Guida all'installazione della ridondanza HA CSR1000v su Amazon AWS

Sommario

Introduzione

Questo documento descrive la guida alla configurazione su come installare i router CSR1000v per l'alta disponibilità sul cloud Amazon AWS. L'obiettivo è quello di fornire agli utenti una conoscenza pratica dell'HA e la capacità di installare un banco di prova completamente funzionale.

Per informazioni più dettagliate su AWS e HA, *consultare* la sezione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Un account Amazon AWS
- 2 CSR1000v e 1 AMI Linux/Windows nella stessa area
- HA versione 1 è supportato sulle versioni di Cisco IOS-XE® da 16.5 a 16.9. A partire dalla versione 16.11, utilizzare HA versione 3.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco IOS-XE® Denali 16.7.1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Obiettivo

In un ambiente con più zone di disponibilità, simulare il traffico continuo dal centro dati privato (VM) a Internet. Simulare un failover HA e osservare che ha esito positivo, in quanto la tabella di routing passa dal traffico CSRHA all'interfaccia privata di CSRHA1.

Topologia

Prima di avviare la configurazione, è importante comprendere completamente la topologia e la progettazione. In questo modo è possibile risolvere eventuali problemi in un secondo momento.

Esistono diversi scenari di installazione di HA in base ai requisiti di rete. Per questo esempio, la ridondanza HA è configurata con queste impostazioni:

- 1x - Regione
- 1x - VPC
- 3x - Zone di disponibilità
- 6x - Interfacce/subnet di rete (3x Public Facing/3x Private Facing)
- 2x - Tabelle di route (pubbliche e private)
- 2 router - CSR1000v (Cisco IOS-XE® Denali 16.3.1a o versioni successive)
- 1x - VM (Linux/Windows)

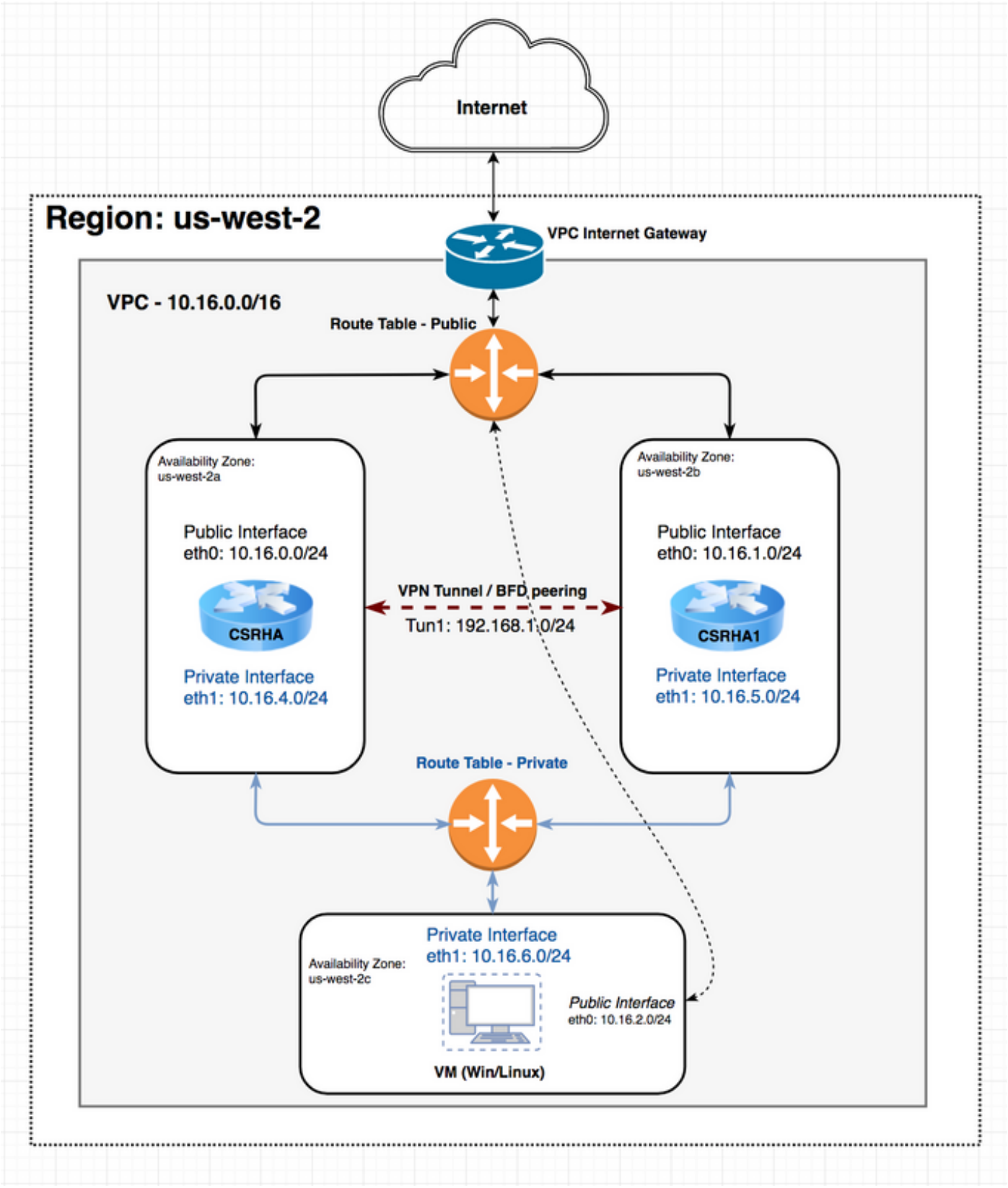
In una coppia HA sono presenti due router CSR1000v, in due diverse zone di disponibilità. Ogni zona di disponibilità può essere considerata come un centro dati separato per una resilienza hardware aggiuntiva.

La terza zona è una VM, che simula un dispositivo in un centro dati privato. Per il momento, l'accesso a Internet è abilitato tramite l'interfaccia pubblica su in modo da poter accedere e configurare la VM. In genere, tutto il traffico normale deve passare attraverso la tabella di route

privata.

Eseguire il ping dell'interfaccia privata della VM → tabella di percorso privata → CSRHA → 8.8.8.8 per la simulazione del traffico. In uno scenario di failover, osservare che la tabella delle route private ha modificato la route in modo che punti all'interfaccia privata di CSRHA1.

Esempio di rete



Terminologia

RTB - ID tabella route.

CIDR - Indirizzo di destinazione per la route da aggiornare nella tabella route.

ENI - ID dell'interfaccia di rete dell'interfaccia Gigabit CSR 1000v alla quale viene instradato il traffico.
Ad esempio, se CSRHA fallisce, CSRHA1 prende il controllo e aggiorna la route nella tabella di route AWS in modo che punti al proprio ENI.

REGION - Area AWS di CSR 1000v.

Restrizioni

- Per le subnet private, non utilizzare l'indirizzo IP 10.0.3.0/24, in quanto viene utilizzato internamente su Cisco CSR 1000v for High Availability. Cisco CSR 1000v deve avere accessibilità pubblica a Internet per poter effettuare chiamate all'API REST che modifichino la tabella di routing AWS.

- Non inserire l'interfaccia gig1 di CSR1000v in un VRF. HA non funziona diversamente.

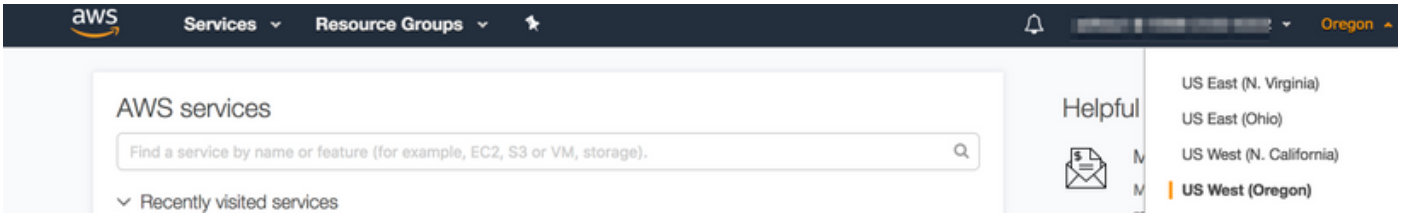
Configurazione

Il flusso generale della configurazione è quello di iniziare dalla funzionalità più completa (Area/VPC) e spostarsi verso la funzionalità più specifica (Interfaccia/subnet). Tuttavia, non esiste un ordine di configurazione specifico. Prima di iniziare, è importante comprendere la topologia.

> **Suggerimento**: Assegnare nomi a tutte le impostazioni (VPC, interfaccia, subnet, tabelle di routing e così via).

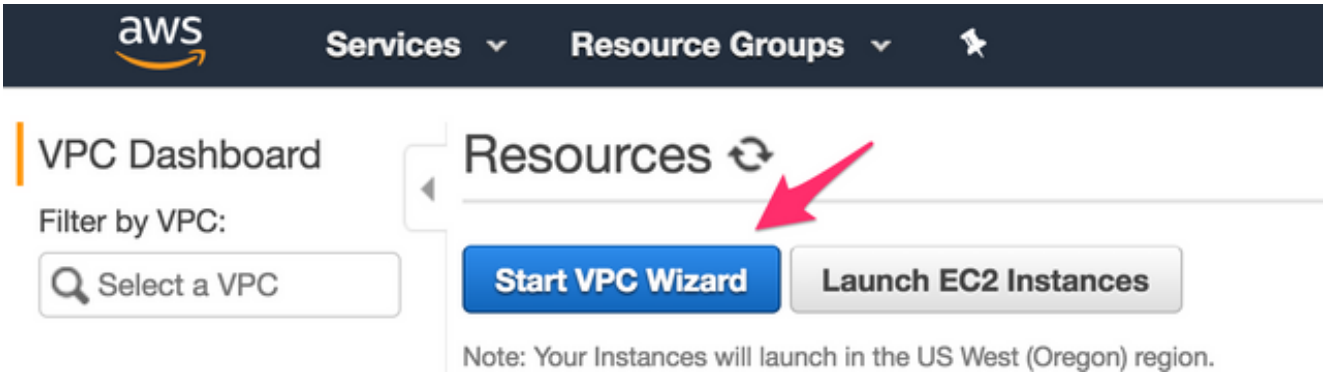
Passaggio 1. Scegliere un'area.

In questo esempio viene utilizzato US West (Oregon).

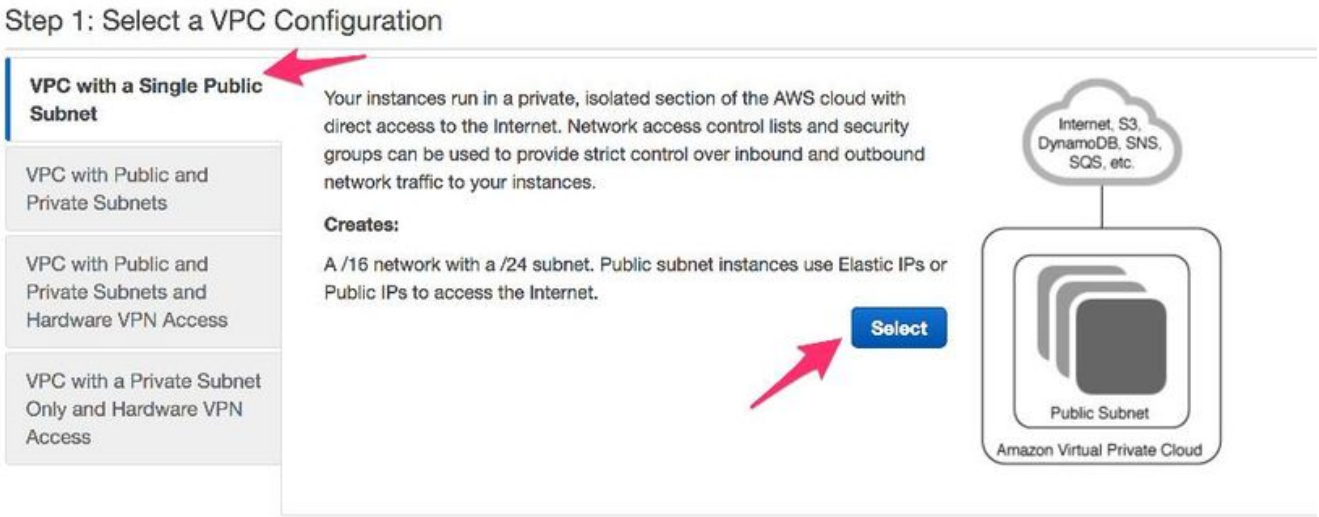


Passaggio 2. Creare un VPC.

1. Sulla console AWS, selezionare **VPC > VPC Dashboard > Start VPC Wizard** (Avvia procedura guidata VPC).



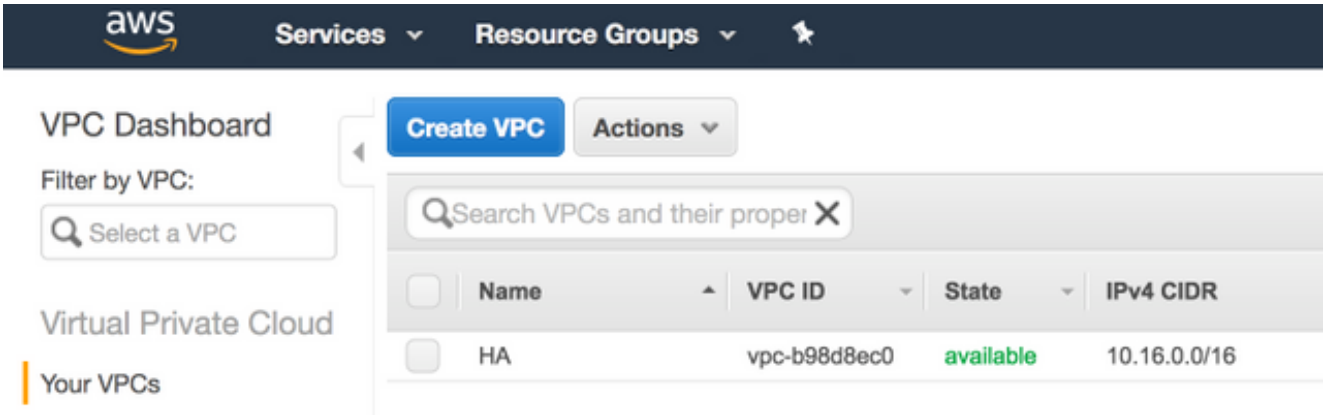
2. Scegliere VPC con una singola subnet pubblica.



3. Quando si crea un VPC, viene assegnata una rete /16 da utilizzare a piacimento.

4. Viene inoltre assegnata una subnet pubblica /24. Le istanze della subnet pubblica utilizzano indirizzi IP elastici o IP pubblici per consentire ai dispositivi di accedere a Internet.

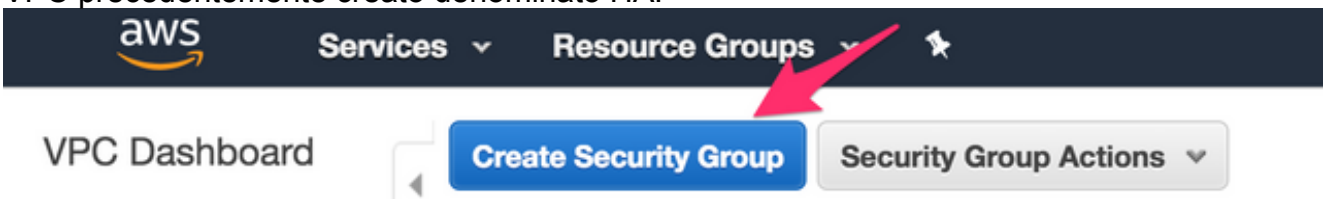
5. viene creato il vpc-b98d8ec0.



Passaggio 3. Creare un gruppo di sicurezza per il VPC.

I gruppi di sicurezza sono simili agli ACL per autorizzare o bloccare il traffico.

1. In Protezione, fare clic su **Gruppi di protezione** e **Creare il gruppo di protezione** associato al VPC precedentemente creato denominato HA.



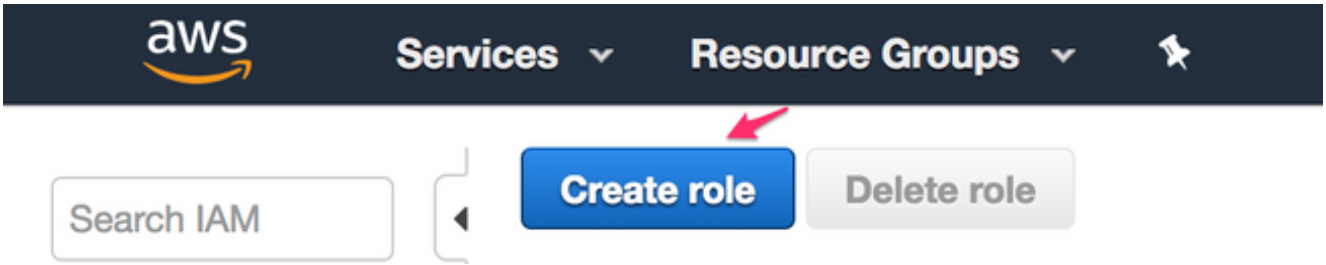
2. In Regole in entrata definire il traffico da consentire per sg-1cf47d6d. In questo esempio viene consentito Tutto il traffico.

Passaggio 4. Creare un ruolo IAM con un criterio e associarlo al VPC.

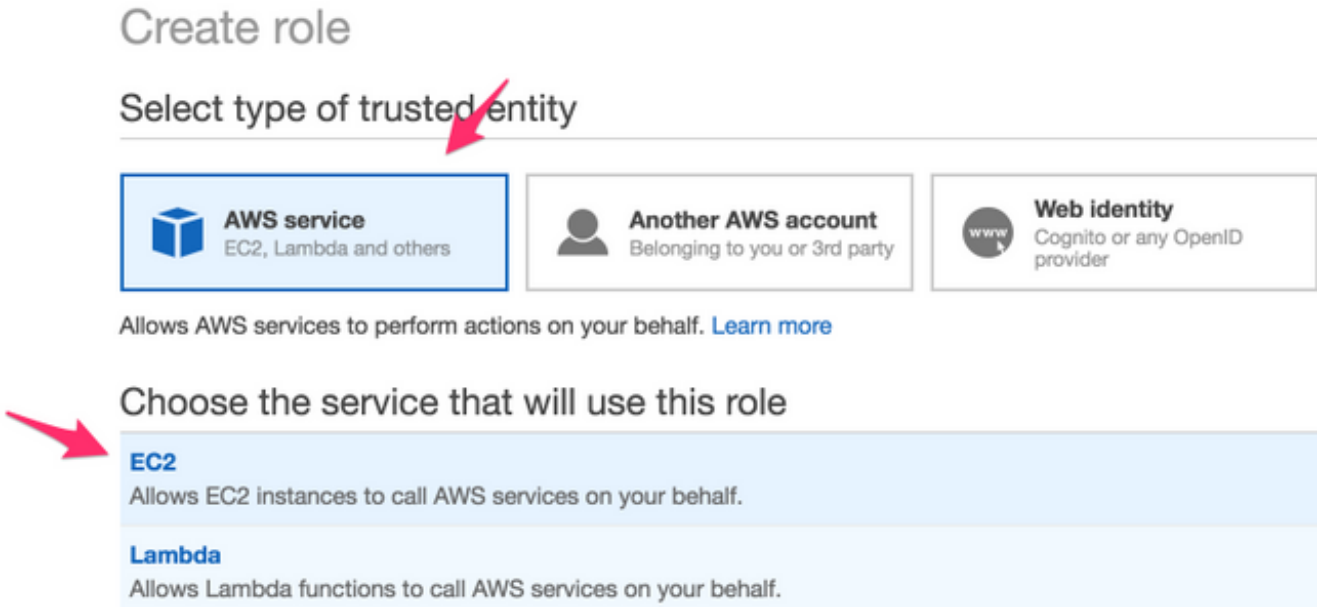
IAM concede al CSR l'accesso alle API Amazon.

CSR1000v viene utilizzato come proxy per chiamare i comandi API AWS per modificare la tabella di routing. Per impostazione predefinita, agli AMI non è consentito accedere alle API. Questa procedura consente di creare un ruolo IAM che viene utilizzato durante l'avvio di un'istanza di CSR. IAM fornisce le credenziali di accesso per i CSR per utilizzare e modificare le API AWS.

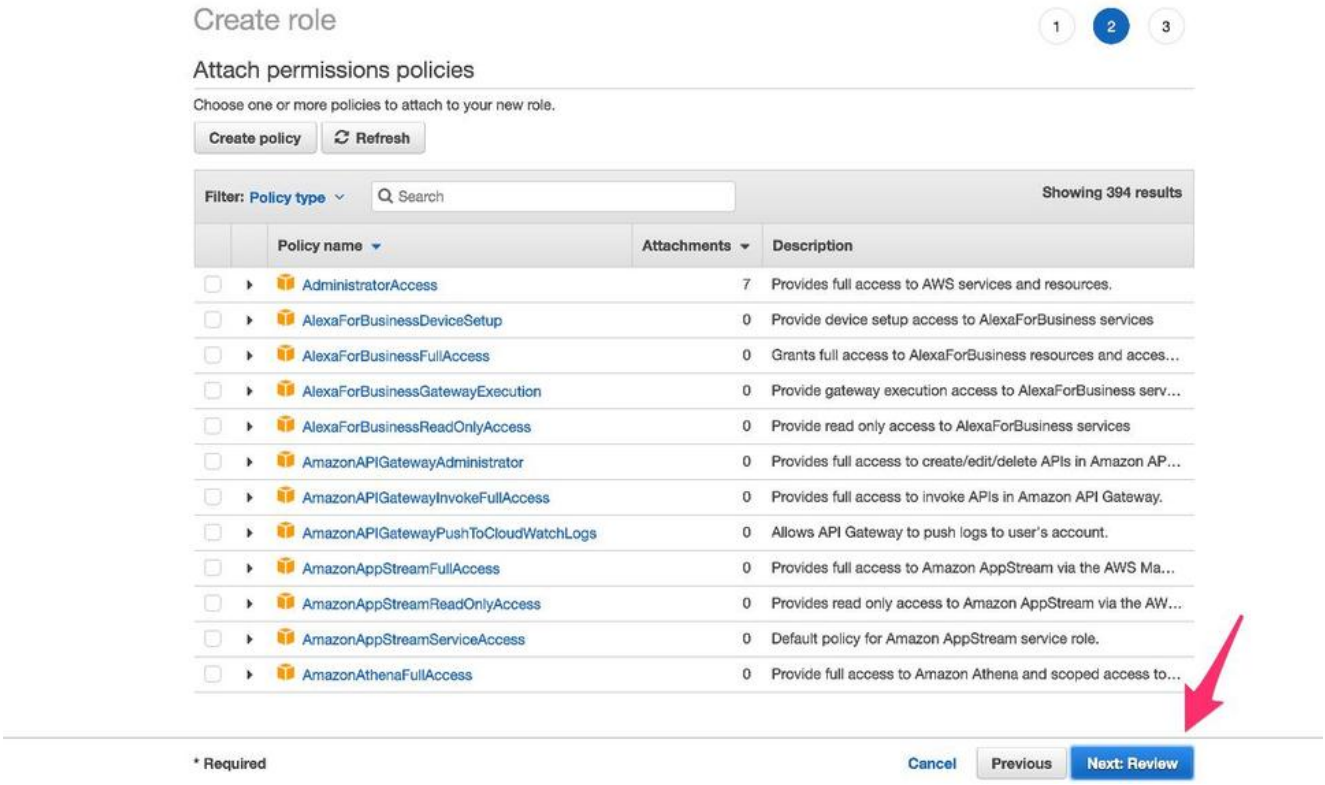
1. Crea ruolo IAM. Passare al dashboard IAM e selezionare **Ruoli > Crea ruolo**, come mostrato nell'immagine.



2. Come mostrato nell'immagine, consentire all'istanza EC2 di chiamare AWS per conto dell'utente.

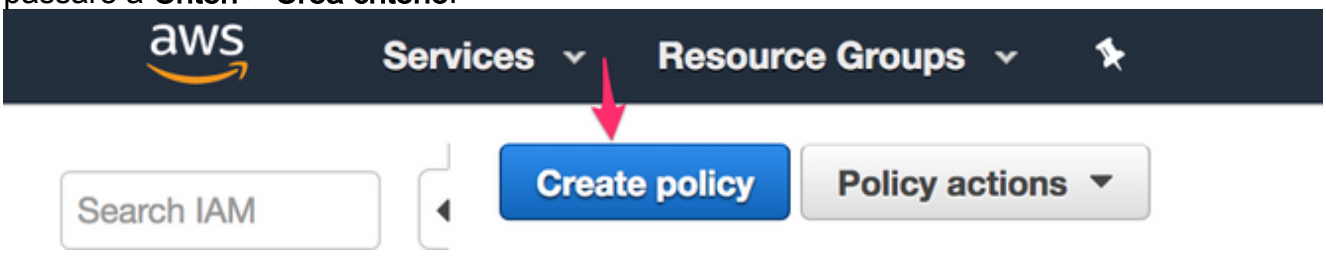


3. Creare un ruolo e fare clic su **Avanti: Rivedere**, come mostrato nell'immagine.

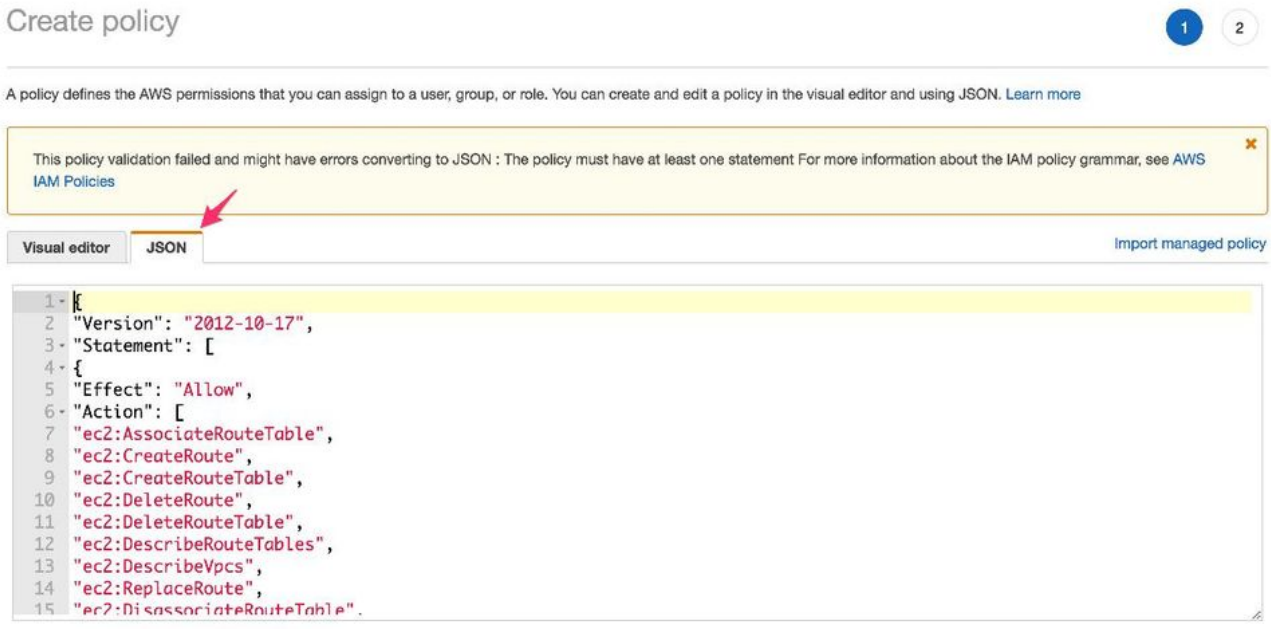


4. Assegnare un nome al ruolo. Per questo esempio, come mostrato nell'immagine, il nome del ruolo è **routetablechange**.

5. Èquindi necessario creare un criterio e associarlo al ruolo creato in precedenza. IAM e passare a **Criteri > Crea criterio**.

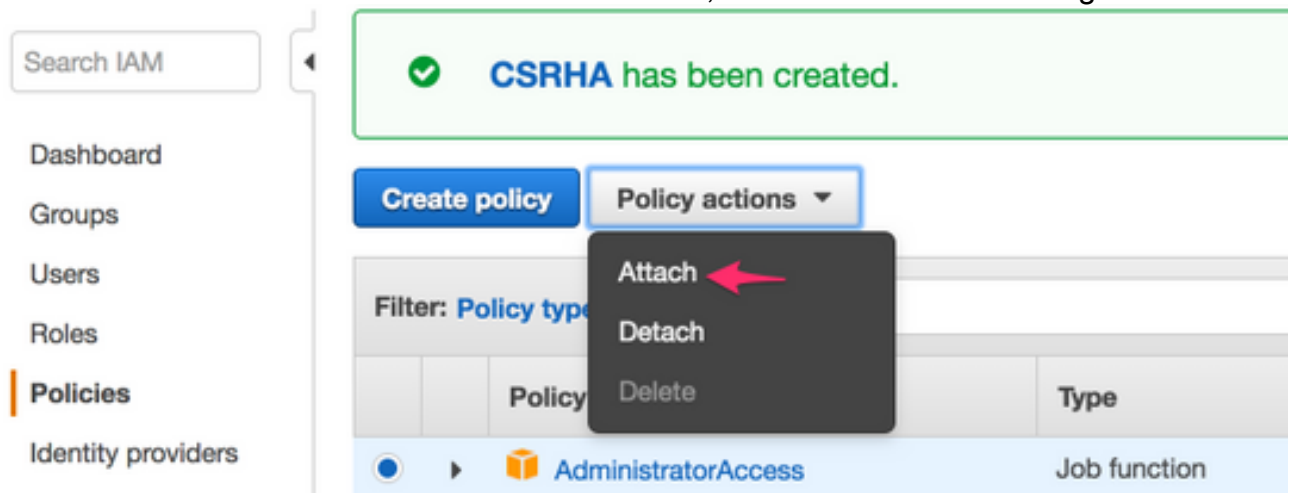



```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:AssociateRouteTable",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:DeleteRoute",
"ec2:DeleteRouteTable",
"ec2:DescribeRouteTables",
"ec2:DescribeVpcs",
"ec2:ReplaceRoute",
"ec2:DisassociateRouteTable",
"ec2:ReplaceRouteTableAssociation"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

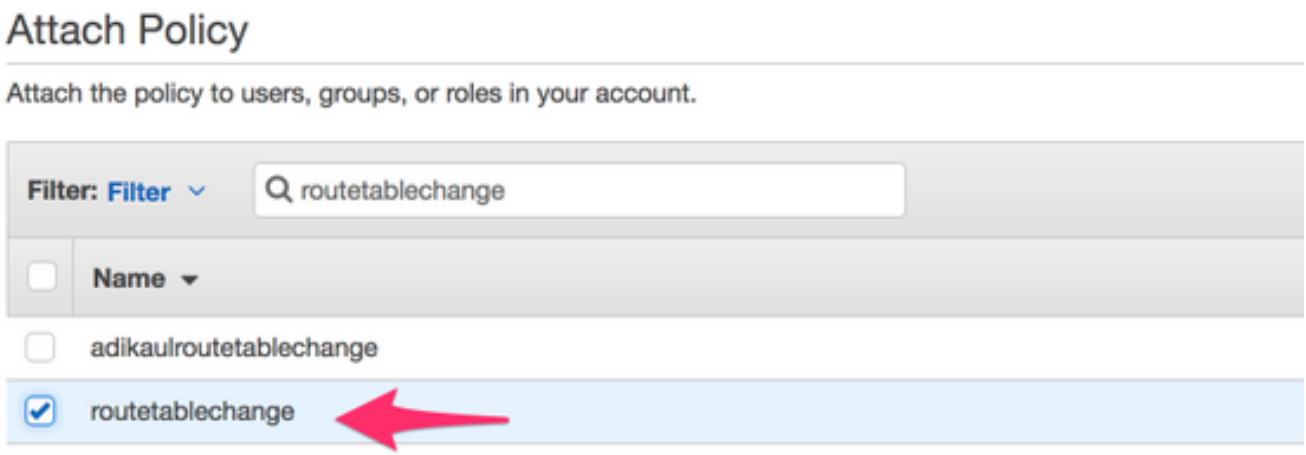


6. Assegnare un nome al criterio e associarlo al ruolo creato. Per questo esempio, il nome del

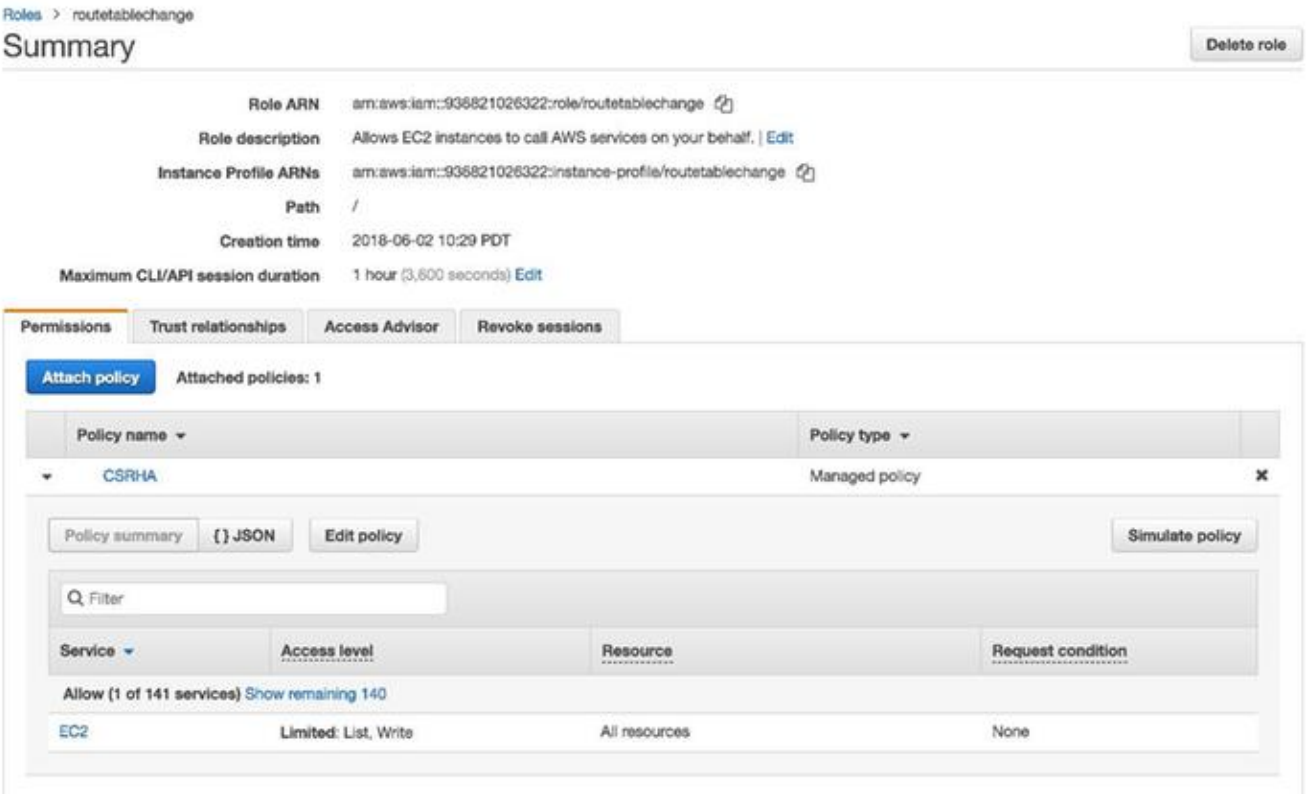
criterio è CSRHA con accesso come amministratore, come mostrato nell'immagine.



7. Come mostrato nell'immagine, associare il criterio al ruolo creato denominato **routetablechange**.



8. Riepilogo.



Passaggio 5. Avviare CSR1000v con il ruolo AMI creato e associare le subnet

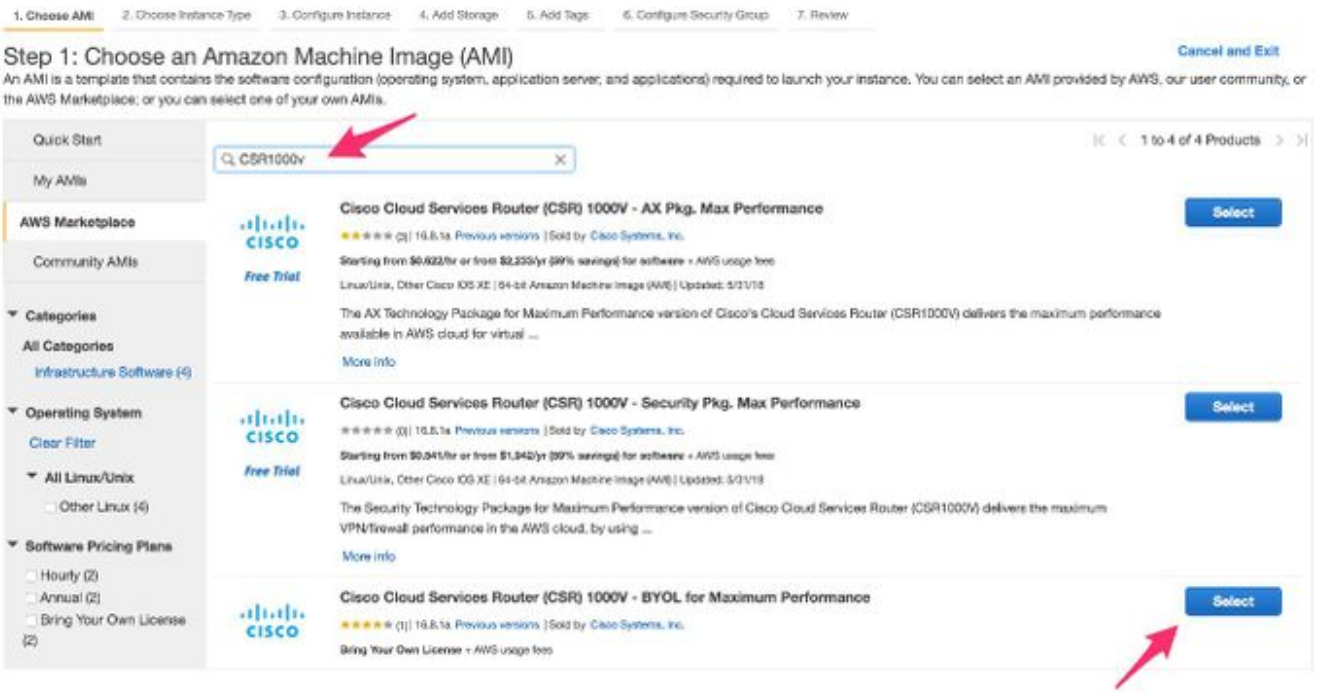
pubbliche/private.

Ogni router CSR100v ha due interfacce (una pubblica e una privata) e si trova nella propria zona di disponibilità. Ciascun CSR può essere considerato come un centro dati separato.

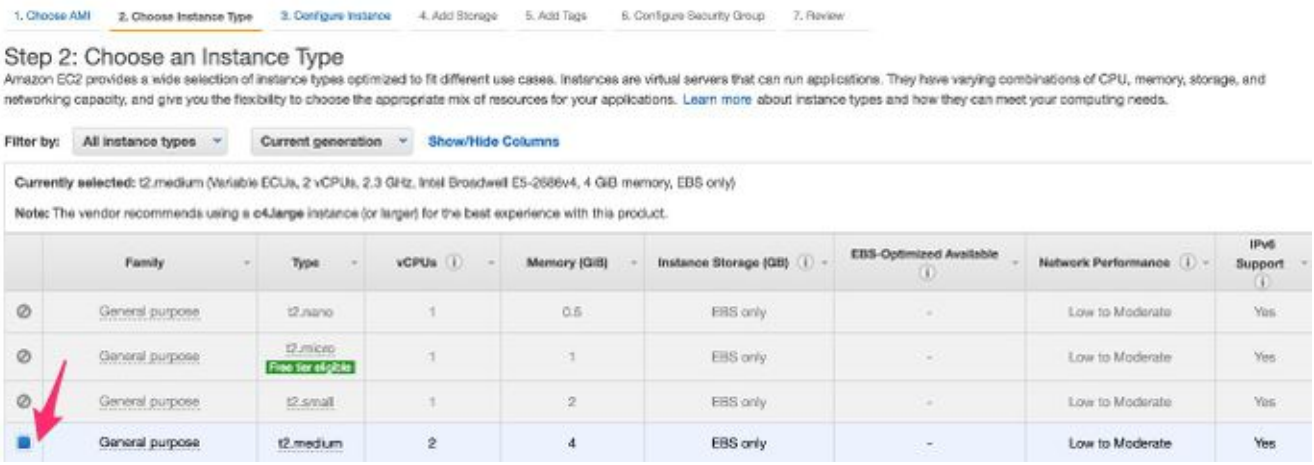
1. Sulla console AWS, selezionare **EC2**, quindi fare clic su **Avvia istanza**.

2. Selezionare AWS Marketplace.

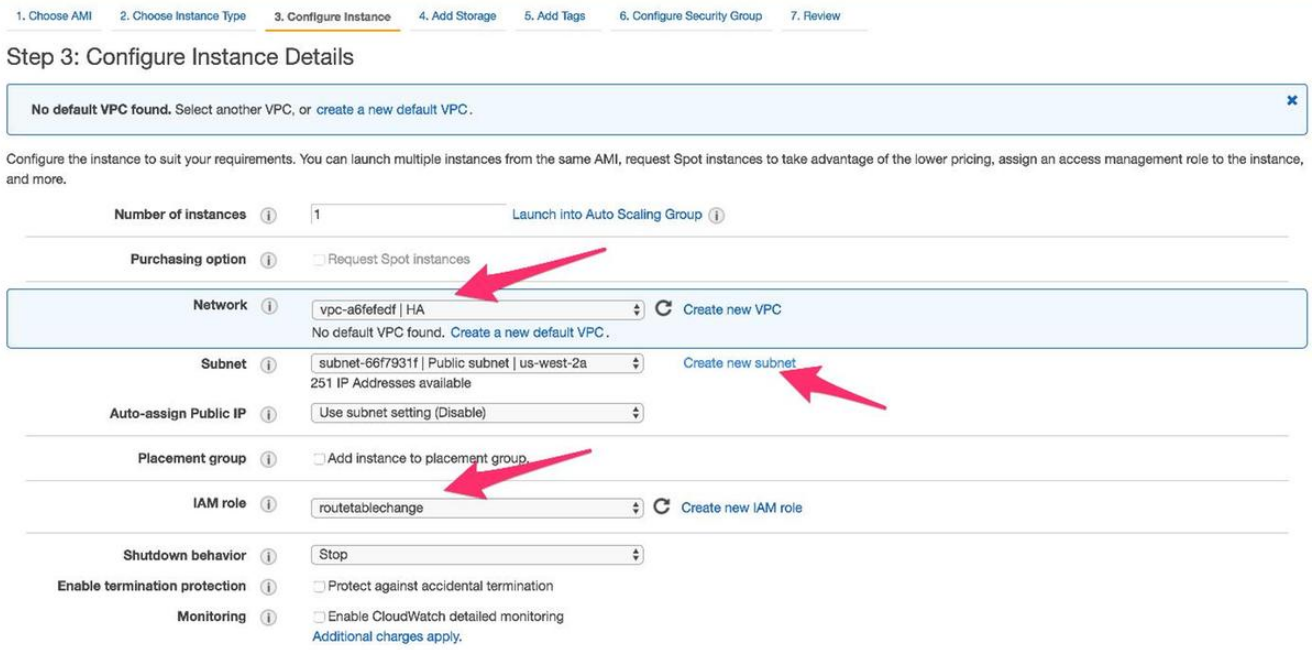
3. Immettere CSR1000v e per questo esempio si usa Cisco Cloud Services Router (CSR) 1000V - BYOL per ottenere le massime prestazioni.



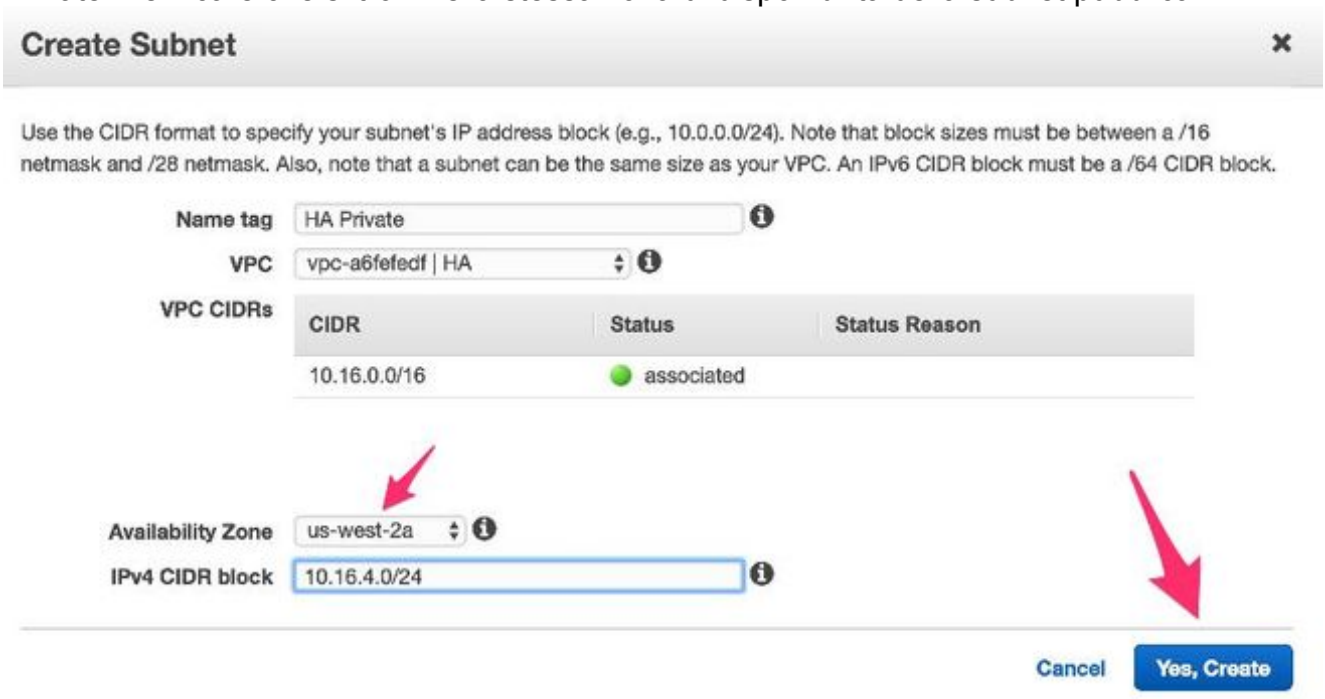
4. Scegliere un tipo di istanza. Per questo esempio, il tipo selezionato è **t2.medium**.



5. Mentre l'istanza è configurata, è necessario assicurarsi di selezionare il VPC creato in precedenza insieme al ruolo IAM indicato sopra. Inoltre, creare una subnet privata che si associa all'interfaccia del lato privato.



6. Fare clic su Crea nuova subnet per subnet privata. Per questo esempio, il tag Name è HA Private. Verificare che si trovi nella stessa zona di disponibilità della subnet pubblica.

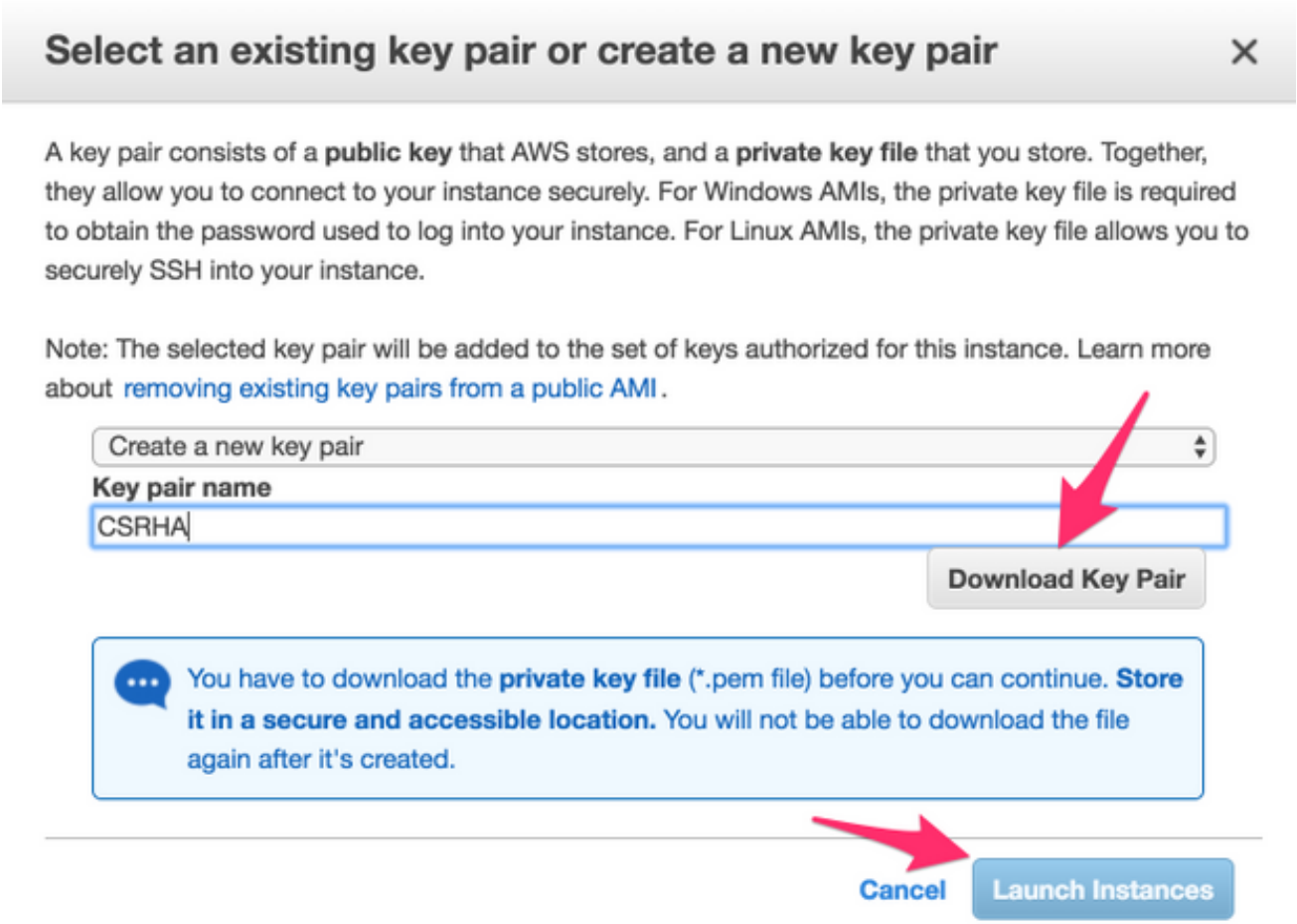


7. Scorrere verso il basso e in Configura dettagli istanza fare clic su **Aggiungi dispositivo**, come mostrato nell'immagine.

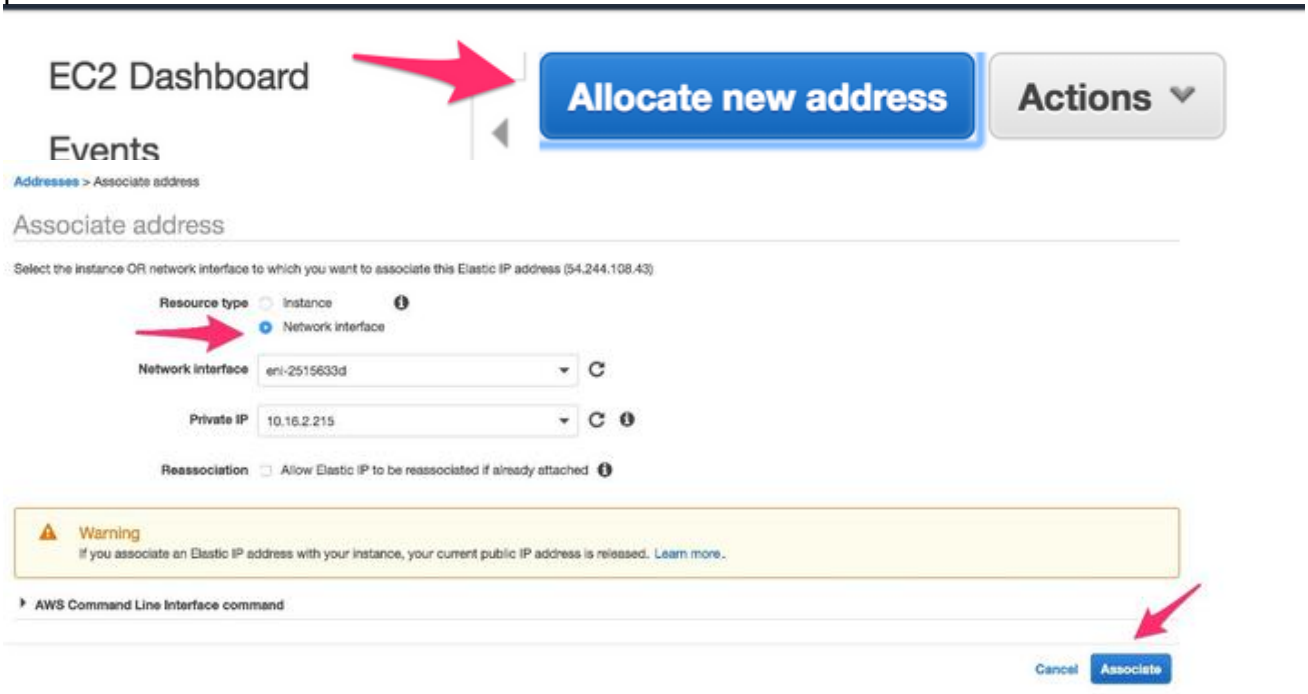
8. Dopo aver aggiunto l'interfaccia secondaria, associare la subnet privata creata chiamata HA Private. Eth0 è l'interfaccia pubblica e Eth1 è l'interfaccia privata. **Nota:** La subnet creata nel passaggio precedente potrebbe non essere visualizzata in questo elenco a discesa. Potrebbe essere necessario aggiornare o annullare la pagina e ricominciare per visualizzare la
subnet.

9. Selezionare il gruppo di sicurezza creato in VPC e assicurarsi che le regole siano definite correttamente.

10. Creare una nuova coppia di chiavi e assicurarsi di scaricare la chiave privata. È possibile riutilizzare un tasto per ogni dispositivo. **Nota:** Se viene persa la chiave privata, non sarà possibile accedere di nuovo al CSR. Non è disponibile alcun metodo per ripristinare le chiavi.

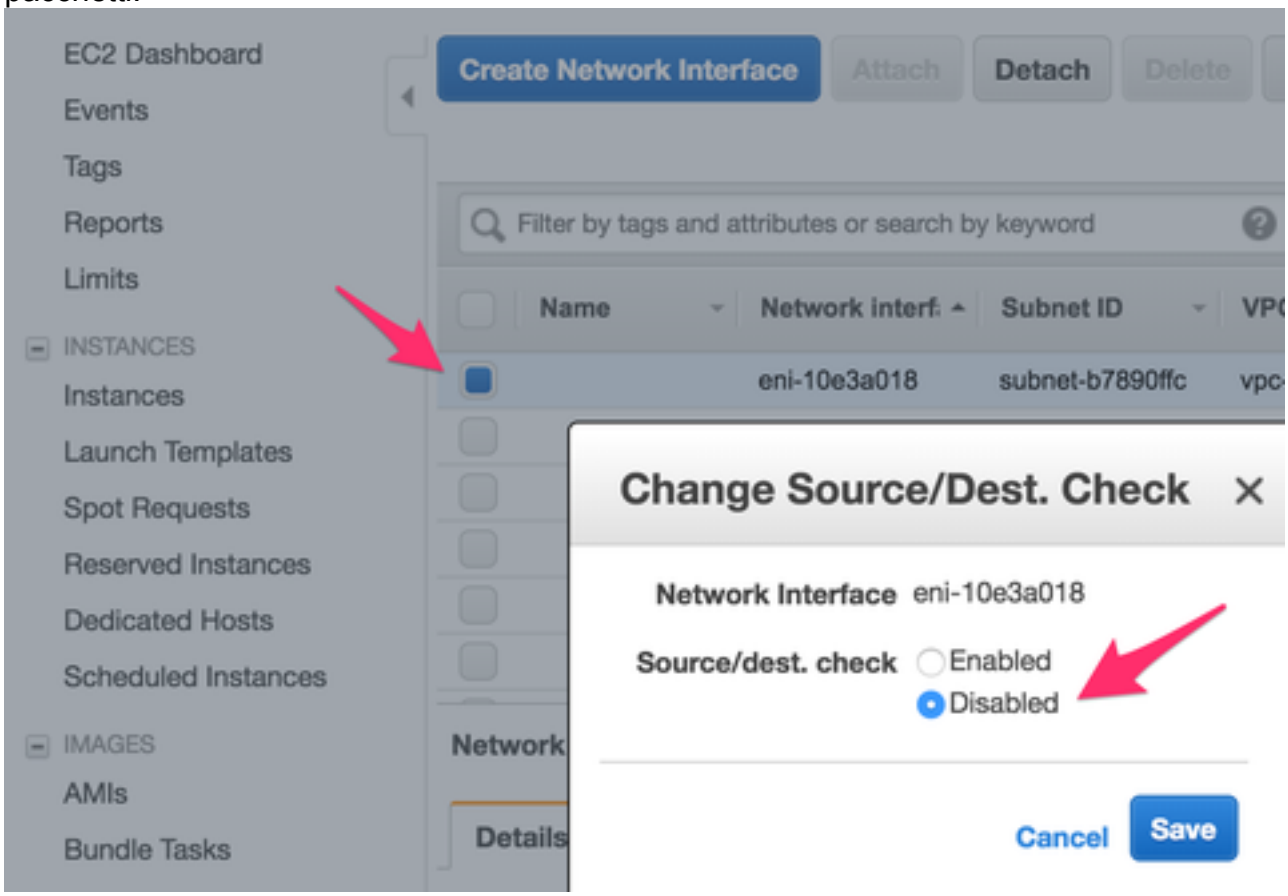


11. Associare l'indirizzo IP elastico all'interfaccia ENI dell'interfaccia pubblica per l'istanza creata e selezionare **Console AWS > Gestione EC2 > Sicurezza di rete > Indirizzi IP elastici**. **Nota:** La terminologia pubblica/privata può confondere l'utente. Ai fini dell'esempio, la definizione di interfaccia pubblica è Eth0, che è l'interfaccia con connessione Internet. Dal punto di vista di AWS, la nostra interfaccia pubblica è il loro ip privato.

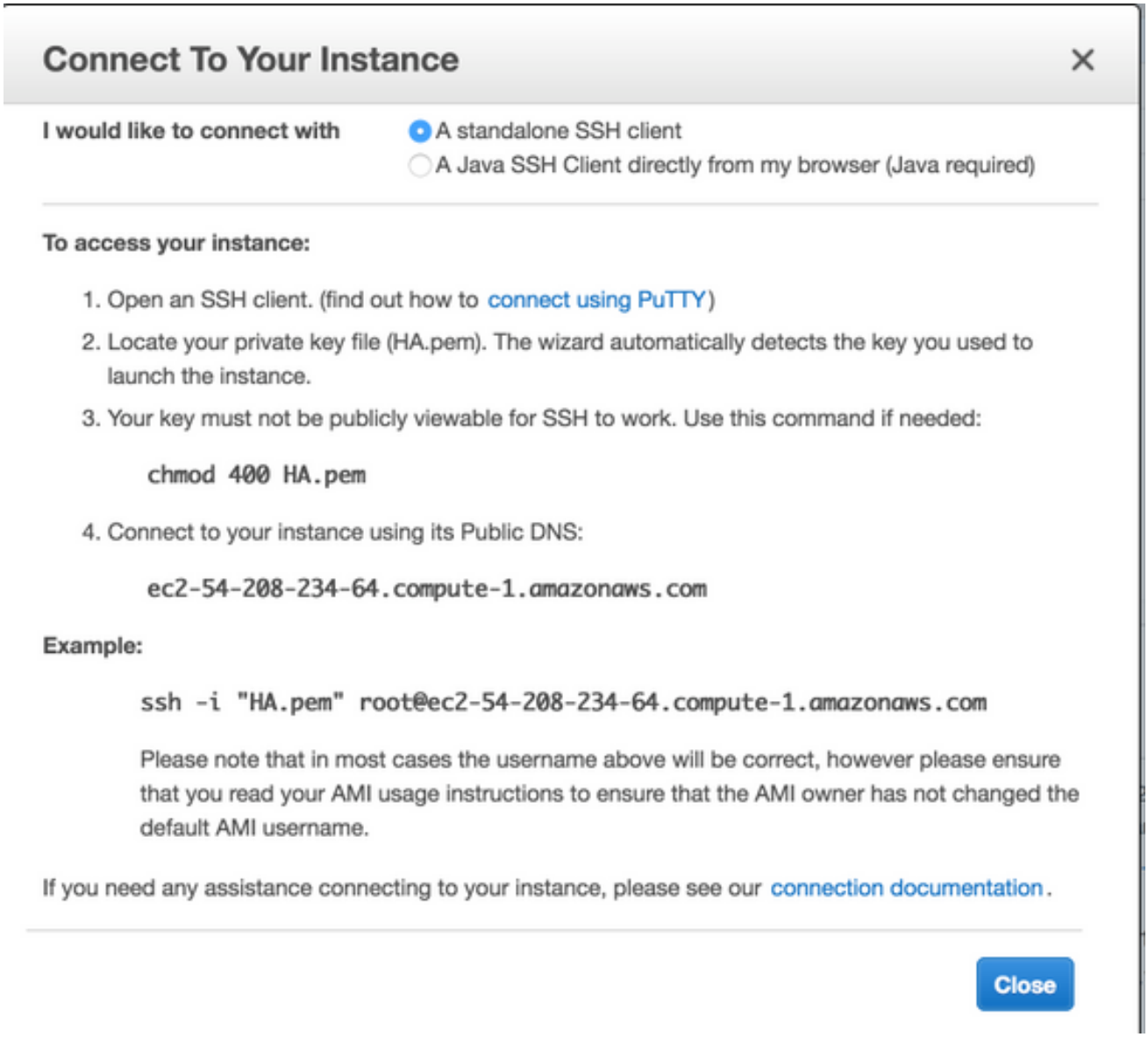


12. Disabilitare il controllo origine/destinazione mentre si passa a **EC2 > Interfacce di rete**. Verificare ogni ENI per il controllo origine/destinazione. Per impostazione predefinita, tutti gli ENI vengono forniti con questo controllo origine/destinazione abilitato. Funzione anti-

spoofing che consente di evitare che un ENI venga sovraccaricato di traffico non effettivamente destinato a tale scopo, verificando che l'ENI sia la destinazione del traffico prima di inoltrarlo. Raramente il router è la destinazione effettiva di un pacchetto. Questa funzionalità deve essere disabilitata su tutti gli ENI di transito CSR o non può inoltrare pacchetti.



13. Collegarsi al CSR1000v. **Nota:** Il nome utente fornito da AWS a SSH nel CSR1000v potrebbe essere erroneamente elencato come root. Se necessario, passare a ec2-user.**Nota:** È necessario essere in grado di eseguire il ping dell'indirizzo DNS su SSH. Ecco il sito ec2-54-208-234-64.compute-1.amazonaws.com. Verificare che la subnet pubblica/eni del router sia associata alla tabella di route pubblica. Andare brevemente al passaggio 8 per informazioni su come associare la subnet alla tabella di routing.



Passaggio 6. Ripetere il passaggio 5 e creare la seconda istanza di CSR1000v per HA.

Subnet pubblica: 10.16.1.0/24

Subnet privata: 10.16.5.0/24

Se non è possibile eseguire il ping dell'indirizzo IP elastico del nuovo AMI, andare brevemente al passaggio 8 e verificare che la subnet pubblica sia associata alla tabella di routing pubblica.

Passaggio 7. Ripetere il passaggio 5 e creare una VM (Linux/Windows) da AMI Marketplace.

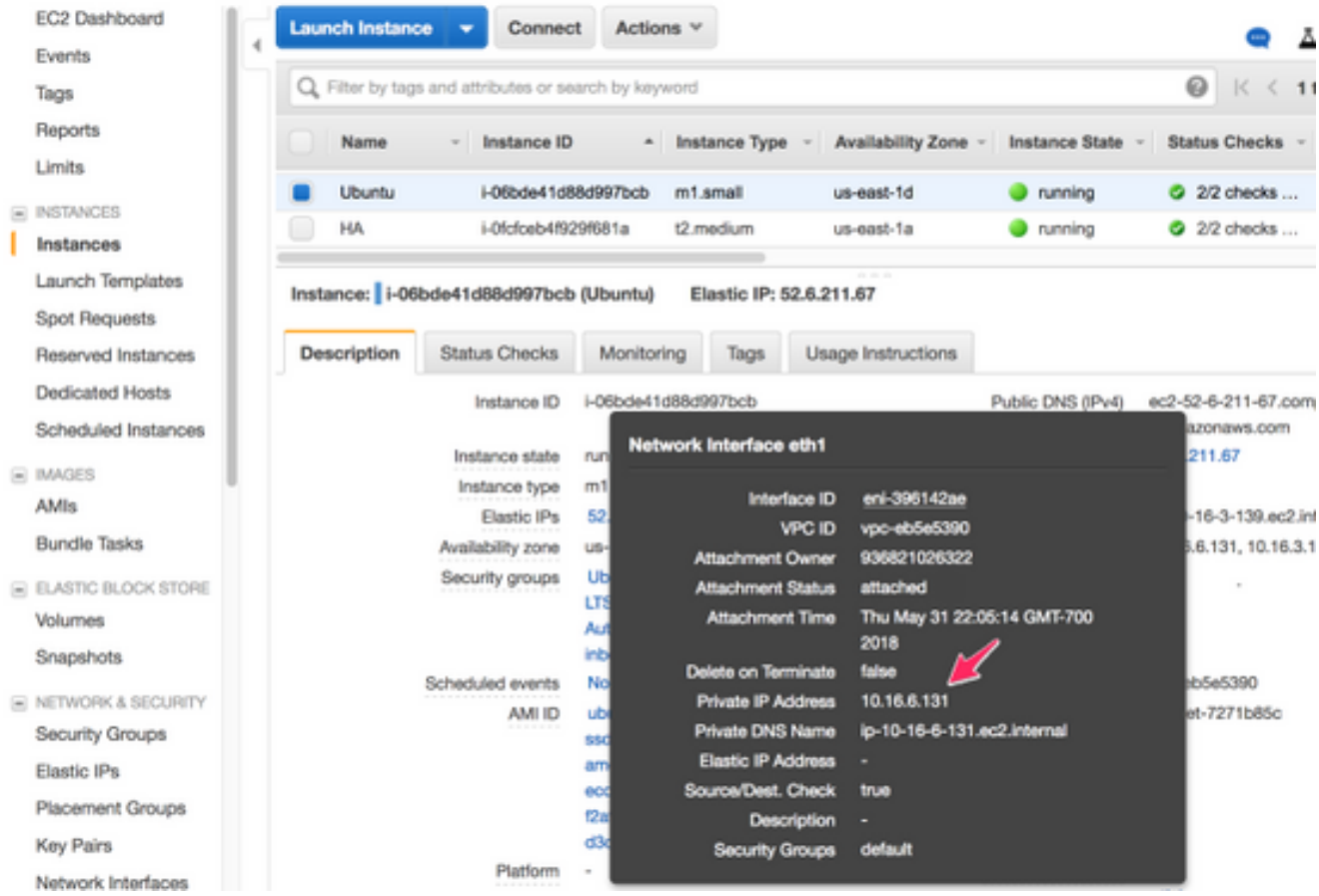
Per questo esempio, utilizzare Ubuntu Server 14.04 LTS sul marketplace.

Subnet pubblica: 10.16.2.0/24

Subnet privata: 10.16.6.0/24

Se non è possibile eseguire il ping dell'indirizzo IP elastico del nuovo AMI, andare brevemente al passaggio 8 e verificare che la subnet pubblica sia associata alla tabella di routing pubblica.

1. Eth0 viene creato per default per l'interfaccia pubblica. Creare una seconda interfaccia denominata eth1 per la subnet privata.



2. L'indirizzo IP configurato in Ubuntu è l'interfaccia privata eth1 assegnata da 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. Invertire l'interfaccia o riavviare la macchina virtuale.

```
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. Eseguire il ping 8.8.8.8 per la prova. Accertarsi che la route 8.8.8.8 sia stata aggiunta in ciascuna fase 7.

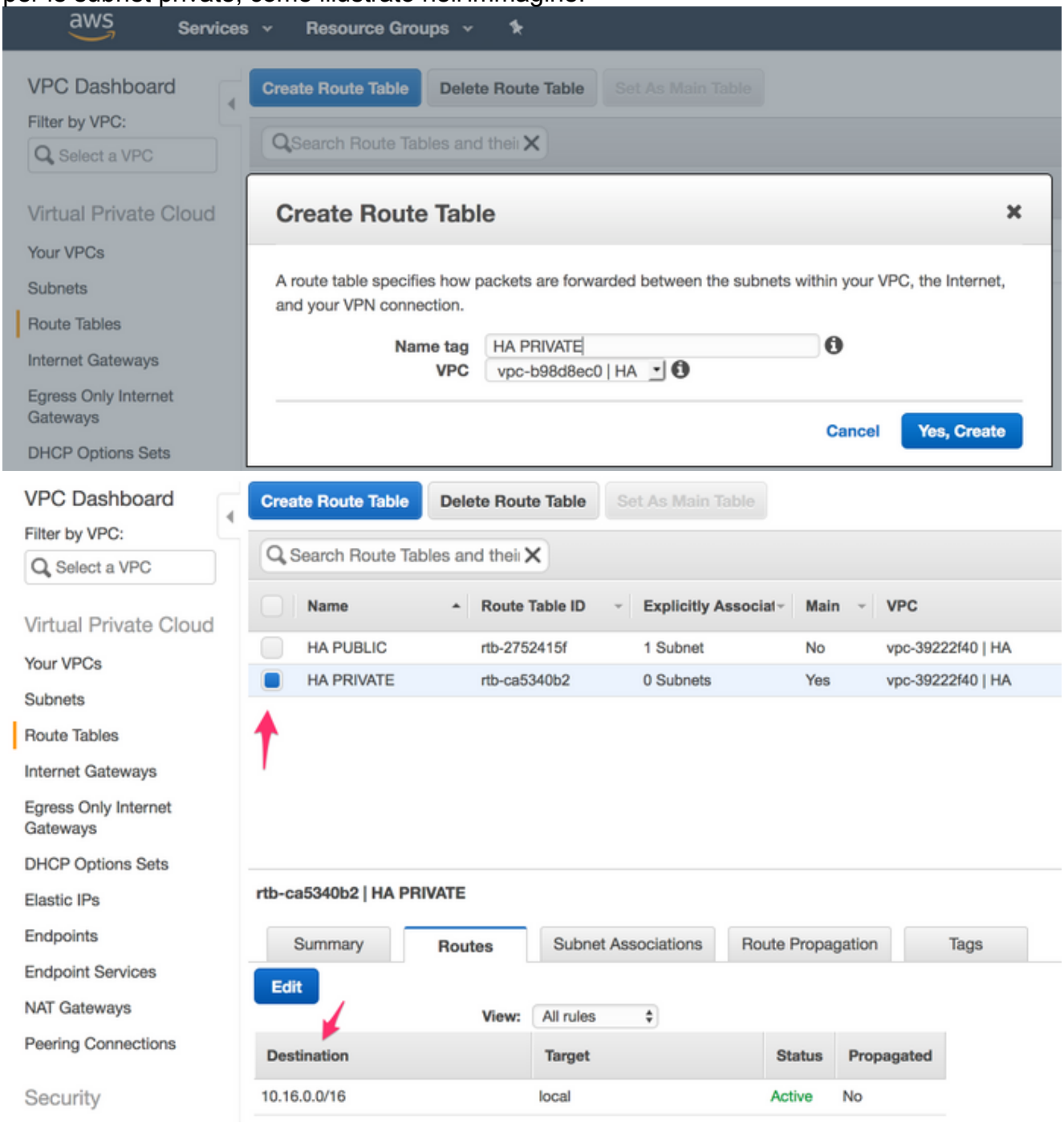
```
ubuntu@ip-10-16-2-139:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.16.2.1 0.0.0.0 UG 0 0 0 eth0
8.8.8.8 10.16.6.1 255.255.255.255 UGH 0 0 0 eth1     <--------------
10.16.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.16.6.0 0.0.0.0 255.255.255.0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

Se 8.8.8.8 non è elencato nella tabella, aggiungerlo manualmente:

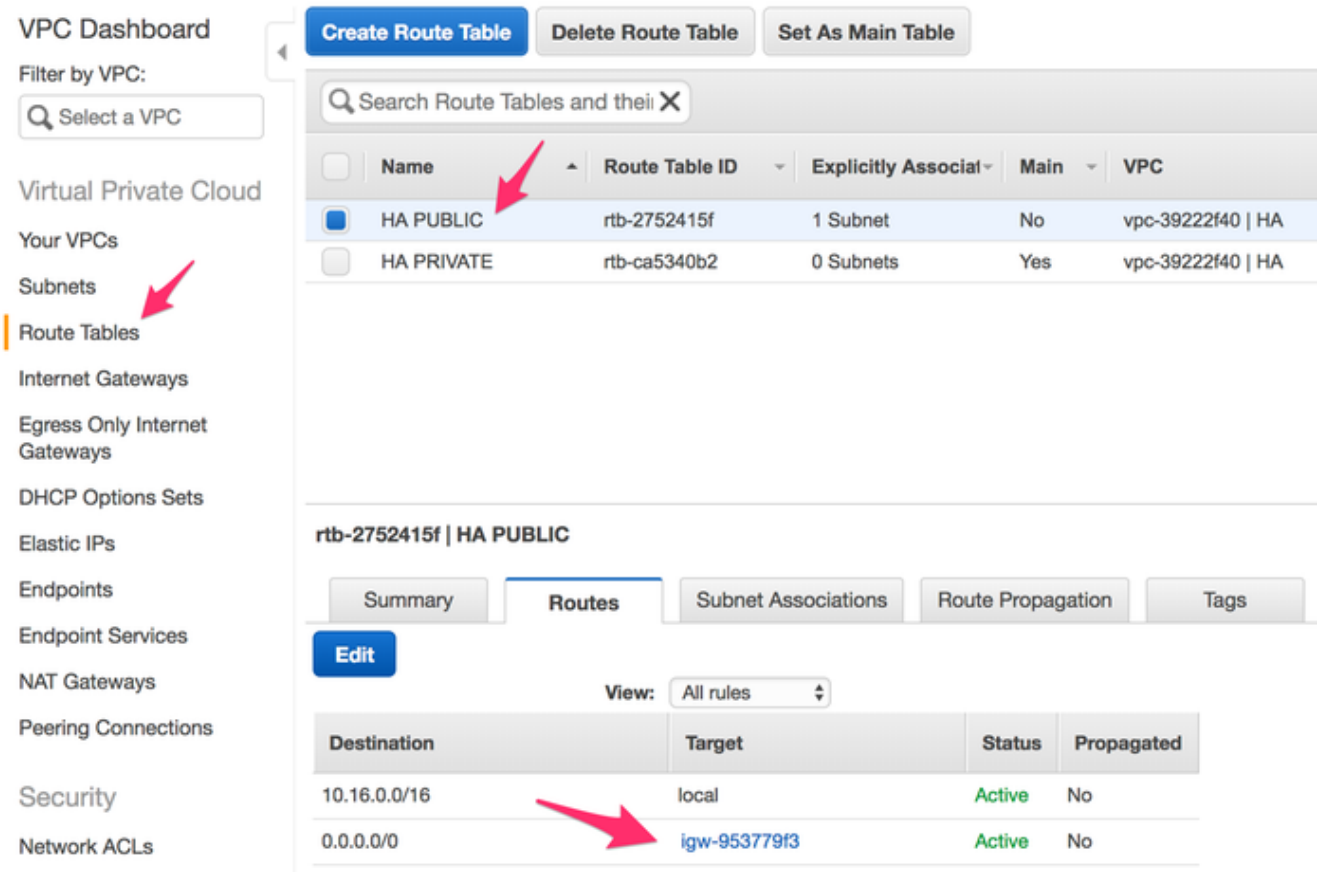
```
ubuntu@ip-10-16-2-139:~$ sudo route add -host 8.8.8.8 gw 10.16.6.1 dev eth1
```

Passaggio 8. Configurare le tabelle di route private e pubbliche.

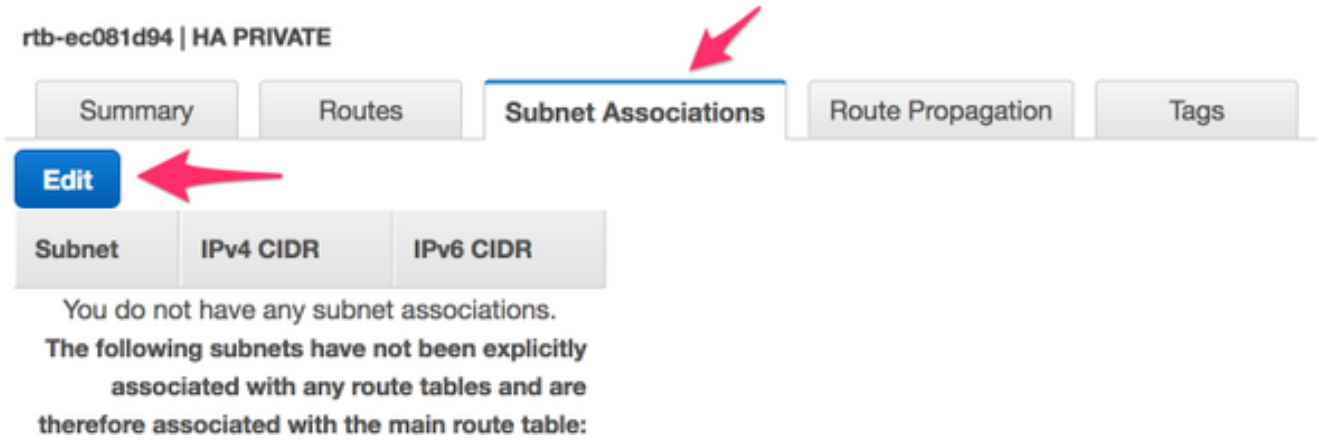
1. Quando si crea una VPC tramite la procedura guidata nel passaggio 2, vengono create automaticamente due tabelle di route. Se esiste una sola tabella di routing, crearne un'altra per le subnet private, come illustrato nell'immagine.



2. Di seguito è riportata una vista delle due tabelle di route. La tabella di route PUBLIC dispone di un gateway Internet (igw-95377973) collegato automaticamente. Etichettare queste due tabelle di conseguenza. La tabella PRIVATE NON deve contenere questa route.



3. Associare tutte le 6 subnet alla tabella di route appropriata 3 Le interfacce pubbliche sono associate alla tabella di route pubblica:Subnet pubbliche: 10.16.0.0/24, 10.16.1.0/24, 10.16.2.0/24 3 Le interfacce private sono associate alla tabella di route privata:Subnet private: 10.16.4.0/24, 10.16.5.0/24, 10.16.6.0/24



Passaggio 9. Configurare Network Address Translation (NAT) e il tunnel GRE con BFD e qualsiasi protocollo di routing.

Configurare il tunnel GRE (Generic Routing Encapsulation) tramite gli IP elastici del CSR 1000v (opzione consigliata per evitare problemi di rinnovo del lease DHCP e il rilevamento di errori falsi). Se è necessaria una convergenza più rapida, i valori BFD (Biderection Forwarding Detection) possono essere configurati in modo da essere più aggressivi di quelli mostrati in questo esempio. Tuttavia, questo può portare ad eventi BFD peer down durante la connettività intermittente. I valori di questo esempio rilevano un errore del peer entro 1,5 secondi. Tra il momento in cui si esegue il comando AWS API e il momento in cui entrano in vigore le modifiche alla tabella di routing VPC, è presente un ritardo variabile di circa pochi secondi.

- Configurazione su CSRHA

  GRE e BFD: utilizzati per rispettare le condizioni per il failover HA

```
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 e routing - Utilizzato per la raggiungibilità Internet delle VM tramite l'interfaccia privata

```
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
```

- Configurazione su CSRHA1

  GRE e BFD: utilizzati per rispettare le condizioni per il failover HA

```
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 e routing - Utilizzato per la raggiungibilità Internet delle VM tramite l'interfaccia privata

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

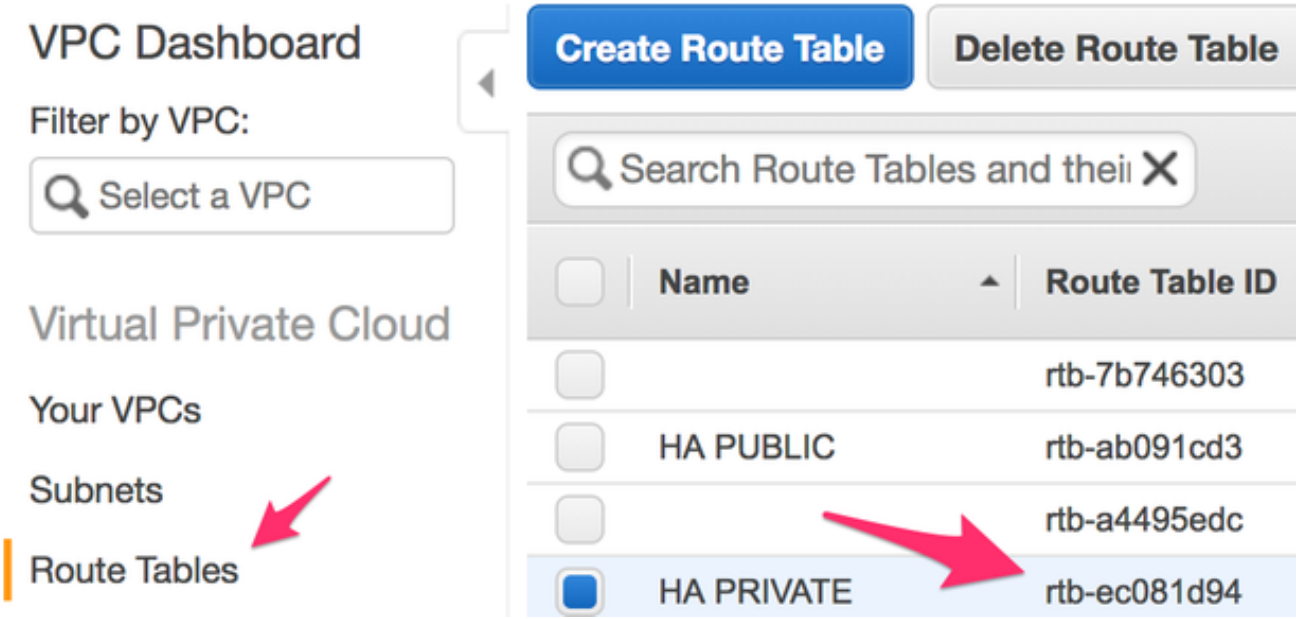
```
  no shutdown
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!
access-list 10 permit 10.16.6.0 0.0.0.255
!
ip route 10.16.6.0 255.255.255.0 GigabitEthernet2 10.16.5.1
```

Passaggio 10. Configurare l'alta disponibilità (Cisco IOS XE Denali 16.3.1a o versioni successive).

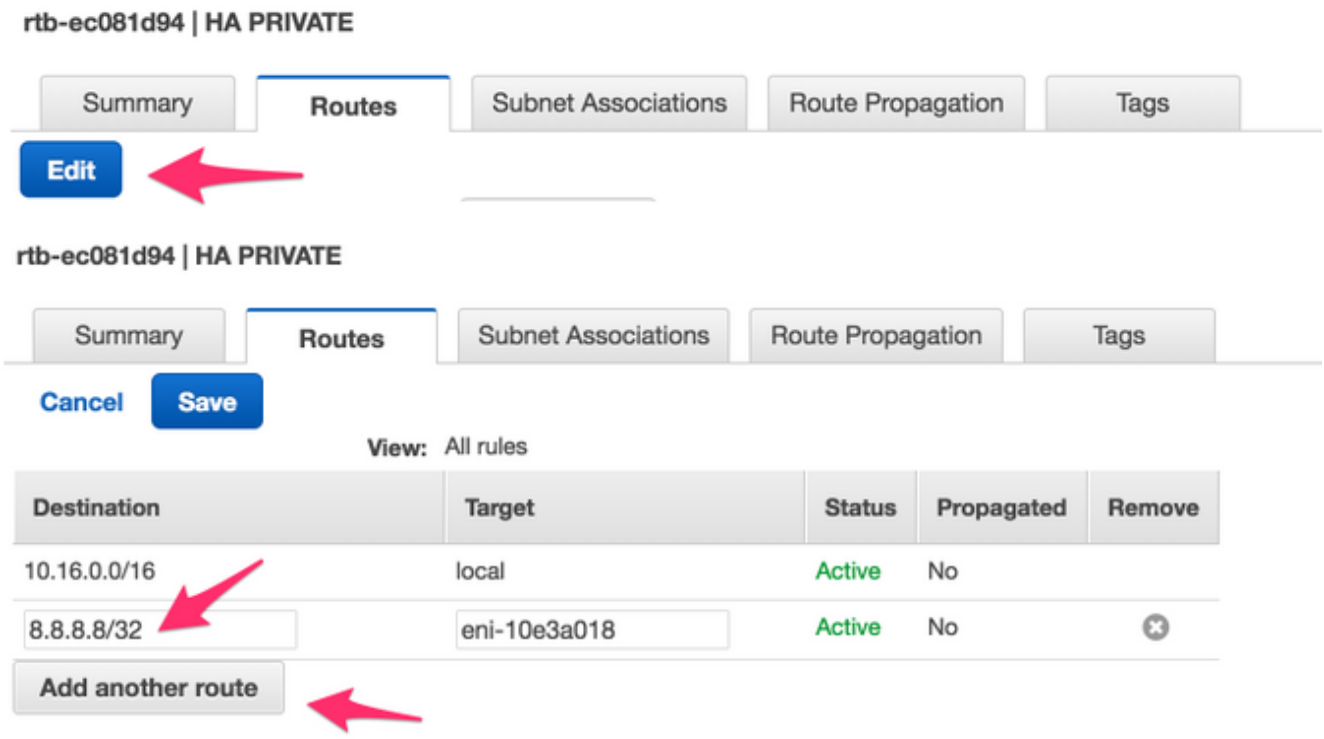
Monitorare gli eventi peer down BFD configurando ogni CSR 1000v con il comando cloud provider aws specificato di seguito. Utilizzare questo comando per definire le modifiche di routing a (VPC) Route-table-id, Network-interface-id e CIDR dopo il rilevamento di un errore AWS HA, ad esempio un peer down BFD.

```
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
```

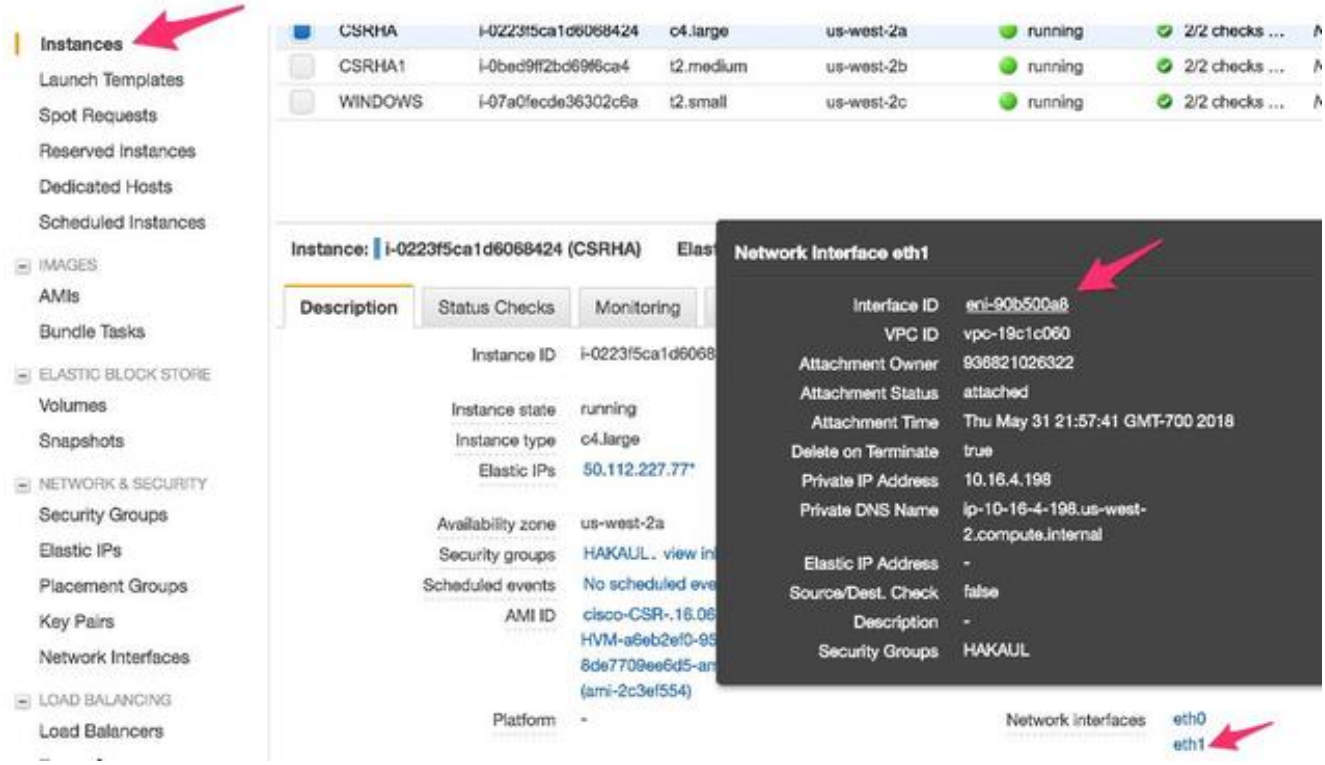
1. L'indirizzo IP peer #bfd è l'indirizzo IP del tunnel peer.
   ```
   CSRHA#show bfd neighbors

   IPv4 Sessions
   NeighAddr LD/RD RH/RS State Int
   192.168.1.2 4097/4097 Up Up Tu1
   ```
2. Il nome della tabella #route-table si trova nella console AWS, selezionare **VPC > Route Tables**. Questa azione altera la tabella di route privata.



3. Il #cidr ip ipaddr/prefix è l'indirizzo di destinazione per la route da aggiornare nella tabella di route. In Console AWS, selezionare **VPC > Tabelle di route**. Scorrere verso il basso, fare clic su **Modifica**, quindi su **Aggiungi un'altra route**. Aggiungere l'indirizzo di destinazione del test 8.8.8.8 e l'ENI privato di CSRHA.



4. Il nome #eni elastic-network-intf viene trovato nell'istanza EC2. Fare clic sull'interfaccia privata eth1 per ciascuno dei CSR corrispondenti e utilizzare l'ID interfaccia.



5. Il nome #region è il nome di codice trovato nel documento AWS. L'elenco potrebbe cambiare o aumentare. Per trovare gli ultimi aggiornamenti, visitare il documento [Regione e zone di disponibilità di] 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)

Esempio di configurazione della ridondanza su 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
```

Esempio di configurazione della ridondanza su 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
```

Verifica dell'elevata disponibilità

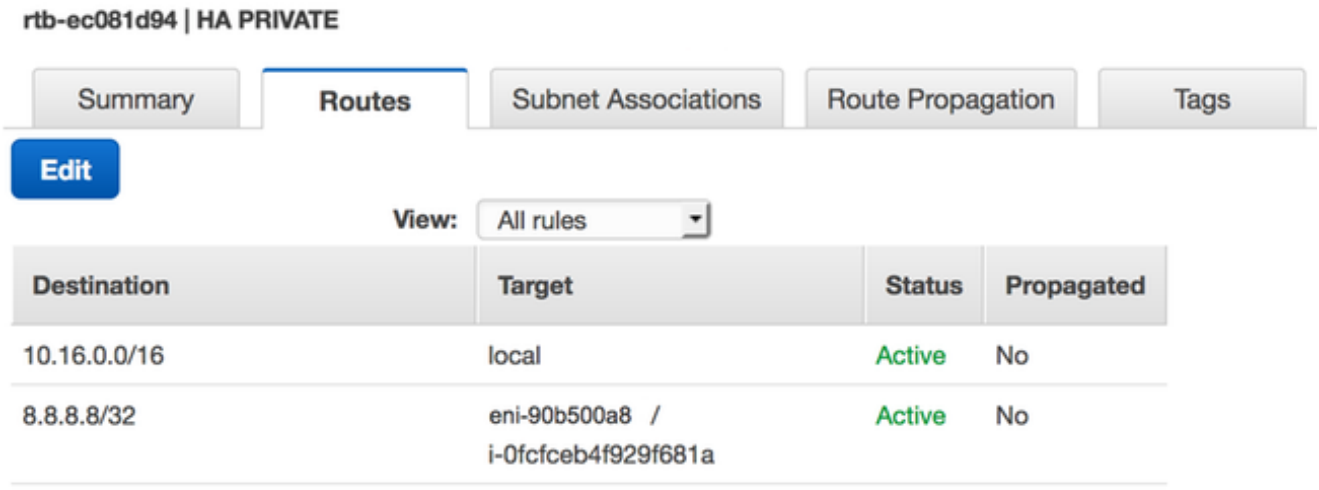
1. Verificare le configurazioni BFD e cloud.

```
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. Eseguire un ping continuo dalla macchina virtuale alla destinazione. Accertarsi che il ping abbia luogo tramite l'interfaccia privata 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
```

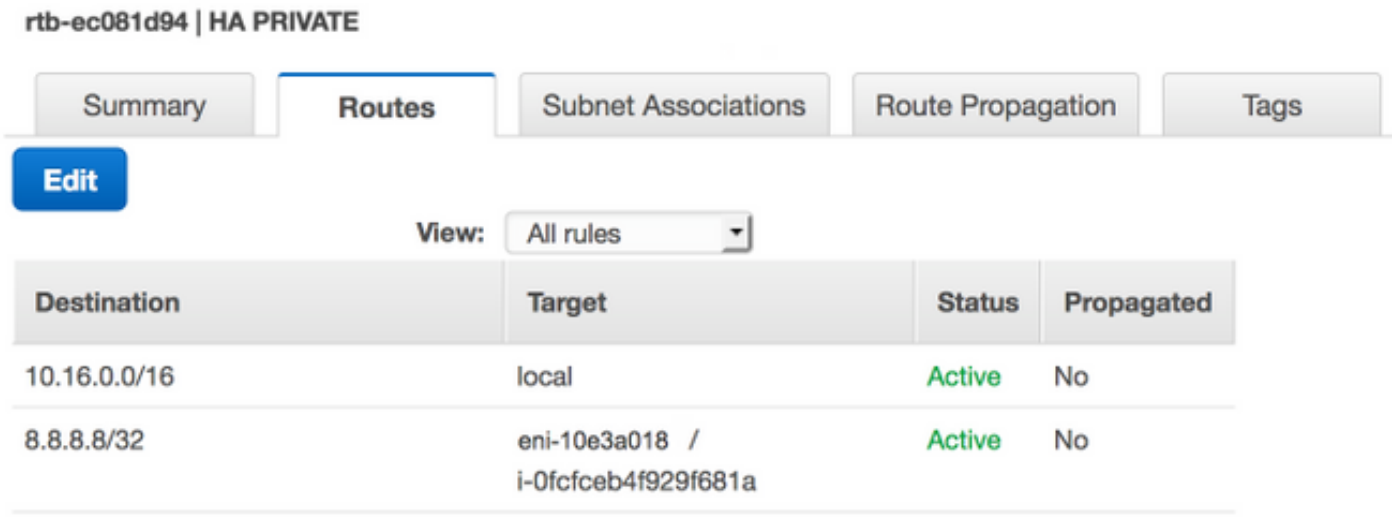
3. Controllare la tabella di route privata. L'eni è attualmente l'interfaccia privata di CSRHA dove si trova il traffico.



4. Arrestare Tunnel1 di CSRHA per simulare un failover HA.

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

5. Si osservi che la tabella di marcia fa riferimento al nuovo ENI, che è l'interfaccia privata di CSRHA1.



Risoluzione dei problemi

- Accertarsi che le risorse siano associate. Durante la creazione di VPC, subnet, interfacce, tabelle di routing e così via, molti di questi elementi non vengono associati automaticamente tra loro. Loro non hanno conoscenza l'uno dell'altro.
- Verificare che l'indirizzo IP elastico e l'eventuale indirizzo IP privato siano associati alle interfacce corrette, con le subnet corrette, aggiunti alla tabella di routing corretta, connessi al router corretto e al VPC e alla zona corretti, collegati al ruolo IAM e ai gruppi di sicurezza.
- Disabilita controllo origine/destinazione per ENI.
- Per Cisco IOS XE 16.3.1a o versioni successive, questi sono i comandi di verifica aggiuntivi disponibili.

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

- Di seguito sono riportati gli errori più comuni rilevati nei debug:

Problema: errore di httpc_send_request

Risoluzione: Http viene utilizzato per inviare la chiamata API dal CSR ad AWS. Verificare che DNS sia in grado di risolvere il nome DNS elencato nell'istanza. Verificare che il traffico HTTP non sia bloccato.

```
*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
```

Problema: la tabella di routing rtb-9c0000f4 e l'interfaccia eni-32791318 appartengono a reti diverse

Risoluzione: Il nome dell'area e l'ENI non sono configurati correttamente in reti diverse. La regione

e l'ENI devono essere nella stessa zona del router.

```
*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>
```

Problema: Non si dispone delle autorizzazioni necessarie per eseguire l'operazione. Messaggio di errore autorizzazione codificata.

Risoluzione: Ruolo/criterio JSON IAM creato in modo errato o non applicato al CSR. Il ruolo IAM autorizza CSR a eseguire chiamate 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: 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>
```

Informazioni correlate

- Ridondanza gateway VPC - Cisco
- Cisco CSR serie 1000v Cloud Services Router Deployment Guide per Amazon Web Services
- Suddivisione tipi di istanza
- EC2 e VPC
- Interfacce di rete elastiche, dalla Guida dell'utente EC2, include il numero di ENI per tipo di istanza
- Enhanced Networking su Linux procedure, informazioni di background utili
- Spiegazione e procedure relative a istanze/locazione dedicate
- Documentazione generale EC2
- Documentazione generale su VPC
- Aree e zone di disponibilità
- CSR1000v High Availability versione 3

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).