在AWS上部署C8000v高可用性配置

目錄

簡介

本文檔介紹如何在Amazon Web Services雲上使用Catalyst 8000v路由器設定高可用性環境。

必要條件

需求

思科建議您事先瞭解以下主題:

- 瞭解AWS控制檯及其元件的一般知識
- 瞭解Cisco IOS® XE軟體
- 有關HA功能的基本知識。

採用元件

此配置示例需要以下元件：

- 具有管理員角色的Amazon AWS帳戶
- 兩台運行Cisco IOS® XE 17.15.3a和1 Ubuntu 22.04 LTS虛擬機器的C8000v裝置 同一區域中的AMI

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

拓撲

有多種基於網路要求的HA部署方案。在本示例中，使用以下設定配置HA冗餘：

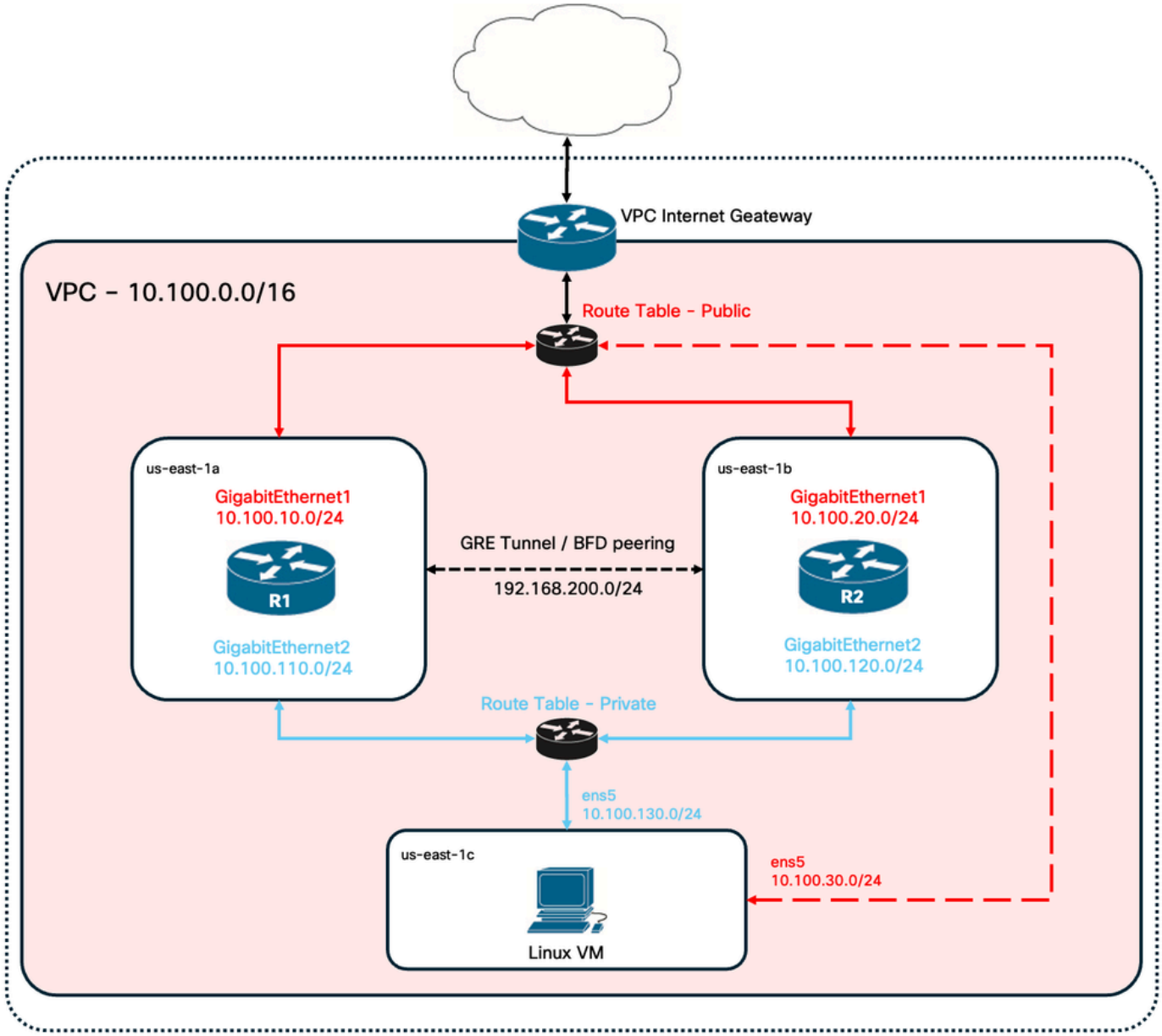
- 1x — 區域
- 1個 — VPC
- 3x — 可用區
- 6x — 網路介面/子網（3x公共介面/3x專用介面）
- 2x — 路由表（公用和專用）
- 2x - C8000v路由器(Cisco IOS® XEDenali 17.15.3a)
- 1個VM(Linux/Windows)

一個HA對中有兩台C8000v路由器，位於兩個不同的可用區中。將每個可用區視為獨立的資料中心，以實現額外的硬體恢復能力。

第三個區域是虛擬機器，用於模擬專用資料中心中的裝置。目前，通過公共介面啟用了Internet訪問，以便您可以訪問和配置VM。通常，所有正常流量必須通過專用路由表。

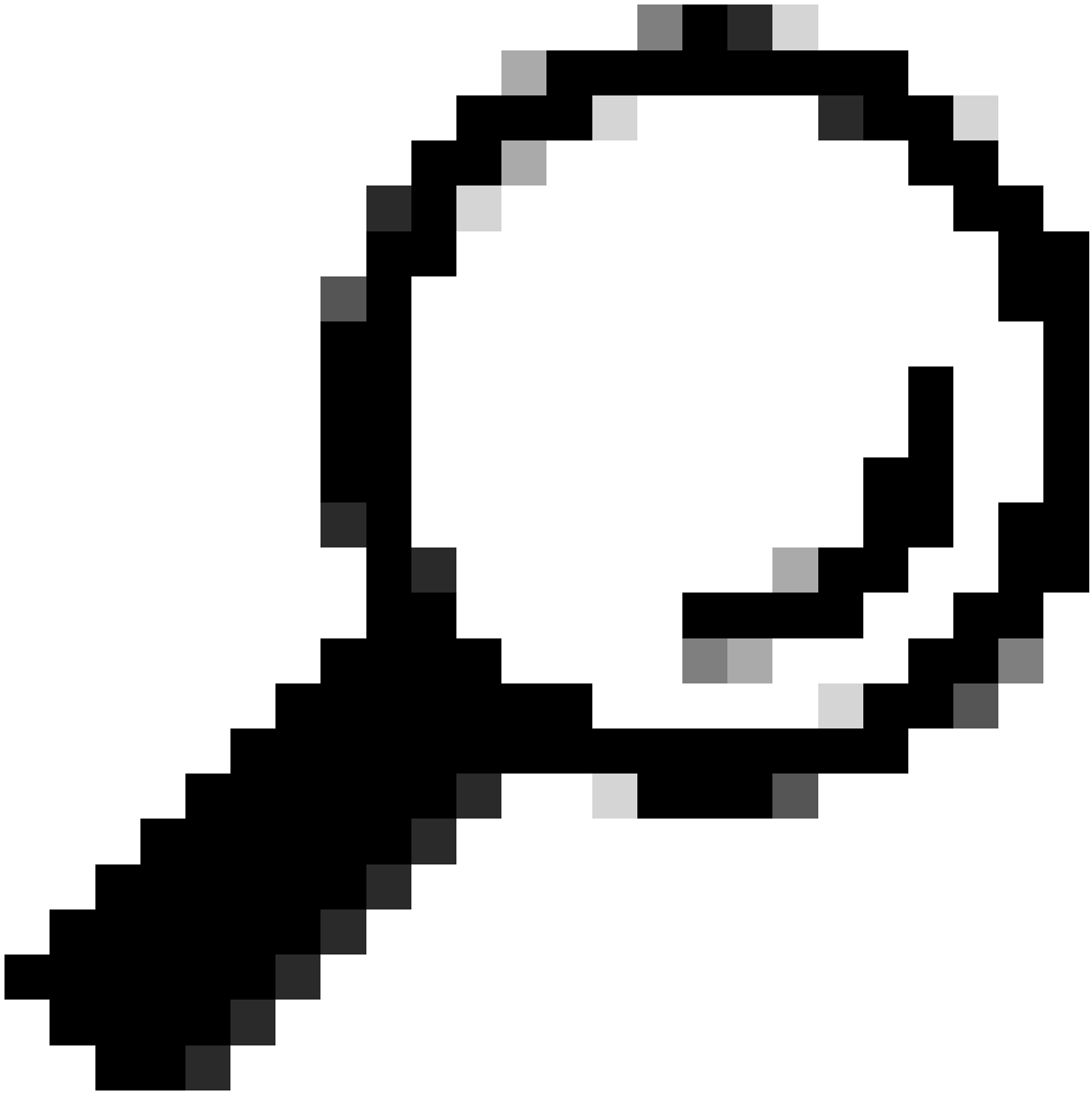
要模擬流量，請從虛擬機器的專用介面啟動ping，通過R1遍歷專用路由表以到達8.8.8.8。發生故障轉移時，請驗證專用路由表是否已自動更新，以通過R2路由器的專用介面路由流量。

網路圖表



表格摘要

為了總結拓撲，下表列出了實驗中每個元件中最重要的值。本表中提供的資訊僅用於本實驗。



提示：使用此表有助於在整個指南中保持對關鍵變數的清晰概述。建議以此格式收集資訊以簡化流程。

裝置	可用區	介面	IP地址	RTB	埃尼
R1	us-east-1a	GigabitEthernet1	10.100.10.254	rtb-0d0e48f25c9b00635（公用）	eni-0645a881c13823696
		GigabitEthernet2	10.100.110.254	rtb-093df10a4de426eb8（專用）	eni-070e14fbfde0d8e3b
R2	us-east-1b	GigabitEthernet1	10.100.20.254	rtb-0d0e48f25c9b00635（公用）	eni-0a7817922ffbb317b

		GigabitEthernet2	10.100.120.254	rtb-093df10a4de426eb8（專用）	eni-0239fda341b4d7e41
Linux虛擬機器	us-east-1c	ens5	10.100.30.254	rtb-0d0e48f25c9b00635（公用）	eni-0b28560781b3435b1
		ens6	10.100.130.254	rtb-093df10a4de426eb8（專用）	eni-05d025e88b6355808

限制

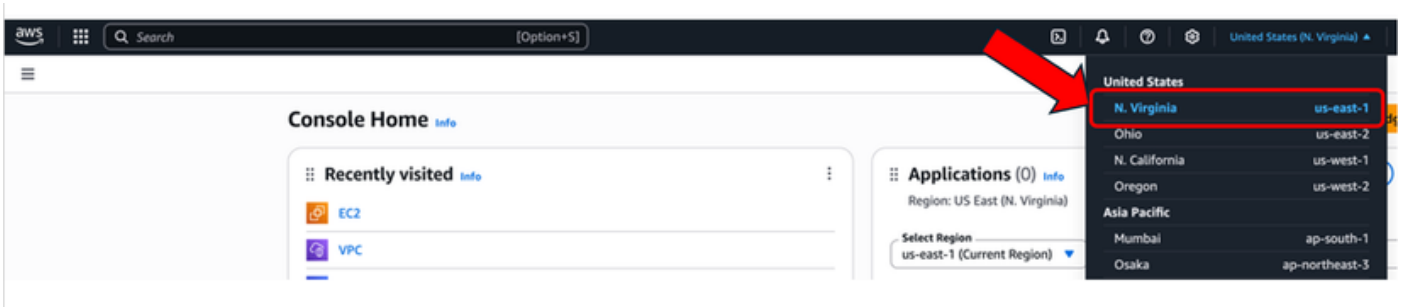
- 在建立的任何子網上，不要使用該子網的第一個可用地址。這些IP地址由AWS服務在內部使用。
- 請勿在VRF中配置C8000v裝置的公共介面。 如果設定了此設定，則HA無法正常工作。

組態

一般配置流程側重於在適當的區域建立所請求的VM，然後向下移動到最具體的配置，例如每個配置的路由和介面。但是，建議先瞭解拓撲，然後按所需的任意順序進行配置。

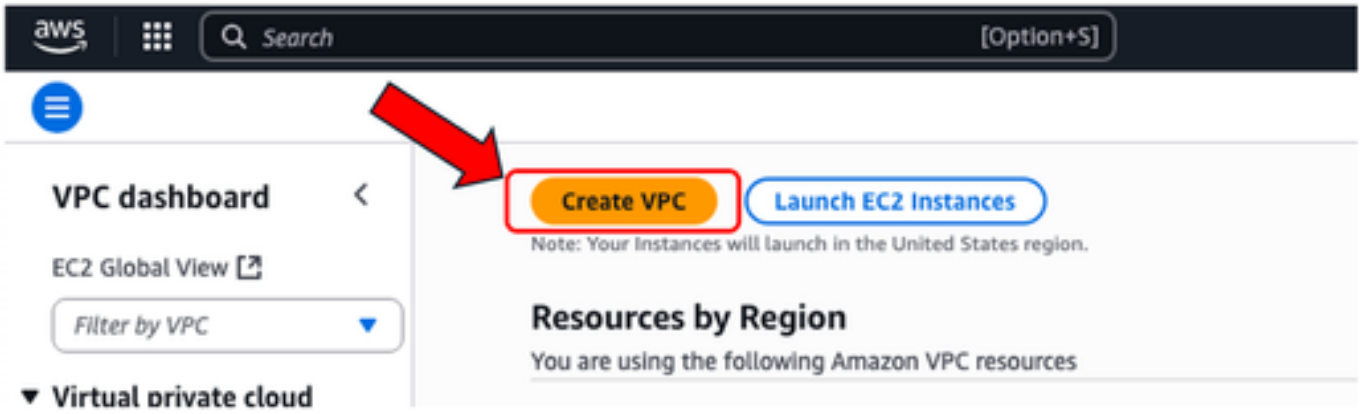
步驟1.選擇區域

在本部署指南中，選擇US West(North Virginia)- us-east-1區域作為VPC區域。



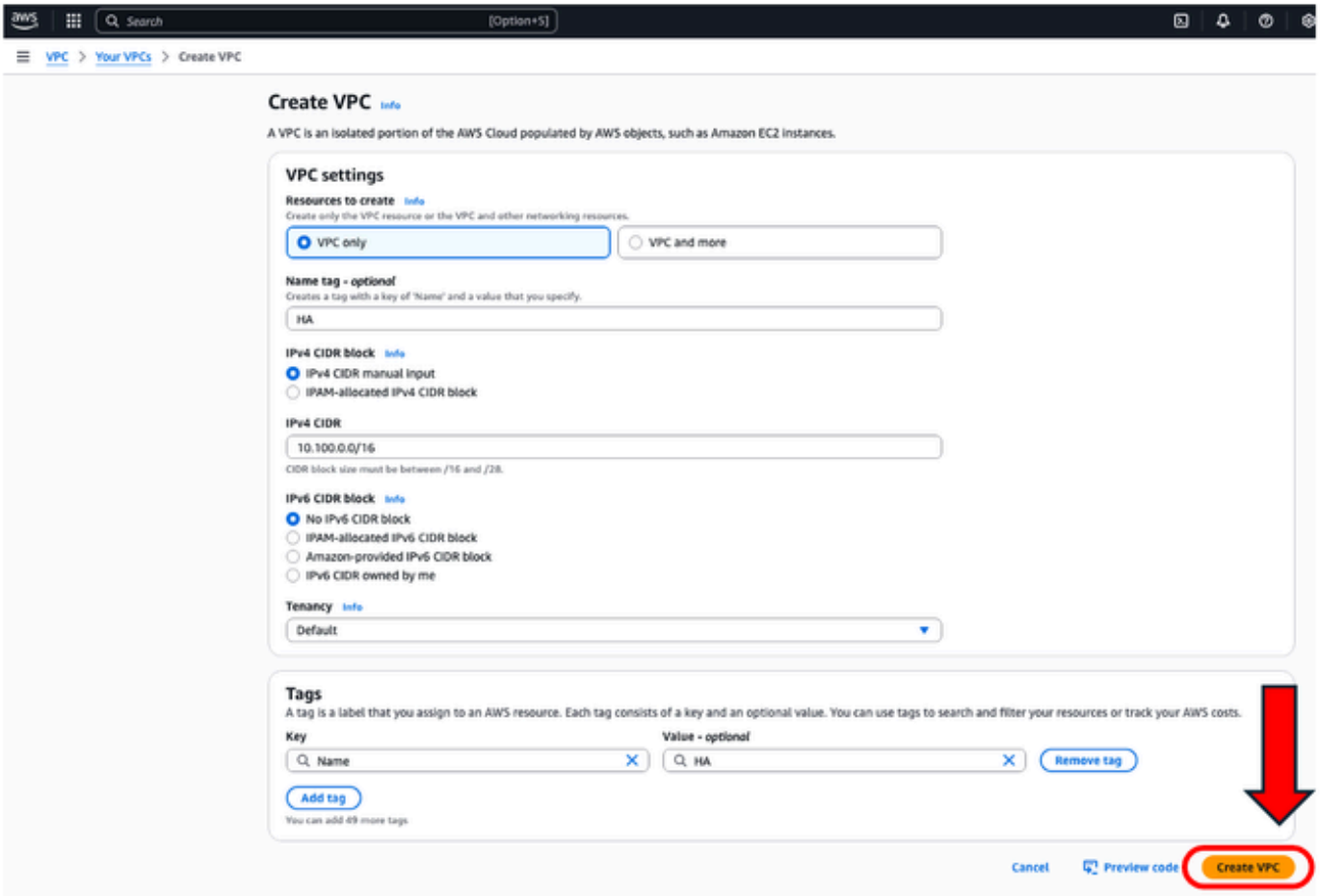
步驟2.建立VPC

在AWS控制檯上，導航至VPC > VPC Dashboard > Create VPC。

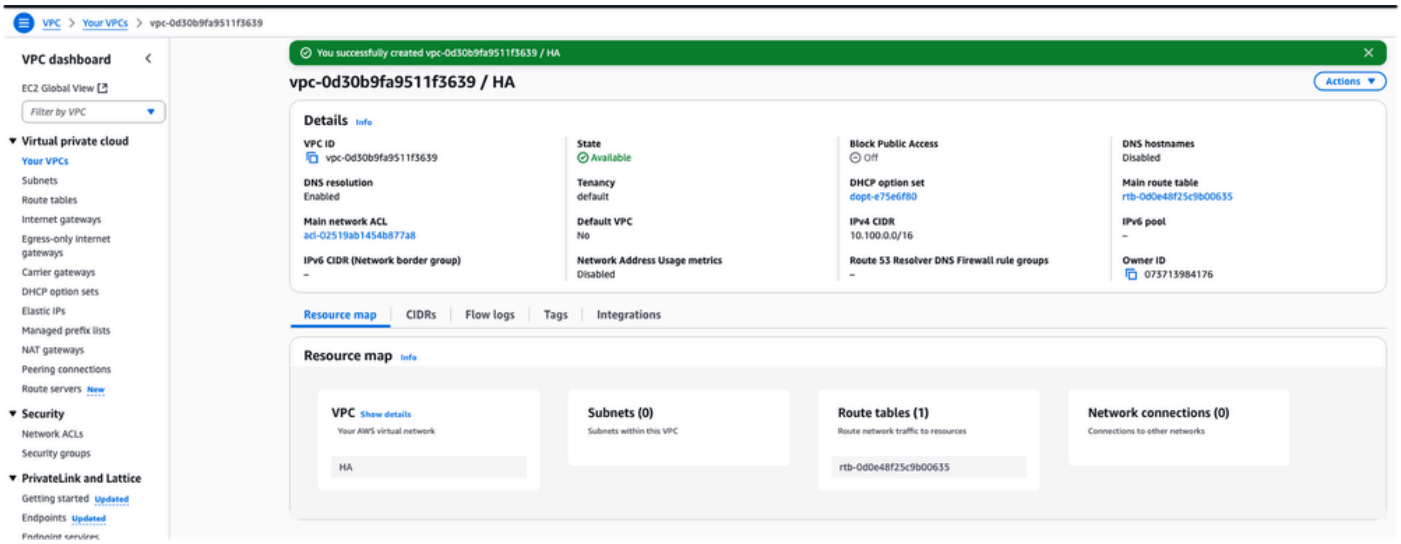


建立VPC時，請選擇VPC only選項。您可以根據需要分配一個/16網路來使用。

在此部署指南中，選擇10.100.0.0/16網路：

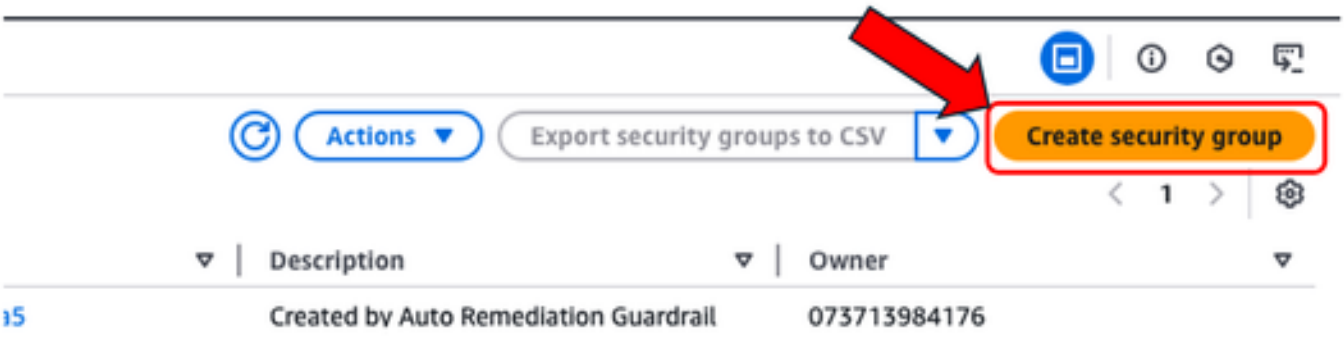


按一下建立VPC後，現在建立了帶有HA標籤的VPC-0d30b9fa9511f3639:

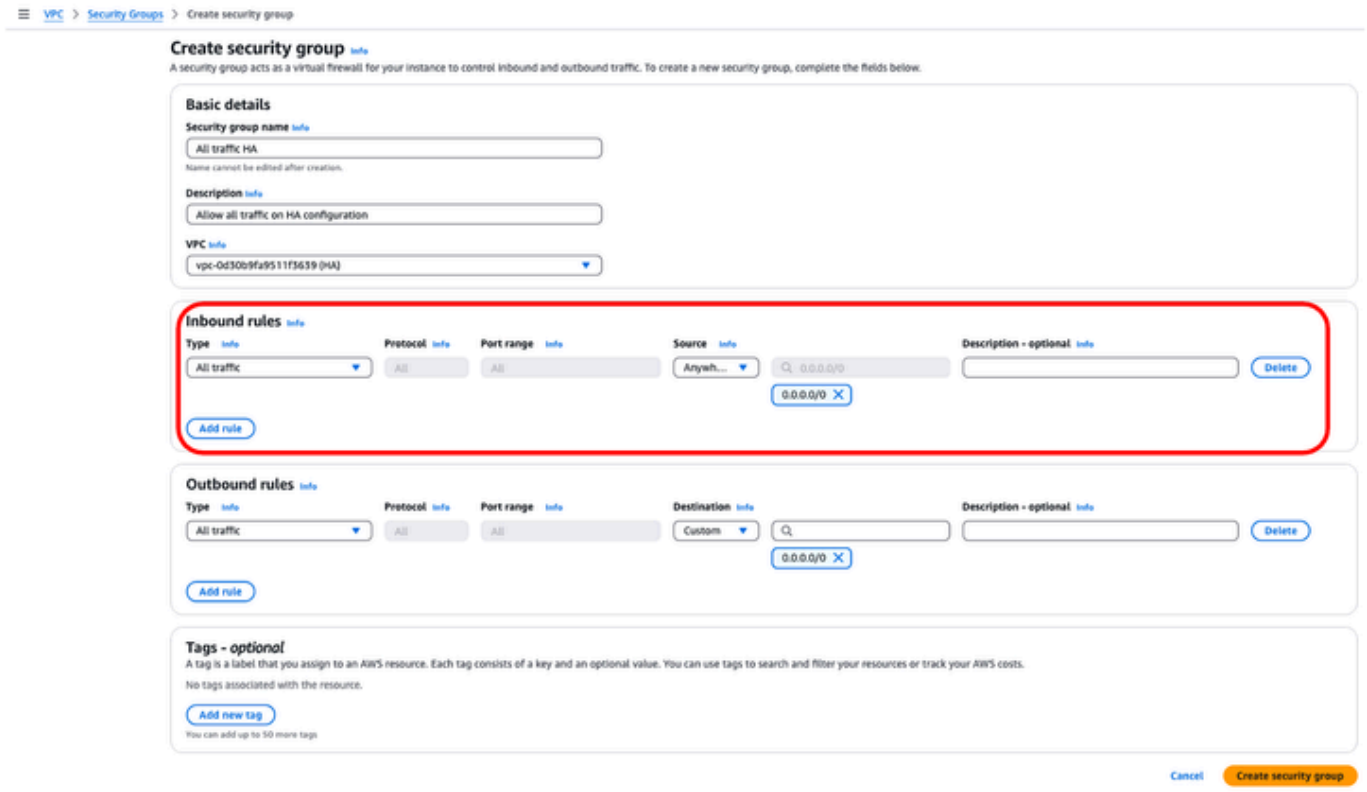


步驟3.為VPC建立安全組

在AWS中，Security Groups的功能與ACL類似，允許或拒絕流量到達VPC中配置的VM。在AWS控制檯上，導航到VPC > VPC Dashboard > Security > Security Groups部分，然後點選Create security group。



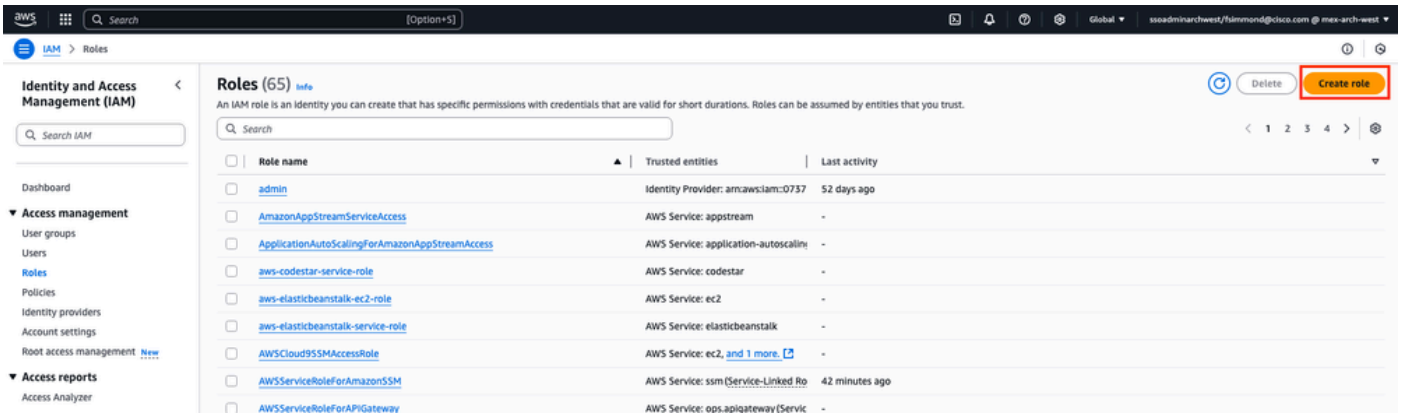
在Inbound Rules（入站規則）下，定義您要允許哪些流量。在本例中，使用0.0.0.0/0網路選擇All Traffic。



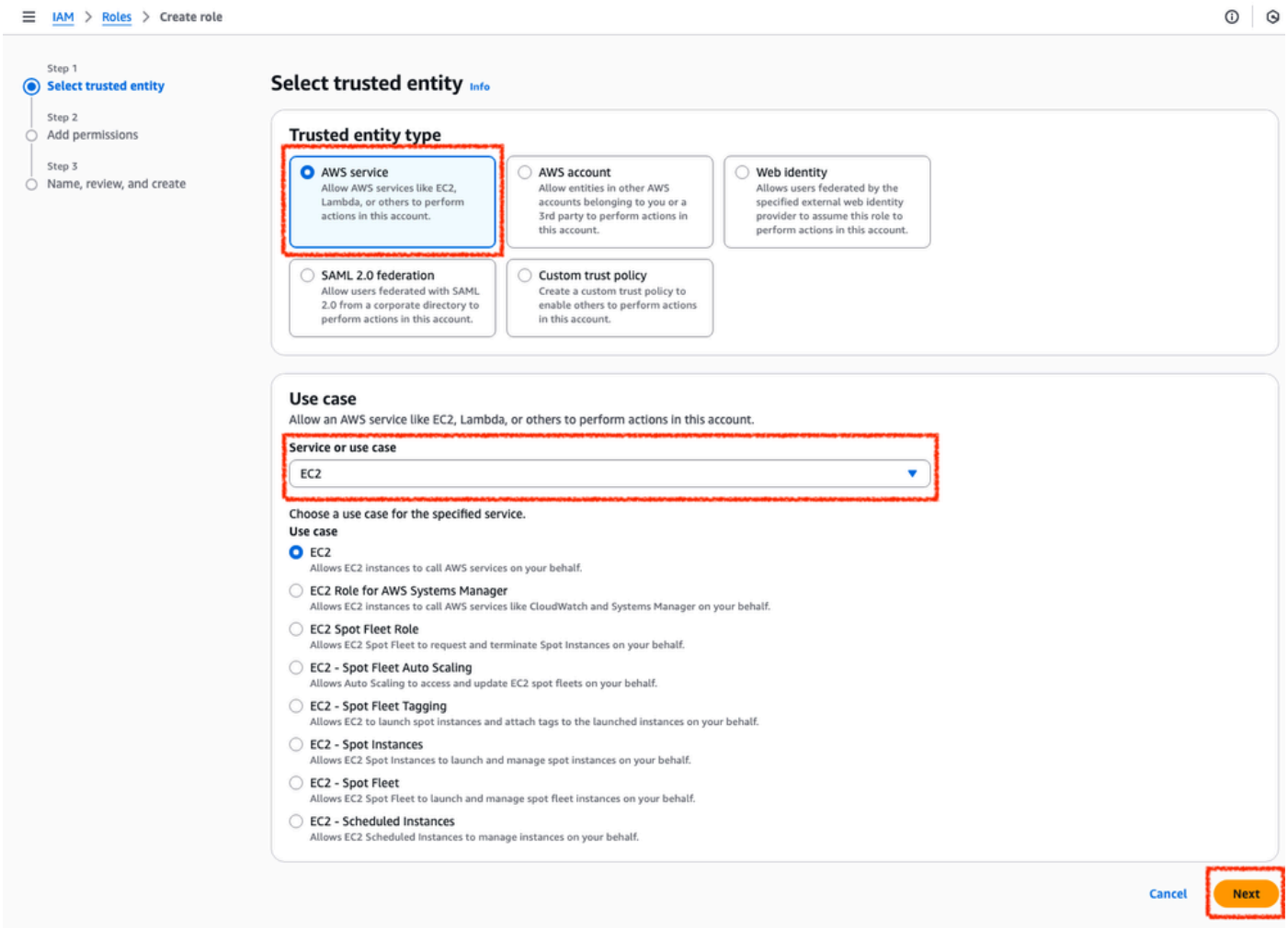
步驟4.使用策略建立IAM角色並與VPC關聯

IAM向您的AMI授予對Amazon API的必要訪問許可權。C8000v用作代理，呼叫AWS API命令來修改AWS中的路由表。預設情況下，EC2例項不允許訪問API。因此，必須建立一個新的IAM角色，該角色將在建立AMI期間應用。

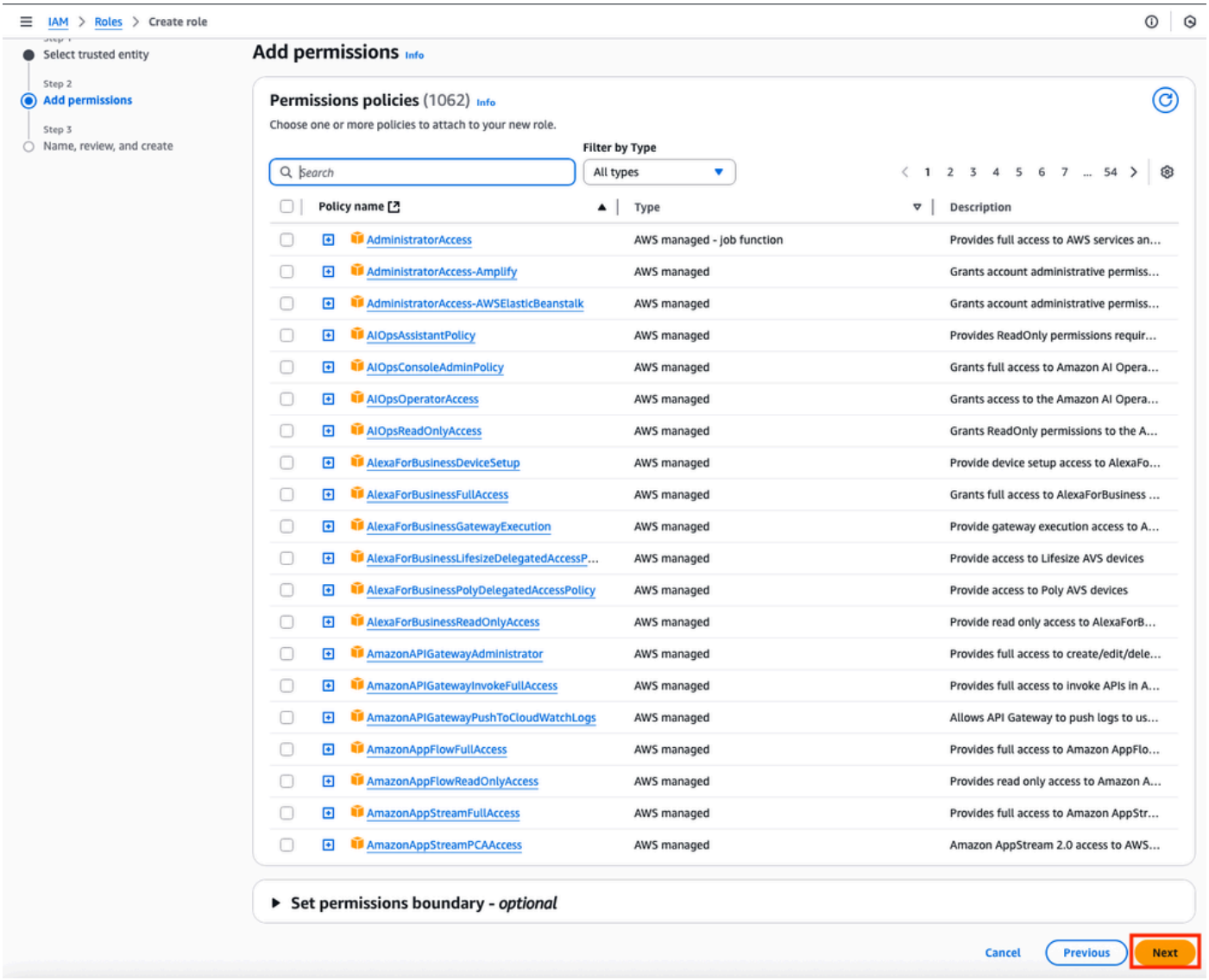
瀏覽到IAM控制面板，然後導航到訪問管理>角色>創建角色。此過程包括3個步驟：



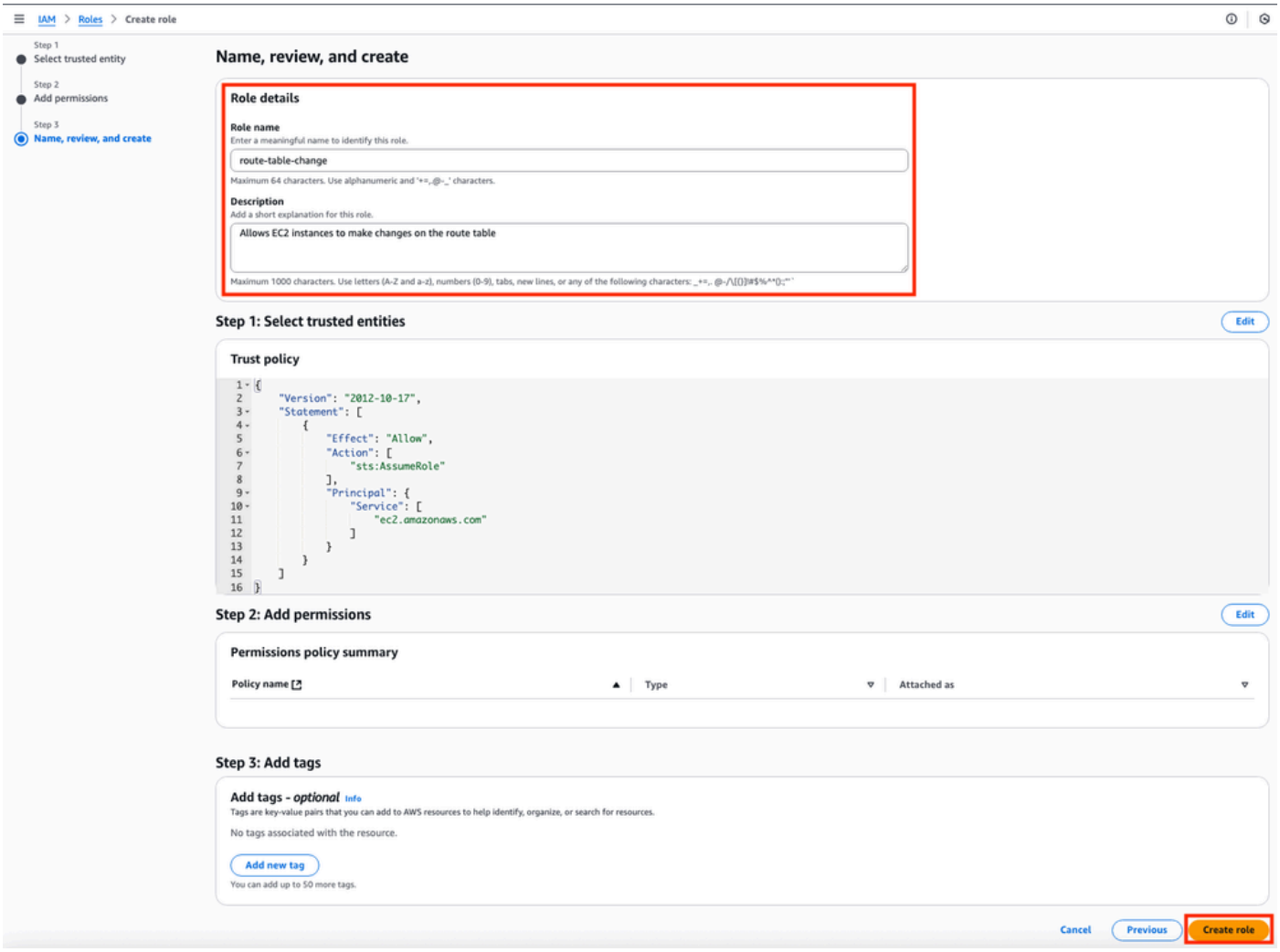
首先，選擇Trusted entity type部分上的AWS Service選項，然後選擇EC2作為為此策略分配的服務。


IAM > Roles > Create role
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

完成後，按一下「Next:

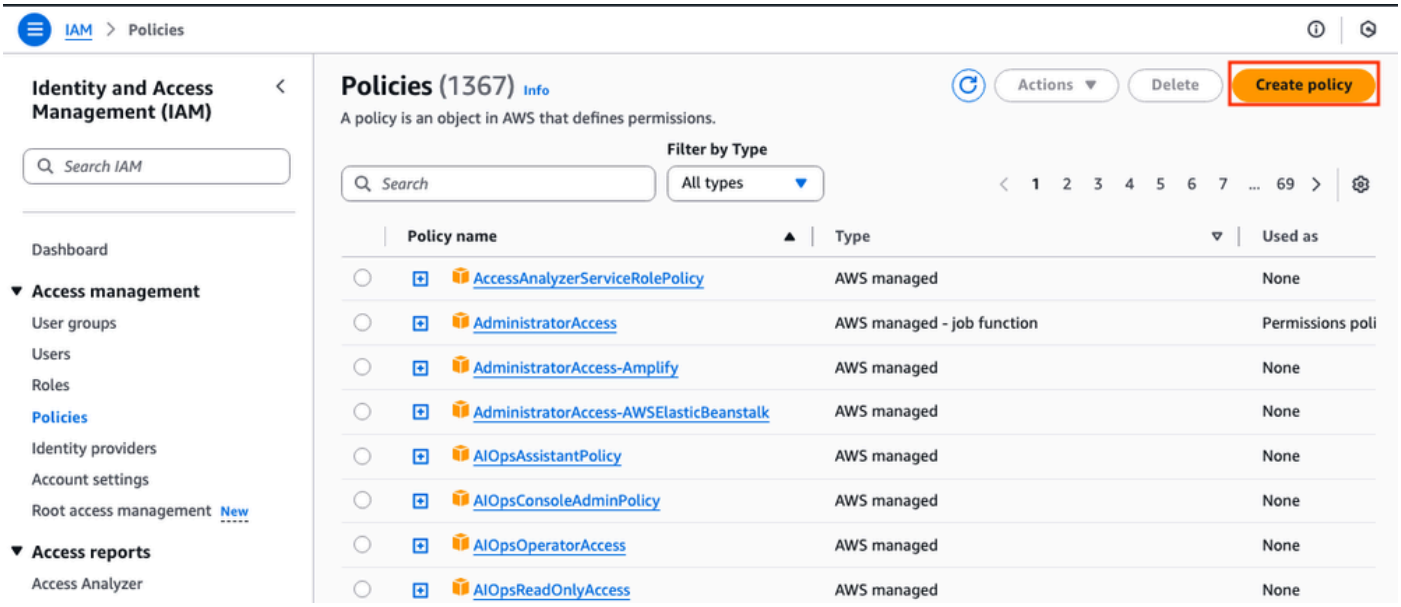


最後，設定Role Name，然後按一下Create Role按鈕。

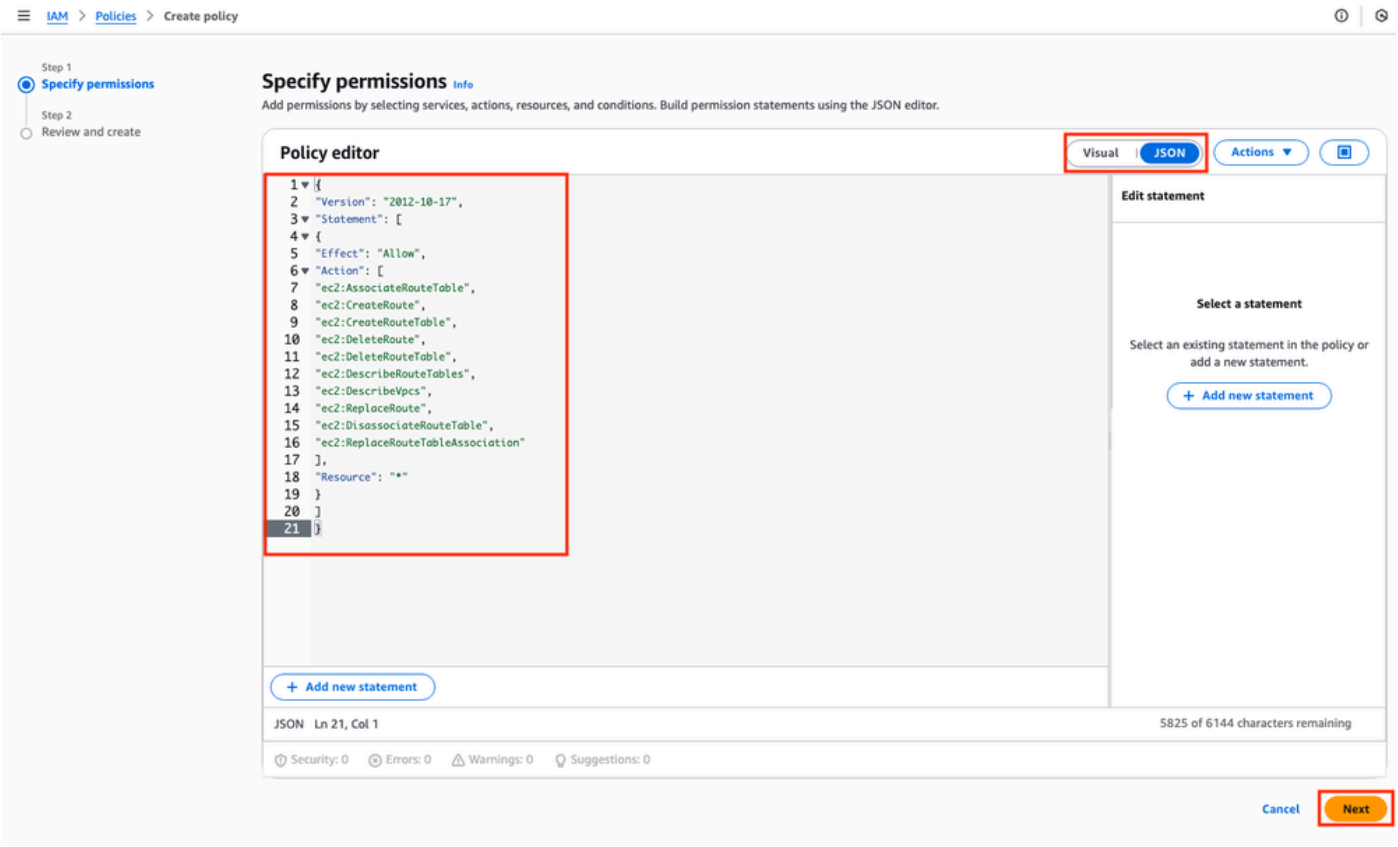


步驟5.建立信任策略並將其附加到IAM角色

建立角色後，必須制定信任策略以獲得在需要時修改AWS路由表的技能。移動到IAM控制面板上的Policies部分。按一下Create Policy按鈕。此過程包括兩個步驟：



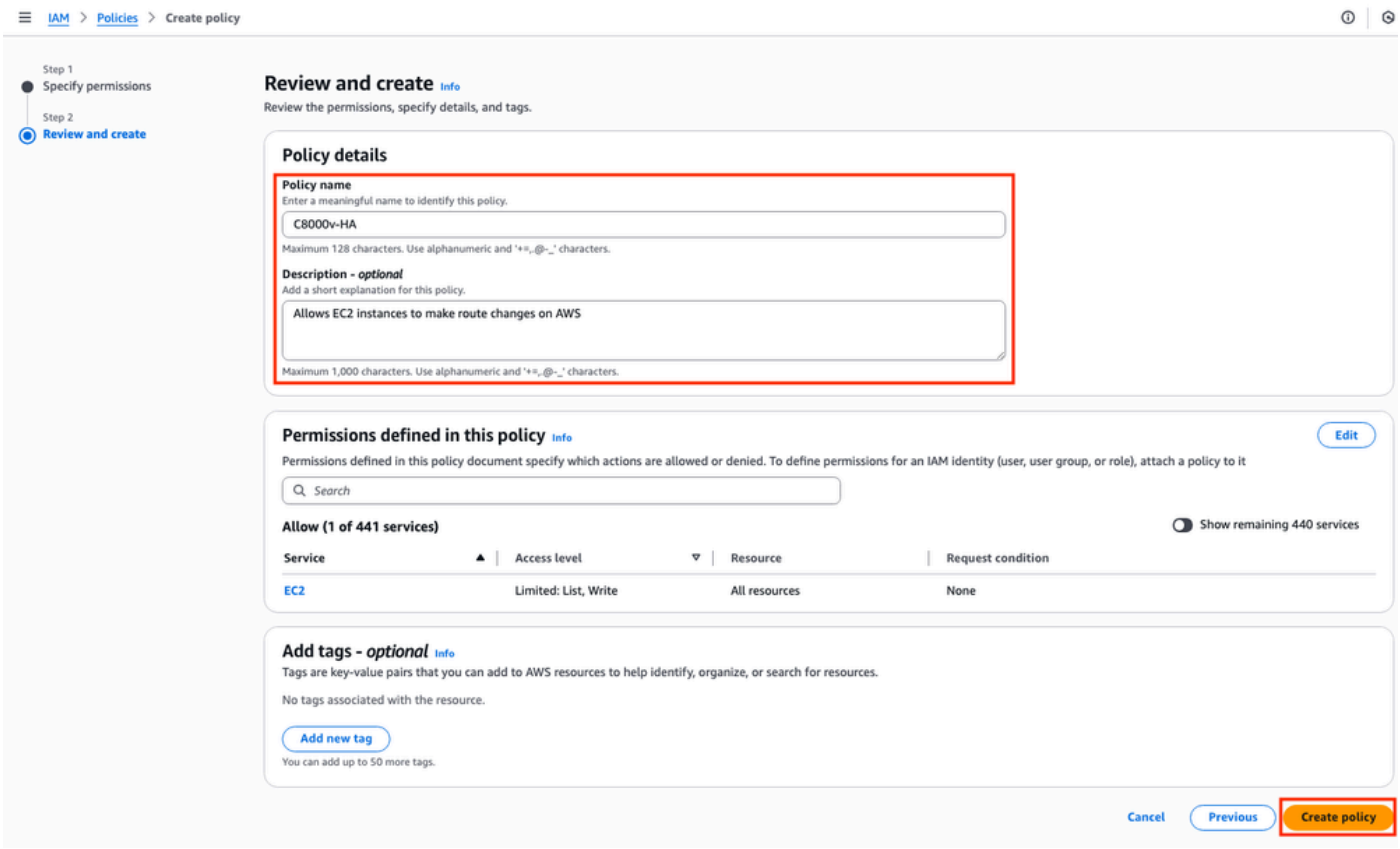
首先，確保Policy Editor正在使用JSON，並應用如下所示的命令。配置後，按一下Next:



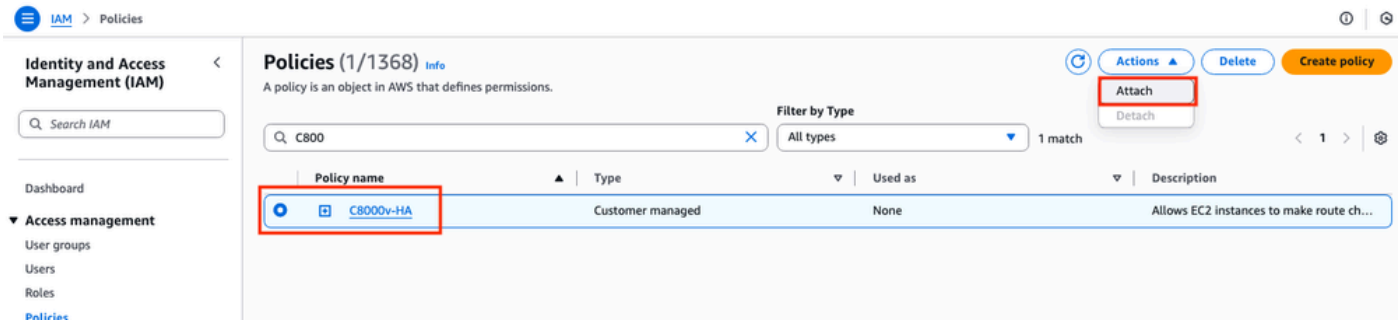
這是影象中使用的文本代碼：

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

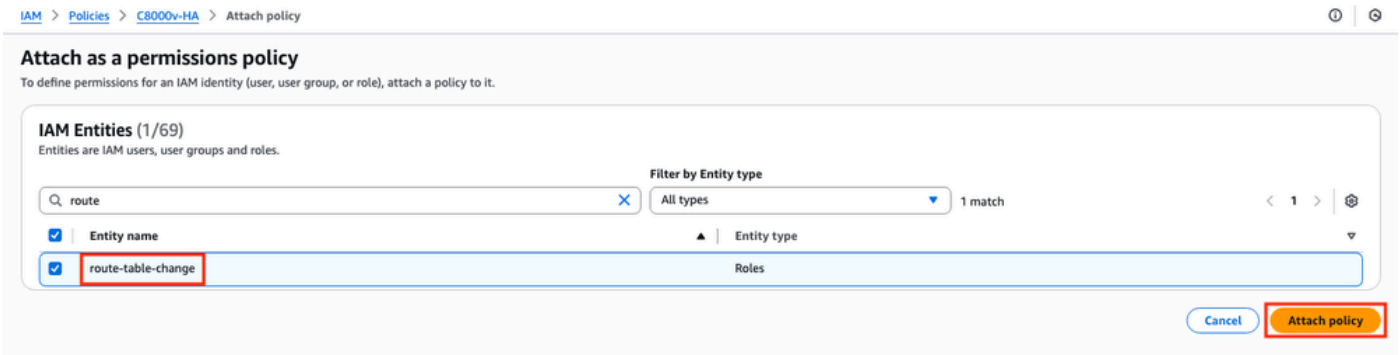
稍後，設定Policy Name，然後按一下Create Policy。



建立策略後，篩選並選擇策略，然後按一下Actions下拉選單上的Attach選項。



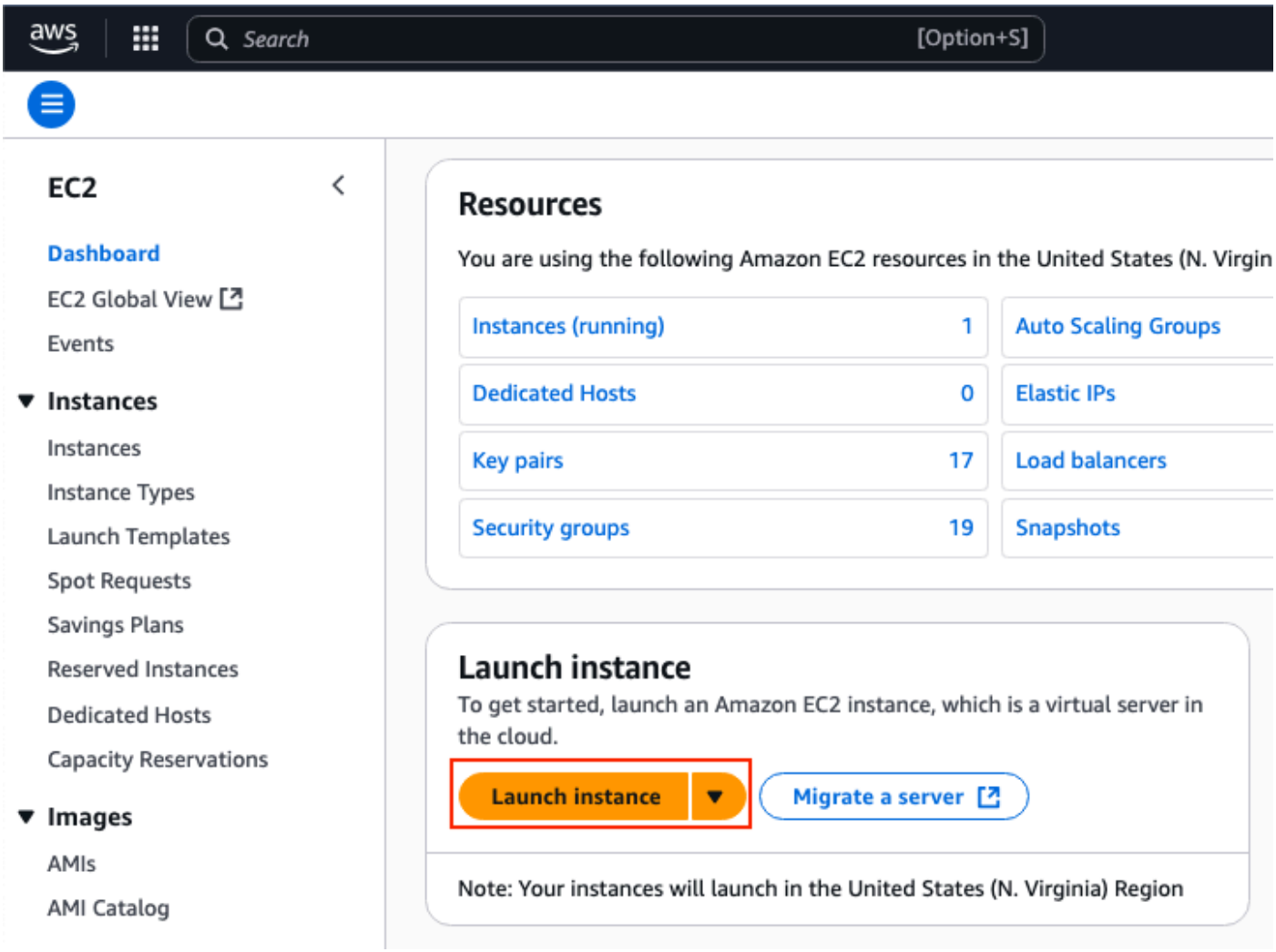
開啟了一個新視窗。在「IAM實體」部分，篩選並選擇已創建的IAM角色，然後單擊Attach policy。



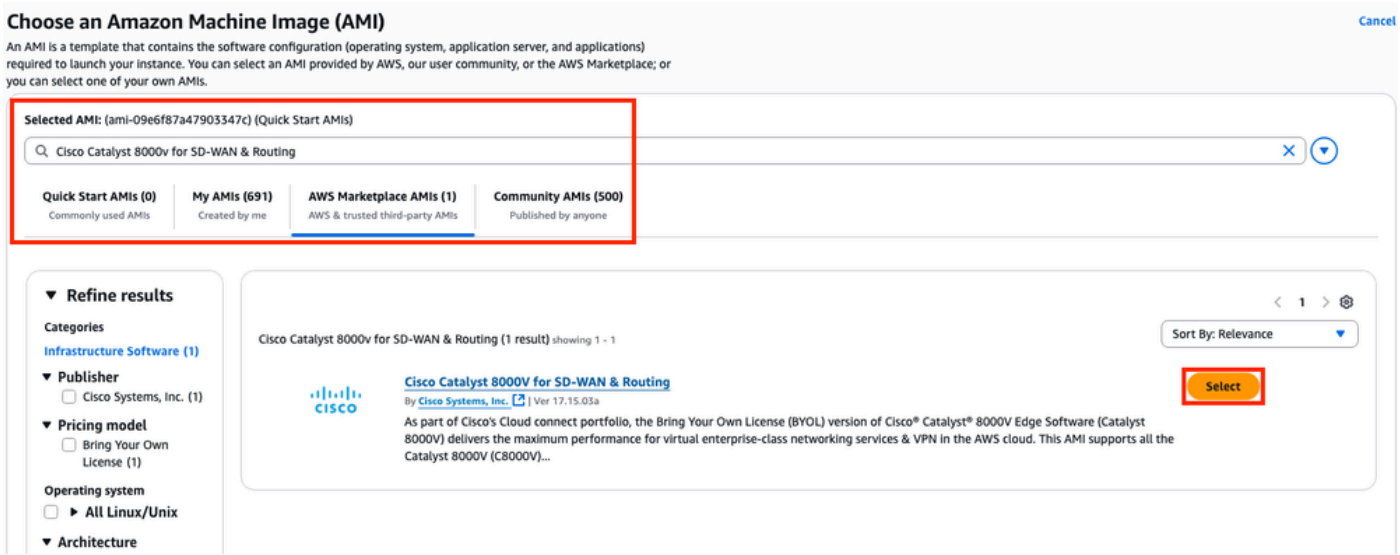
步驟6.配置並啟動C8000v例項

每個C8000v路由器將有2個介面（1個公共介面，1個專用介面），並將在其自己的可用區上建立。

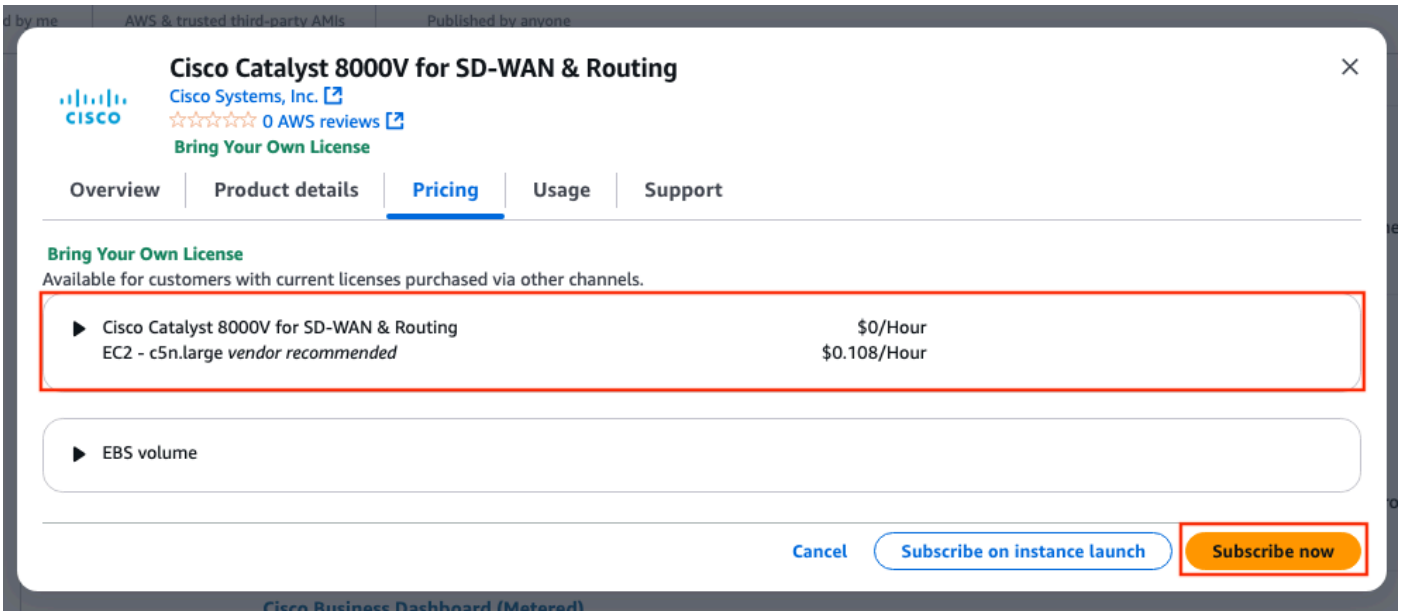
在EC2 Dashboard上，按一下Launch Instances:



使用名稱Cisco Catalyst 8000v for SD-WAN & Routing過濾AMI資料庫。在AWS Marketplace AMIs清單中，按一下Select。

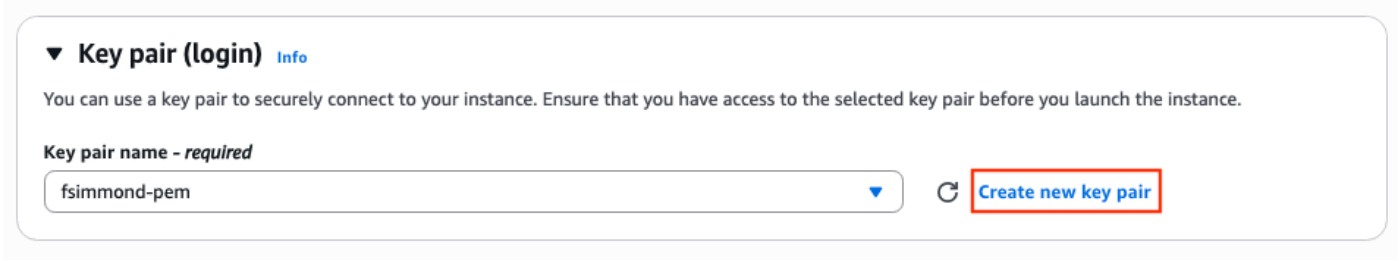


選擇AMI的相應大小。在本例中，選擇了c5n.large大小。這可能取決於您的網路所需的容量。選擇後，按一下Subscribe now。

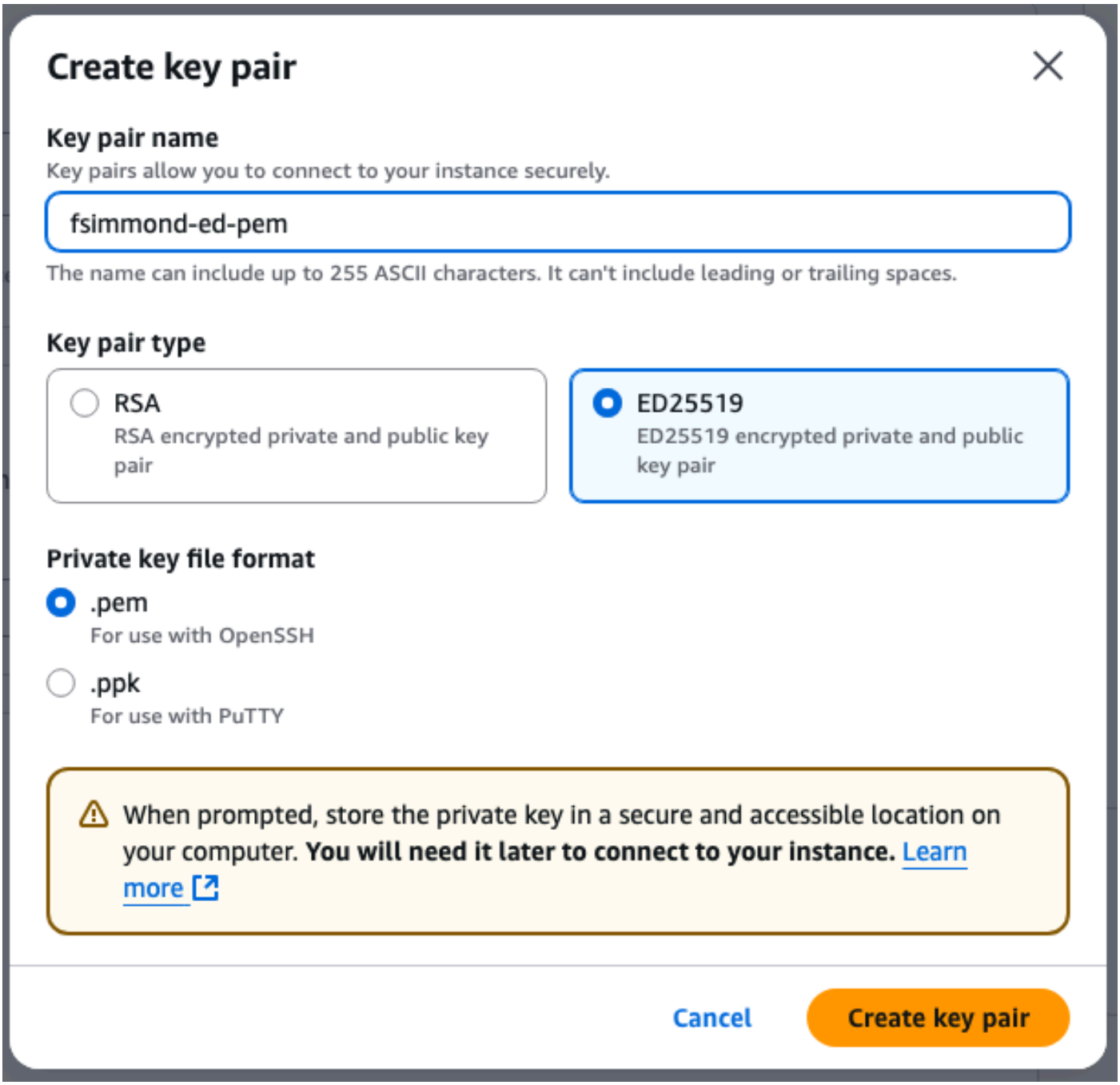


步驟6.1.為遠端訪問配置金鑰對

訂用AMI後，將顯示一個包含多個選項的新視窗。在「Key pair(login)(金鑰對（登入）)」部分，如果不存在金鑰對，請按一下Create new key pair。您可以為每個建立的裝置重複使用單個金鑰。



此時會顯示一個新的彈出視窗。在本例中，將建立具有ED25519加密的.pem金鑰檔案。設定完所有內容後，按一下Create key pair。



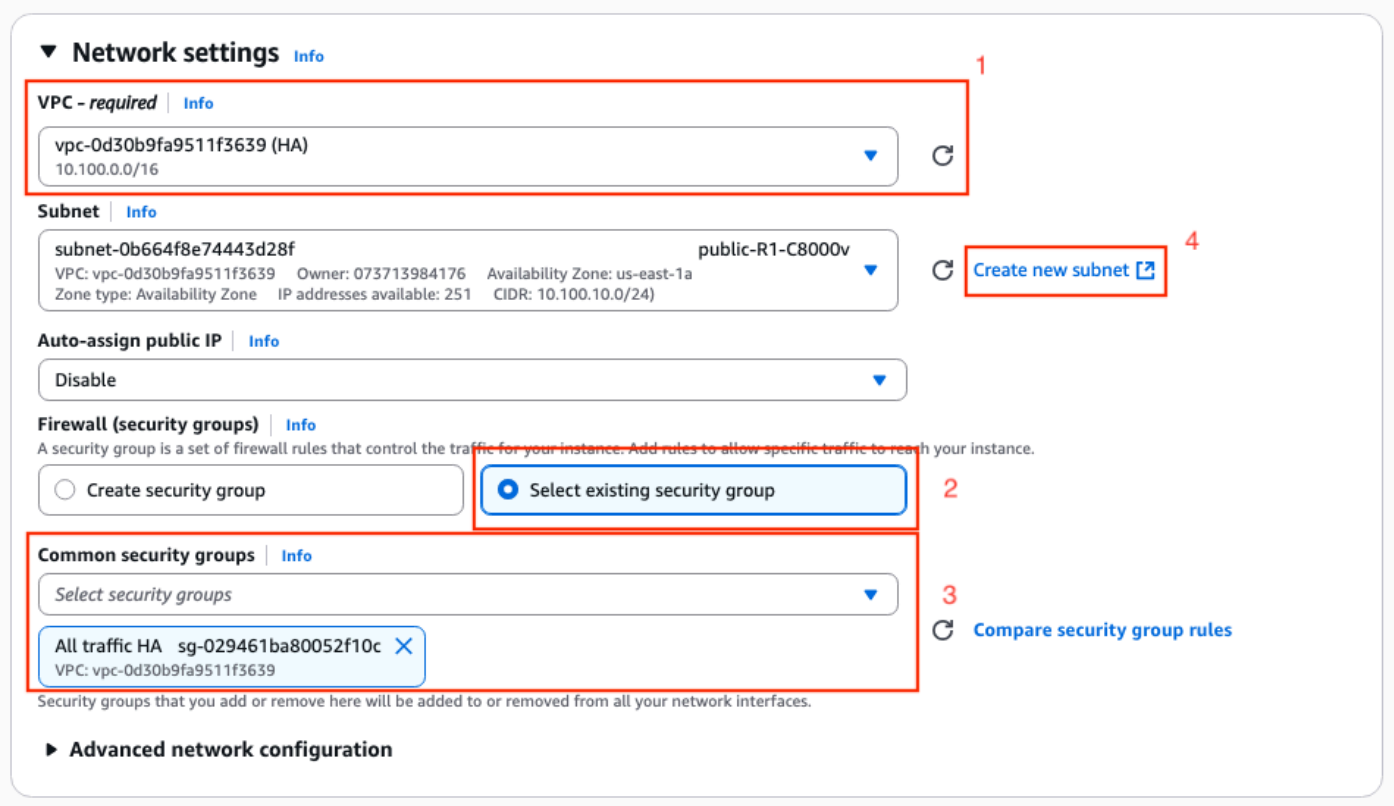
步驟6.2.建立和配置AMI的子網

在「Network Settings」部分中，按一下Edit。本節中的某些新選項現在可用：
1.為此工作選擇所需的VPC。在本示例中，選擇名為HA的VPC。

2.在「防火牆（安全組）」部分中，選擇「選擇現有安全組」。

3.一旦選擇了選項2,Common security groups選項即可用。篩選並選擇所需的安全組。在本例中，選擇了All traffic HA安全組。

4.（可選）如果沒有為這些裝置建立子網，請按一下Create new subnet。



Web瀏覽器上的新頁籤已開啟，可引導您進入建立子網部分：

1.從下拉選單中選擇此配置的相應VPC。

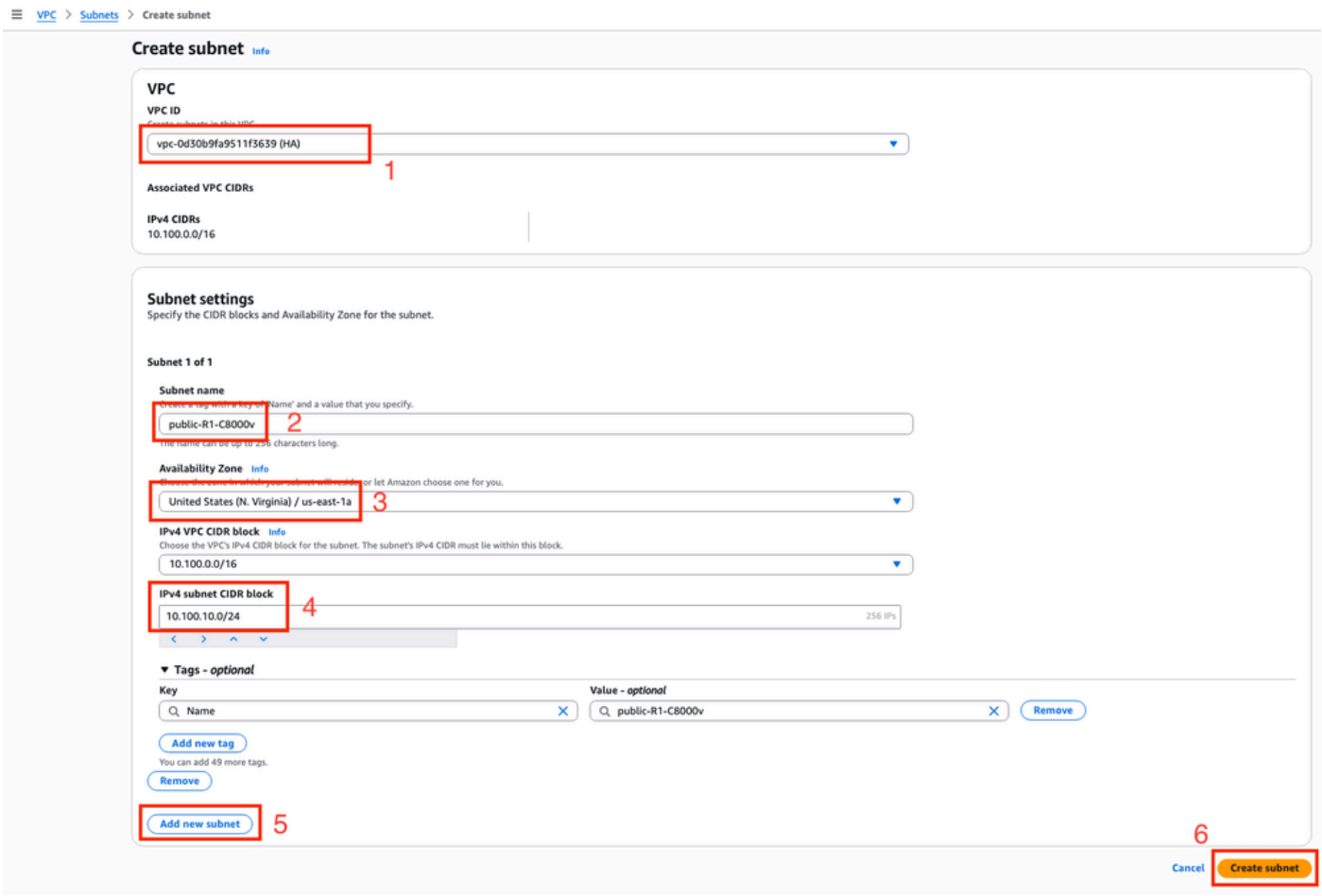
2.設定新子網的名稱。

3.定義此子網的可用性區域。（有關設定的詳細資訊，請參閱本文檔的拓撲部分）

4.設定屬於VPC CIDR塊的子網塊。

5.此外，通過按一下新增新子網部分並為每個子網重複從2到4的步驟，可以建立將要使用的所有子網。

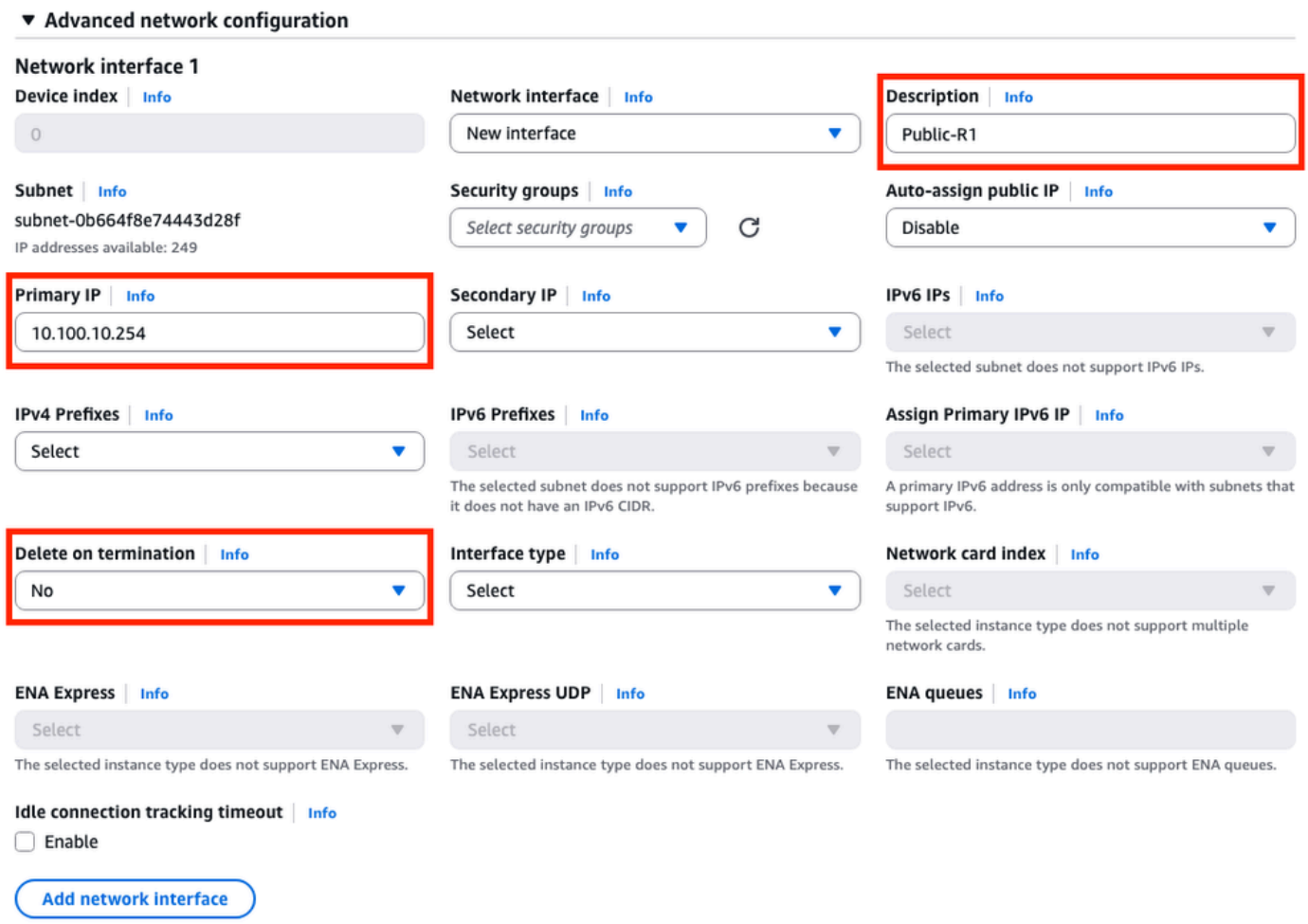
6.完成後，按一下Create subnet。導航到上一頁以繼續設定。



在Network Settings部分的Subnet子部分上，按一下Refresh圖示在下拉選單中獲取建立的子網。

步驟6.3.配置AMI介面

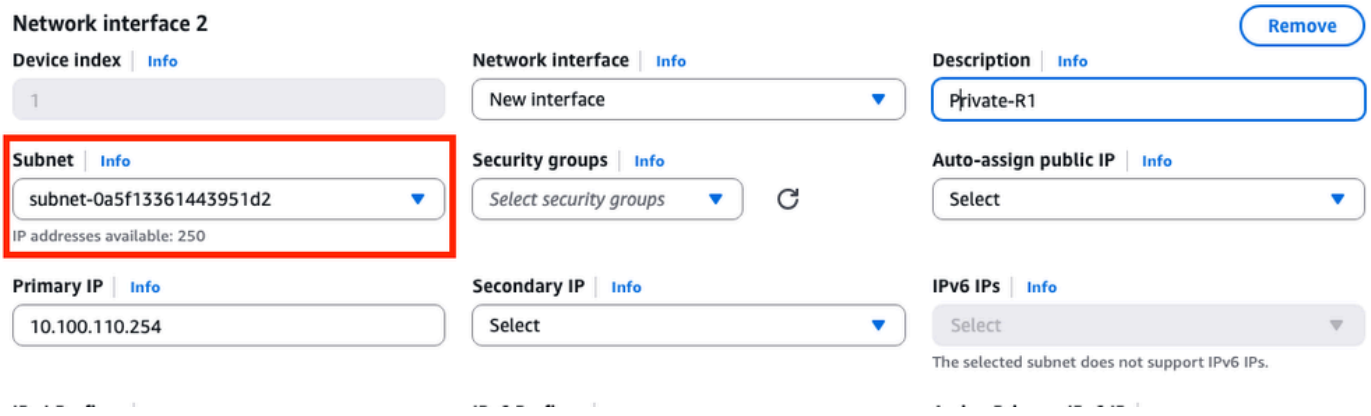
在Network Settings部分中，展開Advanced Network configuration子部分。將顯示以下選項：



在此選單上，設定Description、Primary IP、Delete on termination引數。
對於Primary IP引數，請使用除子網第一個可用地址以外的任何IP地址。這由AWS內部使用。

本示例中的終止時刪除(Delete on termination)引數設定為否(No)。但是，根據您的環境，可以將此選項設定為yes。

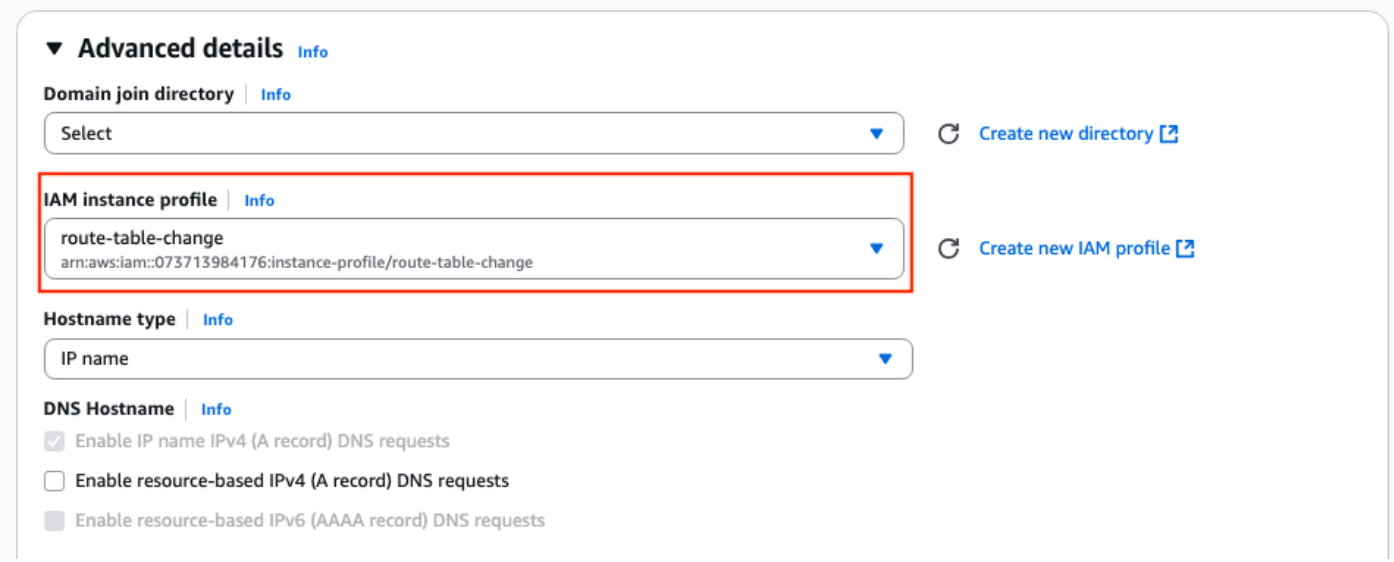
由於此拓撲，專用子網需要第二個介面。按一下「Add network interface」，系統會顯示此提示。但是，該介面提供了選擇子網這一次的選項：



按照在網路介面1上設定的方式設定所有引數後，繼續下一步。

步驟6.4.將IAM例項配置檔案設定為AMI

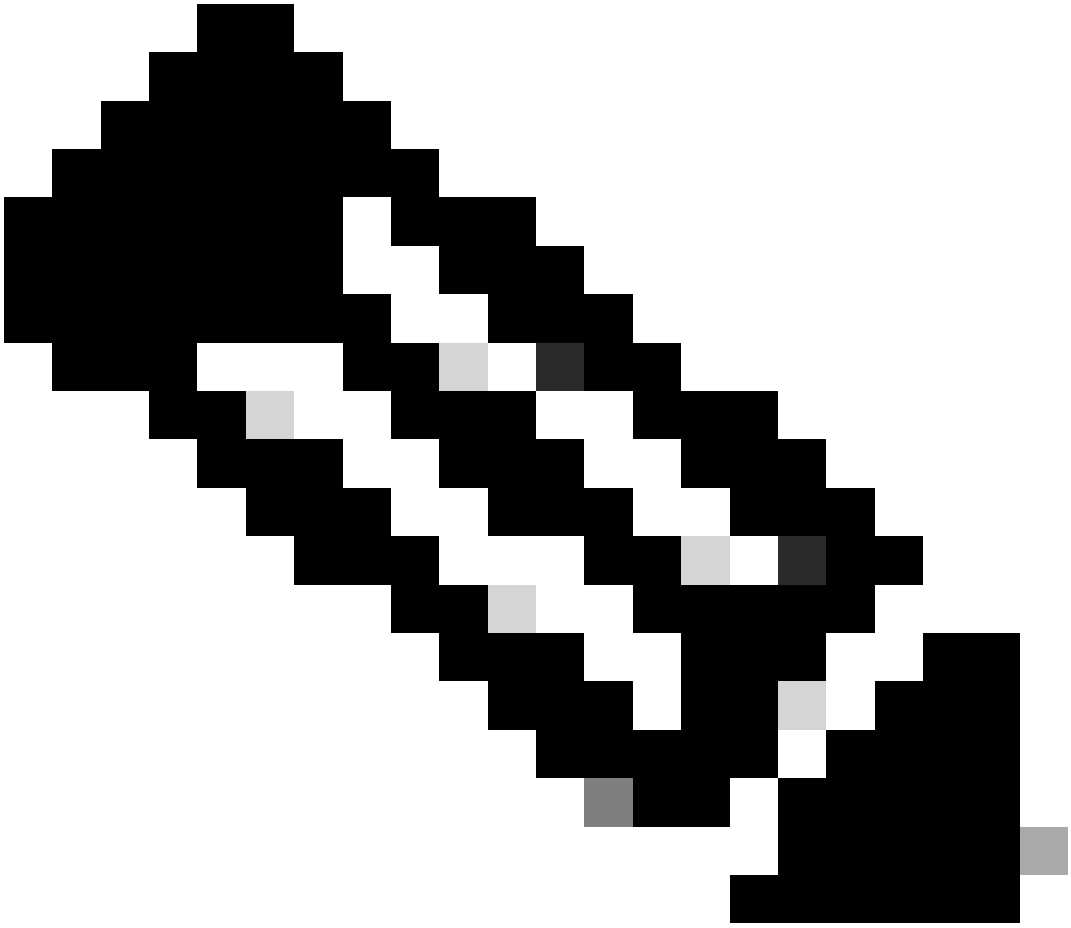
在Advanced details部分下，在IAM例項配置檔案引數中選擇創建的IAM角色：



步驟6.5。（可選）在AMI上設定憑證

在Advanced details部分下，導航到User data - optional部分，並在建立例項時應用此設定以設定使用者名稱和密碼：

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



附註：通過SSH連線到C8000v的AWS提供的使用者名稱可能會錯誤地列為root。如果需要，請將此項更改為ec2-user。

步驟6.6.完成例項配置

配置完所有內容後，按一下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.

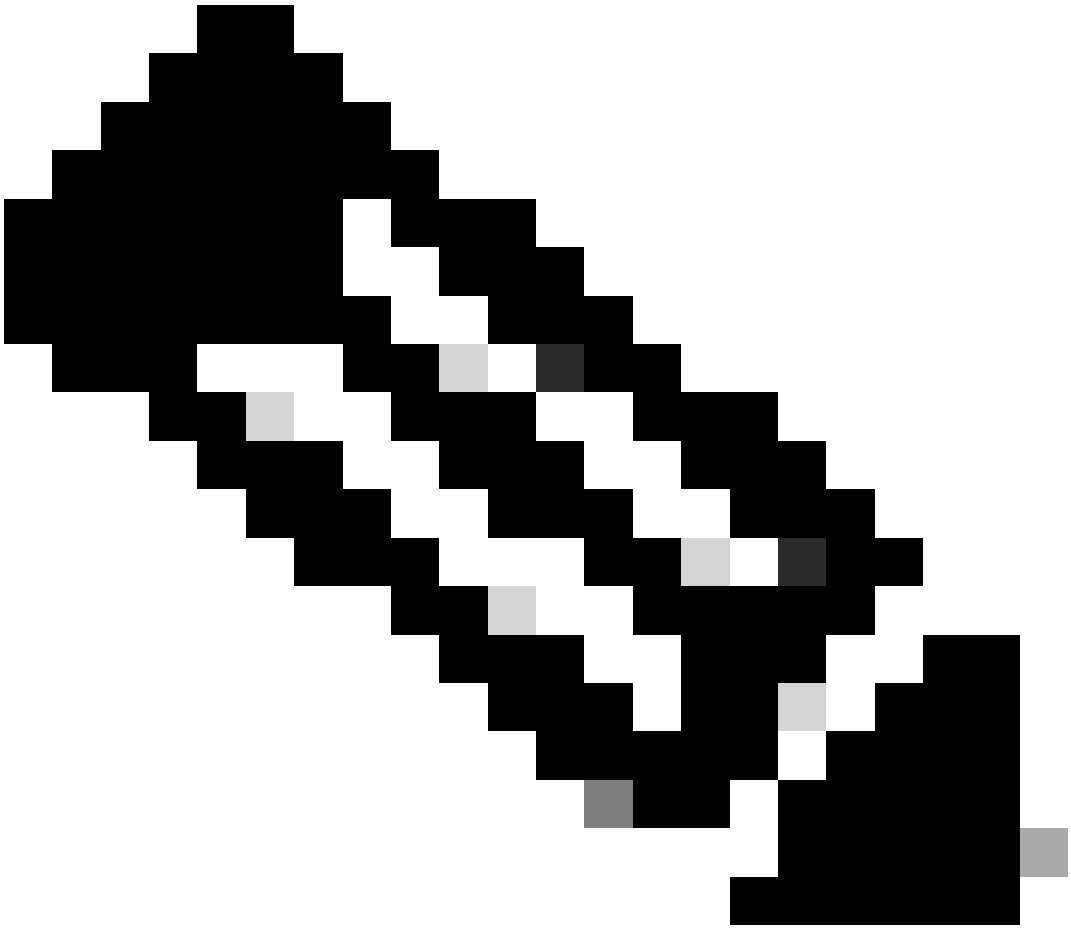
Cancel

Launch instance

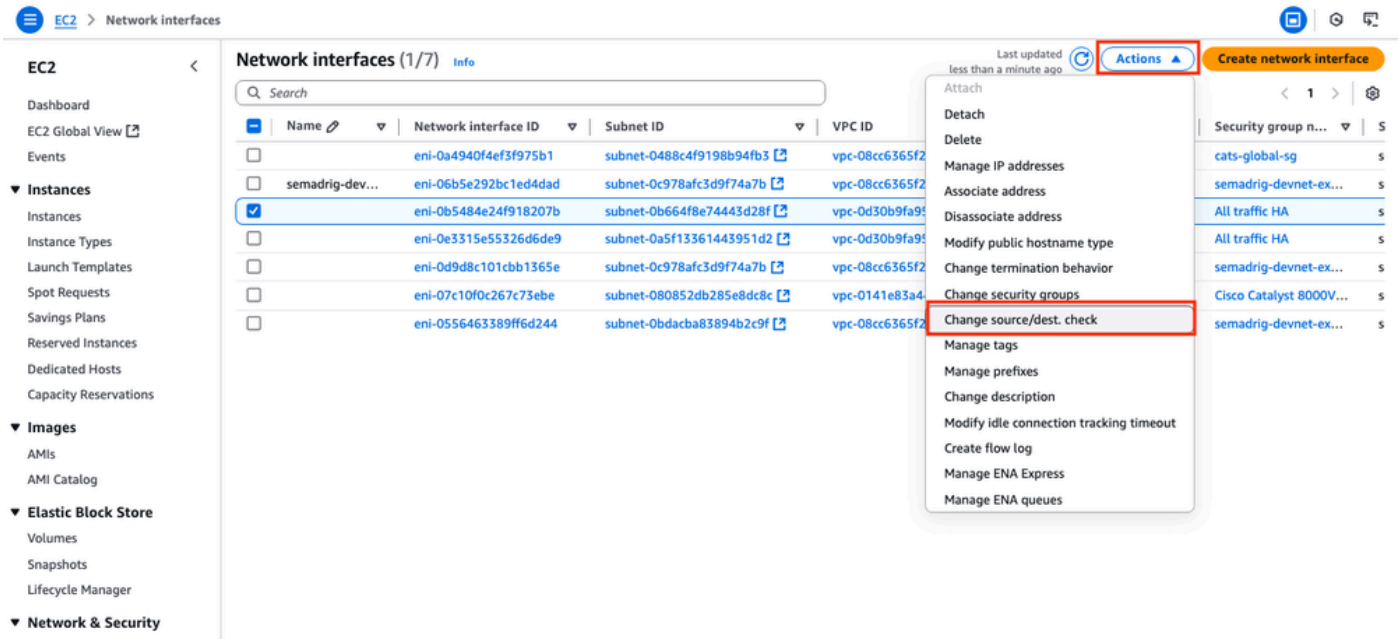
Preview code

步驟6.7.禁用ENI上的源/目標檢查

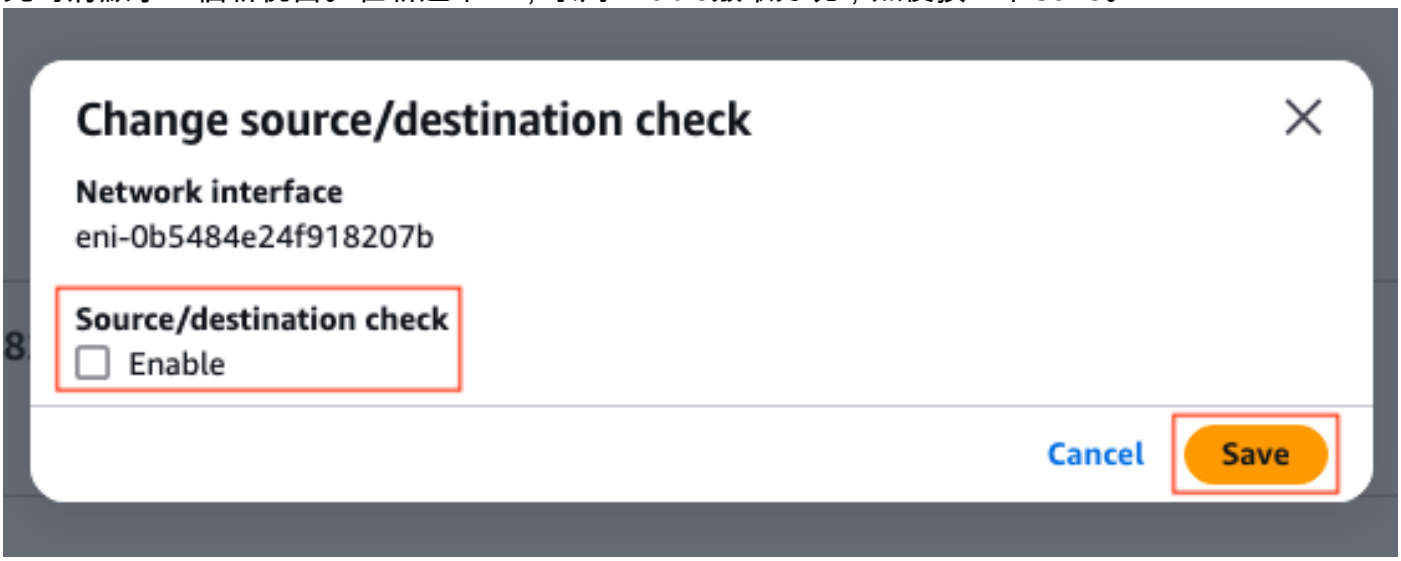
建立例項後，在AWS上禁用src/dst檢查功能以獲取相同子網中介面之間的連線。在EC2 Dashboard > Network & Security > Network interfaces部分，選擇ENI，然後按一下Actions >更改源/目標。檢查。



附註：必須逐一選擇ENI才能使用此選項。



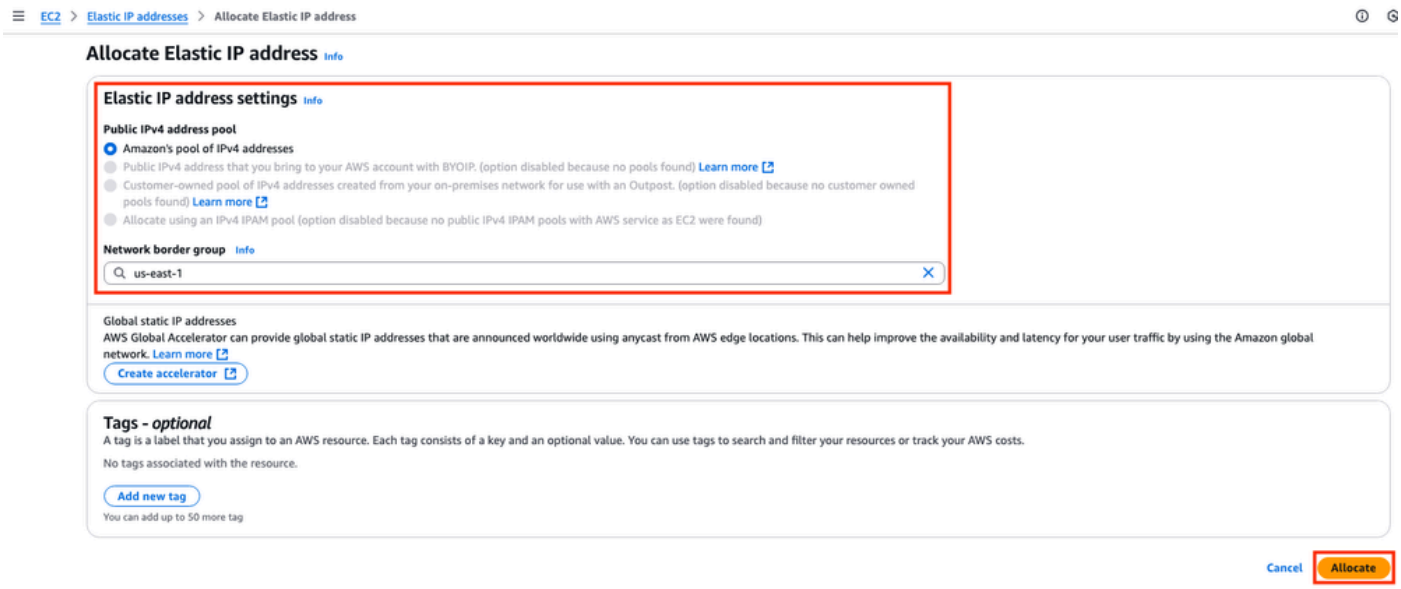
此時將顯示一個新視窗。在新選單上，禁用Enable覈取方塊，然後按一下Save。



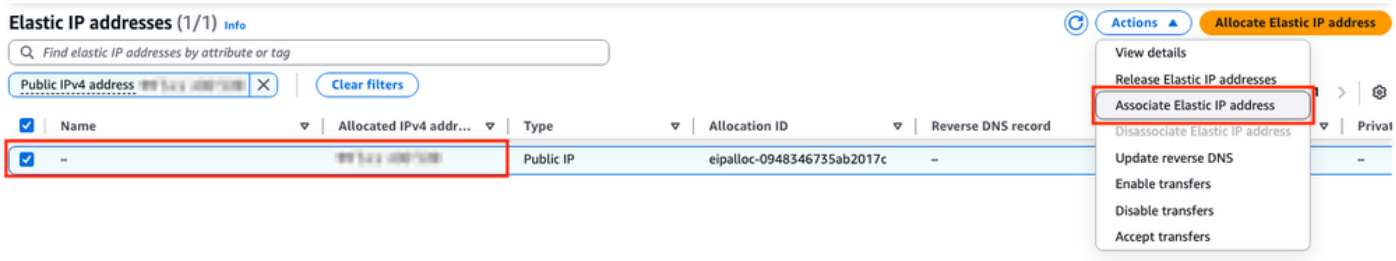
步驟6.8.建立彈性IP並將其關聯到例項的公共ENI

在EC2 Dashboard > Network & Security > Elastic IPs 部分，按一下Allocate Elastic IP address。

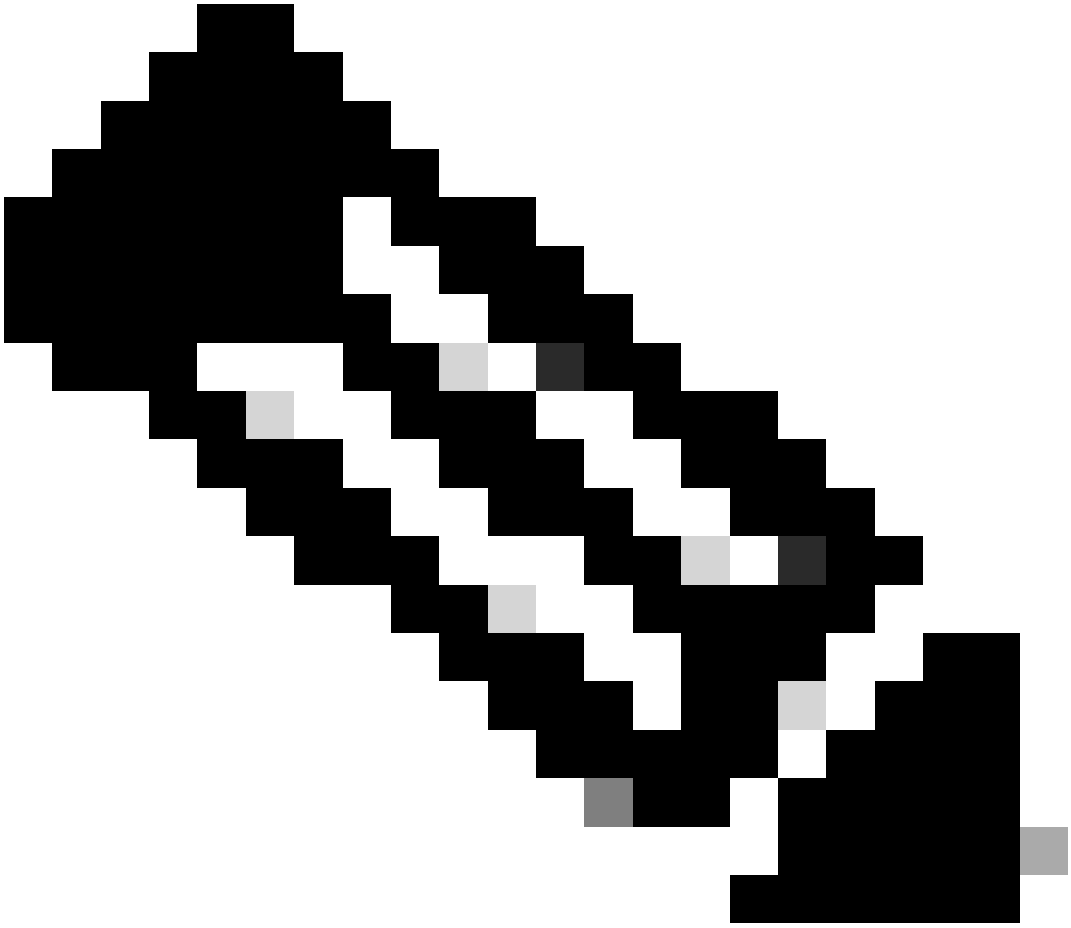
該頁面引導您進入另一個部分。在本例中，同時選擇了Amazon pool of IPv4 addresses選項和可用區域us-east-1。完成後，按一下Allocate。



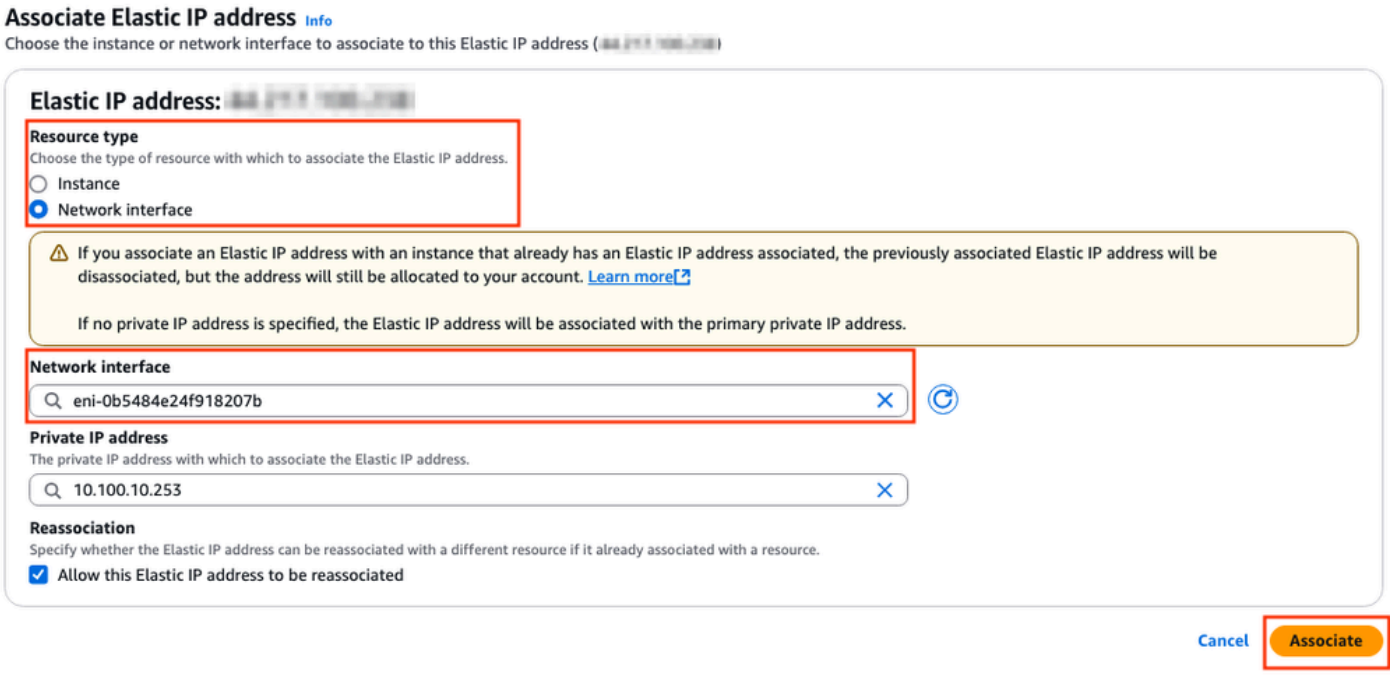
建立IP地址時，將IP地址分配給例項的公用介面。在EC2 Dashboard > Network & Security > Elastic IPs 部分，按一下Actions > Associate Elastic IP address。



在此新部分中，選擇Network interface選項並查詢相應介面的公共ENI。關聯相應的公用IP地址，然後按一下Associate。



附註：要獲取正確的ENI ID，請導航至EC2 Dashboard > Instances部分。然後選擇例項並選中Networking部分。查詢公共介面的IP地址以在同一行上獲取ENI值。



步驟7.重複步驟6，為HA建立第二個C8000v例項

請參考本文檔的拓撲部分，獲取每個介面的相應資訊，並重複從6.1到6.6的相同步驟。

步驟8.重複步驟6，從AMI應用商店建立VM(Linux/Windows)

在本示例中，從AMI Marketplace中選擇Ubuntu伺服器22.04.5 LTS作為內部主機。

預設情況下，會為公共介面建立ens5。在本示例中，為專用子網建立第二個介面（裝置上的ens6）。

<#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
```

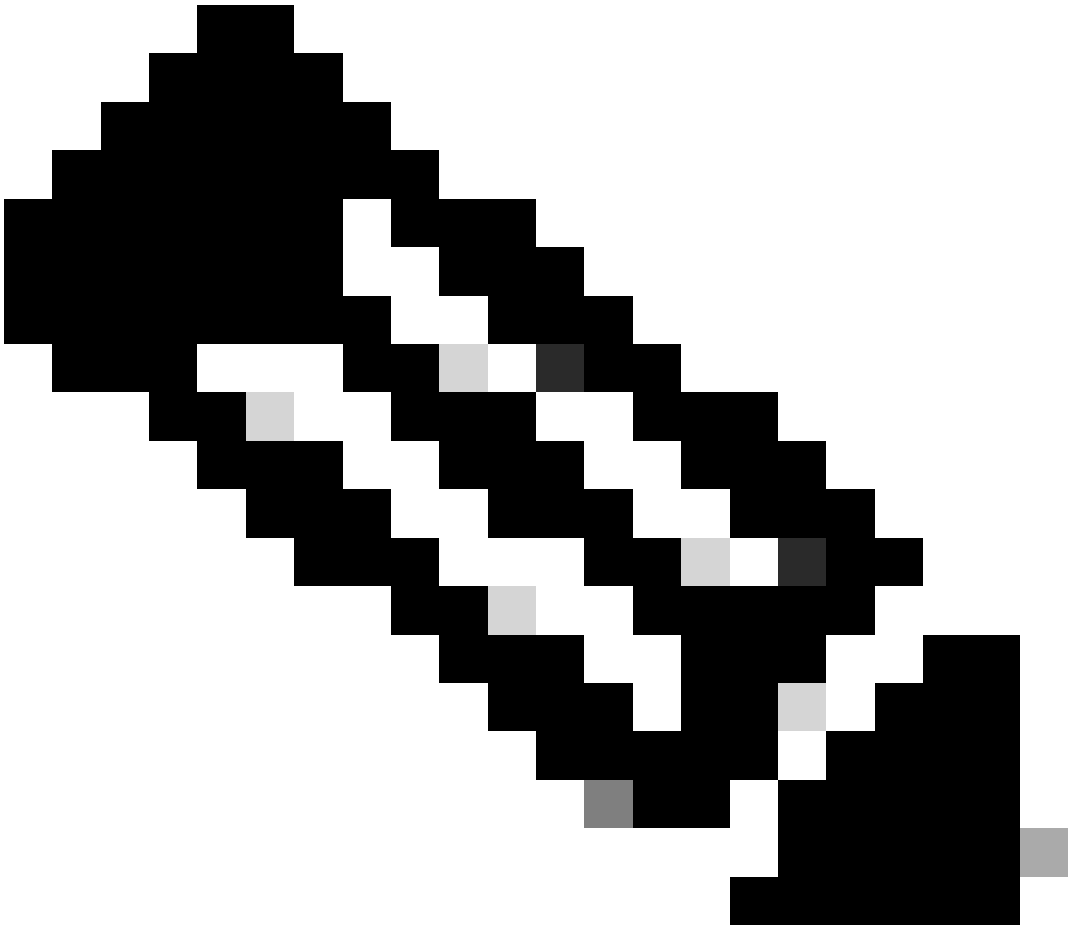
10.100.30.254

```
 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>
```

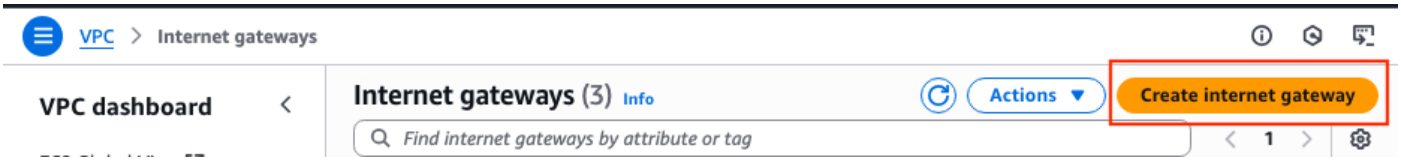
```
ether 02:3b:7e:ad:db:e5 txqueuelen 1000 (Ethernet)
RX packets 119 bytes 16831 (16.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 133 bytes 13816 (13.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



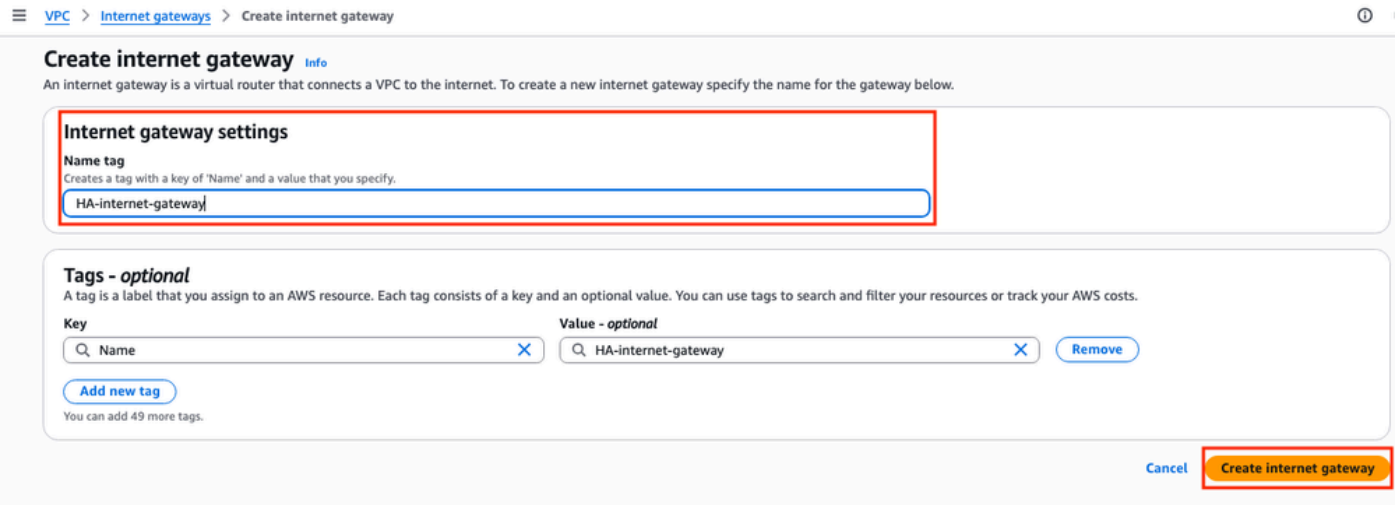
附註：如果對介面進行任何更改，請關閉介面或重新載入VM以應用這些更改。

步驟9.為VPC建立和配置Internet網關(IGW)

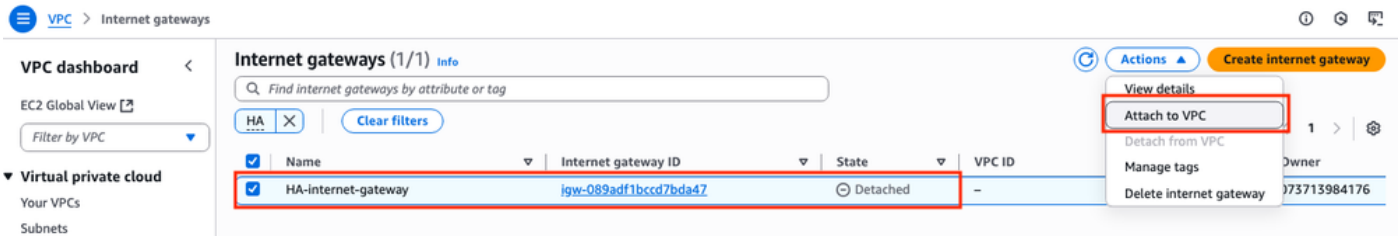
在VPC Dashboard > Virtual private cloud > Internet gateways部分，按一下Create internet gateway。



在此新部分中，為此網關建立**name**標籤，然後按一下**Create internet gateway**。

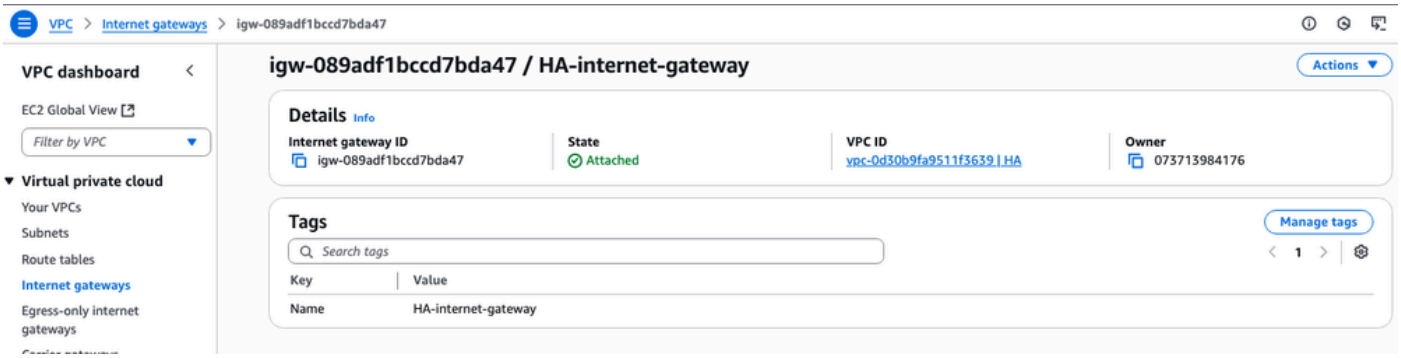


建立IGW後，將其連線到相應的VPC。導航到**VPC Dashboard > Virtual Private Cloud > Internet Gateway**部分，然後選擇相應的IGW。按一下**Actions > Attach to VPC**。



在此新部分中，選擇名為**HA**的VPC。對於此示例，請按一下**Attach internet gateway**。

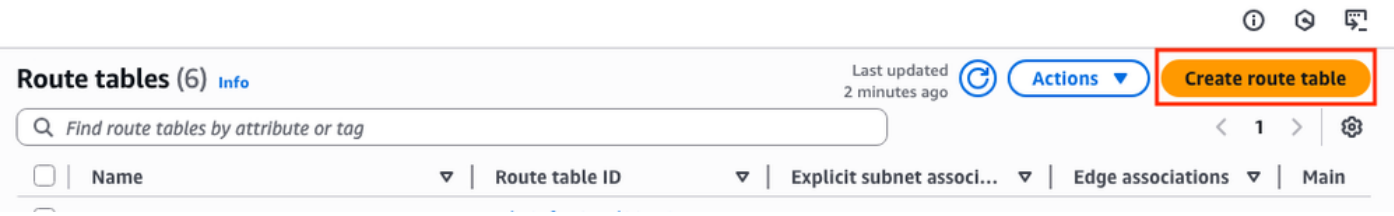
IGW必須如圖所示指示「Attached」（連線）狀態：



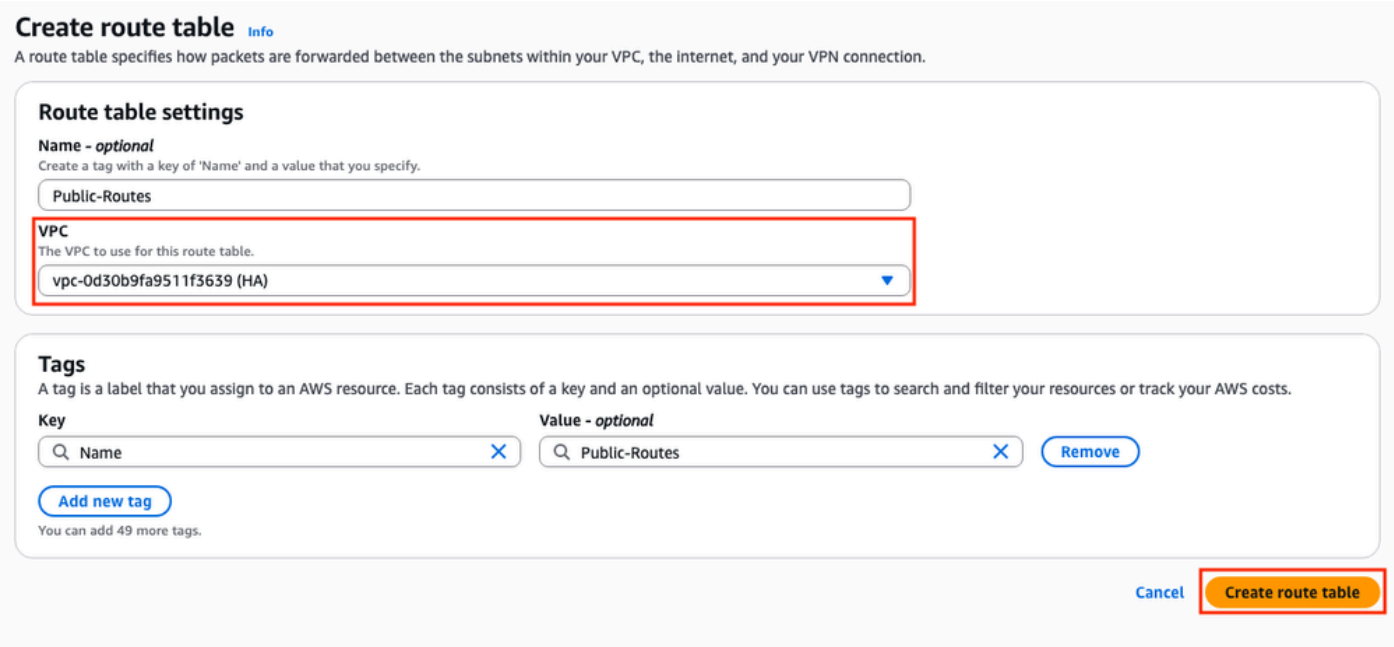
步驟10.在AWS上建立並配置公共和專用子網的路由表

步驟10.1.建立和配置公共路由表

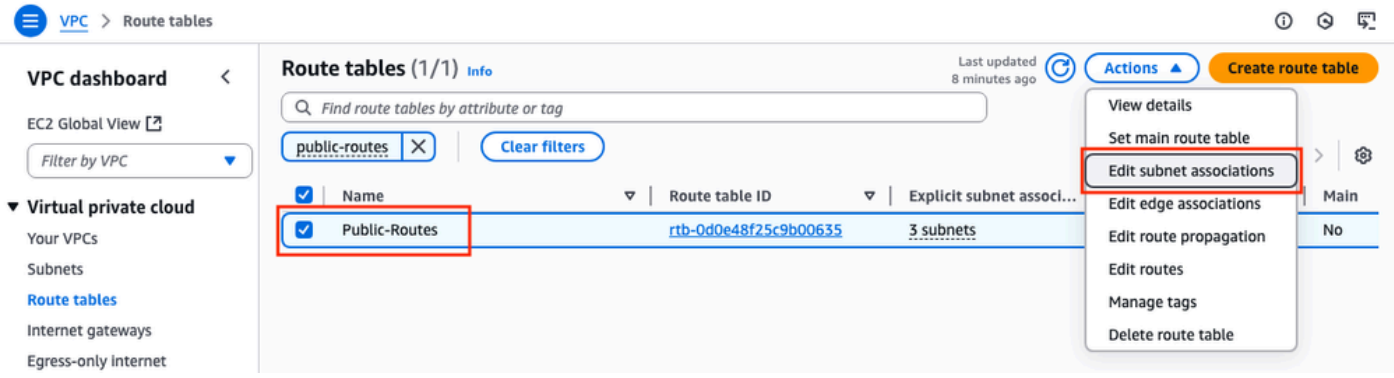
為了在此拓撲上建立HA，請將所有公用和專用子網關聯到其相應的路由表中。在VPC Dashboard > Virtual Private Cloud > Route tables部分中，按一下Create route table。



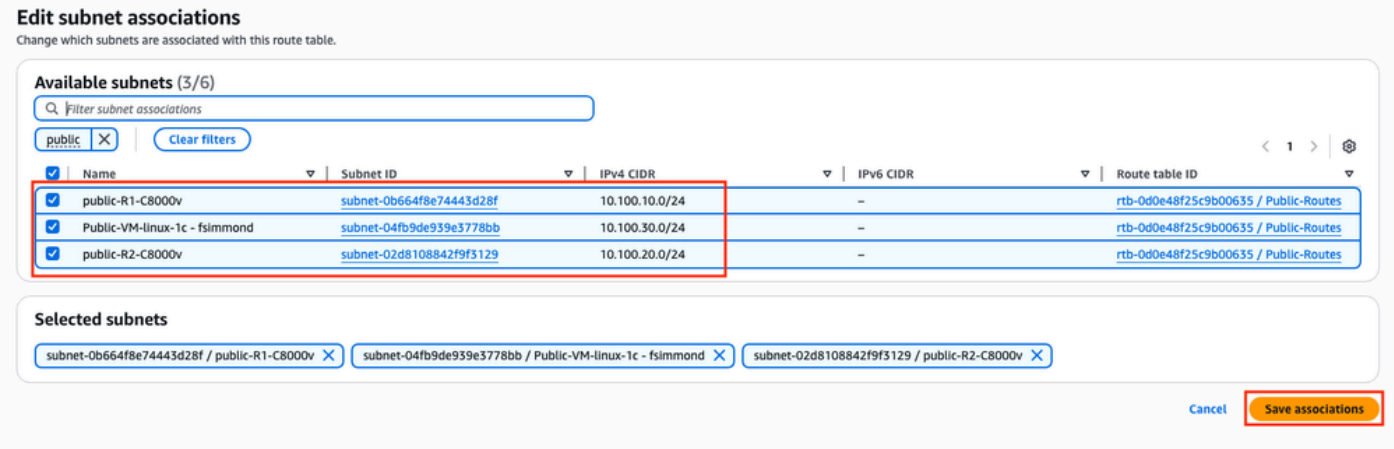
在新區中，為此拓撲選擇對應的VPC。選中後，按一下Create route table。



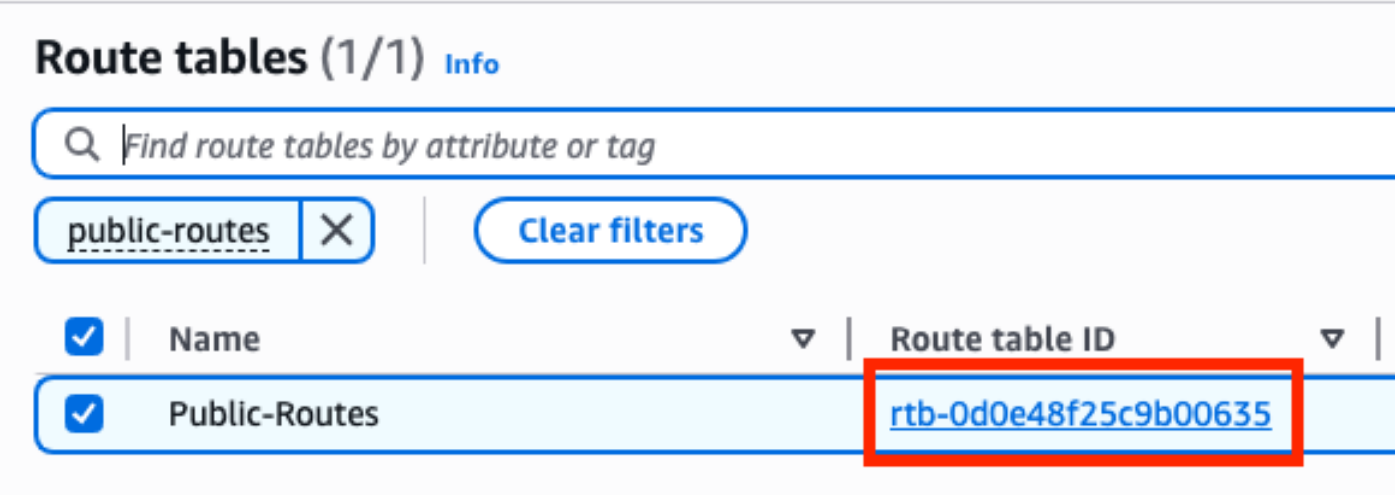
在Route tables部分中，選擇created表，然後按一下Actions > Edit Subnet associations。



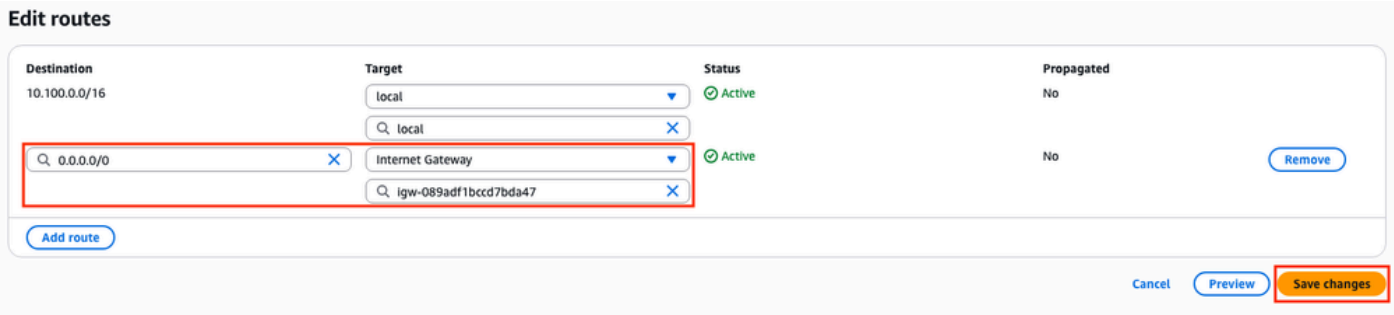
然後，選擇對應的子網，然後按一下Save associations。



關聯子網後，按一下Route table ID超連結為表新增正確的路由。然後，按一下Edit Routes:

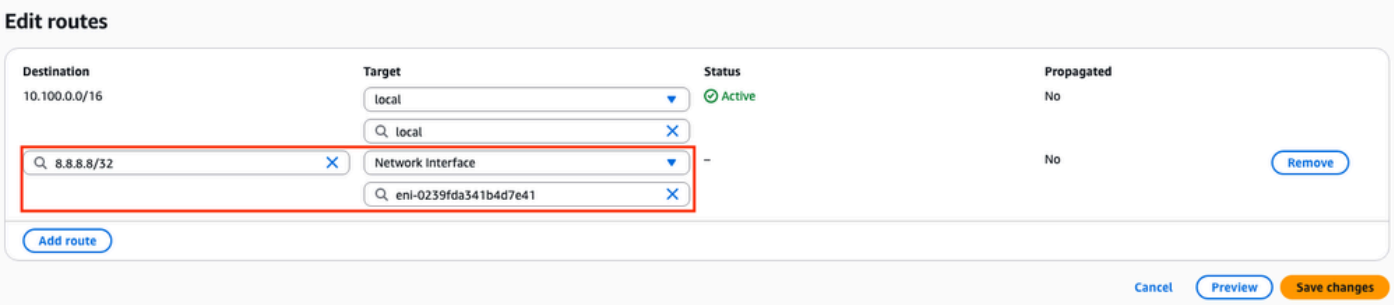


若要存取Internet，請按一下「Add route」，並將此公共路由表與步驟9中使用這些引數建立的IGW連結在一起。選中後，按一下Save changes:



步驟10.2.建立和配置專用路由表

建立公共路由表後，除了在其路由上新增Internet網關外，還要為專用路由和專用子網複製步驟10。在本例中，路由表如下所示，因為8.8.8.8的流量必須通過本例中的專用子網：



步驟11.檢查並配置基本網路配置、網路地址轉換(NAT)、具有BFD的GRE隧道和路由協定

在AWS上準備好例項及其路由配置後，請配置裝置：

C8000v R1配置：

```
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
```

C8000v R2配置：

```
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
```

步驟12.配置高可用性(Cisco IOS® XE Denali 16.3.1a或更高版本)

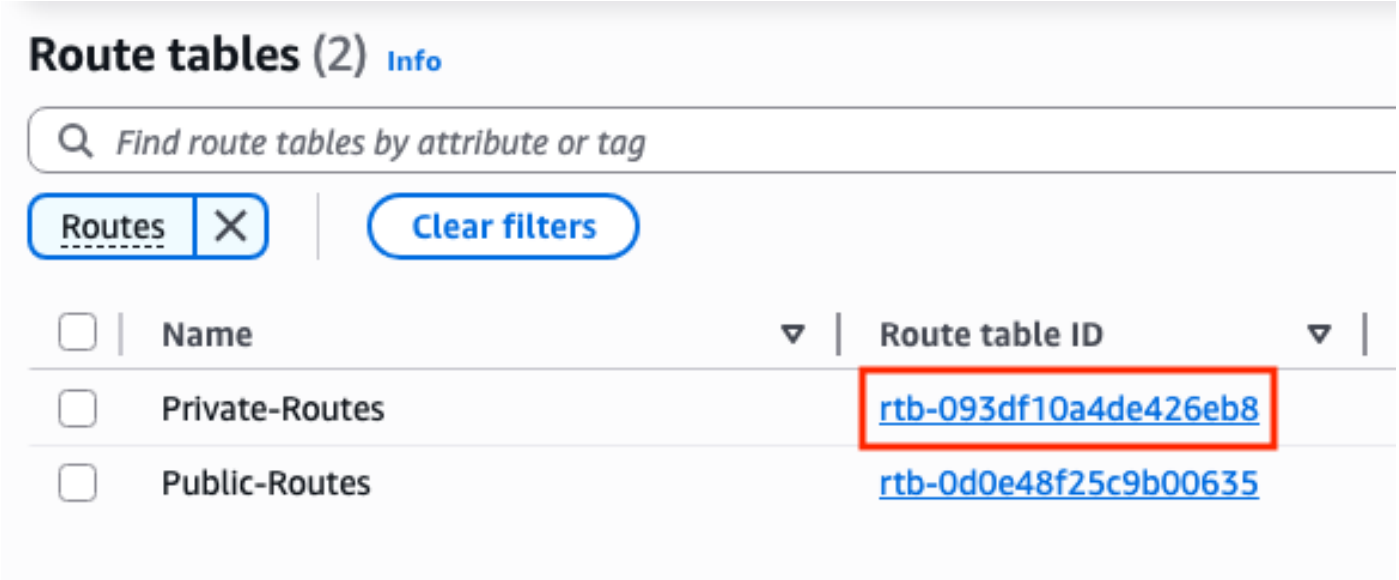
現在設定了VM之間的冗餘和連線，請配置HA設定以定義路由更改。設定Route-table-id、Network-interface-id和CIDR值，這些值必須在AWS HA錯誤（例如BFD對等體關閉）後設定。

```
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>
```

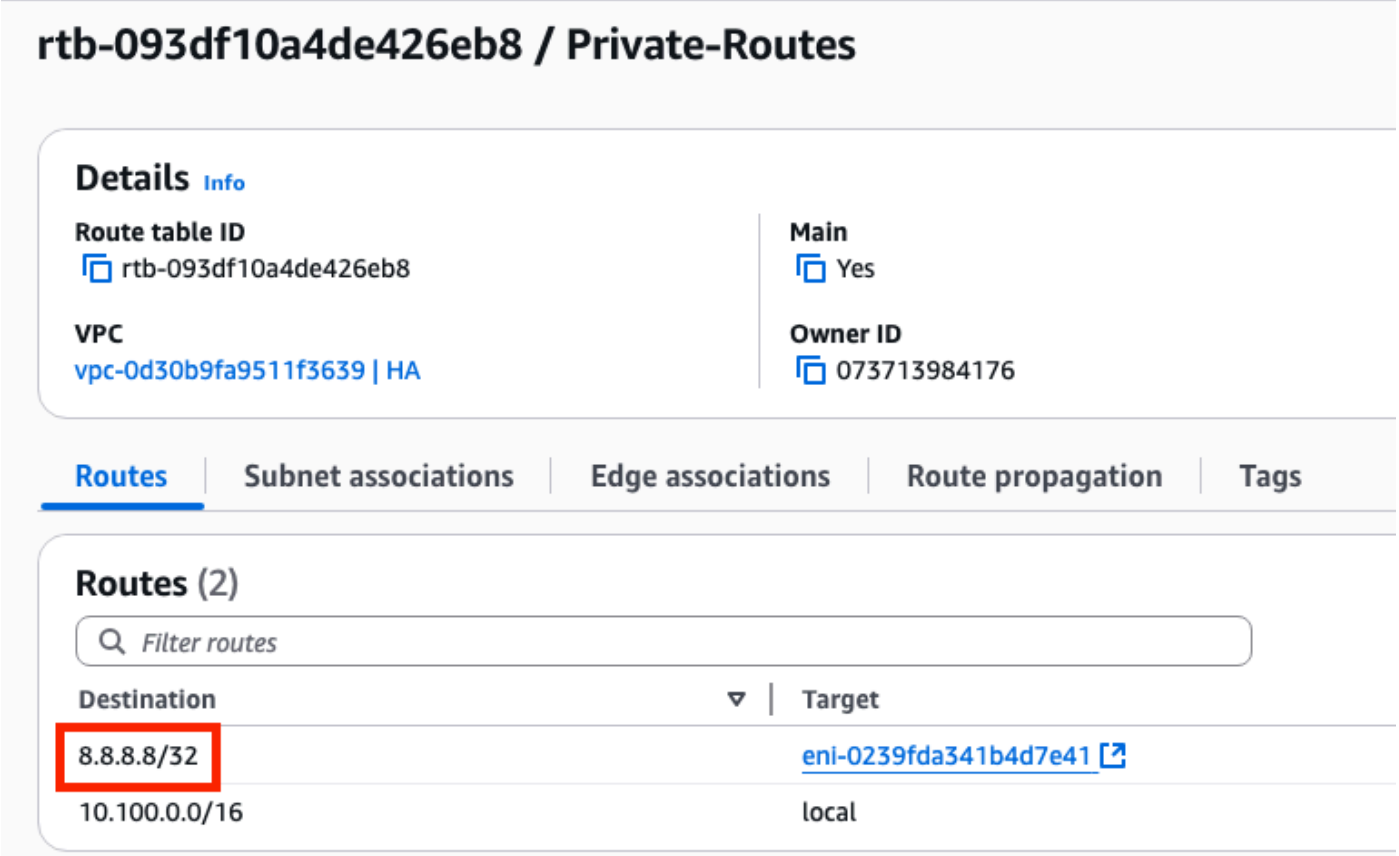
bfd peer引數與通道對等體IP地址相關。可以使用show bfd neighbor輸出檢查此情況：

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

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

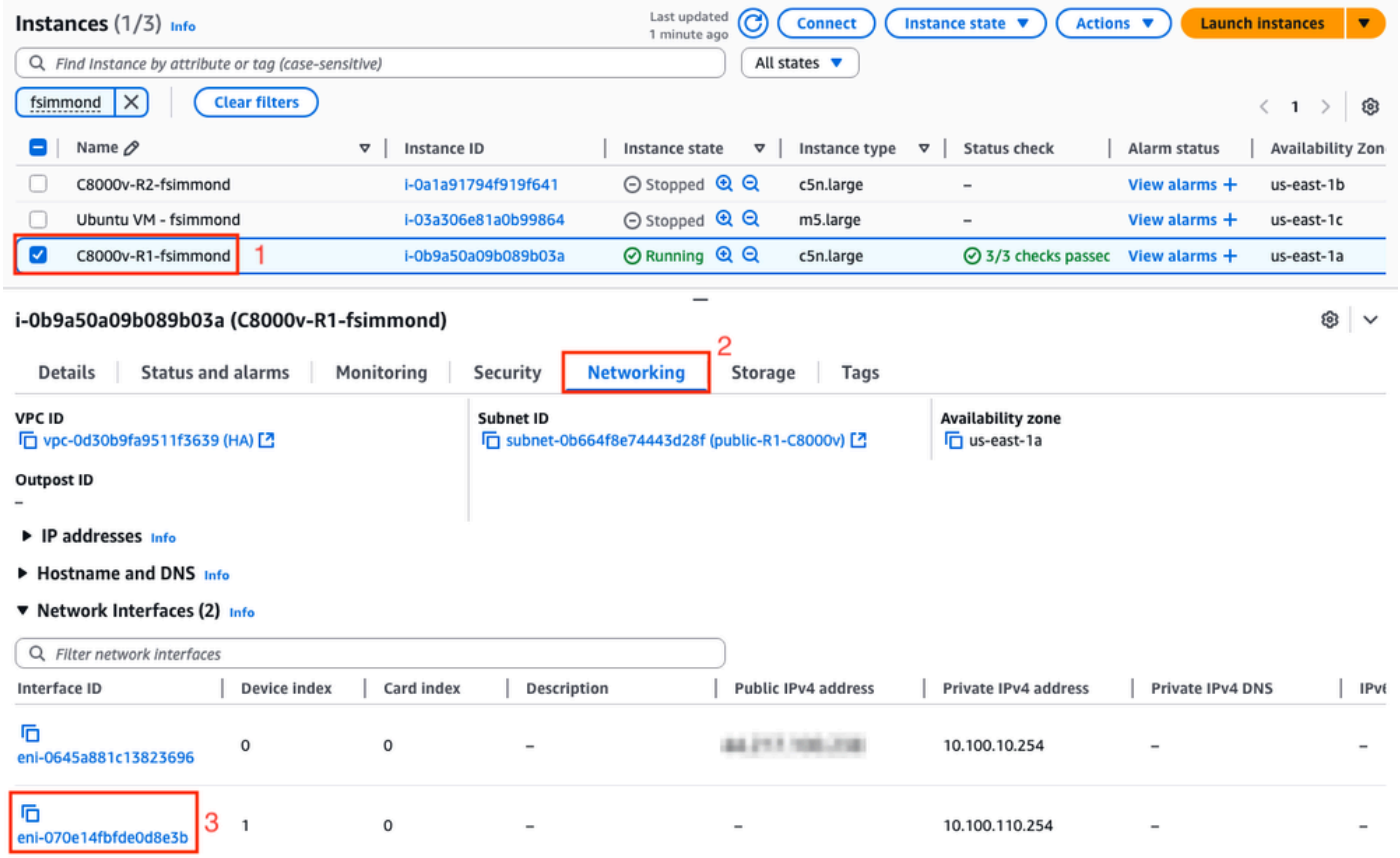
route-table引數與位於VPC Dashboard > Virtual Private Cloud > Route Tables部分中的專用路由表ID相關。複製相應的路由表ID。



cidr ip引數與私有路由表中新增的路由字首相關（在步驟10.2中建立的路由）：



eni引數與所配置的例項的相應專用介面的ENI ID相關。在本示例中，使用例項的GigabitEthernet2介面的ENI ID:



region引數與VPC所在區域的AWS文檔中的代碼名稱相關。在本示例中，使用us-east-1區域。

但是，此清單可以更改或增大。要查詢最新更新，請訪[問AmazonRegion and Availability Zonesdocument。

考慮到所有這些資訊，以下是VPC中每台路由器的配置示例：

C8000v R1的配置示例：

```
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
```

C8000v R2的配置示例：

```
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
```

驗證

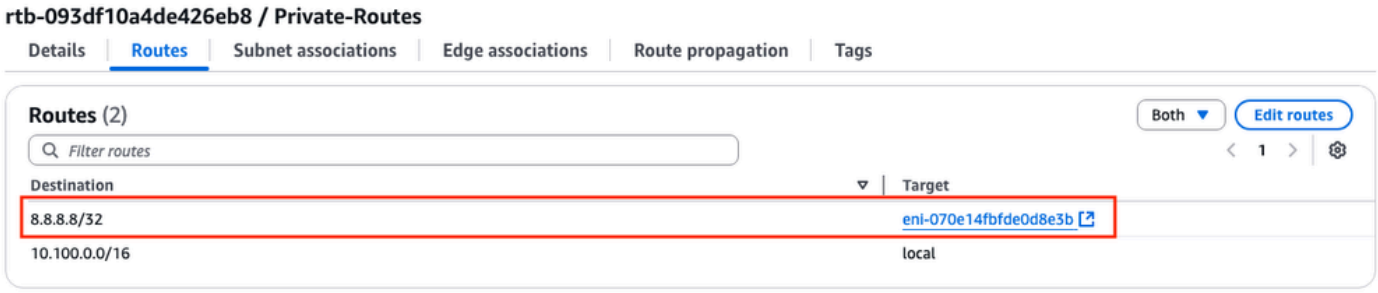
1.檢查C8000v R1例項狀態。確認通道和雲冗餘已啟動且正在運行。

```
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.從路由器後面的主機VM連續對8.8.8.8執行ping操作。請確保ping正在通過專用介面：

```
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.開啟AWS WebGUI並檢查routing 表的狀態。當前ENI屬於R1例項的專用介面：



4.通過關閉R1例項上的Tunnel1介面來模擬HA故障切換事件來觸發路由更改：

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

5.再次檢視AWS上的route 表,ENI ID已更改為R2專用介面ENI ID:

疑難排解

以下是重新建立部署時經常遺忘/配置錯誤的大部分常見問題：

- 確保資源相關聯。建立VPC、子網、介面、路由表等時，其中許多介面不會自動相互關聯。他們彼此不瞭解。
- 確保Elastic IP和任何私有IP與正確的介面、正確的子網、新增到正確的路由表、連線到正確的路由器以及與IAM角色和安全組連結的正確的VPC和區域相關聯。

- 禁用每個ENI的源/目標檢查。
  如果您已經檢查了本節中討論的所有點，但問題仍然存在，請收集這些輸出，測試HA故障切換（如果可能），然後使用Cisco TAC建立案例：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。