CSR1000v HA-implementatiegids voor redundantie op Amazon AWS

Inhoud

Inleiding

Dit document beschrijft de configuratiehandleiding voor het implementeren van CSR1000v-routers voor hoge beschikbaarheid op de Amazon AWS-cloud. Het is bedoeld om gebruikers praktische kennis van HA en het vermogen om een volledig functioneel testbed in te zetten.

Raadpleeg de sectie voor meer informatie over AWS en HA.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Een Amazon AWS account
- 2 CSR1000v en 1 Linux/Windows AMI's in dezelfde regio
- HA versie 1 wordt ondersteund op Cisco IOS-XE® versies 16.5 tot 16.9. Vanaf 16.11 en verder, gebruik HA versie 3.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS-XE® Denali 16.7.1.

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.

Doel

In een omgeving met meerdere beschikbaarheidszones simuleert u continu verkeer van het privédatacenter (VM) naar het internet. Simuleer een HA failover en merk op dat HA slaagt als de routing table switches verkeer van CSRHA naar CSRHA1's private interface wordt bevestigd.

Topologie

Alvorens de configuratie begint, is het belangrijk om de topologie en het ontwerp volledig te begrijpen. Dit helpt om eventuele problemen later op te lossen.

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

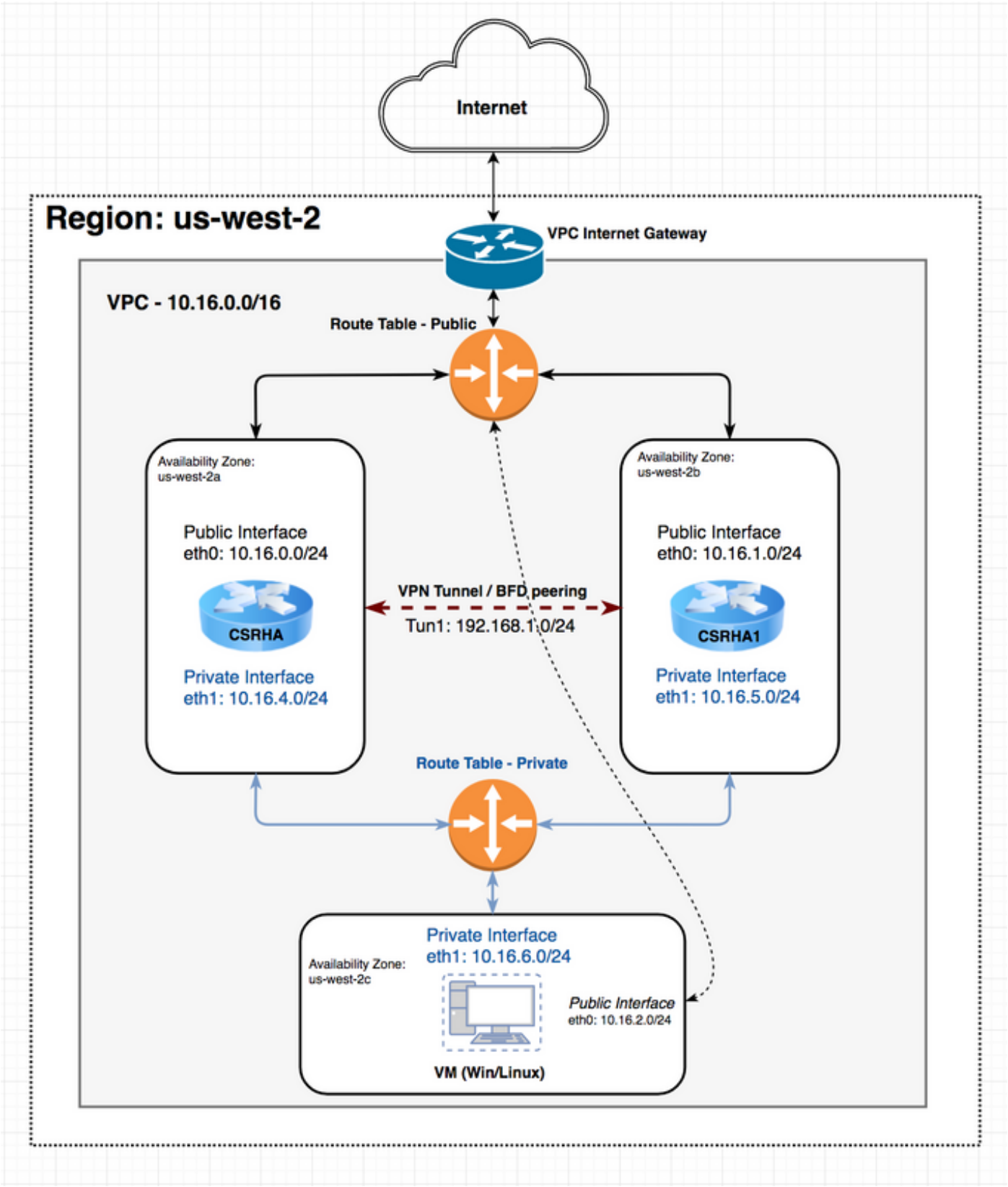
- 1x - Regio
- 1x - VPC
- 3x - Beschikbaarheidszones
- 6x - Netwerkinterfaces/subnetten (3x publiek/3x privé-gericht)
- 2x - Routetabellen (openbaar en privé)
- 2x - CSR1000v-routers (Cisco IOS-XE® Denali 16.3.1a of hoger)
- 1x - VM (Linux/Windows)

Er zijn 2x CSR1000v routers in een HA-paar, in twee verschillende beschikbaarheidszones. Denk aan elke beschikbaarheidszone als een apart datacenter voor extra hardwareresistentie.

De derde zone is een VM, die een apparaat simuleert in een privé datacenter. Voorlopig is internettoegang via de openbare interface ingeschakeld, zodat u de VM kunt openen en configureren. Over het algemeen, zou al normaal verkeer door de privé routetabel moeten stromen.

Pingen van de privé-interface van de VM → privé-routetabel → CSRHA → 8.8.8.8 voor verkeerssimulatie. In een failover scenario, neem waar de privé routetabel de route heeft geschakeld om aan de privé interface van CSRHA1 te richten.

Netwerkdiagram



Terminologie

RTB - De routetabel-ID.

CIDR - Bestemmingsadres voor de route die in de routetabel moet worden bijgewerkt.

ENI - De interface-ID van het netwerk van de CSR 1000v Gigabit-interface waarnaar het verkeer wordt geleid.
Als CSRHA bijvoorbeeld mislukt, neemt CSRHA1 de route in de AWS-routetabel over en werkt deze bij om naar zijn eigen ENI te wijzen.

REGIO - De AWS-regio van CSR 1000v.

Beperkingen

- Voor privé-subnetten gebruikt u het IP-adres 10.0.3.0/24 niet. Dit wordt intern gebruikt op de Cisco CSR 1000v voor hoge beschikbaarheid. Cisco CSR 1000v moet een openbare internettoegankelijkheid hebben om REST API-oproepen te maken die de AWS-routetabel wijzigen.

- Plaats de interface van gig1 van de CSR1000v niet in een VRF. HA werkt niet anders.

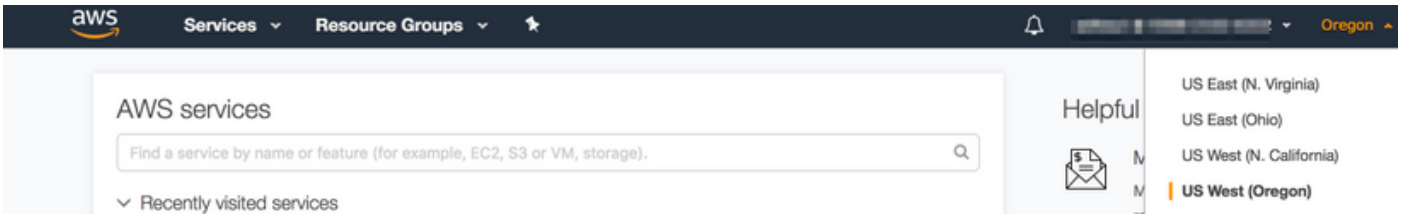
Configuratie

De algemene stroom van configuratie is om bij de hoogste het omringen eigenschap (Regio/VPC) te beginnen en uw manier naar beneden te bewegen aan het meest specifieke (Interface/Subnet). Er is echter geen specifieke volgorde van configuratie. Alvorens u begint, is het belangrijk om de topologie eerst te begrijpen.

> **Tip**: Geef namen aan al uw instellingen (VPC, interface, subnet, routetabellen, enzovoort).

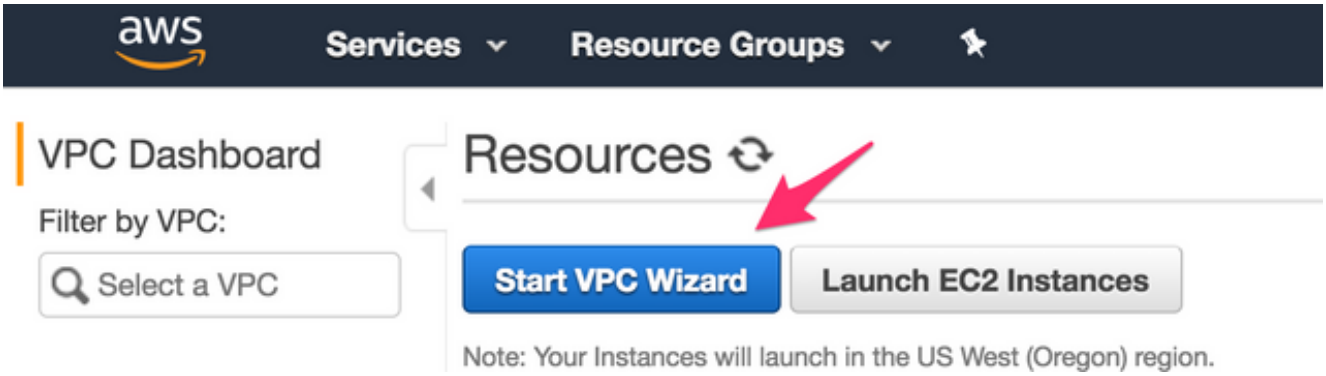
Stap 1. Kies een regio.

In dit voorbeeld wordt het Amerikaanse westen (Oregon) gebruikt.

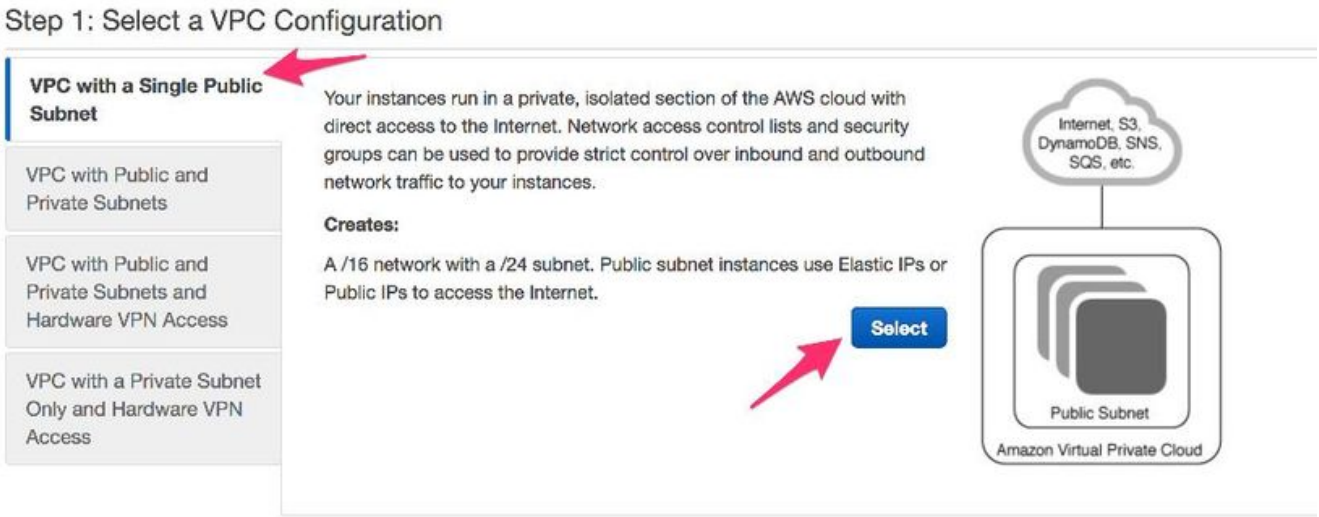


Stap 2. Maak een VPC.

1. Ga in de AWS-console naar **VPC > VPC Dashboard > VPC Wizard starten**.

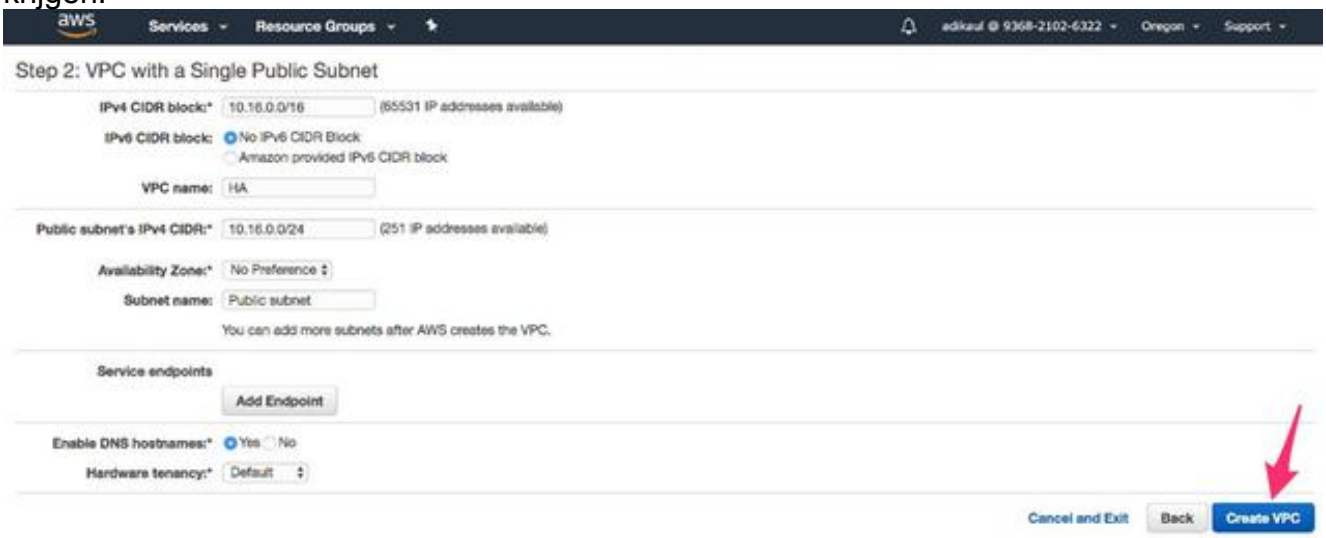


2. Kies VPC met één openbaar subnet.

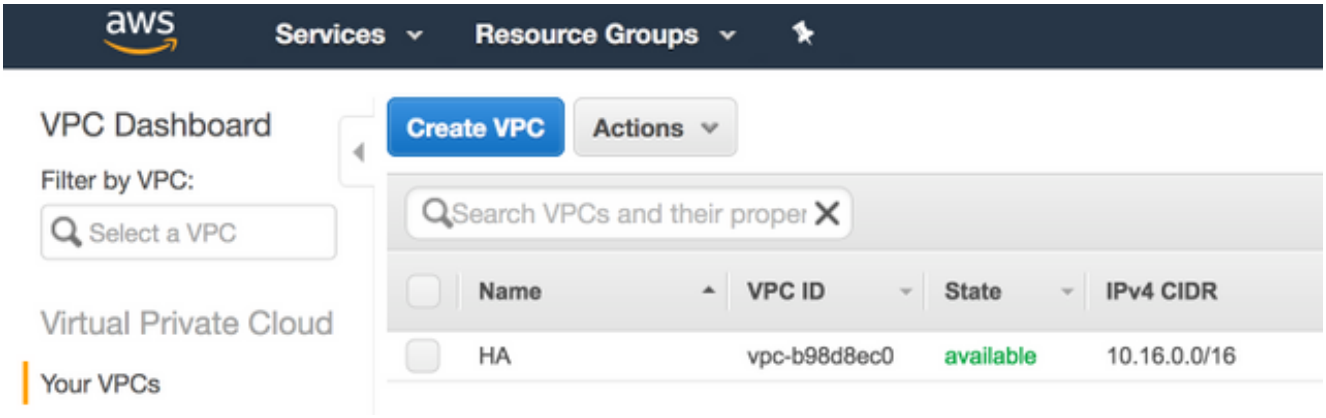


3. Wanneer u een VPC maakt, krijgt u een /16 netwerk toegewezen om te gebruiken zoals u wilt.

4. U wordt ook toegewezen een /24 openbare subnetverbinding. Openbare subnetinstanties gebruiken elastische IP's of openbare IP's voor uw apparaten om toegang tot internet te krijgen.



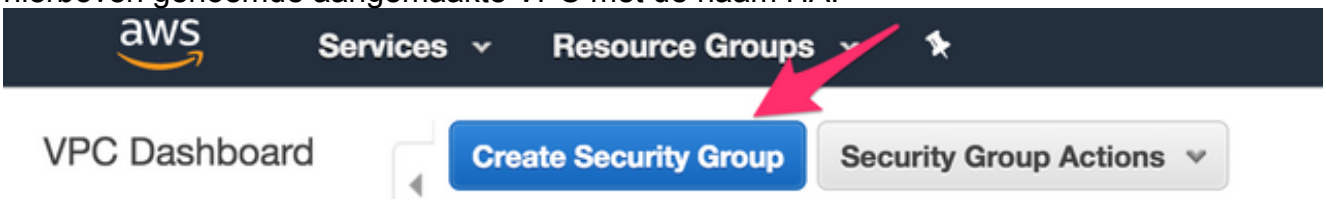
5. vpc-b98d8ec0 wordt gemaakt.



Stap 3. Maak een beveiligingsgroep voor de VPC.

Security Groepen zijn als ACL's om verkeer toe te staan of te weigeren.

1. Klik onder Security op **Security Groups** en **Maak uw Security Group** die is gekoppeld aan de hierboven genoemde aangemaakte VPC met de naam HA.



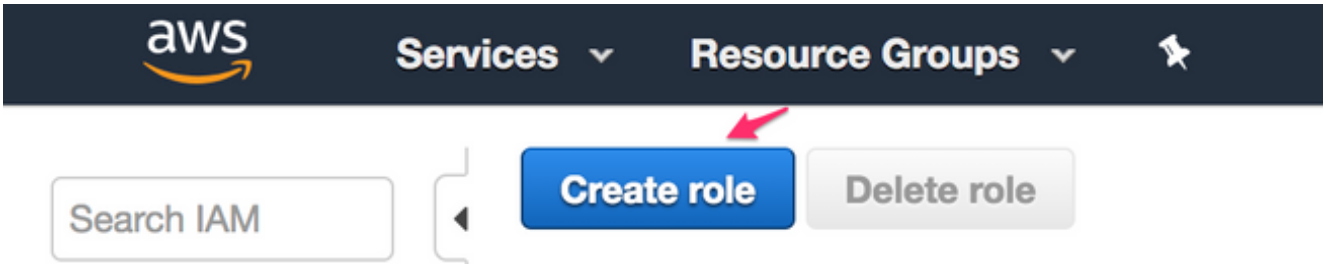
2. Bepaal onder Inkomende regels welk verkeer u wilt toestaan voor sg-1cf47d6d. In dit voorbeeld staat u All Traffic toe.

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

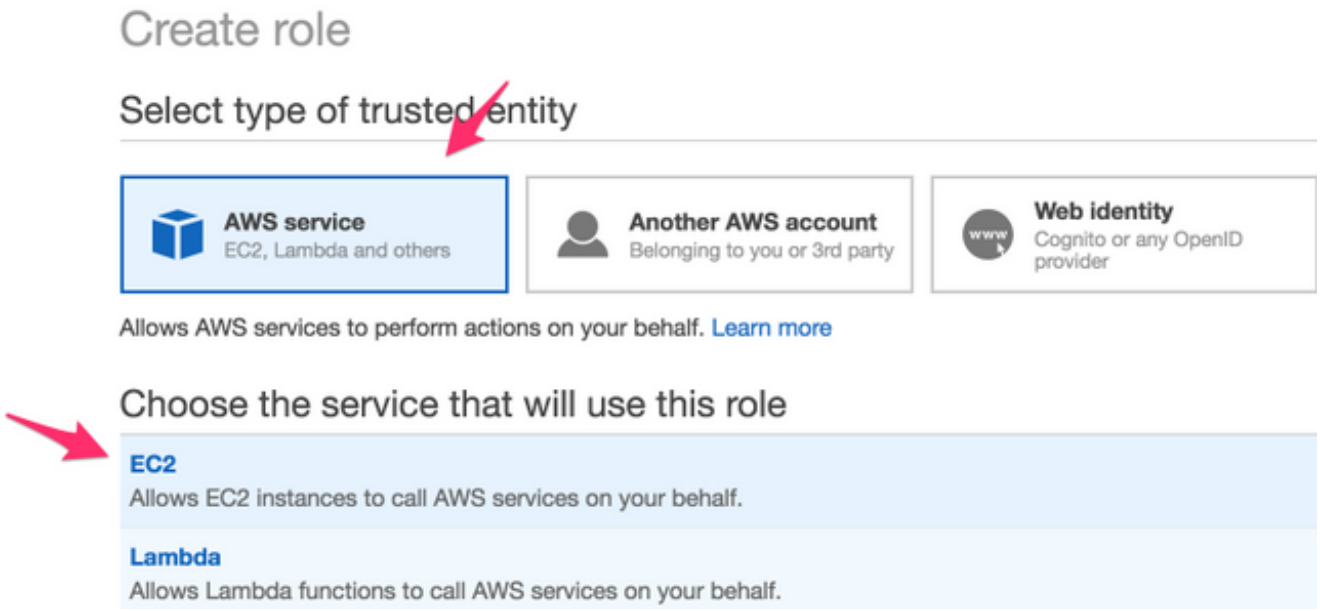
IAM verleent uw MVO toegang tot Amazon API's.

De CSR1000v wordt gebruikt als een proxy om AWS API-opdrachten te bellen om de routetabel te wijzigen. AMI's hebben standaard geen toegang tot API's. Deze procedure creëert een IAM-rol en deze rol wordt gebruikt tijdens de lancering van een CSR-instantie. IAM biedt de toegangsreferenties voor CSR's om AWS API's te gebruiken en aan te passen.

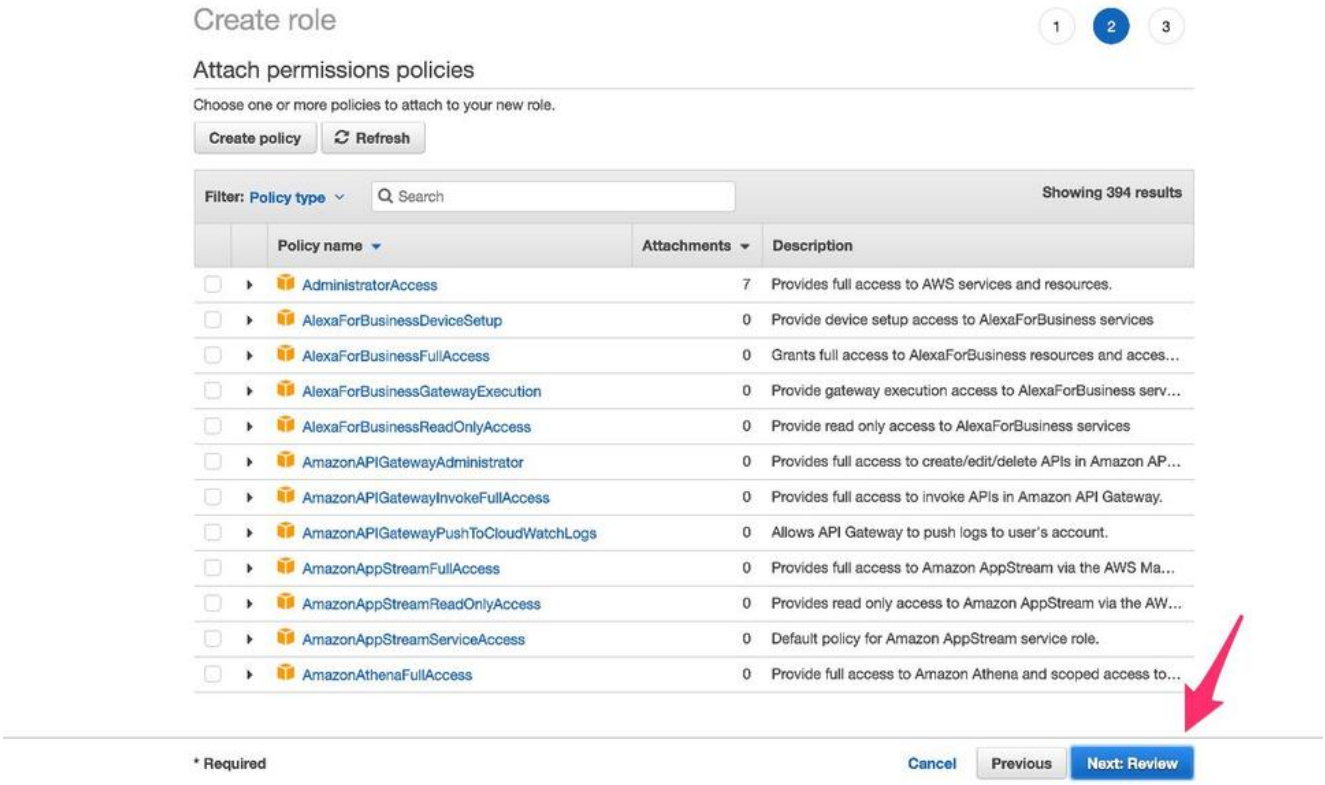
1. Maak een IAM-rol aan. Blader naar het IAM-dashboard en navigeer naar **Rollen > Rol maken**, zoals in de afbeelding.



2. Zoals in de afbeelding wordt getoond, staat u toe dat een EC2-instantie AWS uit uw naam roept.

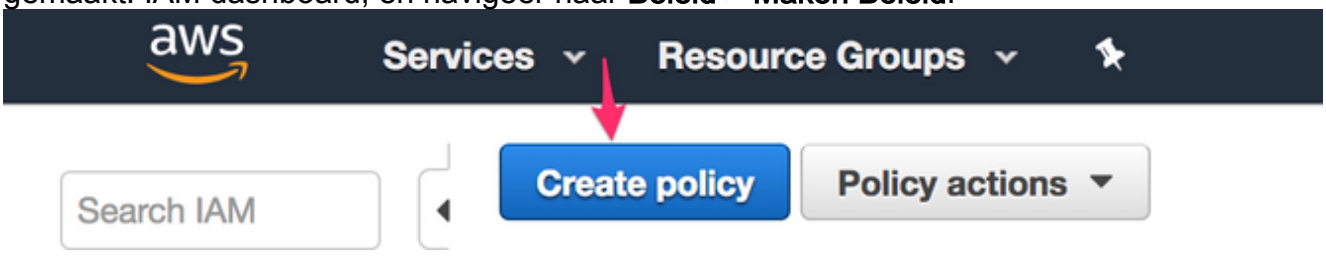


3. Maak een rol en klik op **Volgende: Bekijk** de tekst, zoals in de afbeelding.

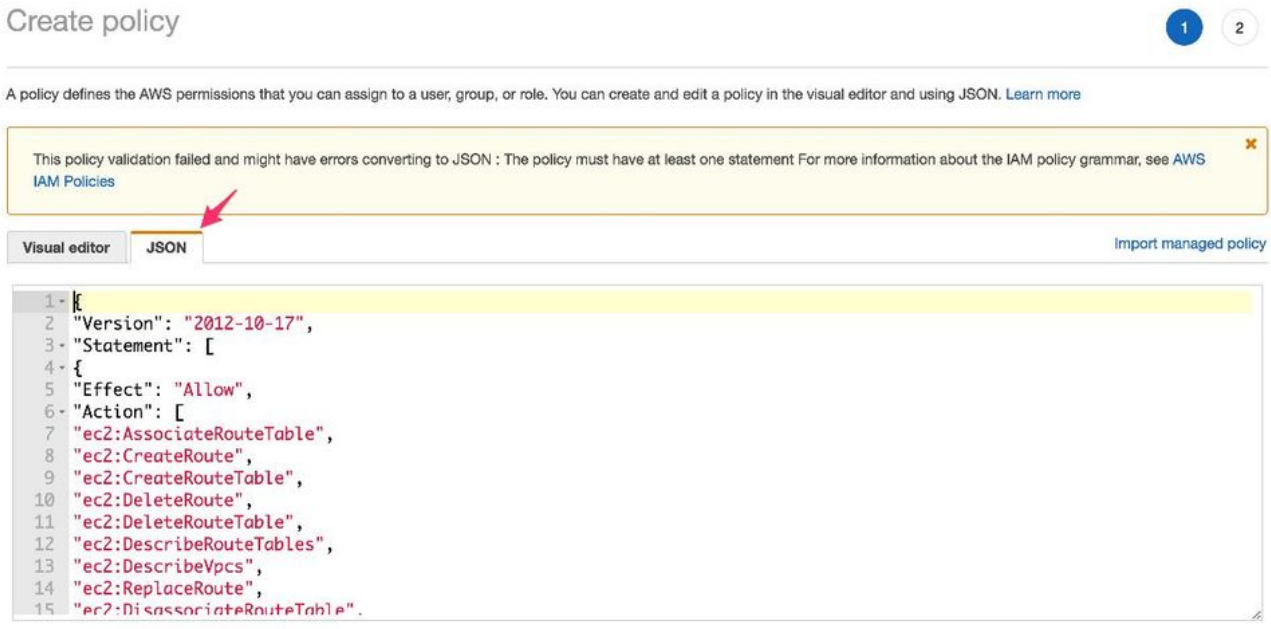


4. Geef het een rolnaam. In dit voorbeeld, zoals in de afbeelding, is de Rol Naam **routebare wijziging**.

5. Vervolgens moet u een beleid maken en dit koppelen aan de rol die u hierboven hebt gemaakt. IAM dashboard, en navigeer naar **Beleid > Maken Beleid**.

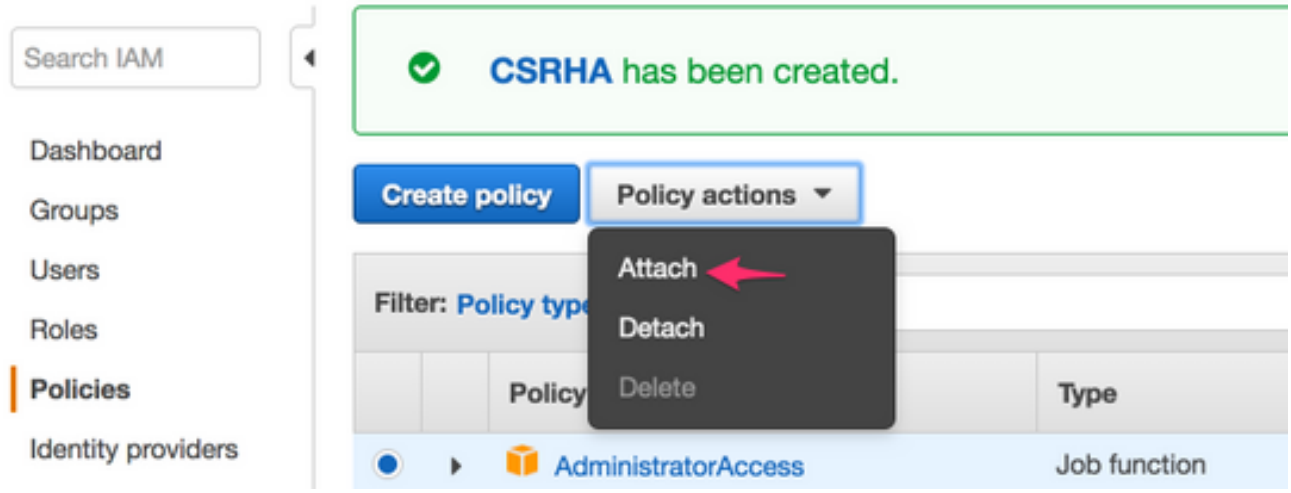



```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:AssociateRouteTable",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:DeleteRoute",
"ec2:DeleteRouteTable",
"ec2:DescribeRouteTables",
"ec2:DescribeVpcs",
"ec2:ReplaceRoute",
"ec2:DisassociateRouteTable",
"ec2:ReplaceRouteTableAssociation"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

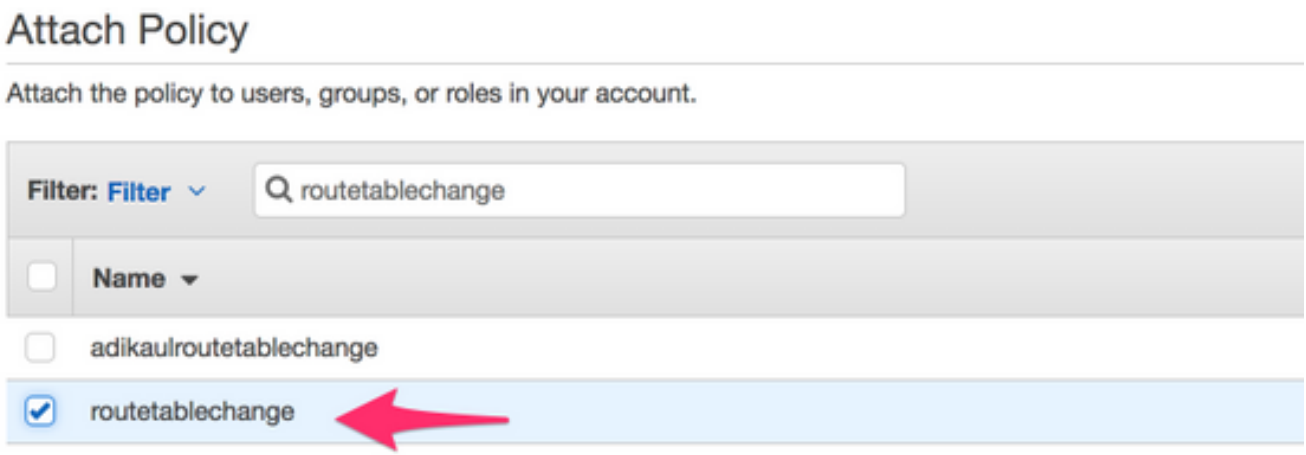


6. Geef het een beleidsnaam en voeg het toe aan de Role die u hebt gemaakt. De beleidsnaam

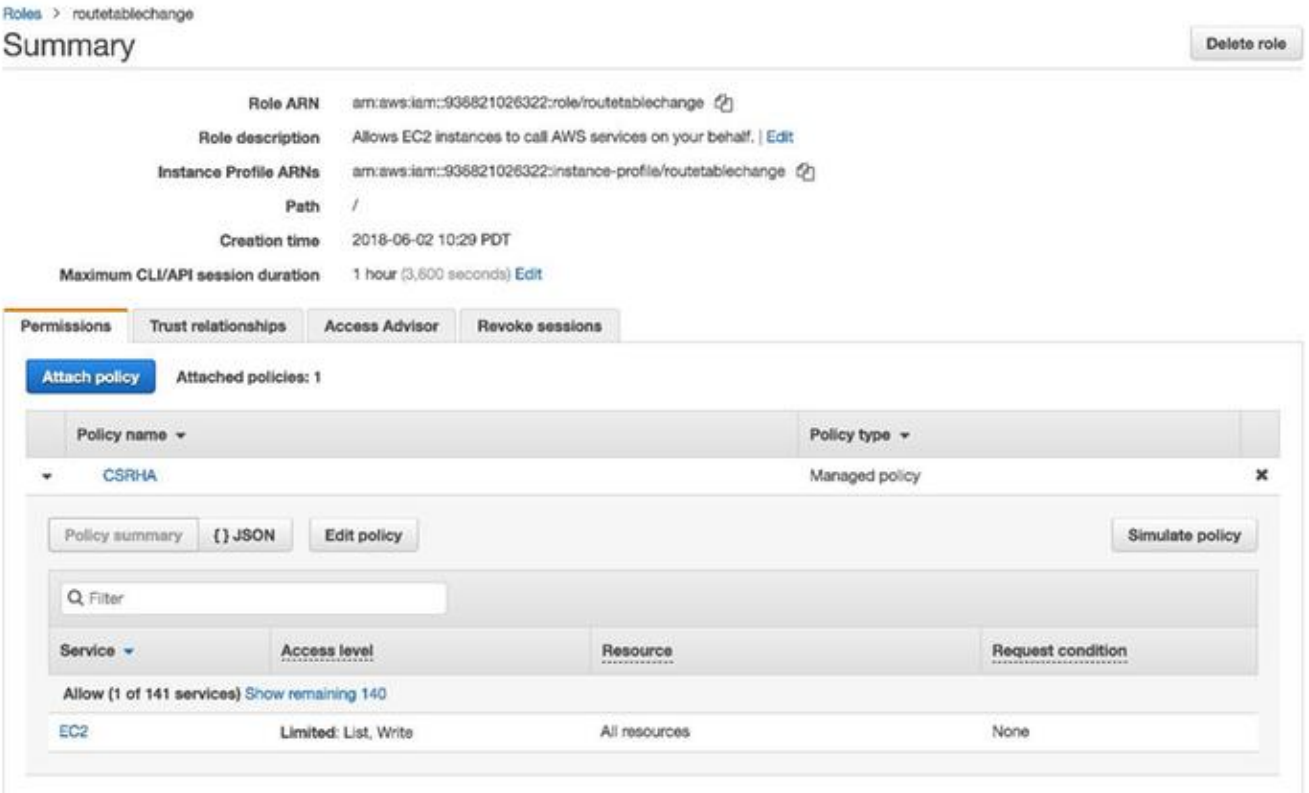
wordt bijvoorbeeld CSRHA met beheerderstoegang genoemd, zoals in het afbeelding wordt getoond.



7. Zoals in de afbeelding wordt getoond, voegt u het beleid toe aan de rol die u hebt gemaakt, de **routeverandering** genoemd.



8. Samenvatting.



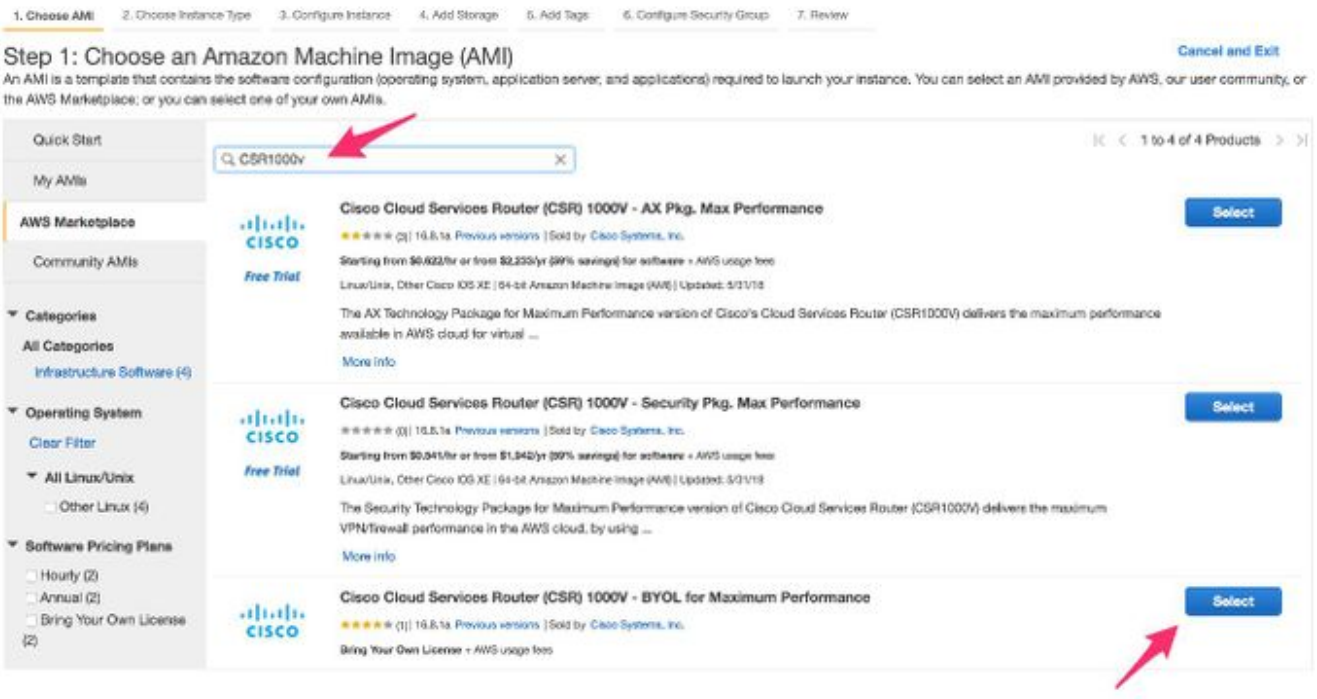
Stap 5. Start de CSR1000v's met de AMI rol die u hebt gemaakt en associeer de publiek/private subnetten.

Elke CSR1000v router heeft 2 interfaces (1 publiek, 1 privaat) en bevindt zich in zijn eigen Availability Zone. U kunt aan elke CSR denken als zijnde in afzonderlijke datacenters.

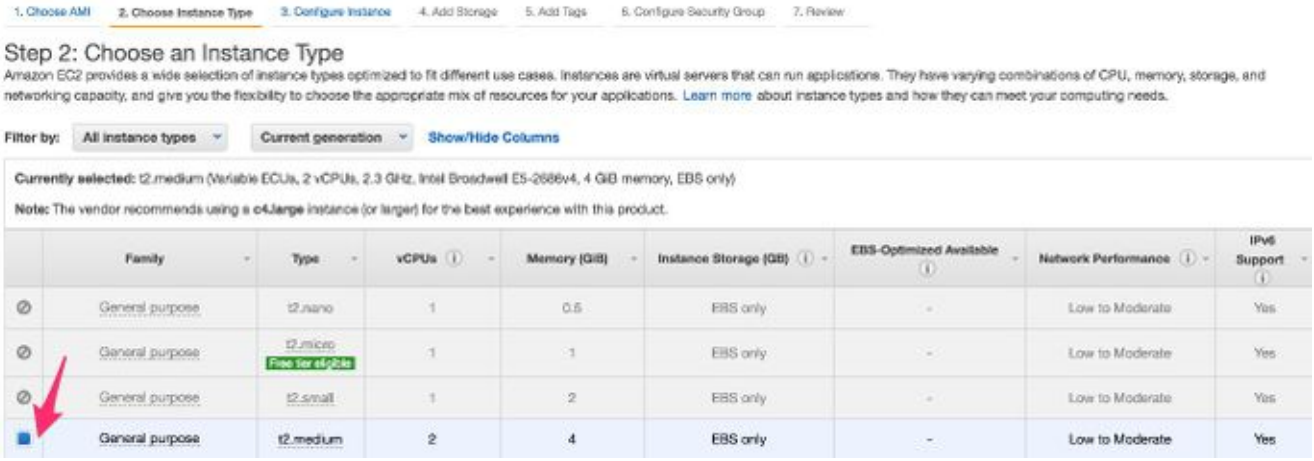
1. Selecteer **EC2** op de AWS-console en klik vervolgens op **Start Instance**.

2. Selecteer AWS Marketplace.

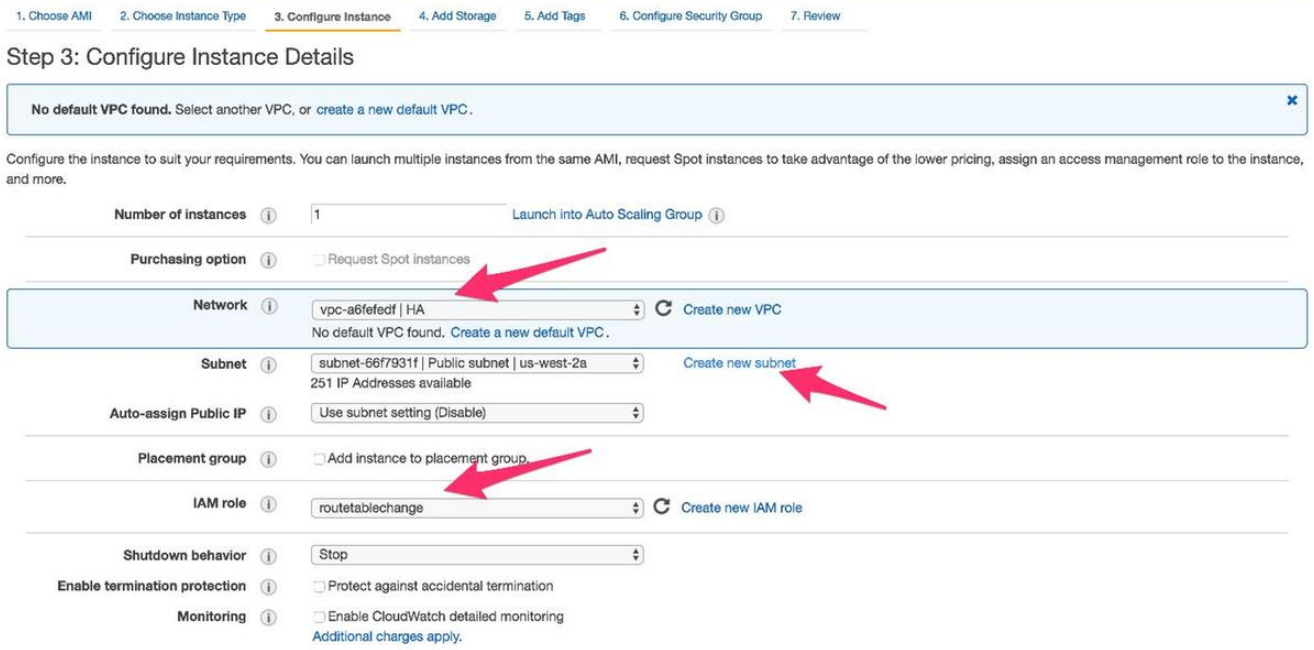
3. Voer CSR1000v in en gebruik bijvoorbeeld Cisco Cloud Services Router (CSR) 1000V - BYOL voor maximale prestaties.



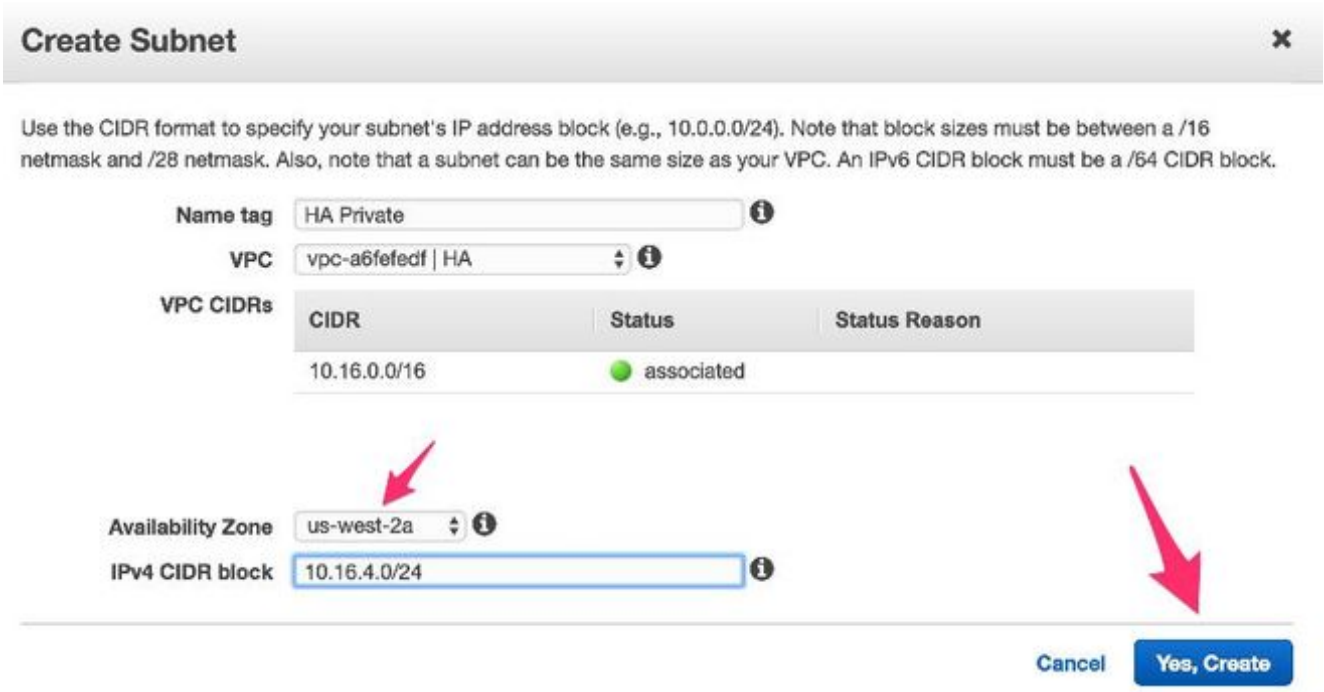
4. Kies een instantietype. Het geselecteerde type is **t2.medium**.



5. Terwijl de instantie is geconfigureerd, moet u de VPC die u hierboven hebt gemaakt selecteren, samen met de IAM-rol hierboven. Bovendien, creeer een Privé Subnet die u aan de privé onder ogen ziende interface associeert.



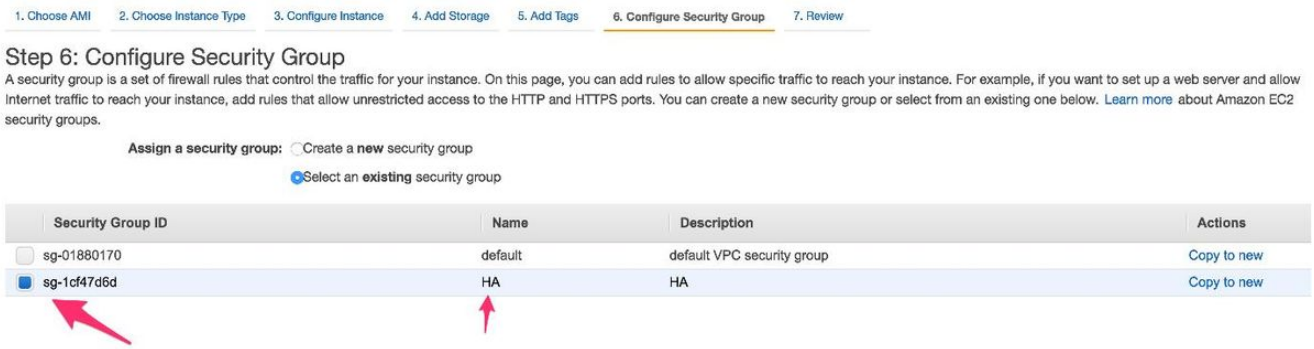
6. Klik op Nieuwe Subnet maken voor Private Subnet. In dit voorbeeld is de naam tag HA Private. Zorg ervoor dat het zich in dezelfde beschikbaarheidszone bevindt als het openbare subnet.



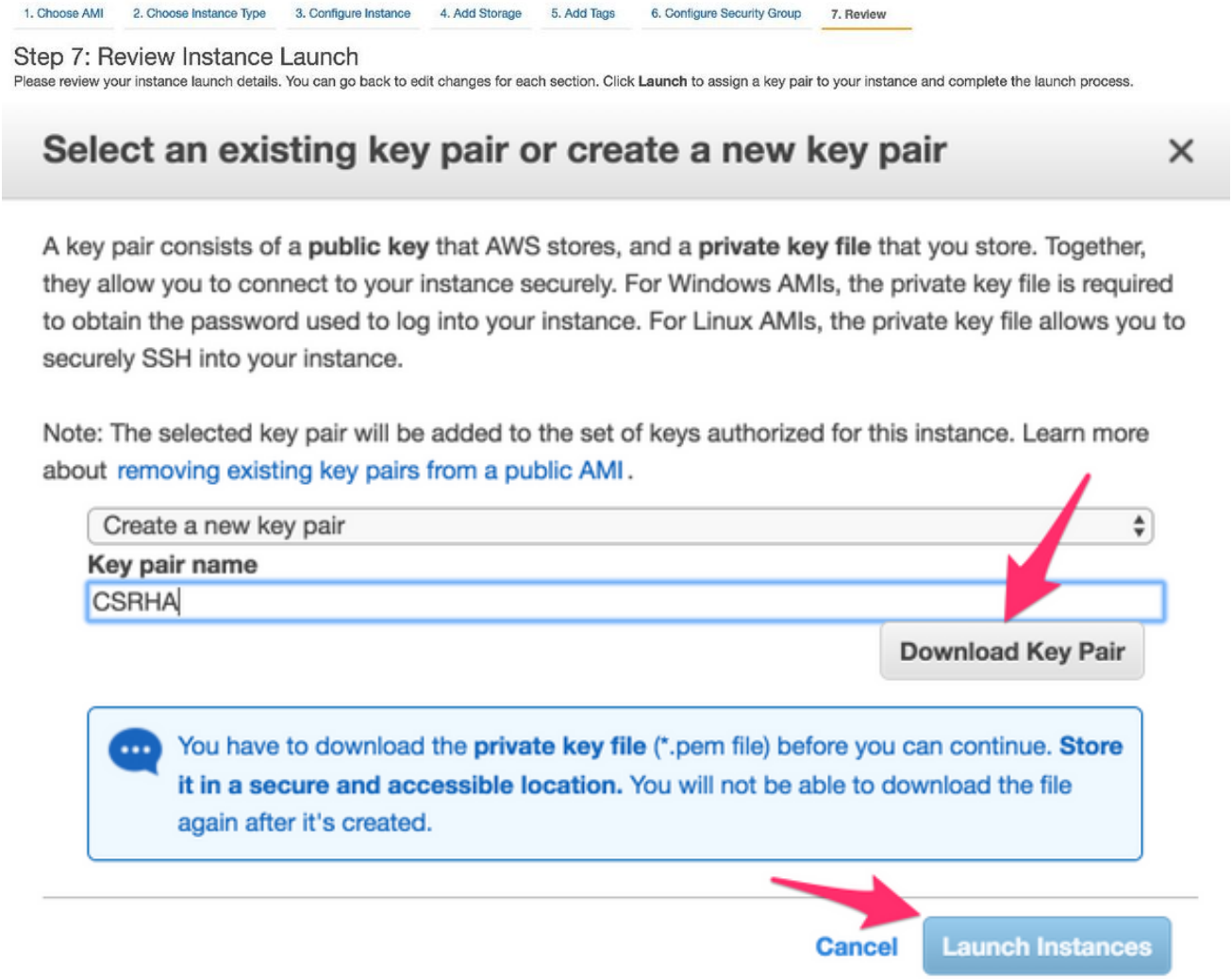
7. Blader naar beneden en klik onder Instantiedetails configureren op **Apparaat toevoegen**, zoals in de afbeelding wordt weergegeven.

8. Nadat de secundaire interface is toegevoegd, associeer het privé-subnetje dat u hebt gemaakt, genaamd HA Private. Eth0 is de openbare interface en Eth1 is de privé-interface. **Opmerking:** Subnet dat in de vorige stap is gemaakt, wordt mogelijk niet in deze vervolgkeuzelijst weergegeven. Het kan noodzakelijk zijn de pagina te verversen of te annuleren en opnieuw te starten om het subnetnummer te laten verschijnen.

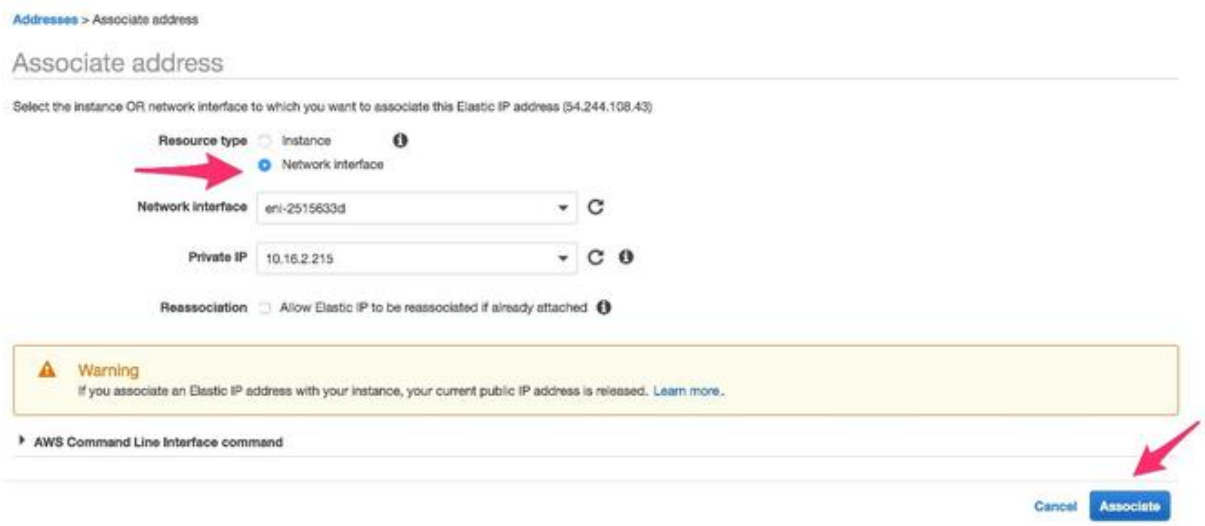
9. Selecteer de beveiligingsgroep die u onder VPC hebt gemaakt en zorg ervoor dat de regels goed worden gedefinieerd.



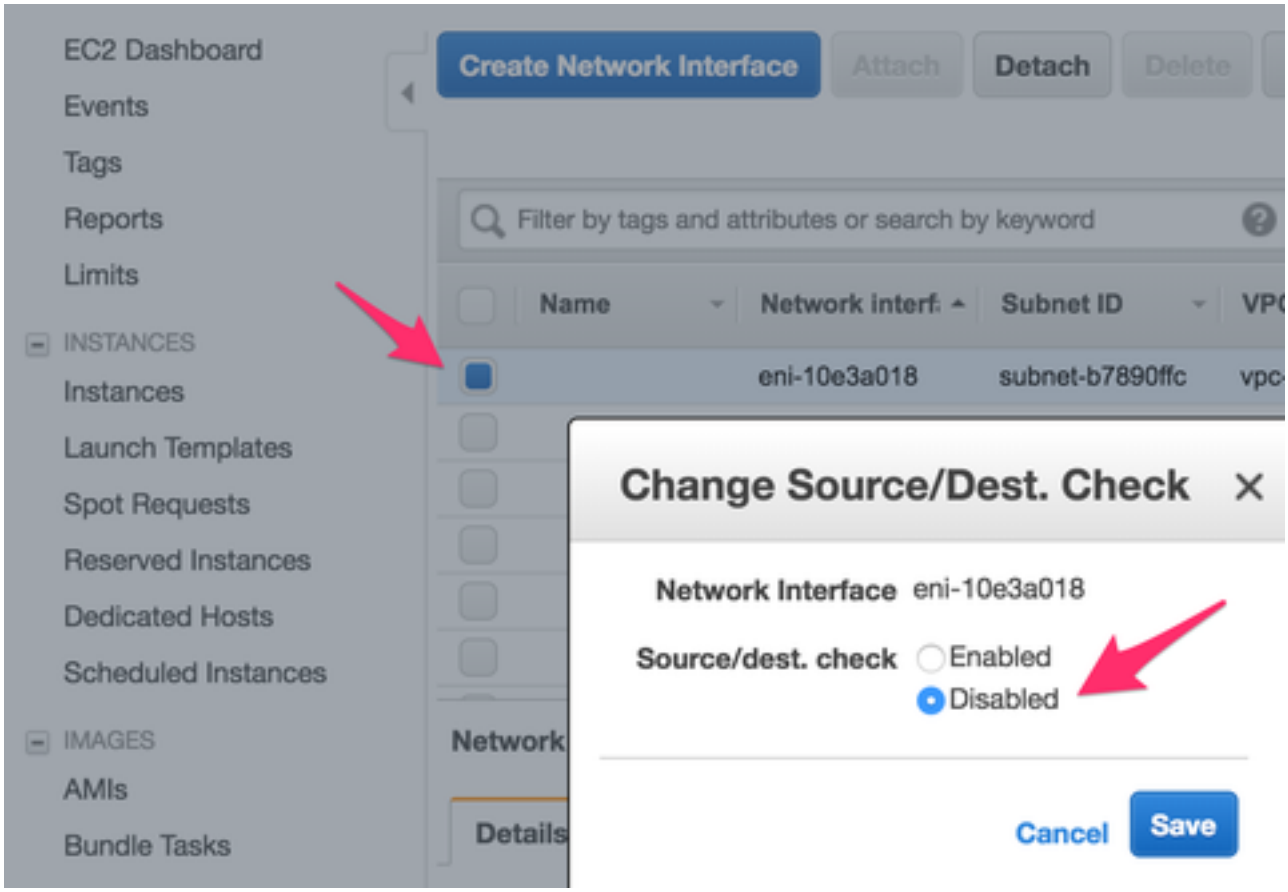
10. Maak een nieuw sleutelpaar en zorg ervoor dat u uw privésleutel downloadt. U kunt één sleutel voor elk apparaat opnieuw gebruiken. **Opmerking:** Als u uw persoonlijke sleutel verliest, kunt u niet opnieuw inloggen bij uw MVO. Er is geen methode om sleutels terug te krijgen.



11. Koppel de elastische IP aan het ENI van Public Interface voor het door u gemaakte exemplaar en navigeer naar de **AWS-console > EC2 Management > Network Security > Elastic IP's**. **Opmerking:** Publieke/private terminologie kan u hier in de war brengen. In dit voorbeeld is de definitie van een openbare interface Eth0, de interface met het internet. Vanuit het oogpunt van AWS, is onze openbare interface hun privé ip.

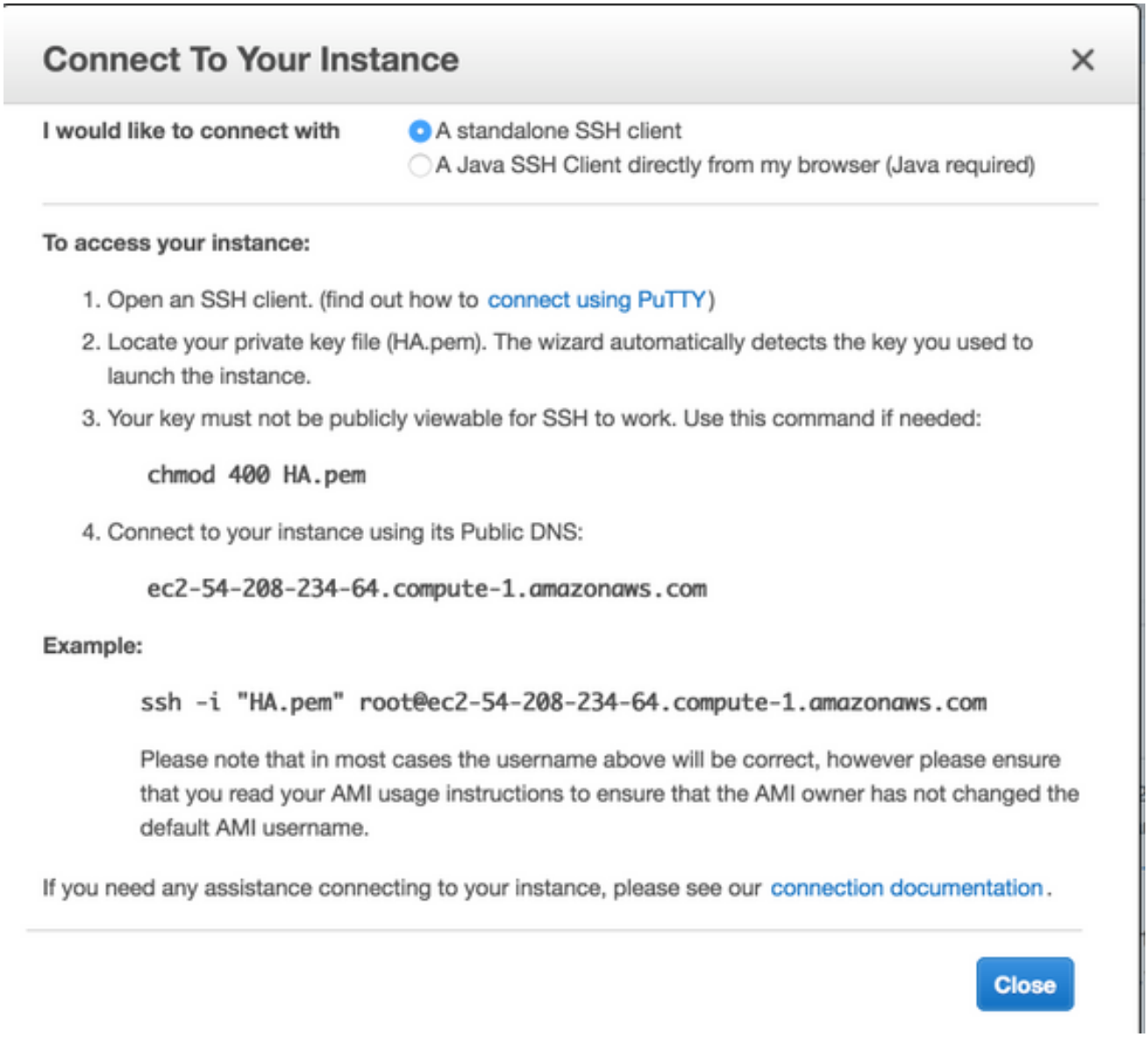


12. Schakel de controle Bron/Diest uit als u naar **EC2 > Network Interfaces** navigeert. Controleer elke ENI voor Source/Dest-controle. Standaard worden alle ENI's geleverd met deze optie Source/Dest. Een anti-spoofing functie bedoeld om te voorkomen dat een ENI overbelast raakt met verkeer dat niet echt bedoeld is voor het door te verifiëren dat de ENI de bestemming van het verkeer is voordat het door te sturen. De router is zelden de daadwerkelijke bestemming van een pakket. Deze optie moet worden uitgeschakeld in alle CSR-transitcentra of kan geen pakketten doorsturen.



13. Maak verbinding met uw CSR1000v. **Opmerking:** De gebruikersnaam die door AWS aan SSH in de CSR1000v is opgegeven, wordt mogelijk onjuist als root vermeld. Wijzig dit indien nodig in ec2-user.**Opmerking:** U moet het DNS-adres naar SSH kunnen pingen. Hier is het ec2-54-208-234-64.compute-1.amazonaws.com. Controleer of het openbare subnetnummer/de openbare netwerkmodule van de router is gekoppeld aan de openbare routertabel. Ga in het kort naar Stap 8 voor het koppelen van het subnetverbinding aan de

routetabel.



Stap 6. Herhaal stap 5 en maak de tweede CSR1000v-instantie voor HA.

Openbare subnetten: 10.16.1.0/24

Private subnet: 10.16.5.0/24

Als u het elastische IP-adres van dit nieuwe AMI niet kunt pingen, gaat u kort naar Stap 8 en zorgt u ervoor dat het openbare subnetnummer aan de openbare routetabel is gekoppeld.

Stap 7. Herhaal stap 5 en maak een VM (Linux/Windows) vanuit de AMI Marketplace.

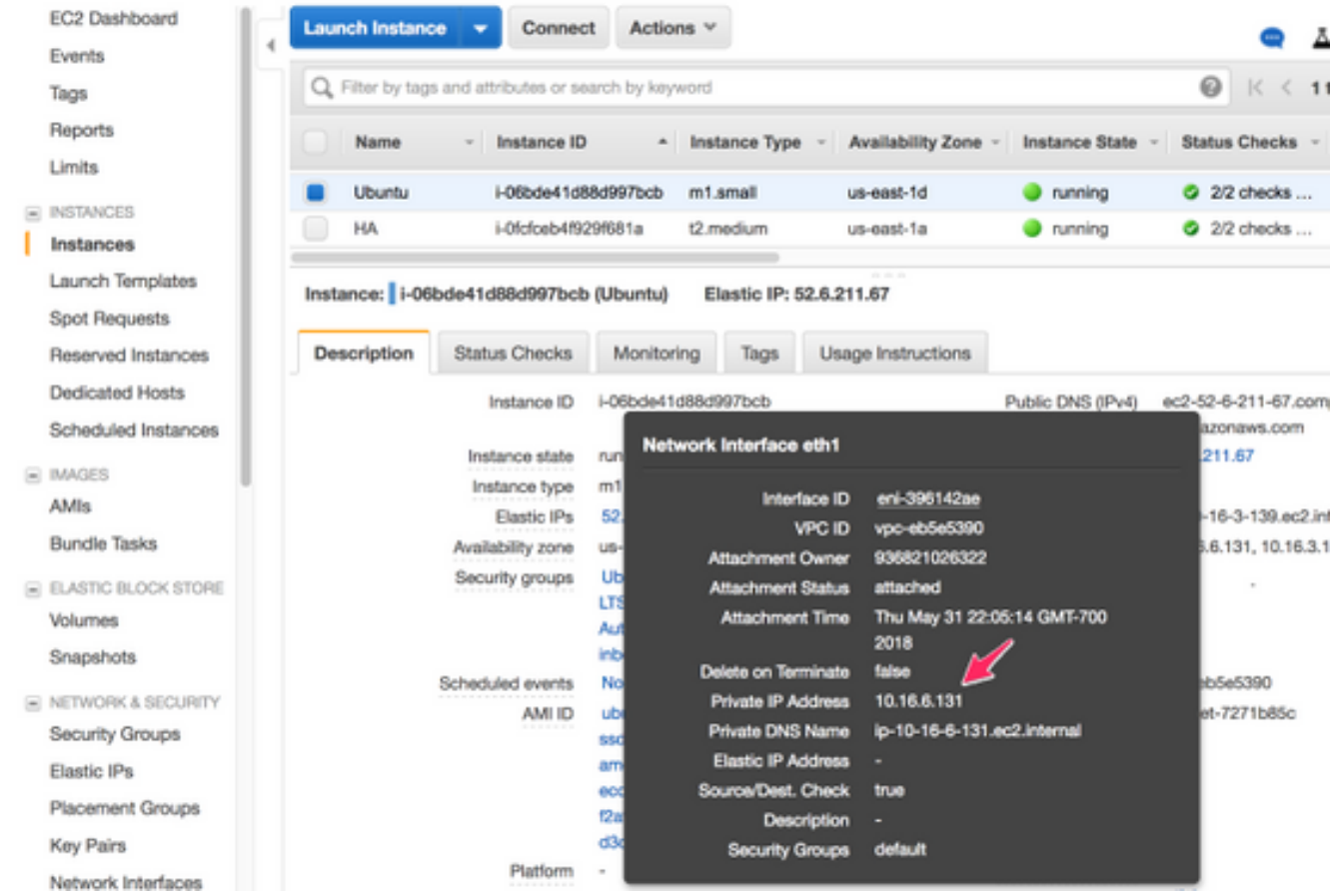
Gebruik bijvoorbeeld Ubuntu Server 14.04 LTS op de marktplaats.

Openbare subnetten: 10.16.2.0/24

Private subnet: 10.16.6.0/24

Als u het elastische IP-adres van dit nieuwe AMI niet kunt pingen, gaat u kort naar Stap 8 en zorgt u ervoor dat het openbare subnetnummer aan de openbare routetabel is gekoppeld.

1. Eth0 wordt standaard aangemaakt voor de openbare interface. Maak een tweede interface met de naam eth1 voor het privé-subsysteem.



2. Het IP-adres dat u in Ubuntu configureert, is de private interface eth1 die door AWS wordt toegewezen.

```
ubuntu@ip-10-16-2-139:~$ cd /etc/network/interfaces.d/

ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo vi eth1.cfg

auto eth1
iface eth1 inet static
  address 10.16.6.131
  netmask 255.255.255.0
  network 10.16.6.0
  up route add -host 8.8.8.8 gw 10.16.6.1 dev eth1
```

3. Schakel de interface af of start de VM opnieuw op.

```
ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo ifdown eth1 && sudo ifup eth1
ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo reboot
```

4. Ping 8.8.8.8 voor de test. Zorg ervoor dat de 8.8.8.8-route is toegevoegd per stap 7.

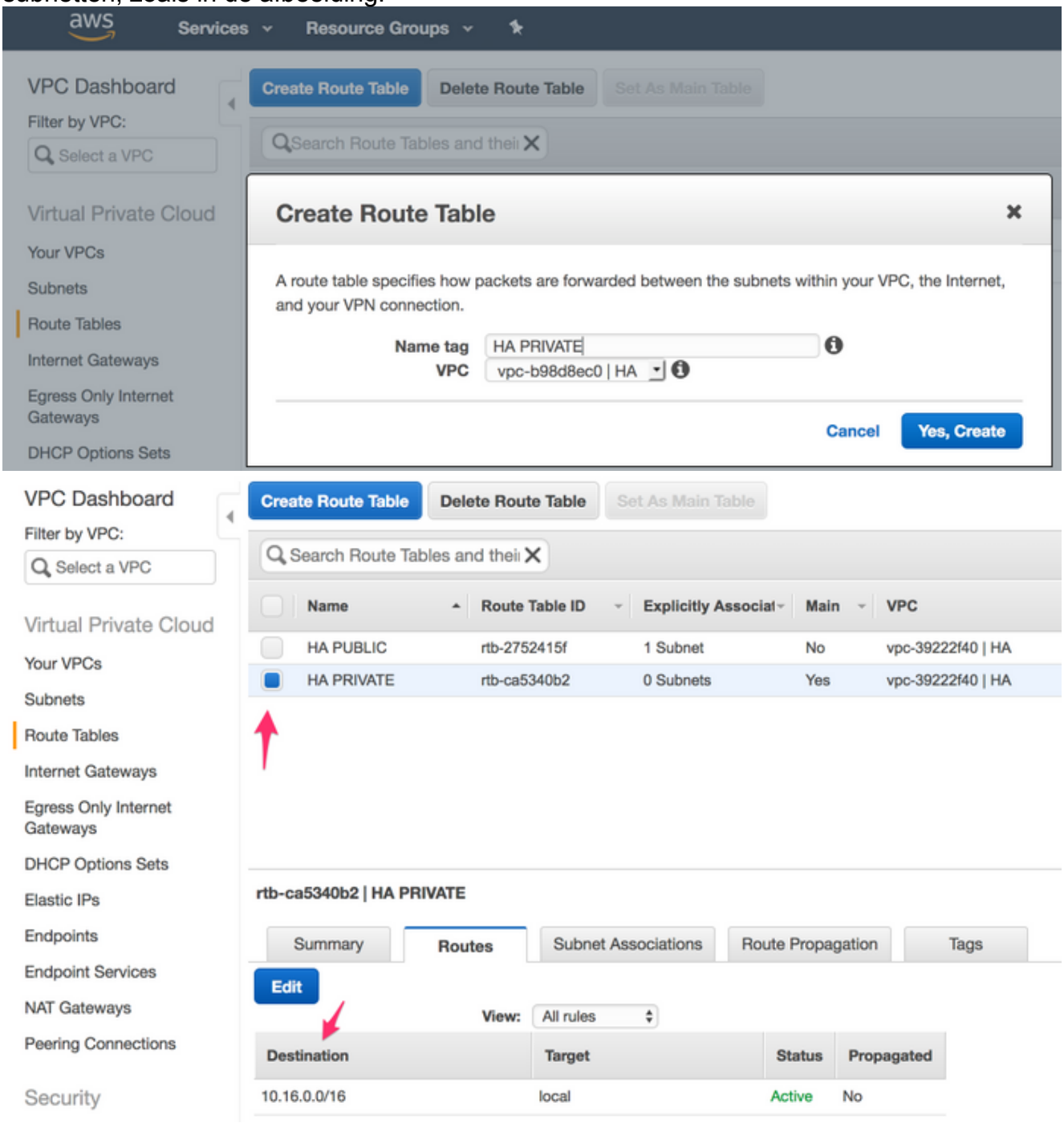
```
ubuntu@ip-10-16-2-139:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.16.2.1 0.0.0.0 UG 0 0 0 eth0
8.8.8.8 10.16.6.1 255.255.255.255 UGH 0 0 0 eth1     <--------------
10.16.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.16.6.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
```

Indien 8.8.8.8 niet in de tabel is vermeld, kunt u het volgende handmatig toevoegen:

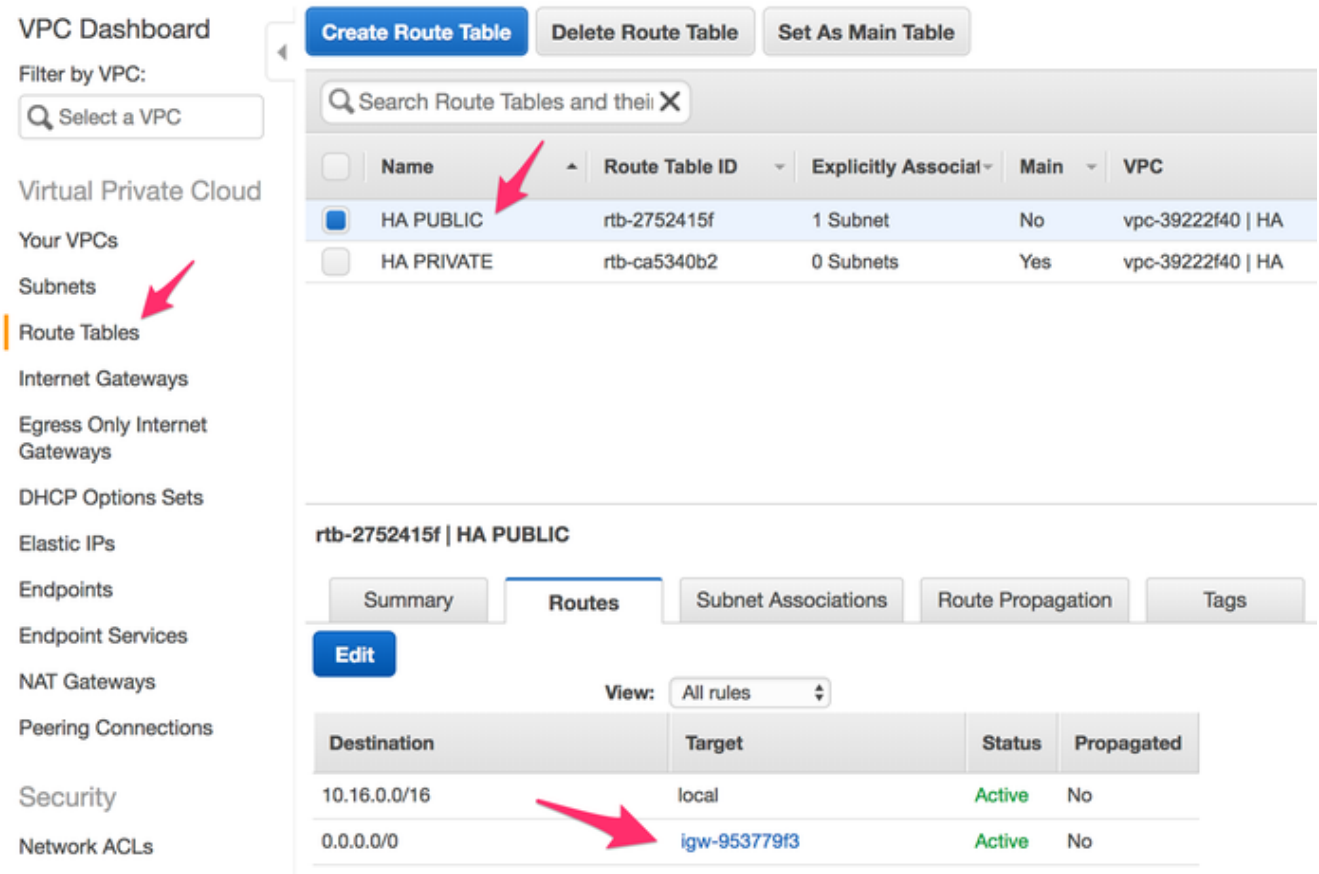
```
ubuntu@ip-10-16-2-139:~$ sudo route add -host 8.8.8.8 gw 10.16.6.1 dev eth1
```

Stap 8. Configuratie van de privé- en de openbare routetabellen.

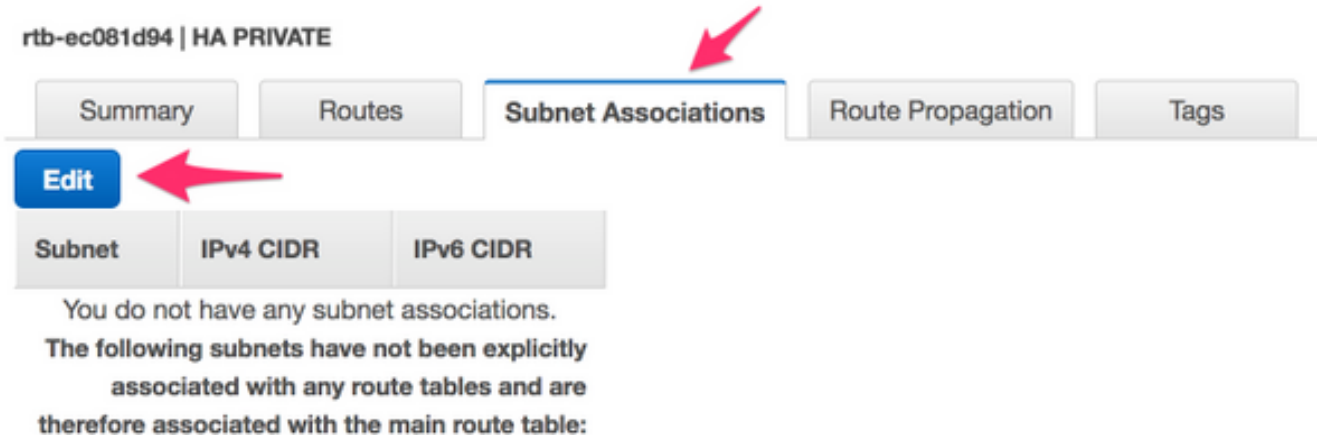
1. Wanneer een VPC door de wizard in Stap 2 wordt gemaakt, worden automatisch twee routelijsten gemaakt. Als er slechts één Route-tabel is, maakt u een andere voor uw privé-subnetten, zoals in de afbeelding.



2. Hier is een overzicht van de twee Routetabellen. De Public Route Table heeft de Internet Gateway (igw-95377973) automatisch aangesloten. Noteer deze twee tabellen dienovereenkomstig. De PRIVATE tabel mag deze route NIET hebben.



3. Associeer alle 6 subnetten aan de juiste routetabel 3 Publieke interfaces worden geassocieerd met de Public Route Table:Openbare subnetten: 10.16.0.0/24, 10.16.1.0/24, 10.16.2.0/24 3 Private interfaces zijn gekoppeld aan de Private Route-tabel:Particuliere subnetten: 10.16.4.0/24, 10.16.5.0/24, 10.16.6.0/24



Stap 9. Configureer Network Address Transaltion (NAT) en GRE Tunnel met BFD en elk Routing Protocol.

Configureer de GRE-tunnel (Generic Routing Encapsulation) door de elastische IP's van de CSR 1000v's (aanbevolen om problemen met DHCP-leasevernieuwing te voorkomen, die foutieve fouten detecteren). De BFD-waarden (Biderection Forwarding Detection) kunnen zo worden geconfigureerd dat ze agressiever zijn dan in dit voorbeeld, als er snellere convergentie nodig is. Dit kan echter leiden tot BFD peer down events tijdens intermitterende connectiviteit. De waarden in dit voorbeeld detecteren peer-falen binnen 1,5 seconden. Er is een variabele vertraging van ongeveer een paar seconden tussen het moment waarop de opdracht AWS API wordt uitgevoerd en het moment waarop de wijzigingen in de VPC-routeringstabel van kracht worden.

- Configuratie op CSRHA

  GRE en BFD - Gebruikt om voorwaarden voor HA failover na te leven

```
interface Tunnel1
  ip address 192.168.1.1 255.255.255.0
  bfd interval 500 min_rx 500 multiplier 3
  tunnel source GigabitEthernet1
  tunnel destination 52.10.183.185 /* Elastic IP of the peer CSR */
!
router eigrp 1
  bfd interface Tunnel1
  network 192.168.1.0
  passive-interface GigabitEthernet1
```

NAT en routing - gebruikt voor bereikbaarheid van VM-internet via de privé-interface

```
interface GigabitEthernet1
  ip address dhcp
  ip nat outside
  no shutdown
!
interface GigabitEthernet2
  ip address dhcp
  ip nat inside
  no shutdown
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!
access-list 10 permit 10.16.6.0 0.0.0.255
!
ip route 10.16.6.0 255.255.255.0 GigabitEthernet2 10.16.4.1
```

- Configuratie op CSRHA1

  GRE en BFD - Gebruikt om voorwaarden voor HA failover na te leven

```
interface Tunnel1
  ip address 192.168.1.2 255.255.255.0
  bfd interval 500 min_rx 500 multiplier 3
  tunnel source GigabitEthernet1
  tunnel destination 50.112.227.77 /* Elastic IP of the peer CSR */
!
router eigrp 1
  bfd interface Tunnel1
  network 192.168.1.0
  passive-interface GigabitEthernet1
```

NAT en routing - gebruikt voor bereikbaarheid van VM-internet via de privé-interface

```
interface GigabitEthernet1
  ip address dhcp
  ip nat outside
  no shutdown
!
interface GigabitEthernet2
  ip address dhcp
  ip nat inside
```

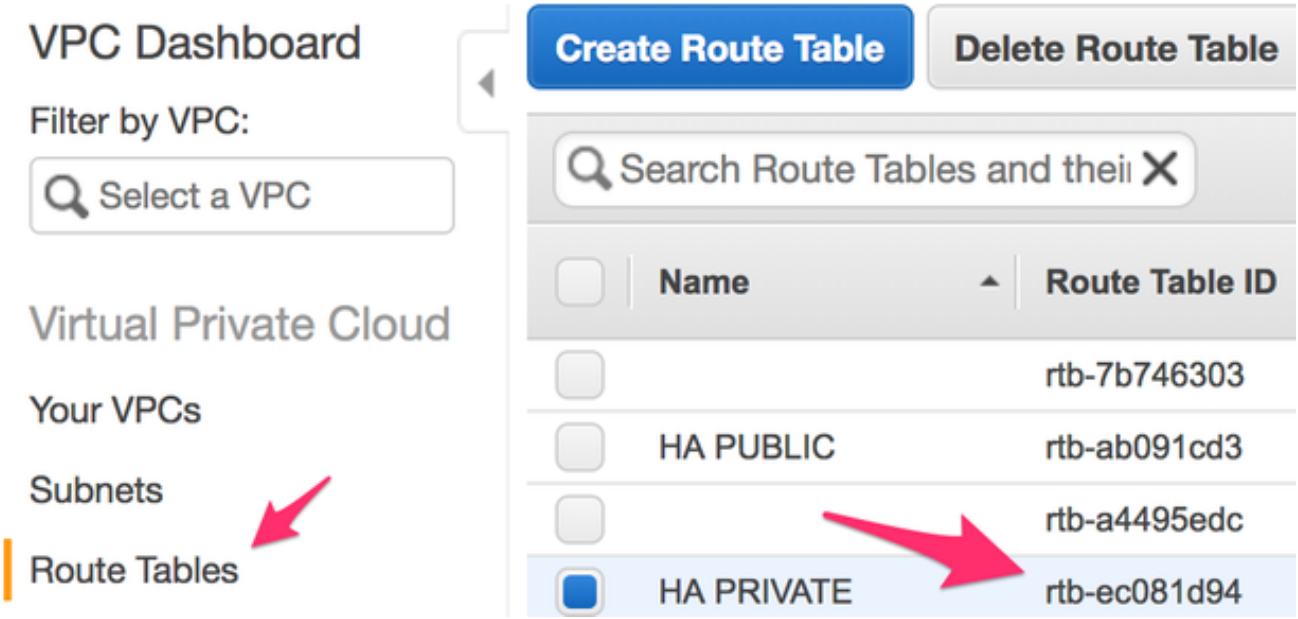
```
  no shutdown
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!
access-list 10 permit 10.16.6.0 0.0.0.255
!
ip route 10.16.6.0 255.255.255.0 GigabitEthernet2 10.16.5.1
```

Stap 10. Configureer hoge beschikbaarheid (Cisco IOS XE Dense 16.3.1a of hoger).

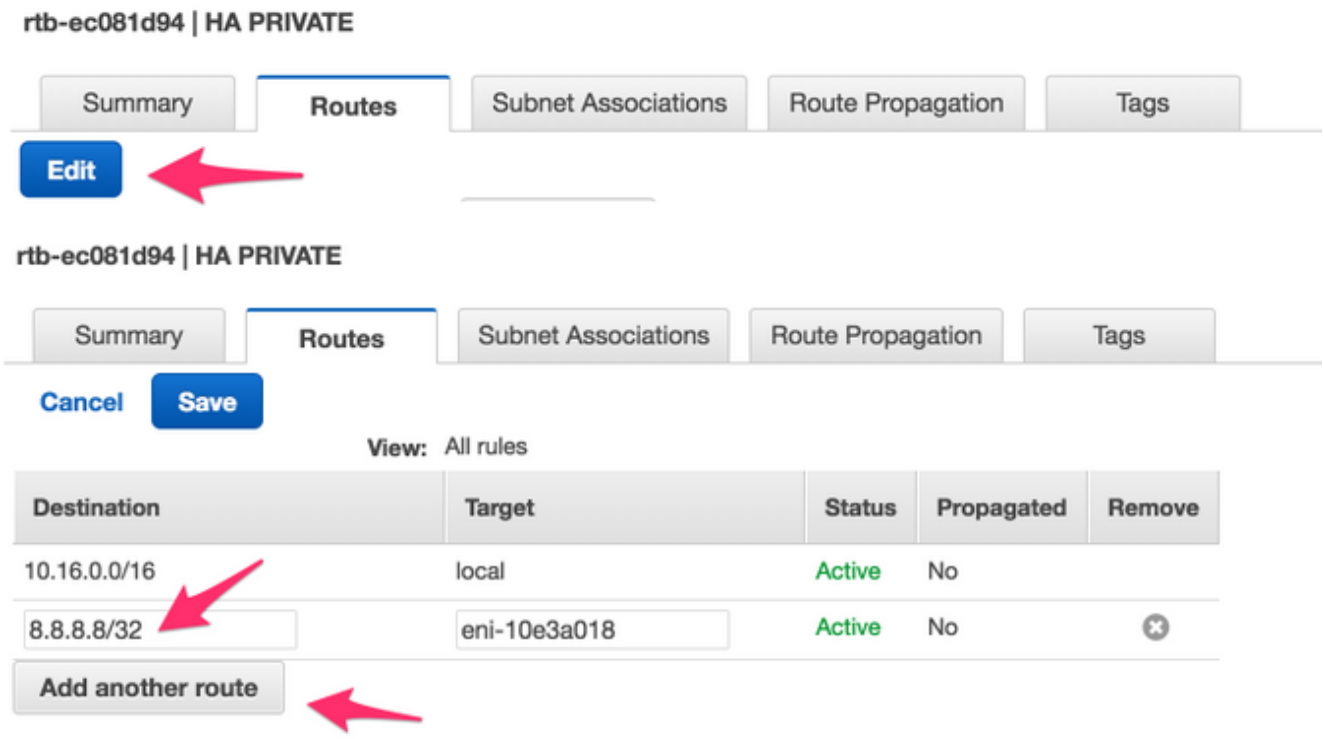
Controleer BFD peer-down gebeurtenissen door elke CSR 1000v te configureren met behulp van de cloud provider was de opdracht hieronder gespecificeerd. Gebruik deze opdracht om de routewijzigingen in (VPC) Route-table-id, Network-interface-id en CIDR te definiëren nadat een AWS HA-fout zoals BFD peer down is gedetecteerd.

```
CSR(config)# redundancy
CSR(config-red)# cloud provider [aws | azure] node-id
# bfd peer ipaddr
# route-table table-name
# cidr ip ipaddr/prefix
# eni elastic-network-intf-name
# region region-name
```

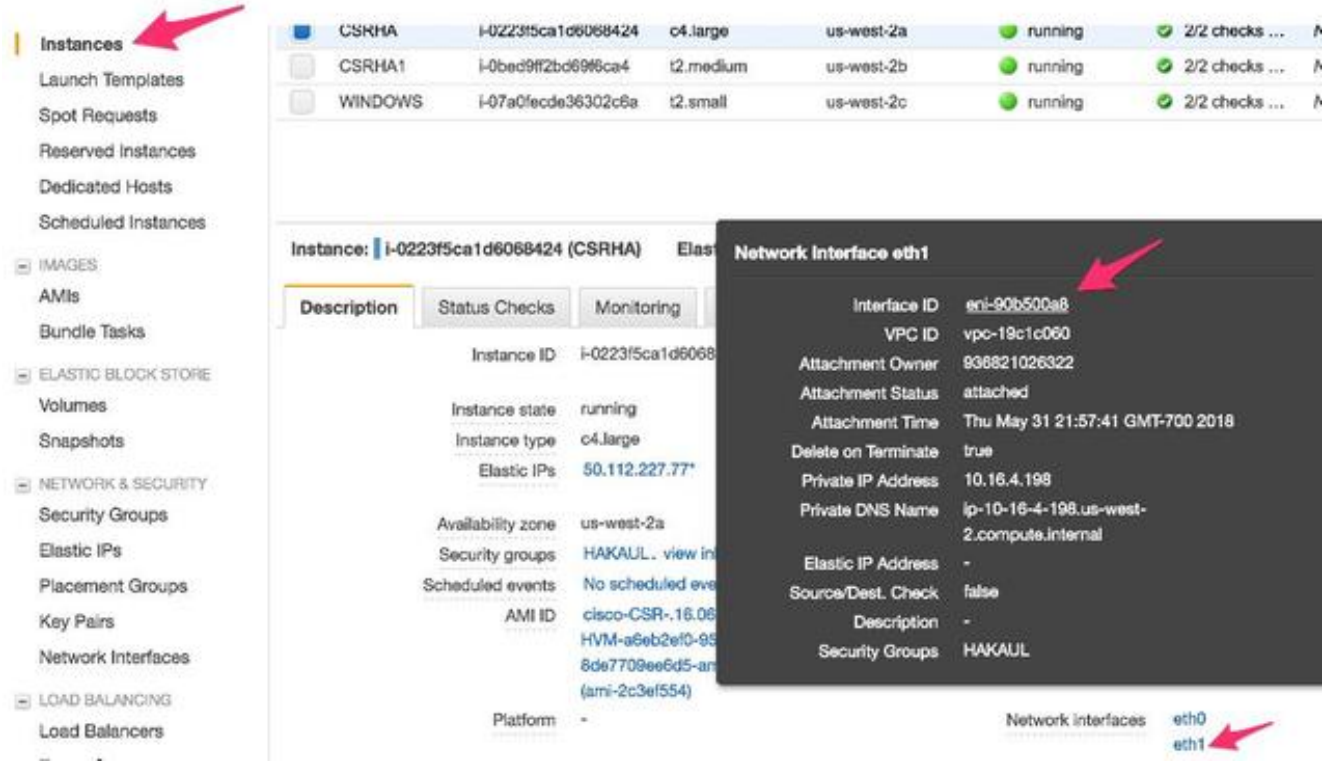
1. De #bfd peer ipaddr is het IP-adres van de peer-tunnel.
   ```
   CSRHA#show bfd neighbors

   IPv4 Sessions
   NeighAddr LD/RD RH/RS State Int
   192.168.1.2 4097/4097 Up Up Tu1
   ```
2. De #route-table tabelnaam vindt u onder AWS-console, navigeren naar **VPC > Routetabellen**. Deze actie wijzigt de Private Route-tabel.



3. Het #cidr ip-ipaddr/prefix is het doeladres voor de route die in de routetabel moet worden bijgewerkt. Navigeer onder AWS-console naar **VPC > Route Tables**. Scroll naar beneden, klik op **Bewerken** en vervolgens op **Een andere route toevoegen**. Voeg ons adres van de testbestemming van 8.8.8.8 en CSRHA's private ENI toe.



4. De #eni elastische-netwerk-intf-naam is te vinden in uw EC2-instantie. Klik op uw Private interface eth1 voor elk van de corresponderende CSR's en gebruik de interface-ID.



5. De #region is de codenaam in het AWS-document. Deze lijst kan worden gewijzigd of uitgebreid. Ga voor de nieuwste updates naar het document Regio's en beschikbaarheidszones van Amazon.

Code	Name
us-east-1	US East (N. Virginia)
us-east-2	US East (Ohio)
us-west-1	US West (N. California)
us-west-2	US West (Oregon)
ca-central-1	Canada (Central)
eu-central-1	EU (Frankfurt)
eu-west-1	EU (Ireland)
eu-west-2	EU (London)
eu-west-3	EU (Paris)
ap-northeast-1	Asia Pacific (Tokyo)
ap-northeast-2	Asia Pacific (Seoul)
ap-northeast-3	Asia Pacific (Osaka-Local)
ap-southeast-1	Asia Pacific (Singapore)
ap-southeast-2	Asia Pacific (Sydney)
ap-south-1	Asia Pacific (Mumbai)
sa-east-1	South America (São Paulo)

Configuratievoorbeeld redundantie op CSRHA

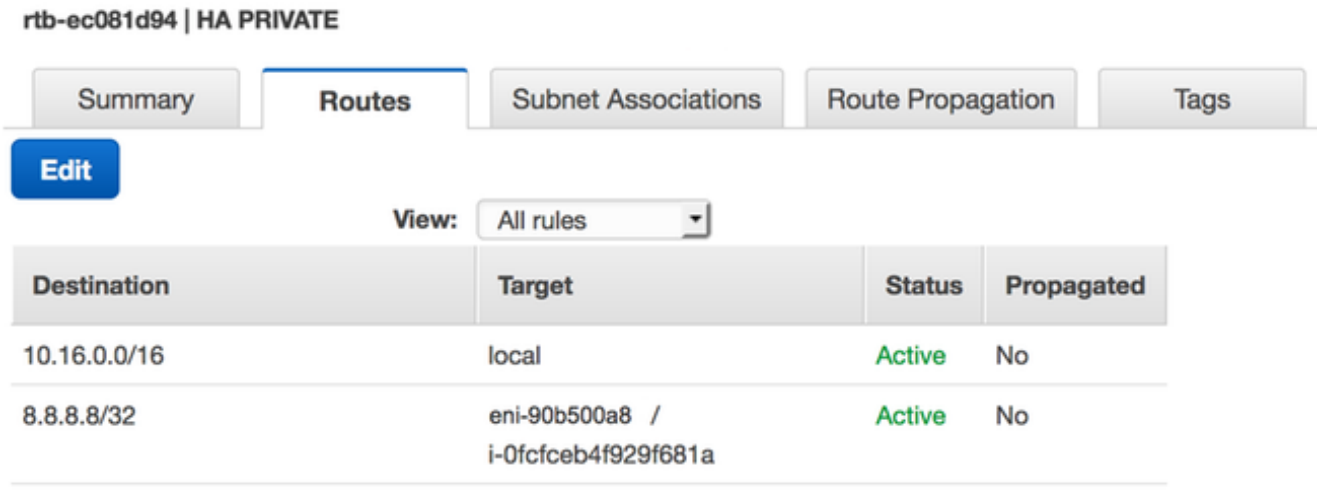
```
redundancy
cloud provider aws 1
  bfd peer 192.168.1.2
  route-table rtb-ec081d94
  cidr ip 8.8.8.8/32
  eni eni-90b500a8
  region us-west-2
```

Configuratievoorbeeld van redundantie op CSRHA1

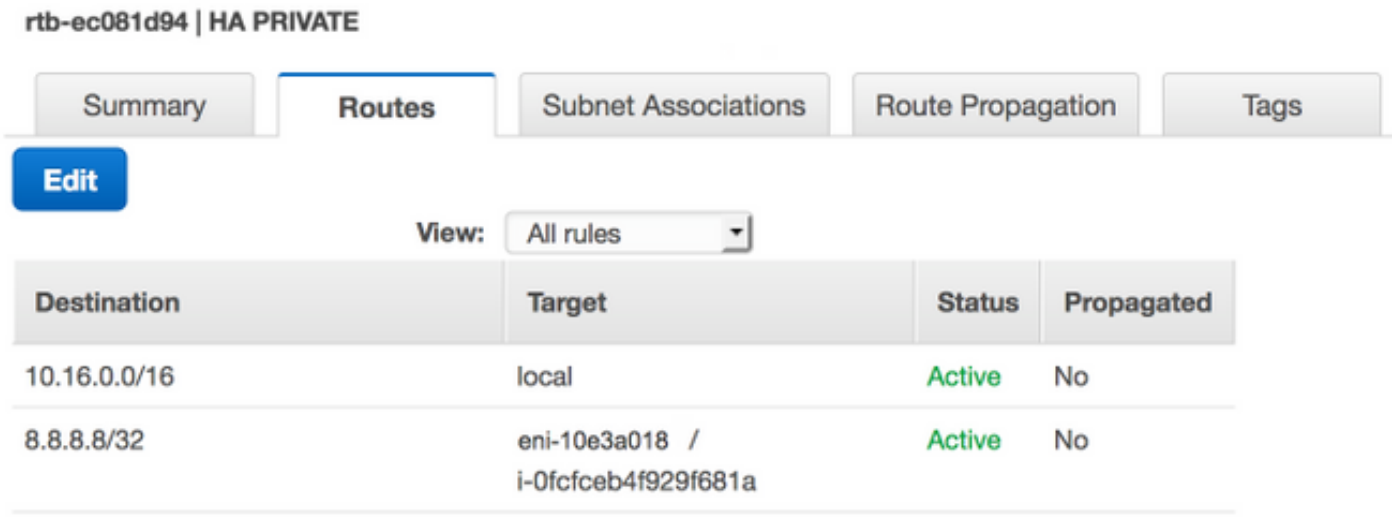
```
redundancy
cloud provider aws 1
  bfd peer 192.168.1.1
  route-table rtb-ec081d94
  cidr ip 8.8.8.8/32
  eni eni-10e3a018
  region us-west-2
```

Controleer hoge beschikbaarheid

1. Controleer BFD- en cloudconfiguraties.
```
CSRHA#show bfd nei

IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
192.168.1.2 4097/4097 Up Up Tu1


CSRHA#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.2 Tu1 12 00:11:57 1 1470 0 2


CSRHA#show redundancy cloud provider aws 1

Cloud HA: work_in_progress=FALSE
Provider : AWS node 1
State : idle
BFD peer     = 192.168.1.2
BFD intf     = Tunnel1
route-table  = rtb-ec081d94
cidr         = 8.8.8.8/32
eni          = eni-90b500a8
region       = us-west-2
```
2. Voer een continue ping uit van de VM naar de bestemming. Verzeker pingelen is door de privé eth1 interface.
```
ubuntu@ip-10-16-3-139:~$ ping -I eth1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 10.16.6.131 eth1: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=50 time=1.60 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=50 time=1.62 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=50 time=1.57 ms
```
3. Controleer de Private Route-tabel. Het eni is momenteel de private interface van CSRHA waar dit het verkeer is.



4. Sluit Tunnel1 van CSRHA af om een HA failover te simuleren.
```
CSRHA(config)#int Tun1
CSRHA(config-if)#shut
```
5. Merk op dat de routetabel verwijst naar het nieuwe ENI, de private interface van CSRHA1.



Problemen oplossen

- Zorg ervoor dat de bronnen worden gekoppeld. Bij het maken van VPC's, subnetten, interfaces, routekaarten, etc. worden veel van deze niet automatisch aan elkaar gekoppeld. Ze kennen elkaar niet.
- Zorg ervoor dat de elastische IP en alle Private IP is gekoppeld aan de juiste interfaces, met de juiste subnetten, toegevoegd aan de juiste routetabel, aangesloten op de juiste router en de juiste VPC en Zone, gekoppeld aan de IAM Role en beveiligingsgroepen.
- Schakel de bron-/droogcontrole per ENI uit.
- Voor Cisco IOS XE 16.3.1a of hoger zijn de extra verificatieopdrachten beschikbaar.

```
show redundancy cloud provider [aws | azure] node-id
debug redundancy cloud [all | trace | detail | error]
debug ip http all
```

- Hier zijn veel voorkomende fouten die worden gezien bij debugs:

Probleem: httpc_send_request mislukt

Resolutie: HTTP wordt gebruikt om de API-oproep van de CSR naar AWS te versturen. Zorg ervoor dat DNS de DNS naam kan oplossen die in uw instantie wordt vermeld. Zorg ervoor dat het http-verkeer niet wordt geblokkeerd.

```
*May 30 20:08:06.922: %VXE_CLOUD_HA-3-FAILED: VXE Cloud HA BFD state transitioned, AWS node 1
event httpc_send_request failed
*May 30 20:08:06.922: CLOUD-HA : AWS node 1 httpc_send_request failed (0x12)
URL=http://ec2.us-east-2b.amazonaws.com
```

Probleem: de routetabel rtb-9c000f4 en de interface eni-32791318 behoren tot verschillende netwerken

Resolutie: De naam van het gebied en ENI worden verkeerd gevormd in verschillende netwerken. Regio en ENI moeten in dezelfde zone liggen als de router.

```
*May 30 23:38:09.141: CLOUD-HA : res content iov_len=284 iov_base=<?xml version="1.0"
encoding="UTF-8"?>
<Response><Errors><Error><Code>InvalidParameterValue</Code><Message>route table rtb-9c0000f4 and
interface eni-32791318 belong to different
networks</Message></Error></Errors><RequestID>af3f228c-d5d8-4b23-b22c-
f6ad999e70bd</RequestID></Response>
```

Probleem: U bent niet geautoriseerd om deze handeling uit te voeren. Gecodeerd bericht van de vergunningsmislukking.

Resolutie: IAM JSON-rol/-beleid is onjuist of niet toegepast op de MVO. De rol van IAM machtigt de MVO om API-oproepen te doen.

```
*May 30 22:22:46.437: CLOUD-HA : res content iov_len=895 iov_base=<?xml version="1.0"
encoding="UTF-8"?>
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not authorized to
perform this operation. Encoded
authorization failure message: qYvEB4MUdOB8m2itSteRgnOuslAaxhAbDph5qGRJkjJbrESajbmF5HWUR-
MmHYeRAlpKZ3Jg_y-
_tMlYel5l_ws8Jd9q2W8YDXBl3uXQqfW_cjjrgy9jhnGY0nOaNu65aLpfqui8kS_4RPOpm5grRFfo99-
8uv_N3mYaBqKFPn3vUcSYKBmxFIIkJKcjY9esOeLIOWDcnYGGu6AGGMoMxWDtk0K8nwk4IjLDcnd2cDXeENS45w1PqzKGPsH
v3wD28TS5xRjIrPXYrT18UpV6lLA_09Oh4737VncQKfzbz4tPpnAkoW0mJLQ1vDpPmNvHUpEng8KrGWYNfbfemoDtWqIdABf
aLLLmh4saNtnQ_OMBoTi4toBLEb2BNdMkl1UVBIxqTqdFUVRS**MSG 00041 TRUNCATED** **MSG 00041
CONTINUATION
#01**qLosAb5Yx0DrOsLSQwzS95VGvQM_n87LBHYbAWWhqWj3UfP_zmiak7dlm9P41mFCucEB3Cs4FRsFtb-
9q44VtyQJaS2sU2nhGe3x4uGEsl7F1pNv5vhVeYOZB3tbOfbV1_Y4trZwYPFgLKgBShZp-WNmUKUJsKc1-
6KGqmp7519imvh66JgwgmU9DT_qAZ-jEjkqWjBrxg6krw</Message></Error></Errors><RequestID>4cf31249-
2a6e-4414-ae8d-6fb825b0f398</RequestID></Response>
```

Gerelateerde informatie

- VPC Gateway-redundantie - Cisco
- Cisco CRS-1000v Series implementatiegids voor cloudservices voor Amazon Web Services
- Indeling van soorten instanties
- EC2 en VPC's
- Elastische netwerkinterfaces, uit de EC2-gebruikershandleiding, bevatten # van ENI's per instantietype
- Uitgebreide netwerken op Linux hoe te, nuttige achtergrondinformatie
- Speciale Instanties/huuruitleg en Hoe
- Algemene EG2-documentatie
- Algemene VPC-documentatie
- Regio's en beschikbaarheidszones
- CSR1000v hoge beschikbaarheid versie 3

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.