AWS 虚拟 Edge 部署指南

2020

VMware SD-WAN 4.1



vmware®

您可以从 VMware 网站下载最新的技术文档：

https://docs.vmware.com/cn/。

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

威睿信息技术（中国）有限公司
北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

版权所有 © 2020 VMware, Inc. 保留所有权利。 版权和商标信息

目录

1 AWS 虚拟 Edge 部署指南 4

AWS 虚拟 Edge 部署概览 4

使用 CloudFormation 部署虚拟 Edge 7

EC2 实例类型 15

确认在 VMware SD-WAN Orchestrator 中激活了虚拟 Edge。 16

AWS 虚拟 Edge 部署指南

1

本文档提供了《AWS 虚拟 Edge 部署指南》的分步说明。

本章讨论了以下主题：

- AWS 虚拟 Edge 部署概览
- 使用 CloudFormation 部署虚拟 Edge
- EC2 实例类型
- 确认在 VMware SD-WAN Orchestrator 中激活了虚拟 Edge。

AWS 虚拟 Edge 部署概览

此《AWS 虚拟 Edge 部署指南》概述提供了一般概览、CloudFormation 模板概览和 CloudFormation 下载（绿地 VPC 模板和棕地模板）。

一般概览

在过去几年中，多云或混合云部署越来越受欢迎，由于企业客户将工作负载移动到公有云计算基础架构，因此他们期望将 SD-WAN 从远程分支扩展到公有云，以保证 SLA。根据以下用例，VMware 提供了两个主要方案：使用分布式 VCG 建立到公有云的 IPSec 隧道或直接在公有云虚拟专用网络中部署虚拟 Edge。本文档介绍了如何在 AWS 中部署虚拟 Edge。

对于要求吞吐量低于 1G 的小型分支部署，可以在专用网络 (AWS VPC) 中部署单个虚拟 Edge。对于要求吞吐量超过 1G 的大型数据中心部署，可以部署 Hub 集群。

注 在 VMware SD-WAN Hub 集群设计中，由于 AWS VPC 路由器不支持动态路由协议，因此需要在 AWS 基础架构中使用第三方 L3 虚拟路由器以在集群中的 Hub 和第 3 层路由器之间运行 BGP，从而在 LAN 中分配路由。在此解决方案中，我们已通过冗余的 Cisco 服务路由器 (Cisco Service Router, CSR) 1000v 进行了验证，而支持 HA 和 BGP 的其他虚拟路由器也应该可以正常工作。

CloudFormation 模板概览

有两个 CloudFormation 默认模板，即“新 - 绿地 VPC”和“现有 - 棕地 VPC”；这两个模板均代表 AWS 中的常见部署，如标题为基本拓扑 的章节中的拓扑图所述。这两个 CloudFormation 默认模板会创建必要的资源，收集 SD-WAN Orchestrator 目标，并收集激活密钥以通过 CLOUD-INIT 进行推送。

注意：无论您选择哪个模板，请确保在部署之前查看和了解该模板。这两个 CloudFormation 模板都旨在用作参考，可能需要进行更改才能适应您的特定环境。

CloudFormation 模板值

下面列出了 CloudFormation 模板中包含的值：

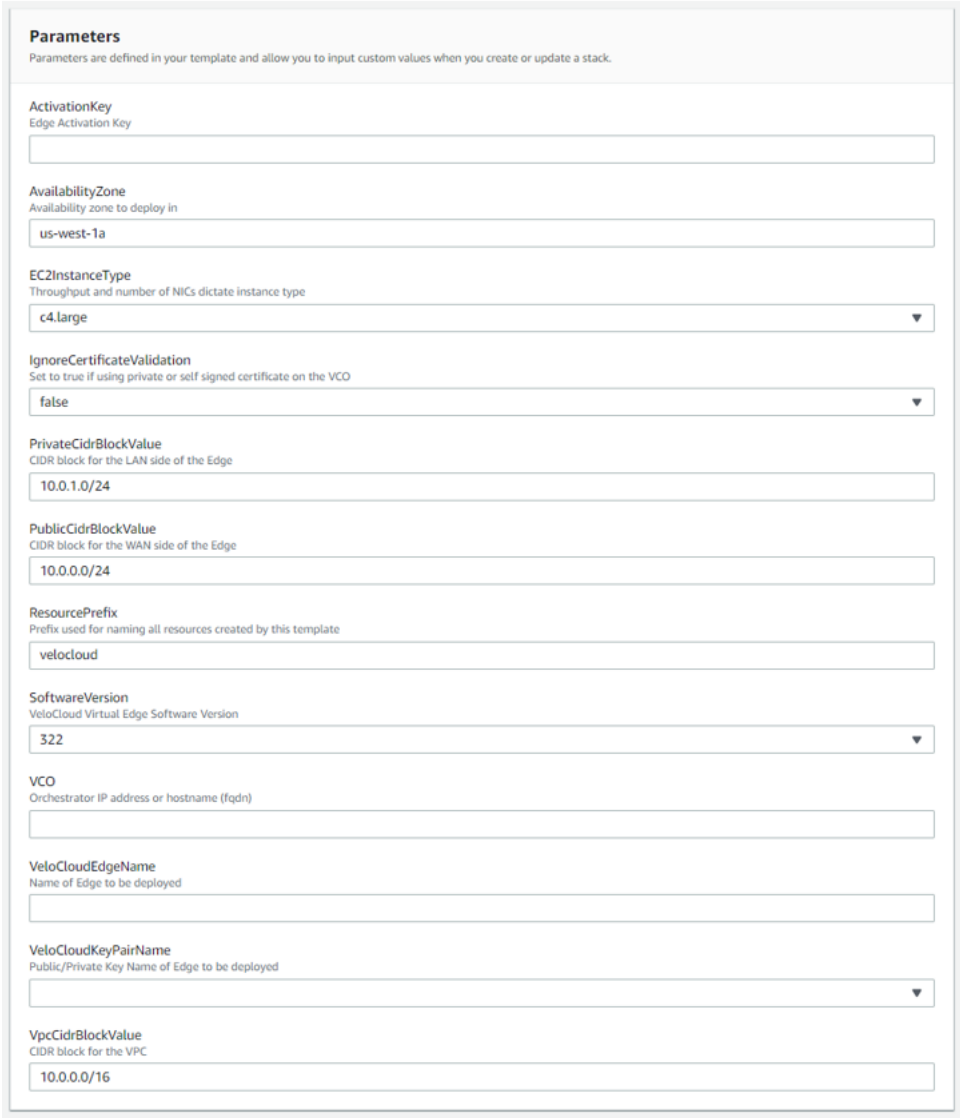
- 将接口连接到 VMware 实例 (GE1 – eth0 / GE2 – eth1 / GE3 – eth2)
- 分配弹性 IP 并连接到 GE2
- 创建 LAN 端和 WAN 端安全组 – 允许的端口：
  - WAN：GE1 & GE2：UDP 2426 – VMware 多路径协议
  - WAN：GE1 & GE2：TCP 22 – SSH 访问（用于支持访问）
  - WAN：GE1 & GE2：UDP 161 – SNMP
  - LAN：GE3 – 仅 ICMP（在部署后添加其他协议或根据需要修改模板）
- 公用路由表（VPC 路由器）：0.0.0.0/0 到 Internet 网关
- 专用路由表（VPC 路由器）：0.0.0.0/0 到 ENI (SD-WAN Edge GE3)
- 在所有接口上禁用源/目标检查

CloudFormation 模板下载

有两个可用模板可供您选择来部署虚拟 Edge，即“新 – 绿地 VPC”或“现有 - 棕地 VPC”。虽然这些模板将激活虚拟 Edge，但拓扑的简单性并不能适应所有环境。因此，您必须相应地编辑您的环境。要更好地了解 CloudFormation 模板结构和语法，请参阅：https://aws.amazon.com/cloudformation/aws-cloudformation-templates/。请参阅下面的章节以了解有关这些模板的更多信息。

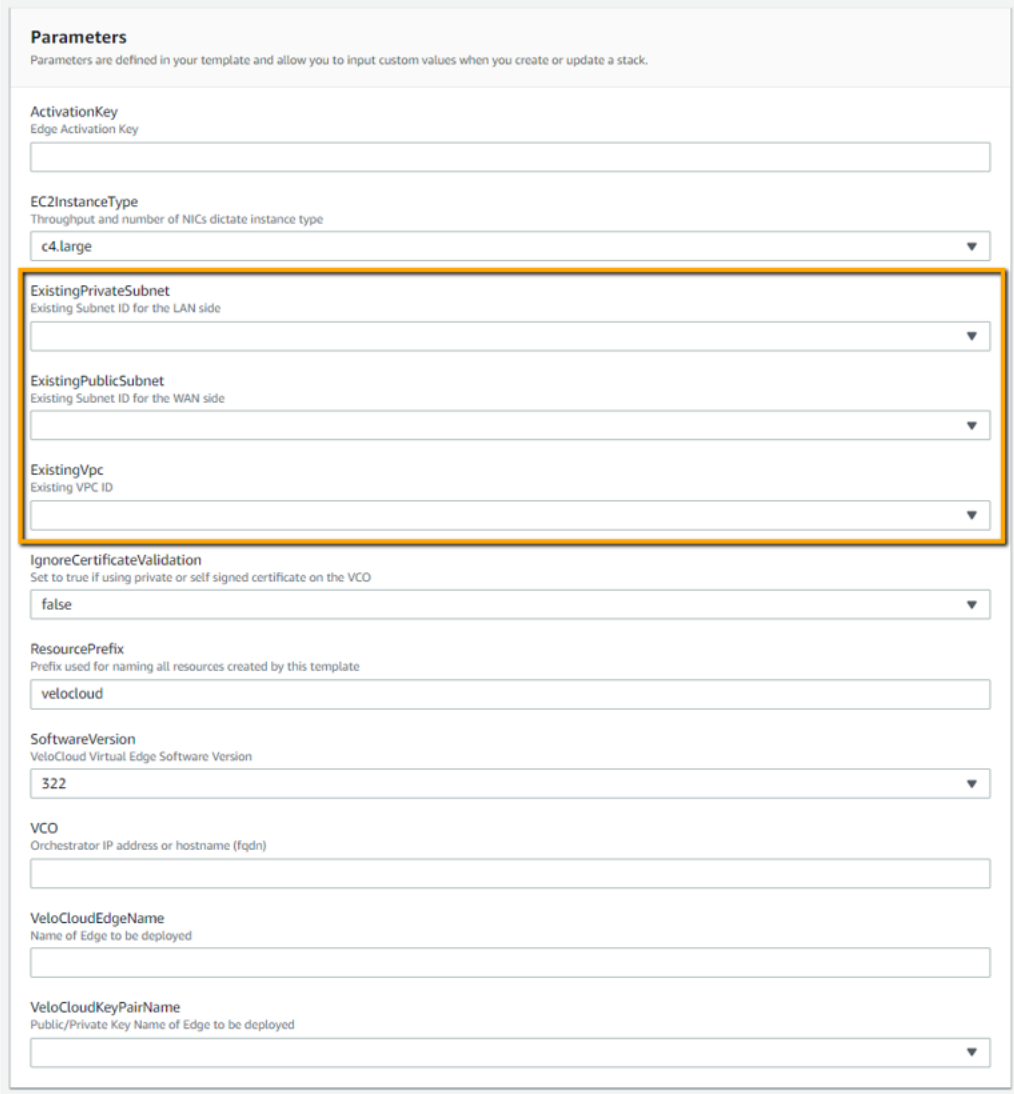
新 – 绿地 VPC 模板

如果要创建新的 VPC，请使用绿地模板。在此处下载“新 – 绿地 VPC”模板：新 – 绿地模板



现有 – 棕地模板

如果使用“现有 – 棕地模板”，则不会创建 VPC、子网和路由表。“现有 – 棕地”模板将显示下拉菜单，其中填充了现有 VPC 和可用于该区域的子网。在此处下载“现有 – 棕地”模板：现有 – 棕地模板。



使用 CloudFormation 部署虚拟 Edge

下面介绍了如何使用 CloudFormation 模板部署虚拟 Edge 的说明。但是，在部署之前，请务必遵循必备条件要求。

必备条件

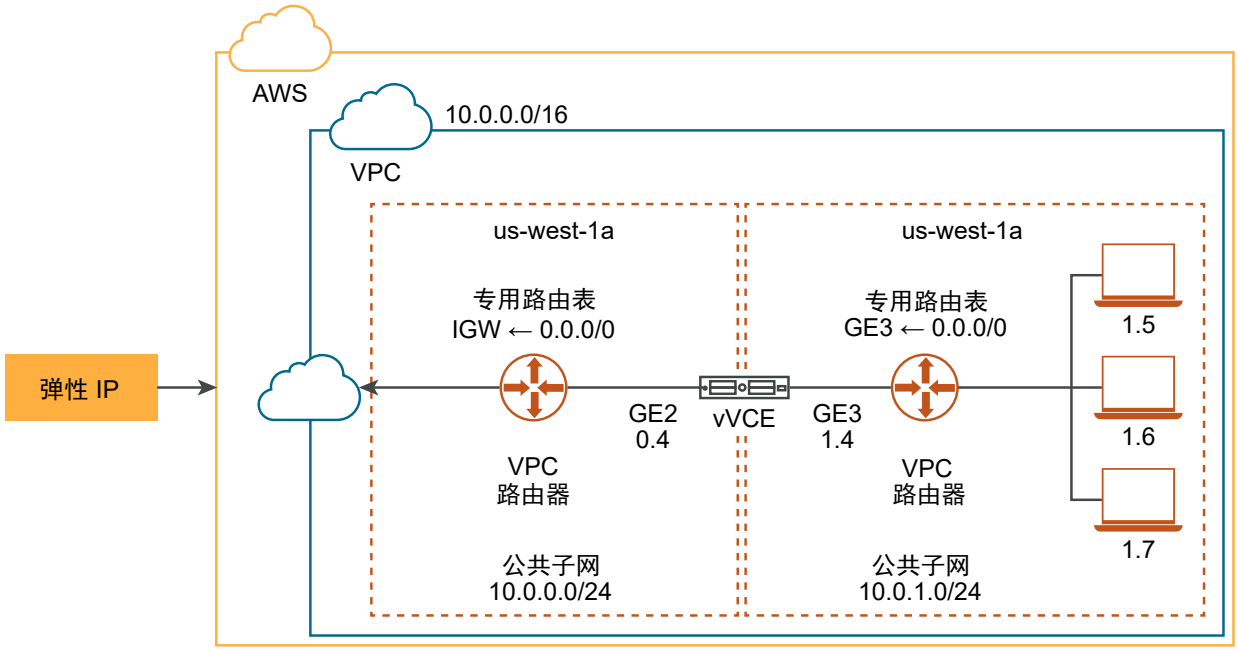
在开始使用 CloudFormation 模板部署虚拟 Edge 之前，需要满足以下条件：

- AWS 帐户和登录信息。
- 熟悉 AWS 网络概念（请参阅：https://docs.aws.amazon.com/zh_cn/vpc/latest/userguide/VPC_Networking.html）
- RSA 公钥（请参阅：https://docs.aws.amazon.com/zh_cn/AWSEC2/latest/UserGuide/ec2-key-pairs.html）

- VMware CloudFormation 模板（以下其中一项）：
  - 绿地部署（在此处下载）
  - 棕地部署（在此处下载）
- 具有 SD-WAN Orchestrator 目标和管理员帐户以进行登录

基本拓扑

在基本拓扑示例中，AWS VPC (10.0.0.0/16) 分为一个公用子网 (10.0.0.0/24) 和一个专用子网 (10.0.1.0/24)。虚拟 Edge 在两个子网之间路由。公用 VPC 路由将所有网络外流量转发到 Internet 网关。专用子网中的 VPC 路由器将所有流量转发到虚拟 Edge（GE3 的 ENI）上面向 LAN 的接口。在该示例中，使用默认路由转发来自工作负载的“所有”流量，但这不是必需的。可以使用 RFC1918 汇总或特定的分支/Hub 前缀减少发送到虚拟 Edge 的内容。例如，如果需要能够通过 SSH 从公开来源的 IP 访问专用子网中的工作负载，则可以配置 VPC 路由器以将默认路由 (0.0.0.0/0) 指向 Internet 网关，并将 RFC1918 汇总指向虚拟 Edge。

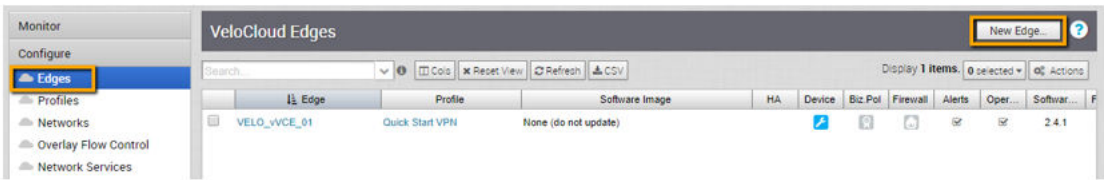


过程：

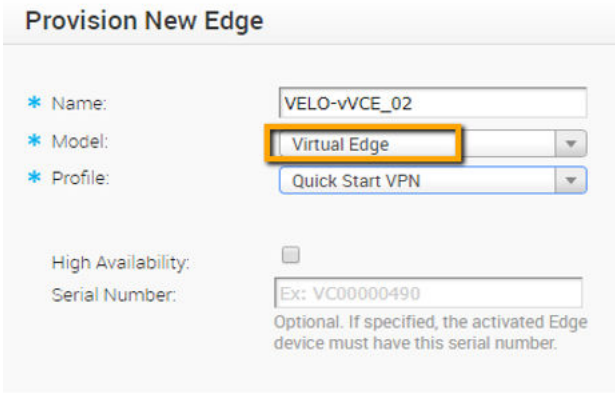
步骤 1：通过 SD-WAN Orchestrator 将虚拟 Edge 添加到企业

1 登录到 SD-WAN Orchestrator。

2 从导航面板转到**配置 (Configure) > Edges**，然后单击 **新建 Edge (New Edge)** 按钮。



将显示**置备新的 Edge (Provision New Edge)** 对话框。



3 在**置备新的 Edge (Provision New Edge)** 对话框中：

a 在**名称 (Name)** 文本框中键入虚拟 Edge 的名称。

b 从**模型 (Model)** 下拉菜单中，选择**虚拟 Edge (Virtual Edge)**。

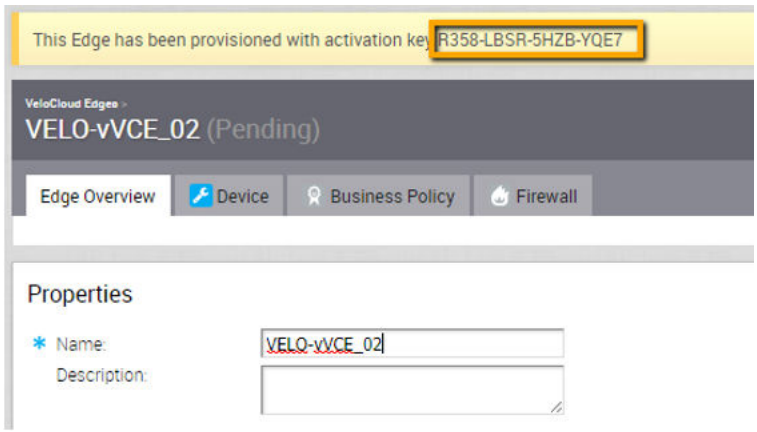
c 在**配置文件 (Profile)** 下拉菜单中，为虚拟 Edge 选择一个配置文件。

d **将“高可用性”(High Availablity) 复选框保持未选中状态，因为它不适用。**

e 将“序列号”(Serial Number) 文本框留空。

f 单击**保存 (Save)**。

4 将使用激活密钥置备虚拟 Edge。记下激活密钥，因为您在部署 CloudFormation 模板时将使用该密钥。



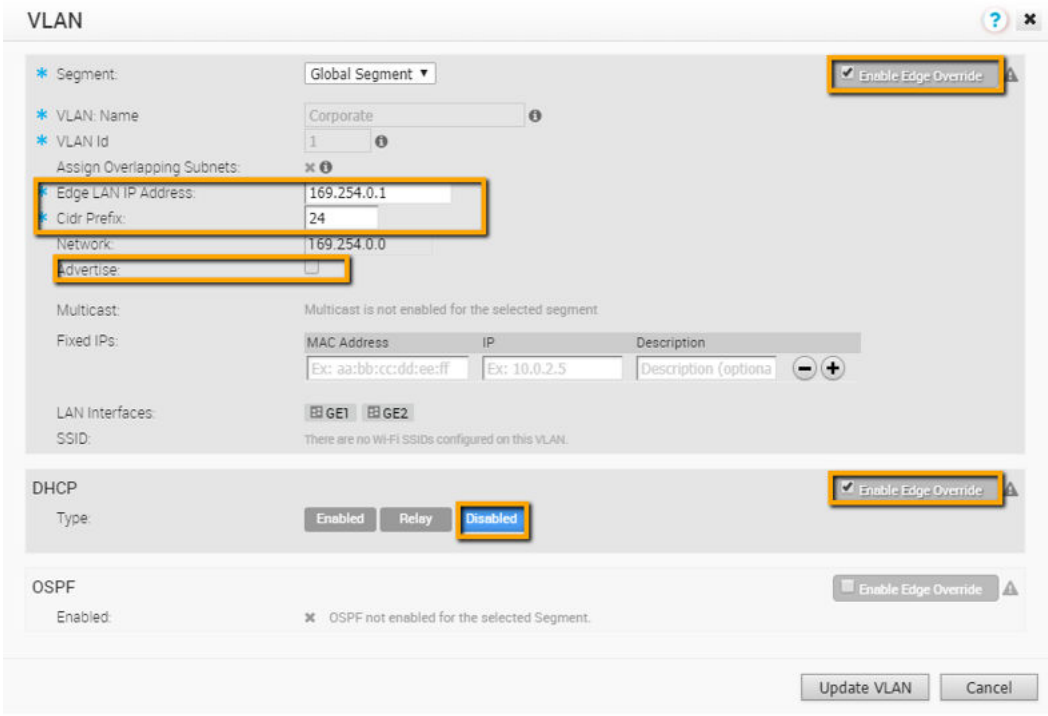
步骤 2：添加 VLAN IP

必须为 VLAN 配置分配一个 IP 地址，才能保存“设备设置”(Device Settings)，但不会使用该 IP 地址。例如，使用 IP 地址 169.254.0.1。请按照以下步骤添加 VLAN IP 地址。

1 对于刚刚创建的虚拟 Edge，单击 SD-WAN Orchestrator 上的**设备 (Device)** 选项卡。

2 向下滚动到**配置 VLAN (Configure VLAN)** 部分，然后单击**添加 VLAN (Add VLAN)** 按钮。

将显示 **VLAN** 对话框。



3 在 **VLAN** 对话框中，完成以下配置：

a 如有需要，请通过选中 **Edge 覆盖 (Edge Override)** 复选框来启用 Edge 覆盖。

b 从**分段 (Segment)** 下拉菜单中选择一个分段。

c **VLAN 名称 (VLAN Name)** 显示默认名称，可以忽略。

d **VLAN ID** 显示默认值，可以忽略。

e 默认情况下，将禁用**分配重叠子网 (Assign Overlapping Subnets)**。

f 在 **Edge LAN IP 地址 (Edge LAN IP Address)** 文本框中输入 169.254.0.1。

g 在 **CIDR 前缀 (Cidr Prefix)** 文本框中输入 24。

h **网络 (Network)** 值将根据 CIDR 前缀进行配置。

i 将 **通告 (Advertise)** 复选框保持未选中状态。

j 剩下字段（“多播”(Multicast)、“固定 IP”(Fixed IPs)、“LAN 接口”(LAN Interfaces) 和 SSID）可以保留其默认设置。

k 如有需要，请通过选中 **Edge 覆盖 (Edge Override)** 复选框来禁用 DHCP，以便启用 SD-WAN Edge 覆盖。

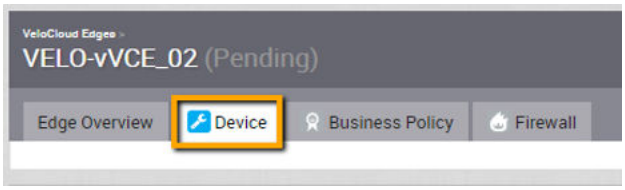
l 对于 **DHCP 类型 (DHCP Type)**，单击**已禁用 (Disabled)**。

m 可以忽略 **OSPF** 区域。

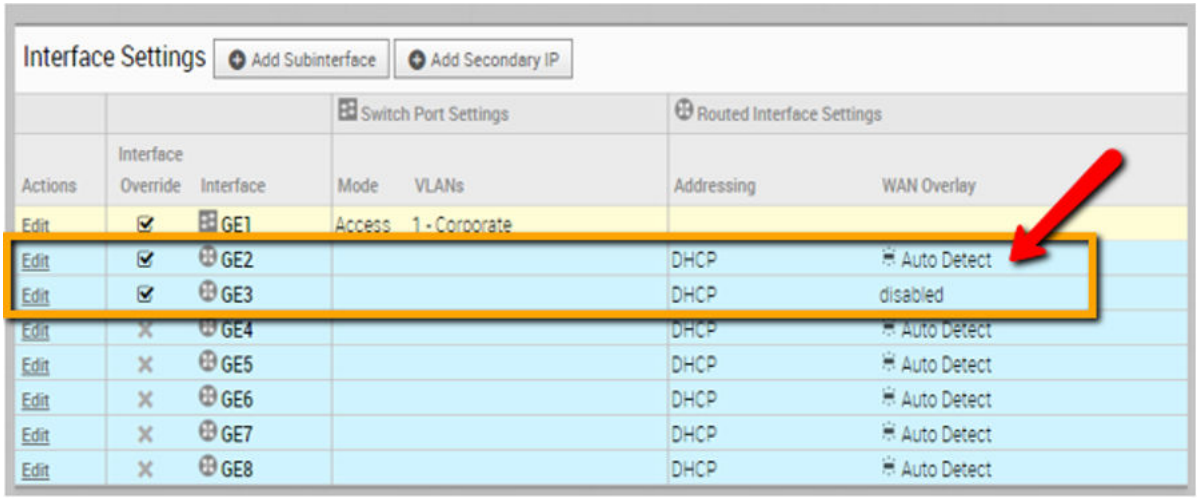
步骤 3：配置虚拟 Edge 接口

警告：在激活 SD-WAN Edge 之前，必须先在 SD-WAN Orchestrator 中配置**设备设置 (Device Settings)**。如果跳过此步骤，将激活虚拟 Edge，但在几分钟后变为脱机状态。

1 导航到虚拟 Edge 的“设备设置”(Device Settings)（**配置 (Configure) > Edge >“设备”(Device)** 选项卡）。



2 向下滚动到 **接口设置 (Interface Settings)** 部分。



3 单击 GE2 接口的**编辑 (Edit)** 链接以更改接口设置。

此时将显示 GE2 接口设置的对话框。

4 在 GE2 **接口设置 (Interface Settings)** 对话框中，单击**覆盖接口 (Override Interface)** 复选框，然后完成以下步骤：

a 在**功能 (Capability)** 下拉菜单中，将 GE2 接口功能从**交换 (Switched)** 更改为**路由 (Routed)**。

b 从**寻址类型 (Addressing Type)** 下拉菜单中选择 DHCP。

c 通过选中 **WAN 覆盖网络 (WAN Overlay)** 复选框来启用 WAN 覆盖网络。

5 单击 GE3 接口的**编辑 (Edit)** 链接以更改接口设置。

此时将显示 GE3 接口设置的对话框。

6 在 GE3“接口设置”(Interface Settings) 对话框中，单击**覆盖接口 (Override Interface)** 复选框，然后完成以下步骤：

a 通过取消选中 **WAN 覆盖网络 (WAN Overlay)** 复选框来禁用 WAN 覆盖网络，因为此接口将用于 LAN 端网关。

b 取消选中 **NAT 直接流量 (NAT Direct Traffic)** 复选框以禁用 NAT 直接流量。

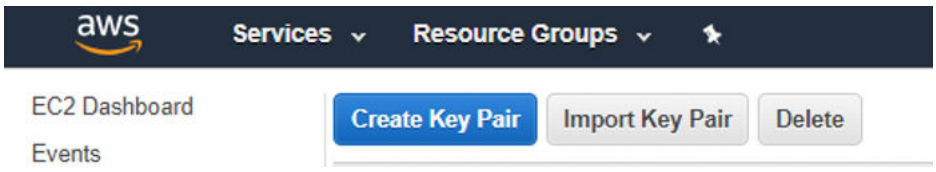
步骤 4：通过 CloudFormation 启动虚拟 Edge

注意：如果这是首次部署虚拟 Edge，则在从 CloudFormation 模板进行部署之前，可能需要在 AWS Marketplace 中“订阅”Edge 版本。

注 有关如何配置 AWS 特定组件的其他信息，请参阅 AWS 文档。

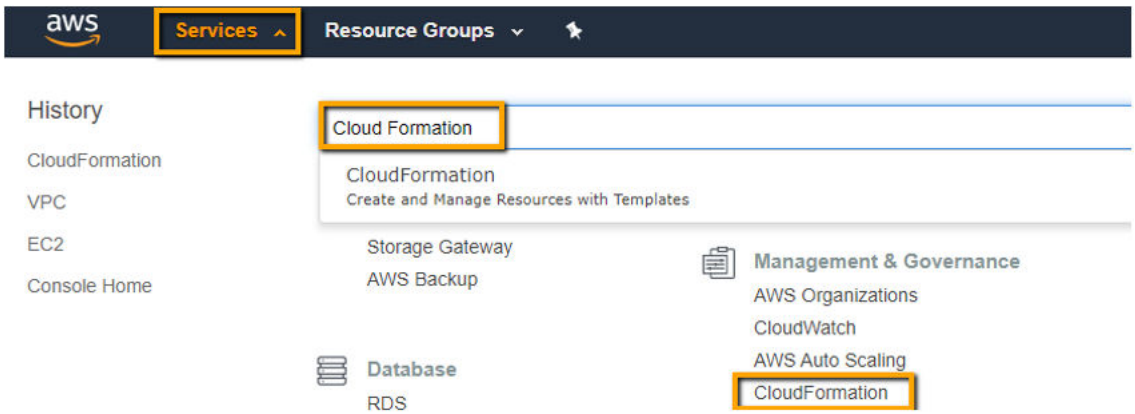
1 登录到 AWS 控制台。

2 创建或导入密钥对。



注意：有关 AWS EC2 实例密钥的更多信息，请参阅：https://docs.aws.amazon.com/zh_cn/AWSEC2/latest/UserGuide/ec2-key-pairs.html

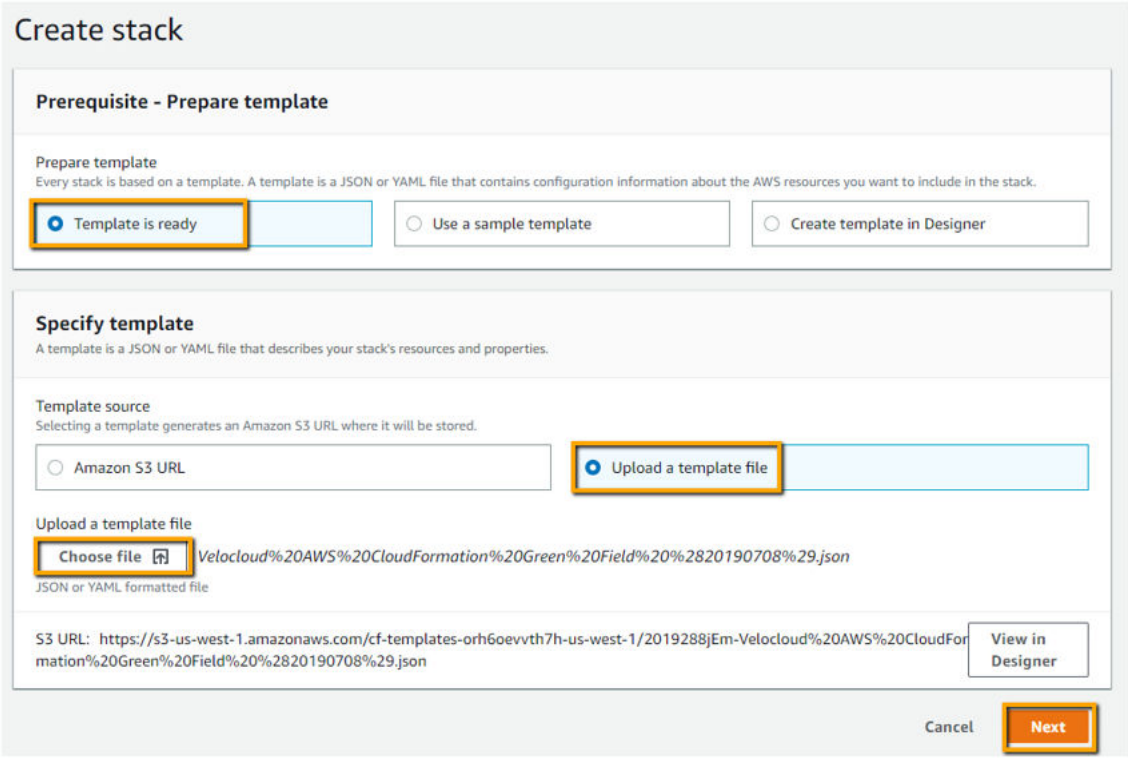
3 导航到 CloudFormation。



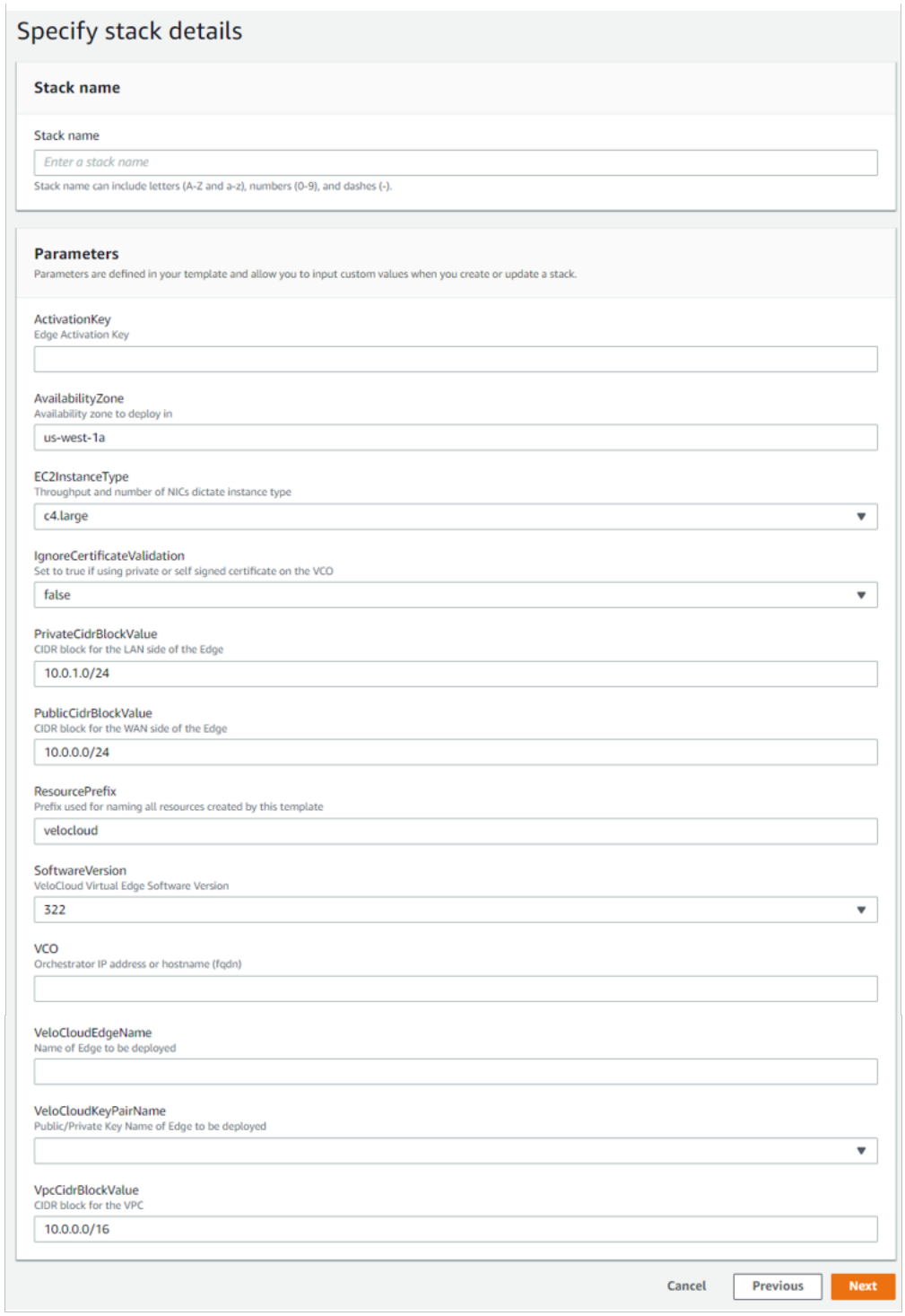
4 创建 CloudFormation 堆栈。



5 上载 CloudFormation 模板。



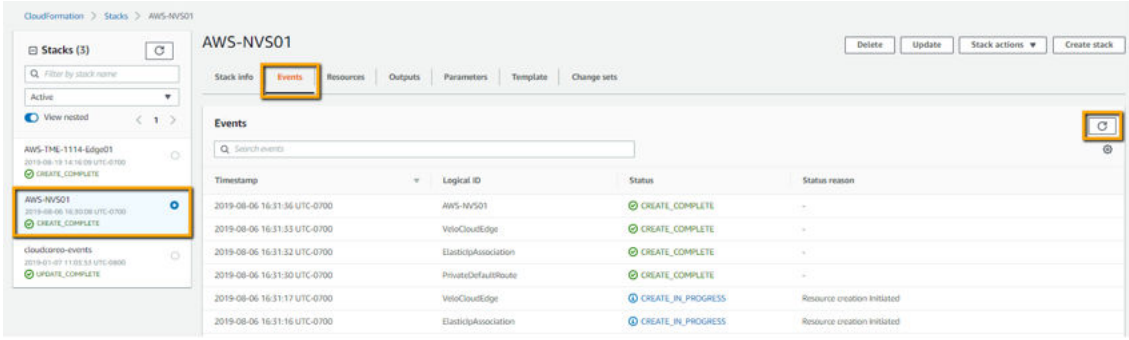
6 按照下图所示，指定堆栈详细信息。



对于剩下的几个屏幕，除非有特定的更改需求，否则可以将这些参数、字段或文本框保留为默认设置。最后一步是创建堆栈。

7 查看并创建堆栈。

8 监控部署进度。



EC2 实例类型

在调整 VMware 虚拟 Edge 大小时，必须考虑带宽吞吐量和网络接口数。所需的最小网络接口数为三个（GE1、GE2 和 GE3）。

许可证和带宽层

吞吐量	30 Mbps	50 Mbps	100 Mbps	200 Mbps	400 Mbps	1 Gbps
vCPU	2	2	2	2	4	4
内存	4 GB	4 GB	4 GB	8 GB	8 GB	8 GB

计算优化型

实例类型	vCPU	内存 (Gb)	最大网卡数
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 实例是新一代 Amazon EC2 计算优化型实例系列。例如，如果需要 C5 实例类型来支持特定区域（例如巴黎区域），则需要 VMware 软件版本 3.3.1 或更高版本。

实例类型	地区	代码 (Code)	受支持
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

实例类型	地区	代码 (Code)	受支持
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

确认在 VMware SD-WAN Orchestrator 中激活了虚拟 Edge。

在 AWS 中运行实例后，如果提供的所有信息正确无误，虚拟 Edge 将使用激活密钥访问 VMware SD-WAN Orchestrator，激活并根据需要执行软件更新（如果已升级，则重新引导）。典型部署时间在三到四分钟之间。

过程：

1 如有必要，请登录到 VMware SD-WAN Orchestrator。

2 转到**监控 (Monitor) > Edge**。

此时将显示 **VeloCloud Edge** 屏幕（请参阅下图）。

3 在 **VeloCloud Edge** 屏幕中，在 **Edge** 列中验证您的虚拟 Edge，如下图所示。

