Configuración de ISE 3.1 a través de AWS Marketplace

Contenido

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

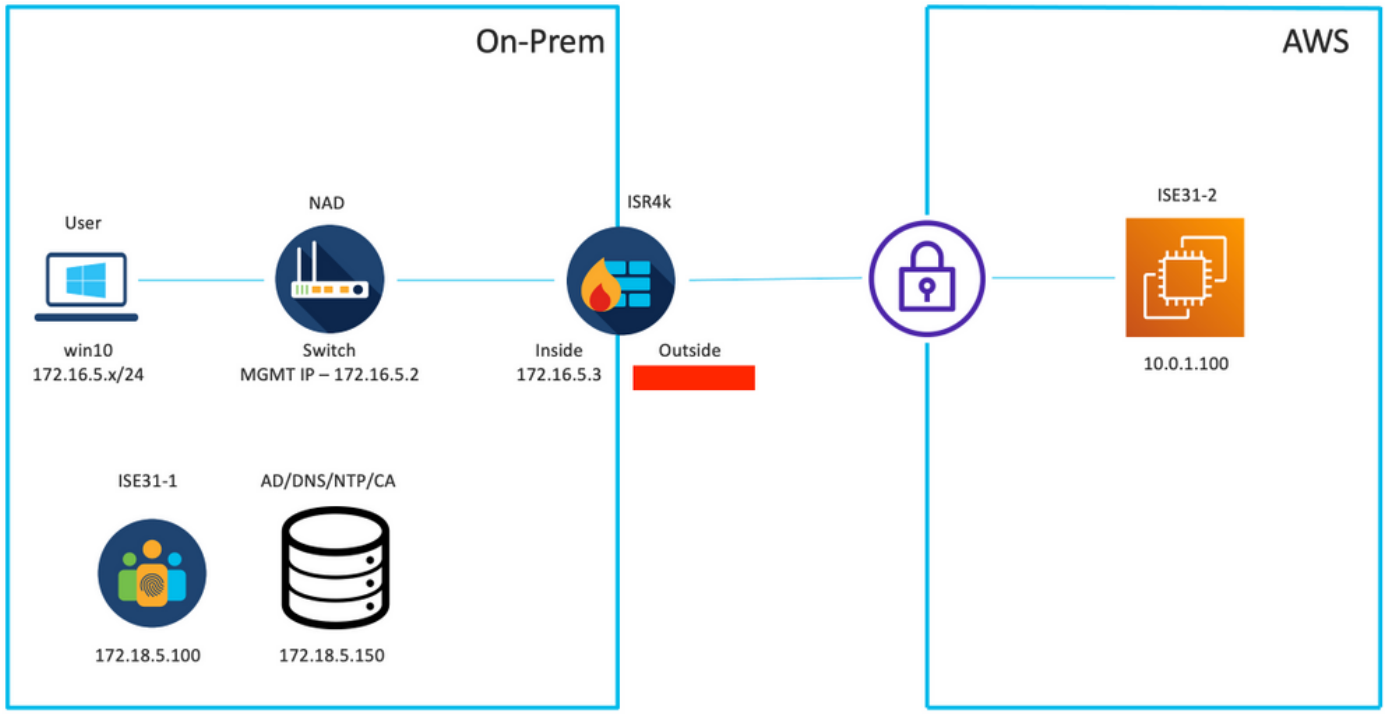
Componentes Utilizados

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

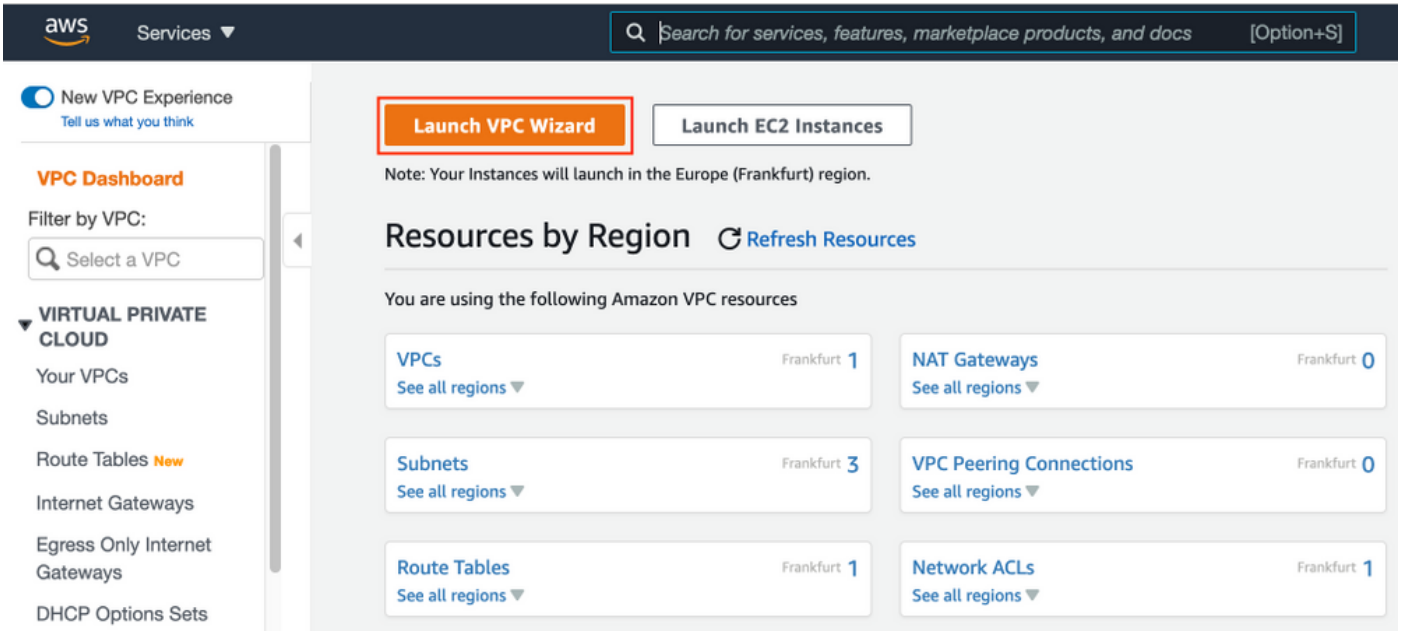


Configuraciones

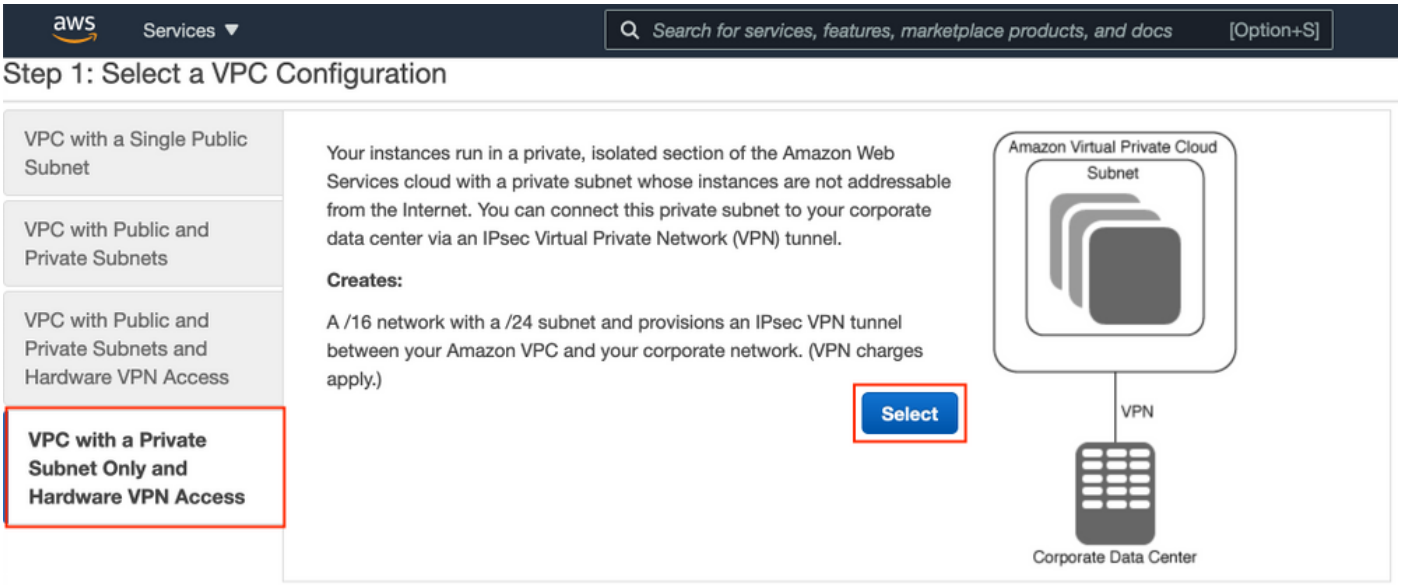
Si todavía no se ha configurado ningún VPC, grupos de seguridad, pares de claves y túnel VPN, debe seguir los pasos opcionales; de lo contrario, comience con el paso 1.

Paso A opcional. Crear VPC

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

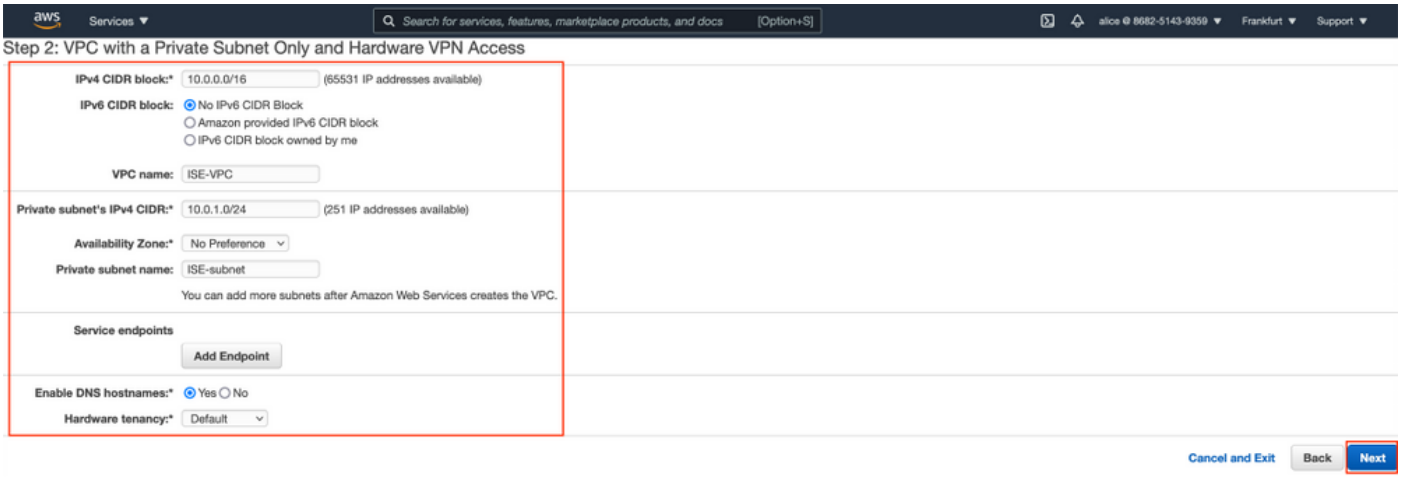


Elija **VPC con Private Subnet Only y Hardware VPN Access** y haga clic en **Select** como se muestra en la imagen.

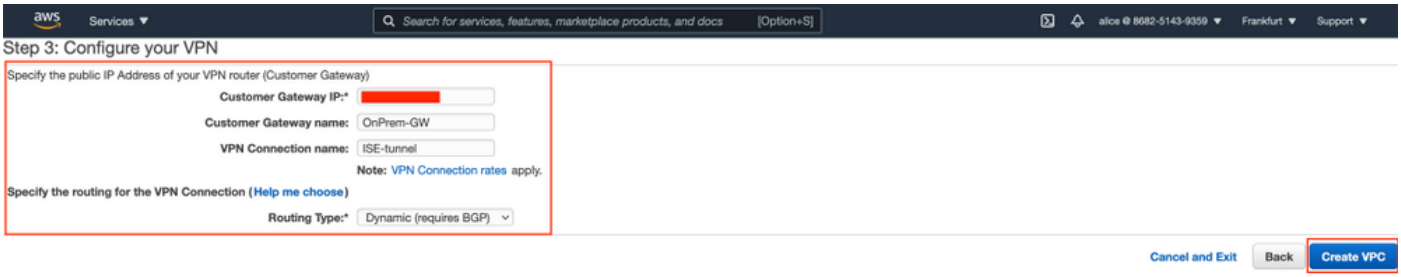


> **Nota:** La selección de VPC en el Paso 1. del asistente de VPC depende de la topología, ya que ISE no está diseñado como servidor expuesto a Internet; se utiliza VPN con subred privada solamente.

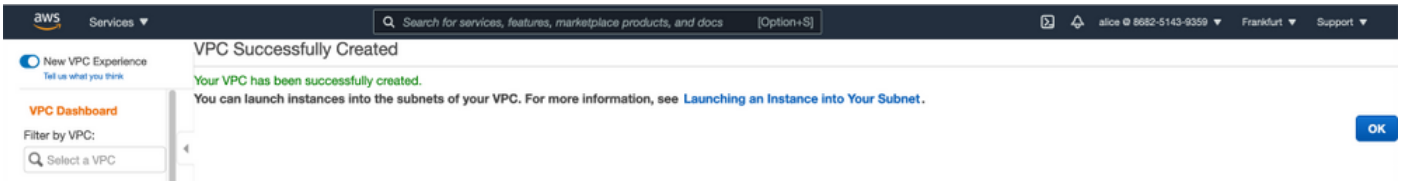
Configure los parámetros de subred privada de VPC según su diseño de red y seleccione **Siguiente**.



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

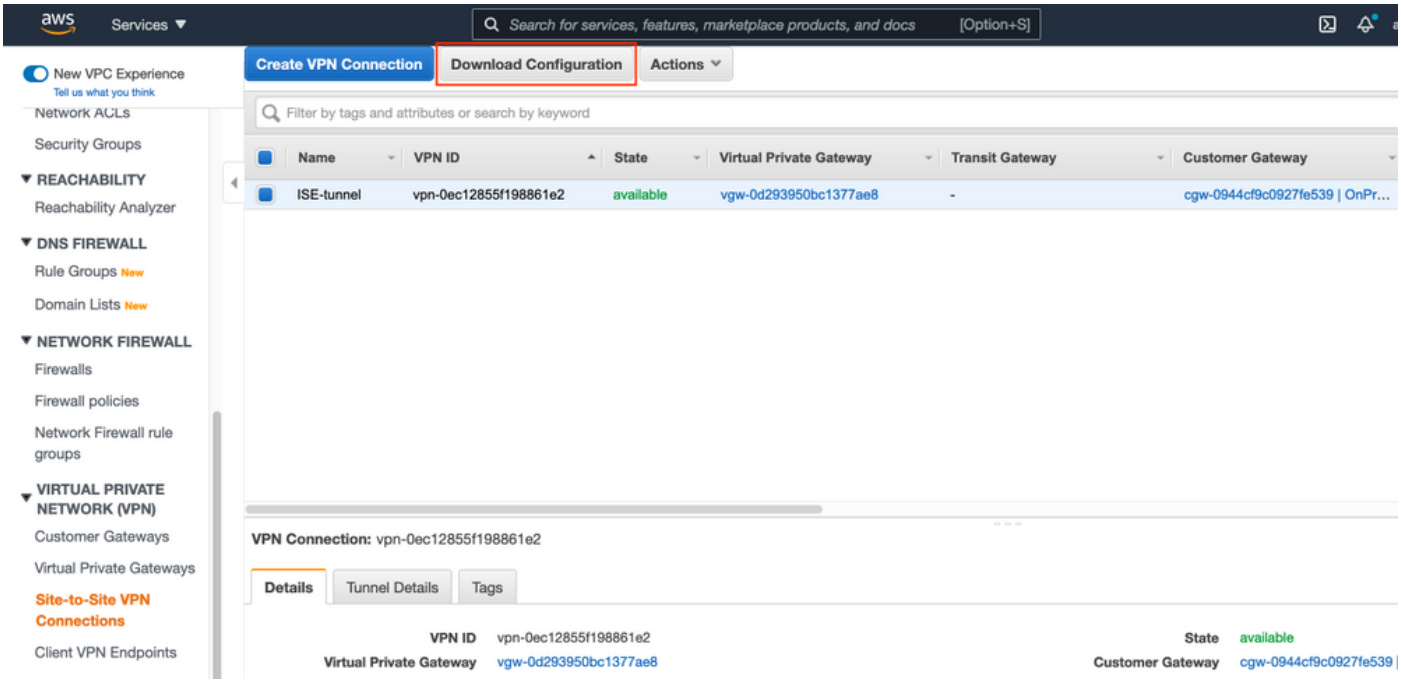


Una vez creado el VPC, se muestra el mensaje **"Su VPC se ha creado correctamente"**. Haga clic en **Aceptar** como se muestra en la imagen.



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.

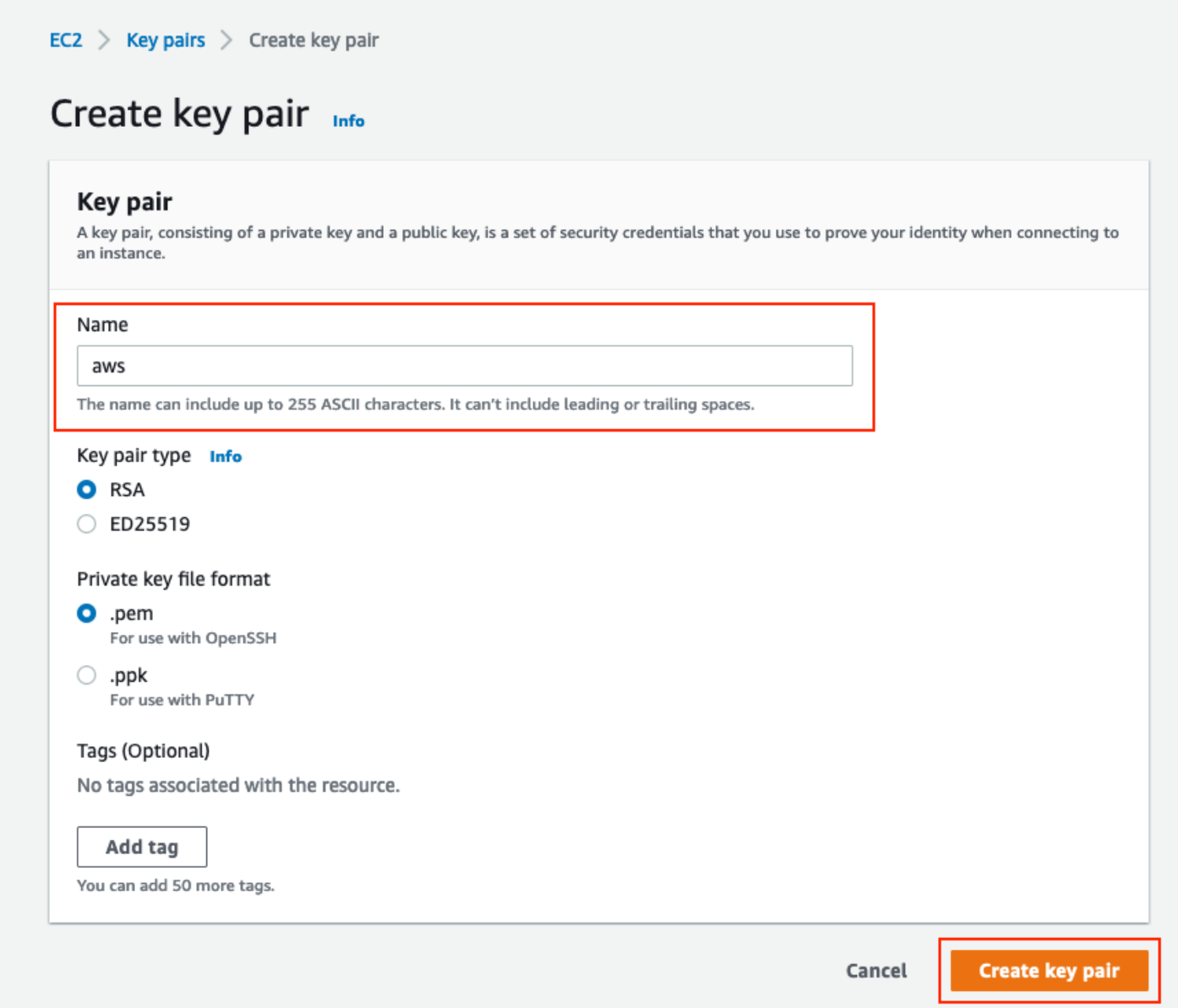


Elija **Proveedor**, **Plataforma** y **Software**, Seleccione **Descarga** como se muestra en la imagen.

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

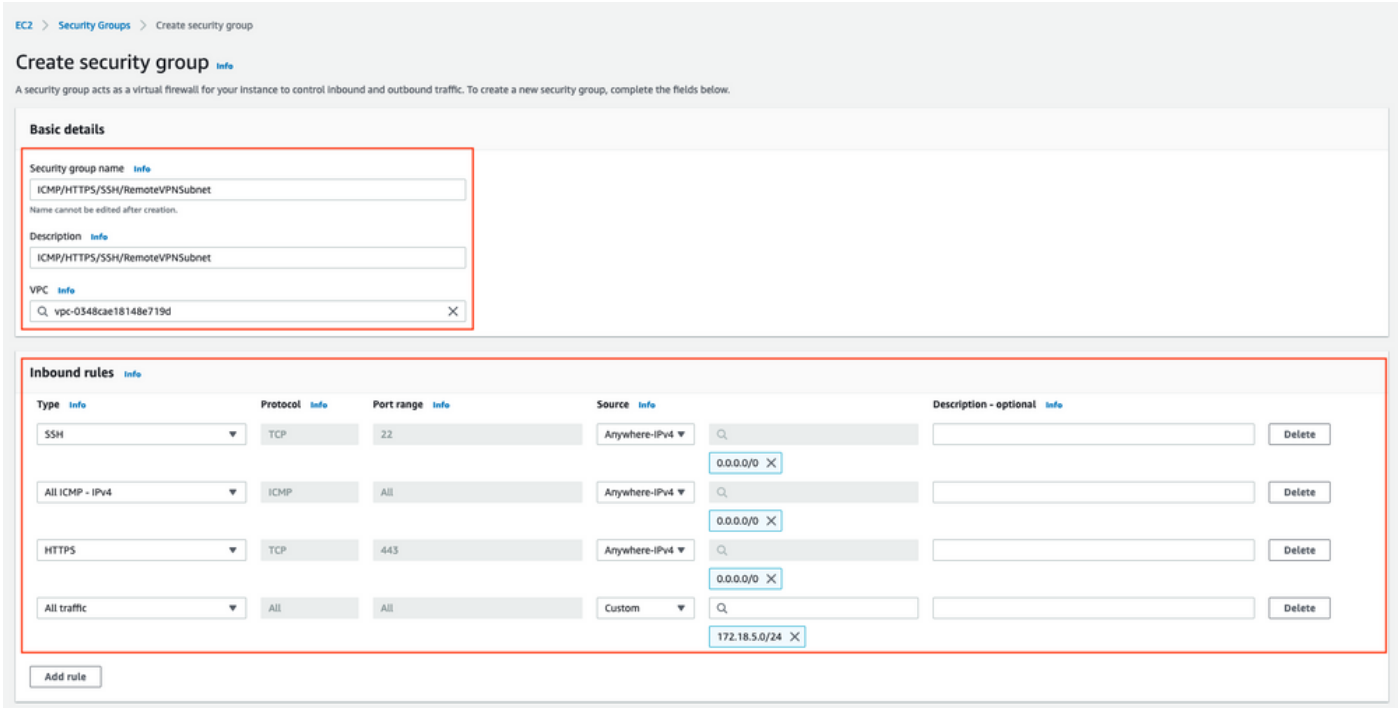
Paso C opcional Crear un par de claves personalizado

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.



Paso D opcional. Crear grupo de seguridad personalizado

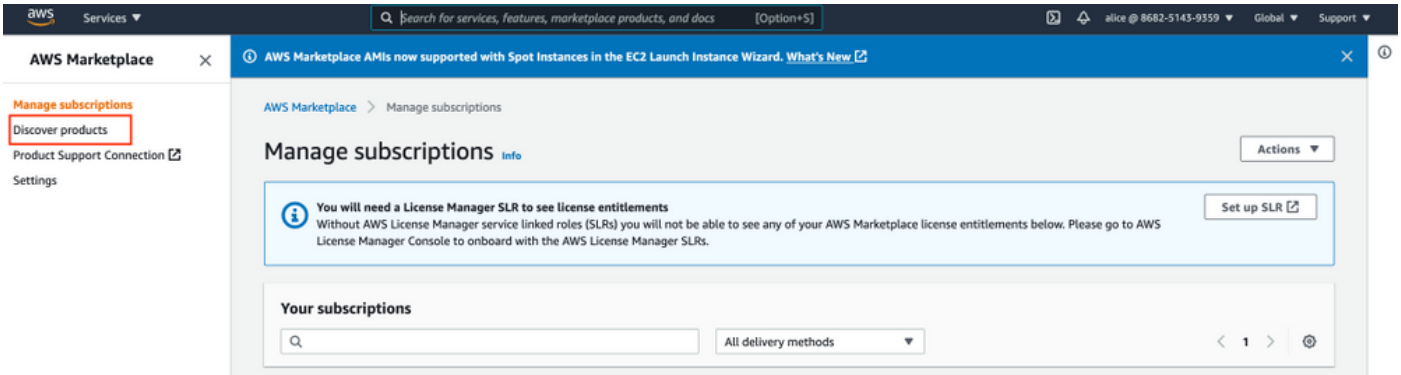
El acceso de instancias de AWS EC2 está protegido por **grupos de seguridad**, para configurar el **grupo de seguridad**, navegue al servicio **EC2**. Seleccione el menú **Grupos de seguridad** en **Red y Seguridad.** Seleccione Crear grupo de seguridad, configure un **nombre**, **descripción,** en el 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.



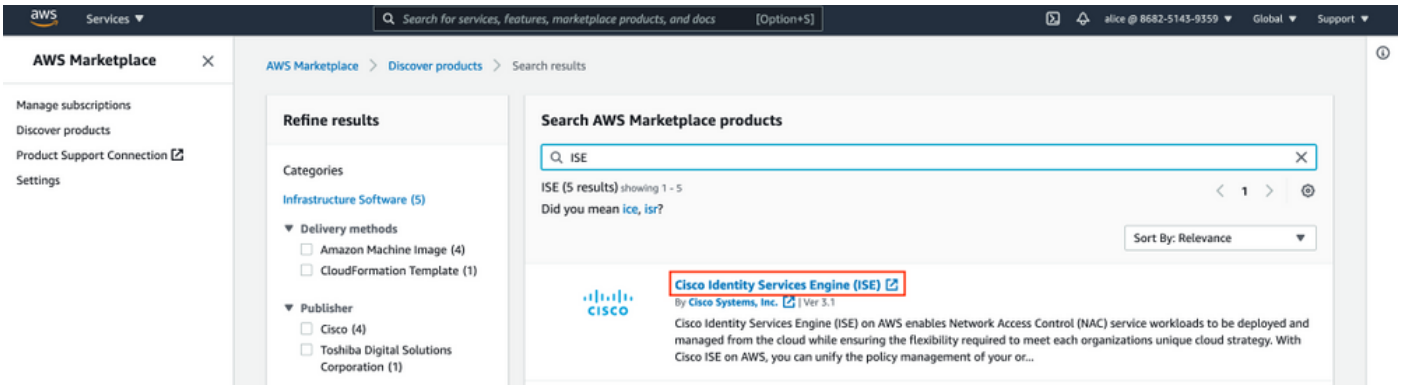
Nota: El grupo de seguridad configurado permite el acceso SSH, ICMP, HTTPS a ISE y a todos los protocolos desde la subred en las instalaciones.

Paso 1. Suscripción al producto AWS ISE Marketplace

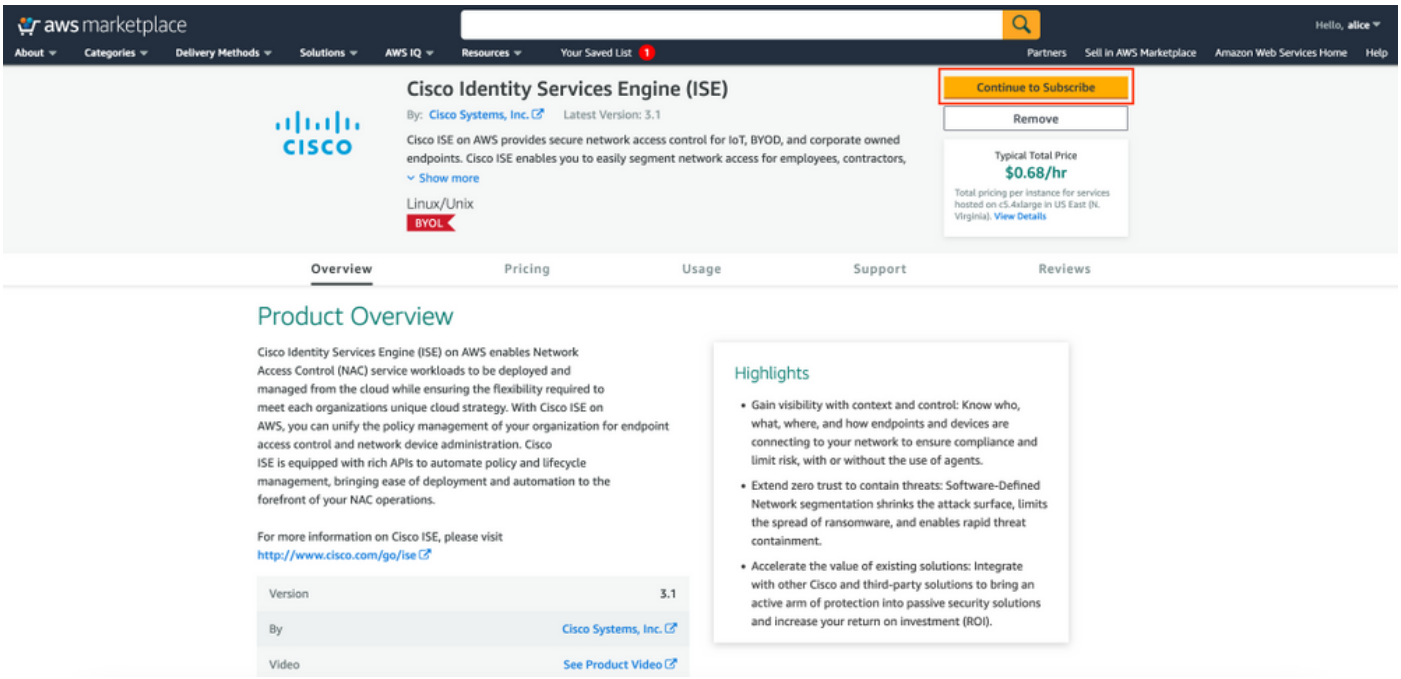
Vaya al servicio **AWS Marketplace Subscriptions**. Seleccione **Discover Products** como se muestra en la imagen.



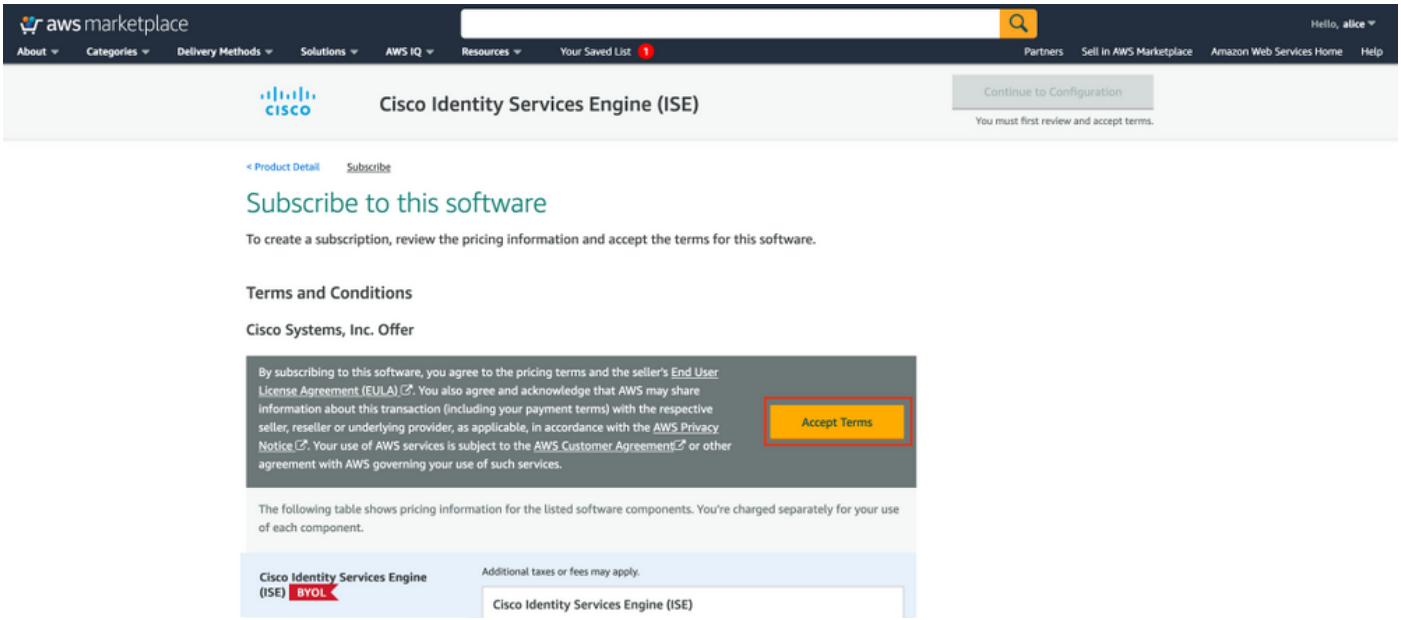
Busque el producto **ISE** y seleccione **Cisco Identity Services Engine (ISE)** como se muestra en la imagen.



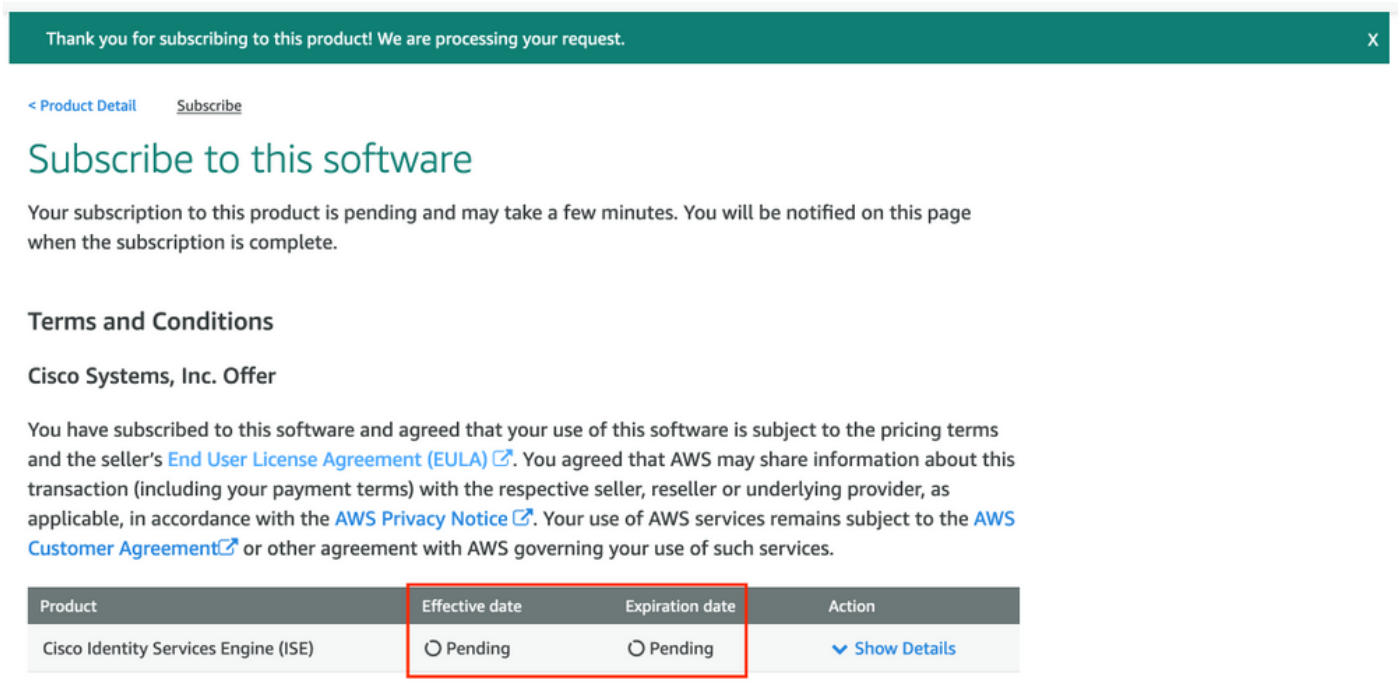
Seleccione el botón **Continuar para suscribirse**



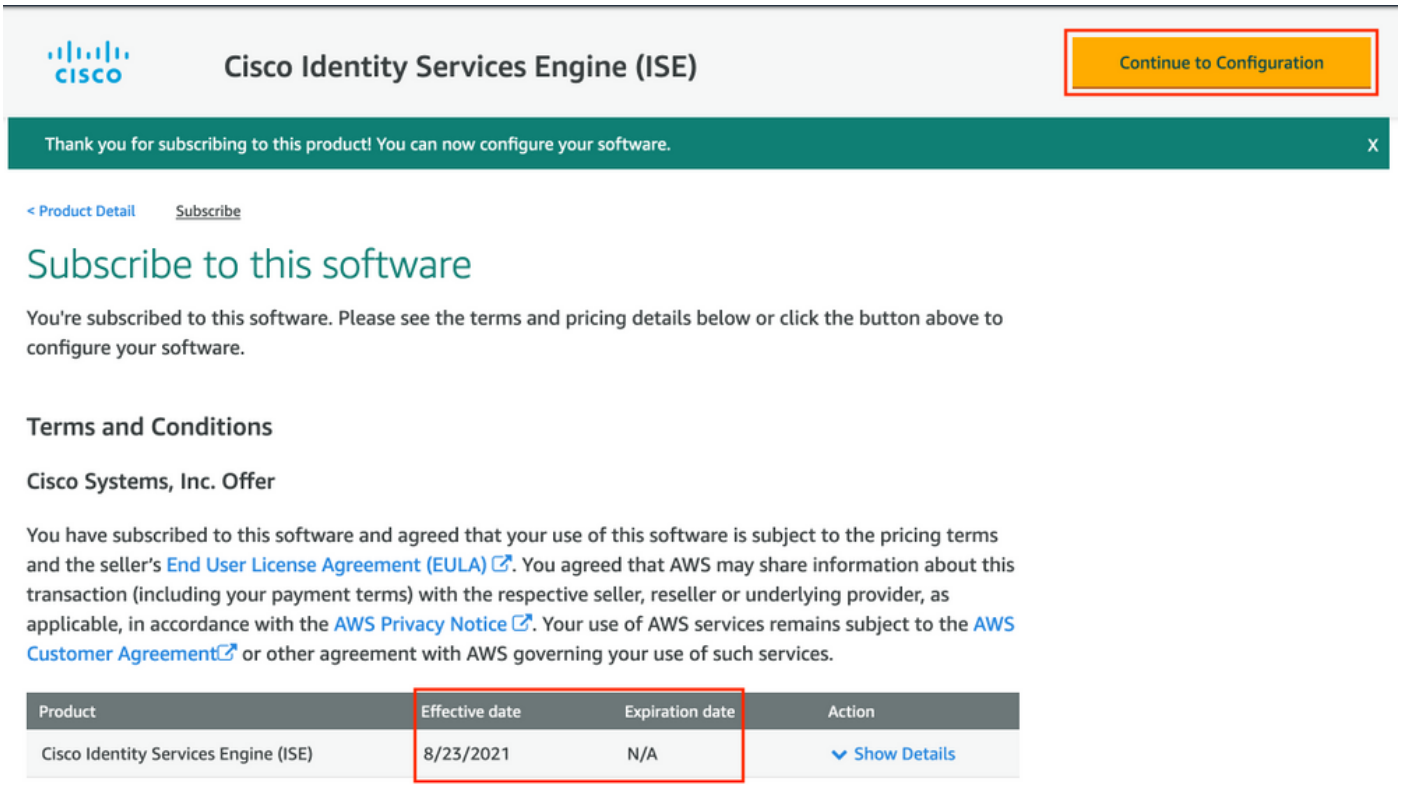
Seleccione el botón **Aceptar términos** como se muestra en la imagen.



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

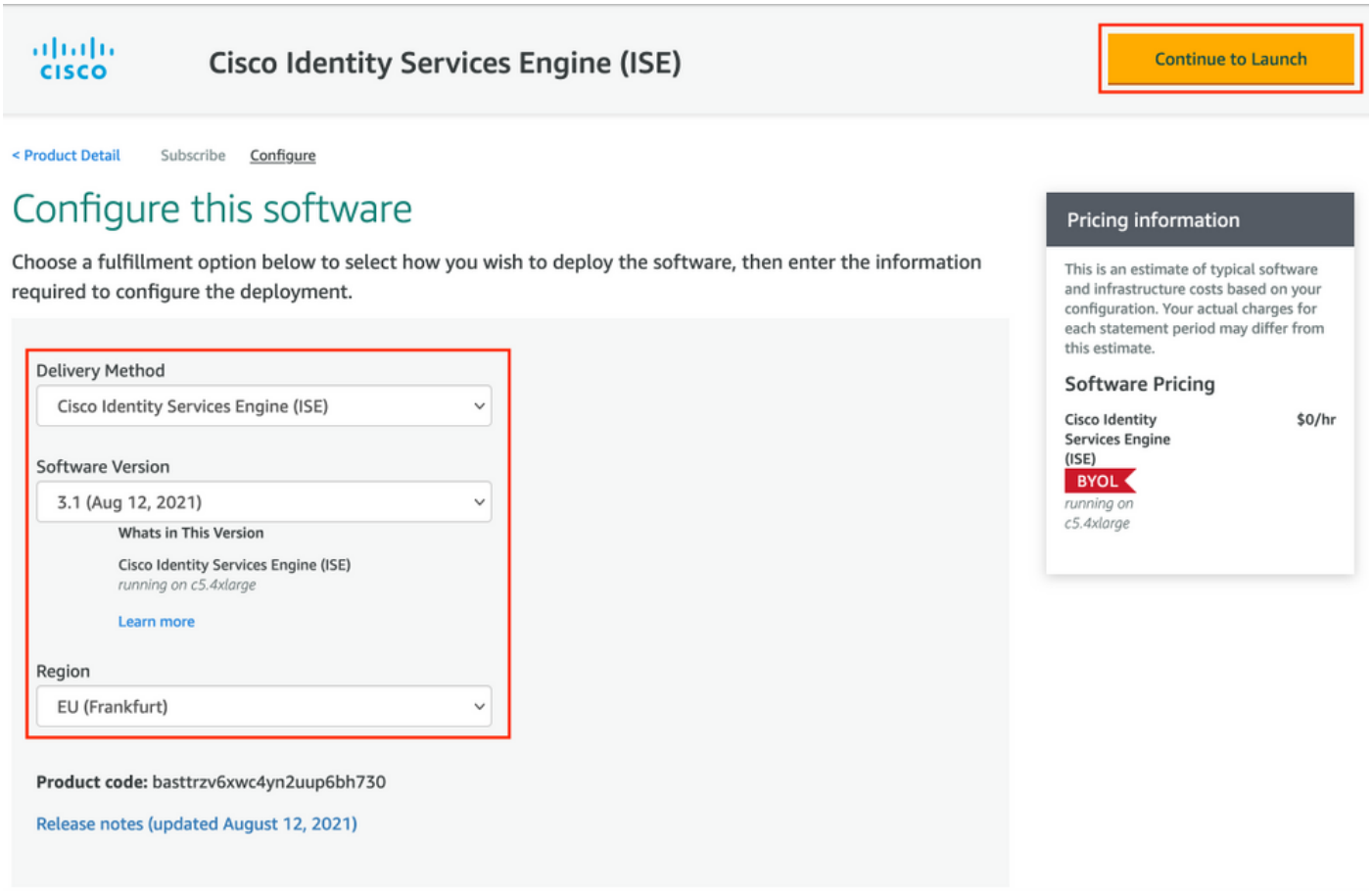


Poco después de la **fecha de entrada en vigor**, los cambios en la fecha de suscripción y la **fecha de vencimiento** cambian a **N/A.** Seleccione **Continuar a la configuración** como se muestra en el ima



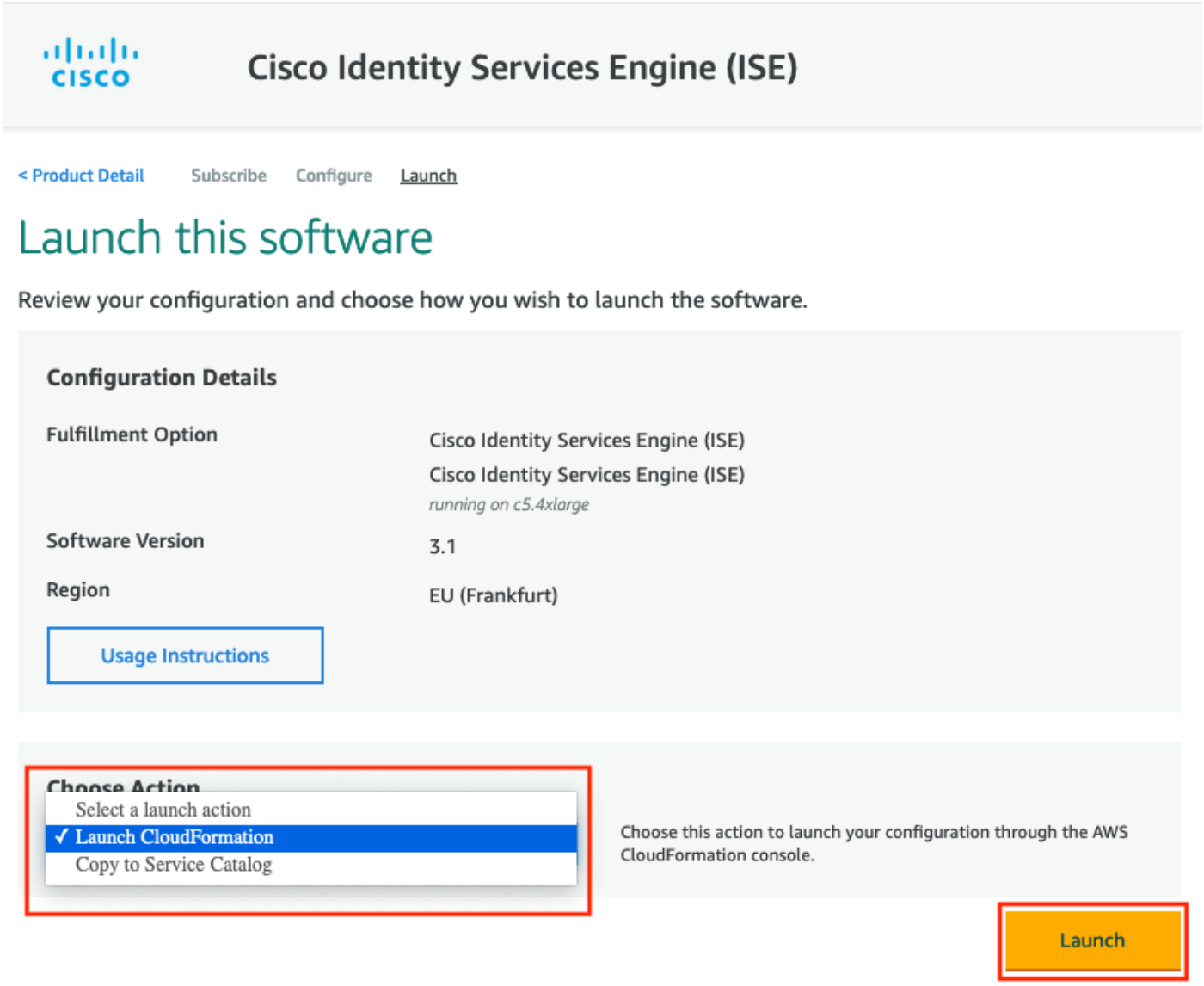
Paso 2. Configuración de ISE en AWS

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.**



Paso 3. Iniciar ISE en AWS

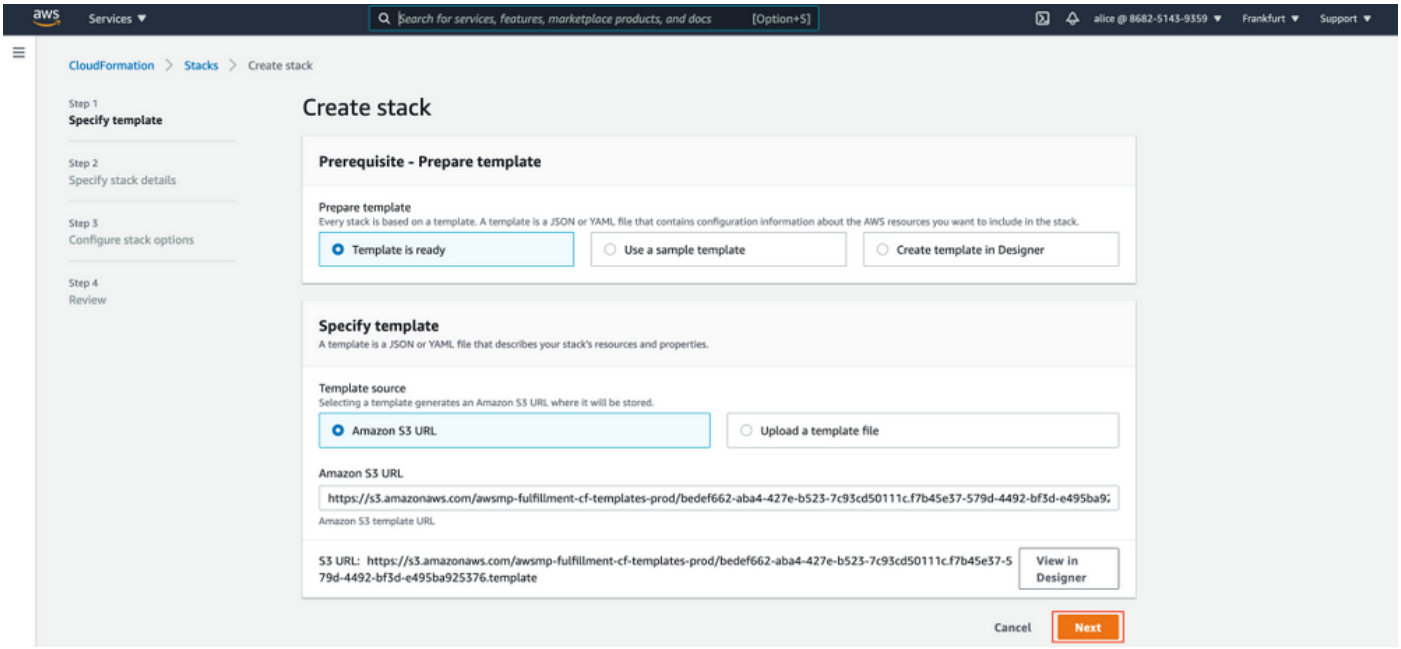
En el menú desplegable Acciones de la pantalla **Iniciar este software**, seleccione **Iniciar formación de nube**.



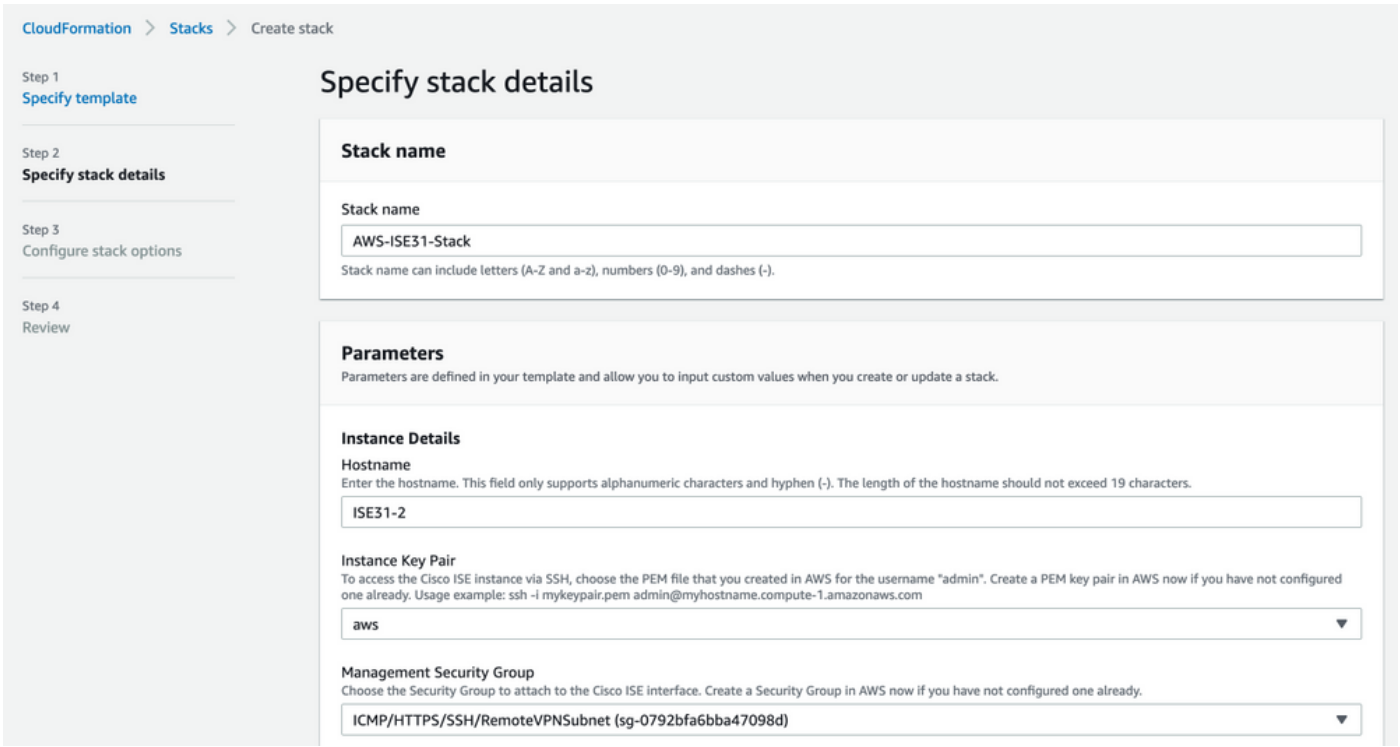
(Opcional) Seleccione **Instrucciones de uso** para familiarizarse con ellas. Seleccione **Iniciar**.

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

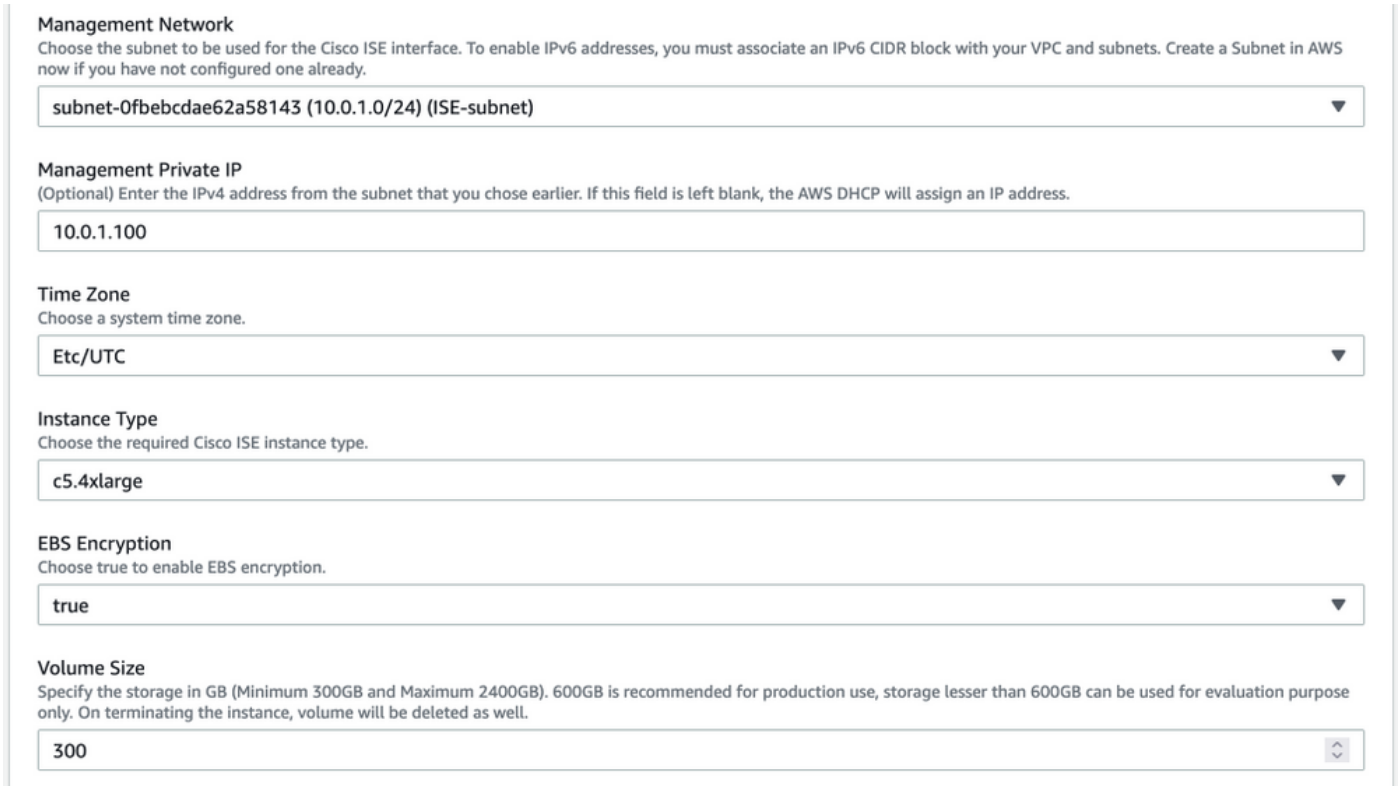
El botón de **inicio** le redirige a la pantalla de configuración de la **pila de formación** en la **nube**. Hay una plantilla prediseñada que se debe utilizar para configurar ISE. Mantenga los parámetros predeterminados y seleccione **Siguiente**.



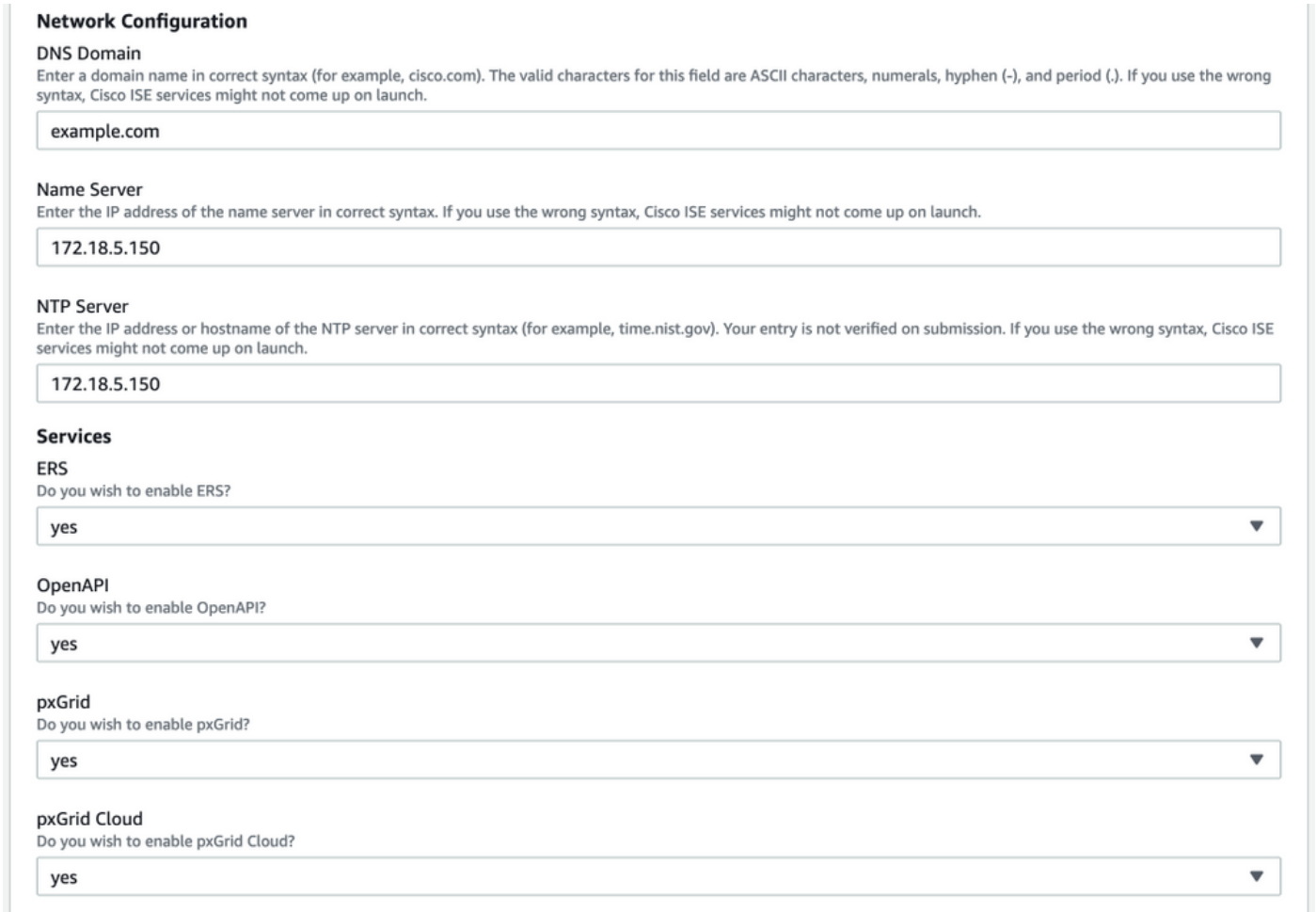
Rellene los datos de la pila de formación de nube con **nombre de pila**. Configure los detalles de la instancia como **nombre de host**, seleccione **par de claves de** instancia y **grupo de seguridad de administración.**



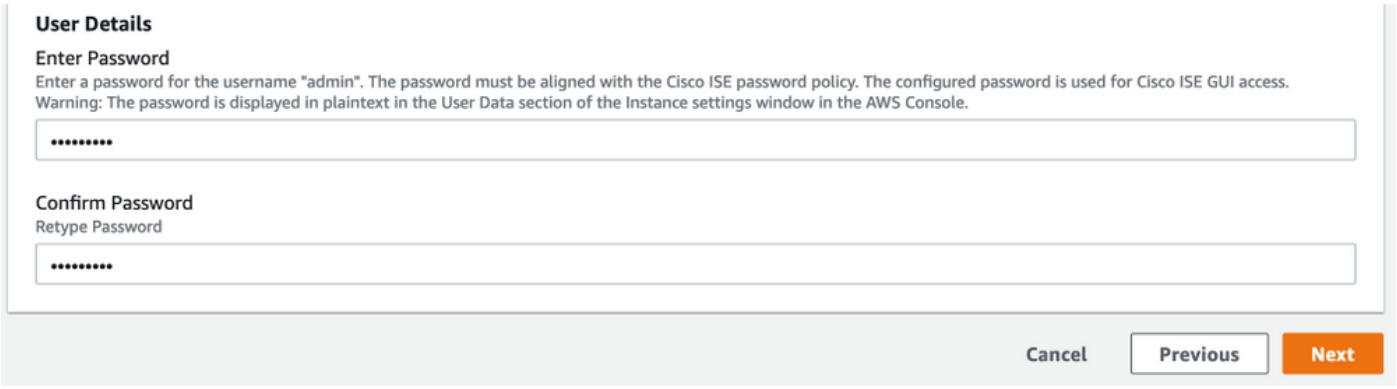
Continuar configuración de detalles de instancia con **Red de administración, IP privada de administración, Zona horaria**, **Tipo de instancia, Cifrado EBS** y **Tamaño del volumen.**



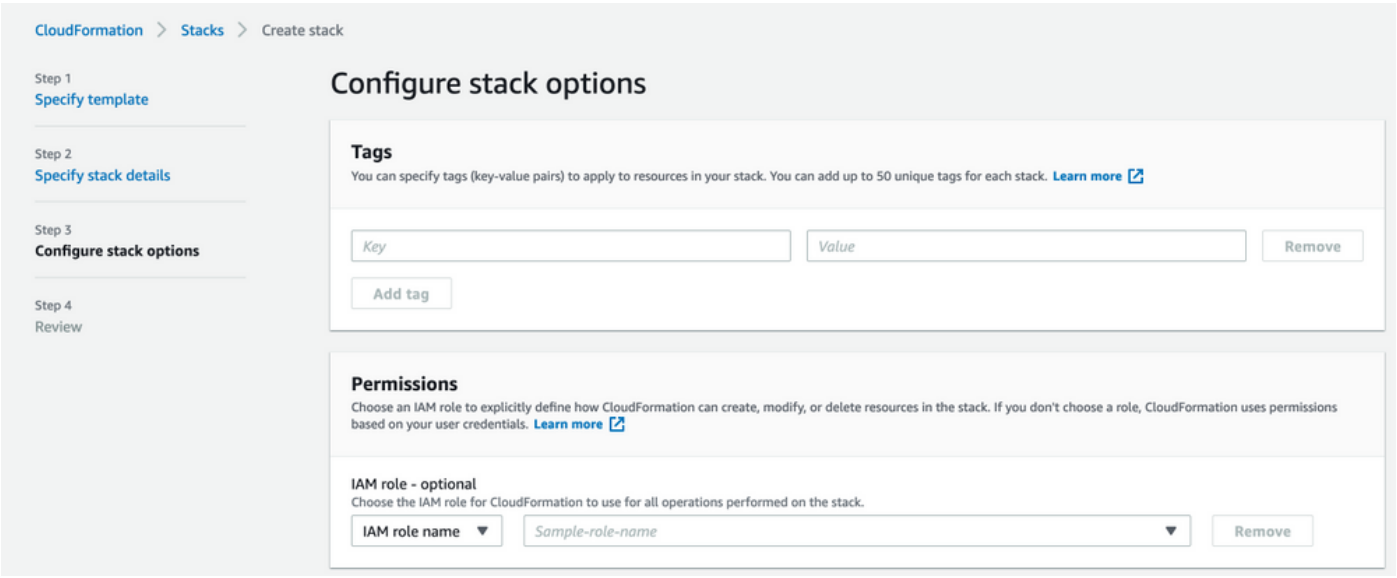
Continuar configuración de detalles de instancia con **dominio DNS, servidor de nombres, servicio NTP** y **servicios**.



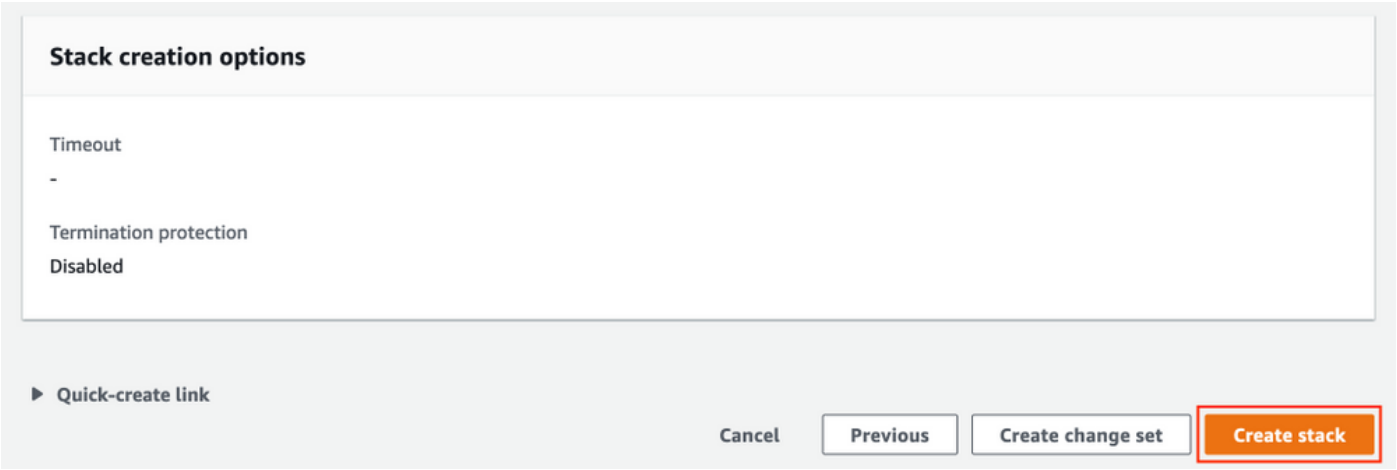
Configure la contraseña de usuario de la GUI y seleccione **Next**.



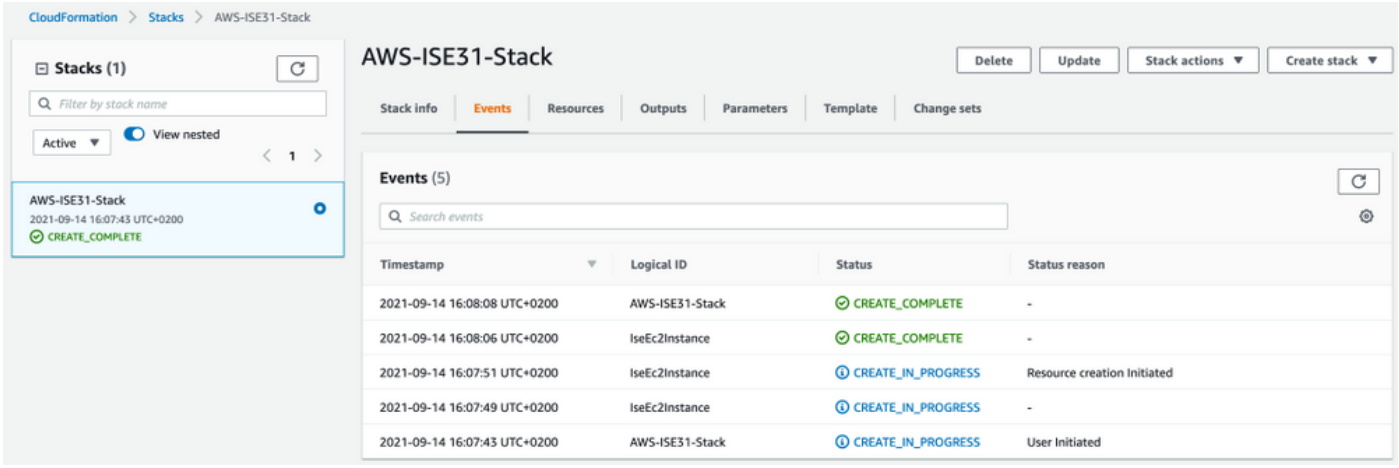
No se requiere ningún cambio en la siguiente pantalla. Seleccione **Next**.



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

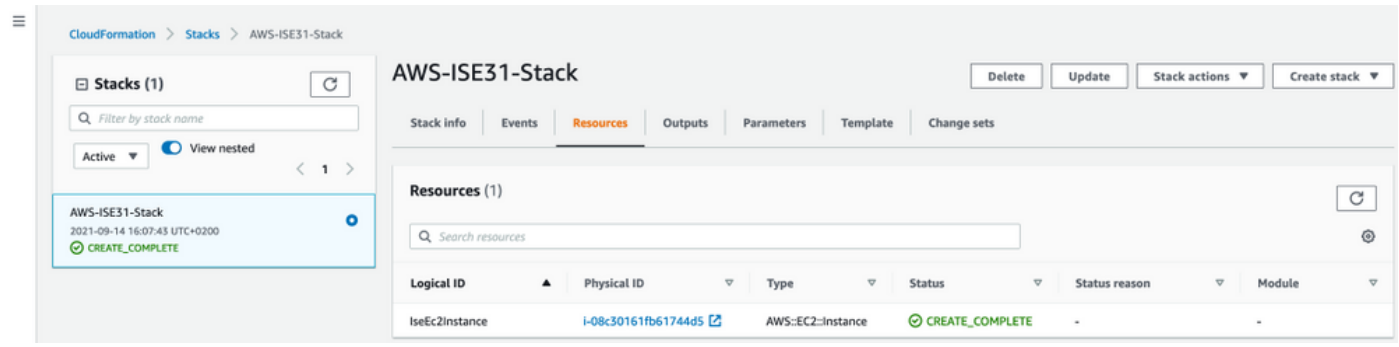


Una vez que se implementa la pila, se debe ver el estado **CREATE_COMPLETE**.

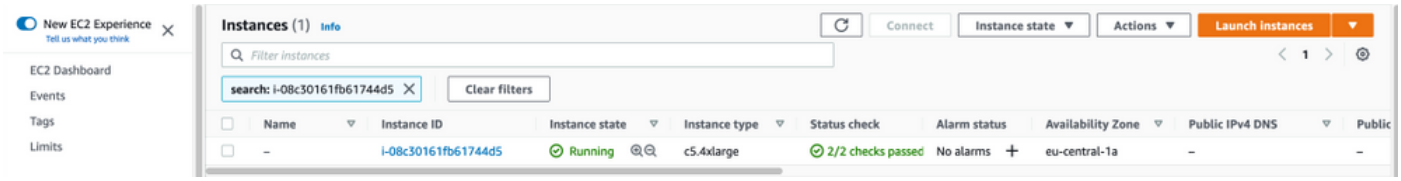


Paso 5. Acceso a ISE en AWS

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 > Intones** 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: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#
```

> **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:

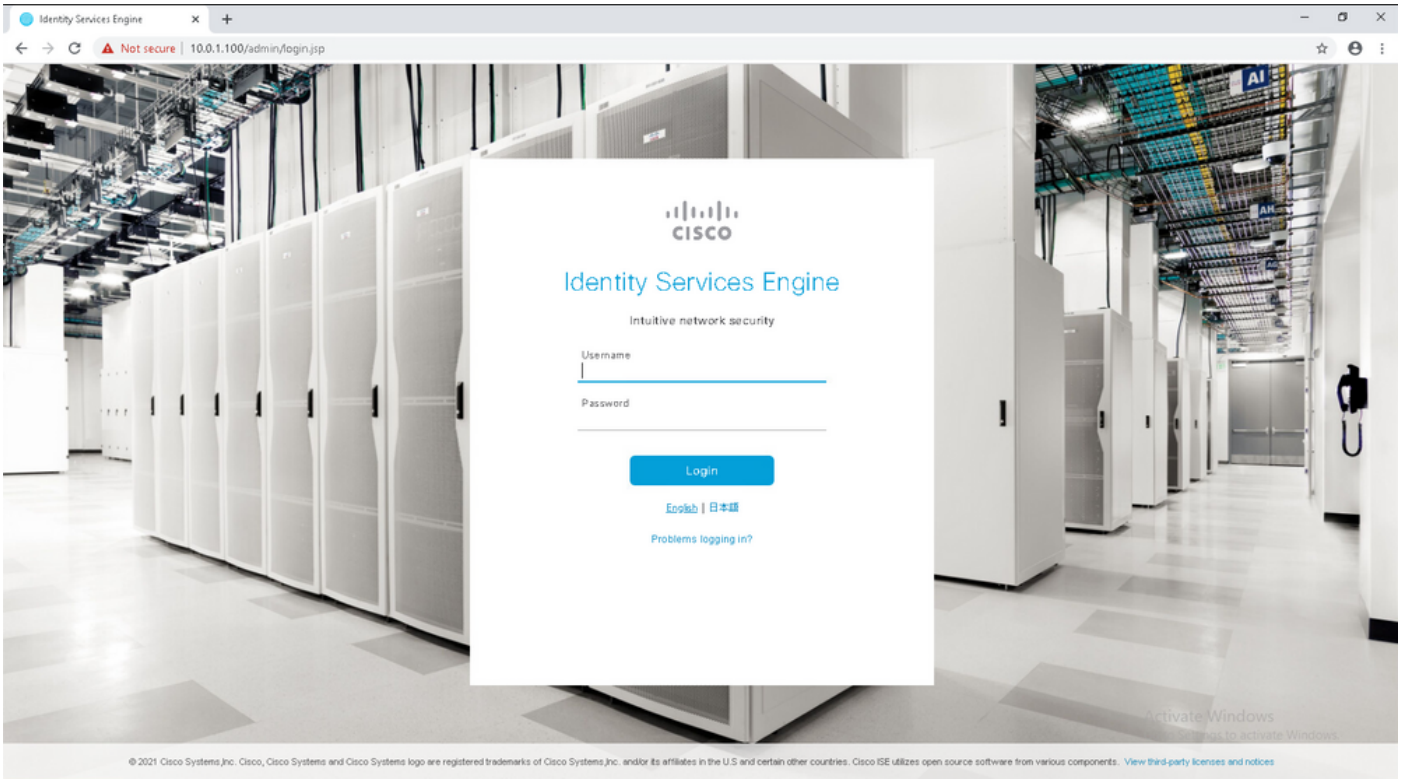
```
ISE31-2/admin# show application status ise

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#
```

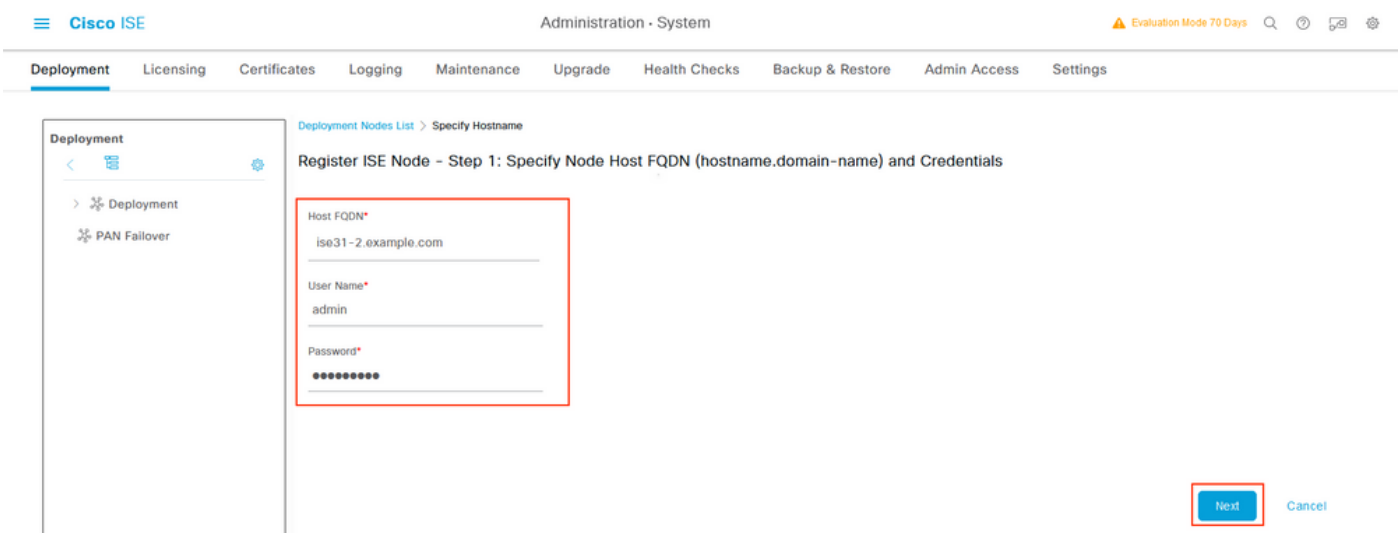
> **Nota:** Se tardan entre 10 y 15 minutos desde que SSH está disponible para que los servicios ISE realicen la transición a un estado en ejecución.

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.**

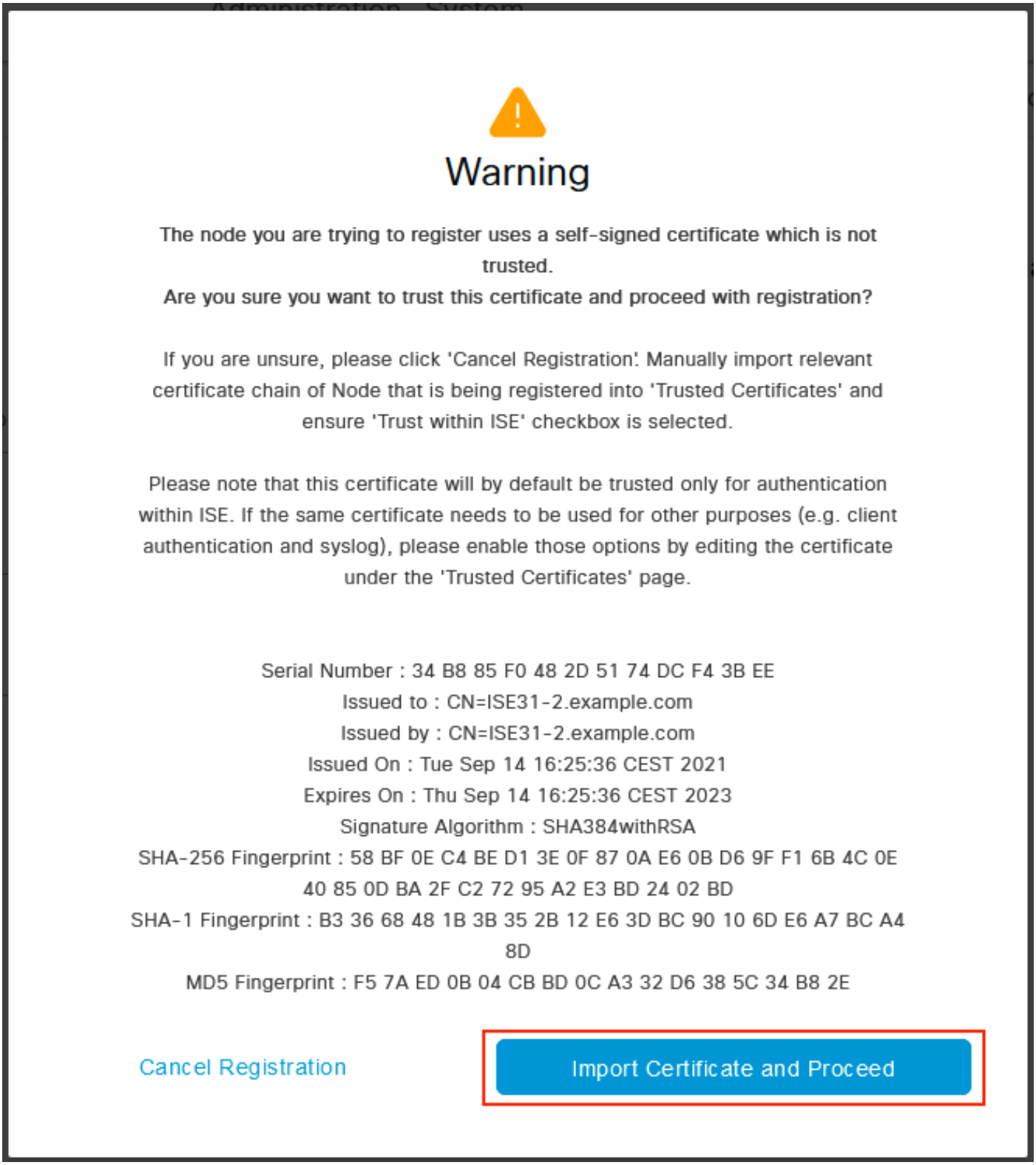


Paso 6. Configuración de la implementación distribuida entre ISE in situ e ISE en AWS

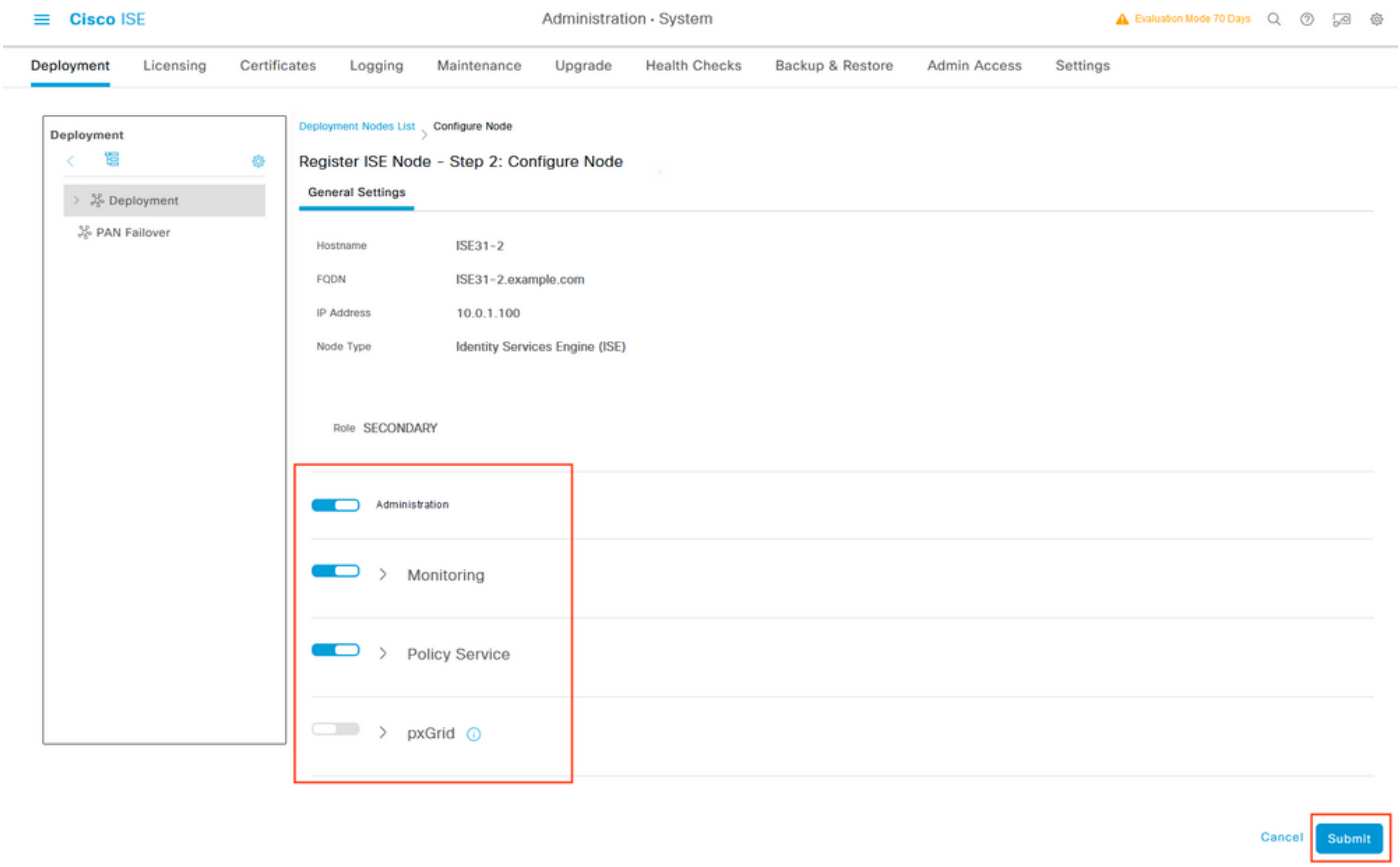
Inicie sesión en In-Prem ISE y navegue hasta **Administration > System > Deployment.** Seleccione el nodo y Seleccione **Make Primary.** Vuelva a **Administration > System > Deployment**, Seleccione **Register**. Configure **FQDN de host** de ISE en AWS, **Nombre de usuario** de la GUI y **Contraseña.**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



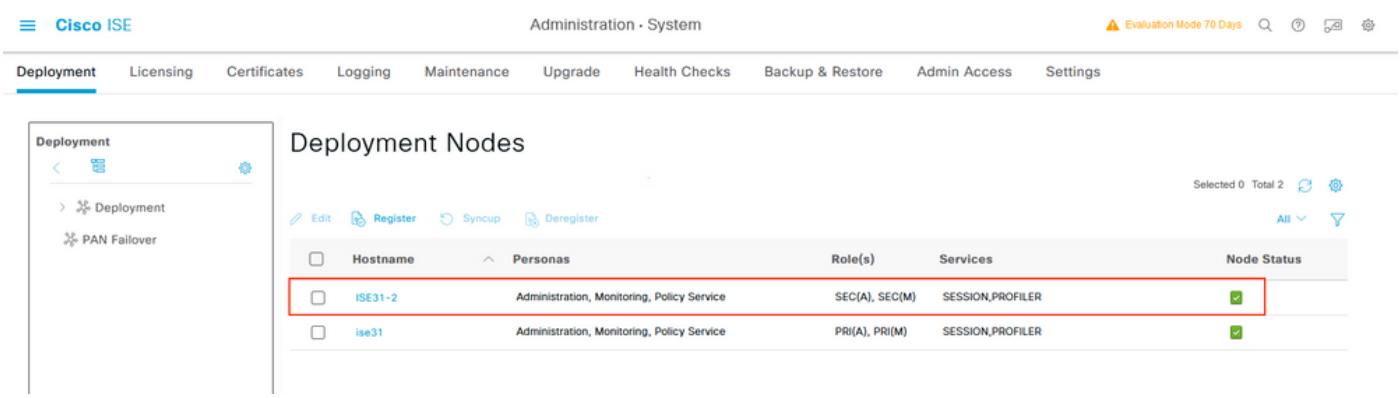
Dado que los certificados autofirmados se utilizan en esta topología, para importar certificados de administrador al **certificado de** importación Select de almacén de confianza **y continuar.**



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

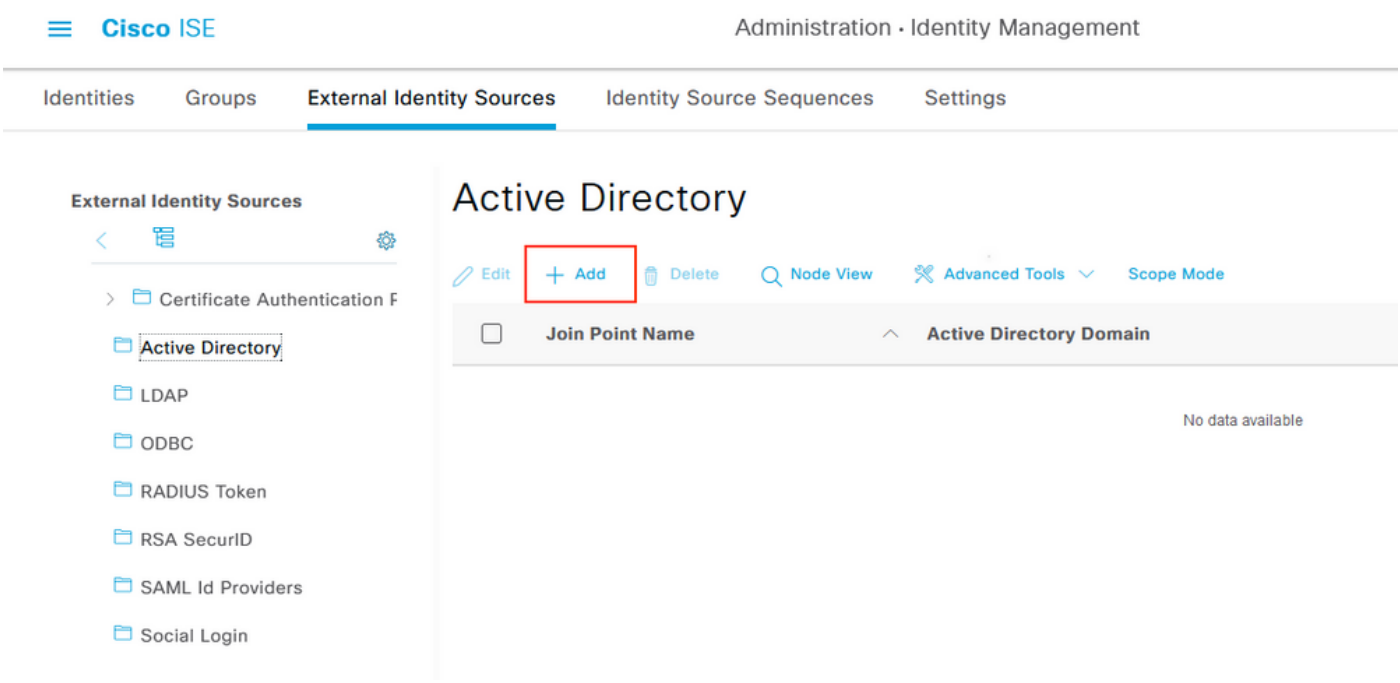


Una vez finalizada la sincronización, el nodo pasa al estado conectado, se muestra la casilla de verificación verde.

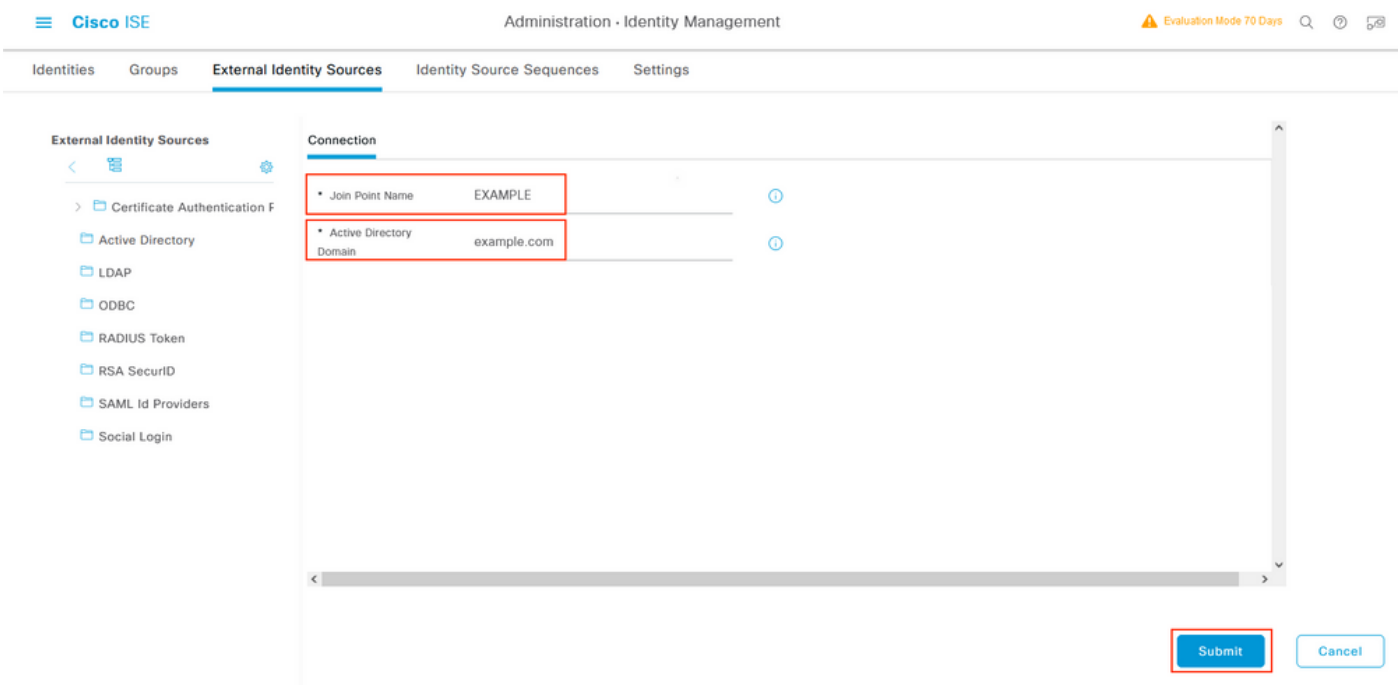


Paso 7. Integración de la implementación de ISE con AD in situ

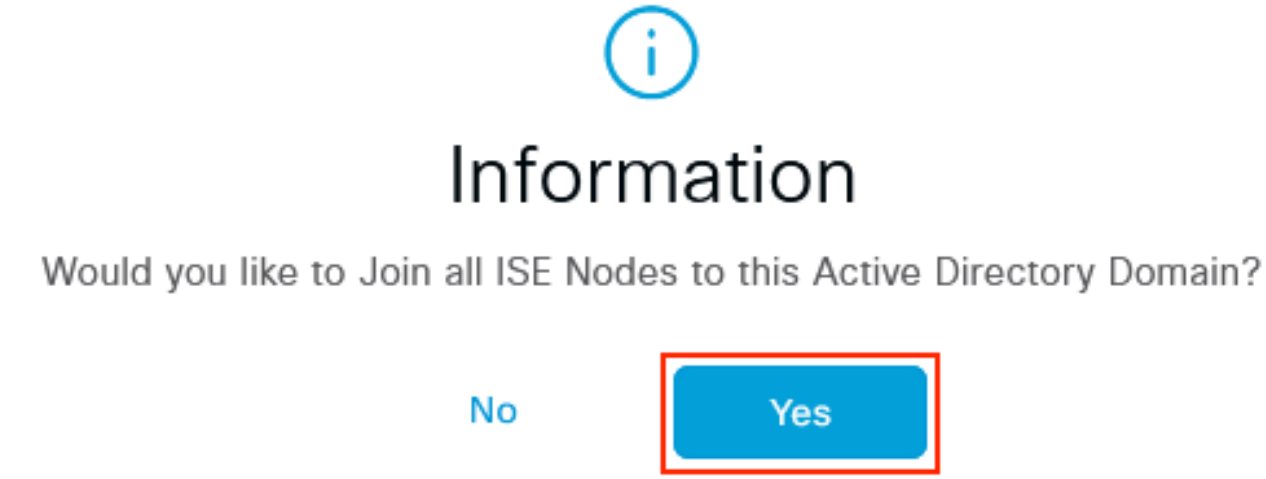
Vaya a **Administration > Identity Management > External Identity Sources**. Seleccione **Active Directory**, Seleccione **Add**.



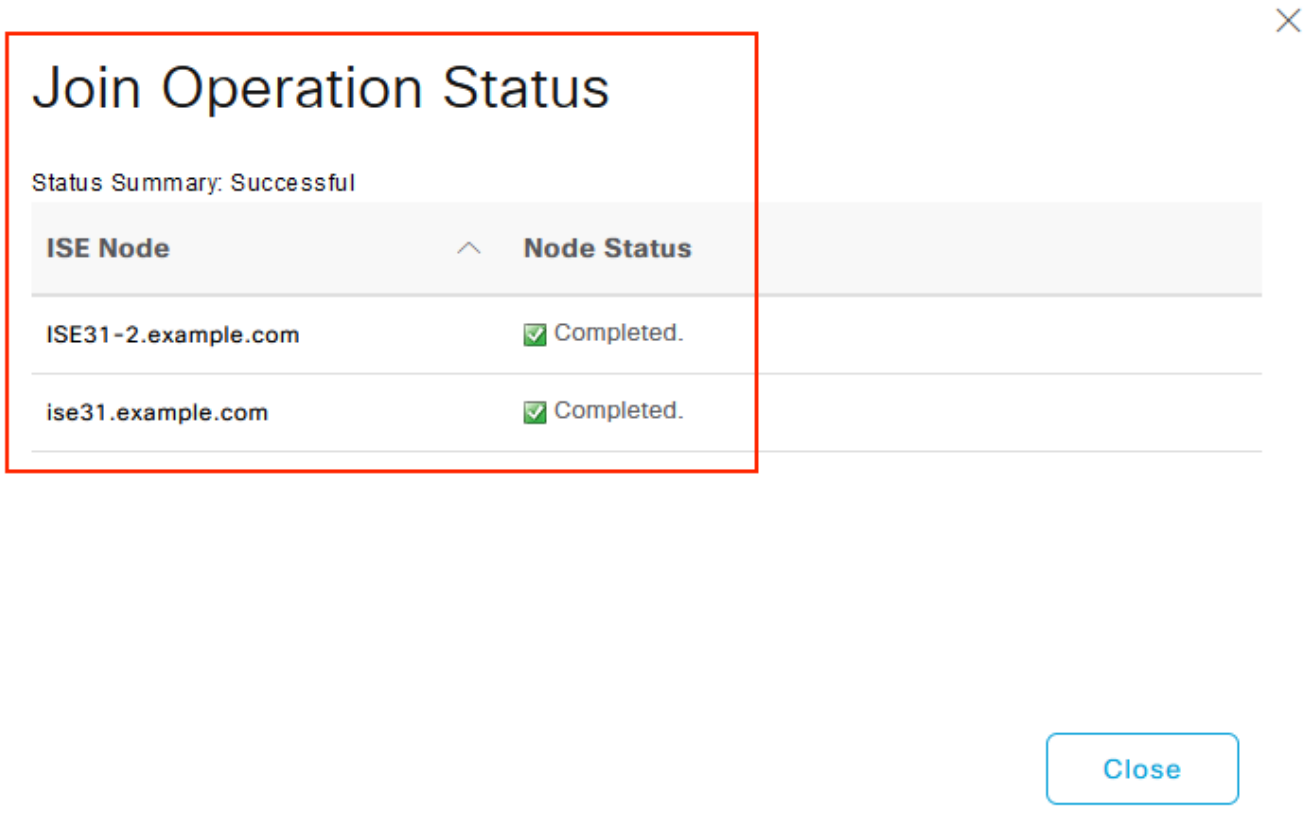
Configure **Joint Point Name** y **Active Directory Domain**, Seleccione **Submit**.



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



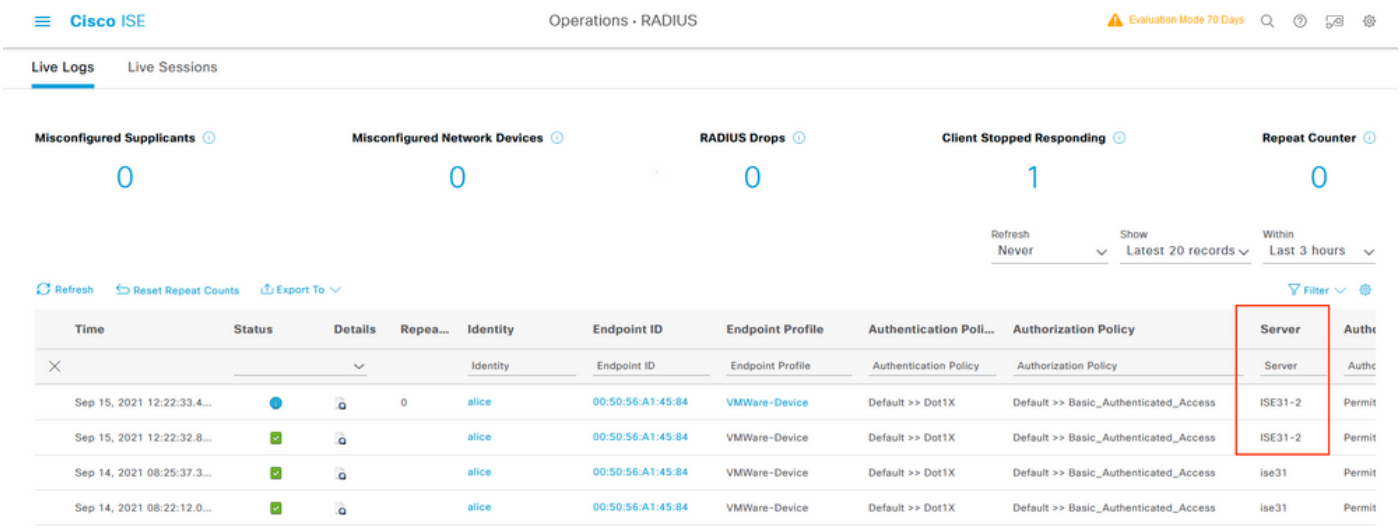
Limitaciones

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.

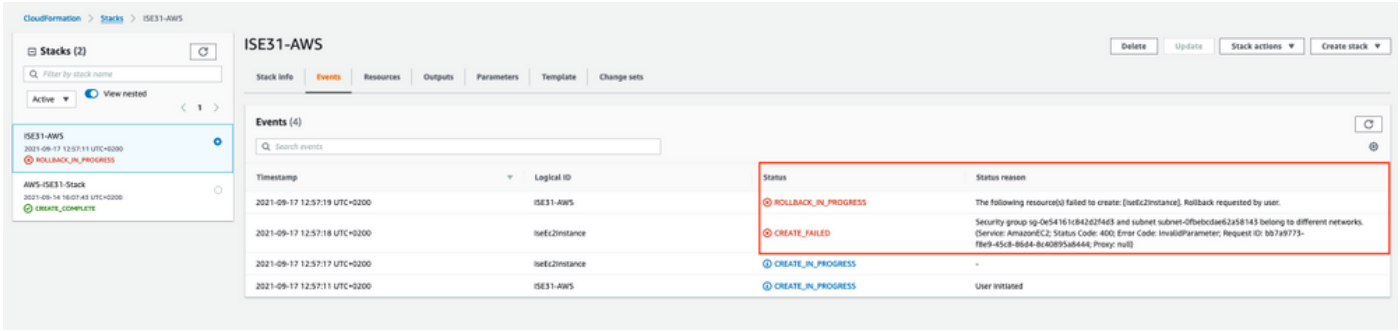


Troubleshoot

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.



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
```