Bereitstellung einer hochverfügbaren C800v-Konfiguration auf AWS

Inhalt

Einleitung

In diesem Dokument wird die Einrichtung einer Hochverfügbarkeitsumgebung mit Catalyst 8000v-Routern in der Amazon Web Services Cloud beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Vorkenntnisse in den folgenden Themen verfügen:

- Allgemeine Kenntnisse der AWS-Konsole und ihrer Komponenten
- Grundlegendes zur Cisco IOS® XE Software
- Grundkenntnisse der HA-Funktion

Verwendete Komponenten

Für dieses Konfigurationsbeispiel sind die folgenden Komponenten erforderlich:

- Ein Amazon AWS-Konto mit Administratorrolle
- Zwei C8000v-Geräte mit Cisco IOS® XE 17.15.3a und 1 Ubuntu 22.04 LTS VM AMIs in derselben Region

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 kennen.

Topologie

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 - C8000v-Router (Cisco IOS® XEDenali 17.15.3a)
- 1x - VM (Linux/Windows)

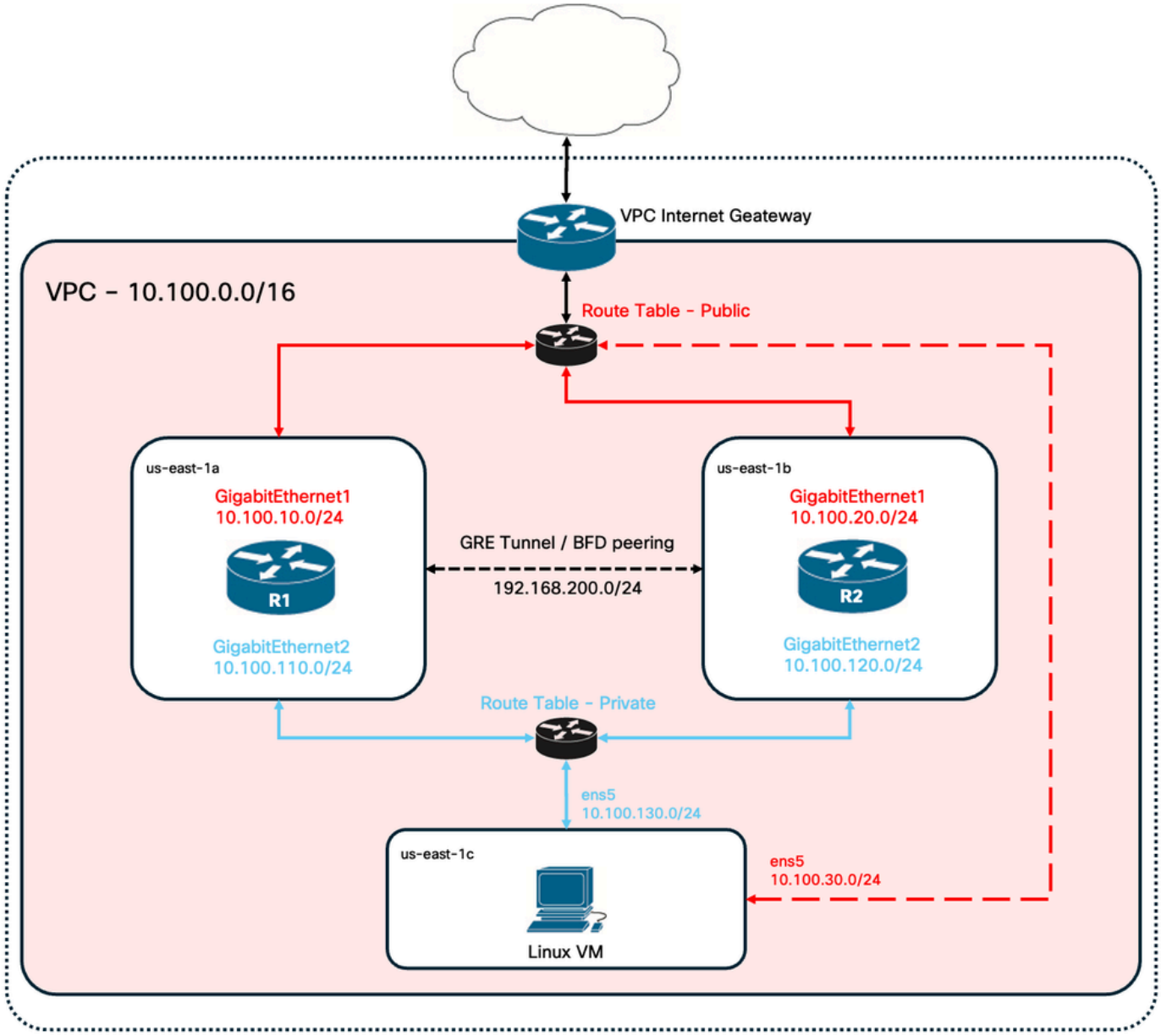
Ein HA-Paar verfügt über 2 C8000v-Router in zwei verschiedenen Verfügbarkeitszonen. Betrachten Sie jede Verfügbarkeitszone als separates Rechenzentrum für zusätzliche Hardware-Ausfallsicherheit.

Die dritte Zone ist eine VM, die ein Gerät in einem privaten Rechenzentrum simuliert. Derzeit wird der Internetzugriff über die öffentliche Schnittstelle aktiviert, sodass Sie auf das virtuelle System

zugreifen und es konfigurieren können. Generell muss der gesamte normale Datenverkehr die private Routing-Tabelle durchlaufen.

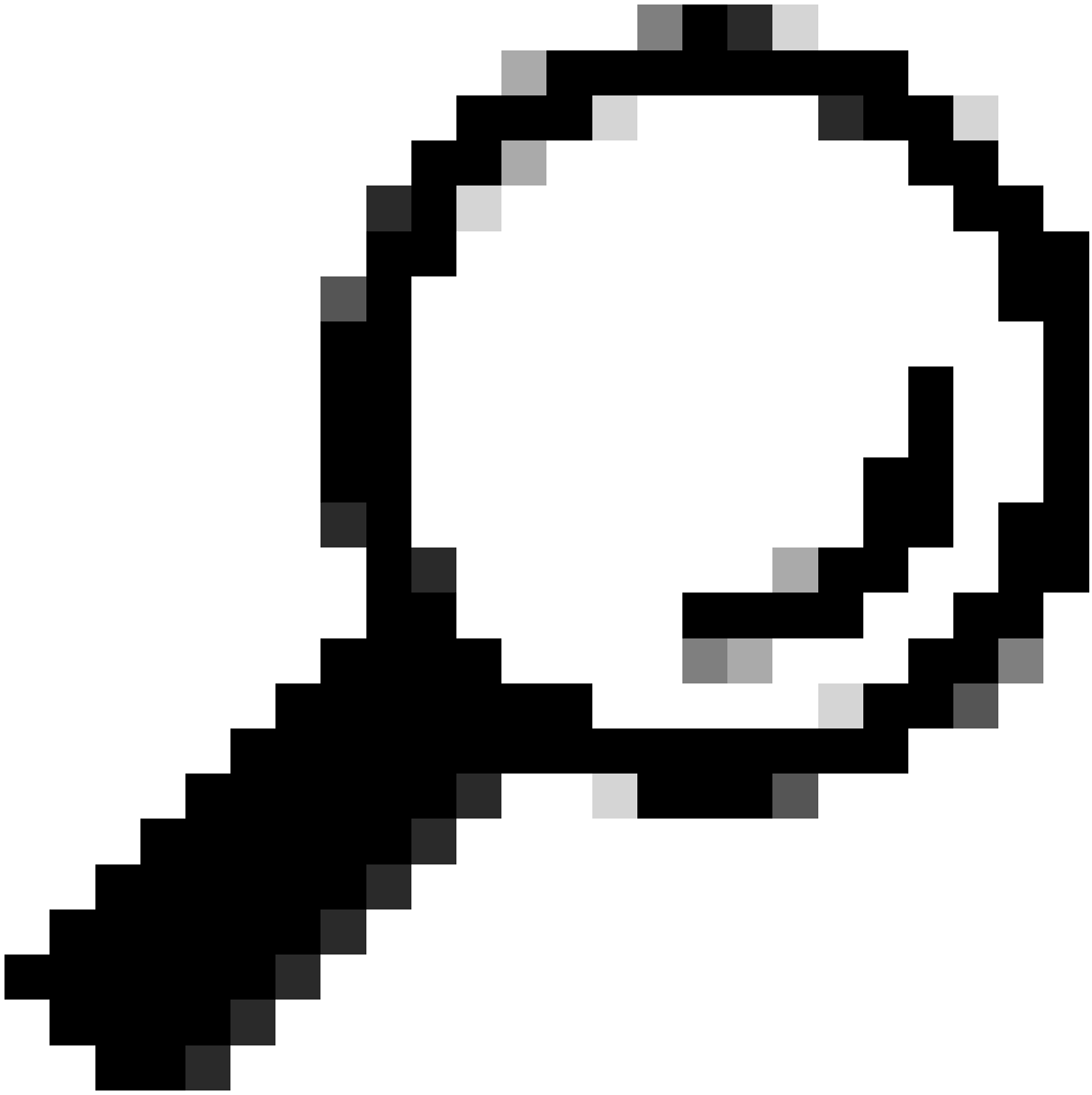
Um den Datenverkehr zu simulieren, initiieren Sie einen Ping von der privaten Schnittstelle des virtuellen Systems, der die private Routing-Tabelle über R1 durchläuft, um 8.8.8.8 zu erreichen. Stellen Sie bei einem Failover sicher, dass die private Routing-Tabelle automatisch aktualisiert wurde, um den Datenverkehr über die private Schnittstelle des R2-Routers weiterzuleiten.

Netzwerkdiagramm



Tabellenübersicht

Um die Topologie zusammenzufassen, sehen Sie hier die Tabelle mit den wichtigsten Werten aus den einzelnen Komponenten der Übung. Die Informationen in dieser Tabelle gelten ausschließlich für diese Übung.



Tipp: Mithilfe dieser Tabelle können Sie sich einen klaren Überblick über die wichtigsten Variablen im Leitfaden verschaffen. Es wird empfohlen, die Informationen in diesem Format zu sammeln, um den Prozess zu optimieren.

"Slot0:"	Verfügbarkeitszone	Schnittstellen	IP-Adressen	RTB	ENI
R1	US-Ost-1a	GigabitEthernet1	10.100.10.254	rtb-0d0e48f25c9b00635 (öffentlich)	eni-0645a881c13823696
		GigabitEthernet2	10.100.110.254	rtb-093df10a4de426eb8 (privat)	eni-070e14fbfde0d8e3b
R2	us-east-1b	GigabitEthernet1	10.100.20.254	rtb-0d0e48f25c9b00635 (öffentlich)	eni-0a7817922ffbb317b

		GigabitEthernet2	10.100.120.254	rtb-093df10a4de426eb8 (privat)	eni-0239fda341b4d7e41
Linux-VM	US-Ost-1c	DE5	10.100.30.254	rtb-0d0e48f25c9b00635 (öffentlich)	eni-0b28560781b3435b1
		n6	10.100.130.254	rtb-093df10a4de426eb8 (privat)	eni-05d025e88b6355808

Einschränkungen

- Verwenden Sie in einem erstellten Subnetz nicht die erste verfügbare Adresse dieses Subnetzes. Diese IP-Adressen werden von den AWS-Diensten intern verwendet.
- Konfigurieren Sie nicht die öffentlichen Schnittstellen der C8000v-Geräte innerhalb einer VRF-Instanz. HA funktioniert nicht ordnungsgemäß, wenn dieser Parameter festgelegt ist.

Konfiguration

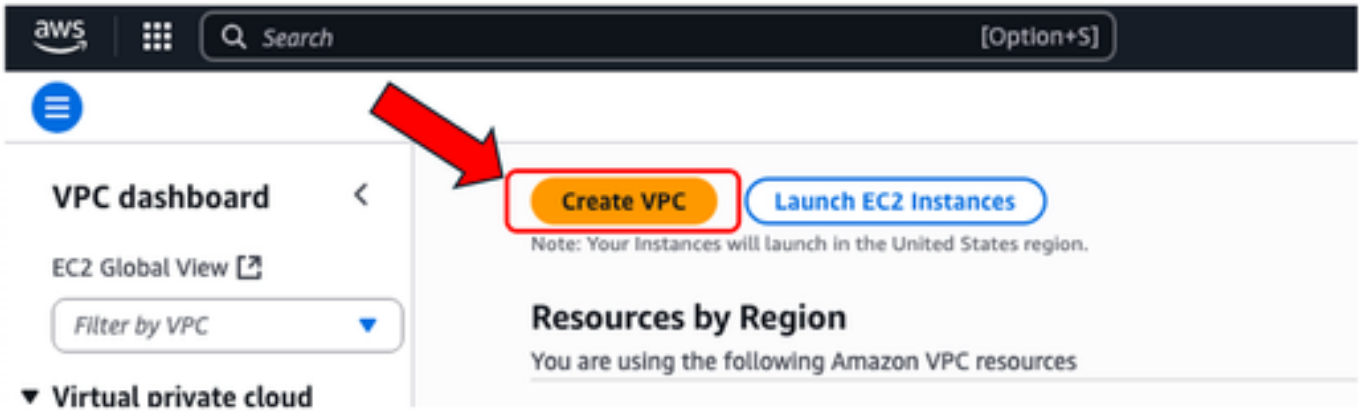
Der allgemeine Konfigurationsablauf konzentriert sich darauf, die angeforderten VMs in der richtigen Region zu erstellen und Sie zur spezifischsten Konfiguration zu bewegen, z. B. zu Routen und Schnittstellen für jede von ihnen. Es wird jedoch empfohlen, die Topologie zuerst zu verstehen und sie in der gewünschten Reihenfolge zu konfigurieren.

Schritt 1: Wählen Sie eine Region

Für diesen Bereitstellungsleitfaden wird die Region West (North Virginia) - us-east-1 als VPC-Region ausgewählt.

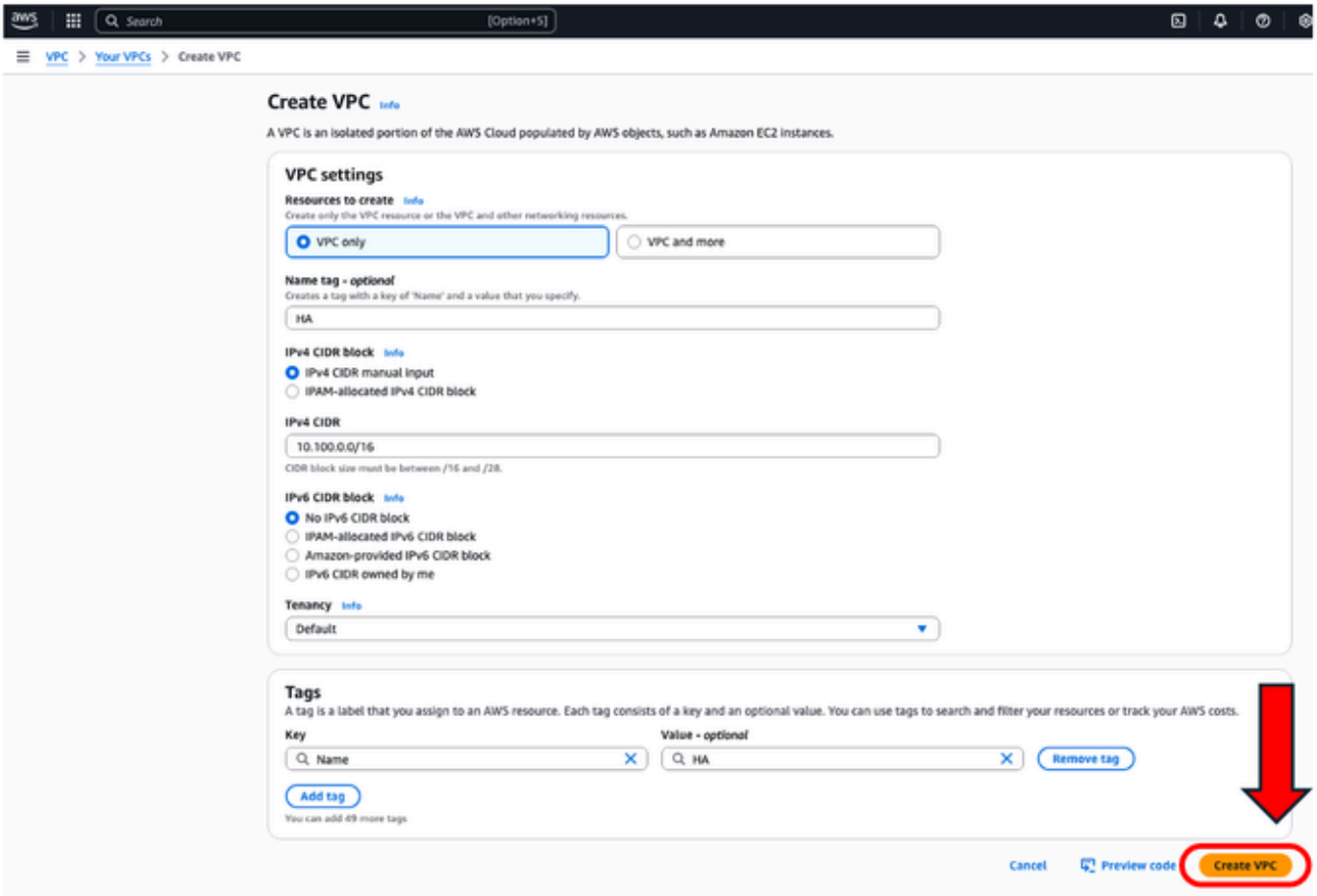
Schritt 2: Erstellen der vPC

Navigieren Sie in der AWS-Konsole zu VPC > VPC Dashboard > Create VPC (VPC erstellen).

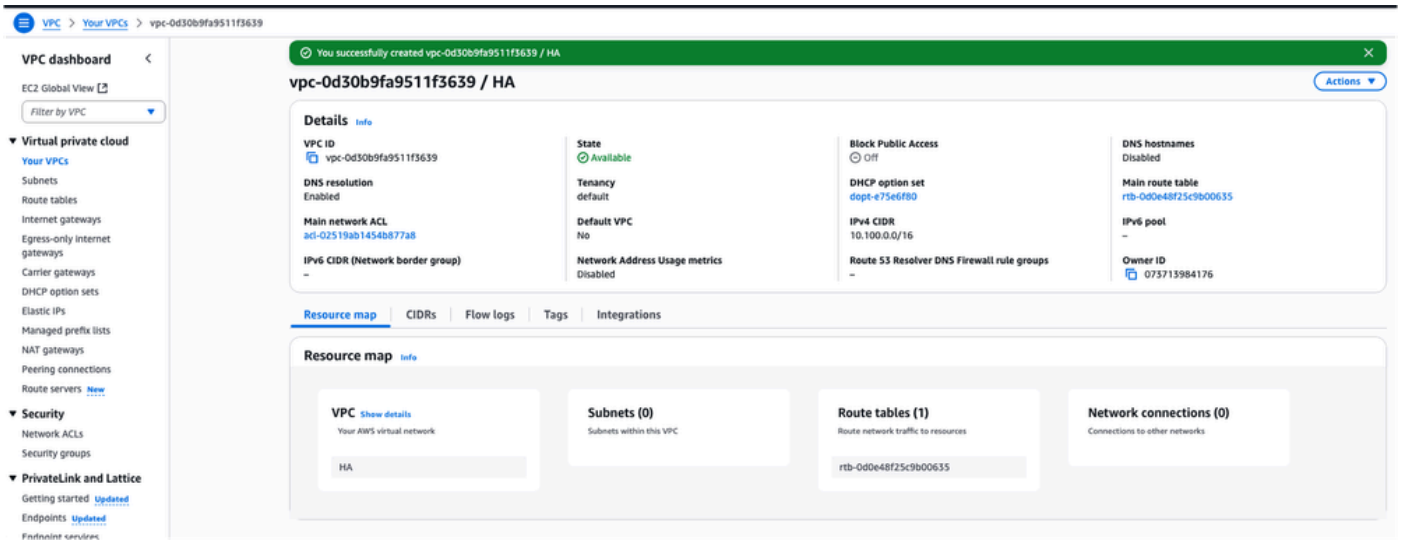


Wenn Sie die VPC erstellen, wählen Sie die Option Nur VPC. Sie können ein /16-Netzwerk für die gewünschte Verwendung zuweisen.

In diesem Bereitstellungsleitfaden wird das Netzwerk 10.100.0.0/16 wie folgt ausgewählt:

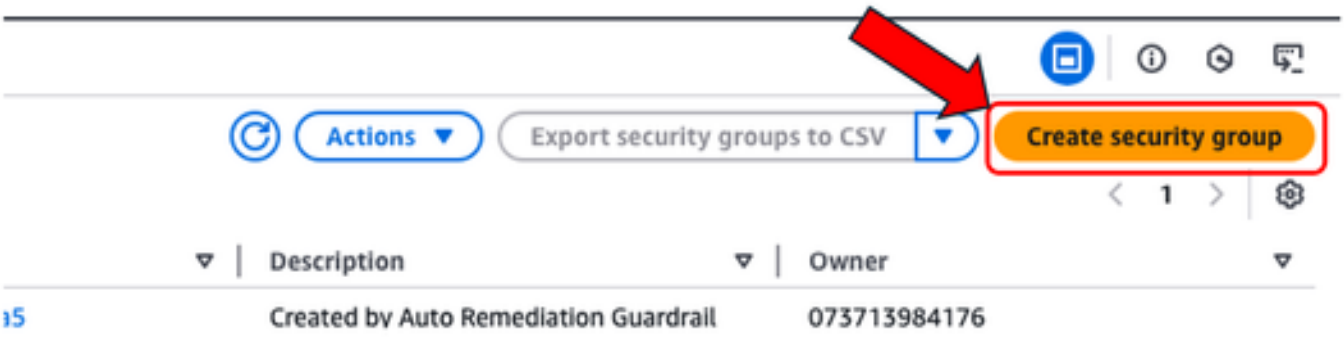


Nachdem Sie auf Create VPC (VPC erstellen) geklickt haben, wird das VPC-0d30b9fa9511f3639 mit dem HA-Tag erstellt:

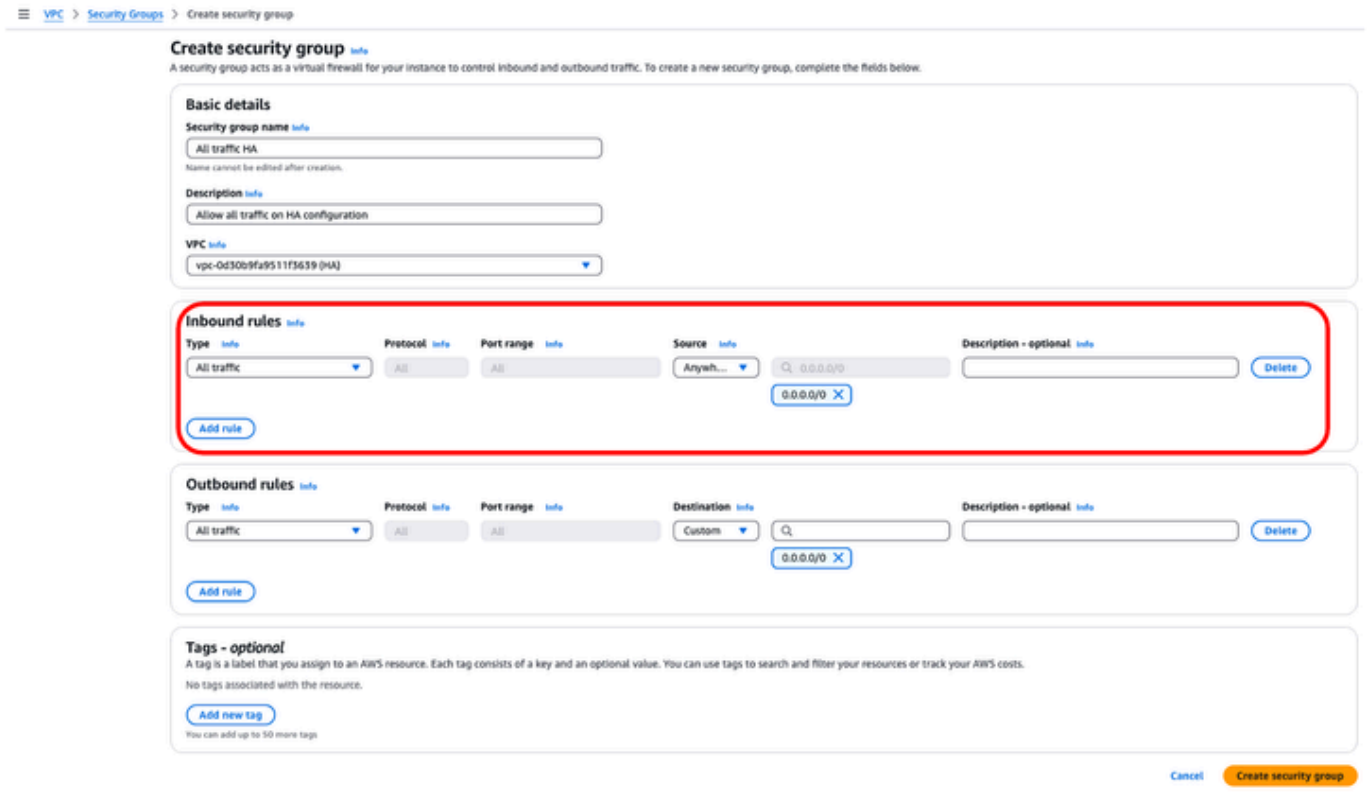


Schritt 3: Erstellen einer Sicherheitsgruppe für die vPC

In AWS funktionieren Sicherheitsgruppen wie ACLs und erlauben oder verweigern den Datenverkehr zu konfigurierten VMs innerhalb einer VPC. Navigieren Sie in der AWS-Konsole zu VPC > VPC Dashboard > Sicherheit > Sicherheitsgruppen, und klicken Sie auf Sicherheitsgruppe erstellen.



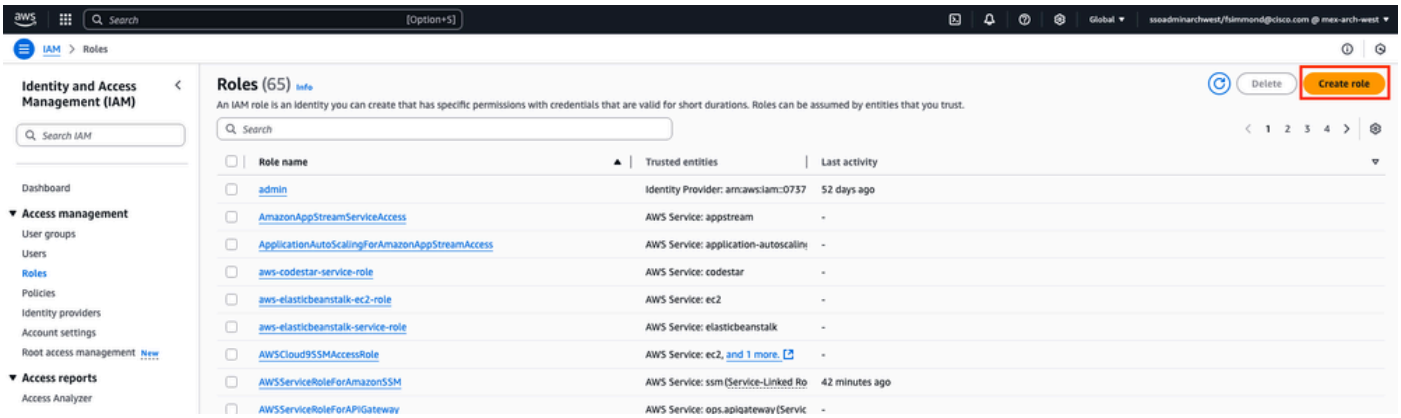
Legen Sie unter Inbound Rules (Eingehende Regeln) fest, welchen Datenverkehr Sie zulassen möchten. In diesem Beispiel wird Gesamter Datenverkehr mithilfe des Netzwerks 0.0.0.0/0 ausgewählt.



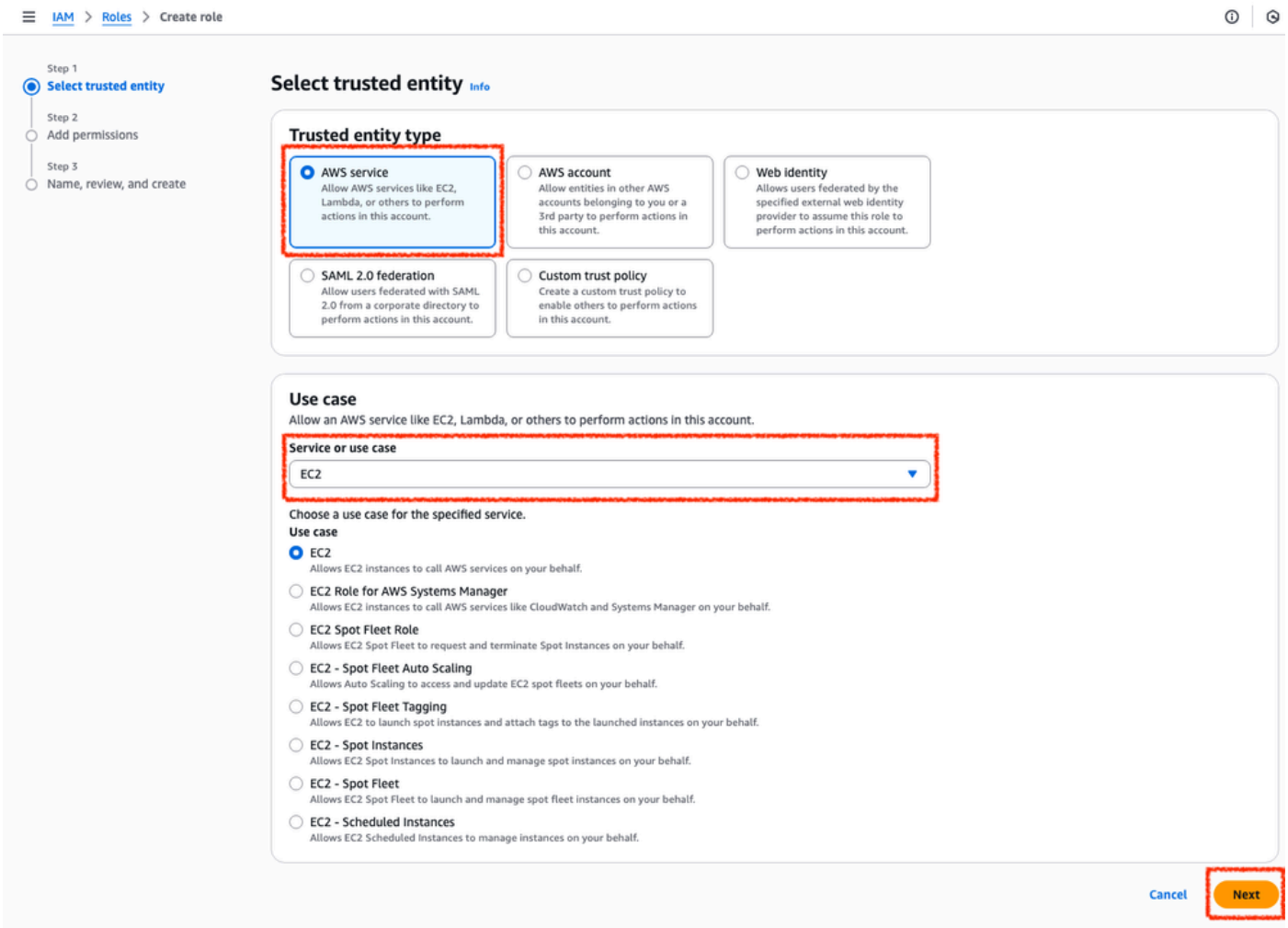
Schritt 4: Erstellen einer IAM-Rolle mit einer Richtlinie und Zuordnen zum VPC

IAM gewährt Ihren AMIs den erforderlichen Zugriff auf Amazon-APIs. Der C8000v wird als Proxy für den Aufruf von AWS API-Befehlen verwendet, um die Routing-Tabelle in AWS zu ändern. Standardmäßig haben EC2-Instanzen keinen Zugriff auf APIs. Aus diesem Grund muss eine neue IAM-Rolle erstellt werden, die bei der Erstellung von AMI angewendet wird.

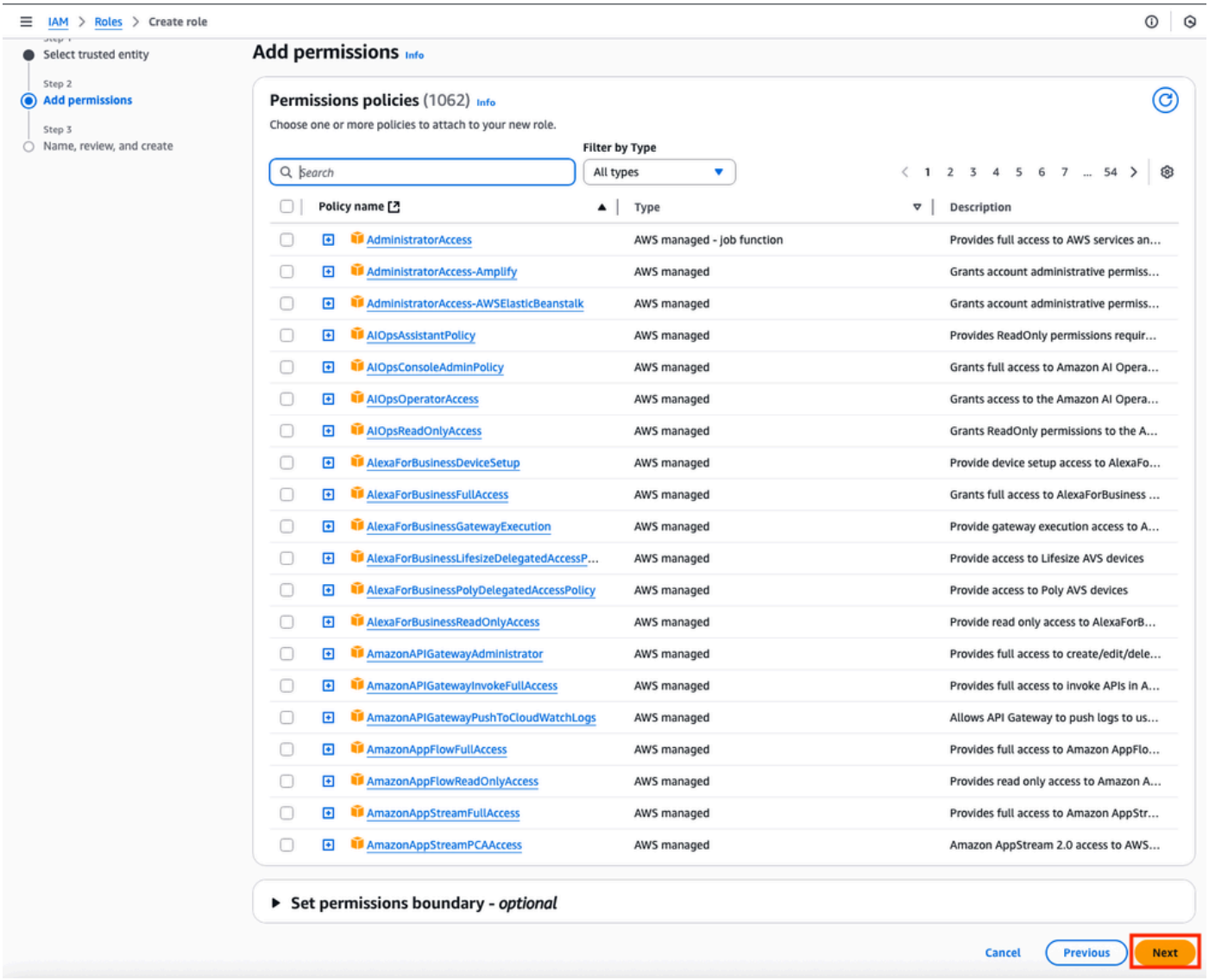
Navigieren Sie zum IAM-Dashboard, und navigieren Sie zu Access Management > Roles > Create Role (Zugriffsverwaltung > Rollen > Rolle erstellen). Dieser Prozess besteht aus drei Schritten:



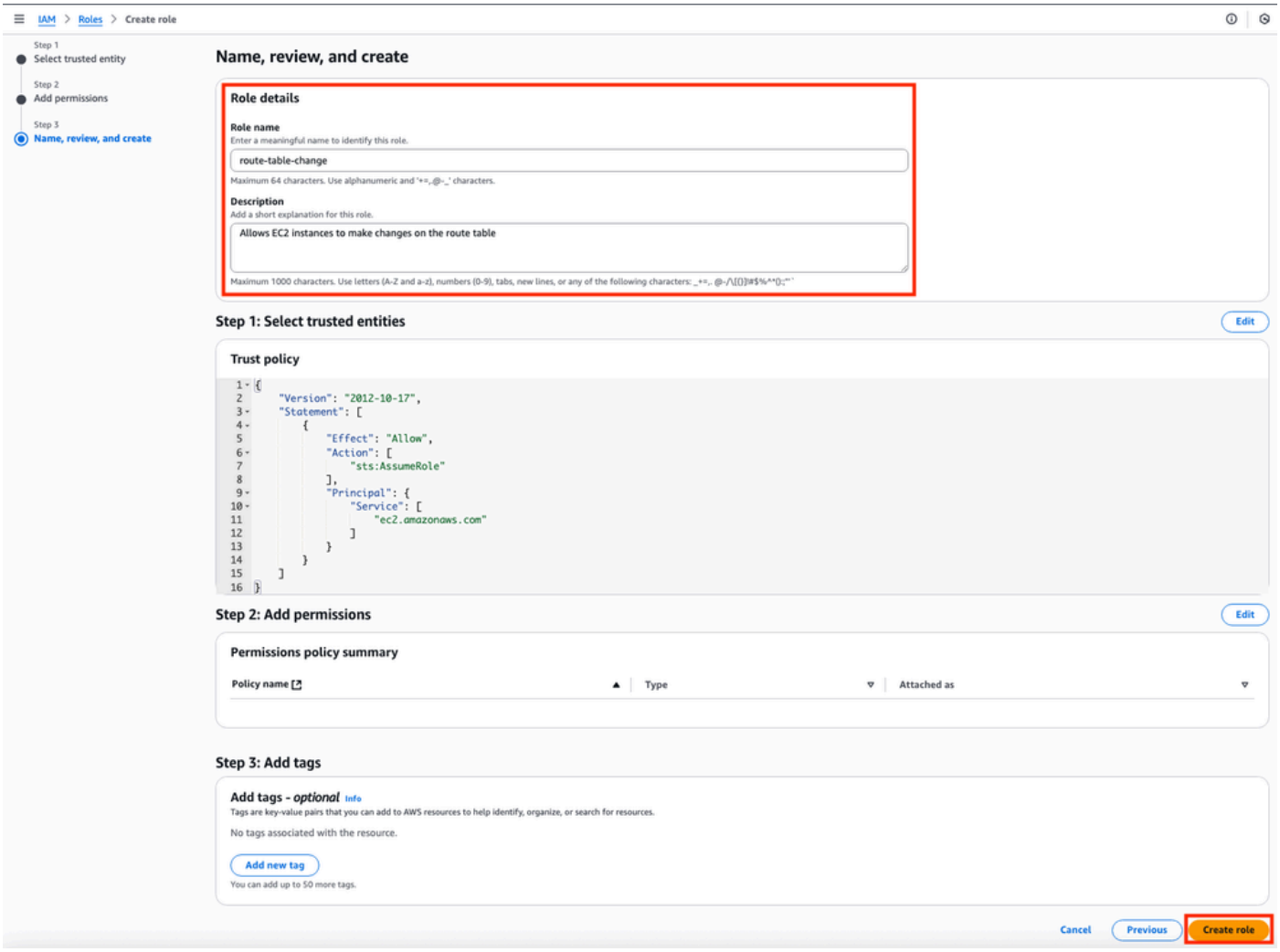
Wählen Sie zunächst die Option AWS-Dienst im Abschnitt Vertrauenswürdiger Entitätstyp und EC2 als den dieser Richtlinie zugewiesenen Dienst aus.



Wenn Sie fertig sind, klicken Sie auf Weiter:

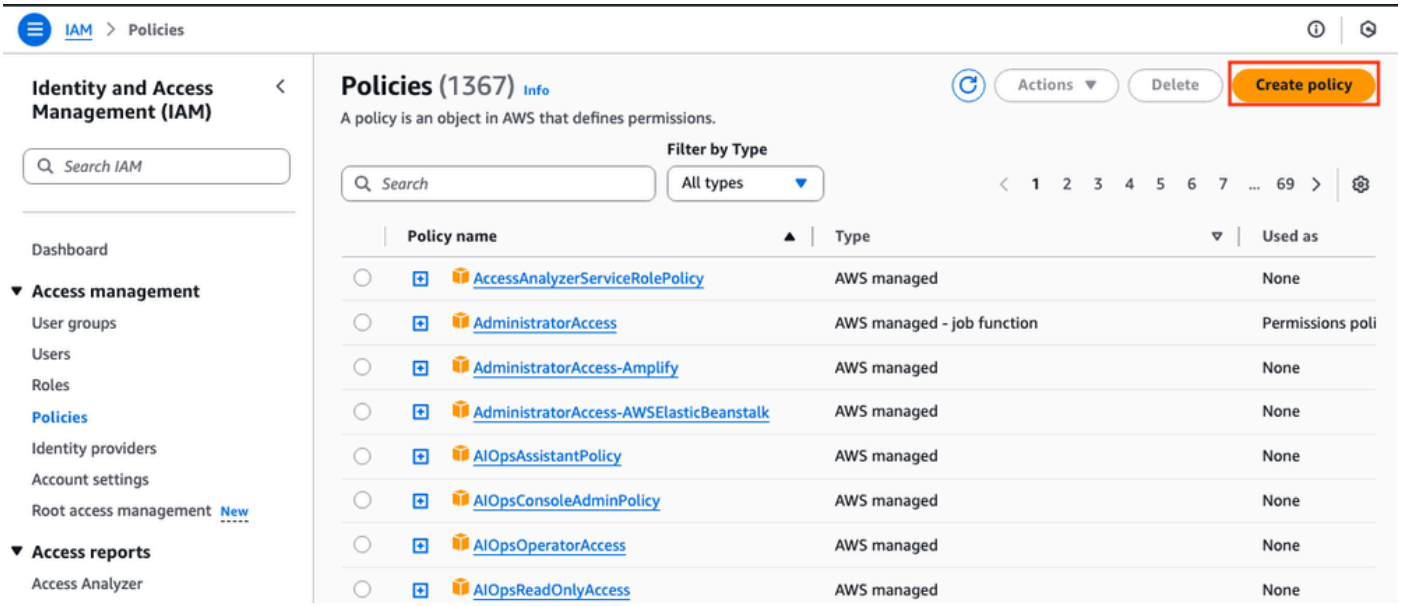


Legen Sie abschließend den Rollennamen fest, und klicken Sie auf die Schaltfläche Rolle erstellen.

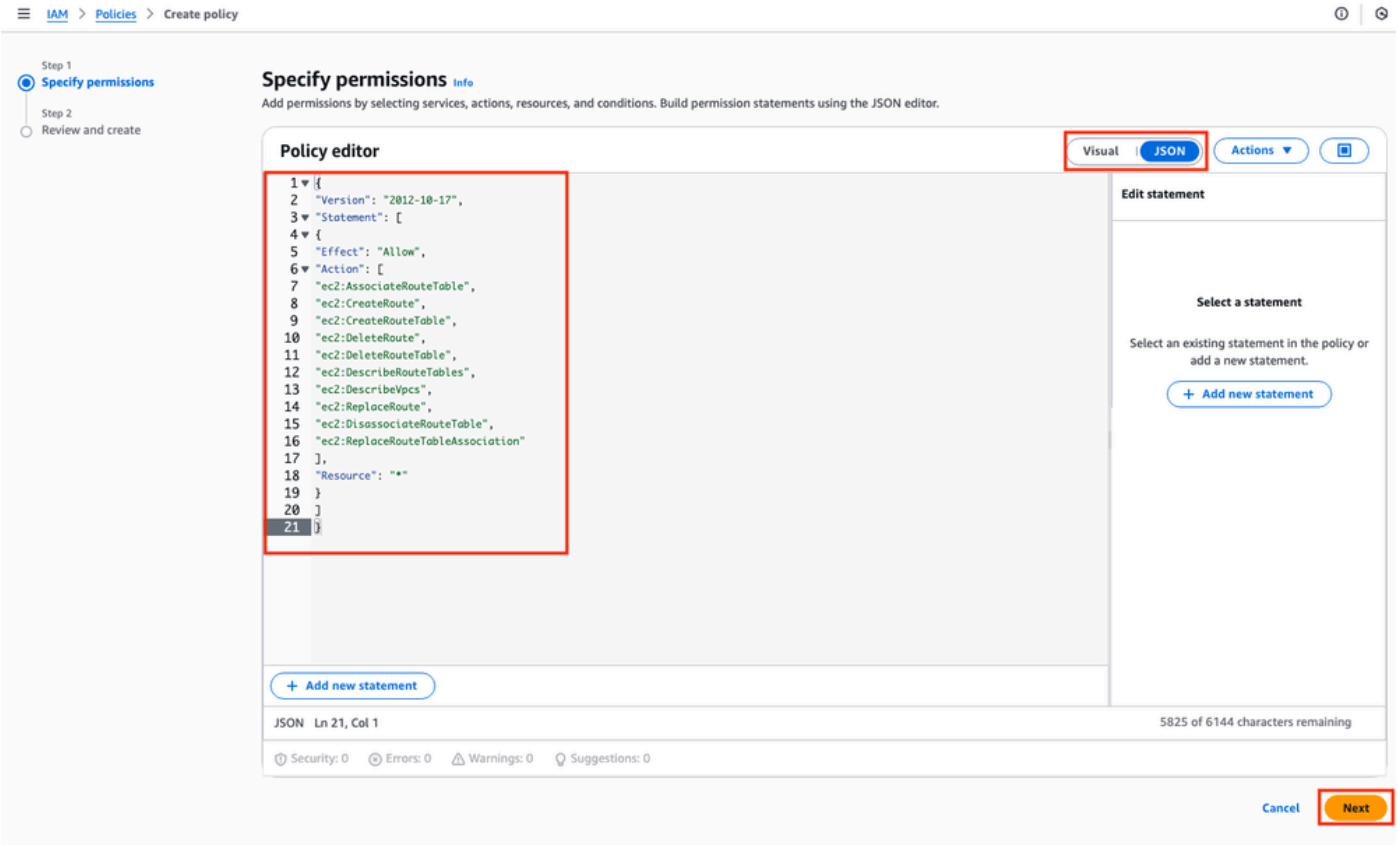


Schritt 5: Erstellen einer Vertrauensrichtlinie und Anhängen an eine IAM-Rolle

Nachdem die Rolle erstellt wurde, muss eine Vertrauensrichtlinie erstellt werden, um die Fähigkeit zum Ändern der AWS-Routing-Tabellen zu erlangen, wenn erforderlich. Wechseln Sie zum Abschnitt Richtlinien im IAM-Dashboard. Klicken Sie auf die Schaltfläche Richtlinie erstellen. Dieser Prozess umfasst zwei Schritte:



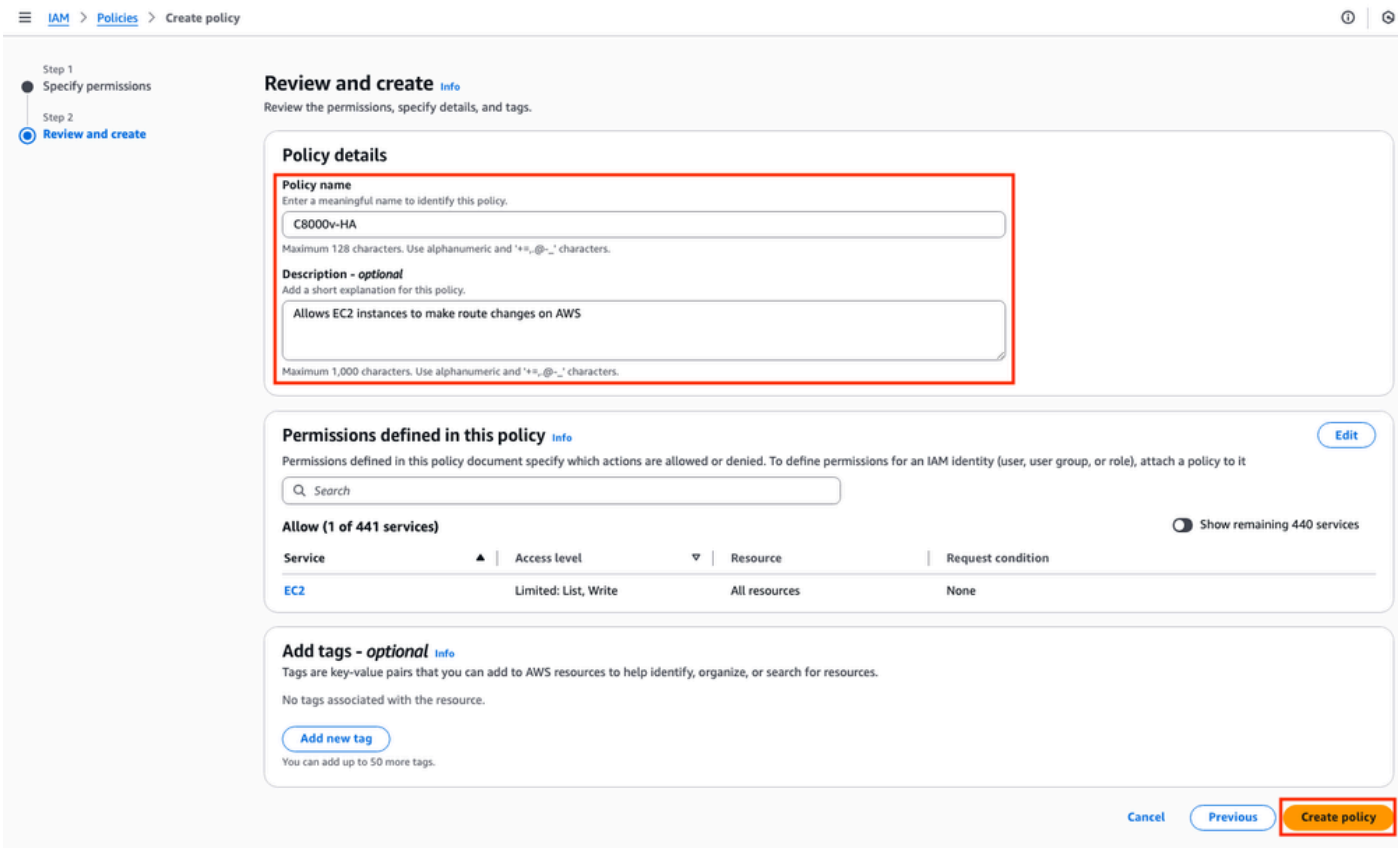
Stellen Sie zunächst sicher, dass der Richtlinien-Editor JSON verwendet, und wenden Sie die unten aufgeführten Befehle an. Klicken Sie nach der Konfiguration auf Weiter:



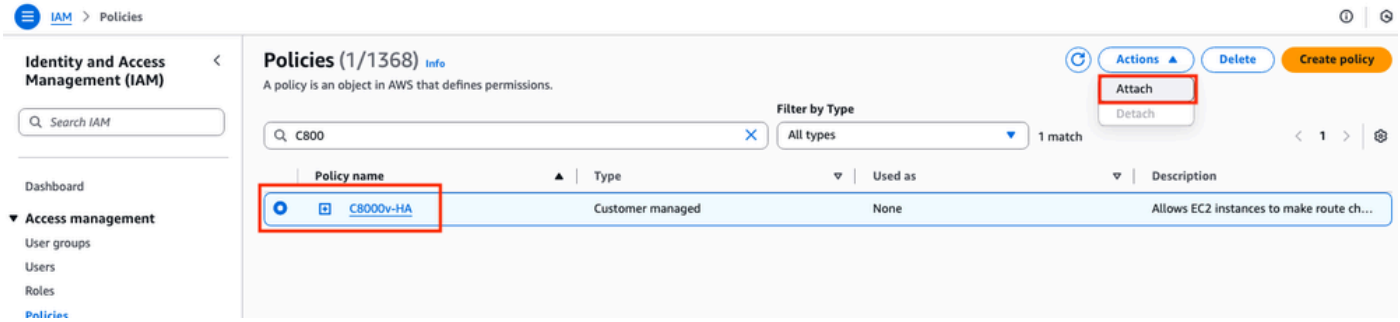
Dies ist der im Bild verwendete Textcode:

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

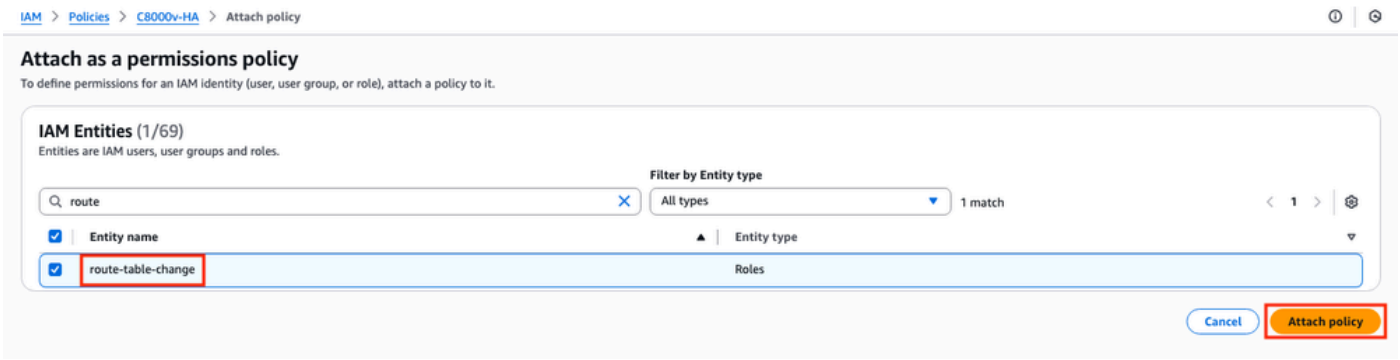
Legen Sie später den Richtliniennamen fest, und klicken Sie auf Richtlinie erstellen.



Sobald die Richtlinie erstellt wurde, filtern Sie die Richtlinie, und wählen Sie sie aus. Klicken Sie dann im Dropdown-Menü "Aktionen" auf die Option Anfügen.



Ein neues Fenster wird geöffnet. Filtern Sie im Abschnitt "IAM Entities" (IAM-Entitäten) die erstellte IAM-Rolle, und klicken Sie auf Attach policy (Richtlinie anhängen).

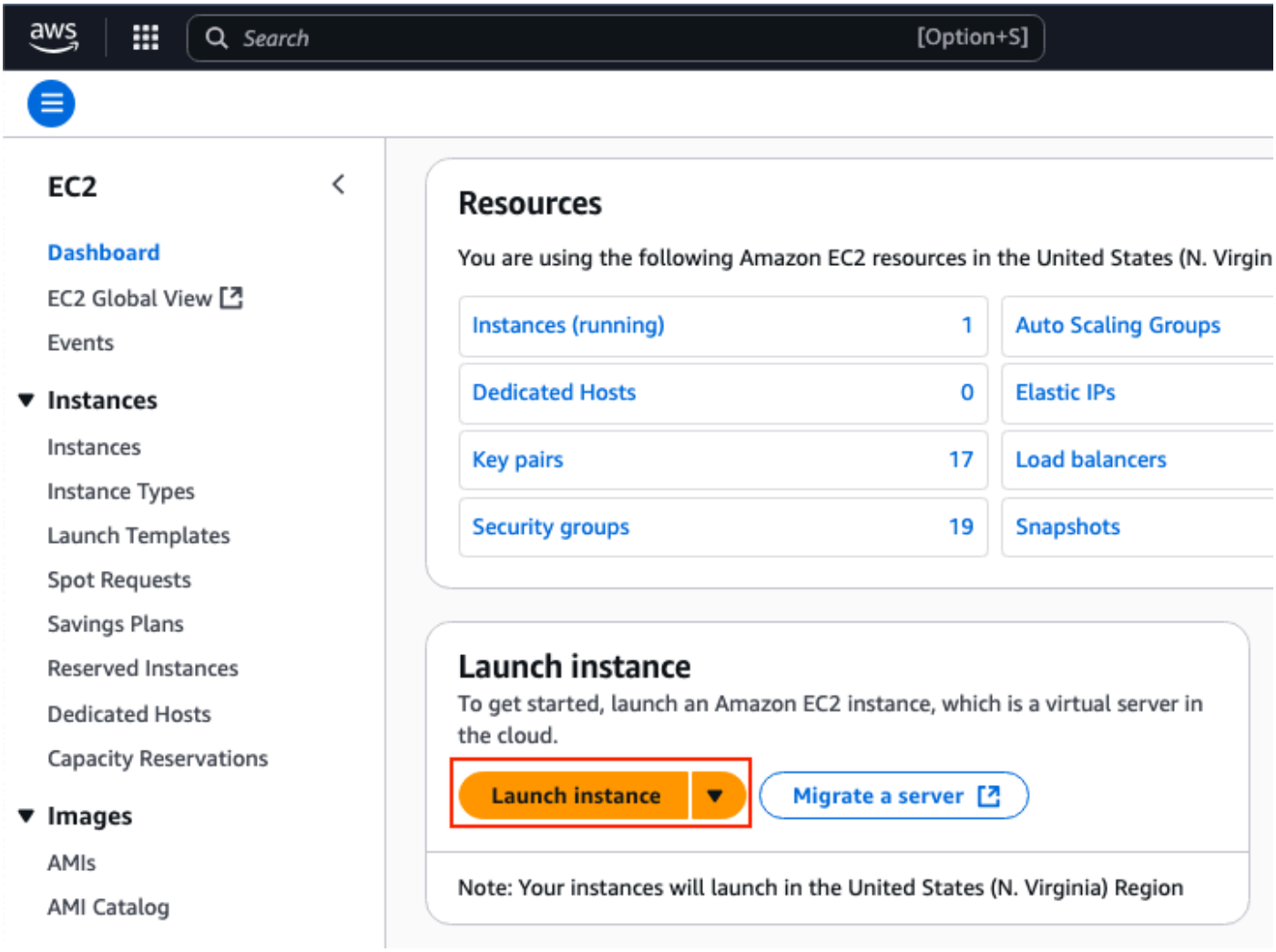


Schritt 6:Konfigurieren und Starten der C8000v-Instanzen

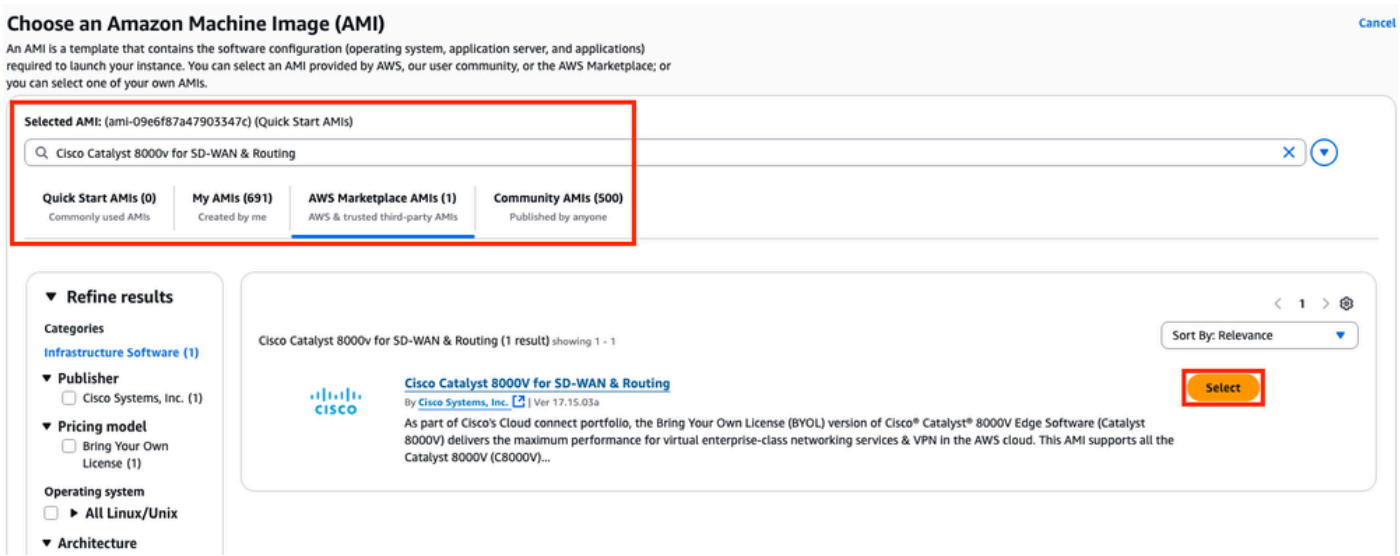
Jeder C8000v-Router verfügt über 2 Schnittstellen (1 öffentlich, 1 privat) und wird in seiner

eigenen Verfügbarkeitszone erstellt.

Klicken Sie im EC2 Dashboard auf Launch Instances (Instanzen starten):

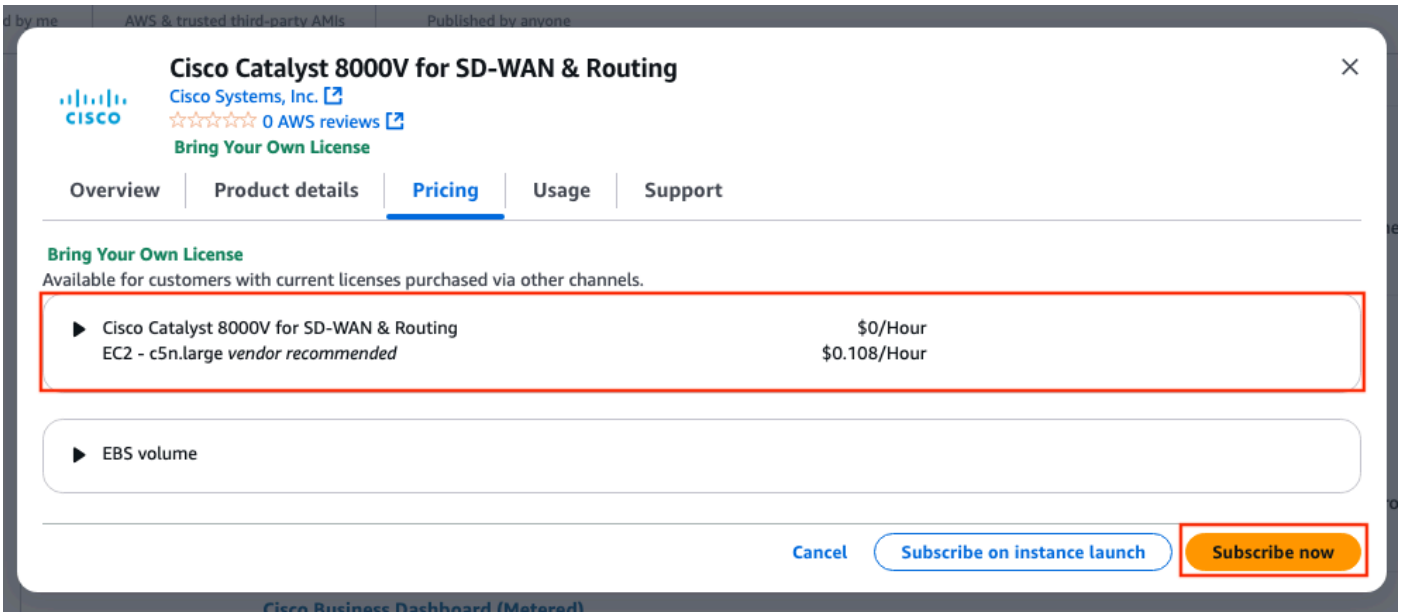


Filtern Sie die AMI-Datenbank mit dem Namen Cisco Catalyst 8000v für SD-WAN & Routing. Klicken Sie in der Liste AWS Marketplace AMIs auf Auswählen.



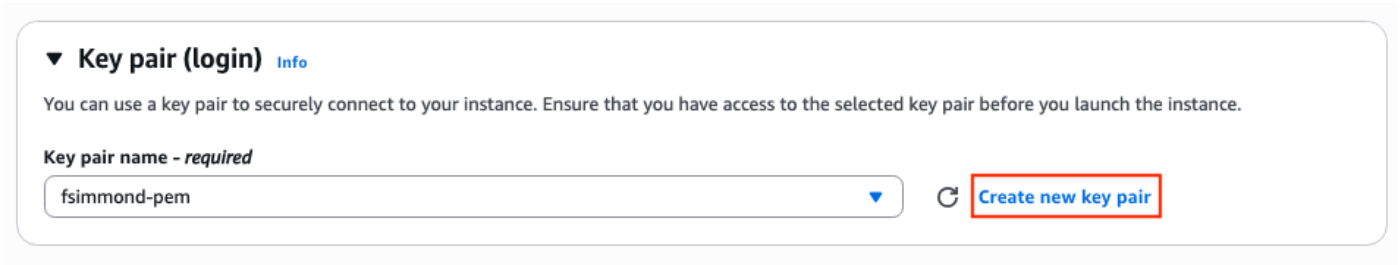
Wählen Sie die entsprechende Größe für die AMI aus. Für dieses Beispiel wird die Größe

c5n.large ausgewählt. Dies kann von der für Ihr Netzwerk erforderlichen Kapazität abhängen. Klicken Sie nach der Auswahl auf Jetzt abonnieren.

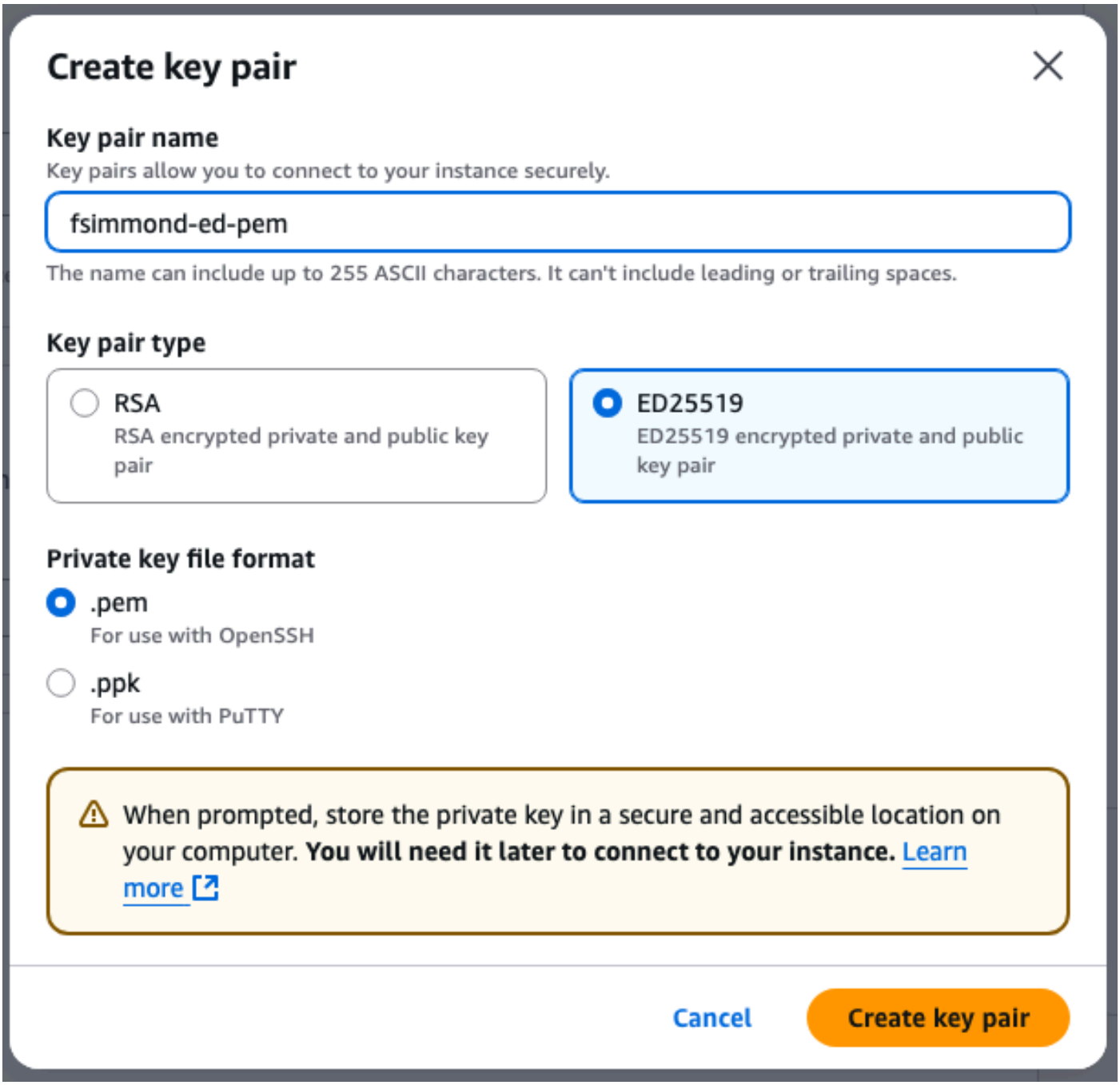


Schritt 6.1. Konfigurieren des Schlüsselpaars für den Remote-Zugriff

Sobald Sie sich für die AMI angemeldet haben, wird ein neues Fenster mit mehreren Optionen angezeigt. Falls im Abschnitt Schlüsselpaar (Anmeldung) kein Schlüsselpaar vorhanden ist, klicken Sie auf Neues Schlüsselpaar erstellen. Sie können für jedes erstellte Gerät einen einzelnen Schlüssel wiederverwenden.



Ein neues Popup-Fenster wird angezeigt. In diesem Beispiel wird eine PEM-Schlüsseldatei mit ED25519-Verschlüsselung erstellt. Sobald alles festgelegt ist, klicken Sie auf Schlüsselpaar erstellen.



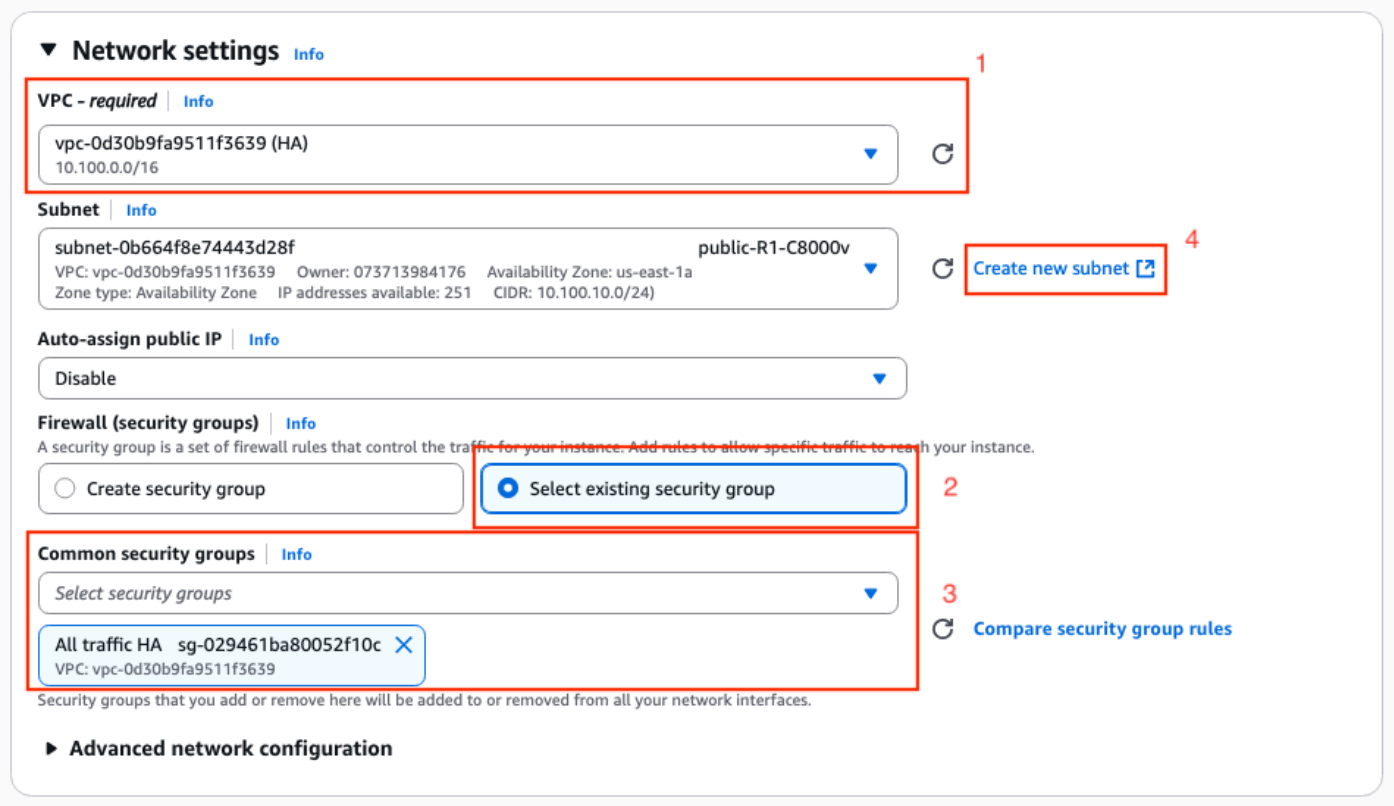
Schritt 6.2: Erstellen und Konfigurieren der Subnetze für die AMI

Klicken Sie im Abschnitt Netzwerkeinstellungen auf Bearbeiten. Einige neue Optionen im Abschnitt sind jetzt verfügbar:
1. Wählen Sie die gewünschte vPC für diese Arbeit. Für dieses Beispiel wird die vPC mit der Bezeichnung HA ausgewählt.

2. Wählen Sie im Abschnitt Firewall (Sicherheitsgruppen) die Option Vorhandene Sicherheitsgruppe auswählen.

3. Nach Auswahl von Option 2 ist die Option Gemeinsame Sicherheitsgruppen verfügbar. Filtern Sie die gewünschte Sicherheitsgruppe, und wählen Sie sie aus. In diesem Beispiel ist die Sicherheitsgruppe HA für den gesamten Datenverkehr ausgewählt.

4. (Optional) Wenn keine Subnetze für dieses Gerät erstellt werden, klicken Sie auf Neues Subnetz erstellen.



Eine neue Registerkarte im Webbrowser ist geöffnet, die Sie zum Abschnitt Subnetz erstellen führt:

1. Wählen Sie die entsprechende vPC für diese Konfiguration aus der Dropdown-Liste aus.

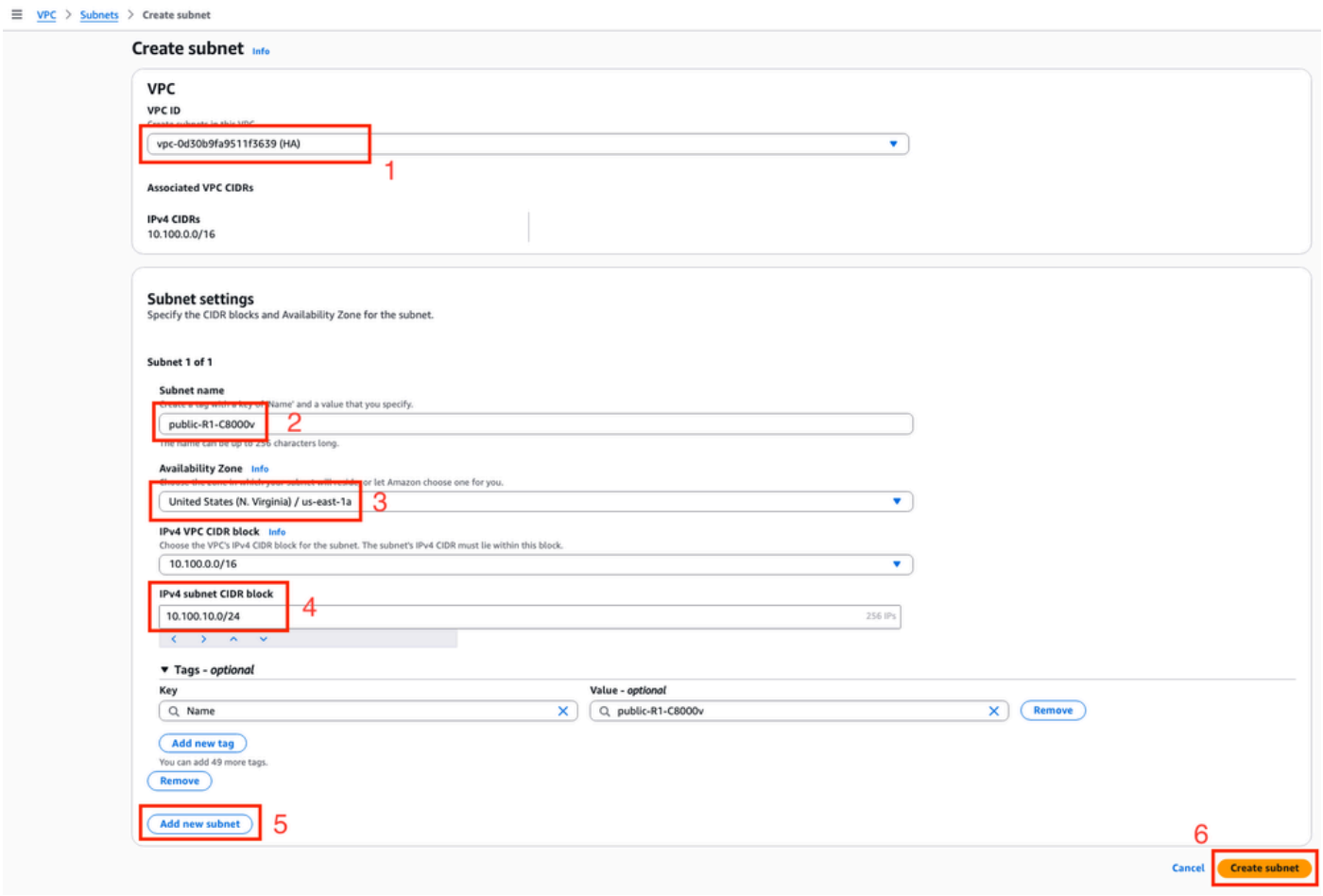
2. Legen Sie einen Namen für das neue Subnetz fest.

3. Definieren Sie die Verfügbarkeitszone für dieses Subnetz. (Weitere Informationen zur Einstellung finden Sie im Abschnitt zur Topologie dieses Dokuments.)

4. Legen Sie den Subnetzblock fest, der zum VPC-CIDR-Block gehört.

5. Außerdem können alle zu verwendenden Subnetze erstellt werden, indem Sie auf den Abschnitt Neues Subnetz hinzufügen klicken und die Schritte 2 bis 4 für jedes Subnetz wiederholen.

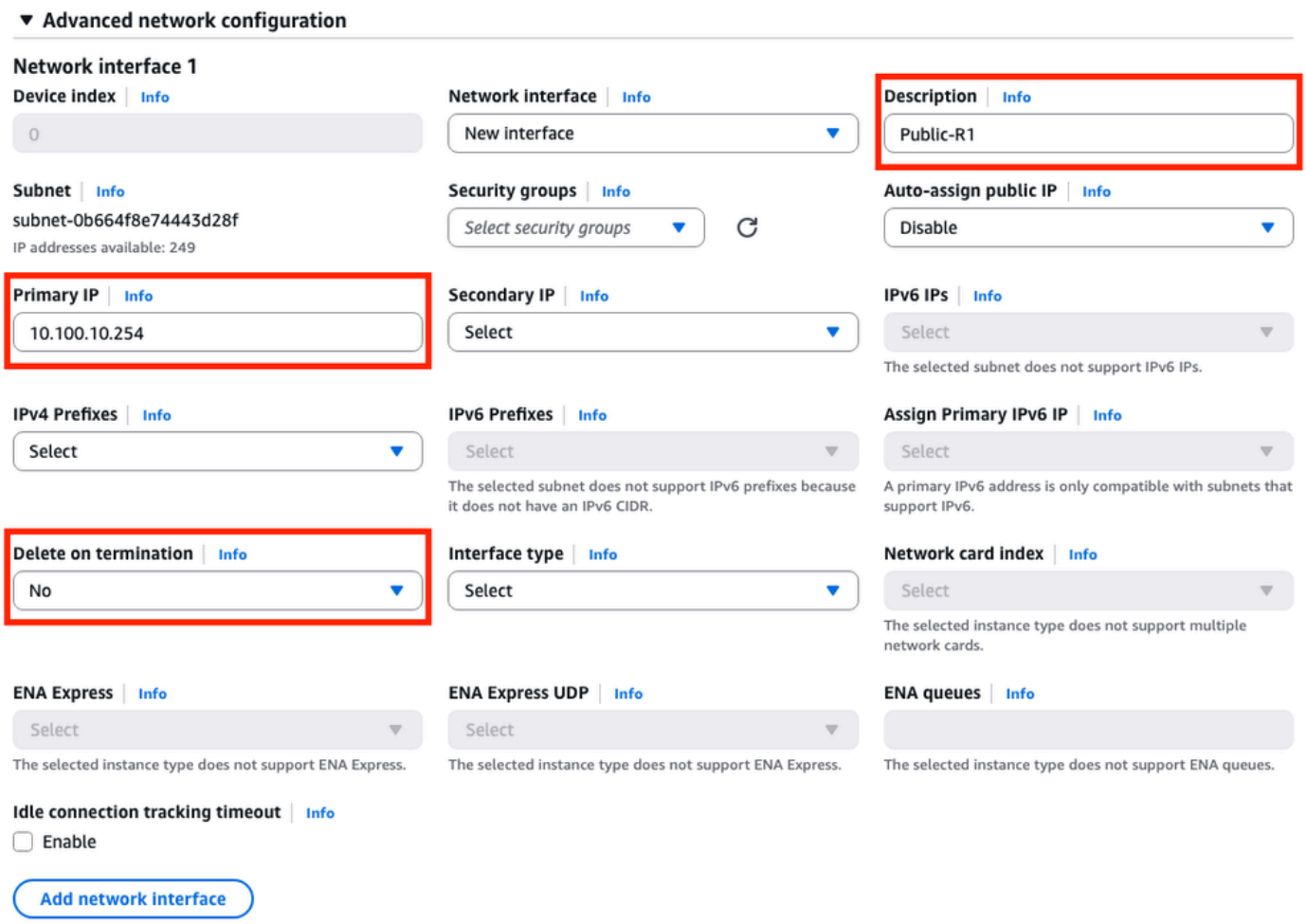
6. Klicken Sie abschließend auf Subnetz erstellen. Navigieren Sie zur vorherigen Seite, um die Einstellungen fortzusetzen.



Klicken Sie im Unterabschnitt Subnetz des Abschnitts Netzwerkeinstellungen auf das Symbol Aktualisieren, um die erstellten Subnetze in der Dropdown-Liste abzurufen.

Schritt 6.3. Konfigurieren der AMI-Schnittstellen

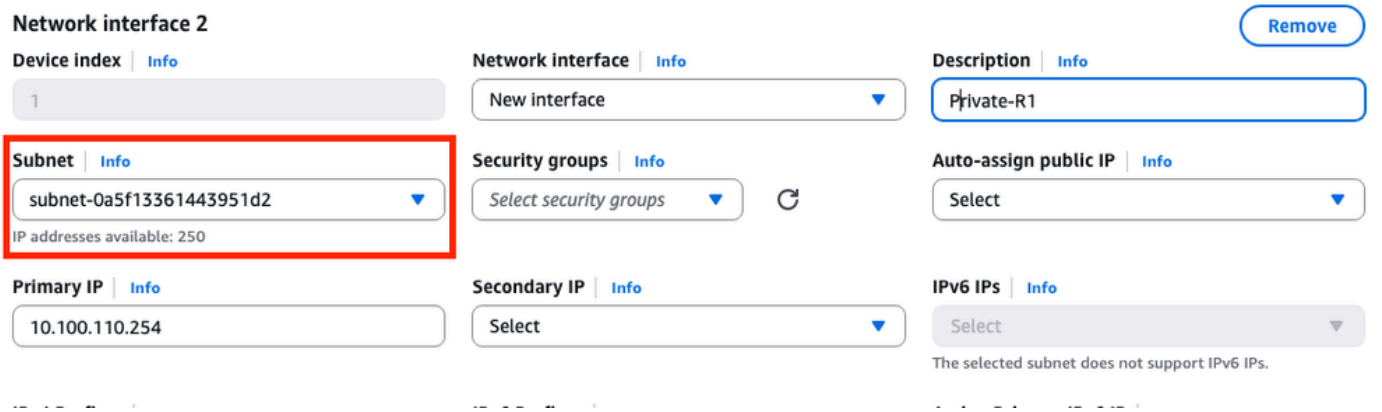
Erweitern Sie im Abschnitt Netzwerkeinstellungen den Unterabschnitt Erweiterte Netzwerkkonfiguration. Diese Optionen werden angezeigt:



In diesem Menü legen Sie die Parameter Description (Beschreibung), Primary IP (Primäre IP) und Delete (Löschen) für die Terminierung fest.
Verwenden Sie als Primary IP-Parameter eine beliebige IP-Adresse mit Ausnahme der ersten verfügbaren Adresse des Subnetzes. Diese wird intern von AWS verwendet.

Der Parameter Delete on termination in diesem Beispiel wird auf No festgelegt. Dies kann jedoch je nach Umgebung auf Ja eingestellt werden.

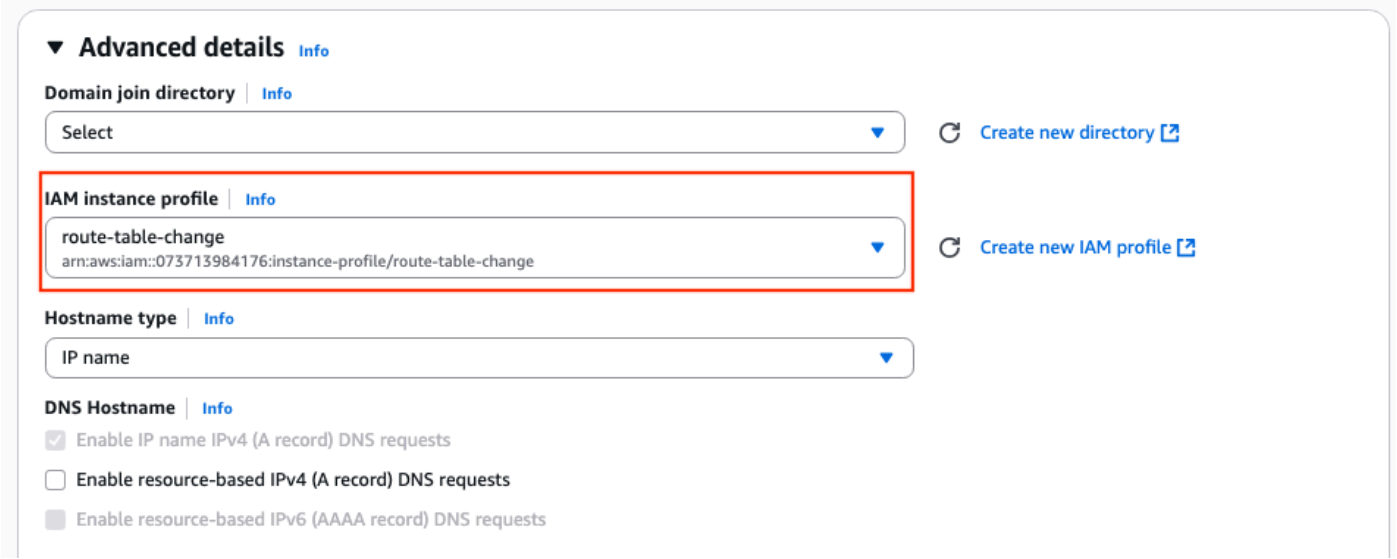
Aufgrund dieser Topologie ist eine zweite Schnittstelle für das private Subnetz erforderlich. Klicken Sie auf Netzwerkschnittstelle hinzufügen, um diese Eingabeaufforderung anzuzeigen. Die Schnittstelle bietet jedoch die Möglichkeit, das Subnetz diesmal auszuwählen:



Fahren Sie mit den nächsten Schritten fort, nachdem Sie alle Parameter wie auf der Netzwerkschnittstelle 1 festgelegt haben.

Schritt 6.4. Setzen Sie das IAM-Instanzprofil auf die AMI

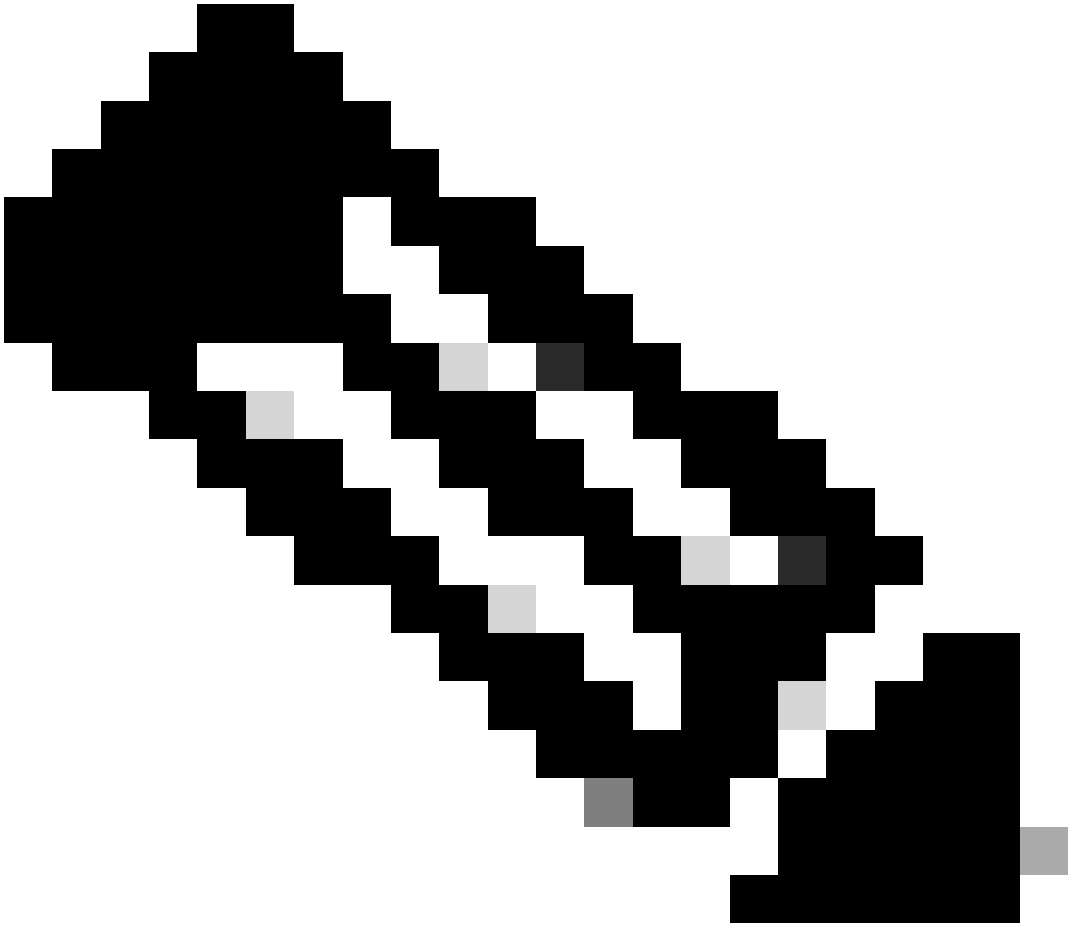
Wählen Sie im Abschnitt Erweiterte Details die erstellte IAM-Rolle im Parameter für das IAM-Instanzprofil aus:



Schritt 6.5. (Optional) Legen Sie die Anmeldeinformationen für die AMI fest

Navigieren Sie im Abschnitt Erweiterte Details zum Abschnitt Benutzerdaten - optional, und wenden Sie diese Einstellung an, um einen Benutzernamen und ein Kennwort festzulegen, während die Instanz erstellt wird:

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



Anmerkung: Der von AWS für SSH im C8000v bereitgestellte Benutzername kann fälschlicherweise als Root aufgeführt werden. Ändern Sie dies ggf. in ec2-user.

Schritt 6.6. Beenden der Instanzkonfiguration

Klicken Sie nach der Konfiguration auf Instanz 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.

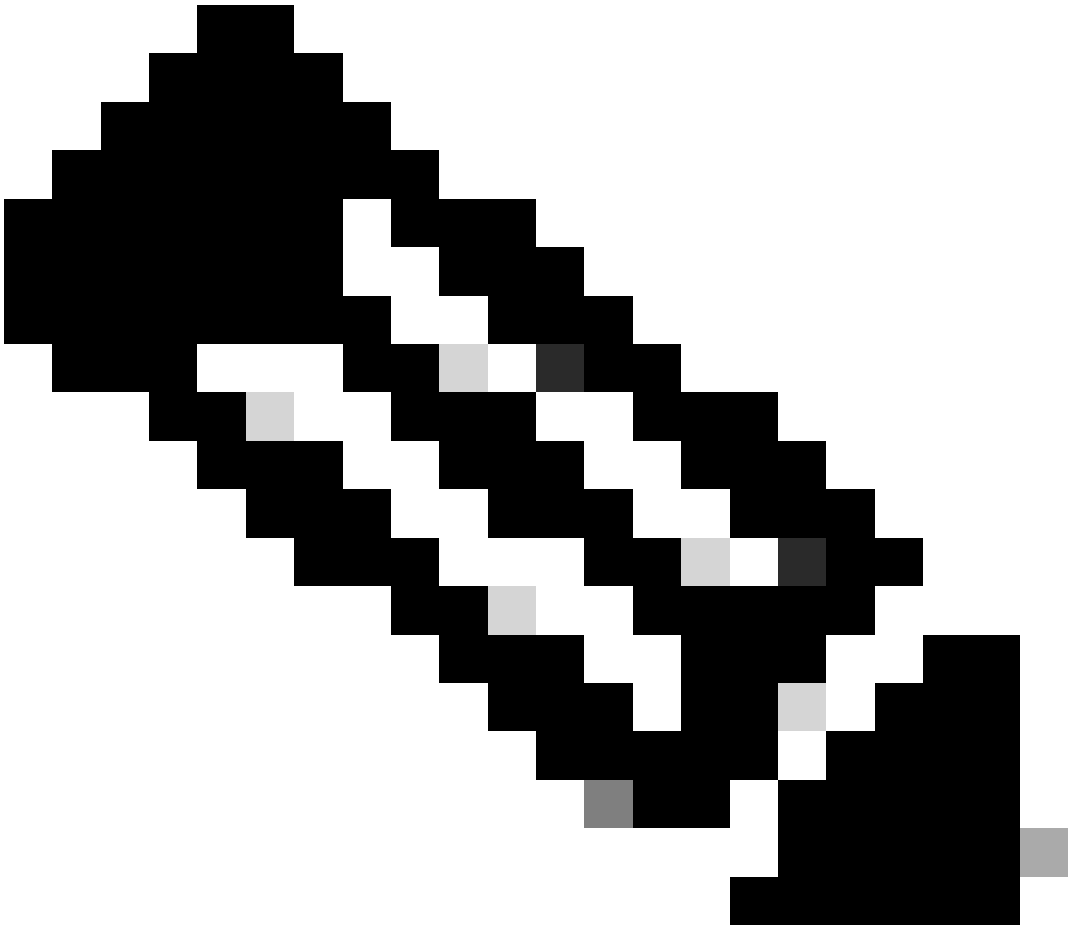
Cancel

Launch instance

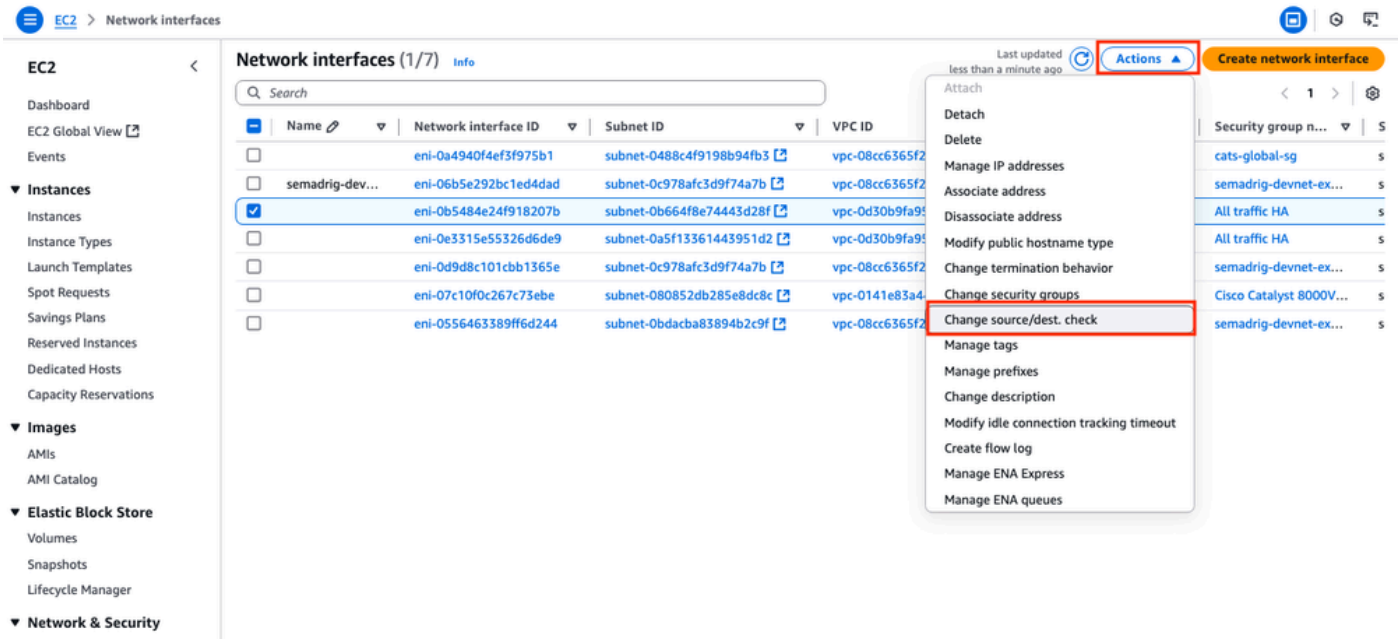
Preview code

Schritt 6.7: Deaktivieren der Quell-/Zielüberprüfung auf den ENIs

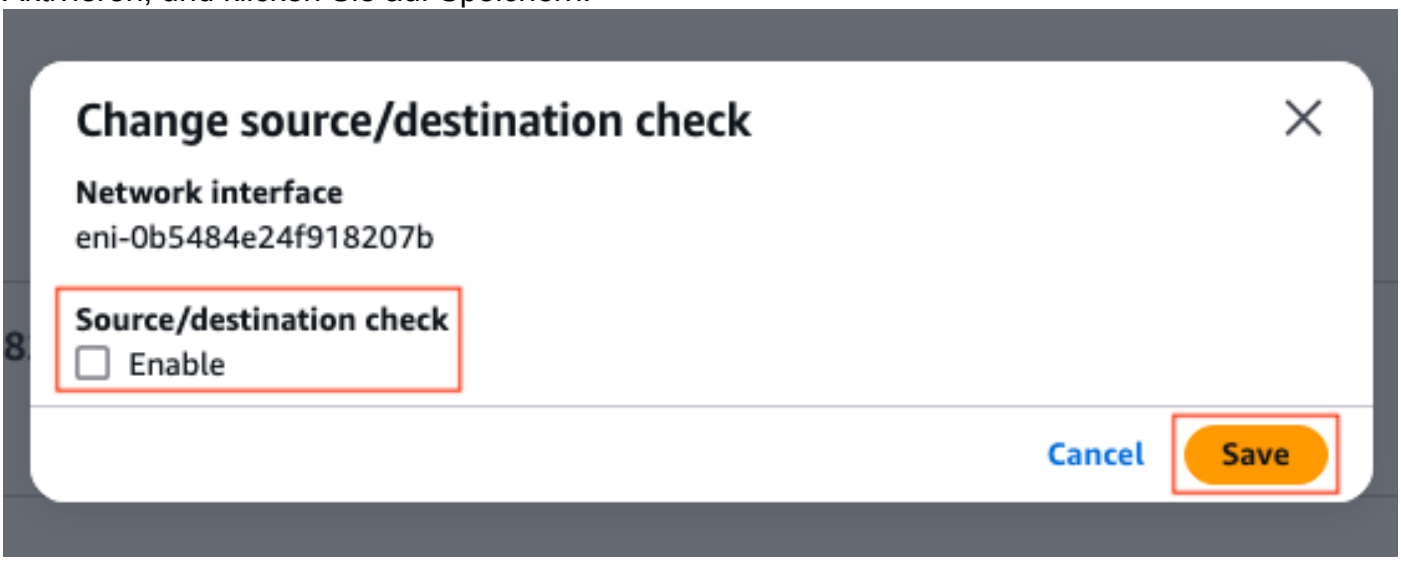
Sobald die Instanz erstellt wurde, deaktivieren Sie die src/dst-Prüffunktion in AWS, um die Verbindung zwischen Schnittstellen im gleichen Subnetz zu erhalten. Wählen Sie im Abschnitt EC2 Dashboard > Network & Security > Network interfaces (EC2-Dashboard > Netzwerk und Sicherheit > Netzwerkschnittstellen) die ENIs aus, und klicken Sie auf Actions (Aktionen). > Quelle/Ziel ändern. überprüfen.



Anmerkung: Sie müssen die ENIs einzeln auswählen, um diese Option verfügbar zu machen.



Ein neues Fenster wird angezeigt. Deaktivieren Sie im neuen Menü das Kontrollkästchen Aktivieren, und klicken Sie auf Speichern.

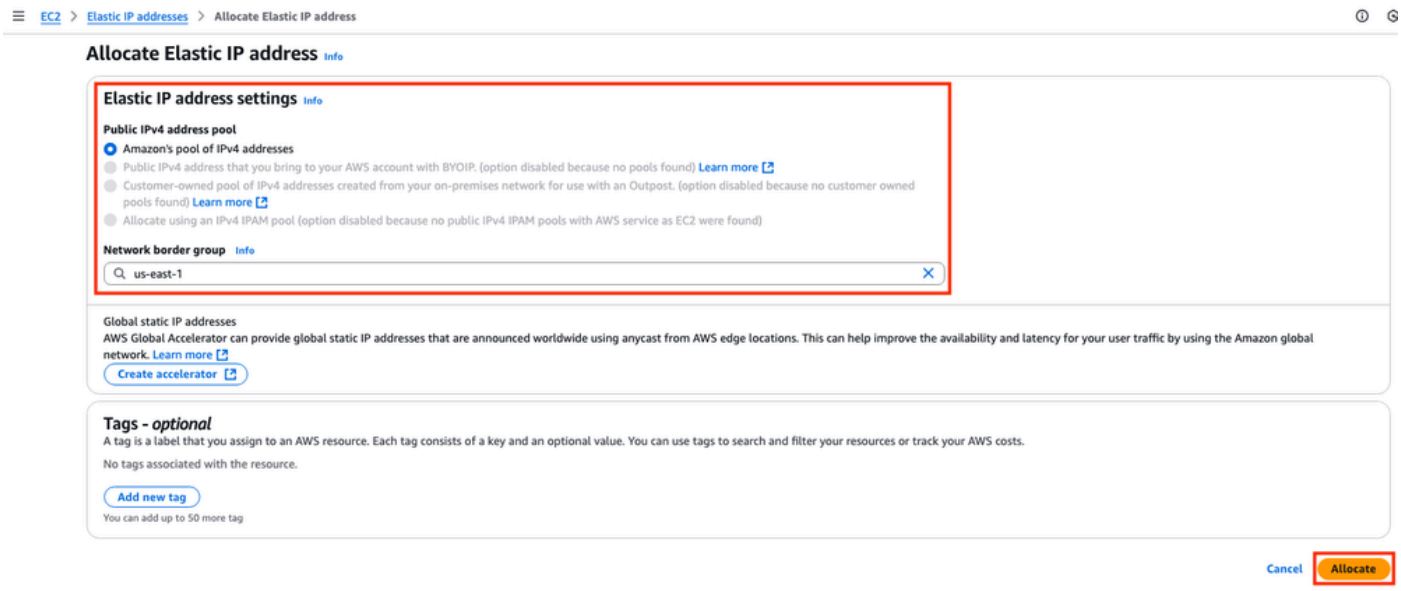


Schritt 6.8. Erstellen und Zuordnen einer elastischen IP zur öffentlichen ENI der Instanz

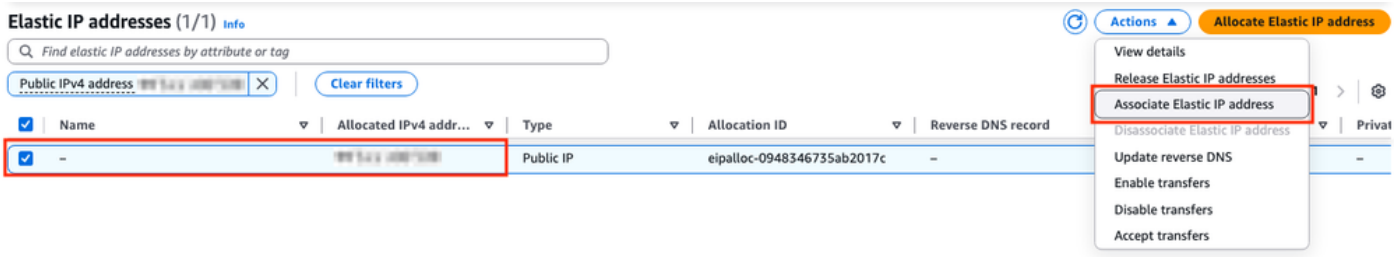
Klicken Sie im Abschnitt EC2 Dashboard > Network & Security > Elastic IPs (Netzwerk und Sicherheit > Elastische IPs) auf Allocate Elastic IP address (Elastische IP-Adresse zuweisen).

Die Seite führt Sie zu einem anderen Abschnitt. In diesem Beispiel wird die Option Amazon-Pool mit IPv4-Adressen zusammen mit der Verfügbarkeitszone us-east-1 ausgewählt. Klicken Sie

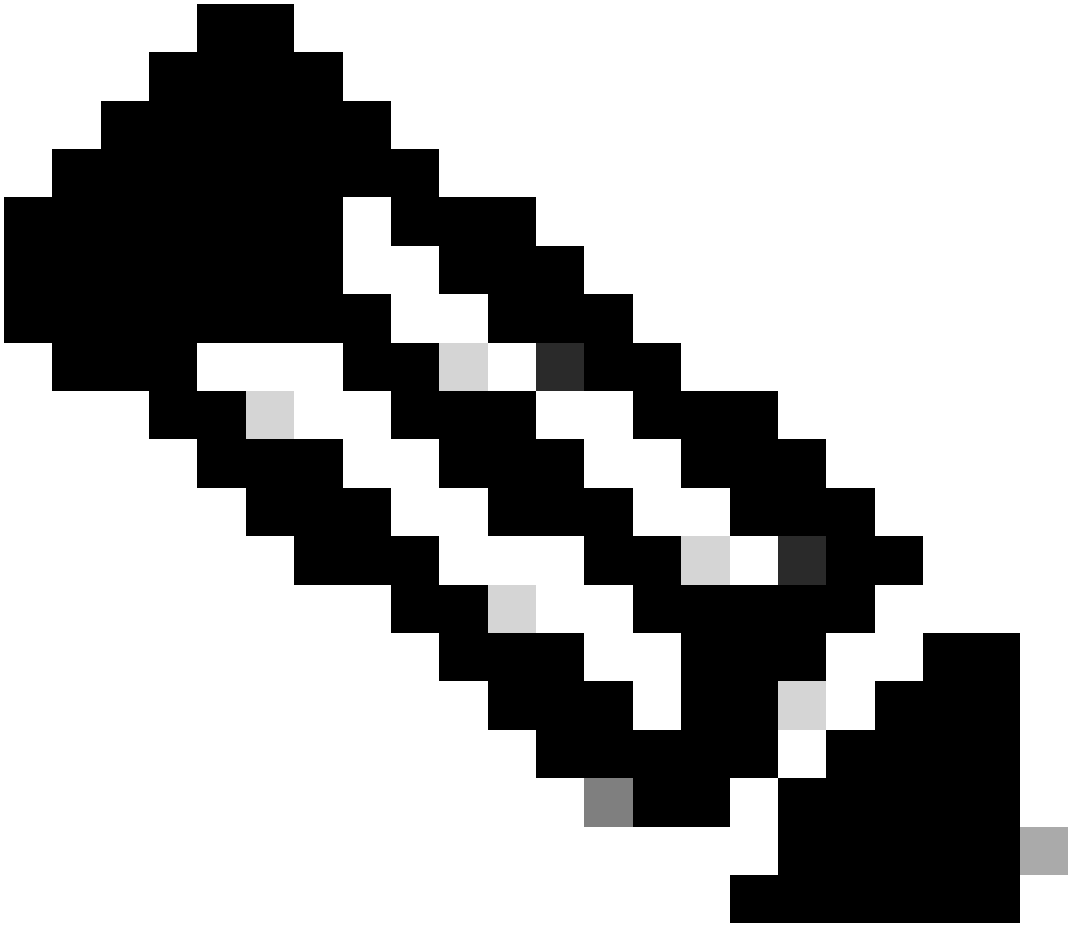
abschließend auf Zuweisen.



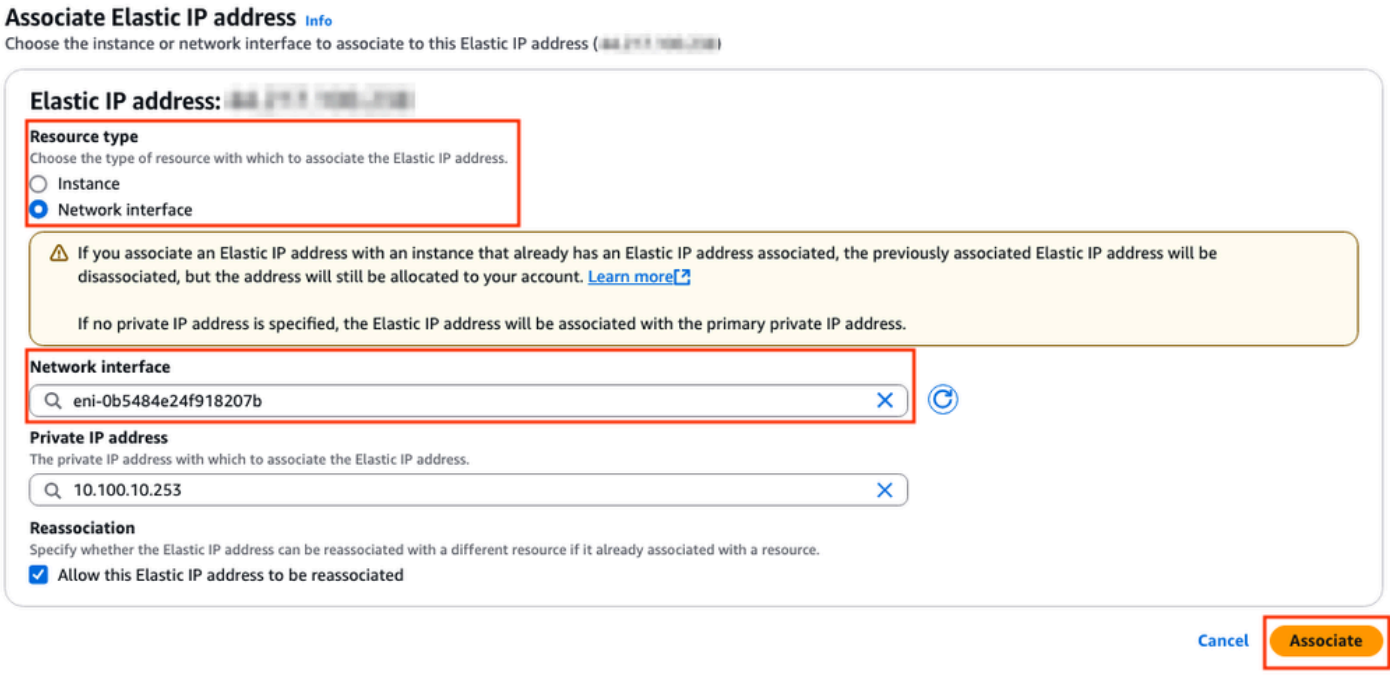
Weisen Sie die IP-Adresse bei der Erstellung der Instanz der öffentlichen Schnittstelle der Instanz zu. Klicken Sie im Abschnitt EC2 Dashboard > Network & Security > Elastic IPs (Netzwerk und Sicherheit > Elastische IP-Adressen) auf Actions > Associate Elastic IP address (Aktionen > Elastische IP-Adresse zuordnen).



Wählen Sie in diesem neuen Abschnitt die Option Network interface (Netzwerkschnittstelle) aus, und suchen Sie nach der öffentlichen ENI der entsprechenden Schnittstelle. Ordnen Sie die entsprechende öffentliche IP-Adresse zu, und klicken Sie auf Zuordnen.



Anmerkung: Um die richtige ENI-ID zu erhalten, navigieren Sie zum Abschnitt EC2 Dashboard > Instances. Wählen Sie dann die Instanz aus, und überprüfen Sie den Abschnitt Networking. Suchen Sie nach der IP-Adresse Ihrer öffentlichen Schnittstelle, um den ENI-Wert in derselben Zeile zu erhalten.



Schritt 7: Wiederholen Sie Schritt 6, um die zweite C8000v-Instanz für HA zu erstellen.

Im Abschnitt zur Topologie dieses Dokuments finden Sie die entsprechenden Informationen zu jeder Schnittstelle. Wiederholen Sie die Schritte 6.1 bis 6.6.

Schritt 8. Wiederholen Sie Schritt 6, um eine VM (Linux/Windows) aus dem AMI Marketplace zu erstellen

Für dieses Beispiel wird Ubuntu Server 22.04.5 LTS im AMI Marketplace als interner Host ausgewählt.

ens5 wird standardmäßig für die öffentliche Schnittstelle erstellt. Erstellen Sie in diesem Beispiel eine zweite Schnittstelle (ens6 auf dem Gerät) für das private Subnetz.

<#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
```

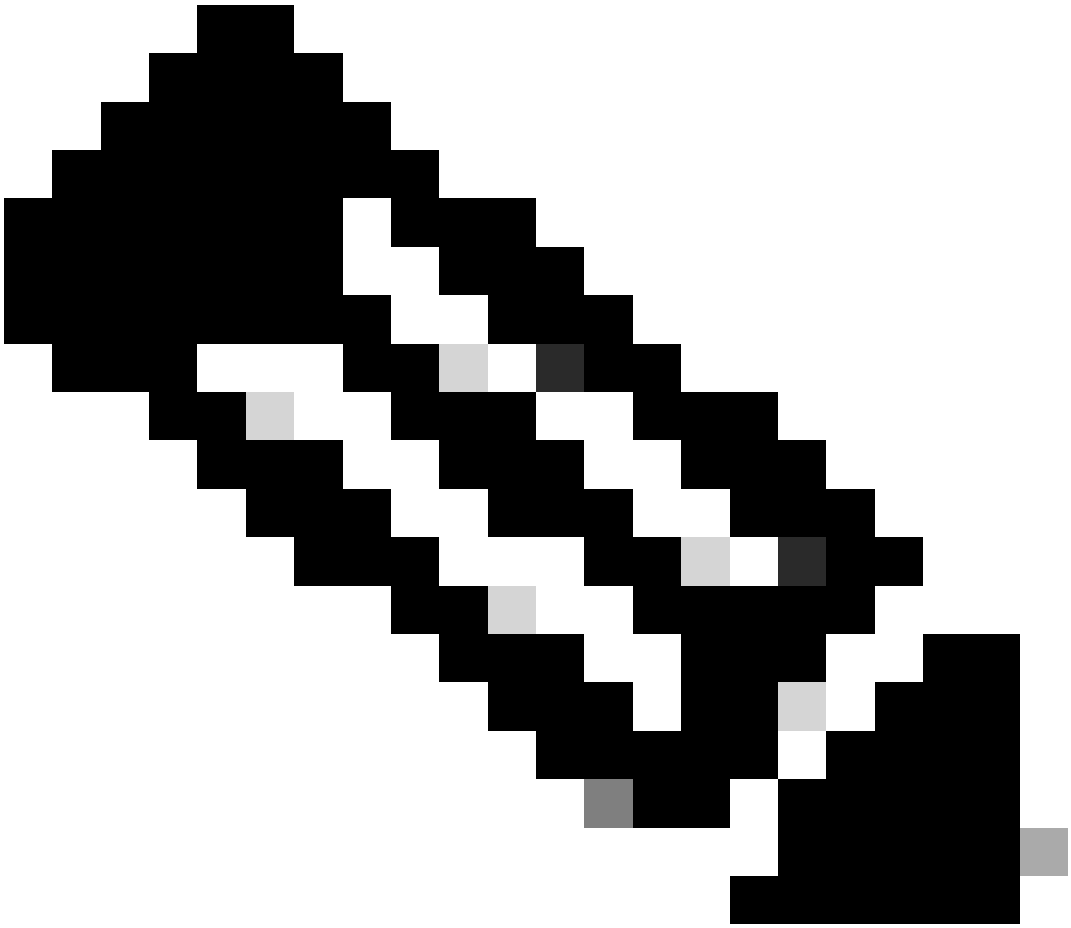
10.100.30.254

```
 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

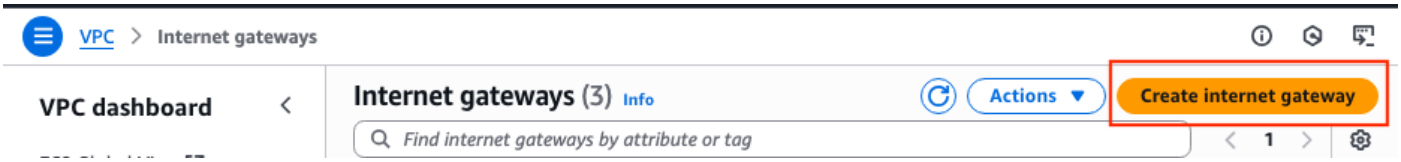
```
 netmask 255.255.255.0 broadcast 10.100.130.255
inet6 fe80::3b:7eff:fead:dbe5 prefixlen 64 scopeid 0x20<link>
ether 02:3b:7e:ad:db:e5 txqueuelen 1000 (Ethernet)
RX packets 119 bytes 16831 (16.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 133 bytes 13816 (13.8 KB)
TX errors 0 dropped 0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



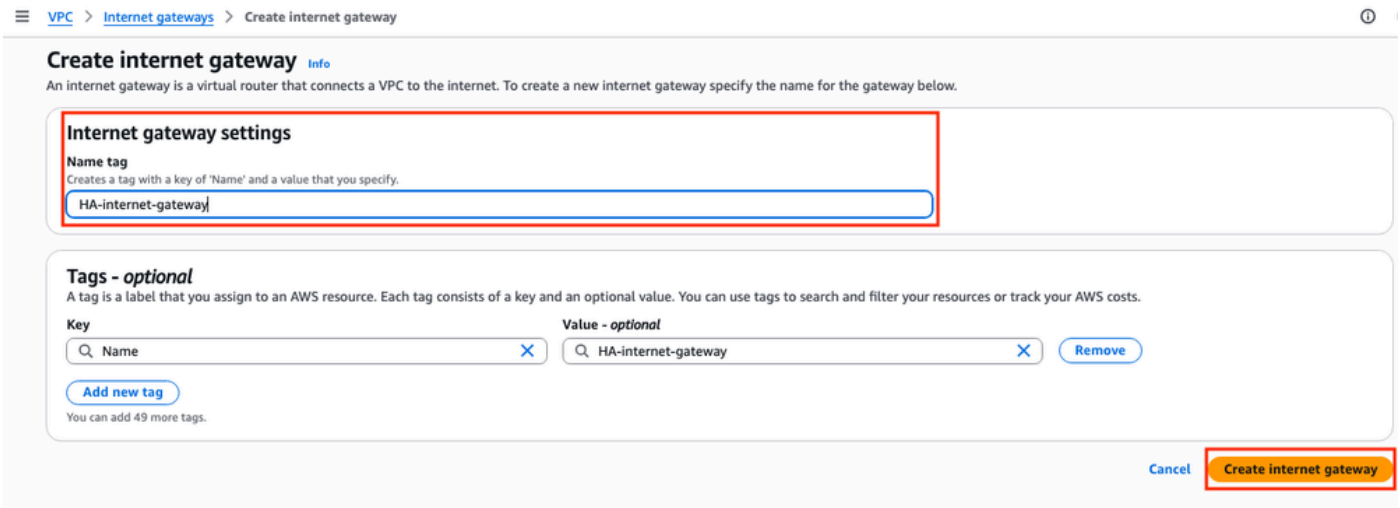
Anmerkung: Wenn Änderungen an den Schnittstellen vorgenommen werden, schlagen Sie mit der Maus über die Schnittstelle oder laden Sie die VM neu, damit diese Änderungen übernommen werden.

Schritt 9: Erstellen und Konfigurieren eines Internet-Gateways (IGW) für die VPC

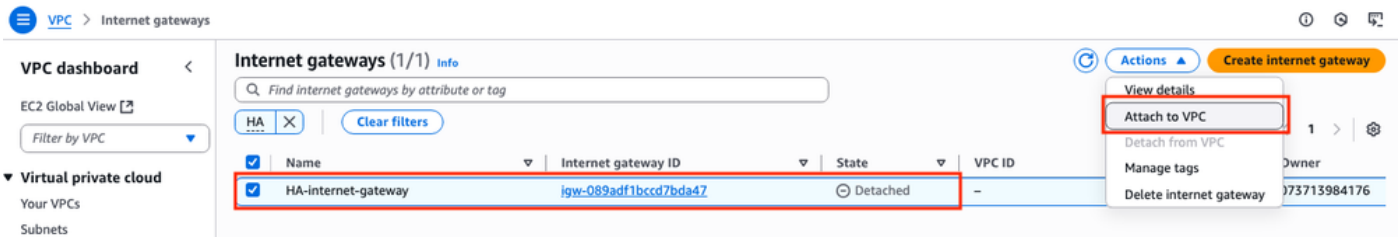
Klicken Sie im Abschnitt **VPC Dashboard > Virtual Private Cloud > Internet-Gateways** auf **Internet-Gateway erstellen**.



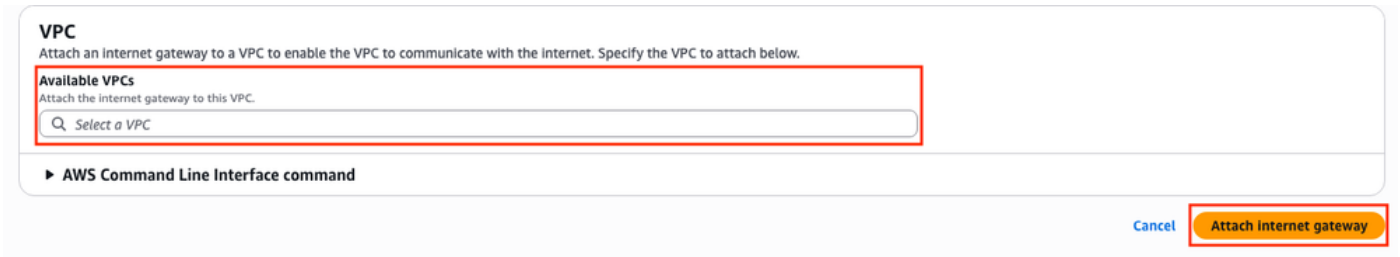
Erstellen Sie in diesem neuen Abschnitt ein **Namensschild** für dieses Gateway, und klicken Sie auf **Internet-Gateway erstellen**.



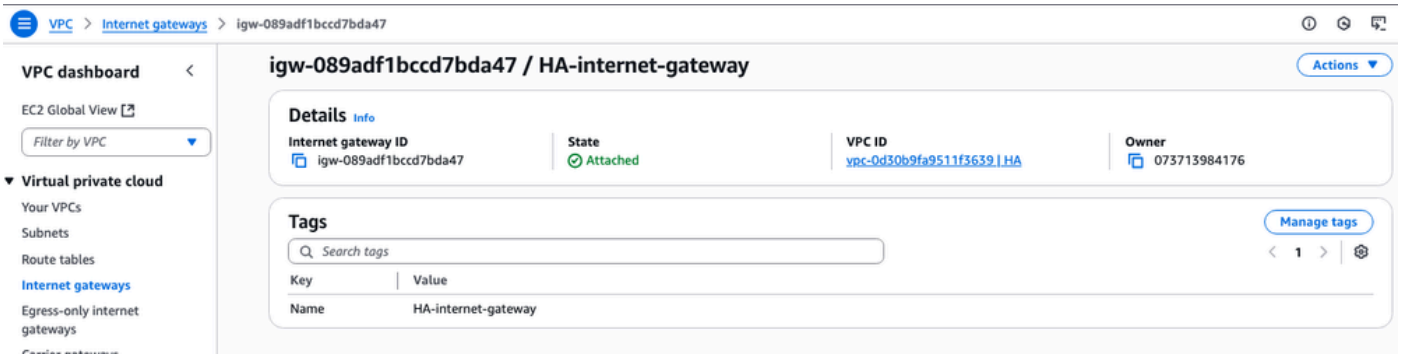
Schließen Sie das IGW nach der Erstellung an die entsprechende vPC an. Navigieren Sie zum Abschnitt **VPC Dashboard > Virtual Private Cloud > Internet Gateway**, und wählen Sie das entsprechende IGW aus. Klicken Sie auf **Aktionen > An vPC anhängen**.



Wählen Sie in diesem neuen Abschnitt die vPC mit dem Namen **HA aus**. Klicken Sie in diesem Beispiel auf **Internet-Gateway anhängen**.



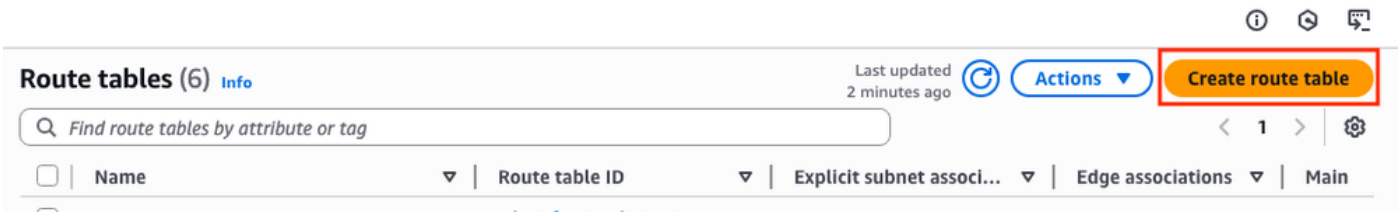
Das IGW muss den angezeigten Zustand " Attached" angeben:



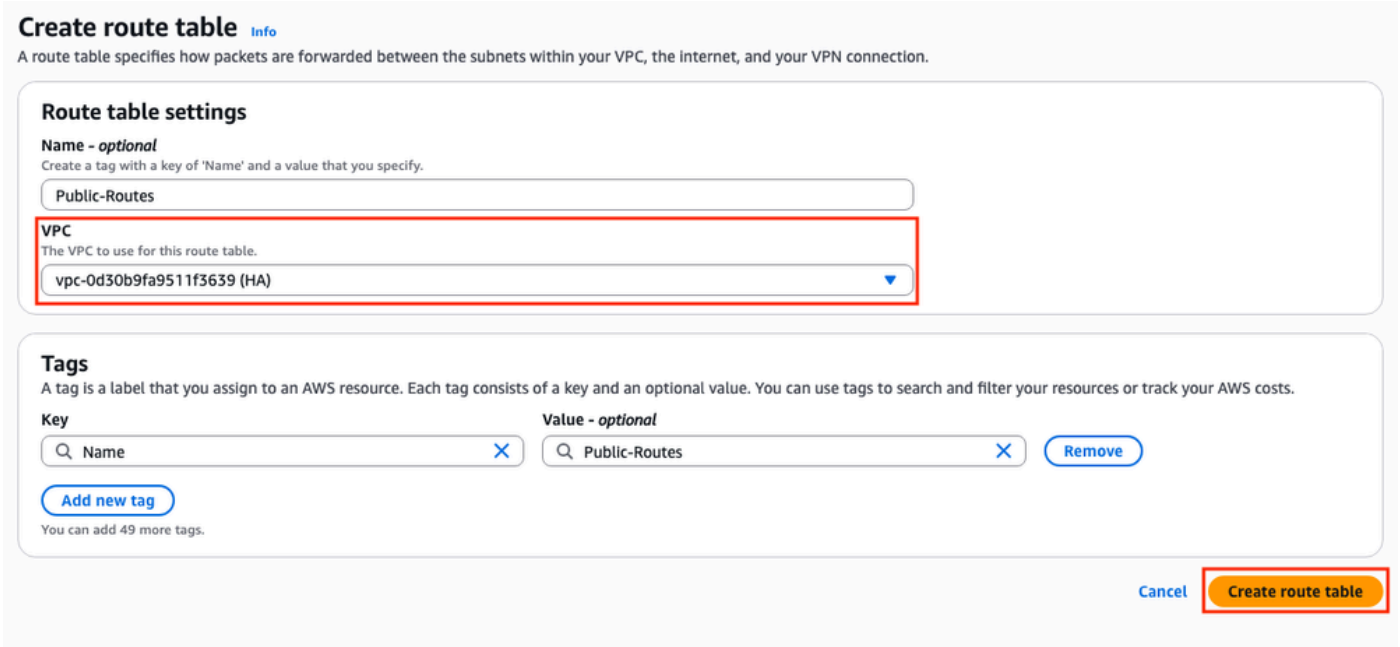
Schritt 10: Erstellen und Konfigurieren von Routing-Tabellen in AWS für öffentliche und private Subnetze

Schritt 10.1: Erstellen und Konfigurieren der öffentlichen Routentabelle

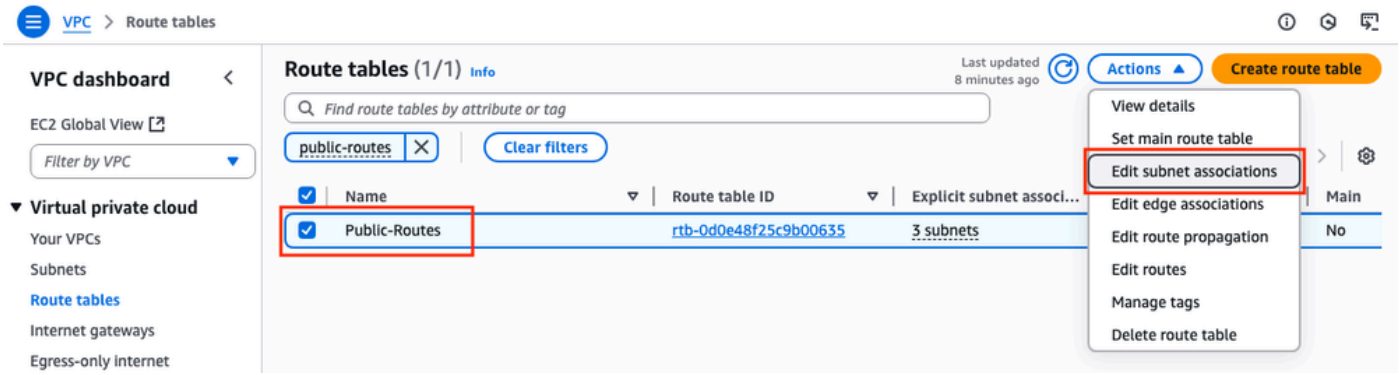
Um die hohe Verfügbarkeit für diese Topologie festzulegen, verknüpfen Sie alle öffentlichen und privaten Subnetze in den entsprechenden Routing-Tabellen. Klicken Sie im Abschnitt VPC Dashboard > Virtual Private Cloud > Routing tables auf Create route table (Routing-Tabelle erstellen).



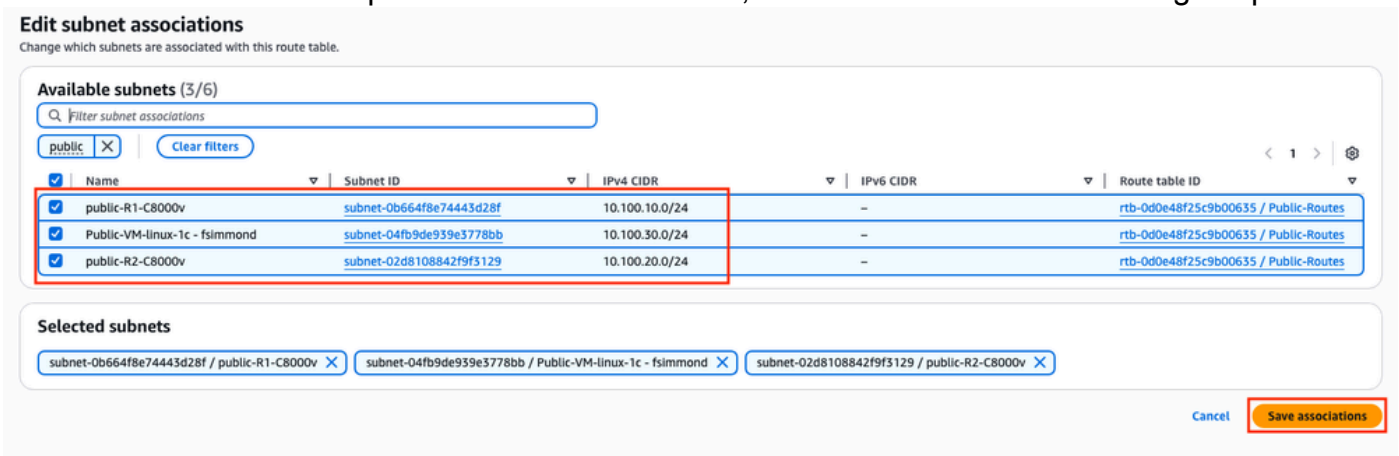
Wählen Sie im neuen Abschnitt die entsprechende vPC für diese Topologie aus. Klicken Sie nach der Auswahl auf Create route table (Weiterleitungstabelle erstellen).



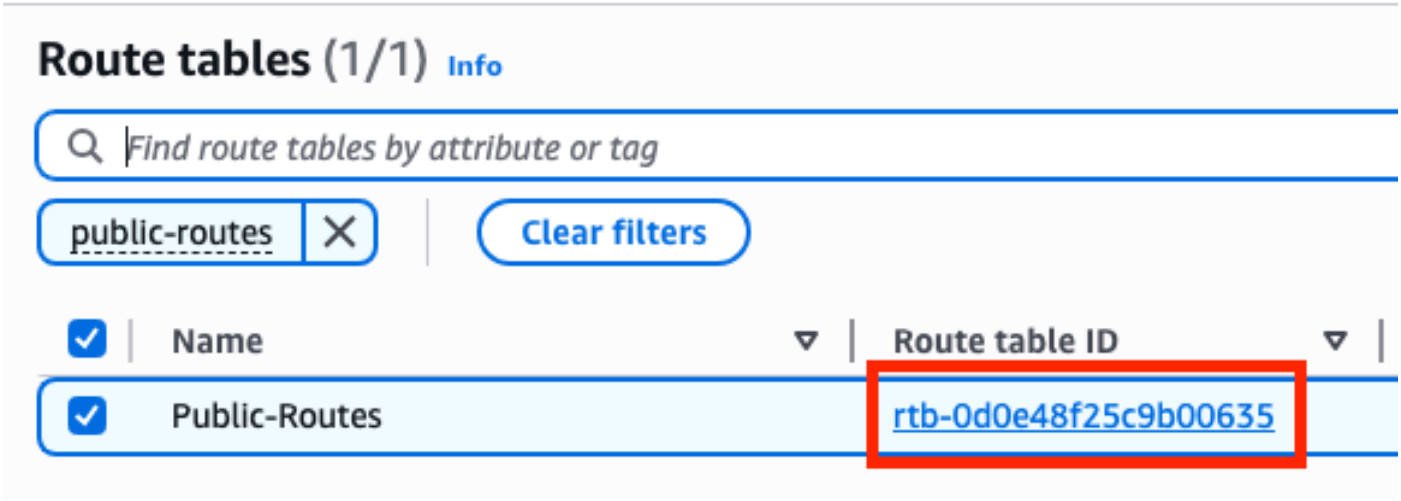
Wählen Sie im Abschnitt "Routentabellen" die erstellte Tabelle aus, und klicken Sie auf Aktionen > Subnetzzuordnungen bearbeiten.



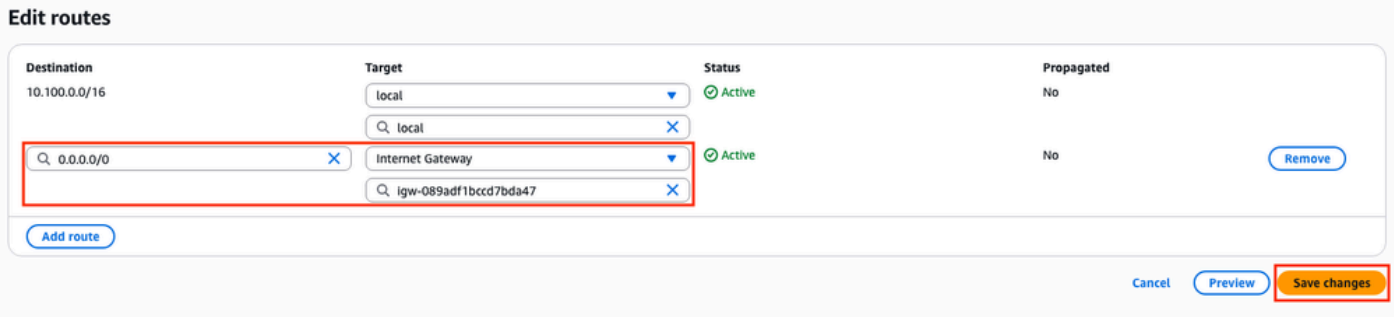
Wählen Sie dann die entsprechenden Subnetze aus, und klicken Sie auf Zuordnungen speichern.



Sobald die Subnetze zugeordnet sind, klicken Sie auf den Hyperlink Route Table ID (Routentabellen-ID), um die richtigen Routen für die Tabelle hinzuzufügen. Klicken Sie dann auf Routen bearbeiten:

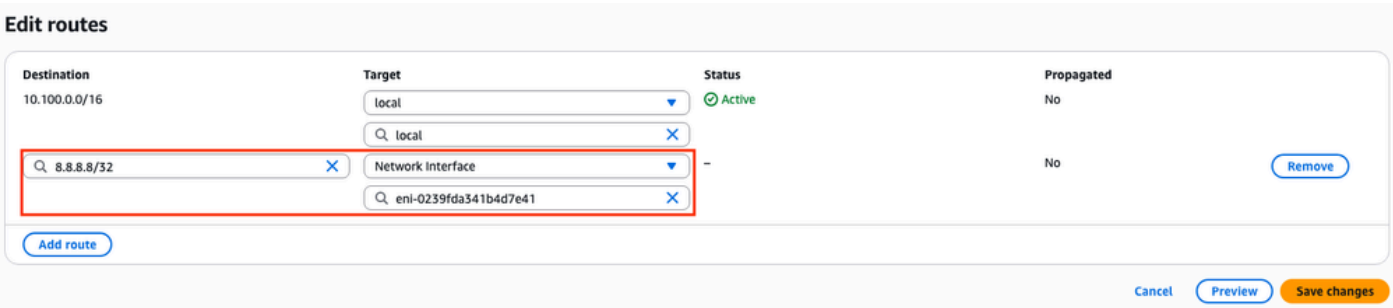


Um Internetzugriff zu erhalten, klicken Sie auf Route hinzufügen und verknüpfen diese öffentliche Routing-Tabelle mit dem in Schritt 9 erstellten IGW mit diesen Parametern. Klicken Sie nach der Auswahl auf Änderungen speichern:



Schritt 10.2: Erstellen und Konfigurieren der privaten Routing-Tabelle

Nachdem die öffentliche Routing-Tabelle erstellt wurde, replizieren Sie die Schritte 10 für die private Route und die privaten Subnetze, mit Ausnahme des Hinzufügens des Internet Gateways zu seinen Routen. In diesem Beispiel sieht die Routing-Tabelle folgendermaßen aus, da der Datenverkehr für 8.8.8.8 das private Subnetz in diesem Beispiel durchlaufen muss:



Schritt 11: Überprüfung und Konfiguration der grundlegenden Netzwerkkonfiguration, Network Address Translation (NAT), GRE-Tunnel mit BFD und Routing-Protokoll

Sobald die Instanzen und ihre Routing-Konfiguration auf AWS vorbereitet sind, konfigurieren Sie die Geräte:

C8000v R1-Konfiguration:

```
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
```

Konfiguration von 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
```

Schritt 12: Konfigurieren der hohen Verfügbarkeit (Cisco IOS® XE Denali 16.3.1a oder höher)

Nachdem die Redundanz und die Verbindung zwischen den virtuellen Systemen festgelegt sind, konfigurieren Sie die HA-Einstellungen, um die Routing-Änderungen zu definieren. Legen Sie die Werte Route-table-id, Network-interface-id und CIDR fest, die nach einem AWS HA-Fehler (z. B.

"BFD peer down") festgelegt werden müssen.

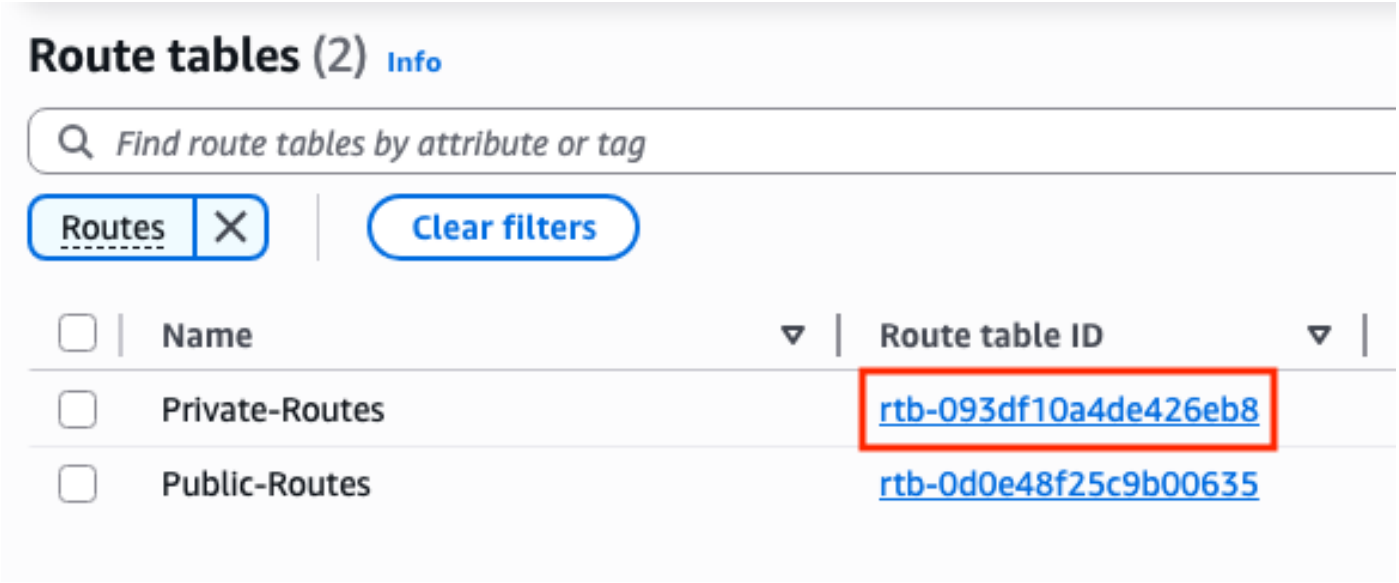
```
Router(config)# redundancy
Router(config-red)# cloud provider aws (node-id)
bfd peer <IP address of the remote device>
route-table <Route table ID>
cidr ip <traffic to be monitored/prefix>
eni <Elastic network interface (ENI) ID>
region <region-name>
```

Der bfd-Peer-Parameter ist mit der Tunnel-Peer-IP-Adresse verknüpft. Dies kann mit der Ausgabe von show bfd neighbor überprüft werden:

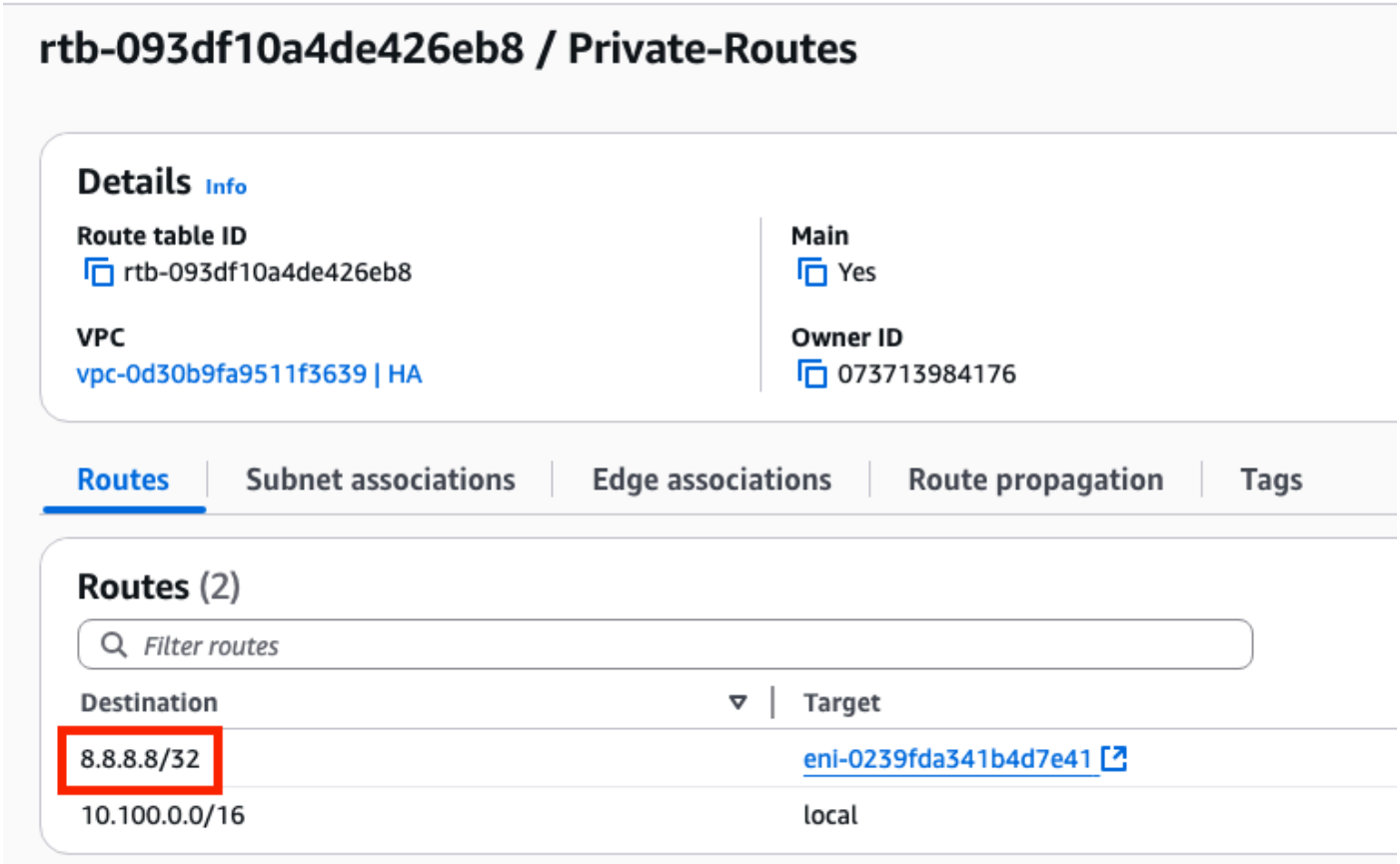
```
R1(config)#do sh bfd neighbors

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

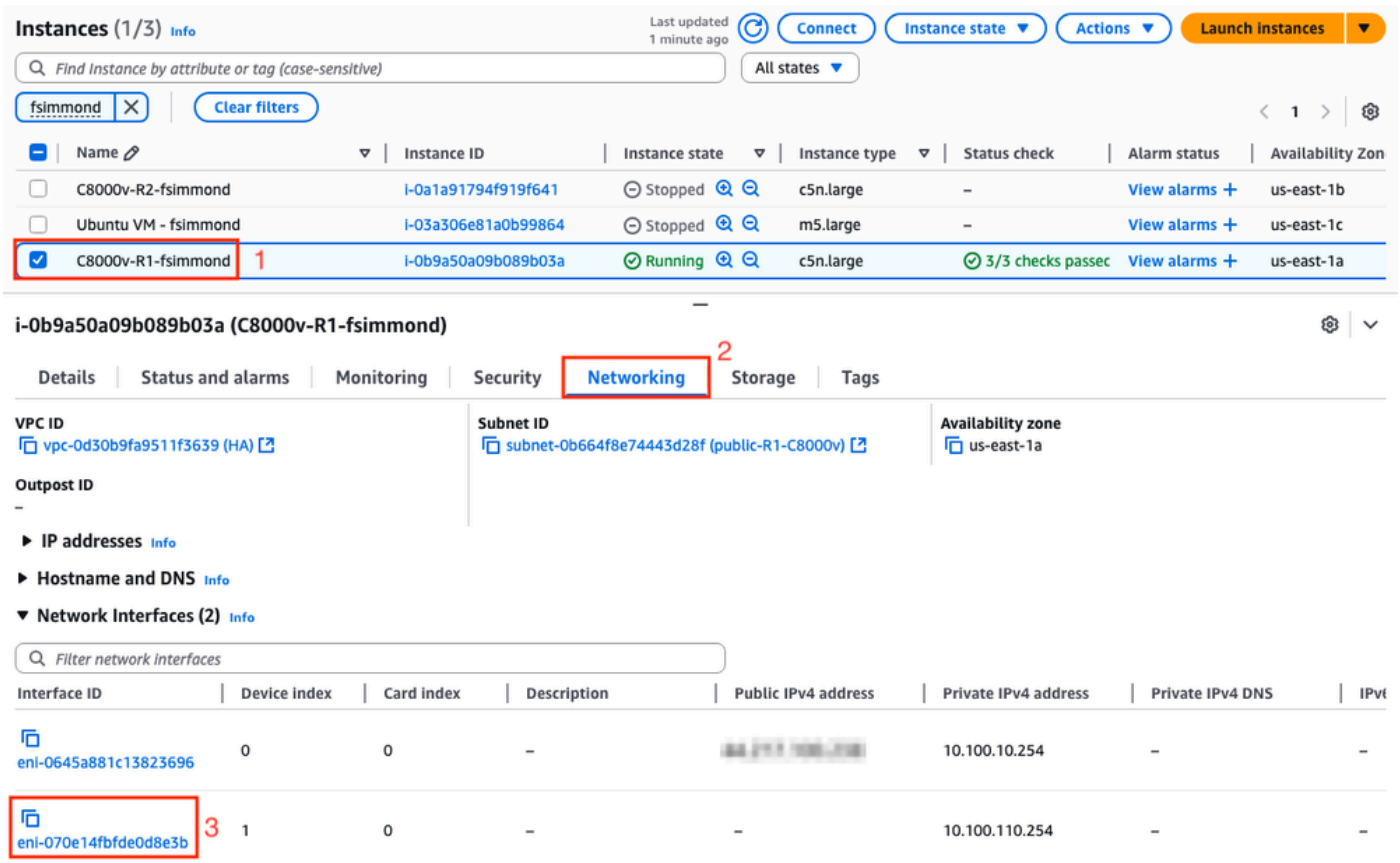
Der Parameter route-table bezieht sich auf die ID der privaten Routing-Tabelle im Abschnitt VPC Dashboard > Virtual Private Cloud > Route Tables. Kopieren Sie die entsprechende Routing-Tabellen-ID.



Der Parameter cidr ip ist mit dem Routenpräfix verknüpft, das in der Tabelle für private Routen (Routen, die in Schritt 10.2 erstellt wurden) hinzugefügt wurde:



Der Parameter eni ist mit der ENI-ID der entsprechenden privaten Schnittstelle der zu konfigurierenden Instanz verknüpft. Für dieses Beispiel wird die ENI-ID der Schnittstelle GigabitEthernet2 der Instanz verwendet:



Der Parameter region bezieht sich auf den Codenamen, der in der AWS-Dokumentation für die Region zu finden ist, in der sich die VPC befindet. Für dieses Beispiel wird die Region us-east-1 verwendet.

Diese Liste kann sich jedoch ändern oder erweitern. Die neuesten Updates finden Sie im Dokument AmazonRegion and Availability Zones.

Unter Berücksichtigung dieser Informationen sehen Sie das Konfigurationsbeispiel für die einzelnen Router in der VPC:

Konfigurationsbeispiel für C800v 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
```

Konfigurationsbeispiel für C800v 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
```

Verifizierung

1. Überprüfen Sie den Status der C8000v R1-Instanz. Stellen Sie sicher, dass die Tunnel- und Cloud-Redundanz einsatzbereit ist.

```
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
```

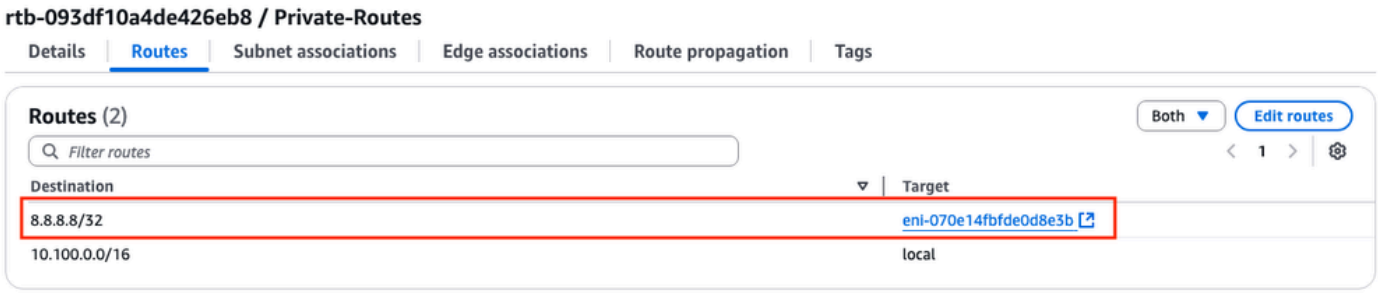
```
0 192.168.200.2 Tu1 10 00:16:52 2 1470 0 2


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. Führen Sie einen kontinuierlichen Ping zu 8.8.8.8 von der Host-VM hinter den Routern aus. Stellen Sie sicher, dass der Ping über die private Schnittstelle gesendet wird:

```
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. Öffnen Sie die AWS WebGUI und überprüfen Sie den Status der Routing-Tabelle. Die aktuelle ENI gehört zur privaten Schnittstelle der R1-Instanz:



4. Lösen Sie die Routenänderung aus, indem Sie die Tunnel1-Schnittstelle der R1-Instanz herunterfahren, um ein HA-Failover-Ereignis zu simulieren:

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

5. Überprüfen Sie erneut in der Routing-Tabelle auf AWS, die ENI-ID hat sich in die private R2-Schnittstelle ENI-ID geändert:

Fehlerbehebung

Dies sind die häufigsten Punkte, die bei der Neuerstellung der Bereitstellung häufig vergessen/falsch konfiguriert werden:

- 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, zur richtigen Routentabelle hinzugefügt, mit dem richtigen Router verbunden und die richtige vPC und Zone mit der IAM-Rolle und den Sicherheitsgruppen verknüpft wurde.

- Deaktivierung der Quell-/Zielprüfung per ENI.
  Falls Sie bereits alle Punkte in diesem Abschnitt überprüft haben und das Problem weiterhin besteht, sammeln Sie die folgenden Ergebnisse, testen Sie nach Möglichkeit das HA-Failover, und erstellen Sie ein Ticket beim Cisco TAC:

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

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.