

Amazon AWSでのCSR1000v HA冗長性デプロイガイド

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[目標](#)

[トポロジ](#)

[ネットワーク図](#)

[用語](#)

[制約事項](#)

[コンフィギュレーション](#)

[ステップ1：地域を選択します。](#)

[ステップ2:VPCを作成します。](#)

[ステップ3:VPCのセキュリティグループを作成します。](#)

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

[ステップ5：作成したAMIロールでCSR1000vを起動し、パブリック/プライベートサブネットを関連付けます。](#)

[ステップ6：ステップ5を繰り返し、HA用に2番目のCSR1000vインスタンスを作成します。](#)

[ステップ7：ステップ5を繰り返し、AMI MarketplaceからVM\(Linux/Windows\)を作成します。](#)

[ステップ8：プライベートおよびパブリックルートテーブルを設定します。](#)

[手順9:BFIDと任意のルーティングプロトコルを使用して、ネットワークアドレス変換\(NAT\)とGREトンネルを設定します。](#)

[ステップ10：ハイアベイラビリティの設定 \(Cisco IOS XE Denali 16.3.1a以降 \)](#)

[ハイアベイラビリティの確認](#)

[トラブルシューティング](#)

[問題：httpc_send_requestが失敗しました](#)

[問題：ルートテーブルrtb-9c0000f4とインターフェイスeni-32791318が異なるネットワークに属している](#)

[問題：この操作を実行する権限がありません。Encoded Authorization Failureメッセージ。](#)

[関連情報](#)

概要

このドキュメントでは、Amazon AWSクラウドでハイアベイラビリティを実現するためにCSR1000vルータをデプロイする方法に関する設定ガイドについて説明します。これは、ユーザーにHAに関する実用的な知識を提供し、完全に機能するテストベッドを導入できるようにすることを目的としています。

AWSとHAの詳細な背景については、セクションを参照してください。

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。

- Amazon AWSアカウント
- 2つのCSR1000vおよび1つのLinux/Windows AMIを同じリージョンに配置
- HAバージョン1は、Cisco IOS-XE®バージョン16.5 ~ 16.9でサポートされます。 16.11以降では、HAバージョン3を使用します。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS-XE® Denali 16.7.1に基づくものです。

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、初期（デフォルト）設定の状態から起動しています。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。

目標

複数のアベイラビリティゾーン環境で、プライベートデータセンター(VM)からインターネットへの連続トラフィックをシミュレートします。HAフェールオーバーをシミュレートし、ルーティングテーブルがトラフィックをCSRHAからCSRHA1のプライベートインターフェイスに切り替えたため、HAが成功することを確認します。

トポロジ

設定を開始する前に、トポロジと設計を完全に理解することが重要です。これは、後で潜在的な問題をトラブルシューティングするのに役立ちます。

ネットワーク要件に基づいて、HA導入の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ています。

- 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:CSR1000vルータ(Cisco IOS-XE® Denali 16.3.1a以降)
- 1x:VM(Linux/Windows)

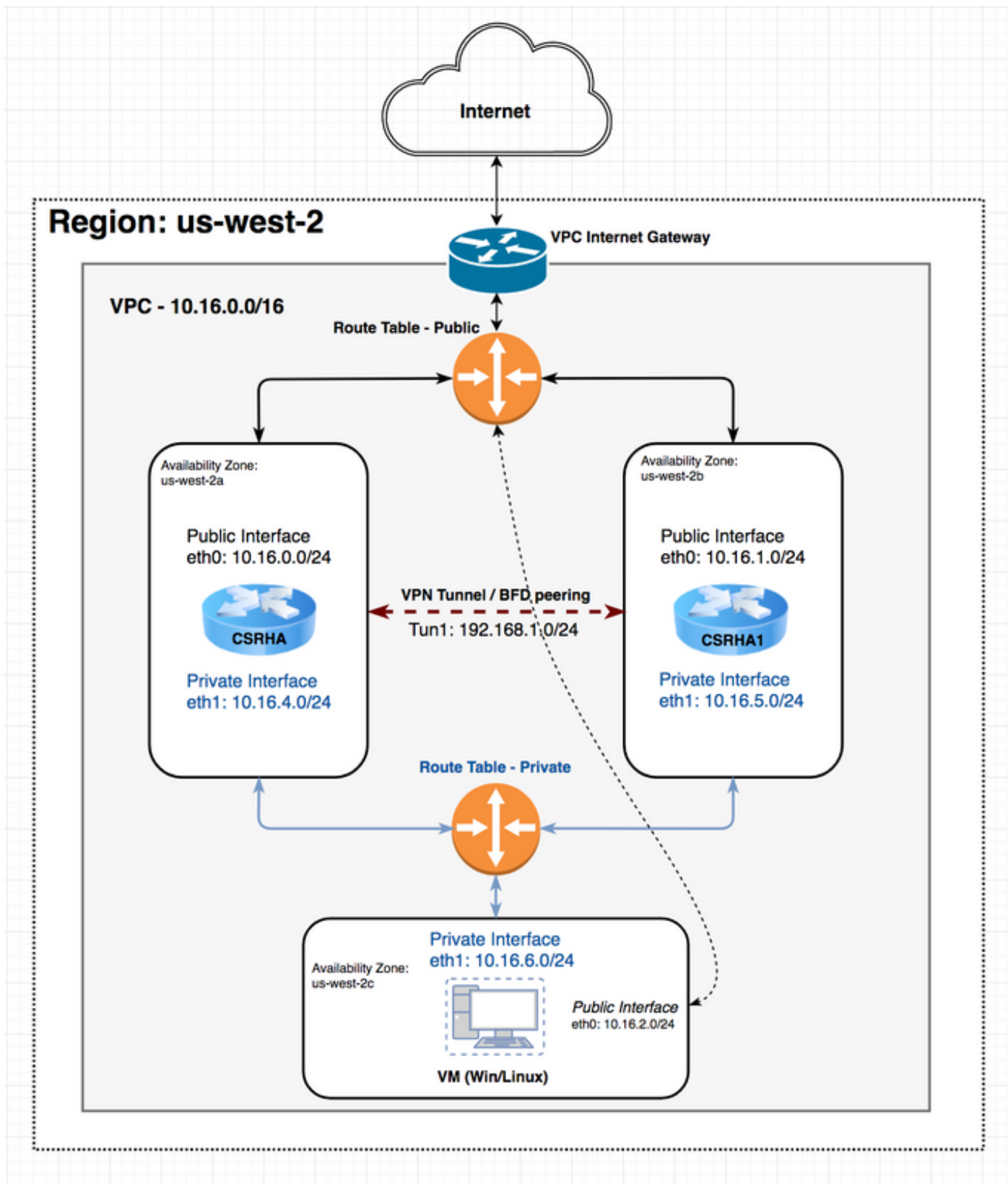
1つのHAペアに2台のCSR1000vルータがあり、2つの異なるアベイラビリティゾーンに存在します。ハードウェアの復元力を高めるために、各可用性ゾーンを個別のデータセンターと考えてください。

3番目のゾーンはVMで、プライベートデータセンター内のデバイスをシミュレートします。現時点では、インターネットアクセスはパブリックインターフェイスを介して有効になっているため

、VMにアクセスして設定できます。通常、すべての通常のトラフィックは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。

トラフィックシミュレーションのため、CSRHA→8.8.8.8を使用→てVMの→プライベートインターフェイスとプライベートルートテーブルにpingを実行します。フェールオーバーシナリオでは、プライベートルートテーブルがCSRHA1のプライベートインターフェイスを指すようにルートを切り替えたことを確認します。

ネットワーク図



用語

RTB : ルートテーブルID。

CIDR : ルートテーブルで更新されるルートの宛先アドレス。

ENI : トラフィックがルーティングされるCSR 1000vギガビットインターフェイスのネットワークインターフェイスID。

たとえば、CSRHAが失敗すると、CSRHA1がAWSルートテーブル内のルートを引き継ぎ、自身のENIを指すように更新します。

REGION:CSR 1000vのAWSリージョン。

制約事項

- プライベートサブネットの場合は、IPアドレス10.0.3.0/24を使用しないでください。これは、ハイアベイラビリティのためにCisco CSR 1000vの内部で使用されます。Cisco CSR 1000vでは、AWSルートテーブルを変更するREST API呼び出しを行うために、パブリックインターネットアクセスIBILITYが必要です。
- CSR1000vのgig1インターフェイスをVRF内に配置しないでください。 HAはそれ以外では動作しません。

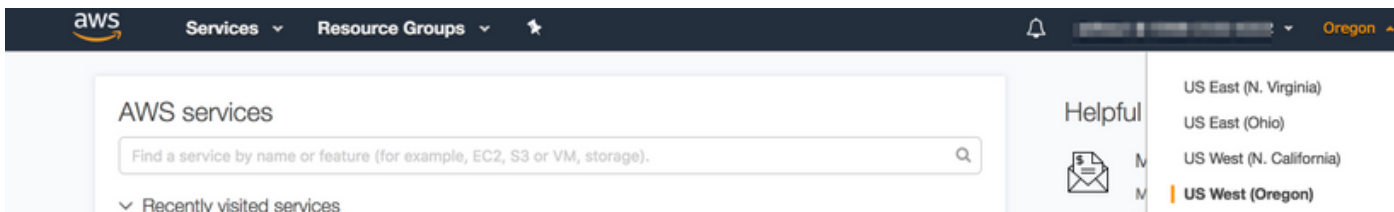
コンフィギュレーション

設定の一般的なフローは、最も包括的な機能（リージョン/VPC）から開始し、最も具体的な機能（インターフェイス/サブネット）まで下っていきます。ただし、特定の設定順序はありません。開始する前に、まずトポロジを理解することが重要です（トポロジの説明を参照）。

ヒント：すべての設定（VPC、インターフェイス、サブネット、ルートテーブルなど）に名前を付けます。

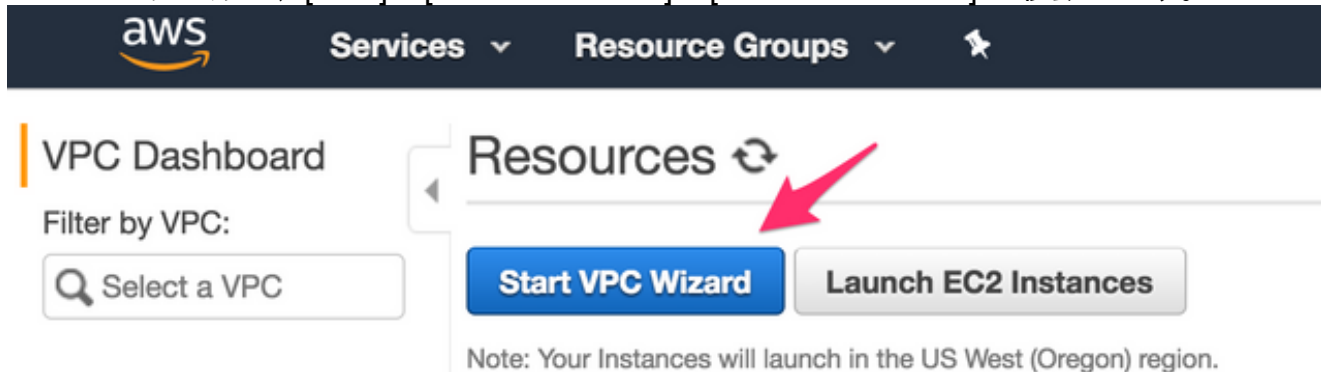
ステップ1：地域を選択します。

この例では、米国西部（オレゴン）を使用します。



ステップ2:VPCを作成します。

1. AWSコンソールで、[VPC] > [VPC Dashboard] > [Start VPC Wizard] に移動します。



2. [VPC with a Single Public Subnet]を選択します。

Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

Creates:

A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.

Select

Internet, S3, DynamoDB, SNS, SQS, etc.

Public Subnet

Amazon Virtual Private Cloud

3. VPCを作成すると、自由に使用する/16ネットワークが割り当てられます。

4. また、/24パブリックサブネットが割り当てられています。パブリックサブネットインスタンスは、デバイスがインターネットにアクセスするためにElastic IPまたはパブリックIPを使用します。

Step 2: VPC with a Single Public Subnet

IPv4 CIDR block* 10.16.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: No IPv6 CIDR Block
 Amazon provided IPv6 CIDR block

VPC name: HA

Public subnet's IPv4 CIDR* 10.16.0.0/24 (251 IP addresses available)

Availability Zone* No Preference

Subnet name: Public subnet

You can add more subnets after AWS creates the VPC.

Service endpoints
Add Endpoint

Enable DNS hostnames* Yes No

Hardware tenancy* Default

Cancel and Exit Back **Create VPC**

5. vpc-b98d8ec0が作成されます。

VPC Dashboard

Filter by VPC:
Select a VPC

Virtual Private Cloud

Your VPCs

Create VPC Actions

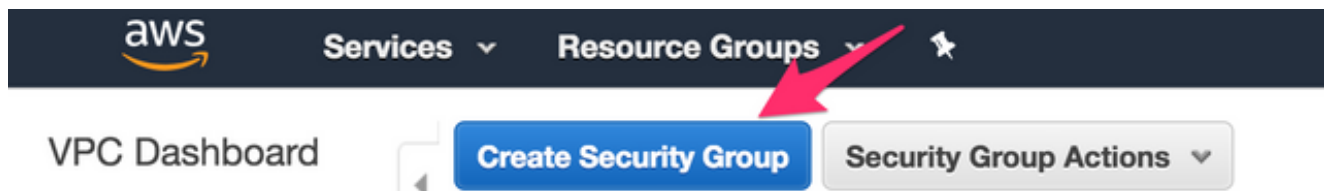
Search VPCs and their proper X

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR
<input type="checkbox"/>	HA	vpc-b98d8ec0	available	10.16.0.0/16

ステップ3:VPCのセキュリティグループを作成します。

セキュリティグループは、トラフィックを許可または拒否するACLのようなものです。

1. Securityの下でSecurity Groupsをクリックし、上記で作成したHAという名前のVPCに関連付けられたCreate your Security Groupをクリックします。



2. [Inbound Rules]で、sg-1cf47d6dに許可するトラフィックを定義します。この例では、[All Traffic]を許可します。

sg-1cf47d6d | HA

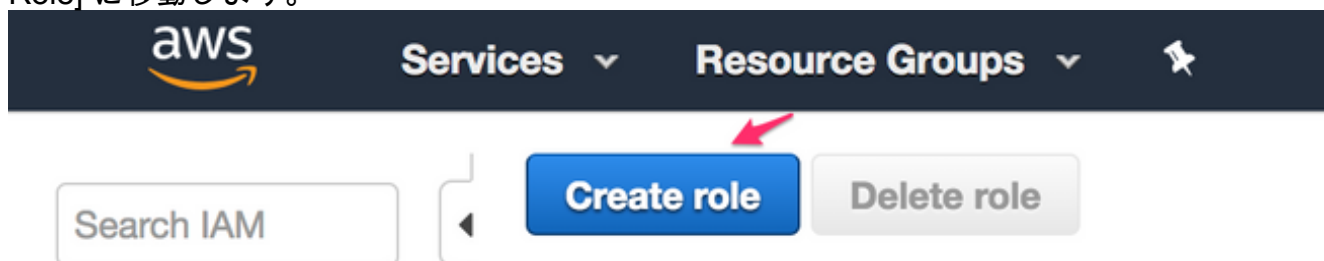


ステップ4：ポリシーを使用してIAMロールを作成し、VPCに関連付けます。

IAMはAmazon APIへのCSRアクセスを許可します。

CSR1000vは、AWS APIコマンドを呼び出して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、AMIはAPIにアクセスできません。この手順ではIAMロールを作成し、このロールはCSRインスタンスの起動時に使用されます。IAMは、CSRがAWS APIを使用および変更するためのアクセス認証情報を提供します。

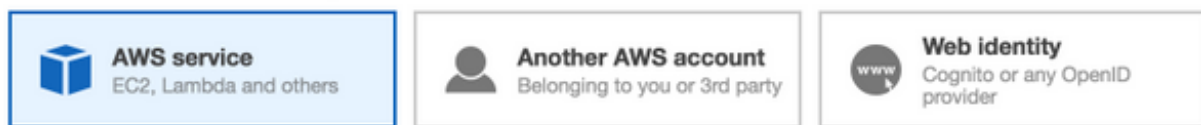
1. IAMロールを作成します。図に示すように、IAMダッシュボードを参照し、[Roles] > [Create Role] に移動します。



2. 図に示すように、代わりにEC2インスタンスがAWSを呼び出すことを許可します。

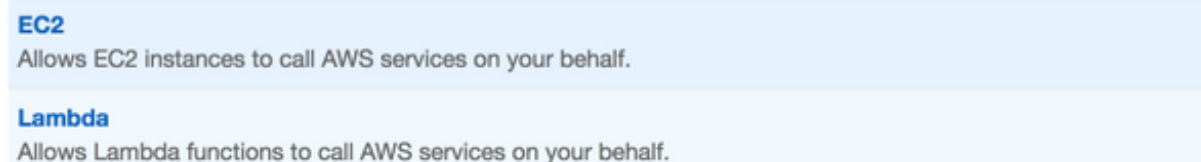
Create role

Select type of trusted entity



Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role



3. ロールを作成し、[Next] をクリックします。図に示すように、確認します。

Create role

Attach permissions policies

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

Create policy Refresh

Filter: Policy type Search Showing 394 results

	Policy name	Attachments	Description
<input type="checkbox"/>	AdministratorAccess	7	Provides full access to AWS services and resources.
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	0	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessFullAccess	0	Grants full access to AlexaForBusiness resources and acces...
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	0	Provide gateway execution access to AlexaForBusiness serv...
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	0	Provide read only access to AlexaForBusiness services
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	0	Provides full access to create/edit/delete APIs in Amazon AP...
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	0	Provides full access to invoke APIs in Amazon API Gateway.
<input type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	0	Allows API Gateway to push logs to user's account.
<input type="checkbox"/>	AmazonAppStreamFullAccess	0	Provides full access to Amazon AppStream via the AWS Ma...
<input type="checkbox"/>	AmazonAppStreamReadOnlyAccess	0	Provides read only access to Amazon AppStream via the AW...
<input type="checkbox"/>	AmazonAppStreamServiceAccess	0	Default policy for Amazon AppStream service role.
<input type="checkbox"/>	AmazonAthenaFullAccess	0	Provide full access to Amazon Athena and scoped access to...

* Required Cancel Previous **Next: Review**

4. ロール名を指定します。この例では、図に示すように、ロール名はroutetablechangeです。

Create role

Review

Provide the required information below and review this role before you create it.

Role name* routetablechange

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

5. 次に、ポリシーを作成し、上で作成したロールに適用する必要があります。IAMダッシュボードで、[ポリシー(Policies)] > [ポリシーの作成(Create Policy)] に移動します。

aws Services Resource Groups

Search IAM Create policy Policy actions

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

Create policy

1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

This policy validation failed and might have errors converting to JSON: The policy must have at least one statement. For more information about the IAM policy grammar, see [AWS IAM Policies](#)

Visual editor JSON

Import managed policy

```
1- {  
2-   "Version": "2012-10-17",  
3-   "Statement": [  
4-     {  
5-       "Effect": "Allow",  
6-       "Action": [  
7-         "ec2:AssociateRouteTable",  
8-         "ec2:CreateRoute",  
9-         "ec2:CreateRouteTable",  
10-        "ec2>DeleteRoute",  
11-        "ec2>DeleteRouteTable",  
12-        "ec2:DescribeRouteTables",  
13-        "ec2:DescribeVpcs",  
14-        "ec2:ReplaceRoute",  
15-        "ec2:DisassociateRouteTable".
```

6. ポリシー名を指定し、作成したロールに関連付けます。この例では、図に示すように、ポリシー名はCSRHA with Administrator Accessです。

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with 'Policies' selected. The main content area displays a green success message: 'CSRHA has been created.' Below this, there are buttons for 'Create policy' and 'Policy actions'. The 'Policy actions' dropdown menu is open, showing options for 'Attach', 'Detach', and 'Delete'. A red arrow points to the 'Attach' option. Below the menu, a table lists policies, with 'AdministratorAccess' highlighted in blue. The table has columns for 'Policy' and 'Type', with 'Job function' listed under 'Type'.

7. 図に示すように、作成したroutetablechangeというロールにポリシーを割り当てます。

Attach Policy

Attach the policy to users, groups, or roles in your account.

The screenshot shows the 'Attach Policy' page in the AWS IAM console. At the top, there is a search bar with the text 'routetablechange'. Below the search bar, there is a table of policies. The first row is 'adikaulroutetablechange' with an unchecked checkbox. The second row is 'routetablechange' with a checked checkbox. A red arrow points to the 'routetablechange' row.

8. サマリー。

Summary

Delete role

Role ARN	arn:aws:iam::936821026322:role/routetablechange ↗
Role description	Allows EC2 instances to call AWS services on your behalf. Edit
Instance Profile ARNs	arn:aws:iam::936821026322:instance-profile/routetablechange ↗
Path	/
Creation time	2018-06-02 10:29 PDT
Maximum CLI/API session duration	1 hour (3,600 seconds) Edit

Permissions Trust relationships Access Advisor Revoke sessions

[Attach policy](#) Attached policies: 1

Policy name	Policy type
CSR1A	Managed policy

Policy summary [JSON] Edit policy [Simulate policy](#)

Q Filter

Service	Access level	Resource	Request condition
Allow (1 of 141 services) Show remaining 140			
EC2	Limited: List, Write	All resources	None

ステップ5：作成したAMIロールでCSR1000vを起動し、パブリック/プライベートサブネットを関連付けます。

各CSR1000v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、それぞれ独自のアベイラビリティゾーンにあります。各CSRは別々のデータセンターにあると考えることができます。

1. AWSコンソールでEC2を選択し、Launch Instanceをクリックします。

EC2 Dashboard

Events

Launch Instance

Connect

Actions

2. [AWS Marketplace]を選択します。

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: 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 in the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

My AMIs

AWS Marketplace



Amazon Linux
Free tier eligible

Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-e251209a

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

3. 「CSR1000v」と入力します。この例では、[Maximum Performance]にCisco Cloud Services Router(CSR)1000V - BYOLを使用します。

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

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.

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Categories

All Categories

Infrastructure Software (4)

Operating System

Clear Filter

All Linux/Unix

Other Linux (4)

Software Pricing Plans

Hourly (2)

Annual (2)

Bring Your Own License (2)

Search: CSR1000v

1 to 4 of 4 Products

Cisco Cloud Services Router (CSR) 1000V - AX Pkg. Max Performance

★★★★☆ (2) | 16.8.1a Previous versions | Sold by Cisco Systems, Inc.

Starting from \$0.622/hr or from \$2,233/yr (89% savings) for software + AWS usage fees

Linux/Unix, Other Cisco IOS XE | 64-bit Amazon Machine Image (AMI) | Updated: 5/31/18

The AX Technology Package for Maximum Performance version of Cisco's Cloud Services Router (CSR1000V) delivers the maximum performance available in AWS cloud for virtual ...

More info

Select

Cisco Cloud Services Router (CSR) 1000V - Security Pkg. Max Performance

★★★★☆ (3) | 16.8.1a Previous versions | Sold by Cisco Systems, Inc.

Starting from \$0.241/hr or from \$1,342/yr (89% savings) for software + AWS usage fees

Linux/Unix, Other Cisco IOS XE | 64-bit Amazon Machine Image (AMI) | Updated: 5/31/18

The Security Technology Package for Maximum Performance version of Cisco Cloud Services Router (CSR1000V) delivers the maximum VPN/firewall performance in the AWS cloud, by using ...

More info

Select

Cisco Cloud Services Router (CSR) 1000V - BYOL for Maximum Performance

★★★★☆ (1) | 16.8.1a Previous versions | Sold by Cisco Systems, Inc.

Bring Your Own License + AWS usage fees

Select

4. インスタンスタイプを選択します。この例では、選択されているタイプはt2.mediumです。

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.medium (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 4 GiB memory, EBS only)

Note: The vendor recommends using a c4.large instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
⊗	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
⊗	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
⊗	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
⊗	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

5. インスタンスが設定されている間は、上記で作成したVPCと上記のIAMロールを選択する必要があります。さらに、プライベート側インターフェイスに関連付けるプライベートサブネットを作成します。

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: Request Spot Instances

Network: vpc-a6fedef | HA Create new VPC

No default VPC found. Create a new default VPC.

Subnet: subnet-66f7931f | Public subnet | us-west-2a Create new subnet

251 IP Addresses available

Auto-assign Public IP: Use subnet setting (Disable)

Placement group: Add instance to placement group

IAM role: routetablechange Create new IAM role

Shutdown behavior: Stop

Enable termination protection: Protect against accidental termination

Monitoring: Enable CloudWatch detailed monitoring Additional charges apply.

6. [Create new Subnet for Private Subnet]をクリックします。この例では、NameタグはHA Privateです。パブリックサブネットと同じアベイラビリティゾーンにあることを確認します。

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: HA Private

VPC: vpc-a6fefedf | HA

VPC CIDRs	CIDR	Status	Status Reason
	10.16.0.0/16	associated	

Availability Zone: us-west-2a

IPv4 CIDR block: 10.16.4.0/24

Buttons: Cancel, Yes, Create

7. 下にスクロールし、[Configure Instance Details]で[Add Device] をクリックします (図を参照)。

1. Choose AMI 2. Choose Instance Type 3. Configure Instance Type 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-66f7931f	Auto-assign	Add IP	

Add Device

8. セカンダリインターフェイスを追加した後、作成したプライベートサブネット (HAプライベート) を関連付けます。Eth0はパブリック側、Eth1はプライベート側のインターフェイスです。注：前の手順で作成したサブネットは、このドロップダウンに表示されないことがあります。サブネットを表示するには、ページを更新またはキャンセルして再起動する必要があります。

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-66f7931f	Auto-assign	Add IP	
eth1	New network interface	subnet-89c5a1f0 (HA Private) 10.16.4.0/24 us-west-2a			

9. VPCで作成したセキュリティグループを選択し、ルールが正しく定義されていることを確認します。

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group: Create a new security group
 Select an existing security group

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-01880170	default	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-1cf47d6d	HA	HA	Copy to new

10. 新しいキーペアを作成し、秘密キーをダウンロードします。デバイスごとに1つのキーを再利用できます。 注：秘密キーを紛失すると、CSRに再びログインできなくなります。キーを回復する方法はありません。

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

Create a new key pair

Key pair name
 CSRHA

[Download Key Pair](#)

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

[Cancel](#) [Launch Instances](#)

11. 作成したインスタンスのパブリックインターフェイスのENIにElastic IPを関連付け、[AWS console] > [EC2 Management] > [Network Security] > [Elastic IP's] に移動します。 注：パブリック/プライベートの用語は、ここで混乱を招く可能性があります。この例では、パブリックインターフェイスの定義は、インターネットに面したインターフェイスである Eth0です。AWSの観点から見ると、パブリックインターフェイスはプライベートIPです。

EC2 Dashboard

Events

[Allocate new address](#)

[Actions](#)

Associate address

Select the instance OR network interface to which you want to associate this Elastic IP address (54.244.108.43)

Resource type Instance Network interface

Network interface: eni-2515633d

Private IP: 10.16.2.215

Reassociation Allow Elastic IP to be reassociated if already attached

Warning
If you associate an Elastic IP address with your instance, your current public IP address is released. [Learn more.](#)

AWS Command Line Interface command

Cancel **Associate**

12. [EC2] > [Network Interfaces] に移動するときに、[Source/Dest Check]を無効にします。各 ENIの送信元/宛先チェックを確認します。デフォルトでは、すべてのENIは、この Source/Destチェックが有効になっています。アンチスプーフィング機能は、ENIがトラフィックを転送する前にトラフィックの宛先であることを確認することによって、ENIが実際には意図されていないトラフィックによってオーバーランすることを回避することを意味しました。ルータがパケットの実際の宛先であることはほとんどありません。この機能は、すべてのCSR中継ENIで無効にする必要があります。無効にしないと、パケットを転送できません。

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with 'INSTANCES' expanded. The main area shows a table of Network Interfaces. A red arrow points to the 'eni-10e3a018' entry. A modal dialog titled 'Change Source/Dest. Check' is open, showing the 'Source/dest. check' option set to 'Disabled' (indicated by a red arrow).

Name	Network interf.	Subnet ID	VPC
<input checked="" type="checkbox"/>	eni-10e3a018	subnet-b7890ffc	vpc-

Change Source/Dest. Check

Network Interface eni-10e3a018

Source/dest. check Enabled Disabled

Cancel Save

13. CSR1000vに接続します。注：AWSがCSR1000vにSSHで提供したユーザ名が、rootとして誤ってリストされる場合があります。必要に応じて、これをec2-userに変更します。注：SSHでDNSアドレスにpingできる必要があります。ec2-54-208-234-64.compute-1.amazonaws.comです。ルータのパブリックサブネット/eniがパブリックルートテーブルに関連付けられていることを確認します。サブネットをルートテーブルに関連付ける方法については、ステップ8に進みます。

Connect To Your Instance



I would like to connect with

A standalone SSH client

A Java SSH Client directly from my browser (Java required)

To access your instance:

1. Open an SSH client. (find out how to [connect using PuTTY](#))
2. Locate your private key file (HA.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:

```
chmod 400 HA.pem
```

4. Connect to your instance using its Public DNS:

```
ec2-54-208-234-64.compute-1.amazonaws.com
```

Example:

```
ssh -i "HA.pem" root@ec2-54-208-234-64.compute-1.amazonaws.com
```

Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

Close

ステップ6 : ステップ5を繰り返し、HA用に2番目のCSR1000vインスタンスを作成します。

パブリックサブネット : 10.16.1.0/24

プライベートサブネット : 10.16.5.0/24

この新しいAMIのelastic ipアドレスにpingできない場合は、手順8に進んで、パブリックサブネットがパブリックルートテーブルに関連付けられていることを確認します。

ステップ7 : ステップ5を繰り返し、AMI MarketplaceからVM(Linux/Windows)を作成します。

この例では、MarketplaceでUbuntu Server 14.04 LTSを使用します。

パブリックサブネット : 10.16.2.0/24

プライベートサブネット : 10.16.6.0/24

この新しいAMIのelastic ipアドレスにpingできない場合は、手順8に進んで、パブリックサブネットがパブリックルートテーブルに関連付けられていることを確認します。

1. Eth0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。プライベートサブネット用にeth1という名前の2番目のインターフェイスを作成します。

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, and NETWORK & SECURITY. The main area displays a list of EC2 instances. One instance, 'Ubuntu' (ID: i-06bde41d88d997bcb), is selected. Below the list, a modal window titled 'Network Interface eth1' is open, showing details for the interface eni-396142ae. A red arrow points to the 'Delete on Terminate' field, which is set to 'false'.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
Ubuntu	i-06bde41d88d997bcb	m1.small	us-east-1d	running	2/2 checks ...
HA	i-0fcb4929f681a	t2.medium	us-east-1a	running	2/2 checks ...

Instance ID	Instance state	Instance type	Elastic IPs	Availability zone	Security groups	Scheduled events	AMI ID	Platform	Public DNS (IPv4)
i-06bde41d88d997bcb	running	m1.small	52.6.211.67	us-east-1d	sg-4a5b5390	None	ubuntu-ssd-ami-20180531	-	ec2-52-6-211-67.com

Field	Value
Interface ID	eni-396142ae
VPC ID	vpc-eb5e5390
Attachment Owner	936821026322
Attachment Status	attached
Attachment Time	Thu May 31 22:06:14 GMT-700 2018
Delete on Terminate	false
Private IP Address	10.16.6.131
Private DNS Name	ip-10-16-6-131.ec2.internal
Elastic IP Address	-
Source/Dest. Check	true
Description	-
Security Groups	default

2. Ubuntuで設定するIPアドレスは、AWSによって割り当てられたeth1プライベートインターフェイスです。

```
ubuntu@ip-10-16-2-139:~$ cd /etc/network/interfaces.d/
```

```
ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo vi eth1.cfg
```

```
auto eth1
iface eth1 inet static
    address 10.16.6.131
    netmask 255.255.255.0
    network 10.16.6.0
up route add -host 8.8.8.8 gw 10.16.6.1 dev eth1
```

3. インターフェイスをフラップするか、VMをリブートします。

```
ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo ifdown eth1 && sudo ifup eth1
```

```
ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo reboot
```

4. テストのために8.8.8.8をpingします。8.8.8.8ルートがステップ7ごとに追加されていることを確認します。

```
ubuntu@ip-10-16-2-139:~$ route -n
```

```
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.16.2.1 0.0.0.0 UG 0 0 0 eth0
8.8.8.8 10.16.6.1 255.255.255.255 UGH 0 0 0 eth1 <-----
10.16.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.16.6.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
```

8.8.8.8が表に記載されていない場合は、手動で追加します。

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

ステップ8 : プライベートおよびパブリックルートテーブルを設定します。

1. ステップ2のウィザードでVPCを作成すると、2つのルートテーブルが自動的に作成されます。ルートテーブルが1つしかない場合は、図に示すように、プライベートサブネット用に別のルートテーブルを作成します。

The screenshot shows the AWS Management Console interface for Route Tables. The top navigation bar includes 'Services' and 'Resource Groups'. The left sidebar shows the 'VPC Dashboard' and 'Virtual Private Cloud' sections. The main content area displays the 'Create Route Table' dialog box, which is open. The dialog box has a title 'Create Route Table' and a close button. Below the title, there is a description: 'A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.' The 'Name tag' field is set to 'HA PRIVATE' and the 'VPC' dropdown is set to 'vpc-b98d8ec0 | HA'. There are 'Cancel' and 'Yes, Create' buttons at the bottom right of the dialog.

Below the dialog, the 'Route Tables' list is visible. It has a search bar and a table with the following columns: 'Name', 'Route Table ID', 'Explicitly Associat', 'Main', and 'VPC'. The table contains two entries:

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associat	Main	VPC
<input type="checkbox"/>	HA PUBLIC	rtb-2752415f	1 Subnet	No	vpc-39222f40 HA
<input checked="" type="checkbox"/>	HA PRIVATE	rtb-ca5340b2	0 Subnets	Yes	vpc-39222f40 HA

A red arrow points to the 'HA PRIVATE' row. Below the table, the details for the selected route table 'rtb-ca5340b2 | HA PRIVATE' are shown. There are tabs for 'Summary', 'Routes', 'Subnet Associations', 'Route Propagation', and 'Tags'. The 'Routes' tab is selected. There is an 'Edit' button and a 'View' dropdown set to 'All rules'. Below this is a table of routes:

Destination	Target	Status	Propagated
10.16.0.0/16	local	Active	No

A red arrow points to the 'Edit' button.

2. 2つのルートテーブルのビューを次に示します。PUBLICルートテーブルには、インターネットゲートウェイ(igw-95377973)が自動的に接続されます。2つのテーブルにラベルを付けます。PRIVATEテーブルにはこのルートを含めることはできません。

VPC Dashboard

Filter by VPC:

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Security

Network ACLs

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associat	Main	VPC
<input checked="" type="checkbox"/>	HA PUBLIC	rtb-2752415f	1 Subnet	No	vpc-39222f40 HA
<input type="checkbox"/>	HA PRIVATE	rtb-ca5340b2	0 Subnets	Yes	vpc-39222f40 HA

rtb-2752415f | HA PUBLIC

Summary Routes Subnet Associations Route Propagation Tags

Edit

View: All rules

Destination	Target	Status	Propagated
10.16.0.0/16	local	Active	No
0.0.0.0/0	igw-953779f3	Active	No

3. 6つのサブネットすべてを適切なルートテーブルに関連付けます 3パブリックインターフェイスは、パブリックルートテーブルに関連付けられています。パブリックサブネット : 10.16.0.0/24, 10.16.1.0/24, 10.16.2.0/24 3プライベートインターフェイスはプライベートルートテーブルに関連付けられます。プライベートサブネット : 10.16.4.0/24, 10.16.5.0/24, 10.16.6.0/24

rtb-ec081d94 | HA PRIVATE

Summary Routes **Subnet Associations** Route Propagation Tags

Edit

Subnet	IPv4 CIDR	IPv6 CIDR
You do not have any subnet associations. The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:		

手順9: BFDと任意のルーティングプロトコルを使用して、ネットワークアドレス変換(NAT)とGREトンネルを設定します。

CSR 1000vのElastic IPを介してGeneric Routing Encapsulation(GRE)トンネルを設定します (誤った障害を検出するDHCPリース更新の問題を回避するために推奨されます)。高速コンバージェンスが必要な場合は、双方向フォワーディング検出(BFD)値を、この例に示す値よりもアグレッシブに設定できます。ただし、これが原因で、断続的な接続中にBFDピアダウンイベントが発生する可能性があります。この例の値は、1.5秒以内にピア障害を検出します。AWS APIコマンドが実行されてからVPCルーティングテーブルの変更が有効になるまでの間に、約20秒の可変遅延があります。

- CSRHAの設定

GREおよびBFD:HAフェールオーバーの状態を確認するために使用されます。

```
interface Tunnell
  ip address 192.168.1.1 255.255.255.0
  bfd interval 500 min_rx 500 multiplier 3
  tunnel source GigabitEthernet1
  tunnel destination 52.10.183.185 /* Elastic IP of the peer CSR */
!
router eigrp 1
  bfd interface Tunnell
  network 192.168.1.0
  passive-interface GigabitEthernet1
```

NATとルーティング : プライベートインターフェイスを介したVMインターネットの到達可能性に使用されます。

```
interface GigabitEthernet1
  ip address dhcp
  ip nat outside
  no shutdown
!
interface GigabitEthernet2
  ip address dhcp
  ip nat inside
  no shutdown
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!
access-list 10 permit 10.16.6.0 0.0.0.255
!
ip route 10.16.6.0 255.255.255.0 GigabitEthernet2 10.16.4.1
```

- CSRHA1の設定

GREおよびBFD:HAフェールオーバーの状態を確認するために使用されます。

```
interface Tunnell
  ip address 192.168.1.2 255.255.255.0
  bfd interval 500 min_rx 500 multiplier 3
  tunnel source GigabitEthernet1
  tunnel destination 50.112.227.77 /* Elastic IP of the peer CSR */
!
router eigrp 1
  bfd interface Tunnell
  network 192.168.1.0
  passive-interface GigabitEthernet1
```

NATとルーティング : プライベートインターフェイスを介したVMインターネットの到達可能性に使用されます。

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

```

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

```

ステップ10 : ハイアベイラビリティの設定 (Cisco IOS XE Denali 16.3.1a以降)

次に示すcloud provider awsコマンドを使用して各CSR 1000vを設定し、BFDピアダウンイベントを監視します。BFDピアダウンなどのAWS HAエラーが検出された後に、(VPC)ルートテーブルID、ネットワークインターフェイスID、およびCIDRへのルーティング変更を定義するには、このコマンドを使用します。

```

CSR(config)# redundancy
CSR(config-red)# cloud provider [aws | azure] node-id
# bfd peer ipaddr
# route-table table-name
# cidr ip ipaddr/prefix
# eni elastic-network-intf-name
# region region-name

```

1. #bfd peer ipaddrは、ピアトンネルIPアドレスです。

```
CSRHA#show bfd neighbors
```

```

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

```

2. AWSコンソール#route-tableの下にテーブル名が表示されます。[VPC] > [Route Tables] に移動します。このアクションにより、プライベートルートテーブルが変更されます。

VPC Dashboard

Filter by VPC:

Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Create Route Table Delete Route Table

Search Route Tables and their

<input type="checkbox"/>	Name	Route Table ID
<input type="checkbox"/>		rtb-7b746303
<input type="checkbox"/>	HA PUBLIC	rtb-ab091cd3
<input type="checkbox"/>		rtb-a4495edc
<input checked="" type="checkbox"/>	HA PRIVATE	rtb-ec081d94

3. #cidr ip ipaddr/prefixは、ルートテーブルで更新されるルートの宛先アドレスです。AWSコンソールで、[VPC] > [Route Tables] に移動します。下にスクロールして[Edit] をクリックし、[Add another route] をクリックします。8.8.8.8のテスト宛先アドレスとCSRHAのプライベートENIを追加します。

rtb-ec081d94 | HA PRIVATE

Summary Routes Subnet Associations Route Propagation Tags

Edit

rtb-ec081d94 | HA PRIVATE

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

View: All rules

Destination	Target	Status	Propagated	Remove
10.16.0.0/16	local	Active	No	
8.8.8.8/32	eni-10e3a018	Active	No	✕

Add another route

4. #eni elastic-network-intf-nameがEC2インスタンスで見つかりました。対応する各CSRのプライベート側インターフェイスeth1をクリックし、インターフェイスIDを使用します。

Instances

Instance Name	Instance ID	Instance Type	Availability Zone	State	Health
CSRHA	i-0223f5ca1d6068424	c4.large	us-west-2a	running	2/2 checks ...
CSRHA1	i-0bed9ff2bd6996ca4	t2.medium	us-west-2b	running	2/2 checks ...
WINDOWS	i-07a0fecde36302c6a	t2.small	us-west-2c	running	2/2 checks ...

Instance: i-0223f5ca1d6068424 (CSRHA) Elastic Network Interfaces

Interface ID	Private IP Address
eni-90b500a8	10.16.4.198

Network interfaces: eth0, eth1

5. 名前は#regionAWSドキュメント内で見つかったコード名です。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。最新のアップデートについては、Amazonの[Region and Availability Zones](#)ドキュメントをご覧ください。

Code	Name
us-east-1	US East (N. Virginia)
us-east-2	US East (Ohio)
us-west-1	US West (N. California)
us-west-2	US West (Oregon)
ca-central-1	Canada (Central)
eu-central-1	EU (Frankfurt)
eu-west-1	EU (Ireland)
eu-west-2	EU (London)
eu-west-3	EU (Paris)
ap-northeast-1	Asia Pacific (Tokyo)
ap-northeast-2	Asia Pacific (Seoul)
ap-northeast-3	Asia Pacific (Osaka-Local)
ap-southeast-1	Asia Pacific (Singapore)
ap-southeast-2	Asia Pacific (Sydney)
ap-south-1	Asia Pacific (Mumbai)
sa-east-1	South America (São Paulo)

CSRHAの冗長性の設定例

```

redundancy
cloud provider aws 1
  bfd peer 192.168.1.2
  route-table rtb-ec081d94
  cidr ip 8.8.8.8/32
  eni eni-90b500a8
  region us-west-2

```

CSRHA1の冗長性の設定例

```

redundancy
cloud provider aws 1
  bfd peer 192.168.1.1
  route-table rtb-ec081d94
  cidr ip 8.8.8.8/32
  eni eni-10e3a018
  region us-west-2

```


ハイアベイラビリティの確認

1. BFDとクラウドの設定を確認します。

```
CSRHA#show bfd nei
```

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

```
CSRHA#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.2 Tu1 12 00:11:57 1 1470 0 2
```

```
CSRHA#show redundancy cloud provider aws 1
```

```
Cloud HA: work_in_progress=FALSE
Provider : AWS node 1
State : idle
BFD peer      = 192.168.1.2
BFD intf      = Tunnel1
route-table   = rtb-ec081d94
cidr          = 8.8.8.8/32
eni           = eni-90b500a8
region       = us-west-2
```

2. VMから宛先に連続してpingを実行します。pingがプライベートeth1インターフェイスを経由していることを確認します。

```
ubuntu@ip-10-16-3-139:~$ ping -I eth1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 10.16.6.131 eth1: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=50 time=1.60 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=50 time=1.62 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=50 time=1.57 ms
```

3. プライベートルートテーブルを確認します。eniは現在、これがトラフィックであるCSRHAのプライベートインターフェイスです。

rtb-ec081d94 | HA PRIVATE

Summary	Routes	Subnet Associations	Route Propagation	Tags
Edit				
View: <input type="text" value="All rules"/>				
Destination	Target	Status	Propagated	
10.16.0.0/16	local	Active	No	
8.8.8.8/32	eni-90b500a8 / i-0fcfceb4f929f681a	Active	No	

4. CSRHAのTunnel1をシャットダウンして、HAフェールオーバーをシミュレートします。

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

5. ルートテーブルがCSRHA1のプライベートインターフェイスである新しいENIを指していることを確認します。

Summary

Routes

Subnet Associations

Route Propagation

Tags

Edit

View: All rules

Destination	Target	Status	Propagated
10.16.0.0/16	local	Active	No
8.8.8.8/32	eni-10e3a018 / i-0fcfcecb4f929f681a	Active	No

トラブルシューティング

- 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場合、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ていること、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ごとにSource/Destチェックを無効にします。
- Cisco IOS XE 16.3.1a以降では、次の追加の検証コマンドを使用できます。

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

- デバッグでよく見られる障害を次に示します。

問題：httpc_send_requestが失敗しました

解決策：Httpは、CSRからAWSにAPIコールを送信するために使用されます。DNSがインスタンスにリストされているDNS名を解決できることを確認します。HTTPトラフィックがブロックされていないことを確認します。

```
*May 30 20:08:06.922: %VXE_CLOUD_HA-3-FAILED: VXE Cloud HA BFD state transitioned, AWS node 1
event httpc_send_request failed
*May 30 20:08:06.922: CLOUD-HA : AWS node 1 httpc_send_request failed (0x12)
URL=http://ec2.us-east-2b.amazonaws.com
```

問題：ルートテーブルrtb-9c0000f4とインターフェイスeni-32791318が異なるネットワークに属している

解決策：リージョン名とENIが異なるネットワークで誤って設定されている。リージョンとENIは

、ルータと同じゾーンに存在する必要があります。

```
*May 30 23:38:09.141: CLOUD-HA : res content iov_len=284 iov_base=<?xml version="1.0"
encoding="UTF-8"?>
<Response><Errors><Error><Code>InvalidParameterValue</Code><Message>route table rtb-9c0000f4 and
interface eni-32791318 belong to different
networks</Message></Error></Errors><RequestID>af3f228c-d5d8-4b23-b22c-
f6ad999e70bd</RequestID></Response>
```

問題：この操作を実行する権限がありません。Encoded Authorization Failureメッセージ。

解決策： IAM JSONロール/ポリシーが正しく作成されていないか、CSRに適用されていません。IAMロールは、CSRがAPI呼び出しを実行することを許可します。

```
*May 30 22:22:46.437: CLOUD-HA : res content iov_len=895 iov_base=<?xml version="1.0"
encoding="UTF-8"?>
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not authorized to
perform this operation. Encoded
authorization failure message: qYvEB4MUdOB8m2itSteRgnOuslAaxhAbDph5qGRJkjjJbrESajbmF5HWUR-
MmHYeRALpKZ3Jg_y-
_tMlYe15l_ws8Jd9q2W8YDXBl3uXQqfW_cjjrgy9jhnGY0nOaNu65aLpfqui8kS_4RPOpm5grRFfo99-
8uv_N3mYaBqKFPn3vUcSYKBmxFIikJKc jY9esOeLIOWDcnYGGu6AGGMoMxWDtk0K8nwk4IjLDcnd2cDXeENS45w1PqzKGPsh
v3wD28TS5xRjIrPXyRt18UpV6lLA_09Oh4737VncQKfzbz4tPpnAkoW0mJLQ1vDpPmNvHUpEng8KrGWYNfbfemoDtWqIdABf
aLLm4saNtnQ_OMBOTi4toBLEb2BNdMkl1UVBIxqTqdFUVRs**MSG 00041 TRUNCATED** **MSG 00041
CONTINUATION
#01**qLosAb5Yx0DrOsLSQwzS95VGvQM_n87LBHYbAWWhqWj3UfP_zmiak7d1m9P41mFCucEB3Cs4FRsFtb-
9q44VtyQJaS2sU2nhGe3x4uGEsl7F1pNv5vhVeYOZB3tbOfbV1_Y4trZwYPPfGkGShZp-WNmUKUJskc1-
6KGqmp7519imvh66Jgwgmu9DT_qAZ-jEjkwjBrxg6krw</Message></Error></Errors><RequestID>4cf31249-
2a6e-4414-ae8d-6fb825b0f398</RequestID></Response>
```

関連情報

- [VPCゲートウェイの冗長性 – Cisco](#)
- [アマゾンウェブサービス向けCisco CSR 1000vシリーズクラウドサービスルータ導入ガイド](#)
- [インスタンスタイプの細分化](#)
- [EC2およびVPC](#)
- [EC2ユーザガイドのElastic Network Interfacesには、インスタンスタイプごとのENIの数が含まれています](#)
- [LinuxでのEnhanced Networkingの使い方、役立つ背景情報](#)
- [専用インスタンス/テナントの説明と操作方法](#)
- [一般的なEC2ドキュメント](#)
- [一般的なVPCドキュメント](#)
- [リージョンとアベイラビリティゾーン](#)
- [CSR1000v高可用性バージョン3](#)

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。