Implementierungsleitfaden für CSR1000v HA-Redundanz auf Amazon AWS

Inhalt

Einleitung

Dieses Dokument beschreibt den Konfigurationsleitfaden zur Bereitstellung von CSR1000v-Routern für hohe Verfügbarkeit in der Amazon AWS-Cloud. Es soll den Benutzern praktische Kenntnisse über Hochverfügbarkeit und die Möglichkeit geben, eine voll funktionsfähige Testumgebung bereitzustellen.

Weitere Hintergrundinformationen zu AWS und HA *finden Sie* im Abschnitt .

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Ein Amazon AWS-Konto
- 2 CSR1000v und 1 Linux/Windows AMIs in derselben Region
- HA-Version 1 wird von Cisco IOS-XE® Versionen 16.5 bis 16.9 unterstützt. Ab 16.11 und höher HA-Version 3 verwenden.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco IOS-XE® Denali 16.7.1.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Ziel

Simulieren Sie in einer Umgebung mit mehreren Verfügbarkeitszonen den kontinuierlichen Datenverkehr vom privaten Rechenzentrum (VM) zum Internet. Simulieren Sie einen HA-Failover, und stellen Sie fest, dass HA erfolgreich ist, wenn die Routing-Tabelle den Datenverkehr von CSRHA auf die private Schnittstelle von CSRHA1 umschaltet.

Topologie

Bevor die Konfiguration beginnt, müssen Topologie und Design vollständig verstanden werden. Dies hilft, potenzielle Probleme später zu beheben.

Abhängig von den Netzwerkanforderungen gibt es verschiedene Szenarien für die Bereitstellung einer hohen Verfügbarkeit. Für dieses Beispiel wird HA-Redundanz mit den folgenden Einstellungen konfiguriert:

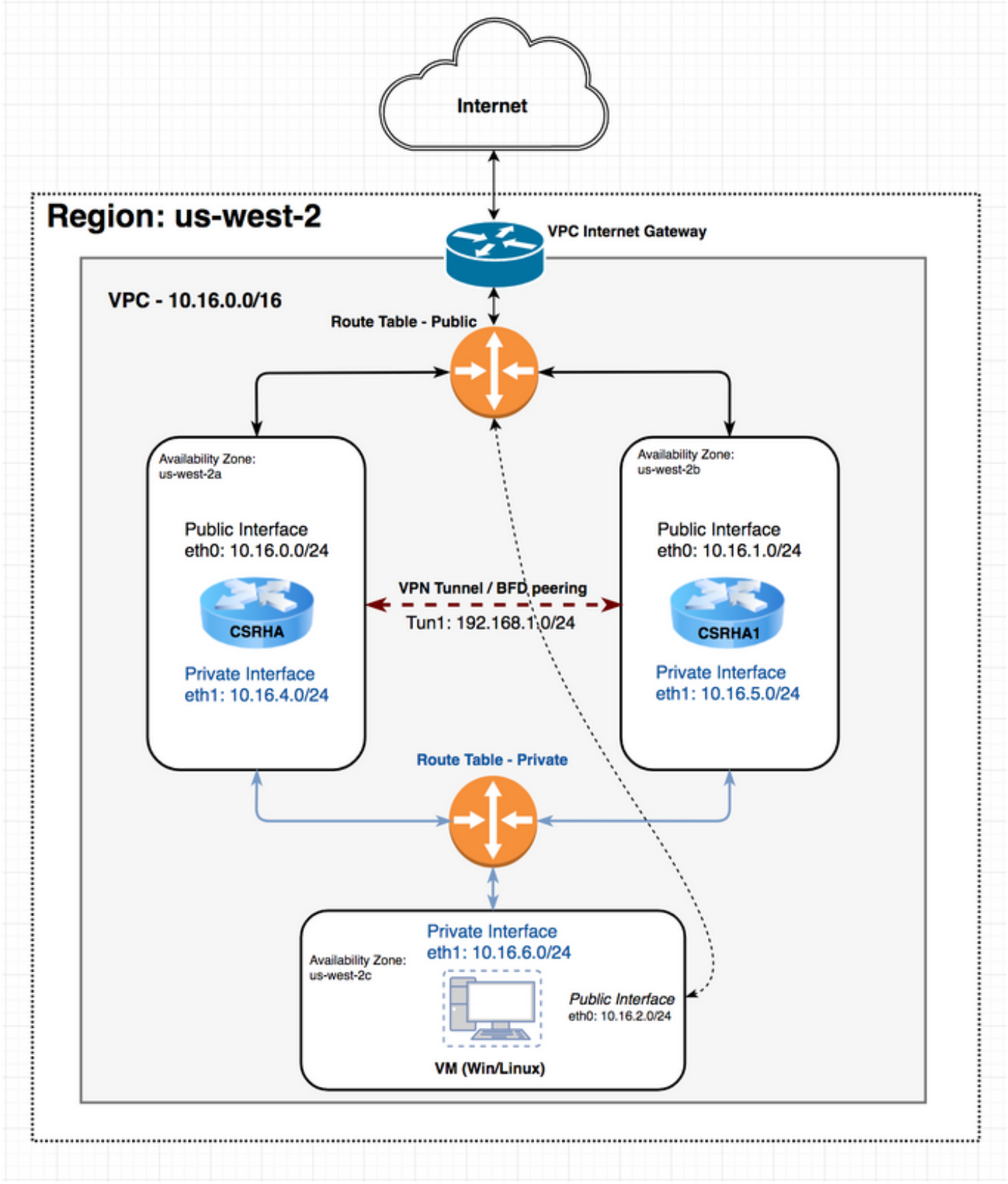
- 1 x - Region
- 1 x - VPC
- 3x - Verfügbarkeitsbereiche
- 6x - Netzwerkschnittstellen/Subnetze (3x zur öffentlichen Ansicht/3x zur privaten Ansicht)
- 2x - Routing-Tabellen (öffentlich und privat)
- 2x - CSR1000v Router (Cisco IOS-XE® Denali 16.3.1a oder höher)
- 1x - VM (Linux/Windows)

In einem HA-Paar gibt es 2 CSR1000v-Router in zwei verschiedenen Verfügbarkeitszonen. Betrachten Sie jede Verfügbarkeitszone als separates Rechenzentrum für zusätzliche Hardware-Ausfallsicherheit.

Die dritte Zone ist eine VM, die ein Gerät in einem privaten Rechenzentrum simuliert. Derzeit wird der Internetzugriff über die öffentliche Schnittstelle auf aktiviert, sodass Sie auf das virtuelle System zugreifen und es konfigurieren können. Generell sollte der gesamte normale Datenverkehr die private Routing-Tabelle durchlaufen.

Pingen Sie die private Schnittstelle des virtuellen Systems → private Routing-Tabelle → CSRHA → 8.8.8.8 für die Verkehrssimulation. In einem Failover-Szenario stellen Sie fest, dass die private Routing-Tabelle die Route so geändert hat, dass sie auf die private Schnittstelle von CSRHA1 verweist.

Netzwerkdiagramm



Terminologie

RTB - Die Routing-Tabellen-ID.

CIDR - Zieladresse für die zu aktualisierende Route in der Routing-Tabelle.

ENI - Die Netzwerkschnittstellen-ID der CSR 1000v Gigabit-Schnittstelle, an die der Datenverkehr weitergeleitet wird.

Wenn beispielsweise CSRHA ausfällt, übernimmt CSRHA1 und aktualisiert die Route in der AWS-Routing-Tabelle, sodass sie auf ihre eigene ENI verweist.

REGION - Die AWS Region der CSR 1000v.

Einschränkungen

- Verwenden Sie für private Subnetze nicht die IP-Adresse 10.0.3.0/24 - diese wird intern auf dem Cisco CSR 1000v für Hochverfügbarkeit verwendet. Der Cisco CSR 1000v muss über eine öffentliche Internetverbindung verfügen, um REST-API-Aufrufe durchführen zu können, die die AWS-Routing-Tabelle ändern.

- Positionieren Sie die gig1-Schnittstelle des CSR1000v nicht innerhalb einer VRF-Instanz. HA funktioniert nicht anders.

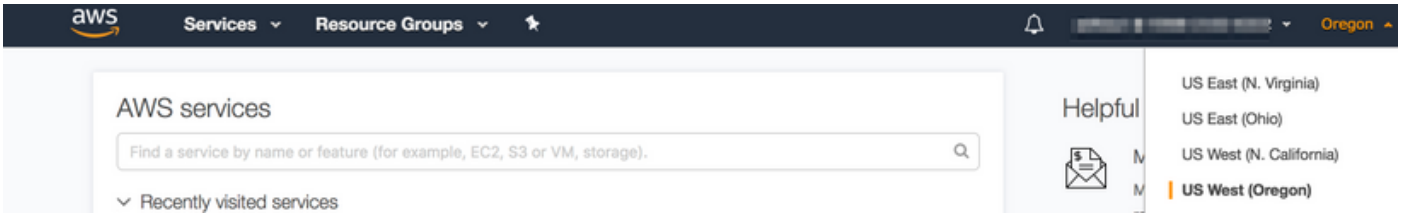
Konfiguration

Der allgemeine Konfigurationsfluss besteht darin, mit der umfassendsten Funktion (Region/VPC) zu beginnen und zum spezifischsten Feature (Schnittstelle/Subnetz) überzugehen. Es gibt jedoch keine bestimmte Reihenfolge der Konfiguration. Bevor Sie beginnen, ist es wichtig, zuerst die Topologie zu verstehen.

> **Tipp:** Geben Sie allen Ihren Einstellungen (VPC, Schnittstelle, Subnetz, Routing-Tabellen usw.) Namen.

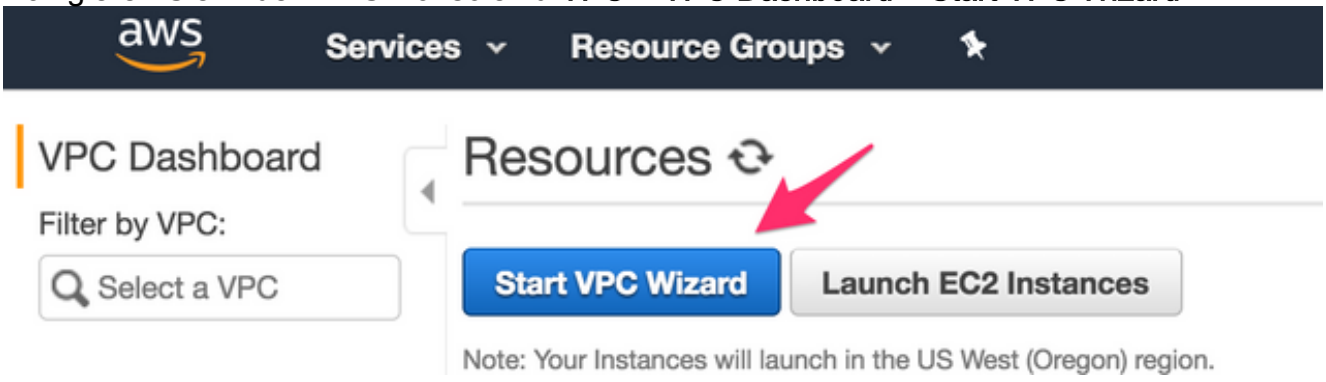
Schritt 1: Wählen Sie eine Region aus.

In diesem Beispiel wird US West (Oregon) verwendet.

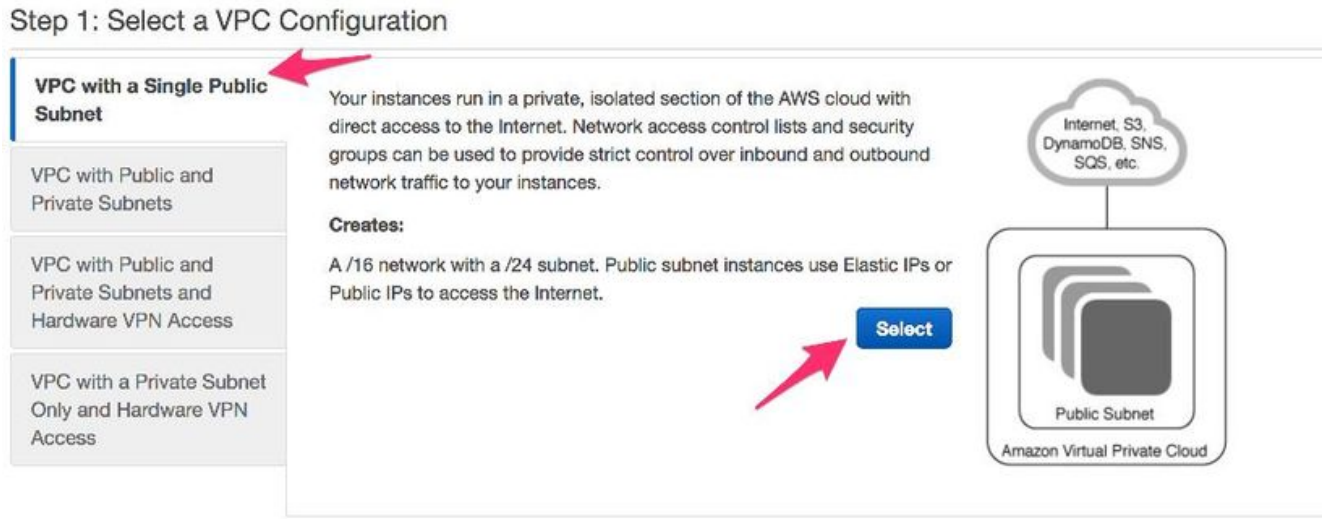


Schritt 2: Erstellen einer vPC

1. Navigieren Sie in der AWS-Konsole zu **VPC > VPC Dashboard > Start VPC Wizard**.

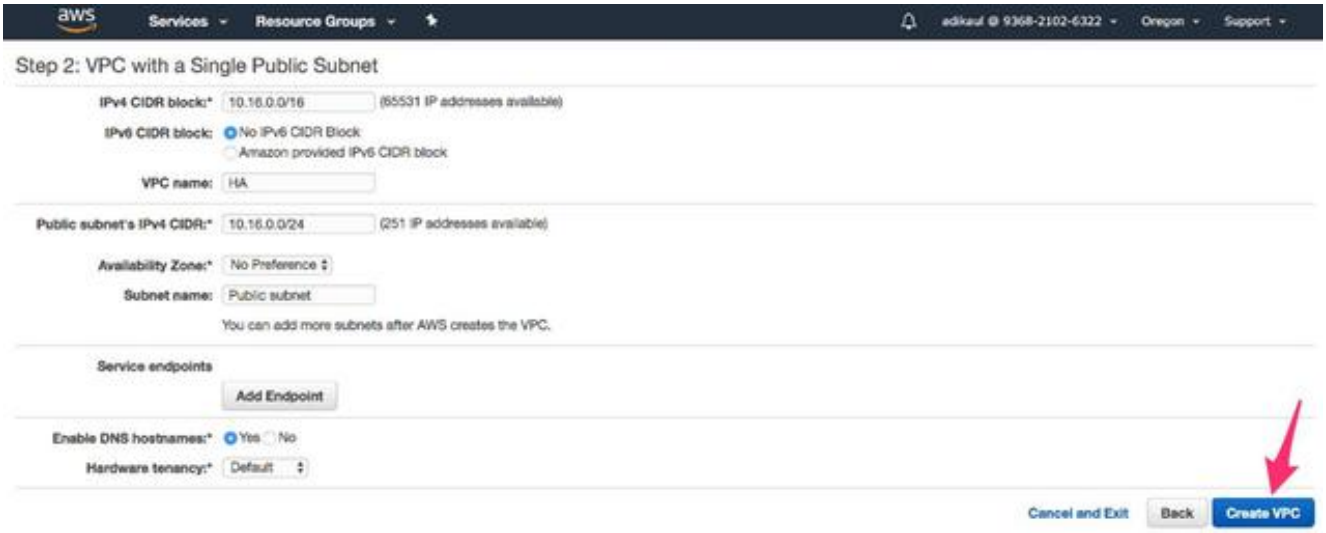


2. Wählen Sie VPC mit einem einzelnen öffentlichen Subnetz aus.

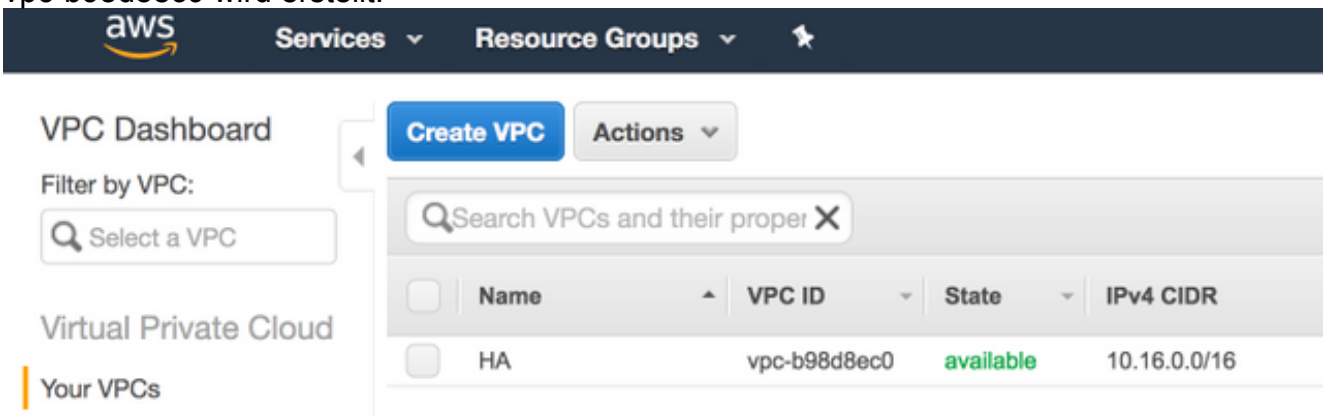


3. Wenn Sie eine VPC erstellen, wird Ihnen ein /16-Netzwerk zugewiesen, das Sie verwenden können.

4. Ihnen wird auch ein öffentliches /24-Subnetz zugewiesen. Öffentliche Subnetzinstanzen verwenden elastische IPs oder öffentliche IPs, damit Ihre Geräte auf das Internet zugreifen können.



5. vpc-b98d8ec0 wird erstellt.



Schritt 3: Erstellen einer Sicherheitsgruppe für die vPC

Sicherheitsgruppen sind wie ACLs, um Datenverkehr zu erlauben oder zu verweigern.

1. Klicken Sie unter Security (Sicherheit) auf **Security Groups (Sicherheitsgruppen)**, und **erstellen Sie Ihre Sicherheitsgruppe**, die mit der oben erstellten VPC mit dem Namen HA verknüpft ist.

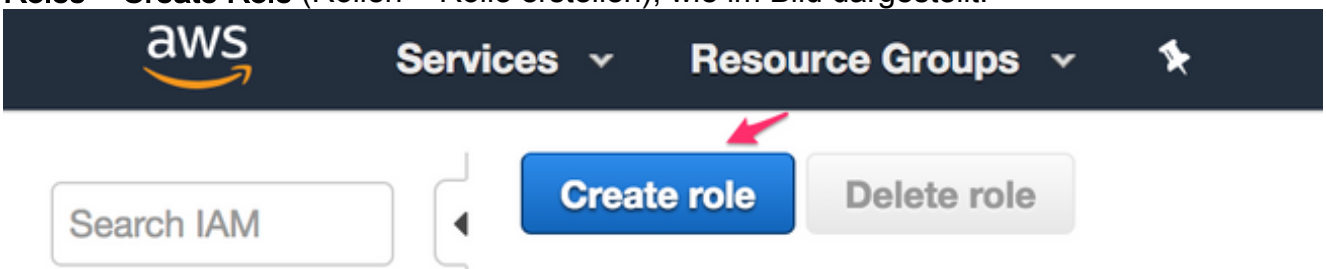
2. Legen Sie unter Inbound Rules (Eingehende Regeln) fest, welchen Datenverkehr Sie für sg-1cf47d6d zulassen möchten. In diesem Beispiel lassen Sie den gesamten Datenverkehr zu.

Schritt 4: Erstellen Sie eine IAM-Rolle mit einer Richtlinie, und ordnen Sie sie der VPC zu.

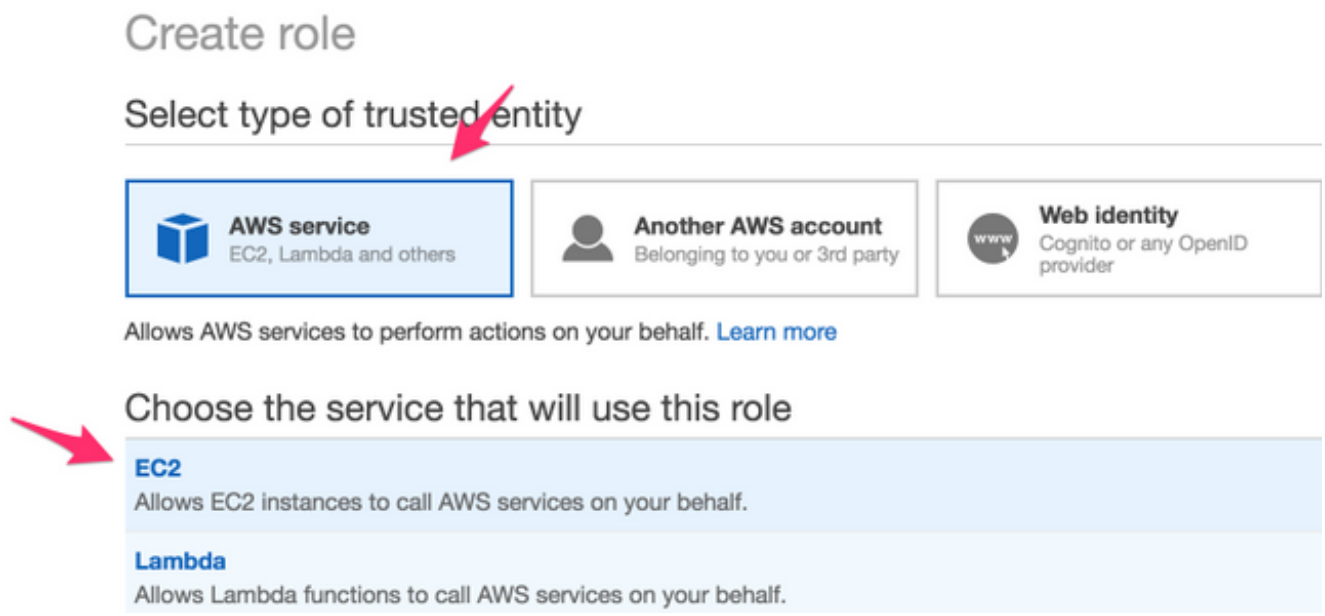
IAM gewährt Ihrem CSR Zugriff auf Amazon APIs.

Der CSR1000v wird als Proxy verwendet, um AWS API-Befehle zum Ändern der Routing-Tabelle aufzurufen. Standardmäßig haben AMIs keinen Zugriff auf APIs. Durch dieses Verfahren wird eine IAM-Rolle erstellt, die beim Starten einer CSR-Instanz verwendet wird. IAM stellt Zugriffsberechtigungen für CSRs bereit, um AWS-APIs zu verwenden und zu ändern.

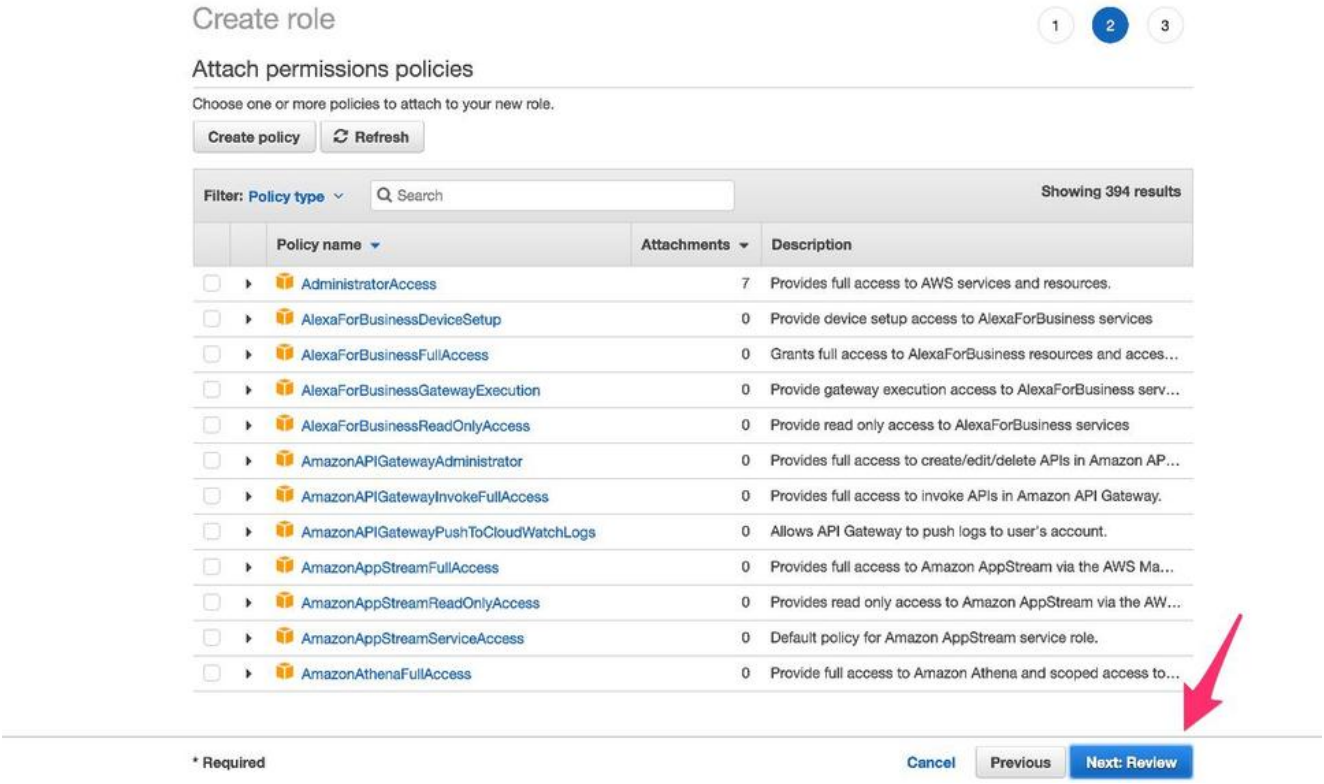
1. Erstellen Sie die IAM-Rolle. Navigieren Sie zum IAM-Dashboard, und navigieren Sie zu **Roles > Create Role** (Rollen > Rolle erstellen), wie im Bild dargestellt.



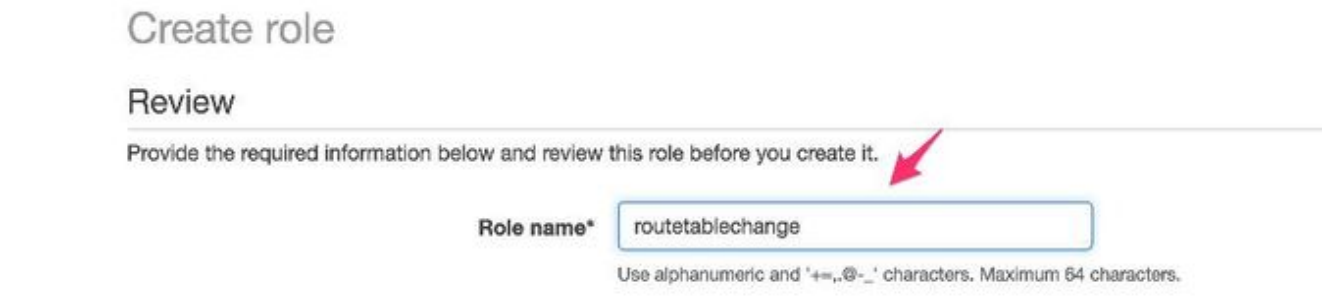
2. Wie im Bild gezeigt, erlauben Sie der EC2-Instanz, AWS in Ihrem Namen aufzurufen.



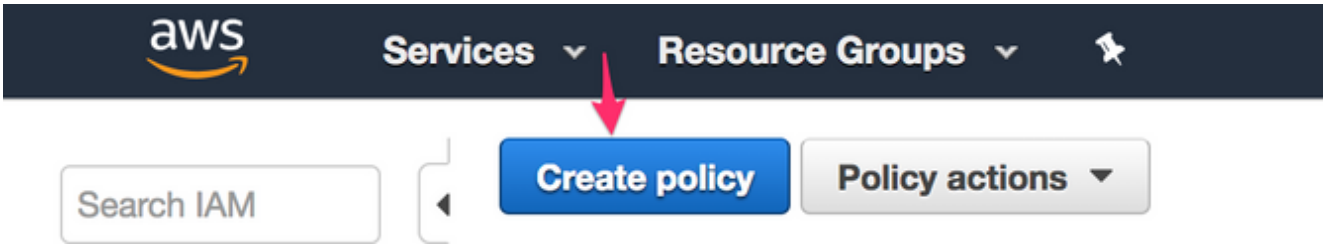
3. Erstellen Sie eine Rolle, und klicken Sie auf **Weiter: Überprüfen Sie**, wie im Bild gezeigt.



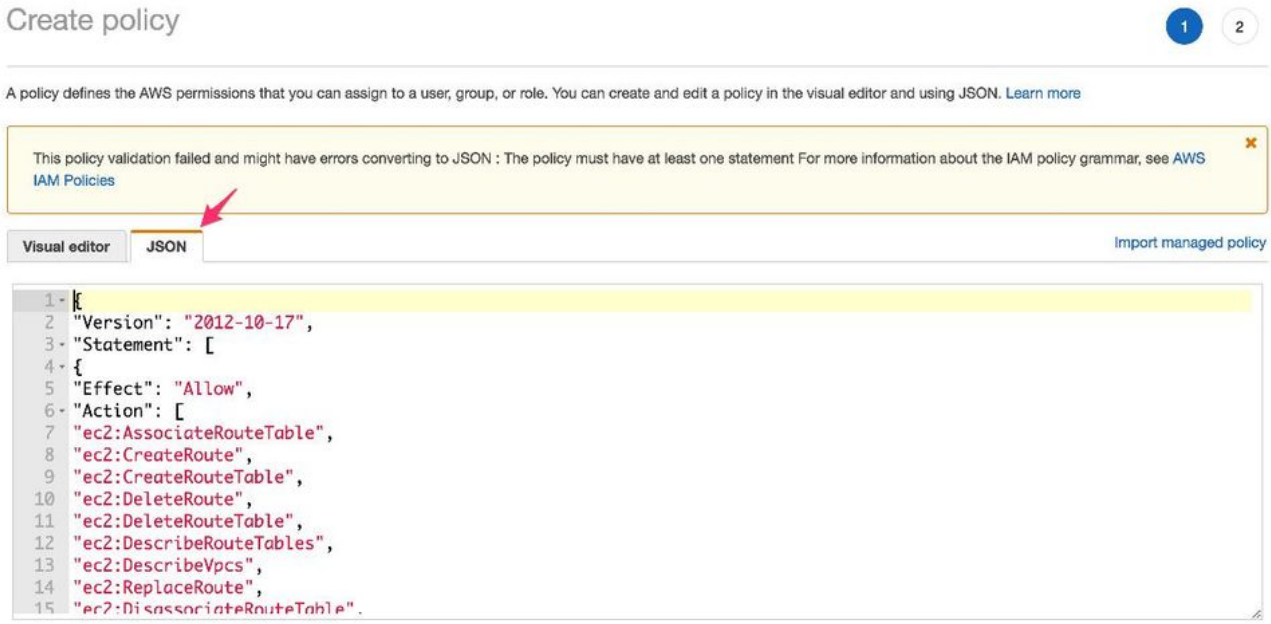
4. Geben Sie ihm einen Rollennamen. Wie im Bild gezeigt, lautet der Rollenname für dieses Beispiel routetablechange...



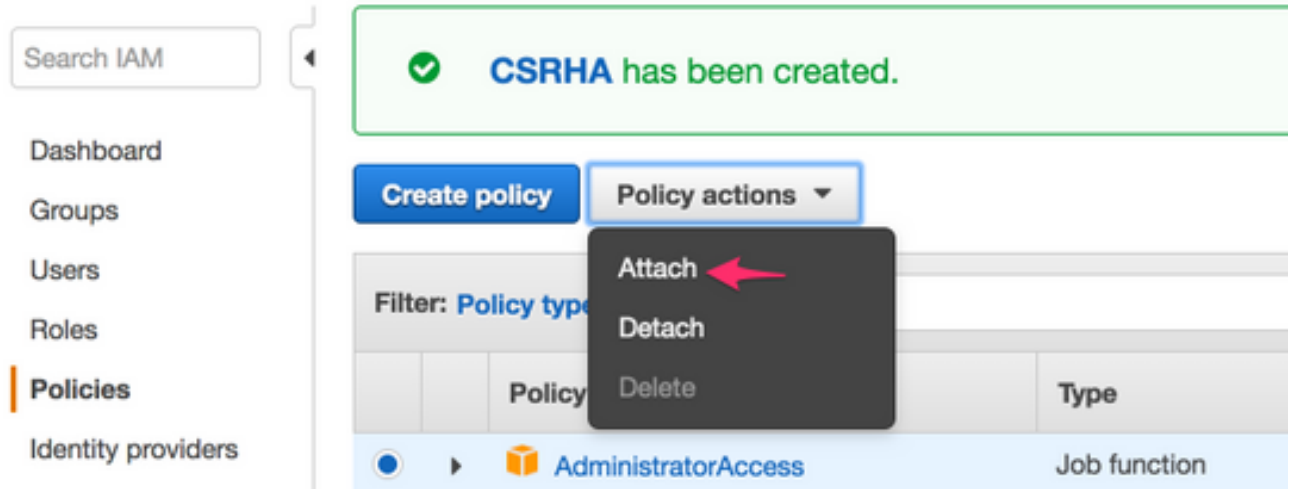
5. Als Nächstes müssen Sie eine Richtlinie erstellen und diese der zuvor erstellten Rolle zuordnen. IAM-Dashboard, und navigieren Sie zu **Policies > Create Policy**.



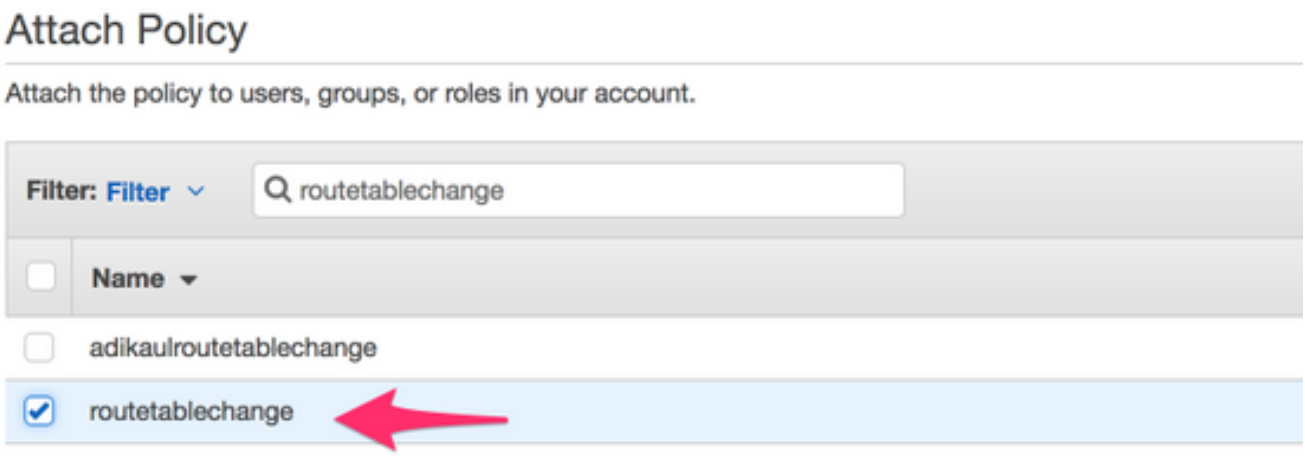

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:AssociateRouteTable",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:DeleteRoute",
"ec2:DeleteRouteTable",
"ec2:DescribeRouteTables",
"ec2:DescribeVpcs",
"ec2:ReplaceRoute",
"ec2:DisassociateRouteTable",
"ec2:ReplaceRouteTableAssociation"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



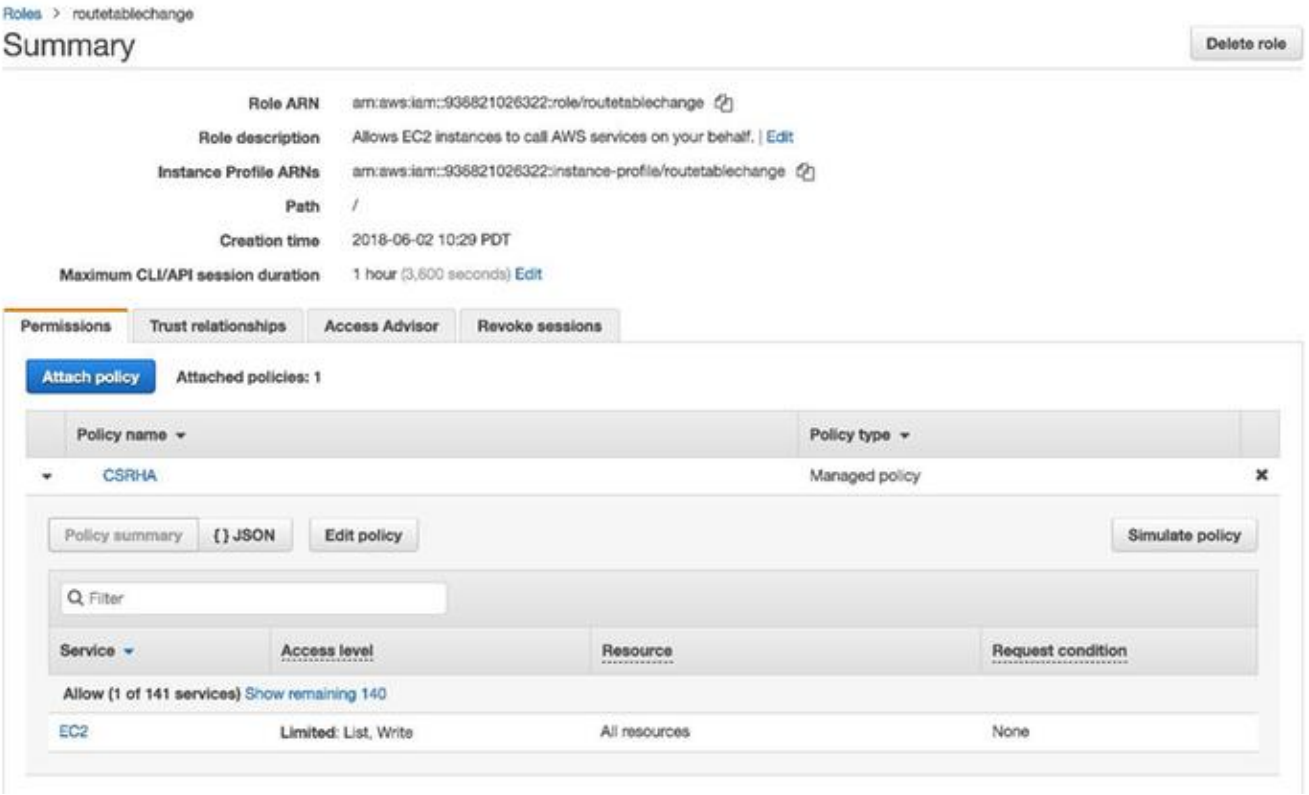
6. Geben Sie ihm einen Richtliniennamen, und hängen Sie ihn an die von Ihnen erstellte Rolle an. In diesem Beispiel heißt der Richtlinienname CSRHA mit Administratorzugriff, wie im Bild gezeigt.



7. Wie im Bild gezeigt, hängen Sie die Richtlinie an die Rolle an, die Sie mit dem Namen routetablechange erstellt **haben**.



8. Zusammenfassung.



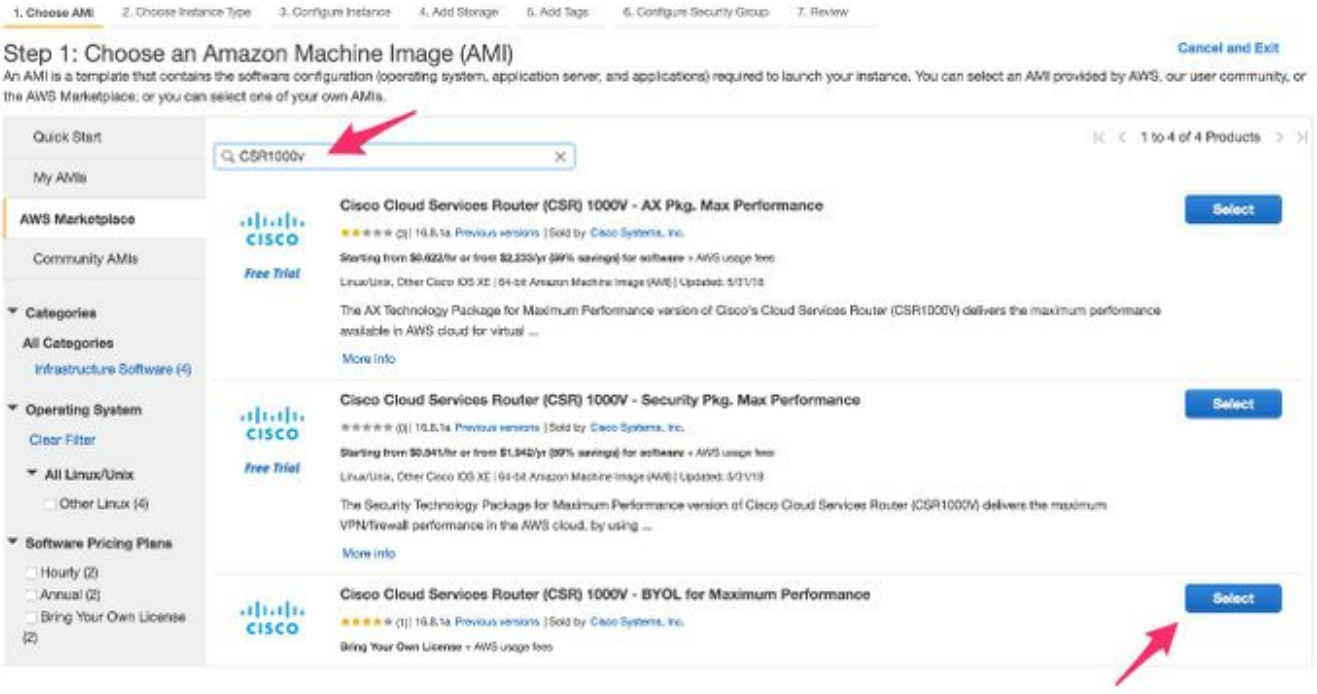
Schritt 5: Starten Sie die CSR1000vS mit der von Ihnen erstellten AMI-Rolle, und ordnen Sie die öffentlichen/privaten Subnetze zu.

Jeder CSR1000v-Router verfügt über 2 Schnittstellen (1 öffentlich, 1 privat) und befindet sich in einer eigenen Verfügbarkeitszone. Sie können sich vorstellen, dass sich die einzelnen CSR in separaten Rechenzentren befinden.

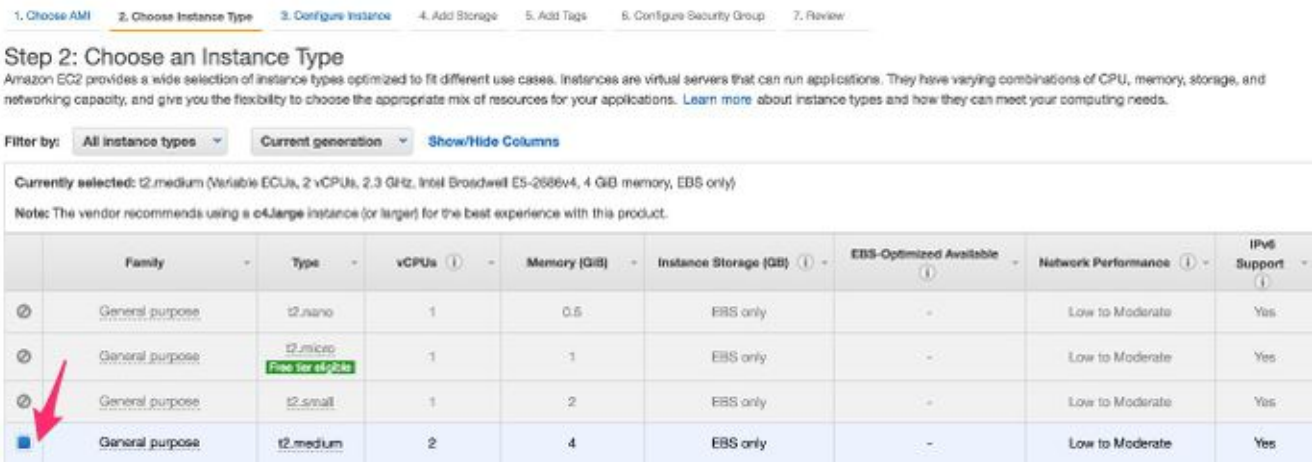
1. Wählen Sie auf der AWS-Konsole **EC2 aus**, und klicken Sie dann auf **Instanz starten**.

2. Wählen Sie AWS Marketplace aus.

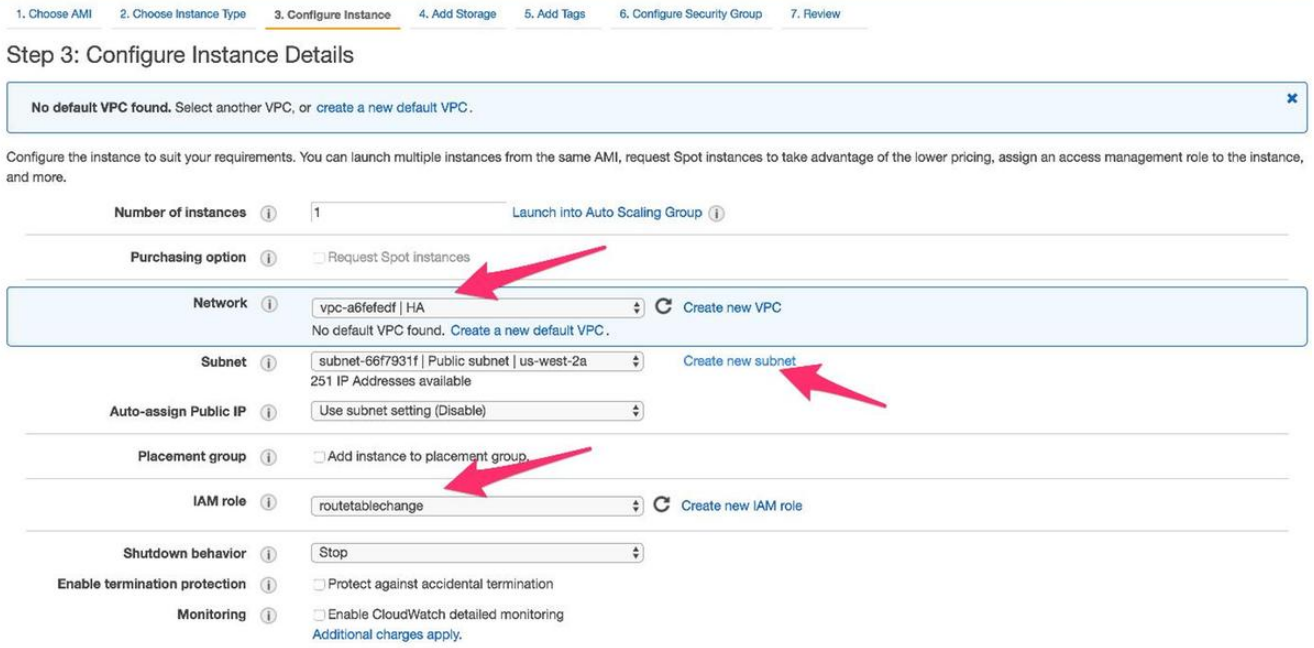
3. Geben Sie CSR1000v ein, und verwenden Sie in diesem Beispiel den Cisco Cloud Services Router (CSR) 1000V - BYOL für maximale Leistung.



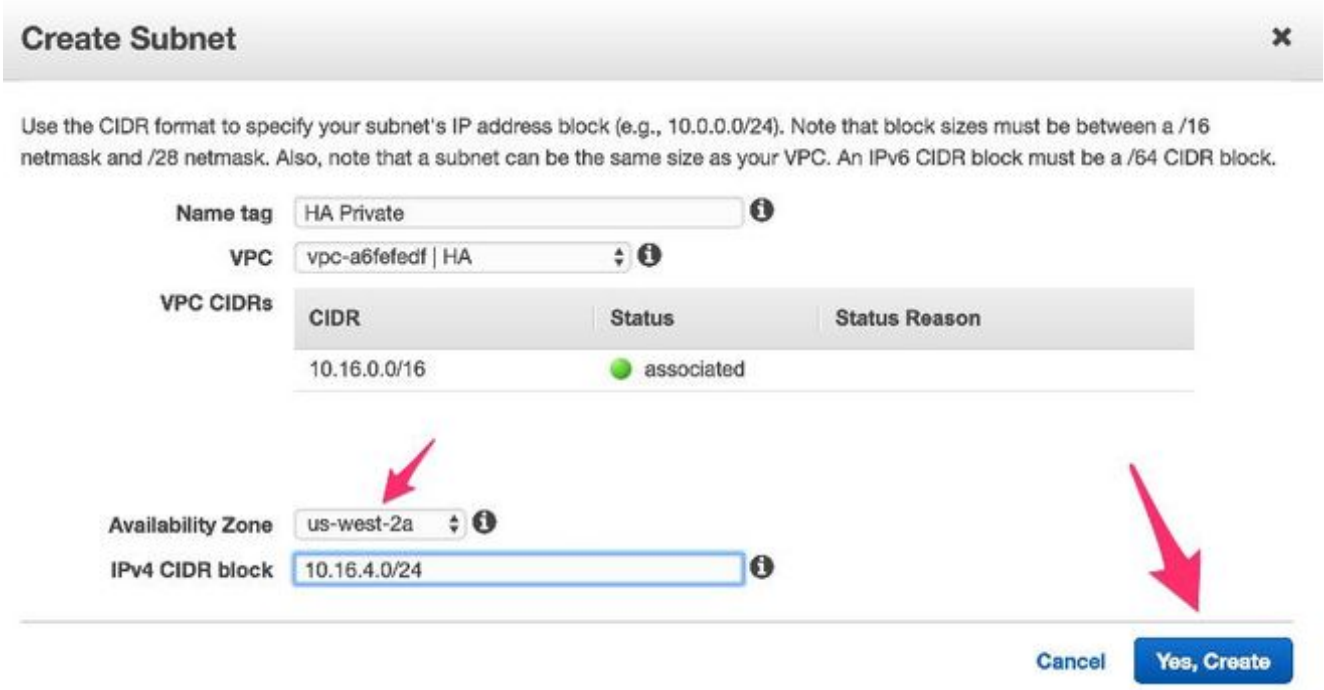
4. Wählen Sie einen Instanztyp aus. Für dieses Beispiel ist der ausgewählte Typ **t2.medium**.



5. Während die Instanz konfiguriert ist, müssen Sie sicherstellen, dass Sie die oben erstellte vPC zusammen mit der oben angegebenen IAM-Rolle auswählen. Außerdem erstellen Sie ein privates Subnetz, das Sie mit der Schnittstelle zur privaten Verbindung verknüpfen.



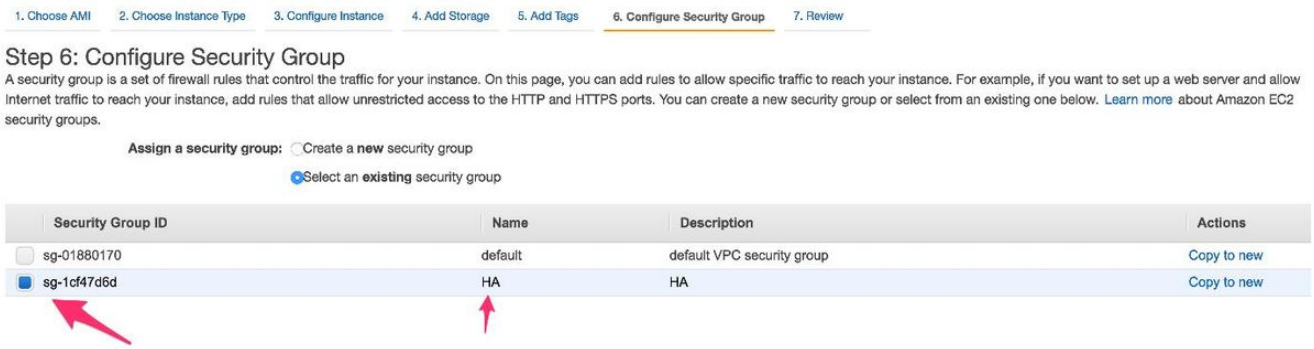
6. Klicken Sie auf Neues Subnetz für privates Subnetz erstellen. In diesem Beispiel lautet das Name-Tag HA Private. Stellen Sie sicher, dass sie sich in derselben Verfügbarkeitszone wie das öffentliche Subnetz befindet.



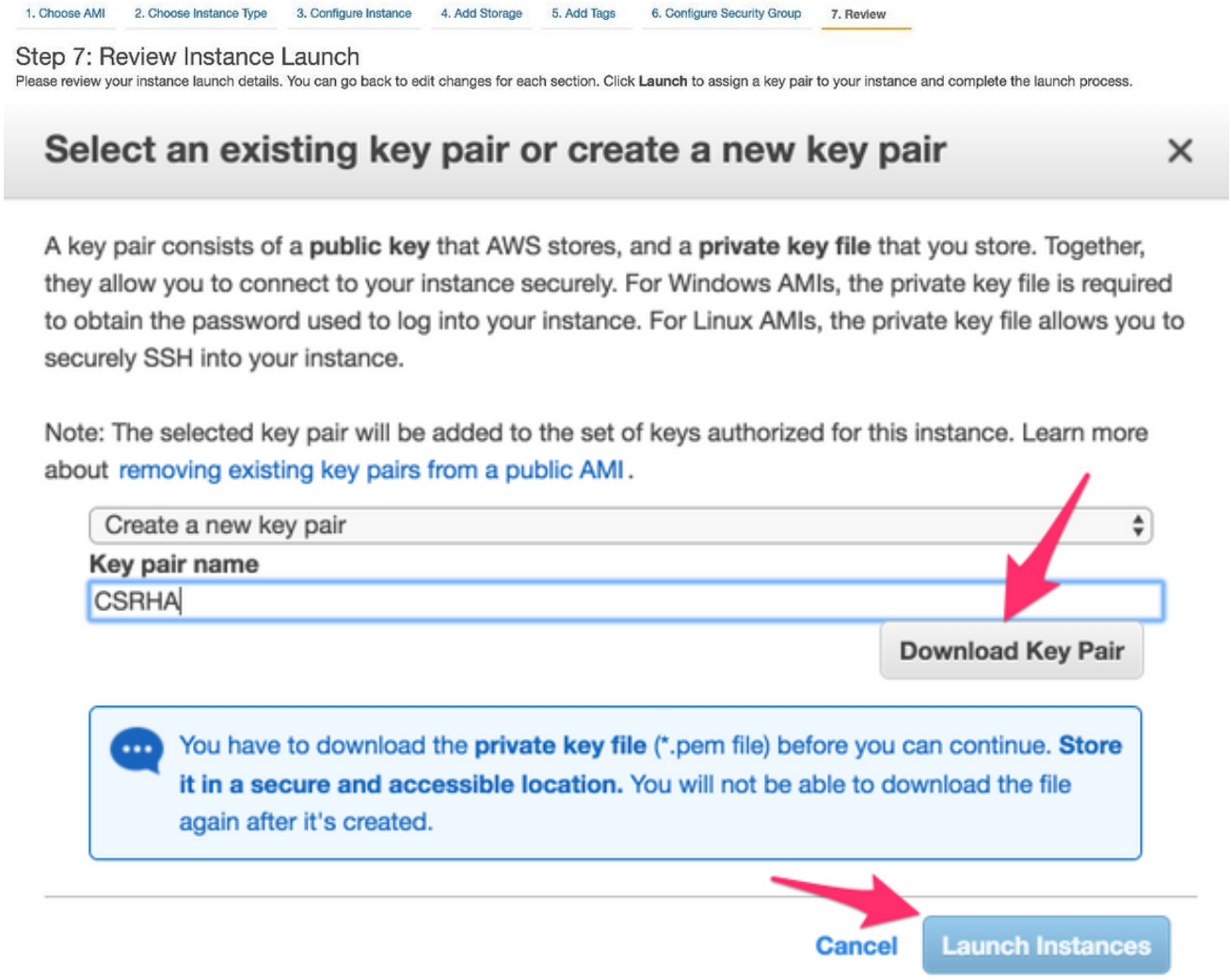
7. Blättern Sie nach unten, und klicken Sie unter "Instanzdetails konfigurieren" auf **Gerät hinzufügen**, wie im Bild dargestellt.

8. Nachdem die sekundäre Schnittstelle hinzugefügt wurde, verknüpfen Sie das von Ihnen erstellte private Subnetz mit dem Namen HA Private. Eth0 ist die öffentliche Schnittstelle, und Eth1 ist die private Schnittstelle. **Anmerkung:** Das im vorherigen Schritt erstellte Subnetz wird in dieser Dropdown-Liste möglicherweise nicht angezeigt. Möglicherweise müssen Sie die Seite aktualisieren oder abbrechen und von vorne beginnen, damit das Subnetz angezeigt
wird.

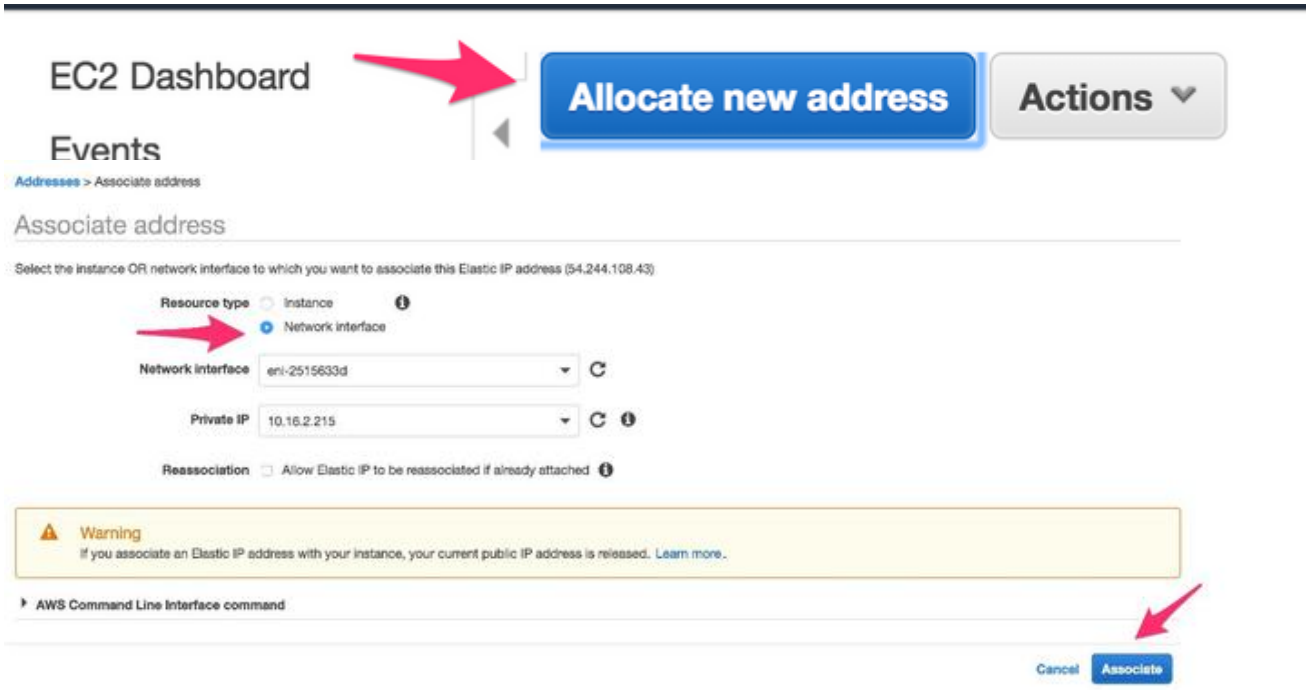
9. Wählen Sie die Sicherheitsgruppe aus, die Sie unter VPC erstellt haben, und stellen Sie sicher, dass die Regeln korrekt definiert sind.



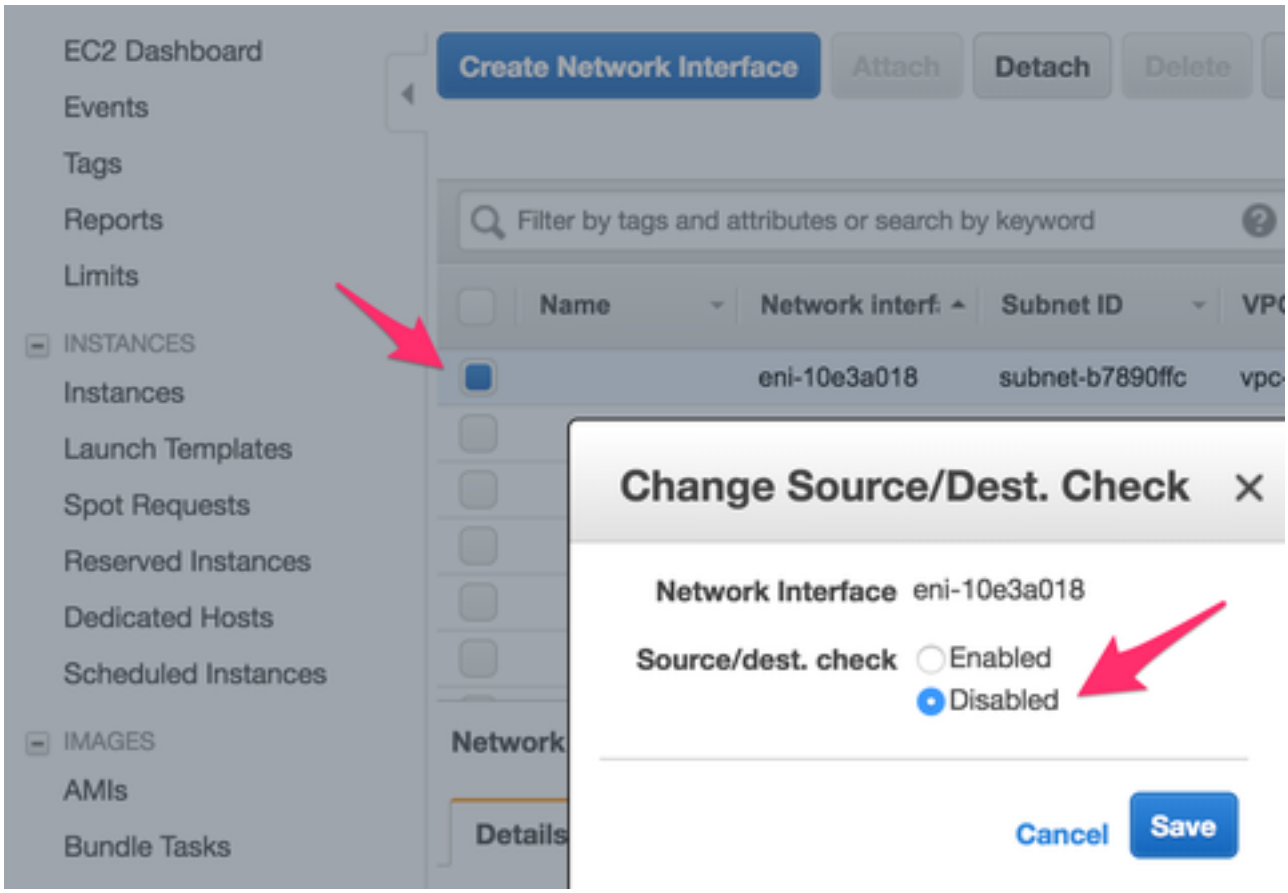
10. Erstellen Sie ein neues Schlüsselpaar, und laden Sie Ihren privaten Schlüssel herunter. Sie können für jedes Gerät einen Schlüssel wiederverwenden. **Anmerkung:** Wenn Sie Ihren privaten Schlüssel verlieren, können Sie sich nicht wieder bei Ihren CSRs anmelden. Es gibt keine Methode, Schlüssel wiederherzustellen.



11. Verknüpfen Sie die Elastic IP mit der ENI der öffentlichen Schnittstelle für die von Ihnen erstellte Instanz, und navigieren Sie zu **AWS console > EC2 Management > Network Security > Elastic IPs**. **Anmerkung:** Öffentliche/private Terminologie kann Sie hier verwirren. Für dieses Beispiel ist die Definition einer öffentlichen Schnittstelle Eth0, die Schnittstelle für das Internet. Aus Sicht von AWS ist unsere öffentliche Schnittstelle ihre private IP.

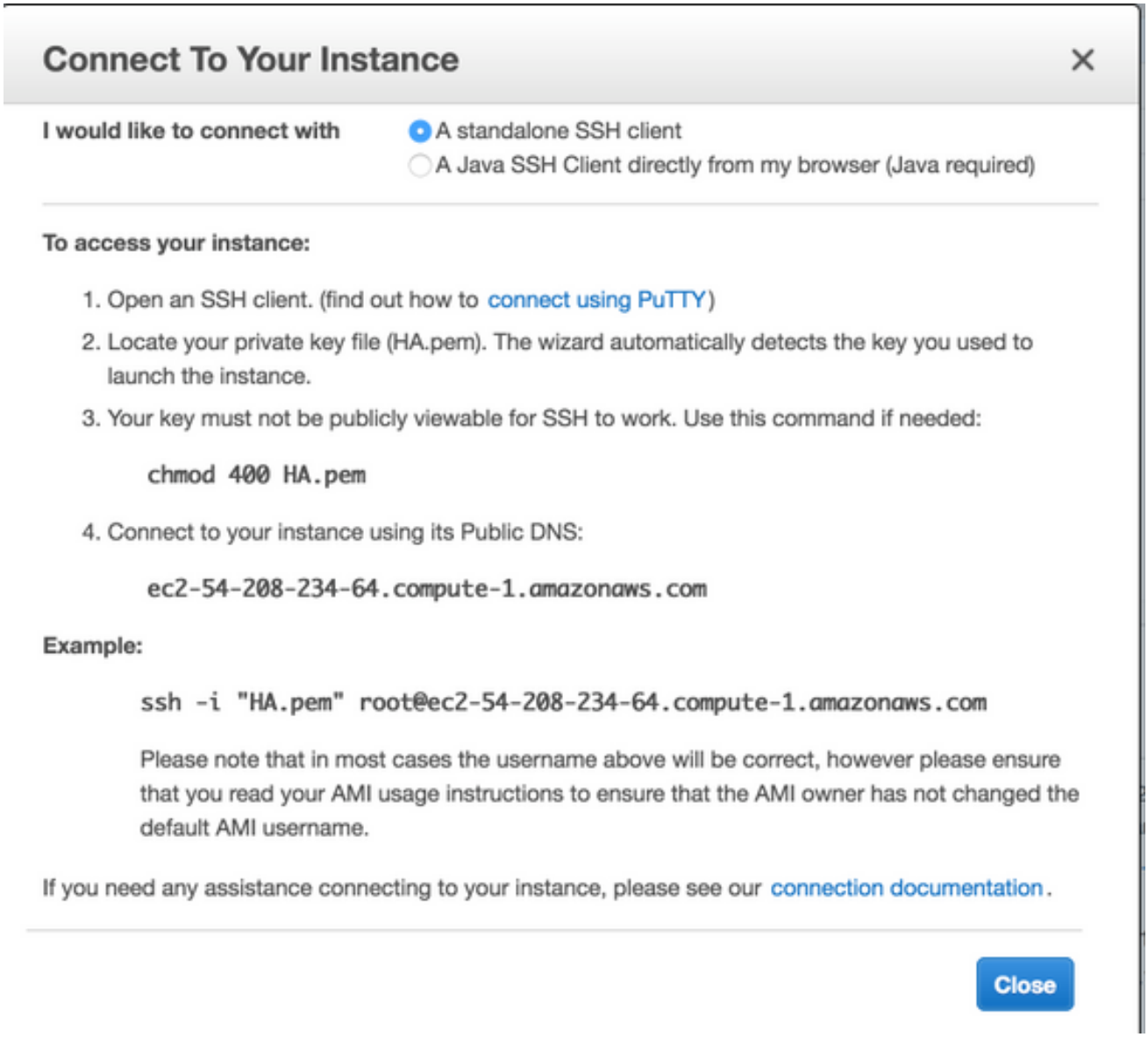


12. Deaktivieren Sie die Quell-/Zielüberprüfung, während Sie zu **EC2 > Network Interfaces** navigieren. Überprüfen Sie jede ENI für die Quell-/Zielprüfung. Standardmäßig ist diese Quell-/Zielprüfung bei allen ENIs aktiviert. Eine Anti-Spoofing-Funktion, mit der verhindert werden soll, dass eine ENI mit Datenverkehr überlaufen wird, der eigentlich nicht für sie bestimmt ist, indem vor der Weiterleitung überprüft wird, ob die ENI das Ziel des Datenverkehrs ist. Der Router ist selten das tatsächliche Ziel eines Pakets. Diese Funktion muss auf allen CSR-Transit-ENIs deaktiviert werden, da sie Pakete nicht weiterleiten kann.



13. Stellen Sie eine Verbindung zum CSR1000v her. **Anmerkung:** Der von AWS für SSH im CSR1000v bereitgestellte Benutzername wird möglicherweise fälschlicherweise als Root

aufgeführt. Ändern Sie dies ggf. in ec2-user.**Anmerkung:** Sie müssen in der Lage sein, die DNS-Adresse an SSH zu pingen. Hier ist es ec2-54-208-234-64.compute-1.amazonaws.com. Überprüfen Sie, ob das öffentliche Subnetz/die öffentliche Subnetznummer des Routers mit der öffentlichen Routentabelle verknüpft ist. Fahren Sie kurz mit Schritt 8 fort, um das Subnetz der Routentabelle zuzuordnen.



Schritt 6: Wiederholen Sie Schritt 5, und erstellen Sie die zweite CSR1000v-Instanz für HA.

Öffentliches Subnetz: 10.16.1.0/24

Privates Subnetz: 10.16.5.0/24

Wenn Sie die elastische IP-Adresse dieser neuen AMI nicht pingen können, gehen Sie kurz zu Schritt 8, und stellen Sie sicher, dass das öffentliche Subnetz mit der öffentlichen Routing-Tabelle verknüpft ist.

Schritt 7: Wiederholen Sie Schritt 5 und erstellen Sie eine VM (Linux/Windows) aus dem AMI Marketplace.

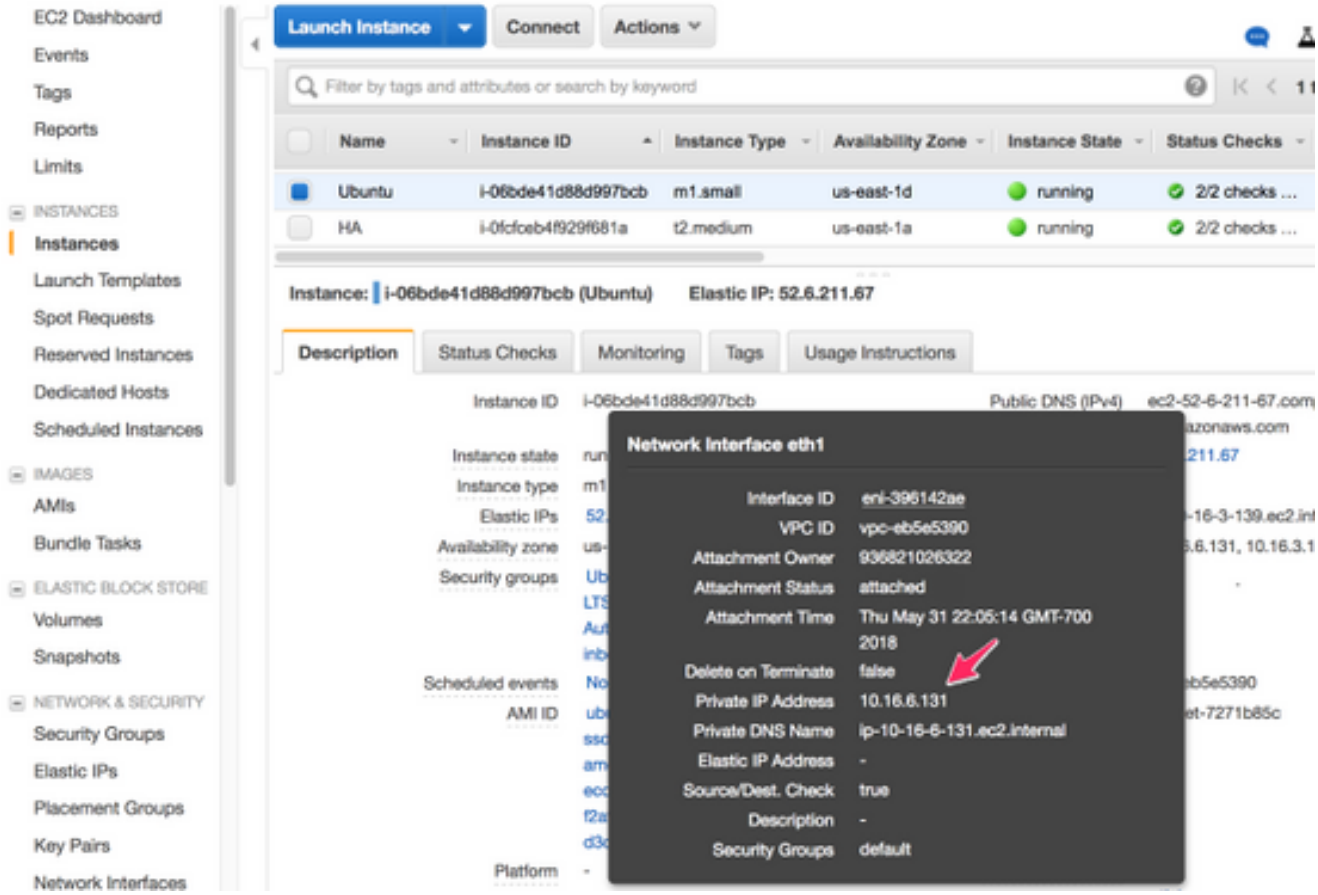
Verwenden Sie für dieses Beispiel Ubuntu Server 14.04 LTS auf dem Markt.

Öffentliches Subnetz: 10.16.2.0/24

Privates Subnetz: 10.16.6.0/24

Wenn Sie die elastische IP-Adresse dieser neuen AMI nicht pingen können, gehen Sie kurz zu Schritt 8, und stellen Sie sicher, dass das öffentliche Subnetz mit der öffentlichen Routing-Tabelle verknüpft ist.

1. Eth0 wird standardmäßig für die öffentliche Schnittstelle erstellt. Erstellen Sie eine zweite Schnittstelle namens eth1 für das private Subnetz.



2. Die IP-Adresse, die Sie unter Ubuntu konfigurieren, ist die private Schnittstelle eth1, die von AWS zugewiesen wird.

```
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. Klappen Sie die Schnittstelle zu, oder starten Sie das virtuelle System neu.

```
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. Pingen Sie 8.8.8.8 für den Test. Stellen Sie sicher, dass die Route 8.8.8.8 für Schritt 7 hinzugefügt wurde.

```
ubuntu@ip-10-16-2-139:~$ route -n
Kernel IP routing table
```

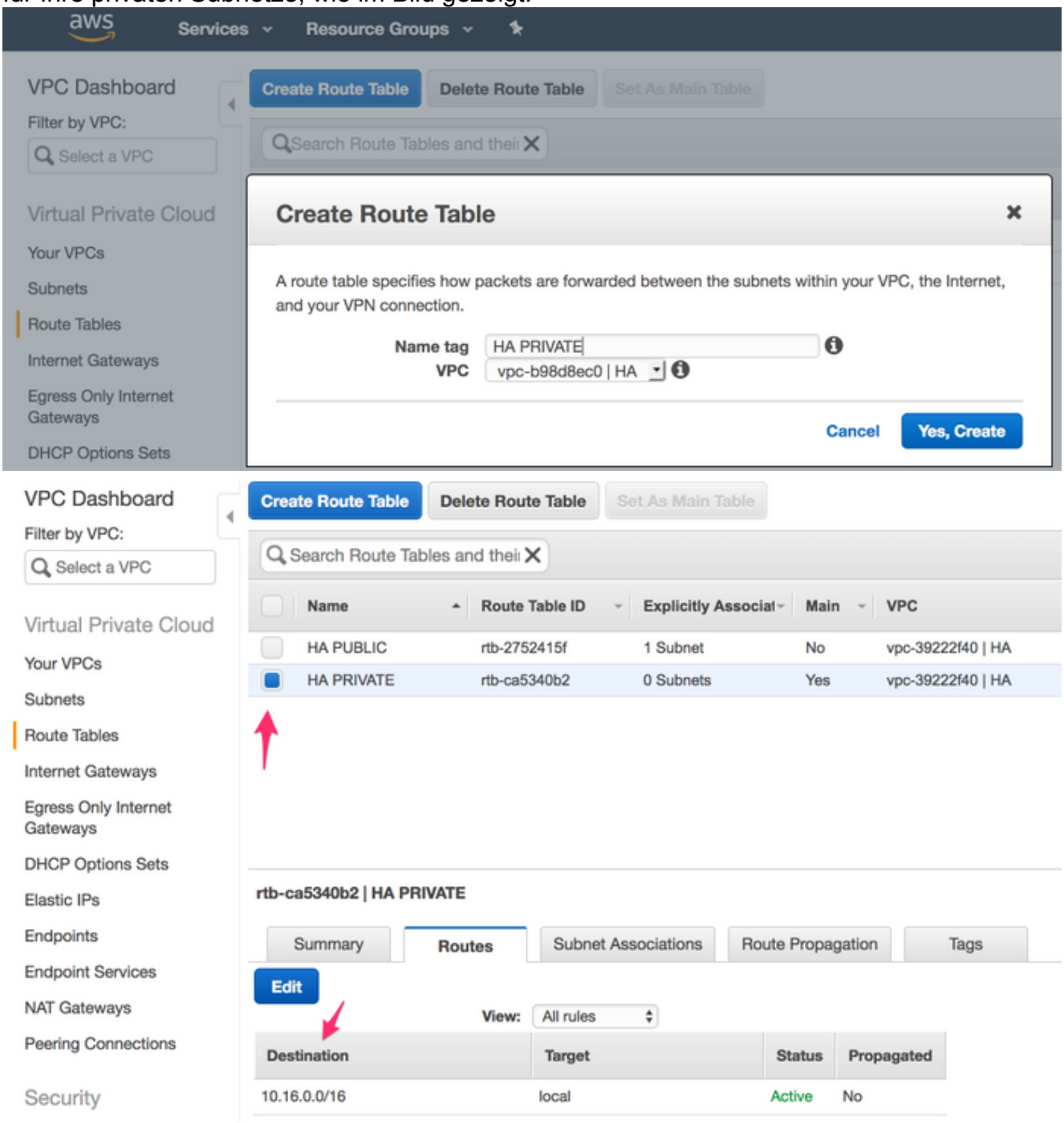
```
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.16.2.1 0.0.0.0 UG 0 0 0 eth0
8.8.8.8 10.16.6.1 255.255.255.255 UGH 0 0 0 eth1     <--------------
10.16.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.16.6.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
```

Wenn 8.8.8.8 nicht in der Tabelle aufgeführt ist, fügen Sie es manuell hinzu:

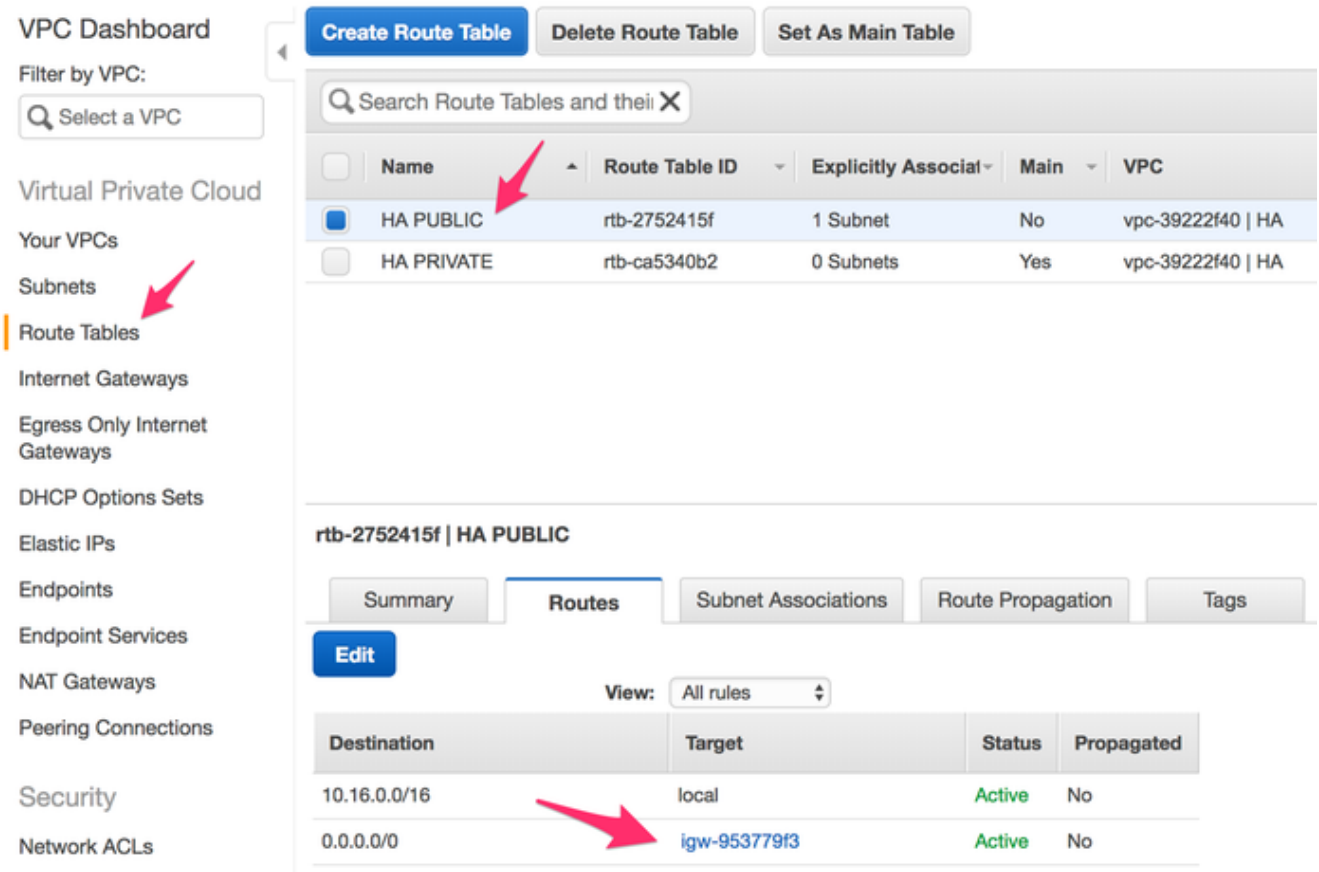
```
ubuntu@ip-10-16-2-139:~$ sudo route add -host 8.8.8.8 gw 10.16.6.1 dev eth1
```

Schritt 8: Konfigurieren der privaten und öffentlichen Routentabellen

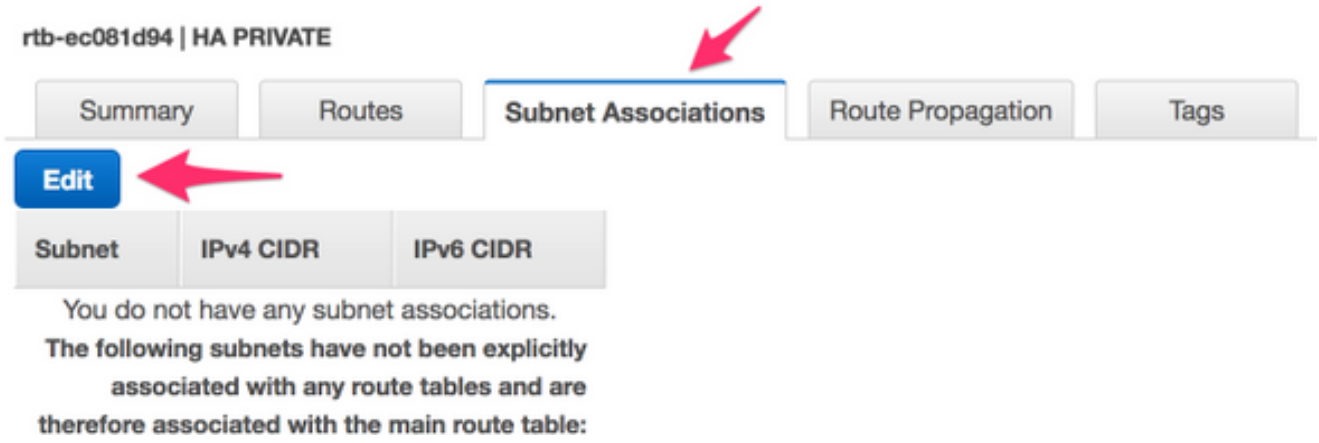
1. Wenn eine vPC durch den Assistenten in Schritt 2 erstellt wird, werden automatisch zwei Routing-Tabellen erstellt. Wenn es nur eine Routing-Tabelle gibt, erstellen Sie eine weitere für Ihre privaten Subnetze, wie im Bild gezeigt.



2. Hier sehen Sie die beiden Routing-Tabellen. An die PUBLIC Route Table wurde automatisch das Internet-Gateway (igw-95377973) angefügt. Bezeichnen Sie diese beiden Tabellen entsprechend. Die PRIVATE-Tabelle sollte NICHT diese Route haben.



3. Ordnen Sie alle 6 Subnetze der richtigen Routing-Tabelle zu. Der öffentlichen Weiterleitungstabelle sind drei öffentliche Schnittstellen zugeordnet:Öffentliche Subnetze: 10.16.0.0/24, 10.16.1.0/24, 10.16.2.0/24 Der Tabelle für private Routen sind drei private Schnittstellen zugeordnet:Private Subnetze: 10.16.4.0/24, 10.16.5.0/24, 10.16.6.0/24



Schritt 9: Konfigurieren Sie Network Address Translation (NAT) und GRE Tunnel mit BFD und einem beliebigen Routing-Protokoll.

Konfigurieren Sie den Generic Routing Encapsulation (GRE)-Tunnel über die elastischen IPs der CSR 1000vS (empfohlen, um Probleme mit der DHCP-Lease-Verlängerung zu vermeiden, die falsche Fehler erkennen). Die BFD-Werte (Biderection Forwarding Detection) können aggressiver konfiguriert werden als in diesem Beispiel, wenn schnellere Konvergenz erforderlich ist. Dies kann jedoch dazu führen, dass BFD-Peer-Down-Ereignisse bei einer unterbrochenen Verbindung auftreten. Die Werte in diesem Beispiel erkennen einen Peerfehler innerhalb von 1,5 Sekunden. Zwischen der Ausführung des AWS API-Befehls und dem Wirksamwerden der VPC-Routing-Tabelle liegt eine variable Verzögerung von etwa einigen Sekunden.

- Konfiguration auf CSRHA

  GRE und BFD - dienen zur Beobachtung der Bedingungen für einen HA-Failover

```
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 und Routing - für die Internetverbindung virtueller Systeme über die private Schnittstelle

```
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
```

- Konfiguration auf CSRHA1

  GRE und BFD - dienen zur Beobachtung der Bedingungen für einen HA-Failover

```
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 und Routing - für die Internetverbindung virtueller Systeme über die private Schnittstelle

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

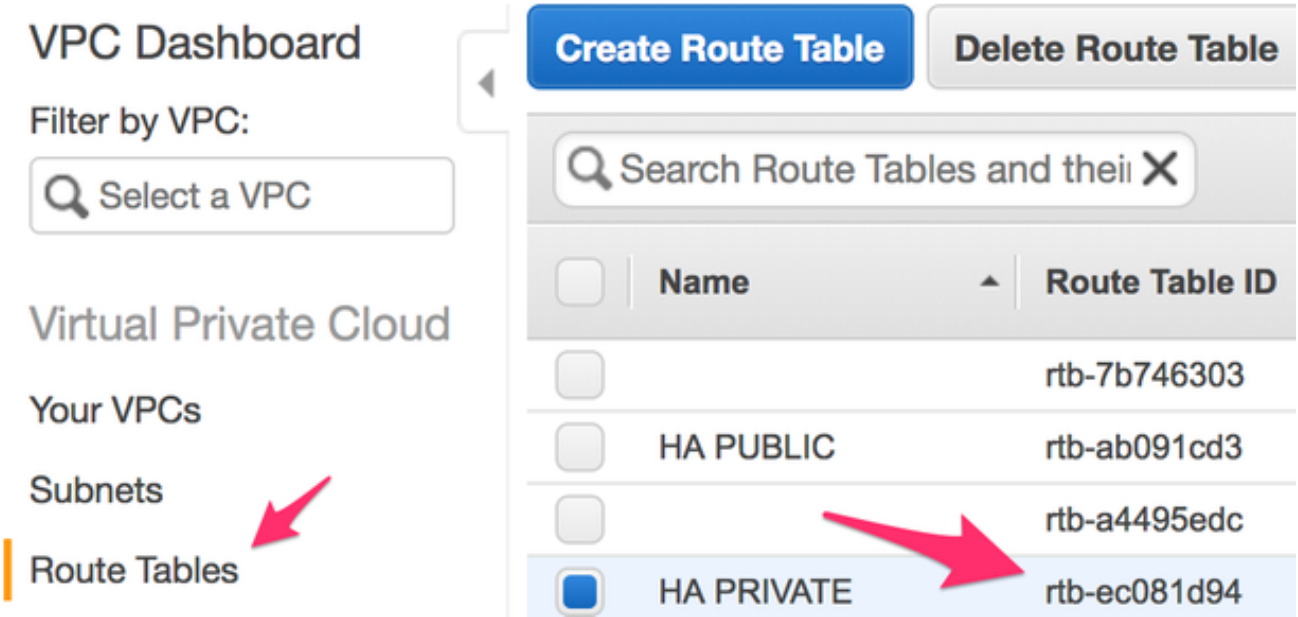
```
  no shutdown
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!
access-list 10 permit 10.16.6.0 0.0.0.255
!
ip route 10.16.6.0 255.255.255.0 GigabitEthernet2 10.16.5.1
```

Schritt 10: Konfigurieren der hohen Verfügbarkeit (Cisco IOS XE Denali 16.3.1a oder höher)

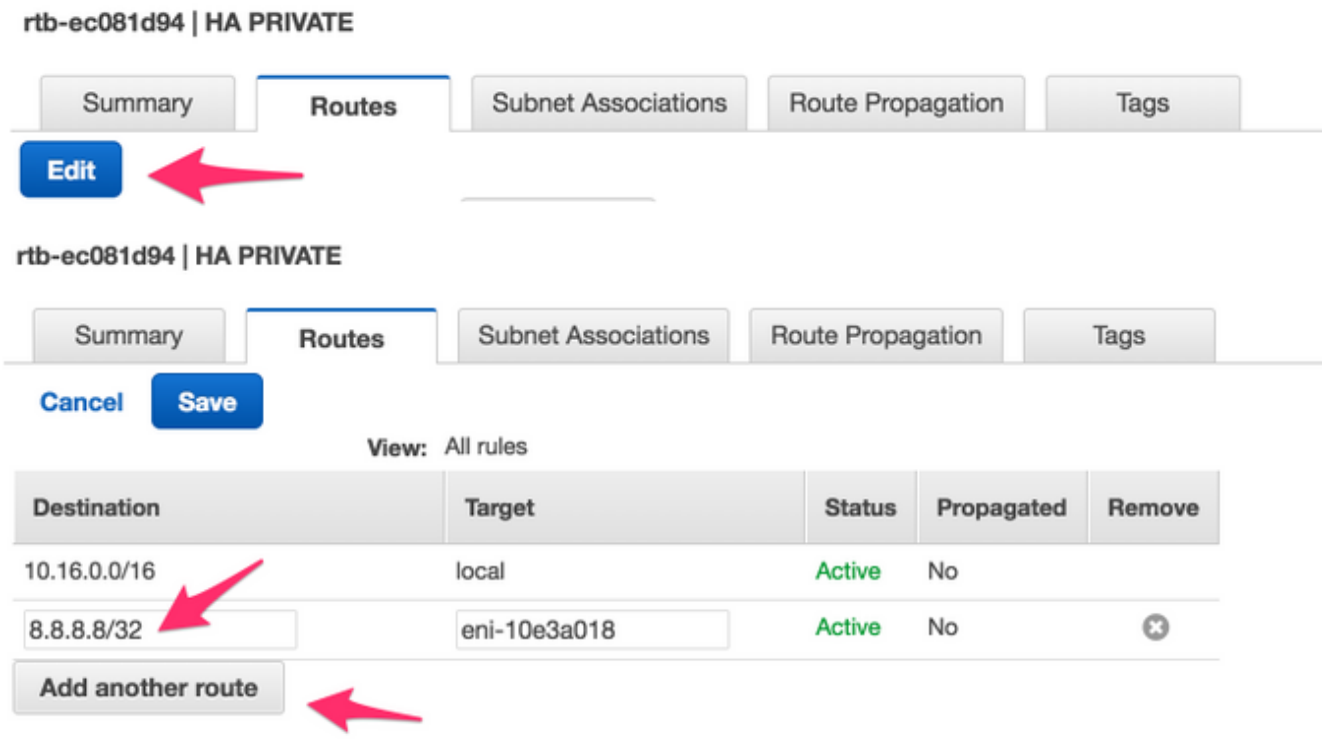
Überwachen Sie BFD-Peer-Down-Ereignisse, indem Sie jeden CSR 1000v mit dem unten angegebenen Befehl "cloud provider aws" konfigurieren. Verwenden Sie diesen Befehl, um die Routing-Änderungen an (VPC) Route-table-id, Network-interface-id und CIDR zu definieren, nachdem ein AWS HA-Fehler wie ein ausgefallener BFD-Peer erkannt wurde.

```
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
```

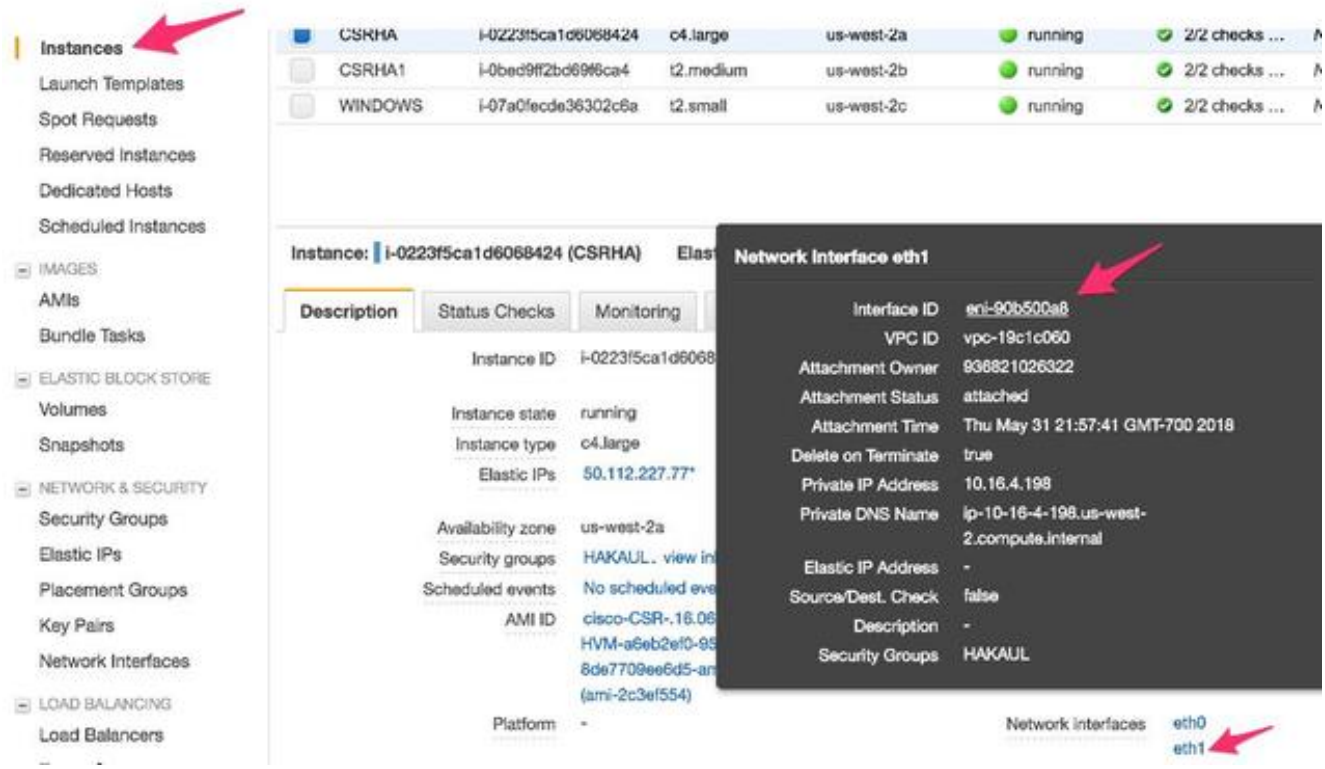
1. Die #bfd Peer-IP-Adresse ist die IP-Adresse des Peer-Tunnels.
   ```
   CSRHA#show bfd neighbors

   IPv4 Sessions
   NeighAddr LD/RD RH/RS State Int
   192.168.1.2 4097/4097 Up Up Tu1
   ```
2. Der Tabellenname #route-table befindet sich unter AWS console. Navigieren Sie zu **VPC > Route Tables**. Durch diese Aktion wird die private Routing-Tabelle geändert.



3. Die Zieladresse für die in der Routing-Tabelle zu aktualisierende Route wird mit dem Präfix #cidr ip ipadr/prefix angegeben. Navigieren Sie unter der AWS-Konsole zu **VPC > Routing-Tabellen**. Scrollen Sie nach unten, klicken Sie auf **Edit** und dann auf **Add another route**. Fügen Sie unsere Testzieladresse 8.8.8.8 und die private ENI von CSRHA hinzu.



4. Der Name #eni elastischer-network-intf befindet sich in Ihrer EC2-Instanz. Klicken Sie für jede der entsprechenden CSRs auf die Schnittstelle eth1, und verwenden Sie die Schnittstellen-ID.



5. Der Name #region ist der Codename im AWS-Dokument. Diese Liste kann sich ändern oder erweitern. Die neuesten Updates finden Sie im Dokument Amazon Region and Availability Zones.

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)

Redundanzkonfigurationsbeispiel für CSRHA

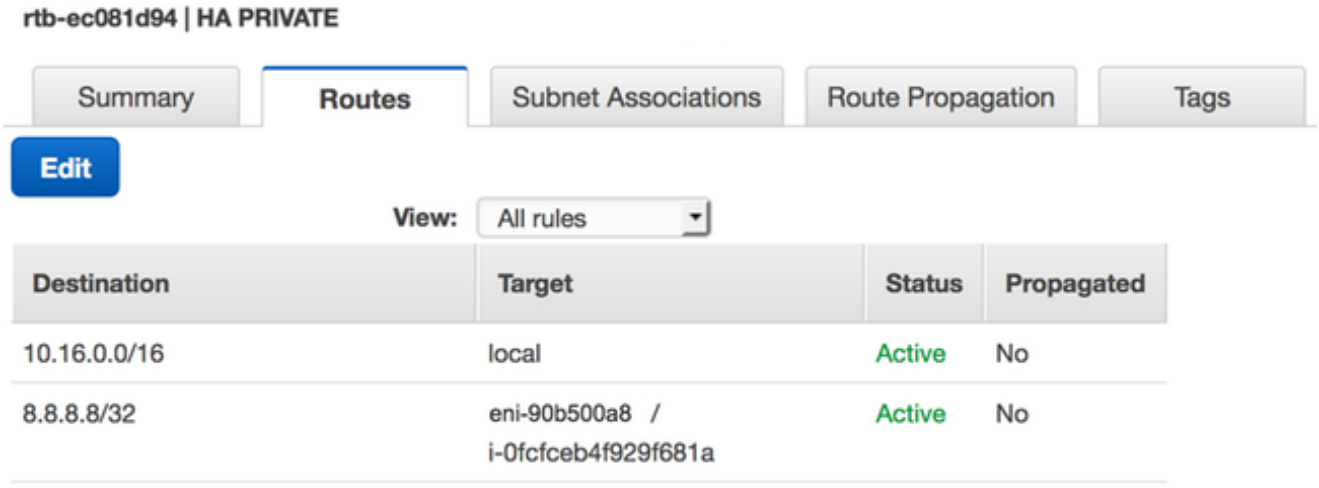
```
redundancy
cloud provider aws 1
  bfd peer 192.168.1.2
  route-table rtb-ec081d94
  cidr ip 8.8.8.8/32
  eni eni-90b500a8
  region us-west-2
```

Redundanzkonfigurationsbeispiel für CSRHA1

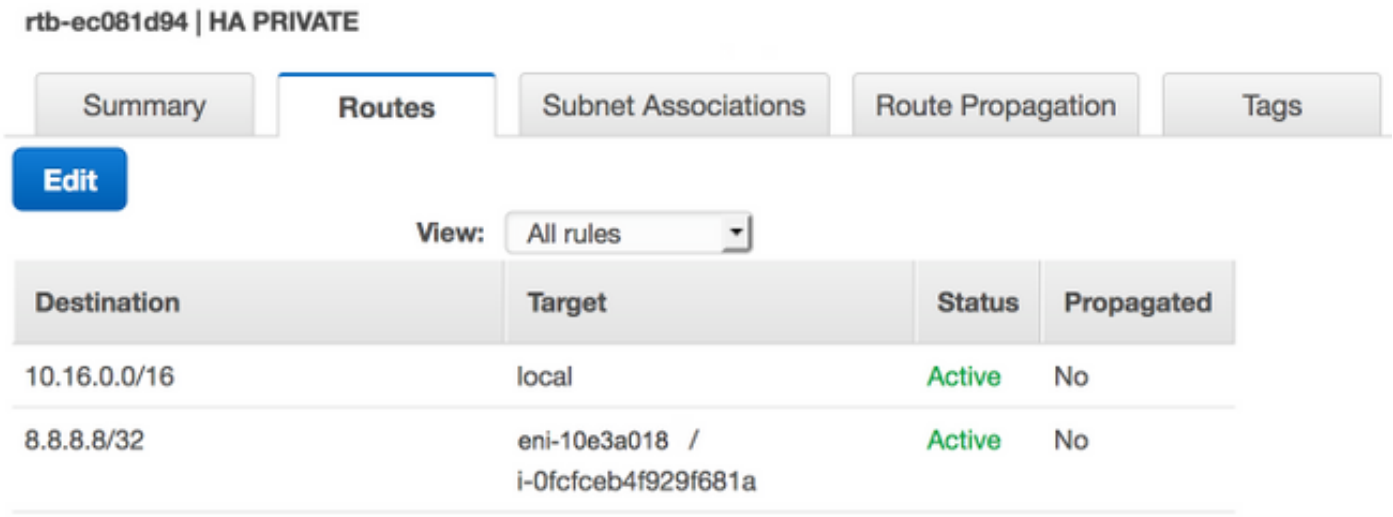
```
redundancy
cloud provider aws 1
  bfd peer 192.168.1.1
  route-table rtb-ec081d94
  cidr ip 8.8.8.8/32
  eni eni-10e3a018
  region us-west-2
```

Überprüfen der Hochverfügbarkeit

1. Überprüfung der BFD- und Cloud-Konfigurationen
```
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. Führen Sie einen kontinuierlichen Ping von der VM zum Ziel aus. Stellen Sie sicher, dass der Ping über die private eth1-Schnittstelle erfolgt.
```
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. Überprüfen Sie die Private Route Table. Das eni ist derzeit die private Schnittstelle von CSRHA, wo dies der Verkehr ist.



4. Fahren Sie Tunnel1 von CSRHA herunter, um ein HA-Failover zu simulieren.
```
CSRHA(config)#int Tun1
CSRHA(config-if)#shut
```
5. Beachten Sie, dass die Routing-Tabelle auf die neue ENI verweist, die die private Schnittstelle von CSRHA1 darstellt.



Fehlerbehebung

- Stellen Sie sicher, dass Ressourcen zugeordnet sind. Beim Erstellen von vPC, Subnetzen, Schnittstellen, Routing-Tabellen usw. werden viele dieser Elemente nicht automatisch miteinander verknüpft. Sie kennen sich nicht.
- Stellen Sie sicher, dass die elastische IP und jede private IP mit den richtigen Schnittstellen und Subnetzen verknüpft ist, der richtigen Routentabelle hinzugefügt, mit dem richtigen Router und der richtigen VPC und Zone verbunden und mit der IAM-Rolle und den Sicherheitsgruppen verknüpft ist.
- Deaktivierung der Quell-/Zielprüfung per ENI.
- Für Cisco IOS XE 16.3.1a oder höher sind diese zusätzlichen Verifizierungsbefehle verfügbar.

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

- Häufige Fehler bei Debugging-Vorgängen:

Problem: httpc_send_request fehlgeschlagen

Auflösung: HTTP wird verwendet, um den API-Aufruf vom CSR an AWS zu senden. Stellen Sie sicher, dass DNS den in Ihrer Instanz aufgelisteten DNS-Namen auflösen kann. Stellen Sie sicher, dass der HTTP-Verkehr nicht blockiert wird.

```
*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
```

Problem: Routing-Tabelle rtb-9c000f4 und Schnittstelle eni-32791318 gehören zu verschiedenen Netzwerken

Auflösung: Regionsname und ENI sind in verschiedenen Netzwerken falsch konfiguriert. Region und ENI sollten sich in derselben Zone wie der Router befinden.

```
*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>
```

Problem: Sie sind nicht autorisiert, diesen Vorgang auszuführen. Verschlüsselte Autorisierungsfehlermeldung.

Auflösung: IAM JSON-Rolle/-Richtlinie falsch erstellt oder nicht auf CSR angewendet Die IAM-Rolle autorisiert den CSR zum Durchführen von API-Aufrufen.

```
*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>
```

Zugehörige Informationen

- Redundante VPC-Gateways - Cisco
- Bereitstellungsleitfaden für Cisco CSR 1000v Cloud Services Router für Amazon Web Services
- Instanztypen-Aufschlüsselung
- EC2 und VPC
- Elastische Netzwerkschnittstellen gemäß EC2-Benutzerhandbuch enthalten die Anzahl der ENIs pro Instanztyp.
- Anleitungen für erweiterte Netzwerkfunktionen unter Linux, nützliche Hintergrundinformationen
- Dedizierte Instanzen/Tenancy Erläuterung und Anleitung
- Allgemeine EC2-Dokumentation
- Allgemeine VPC-Dokumentation
- Regionen und Verfügbarkeitsbereiche
- CSR1000v Hochverfügbarkeit Version 3

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.