

Implante a configuração de alta disponibilidade do C8000v no AWS

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Topologia](#)

[Diagrama de Rede](#)

[Resumo da Tabela](#)

[Restrições](#)

[Configuração](#)

[Etapa 1. Selecionar uma Região](#)

[Etapa 2. Criar o VPC](#)

[Etapa 3. Criar um Grupo de Segurança para o VPC](#)

[Etapa 4. Criar uma Função IAM com uma Política e Associar ao VPC](#)

[Etapa 5. Criar e Anexar uma Diretiva de Confiança a uma Função do IAM](#)

[Etapa 6. Configurar e iniciar as instâncias do C8000v](#)

[Etapa 6.1. Configurar o par de chaves para acesso remoto](#)

[Etapa 6.2. Criar e Configurar as Sub-Redes para o AMI](#)

[Etapa 6.3. Configurar as interfaces AMI](#)

[Etapa 6.4. Definir o perfil da instância IAM como AMI](#)

[Etapa 6.5. \(Opcional\) Definir as Credenciais no AMI](#)

[Etapa 6.6. Finalizar a Configuração da Instância](#)

[Etapa 6.7. Desativar a verificação da origem/destino nos ENI](#)

[Etapa 6.8. Criar e associar um IP elástico ao ENI público da instância](#)

[Etapa 7. Repita a Etapa 6 para criar a segunda instância do C8000v para HA](#)

[Etapa 8. Repita a Etapa 6 para criar uma VM \(Linux/Windows\) no AMI Marketplace.](#)

[Etapa 9. Criar e Configurar um Gateway de Internet \(IGW\) para o VPC](#)

[Etapa 10. Criar e Configurar Tabelas de Rotas no AWS para sub-redes Públicas e Privadas](#)

[Etapa 10.1. Criar e configurar a tabela de rotas públicas](#)

[Etapa 10.2. Criar e Configurar a Tabela de Rotas Privadas](#)

[Etapa 11. Verificar e Configurar a Configuração Básica de Rede, Network Address Translation \(NAT\), Túnel GRE com BFD e Protocolo de Roteamento](#)

[Etapa 12. Configurar a alta disponibilidade \(Cisco IOS® XE Denali 16.3.1a ou posterior\)](#)

[Verificação](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar um ambiente de alta disponibilidade com roteadores

Catalyst 8000v na nuvem do Amazon Web Services.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento anterior sobre estes tópicos:

- Conhecimento geral do AWS Console e seus componentes
- Compreensão do software Cisco IOS® XE
- Conhecimento básico do recurso HA.

Componentes Utilizados

Estes componentes são necessários para este exemplo de configuração:

- Uma conta do Amazon AWS com função de administrador
- Dois dispositivos C8000v executando Cisco IOS® XE 17.15.3a e 1 Ubuntu 22.04 LTS VM IAM na mesma região

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Topologia

Há vários cenários de implantação de HA com base nos requisitos de rede. Para este exemplo, a redundância de HA é configurada com estas configurações:

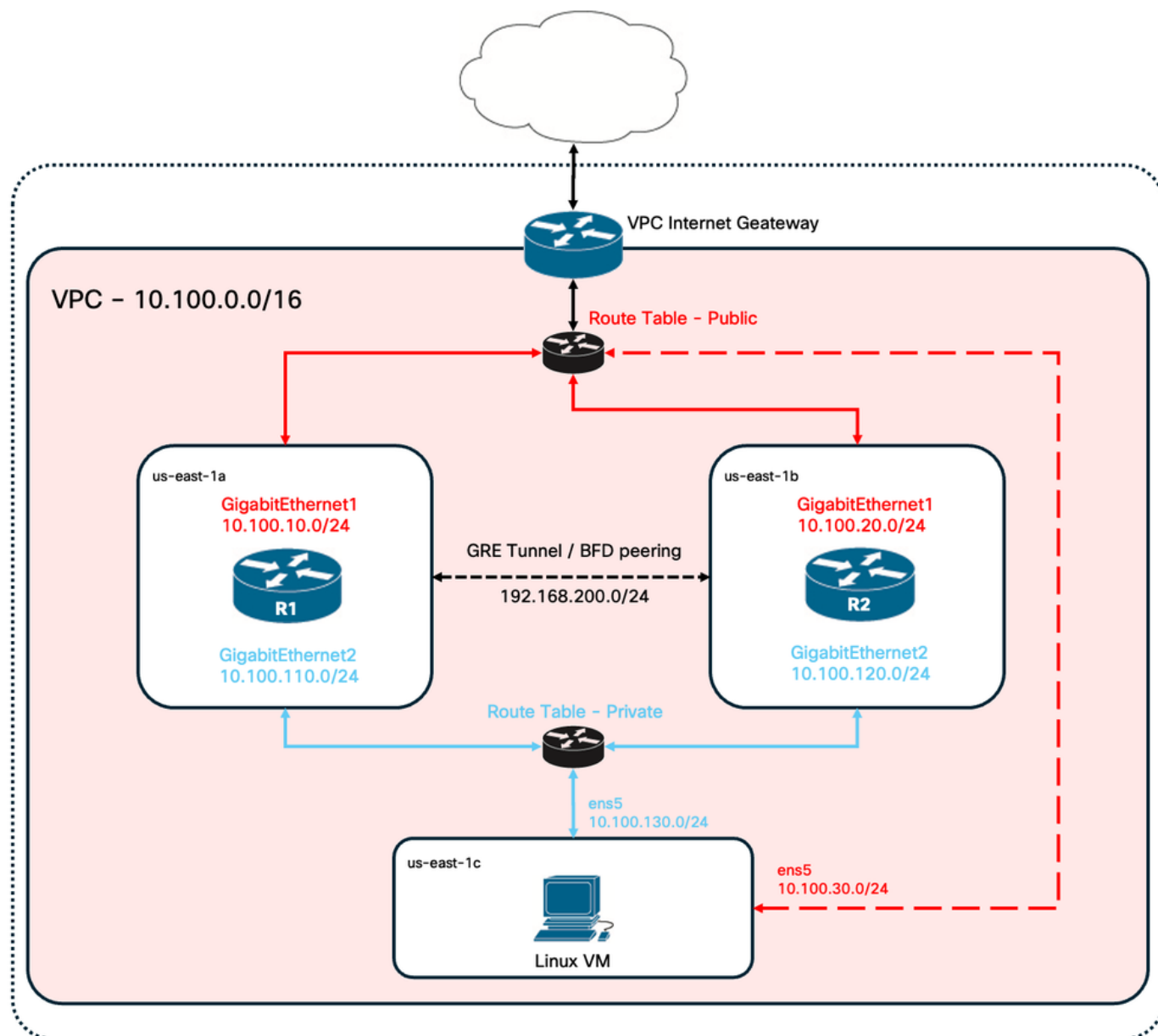
- 1x - Região
- 1x - VPC
- 3x - Zonas de disponibilidade
- 6x - Interfaces/sub-redes de rede (3x pública/3x privada)
- 2x - Tabelas de rota (pública e privada)
- 2x - Roteadores C8000v (Cisco IOS® XE Denali 17.15.3a)
- 1x - VM (Linux/Windows)

Há 2 roteadores C8000v em um par HA, em duas zonas de disponibilidade diferentes. Pense em cada zona de disponibilidade como um data center separado para obter resiliência de hardware adicional.

A terceira zona é uma VM, que simula um dispositivo em um data center privado. Por enquanto, o acesso à Internet é habilitado através da interface pública para que você possa acessar e configurar a VM. Geralmente, todo o tráfego normal deve fluir pela tabela de rotas privadas.

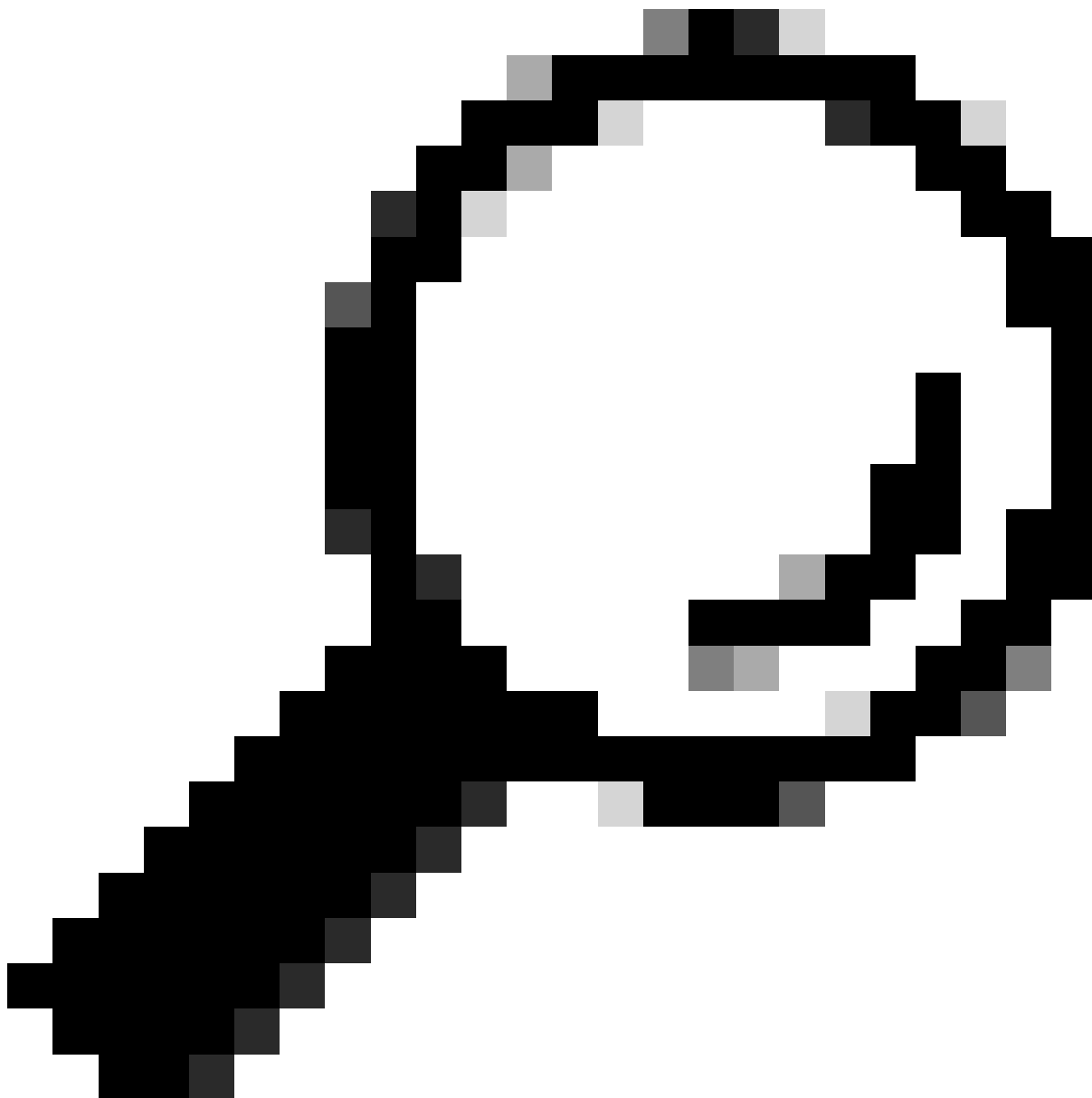
Para simular o tráfego, inicie um ping a partir da interface privada da máquina virtual, atravessando a tabela de rota privada através de R1 para alcançar 8.8.8.8. No caso de um failover, verifique se a tabela de rota privada foi atualizada automaticamente para rotear o tráfego através da interface privada do roteador R2.

Diagrama de Rede



Resumo da Tabela

Para resumir a topologia, esta é a tabela com os valores mais importantes de cada componente no laboratório. As informações fornecidas nesta tabela são exclusivas para este laboratório.



Dica: o uso desta tabela ajuda a manter uma visão geral clara das principais variáveis em todo o guia. É recomendável coletar as informações neste formato para simplificar o processo.

Dispositivo	Zona de Disponibilidade	Interfaces	Endereços IP	RTB	ENI
R1	us-east-1a	GigabitEthernet1	10.100.10.254	rtb-0d0e48f25c9b00635 (público)	eni-0645a881c13823696
		GigabitEthernet2	10.100.110.254	rtb-093df10a4de426eb8 (privado)	eni-070e14fbfde0d8e3b
R2	us-east-1b	GigabitEthernet1	10.100.20.254	rtb-0d0e48f25c9b00635	eni-0a7817922ffbb317b

				(público)	
		GigabitEthernet2	10.100.120.254	rtb-093df10a4de426eb8 (privado)	eni-0239fda341b4d7e41
VM Linux	us-east-1c	ens5	10.100.30.254	rtb-0d0e48f25c9b00635 (público)	eni-0b28560781b3435b1
		ens6	10.100.130.254	rtb-093df10a4de426eb8 (privado)	eni-05d025e88b6355808

Restrições

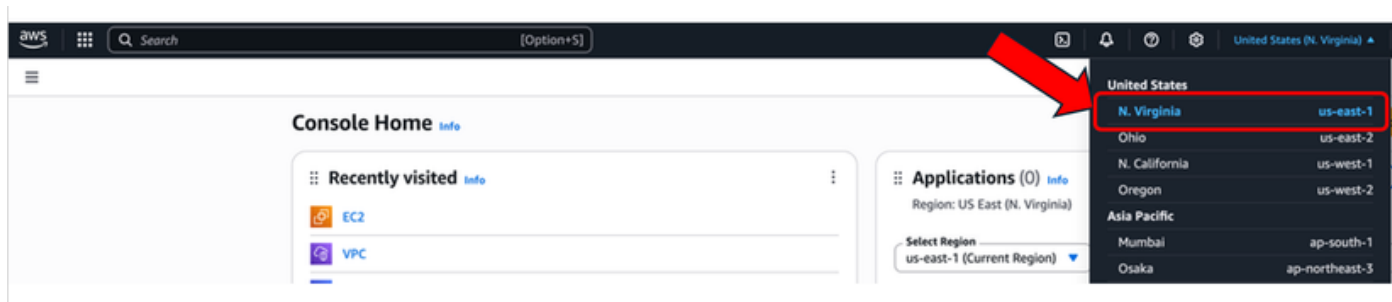
- Em qualquer sub-rede criada, não use o primeiro endereço disponível dessa sub-rede. Esses endereços IP são usados internamente pelos serviços AWS.
- Não configure as interfaces públicas dos dispositivos C8000v dentro de um VRF. O HA não funcionará corretamente se isso estiver definido.

Configuração

O fluxo geral de configuração se concentra em criar as VMs solicitadas na região apropriada e seguir para a configuração mais específica, como rotas e interfaces de cada uma delas. No entanto, é recomendável entender a topologia primeiro e configurá-la na ordem desejada.

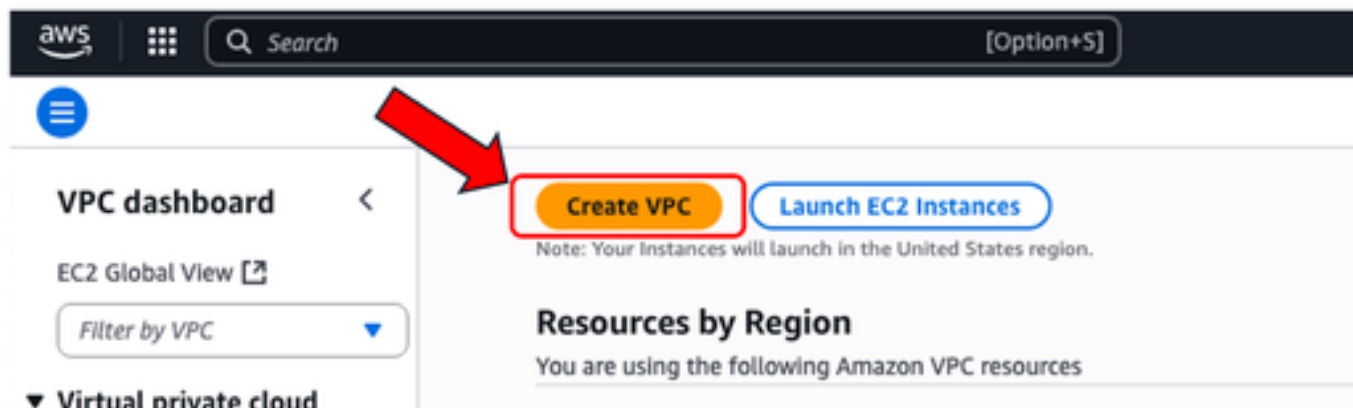
Etapa 1. Selecionar uma Região

Para este guia de implantação, a região Oeste dos EUA (Virgínia do Norte) - leste dos EUA-1 é selecionada como a região VPC.



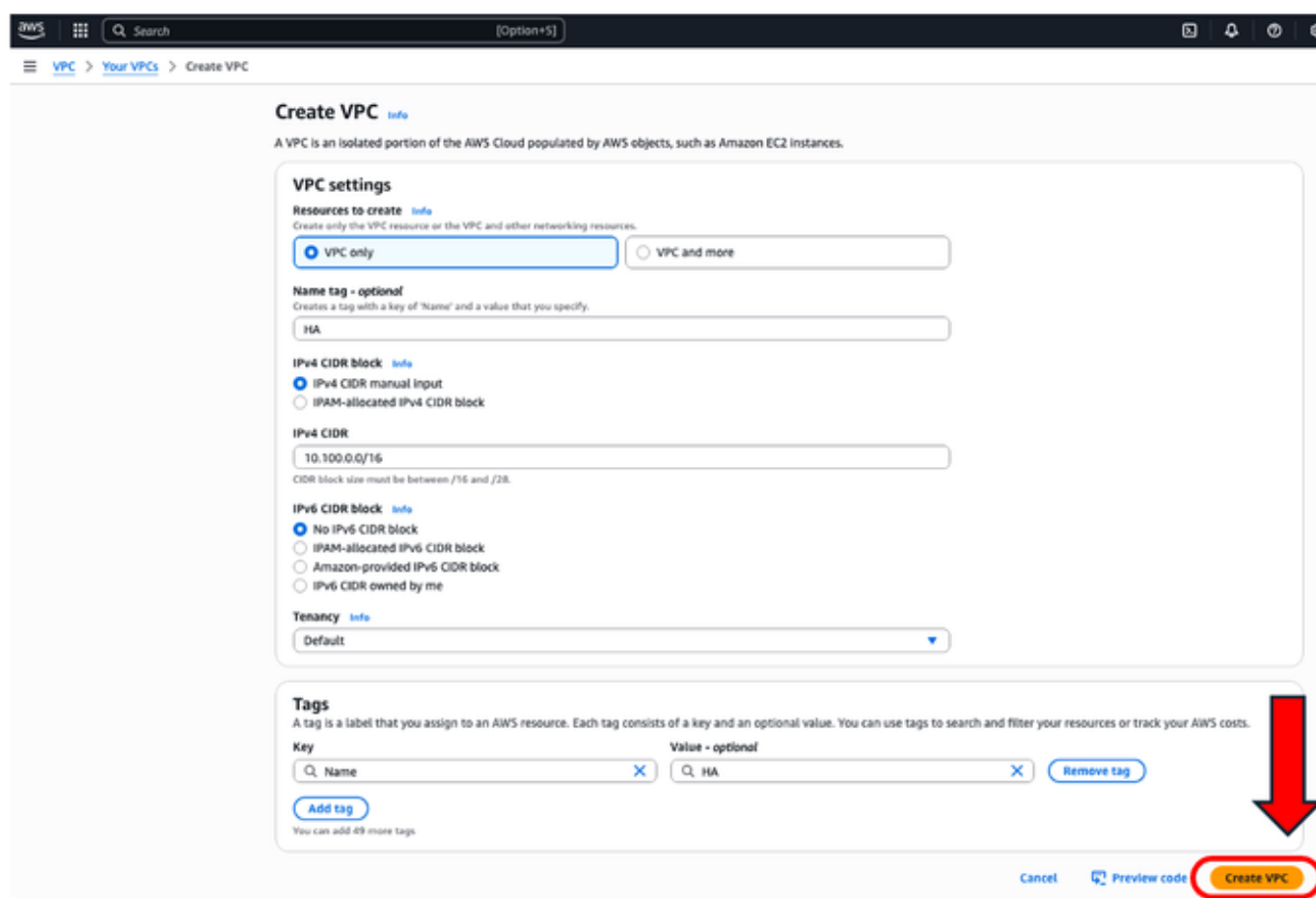
Etapa 2. Criar o VPC

No AWS Console, navegue para VPC > VPC Dashboard > Create VPC.

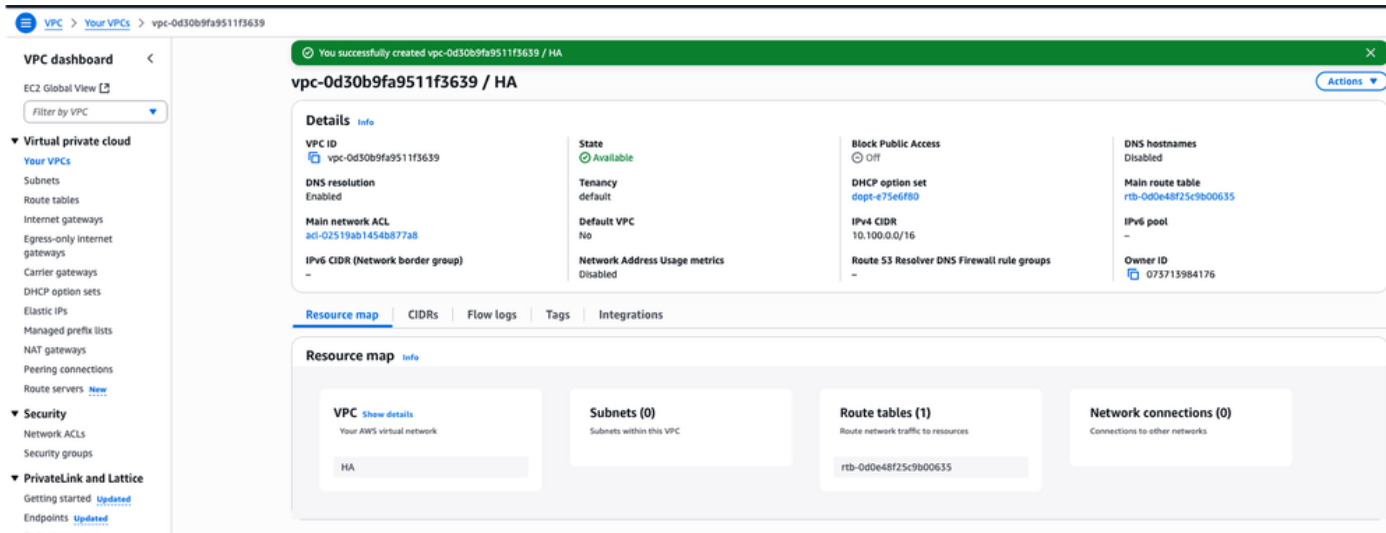


Ao criar o VPC, selecione a opção VPC only. Você pode atribuir uma rede /16 para usar como desejar.

Neste guia de implantação, a rede 10.100.0.0/16 é selecionada:

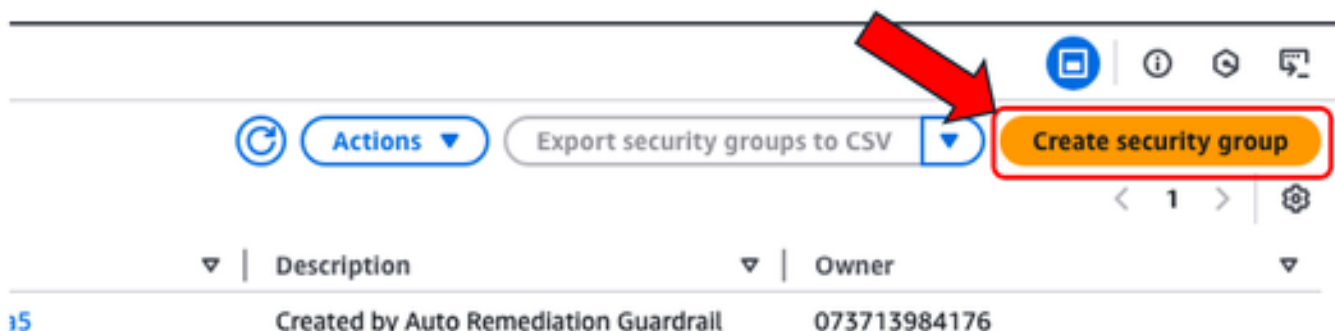


Após clicar em Create VPC, a marca VPC-0d30b9fa9511f3639 com HA é agora criada:



Etapa 3. Criar um Grupo de Segurança para o VPC

No AWS, os Grupos de Segurança funcionam como ACLs, permitindo ou negando o tráfego para VMs configuradas em um VPC. No Console do AWS, navegue para a seção VPC > VPC Dashboard > Segurança > Grupos de Segurança e clique em Criar grupo de segurança.



Em Inbound Rules (Regras de entrada), defina o tráfego que você deseja permitir. Para este exemplo, Todo o tráfego é selecionado usando a rede 0.0.0.0/0.

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

Inbound rules info

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

Add rule

Outbound rules info

Type	Protocol	Port range	Destination	Description - optional	
All traffic	All	All	Custom		Delete
			0.0.0.0/0		

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

Etapa 4. Criar uma Função IAM com uma Política e Associar ao VPC

O IAM concede aos seus AMIs o acesso necessário às APIs da Amazon. O C8000v é usado como um proxy para chamar comandos API do AWS para modificar a tabela de rotas no AWS. Por padrão, as instâncias EC2 não têm permissão para acessar as APIs. Por esse motivo, uma nova função do IAM deve ser criada e será aplicada durante as criações do AMI.

Navegue até o painel IAM e vá até Gerenciamento de acesso > Funções > Criar função. Esse processo consiste em 3 etapas:

AWS IAM > Roles

Roles (65) info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

☐	Role name	Trusted entities	Last activity
☐	admin	Identity Provider: amaws:iam:0737	52 days ago
☐	AmazonAppStreamServiceAccess	AWS Service: appstream	-
☐	ApplicationAutoScalingForAmazonAppStreamAccess	AWS Service: application-autoscaling	-
☐	aws-codestar-service-role	AWS Service: codestar	-
☐	aws-elasticbeanstalk-ec2-role	AWS Service: ec2	-
☐	aws-elasticbeanstalk-service-role	AWS Service: elasticbeanstalk	-
☐	AWSCloud9SSMAccessRole	AWS Service: ec2 and 1 more	-
☐	AWSServiceRoleForAmazonSSM	AWS Service: ssm (Service-Linked Role)	42 minutes ago
☐	AWSServiceRoleForAPIGateway	AWS Service: apigateway (Service-Linked Role)	-

Create role

Primeiro, selecione a opção AWS Service na seção Tipo de entidade confiável e EC2 como o serviço atribuído para esta política.

- 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

Ao terminar, clique em Avançar:

IAM > Roles > Create role

Step 1

Step 2

Step 3

Step 4

Select trusted entity

Add permissions

Name, review, and create

Add permissions Info

Permissions policies (1062) Info

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

Search

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

Por fim, defina o Nome da função e clique no botão Criar função.

Step 1

Step 2

Step 3

Select trusted entity

Add permissions

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

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

Permissions policy summary

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

Step 3: Add tags

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 role

Etapa 5. Criar e Anexar uma Diretiva de Confiança a uma Função do IAM

Depois que a Função é criada, uma Política de Confiança deve ser feita para adquirir a habilidade de modificar as tabelas de roteamento AWS quando necessário. Vá para a seção Políticas no dashboard do IAM. Clique no botão Create Policy. Esse processo consiste em duas etapas:

IAM

> Policies

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Policies (1367)

Info

Actions

Delete

Create policy

A policy is an object in AWS that defines permissions.

Filter by Type

All types

Search

< 1 2 3 4 5 6 7 ... 69 >

	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

Primeiro, certifique-se de que o editor de políticas esteja usando JSON e aplique os comandos mostrados abaixo. Depois de configurada, clique em Avançar:

Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual | **JSON** | Actions ▾ | [Icon]

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "ec2:AssociateRouteTable",  
8         "ec2:CreateRoute",  
9         "ec2:CreateRouteTable",  
10        "ec2>DeleteRoute",  
11        "ec2>DeleteRouteTable",  
12        "ec2:DescribeRouteTables",  
13        "ec2:DescribeVpcs",  
14        "ec2:ReplaceRoute",  
15        "ec2:DisassociateRouteTable",  
16        "ec2:ReplaceRouteTableAssociation"  
17      ],  
18      "Resource": "*"   
19    }  
20  ]  
21 }
```

+ Add new statement

JSON Ln 21, Col 1

5825 of 6144 characters remaining

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Cancel **Next**

Este é o código de texto usado na imagem:

```
{  
"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": "*"   
},  
],  
}
```

Posteriormente, defina o Nome da política e clique em Criar política.

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**

Depois que a diretiva for criada, filtre e selecione a diretiva e clique na opção Anexar no menu suspenso Ações.

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

Search C800

All types 1 match

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

Actions Attach Detach

Uma nova janela está aberta. Na seção Entidades IAM, filtre e selecione a função IAM criada e clique em Anexar política.

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

Search route

All types 1 match

Entity name	Entity type
route-table-change	Roles

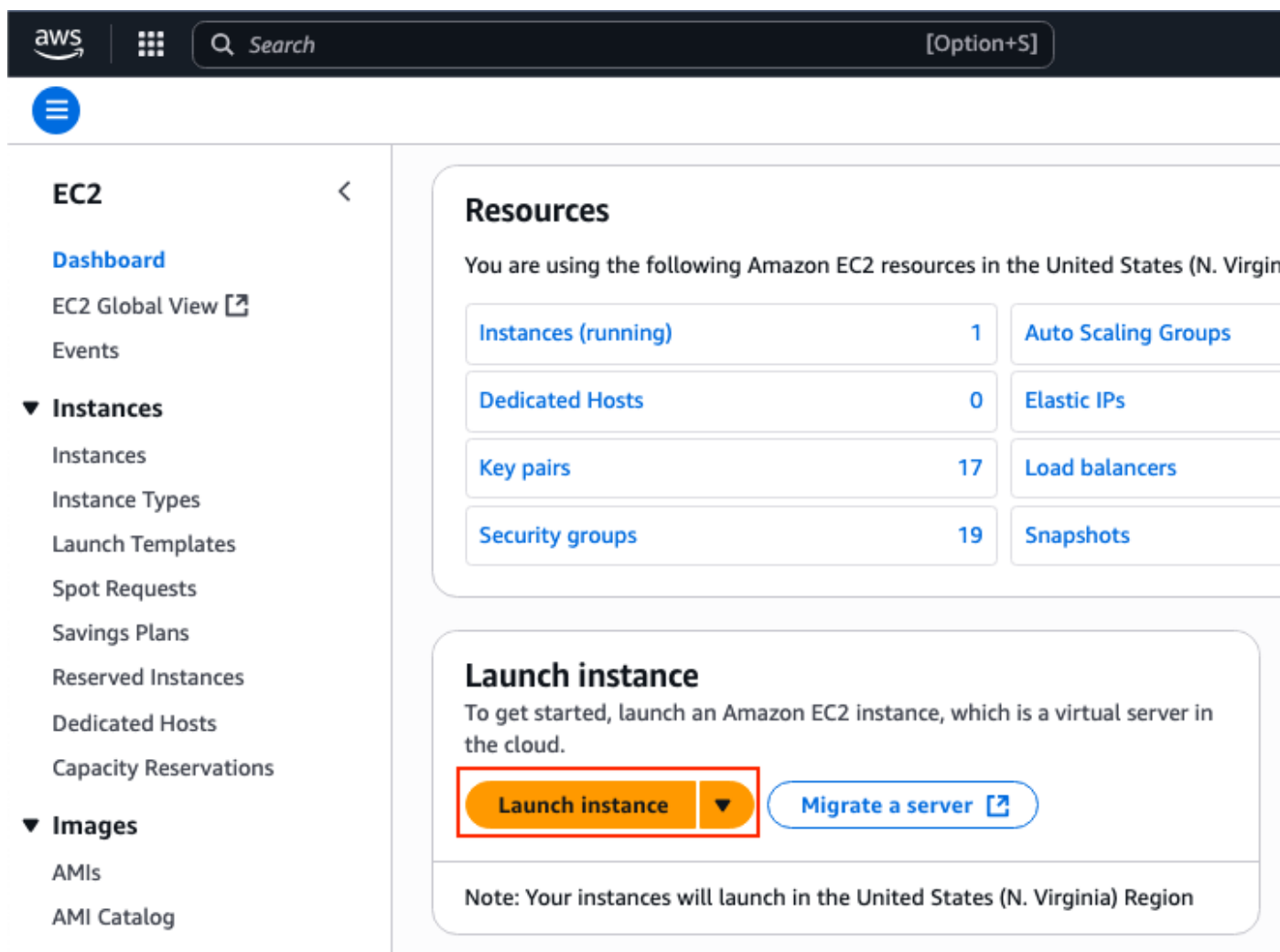
Cancel **Attach policy**

Etapa 6. Configurar e iniciar as instâncias do C8000v

Cada roteador C8000v terá 2 interfaces (1 pública, 1 privada) e será criado em sua própria zona

de disponibilidade.

No Painel EC2, clique em Iniciar instâncias:



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

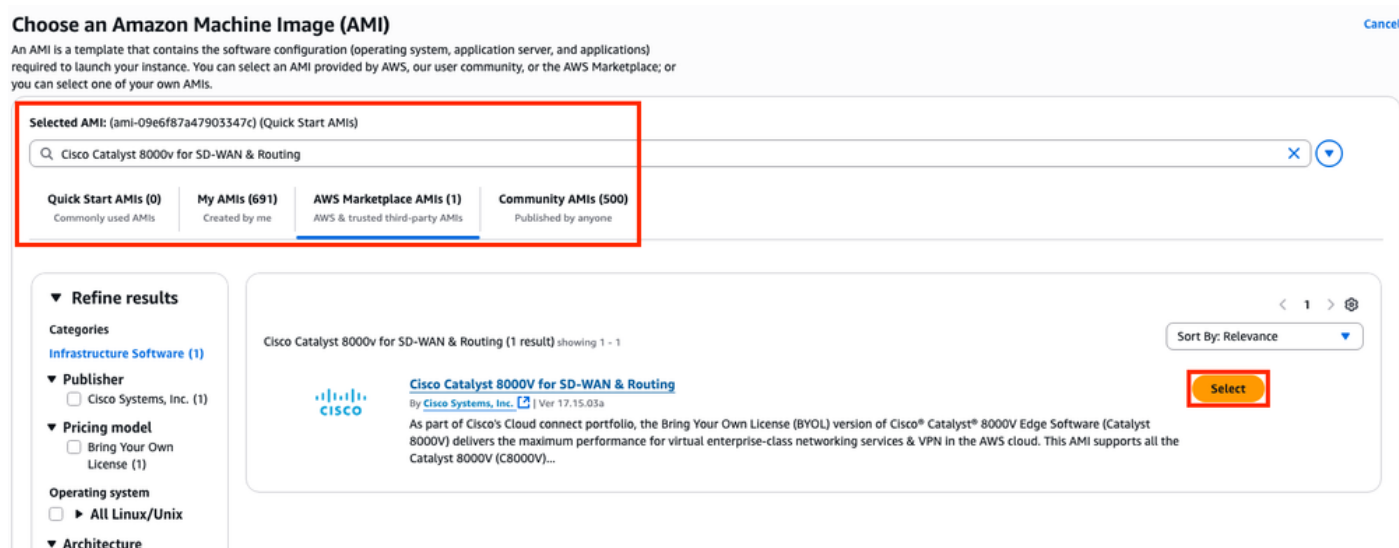
Launch instance

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

Filtre o banco de dados AMI com o nome Cisco Catalyst 8000v para SD-WAN e roteamento. Na lista AWS Marketplace AMIs, clique em Select.



Choose an Amazon Machine Image (AMI)

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)**

Commonly used AMIs Created by me AWS & trusted third-party AMIs Published by anyone

▼ **Refine results**

Categories

[Infrastructure Software \(1\)](#)

▼ **Publisher**

☐ Cisco Systems, Inc. (1)

▼ **Pricing model**

☐ Bring Your Own License (1)

Operating system

☐ All Linux/Unix

▼ **Architecture**

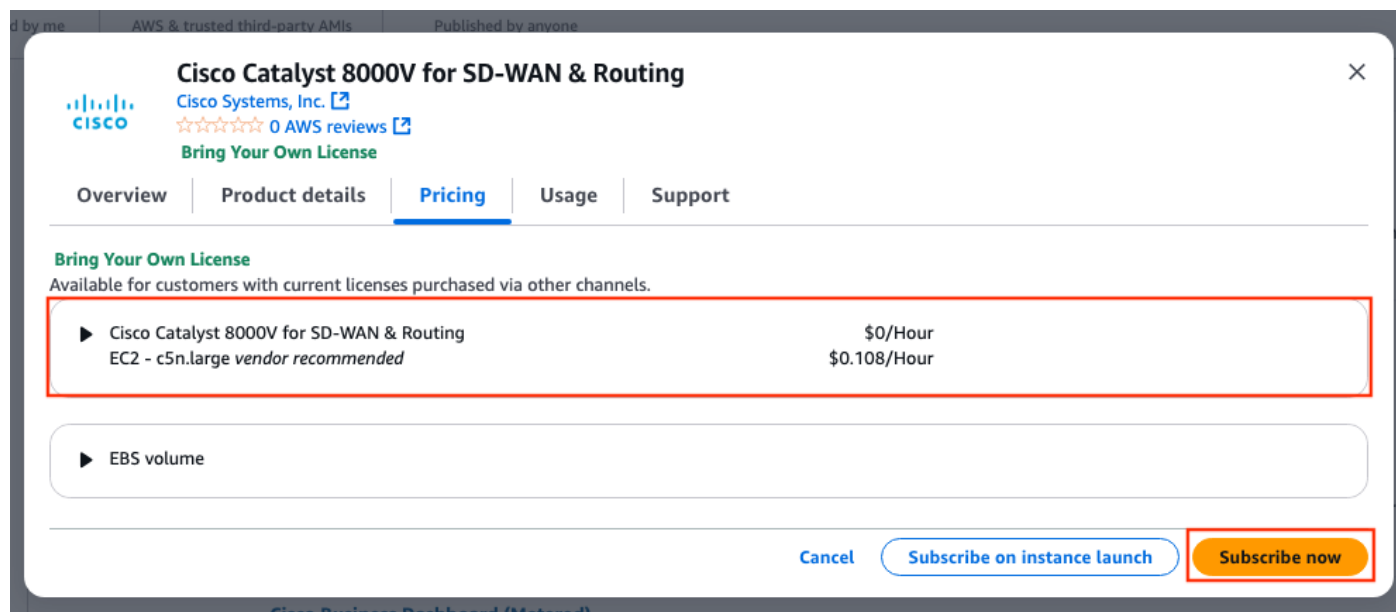
Cisco Catalyst 8000v for SD-WAN & Routing (1 result) showing 1 - 1

Sort By: Relevance

[Select](#)

Selecione o tamanho correspondente para o AMI. Para este exemplo, o tamanho c5n.large é

selecionado. Isso pode depender da capacidade necessária para sua rede. Depois de selecionado, clique em Inscrever-se agora.



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.

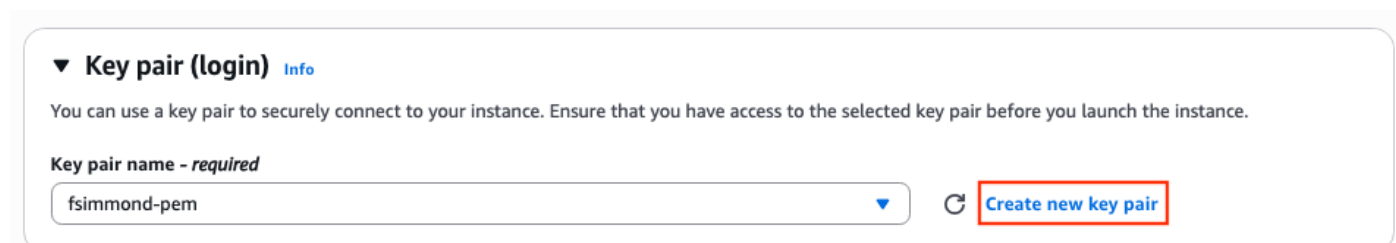
▶ Cisco Catalyst 8000V for SD-WAN & Routing EC2 - c5n.large <i>vendor recommended</i>	\$0/Hour \$0.108/Hour
--	--------------------------

▶ EBS volume

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

Etapa 6.1. Configurar o par de chaves para acesso remoto

Uma vez inscrita na AMI, uma nova janela com várias opções é exibida. Na seção Par de chaves (login), se um par de chaves não estiver presente, clique em Criar novo par de chaves. Você pode reutilizar uma única chave para cada dispositivo criado.



▼ **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](#)

Uma nova janela pop-up será exibida. Para este exemplo, é criado um arquivo de chave .pem com criptografia ED25519. Depois que tudo estiver definido, clique em Criar par de chaves.

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

Etapa 6.2. Criar e Configurar as Sub-Redes para o AMI

Na seção Configurações de rede, clique em Editar. Algumas novas opções dentro da seção já estão disponíveis:

1. Selecione o VPC desejado para este trabalho. Para este exemplo, o VPC chamado HA é selecionado.
2. Na seção Firewall (grupos de segurança), selecione Select existing security group.
3. Depois que a opção 2 for selecionada, a opção Grupos de segurança comuns estará disponível. Filtre e selecione o grupo de segurança desejado. Para este exemplo, o grupo de segurança All traffic HA está selecionado.
4. (Opcional) Se nenhuma sub-rede para esses dispositivos for criada, clique em Criar nova sub-

rede.

▼ 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

Uma nova guia no navegador da Web é aberta, levando-o à seção Criar sub-rede:

1. Selecione o VPC correspondente para esta configuração na lista suspensa.
2. Defina um nome para a nova sub-rede.
3. Defina a Zona de Disponibilidade para esta sub-rede. (Consulte a seção Topologia deste documento para obter mais informações sobre a configuração)
4. Defina o bloco de sub-rede que pertence ao bloco CIDR do VPC.
5. Além disso, todas as sub-redes que serão usadas poderão ser criadas clicando-se na seção Adicionar nova sub-rede e repita as etapas de 2 a 4 para cada sub-rede.
6. Quando terminar, clique em Criar sub-rede. Navegue até a página anterior para continuar com as configurações.

☰ VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID

Choose a VPC to create the subnet in.

vpc-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 or "Name" and a value that you specify.

public-R1-C8000v 2

The name can be up to 256 characters long.

Availability Zone Info

Choose 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

[Add new tag](#)

You can add 49 more tags.

[Remove](#)

[Add new subnet](#) 5

6

[Cancel](#) [Create subnet](#)

Na subseção Subnet da seção Network Settings, clique no ícone Refresh para obter as sub-redes criadas na lista suspensa.

Etapas 6.3. Configurar as interfaces AMI

Na seção Network Settings, expanda a subseção Advanced Network configuration. Estas opções são exibidas:

▼ 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

ENA Express UDP [Info](#)

Select

The selected instance type does not support ENA Express.

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.

Neste menu, defina os parâmetros Description, Primary IP, Delete on termination.

Para o parâmetro Primary IP, use qualquer endereço IP, exceto o primeiro endereço disponível da sub-rede. Isso é usado internamente pela AWS.

O parâmetro Delete on termination neste exemplo está definido como No. No entanto, isso pode ser definido como sim, dependendo do seu ambiente.

Devido a essa topologia, uma segunda interface é necessária para a sub-rede privada. Clique em Add network interface e este prompt será exibido. No entanto, a interface oferece a opção de selecionar a sub-rede desta vez:

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

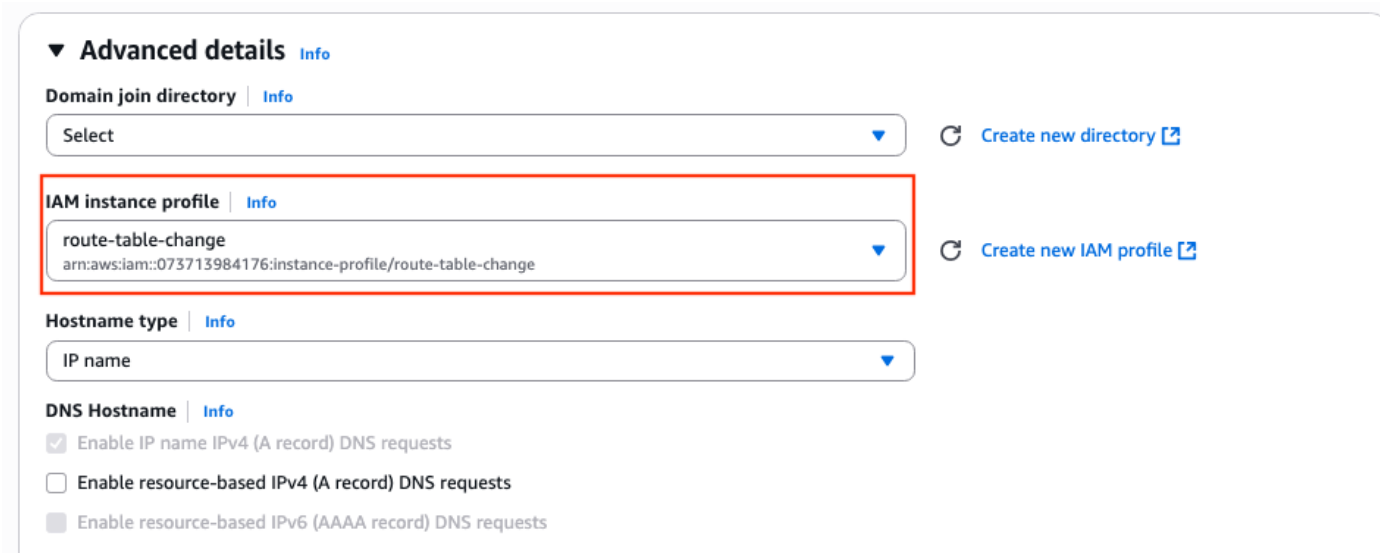
The selected subnet does not support IPv6 IPs.

Remove

Depois que todos os parâmetros estiverem definidos como foi feito na Interface de rede 1, continue com as próximas etapas.

Etapa 6.4. Definir o perfil da instância IAM como AMI

Na seção Detalhes avançados, selecione a função IAM criada no parâmetro perfil da instância IAM:



▼ 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

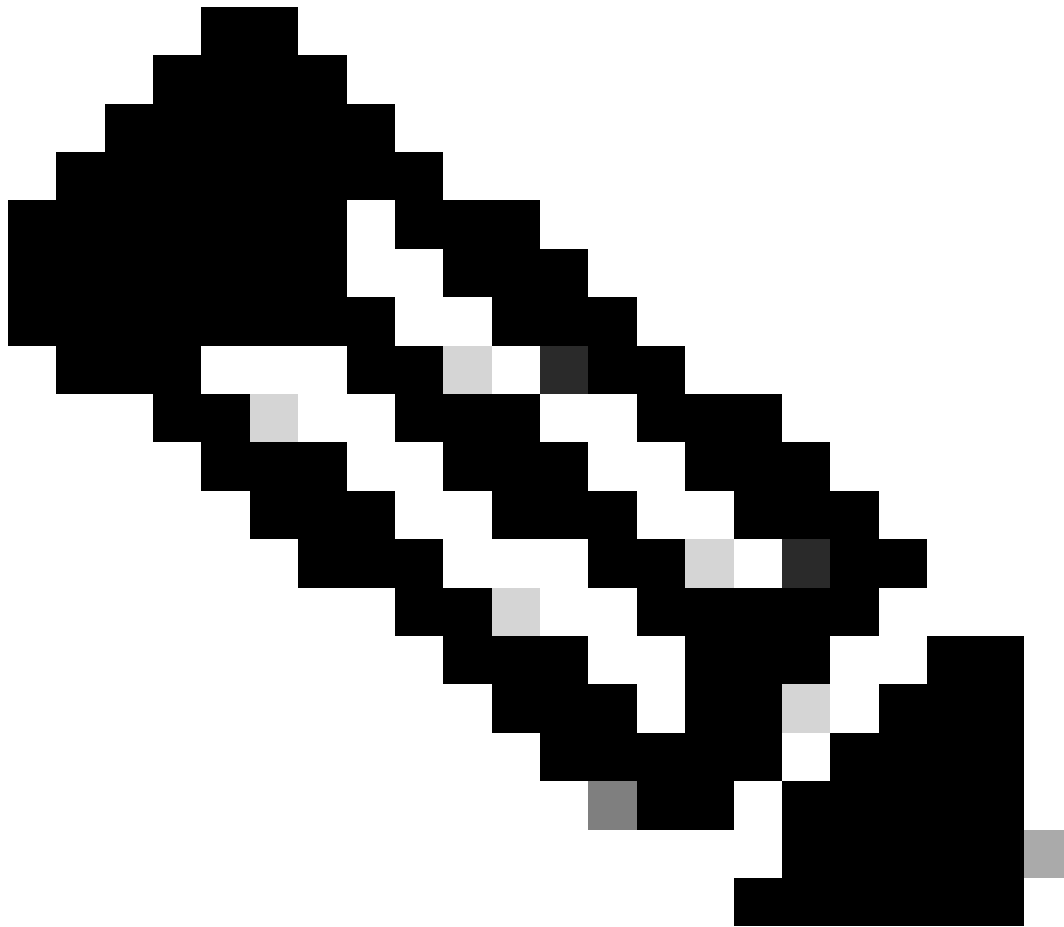
DNS Hostname | [Info](#)

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

Etapa 6.5. (Opcional) Definir as Credenciais no AMI

Na seção Detalhes avançados, navegue até a seção Dados do usuário - opcional e aplique esta configuração para definir um nome de usuário e uma senha enquanto a instância é criada:

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



Note: O nome de usuário fornecido pelo AWS para SSH no C8000v pode estar listado incorretamente como raiz. Altere isso para ec2-user se necessário.

Etapa 6.6. Finalizar a Configuração da Instância

Depois que tudo estiver configurado, clique em Iniciar instância:

▼ 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.



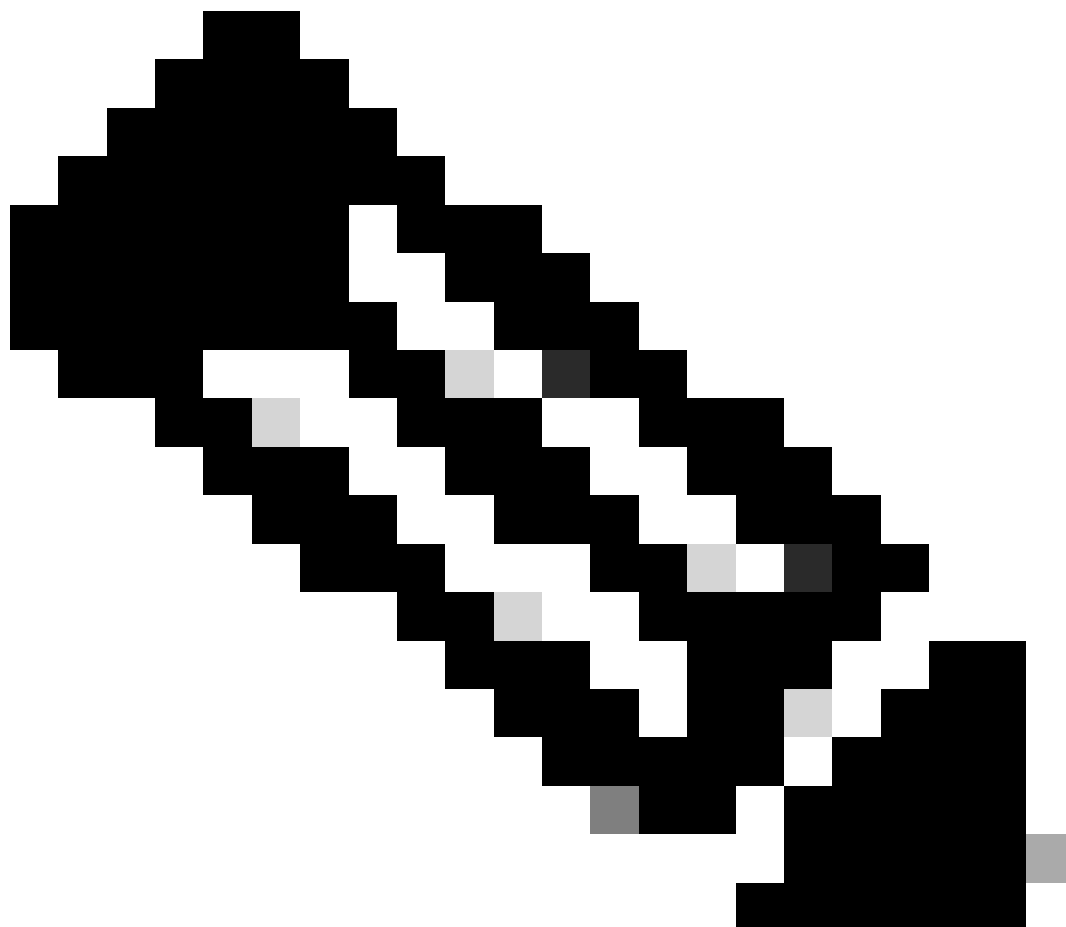
[Cancel](#)

[Launch instance](#)

 [Preview code](#)

Etapa 6.7. Desativar a verificação da origem/destino nos ENI

Depois que a Instância for criada, desabilite a funcionalidade de verificação de src/dst no AWS para obter a conectividade entre interfaces na mesma sub-rede. Na seção EC2 Dashboard > Network & Security > Network interfaces, selecione os ENIs e clique em Actions > Alterar origem/destino. verificar.



Note: Você deve selecionar os ENIs um por um para disponibilizar essa opção.

The screenshot shows the AWS Management Console for the 'Network interfaces' section. On the left, there's a navigation menu with 'EC2' selected. The main area shows a table of network interfaces. The 'eni-0b5484e24f918207b' interface is selected. The 'Actions' dropdown menu is open, and the option 'Change source/dest. check' is highlighted. The table has columns for Name, Network interface ID, Subnet ID, and VPC ID.

	Name	Network interface ID	Subnet ID	VPC ID
☐		eni-0a4940f4ef3f975b1	subnet-0488c4f9198b94fb3	vpc-08cc6365f2
☐	semadrig-dev...	eni-06b5e292bc1ed4dad	subnet-0c978afc3d9f74a7b	vpc-08cc6365f2
☒		eni-0b5484e24f918207b	subnet-0b664f8e74443d28f	vpc-0d30b9fa95
☐		eni-0e3315e5326d6de9	subnet-0a5f13361443951d2	vpc-0d30b9fa95
☐		eni-0d9d8c101cbb1365e	subnet-0c978afc3d9f74a7b	vpc-08cc6365f2
☐		eni-07c10f0c267c73ebe	subnet-080852db285e8dc8c	vpc-0141e83a4
☐		eni-0556463389ff6d244	subnet-0bdacba83894b2c9f	vpc-08cc6365f2

Uma nova janela é exibida. No novo menu, desative a caixa de seleção Enable e clique em Save.

The screenshot shows a modal dialog box titled 'Change source/destination check' for the network interface 'eni-0b5484e24f918207b'. Inside the dialog, there is a checkbox labeled 'Source/destination check' which is currently unchecked. At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Save'. The 'Save' button is highlighted with a red box.

Etapa 6.8. Criar e associar um IP elástico ao ENI público da instância

Na seção EC2 Dashboard > Network & Security > Elastic IPs, clique em Allocate Elastic IP address.

The screenshot shows the AWS Management Console for the 'Elastic IP addresses' section. The 'Actions' dropdown menu is open, and the option 'Allocate Elastic IP address' is highlighted. The page includes a search bar with the placeholder text 'Find elastic IP addresses by attribute or tag'.

A página o conduz à outra seção. Para este exemplo, a opção Amazon pool of IPv4 addresses é selecionada junto com a zona de disponibilidade us-east-1. Uma vez concluída, clique em Allocate.

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](#)

us-east-1

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](#)

Quando o endereço IP for criado, atribua-o à interface pública da instância. Na seção EC2 Dashboard > Network & Security > Elastic IPs, clique em Actions > Associate Elastic IP address.

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

Find elastic IP addresses by attribute or tag

Public IPv4 address [Clear filters](#)

☒	Name	Allocated IPv4 address	Type	Allocation ID	Reverse DNS record	
☒	-	192.168.1.1	Public IP	eipalloc-0948346735ab2017c	-	

Actions [Allocate Elastic IP address](#)

[View details](#)

[Release Elastic IP addresses](#)

[Associate Elastic IP address](#)

[Disassociate Elastic IP address](#)

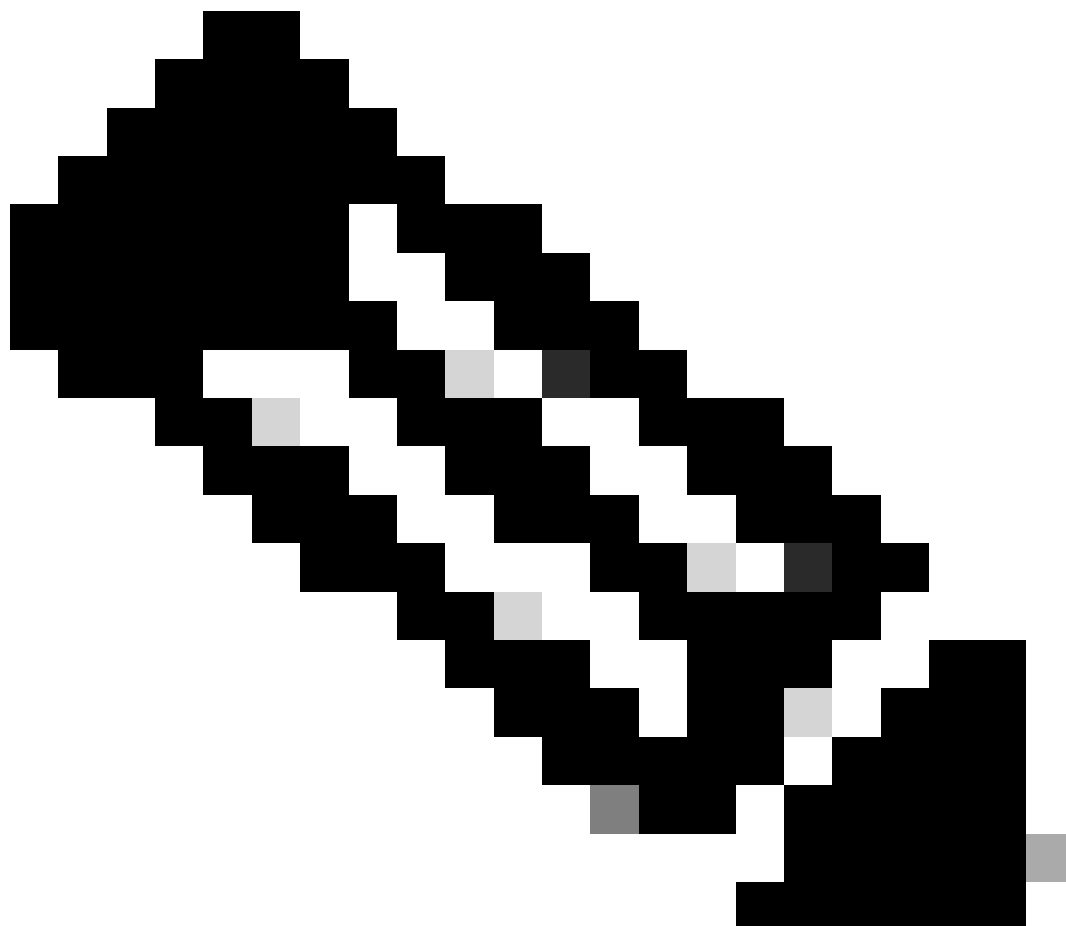
[Update reverse DNS](#)

[Enable transfers](#)

[Disable transfers](#)

[Accept transfers](#)

Nesta nova seção, selecione a opção Network interface e procure o ENI público da interface correspondente. Associe o endereço IP público correspondente e clique em Associate.



Note: Para obter a ID ENI apropriada, navegue para a seção EC2 Dashboard > Instances. Em seguida, selecione a instância e marque a seção Networking. Procure o endereço IP de sua interface pública para obter o valor ENI na mesma linha.

Associate Elastic IP address [Info](#)

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

Elastic IP address: [Add IP address](#)

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
eni-0b5484e24f918207b

Private IP address
The private IP address with which to associate the Elastic IP address.
10.100.10.253

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](#)

Etapa 7. Repita a Etapa 6 para criar a segunda instância do C8000v para HA

Consulte a seção Topologia deste documento para obter as informações correspondentes para cada interface e repita as mesmas etapas de 6.1 a 6.6.

Etapa 8. Repita a Etapa 6 para criar uma VM (Linux/Windows) no AMI Marketplace.

Para este exemplo, o servidor Ubuntu 22.04.5 LTS é selecionado no AMI Marketplace como o host interno.

O ens5 é criado por padrão para a interface pública. Para este exemplo, crie uma segunda interface (ens6 no dispositivo) para a sub-rede privada.

<#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
```

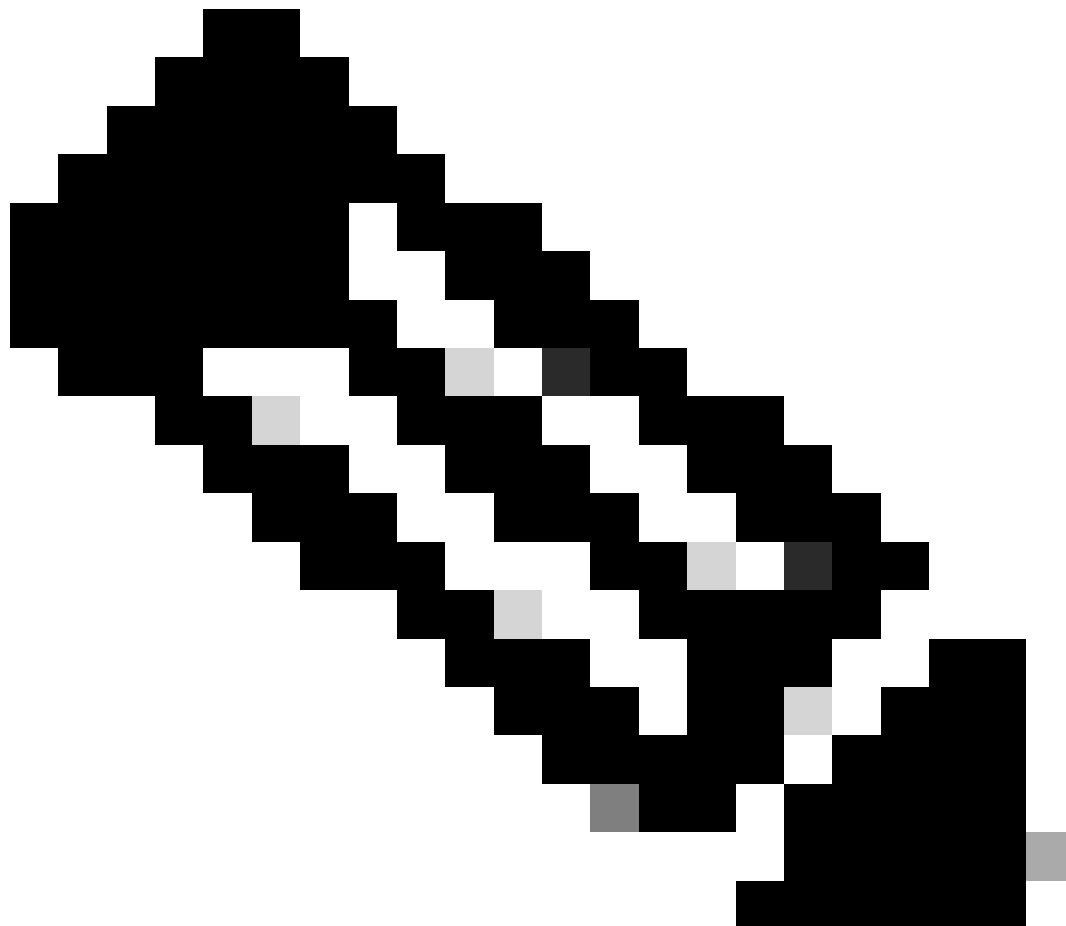
10.100.30.254

```
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

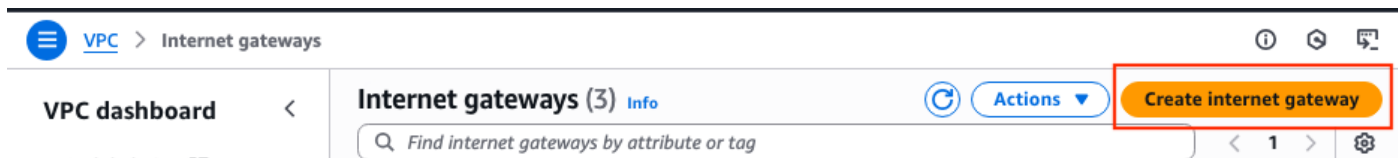
```
netmask 255.255.255.0 broadcast 10.100.130.255
inet6 fe80::3b:7eff:fead:db:e5 prefixlen 64 scopeid 0x20<link>
ether 02:3b:7e:ad:db:e5 txqueuelen 1000 (Ethernet)
RX packets 119 bytes 16831 (16.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 133 bytes 13816 (13.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



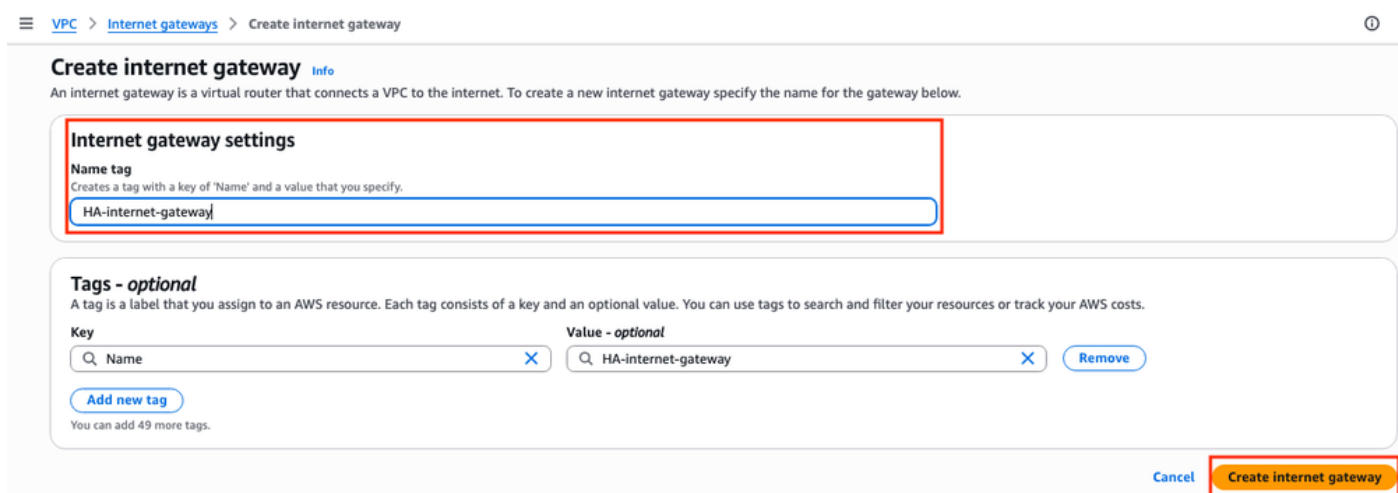
Note: Se for feita alguma alteração nas interfaces, sincronize a interface ou recarregue a VM para aplicar essas alterações.

Etapa 9. Criar e Configurar um Gateway de Internet (IGW) para o VPC

Na seção **VPC Dashboard > Virtual Private Cloud > Internet Gateways**, clique em **Create Internet Gateway**.



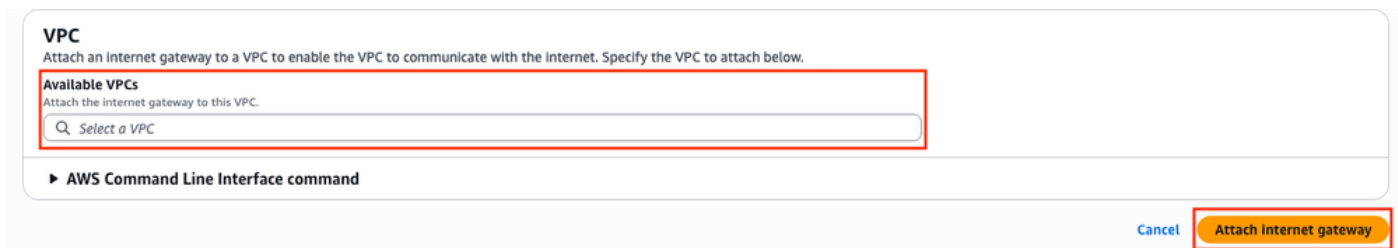
Nesta nova seção, crie uma marca **name** para este gateway e clique em **Create internet gateway**.



Depois que o IGW for criado, anexe-o ao VPC correspondente. Navegue até a seção **VPC Dashboard > Virtual Private Cloud > Internet Gateway** e selecione o IGW correspondente. Clique em **Ações > Anexar ao VPC**.



Nesta nova seção, selecione o VPC chamado **HA**. Para este exemplo, clique em **Anexar gateway de Internet**.



O IGW deve indicar o estado Attached (Anexado) como mostrado:

VPC dashboard < igw-089adf1bccd7bda47 / HA-internet-gateway

Details Info

Internet gateway ID: igw-089adf1bccd7bda47

State: Attached

VPC ID: vpc-0d30b9fa9511f3639 | HA

Owner: 073713984176

Tags

Search tags

Key	Value
Name	HA-internet-gateway

Etapa 10. Criar e Configurar Tabelas de Rotas no AWS para sub-redes Públicas e Privadas

Etapa 10.1. Criar e configurar a tabela de rotas públicas

Para estabelecer o HA nessa topologia, associe todas as sub-redes públicas e privadas em suas tabelas de rota correspondentes. Na seção VPC Dashboard > Virtual Private Cloud > Route tables, clique em Create route table.

Route tables (6) Info

Last updated 2 minutes ago

Actions

Create route table

Find route tables by attribute or tag

Name	Route table ID	Explicit subnet associ...	Edge associations	Main
------	----------------	---------------------------	-------------------	------

Na nova seção, selecione o VPC correspondente para esta topologia. Depois de selecionado, clique em Create route table.

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

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

Public-Routes

VPC

The VPC to use for this route table.

vpc-0d30b9fa9511f3639 (HA)

Tags

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

Name

Value - optional

Public-Routes

Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

Na seção Tabelas de rota, selecione a tabela criada e clique em Ações > Editar associações de sub-rede.

VPC > Route tables

Route tables (1/1) Info

Find route tables by attribute or tag

public-routes X Clear filters

Public-Routes rtb-0d0e48f25c9b00635 3 subnets

Actions

- View details
- Set main route table
- Edit subnet associations
- Edit edge associations
- Edit route propagation
- Edit routes
- Manage tags
- Delete route table

Em seguida, selecione as sub-redes correspondentes e clique em Salvar associações.

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (3/6)

Filter subnet associations

public X 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 X subnet-04fb9de939e3778bb / Public-VM-linux-1c - fsmmond X subnet-02d8108842f9f3129 / public-R2-C8000v X

Cancel Save associations

Quando as sub-redes estiverem associadas, clique no hiperlink ID da tabela de rotas para adicionar as rotas apropriadas para a tabela. Em seguida, clique em Edit Routes:

Route tables (1/1) Info

Find route tables by attribute or tag

public-routes X Clear filters

Name	Route table ID
Public-Routes	rtb-0d0e48f25c9b00635

Para obter acesso à Internet, clique em Add route e vincule essa rota pública tabela com a IGW criada na Etapa 9 com esses parâmetros. Depois de selecionado, clique em Salvar alterações:

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](#)

Etapa 10.2. Criar e Configurar a Tabela de Rotas Privadas

Agora que a tabela de rotas públicas foi criada, replique as Etapas 10 para a rota privada e as sub-redes privadas, com exceção da adição do gateway de Internet em suas rotas. Para este exemplo, a tabela de roteamento se parece com isso, já que o tráfego para 8.8.8.8 deve passar pela sub-rede privada neste exemplo:

Edit routes

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

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

Etapa 11. Verificar e configurar a configuração básica da rede, a conversão de endereços de rede (NAT), o túnel GRE com BFD e o protocolo de roteamento

Depois que as Instâncias e sua configuração de roteamento no AWS estiverem preparadas, configure os dispositivos:

Configuração do C8000v R1:

```
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

```

Configuração do C8000v R2:

```

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

```

Etapa 12. Configurar a alta disponibilidade (Cisco IOS® XE Denali 16.3.1a ou posterior)

Agora que a redundância e a conexão entre as VMs estão definidas, defina as configurações de HA para definir as alterações de roteamento. Defina os valores Route-table-id, Network-interface-id e CIDR que devem ser definidos após um erro AWS HA, como BFD peer down.

```
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>
```

O parâmetro `bfd peer` está relacionado ao endereço IP do par de túnel. Isso pode ser verificado usando a saída de `show bfd neighbor`:

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

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

O parâmetro `route-table` está relacionado à ID da tabela de rota privada localizada na seção VPC Dashboard > Virtual Private Cloud > Route Tables. Copie a ID da tabela de rota correspondente.

Route tables (2) [Info](#)

Find route tables by attribute or tag

Routes × Clear filters

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

O parâmetro `cidr ip` está relacionado com o prefixo de rota adicionado na tabela de rota privada (rotas criadas na Etapa 10.2):

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

O parâmetro eni está relacionado com a ID ENI da interface privada correspondente da Instância que está sendo configurada. Para este exemplo, o ID ENI da interface GigabitEthernet2 da instância é usado:

Instances (1/3) Info

Last updated 1 minute ago

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

All states

fsimmond

Clear filters

< 1 >

	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)

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

VPC ID vpc-0d30b9fa9511f3639 (HA)

Subnet ID subnet-0b664f8e74443d28f (public-R1-C8000v)

Availability zone us-east-1a

Outpost ID -

IP addresses Info

Hostname and DNS Info

Network Interfaces (2) Info

Filter network interfaces

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

O parâmetro region está relacionado ao nome de código encontrado na documentação do AWS para a região onde o VPC está localizado. Para este exemplo, a região us-east-1 é usada.

No entanto, essa lista pode mudar ou crescer. Para encontrar as atualizações mais recentes, visite o documento [AmazonRegion and AvailabilityZones](#).

Levando todas essas informações em consideração, aqui está o exemplo de configuração para cada roteador no VPC:

Exemplo de configuração para C8000v R1:

```
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
```

Exemplo de configuração para C8000v R2:

```
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
```

Verificação

1. Verifique o status da instância do C8000v R1. Confirme se a redundância de Túnel e Nuvem está ativa e em execução.

```
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 HoId Uptime SRTT RT0 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. Execute um ping contínuo para 8.8.8.8 a partir da VM do Host que está atrás dos roteadores. Certifique-se de que o ping esteja passando pela interface privada:

```
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. Abra o AWS WebGUI e verifique o status da tabela de roteamento. O ENI atual pertence à interface privada da instância de R1:

rtb-093df10a4de426eb8 / Private-Routes

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (2)		Both	Edit routes
Destination	Target		
8.8.8.8/32	eni-070e14fbfde0d8e3b		
10.100.0.0/16	local		

4. Dispare a alteração de rota desligando a interface Tunnel1 na Instância R1 para simular um evento de failover de HA:

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

5. Verifique novamente na tabela route em AWS, o ID ENI foi alterado para o ID ENI da interface privada do R2:

Routes (2)

Destination



Target

8.8.8.8/32

[eni-0239fda341b4d7e41](#)

10.100.0.0/16

local

Troubleshooting

Estes são os pontos mais comuns que geralmente são esquecidos/configurados incorretamente durante a recriação da implantação:

- Verifique se os recursos estão associados. Ao criar VPC, Sub-redes, Interfaces, Tabelas de Rotas e assim por diante, muitos deles não são associados uns aos outros automaticamente. Eles não têm conhecimento um do outro.
- Certifique-se de que o IP elástico e qualquer IP privado estejam associados às interfaces corretas, com as sub-redes corretas, adicionadas à tabela de rotas correta, conectadas ao roteador correto e ao VPC e zona corretos, vinculados à função IAM e aos grupos de segurança.
- Desabilitar verificação de Origem/Destino por ENI.
Caso você já tenha verificado todos os pontos discutidos nesta seção e o problema ainda esteja presente, reúna essas saídas, teste o failover de HA, se possível, e abra um caso no Cisco TAC:

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.