AWS Marketplace를 통해 ISE 3.1 구성

목차

소개

이 문서에서는 AWS(Amazon Web Services)에서 Amazon Machine Images(AMI)를 통해 ISE(Identity Services Engine) 3.1을 설치하는 방법에 대해 설명합니다. 버전 3.1에서 ISE는 CFT(CloudFormation Templates)의 도움을 받아 Amazon Elastic Compute Cloud(EC2) 인스턴스로 구축할 수 있습니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- ISE

- AWS 및 VPC, EC2, CloudFormation과 같은 개념

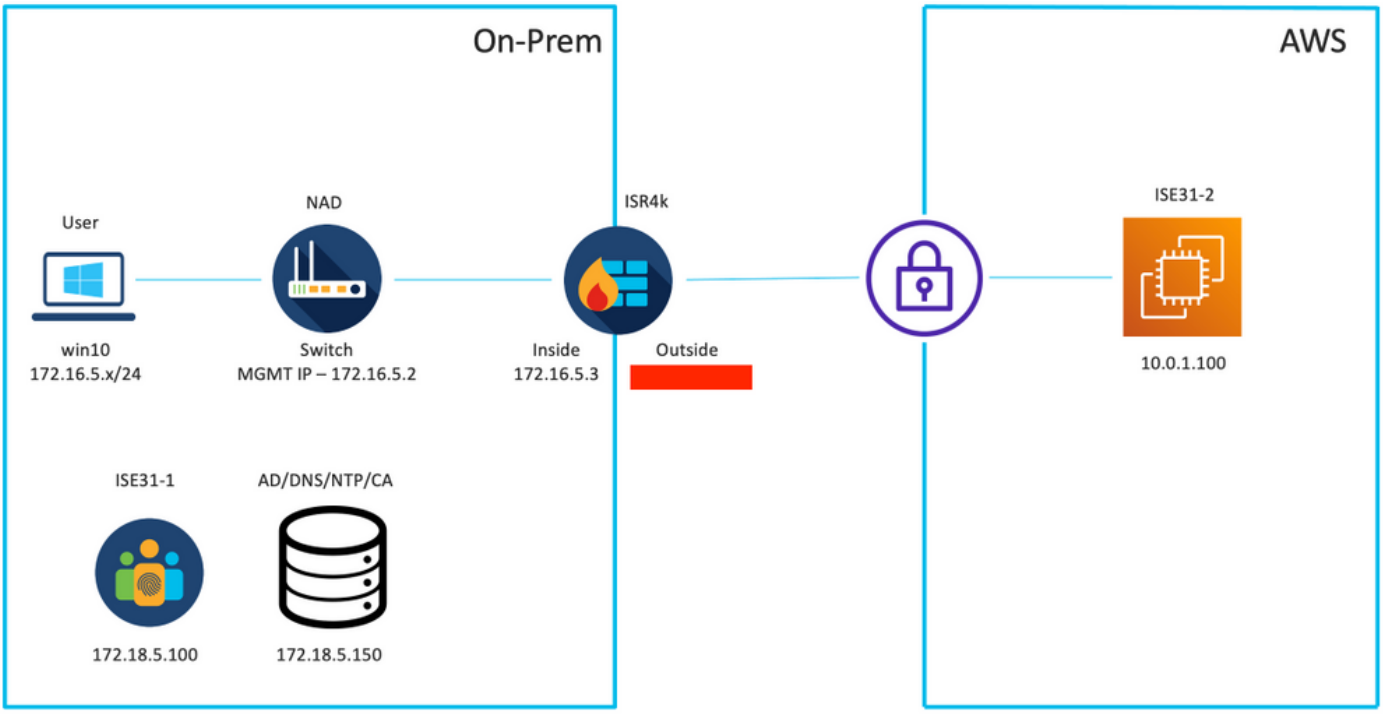
사용되는 구성 요소

이 문서의 정보는 Cisco ISE 버전 3.1을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

네트워크 토폴로지

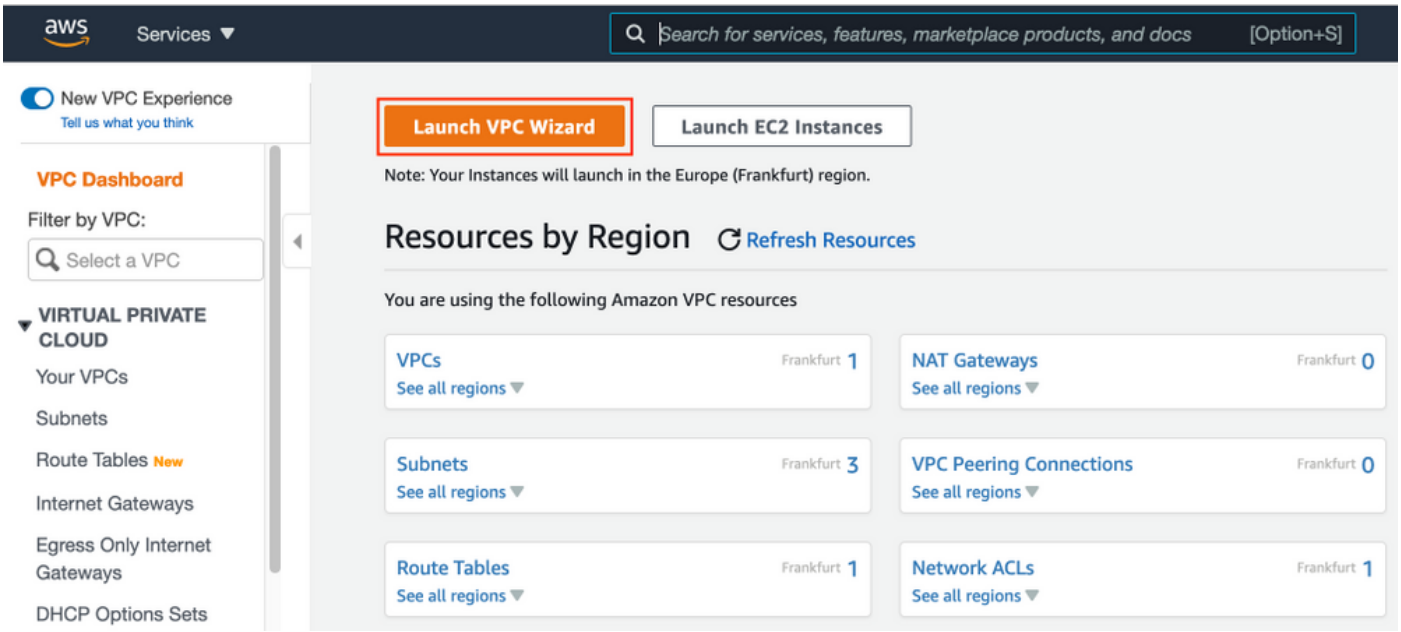


구성

VPC, 보안 그룹, 키 쌍 및 VPN 터널이 아직 구성되지 않은 경우, 옵션 단계를 따라야 하며, 그렇지 않은 경우 1단계로 시작해야 합니다.

선택 단계 A. VPC 생성

VPC AWS Service로 이동합니다. 이미지**에** 표시된 대로 Launch VPC Wizard(VPC 마법사 시작)를 선택합니다.



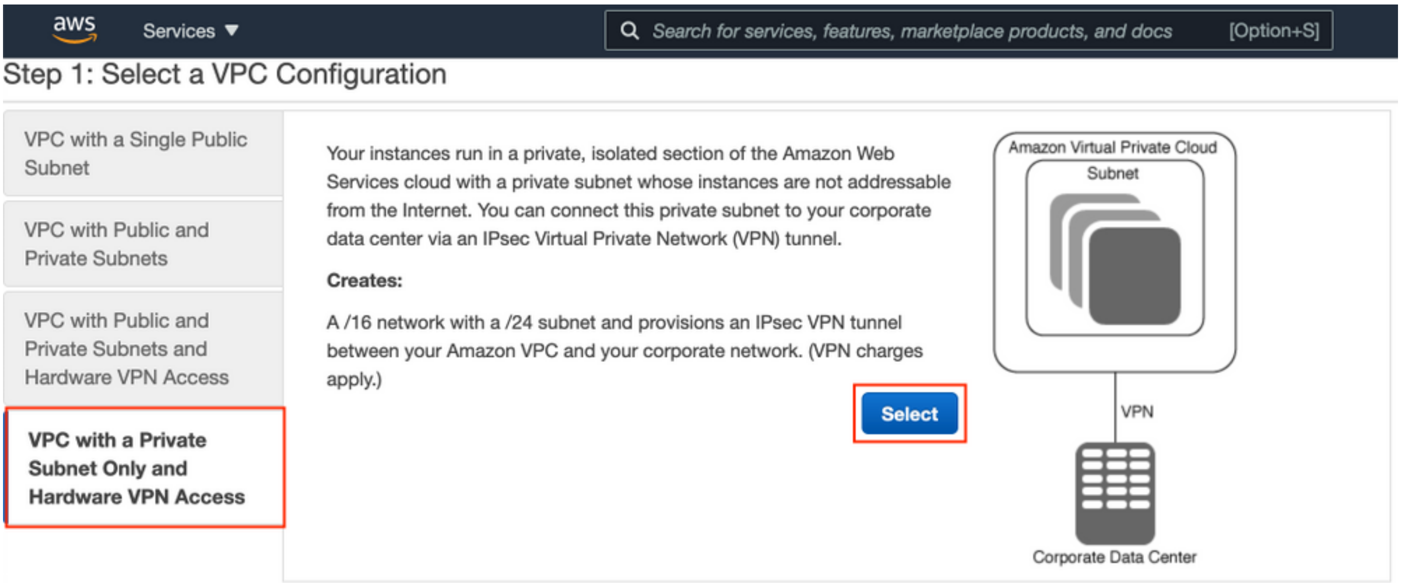
Note: Your Instances will launch in the Europe (Frankfurt) region.

Resources by Region
Refresh Resources

You are using the following Amazon VPC resources

VPCs See all regions ▼	Frankfurt 1	NAT Gateways See all regions ▼	Frankfurt 0
Subnets See all regions ▼	Frankfurt 3	VPC Peering Connections See all regions ▼	Frankfurt 0
Route Tables See all regions ▼	Frankfurt 1	Network ACLs See all regions ▼	Frankfurt 1

프라이빗 **서브넷만 및 하드웨어 VPN 액세스가 있는 VPC**를 선택하고 이미지에 표시된 대로 **선택**을 클릭합니다.


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

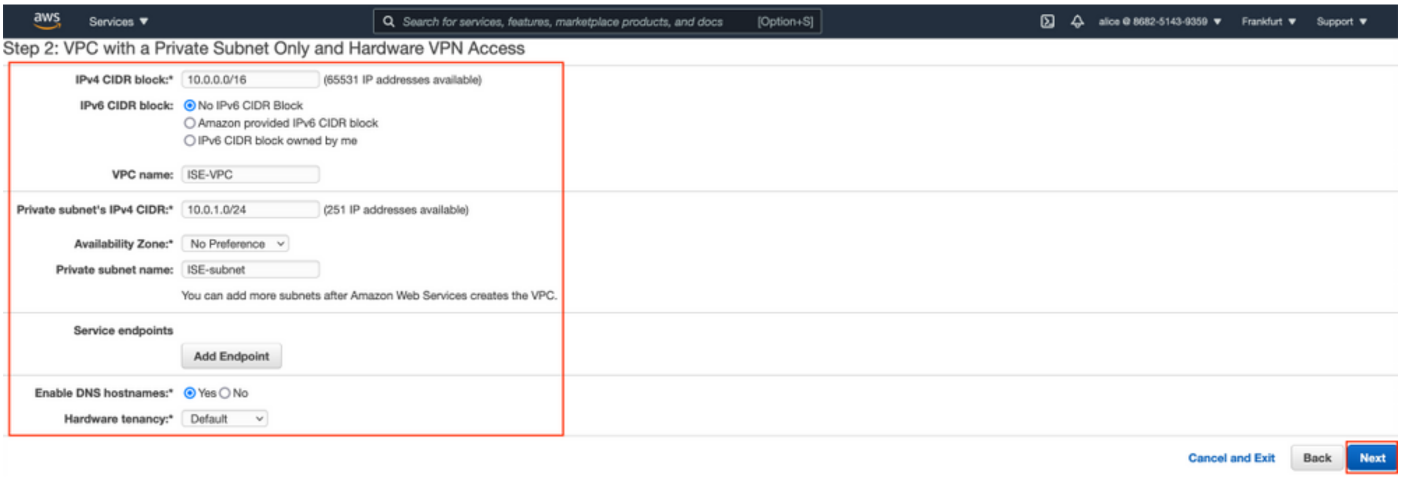
Your instances run in a private, isolated section of the Amazon Web Services cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate data center via an IPsec Virtual Private Network (VPN) tunnel.

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.)

> **참고:** VPC 마법사의 1단계에서 VPC를 선택하는 것은 ISE가 인터넷에 노출된 서버로 설계되지 않았기 때문에 토폴로지에 따라 달라집니다. 프라이빗 서브넷이 있는 VPN만 사용됩니다.

네트워크 설계에 따라 VPC 프라이빗 서브넷 설정을 구성하고 다음을 **선택합니다**.



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

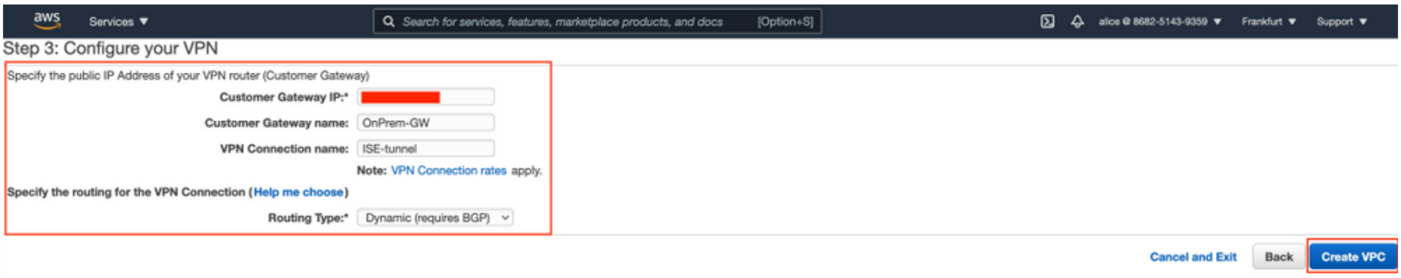
You can add more subnets after Amazon Web Services creates the VPC.

Service endpoints

Enable DNS hostnames:* ● Yes ○ No

Hardware tenancy:* Default

네트워크 설계에 따라 VPN을 구성하고 VPC 생성을 **선택합니다**.



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

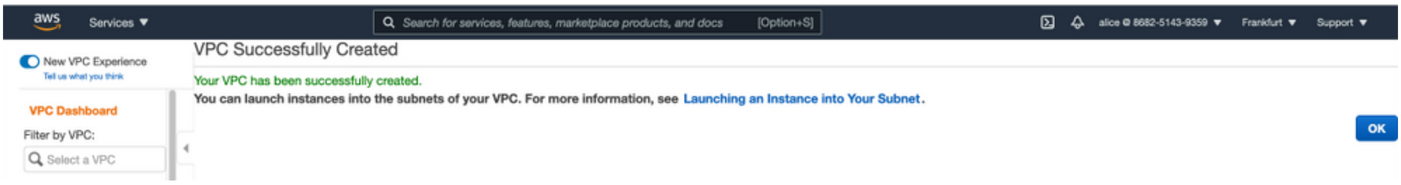
VPN Connection name: ISE-tunnel

Note: VPN Connection rates apply.

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

Routing Type:* Dynamic (requires BGP)

VPC가 생성되면 **"Your VPC has been successfully created"** 메시지가 표시됩니다. 이미지에 표시된 대로 확인을 클릭합니다.



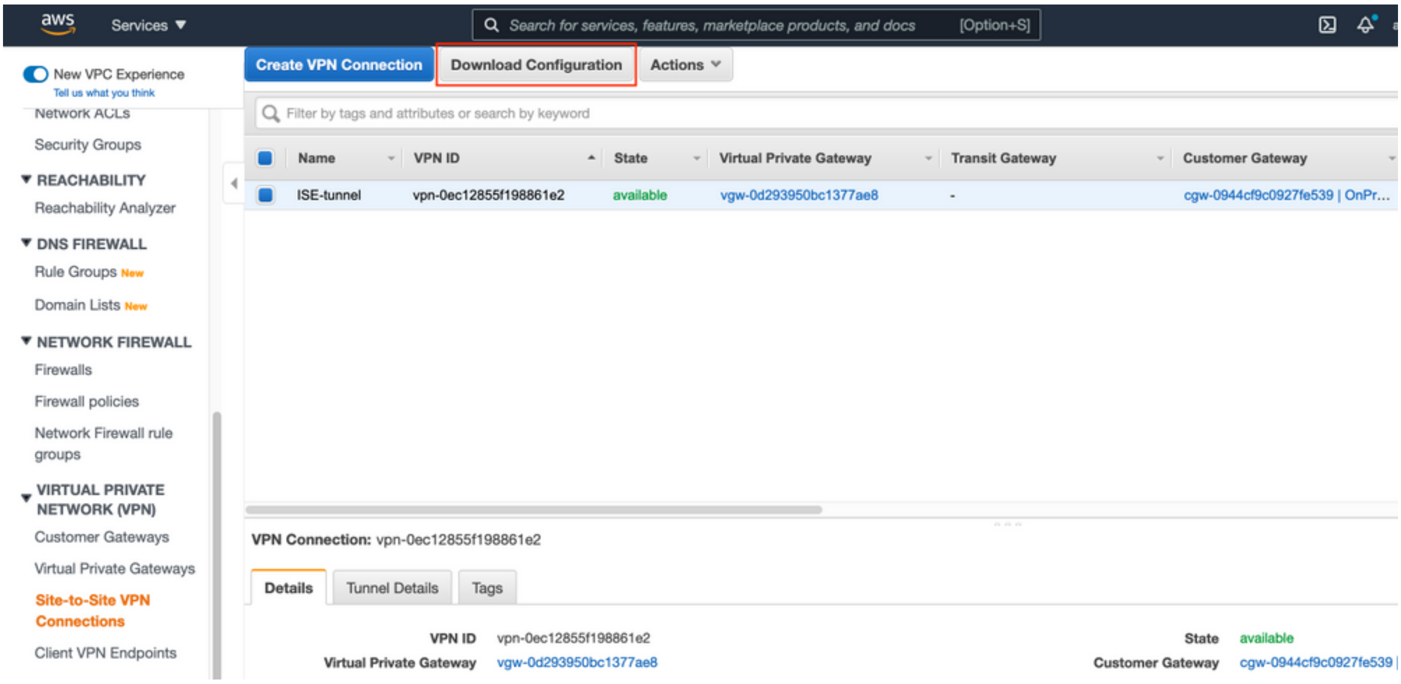
VPC Successfully Created

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.

옵션 단계 B. 온프레미스 VPN 헤드엔드 디바이스 구성

VPC AWS Service로 이동합니다. Site-**to-Site VPN connections(사이트 대 사이트 VPN 연결)**를 선택하고 새로 생성된 VPN 터널을 선택한 다음 이미지에 표시된 대로 **Download Configuration(컨피그레이션 다운로드)**을 선택합니다.



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

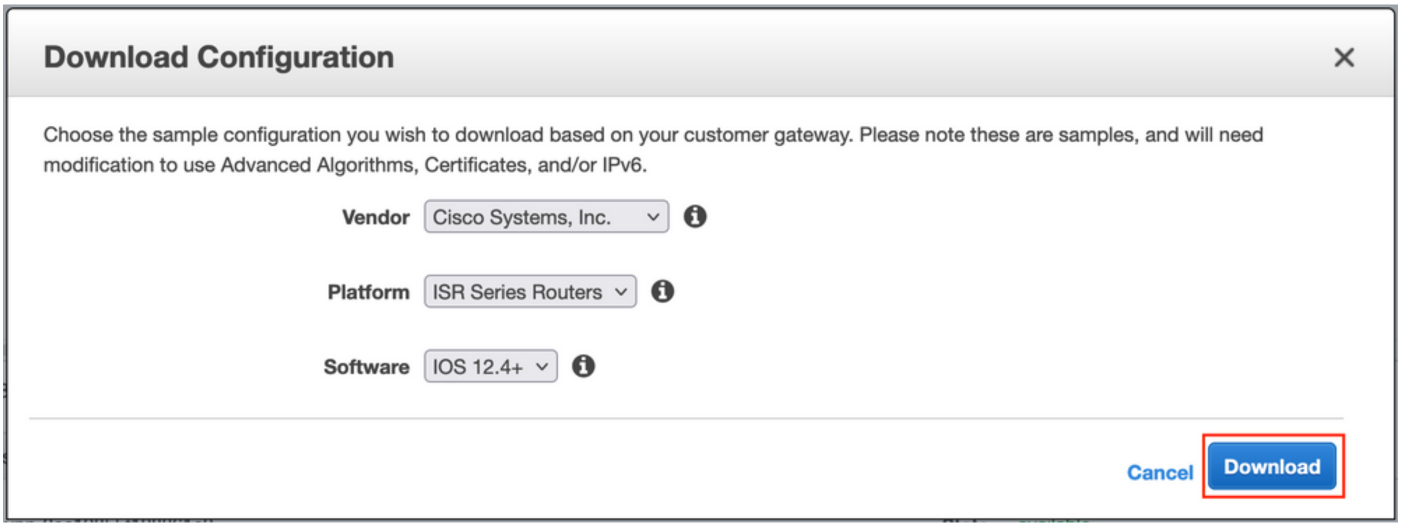
VPN ID vpn-0ec12855f198861e2

Virtual Private Gateway vgw-0d293950bc1377ae8

State available

Customer Gateway cgw-0944cf9c0927fe539 |

이미지에 표시된 대로 **Vendor**, **Platform** and **Software**를 선택하고 **Download**를 선택합니다.



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.

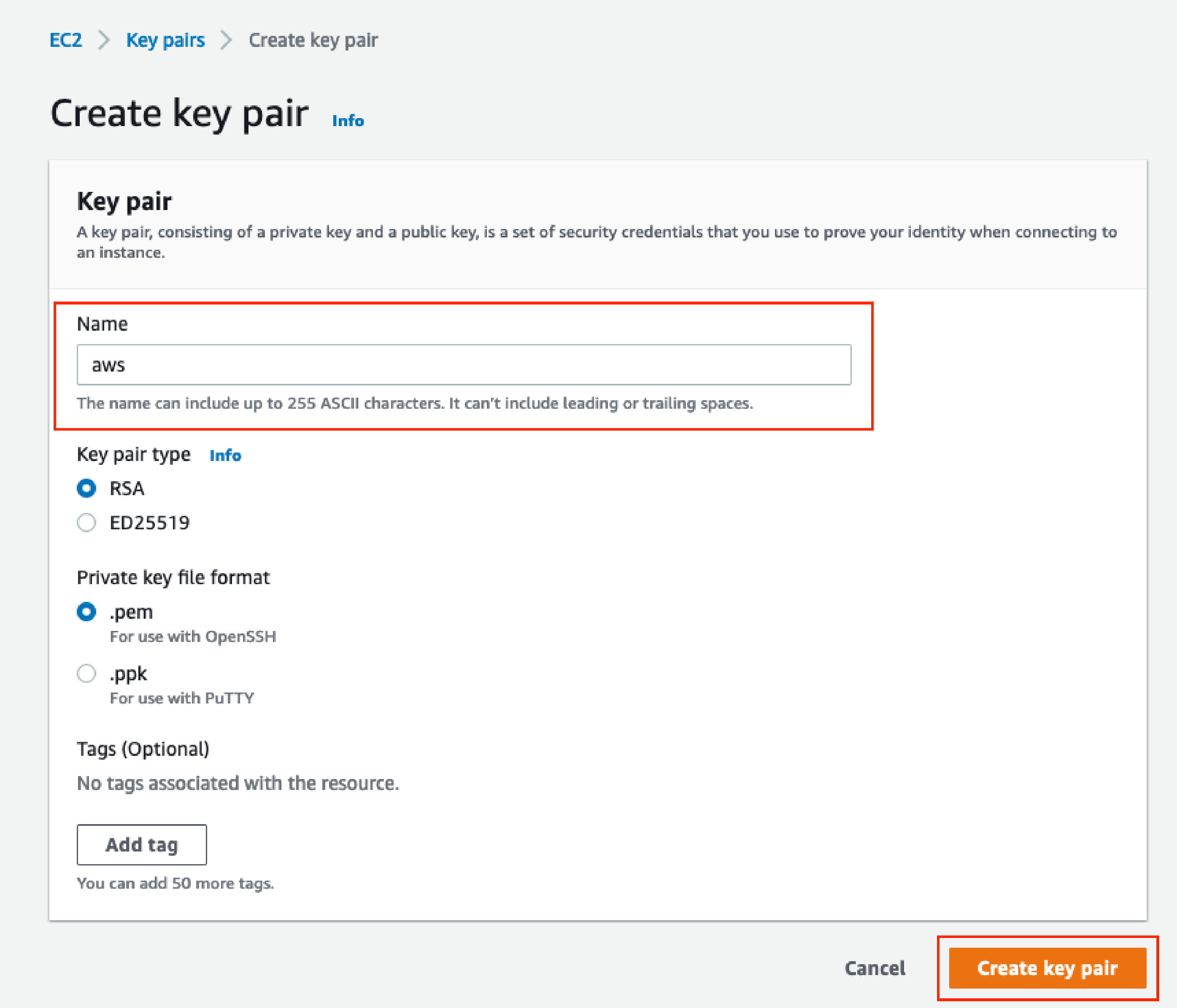
Platform: ISR Series Routers

Software: IOS 12.4+

온프레미스 VPN 헤드엔드 디바이스에 다운로드된 컨피그레이션을 적용합니다.

선택 단계 C. 사용자 지정 키 쌍 만들기

AWS EC2 인스턴스는 키 쌍의 도움을 받아 액세스합니다. 키 쌍을 생성하려면 **EC2** 서비스로 이동합니다. Network **& Security(네트워크 및 보안**)에서 Key Pairs(키 쌍**) 메뉴를 선택합니다.** Create **Key Pair(키 쌍 생성**)를 선택하고 **Name(이름**)을 **지정하고** 다른 값을 기본값으로 유지하고 Create Key Pair(키 쌍 생성)**를** 다시 선택합니다.



EC2 > Key pairs > Create key pair

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.

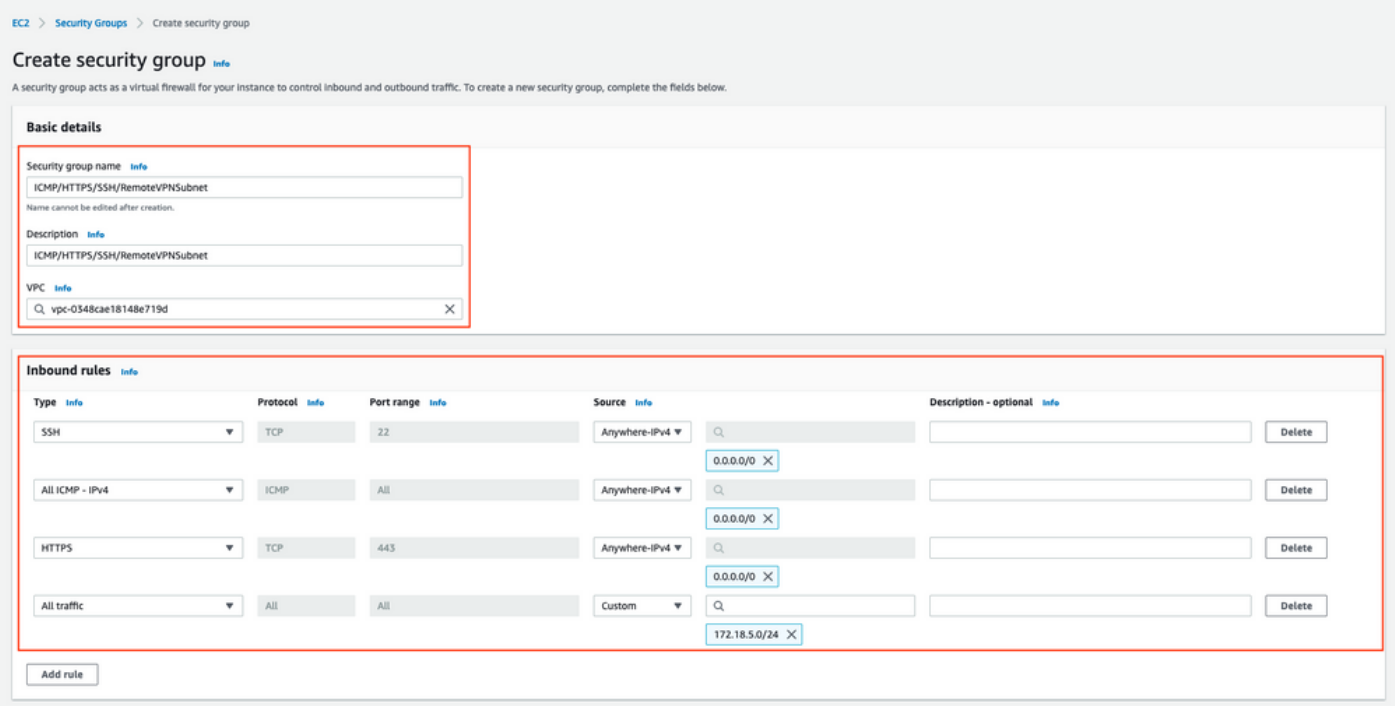
Add tag

You can add 50 more tags.

Cancel | Create key pair

선택 단계 D. 사용자 지정 보안 그룹 생성

AWS EC2 인스턴스 액세스는 **보안 그룹**에 의해 보호되며 **보안 그룹**을 구성하려면 **EC2** 서비스로 이동합니다. Network **& Security**(**네트워크 및 보안**)에서 Security Groups(보안 그룹**) 메뉴를 선택합니다.** Create **Security Group(보안 그룹 생성**)을 선택하고 **Name**(**이름**) **Description(설명)을** 구성합니다. **VPC** 필드에서 새로 구성된 VPC를 **선택합니다.** ISE**와의** 통신을 허용하도록 인바운드 규칙을 구성합니다. 이미지**에** 표시된 대로 Create Security Group을 선택합니다.



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

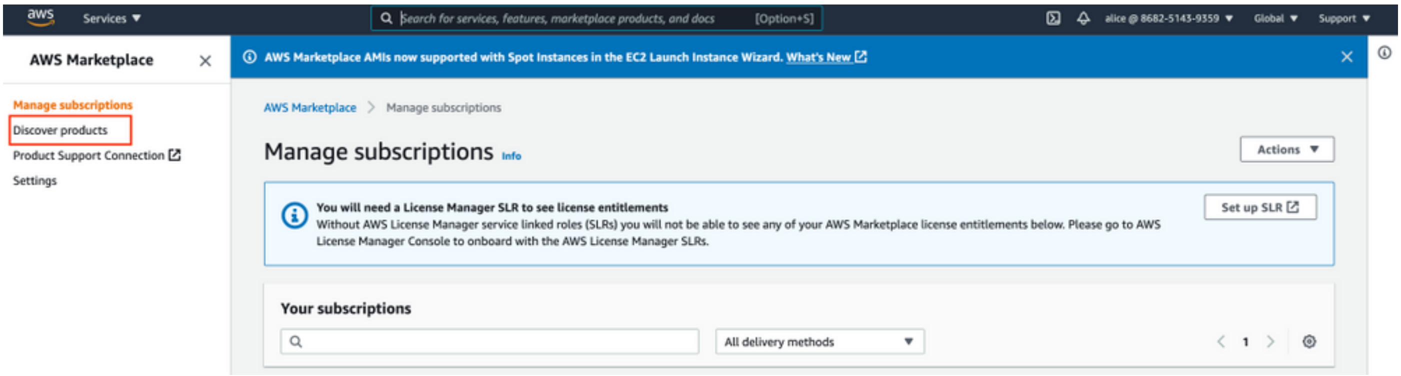
Inbound rules Info

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

참고: 구성된 보안 그룹은 SSH, ICMP, ISE에 대한 HTTPS 액세스 및 온프레미스 서브넷에서 모든 프로토콜 액세스를 허용합니다.

1단계. AWS ISE Marketplace 제품 구독

AWS Marketplace **Subscriptions** AWS Service로 이동합니다. 이미지**에** 표시된 대로 제품 검색을 선택합니다.



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

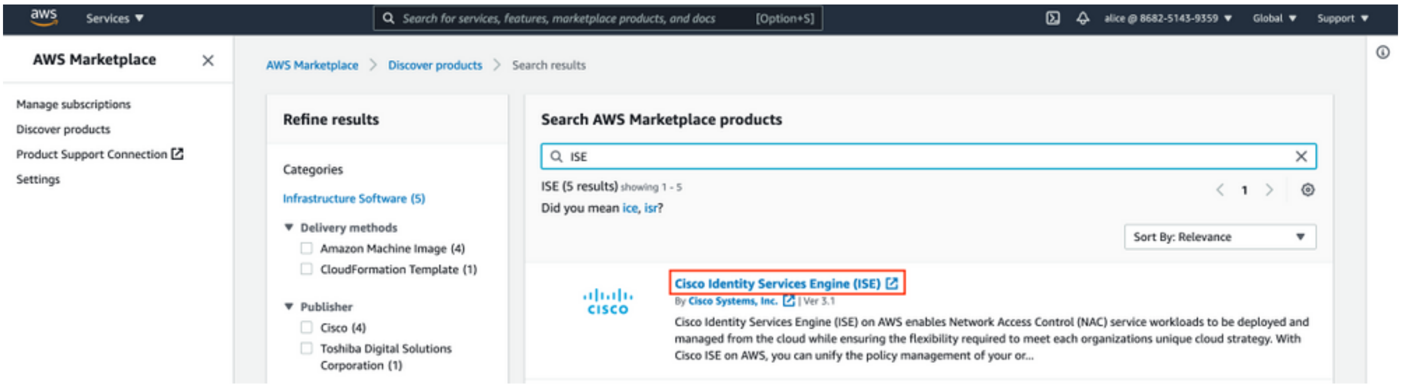
AWS Marketplace > Manage subscriptions

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.

ISE 제품을 검색하고 이미지**에** 표시된 대로 Cisco ISE**(Identity Services Engine)**를 선택합니다.



aws
Services
Search for services, features, marketplace products, and docs [Option+S]
alice @ 8682-5143-9359
Global
Support
AWS Marketplace
Manage subscriptions
Discover products
Product Support Connection
Settings

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
Sort By: Relevance

ISE (5 results) showing 1 - 5

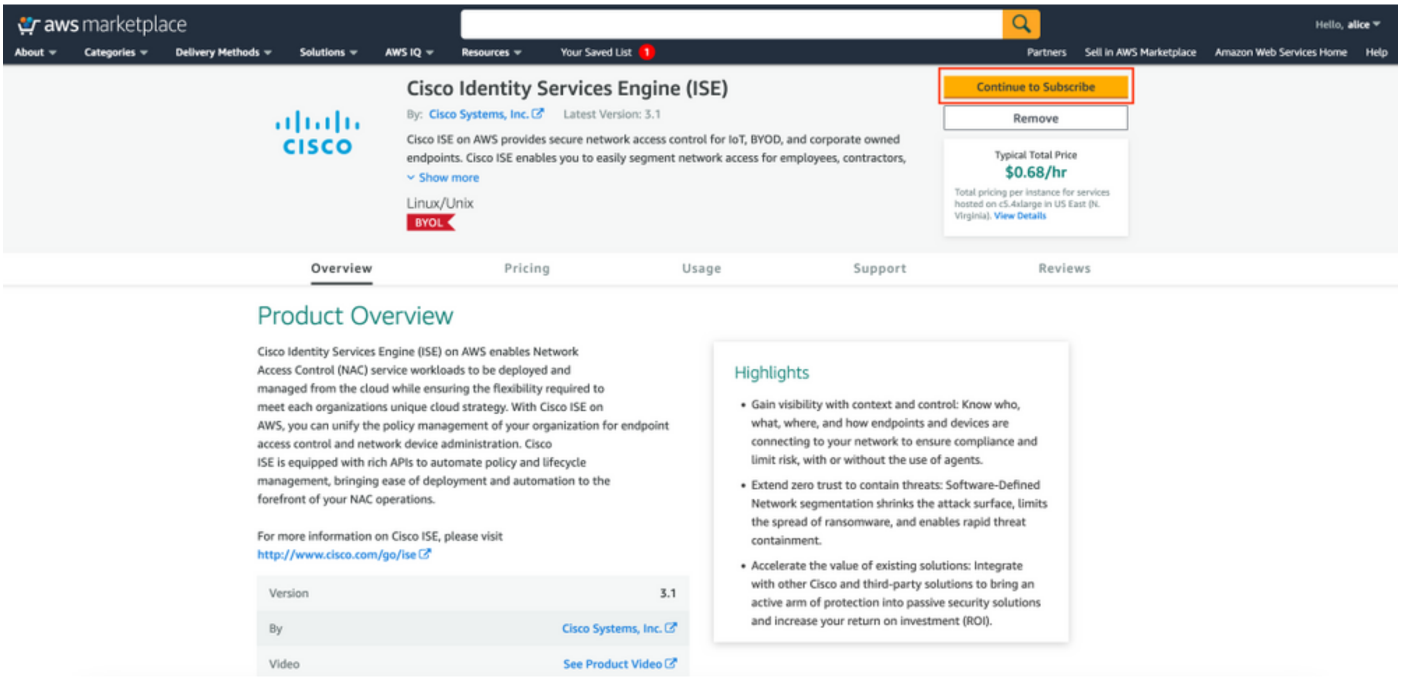
Did you mean ice, isr?

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...

Continue **to Subscribe** 버튼 선택



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,

Linux/Unix

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.

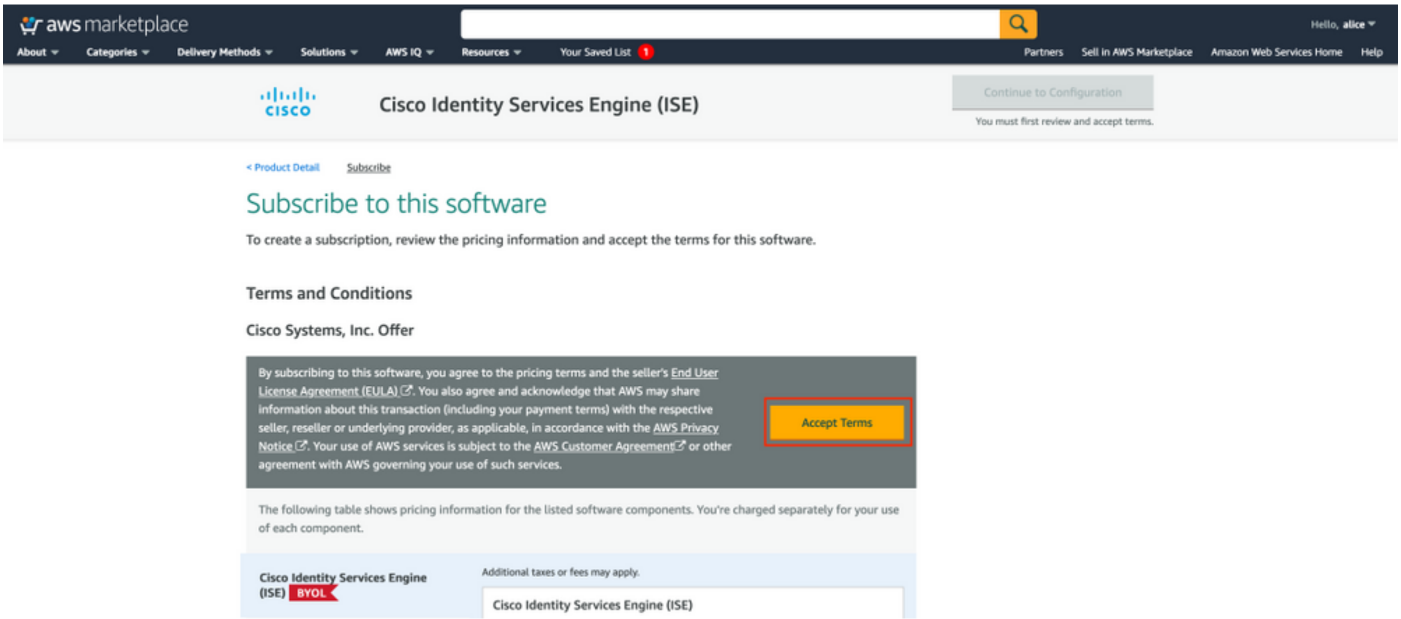
For more information on Cisco ISE, please visit http://www.cisco.com/go/ise

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).

이미지**에** 표시된 대로 조건 수락 버튼을 선택합니다.



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.

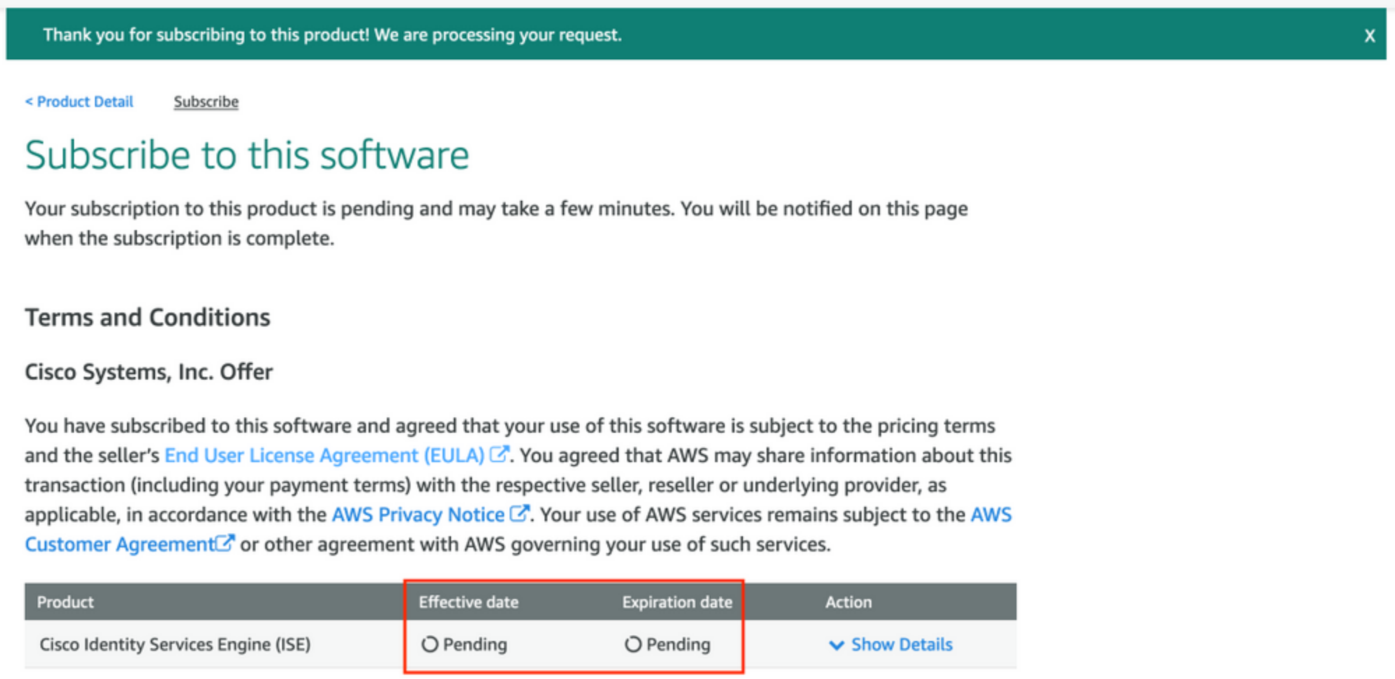
The following table shows pricing information for the listed software components. You're charged separately for your use of each component.

Cisco Identity Services Engine (ISE)

Additional taxes or fees may apply.

Cisco Identity Services Engine (ISE)

일단 가입하면 이미지에 표시된 대로 **유효** 및 **만료일**의 상태를 Pending(**보류**)으로 변경합니다.



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.

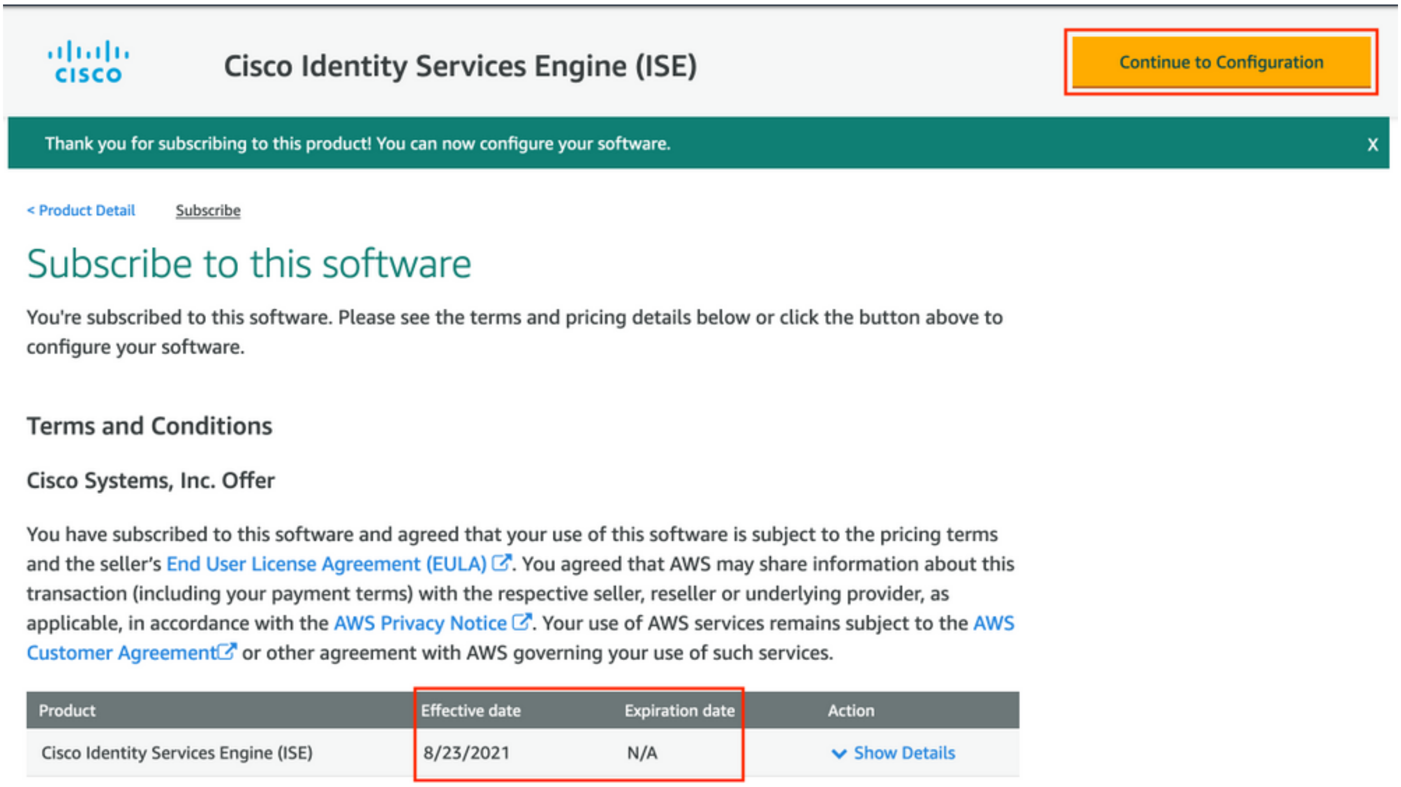
Terms and Conditions

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

유효 일자가 서브스크립션 날짜로 변경되고 **만료 날짜가 N/A**로 **변경된** 직후 이마**에** 표시된 대로 Continue to Configuration을 선택합니다.



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

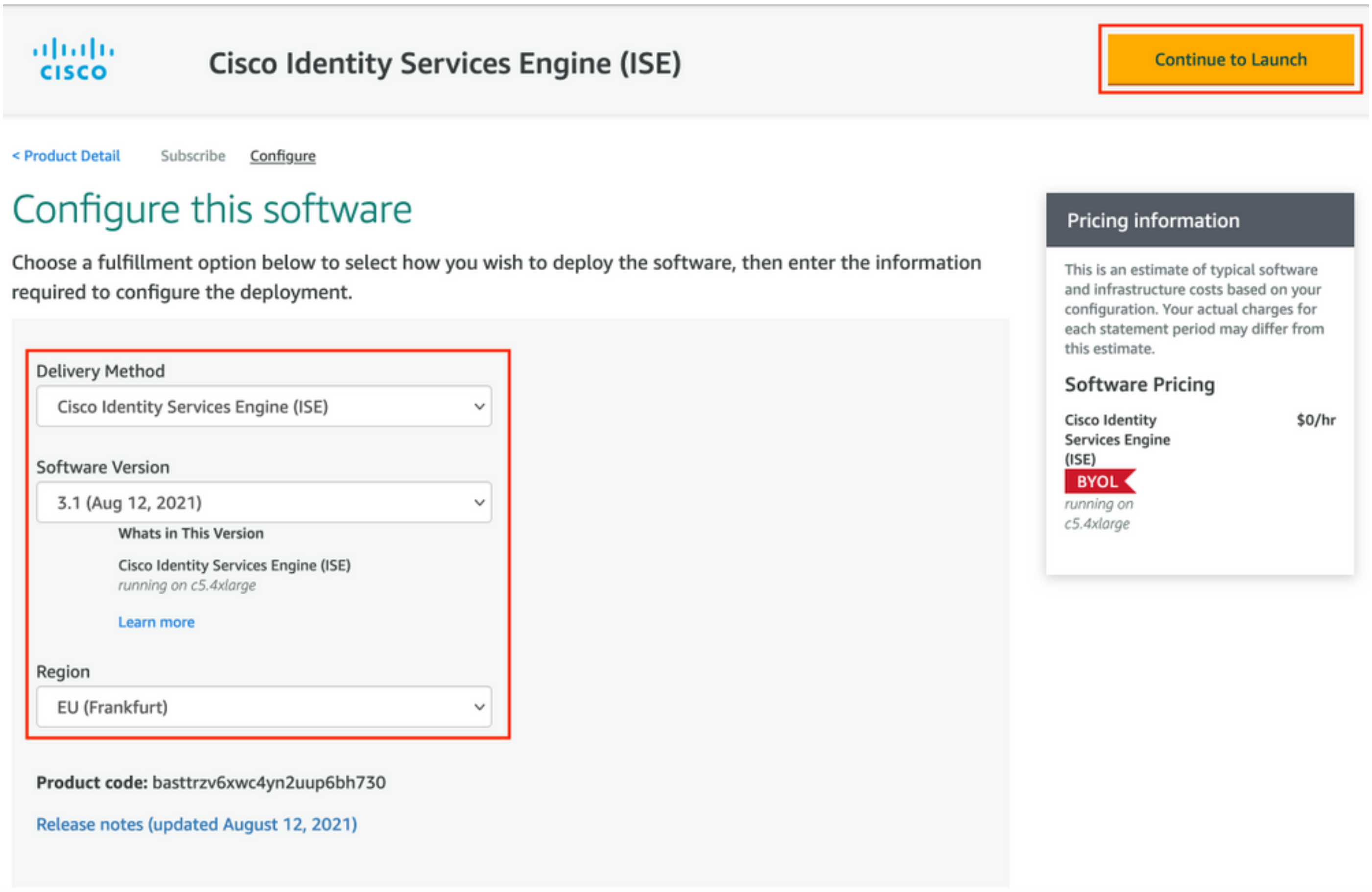
Cisco Systems, Inc. Offer

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

2단계. AWS에서 ISE 구성

Configure this software screen의 Delivery Method 메뉴**에서 Cisco ISE(Identity Services Engine)를** 선택합니다**.** Software Version(**소프트웨어 버전)에서 3.1(2021년 8월 12일)**을 선택합니다. ISE가 구축될 예정인 영역을 선택합니다. Continue **to Launch를 선택합니다.**



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

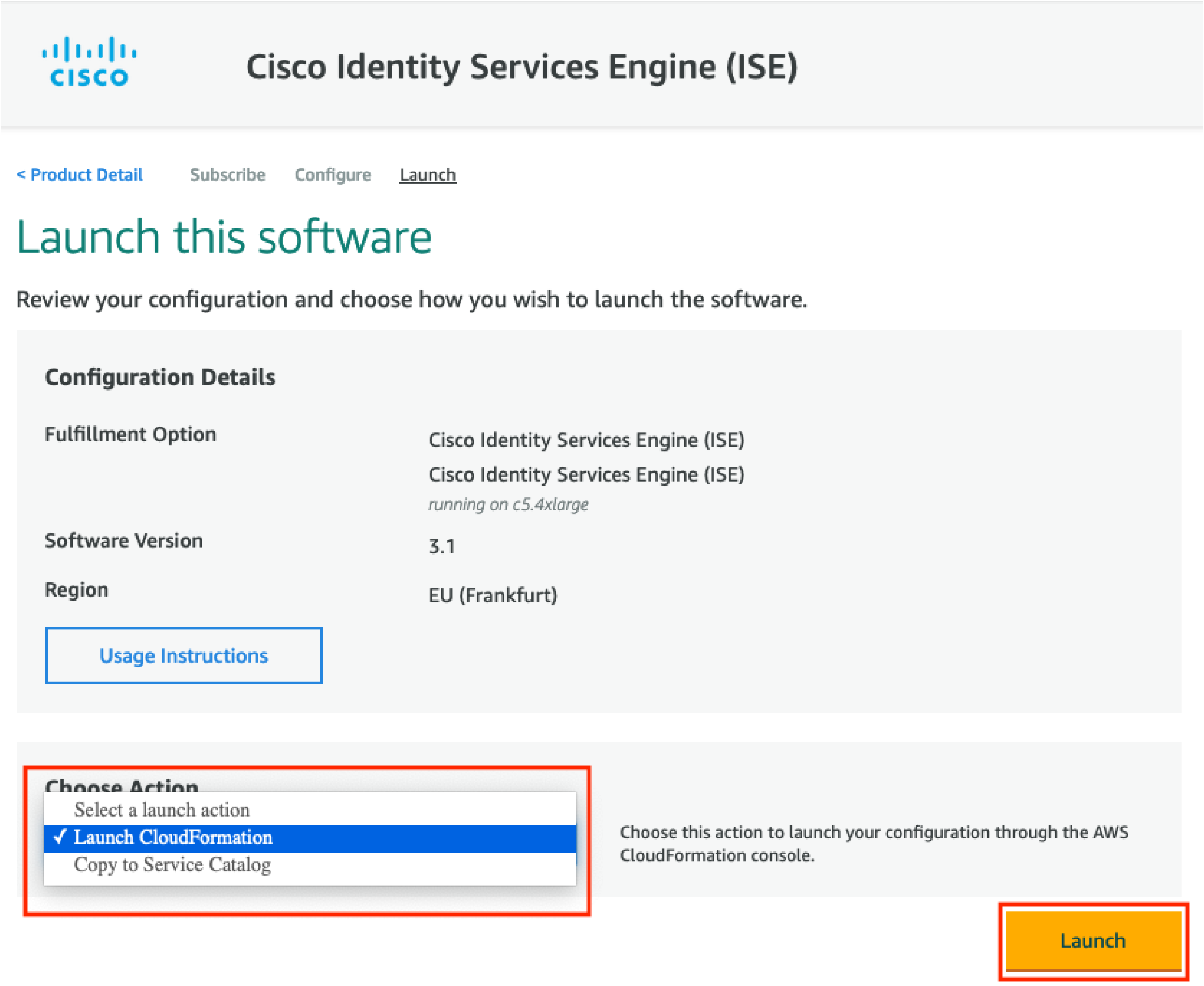
This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

Software Pricing

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

3단계. AWS에서 ISE 시작

Launch this Software 화면의 Actions(작업) 드롭다운 메뉴**에서 Launch CloudFormation(CloudFormation 실행)을 선택합니다**.


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

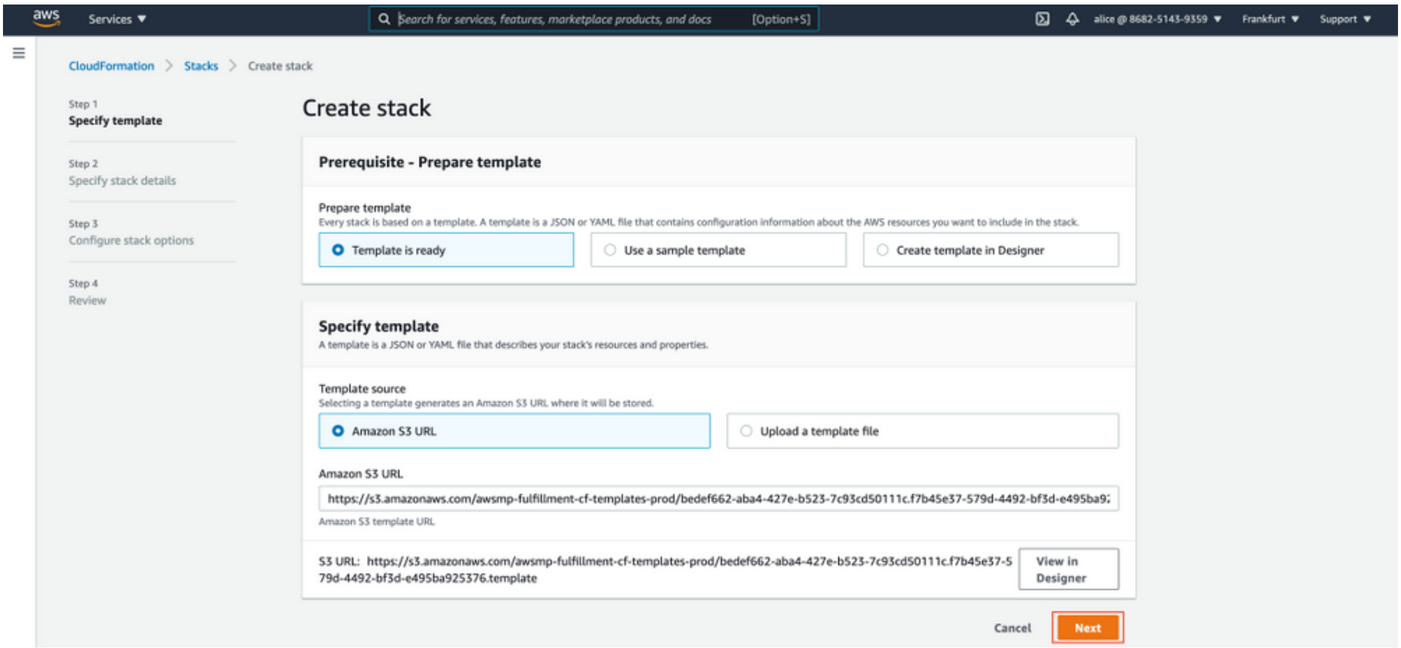
Fulfillment Option	Cisco Identity Services Engine (ISE) Cisco Identity Services Engine (ISE) *running on c5.4xlarge*
Software Version	3.1
Region	EU (Frankfurt)

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

(선택 사항) 사용 **지침**을 선택하여 해당 지침을 숙지하십시오. Launch를 **선택합니다**.

4단계. AWS에서 ISE용 CloudFormation 스택 구성

Launch(시작) 버튼을 누르면 CloudFormation **Stack** 설정 화면**으로** 리디렉션됩니다. ISE를 설정하는 데 반드시 사용해야 하는 미리 작성된 템플릿이 있습니다. 기본 설정을 유지하고 다음을 **선택합니다**.



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.

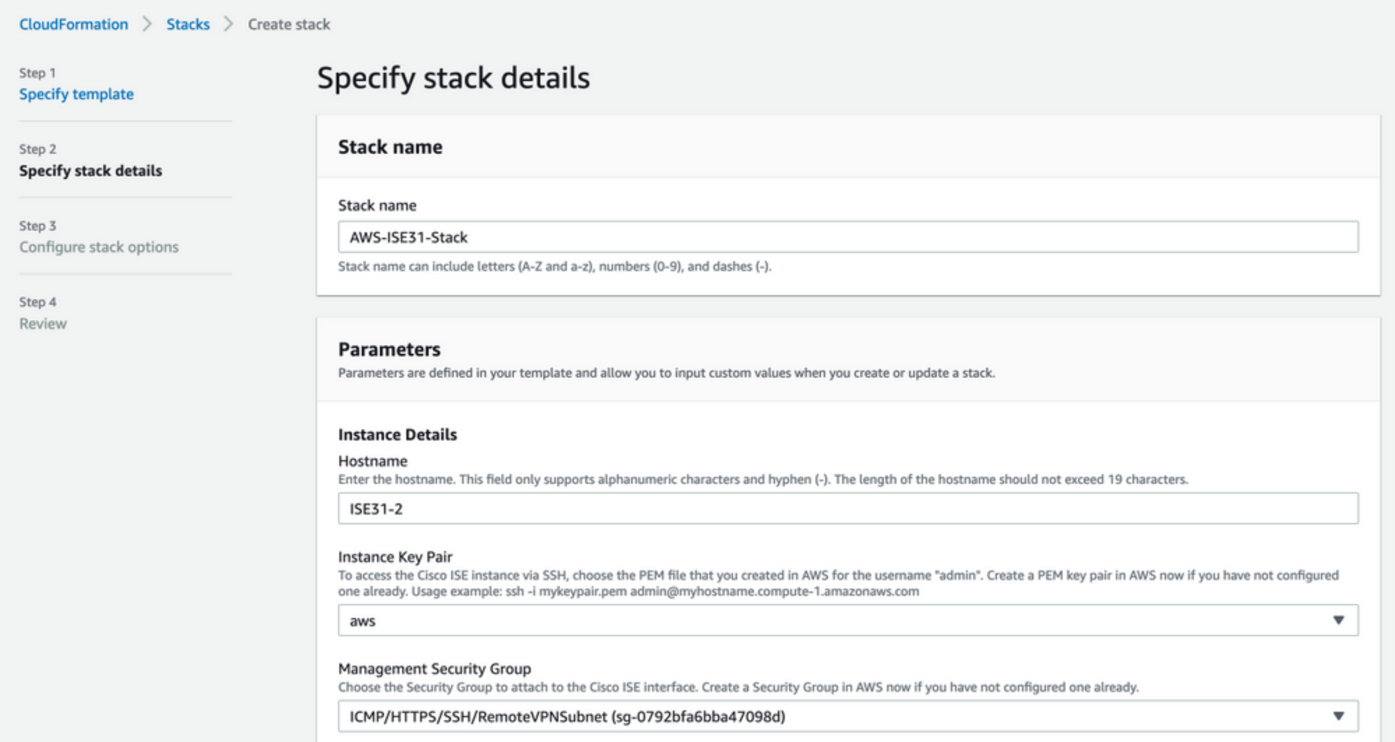
Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

● 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 스택 데이터를 **스택 이름**으로 **채웁니다**. Hostname(호스트 이름)과 같은 인스턴스 **세부 정보**를 구성하고 Instance **Key Pair(인스턴스 키 쌍**) 및 Management Security Group(**관리 보안 그룹)을 선택합니다.**



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.

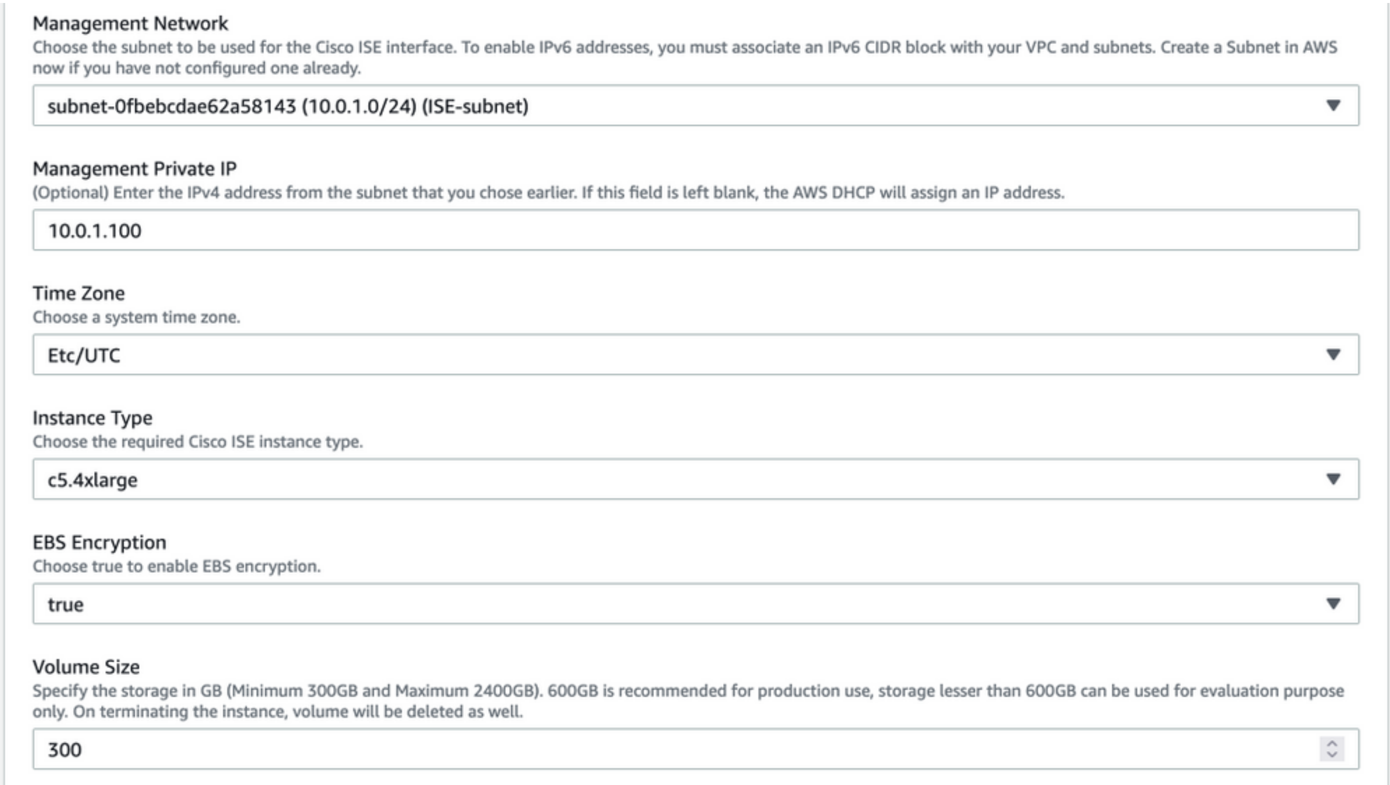
Instance Details

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) ▼

관리 네트워크, 관리 전용 IP, 표준 시간대, 인스턴스 유형, EBS 암호화 및 **볼륨 크기를** 사용하여 인스턴스 세부 정보 구성을 **계속합니다.**



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 ▼

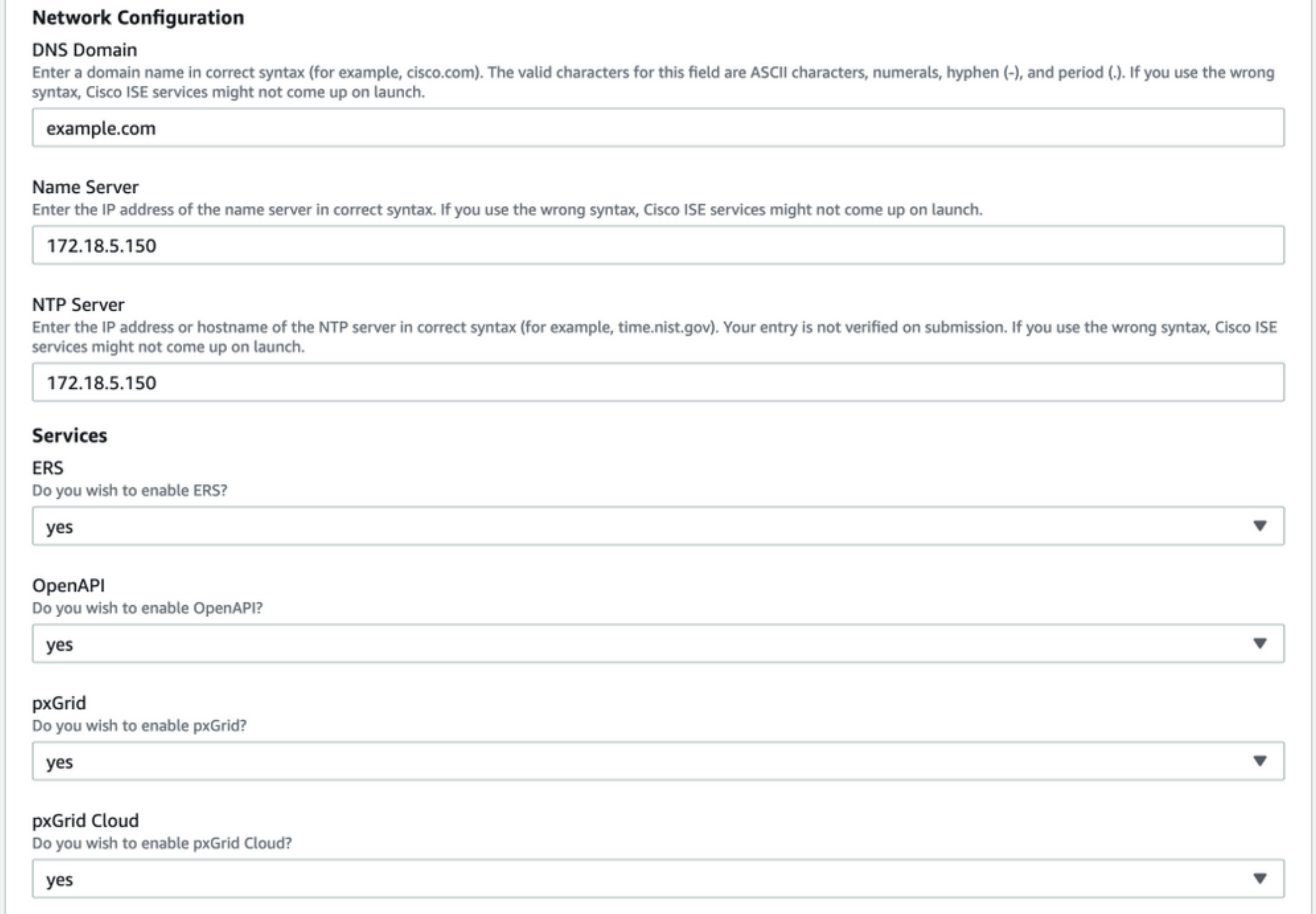
EBS Encryption
Choose true to enable EBS encryption.

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 도메인, 이름 서버, NTP 서비스 및 **서비스**를 사용하여 인스턴스 세부 정보 구성을 **계속합니다**.



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 ▼

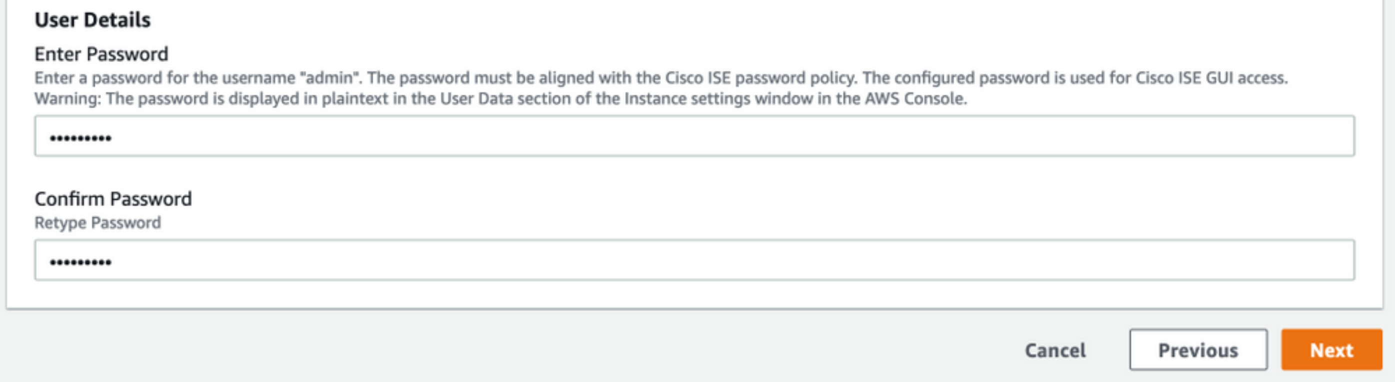
pxGrid
Do you wish to enable pxGrid?

yes ▼

pxGrid Cloud
Do you wish to enable pxGrid Cloud?

yes ▼

GUI 사용자 비밀번호를 구성하고 **Next**를 선택합니다.


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.

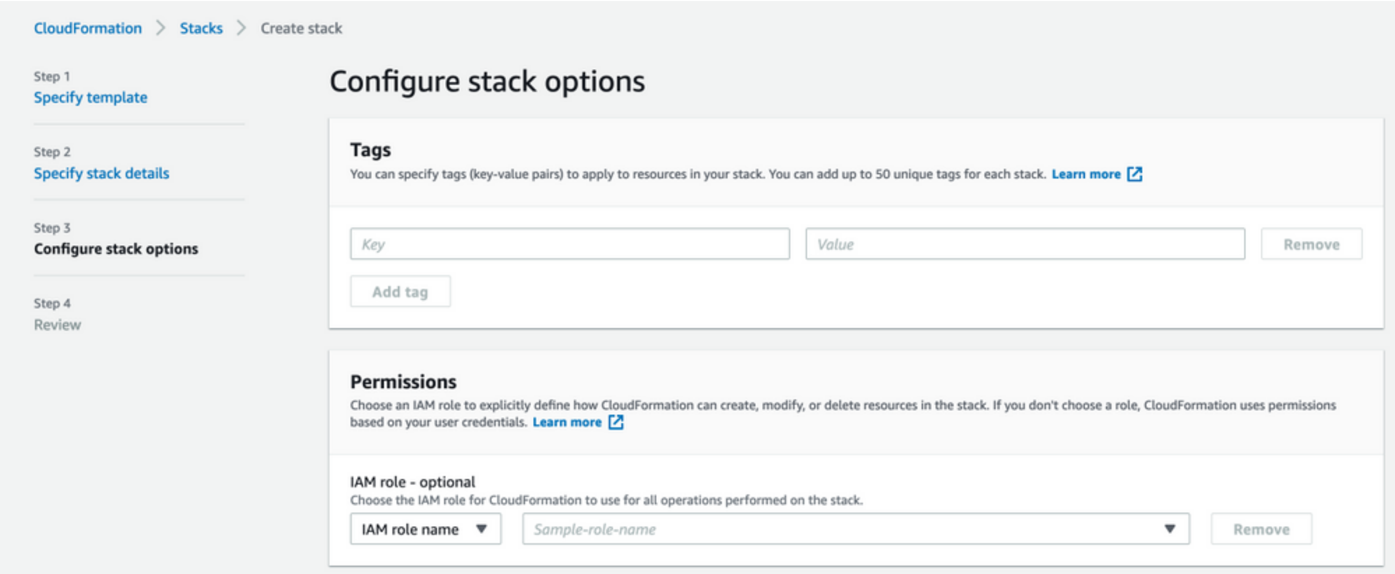
•••••••••

Confirm Password

Retype Password

•••••••••

다음 화면에는 변경이 필요하지 않습니다. 다음을 **선택합니다**.



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

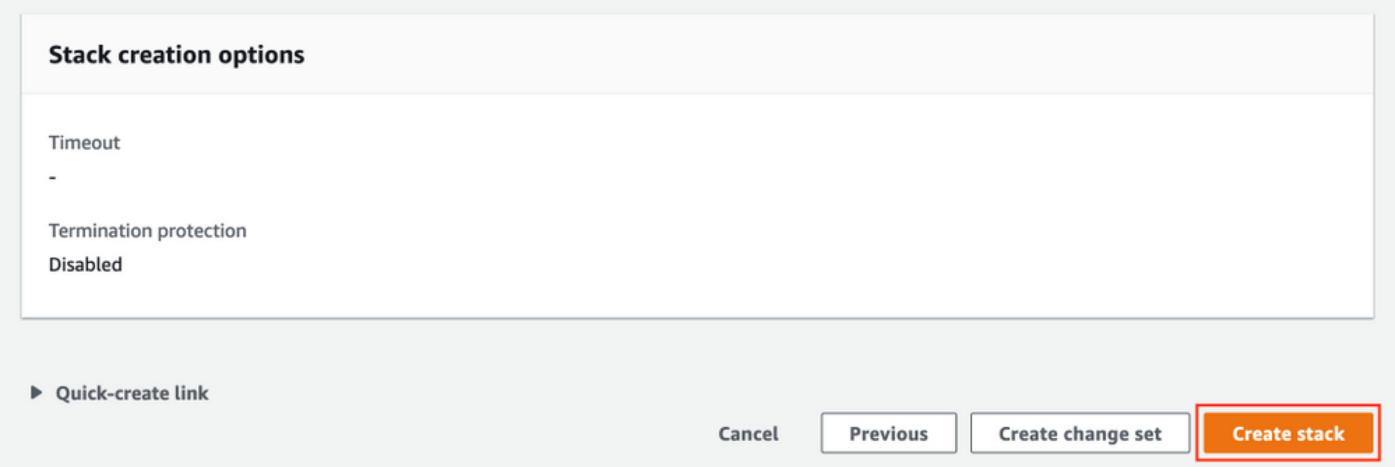
Permissions

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.

Review **Stack** 화면으로 이동하여 아래로 스크롤한 다음 Select **Create stack**.


Stack creation options

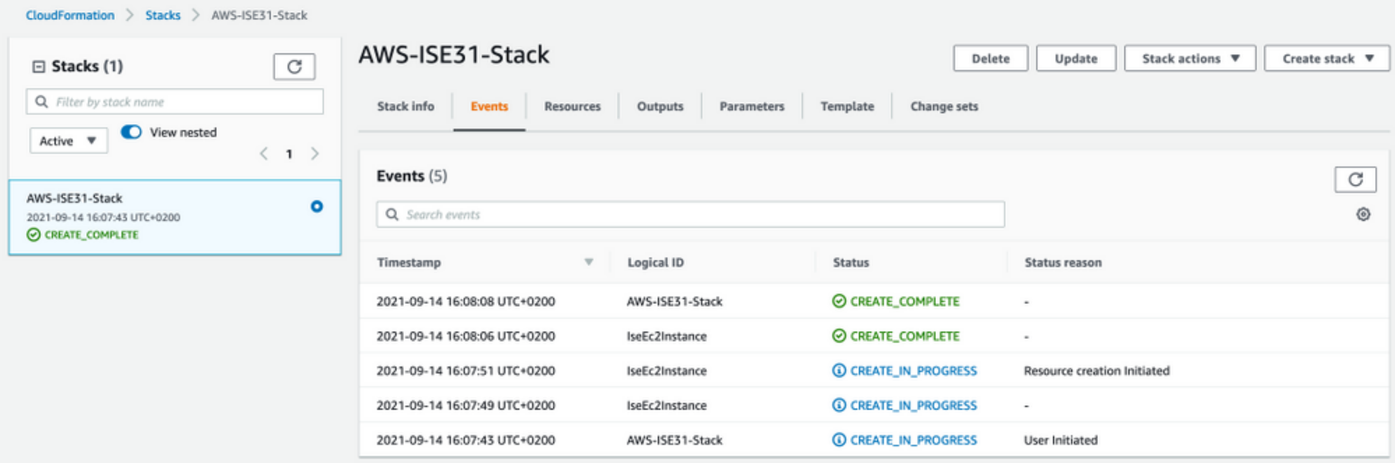
Timeout

-

Termination protection

Disabled

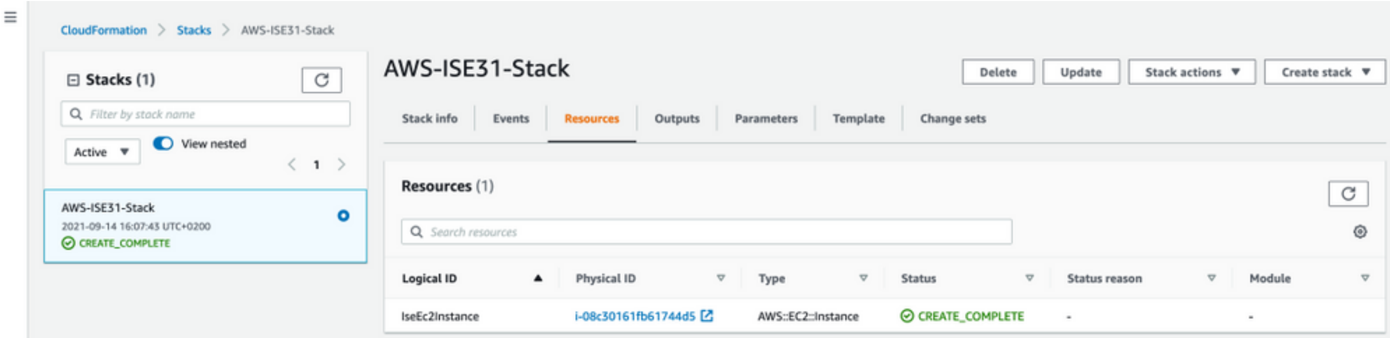
Stack이 구축되면 CREATE_**COMPLETE** 상태를 확인해야 합니다.



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

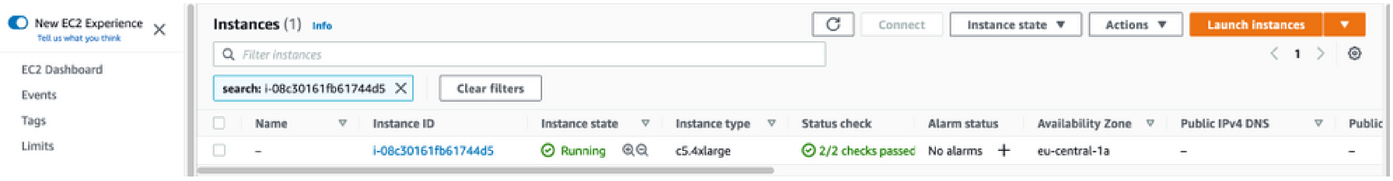
5단계. AWS에서 ISE에 액세스

ISE 인스턴스에 액세스하려면 Resources(**리소스**) 탭으로 이동하여 CloudForms에서 생성된 EC2 인스턴스를 확인합니다(또는 이미지에 표시된 대로 EC2 인스턴스를 보기 위해 **Services(서비스) > EC2 > Instances(EC2 인스턴스)**로 이동합니다.



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

Physical **ID(물리적 ID)**를 선택하여 **EC2 Instances** 메뉴를 엽니다. 상태 **확인**에 **2/2 검사**가 통과되었는지 확인합니다.



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	-	-

인스턴스 **ID를 선택합니다**. ISE는 SSH 또는 HTTPS 프로토콜을 사용하여 **사설 IPv4 주소/개인 IPv4 DNS**를 통해 액세스할 수 있습니다.

> **참고:** Private IPv4 **address/Private IPv4 DNS를** 통해 ISE에 액세스하는 경우 ISE 프라이빗 주소에 대한 네트워크 연결이 있는지 확인합니다.

SSH를 통해 개인 IPv4 **주소**를 통해 액세스되는 ISE의 예:

```
[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#
```

> **참고:** SSH를 통해 ISE에 액세스하는 데 약 20분이 걸립니다. ISE에 대한 연결이 "**권한**이 **거부됨(publickey)"**과 함께 실패할 때까지**는**. 오류 메시지.

서비스**가** 실행 중인지 확인하려면 show application status ise를 사용합니다.

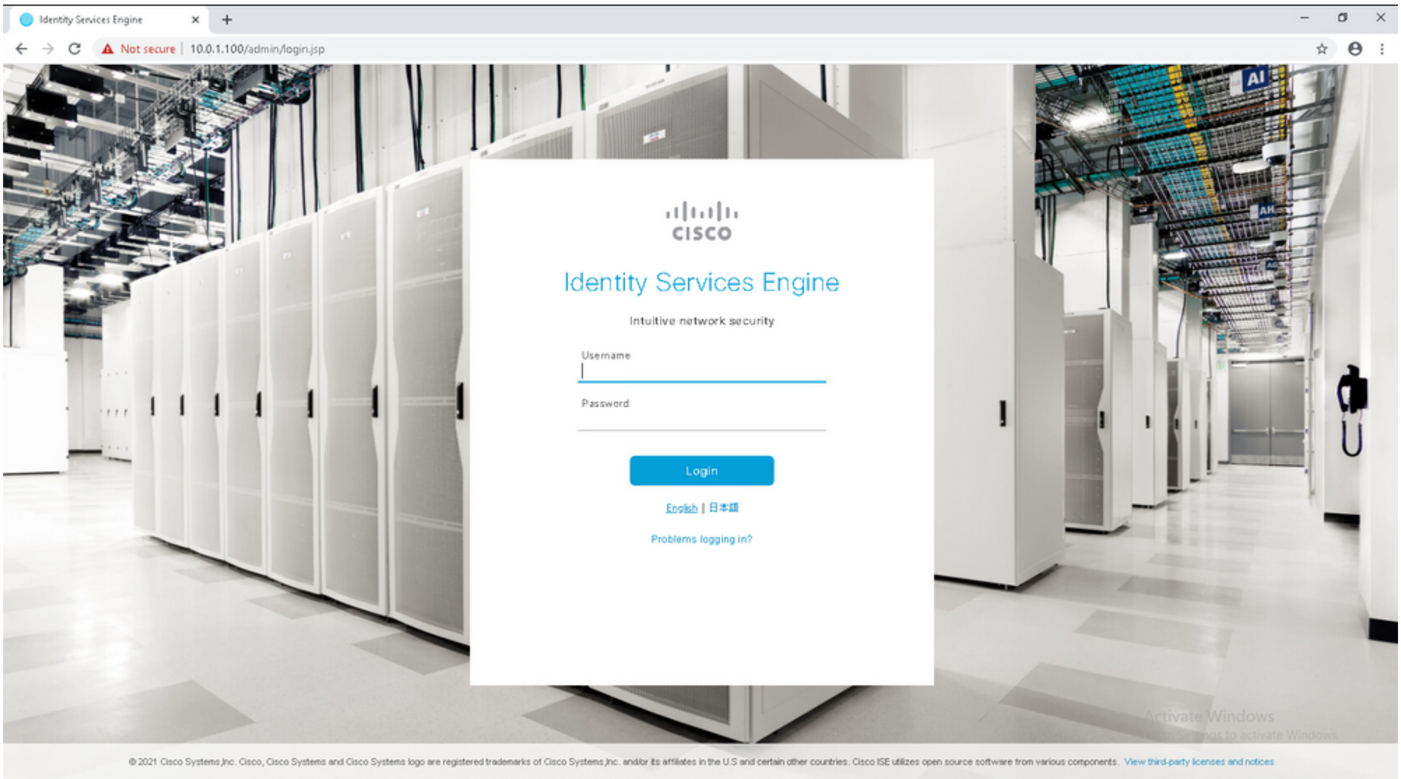
```
ISE31-2/admin# show application status ise

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#
```

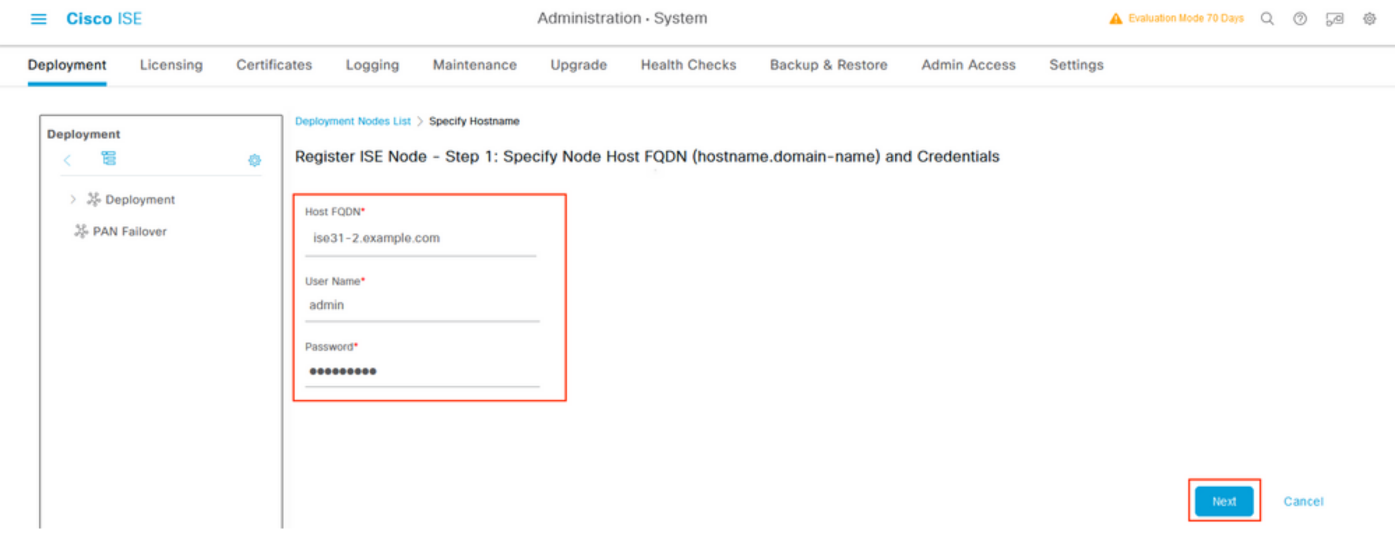
> **참고:** ISE 서비스가 실행 중인 상태로 전환하기 위해 SSH를 사용할 수 있으므로 약 10-15분이 소요됩니다.

애플리케이션 **서버**가 **실행** 중인 경우 이미지에 표시된 대로 GUI를 통해 ISE에 액세스할 수 있습니다.


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
Activate Windows

6단계. AWS에서 온프레미스 ISE와 ISE 간에 분산 배포를 구성합니다.

On-Prem ISE에 로그인하고 Administration(관리) > **System(시스템) > Deployment(구축)로 이동합니다.** 노드를 선택하고 Make Primary(기본 노드 **만들기)를 선택합니다.** Administration(관리) **> System(시스템) > Deployment(구축)로** 다시 이동하고 Register(**등록**)를 **선택합니다**. AWS, GUI **사용자 이름** 및 비밀번호에서 ISE의 **호스트 FQDN**을 **구성합니다.** 다음을 **클릭합니다.**



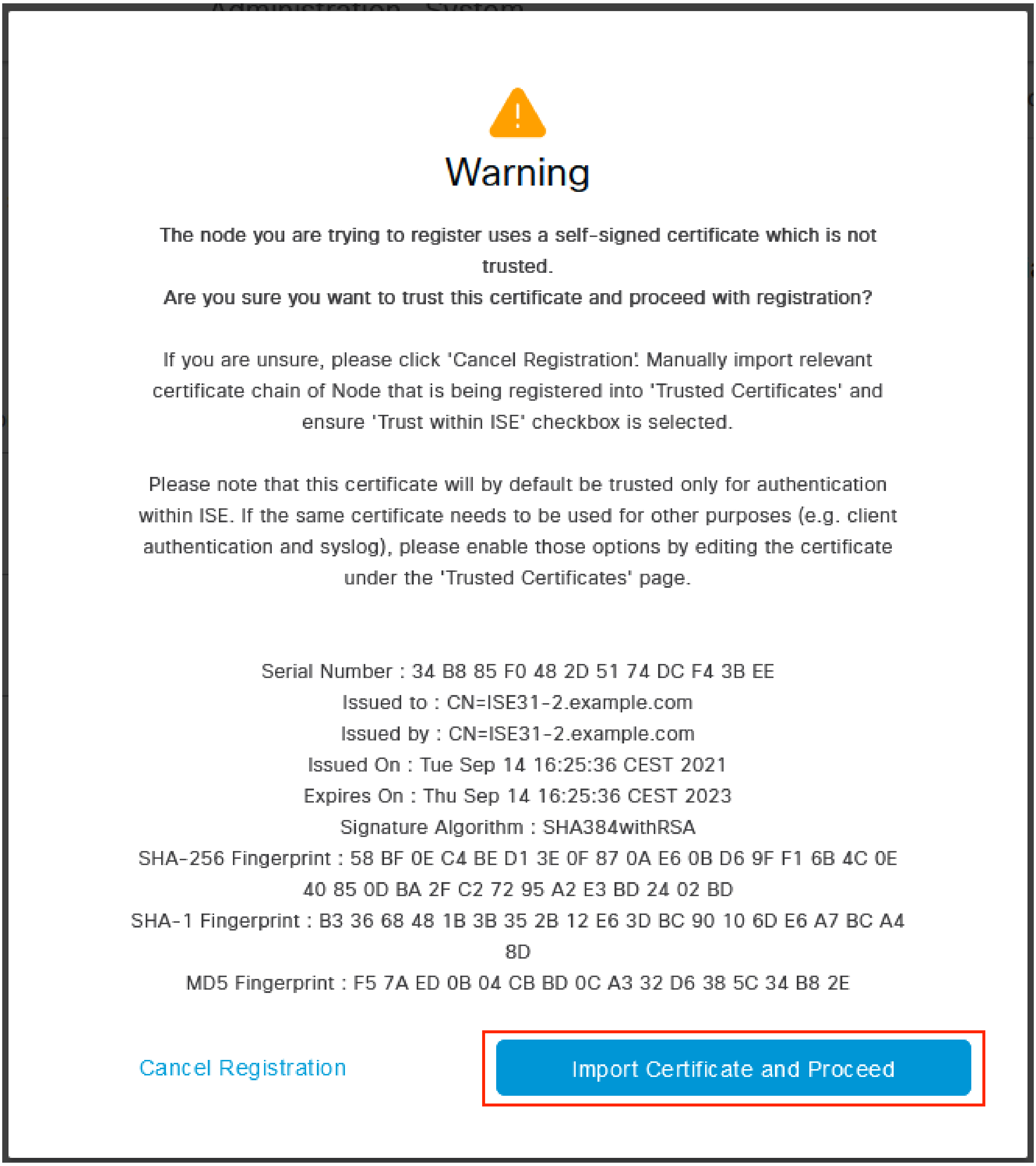
Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

Host FQDN*: ise31-2.example.com

User Name*: admin

Password*: ●●●●●●●●●

이 토폴로지에서는 자체 서명 인증서가 사용되므로, 관리자 인증서를 Trusted Store Select Import Certificate and Proceed(신뢰할 수 있는 저장소 선택 인증서 가져오기 **및 계속)로 교차 가져오기**에 **사용합니다.**



Warning

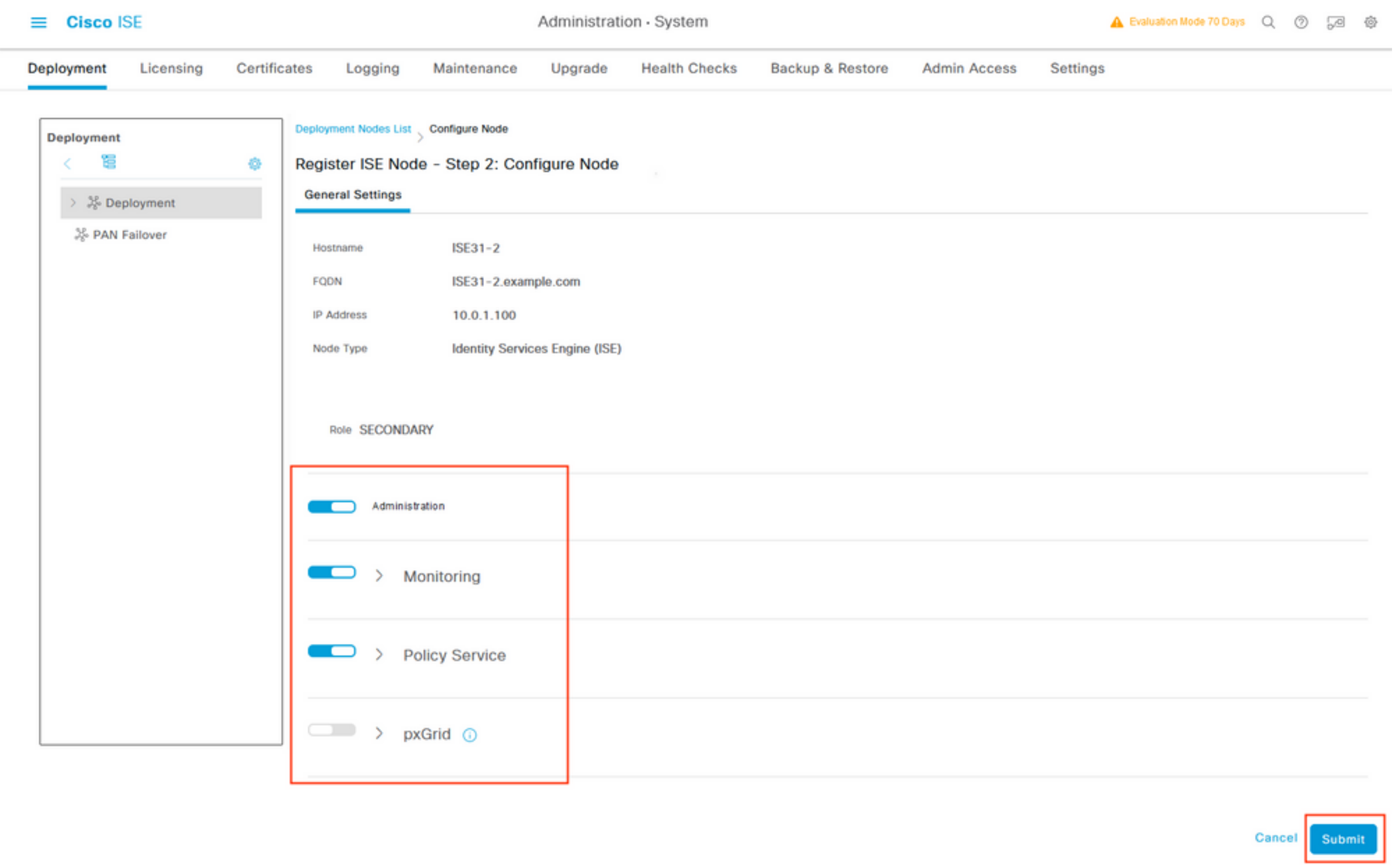
The node you are trying to register uses a self-signed certificate which is not trusted.
Are you sure you want to trust this certificate and proceed with registration?

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

원하는 Personas(페르소나)를 선택하고 Submit(제출)을 **클릭합니다**.



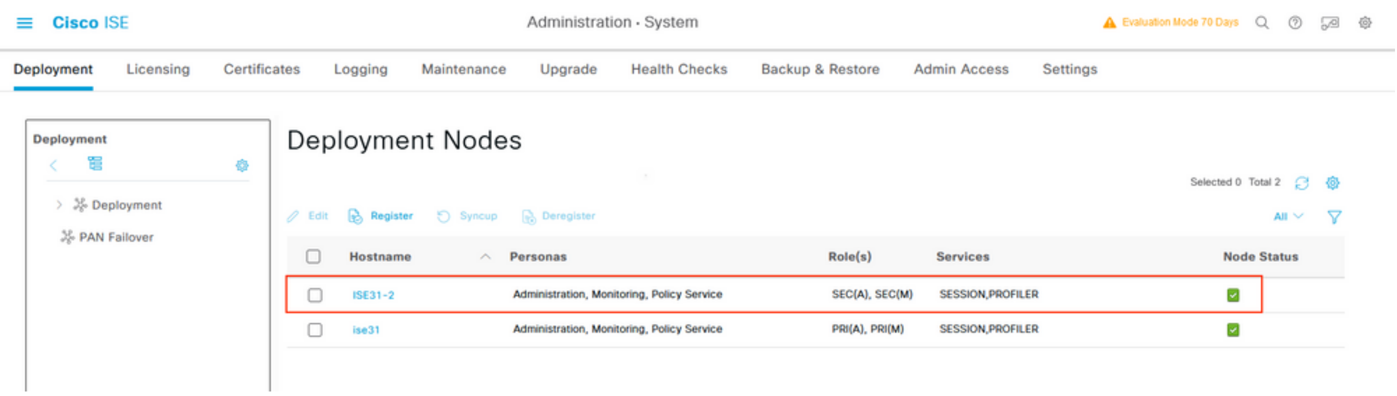
Register ISE Node - Step 2: Configure Node

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

동기화가 완료되면 노드가 연결된 상태로 전환되고 녹색 확인란이 표시됩니다.

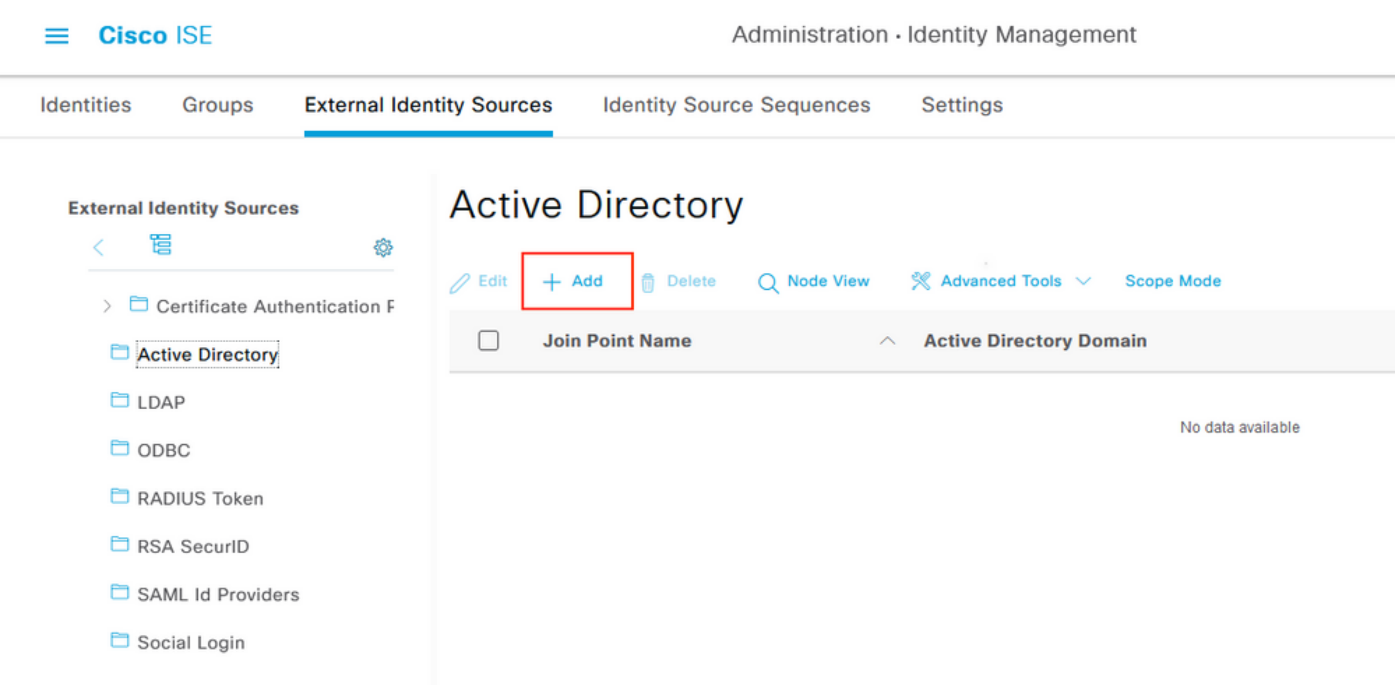


Deployment Nodes

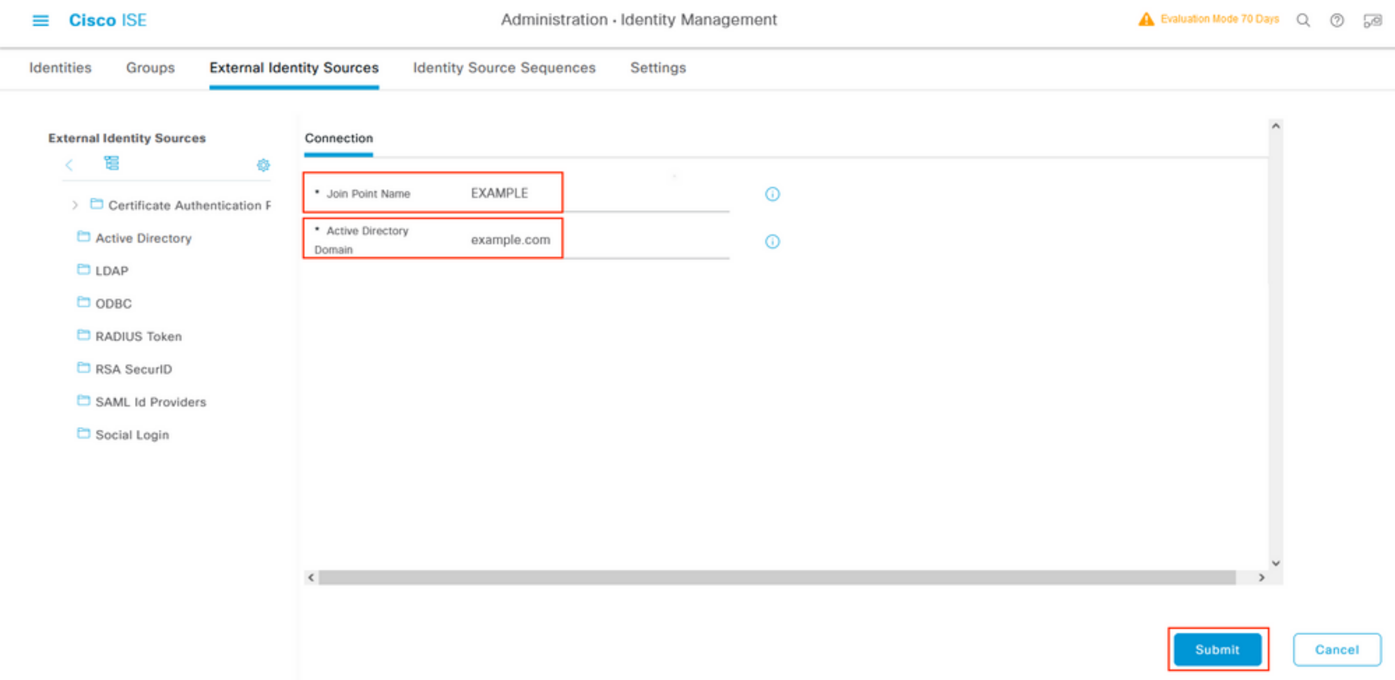
□	Hostname	Personas	Role(s)	Services	Node Status
□	ISE31-2	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	SESSION,PROFILER	✓
□	ise31	Administration, Monitoring, Policy Service	PRI(A), PRI(M)	SESSION,PROFILER	✓

7단계. ISE 구축을 온프레미스 AD와 통합

Administration(관리) **> Identity Management(ID 관리) > External Identity Sources(외부 ID 소스)로 이동합니다**. Active **Directory를** 선택하고 Add를 **선택합니다**.



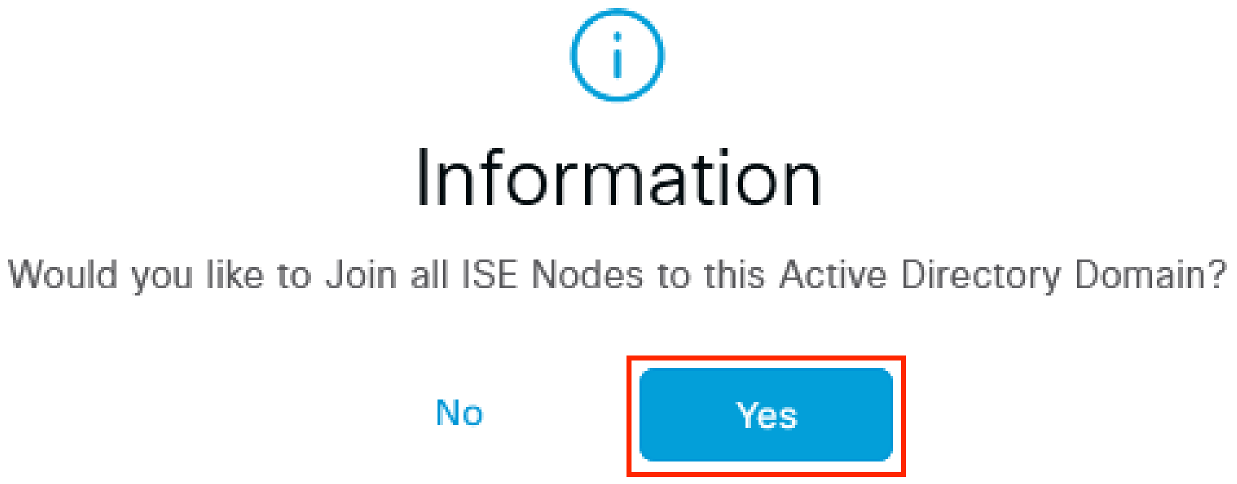
Joint **Point Name** 및 **Active Directory Domain을 구성하고 Submit**(제출)을 **선택합니다**.



* Join Point Name EXAMPLE

* Active Directory Domain example.com

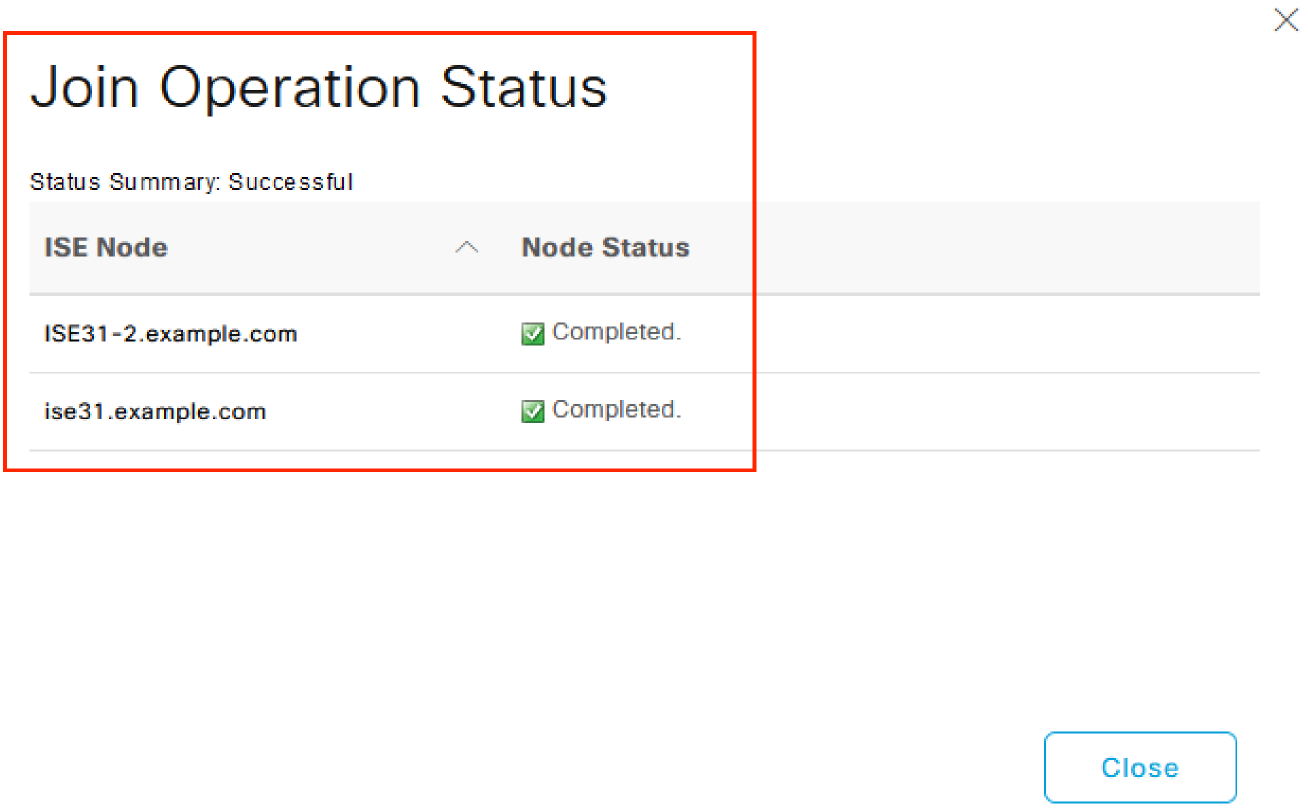
두 노드를 모두 Active Directory와 통합하려면 예를 **선택합니다**.



Information

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

AD **사용자 이름** 및 **암호**를 입력하고 **확인**을 클릭합니다. ISE 노드가 Active Directory와 성공적으로 통합되면 노드 상태가 완료됨으로 변경됩니다.



Join Operation Status

Status Summary: Successful

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

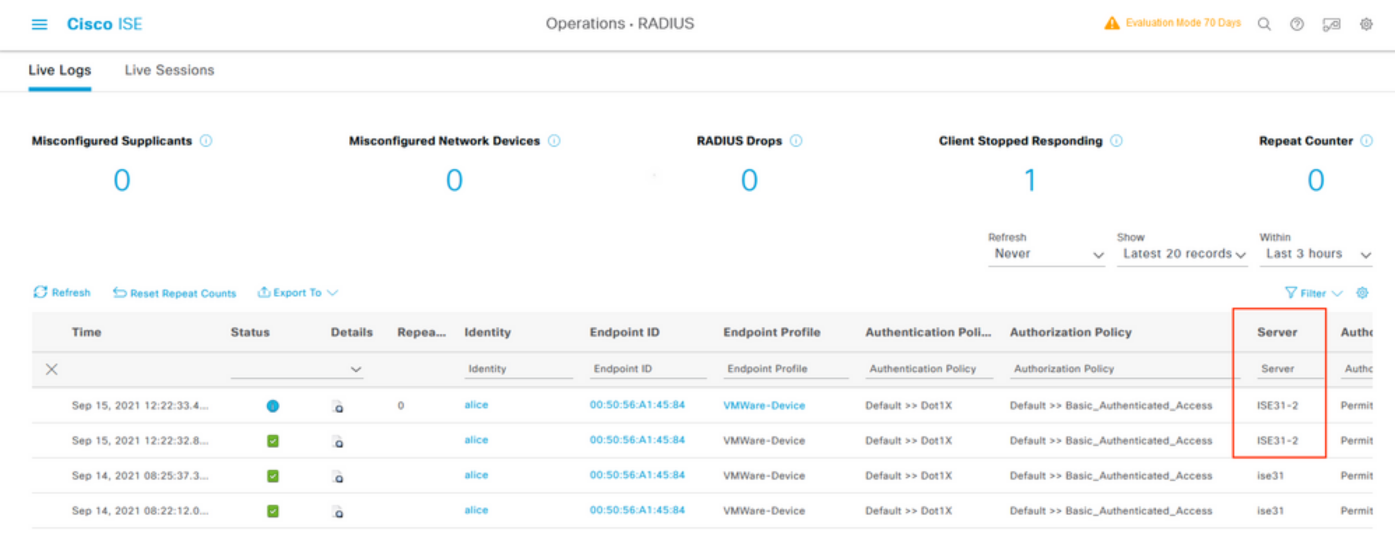
제한 사항

AWS 제한 사항에 대한 ISE의 경우 ISE 관리 설명서의 알려진 제한 사항 섹션을 참조하십시오.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

AWS에 있는 ISE PSN에서 인증이 수행되는지 확인하려면 **Operations(운영) > Radius(Radius) > Live Logs(라이브 로그)**로 이동하고 AWS PSN의 **Server(서버)** 열 ISE를 확인합니다.



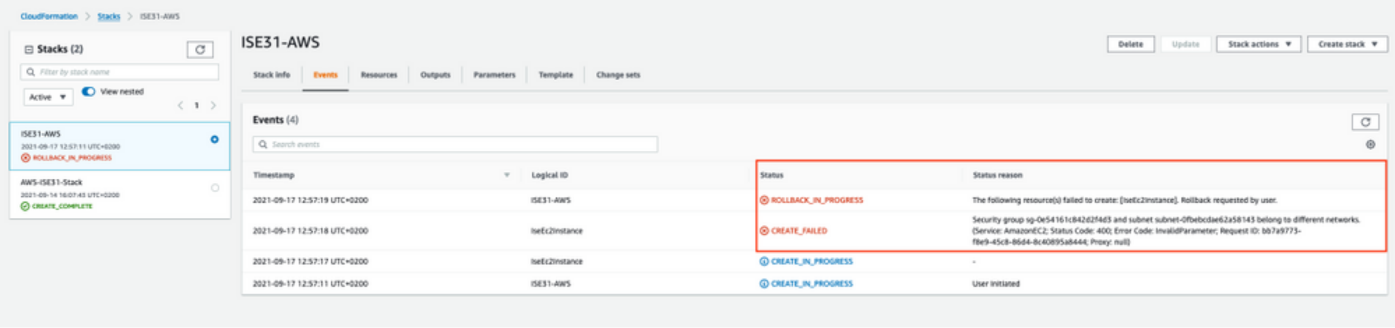
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Poli...	Authorization Policy	Server	Authc
Sep 15, 2021 12:22:33.4...	●		0	alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE31-2	Permit
Sep 15, 2021 12:22:32.8...	✓			alice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

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

CloudFormation 스택 생성 실패

여러 가지 이유로 인해 CloudFormation 스택 생성이 실패할 수 있습니다. 그 중 하나는 ISE의 관리 네트워크와 다른 VPN에서 보안 그룹을 선택하는 것입니다. 오류는 이미지의 오류와 같습니다.



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

해결책:

동일한 VPC에서 보안 그룹을 선택해야 합니다. VPC 서비스 아래**의 보안 그룹**으로 이동하고 **보안 그룹 ID**를 메모하고, **보안 그룹 ID**가 올바른 VPC(ISE가 상주하는)에 해당하는지 확인하고 **VPC ID를 확인합니다**.

연결 문제

AWS에서 ISE에 대한 연결이 작동하지 않을 수 있는 여러 문제가 있을 수 있습니다.

1. 잘못 구성된 **보안 그룹**으로 인한 연결 문제

해결책: **보안 그룹**이 잘못 구성된 경우 온프레미스 네트워크 또는 AWS 네트워크 내에서도 ISE에

연결할 수 없습니다. 필요한 프로토콜 및 포트가 ISE 네트워크와 연결된 **보안 그룹**에서 허용되는지 확인합니다. 열려는 필수 포트에 대해서는 ISE 포트 참조를 참조하십시오.

2. 잘못 구성된 라우팅으로 인한 연결 문제

해결책: 토폴로지의 복잡성으로 인해 온프레미스 네트워크와 AWS 간의 일부 경로를 놓치기 쉽습니다. ISE 기능을 사용하기 전에 엔드 투 엔드 연결이 제대로 되어 있는지 확인하십시오.

부록

스위치 AAA/Radius 관련 컨피그레이션

```
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
```