

在AWS上部署C8000v高可用性配置

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[拓扑](#)

[网络图](#)

[表摘要](#)

[限制](#)

[配置](#)

[步骤1.选择区域](#)

[步骤2.创建VPC](#)

[步骤3.创建VPC的安全组](#)

[步骤4.使用策略创建IAM角色并关联到VPC](#)

[步骤5.创建信任策略并将其附加到IAM角色](#)

[步骤6.配置并启动C8000v实例](#)

[步骤6.1.配置远程访问密钥对](#)

[步骤6.2.创建并配置AMI的子网](#)

[步骤6.3.配置AMI接口](#)

[步骤6.4.将IAM实例配置文件设置为AMI](#)

[第6.5步 \(可选 \) 在AMI上设置凭证](#)

[步骤6.6.完成实例配置](#)

[步骤6.7.禁用ENI上的源/目标检查](#)

[步骤6.8.创建弹性IP并将其关联到实例的公共ENI](#)

[步骤7.重复步骤6，创建高可用性第二个C8000v实例](#)

[步骤8.重复步骤6，从AMI市场创建VM\(Linux/Windows\)](#)

[步骤9.创建并配置VPC的Internet网关\(IGW\)](#)

[步骤10.在AWS上创建并配置公共子网和专用子网的路由表](#)

[步骤10.1.创建并配置公共路由表](#)

[步骤10.2.创建并配置专用路由表](#)

[步骤11.检查并配置基本网络配置、网络地址转换\(NAT\)、具有BFD的GRE隧道和路由协议](#)

[步骤12.配置高可用性\(Cisco IOS@ XE Denali 16.3.1a或更高版本\)](#)

[确认](#)

[故障排除](#)

简介

本文档介绍如何在Amazon Web Services云上使用Catalyst 8000v路由器设置高可用性环境。

先决条件

要求

思科建议您事先了解以下主题：

- AWS控制台及其组件的一般知识
- 了解Cisco IOS® XE软件
- HA功能基础知识。

使用的组件

此配置示例需要以下组件：

- 具有管理员角色的Amazon AWS帐户
- 运行Cisco IOS® XE 17.15.3a和1 Ubuntu 22.04 LTS虚拟机的两台C8000v设备 同一区域中的AMI

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。

拓扑

根据网络要求有多种高可用性部署方案。在本示例中，HA冗余使用以下设置进行配置：

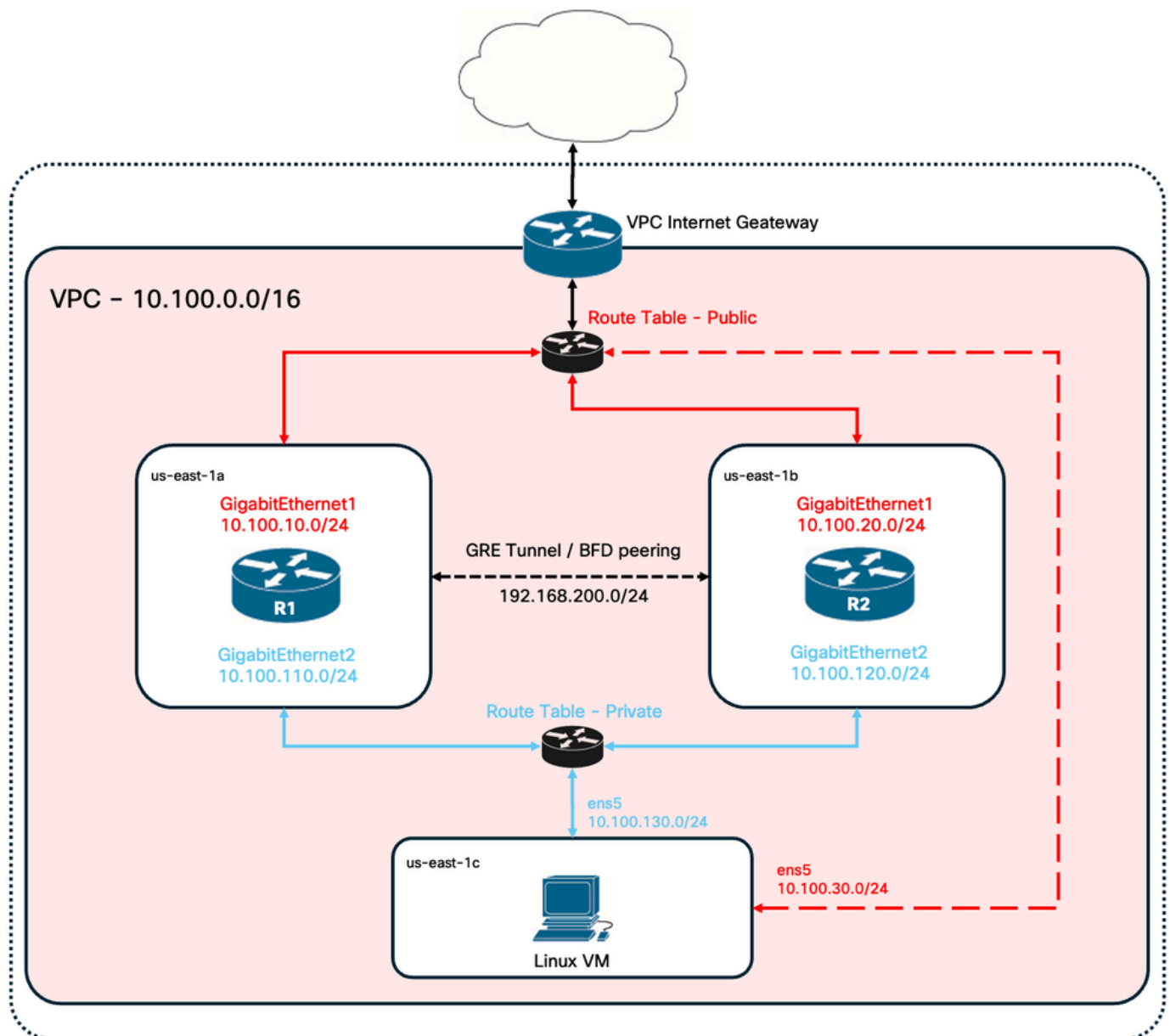
- 1x — 区域
- 1个 — VPC
- 3倍 — 可用区
- 6x — 网络接口/子网（3x面向公共/3x面向专用）
- 2x — 路由表（公共路由表和私有路由表）
- 2x - C8000v路由器(Cisco IOS® XEDenali 17.15.3a)
- 1x — 虚拟机(Linux/Windows)

一个HA对中有2台C8000v路由器，位于两个不同的可用区域中。将每个可用性区域视为独立的数据中心，以提供额外的硬件恢复能力。

第三个区域是模拟专用数据中心中的设备的VM。目前，通过公共接口启用互联网访问，以便您可以访问和配置VM。通常，所有正常流量必须通过专用路由表。

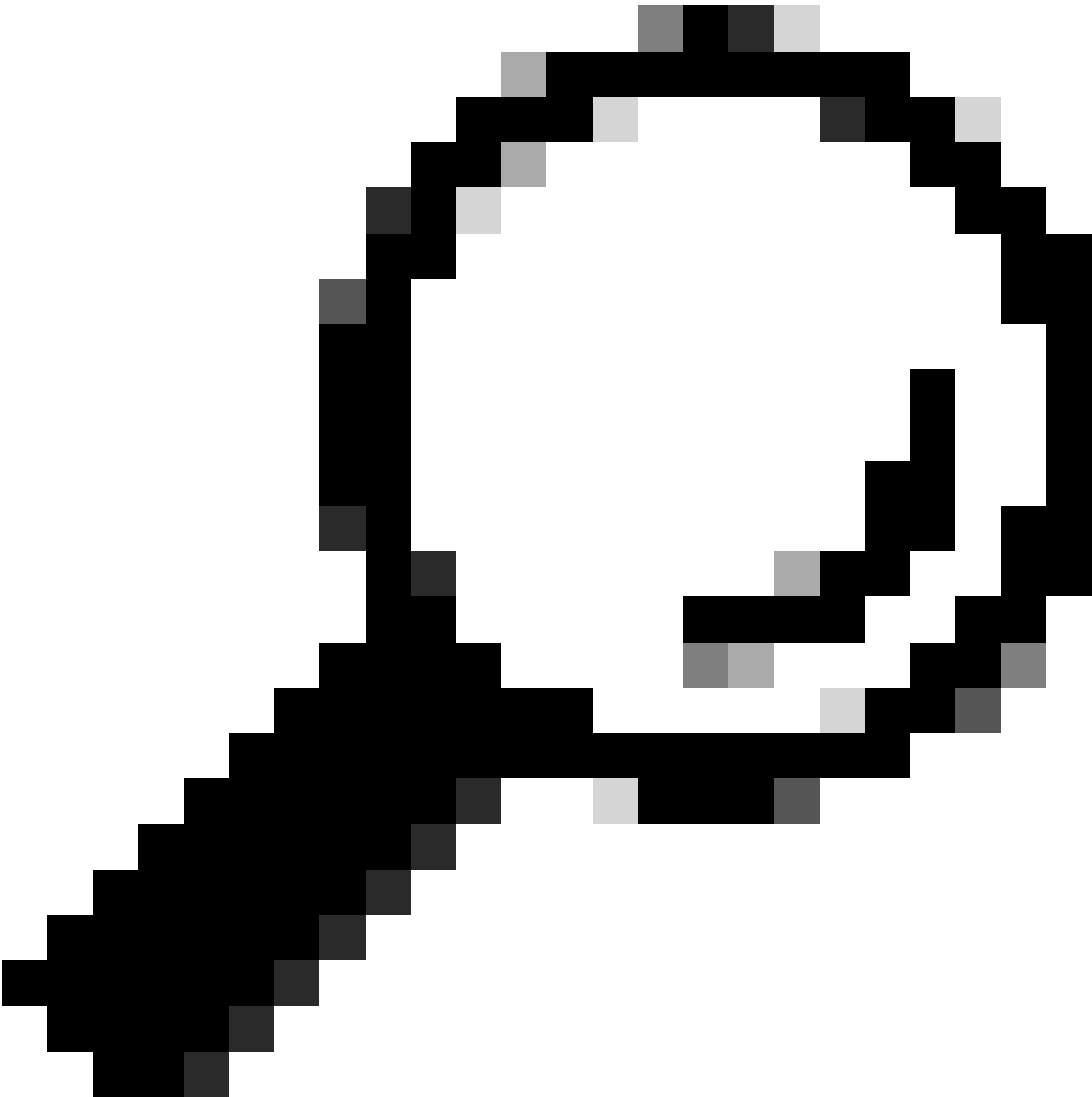
要模拟流量，请从虚拟机的专用接口发起ping，通过R1遍历专用路由表以到达8.8.8.8。发生故障转移时，请验证专用路由表是否已自动更新，以通过R2路由器的专用接口路由流量。

网络图



表摘要

总结拓扑时，请看下表，其中包含实验中每个组件的最重要值。本表中提供的信息仅用于本实验。



提示：使用此表有助于在整个指南中清晰地概述关键变量。建议收集此格式的信息以简化流程。

设备	可用区	接口	IP 地址	RTB	埃尼
R1	us-east-1a	GigabitEthernet1	10.100.10.254	rtb-0d0e48f25c9b00635 (公共)	eni-0645a881c13823696
		GigabitEthernet2	10.100.110.254	rtb-093df10a4de426eb8 (专用)	eni-070e14fbfde0d8e3b
R2	us-east-1b	GigabitEthernet1	10.100.20.254	rtb-0d0e48f25c9b00635 (公共)	eni-0a7817922ffbb317b

		GigabitEthernet2	10.100.120.254	rtb-093df10a4de426eb8 (专用)	eni-0239fda341b4d7e41
Linux虚拟机	us-east-1c	ENS5	10.100.30.254	rtb-0d0e48f25c9b00635 (公共)	eni-0b28560781b3435b1
		ENS6	10.100.130.254	rtb-093df10a4de426eb8 (专用)	eni-05d025e88b6355808

限制

- 在创建的任何子网上，请勿使用该子网的第一个可用地址。这些IP地址由AWS服务在内部使用。
- 请勿在VRF中配置C8000v设备的公共接口。 如果设置了此项，则HA无法正常工作。

配置

一般配置流程侧重于在适当的区域创建所请求的虚拟机，然后向下移动到最具体的配置，例如每个虚拟机的路由和接口。但是，建议先了解拓扑，然后按所需的任意顺序进行配置。

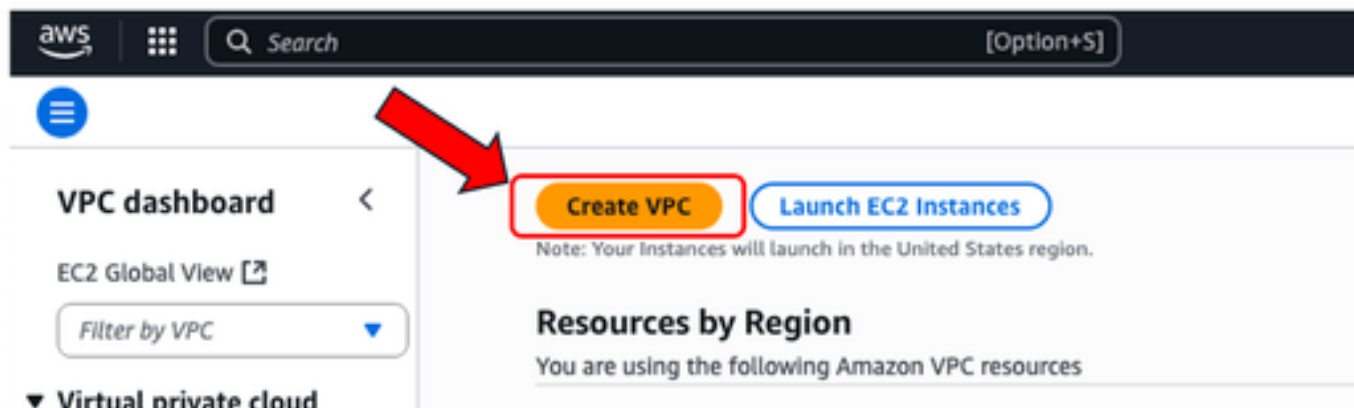
步骤1.选择区域

在本部署指南中，美国西部（北弗吉尼亚） — 美国东部-1区域被选为VPC区域。



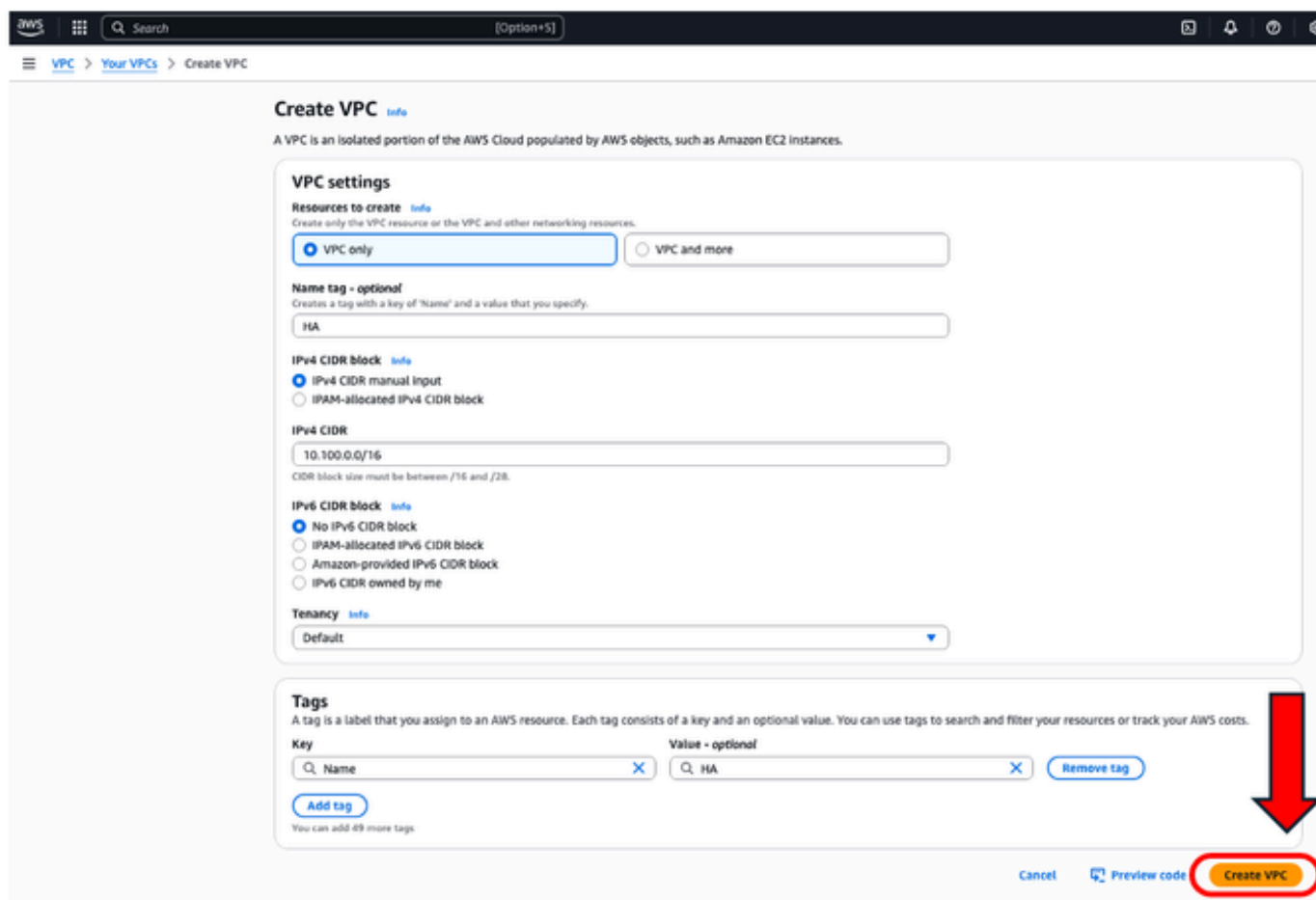
步骤2.创建VPC

在AWS控制台上，导航到VPC > VPC Dashboard > Create VPC。

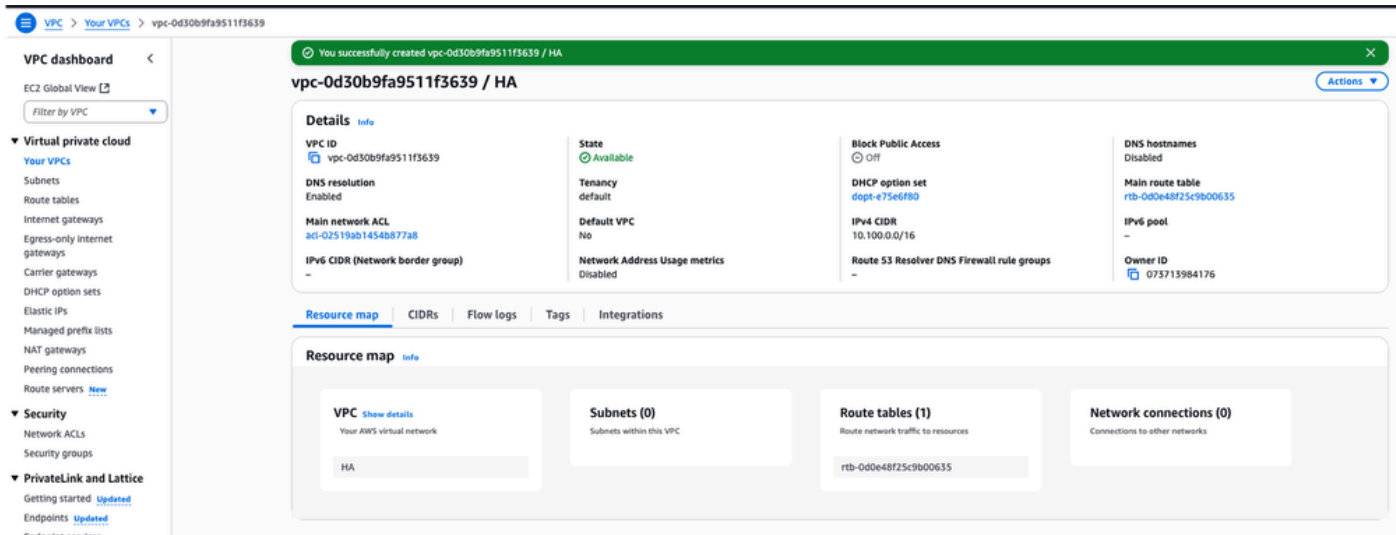


创建VPC时，请选择仅VPC选项。您可以根据需要分配要使用的/16网络。

在本部署指南中，选择10.100.0.0/16网络：

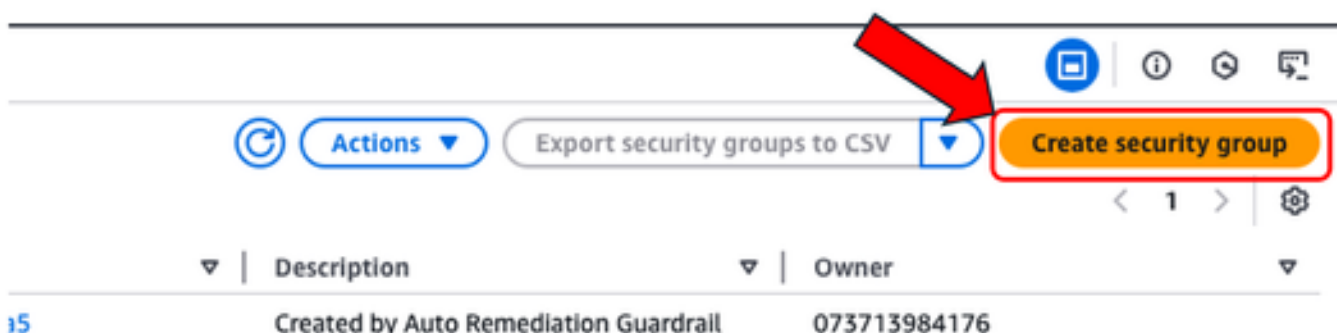


单击创建VPC后，现在创建了带HA标记的VPC-0d30b9fa9511f3639:



步骤3.创建VPC的安全组

在AWS中，安全组与ACL类似，允许或拒绝流量流向VPC中配置的VM。在AWS控制台上，导航到VPC > VPC Dashboard > Security > Security Groups部分，然后点击Create security group。



在Inbound Rules下，定义要允许的流量。在本示例中，All Traffic通过使用0.0.0.0/0网络进行选择。

☰ VPC > Security Groups > Create security group

Create security group info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name info

Name cannot be edited after creation.

Description info

VPC info

vpc-0d30b9fa9511f3639 (HA) ▾

Inbound rules

Type	Protocol	Port range	Source	Description - optional	
All traffic ▾	All	All	Anywh... ▾		Delete
0.0.0.0/0 X					
Add rule					

Outbound rules

Type	Protocol	Port range	Destination	Description - optional	
All traffic ▾	All	All	Custom ▾		Delete
0.0.0.0/0 X					
Add rule					

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)

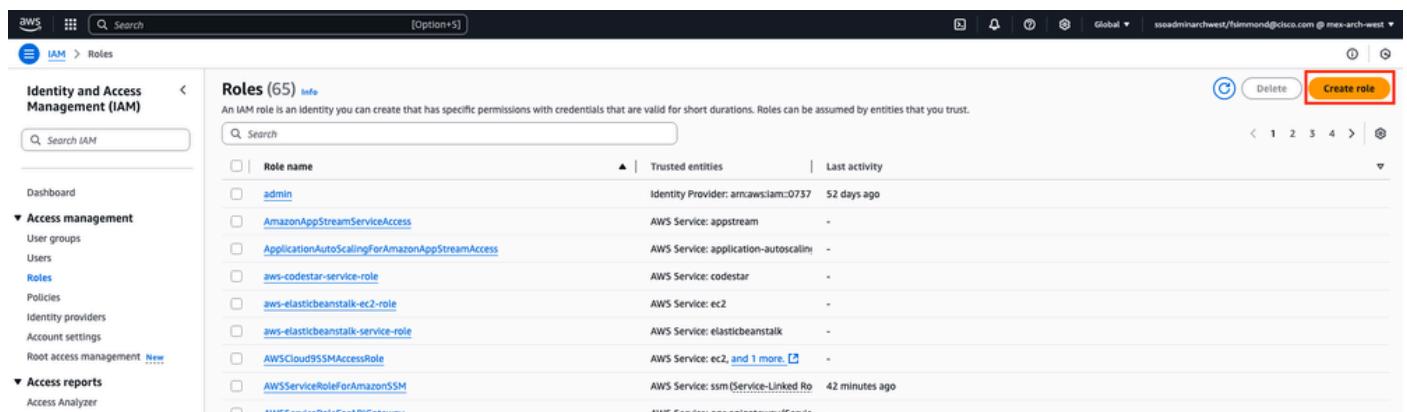
You can add up to 50 more tags.

[Cancel](#) [Create security group](#)

步骤4.使用策略创建IAM角色并关联到VPC

IAM授予您的AMI访问Amazon API所需的权限。C8000v用作代理，以调用AWS API命令来修改AWS中的路由表。默认情况下，EC2实例不允许访问API。因此，必须创建新的IAM角色，该角色将在AMI创建期间应用。

浏览到IAM控制面板，然后导航到访问管理>角色>创建角色。此过程包括3个步骤：



首先，选择Trusted entity type部分上的AWS Service选项，然后选择EC2作为为此策略分配的服务。

。

- Step 1
● **Select trusted entity**
- Step 2
○ Add permissions
- Step 3
○ Name, review, and create

Select trusted entity Info

Trusted entity type

☒ **AWS service**

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**

Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

☒ **EC2**

Allows EC2 instances to call AWS services on your behalf.

☐ **EC2 Role for AWS Systems Manager**

Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

☐ **EC2 Spot Fleet Role**

Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

☐ **EC2 - Spot Fleet Auto Scaling**

Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

☐ **EC2 - Spot Fleet Tagging**

Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

☐ **EC2 - Spot Instances**

Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

☐ **EC2 - Spot Fleet**

Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

☐ **EC2 - Scheduled Instances**

Allows EC2 Scheduled Instances to manage instances on your behalf.

Cancel

Next

完成后，单击Next:

IAM > Roles > Create role

Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Name, review, and create

Add permissions

Info

Permissions policies (1062) [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type

All types

< 1 2 3 4 5 6 7 ... 54 >

☐	Policy name ?	Type	Description
☐	AdministratorAccess	AWS managed - job function	Provides full access to AWS services an...
☐	AdministratorAccess-Amplify	AWS managed	Grants account administrative permis...
☐	AdministratorAccess-AWSElasticBeanstalk	AWS managed	Grants account administrative permis...
☐	AIOpsAssistantPolicy	AWS managed	Provides ReadOnly permissions requir...
☐	AIOpsConsoleAdminPolicy	AWS managed	Grants full access to Amazon AI Opera...
☐	AIOpsOperatorAccess	AWS managed	Grants access to the Amazon AI Opera...
☐	AIOpsReadOnlyAccess	AWS managed	Grants ReadOnly permissions to the A...
☐	AlexaForBusinessDeviceSetup	AWS managed	Provide device setup access to AlexaFo...
☐	AlexaForBusinessFullAccess	AWS managed	Grants full access to AlexaForBusiness ...
☐	AlexaForBusinessGatewayExecution	AWS managed	Provide gateway execution access to A...
☐	AlexaForBusinessLifesizeDelegatedAccessP...	AWS managed	Provide access to Lifesize AVS devices
☐	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	Provide access to Poly AVS devices
☐	AlexaForBusinessReadOnlyAccess	AWS managed	Provide read only access to AlexaForB...
☐	AmazonAPIGatewayAdministrator	AWS managed	Provides full access to create/edit/dele...
☐	AmazonAPIGatewayInvokeFullAccess	AWS managed	Provides full access to invoke APIs in A...
☐	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	Allows API Gateway to push logs to us...
☐	AmazonAppFlowFullAccess	AWS managed	Provides full access to Amazon AppFlo...
☐	AmazonAppFlowReadOnlyAccess	AWS managed	Provides read only access to Amazon A...
☐	AmazonAppStreamFullAccess	AWS managed	Provides full access to Amazon AppStr...
☐	AmazonAppStreamPCAAccess	AWS managed	Amazon AppStream 2.0 access to AWS...

► Set permissions boundary - optional

Cancel

Previous

Next

最后，设置Role Name并单击Create Role按钮。

IAM > Roles > Create role

Step 1 Select trusted entity
Step 2 Add permissions
Step 3 Name, review, and create

Name, review, and create

Role details
Role name
Enter a meaningful name to identify this role.
route-table-change
Maximum 64 characters. Use alphanumeric and "+,=,@,_" characters.
Description
Add a short explanation for this role.
Allows EC2 instances to make changes on the route table
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, @-^![]{}#%*~'":;.,-~

Step 1: Select trusted entities [Edit](#)

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "sts:AssumeRole"  
8       ],  
9       "Principal": {  
10        "Service": [  
11          "ec2.amazonaws.com"  
12        ]  
13      }  
14    }  
15  ]  
16 }
```

Step 2: Add permissions [Edit](#)

Permissions policy summary

Policy name	Type	Attached as
-------------	------	-------------

Step 3: Add tags

Add tags - optional [Info](#)
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
No tags associated with the resource.
[Add new tag](#)
You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create role](#)

步骤5.创建信任策略并将其附加到IAM角色

创建角色后，必须制定信任策略，以便在需要时获取修改AWS路由表的技能。转到IAM控制面板上的Policies部分。单击Create Policy按钮。此过程包括两个步骤：

IAM > Policies

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**
- Identity providers
- Account settings
- Root access management [New](#)

Access reports

- Access Analyzer

Policies (1367) [Info](#)

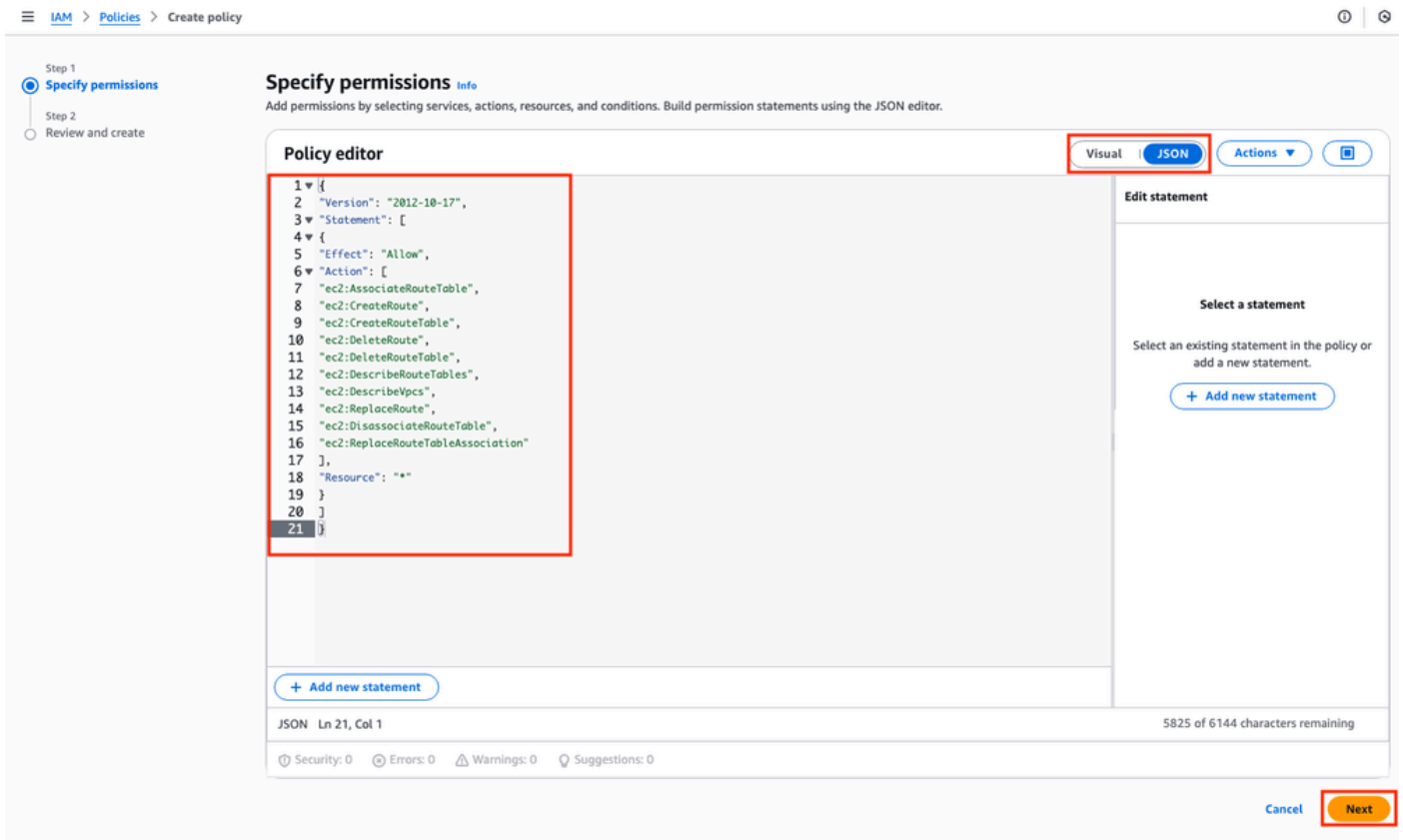
A policy is an object in AWS that defines permissions.

Filter by Type
Search All types

< 1 2 3 4 5 6 7 ... 69 > [Settings](#)

	Policy name	Type	Used as
☐	AccessAnalyzerServiceRolePolicy	AWS managed	None
☐	AdministratorAccess	AWS managed - job function	Permissions poli
☐	AdministratorAccess-Amplify	AWS managed	None
☐	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None
☐	AIOpsAssistantPolicy	AWS managed	None
☐	AIOpsConsoleAdminPolicy	AWS managed	None
☐	AIOpsOperatorAccess	AWS managed	None
☐	AIOpsReadOnlyAccess	AWS managed	None

首先，确保Policy Editor使用JSON并应用如下所示的命令。配置后，单击Next:



以下是图像中使用的文本代码：

```
{  
"Version": "2012-10-17",  
"Statement": [  
{  
"Effect": "Allow",  
"Action": [  
"ec2:AssociateRouteTable",  
"ec2:CreateRoute",  
"ec2:CreateRouteTable",  
"ec2>DeleteRoute",  
"ec2>DeleteRouteTable",  
"ec2:DescribeRouteTables",  
"ec2:DescribeVpcs",  
"ec2:ReplaceRoute",  
"ec2:DisassociateRouteTable",  
"ec2:ReplaceRouteTableAssociation"  
],  
"Resource": "*"   
},  
]  
}
```

稍后，设置Policy Name并单击Create Policy。

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.
C8000v-HA
Maximum 128 characters. Use alphanumeric and '+', '@', '-', '_' characters.

Description - optional
Add a short explanation for this policy.
Allows EC2 instances to make route changes on AWS
Maximum 1,000 characters. Use alphanumeric and '+', '@', '-', '_' characters.

Permissions defined in this policy

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (1 of 441 services) Show remaining 440 services

Service	Access level	Resource	Request condition
EC2	Limited: List, Write	All resources	None

Add tags - optional

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
No tags associated with the resource.

Add new tag
You can add up to 50 more tags.

Cancel Previous **Create policy**

创建策略后，过滤并选择策略，然后单击操作下拉菜单上的附加选项。

IAM > Policies

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**

Policies (1/1368)

A policy is an object in AWS that defines permissions.

Filter by Type
All types 1 match

Search C800

Policy name	Type	Used as	Description
C8000v-HA	Customer managed	None	Allows EC2 instances to make route ch...

Actions Attach Detach

新窗口已打开。在IAM Entities部分，过滤并选择创建的IAM角色，然后点击Attach policy。

IAM > Policies > C8000v-HA > Attach policy

Attach as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

IAM Entities (1/69)
Entities are IAM users, user groups and roles.

Filter by Entity type
All types 1 match

Search route

Entity name	Entity type
route-table-change	Roles

Cancel **Attach policy**

步骤6.配置并启动C8000v实例

每个C8000v路由器将有2个接口（1个公共接口，1个专用接口），并将在其自己的可用区上创建。

在EC2 Dashboard上，单击Launch Instances:

aws

Search

[Option+S]

☰

EC2

Dashboard

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

▼ Images

AMIs

AMI Catalog

Resources

You are using the following Amazon EC2 resources in the United States (N. Virgin

Instances (running)	1	Auto Scaling Groups
Dedicated Hosts	0	Elastic IPs
Key pairs	17	Load balancers
Security groups	19	Snapshots

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

▼

Migrate a server

Note: Your instances will launch in the United States (N. Virginia) Region

使用名称Cisco Catalyst 8000v for SD-WAN & Routing过滤AMI数据库。在AWS Marketplace AMIs列表上，单击Select。

Choose an Amazon Machine Image (AMI)

Cancel

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Selected AMI: (ami-09e6f87a47903347c) (Quick Start AMIs)

Q Cisco Catalyst 8000v for SD-WAN & Routing

×

⌵

Quick Start AMIs (0)

My AMIs (691)

AWS Marketplace AMIs (1)

Community AMIs (500)

▼ Refine results

Categories

Infrastructure Software (1)

▼ Publisher

☐ Cisco Systems, Inc. (1)

▼ Pricing model

☐ Bring Your Own License (1)

Operating system

☐ All Linux/Unix

▼ Architecture

Cisco Catalyst 8000v for SD-WAN & Routing (1 result) showing 1 - 1

Sort By: Relevance

1

⌵

⏮

⏪

⏩

⏭

CISCO

Cisco Catalyst 8000V for SD-WAN & Routing

By Cisco Systems, Inc. | Ver 17.15.03a

As part of Cisco's Cloud connect portfolio, the Bring Your Own License (BYOL) version of Cisco® Catalyst® 8000V Edge Software (Catalyst 8000V) delivers the maximum performance for virtual enterprise-class networking services & VPN in the AWS cloud. This AMI supports all the Catalyst 8000V (C8000V)...

Select

选择AMI的相应大小。在本例中，c5n.large大小被选中。这取决于您的网络所需的容量。选择后，单击Subscribe now。

Published by me | AWS & trusted third-party AMIs | Published by anyone

Cisco Catalyst 8000V for SD-WAN & Routing

Cisco Systems, Inc. [0 AWS reviews](#)
[Bring Your Own License](#)

Overview | Product details | **Pricing** | Usage | Support

Bring Your Own License
Available for customers with current licenses purchased via other channels.

▶ Cisco Catalyst 8000V for SD-WAN & Routing EC2 - c5n.large <i>vendor recommended</i>	\$0/Hour \$0.108/Hour
▶ EBS volume	

Cancel [Subscribe on instance launch](#) [Subscribe now](#)

步骤6.1.配置远程访问密钥对

订用AMI后，将显示一个包含多个选项的新窗口。在Key pair(login)部分中，如果不存在密钥对，请单击Create new key pair。您可以为每个创建的设备重复使用单个密钥。

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

fsimmond-pem ▼ [Create new key pair](#)

系统将显示新的弹出窗口。在本示例中，将创建具有ED25519加密的.pem密钥文件。设置完所有内容后，单击Create key pair。

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

fsimmond-ed-pem

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☐ RSA
RSA encrypted private and public key pair

☒ ED25519
ED25519 encrypted private and public key pair

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

 When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#) 

Cancel

Create key pair

步骤6.2.创建并配置AMI的子网

在Network Settings部分中，单击Edit。部分中的一些新选项现在可用：

- 1.为此工作选择所需的VPC。在本示例中，选择名为HA的VPC。
- 2.在“防火墙（安全组）”部分，选择“选择现有安全组”。
- 3.选择选项2后，Common security groups选项将可用。过滤并选择所需的安全组。在本示例中，选择All traffic HA安全组。
- 4.（可选）如果没有为这些设备创建子网，请单击Create new subnet。

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-0d30b9fa9511f3639 (HA)
10.100.0.0/16

Subnet [Info](#)

subnet-0b664f8e74443d28f public-R1-C8000v
VPC: vpc-0d30b9fa9511f3639 Owner: 073713984176 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.100.10.0/24

Auto-assign public IP [Info](#)

Disable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group ☒ Select existing security group

Common security groups [Info](#)

Select security groups

All traffic HA sg-029461ba80052f10c X
VPC: vpc-0d30b9fa9511f3639

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

1

4

2

3

Create new subnet

Compare security group rules

Web浏览器上一个新的选项卡打开，引导您进入创建子网部分：

- 1.从下拉列表中选择此配置的相应VPC。
- 2.设置新子网的名称。
- 3.定义此子网的可用性区。（有关设置的详细信息，请参阅本文档的拓扑部分）
- 4.设置属于VPC CIDR块的子网块。
- 5.此外，单击Add new subnet部分可创建将要使用的所有子网，并对每个子网重复从2到4的步骤。
- 6.完成后，单击创建子网。导航到上一页以继续设置。

☰ VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID

Create a new VPC or select an existing VPC.

vpw-0d30b9fa9511f3639 (HA) 1

Associated VPC CIDRs

IPv4 CIDRs

10.100.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Associate a tag with a key of "Name" and a value that you specify.

public-R1-C8000v 2

The name can be up to 256 characters long.

Availability Zone Info

Select an Availability Zone for your subnet, or let Amazon choose one for you.

United States (N. Virginia) / us-east-1a 3

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.100.0.0/16

IPv4 subnet CIDR block

10.100.10.0/24 4 256 IPs

< > ^ v

Tags - optional

Key	Value - optional	
Q Name	Q public-R1-C8000v	Remove

You can add 49 more tags.

Add new tag

Remove

Add new subnet 5

6

Cancel Create subnet

在Network Settings部分的Subnet子部分中，单击Refresh图标在下拉列表中获取创建的子网。

步骤6.3. 配置AMI接口

在Network Settings部分中，展开Advanced Network configuration子部分。将显示以下选项：

▼ Advanced network configuration

Network interface 1

Device index | Info

0

Subnet | Info

subnet-0b664f8e74443d28f

IP addresses available: 249

Primary IP | Info

10.100.10.254

IPv4 Prefixes | Info

Select

Delete on termination | Info

No

ENA Express | Info

Select

The selected instance type does not support ENA Express.

Idle connection tracking timeout | Info

☐ Enable

Add network interface

Network interface | Info

New interface

Security groups | Info

Select security groups

Secondary IP | Info

Select

IPv6 Prefixes | Info

Select

The selected subnet does not support IPv6 prefixes because it does not have an IPv6 CIDR.

Interface type | Info

Select

Description | Info

Public-R1

Auto-assign public IP | Info

Disable

IPv6 IPs | Info

Select

The selected subnet does not support IPv6 IPs.

Assign Primary IPv6 IP | Info

Select

A primary IPv6 address is only compatible with subnets that support IPv6.

Network card index | Info

Select

The selected instance type does not support multiple network cards.

ENA queues | Info

The selected instance type does not support ENA queues.

在此菜单上，设置Description、Primary IP、Delete on termination参数。
对于Primary IP参数，请使用除子网第一个可用地址以外的任何IP地址。这由AWS内部使用。

本示例中的终止时删除参数设置为否。但是，这可以设置为yes，具体取决于您的环境。

由于此拓扑，专用子网需要第二个接口。单击Add network interface，将显示此提示。但是，接口提供选择子网这一次的选项：

Network interface 2

Device index | Info

1

Subnet | Info

subnet-0a5f13361443951d2

IP addresses available: 250

Primary IP | Info

10.100.110.254

Network interface | Info

New interface

Security groups | Info

Select security groups

Secondary IP | Info

Select

Description | Info

Private-R1

Auto-assign public IP | Info

Select

IPv6 IPs | Info

Select

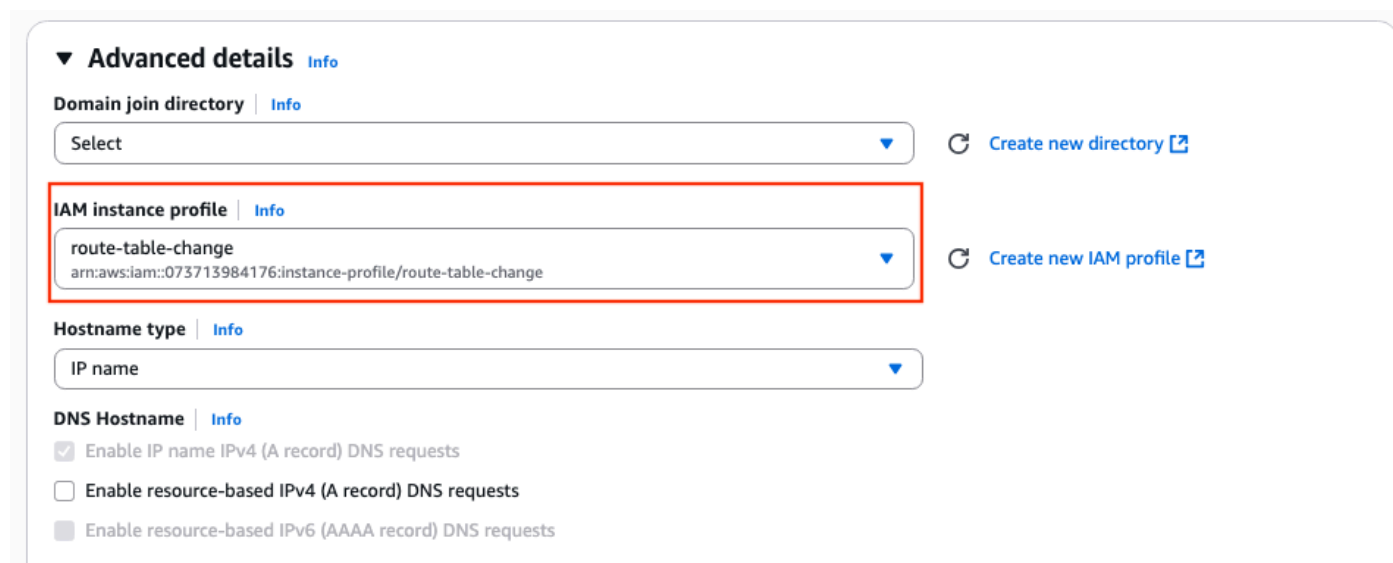
The selected subnet does not support IPv6 IPs.

Remove

按照在网络接口1上设定的方式设置所有参数后，继续执行后续步骤。

步骤6.4.将IAM实例配置文件设置为AMI

在Advanced details部分下，在IAM实例配置文件参数上选择创建的IAM角色：



▼ Advanced details [Info](#)

Domain join directory | [Info](#)

Select [Create new directory](#)

IAM instance profile | [Info](#)

route-table-change
arn:aws:iam::073713984176:instance-profile/route-table-change [Create new IAM profile](#)

Hostname type | [Info](#)

IP name

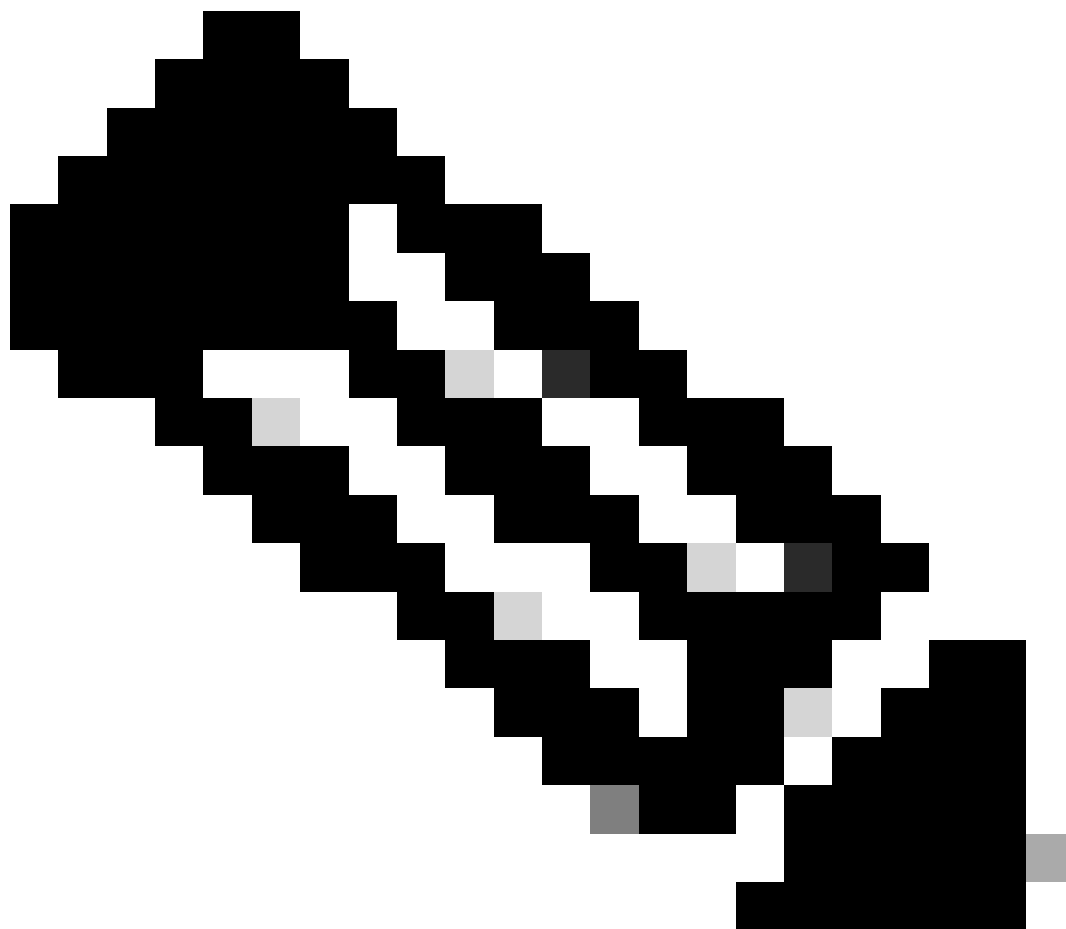
DNS Hostname | [Info](#)

- ☒ Enable IP name IPv4 (A record) DNS requests
- ☐ Enable resource-based IPv4 (A record) DNS requests
- ☐ Enable resource-based IPv6 (AAAA record) DNS requests

第6.5步（可选）在AMI上设置凭证

在Advanced details部分下，导航到User data - optional部分，并应用此设置以在创建实例时设置用户名和密码：

```
ios-config-1="username <username> priv 15 pass <password>"
```



注意：通过SSH连接到C8000v的AWS提供的用户名可能错误地列为root。如有必要，请将其更改为ec2-user。

步骤6.6.完成实例配置

完成所有配置后，单击Launch Instance:

▼ Summary

Number of instances | [Info](#)

1

Software Image (AMI)

Cisco Catalyst 8000V for SD-WA...[read more](#)

ami-03cc286883c62bdee

Virtual server type (instance type)

c5n.large

Firewall (security group)

All traffic HA

Storage (volumes)

1 volume(s) - 16 GiB

 **Free tier:** In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



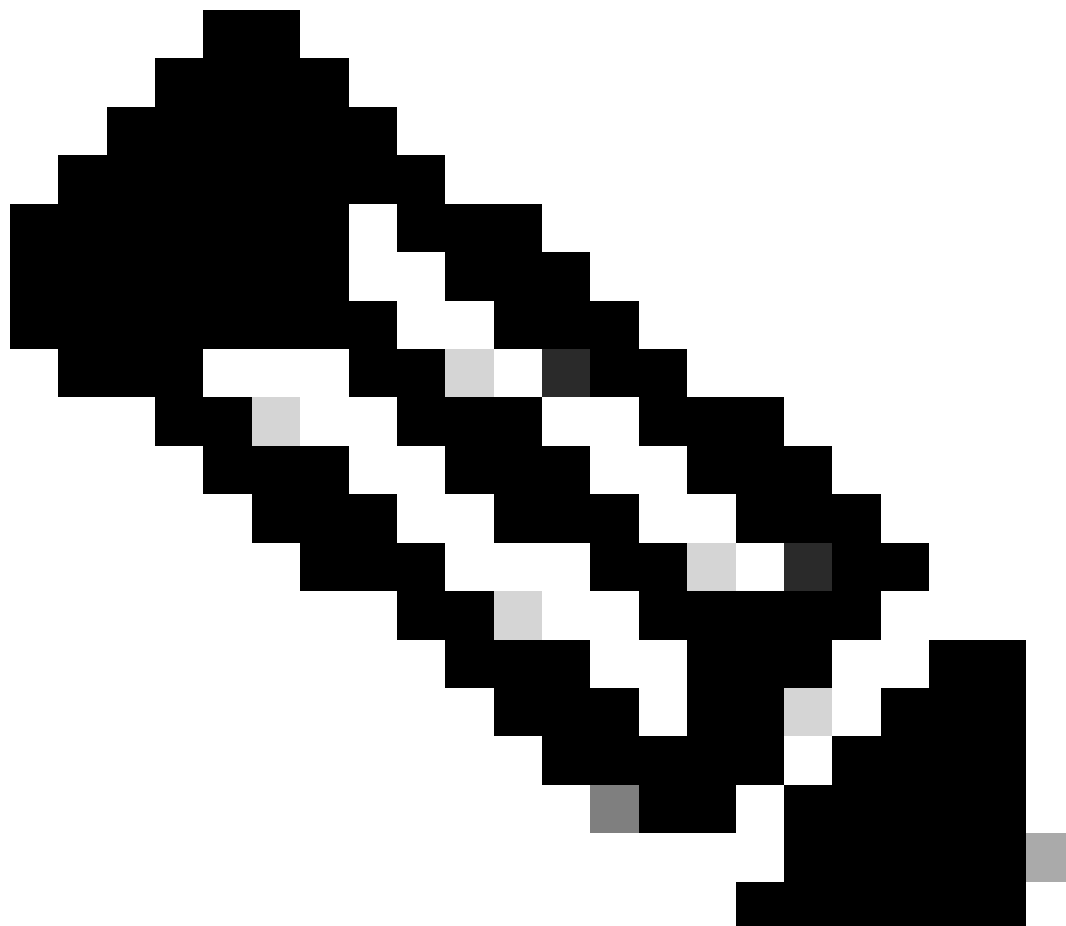
[Cancel](#)

[Launch instance](#)

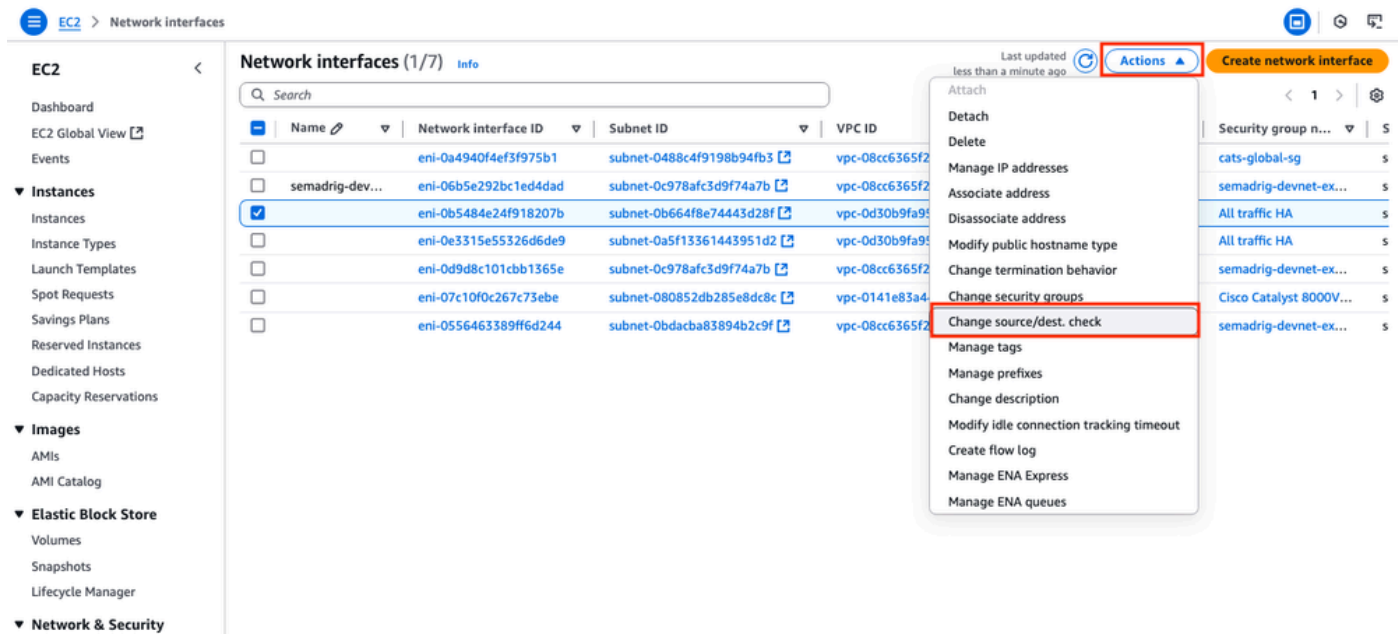
 [Preview code](#)

步骤6.7.禁用ENI上的源/目标检查

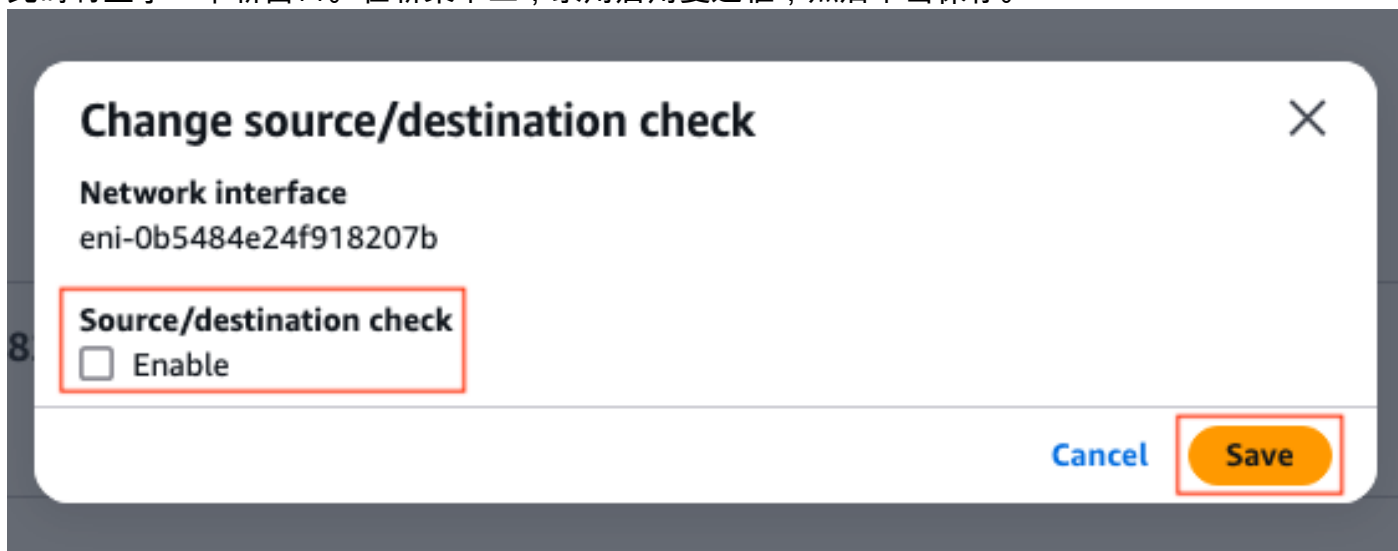
创建实例后，在AWS上禁用src/dst检查功能以获得相同子网中接口之间的连接。在EC2 Dashboard > Network & Security > Network interfaces 部分中，选择ENIs，然后单击Actions >更改源/目标检查。



注意：必须逐一选择ENI才能使用此选项。

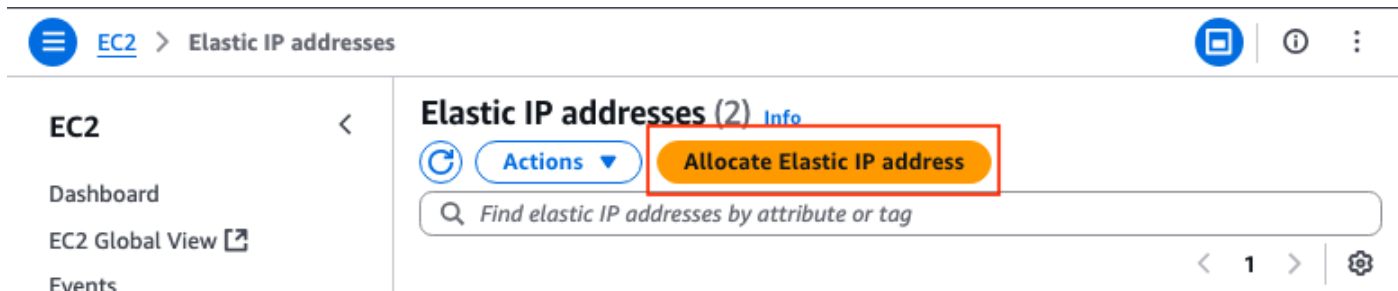


此时将显示一个新窗口。在新菜单上，禁用启用复选框，然后单击保存。



步骤6.8.创建弹性IP并将其关联到实例的公共ENI

在EC2 Dashboard > Network & Security > Elastic IPs 部分中，单击Allocate Elastic IP address。



该页面引导您进入另一个部分。在本例中，选择Amazon pool of IPv4 addresses选项以及可用区域us-east-1。完成后，单击Allocate。

EC2 > Elastic IP addresses > Allocate Elastic IP address

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Public IPv4 address pool

- ☒ Amazon's pool of IPv4 addresses
- ☐ Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) [Learn more](#)
- ☐ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) [Learn more](#)
- ☐ Allocate using an IPv4 IPAM pool (option disabled because no public IPv4 IPAM pools with AWS service as EC2 were found)

Network border group [Info](#)

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

[Create accelerator](#)

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tag

[Cancel](#) [Allocate](#)

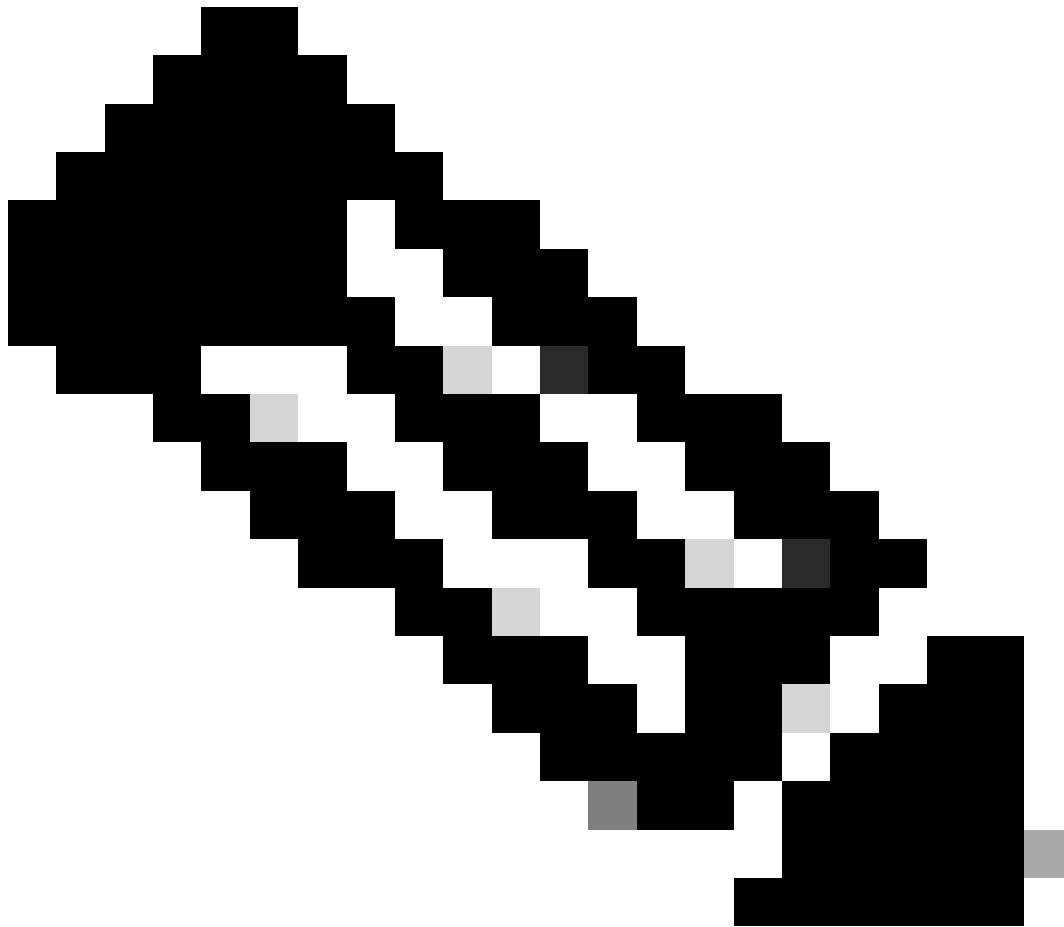
创建IP地址后，将IP地址分配给实例的公用接口。在EC2 Dashboard > Network & Security > Elastic IPs 部分上，单击Actions > Associate Elastic IP address。

Elastic IP addresses (1/1) [Info](#)

[Public IPv4 address](#) [Clear filters](#)

☒	Name	Allocated IPv4 address	Type	Allocation ID	Reverse DNS record	
☒	-	-	Public IP	eipalloc-0948346735ab2017c	-	Actions View details Release Elastic IP addresses Associate Elastic IP address Disassociate Elastic IP address Update reverse DNS Enable transfers Disable transfers Accept transfers

在此新部分中，选择Network interface选项并查找相应接口的公共ENI。关联相应的公有IP地址，然后单击Associate。



注意：要获取正确的ENI ID，请导航至EC2 Dashboard > Instances部分。然后选择实例并选中Networking部分。查找公共接口的IP地址，获取同一行上的ENI值。

Associate Elastic IP address [Info](#)

Choose the instance or network interface to associate to this Elastic IP address ([Add IP to your account](#))

Elastic IP address: 10.100.100.254

Resource type
Choose the type of resource with which to associate the Elastic IP address.
☐ Instance
☒ Network interface

⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Network interface

Private IP address
The private IP address with which to associate the Elastic IP address.

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
☒ Allow this Elastic IP address to be reassociated

[Cancel](#) [Associate](#)

步骤7.重复步骤6，创建高可用性第二个C8000v实例

请参考本文档的拓扑部分，了解每个接口的相应信息，并重复从6.1到6.6的相同步骤。

步骤8.重复步骤6，从AMI市场创建VM(Linux/Windows)

在本示例中，从AMI市场中选择Ubuntu服务器22.04.5 LTS作为内部主机。

默认情况下，会为公共接口创建ens5。在本示例中，为专用子网创建第二个接口（设备上的ens6）。

<#root>

```
ubuntu@ip-10-100-30-254:~$ sudo apt install net-tools
```

```
...
```

```
ubuntu@ip-10-100-30-254:~$ ifconfig
```

```
ens5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
```

```
inet
```

10.100.30.254

```
netmask 255.255.255.0 broadcast 10.100.30.255
```

```
inet6 fe80::51:19ff:fea2:1151 prefixlen 64 scopeid 0x20<link>
```

```
ether 02:51:19:a2:11:51 txqueuelen 1000 (Ethernet)
```

```
RX packets 1366 bytes 376912 (376.9 KB)
```

```
RX errors 0 dropped 0 overruns 0 frame 0
```

```
TX packets 1417 bytes 189934 (189.9 KB)
```

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
ens6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
```

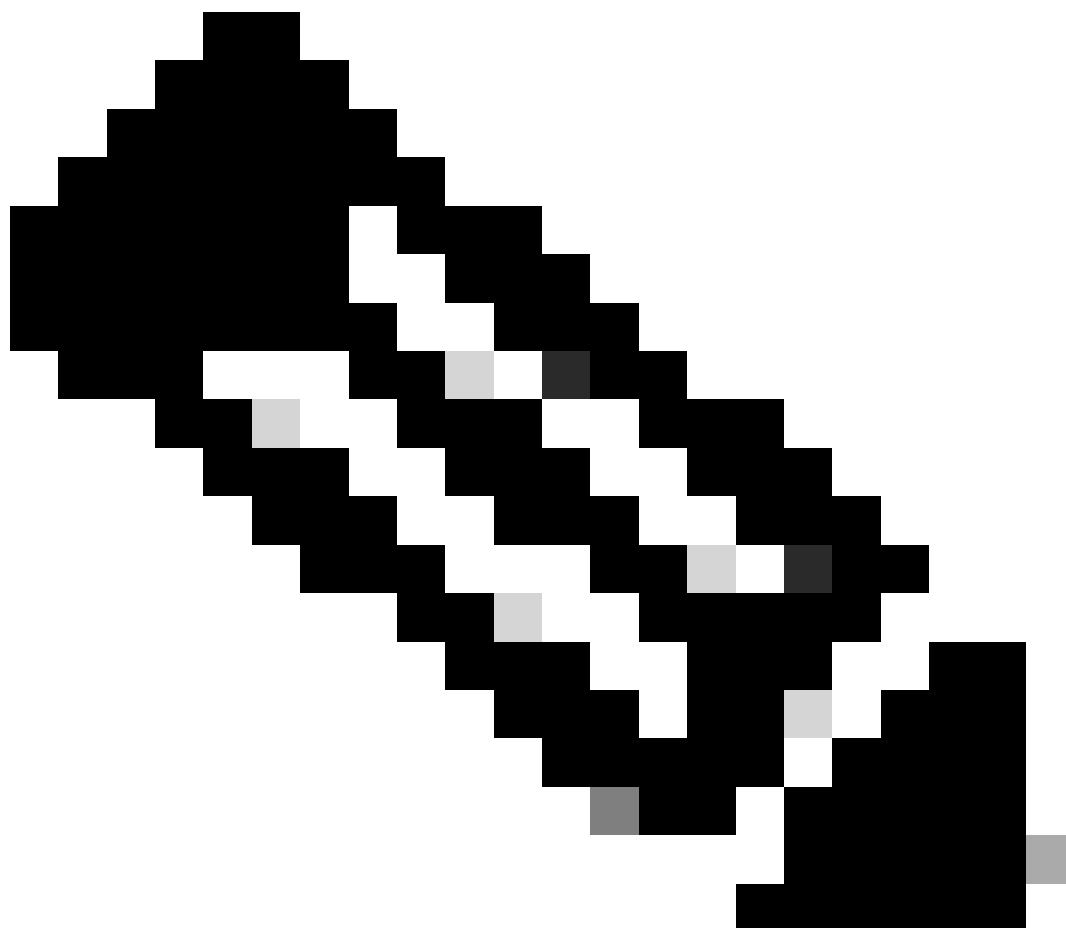
```
inet
```

10.100.130.254

```
netmask 255.255.255.0 broadcast 10.100.130.255
```

```
inet6 fe80::3b:7eff:fead:db5 prefixlen 64 scopeid 0x20<link>
```

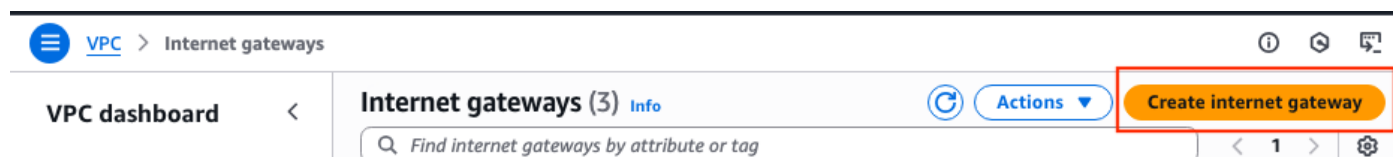
```
ether 02:3b:7e:ad:db:e5 txqueuelen 1000 (Ethernet)
RX packets 119 bytes 16831 (16.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 133 bytes 13816 (13.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



注意：如果对接口进行了任何更改，请摆动接口或重新加载VM以应用这些更改。

步骤9.创建并配置VPC的Internet网关(IGW)

在**VPC Dashboard > Virtual private cloud > Internet gateways**部分中，单击**Create internet gateway**。



在此新部分中，为此网关创建name标记，然后单击Create internet gateway。

VPC > Internet gateways > Create internet gateway

Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

HA-internet-gateway

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Q Name

Value - optional

Q HA-internet-gateway

Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

创建IGW后，将其连接到相应的VPC。导航到VPC Dashboard > Virtual Private Cloud > Internet Gateway部分并选择相应的IGW。单击操作>连接到VPC。

VPC > Internet gateways

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Internet gateways (1/1)

Find internet gateways by attribute or tag

HA

Clear filters

☒	Name	Internet gateway ID	State	VPC ID
☒	HA-internet-gateway	igw-089adf1bccd7bda47	Detached	-

Actions

Create internet gateway

View details

Attach to VPC

Detach from VPC

Manage tags

Delete internet gateway

在此新部分中，选择名为HA的VPC。对于此示例，请单击连接互联网网关。

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

Q Select a VPC

AWS Command Line Interface command

Cancel

Attach internet gateway

IGW必须如图所示指示连接状态：

VPC > Internet gateways > igw-089adf1bccd7bda47

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

igw-089adf1bccd7bda47 / HA-internet-gateway

Actions

Details

Internet gateway ID

igw-089adf1bccd7bda47

State

Attached

VPC ID

vpc-0d30b9fa9511f3639 | HA

Owner

073713984176

Tags

Search tags

Key

Value

Name

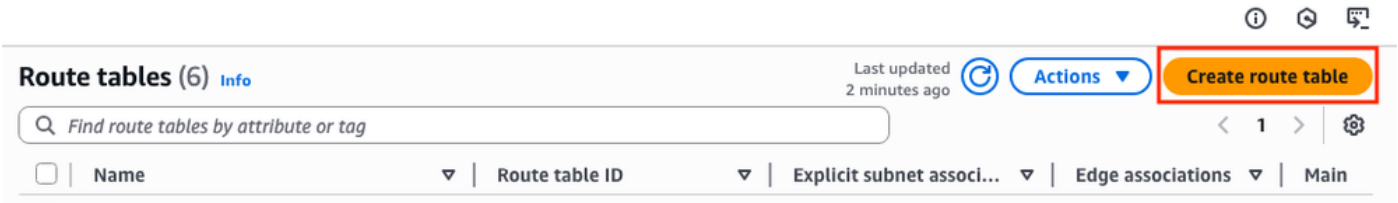
HA-internet-gateway

Manage tags

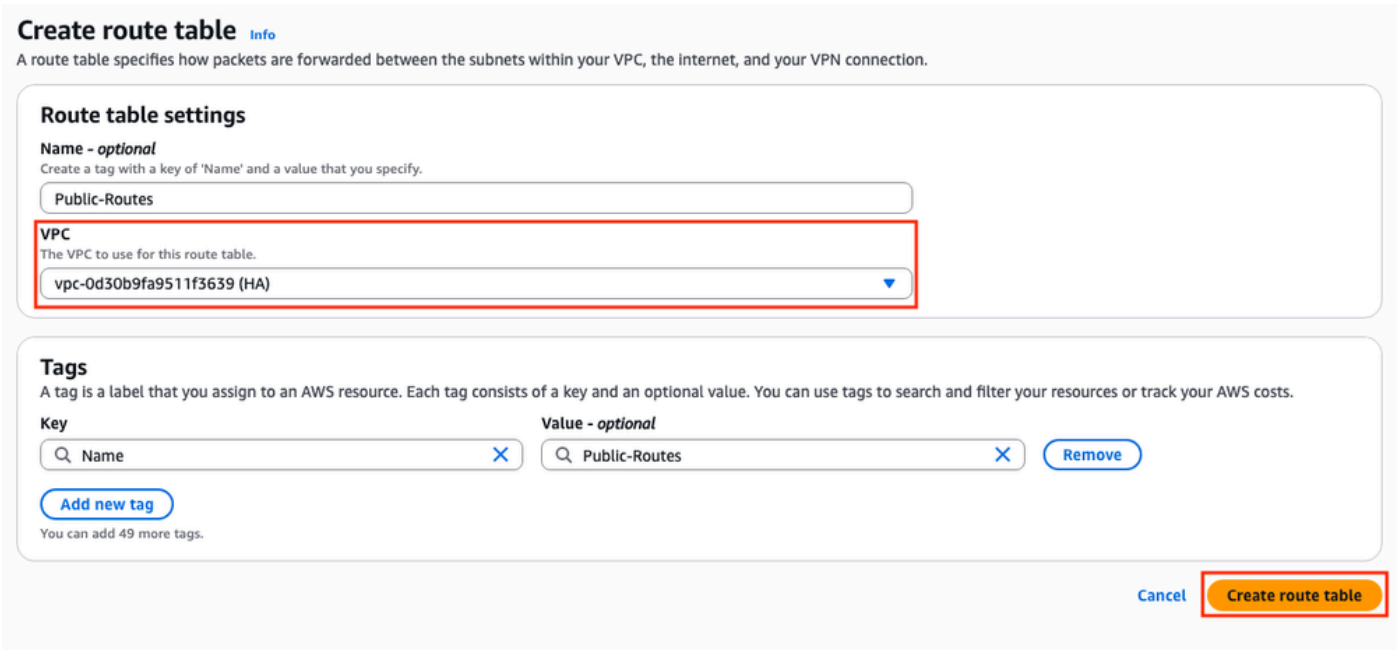
步骤10.在AWS上创建并配置公共子网和专用子网的路由表

步骤10.1.创建并配置公共路由表

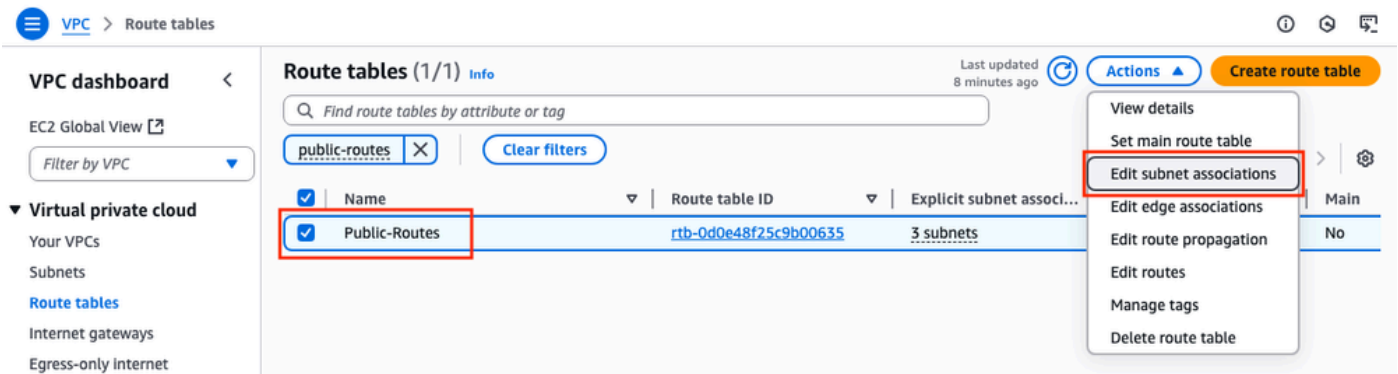
要在此拓扑上建立HA，请将所有公共子网和专用子网关联到其相应的路由表中。在VPC Dashboard > Virtual Private Cloud > Route tables部分中，单击Create route table。



在新部分中，为此拓扑选择对应的VPC。选中后，单击Create route table。



在路由表部分中，选择创建的表，然后单击操作>编辑子网关联。



然后，选择对应的子网，然后单击保存关联。

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (3/6)

public Clear filters

☒	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☒	public-R1-C8000v	subnet-0b664f8e74443d28f	10.100.10.0/24	-	rtb-0d0e48f25c9b00635 / Public-Routes
☒	Public-VM-linux-1c - fsmmond	subnet-04fb9de939e3778bb	10.100.30.0/24	-	rtb-0d0e48f25c9b00635 / Public-Routes
☒	public-R2-C8000v	subnet-02d8108842f9f3129	10.100.20.0/24	-	rtb-0d0e48f25c9b00635 / Public-Routes

Selected subnets
subnet-0b664f8e74443d28f / public-R1-C8000v subnet-04fb9de939e3778bb / Public-VM-linux-1c - fsmmond subnet-02d8108842f9f3129 / public-R2-C8000v

Cancel Save associations

关联子网后，单击Route table ID超链接为表添加正确的路由。然后，单击Edit Routes:

Route tables (1/1) [Info](#)

public-routes Clear filters

☒	Name	Route table ID
☒	Public-Routes	rtb-0d0e48f25c9b00635

要访问Internet，请单击Add route并将此公共路由表与IGW链接，该IGW是在第9步使用这些参数创建的。选中后，单击Save changes:

Edit routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	Active	No

Add route Cancel Preview Save changes

步骤10.2.创建并配置专用路由表

创建公共路由表后，除了在其路由上添加Internet网关外，还要为私有路由和私有子网复制步骤10。在本示例中，路由表如下所示，因为8.8.8.8的流量必须通过本示例中的专用子网：

Edit routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	Active	No
8.8.8.8/32	Network interface	-	No
	eni-0239fda341b4d7e41		

[Add route](#) [Cancel](#) [Preview](#) [Save changes](#)

步骤11.检查并配置基本网络配置、网络地址转换(NAT)、具有BFD的GRE隧道和路由协议

在AWS上准备好实例及其路由配置后，请配置设备：

C8000v R1配置：

```
interface Tunnel1
ip address 192.168.200.1 255.255.255.0
bfd interval 500 min_rx 500 multiplier 3
tunnel source GigabitEthernet1
tunnel destination <Public IPv4 address of C8000v R2>
!
interface GigabitEthernet1
ip address 10.100.10.254 255.255.255.0
ip nat outside
negotiation auto
!
interface GigabitEthernet2
ip address 10.100.110.254 255.255.255.0
ip nat inside
negotiation auto
!
router eigrp 1
bfd interface Tunnel1
network 192.168.200.0
passive-interface GigabitEthernet1
!
ip access-list standard 10
10 permit 10.100.130.0 0.0.0.255
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 10.100.10.1
ip route 10.100.130.0 255.255.255.0 GigabitEthernet2 10.100.110.1
```

C8000v R2配置：

```
interface Tunnel1
ip address 192.168.200.2 255.255.255.0
bfd interval 500 min_rx 500 multiplier 3
tunnel source GigabitEthernet1
```



```

tunnel destination<Public IPv4 address of C8000v R1>
!
interface GigabitEthernet1
ip address 10.100.20.254 255.255.255.0
ip nat outside
negotiation auto
!
interface GigabitEthernet2
ip address 10.100.120.254 255.255.255.0
negotiation auto
!
router eigrp 1
bfd interface Tunnel1
network 192.168.200.0
passive-interface GigabitEthernet1
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 10.100.20.1
ip route 10.100.130.0 255.255.255.0 GigabitEthernet2 10.100.120.1
!
ip access-list standard 10
10 permit 10.100.130.0 0.0.0.255
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!

ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 10.100.20.1
ip route 10.100.130.0 255.255.255.0 GigabitEthernet2 10.100.120.1

```

步骤12.配置高可用性(Cisco IOS® XE Denali 16.3.1a或更高版本)

设置了VM之间的冗余和连接后，请配置HA设置以定义路由更改。设置Route-table-id、Network-interface-id和CIDR值，这些值在AWS HA错误（例如BFD对等体关闭）后必须设置。

```

Router(config)# redundancy
Router(config-red)# cloud provider aws (node-id)
bfd peer <IP address of the remote device>
route-table <Route table ID>
cidr ip <traffic to be monitored/prefix>
eni <Elastic network interface (ENI) ID>
region <region-name>

```

bfd peer参数与隧道对等IP地址相关。可使用show bfd neighbor输出检查此情况：

```
R1(config)#do sh bfd neighbors
```

```

IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
192.168.200.2 4097/4097 Up Up Tu1

```

route-table参数与位于VPC Dashboard > Virtual Private Cloud > Route Tables部分中的专用路由表ID相关。复制相应的路由表ID。

Route tables (2) Info

Find route tables by attribute or tag

Routes

X

Clear filters

☐	Name	Route table ID
☐	Private-Routes	rtb-093df10a4de426eb8
☐	Public-Routes	rtb-0d0e48f25c9b00635

cidr ip参数与私有路由表中添加的路由前缀相关（步骤10.2中创建的路由）：

rtb-093df10a4de426eb8 / Private-Routes

Details Info

Route table ID

rtb-093df10a4de426eb8

VPC

vpc-0d30b9fa9511f3639

 | HA

Main

Yes

Owner ID

073713984176

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Filter routes

Destination	Target
8.8.8.8/32	eni-0239fda341b4d7e41
10.100.0.0/16	local

eni参数与所配置实例的相应专用接口的ENI ID相关。在本示例中，使用实例接口GigabitEthernet2的ENI ID:

Instances (1/3) [Info](#) Last updated 1 minute ago [Connect](#) [Instance state](#) [Actions](#) [Launch Instances](#)

[All states](#)

[fsimmond](#) [Clear filters](#) < 1 > [Settings](#)

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
☐	C8000v-R2-fsimmond	i-0a1a91794f919f641	Stopped	c5n.large	-	View alarms +	us-east-1b
☐	Ubuntu VM - fsimmond	i-03a306e81a0b99864	Stopped	m5.large	-	View alarms +	us-east-1c
☒	C8000v-R1-fsimmond	i-0b9a50a09b089b03a	Running	c5n.large	3/3 checks passed	View alarms +	us-east-1a

i-0b9a50a09b089b03a (C8000v-R1-fsimmond) [Settings](#) [Down Arrow](#)

[Details](#) [Status and alarms](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

VPC ID
vpc-0d30b9fa9511f3639 (HA) [Info](#)

Subnet ID
subnet-0b664f8e74443d28f (public-R1-C8000v) [Info](#)

Availability zone
us-east-1a

Outpost ID
-

[IP addresses](#) [Info](#)

[Hostname and DNS](#) [Info](#)

[Network Interfaces \(2\)](#) [Info](#)

Interface ID	Device index	Card index	Description	Public IPv4 address	Private IPv4 address	Private IPv4 DNS	IPv6
eni-0645a881c13823696	0	0	-	104.213.108.218	10.100.10.254	-	-
eni-070e14fbfde0d8e3b	1	0	-	-	10.100.110.254	-	-

region参数与VPC所在区域的AWS文档中的代码名称相关。在本示例中，使用us-east-1区域。

但是，此列表可以更改或增加。要查找最新更新，请访问[AmazonRegion and Availability Zones](#)文档。

考虑到所有这些信息，下面是VPC中每台路由器的配置示例：

C8000v R1的配置示例：

```

redundancy
cloud provider aws 1
bfd peer 192.168.200.2
route-table rtb-093df10a4de426eb8
cidr ip 8.8.8.8/32
eni eni-070e14fbfde0d8e3b
region us-east-1

```

C8000v R2的配置示例：

```

redundancy
cloud provider aws 1
bfd peer 192.168.200.1
route-table rtb-093df10a4de426eb8
cidr ip 8.8.8.8/32

```

```
eni eni-0239fda341b4d7e41
region us-east-1
```

确认

1.检查C8000v R1实例状态。确认隧道和云冗余已启动且正在运行。

```
R1#show bfd neighbors
```

```
IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
192.168.200.2 4097/4097 Up Up Tu1
```

```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.200.2 Tu1 10 00:16:52 2 1470 0 2
```

```
R1#show redundancy cloud provider aws 1
Provider : AWS node 1
BFD peer = 192.168.200.2
BFD intf = Tunnel1
route-table = rtb-093df10a4de426eb8
cidr = 8.8.8.8/32
eni = eni-070e14fbfde0d8e3b
region = us-east-1
```

2.从路由器后面的主机VM连续对8.8.8.8执行ping操作。请确保ping通过专用接口：

```
ubuntu@ip-10-100-30-254:~$ ping -I ens6 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 10.100.130.254 ens6: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=1.36 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=1.30 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=1.34 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=1.28 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=1.31 ms
```

3.打开AWS WebGUI并检查路由表的状态。当前ENI属于R1实例的专用接口：

rtb-093df10a4de426eb8 / Private-Routes

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both

Edit routes

< 1 >

Filter routes

Destination	Target
8.8.8.8/32	eni-070e14fbfde0d8e3b
10.100.0.0/16	local

4.通过关闭R1实例上的Tunnel1接口来模拟HA故障切换事件，从而触发路由更改：

```
R1#config t
R1(config)#interface tunnel1
R1(config-if)#shut
```

5.再次查看AWS上的route 表,ENI ID已更改为R2的专用接口ENI ID:

rtb-093df10a4de426eb8 / Private-Routes

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Filter routes

Destination

8.8.8.8/32

10.100.0.0/16

Target

eni-0239fda341b4d7e41

local

故障排除

以下是重新创建部署时经常遗忘/配置错误的大部分常见问题：

- 确保资源已关联。创建VPC、子网、接口、路由表等时，其中许多接口不会自动相互关联。他们彼此并不了解。
- 确保Elastic IP和任何私有IP与正确的接口、正确的子网、添加到正确的路由表、连接到正确的路由器，以及与IAM角色和安全组链接的正确的VPC和区域。
- 禁用每个ENI的源/目标检查。
如果您已经检查了本部分讨论的所有要点，但问题仍然存在，请收集这些输出，测试高可用性故障切换（如果可能），并使用Cisco TAC创建案例：

```
show redundancy cloud provider aws <node-id>
debug redundancy cloud all
debug ip http all
```

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）。