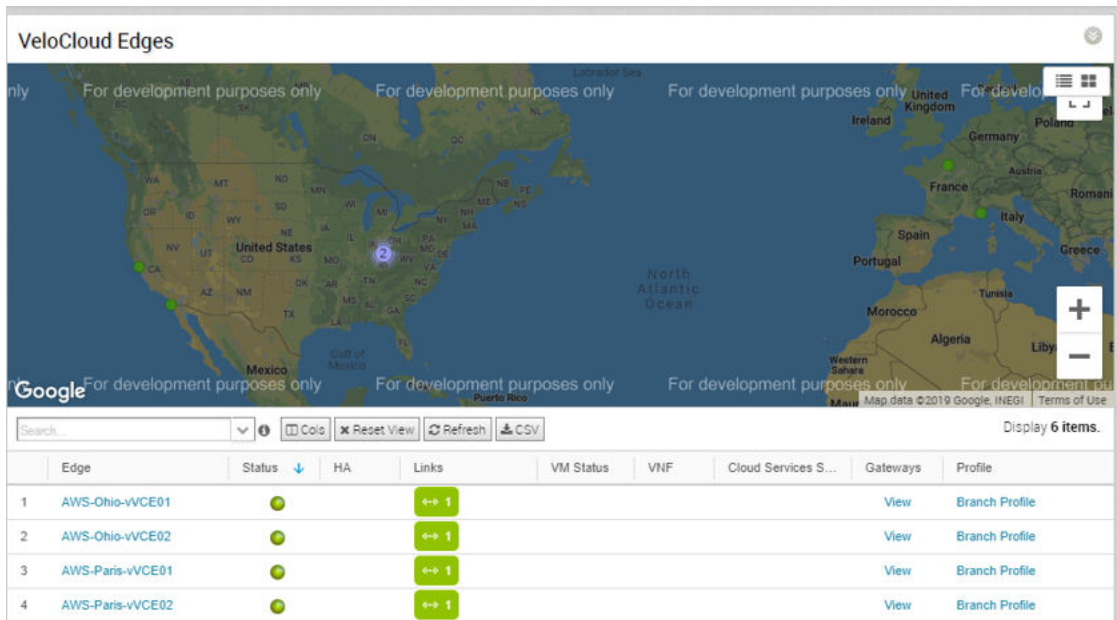
執行個體類型	區域	代碼 (Code)	支援的
C5	俄亥俄州	3.2.2	否
C4	俄亥俄州	3.2.2	是
C4	俄亥俄州	3.3.1	是

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

一旦執行個體在 AWS 中執行，且提供的所有資訊都正確後，虛擬 Edge 將使用啟用金鑰向外連接至 VMware SD-WAN Orchestrator，並視需要啟動和執行軟體更新 (升級後會重新開機)。部署時間通常為三到四分鐘。

程序：

- 1 如有必要，請登入 VMware SD-WAN Orchestrator。
- 2 移至**監控 (Monitor) > Edge**。
隨即顯示 **VeloCloud Edge** 畫面 (請參閱下圖)。
- 3 在 **VeloCloud Edge** 畫面中，確認 **Edge** 資料行中的虛擬 Edge，如下圖所示。



The screenshot shows the 'VeloCloud Edges' interface. At the top, there is a map of the United States with several green dots indicating edge locations. Below the map is a search bar and a table of edge instances. The table has columns for Edge, Status, HA, Links, VM Status, VNF, Cloud Services S..., Gateways, and Profile. There are four rows of data, each representing an edge instance with a status of 'OK' and a link to view the branch profile.

Edge	Status	HA	Links	VM Status	VNF	Cloud Services S...	Gateways	Profile
1 AWS-Ohio-VCE01	OK		↔ 1				View	Branch Profile
2 AWS-Ohio-VCE02	OK		↔ 1				View	Branch Profile
3 AWS-Paris-VCE01	OK		↔ 1				View	Branch Profile
4 AWS-Paris-VCE02	OK		↔ 1				View	Branch Profile