

Configuración de ISE 3.1 a través de AWS Marketplace

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Topología de red](#)

[Configuraciones](#)

[Paso A opcional. Crear VPC](#)

[Paso B opcional. Configuración del dispositivo de cabecera VPN en las instalaciones](#)

[Paso C opcional Crear un par de claves personalizado](#)

[Paso D opcional. Crear grupo de seguridad personalizado](#)

[Paso 1. Suscripción al producto AWS ISE Marketplace](#)

[Paso 2. Configuración de ISE en AWS](#)

[Paso 3. Iniciar ISE en AWS](#)

[Paso 4. Configuración de la pila de formación de nube para ISE en AWS](#)

[Paso 5. Acceso a ISE en AWS](#)

[Paso 6. Configuración de la implementación distribuida entre ISE in situ e ISE en AWS](#)

[Paso 7. Integración de la implementación de ISE con AD in situ](#)

[Limitaciones](#)

[Verificación](#)

[Troubleshoot](#)

[Error al crear la pila de formación de la nube](#)

[Inconvenientes de conectividad](#)

[Appendix](#)

[Configuración relacionada con el switch AAA/Radius](#)

Introducción

Este documento describe cómo instalar Identity Services Engine (ISE) 3.1 a través de Amazon Machine Images (AMI) en Amazon Web Services (AWS). Desde la versión 3.1, ISE se puede implementar como una instancia de Amazon Elastic Compute Cloud (EC2) con la ayuda de CloudFormation Templates (CFT).

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

- ISE
- AWS y sus conceptos como VPC, EC2, CloudFormation

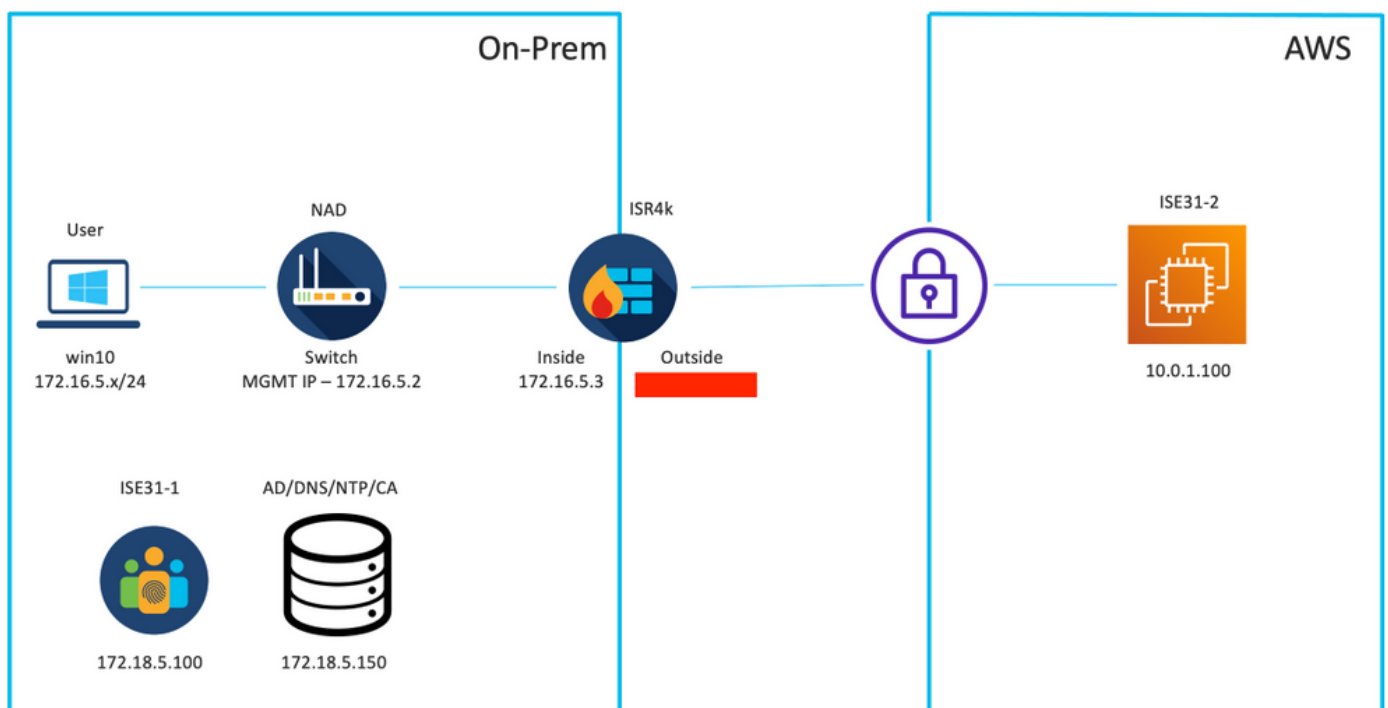
Componentes Utilizados

La información de este documento se basa en la versión 3.1 de Cisco ISE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Topología de red



Configuraciones

Si todavía no se ha configurado ningún VPC, grupos de seguridad, pares de claves y túnel VPN, debe seguir los pasos opcionales; de lo contrario, comience con el paso 1.

Paso A opcional. Crear VPC

Vaya al servicio **VPC AWS**. Seleccione **Iniciar Asistente de VPC** como se muestra en la imagen.

The screenshot shows the AWS VPC Dashboard for the Frankfurt region. At the top, there are buttons for "Launch VPC Wizard" (highlighted in orange) and "Launch EC2 Instances". A note states: "Note: Your Instances will launch in the Europe (Frankfurt) region." Below this, the "Resources by Region" section shows a list of resources:

Resource Type	Count
VPCs	1
NAT Gateways	0
Subnets	3
VPC Peering Connections	0
Route Tables	1
Network ACLs	1

Elija VPC con Private Subnet Only y Hardware VPN Access y haga clic en **Select** como se muestra en la imagen.

The screenshot shows "Step 1: Select a VPC Configuration" in the AWS VPC Wizard. On the left, there are four VPC configuration options:

- 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** (highlighted with a red border)

The main content area describes the selected 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." It also includes a "Creates:" section: "A /16 network with a /24 subnet and provisions an IPsec VPN tunnel between your Amazon VPC and your corporate network. (VPN charges apply.)" A blue "Select" button is highlighted with a red border. To the right, a diagram shows an "Amazon Virtual Private Cloud Subnet" connected via "VPN" to a "Corporate Data Center".

Nota: La selección de VPC en el Paso 1. del asistente de VPC depende de la topología, ya que ISE no está diseñado como servidor expuesto a Internet; se utiliza VPN con subred privada solamente.

Configure los parámetros de subred privada de VPC según su diseño de red y seleccione **Siguiente**.

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

Cancel and Exit Back Next

Configure su VPN según su diseño de red y seleccione **Crear VPC**.

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)

Cancel and Exit Back Create VPC

Una vez creado el VPC, se muestra el mensaje "Su VPC se ha creado correctamente". Haga clic en **Aceptar** como se muestra en la imagen.

VPC Successfully Created

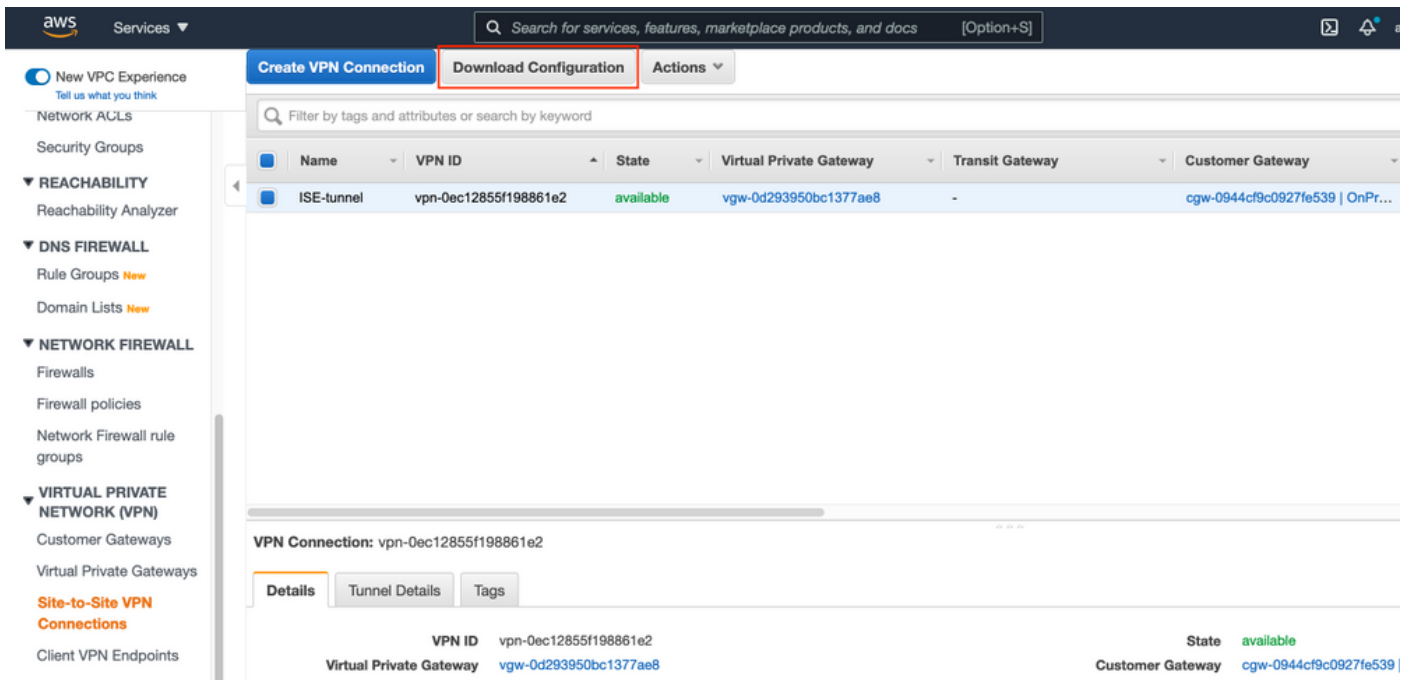
Your VPC has been successfully created.

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

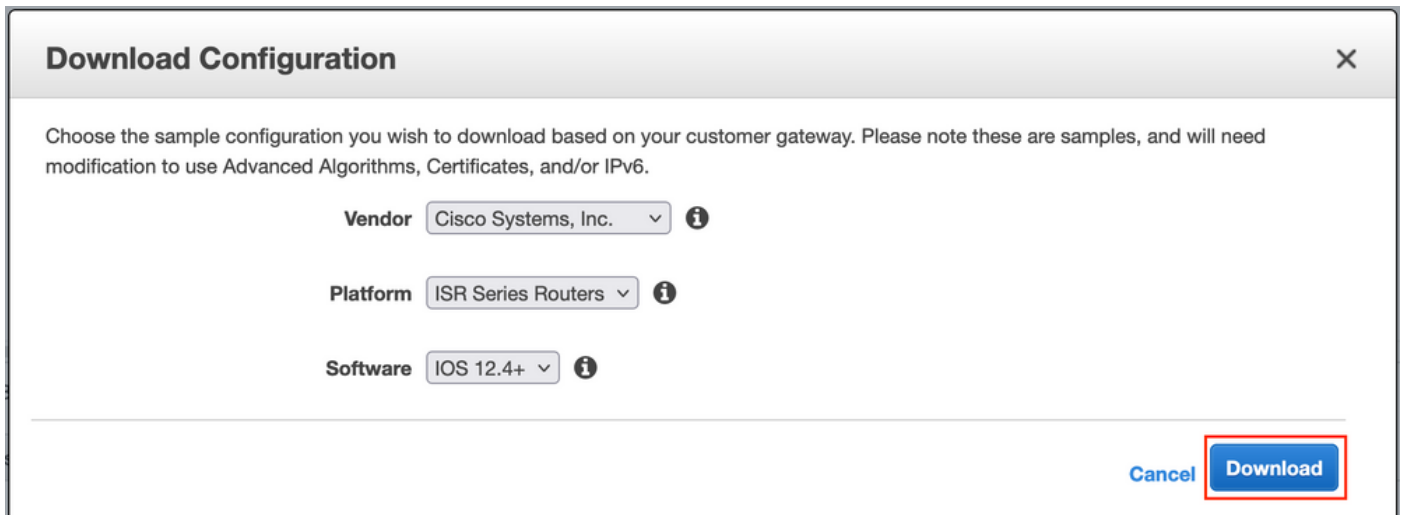
OK

Paso B opcional. Configuración del dispositivo de cabecera VPN en las instalaciones

Vaya al servicio VPC AWS. Elija **conexiones VPN de sitio a sitio**, seleccione el túnel VPN recién creado y seleccione **Configuración de descarga** como se muestra en la imagen.



Elija **Proveedor**, **Plataforma** y **Software**, Seleccione **Descarga** como se muestra en la imagen.



Aplice la configuración descargada en el dispositivo de cabecera VPN en las instalaciones.

Paso C opcional Crear un par de claves personalizado

Se accede a las instancias de AWS EC2 con la ayuda de pares clave. Para crear un par de claves, navegue al servicio **EC2**. Seleccione **el menú Pares de Teclas en Red y Seguridad**. Seleccione **Crear par de claves**, asígnele un **nombre**, deje otros valores como predeterminados y seleccione **Crear par de claves de nuevo**.

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

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

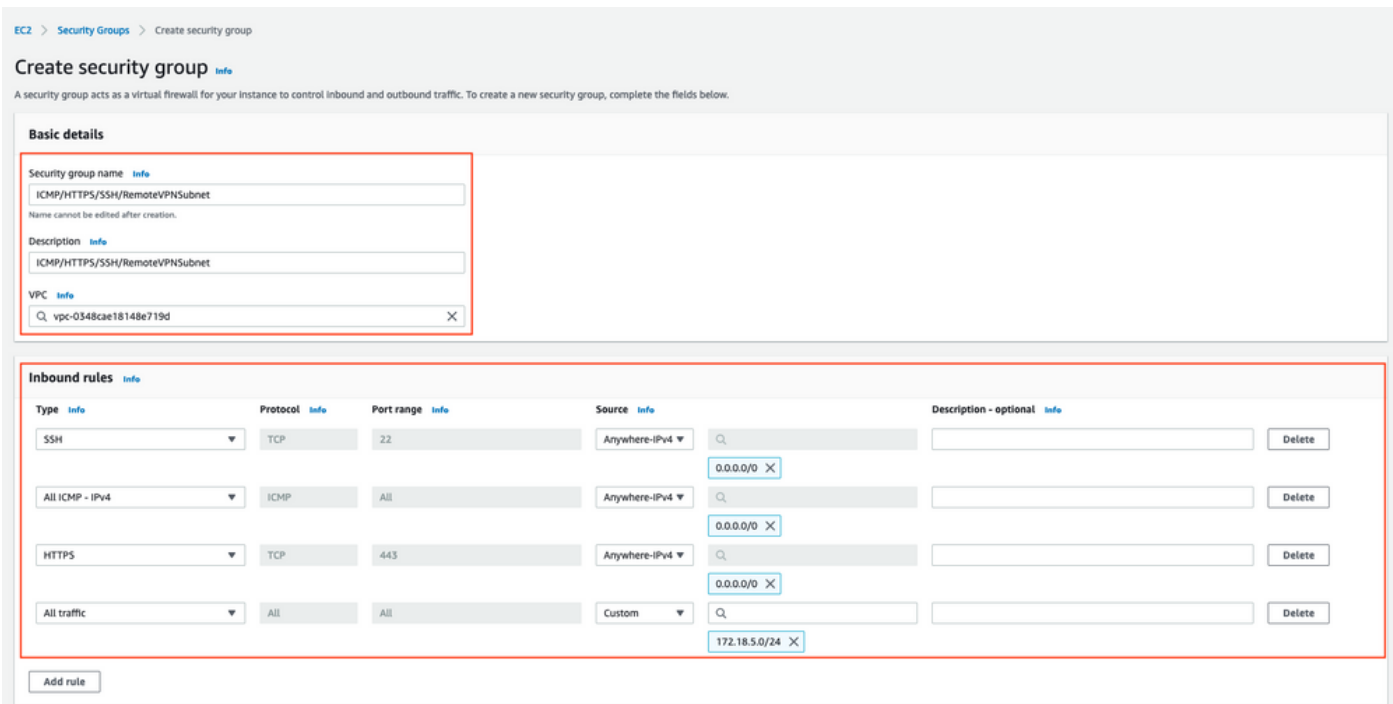
Tags (Optional)

No tags associated with the resource.

You can add 50 more tags.

Paso D opcional. Crear grupo de seguridad personalizado

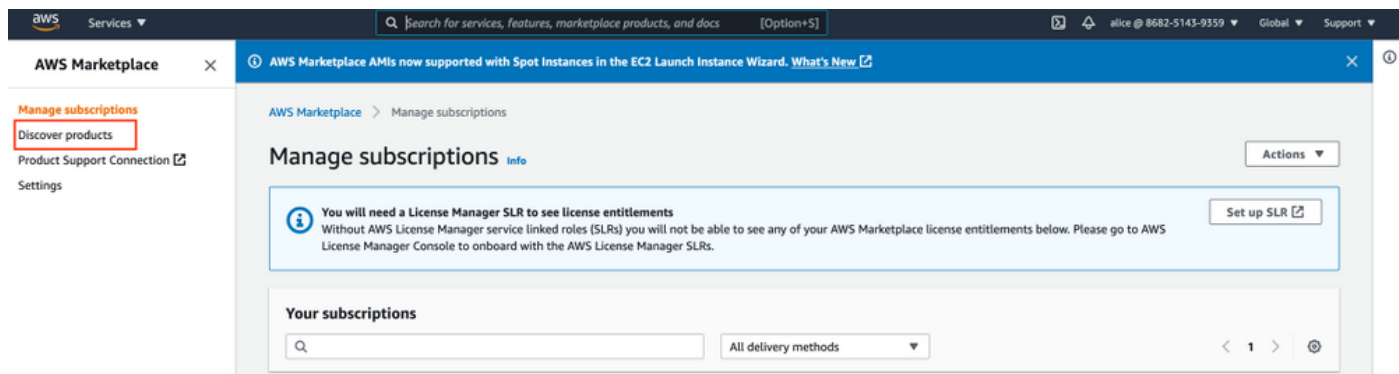
El acceso de instancias de AWS EC2 está protegido por **grupos de seguridad**, para configurar el **grupo de seguridad**, navegue al servicio **EC2**. Seleccione el menú **Grupos de seguridad** en **Red y Seguridad**. Seleccione **Crear grupo de seguridad**, configure un **nombre**, **descripción**, en el campo **VPC** seleccione **VPC** recientemente configurado. Configure **las reglas entrantes** para permitir la comunicación a ISE. Seleccione **Crear grupo de seguridad** como se muestra en la imagen.



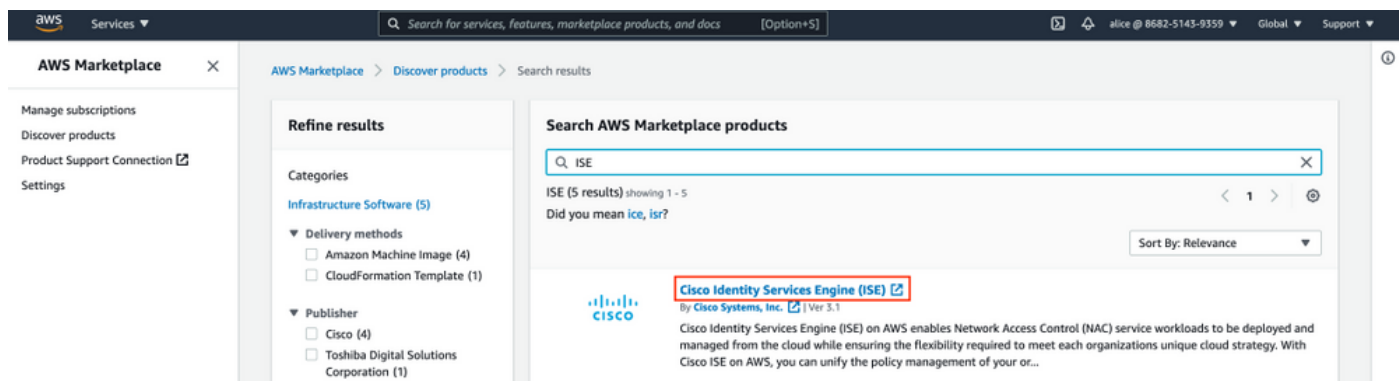
Nota: El grupo de seguridad configurado permite el acceso SSH, ICMP, HTTPS a ISE y a todos los protocolos desde la subred en las instalaciones.

Paso 1. Suscripción al producto AWS ISE Marketplace

Vaya al servicio **AWS Marketplace Subscriptions**. Seleccione **Discover Products** como se muestra en la imagen.



Busque el producto **ISE** y seleccione **Cisco Identity Services Engine (ISE)** como se muestra en la imagen.



Seleccione el botón **Continuar para suscribirse**

aws marketplace

Categories ▾ Delivery Methods ▾ Solutions ▾ AWS IQ ▾ Resources ▾ Your Saved List 1

Hello, alice ▾

Partners Sell in AWS Marketplace Amazon Web Services Home Help

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**

Continue to Subscribe

Remove

Typical Total Price
\$0.68/hr

Total pricing per instance for services hosted on c5.4xlarge in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Reviews

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).

Seleccione el botón **Aceptar términos** como se muestra en la imagen.

aws marketplace

Categories ▾ Delivery Methods ▾ Solutions ▾ AWS IQ ▾ Resources ▾ Your Saved List 1

Hello, alice ▾

Partners Sell in AWS Marketplace Amazon Web Services Home Help

Cisco Identity Services Engine (ISE)

Continue to Configuration

You must first review and accept terms.

[Product Detail](#) [Subscribe](#)

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.

Accept Terms

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)	Cisco Identity Services Engine (ISE)

Una vez suscrito, el estado de **fecha de vigencia y vencimiento** con el cambio a pendiente como se muestra en la imagen.

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

Poco después de la **fecha de entrada en vigor**, los cambios en la fecha de suscripción y la **fecha de vencimiento** cambian a **N/A**. Seleccione **Continuar a la configuración** como se muestra en el ima



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

Paso 2. Configuración de ISE en AWS

En el menú Método de entrega de la **pantalla Configurar este software** seleccione **Cisco Identity Services Engine (ISE)**. En la **versión de software** seleccione **3.1 (12 de agosto de 2021)**. Seleccione la **región**, donde se planea implementar ISE. Seleccione **Continuar para iniciar**.



[< 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) **\$0/hr**

BYOL

running on c5.4xlarge

Paso 3. Iniciar ISE en AWS

En el menú desplegable Acciones de la pantalla **Iniciar este software**, seleccione **Iniciar formación de nube**.



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) <i>running on c5.4xlarge</i>
Software Version	3.1
Region	EU (Frankfurt)

[Usage Instructions](#)

Choose Action

- Select a launch action
- Launch CloudFormation
- Copy to Service Catalog

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

[Launch](#)

(Opcional) Seleccione **Instrucciones de uso** para familiarizarse con ellas. Seleccione **Iniciar**.

Paso 4. Configuración de la pila de formación de nube para ISE en AWS

El botón de **inicio** le dirige a la pantalla de configuración de la **pila de formación** en la **nube**. Hay una plantilla prediseñada que se debe utilizar para configurar ISE. Mantenga los parámetros predeterminados y seleccione **Siguiente**.

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/awssmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e57-579d-4492-bf3d-e495ba9:

Amazon S3 template URL
S3 URL: https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/bedef662-aba4-427e-b523-7c93cd50111c.f7b45e57-579d-4492-bf3d-e495ba925376.template [View in Designer](#)

Cancel [Next](#)

Rellene los datos de la pila de formación de nube con **nombre de pila**. Configure los detalles de la instancia como **nombre de host**, seleccione **par de claves de instancia** y **grupo de seguridad de administración**.

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/RemoteVPSubnet (sg-0792bfa6bba47098d)

Continuar configuración de detalles de instancia con **Red de administración**, **IP privada de administración**, **Zona horaria**, **Tipo de instancia**, **Cifrado EBS** y **Tamaño del volumen**.

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-0fbecdae62a58143 (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 ↕

Continuar configuración de detalles de instancia con **dominio DNS, servidor de nombres, servicio NTP y servicios.**

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 ▼

Configure la contraseña de usuario de la GUI y seleccione **Next**.

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

.....

Cancel Previous **Next**

No se requiere ningún cambio en la siguiente pantalla. Seleccione **Next**.

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](#)

Key Value Remove

Add tag

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.

IAM role name Sample-role-name Remove

Vaya a la pantalla **Revisar pila**, desplácese hacia abajo y seleccione **Crear pila**.

Stack creation options

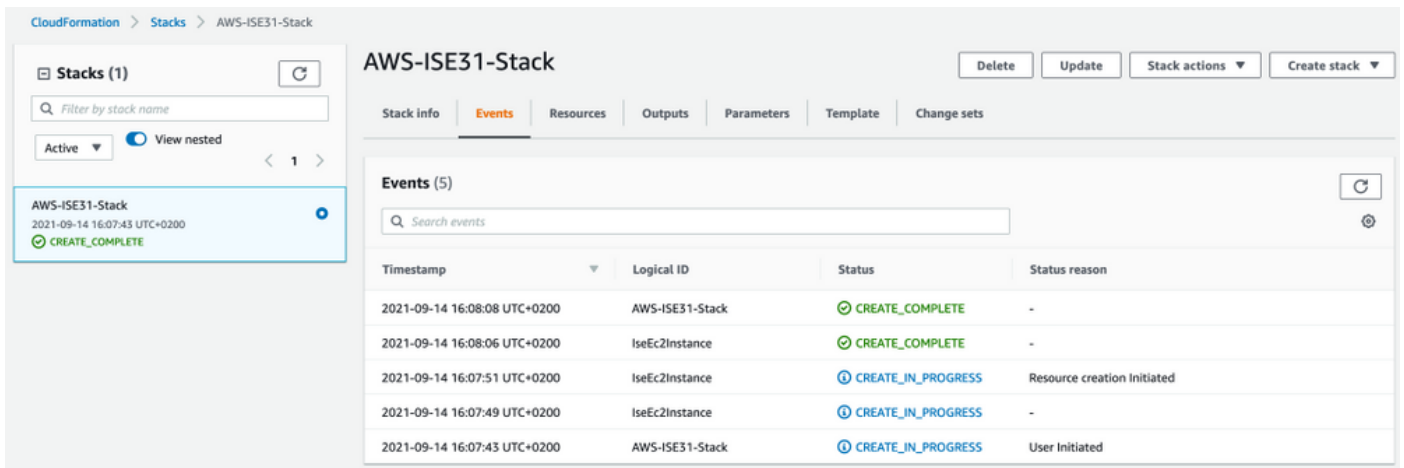
Timeout
-

Termination protection
Disabled

► Quick-create link

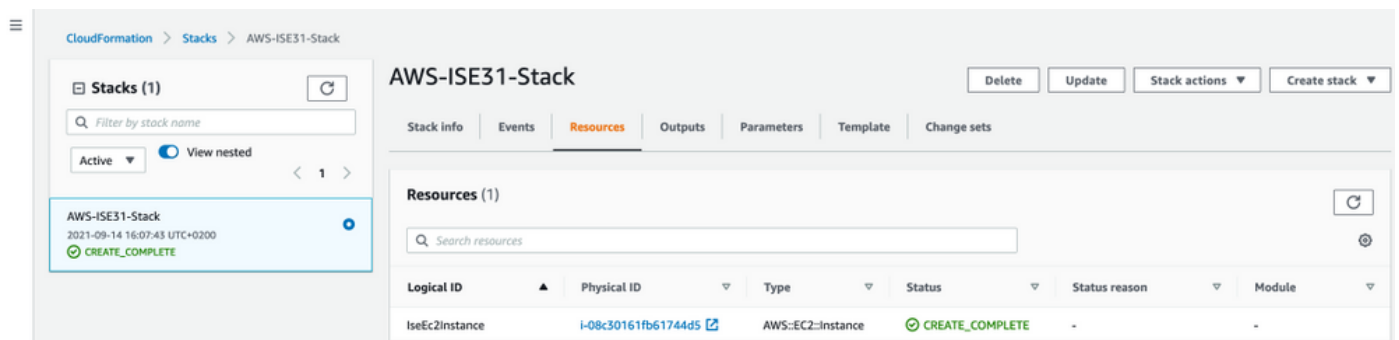
Cancel Previous Create change set **Create stack**

Una vez que se implementa la pila, se debe ver el estado **CREATE_COMPLETE**.

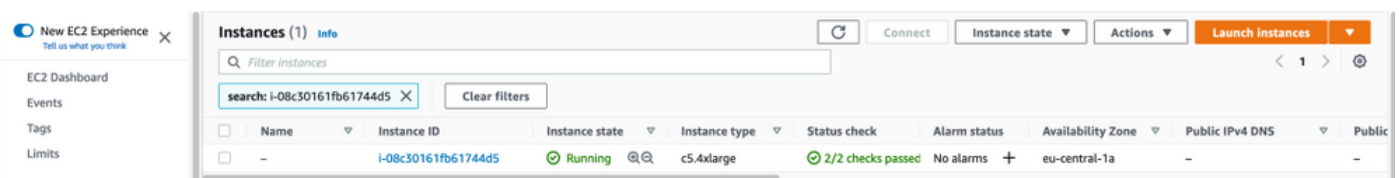


Paso 5. Acceso a ISE en AWS

Para acceder a la instancia de ISE, navegue a la ficha **Resources** para ver la instancia EC2 creada desde CloudForms (también navegue hasta **Services > EC2 > Instones** para ver las instancias EC2) como se muestra en la imagen.



Seleccione **Physical ID** para abrir el menú **EC2 Instancias**. Asegúrese de que la **verificación de estado** tenga el estado **2/2 verificaciones pasadas**.



Seleccione **ID de instancia**. Se puede acceder a ISE a través de la **dirección IPv4 privada/DNS IPv4 privado** con el protocolo SSH o HTTPS.

Nota: Si accede a ISE a través de la **dirección IPv4 privada/DNS IPv4 privado**, asegúrese de que haya conectividad de red hacia la dirección privada de ISE.

Ejemplo de ISE al que se accede a través de **dirección IPv4 privada** a través de 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:G5NdGZ1rgPYnjlndPcXOLcJg9VICLSxnZA0kn0CfMPs.
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#

Nota: Se tardan unos 20 minutos en llegar a ISE a través de SSH. Hasta ese momento, la conectividad con ISE falla con "**Permiso denegado (clave pública)**". .

Utilice **show application status ise** para verificar que los servicios se estén ejecutando:

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

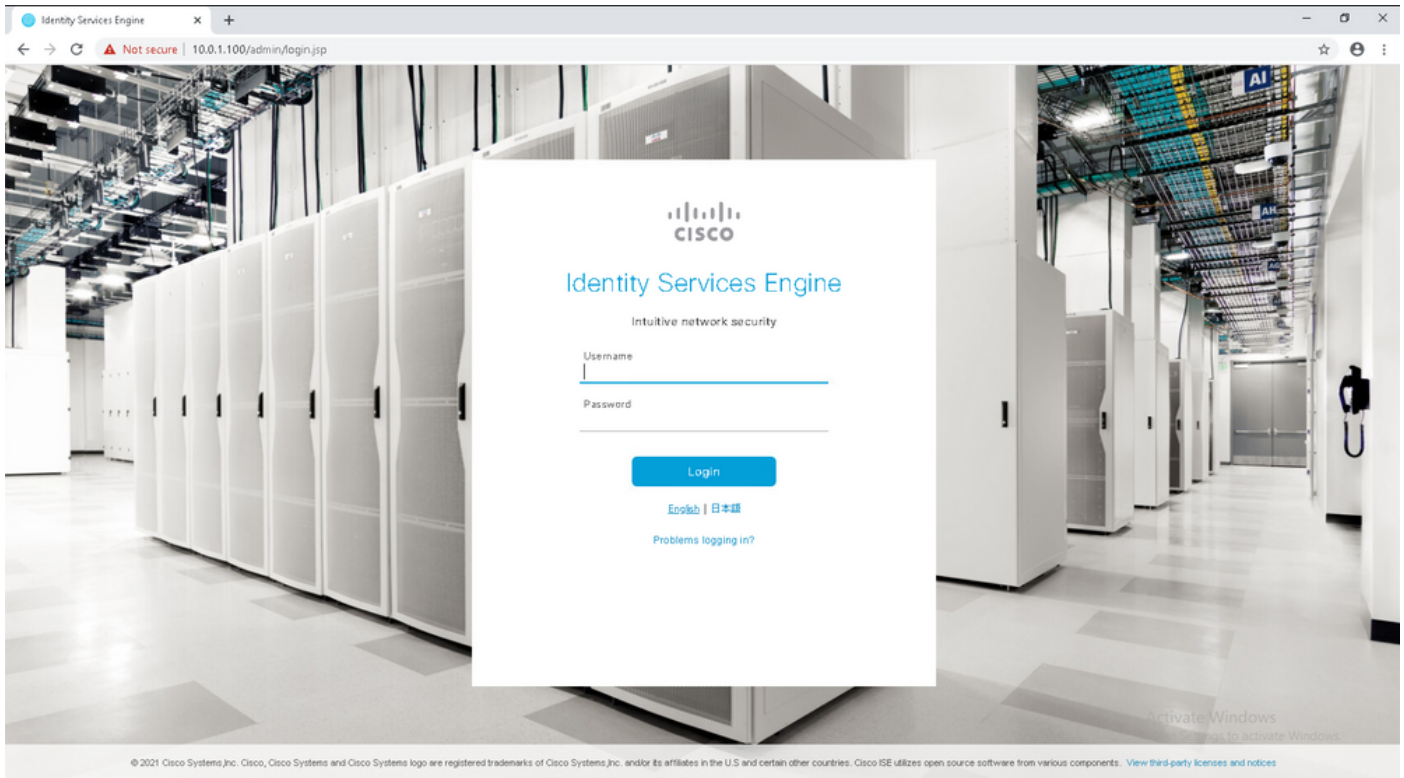
```
ISE PROCESS NAME STATE PROCESS ID
```

```
-----  
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#
```

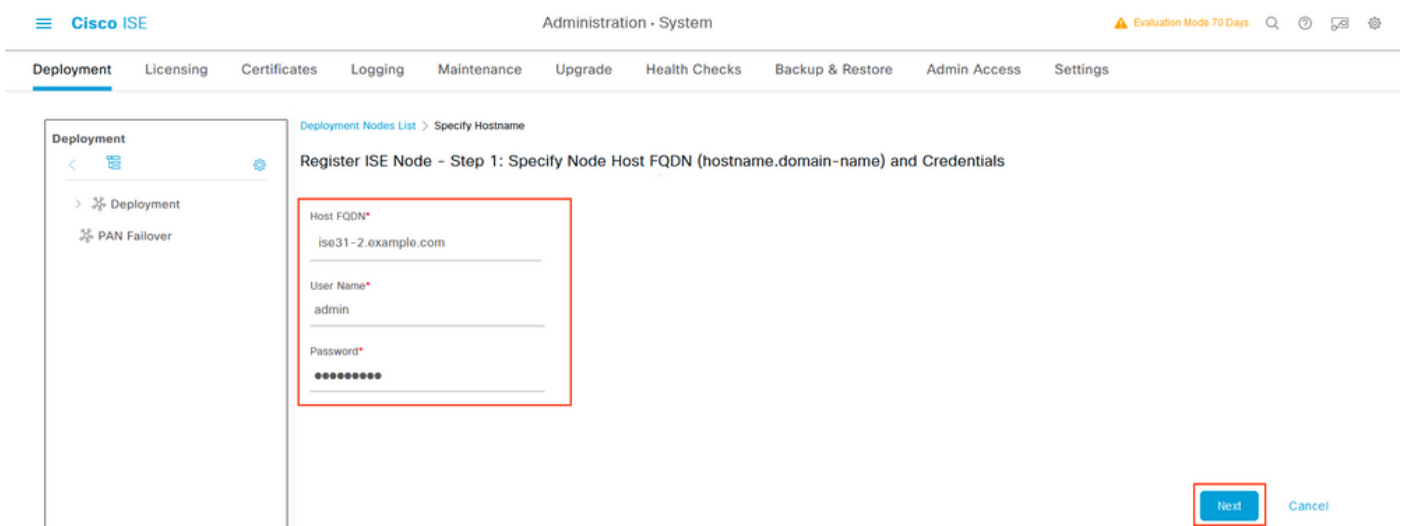
Nota: Se tardan entre 10 y 15 minutos desde que SSH está disponible para que los servicios ISE realicen la transición a un estado en ejecución.

Una vez que el **servidor de aplicaciones** esté ejecutando State, puede acceder a ISE a través de la GUI, como se muestra en la imagen.



Paso 6. Configuración de la implementación distribuida entre ISE in situ e ISE en AWS

Inicie sesión en In-Prem ISE y navegue hasta **Administration > System > Deployment**. Seleccione el nodo y Seleccione **Make Primary**. Vuelva a **Administration > System > Deployment**, Seleccione **Register**. Configure **FQDN de host** de ISE en AWS, **Nombre de usuario** de la GUI y **Contraseña**. Haga clic en **Next (Siguiete)**.



Dado que los certificados autofirmados se utilizan en esta topología, para importar certificados de administrador al **certificado de importación** Select de almacén de confianza y **continuar**.



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

[Cancel Registration](#)

[Import Certificate and Proceed](#)

Seleccione las Personas de su elección y haga clic en **Enviar**.

Cisco ISE Administration - System Evaluation Mode 70 Days

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Deployment Nodes List > Configure Node

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 ⓘ

Cancel Submit

Una vez finalizada la sincronización, el nodo pasa al estado conectado, se muestra la casilla de verificación verde.

Cisco ISE Administration - System Evaluation Mode 70 Days

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Deployment Nodes

Selected 0 Total 2

Edit Register Syncup Deregister

<input type="checkbox"/>	Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	ISE31-2	Administration, Monitoring, Policy Service	SEC(A), SEC(M)	SESSION, PROFILER	<input checked="" type="checkbox"/>
<input type="checkbox"/>	ise31	Administration, Monitoring, Policy Service	PRI(A), PRI(M)	SESSION, PROFILER	<input checked="" type="checkbox"/>

Paso 7. Integración de la implementación de ISE con AD in situ

Vaya a **Administration > Identity Management > External Identity Sources**. Seleccione **Active Directory**, Seleccione **Add**.

External Identity Sources

- <
- > Certificate Authentication F
- Active Directory**
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

Active Directory

Edit **+ Add** Delete Node View Advanced Tools Scope Mode

Join Point Name ^ **Active Directory Domain**

No data available

Configure **Joint Point Name** y **Active Directory Domain**, Seleccione **Submit**.

External Identity Sources

- <
- > Certificate Authentication F
- Active Directory**
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

Connection

* Join Point Name	EXAMPLE	
* Active Directory Domain	example.com	

Submit

Cancel

Para integrar ambos nodos con Active Directory, seleccione **Yes**.



Information

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

No

Yes

Ingrese **AD User Name** y **Password**, haga clic en **OK**. Una vez que los nodos ISE se integran correctamente con Active Directory, el estado del nodo cambia a Completed (Finalizado).



Join Operation Status

Status Summary: Successful

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

Close

Limitaciones

Para conocer las limitaciones de ISE en AWS, consulte la sección [Limitaciones conocidas](#) de la Guía de administración de ISE.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para verificar que la autenticación se realiza en el ISE PSN ubicado en AWS, navegue hasta **Operaciones > Radius > Registros en directo** y confirme en la columna **Servidor ISE en AWS PSN**.

The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are navigation tabs for 'Live Logs' and 'Live Sessions'. Below this, there are several summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (0), 'Client Stopped Responding' (1), and 'Repeat Counter' (0). Below these cards, there are buttons for 'Refresh', 'Reset Repeat Counts', and 'Export To'. A table below shows RADIUS logs with columns for Time, Status, Details, Repea..., Identity, Endpoint ID, Endpoint Profile, Authentication Poli..., Authorization Policy, Server, and Authc. The 'Server' column is highlighted with a red box, showing values like 'ISE31-2' and 'ise31'.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Error al crear la pila de formación de la nube

La creación de la pila de formación de la nube puede fallar por varias razones, una de ellas es cuando se selecciona ese grupo de seguridad de la VPN, que es diferente de la red de administración de ISE. El error se parece al de la imagen.

The screenshot shows the AWS CloudFormation console for the 'ISE31-AWS' stack. The 'Events' tab is selected, showing a list of events. A red box highlights an error event with the status 'CREATE_FAILED'. The status reason is: 'Security group sg-0451161c8123f4e3 and subnet subnet-0fb0cda61258143 belong to different networks. (Service: AmazonEC2; Status Code: 400; Errr Code: InvalidParameter; Request ID: b07d9773-f8e9-45c8-8644-8c40895a8444; Proxy: null)'. The stack name 'ISE31-AWS' is also visible in the left sidebar.

Solución:

Asegúrese de recoger el grupo de seguridad del mismo VPC. Navegue hasta **Grupos de Seguridad** bajo el **Servicio VPC**, y observe la **ID de grupo de seguridad**, asegúrese de que corresponde al VPC correcto (donde reside ISE), verifique la **ID de VPC**.

Inconvenientes de conectividad

Puede haber varios problemas que pueden hacer que la conectividad a ISE en AWS no funcione.

1. Problema de conectividad debido a **grupos de seguridad** mal configurados.

Solución: ISE no se puede alcanzar desde la red in situ o incluso dentro de las redes AWS si se configuran incorrectamente **grupos de seguridad**. Asegúrese de que los protocolos y puertos requeridos estén permitidos en el **grupo de seguridad** asociado a la red ISE. Refiérase a [Referencia de Puertos ISE](#) para los Puertos Requeridos que se abrirán.

2. Problemas de conectividad debido a un ruteo mal configurado.

Solución: Debido a la complejidad de la topología, es fácil perderse algunas rutas entre la red en las instalaciones y AWS. Antes de poder utilizar las funciones de ISE, asegúrese de que existe una conectividad integral.

Appendix

Configuración relacionada con el 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
```