ISE 3.1 configureren via AWS-marktplaats

Inhoud

Inleiding

Dit document beschrijft hoe je Identity Services Engine (ISE) 3.1 kunt installeren via Amazon Machine Images (AMI) in Amazon Web Services (AWS). Vanaf versie 3.1 kan ISE worden ingezet als een Amazon Elastic Compute Cloud (EC2)-exemplaar, met behulp van CloudFormation Templates (CFT).

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- ISE

- AWS en zijn concepten zoals VPC, EC2, CloudFormat

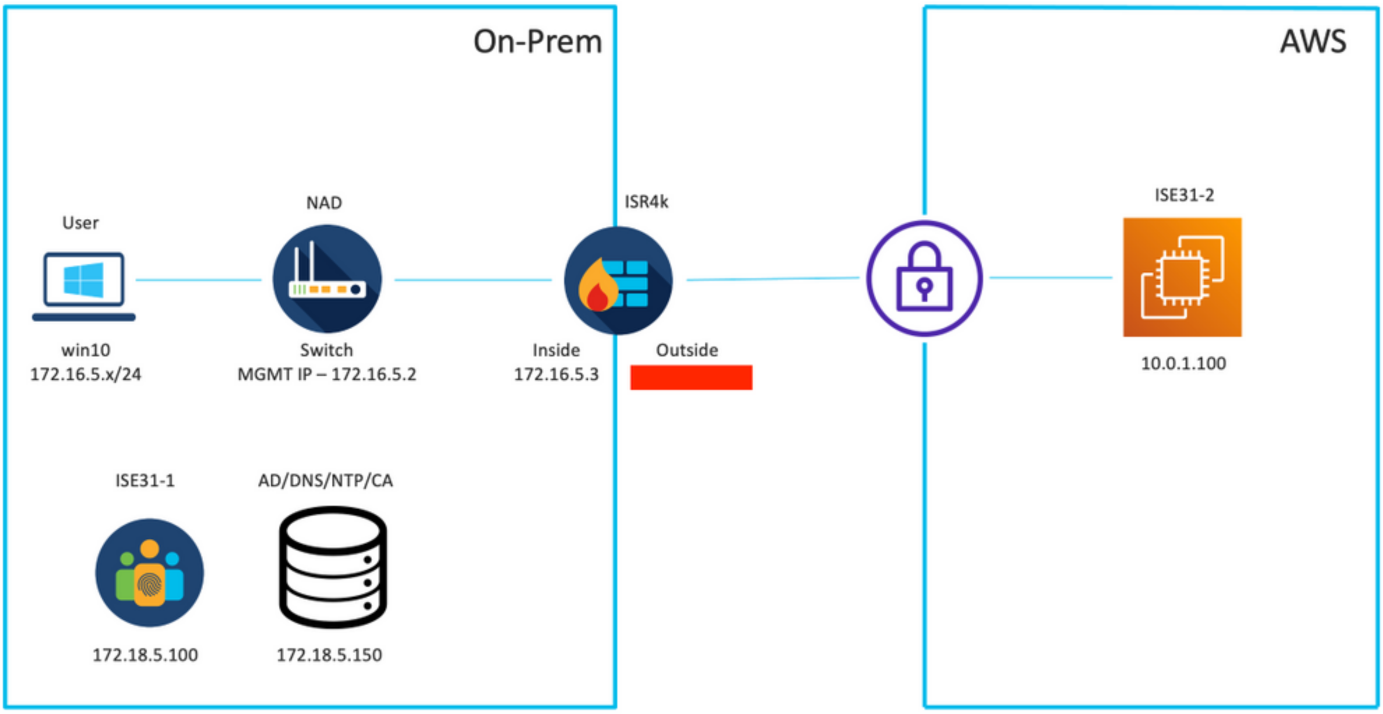
Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ISE versie 3.1.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Netwerktopologie

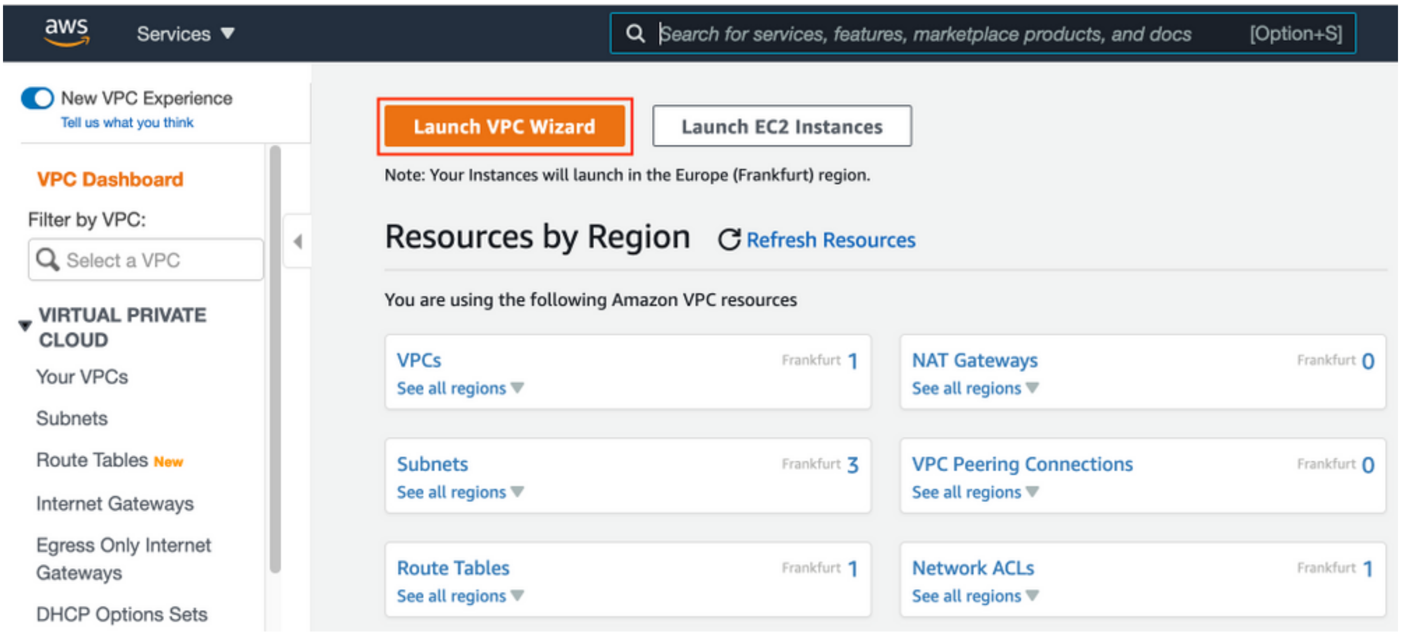


Configuraties

Als er nog geen VPC, Security Groepen, Key Parks en VPN-tunnel zijn geconfigureerd, moet u optionele stappen volgen, anders start u met Stap 1.

Optioneel Stap A. Maak VPC

Navigeer naar **VPC** AWS Service. Selecteer de **VPC Wizard starten** zoals in de afbeelding.



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

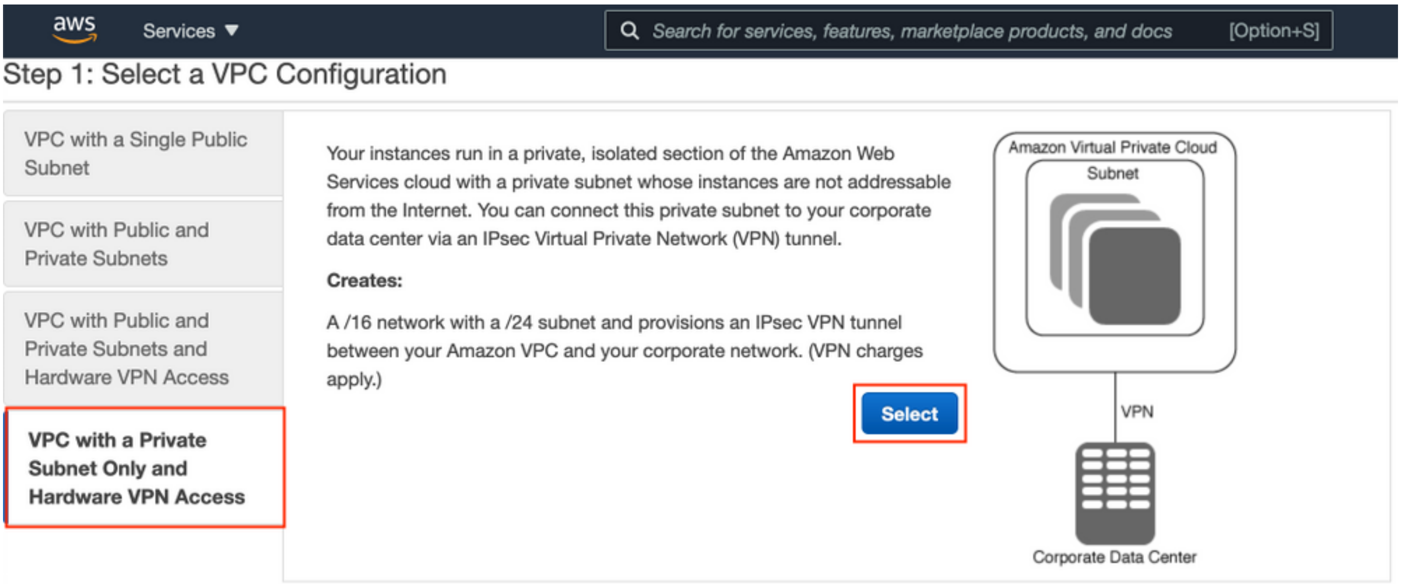
Resources by Region

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

Kies **VPC met alleen Private Subnet en hardware VPN Access** en klik op **Selecteren** zoals in de afbeelding.


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

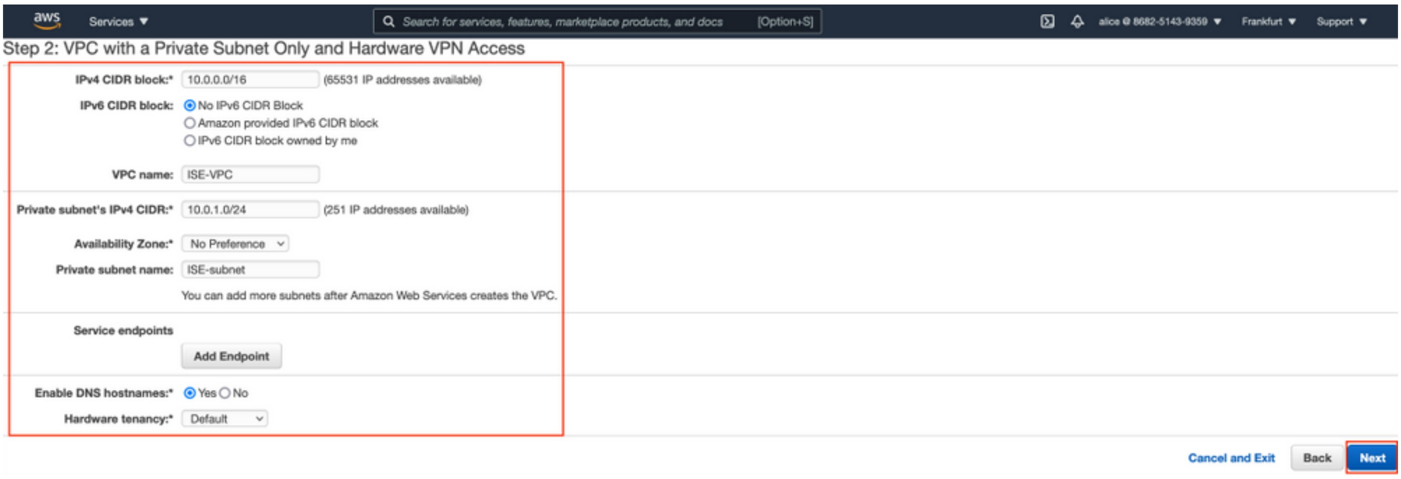
Your instances run in a private, isolated section of the Amazon Web Services cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate data center via an IPsec Virtual Private Network (VPN) tunnel.

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.)

> **Opmerking:** De selectie van VPC in Stap 1. van de wizard VPC hangt af van de topologie aangezien ISE niet is ontworpen als Internet-blootgestelde server - VPN met alleen privé-plus wordt gebruikt.

Configureer de VPC Private Subnet-instellingen volgens het netwerkontwerp en selecteer **Volgende**.



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.

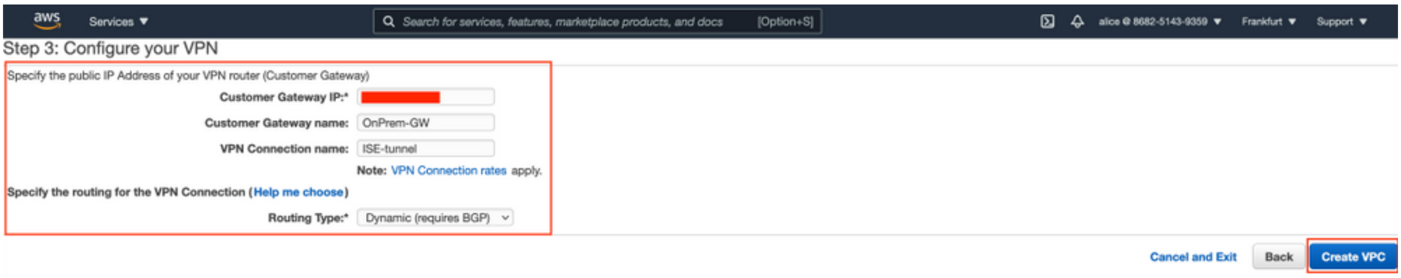
Service endpoints

Add Endpoint

Enable DNS hostnames:* ● Yes ○ No

Hardware tenancy:* Default

Configureer uw VPN overeenkomstig uw netwerkontwerp en selecteer **VPC maken**.



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

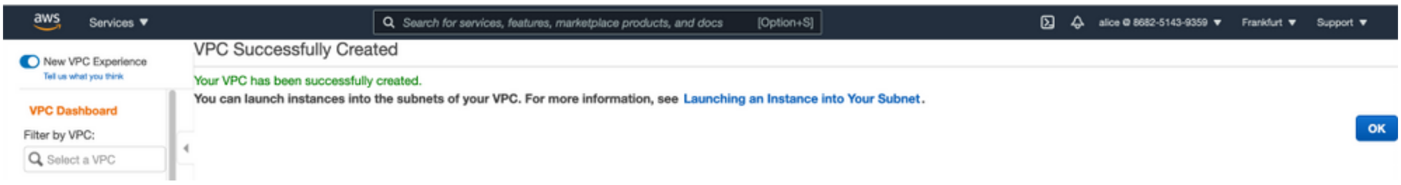
VPN Connection name: ISE-tunnel

Note: VPN Connection rates apply.

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

Routing Type:* Dynamic (requires BGP)

Nadat de VPC is gecreëerd, **wordt** het bericht**"Uw VPC is gemaakt"** weergegeven. Klik op **OK** zoals in de afbeelding.



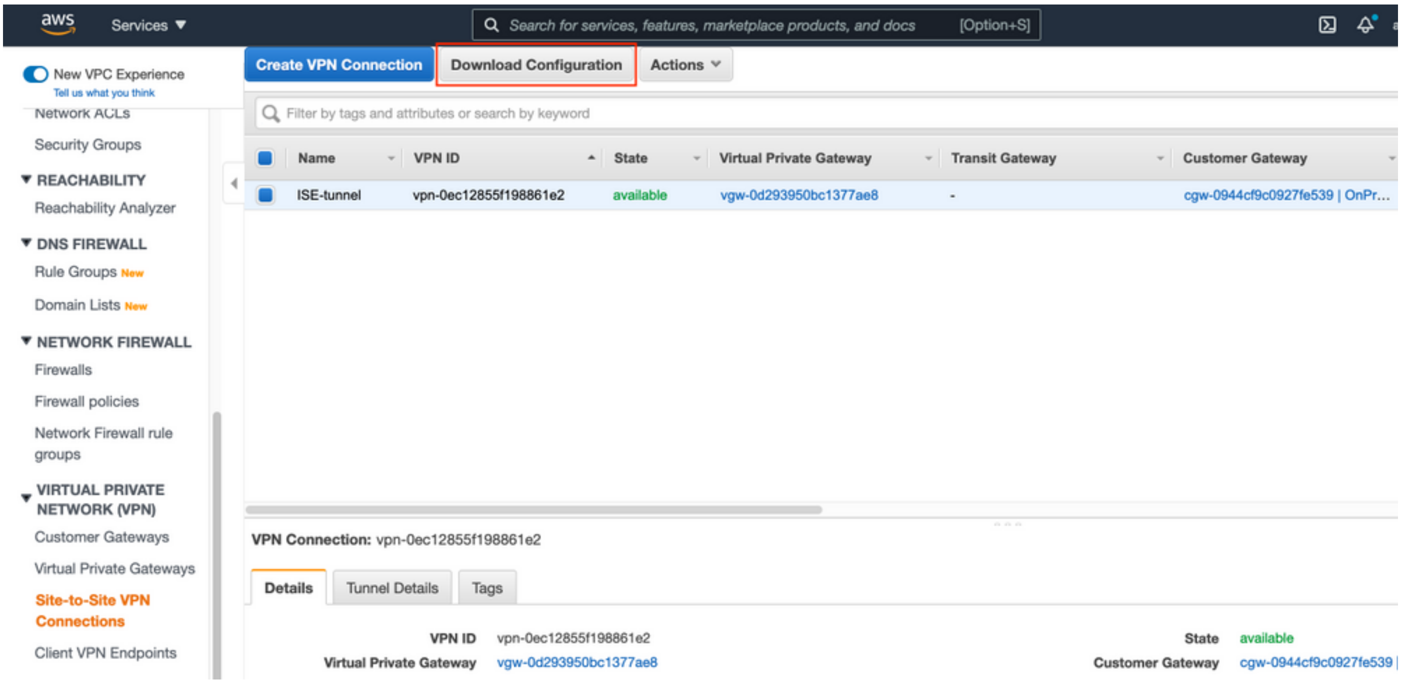
VPC Successfully Created

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.

Optioneel Stap B. Configureren van VPN-head-end apparaat

Navigeer naar **VPC** AWS Service. Kies **Site-to-Site VPN-verbindingen**, selecteer de nieuwe VPN-tunnel en selecteer **Downloadconfiguratie** zoals in de afbeelding.



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

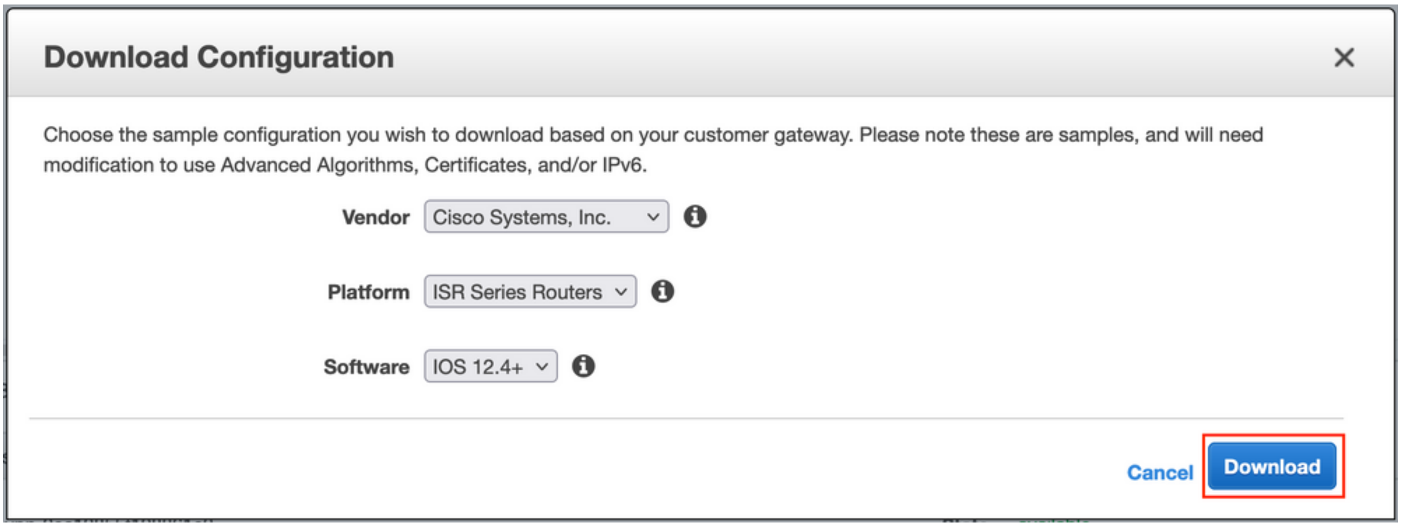
VPN ID vpn-0ec12855f198861e2

State available

Virtual Private Gateway vgw-0d293950bc1377ae8

Customer Gateway cgw-0944cf9c0927fe539 |

Kies **de verkoper**, **platform** en **software**, selecteer **Download** zoals in de afbeelding.



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.

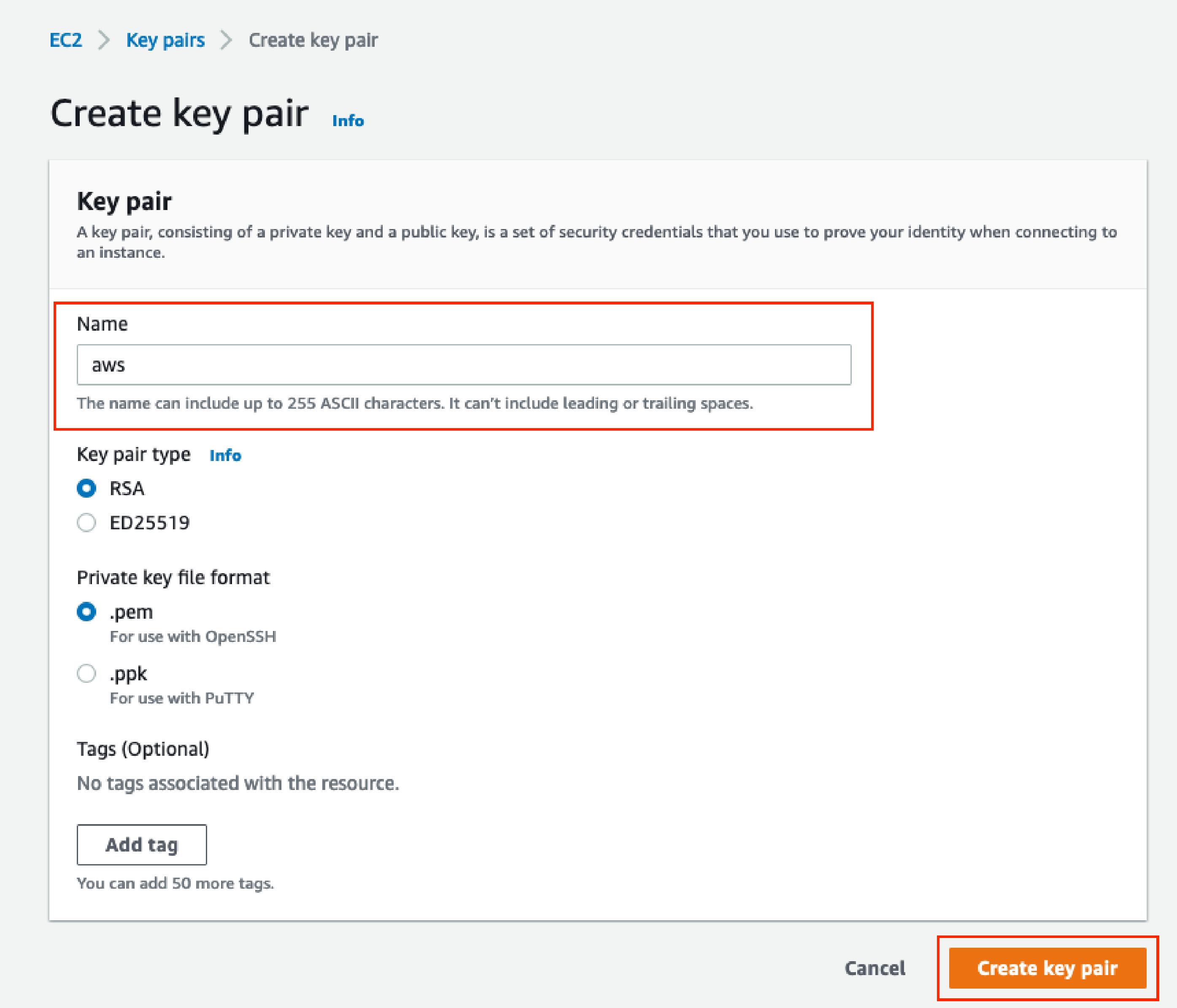
Platform: ISR Series Routers

Software: IOS 12.4+

Toepassen gedownload configuratie op Prem VPN head-end apparaat.

Optioneel stap C. Aangepaste toetstitel maken

AWS EC2-instanties worden benaderd met behulp van sleutelparen. Om een sleutelpaar te creëren, navigeer naar **EC2** Service. Selecteer **het** menu **Toetsen** onder **Netwerk & Beveiliging.** Selecteer **Belangrijkste paar maken**, geef het een **naam,** laat andere waarden standaard achter en selecteer Opnieuw **Key** Pair **maken**.



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

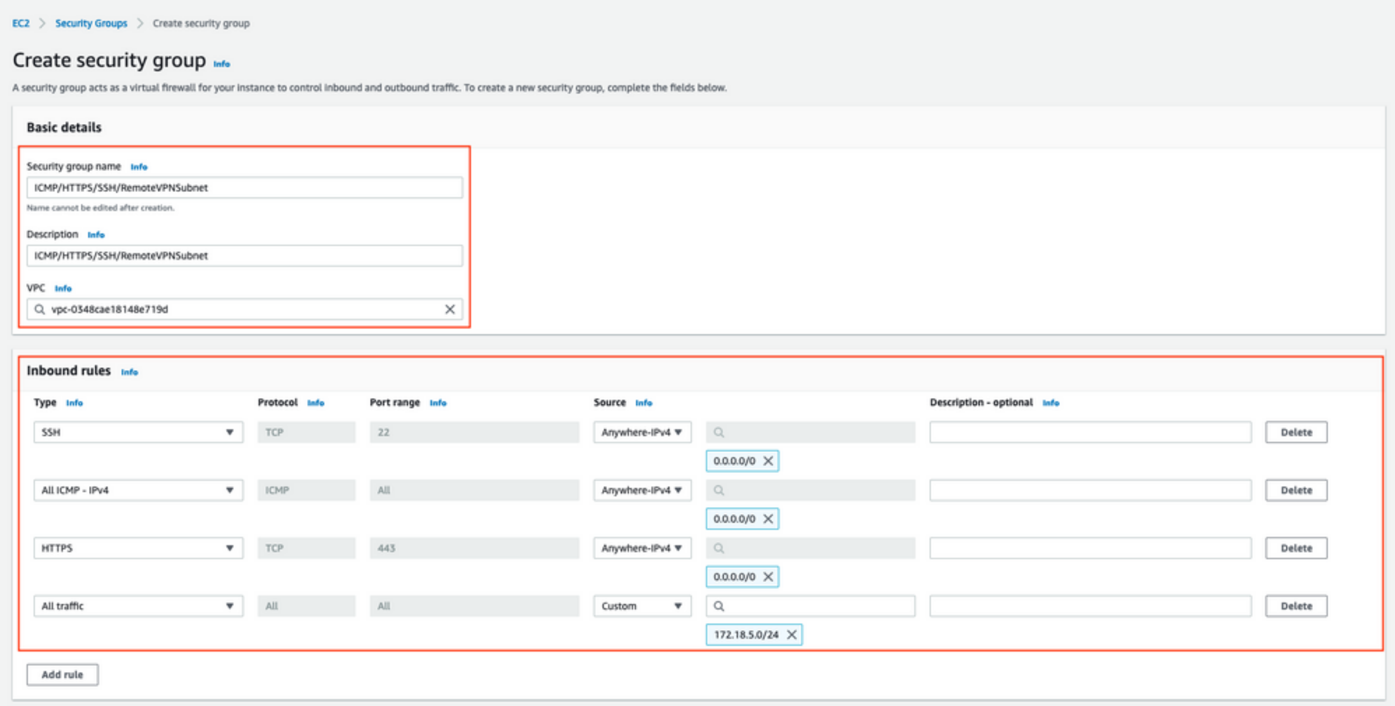
Tags (Optional)

No tags associated with the resource.

You can add 50 more tags.

Optioneel Stap D. Maak een aangepaste beveiligingsgroep.

AWS EC2 instanties die toegang hebben wordt beschermd door **Beveiligingsgroepen**, om **Security Group** te configureren, navigeer naar **EC2** Service. Selecteer het menu **Beveiligingsgroepen** onder **Netwerkbeveiliging en -beveiliging.** Selecteer **Security Group maken,** stel een **naam**, **omschrijving,** in het **VPC**-veld dat net is ingesteld **op VPC.** Configureer **inkomende regels** zodat communicatie met ISE mogelijk is. Selecteer **Beveiligingsgroep maken** zoals in de afbeelding.



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

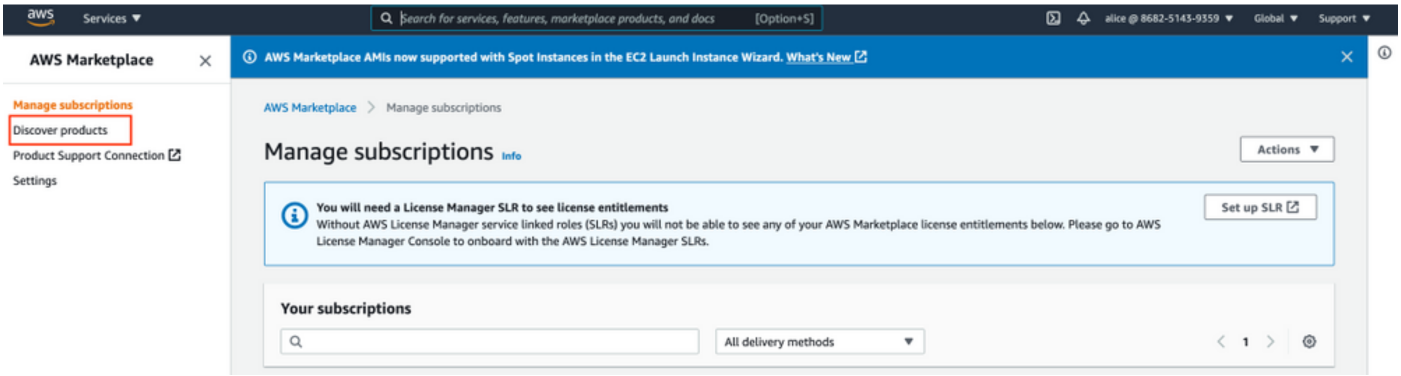
Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
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

Opmerking: De ingesteld Security Group maakt SSH, ICMP, HTTPS toegang tot ISE en alle protocollen toegang tot On-Prem subnet mogelijk.

Stap 1. Abonneren op AWS ISE-marktproduct

Navigeer naar **AWS** Service **op** marktplaats **abonnementen** op AWS. Selecteer **Producten** ontdekken zoals in de afbeelding.



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

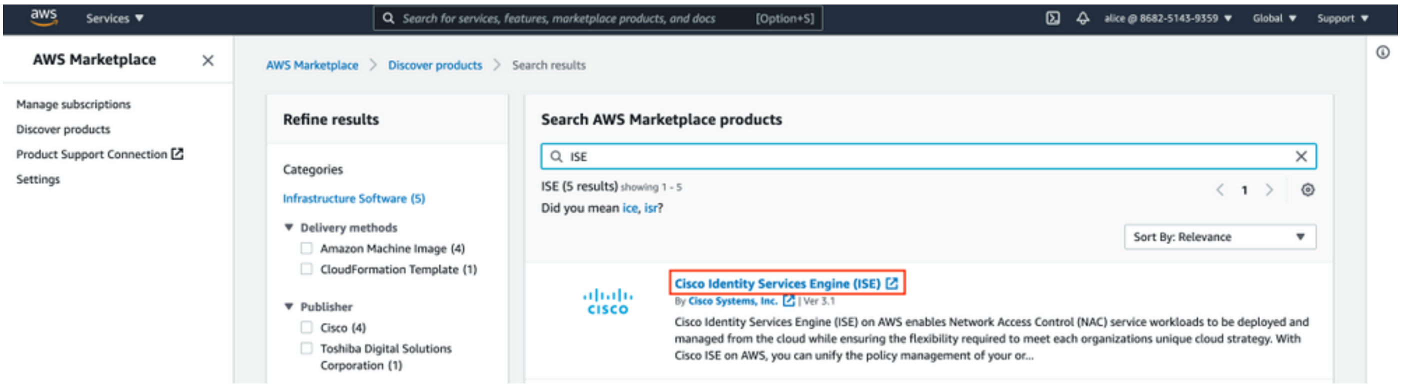
AWS Marketplace > Manage subscriptions

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.

Zoek naar **ISE-**product en selecteer **Cisco Identity Services Engine (ISE)** zoals in de afbeelding.



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
1
Sort By: Relevance ▼
cisco

ISE (5 results) showing 1 - 5

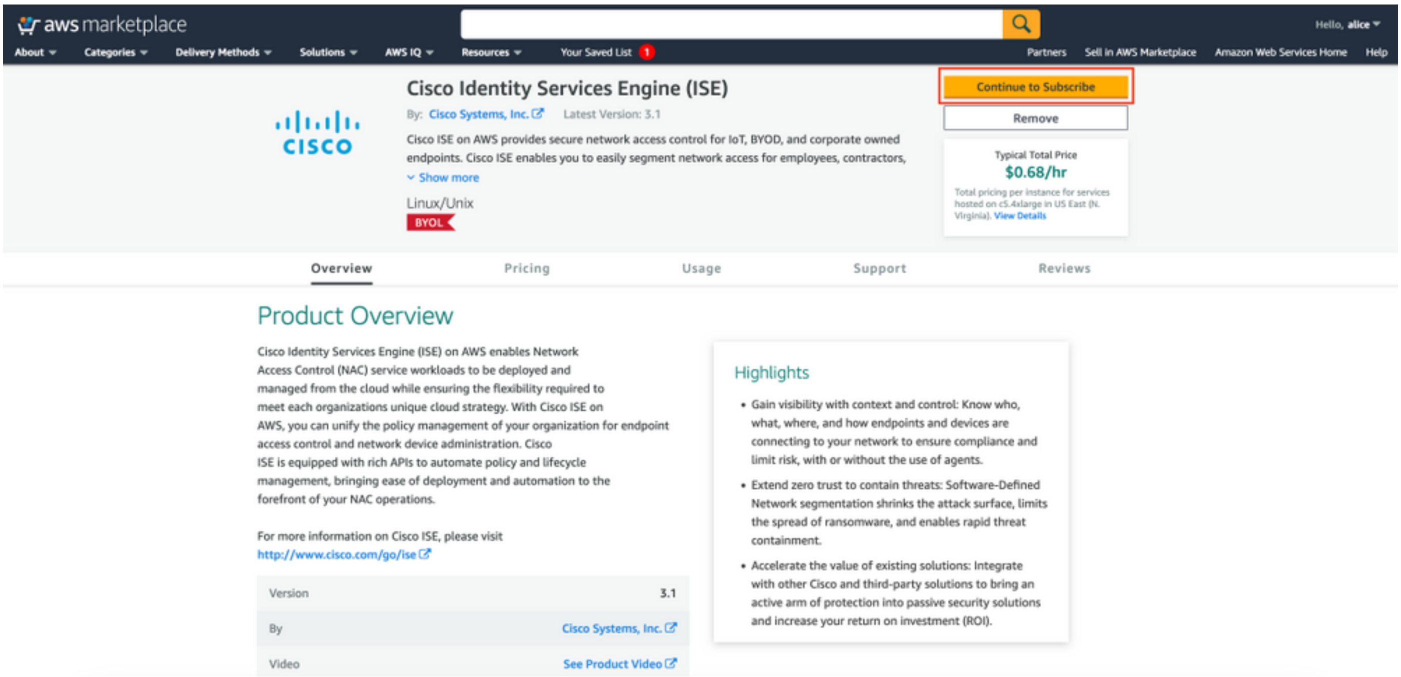
Did you mean ice, isr?

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...

Selecteer **Doorgaan met abonnement**



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.

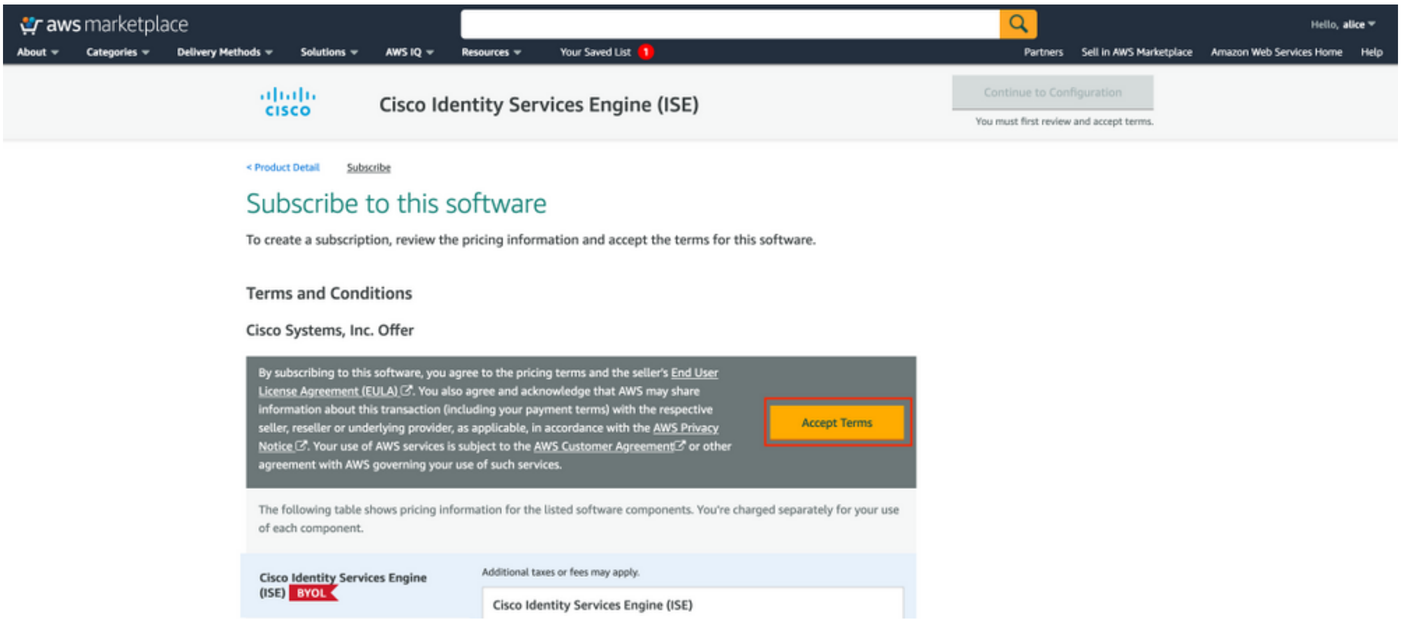
For more information on Cisco ISE, please visit http://www.cisco.com/go/ise

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).

Selecteer de knop **Bepalingen accepteren** zoals in de afbeelding.



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.

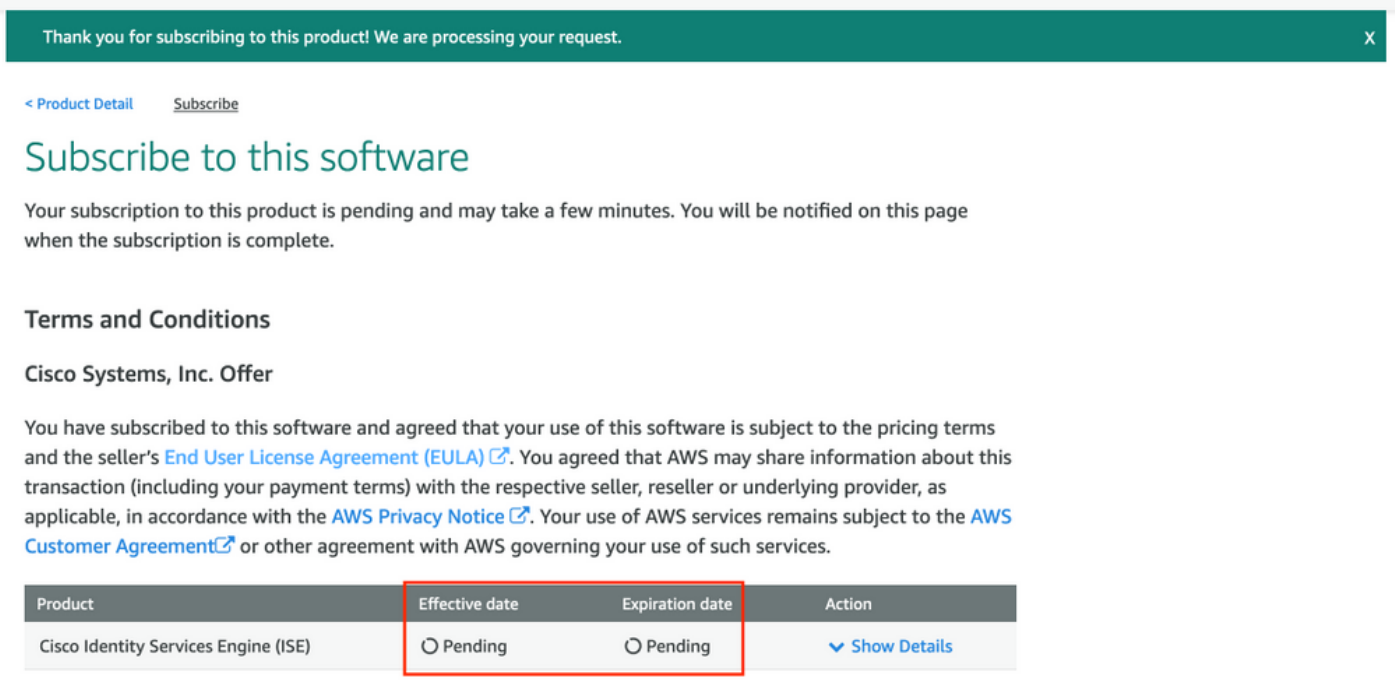
The following table shows pricing information for the listed software components. You're charged separately for your use of each component.

Cisco Identity Services Engine (ISE) BYOL

Additional taxes or fees may apply.

Cisco Identity Services Engine (ISE)

Zodra u de status van de **effectieve** en **vervaldatum hebt** ingetekend, wordt de tekst gewijzigd in afwachting van de afbeelding.



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.

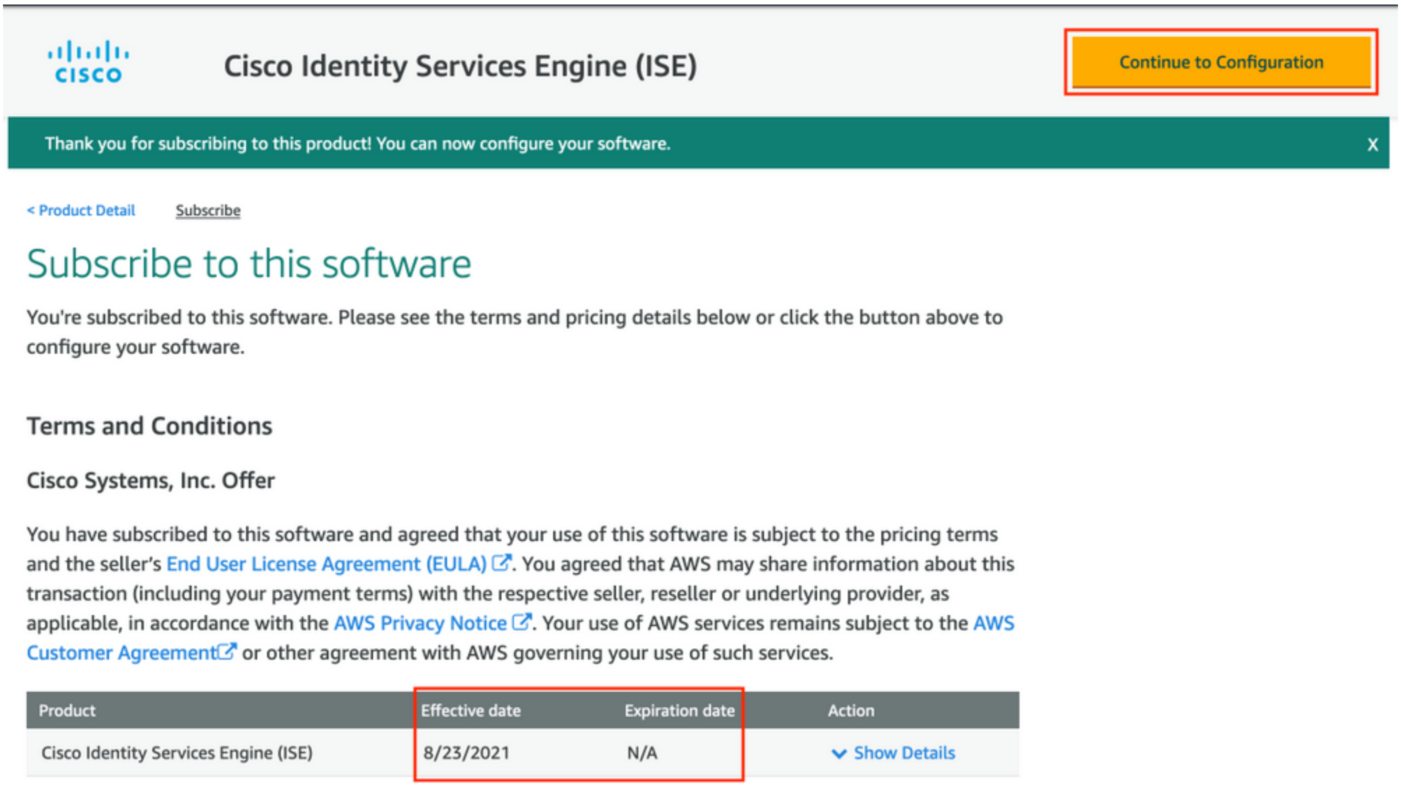
Terms and Conditions

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

Kort na de **ingangsdatum** verandert de datum van abonnement en de **vervaldatum** in **nvt.** Selecteer **Doorgaan naar configuratie** zoals in de afbeelding



Cisco Identity Services Engine (ISE)

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

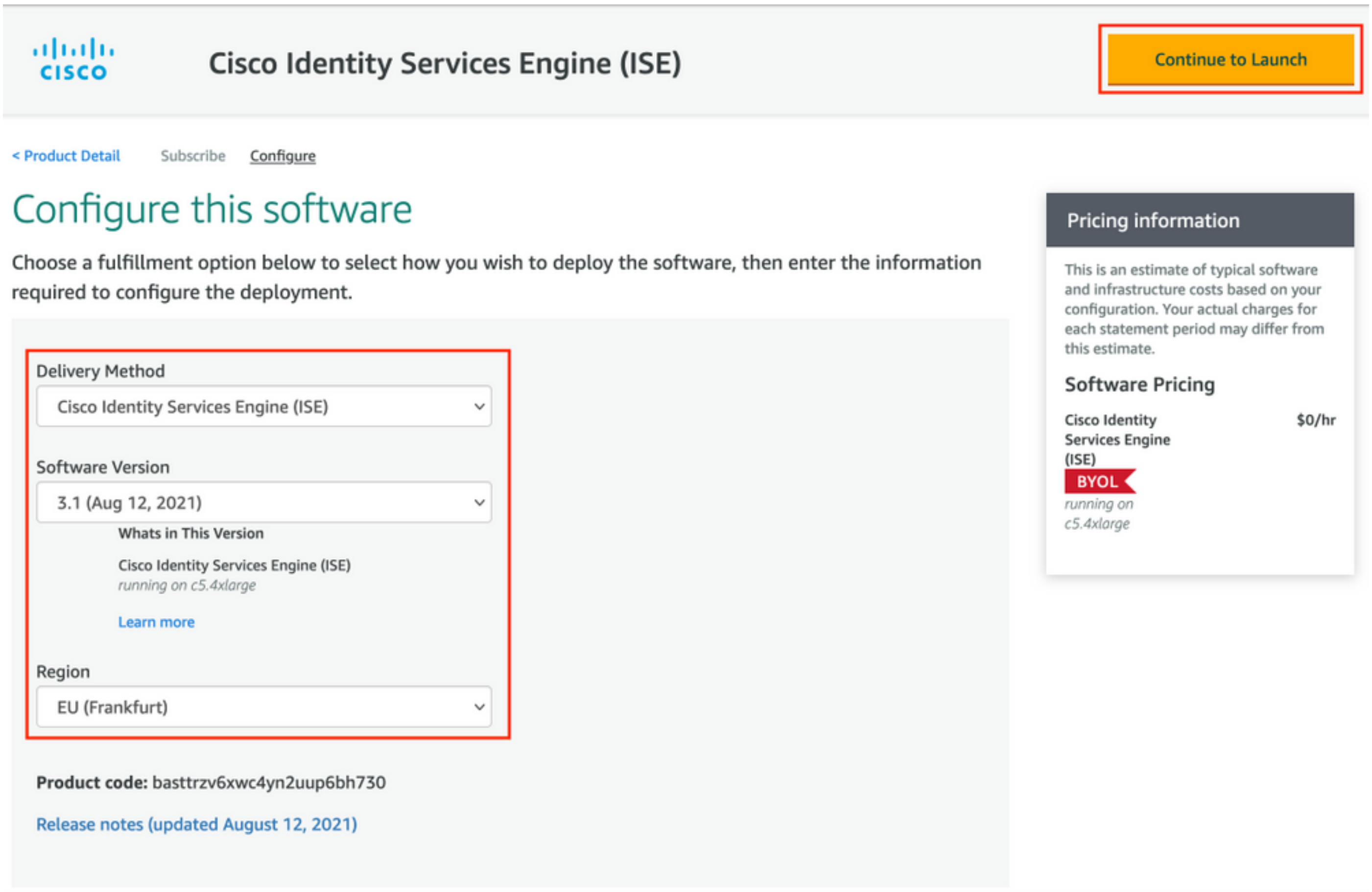
Cisco Systems, Inc. Offer

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

Stap 2. Configureer ISE op AWS

Selecteer in het menu Delivery Methode van het **venster Configure dit softwarescherm** en **selecteer Cisco Identity Services Engine (ISE).** Selecteer in de **softwareversie** 3.1 **(augustus 2021)**. Selecteer het **gebied** waar ISE is gepland voor gebruik. Selecteer **Doorgaan met starten.**



Cisco Identity Services Engine (ISE)

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

Region: EU (Frankfurt)

Product code: basttrzv6xwc4yn2uup6bh730

Pricing information

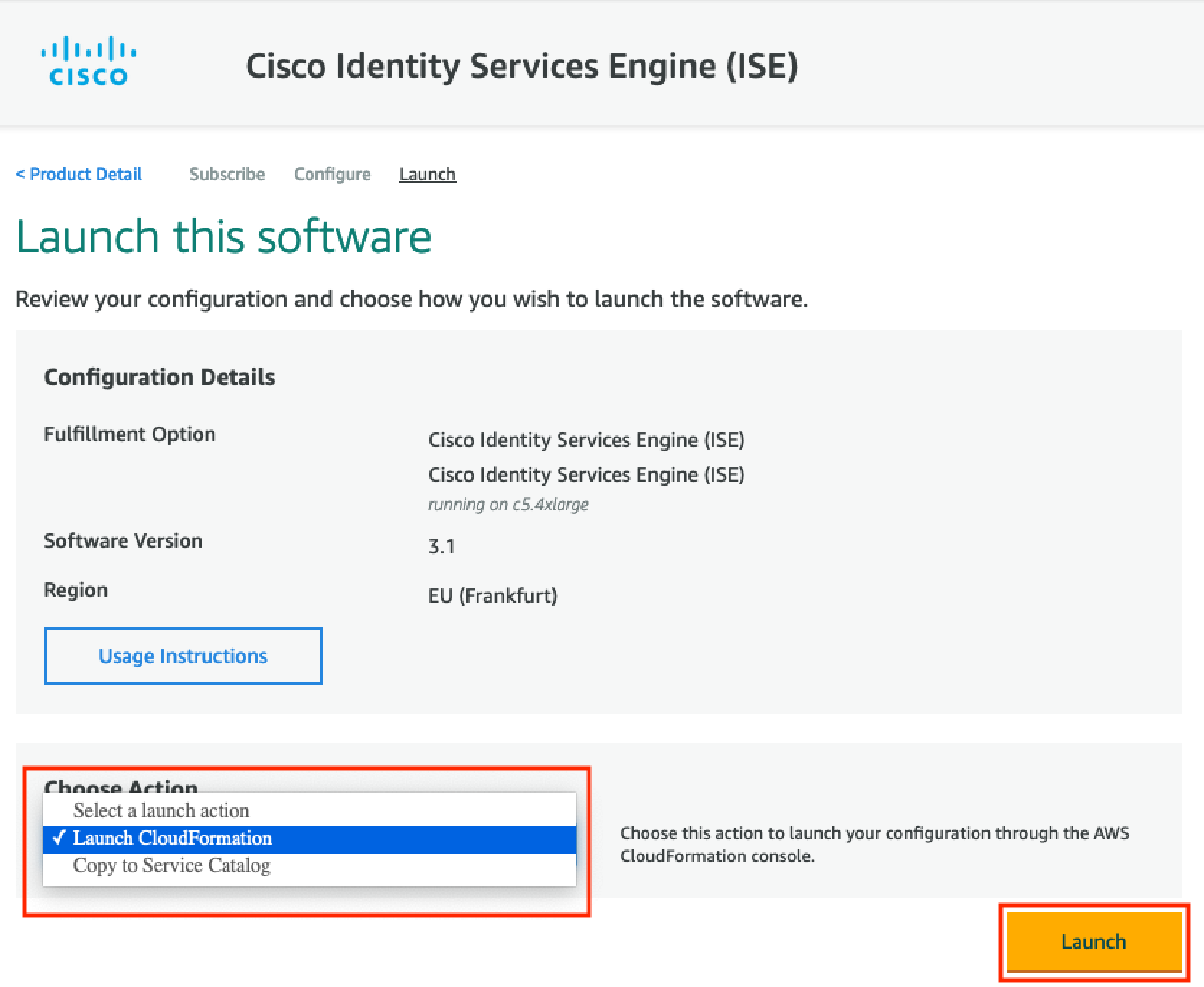
This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

Software Pricing

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

Stap 3. Start ISE op AWS

Selecteer in het vervolgkeuzemenu Handelingen in het **Software-**scherm starten de optie **CloudFormation starten**.


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

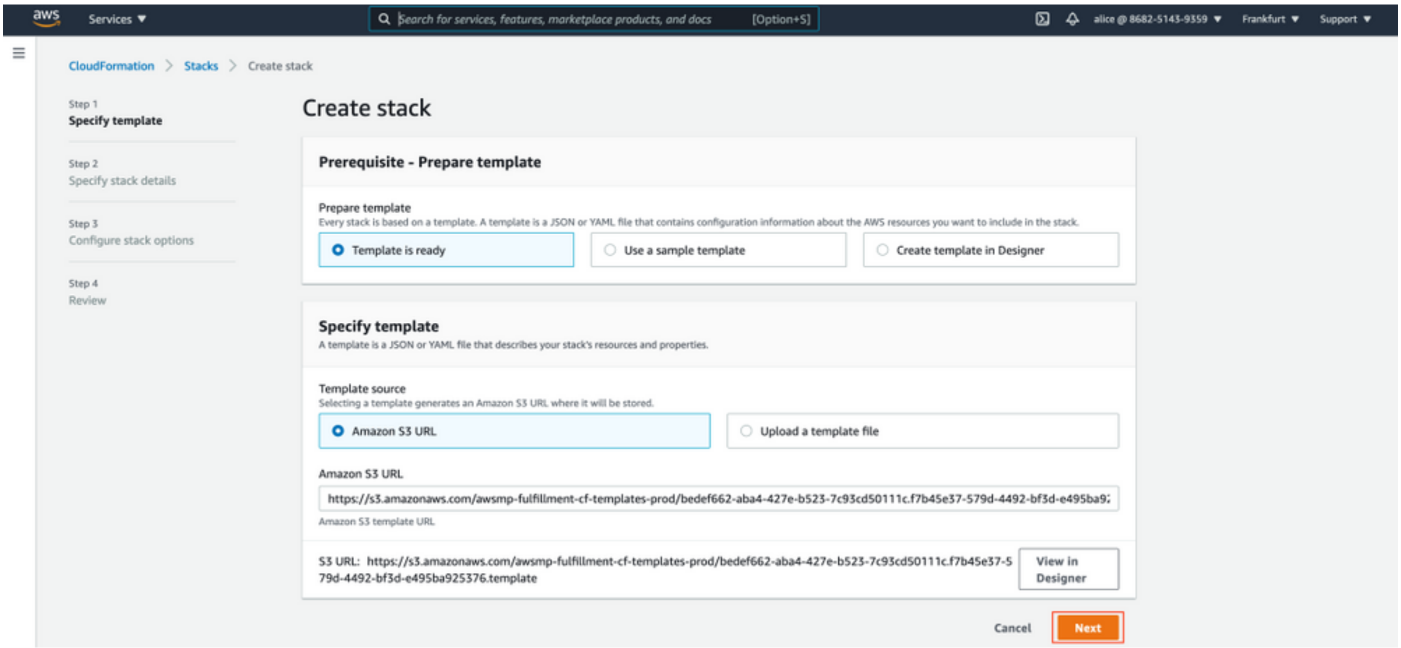
Fulfillment Option	Cisco Identity Services Engine (ISE) Cisco Identity Services Engine (ISE) *running on c5.4xlarge*
Software Version	3.1
Region	EU (Frankfurt)

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

(Optioneel) Selecteer **Gebruik-instructies** om uzelf hiermee bekend te maken. Selecteer **Start**.

Stap 4. Configuratie van CloudFormation Stack voor ISE op AWS

De knop **Start** richt u terug naar het setup-venster van de **CloudFormation** Stack. Er is een voorgebouwde sjabloon die gebruikt moet worden om ISE in te stellen. Houd standaardinstellingen en selecteer **Volgende**.



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.

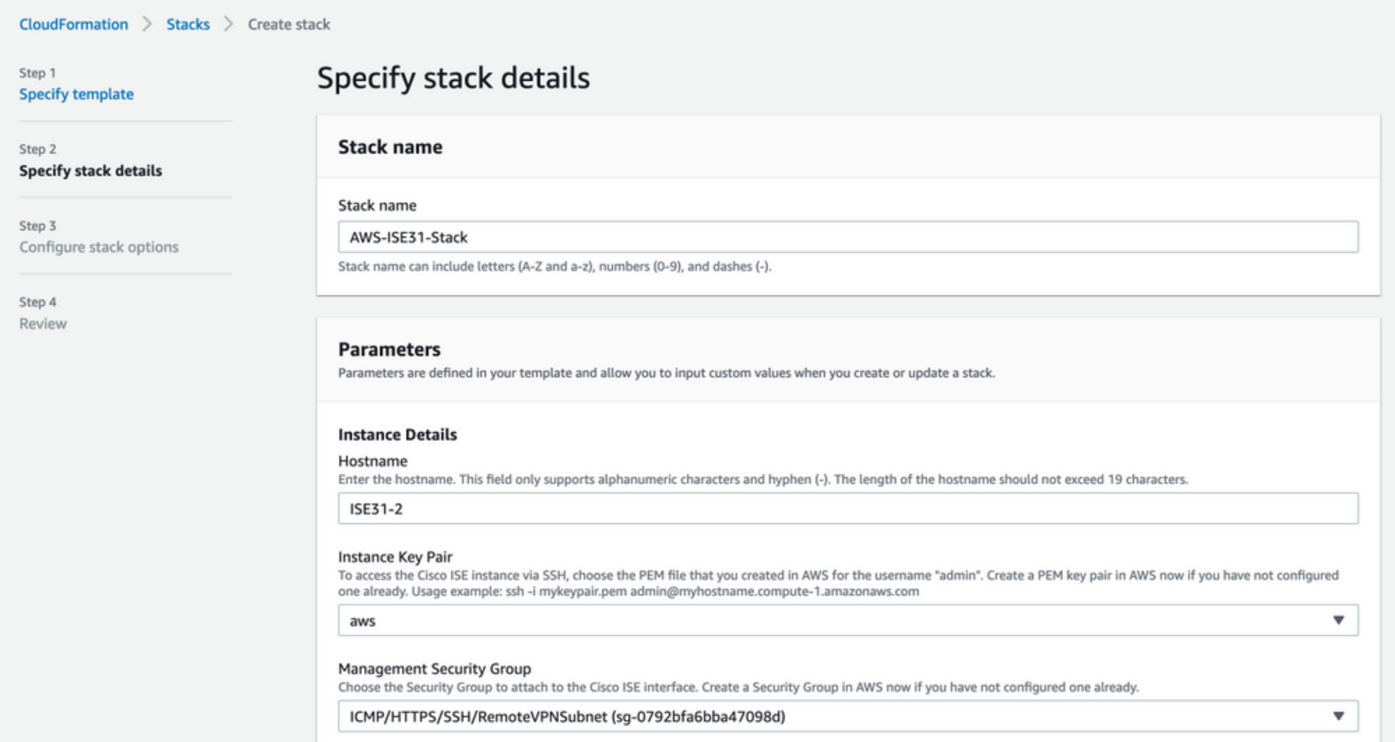
Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

● 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

Populeren de gegevens van de StackStack van de CloudFormation met **de Naam van de Stack**. Instantiegegevens zoals **Hostname** configureren, selecteer Instantie-**toetstitel** en **Beveiligingsgroep beheren.**



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.

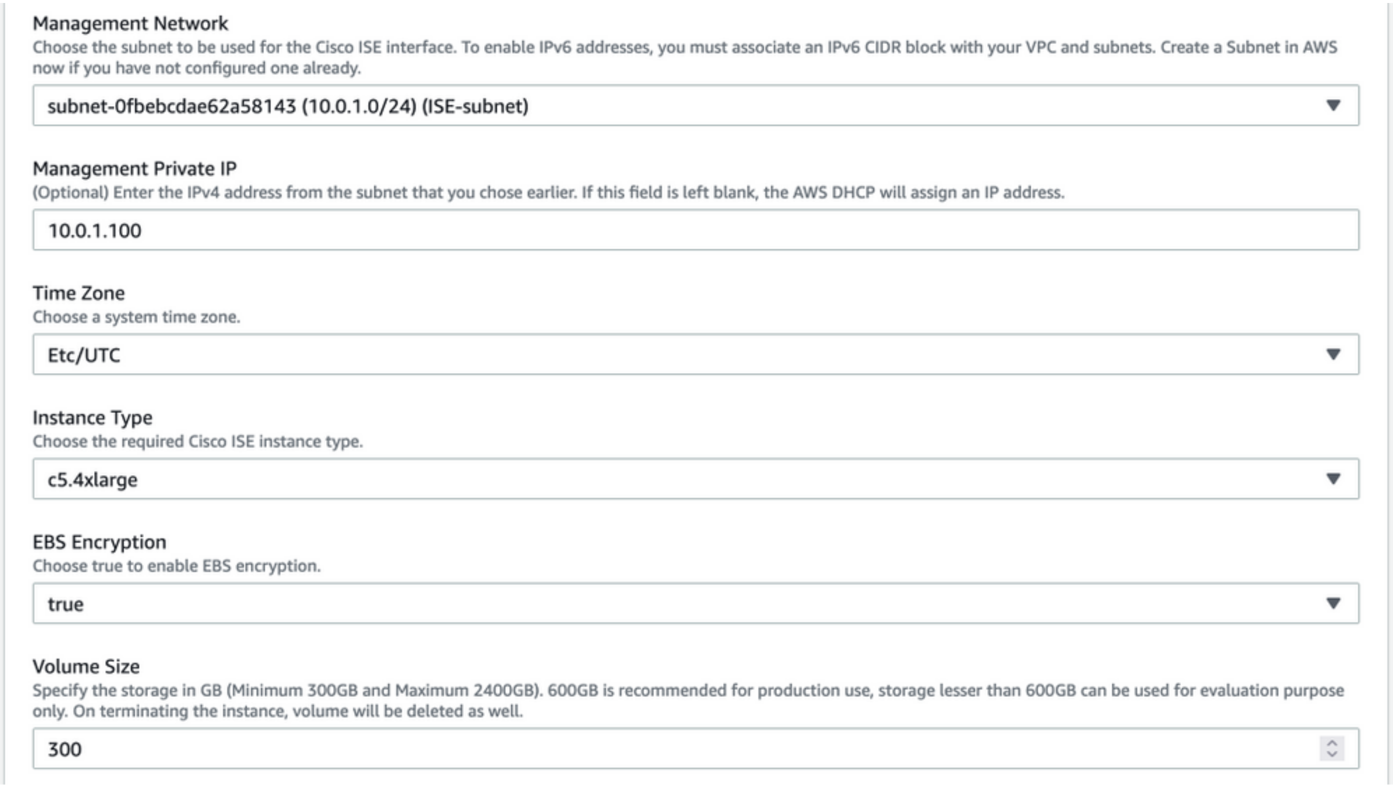
Instance Details

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) ▼

Zet de configuratie van de Instantiegegevens voort met **Management Network, Management Private IP, Time Zone**, **Instantietype, EBS Encryption** en **Volume Size.**



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.

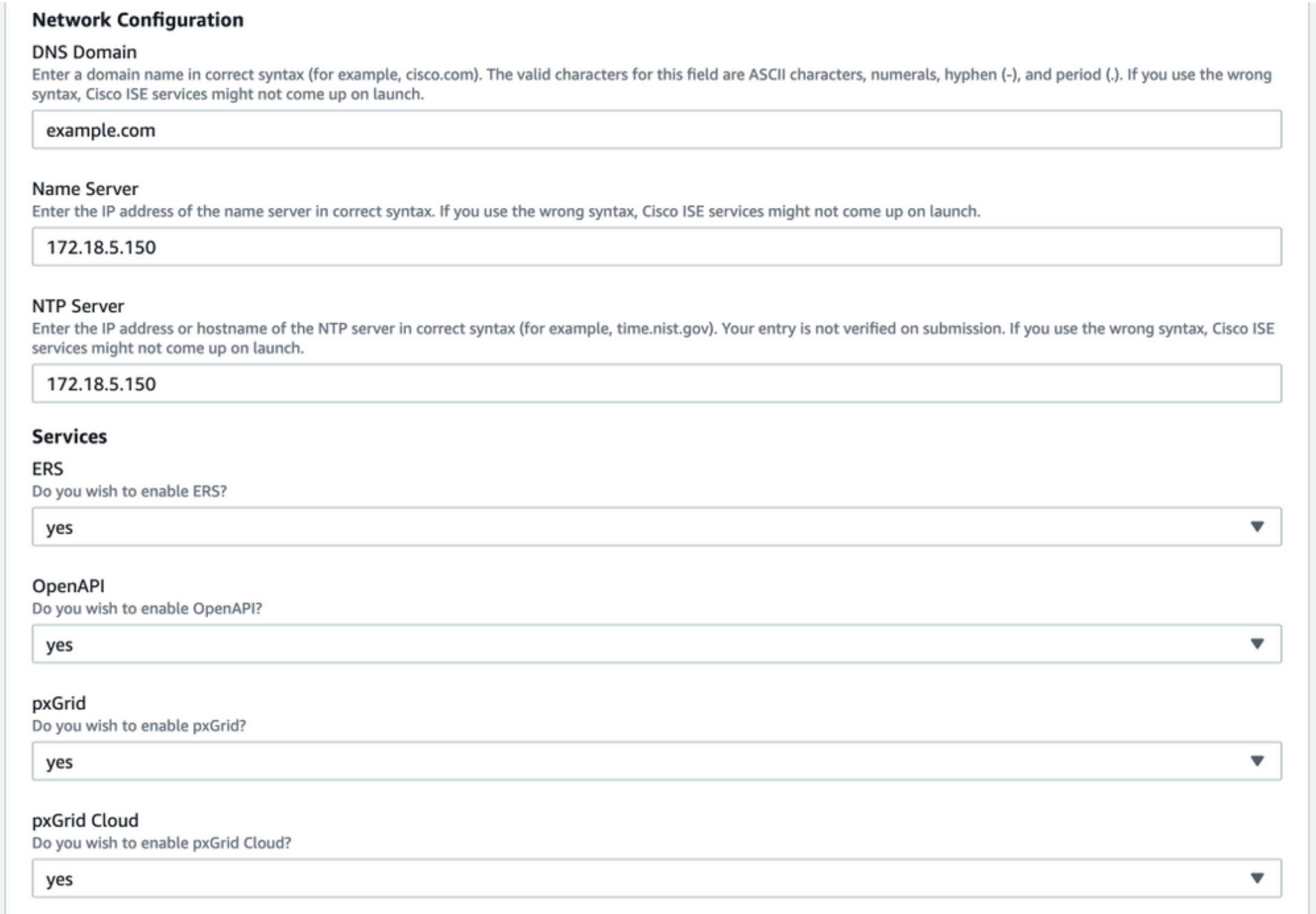
true

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

Doorgaan met configuratie van Instantiegegevens met **DNS-domein, Naamserver, NTP-**service en **-services**.



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?

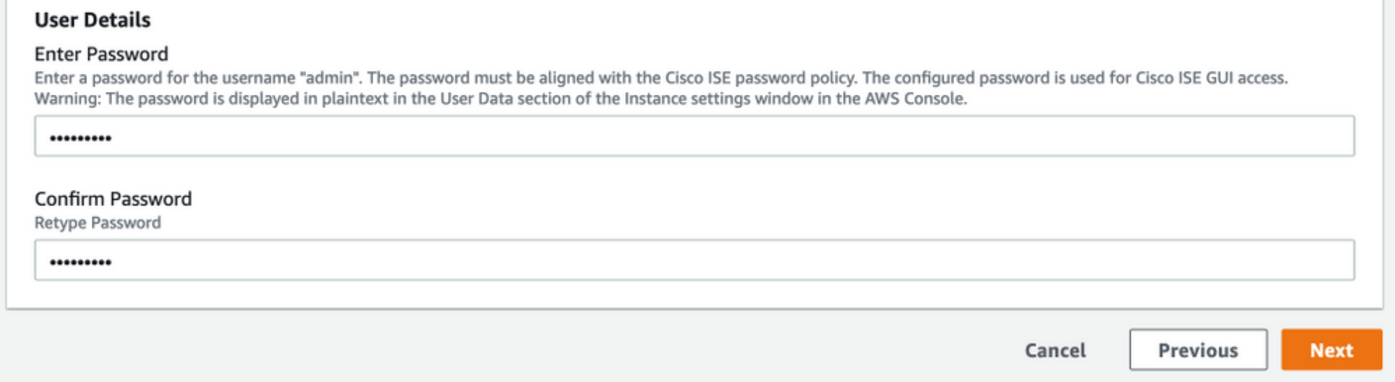
yes

pxGrid Cloud

Do you wish to enable pxGrid Cloud?

yes

Configureer het gebruikerswachtwoord in de GUI en selecteer **Volgende**.



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.

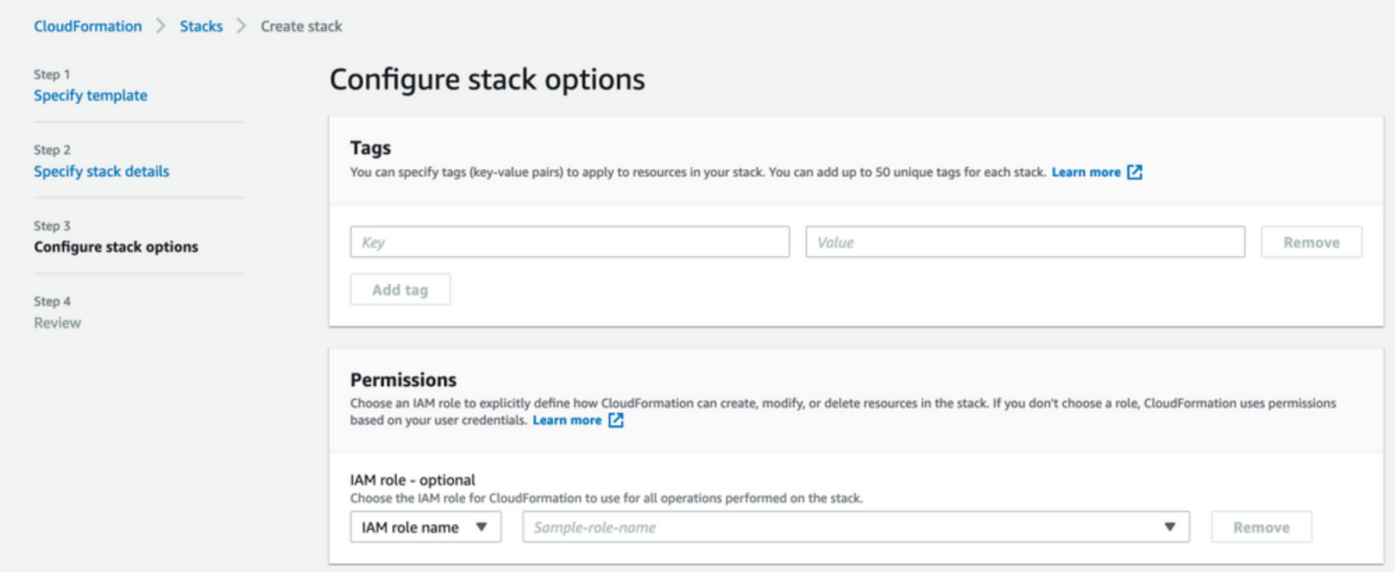
•••••••••

Confirm Password

Retype Password

•••••••••

Er zijn geen wijzigingen vereist op het volgende scherm. Selecteer **Volgende**.



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

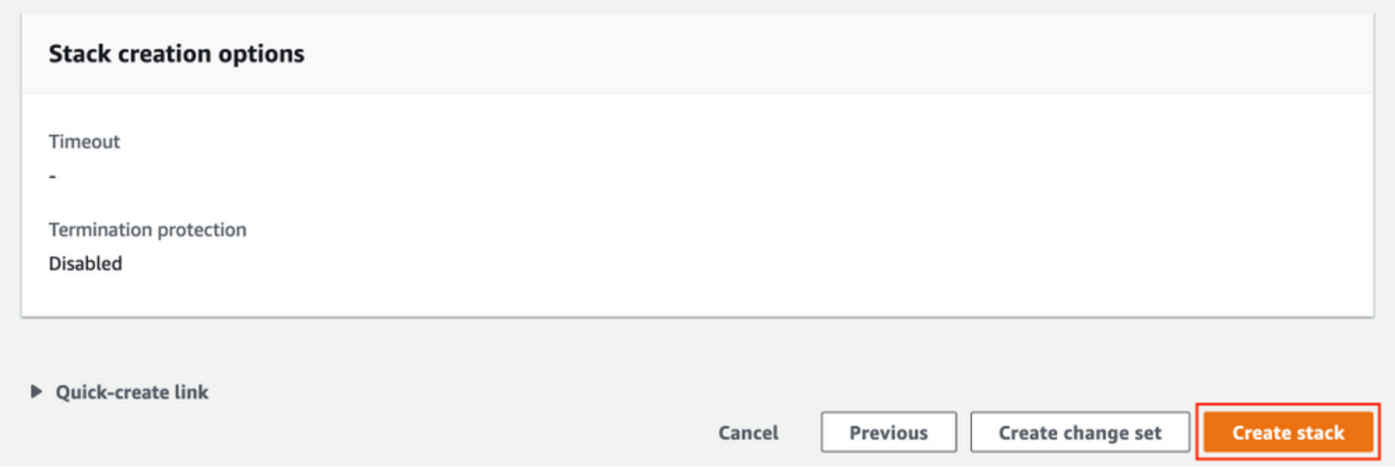
Permissions

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.

Ga over het scherm **Review Stack**, scrollen en selecteer **Stack maken**.



Stack creation options

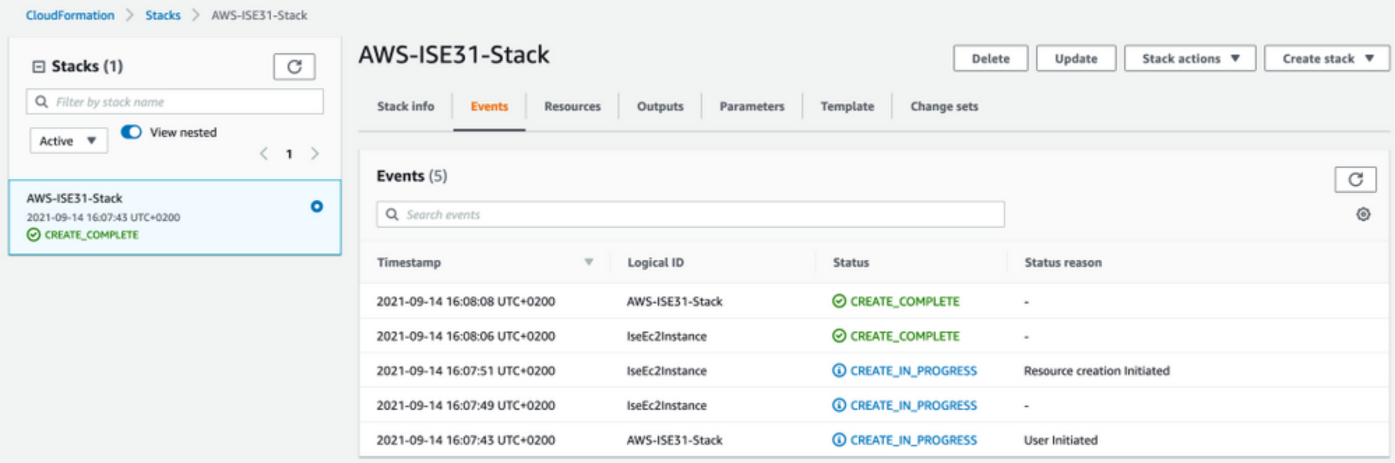
Timeout

-

Termination protection

Disabled

Zodra de Stack is ingezet moet **CREATE_COMPLETE** status worden gezien.



CloudFormation > Stacks > AWS-ISE31-Stack

Stacks (1)

Active ▼ View nested

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

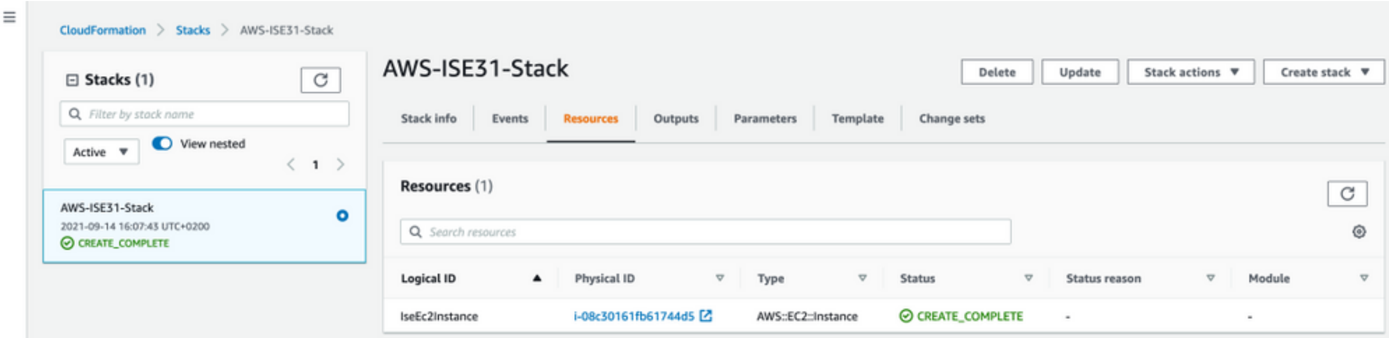
AWS-ISE31-Stack

Events (5)

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

Stap 5. Access ISE op AWS

Om toegang tot ISE te krijgen, navigeer naar het tabblad **Resources** om de EC2-instantie te bekijken die is gemaakt met CloudForm (in plaats daarvan navigeer naar **Services > EC2 > Instellingen** om de EC2-instanties te bekijken zoals in de afbeelding wordt getoond.



CloudFormation > Stacks > AWS-ISE31-Stack

Stacks (1)

Active ▼ View nested

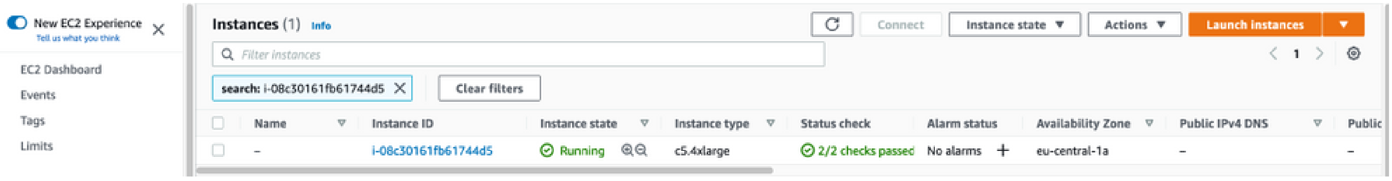
AWS-ISE31-Stack
2021-09-14 16:07:43 UTC+0200
CREATE_COMPLETE

AWS-ISE31-Stack

Resources (1)

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

Selecteer **Physical ID** om het **EC2-**menu te openen. Zorg ervoor dat de **statuscontrole 2/2 controles** heeft **doorlopen** status.



Instances (1) Info

search: i-08c30161fb61744d5

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	-	-

Selecteer **Instantie-ID**. ISE kan worden benaderd via **Private IPv4-adres/Private IPv4 DNS** met SSH of HTTPS-protocol.

> **Opmerking:** Als u toegang tot ISE hebt via **Private IPv4-adres/Private IPv4 DNS,** zorg er **voor dat** er netwerkconnectiviteit is voor ISE privé-adres.

Voorbeeld van ISE benaderd via **Private IPv4 Address** via SSH:

```
[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#
```

> **Opmerking:** Het duurt ongeveer 20 minuten voordat ISE via SSH toegankelijk is. Tot die tijd faalt de verbinding met ISE met "**Toestemming ontzegd (openbare sleutel).**" (Het stuurprogramma van de VPN-client heeft een fout aangetroffen.) getoond.

Gebruik **de** optie **showapplicatiestatus** om te controleren of de services actief zijn:

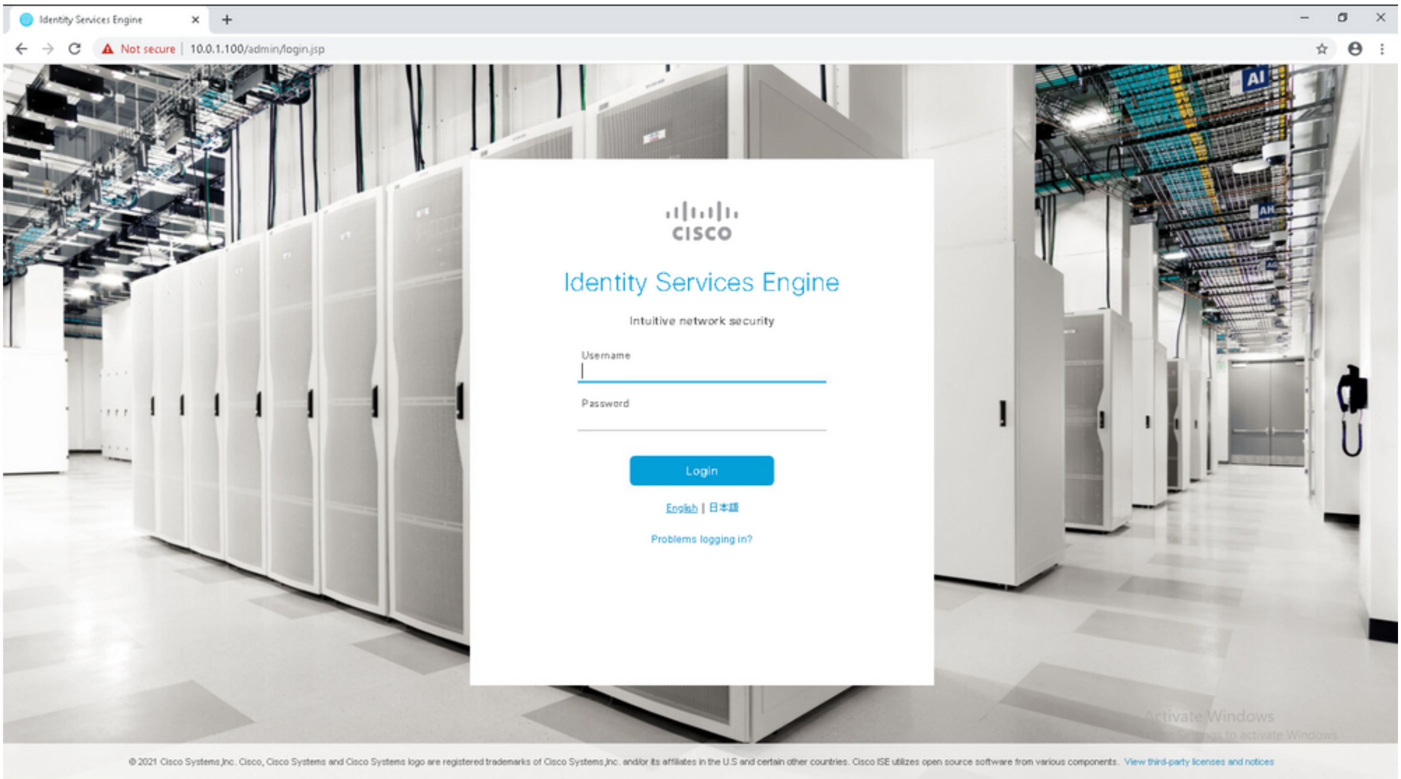
```
ISE31-2/admin# show application status ise

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#
```

> **Opmerking:** Het duurt ongeveer 10-15 minuten aangezien SSH beschikbaar is voor ISE-services om te kunnen overgaan naar een actieve staat.

Nadat de **Application Server** in **bedrijf** is in **de staat**, kunt u ISE via GUI benaderen zoals in de afbeelding wordt weergegeven.



Identity Services Engine

Intuitive network security

Username

Password

Login

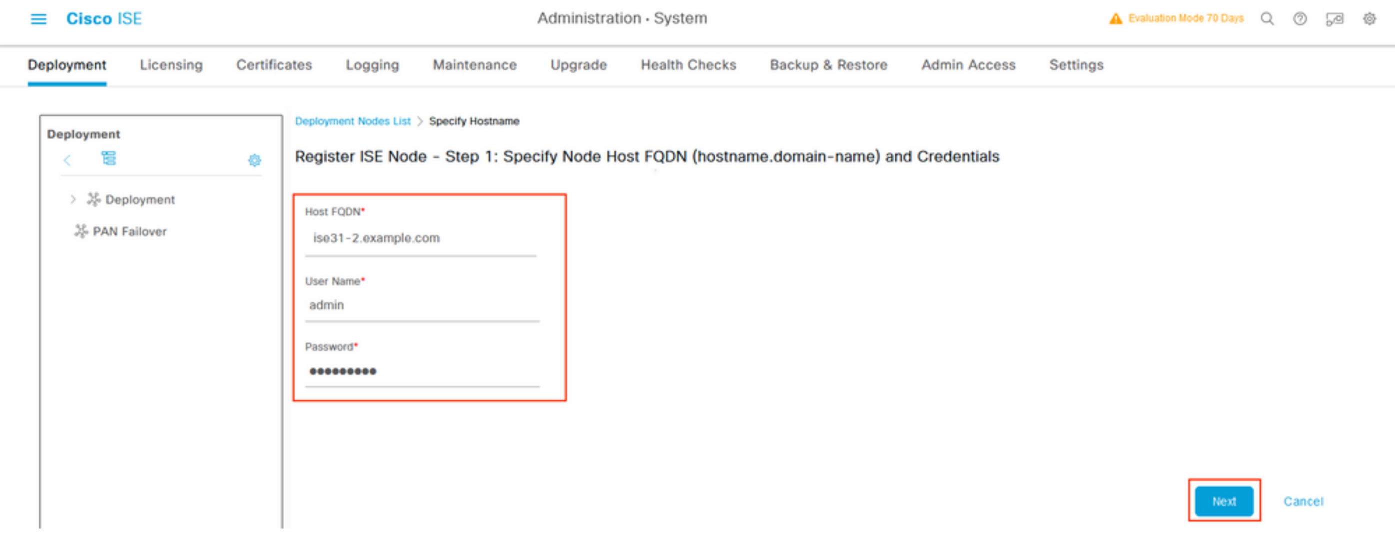
English | 日本語

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

Stap 6. Configureer gedistribueerde implementatie tussen ISE en ISE op AWS op Prem

Meld u aan bij On-Prem ISE en navigeer naar **Administratie > Systeem > Plaatsing.** Selecteer het knooppunt en selecteer **Primair maken.** Navigeer terug naar **Beheer > Systeem > Plaatsing**, selecteer **Registreer**. Configuratie van **Host FQDN** van ISE op AWS, **gebruikersnaam** en **wachtwoord** van GUI**.** Klik op **Volgende.**



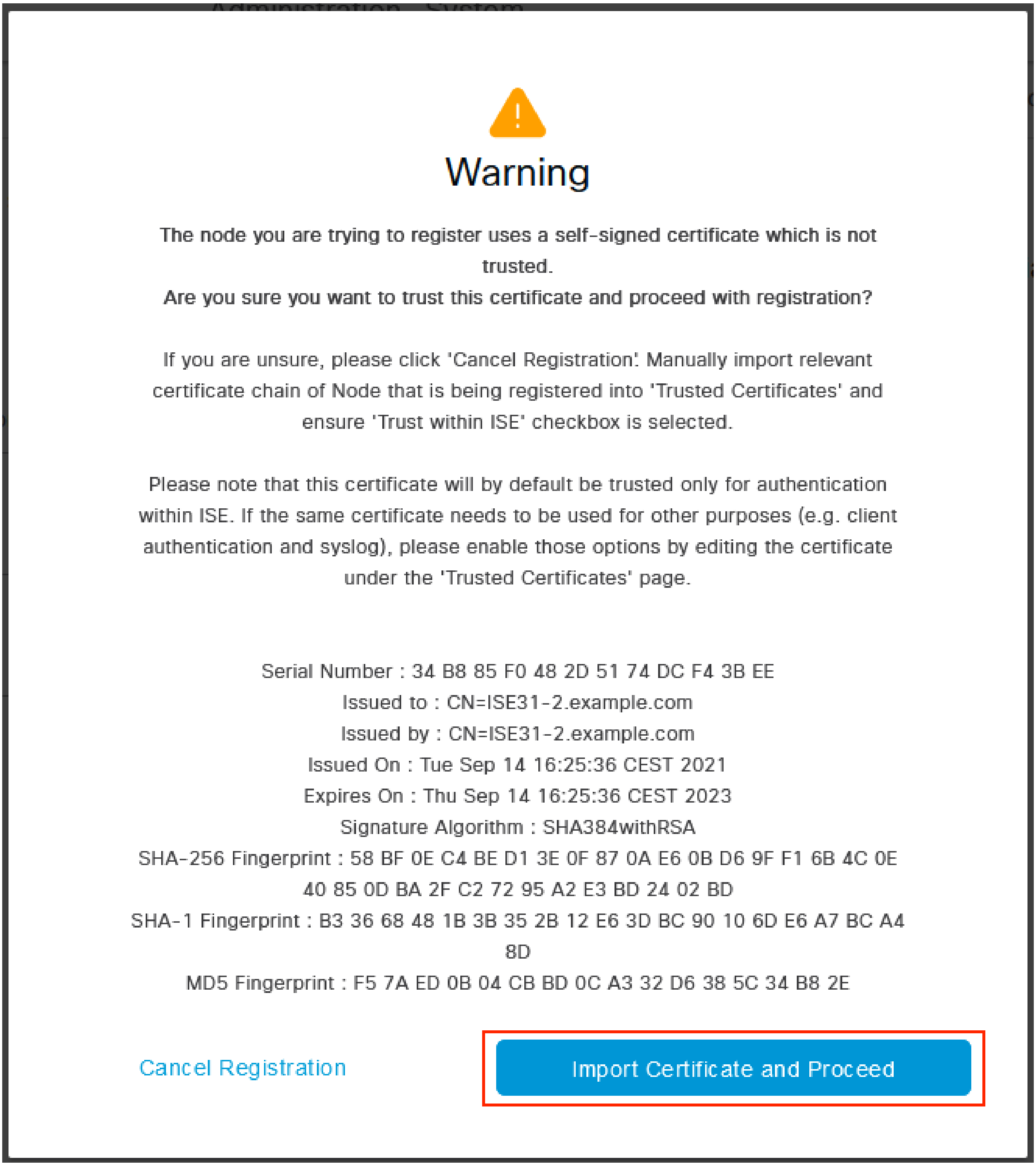
Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

Host FQDN*
ise31-2.example.com

User Name*
admin

Password*
●●●●●●●●●

Omdat de zelfgetekende certificaten in deze topologie worden gebruikt, kunt u Admin-certificaten aan de Trusted Store Selecteren **Importeren en vervolgens doorgaan.**



Warning

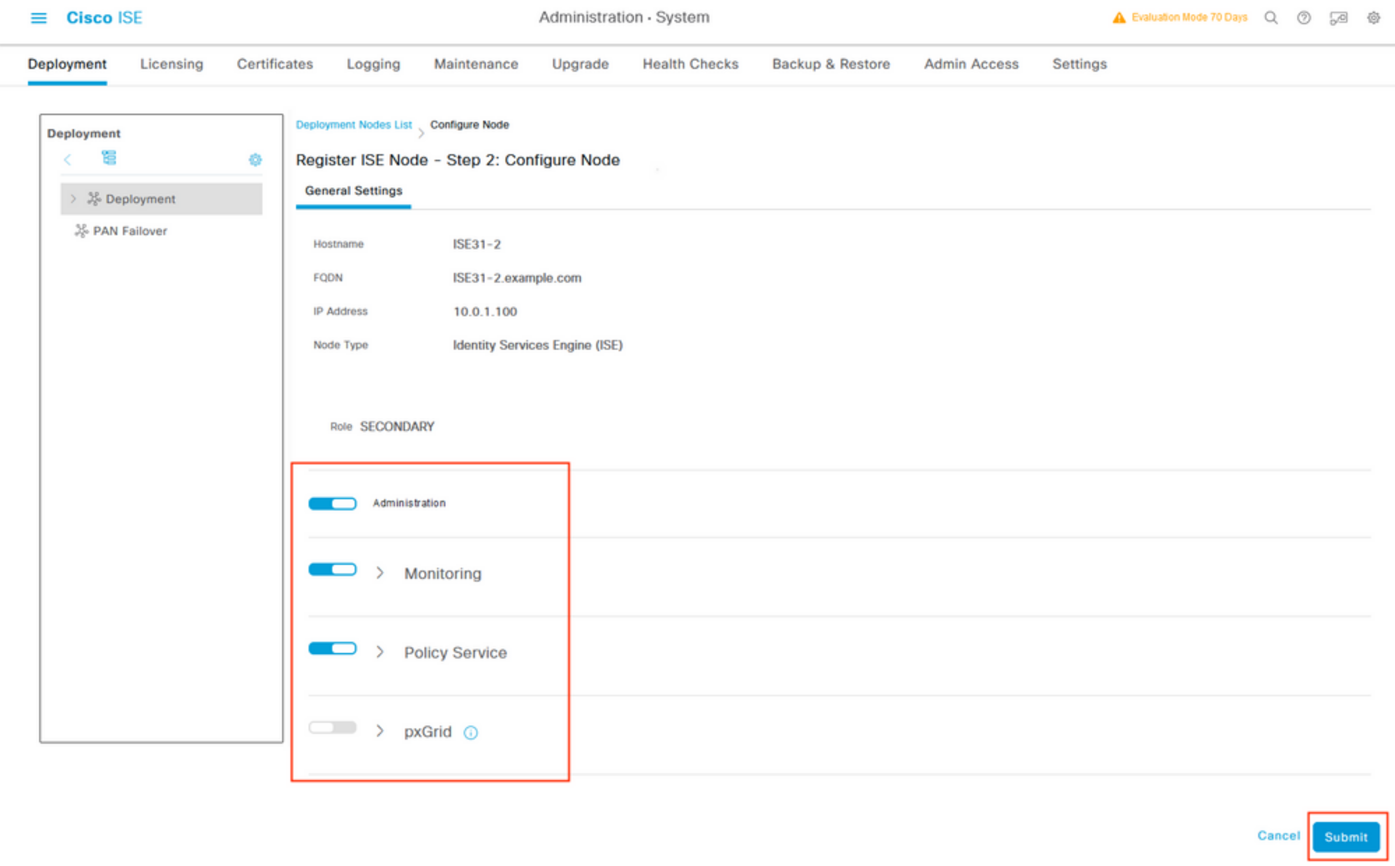
The node you are trying to register uses a self-signed certificate which is not trusted.
Are you sure you want to trust this certificate and proceed with registration?

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

Selecteer de persona's van uw keuze en klik op **Indienen**.



Register ISE Node - Step 2: Configure Node

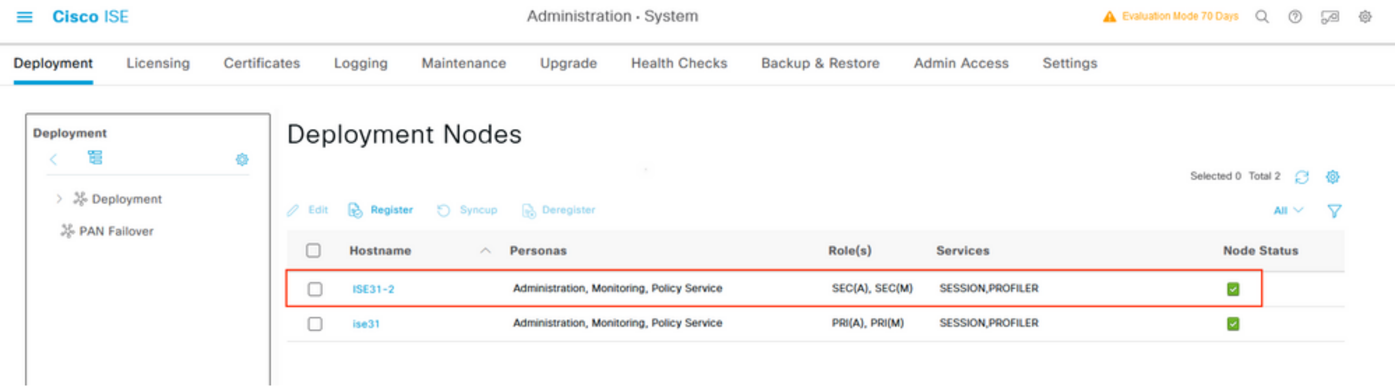
General Settings

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

Nadat de synchronisatie is voltooid, wordt het knooppunt naar de aangesloten toestand overgeschakeld en wordt het groene selectieteken ertegen weergegeven.

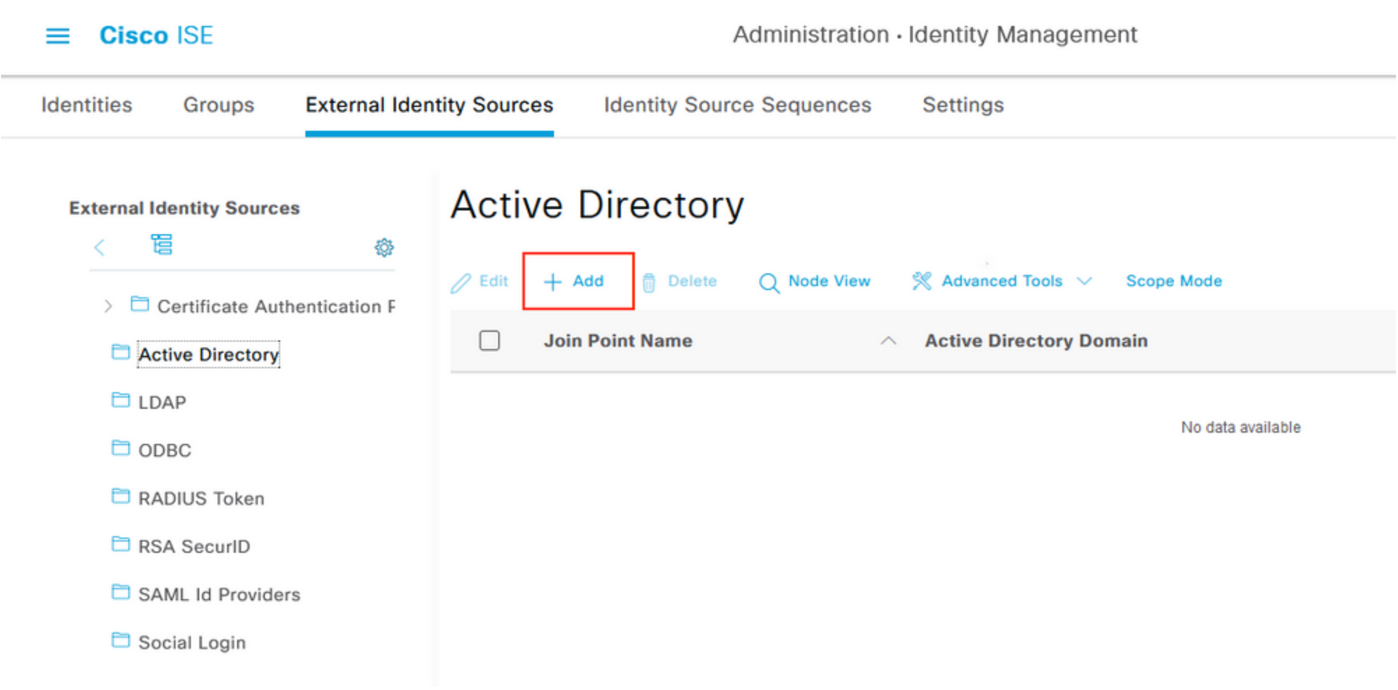


Deployment Nodes

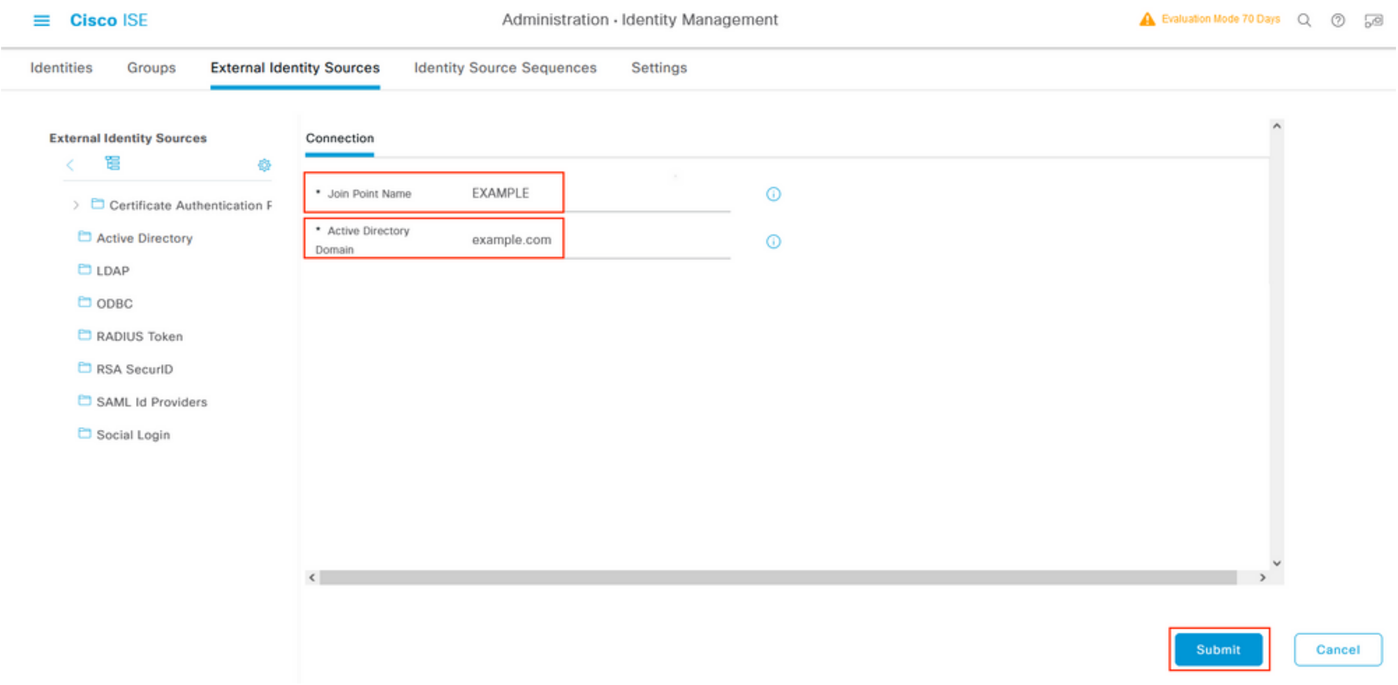
□	Hostname	Personas	Role(s)	Services	Node Status
□	ISE31-2	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	SESSION,PROFILER	✓
□	ise31	Administration, Monitoring, Policy Service	PRI(A), PRI(M)	SESSION,PROFILER	✓

Stap 7. Integratie van ISE met on-Prem AD

Navigeer naar **Administratie > identiteitsbeheer > Externe identiteitsbronnen**. Selecteer **Actieve Map** en selecteer **Toevoegen**.



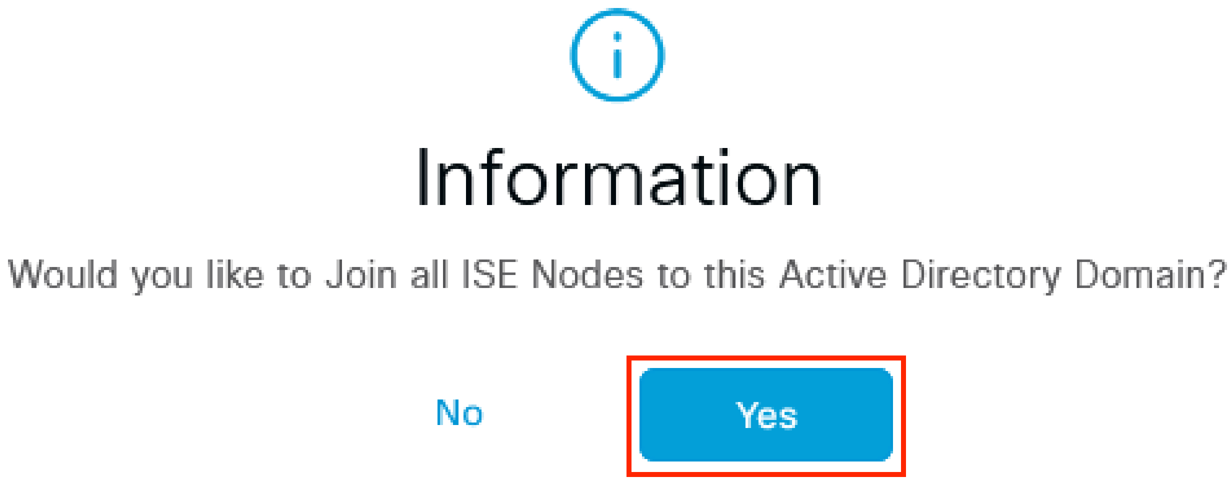
Configuratie **Joint Point Name** en **Active Directory Domain**, selecteer **Inzenden**.



* Join Point Name EXAMPLE

* Active Directory Domain example.com

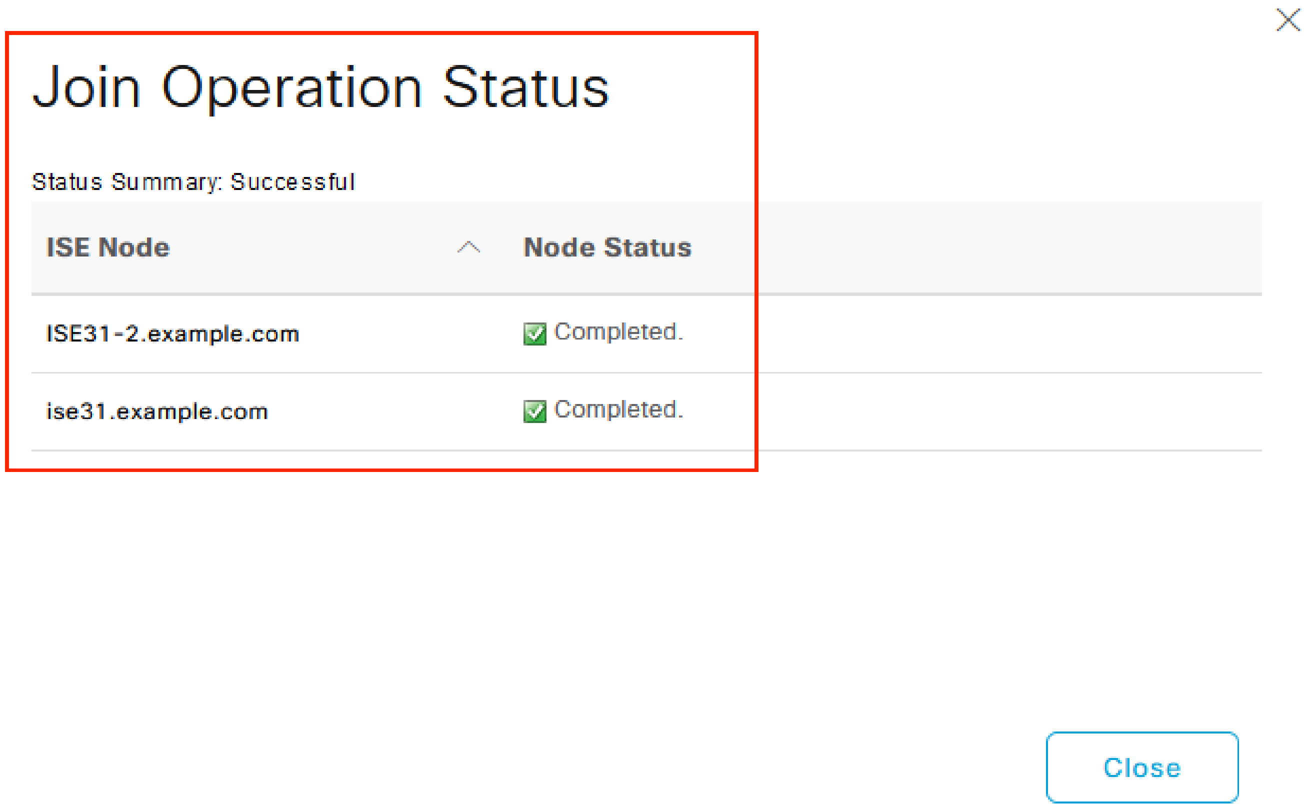
Om beide knooppunten met Actieve Map te integreren selecteert u **Ja**.



Information

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

Voer **AD-gebruikersnaam** en **wachtwoord in** en klik op **OK**. Zodra de ISE-knooppunten met succes zijn geïntegreerd in de actieve map, verandert de status van knooppunt in voltooid.



Join Operation Status

Status Summary: Successful

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

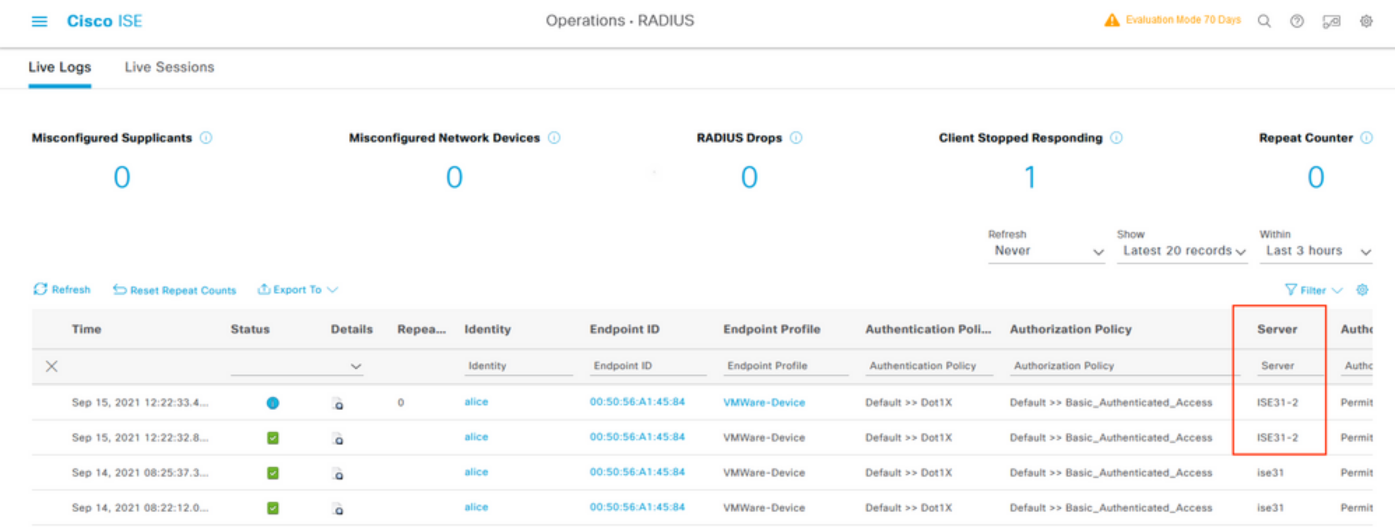
Beperkingen

Raadpleeg voor ISE over AWS-beperkingen het gedeelte met bekende beperkingen van de ISE Admin Guide.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Om verificatie van de verificatie op ISE PSN op AWS uit te voeren, navigeer naar **Operations > Straal > Live Logs** en bevestig in de **serverkolom** ISE op AWS PSN.



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

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

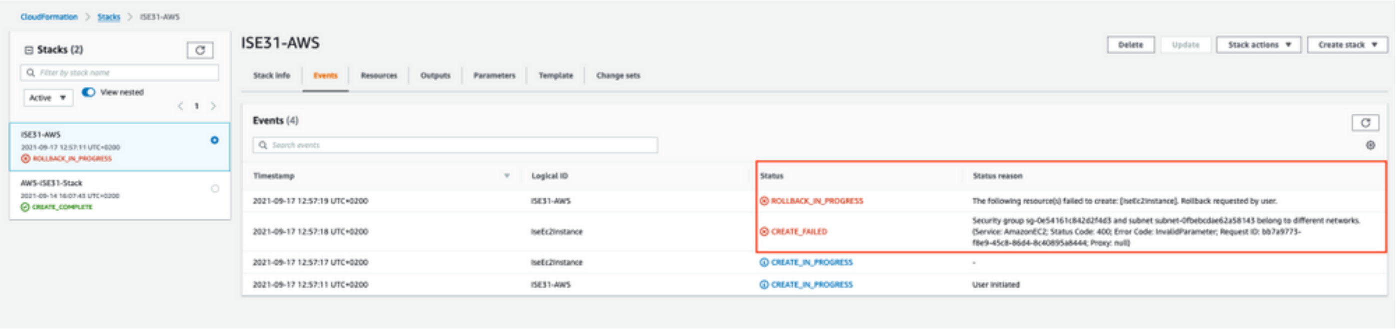
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Poli...	Authorization Policy	Server	Authc
Sep 15, 2021 12:22:33.4...	●		0	alice	00:50:56:A1:45:84	VMWare-Device	Default >> Dot1X	Default >> Basic_Authenticated_Access	ISE31-2	Permit
Sep 15, 2021 12:22:32.8...	✓			alice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

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Creatie van CloudFormation Stack is mislukt

Creatie van de Stack van de CloudFormation kan om meerdere redenen falen, is één van hen wanneer u die Veiligheidsgroep van VPN selecteert die van het Netwerk van het Beheer van ISE verschilt. De fout lijkt op de fout in de afbeelding.



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

Events (4)

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

Oplossing:

Zorg ervoor dat u de Security Group van dezelfde VPC oppelt. Navigeer naar **beveiligingsgroepen** onder de **VPC-**service en neem nota van de **beveiligingsgroep-ID**, controleer of deze overeenkomt met de juiste VPC (waar ISE verblijft), controleer **VPC-id**.

Connectiviteitsproblemen

Er kunnen meerdere problemen zijn die de verbinding met ISE op AWS niet kunnen veroorzaken.

1. Connectiviteitsprobleem als gevolg van foutieve **beveiligingsgroepen.**

Oplossing: ISE kan niet bereikbaar zijn via het On-Prem netwerk of zelfs binnen AWS netwerken als **Beveiligingsgroepen** verkeerd zijn geconfigureerd. Zorg ervoor dat de vereiste protocollen en poorten zijn toegestaan in de **Security Group** die aan het ISE-netwerk is gekoppeld. Raadpleeg de ISE-poortreferentie voor vereiste poorten om te openen.

2. Connectiviteitsproblemen als gevolg van foutieve routing.

Oplossing: Vanwege de complexiteit van de topologie is het makkelijk om bepaalde routes tussen het On-Prem netwerk en AWS te missen. Voordat u ISE-functies kunt gebruiken, dient u ervoor te zorgen dat de end-to-end connectiviteit op zijn plaats is.

Bijlage

Configuratie van switch AAA/Radius

```
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
```