Implementación de la configuración de alta disponibilidad de C8000v en AWS

Contenido

Introducción

Este documento describe cómo configurar un entorno de alta disponibilidad con routers Catalyst 8000v en la nube de Amazon Web Services.

Prerequisites

Requirements

Cisco recomienda tener conocimientos previos sobre estos temas:

- Conocimiento general de AWS Console y sus componentes
- Información sobre el software Cisco IOS® XE
- Conocimiento básico de la función HA.

Componentes Utilizados

Estos componentes son necesarios para este ejemplo de configuración:

- Una cuenta de Amazon AWS con función de administrador
- Dos dispositivos C8000v con Cisco IOS® XE 17.15.3a y una máquina virtual Ubuntu 22.04 LTS AMI en la misma región

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Topología

Hay varias situaciones de implementación de HA basadas en los requisitos de la red. Para este ejemplo, la redundancia de HA se configura con estas configuraciones:

- 1x - Región
- 1 VPC
- 3x - Zonas de disponibilidad
- 6x - Interfaces/subredes de red (3x de orientación pública/3x de orientación privada)
- 2x - Tablas de ruta (pública y privada)
- 2 routers C8000v (Cisco IOS® XEDenali 17.15.3a)
- 1x - VM (Linux/Windows)

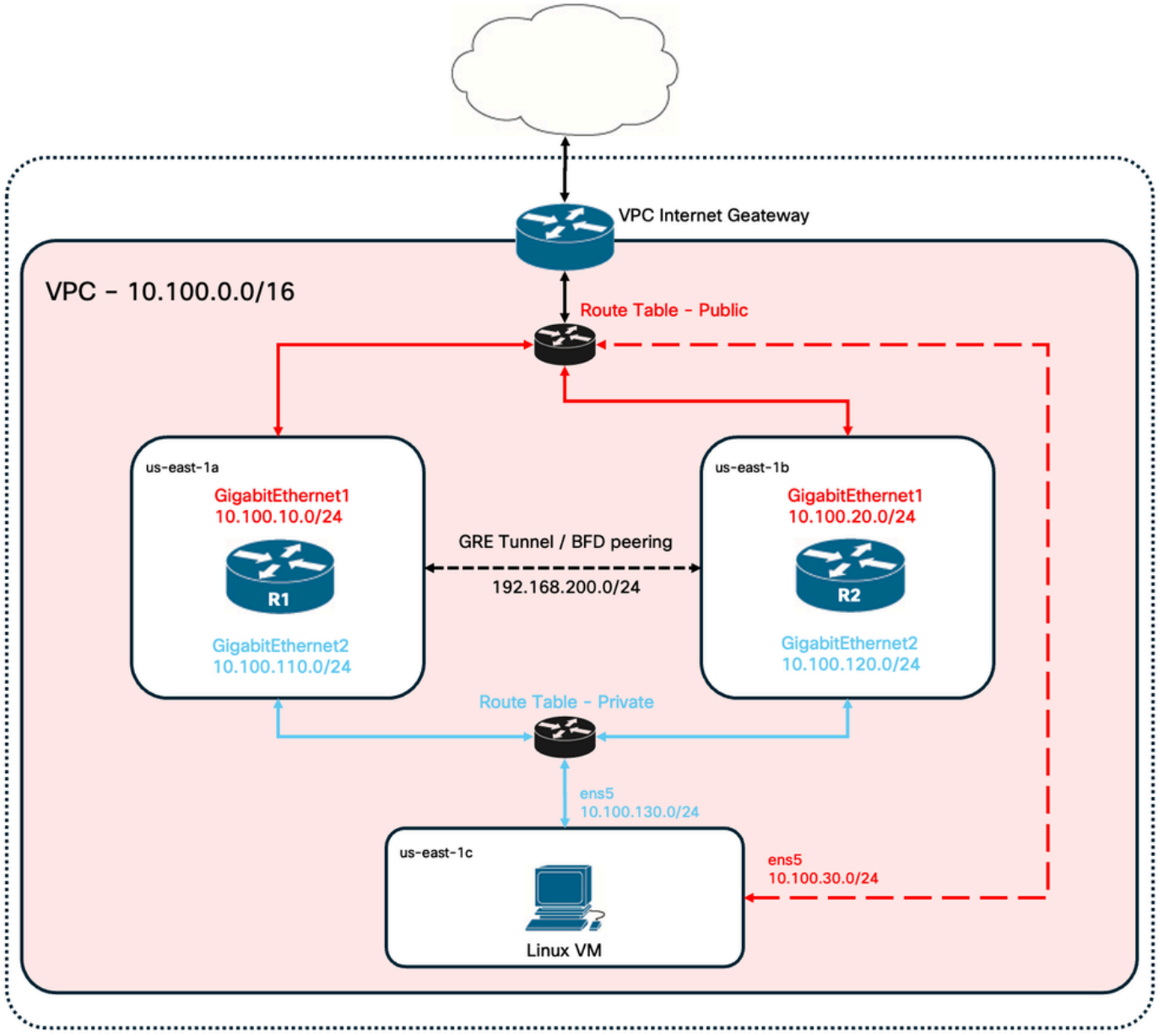
Hay 2 routers C8000v en un par HA, en dos zonas de disponibilidad diferentes. Considere cada zona de disponibilidad como un Data Center independiente para disfrutar de una resistencia de hardware adicional.

La tercera zona es una VM, que simula un dispositivo en un Data Center privado. Por ahora, el acceso a Internet está habilitado a través de la interfaz pública para que pueda acceder y configurar la VM. Generalmente, todo el tráfico normal debe fluir a través de la tabla de rutas

privadas.

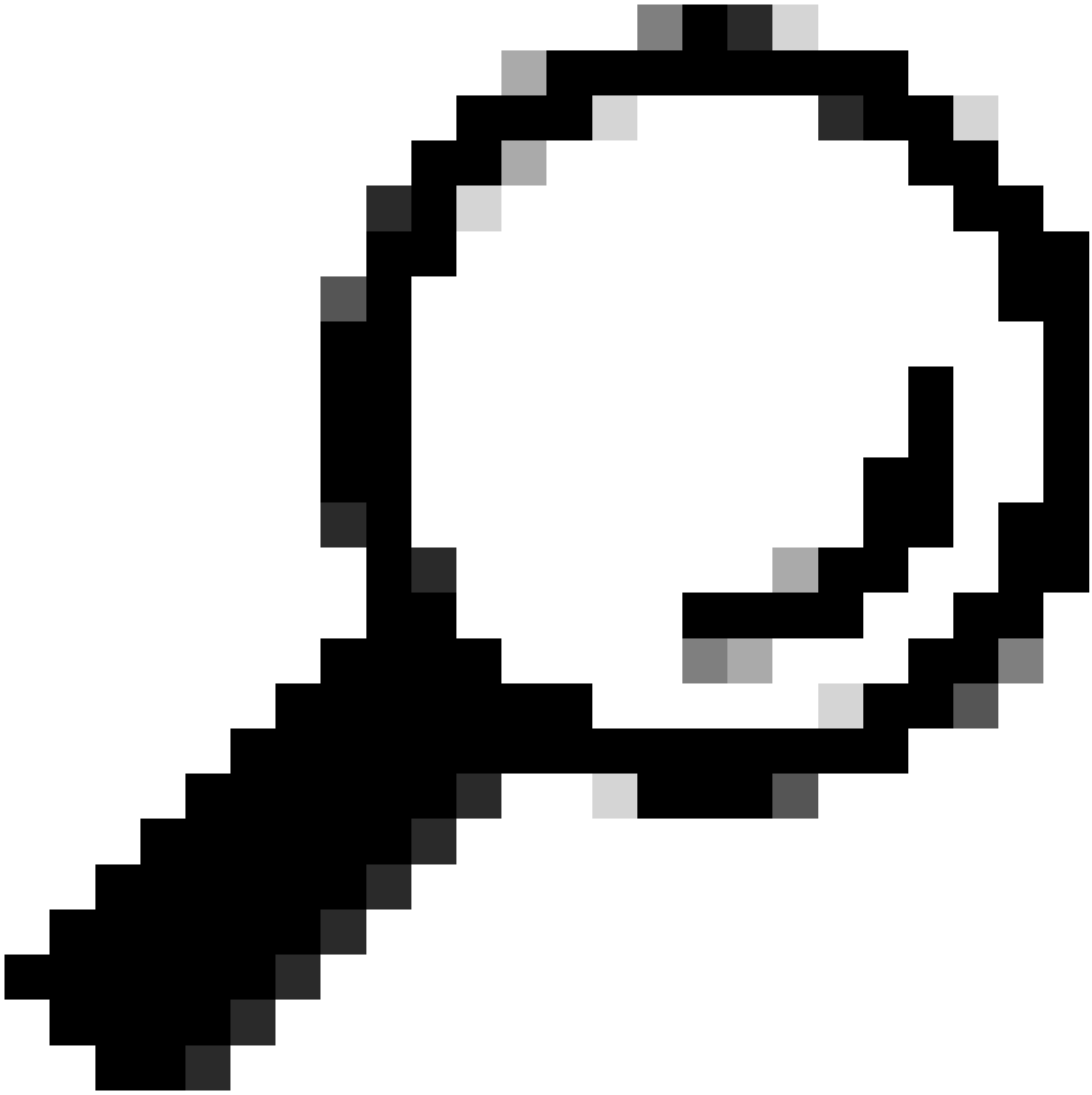
Para simular el tráfico, inicie un ping desde la interfaz privada de la máquina virtual, atravesando la tabla de rutas privadas a través de R1 para alcanzar 8.8.8.8. En caso de una conmutación por error, verifique que la tabla de rutas privadas se haya actualizado automáticamente para enrutar el tráfico a través de la interfaz privada del router R2.

Diagrama de la red



Resumen de tabla

Para resumir la topología, aquí está la tabla con los valores más importantes de cada componente en el laboratorio. La información proporcionada en esta tabla es exclusiva para este laboratorio.



Sugerencia: el uso de esta tabla ayuda a mantener una visión general clara de las variables clave en toda la guía. Se recomienda recopilar la información en este formato para simplificar el proceso.

Dispositivo	Zona de disponibilidad	Interfaces	Direcciones de IP	RTB	ENI
R1	us-east-1a	GigabitEthernet1	10.100.10.254	rtb-0d0e48f25c9b00635 (pública)	eni-0645a88c13823696
		GigabitEthernet2	10.100.110.254	rtb-093df10a4de426eb8 (privado)	eni-070e14fbfde0d8e3b
R2	us-east-1b	GigabitEthernet1	10.100.20.254	rtb-0d0e48f25c9b00635	eni-0a7817922ffbb317b

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

Restricciones

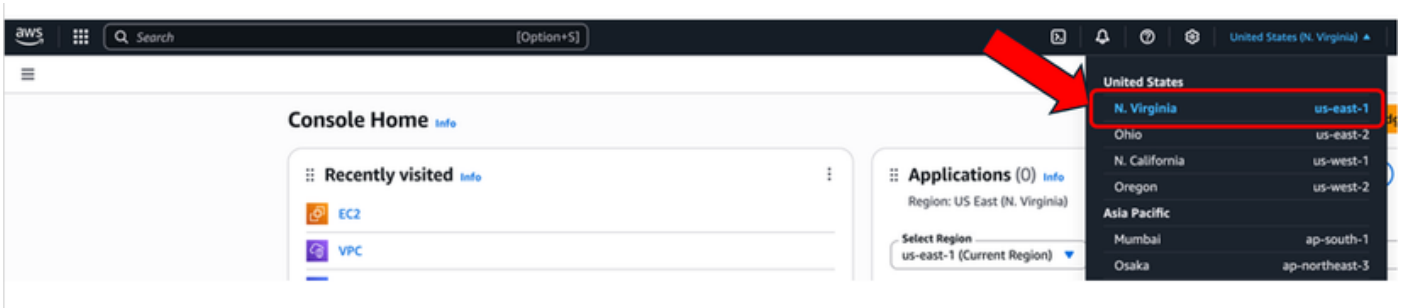
- En cualquier subred creada, no utilice la primera dirección disponible de esa subred. Estas direcciones IP son utilizadas internamente por los servicios de AWS.
- No configure las interfaces públicas de los dispositivos C8000v dentro de un VRF. HA no funciona correctamente si se configura.

Configuración

El flujo general de configuración se centra en crear las VM solicitadas en la región adecuada y avanzar hacia la configuración más específica, como las rutas e interfaces de cada una de ellas. Sin embargo, se recomienda entender primero la topología y configurarla en el orden que se desee.

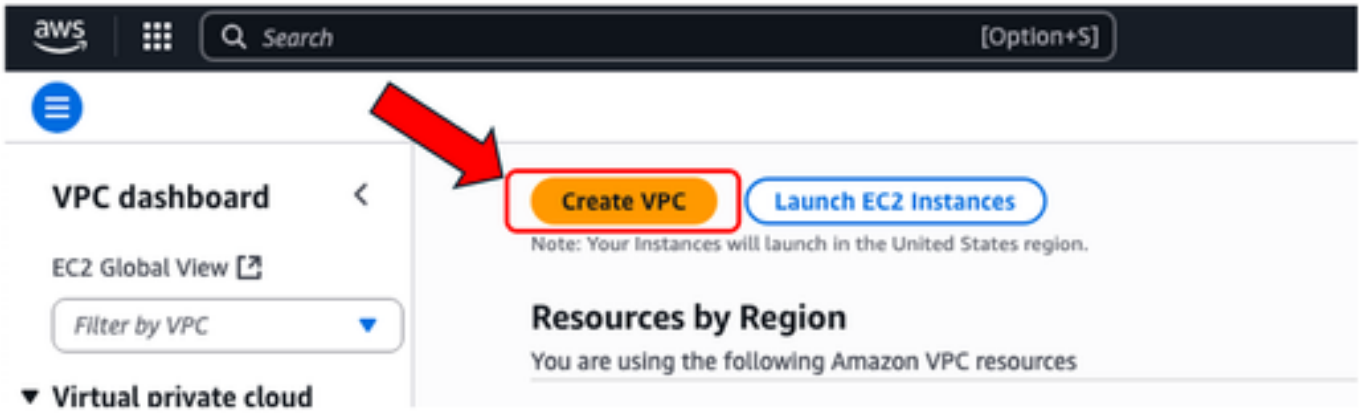
Paso 1. Seleccione una región

Para esta guía de implementación, la región US West (North Virginia) - us-east-1 se selecciona como la región VPC.



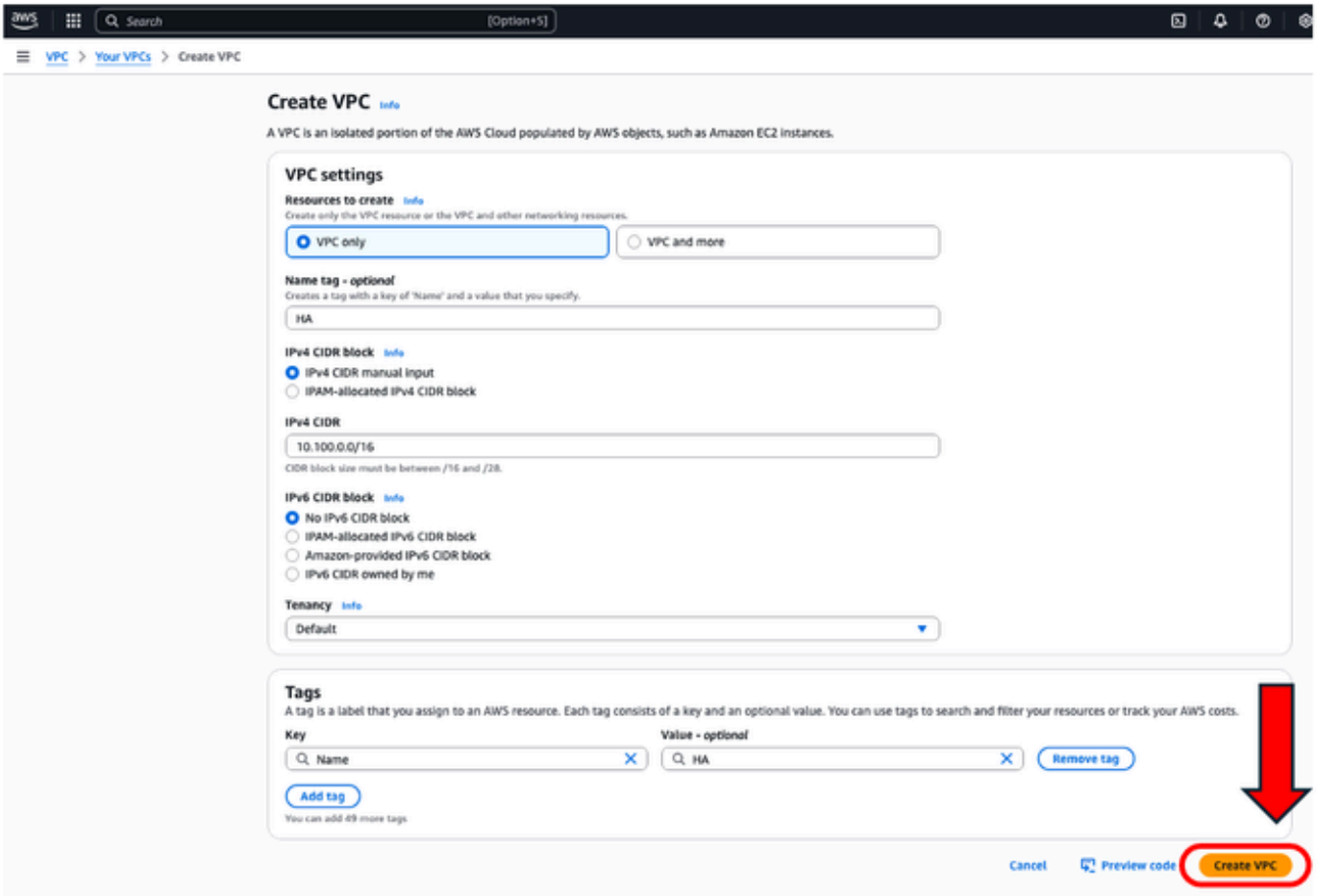
Paso 2. Crear el VPC

En la consola de AWS, navegue hasta VPC > VPC Dashboard > Create VPC.

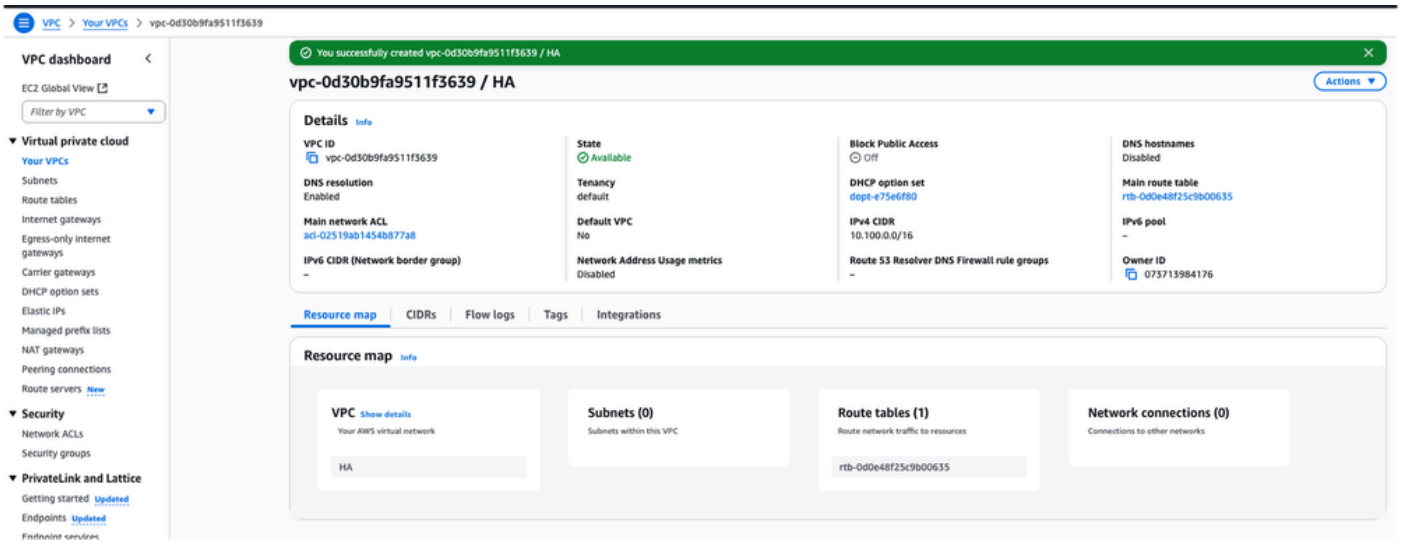


Cuando cree el VPC, seleccione la opción VPC only. Puede asignar una red /16 para que la utilice como desee.

En esta guía de implementación, se selecciona la red 10.100.0.0/16:

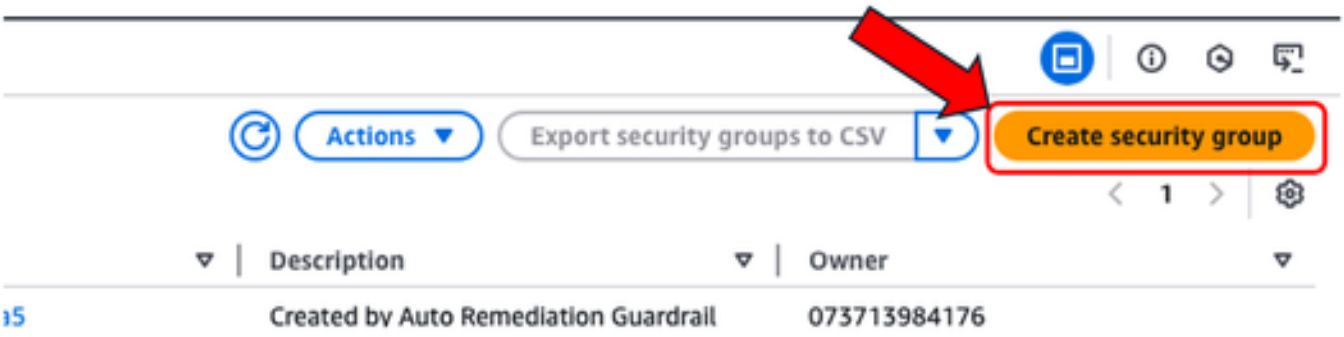


Después de hacer clic en Create VPC, el VPC-0d30b9fa9511f3639 con etiqueta HA ahora se crea:

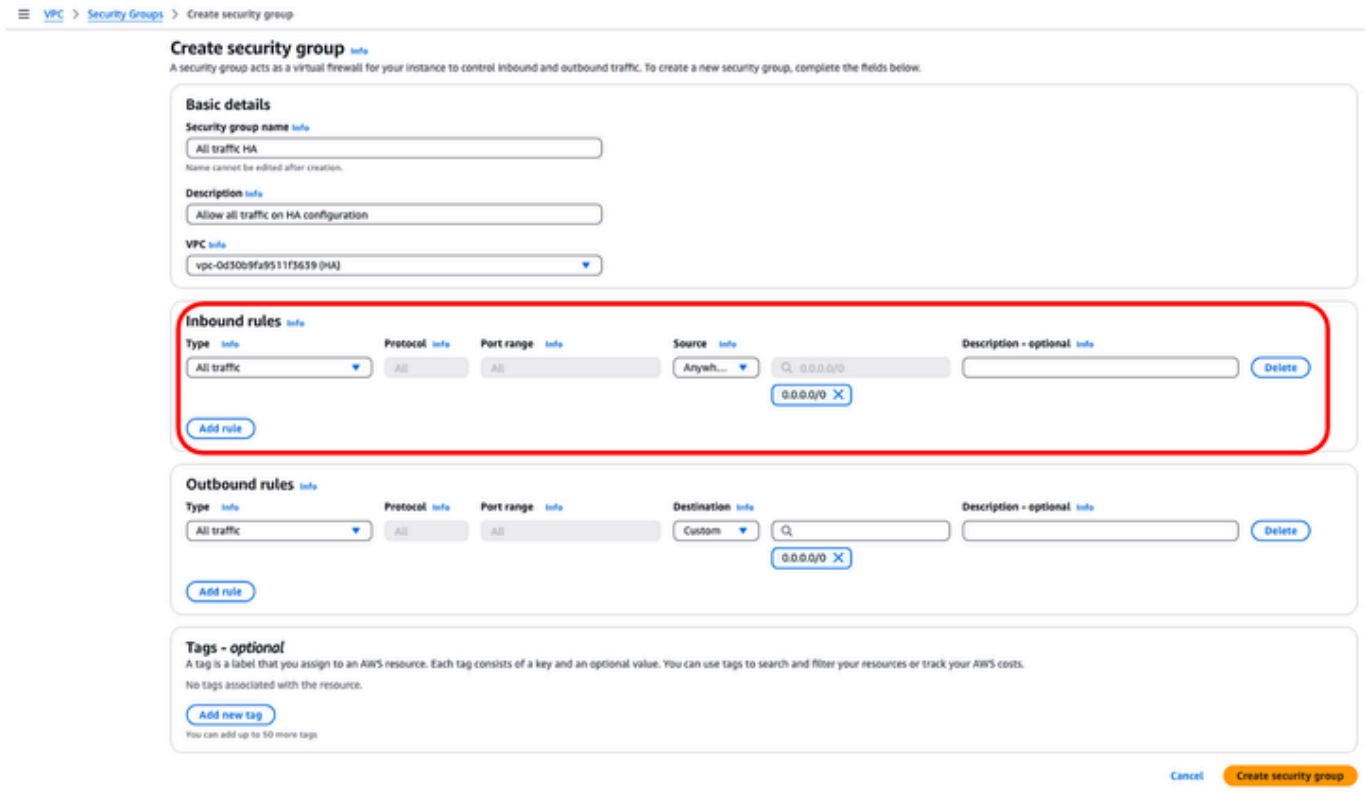


Paso 3. Crear un grupo de seguridad para VPC

En AWS, los grupos de seguridad funcionan como ACL, lo que permite o deniega el tráfico a las VM configuradas dentro de una VPC. En la consola de AWS, navegue hasta la sección VPC > VPC Dashboard > Security > Security Groups y haga clic en Create security group .



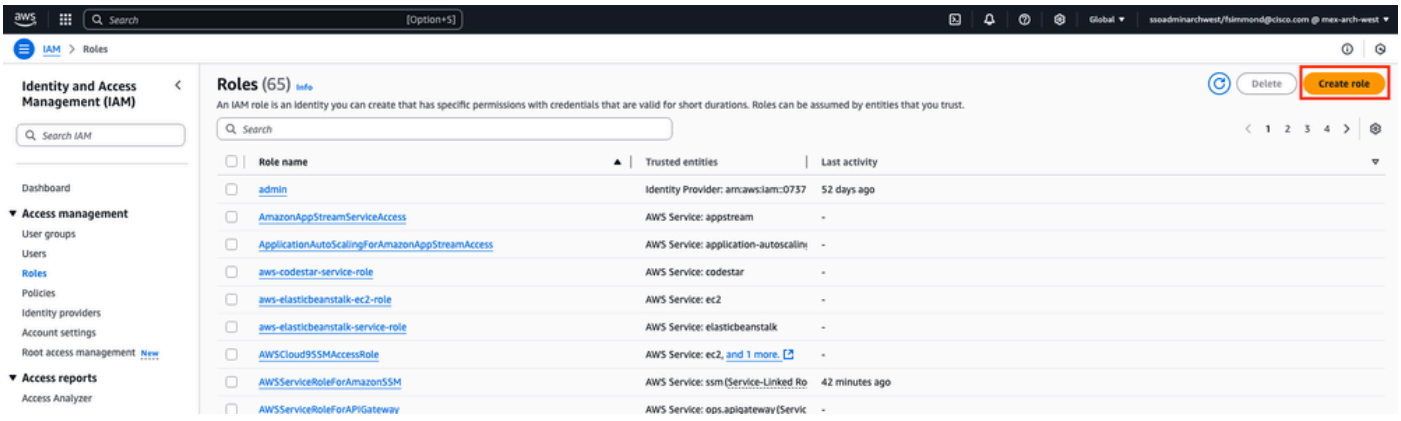
En Reglas de entrada, defina el tráfico que desea permitir. Para este ejemplo, Todo el tráfico se selecciona mediante la red 0.0.0.0/0.



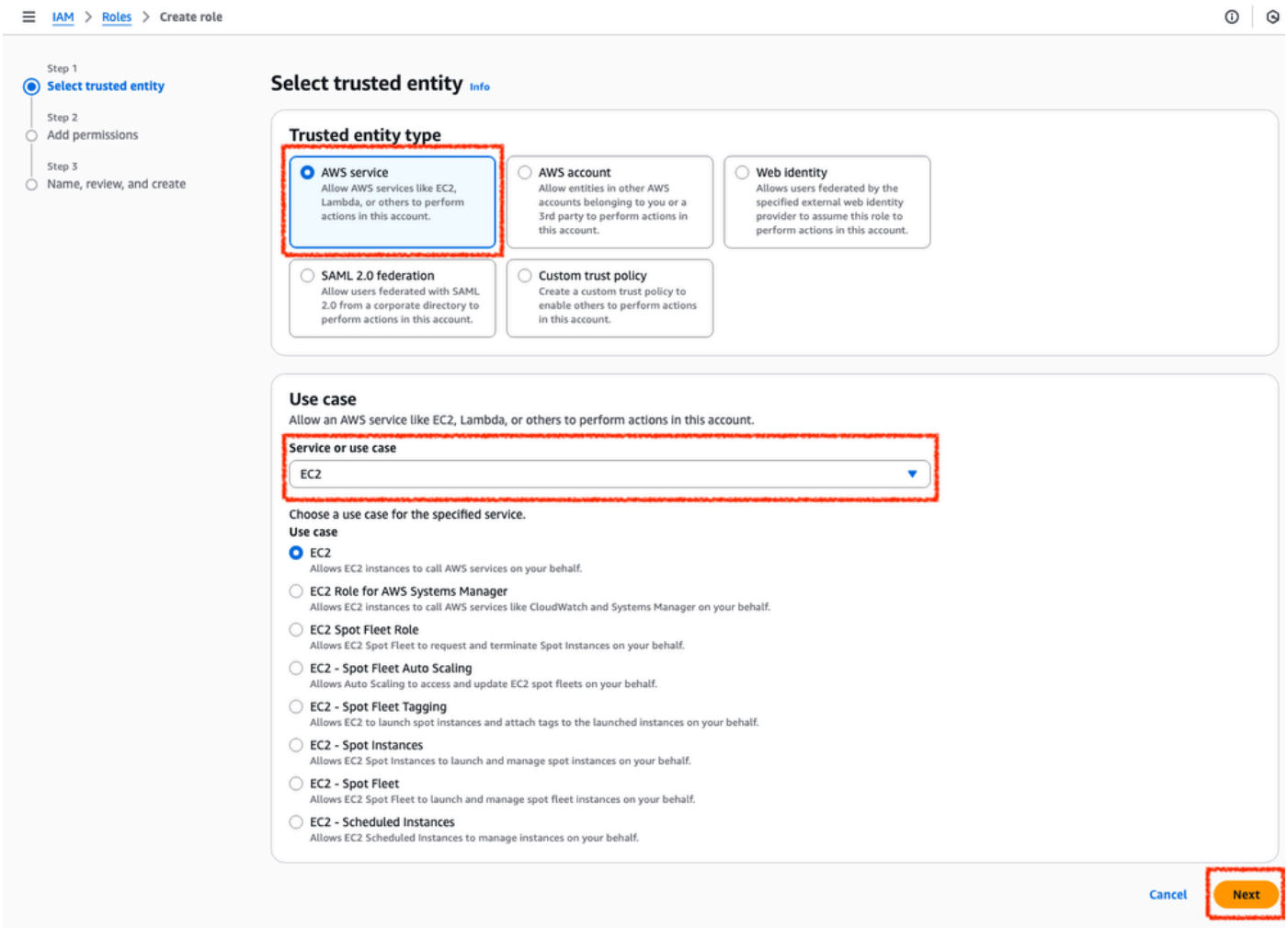
Paso 4. Crear un rol de IAM con una política y asociarlo a VPC

IAM otorga a sus AMI el acceso necesario a las API de Amazon. El C8000v se utiliza como proxy para llamar a los comandos API de AWS para modificar la tabla de rutas en AWS. De forma predeterminada, las instancias EC2 no tienen permiso para acceder a las API. Por este motivo, se debe crear una nueva función IAM que se aplicará durante las creaciones de AMI.

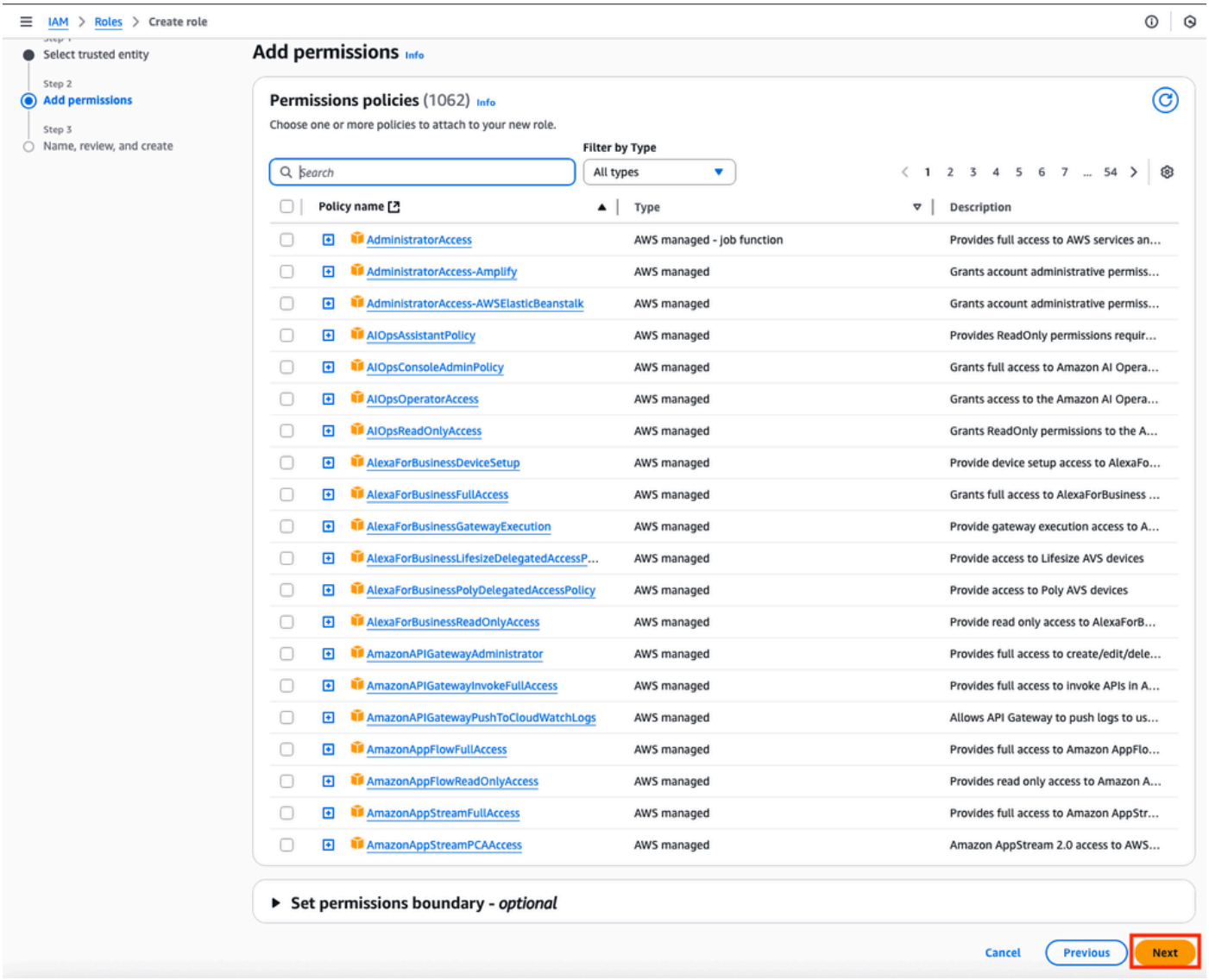
Vaya al panel de IAM y vaya a Access Management > Roles > Create Role. Este proceso consta de 3 pasos:



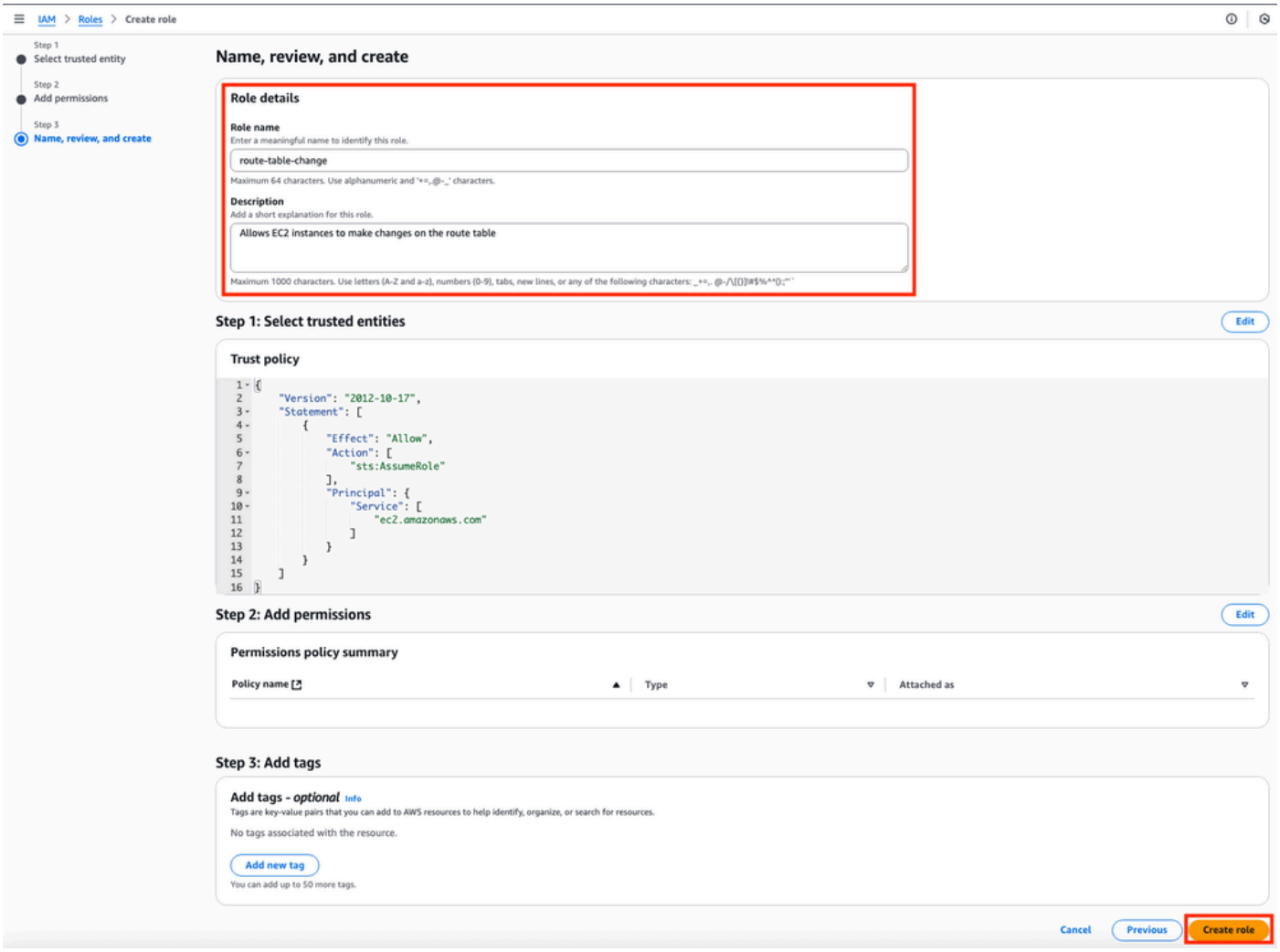
Primero, seleccione la opción AWS Service en la sección Trusted entity type y EC2 como el servicio asignado para esta política.



Cuando haya terminado, haga clic en Next:

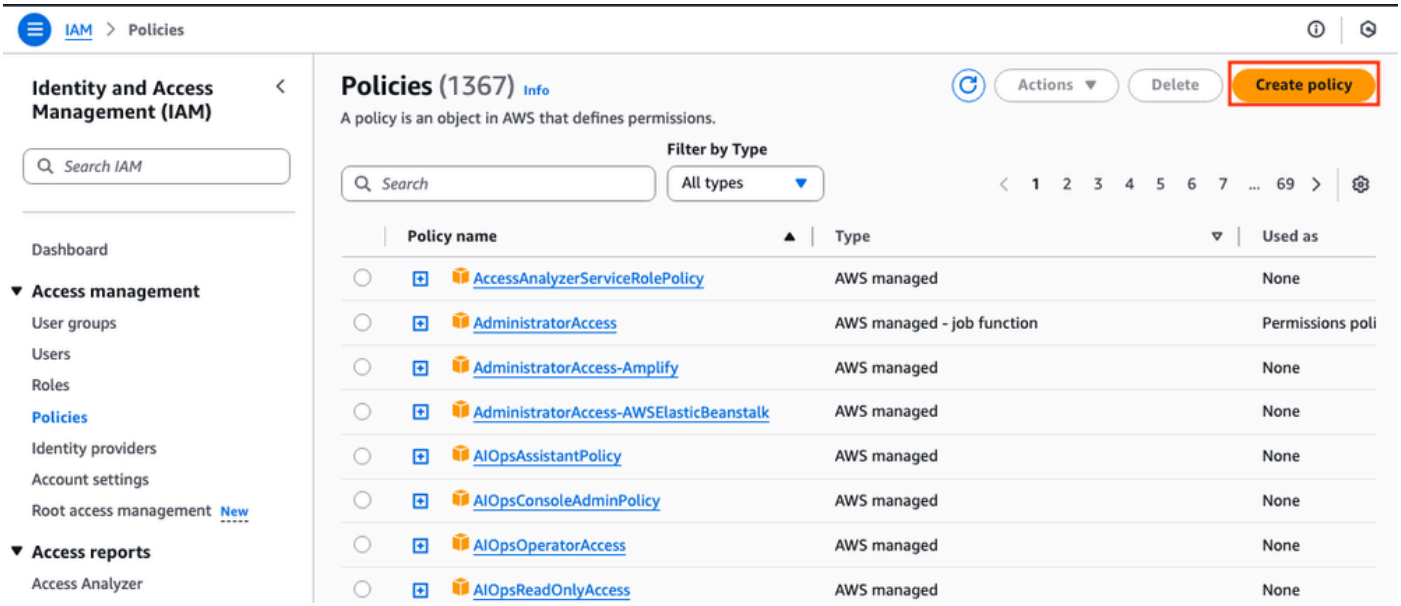


Por último, establezca el nombre del rol y haga clic en el botón Create Role.

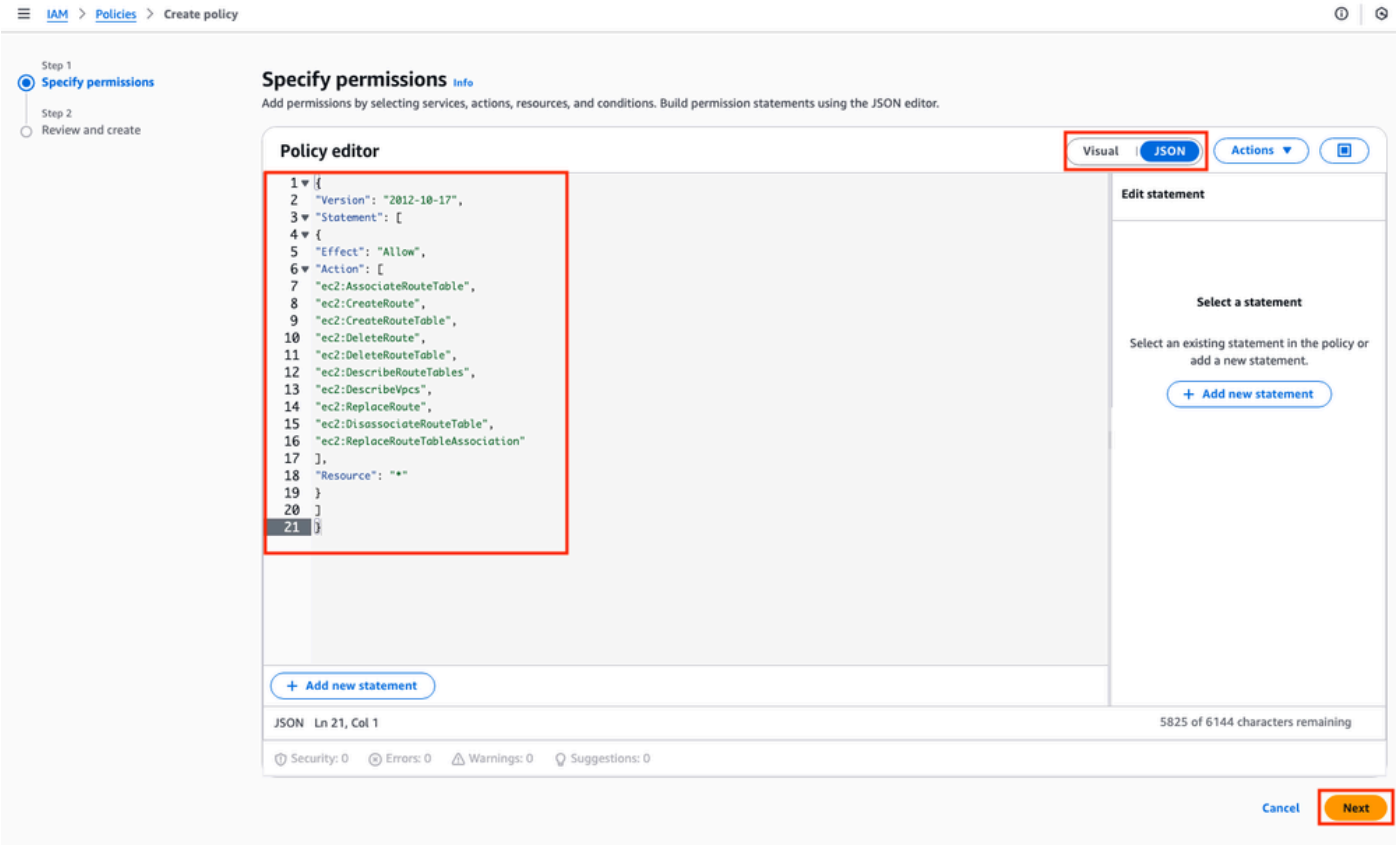


Paso 5. Crear y adjuntar una política de confianza a un rol de IAM

Una vez creado el rol, se debe crear una política de confianza para adquirir la habilidad de modificar las tablas de ruteo de AWS cuando sea necesario. Vaya a la sección Directivas del panel de IAM. Haga clic en el botón Create Policy. Este proceso consta de 2 pasos:



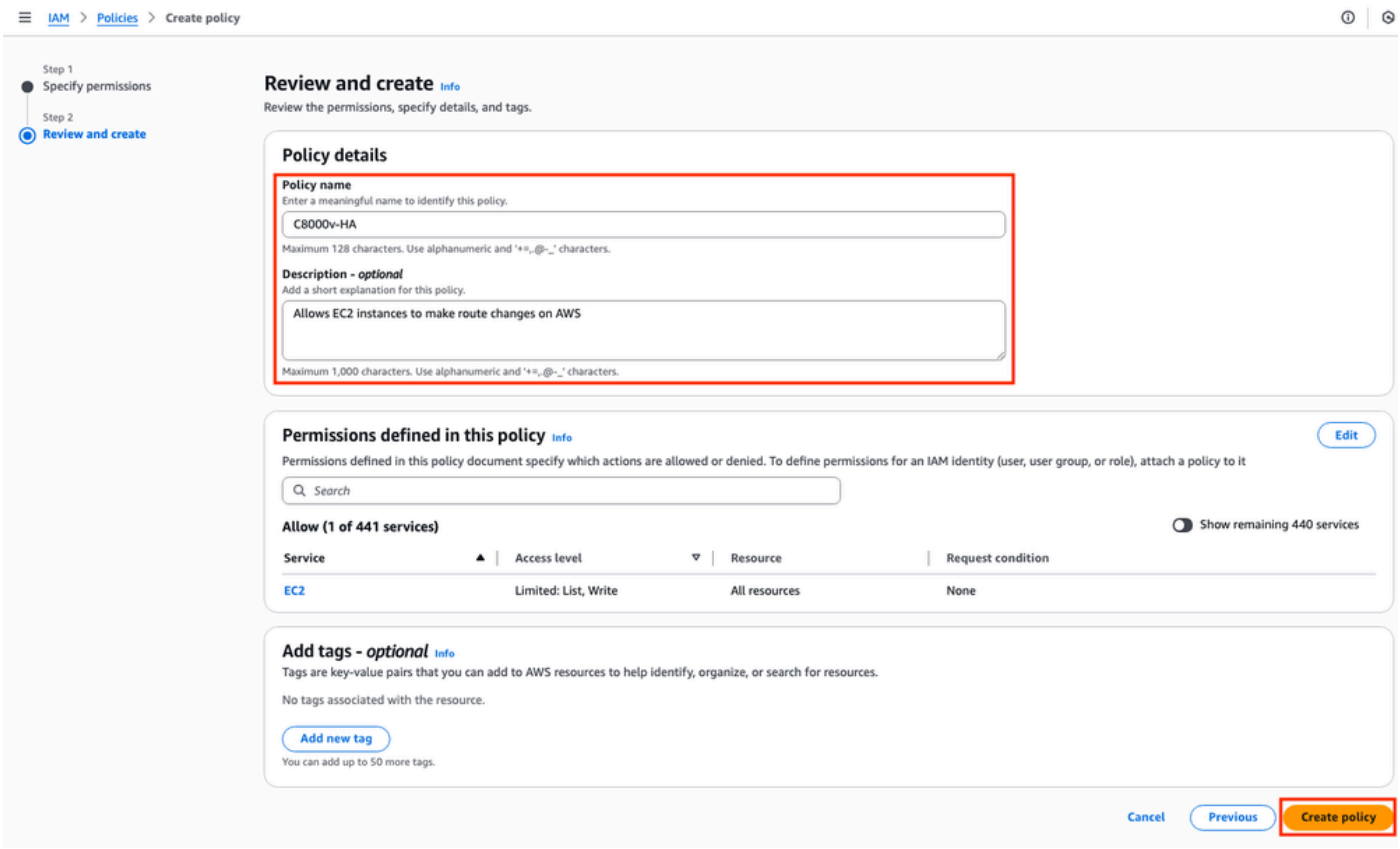
En primer lugar, asegúrese de que el Editor de directivas esté utilizando JSON y aplique los comandos que se muestran a continuación. Una vez configurado, haga clic en Next:



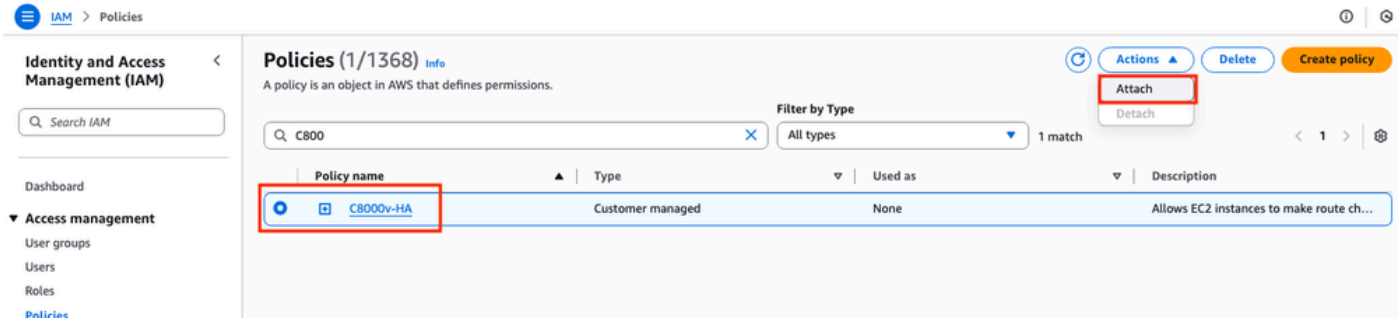
Este es el código de texto utilizado en la imagen:

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

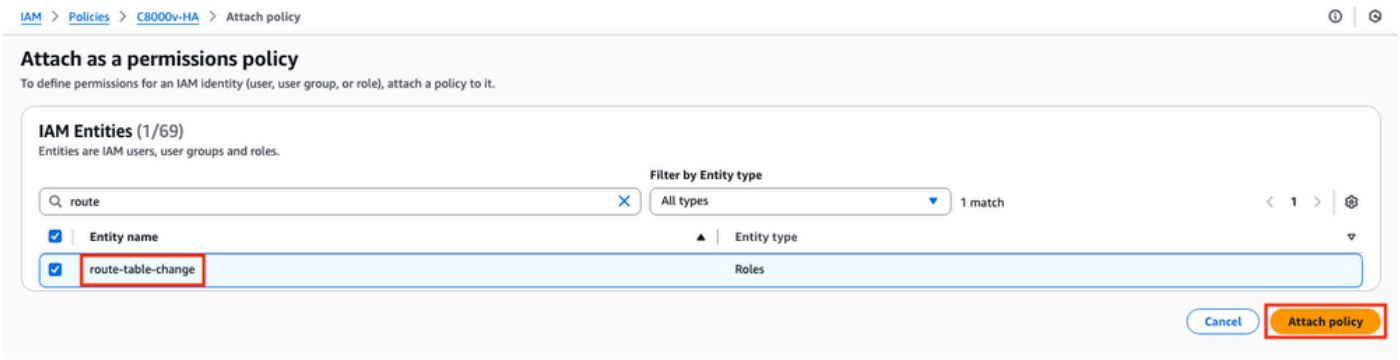
Más adelante, establezca el Nombre de directiva y haga clic en Crear directiva.



Una vez creada la directiva, filtre y seleccione la directiva y, a continuación, haga clic en la opción Adjuntar del menú desplegable Acciones.



Hay una nueva ventana abierta. En la sección Entidades IAM, filtre y seleccione el Rol IAM creado y haga clic en Adjuntar directiva.

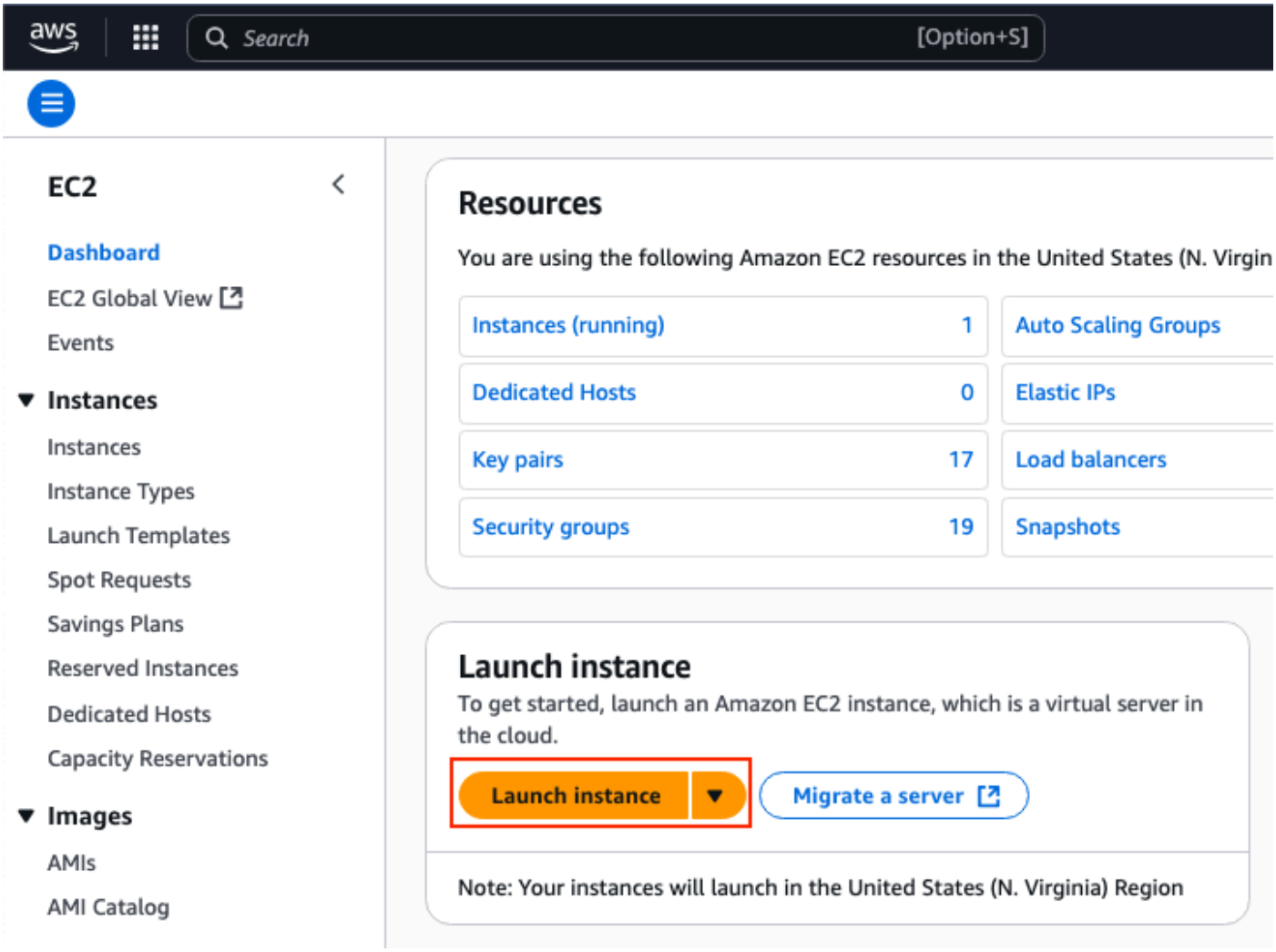


Paso 6.Configuración e inicio de las instancias de C8000v

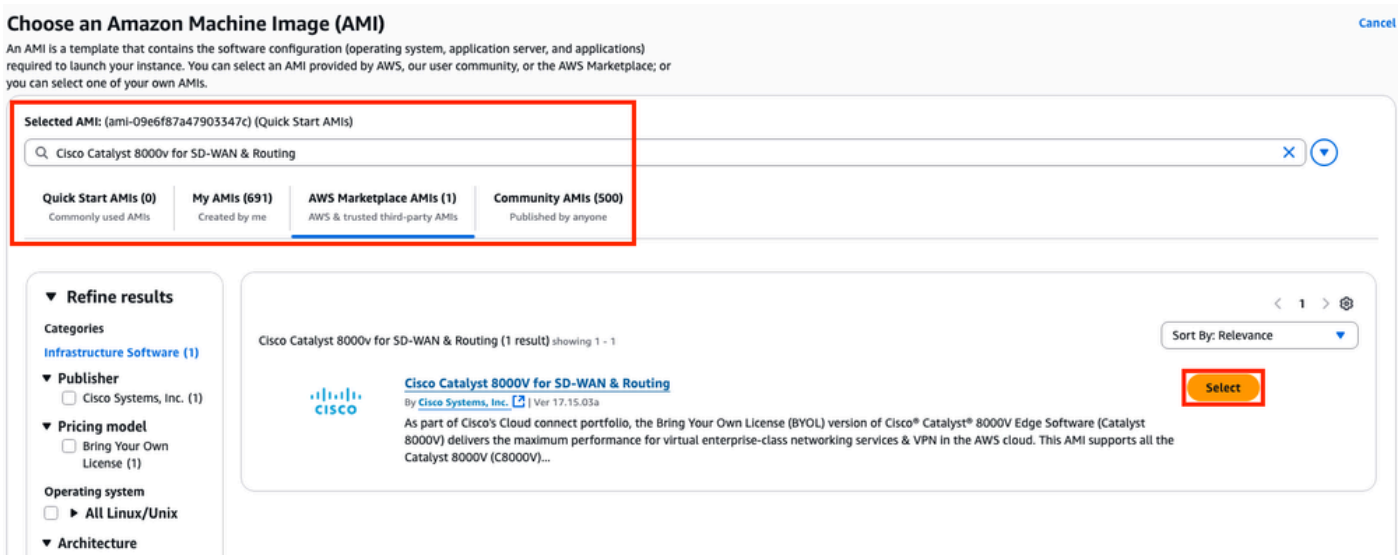
Cada router C8000v va a tener 2 interfaces (1 pública y 1 privada) y se va a crear en su propia

zona de disponibilidad.

En el Panel EC2, haga clic en Iniciar instancias:

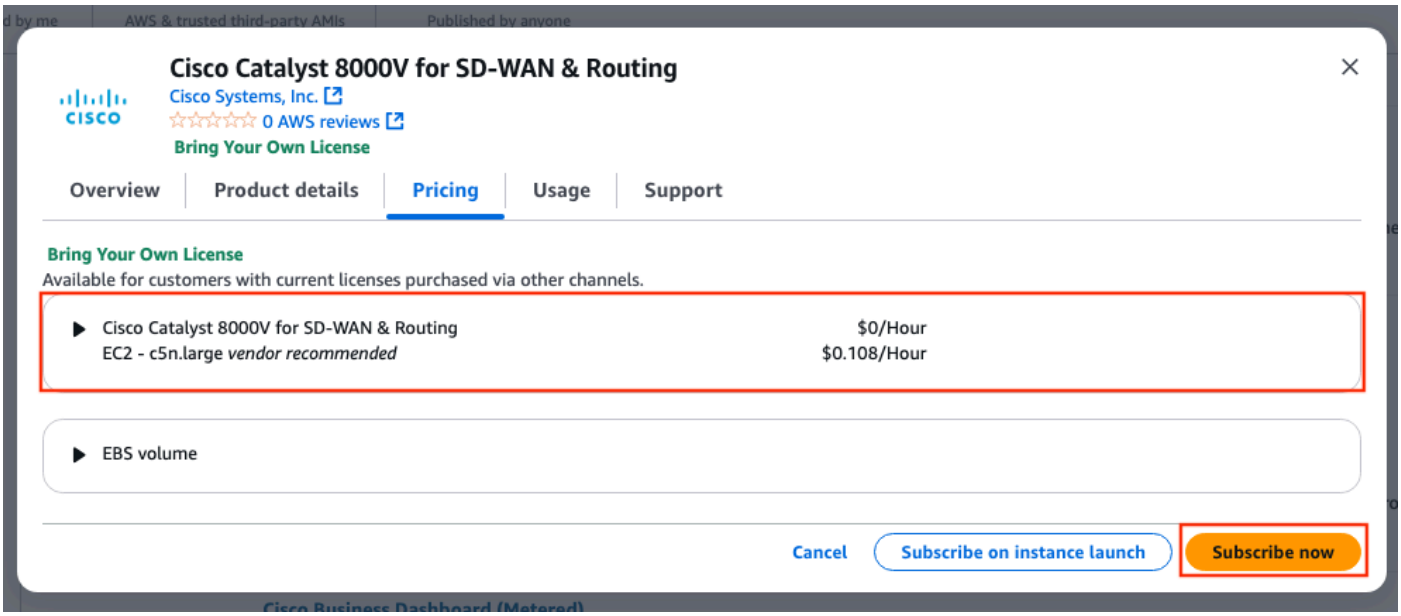


Filtre la base de datos de AMI con el nombre Cisco Catalyst 8000v para SD-WAN y routing. En la lista AMI de AWS Marketplace, haga clic en Seleccionar.



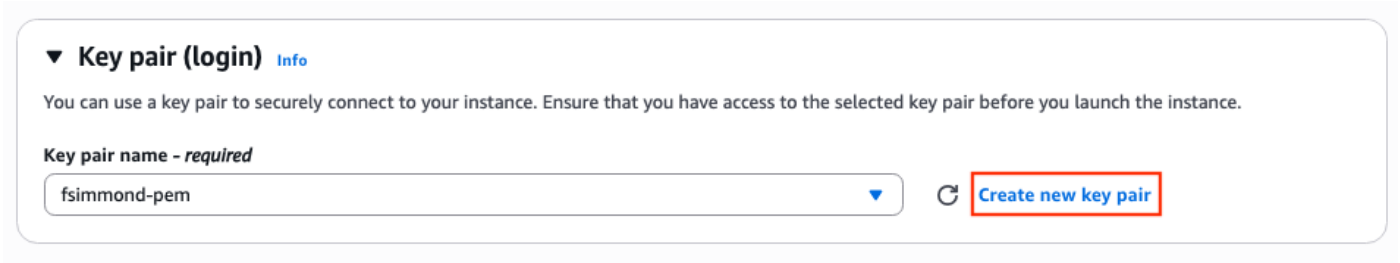
Seleccione el tamaño correspondiente para el AMI. Para este ejemplo, se selecciona el tamaño

c5n.large. Esto puede depender de la capacidad necesaria para la red. Una vez seleccionado, haga clic en Suscribirse ahora.

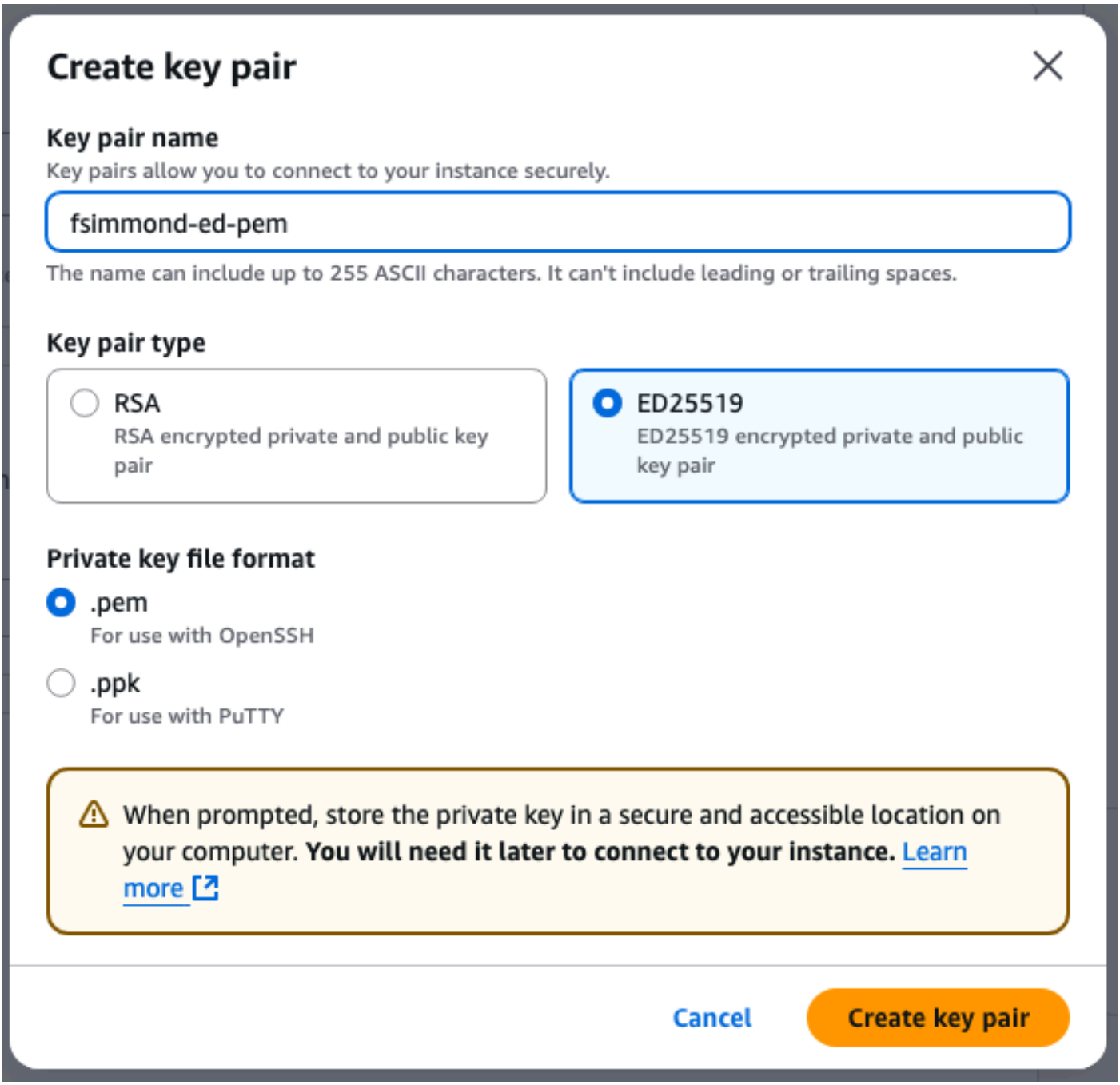


Paso 6.1. Configuración del par de claves para el acceso remoto

Una vez suscrito al AMI, se muestra una nueva ventana con varias opciones. En la sección Par de claves (inicio de sesión), si no hay ninguno, haga clic en Crear nuevo par de claves. Puede reutilizar una sola clave para cada dispositivo creado.



Se muestra una nueva ventana emergente. Para este ejemplo, se crea un archivo de clave .pem con cifrado ED25519. Una vez que todo esté configurado, haga clic en Create key pair.



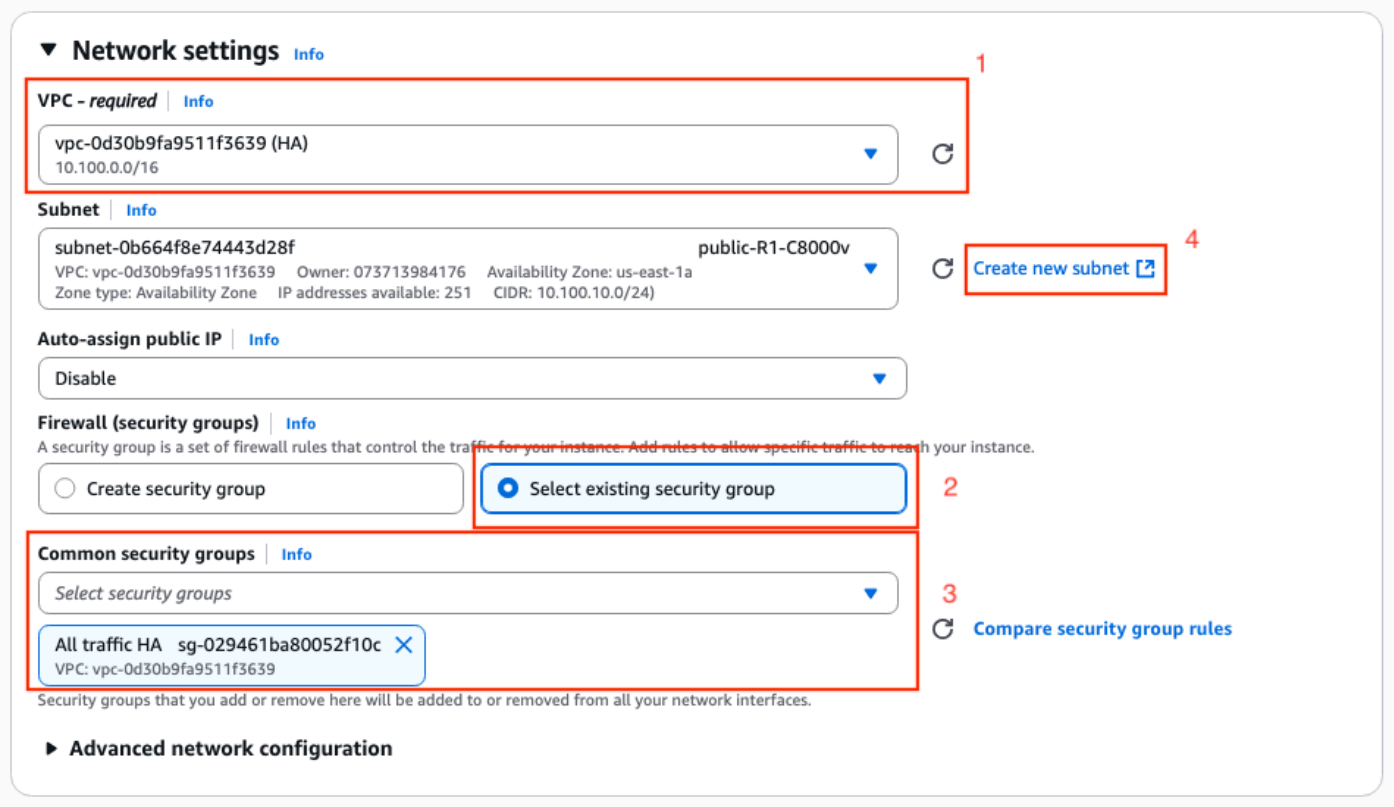
Paso 6.2. Crear y configurar las subredes para el AMI

En la sección Configuración de red, haga clic en Editar. Ahora hay disponibles algunas opciones nuevas dentro de la sección:
1. Seleccione el VPC deseado para este trabajo. Para este ejemplo, se selecciona el VPC llamado HA.

2. En la sección Firewall (grupos de seguridad), seleccione Seleccionar grupo de seguridad existente.

3. Una vez seleccionada la opción 2, está disponible la opción Grupos de seguridad comunes. Filtre y seleccione el grupo de seguridad deseado. Para este ejemplo, se selecciona el grupo de seguridad Todo el tráfico HA.

4. (Opcional) Si no se crean subredes para estos dispositivos, haga clic en Create new subnet.



Se abre una nueva pestaña en el navegador web, que le lleva a la sección Crear subred:

1. Seleccione el VPC correspondiente para esta configuración de la lista desplegable.

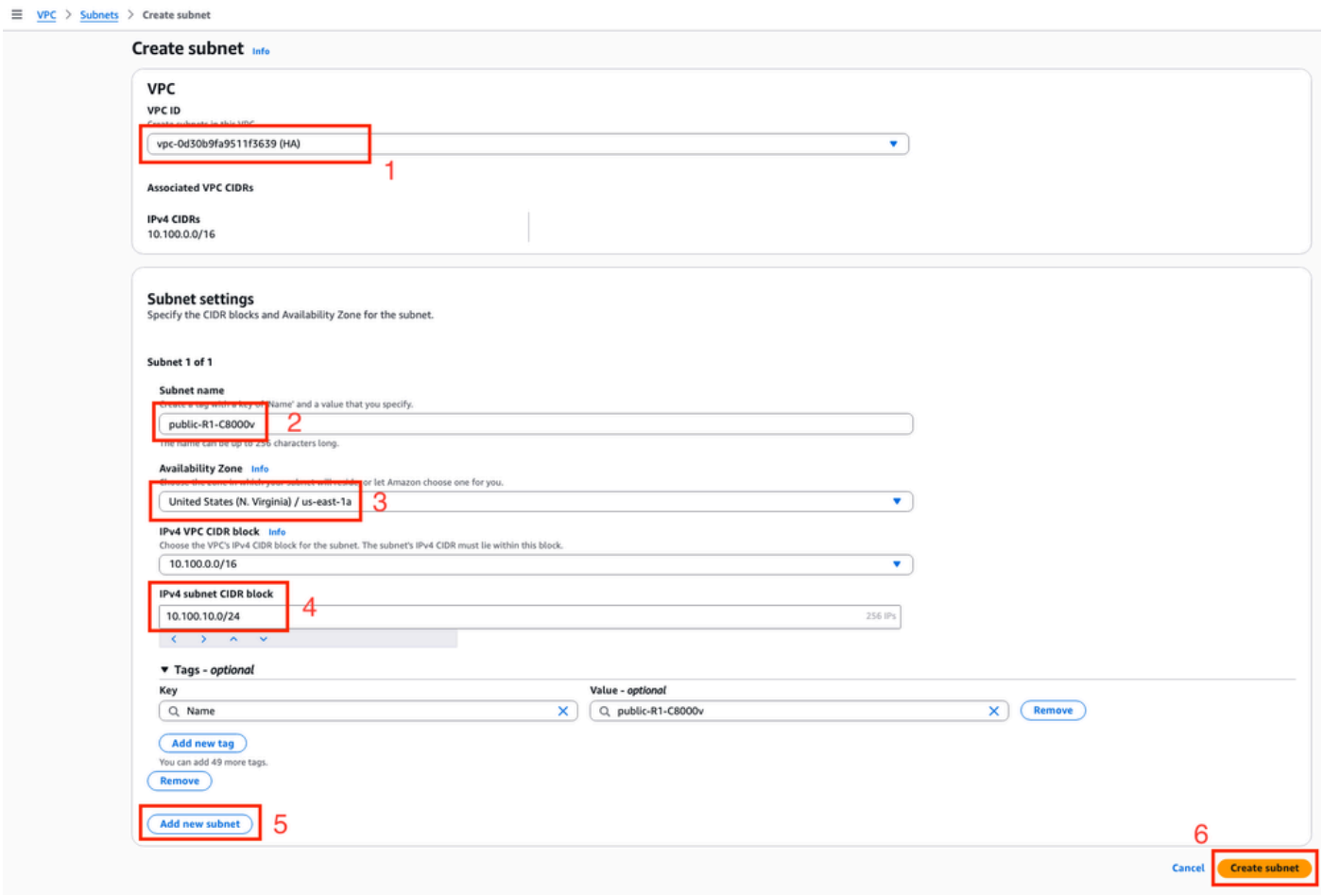
2. Establezca un nombre para la nueva subred.

3. Defina la zona de disponibilidad para esta subred. (Consulte la sección Topología de este documento para obtener más información sobre la configuración)

4. Establezca el bloque de subred que pertenece al bloque CIDR de VPC.

5. Además, todas las subredes que se van a utilizar se pueden crear haciendo clic en la sección Agregar nueva subred y repita los pasos del 2 al 4 para cada subred.

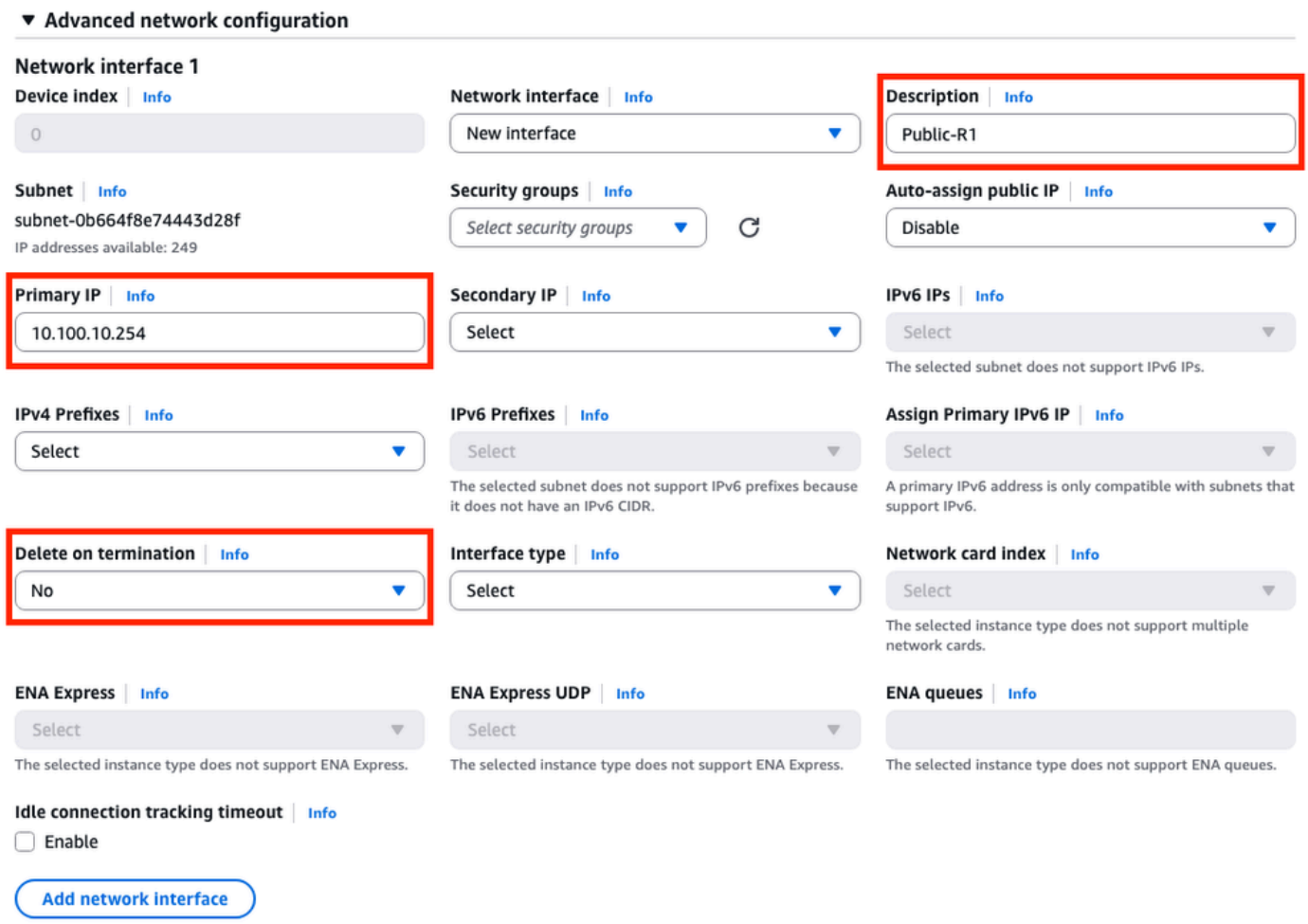
6. Una vez finalizado, haga clic en Create subnet. Vaya a la página anterior para continuar con la configuración.



En la subsección Subnet de la sección Network Settings, haga clic en el icono Refresh para obtener las subredes creadas en la lista desplegable.

Paso 6.3. Configuración de las interfaces AMI

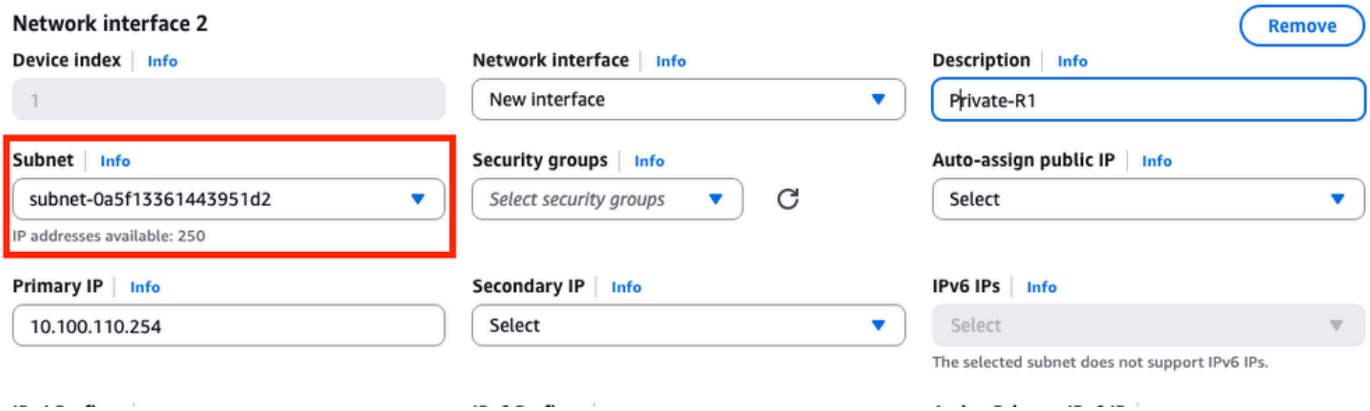
En la sección Network Settings, expanda la subsección Advanced Network configuration. Se muestran estas opciones:



En este menú, establezca los parámetros Description, Primary IP, Delete on termination. Para el parámetro Primary IP, utilice cualquier dirección IP excepto la primera dirección disponible de la subred. AWS lo utiliza internamente.

El parámetro Delete on termination de este ejemplo se establece como No. Sin embargo, se puede establecer en sí dependiendo de su entorno.

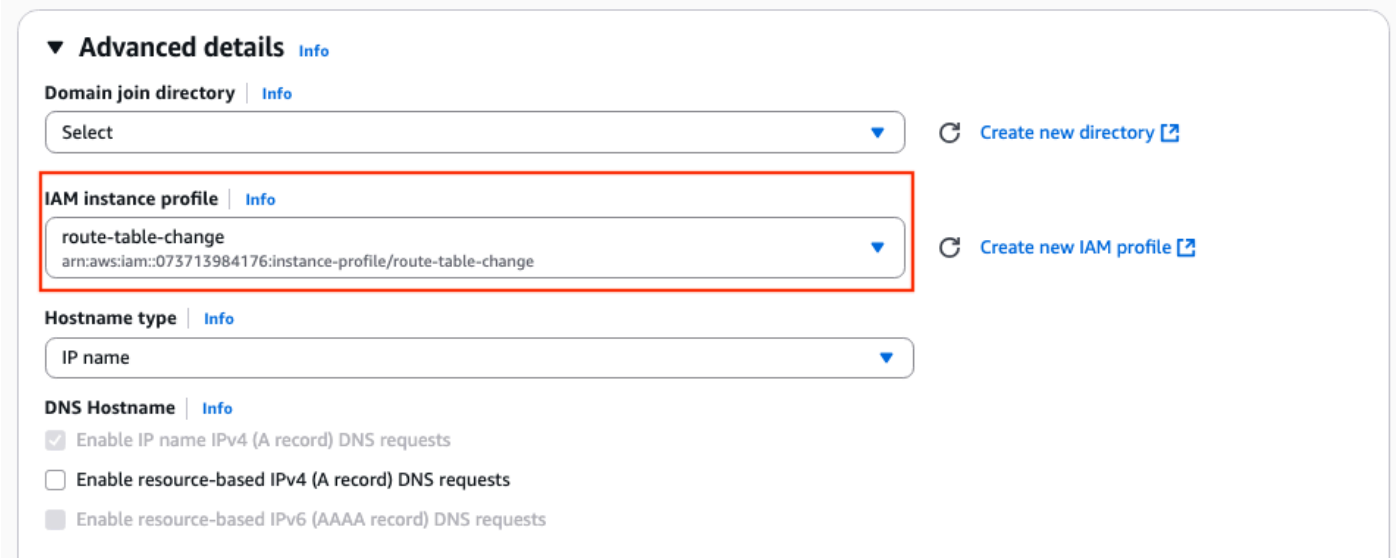
Debido a esta topología, se necesita una segunda interfaz para la subred privada. Haga clic en Add network interface y se mostrará este mensaje. Sin embargo, la interfaz proporciona la opción de seleccionar la subred esta vez:



Una vez que todos los parámetros se hayan configurado como se realizó en la Interfaz de red 1, continúe con los siguientes pasos.

Paso 6.4. Establecer el perfil de instancia de IAM en el AMI

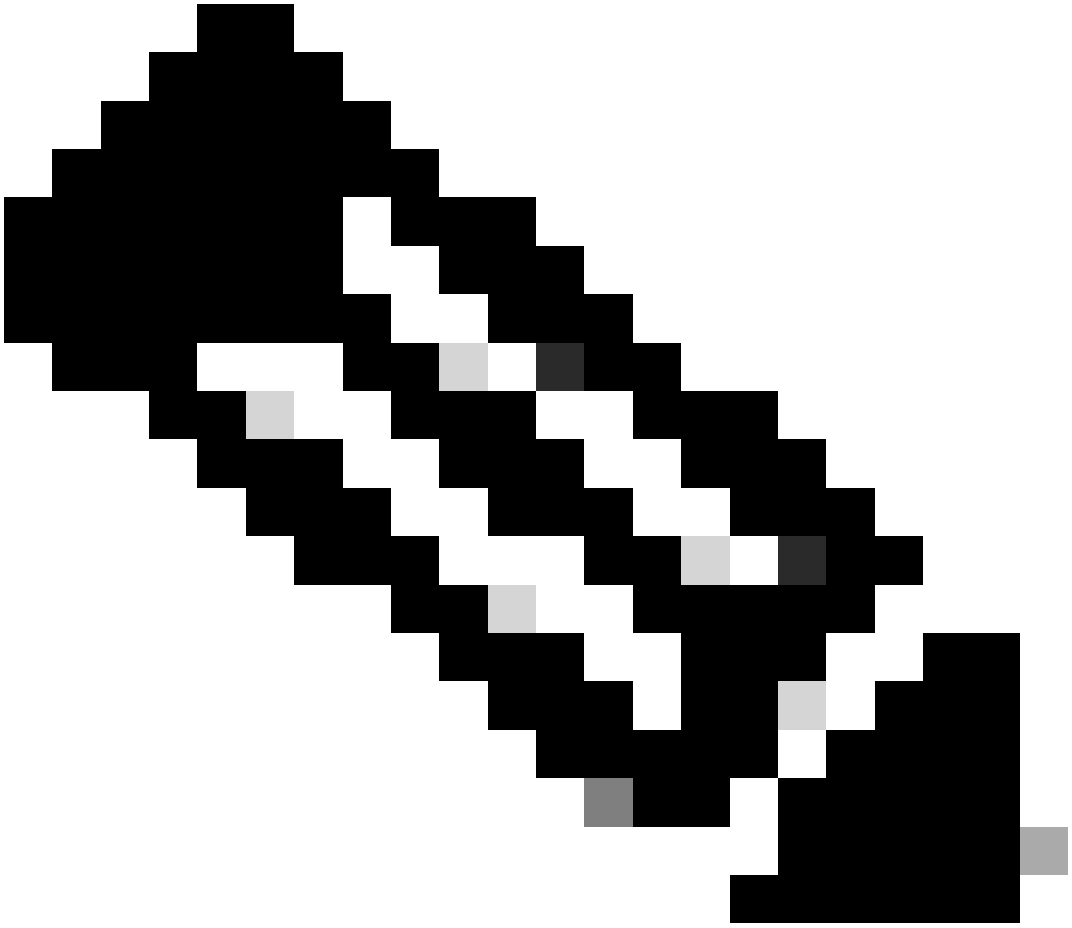
En la sección Detalles avanzados, seleccione el rol IAM creado en el parámetro de perfil de instancia de IAM:



Paso 6.5. (Opcional) Establezca las credenciales en el AMI

En la sección Detalles avanzados, navegue hasta la sección Datos de usuario - opcional y aplique esta configuración para establecer un nombre de usuario y una contraseña mientras se crea la instancia:

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



Nota: El nombre de usuario proporcionado por AWS a SSH en el C8000v se puede enumerar incorrectamente como raíz. Cambie esto a ec2-user si es necesario.

Paso 6.6. Finalización de la configuración de la instancia

Una vez que todo esté configurado, haga clic en Iniciar instancia:

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.

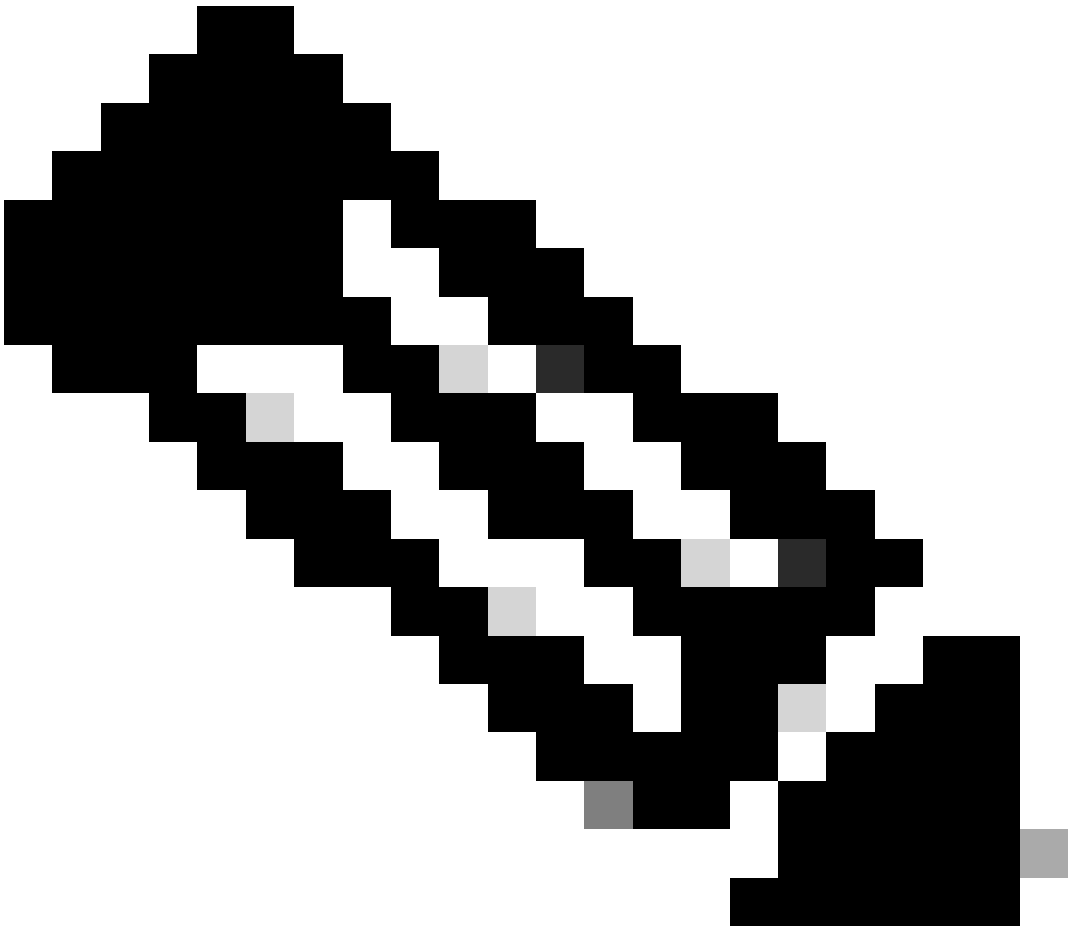
Cancel

Launch instance

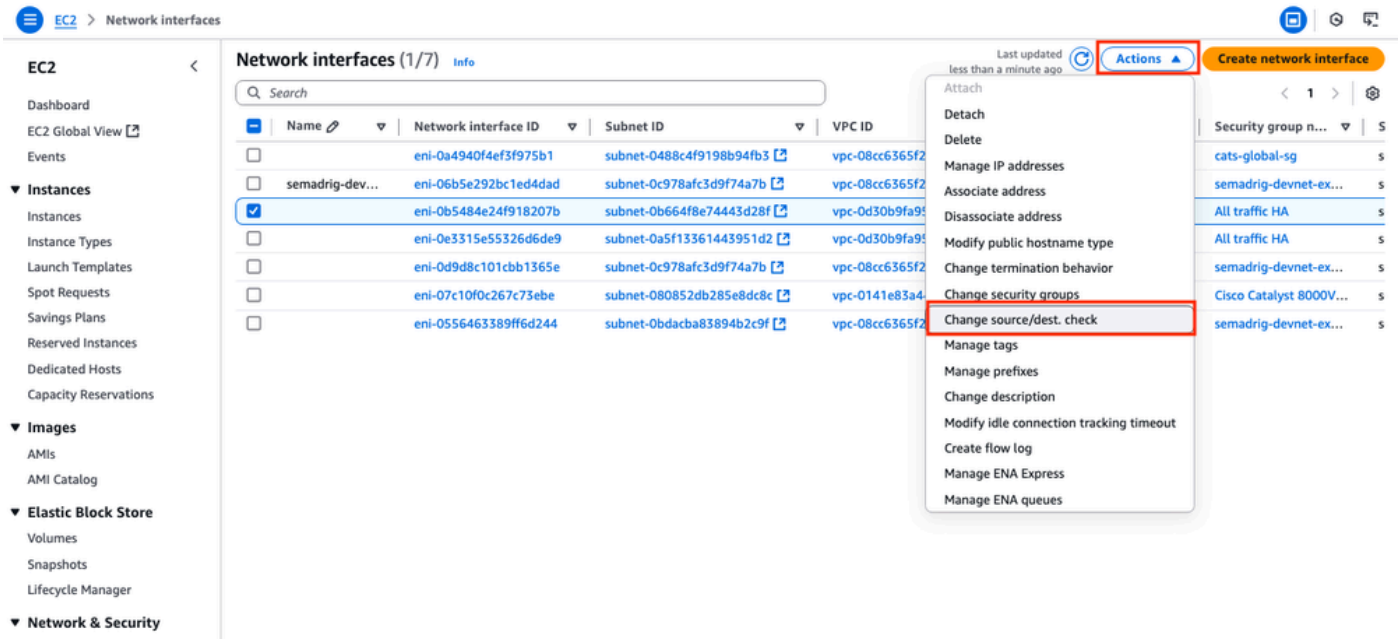
Preview code

Paso 6.7. Inhabilitación de la Verificación de Origen/Destino en los ENI

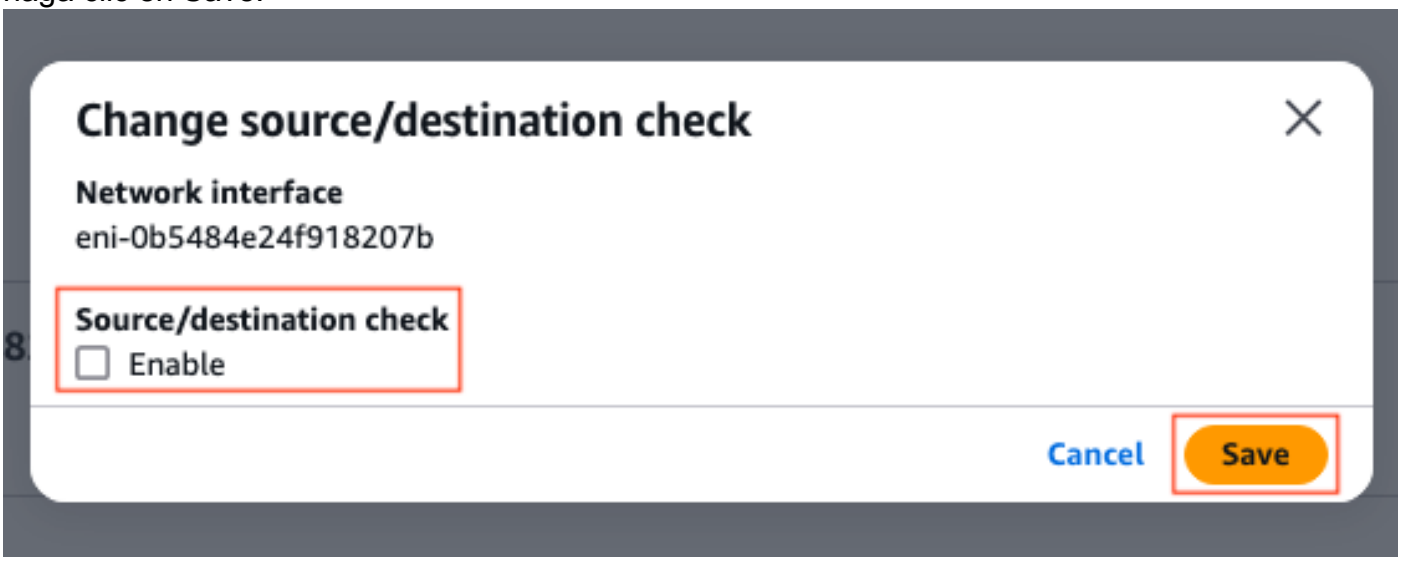
Una vez creada la instancia, inhabilite la funcionalidad de verificación src/dst en AWS para obtener la conectividad entre interfaces en la misma subred. En la sección Panel EC2 > Red y seguridad > Interfaces de red, seleccione las ENIs y haga clic en Acciones > Cambiar origen/destino. comprobar.



Nota: Debe seleccionar las ENI una por una para que esta opción esté disponible.



Se muestra una nueva ventana. En el nuevo menú, desactive la casilla de verificación Enable y haga clic en Save.

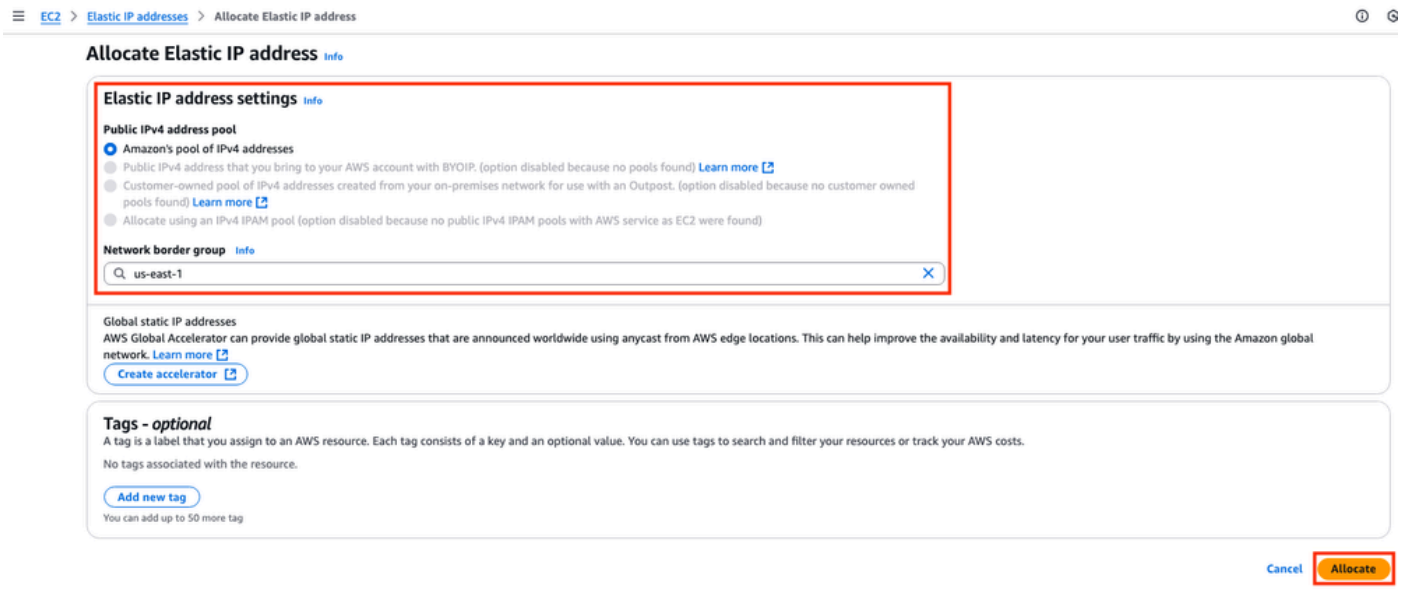


Paso 6.8. Crear y asociar una IP elástica al ENI público de la instancia

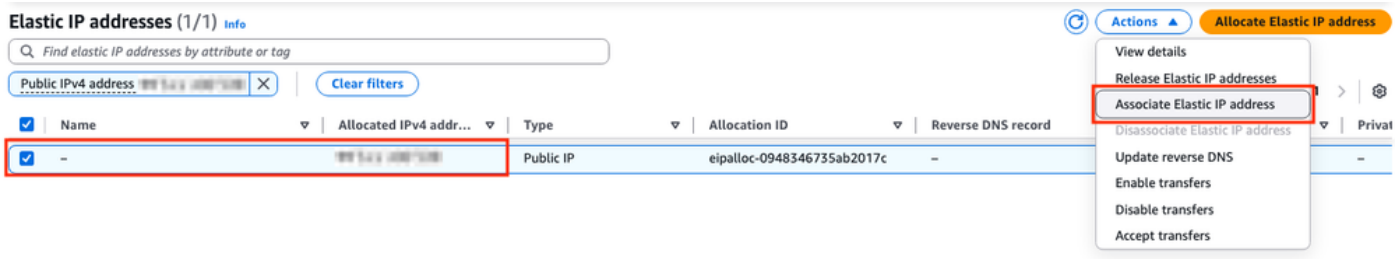
En la sección Panel EC2 > Red y seguridad > IP elásticas, haga clic en Asignar dirección IP elástica.

La página le lleva a la otra sección. Para este ejemplo, se selecciona la opción Grupo de direcciones IPv4 de Amazon junto con la zona de disponibilidad us-east-1. Una vez finalizado,

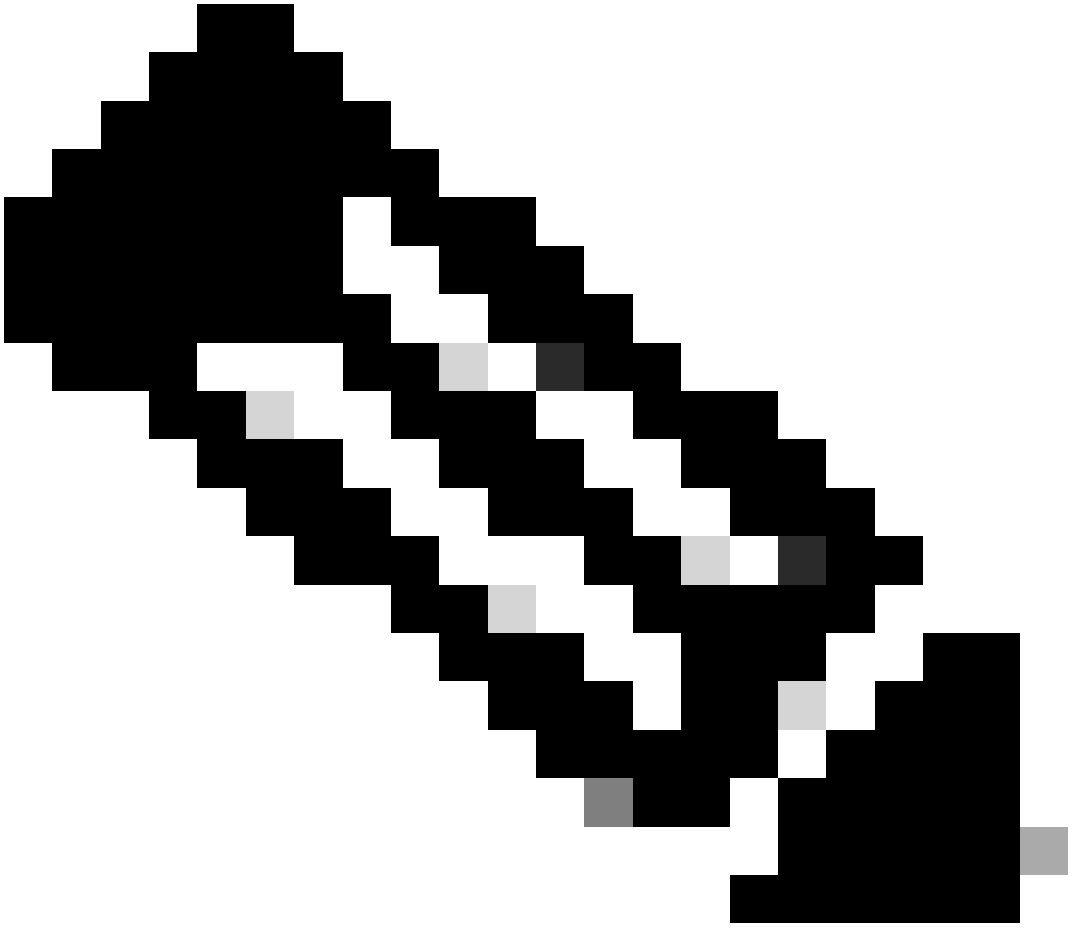
haga clic en Asignar.



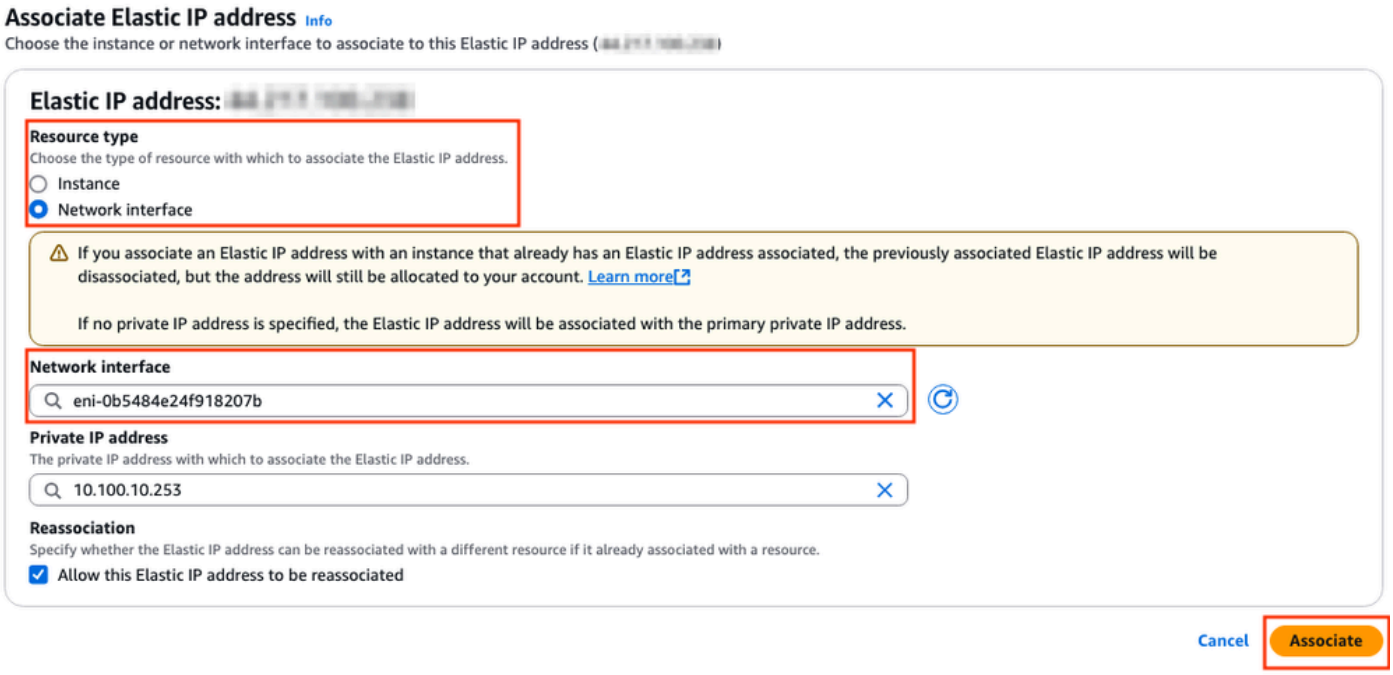
Cuando se cree la dirección IP, asígnela a la interfaz pública de la instancia. En la sección Panel EC2 > Red y seguridad > IP elásticas, haga clic en Acciones > Asociar dirección IP elástica.



En esta nueva sección, seleccione la opción Network interface y busque el ENI público de la interfaz correspondiente. Asocie la dirección IP pública correspondiente y haga clic en Associate.



Nota: Para obtener la ID de ENI adecuada, navegue hasta la sección Panel EC2 > Instancias. A continuación, seleccione la instancia y compruebe la sección Networking. Busque la dirección IP de su interfaz pública para obtener el valor ENI en la misma fila.



Paso 7. Repita el paso 6 para crear la segunda instancia de C8000v para HA

Consulte la sección Topología de este documento para obtener la información correspondiente para cada interfaz y repita los mismos pasos de 6.1 a 6.6.

Paso 8. Repita el paso 6 para crear una máquina virtual (Linux/Windows) desde AMI Marketplace

Para este ejemplo, el servidor Ubuntu 22.04.5 LTS se selecciona del AMI Marketplace como el host interno.

ens5 se crea de forma predeterminada para la interfaz pública. Para este ejemplo, cree una segunda interfaz (ens6 en el dispositivo) para la subred 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
```

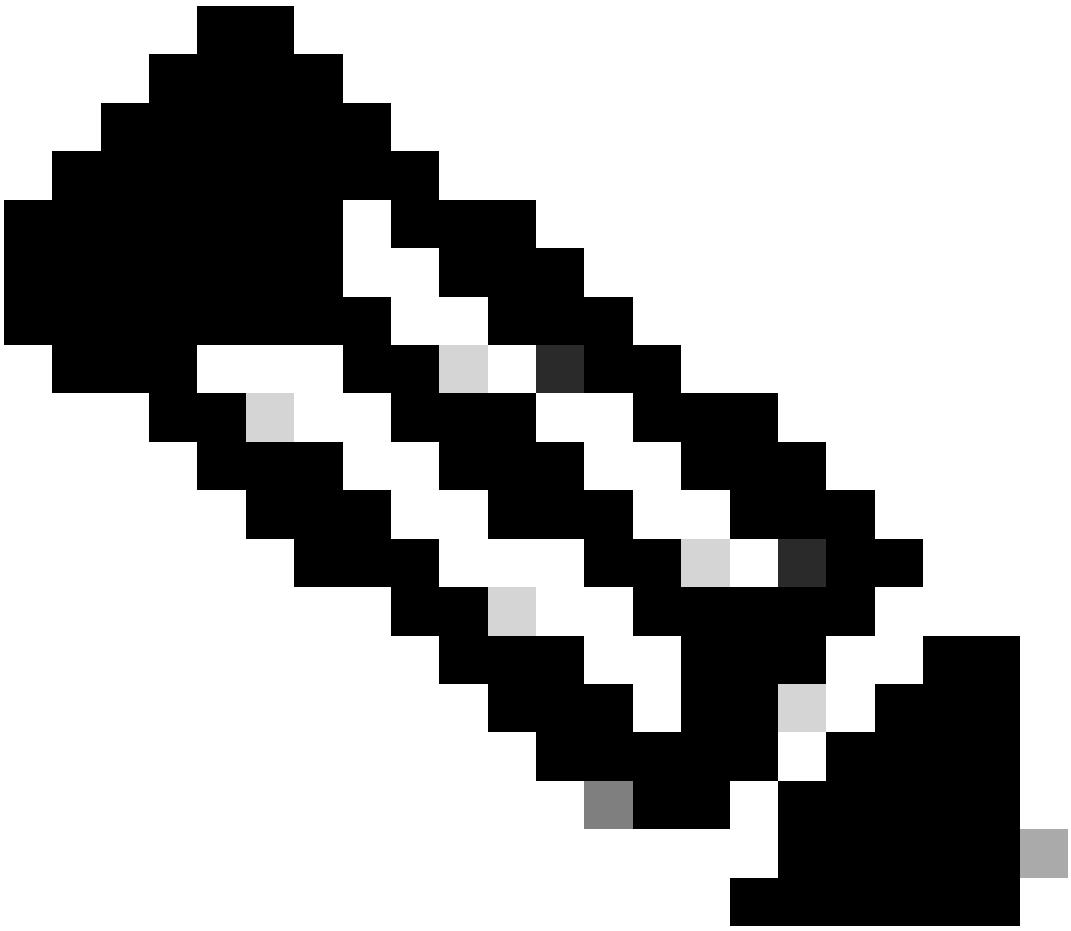
10.100.30.254

```
 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
```

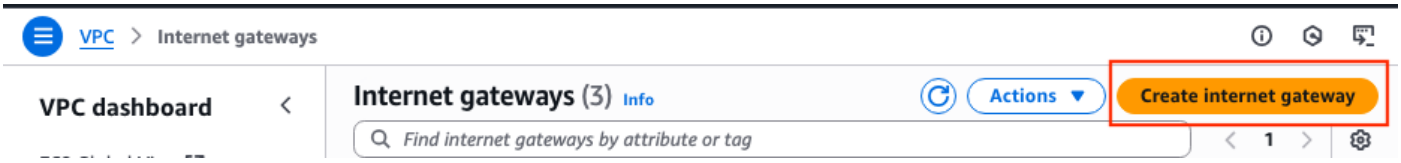


> Nota: Si se realiza algún cambio en las interfaces, agite la interfaz o recargue la VM para que se apliquen estos cambios.

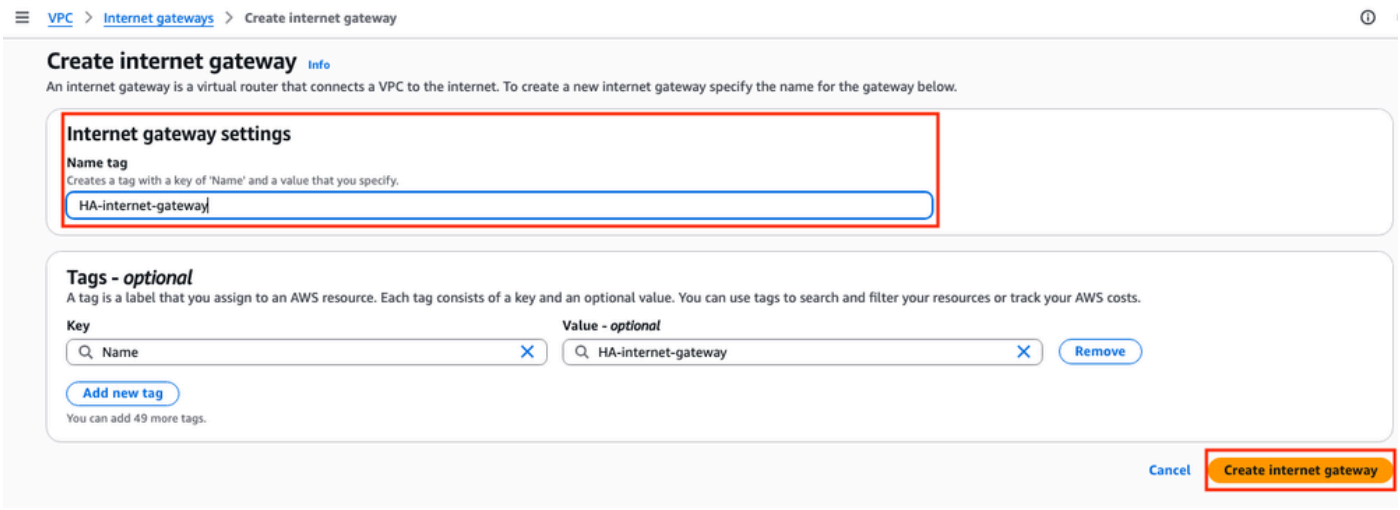
Paso 9. Creación y configuración de una puerta de enlace a Internet (IGW) para VPC

En la sección **VPC Dashboard > Virtual private cloud > Internet gateways**, haga clic en

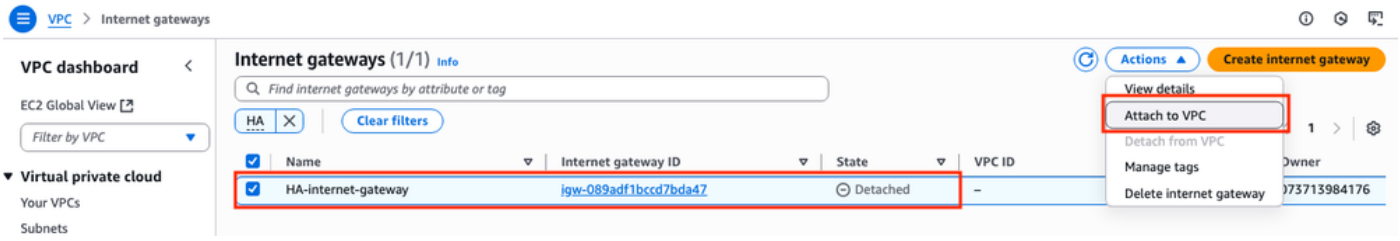
Create internet gateway.



En esta nueva sección, cree una **etiqueta name** para este gateway y haga clic en **Create internet gateway**.

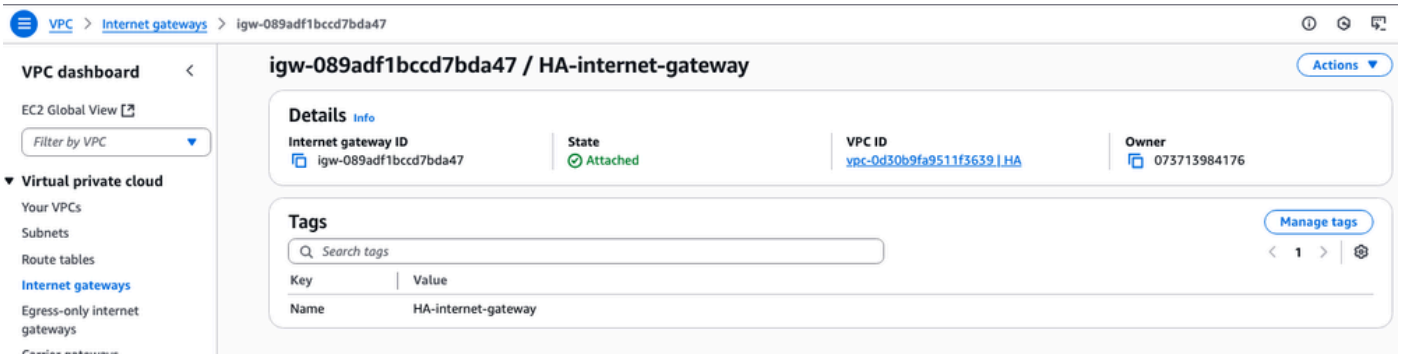


Una vez creado el IGW, adjúntelo a su VPC correspondiente. Vaya a la sección **Panel de VPC > Nube privada virtual > Gateway de Internet** y seleccione el IGW correspondiente. Haga clic en **Acciones > Adjuntar a VPC**.



En esta nueva sección, seleccione el VPC llamado **HA**. Para este ejemplo, haga clic en **Adjuntar gateway de Internet**.

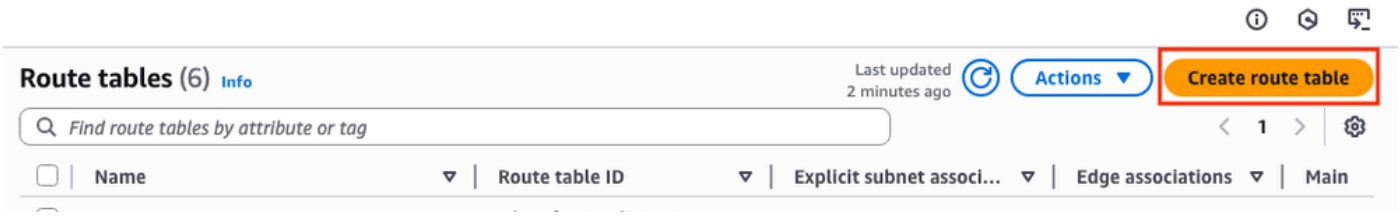
El IGW debe indicar el estado Adjunto tal como se muestra:



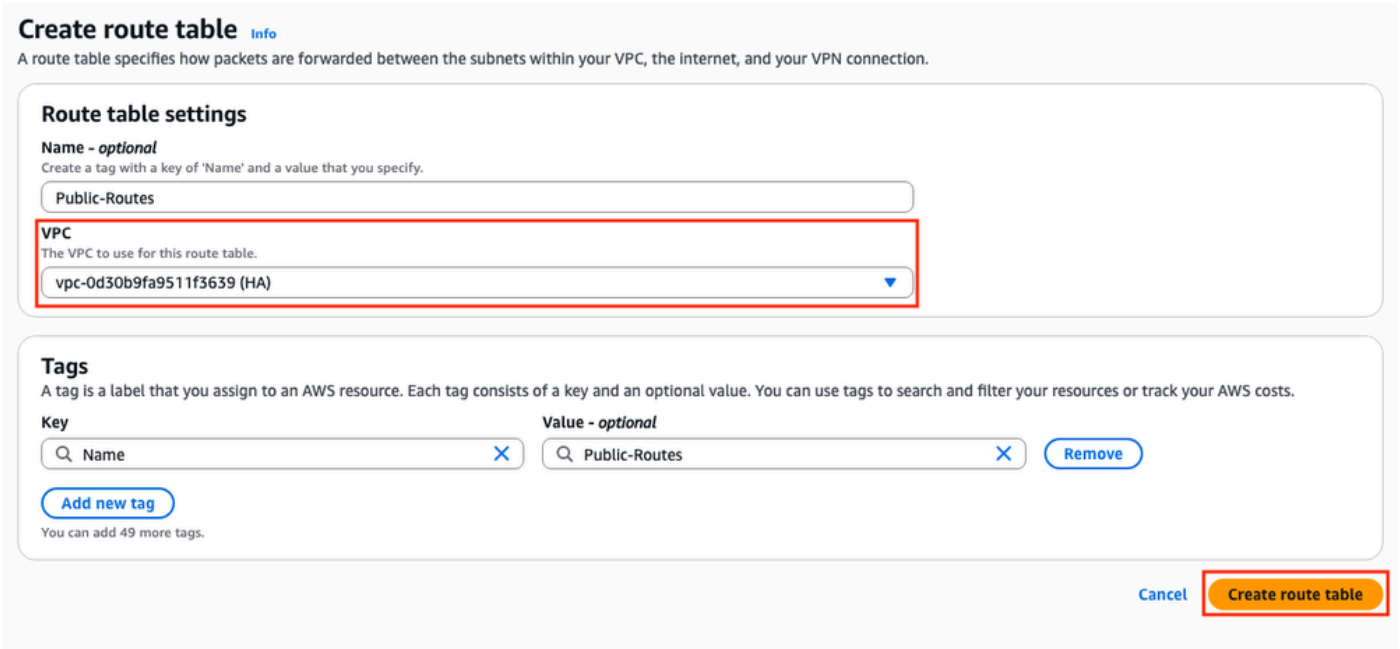
Paso 10. Crear y configurar tablas de rutas en AWS para subredes públicas y privadas

Paso 10.1. Crear y configurar la tabla de ruta pública

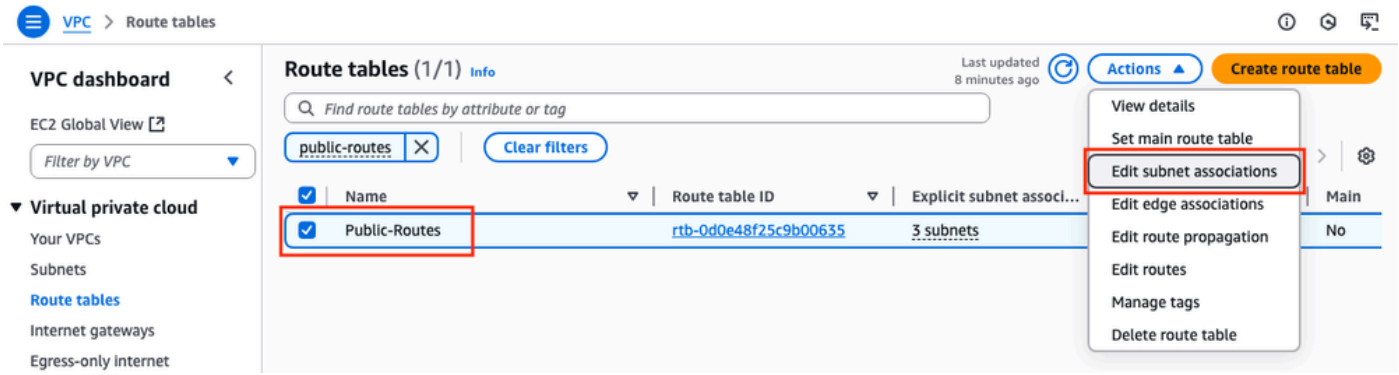
Para establecer el HA en esta topología, asocie todas las subredes públicas y privadas en sus tablas de rutas correspondientes. En la sección Panel de VPC > Nube privada virtual > Tablas de ruta, haga clic en Crear tabla de ruta.



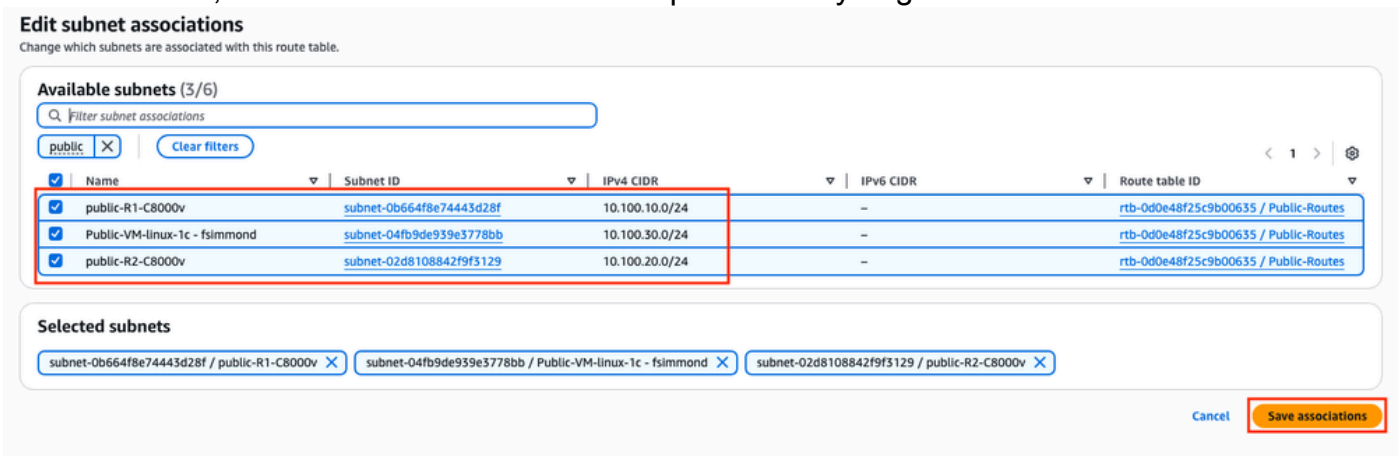
En la nueva sección, seleccione el VPC correspondiente para esta topología. Una vez seleccionado, haga clic en Create route table.



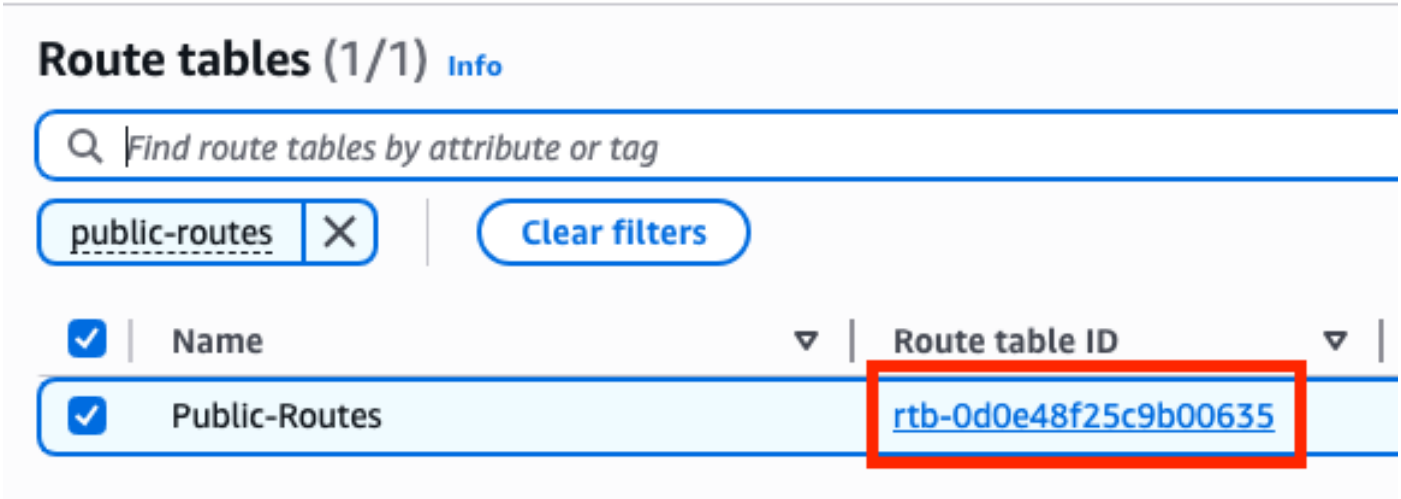
En la sección Tablas de ruta, seleccione la tabla creada y haga clic en Acciones > Editar asociaciones de subred.



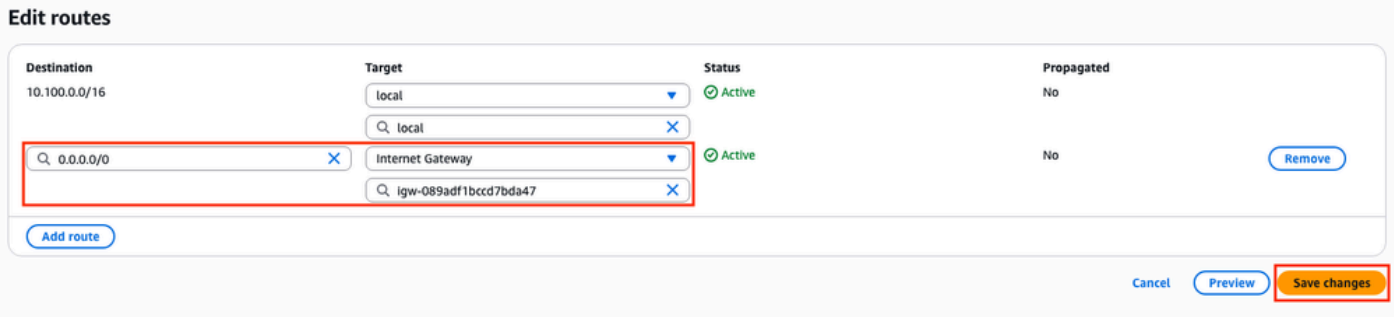
A continuación, seleccione las subredes correspondientes y haga clic en Guardar asociaciones.



Una vez asociadas las subredes, haga clic en el hipervínculo Route table ID para agregar las rutas adecuadas para la tabla. A continuación, haga clic en Editar rutas:

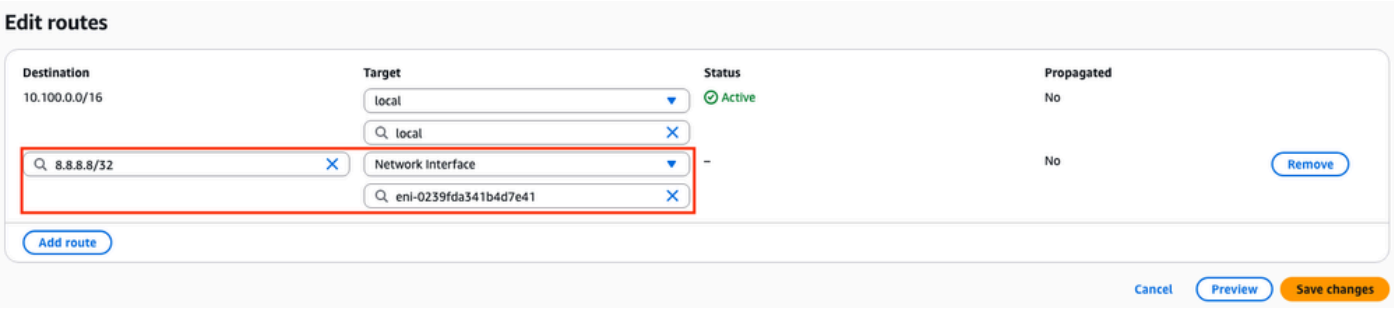


Para obtener acceso a Internet, haga clic en Add route y vincule esta tabla de public route con el IGW creado en el Paso 9 con estos parámetros. Una vez seleccionado, haga clic en Guardar cambios:



Paso 10.2. Crear y configurar la tabla de rutas privadas

Ahora que se ha creado la tabla de rutas públicas, replique los pasos 10 para la ruta privada y las subredes privadas, excepto para la adición de la puerta de enlace de Internet en sus rutas. Para este ejemplo, la tabla de ruteo tiene este aspecto ya que el tráfico para 8.8.8.8 debe pasar a través de la subred privada en este ejemplo:



Paso 11. Verifique y configure la configuración de red básica, traducción de direcciones de red (NAT), túnel GRE con BFD y protocolo de ruteo

Una vez preparadas las Instancias y su configuración de ruteo en AWS, configure los dispositivos:

Configuración de 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
```

Configuración de 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
```

Paso 12. Configuración de alta disponibilidad (Denominación 16.3.1a o posterior de Cisco IOS® XE)

Ahora que la redundancia y la conexión entre las VM están configuradas, configure los ajustes de HA para definir los cambios de ruteo. Establezca los valores Route-table-id, Network-interface-id y CIDR que se deben establecer después de un error AWS HA como un peer BFD down.

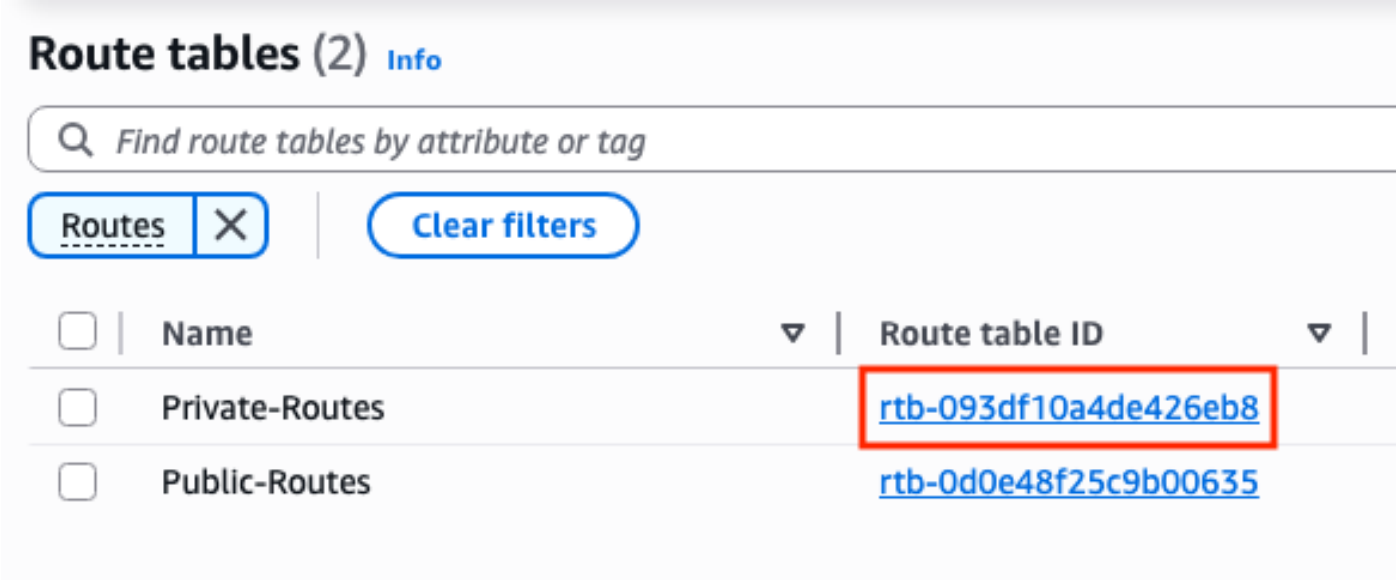
```
Router(config)# redundancy
Router(config-red)# cloud provider aws (node-id)
bfd peer <IP address of the remote device>
route-table <Route table ID>
cidr ip <traffic to be monitored/prefix>
eni <Elastic network interface (ENI) ID>
region <region-name>
```

El parámetro bfd peer está relacionado con la dirección IP del peer del túnel. Esto se puede verificar usando el resultado de show bfd neighbor:

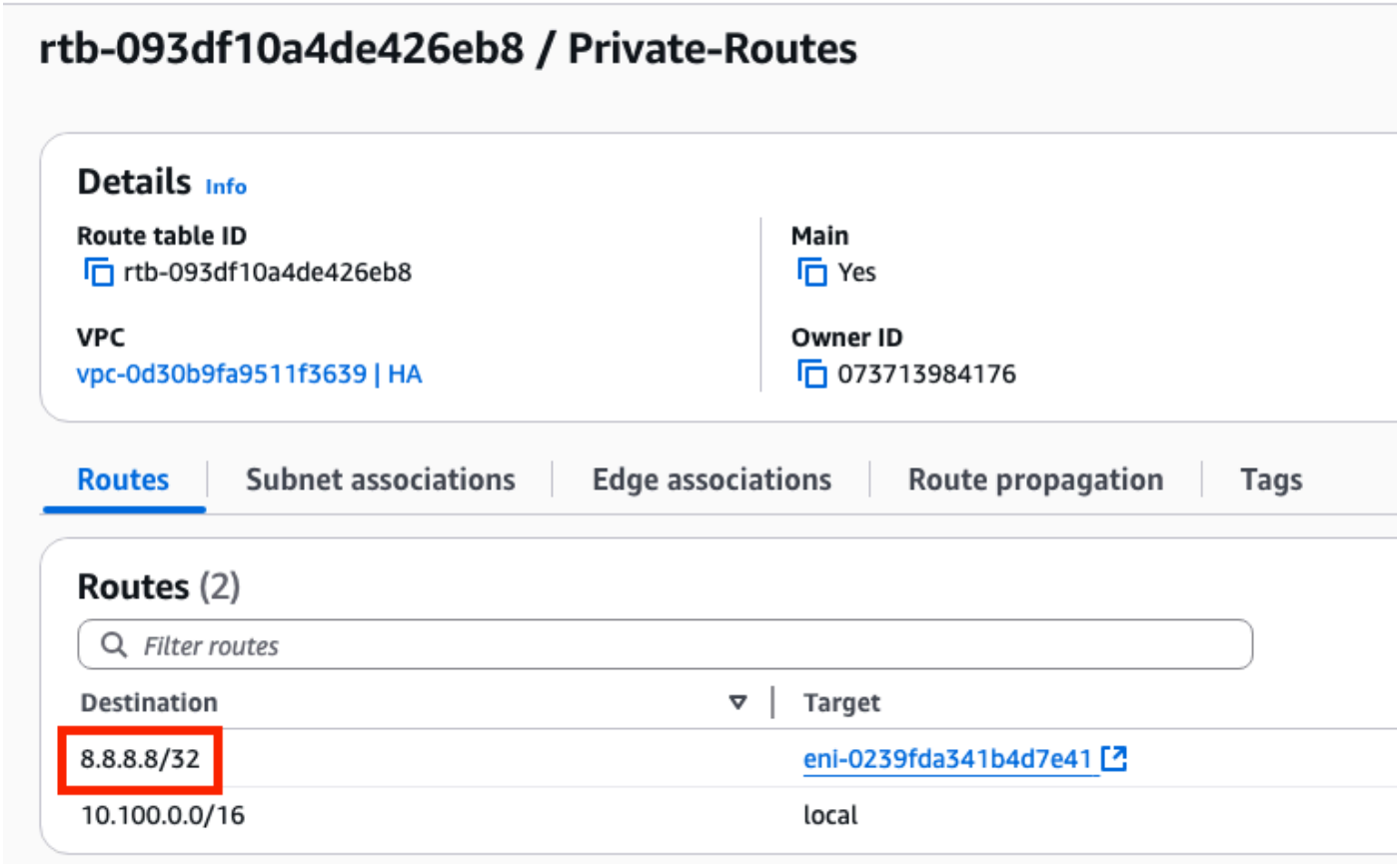
```
R1(config)#do sh bfd neighbors

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

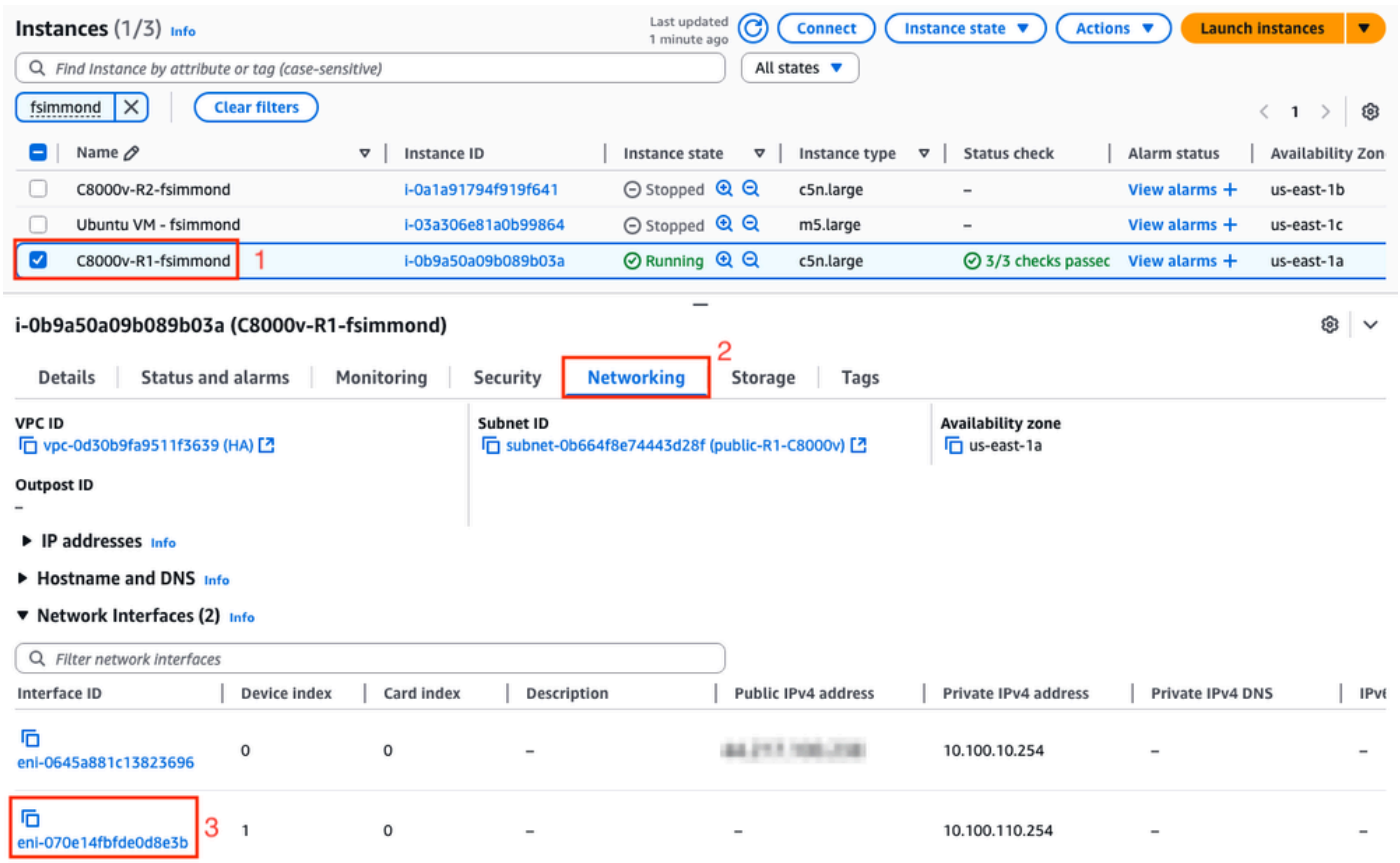
El parámetro route-table está relacionado con el ID de la tabla de rutas privadas que se encuentra en la sección Panel de VPC > Nube privada virtual > Tablas de rutas. Copie el ID de la tabla de rutas correspondiente.



El parámetro cidr ip está relacionado con el prefijo de ruta agregado en la tabla de rutas privadas (rutas creadas en el paso 10.2):



El parámetro eni está relacionado con el ID de ENI de la interfaz privada correspondiente de la instancia que se está configurando. Para este ejemplo, se utiliza el ID de ENI de la interfaz GigabitEthernet2 de la instancia:



El parámetro region está relacionado con el nombre de código que se encuentra en la documentación de AWS para la región donde se encuentra VPC. Para este ejemplo, se utiliza la región us-east-1.

Sin embargo, esta lista puede cambiar o aumentar. Para encontrar las actualizaciones más recientes, visite el documento AmazonRegion and Availability Zones.

Teniendo en cuenta toda esta información, aquí está el ejemplo de configuración para cada router en el VPC:

Ejemplo de configuración 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
```

Ejemplo de configuración 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
```

Verificación

1. Compruebe el estado de la instancia de C8000v R1. Confirme que el túnel y la redundancia de nube estén en funcionamiento.

```
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
```

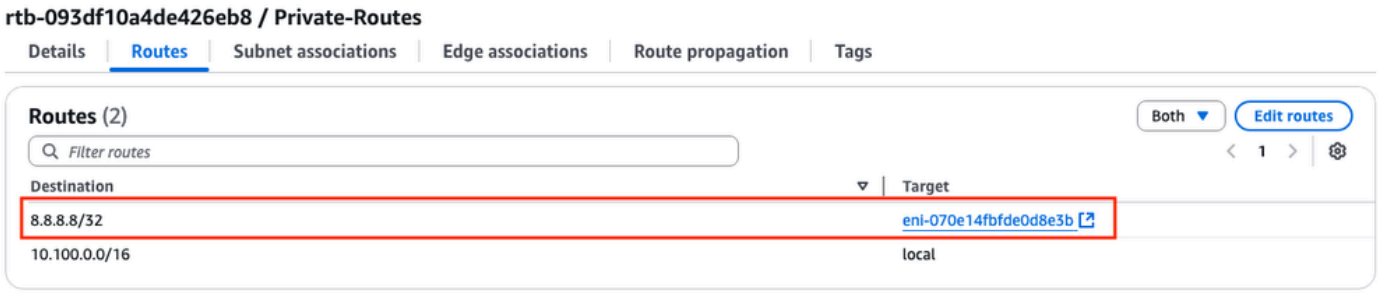
```
0 192.168.200.2 Tu1 10 00:16:52 2 1470 0 2


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. Ejecute un ping continuo a 8.8.8.8 desde la máquina virtual host que está detrás de los routers. Asegúrese de que el ping esté pasando a través de la interfaz 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 AWS WebGUI y verifique el estado de la tabla de ruteo. El ENI actual pertenece a la interfaz privada de la instancia R1:



4. Active el cambio de ruta cerrando la interfaz Tunnel1 en la instancia R1 para simular un evento de failover HA:

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

5. Verifique nuevamente en la tabla route en AWS, el ID ENI ha cambiado al ID ENI de la interfaz privada R2:

Troubleshoot

Estos son los puntos más comunes que a menudo se olvidan o se configuran mal al recrear la implementación:

- Asegúrese de que los recursos están asociados. Al crear VPC, subredes, interfaces, tablas de ruta, etc., muchas de estas no se asocian entre sí automáticamente. No tienen conocimiento el uno del otro.
- Asegúrese de que la IP elástica y cualquier IP privada estén asociadas con las interfaces correctas, con las subredes adecuadas, agregadas a la tabla de rutas correcta, conectadas al router correcto y la VPC y zona correctas, vinculadas con el rol IAM y los grupos de seguridad.

- Desactive la comprobación de origen/destino por ENI.
  En caso de que ya haya comprobado todos los puntos tratados en esta sección y el problema siga presente, recopile estos resultados, pruebe la conmutación por fallo de HA, si es posible, y abra un caso con el TAC de Cisco:

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).