

Distribuisci configurazione alta disponibilità C8000v su AWS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Topologia](#)

[Esempio di rete](#)

[Riepilogo tabella](#)

[Restrizioni](#)

[Configurazione](#)

[Passaggio 1. Selezionare un'area](#)

[Passaggio 2. Creare il VPC](#)

[Passaggio 3. Creare un gruppo di sicurezza per il VPC](#)

[Passaggio 4. Creare un ruolo IAM con un criterio e associarsi al VPC](#)

[Passaggio 5. Creare e allegare un criterio di attendibilità a un ruolo IAM](#)

[Passaggio 6. Configurare e avviare le istanze di C8000v](#)

[Passaggio 6.1. Configurazione della coppia di chiavi per l'accesso remoto](#)

[Passaggio 6.2. Creazione e configurazione delle subnet per l'AMI](#)

[Passaggio 6.3. Configurazione delle interfacce AMI](#)

[Passaggio 6.4. Impostare il profilo dell'istanza IAM su AMI](#)

[Passaggio 6.5. \(Facoltativo\) Impostazione delle credenziali sull'AMI](#)

[Passaggio 6.6. Completamento della configurazione dell'istanza](#)

[Passaggio 6.7. Disattivare il controllo dell'origine/destinazione negli ENI](#)

[Passaggio 6.8. Creazione e associazione di un indirizzo IP elastico all'ENI pubblico dell'istanza](#)

[Passaggio 7. Ripetere il passaggio 6 per creare la seconda istanza C8000v per HA](#)

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

[Passaggio 9. Creare e configurare un gateway Internet \(IGW\) per il VPC](#)

[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](#)

[Passaggio 10.2. Creazione e configurazione della tabella di route privata](#)

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

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

[Verifica](#)

[Risoluzione dei problemi](#)

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® XE Denali 17.15.3a)
- 1x - VM (Linux/Windows)

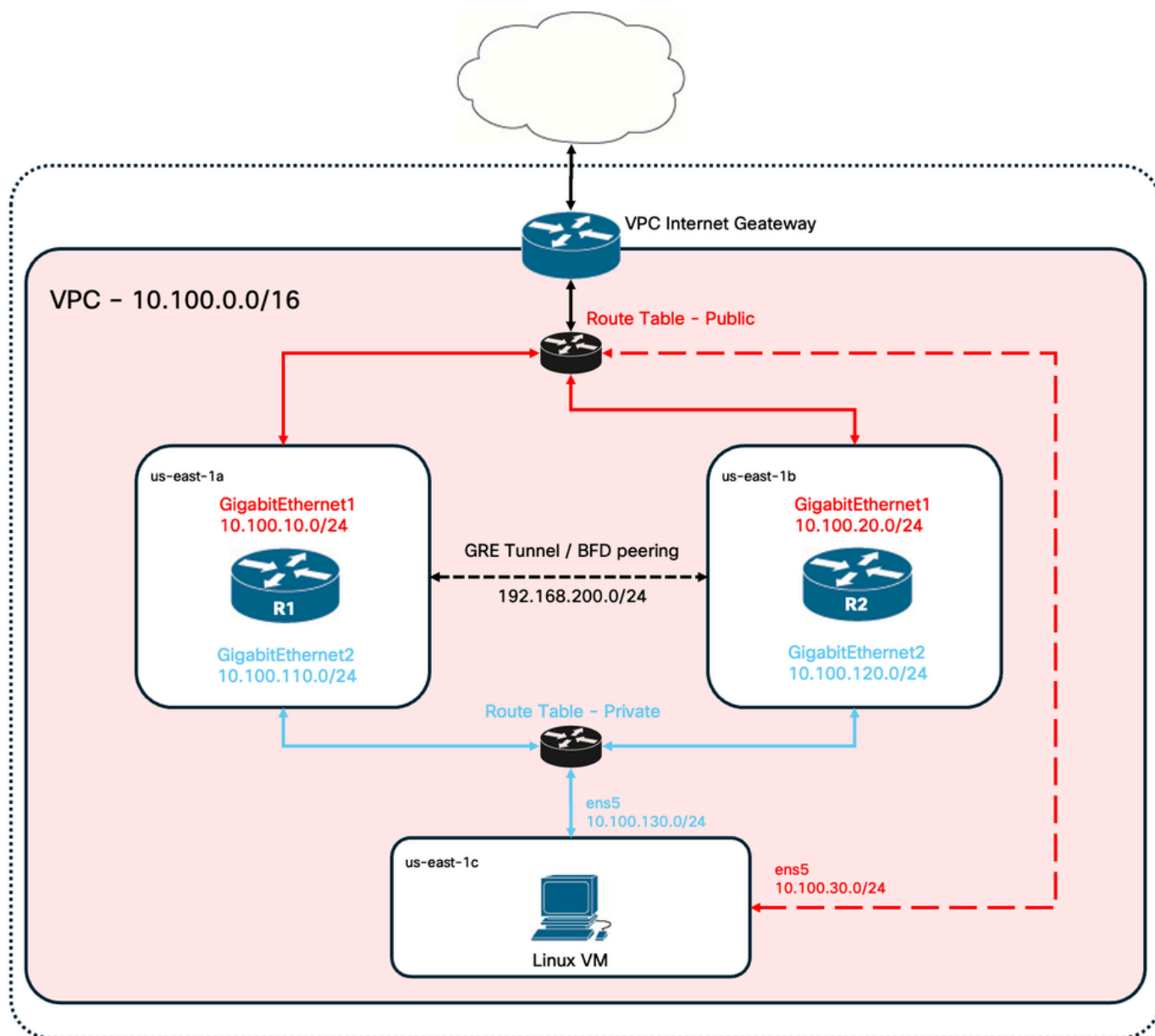
In una coppia HA sono presenti 2 router C8000v, in due diverse zone di disponibilità. Ogni zona di disponibilità può essere considerata come un centro dati separato per una resilienza hardware aggiuntiva.

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.

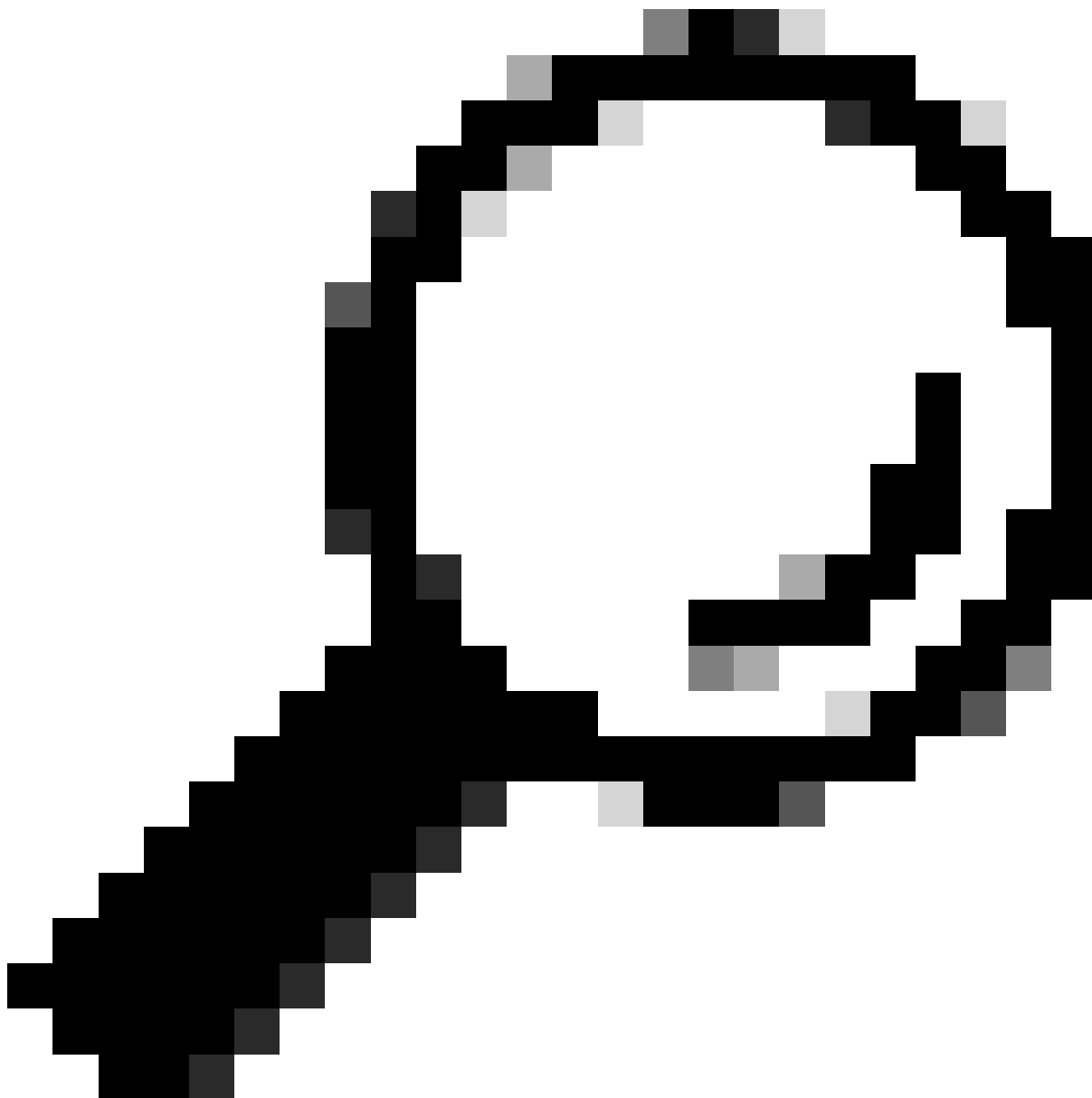
Per simulare il traffico, avviare un ping dall'interfaccia privata della macchina virtuale, attraversando la tabella di routing privata attraverso R1 fino a raggiungere la posizione 8.8.8.8. In caso di failover, verificare che la tabella di routing privata sia stata aggiornata automaticamente in modo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

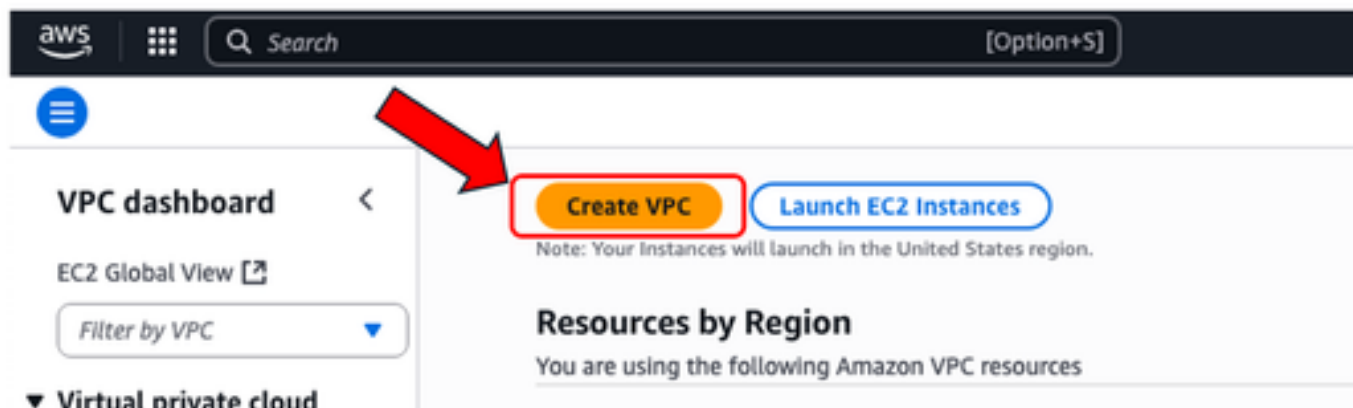
Passaggio 1. Selezionare un'area

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.

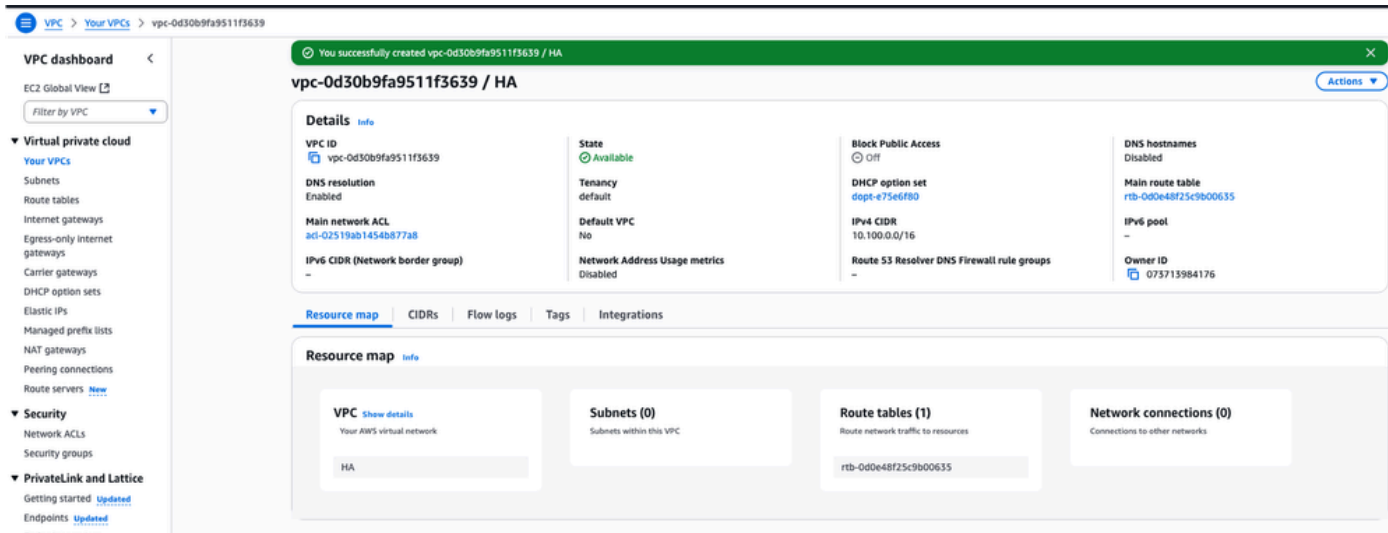


Quando si crea il VPC, selezionare l'opzione Solo VPC. È possibile assegnare una rete /16 da utilizzare come desiderato.

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

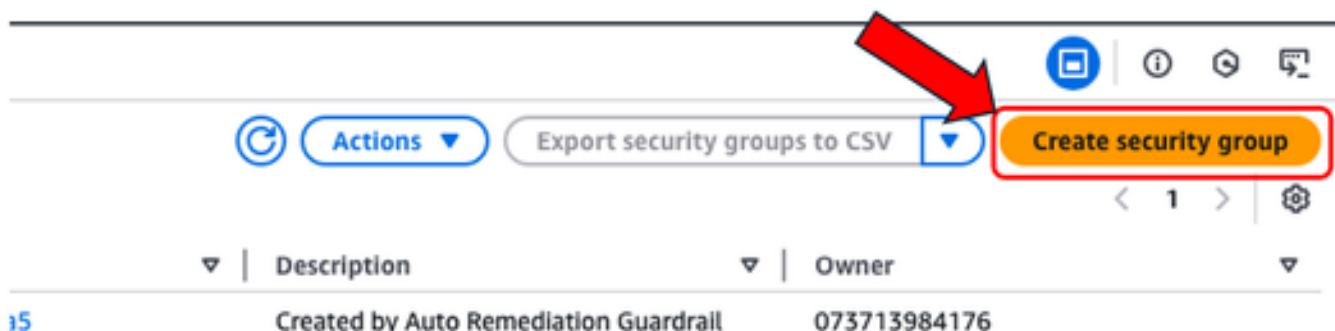
The image shows the 'Create VPC' form in the AWS console. The form is titled 'Create VPC' and includes a description: 'A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.' The 'VPC settings' section contains several options: 'Resources to create' (VPC only selected), 'Name tag - optional' (optional), 'IPv4 CIDR block' (IPv4 CIDR manual input selected, 10.100.0.0/16), 'IPv6 CIDR block' (No IPv6 CIDR block selected), and 'Tenancy' (Default). A red arrow points to the 'Create VPC' button at the bottom right. The form also includes a 'Tags' section with a key-value pair (Name, HA) and an 'Add tag' button.

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.

VPC > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

Inbound rules Info

Type	Protocol	Port range	Source	Description - optional	
All traffic	All	All	Anywhere...		Delete
0.0.0.0/0					

Add rule

Outbound rules Info

Type	Protocol	Port range	Destination	Description - optional	
All traffic	All	All	Custom		Delete
0.0.0.0/0					

Add rule

Tags - optional Info

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Create security group

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:

AWS IAM > Roles

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Roles (65) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

☐	Role name	Trusted entities	Last activity
☐	admin	Identity Provider: amaws:iam::0737	52 days ago
☐	AmazonAppStreamServiceAccess	AWS Service: appstream	-
☐	ApplicationAutoScalingForAmazonAppStreamAccess	AWS Service: application-autoscaling	-
☐	aws-codestar-service-role	AWS Service: codestar	-
☐	aws-elasticbeanstalk-ec2-role	AWS Service: ec2	-
☐	aws-elasticbeanstalk-service-role	AWS Service: elasticbeanstalk	-
☐	AWSCloud9SSMAccessRole	AWS Service: ec2 and 1 more	-
☐	AWSServiceRoleForAmazonSSM	AWS Service: ssm (Service-Linked Role)	42 minutes ago
☐	AWSServiceRoleForAPIGateway	AWS Service: ops.apigateway (Service-Linked Role)	-

Create role

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

- Step 1
● **Select trusted entity**
- Step 2
○ Add permissions
- Step 3
○ Name, review, and create

Select trusted entity Info

Trusted entity type

☒ **AWS service**

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**

Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

☒ **EC2**

Allows EC2 instances to call AWS services on your behalf.

☐ **EC2 Role for AWS Systems Manager**

Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

☐ **EC2 Spot Fleet Role**

Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

☐ **EC2 - Spot Fleet Auto Scaling**

Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

☐ **EC2 - Spot Fleet Tagging**

Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

☐ **EC2 - Spot Instances**

Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

☐ **EC2 - Spot Fleet**

Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

☐ **EC2 - Scheduled Instances**

Allows EC2 Scheduled Instances to manage instances on your behalf.

Cancel

Next

Al termine, fare clic su Avanti:

IAM > Roles > Create role

Step 1

Step 2

Step 3

Step 4

Select trusted entity

Add permissions

Name, review, and create

Add permissions Info

Permissions policies (1062) Info

Choose one or more policies to attach to your new role.

Search

Filter by Type

All types

< 1 2 3 4 5 6 7 ... 54 >

☐	Policy name	Type	Description
☐	AdministratorAccess	AWS managed - job function	Provides full access to AWS services an...
☐	AdministratorAccess-Amplify	AWS managed	Grants account administrative permis...
☐	AdministratorAccess-AWSElasticBeanstalk	AWS managed	Grants account administrative permis...
☐	AIOpsAssistantPolicy	AWS managed	Provides ReadOnly permissions requir...
☐	AIOpsConsoleAdminPolicy	AWS managed	Grants full access to Amazon AI Opera...
☐	AIOpsOperatorAccess	AWS managed	Grants access to the Amazon AI Opera...
☐	AIOpsReadOnlyAccess	AWS managed	Grants ReadOnly permissions to the A...
☐	AlexaForBusinessDeviceSetup	AWS managed	Provide device setup access to AlexaFo...
☐	AlexaForBusinessFullAccess	AWS managed	Grants full access to AlexaForBusiness ...
☐	AlexaForBusinessGatewayExecution	AWS managed	Provide gateway execution access to A...
☐	AlexaForBusinessLifesizeDelegatedAccessP...	AWS managed	Provide access to Lifesize AVS devices
☐	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	Provide access to Poly AVS devices
☐	AlexaForBusinessReadOnlyAccess	AWS managed	Provide read only access to AlexaForB...
☐	AmazonAPIGatewayAdministrator	AWS managed	Provides full access to create/edit/dele...
☐	AmazonAPIGatewayInvokeFullAccess	AWS managed	Provides full access to invoke APIs in A...
☐	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	Allows API Gateway to push logs to us...
☐	AmazonAppFlowFullAccess	AWS managed	Provides full access to Amazon AppFlo...
☐	AmazonAppFlowReadOnlyAccess	AWS managed	Provides read only access to Amazon A...
☐	AmazonAppStreamFullAccess	AWS managed	Provides full access to Amazon AppStr...
☐	AmazonAppStreamPCAAccess	AWS managed	Amazon AppStream 2.0 access to AWS...

► Set permissions boundary - optional

Cancel Previous **Next**

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

Step 1: Select trusted entity

Step 2: Add permissions

Step 3: Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

route-table-change

Maximum 64 characters. Use alphanumeric and "+,=,_,@,-" characters.

Description
Add a short explanation for this role.

Allows EC2 instances to make changes on the route table

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: "_+=, @-/\[\]#%*~!&:;','"

Step 1: Select trusted entities [Edit](#)

Trust policy

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "sts:AssumeRole"
8       ],
9       "Principal": {
10        "Service": [
11          "ec2.amazonaws.com"
12        ]
13      }
14    }
15  ]
16 }

```

Step 2: Add permissions [Edit](#)

Permissions policy summary

Policy name	Type	Attached as

Step 3: Add tags

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create role](#)

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:

Identity and Access Management (IAM)

[Policies](#)

Policies (1367) [Info](#)

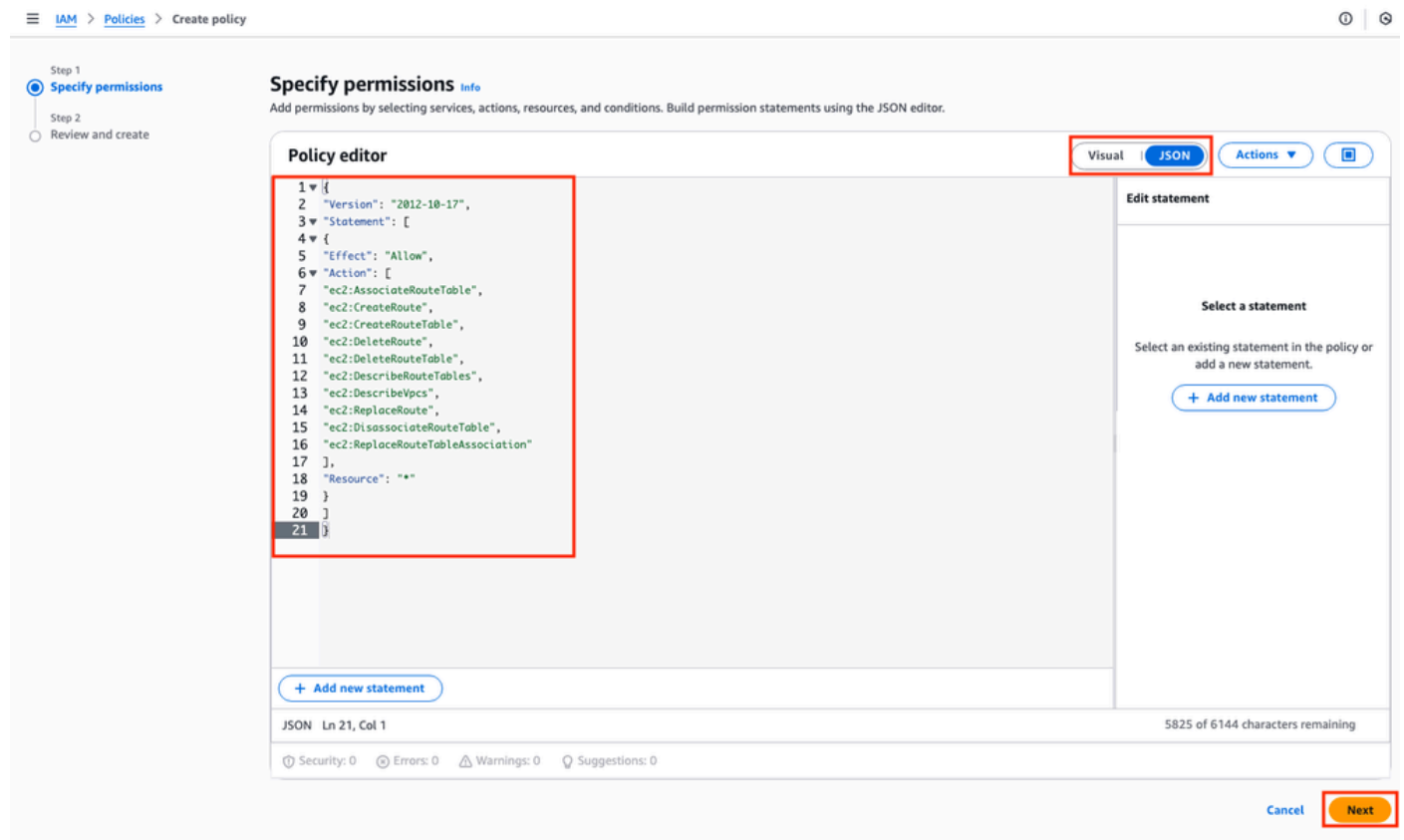
A policy is an object in AWS that defines permissions.

[Actions](#) [Delete](#) [Create policy](#)

Filter by Type: All types

Policy name	Type	Used as
AccessAnalyzerServiceRolePolicy	AWS managed	None
AdministratorAccess	AWS managed - job function	Permissions poli
AdministratorAccess-Amplify	AWS managed	None
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None
AIOpsAssistantPolicy	AWS managed	None
AIOpsConsoleAdminPolicy	AWS managed	None
AIOpsOperatorAccess	AWS managed	None
AIOpsReadOnlyAccess	AWS managed	None

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.

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

C8000v-HA

Maximum 128 characters. Use alphanumeric and '+', '@', '-', '_' characters.

Description - optional
Add a short explanation for this policy.

Allows EC2 instances to make route changes on AWS

Maximum 1,000 characters. Use alphanumeric and '+', '@', '-', '_' characters.

Permissions defined in this policy

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (1 of 441 services) Show remaining 440 services

Service	Access level	Resource	Request condition
EC2	Limited: List, Write	All resources	None

Add tags - optional

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous **Create policy**

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

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**

Policies (1/1368)

A policy is an object in AWS that defines permissions.

Filter by Type

Search C800 All types 1 match

Policy name	Type	Used as	Description
C8000v-HA	Customer managed	None	Allows EC2 instances to make route ch...

Actions Attach Detach Delete Create policy

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

IAM > Policies > C8000v-HA > Attach policy

Attach as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

IAM Entities (1/69)
Entities are IAM users, user groups and roles.

Search route All types 1 match

Entity name	Entity type
route-table-change	Roles

Cancel **Attach policy**

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:

EC2

[Dashboard](#)

[EC2 Global View](#)

[Events](#)

▼ **Instances**

- [Instances](#)
- [Instance Types](#)
- [Launch Templates](#)
- [Spot Requests](#)
- [Savings Plans](#)
- [Reserved Instances](#)
- [Dedicated Hosts](#)
- [Capacity Reservations](#)

▼ **Images**

- [AMIs](#)
- [AMI Catalog](#)

Resources

You are using the following Amazon EC2 resources in the United States (N. Virgin

Instances (running)	1	Auto Scaling Groups
Dedicated Hosts	0	Elastic IPs
Key pairs	17	Load balancers
Security groups	19	Snapshots

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) [Migrate a server](#)

Note: Your instances will launch in the United States (N. Virginia) Region

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.

Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Selected AMI: (ami-09e6f87a47903347c) (Quick Start AMIs)

Q Cisco Catalyst 8000v for SD-WAN & Routing

Quick Start AMIs (0) **My AMIs (691)** **AWS Marketplace AMIs (1)** **Community AMIs (500)**

Commonly used AMIs Created by me AWS & trusted third-party AMIs Published by anyone

▼ **Refine results**

Categories

[Infrastructure Software \(1\)](#)

▼ **Publisher**

☐ Cisco Systems, Inc. (1)

▼ **Pricing model**

☐ Bring Your Own License (1)

Operating system

☐ All Linux/Unix

▼ **Architecture**

Cisco Catalyst 8000v for SD-WAN & Routing (1 result) showing 1 - 1

Sort By: Relevance

Cisco Catalyst 8000v for SD-WAN & Routing

By Cisco Systems, Inc. | Ver 17.15.03a

As part of Cisco's Cloud connect portfolio, the Bring Your Own License (BYOL) version of Cisco® Catalyst® 8000V Edge Software (Catalyst 8000V) delivers the maximum performance for virtual enterprise-class networking services & VPN in the AWS cloud. This AMI supports all the Catalyst 8000V (C8000V)...

Select

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).

The screenshot shows the AWS Marketplace page for the Cisco Catalyst 8000V for SD-WAN & Routing. The page is titled "Cisco Catalyst 8000V for SD-WAN & Routing" and is published by Cisco Systems, Inc. The "Pricing" tab is selected, showing the product is available for customers with current licenses purchased via other channels. The pricing table shows the product is available for \$0/Hour and \$0.108/Hour. The "Subscribe now" button is highlighted with a red box.

Product	Price
Cisco Catalyst 8000V for SD-WAN & Routing	\$0/Hour
EC2 - c5n.large vendor recommended	\$0.108/Hour

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.

The screenshot shows the AWS console's "Key pair (login)" section. It includes a dropdown menu for "Key pair name - required" with the value "fsimmond-pem". The "Create new key pair" button is highlighted with a red box.

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**.

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

fsimmond-ed-pem

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☐ RSA
RSA encrypted private and public key pair

☒ ED25519
ED25519 encrypted private and public key pair

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

 When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#) 

Cancel

Create key pair

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.

The screenshot shows the 'Network settings' section of an AWS console page. It includes several sub-sections: 'VPC - required', 'Subnet', 'Auto-assign public IP', 'Firewall (security groups)', and 'Common security groups'. Red boxes and numbers highlight specific elements: 1 points to the VPC dropdown menu; 2 points to the 'Select existing security group' button; 3 points to the 'Compare security group rules' link; and 4 points to the 'Create new subnet' button. The 'Subnet' section shows details for 'subnet-0b664f8e74443d28f' in the 'public-R1-C8000v' availability zone. The 'Common security groups' section shows a selected group 'All traffic HA sg-029461ba80052f10c'.

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-0d30b9fa9511f3639 (HA)
10.100.0.0/16

Subnet [Info](#)

subnet-0b664f8e74443d28f public-R1-C8000v
VPC: vpc-0d30b9fa9511f3639 Owner: 073713984176 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.100.10.0/24

Auto-assign public IP [Info](#)

Disable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group ☒ Select existing security group

Common security groups [Info](#)

Select security groups

All traffic HA sg-029461ba80052f10c X
VPC: vpc-0d30b9fa9511f3639

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

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.

VPC > Subnets > Create subnet

Create subnet Info

VPC
VPC ID
vpc-d30b9fa9511f3639 (HA) 1

Associated VPC CIDRs
IPv4 CIDRs
10.100.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
public-R1-C8000v 2

Availability Zone Info
United States (N. Virginia) / us-east-1a 3

IPv4 VPC CIDR block Info
10.100.0.0/16

IPv4 subnet CIDR block 4
10.100.10.0/24 256 IPs

▼ Tags - optional

Key
Q Name X

Value - optional
Q public-R1-C8000v X Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet 5

6
Cancel Create subnet

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:

▼ Advanced network configuration

Network interface 1

Device index [Info](#)

0

Subnet [Info](#)

subnet-0b664f8e74443d28f

IP addresses available: 249

Primary IP [Info](#)

10.100.10.254

IPv4 Prefixes [Info](#)

Select

Delete on termination [Info](#)

No

ENA Express [Info](#)

Select

The selected instance type does not support ENA Express.

Idle connection tracking timeout [Info](#)

☐ Enable

Add network interface

Network interface [Info](#)

New interface

Security groups [Info](#)

Select security groups

Secondary IP [Info](#)

Select

IPv6 Prefixes [Info](#)

Select

The selected subnet does not support IPv6 prefixes because it does not have an IPv6 CIDR.

Interface type [Info](#)

Select

ENA Express UDP [Info](#)

Select

The selected instance type does not support ENA Express.

Description [Info](#)

Public-R1

Auto-assign public IP [Info](#)

Disable

IPv6 IPs [Info](#)

Select

The selected subnet does not support IPv6 IPs.

Assign Primary IPv6 IP [Info](#)

Select

A primary IPv6 address is only compatible with subnets that support IPv6.

Network card index [Info](#)

Select

The selected instance type does not support multiple network cards.

ENA queues [Info](#)

The selected instance type does not support ENA queues.

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:

Network interface 2

Device index [Info](#)

1

Subnet [Info](#)

subnet-0a5f13361443951d2

IP addresses available: 250

Primary IP [Info](#)

10.100.110.254

Network interface [Info](#)

New interface

Security groups [Info](#)

Select security groups

Secondary IP [Info](#)

Select

Description [Info](#)

Private-R1

Auto-assign public IP [Info](#)

Select

IPv6 IPs [Info](#)

Select

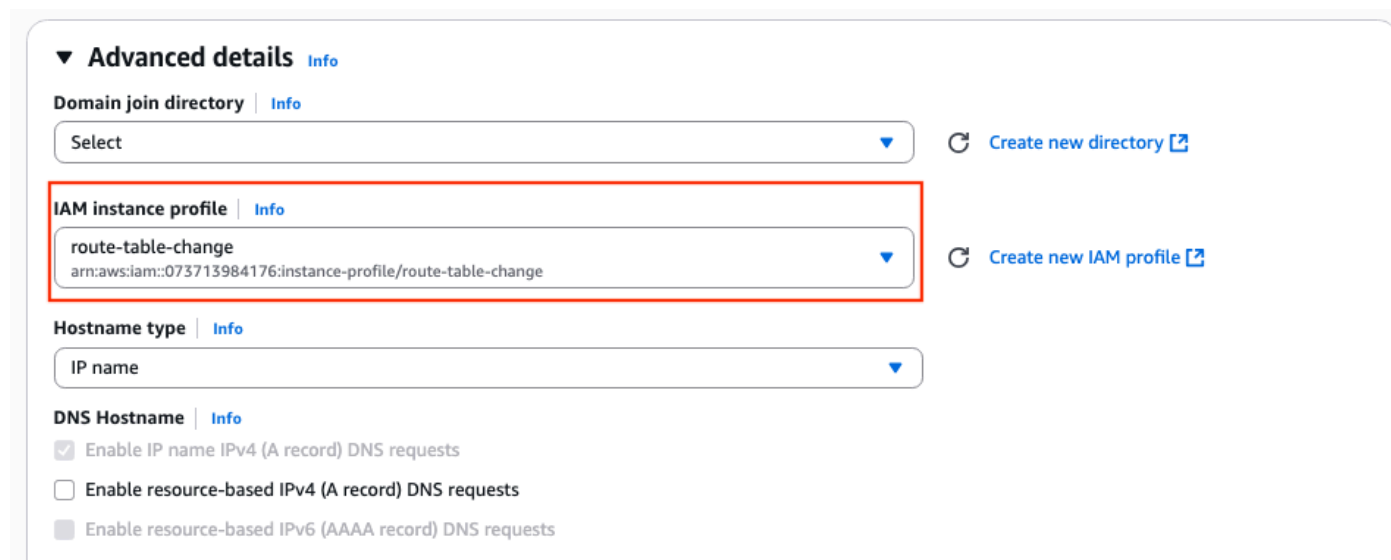
The selected subnet does not support IPv6 IPs.

Remove

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:



▼ Advanced details [Info](#)

Domain join directory | [Info](#)

Select [Create new directory](#)

IAM instance profile | [Info](#)

route-table-change
arn:aws:iam::073713984176:instance-profile/route-table-change [Create new IAM profile](#)

Hostname type | [Info](#)

IP name

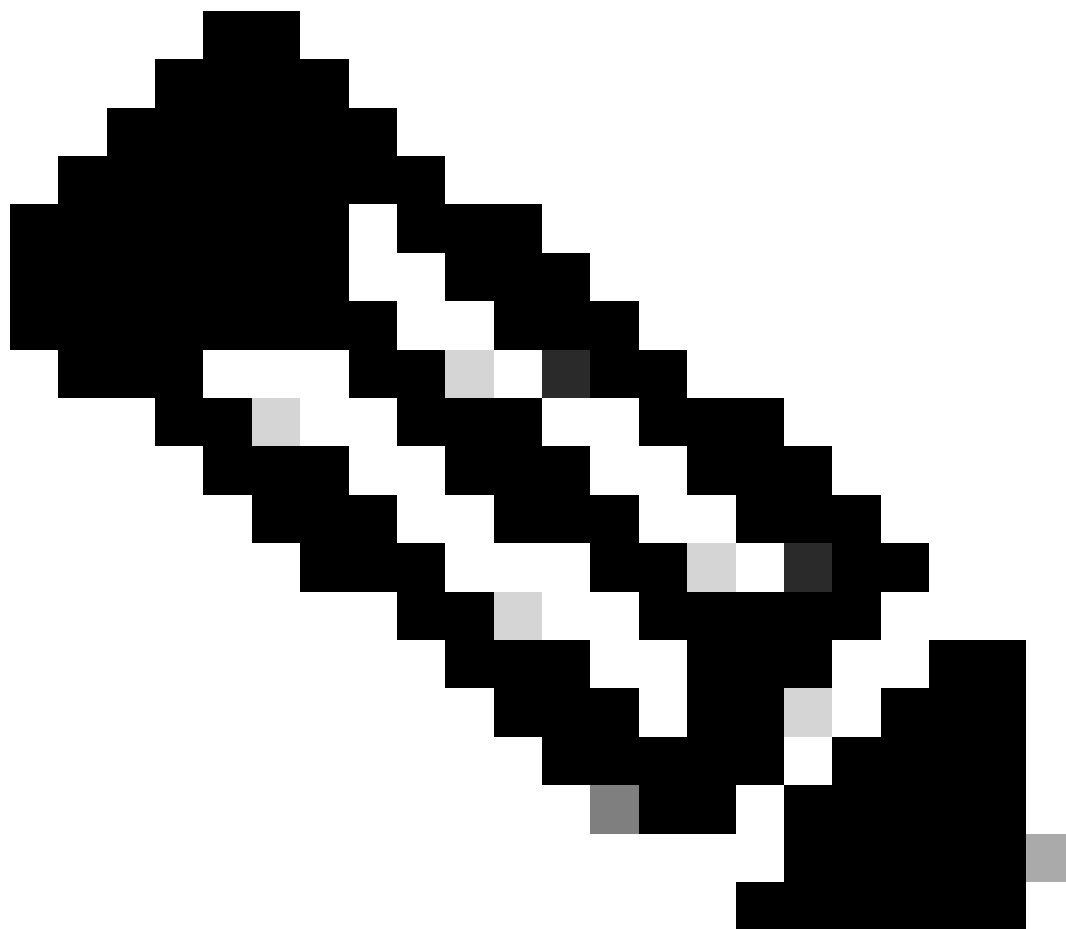
DNS Hostname | [Info](#)

- ☒ Enable IP name IPv4 (A record) DNS requests
- ☐ Enable resource-based IPv4 (A record) DNS requests
- ☐ Enable resource-based IPv6 (AAAA record) DNS requests

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](#)

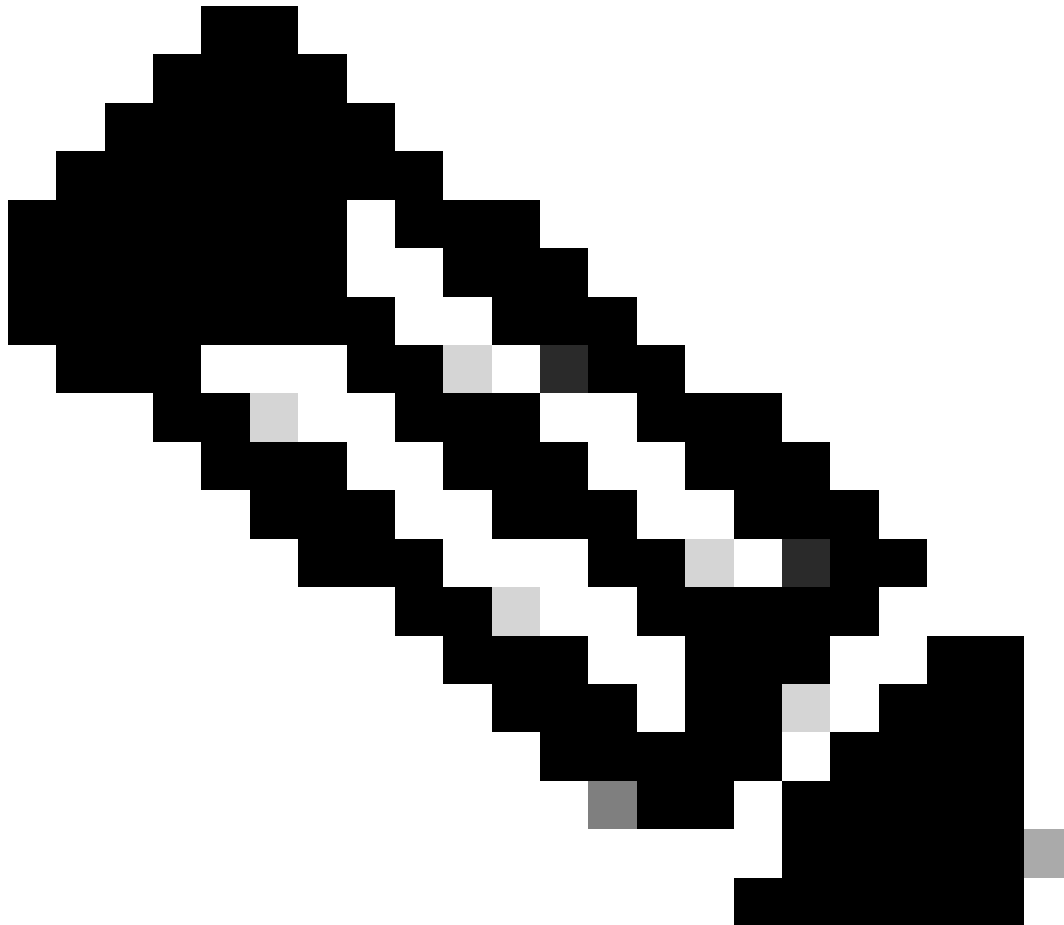
[Launch instance](#)



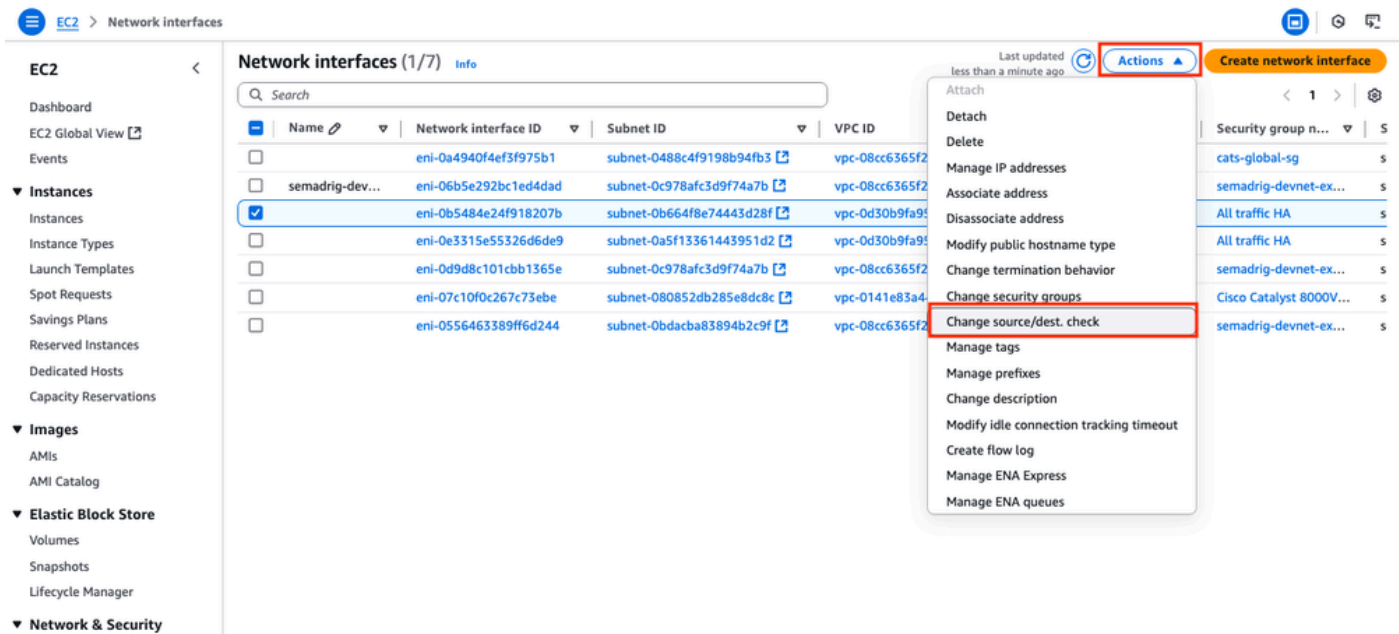
[Preview code](#)

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

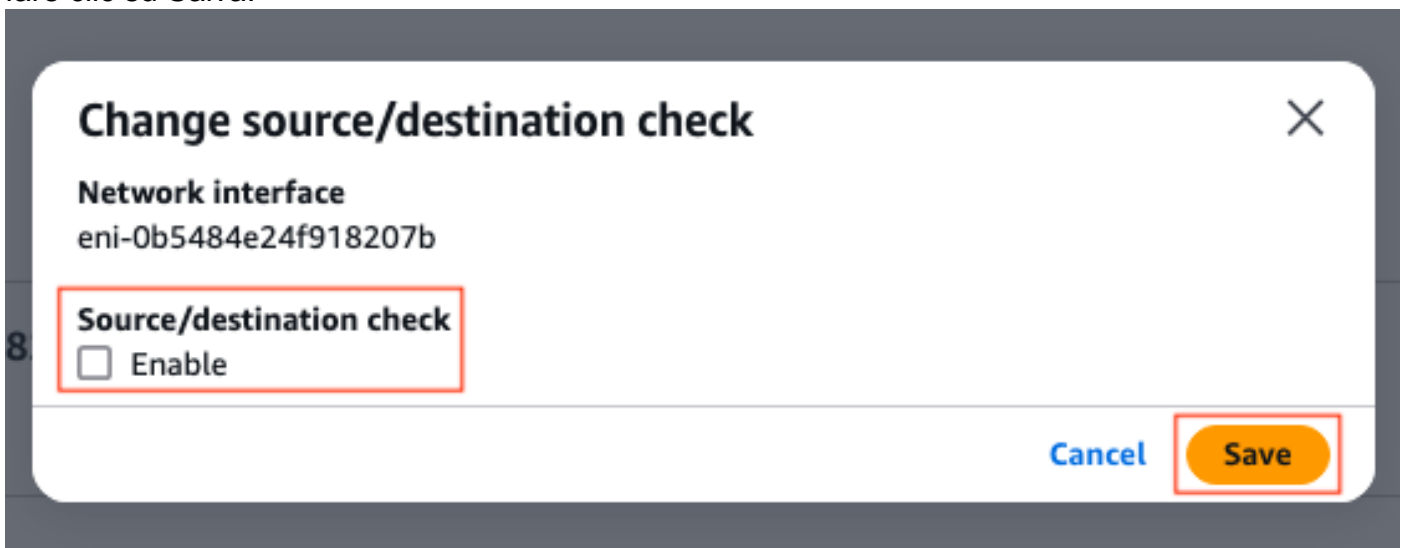
Una volta creata l'istanza, disabilitare la funzionalità di controllo src/dst in AWS per ottenere la connettività tra le interfacce nella stessa subnet. Nella sezione EC2 Dashboard > Rete e sicurezza > Interfacce di rete, selezionare gli ENI e fare clic su Azioni > Cambia origine/destinazione. controllare.



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

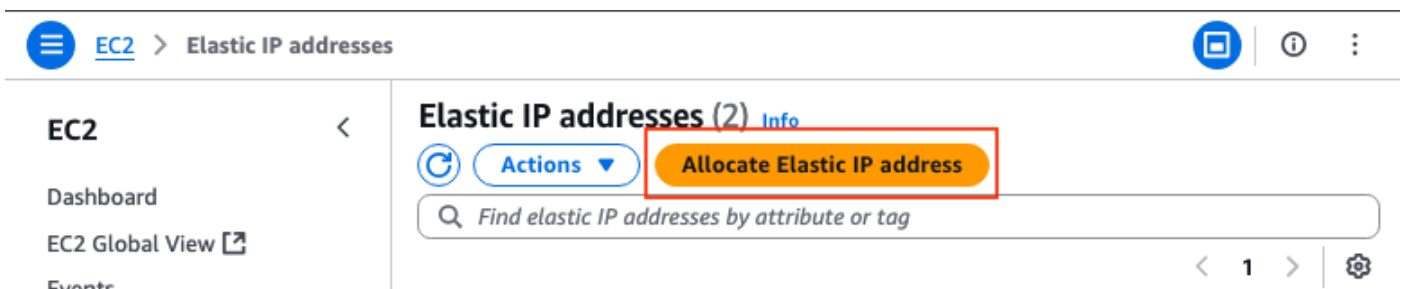


Viene visualizzata una nuova finestra. Nel menu Nuovo, disattivare la casella di controllo Abilita e fare clic su Salva.



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.

EC2 > Elastic IP addresses > Allocate Elastic IP address

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Public IPv4 address pool

- ☒ Amazon's pool of IPv4 addresses
 - ☐ Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) [Learn more](#)
 - ☐ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) [Learn more](#)
 - ☐ Allocate using an IPv4 IPAM pool (option disabled because no public IPv4 IPAM pools with AWS service as EC2 were found)

Network border group [Info](#)

us-east-1

Global static IP addresses
AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

[Create accelerator](#)

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
No tags associated with the resource.

[Add new tag](#)
You can add up to 50 more tag

[Cancel](#) [Allocate](#)

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.

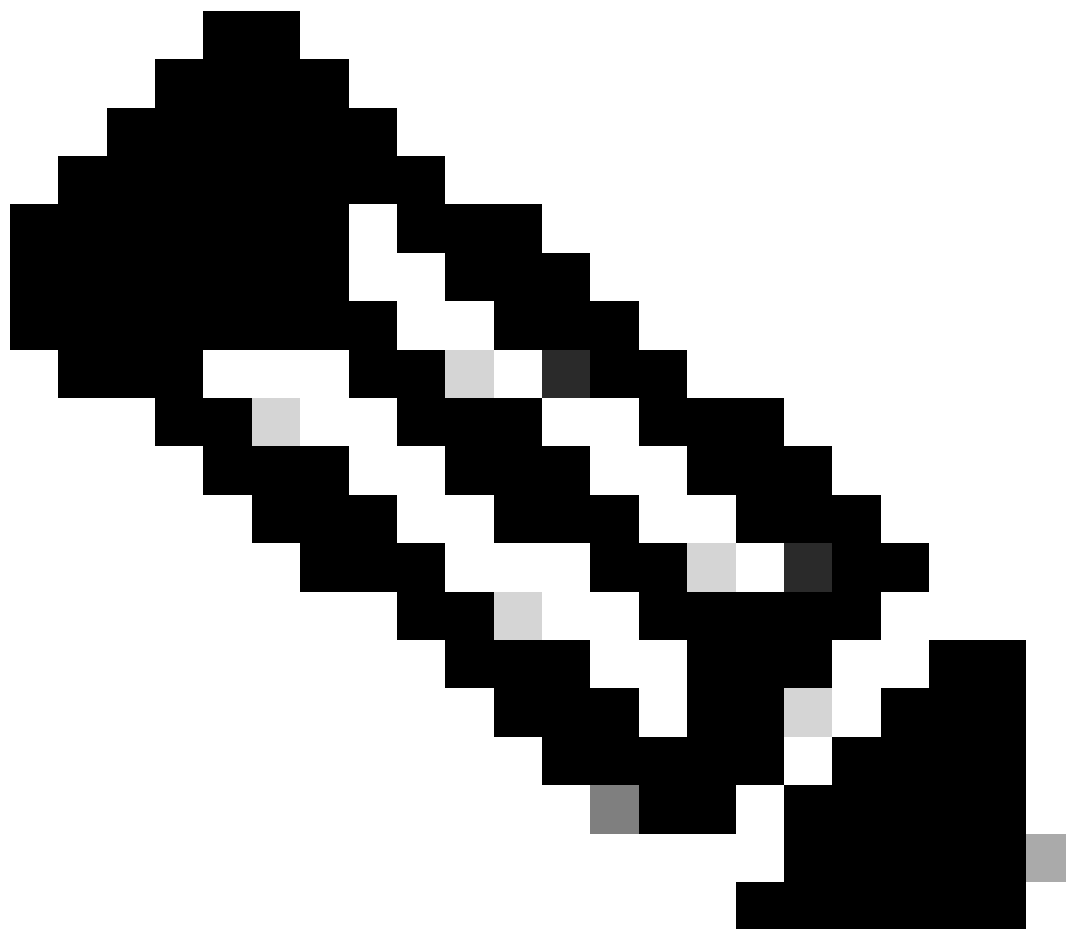
Elastic IP addresses (1/1) [Info](#)

Find elastic IP addresses by attribute or tag

Public IPv4 address [Clear filters](#)

☒	Name	Allocated IPv4 address	Type	Allocation ID	Reverse DNS record	
☒	-	10.0.0.1	Public IP	eipalloc-0948346735ab2017c	-	View details Release Elastic IP addresses Associate Elastic IP address Disassociate Elastic IP address Update reverse DNS Enable transfers Disable transfers Accept transfers

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.

Associate Elastic IP address [Info](#)

Choose the instance or network interface to associate to this Elastic IP address ([see IP address](#))

Elastic IP address: [see IP address](#)

Resource type
Choose the type of resource with which to associate the Elastic IP address.
☐ Instance
☒ Network interface

⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Network interface

Private IP address
The private IP address with which to associate the Elastic IP address.

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
☒ Allow this Elastic IP address to be reassociated

[Cancel](#) [Associate](#)

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
```

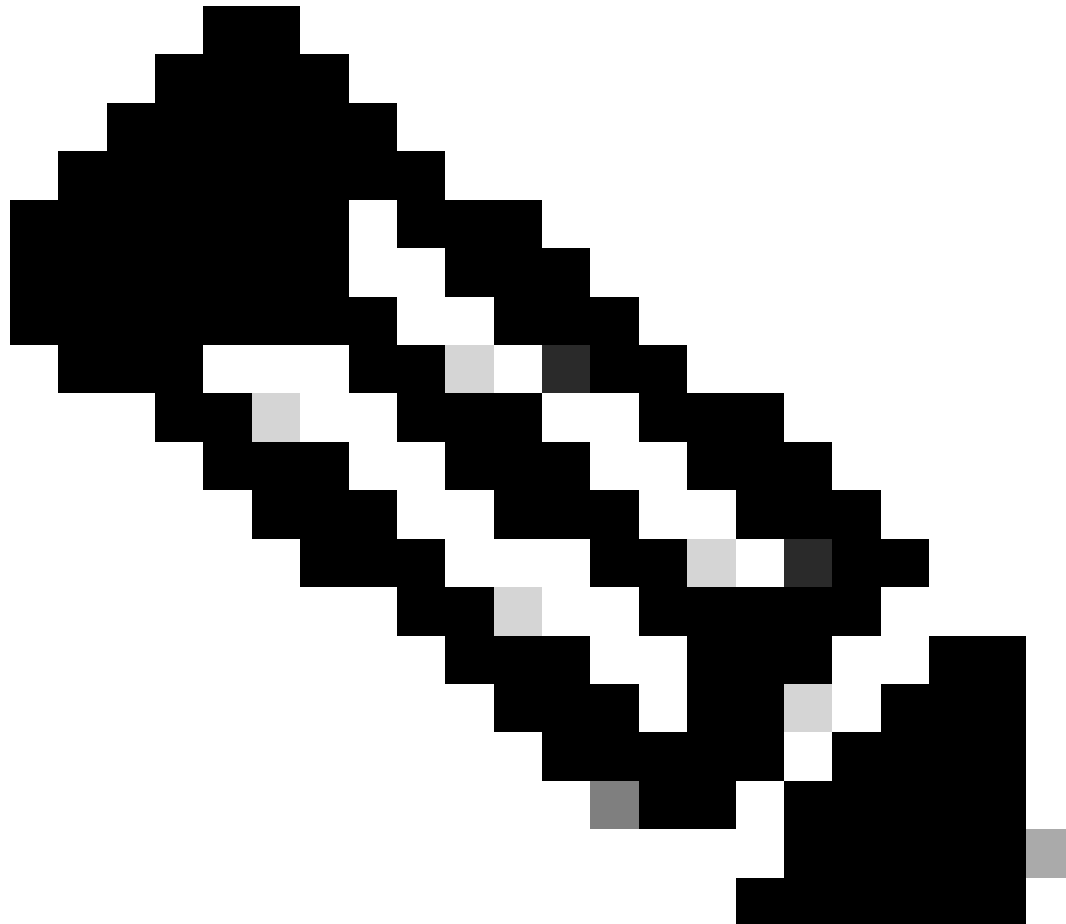
```
10.100.30.254
```

```
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

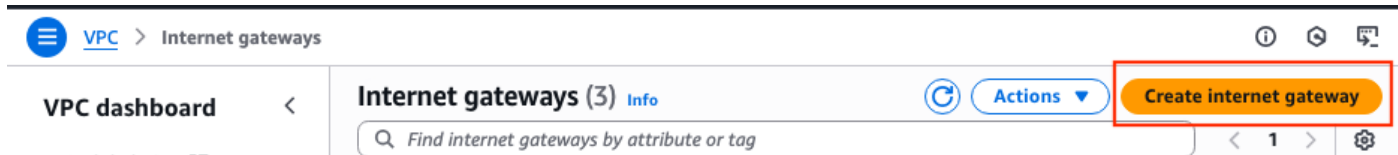
```
netmask 255.255.255.0 broadcast 10.100.130.255
inet6 fe80::3b:7eff:fead:dbe5 prefixlen 64 scopeid 0x20<link>
ether 02:3b:7e:ad:db:e5 txqueuelen 1000 (Ethernet)
RX packets 119 bytes 16831 (16.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 133 bytes 13816 (13.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



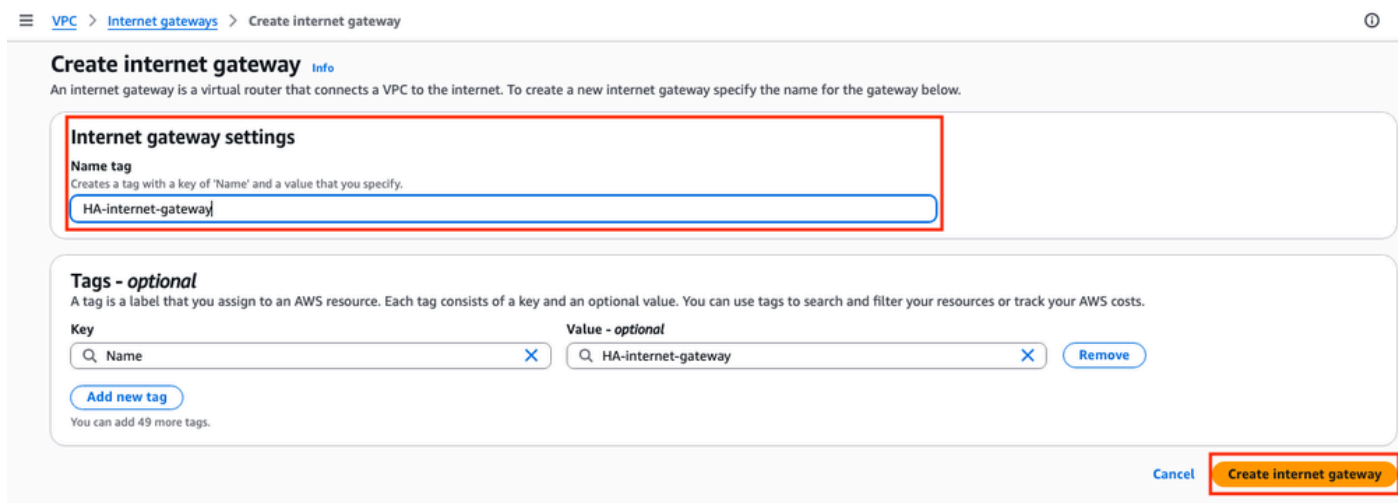
Nota: Se vengono apportate modifiche alle interfacce, eseguire il flap dell'interfaccia o ricaricare la VM per applicare le modifiche.

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**.



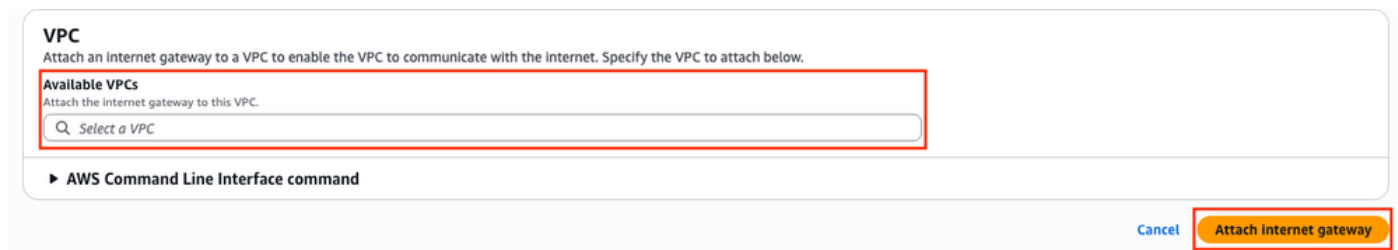
In questa nuova sezione creare un **tag name** per il gateway e fare clic su **Crea gateway Internet**.



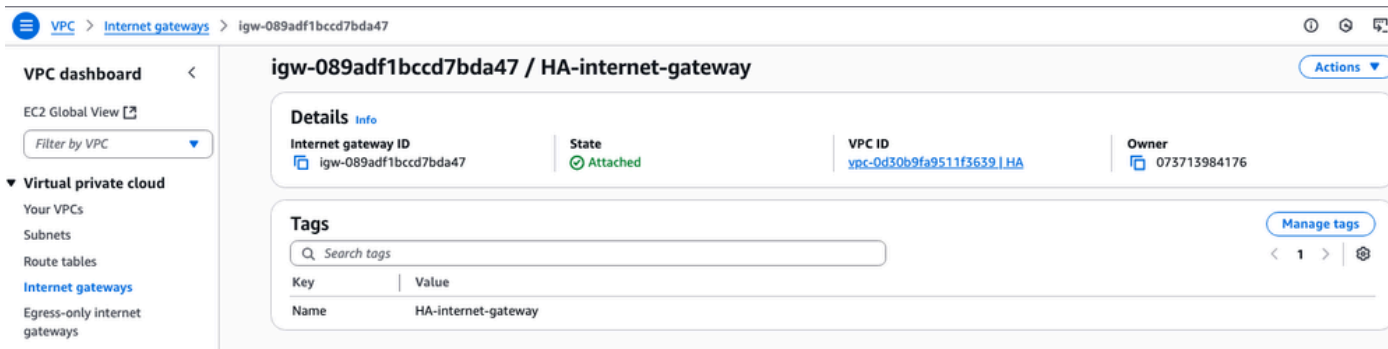
Una volta creato l'IGW, collegarlo al VPC corrispondente. Passare alla sezione **VPC Dashboard > Virtual Private Cloud > Internet Gateway** e selezionare l'IGW corrispondente. Fare clic su **Azioni > Associa a VPC**.



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



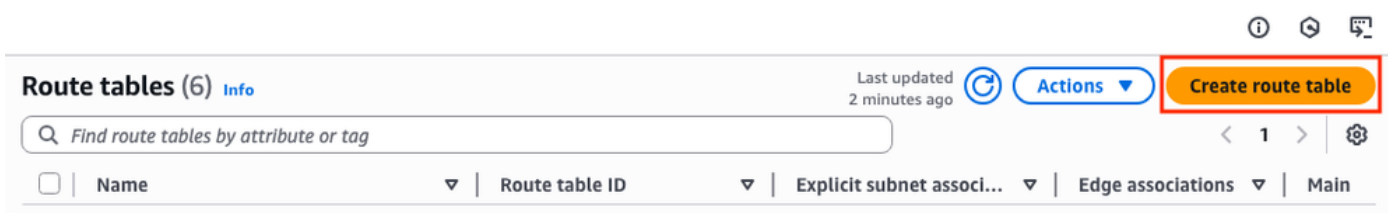
L'IGW deve indicare lo stato Attaccato come mostrato:



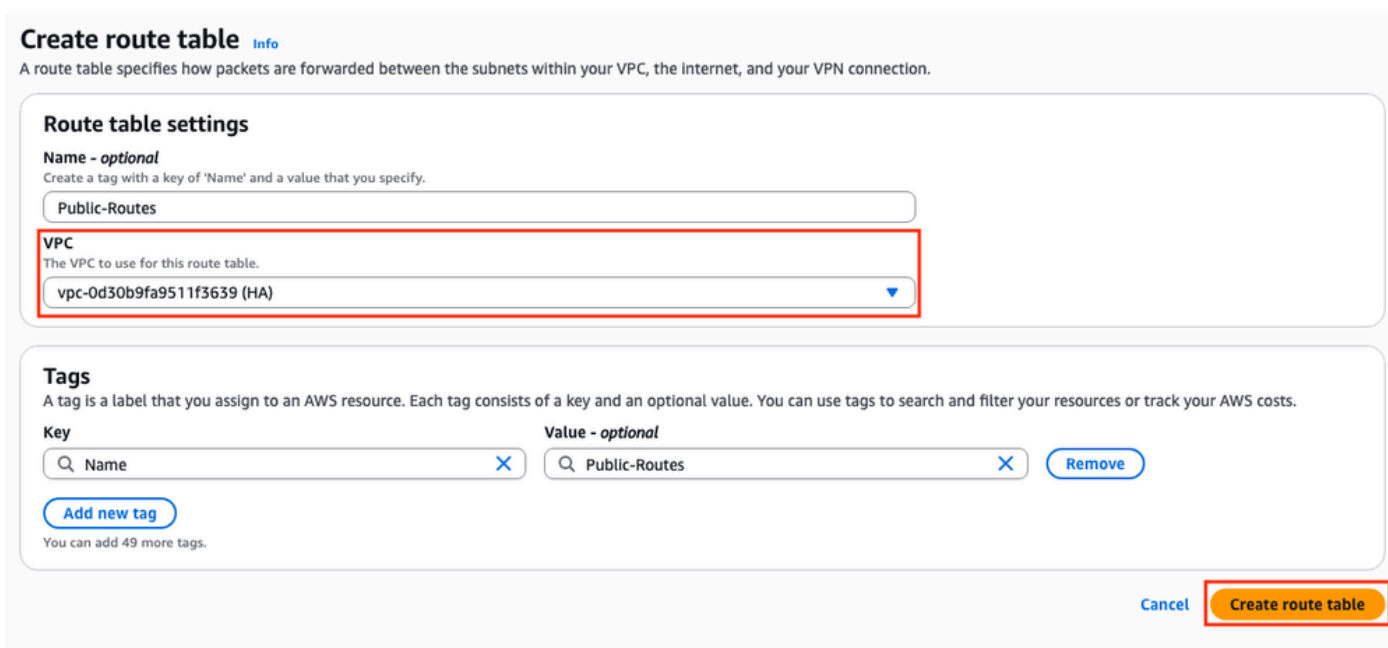
Passaggio 10. Creare e configurare le tabelle di routing in AWS per le subnet pubbliche e private

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.

VPC > Route tables

Route tables (1/1) Info Last updated 8 minutes ago Actions Create route table

Find route tables by attribute or tag

public-routes X Clear filters

☒	Name	Route table ID	Explicit subnet associ...	Main
☒	Public-Routes	rtb-0d0e48f25c9b00635	3 subnets	No

- View details
- Set main route table
- Edit subnet associations**
- Edit edge associations
- Edit route propagation
- Edit routes
- Manage tags
- Delete route table

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

Edit subnet associations
Change which subnets are associated with this route table.

Available subnets (3/6)
Filter subnet associations

public X Clear filters

☒	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☒	public-R1-C8000v	subnet-0b664f8e74443d28f	10.100.10.0/24	-	rtb-0d0e48f25c9b00635 / Public-Routes
☒	Public-VM-linux-1c - fsmmond	subnet-04fb9de939e3778bb	10.100.30.0/24	-	rtb-0d0e48f25c9b00635 / Public-Routes
☒	public-R2-C8000v	subnet-02d8108842f9f3129	10.100.20.0/24	-	rtb-0d0e48f25c9b00635 / Public-Routes

Selected subnets

subnet-0b664f8e74443d28f / public-R1-C8000v X subnet-04fb9de939e3778bb / Public-VM-linux-1c - fsmmond X subnet-02d8108842f9f3129 / public-R2-C8000v X

Cancel Save associations

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:

Route tables (1/1) Info

Find route tables by attribute or tag

public-routes X Clear filters

☒	Name	Route table ID
☒	Public-Routes	rtb-0d0e48f25c9b00635

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:

Edit routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	Active	No

Buttons: Add route, Cancel, Preview, Save changes

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:

Edit routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	Active	No
8.8.8.8/32	Network interface	-	No

Buttons: Add route, Cancel, Preview, Save changes

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 C800v 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 C800v 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.

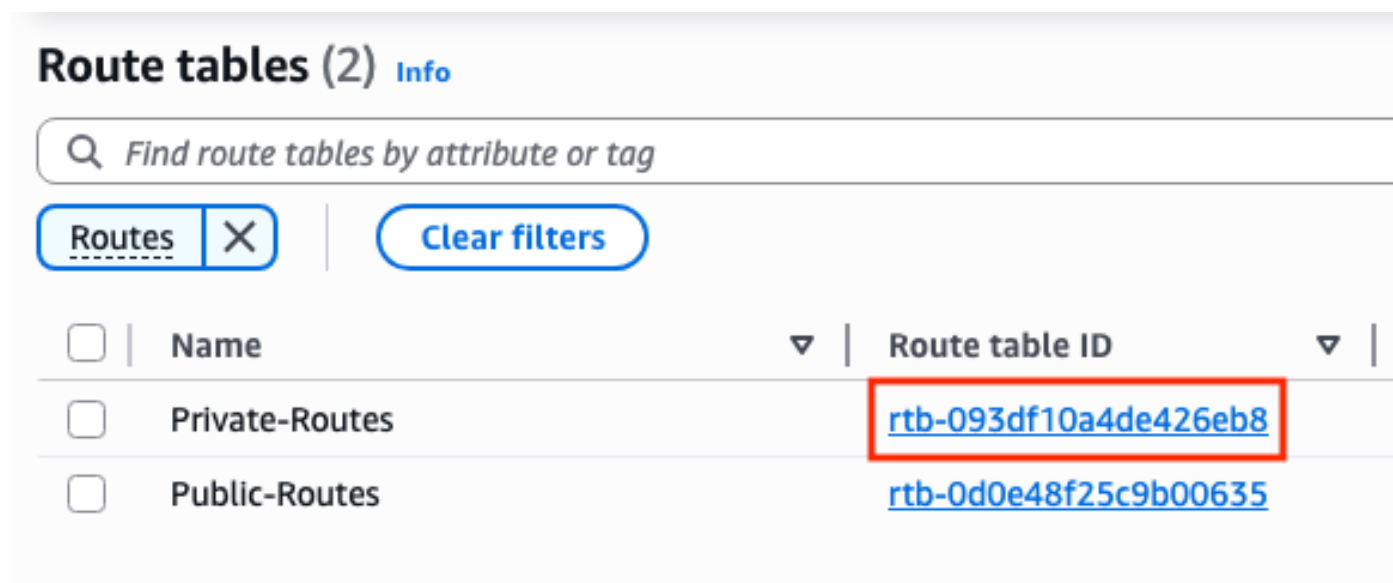
```
Router(config)# redundancy
Router(config-red)# cloud provider aws (node-id)
bfd peer <IP address of the remote device>
route-table <Route table ID>
cidr ip <traffic to be monitored/prefix>
eni <Elastic network interface (ENI) ID>
region <region-name>
```

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.



Route tables (2) [Info](#)

Find route tables by attribute or tag

Routes X Clear filters

☐	Name	Route table ID
☐	Private-Routes	rtb-093df10a4de426eb8
☐	Public-Routes	rtb-0d0e48f25c9b00635

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

rtb-093df10a4de426eb8 / Private-Routes

Details [Info](#)

Route table ID

 rtb-093df10a4de426eb8

VPC

 vpc-0d30b9fa9511f3639 | HA

Main

 Yes

Owner ID

 073713984176

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

 [Filter routes](#)

Destination



Target

8.8.8.8/32

[eni-0239fda341b4d7e41](#) 

10.100.0.0/16

local

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:

Instances (1/3) [Info](#)

Last updated 1 minute ago 

[Connect](#)

[Instance state](#)

[Actions](#)

[Launch instances](#)

 Find Instance by attribute or tag (case-sensitive)

[All states](#)

[fsimmond](#) 

[Clear filters](#)

 Name

 Instance ID

 Instance state

 Instance type

 Status check

 Alarm status

 Availability Zone

☐	C8000v-R2-fsimmond	i-0a1a91794f919f641	 Stopped 	c5n.large	-	View alarms 	us-east-1b
☐	Ubuntu VM - fsimmond	i-03a306e81a0b99864	 Stopped 	m5.large	-	View alarms 	us-east-1c
☒	C8000v-R1-fsimmond	i-0b9a50a09b089b03a	 Running 	c5n.large	 3/3 checks passed	View alarms 	us-east-1a

i-0b9a50a09b089b03a (C8000v-R1-fsimmond)





Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

VPC ID

 vpc-0d30b9fa9511f3639 (HA) 

Subnet ID

 subnet-0b664f8e74443d28f (public-R1-C8000v) 

Availability zone

 us-east-1a

Outpost ID

-

▶ IP addresses [Info](#)

▶ Hostname and DNS [Info](#)

▼ Network Interfaces (2) [Info](#)

 [Filter network interfaces](#)

Interface ID	Device index	Card index	Description	Public IPv4 address	Private IPv4 address	Private IPv4 DNS	IPv6
 eni-0645a881c13823696	0	0	-	 10.100.110.254	10.100.10.254	-	-
 eni-070e14fbfde0d8e3b	1	0	-	-	10.100.110.254	-	-

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 Zones](#) document.

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 HoId Uptime SRTT RT0 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:

rtb-093df10a4de426eb8 / Private-Routes

Details | **Routes** | Subnet associations | Edge associations | Route propagation | Tags

Routes (2)

Filter routes

Destination	Target
8.8.8.8/32	eni-070e14fbfde0d8e3b
10.100.0.0/16	local

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:

Routes (2)

Destination

▼ | Target

8.8.8.8/32

[eni-0239fda341b4d7e41](#)

10.100.0.0/16

local

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).