Amazon AWS上的CSR1000v HA冗餘部署指南

目錄

簡介

本文檔介紹如何在Amazon AWS雲上部署CSR1000v路由器以實現高可用性的配置指南。其目的是讓使用者實際瞭解HA並有能力部署一個功能完整的測試平台。

有關AWS和HA的更多深入背景，*請參閱*一節。

必要條件

需求

思科建議您瞭解以下主題：

- Amazon AWS賬戶
- 同一區域中有2個CSR1000v和1個Linux/Windows AMI
- Cisco IOS-XE® 16.5到16.9版支援HA版本1。 從16.11及更高版本開始使用HA版本3。

採用元件

本檔案中的資訊是根據Cisco IOS-XE® Denali 16.7.1。

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。

目標

在多可用區環境中，模擬從專用資料中心(VM)到Internet的連續流量。模擬HA容錯移轉，並觀察HA是否成功，因為路由表已確認從CSRHA到CSRHA1的專用介面的流量。

拓撲

在配置開始之前，必須完全瞭解拓撲和設計。這有助於排除以後可能出現的問題。

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：

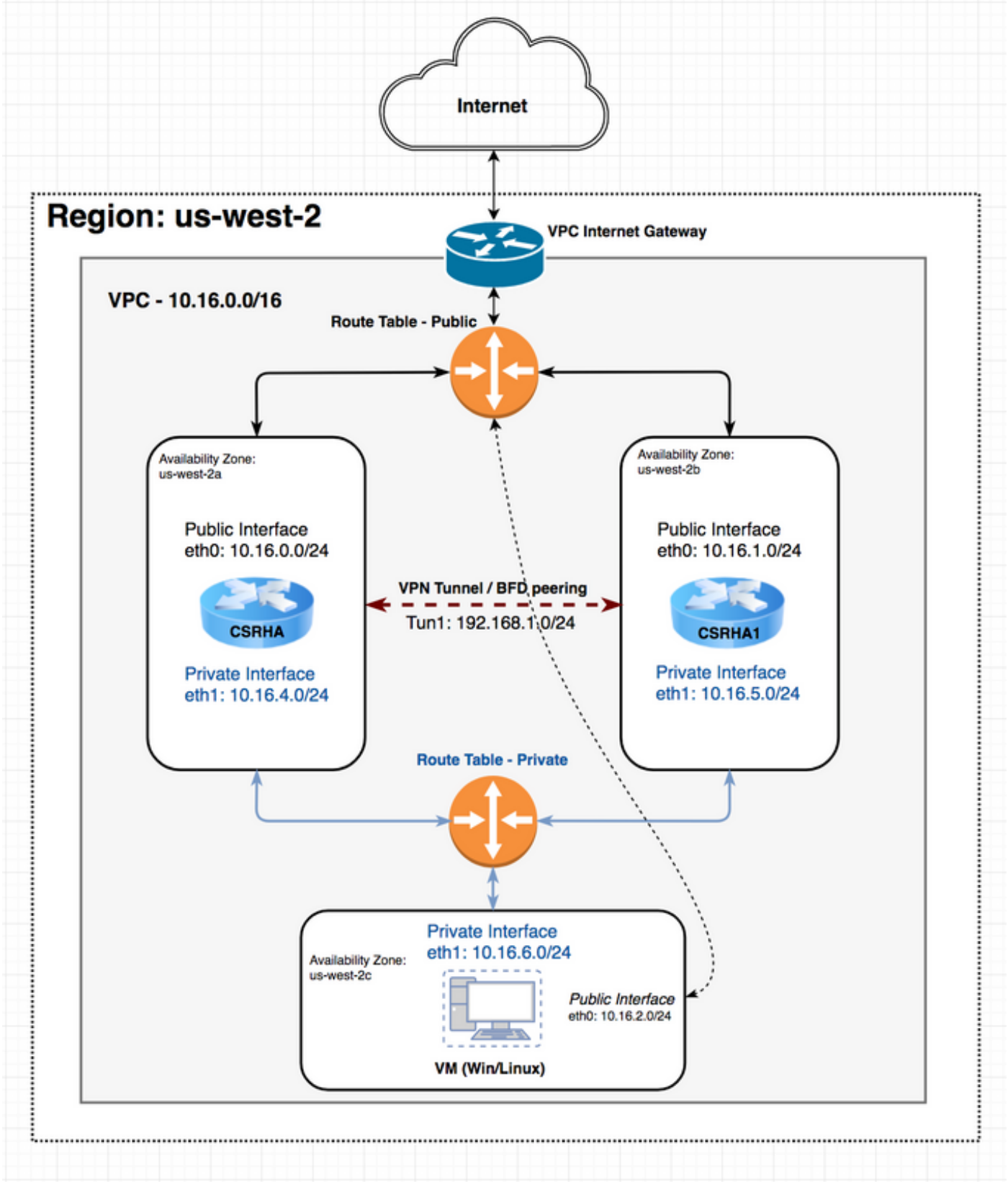
- 1x — 區域
- 1個 — VPC
- 3x — 可用區
- 6x — 網路介面/子網（3x公共介面/3x專用介面）
- 2x — 路由表（公用和專用）
- 2x - CSR1000v路由器(Cisco IOS-XE® Denali 16.3.1a或更高版本)
- 1x — 虛擬機器(Linux/Windows)

一個HA對中有2台CSR1000v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，通過上的公共介面啟用了Internet訪問，以便您可以訪問和配置VM。通常，所有正常流量都應通過專用路由表。

在CSRHA 8.8.8.8上對VM的→用介面Ping→專用→由表，以進行流量模擬。在故障轉移場景中，觀察私有路由表已將路由交換為指向CSRHA1的私有介面。

網路圖表



技術

RTB — 路由表ID。

CIDR — 要在路由表中更新的路由的目標地址。

ENI — 將流量路由到的CSR 1000v gigabit介面的網路介面ID。
例如，如果CSRHA發生故障，則CSRHA1會接管並更新AWS路由表中的路由，使其指向自己的

ENI。

區域 — CSR 1000v的AWS區域。

限制

- 對於專用子網，請勿使用IP地址10.0.3.0/24，該地址在Cisco CSR 1000v內部使用，以實現高可用性。Cisco CSR 1000v需要具有公共網際網路訪問能力，才能進行更改AWS路由表的REST API呼叫。
- 請勿將CSR1000v的gig1介面放在VRF中。 HA無法正常工作。

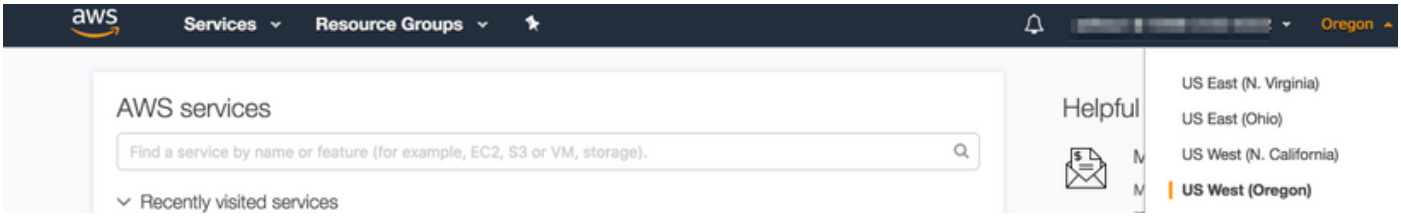
組態

一般配置流程是從最頂層的功能（區域/VPC）開始，然後向下移動到最具體的功能（介面/子網）。 但是，沒有特定的配置順序。開始之前，首先瞭解拓撲非常重要。

提示：為您的所有設定（VPC、介面、子網、路由表等）指定名稱。

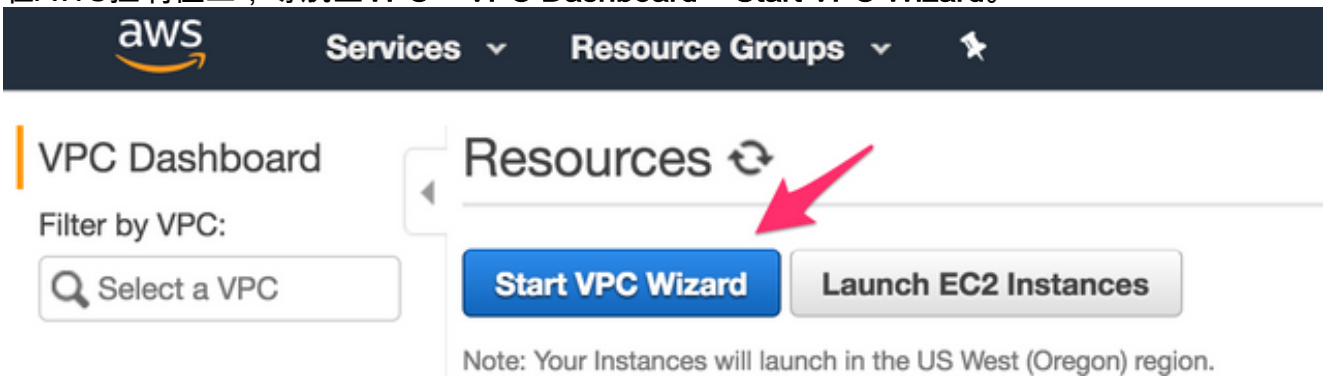
步驟1.選擇區域。

本示例使用US West(Oregon)。

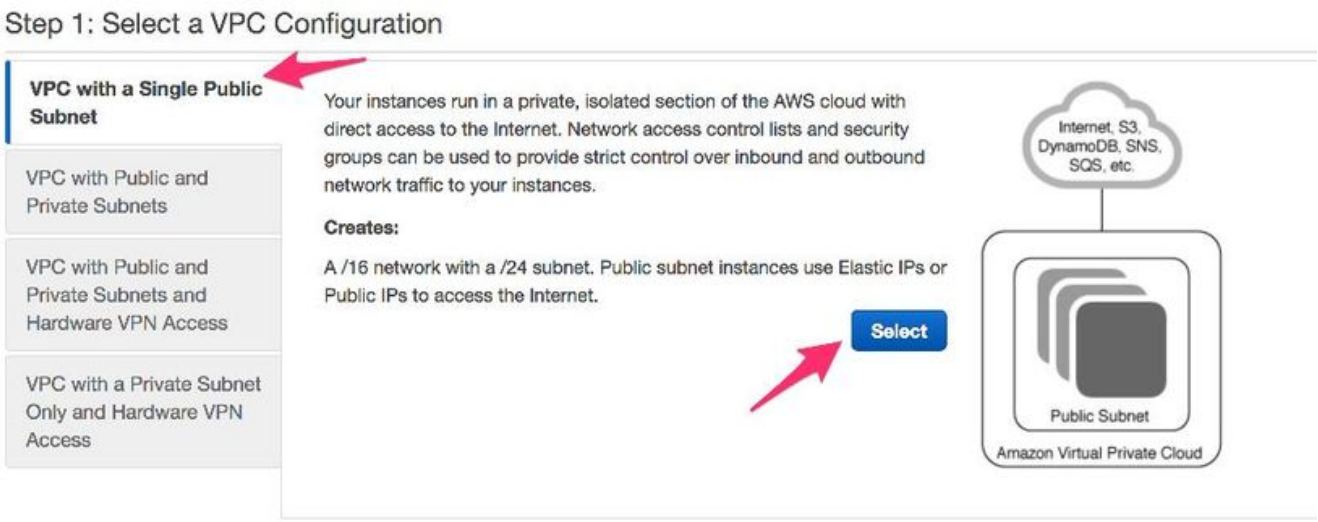


步驟2.建立VPC。

1. 在AWS控制檯上，導航至**VPC > VPC Dashboard > Start VPC Wizard**。

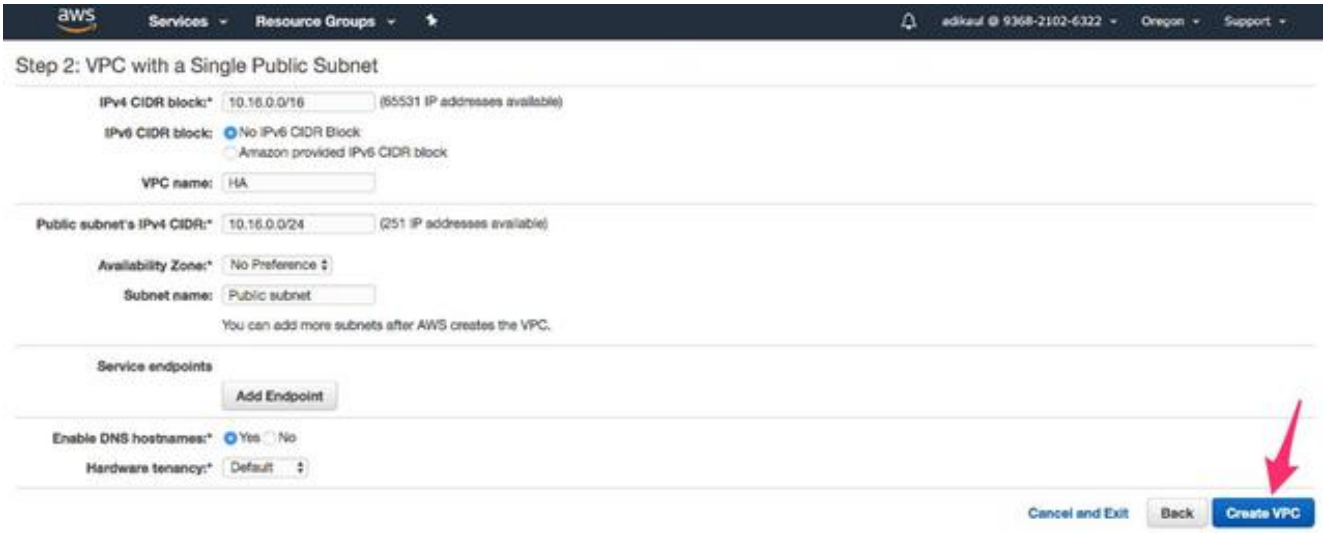


2. 選擇具有單個公共子網的VPC。

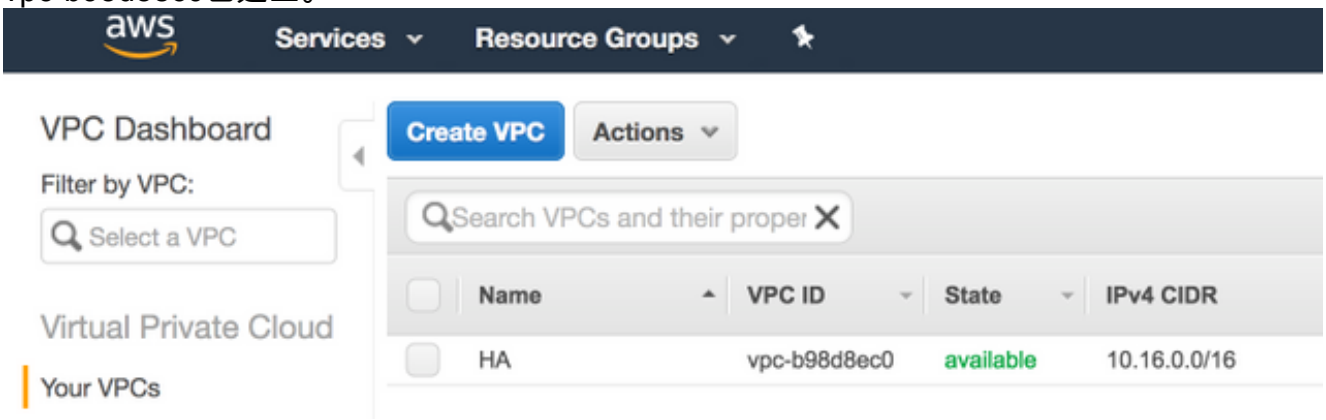


3. 建立VPC時，會為您分配一個/16網路，供您隨意使用。

4. 系統還會為您分配一個/24公共子網。公共子網例項使用彈性IP或公共IP讓您的裝置訪問Internet。



5. vpc-b98d8ec0已建立。



步驟3.為VPC建立安全組。

安全組類似於允許或拒絕流量的ACL。

1. 在Security下，點選**Security Groups**和**Create your Security Group**（建立與上面建立的名為HA的VPC相關的安全組）。

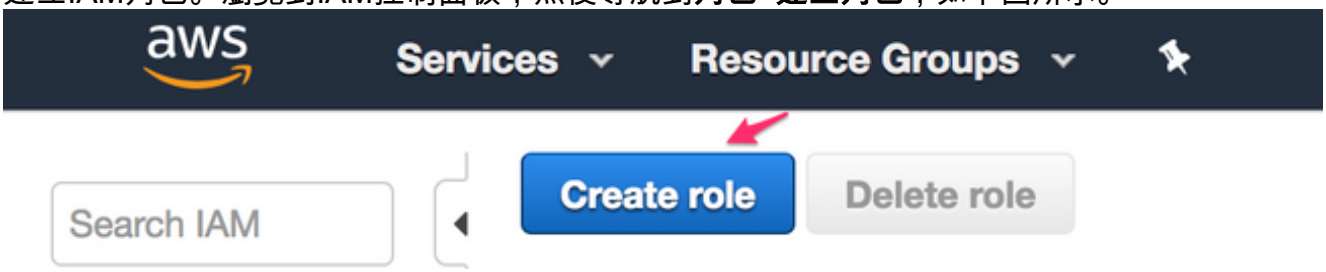
2. 在Inbound Rules（入站規則）下，定義要允許sg-1cf47d6d的流量。在本例中，您允許所有流量。

步驟4.使用策略建立IAM角色並將其與VPC關聯。

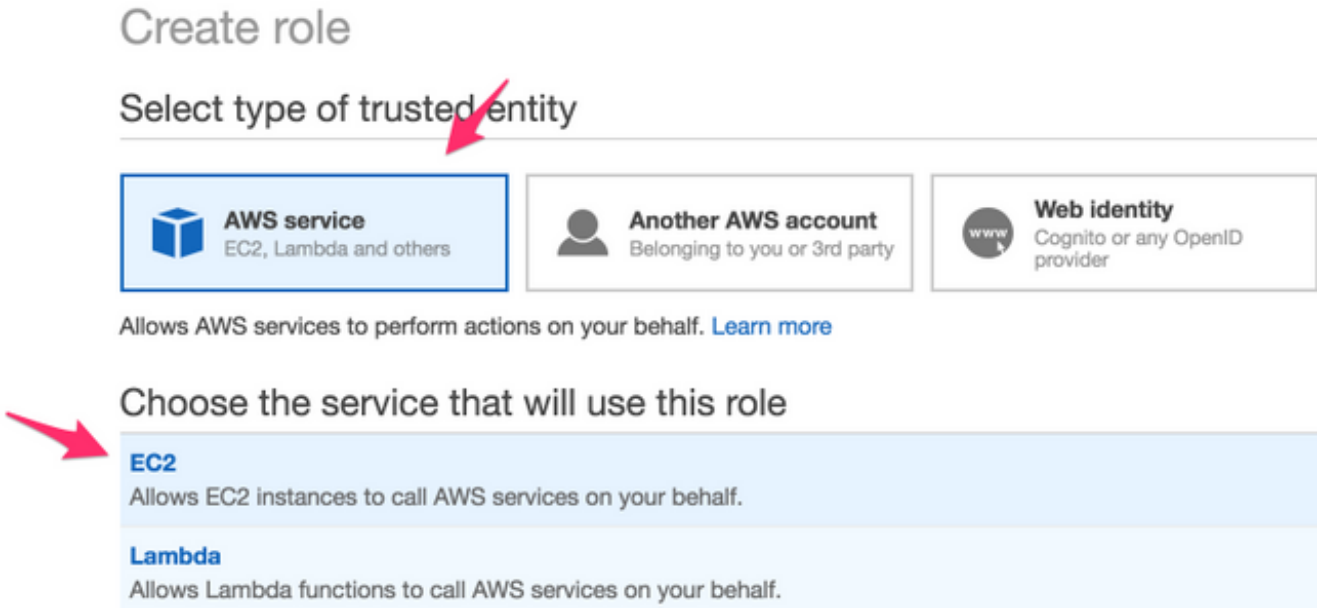
IAM授予您的CSR訪問Amazon API的許可權。

CSR1000v用作代理，以呼叫AWS API命令來修改路由表。預設情況下，不允許AMI訪問API。此過程將建立IAM角色，並在CSR例項啟動期間使用此角色。IAM為CSR提供使用和修改AWS API的訪問憑證。

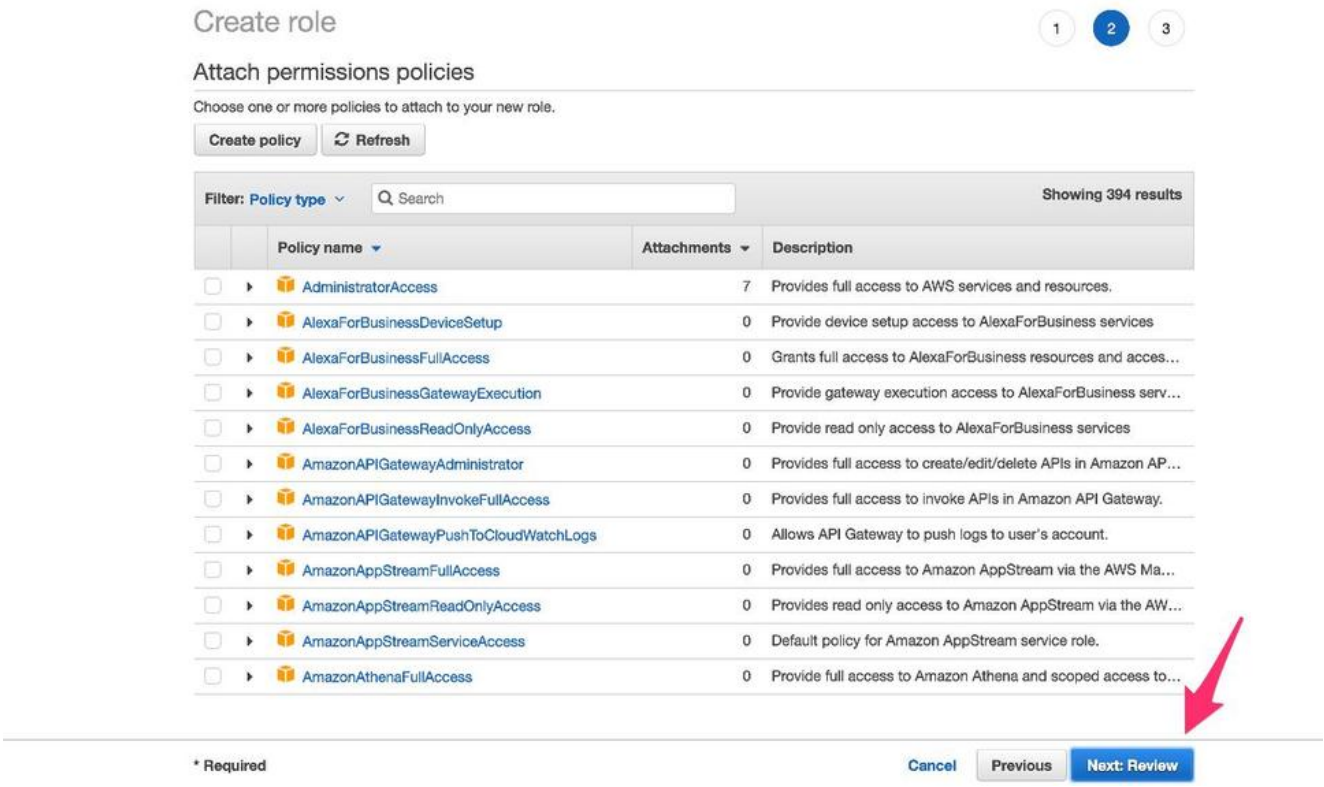
1. 建立IAM角色。瀏覽到IAM控制面板，然後導航到**角色>建立角色**，如下圖所示。



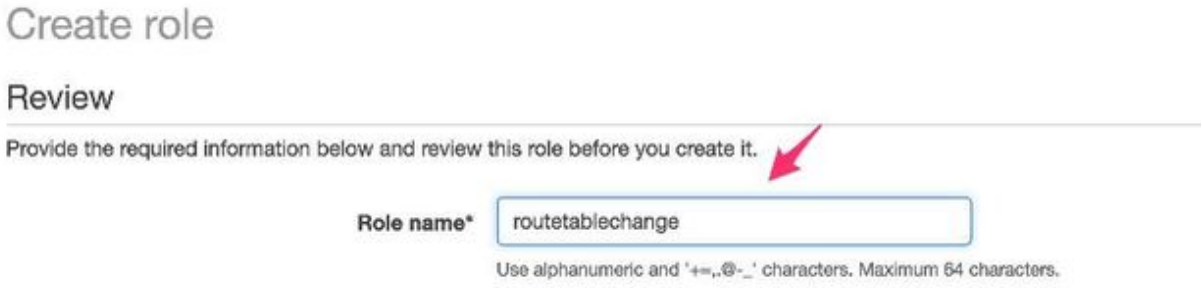
2. 如圖所示，允許EC2例項代表您呼叫AWS。



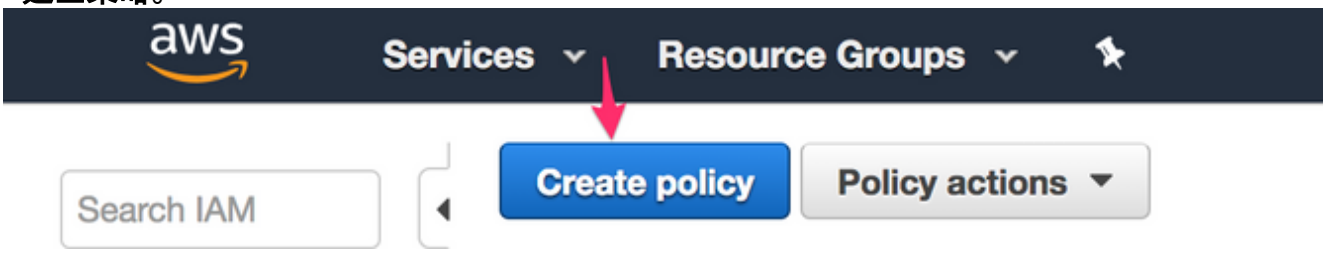
3. 建立角色並點選**下一步：檢查**，如下圖所示。



4. 為其指定角色名稱。在本例中，如圖所示，角色名稱為**routetablechange**。

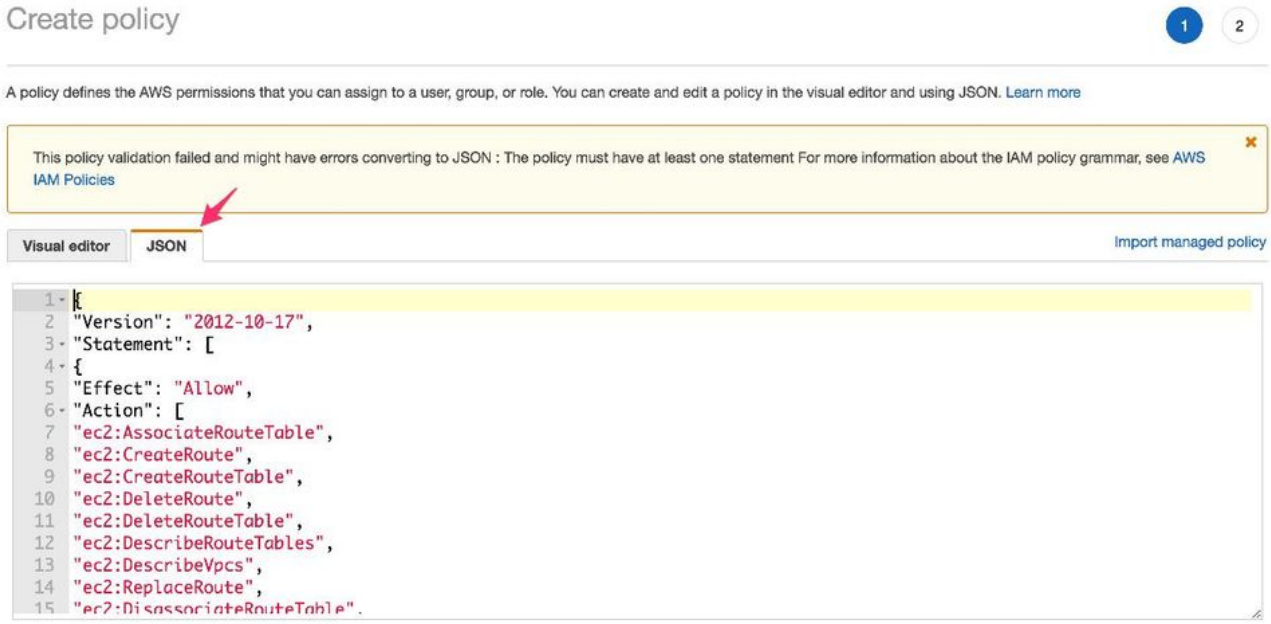


5. 接下來，您需要建立一個策略，並將其附加到上面建立的角色。IAM控制面板，並導航至**策略>建立策略**。

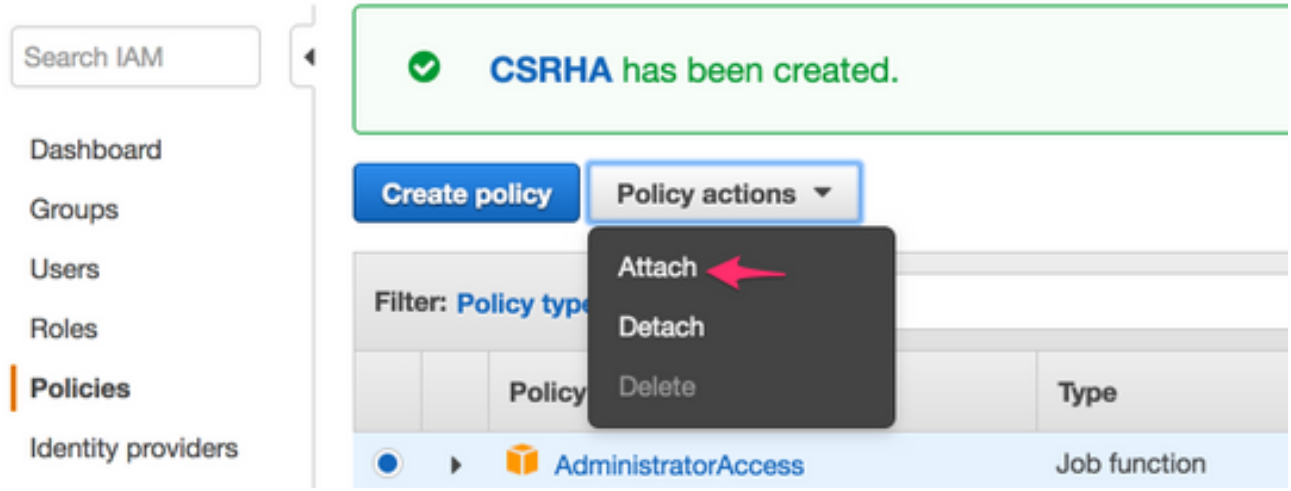



```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:AssociateRouteTable",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:DeleteRoute",
"ec2:DeleteRouteTable",
"ec2:DescribeRouteTables",
"ec2:DescribeVpcs",
"ec2:ReplaceRoute",
"ec2:DisassociateRouteTable",
"ec2:ReplaceRouteTableAssociation"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

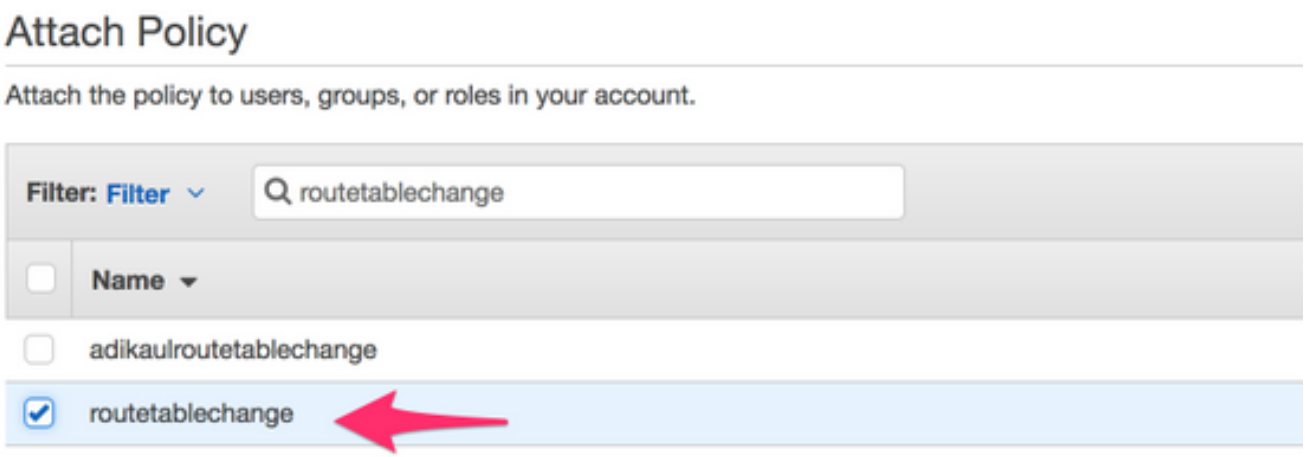
```
"Resource": "*"
}
]
}
```



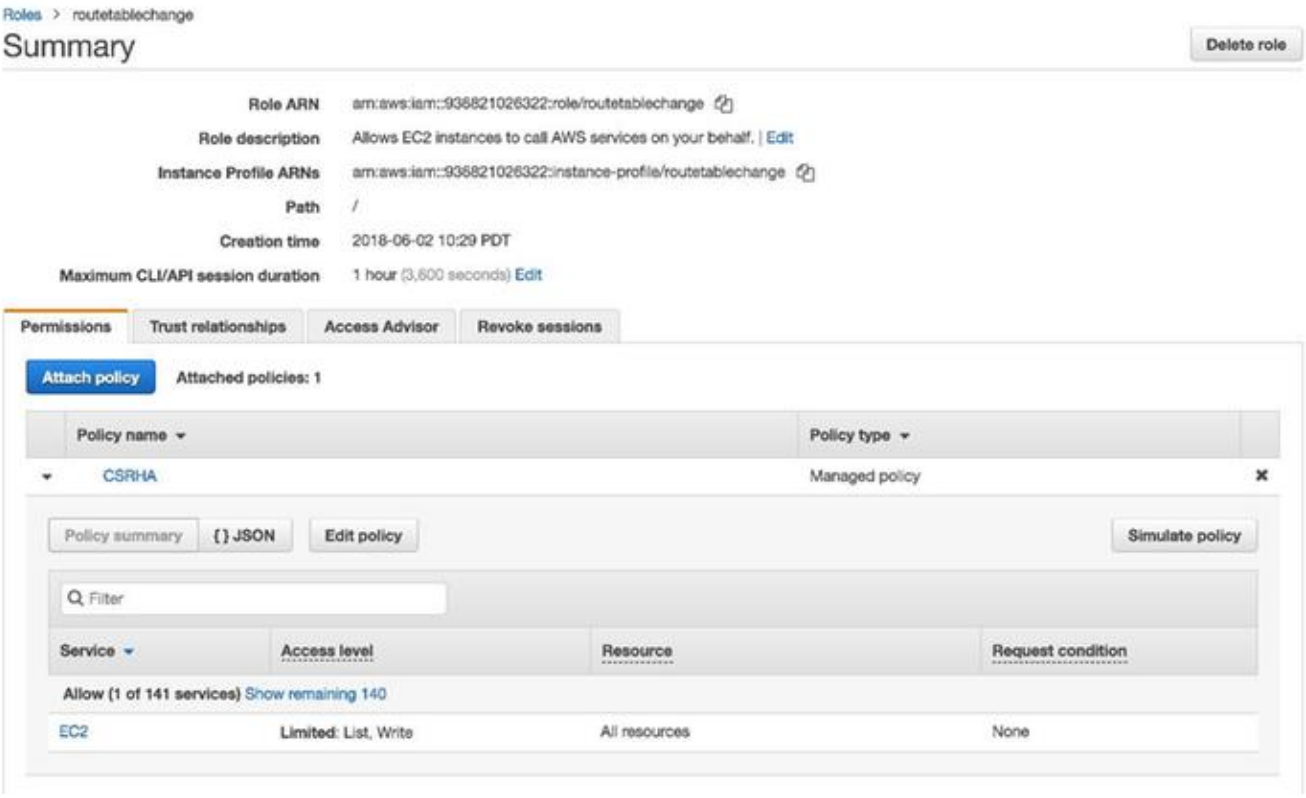
6. 為其指定一個策略名稱，並將其附加到您建立的角色。在本示例中，策略名稱稱為具有管理員訪問許可權的CSRHA，如下圖所示。



7. 如圖所示，將策略附加到您建立的名為**routetablechange**的角色。



8. 摘要.



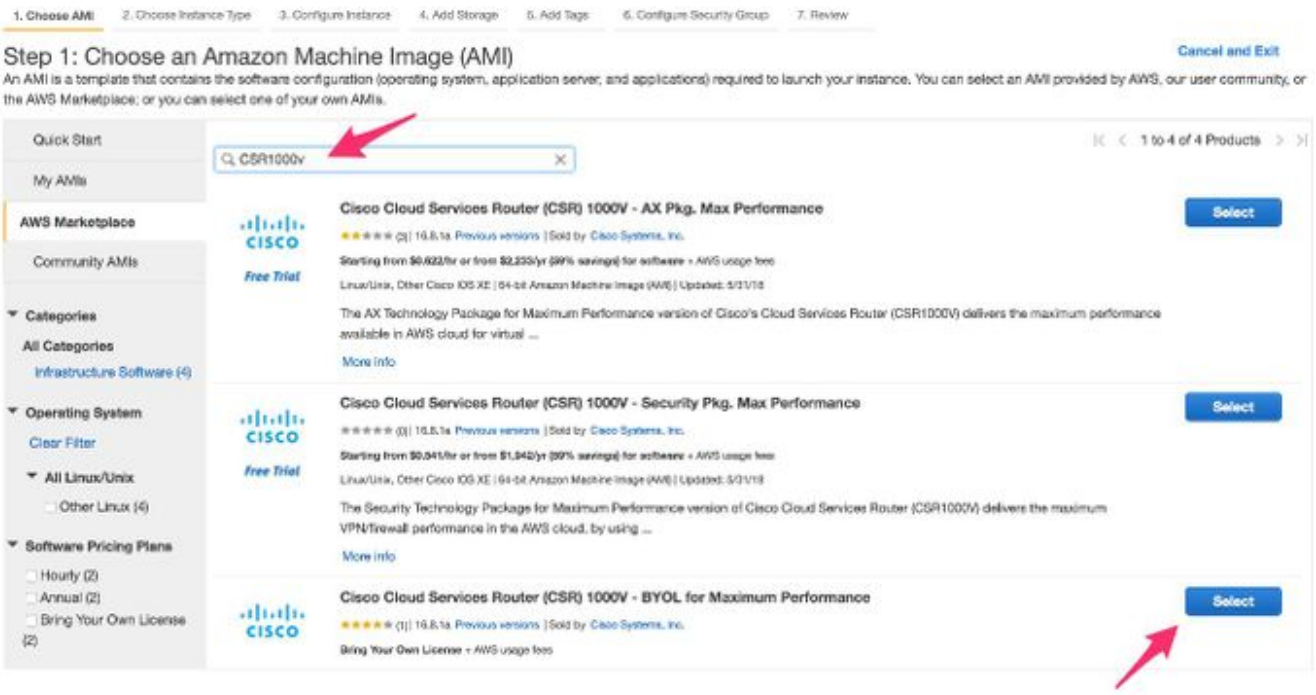
步驟5.使用您建立的AMI角色啟動CSR1000v並關聯公共/專用子網。

每個CSR1000v路由器有2個介面（1個公共介面，1個專用介面），並位於自己的可用區中。您可以將每個CSR視為位於單獨的資料中心中。

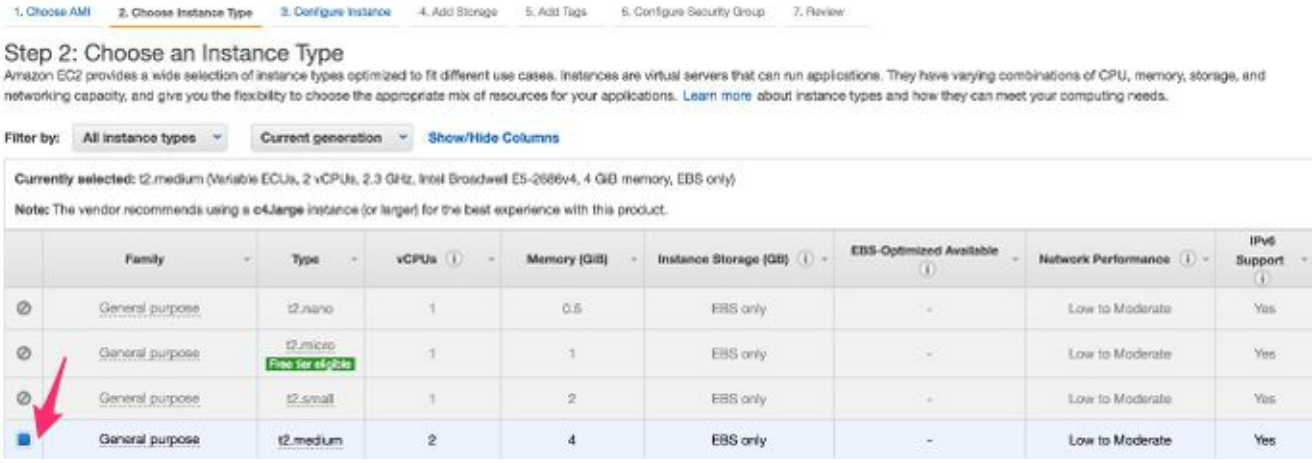
1. 在AWS控制檯上，選擇**EC2**，然後按一下**Launch Instance**。

2. 選擇AWS Marketplace。

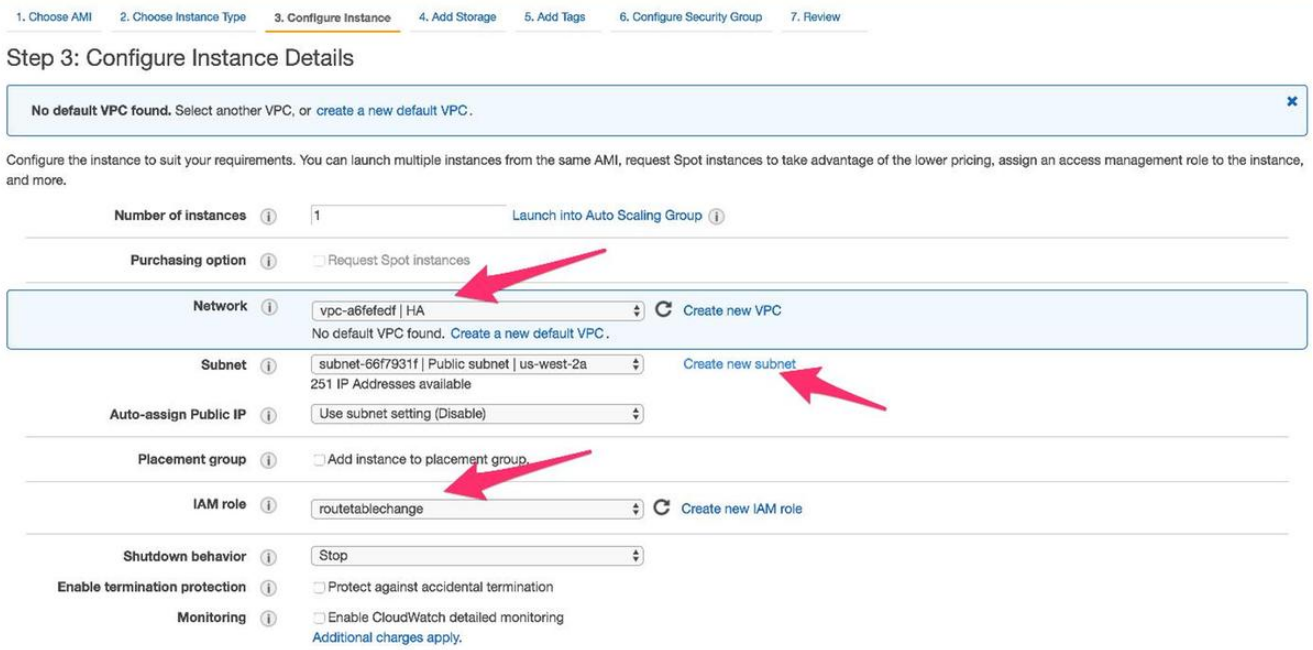
3. 輸入CSR1000v，在本範例中，您使用思科雲端服務路由器(CSR)1000V - BYOL來達到最佳效能。



4. 選擇例項型別。在本示例中，選定的型別為**t2.medium**。

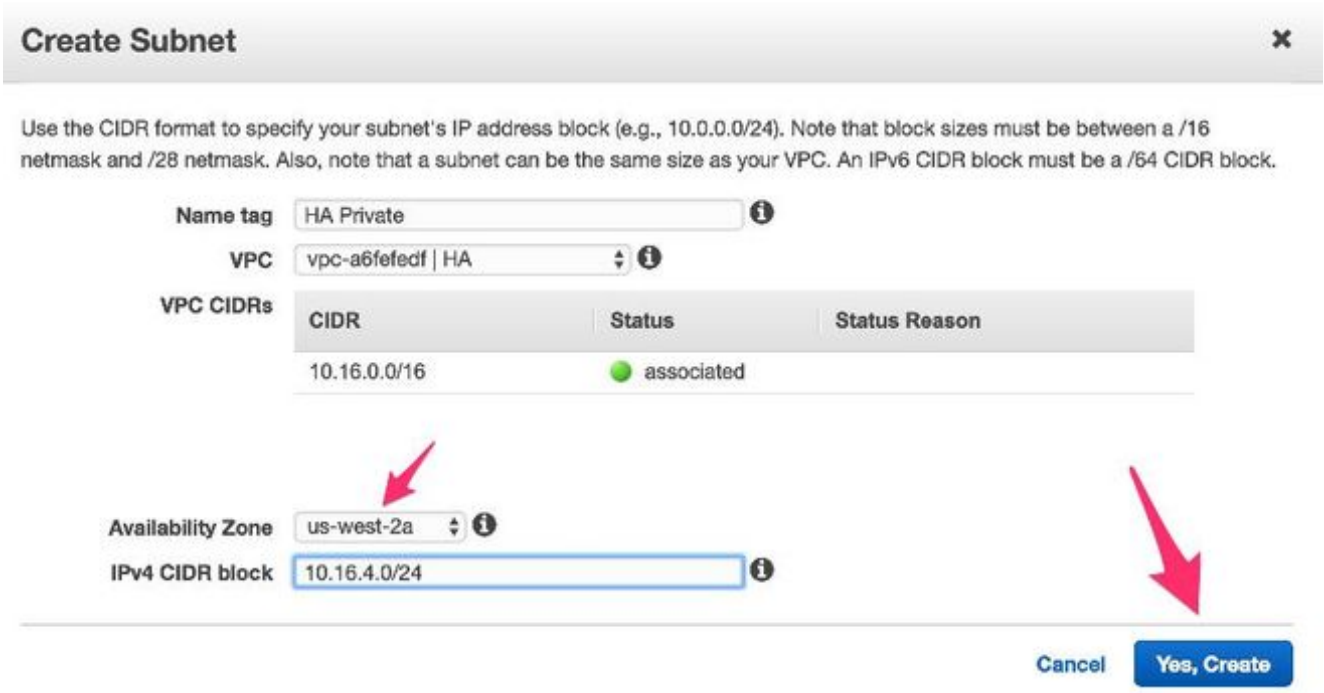


5. 配置例項時，您需要確保選擇上面建立的VPC以及上面的IAM角色。此外，請建立一個與面向專用介面的專用子網。



6. 點選Create new Subnet for Private Subnet。在本示例中， Name標籤是HA Private。確保它

與公共子網位於同一可用區域。

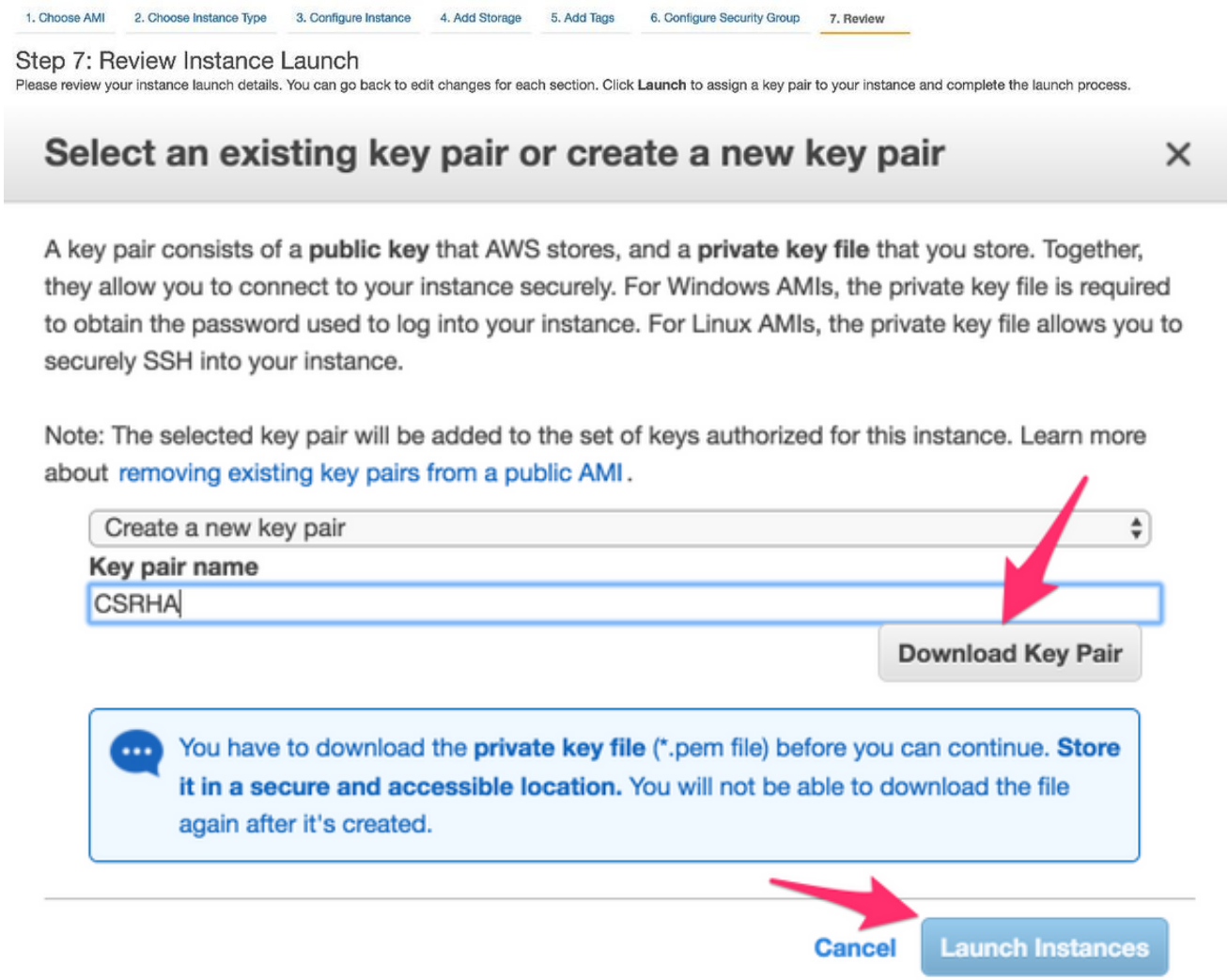


7. 向下滾動，在「Configure Instance Details」下，按一下**Add Device**，如下圖所示。

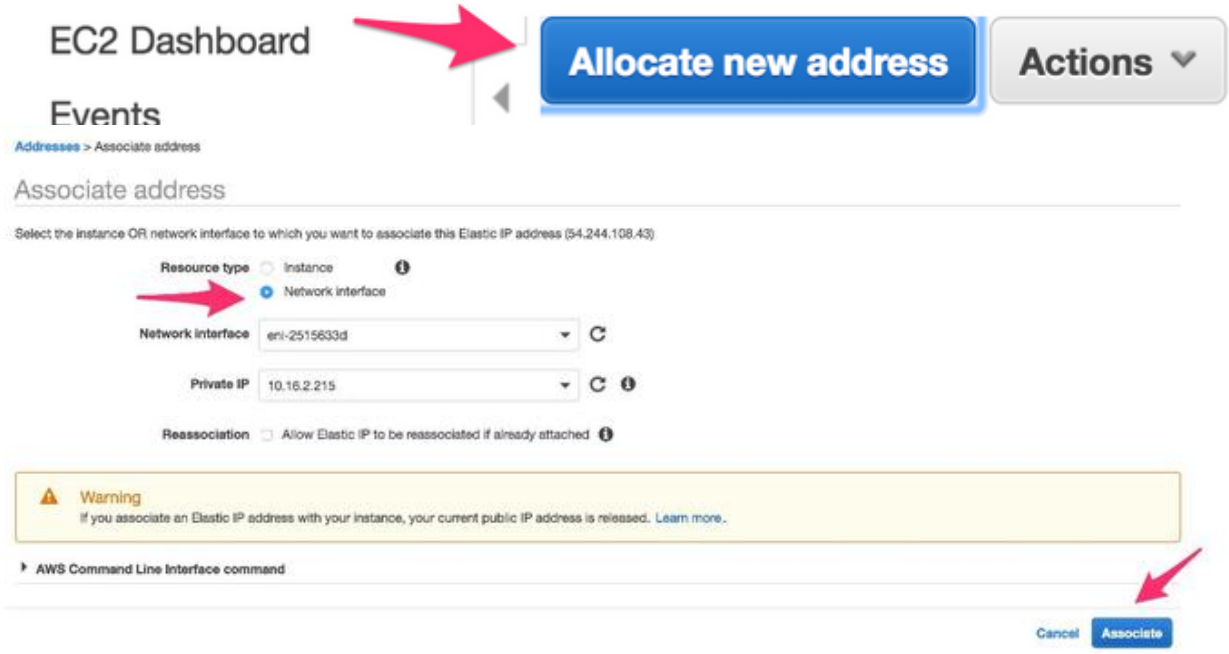
8. 新增輔助介面後，關聯您建立的名為HA Private的專用子網。Eth0是公共介面，Eth1是專用介面。 **附註**：在此下拉選單中不會顯示上一步建立的子網。您可能需要刷新或取消該頁，然後重新開始才能顯示子網。

9. 選擇您在VPC下建立的安全組，並確保規則定義正確。

10. 建立新的金鑰對並確保下載私鑰。您可以為每台裝置重複使用一個金鑰。 **附註**：如果您丟失了私鑰，則無法再次登入您的CSR。沒有方法恢復金鑰。

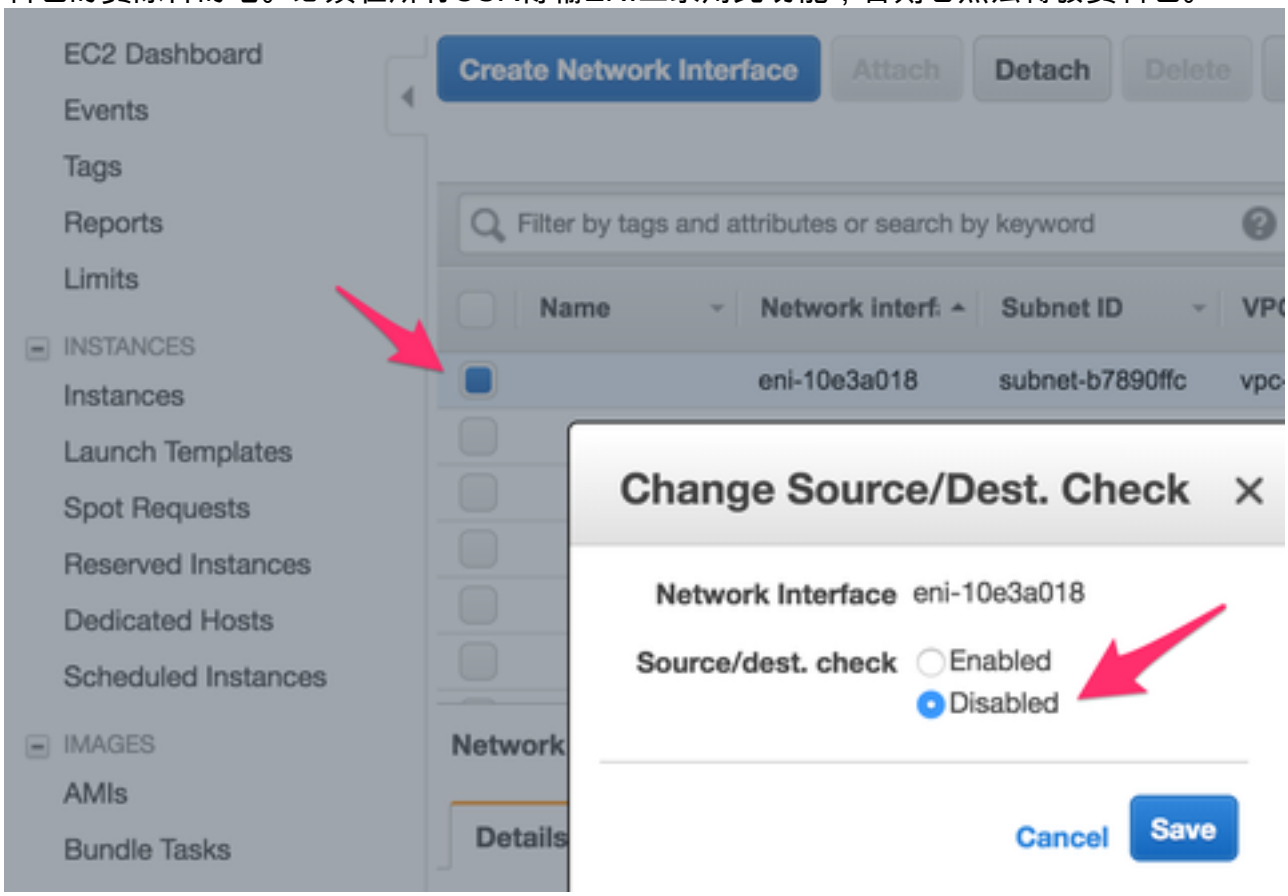


11. 將Elastic IP與您建立的例項的公共介面的ENI相關聯，然後導航至**AWS控制檯> EC2管理>網路安全> Elastic IP。 附註**：公共術語/私人術語可能會在這裡混淆您。在本示例中，公共介面的定義是Eth0，即面向網際網路的介面。從AWS的角度來看，我們的公共介面是他們的私有IP。

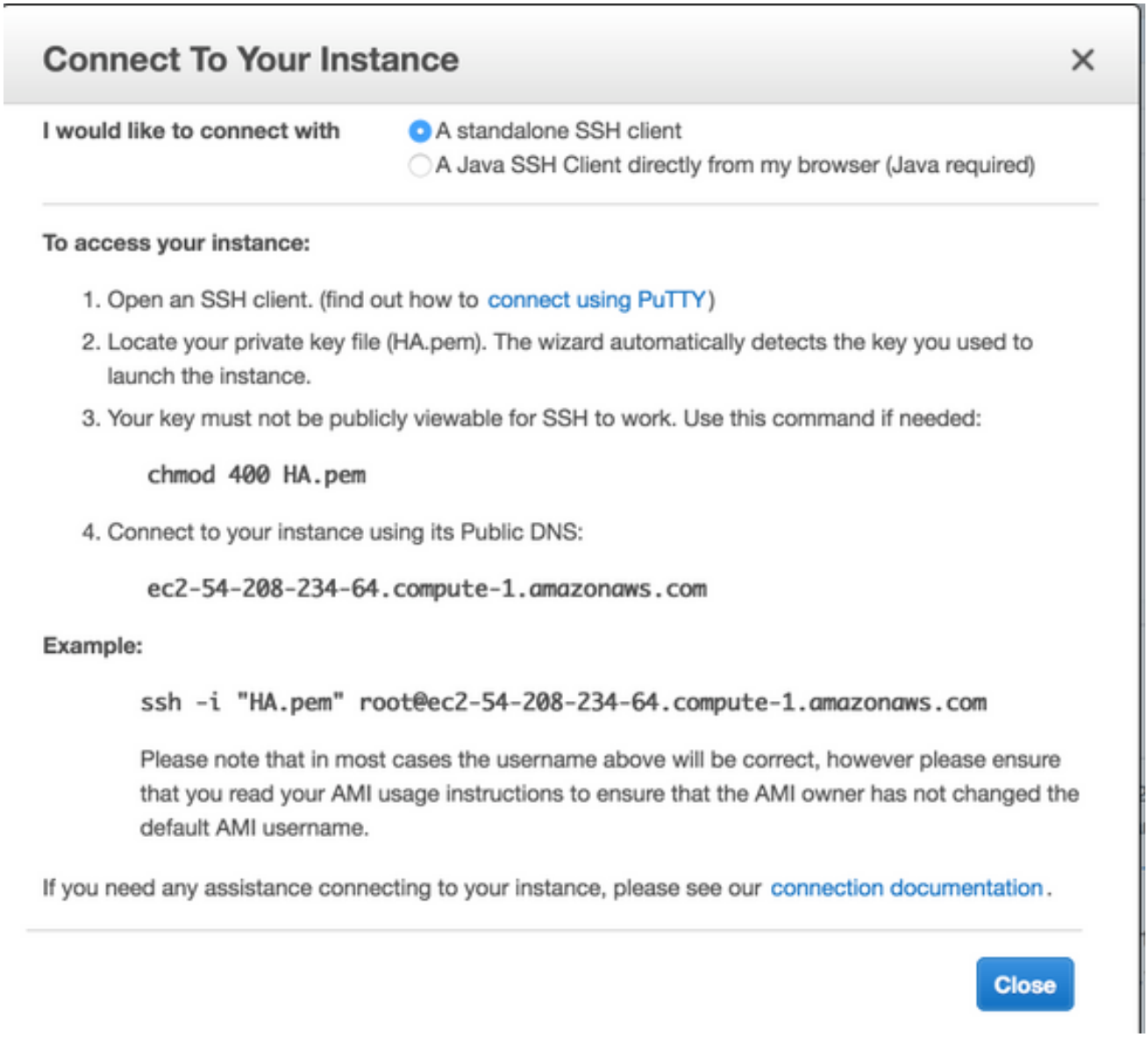


12. 導航到**EC2 > Network Interfaces**時，禁用Source/Dest Check。驗證每個ENI以進行源/目標檢查。 預設情況下，所有ENI都啟用此源/目標檢查。一種反欺騙功能，旨在通過在轉發流量

之前驗證ENI是流量的目的地，從而避免讓ENI出現並非真正針對它的流量。路由器很少是資料包的實際目的地。必須在所有CSR傳輸ENI上禁用此功能，否則它無法轉發資料包。



13. 連線到您的CSR1000v。 **附註**：通過SSH連線到CSR1000v的AWS提供的使用者名稱可能錯誤地列為root。如果需要，請將其更改為ec2-user。**附註**：在中必須能夠對DNS地址執行SSH執行ping操作。此處為ec2-54-208-234-64.compute-1.amazonaws.com。檢查路由器的公共子網/埃尼是否與公共路由表關聯。請簡要轉到步驟8，瞭解如何將子網與路由表相關聯。



步驟6.重複步驟5，為HA建立第二個CSR1000v執行個體。

公共子網： 10.16.1.0/24

專用子網：10.16.5.0/24

如果無法ping通這個新AMI的彈性IP地址，請簡要轉到步驟8，並確保公用子網與公用路由表關聯。

步驟7.重複步驟5並從AMI應用商店建立VM(Linux/Windows)。

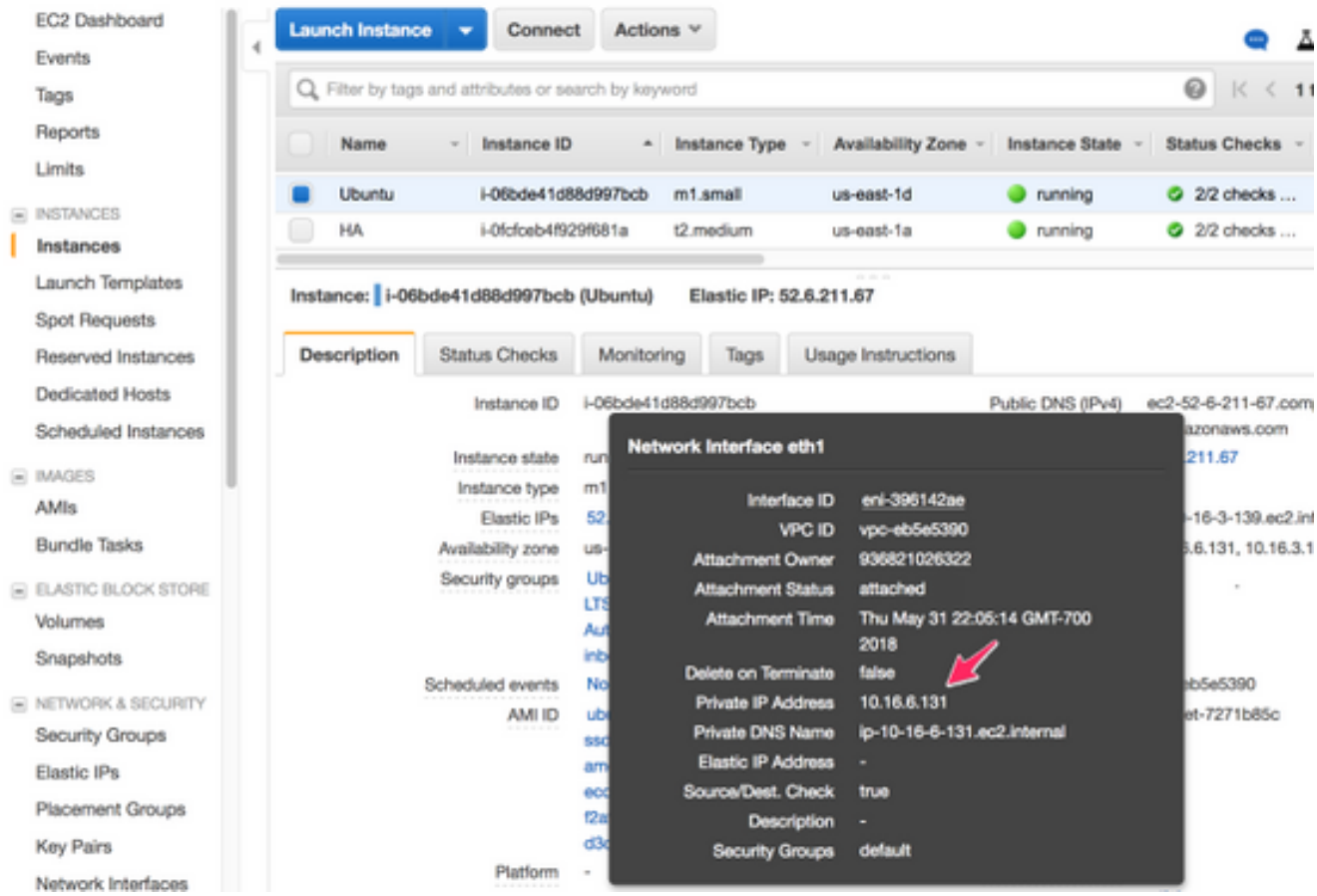
在本示例中，請使用Ubuntu Server 14.04 LTS。

公共子網： 10.16.2.0/24

專用子網：10.16.6.0/24

如果無法ping通這個新AMI的彈性IP地址，請簡要轉到步驟8，並確保公用子網與公用路由表關聯。

1. 預設情況下，會為公共介面建立Eth0。為專用子網建立另一個名為eth1的介面。



2. 您在Ubuntu中配置的IP地址是AWS分配的eth1專用介面。

```
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. 關閉介面或重新啟動VM。

```
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. Ping 8.8.8.8進行測試。確保已在步驟7中新增了8.8.8.8路由。

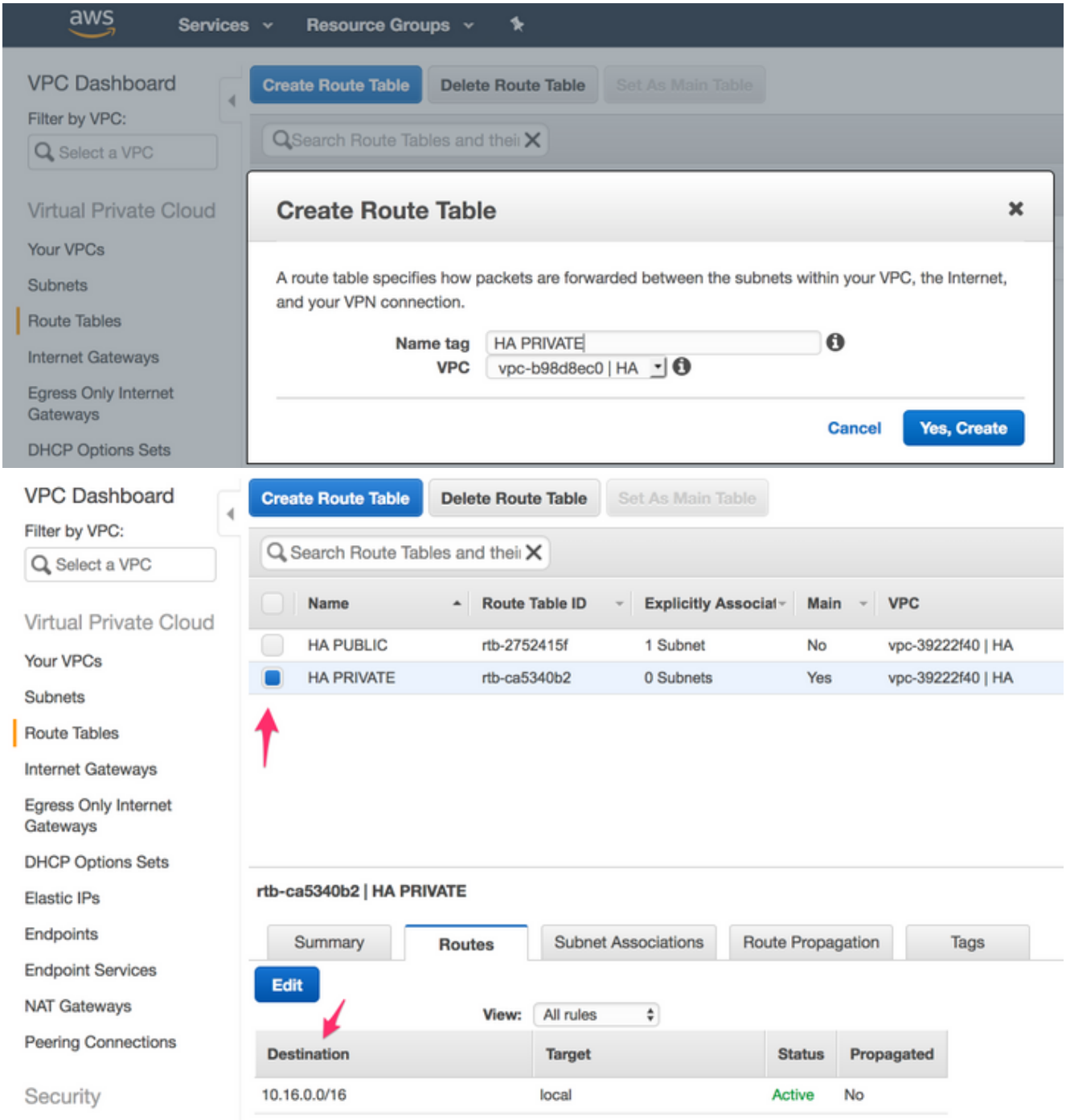
```
ubuntu@ip-10-16-2-139:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.16.2.1 0.0.0.0 UG 0 0 0 eth0
8.8.8.8 10.16.6.1 255.255.255.255 UGH 0 0 0 eth1     <--------------
10.16.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.16.6.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
```

如果未在表中列出8.8.8.8，請手動新增：

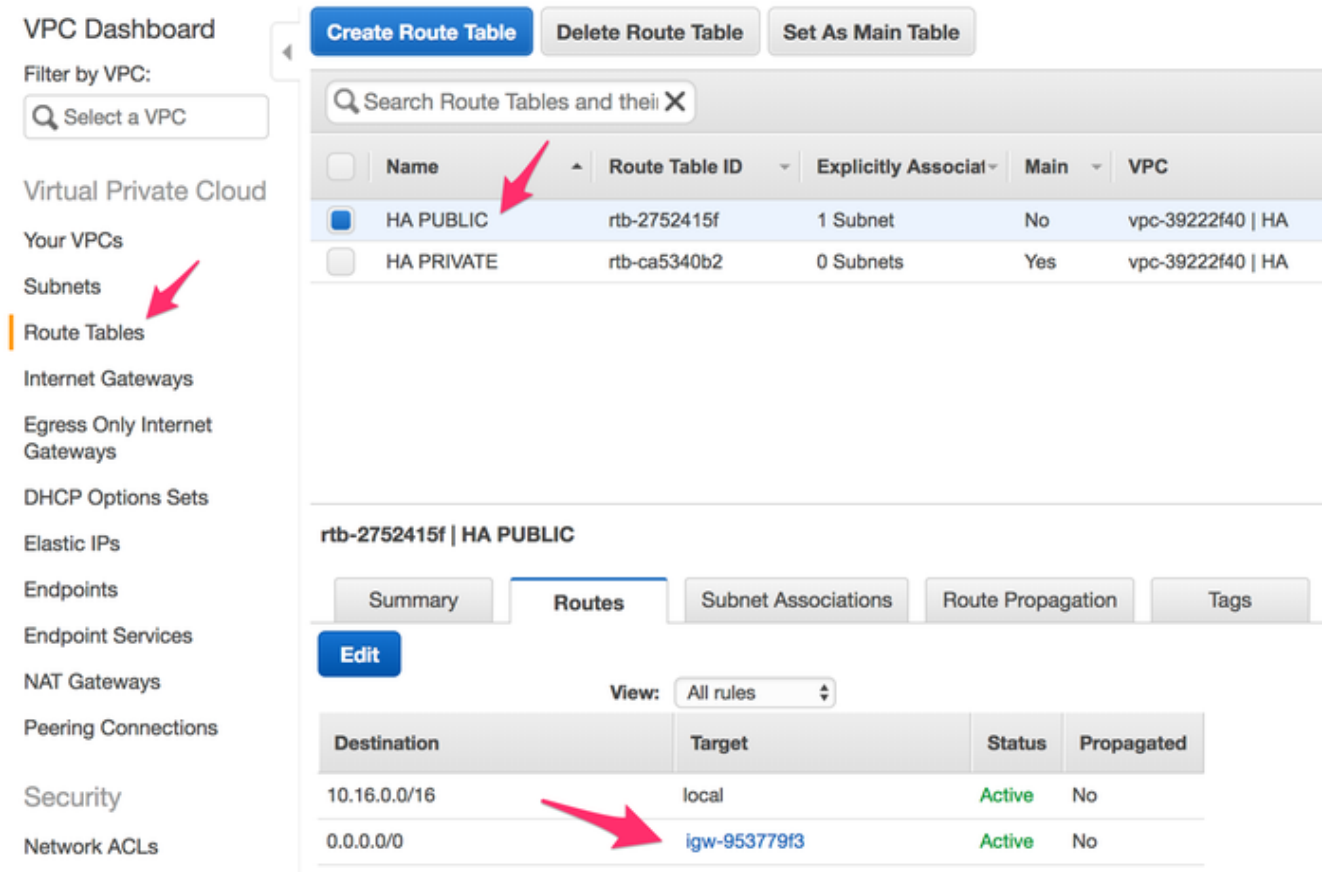
```
ubuntu@ip-10-16-2-139:~$ sudo route add -host 8.8.8.8 gw 10.16.6.1 dev eth1
```

步驟8.配置私有路由表和公共路由表。

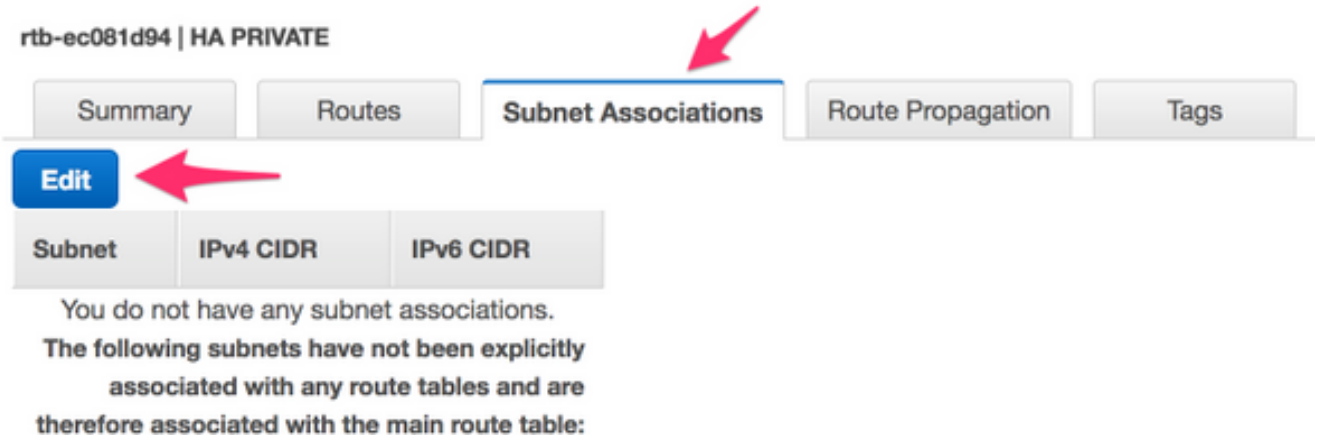
1. 通過步驟2中的嚮導建立VPC時，將自動建立兩個路由表。如果只有一個路由表，請為您的專用子網建立另一個路由表，如下圖所示。



2. 以下是兩個路由表的檢視。公共路由表已自動連線Internet網關(igw-95377973)。請相應地為這兩個表新增標籤。PRIVATE表不應具有此路由。



3. 將所有6個子網關聯到正確的路由表 3個公共介面與公共路由表關聯：公共子網：10.16.0.0/24, 10.16.1.0/24, 10.16.2.0/24 3個專用介面與專用路由表關聯：專用子網：10.16.4.0/24、10.16.5.0/24、10.16.6.0/24



步驟9.使用BFD和任何路由協定配置網路地址轉換(NAT)和GRE隧道。

透過CSR 1000v的彈性IP設定通用路由封裝(GRE)通道（建議避免偵測false失敗的DHCP租約續約問題。）如果需要更快的收斂，則雙向轉發檢測(BFD)值可以配置為比本示例所示值更積極。但是，這可能會導致在間歇性連線期間發生BFD對等體關閉事件。此示例中的值在1.5秒內檢測對等體故障。在執行AWS API命令的時間和VPC路由表更改生效的時間之間，存在大約幾秒的可變延遲。

- CSRHA上的配置
  GRE和BFD — 用於觀察HA故障轉移的條件

```
interface Tunnel1
  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 Tunnel1
  network 192.168.1.0
  passive-interface GigabitEthernet1
```

NAT和路由 — 用於通過專用介面實現虛擬機器網際網路可達性

```
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
```

- CSRHA1上的配置

GRE和BFD — 用於觀察HA故障轉移的條件

```
interface Tunnel1
  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 Tunnel1
  network 192.168.1.0
  passive-interface GigabitEthernet1
```

NAT和路由 — 用於通過專用介面實現虛擬機器網際網路可達性

```
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
```

步驟10.配置高可用性（Cisco IOS XE Denali 16.3.1a或更高版本）。

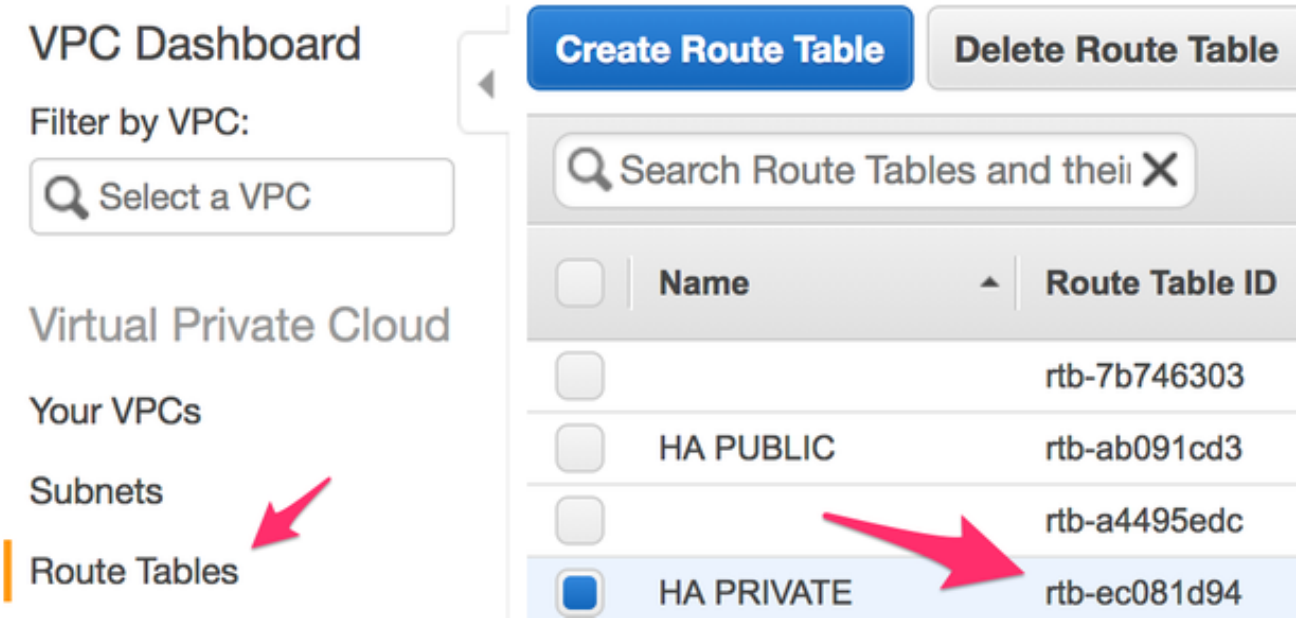
使用下面指定的雲提供商aws命令配置每個CSR 1000v，監控BFD對等體關閉事件。在檢測到AWS HA錯誤（例如BFD對等體關閉）後，使用此命令定義對(VPC)Route-table-id、Network-interface-id和CIDR的路由更改。

```
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
```

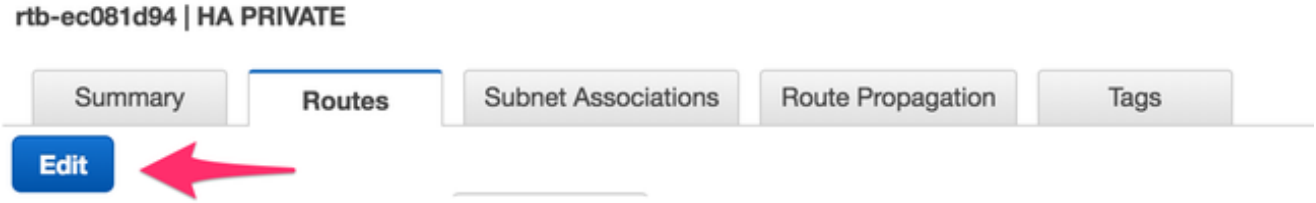
1. 第#bfd對等ipaddr是對等通道IP地址。

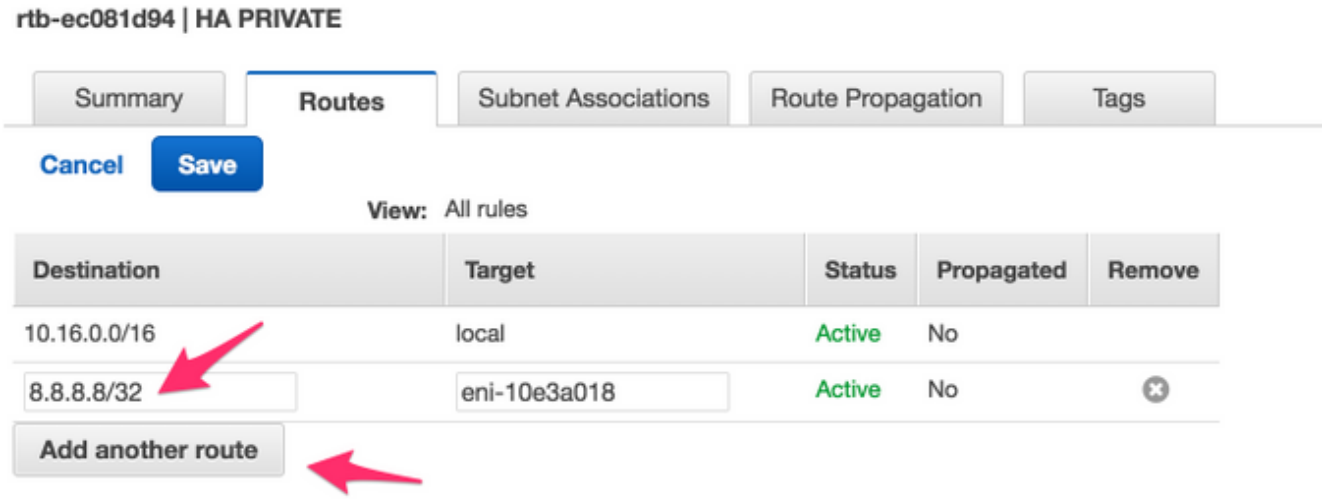
```
CSRHA#show bfd neighbors

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

2. 在AWS#route-table制台下找到路由表名稱，請導航至**VPC > Route Tables**。此操作會更改專用路由表。

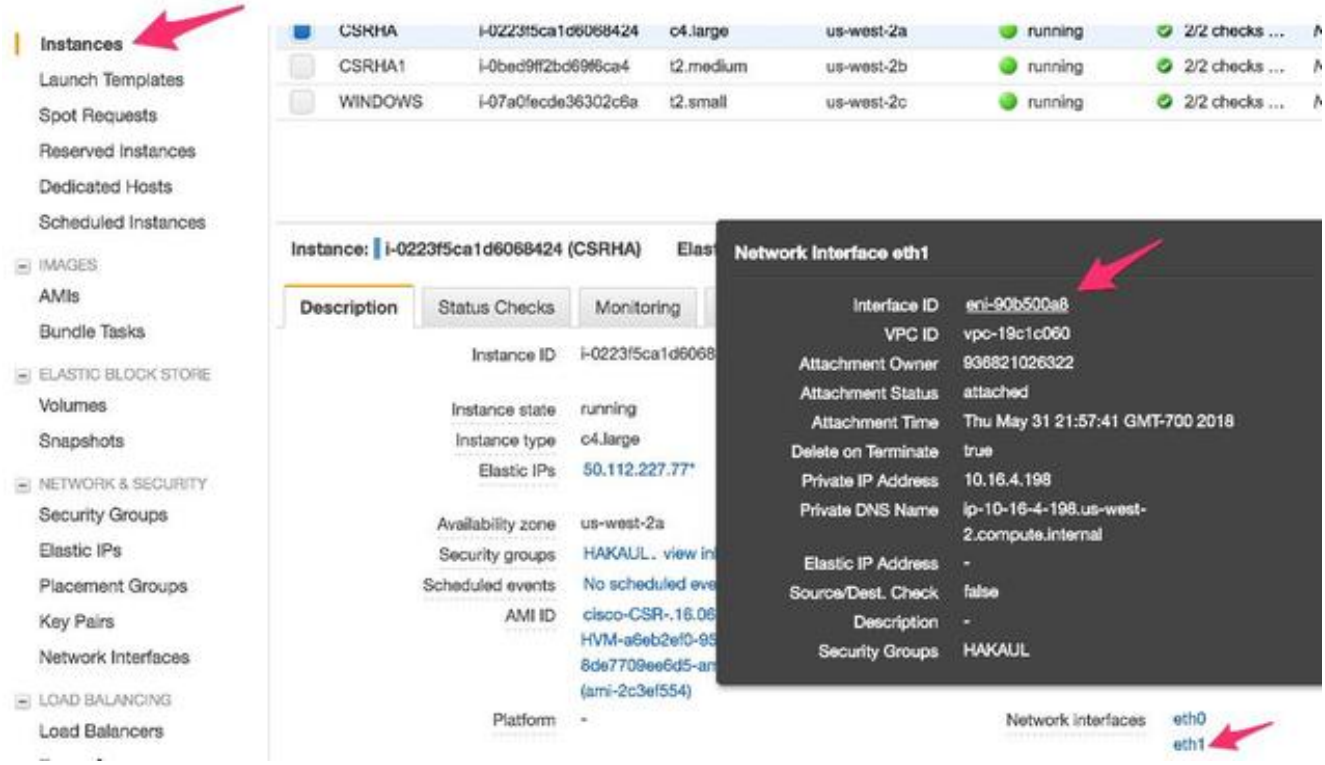


3. #cidr ip ipaddr/字首是路由表中要更新的路由的目標地址。在AWS控制檯下，導航到**VPC >路由表**。向下滾動，按一下**Edit**，然後按一下**Add another route**。新增我們的測試目的地址8.8.8.8和CSRHA的專用ENI。





4. 在#eni例項中找到elastic-network-intf-name。按一下每個相應CSR的專用介面eth1，並使用介面ID。



5. AWS#region稱是在AWS文檔中找到的代碼名稱。此清單可能會更改或增大。要查詢最新更新，請訪問Amazon的區域和可用區文檔。

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)

CSRHA上的冗餘配置示例

```
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
```

CSRHA1上的冗餘配置示例

```
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
```

驗證高可用性

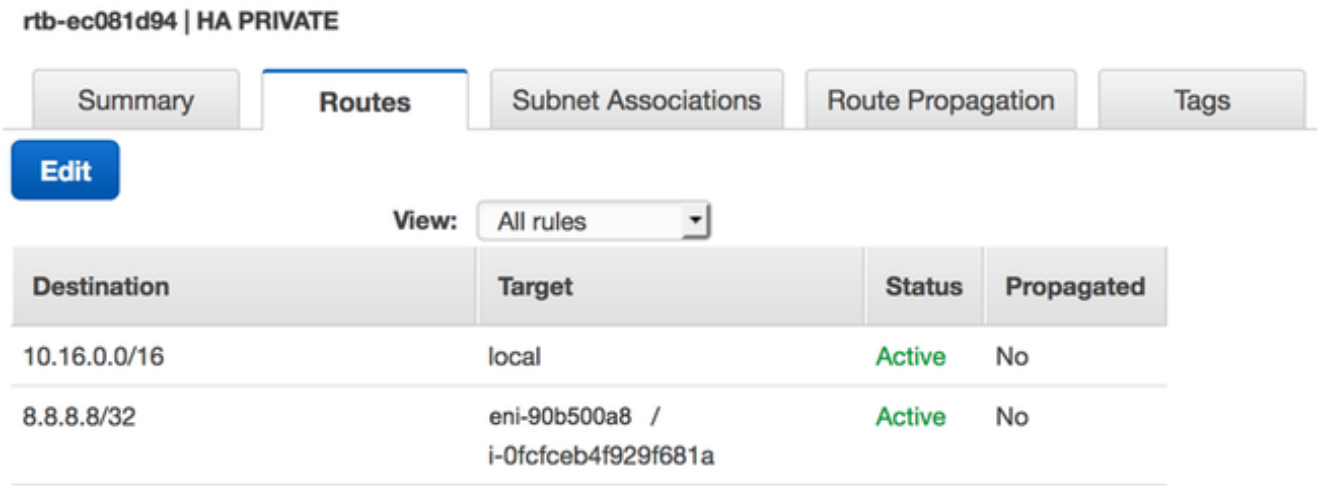
1. 檢查BFD和雲配置。

```
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. 從VM對目標運行連續ping。確保ping通過專用eth1介面。

```
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
```

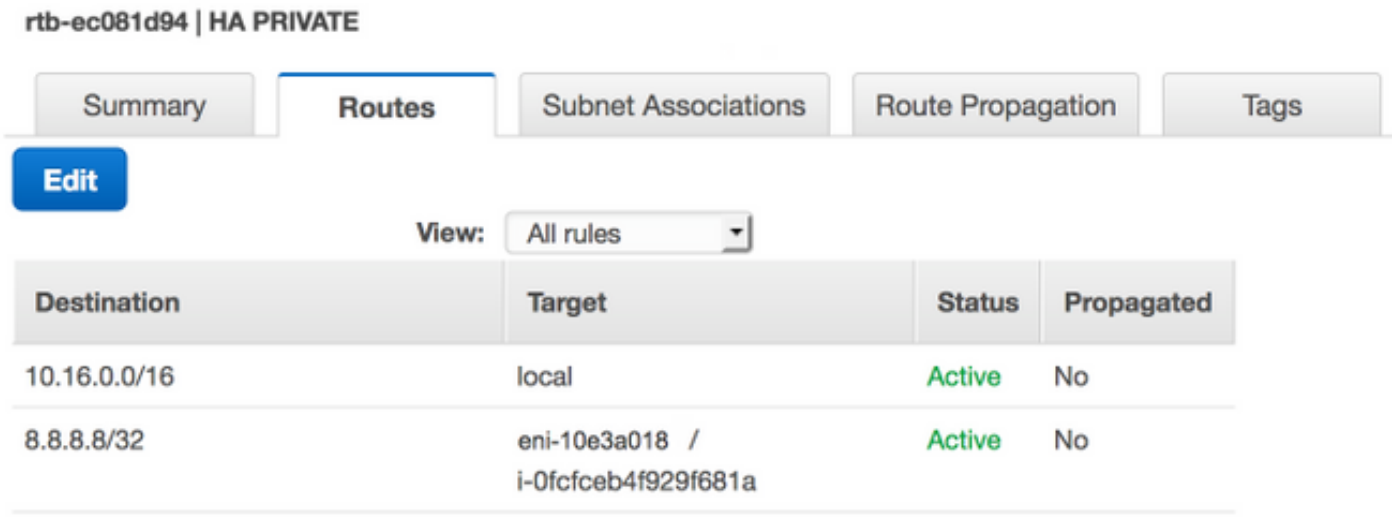
3. 檢查專用路由表。Eni目前是CSRHA的專用介面，此介面是流量。



4. 關閉CSRHA的Tunnel1以模擬HA故障切換。

```
CSRHA(config)#int Tun1
CSRHA(config-if)#shut
```

5. 請注意，路由表指向新的ENI，即CSRHA1的專用介面。



疑難排解

- 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和任何專用IP與正確的介面關聯，並將正確的子網新增到正確的路由表中，連線到正確的路由器以及正確的VPC和區域，並與IAM角色和安全組關聯。
- 禁用每個ENI的源/目標檢查。
- 對於Cisco IOS XE 16.3.1a或更高版本，這是可用的其他驗證命令。

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

- 以下是調試中常見的故障：

問題： httpc_send_request失敗

解析度：Http用於從CSR向AWS傳送API呼叫。確保DNS可以解析例項中列出的DNS名稱。確保http流量未被阻止。

```
*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
```

問題：路由表rtb-9c0000f4和介面eni-32791318屬於不同的網路

解析度：不同網路中的區域名稱和ENI配置不正確。區域和ENI應與路由器位於同一區域。

```
*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>
```

問題：您無權執行此操作。編碼授權失敗消息。

解析度：IAM JSON角色/策略建立錯誤或未應用於CSR。IAM角色授權CSR進行API呼叫。

```
*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: qYvEB4MUdOB8m2itSteRgnOuslAaxhAbDph5qGRJkjJbrESajbmF5HWUR-
MmHYeRAlpKZ3Jg_y-
_tMlYel5l_ws8Jd9q2W8YDXBl3uXQqfW_cjjrgy9jhnGY0nOaNu65aLpfqui8kS_4RPOpm5grRFfo99-
8uv_N3mYaBqKFPn3vUcSYKBmxFIIkJKcjY9esOeLIOWDcnYGGu6AGGMoMxWDtk0K8nwk4IjLDcnd2cDXeENS45w1PqzKGPsH
v3wD28TS5xRjIrPXYrT18UpV6lLA_09Oh4737VncQKfzbz4tPpnAkoW0mJLQ1vDpPmNvHUpEng8KrGWYNfbfemoDtWqIdABf
aLLLmh4saNtnQ_OMBoTi4toBLEb2BNdMkl1UVBIxqTqdFUVRS**MSG 00041 TRUNCATED** **MSG 00041
CONTINUATION
#01**qLosAb5Yx0DrOsLSQwzS95VGvQM_n87LBHYbAWWhqWj3UfP_zmiak7dlm9P41mFCucEB3Cs4FRsFtb-
9q44VtyQJaS2sU2nhGe3x4uGEsl7F1pNv5vhVeYOZB3tbOfbV1_Y4trZwYPFgLKgBShZp-WNmUKUJsKc1-
6KGqmp7519imvh66JgwgmU9DT_qAZ-jEjkqWjBrxg6krw</Message></Error></Errors><RequestID>4cf31249-
2a6e-4414-ae8d-6fb825b0f398</RequestID></Response>
```

相關資訊

- VPC閘道備援 — Cisco
- 適用於Amazon Web Services的Cisco CSR 1000v系列雲服務路由器部署指南
- 例項型別細分
- EC2和VPC
- 《EC2使用手冊》中的「彈性網路介面」包括每個例項型別的ENI數量
- 增強的Linux網路操作說明，有用的背景資訊
- 專用例項/租賃說明和操作說明
- 一般EC2文檔
- 一般VPC文檔
- 區域和可用區域
- CSR1000v高可用性版本3

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）。