

# AWS Virtual Edge Deployment Guide

2020

VMware SD-WAN 3.4

You can find the most up-to-date technical documentation on the VMware website at:

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

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

Copyright © 2020 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

|          |  |          |
|----------|--|----------|
| <b>1</b> | <b>AWS Virtual Edge Deployment Guide</b>                               | <b>4</b> |
|          | AWS Virtual Edge Deployment Overview                                   | 4        |
|          | Deploying Virtual Edge with CloudFormation                             | 7        |
|          | EC2 Instance Types   | 15       |
|          | Verify the Virtual Edge is Activated in the VMware SD-WAN Orchestrator | 16       |

# AWS Virtual Edge Deployment Guide

# 1

This document provides step-by-step instructions for the AWS Virtual Edge Deployment Guide.

This chapter includes the following topics:

- [AWS Virtual Edge Deployment Overview](#)
- [Deploying Virtual Edge with CloudFormation](#)
- [EC2 Instance Types](#)
- [Verify the Virtual Edge is Activated in the VMware SD-WAN Orchestrator](#)

## AWS Virtual Edge Deployment Overview

This overview of the AWS Virtual Edge Deployment Guide provides a general overview, a CloudFormation Template Overview, and CloudFormation Downloads (Green Field VPC Template and Brown Field Template).

### General Overview

Multi-cloud or hybrid cloud deployments have become increasingly popular over the past few years, and as Enterprise customers move their workload to the Public Cloud infrastructure, they expect to extend SD-WAN from remote branches to the Public Cloud to guarantee SLA. There are two main options offered by VMware SD-WAN depending on the following use cases: leveraging distributed VCGs to establish IPsec towards Public Cloud or deploying the Virtual Edges directly in public cloud virtual private network. This document describes how to deploy Virtual Edges in AWS.

For a small branch deployment that demands a throughput less than 1G, a single Virtual Edge can be deployed in the private network (AWS VPC). For larger data center deployments that demand multi-gig throughput, hub clustering can be deployed.

---

**Note** In the VMware SD-WAN Hub clustering design, since the AWS VPC Router does not support dynamic routing protocol, a third-party L3 virtual router is required in the AWS infrastructure to run BGP between hubs in the cluster and the Layer 3 router for route distribution in LAN. In this solution, we verified with a redundant Cisco Service Router (CSR) 1000v, but other virtual routers that support HA and BGP are expected to work as well.

---

## CloudFormation Template Overview

There are two CloudFormation default templates, "New - Green Field VPC" and "Existing - Brown Field VPC;" both represent a common deployment within AWS, as indicated in the topology illustration in the section titled, [Basic Topology](#). These two CloudFormation default templates create necessary resources, collect the SD-WAN Orchestrator target, and collect the activation key to push via the CLOUD-INIT.

CAUTION: No matter which template you choose, make sure that you review and understand the template before deploying. Both CloudFormation templates are intended to be used as a reference, and they might need altering to accommodate your specific environment.

### CloudFormation Template Values

Listed below are the values included in the CloudFormation templates:

- Attach Interfaces to VMware SD-WAN Instance (GE1 – eth0 / GE2 – eth1 / GE3 – eth2)
- Allocate Elastic IP and attach to GE2
- Create LAN-side and WAN-side Security Groups – Allowed Ports:
  - WAN: GE1 & GE2: UDP 2426 – VMware SD-WAN Multipath Protocol
  - WAN: GE1 & GE2: TCP 22 – SSH Access (for Support Access)
  - WAN: GE1 & GE2: UDP 161 – SNMP
  - LAN: GE3 – ICMP Only (add additional protocols after deployment or modify the template as needed)
- Public Route Table (VPC Router): 0.0.0.0/0 to the Internet Gateway
- Private Route Table (VPC Router): 0.0.0.0/0 to ENI (SD-WAN Edge GE3)
- Disable Source/Destination Check on all interfaces

## CloudFormation Template Downloads

There are two available templates for you to choose from to deploy a Virtual Edge, either New - Green Field VPC or Existing - Brown Field VPC. While these template will activate a Virtual Edge, the simplicity of the topology will not accommodate all environments. Therefore, you must edit your environment accordingly. For a better understanding of the CloudFormation template structure and syntax see: <https://aws.amazon.com/cloudformation/aws-cloudformation-templates/> See sections below for more information about these templates.

### NEW – Green Field VPC Template

Use the Green Field template if you want to create a new VPC. Download the New - Green Field template here: [NEW – Green Field Template](#)

**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

### EXISTING – Brown Field Template

If you use the EXISTING – Brown Field template, the VPC, subnets, and route tables will not be created. The EXISTING – Brown Field template will display drop-down menus that are populated with existing VPC and subnets available for that region. Download the “EXISTING – Brown Field” template here: [EXISTING – Brown Field Template](#).

**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

## Deploying Virtual Edge with CloudFormation

Instructions on how to deploy a Virtual Edge with CloudFormation templates are described below. However, make sure to adhere to the prerequisite requirements prior to deployment.

### Prerequisites

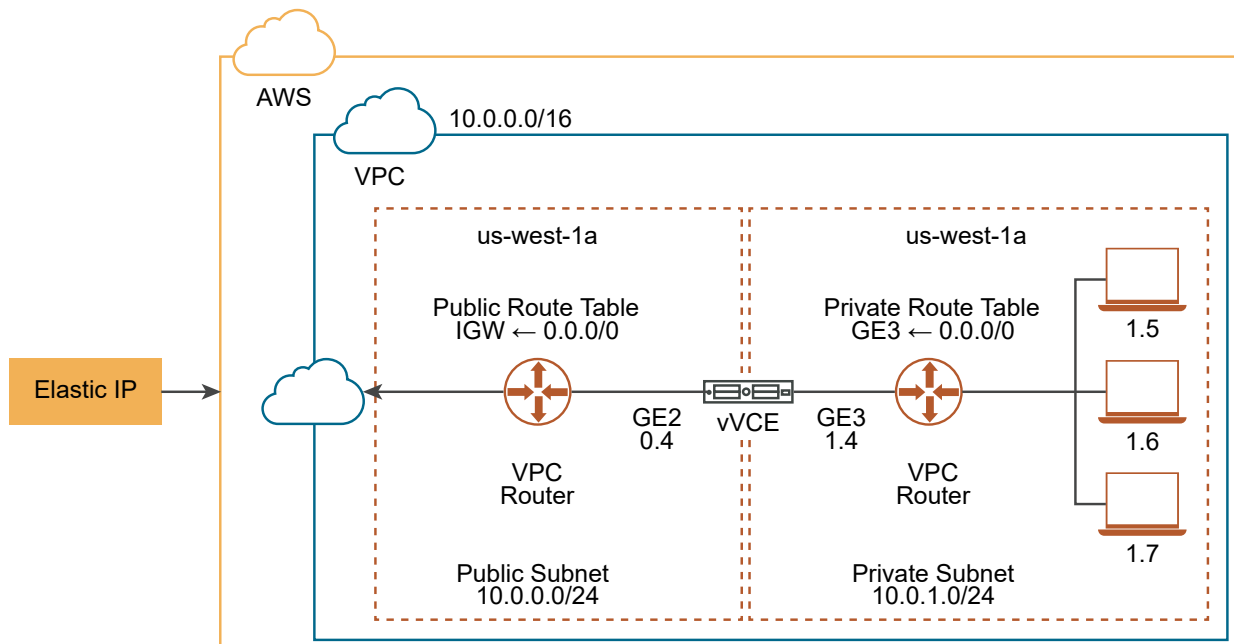
The following are required before you begin to deploy the Virtual Edge with CloudFormation templates:

- AWS account and login information
- Familiarity with AWS networking concepts (see: [https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Networking.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Networking.html))
- RSA Public Key (see: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>)

- VMware SD-WAN CloudFormation Template (one of the following):
  - Green Field Deployment (download [here](#))
  - Brown Field Deployment (download [here](#))
- SD-WAN Orchestrator target and admin account to login

## Basic Topology

In a basic topology example, the AWS VPC (10.0.0.0/16) is divided into a Public subnet (10.0.0.0/24) and a Private subnet (10.0.1.0/24). The Virtual Edge routes between the two subnets. The Public VPC Routes will forward all offnet traffic to the Internet Gateway. The VPC Router in the Private subnet will forward all traffic to the LAN facing interface on the Virtual Edge (ENI of GE3). In this example, a default route is used to forward all traffic from the workloads, but is not necessary. RFC1918 summarization or specific branch/hub prefixes can be used to narrow what is sent to the Virtual Edge. For example, if the workloads in the Private Subnet need to be accessible via the SSH from publicly sourced IPs, then the VPC Router could be configured to point the default route (0.0.0.0/0) to the Internet Gateway and RFC1918 summarization to the Virtual Edge.

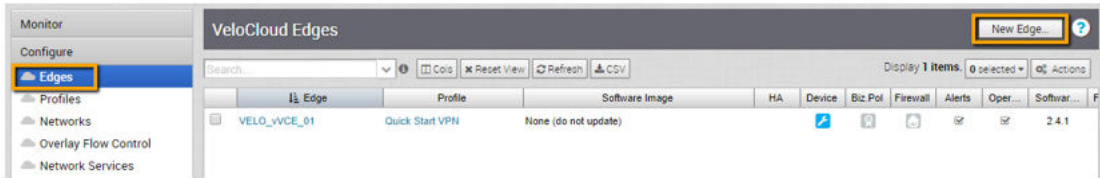


## Procedures:

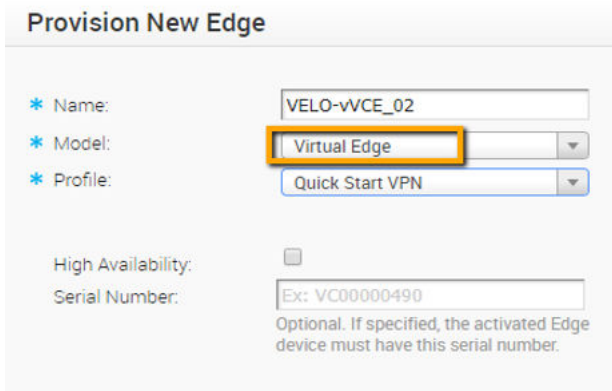
### Step 1: Add the Virtual Edge to the Enterprise via the SD-WAN Orchestrator

- 1 Login to the SD-WAN Orchestrator.
- 2 Go to **Configure > Edges** from the navigation panel, and click the **New Edge** button.

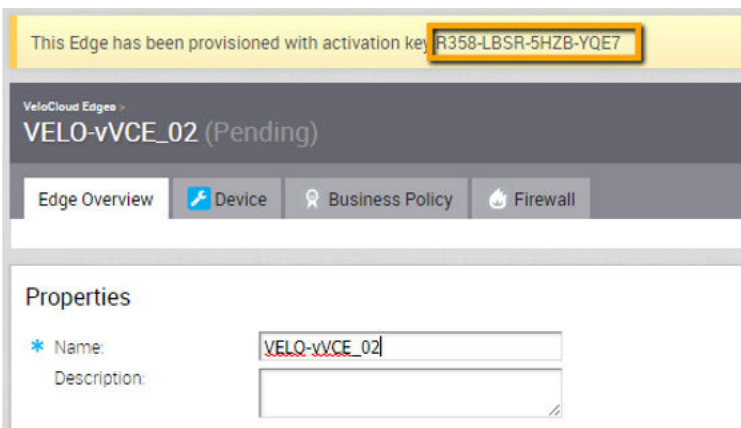




The **Provision New Edge** dialog displays.



- 3 In the **Provision New Edge** dialog box:
  - a Type in a name for the Virtual Edge in the **Name** text box.
  - b In the **Model** drop-down menu, choose **Virtual Edge**.
  - c In the **Profile** dropw-down menu, choose a profile for the Virtual Edge.
  - d **Leave the High Availability checkbox unchecked because it does not apply.**
  - e Leave the Serial Number text box blank.
  - f Click **Save**.
- 4 The Virtual Edge will be provisioned with an activation key. Make a note of the activation key, as it will be used when you deploy the CloudFormation template.



## Step 2: Add VLAN IP

The VLAN configuration must have an IP address assigned to it in order to save the Device Settings, but the IP address will not be used. For example, use IP address 169.254.0.1. Follow the steps below to add the VLAN IP address.

- 1 For the Virtual Edge that was just created, click the **Device** tab on the SD-WAN Orchestrator.
- 2 Scroll down to the **Configure VLAN** section, and click the **Add VLAN** button.

The **VLAN** dialog box displays.

The screenshot shows the 'VLAN' configuration dialog box. Key fields and their values are as follows:

- Segment:** Global Segment
- VLAN Name:** Corporate
- VLAN Id:** 1
- Assign Overlapping Subnets:** Disabled
- 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, 10.0.2.5, Description (optional)
- LAN Interfaces:** GE1, GE2
- SSID:** There are no Wi-Fi SSIDs configured on this VLAN.
- DHCP Type:** Disabled
- OSPF:** Enabled (Note: OSPF not enabled for the selected Segment)

Buttons at the bottom right: Update VLAN, Cancel.

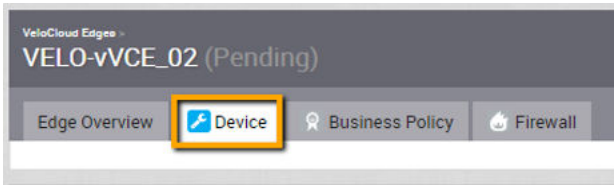
- 3 In the **VLAN** dialog box complete the following:
  - a As necessary, enable Edge override by checking the **Edge Override** checkbox.
  - b Choose a segment from the **Segment** drop-down menu.
  - c The **VLAN Name** displays the default name and can be ignored.
  - d The **VLAN ID** displays the default value and can be ignored.
  - e **Assign Overlapping Subnets** is disabled by default.
  - f Enter 169.254.0.1 in the **Edge LAN IP Address** text box.
  - g Enter 24 in the **Cidr Prefix** text box.
  - h The **Network** value will be configured based on the Cidr Prefix.
  - i Leave the **Advertise** checkbox unchecked.
  - j The remaining fields (Multicast, Fixed IPs, LAN Interfaces, and SSID) can be left at their default settings.

- k As necessary, enable SD-WAN Edge override by checking the **Edge Override** checkbox to disable DHCP.
- l For the **DHCP Type**, click **Disabled**.
- m The **OSPF** area, can be ignored.

### Step 3: Configure Virtual Edge Interfaces

**WARNING:** The **Device Settings** must be configured first in the SD-WAN Orchestrator first before SD-WAN Edge activation. If you skip this step, the Virtual Edge will activate, but will go offline a few minutes later.

- 1 Navigate to the Virtual Edge's Device Settings (**Configure > Edge > Device tab**).



- 2 Scroll down to the **Interface Settings** section.

The screenshot shows the 'Interface Settings' section with a table of interfaces. A red arrow points to the 'Auto Detect' checkbox for the GE2 interface, which is highlighted with a yellow box.

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

- 3 Click the **Edit** link for the GE2 interface to change the interface settings.  
The dialog box for the GE2 interface settings displays.
- 4 In the GE2 **Interface Settings** dialog box, click the **Override Interface** checkbox and complete the following steps:
  - a In the **Capability** drop-down menu, change the GE2 interface capability from **Switched** to **Routed**.
  - b Choose DHCP from the **Addressing Type** drop-down menu.
  - c Enable the WAN Overlay by checking the **WAN Overlay** checkbox.
- 5 Click the **Edit** link for the GE2 interface to change the interface settings.

The dialog box for the GE3 interface settings displays.

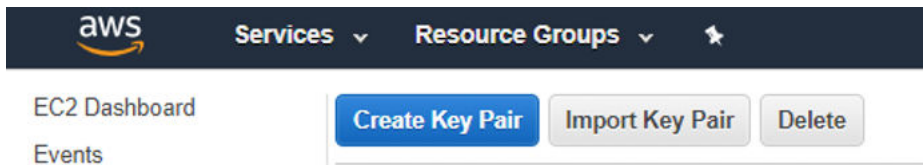
- 6 In the GE3 interface settings dialog box, click the **Override Interface** checkbox and complete the following steps:
  - a Disable the WAN Overlay by unchecking the **WAN Overlay** checkbox, as this interface will be used for the LAN-side gateway.
  - b Uncheck the **NAT Direct Traffic** checkbox to disable NAT direct traffic.

## Step 4: Launch Virtual Edge via CloudFormation

**NOTE:** If this is the first deployment of the Virtual Edge, you may need to “Subscribe” to the Edge version in the AWS Marketplace before deploying from the CloudFormation Template.

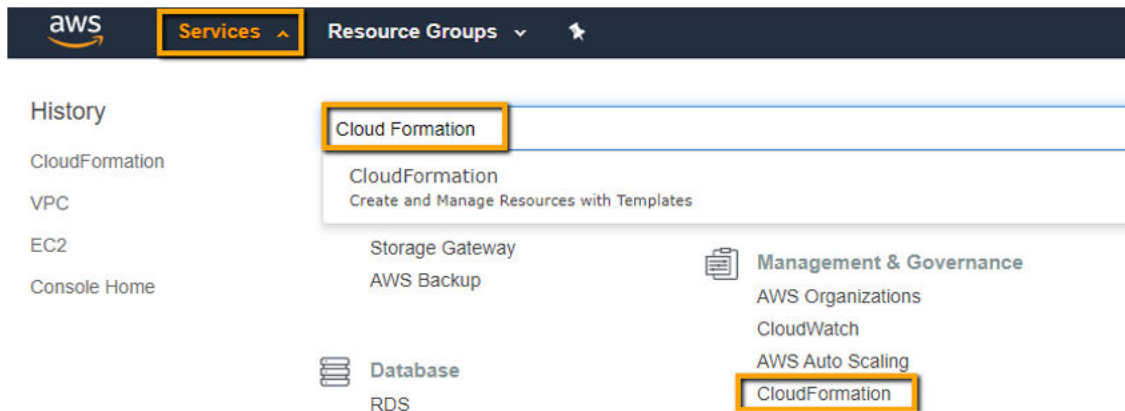
**Note** For additional information on how to configure AWS specific components, please refer to the AWS documentation.

- 1 Log into the AWS console.
- 2 Create or Import a Key Pair.



**NOTE:** For additional information regarding AWS EC2 Instance Keys see: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html>

- 3 Navigate to CloudFormation.



- 4 Create a CloudFormation stack.



5 Upload the CloudFormation template.

**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 Specify the stack details as indicated in the image below.

### 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)

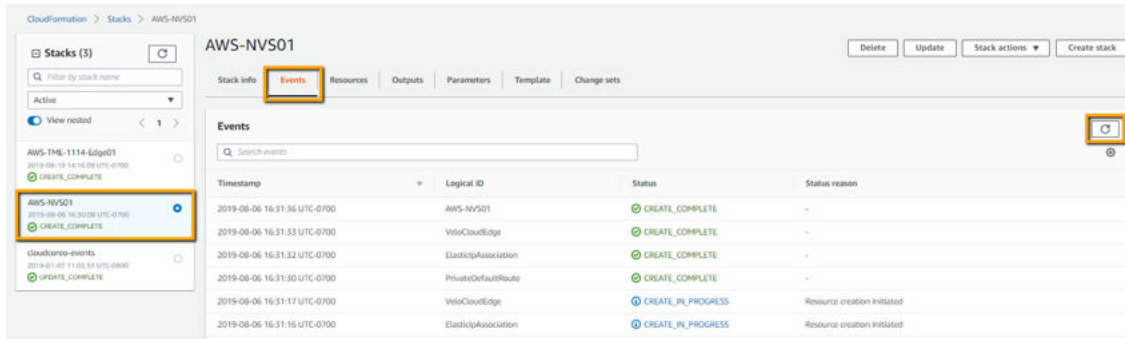
**VeloCloudEdgeName**  
Name of Edge to be deployed

**VeloCloudKeyPairName**  
Public/Private Key Name of Edge to be deployed

**VpcCidrBlockValue**  
CIDR block for the VPC

For the few remaining screens, you can leave those parameters, fields, or text boxes as default settings unless you have a specific need to change them. The final step is to create the stack.

- 7 Review and create the stack.
- 8 Monitor your deployment progress.



## EC2 Instance Types

Bandwidth throughput and the number of network interfaces must be considered when sizing the VMware SD-WAN Virtual Edge. The minimum number of network interfaces required is three (GE1, GE2, and GE3).

### License and Bandwidth Tier

| Throughput | 30 Mbps | 50 Mbps | 100 Mbps | 200 Mbps | 400 Mbps | 1 Gbps |
|------------|---------|---------|----------|----------|----------|--------|
| vCPU       | 2       | 2       | 2        | 2        | 4        | 4      |
| Memory     | 4 GB    | 4 GB    | 4 GB     | 8 GB     | 8 GB     | 8 GB   |

## Compute Optimized

| Instance Type | vCPUs | Memory (Gb) | Max NICs |
|---------------|-------|-------------|----------|
| 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 instances are the next generation of the Amazon EC2 Compute Optimized instance family. If C5 instance type is required, for example, to support a specific region like the Paris region, then the VMware SD-WAN software version 3.3.1 or newer is required.

| Instance Typ | Region | Code  | Supported |
|--------------|--------|-------|-----------|
| C5           | Paris  | 3.3.1 | Yes       |
| C5           | Paris  | 3.2.2 | No        |
| C4           | Paris  | 3.3.1 | No        |
| C5           | Ohio   | 3.3.1 | Yes       |

| Instance Typ | Region | Code  | Supported |
|--------------|--------|-------|-----------|
| C5           | Ohio   | 3.2.2 | No        |
| C4           | Ohio   | 3.2.2 | Yes       |
| C4           | Ohio   | 3.3.1 | Yes       |

## Verify the Virtual Edge is Activated in the VMware SD-WAN Orchestrator

Once the instance is running in AWS and all information provided was correct, the Virtual Edge will reach out to the VMware SD-WAN Orchestrator with the activation key, activate and perform the software update if needed (and reboot if upgraded). The typical deployment time is between three to four minutes.

### Procedures:

- 1 If necessary, login to the VMware SD-WAN Orchestrator.
- 2 Go to **Monitor > Edges**.

The **VeloCloud Edges** screen displays (see image below).

- 3 In the **VeloCloud Edges** screen, verify your Virtual Edge in the **Edges** column as shown in the image below.

