

Déployer la configuration de haute disponibilité C8000v sur AWS

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Topologie](#)

[Diagramme du réseau](#)

[Résumé du tableau](#)

[Restrictions](#)

[Configuration](#)

[Étape 1. Sélectionnez une région](#)

[Étape 2 : création du VPC](#)

[Étape 3. Création d'un groupe de sécurité pour le VPC](#)

[Étape 4 : création d'un rôle IAM avec une stratégie et association au VPC](#)

[Étape 5. Création et association d'une stratégie d'approbation à un rôle IAM](#)

[Étape 6. Configuration et lancement des instances C8000v](#)

[Étape 6.1. Configuration de la paire de clés pour l'accès à distance](#)

[Étape 6.2. Création et configuration des sous-réseaux pour l'AMI](#)

[Étape 6.3. Configuration des interfaces AMI](#)

[Étape 6.4. Définition du profil d'instance IAM sur AMI](#)

[Étape 6.5. \(Facultatif\) Définition des informations d'identification sur l'AMI](#)

[Étape 6.6. Terminer la configuration de l'instance](#)

[Étape 6.7. Désactivation de la vérification de la source/destination sur les ENI](#)

[Étape 6.8. Création et association d'une adresse IP élastique à l'interface ENI publique de l'instance](#)

[Étape 7. Répétez l'étape 6 pour créer la deuxième instance C8000v pour HA](#)

[Étape 8. Répétez l'étape 6 pour créer une machine virtuelle \(Linux/Windows\) à partir d'AMI Marketplace](#)

[Étape 9. Création et configuration d'une passerelle Internet \(IGW\) pour le VPC](#)

[Étape 10. Création et configuration de tables de routage sur AWS pour les sous-réseaux publics et privés](#)

[Étape 10.1. Création et configuration de la table de routage publique](#)

[Étape 10.2. Création et configuration de la table de routage privée](#)

[Étape 11. Vérification et configuration de la configuration réseau de base, de la traduction d'adresses de réseau \(NAT\), du tunnel GRE avec BFD et du protocole de routage](#)

[Étape 12. Configuration de la haute disponibilité \(Cisco IOS® XE Denali 16.3.1a ou version ultérieure\)](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer un environnement de haute disponibilité avec des routeurs Catalyst 8000v sur le cloud Amazon Web Services.

Conditions préalables

Exigences

Cisco vous recommande d'avoir une connaissance préalable des sujets suivants :

- Connaissance générale de la console AWS et de ses composants
- Compréhension du logiciel Cisco IOS® XE
- Connaissances de base de la fonctionnalité HA.

Composants utilisés

Ces composants sont requis pour cet exemple de configuration :

- Un compte Amazon AWS avec un rôle administrateur
- Deux périphériques C8000v exécutant Cisco IOS® XE 17.15.3a et 1 machine virtuelle Ubuntu 22.04 LTS IAM dans la même région

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Topologie

Il existe différents scénarios de déploiement haute disponibilité en fonction des besoins du réseau. Dans cet exemple, la redondance haute disponibilité est configurée avec les paramètres suivants :

- 1x - Région
- 1x - VPC
- 3x - Zones de disponibilité
- 6x - Interfaces/sous-réseaux réseau (3x face publique/3x face privée)
- 2x - Tables de routage (publiques et privées)
- 2 routeurs C8000v (Cisco IOS® XE Denali 17.15.3a)
- 1x - VM (Linux/Windows)

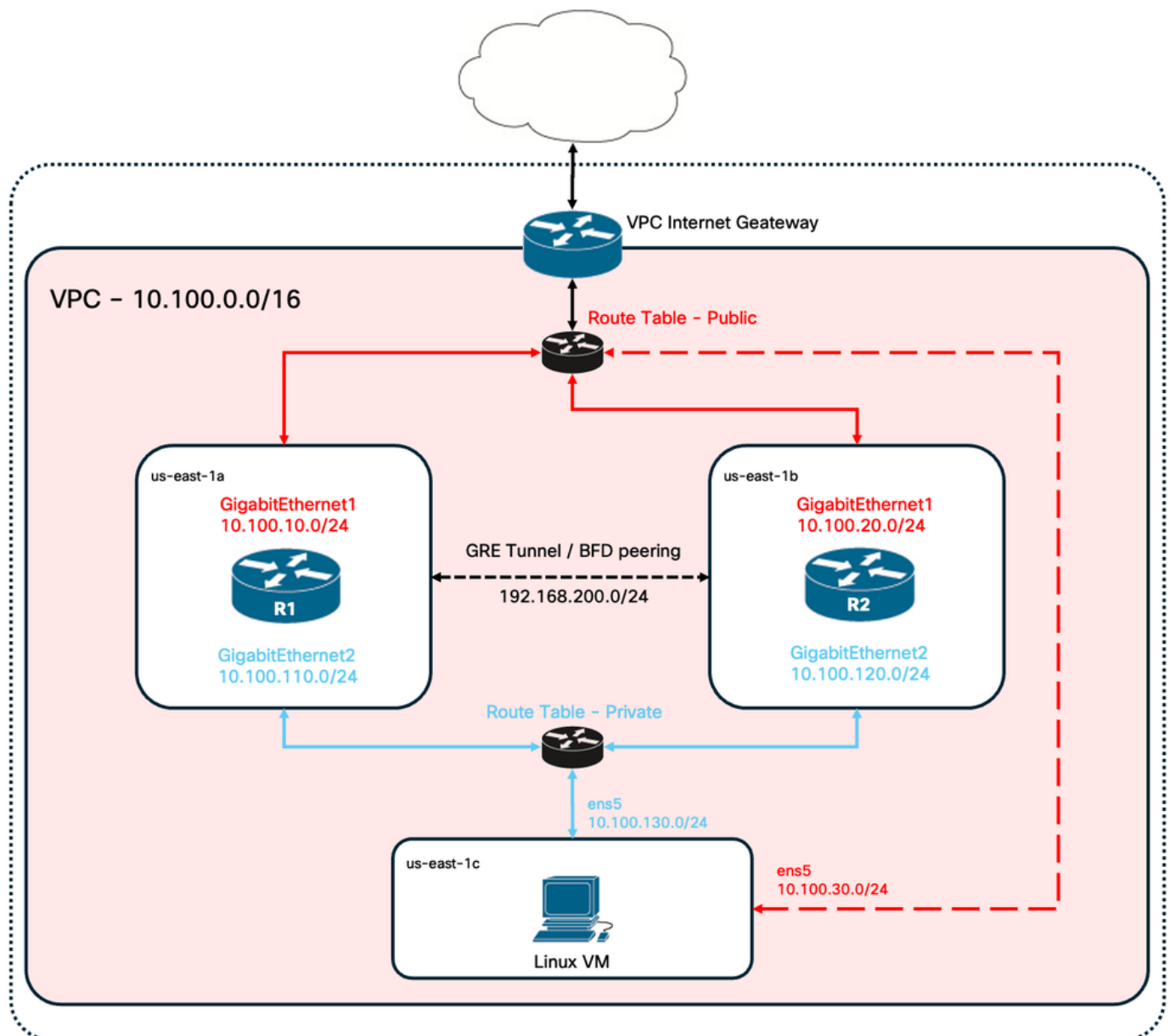
Une paire haute disponibilité comprend 2 routeurs C8000v, dans deux zones de disponibilité différentes. Considérez chaque zone de disponibilité comme un data center distinct pour une résilience matérielle supplémentaire.

La troisième zone est une machine virtuelle, qui simule un périphérique dans un data center privé.

Pour l'instant, l'accès à Internet est activé via l'interface publique afin que vous puissiez accéder à la machine virtuelle et la configurer. En règle générale, tout le trafic normal doit transiter par la table de routage privé.

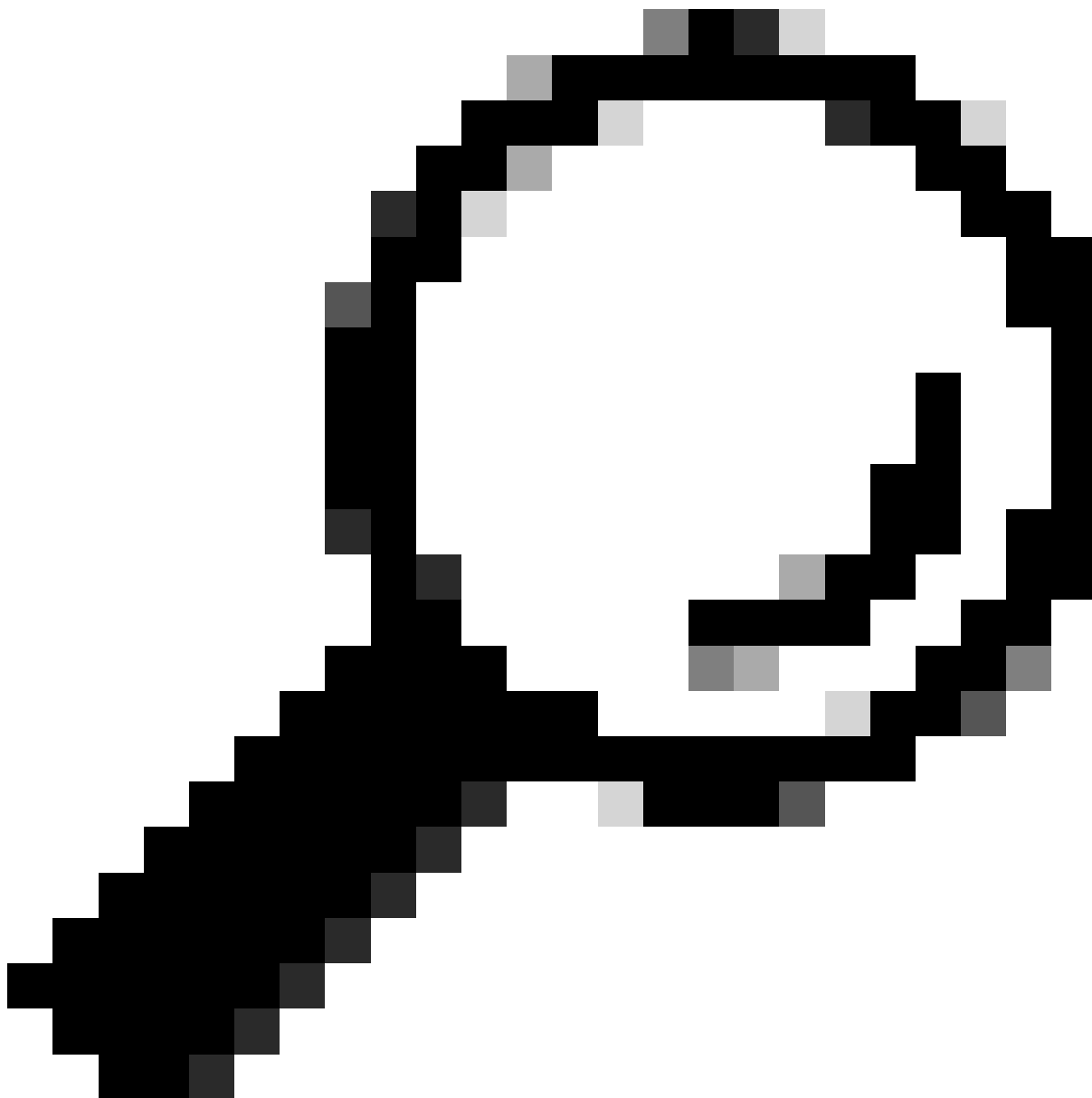
Pour simuler le trafic, lancez une requête ping à partir de l'interface privée de la machine virtuelle, en traversant la table de routage privé via R1 pour atteindre 8.8.8.8. En cas de basculement, vérifiez que la table de routage privé a été mise à jour automatiquement pour router le trafic via l'interface privée du routeur R2.

Diagramme du réseau



Résumé du tableau

Pour résumer la topologie, voici le tableau contenant les valeurs les plus importantes de chaque composant des travaux pratiques. Les informations fournies dans ce tableau sont réservées à ces travaux pratiques.



Conseil : ce tableau permet de conserver une vue d'ensemble claire des variables clés tout au long du guide. Il est recommandé de recueillir les renseignements dans ce format afin de simplifier le processus.

Périphérique	Zone de disponibilité	Interfaces	Adresses IP	RTB	ENI
R1	us-east-1a	GigabitEthernet1	10.100.10.254	rtb-0d0e48f25c9b00635 (public)	eni-0645a881c13823696
		GigabitEthernet2	10.100.110.254	rtb-093df10a4de426eb8 (privé)	eni-070e14fbfde0d8e3b
R2	us-east-1b	GigabitEthernet1	10.100.20.254	rtb-0d0e48f25c9b00635	eni-0a7817922ffbb317b

				(public)	
		GigabitEthernet2	10.100.120.254	rtb-093df10a4de426eb8 (privé)	eni-0239fda341b4d7e41
VM Linux	us-east-1c	Rens5	10.100.30.254	rtb-0d0e48f25c9b00635 (public)	eni-0b28560781b3435b1
		en6	10.100.130.254	rtb-093df10a4de426eb8 (privé)	eni-05d025e88b6355808

Restrictions

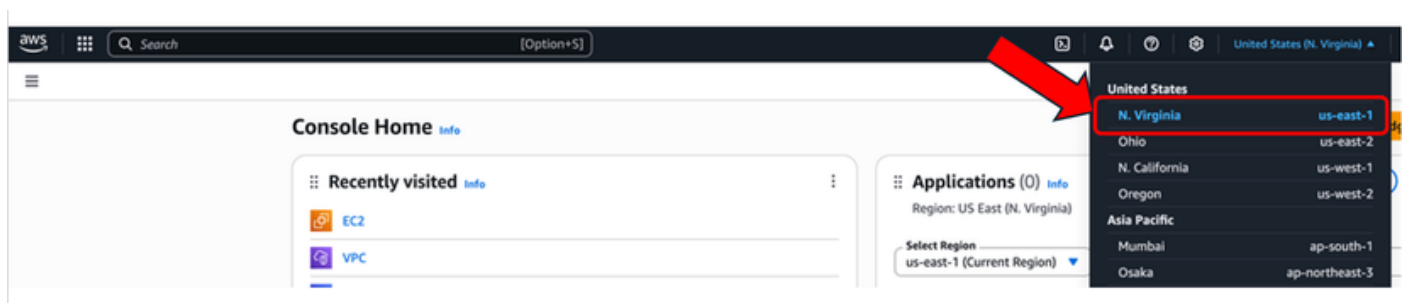
- Sur tout sous-réseau créé, n'utilisez pas la première adresse disponible de ce sous-réseau. Ces adresses IP sont utilisées par les services AWS en interne.
- Ne configurez pas les interfaces publiques des périphériques C8000v à l'intérieur d'un VRF. La haute disponibilité ne fonctionne pas correctement si elle est définie.

Configuration

Le flux général de configuration est axé sur la création des machines virtuelles demandées dans la région appropriée et sur la configuration la plus spécifique, comme les routes et les interfaces de chacune d'elles. Cependant, il est recommandé de comprendre la topologie en premier et de la configurer dans l'ordre souhaité.

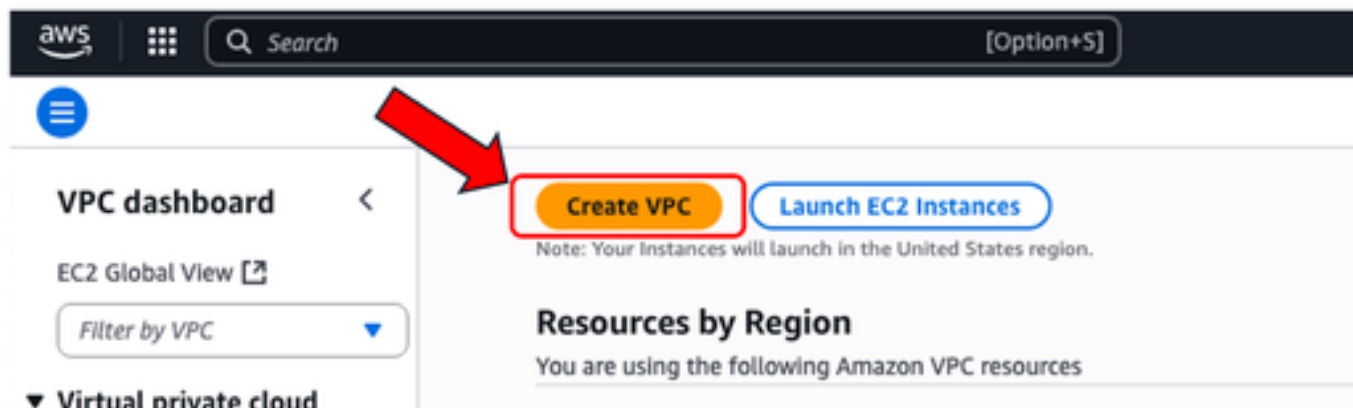
Étape 1. Sélectionnez une région

Pour ce guide de déploiement, la région US West (North Virginia) - us-east-1 est sélectionnée comme région VPC.



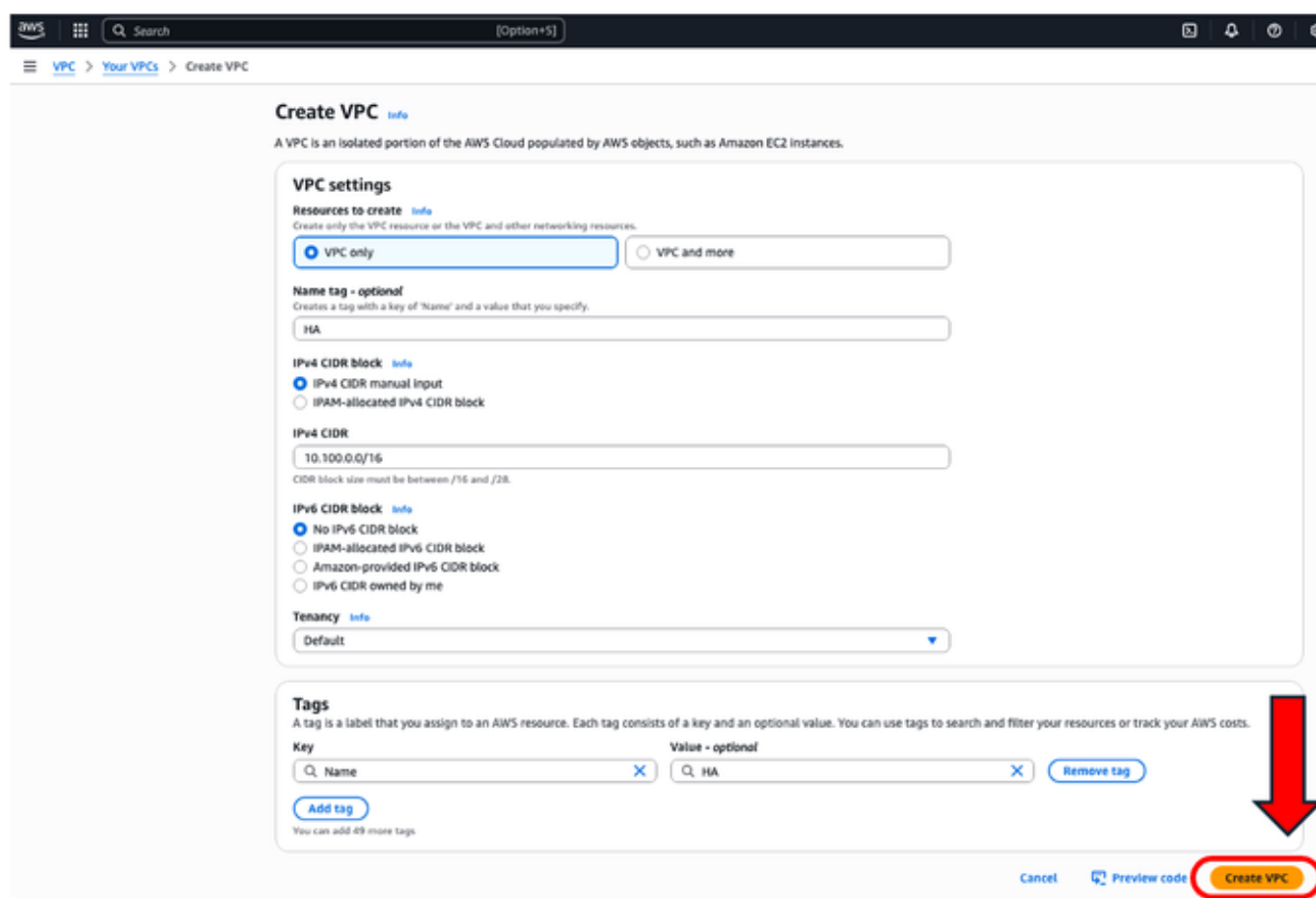
Étape 2 : création du VPC

Sur la console AWS, accédez à VPC > Tableau de bord VPC > Créer VPC.

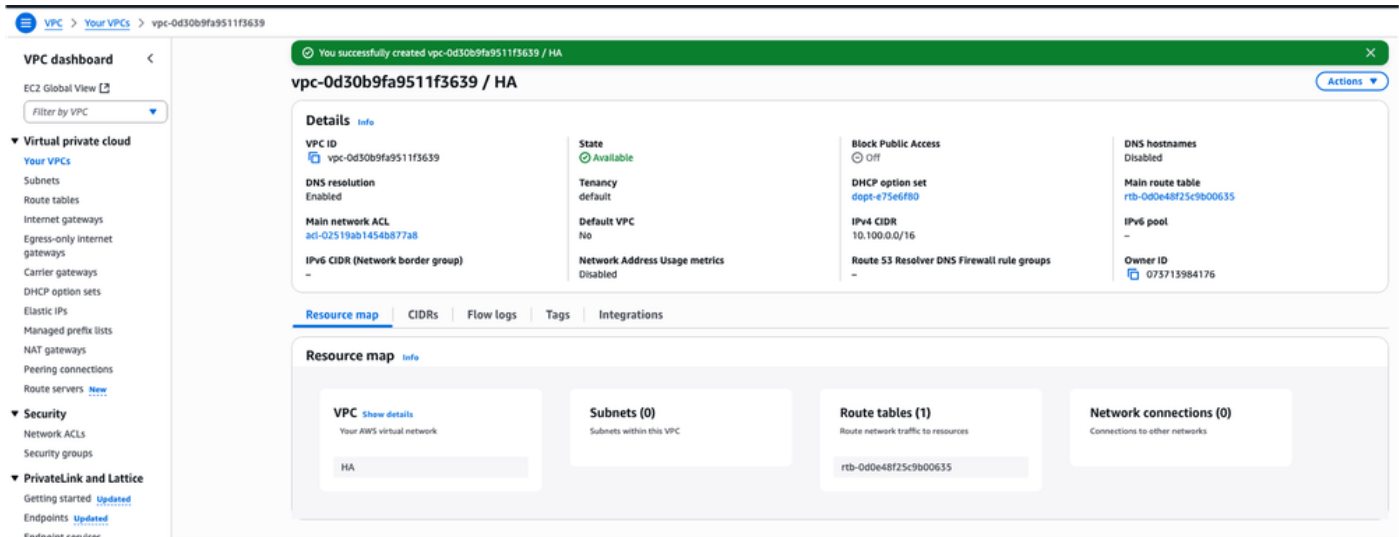


Lorsque vous créez le VPC, sélectionnez l'option VPC only. Vous pouvez affecter un réseau /16 à utiliser comme vous le souhaitez.

Dans ce guide de déploiement, le réseau 10.100.0.0/16 est sélectionné :

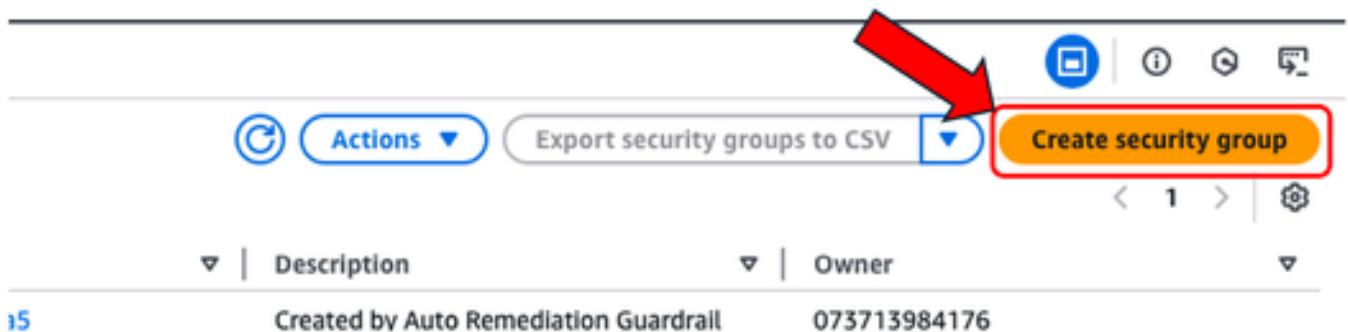


Après avoir cliqué sur Create VPC, la balise VPC-0d30b9fa9511f3639 with HA est maintenant créée :



Étape 3. Création d'un groupe de sécurité pour le VPC

Dans AWS, les groupes de sécurité fonctionnent comme des listes de contrôle d'accès, autorisant ou refusant le trafic vers les machines virtuelles configurées au sein d'un VPC. Dans la console AWS, accédez à VPC > Tableau de bord VPC > Sécurité > section Groupes de sécurité et cliquez sur Créer un groupe de sécurité.



Sous Inbound Rules, définissez le trafic que vous souhaitez autoriser. Dans cet exemple, Tout le trafic est sélectionné à l'aide du réseau 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

Étape 4 : création d'un rôle IAM avec une stratégie et association au VPC

IAM accorde à vos AMI l'accès requis aux API Amazon. Le C8000v est utilisé comme proxy pour appeler les commandes API AWS afin de modifier la table de routage dans AWS. Par défaut, les instances EC2 ne sont pas autorisées à accéder aux API. Pour cette raison, un nouveau rôle IAM doit être créé et appliqué lors des créations AMI.

Accédez au tableau de bord IAM et accédez à Access Management > Roles > Create Role. Ce processus se compose de 3 étapes :

AWS IAM > Roles

Identity and Access Management (IAM)

Roles (65) info

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.

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)	-

Tout d'abord, sélectionnez l'option AWS Service dans la section Trusted entity type et EC2 comme service affecté à cette stratégie.

- 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

Lorsque vous avez terminé, cliquez sur Next :

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.

Search

Filter by Type

All types

< 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**

Enfin, définissez le nom du rôle et cliquez sur le bouton Créer un rôle.

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](#)

Étape 5. Création et association d'une stratégie d'approbation à un rôle IAM

Une fois le rôle créé, une stratégie d'approbation doit être définie pour acquérir la capacité de modifier les tables de routage AWS si nécessaire. Accédez à la section Stratégies du tableau de bord IAM. Cliquez sur le bouton Créer une stratégie. Ce processus se compose de 2 étapes :

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**
- Identity providers
- Account settings
- Root access management

Access reports

- Access Analyzer

Policies (1367)

A policy is an object in AWS that defines permissions.

Filter by Type: All types

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

Tout d'abord, assurez-vous que l'Éditeur de stratégie utilise JSON et appliquez les commandes qui sont montrées ci-dessous. Une fois configuré, cliquez sur Next :

The screenshot shows the AWS IAM 'Specify permissions' console. The 'Policy editor' tab is active, displaying a JSON policy document. The JSON 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 'JSON' tab is selected in the editor. The 'Add new statement' button is visible at the bottom left. The status bar at the bottom shows 'JSON Ln 21, Col 1' and '5825 of 6144 characters remaining'. The 'Next' button is highlighted in orange at the bottom right.

Il s'agit du code texte utilisé dans l'image :

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

Définissez ultérieurement le nom de la stratégie et cliquez sur Créer une stratégie.

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**

Une fois la stratégie créée, filtrez et sélectionnez la stratégie, puis cliquez sur l'option Attacher dans le menu déroulant Actions.

Identity and Access Management (IAM)

Policies (1/1368)

A policy is an object in AWS that defines permissions.

Search C800

Filter by Type: 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

Une nouvelle fenêtre est ouverte. Dans la section Entités IAM, filtrez et sélectionnez le rôle IAM créé, puis cliquez sur Attacher une stratégie.

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

Filter by Entity type: All types 1 match

Entity name	Entity type
route-table-change	Roles

Cancel **Attach policy**

Étape 6. Configuration et lancement des instances C8000v

Chaque routeur C8000v aura 2 interfaces (1 publique, 1 privée) et sera créé sur sa propre zone

de disponibilité.

Dans le tableau de bord EC2, cliquez sur Launch Instances :

EC2

[Dashboard](#)

[EC2 Global View](#)

[Events](#)

▼ **Instances**

- [Instances](#)
- [Instance Types](#)
- [Launch Templates](#)
- [Spot Requests](#)
- [Savings Plans](#)
- [Reserved Instances](#)
- [Dedicated Hosts](#)
- [Capacity Reservations](#)

▼ **Images**

- [AMIs](#)
- [AMI Catalog](#)

Resources

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

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

Filtrez la base de données AMI avec le nom Cisco Catalyst 8000v pour SD-WAN et routage. Dans la liste AMI AWS Marketplace, cliquez sur Sélectionner.

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)**

Commonly used AMIs Created by me AWS & trusted third-party AMIs Published by anyone

▼ **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

Cisco Catalyst 8000v for SD-WAN & Routing

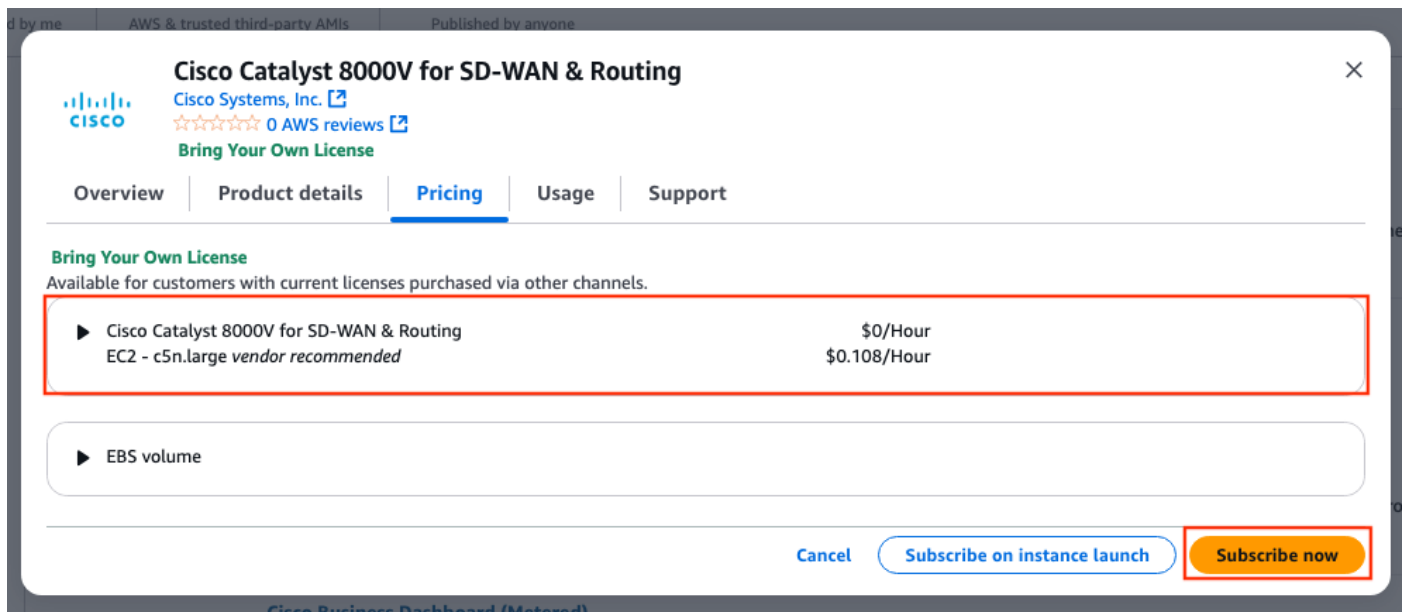
By Cisco Systems, Inc. | Ver 17.15.03a

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](#)

Sélectionnez la taille correspondante pour l'AMI. Pour cet exemple, la taille c5n.large est

sélectionnée. Cela dépend de la capacité requise pour votre réseau. Une fois sélectionné, cliquez sur Subscribe now.



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.

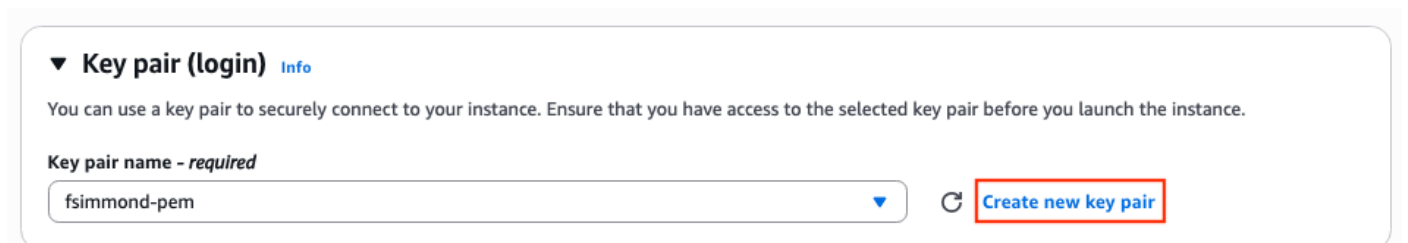
▶ Cisco Catalyst 8000V for SD-WAN & Routing EC2 - c5n.large <i>vendor recommended</i>	\$0/Hour \$0.108/Hour
--	--------------------------

▶ EBS volume

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

Étape 6.1. Configuration de la paire de clés pour l'accès à distance

Une fois inscrit à l'AMI, une nouvelle fenêtre avec plusieurs options s'affiche. Dans la section Paire de clés (connexion), si aucune paire de clés n'est présente, cliquez sur Créer une nouvelle paire de clés. Vous pouvez réutiliser une seule clé pour chaque périphérique créé.



▼ **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](#)

Une nouvelle fenêtre contextuelle s'affiche. Pour cet exemple, un fichier de clé .pem avec chiffrement ED25519 est créé. Une fois que tout est défini, cliquez sur Créer une paire de clés.

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

Étape 6.2. Création et configuration des sous-réseaux pour l'AMI

Dans la section Paramètres réseau, cliquez sur Modifier. De nouvelles options sont désormais disponibles dans la section :

1. Sélectionnez le VPC souhaité pour ce travail. Dans cet exemple, le VPC appelé HA est sélectionné.
2. Dans la section Pare-feu (groupes de sécurité), sélectionnez Sélectionner un groupe de sécurité existant.
3. Une fois l'option 2 sélectionnée, l'option Groupes de sécurité communs est disponible. Filtrez et sélectionnez le groupe de sécurité souhaité. Dans cet exemple, le groupe de sécurité Tout le trafic HA est sélectionné.

4. (Facultatif) Si aucun sous-réseau n'est créé pour ces périphériques, cliquez sur Create new subnet.

The screenshot shows the 'Network settings' section of an AWS console. It includes a 'VPC - required' dropdown menu (annotated with a red '1'), a 'Subnet' section with a dropdown menu (annotated with a red '4') and a 'Create new subnet' button, an 'Auto-assign public IP' dropdown menu set to 'Disable', and a 'Firewall (security groups)' section. In the firewall section, the 'Select existing security group' radio button is selected (annotated with a red '2'). Below this, a 'Common security groups' section shows a list of security groups, with 'All traffic HA sg-029461ba80052f10c' selected (annotated with a red '3'). A 'Compare security group rules' button is also visible. The bottom of the section has an 'Advanced network configuration' link.

Un nouvel onglet du navigateur Web est ouvert, vous menant à la section Créer un sous-réseau :

1. Sélectionnez le VPC correspondant à cette configuration dans la liste déroulante.
2. Attribuez un nom au nouveau sous-réseau.
3. Définissez la zone de disponibilité pour ce sous-réseau. (Reportez-vous à la section Topologie de ce document pour plus d'informations sur le paramètre)
4. Définissez le bloc de sous-réseau qui appartient au bloc CIDR du VPC.
5. En outre, tous les sous-réseaux qui vont être utilisés peuvent être créés en cliquant sur la section Ajouter un nouveau sous-réseau et répétez les étapes de 2 à 4 pour chaque sous-réseau.
6. Une fois terminé, cliquez sur Créer un sous-réseau. Accédez à la page précédente pour continuer avec les paramètres.

☰ VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID

Choose a VPC to create the subnet in.

vpc-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

Associate a tag with a key of "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](#)

Dans la sous-section Subnet de la section Network Settings, cliquez sur l'icône Refresh pour afficher les sous-réseaux créés dans la liste déroulante.

Étape 6.3. Configuration des interfaces AMI

Dans la section Paramètres réseau, développez la sous-section Configuration réseau avancée. Les options suivantes s'affichent :

▼ 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.

Dans ce menu, définissez les paramètres Description, Primary IP, Delete on termination. Pour le paramètre Primary IP, utilisez n'importe quelle adresse IP à l'exception de la première adresse disponible du sous-réseau. Il est utilisé en interne par AWS.

Le paramètre Delete on termination de cet exemple est défini sur No. Toutefois, cette valeur peut être définie sur yes en fonction de votre environnement.

En raison de cette topologie, une seconde interface est nécessaire pour le sous-réseau privé. Cliquez sur Add network interface et cette invite s'affiche. Cependant, l'interface permet de sélectionner le sous-réseau cette fois-ci :

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

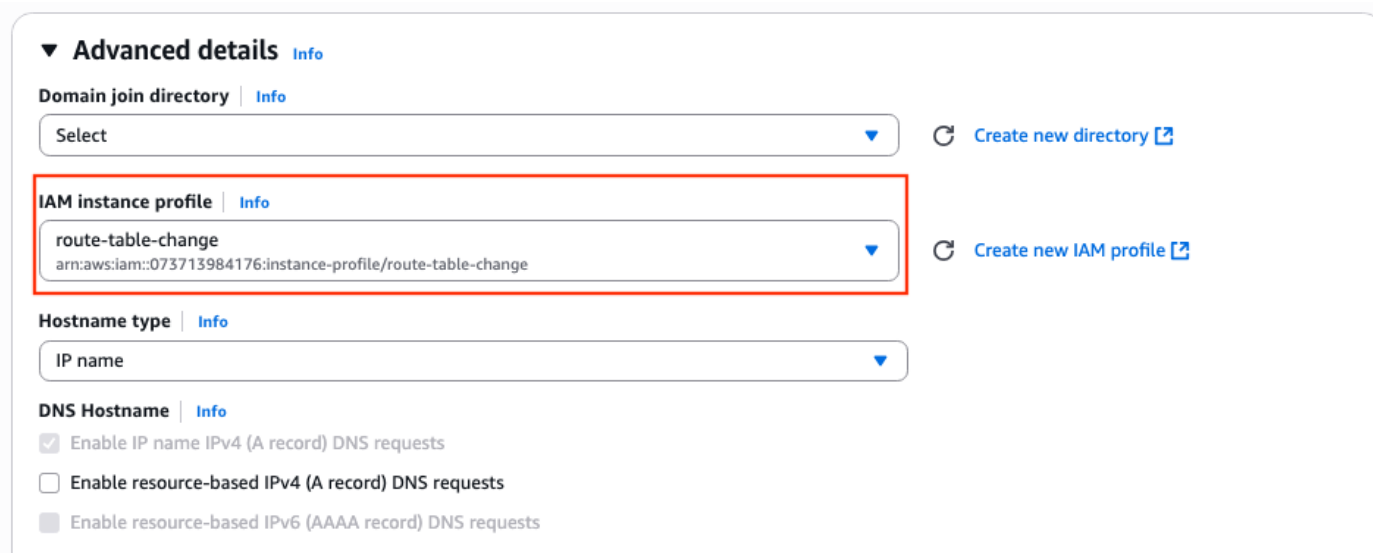
The selected subnet does not support IPv6 IPs.

Remove

Une fois que tous les paramètres ont été définis comme sur l'interface réseau 1, passez aux étapes suivantes.

Étape 6.4. Définition du profil d'instance IAM sur AMI

Dans la section Détails avancés, sélectionnez le rôle IAM créé sur le paramètre de profil d'instance IAM :



▼ 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

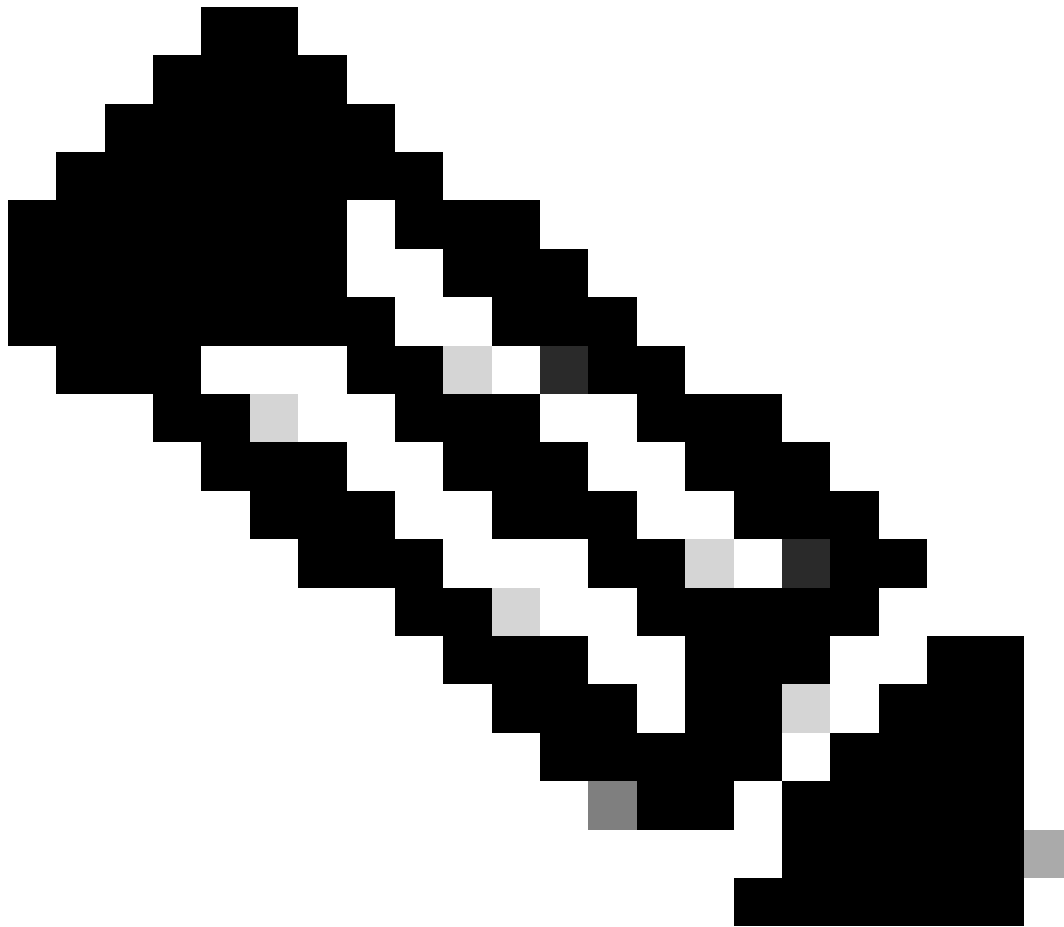
DNS Hostname | [Info](#)

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

Étape 6.5. (Facultatif) Définition des informations d'identification sur l'AMI

Sous la section Détails avancés, accédez à la section Données utilisateur - facultatif et appliquez ce paramètre pour définir un nom d'utilisateur et un mot de passe lors de la création de l'instance :

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



Remarque : Le nom d'utilisateur fourni par AWS à SSH dans le C8000v peut être incorrectement répertorié comme racine. Remplacez-le par ec2-user si nécessaire.

Étape 6.6. Terminer la configuration de l'instance

Une fois que tout est configuré, cliquez sur Launch Instance :

▼ 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

i **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.



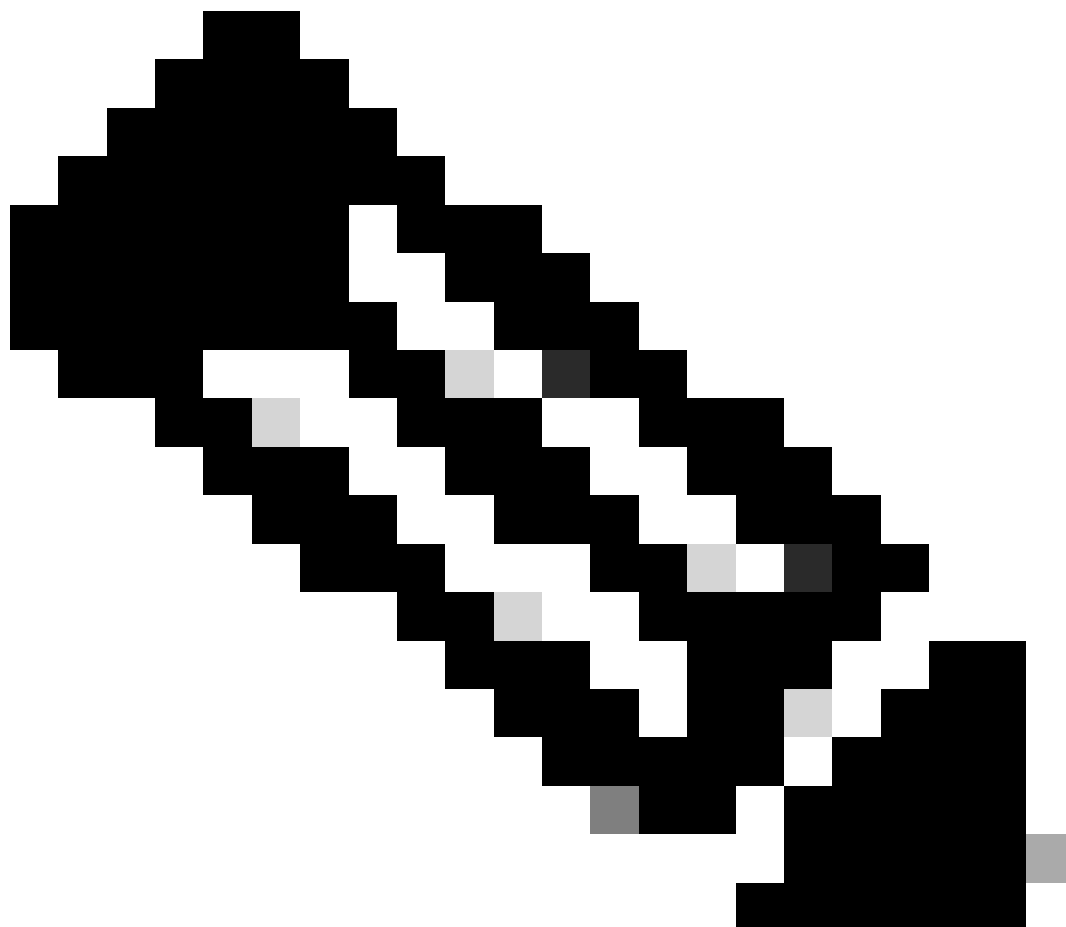
[Cancel](#)

[Launch instance](#)

 [Preview code](#)

Étape 6.7. Désactivation de la vérification de la source/destination sur les ENI

Une fois l'instance créée, désactivez la fonctionnalité de vérification src/dst sur AWS pour obtenir la connectivité entre les interfaces du même sous-réseau. Dans la section EC2 Dashboard > Network & Security > Network interfaces, sélectionnez les ENI et cliquez sur Actions > Modifier la source/dest. vérifiez.



Remarque : Vous devez sélectionner les ENI un par un pour que cette option soit disponible.

The screenshot shows the AWS Management Console 'Network interfaces' page. The left sidebar contains navigation links for EC2, Dashboard, EC2 Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, and Network & Security. The main content area shows a table of network interfaces. The 'eni-0b5484e24f918207b' interface is selected. The 'Actions' dropdown menu is open, and 'Change source/dest. check' is highlighted. The table has columns for Name, Network interface ID, Subnet ID, and VPC ID.

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

Une nouvelle fenêtre s'affiche. Dans le nouveau menu, désactivez la case à cocher Enable et cliquez sur Save.

The screenshot shows the 'Change source/destination check' dialog box. The title is 'Change source/destination check'. Below the title, it says 'Network interface' and 'eni-0b5484e24f918207b'. There is a section titled 'Source/destination check' with an unchecked checkbox labeled 'Enable'. At the bottom right, there are 'Cancel' and 'Save' buttons. The 'Save' button is highlighted.

Étape 6.8. Création et association d'une adresse IP élastique à l'interface ENI publique de l'instance

Dans la section EC2 Dashboard > Network & Security > Elastic IPs, cliquez sur Allocate Elastic IP address.

The screenshot shows the AWS Management Console 'Elastic IP addresses' page. The left sidebar contains navigation links for EC2, Dashboard, EC2 Global View, and Events. The main content area shows the 'Elastic IP addresses' page with a search bar and a table. The 'Allocate Elastic IP address' button is highlighted.

La page vous mène à l'autre section. Dans cet exemple, l'option Pool d'adresses IPv4 d'Amazon

est sélectionnée avec la zone de disponibilité us-east-1. Une fois terminé, cliquez sur Allocate.

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](#)

Lorsque l'adresse IP est créée, attribuez-la à l'interface publique de l'instance. Dans la section EC2 Dashboard > Network & Security > Elastic IPs, cliquez sur Actions > Associate Elastic IP address.

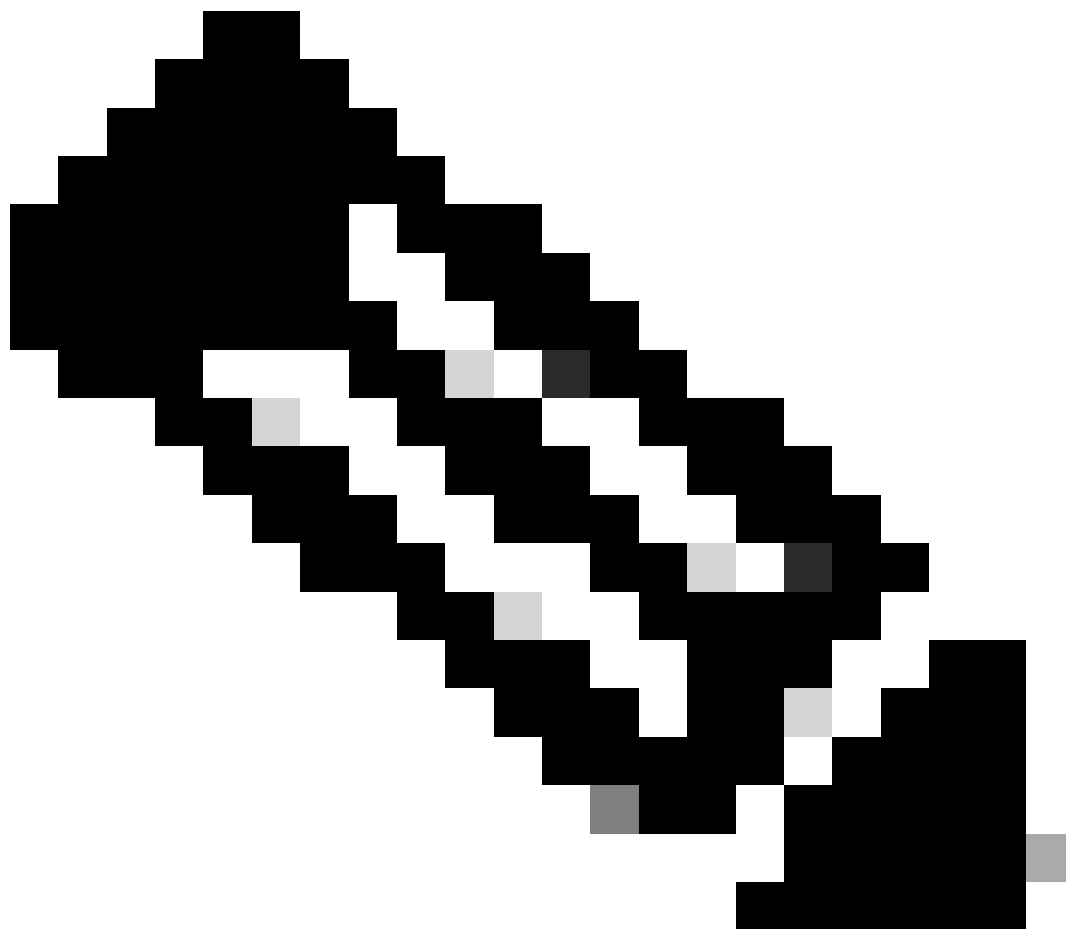
Elastic IP addresses (1/1) [Info](#)

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	-	Actions View details Release Elastic IP addresses Associate Elastic IP address Disassociate Elastic IP address Update reverse DNS Enable transfers Disable transfers Accept transfers

Dans cette nouvelle section, sélectionnez l'option Network interface et recherchez l'ENI public de l'interface correspondante. Associez l'adresse IP publique correspondante et cliquez sur Associate.



Remarque : Pour obtenir l'ID ENI approprié, accédez à la section EC2 Dashboard > Instances. Sélectionnez ensuite l'instance et consultez la section Mise en réseau. Recherchez l'adresse IP de votre interface publique pour obtenir la valeur ENI sur la même ligne.

Associate Elastic IP address [Info](#)

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

Elastic 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
eni-0b5484e24f918207b

Private IP address
The private IP address with which to associate the Elastic IP address.
10.100.10.253

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](#)

Étape 7. Répétez l'étape 6 pour créer la deuxième instance C8000v pour HA

Reportez-vous à la section Topologie de ce document pour obtenir les informations correspondantes pour chaque interface et répétez les mêmes étapes de 6.1 à 6.6.

Étape 8. Répétez l'étape 6 pour créer une machine virtuelle (Linux/Windows) à partir d'AMI Marketplace

Dans cet exemple, le serveur Ubuntu 22.04.5 LTS est sélectionné dans AMI Marketplace en tant qu'hôte interne.

ens5 est créé par défaut pour l'interface publique. Dans cet exemple, créez une seconde interface (ens6 sur le périphérique) pour le sous-réseau privé.

<#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)
```

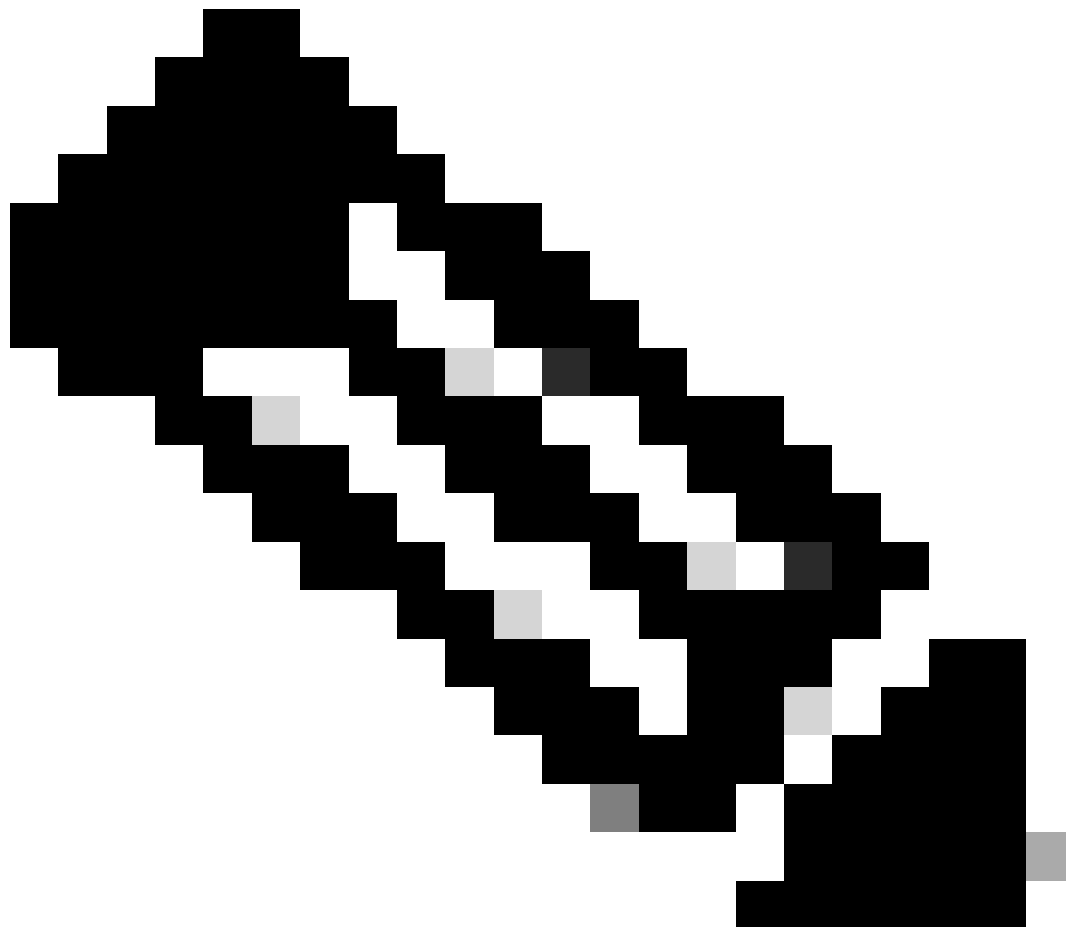
```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
inet
```

10.100.130.254

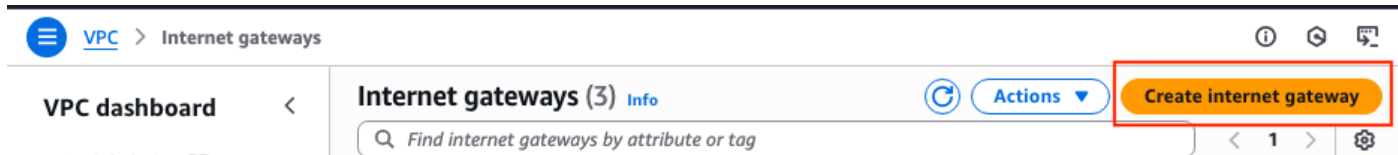
```
netmask 255.255.255.0 broadcast 10.100.130.255
inet6 fe80::3b:7eff:fead:dbe5 prefixlen 64 scopeid 0x20<link>
ether 02:3b:7e:ad:db:e5 txqueuelen 1000 (Ethernet)
RX packets 119 bytes 16831 (16.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 133 bytes 13816 (13.8 KB)
TX errors 0 dropped 0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



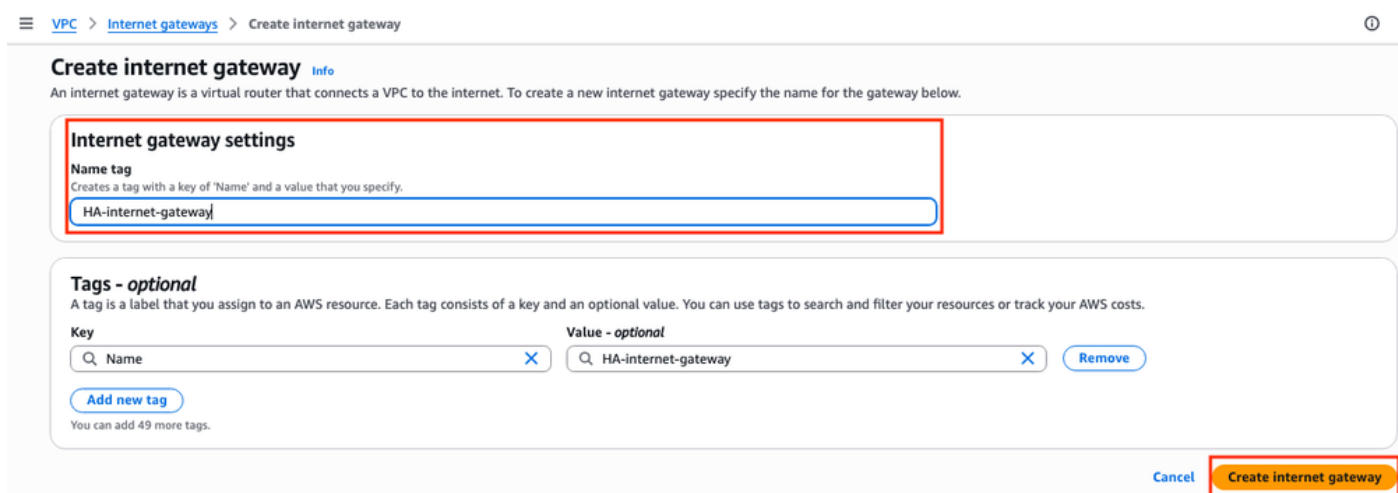
Remarque : Si des modifications sont apportées aux interfaces, faites un battement sur l'interface ou rechargez la VM pour que ces modifications soient appliquées.

Étape 9. Création et configuration d'une passerelle Internet (IGW) pour le VPC

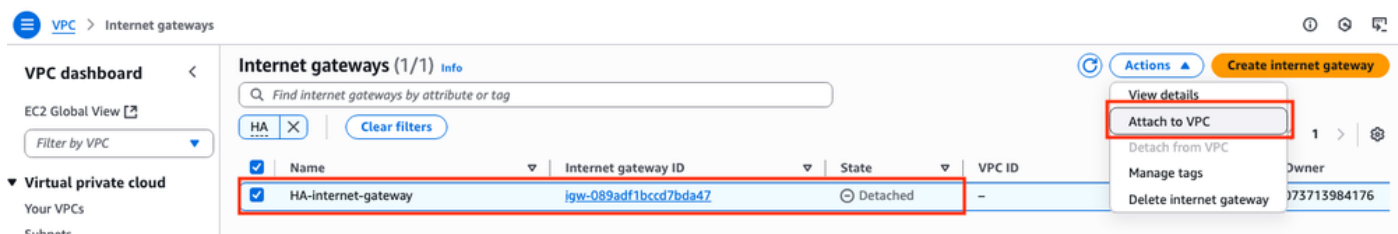
Dans la section **Tableau de bord VPC > Cloud privé virtuel > Passerelles Internet**, cliquez sur **Créer une passerelle Internet**.



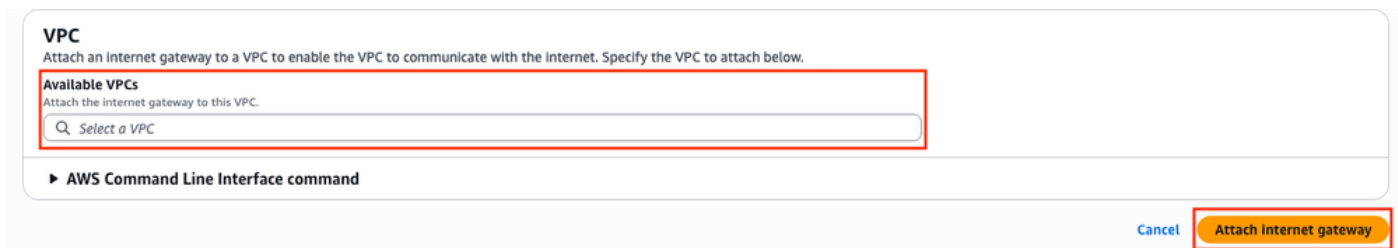
Dans cette nouvelle section, créez une **balise de nom** pour cette passerelle et cliquez sur **Créer une passerelle Internet**.



Une fois l'IGW créé, reliez-le à votre VPC correspondant. Accédez à la section **Tableau de bord VPC > Cloud privé virtuel > Passerelle Internet** et sélectionnez l'IGW correspondant. Cliquez sur **Actions > Attach to VPC**.



Dans cette nouvelle section, sélectionnez le VPC appelé **HA**. Pour cet exemple, cliquez sur **Attach internet gateway**.



L'IGW doit indiquer l'état Attached tel qu'il est affiché :

VPC dashboard < igw-089adf1bccd7bda47

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

igw-089adf1bccd7bda47 / HA-internet-gateway

Actions

Details

Internet gateway ID: igw-089adf1bccd7bda47

State: Attached

VPC ID: vpc-0d30b9fa9511f3639 | HA

Owner: 073713984176

Tags

Search tags

Key: Name, Value: HA-internet-gateway

Manage tags

Étape 10. Création et configuration de tables de routage sur AWS pour les sous-réseaux publics et privés

Étape 10.1. Création et configuration de la table de routage publique

Afin d'établir la haute disponibilité sur cette topologie, associez tous les sous-réseaux publics et privés sur leurs tables de routage correspondantes. Dans la section Tableau de bord VPC > Cloud privé virtuel > Tables de routage, cliquez sur Créer une table de routage.

Route tables (6) Info

Last updated 2 minutes ago

Actions

Create route table

Find route tables by attribute or tag

Name, Route table ID, Explicit subnet associations, Edge associations, Main

Dans la nouvelle section, sélectionnez le VPC correspondant à cette topologie. Une fois sélectionné, cliquez sur Create route table.

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

Create a tag with a key of 'Name' and a value that you specify.

Public-Routes

VPC

The VPC to use for this route table.

vpc-0d30b9fa9511f3639 (HA)

Tags

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.

Key: Name, Value - optional: Public-Routes

Add new tag

You can add 49 more tags.

Cancel, Create route table

Dans la section Tables de routage, sélectionnez la table créée et cliquez sur Actions > Modifier les associations de sous-réseau.

Menu icon VPC > Route tables

EC2 Global View [icon]
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 X 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

Create route table

Sélectionnez ensuite les sous-réseaux correspondants et cliquez sur Save associations.

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (3/6)

Filter subnet associations

public X 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 X subnet-04fb9de939e3778bb / Public-VM-linux-1c - fsmmond X subnet-02d8108842f9f3129 / public-R2-C8000v X

Cancel Save associations

Une fois les sous-réseaux associés, cliquez sur le lien hypertexte ID de table de routage pour ajouter les routes appropriées pour la table. Cliquez ensuite sur Edit Routes:

Route tables (1/1) Info

Find route tables by attribute or tag

public-routes X Clear filters

☒	Name	Route table ID
☒	Public-Routes	rtb-0d0e48f25c9b00635

Afin d'obtenir l'accès à Internet, cliquez sur Add route et liez cette table de route publique avec le IGW créé à l'étape 9 avec ces paramètres. Une fois sélectionné, cliquez sur Enregistrer les modifications :

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](#)

Étape 10.2. Création et configuration de la table de routage privée

Maintenant que la table de routage publique est créée, répliquez les étapes 10 pour la route privée et les sous-réseaux privés, à l'exception de l'ajout de la passerelle Internet sur ses routes. Pour cet exemple, la table de routage ressemble à ceci puisque le trafic pour 8.8.8.8 doit passer par le sous-réseau privé dans cet exemple :

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](#)

Étape 11. Vérification et configuration de la configuration réseau de base, de la traduction d'adresses de réseau (NAT), du tunnel GRE avec BFD et du protocole de routage

Une fois que les instances et leur configuration de routage sur AWS sont préparées, configurez les périphériques :

Configuration de 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

```

Configuration de 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

```

Étape 12. Configuration de la haute disponibilité (Cisco IOS® XE Denali 16.3.1a ou version ultérieure)

Maintenant que la redondance et la connexion entre les machines virtuelles sont définies, configurez les paramètres de haute disponibilité pour définir les modifications de routage. Définissez les valeurs Route-table-id, Network-interface-id et CIDR qui doivent être définies après

une erreur AWS HA telle que BFD peer down.

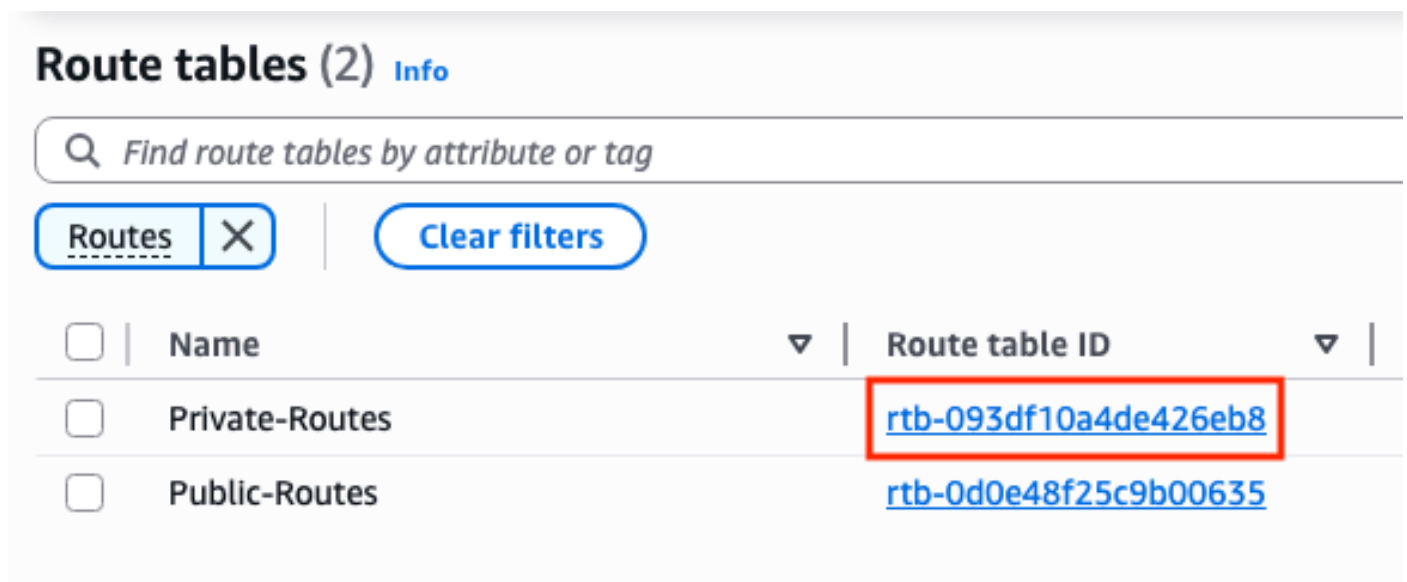
```
Router(config)# redundancy
Router(config-red)# cloud provider aws (node-id)
bfd peer <IP address of the remote device>
route-table <Route table ID>
cidr ip <traffic to be monitored/prefix>
eni <Elastic network interface (ENI) ID>
region <region-name>
```

Le paramètre bfd peer est lié à l'adresse IP de l'homologue de tunnel. Ceci peut être vérifié en utilisant la sortie show bfd neighbor :

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

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

Le paramètre route-table est lié à l'ID de table de routage privée situé dans la section Tableau de bord VPC > Cloud privé virtuel > Tables de routage. Copiez l'ID de table de routage correspondant.



The screenshot shows the AWS Management Console interface for 'Route tables (2)'. It includes a search bar, a filter button labeled 'Routes', and a 'Clear filters' button. Below, a table lists route tables. The 'Private-Routes' entry is highlighted with a red box, showing its ID as 'rtb-093df10a4de426eb8'. The 'Public-Routes' entry shows its ID as 'rtb-0d0e48f25c9b00635'.

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

Le paramètre cidr ip est lié au préfixe de route ajouté sur la table de route privée (routes créées à l'étape 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)

Filter routes

Destination



Target

8.8.8.8/32

eni-0239fda341b4d7e41

10.100.0.0/16

local

Le paramètre eni est associé à l'ID ENI de l'interface privée correspondante de l'instance en cours de configuration. Pour cet exemple, l'ID ENI de l'interface GigabitEthernet2 de l'instance est utilisé :

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 passec	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	IPv4
eni-0645a881c13823696	0	0	-	10.100.110.254	10.100.10.254	-	-
eni-070e14fbfde0d8e3b	1	0	-	-	10.100.110.254	-	-

Le paramètre region est associé au nom de code trouvé dans la documentation AWS pour la région où le VPC est situé. Pour cet exemple, la région us-east-1 est utilisée.

Toutefois, cette liste peut changer ou s'allonger. Pour obtenir les dernières mises à jour, consultez le document [AmazonRegion and Availability Zones](#).

En tenant compte de toutes ces informations, voici l'exemple de configuration pour chaque routeur du VPC :

Exemple de configuration pour 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
```

Exemple de configuration pour 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
```

Vérification

1. Vérifiez l'état de l'instance C8000v R1. Vérifiez que la redondance du tunnel et du cloud est opérationnelle.

```
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. Exécutez une requête ping continue vers 8.8.8.8 à partir de la machine virtuelle hôte qui se trouve derrière les routeurs. Assurez-vous que la requête ping passe par l'interface privée :

```
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. Ouvrez l'interface utilisateur graphique Web AWS et vérifiez l'état de la table de routage. L'interface ENI actuelle appartient à l'interface privée de l'instance de R1 :

rtb-093df10a4de426eb8 / Private-Routes

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (2)		Both	Edit routes
Destination	Target		
8.8.8.8/32	eni-070e14fbfde0d8e3b		
10.100.0.0/16	local		

4. Déclenchez le changement de route en arrêtant l'interface Tunnel1 sur l'instance R1 pour simuler un événement de basculement de haute disponibilité :

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

5. Vérifiez à nouveau dans la table de routage sur AWS, l'ID ENI a changé en l'ID ENI de l'interface privée de R2 :

Routes (2)

Destination



Target

8.8.8.8/32

[eni-0239fda341b4d7e41](#)

10.100.0.0/16

local

Dépannage

Voici la plupart des points communs souvent oubliés/mal configurés lors de la recreation du déploiement :

- Assurez-vous que les ressources sont associées. Lors de la création de VPC, de sous-réseaux, d'interfaces, de tables de routage, etc., bon nombre d'entre eux ne sont pas associés automatiquement. Ils ne se connaissent pas.
- Assurez-vous que l'adresse IP élastique et toute adresse IP privée sont associées aux interfaces appropriées, avec les sous-réseaux appropriés, ajoutées à la table de routage appropriée, connectées au routeur approprié, et au VPC et à la zone appropriés, liés au rôle IAM et aux groupes de sécurité.
- Désactivez le contrôle de la source/destination par ENI.
Si vous avez déjà vérifié tous les points abordés dans cette section et que le problème persiste, collectez ces résultats, testez le basculement de la haute disponibilité, si possible, et ouvrez un dossier auprès du TAC Cisco :

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.