

C8000v High Availability Configuration implementeren op AWS

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Topologie](#)

[Netwerkdigram](#)

[Tabeloverzicht](#)

[Beperkingen](#)

[Configuratie](#)

[Stap 1. Selecteer een regio](#)

[Stap 2. De VPC maken](#)

[Stap 3. Een beveiligingsgroep voor de VPC maken](#)

[Stap 4. Maak een IAM-rol met een beleid en koppel aan de VPC](#)

[Stap 5. Een vertrouwensbeleid maken en koppelen aan een IAM-rol](#)

[Stap 6. De C8000v-exemplaren configureren en starten](#)

[Stap 6.1. Het sleutelpaar configureren voor externe toegang](#)

[Stap 6.2. De subnetten voor de AMI maken en configureren](#)

[Stap 6.3. De AMI-interfaces configureren](#)

[Stap 6.4. Stel het IAM-instantieprofiel in op de AMI](#)

[Stap 6.5. \(Optioneel\) Stel de referenties in op de AMI](#)

[Stap 6.6. De instantieconfiguratie voltooien](#)

[Stap 6.7. Bron-/bestemmingscontrole op de ENI's uitschakelen](#)

[Stap 6.8. Een elastisch IP maken en koppelen aan het openbare ENI van de instantie](#)

[Stap 7. Herhaal stap 6 om de tweede C8000v-instantie voor HA te maken](#)

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

[Stap 9. Een Internet Gateway \(IGW\) voor de VPC maken en configureren](#)

[Stap 10. Routetabellen maken en configureren op AWS voor publieke en private subnetten](#)

[Stap 10.1. De openbare routetabel maken en configureren](#)

[Stap 10.2. De privéroudetabel maken en configureren](#)

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

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

[Verificatie](#)

[Problemen oplossen](#)

Inleiding

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

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

Voorwaarden

Vereisten

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

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

Gebruikte componenten

Deze onderdelen zijn vereist voor dit configuratievoorbeeld:

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

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

Topologie

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

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

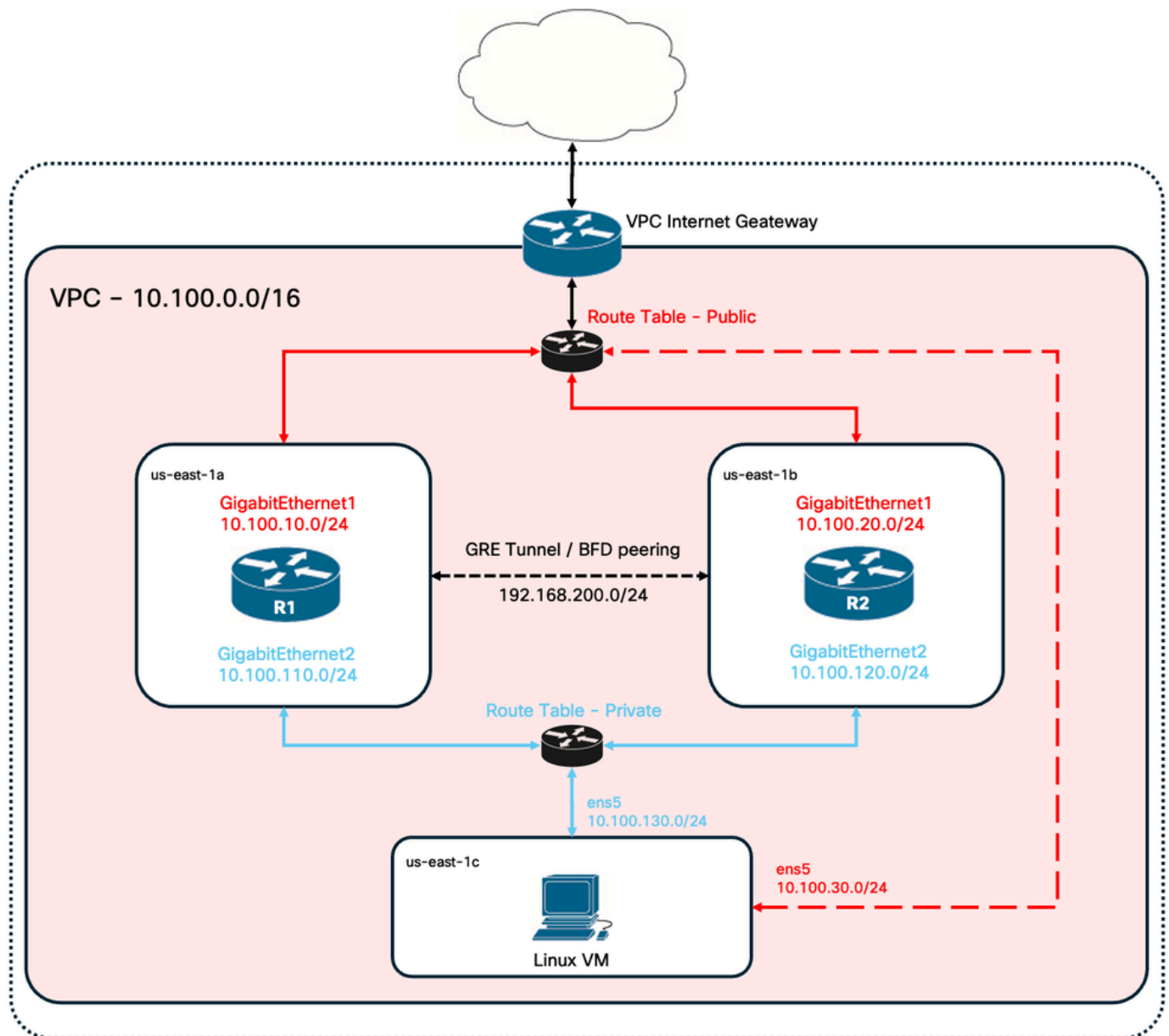
Er zijn 2 C8000v-routers in een HA-paar, in twee verschillende beschikbaarheidszones. Beschouw elke beschikbaarheidszone als een afzonderlijk datacenter voor extra hardwarematige veerkracht.

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

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

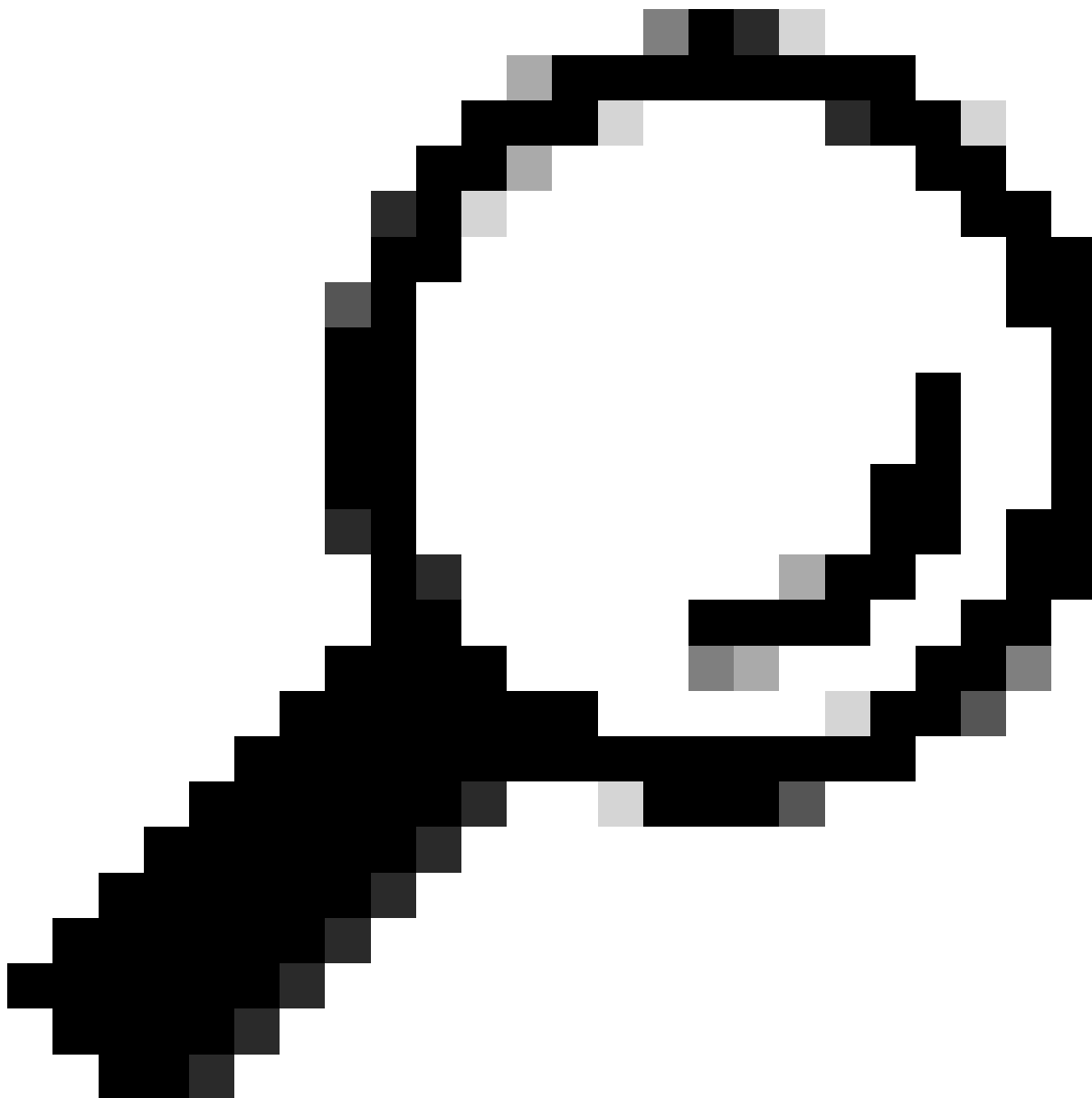
doorloopt u de privé-routetabel door R1 om 8.8.8.8 te bereiken. Controleer in het geval van een failover of de privé-routetabel automatisch is bijgewerkt om het verkeer door de privé-interface van de R2-router te leiden.

Netwerkdigram



Tabeloverzicht

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



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

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

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

Beperkingen

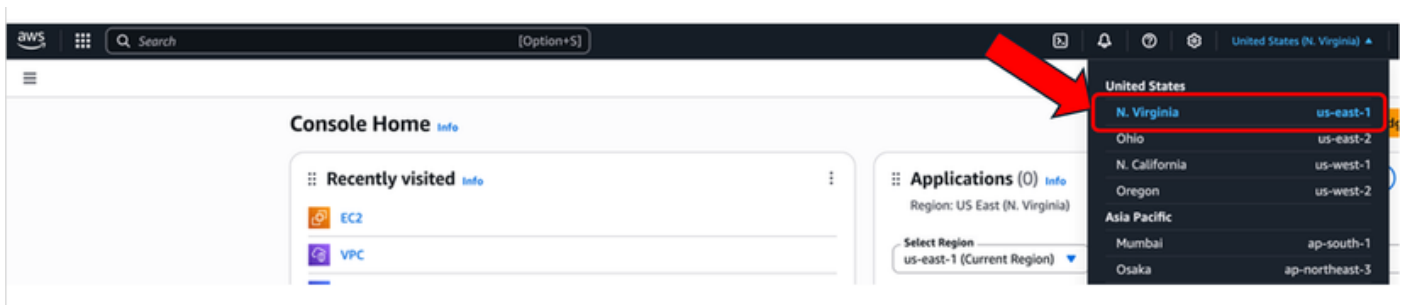
- Gebruik op een gemaakt subnet niet het eerste beschikbare adres van dat subnet. Deze IP-adressen worden intern door de AWS-diensten gebruikt.
- Configureer de openbare interfaces van de C8000v-apparaten niet in een VRF. HA werkt niet goed als dit is ingesteld.

Configuratie

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

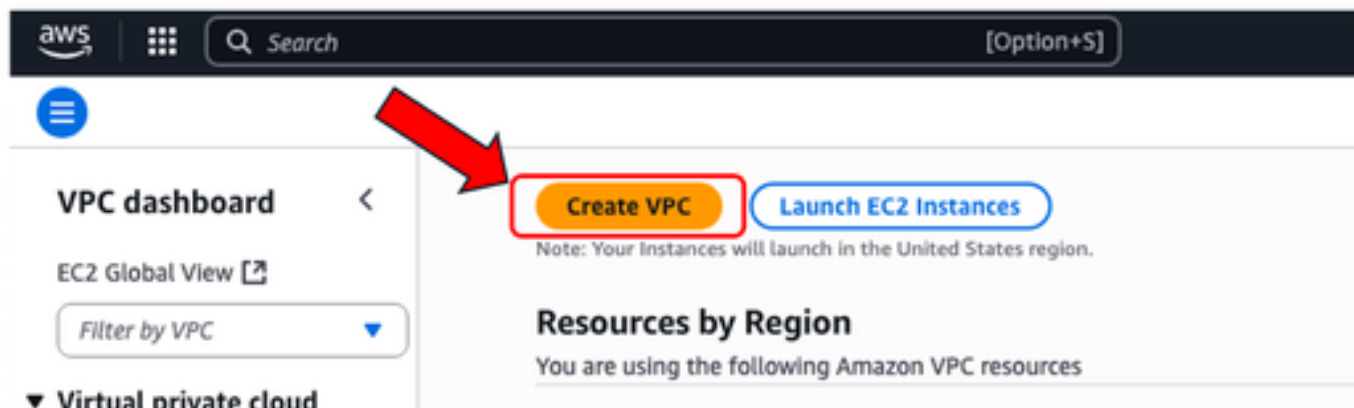
Stap 1. Selecteer een regio

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



Stap 2. De VPC maken

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



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

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

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

VPC > Your VPCs > vpc-0d30b9fa9511f3639

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

Security

Network ACLs

Security groups

PrivateLink and Lattice

Getting started

Endpoints

Endpoint services

You successfully created vpc-0d30b9fa9511f3639 / HA

vpc-0d30b9fa9511f3639 / HA

Details

VPC ID: vpc-0d30b9fa9511f3639

DNS resolution: Enabled

Main network ACL: acl-02519ab1454b877a8

IPv6 CIDR (Network border group): -

State: Available

Tenancy: default

Default VPC: No

Network Address Usage metrics: Disabled

Block Public Access: Off

DHCP option set: dhcp-475cd6f80

IPv4 CIDR: 10.100.0.0/16

Route 53 Resolver DNS Firewall rule groups: -

DNS hostnames: Disabled

Main route table: rtb-0d0e48f25c9b00635

IPv6 pool: -

Owner ID: 073713984176

Resource map

CIDRs | Flow logs | Tags | Integrations

VPC (Show details)

Your AWS virtual network

HA

Subnets (0)

Subnets within this VPC

Route tables (1)

Route network traffic to resources

rtb-0d0e48f25c9b00635

Network connections (0)

Connections to other networks

Stap 3. Een beveiligingsgroep voor de VPC maken

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

Actions

Export security groups to CSV

Create security group

15

Description	Owner
Created by Auto Remediation Guardrail	073713984176

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

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

Name cannot be edited after creation.

Description info

VPC info

Inbound rules info

Type	Protocol	Port range	Source	Description - optional	
All traffic	All	All	Anywhere...		Delete
			0.0.0.0/0		
			0.0.0.0/0		

Add rule

Outbound rules info

Type	Protocol	Port range	Destination	Description - optional	
All traffic	All	All	Custom		Delete
			0.0.0.0/0		

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

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

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

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

AWS IAM Roles (65)

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)	-

Create role

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

- 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

Als u klaar bent, klikt u op Volgende:

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

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

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](#)

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

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

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

Search

All types

< 1 2 3 4 5 6 7 ... 69 > [Settings](#)

	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

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

The screenshot shows the AWS IAM Policy Editor interface. The breadcrumb navigation at the top indicates the path: IAM > Policies > Create policy. The left sidebar shows two steps: 'Specify permissions' (selected) and 'Review and create'. The main area is titled 'Specify permissions' and includes a sub-header 'Policy editor'. At the top of the editor, there are three tabs: 'Visual', 'JSON' (which is selected and highlighted with a red box), and 'Actions'. Below the tabs, the JSON editor contains a pre-defined policy document for EC2 route table actions. The JSON text 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 }
```

Below the JSON editor, there is a '+ Add new statement' button. To the right of the JSON editor is a panel titled 'Edit statement' with the text 'Select a statement' and 'Select an existing statement in the policy or add a new statement.' Below this text is a '+ Add new statement' button. At the bottom of the editor, there is a status bar showing 'JSON Ln 21, Col 1' and '5825 of 6144 characters remaining'. Below the status bar, there are icons for 'Security: 0', 'Errors: 0', 'Warnings: 0', and 'Suggestions: 0'. At the bottom right of the interface, there are 'Cancel' and 'Next' buttons, with the 'Next' button highlighted by a red box.

Dit is de tekst die in de afbeelding wordt gebruikt:

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

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

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**

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

IAM > Policies

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

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

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**

Stap 6. De C8000v-instanties configureren en starten

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

beschikbaarheidszone.

Klik op het EC2-dashboard op Instanties starten:

The screenshot shows the AWS Management Console EC2 dashboard. The left sidebar contains the navigation menu with 'EC2' selected. The main content area displays 'Resources' and a 'Launch instance' button highlighted with a red box.

Resources

You are using the following Amazon EC2 resources in the United States (N. Virgin

Resource	Count
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.

Launch instance **Migrate a server**

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

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

The screenshot shows the 'Choose an Amazon Machine Image (AMI)' page. The search bar contains 'Cisco Catalyst 8000v for SD-WAN & Routing'. The 'AWS Marketplace AMIs (1)' tab is selected, showing the 'Cisco Catalyst 8000v for SD-WAN & Routing' AMI. The 'Select' button is highlighted with a red box.

Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

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

Q Cisco Catalyst 8000v for SD-WAN & Routing

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

Cisco Catalyst 8000v for SD-WAN & Routing

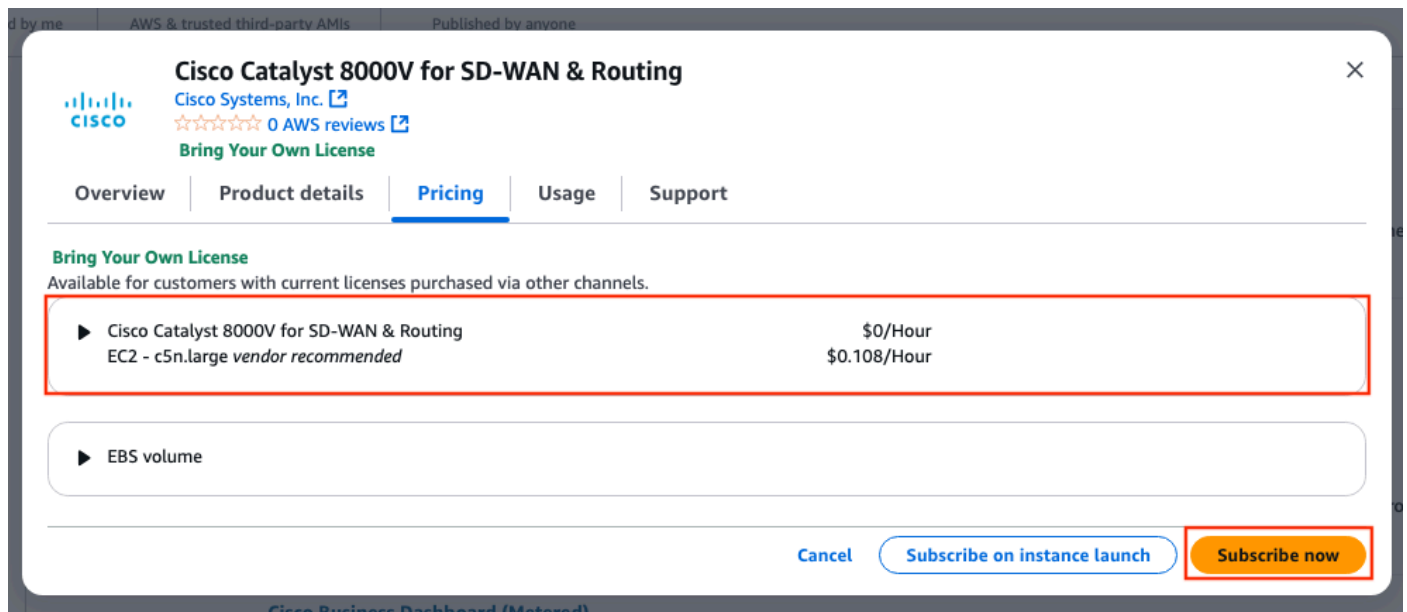
By Cisco Systems, Inc. | Ver 17.15.03a

As part of Cisco's Cloud connect portfolio, the Bring Your Own License (BYOL) version of Cisco® Catalyst® 8000V Edge Software (Catalyst 8000V) delivers the maximum performance for virtual enterprise-class networking services & VPN in the AWS cloud. This AMI supports all the Catalyst 8000V (C8000V)...

Select

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

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



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.

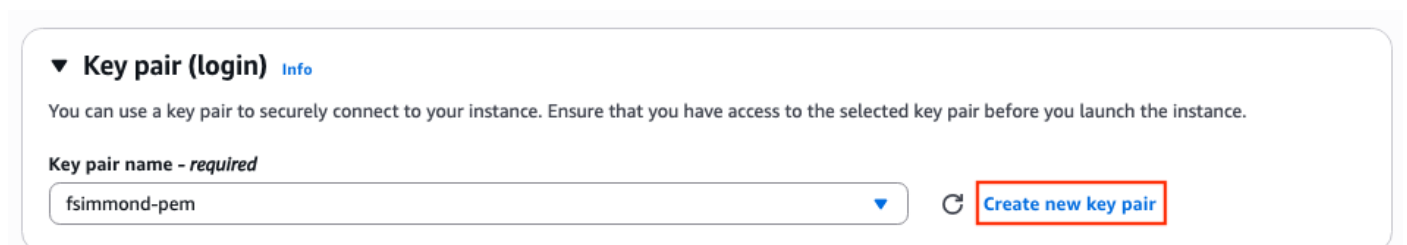
▶ Cisco Catalyst 8000V for SD-WAN & Routing EC2 - c5n.large <i>vendor recommended</i>	\$0/Hour \$0.108/Hour
--	--------------------------

▶ EBS volume

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

Stap 6.1. Het sleutelpaar configureren voor externe toegang

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



▼ **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](#)

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

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

Stap 6.2. De subnetten voor de AMI maken en configureren

Klik in het gedeelte Netwerkinstellingen op Bewerken. Enkele nieuwe opties in de sectie zijn nu beschikbaar:

1. Selecteer de gewenste VPC voor dit werk. In dit voorbeeld wordt de VPC met de naam HA geselecteerd.
2. Selecteer in het gedeelte Firewall (beveiligingsgroepen) de optie Selecteer bestaande beveiligingsgroep.
3. Zodra optie 2 is geselecteerd, is de optie Gemeenschappelijke beveiligingsgroepen beschikbaar. Filter en selecteer de gewenste beveiligingsgroep. In dit voorbeeld wordt de beveiligingsgroep Alle HA-verkeer geselecteerd.

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

The screenshot shows the 'Network settings' page in the AWS Management Console. It includes sections for VPC, Subnet, Auto-assign public IP, Firewall (security groups), and Common security groups. Red boxes and numbers highlight specific elements: 1. The VPC dropdown menu. 2. The 'Select existing security group' button. 3. The 'Compare security group rules' link. 4. The 'Create new subnet' button.

▼ 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

[Compare security group rules](#)

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

► **Advanced network configuration**

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

1. Selecteer de bijbehorende VPC voor deze configuratie in de vervolgkeuzelijst.
2. Stel een naam in voor het nieuwe subnet.
3. Definieer de beschikbaarheidszone voor dit subnet. (Raadpleeg de sectie Topologie van dit document voor meer informatie over de instelling)
4. Stel het subnetblok in dat hoort bij het VPC CIDR-blok.
5. Bovendien kunnen alle subnetten die worden gebruikt, worden gemaakt door op het gedeelte Nieuw subnet toevoegen te klikken en de stappen van 2 tot 4 voor elk subnet te herhalen.
6. Als u klaar bent, klikt u op Subnet maken. Navigeer naar de vorige pagina om verder te gaan met de instellingen.

☰ VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID

vpce-0d30b9fa9511f3639 (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

public-R1-CB000v 2

The name can be up to 256 characters long.

Availability Zone Info

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 4

10.100.10.0/24 256 IPs

< > ^ v

▼ Tags - optional

Key	Value - optional	
Q Name	Q public-R1-CB000v	Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet 5

6

Cancel Create subnet

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

Stap 6.3. De AMI-interfaces configureren

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

▼ 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.

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

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

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

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

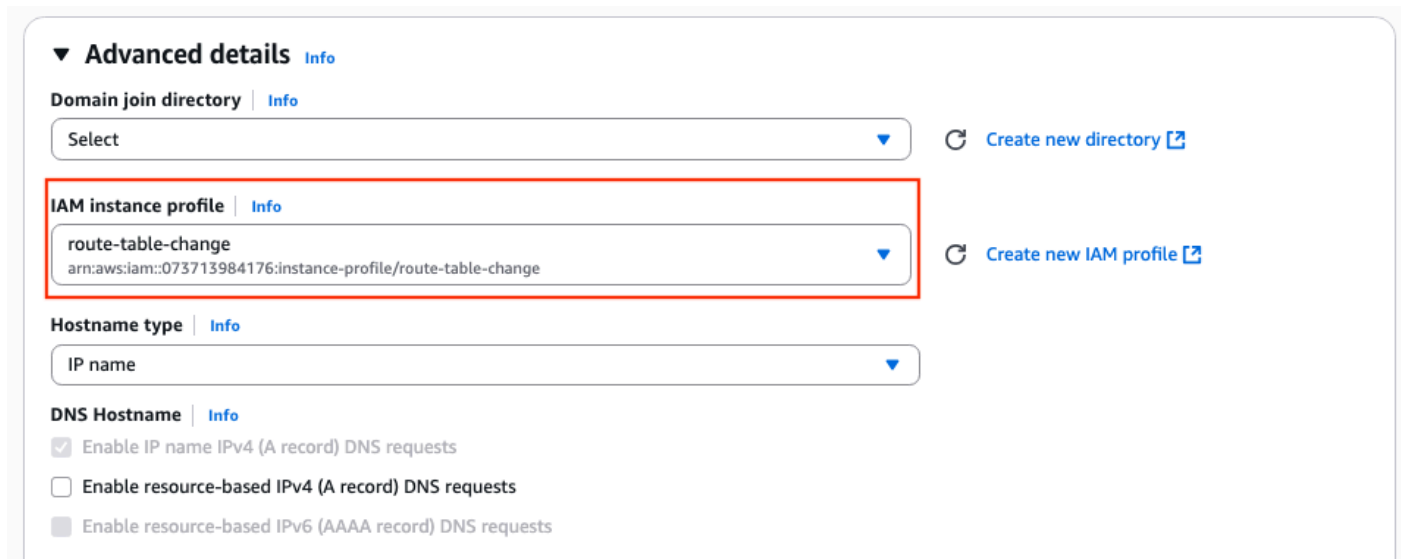
The selected subnet does not support IPv6 IPs.

[Remove](#)

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

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

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



▼ 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

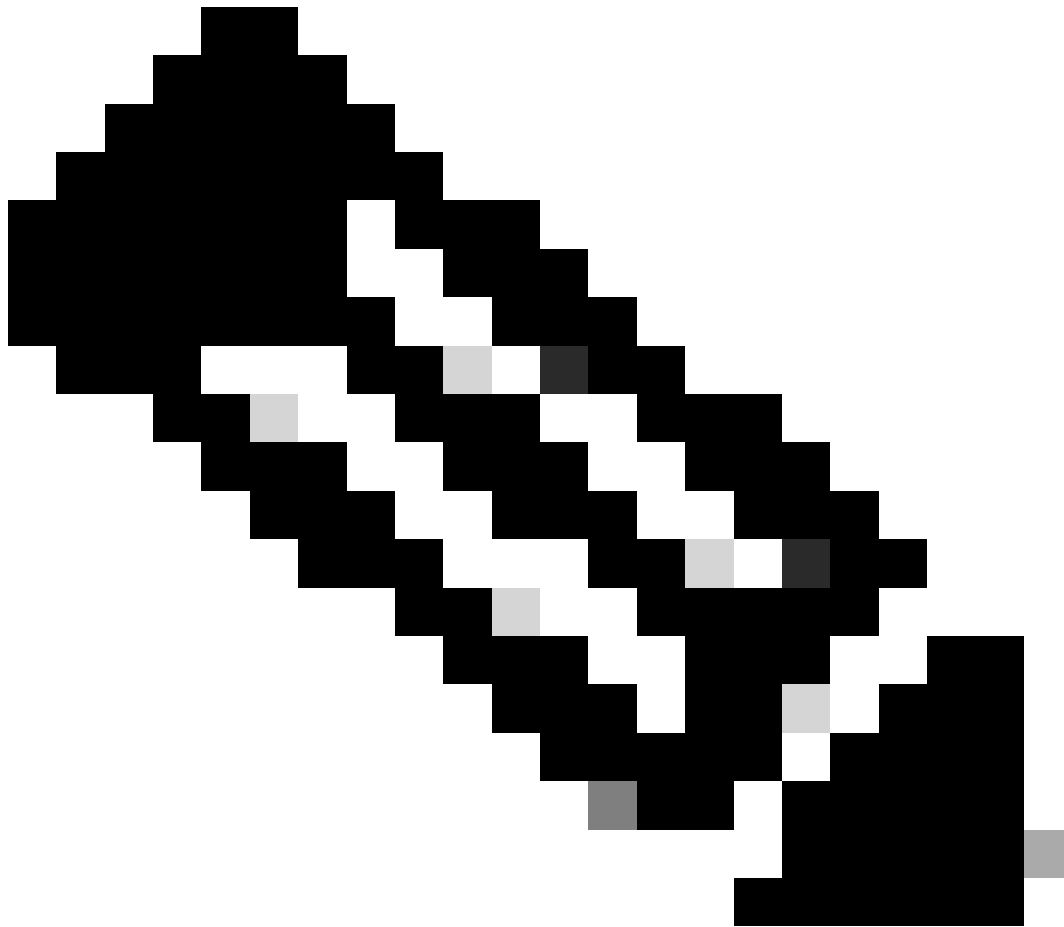
DNS Hostname | [Info](#)

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

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

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

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



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

Stap 6.6. De instantieconfiguratie voltooien

Als alles is geconfigureerd, klikt u op Installatie starten:

▼ Summary

Number of instances | [Info](#)

1

Software Image (AMI)

Cisco Catalyst 8000V for SD-WA...[read more](#)

ami-03cc286883c62bdee

Virtual server type (instance type)

c5n.large

Firewall (security group)

All traffic HA

Storage (volumes)

1 volume(s) - 16 GiB



Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



[Cancel](#)

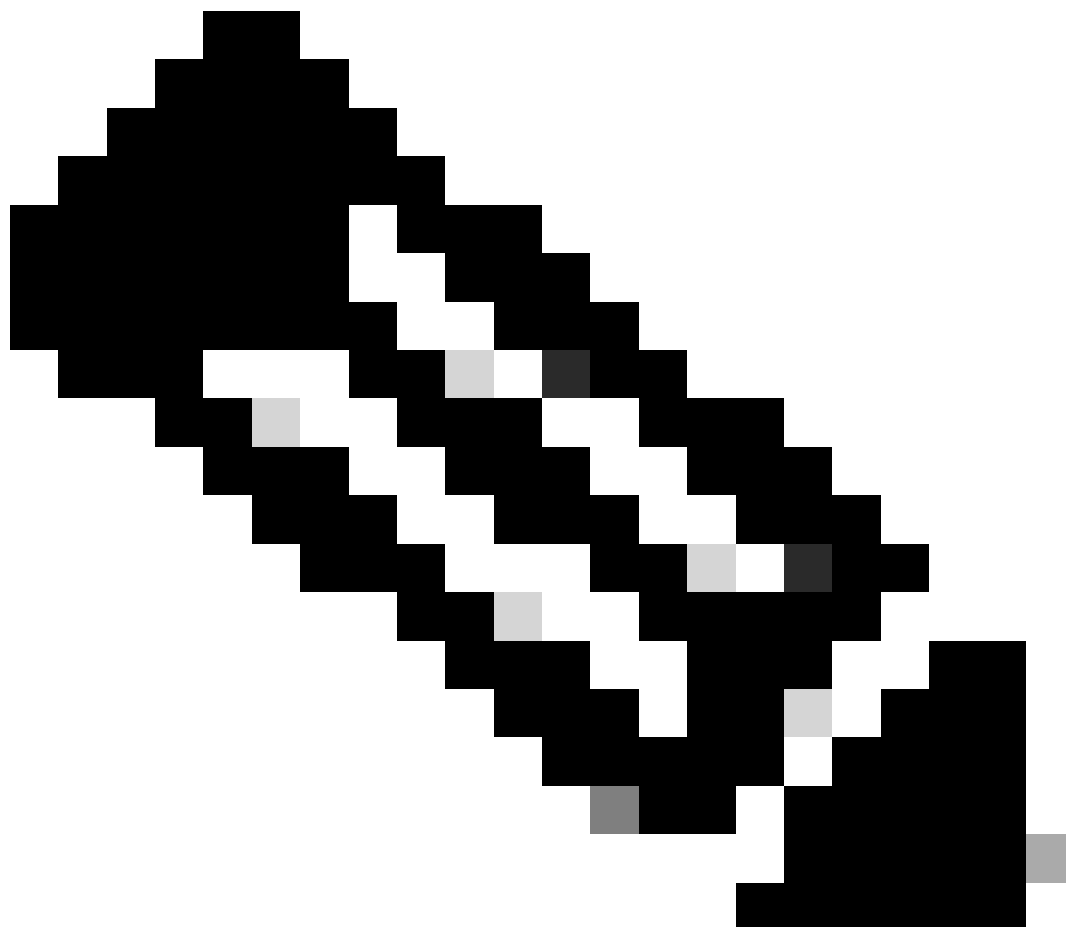
[Launch instance](#)



[Preview code](#)

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

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



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

EC2 > Network interfaces

Network interfaces (1/7) Info

	Name	Network interface ID	Subnet ID	VPC ID
☐		eni-0a4940f4ef3f975b1	subnet-0488c4f9198b94fb3	vpc-08cc6365f2
☐	semadrig-dev...	eni-06b5e292bc1ed4dad	subnet-0c978afc3d9f74a7b	vpc-08cc6365f2
☒		eni-0b5484e24f918207b	subnet-0b664f8e74443d28f	vpc-0d30b9fa95
☐		eni-0e3315e55326d6de9	subnet-0a5f13361443951d2	vpc-0d30b9fa95
☐		eni-0d9d8c101cbb1365e	subnet-0c978afc3d9f74a7b	vpc-08cc6365f2
☐		eni-07c10f0c267c73ebe	subnet-080852db285e8dc8c	vpc-0141e83a4
☐		eni-0556463389ff6d244	subnet-0bdacba83894b2c9f	vpc-08cc6365f2

Actions menu options:

- Attach
- Detach
- Delete
- Manage IP addresses
- Associate address
- Disassociate address
- Modify public hostname type
- Change termination behavior
- Change security groups
- Change source/dest. check**
- Manage tags
- Manage prefixes
- Change description
- Modify idle connection tracking timeout
- Create flow log
- Manage ENA Express
- Manage ENA queues

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

Change source/destination check

Network interface
eni-0b5484e24f918207b

Source/destination check
☐ Enable

Cancel Save

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

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

EC2 > Elastic IP addresses

Elastic IP addresses (2) Info

Actions Allocate Elastic IP address

Find elastic IP addresses by attribute or tag

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

Toewijzen.

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](#)

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

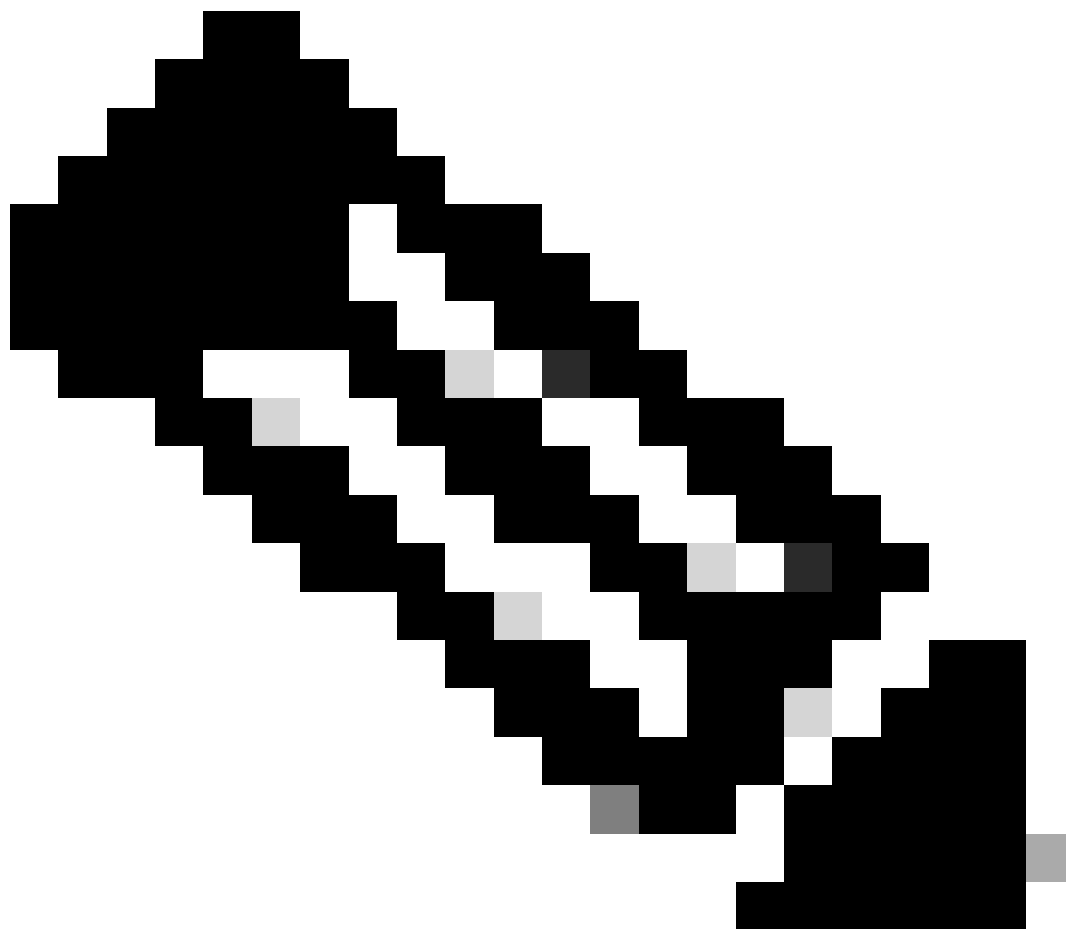
Elastic IP addresses (1/1) [Info](#)

Find elastic IP addresses by attribute or tag

Public IPv4 address [Clear filters](#)

☒	Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	
☒	-	-	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

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



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

Associate Elastic IP address [Info](#)

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

Elastic IP address:

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](#)

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

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

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

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

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

<#root>

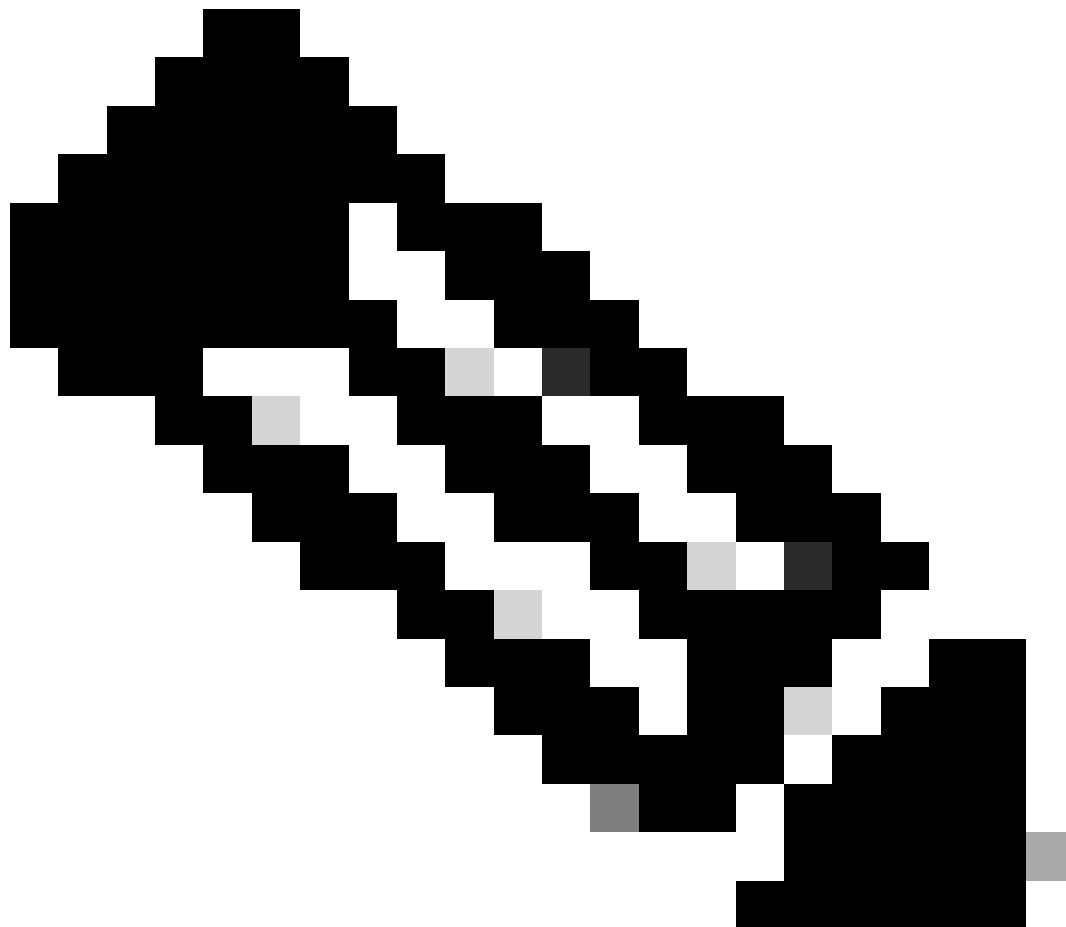
```
ubuntu@ip-10-100-30-254:~$ sudo apt install net-tools
...
ubuntu@ip-10-100-30-254:~$ ifconfig
ens5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
inet
10.100.30.254

netmask 255.255.255.0 broadcast 10.100.30.255
inet6 fe80::51:19ff:fea2:1151 prefixlen 64 scopeid 0x20<link>
ether 02:51:19:a2:11:51 txqueuelen 1000 (Ethernet)
RX packets 1366 bytes 376912 (376.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1417 bytes 189934 (189.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
inet
```

10.100.130.254

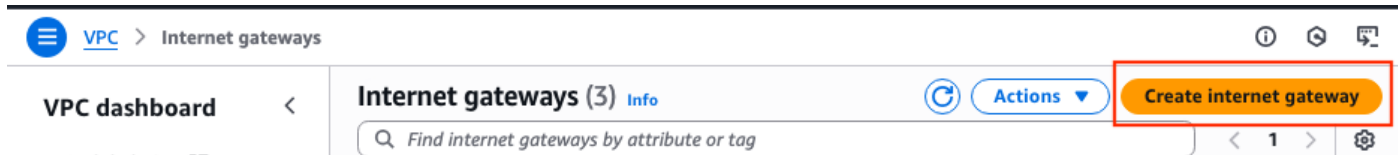
```
netmask 255.255.255.0 broadcast 10.100.130.255
inet6 fe80::3b:7eff:fead:db:e5 prefixlen 64 scopeid 0x20<link>
ether 02:3b:7e:ad:db:e5 txqueuelen 1000 (Ethernet)
RX packets 119 bytes 16831 (16.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 133 bytes 13816 (13.8 KB)
TX errors 0 dropped 0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



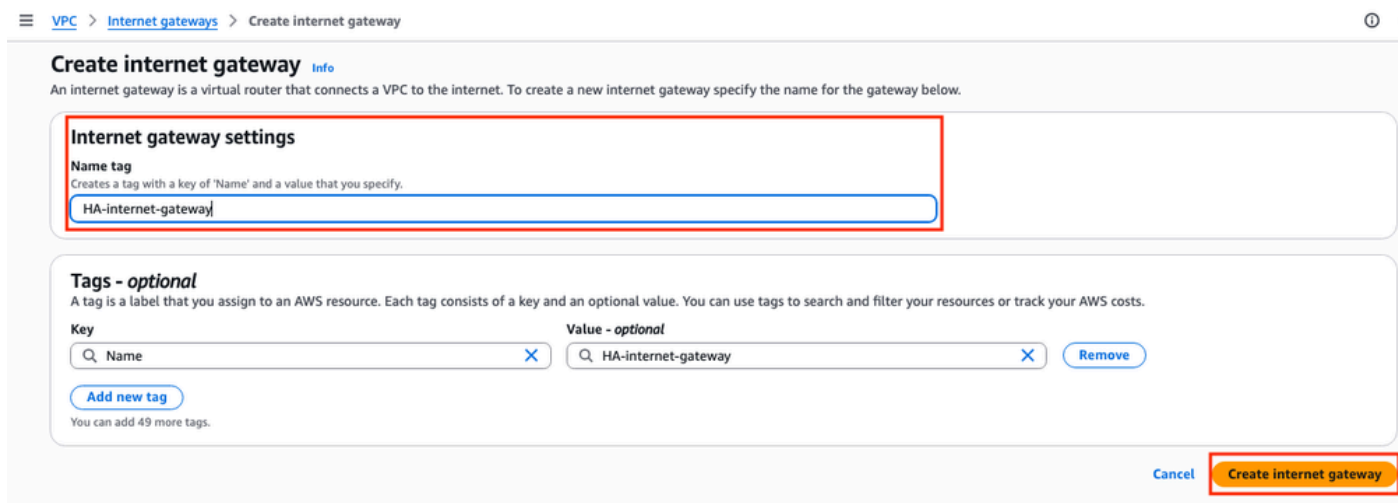
Opmerking: als er wijzigingen zijn aangebracht in de interfaces, klept u de interface of laadt u de VM opnieuw om deze wijzigingen te laten toepassen.

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

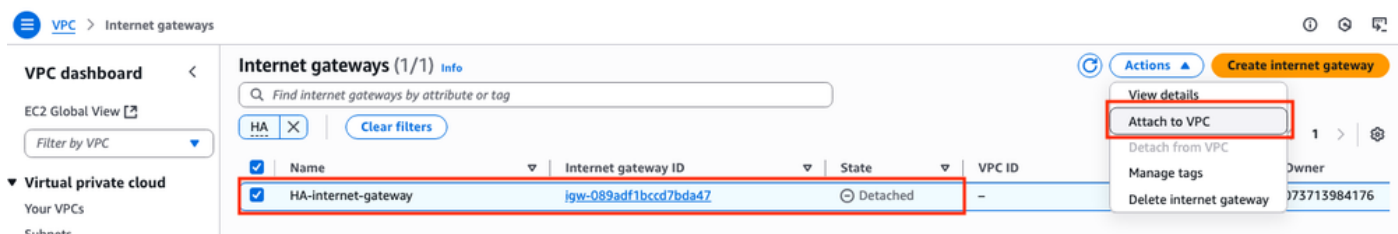
Klik in het gedeelte **VPC Dashboard > Virtual private cloud > Internet gateways** op **Internetgateway maken**.



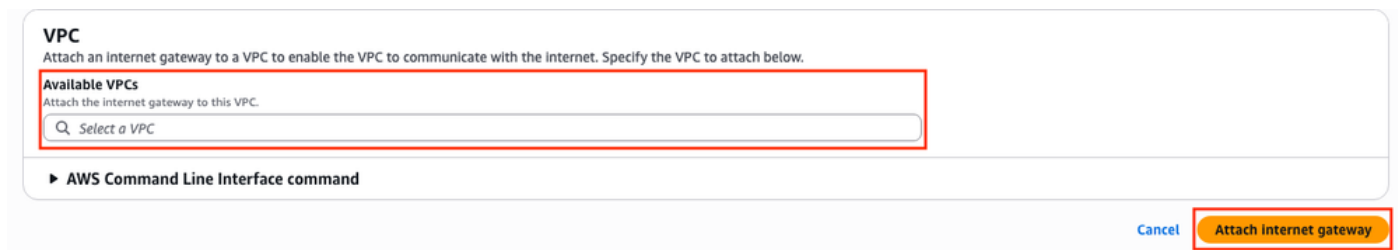
Maak in deze nieuwe sectie een **naamlabel** aan voor deze gateway en klik op **Internetgateway maken**.



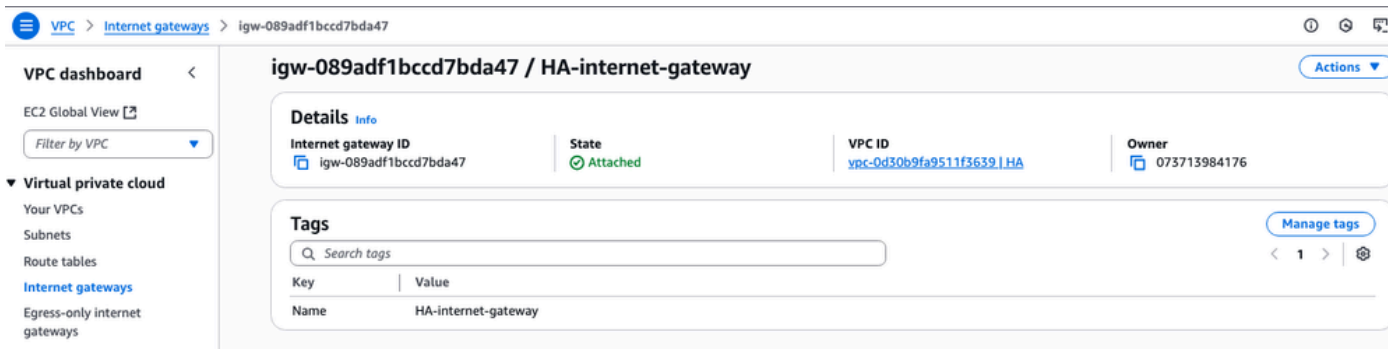
Zodra de IGW is gemaakt, koppelt u deze aan uw corresponderende VPC. Navigeer naar het gedeelte **VPC Dashboard > Virtual Private Cloud > Internet Gateway** en selecteer de bijbehorende IGW. Klik op **Acties > Bijvoegen aan VPC**.



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



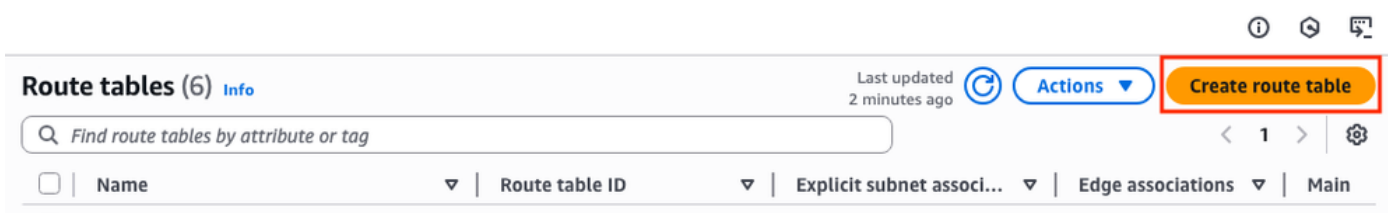
De IGW moet de bijgevoegde status aangeven zoals deze wordt weergegeven:



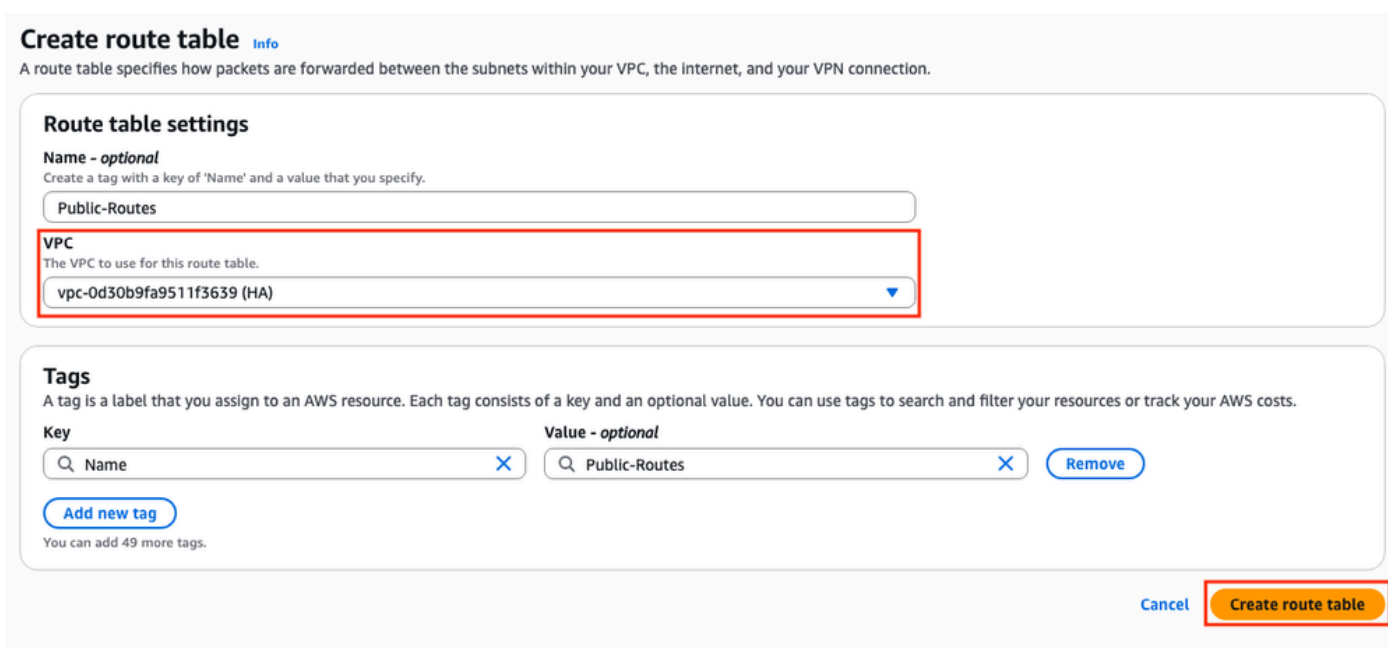
Stap 10. Routetabellen maken en configureren op AWS voor publieke en private subnetten

Stap 10.1. De openbare routetabel maken en configureren

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



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



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

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

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

Actions

- View details
- Set main route table
- Edit subnet associations**
- Edit edge associations
- Edit route propagation
- Edit routes
- Manage tags
- Delete route table

Selecteer vervolgens de corresponderende subnetten en klik op Associaties opslaan.

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

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

Route tables (1/1) Info

Find route tables by attribute or tag

public-routes

Clear filters

Name	Route table ID
Public-Routes	rtb-0d0e48f25c9b00635

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

Edit routes

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

Buttons: Add route, Cancel, Preview, Save changes

Stap 10.2. De privéroudetabel maken en configureren

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

Edit routes

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

Buttons: Add route, Cancel, Preview, Save changes

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

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

Configuratie C8000v R1:

```
interface Tunnel1
ip address 192.168.200.1 255.255.255.0
bfd interval 500 min_rx 500 multiplier 3
tunnel source GigabitEthernet1
tunnel destination <Public IPv4 address of C8000v R2>
!
interface GigabitEthernet1
ip address 10.100.10.254 255.255.255.0
ip nat outside
negotiation auto
!
interface GigabitEthernet2
ip address 10.100.110.254 255.255.255.0
ip nat inside
negotiation auto
!
router eigrp 1
bfd interface Tunnel1
```



```

network 192.168.200.0
passive-interface GigabitEthernet1
!
ip access-list standard 10
10 permit 10.100.130.0 0.0.0.255
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 10.100.10.1
ip route 10.100.130.0 255.255.255.0 GigabitEthernet2 10.100.110.1

```

Configuratie C8000v R2:

```

interface Tunnel1
ip address 192.168.200.2 255.255.255.0
bfd interval 500 min_rx 500 multiplier 3
tunnel source GigabitEthernet1
tunnel destination<Public IPv4 address of C8000v R1>
!
interface GigabitEthernet1
ip address 10.100.20.254 255.255.255.0
ip nat outside
negotiation auto
!
interface GigabitEthernet2
ip address 10.100.120.254 255.255.255.0
negotiation auto
!
router eigrp 1
bfd interface Tunnel1
network 192.168.200.0
passive-interface GigabitEthernet1
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 10.100.20.1
ip route 10.100.130.0 255.255.255.0 GigabitEthernet2 10.100.120.1
!
ip access-list standard 10
10 permit 10.100.130.0 0.0.0.255
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!

ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 10.100.20.1
ip route 10.100.130.0 255.255.255.0 GigabitEthernet2 10.100.120.1

```

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

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

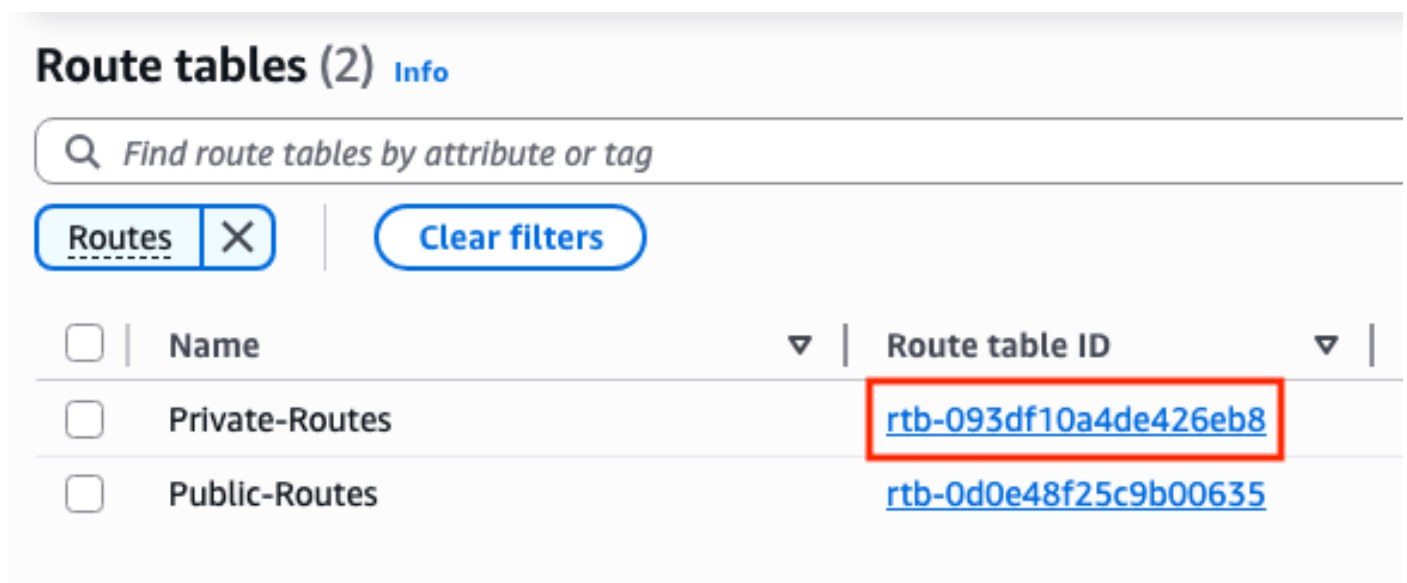
```
Router(config)# redundancy
Router(config-red)# cloud provider aws (node-id)
bfd peer <IP address of the remote device>
route-table <Route table ID>
cidr ip <traffic to be monitored/prefix>
eni <Elastic network interface (ENI) ID>
region <region-name>
```

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

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

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

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



Route tables (2) [Info](#)

Find route tables by attribute or tag

Routes X Clear filters

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

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

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)



Destination



Target

8.8.8.8/32

 eni-0239fda341b4d7e41 

10.100.0.0/16

local

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

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

Last updated 1 minute ago 

[Connect](#)

[Instance state](#)

[Actions](#)

[Launch instances](#)

[All states](#)

 fsimmond



[Clear filters](#)

< 1 >



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

i-0b9a50a09b089b03a (C8000v-R1-fsimmond)





Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

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

Subnet ID  subnet-0b664f8e74443d28f (public-R1-C8000v) [Info](#)

Availability zone  us-east-1a

Outpost ID

-

▶ IP addresses [Info](#)

▶ Hostname and DNS [Info](#)

▼ Network Interfaces (2) [Info](#)

Interface ID	Device index	Card index	Description	Public IPv4 address	Private IPv4 address	Private IPv4 DNS	IPv6
 eni-0645a881c13823696	0	0	-	 100.110.110.254	10.100.10.254	-	-
 eni-070e14fbfde0d8e3b	1	0	-	-	10.100.110.254	-	-

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

Deze lijst kan echter veranderen of groeien. Ga voor de laatste updates naar [AmazonRegion en het document Beschikbaarheidszones](#).

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

Configuratievoorbeeld voor C8000v R1:

```
redundancy
cloud provider aws 1
bfd peer 192.168.200.2
route-table rtb-093df10a4de426eb8
cidr ip 8.8.8.8/32
eni eni-070e14fbfde0d8e3b
region us-east-1
```

Configuratievoorbeeld voor C8000v R2:

```
redundancy
cloud provider aws 1
bfd peer 192.168.200.1
route-table rtb-093df10a4de426eb8
cidr ip 8.8.8.8/32
eni eni-0239fda341b4d7e41
region us-east-1
```

Verificatie

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

```
R1#show bfd neighbors
```

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

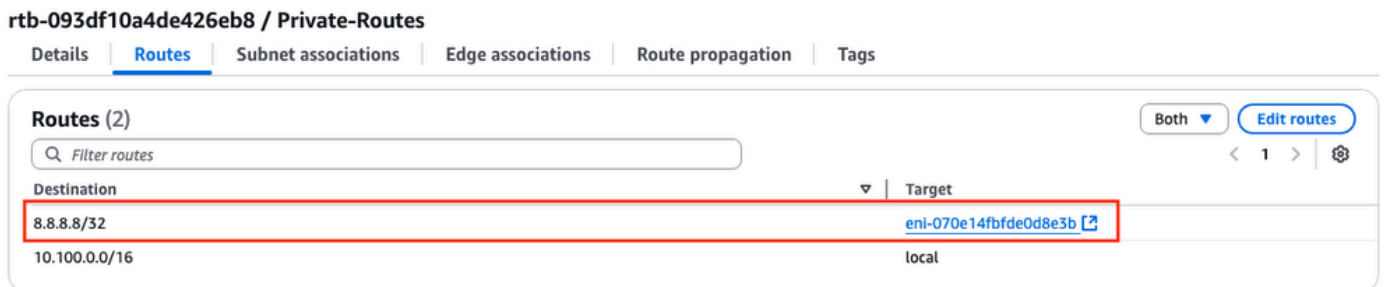
```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface HoId Uptime SRTT RT0 Q Seq
(sec) (ms) Cnt Num
0 192.168.200.2 Tu1 10 00:16:52 2 1470 0 2
```

```
R1#show redundancy cloud provider aws 1
Provider : AWS node 1
BFD peer = 192.168.200.2
BFD intf = Tunnel1
route-table = rtb-093df10a4de426eb8
cidr = 8.8.8.8/32
eni = eni-070e14fbfde0d8e3b
region = us-east-1
```

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

```
ubuntu@ip-10-100-30-254:~$ ping -I ens6 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 10.100.130.254 ens6: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=1.36 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=1.30 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=1.34 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=1.28 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=1.31 ms
```

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



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

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

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

Routes (2)

Destination



Target

8.8.8.8/32

[eni-0239fda341b4d7e41](#)

10.100.0.0/16

local

Problemen oplossen

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

- Zorg ervoor dat de middelen worden gekoppeld. Bij het maken van VPC, subnetten, interfaces, routetabellen, enzovoort, worden veel van deze niet automatisch aan elkaar gekoppeld. Ze hebben geen kennis van elkaar.
- Zorg ervoor dat de Elastic IP en eventuele Private IP is gekoppeld aan de juiste Interfaces, met de juiste subnetten, toegevoegd aan de juiste Route Table, aangesloten op de juiste router, en de juiste VPC en Zone, gekoppeld aan de IAM Rol en beveiligingsgroepen.
- Schakel de controle Bron/Dest uit per ENI.
Als u al alle punten hebt gecontroleerd die in dit gedeelte worden besproken en het probleem nog steeds aanwezig is, verzamelt u deze uitgangen, test u de HA-failover, indien mogelijk, en opent u een case met Cisco TAC:

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

Over deze vertaling

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