# Déployer la configuration de haute disponibilité C8000v sur AWS

## Table des matières

# 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® XEDenali 17.15.3a)
- 1x - VM (Linux/Windows)

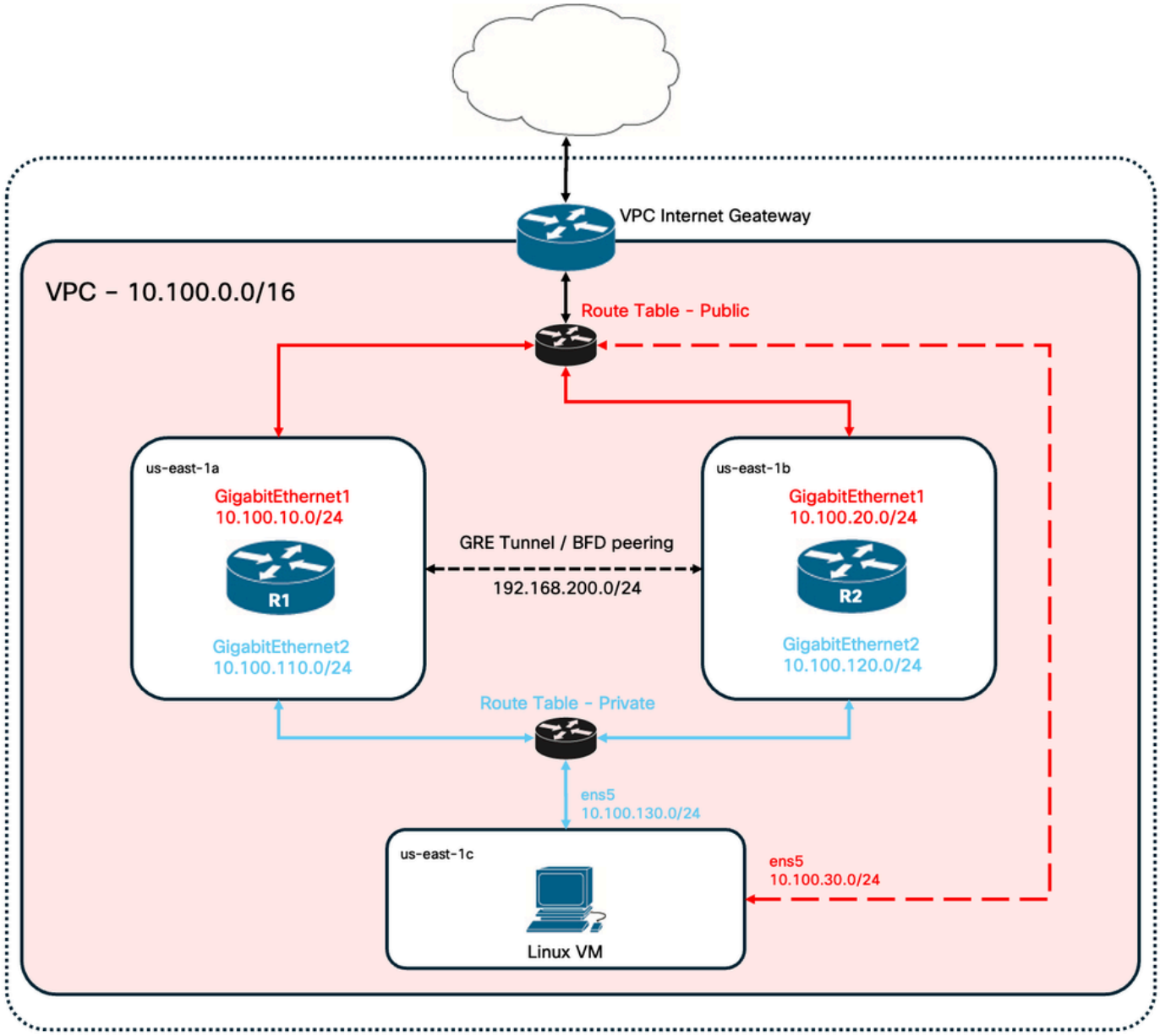
Une paire haute disponibilité comprend 2 routeurs C8000v, dans deux zones de disponibilité différentes. Considérez chaque zone de disponibilité comme un data center distinct pour une résilience matérielle supplémentaire.

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.

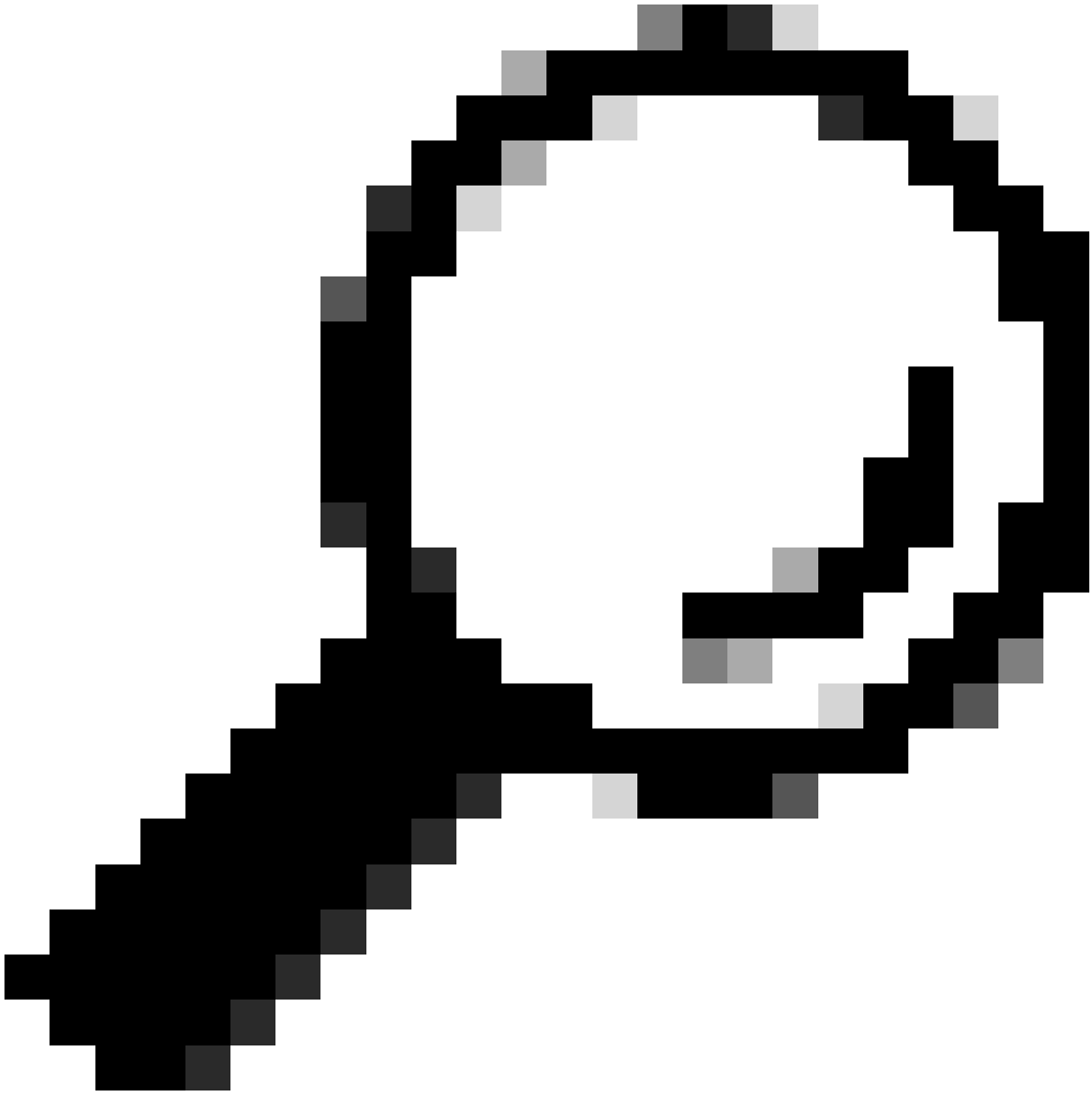
Pour simuler le trafic, lancez une requête ping à partir de l'interface privée de la machine virtuelle, en traversant la table de routage privé via R1 pour atteindre 8.8.8.8. En cas de basculement, vérifiez que la table de routage privé a été mise à jour automatiquement pour router le trafic via l'interface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

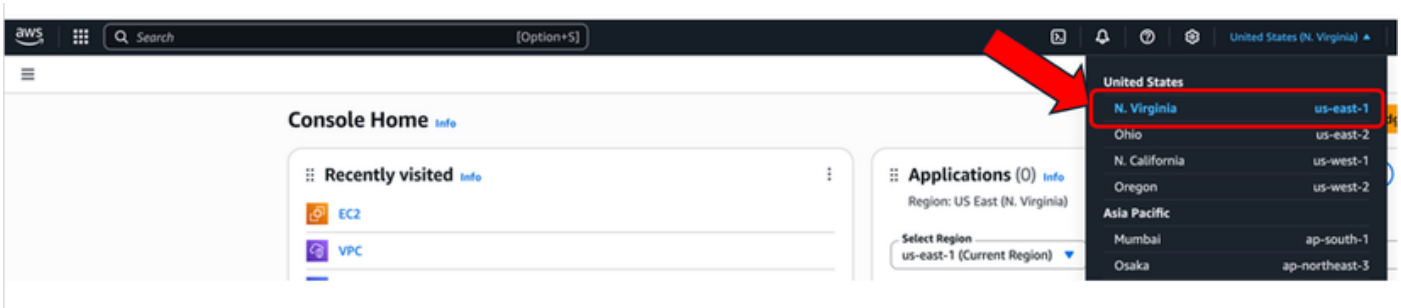
- Sur tout sous-réseau créé, n'utilisez pas la première adresse disponible de ce sous-réseau. Ces adresses IP sont utilisées par les services AWS en interne.
- Ne configurez pas les interfaces publiques des périphériques C8000v à l'intérieur d'un VRF. La haute disponibilité ne fonctionne pas correctement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

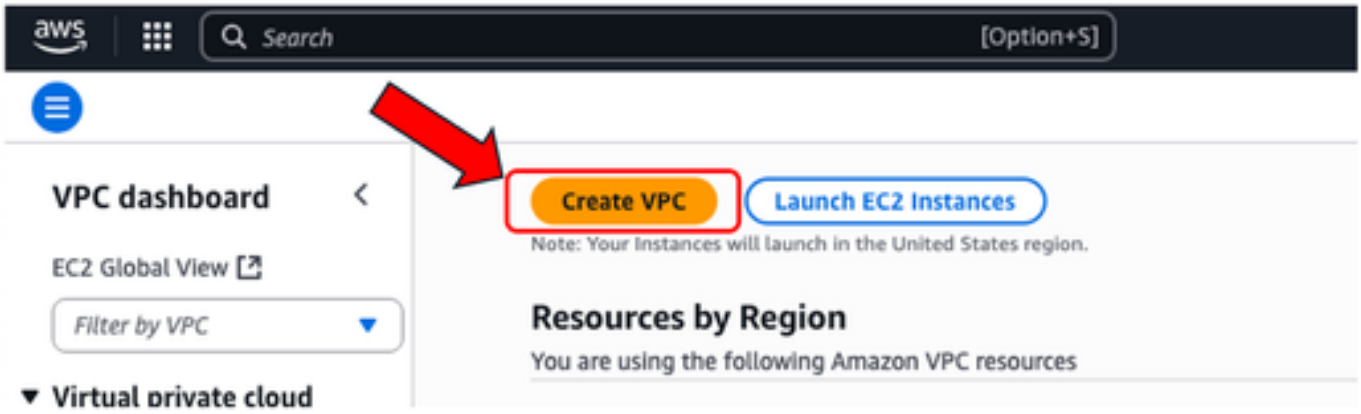
## Étape 1. Sélectionnez une région

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



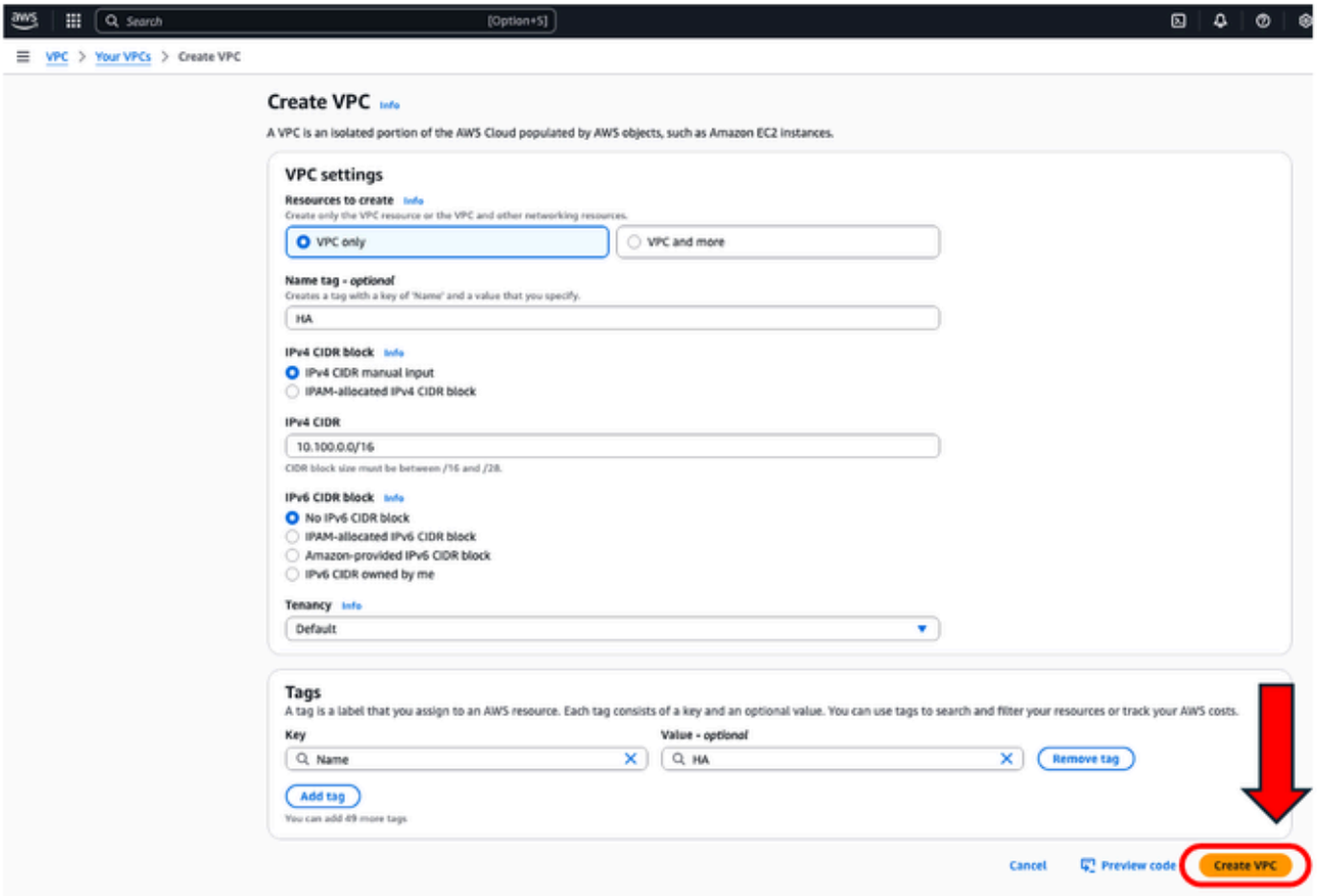

## Étape 2 : création du VPC

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

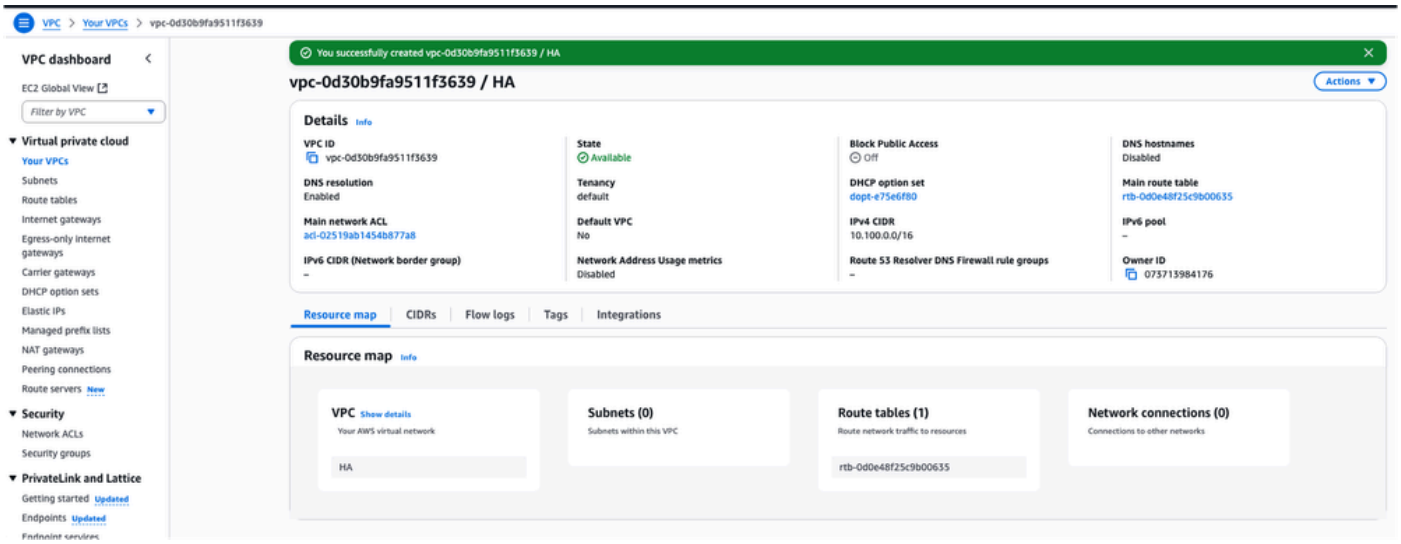



Lorsque vous créez le VPC, sélectionnez l'option VPC only. Vous pouvez affecter un réseau /16 à utiliser comme vous le souhaitez.

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

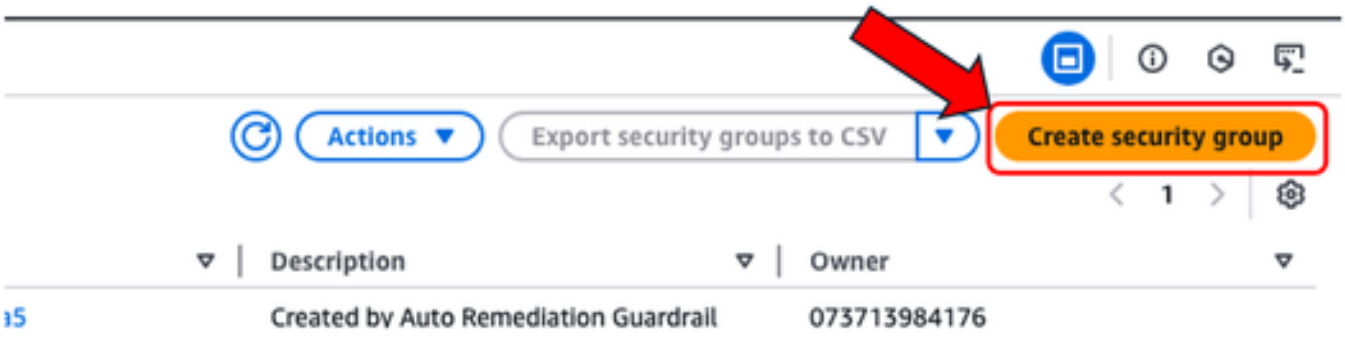



Après avoir cliqué sur Create VPC, la balise VPC-0d30b9fa9511f3639 with HA est maintenant créée :

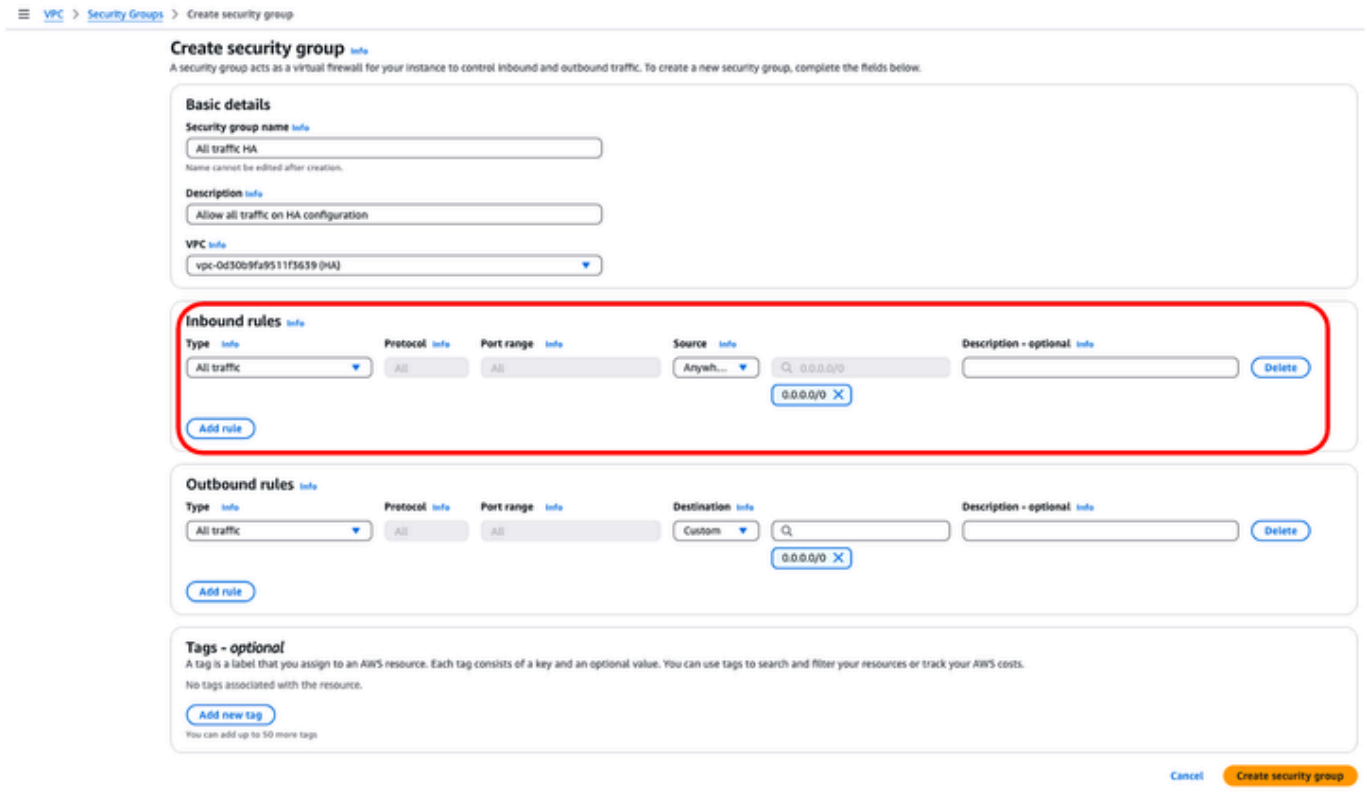



## Étape 3. Création d’un groupe de sécurité pour le VPC

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.



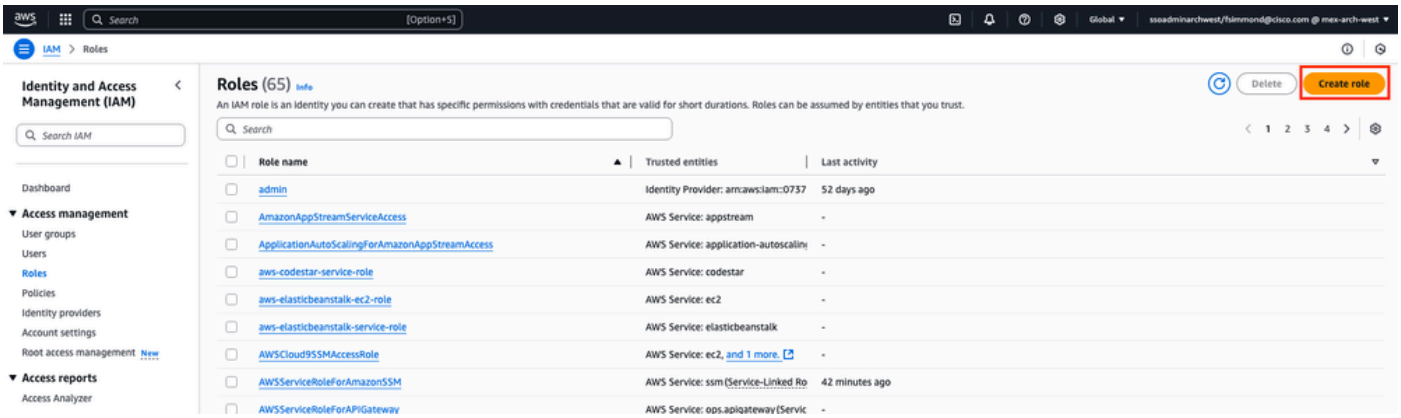

Sous Inbound Rules, définissez le trafic que vous souhaitez autoriser. Dans cet exemple, Tout le trafic est sélectionné à l'aide du réseau 0.0.0.0/0.



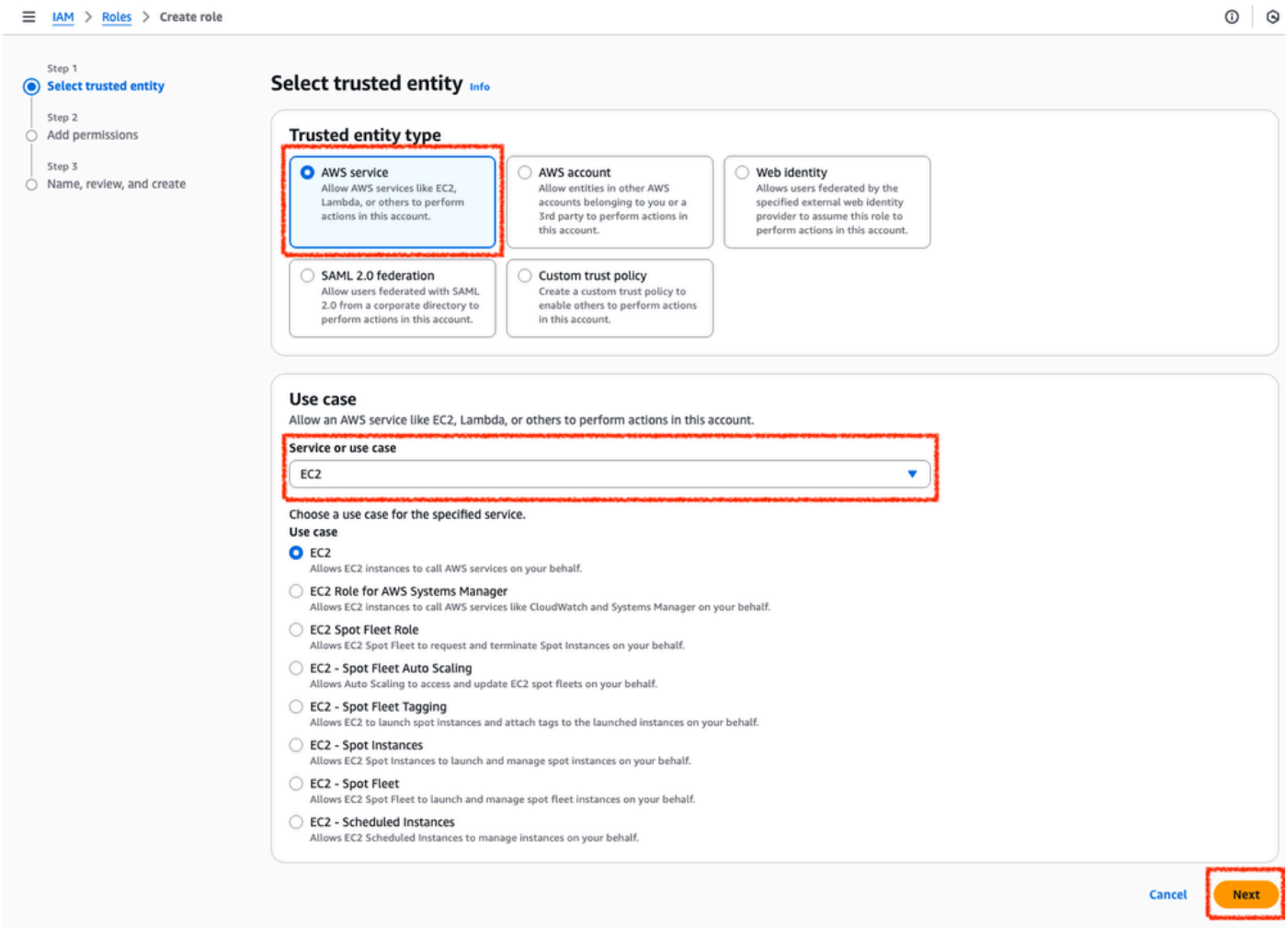

## Étape 4 : création d'un rôle IAM avec une stratégie et association au VPC

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.

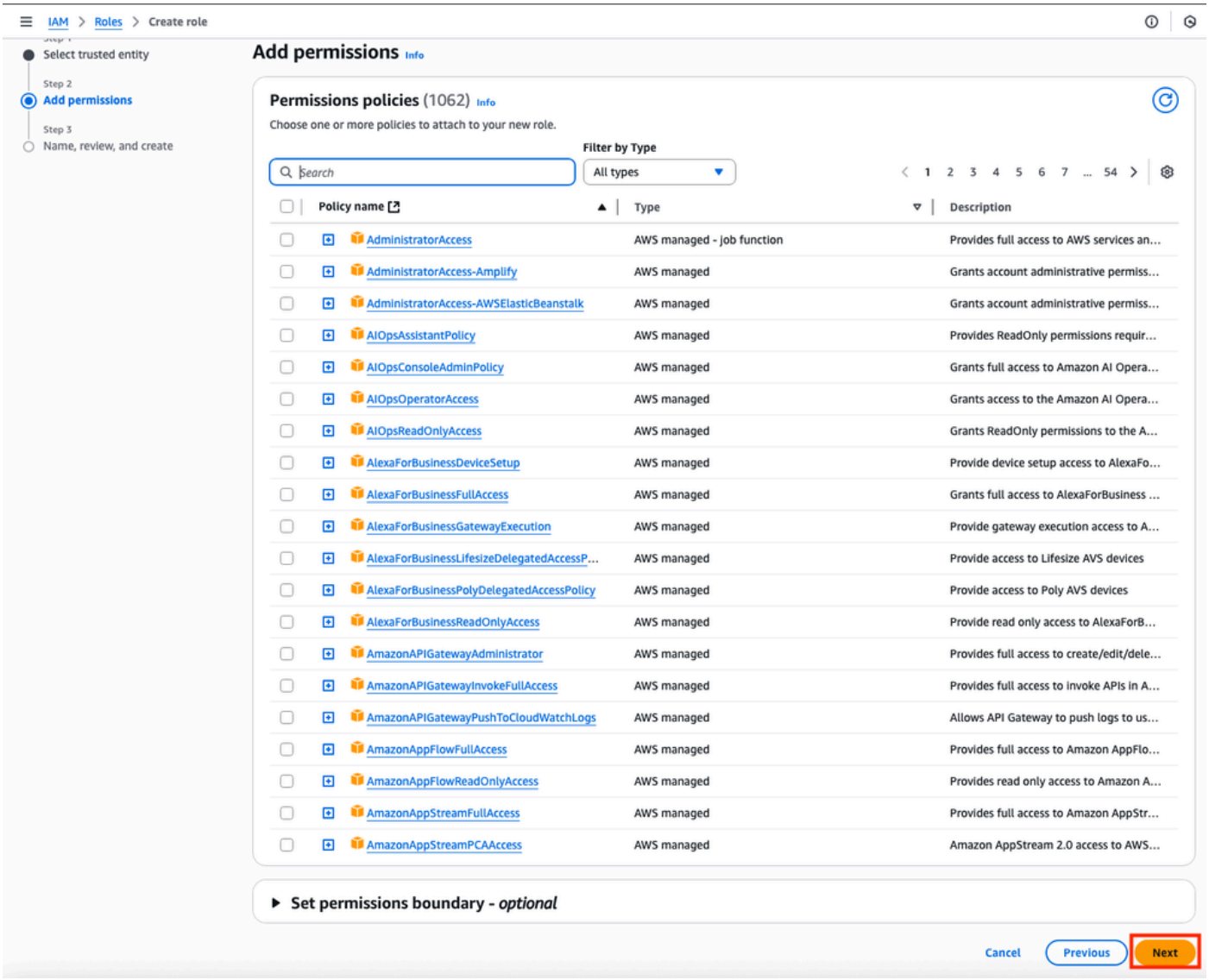
Accédez au tableau de bord IAM et accédez à Access Management > Roles > Create Role. Ce processus se compose de 3 étapes :



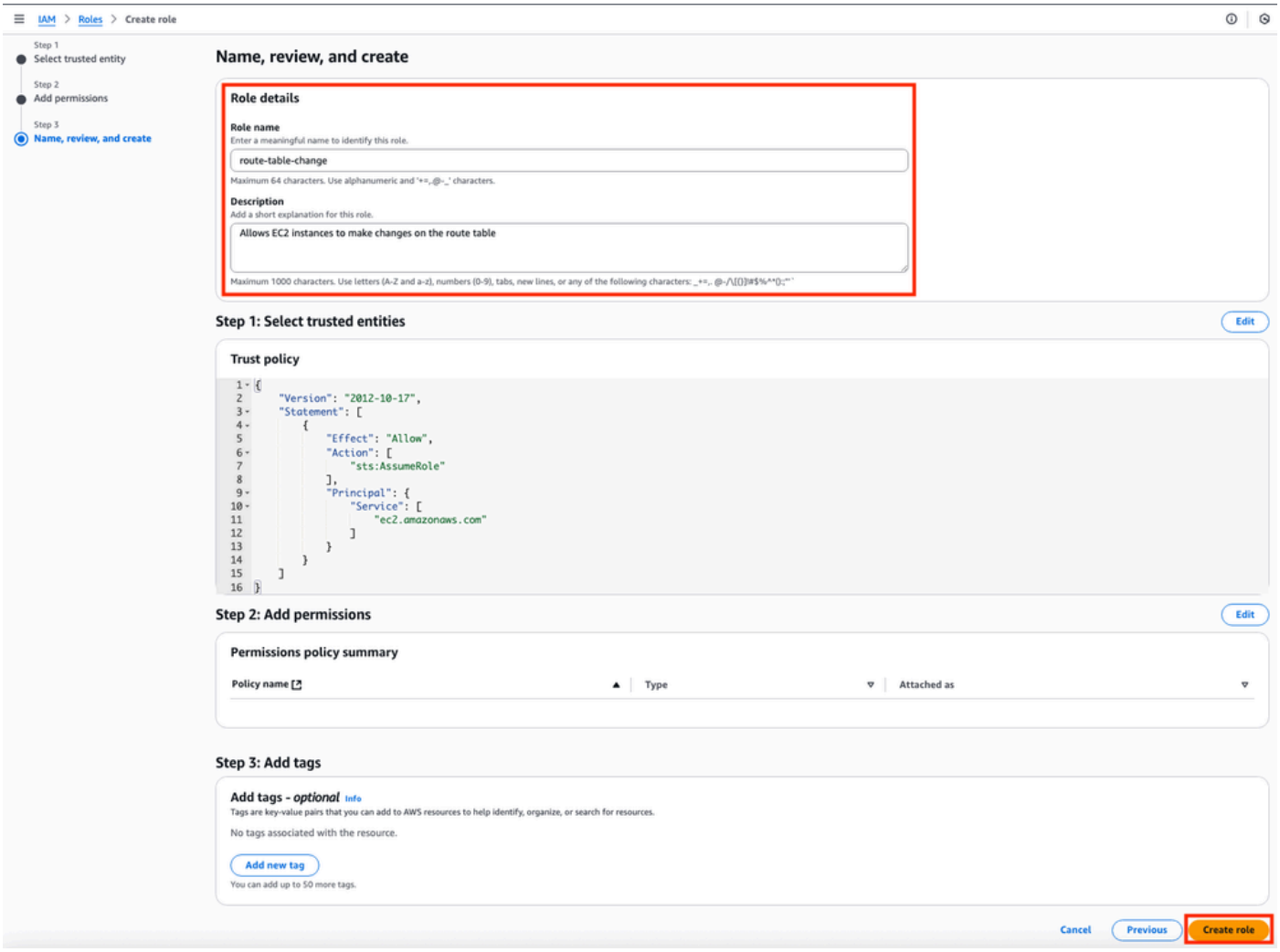

Tout d'abord, sélectionnez l'option AWS Service dans la section Trusted entity type et EC2 comme service affecté à cette stratégie.




Lorsque vous avez terminé, cliquez sur Next :

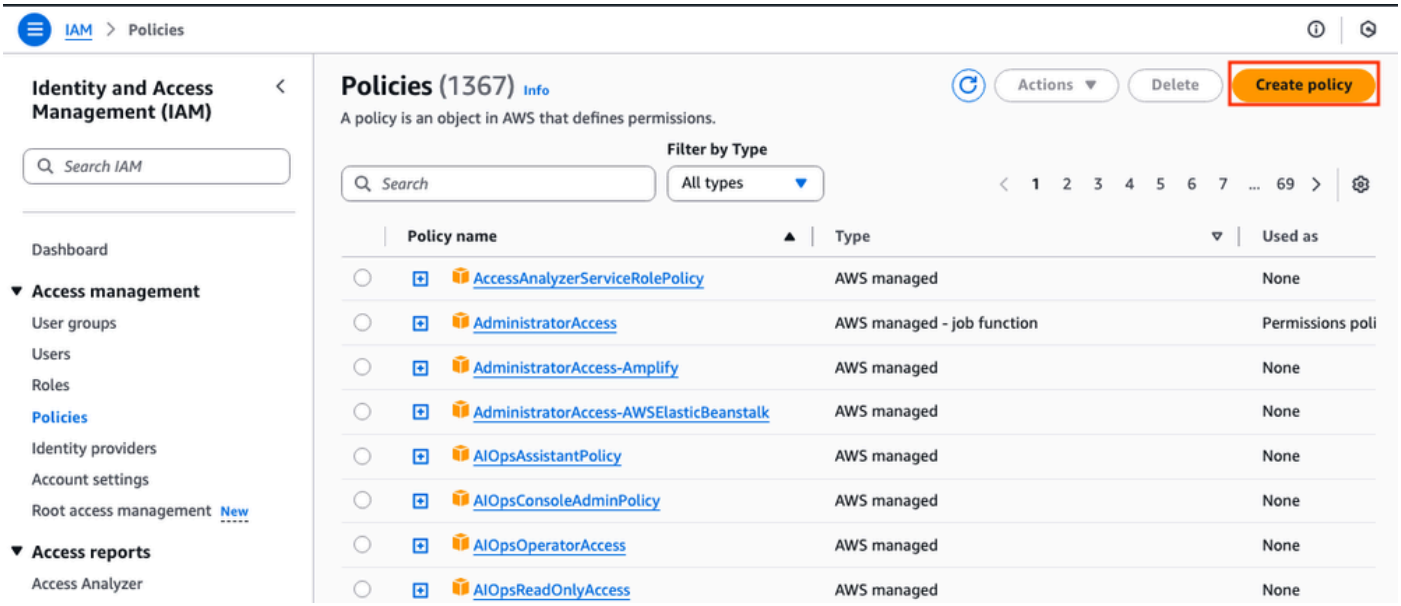



Enfin, définissez le nom du rôle et cliquez sur le bouton Créer un rôle.

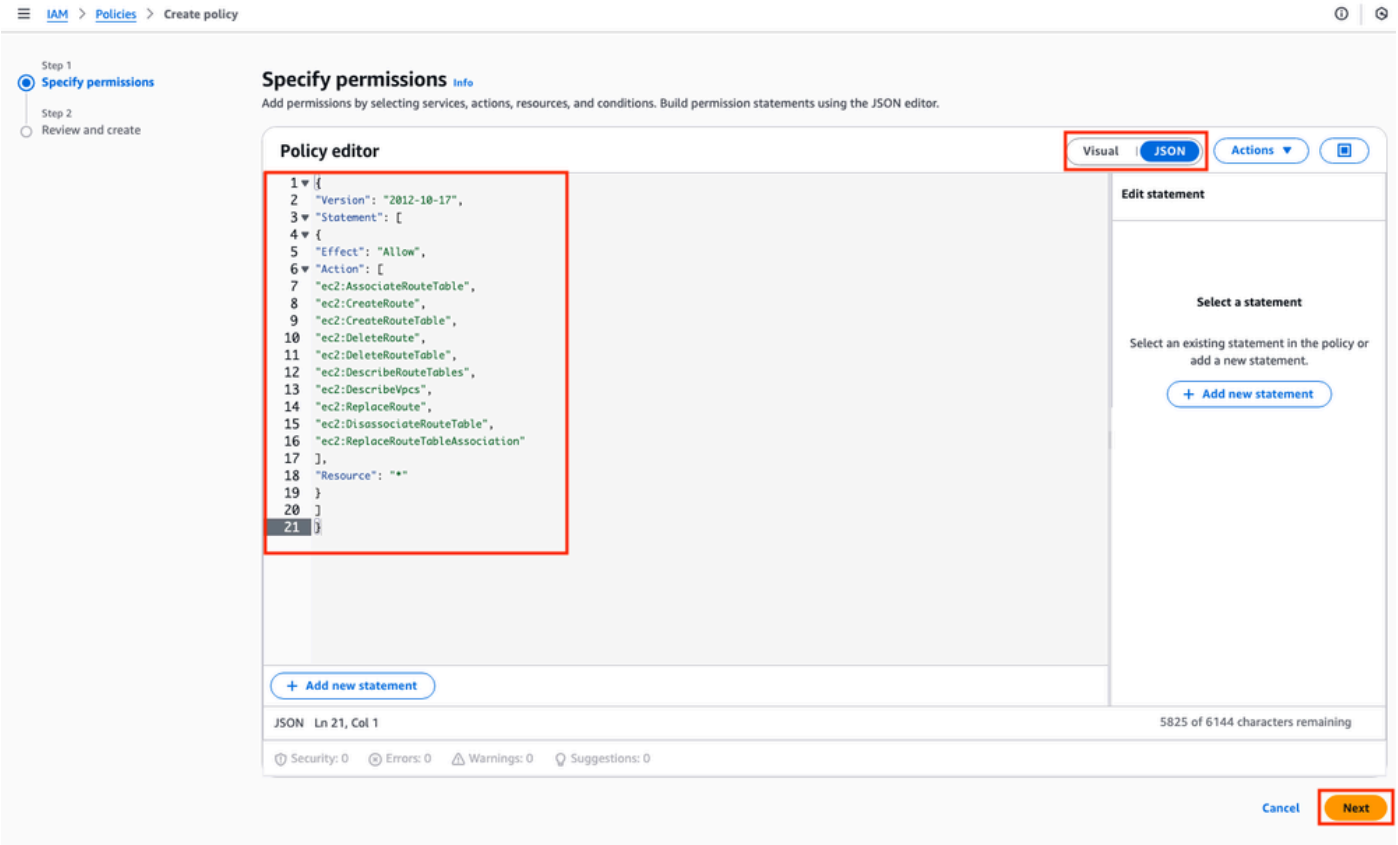



## Étape 5. Création et association d'une stratégie d'approbation à un rôle IAM

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 :



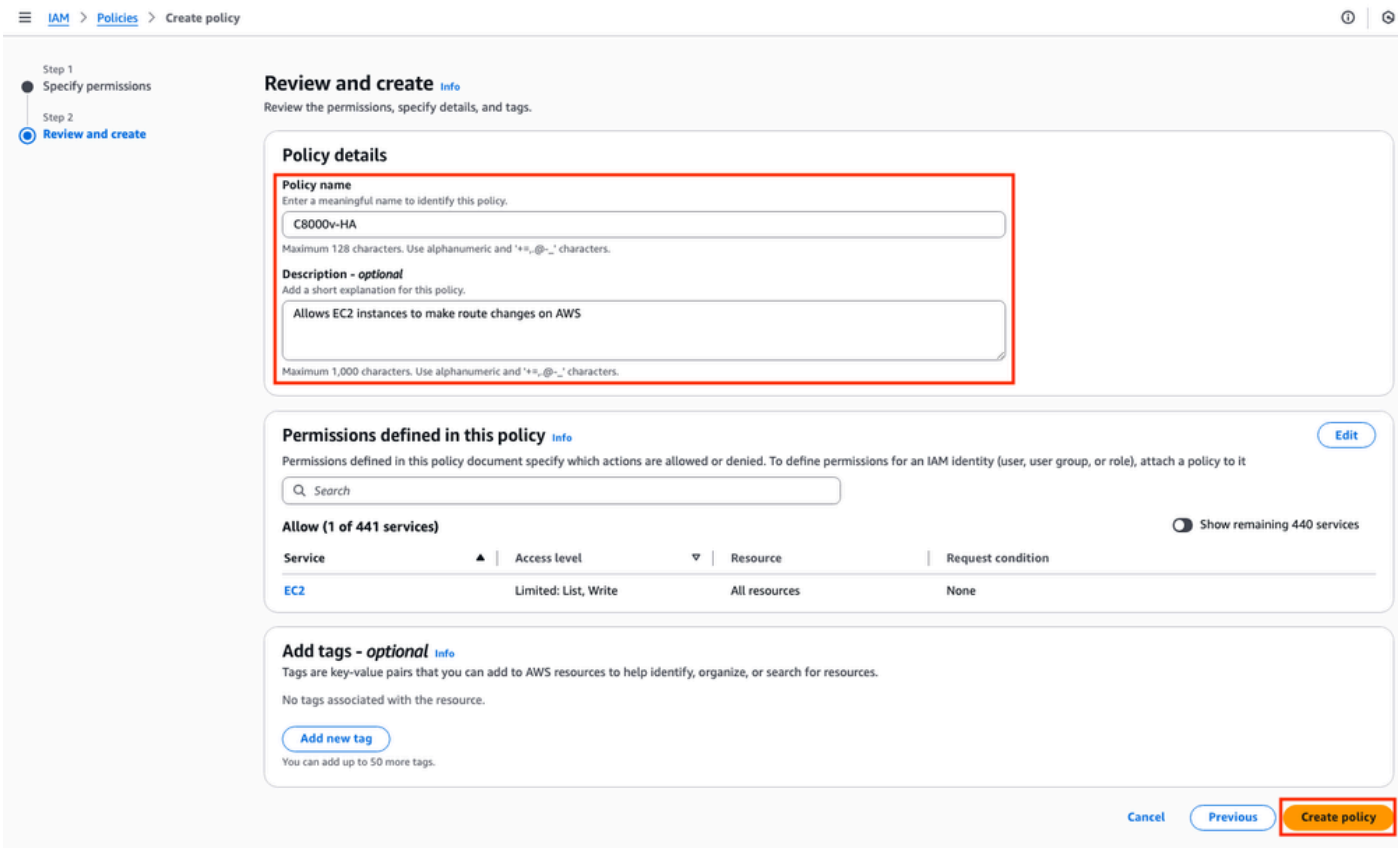
Tout d'abord, assurez-vous que l'Éditeur de stratégie utilise JSON et appliquez les commandes qui sont montrées ci-dessous. Une fois configuré, cliquez sur Next :



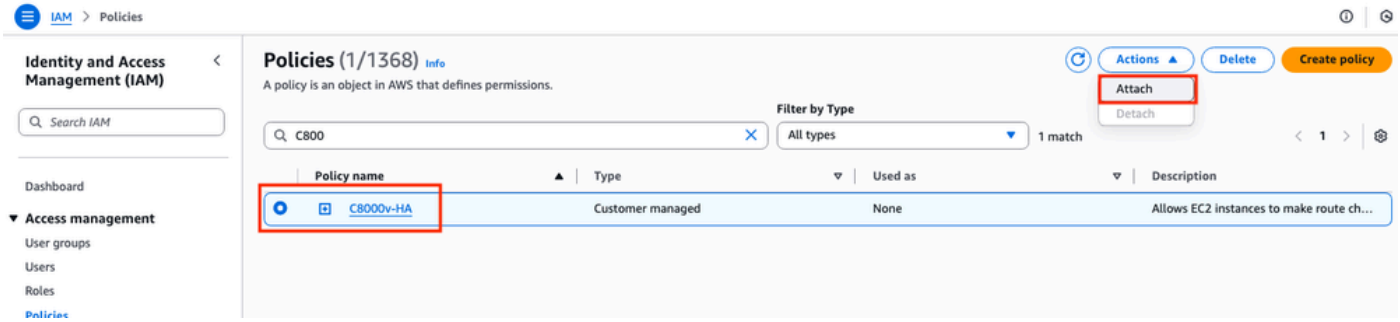

Il s'agit du code texte utilisé dans l'image :

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

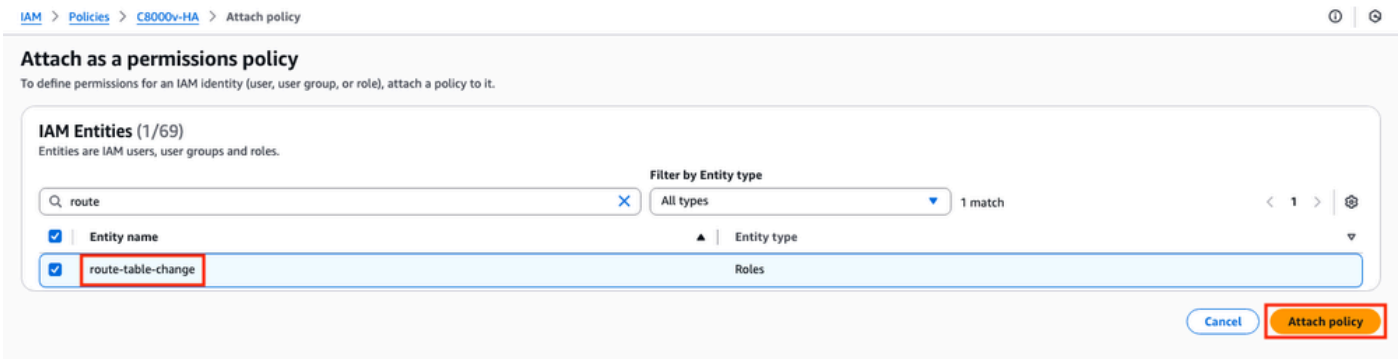
Définissez ultérieurement le nom de la stratégie et cliquez sur Créer une stratégie.




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




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

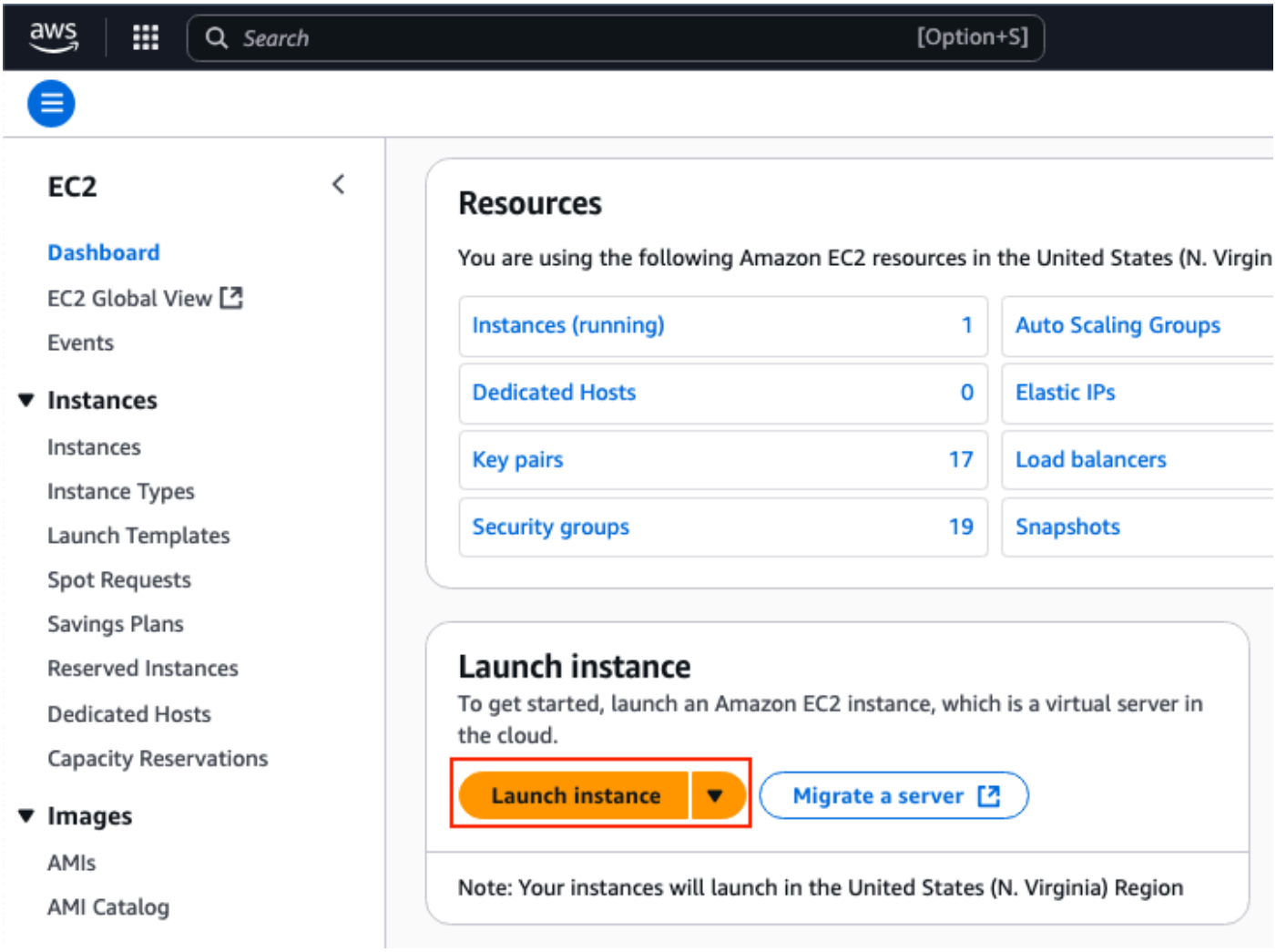



## Étape 6.Configuration et lancement des instances C8000v

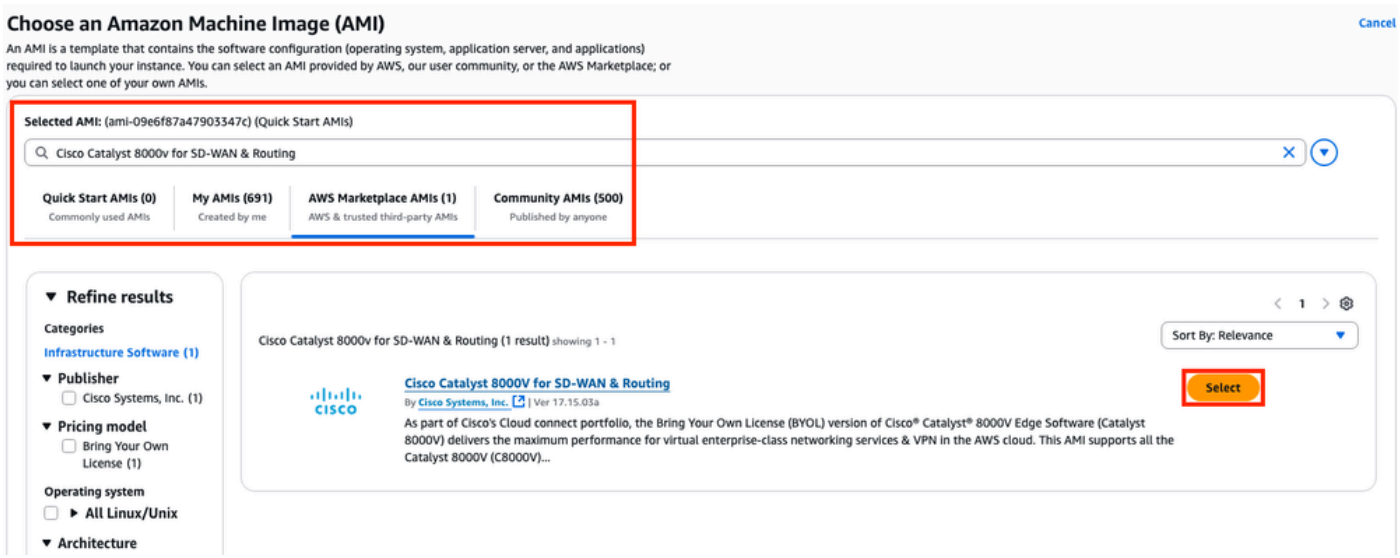
Chaque routeur C8000v aura 2 interfaces (1 publique, 1 privée) et sera créé sur sa propre zone

de disponibilité.

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

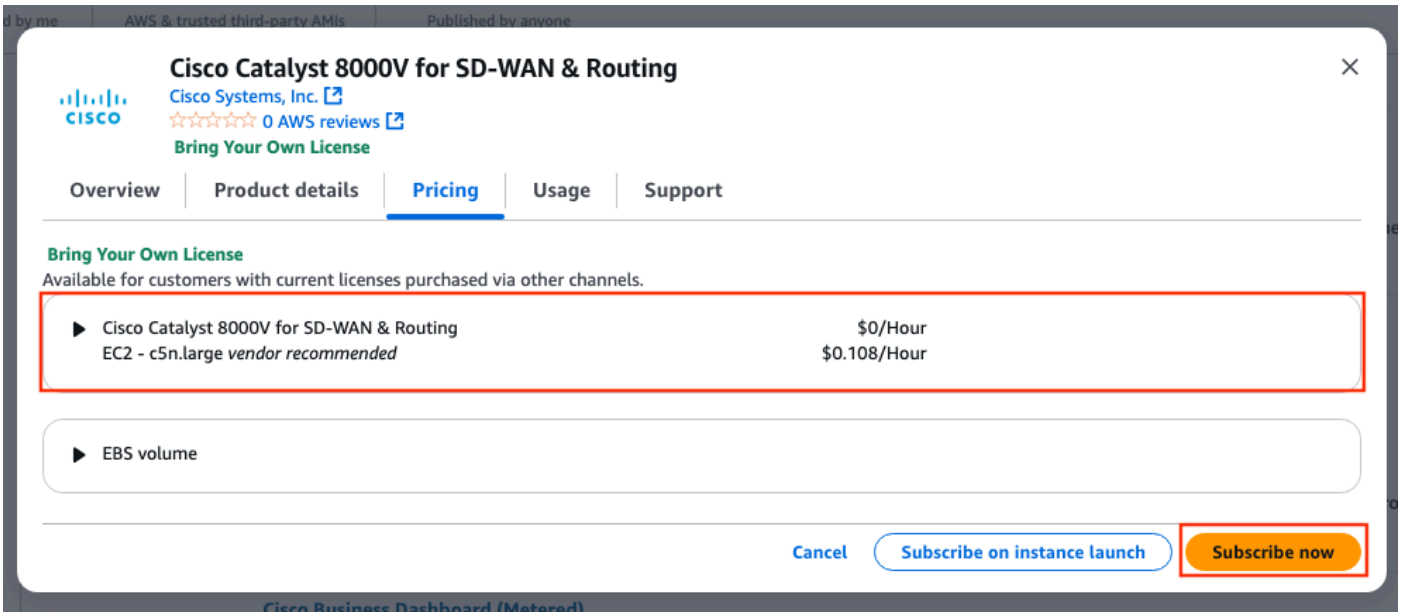



Filtrez la base de données AMI avec le nom Cisco Catalyst 8000v pour SD-WAN et routage. Dans la liste AMI AWS Marketplace, cliquez sur Sélectionner.



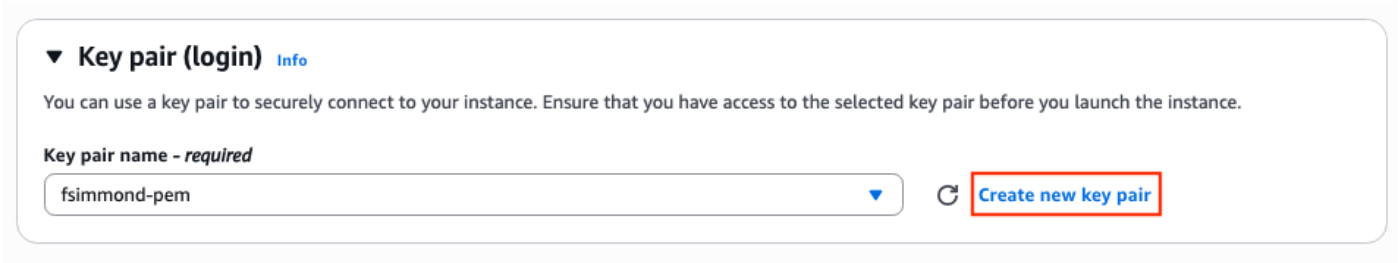

Sélectionnez la taille correspondante pour l'AMI. Pour cet exemple, la taille c5n.large est

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

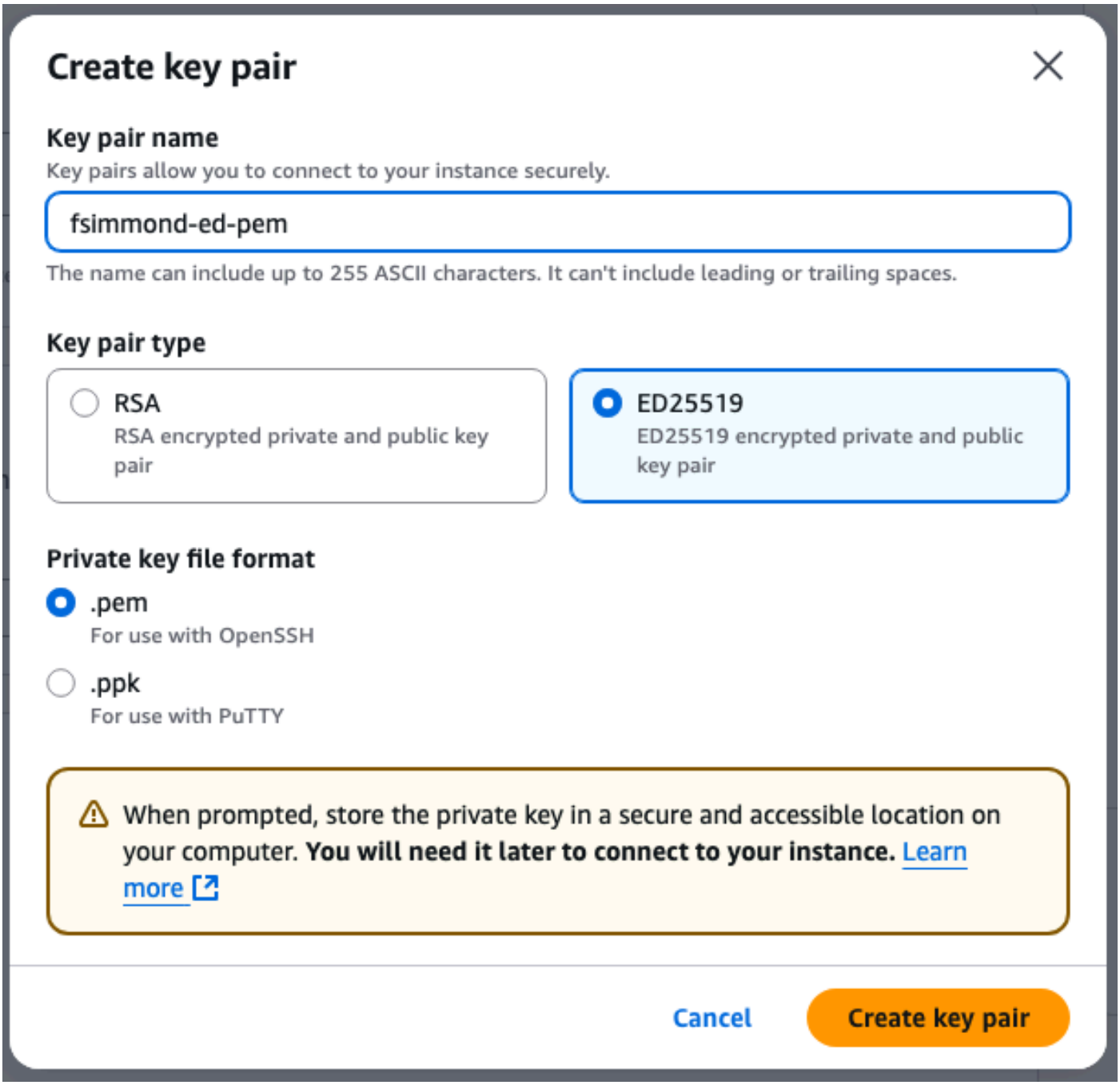



Étape 6.1. Configuration de la paire de clés pour l'accès à distance

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.




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.



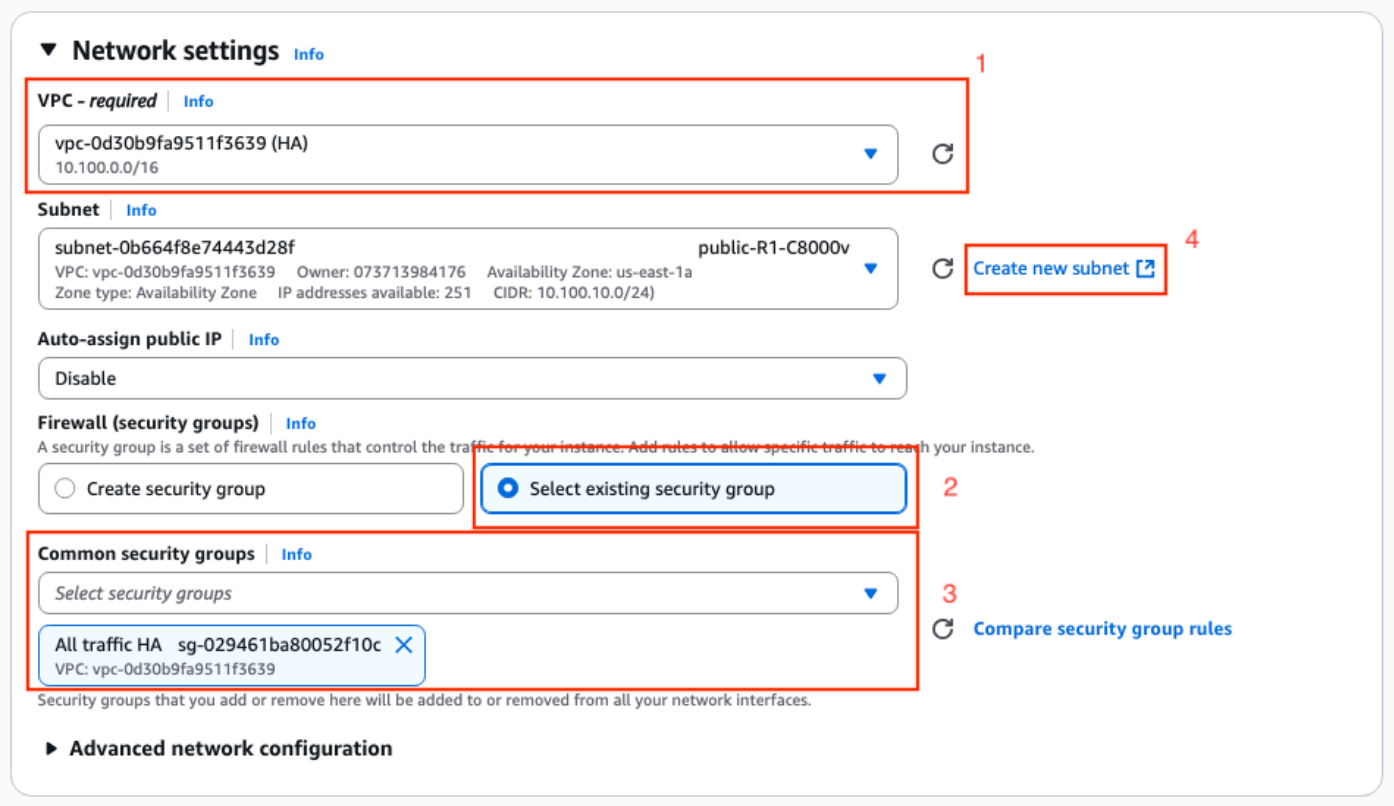

Étape 6.2. Création et configuration des sous-réseaux pour l'AMI

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.




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.

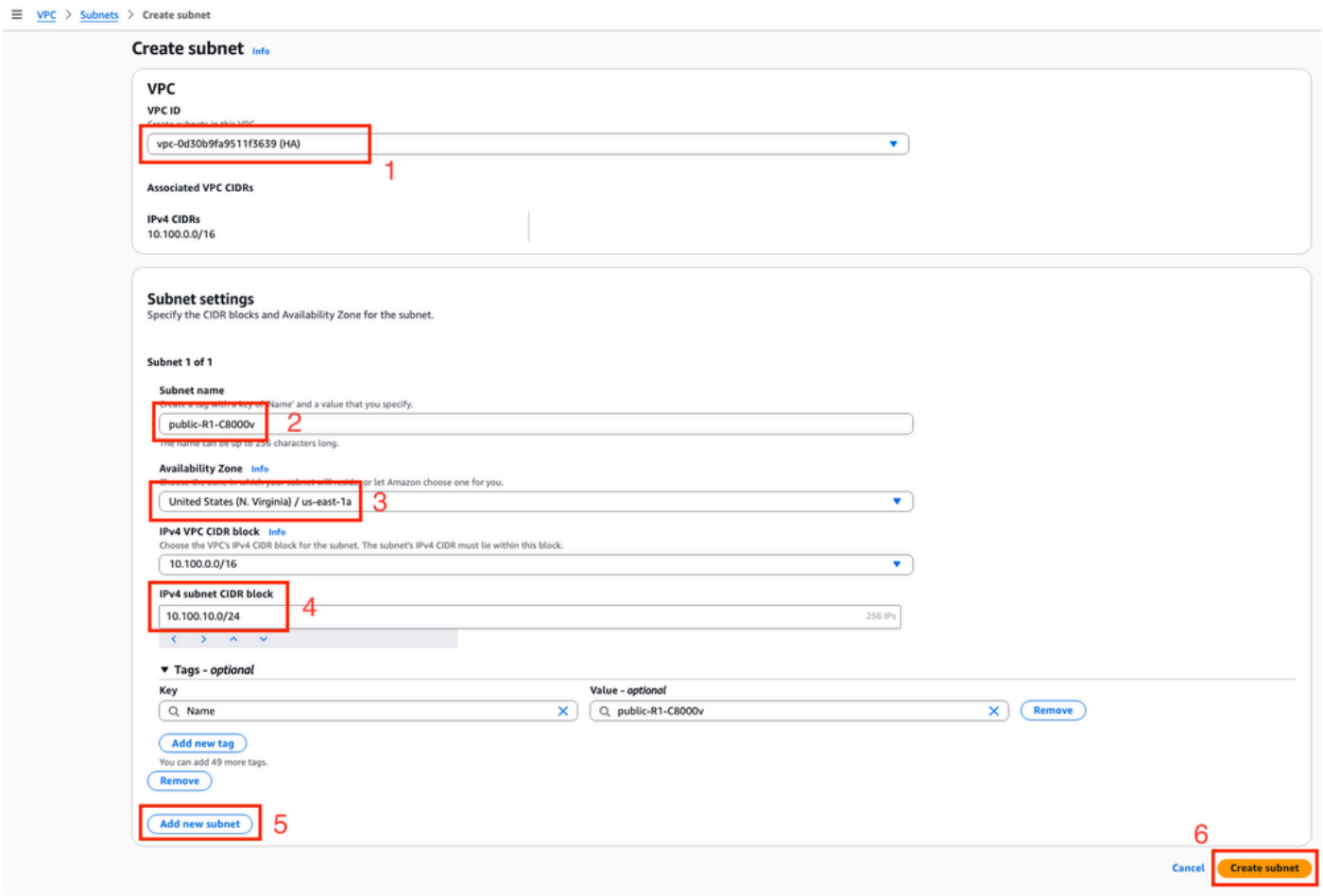
2. Attribuez un nom au nouveau sous-réseau.

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.

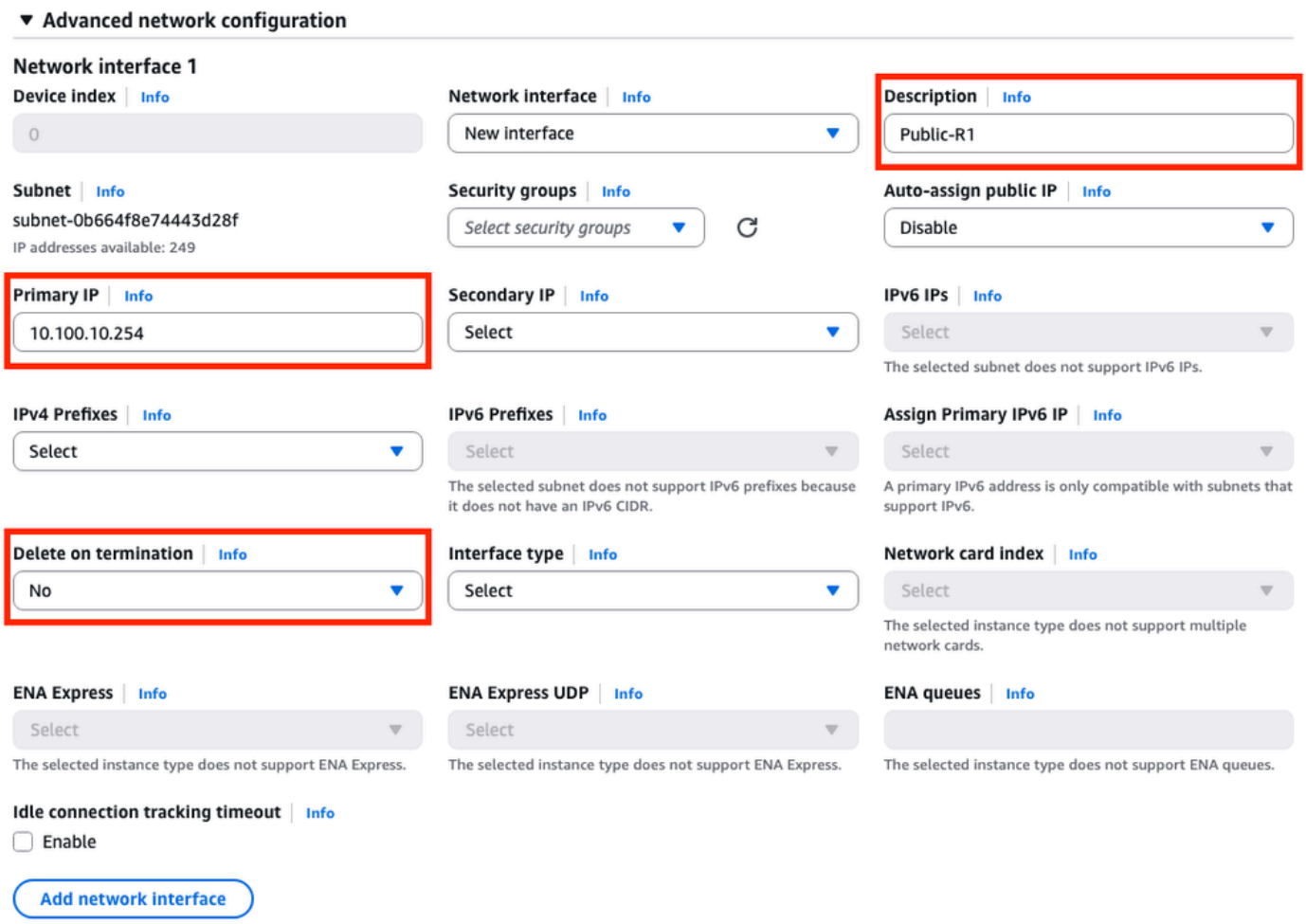
6. Une fois terminé, cliquez sur Créer un sous-réseau. Accédez à la page précédente pour continuer avec les paramètres.




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

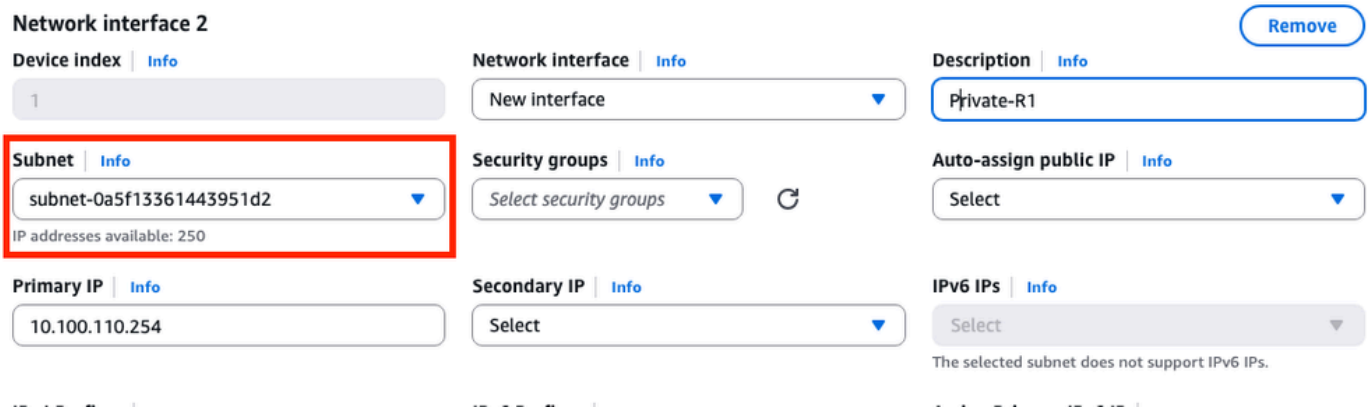
Dans la section Paramètres réseau, développez la sous-section Configuration réseau avancée. Les options suivantes s'affichent :




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.

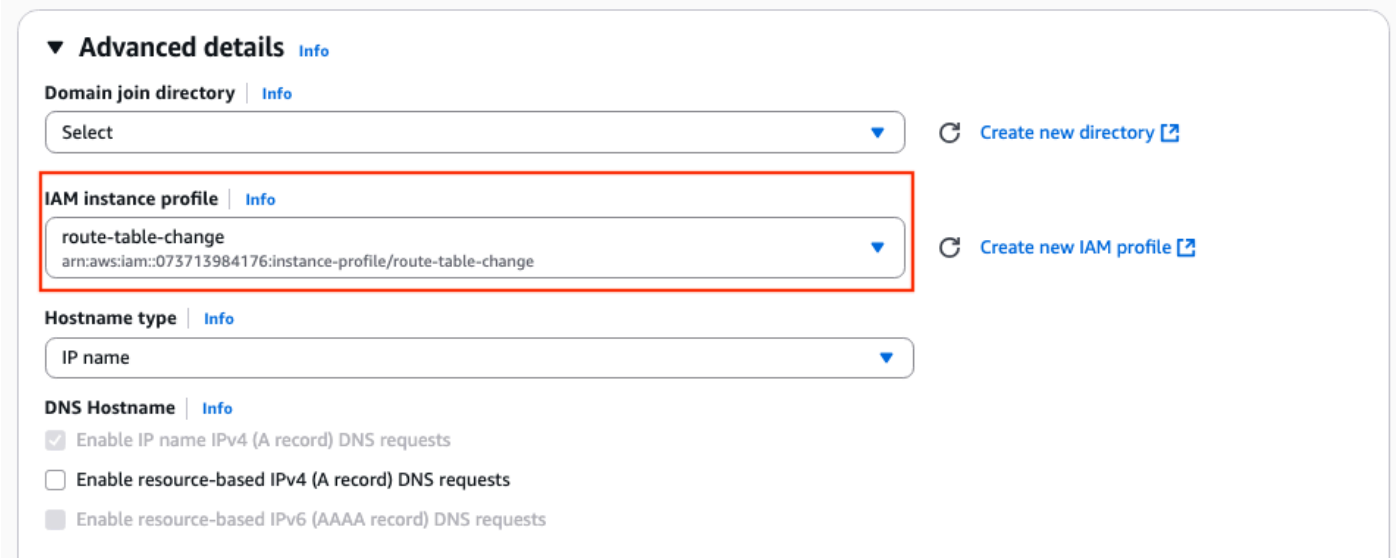
En raison de cette topologie, une seconde interface est nécessaire pour le sous-réseau privé. Cliquez sur Add network interface et cette invite s'affiche. Cependant, l'interface permet de sélectionner le sous-réseau cette fois-ci :



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

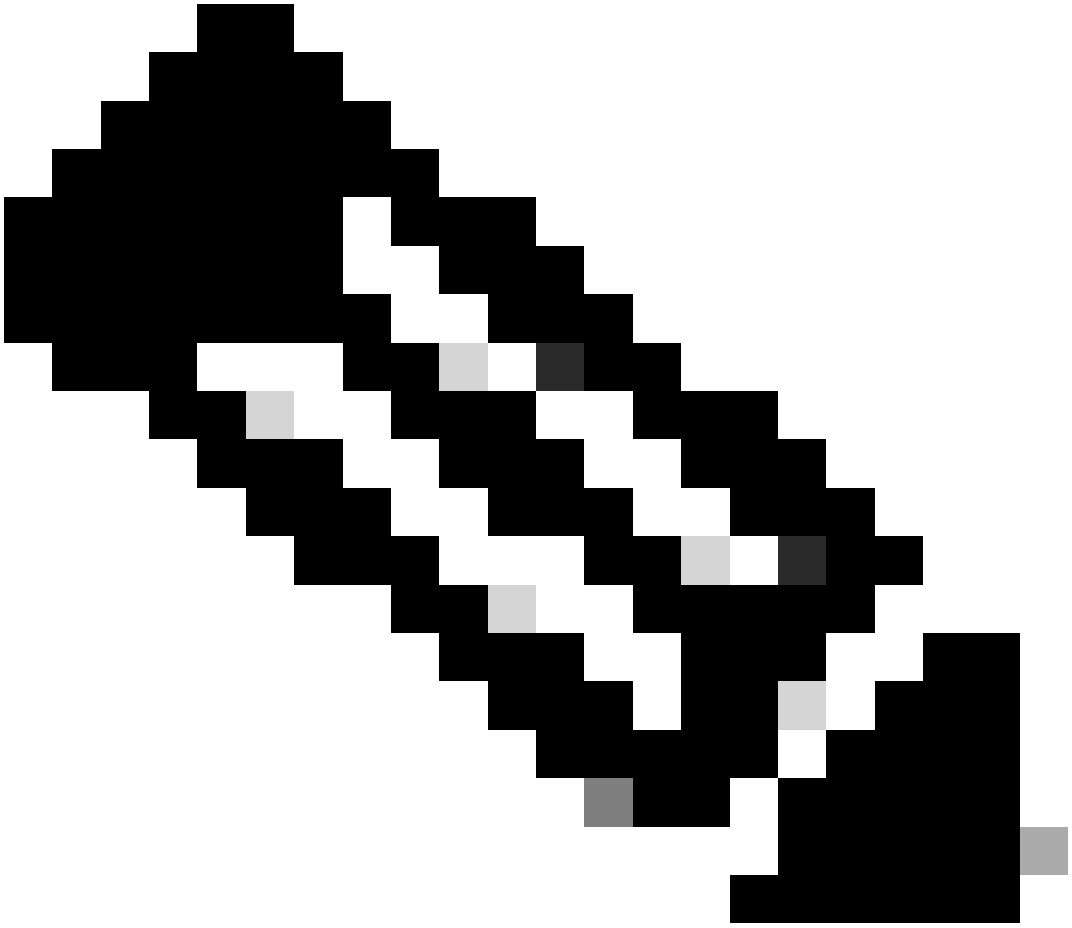
Dans la section Détails avancés, sélectionnez le rôle IAM créé sur le paramètre de profil d'instance IAM :




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

**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

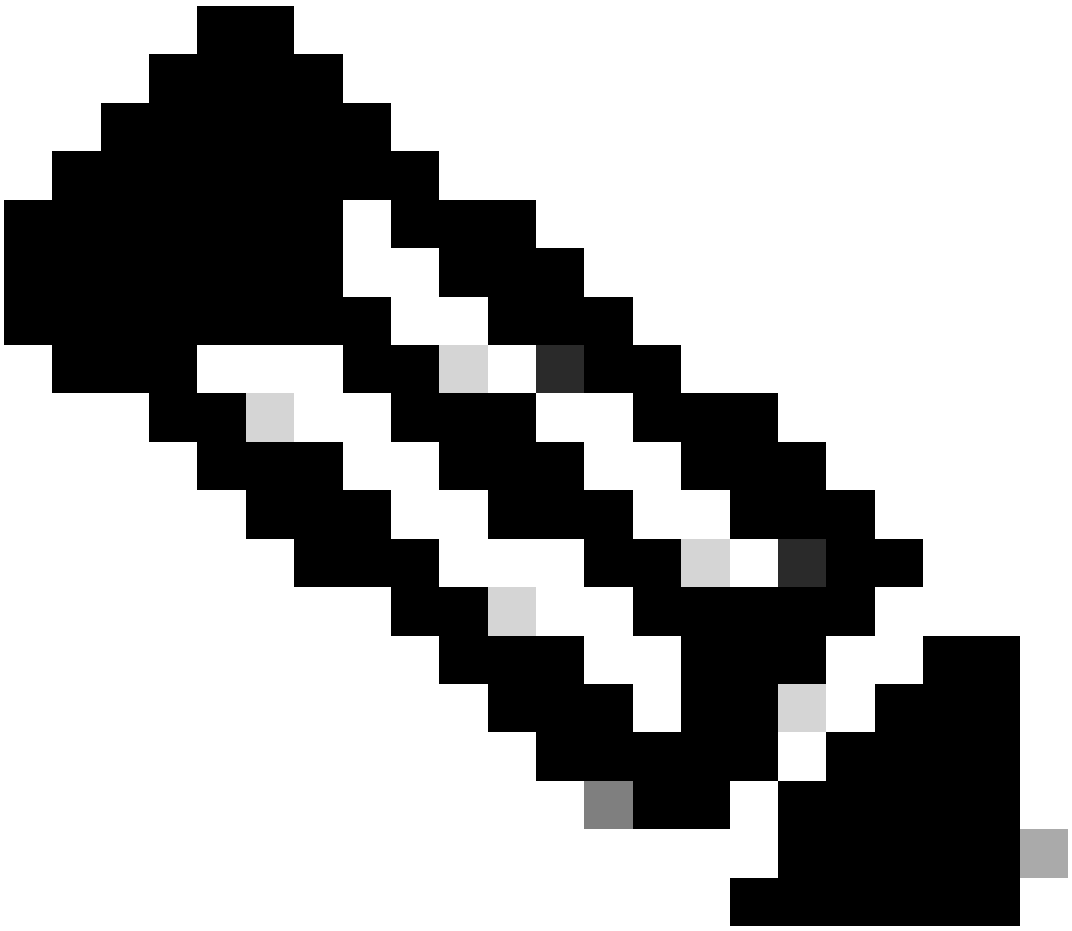
Launch instance

Preview code

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

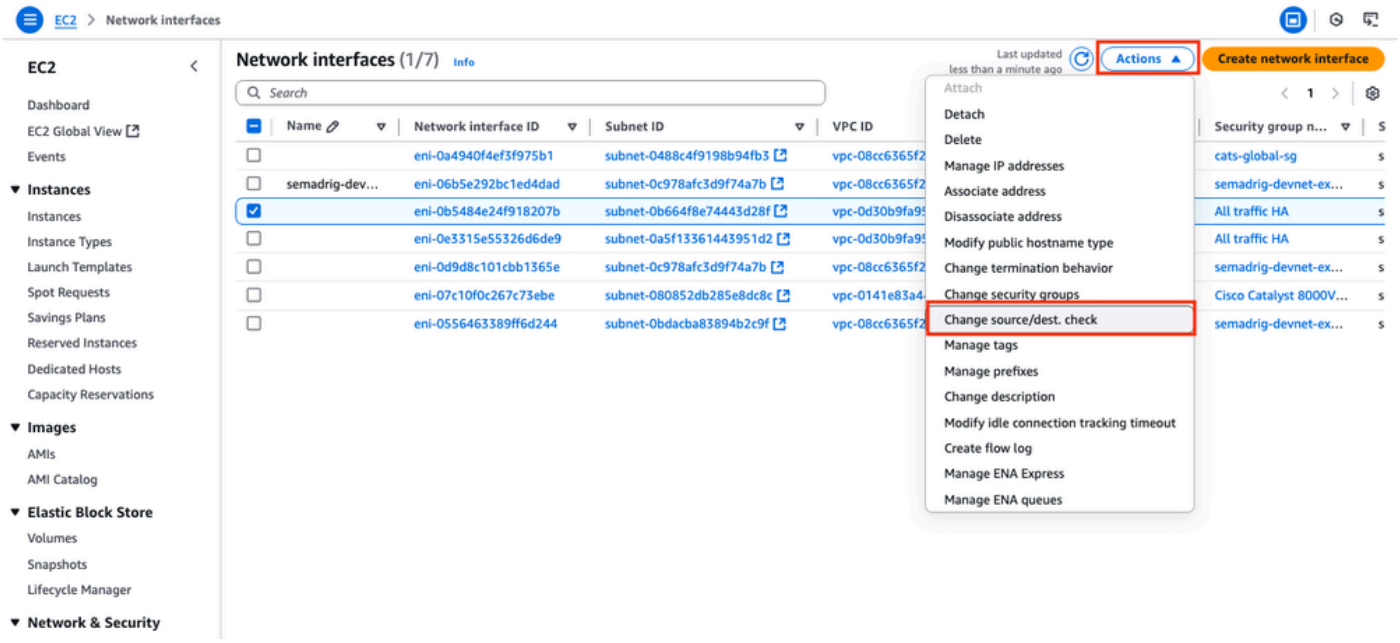
Une fois l'instance créée, désactivez la fonctionnalité de vérification src/dst sur AWS pour obtenir la connectivité entre les interfaces du même sous-réseau. Dans la section EC2 Dashboard > Network & Security > Network interfaces, sélectionnez les ENI et cliquez sur Actions > Modifier la source/dest.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

---

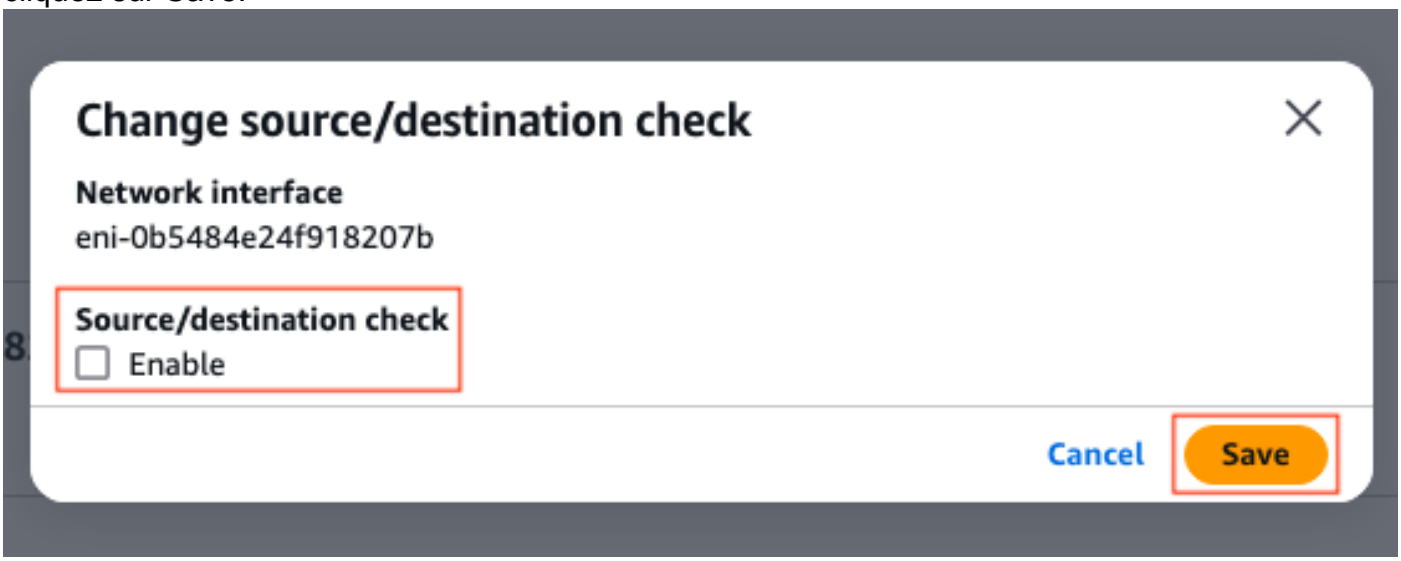


Remarque : Vous devez sélectionner les ENI un par un pour que cette option soit disponible.

---

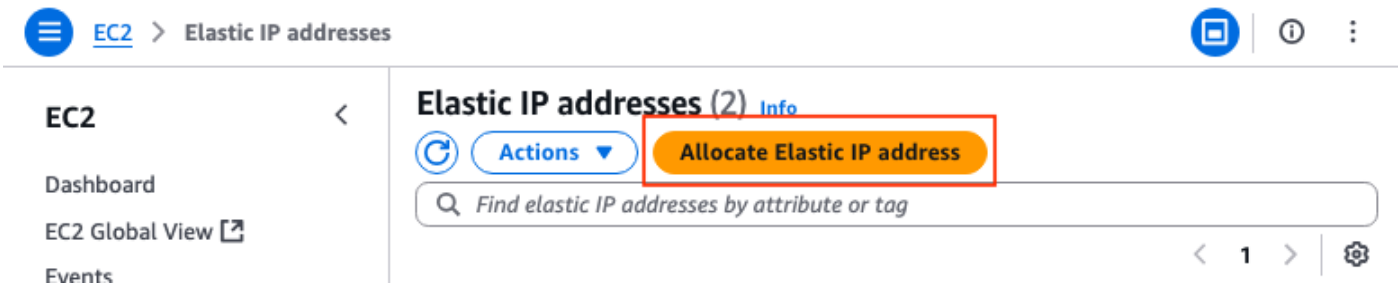



Une nouvelle fenêtre s'affiche. Dans le nouveau menu, désactivez la case à cocher Enable et cliquez sur Save.



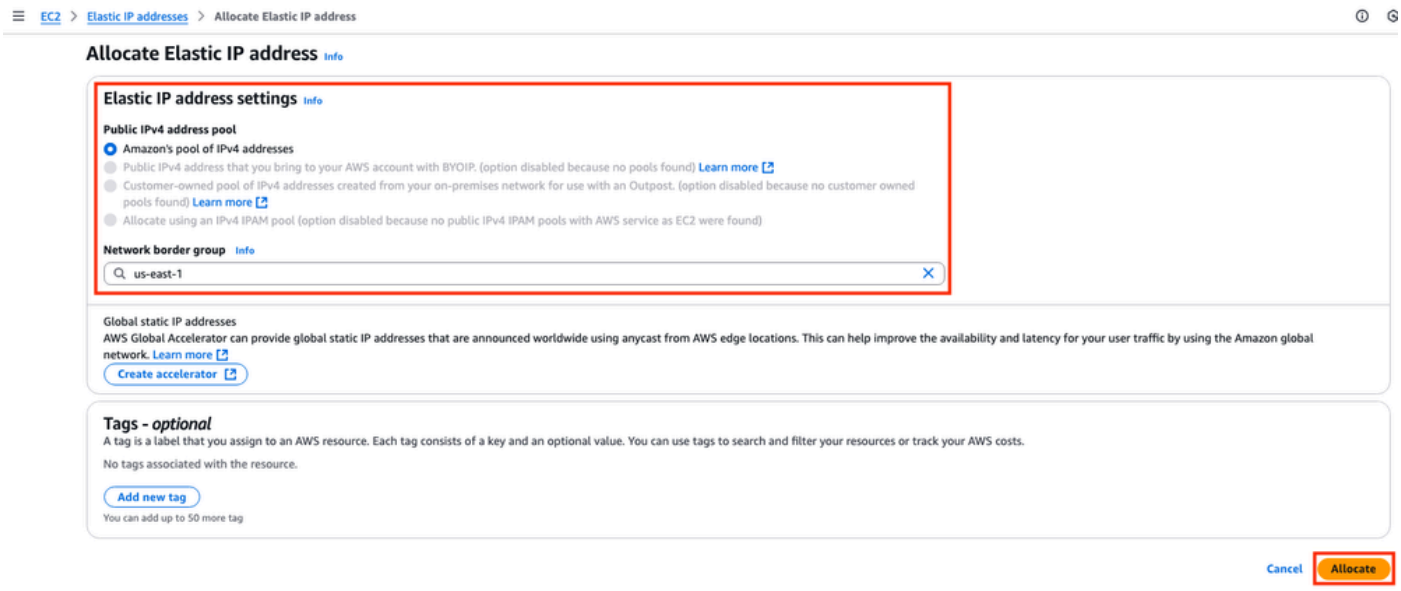

Étape 6.8. Création et association d’une adresse IP élastique à l’interface ENI publique de l’instance

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

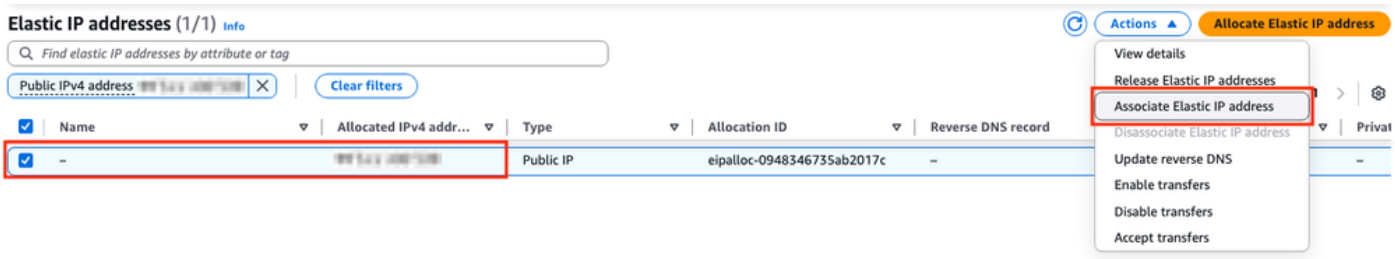



La page vous mène à l'autre section. Dans cet exemple, l'option Pool d'adresses IPv4 d'Amazon

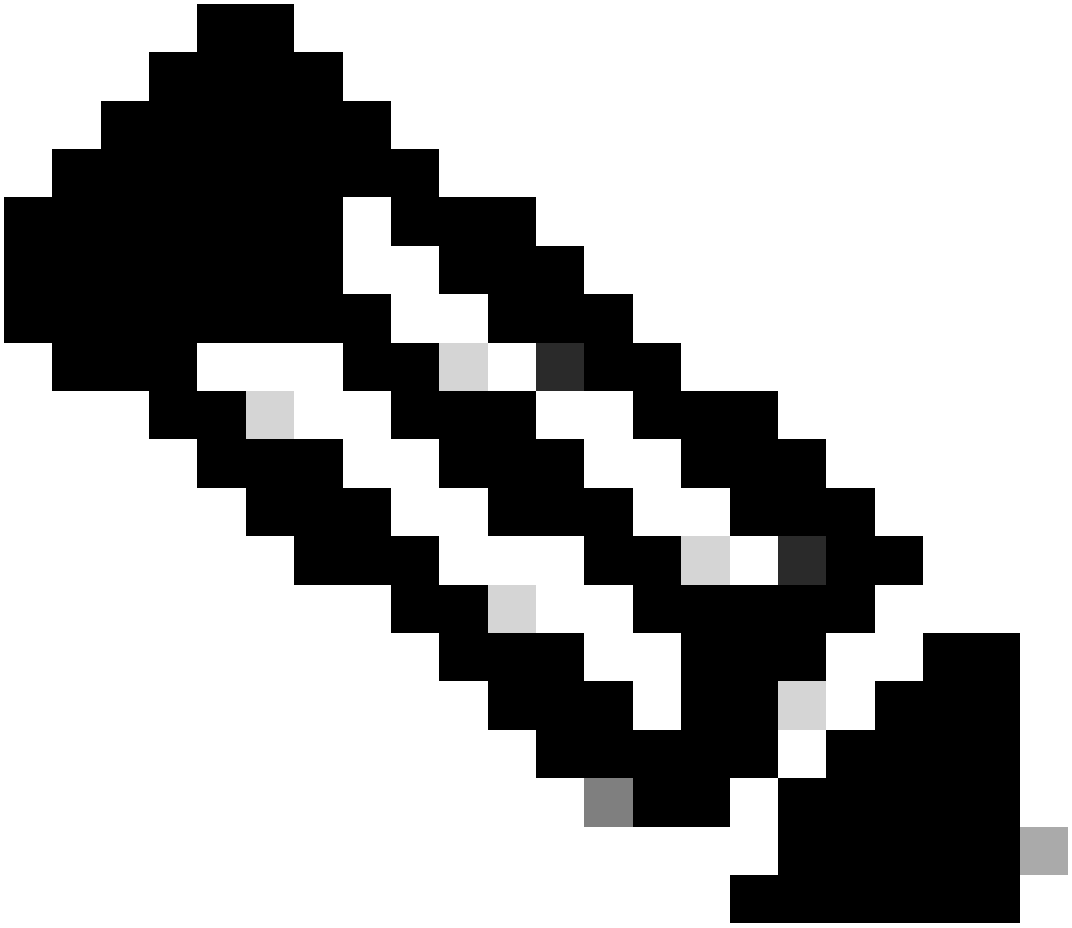
est sélectionnée avec la zone de disponibilité us-east-1. Une fois terminé, cliquez sur Allocate.



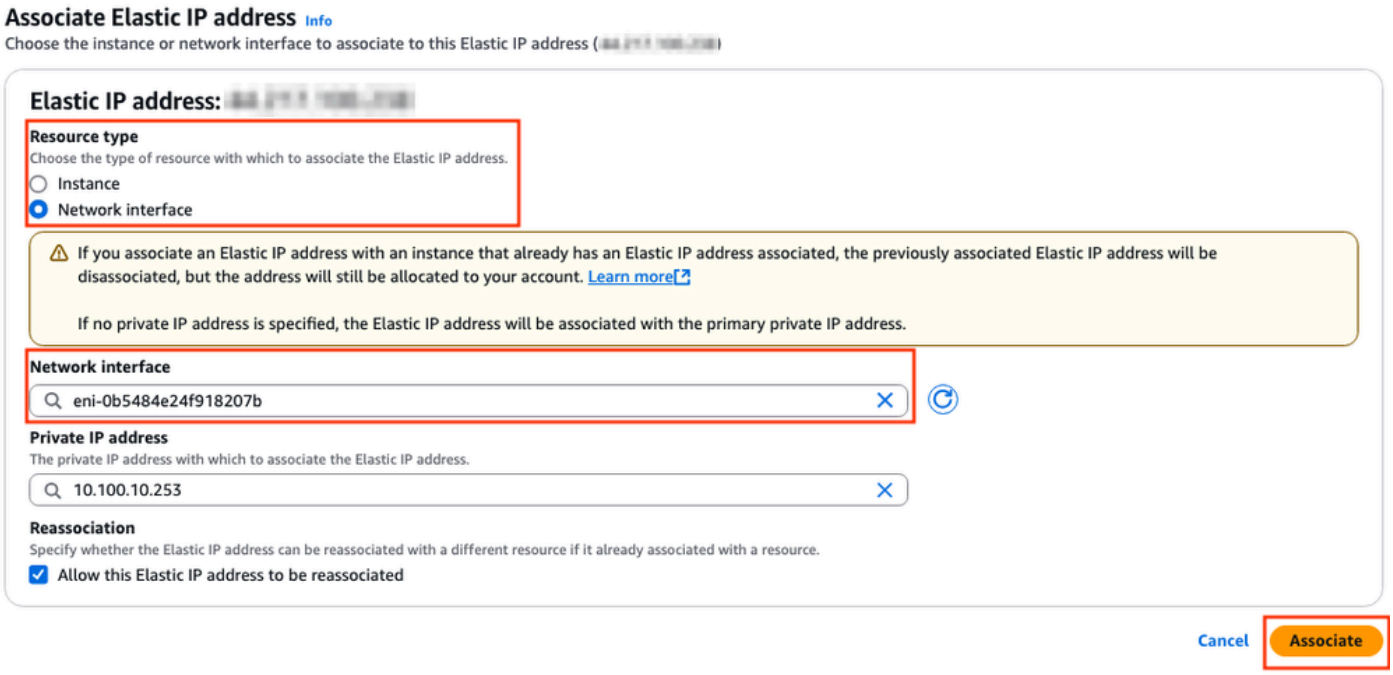

Lorsque l'adresse IP est créée, attribuez-la à l'interface publique de l'instance. Dans la section EC2 Dashboard > Network & Security > Elastic IPs, cliquez sur Actions > Associate Elastic IP address.




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.




## 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**

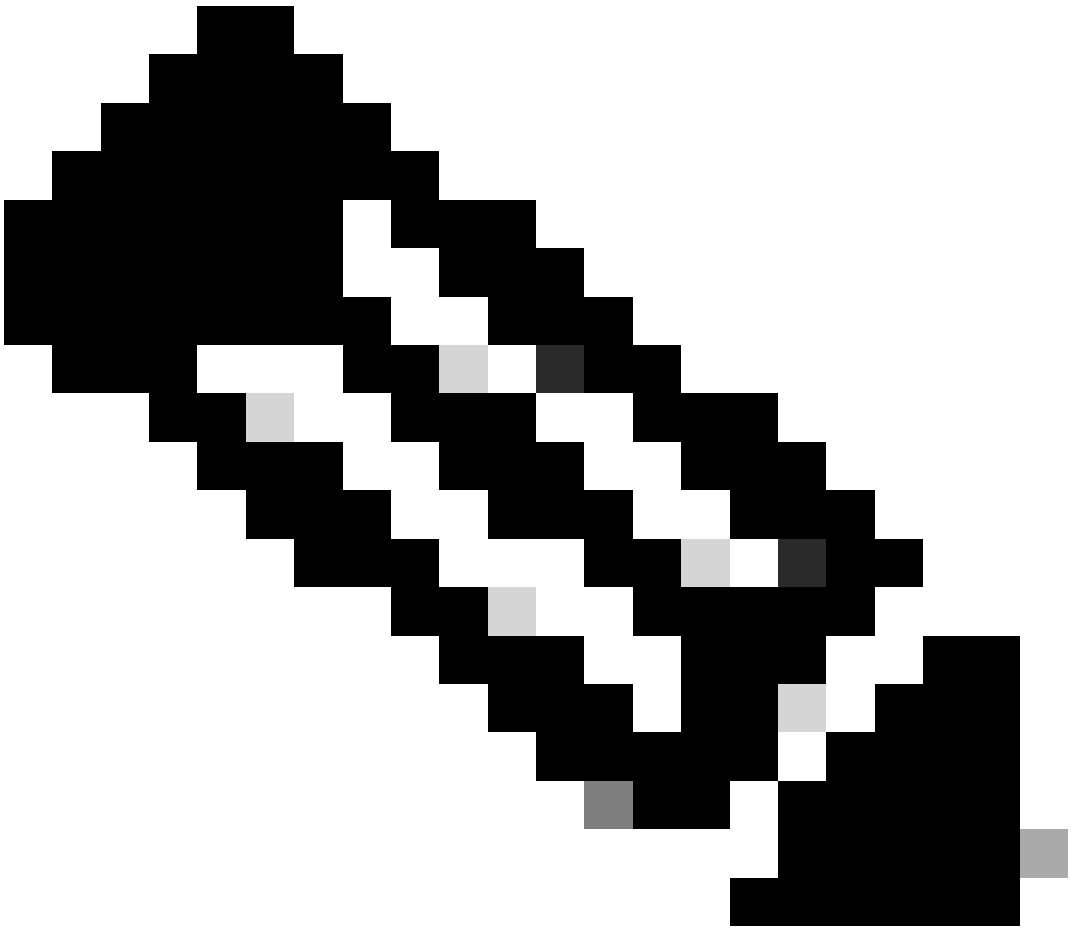
```
 netmask 255.255.255.0 broadcast 10.100.30.255
inet6 fe80::51:19ff:fea2:1151 prefixlen 64 scopeid 0x20<link>
ether 02:51:19:a2:11:51 txqueuelen 1000 (Ethernet)
RX packets 1366 bytes 376912 (376.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1417 bytes 189934 (189.9 KB)
TX errors 0 dropped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

---

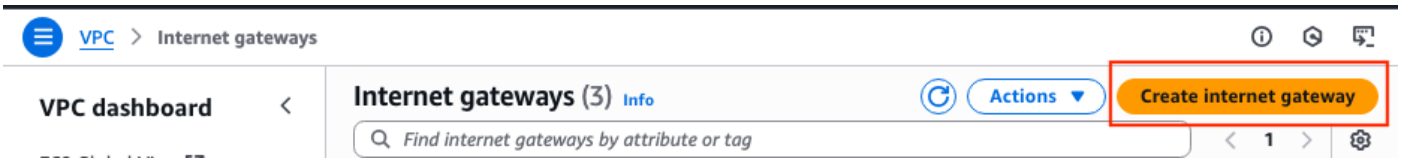


> Remarque : Si des modifications sont apportées aux interfaces, faites un battement sur l'interface ou rechargez la VM pour que ces modifications soient appliquées.

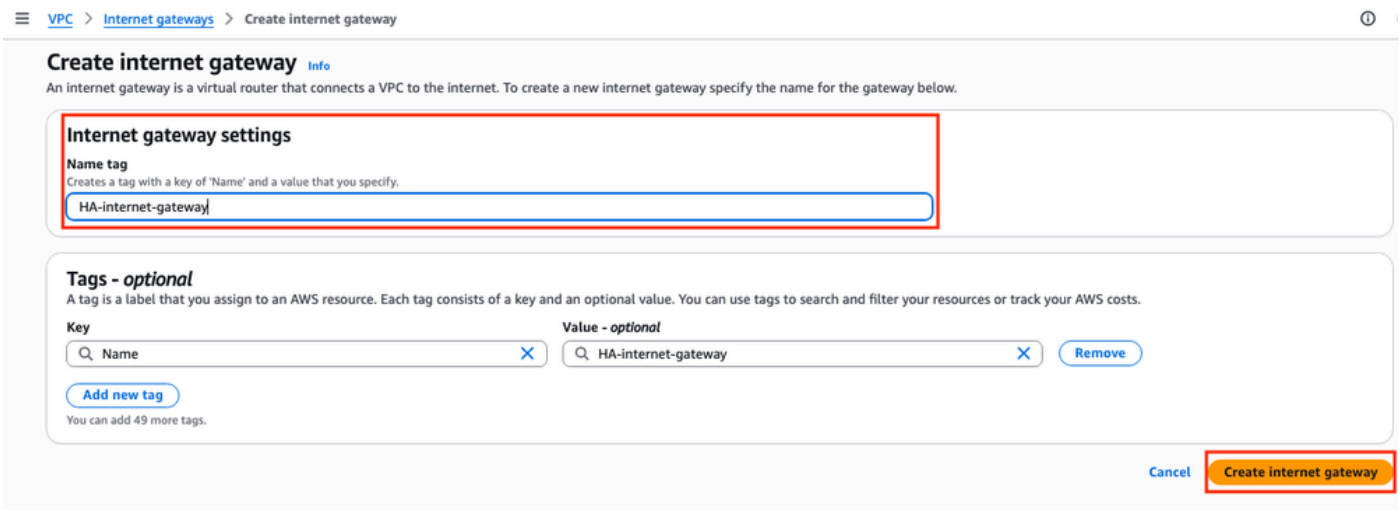
---

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

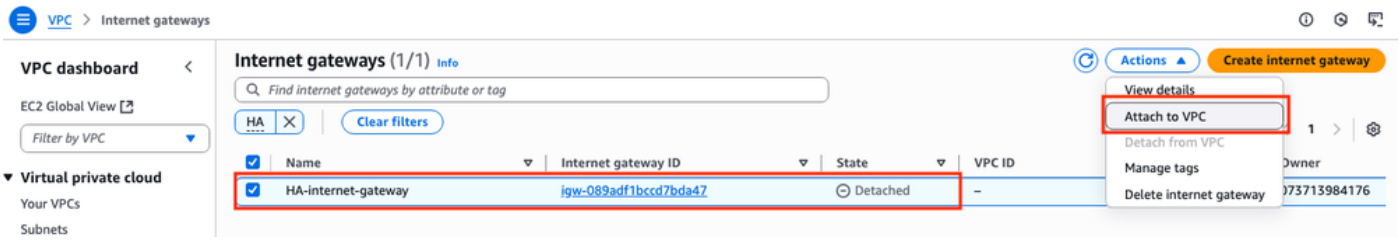
Dans la section **Tableau de bord VPC > Cloud privé virtuel > Passerelles Internet**, cliquez sur **Créer une passerelle Internet**.



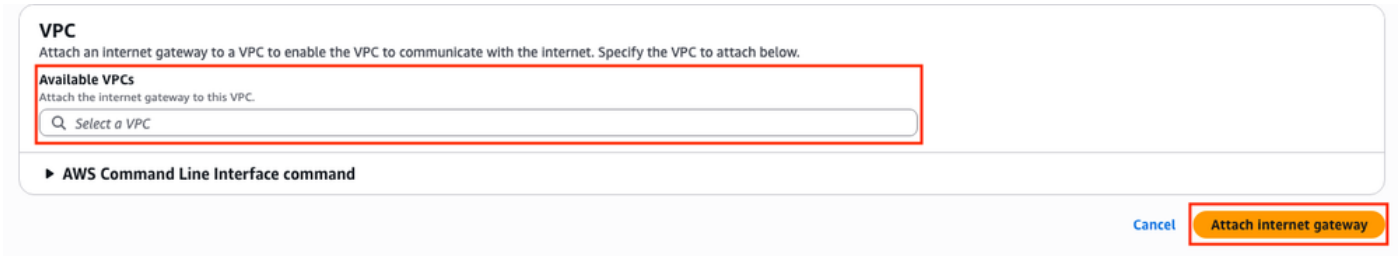

Dans cette nouvelle section, créez une **balise de nom** pour cette passerelle et cliquez sur **Créer une passerelle Internet**.



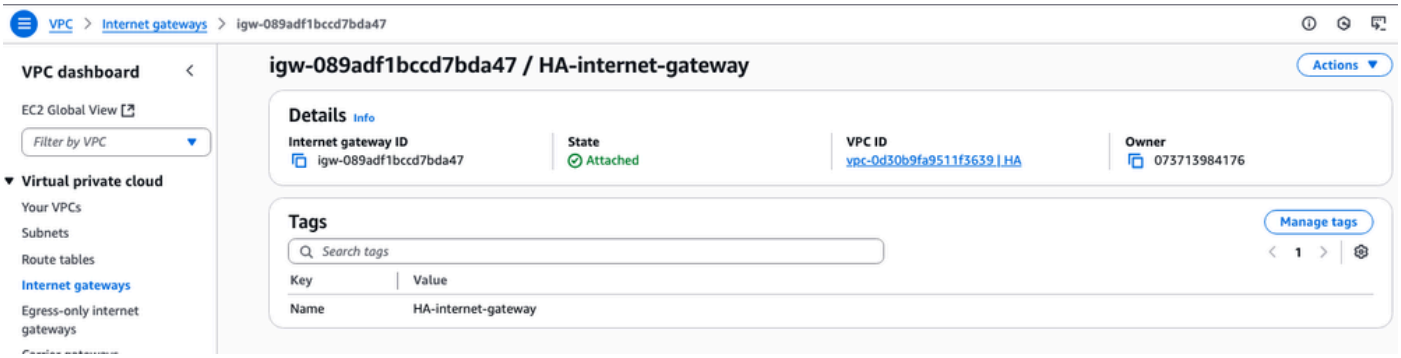

Une fois l'IGW créé, reliez-le à votre VPC correspondant. Accédez à la section **Tableau de bord VPC > Cloud privé virtuel > Passerelle Internet** et sélectionnez l'IGW correspondant. Cliquez sur **Actions > Attach to VPC**.




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



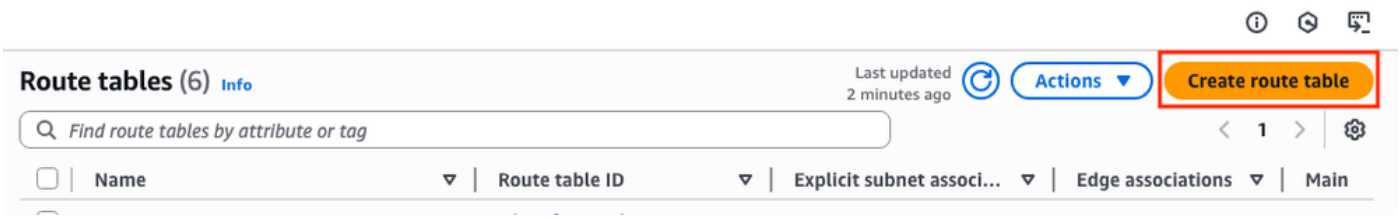

L'IGW doit indiquer l'état Attached tel qu'il est affiché :



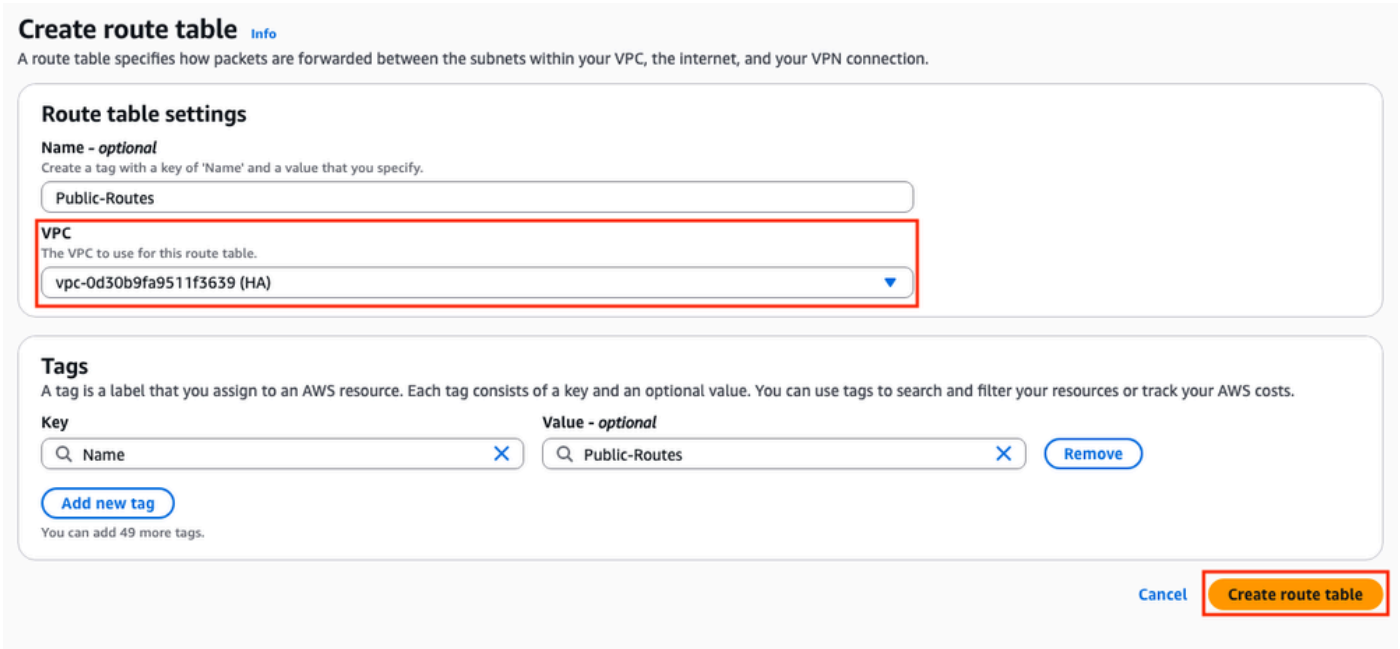

## Étape 10. Création et configuration de tables de routage sur AWS pour les sous-réseaux publics et privés

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

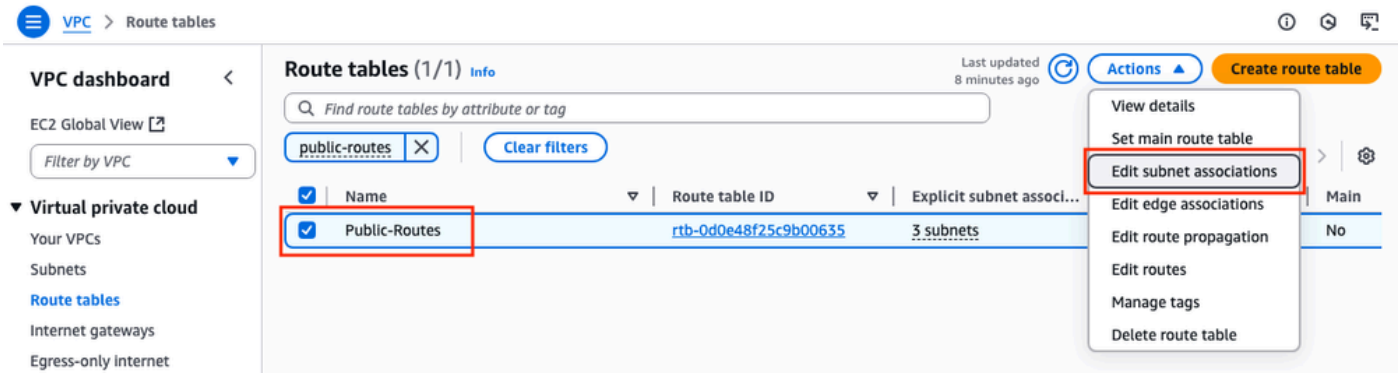
Afin d'établir la haute disponibilité sur cette topologie, associez tous les sous-réseaux publics et privés sur leurs tables de routage correspondantes. Dans la section Tableau de bord VPC > Cloud privé virtuel > Tables de routage, cliquez sur Créer une table de routage.



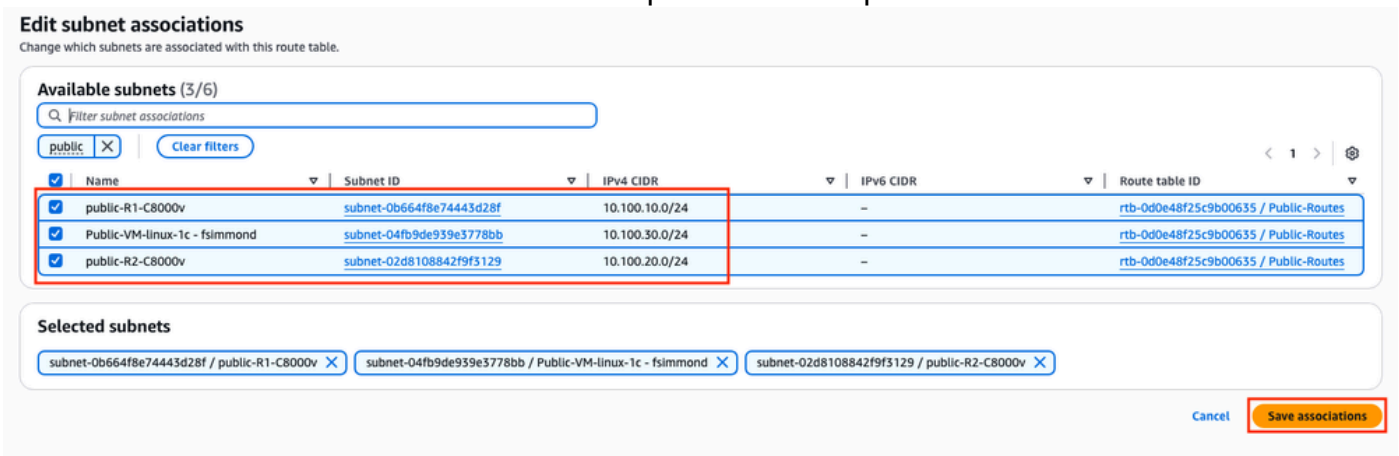

Dans la nouvelle section, sélectionnez le VPC correspondant à cette topologie. Une fois sélectionné, cliquez sur Create route table.



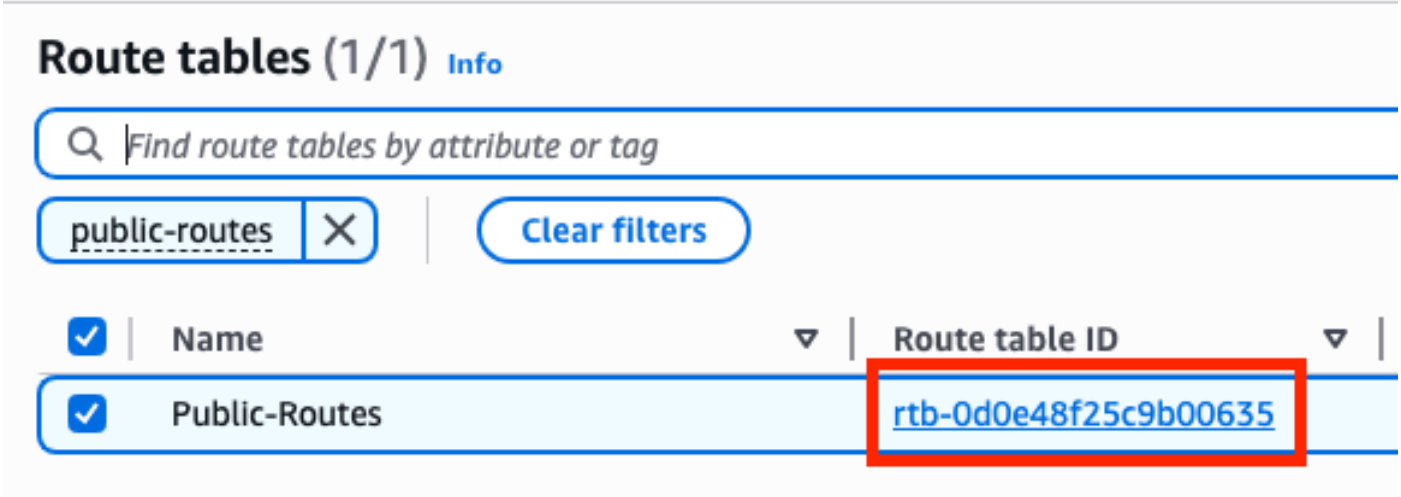

Dans la section Tables de routage, sélectionnez la table créée et cliquez sur Actions > Modifier les associations de sous-réseau.



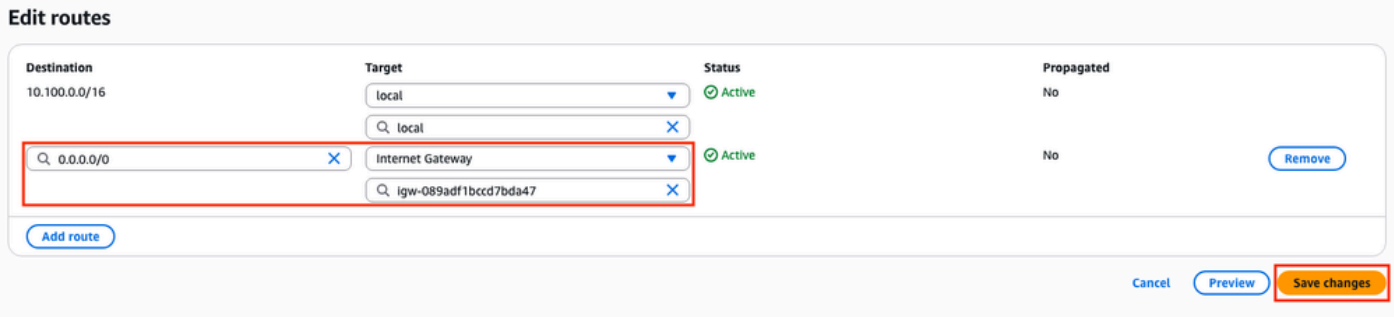

Sélectionnez ensuite les sous-réseaux correspondants et cliquez sur Save associations.




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:

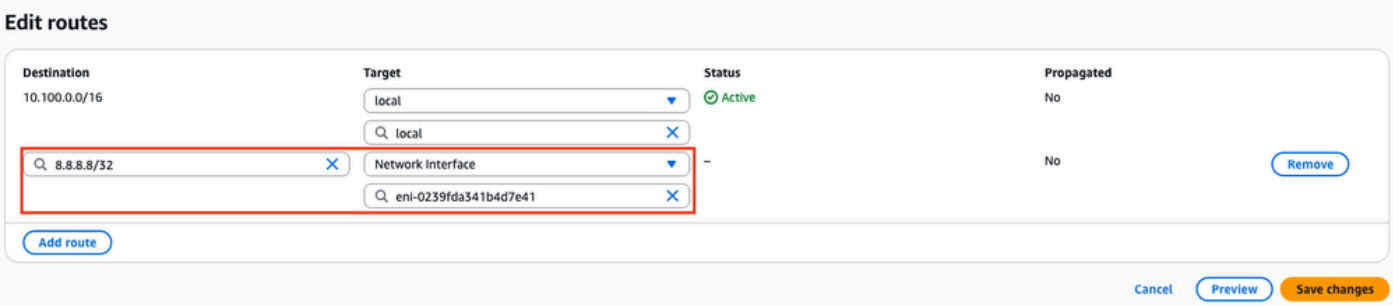



Afin d'obtenir l'accès à Internet, cliquez sur Add route et liez cette table de route publique avec le IGW créé à l'étape 9 avec ces paramètres. Une fois sélectionné, cliquez sur Enregistrer les modifications :




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 :




## 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.

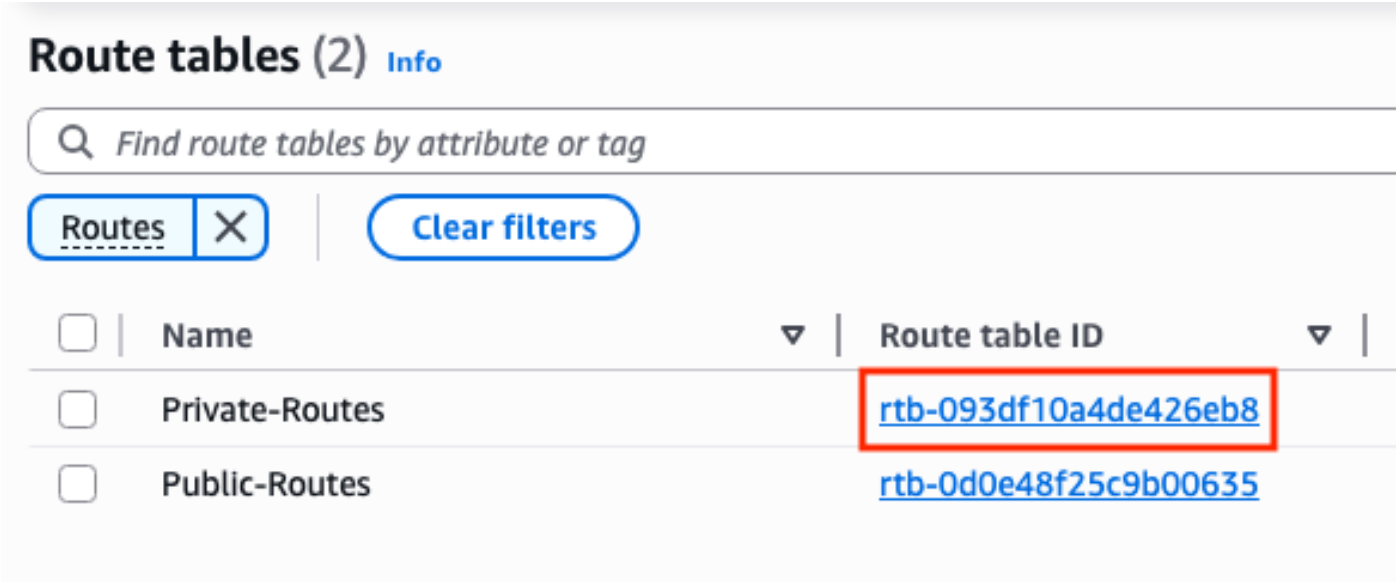
```
Router(config)# redundancy
Router(config-red)# cloud provider aws (node-id)
bfd peer <IP address of the remote device>
route-table <Route table ID>
cidr ip <traffic to be monitored/prefix>
eni <Elastic network interface (ENI) ID>
region <region-name>
```

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 :

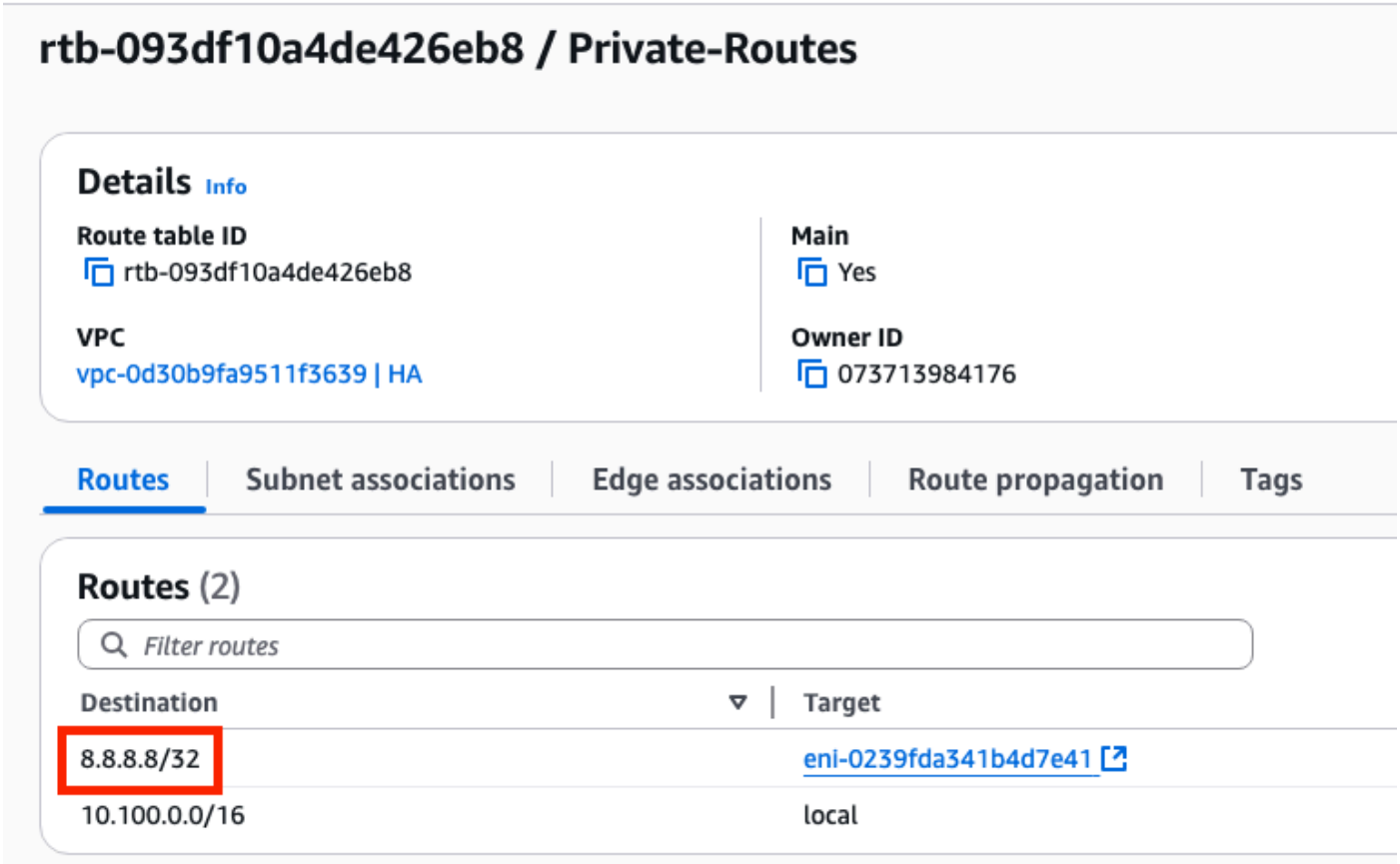
```
R1(config)#do sh bfd neighbors

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

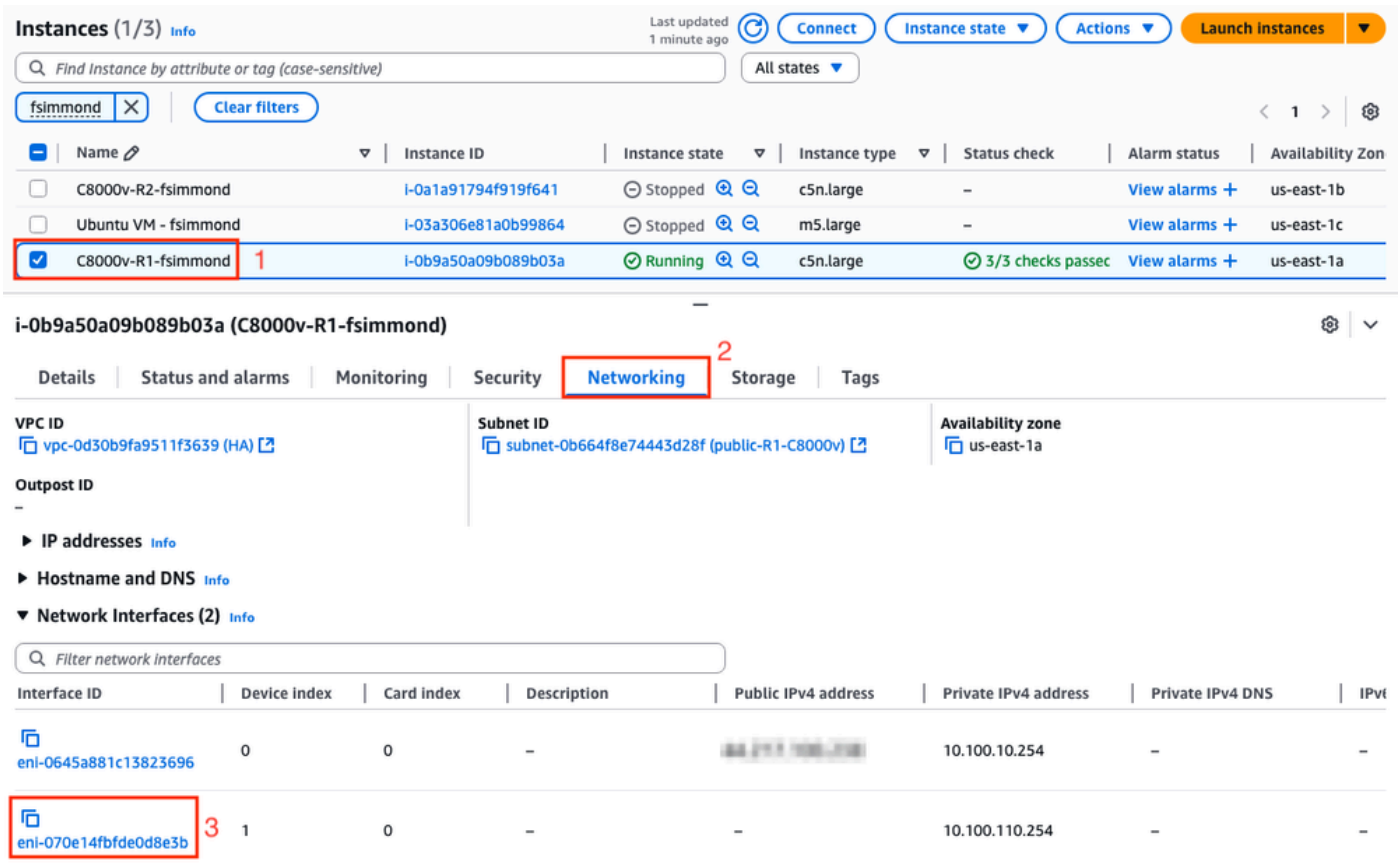
Le paramètre route-table est lié à l'ID de table de routage privée situé dans la section Tableau de bord VPC > Cloud privé virtuel > Tables de routage. Copiez l'ID de table de routage correspondant.




Le paramètre cidr ip est lié au préfixe de route ajouté sur la table de route privée (routes créées à l'étape 10.2) :




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 :



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
```

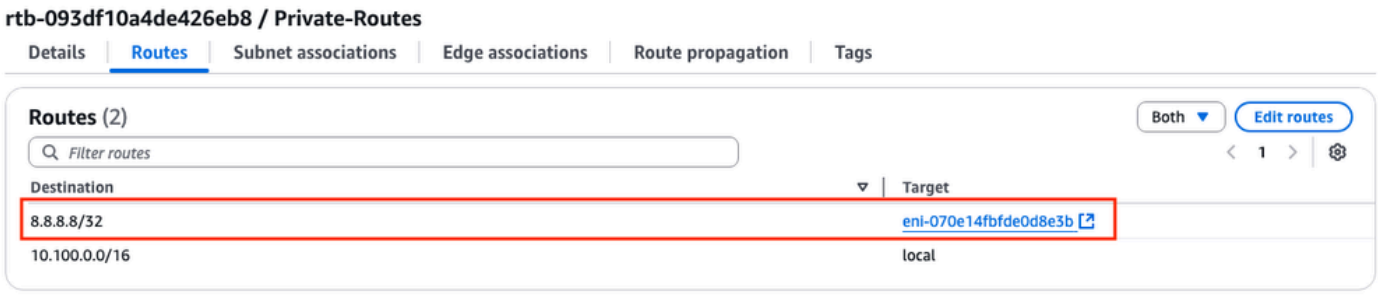
```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.200.2 Tu1 10 00:16:52 2 1470 0 2
```

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

2. 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 :




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 :


# Dépannage

Voici la plupart des points communs souvent oubliés/mal configurés lors de la recréation 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.