

Bereitstellung einer hochverfügbaren C800v-Konfiguration auf AWS

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Topologie](#)

[Netzwerkdiagramm](#)

[Tabellenübersicht](#)

[Einschränkungen](#)

[Konfiguration](#)

[Schritt 1: Wählen Sie eine Region](#)

[Schritt 2: Erstellen der vPC](#)

[Schritt 3: Erstellen einer Sicherheitsgruppe für die vPC](#)

[Schritt 4: Erstellen einer IAM-Rolle mit einer Richtlinie und Zuordnen zum VPC](#)

[Schritt 5: Erstellen einer Vertrauensrichtlinie und Anhängen an eine IAM-Rolle](#)

[Schritt 6: Konfigurieren und Starten der C800v-Instanzen](#)

[Schritt 6.1. Konfigurieren des Schlüsselpaars für den Remote-Zugriff](#)

[Schritt 6.2: Erstellen und Konfigurieren der Subnetze für die AMI](#)

[Schritt 6.3. Konfigurieren der AMI-Schnittstellen](#)

[Schritt 6.4. Setzen Sie das IAM-Instanzprofil auf die AMI](#)

[Schritt 6.5. \(Optional\) Legen Sie die Anmeldeinformationen für die AMI fest](#)

[Schritt 6.6. Beenden der Instanzkonfiguration](#)

[Schritt 6.7: Deaktivieren der Quell-/Zielüberprüfung auf den ENIs](#)

[Schritt 6.8. Erstellen und Zuordnen einer elastischen IP zur öffentlichen ENI der Instanz](#)

[Schritt 7: Wiederholen Sie Schritt 6, um die zweite C800v-Instanz für HA zu erstellen.](#)

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

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

[Schritt 10: Erstellen und Konfigurieren von Routing-Tabellen in AWS für öffentliche und private Subnetze](#)

[Schritt 10.1: Erstellen und Konfigurieren der öffentlichen Routentabelle](#)

[Schritt 10.2: Erstellen und Konfigurieren der privaten Routing-Tabelle](#)

[Schritt 11: Überprüfung und Konfiguration der grundlegenden Netzwerkconfiguration, Network Address Translation \(NAT\), GRE-Tunnel mit BFD und Routing-Protokoll](#)

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

[Verifizierung](#)

[Fehlerbehebung](#)

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® XE Denali 17.15.3a)
- 1x - VM (Linux/Windows)

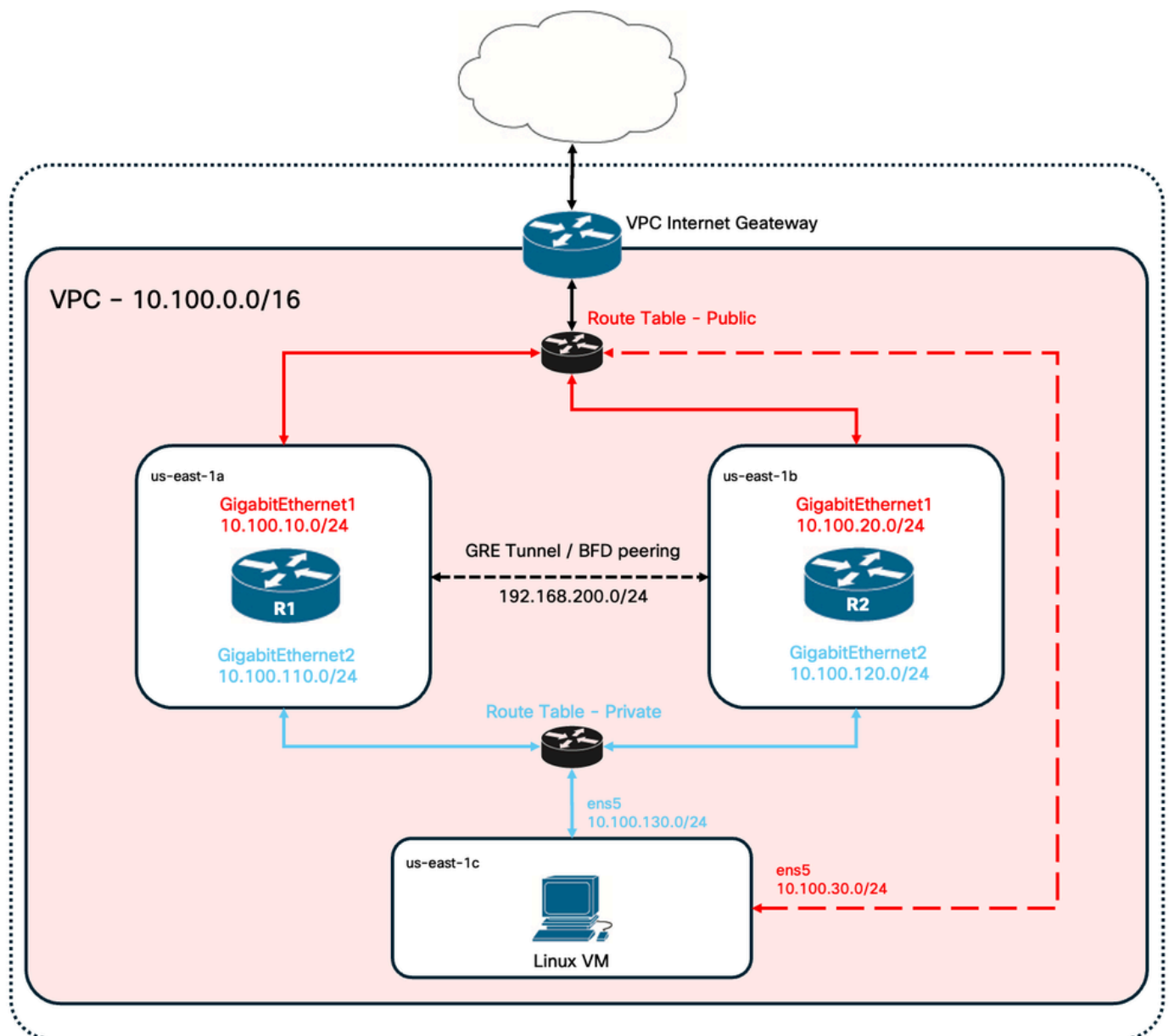
Ein HA-Paar verfügt über 2 C8000v-Router in zwei verschiedenen Verfügbarkeitszonen. Betrachten Sie jede Verfügbarkeitszone als separates Rechenzentrum für zusätzliche Hardware-Ausfallsicherheit.

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.

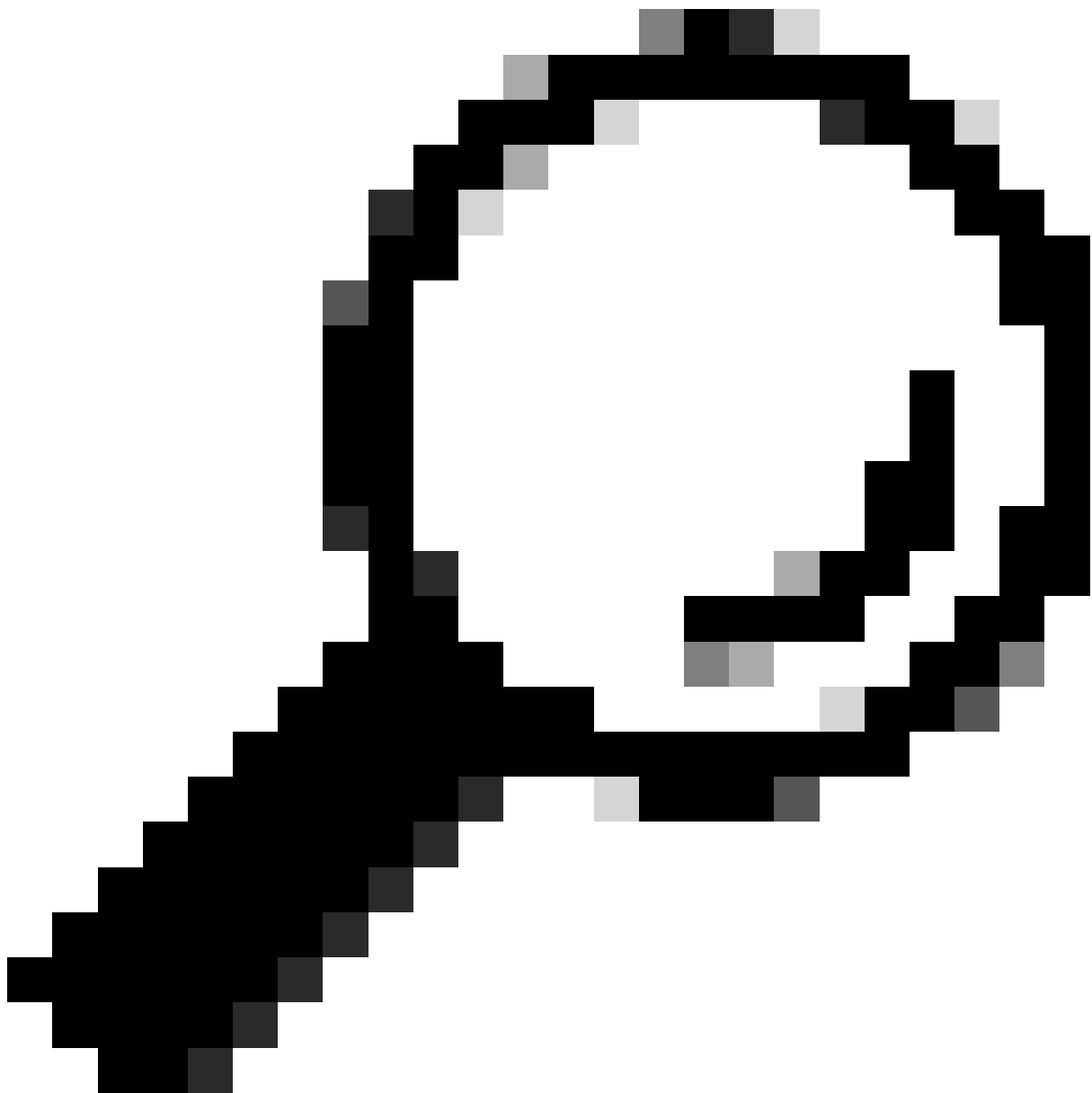
Um den Datenverkehr zu simulieren, initiieren Sie einen Ping von der privaten Schnittstelle des virtuellen Systems, der die private Routing-Tabelle über R1 durchläuft, um 8.8.8.8 zu erreichen. Stellen Sie bei einem Failover sicher, dass die private Routing-Tabelle automatisch aktualisiert wurde, um den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

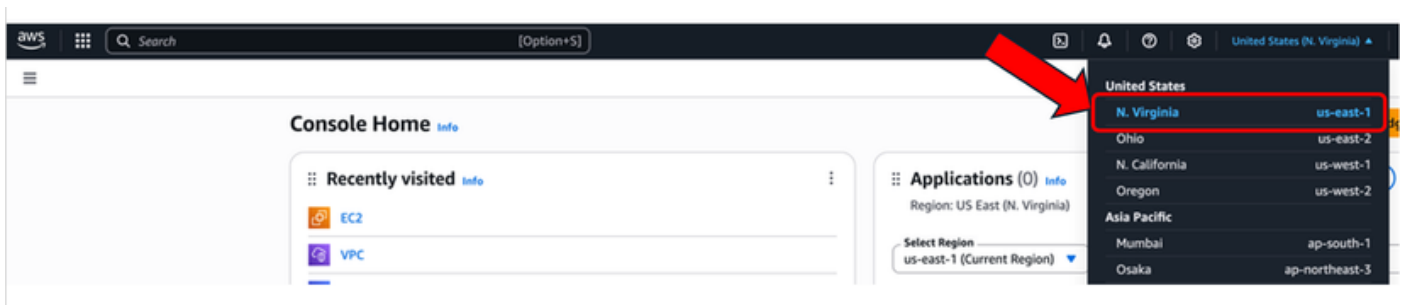
- Verwenden Sie in einem erstellten Subnetz nicht die erste verfügbare Adresse dieses Subnetzes. Diese IP-Adressen werden von den AWS-Diensten intern verwendet.
- Konfigurieren Sie nicht die öffentlichen Schnittstellen der C8000v-Geräte innerhalb einer VRF-Instanz. HA funktioniert nicht ordnungsgemäß,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

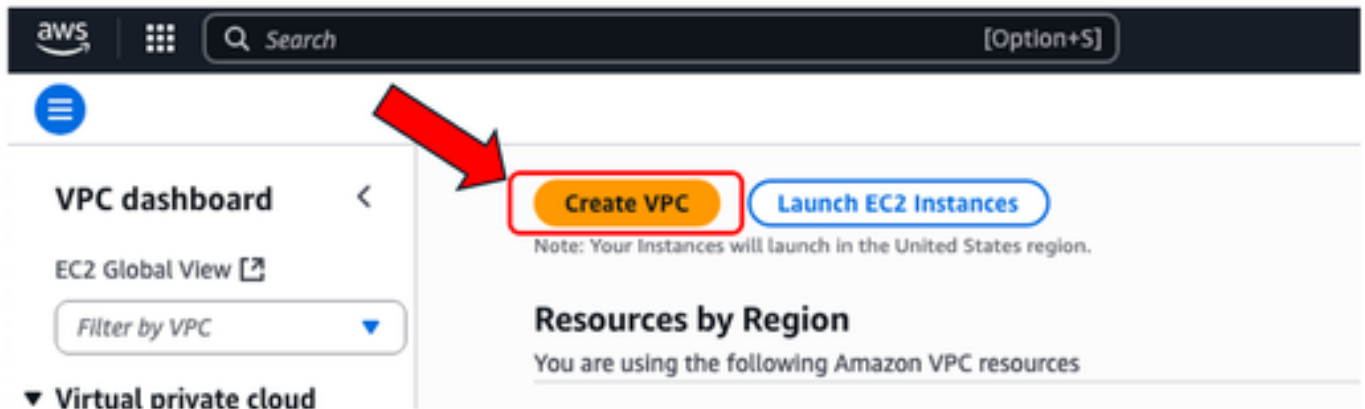
Schritt 1: Wählen Sie eine Region

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



Schritt 2: Erstellen der vPC

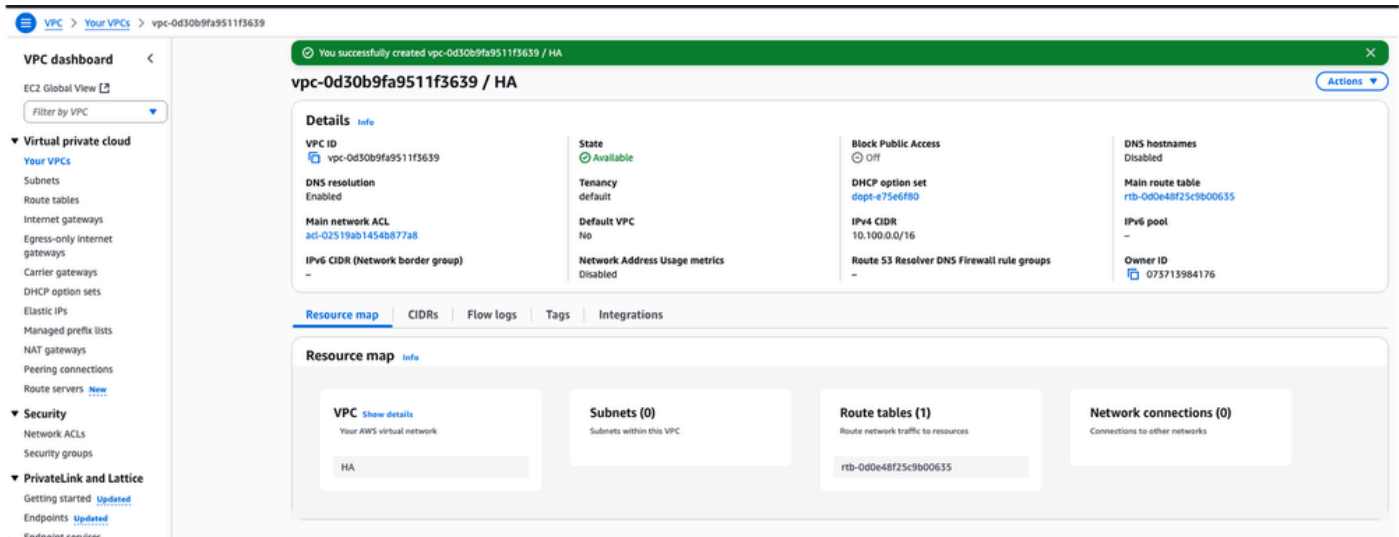
Navigieren Sie in der AWS-Konsole zu VPC > VPC Dashboard > Create VPC (VPC erstellen).



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

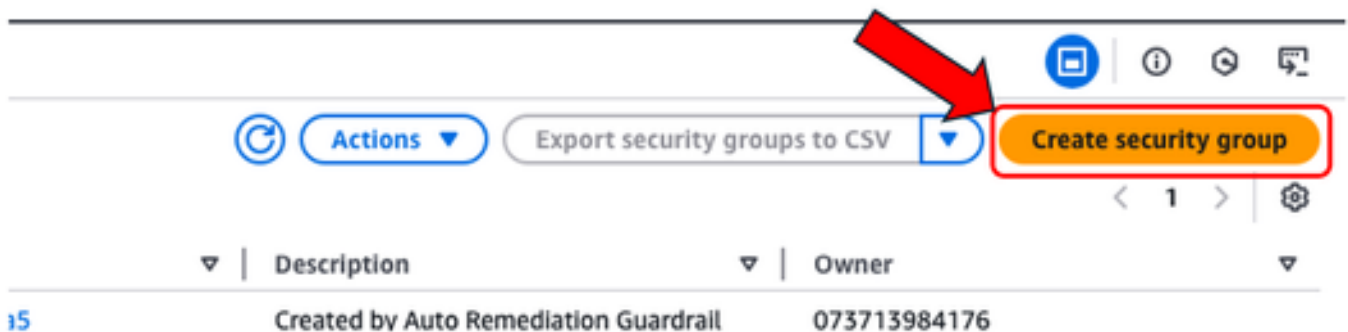
In diesem Bereitstellungsleitfaden wird das Netzwerk 10.100.0.0/16 wie folgt ausgewählt:

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.

VPC > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

All traffic HA

Name cannot be edited after creation.

Description Info

Allow all traffic on HA configuration

VPC Info

vpc-0d30b9fa9511f3639 (HA) ▼

Inbound rules Info

Type Info Protocol Info Port range Info Source Info Description - optional Info

All traffic ▼ All All Anywh... 0.0.0.0/0 0.0.0.0/0 X Delete

Add rule

Outbound rules Info

Type Info Protocol Info Port range Info Destination Info Description - optional Info

All traffic ▼ All All Custom 0.0.0.0/0 X Delete

Add rule

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Create security group

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:

AWS IAM Roles

Identity and Access Management (IAM)

Roles (65) Info Delete Create role

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

☐	Role name	Trusted entities	Last activity
☐	admin	Identity Provider: amaws:iam:0737	52 days ago
☐	AmazonAppStreamServiceAccess	AWS Service: appstream	-
☐	ApplicationAutoScalingForAmazonAppStreamAccess	AWS Service: application-autoscaling	-
☐	aws-codestar-service-role	AWS Service: codestar	-
☐	aws-elasticbeanstalk-ec2-role	AWS Service: ec2	-
☐	aws-elasticbeanstalk-service-role	AWS Service: elasticbeanstalk	-
☐	AWSCloud9SSMAccessRole	AWS Service: ec2 and 1 more	-
☐	AWSServiceRoleForAmazonSSM	AWS Service: ssm (Service-Linked Role)	42 minutes ago
☐	AWSServiceRoleForAPIGateway	AWS Service: ops.apigateway (Service-Linked Role)	-

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

- Step 1
● **Select trusted entity**
- Step 2
○ Add permissions
- Step 3
○ Name, review, and create

Select trusted entity Info

Trusted entity type

☒ **AWS service**

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**

Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

☒ **EC2**

Allows EC2 instances to call AWS services on your behalf.

☐ **EC2 Role for AWS Systems Manager**

Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

☐ **EC2 Spot Fleet Role**

Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

☐ **EC2 - Spot Fleet Auto Scaling**

Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

☐ **EC2 - Spot Fleet Tagging**

Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

☐ **EC2 - Spot Instances**

Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

☐ **EC2 - Spot Fleet**

Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

☐ **EC2 - Scheduled Instances**

Allows EC2 Scheduled Instances to manage instances on your behalf.

Cancel

Next

Wenn Sie fertig sind, klicken Sie auf Weiter:

IAM > Roles > Create role

Step 1

Step 2

Step 3

Step 4

Select trusted entity

Add permissions

Name, review, and create

Add permissions

Info

Permissions policies (1062)

Info

Choose one or more policies to attach to your new role.

Filter by Type

All types

Search

1 2 3 4 5 6 7 ... 54

☐	Policy name	Type	Description
☐	AdministratorAccess	AWS managed - job function	Provides full access to AWS services an...
☐	AdministratorAccess-Amplify	AWS managed	Grants account administrative permis...
☐	AdministratorAccess-AWSElasticBeanstalk	AWS managed	Grants account administrative permis...
☐	AIOpsAssistantPolicy	AWS managed	Provides ReadOnly permissions requir...
☐	AIOpsConsoleAdminPolicy	AWS managed	Grants full access to Amazon AI Opera...
☐	AIOpsOperatorAccess	AWS managed	Grants access to the Amazon AI Opera...
☐	AIOpsReadOnlyAccess	AWS managed	Grants ReadOnly permissions to the A...
☐	AlexaForBusinessDeviceSetup	AWS managed	Provide device setup access to AlexaFo...
☐	AlexaForBusinessFullAccess	AWS managed	Grants full access to AlexaForBusiness ...
☐	AlexaForBusinessGatewayExecution	AWS managed	Provide gateway execution access to A...
☐	AlexaForBusinessLifesizeDelegatedAccessP...	AWS managed	Provide access to Lifesize AVS devices
☐	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	Provide access to Poly AVS devices
☐	AlexaForBusinessReadOnlyAccess	AWS managed	Provide read only access to AlexaForB...
☐	AmazonAPIGatewayAdministrator	AWS managed	Provides full access to create/edit/dele...
☐	AmazonAPIGatewayInvokeFullAccess	AWS managed	Provides full access to invoke APIs in A...
☐	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	Allows API Gateway to push logs to us...
☐	AmazonAppFlowFullAccess	AWS managed	Provides full access to Amazon AppFlo...
☐	AmazonAppFlowReadOnlyAccess	AWS managed	Provides read only access to Amazon A...
☐	AmazonAppStreamFullAccess	AWS managed	Provides full access to Amazon AppStr...
☐	AmazonAppStreamPCAAccess	AWS managed	Amazon AppStream 2.0 access to AWS...

Set permissions boundary - optional

Cancel Previous Next

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

Step 1: Select trusted entity

Step 2: Add permissions

Step 3: Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

route-table-change

Maximum 64 characters. Use alphanumeric and "+,=,_,@,-" characters.

Description
Add a short explanation for this role.

Allows EC2 instances to make changes on the route table

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, @-/\[\]`#%*~!~;"',:~"

Step 1: Select trusted entities [Edit](#)

Trust policy

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "sts:AssumeRole"
8       ],
9       "Principal": {
10        "Service": [
11          "ec2.amazonaws.com"
12        ]
13      }
14    }
15  ]
16 }

```

Step 2: Add permissions [Edit](#)

Permissions policy summary

Policy name	Type	Attached as
-------------	------	-------------

Step 3: Add tags

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create role](#)

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:

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**
- Identity providers
- Account settings
- Root access management [New](#)

Access reports

- Access Analyzer

Policies (1367) [Info](#)

A policy is an object in AWS that defines permissions.

Filter by Type: All types

Search

Policy name	Type	Used as
AccessAnalyzerServiceRolePolicy	AWS managed	None
AdministratorAccess	AWS managed - job function	Permissions poli
AdministratorAccess-Amplify	AWS managed	None
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None
AIOpsAssistantPolicy	AWS managed	None
AIOpsConsoleAdminPolicy	AWS managed	None
AIOpsOperatorAccess	AWS managed	None
AIOpsReadOnlyAccess	AWS managed	None

[Create policy](#)

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:

The screenshot shows the AWS IAM Policy Editor interface. The 'Specify permissions' step is active. The 'Policy editor' section has the 'JSON' tab selected. The JSON code is as follows:

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "ec2:AssociateRouteTable",  
8         "ec2:CreateRoute",  
9         "ec2:CreateRouteTable",  
10        "ec2>DeleteRoute",  
11        "ec2>DeleteRouteTable",  
12        "ec2:DescribeRouteTables",  
13        "ec2:DescribeVpcs",  
14        "ec2:ReplaceRoute",  
15        "ec2:DisassociateRouteTable",  
16        "ec2:ReplaceRouteTableAssociation"  
17      ],  
18      "Resource": "*"   
19    }  
20  ]  
21 }
```

The 'Next' button is highlighted in the bottom right corner.

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 Richtlinienennamen fest, und klicken Sie auf Richtlinie erstellen.

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

C8000v-HA

Maximum 128 characters. Use alphanumeric and '+', '@', '-', '_' characters.

Description - optional
Add a short explanation for this policy.

Allows EC2 instances to make route changes on AWS

Maximum 1,000 characters. Use alphanumeric and '+', '@', '-', '_' characters.

Permissions defined in this policy

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (1 of 441 services) Show remaining 440 services

Service	Access level	Resource	Request condition
EC2	Limited: List, Write	All resources	None

Add tags - optional

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous **Create policy**

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.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**

Policies (1/1368)

A policy is an object in AWS that defines permissions.

Filter by Type

Search C800 All types 1 match

Policy name	Type	Used as	Description
C8000v-HA	Customer managed	None	Allows EC2 instances to make route ch...

Actions Attach Detach Delete Create policy

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).

IAM > Policies > C8000v-HA > Attach policy

Attach as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

IAM Entities (1/69)
Entities are IAM users, user groups and roles.

Search route All types 1 match

Entity name	Entity type
route-table-change	Roles

Cancel **Attach policy**

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):

The screenshot shows the AWS Management Console for the EC2 service. The left-hand navigation pane is visible, with 'Instances' selected. The main area displays 'Resources' and a 'Launch instance' button, which is highlighted with a red rectangular box. Below the button is a note about the region.

Resources	
Instances (running)	1
Dedicated Hosts	0
Key pairs	17
Security groups	19
Auto Scaling Groups	
Elastic IPs	
Load balancers	
Snapshots	

Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the United States (N. Virginia) Region

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.

The screenshot shows the 'Choose an Amazon Machine Image (AMI)' page. The search results for 'Cisco Catalyst 8000v for SD-WAN & Routing' are displayed. The 'AWS Marketplace AMIs' tab is selected, and the 'Select' button is highlighted with a red rectangular box.

Selected AMI: (ami-09e6f87a47903347c) (Quick Start AMIs)

Quick Start AMIs (0) | My AMIs (691) | **AWS Marketplace AMIs (1)** | Community AMIs (500)

Refine results

Categories: Infrastructure Software (1)

Publisher: Cisco Systems, Inc. (1)

Pricing model: Bring Your Own License (1)

Operating system: All Linux/Unix

Architecture

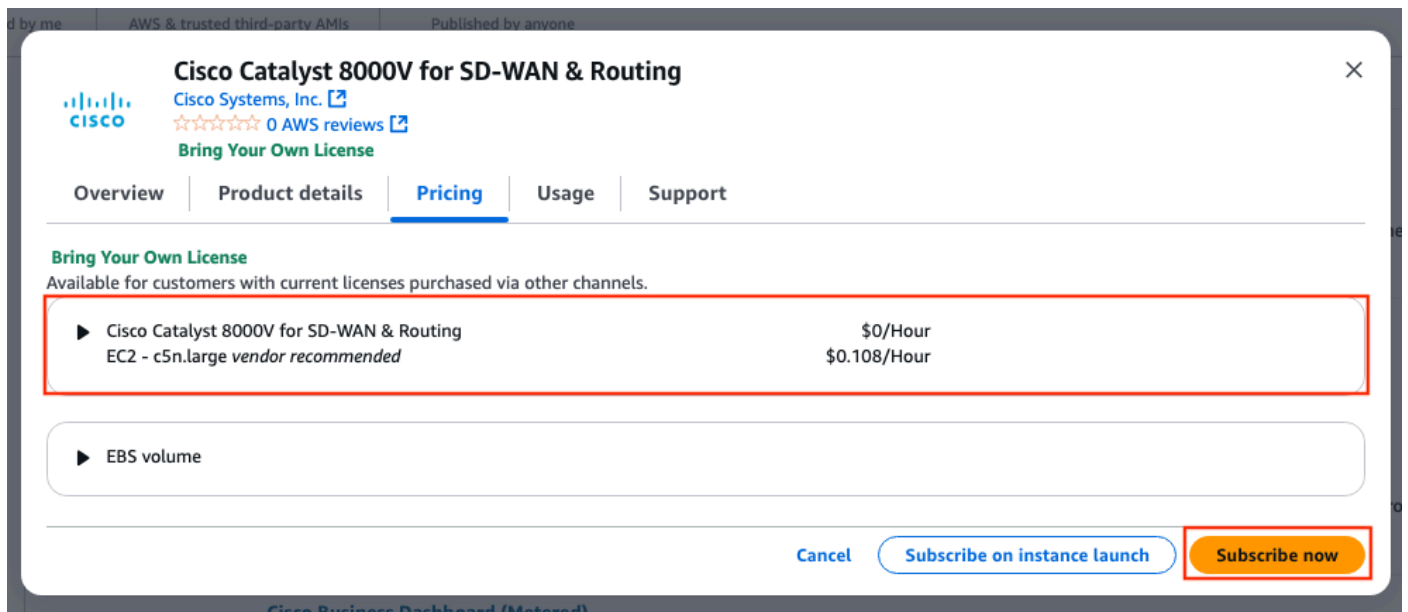
Cisco Catalyst 8000v for SD-WAN & Routing (1 result) showing 1 - 1

Sort By: Relevance

Select

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.



Cisco Catalyst 8000V for SD-WAN & Routing
Cisco Systems, Inc. [0 AWS reviews](#)
[Bring Your Own License](#)

Overview | Product details | **Pricing** | Usage | Support

Bring Your Own License
Available for customers with current licenses purchased via other channels.

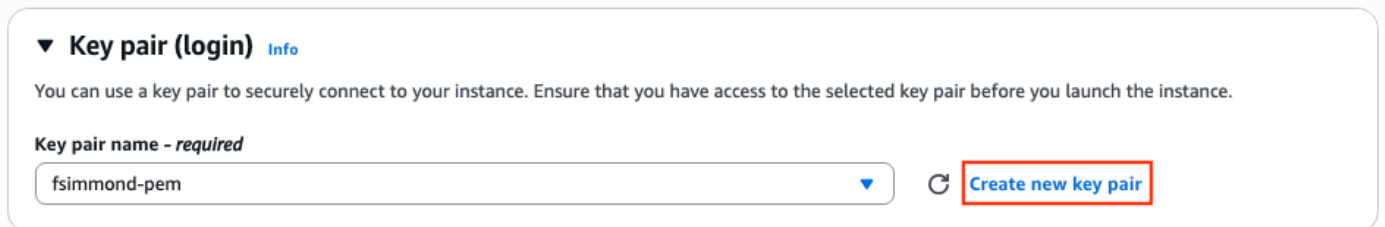
▶ Cisco Catalyst 8000V for SD-WAN & Routing EC2 - c5n.large <i>vendor recommended</i>	\$0/Hour \$0.108/Hour
--	--------------------------

▶ EBS volume

Cancel [Subscribe on instance launch](#) **Subscribe now**

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.



▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

fsimmond-pem ▼ [Create new key pair](#)

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.

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

fsimmond-ed-pem

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☐ RSA
RSA encrypted private and public key pair

☒ ED25519
ED25519 encrypted private and public key pair

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

 When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#) 

Cancel

Create key pair

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.

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-0d30b9fa9511f3639 (HA)
10.100.0.0/16

Subnet [Info](#)

subnet-0b664f8e74443d28f public-R1-C8000v
VPC: vpc-0d30b9fa9511f3639 Owner: 073713984176 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.100.10.0/24

Auto-assign public IP [Info](#)

Disable

Firewall (security groups) [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group ☒ Select existing security group

Common security groups [Info](#)

Select security groups

All traffic HA sg-029461ba80052f10c X
VPC: vpc-0d30b9fa9511f3639

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► **Advanced network configuration**

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.

☰ VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID

Choose a VPC to create the subnet in.

vpc-d30b9fa9511f3639 (HA) 1

Associated VPC CIDRs

IPv4 CIDRs

10.100.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Associate a tag with a key or "Name" and a value that you specify.

public-R1-C8000v 2

The name can be up to 256 characters long.

Availability Zone Info

Choose an Availability Zone for your subnet, or let Amazon choose one for you.

United States (N. Virginia) / us-east-1a 3

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.100.0.0/16

IPv4 subnet CIDR block

10.100.10.0/24 4

256 IPs

< > ^ v

▼ Tags - optional

Key	Value - optional	
Q Name	Q public-R1-C8000v	Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet 5

6

Cancel Create subnet

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 Netzwerkconfiguration. Diese Optionen werden angezeigt:

▼ Advanced network configuration

Network interface 1

Device index [Info](#)

0

Subnet [Info](#)

subnet-0b664f8e74443d28f

IP addresses available: 249

Primary IP [Info](#)

10.100.10.254

IPv4 Prefixes [Info](#)

Select

Delete on termination [Info](#)

No

ENA Express [Info](#)

Select

The selected instance type does not support ENA Express.

Idle connection tracking timeout [Info](#)

☐ Enable

[Add network interface](#)

Network interface [Info](#)

New interface

Security groups [Info](#)

Select security groups

Secondary IP [Info](#)

Select

IPv6 Prefixes [Info](#)

Select

The selected subnet does not support IPv6 prefixes because it does not have an IPv6 CIDR.

Interface type [Info](#)

Select

ENA Express UDP [Info](#)

Select

The selected instance type does not support ENA Express.

Description [Info](#)

Public-R1

Auto-assign public IP [Info](#)

Disable

IPv6 IPs [Info](#)

Select

The selected subnet does not support IPv6 IPs.

Assign Primary IPv6 IP [Info](#)

Select

A primary IPv6 address is only compatible with subnets that support IPv6.

Network card index [Info](#)

Select

The selected instance type does not support multiple network cards.

ENA queues [Info](#)

The selected instance type does not support ENA queues.

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:

Network interface 2

Device index [Info](#)

1

Subnet [Info](#)

subnet-0a5f13361443951d2

IP addresses available: 250

Primary IP [Info](#)

10.100.110.254

Network interface [Info](#)

New interface

Security groups [Info](#)

Select security groups

Secondary IP [Info](#)

Select

Description [Info](#)

Private-R1

Auto-assign public IP [Info](#)

Select

IPv6 IPs [Info](#)

Select

The selected subnet does not support IPv6 IPs.

[Remove](#)

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:

▼ Advanced details [Info](#)

Domain join directory | [Info](#)

Select [Create new directory](#)

IAM instance profile | [Info](#)

route-table-change
arn:aws:iam::073713984176:instance-profile/route-table-change [Create new IAM profile](#)

Hostname type | [Info](#)

IP name

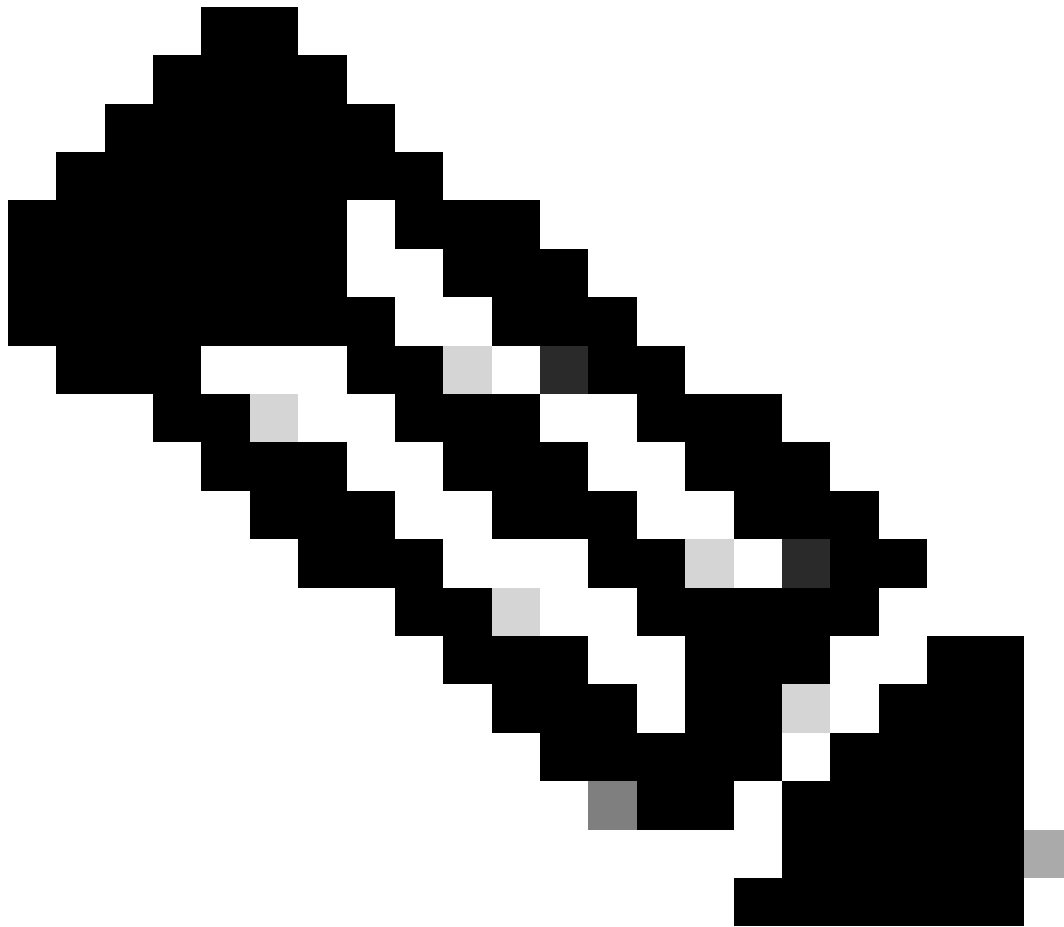
DNS Hostname | [Info](#)

- ☒ Enable IP name IPv4 (A record) DNS requests
- ☐ Enable resource-based IPv4 (A record) DNS requests
- ☐ Enable resource-based IPv6 (AAAA record) DNS requests

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.



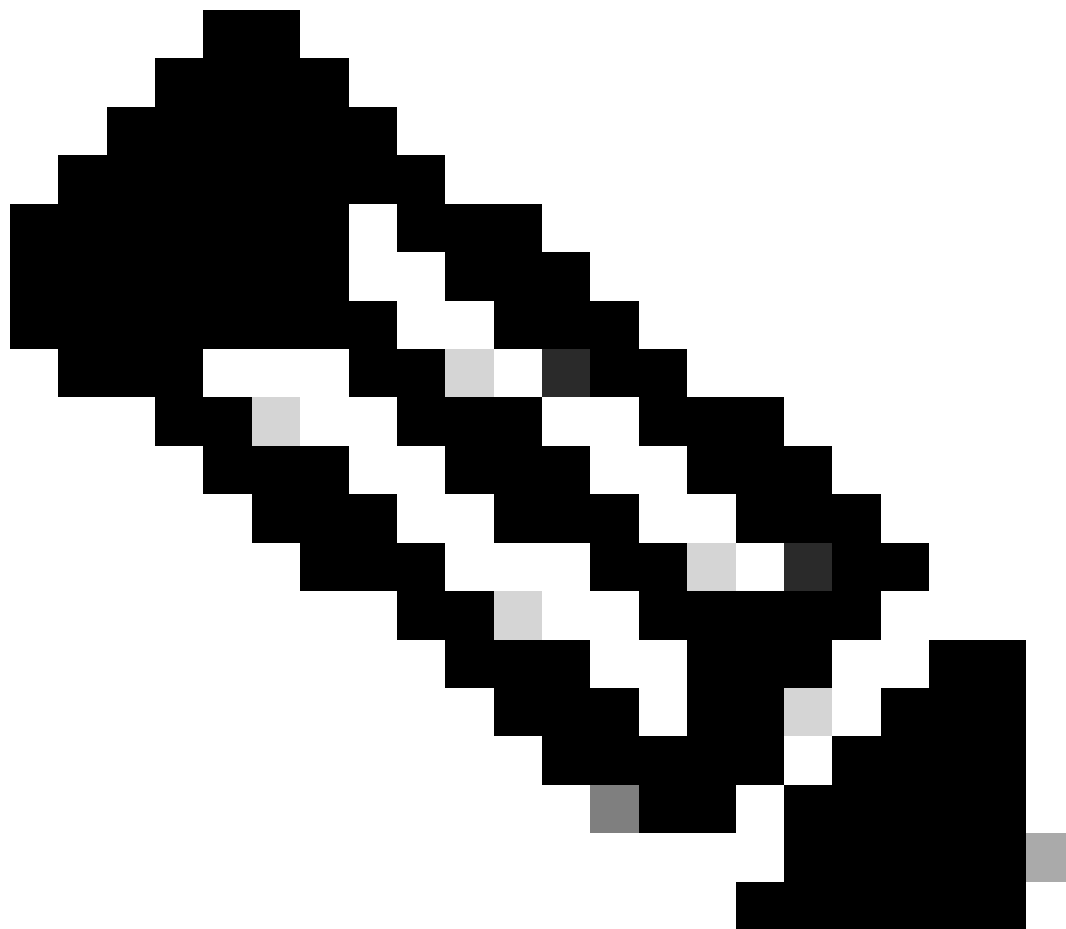
[Cancel](#)

[Launch instance](#)

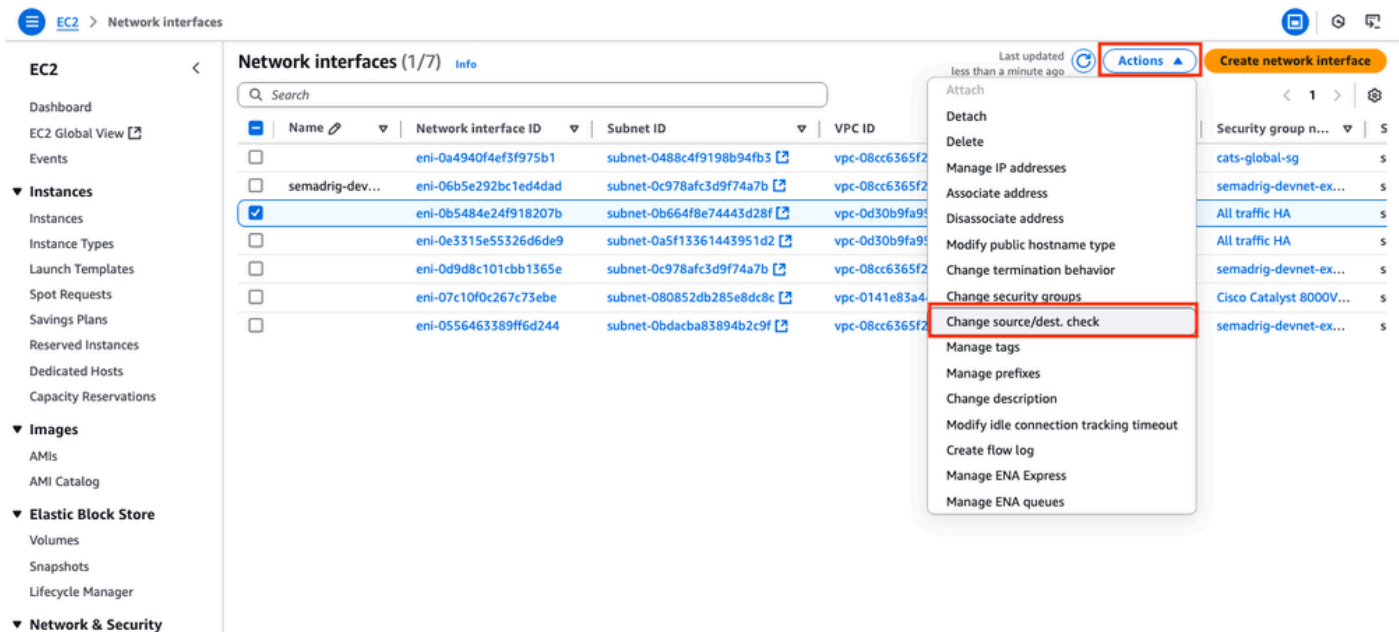
 [Preview code](#)

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

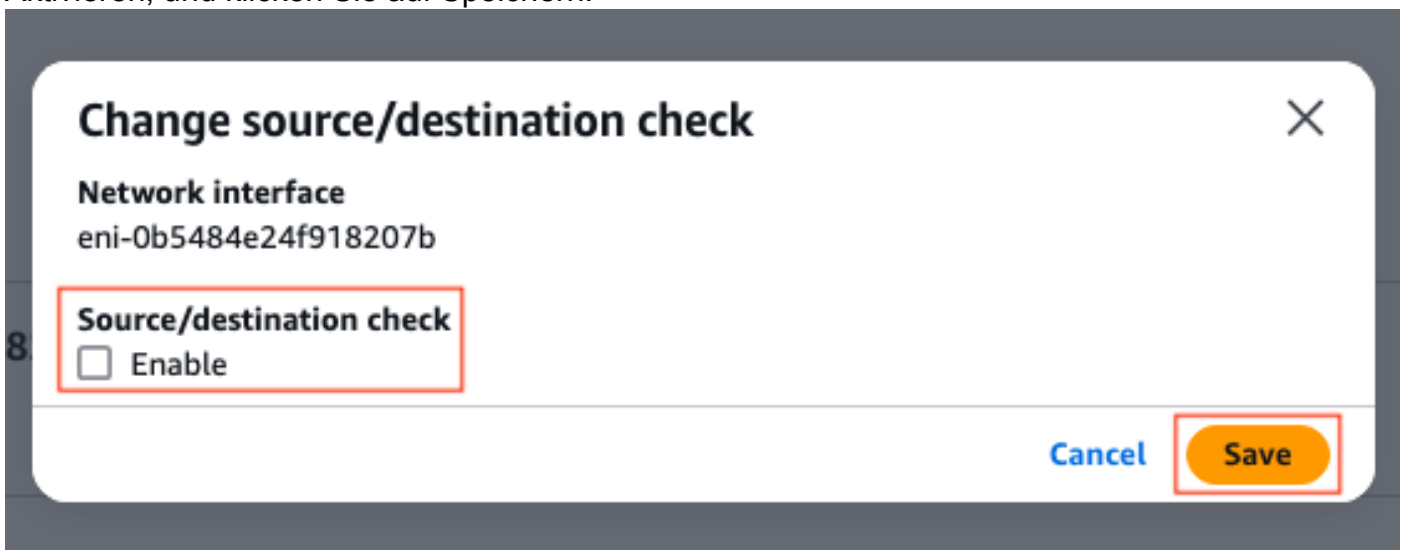
Sobald die Instanz erstellt wurde, deaktivieren Sie die src/dst-Prüffunktion in AWS, um die Verbindung zwischen Schnittstellen im gleichen Subnetz zu erhalten. Wählen Sie im Abschnitt EC2 Dashboard > Network & Security > Network interfaces (EC2-Dashboard > Netzwerk und Sicherheit > Netzwerkschnittstellen)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

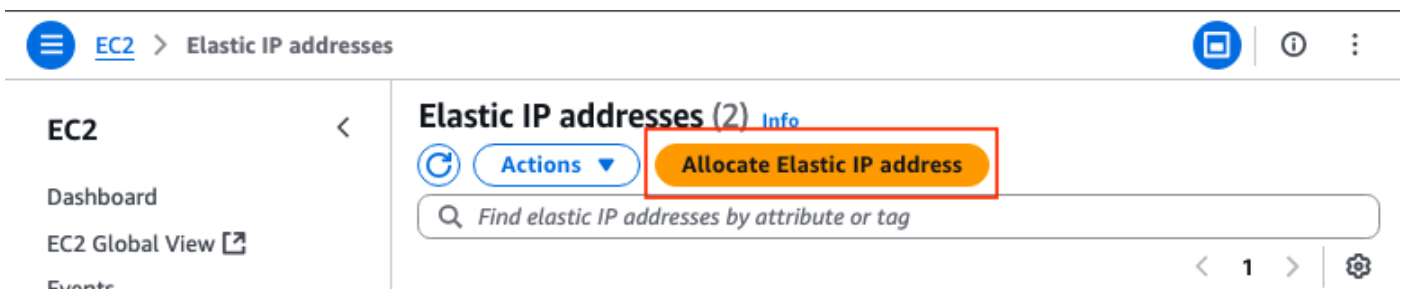


Ein neues Fenster wird angezeigt. Deaktivieren Sie im neuen Menü das Kontrollkästchen Aktivieren, und klicken Sie auf Speichern.



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.

EC2 > Elastic IP addresses > Allocate Elastic IP address

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Public IPv4 address pool

- ☒ Amazon's pool of IPv4 addresses
 - Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) [Learn more](#)
 - Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) [Learn more](#)
 - Allocate using an IPv4 IPAM pool (option disabled because no public IPv4 IPAM pools with AWS service as EC2 were found)

Network border group [Info](#)

us-east-1

Global static IP addresses
AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

[Create accelerator](#)

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
No tags associated with the resource.
[Add new tag](#)
You can add up to 50 more tag

[Cancel](#) [Allocate](#)

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).

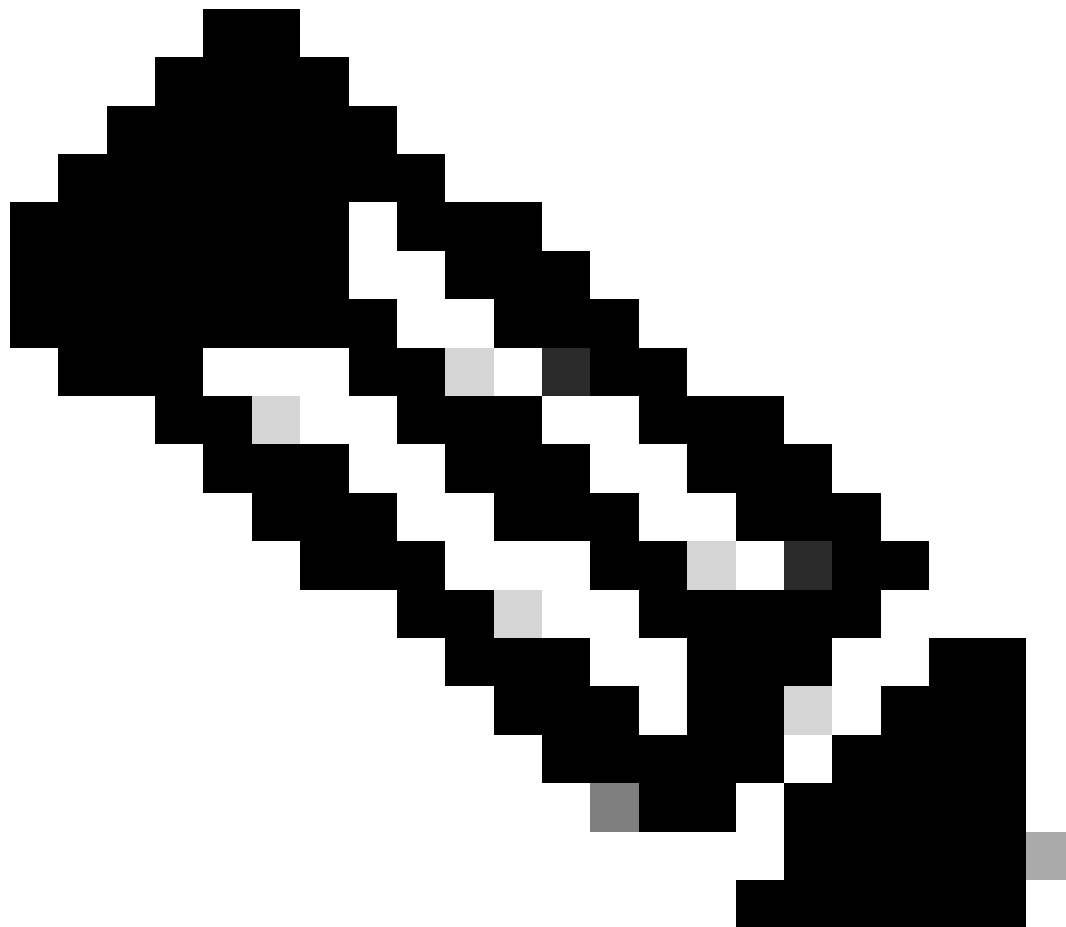
Elastic IP addresses (1/1) [Info](#)

Find elastic IP addresses by attribute or tag

Public IPv4 address [New Elastic IP address](#) [Clear filters](#)

☒	Name	Allocated IPv4 address	Type	Allocation ID	Reverse DNS record	
☒	-	192.168.1.1	Public IP	eipalloc-0948346735ab2017c	-	View details Release Elastic IP addresses Associate Elastic IP address Disassociate Elastic IP address Update reverse DNS Enable transfers Disable transfers Accept transfers

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.

Associate Elastic IP address [Info](#)

Choose the instance or network interface to associate to this Elastic IP address ([ask for help](#))

Elastic IP address: ea-2717-1000-2718

Resource type
Choose the type of resource with which to associate the Elastic IP address.
☐ Instance
☒ Network interface

⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Network interface

Private IP address
The private IP address with which to associate the Elastic IP address.

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
☒ Allow this Elastic IP address to be reassociated

[Cancel](#) [Associate](#)

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
```

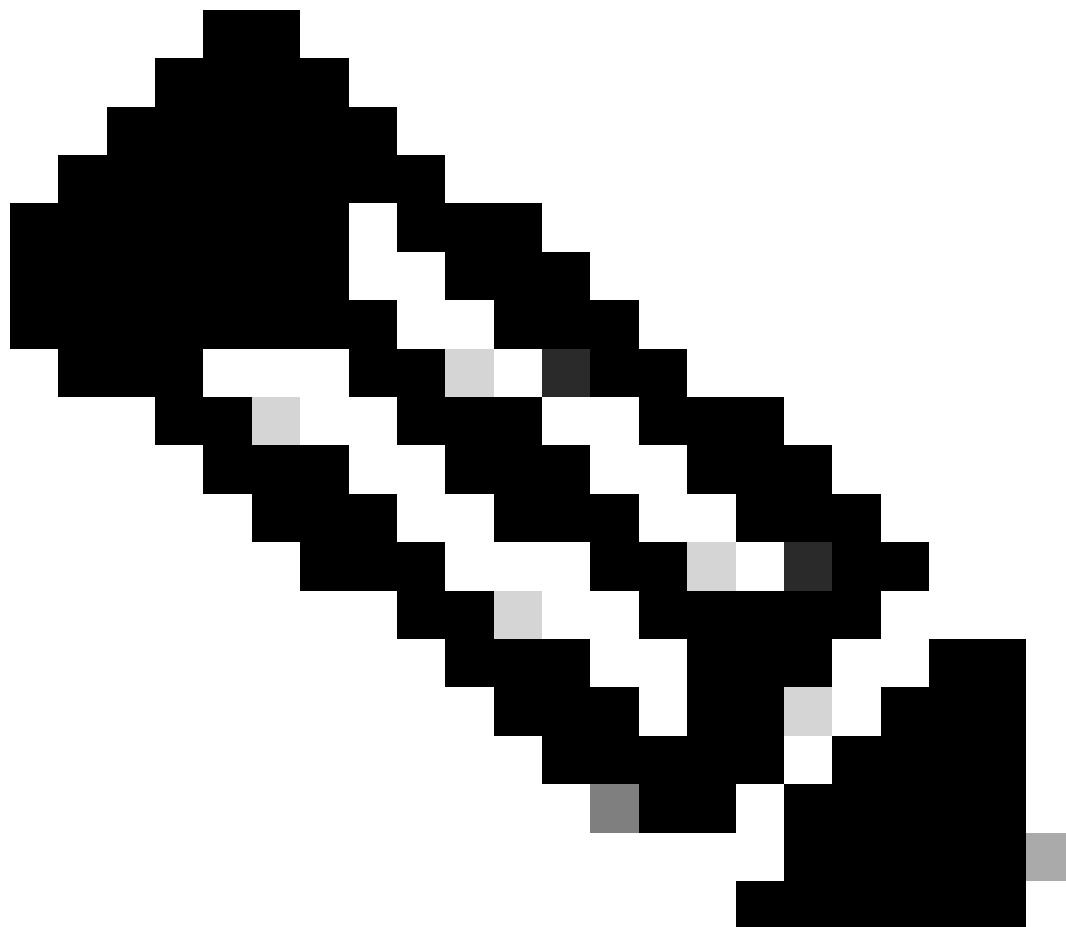
```
TX packets 1417 bytes 189934 (189.9 KB)
```

```
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

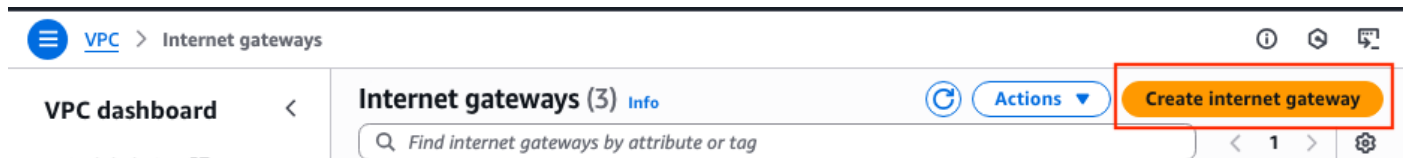
```
netmask 255.255.255.0 broadcast 10.100.130.255
inet6 fe80::3b:7eff:fead:dbe5 prefixlen 64 scopeid 0x20<link>
ether 02:3b:7e:ad:db:e5 txqueuelen 1000 (Ethernet)
RX packets 119 bytes 16831 (16.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 133 bytes 13816 (13.8 KB)
TX errors 0 dropped 0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



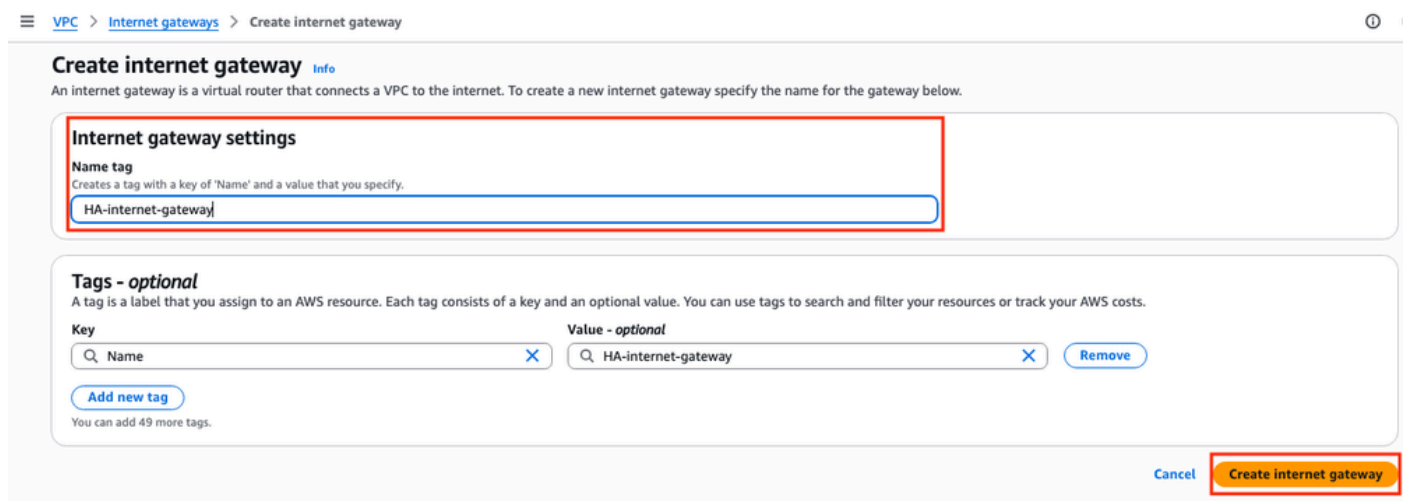
Anmerkung: Wenn Änderungen an den Schnittstellen vorgenommen werden, schlagen Sie mit der Maus über die Schnittstelle oder laden Sie die VM neu, damit diese Änderungen übernommen werden.

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**.



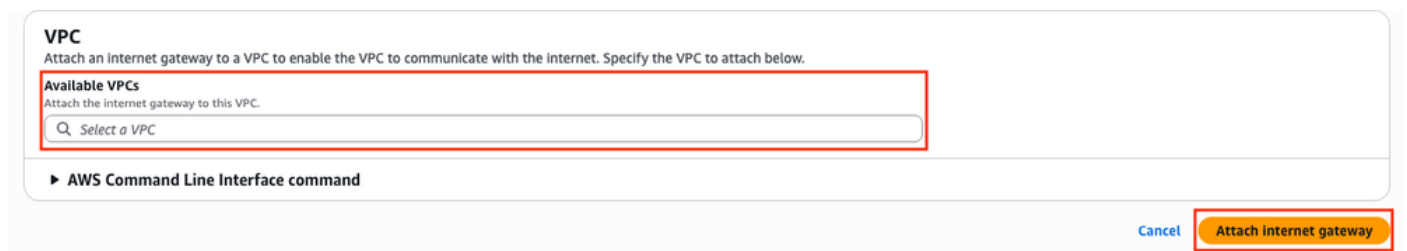
Erstellen Sie in diesem neuen Abschnitt ein **Namensschild** für dieses Gateway, und klicken Sie auf **Internet-Gateway erstellen**.



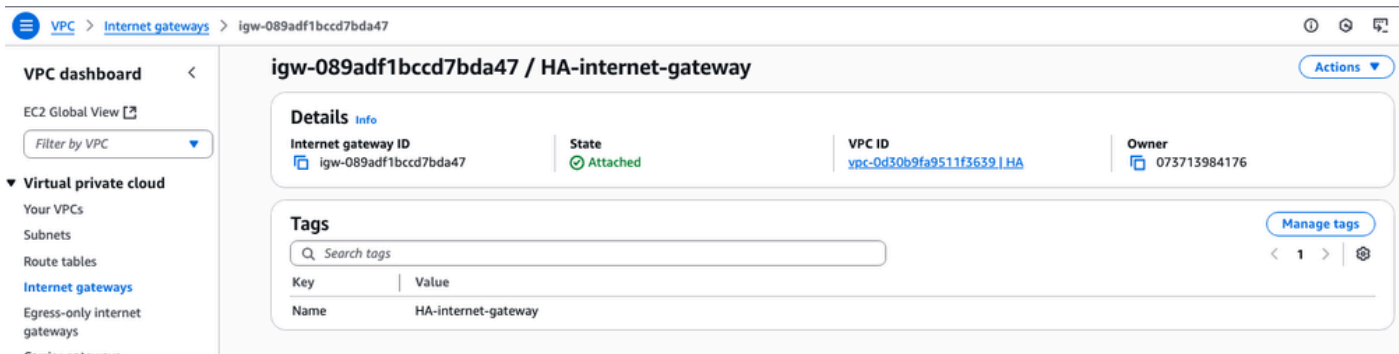
Schließen Sie das IGW nach der Erstellung an die entsprechende vPC an. Navigieren Sie zum Abschnitt **VPC Dashboard > Virtual Private Cloud > Internet Gateway**, und wählen Sie das entsprechende IGW aus. Klicken Sie auf **Aktionen > An vPC anhängen**.



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



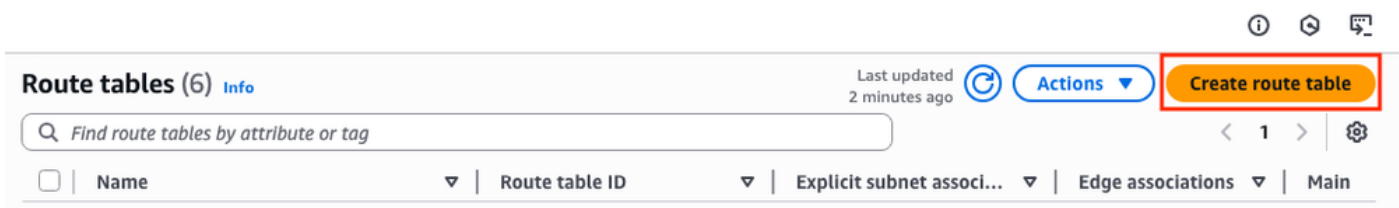
Das IGW muss den angezeigten Zustand "Attached" angeben:



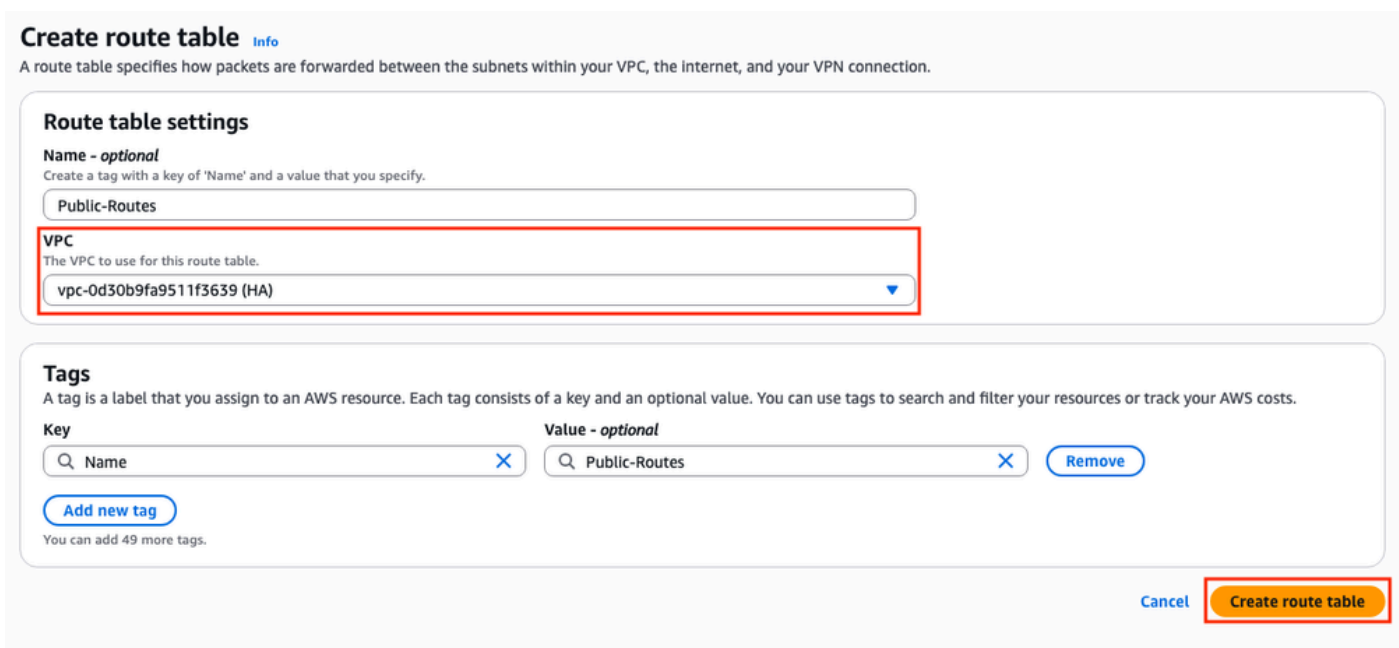
Schritt 10: Erstellen und Konfigurieren von Routing-Tabellen in AWS für öffentliche und private Subnetze

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.

VPC > Route tables

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet

Route tables (1/1) Info

Last updated 8 minutes ago

Find route tables by attribute or tag

public-routes

Clear filters

Actions

Create route table

View details

Set main route table

Edit subnet associations

Edit edge associations

Edit route propagation

Edit routes

Manage tags

Delete route table

Name	Route table ID	Explicit subnet associ...
Public-Routes	rtb-0d0e48f25c9b00635	3 subnets

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

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (3/6)

Filter subnet associations

public

Clear filters

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
public-R1-C8000v	subnet-0b664f8e74443d28f	10.100.10.0/24	-	rtb-0d0e48f25c9b00635 / Public-Routes
Public-VM-linux-1c - fsmmond	subnet-04fb9de939e3778bb	10.100.30.0/24	-	rtb-0d0e48f25c9b00635 / Public-Routes
public-R2-C8000v	subnet-02d8108842f9f3129	10.100.20.0/24	-	rtb-0d0e48f25c9b00635 / Public-Routes

Selected subnets

subnet-0b664f8e74443d28f / public-R1-C8000v

subnet-04fb9de939e3778bb / Public-VM-linux-1c - fsmmond

subnet-02d8108842f9f3129 / public-R2-C8000v

Cancel

Save associations

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:

Route tables (1/1) Info

Find route tables by attribute or tag

public-routes

Clear filters

Name	Route table ID
Public-Routes	rtb-0d0e48f25c9b00635

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:

Edit routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	Active	No

[Add route](#) [Cancel](#) [Preview](#) [Save changes](#)

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:

Edit routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	Active	No
8.8.8.8/32	Network interface	-	No

[Add route](#) [Cancel](#) [Preview](#) [Save changes](#)

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.

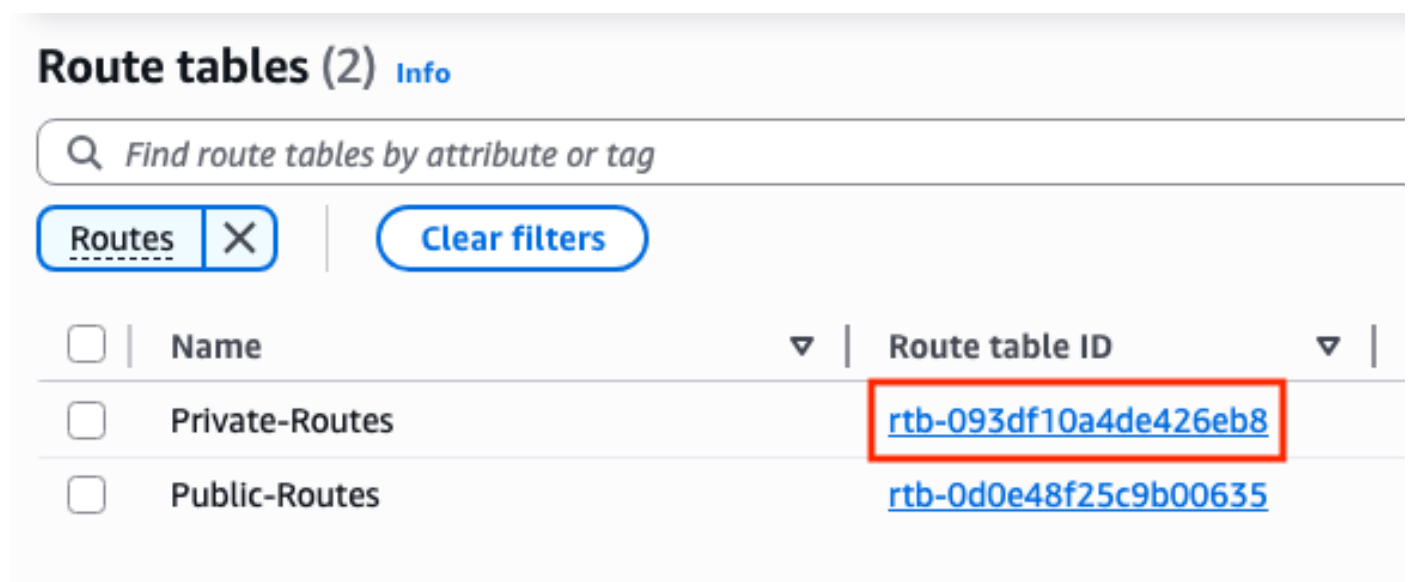
```
Router(config)# redundancy
Router(config-red)# cloud provider aws (node-id)
bfd peer <IP address of the remote device>
route-table <Route table ID>
cidr ip <traffic to be monitored/prefix>
eni <Elastic network interface (ENI) ID>
region <region-name>
```

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.



☐	Name	Route table ID
☐	Private-Routes	rtb-093df10a4de426eb8
☐	Public-Routes	rtb-0d0e48f25c9b00635

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:

rtb-093df10a4de426eb8 / Private-Routes

Details Info

Route table ID

 rtb-093df10a4de426eb8

VPC

vpc-0d30b9fa9511f3639 | HA

Main

☒ Yes

Owner ID

 073713984176

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

 *Filter routes*

Destination

8.8.8.8/32

10.100.0.0/16

▼ | Target

eni-0239fda341b4d7e41 [↗](#)

local

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:

Instances (1/3) [Info](#)

Last updated
1 minute ago

Connect

Instance state ▼

Actions

Launch instances

🔍 Find Instance by attribute or tag (case-sensitive)

All states ▼

fsimmond

[Clear filters](#)

< 1 > |

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
☐	C8000v-R2-fsimmond	I-0a1a91794f919f641	⊖ Stopped	c5n.large	–	View alarms	us-east-1b
☐	Ubuntu VM - fsimmond	I-03a306e81a0b99864	⊖ Stopped	m5.large	–	View alarms	us-east-1c
☒	C8000v-R1-fsimmond	I-0b9a50a09b089b03a	⊕ Running	c5n.large	⊕ 3/3 checks pass	View alarms	us-east-1a

i-0b9a50a09b089b03a (C8000v-R1-fsimmond)

Details | Status and alarms | Monitoring | Security | **Networking** | Storage | Tags

VPC ID
vpc-0d30b9fa9511f3639 (HA) [↗](#)

Subnet ID
 subnet-0b664f8e74443d28f (public-R1-C8000v) 

Availability zone
us-east-1a

Outpost ID

► IP addresses [Info](#)

▶ **Hostname and DNS** [Info](#)

▼ Network Interfaces (2) [Info](#)

🔍 *Filter network interfaces*

Interface ID	Device Index	Card index	Description	Public IPv4 address	Private IPv4 address	Private IPv4 DNS	IPv6
 eni-0645a881c13823696	0	0	-	104.211.9.100(100)	10.100.10.254	-	-
 eni-070e14fbfde0d8e3b	3 1	0	-	-	10.100.110.254	-	-

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
```

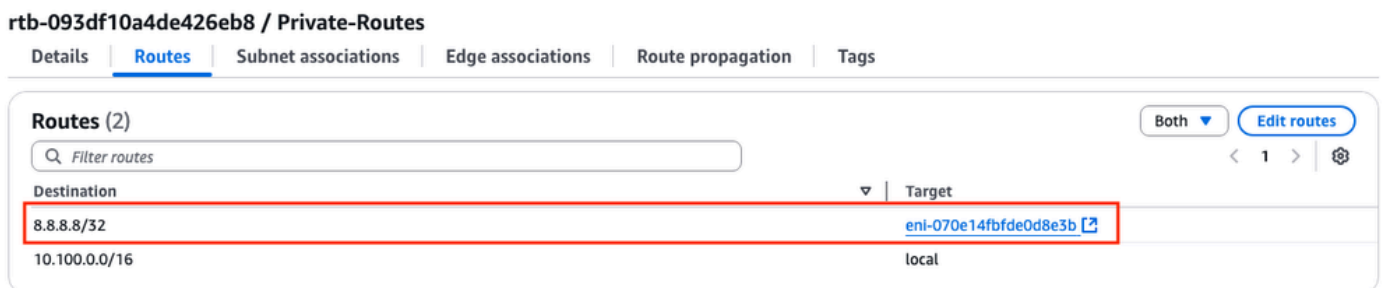
```
0 192.168.200.2 Tu1 10 00:16:52 2 1470 0 2
```

```
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:

Routes (2)

Destination



Target

8.8.8.8/32

[eni-0239fda341b4d7e41](#)

10.100.0.0/16

local

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.