Implante a configuração de alta disponibilidade do C8000v no AWS

Contents

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:

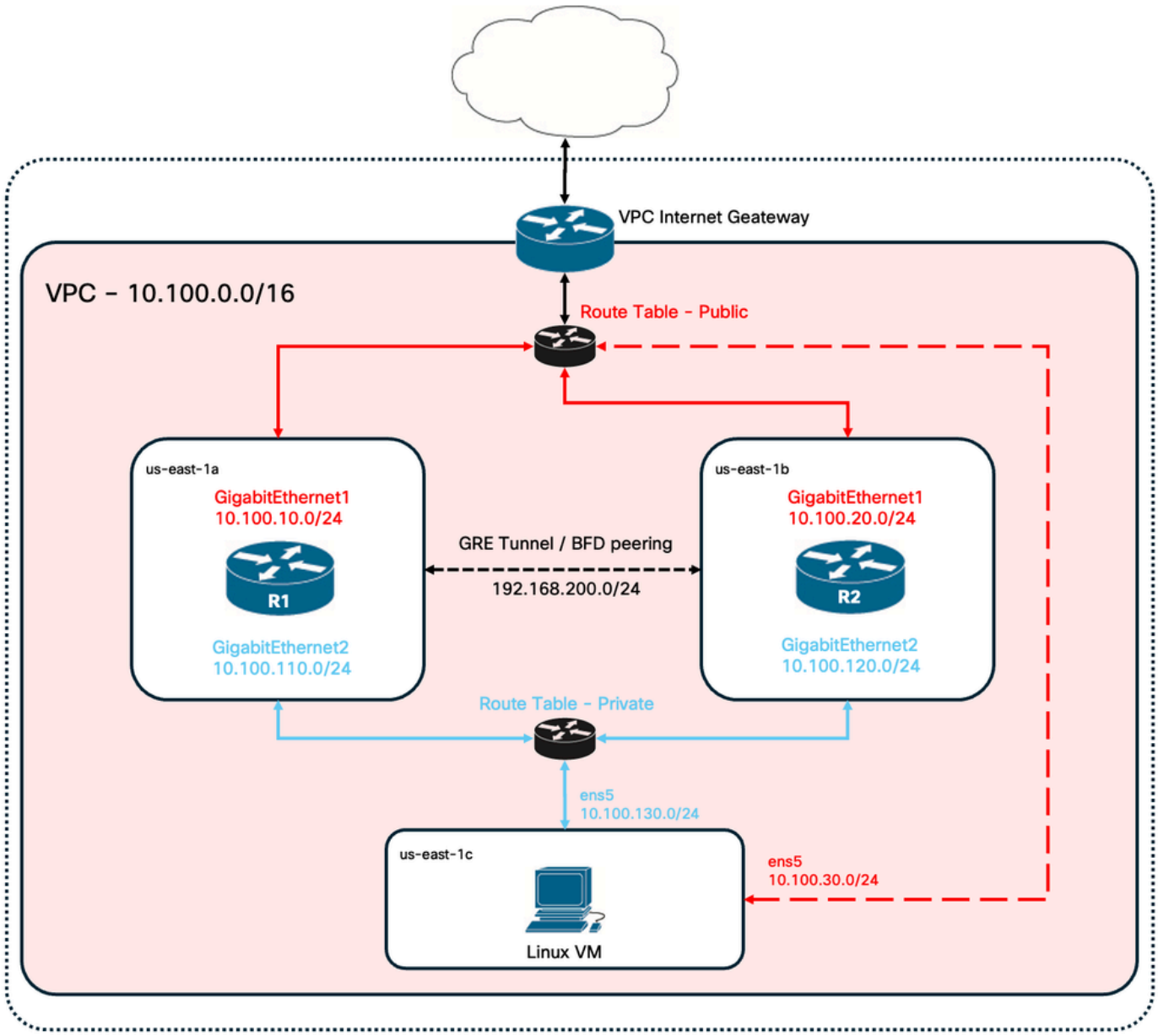
- 1x - Região
- 1x - VPC
- 3x - Zonas de disponibilidade
- 6x - Interfaces/sub-redes de rede (3x pública/3x privada)
- 2x - Tabelas de rota (pública e privada)
- 2x - Roteadores C8000v (Cisco IOS® XEDenali 17.15.3a)
- 1x - VM (Linux/Windows)

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.

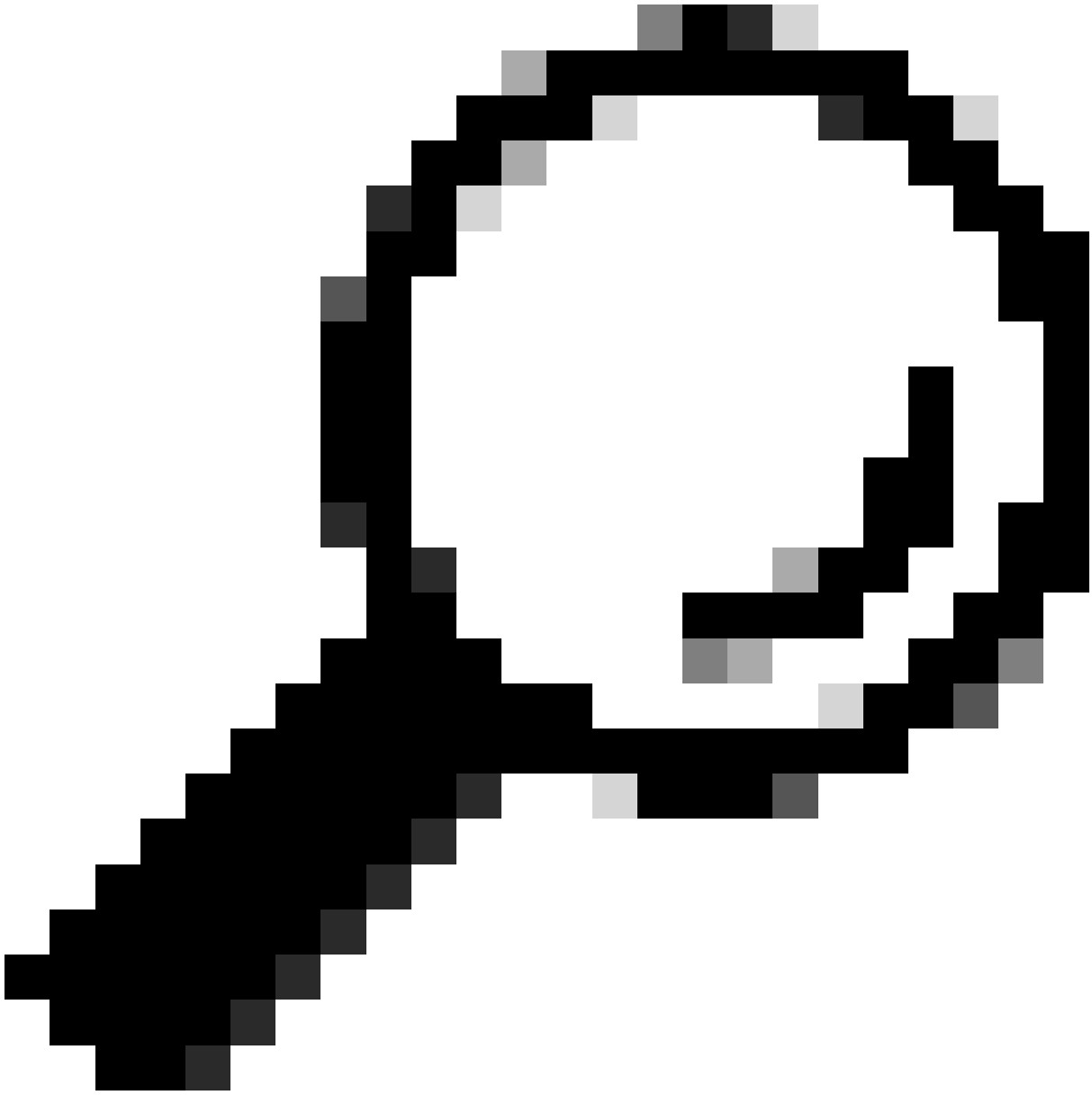
Para simular o tráfego, inicie um ping a partir da interface privada da máquina virtual, atravessando a tabela de rota privada através de R1 para alcançar 8.8.8.8. No caso de um failover, verifique se a tabela de rota privada foi atualizada automaticamente para rotear o tráfego através da interface privada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

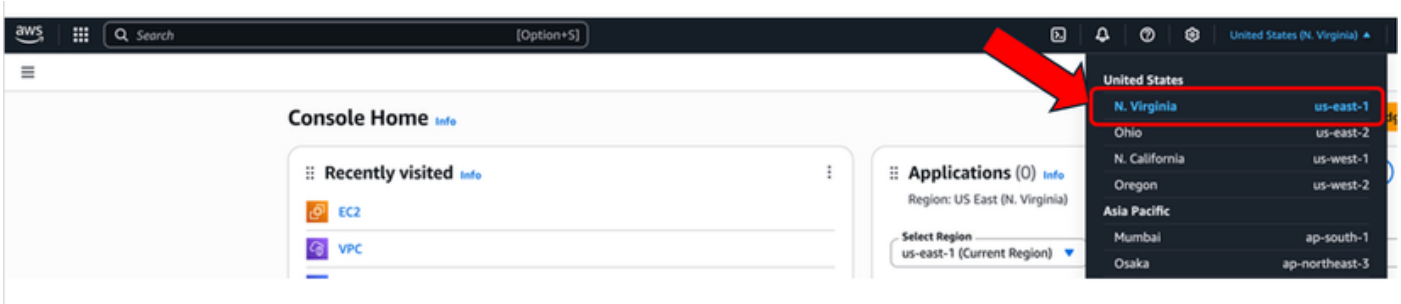
- Em qualquer sub-rede criada, não use o primeiro endereço disponível dessa sub-rede. Esses endereços IP são usados internamente pelos serviços AWS.
- Não configure as interfaces públicas dos dispositivos C8000v dentro de um VRF. O HA não funcionará corretamente se isso estiver definido.

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.

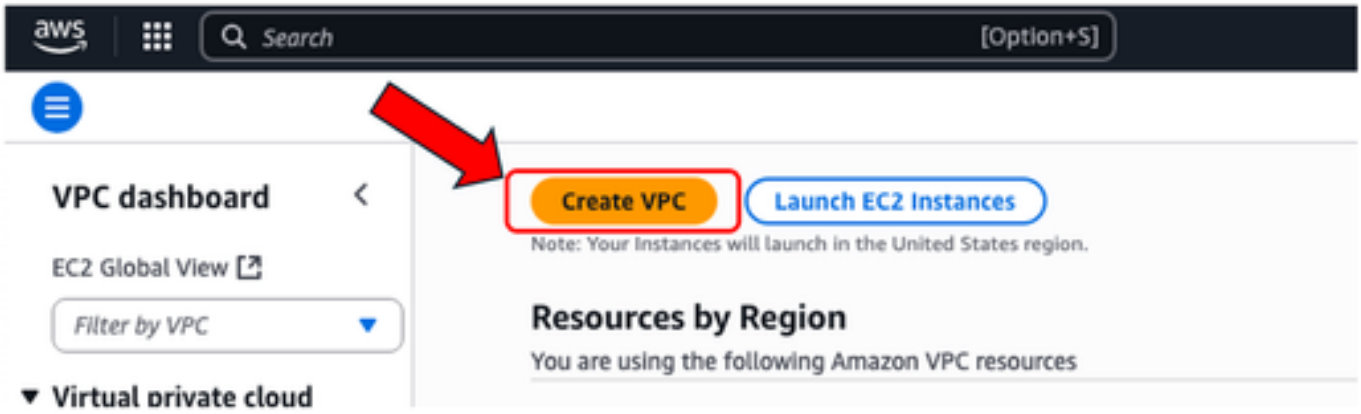
Etapa 1. Selecionar uma Região

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



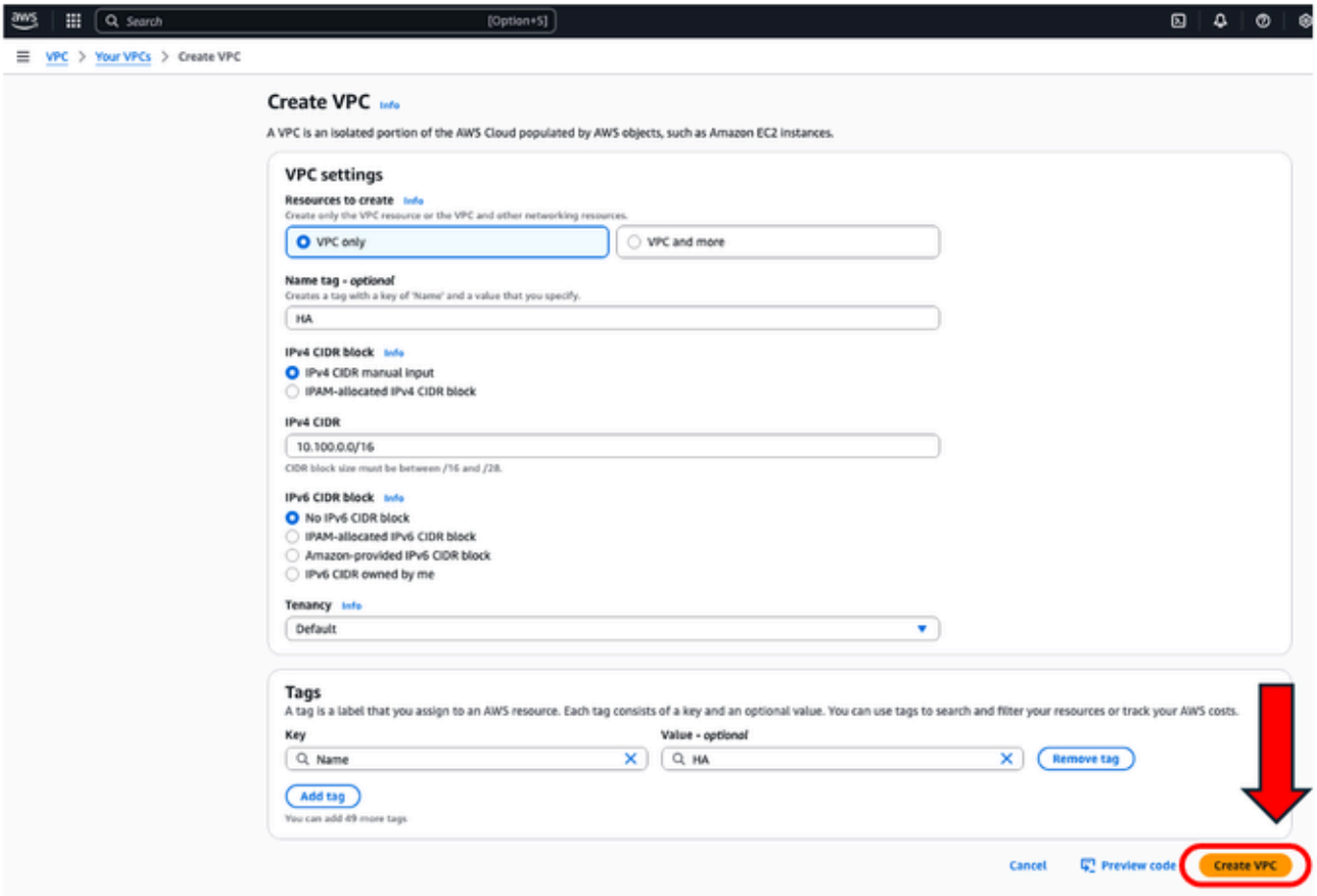
Etapa 2. Criar o VPC

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

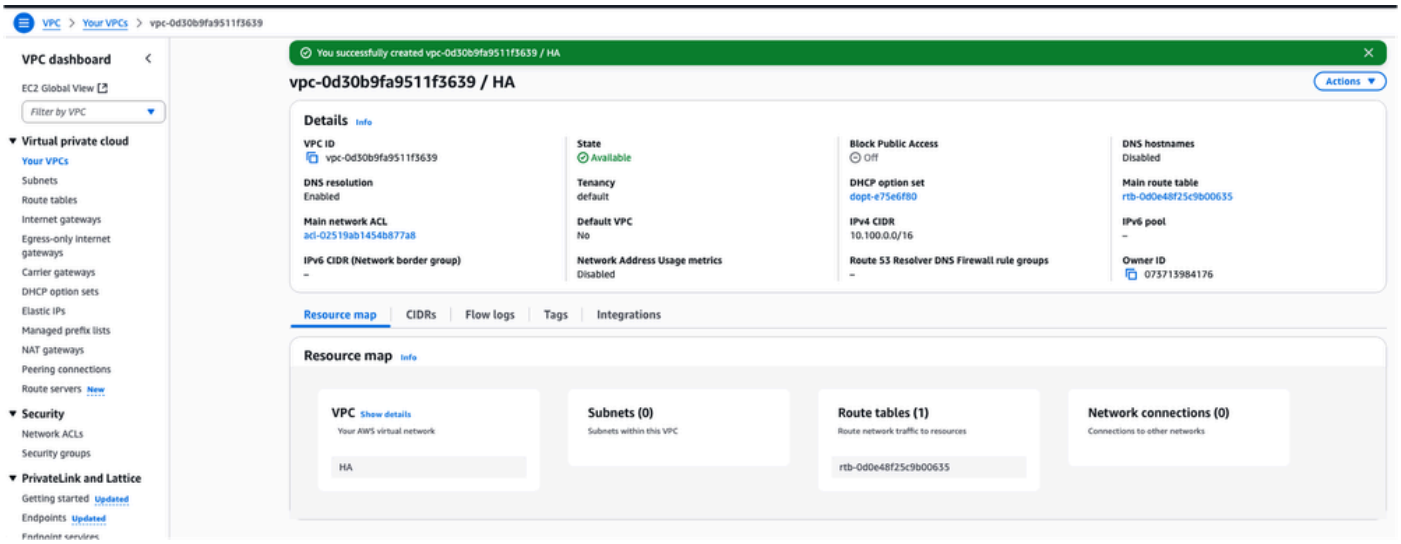


Ao criar o VPC, selecione a opção VPC only. Você pode atribuir uma rede /16 para usar como desejar.

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

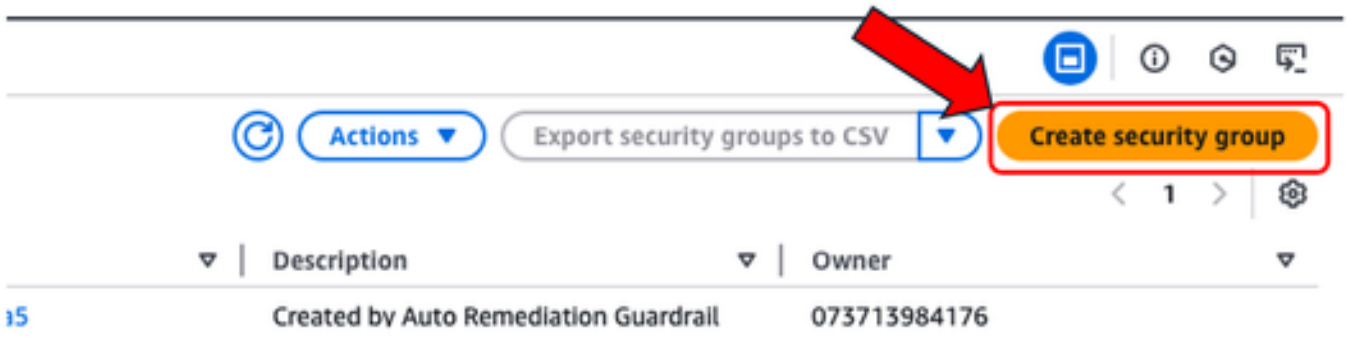


Após clicar em Create VPC, a marca VPC-0d30b9fa9511f3639 com HA é agora criada:

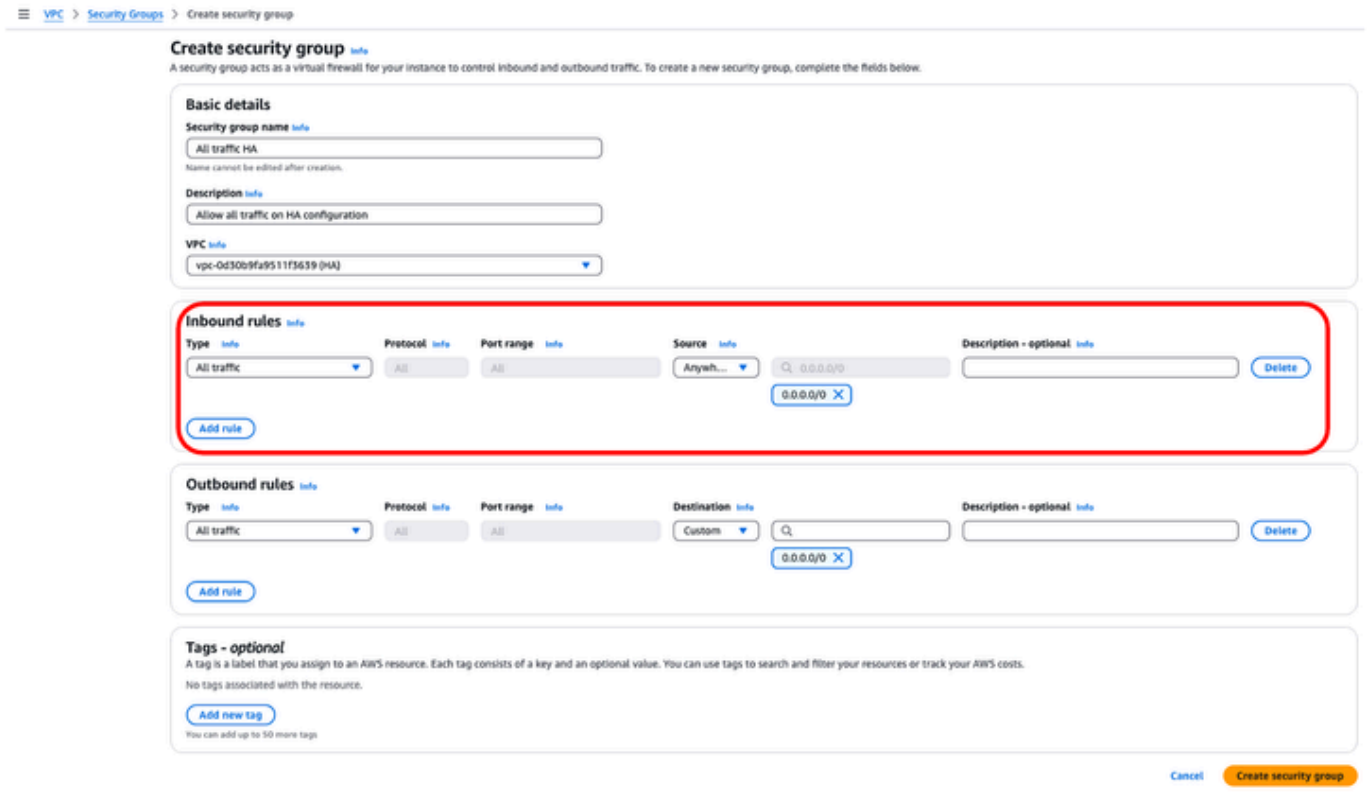


Etapa 3. Criar um Grupo de Segurança para o VPC

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.



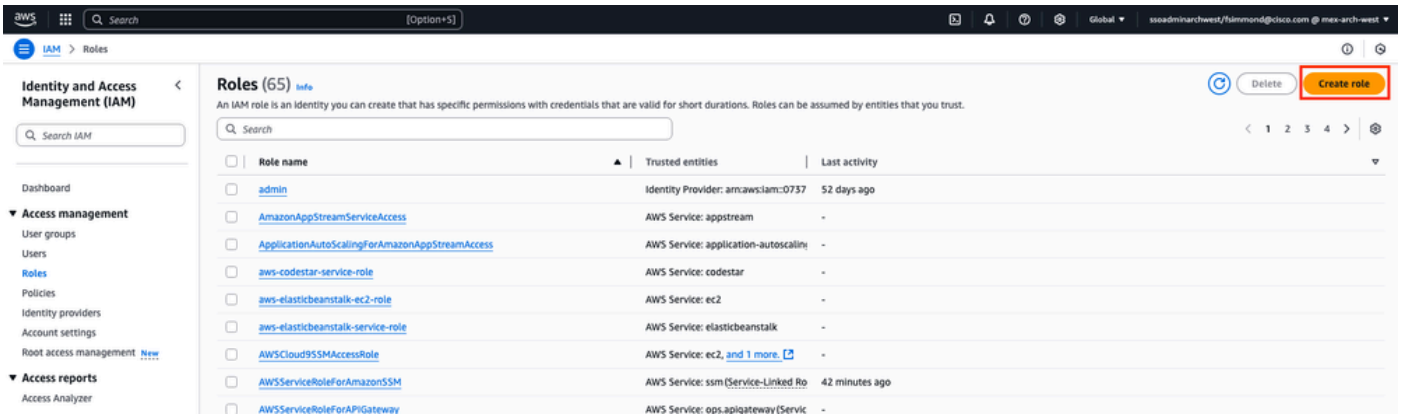
Em Inbound Rules (Regras de entrada), defina o tráfego que você deseja permitir. Para este exemplo, Todo o tráfego é selecionado usando a rede 0.0.0.0/0.



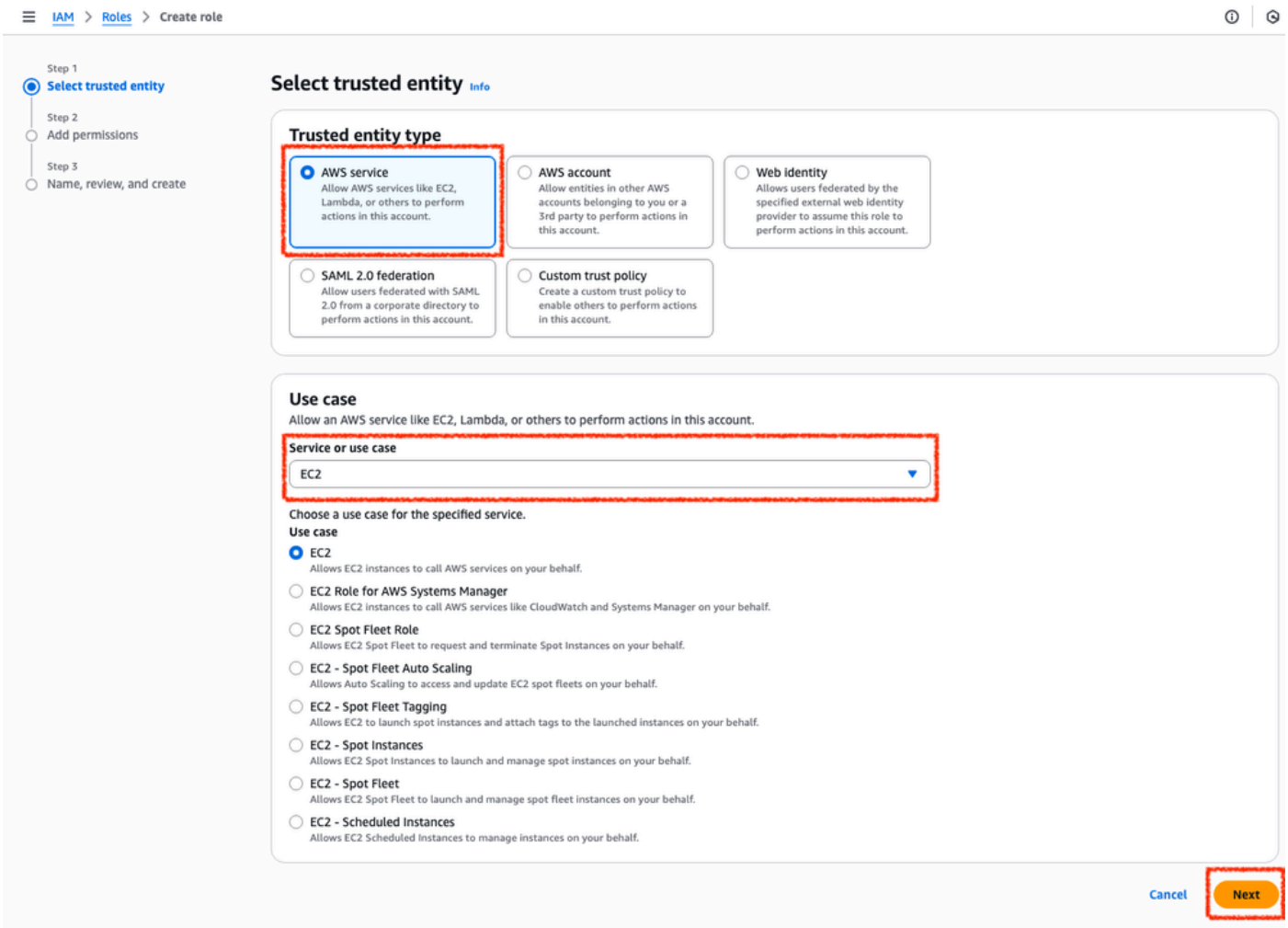
Etapa 4. Criar uma Função IAM com uma Política e Associar ao VPC

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.

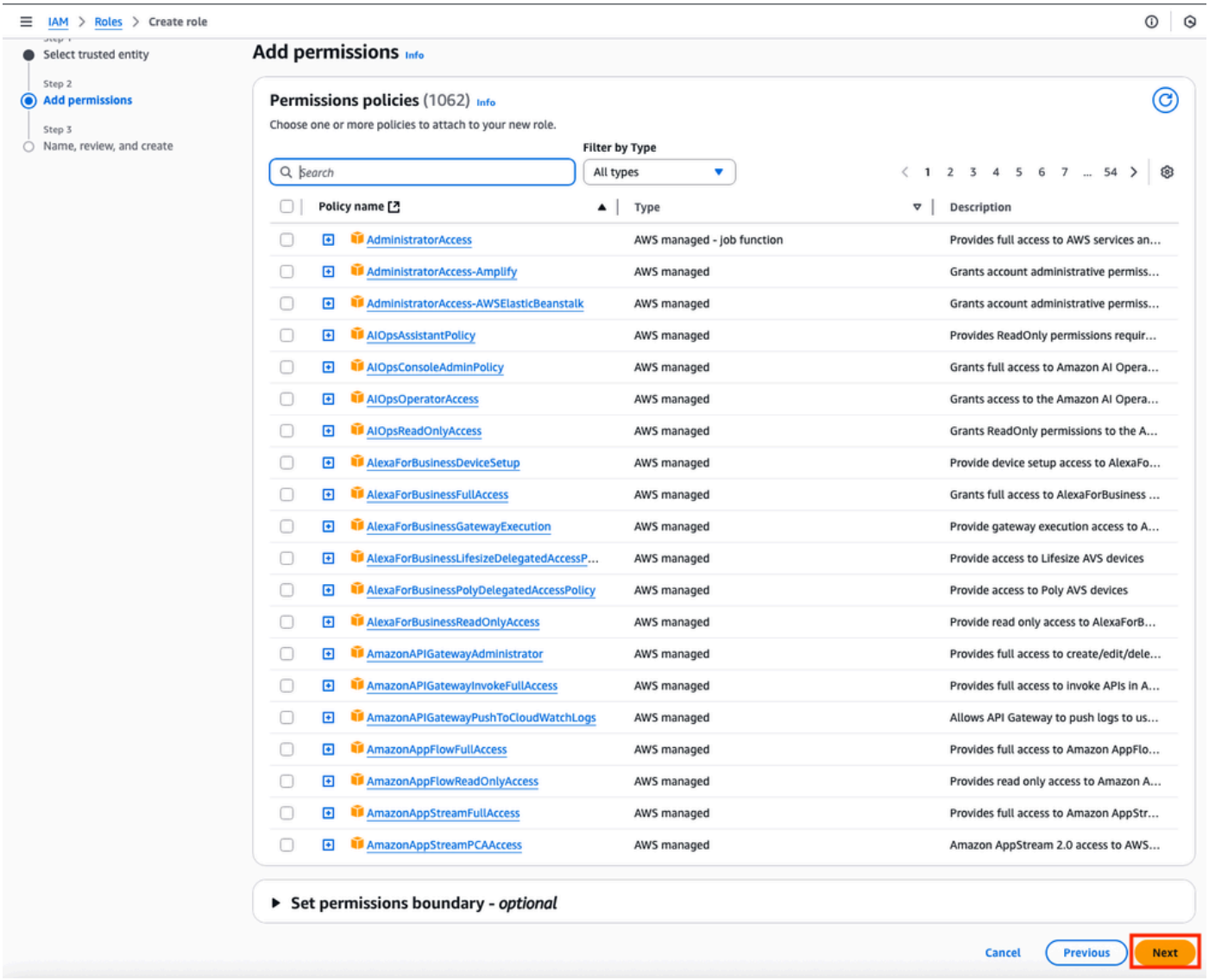
Navegue até o painel IAM e vá até Gerenciamento de acesso > Funções > Criar função. Esse processo consiste em 3 etapas:



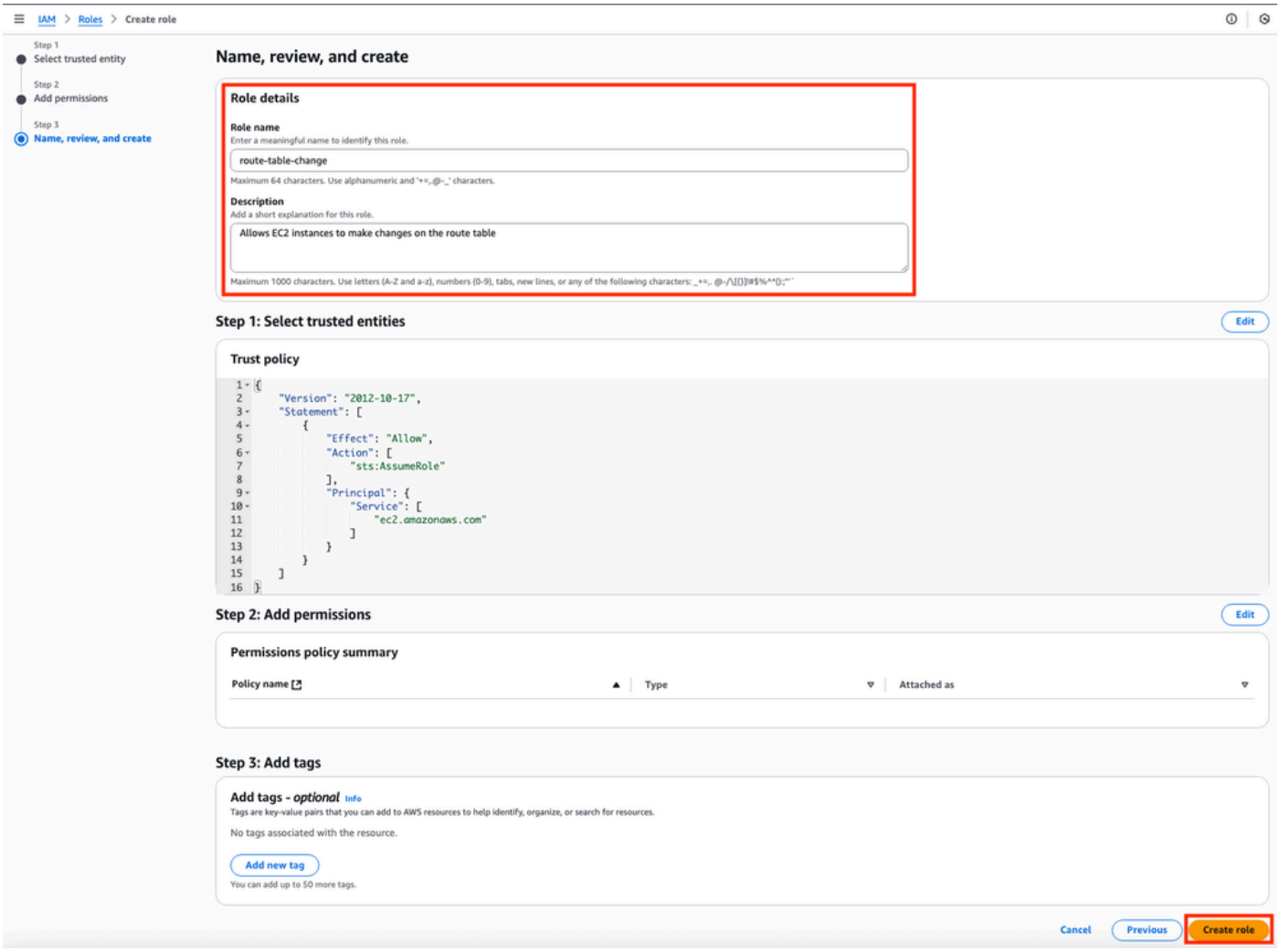
Primeiro, selecione a opção AWS Service na seção Tipo de entidade confiável e EC2 como o serviço atribuído para esta política.



Ao terminar, clique em Avançar:

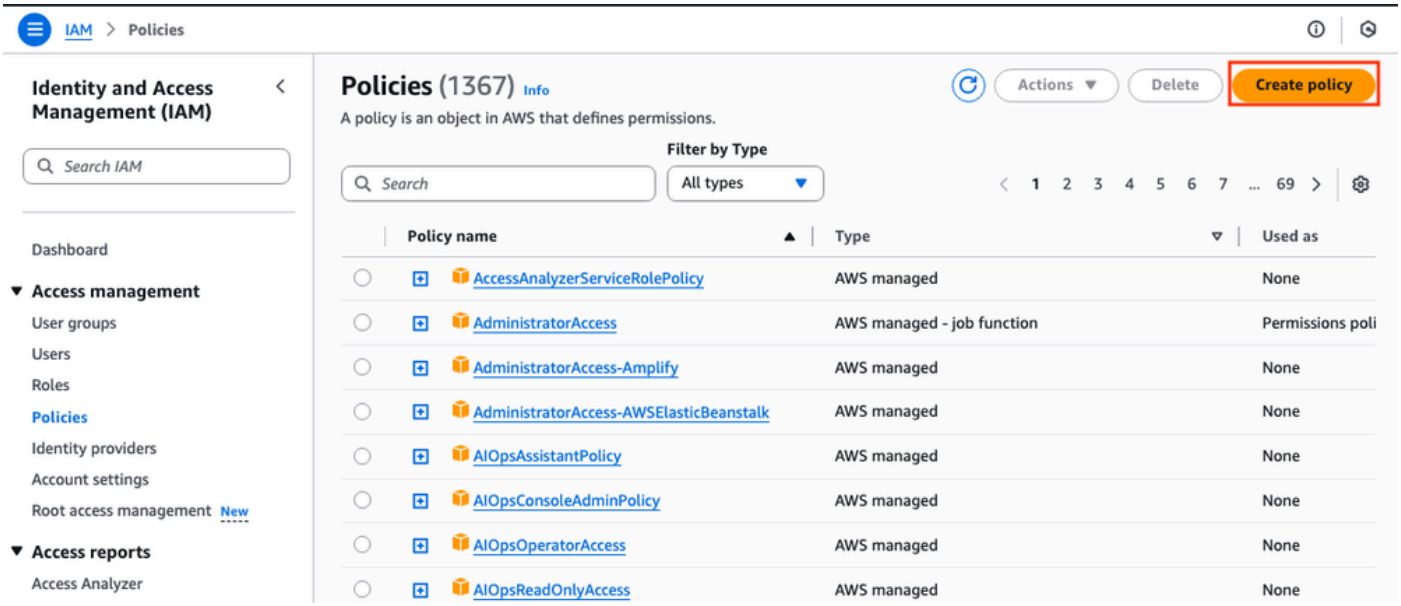


Por fim, defina o Nome da função e clique no botão Criar função.

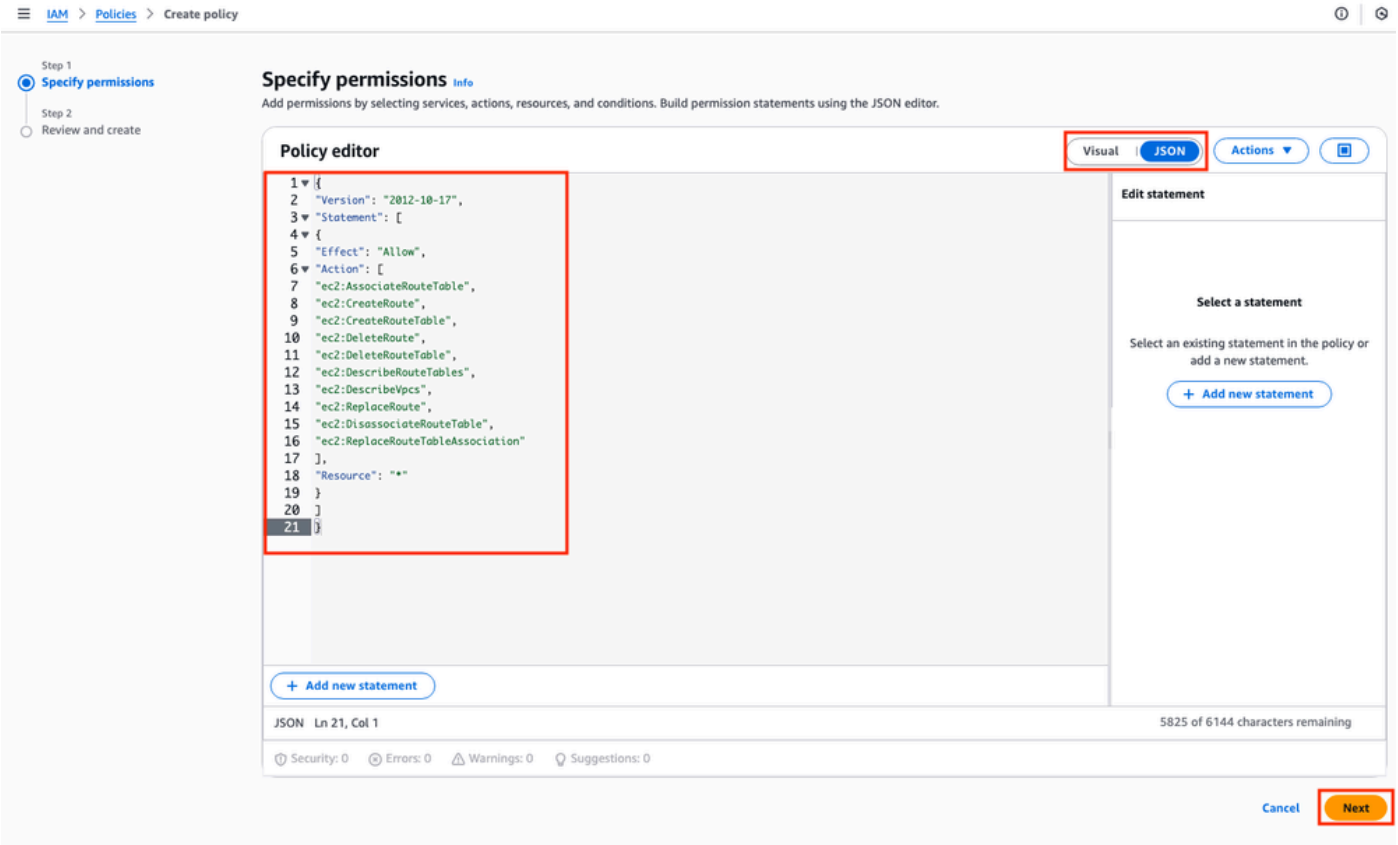


Etapa 5. Criar e Anexar uma Diretiva de Confiança a uma Função do IAM

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:



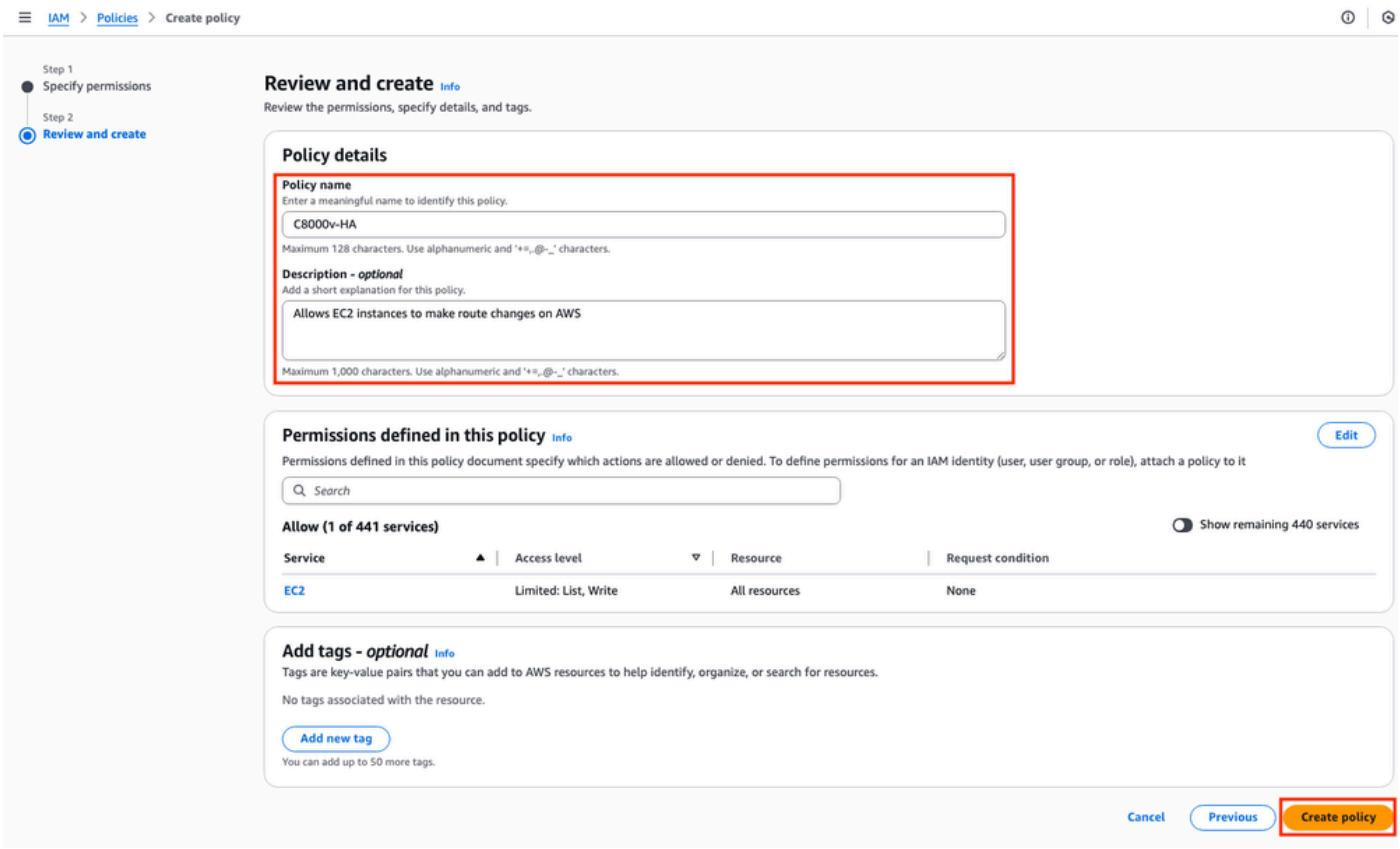
Primeiro, certifique-se de que o editor de políticas esteja usando JSON e aplique os comandos mostrados abaixo. Depois de configurada, clique em Avançar:



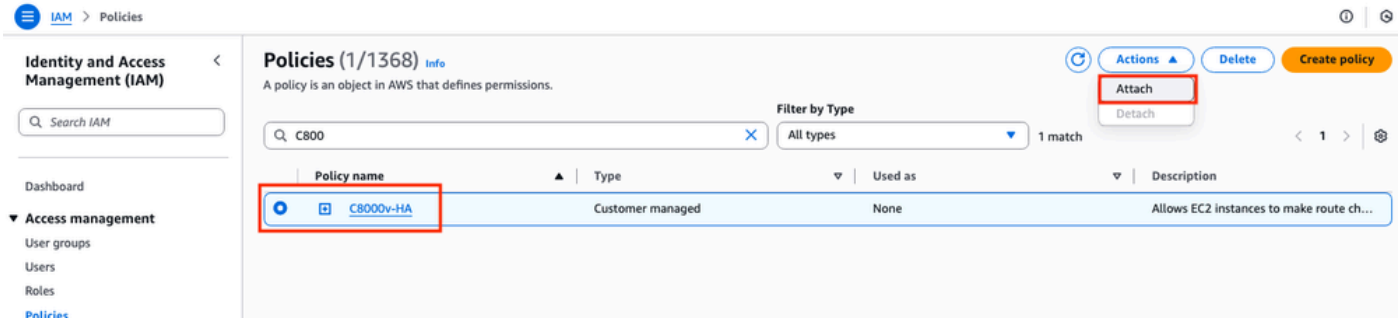
Este é o código de texto usado na imagem:

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

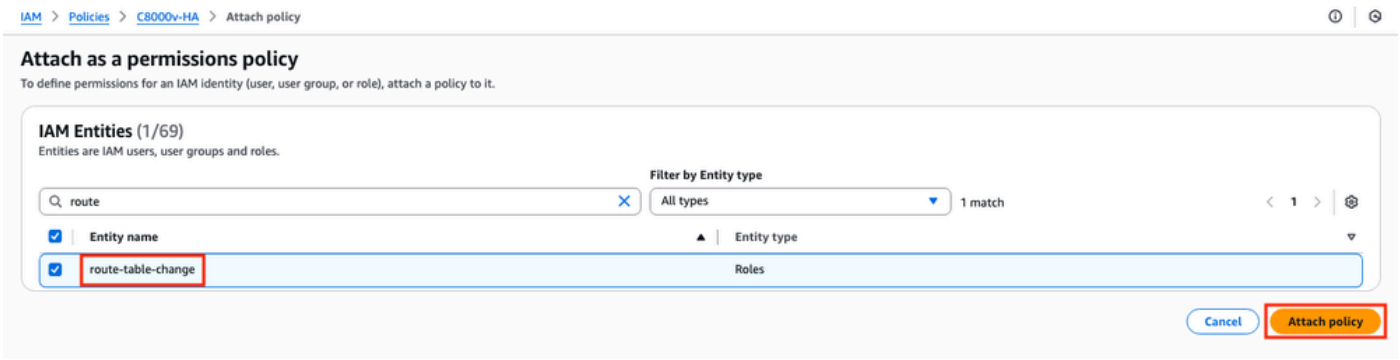
Posteriormente, defina o Nome da política e clique em Criar política.



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



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

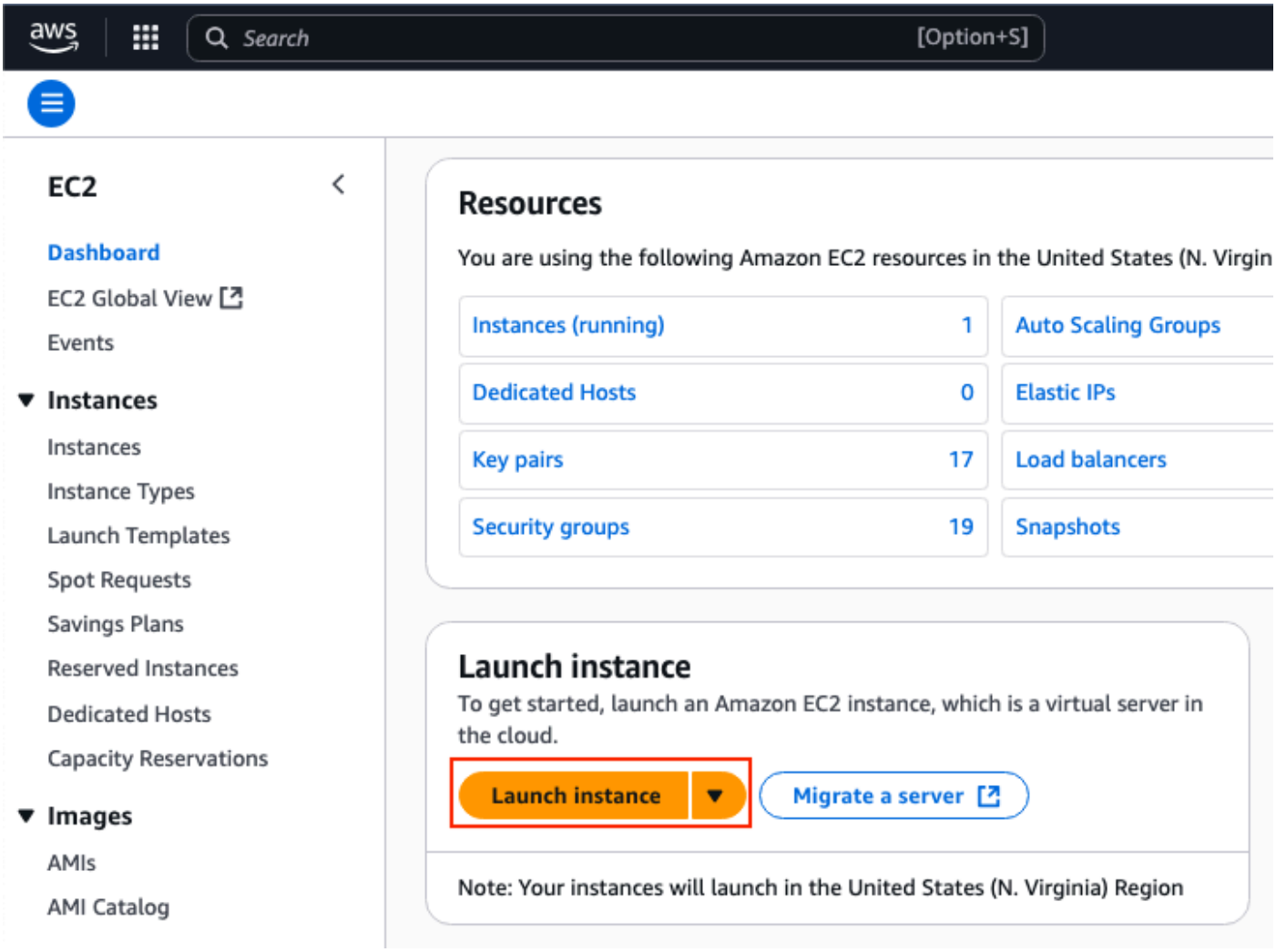


Etapa 6.Configurar e iniciar as instâncias do C8000v

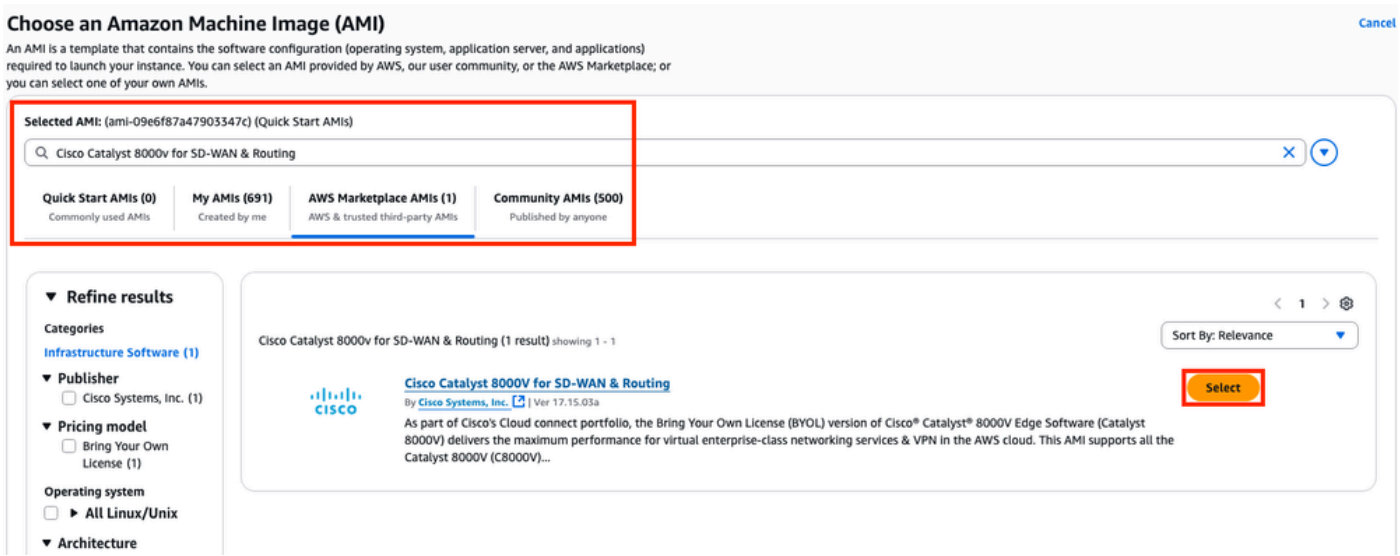
Cada roteador C8000v terá 2 interfaces (1 pública, 1 privada) e será criado em sua própria zona

de disponibilidade.

No Painel EC2, clique em Iniciar instâncias:

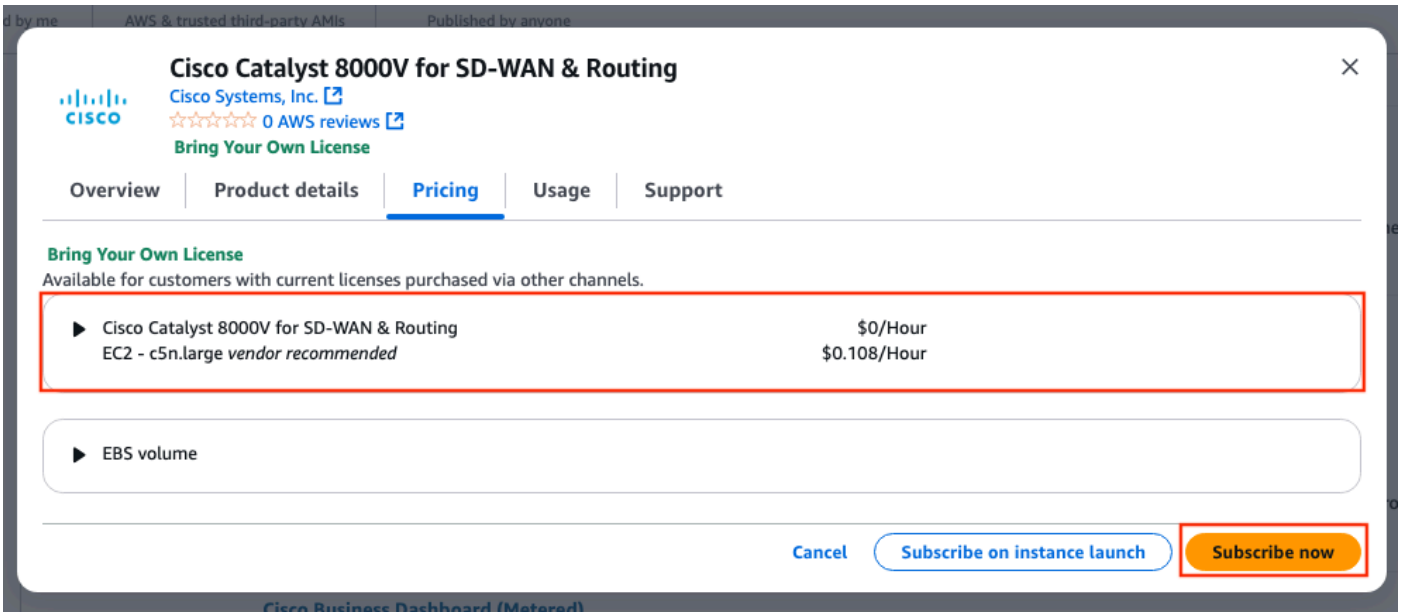


Filtre o banco de dados AMI com o nome Cisco Catalyst 8000v para SD-WAN e roteamento. Na lista AWS Marketplace AMIs, clique em Select.



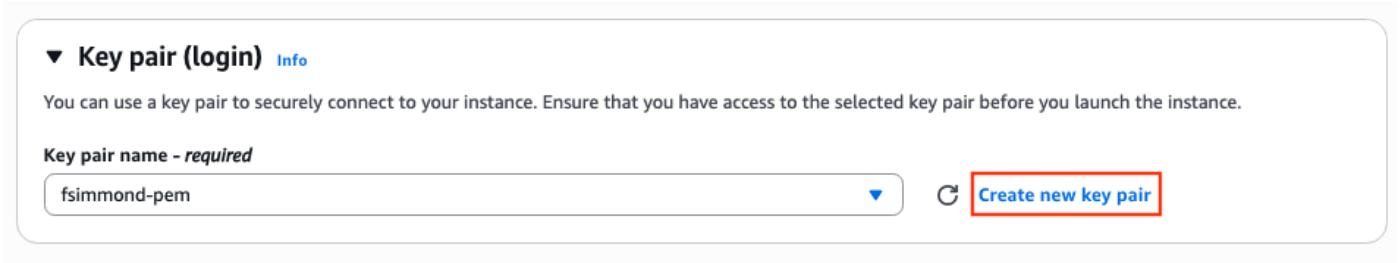
Selecione o tamanho correspondente para o AMI. Para este exemplo, o tamanho c5n.large é

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

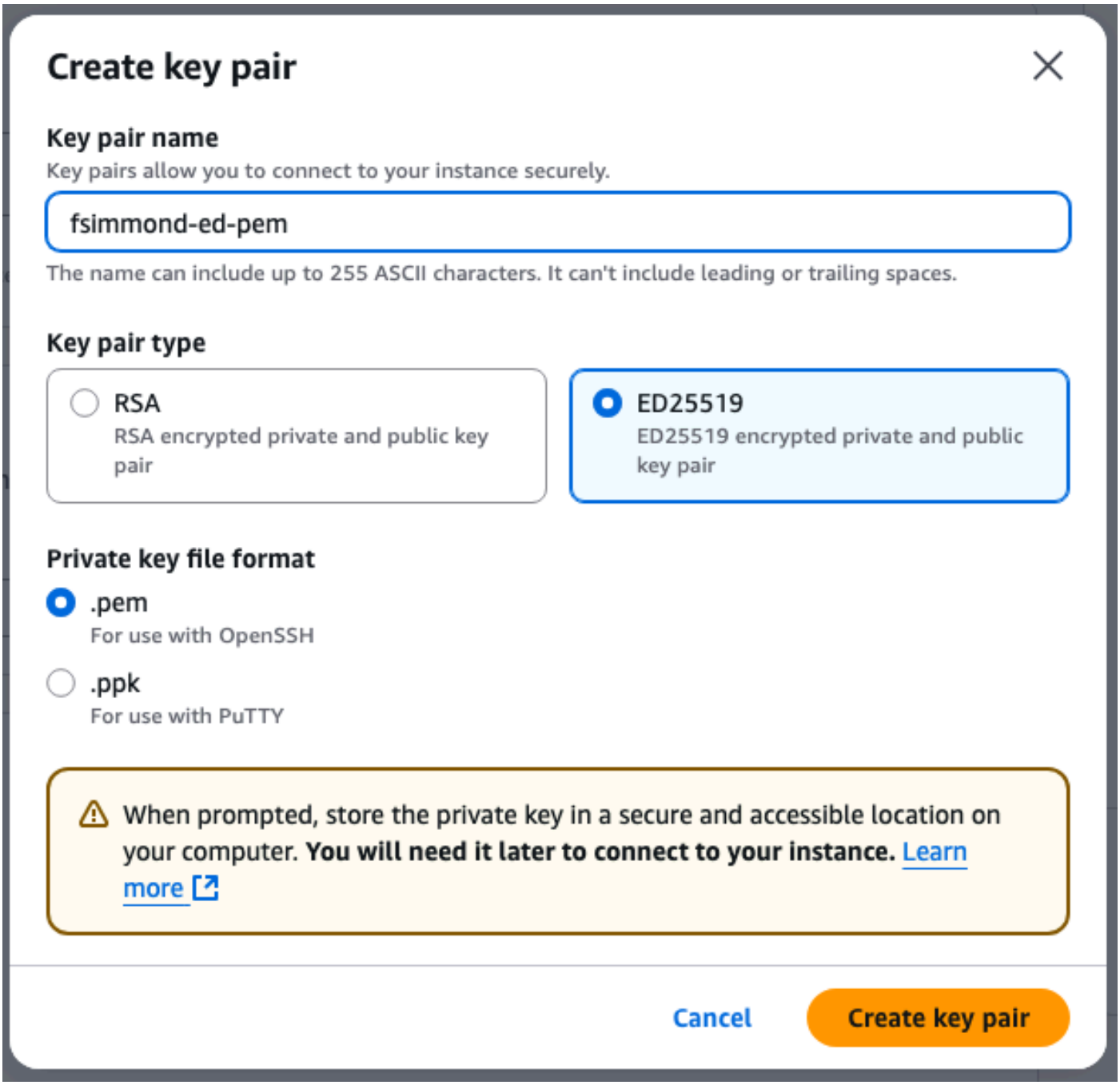


Etapa 6.1. Configurar o par de chaves para acesso remoto

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.



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.



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

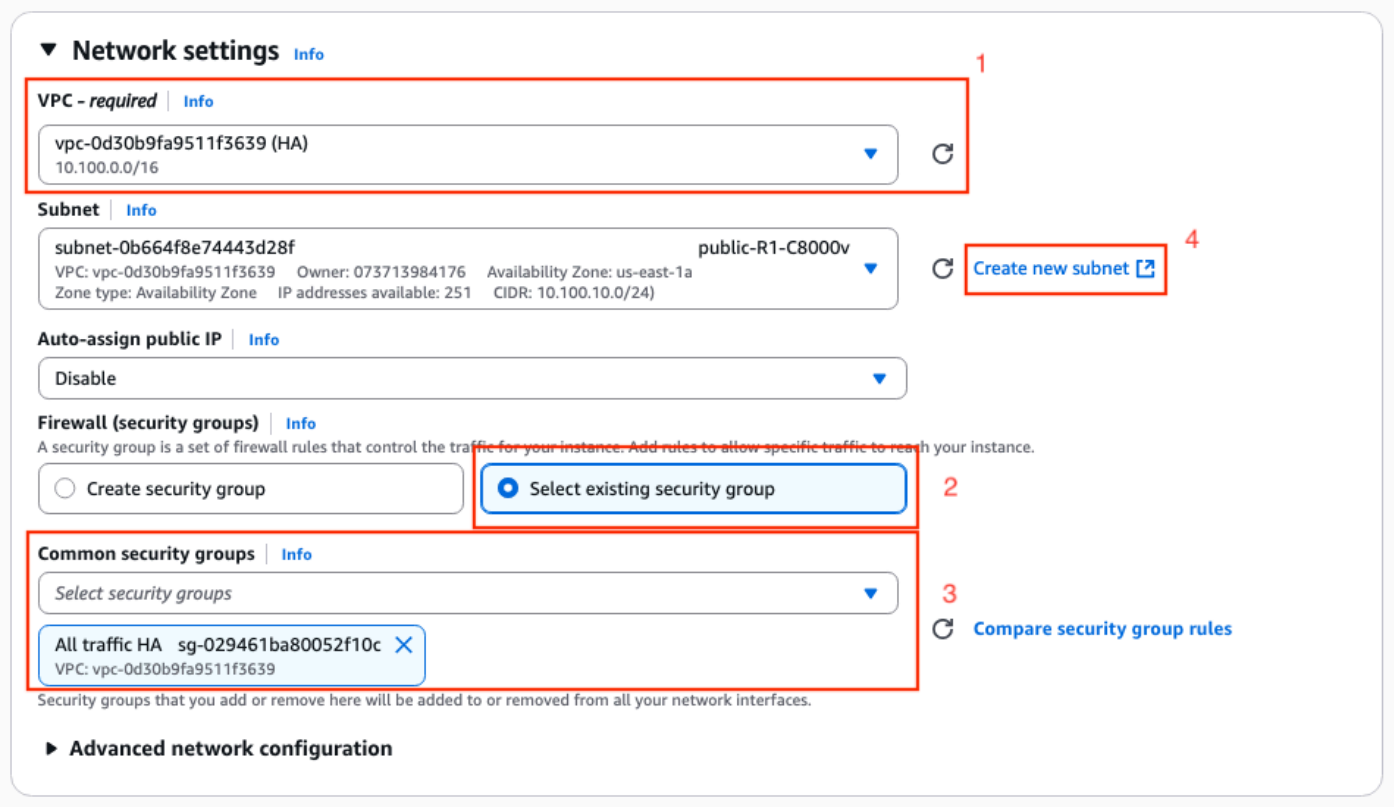
Na seção Configurações de rede, clique em Editar. Algumas novas opções dentro da seção já estão disponíveis:
1. Selecione o VPC desejado para este trabalho. Para este exemplo, o VPC chamado HA é selecionado.

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.



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.

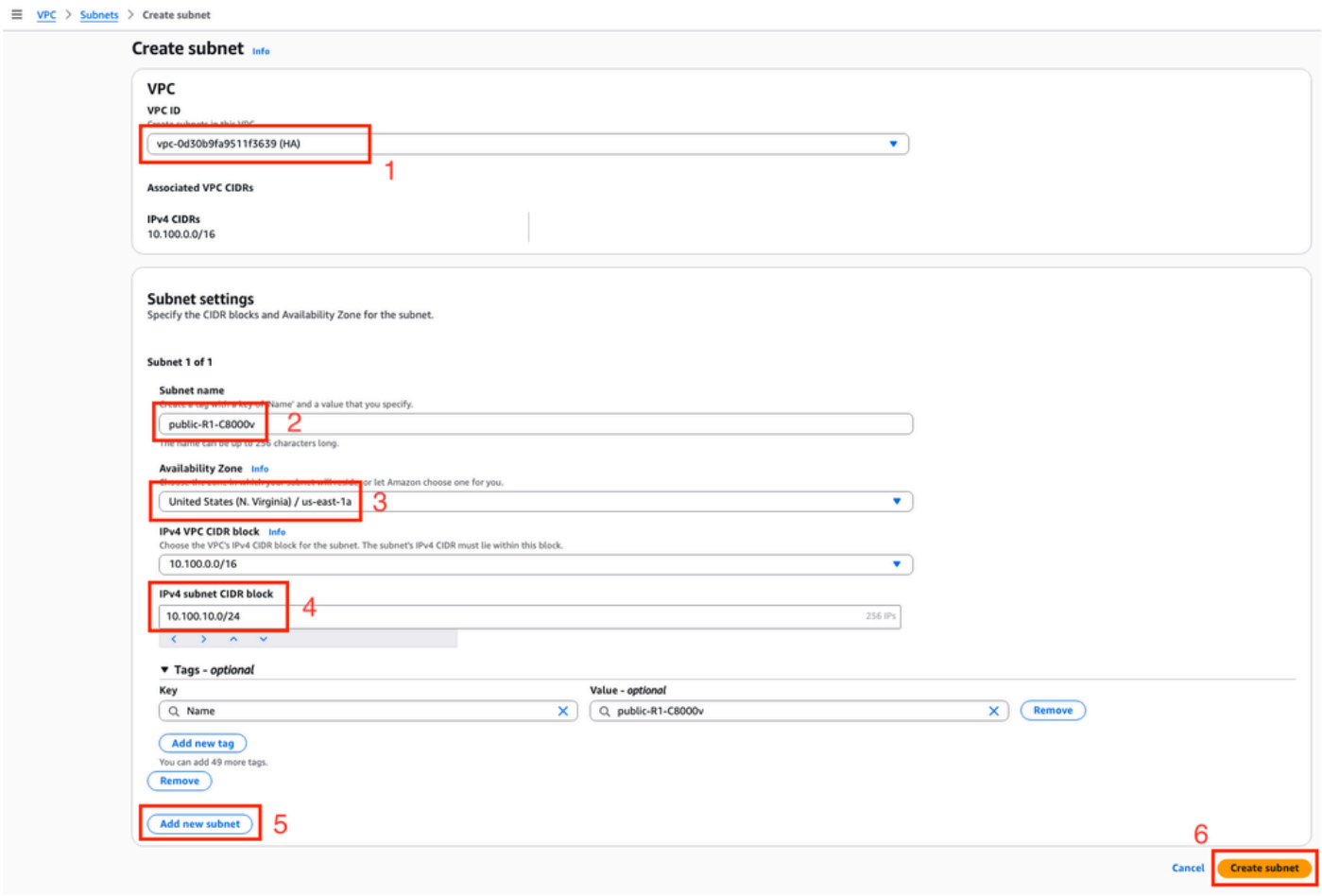
2. Defina um nome para a nova sub-rede.

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.

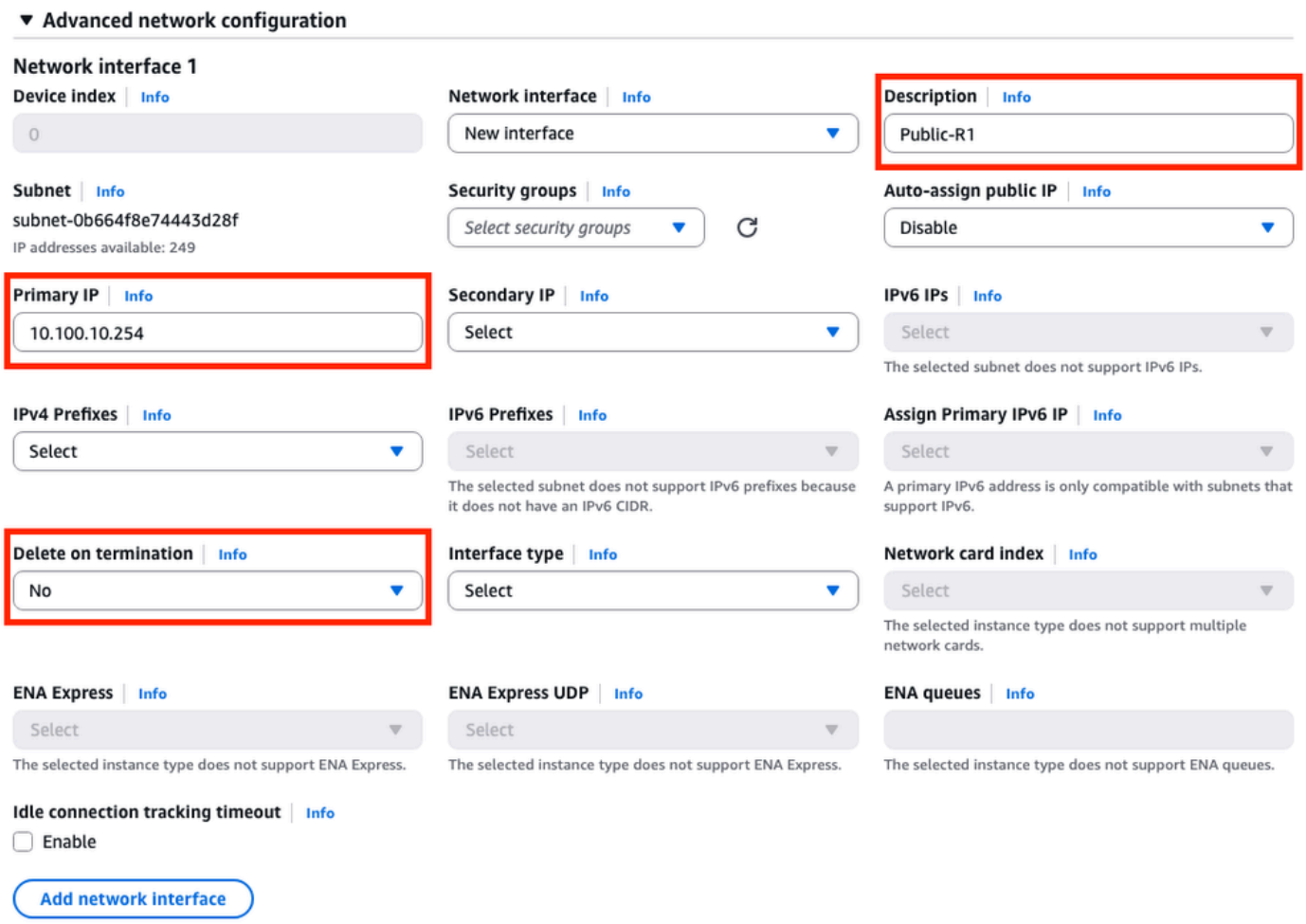
6. Quando terminar, clique em Criar sub-rede. Navegue até a página anterior para continuar com as configurações.



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

Etapa 6.3. Configurar as interfaces AMI

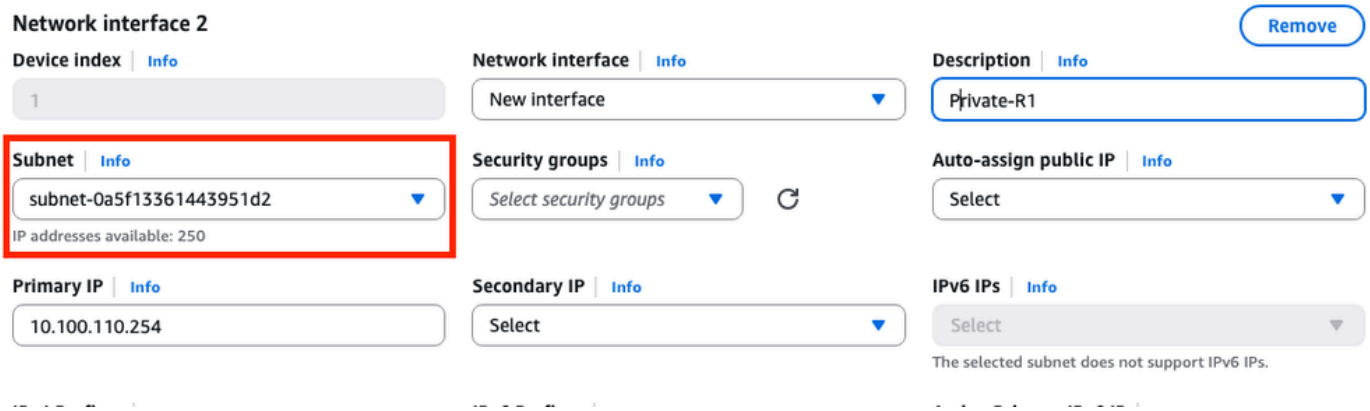
Na seção Network Settings, expanda a subseção Advanced Network configuration. Estas opções são exibidas:



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.

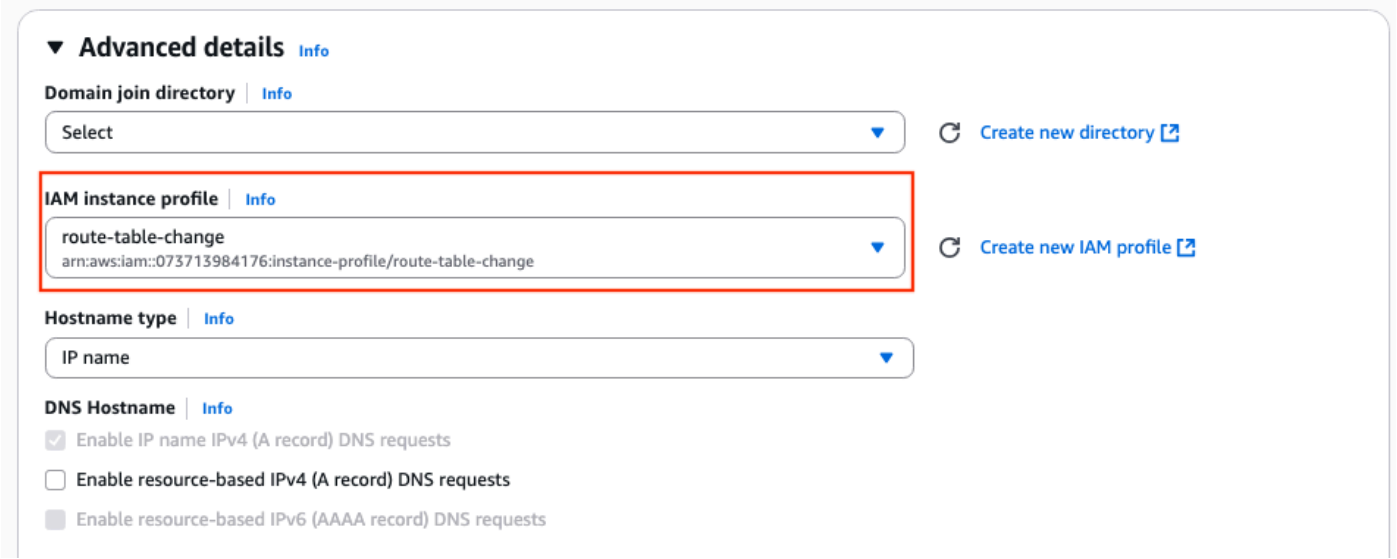
Devido a essa topologia, uma segunda interface é necessária para a sub-rede privada. Clique em Add network interface e este prompt será exibido. No entanto, a interface oferece a opção de selecionar a sub-rede desta vez:



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

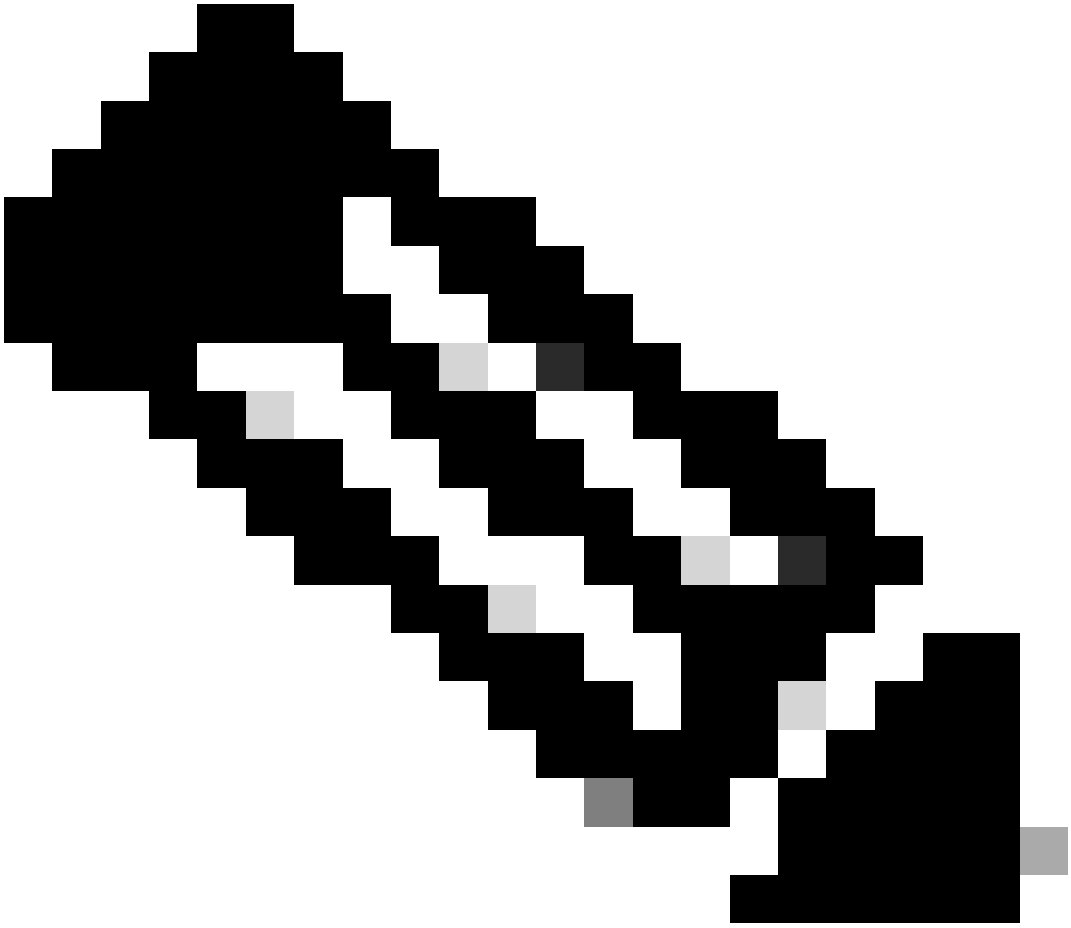
Na seção Detalhes avançados, selecione a função IAM criada no parâmetro perfil da instância IAM:



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.

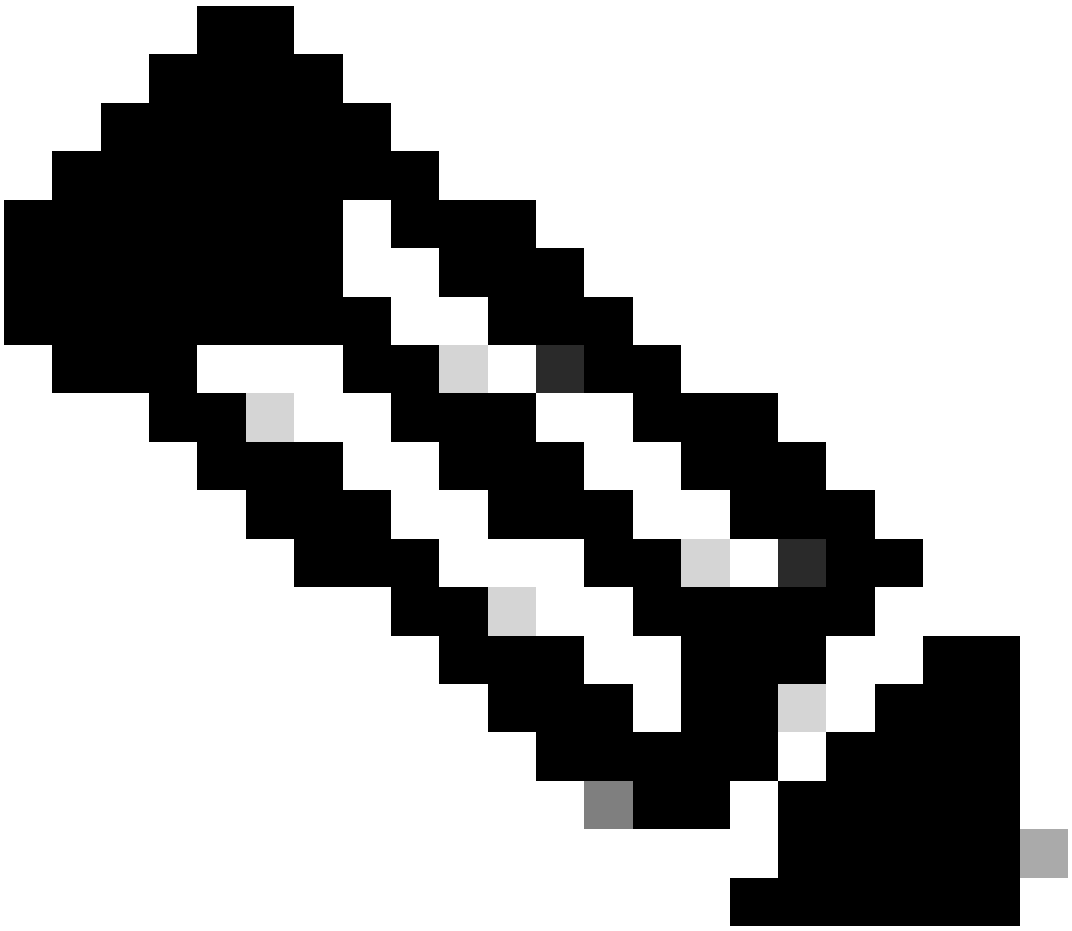
Cancel

Launch instance

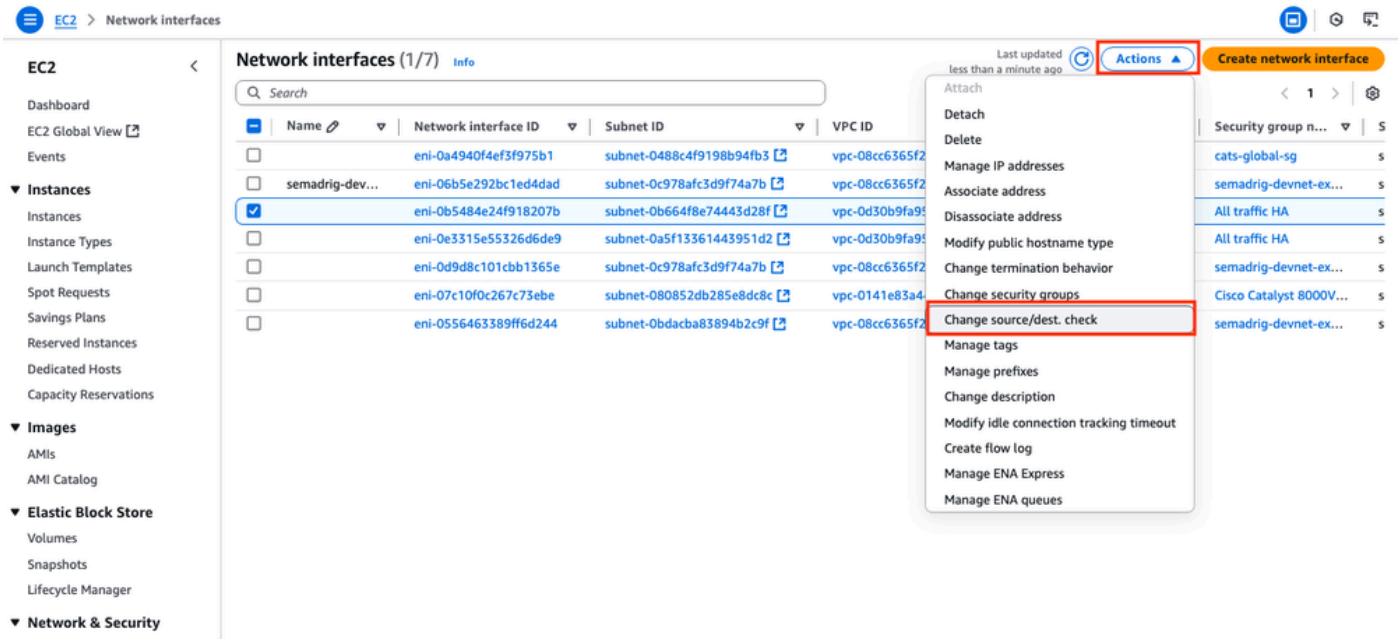
Preview code

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

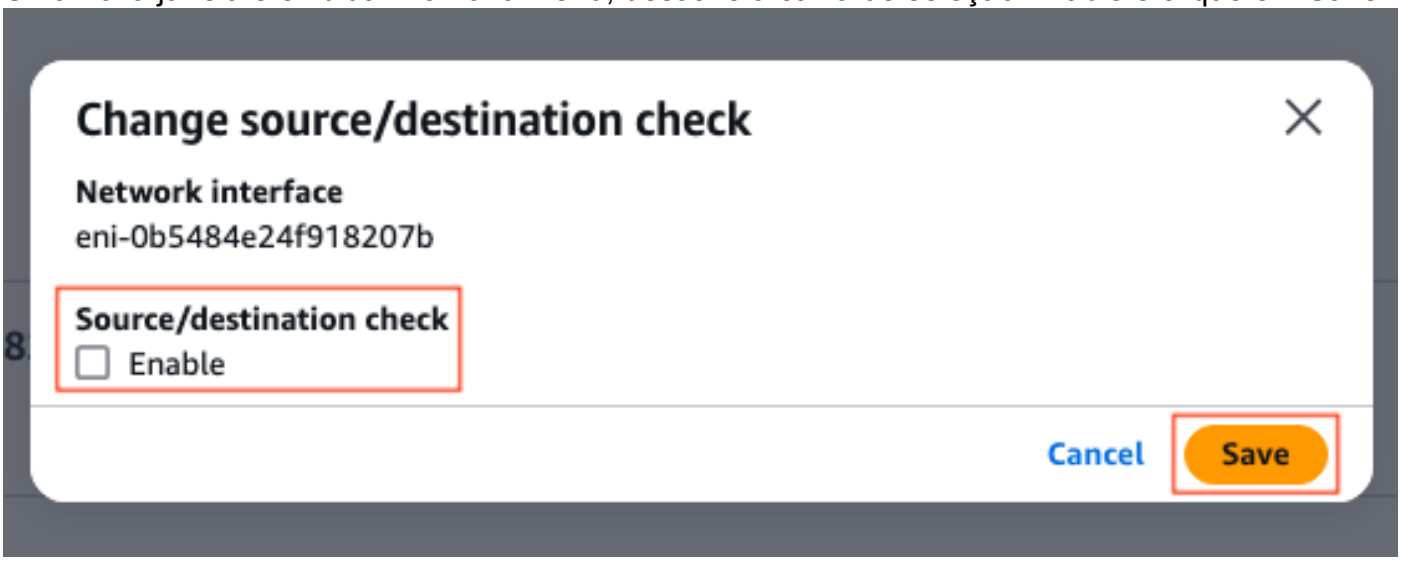
Depois que a Instância for criada, desabilite a funcionalidade de verificação de src/dst no AWS para obter a conectividade entre interfaces na mesma sub-rede. Na seção EC2 Dashboard > Network & Security > Network interfaces, selecione os ENIs e clique em Actions > Alterar origem/destino. verificar.



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

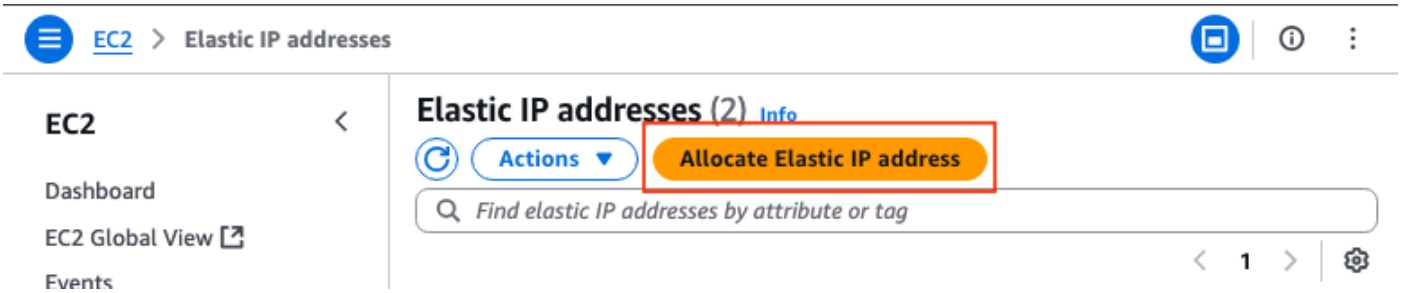


Uma nova janela é exibida. No novo menu, desative a caixa de seleção Enable e clique em Save.

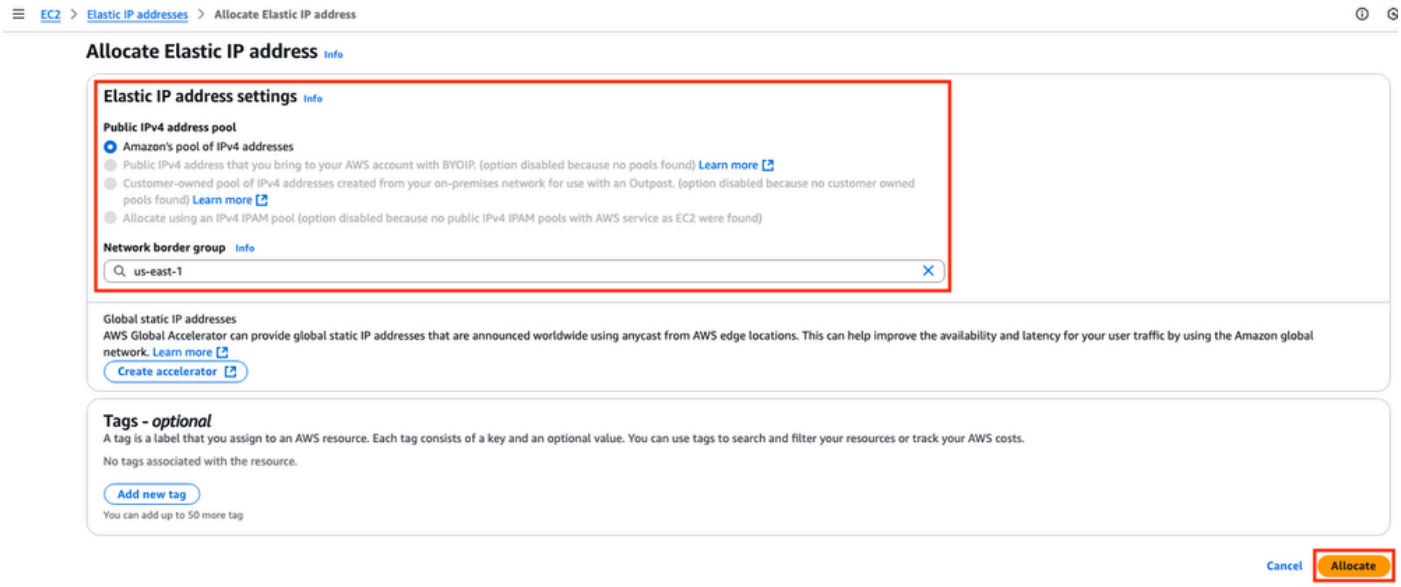


Etapa 6.8. Criar e associar um IP elástico ao ENI público da instância

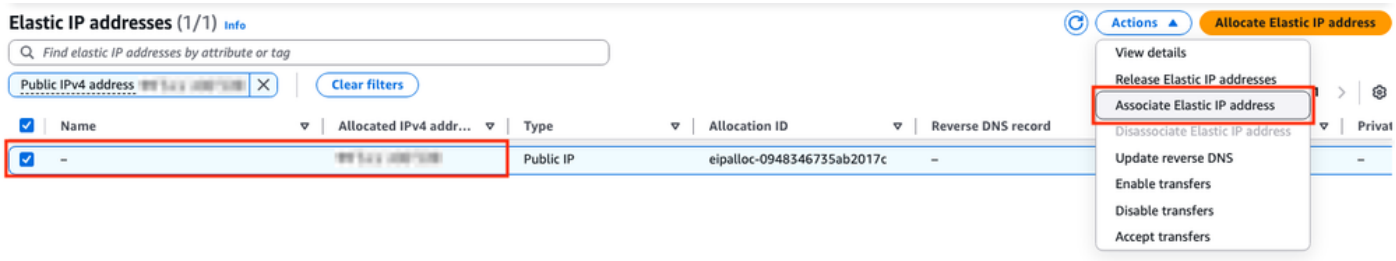
Na seção EC2 Dashboard > Network & Security > Elastic IPs, clique em Allocate Elastic IP address.



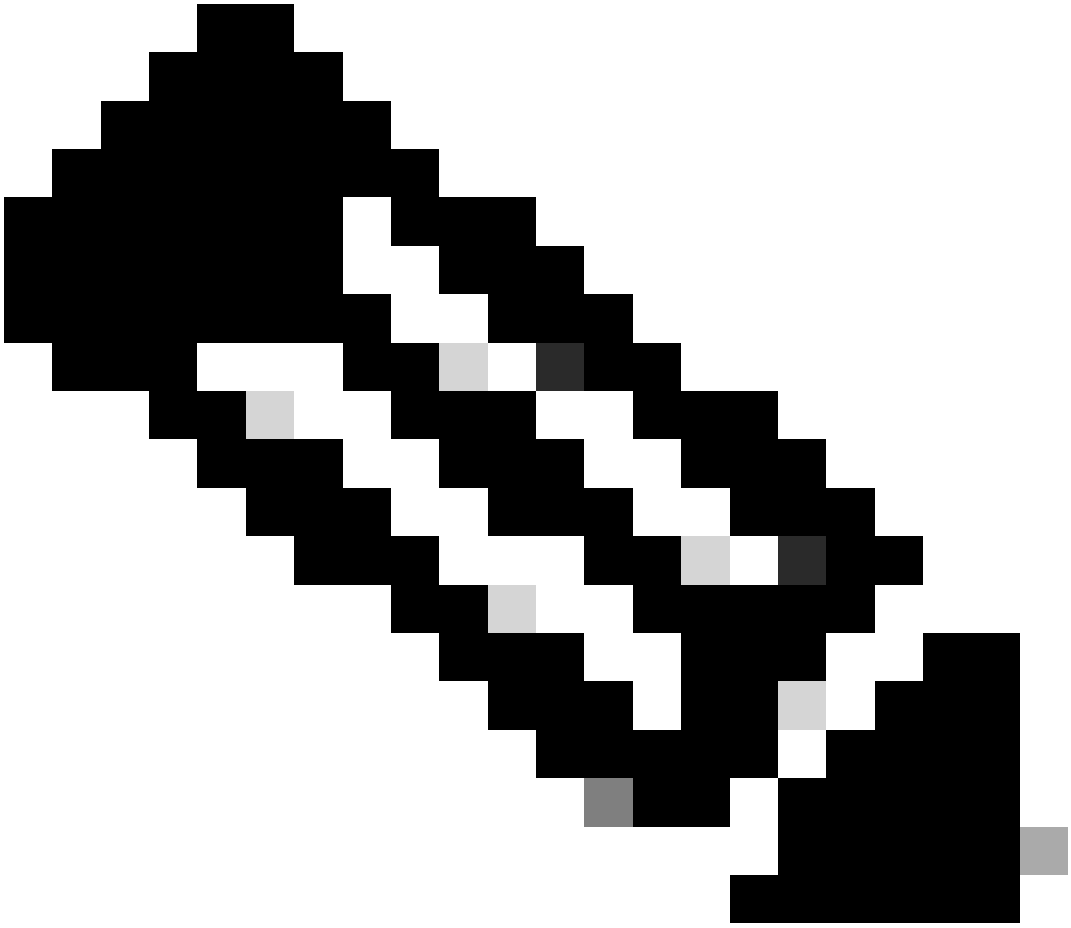
A página o conduz à outra seção. Para este exemplo, a opção Amazon pool of IPv4 addresses é selecionada junto com a zona de disponibilidade us-east-1. Uma vez concluída, clique em Allocate.



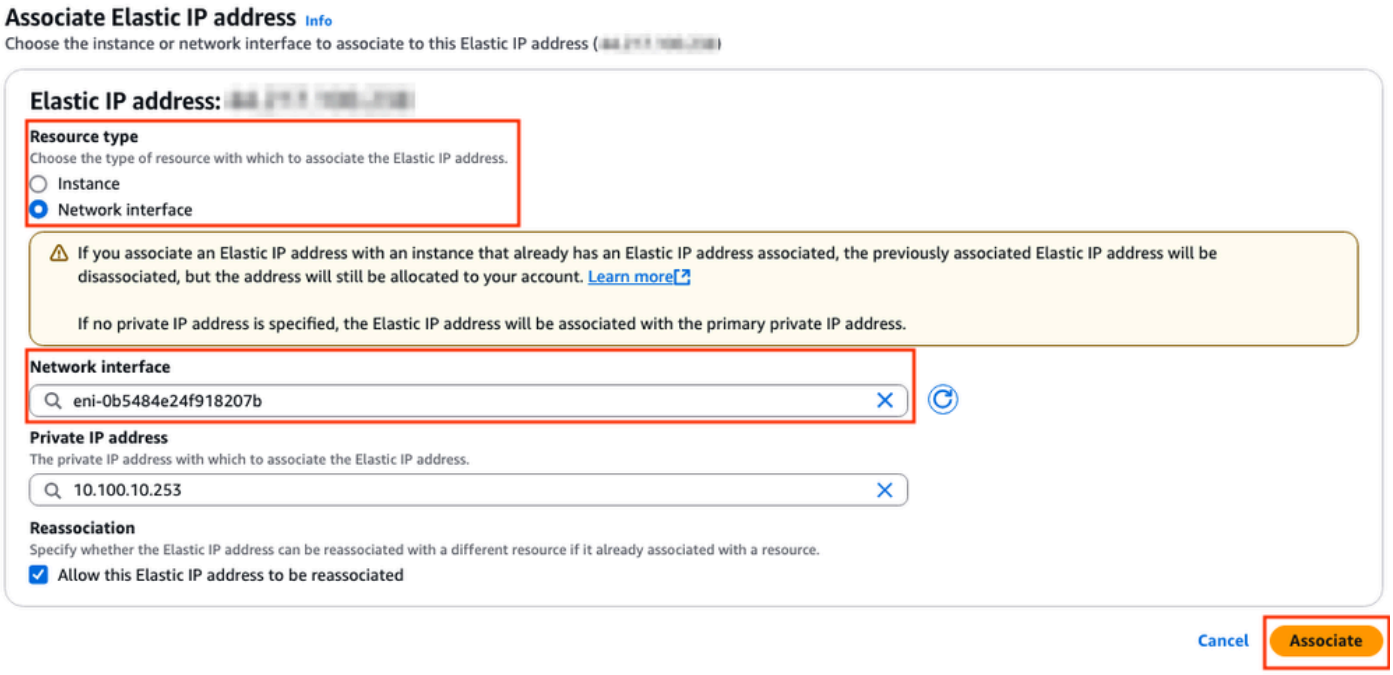
Quando o endereço IP for criado, atribua-o à interface pública da instância. Na seção EC2 Dashboard > Network & Security > Elastic IPs, clique em Actions > Associate Elastic IP address.



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.



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
```

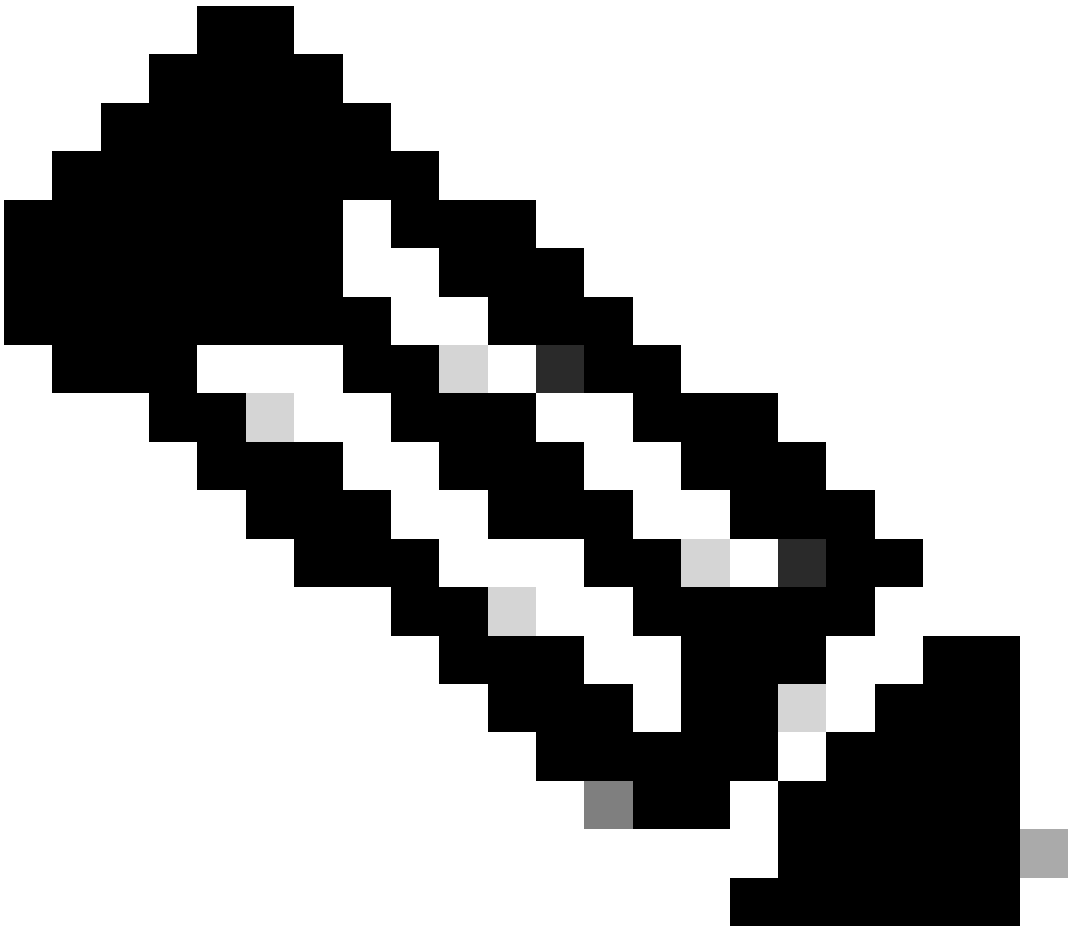
10.100.30.254

```
 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

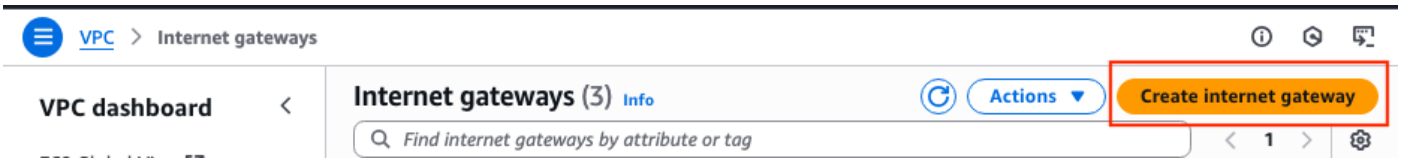
```
 netmask 255.255.255.0 broadcast 10.100.130.255
inet6 fe80::3b:7eff:fead:dbe5 prefixlen 64 scopeid 0x20<link>
ether 02:3b:7e:ad:db:e5 txqueuelen 1000 (Ethernet)
RX packets 119 bytes 16831 (16.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 133 bytes 13816 (13.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



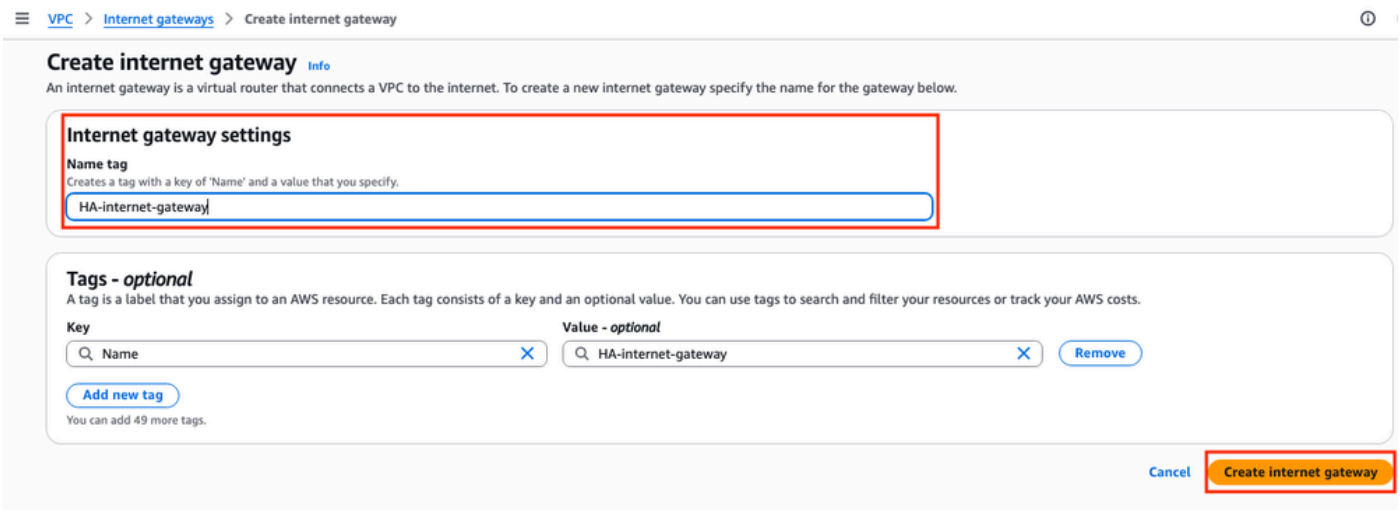
Note: Se for feita alguma alteração nas interfaces, sincronize a interface ou recarregue a VM para aplicar essas alterações.

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

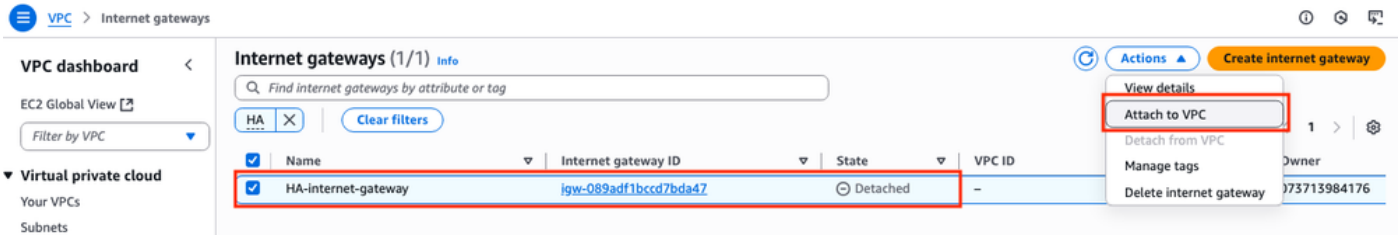
Na seção **VPC Dashboard > Virtual Private Cloud > Internet Gateways**, clique em **Create Internet Gateway**.



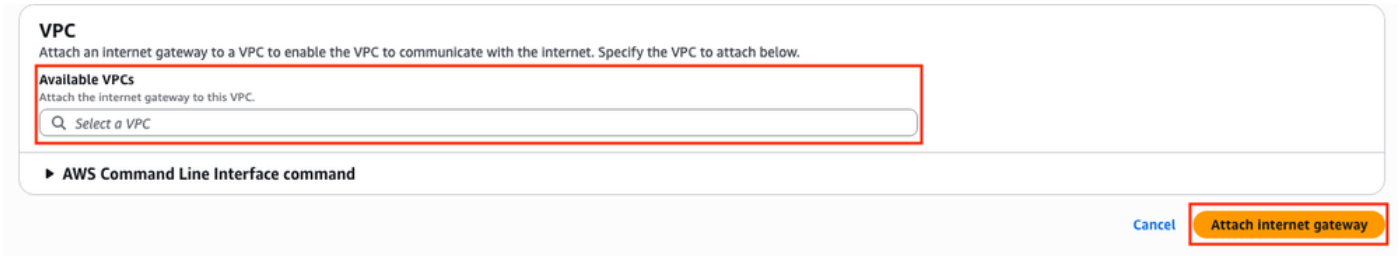
Nesta nova seção, crie uma marca **name** para este gateway e clique em **Create internet gateway**.



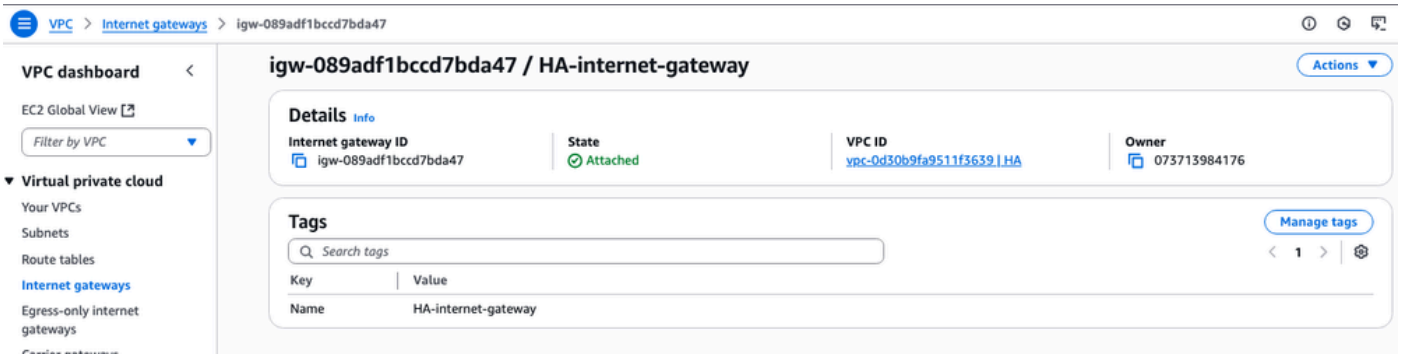
Depois que o IGW for criado, anexe-o ao VPC correspondente. Navegue até a seção **VPC Dashboard > Virtual Private Cloud > Internet Gateway** e selecione o IGW correspondente. Clique em **Ações > Anexar ao VPC**.



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



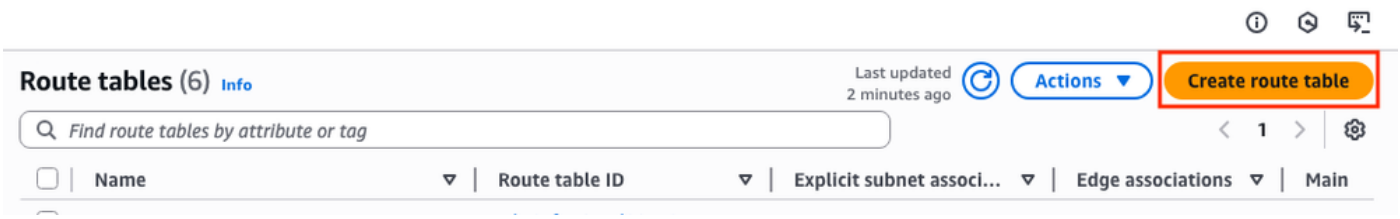
O IGW deve indicar o estado Attached (Anexado) como mostrado:



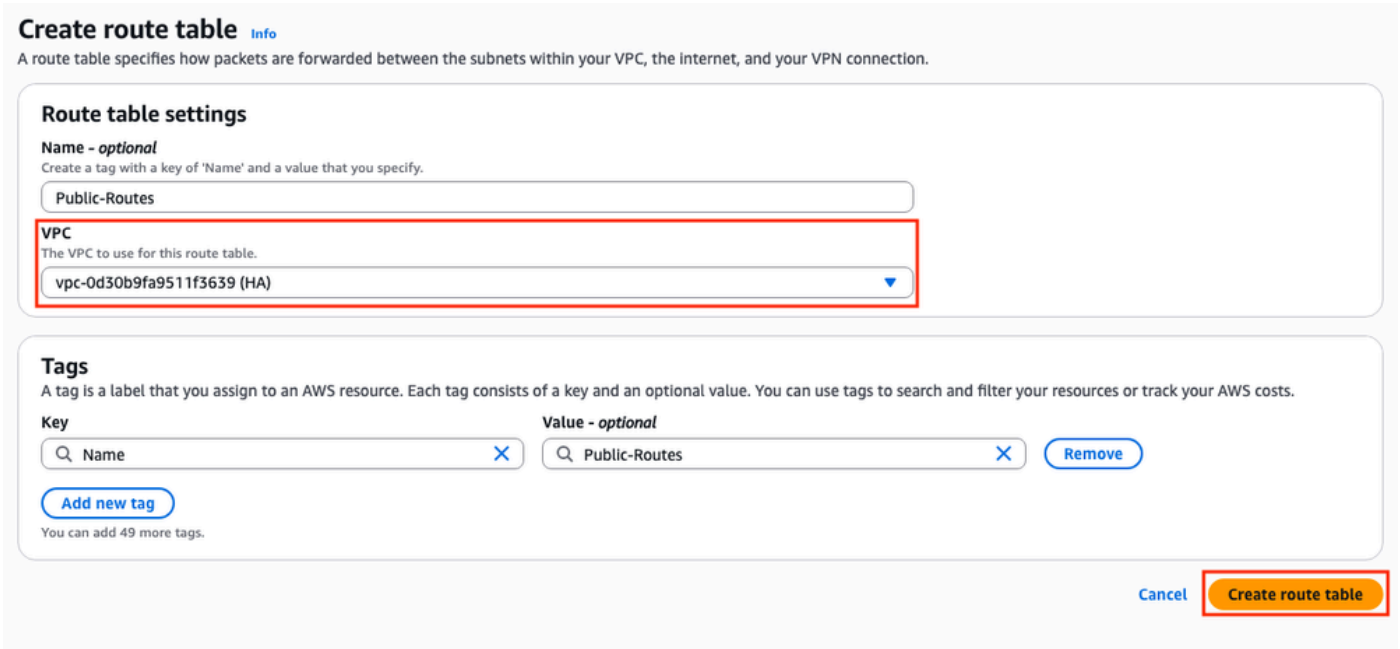
Etapa 10. Criar e Configurar Tabelas de Rotas no AWS para sub-redes Públicas e Privadas

Etapa 10.1. Criar e configurar a tabela de rotas públicas

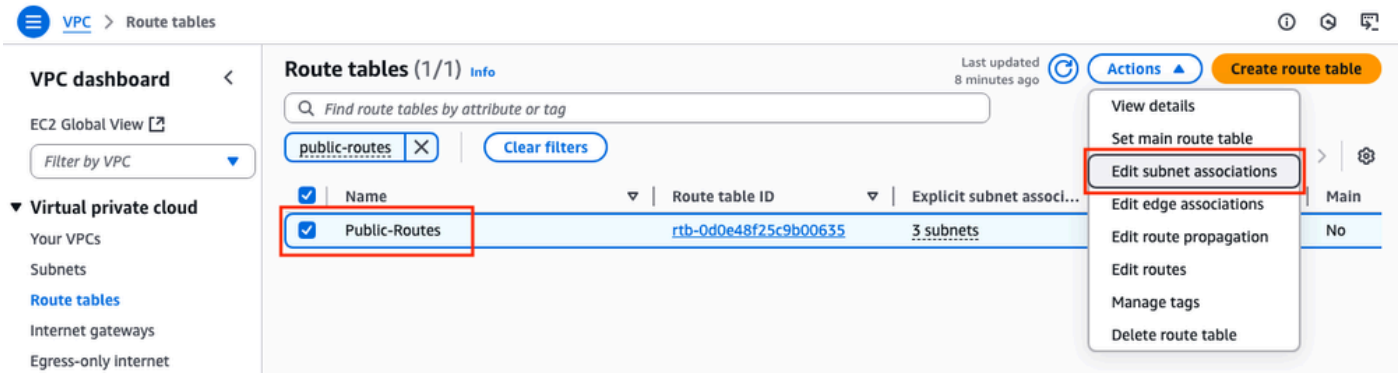
Para estabelecer o HA nessa topologia, associe todas as sub-redes públicas e privadas em suas tabelas de rota correspondentes. Na seção VPC Dashboard > Virtual Private Cloud > Route tables, clique em Create route table.



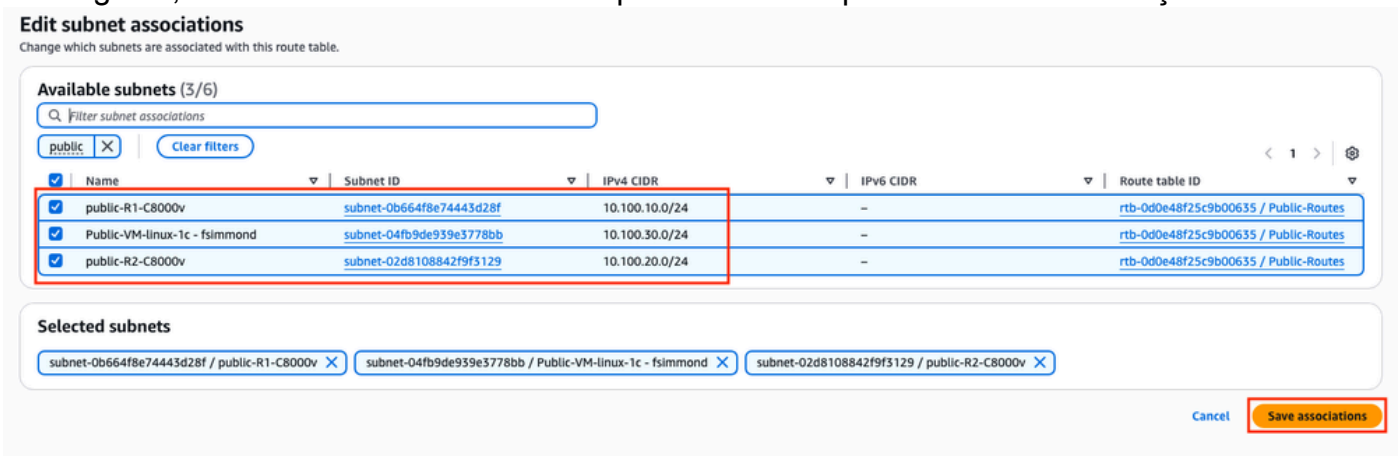
Na nova seção, selecione o VPC correspondente para esta topologia. Depois de selecionado, clique em Create route table.



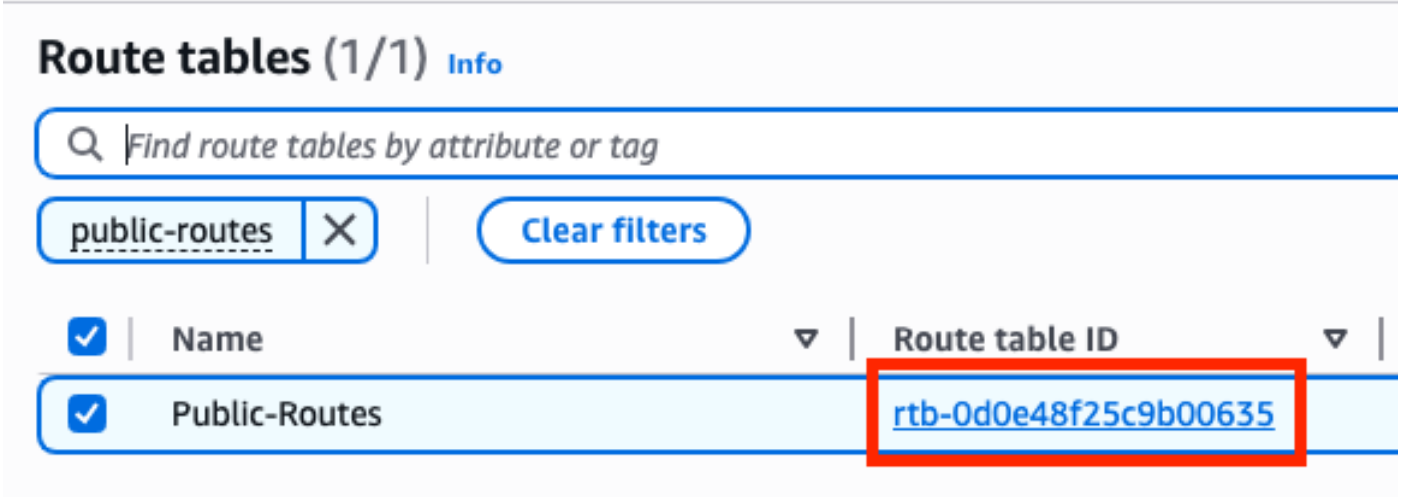
Na seção Tabelas de rota, selecione a tabela criada e clique em Ações > Editar associações de sub-rede.



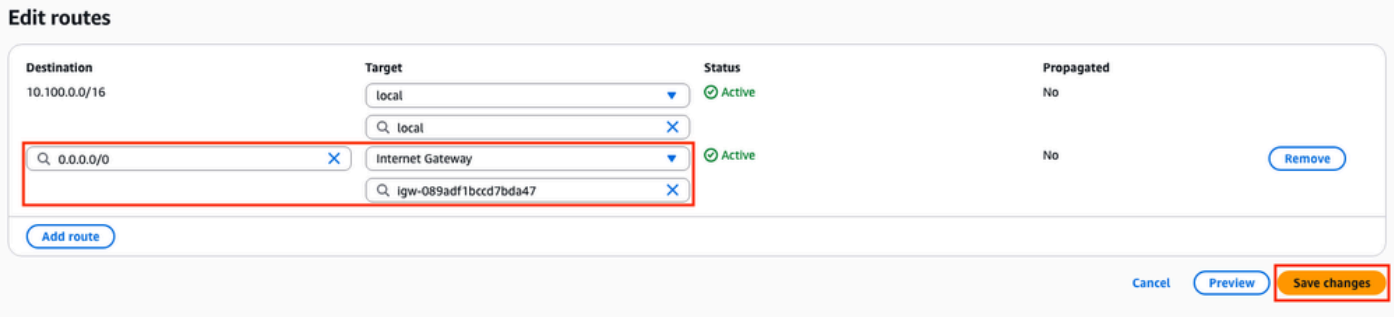
Em seguida, selecione as sub-redes correspondentes e clique em Salvar associações.



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:

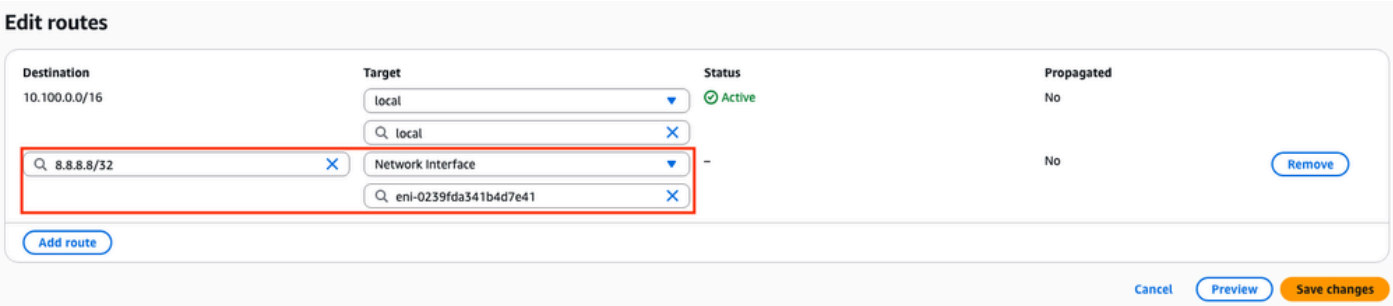


Para obter acesso à Internet, clique em Add route e vincule essa rota pública tabela com a IGW criada na Etapa 9 com esses parâmetros. Depois de selecionado, clique em Salvar alterações:



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:



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.

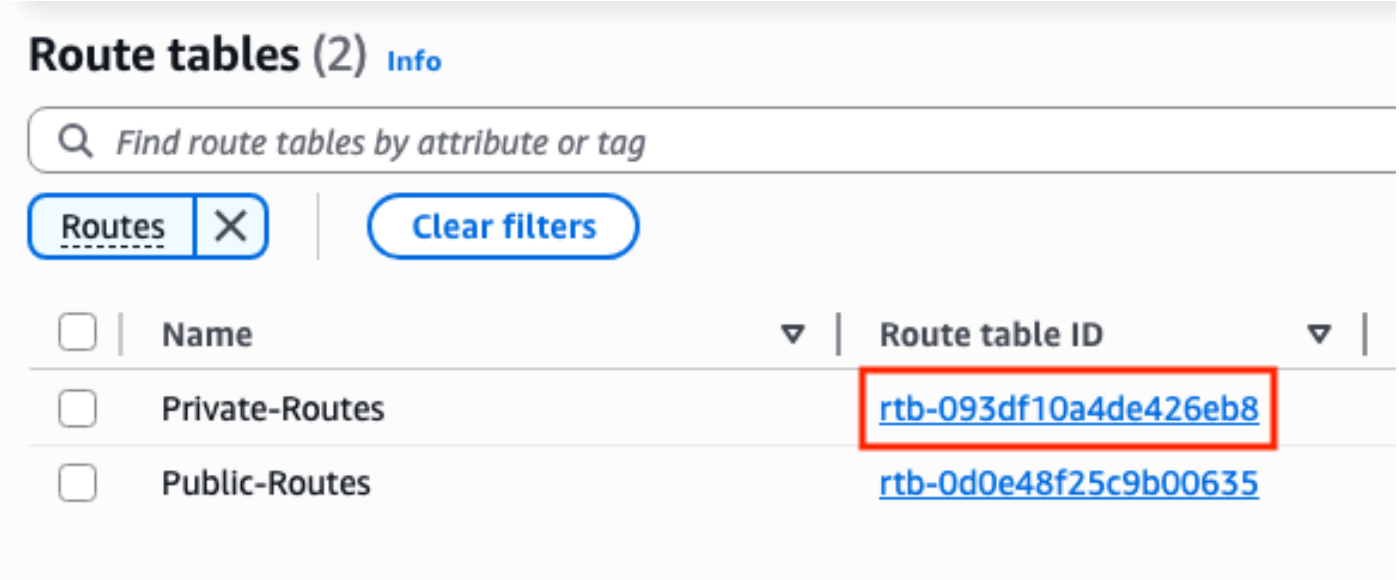
```
Router(config)# redundancy
Router(config-red)# cloud provider aws (node-id)
bfd peer <IP address of the remote device>
route-table <Route table ID>
cidr ip <traffic to be monitored/prefix>
eni <Elastic network interface (ENI) ID>
region <region-name>
```

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

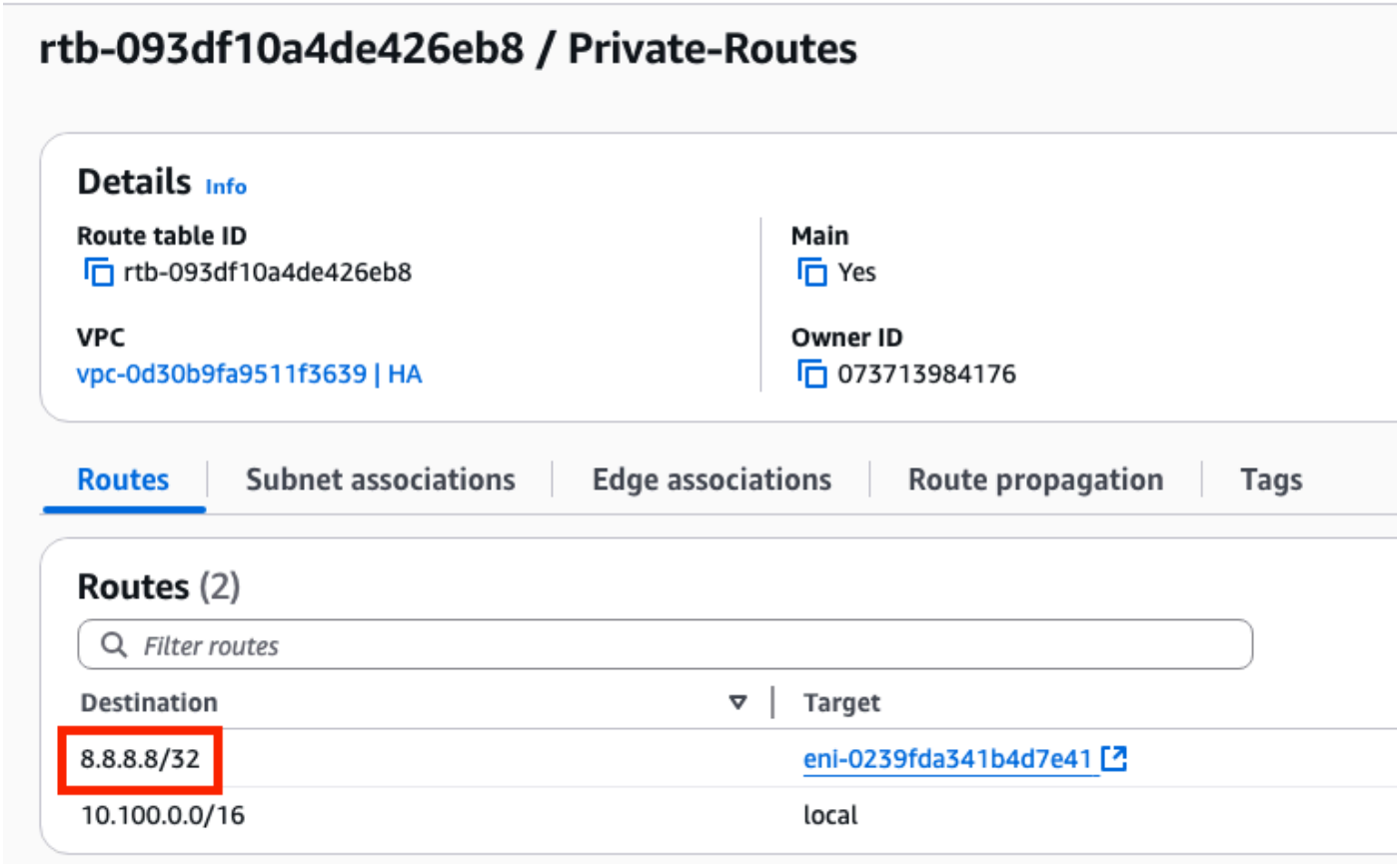
```
R1(config)#do sh bfd neighbors

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

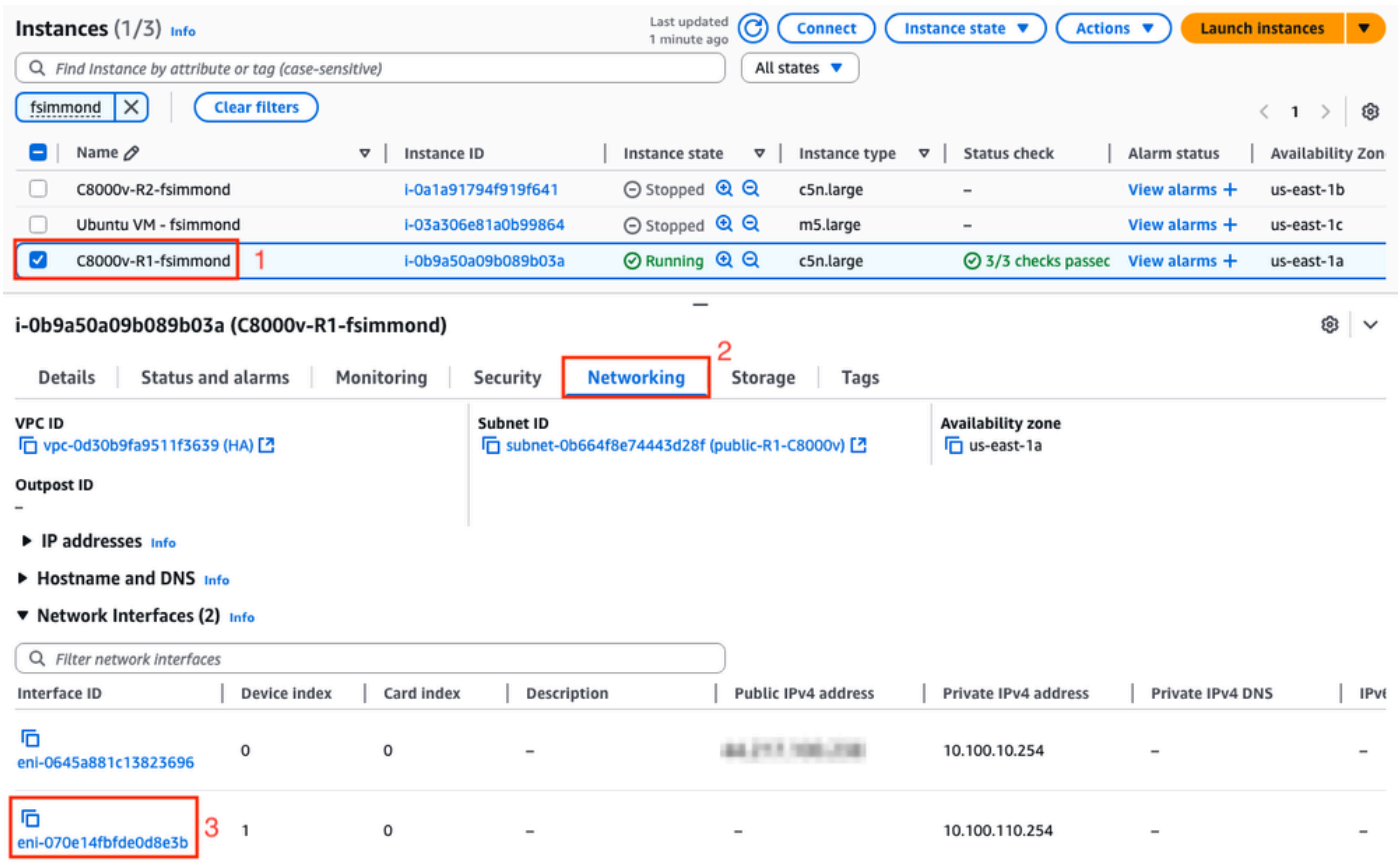
O parâmetro route-table está relacionado à ID da tabela de rota privada localizada na seção VPC Dashboard > Virtual Private Cloud > Route Tables. Copie a ID da tabela de rota correspondente.



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



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:



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
```

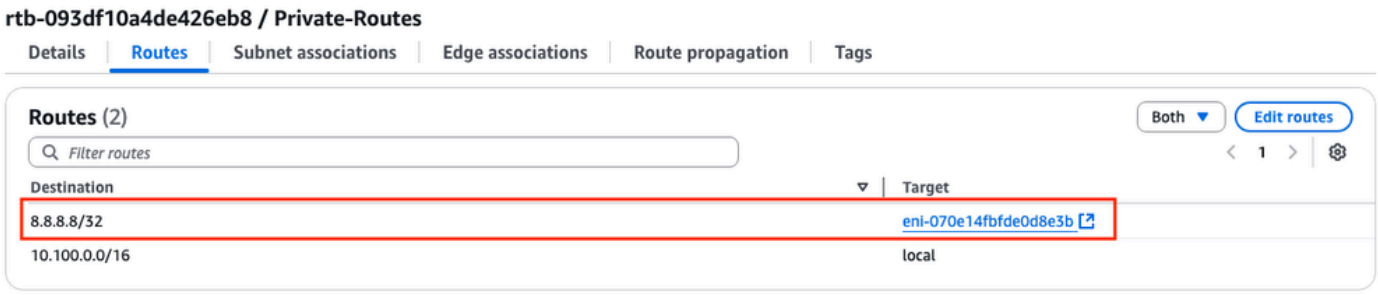
```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.200.2 Tu1 10 00:16:52 2 1470 0 2
```

```
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. 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:



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:

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.