

Guide de déploiement de la redondance CSR1000v HA sur Amazon AWS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Objectif](#)

[Topologie](#)

[Diagramme du réseau](#)

[Terminologie](#)

[Restrictions](#)

[Configuration](#)

[Étape 1. Choisissez une région.](#)

[Étape 2 : création d'un VPC](#)

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

[Étape 4. Créez un rôle IAM avec une stratégie et associez-le au VPC.](#)

[Étape 5. Lancez les CSR1000v avec le rôle AMI que vous avez créé et associez les sous-réseaux publics/privés.](#)

[Étape 6. Répétez l'étape 5 et créez la deuxième instance CSR1000v pour HA.](#)

[Étape 7. Répétez l'étape 5 et créez une machine virtuelle \(Linux/Windows\) à partir d'AMI Marketplace.](#)

[Étape 8 : configuration des tables de routage privée et publique](#)

[Étape 9 : configuration de la traduction d'adresses de réseau \(NAT\) et du tunnel GRE avec BFD et tout protocole de routage](#)

[Étape 10. Configuration de la haute disponibilité \(Cisco IOS XE Denali 16.3.1a ou version ultérieure\)](#)

[Vérifier la haute disponibilité](#)

[Dépannage](#)

[Problème : httpc_send_request a échoué](#)

[Problème : la table de routage rtb-9c000f4 et l'interface eni-32791318 appartiennent à des réseaux différents](#)

[Problème : Vous n'êtes pas autorisé à effectuer cette opération. Message d'échec d'autorisation codé.](#)

[Informations connexes](#)

Introduction

Ce document décrit le guide de configuration sur la façon de déployer des routeurs CSR1000v pour la haute disponibilité sur le cloud Amazon AWS. Il vise à donner aux utilisateurs une connaissance pratique de la haute disponibilité et la capacité de déployer un banc d'essai entièrement fonctionnel.

Pour plus d'informations sur AWS et HA, *reportez-vous* à la section.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Un compte Amazon AWS
- 2 CSR1000v et 1 AMI Linux/Windows dans la même région
- HA version 1 est pris en charge sur Cisco IOS-XE® versions 16.5 à 16.9. À partir de la version 16.11, utilisez HA version 3.

Components Used

Les informations contenues dans ce document sont basées sur Cisco IOS-XE® Denali 16.7.1.

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.

Objectif

Dans un environnement à zones de disponibilité multiples, simulez le trafic continu du data center privé (VM) vers Internet. Simulez un basculement de haute disponibilité et observez que la haute disponibilité réussit lorsque la table de routage commute le trafic de CSRHA vers l'interface privée de CSRHA1.

Topologie

Avant de commencer la configuration, il est important de bien comprendre la topologie et la conception. Cela permet de résoudre les problèmes potentiels ultérieurement.

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 :

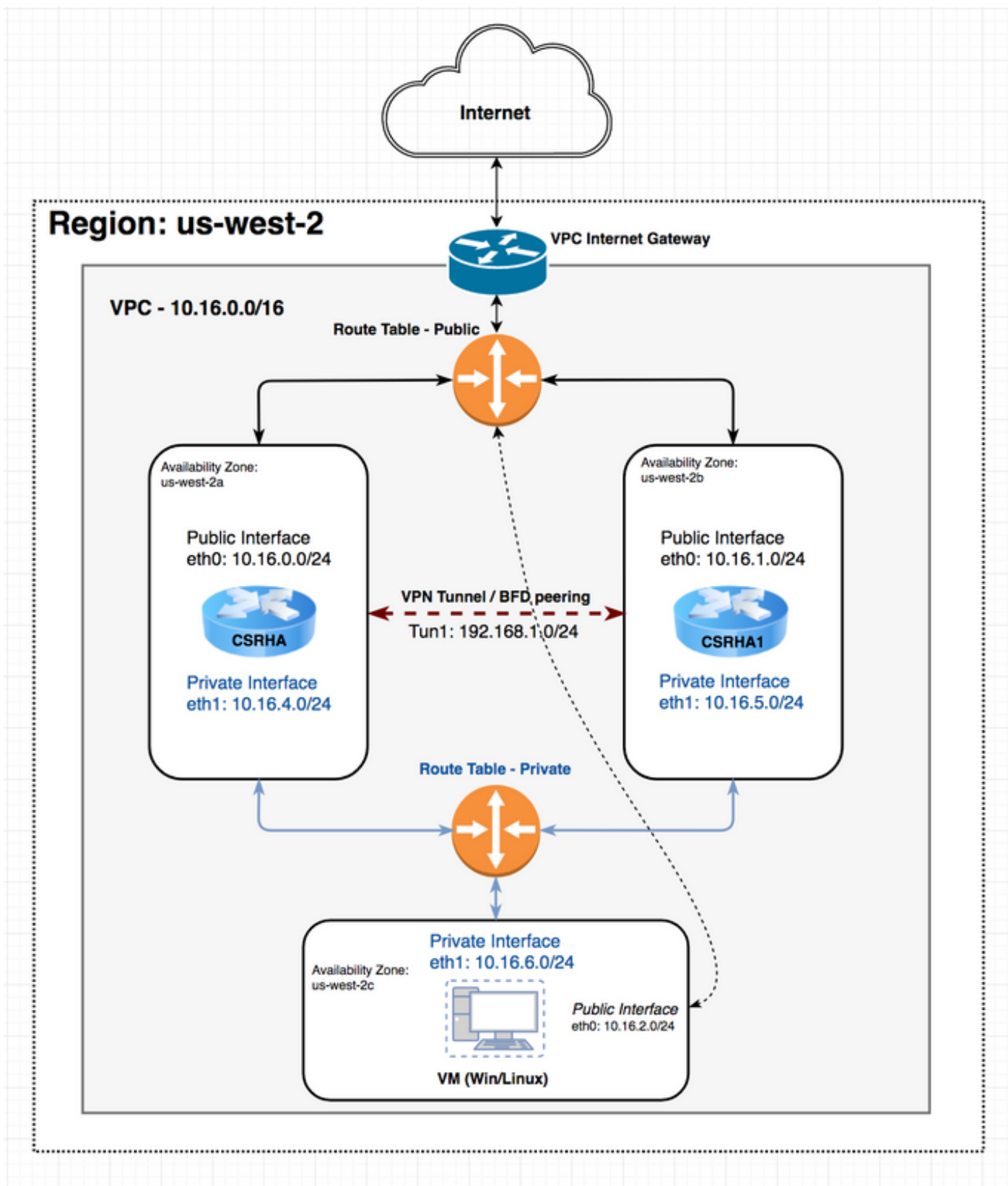
- 1x - Région
- 1x - VPC
- 3x - Zones de disponibilité
- 6x - Interfaces/sous-réseaux réseau (3x face publique/3x face privée)
- 2x - Tables de routage (publiques et privées)
- 2x - routeurs CSR1000v (Cisco IOS-XE® Denali 16.3.1a ou version ultérieure)
- 1x - VM (Linux/Windows)

Une paire haute disponibilité comprend deux routeurs CSR1000v, 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 sur afin que vous puissiez accéder à la machine virtuelle et la configurer. En général, tout le trafic normal doit transiter par la table de routage privé.

Envoyez une requête ping à l'interface privée de la VM → table de routage privé → CSRHA → 8.8.8.8 pour la simulation du trafic. Dans un scénario de basculement, observez que la table de routage privé a commuté la route vers l'interface privée de CSRHA1.

Diagramme du réseau



Terminologie

RTB : ID de la table de routage.

CIDR : adresse de destination de la route à mettre à jour dans la table de routage.

ENI : ID d'interface réseau de l'interface Gigabit CSR 1000v vers laquelle le trafic est acheminé. Par exemple, si CSRHA échoue, CSRHA1 prend le relais et met à jour la route dans la table de

route AWS pour pointer vers son propre ENI.

REGION - Région AWS de CSR 1000v.

Restrictions

- Pour les sous-réseaux privés, n'utilisez pas l'adresse IP 10.0.3.0/24, qui est utilisée en interne sur le routeur Cisco CSR 1000v pour la haute disponibilité. Le routeur Cisco CSR 1000v doit disposer d'une accessibilité Internet publique pour effectuer des appels REST API qui modifient la table de routage AWS.
- Ne placez pas l'interface gig1 du routeur CSR1000v dans un VRF. La haute disponibilité ne fonctionne pas autrement.

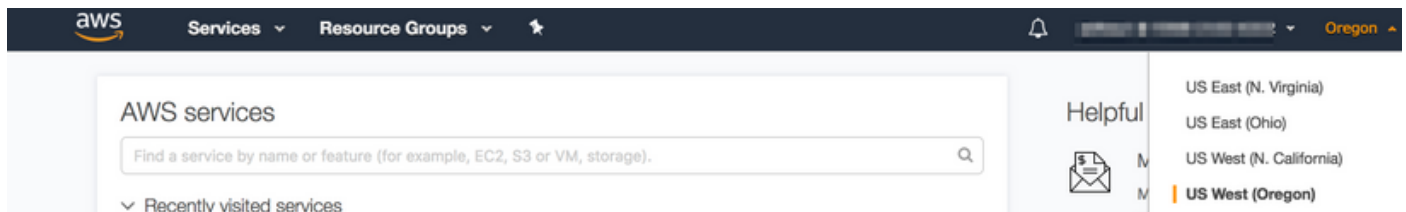
Configuration

Le flux général de configuration doit commencer par la fonctionnalité la plus englobante (Région/VPC) et descendre jusqu'à la fonctionnalité la plus spécifique (Interface/sous-réseau). Cependant, il n'existe pas d'ordre de configuration spécifique. Avant de commencer, il est important de bien comprendre la topologie.

Astuce : Donnez des noms à tous vos paramètres (VPC, Interface, Sous-réseau, Tables de routage, etc.).

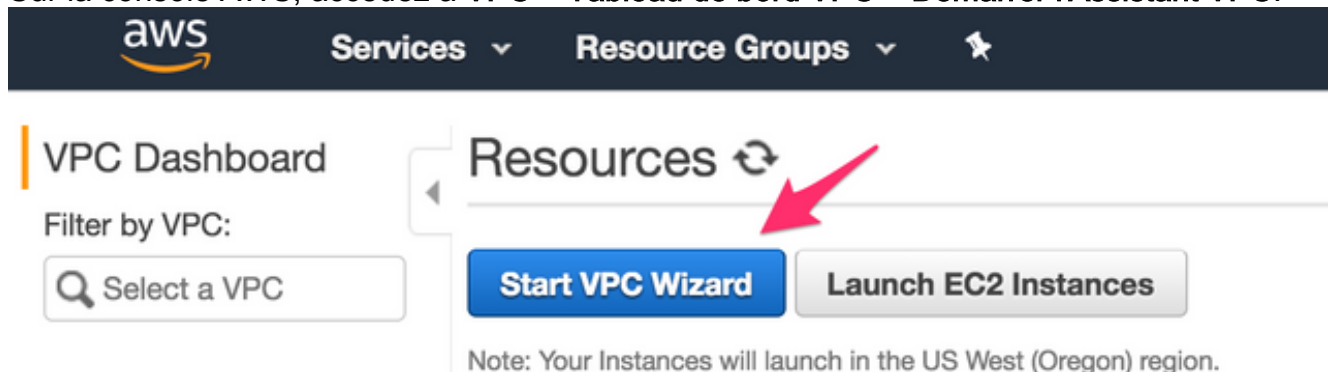
Étape 1. Choisissez une région.

Cet exemple utilise US West (Oregon).



Étape 2 : création d'un VPC

1. Sur la console AWS, accédez à VPC > Tableau de bord VPC > Démarrer l'Assistant VPC.



2. Sélectionnez VPC avec un sous-réseau public unique.

Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

Creates:

A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.

Select

Internet, S3, DynamoDB, SNS, SQS, etc.

Public Subnet

Amazon Virtual Private Cloud

3. Lorsque vous créez un VPC, un réseau /16 vous est affecté pour être utilisé comme vous le souhaitez.

4. Un sous-réseau public /24 vous est également attribué. Les instances de sous-réseau public utilisent des adresses IP élastiques ou des adresses IP publiques pour que vos périphériques puissent accéder à Internet.

Step 2: VPC with a Single Public Subnet

IPv4 CIDR block*: 10.16.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: No IPv6 CIDR Block
 Amazon provided IPv6 CIDR block

VPC name: HA

Public subnet's IPv4 CIDR*: 10.16.0.0/24 (251 IP addresses available)

Availability Zone*: No Preference

Subnet name: Public subnet

You can add more subnets after AWS creates the VPC.

Service endpoints

Enable DNS hostnames*: Yes No

Hardware tenancy*: Default

5. vpc-b98d8ec0 est créé.

VPC Dashboard

Filter by VPC:

Virtual Private Cloud

Your VPCs

Search VPCs and their proper X

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR
<input type="checkbox"/>	HA	vpc-b98d8ec0	available	10.16.0.0/16

Étape 3 : création d'un groupe de sécurité pour le VPC

Les groupes de sécurité sont comme des listes de contrôle d'accès pour autoriser ou refuser le trafic.

1. Sous Sécurité, cliquez sur **Groupes de sécurité** et créez votre groupe de sécurité associé au VPC créé ci-dessus nommé HA.



2. Sous Inbound Rules, définissez le trafic que vous souhaitez autoriser pour sg-1cf47d6d. Dans cet exemple, vous autorisez tout le trafic.

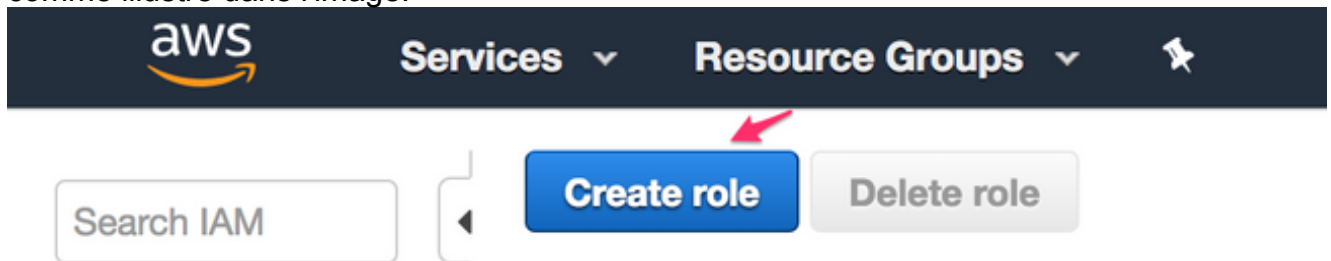


Étape 4. Créez un rôle IAM avec une stratégie et associez-le au VPC.

IAM accorde à votre CSR l'accès aux API Amazon.

Le routeur CSR1000v est utilisé comme proxy pour appeler les commandes de l'API AWS afin de modifier la table de routage. Par défaut, les AMI ne sont pas autorisés à accéder aux API. Cette procédure crée un rôle IAM qui est utilisé lors du lancement d'une instance CSR. IAM fournit les informations d'identification d'accès permettant aux CSR d'utiliser et de modifier les API AWS.


1. Créer un rôle IAM. Accédez au tableau de bord IAM et accédez à **Rôles > Créer un rôle**, comme illustré dans l'image.





2. Comme l'illustre l'image, autorisez l'instance EC2 à appeler AWS en votre nom.

Create role

Select type of trusted entity

**AWS service**
EC2, Lambda and others

**Another AWS account**
Belonging to you or 3rd party

**Web identity**
Cognito or any OpenID provider

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

3. Créez un rôle et cliquez sur **Suivant : Vérifiez**, comme le montre l'image.

Create role

1 2 3

Attach permissions policies

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

[Create policy](#) [Refresh](#)

Filter: Policy type Showing 394 results

	Policy name	Attachments	Description
<input type="checkbox"/>	AdministratorAccess	7	Provides full access to AWS services and resources.
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	0	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessFullAccess	0	Grants full access to AlexaForBusiness resources and acces...
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	0	Provide gateway execution access to AlexaForBusiness serv...
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	0	Provide read only access to AlexaForBusiness services
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	0	Provides full access to create/edit/delete APIs in Amazon AP...
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	0	Provides full access to invoke APIs in Amazon API Gateway.
<input type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	0	Allows API Gateway to push logs to user's account.
<input type="checkbox"/>	AmazonAppStreamFullAccess	0	Provides full access to Amazon AppStream via the AWS Ma...
<input type="checkbox"/>	AmazonAppStreamReadOnlyAccess	0	Provides read only access to Amazon AppStream via the AW...
<input type="checkbox"/>	AmazonAppStreamServiceAccess	0	Default policy for Amazon AppStream service role.
<input type="checkbox"/>	AmazonAthenaFullAccess	0	Provide full access to Amazon Athena and scoped access to...

* Required

Cancel

Previous

Next: Review

4. Donnez-lui un nom de rôle. Pour cet exemple, comme le montre l'image, le nom du rôle est **routetablechange**.

Create role

Review

Provide the required information below and review this role before you create it.

Role name*

routetablechange

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

5. Ensuite, vous devez créer une stratégie et l'associer au rôle que vous avez créé ci-dessus. Tableau de bord IAM et accédez à **Politiques > Créer une politique**.

aws Services Resource Groups

Search IAM Create policy Policy actions

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

Create policy

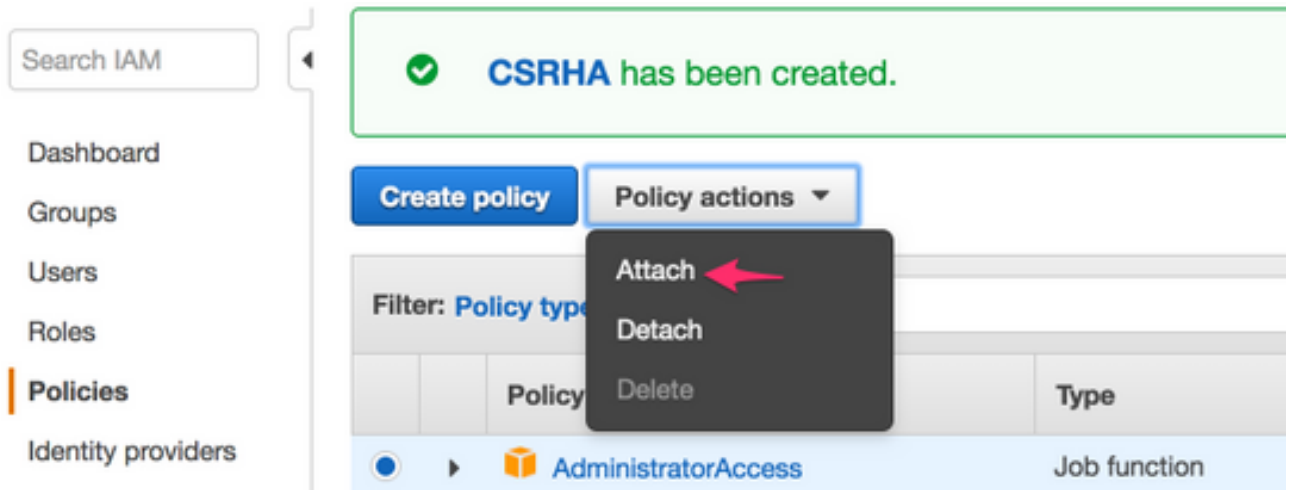
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

This policy validation failed and might have errors converting to JSON: The policy must have at least one statement For more information about the IAM policy grammar, see [AWS IAM Policies](#)

Visual editor JSON Import managed policy

```
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".
```

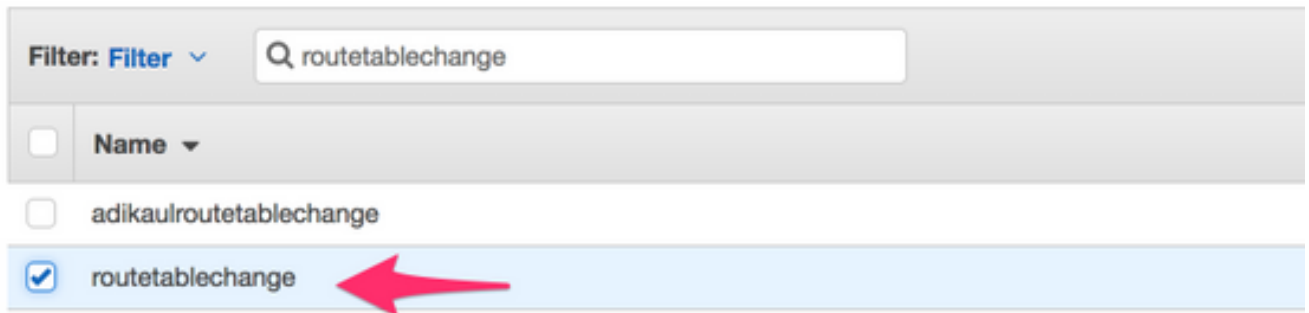
6. Donnez-lui un nom de stratégie et associez-le au rôle que vous avez créé. Dans cet exemple, le nom de la stratégie est CSRHA avec accès administrateur, comme illustré dans l'image.



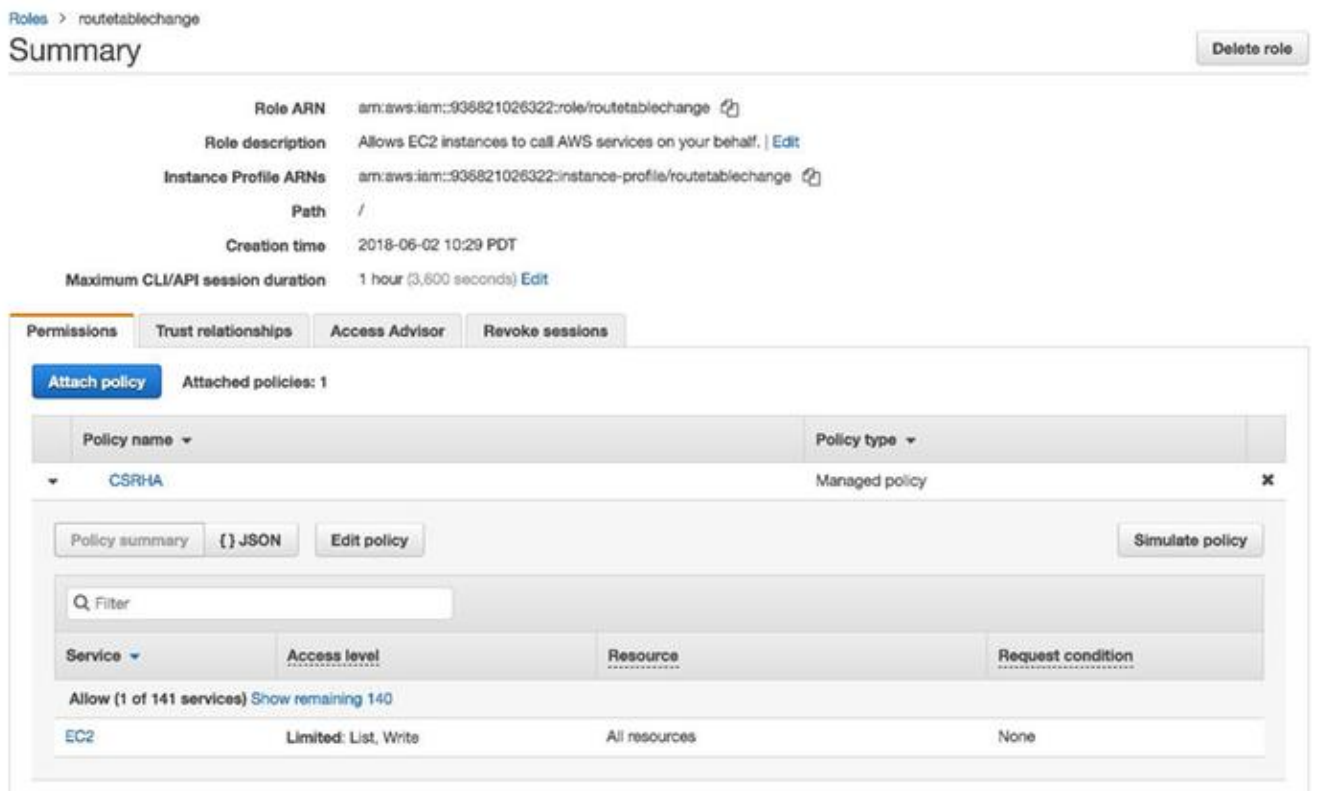
7. Comme l'illustre l'image, associez la stratégie au rôle que vous avez créé appelé **routetablechange**.

Attach Policy

Attach the policy to users, groups, or roles in your account.



8. Résumé.



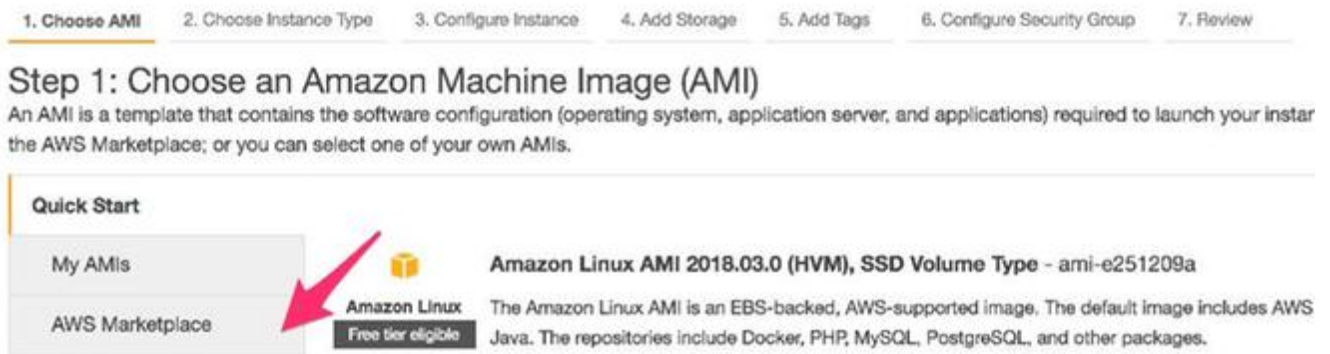
Étape 5. Lancez les CSR1000v avec le rôle AMI que vous avez créé et associez les sous-réseaux publics/privés.

Chaque routeur CSR1000v possède 2 interfaces (1 publique, 1 privée) et se trouve dans sa propre zone de disponibilité. Vous pouvez penser que chaque CSR se trouve dans des data centers distincts.

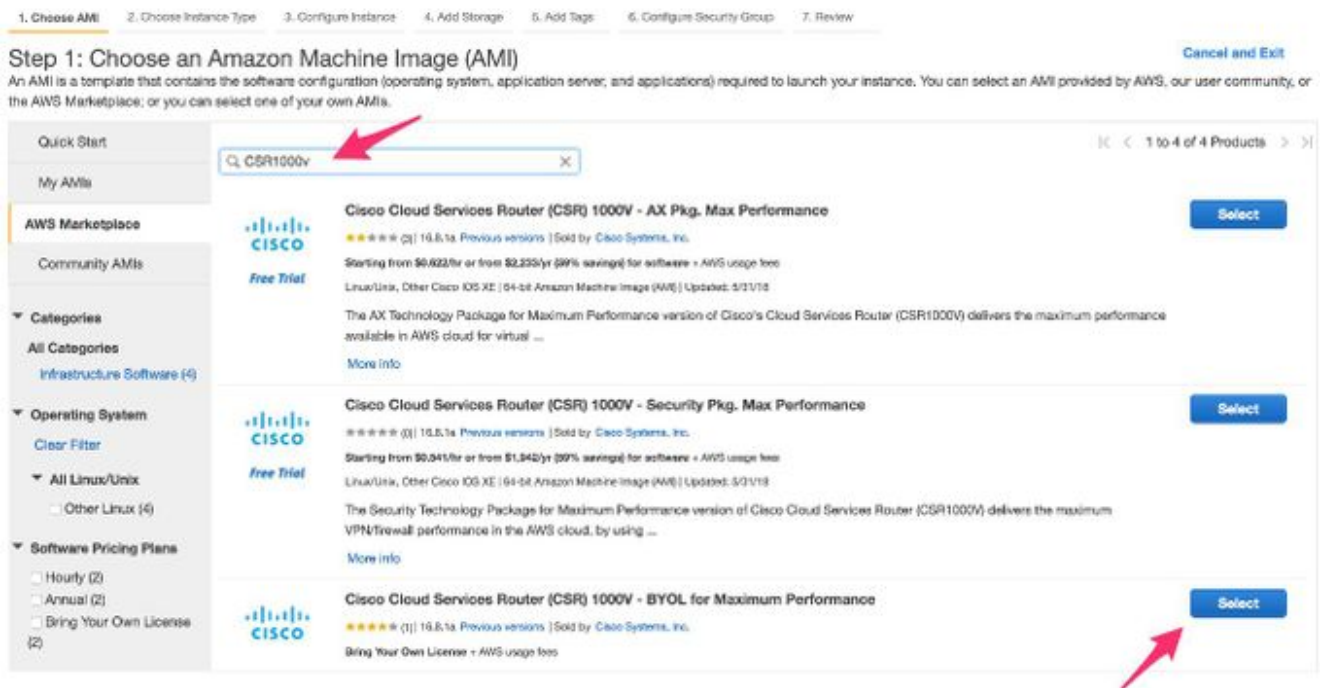
1. Sur la console AWS, sélectionnez **EC2**, puis cliquez sur **Launch Instance**.



2. Sélectionnez AWS Marketplace.



3. Entrez CSR1000v et, dans cet exemple, utilisez le routeur de services cloud Cisco (CSR) 1000V - BYOL pour des performances maximales.



4. Sélectionnez un type d'instance. Dans cet exemple, le type sélectionné est **t2.medium**.

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.medium (Variable ECU's, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 4 GiB memory, EBS only)

Note: The vendor recommends using a c4.large instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

5. Lorsque l'instance est configurée, vous devez vous assurer de sélectionner le VPC que vous avez créé ci-dessus avec le rôle IAM ci-dessus. En outre, créez un sous-réseau privé que vous associez à l'interface privée.

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: Request Spot instances

Network: vpc-a6fedef | HA [Create new VPC](#)
No default VPC found. [Create a new default VPC.](#)

Subnet: subnet-66f7931f | Public subnet | us-west-2a [Create new subnet](#)
251 IP Addresses available

Auto-assign Public IP: Use subnet setting (Disable)

Placement group: Add instance to placement group

IAM role: routetablechange [Create new IAM role](#)

Shutdown behavior: Stop

Enable termination protection: Protect against accidental termination

Monitoring: Enable CloudWatch detailed monitoring
Additional charges apply.

6. Cliquez sur Create new Subnet for Private Subnet. Dans cet exemple, la balise Name est HA Private. Assurez-vous qu'il se trouve dans la même zone de disponibilité que le sous-réseau public.

Create Subnet



Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: HA Private

VPC: vpc-a6fefedf | HA

VPC CIDRs	CIDR	Status	Status Reason
	10.16.0.0/16	associated	

Availability Zone: us-west-2a

IPv4 CIDR block: 10.16.4.0/24

Cancel Yes, Create

7. Faites défiler vers le bas et sous Configurer les détails de l'instance, cliquez sur **Ajouter un périphérique**, comme illustré dans l'image.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-66f7931f	Auto-assign	Add IP	

Add Device

8. Une fois l'interface secondaire ajoutée, associez le sous-réseau privé que vous avez créé appelé HA Private. Eth0 est l'interface publique et Eth1 est l'interface privée. **Note:** Le sous-réseau créé à l'étape précédente peut ne pas apparaître dans cette liste déroulante. Vous devrez peut-être actualiser ou annuler la page et recommencer pour que le sous-réseau apparaisse.

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-66f7931f	Auto-assign	Add IP	
eth1	New network interface	subnet-66f7931f (Public subnet) 10.16.0.0/24 us-west-2a ✓ subnet-89c5a1f0 (HA Private) 10.16.4.0/24 us-west-2a			

9. Sélectionnez le groupe de sécurité que vous avez créé sous VPC et assurez-vous que les règles sont correctement définies.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group Select an existing security group

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-01880170	default	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-1cf47d6d	HA	HA	Copy to new

10. Créez une nouvelle paire de clés et assurez-vous de télécharger votre clé privée. Vous pouvez réutiliser une clé pour chaque périphérique. **Note:** Si vous perdez votre clé privée, vous ne pourrez plus vous connecter à votre CSR. Il n'existe aucune méthode de récupération des clés.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name
CSRHA

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel Launch Instances

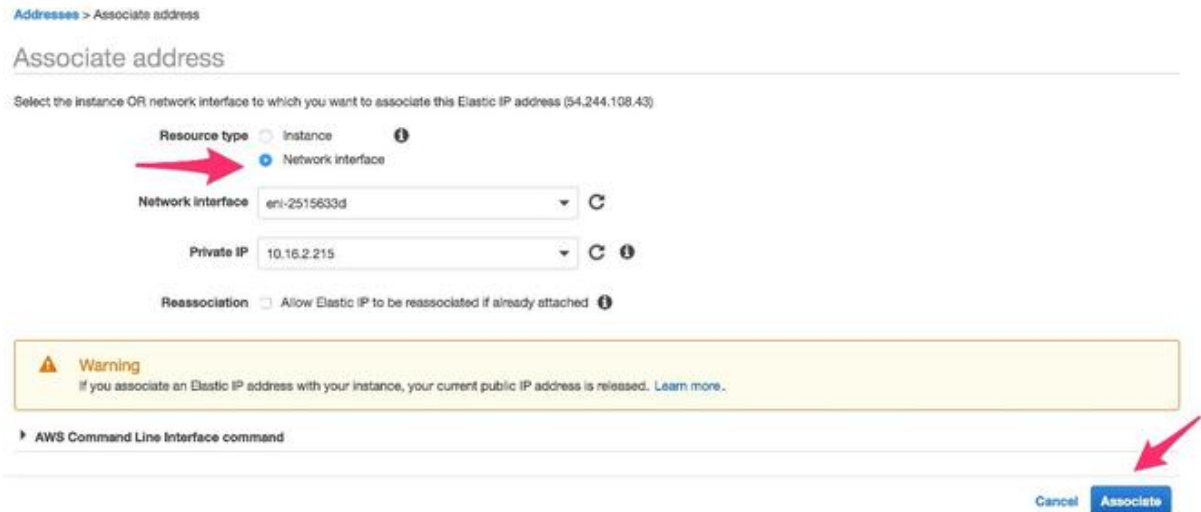
11. Associez l'IP élastique à l'ENI de l'interface publique pour l'instance que vous avez créée et accédez à **AWS console > EC2 Management > Network Security > Elastic IP's**. **Note:** La terminologie publique/privée peut vous dérouter ici. Pour les besoins de cet exemple, la définition d'une interface publique est Eth0, qui est l'interface Internet. Du point de vue d'AWS, notre interface publique est leur adresse IP privée.

EC2 Dashboard

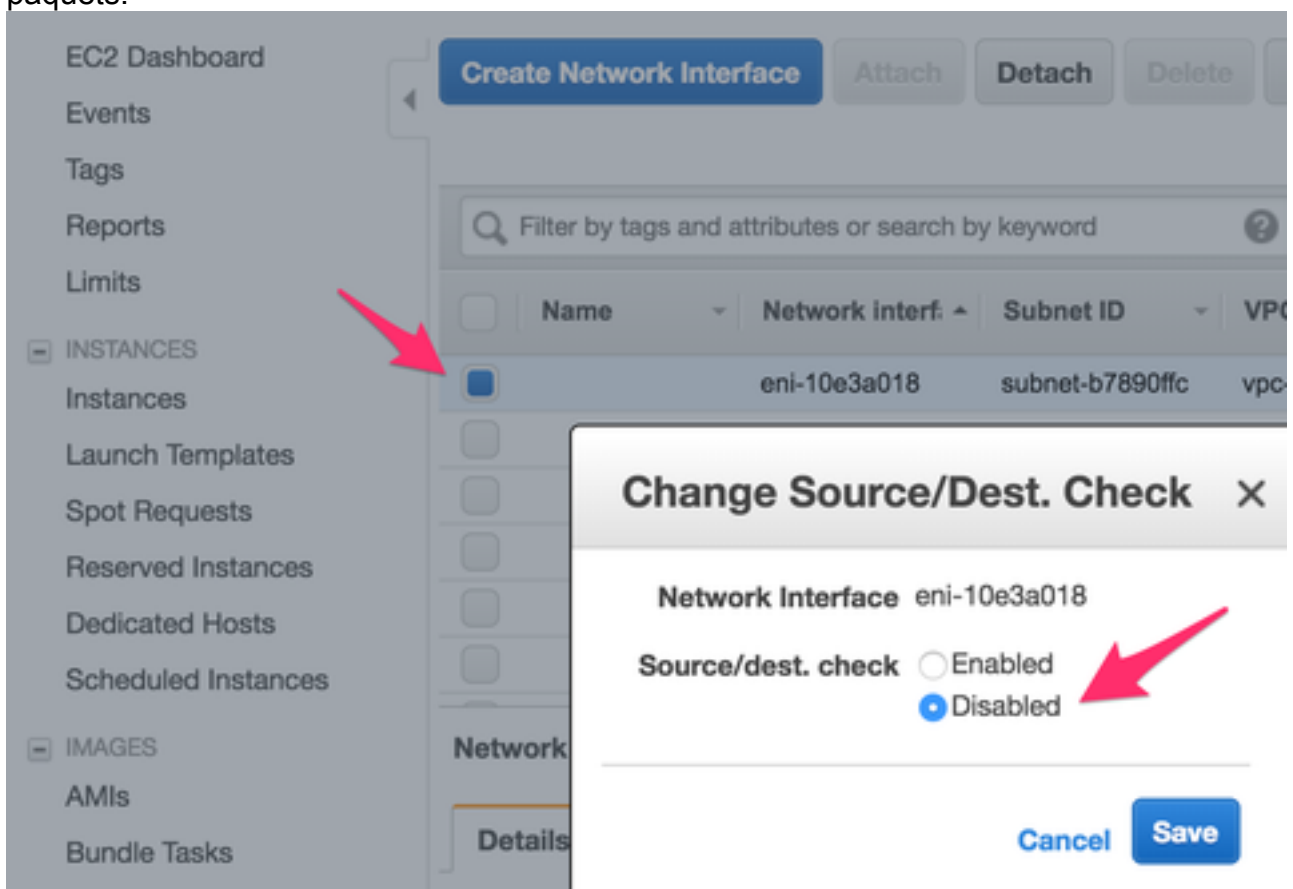
Events

Allocate new address

Actions



12. Désactivez Source/Dest Check lorsque vous accédez à **EC2 > Network Interfaces**. Vérifiez chaque ENI pour le contrôle Source/Dest. Par défaut, cette vérification de la source/destination est activée pour tous les ENI. Fonction anti-usurpation destinée à éviter qu'un ENI soit submergé par du trafic qui n'est pas réellement destiné à lui en vérifiant que l'ENI est la destination du trafic avant de le transmettre. Le routeur est rarement la destination réelle d'un paquet. Cette fonctionnalité doit être désactivée sur tous les ENI de transit CSR ou elle ne peut pas transférer de paquets.



13. Connectez-vous à votre routeur CSR1000v. **Note:** Le nom d'utilisateur fourni par AWS à SSH dans le CSR1000v peut être incorrectement répertorié comme racine. Remplacez-le par `ec2-user` si nécessaire. **Note:** Vous devez pouvoir envoyer une requête ping à l'adresse DNS vers SSH dans. Le voici : `ec2-54-208-234-64.compute-1.amazonaws.com`. Vérifiez que le sous-réseau/eni public du routeur est associé à la table de routage publique. Passez brièvement à l'étape 8 pour savoir comment associer le sous-réseau à la table de

routage.

Connect To Your Instance ✕

I would like to connect with A standalone SSH client
 A Java SSH Client directly from my browser (Java required)

To access your instance:

1. Open an SSH client. (find out how to [connect using PuTTY](#))
2. Locate your private key file (HA.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:

```
chmod 400 HA.pem
```
4. Connect to your instance using its Public DNS:

```
ec2-54-208-234-64.compute-1.amazonaws.com
```

Example:

```
ssh -i "HA.pem" root@ec2-54-208-234-64.compute-1.amazonaws.com
```

Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

[Close](#)

Étape 6. Répétez l'étape 5 et créez la deuxième instance CSR1000v pour HA.

Sous-réseau public : 10.16.1.0/24

Sous-réseau privé : 10.16.5.0/24

Si vous ne parvenez pas à envoyer une requête ping à l'adresse IP élastique de ce nouvel AMI, passez brièvement à l'étape 8 et vérifiez que le sous-réseau public est associé à la table de routage public.

Étape 7. Répétez l'étape 5 et créez une machine virtuelle (Linux/Windows) à partir d'AMI Marketplace.

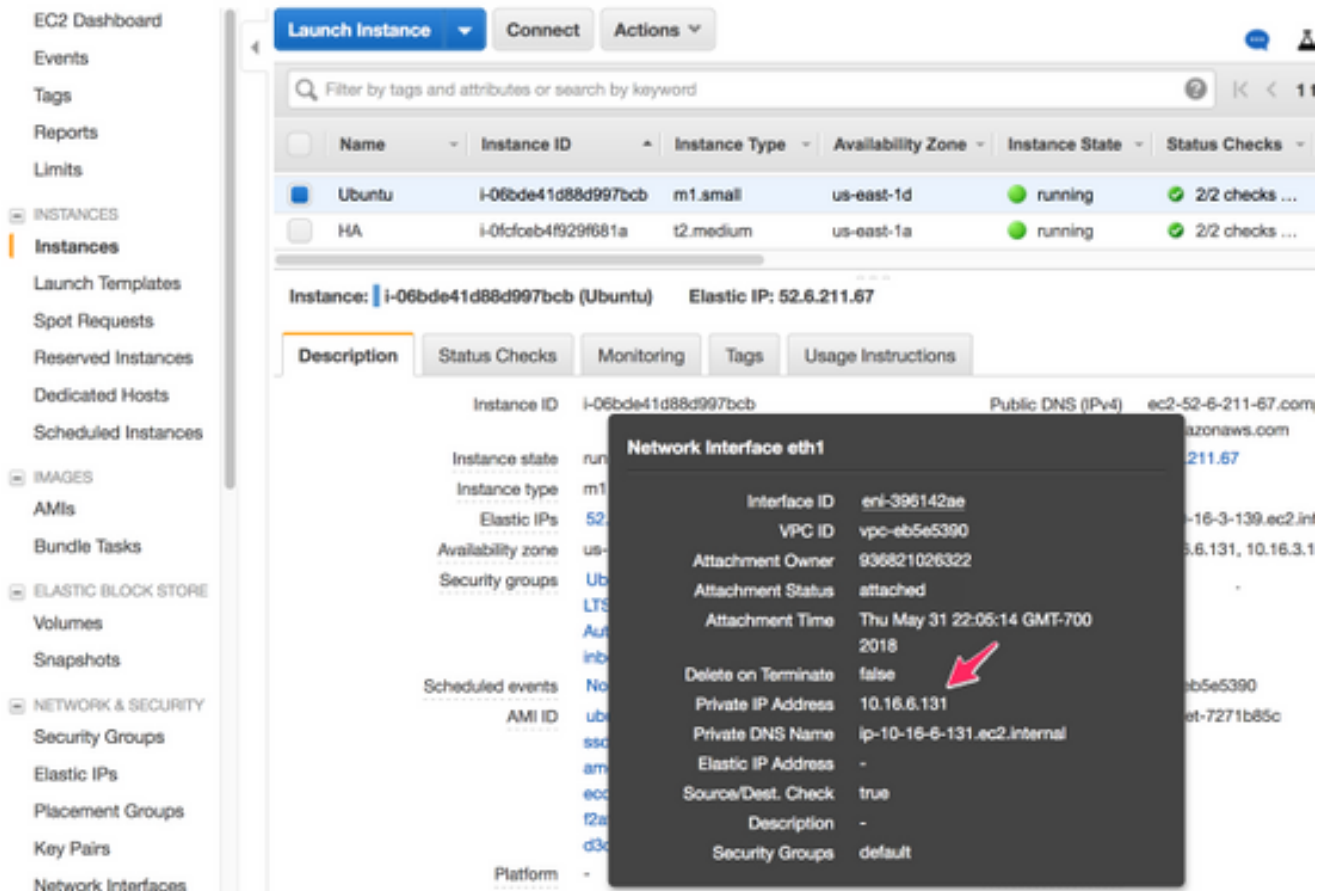
Pour cet exemple, utilisez Ubuntu Server 14.04 LTS sur le marché.

Sous-réseau public : 10.16.2.0/24

Sous-réseau privé : 10.16.6.0/24

Si vous ne parvenez pas à envoyer une requête ping à l'adresse IP élastique de ce nouvel AMI, passez brièvement à l'étape 8 et vérifiez que le sous-réseau public est associé à la table de routage public.

1. Eth0 est créé par défaut pour l'interface publique. Créez une deuxième interface appelée eth1 pour le sous-réseau privé.



2. L'adresse IP que vous configurez dans Ubuntu est l'interface privée eth1 attribuée par AWS.

```
ubuntu@ip-10-16-2-139:~$ cd /etc/network/interfaces.d/
```

```
ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo vi eth1.cfg
```

```
auto eth1
iface eth1 inet static
    address 10.16.6.131
    netmask 255.255.255.0
    network 10.16.6.0
up route add -host 8.8.8.8 gw 10.16.6.1 dev eth1
```

3. Effleurez l'interface ou redémarrez la machine virtuelle.

```
ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo ifdown eth1 && sudo ifup eth1
```

```
ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo reboot
```

4. Envoyez une requête ping 8.8.8.8 pour le test. Assurez-vous que la route 8.8.8.8 a été ajoutée à l'étape 7.

```
ubuntu@ip-10-16-2-139:~$ route -n
```

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

Si 8.8.8.8 n'est pas répertorié dans le tableau, ajoutez-le manuellement :

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

Étape 8 : configuration des tables de routage privée et publique

1. Lorsqu'un VPC est créé via l'assistant à l'étape 2, deux tables de routage sont automatiquement créées. S'il n'existe qu'une seule table de routage, créez-en une autre pour vos sous-réseaux privés, comme illustré dans l'image.

The image shows two screenshots from the AWS Management Console. The top screenshot shows the 'Create Route Table' dialog box. The 'Name tag' is 'HA PRIVATE' and the 'VPC' is 'vpc-b98d8ec0 | HA'. The bottom screenshot shows the 'Route Tables' list with two entries: 'HA PUBLIC' (rtb-2752415f) and 'HA PRIVATE' (rtb-ca5340b2). The 'HA PRIVATE' entry is selected, and the 'Routes' tab is active, showing a single route with destination '10.16.0.0/16' and target 'local'.

Create Route Table Dialog:

Name tag: HA PRIVATE
VPC: vpc-b98d8ec0 | HA

Route Tables List:

Name	Route Table ID	Explicitly Associat	Main	VPC
HA PUBLIC	rtb-2752415f	1 Subnet	No	vpc-39222f40 HA
HA PRIVATE	rtb-ca5340b2	0 Subnets	Yes	vpc-39222f40 HA

Route Details for rtb-ca5340b2 | HA PRIVATE:

Destination	Target	Status	Propagated
10.16.0.0/16	local	Active	No

2. Voici une vue des deux tables de routage. La passerelle Internet (igw-95377973) est automatiquement associée à la table de routage PUBLIC. Étiquetez ces deux tableaux en conséquence. La table PRIVATE NE doit PAS avoir cette route.

VPC Dashboard

Filter by VPC:

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Security

Network ACLs

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associat	Main	VPC
<input checked="" type="checkbox"/>	HA PUBLIC	rtb-2752415f	1 Subnet	No	vpc-39222f40 HA
<input type="checkbox"/>	HA PRIVATE	rtb-ca5340b2	0 Subnets	Yes	vpc-39222f40 HA

rtb-2752415f | HA PUBLIC

Summary Routes Subnet Associations Route Propagation Tags

Edit

View: All rules

Destination	Target	Status	Propagated
10.16.0.0/16	local	Active	No
0.0.0.0/0	igw-953779f3	Active	No

3. Associez les 6 sous-réseaux à la table de routage appropriée 3 Les interfaces publiques sont associées à la table de routage publique :Sous-réseaux publics : 10.16.0.0/24, 10.16.1.0/24, 10.16.2.0/24 3 Les interfaces privées sont associées à la table de routage privé :Sous-réseaux privés : 10.16.4.0/24, 10.16.5.0/24, 10.16.6.0/24

rtb-ec081d94 | HA PRIVATE

Summary Routes **Subnet Associations** Route Propagation Tags

Edit

Subnet	IPv4 CIDR	IPv6 CIDR
You do not have any subnet associations. The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:		

Étape 9 : configuration de la traduction d'adresses de réseau (NAT) et du tunnel GRE avec BFD et tout protocole de routage

Configurez le tunnel GRE (Generic Routing Encapsulation) via les adresses IP élastiques des routeurs CSR 1000v (recommandé pour éviter les problèmes de renouvellement de bail DHCP, qui détectent les erreurs). Les valeurs BFD (Bidirection Forwarding Detection) peuvent être configurées pour être plus agressives que celles indiquées dans cet exemple, si une convergence plus rapide est requise. Cependant, cela peut entraîner des événements d'homologue inactif BFD pendant une connectivité intermittente. Les valeurs de cet exemple détectent une défaillance d'homologue dans un délai de 1,5 seconde. Il existe un délai variable d'environ quelques secondes entre l'exécution de la commande AWS API et l'entrée en vigueur des modifications de

la table de routage VPC.

- Configuration sur CSRHA

GRE et BFD : utilisés pour observer les conditions de basculement haute disponibilité

```
interface Tunnell
  ip address 192.168.1.1 255.255.255.0
  bfd interval 500 min_rx 500 multiplier 3
  tunnel source GigabitEthernet1
  tunnel destination 52.10.183.185 /* Elastic IP of the peer CSR */
!
router eigrp 1
  bfd interface Tunnell
  network 192.168.1.0
  passive-interface GigabitEthernet1
```

NAT et routage : utilisés pour l'accessibilité Internet des VM via l'interface privée

```
interface GigabitEthernet1
  ip address dhcp
  ip nat outside
  no shutdown
!
interface GigabitEthernet2
  ip address dhcp
  ip nat inside
  no shutdown
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!
access-list 10 permit 10.16.6.0 0.0.0.255
!
ip route 10.16.6.0 255.255.255.0 GigabitEthernet2 10.16.4.1
```

- Configuration sur CSRHA1

GRE et BFD : utilisés pour observer les conditions de basculement haute disponibilité

```
interface Tunnell
  ip address 192.168.1.2 255.255.255.0
  bfd interval 500 min_rx 500 multiplier 3
  tunnel source GigabitEthernet1
  tunnel destination 50.112.227.77 /* Elastic IP of the peer CSR */
!
router eigrp 1
  bfd interface Tunnell
  network 192.168.1.0
  passive-interface GigabitEthernet1
```

NAT et routage : utilisés pour l'accessibilité Internet des VM via l'interface privée

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

```

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

```

Étape 10. Configuration de la haute disponibilité (Cisco IOS XE Denali 16.3.1a ou version ultérieure)

Surveillez les événements d'homologue BFD en configurant chaque CSR 1000v à l'aide de la commande `aws` du fournisseur cloud spécifiée ci-dessous. Utilisez cette commande pour définir les modifications de routage vers (VPC) Route-table-id, Network-interface-id et CIDR après la détection d'une erreur AWS HA, telle que BFD peer down.

```

CSR(config)# redundancy
CSR(config-red)# cloud provider [aws | azure] node-id
# bfd peer ipaddr
# route-table table-name
# cidr ip ipaddr/prefix
# eni elastic-network-intf-name
# region region-name

```

1. L'adresse IP de l'homologue `#bfd` est l'adresse IP du tunnel homologue.

```
CSRHA#show bfd neighbors
```

```

IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
192.168.1.2 4097/4097 Up Up Tu1

```

2. Le nom de table `#route-table` se trouve sous la console AWS, naviguez vers **VPC > Tables de routage**. Cette action modifie la table de routage privée.

The screenshot shows the AWS VPC console interface. On the left, the 'Route Tables' link is highlighted with a red arrow. The main content area displays a table of route tables. The 'HA PRIVATE' route table is selected, with a red arrow pointing to its name. The table has columns for 'Name' and 'Route Table ID'.

Name	Route Table ID
	rtb-7b746303
HA PUBLIC	rtb-ab091cd3
	rtb-a4495edc
HA PRIVATE	rtb-ec081d94

3. L'adresse/préfixe `#cidr ip ipaddr` est l'adresse de destination de la route à mettre à jour dans la table de routage. Sous la console AWS, accédez à **VPC > Tables de routage**. Faites défiler vers le bas, cliquez sur **Edit**, puis sur **Add another route**. Ajoutez l'adresse de destination de test 8.8.8.8 et l'ENI privé de la CSRHA.

rtb-ec081d94 | HA PRIVATE

Summary Routes Subnet Associations Route Propagation Tags

Edit

rtb-ec081d94 | HA PRIVATE

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

View: All rules

Destination	Target	Status	Propagated	Remove
10.16.0.0/16	local	Active	No	
8.8.8.8/32	eni-10e3a018	Active	No	✕

Add another route

4. Le nom #eni élastique-network-intf-name se trouve dans votre instance EC2. Cliquez sur votre interface privée eth1 pour chacun des CSR correspondants et utilisez l'ID d'interface.

Instances

Instance	AMI	Instance Type	Availability Zone	State	Checks
CSRHA	i-0223f5ca1d6068424	c4.large	us-west-2a	running	2/2 checks ...
CSRHA1	i-0bed9ff2bd6996ca4	t2.medium	us-west-2b	running	2/2 checks ...
WINDOWS	i-07a0fecde36302c6a	t2.small	us-west-2c	running	2/2 checks ...

Instance: i-0223f5ca1d6068424 (CSRHA) Elastic Network Interfaces

Interface ID	VPC ID	Attachment Owner	Attachment Status	Attachment Time	Delete on Terminate	Private IP Address	Private DNS Name	Elastic IP Address	Source/Dest. Check	Description	Security Groups
eni-90b500a8	vpc-19c1c060	936821026322	attached	Thu May 31 21:57:41 GMT-700 2018	true	10.16.4.198	ip-10-16-4-198.us-west-2.compute.internal	-	false	-	HAKAUL

Network interfaces eth0 eth1

5. Le nom #region est le nom de code trouvé dans le document AWS. Cette liste peut être modifiée ou étendue. Pour trouver les dernières mises à jour, consultez le document [Région et zones de disponibilité d'Amazon](#).

Code	Name
us-east-1	US East (N. Virginia)
us-east-2	US East (Ohio)
us-west-1	US West (N. California)
us-west-2	US West (Oregon)
ca-central-1	Canada (Central)
eu-central-1	EU (Frankfurt)
eu-west-1	EU (Ireland)
eu-west-2	EU (London)
eu-west-3	EU (Paris)
ap-northeast-1	Asia Pacific (Tokyo)
ap-northeast-2	Asia Pacific (Seoul)
ap-northeast-3	Asia Pacific (Osaka-Local)
ap-southeast-1	Asia Pacific (Singapore)
ap-southeast-2	Asia Pacific (Sydney)
ap-south-1	Asia Pacific (Mumbai)
sa-east-1	South America (São Paulo)

Exemple de configuration de redondance sur CSRHA

```

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

```

Exemple de configuration de redondance sur CSRHA1

```

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

```

Vérifier la haute disponibilité

1. Vérifiez les configurations BFD et cloud.

```
CSRHA#show bfd nei
```

```
IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
192.168.1.2 4097/4097 Up Up Tu1
```

```
CSRHA#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.2 Tu1 12 00:11:57 1 1470 0 2
```

```
CSRHA#show redundancy cloud provider aws 1
```

```
Cloud HA: work_in_progress=FALSE
Provider : AWS node 1
State : idle
BFD peer      = 192.168.1.2
BFD intf      = Tunnel1
route-table   = rtb-ec081d94
cidr          = 8.8.8.8/32
eni           = eni-90b500a8
region        = us-west-2
```

2. Exécutez une requête ping continue de la machine virtuelle vers la destination. Assurez-vous que la requête ping passe par l'interface privée eth1.

```
ubuntu@ip-10-16-3-139:~$ ping -I eth1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 10.16.6.131 eth1: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=50 time=1.60 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=50 time=1.62 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=50 time=1.57 ms
```

3. Vérifiez la table de routage privé. L'interface eni est actuellement l'interface privée de CSRHA où il s'agit du trafic.

rtb-ec081d94 | HA PRIVATE

Summary	Routes	Subnet Associations	Route Propagation	Tags
Edit				
View: <input type="text" value="All rules"/>				
Destination	Target	Status	Propagated	
10.16.0.0/16	local	Active	No	
8.8.8.8/32	eni-90b500a8 / i-0fcfceb4f929f681a	Active	No	

4. Arrêtez Tunnel1 de CSRHA pour simuler un basculement HA.

```
CSRHA(config)#int Tu1
CSRHA(config-if)#shut
```

5. Notez que la table de routage pointe vers la nouvelle interface ENI qui est l'interface privée de CSRHA1.

Destination	Target	Status	Propagated
10.16.0.0/16	local	Active	No
8.8.8.8/32	eni-10e3a018 / i-0fcfceb4f929f681a	Active	No

Dépannage

- 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 de ces éléments 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, associées au rôle IAM et aux groupes de sécurité.
- Désactivez le contrôle de la source/destination par ENI.
- Pour Cisco IOS XE 16.3.1a ou version ultérieure, il s'agit des commandes de vérification supplémentaires disponibles.

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

- Voici les échecs courants observés dans les débogages :

Problème : httpc_send_request a échoué

Résolution : Le protocole HTTP est utilisé pour envoyer l'appel d'API du CSR à AWS. Assurez-vous que DNS peut résoudre le nom DNS répertorié dans votre instance. Assurez-vous que le trafic http n'est pas bloqué.

```
*May 30 20:08:06.922: %VXE_CLOUD_HA-3-FAILED: VXE Cloud HA BFD state transitioned, AWS node 1
event httpc_send_request failed
*May 30 20:08:06.922: CLOUD-HA : AWS node 1 httpc_send_request failed (0x12)
URL=http://ec2.us-east-2b.amazonaws.com
```

Problème : la table de routage rtb-9c000f4 et l'interface eni-32791318 appartiennent à des réseaux différents

Résolution : Le nom de la région et l'ENI sont incorrectement configurés dans différents réseaux. Region et ENI doivent se trouver dans la même zone que le routeur.

```
*May 30 23:38:09.141: CLOUD-HA : res content iov_len=284 iov_base=<?xml version="1.0"
encoding="UTF-8"?>
<Response><Errors><Error><Code>InvalidParameterValue</Code><Message>route table rtb-9c0000f4 and
interface eni-32791318 belong to different
networks</Message></Error></Errors><RequestID>af3f228c-d5d8-4b23-b22c-
f6ad999e70bd</RequestID></Response>
```

Problème : Vous n'êtes pas autorisé à effectuer cette opération. Message d'échec d'autorisation codé.

Résolution : Rôle/stratégie JSON IAM créé de manière incorrecte ou non appliqué au CSR. Le rôle IAM autorise le CSR à effectuer des appels API.

```
*May 30 22:22:46.437: CLOUD-HA : res content iov_len=895 iov_base=<?xml version="1.0"
encoding="UTF-8"?>
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not authorized to
perform this operation. Encoded
authorization failure message: qYvEB4MUdOB8m2itSteRgnOuslAaxhAbDph5qGRJkjjJbrESajbmF5HWUR-
MmHYeRALpKZ3Jg_y-
_tMlYe15l_ws8Jd9q2W8YDXB13uXQqfW_cjJrgy9jhnGY0nOaNu65aLpfqui8kS_4RPOpm5grRFFfo99-
8uv_N3mYaBqKFPn3vUcSYKBmxFIikJKc jY9esOeLIOWDcnYGGu6AGGMoMxWdtk0K8nwk4IjLdCnd2cDXeENS45w1PqzKGPsh
v3wD28TS5xRjIrPXyrT18UpV61LA_090h4737VncQKfzbz4tPpnAkoW0mJLQ1vDpPmNvHUPeng8KrGWYNfbfemoDtWqIdABf
aLLLmh4saNtnQ_OMBoTi4toBLEb2BNdMkl1UVBIxqTqdFUVRS**MSG 00041 TRUNCATED** **MSG 00041
CONTINUATION
#01**qLosAb5Yx0DrOsLSQwzS95VGvQM_n87LBHYbAWWhqWj3UfP_zmiak7d1m9P41mFCucEB3Cs4FRsFtb-
9q44VtyQJaS2sU2nhGe3x4uGEsl7F1pNv5vhVeYOZB3tbOfbV1_Y4trZwYPPfGLKgBShZp-WNmUKUJJsKcl-
6KGGmp7519imvh66Jgwgmu9DT_qAZ-jEjKqWjBrxg6krw</Message></Error></Errors><RequestID>4cf31249-
2a6e-4414-ae8d-6fb825b0f398</RequestID></Response>
```

Informations connexes

- [Redondance de la passerelle VPC - Cisco](#)
- [Guide de déploiement des routeurs de services cloud de la gamme Cisco CSR 1000v pour les services Web Amazon](#)
- [Répartition des types d'instance](#)
- [EC2 et VPC](#)
- [Interfaces réseau élastiques, du guide de l'utilisateur d'EC2, avec le nombre d'ENI par type d'instance](#)
- [Mise en réseau améliorée sous Linux : conseils pratiques, informations de base utiles](#)
- [Explication des instances/locataires dédiés et procédures](#)
- [Documentation générale EC2](#)
- [Documentation générale VPC](#)
- [Régions et zones de disponibilité](#)
- [CSR1000v Haute disponibilité version 3](#)

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.