AWS MarketplaceによるISE 3.1の設定

内容

概要

このドキュメントでは、Amazon Web Services(AWS)のAmazon Machine Images(AMI)を介してIdentity Services Engine(ISE)3.1をインストールする方法について説明します。 バージョン3.1以降のISEは、CloudFormationテンプレート(CFT)の助けを借りて、Amazon Elastic Compute Cloud(EC2)インスタンスとして展開できます。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- ISE

- AWSと、VPC、EC2、CloudFormationなどの概念

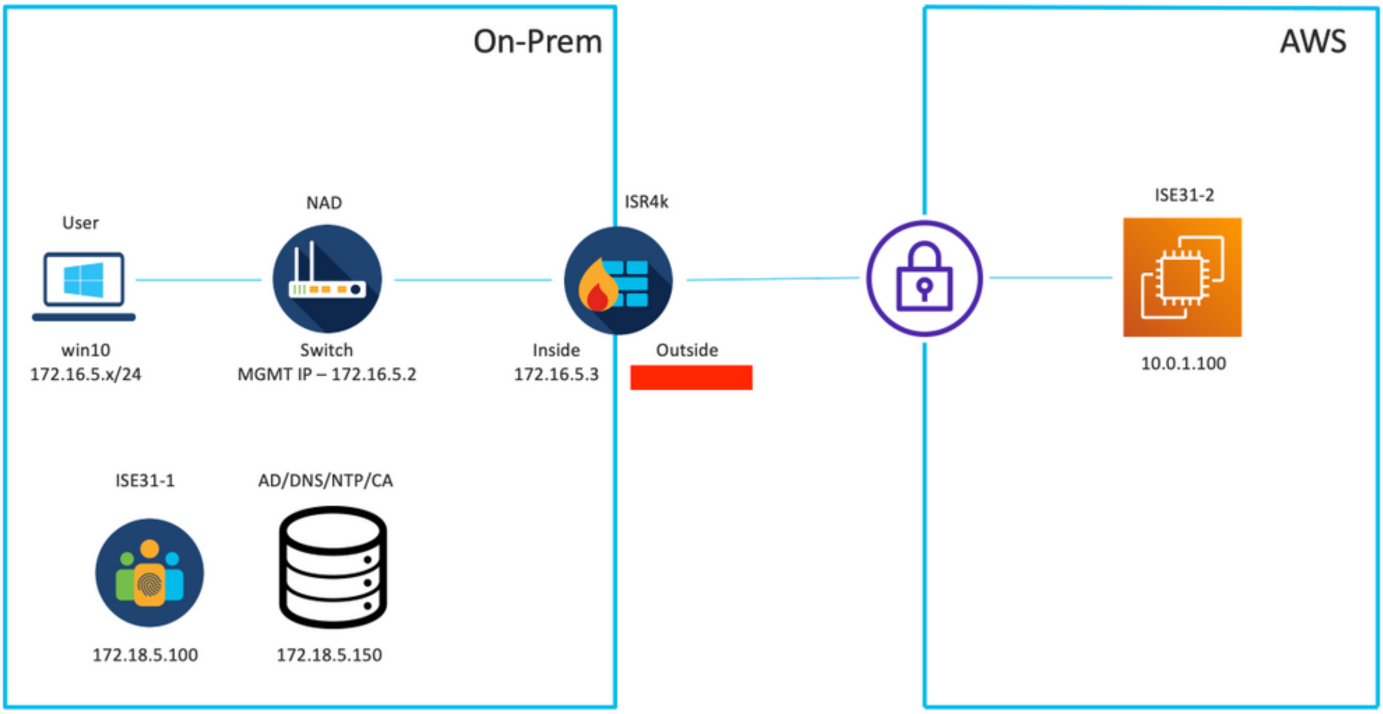
使用するコンポーネント

このドキュメントの情報は、Cisco ISEバージョン3.1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。

設定

Network Topology

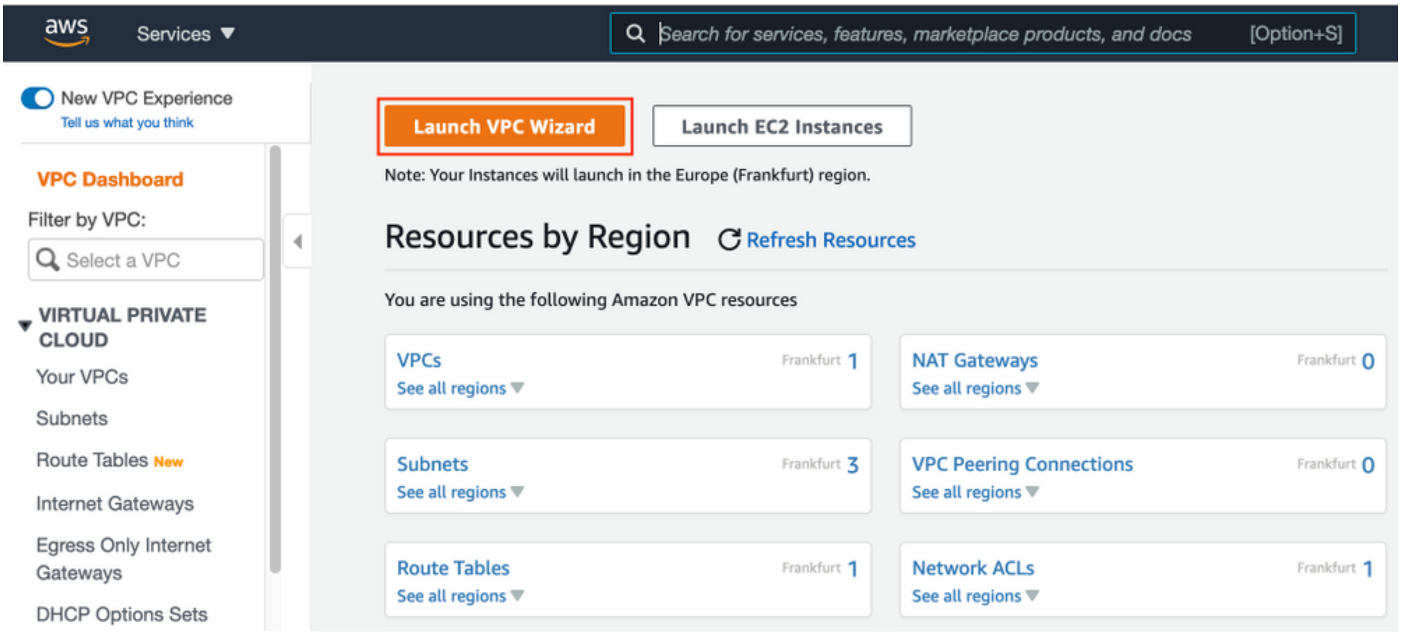


設定

VPC、セキュリティグループ、キーペア、およびVPNトンネルがまだ設定されていない場合は、オプションの手順に従う必要があります。そうでない場合は、手順1から開始します。

ステップA. VPCの作成（オプション）

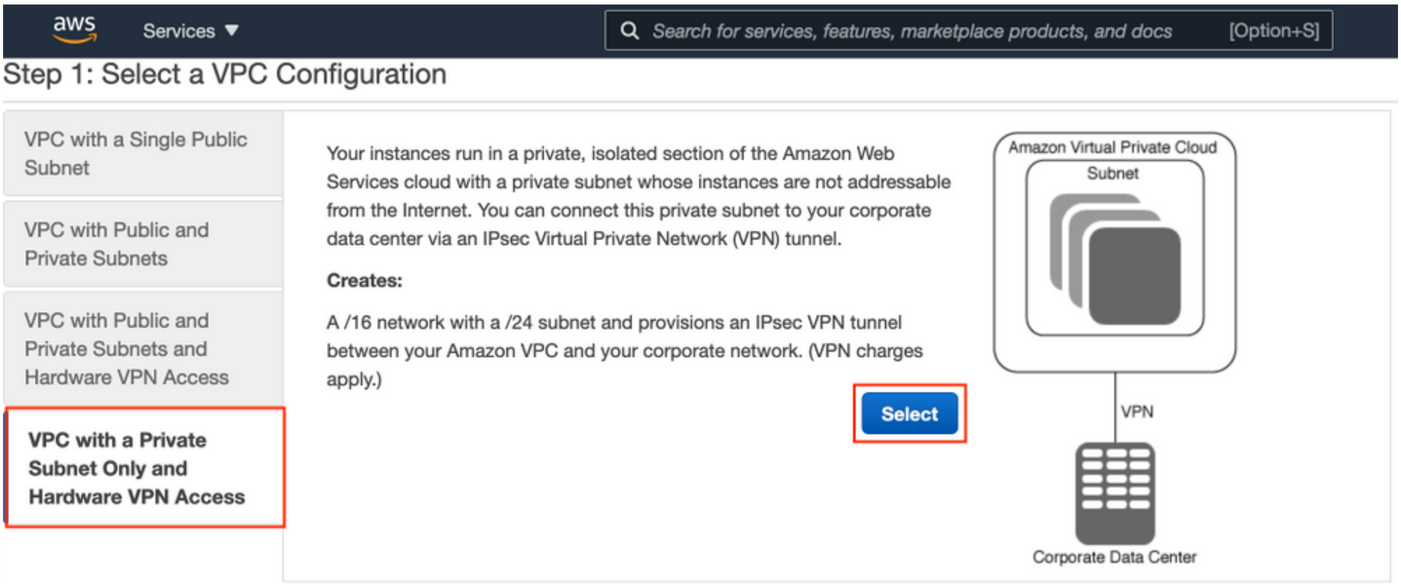
VPC AWSサービ**スに**移動します。図に示**すように、[Launch VPC Wizard]**を選択します。


aws
Services ▼
Search for services, features, marketplace products, and docs
[Option+S]
New VPC Experience
Tell us what you think
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Launch VPC Wizard
Launch EC2 Instances
Resources by Region
Refresh Resources
VPCs Frankfurt 1 See all regions ▼
NAT Gateways Frankfurt 0 See all regions ▼
Subnets Frankfurt 3 See all regions ▼
VPC Peering Connections Frankfurt 0 See all regions ▼
Route Tables Frankfurt 1 See all regions ▼
Network ACLs Frankfurt 1 See all regions ▼

Note: Your Instances will launch in the Europe (Frankfurt) region.

You are using the following Amazon VPC resources

[VPC with **Private Subnet Only and Hardware VPN Access]を選択し、図に示すように[Select]**をクリックします。


aws
Services ▼
Search for services, features, marketplace products, and docs
[Option+S]
VPC with a Single Public Subnet
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access
VPC with a Private Subnet Only and Hardware VPN Access
Select
Amazon Virtual Private Cloud
Subnet
VPN
Corporate Data Center

Step 1: Select a VPC Configuration

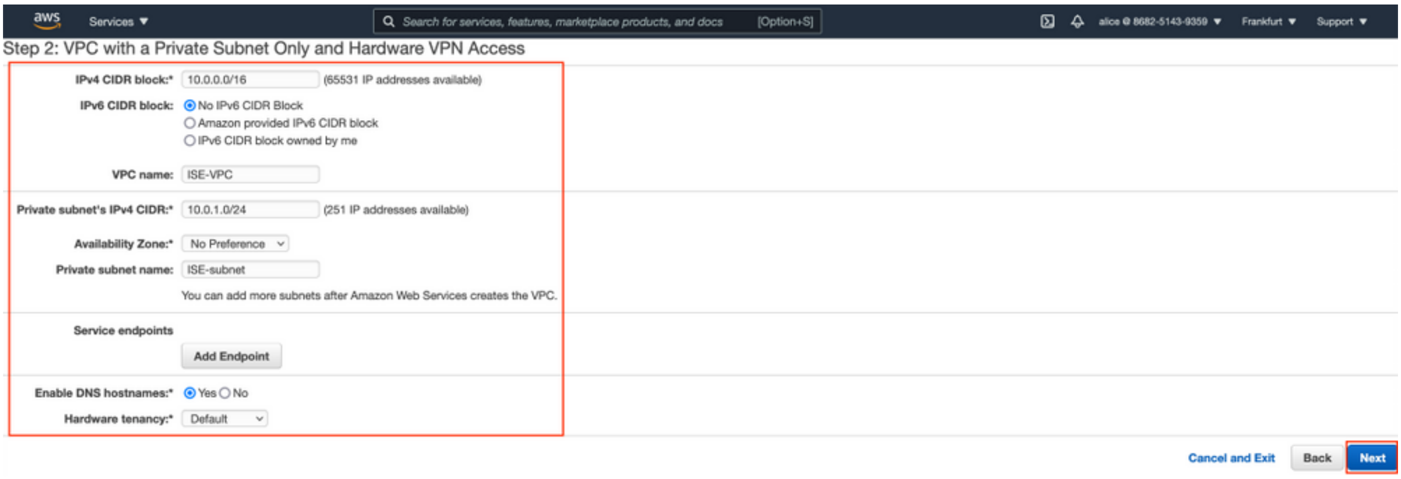
Your instances run in a private, isolated section of the Amazon Web Services cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate data center via an IPsec Virtual Private Network (VPN) tunnel.

Creates:

A /16 network with a /24 subnet and provisions an IPsec VPN tunnel between your Amazon VPC and your corporate network. (VPN charges apply.)

> **注：**VPCウィザードのステップ1.のVPCの選択は、トポロジによって異なります。これは、ISEがインターネット公開サーバとして設計されていないためです。プライベートサブネットを持つVPNのみが使用されるためです。

ネットワーク設計に従ってVPCプライベートサブネット設定を設定し、[次へ]を**選択します。**


aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
alice @ 8682-5143-9359 ▼
Frankfurt ▼
Support ▼

Step 2: VPC with a Private Subnet Only and Hardware VPN Access

IPv4 CIDR block:* 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: ● No IPv6 CIDR Block ○ Amazon provided IPv6 CIDR block ○ IPv6 CIDR block owned by me

VPC name: ISE-VPC

Private subnet's IPv4 CIDR:* 10.0.1.0/24 (251 IP addresses available)

Availability Zone:* No Preference

Private subnet name: ISE-subnet

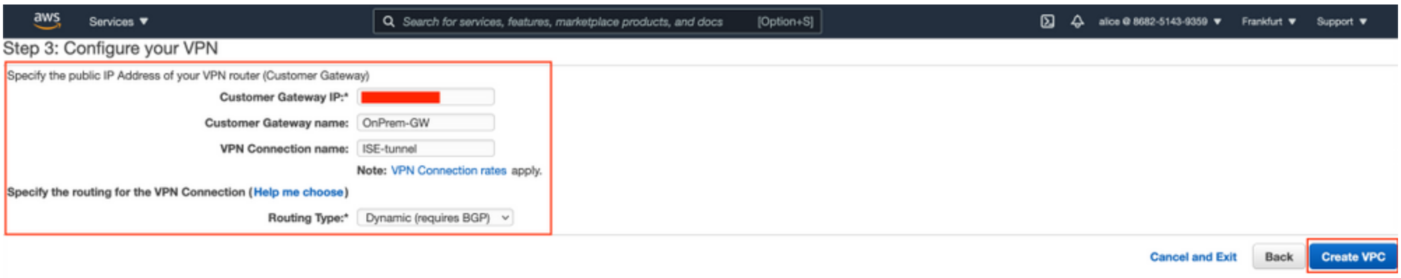
You can add more subnets after Amazon Web Services creates the VPC.

Service endpoints

Enable DNS hostnames:* ● Yes ○ No

Hardware tenancy:* Default

ネットワーク設計に従ってVPNを設定し、[Create VPC]を**選択します**。


aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
alice @ 8682-5143-9359 ▼
Frankfurt ▼
Support ▼

Step 3: Configure your VPN

Specify the public IP Address of your VPN router (Customer Gateway)

Customer Gateway IP:* [redacted]

Customer Gateway name: OnPrem-GW

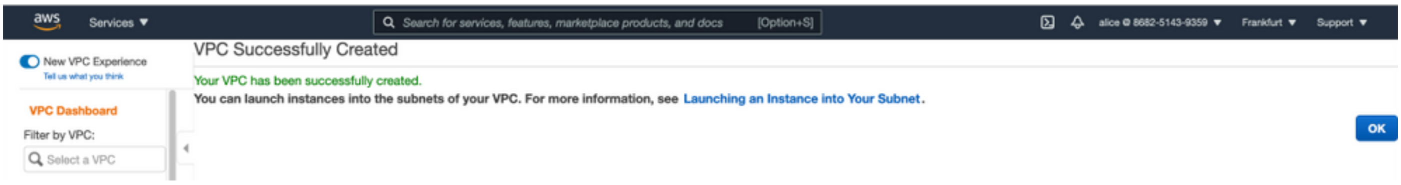
VPN Connection name: ISE-tunnel

Note: VPN Connection rates apply.

Specify the routing for the VPN Connection (Help me choose)

Routing Type:* Dynamic (requires BGP)

VPCが作成されると、「Your VPC has been successfully created」**というメッセージが表示**されます。図に示**すように**[OK]をクリックします。



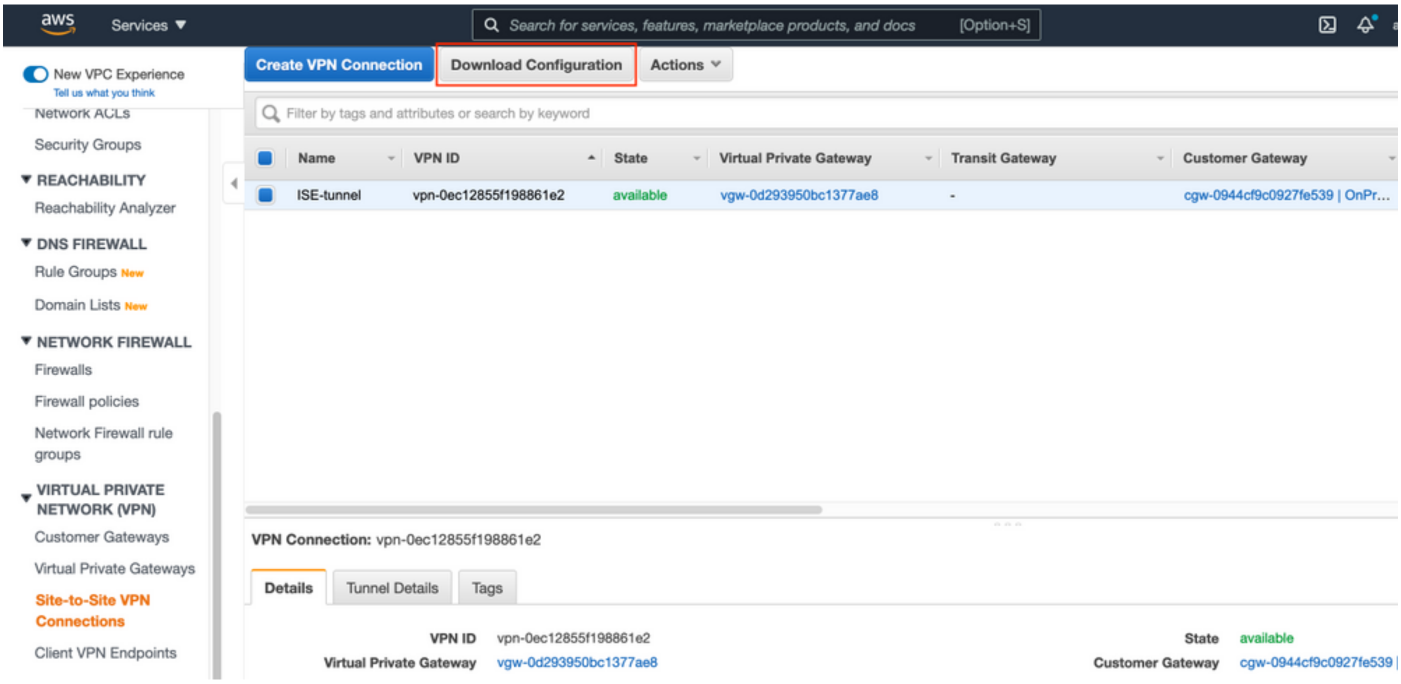
VPC Successfully Created

Your VPC has been successfully created.

You can launch instances into the subnets of your VPC. For more information, see Launching an Instance into Your Subnet.

オプションの手順B.オンプレミスVPNヘッドエンドデバイスの設定

VPC AWSサービ**スに**移動します。図に示すように**Site-to-Site VPN connectionsを選択**し、新しく作成したVPNトンネルを選択し、**Download Configuration**を選択します。



Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway
ISE-tunnel	vpn-0ec12855f198861e2	available	vgw-0d293950bc1377ae8	-	cgw-0944cf9c0927fe539 | OnPr...

VPN Connection: vpn-0ec12855f198861e2

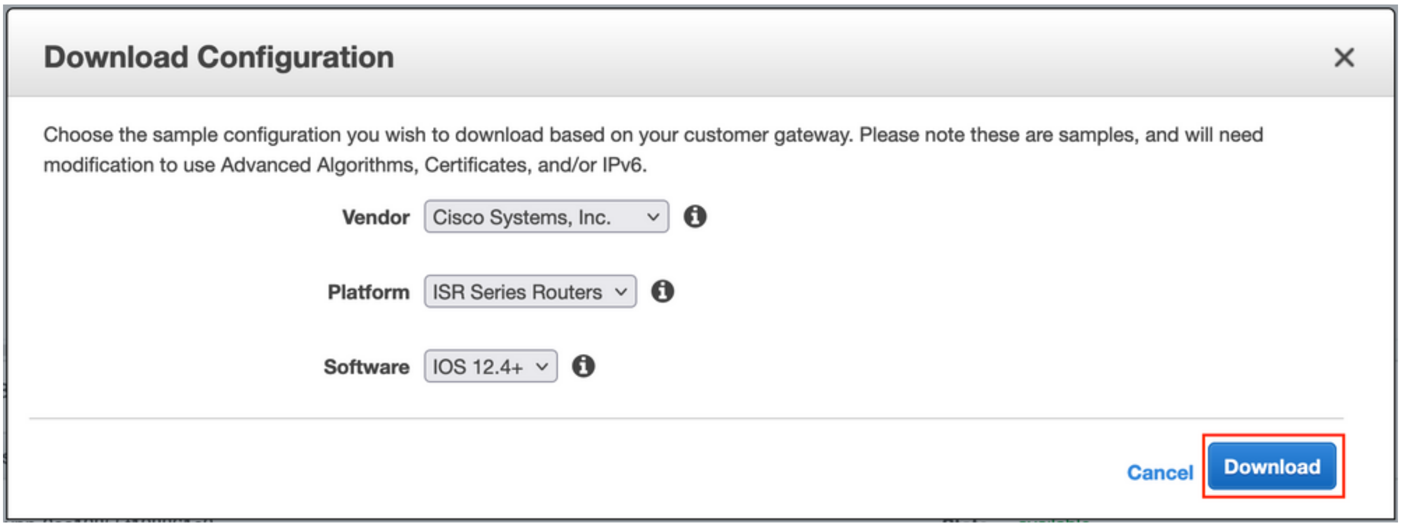
VPN ID vpn-0ec12855f198861e2

Virtual Private Gateway vgw-0d293950bc1377ae8

State available

Customer Gateway cgw-0944cf9c0927fe539 |

図に示すように、[Vendor] 、[Platform] および[Software] を選択し、[Download] を選択します。



Download Configuration

Choose the sample configuration you wish to download based on your customer gateway. Please note these are samples, and will need modification to use Advanced Algorithms, Certificates, and/or IPv6.

Vendor: Cisco Systems, Inc.

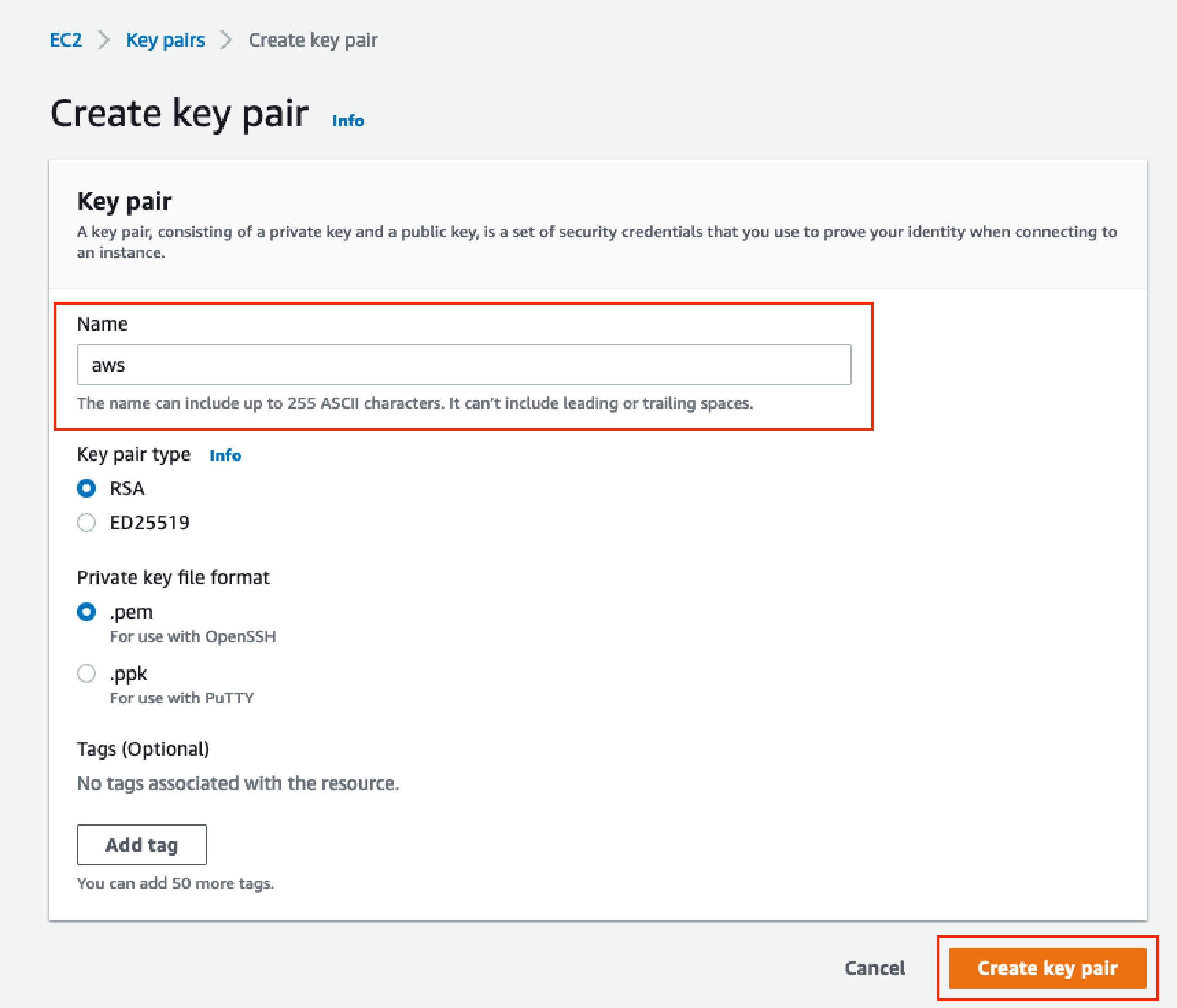
Platform: ISR Series Routers

Software: IOS 12.4+

ダウンロードした設定をオンプレミスVPNヘッドエンドデバイスに適用します。

オプションのステップC.カスタムキーペアの作成

AWS EC2インスタンスには、キーペアを使用してアクセスします。キーペアを作成するには、[**EC**2 Service]に移動します。[ネットワー**クとセキュリティ**]の[キー**ペア]メニューを選択します。** Create Key Pair**を選択して**、名前を付け**て、他の**値をデフォルトのままにし、もう一度Create Key Pair**を選択**します。



Create key pair Info

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

aws

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

Key pair type Info

● RSA

○ ED25519

Private key file format

● .pem
For use with OpenSSH

○ .ppk
For use with PuTTY

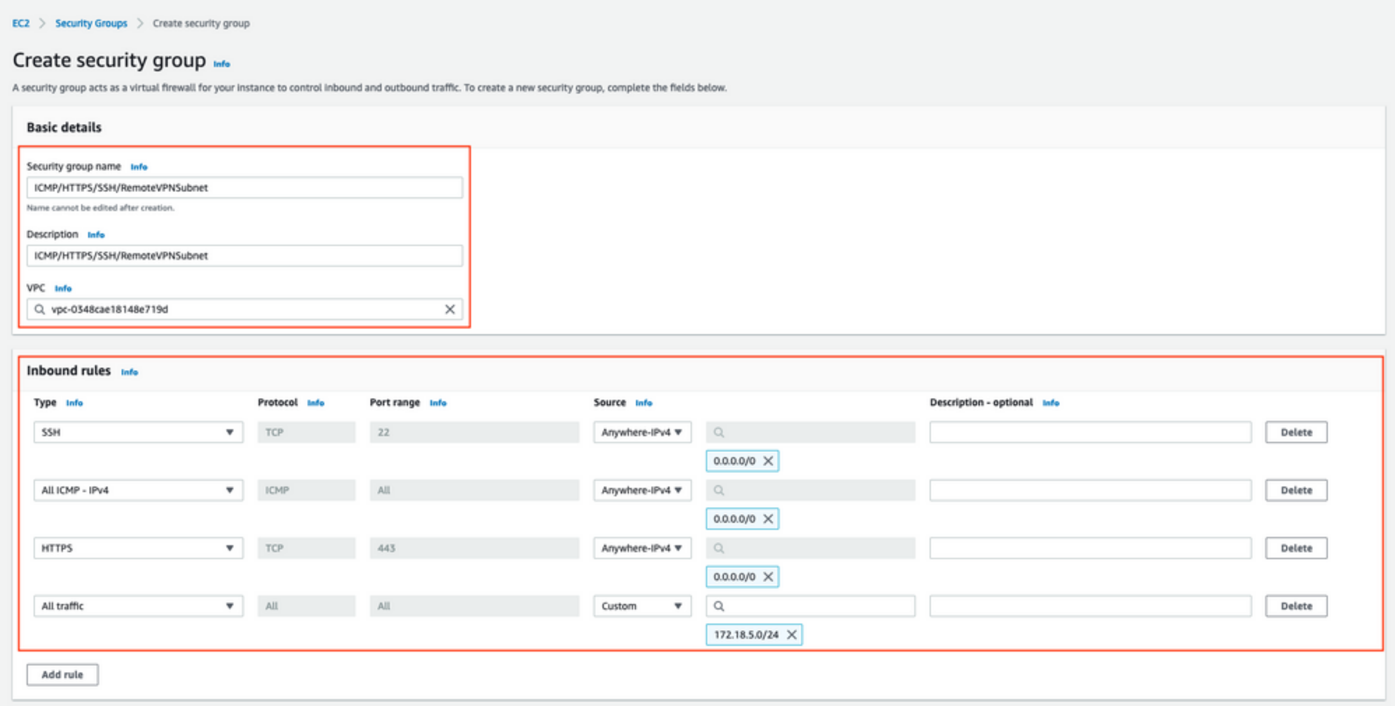
Tags (Optional)

No tags associated with the resource.

You can add 50 more tags.

オプションのステップD：カスタムセキュリティグループの作成

AWS EC2インスタンスのアクセスはセキュリティ・ グループによって保護され、セキュリティ・グループを構成するために、EC2サービスに移動します。[ネットワークとセキュリティ]の[セキュリティグループ]メニューを選択します。[Create Security Group]を選択し、[Name]、[Description]を設定します。[VPC]フィールドで、新しく設定したVPCを選択します。ISEへの通信を許可するように着信ルールを設定します。図に示すように[Create Security Group]を選択します。



EC2 > 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: ICMP/HTTPS/SSH/RemoteVPNSubnet

Name cannot be edited after creation.

Description Info: ICMP/HTTPS/SSH/RemoteVPNSubnet

VPC Info: vpc-0348cae18148e719d

Inbound rules Info

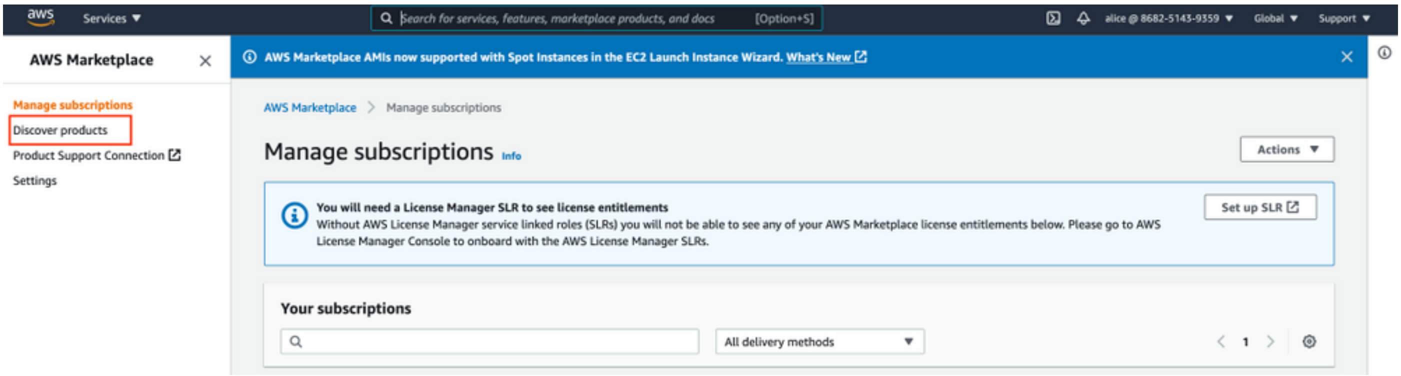
Type	Protocol	Port range	Source		Description - optional	
SSH	TCP	22	Anywhere-IPv4	0.0.0.0/0		Delete
All ICMP - IPv4	ICMP	All	Anywhere-IPv4	0.0.0.0/0		Delete
HTTPS	TCP	443	Anywhere-IPv4	0.0.0.0/0		Delete
All traffic	All	All	Custom	172.18.5.0/24		Delete

Add rule

注：設定されたセキュリティグループは、ISEへのSSH、ICMP、HTTPSアクセス、およびすべてのプロトコルへのオンプレミスサブネットからのアクセスを許可します。

ステップ1:AWS ISE Marketplace製品の登録

AWS Marketplace Subscriptions **AWS Serviceに移動**します。図に示す**[Discover Products]**を選択します。



AWS Marketplace AMIs now supported with Spot Instances in the EC2 Launch Instance Wizard. What's New

AWS Marketplace > Manage subscriptions

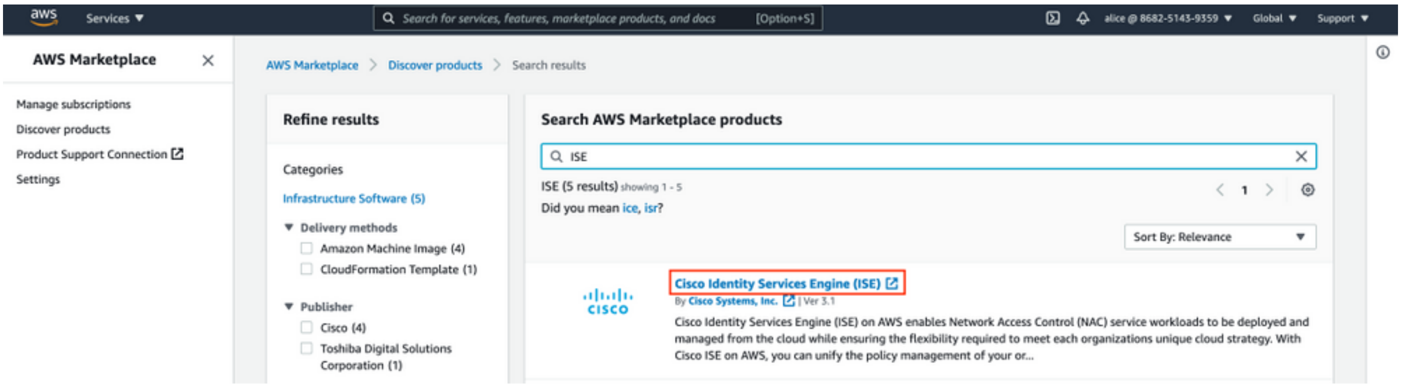
Manage subscriptions Info

You will need a License Manager SLR to see license entitlements

Without AWS License Manager service linked roles (SLRs) you will not be able to see any of your AWS Marketplace license entitlements below. Please go to AWS License Manager Console to onboard with the AWS License Manager SLRs.

Your subscriptions

図に示すように**ISE製**品を検索し、**Cisco Identity Services Engine(ISE)**を選択します。



AWS Marketplace > Discover products > Search results

Refine results

Categories

Infrastructure Software (5)

Delivery methods

□ Amazon Machine Image (4)

□ CloudFormation Template (1)

Publisher

□ Cisco (4)

□ Toshiba Digital Solutions Corporation (1)

Search AWS Marketplace products

ISE

ISE (5 results) showing 1 - 5

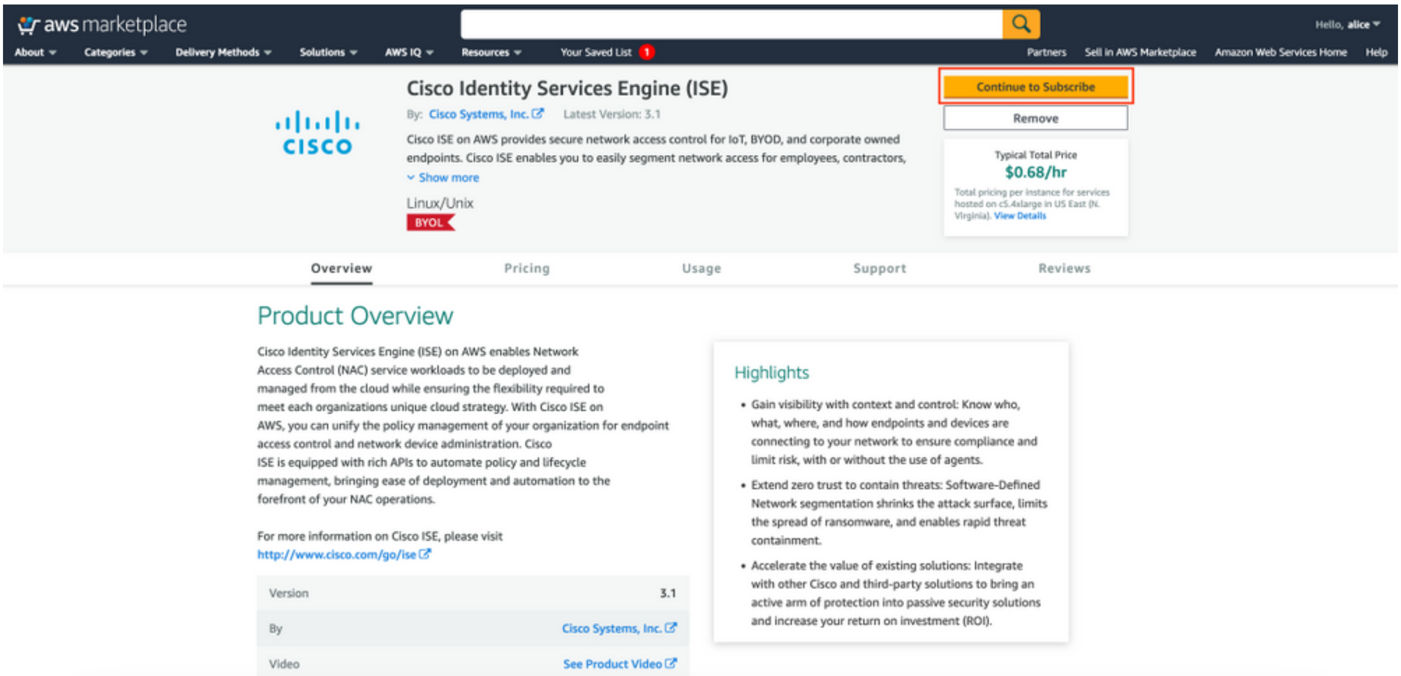
Did you mean ice, isr?

Cisco Identity Services Engine (ISE)

By Cisco Systems, Inc. | Ver 3.1

Cisco Identity Services Engine (ISE) on AWS enables Network Access Control (NAC) service workloads to be deployed and managed from the cloud while ensuring the flexibility required to meet each organizations unique cloud strategy. With Cisco ISE on AWS, you can unify the policy management of your or...

「購読を**続行」ボタンを選択**します



Cisco Identity Services Engine (ISE)

By: Cisco Systems, Inc. Latest Version: 3.1

Cisco ISE on AWS provides secure network access control for IoT, BYOD, and corporate owned endpoints. Cisco ISE enables you to easily segment network access for employees, contractors,

Show more

Linux/Unix

BYOL

Typical Total Price
$0.68/hr
Total pricing per instance for services hosted on c5.4xlarge in US East (N. Virginia). View Details

Product Overview

Cisco Identity Services Engine (ISE) on AWS enables Network Access Control (NAC) service workloads to be deployed and managed from the cloud while ensuring the flexibility required to meet each organizations unique cloud strategy. With Cisco ISE on AWS, you can unify the policy management of your organization for endpoint access control and network device administration. Cisco ISE is equipped with rich APIs to automate policy and lifecycle management, bringing ease of deployment and automation to the forefront of your NAC operations.

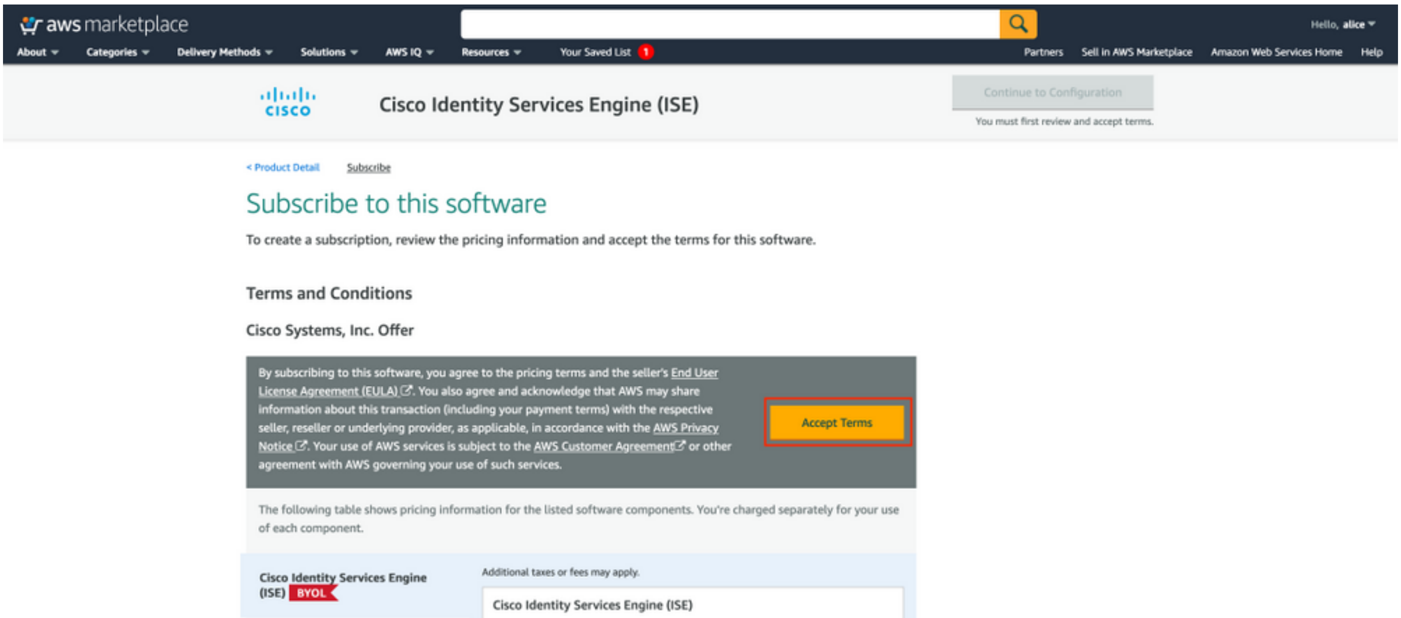
For more information on Cisco ISE, please visit http://www.cisco.com/go/ise

Version	3.1
By	Cisco Systems, Inc.
Video	See Product Video

Highlights

- Gain visibility with context and control: Know who, what, where, and how endpoints and devices are connecting to your network to ensure compliance and limit risk, with or without the use of agents.
- Extend zero trust to contain threats: Software-Defined Network segmentation shrinks the attack surface, limits the spread of ransomware, and enables rapid threat containment.
- Accelerate the value of existing solutions: Integrate with other Cisco and third-party solutions to bring an active arm of protection into passive security solutions and increase your return on investment (ROI).

図に示す**ように、**[Accept Terms]ボタンを選択します。



Cisco Identity Services Engine (ISE)

You must first review and accept terms.

Subscribe to this software

To create a subscription, review the pricing information and accept the terms for this software.

Terms and Conditions

Cisco Systems, Inc. Offer

By subscribing to this software, you agree to the pricing terms and the seller's End User License Agreement (EULA). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. Your use of AWS services is subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services.

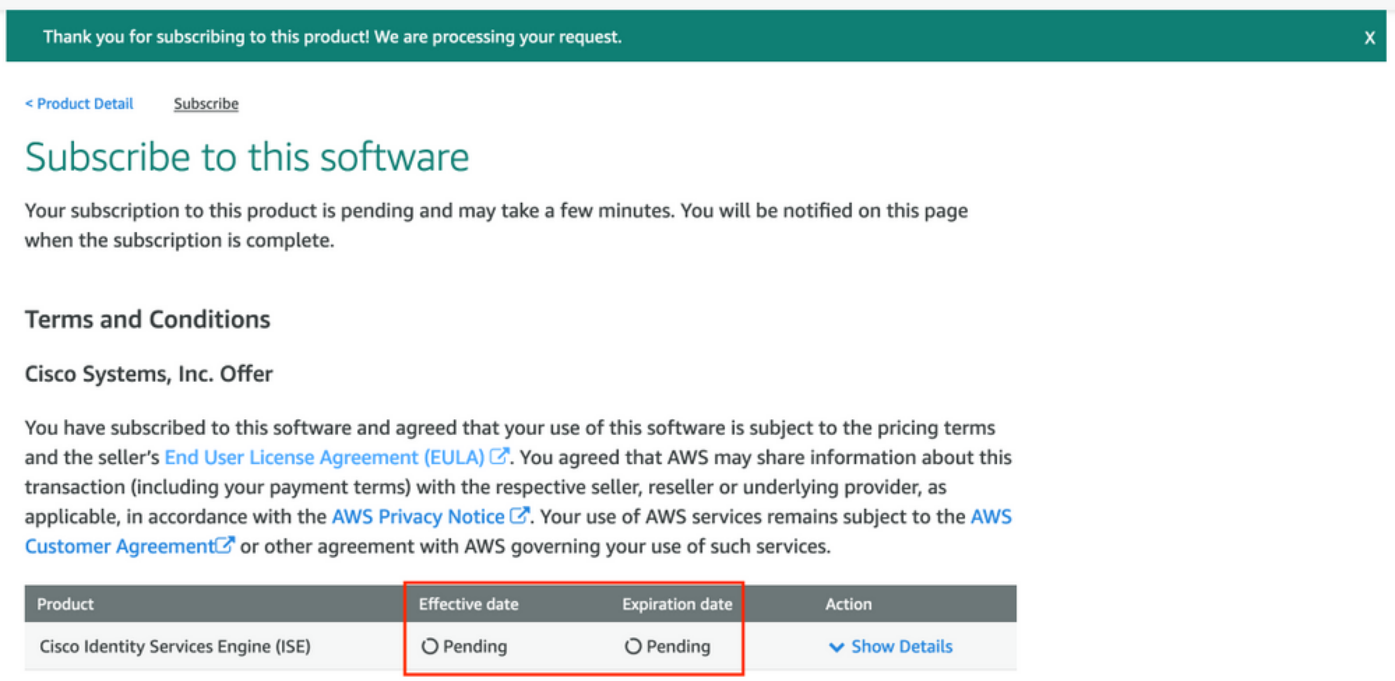
The following table shows pricing information for the listed software components. You're charged separately for your use of each component.

Cisco Identity Services Engine (ISE) BYOL

Additional taxes or fees may apply.

Cisco Identity Services Engine (ISE)

登録済みのステータスが[Effective]と[Expiration date]に変**更され**たら、図に示すように[Pending]。



Thank you for subscribing to this product! We are processing your request. X

< Product Detail   Subscribe

Subscribe to this software

Your subscription to this product is pending and may take a few minutes. You will be notified on this page when the subscription is complete.

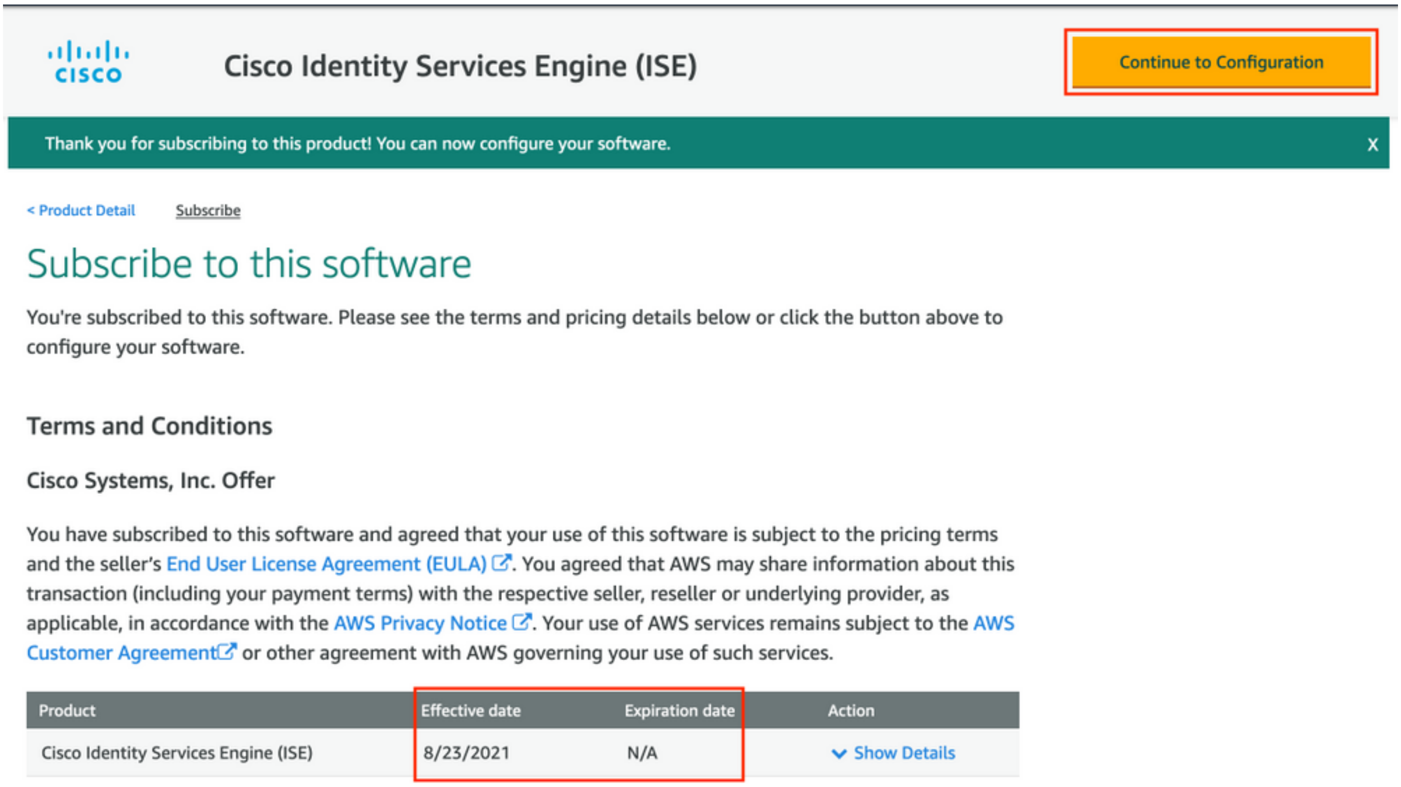
Terms and Conditions

Cisco Systems, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. Your use of AWS services remains subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services.

Product	Effective date	Expiration date	Action
Cisco Identity Services Engine (ISE)	○ Pending	○ Pending	Show Details

発効日が加入日に変更され、有効期限が該当なしに変更された直後imaに示すように、[Continue to Configuration]を選択します



Cisco Identity Services Engine (ISE)   Continue to Configuration

Thank you for subscribing to this product! You can now configure your software. X

< Product Detail   Subscribe

Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

Terms and Conditions

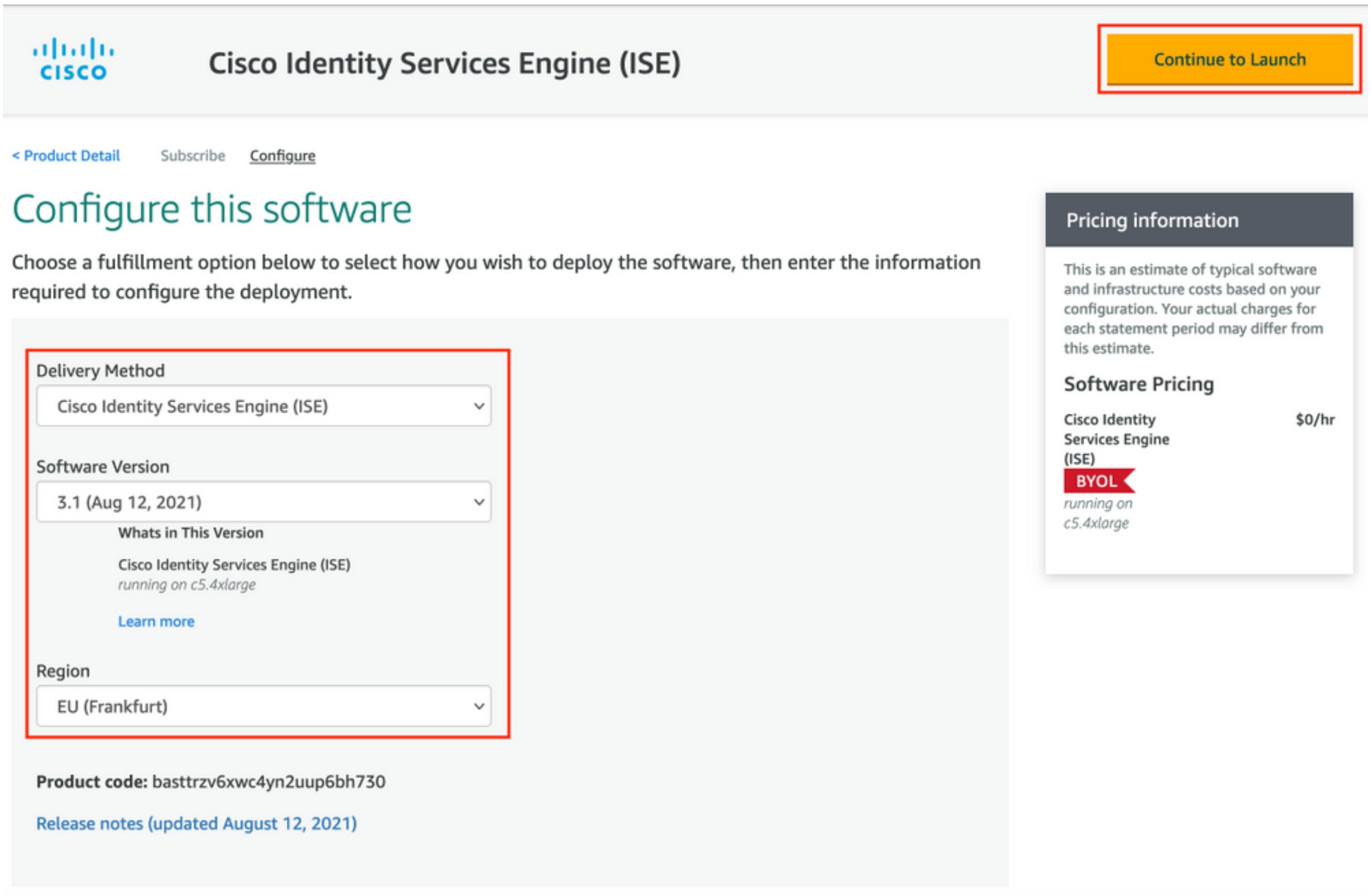
Cisco Systems, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. Your use of AWS services remains subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services.

Product	Effective date	Expiration date	Action
Cisco Identity Services Engine (ISE)	8/23/2021	N/A	Show Details

ステップ2:AWSでのISEの設定

[Configure this software]画面の[Delivery Method]メニューで、[Cisco Identity Services Engine (ISE)]を選択します。 [Software Version]で[3.1 (Aug 12, 2021)]を選択します。 ISEの導入が計画されている[Region]を選択します。 「起動の続行」を選択します。



Cisco Identity Services Engine (ISE)

Continue to Launch

< Product Detail Subscribe Configure

Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Delivery Method
Cisco Identity Services Engine (ISE)

Software Version
3.1 (Aug 12, 2021)

Whats in This Version

Cisco Identity Services Engine (ISE)
running on c5.4xlarge

Learn more

Region
EU (Frankfurt)

Product code: basttrzv6xwc4yn2uup6bh730

Release notes (updated August 12, 2021)

Pricing information

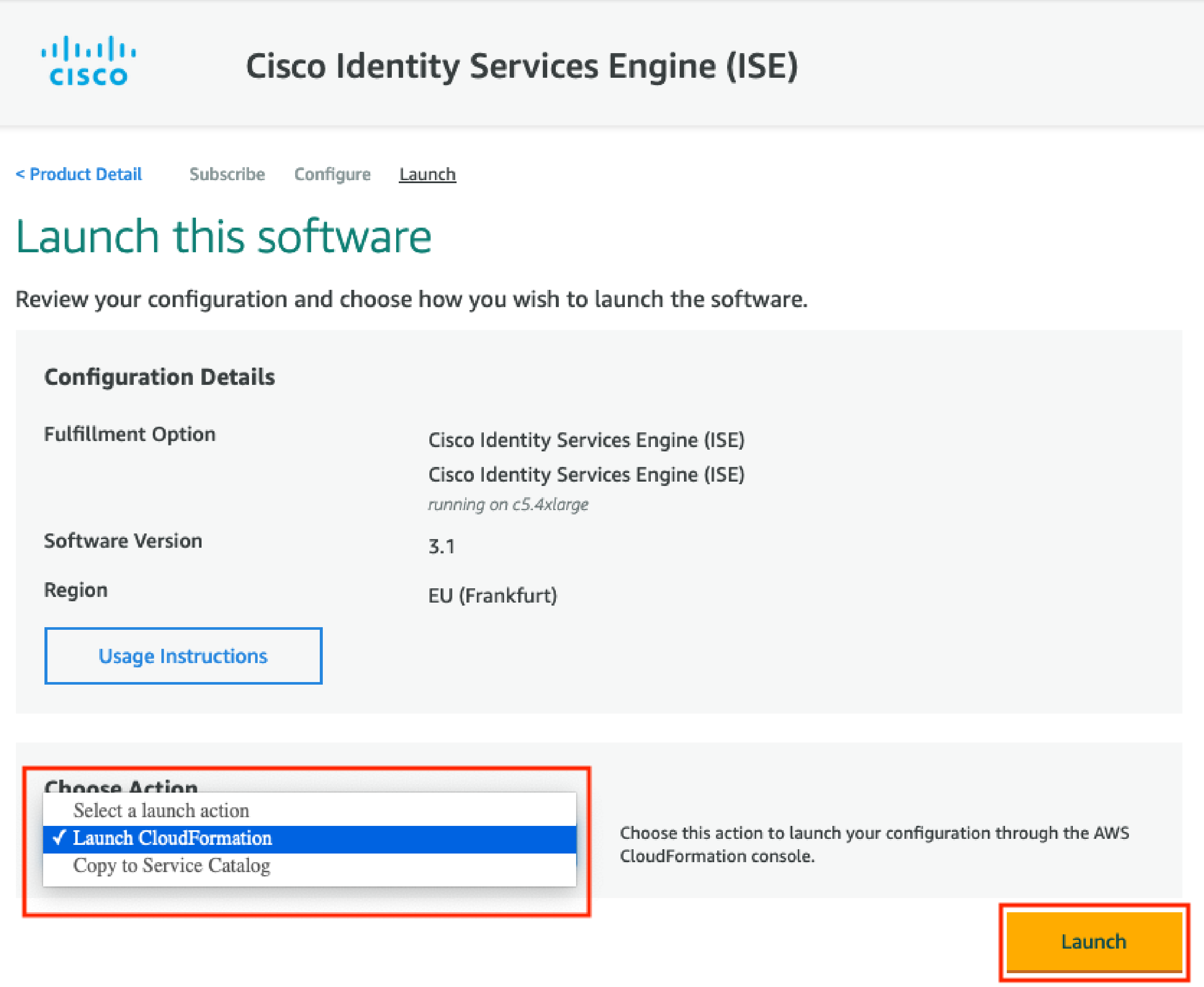
This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

Software Pricing

Cisco Identity Services Engine (ISE) BYOL *running on c5.4xlarge*	$0/hr

ステップ3:AWSでのISEの起動

[Launch this Software]画面の[Actions]ドロップダウンメニューから、**[Launch CloudFormation]**を選択します。



Cisco Identity Services Engine (ISE)

< Product Detail　Subscribe　Configure　Launch

Launch this software

Review your configuration and choose how you wish to launch the software.

Configuration Details

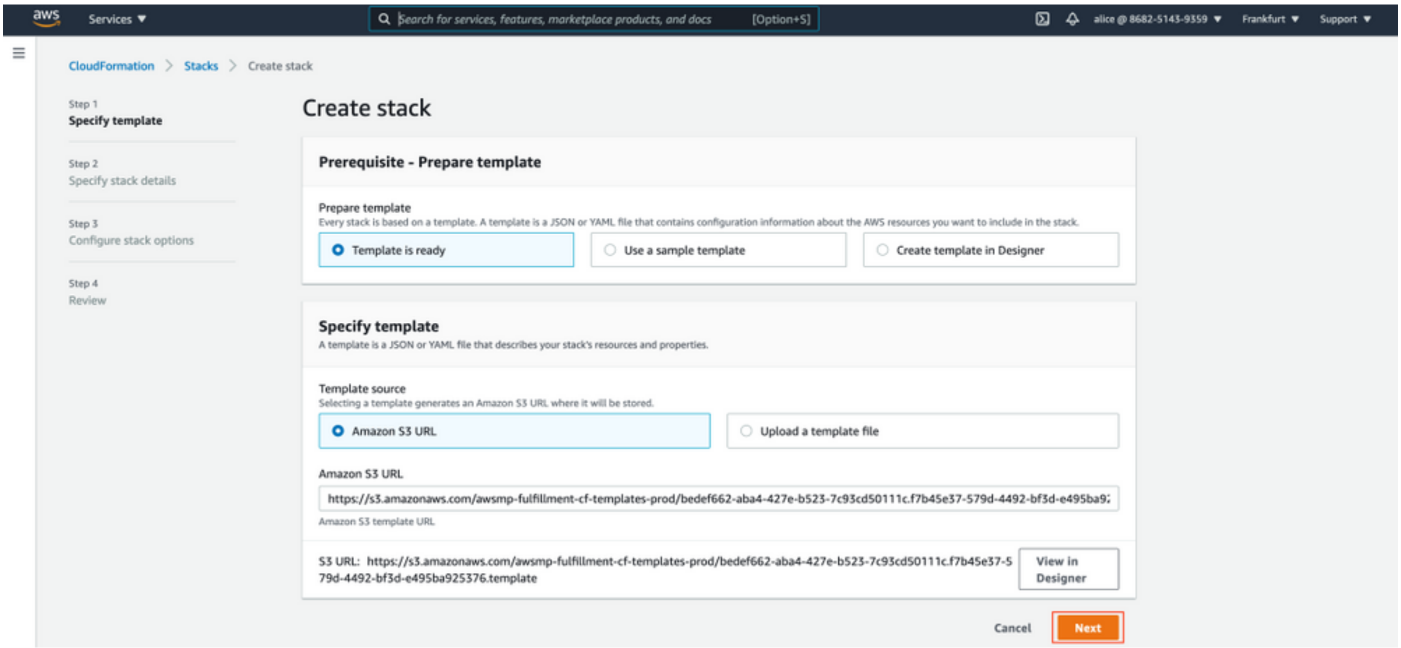
Fulfillment Option	Cisco Identity Services Engine (ISE) Cisco Identity Services Engine (ISE) *running on c5.4xlarge*
Software Version	3.1
Region	EU (Frankfurt)

Choose this action to launch your configuration through the AWS CloudFormation console.

（オプション）使用方法**の説明を**選択して使い慣れさせてください。「起動」を**選択します。**

ステップ4:AWSでのISE用のCloudFormationスタックの設定

起動ボタンを押すと、CloudFormationスタックの**設定画面に**移動します。ISEのセットアップに使用する必要がある事前に作成されたテンプレートがあります。デフォルト設定のまま、[次へ]を**選択します。**


aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
alice @ 8682-5143-9359 ▼
Frankfurt ▼
Support ▼

CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

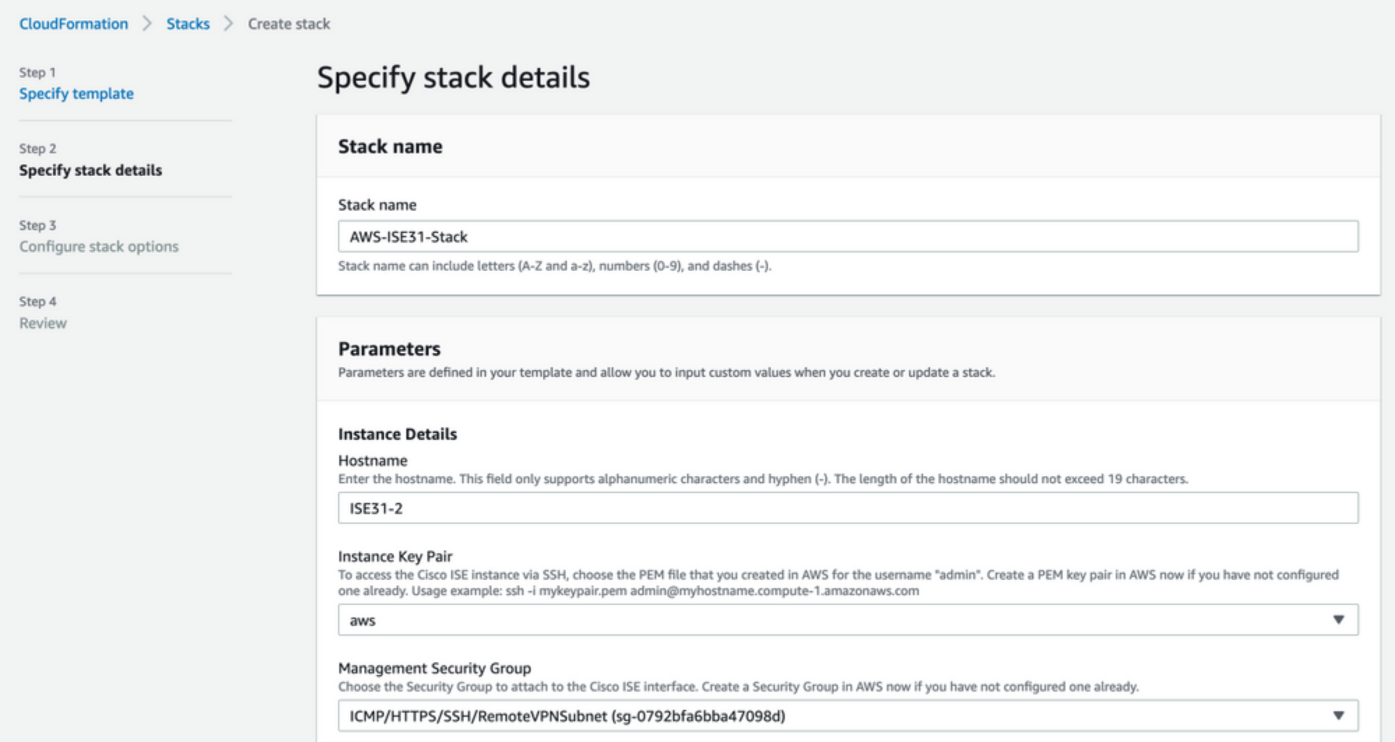
Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

● Amazon S3 URL ○ Upload a template file

Amazon S3 URL
https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e37-579d-4492-bf3d-e495ba9:
Amazon S3 template URL

S3 URL: https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e37-579d-4492-bf3d-e495ba925376.template

CloudFormationスタックデータにスタック**名を入力します。**ホスト名などのインスタンスの詳細**を構成**し、[インスタンス**キーペア]**と[管理セキュ**リティグループ]を選択します。**


CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Specify stack details

Stack name

Stack name
AWS-ISE31-Stack
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

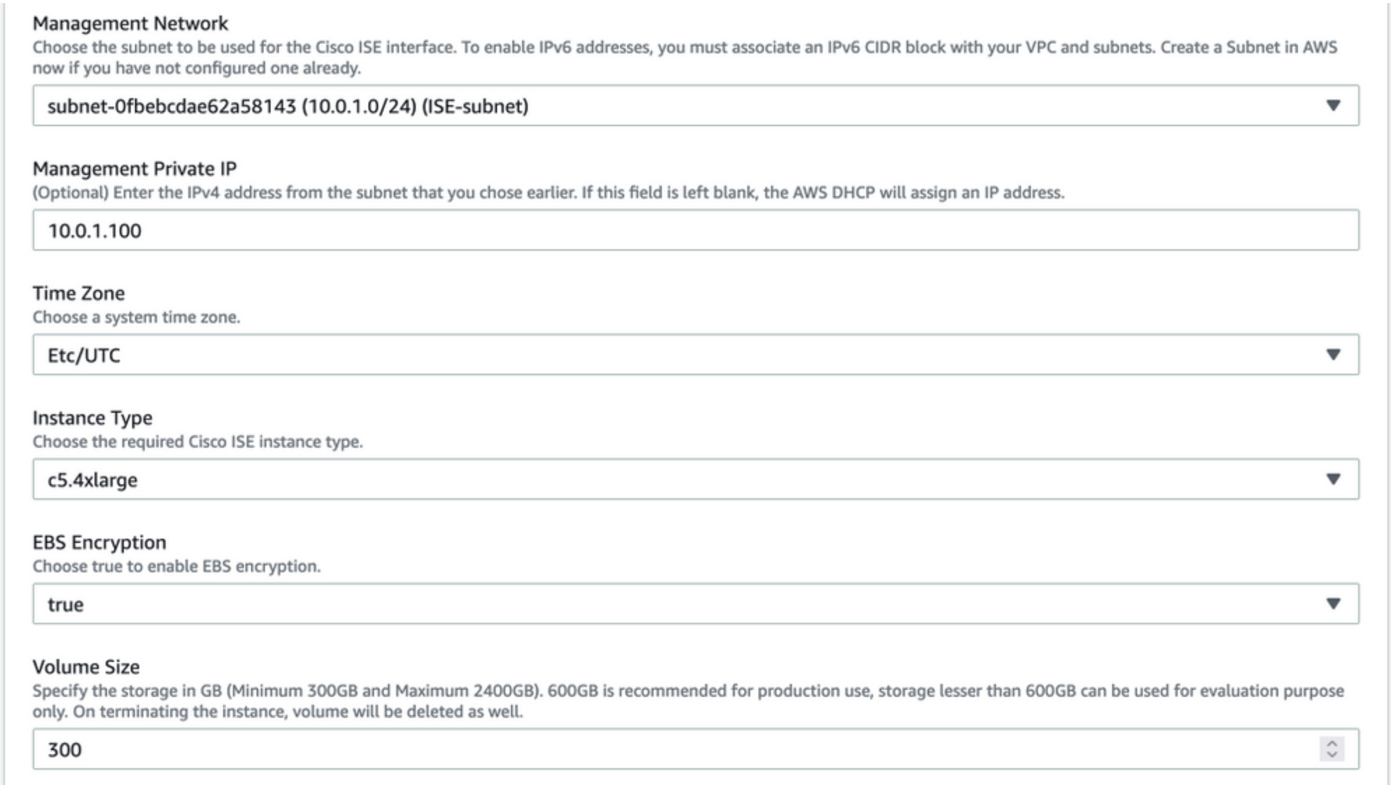
Instance Details

Hostname
Enter the hostname. This field only supports alphanumeric characters and hyphen (-). The length of the hostname should not exceed 19 characters.
ISE31-2

Instance Key Pair
To access the Cisco ISE instance via SSH, choose the PEM file that you created in AWS for the username "admin". Create a PEM key pair in AWS now if you have not configured one already. Usage example: ssh -i mykeypair.pem admin@myhostname.compute-1.amazonaws.com
aws ▼

Management Security Group
Choose the Security Group to attach to the Cisco ISE interface. Create a Security Group in AWS now if you have not configured one already.
ICMP/HTTPS/SSH/RemoteVPNSubnet (sg-0792bfa6bba47098d) ▼

[管理ネットワーク]、[管理プライベートIP]、[タイ**ムゾーン]、[インスタンスタイプ]、[EBS暗号化]、[ボリ**ュームサイズ]を**使用して構成を続行**



Management Network

Choose the subnet to be used for the Cisco ISE interface. To enable IPv6 addresses, you must associate an IPv6 CIDR block with your VPC and subnets. Create a Subnet in AWS now if you have not configured one already.

subnet-0fbebcdae62a58143 (10.0.1.0/24) (ISE-subnet) ▼

Management Private IP

(Optional) Enter the IPv4 address from the subnet that you chose earlier. If this field is left blank, the AWS DHCP will assign an IP address.

10.0.1.100

Time Zone

Choose a system time zone.

Etc/UTC ▼

Instance Type

Choose the required Cisco ISE instance type.

c5.4xlarge ▼

EBS Encryption

Choose true to enable EBS encryption.

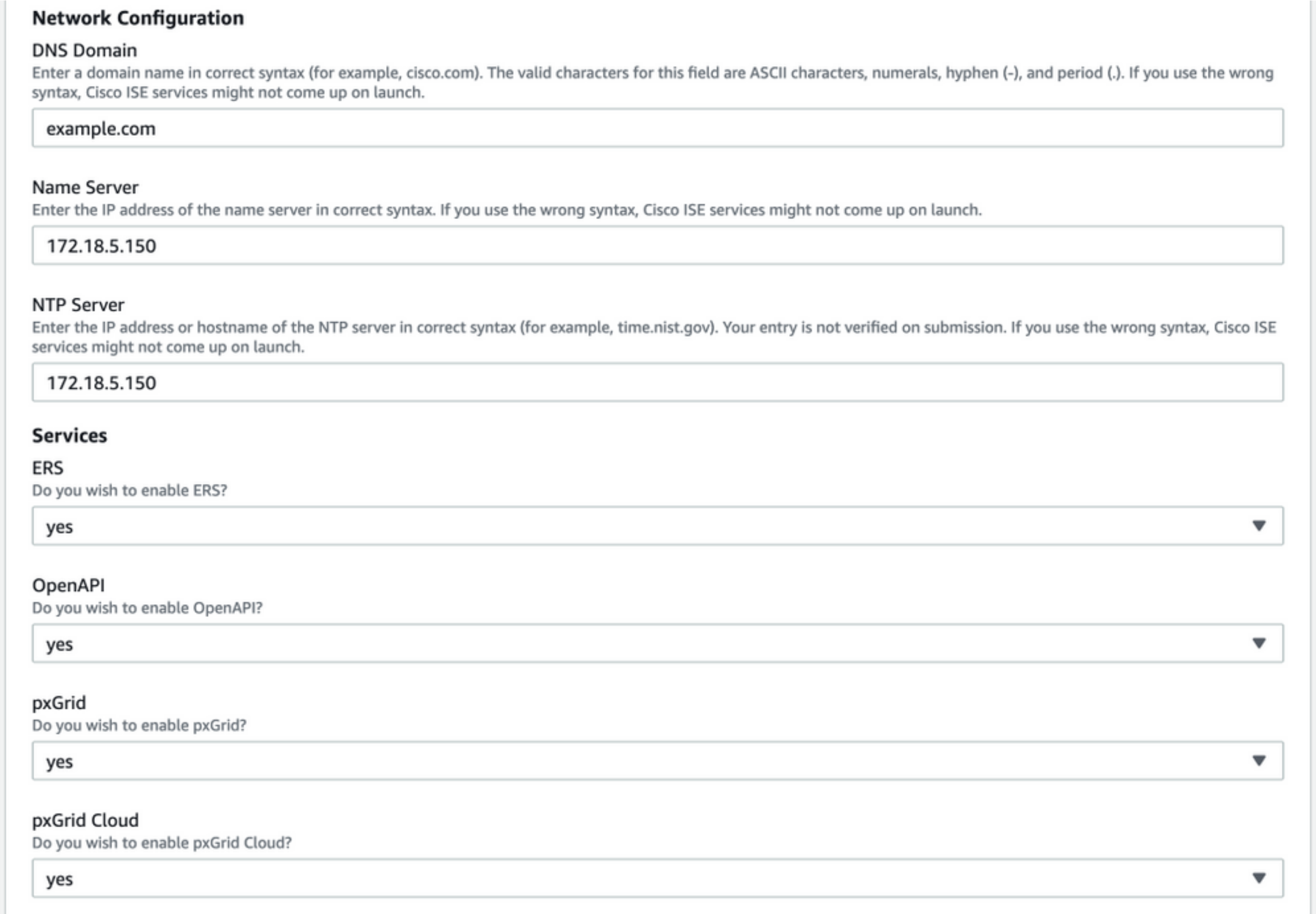
true ▼

Volume Size

Specify the storage in GB (Minimum 300GB and Maximum 2400GB). 600GB is recommended for production use, storage lesser than 600GB can be used for evaluation purpose only. On terminating the instance, volume will be deleted as well.

300

DNSドメイン、ネームサーバ、NTPサービス、およびサービスを使用してインスタンスの詳細の構成を続行します。



Network Configuration

DNS Domain

Enter a domain name in correct syntax (for example, cisco.com). The valid characters for this field are ASCII characters, numerals, hyphen (-), and period (.). If you use the wrong syntax, Cisco ISE services might not come up on launch.

example.com

Name Server

Enter the IP address of the name server in correct syntax. If you use the wrong syntax, Cisco ISE services might not come up on launch.

172.18.5.150

NTP Server

Enter the IP address or hostname of the NTP server in correct syntax (for example, time.nist.gov). Your entry is not verified on submission. If you use the wrong syntax, Cisco ISE services might not come up on launch.

172.18.5.150

Services

ERS

Do you wish to enable ERS?

yes ▼

OpenAPI

Do you wish to enable OpenAPI?

yes ▼

pxGrid

Do you wish to enable pxGrid?

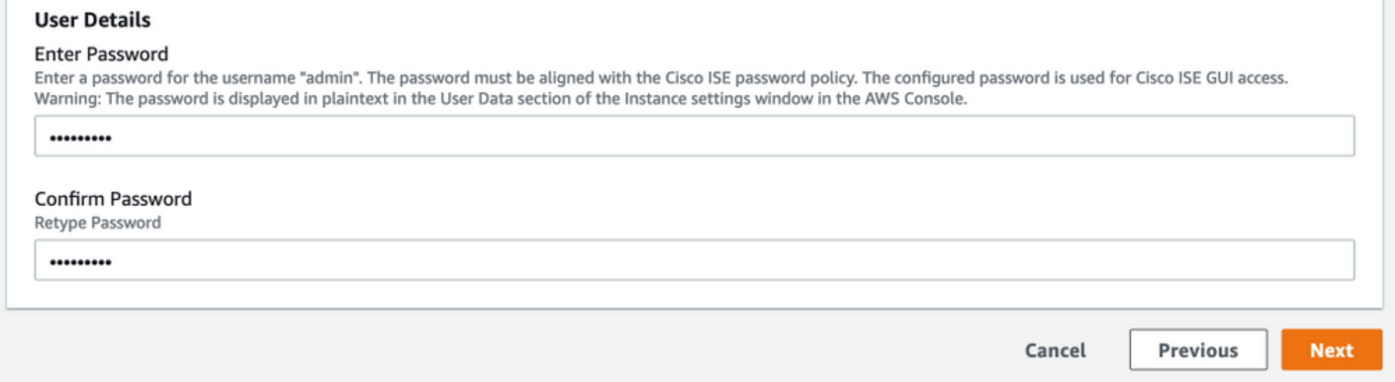
yes ▼

pxGrid Cloud

Do you wish to enable pxGrid Cloud?

yes ▼

GUIユーザー・パスワードを構成し、「**Next**」を選択します。



User Details

Enter Password

Enter a password for the username "admin". The password must be aligned with the Cisco ISE password policy. The configured password is used for Cisco ISE GUI access.
Warning: The password is displayed in plaintext in the User Data section of the Instance settings window in the AWS Console.

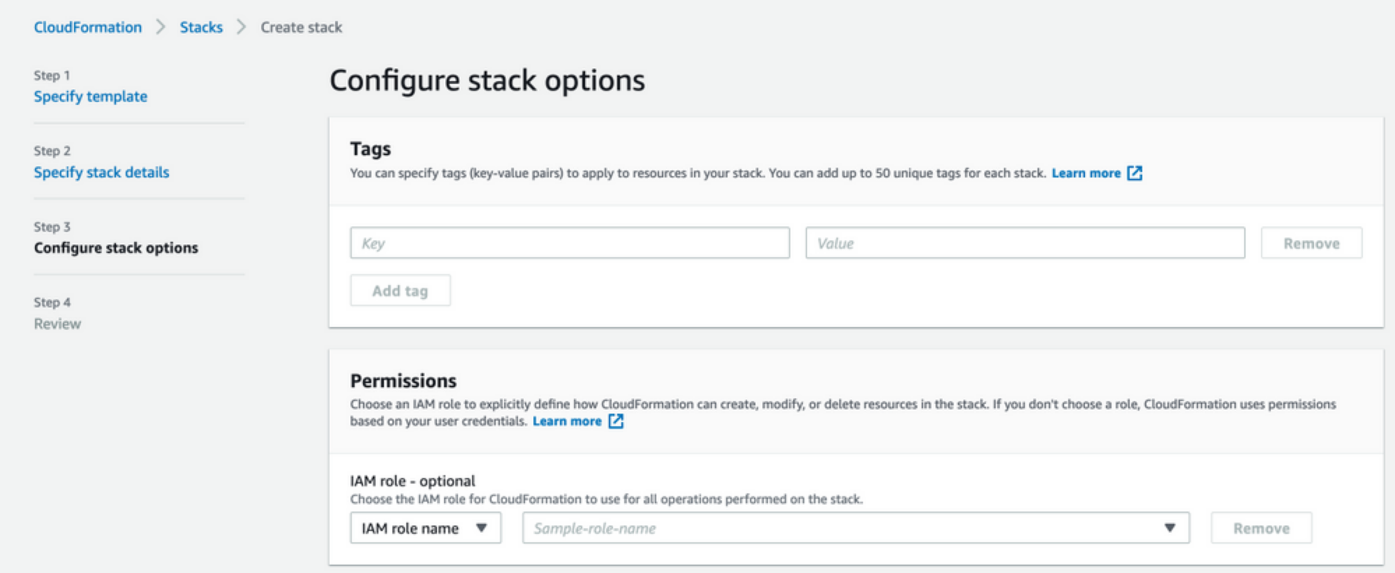
•••••••••

Confirm Password

Retype Password

•••••••••

次の画面では変更は必要ありません。[次へ（Next）] を選択します。



CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Configure stack options

Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. Learn more

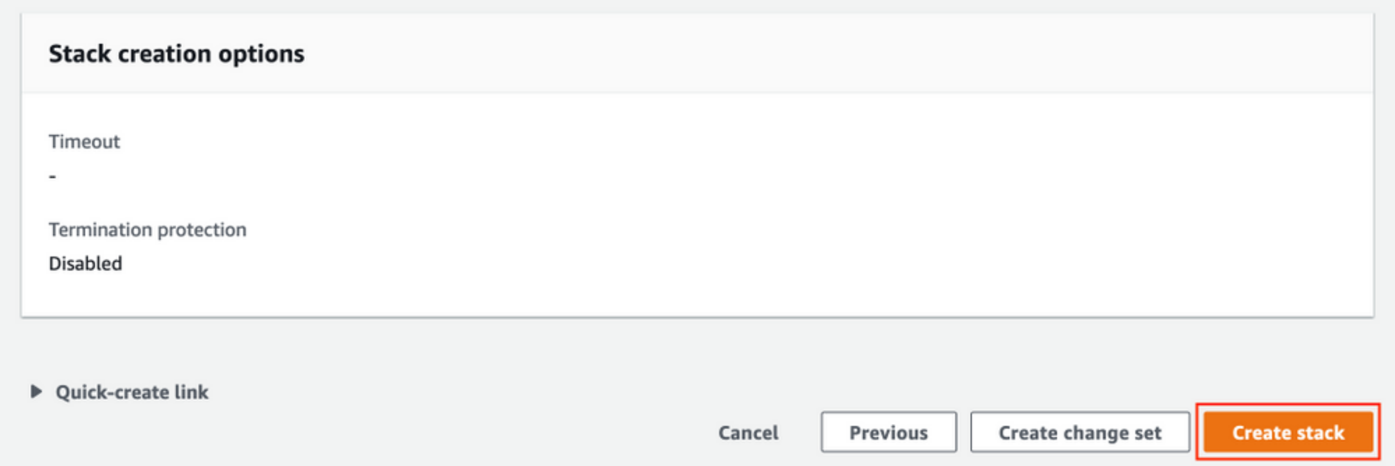
Permissions

Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more

IAM role - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

[スタックの確認]画面**に移動**し、下にスクロールして[スタックの作**成]を選択します**。



Stack creation options

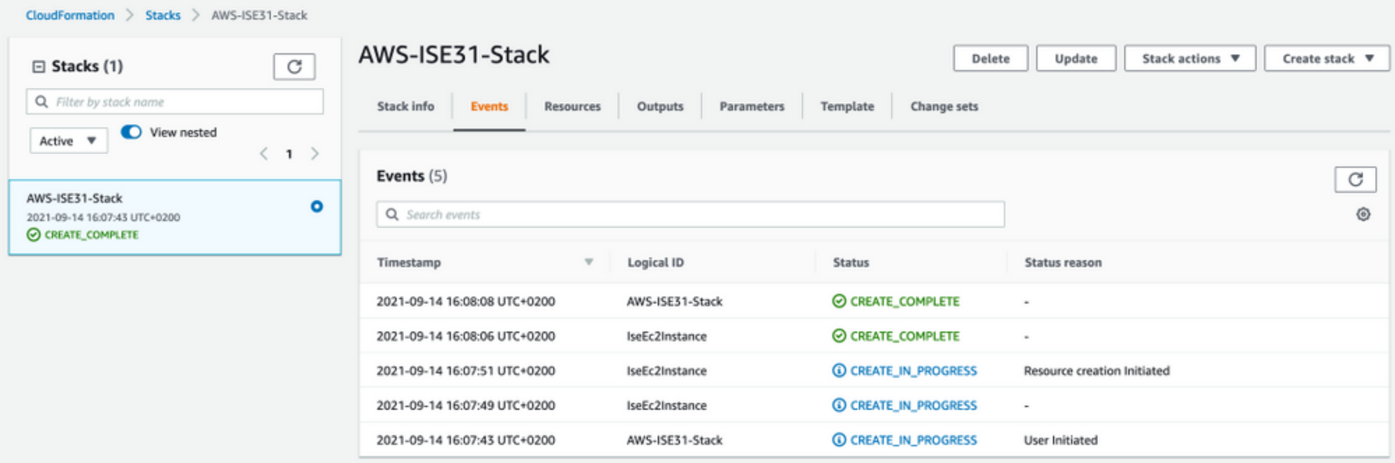
Timeout

-

Termination protection

Disabled

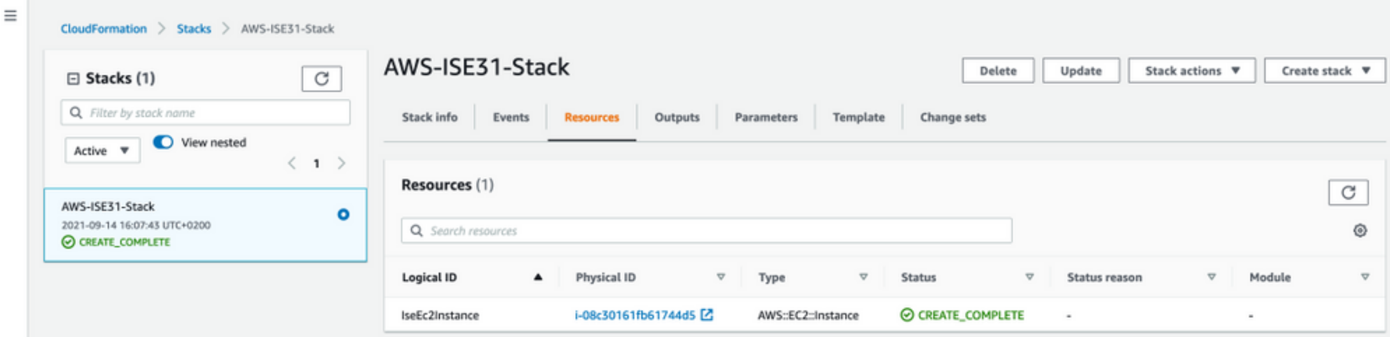
スタックが展開されると、**CREATE_COMPLETEステータス**が表示されます。



Timestamp	Logical ID	Status	Status reason
2021-09-14 16:08:08 UTC+0200	AWS-ISE31-Stack	CREATE_COMPLETE	-
2021-09-14 16:08:06 UTC+0200	IseEc2Instance	CREATE_COMPLETE	-
2021-09-14 16:07:51 UTC+0200	IseEc2Instance	CREATE_IN_PROGRESS	Resource creation Initiated
2021-09-14 16:07:49 UTC+0200	IseEc2Instance	CREATE_IN_PROGRESS	-
2021-09-14 16:07:43 UTC+0200	AWS-ISE31-Stack	CREATE_IN_PROGRESS	User Initiated

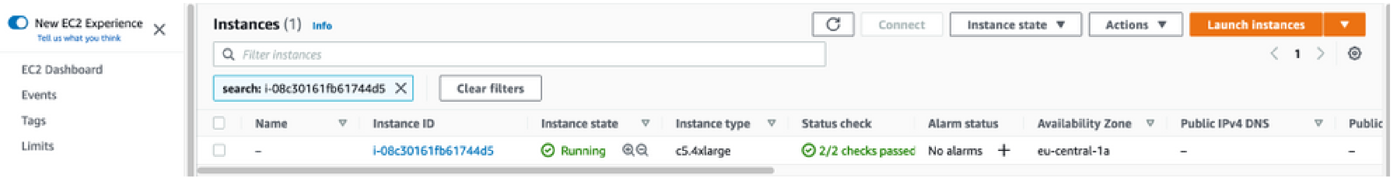
ステップ5:AWSでISEにアクセスする

ISEインスタンスにアクセスするには、[Resources] タブに移動し、CloudFormsから作成されたEC2インスタンスを表示します(図に示すように、**[Services] > [EC2] > [Instances]に移動し**て)。



Logical ID	Physical ID	Type	Status	Status reason	Module
IseEc2Instance	i-08c30161fb61744d5	AWS::EC2::Instance	CREATE_COMPLETE	-	-

[Physical ID]**を選択**して、**[EC2 Instances]メニューを**開きます。ステータスチェッ**クに合格**ステータス**が2/2であることを確認**します。



Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public
-	i-08c30161fb61744d5	Running	c5.4xlarge	2/2 checks passed	No alarms	eu-central-1a	–	–

[インスタン**スID]を選択します**。ISEには、SSHまたはHTTPSプロトコルを使用して**プライベートIPv4アドレス/プライベートIPv4 DNS**を介してアクセスできます。

> **注**：プライベート**IPv4**アドレス/プライベートIPv4 DNSを介してISEにアクセスする場合は、ISEプライベートアドレスへのネットワーク接続があることを確認します。

SSHを介してプライベートIPv4**アドレスでアクセス**したISEの例：

```
[centos@ip-172-31-42-104 ~]$ ssh -i aws.pem admin@10.0.1.100
The authenticity of host '10.0.1.100 (10.0.1.100)' can't be established.
ECDSA key fingerprint is SHA256:G5NdGZ1rgPYnjnldPcXOLcJg9VICLSxnZA0kn0CfMPs.
ECDSA key fingerprint is MD5:aa:e1:7f:8f:35:e8:44:13:f3:48:be:d3:4f:5f:05:f8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.100' (ECDSA) to the list of known hosts.
Last login: Tue Sep 14 14:36:39 2021 from 172.31.42.104
Failed to log in 0 time(s)
```

```
ISE31-2/admin#
```

> **注：**ISEがSSH経由でアクセスできるまでに約20分かかります。その時点まで、ISEへの接続が「**Permission denied (publickey)」で失敗します。** というエラー メッセージが表示されます。

show application status iseを使用**して、サービスが実行**されていることを確認します。

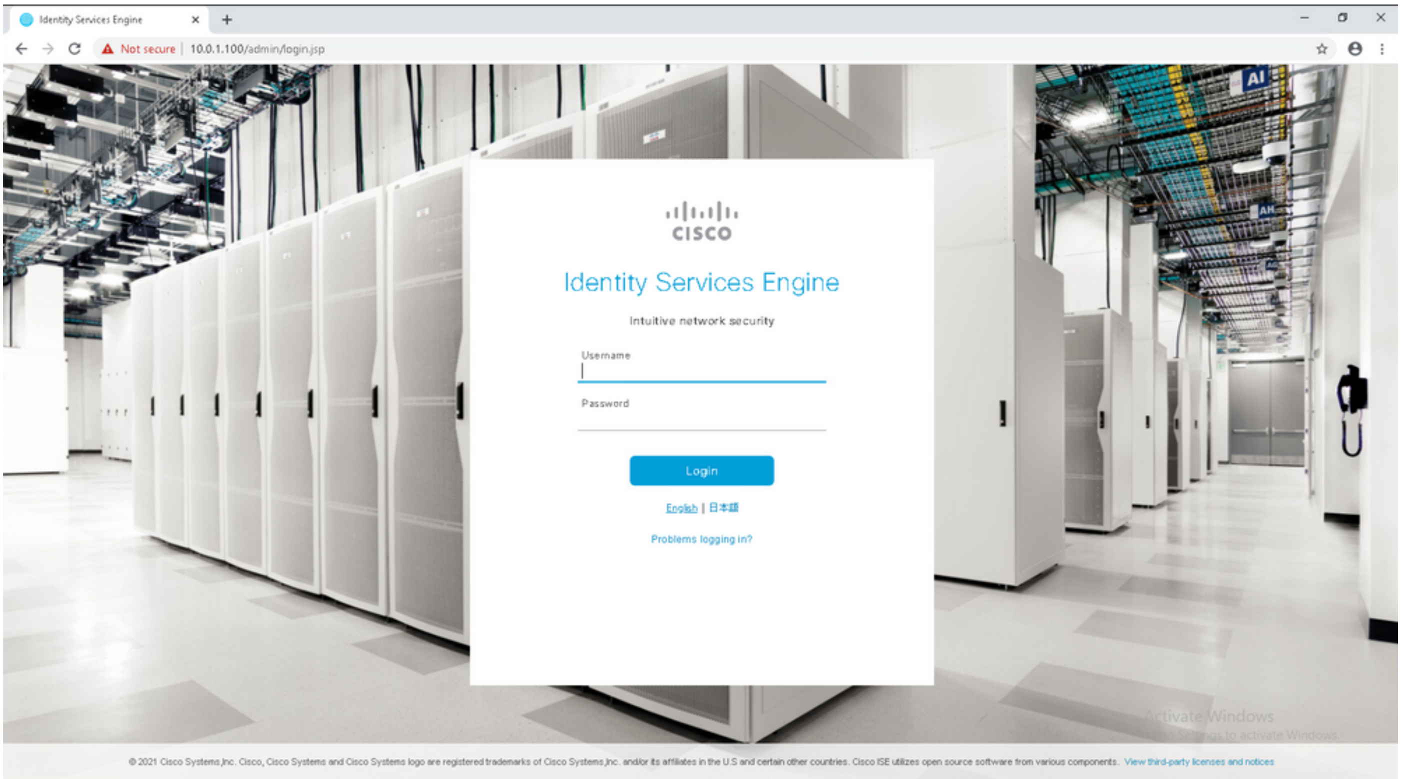
```
ISE31-2/admin# show application status ise

ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 27703
Database Server running 127 PROCESSES
Application Server                       running         47142
Profiler Database running 38593
ISE Indexing Engine running 48309
AD Connector running 56223
M&T Session Database running 37058
M&T Log Processor running 47400
Certificate Authority Service running 55683
EST Service running
SXP Engine Service disabled
TC-NAC Service disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 30760
ISE API Gateway Database Service running 35316
ISE API Gateway Service running 44900
Segmentation Policy Service disabled
REST Auth Service disabled
SSE Connector disabled
Hermes (pxGrid Cloud Agent) Service disabled

ISE31-2/admin#
```

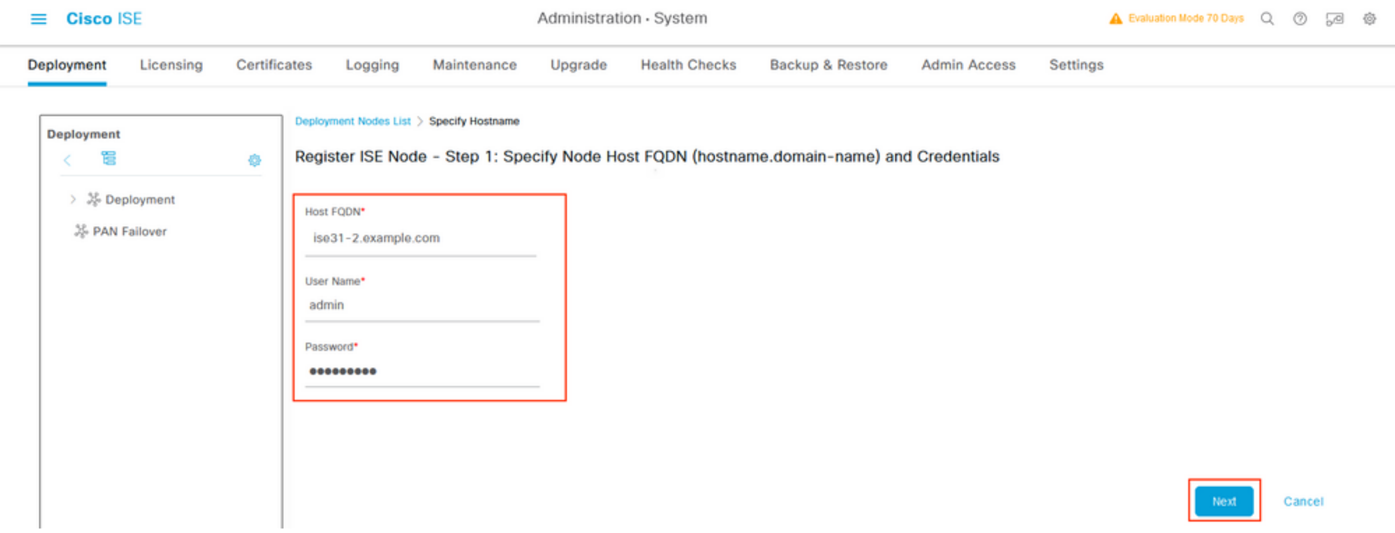
> **注：**ISEサービスが実行状態に移行するためにSSHが使用できるようになってから、約10 ~ 15分かかります。

Application Serverが実行**状態に**なっ**たら、図に示す**ようにGUIからISEにアクセスできます。


Identity Services Engine
Not secure | 10.0.1.100/admin/login.jsp
cisco
Identity Services Engine
Intuitive network security
Username
Password
Login
English | 日本語
Problems logging in?
© 2021 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc. and/or its affiliates in the U.S and certain other countries. Cisco ISE utilizes open source software from various components. View third-party licenses and notices

ステップ6：オンプレミスISEとAWS上のISEの間の分散デプロイを設定する

On-Prem ISEにログインし、**[Administration]** > **[System]** > **[Deployment]に移動します。**ノードを選択し、「プライマリに**設定」を選択します。[Administration]** > **[System]** > **[Deployment]に戻り**、[Register]を選択**します**。AWS、**GUIユーザー**名、およびパスワードでISEのホス**トFQDNを**設定**します。**[next] をクリックします。



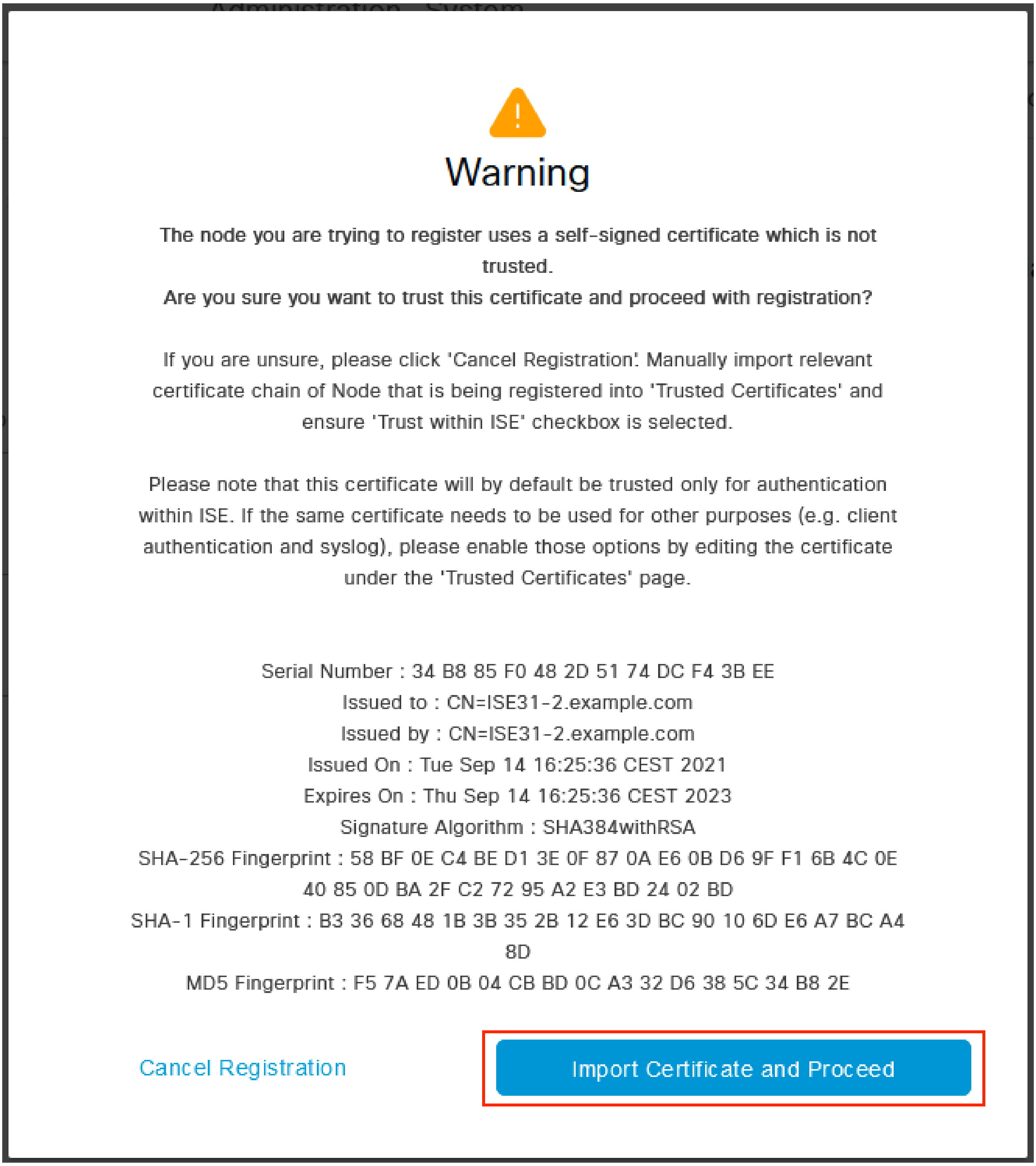
Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

Host FQDN*: ise31-2.example.com

User Name*: admin

Password*: ●●●●●●●●●

このトポロジでは自己署名証明書が使用されるため、信頼ストアに管理者証明書をクロスインポートするには[証明書のインポートと**続行]を選択します。**



Warning

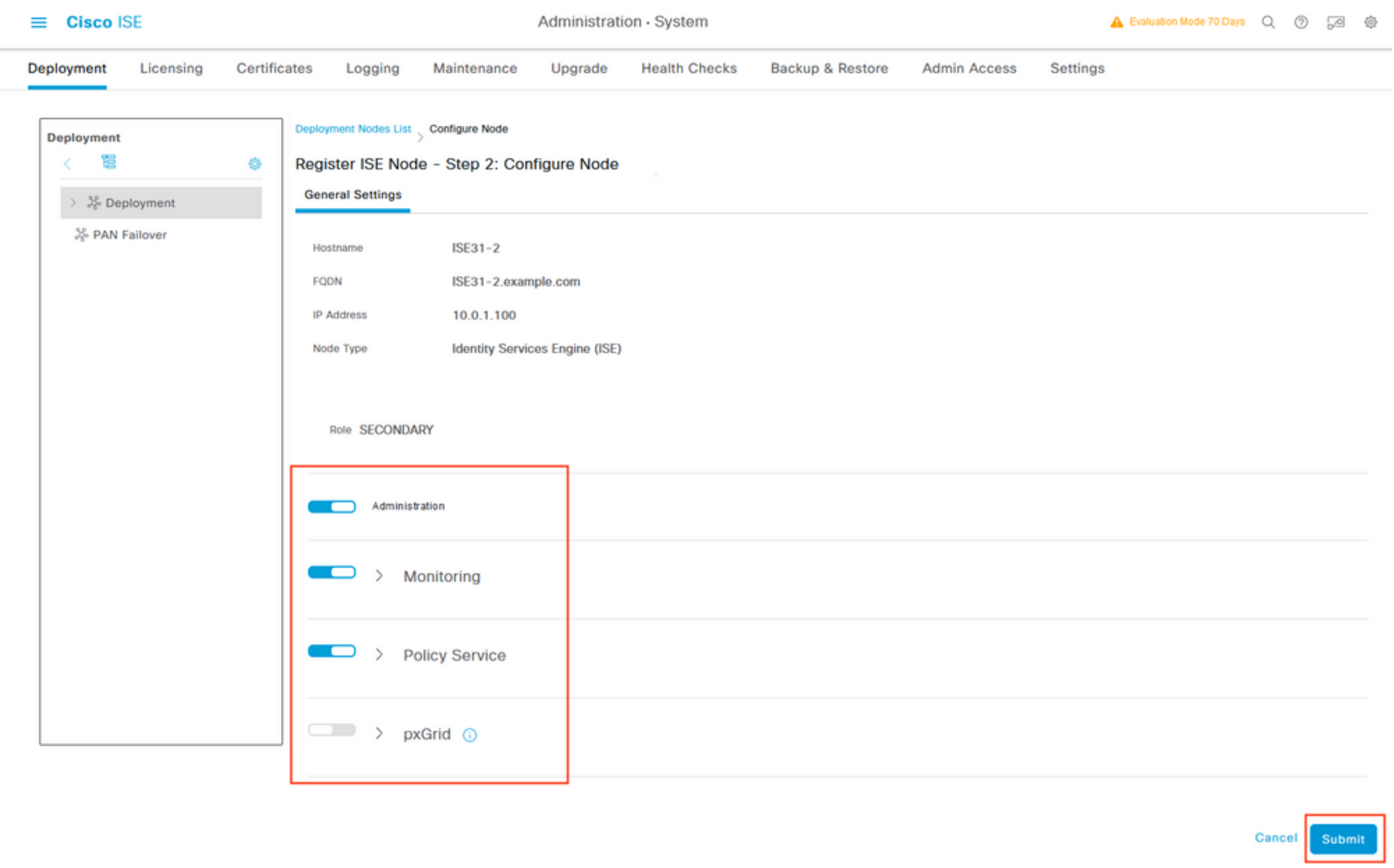
The node you are trying to register uses a self-signed certificate which is not trusted.
Are you sure you want to trust this certificate and proceed with registration?

If you are unsure, please click 'Cancel Registration'. Manually import relevant certificate chain of Node that is being registered into 'Trusted Certificates' and ensure 'Trust within ISE' checkbox is selected.

Please note that this certificate will by default be trusted only for authentication within ISE. If the same certificate needs to be used for other purposes (e.g. client authentication and syslog), please enable those options by editing the certificate under the 'Trusted Certificates' page.

Serial Number : 34 B8 85 F0 48 2D 51 74 DC F4 3B EE
Issued to : CN=ISE31-2.example.com
Issued by : CN=ISE31-2.example.com
Issued On : Tue Sep 14 16:25:36 CEST 2021
Expires On : Thu Sep 14 16:25:36 CEST 2023
Signature Algorithm : SHA384withRSA
SHA-256 Fingerprint : 58 BF 0E C4 BE D1 3E 0F 87 0A E6 0B D6 9F F1 6B 4C 0E 40 85 0D BA 2F C2 72 95 A2 E3 BD 24 02 BD
SHA-1 Fingerprint : B3 36 68 48 1B 3B 35 2B 12 E6 3D BC 90 10 6D E6 A7 BC A4 8D
MD5 Fingerprint : F5 7A ED 0B 04 CB BD 0C A3 32 D6 38 5C 34 B8 2E

選択したペルソナを選択し、[送信]をクリックします。



Register ISE Node - Step 2: Configure Node

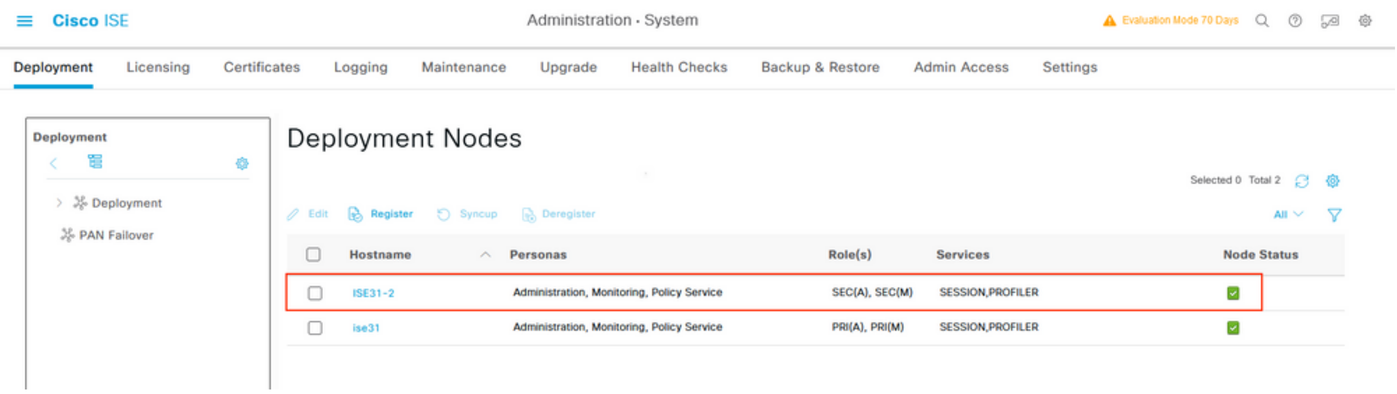
General Settings

Hostname	ISE31-2
FQDN	ISE31-2.example.com
IP Address	10.0.1.100
Node Type	Identity Services Engine (ISE)

Role SECONDARY

- ● Administration
- ● Monitoring
- ● Policy Service
- ○ pxGrid

同期が完了すると、ノードは接続状態に移行し、緑色のチェックボックスが表示されます。

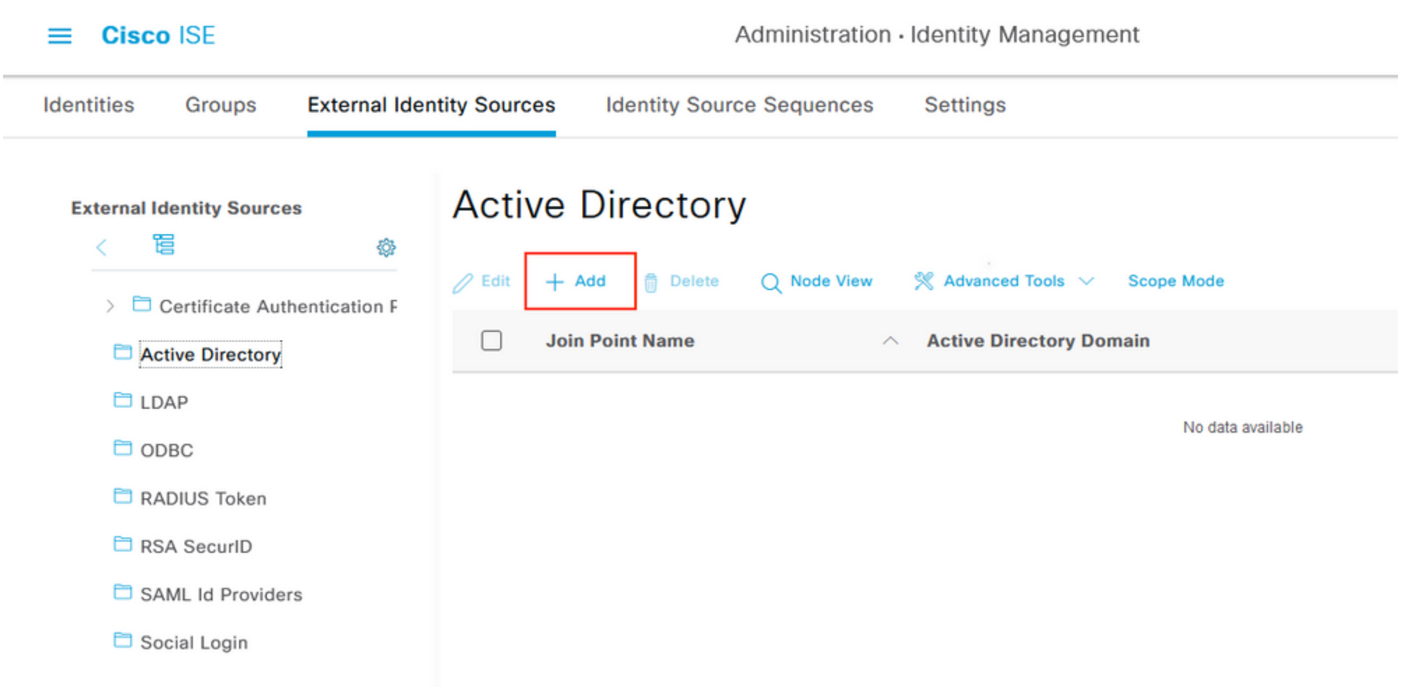


Deployment Nodes

□	Hostname	Personas	Role(s)	Services	Node Status
□	ISE31-2	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	SESSION,PROFILER	✓
□	ise31	Administration, Monitoring, Policy Service	PRI(A), PRI(M)	SESSION,PROFILER	✓

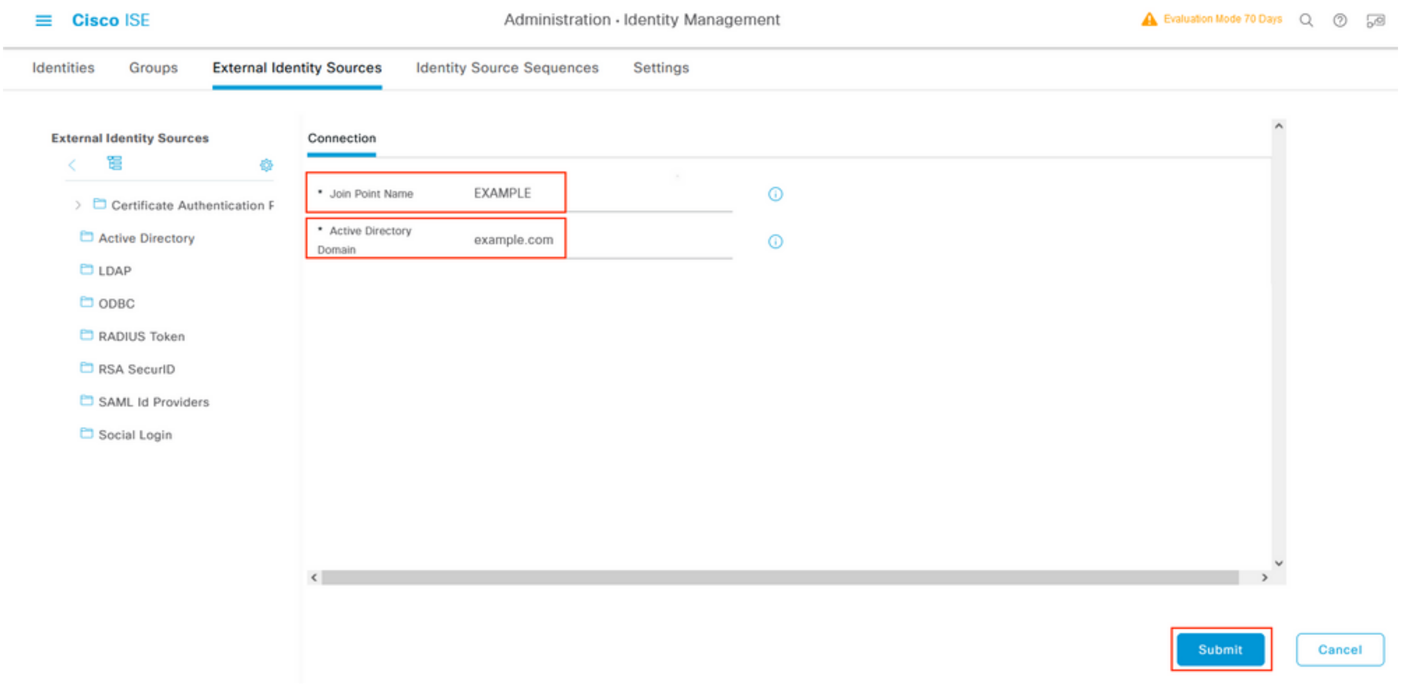
ステップ7:ISE導入とオンプレミスADの統合

[Administration] **> [Identity Management] > [External Identity Sources]** に移動します。**[Active Directory]**を選択し、[追加]を選択します。



□	Join Point Name	Active Directory Domain
		No data available

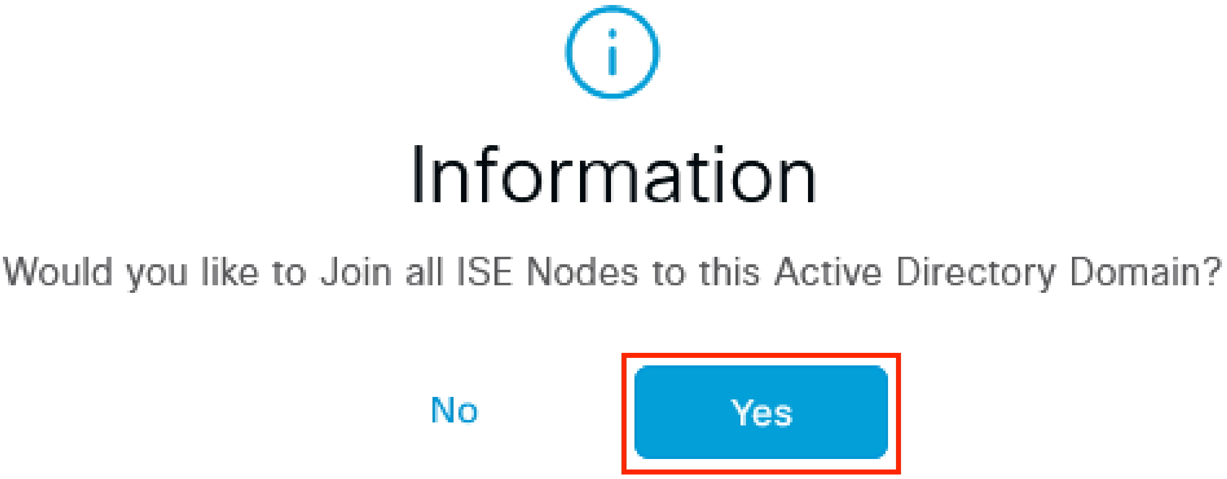
ジョイントポイント名とActive Directoryドメインを設定し、[送信]を選択します。



* Join Point Name EXAMPLE

* Active Directory Domain example.com

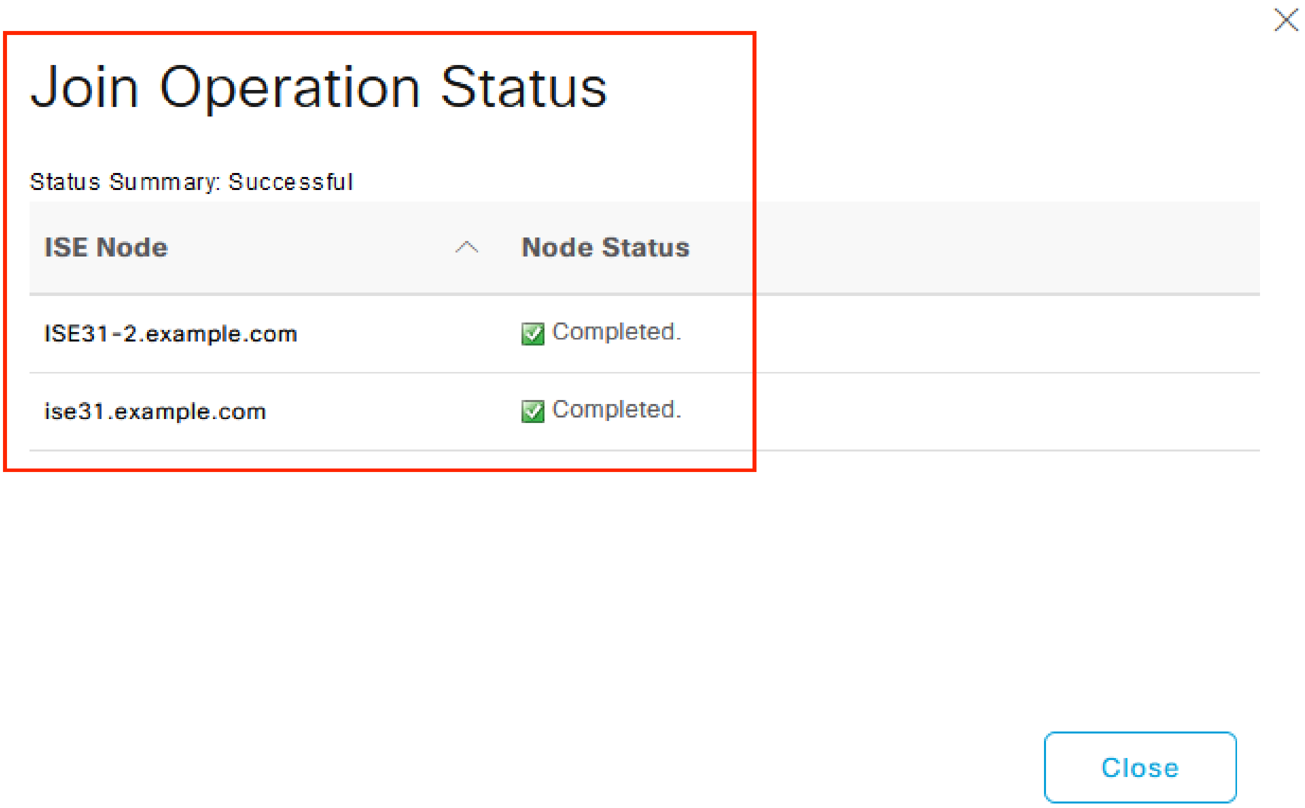
両方のノードをActive Directoryと統合するには、[はい]を選択します。



Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

ADユーザー名とパスワードを入力し、[OK]をクリックします。ISEノードがActive Directoryに正常に統合されると、[Node Status]が[Completed]に変わります。



Join Operation Status

Status Summary: Successful

ISE Node	Node Status
ISE31-2.example.com	✓ Completed.
ise31.example.com	✓ Completed.

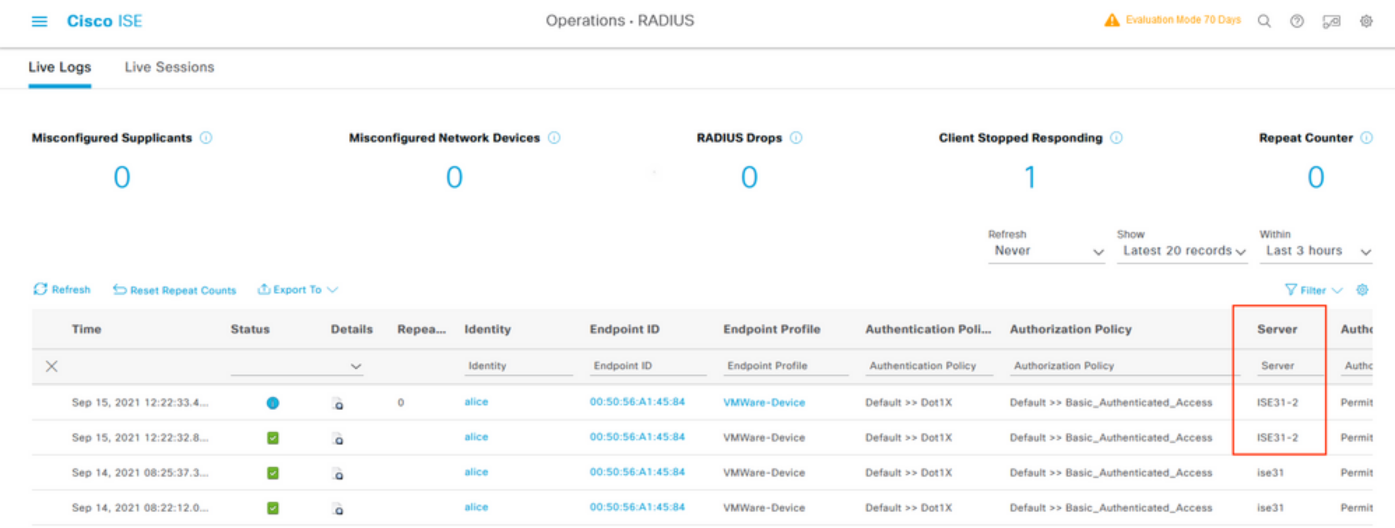
制限

AWSでのISEの制限については、『ISE Admin Guide』の「Known Limitations」セクションを参照してください。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

認証がAWSにあるISE PSNで実行されていることを確認するには、[Operations] > [Radius] > [Live Logs]に移動し、[Server]列でAWS PSNのISEが確認されます。



Misconfigured Supplicants: 0
Misconfigured Network Devices: 0
RADIUS Drops: 0
Client Stopped Responding: 1
Repeat Counter: 0

Refresh: Never
Show: Latest 20 records
Within: Last 3 hours

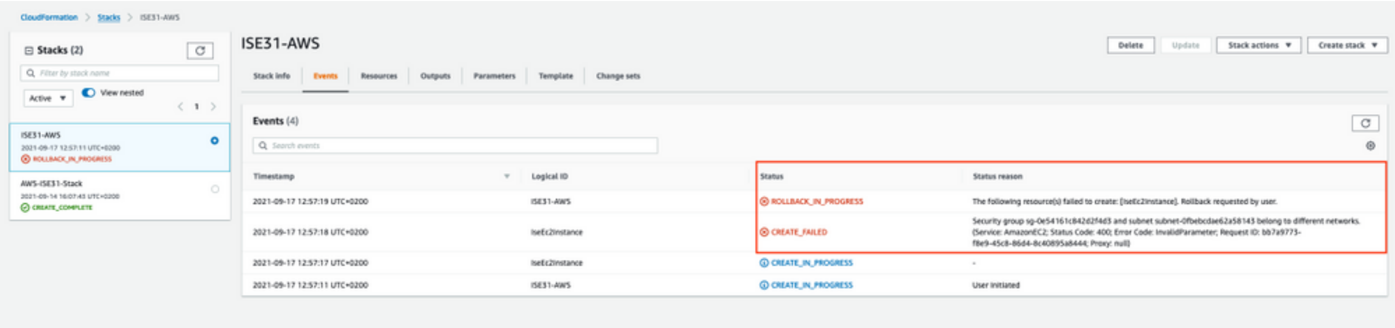
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Poli...	Authorization Policy	Server	Autho
Sep 15, 2021 12:22:33.4...	●		0	alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE31-2	Permit
Sep 15, 2021 12:22:32.8...	✓			alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE31-2	Permit
Sep 14, 2021 08:25:37.3...	✓			alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ise31	Permit
Sep 14, 2021 08:22:12.0...	✓			alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ise31	Permit

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

CloudFormationスタックの作成に失敗しました

CloudFormationスタックの作成は、複数の理由により失敗する可能性があります。そのうちの1つは、ISEの管理ネットワークとは異なるVPNからそのセキュリティグループを選択した場合です。エラーは図の中のエラーのように表示されます。



ISE31-AWS 2021-09-17 12:57:11 UTC+0200 ROLLBACK_IN_PROGRESS

AWS-ISE31-Stack 2021-09-14 16:07:43 UTC+0200 CREATE_COMPLETE

Timestamp	Logical ID	Status	Status reason
2021-09-17 12:57:19 UTC+0200	ISE31-AWS	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [IseEc2Instance]. Rollback requested by user.
2021-09-17 12:57:18 UTC+0200	IseEc2Instance	CREATE_FAILED	Security group sg-0e54161c842d2f4d3 and subnet subnet-0fbebcdae62a58143 belong to different networks. (Service: AmazonEC2; Status Code: 400; Error Code: InvalidParameter; Request ID: bb7a9773-f8e9-45c8-86d4-8c40895a8444; Proxy: null)
2021-09-17 12:57:17 UTC+0200	IseEc2Instance	CREATE_IN_PROGRESS	-
2021-09-17 12:57:11 UTC+0200	ISE31-AWS	CREATE_IN_PROGRESS	User Initiated

ソリューション：

同じVPCからセキュリティグループを選択してください。[VPC Service]の下の**[Security Groups]**に移動し、**[Security Group ID]**に注目し、適切なVPC(ISEが存在する場合**)に対応していることを確認し**、VPC IDを確認します。

接続性の問題

AWS上のISEへの接続が機能しない原因となる問題が複数ある可能性があります。

1.セキュリティグループの設定ミスによる接続**の問題です。**

ソリューション：ISEは、セキュリティグループの設定に誤りがあると、オンプレミスネットワークまたはAWSネットワーク内から**アクセス**できません。必要なプロトコルとポートがISEネットワークに関連付けられたセキュリ**ティグループで許可**されていることを確認してください。開く必要のあるポートについては、『ISEポートリファレンス』を参照してください。

2.ルーティングの設定ミスによる接続の問題

ソリューション：トポロジが複雑なため、オンプレミスネットワークとAWS間のルートを簡単に失うことができます。ISE機能を使用する前に、エンドツーエンド接続が確立されていることを確認します。

付録

スイッチAAA/Radius関連の設定

```
aaa new-model
!
!
aaa group server radius ISE-Group
server name ISE31-2
server name ISE31-1
!
aaa authentication dot1x default group ISE-Group
aaa authorization network default group ISE-Group
aaa accounting dot1x default start-stop group ISE-Group
!
aaa server radius dynamic-author
client 172.18.5.100 server-key cisco
client 10.0.1.100 server-key cisco
!
aaa session-id common
!
dot1x system-auth-control
!
vlan 1805
!
interface GigabitEthernet1/0/2
description VMWIN10
switchport access vlan 1805
switchport mode access
authentication host-mode multi-auth
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
!
interface Vlan1805
ip address 172.18.5.3 255.255.255.0
!
!
radius server ISE31-1
address ipv4 172.18.5.100 auth-port 1645 acct-port 1646
key cisco
!
radius server ISE31-2
address ipv4 10.0.1.100 auth-port 1645 acct-port 1646
key cisco
```