

AWSでのC8000vハイアベイラビリティコンフィギュレーションのデプロイ

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[トポロジ](#)

[ネットワーク図](#)

[表の要約](#)

[制約事項](#)

[コンフィギュレーション](#)

[ステップ 1 : 地域を選択](#)

[ステップ 2 : VPCの作成](#)

[ステップ 3 : VPCのセキュリティグループの作成](#)

[ステップ 4 : ポリシーを使用してIAMロールを作成し、VPCに関連付ける](#)

[ステップ 5 : IAMロールに対する信頼ポリシーの作成と適用](#)

[手順6:C8000vインスタンスの設定と起動](#)

[ステップ 6.1 : リモートアクセス用のキーペアの設定](#)

[ステップ 6.2 : AMIのサブネットの作成および設定](#)

[ステップ 6.3 : AMIインターフェイスの設定](#)

[ステップ 6.4 : IAMインスタンスプロファイルをAMIに設定する](#)

[ステップ 6.5 : \(オプション \) AMIでのクレデンシャルの設定](#)

[ステップ 6.6 : インスタンス設定の完了](#)

[ステップ 6.7 : ENIでの送信元/宛先チェックの無効化](#)

[ステップ 6.8 : インスタンスのパブリックENIへのElastic IPの作成と関連付け](#)

[手順 7 : 手順6を繰り返して、HA用に2つ目のC8000vインスタンスを作成します](#)

[ステップ 8 : 手順6を繰り返して、AMI MarketplaceからVM\(Linux/Windows\)を作成します](#)

[ステップ 9 : VPC用のインターネットゲートウェイ\(IGW\)の作成と設定](#)

[ステップ 10 : パブリックおよびプライベートサブネット用のルートテーブルをAWSで作成および設定する](#)

[ステップ 10.1 : パブリックルートテーブルの作成と設定](#)

[ステップ 10.2 : プライベートルートテーブルの作成と設定](#)

[ステップ 11基本的なネットワーク設定、ネットワークアドレス変換\(NAT\)、BFDを使用したGREトンネル、およびルーティングプロトコルの確認と設定](#)

[ステップ 12ハイアベイラビリティの設定\(Cisco IOS® XE Denali 16.3.1a以降\)](#)

[検証](#)

[トラブルシュート](#)

はじめに

このドキュメントでは、Amazon Web Servicesクラウド上のCatalyst 8000vルータでハイアベイラビリティ環境をセットアップする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AWSコンソールとそのコンポーネントに関する一般的な知識
- Cisco IOS® XEソフトウェアについて
- HA機能に関する基礎知識

使用するコンポーネント

この設定例では、次のコンポーネントが必要です。

- 管理者ロールを持つAmazon AWSアカウント
- Cisco IOS® XE 17.15.3aを実行するC8000vデバイス2台とUbuntu 22.04 LTS VM 1台 同じリージョン内のAMI

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トポロジ

HA導入には、ネットワーク要件に基づくさまざまなシナリオがあります。この例では、HA冗長性は次の設定で設定されます。

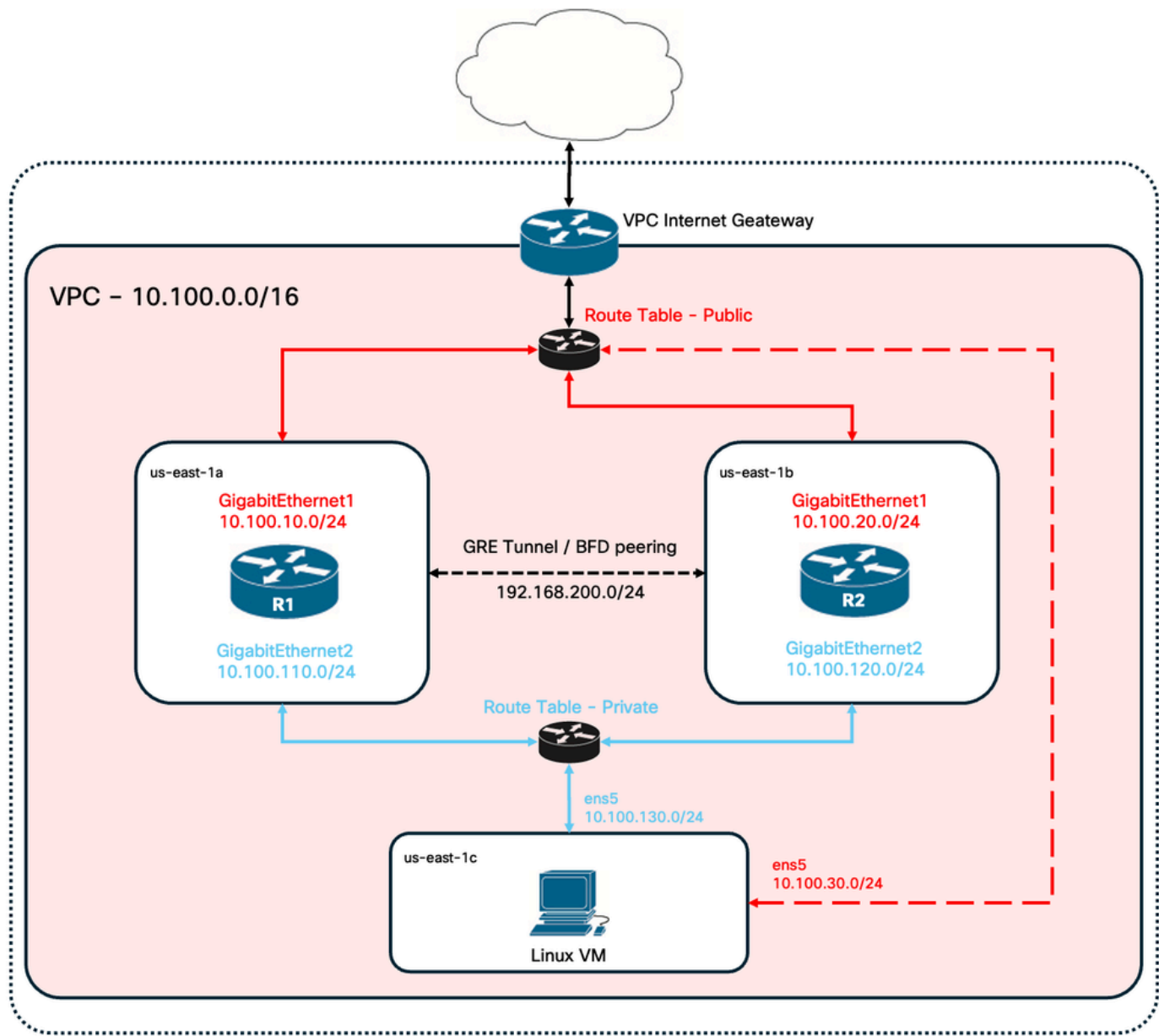
- 1x – 地域
- 1x - VPC
- 3x：アベイラビリティゾーン
- 6x – ネットワークインターフェイス/サブネット（3xパブリック側/3xプライベート側）
- 2x – ルートテーブル（パブリックおよびプライベート）
- 2x - C8000vルータ(Cisco IOS® XEDenali 17.15.3a)
- 1x - VM(Linux/Windows)

HAペアの2台のC8000vルータは、2つの異なるアベイラビリティゾーンにあります。各アベイラビリティゾーンを、ハードウェアの復元力を高める個別のデータセンターと考えてください。

3番目のゾーンはVMで、プライベートデータセンターのデバイスをシミュレートします。ここでは、パブリックインターフェイスからインターネットアクセスを有効にして、VMにアクセスして設定できるようにします。一般に、通常のトラフィックはすべて、プライベートルートテーブルを通過する必要があります。

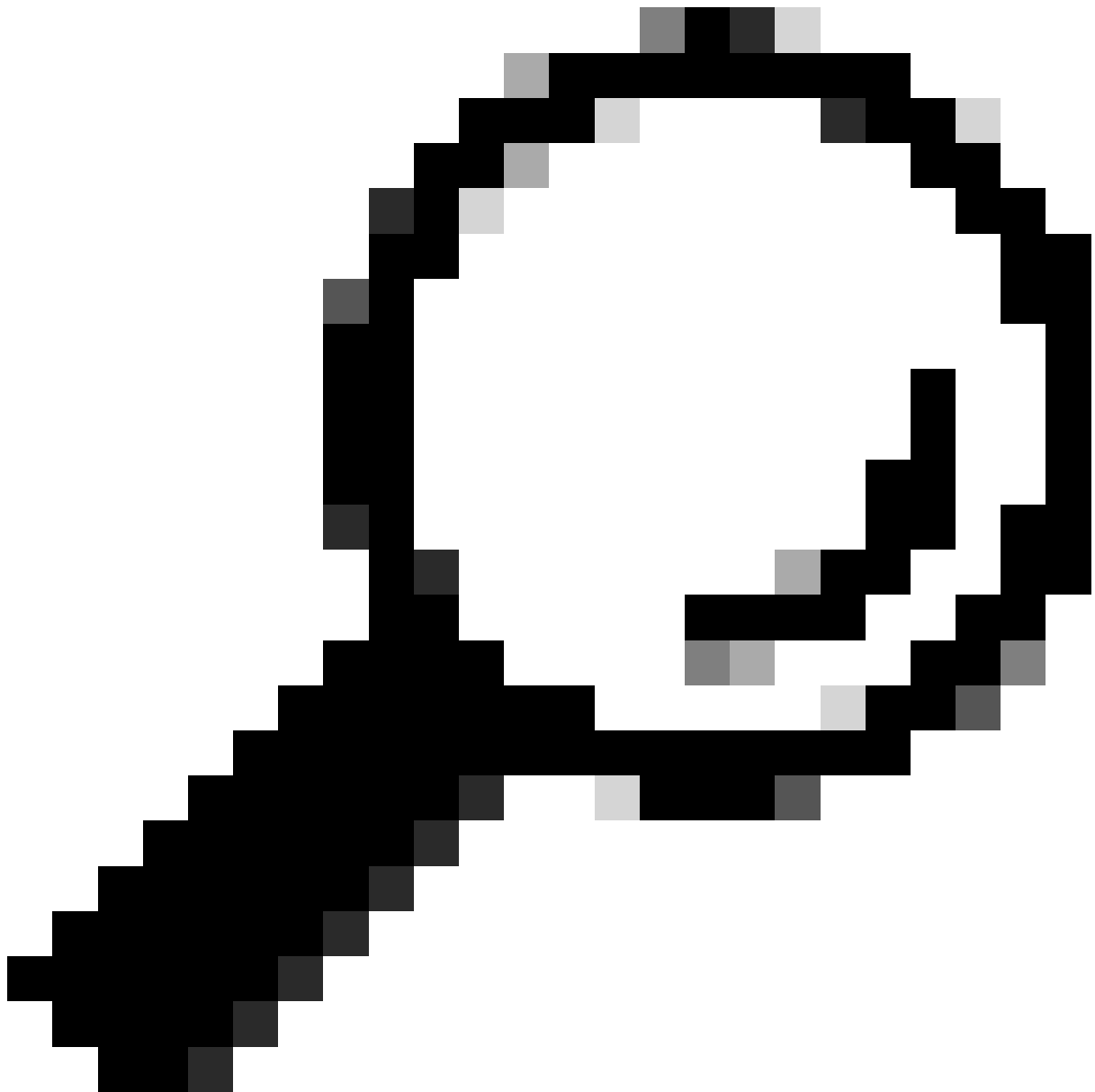
トラフィックをシミュレートするには、仮想マシンのプライベートインターフェイスからpingを開始し、R1経由でプライベートルートテーブルを通過して8.8.8.8に到達します。フェールオーバーが発生した場合は、R2ルータのプライベートインターフェイスを介してトラフィックをルーティングするように、プライベートルートテーブルが自動的に更新されていることを確認します。

ネットワーク図



表の要約

トポロジを要約するために、この表にはラボの各コンポーネントの最も重要な値を示します。この表に記載された情報は、このラボ演習の情報とは排他的です。



ヒント:この表を使用すると、ガイド全体を通じて主要な変数の概要を明確に把握するのに役立ちます。プロセスを合理化するために、この形式で情報を収集することをお勧めします。

デバイス	アベイラビリティゾーン	インターフェイス	[IP アドレス (IP Addresses)]	RTB	エニ
R1	us-east-1a	GigabitEthernet1	10.100.10.254	rtb-0d0e48f25c9b00635 (パブリック)	eni-0645a881c13823696
		GigabitEthernet2	10.100.110.254	rtb-093df10a4de426eb8 (プライベート)	eni-070e14fbfde0d8e3b

R2	us-east-1b	GigabitEthernet1	10.100.20.254	rtb-0d0e48f25c9b00635 (パブリック)	eni-0a7817922ffbb317b
		GigabitEthernet2	10.100.120.254	rtb-093df10a4de426eb8 (プライベート)	eni-0239fda341b4d7e41
Linux仮想マシン	米国東部-1c	ens5	10.100.30.254	rtb-0d0e48f25c9b00635 (パブリック)	eni-0b28560781b3435b1
		ens6	10.100.130.254	rtb-093df10a4de426eb8 (プライベート)	eni-05d025e88b6355808

制約事項

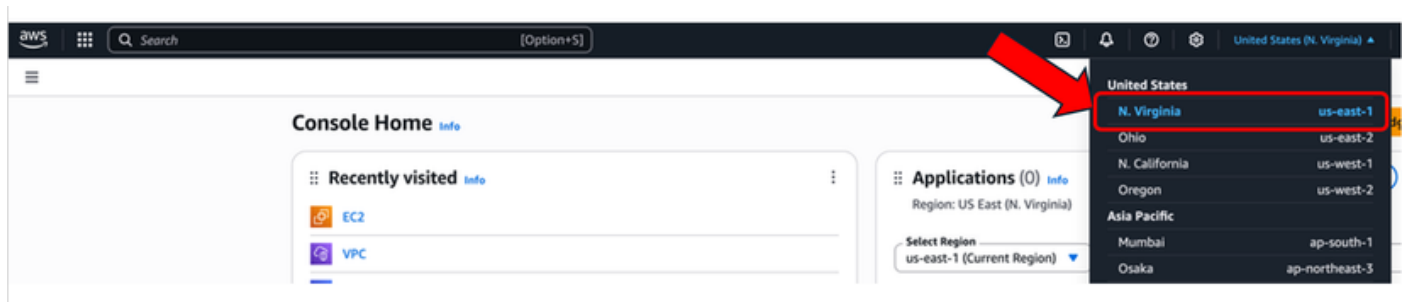
- 作成されたサブネットでは、そのサブネットの最初に使用可能なアドレスを使用しないでください。これらのIPアドレスは、AWSサービスによって内部的に使用されます。
- VRF内でC8000vデバイスのパブリックインターフェイスを設定しないでください。これが設定されていると、HAが正しく動作しません。

コンフィギュレーション

設定の一般的なフローは、要求されたVMを適切な領域に作成し、各VMのルートやインターフェイスなど、最も具体的な設定に移行することに重点を置いています。ただし、最初にトポロジを理解し、必要な順序でトポロジを設定することをお勧めします。

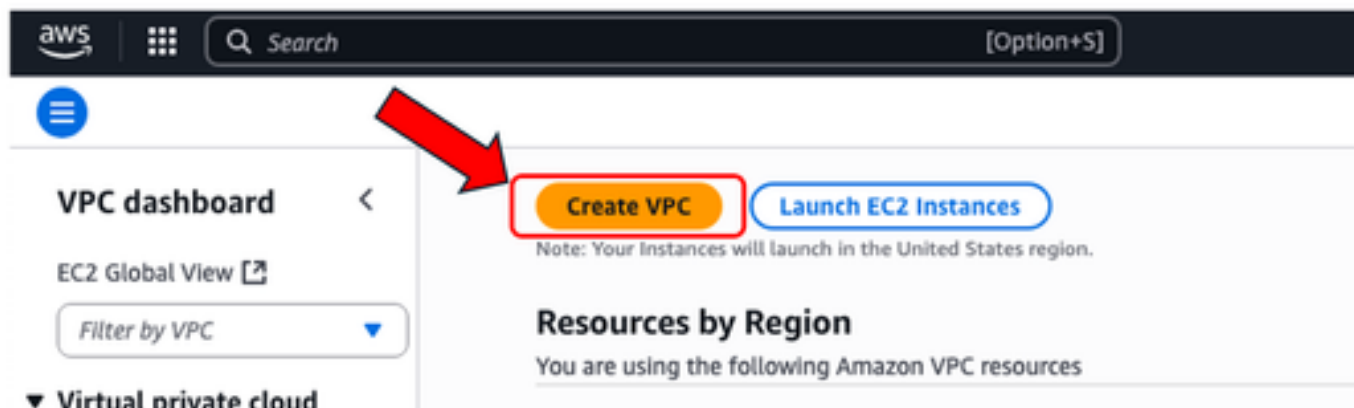
ステップ 1：地域の選択

この導入ガイドでは、VPCリージョンとして米国西部（バージニア北部） – us-east-1リージョンが選択されています。



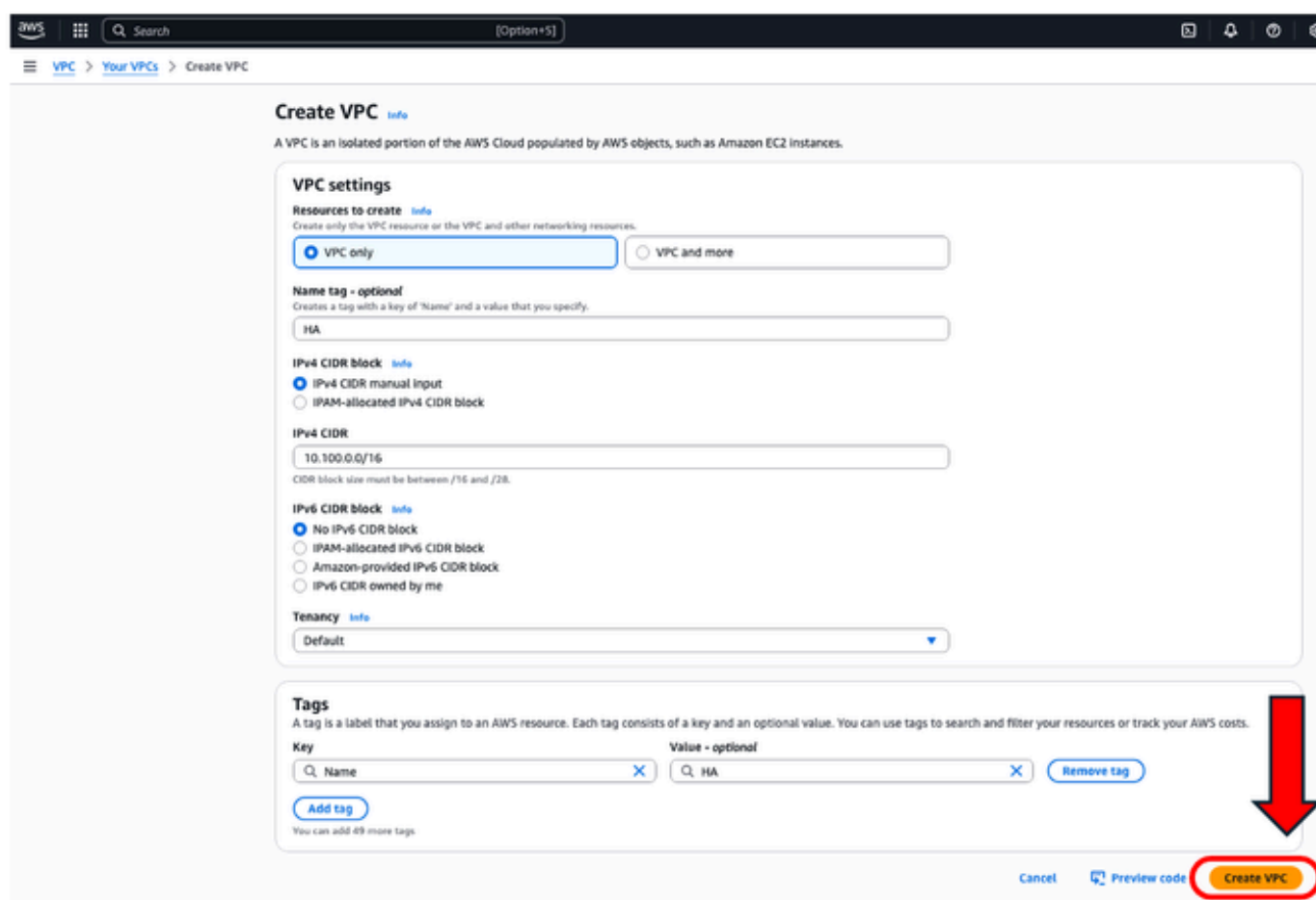
ステップ 2：VPCの作成

AWSコンソールで、[VPC] > [VPCダッシュボード] > [VPCの作成]に移動します。

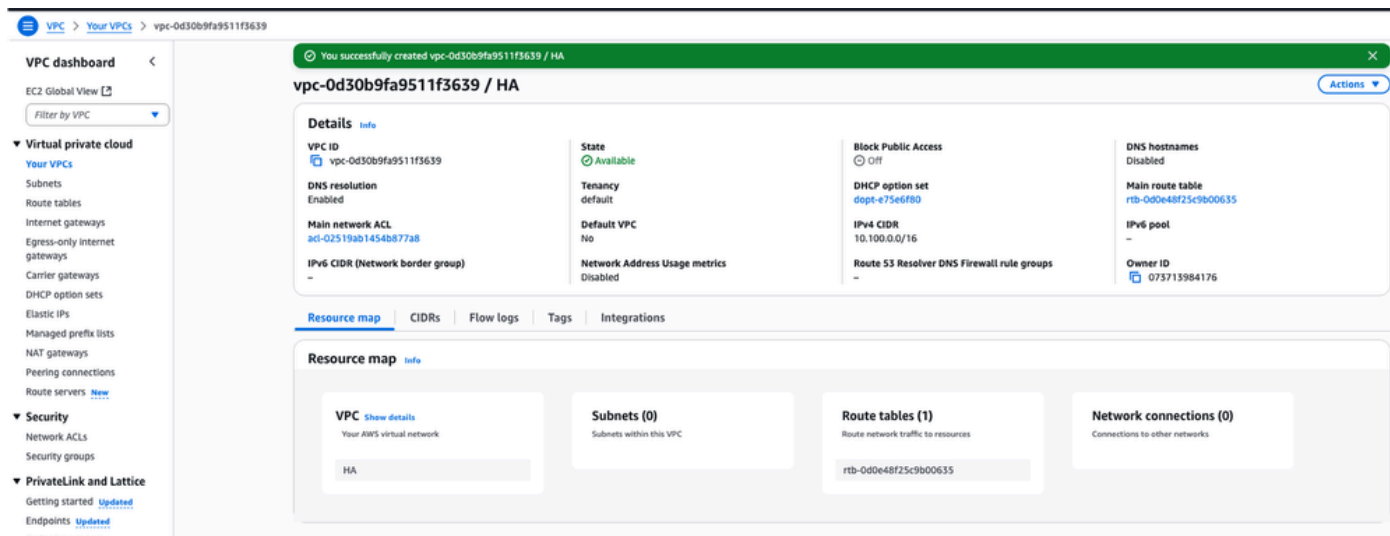


VPCを作成する際には、VPC onlyオプションを選択します。必要に応じて、/16ネットワークを割り当てて使用できます。

この導入ガイドでは、10.100.0.0/16ネットワークを選択します。

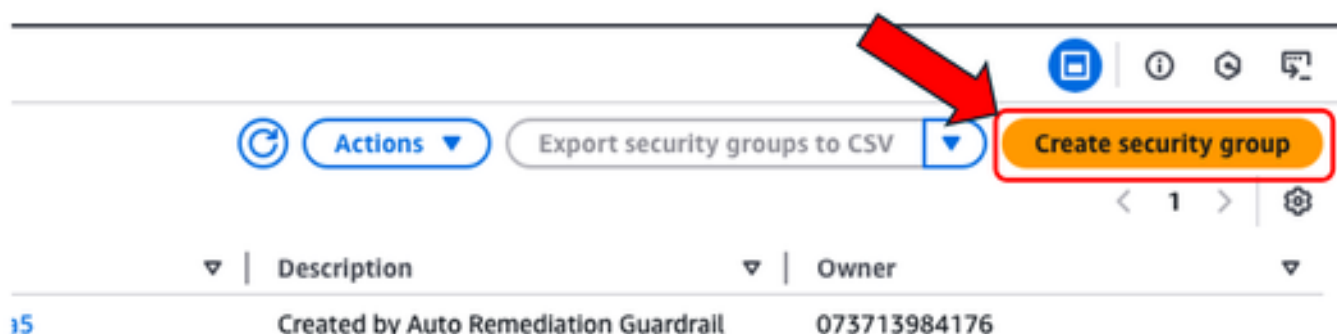


Create VPCをクリックすると、HAタグが付いたVPC-0d30b9fa9511f3639が作成されます。



ステップ 3 : VPCのセキュリティグループの作成

AWSでは、セキュリティグループはACLと同様に機能し、VPC内の構成済みVMへのトラフィックを許可または拒否します。AWSコンソールで、[VPC] > [VPCダッシュボード] > [セキュリティ] > [セキュリティグループ] セクションに移動し、[セキュリティグループの作成] をクリックします。



Inbound Rulesで、許可するトラフィックを定義します。この例では、0.0.0.0/0ネットワークを使用してAll Trafficを選択しています。

Create security group

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

Name cannot be edited after creation.

Description

VPC

Inbound rules

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

Outbound rules

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

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.

You can add up to 50 more tags.

ステップ 4：ポリシーを使用してIAMロールを作成し、VPCに関連付ける

IAMはAMIにAmazon APIへの必要なアクセス権を付与します。C8000vは、AWS APIコマンドを呼び出してAWSのルートテーブルを変更するためのプロキシとして使用されます。デフォルトでは、EC2インスタンスはAPIへのアクセスを許可されていません。このため、AMIの作成時に適用される新しいIAMロールを作成する必要があります。

IAMダッシュボードを参照し、Access Management > Roles > Create Roleに移動します。このプロセスは、次の3つのステップで構成されます。

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)

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.

☐	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)	-

最初に、Trusted entity typeセクションでAWS Serviceオプションを選択し、このポリシーに割り当てられたサービスとしてEC2を選択します。

- 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

終了したら、Nextをクリックします。

IAM > Roles > Create role

Step 1: Select trusted entity
Step 2: **Add permissions**
Step 3: Name, review, and create

Add permissions Info

Permissions policies (1062) Info

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

Filter by Type: All types

Search:

☐	Policy name Info	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**

最後に、ロール名を設定して、Create Roleボタンをクリックします。

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](#)

ステップ 5 : IAMロールに対する信頼ポリシーの作成と適用

ロールを作成したら、必要に応じてAWSルーティングテーブルを変更するスキルを習得するために、信頼ポリシーを作成する必要があります。IAMダッシュボードのポリシーセクションに移動します。Create Policyボタンをクリックします。このプロセスは、次の2つの手順で構成されます。

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**
- Identity providers
- Account settings
- Root access management [New](#)

Access reports

- Access Analyzer

Policies (1367) [Info](#)

A policy is an object in AWS that defines permissions.

Filter by Type

Search

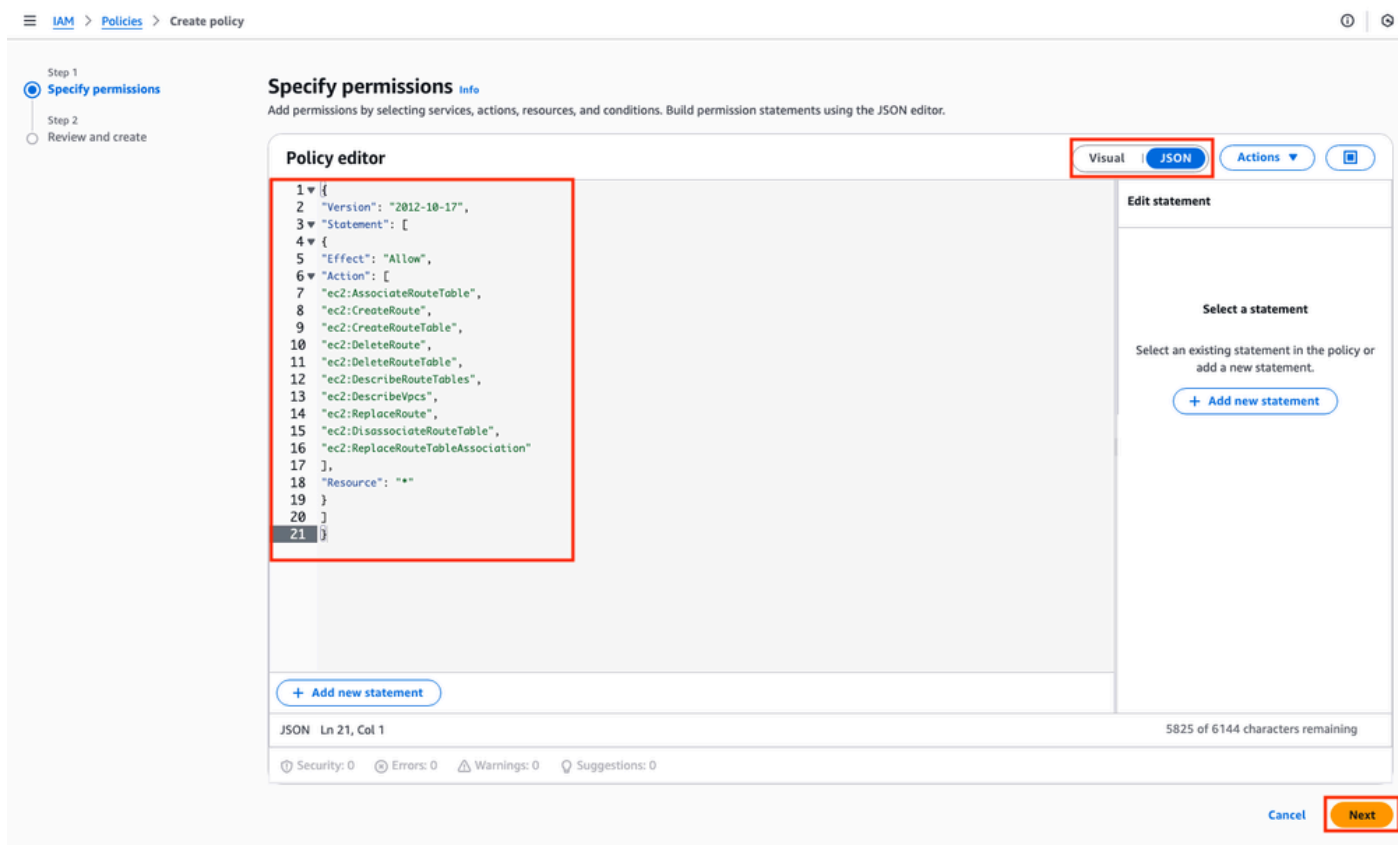
All types

1 2 3 4 5 6 7 ... 69

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

[Create policy](#)

まず、ポリシーエディタでJSONが使用されていることを確認し、次に示すコマンドを適用します。設定が完了したら、Nextをクリックします。



次に、このイメージで使用されているテキストコードを示します。

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

後で、Policy Nameを設定して、Create Policyをクリックします。

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**

ポリシーを作成したら、フィルタリングを行ってポリシーを選択し、ActionsドロップダウンメニューでAttachオプションをクリックします。

IAM > Policies

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

新しいウィンドウが開きます。IAM Entitiesセクションで、作成したIAM Roleをフィルタリングして選択し、Attach policyをクリックします。

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.

Filter by Entity type

Search route

All types 1 match

Entity name	Entity type
route-table-change	Roles

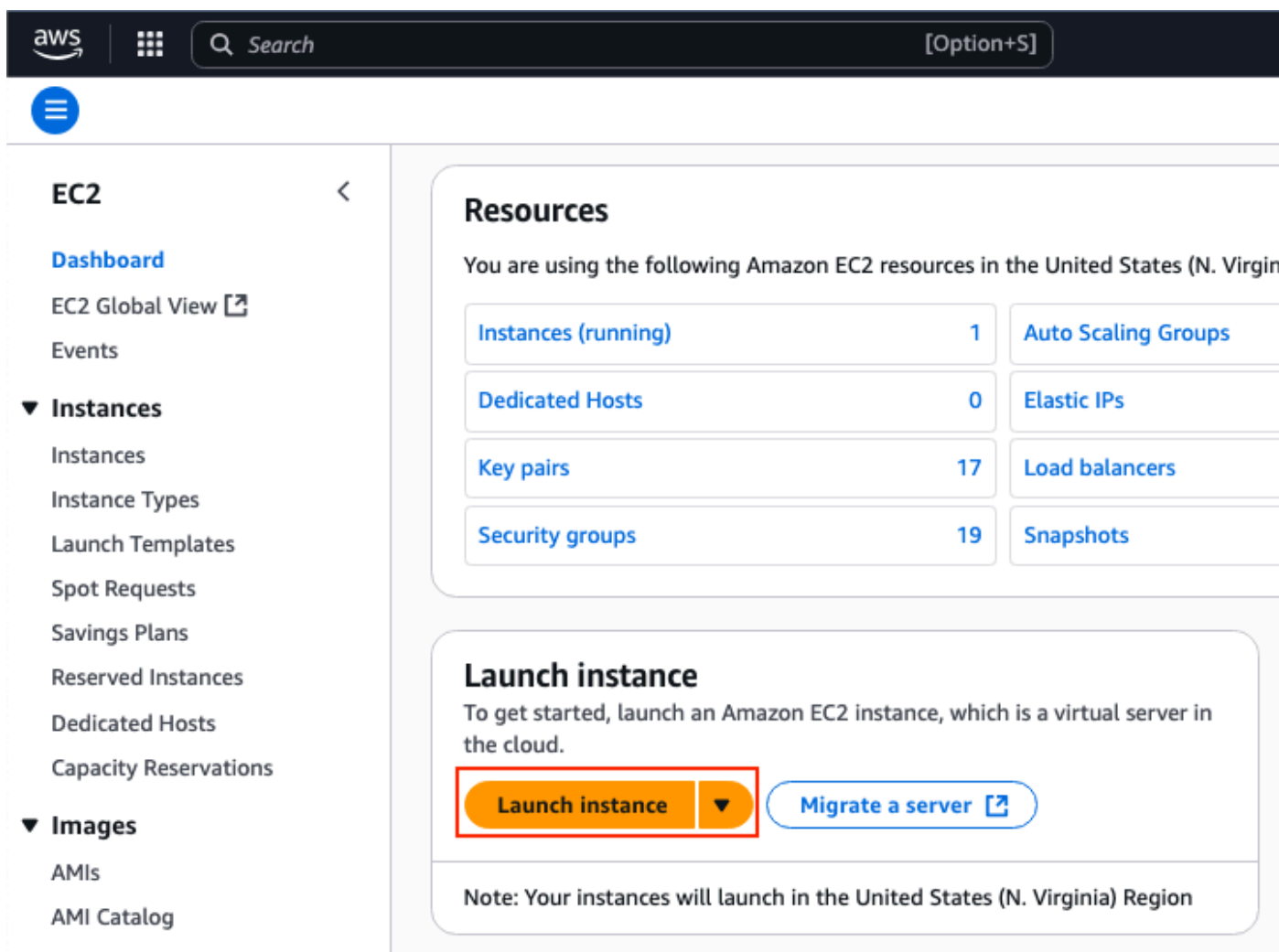
Cancel **Attach policy**

ステップ6:C8000vインスタンの設定と起動

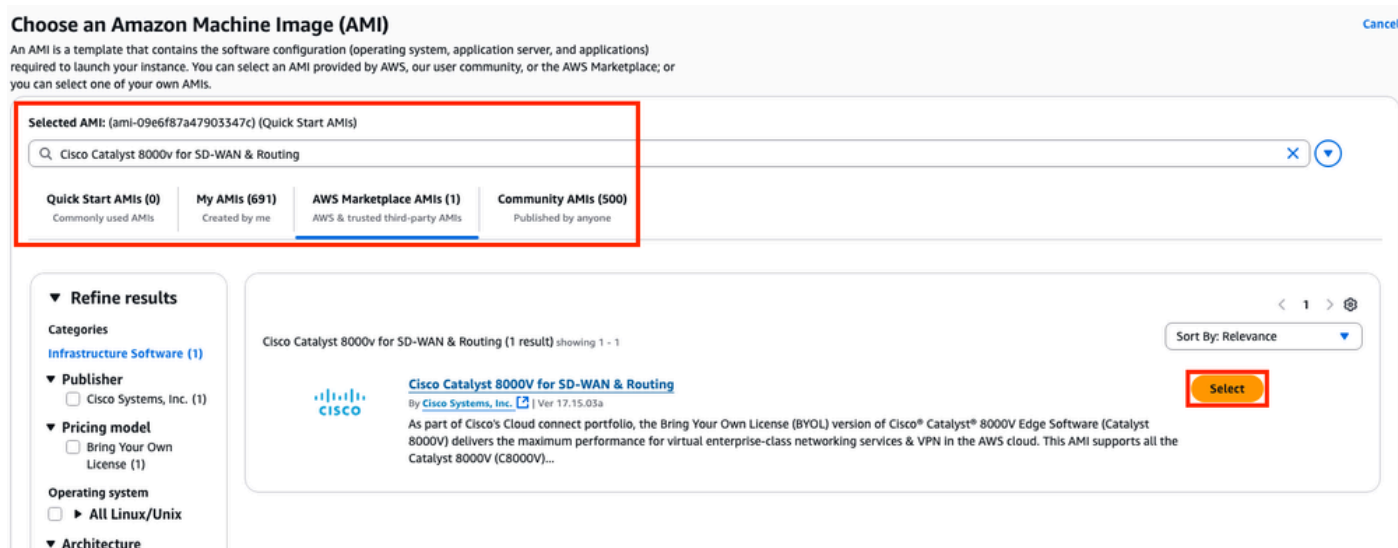
各C8000vルータには2つのインターフェイス (パブリック1つ、プライベート1つ) があり、独自

のアベイラビリティーゾーンに作成されます。

EC2ダッシュボードで、インスタンスの起動をクリックします。

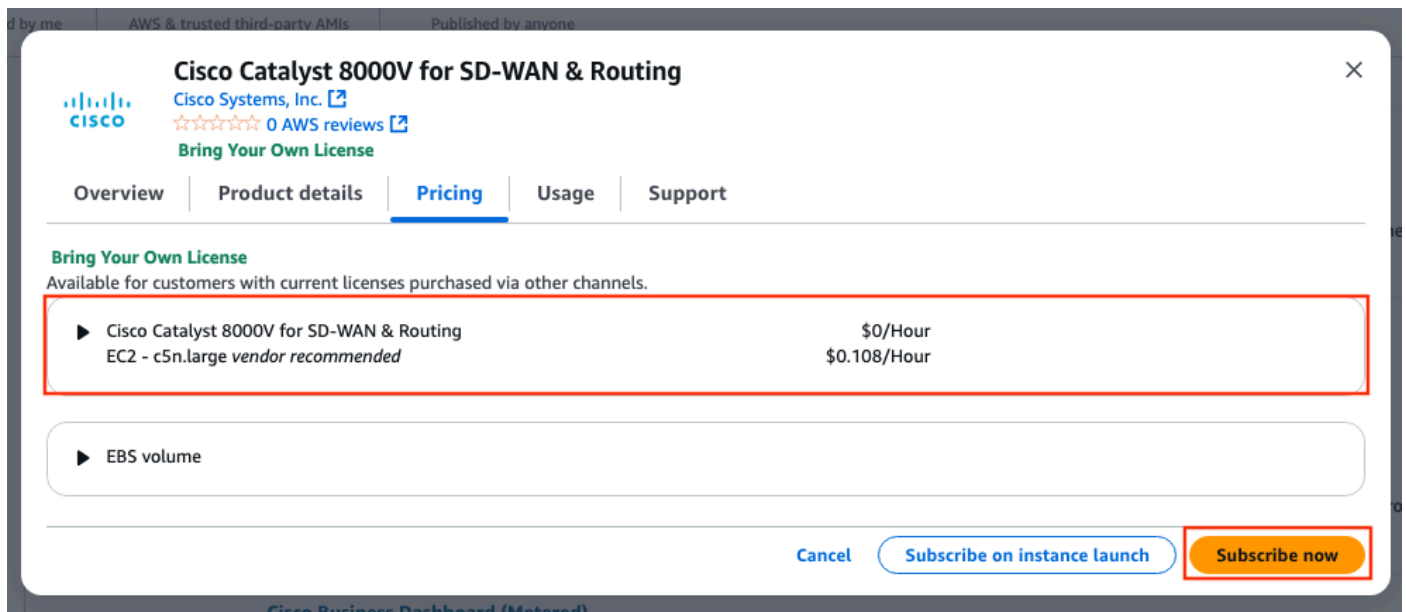


Cisco Catalyst 8000v for SD-WAN & Routingという名前でAMIデータベースをフィルタ処理します。AWS Marketplace AMIsリストで、Selectをクリックします。



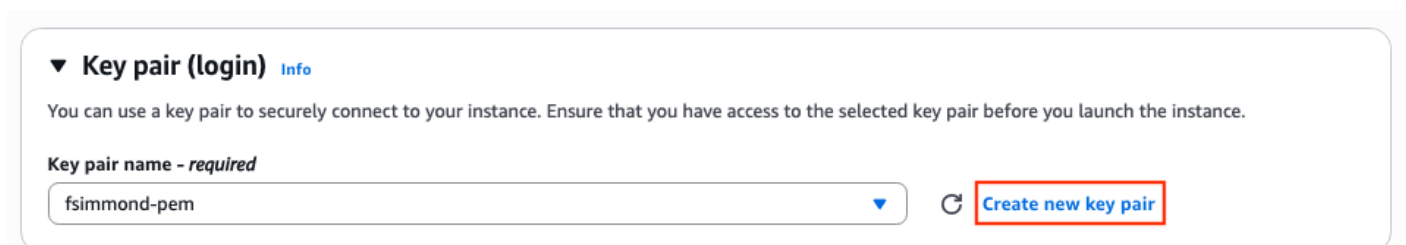
AMIに対応するサイズを選択します。この例では、c5n.largeサイズが選択されています。これは

、ネットワークに必要な容量によって異なります。選択したら、Subscribe nowをクリックします。



ステップ 6.1：リモートアクセス用のキーペアの設定

AMIに登録すると、複数のオプションを含む新しいウィンドウが表示されます。Key pair (login)セクションで、キーペアが存在しない場合は、Create new key pairをクリックします。作成したデバイスごとに1つのキーを再利用できます。



新しいポップアップウィンドウが表示されます。この例では、ED25519暗号化を使用した.pemキーファイルが作成されます。すべてが設定されたら、Create key pairをクリックします。

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

ステップ 6.2 : AMIのサブネットの作成および設定

Network Settingsセクションで、Editをクリックします。セクション内の新しいオプションが利用可能になりました。

1. この作業で使用するVPCを選択します。この例では、HAという名前のVPCが選択されます。
2. Firewall (security groups)セクションで、Select existing security groupを選択します。
3. オプション2を選択すると、「共通セキュリティグループ」オプションが使用可能になります。フィルタリングを行い、目的のセキュリティグループを選択します。この例では、All traffic HAセキュリティグループが選択されています。
4. (オプション) これらのデバイスのサブネットが作成されていない場合は、Create new subnetをクリックします。

▼ **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**

1

4 Create new subnet

2

3 Compare security group rules

Webブラウザの新しいタブが開き、「サブネットの作成」セクションが表示されます。

1. ドロップダウンリストから、この設定に対応するVPCを選択します。
2. 新しいサブネットの名前を設定します。
3. このサブネットの可用性ゾーンを定義します。(設定の詳細については、このドキュメントの「トポロジ」セクションを参照してください)。
4. VPC CIDRブロックに属するサブネットブロックを設定します。
5. さらに、使用されるすべてのサブネットは、「新しいサブネットの追加」セクションをクリックして各サブネットについて2 ~ 4の手順を繰り返すことで作成できます。
6. 終了したら、Create subnetをクリックします。前のページに移動して、設定を続行します。

☰ VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID

Choose a VPC to create the subnet in.

vpc-0d30b9fa9511f3639 (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

Associate a tag with a key or "Name" and a value that you specify.

public-R1-C8000v 2

The name can be up to 256 characters long.

Availability Zone Info

Choose an Availability Zone for your subnet, or let Amazon choose one for you.

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

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.100.0.0/16

IPv4 subnet CIDR block

10.100.10.0/24 4 256 IPs

< > ^ v

▼ **Tags - optional**

Key	Value - optional	
Q Name	Q public-R1-C8000v	Remove

[Add new tag](#)

You can add 49 more tags.

[Remove](#)

[Add new subnet](#) 5

6

[Cancel](#) [Create subnet](#)

Network SettingsセクションのSubnetサブセクションで、Refreshアイコンをクリックして、作成されたサブネットをドロップダウンリストに表示します。

ステップ 6.3 : AMIインターフェイスの設定

Network Settingsセクションで、Advanced Network configuration サブセクションを展開します。次のオプションが表示されます。

▼ 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.

このメニューで、Description、Primary IP、Delete on terminationの各パラメータを設定します。Primary IPパラメータには、サブネットの最初に使用可能なアドレスを除くすべてのIPアドレスを使用します。これはAWSによって内部的に使用されます。

この例では、Delete on terminationパラメータはNoに設定されています。ただし、環境によってはyesに設定することもできます。

このトポロジのため、プライベートサブネットには2番目のインターフェイスが必要です。Add network interfaceをクリックすると、次のプロンプトが表示されます。ただし、インターフェイスは今回サブネットを選択するオプションを提供します。

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

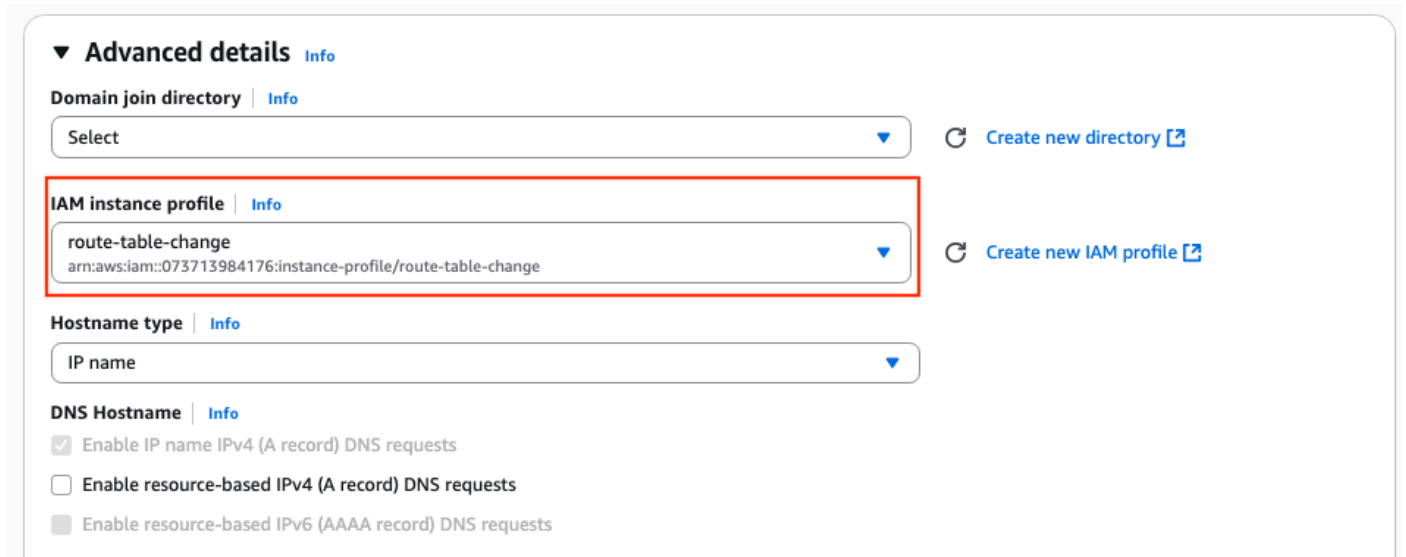
The selected subnet does not support IPv6 IPs.

[Remove](#)

すべてのパラメータをネットワークインターフェイス1で行ったように設定したら、次の手順に進みます。

ステップ 6.4 : IAMインスタンスプロファイルをAMIに設定する

Advanced detailsセクションで、IAM instance profileパラメータで作成したIAMロールを選択します。



▼ 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

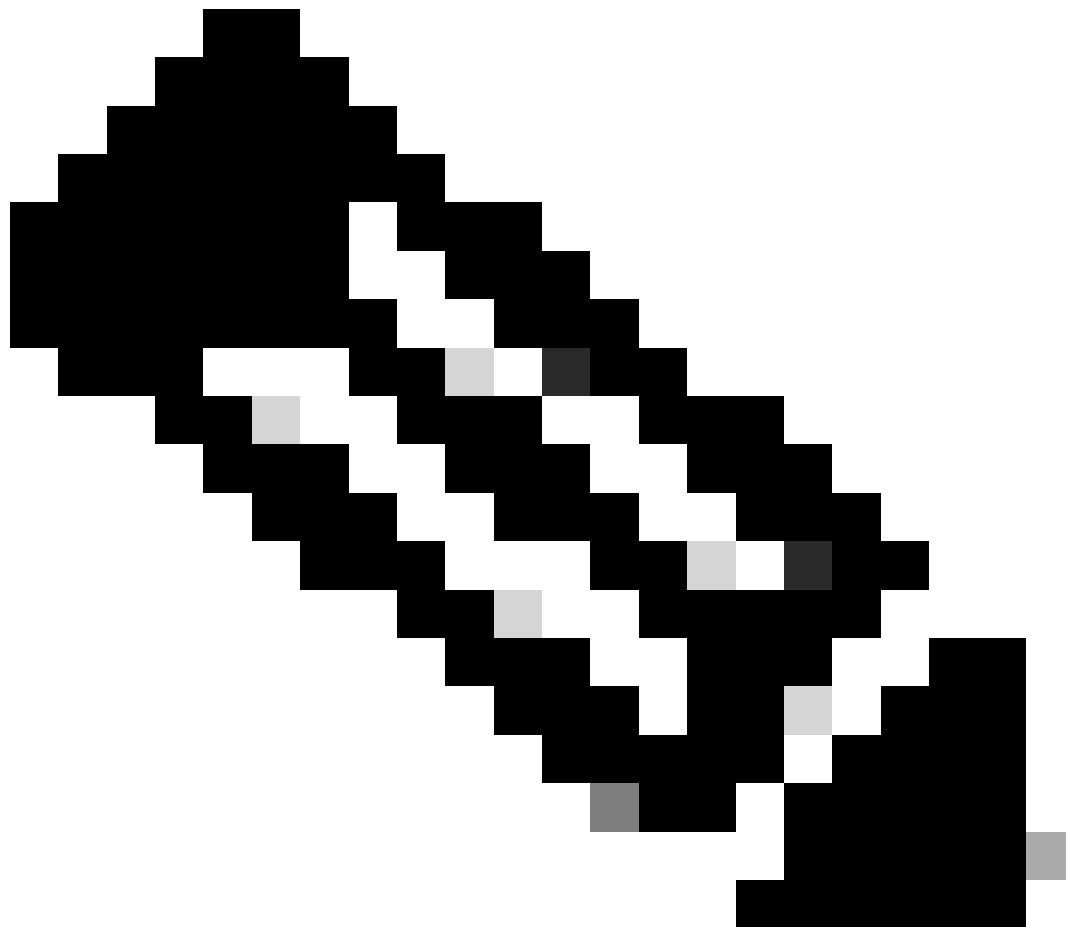
DNS Hostname | [Info](#)

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

ステップ6.5: (オプション) AMIでのクレデンシャルの設定

Advanced detailsセクションで、User data - optional セクションに移動し、この設定を適用してインスタンスの作成中にユーザ名とパスワードを設定します。

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



注:AWSがSSHを使用してC8000vに入力したユーザ名が、ルートとして誤ってリストされる可能性があります。必要に応じて、これをec2-userに変更します。

ステップ 6.6 : インスタンス設定の完了

すべてが設定されたら、Launch Instanceをクリックします。

▼ 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.



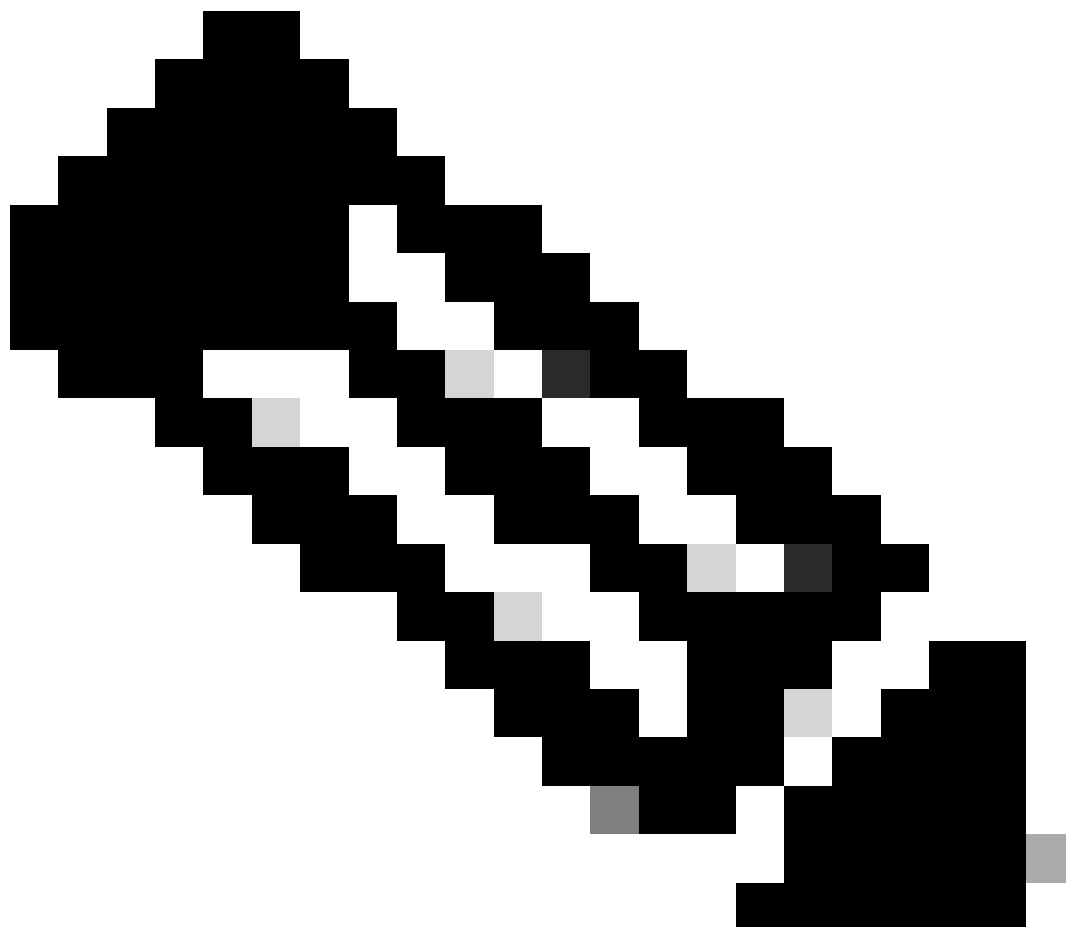
[Cancel](#)

[Launch instance](#)

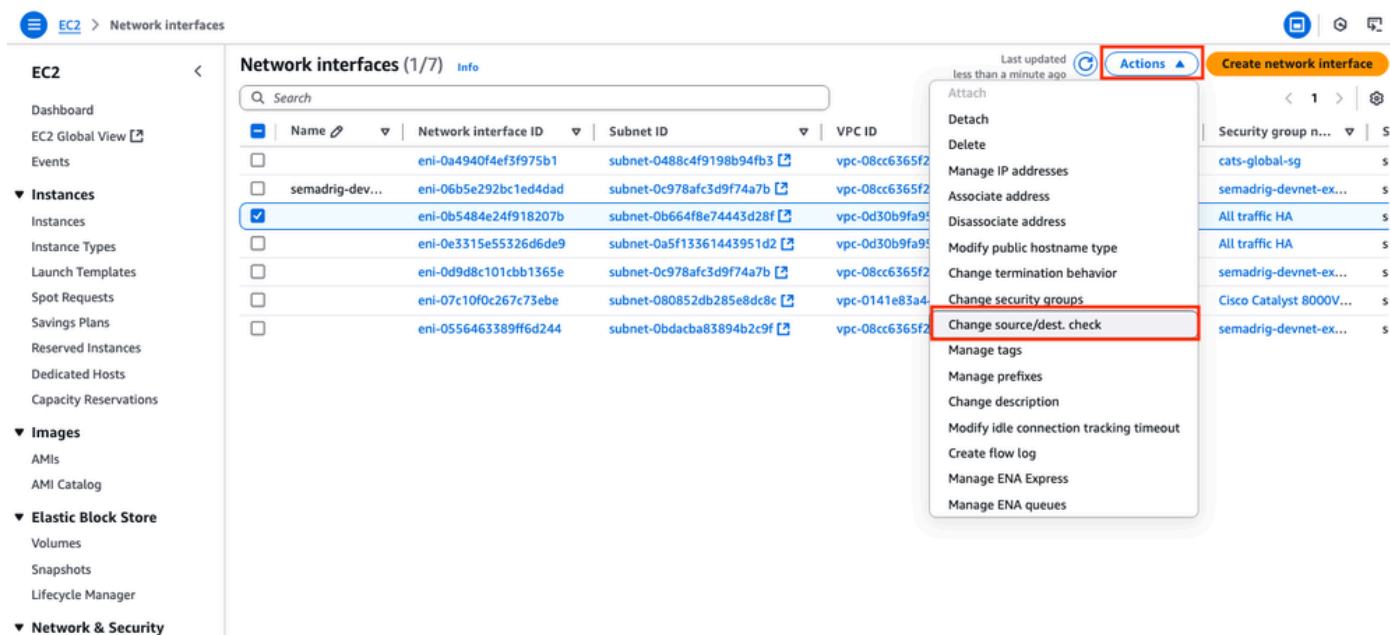
 [Preview code](#)

ステップ 6.7 : ENIでの送信元/宛先チェックの無効化

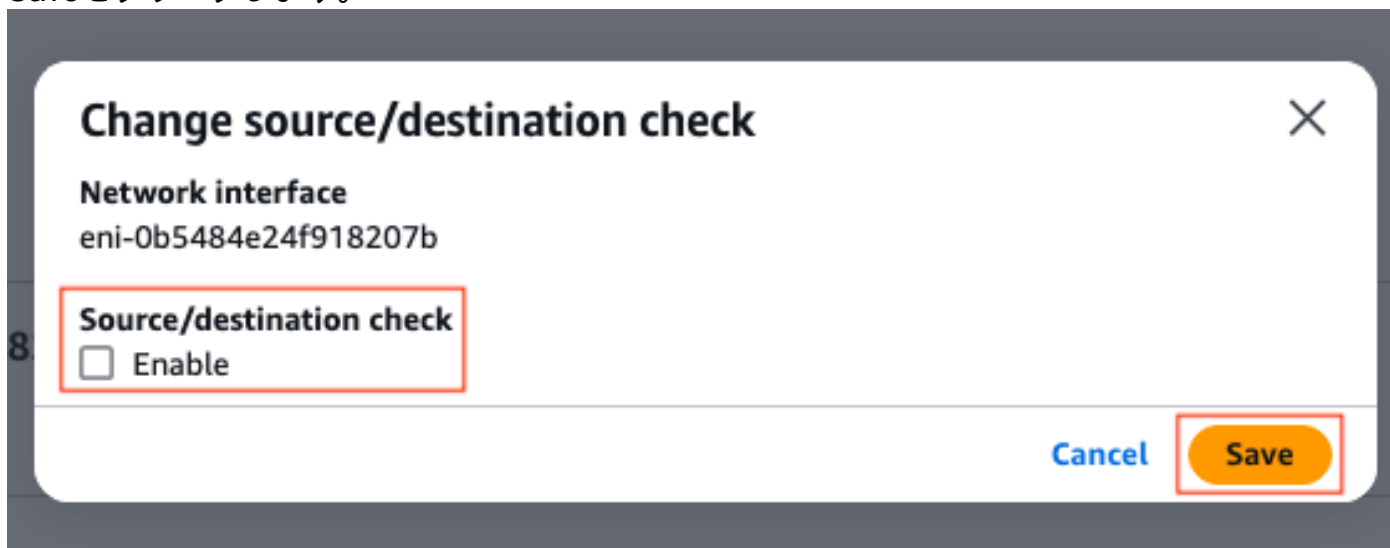
インスタンスが作成されたら、AWSでsrc/dstチェック機能を無効にして、同じサブネットのインターフェイス間の接続を取得します。EC2 Dashboard > Network & Security > Network interfacesセクションで、ENIsを選択して、Actionsをクリックします > Change source/dest. checkを選択します。



注：このオプションを使用できるようにするには、ENIを1つずつ選択する必要があります。

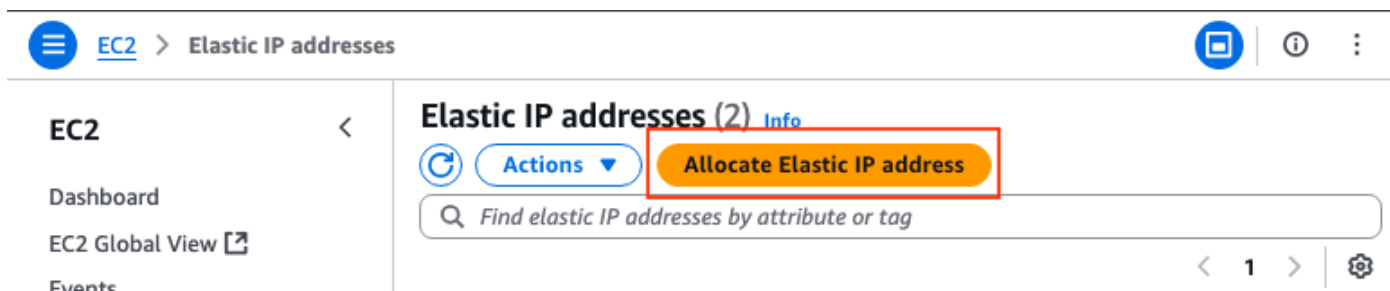


新しいウィンドウが表示されます。新しいメニューでEnableチェックボックスをオフにして、Saveをクリックします。



ステップ 6.8 : インスタンスのパブリックENIへのElastic IPの作成と関連付け

EC2ダッシュボード>ネットワークとセキュリティ> Elastic IPsセクションで、Allocate Elastic IP addressをクリックします。



別のセクションに移動します。この例では、アベイラビリティーゾーンus-east-1とともにAmazon pool of IPv4 addressesオプションが選択されています。終了したら、Allocateをクリック

クします。

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](#)

IPアドレスが作成されたら、インスタンスのパブリックインターフェイスにIPアドレスを割り当てます。EC2 Dashboard > Network & Security > Elastic IPsセクションで、Actions > Associate Elastic IP addressの順にクリックします。

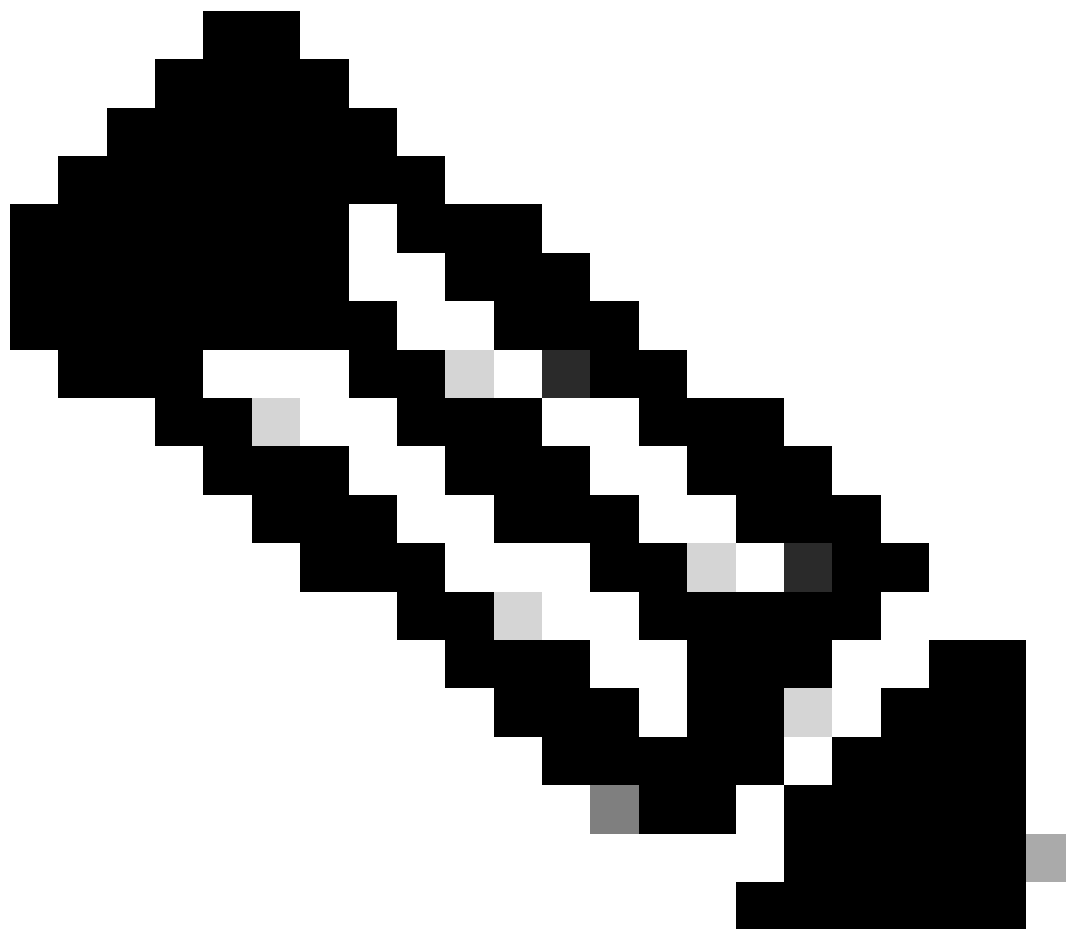
Elastic IP addresses (1/1) [Info](#)

Find elastic IP addresses by attribute or tag

Public IPv4 address [Clear filters](#)

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

この新しいセクションでは、Network interfaceオプションを選択し、対応するインターフェイスのパブリックENIを探します。対応するパブリックIPアドレスを関連付け、Associateをクリックします。



注：適切なENI IDを取得するには、EC2ダッシュボード>インスタンスセクションに移動します。次にインスタンスを選択し、Networkingセクションにチェックマークを入れます。パブリックインターフェイスのIPアドレスを探して、同じ行のENI値を取得します。

Associate Elastic IP address [Info](#)

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

Elastic IP address: [Add 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
eni-0b5484e24f918207b

Private IP address
The private IP address with which to associate the Elastic IP address.
10.100.10.253

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](#)

手順 7：手順6を繰り返して、HA用に2つ目のC8000vインスタンスを作成します

このドキュメントの「トポロジ」のセクションを参照して各インターフェイスに対応する情報を把握し、6.1から6.6に同じ手順を繰り返してください。

ステップ 8：手順6を繰り返して、AMI MarketplaceからVM(Linux/Windows)を作成します

この例では、Ubuntuサーバ22.04.5 LTSがAMI Marketplaceから内部ホストとして選択されています。

ens5はデフォルトでパブリックインターフェイス用に作成されます。この例では、プライベートサブネット用の2番目のインターフェイス (デバイス上のens6) を作成します。

<#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
```

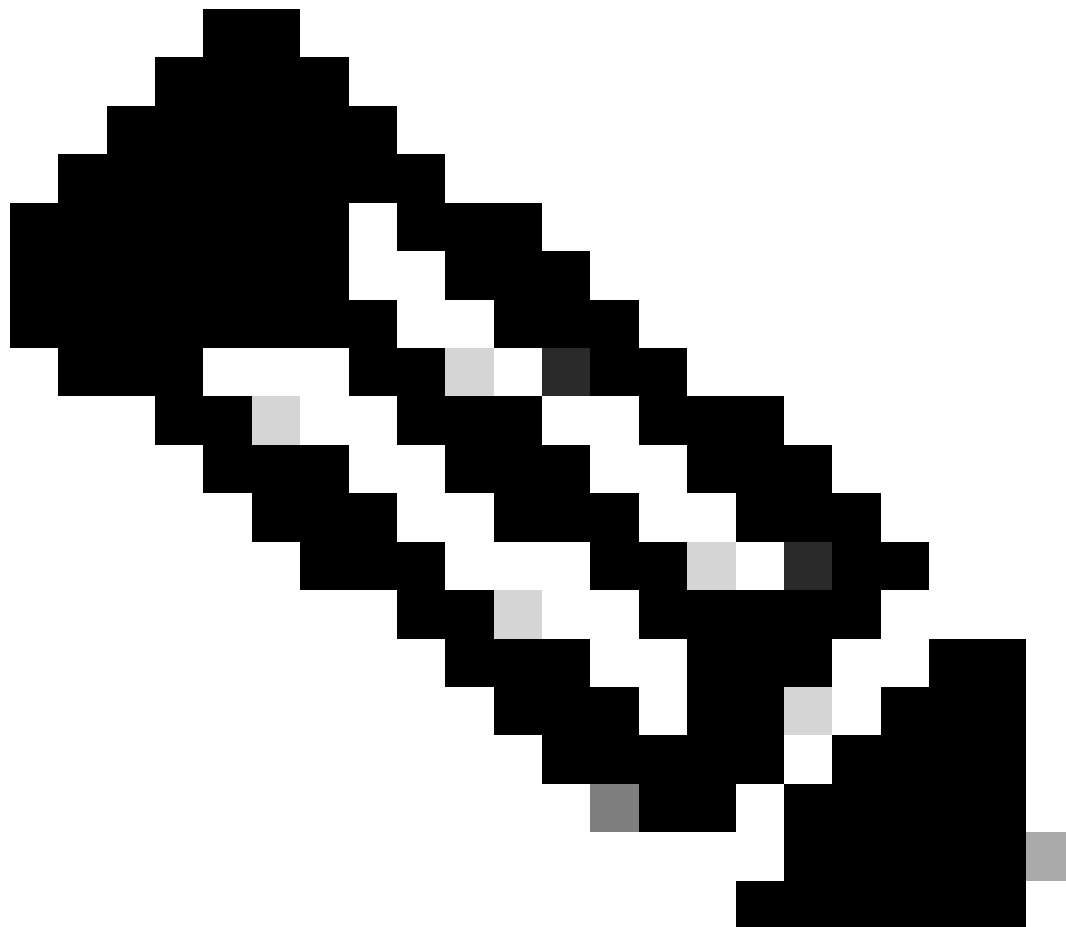
```
10.100.30.254
```

```
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

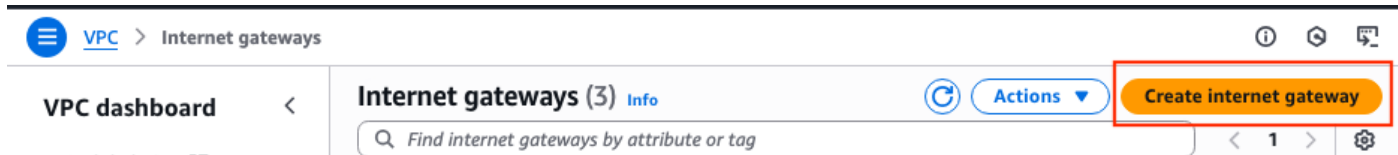
```
netmask 255.255.255.0 broadcast 10.100.130.255
inet6 fe80::3b:7eff:fead:db:e5 prefixlen 64 scopeid 0x20<link>
ether 02:3b:7e:ad:db:e5 txqueuelen 1000 (Ethernet)
RX packets 119 bytes 16831 (16.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 133 bytes 13816 (13.8 KB)
TX errors 0 dropped 0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



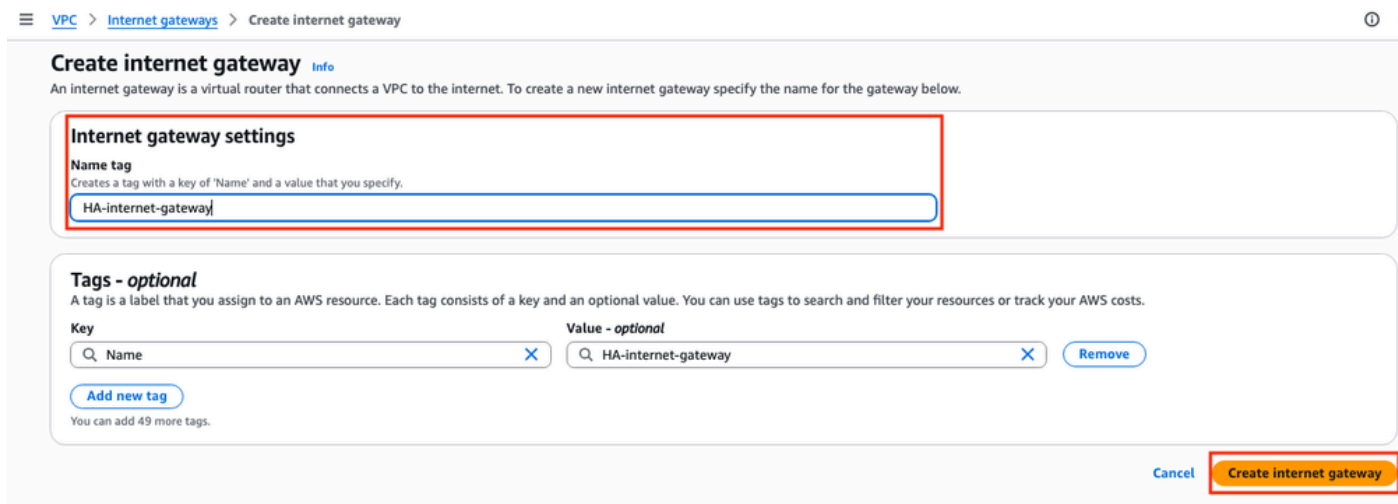
注：インターフェイスに何らかの変更が加えられた場合は、インターフェイスのフラッシュまたはVMのリロードを実行して、これらの変更を適用してください。

ステップ 9：VPC用のインターネットゲートウェイ(IGW)の作成と設定

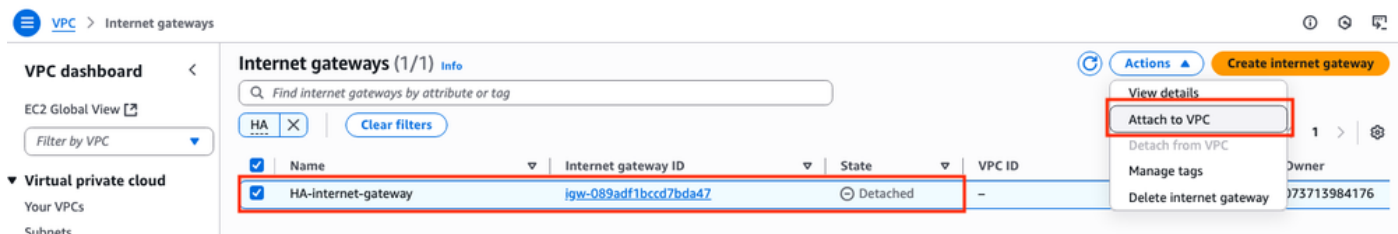
VPCダッシュボード>仮想プライベートクラウド>インターネットゲートウェイセクションで、インターネットゲートウェイの作成をクリックします。



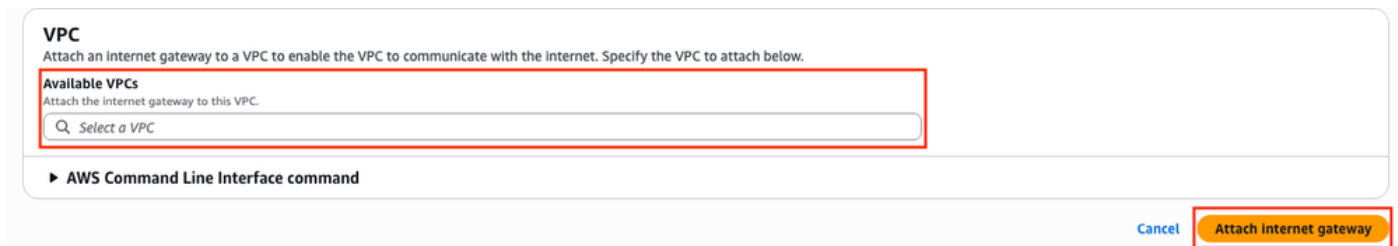
この新しいセクションで、このゲートウェイの**name tag**を作成し、**Create internet gateway**をクリックします。



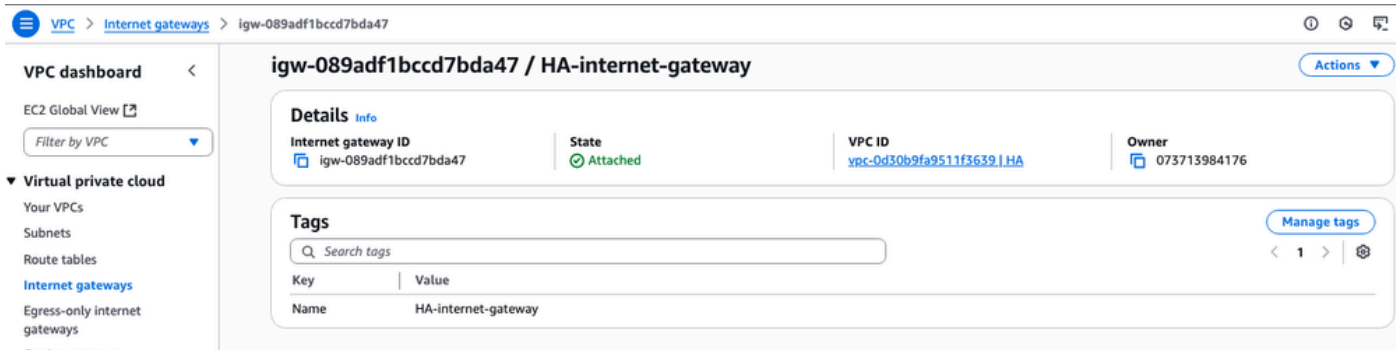
IGWを作成したら、対応するVPCに接続します。**VPCダッシュボード>仮想プライベートクラウド>インターネットゲートウェイセクション**に移動し、対応するIGWを選択します。**Actions > Attach to VPC**の順にクリックします。



この新しいセクションでは、**HA**という名前のVPCを選択します。この例では、**Attach internet gateway**をクリックします。



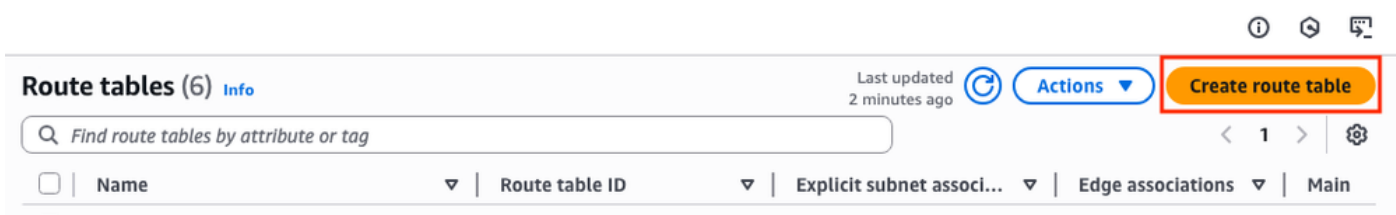
IGWでは、次に示すようにAttachedステータスを示す必要があります。



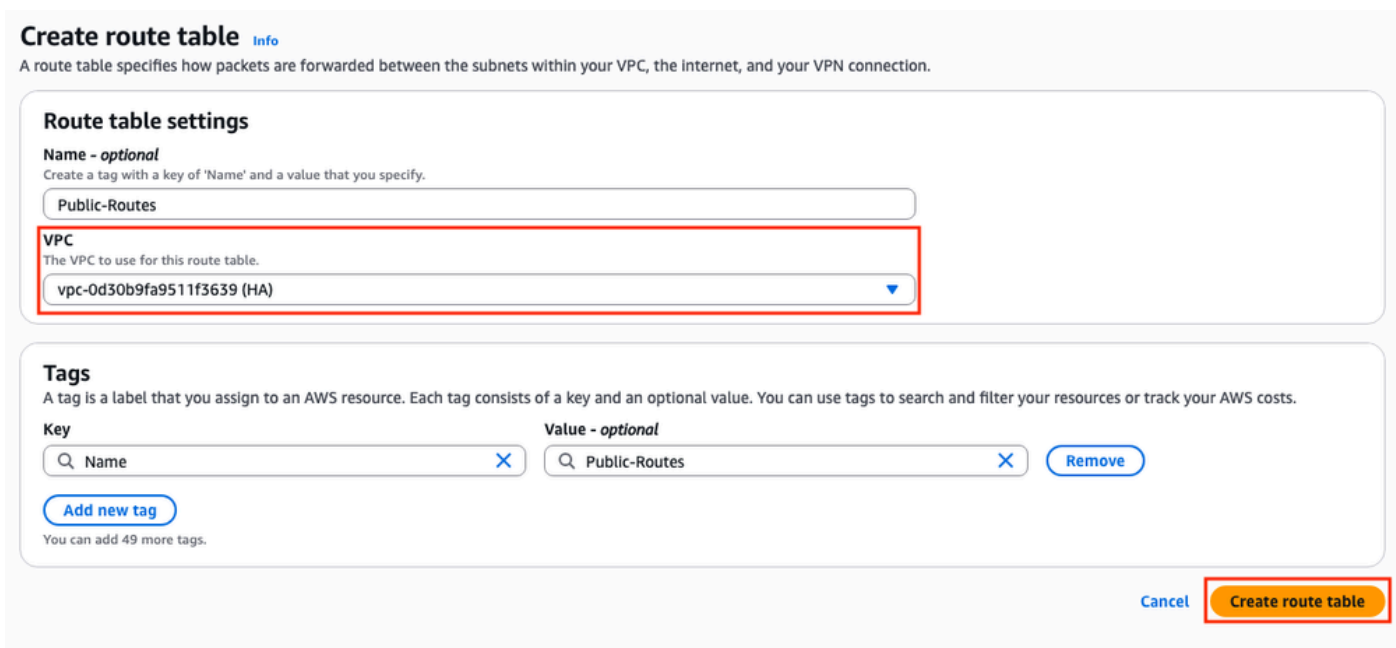
ステップ 10：パブリックおよびプライベートサブネット用のルートテーブルをAWSで作成および設定する

ステップ 10.1：パブリックルートテーブルの作成と設定

このトポロジでHAを確立するには、すべてのパブリックサブネットとプライベートサブネットを対応するルートテーブルに関連付けます。VPCダッシュボード>仮想プライベートクラウド>ルートテーブルセクションで、ルートテーブルの作成をクリックします。



新しいセクションで、このトポロジに対応するVPCを選択します。選択したら、Create route tableをクリックします。



Route tablesセクションで、createdテーブルを選択し、Actions > Edit Subnet associationsの順にクリックします。

☰ VPC > Route tables

EC2 Global View

Filter by VPC

▼ Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only Internet

Route tables (1/1) Info

Last updated 8 minutes ago

Find route tables by attribute or tag

public-routes Clear filters

☒	Name	Route table ID	Explicit subnet associ...
☒	Public-Routes	rtb-0d0e48f25c9b00635	3 subnets

Actions

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

Main No

次に、対応するサブネットを選択し、Save associationsをクリックします。

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (3/6)

Filter subnet associations

public 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](#) [subnet-04fb9de939e3778bb / Public-VM-linux-1c - fsmmond](#) [subnet-02d8108842f9f3129 / public-R2-C8000v](#)

Cancel **Save associations**

サブネットを関連付けたら、ルートテーブルIDハイパーリンクをクリックして、テーブルに適切なルートを追加します。次に、Edit Routesをクリックします。

Route tables (1/1) Info

Find route tables by attribute or tag

public-routes Clear filters

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

インターネットアクセスを取得するには、Add routeをクリックし、このパブリックルートテーブルと、ステップ9で作成したIGWを、上記のパラメータでリンクします。選択したら、Save changesをクリックします。

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

ステップ 10.2 : プライベートルートテーブルの作成と設定

パブリックルートテーブルが作成されたので、ルートにインターネットゲートウェイを追加する以外は、プライベートルートとプライベートサブネットに手順10を繰り返します。この例では、8.8.8.8のトラフィックはプライベートサブネットを通過する必要があるため、ルーティングテーブルは次のようになります。

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

ステップ 11基本的なネットワーク設定、ネットワークアドレス変換(NAT)、BFDを使用したGREトンネル、およびルーティングプロトコルの確認と設定

AWSでインスタンスとそのルーティング設定を準備したら、デバイスを設定します。

C8000v R1の設定 :

```
interface Tunnel1
ip address 192.168.200.1 255.255.255.0
bfd interval 500 min_rx 500 multiplier 3
tunnel source GigabitEthernet1
tunnel destination <Public IPv4 address of C8000v R2>
!
interface GigabitEthernet1
ip address 10.100.10.254 255.255.255.0
ip nat outside
negotiation auto
!
interface GigabitEthernet2
ip address 10.100.110.254 255.255.255.0
ip nat inside
negotiation auto
!
router eigrp 1
bfd interface Tunnel1
network 192.168.200.0
```



```

passive-interface GigabitEthernet1
!
ip access-list standard 10
10 permit 10.100.130.0 0.0.0.255
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 10.100.10.1
ip route 10.100.130.0 255.255.255.0 GigabitEthernet2 10.100.110.1

```

C8000v R2の設定：

```

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

```

ステップ 12ハイアベイラビリティの設定(Cisco IOS® XE Denali 16.3.1a以降)

VM間の冗長性と接続が設定されたので、ルーティングの変更を定義するHA設定を設定します。BFDピアダウンなどのAWS HAエラーの後で設定する必要があるRoute-table-id、Network-interface-id、およびCIDR値を設定します。

```

Router(config)# redundancy
Router(config-red)# cloud provider aws (node-id)

```

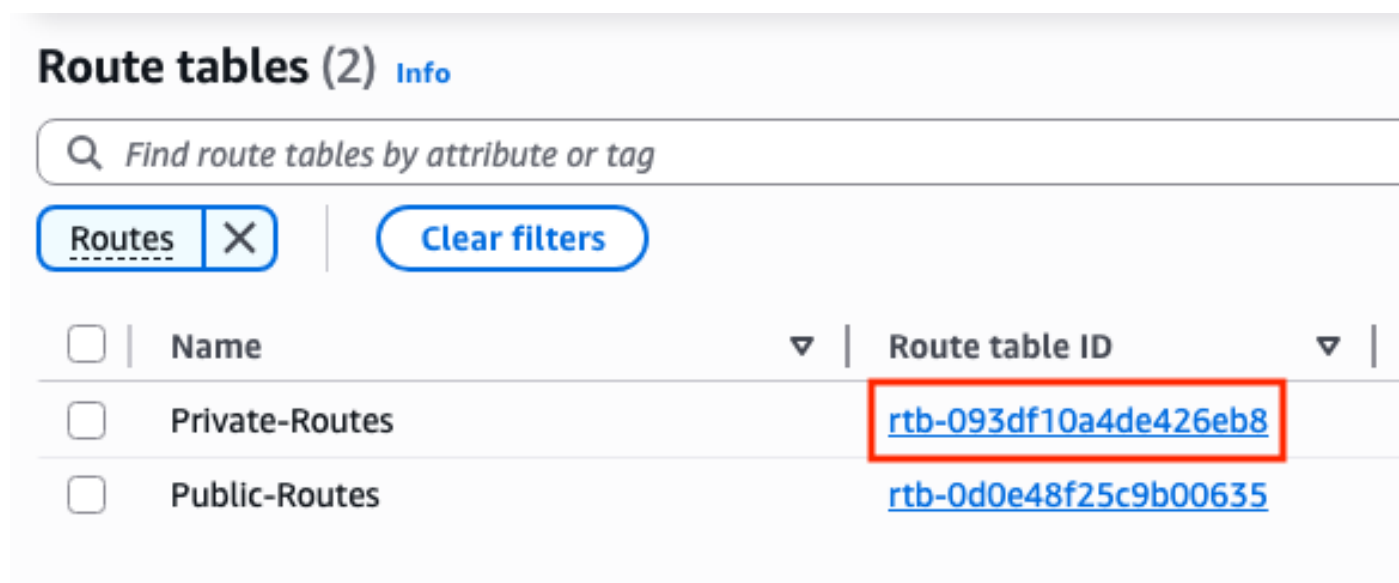
```
bfd peer <IP address of the remote device>
route-table <Route table ID>
cidr ip <traffic to be monitored/prefix>
eni <Elastic network interface (ENI) ID>
region <region-name>
```

bfd peerパラメータはトンネルピアのIPアドレスに関連しています。これは、show bfd neighborの出力を使用して確認できます。

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

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

route-tableパラメータは、VPCダッシュボード>仮想プライベートクラウド>ルートテーブルセクションにあるプライベートルートテーブルIDに関連します。対応するルートテーブルIDをコピーします。



The screenshot shows the AWS VPC console's 'Route tables (2)' page. It includes a search bar, a 'Routes' filter button, and a 'Clear filters' button. A table lists route tables with columns for Name and Route table ID. The 'Private-Routes' entry is selected, and its ID 'rtb-093df10a4de426eb8' is highlighted with a red box.

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

cidr ipパラメータは、プライベートルートテーブルに追加されたルートプレフィックス (手順 10.2で作成されたルート) に関連します。

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

eniパラメータは、設定されるインスタンスの対応するプライベートインターフェイスのENI IDに関連します。この例では、インスタンスのインターフェイスGigabitEthernet2のENI IDが使用されます。

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](#)

< 1 > 

	Name Info	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
☐	C8000v-R2-fsimmond	i-0a1a91794f919f641	 Stopped Info Refresh	c5n.large	-	View alarms +	us-east-1b
☐	Ubuntu VM - fsimmond	i-03a306e81a0b99864	 Stopped Info Refresh	m5.large	-	View alarms +	us-east-1c
☒	C8000v-R1-fsimmond	i-0b9a50a09b089b03a	 Running Info Refresh	c5n.large	 3/3 checks passed	View alarms +	us-east-1a

i-0b9a50a09b089b03a (C8000v-R1-fsimmond)

 ▼

[Details](#) | [Status and alarms](#) | [Monitoring](#) | [Security](#) | [Networking](#) ² | [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	-	 10.100.100.254	10.100.10.254	-	-
 eni-070e14fbfde0d8e3b	1	0	-	-	10.100.110.254	-	-

region/パラメータは、VPCが配置されているリージョンのAWSドキュメントで見つかったコード名に関連しています。この例では、us-east-1 リージョンが使用されます。

ただし、このリストは変更されたり拡大したりする可能性があります。最新の更新プログラムについては、[AmazonRegion and Availability](#)ゾーンのドキュメントを参照してください。

これらの情報をすべて考慮した、VPC内の各ルータの設定例を次に示します。

C8000v R1の設定例：

```
redundancy
cloud provider aws 1
bfd peer 192.168.200.2
route-table rtb-093df10a4de426eb8
cidr ip 8.8.8.8/32
eni eni-070e14fbfde0d8e3b
region us-east-1
```

C8000v R2の設定例：

```
redundancy
cloud provider aws 1
bfd peer 192.168.200.1
route-table rtb-093df10a4de426eb8
cidr ip 8.8.8.8/32
eni eni-0239fda341b4d7e41
region us-east-1
```

検証

1. C8000v R1インスタンスのステータスを確認します。トンネルとクラウドの冗長性が稼働していることを確認します。

```
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. ルータの背後にあるホストVMから8.8.8.8に対して連続pingを実行します。pingがプライベートインターフェイスを通過することを確認してください。

```
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. AWS WebGUIを開き、ルーティングテーブルのステータスを確認します。現在のENIは、R1インスタンスのプライベートインターフェイスに属しています。

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. HAフェールオーバーイベントをシミュレートするために、R1インスタンスでTunnel1インターフェイスをシャットダウンして、ルート変更をトリガーします。

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

5. AWSのルートテーブルで再度チェックしてください。ENI IDはR2プライベートインターフェイスENI IDに変更されました。

Routes (2)

Destination

8.8.8.8/32

10.100.0.0/16

▼

Target

[eni-0239fda341b4d7e41](#)

local

トラブルシューティング

次に、展開の再作成時に忘れられたり、設定が誤っていたりすることの多い一般的なポイントの大部分を示します。

- リソースが関連付けられていることを確認します。VPC、サブネット、インターフェイス、ルートテーブルなどを作成するとき、これらの多くは自動的に相互に関連付けられません。彼らはお互いに何の知識も持っていない。
- Elastic IPと任意のプライベートIPが正しいインターフェイスに関連付けられており、正しいサブネットが正しいルートテーブルに追加され、正しいルータに接続され、正しいVPCとゾーンがIAMロールとセキュリティグループにリンクされていることを確認します。
- ENIごとのSource/Destチェックを無効にします。
このセクションで説明したすべての点を確認しても問題が解決しない場合は、次の出力を収集し、可能であればHAフェールオーバーをテストしてから、Cisco TACでケースをオープンしてください。

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。