配置和验证适用于Multicloud - AWS的Cloud OnRamp

目录

简介

本文档介绍如何配置和验证Cisco SD-WAN Cloud OnRamp，以实现与Amazon Web Services (AWS)的多云集成。

先决条件

确保您具有以下优势：

- AWS云帐户详细信息。
- 订购AWS市场。
- Cisco SD-WAN Manager必须有两个可用的Catalyst 8000V OTP令牌才能在其证书选项卡中创建云网关。

要求

Cisco 建议您了解以下主题：

- 思科软件定义的广域网(SD-WAN)
- AWS

使用的组件

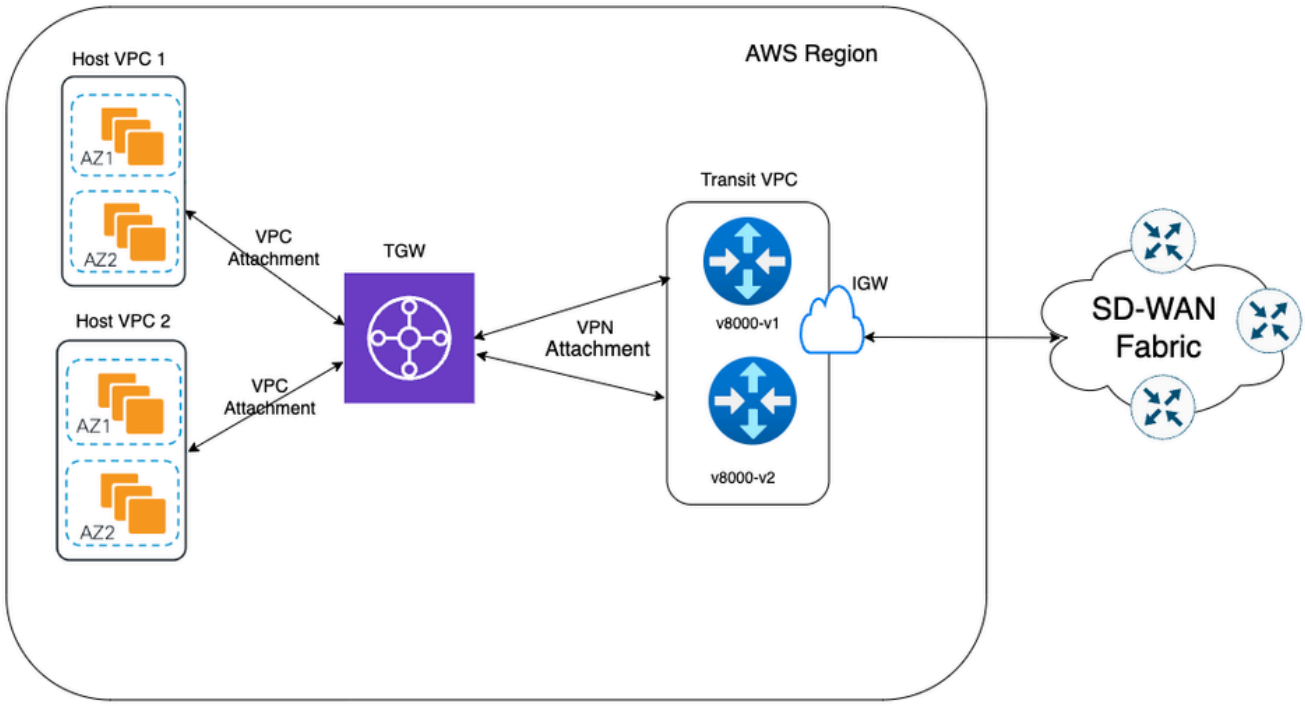
本文档基于以下软件和硬件版本：

- 思科Catalyst SD-WAN Manager版本20.9.4.1
- 思科Catalyst SD-WAN控制器版本20.9.4
- 思科边缘路由器版本17.9.04a

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

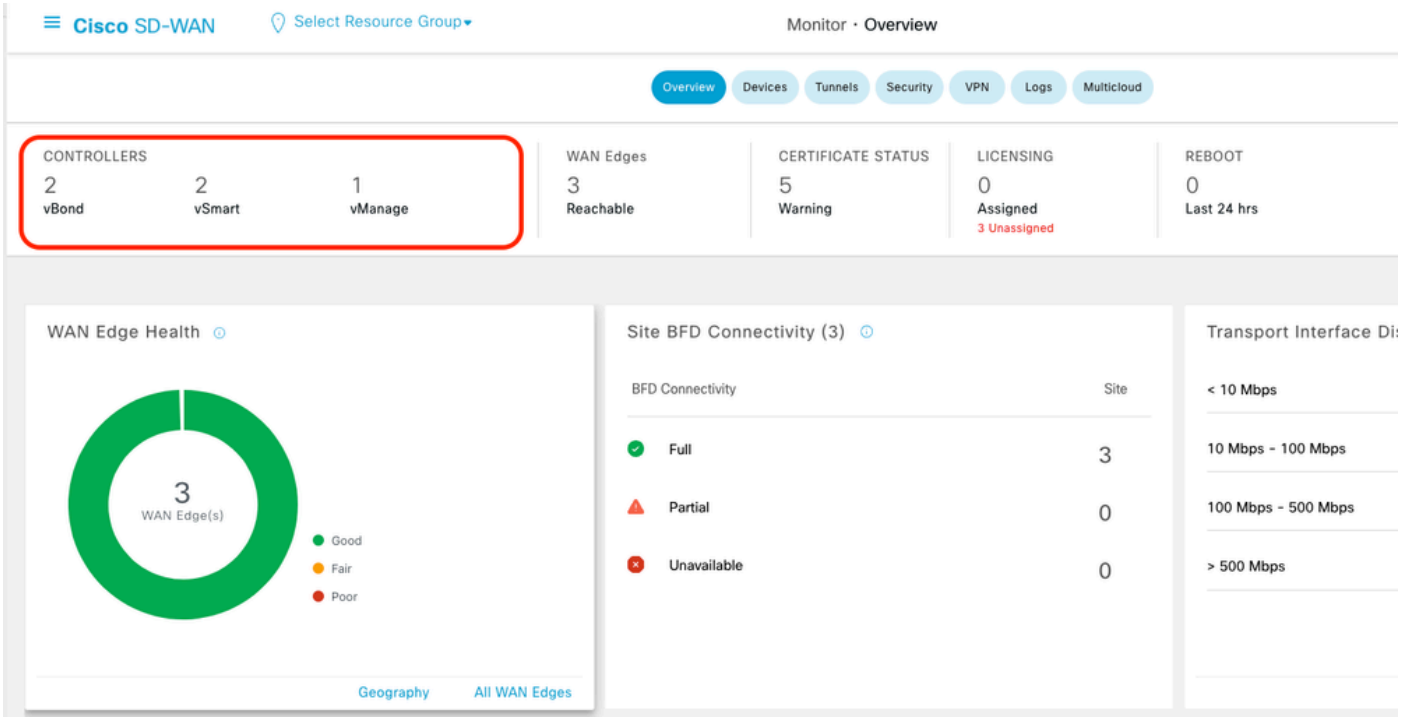
配置

网络图



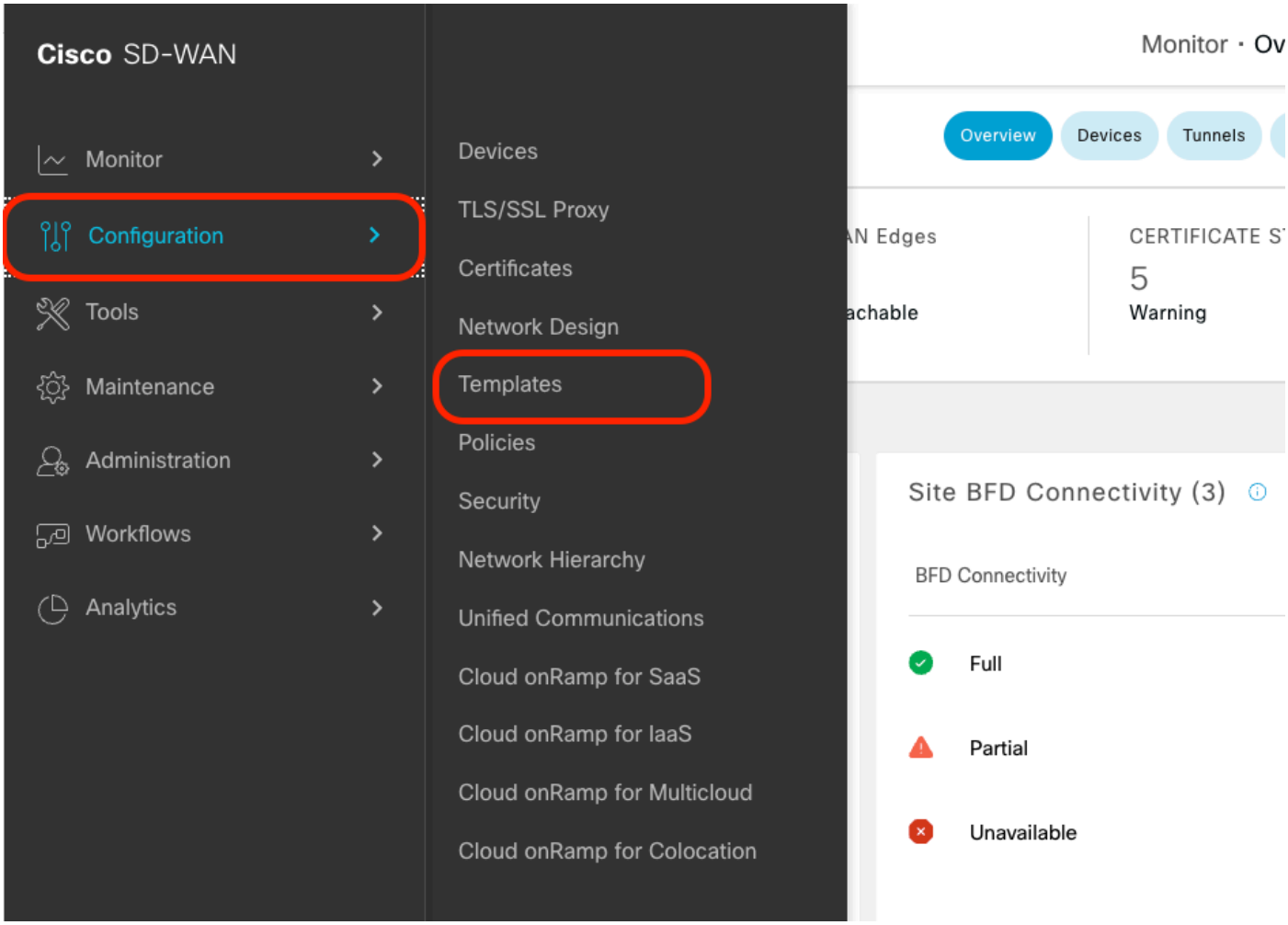
配置

登录Catalyst SD-WAN Manager GUI，验证所有控制器都已启动。

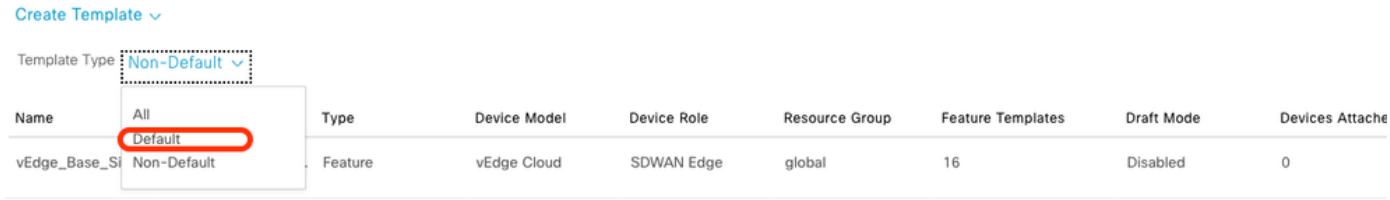


步骤1.将AWS设备模板附加到两个C8000v设备

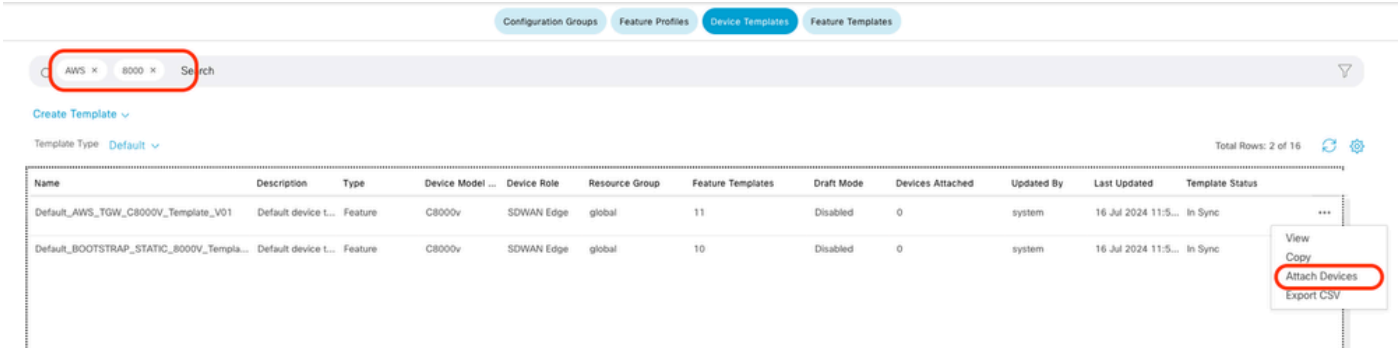
在Cisco SD-WAN Manager菜单上，导航至配置>模板。



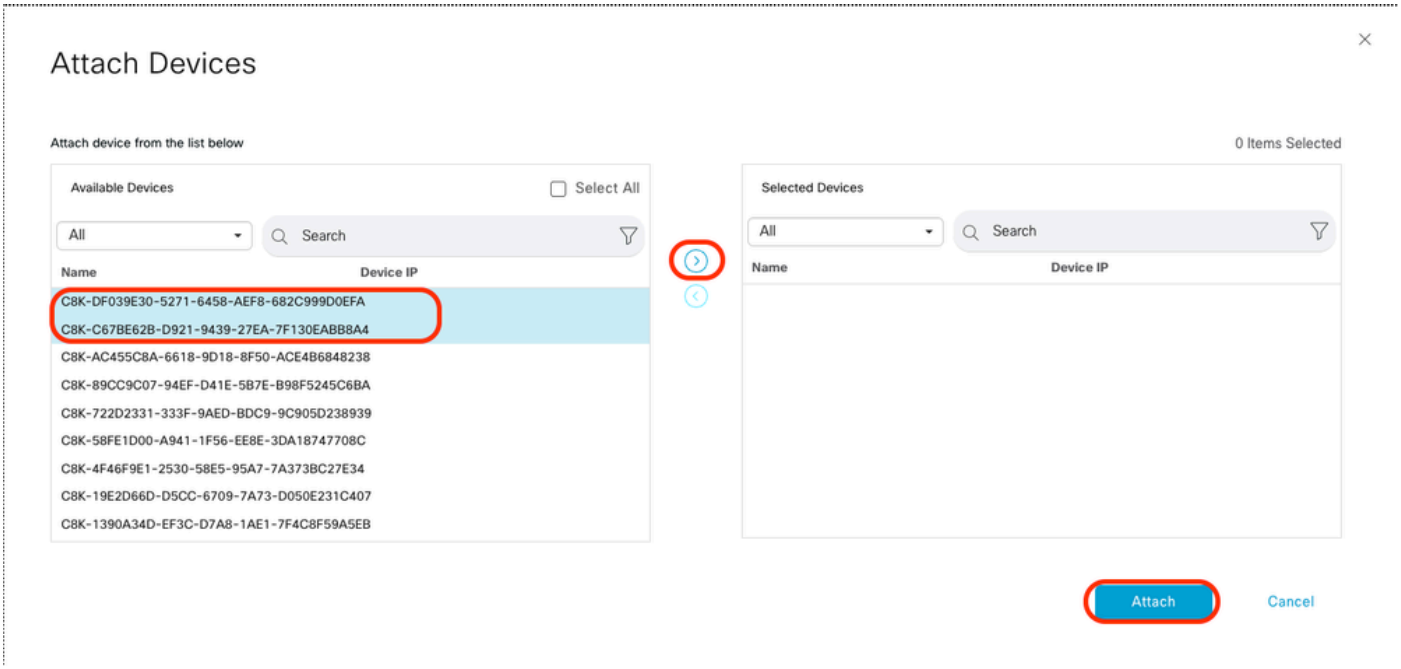
单击Device Templates > From Template。键入下拉菜单并选择Default。



在搜索栏中，键入AWS和C8000v。然后，点击Default_AWS_TGW_C8000V_Template_V01模板旁边的3点(...)。在下拉菜单中选择Attach Devices。



选择两台C8000v设备。单击向右箭头，然后单击连接。



点击设备上的3个点(...)并导航至编辑设备模板。

单击下拉菜单并选择Color，输入Hostname、System IP、Site ID。输入这些详细信息后，单击更新。

输入每台设备的值，然后单击Update。

示例：

<#root>

On

Device 1

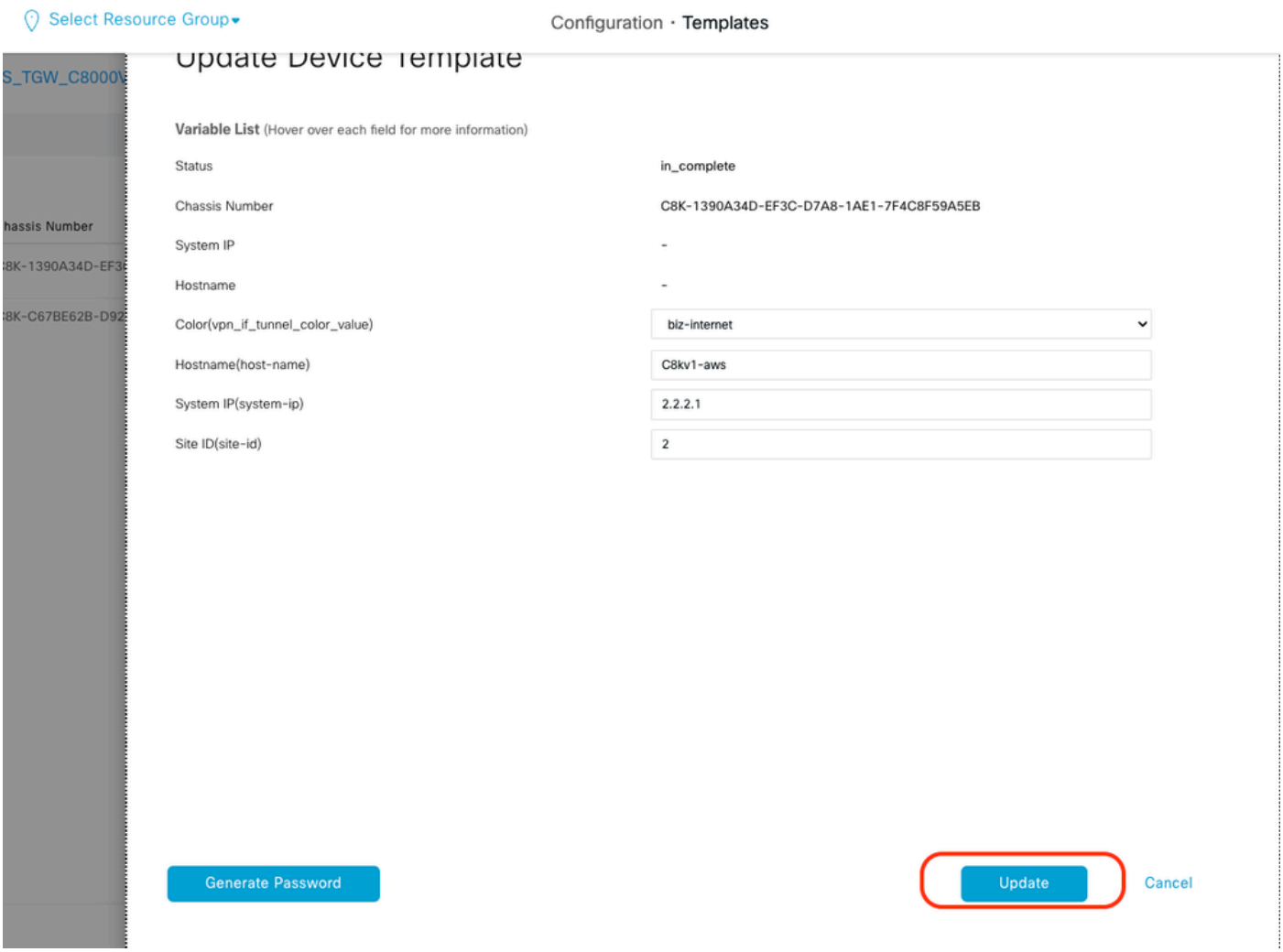
Color: Select biz-internet from Dropdown
Hostname: C8kv1-aws
System IP: 10.2.2.1
Site: ID 2

<#root>

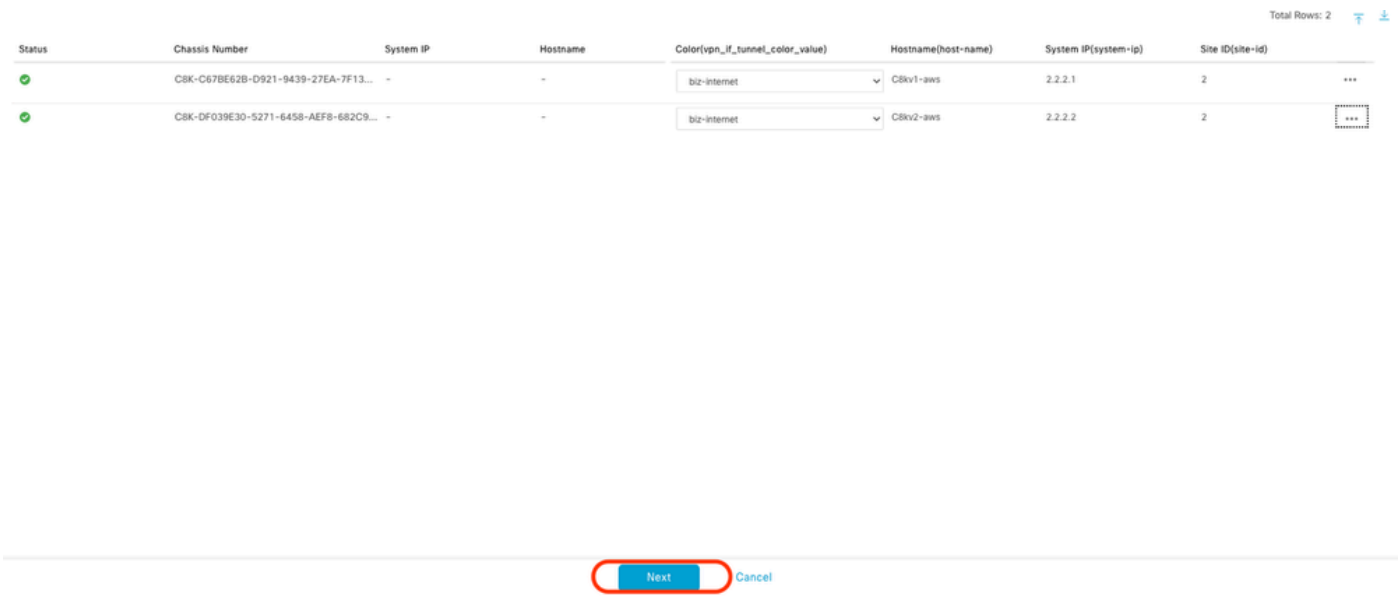
On

Device 2

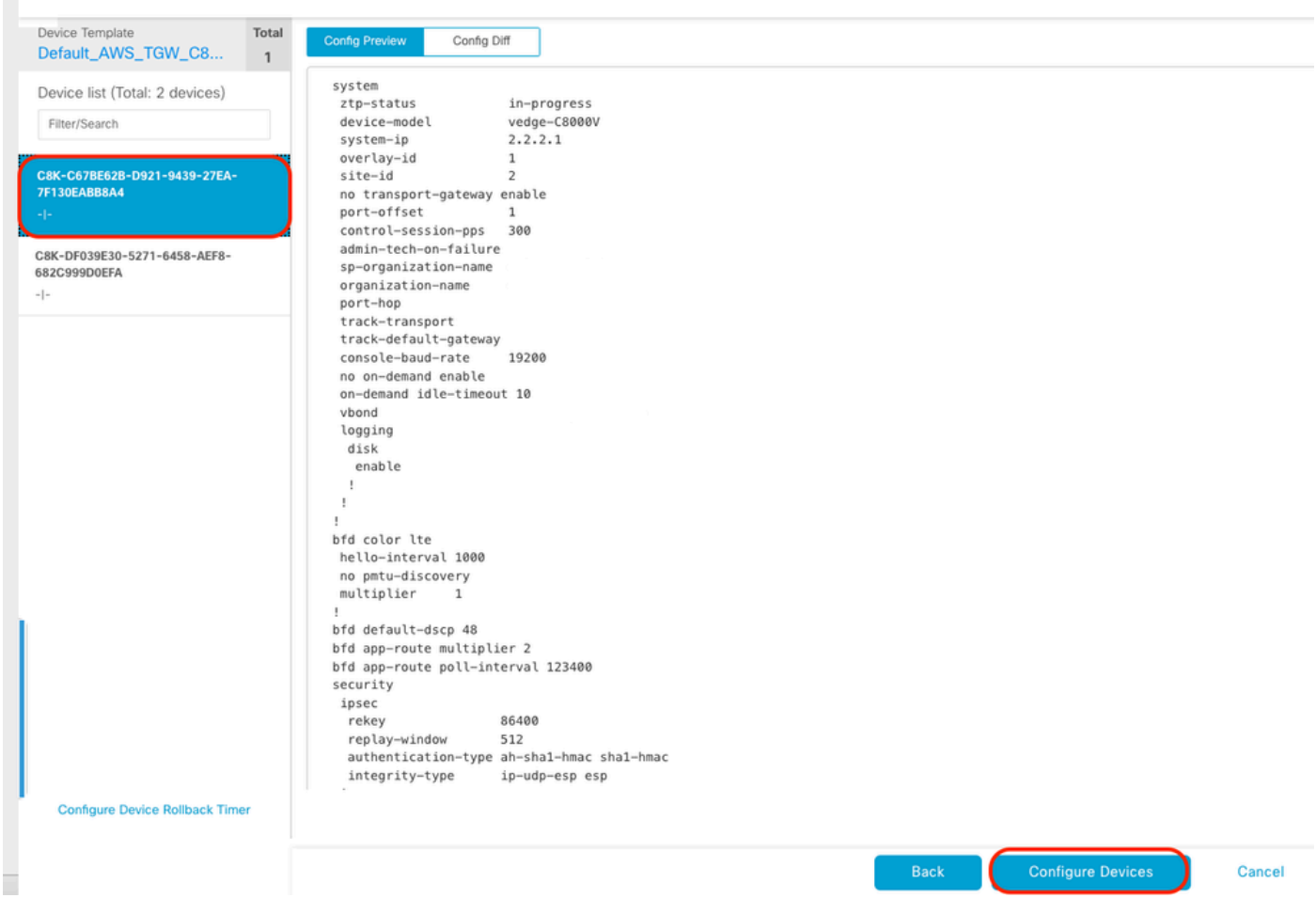
Color: biz-internet Color: biz-internet
Hostname: C8kv2-aws
System IP: 10.2.2.2
Site: ID 2



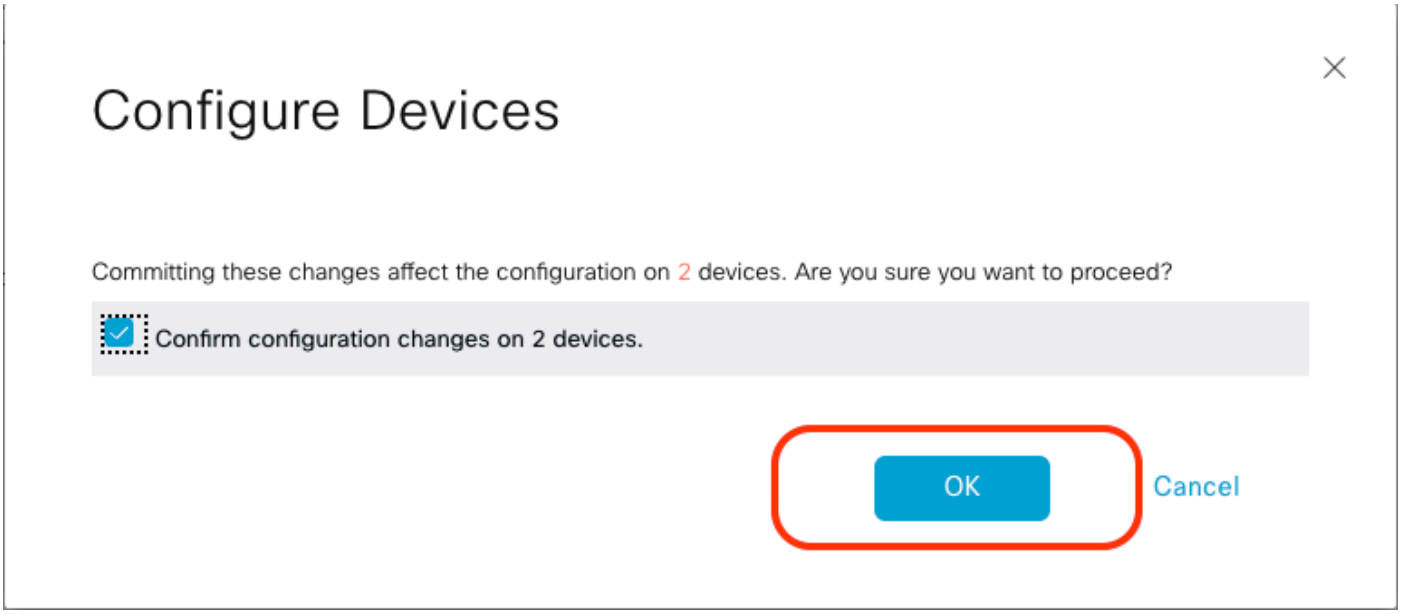
当您完成了对这两个设备的操作时，单击Next。



单击其中一台设备，确保配置正确。单击Configure Devices。



在弹出窗口中，点击2台设备上确认配置更改复选框，然后点击确定。



确认已安排将模板附加到设备。

第二步：配置SD-WAN与AWS的集成

您可以通过Cisco Catalyst SD-WAN Manager为多云环境配置和管理Cloud onRamp。

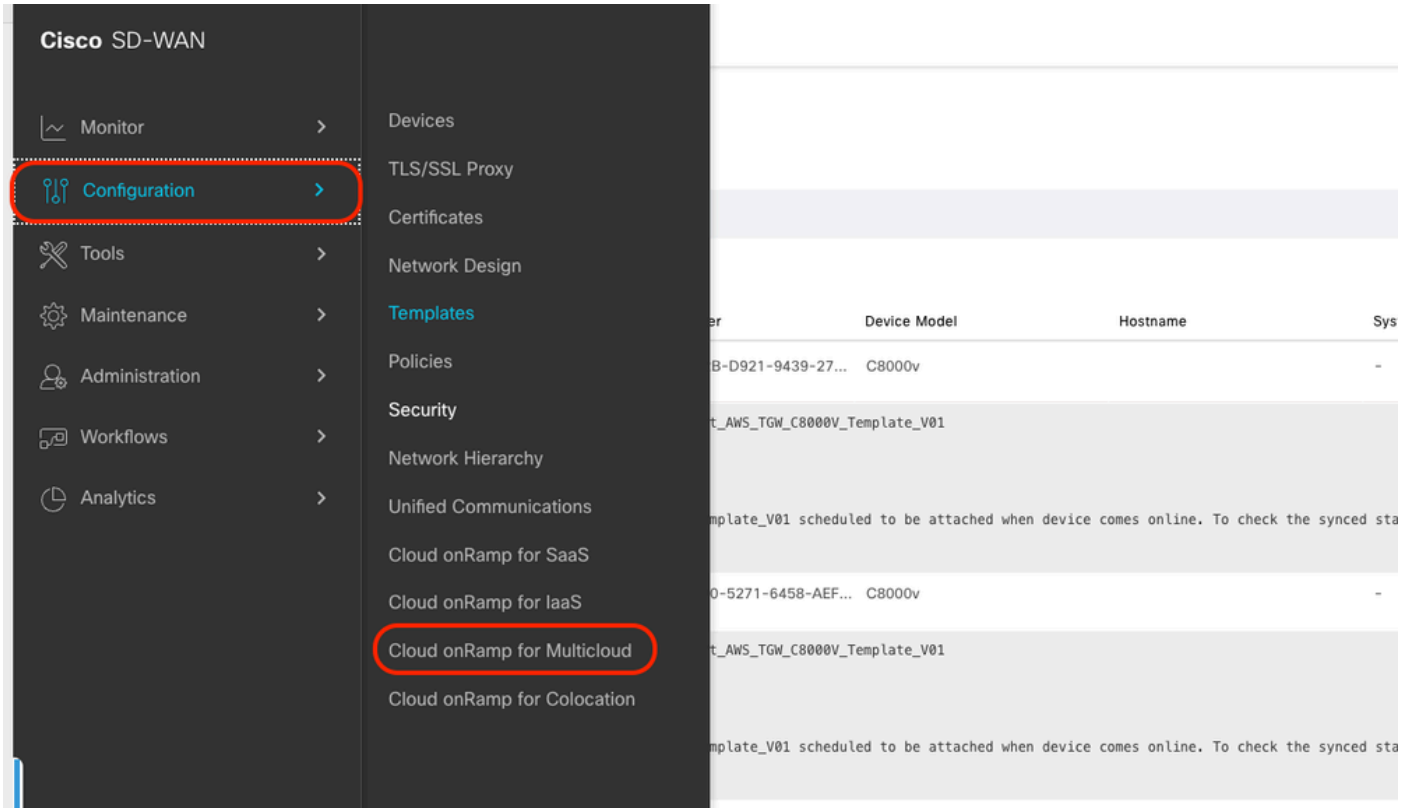
Cisco Catalyst SD-WAN Manager中的配置向导会自动将中转网关启用到您的公共云帐户，并自动建立公共云应用与重叠网络中分支机构中这些应用的用户之间的连接。此功能可与思科云路由器上的AWS虚拟私有云(VPC)配合使用。

传输网关是可用于互连VPC和内部网络的网络传输集线器。您可以将VPC或VPN连接连接到传输网关。它充当在VPC和VPN连接之间传输的流量的虚拟路由器。

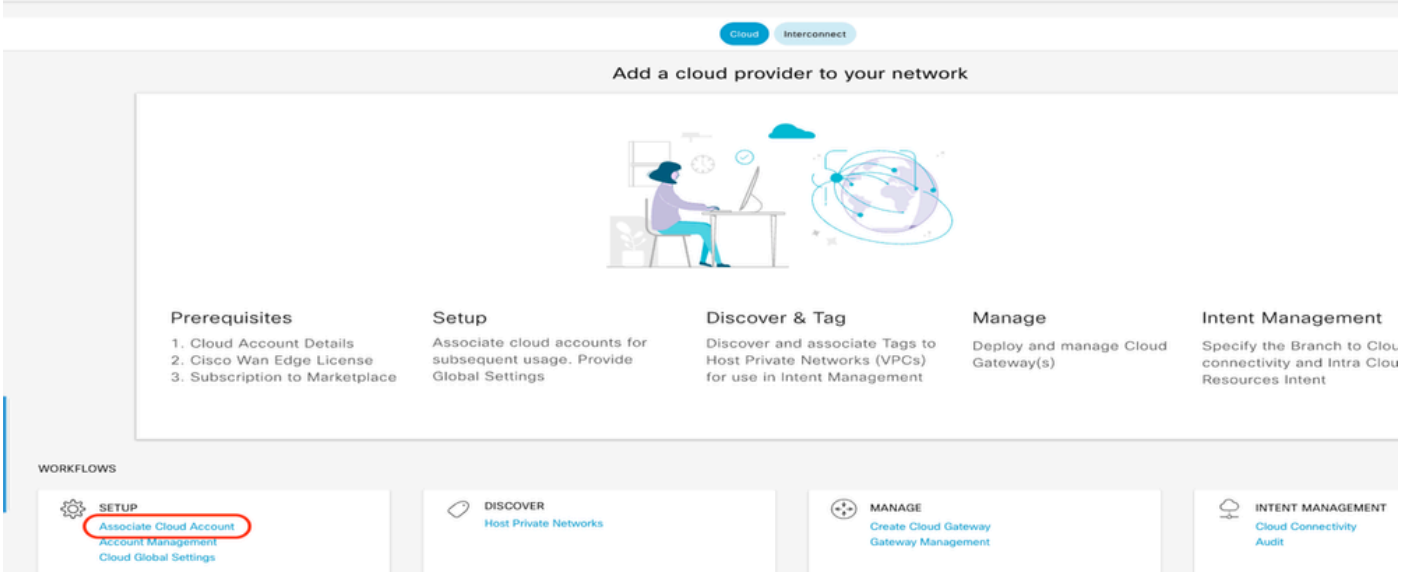
Cloud OnRamp for Multicloud支持与多个AWS帐户集成。

创建AWS云帐户

导航到配置>多云的Cloud onRamp。

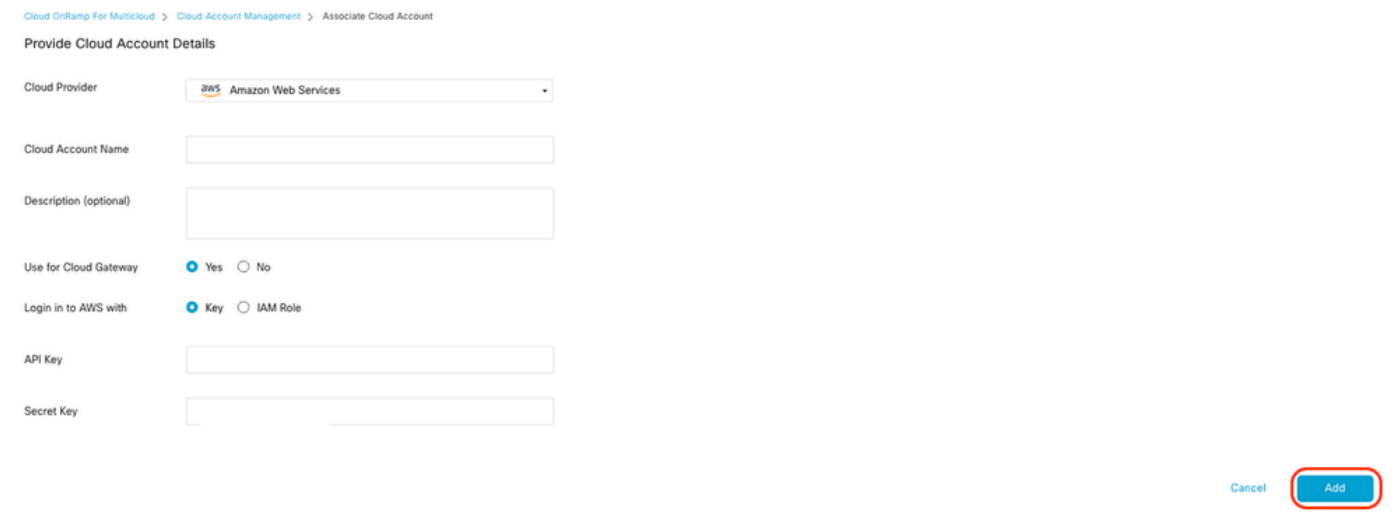


在Workflows > Setup中点击Associate Cloud Account。

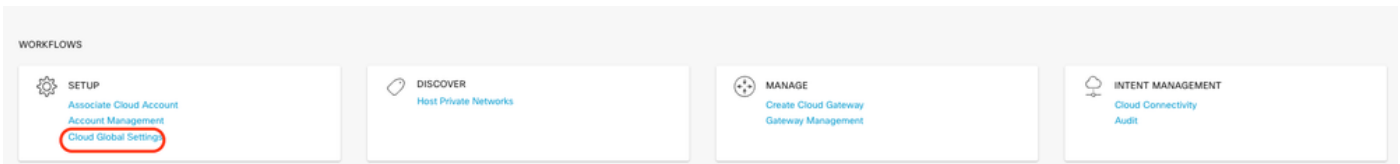


- 在“云提供商”字段中，从下拉列表中选择Amazon Web Services。
- 在云帐户名称字段中输入帐户名称。
- 选择是创建云网关。
- 在Log in AWS With字段中选择您要使用的身份验证模式。
  - 密钥
  - IAM角色

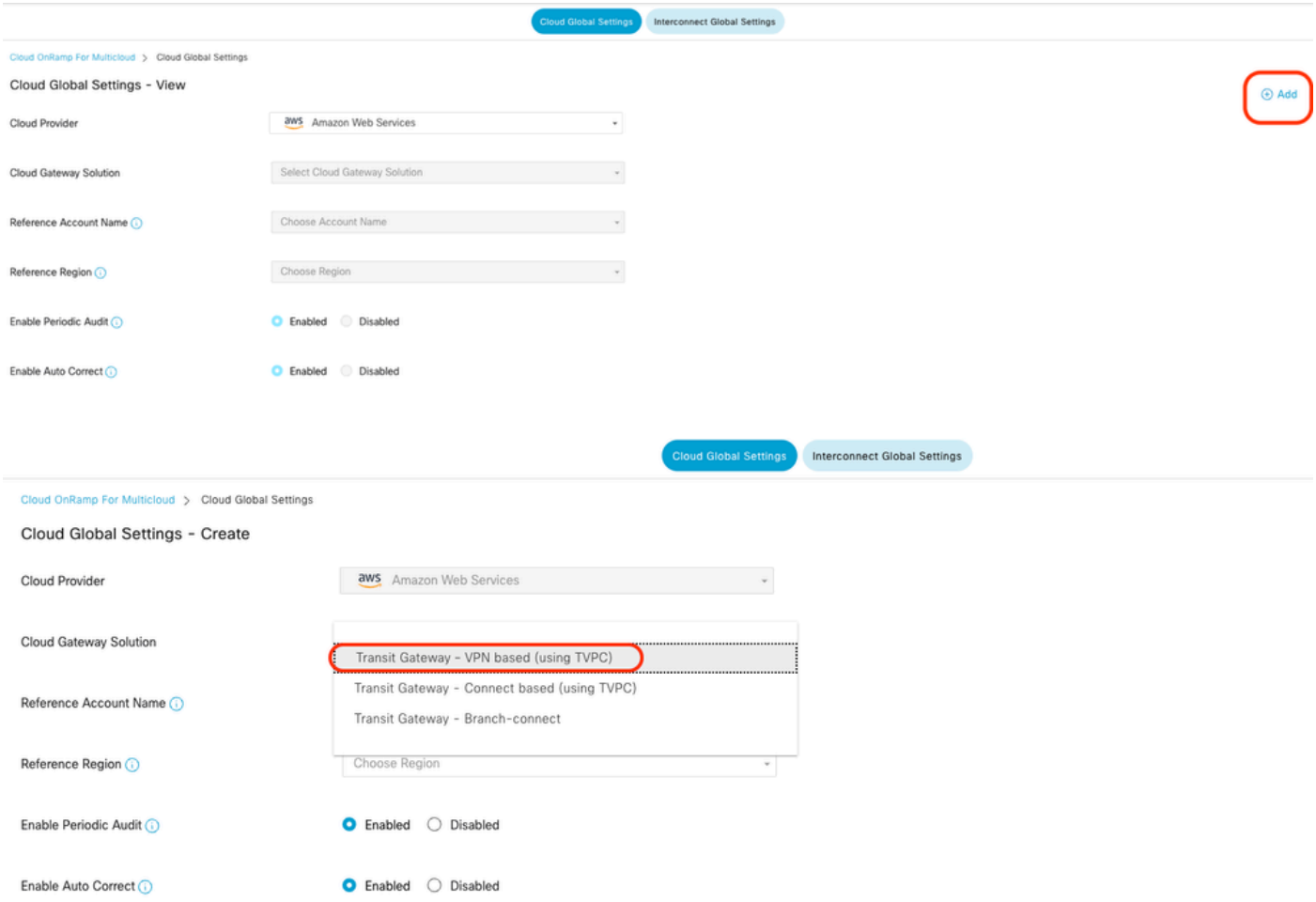
如果您选择Key model（密钥模型），则请在各自的字段中提供API Key和Secret Key。



配置云全局设置。单击Workflows > Setup > Cloud Global Settings。



点击添加，点击云网关解决方案上的下拉菜单，然后选择传输网关- VPN Base（使用TVPC）。

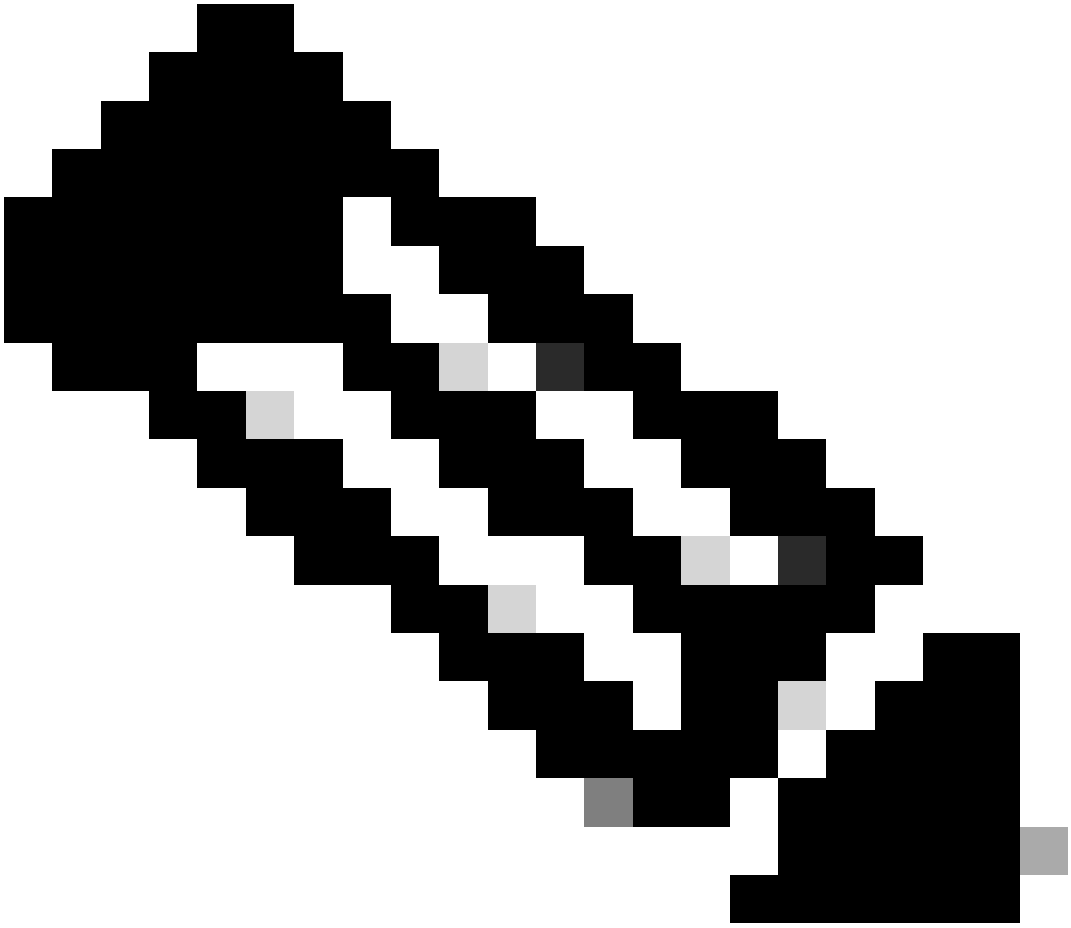


- 单击Reference Account Name下拉菜单并选择帐户。
- 单击参照区域的下拉菜单，然后从下拉菜单中选择任何区域。
- 在软件映像字段中：

  a. 点击BYOL以使用自带许可证软件映像，或者点击PAYG以使用即用即付软件映像。

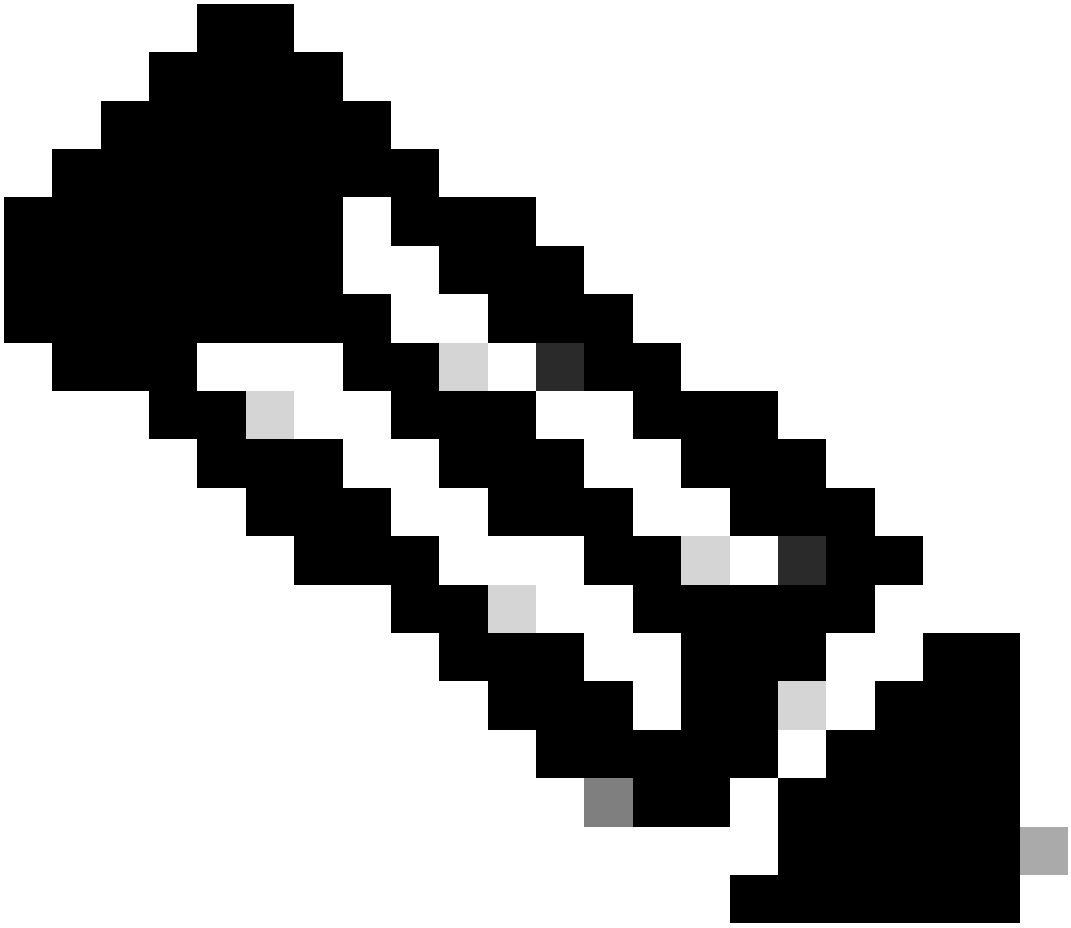
  b. 从下拉列表中选择software image。

- 点击Instance Size下拉菜单，然后为在Transit VPC中运行的实例选择大小C5n.large(2 CPU)。
- 输入IP subnet pool x.x.x.x/24。



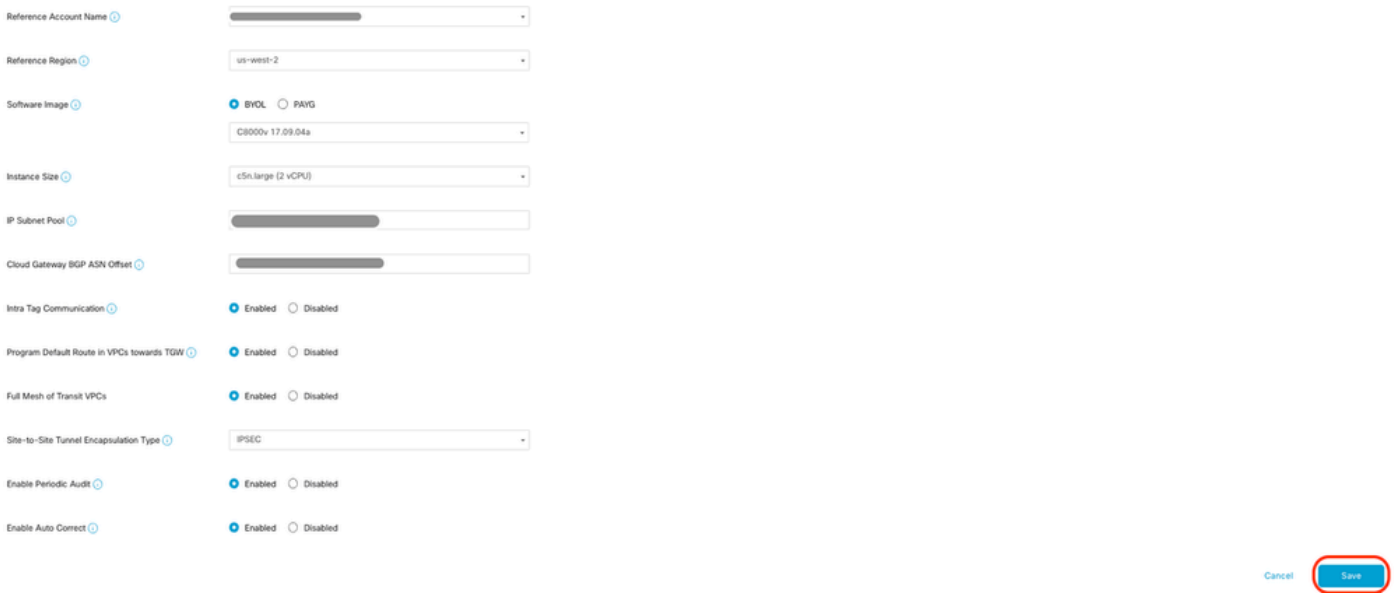
注意：当几个云网关已在使用池时，您无法修改池。 不允许子网重叠。

- 输入Cloud Gateway BGP ASN Offset 68520。

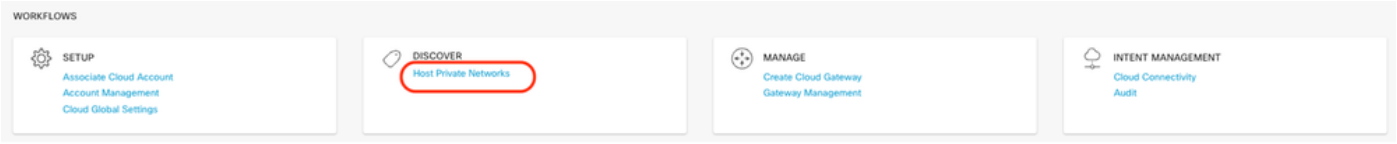


注意：可接受的起始偏移范围为64520到65500。它必须是10的倍数。

- 单击Site-to-Site Tunnel Encapsulation。 键入下拉菜单，然后选择IPSEC。
- 其余单选按钮将保留为默认值，并处于启用状态。



接下来，您需要通过返回Cloud OnRamp For Multicloud主控制面板中的Discover下单击Host Private Networks来配置主机VPC。



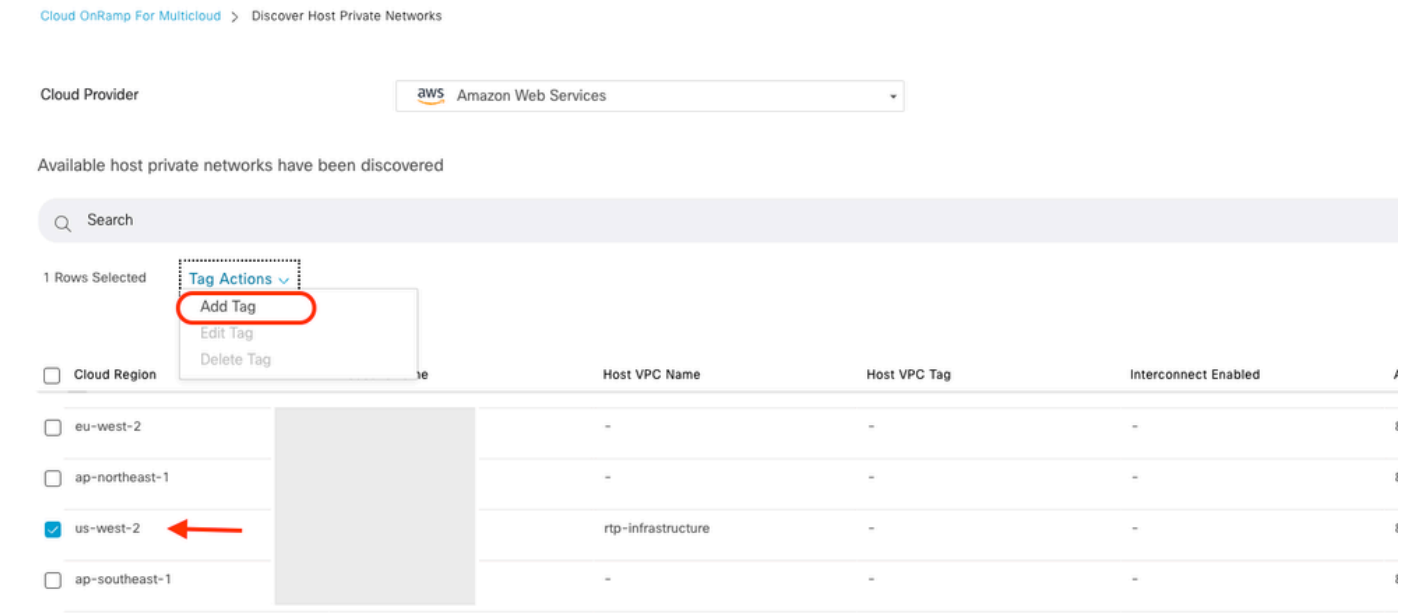
- 选择连接到传输网关的主机VPC或VPC。
- 点击区域下拉列表以根据特定区域选择VPC。
- 单击Tag操作执行以下操作：

  Add Tag -将所选VPC分组并一起进行标记。

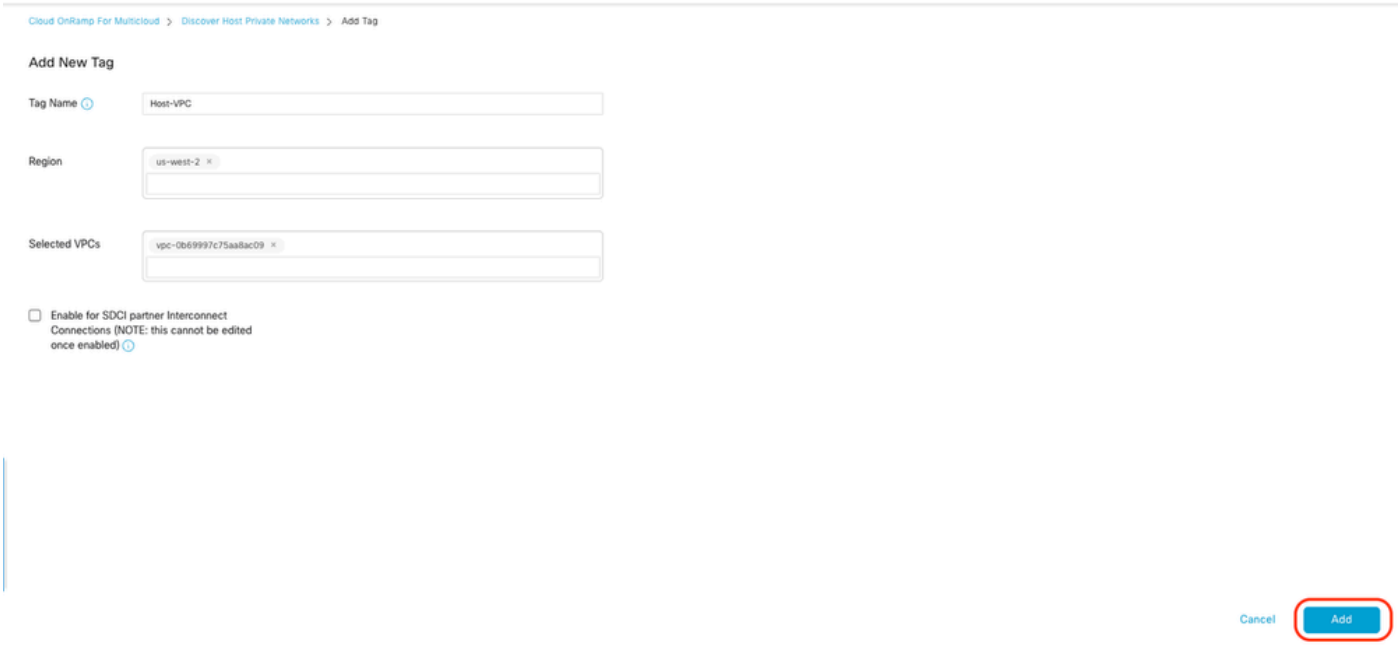
  编辑标记- 将所选VPC从一个标记迁移到另一个标记。

  Delete Tag - 删除所选VPC的标记。

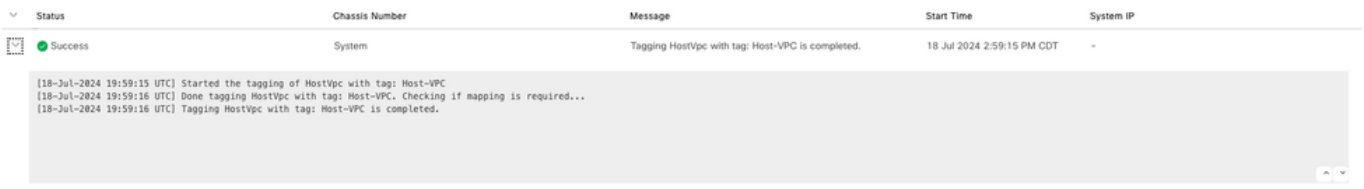
多个主机VPC可以分组到一个标记下。同一标记下的所有VPC都被视为单一单元。标记可确保连接，并且对于查看意图管理中的VPC至关重要。



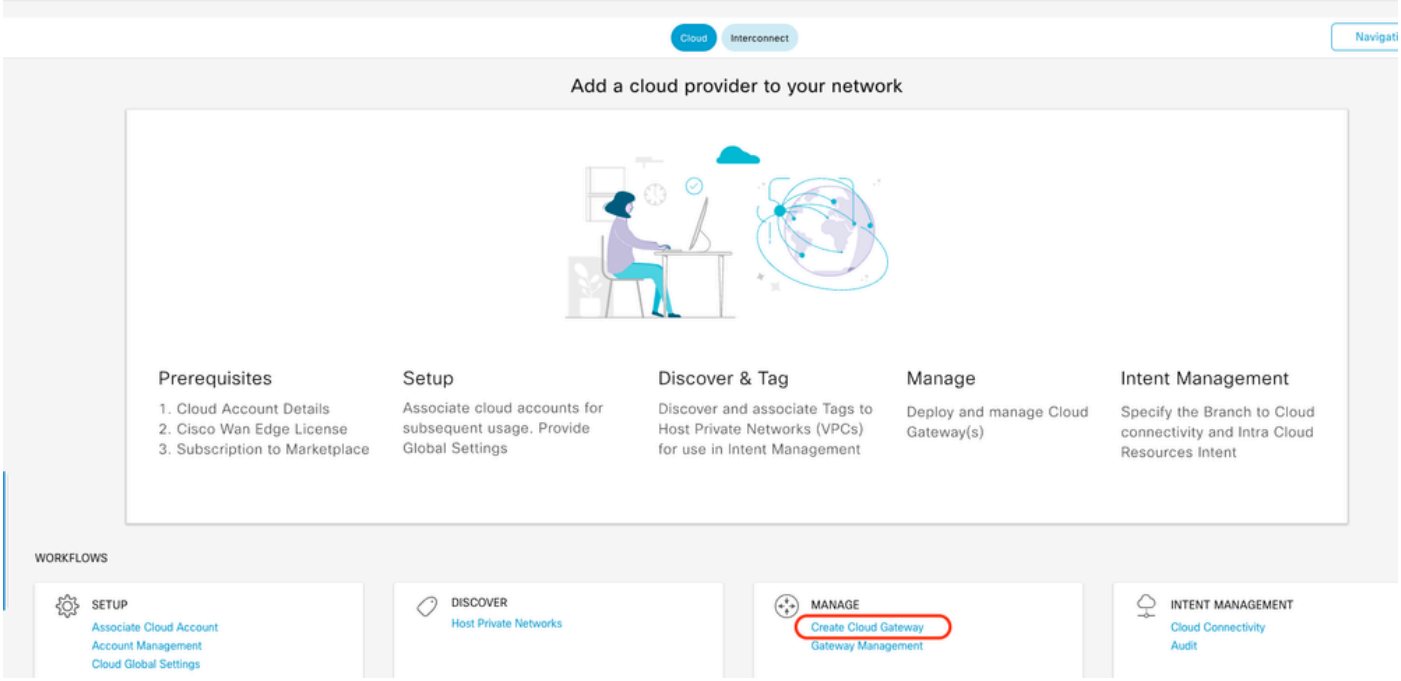
输入标记名称（标记名称可以为任何名称），然后单击添加。



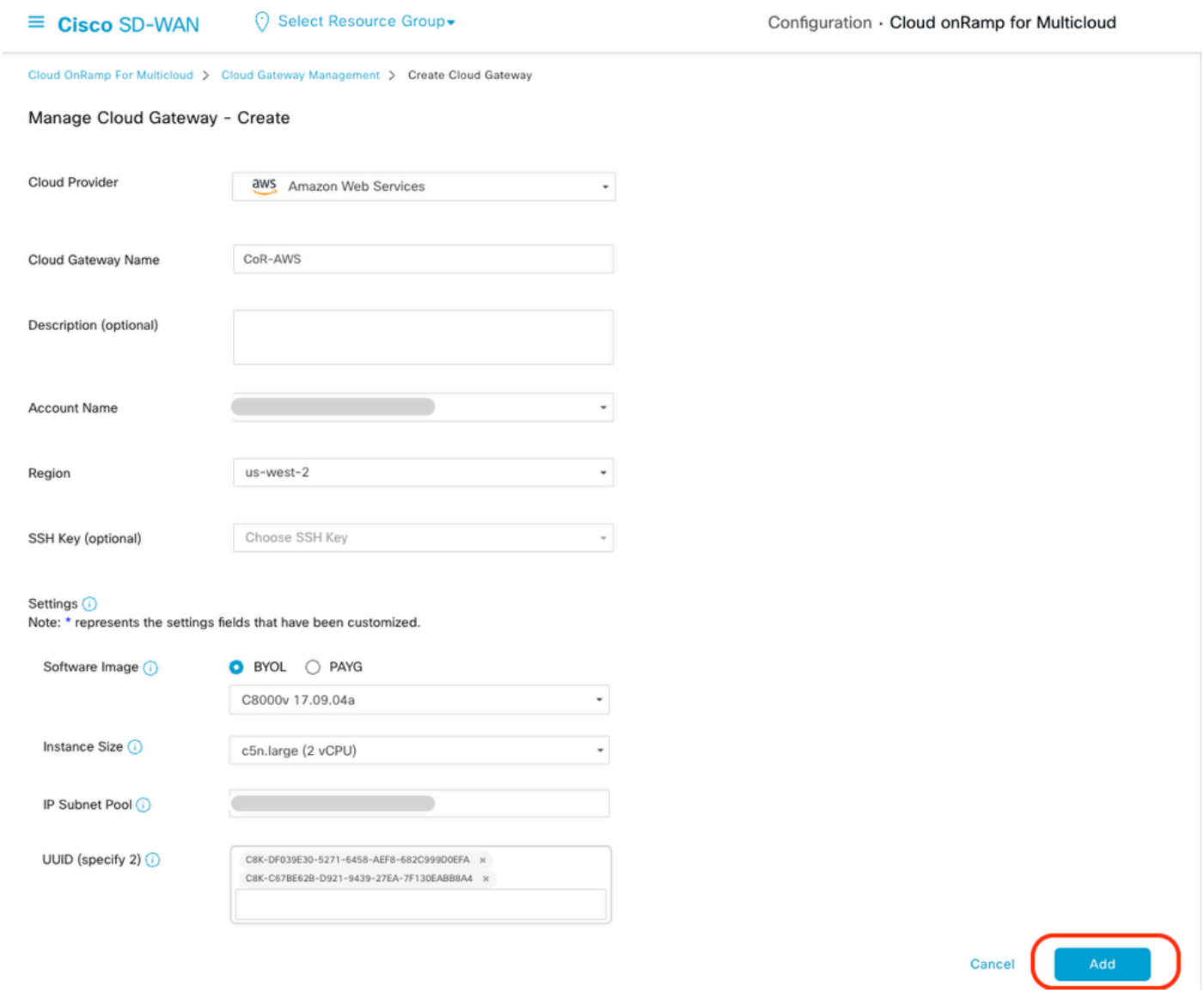
VPC标记已成功完成。



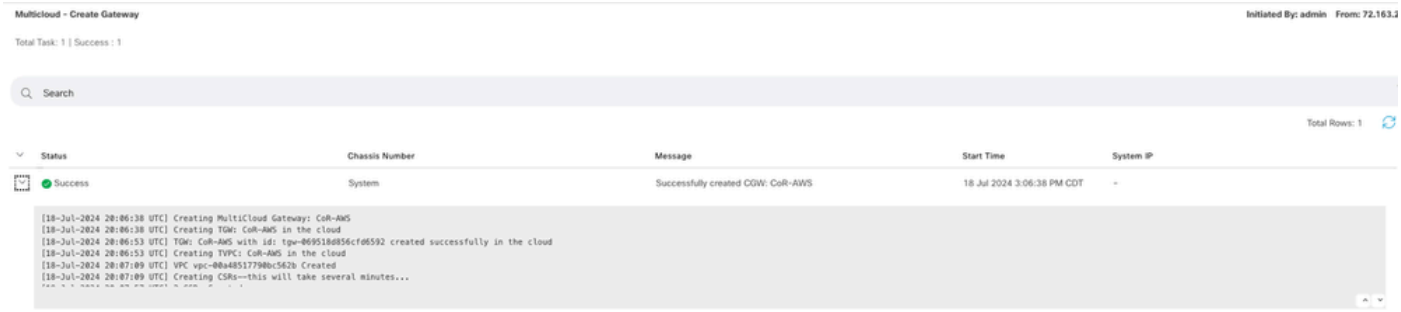
返回Cloud onRamp for Multicloud，在MANAGE下单击Create Cloud Gateway。

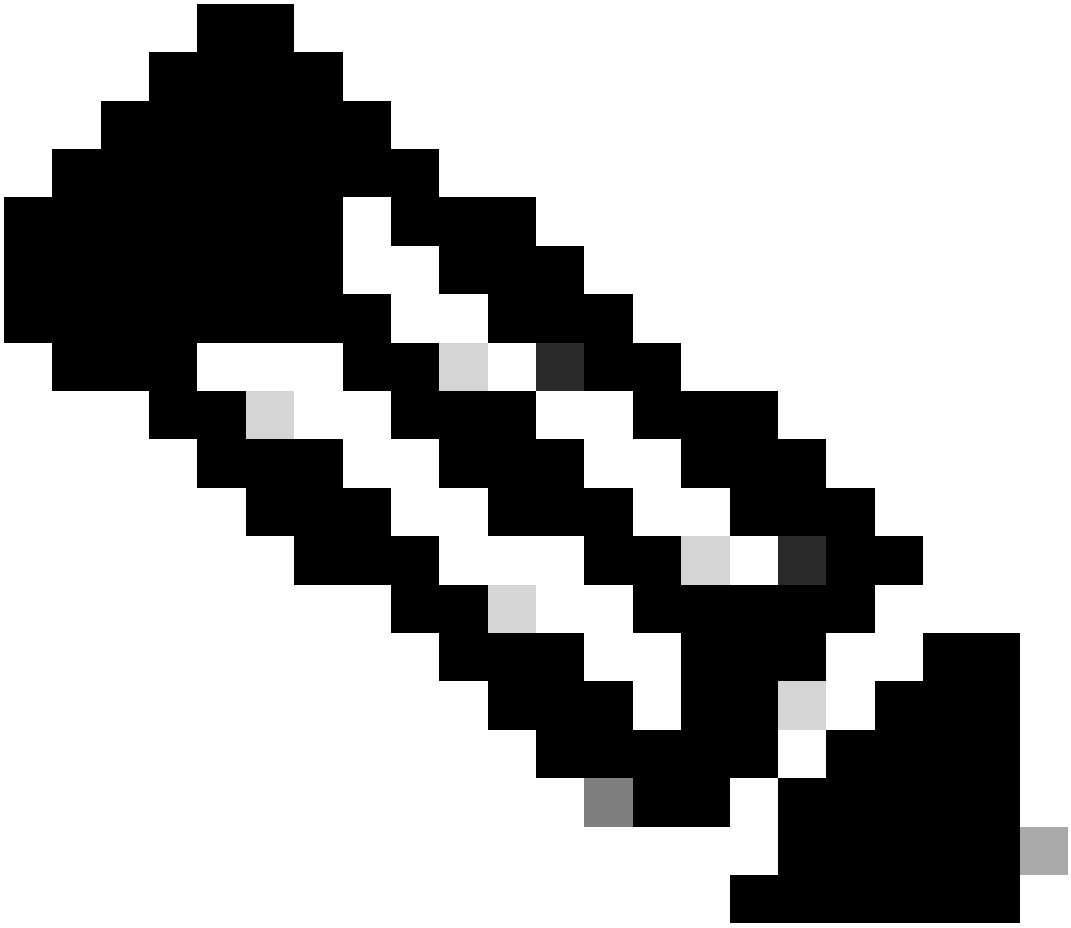


- 点击云提供商的下拉菜单，然后选择AWS。
- 输入云网关名称。
- 点击Account Name下拉菜单，其中包含之前已填写的帐户信息。
- 单击Region下拉菜单并选择对主机VPC进行标记的region。
- 软件映像、实例大小和IP子网池会从之前填满的全局云网关自动填充。
- 单击UUID下拉菜单。将显示先前在设备模板中连接的C8000v的两个UUID。选择这些选项，然后单击Add。

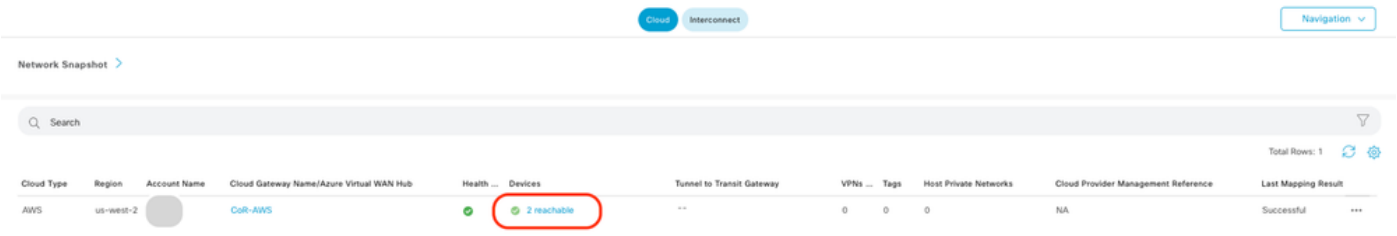


现在云网关开始创建，然后等待云网关的部署成功。

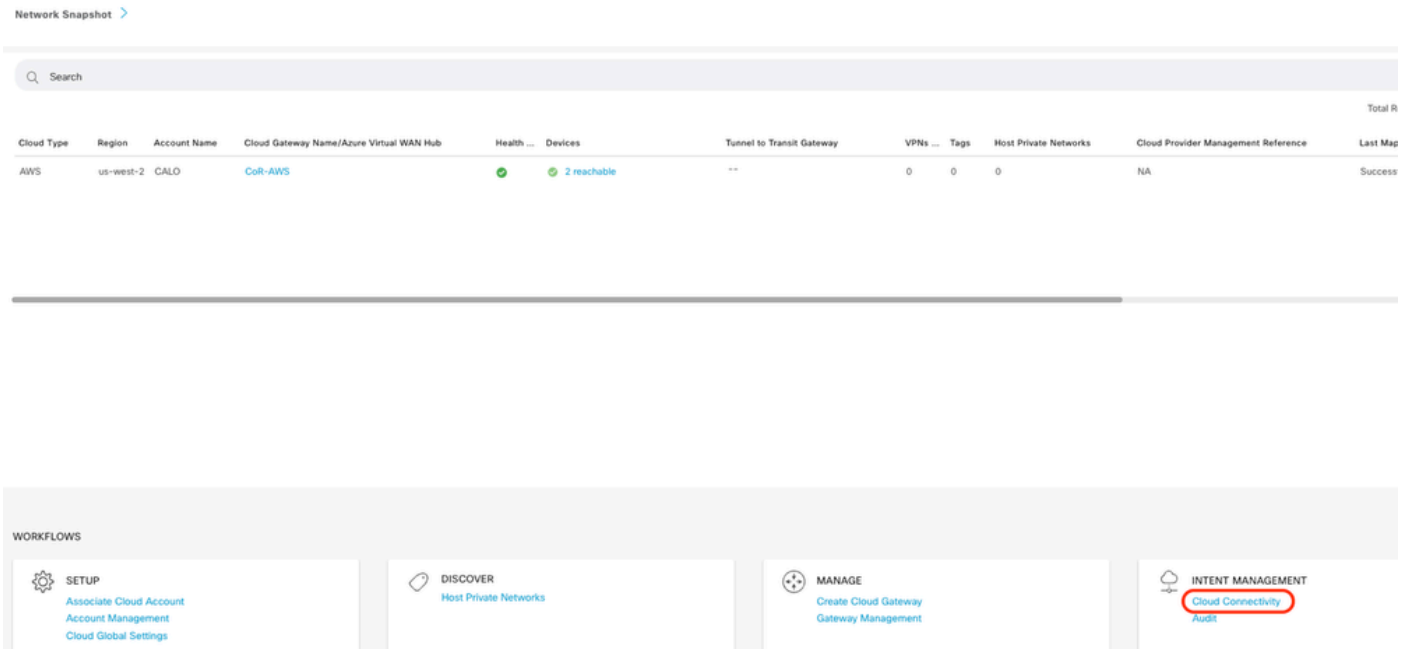




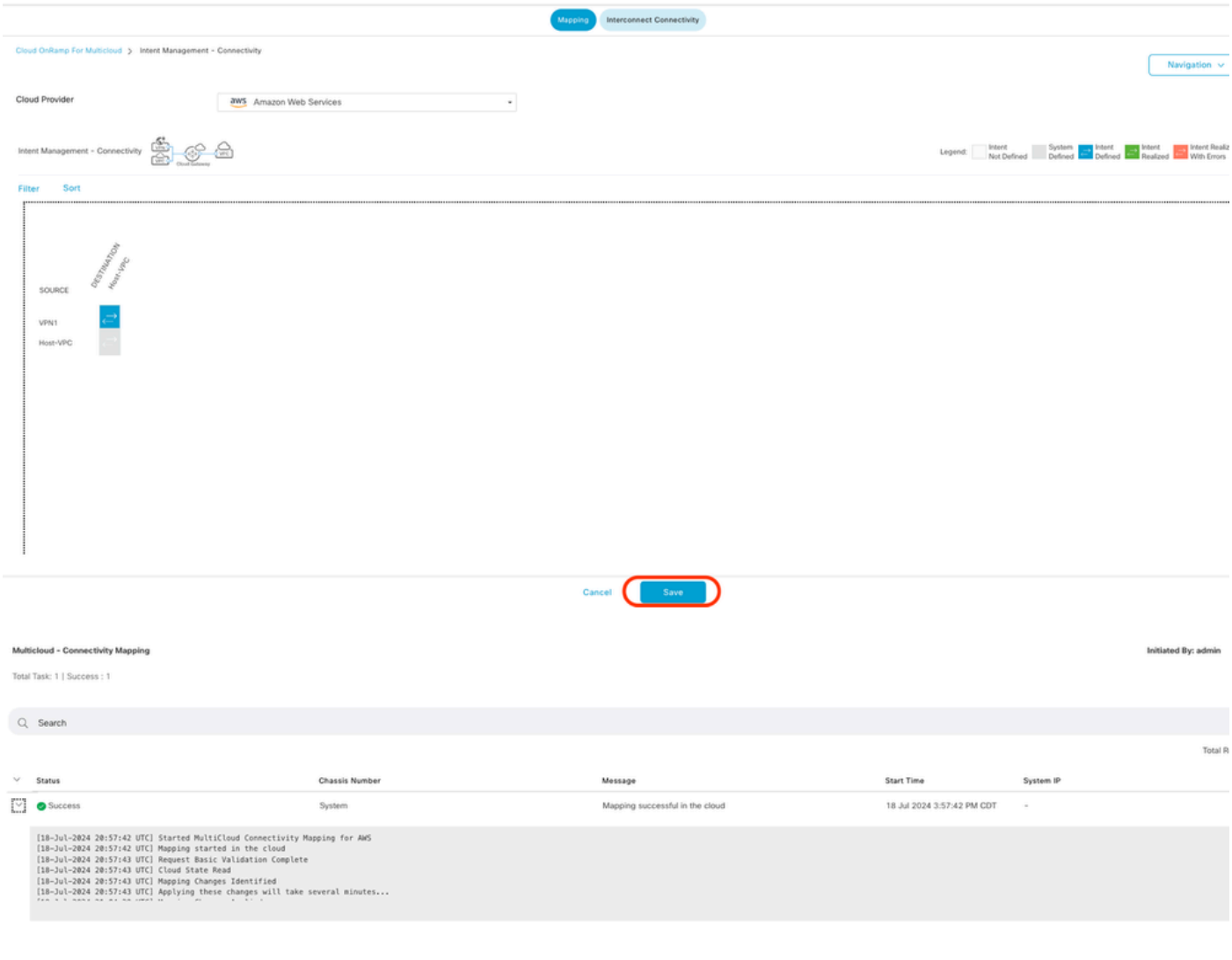
注意：完成此过程后，WAN边缘需要几分钟才能到达。



可以访问AWS中部署的两台C8000v设备。现在，单击Cloud Connectivity。

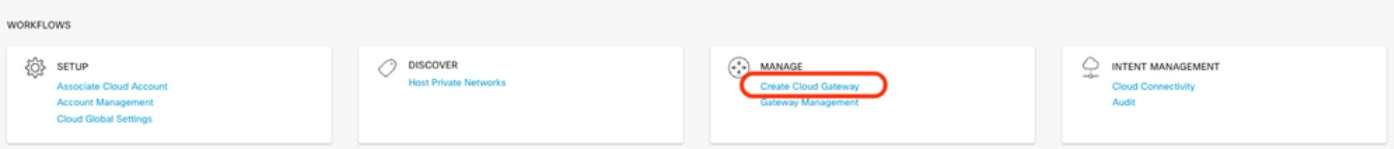


单击Edit执行VPN映射，并选择VPN 1，然后单击Save。

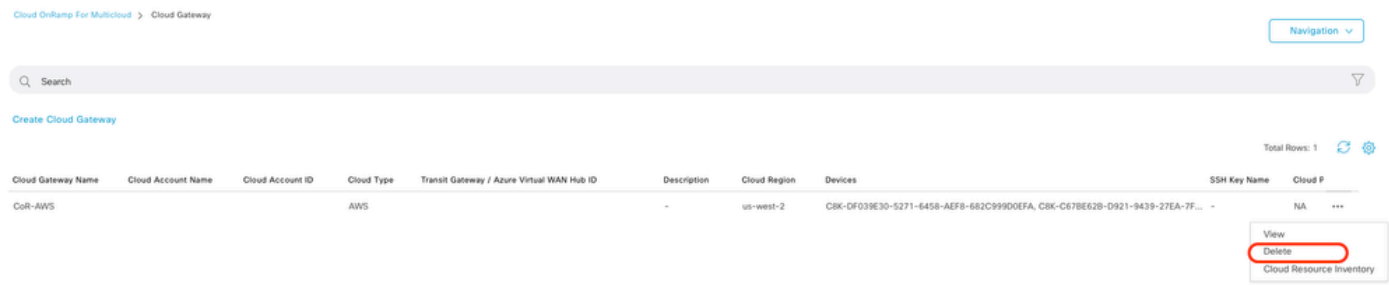


步骤3.如何删除云网关

要删除云网关，请在Manage下选择Gateway Management。



然后，点击所需云网关上的3个点(...)，然后点击删除。



验证

本节介绍用于验证的结果。

映射后，验证AWS中的两台C8000v上是否都存在VPN 1服务VPN (VRF)。

<#root>

```
C8kv1-aws#show ip vrf
  Name                              Default RD            Interfaces
 1                                   1:1                   Tu100001
                                                           Tu100002
  65528                             <not set>             Lo65528
  65529                             <not set>             Lo65529
  Mgmt-intf                         1:512                    Gi1

C8kv2-aws#show ip vrf
  Name                              Default RD            Interfaces
1                                   1:1                   Tu100001
                                                          Tu100002
  65528                             <not set>             Lo65528
  65529                             <not set>             Lo65529
  Mgmt-intf                         1:512                    Gi1
```

您还可以看到从本地分支路由器获取的OMP路由，以及从主机VPC获取的BGP路由。

```
C8kv1-aws#show ip route vrf 1
Routing Table: 1

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
m        10.1.50.64/26 [251/0] via 10.1.1.231, 02:55:52, Sdwan-system-intf
B        10.2.0.0/16 [20/100] via 169.254.0.17, 02:55:22
                     [20/100] via 169.254.0.13, 02:55:22
m        10.2.112.192/26 [251/0] via 10.1.1.221, 02:55:52, Sdwan-system-intf
m        10.2.193.0/26 [251/0] via 10.1.1.101, 02:55:52, Sdwan-system-intf
      169.254.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        169.254.0.12/30 is directly connected, Tunnel100001
L        169.254.0.14/32 is directly connected, Tunnel100001
C        169.254.0.16/30 is directly connected, Tunnel100002
L        169.254.0.18/32 is directly connected, Tunnel100002
B     172.31.0.0/16 [20/100] via 169.254.0.17, 02:55:22
                    [20/100] via 169.254.0.13, 02:55:22

C8kv2-aws#show ip route vrf 1
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
m        10.1.50.64/26 [251/0] via 10.1.1.231, 02:57:17, Sdwan-system-intf
B        10.2.0.0/16 [20/100] via 169.254.0.9, 02:57:08
                     [20/100] via 169.254.0.5, 02:57:08
m        10.2.112.192/26 [251/0] via 10.1.1.221, 02:57:17, Sdwan-system-intf
m        10.2.193.0/26 [251/0] via 10.1.1.101, 02:57:17, Sdwan-system-intf
      169.254.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        169.254.0.4/30 is directly connected, Tunnel100001
```

```
L        169.254.0.6/32 is directly connected, Tunnel100001
C        169.254.0.8/30 is directly connected, Tunnel100002
L        169.254.0.10/32 is directly connected, Tunnel100002
B     172.31.0.0/16 [20/100] via 169.254.0.9, 02:57:08
                    [20/100] via 169.254.0.5, 02:57:08
```

相关信息

SD-WAN Cloud OnRamp配置指南

技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。