Distribuisci configurazione alta disponibilità C8000v su AWS

Sommario

Introduzione

Questo documento descrive come configurare un ambiente ad alta disponibilità con router Catalyst 8000v su cloud Amazon Web Services.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze generali di AWS Console e dei suoi componenti
- Informazioni sul software Cisco IOS® XE
- Conoscenze base della funzionalità HA.

Componenti usati

Per questo esempio di configurazione sono necessari i seguenti componenti:

- Account Amazon AWS con ruolo di amministratore
- Due dispositivi C800v con Cisco IOS® XE 17.15.3a e 1 Ubuntu 22.04 LTS VM AMI nella stessa regione

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.

Topologia

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 - C800v (Cisco IOS® XEDenali 17.15.3a)
- 1x - VM (Linux/Windows)

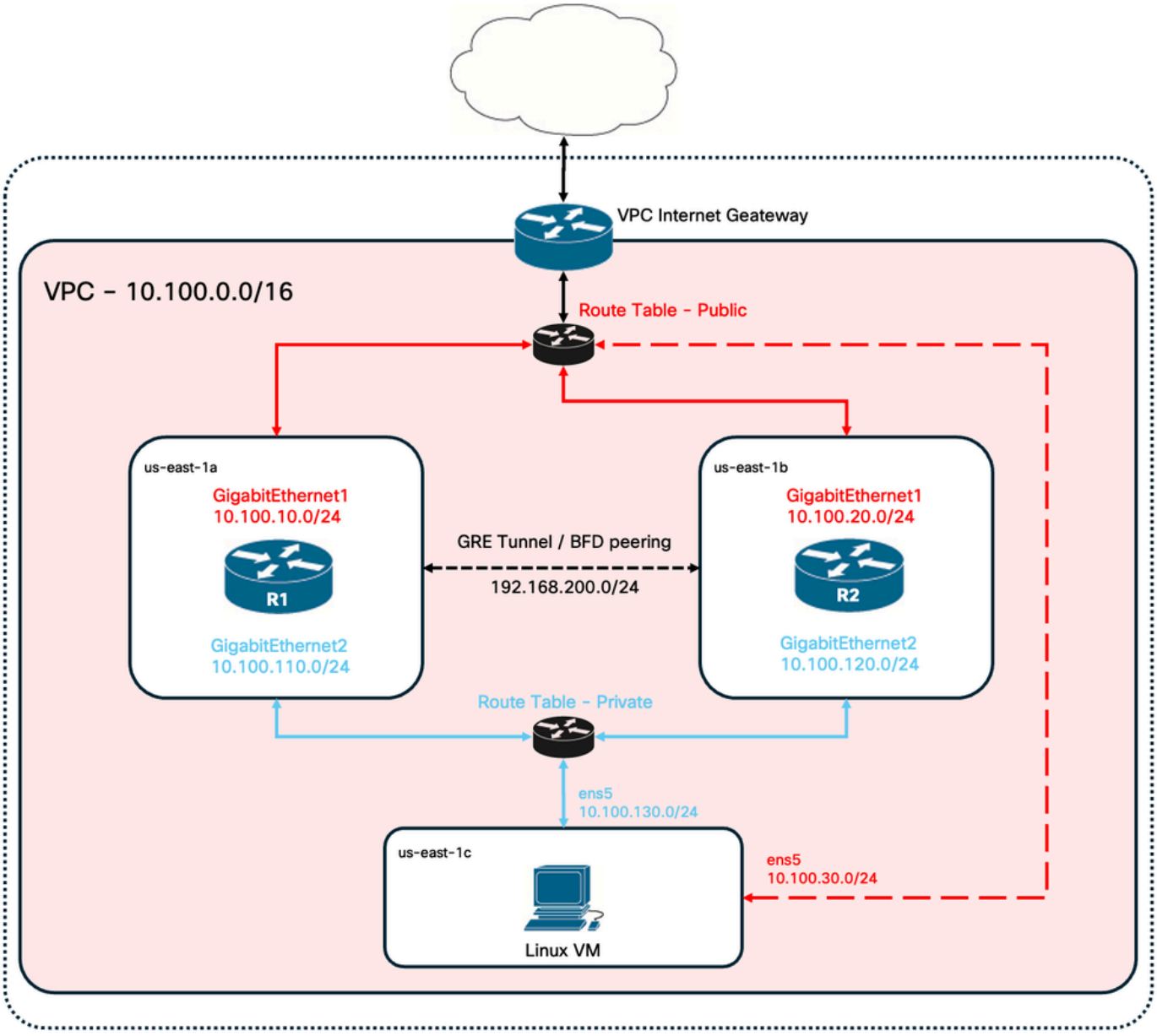
In una coppia HA sono presenti 2 router C8000v, in due diverse zone di disponibilità. Ogni zona di disponibilità può essere considerata come un centro dati separato per una resilienza hardware aggiuntiva.

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 in modo che sia possibile accedere e configurare la VM. In genere, tutto il traffico normale deve passare attraverso la tabella di route

privata.

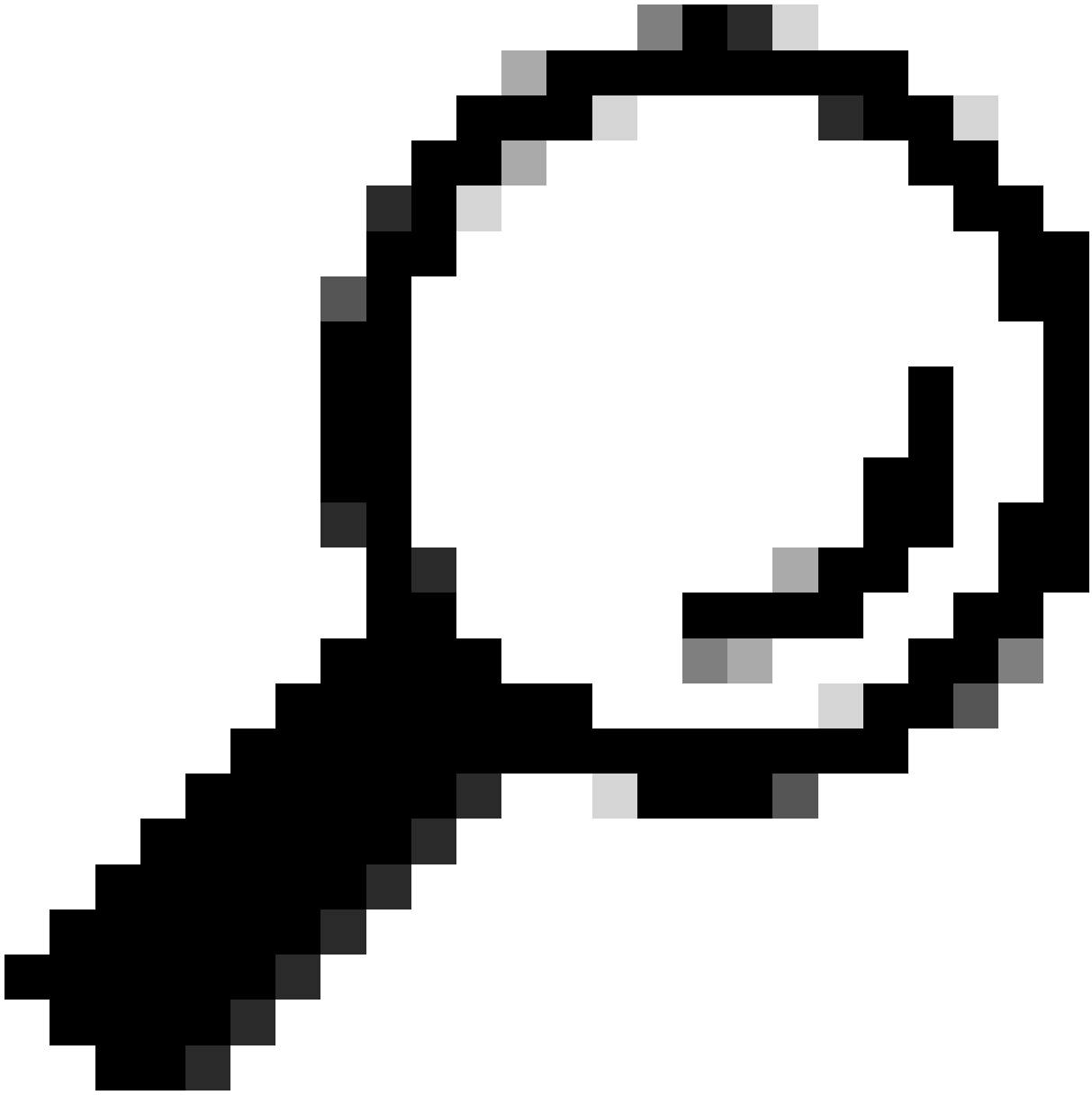
Per simulare il traffico, avviare un ping dall'interfaccia privata della macchina virtuale, attraversando la tabella di routing privata attraverso R1 fino a raggiungere la posizione 8.8.8.8. In caso di failover, verificare che la tabella di routing privata sia stata aggiornata automaticamente in modo da instradare il traffico attraverso l'interfaccia privata del router R2.

Esempio di rete



Riepilogo tabella

Per riepilogare la topologia, di seguito è riportata la tabella con i valori più importanti di ciascun componente del laboratorio. Le informazioni fornite in questa tabella sono esclusive per questa esercitazione.



Suggerimento: l'utilizzo di questa tabella consente di avere una panoramica chiara delle variabili chiave nella guida. Si consiglia di raccogliere le informazioni in questo formato per semplificare il processo.

Sul dispositivo bootflash o slot0:	Area Disponibilità	Interfacce	Indirizzi IP	RTB	ENI
R1	us-east-1a	Gigabit Ethernet 1	10.100.10.254	rtb-0d0e48f25c9b00635 (pubblico)	eni-0645a881c13823696
		Gigabit Ethernet 2	10.100.110.254	rtb-093df10a4de426eb8 (privata)	eni-070e14fbfde0d8e3b

R2	us-east-1b	Gigabit Ethernet 1	10.100.20.254	rtb-0d0e48f25c9b00635 (pubblico)	eni-0a7817922ffbb317b
		Gigabit Ethernet 2	10.100.120.254	rtb-093df10a4de426eb8 (privata)	eni-0239fda341b4d7e41
VM Linux	us-east-1c	ens5	10.100.30.254	rtb-0d0e48f25c9b00635 (pubblico)	eni-0b28560781b3435b1
		6	10.100.130.254	rtb-093df10a4de426eb8 (privata)	eni-05d025e88b635808

Restrizioni

- Non utilizzare il primo indirizzo disponibile di una subnet in qualsiasi subnet creata. Questi indirizzi IP vengono utilizzati internamente dai servizi AWS.
- Non configurare le interfacce pubbliche dei dispositivi C800v all'interno di un VRF. HA non funziona correttamente se è impostato.

Configurazione

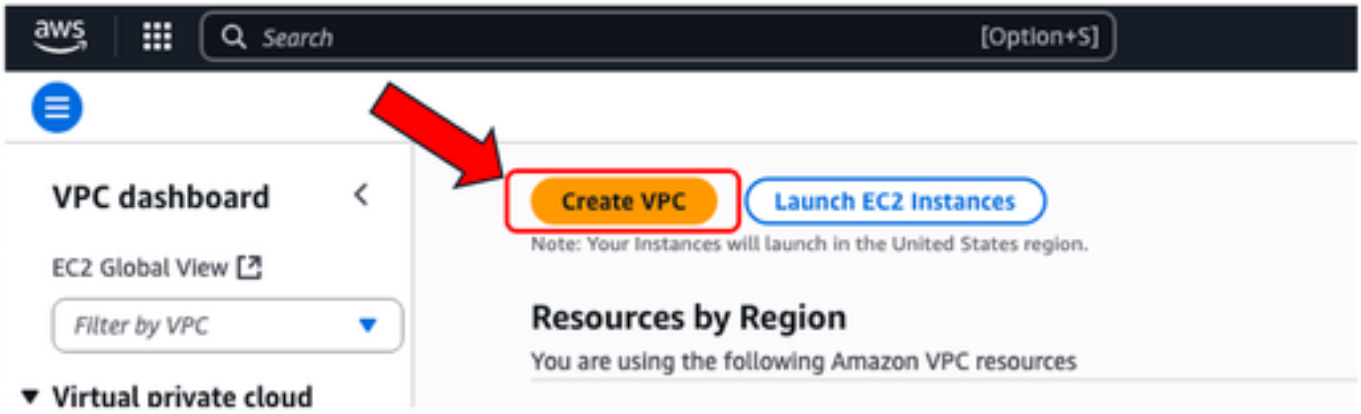
Il flusso generale della configurazione è finalizzato a creare le VM richieste nella regione appropriata e a passare alla configurazione più specifica, ad esempio percorsi e interfacce di ognuna di esse. È tuttavia consigliabile comprendere innanzitutto la topologia e configurarla nell'ordine desiderato.

Passaggio 1. Selezionare un'area

Per questa guida all'installazione, la regione US West (North Virginia) - us-east-1 è selezionata come regione VPC.

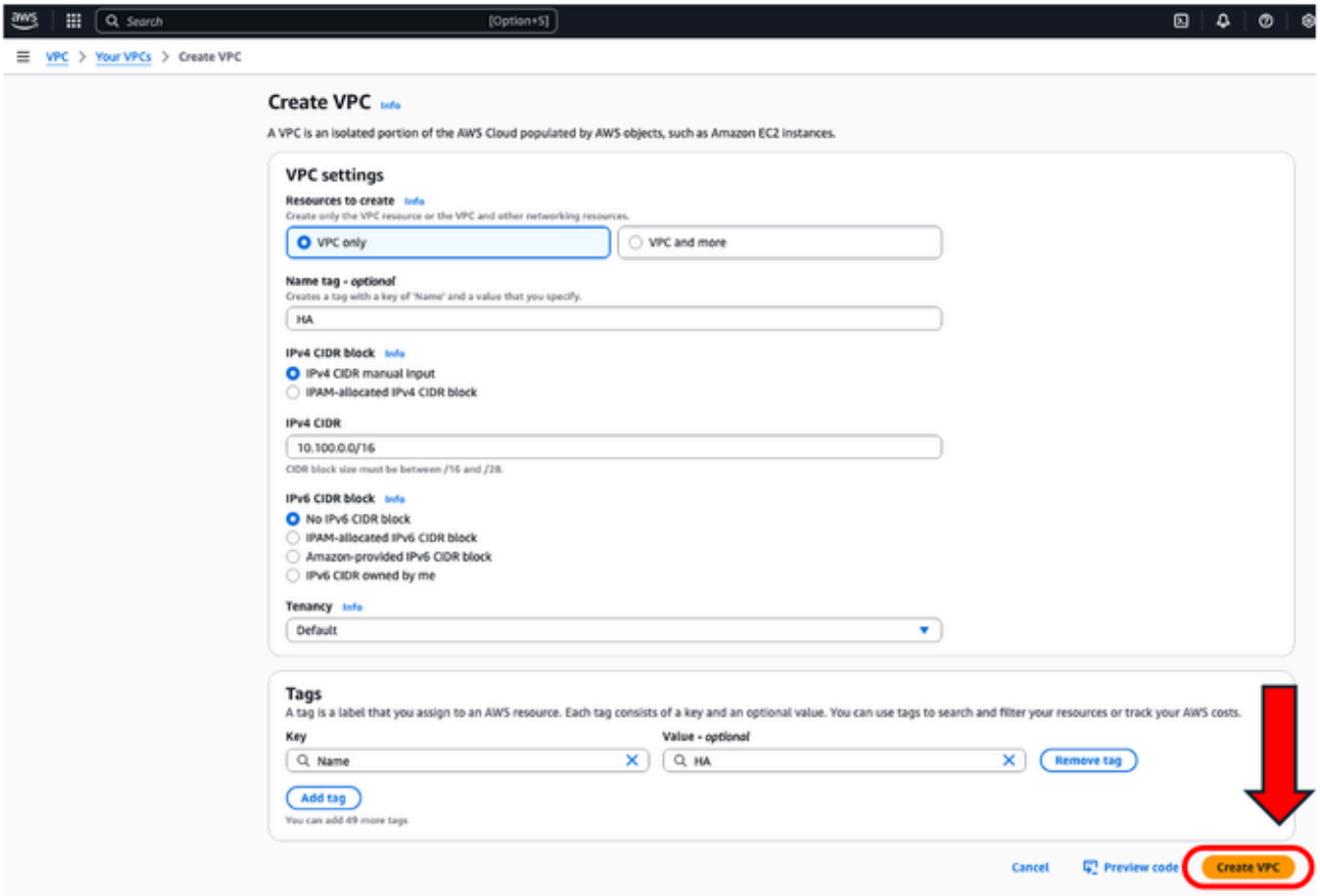
Passaggio 2. Creare il VPC

Dalla console AWS, selezionare VPC > VPC Dashboard > Create VPC.

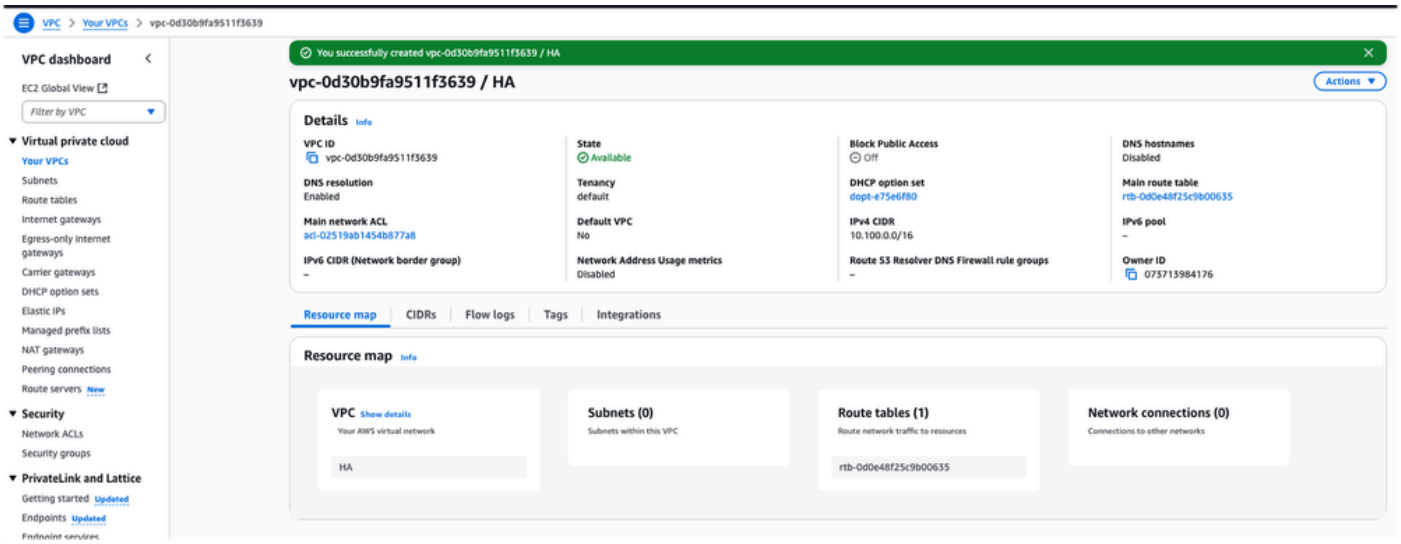


Quando si crea il VPC, selezionare l'opzione Solo VPC. È possibile assegnare una rete /16 da utilizzare come desiderato.

In questa guida alla distribuzione viene selezionata la rete 10.100.0.0/16:

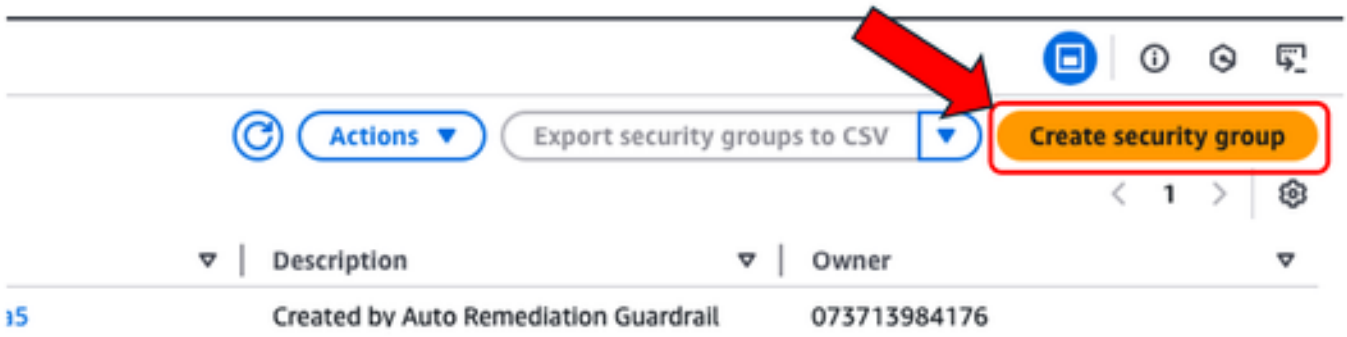


Dopo aver fatto clic su Create VPC, viene creato il VPC-0d30b9fa9511f3639 con tag HA:

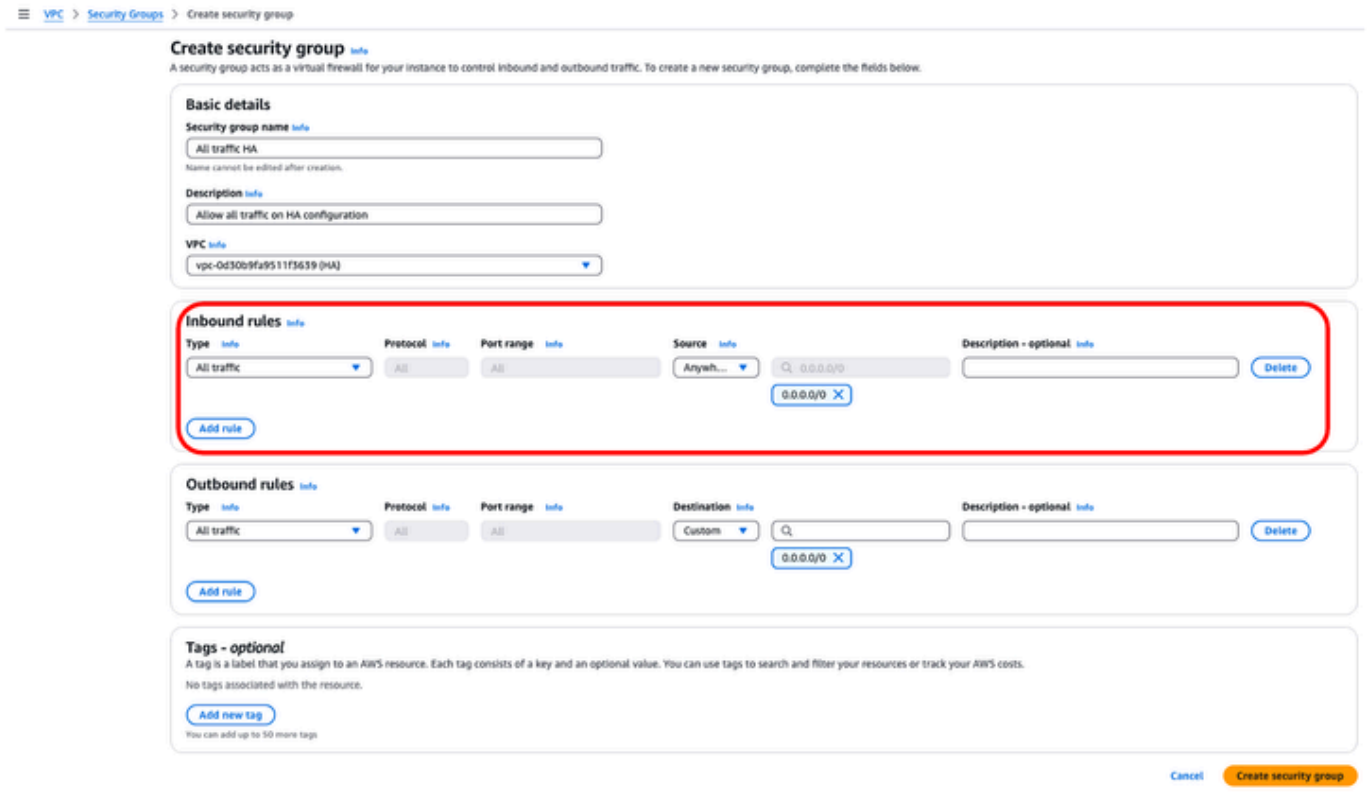


Passaggio 3. Creare un gruppo di sicurezza per il VPC

In AWS, i gruppi di sicurezza funzionano come ACL, consentendo o negando il traffico alle macchine virtuali configurate all'interno di un VPC. Sulla console AWS, selezionare VPC > Dashboard VPC > Sicurezza > Gruppi di sicurezza e fare clic su Crea gruppo di sicurezza.



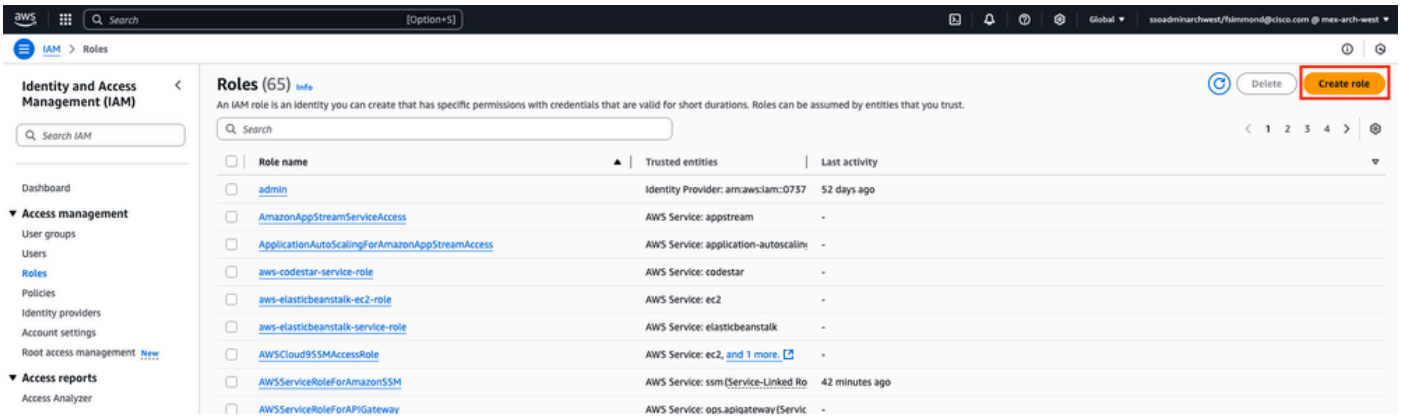
In Regole in entrata definire il traffico che si desidera consentire. Per questo esempio, All Traffic viene selezionato utilizzando la rete 0.0.0.0/0.



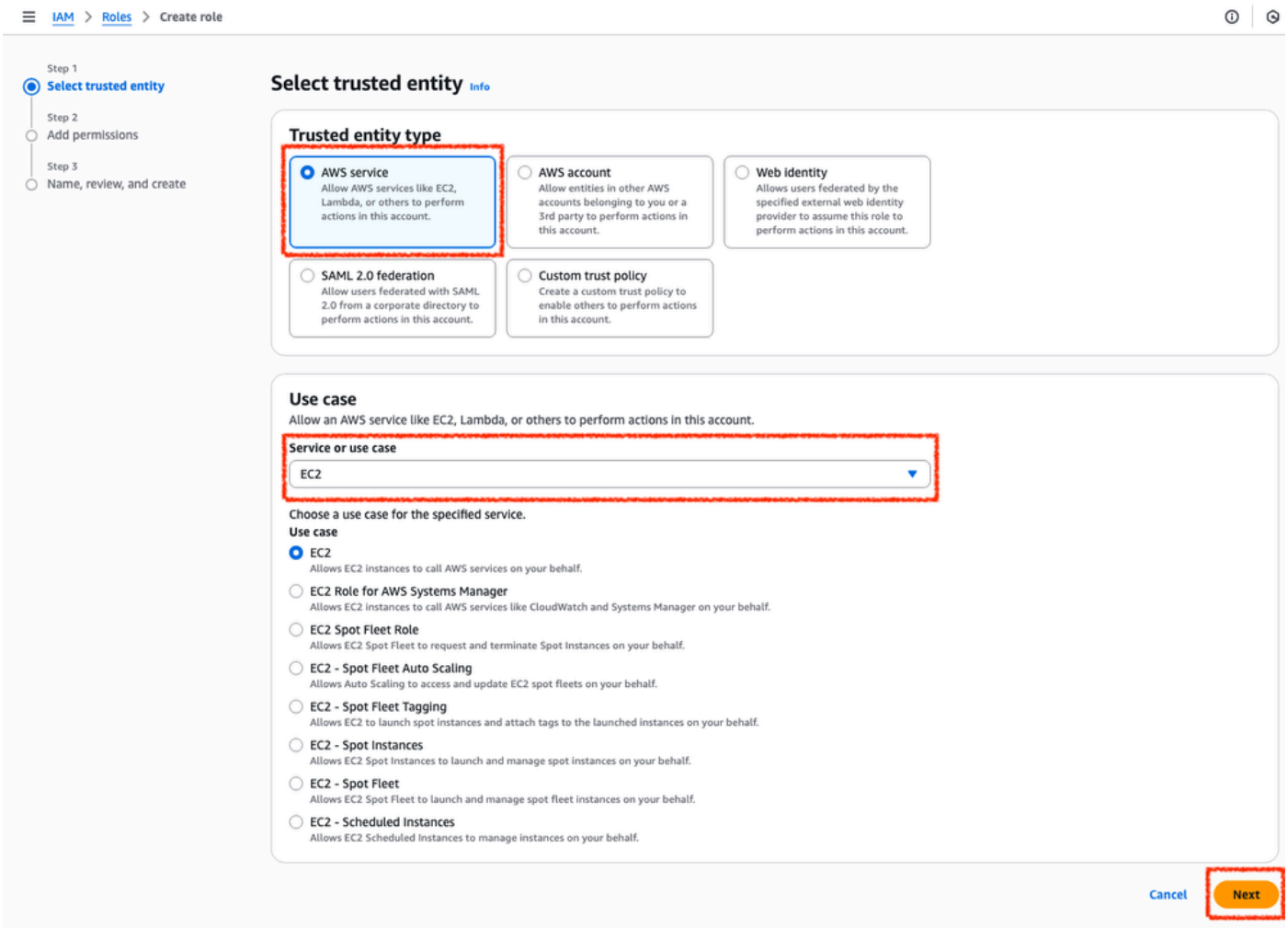
Passaggio 4. Creare un ruolo IAM con un criterio e associarsi al VPC

IAM concede agli AMI l'accesso richiesto alle API Amazon. Il C8000v viene utilizzato come proxy per chiamare i comandi API AWS per modificare la tabella di route in AWS. Per impostazione predefinita, alle istanze EC2 non è consentito l'accesso alle API. Per questo motivo, è necessario creare un nuovo ruolo IAM che verrà applicato durante le creazioni AMI.

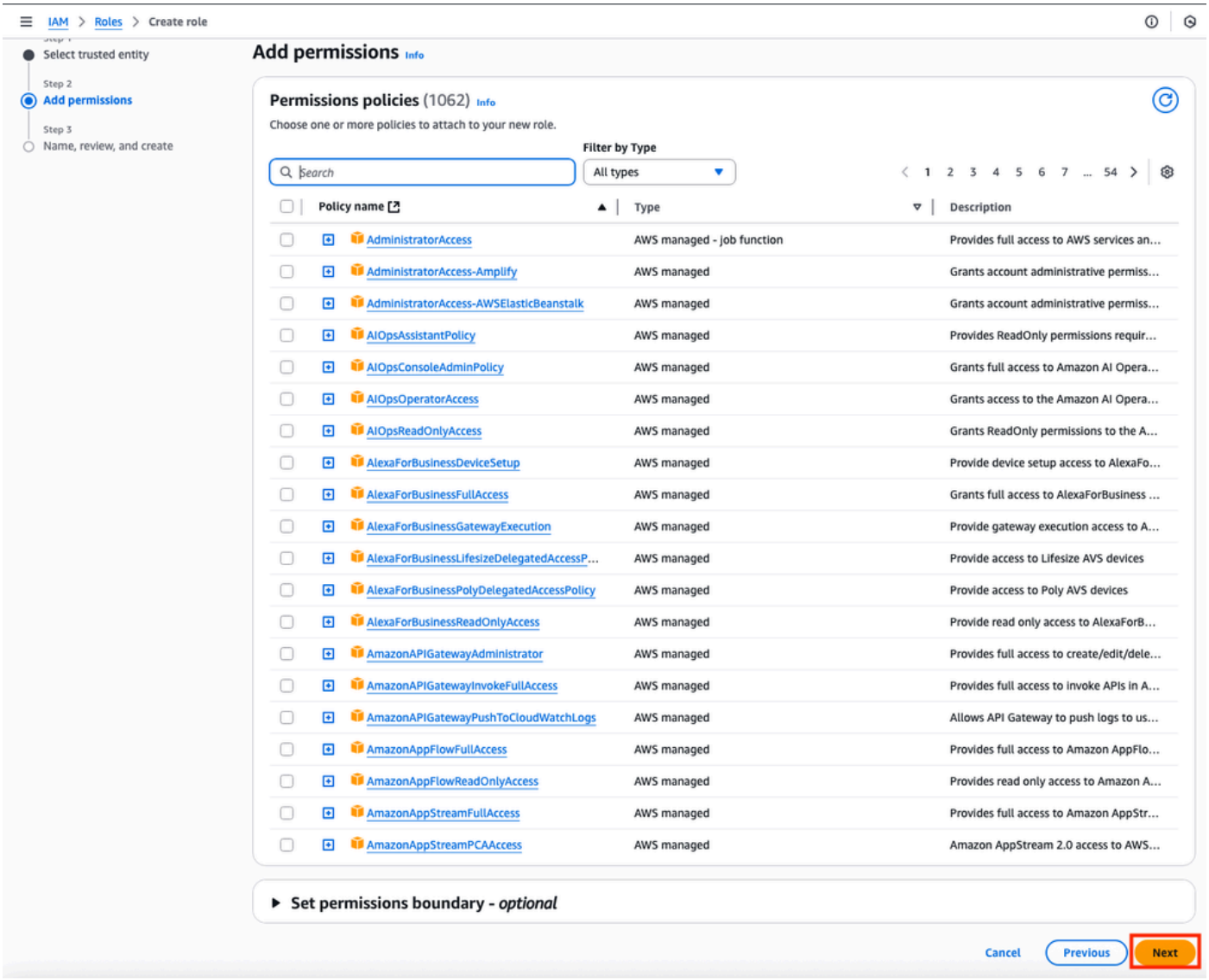
Passare al dashboard IAM e selezionare Gestione accesso > Ruoli > Crea ruolo. Questo processo si articola in 3 fasi:



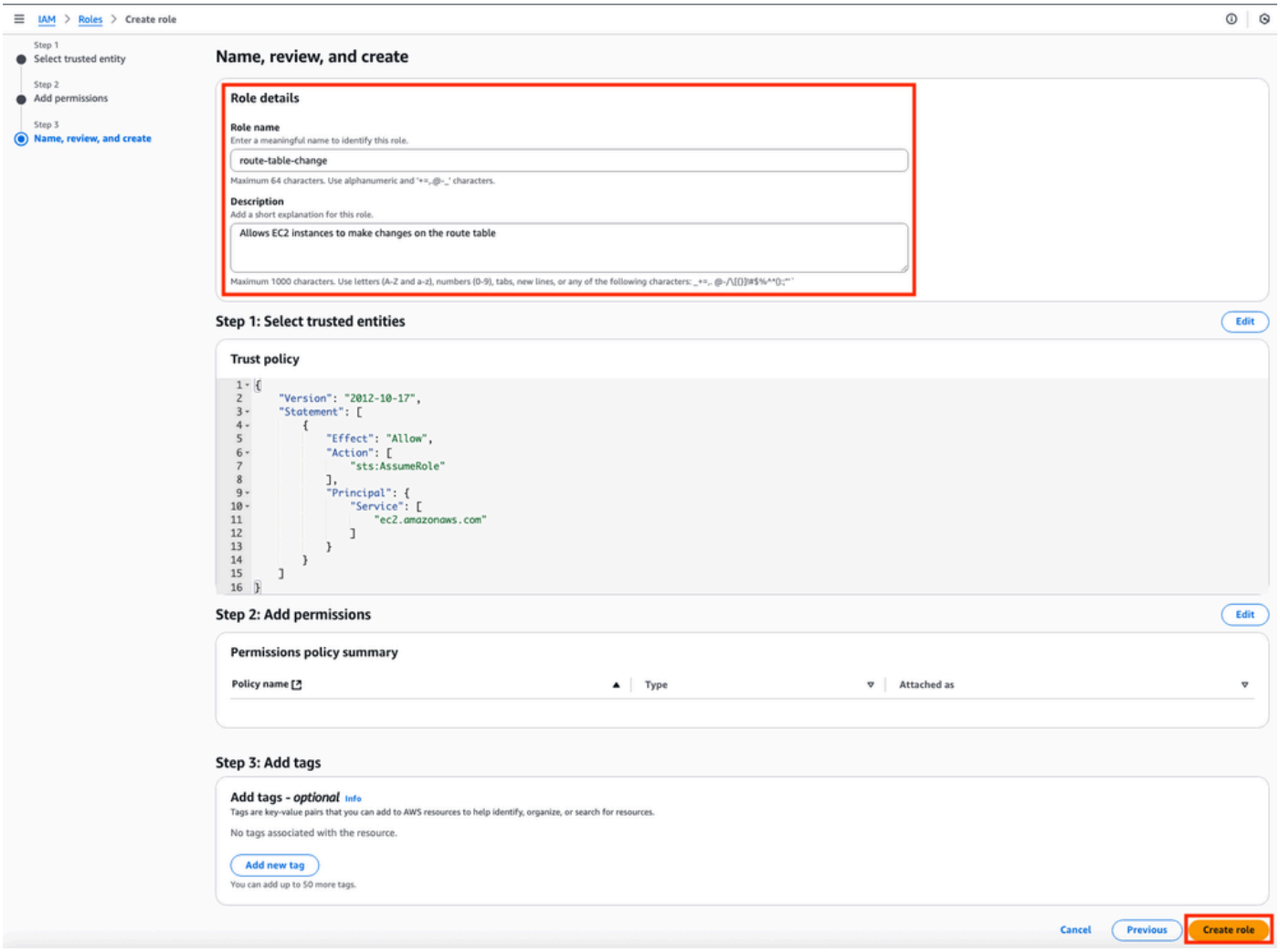
Selezionare innanzitutto l'opzione Servizio AWS nella sezione Tipo di entità attendibile ed EC2 come servizio assegnato per questo criterio.



Al termine, fare clic su Avanti:

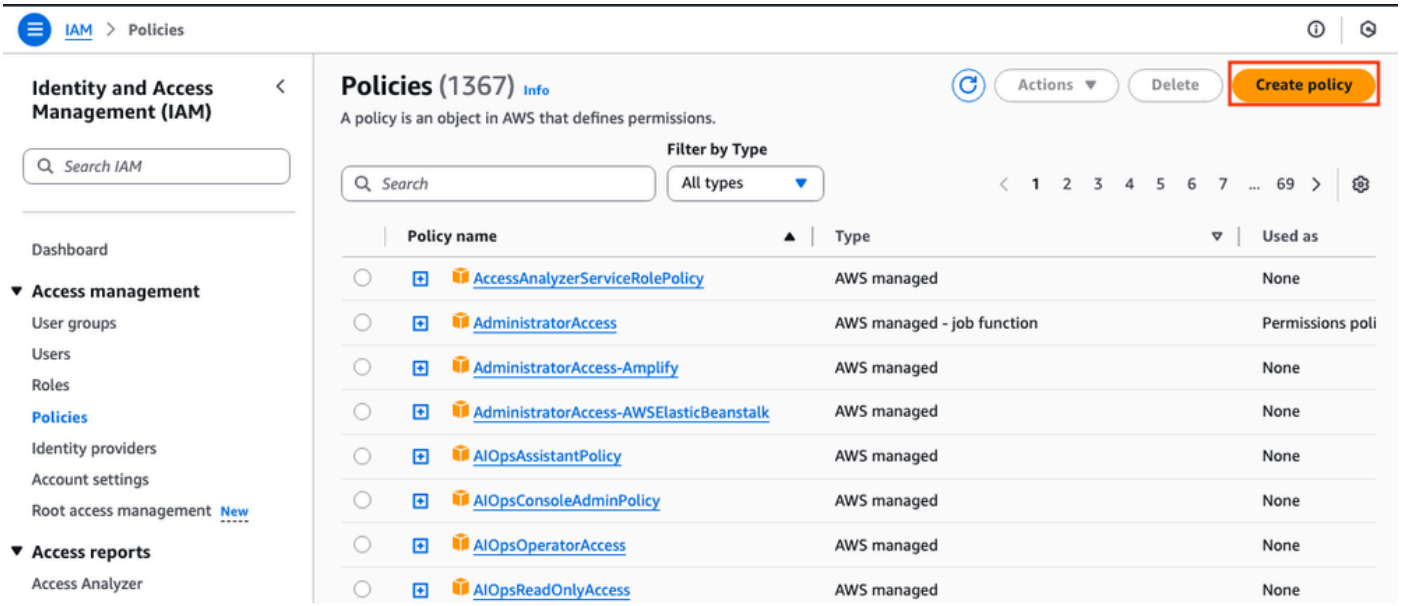


Infine, impostare il Nome ruolo e fare clic sul pulsante Crea ruolo.

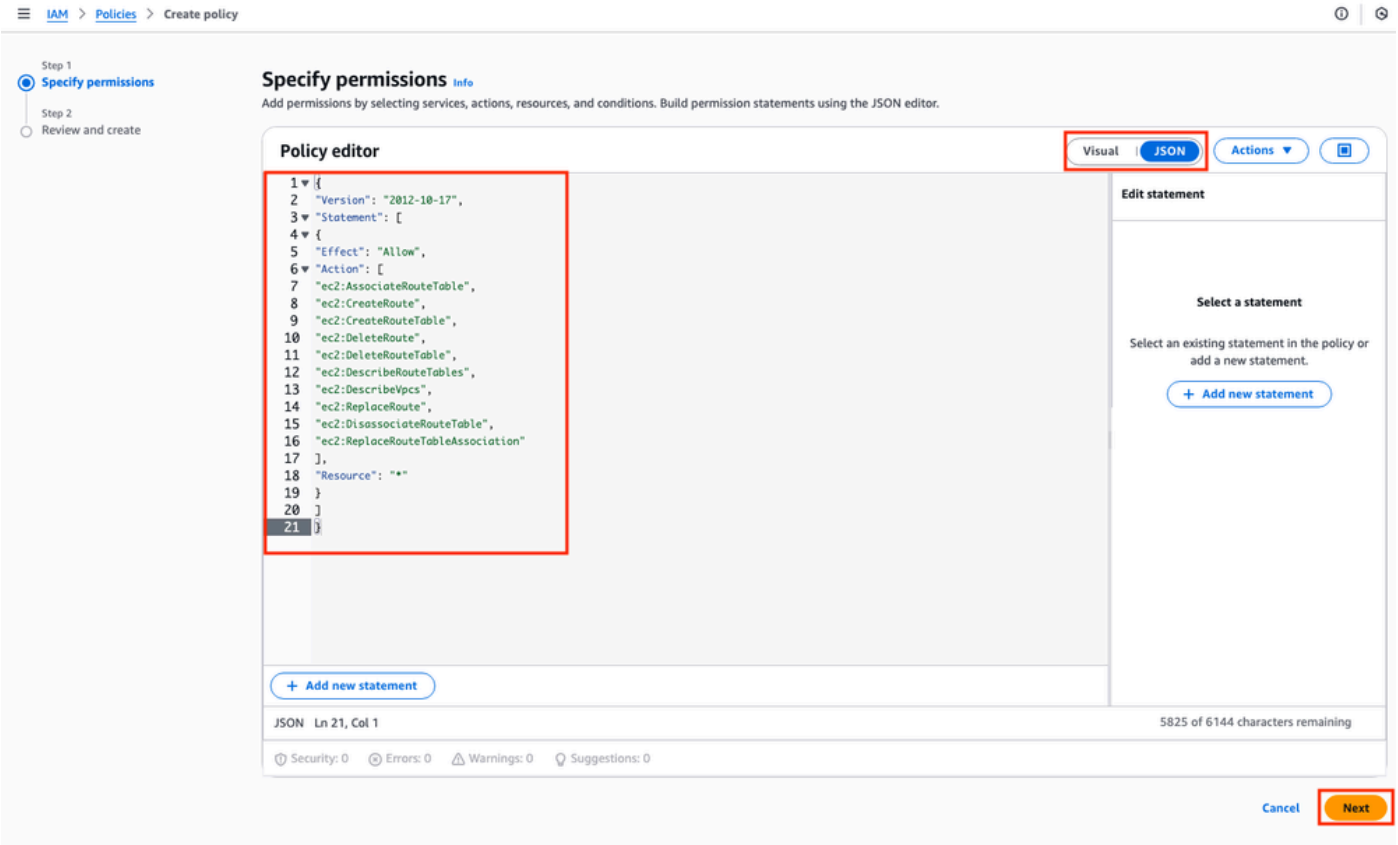


Passaggio 5. Creare e allegare un criterio di attendibilità a un ruolo IAM

Dopo aver creato il ruolo, è necessario creare un criterio di attendibilità per acquisire la capacità di modificare le tabelle di routing AWS quando necessario. Passare alla sezione Criteri del dashboard IAM. Fare clic sul pulsante Crea criterio. Questo processo si compone di due fasi:



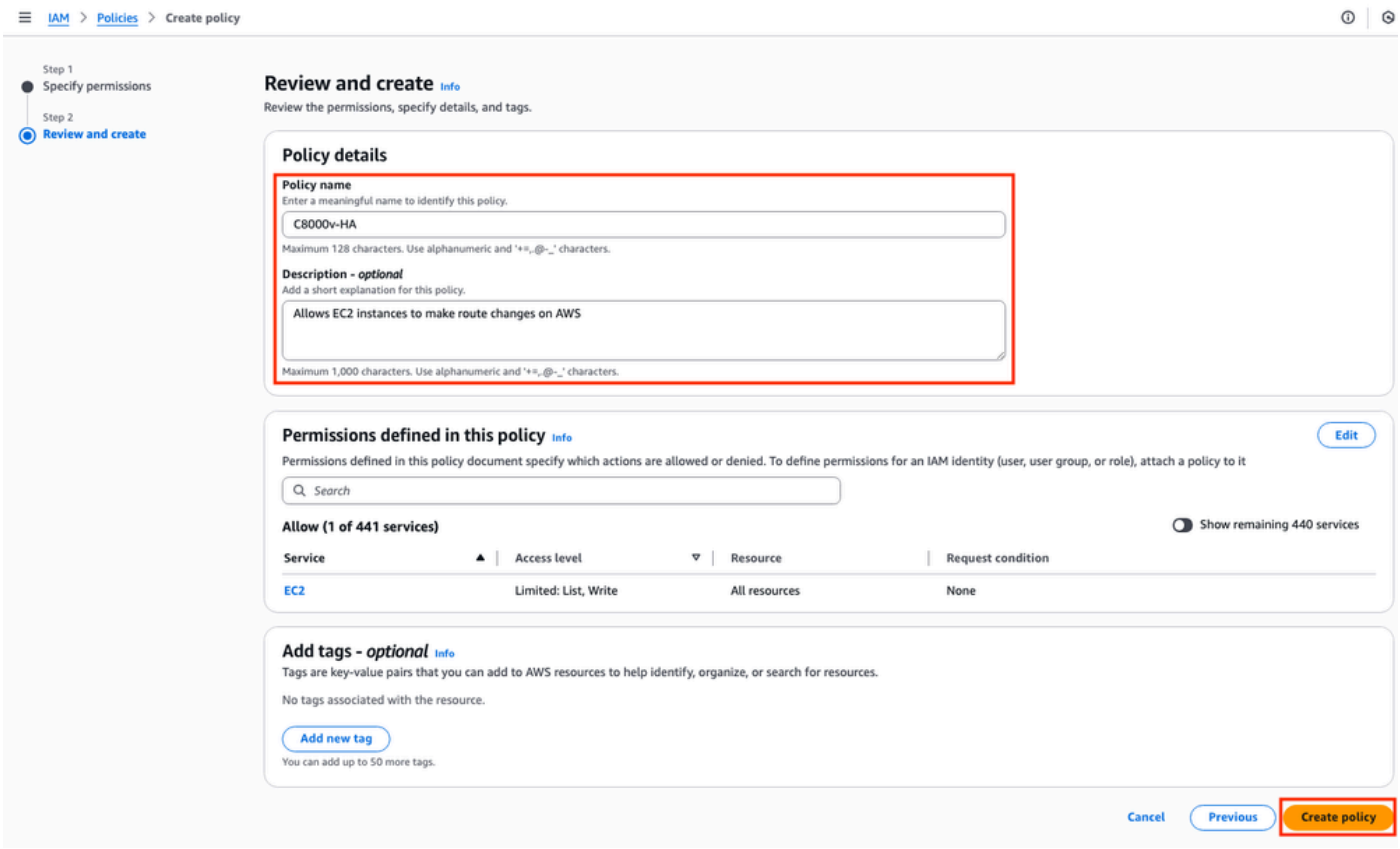
Verificare innanzitutto che l'editor dei criteri utilizzi JSON e applicare i comandi illustrati di seguito. Una volta configurata, fare clic su Avanti:



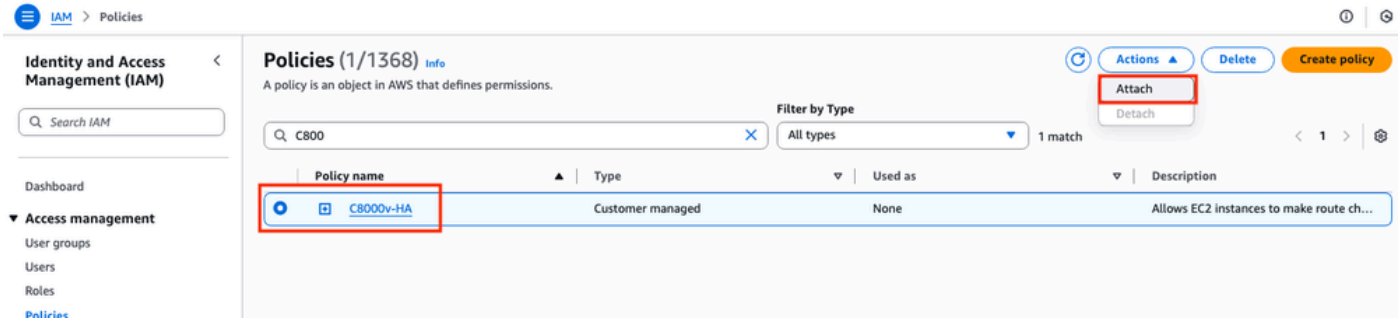
Questo è il codice di testo usato nell'immagine:

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

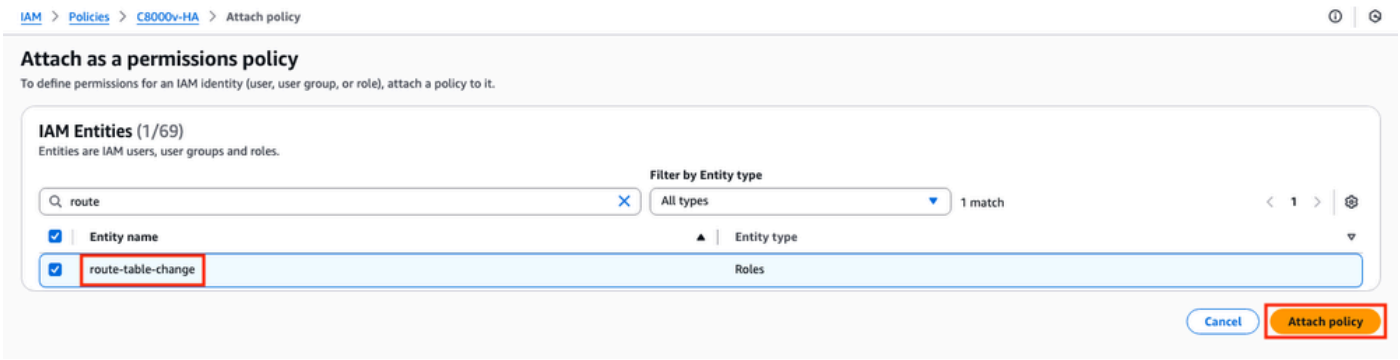
In seguito, impostare il nome del criterio e fare clic su Crea criterio.



Una volta creato il criterio, filtrare e selezionare il criterio, quindi fare clic su Allega opzione nel menu a discesa Azioni.



È aperta una nuova finestra. Nella sezione Entità IAM filtrare e selezionare il ruolo IAM creato e fare clic su Allega criterio.

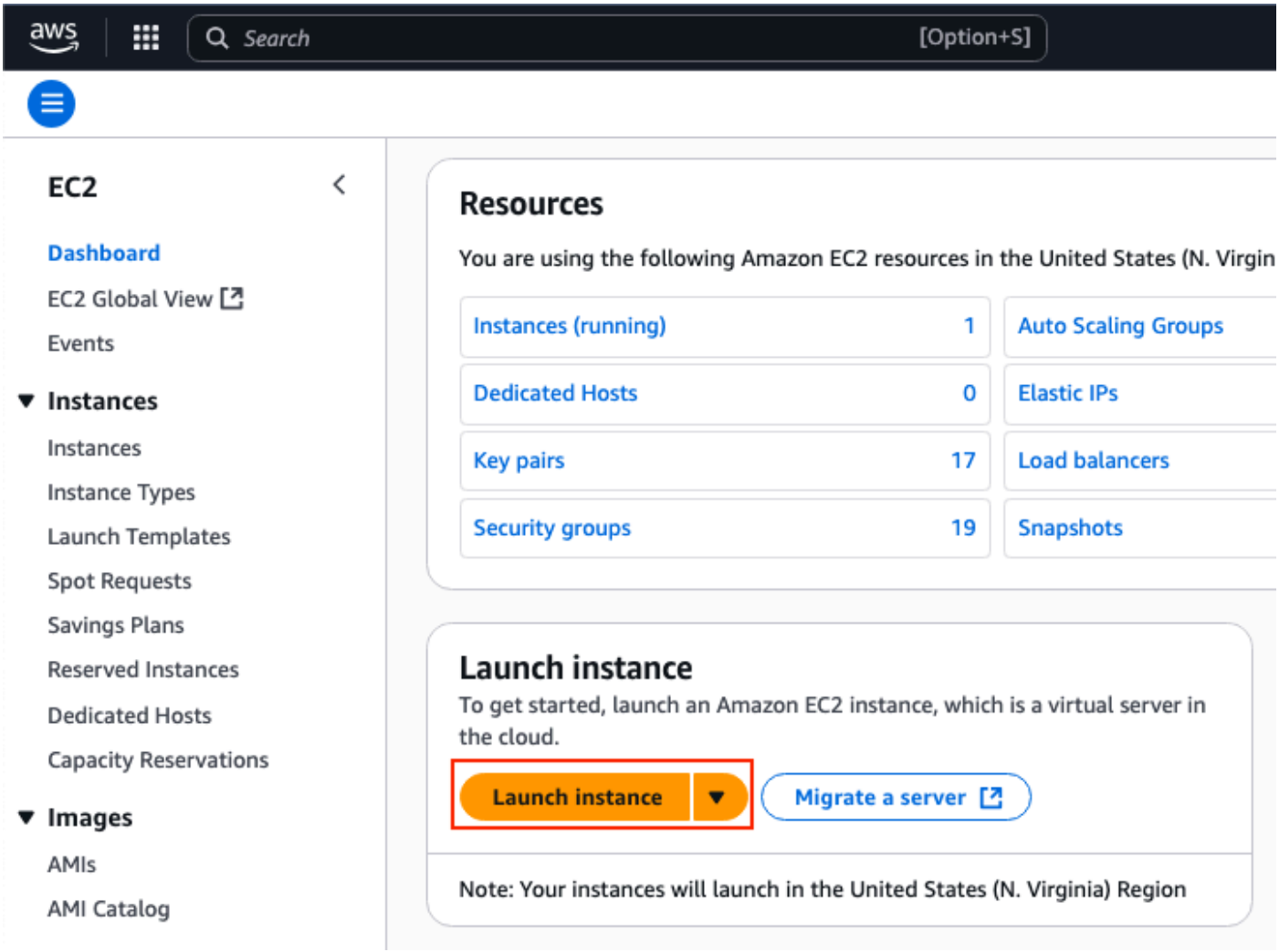


Passaggio 6.Configurare e avviare le istanze di C8000v

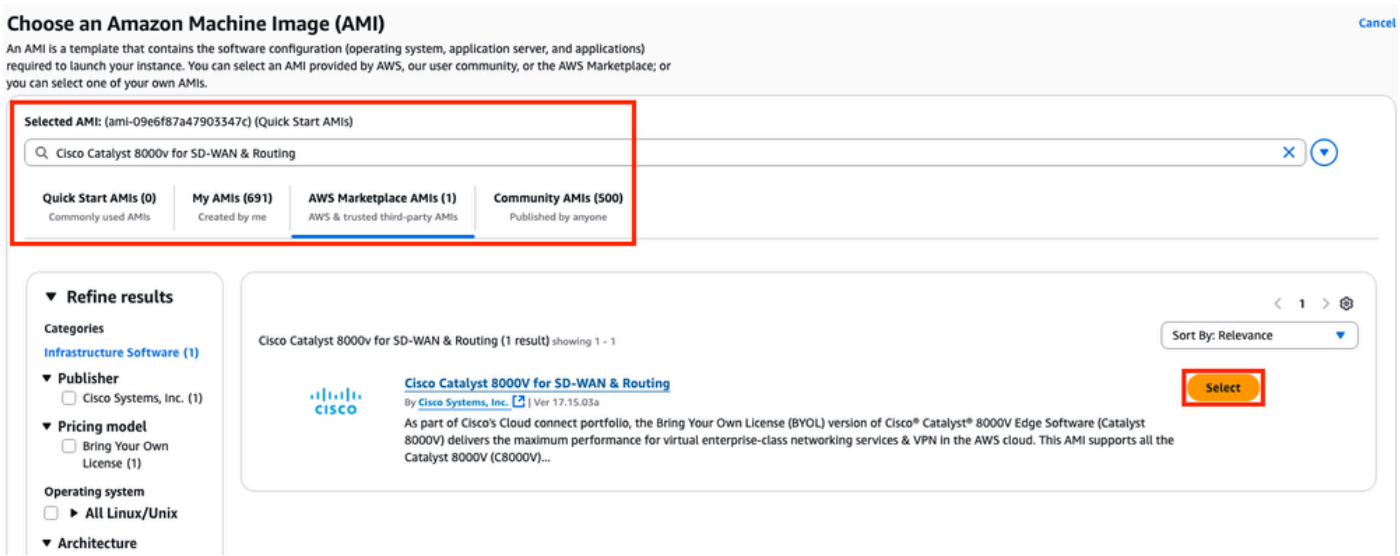
Ogni router C800v avrà due interfacce (una pubblica e una privata) e verrà creato nella propria

zona di disponibilità.

Nel dashboard EC2, fare clic su Avvia istanze:

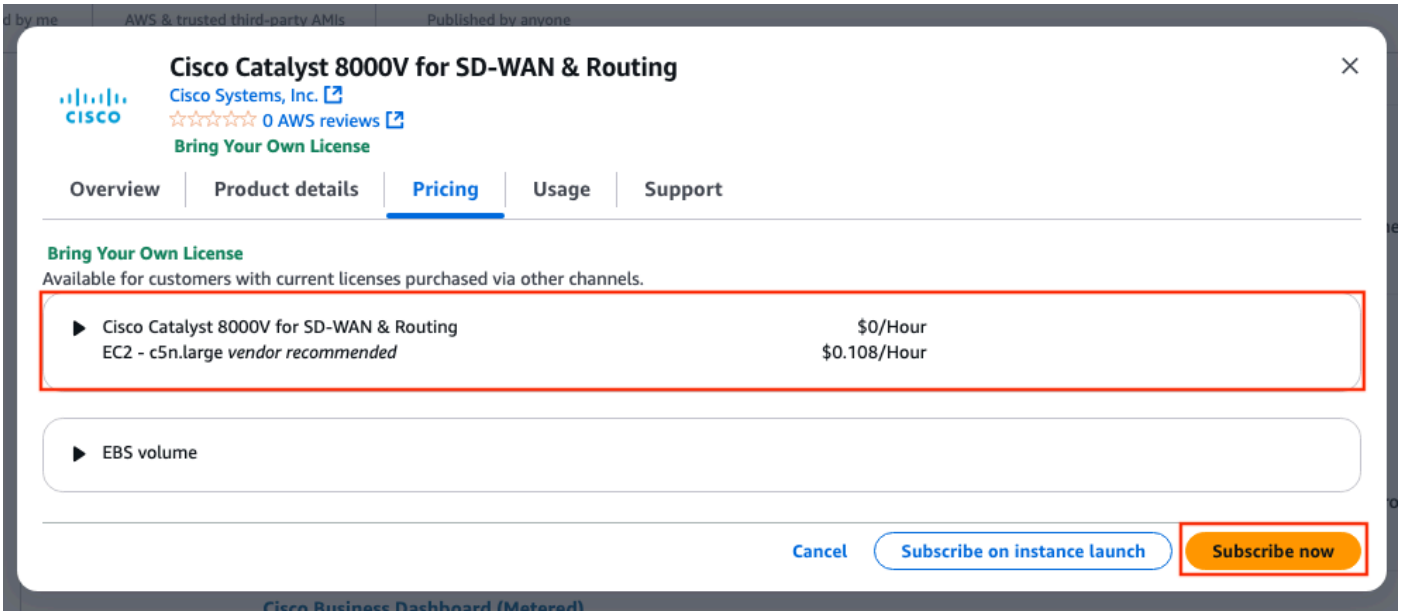


Filtrare il database AMI con il nome Cisco Catalyst 8000v per SD-WAN e routing. Nell'elenco AMI di AWS Marketplace, fare clic su Seleziona.



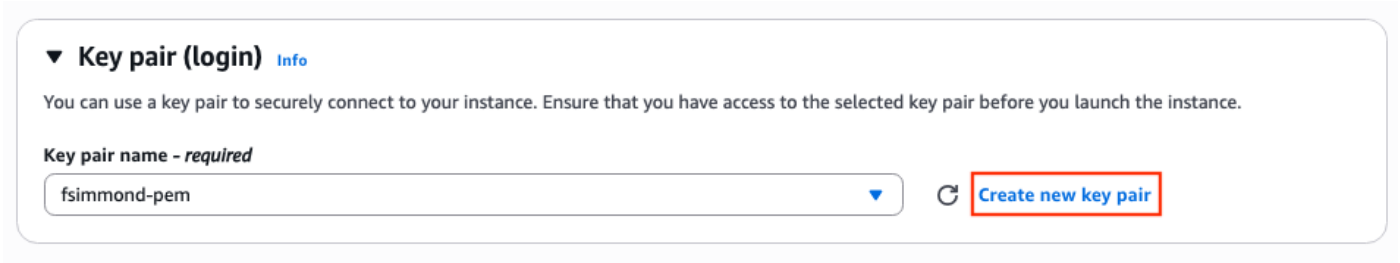
Selezionare le dimensioni corrispondenti per l'AMI. Per questo esempio, viene selezionata la

dimensione c5n.large. Ciò può dipendere dalla capacità richiesta per la rete. Dopo aver selezionato questa opzione, fare clic su Subscribe now (Sottoscrivi ora).

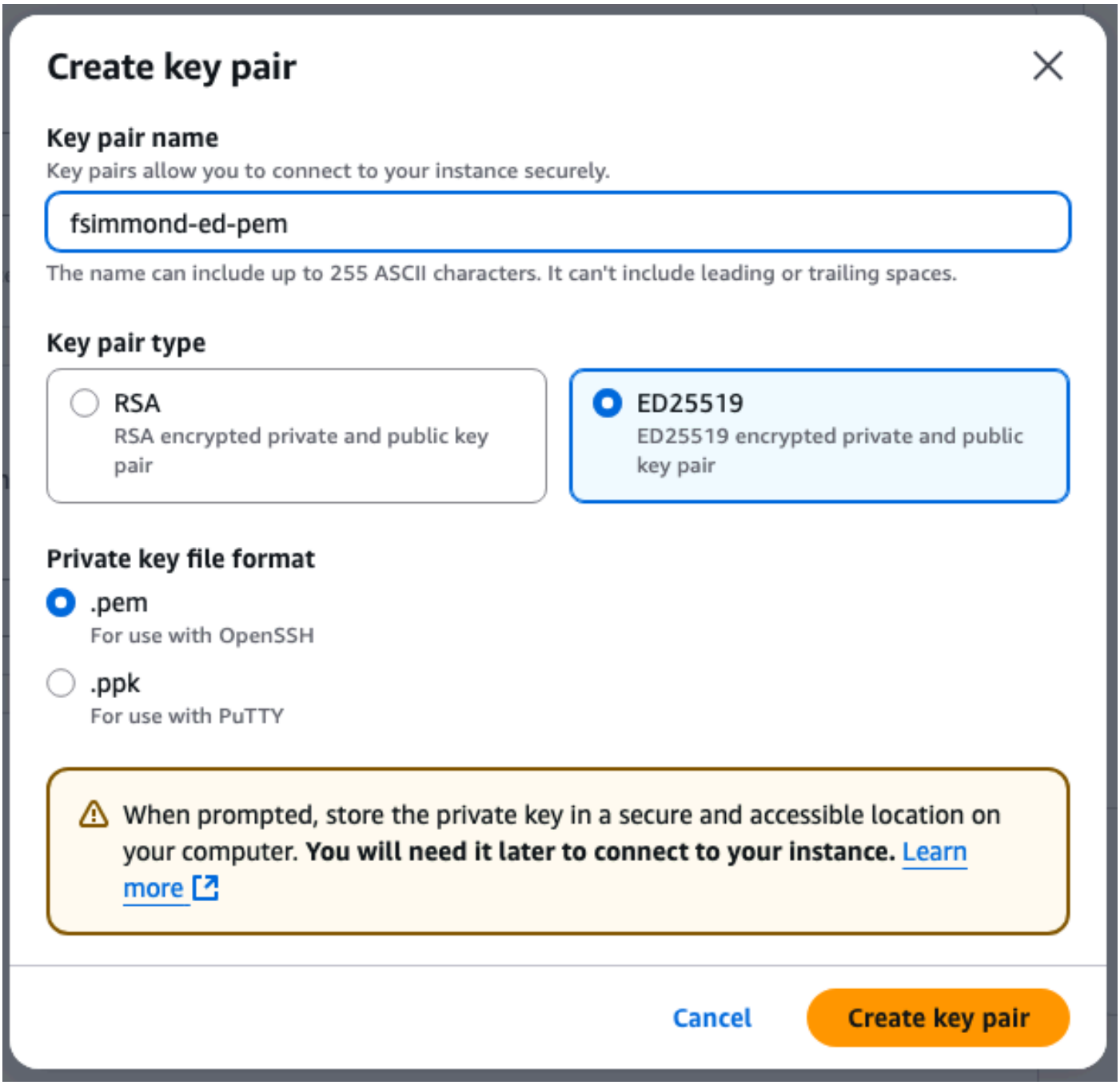


Passaggio 6.1. Configurazione della coppia di chiavi per l'accesso remoto

Una volta effettuata la sottoscrizione all'AMI, viene visualizzata una nuova finestra con più opzioni. Se nella sezione Coppia di chiavi (accesso) non è presente una coppia di chiavi, fare clic su Crea nuova coppia di chiavi. È possibile riutilizzare un singolo tasto per ogni dispositivo creato.



Viene visualizzata una nuova finestra popup. In questo esempio, viene creato un file di chiave .pem con crittografia ED25519. Una volta impostati tutti gli elementi, fare clic su Crea coppia di chiavi.



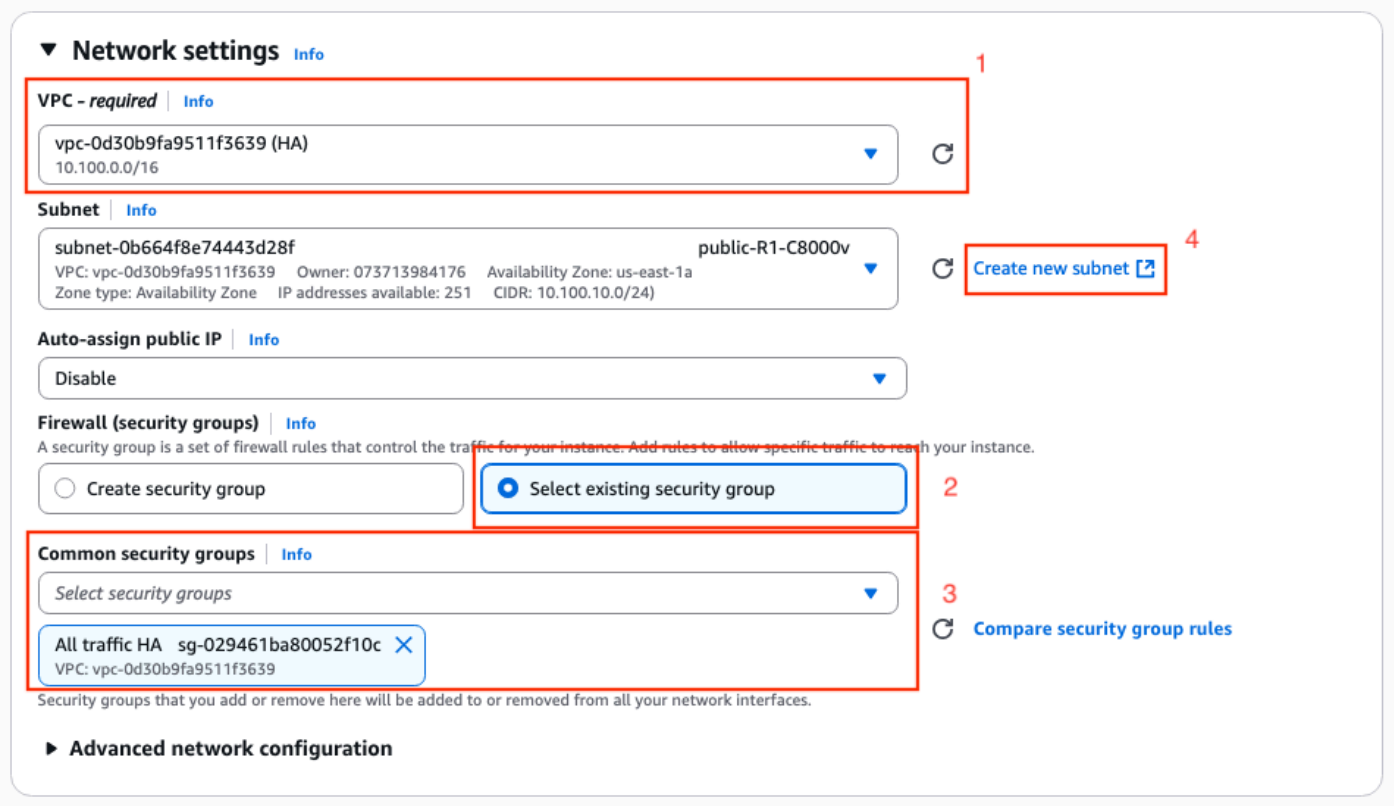
Passaggio 6.2. Creazione e configurazione delle subnet per l'AMI

Nella sezione Impostazioni di rete fare clic su Modifica. Sono ora disponibili alcune nuove opzioni all'interno della sezione:
1. Selezionare il VPC desiderato per questa operazione. Per questo esempio viene selezionato il VPC denominato HA.

2. Nella sezione Firewall (gruppi di sicurezza), selezionare Seleziona gruppo di sicurezza esistente.

3. Una volta selezionata l'opzione 2, è disponibile l'opzione Gruppi di sicurezza comuni. Filtrare e selezionare il gruppo di sicurezza desiderato. Per questo esempio, viene selezionato il gruppo di sicurezza Tutto il traffico HA.

4. (Facoltativo) Se non vengono create subnet per queste periferiche, fare clic su Crea nuova subnet.



Nel browser Web è aperta una nuova scheda che conduce alla sezione Creazione subnet:

1. Selezionare il VPC corrispondente per questa configurazione dall'elenco a discesa.

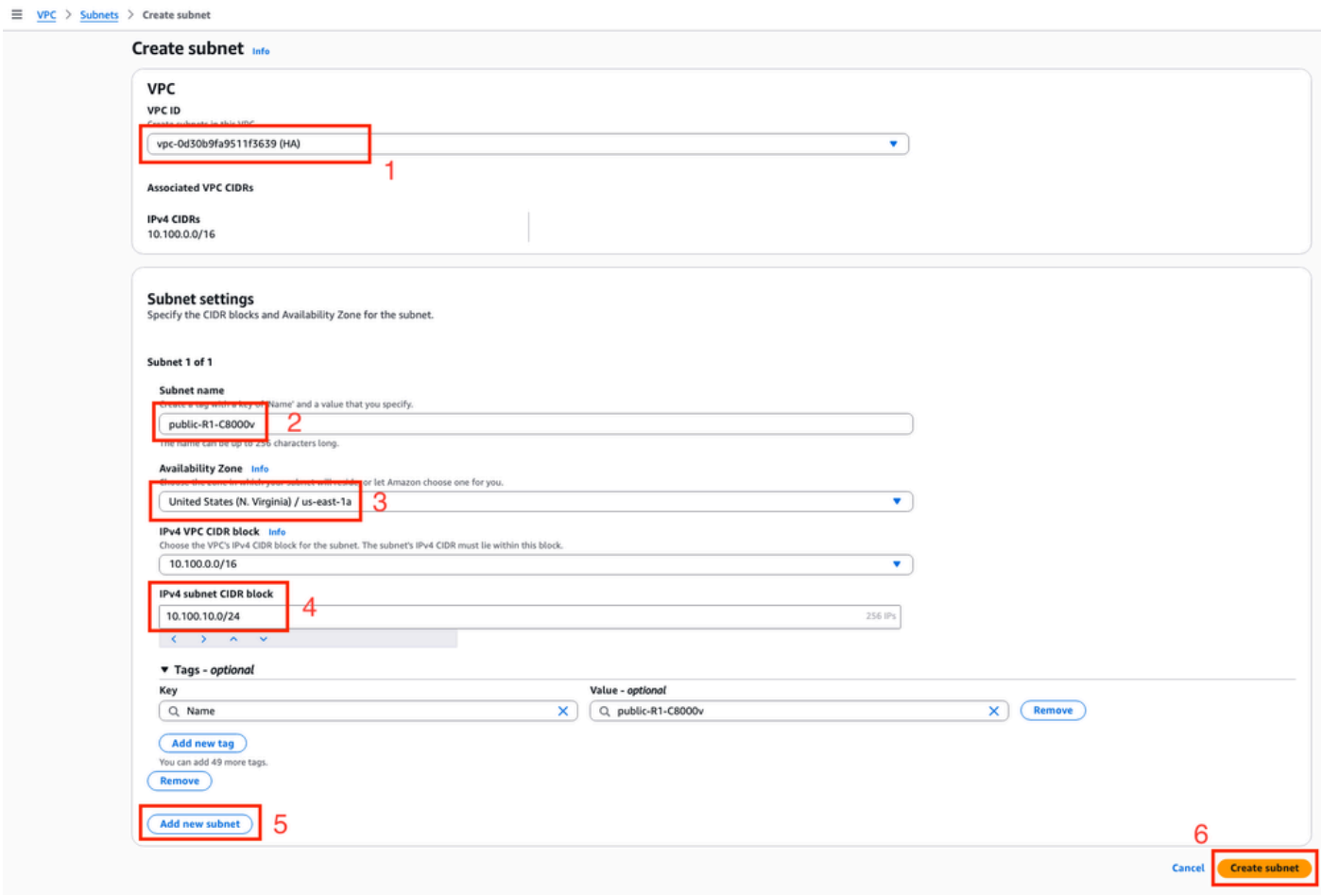
2. Impostare un nome per la nuova subnet.

3. Definire la zona di disponibilità per questa subnet. (per ulteriori informazioni sull'impostazione, fare riferimento alla sezione Topologia di questo documento)

4. Impostare il blocco subnet che appartiene al blocco CIDR VPC.

5. È inoltre possibile creare tutte le subnet da utilizzare facendo clic sulla sezione Aggiungi nuova subnet e ripetendo i passaggi da 2 a 4 per ciascuna subnet.

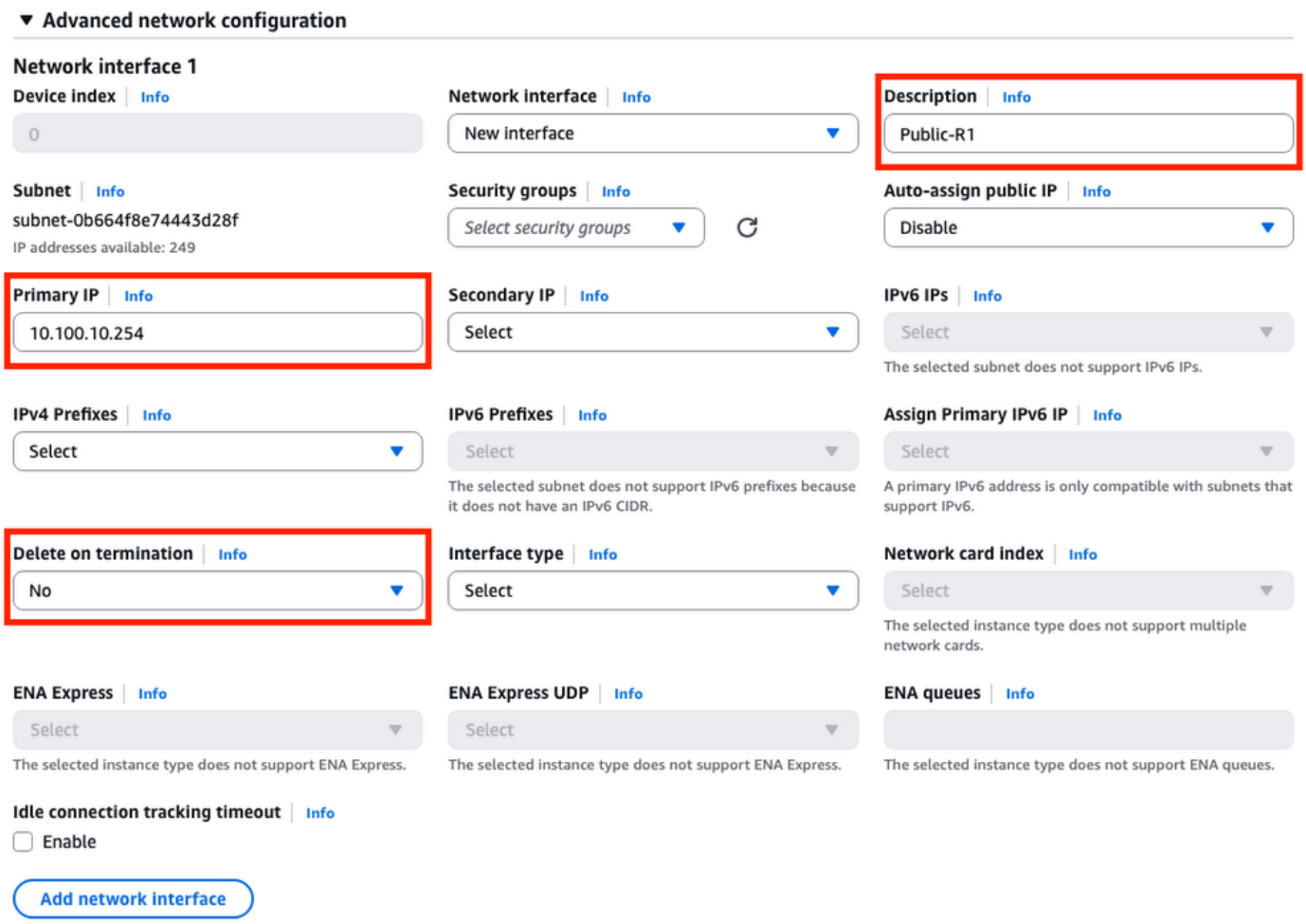
6. Al termine, fare clic su Crea subnet. Passare alla pagina precedente per continuare con le impostazioni.



Nella sottosezione Subnet della sezione Impostazioni di rete fare clic su Icona Aggiorna per visualizzare le subnet create nell'elenco a discesa.

Passaggio 6.3. Configurazione delle interfacce AMI

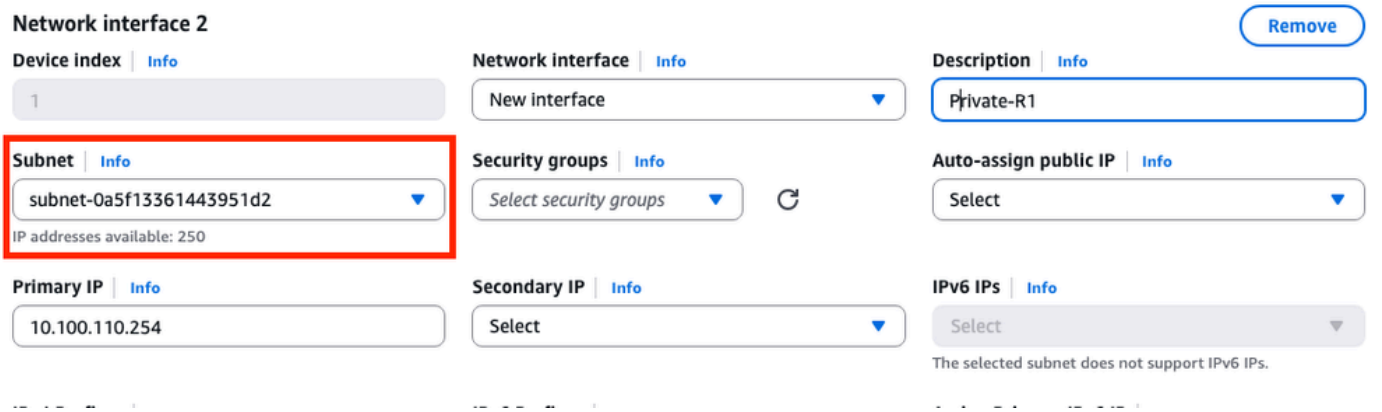
Nella sezione Impostazioni di rete espandere la sottosezione Configurazione di rete avanzata. Vengono visualizzate le seguenti opzioni:



In questo menu, impostare i parametri Description, Primary IP, Delete on terminal (Descrizione, IP primario, Elimina su terminazione).
Per il parametro Primary IP, utilizzare qualsiasi indirizzo IP ad eccezione del primo indirizzo disponibile della subnet. Viene utilizzato internamente da AWS.

Il parametro Elimina alla cessazione in questo esempio è impostato su No. Tuttavia, è possibile impostare questa opzione su yes a seconda dell'ambiente.

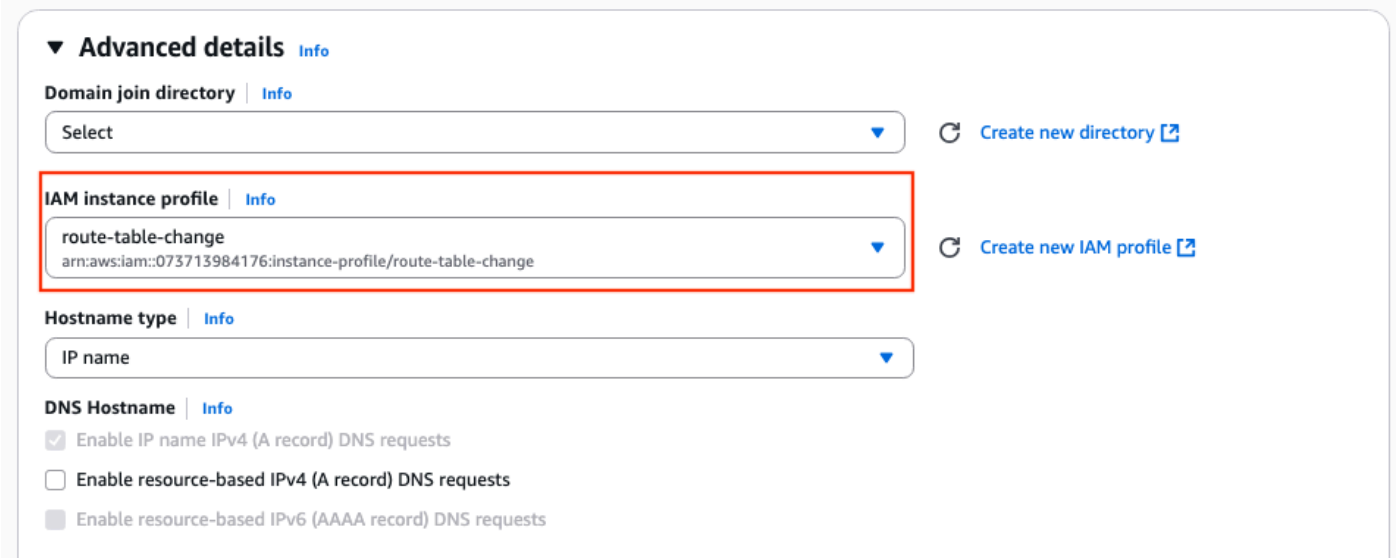
A causa di questa topologia, è necessaria una seconda interfaccia per la subnet privata. Fare clic su Add network interface (Aggiungi interfaccia di rete) per visualizzare il prompt. Tuttavia, l'interfaccia fornisce l'opzione per selezionare la subnet questa volta:



Dopo aver impostato tutti i parametri come nell'interfaccia di rete 1, continuare con i passaggi successivi.

Passaggio 6.4. Impostare il profilo dell'istanza IAM su AMI

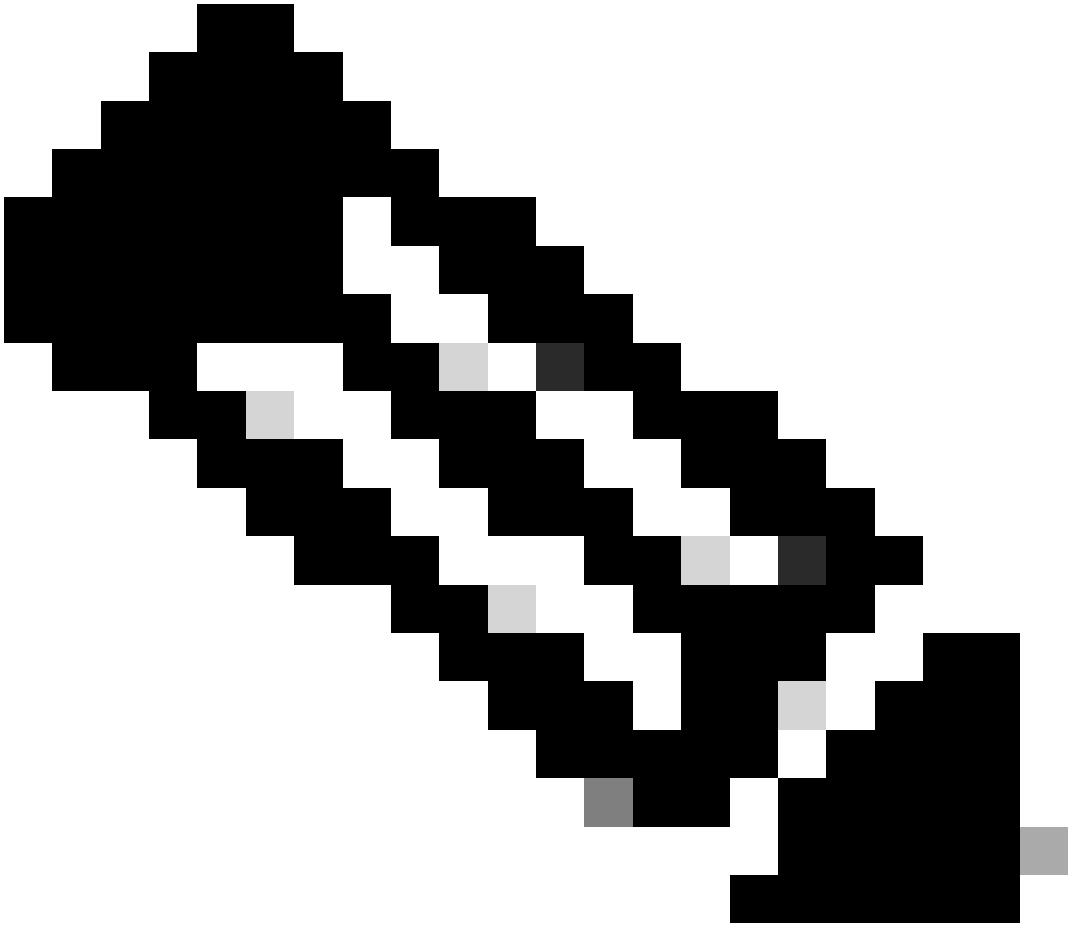
Nella sezione Dettagli avanzati, selezionare il ruolo IAM creato nel parametro di profilo dell'istanza IAM:



Passaggio 6.5. (Facoltativo) Impostazione delle credenziali sull'AMI

Nella sezione Dettagli avanzati passare alla sezione Dati utente - facoltativo e applicare questa impostazione per impostare un nome utente e una password durante la creazione dell'istanza:

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



Nota: Il nome utente fornito da AWS a SSH nel C800v può essere erroneamente elencato come root. Se necessario, passare a ec2-user.

Passaggio 6.6. Completamento della configurazione dell'istanza

Una volta configurati tutti gli elementi, fare clic su Avvia istanza:

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.

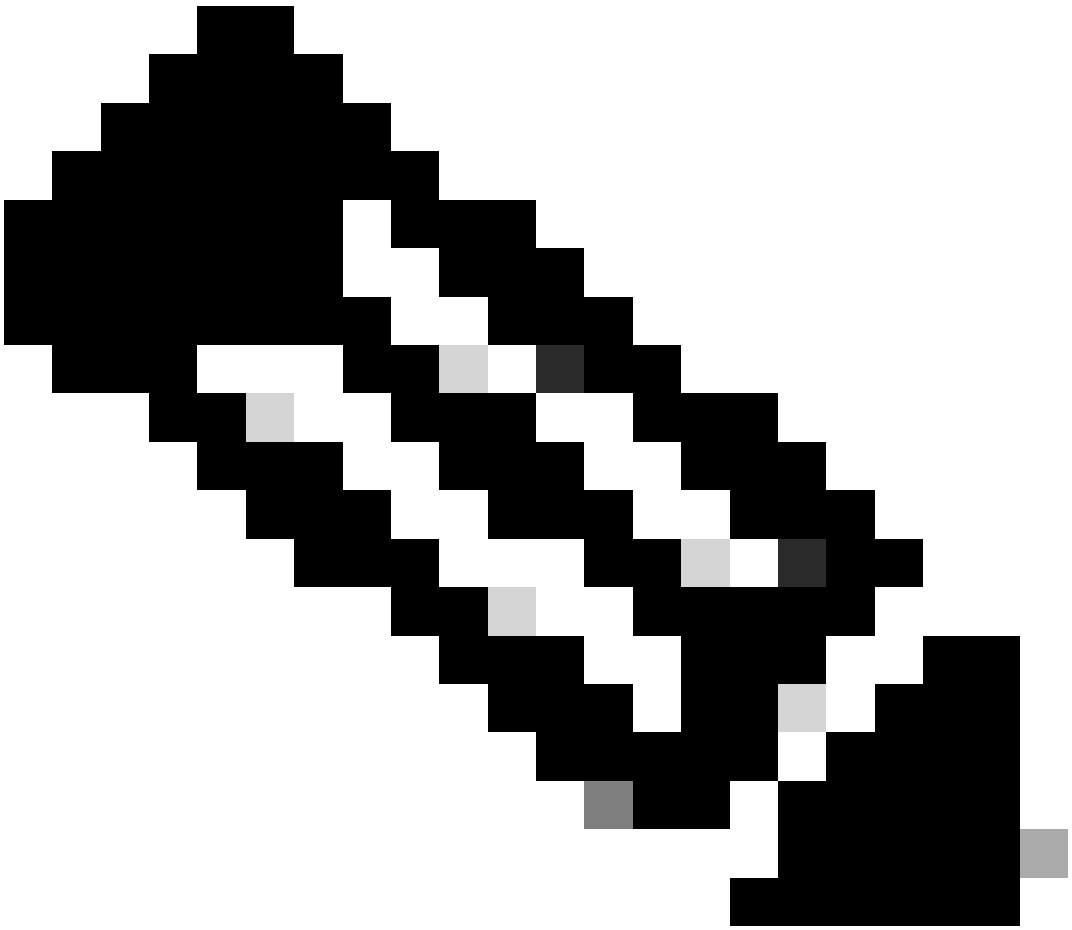
Cancel

Launch instance

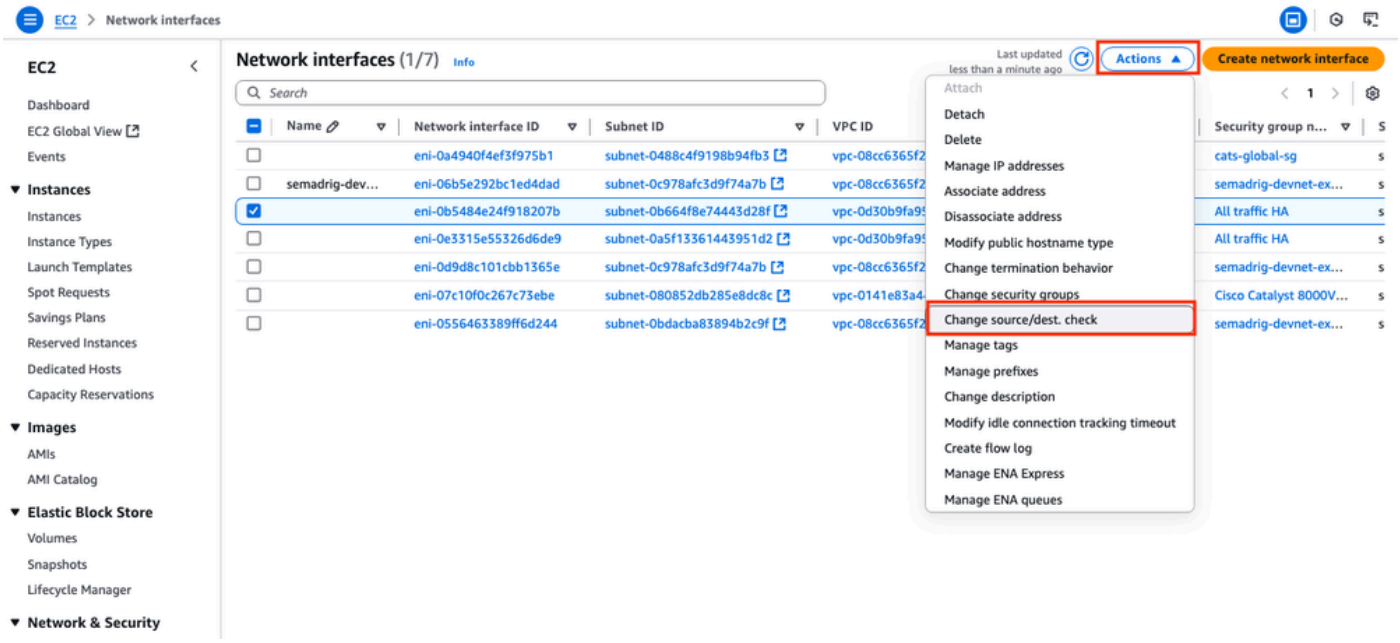
Preview code

Passaggio 6.7. Disattivare il controllo dell'origine/destinazione negli ENI

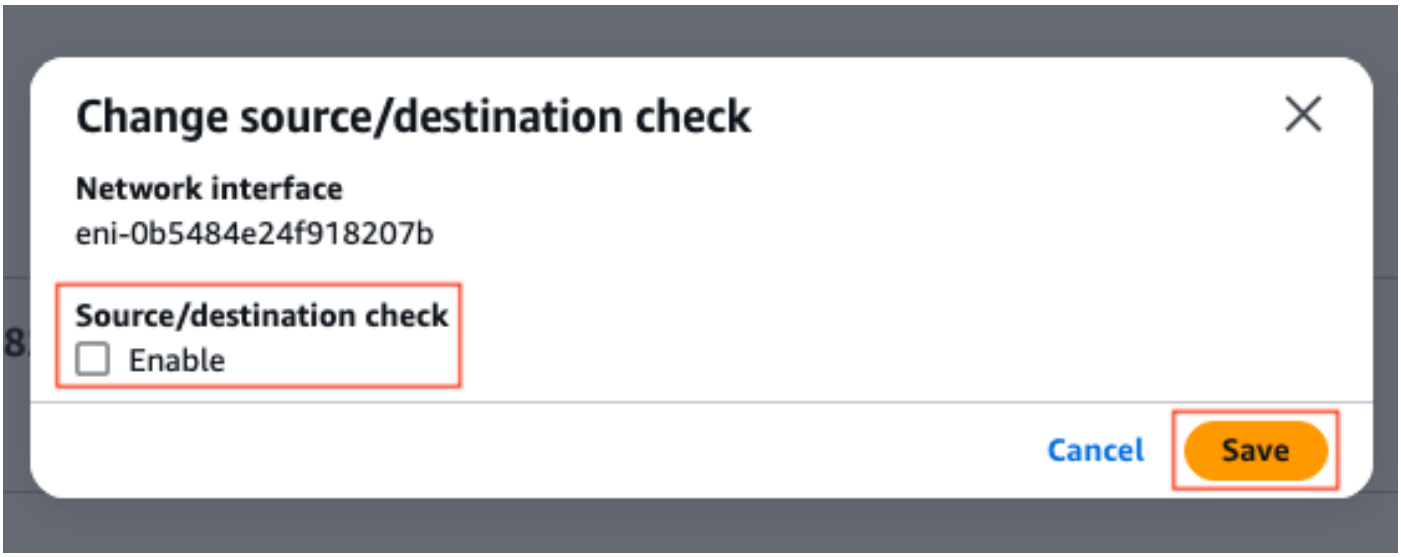
Una volta creata l'istanza, disabilitare la funzionalità di controllo src/dst in AWS per ottenere la connettività tra le interfacce nella stessa subnet. Nella sezione EC2 Dashboard > Rete e sicurezza > Interfacce di rete, selezionare gli ENI e fare clic su Azioni > Cambia origine/destinazione. controllare.



Nota: Per rendere disponibile questa opzione, è necessario selezionare uno alla volta l'ENI.



Viene visualizzata una nuova finestra. Nel menu Nuovo, disattivare la casella di controllo Abilita e fare clic su Salva.

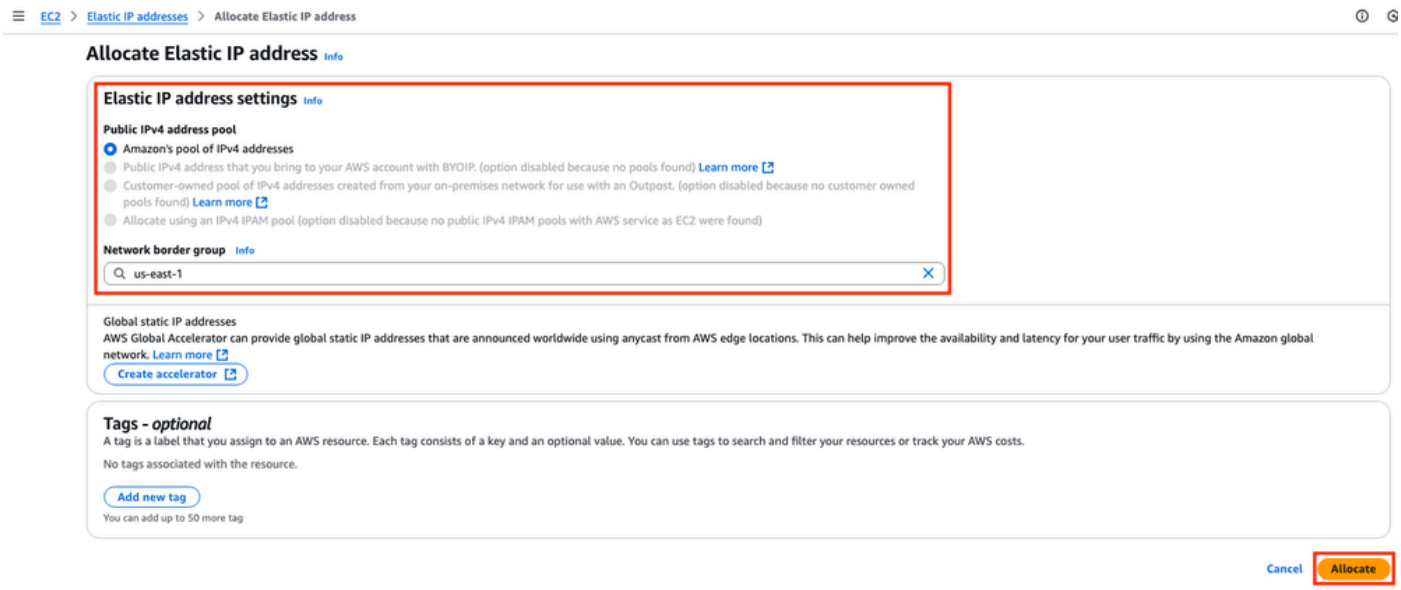


Passaggio 6.8. Creazione e associazione di un indirizzo IP elastico all'ENI pubblico dell'istanza

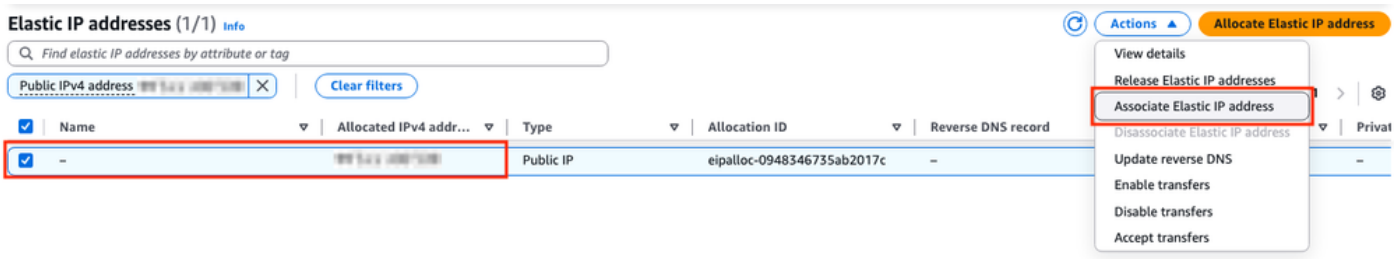
Nella sezione EC2 Dashboard > Rete e sicurezza > IP elastici, fare clic su Alloca indirizzo IP elastico.

La pagina consente di passare a un'altra sezione. Per questo esempio, l'opzione Pool Amazon di indirizzi IPv4 è selezionata insieme alla zona di disponibilità us-east-1. Al termine, fare clic su

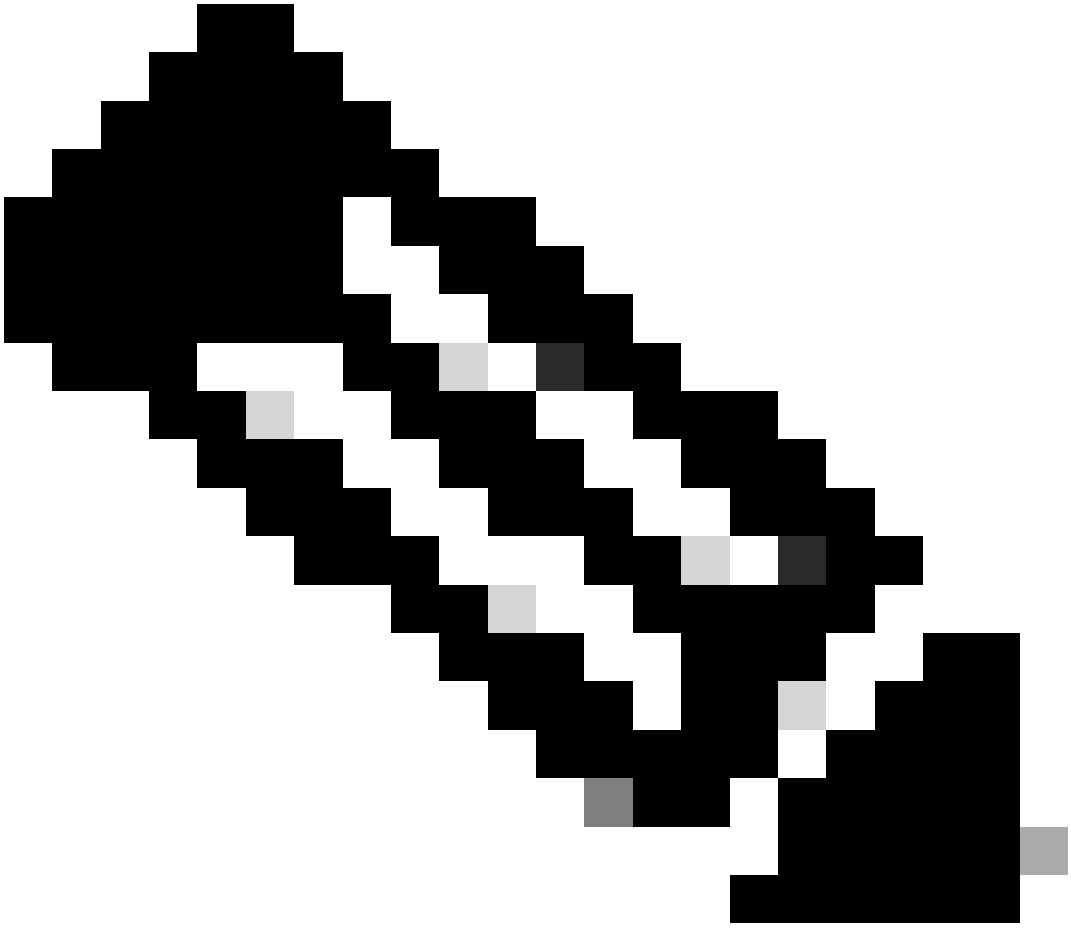
Alloca.



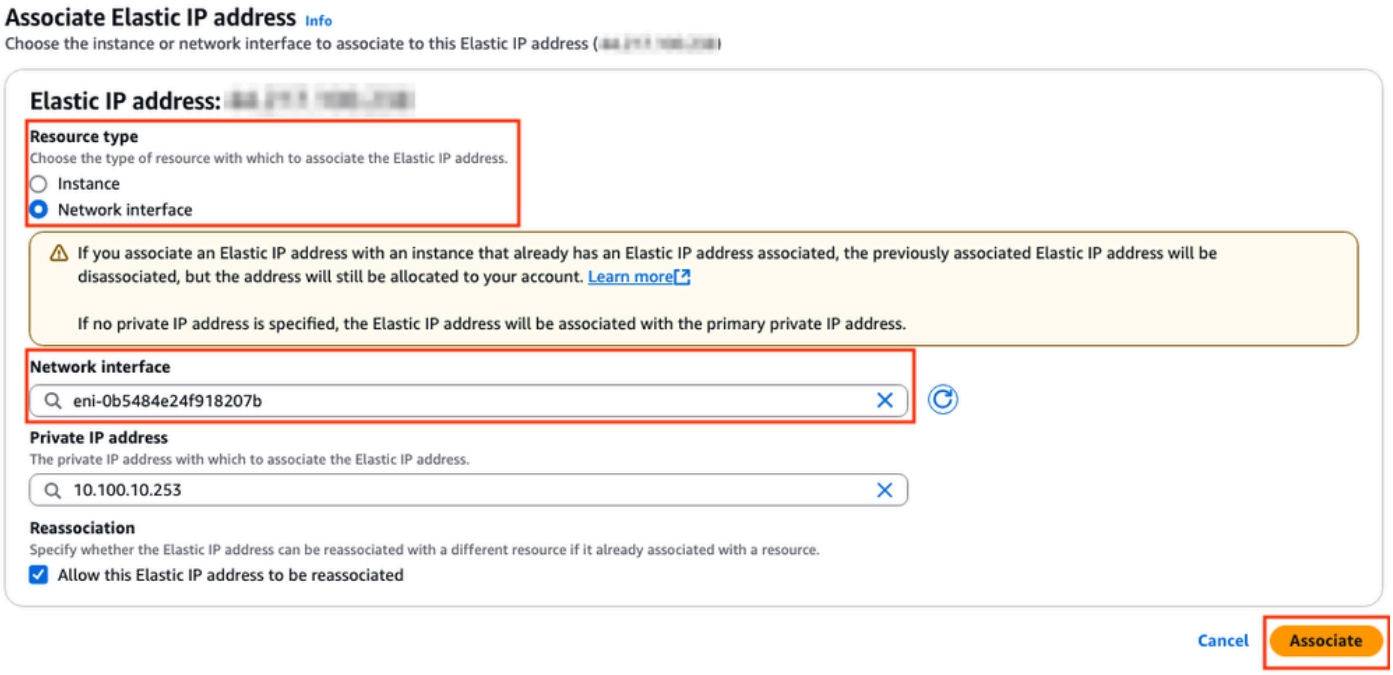
Al momento della creazione dell'indirizzo IP, assegnarlo all'interfaccia pubblica dell'istanza. Nella sezione EC2 Dashboard > Rete e sicurezza > IP elastici, fare clic su Azioni > Associa indirizzo IP elastico.



In questa nuova sezione, selezionare l'opzione Network interface (Interfaccia di rete) e cercare l'ENI pubblico dell'interfaccia corrispondente. Associare l'indirizzo IP pubblico corrispondente e fare clic su Associa.



Nota: Per ottenere l'ID ENI corretto, passare alla sezione Dashboard EC2 > Istanze. Selezionare quindi l'istanza e controllare la sezione Rete. Cercare l'indirizzo IP dell'interfaccia pubblica per ottenere il valore ENI sulla stessa riga.



Passaggio 7. Ripetere il passaggio 6 per creare la seconda istanza C8000v per HA

Fare riferimento alla sezione Topologia di questo documento per avere le informazioni corrispondenti per ciascuna interfaccia e ripetere gli stessi passaggi da 6.1 a 6.6.

Passaggio 8. Ripetere il passaggio 6 per creare una macchina virtuale (Linux/Windows) da AMI Marketplace

Per questo esempio, Ubuntu server 22.04.5 LTS è selezionato da AMI Marketplace come host interno.

ens5 viene creato per impostazione predefinita per l'interfaccia pubblica. Per questo esempio, creare una seconda interfaccia (ens6 sul dispositivo) per la subnet privata.

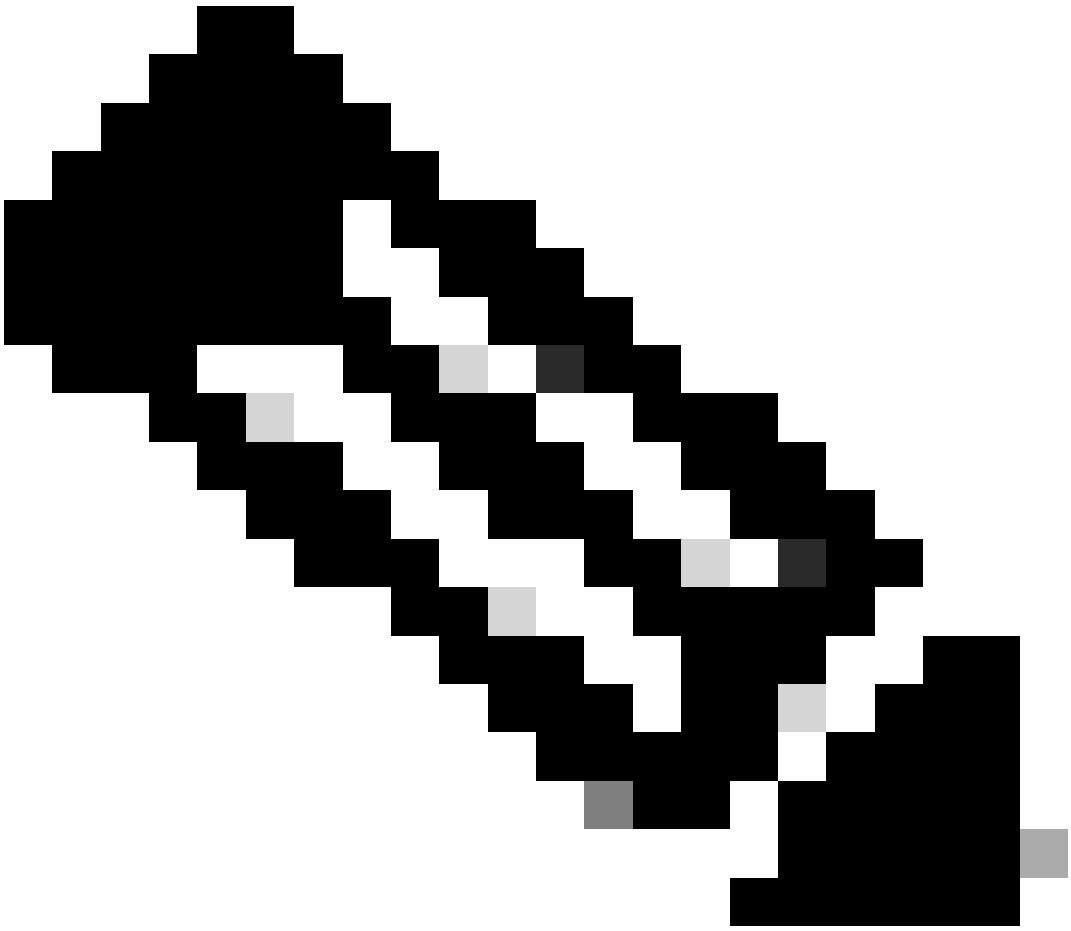
<#root>

```
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
```

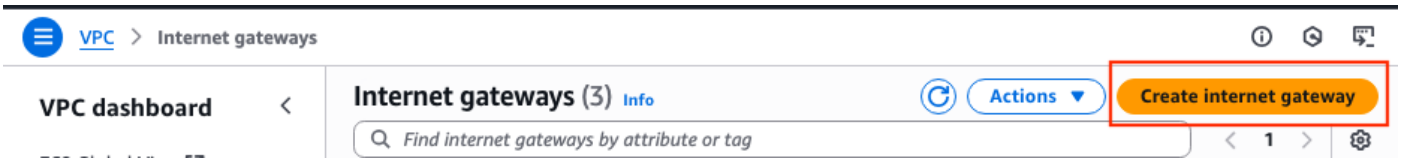
```
10.100.130.254

 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
```



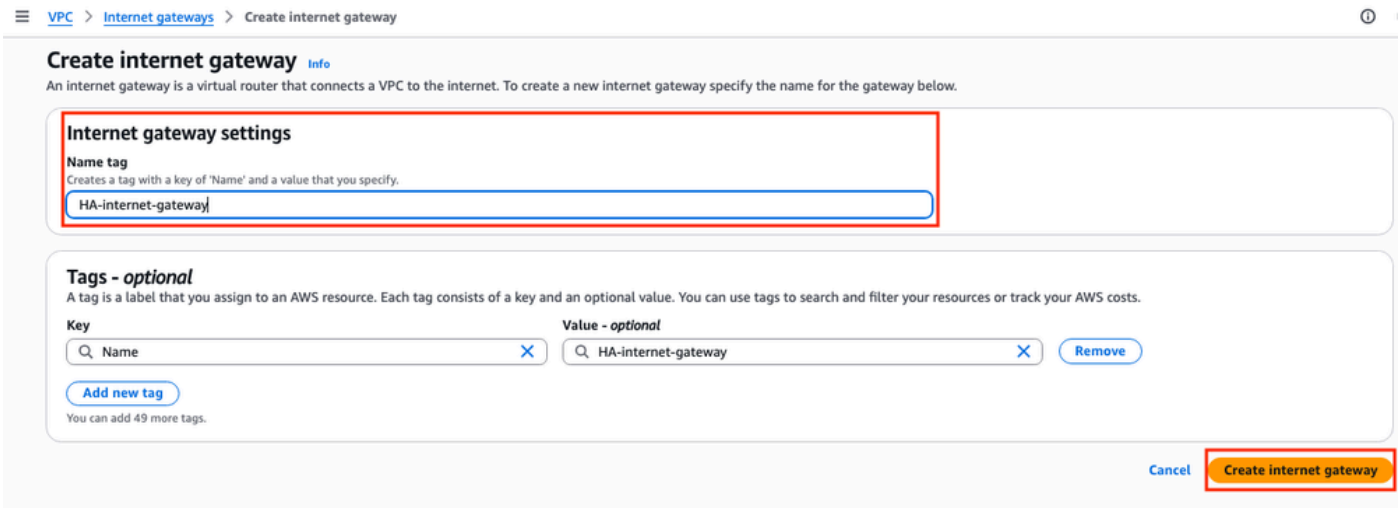
> Nota: Se vengono apportate modifiche alle interfacce, eseguire il flap dell'interfaccia o ricaricare la VM per applicare le modifiche.

Passaggio 9. Creare e configurare un gateway Internet (IGW) per il VPC

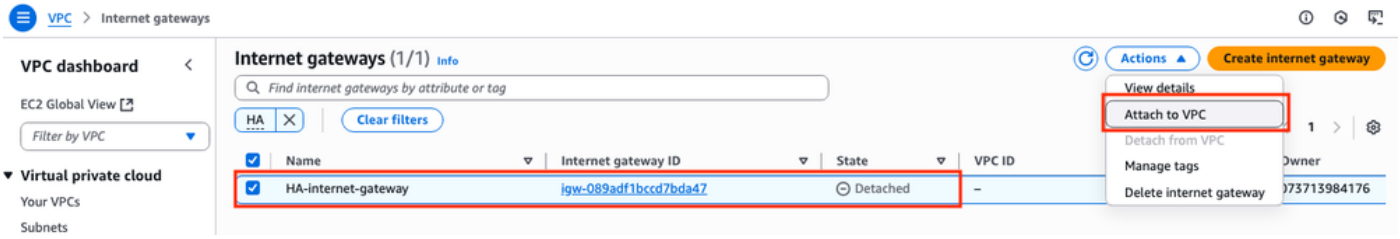
Nella sezione **Dashboard VPC > Virtual Private Cloud > Internet Gateway** fare clic su **Crea gateway Internet**.



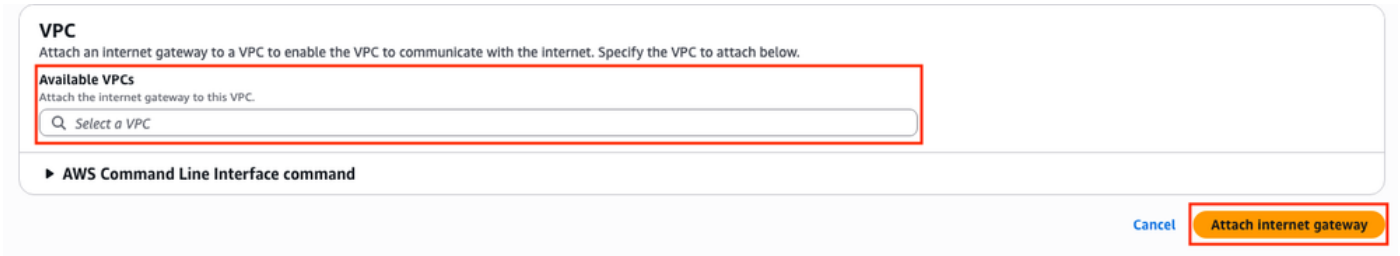
In questa nuova sezione creare un **tag name** per il gateway e fare clic su **Crea gateway Internet**.



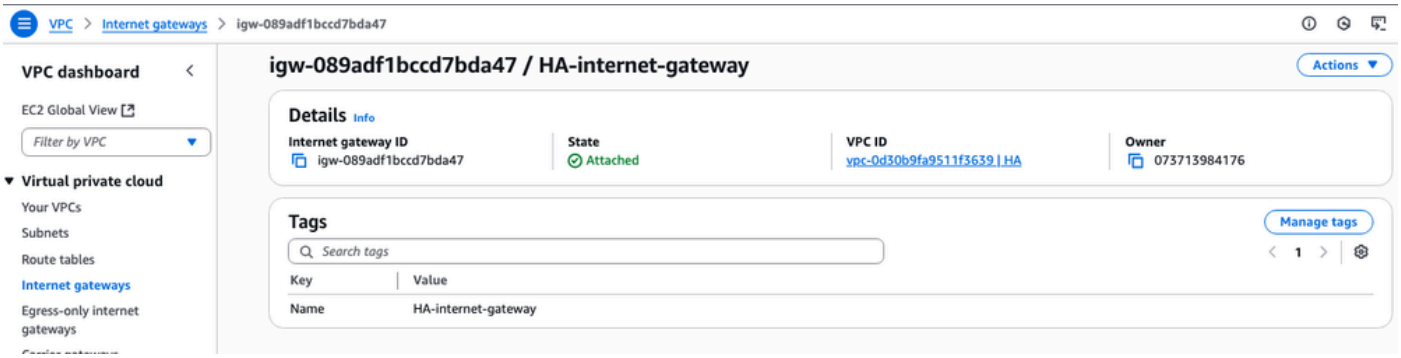
Una volta creato l'IGW, collegarlo al VPC corrispondente. Passare alla sezione **VPC Dashboard > Virtual Private Cloud > Internet Gateway** e selezionare l'IGW corrispondente. Fare clic su **Azioni > Associa a VPC**.



In questa nuova sezione selezionare il VPC denominato **HA**. Per questo esempio, fare clic su **Collega gateway Internet**.



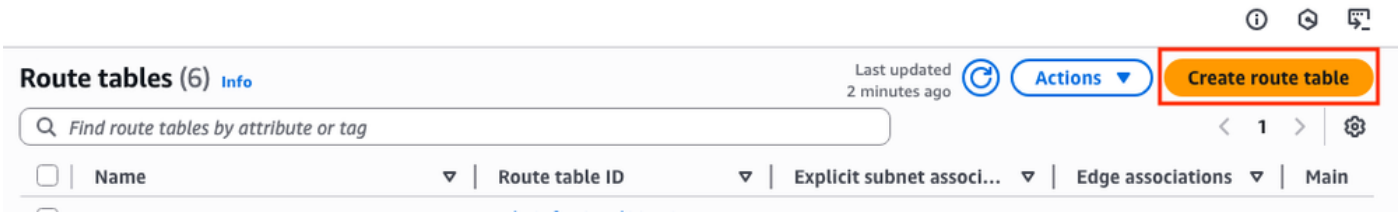
L'IGW deve indicare lo stato Attaccato come mostrato:



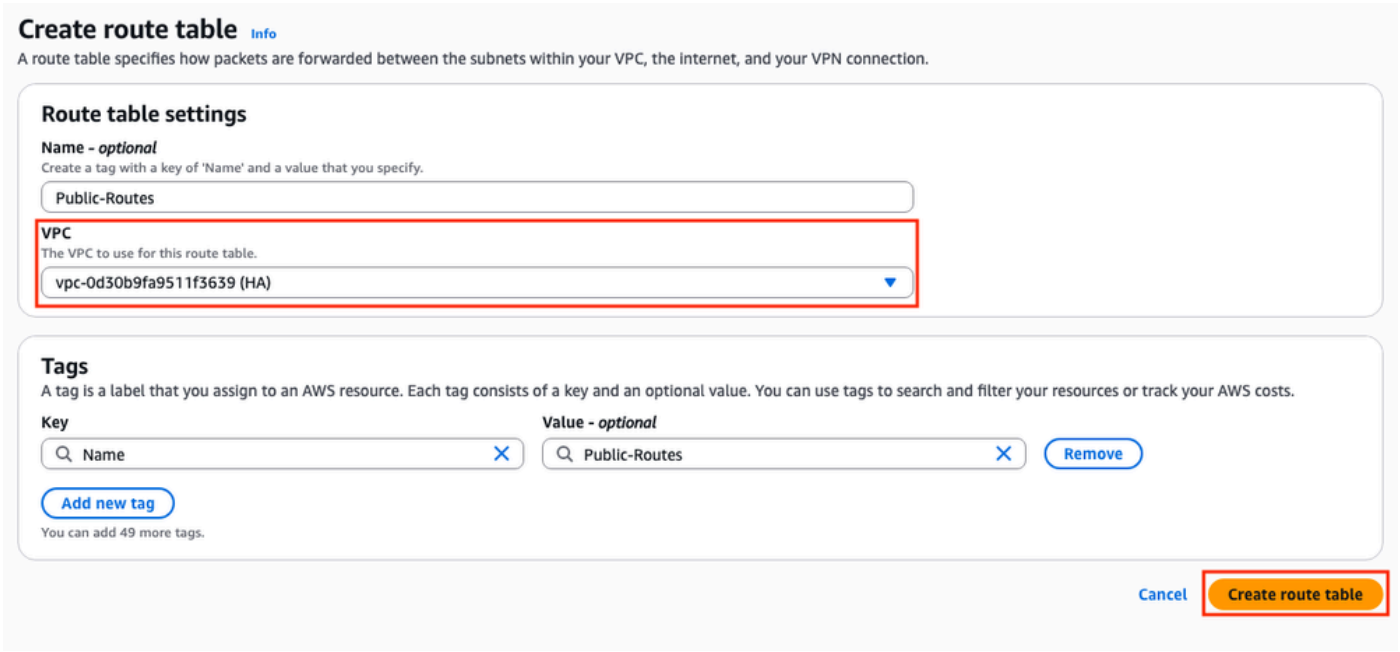
Passaggio 10. Creare e configurare le tabelle di routing in AWS per le subnet pubbliche e private

Passaggio 10.1. Creare e configurare la tabella di route pubblica

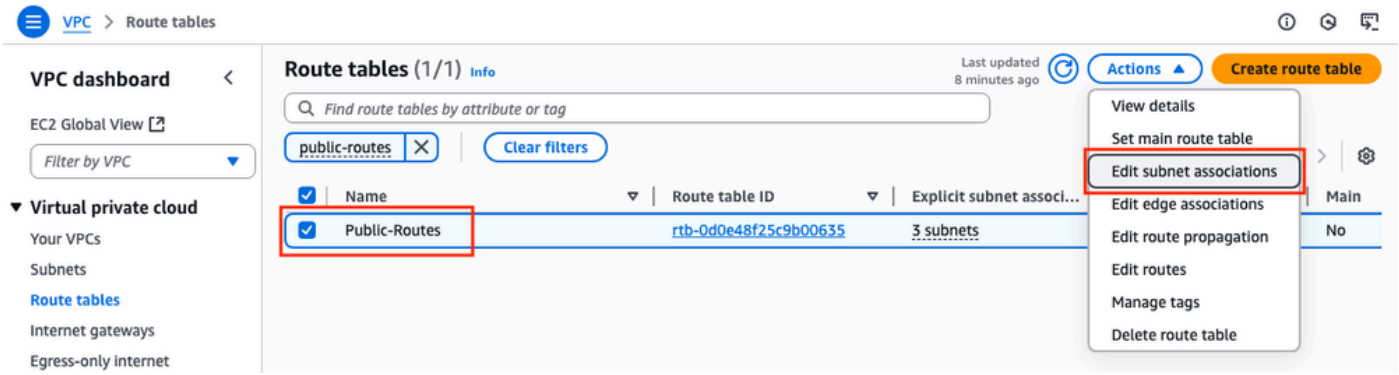
Per stabilire l'HA su questa topologia, associare tutte le subnet pubbliche e private alle tabelle di route corrispondenti. Nella sezione Dashboard VPC > Virtual Private Cloud > Route tables, fare clic su Create route table.



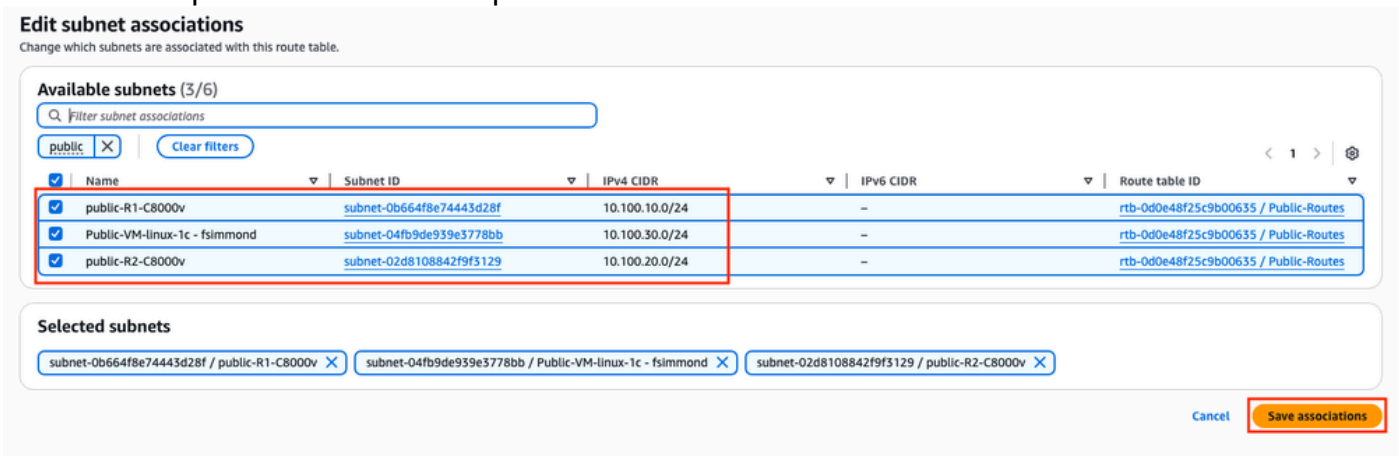
Nella nuova sezione selezionare il VPC corrispondente per questa topologia. Una volta selezionato, fare clic su Crea tabella di route.



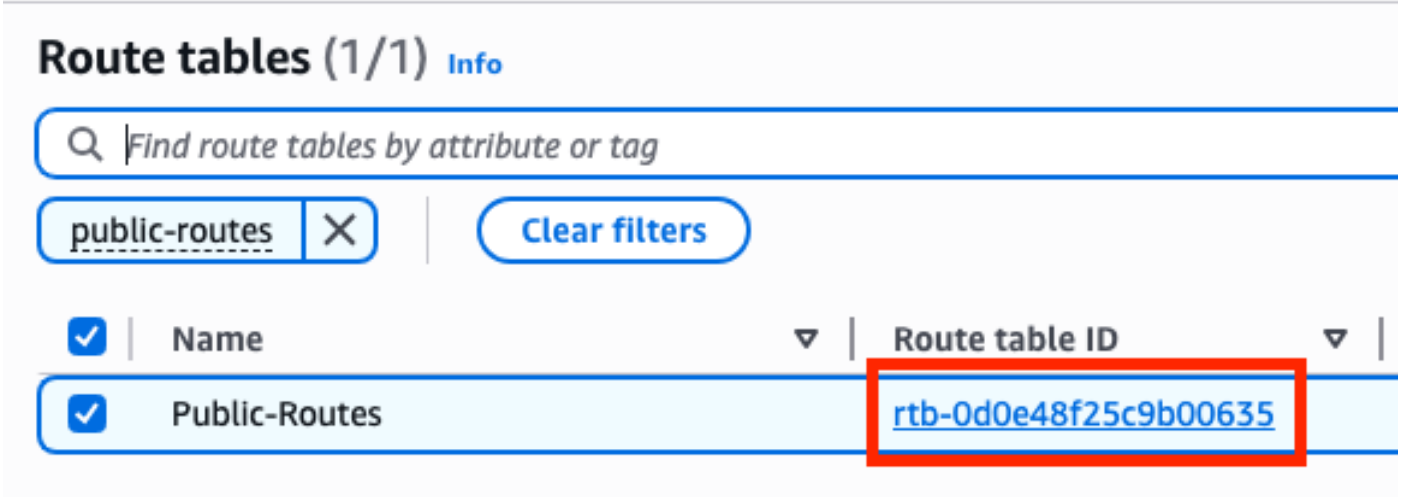
Nella sezione Tabelle di instradamento, selezionare la tabella creata e fare clic su Azioni > Modifica associazioni subnet.



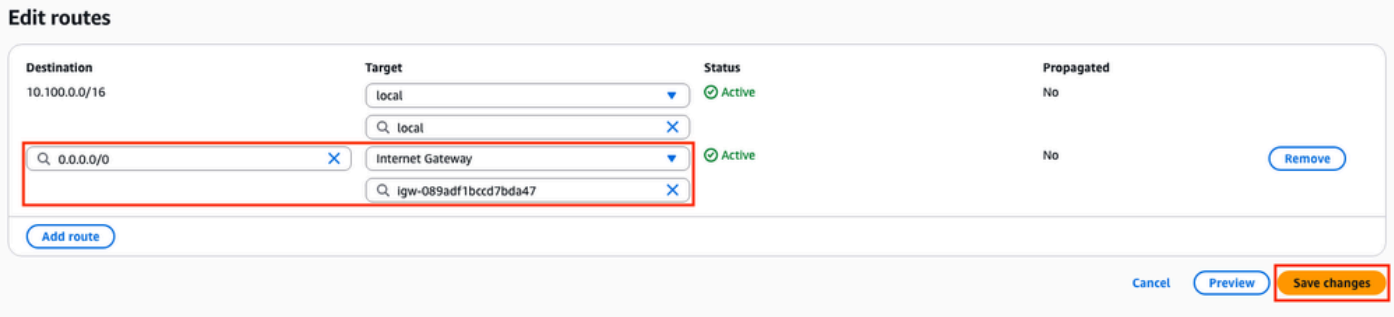
Selezionare quindi le subnet corrispondenti e fare clic su Salva associazioni.



Una volta associate le subnet, fare clic sul collegamento ipertestuale ID tabella route per aggiungere le route appropriate per la tabella. Quindi, fare clic su Modifica instradamenti:

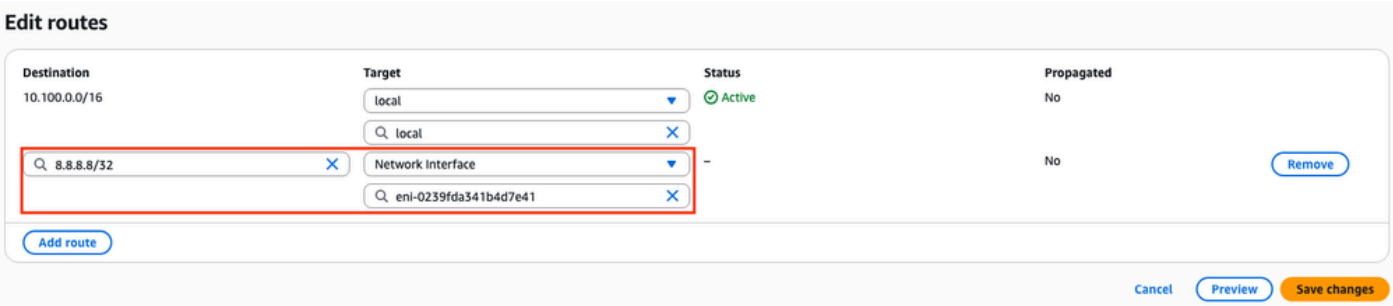


Per ottenere l'accesso a Internet, fare clic su Add route e collegare questa tabella di route pubblica con l'IGW creato nel passo 9 con questi parametri. Una volta selezionato, fare clic su Salva modifiche:



Passaggio 10.2. Creazione e configurazione della tabella di route privata

Dopo aver creato la tabella delle route pubbliche, replicare il passaggio 10 per la route privata e le subnet private, ad eccezione dell'aggiunta del gateway Internet sulle relative route. Nell'esempio, la tabella di routing è simile alla seguente, in quanto il traffico della versione 8.8.8.8 deve passare attraverso la subnet privata illustrata nell'esempio:



Passaggio 11. Controllare e configurare la configurazione di rete base, Network Address Translation (NAT), il tunnel GRE con BFD e il protocollo di routing

Una volta preparate le istanze e la relativa configurazione di routing su AWS, configurare i dispositivi:

Configurazione C800v 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
```

Configurazione C800v 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
```

Passaggio 12. Configurazione dell'alta disponibilità (Cisco IOS® XE Denali 16.3.1a o versioni successive)

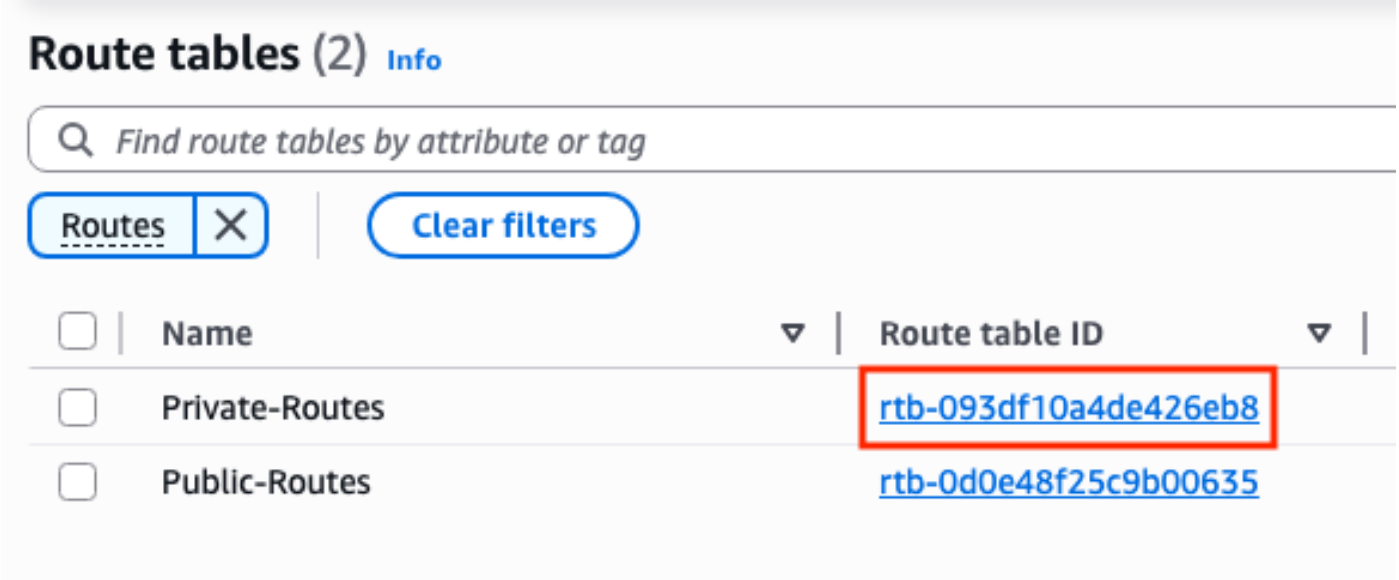
Dopo aver impostato la ridondanza e la connessione tra le VM, configurare le impostazioni HA per definire le modifiche di routing. Impostare i valori Route-table-id, Network-interface-id e CIDR che devono essere impostati dopo un errore AWS HA, ad esempio peer down BFD.

```
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>
```

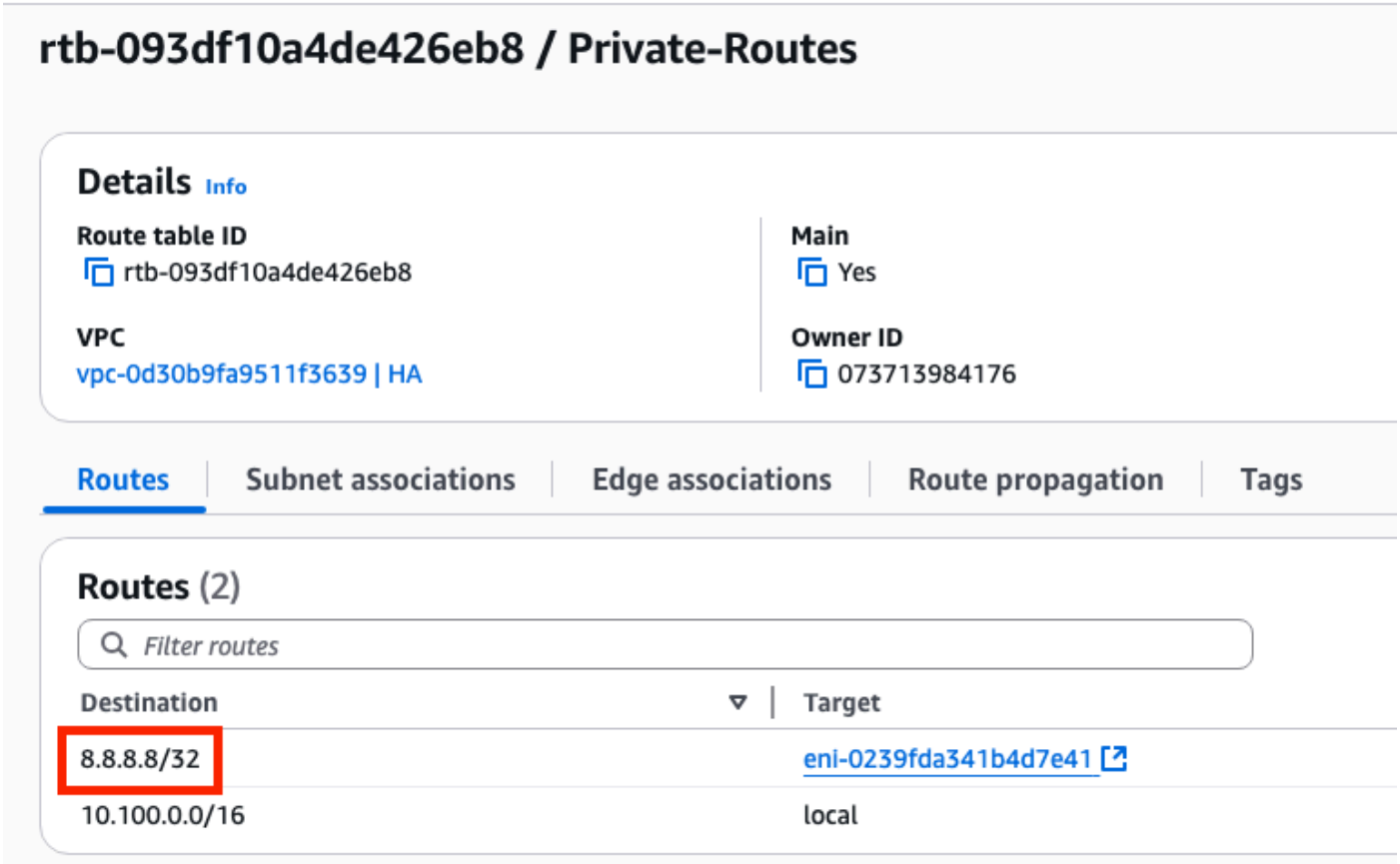
Il parametro bfd peer è correlato all'indirizzo IP del peer del tunnel. Per controllare questa condizione, usare l'output show bfd neighbors:

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

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

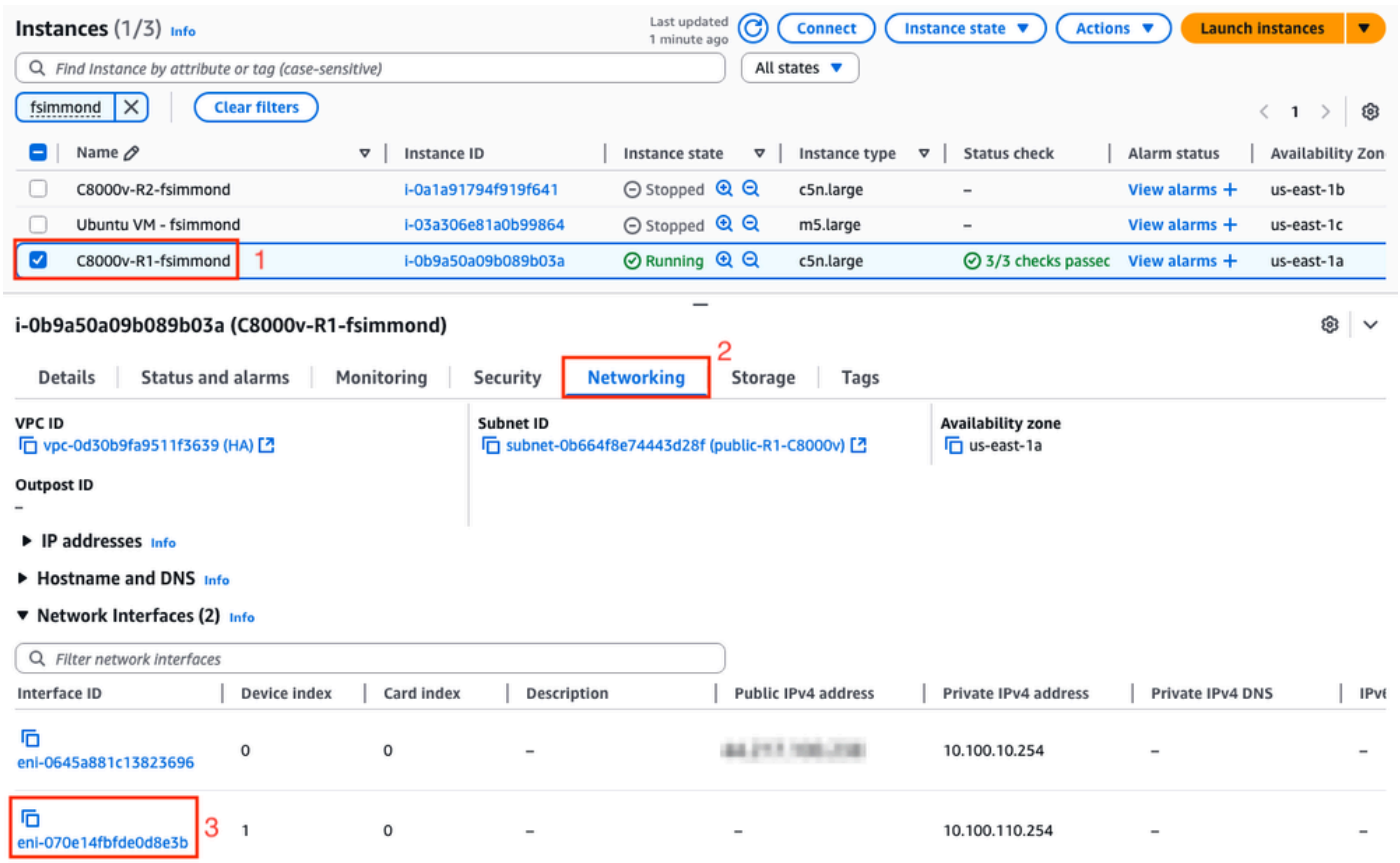
Il parametro route-table è correlato all'ID della tabella di route privata che si trova nella sezione Dashboard VPC > Virtual Private Cloud > Route Tables. Copiare l'ID tabella di route corrispondente.



Il parametro cidr ip è correlato al prefisso della route aggiunto nella tabella della route privata (route create al passaggio 10.2):



Il parametro eni è correlato all'ID ENI dell'interfaccia privata corrispondente dell'istanza in fase di configurazione. Per questo esempio, viene utilizzato l'ID ENI dell'interfaccia Gigabit Ethernet2 dell'istanza:



Il parametro region è correlato al nome di codice indicato nella documentazione di AWS per l'area in cui si trova il VPC. Per questo esempio, viene utilizzata la regione us-east-1.

L'elenco può tuttavia essere modificato o ampliato. Per trovare gli ultimi aggiornamenti, visitare il documento AmazonRegion and Availability Zonesdocument.

Tenendo conto di tutte queste informazioni, ecco l'esempio di configurazione per ciascun router del VPC:

Esempio di configurazione per C800v 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
```

Esempio di configurazione per C800v 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
```

Verifica

1. Verificare lo stato dell'istanza C8000v R1. Confermare che la ridondanza tunnel e cloud sia attiva e in esecuzione.

```
R1#show bfd neighbors

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

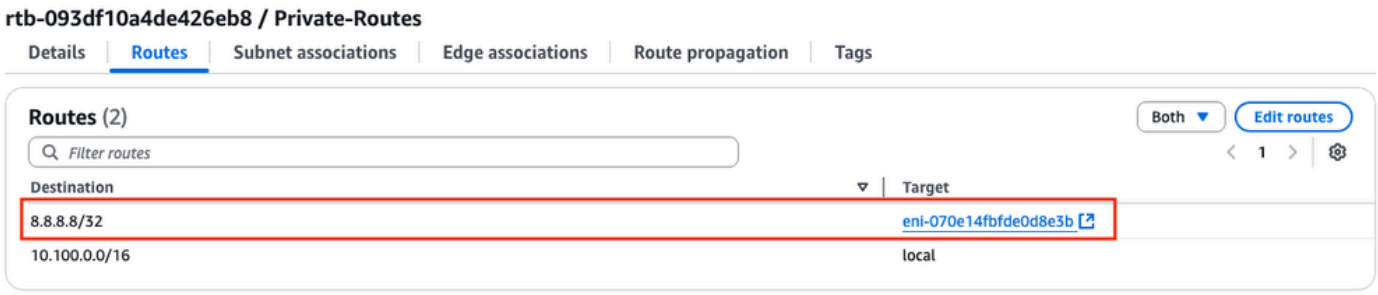
```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.200.2 Tu1 10 00:16:52 2 1470 0 2
```

```
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. Eseguire un ping continuo fino a 8.8.8.8 dalla VM host dietro i router. Verificare che il ping stia passando attraverso l'interfaccia privata:

```
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. Aprire AWS WebGUI e controllare lo stato della tabella di routing. L'ENI corrente appartiene all'interfaccia privata dell'istanza di R1:



4. Attivare la modifica del percorso chiudendo l'interfaccia Tunnel1 sull'istanza R1 per simulare un evento di failover HA:

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

5. Controllare nuovamente alla tabella di rotta su AWS, l'ID ENI è stato modificato in ID ENI dell'interfaccia privata R2:

Risoluzione dei problemi

Questi sono i punti più comuni che vengono spesso dimenticati/configurati in modo errato durante la ricreazione dell'installazione:

- Verificare 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.
  Se sono già stati controllati tutti i punti discussi in questa sezione e il problema è ancora presente, raccogliere questi output, verificare il failover HA, se possibile, e aprire una richiesta con Cisco TAC:

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

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).