C8000v High Availability Configuration implementeren op AWS

Inhoud

Inleiding

In dit document wordt beschreven hoe u een omgeving met hoge beschikbaarheid kunt instellen

met Catalyst 8000v-routers op de cloud van Amazon Web Services.

Voorwaarden

Vereisten

Cisco raadt u aan om voorkennis te hebben van de volgende onderwerpen:

- Algemene kennis van AWS Console en zijn componenten
- Kennis van Cisco IOS® XE-software
- Basiskennis van de HA-functie.

Gebruikte componenten

Deze onderdelen zijn vereist voor dit configuratievoorbeeld:

- Een Amazon AWS-account met beheerdersrol
- Twee C8000v-apparaten met Cisco IOS® XE 17.15.3a en 1 Ubuntu 17 .04 LTS VM AMI's in dezelfde regio

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Topologie

Er zijn verschillende scenario's voor HA-implementatie op basis van de netwerkvereisten. In dit voorbeeld wordt HA-redundantie geconfigureerd met de volgende instellingen:

- 1x - Regio
- 1x - VPC
- 3x - Beschikbaarheidszones
- 6x - Netwerkinterfaces/subnetten (3x openbaar/3x privé)
- 2x - Routetafels (openbaar en privé)
- 2x - C8000v-routers (Cisco IOS® XEDenali 17.15.3a)
- 1x - VM (Linux/Windows)

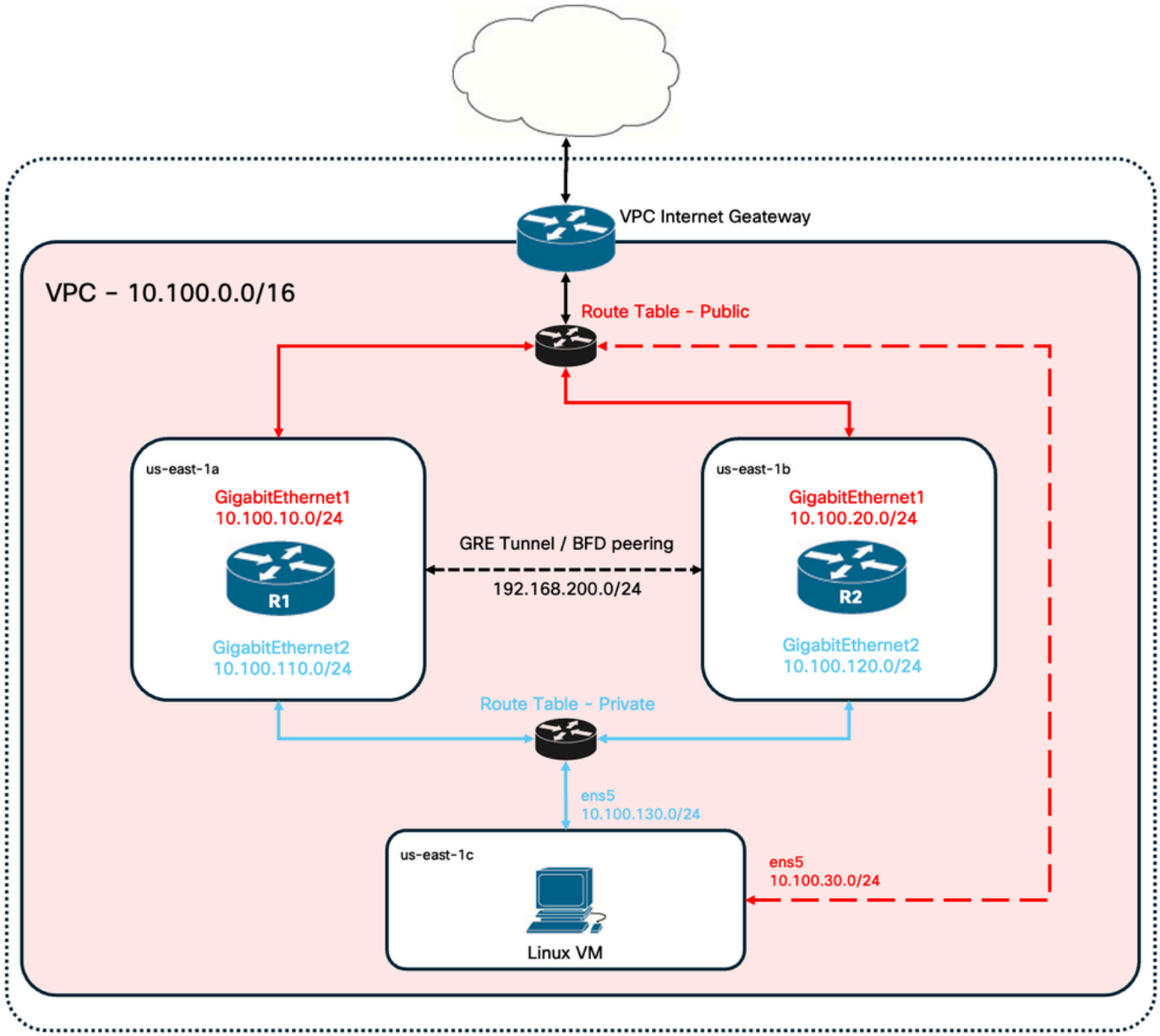
Er zijn 2 C8000v-routers in een HA-paar, in twee verschillende beschikbaarheidszones. Beschouw elke beschikbaarheidszone als een afzonderlijk datacenter voor extra hardwarematige veerkracht.

De derde zone is een VM, die een apparaat in een privédatacenter simuleert. Voorlopig is internettoegang ingeschakeld via de openbare interface, zodat u de VM kunt openen en configureren. Over het algemeen moet al het normale verkeer door de privéroutetafel stromen.

Om het verkeer te simuleren, start u een ping vanaf de privé-interface van de virtuele machine en

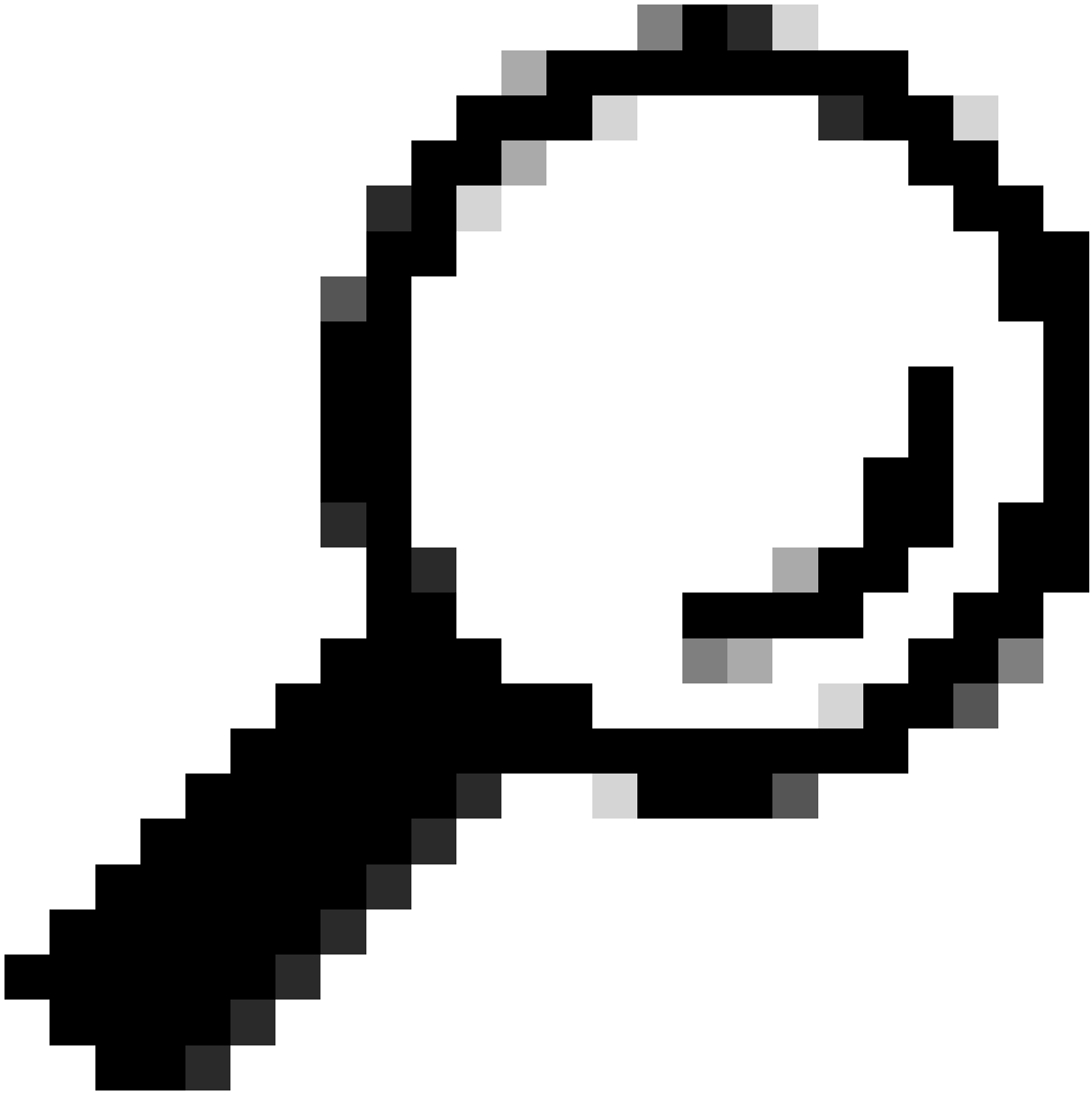
doorloopt u de privé-routetabel door R1 om 8.8.8.8 te bereiken. Controleer in het geval van een failover of de privéroutetabel automatisch is bijgewerkt om het verkeer door de privéinterface van de R2-router te leiden.

Netwerkdiagram



Tabeloverzicht

Om de topologie samen te vatten, hier is de tabel met de belangrijkste waarden van elke component in het lab. De informatie in deze tabel is exclusief voor dit lab.



Tip: Met behulp van deze tabel kunt u een duidelijk overzicht van de belangrijkste variabelen in de hele gids behouden. Het verzamelen van de informatie in dit formaat wordt aanbevolen om het proces te stroomlijnen.

Apparaat	beschikbaarheidszone	Interfaces	IP-adressen	RTB	ENI
R1	US-EAST-1A	Gigabit Ethernet1	10.100.10.254	RTB-0D0E48F25C9B00635 (openbaar)	ENI-0645A881C13823696
		Gigabit Ethernet2	10.100.110.254	RTB-093DF10A4DE426EB8 (particulier)	ENI-070E14FBFDE0D8E3
R2	US-EAST-1B	Gigabit Ethernet1	10.100.20.254	RTB-0D0E48F25C9B00635 (openbaar)	ENI-0A7817922FFBB317B

		Gigabit Ethernet2	10.100.120.254	RTB-093DF10A4DE426EB8 (particulier)	ENI-0239FDA341B4D7E41
Linux-VM	US-EAST-1C	ENS5	10.100.30.254	RTB-0D0E48F25C9B00635 (openbaar)	ENI-0B28560781B3435B1
		ENS6	10.100.130.254	RTB-093DF10A4DE426EB8 (particulier)	ENI-05D025E88B6355808

Beperkingen

- Gebruik op een gemaakt subnet niet het eerste beschikbare adres van dat subnet. Deze IP-adressen worden intern door de AWS-diensten gebruikt.
- Configureer de openbare interfaces van de C8000v-apparaten niet in een VRF. HA werkt niet goed als dit is ingesteld.

Configuratie

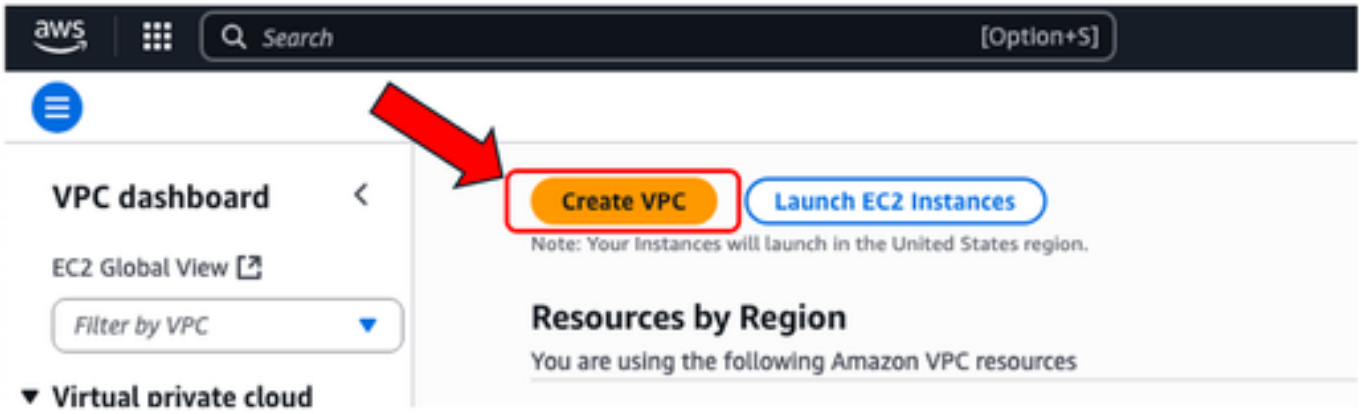
De algemene stroom van configuratie is gericht op het maken van de gevraagde VM's in de juiste regio en het verplaatsen van uw weg naar de meest specifieke configuratie, zoals routes en interfaces van elk van hen. Het wordt echter aanbevolen om eerst de topologie te begrijpen en deze in elke gewenste volgorde te configureren.

Stap 1. Selecteer een regio

Voor deze implementatiegids wordt de regio US-West (North Virginia) - us-east-1 geselecteerd als de VPC-regio.

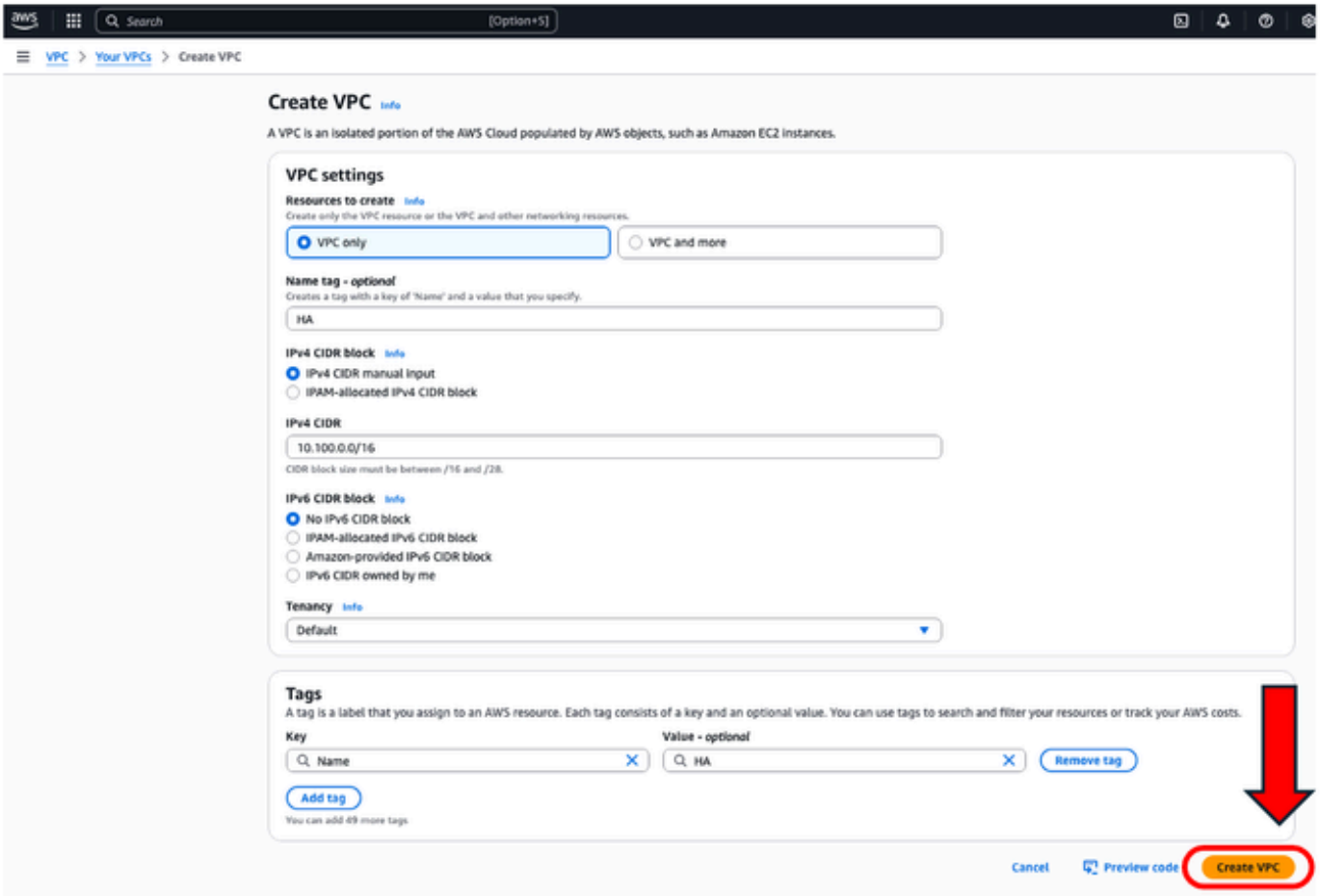
Stap 2. De VPC maken

Navigeer op de AWS-console naar VPC > VPC Dashboard > VPC maken.

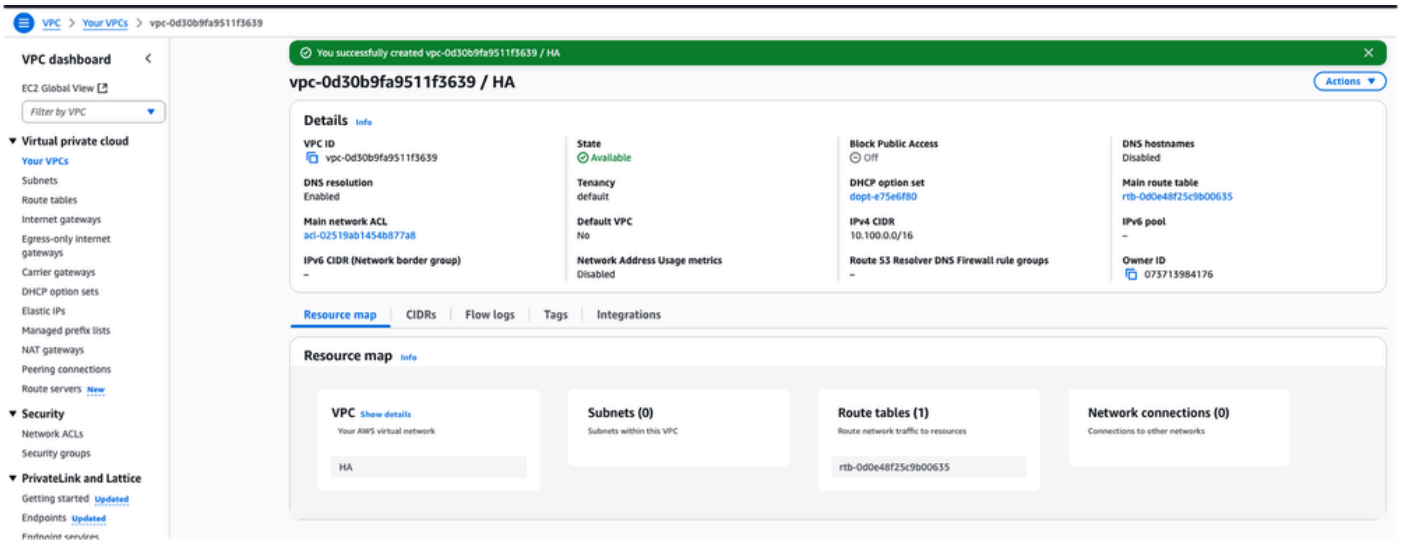


Wanneer u de VPC maakt, selecteert u de optie Alleen VPC. U kunt een /16-netwerk toewijzen om te gebruiken zoals u wilt.

In deze implementatiegids wordt het 10.100.0.0/16-netwerk geselecteerd:

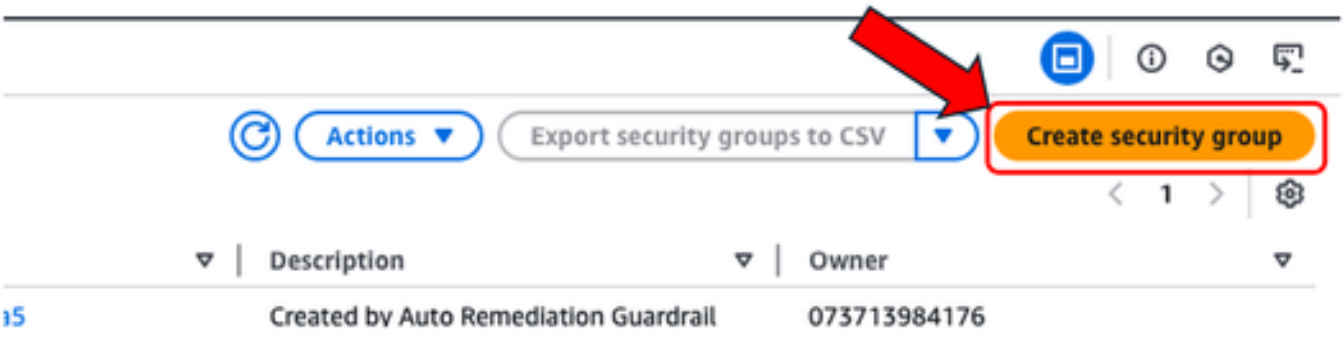


Nadat u op VPC maken hebt geklikt, wordt nu de VPC-0d30b9fa9511f3639 met HA-tag gemaakt:

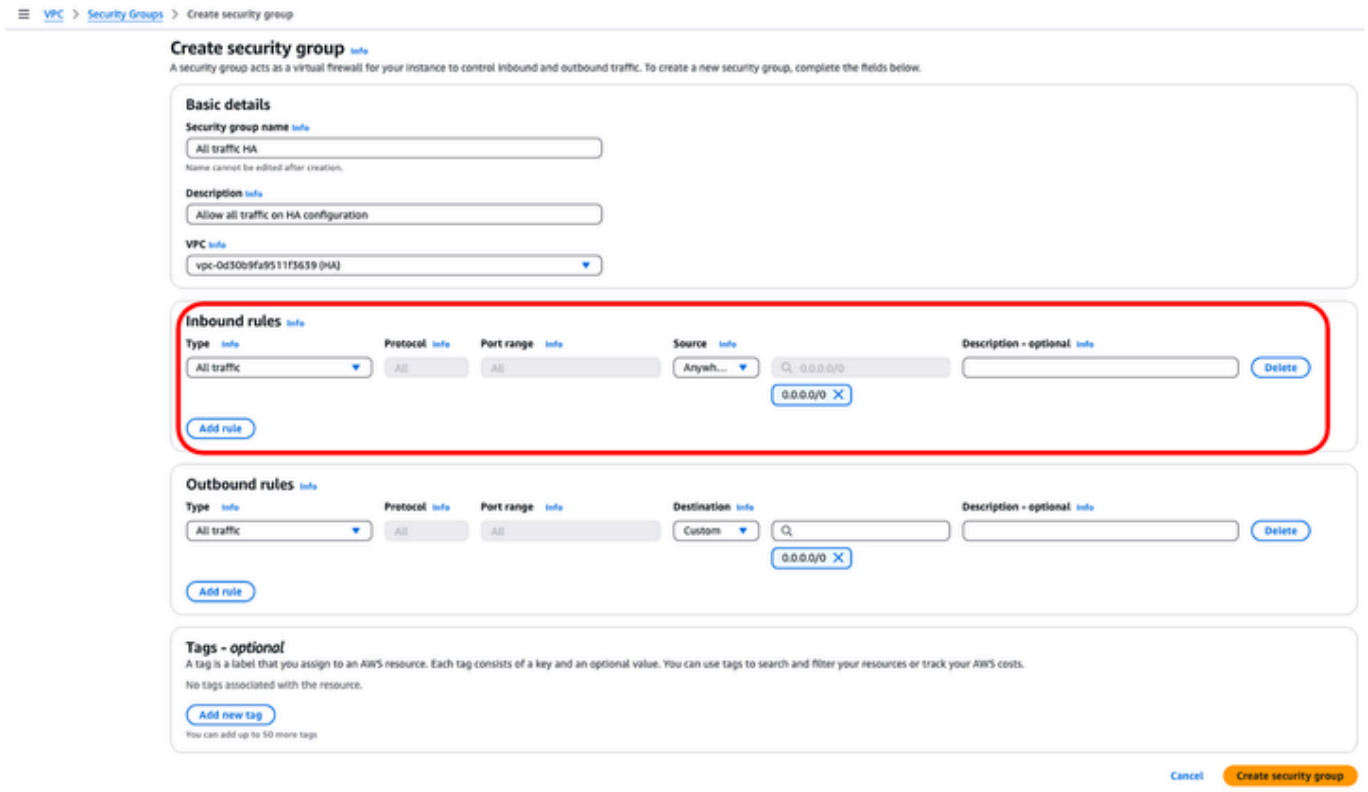


Stap 3. Een beveiligingsgroep voor de VPC maken

In AWS werken beveiligingsgroepen zoals ACL's, waardoor verkeer naar geconfigureerde VM's binnen een VPC wordt toegestaan of geweigerd. Navigeer in de AWS-console naar VPC > VPC Dashboard > Security > Security Groups en klik op Create security group.



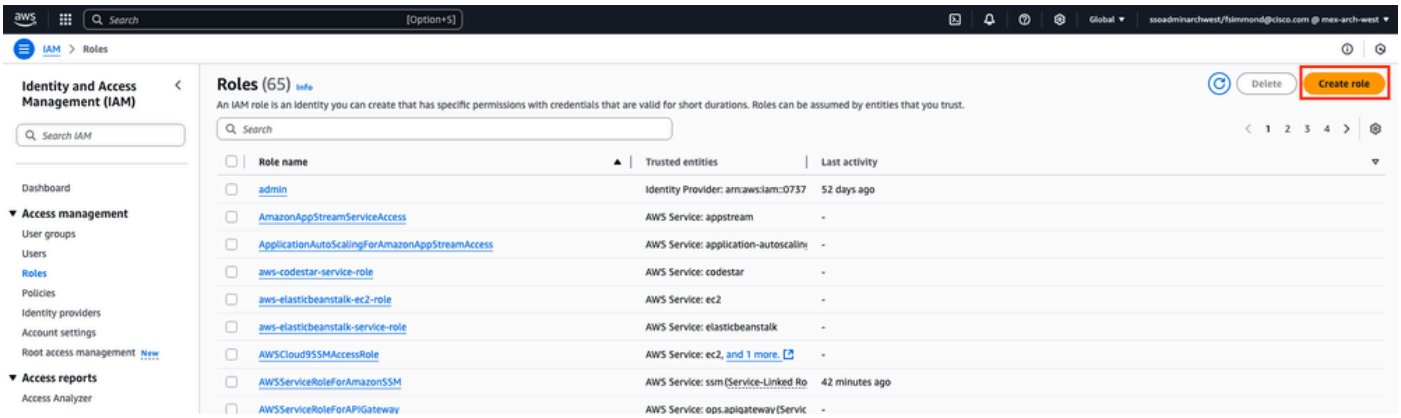
Bepaal onder Inbound Rules welk verkeer u wilt toestaan. In dit voorbeeld wordt Alle verkeer geselecteerd met behulp van het netwerk 0.0.0.0/0.



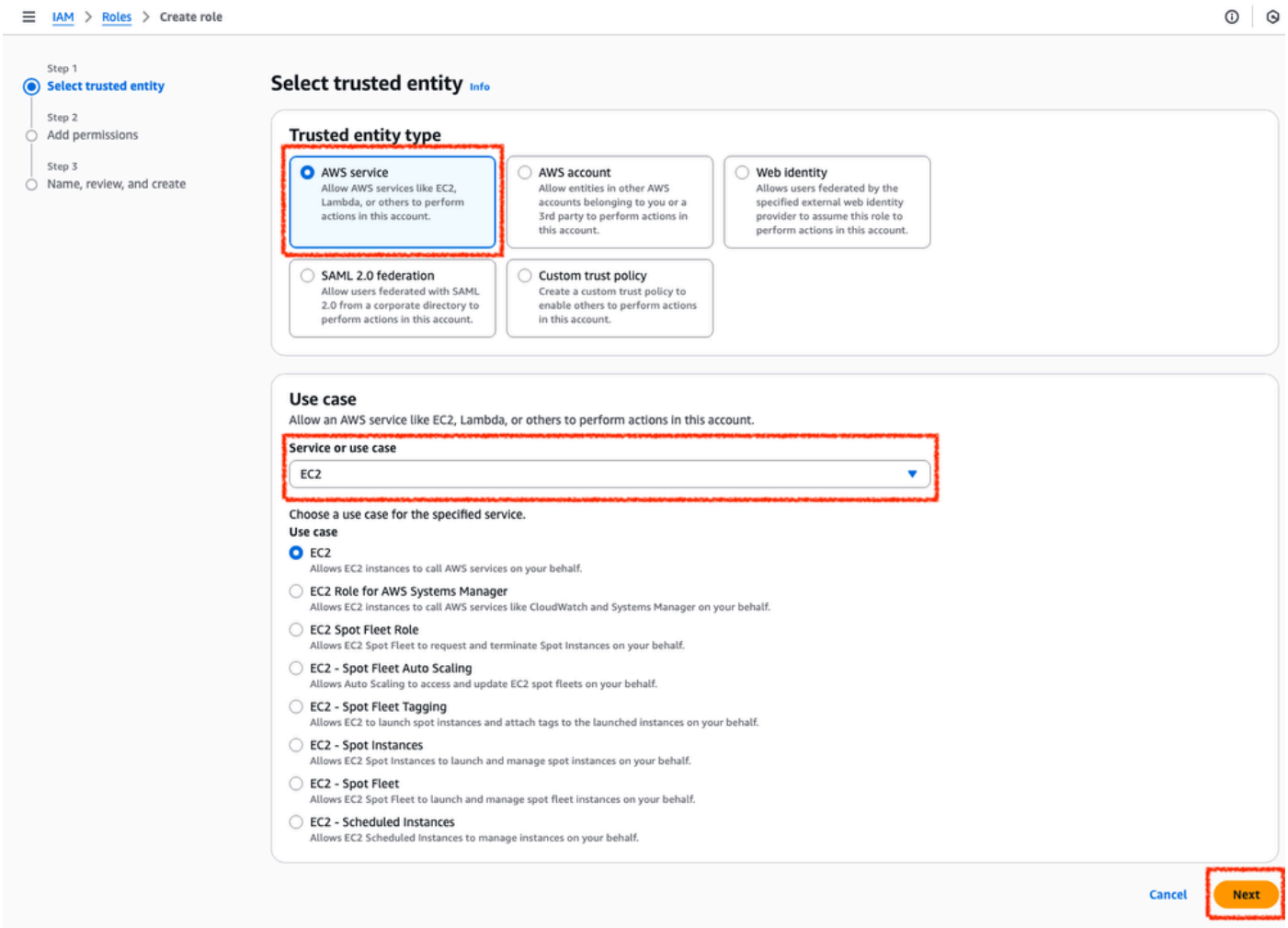
Stap 4. Maak een IAM-rol met een beleid en koppel aan de VPC

IAM verleent uw AMI's de vereiste toegang tot Amazon API's. De C8000v wordt gebruikt als een proxy om AWS API-opdrachten aan te roepen om de routetabel in AWS aan te passen. Standaard hebben EC2-instanties geen toegang tot API's. Om deze reden moet een nieuwe IAM-rol worden gecreëerd die zal worden toegepast tijdens AMI-creaties.

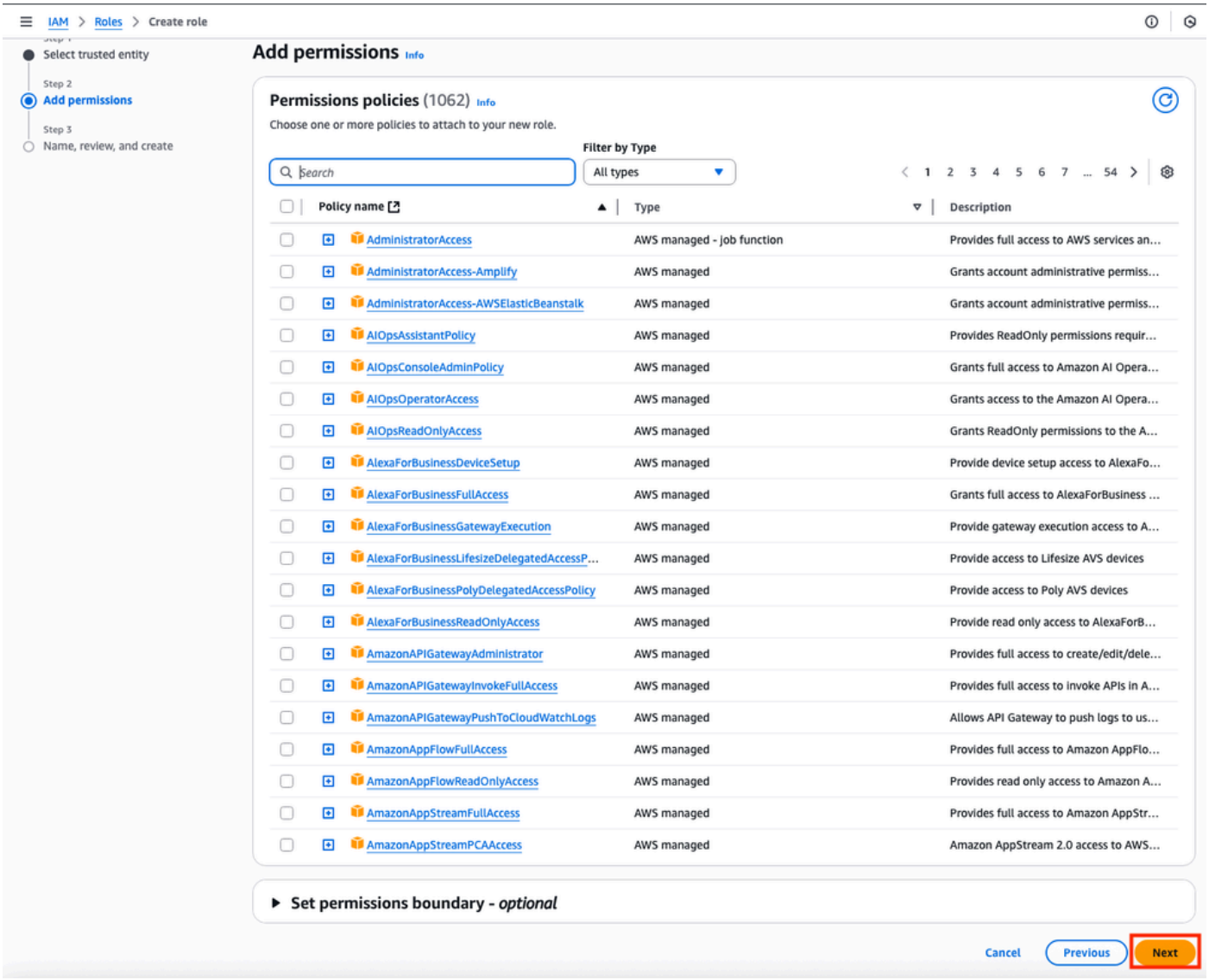
Blader naar het IAM-dashboard en navigeer naar Access Management > Rollen > Rol maken. Dit proces bestaat uit 3 stappen:



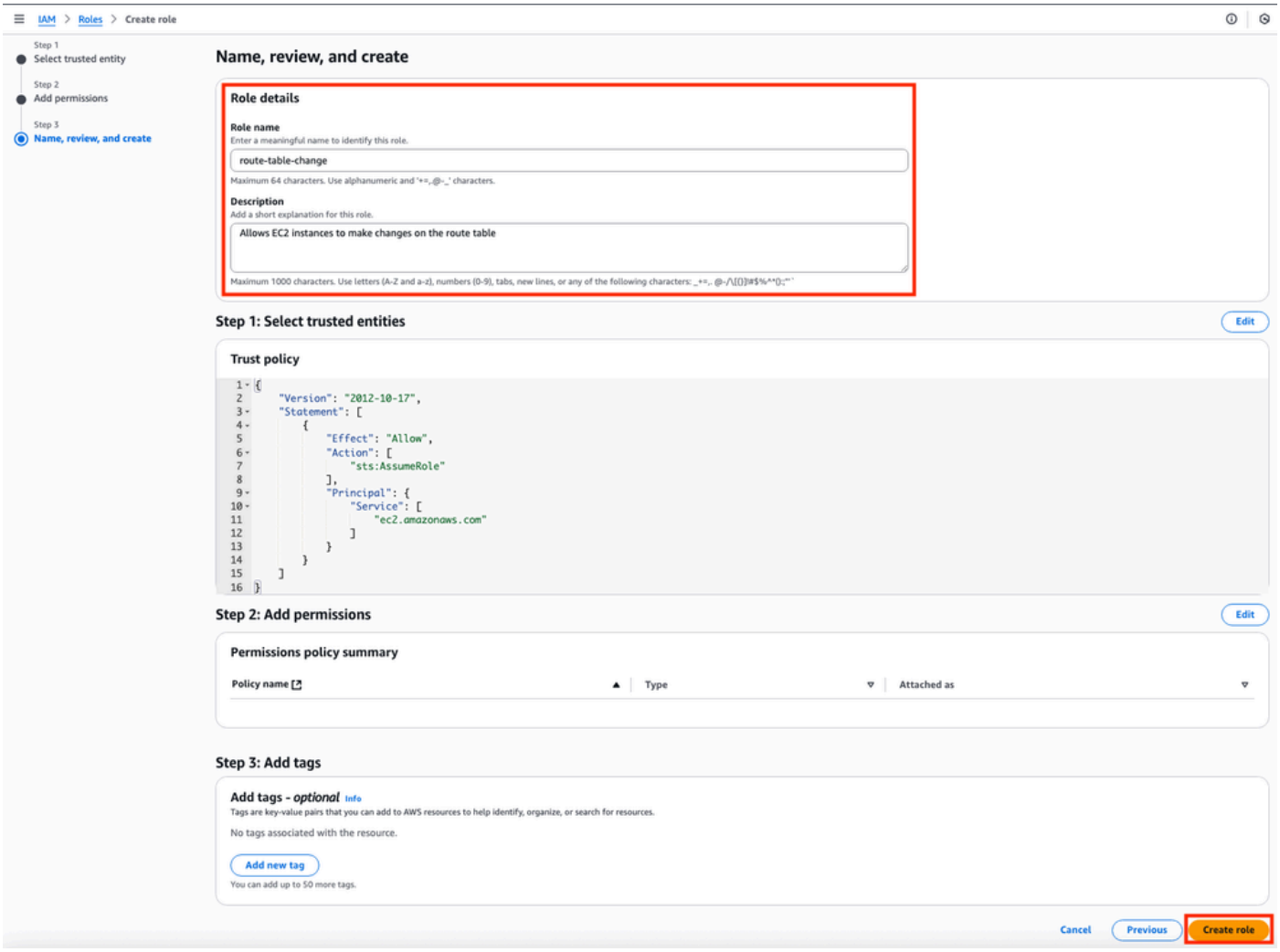
Selecteer eerst de optie AWS-service in de sectie Vertrouwd entiteitstype en EC2 als de service die voor dit beleid is toegewezen.



Als u klaar bent, klikt u op Volgende:

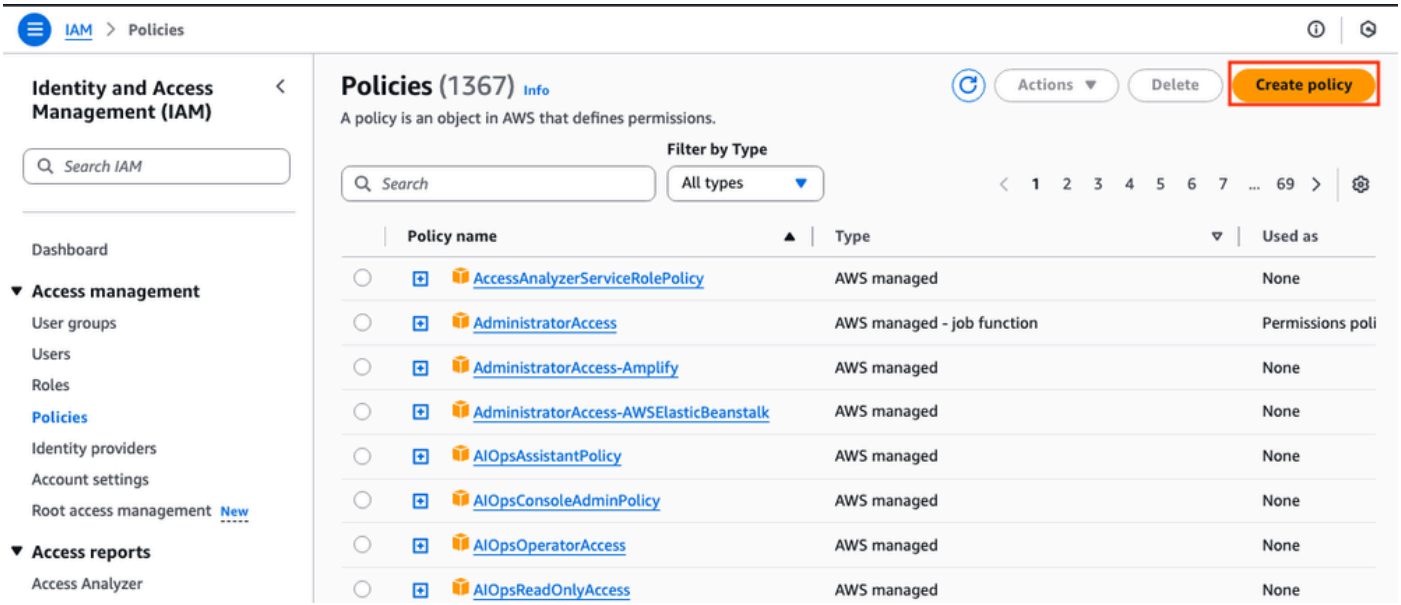


Stel ten slotte de rolnaam in en klik op de knop Rol maken.

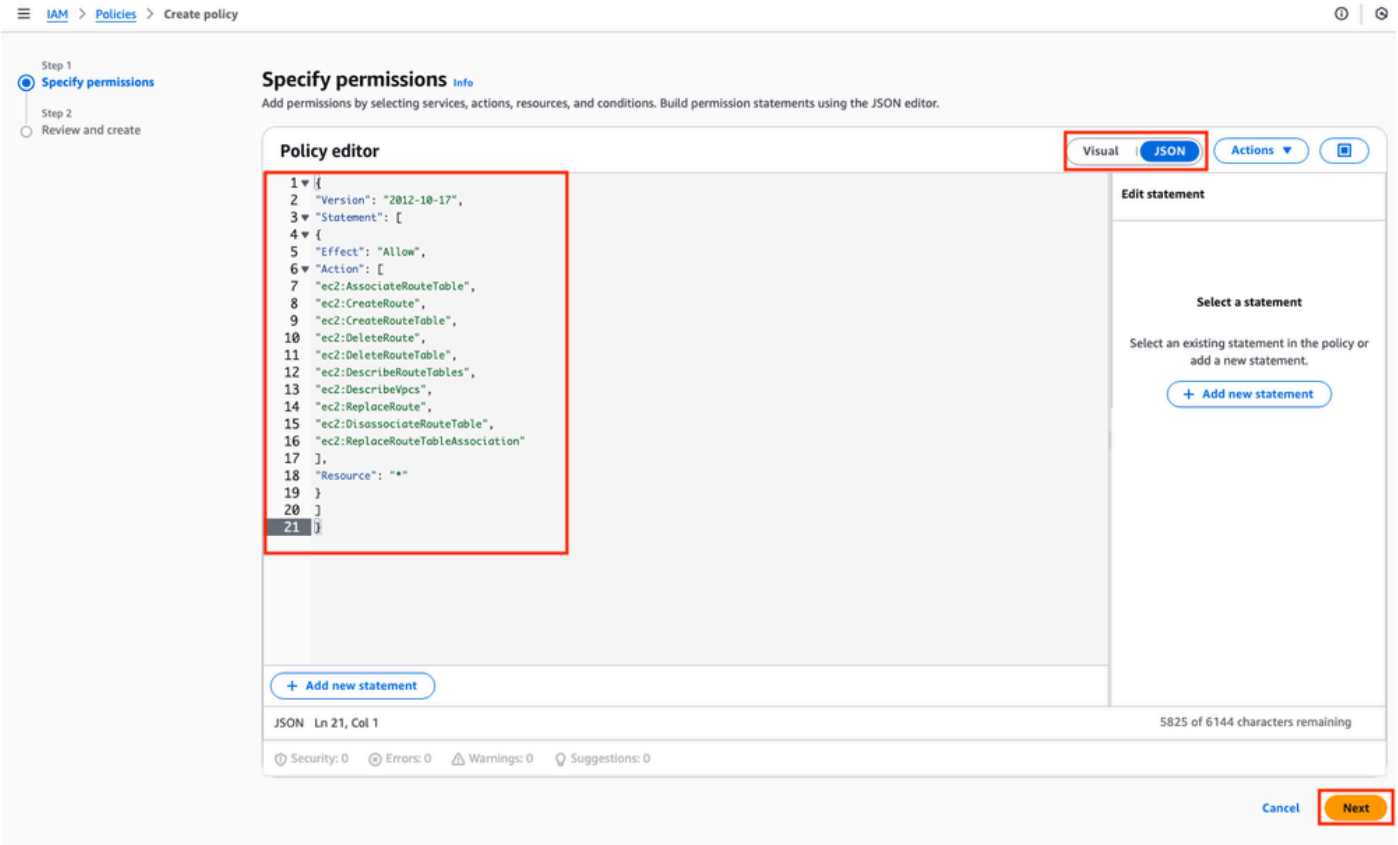


Stap 5. Een vertrouwensbeleid maken en koppelen aan een IAM-rol

Zodra de rol is gemaakt, moet een vertrouwensbeleid worden gemaakt om de vaardigheid te verwerven om de AWS-routeringstabellen te wijzigen wanneer dat nodig is. Ga naar het gedeelte Beleid op het IAM-dashboard. Klik op Beleid maken. Dit proces bestaat uit 2 stappen:



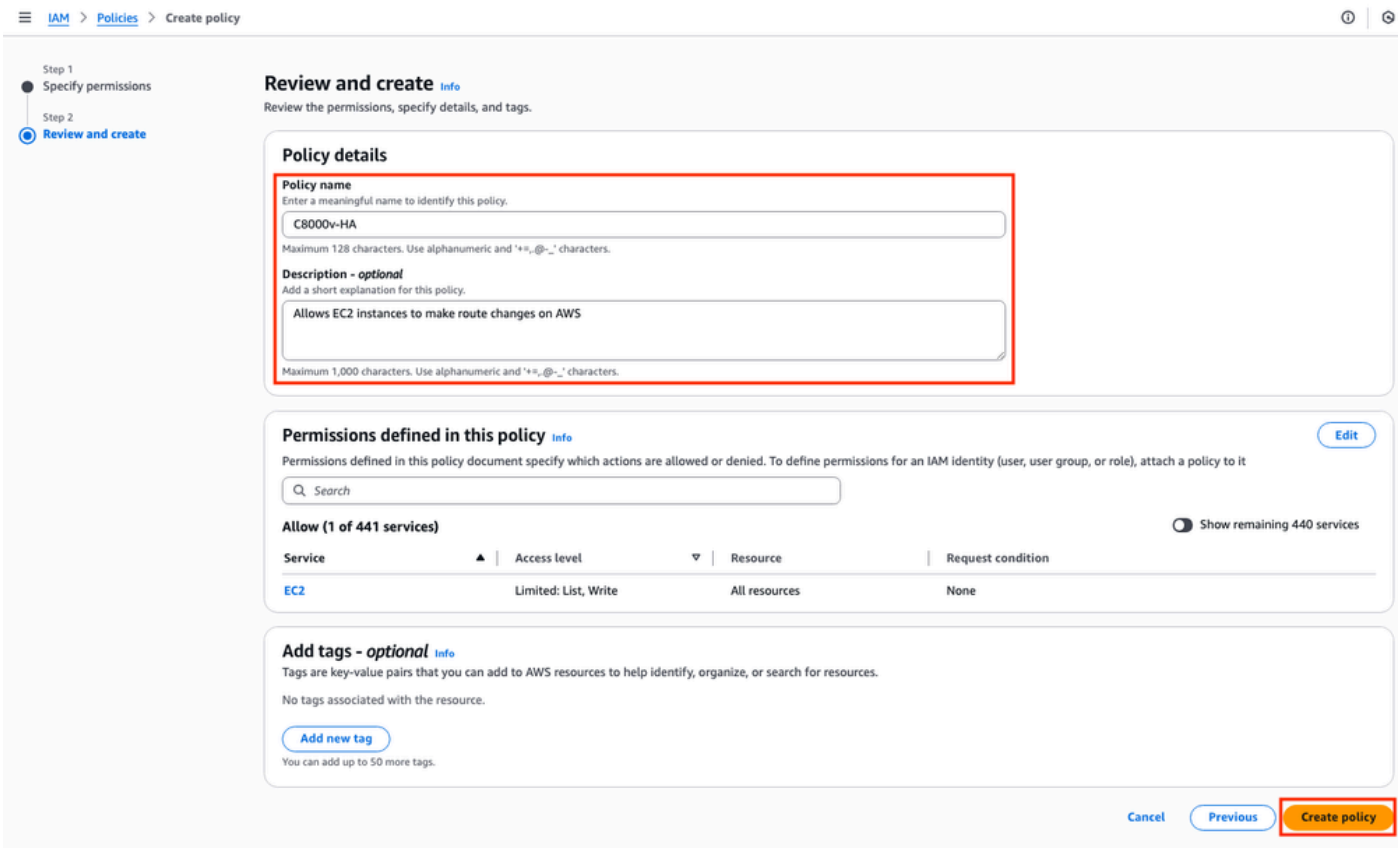
Zorg er eerst voor dat de Beleidseditor JSON gebruikt en pas de onderstaande opdrachten toe. Klik na configuratie op Volgende:



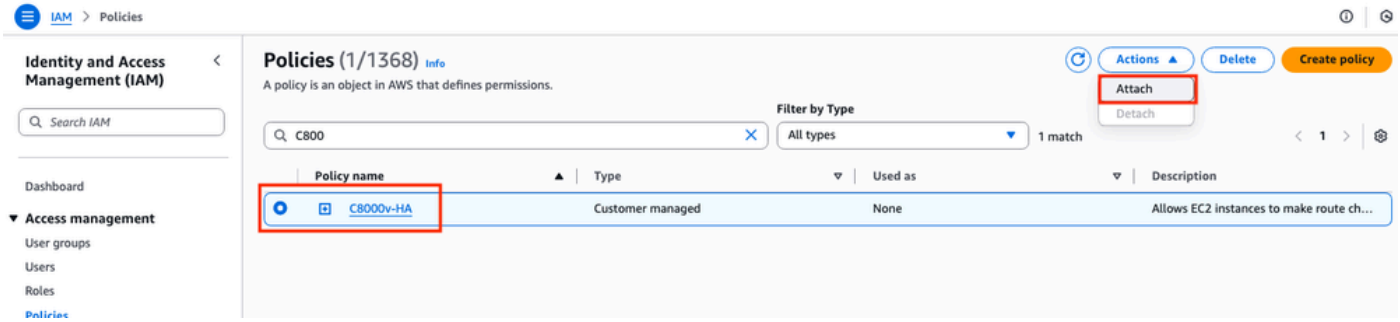
Dit is de tekst die in de afbeelding wordt gebruikt:

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

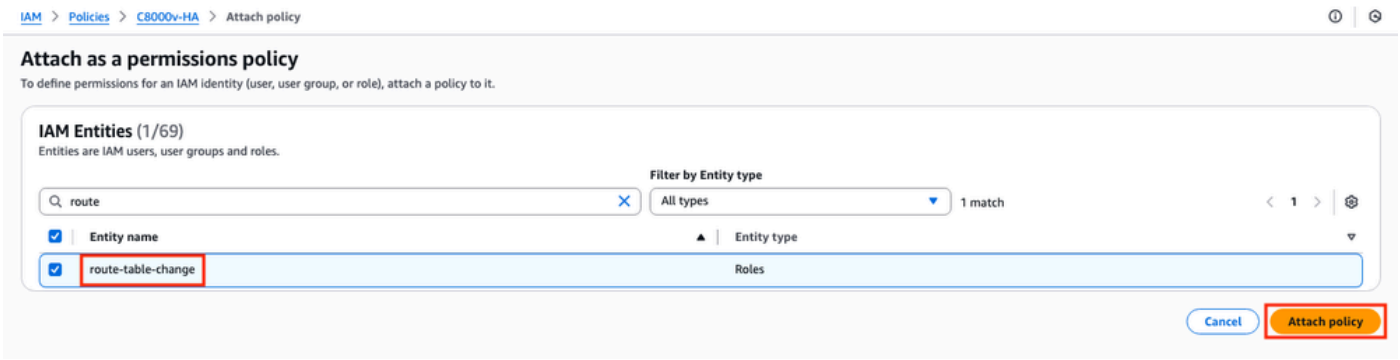
Stel later de naam van het beleid in en klik op Beleid maken.



Nadat het beleid is gemaakt, filtert u het beleid en selecteert u het vervolgens klikt u op de optie Bijvoegen in het vervolgkeuzemenu Acties.



Er is een nieuw venster geopend. In de sectie IAM-entiteiten filtert en selecteert u de gemaakte IAM-rol en klikt u op Bijvoegen.

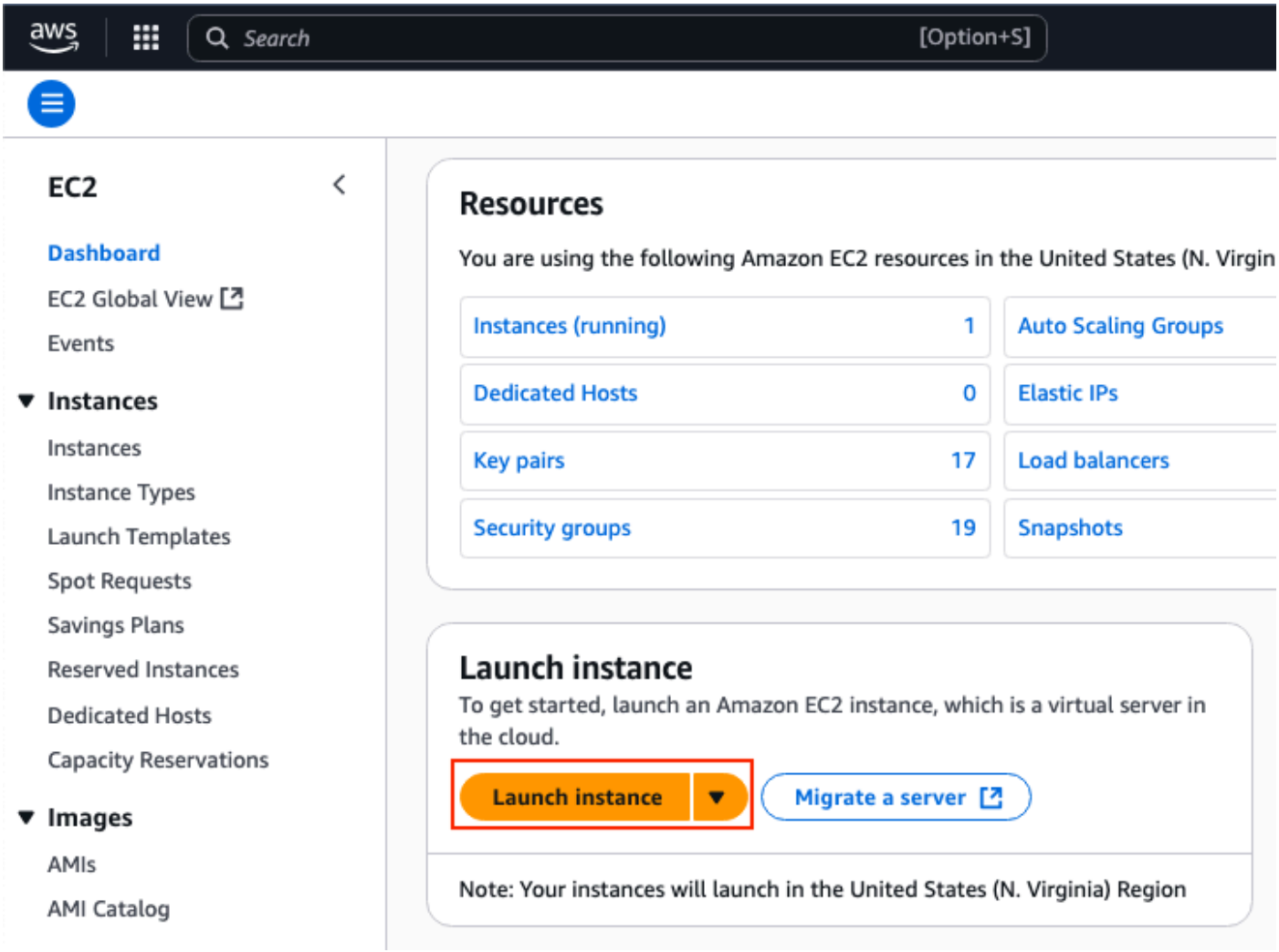


Stap 6.De C8000v-instanties configureren en starten

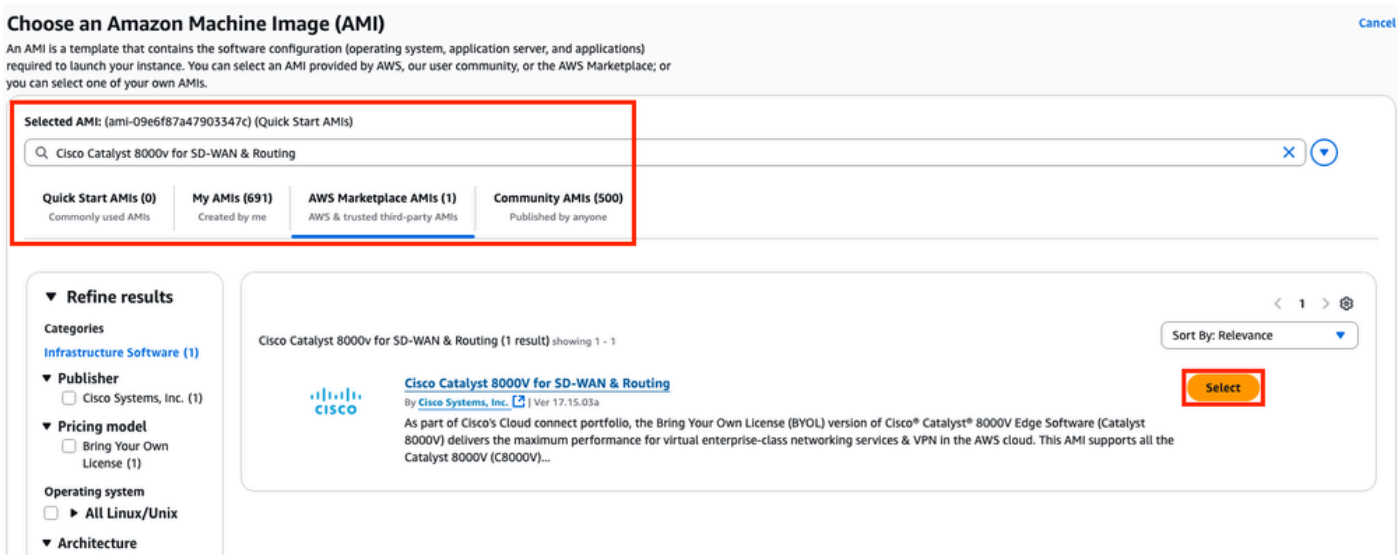
Elke C8000v-router heeft 2 interfaces (1 openbaar, 1 privé) en wordt gemaakt op zijn eigen

beschikbaarheidszone.

Klik op het EC2-dashboard op Instanties starten:

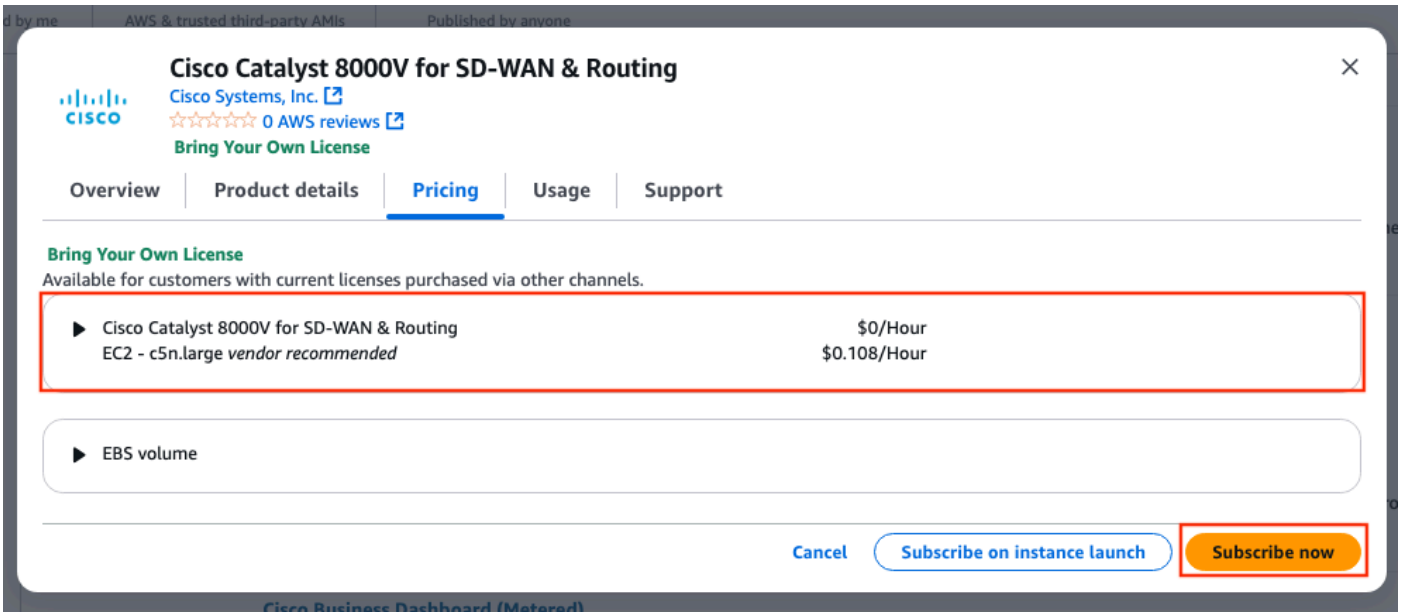


Filter de AMI database met de naam Cisco Catalyst 8000v voor SD-WAN & Routing. Klik in de lijst AMI's van AWS Marketplace op Selecteren.



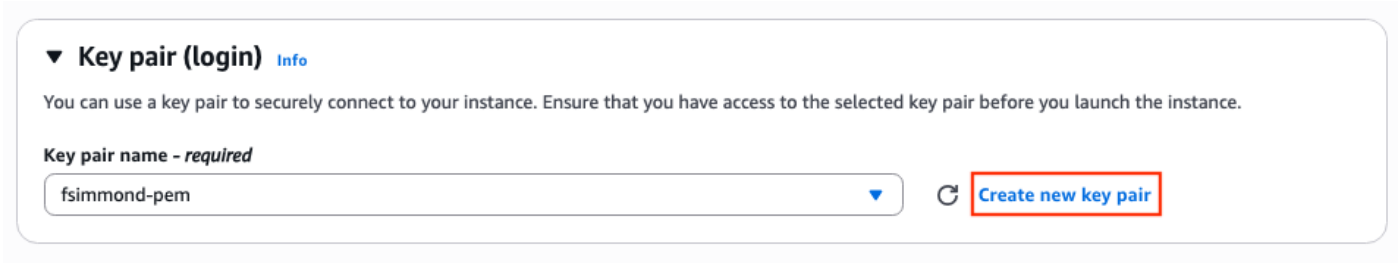
Selecteer de corresponderende grootte voor de AMI. In dit voorbeeld wordt de grootte c5n.large

geselecteerd. Dit kan afhankelijk zijn van de capaciteit die nodig is voor uw netwerk. Klik op Nu abonneren zodra u bent geselecteerd.

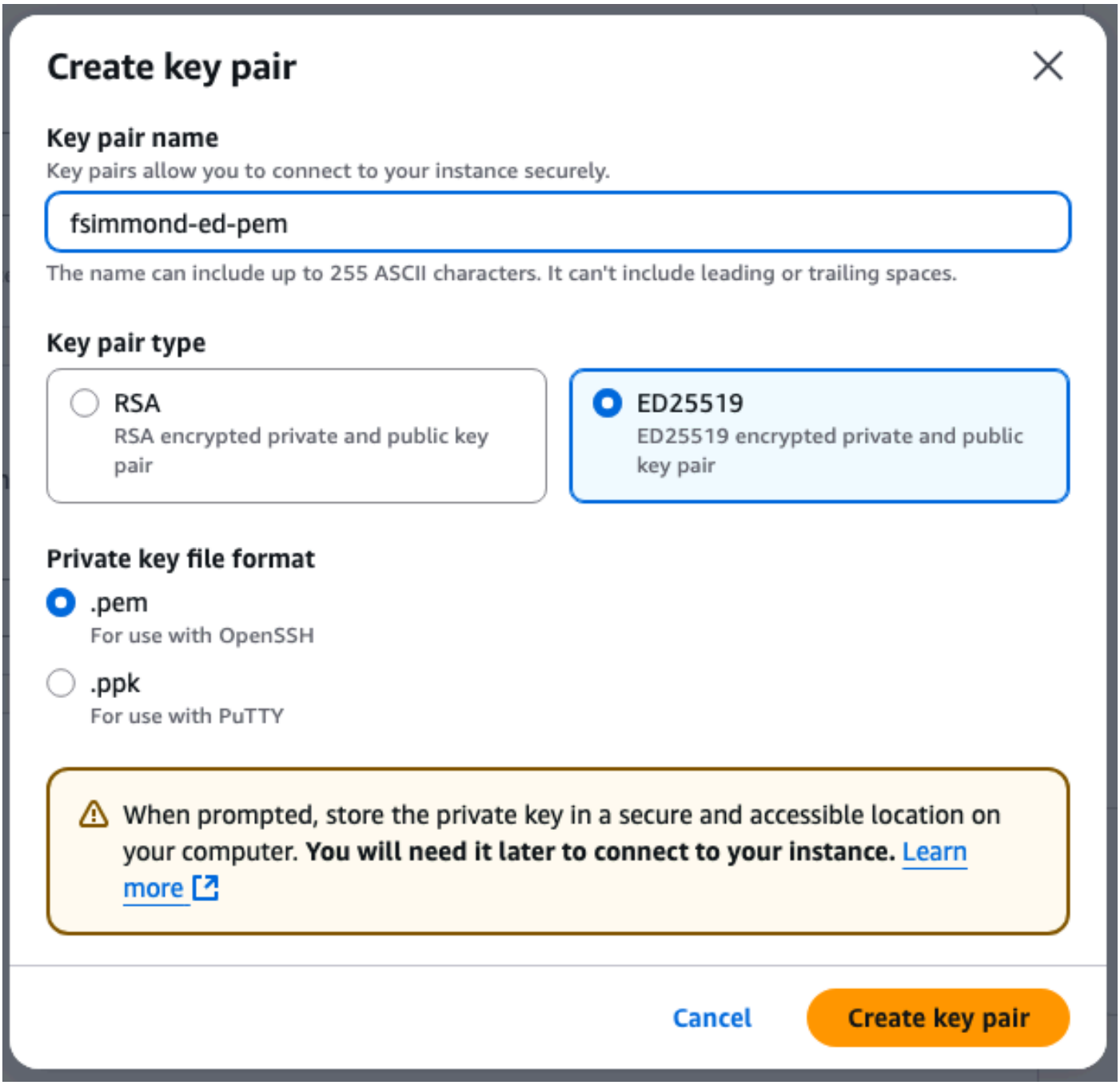


Stap 6.1. Het sleutelpaar configureren voor externe toegang

Eenmaal geabonneerd op de AMI, wordt een nieuw venster met meerdere opties weergegeven. Klik in het gedeelte Sleutelpaar (inloggen) op Nieuw sleutelpaar maken als er geen sleutelpaar aanwezig is. U kunt een enkele sleutel opnieuw gebruiken voor elk apparaat dat is gemaakt.



Er wordt een nieuw pop-upvenster weergegeven. In dit voorbeeld wordt een .pem-sleutelbestand met ED25519-codering gemaakt. Zodra alles is ingesteld, klikt u op Sleutelpaar maken.



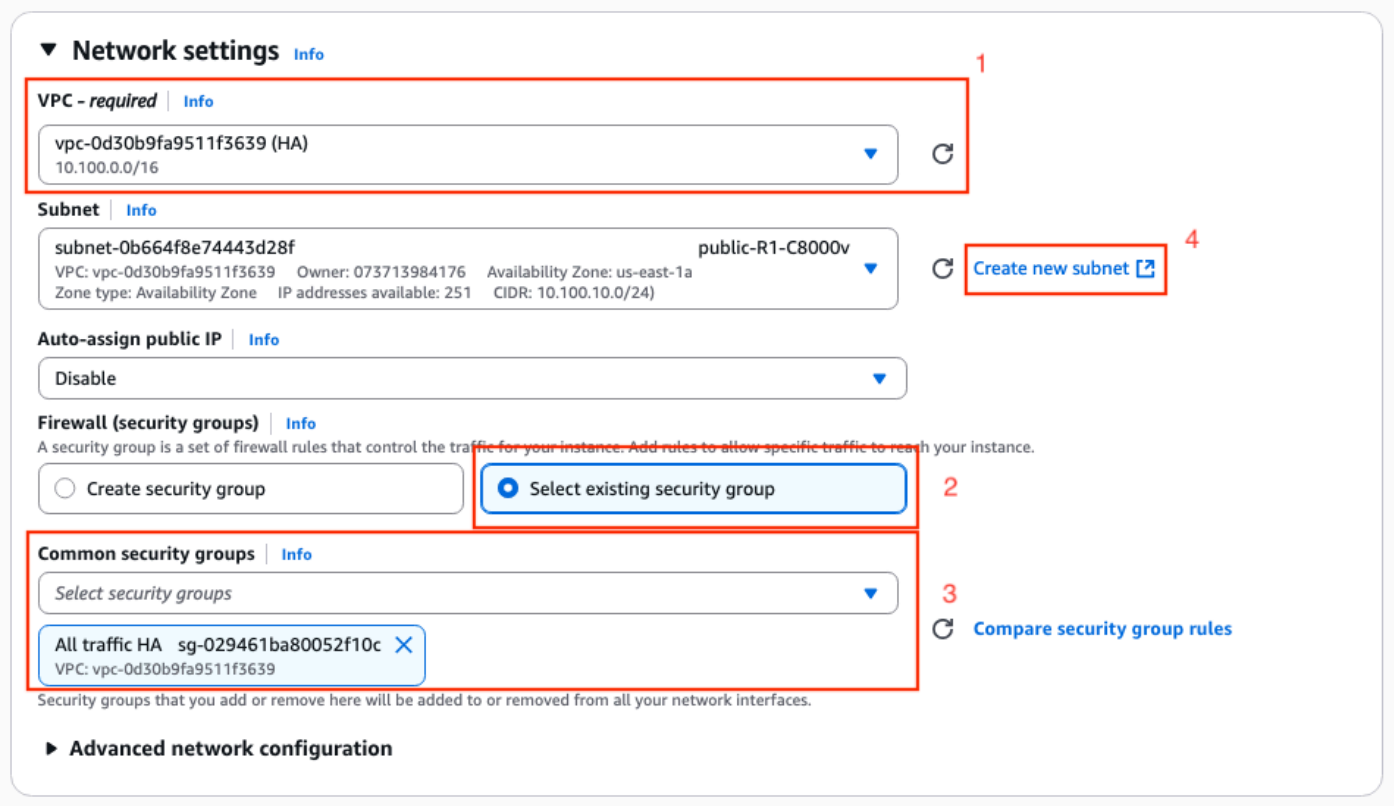
Stap 6.2. De subnetten voor de AMI maken en configureren

Klik in het gedeelte Netwerkinstellingen op Bewerken. Enkele nieuwe opties in de sectie zijn nu beschikbaar:
1. Selecteer de gewenste VPC voor dit werk. In dit voorbeeld wordt de VPC met de naam HA geselecteerd.

2. Selecteer in het gedeelte Firewall (beveiligingsgroepen) de optie Selecteer bestaande beveiligingsgroep.

3. Zodra optie 2 is geselecteerd, is de optie Gemeenschappelijke beveiligingsgroepen beschikbaar. Filter en selecteer de gewenste beveiligingsgroep. In dit voorbeeld wordt de beveiligingsgroep Alle HA-verkeer geselecteerd.

4. (Optioneel) Als er geen subnetten voor deze apparaten zijn gemaakt, klikt u op Nieuw subnet maken.



Er wordt een nieuw tabblad in de webbrowser geopend, dat u naar het gedeelte Subnet maken leidt:

1. Selecteer de bijbehorende VPC voor deze configuratie in de vervolgkeuzelijst.

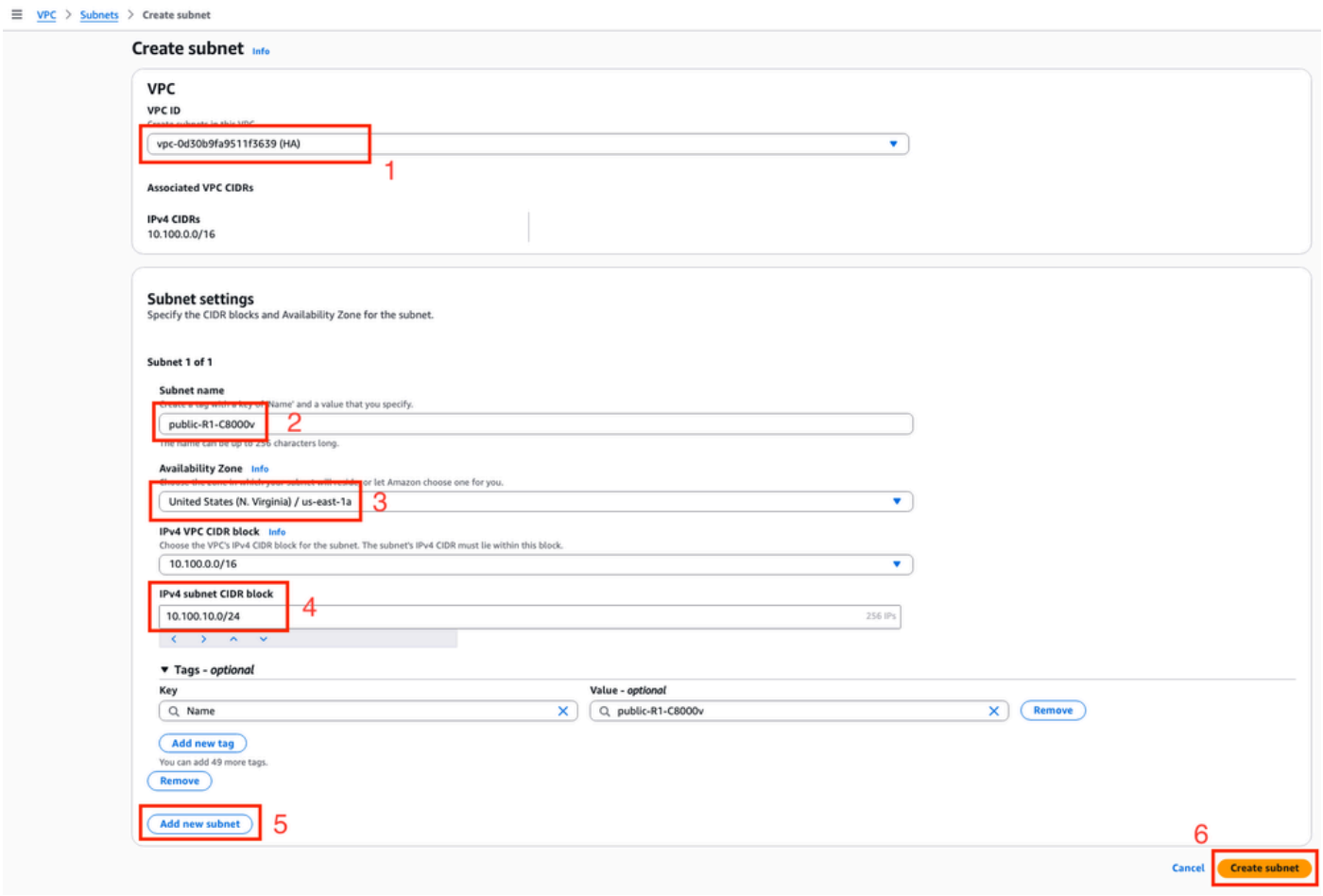
2. Stel een naam in voor het nieuwe subnet.

3. Definieer de beschikbaarheidszone voor dit subnet. (Raadpleeg de sectie Topologie van dit document voor meer informatie over de instelling)

4. Stel het subnetblok in dat hoort bij het VPC CIDR-blok.

5. Bovendien kunnen alle subnetten die worden gebruikt, worden gemaakt door op het gedeelte Nieuw subnet toevoegen te klikken en de stappen van 2 tot 4 voor elk subnet te herhalen.

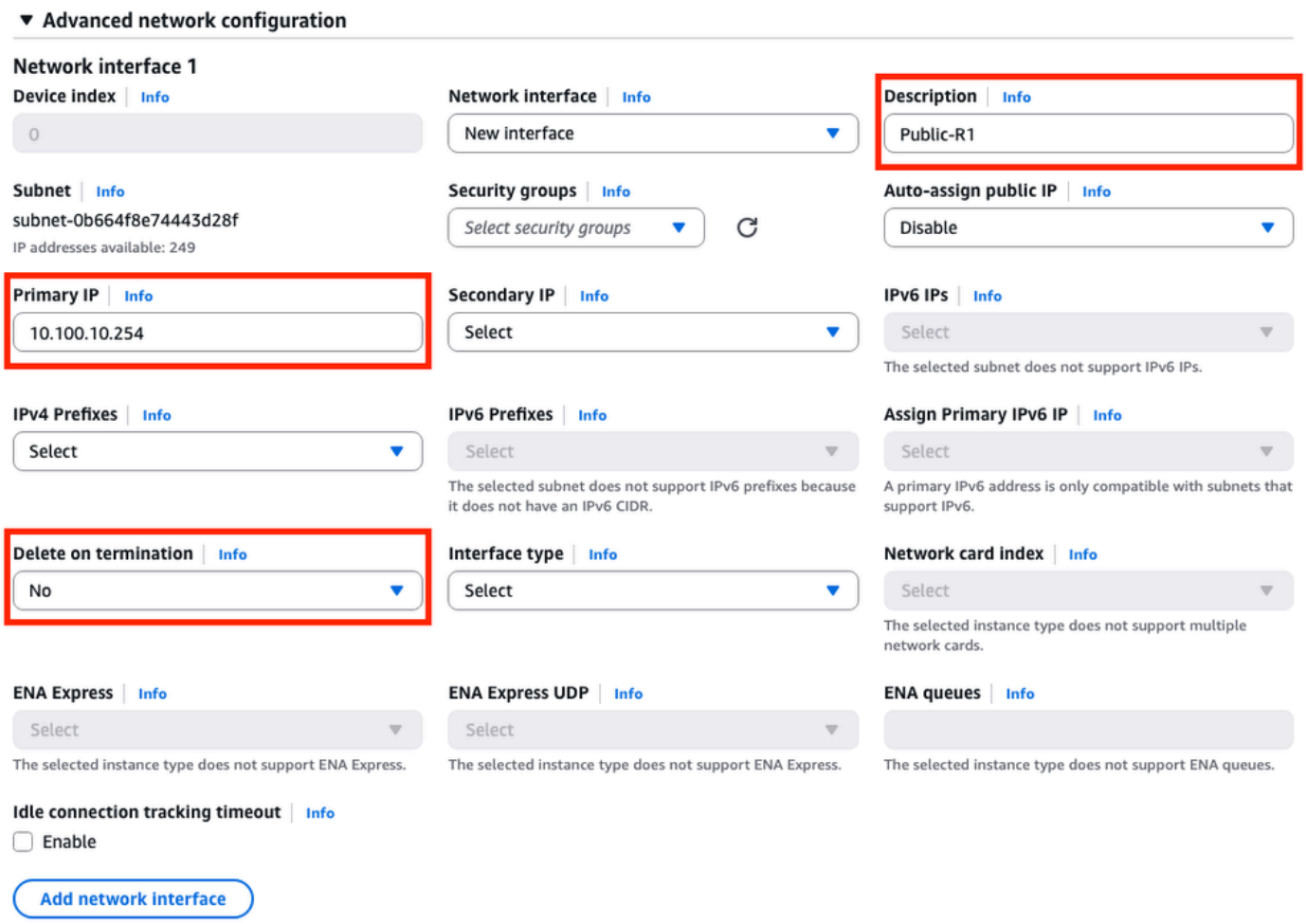
6. Als u klaar bent, klikt u op Subnet maken. Navigeer naar de vorige pagina om verder te gaan met de instellingen.



Klik in het subgedeelte Subnet van het gedeelte Netwerkinstellingen op het pictogram Vernieuwen om de gemaakte subnetten in de vervolgkeuzelijst op te halen.

Stap 6.3. De AMI-interfaces configureren

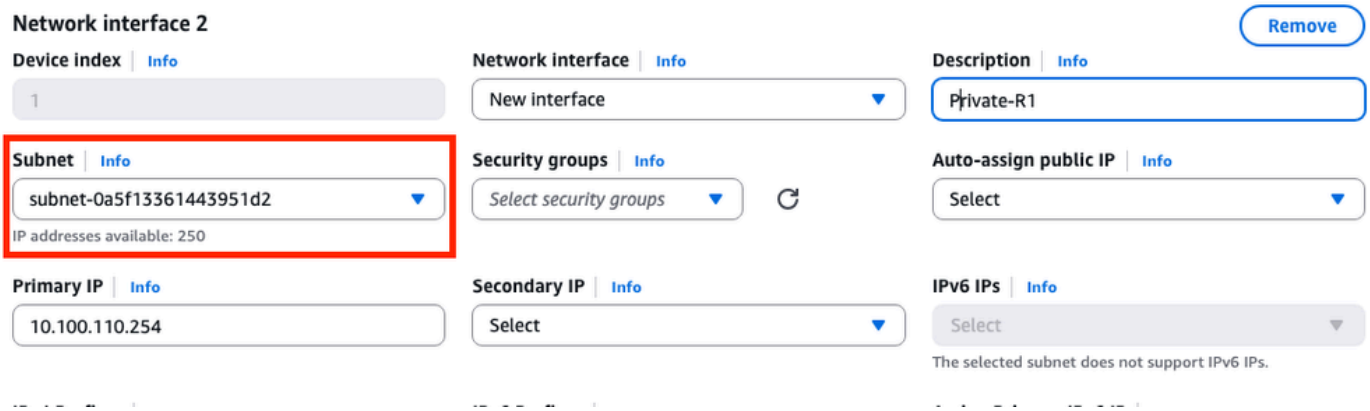
Vouw in het gedeelte Netwerkinstellingen de subsectie Geavanceerde netwerkconfiguratie uit. Deze opties worden weergegeven:



Stel in dit menu de parameters Beschrijving, Primair IP, Verwijderen bij beëindiging in. Gebruik voor de primaire IP-parameter elk IP-adres, behalve het eerste beschikbare adres van het subnet. Dit wordt intern gebruikt door AWS.

De parameter Verwijderen bij beëindiging in dit voorbeeld is ingesteld als Nee. Dit kan echter worden ingesteld op ja, afhankelijk van uw omgeving.

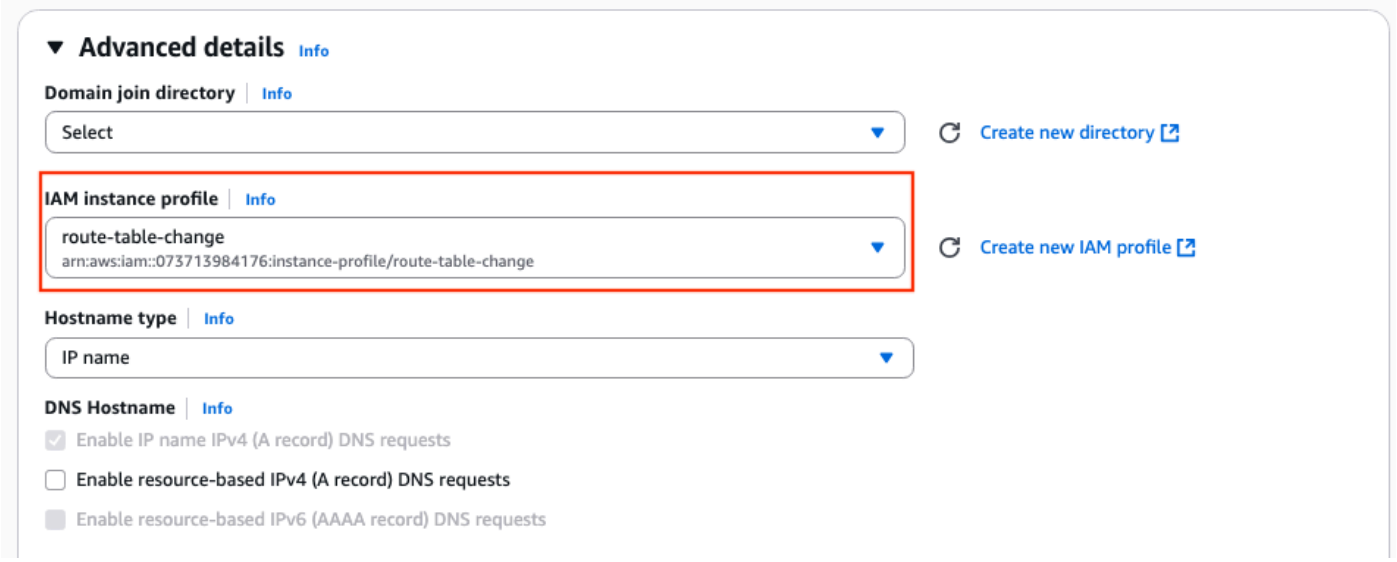
Vanwege deze topologie is een tweede interface nodig voor het private subnet. Klik op Netwerkinterface toevoegen en deze prompt wordt weergegeven. De interface biedt echter de optie om dit keer het subnet te selecteren:



Als alle parameters zijn ingesteld zoals is gedaan in de netwerkinterface 1, gaat u verder met de volgende stappen.

Stap 6.4. Stel het IAM-instantieprofiel in op de AMI

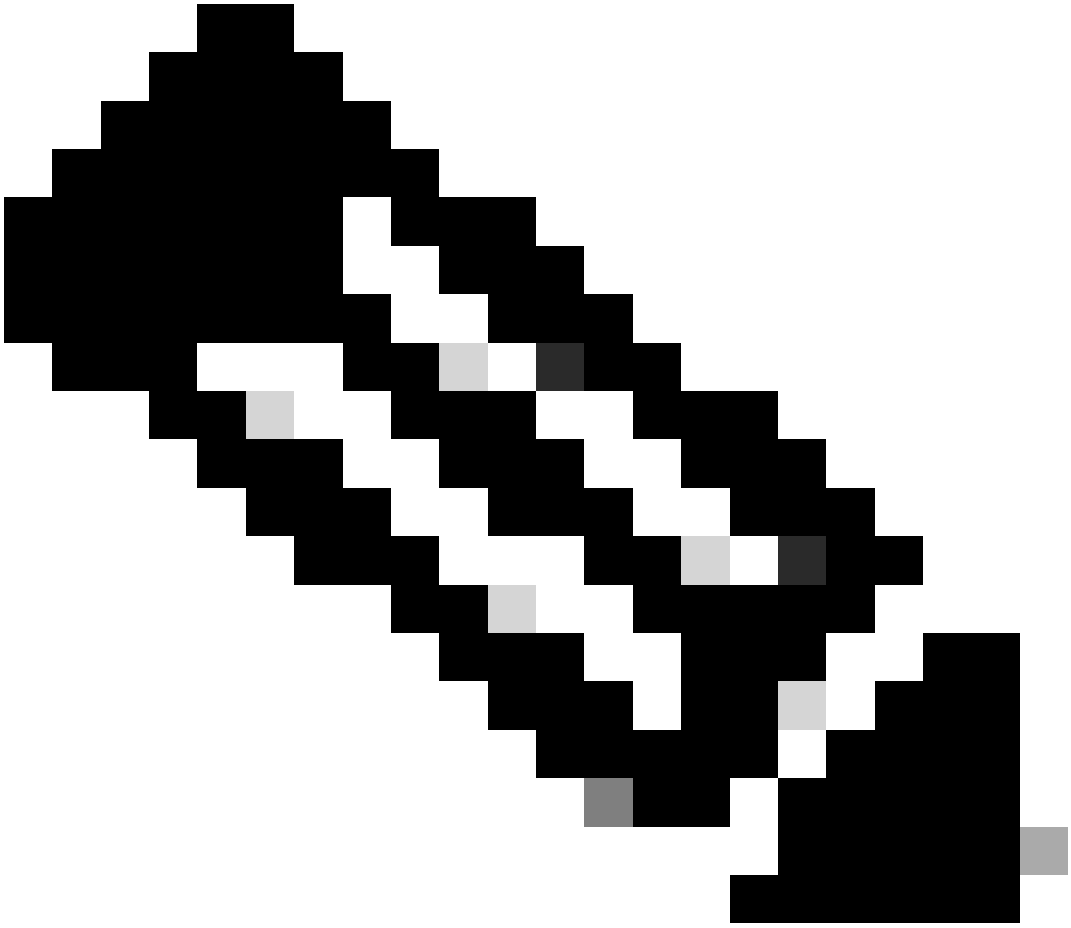
Selecteer in het gedeelte Geavanceerde details de gemaakte IAM-rol in de parameter IAM-instantieprofiel:



Stap 6.5. (Optioneel) Stel de referenties in op de AMI

Navigeer onder de sectie Geavanceerde details naar de sectie Gebruikersgegevens - optioneel en pas deze instelling toe om een gebruikersnaam en wachtwoord in te stellen terwijl de instantie wordt gemaakt:

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



Opmerking: de gebruikersnaam die door AWS aan SSH in de C8000v is opgegeven, kan onjuist als root worden vermeld. Wijzig dit indien nodig in ec2-gebruiker.

Stap 6.6. De instantieconfiguratie voltooien

Als alles is geconfigureerd, klikt u op Installatie starten:

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.

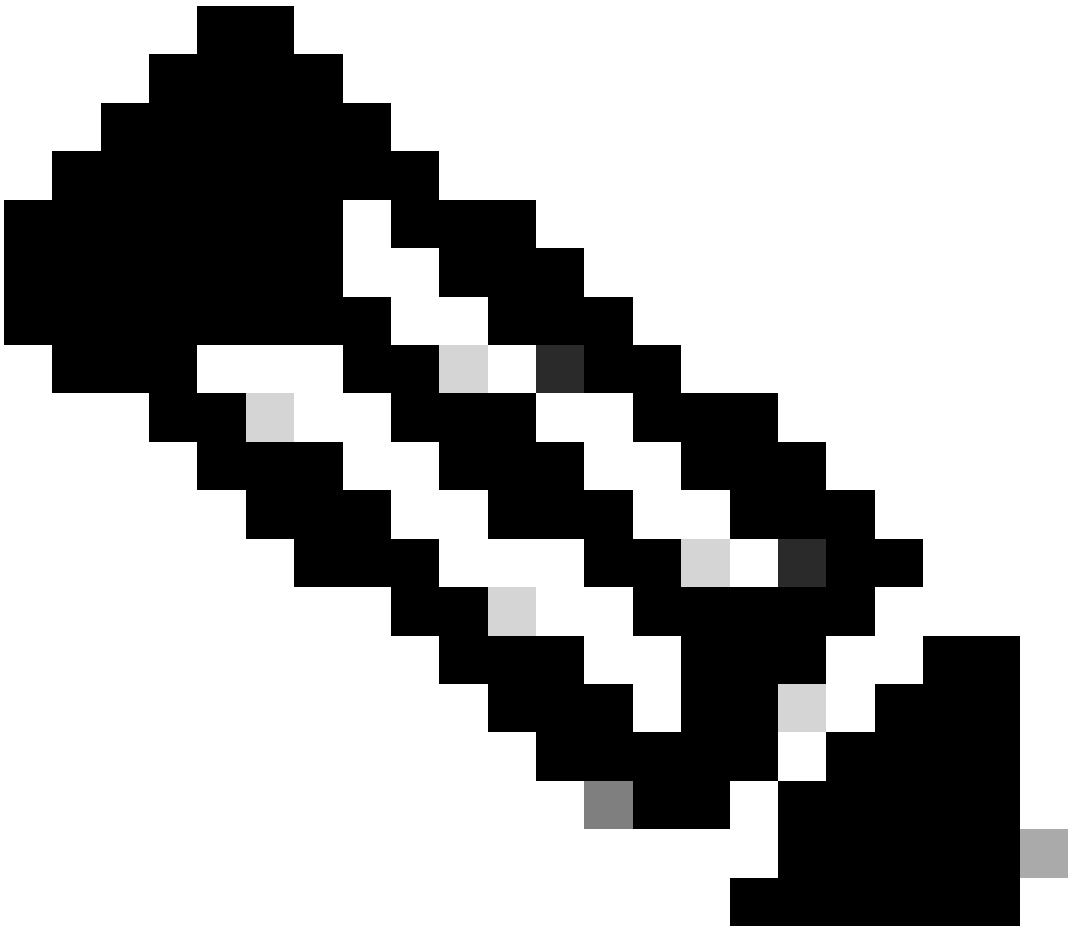
Cancel

Launch instance

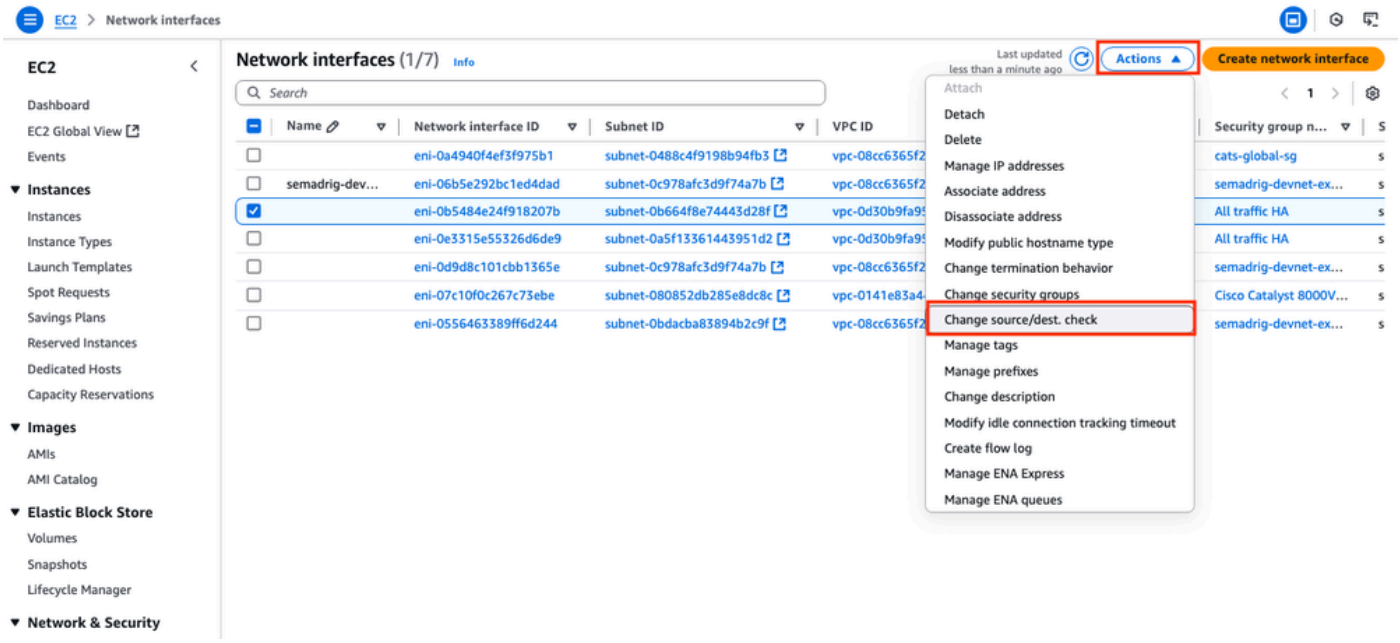
Preview code

Stap 6.7. Bron-/bestemmingscontrole op de ENI's uitschakelen

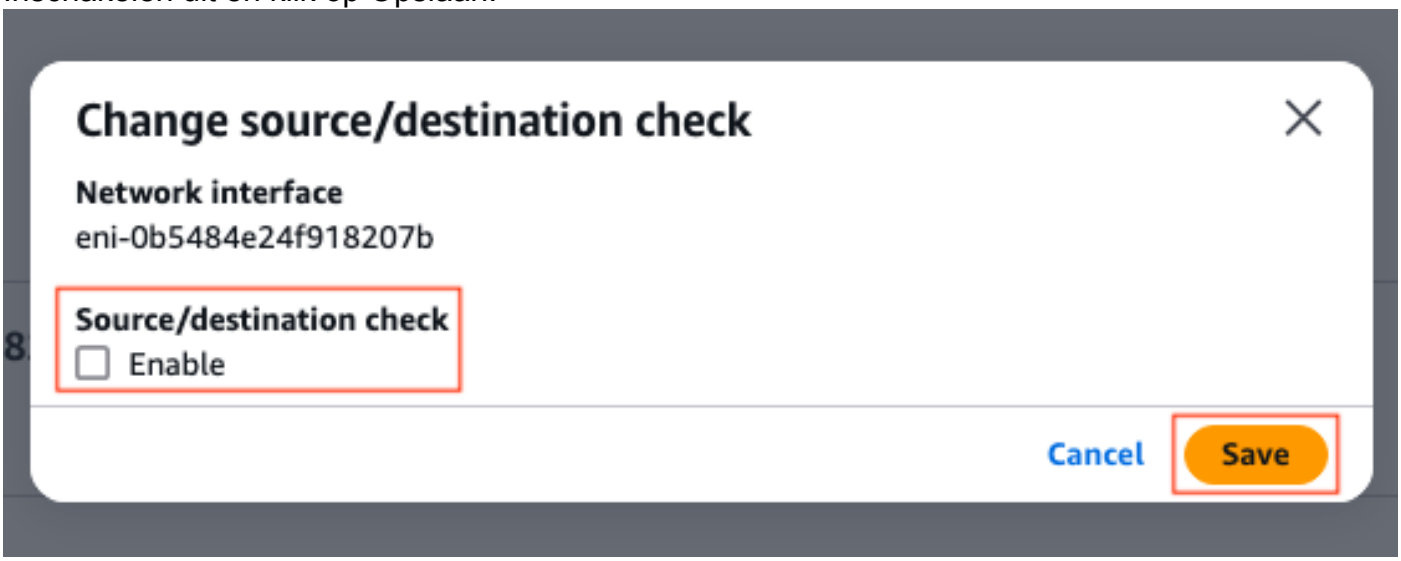
Als de instantie eenmaal is gemaakt, schakelt u de src/dst-controlefunctionaliteit op AWS uit om de connectiviteit tussen interfaces in hetzelfde subnet te verkrijgen. Selecteer in het gedeelte EC2 Dashboard > Network & Security > Network interfaces de ENI's en klik op Actions > Broncode wijzigen/uitzetten. controleren.



Opmerking: U moet de ENI's één voor één selecteren om deze optie beschikbaar te krijgen.



Er wordt een nieuw venster weergegeven. Schakel in het nieuwe menu het selectievakje Inschakelen uit en klik op Opslaan.

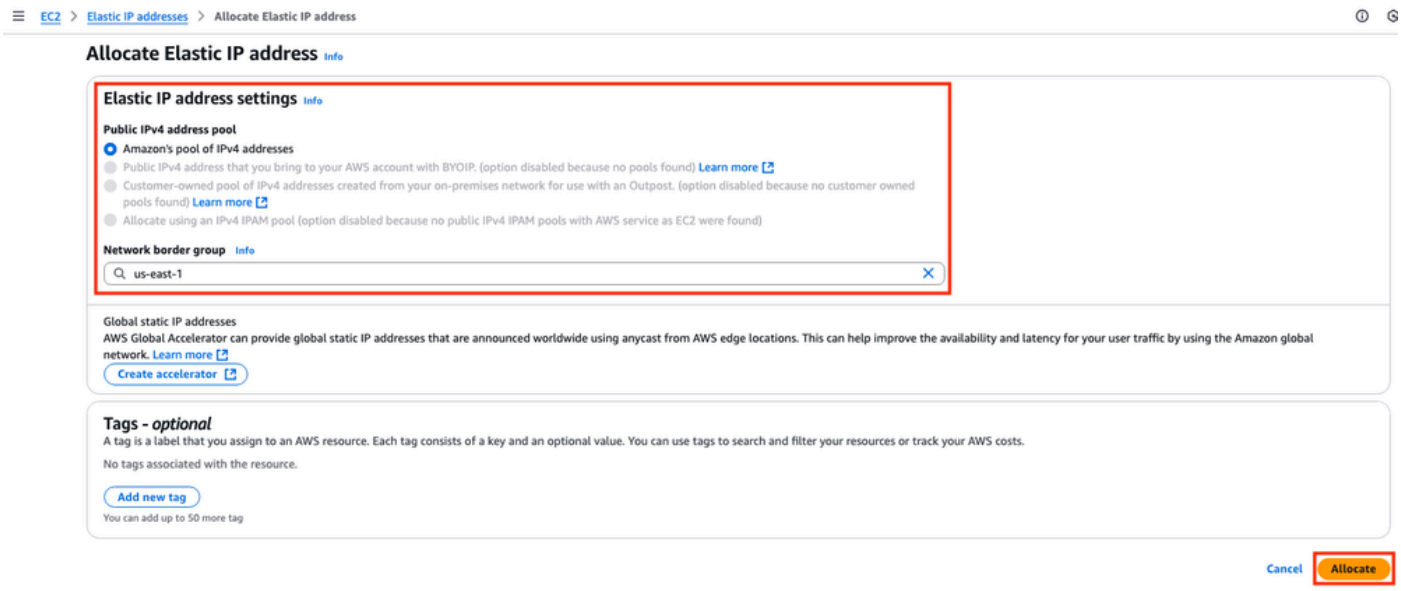


Stap 6.8. Een elastisch IP maken en koppelen aan het openbare ENI van de instantie

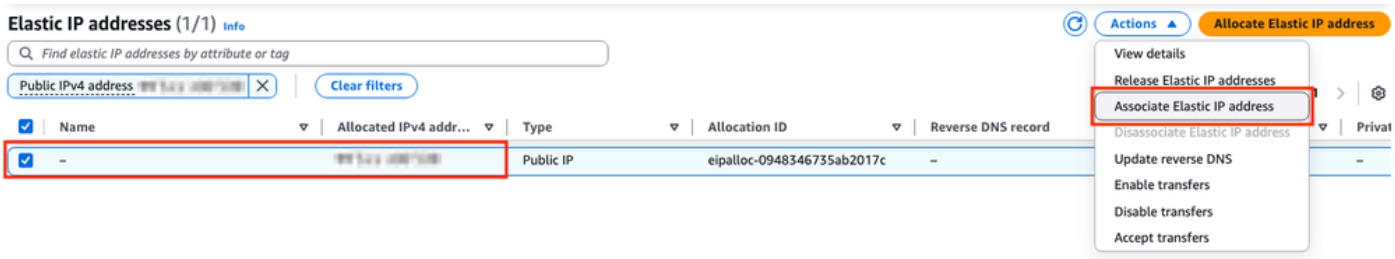
Klik in het gedeelte EC2 Dashboard > Network & Security > Elastic IPs op Allocate Elastic IP address (Elastisch IP-adres toewijzen).

De pagina leidt u naar de andere sectie. Voor dit voorbeeld wordt de optie Amazon-pool van IPv4-adressen geselecteerd samen met de beschikbaarheidszone us-east-1. Als u klaar bent, klikt u op

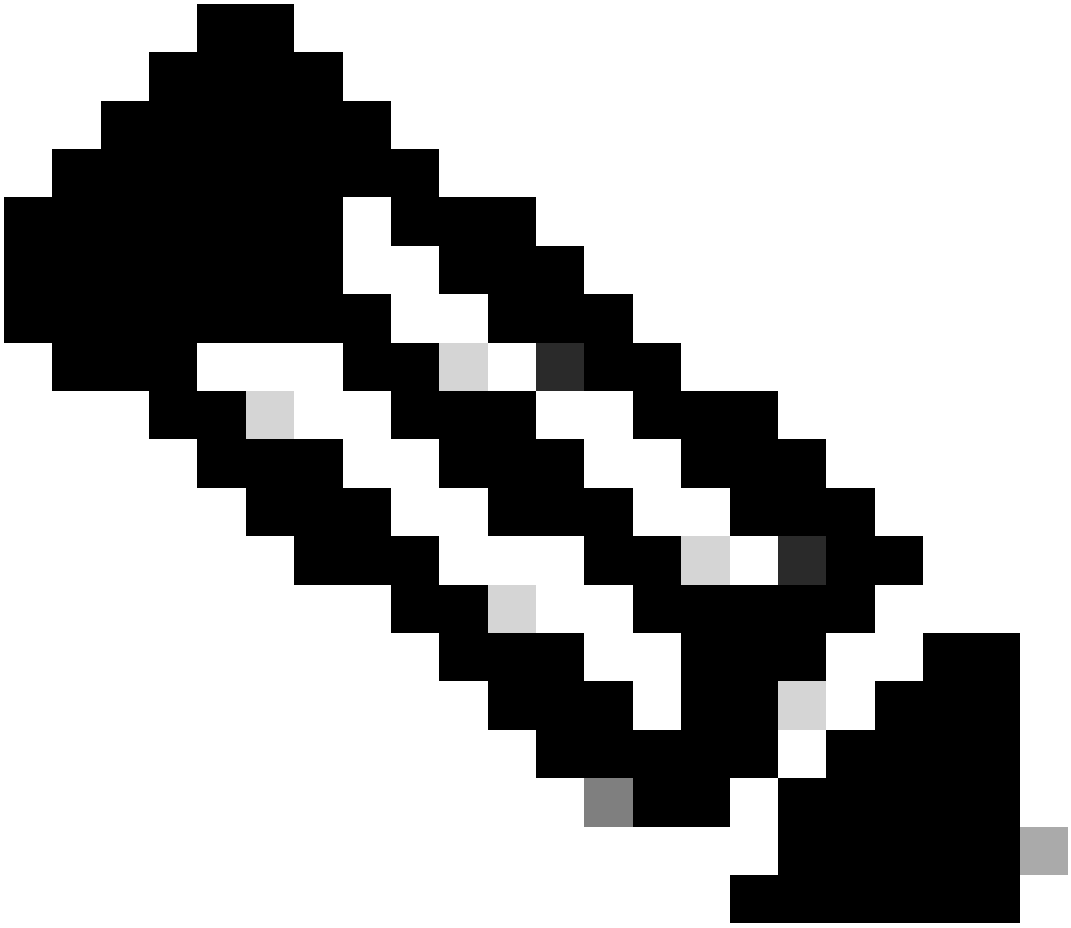
Toewijzen.



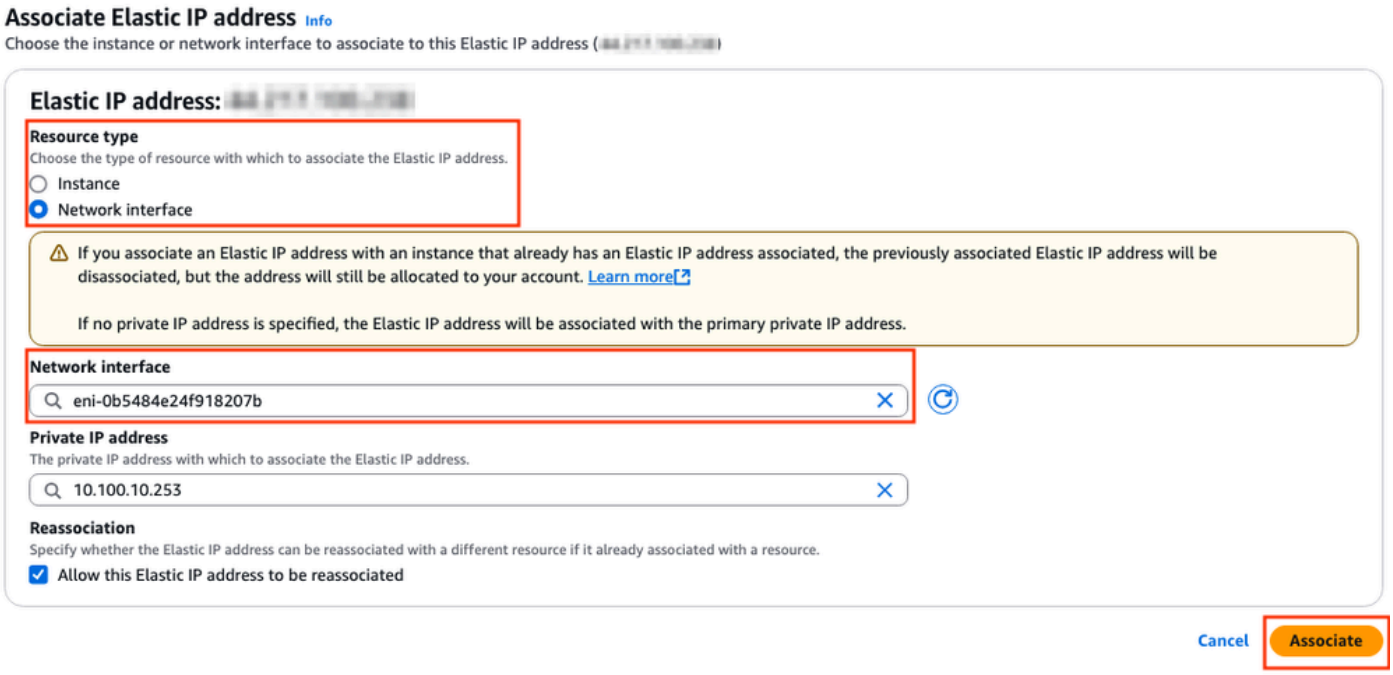
Wanneer het IP-adres is gemaakt, wijst u het IP-adres toe aan de openbare interface van de instantie. Klik in het gedeelte EC2 Dashboard > Network & Security > Elastic IPs op Actions > Associate Elastic IP address (Acties > Elastisch IP-adres koppelen).



Selecteer in deze nieuwe sectie de optie Netwerkinterface en zoek naar het openbare ENI van de bijbehorende interface. Koppel het bijbehorende openbare IP-adres en klik op Associëren.



Opmerking: Ga naar het gedeelte EC2 Dashboard > Instanties om de juiste ENI-ID te krijgen. Selecteer vervolgens de instantie en controleer de sectie Networking. Zoek naar het IP-adres van uw openbare interface om de ENI-waarde op dezelfde rij te krijgen.



Stap 7. Herhaal stap 6 om de tweede C8000v-instantie voor HA te maken

Raadpleeg de sectie Topologie van dit document voor de bijbehorende informatie voor elke interface en herhaal dezelfde stappen van 6.1 tot 6.6.

Stap 8. Herhaal stap 6 om een VM (Linux/Windows) te maken vanuit de AMI Marketplace

In dit voorbeeld wordt Ubuntu server 22.04.5 LTS geselecteerd uit de AMI Marketplace als de interne host.

ENS5 wordt standaard gemaakt voor de openbare interface. Maak in dit voorbeeld een tweede interface (ens6 op het apparaat) voor het privé-subnet.

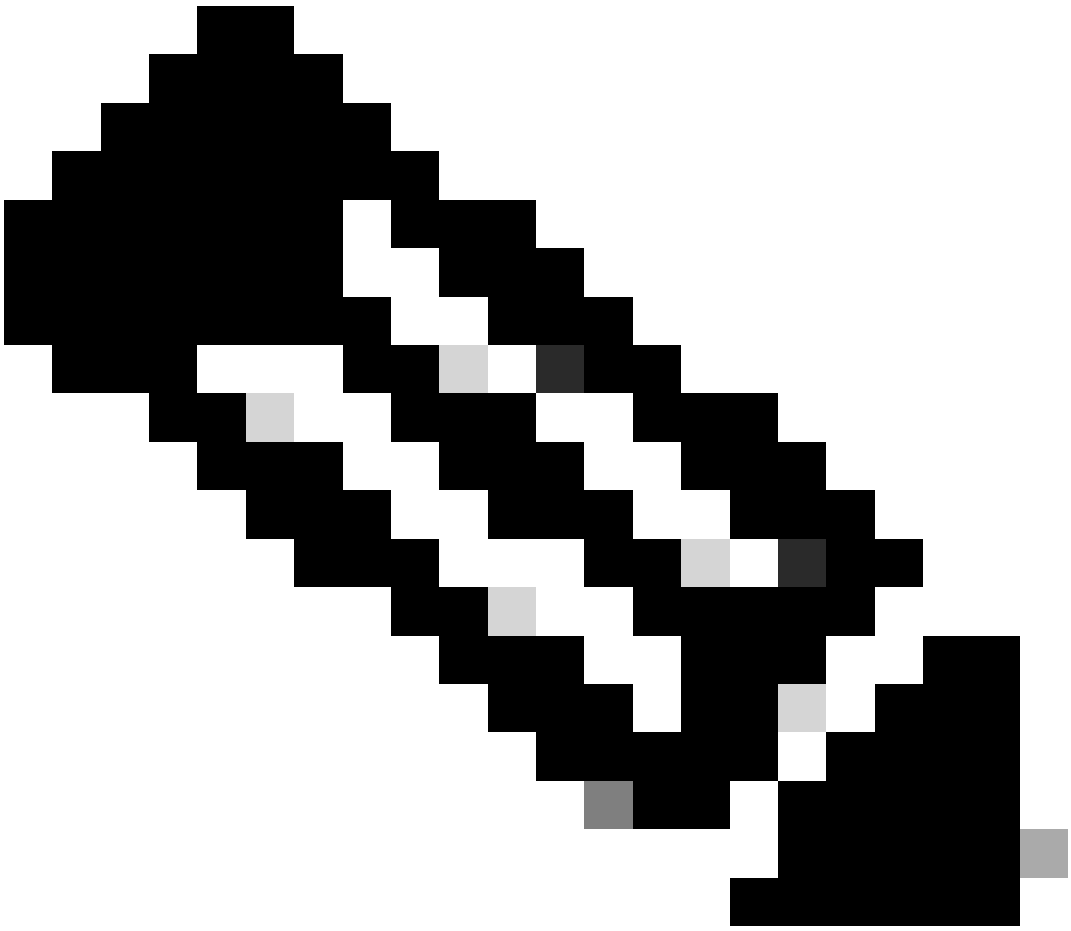
<#root>

```
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
```

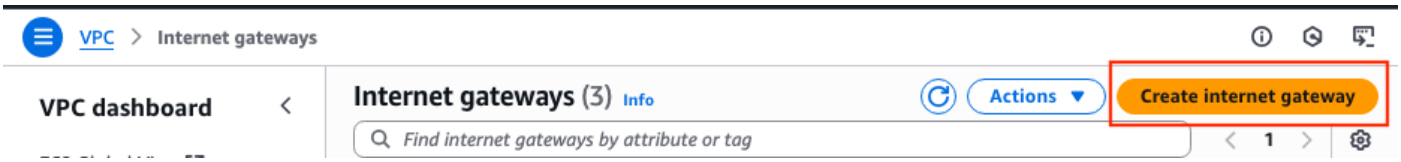
```
10.100.130.254

 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
```



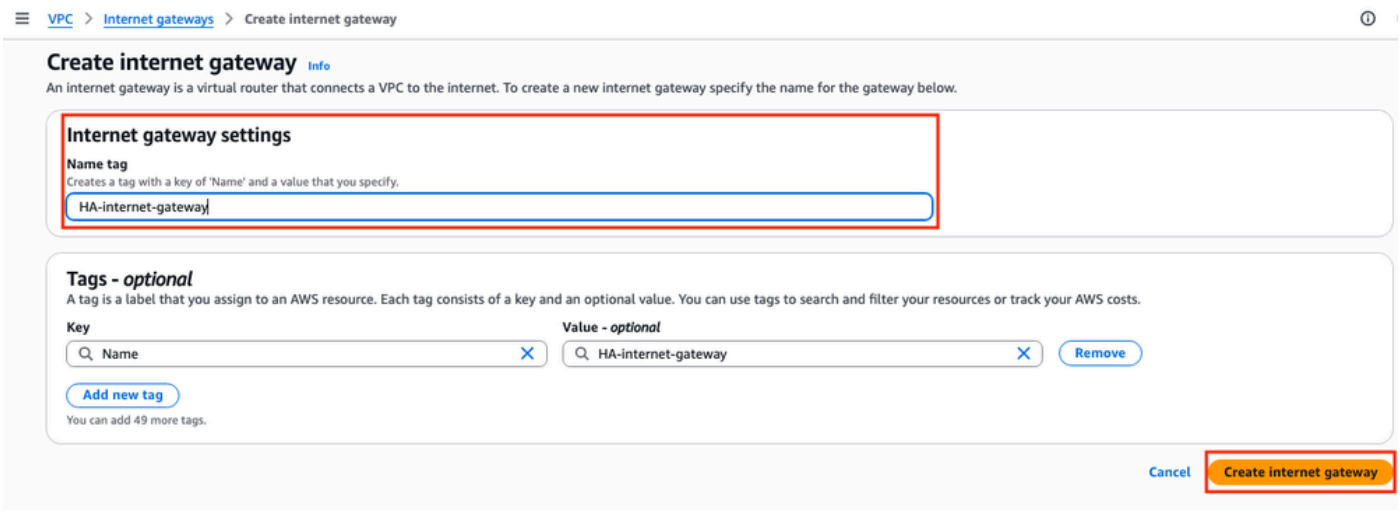
> Opmerking: als er wijzigingen zijn aangebracht in de interfaces, klept u de interface of laadt u de VM opnieuw om deze wijzigingen te laten toepassen.

Stap 9. Een Internet Gateway (IGW) voor de VPC maken en configureren

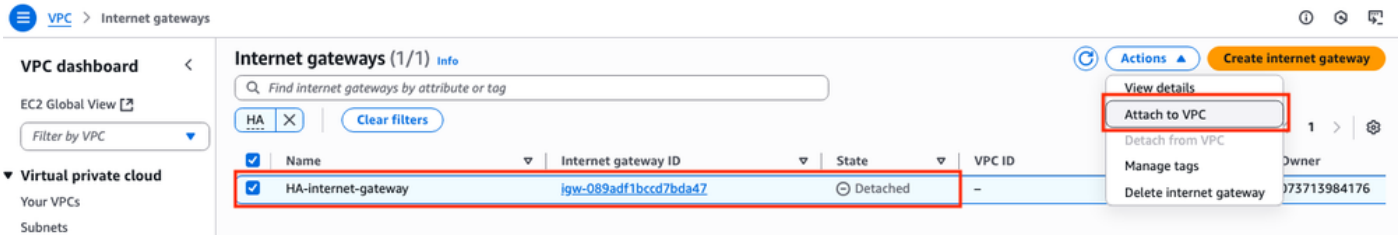
Klik in het gedeelte **VPC Dashboard > Virtual private cloud > Internet gateways** op **Internetgateway maken**.



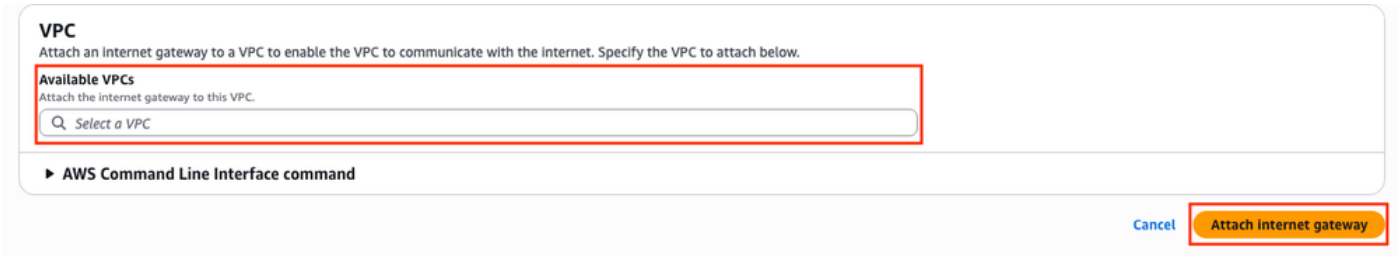
Maak in deze nieuwe sectie een **naamlabel aan** voor deze gateway en klik op **Internetgateway maken**.



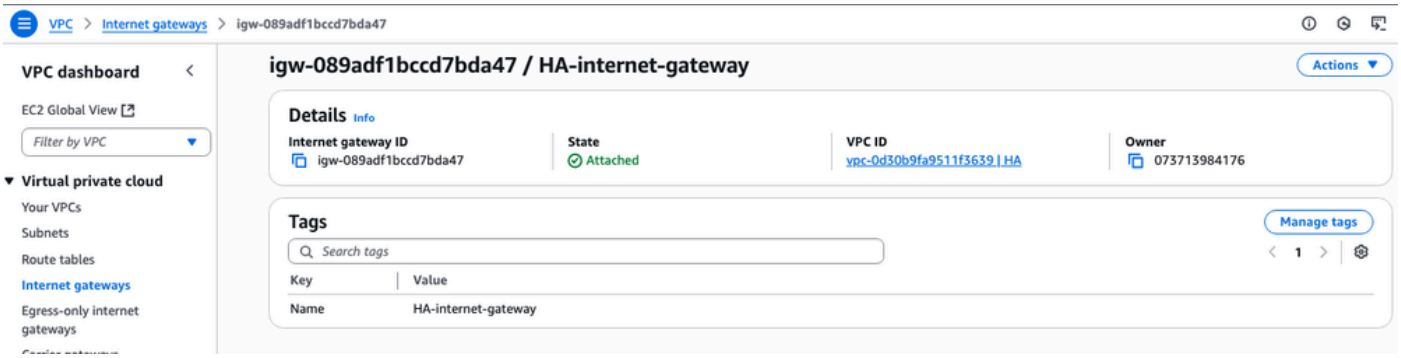
Zodra de IGW is gemaakt, koppelt u deze aan uw corresponderende VPC. Navigeer naar het gedeelte **VPC Dashboard > Virtual Private Cloud > Internet Gateway** en selecteer de bijbehorende IGW. Klik op **Acties > Bijvoegen aan VPC**.



Selecteer in deze nieuwe sectie de VPC met de naam **HA**. Klik in dit voorbeeld op **Internetgateway koppelen**.



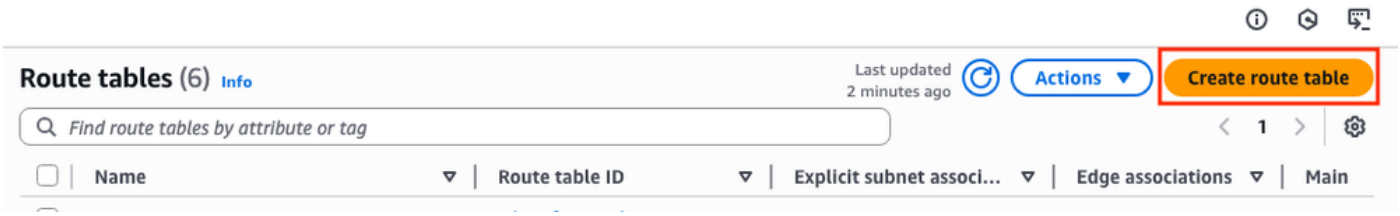
De IGW moet de bijgevoegde status aangeven zoals deze wordt weergegeven:



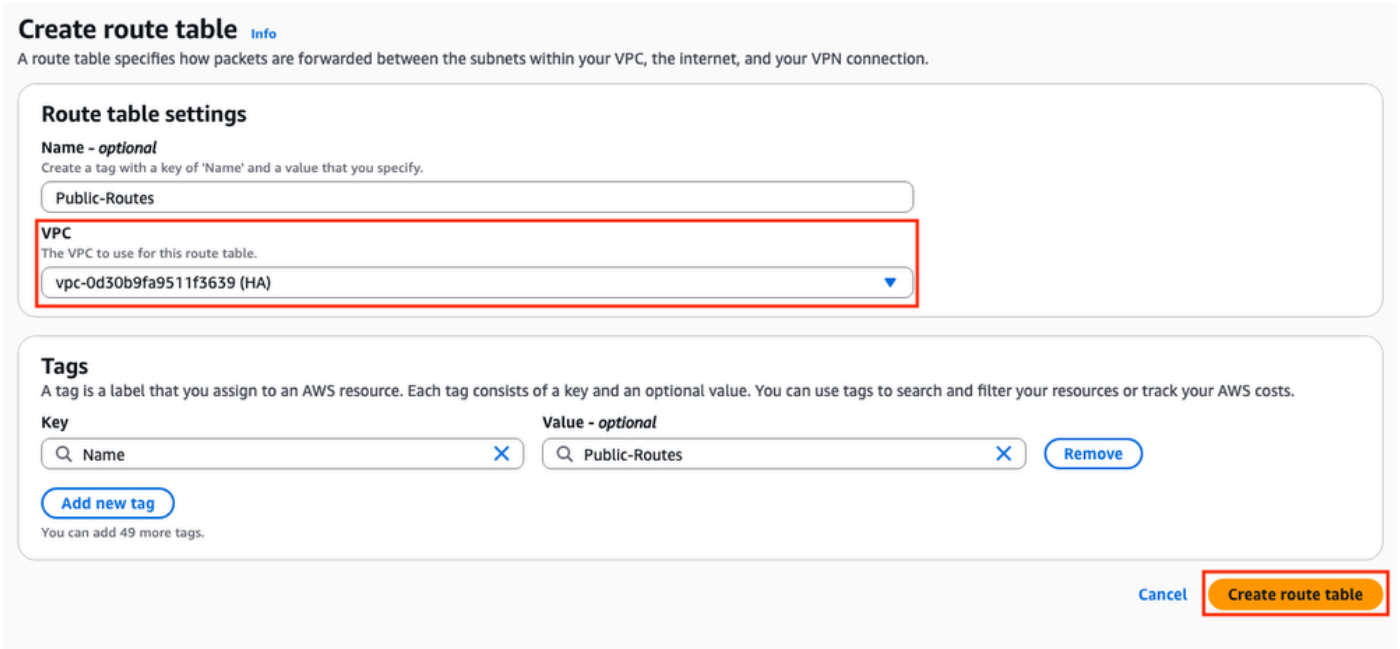
Stap 10. Routetabellen maken en configureren op AWS voor publieke en private subnetten

Stap 10.1. De openbare routetabel maken en configureren

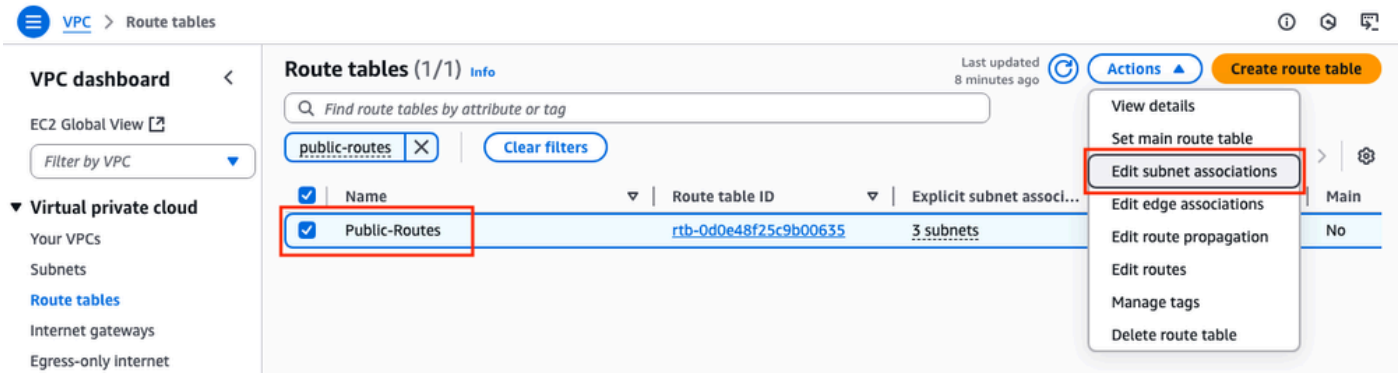
Om de HA op deze topologie vast te stellen, associëren alle publieke en private subnetten op hun overeenkomstige routetabellen. Klik in het gedeelte VPC Dashboard > Virtual Private Cloud > Routetabellen op Routetabel maken.



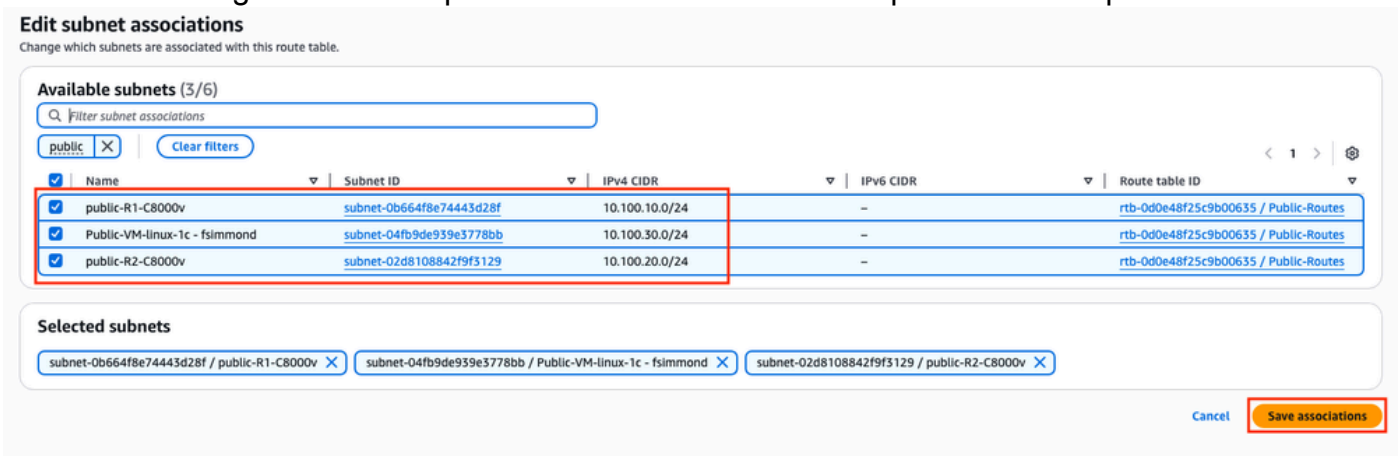
Selecteer in de nieuwe sectie de corresponderende VPC voor deze topologie. Klik op Routetabel maken als u deze optie hebt geselecteerd.



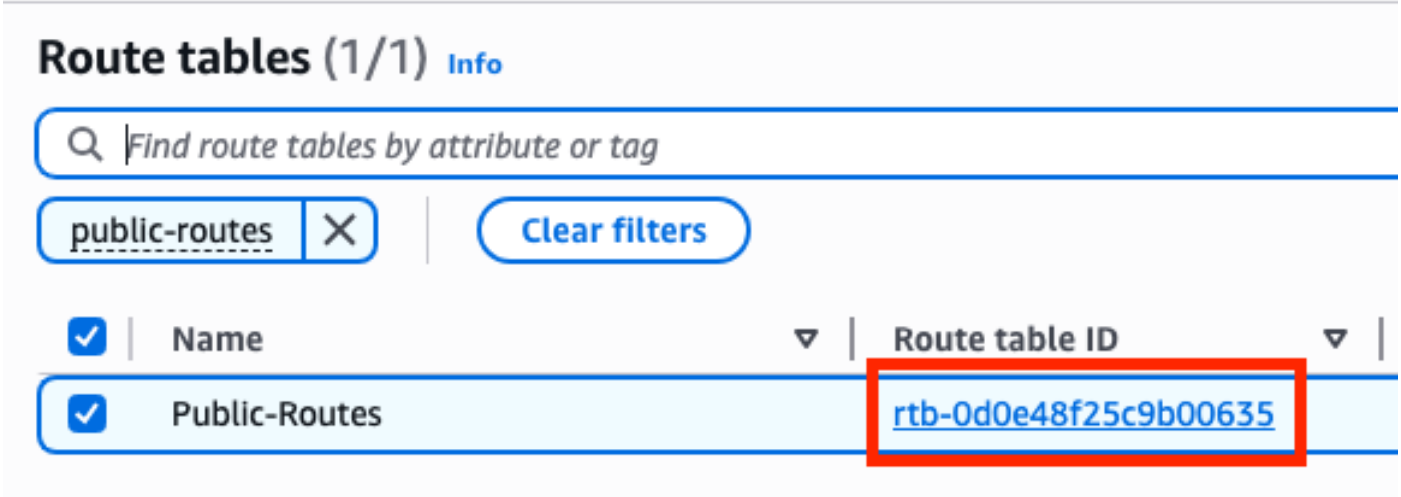
Selecteer in de sectie Routetabellen de gemaakte tabel en klik op Acties > Subnetassociaties bewerken.



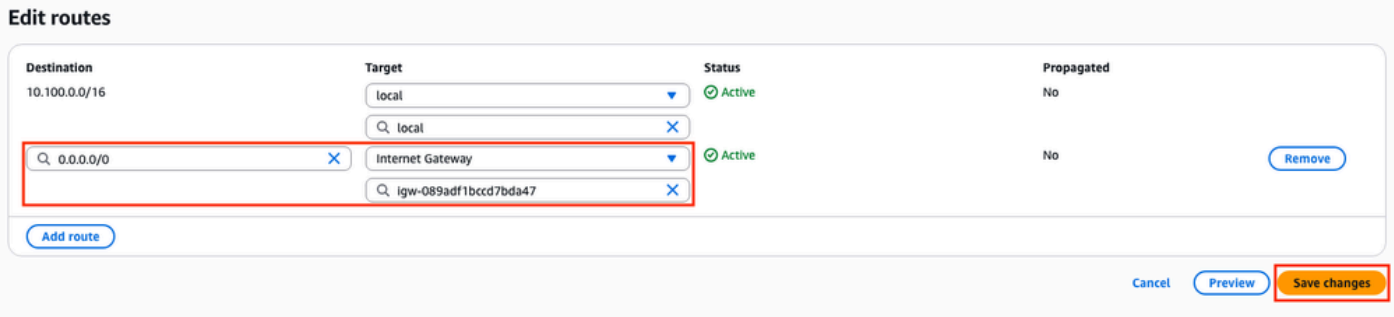
Selecteer vervolgens de corresponderende subnetten en klik op Associaties opslaan.



Zodra de subnetten zijn gekoppeld, klikt u op de ID-hyperlink van de routetabel om de juiste routes voor de tabel toe te voegen. Klik vervolgens op Routes bewerken:

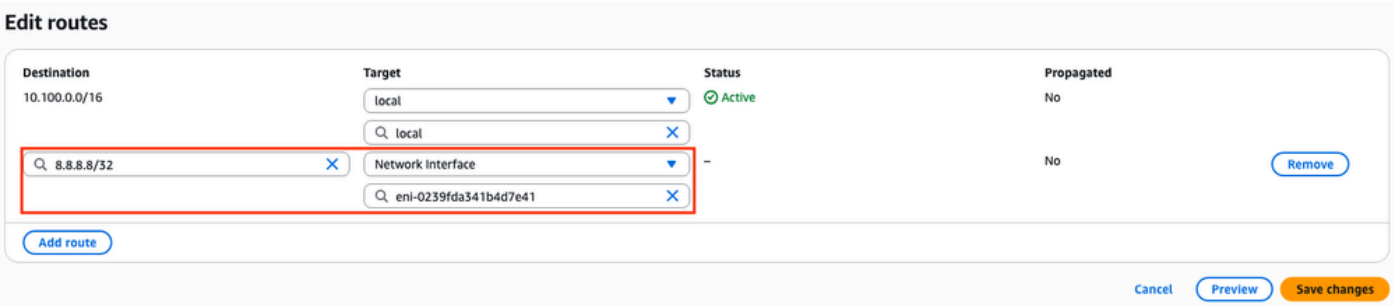


Om toegang tot internet te krijgen, klikt u op Route toevoegen en koppelt u deze openbare routetabel aan de IGW gemaakt op Stap 9 met deze parameters. Klik op Wijzigingen opslaan zodra u deze optie hebt geselecteerd:



Stap 10.2. De privéroutetabel maken en configureren

Nu de openbare routetabel is gemaakt, repliceert u stap 10 voor de privéroute en privésubnetten, behalve voor de toevoeging van de Internet Gateway op de routes. In dit voorbeeld ziet de routeringstabel er als volgt uit, omdat het verkeer voor 8.8.8.8 door het privé-subnet moet gaan in dit voorbeeld:



Stap 11. Basisnetwerkconfiguratie, netwerkadresvertaling (NAT), GRE-tunnel met BFD en routeringsprotocol controleren en configureren

Nadat de Instances en de routeringsconfiguratie op AWS zijn voorbereid, configureert u de apparaten:

Configuratie 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
```

Configuratie 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
```

Stap 12. Hoge beschikbaarheid configureren (Cisco IOS® XE Denali 16.3.1a of hoger)

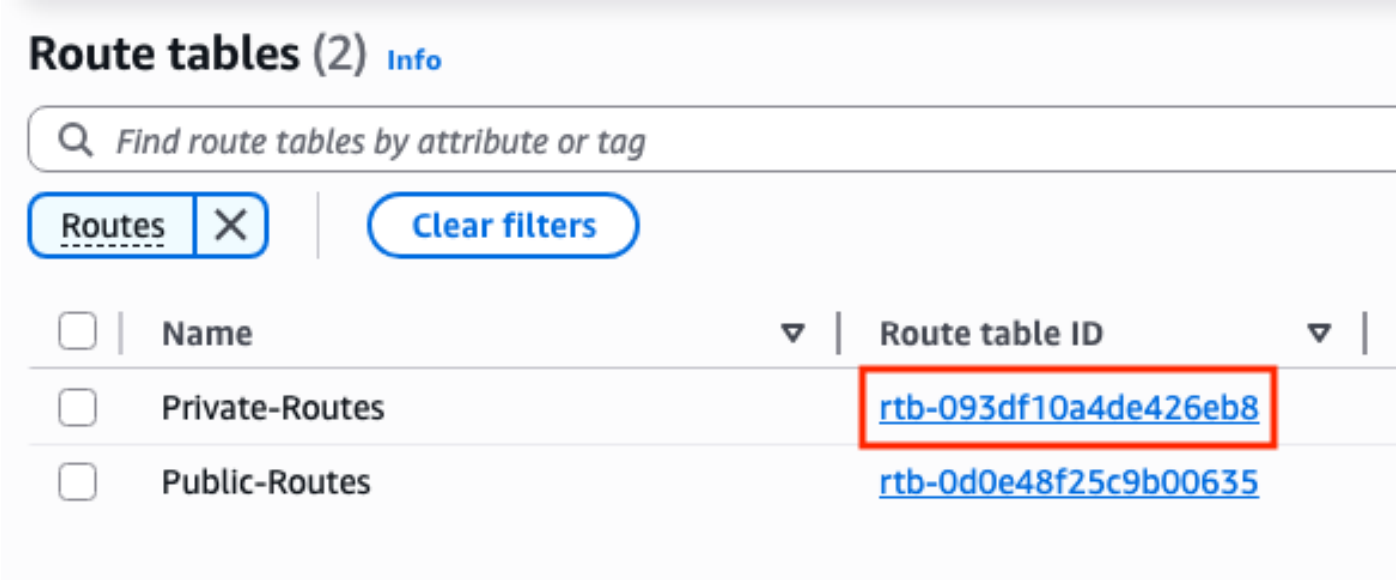
Nu de redundantie en verbinding tussen VM's zijn ingesteld, configureert u de instellingen voor de hoge beschikbaarheid om de routeringswijzigingen te definiëren. Stel de waarden Route-table-id, Network-interface-id en CIDR in die moeten worden ingesteld na een AWS HA-fout zoals BFD peer down.

```
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>
```

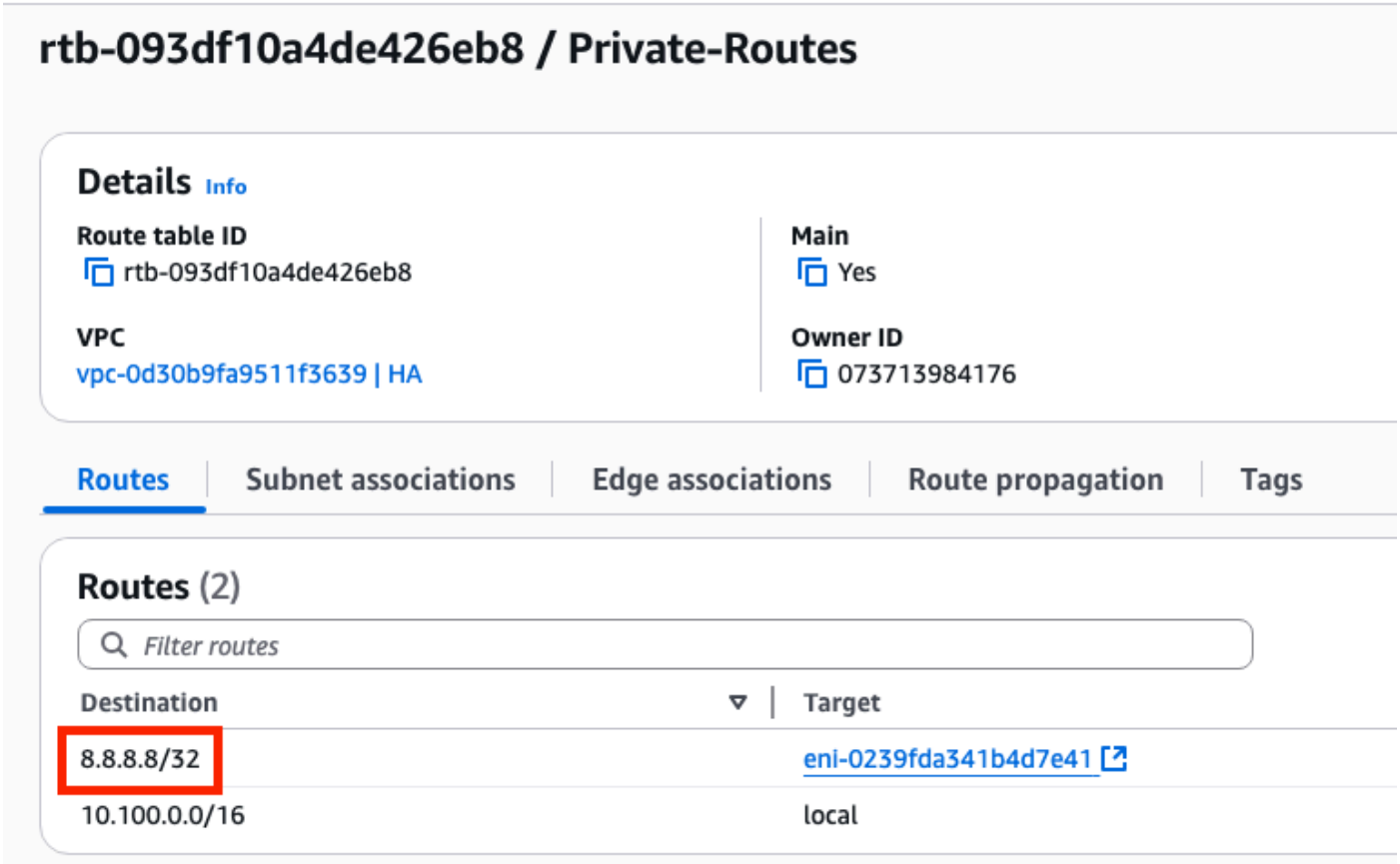
De bfd peer parameter is gerelateerd aan het Tunnel peer IP adres. Dit kan worden gecontroleerd met behulp van de show bfd buur uitgang:

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

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

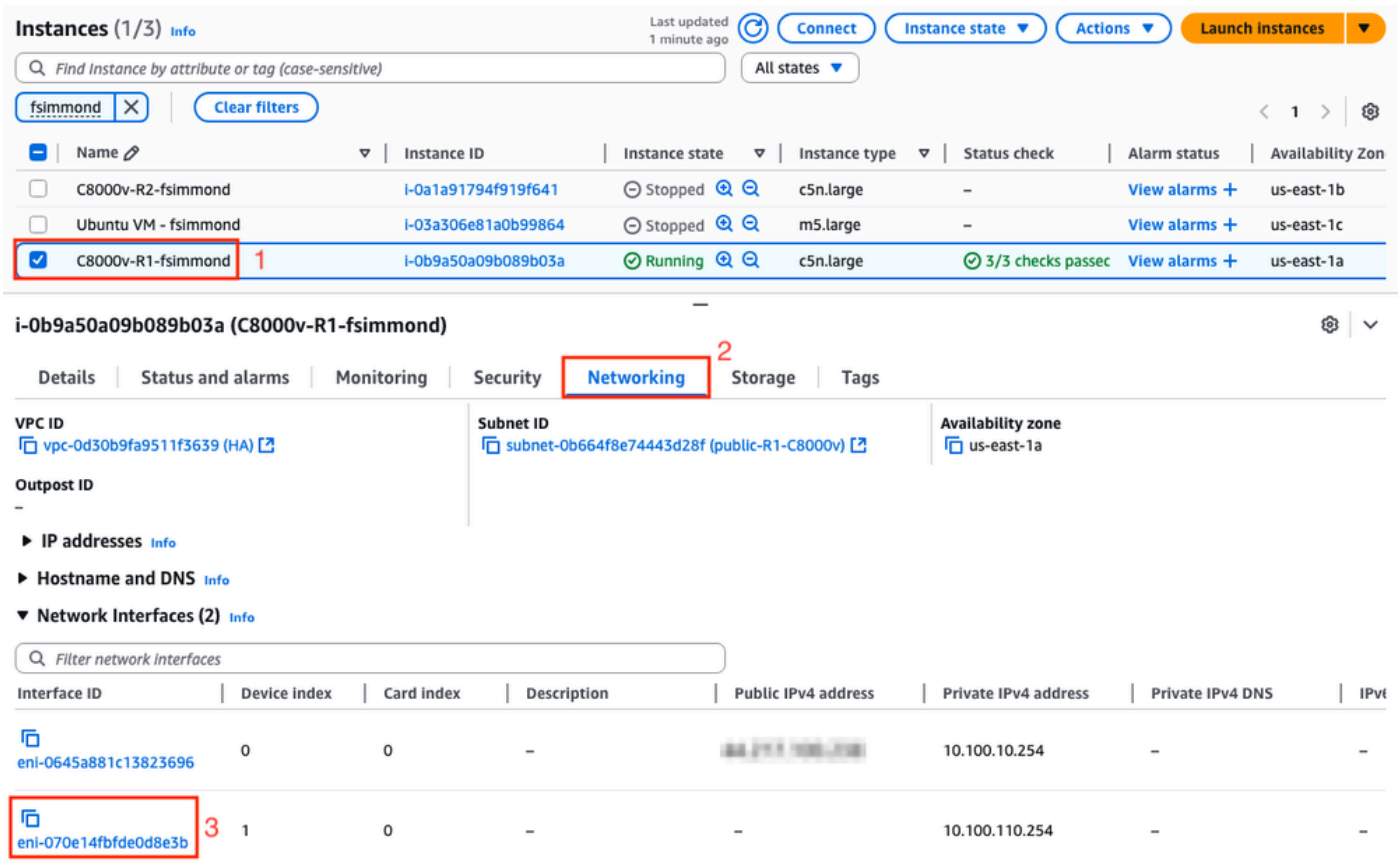
De parameter routetabel is gerelateerd aan de ID van de privéroutetabel in het gedeelte VPC Dashboard > Virtual Private Cloud > Routetabellen. Kopieer de bijbehorende Route Table ID.



De parameter cidrip is gerelateerd aan het routevoorvoegsel dat is toegevoegd aan de privéroutetabel (routes die zijn gemaakt in stap 10.2):



De parameter eni is gerelateerd aan de ENI-ID van de corresponderende privé-interface van de instantie die wordt geconfigureerd. In dit voorbeeld wordt de ENI-ID van de GigabitEthernet2-interface van de instantie gebruikt:



De regioparameter is gerelateerd aan de codenaam in de AWS-documentatie voor de regio waar de VPC zich bevindt. In dit voorbeeld wordt de us-east-1 regio gebruikt.

Deze lijst kan echter veranderen of groeien. Ga voor de laatste updates naar AmazonRegion en het document Beschikbaarheidszones.

Rekening houdend met al deze informatie, is hier het configuratievoorbeeld voor elke router in de VPC:

Configuratievoorbeeld voor 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
```

Configuratievoorbeeld voor 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
```

Verificatie

1. Controleer die status van de C8000v R1-instantie. Bevestig dat de Tunnel en de Cloud-redundantie actief zijn.

```
R1#show bfd neighbors

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

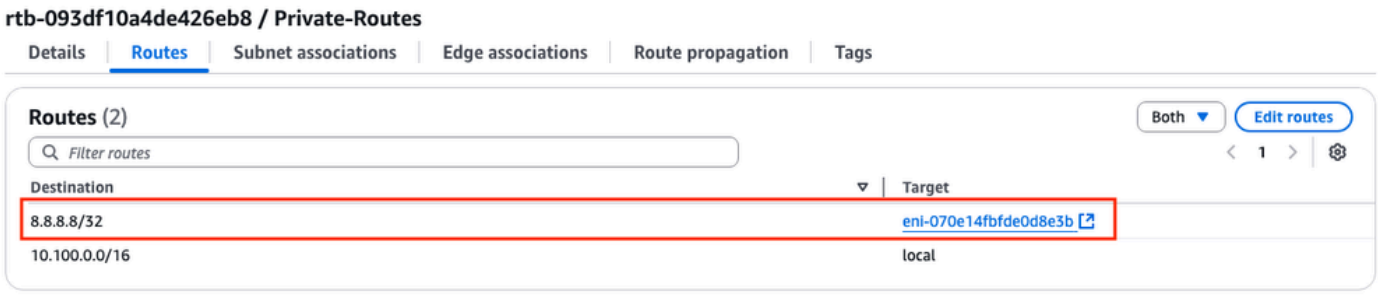
```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.200.2 Tu1 10 00:16:52 2 1470 0 2
```

```
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. Voer een continue ping uit naar 8.8.8.8 vanaf de host-VM die zich achter de routers bevindt. Zorg ervoor dat de ping via de privé-interface verloopt:

```
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. Open de AWS WebGUI en controleer de status van de routing tabel. De huidige ENI behoort tot de privé-interface van de R1-instantie:



4. Activeer de routewijziging door de Tunnel1-interface op de R1-instantie af te sluiten om een HA-failover-gebeurtenis te simuleren:

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

5. Controleer nogmaals bij de route tabel op AWS, de ENI ID is veranderd in de R2 private interface ENI ID:

Problemen oplossen

Dit zijn de meest voorkomende punten die vaak worden vergeten / verkeerd geconfigureerd tijdens het opnieuw maken van de implementatie:

- Zorg ervoor dat de middelen worden gekoppeld. Bij het maken van VPC, subnetten, interfaces, routetabellen, enzovoort, worden veel van deze niet automatisch aan elkaar gekoppeld. Ze hebben geen kennis van elkaar.
- Zorg ervoor dat de Elastic IP en eventuele Private IP is gekoppeld aan de juiste Interfaces, met de juiste subnetten, toegevoegd aan de juiste Route Table, aangesloten op de juiste router, en de juiste VPC en Zone, gekoppeld aan de IAM Rol en beveiligingsgroepen.

- Schakel de controle Bron/Dest uit per ENI.
  Als u al alle punten hebt gecontroleerd die in dit gedeelte worden besproken en het probleem nog steeds aanwezig is, verzamelt u deze uitgangen, test u de HA-failover, indien mogelijk, en opent u een case met Cisco TAC:

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.