Implemente Identity Services Engine (ISE) versión 3.4 en AWS

Contenido

Introducción

Este documento describe cómo configurar Cisco ISE en AWS mediante:

- Plantilla de formación en la nube (CFT)
- Amazon Machine Image (AMI)

Prerequisites

Requirements

Cisco recomienda conocer estos temas antes de continuar con esta implementación:

- Cisco Identity Services Engine (ISE)
- Gestión de instancias y redes AWS EC2
- Generación y uso de pares de claves SSH
- Comprensión básica de VPC, grupos de seguridad y configuración DNS/NTP en AWS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Identity Services Engine (ISE)
- Consola de nube de Amazon Web Services (AWS)

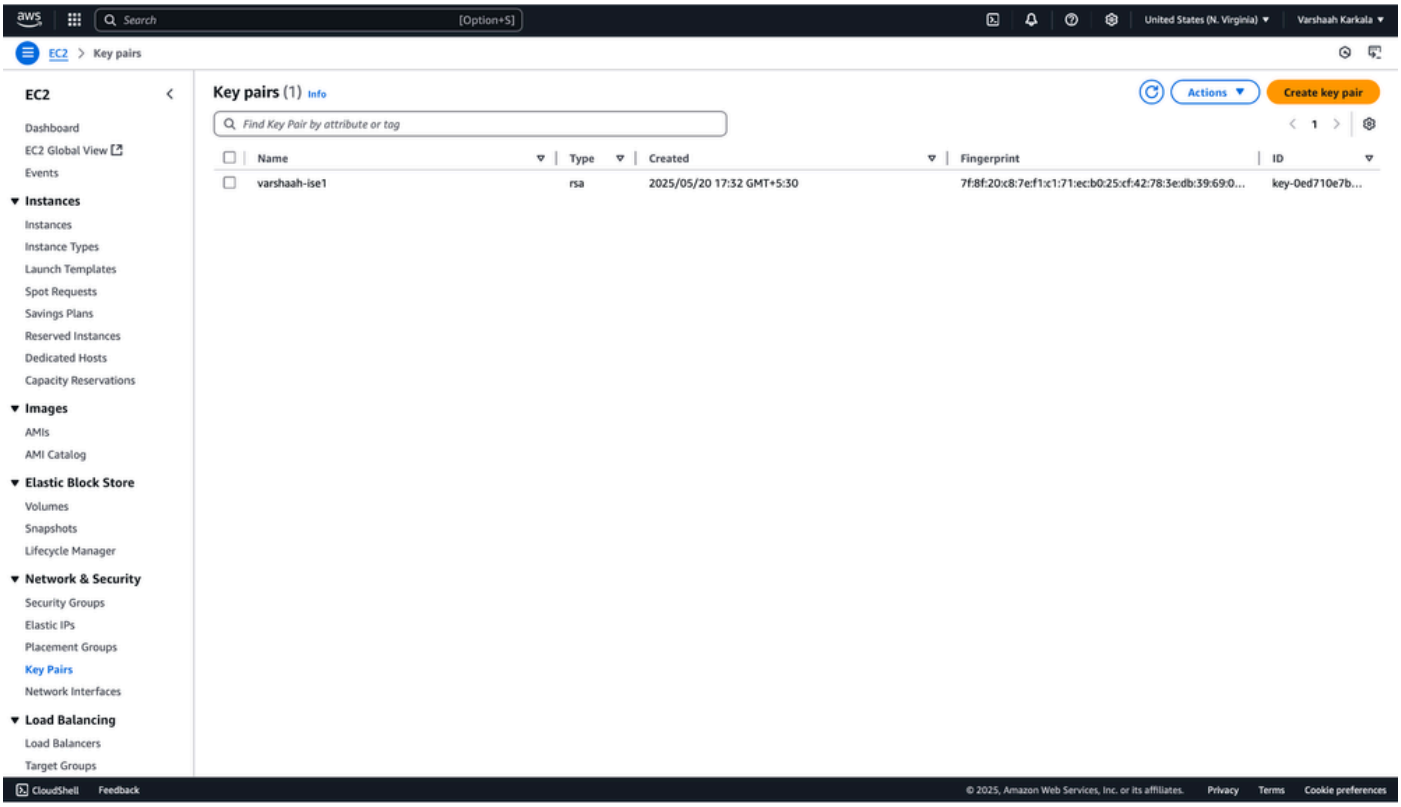
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

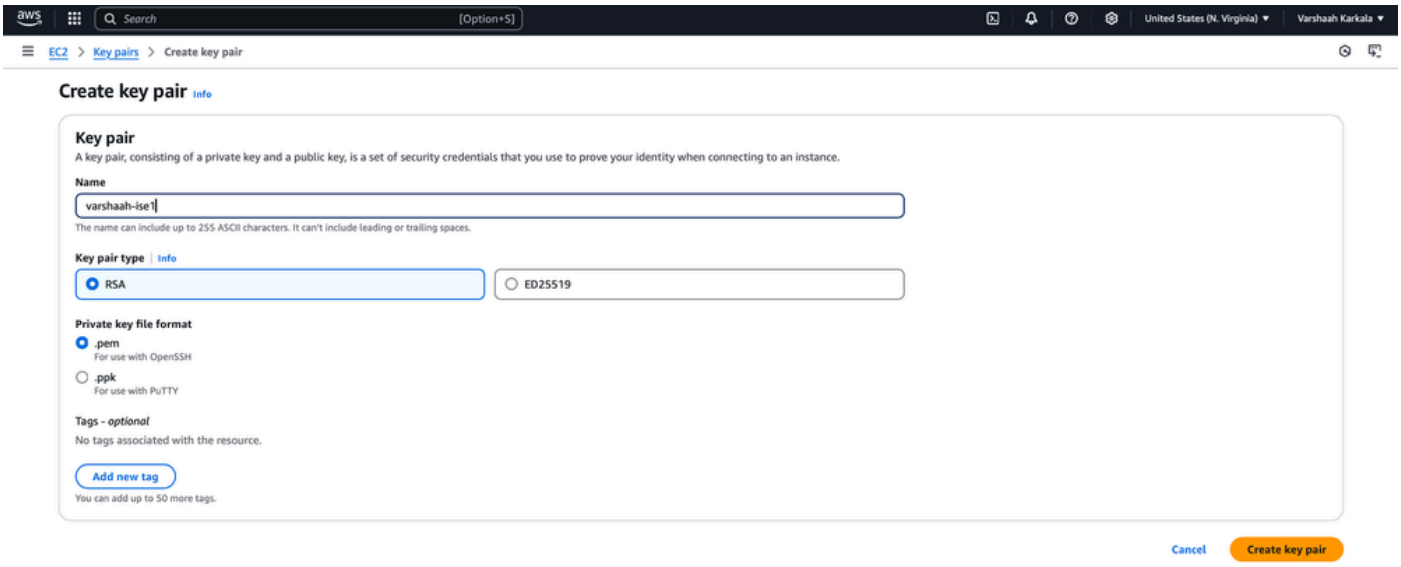
Parte 1: Generación de un conjunto de key-pair SSH

1. Para esta implementación, puede utilizar un par de claves existente o crear uno nuevo.

2. Para crear un nuevo par, navegue hasta EC2 > Red y seguridad > Pares de llaves y haga clic en Crear par de llaves.



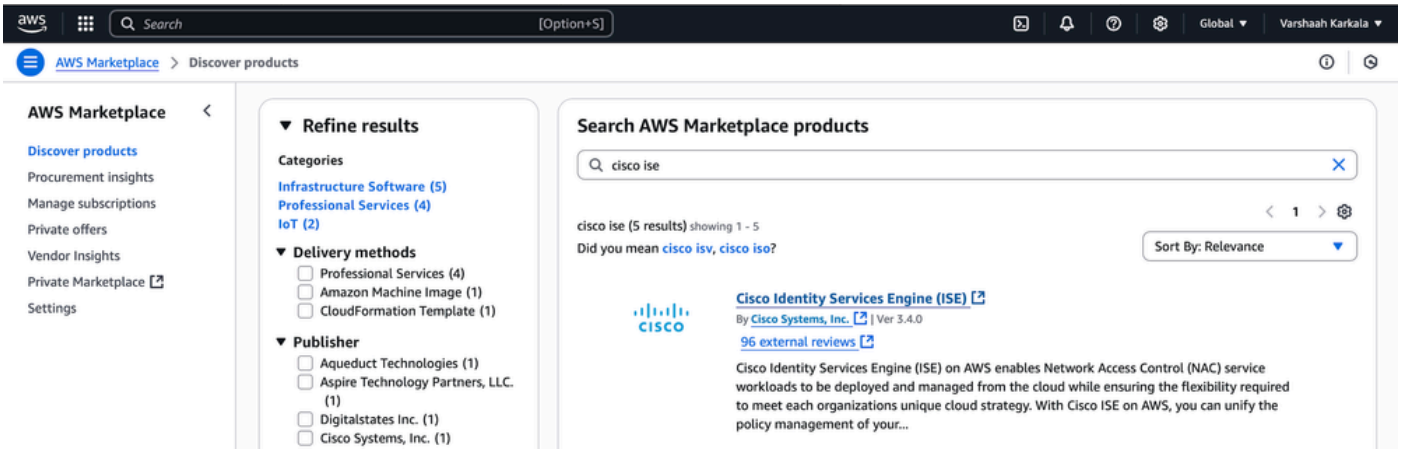
3. Introduzca el nombre del par de claves y haga clic en Crear par de claves.

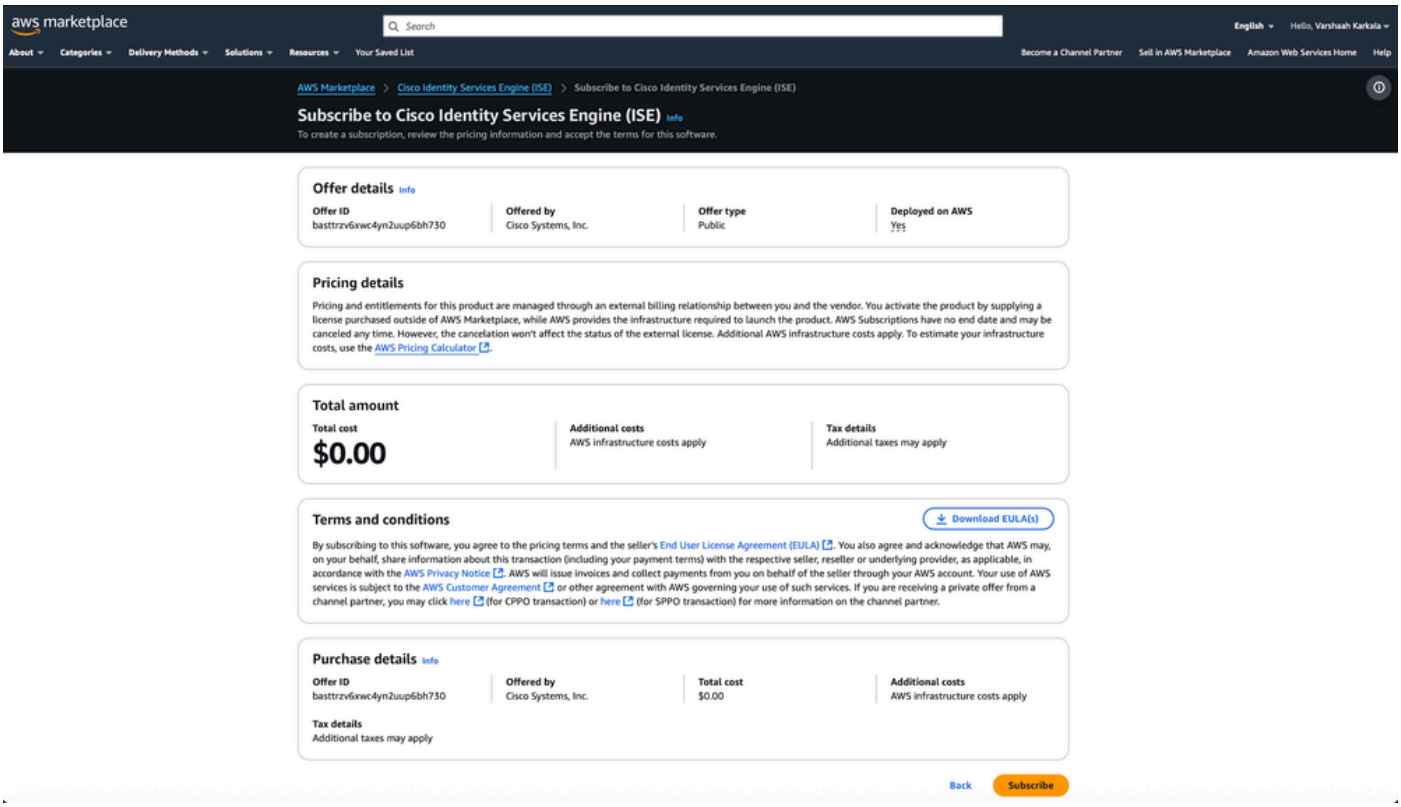


El archivo de par de claves (.pem) se descarga en el equipo local. Asegúrese de mantener este archivo seguro, ya que es la única manera en la que puede acceder a su instancia EC2 una vez que se ha iniciado.

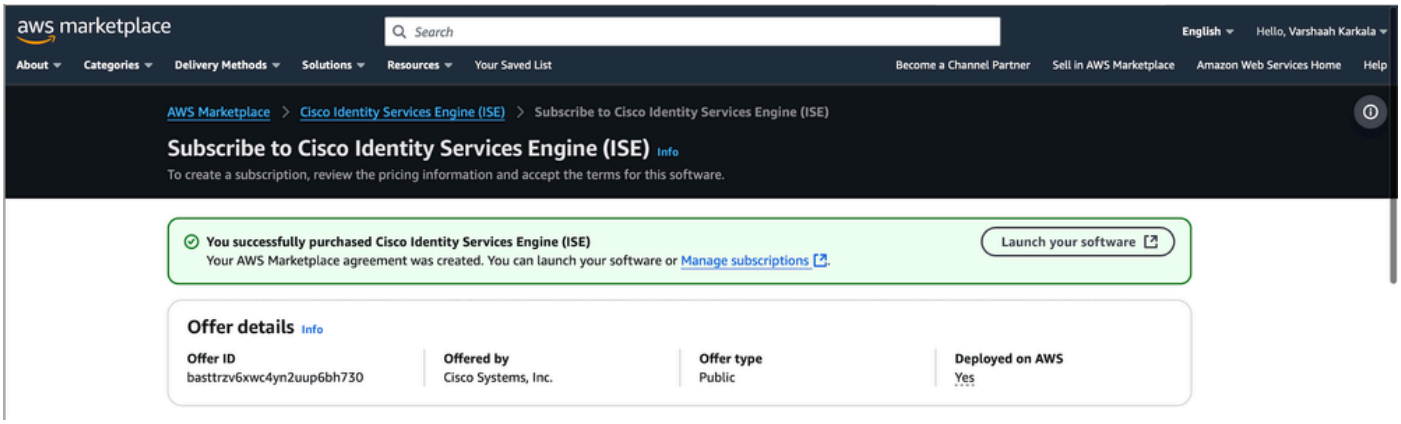
Parte 2: Configuración de ISE mediante la plantilla de formación en la nube (CFT)

1. Inicie sesión en AWS Management Console y busque AWS Marketplace Subscriptions.
2. En la barra de búsqueda, escriba "cisco ise" y seleccione Cisco Identity Services Engine (ISE) en los resultados. Haga clic en Subscribe.

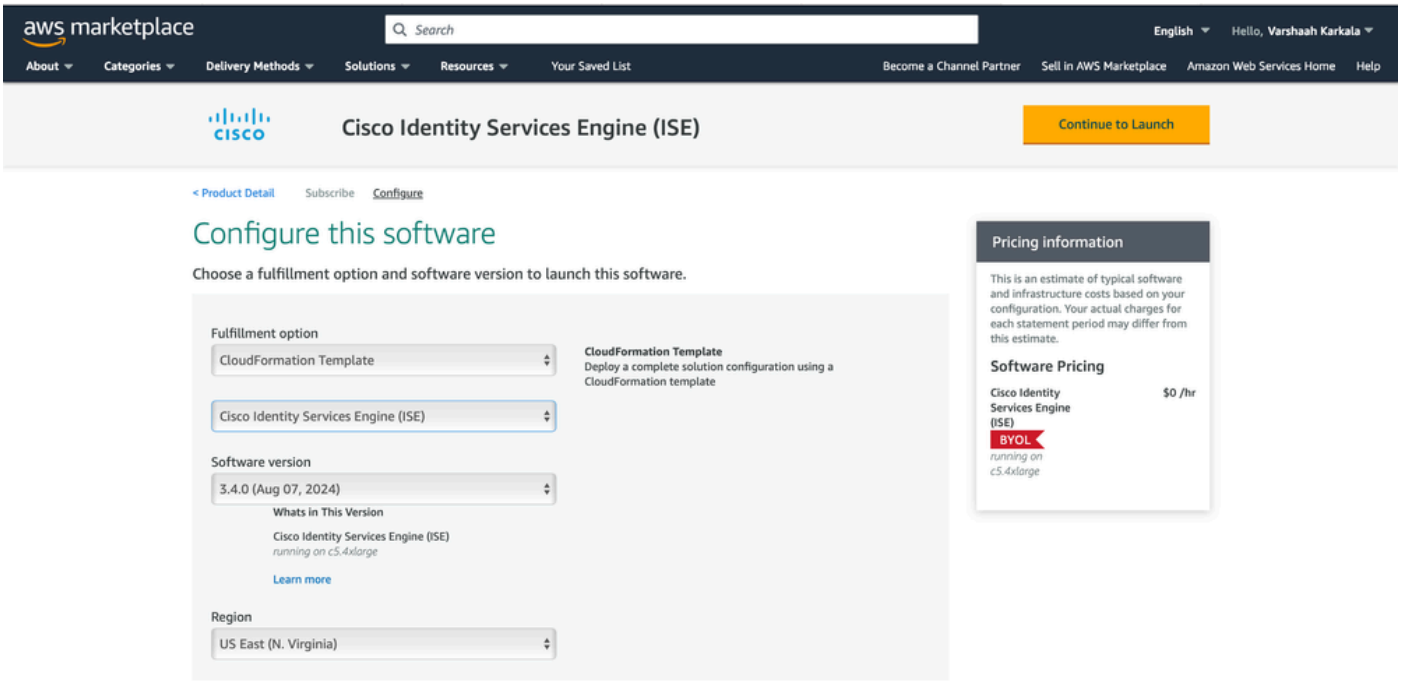




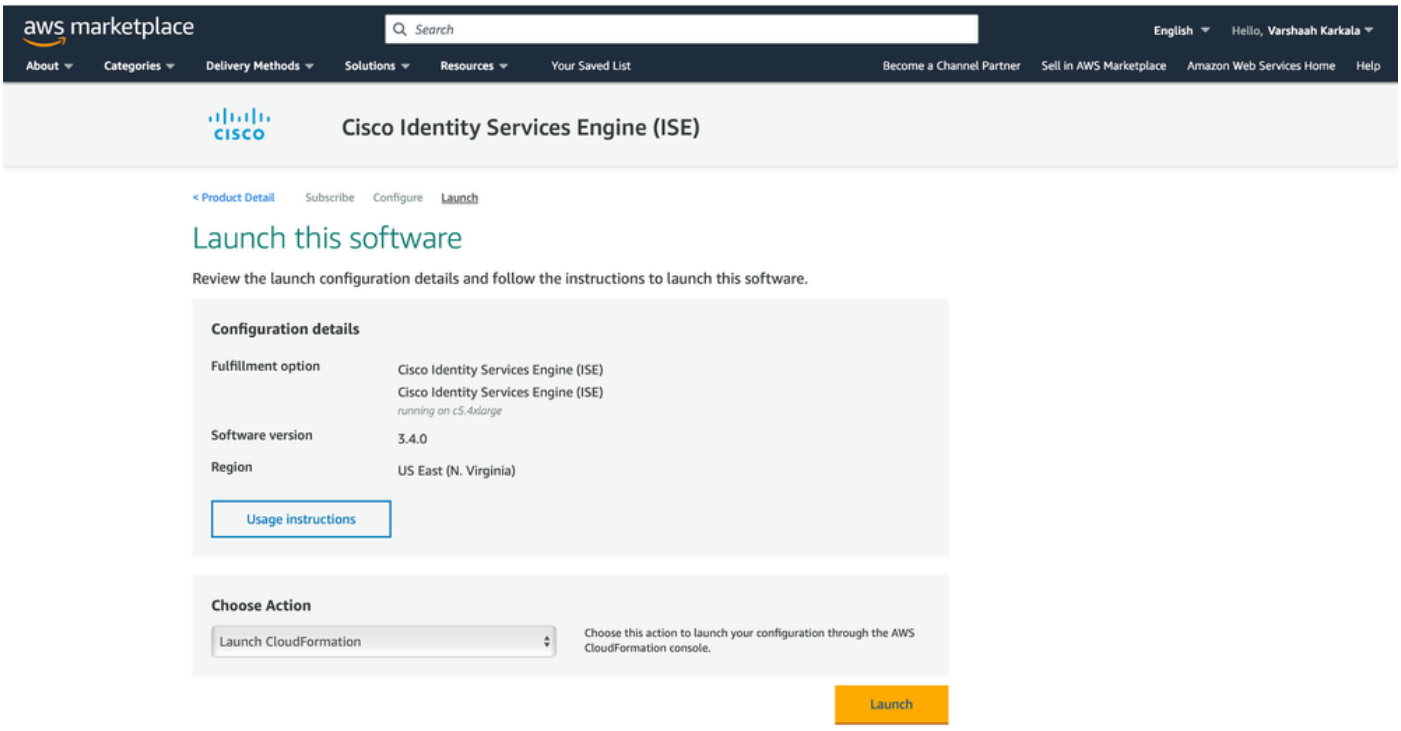
3. Después de la suscripción, seleccione Iniciar el software.



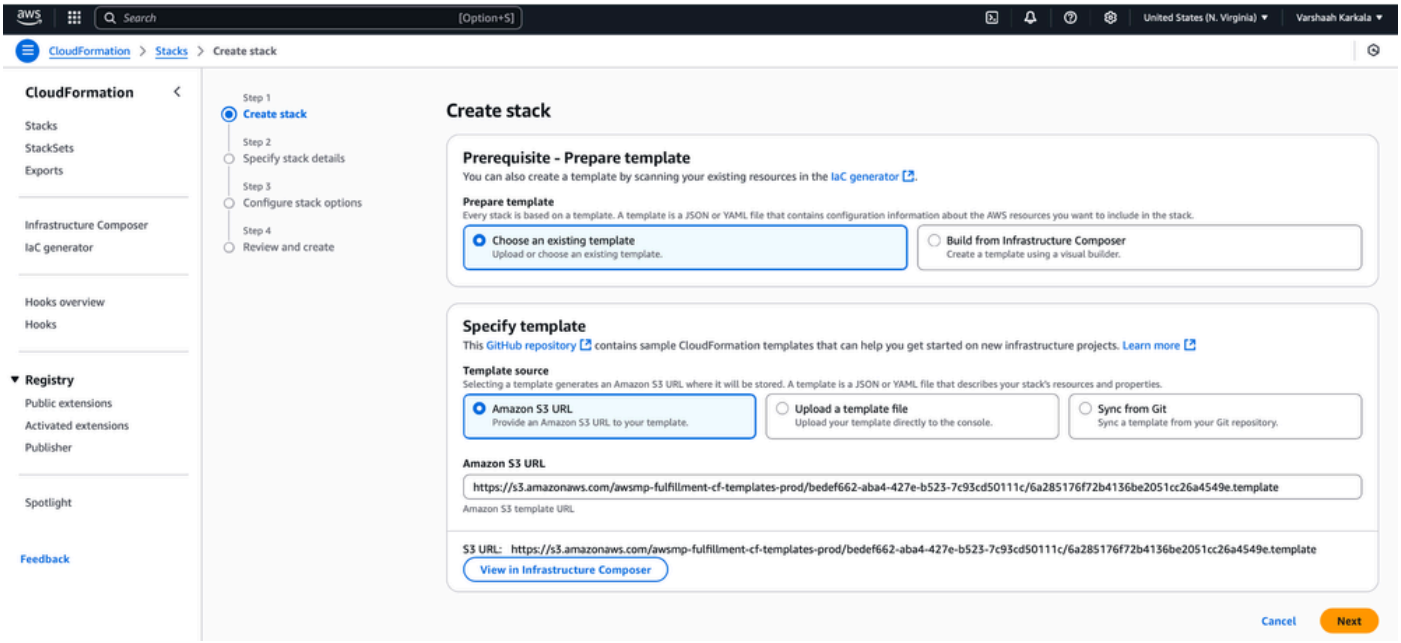
4. En Opción de cumplimiento, elija Plantilla de formación en la nube. Elija la versión de software (versión de ISE), la región donde desea implementar la instancia y haga clic en Continuar para iniciar.



5. En la siguiente página, seleccione Iniciar CloudFormation como la acción.

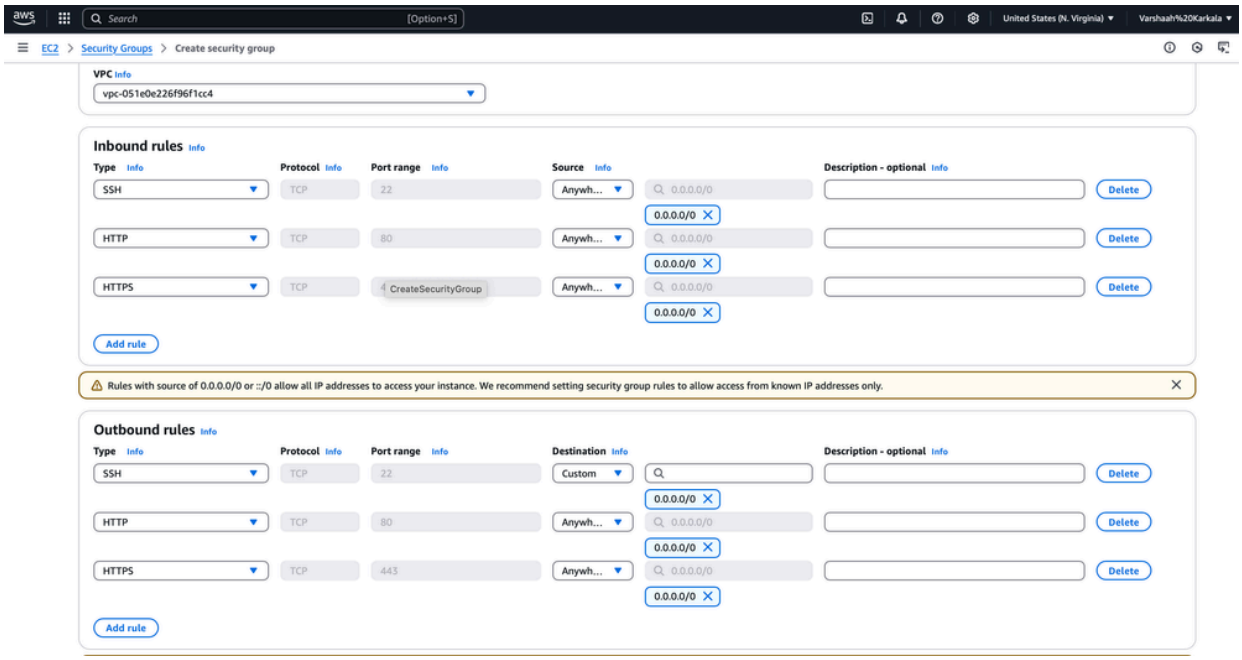


6. En los ajustes de pila, mantenga los ajustes predeterminados y haga clic en Next (Siguiente).



7. Introduzca los parámetros necesarios:

- Nombre de la pila: Proporcione un nombre único para la pila.
- Hostname: Asigne el nombre de host para el nodo de ISE.
- Par de claves: Seleccione el par de claves generado o preexistente para acceder a la instancia EC2 más adelante.
- Grupo de seguridad de administración:
    - Utilice el grupo de seguridad predeterminado (como se muestra a continuación) o cree uno personalizado a través del panel EC2.
    - Para crear un nuevo grupo de seguridad, navegue hasta el Panel EC2 y vaya a Red y seguridad > Grupos de seguridad para crear un nuevo grupo de seguridad.
    - Haga clic en Crear grupo de seguridad e introduzca los detalles necesarios.
    - Asegúrese de que el grupo de seguridad esté configurado para permitir el tráfico entrante y saliente requerido. Por ejemplo, habilite el acceso SSH (puerto 22) desde su dirección IP para el acceso CLI.

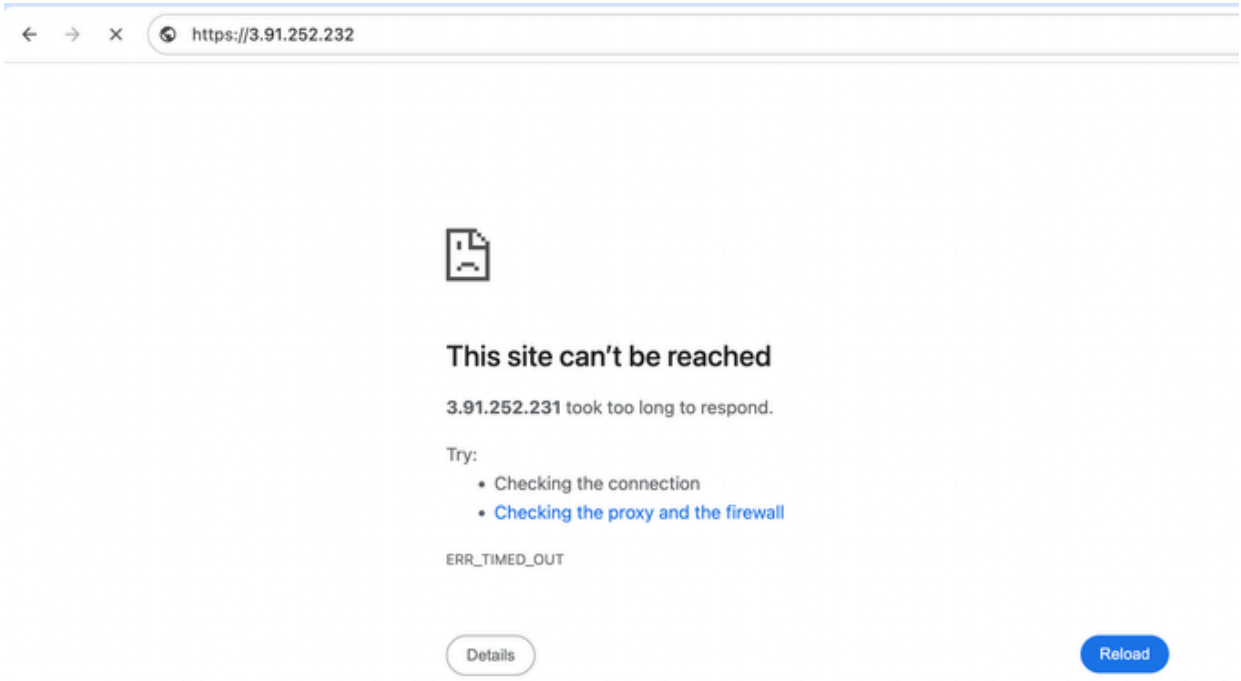


- Si el acceso SSH no está configurado correctamente, puede encontrar un error "Operation timed out" cuando intente conectarse vía SSH.

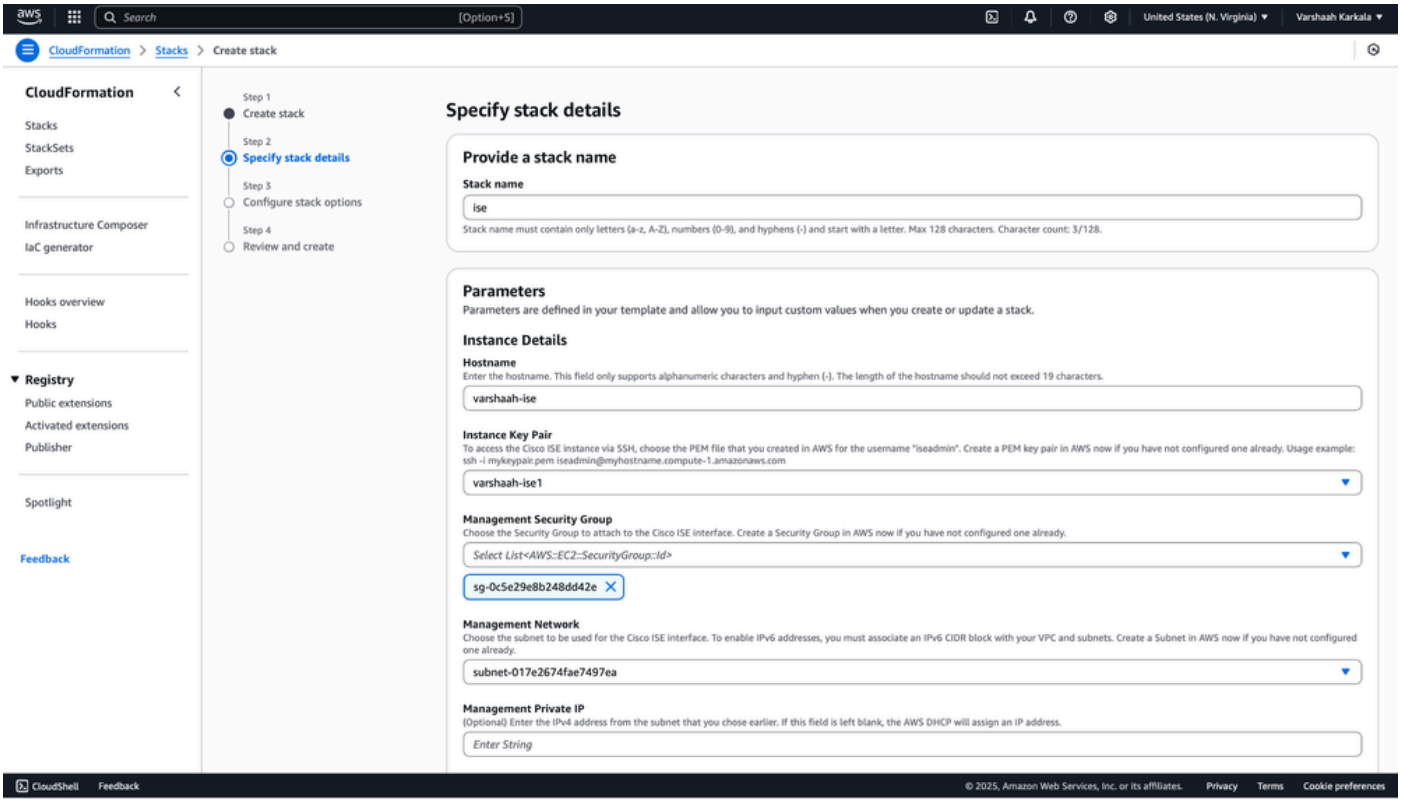
```
[                    -M-L63P Downloads % chmod 400 varshaah-ise1.pem
[                    -M-L63P Downloads % ssh -i varshaah-ise1.pem admin@3.91.252.232

ssh: connect to host 3.91.252.232 port 22: Operation timed out
```

- Si no se configura el acceso HTTP/HTTPS, es posible que vea el error "No se puede acceder a este sitio" al intentar acceder a la GUI.



- Red de administración: se ha seleccionado una de las subredes existentes.



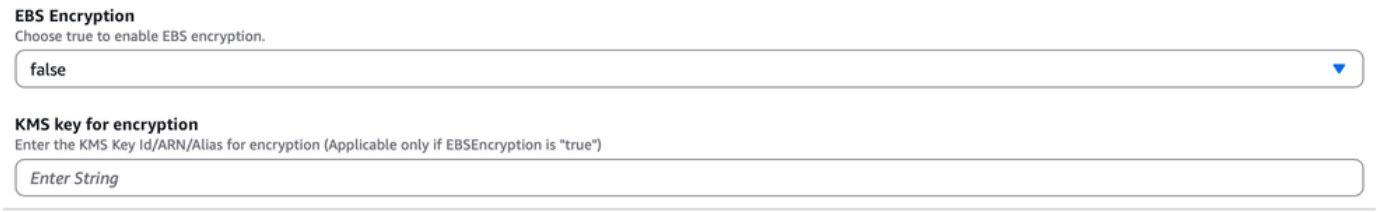
Si su diseño requiere una implementación distribuida con algunos nodos alojados en AWS y otros en las instalaciones, configure un VPC dedicado con una subred privada y establezca un túnel VPN al dispositivo de cabecera VPN en las instalaciones para habilitar la conectividad entre los nodos ISE alojados en AWS y en las instalaciones.

Para obtener pasos detallados sobre la configuración del Dispositivo de Cabecera VPN, consulte

esta guía.

8. Cifrado EBS

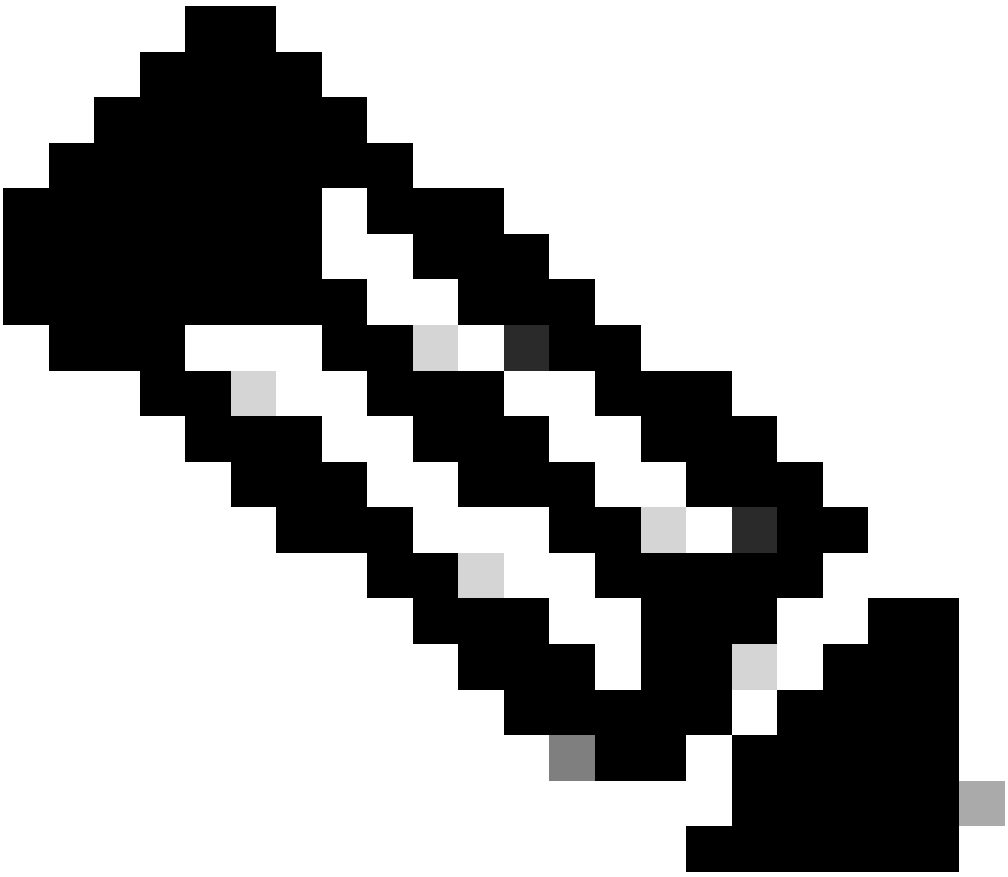
- Desplácese hacia abajo para localizar los parámetros de encriptación EBS.
- Establezca Cifrado EBS en False a menos que tenga necesidades de cifrado específicas.



9. Configuración de red:

- Desplácese hacia abajo hasta las opciones de acceso para configurar los parámetros de red, como el dominio DNS, el servidor de nombres principal y el servidor NTP principal.

  Asegúrese de que estos valores se introducen con precisión.



Nota: Una sintaxis incorrecta puede impedir que los servicios ISE se inicien correctamente tras la implementación.

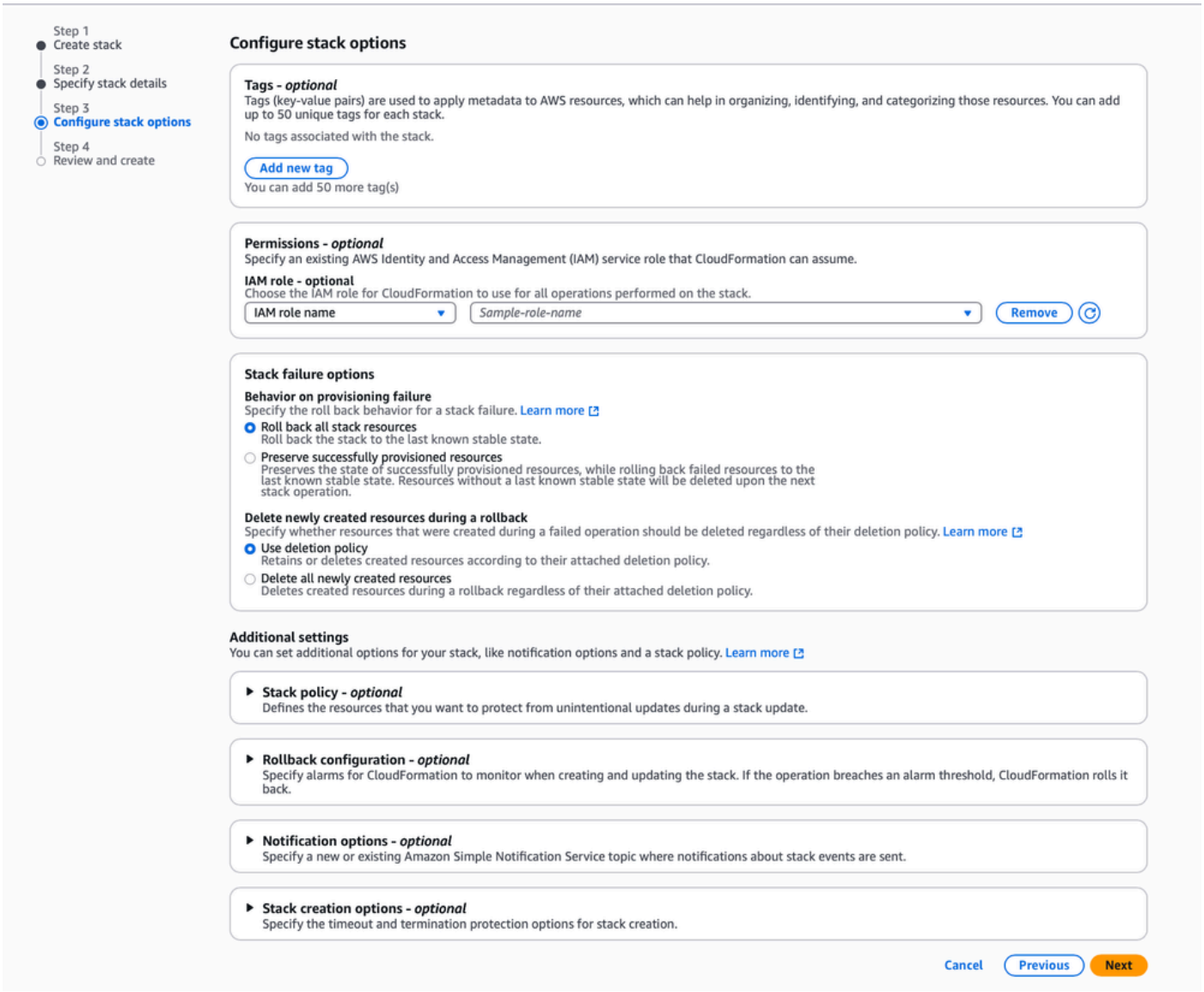
10. Detalles del servicio y del usuario:

- Desplácese hacia abajo hasta encontrar la opción para habilitar los servicios ERS y pxGrid
- Elija si desea habilitar los servicios ERS y pxGrid seleccionando yes o no.
- En Detalles del usuario, establezca la contraseña para el usuario admin predeterminado.

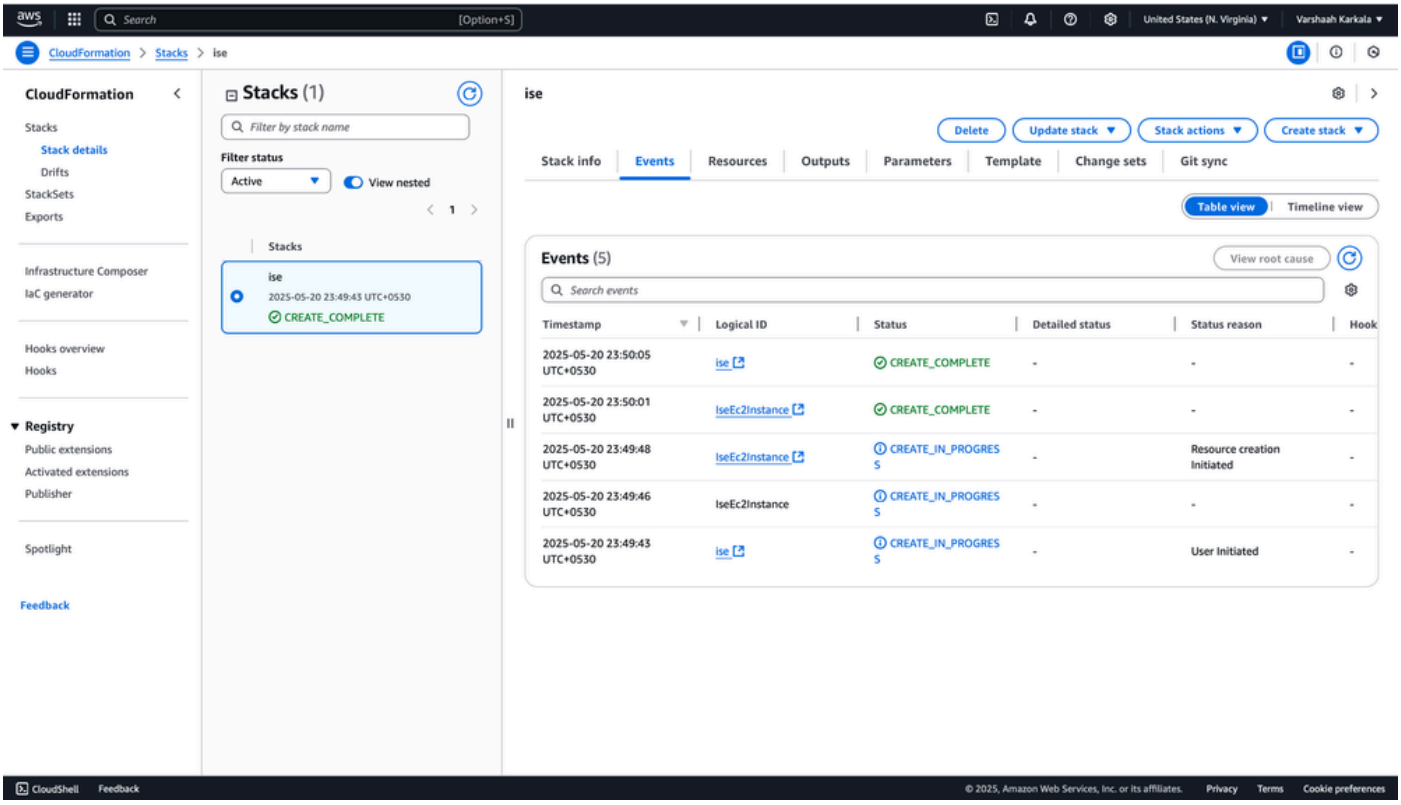
- Haga clic en Next (Siguiente).

11. Configurar opciones de pila:

- Deje todas las opciones predeterminadas tal como están y haga clic en Next.



12. Revise la plantilla para asegurarse de que todas las configuraciones son correctas y, a continuación, haga clic en Enviar. Una vez creada la plantilla, se asemeja al ejemplo que se muestra a continuación:



13. Acceda a los detalles de la pila:
Navegue hasta el servicio CloudFormation en la consola de administración de AWS y vaya a la sección Stacks. Busque la pila implementada en la lista.

14. Pestaña Ver Salidas:

Seleccione su pila y abra la pestaña Salidas. Aquí encontrará información importante generada durante el proceso de implementación, como:

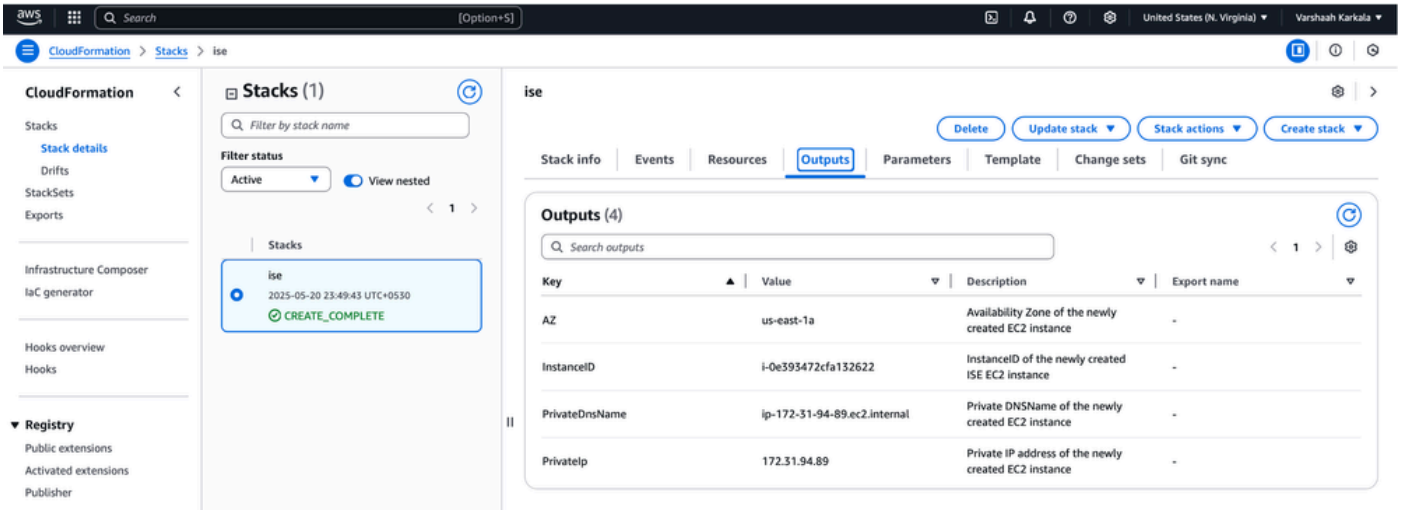
· Zona de disponibilidad: Región en la que se implementan los recursos.

· ID de instancia: Identificador único de la instancia implementada.

· Nombre DNS: El nombre DNS privado de la instancia, que se puede utilizar para el acceso remoto.

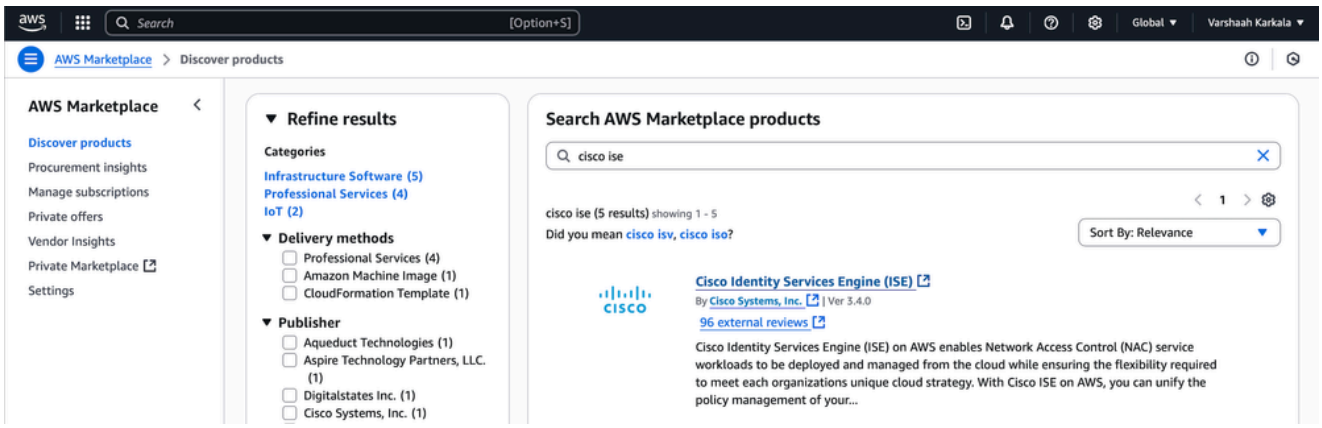
•Dirección IP: La dirección IP pública o privada de la instancia, en función de la configuración.

Esta información le ayuda a conectarse a la instancia y a verificar su disponibilidad. La ficha Salidas se parece a este ejemplo:



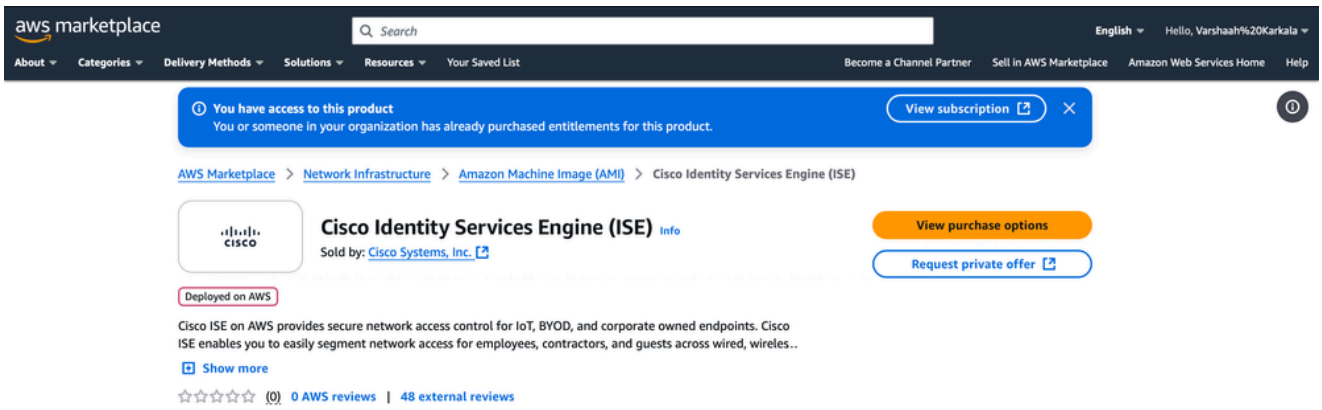
Parte 3: Configuración de ISE con Amazon Machine Image (AMI)

1. Inicie sesión en AWS Management Console y busque AWS Marketplace Subscriptions.
2. En la barra de búsqueda, escriba "cisco ise" y seleccione Cisco Identity Services Engine (ISE) en los resultados.

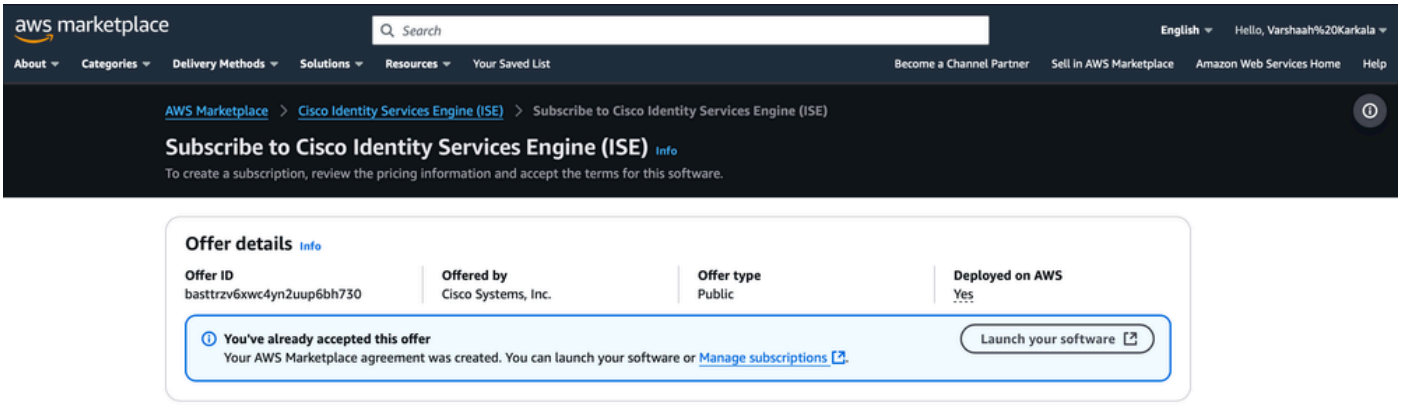


ISE en AWS Marketplace

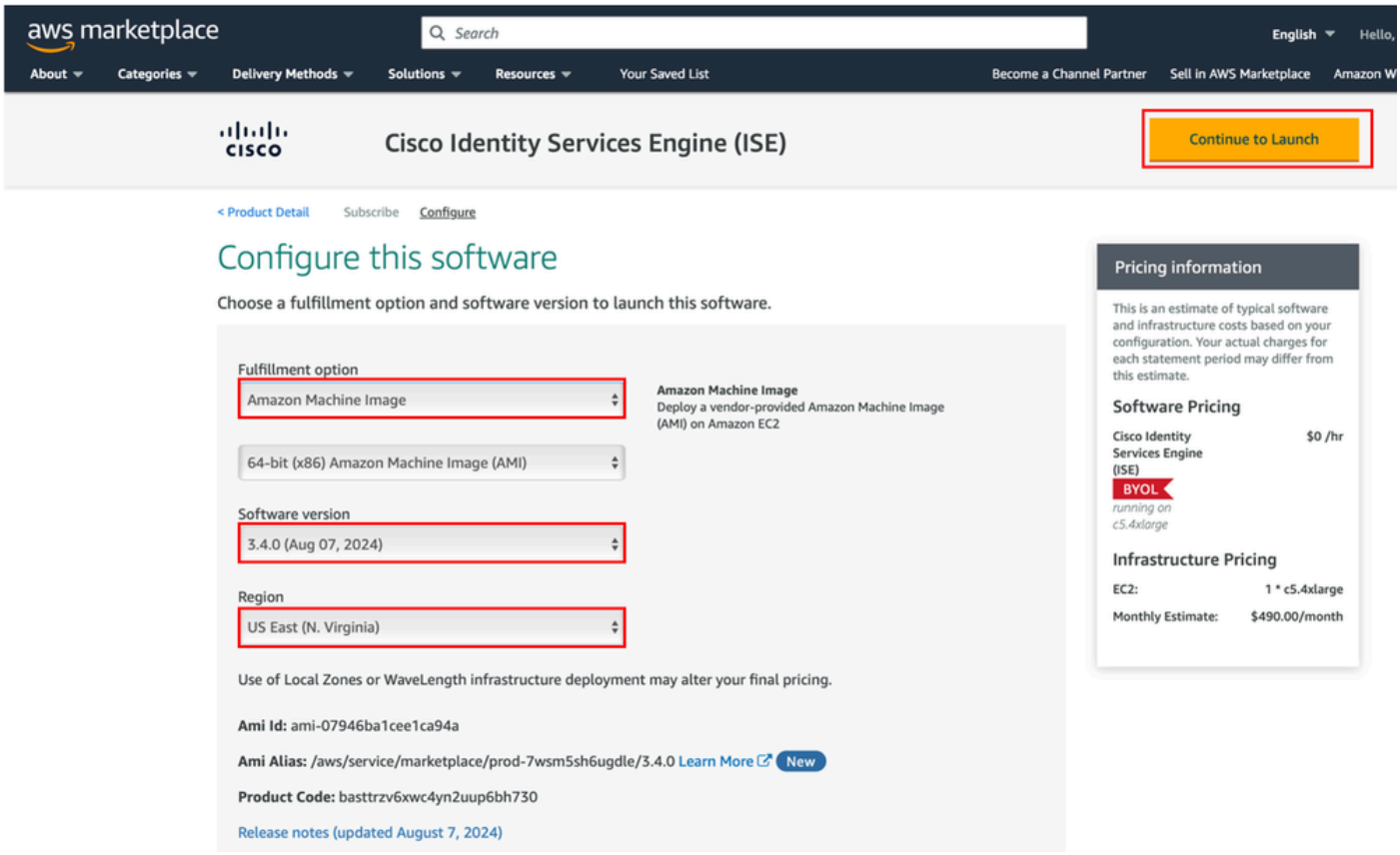
3. Haga clic en Ver opciones de compra.



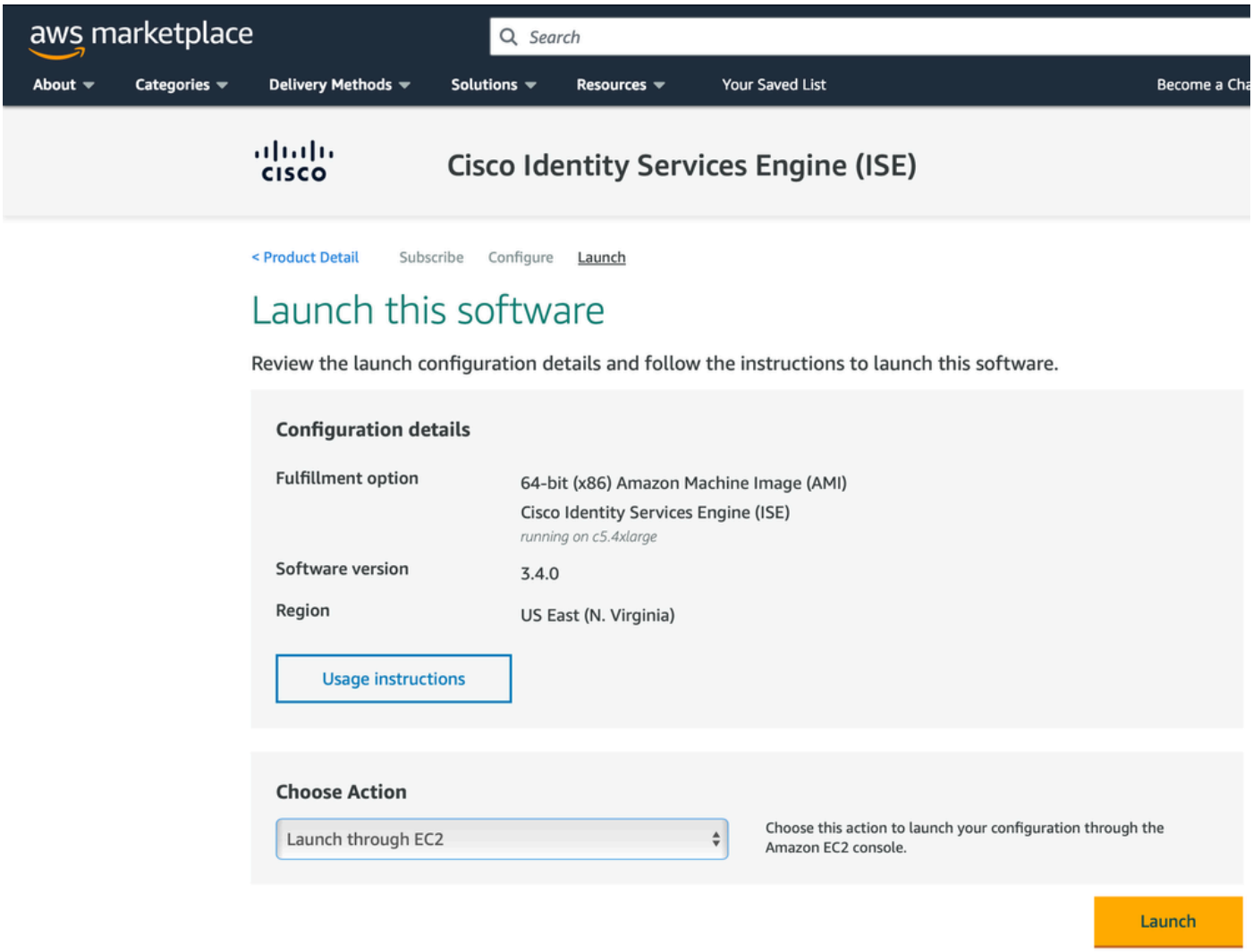
4. Haga clic en Iniciar el software.



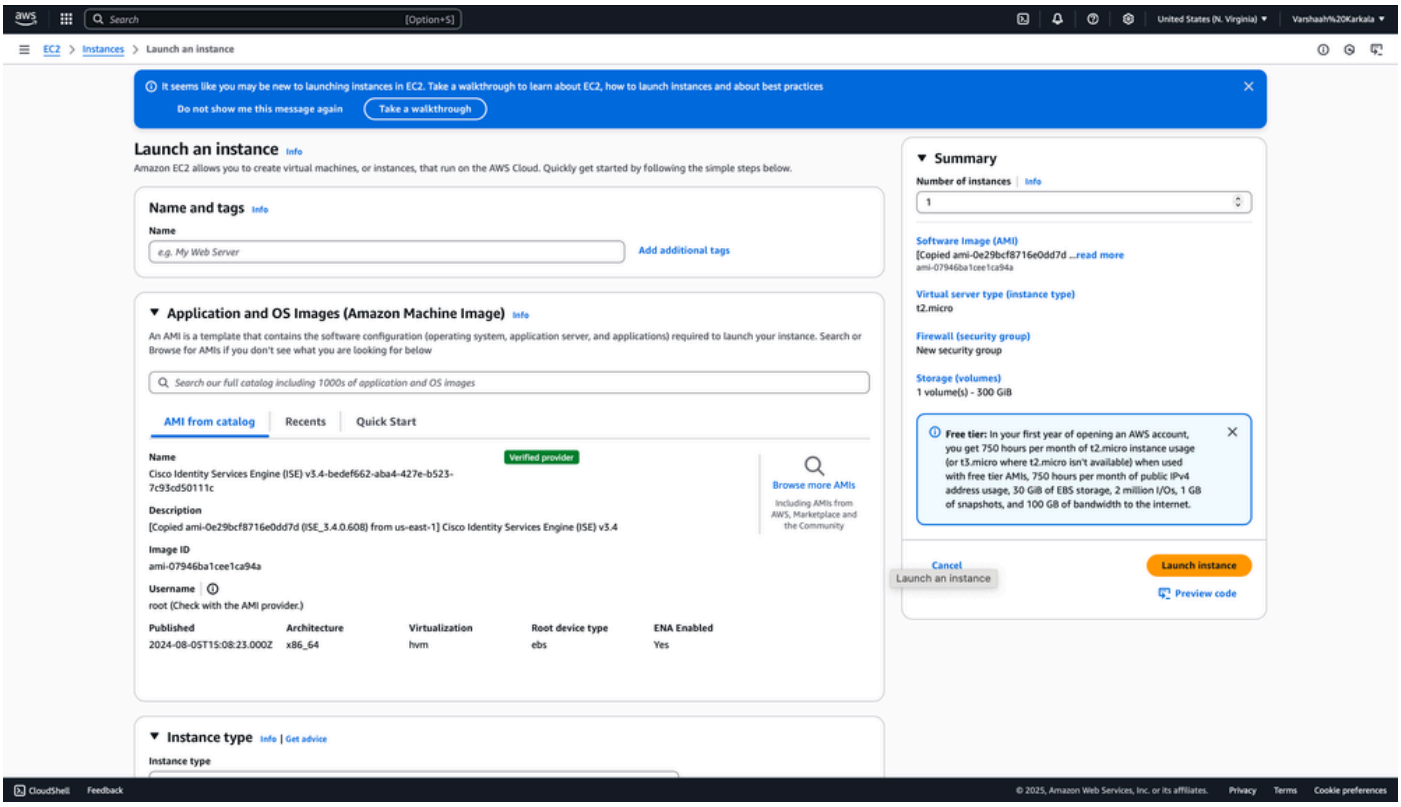
5. En la opción de cumplimentación, seleccione Amazon Machine Image. Seleccione la versión de software que desee y la región AWS, a continuación, haga clic en Continuar para iniciar.



6. En el menú desplegable Elegir acción, seleccione Iniciar a EC2 y, a continuación, haga clic en Iniciar para continuar.



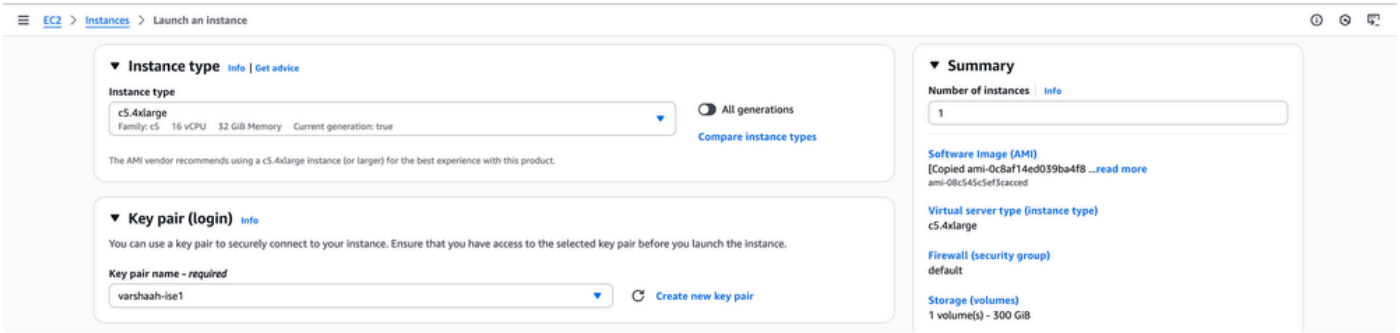
7. Se le redirige a la página EC2 Launch an Instance para configurar los parámetros de la instancia.



8. Desplácese hasta la sección Tipo de Instancia y seleccione un tipo de instancia adecuado en función de los requisitos de despliegue.

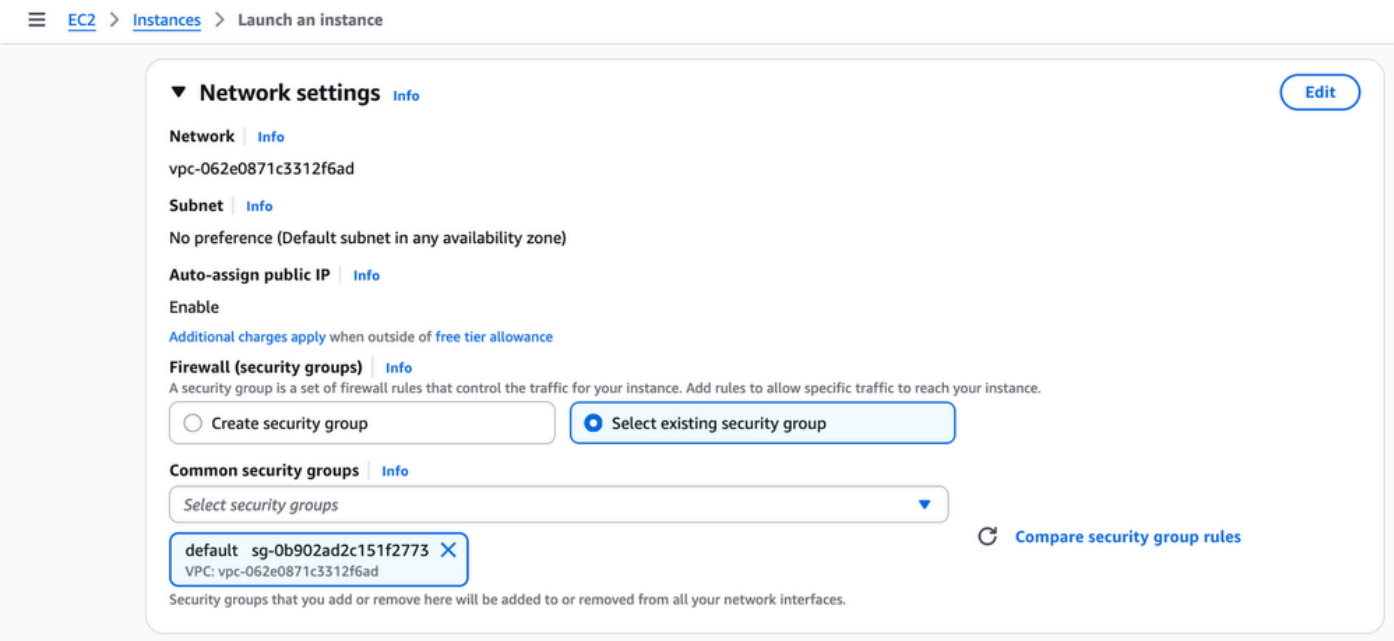
En Key pair (inicio de sesión), seleccione el par de claves que se generó anteriormente o cree uno nuevo (consulte los pasos de creación de pares de claves proporcionados anteriormente).

Establezca el Número de instancias en 1.



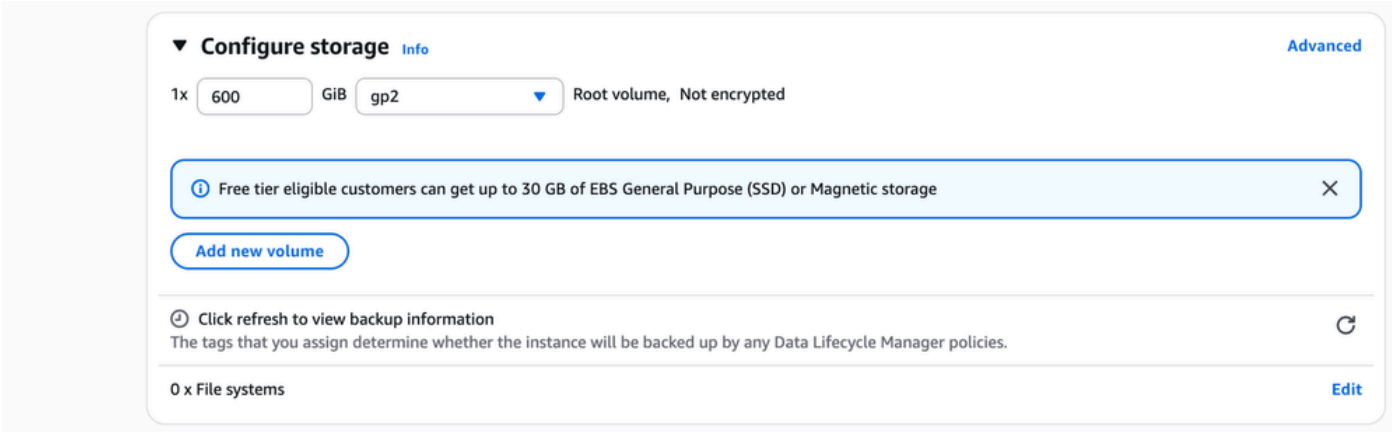
9. En la sección Configuración de red:

- Configure el VPC y la subred según sea necesario.
- Para el grupo de seguridad, seleccione uno existente o cree un nuevo grupo (como se muestra en el ejemplo).



10. En la sección Configure Storage, configure el tamaño de volumen deseado.

Ejemplo: 600 GiB con el tipo de volumen gp2.



11. En la sección Detalles Avanzados, configure cualquier configuración adicional necesaria para la implementación, como el perfil de instancia de IAM, los datos de usuario o el comportamiento de apagado.

▼ **Advanced details** Info

Domain join directory | Info

Select ▼ Create new directory

IAM instance profile | Info

Select ▼ Create new IAM profile

Hostname type | Info

IP name ▼

DNS Hostname | Info

- Enable IP name IPv4 (A record) DNS requests
- Enable resource-based IPv4 (A record) DNS requests
- Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery | Info

Default ▼

Shutdown behavior | Info

Stop ▼

Stop - Hibernate behavior | Info

Disable ▼

Termination protection | Info

Disable ▼

Stop protection | Info

Select ▼

Detailed CloudWatch monitoring | Info

Disable ▼

Credit specification | Info

Standard ▼

Placement group | Info

Select ▼ Create new placement group

EBS-optimized instance | Info

Disable ▼

Instance bandwidth configuration | Info

Default ▼

Purchasing option | Info

- (●) None
- ( ) Capacity Blocks
  Launch instances for your active capacity blocks
- ( ) Spot instances
  Request Spot Instances at the Spot price, capped at the On-Demand price

Capacity reservation | Info

None ▼

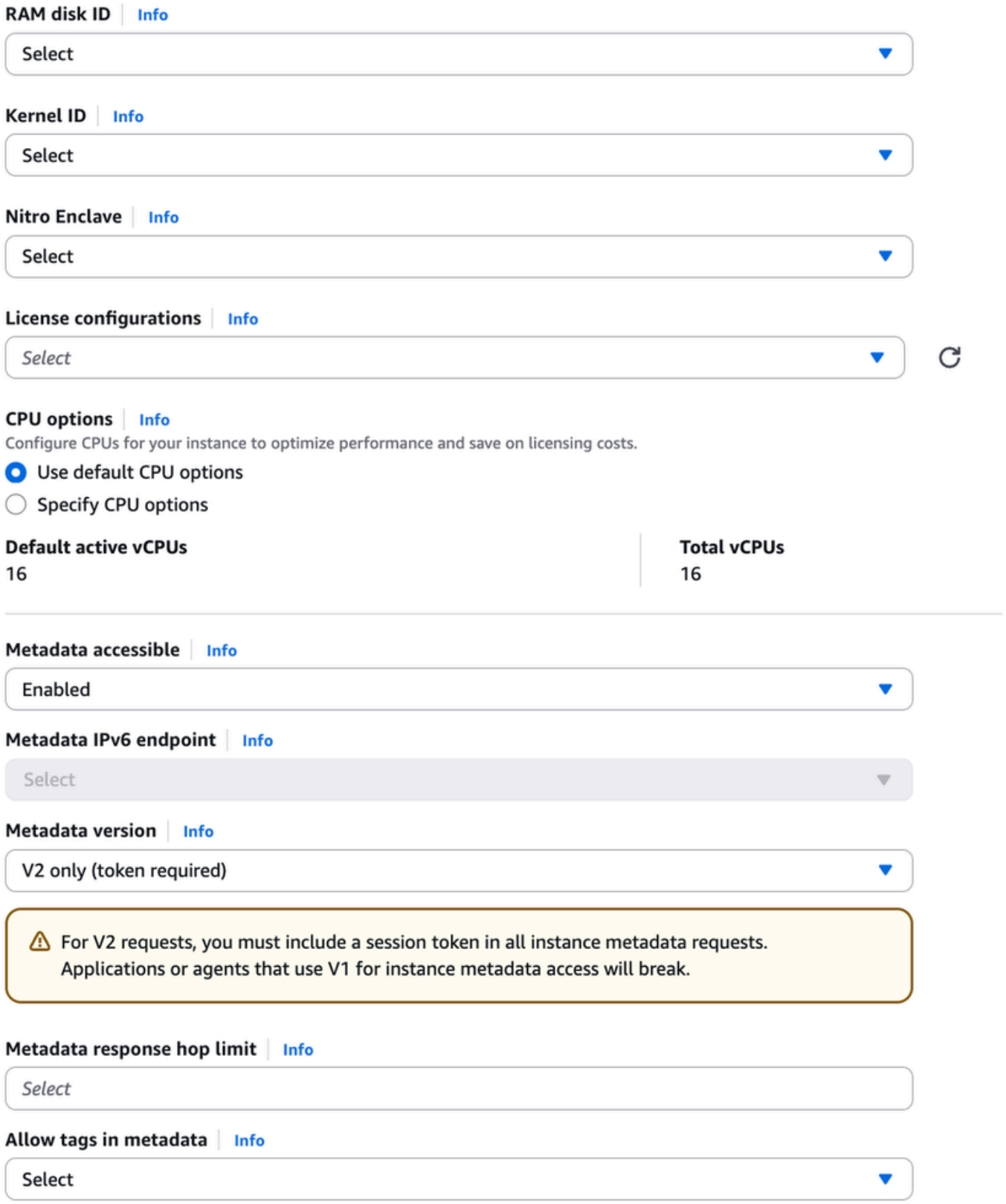
Tenancy | Info

Dedicated - run a dedicated instance ▼

Additional charges apply

12. En la sección Versión de metadatos:

- Para ISE versión 3.4 y posterior, seleccione V2 only (se requiere token); esta es la opción recomendada.
- Para las versiones de ISE anteriores a la 3.4, elija V1 y V2 (token opcional) para garantizar la compatibilidad.



13. En el campo Datos del usuario, proporcione los parámetros de configuración iniciales para la instancia de ISE, incluidos el nombre de host, DNS, el servidor NTP, la zona horaria, ERS y las credenciales de administrador.

Ejemplo:
hostname=varshaahise2

primarynameserver=x.x.x.x

dnsdomain=varsha.local

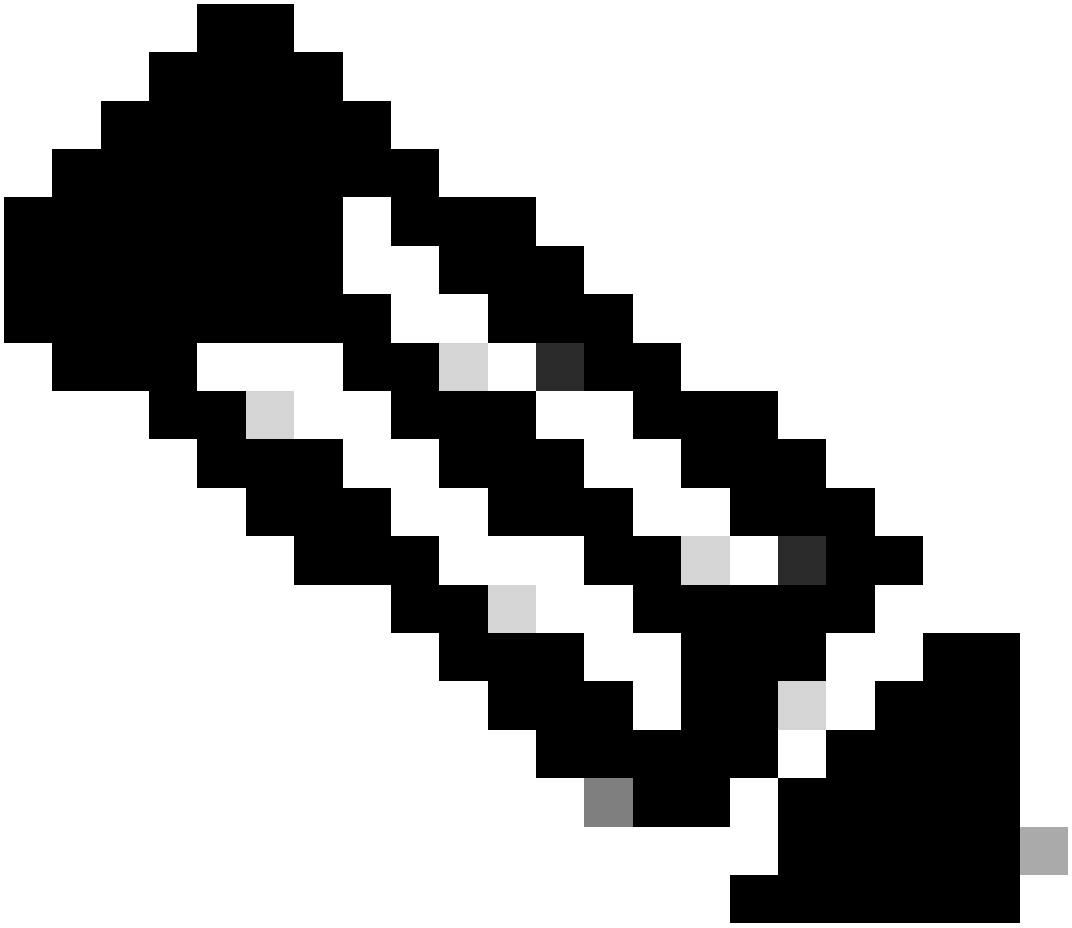
ntpserver=x.x.x.x

timezone=Asia/Calcuta

username=admin

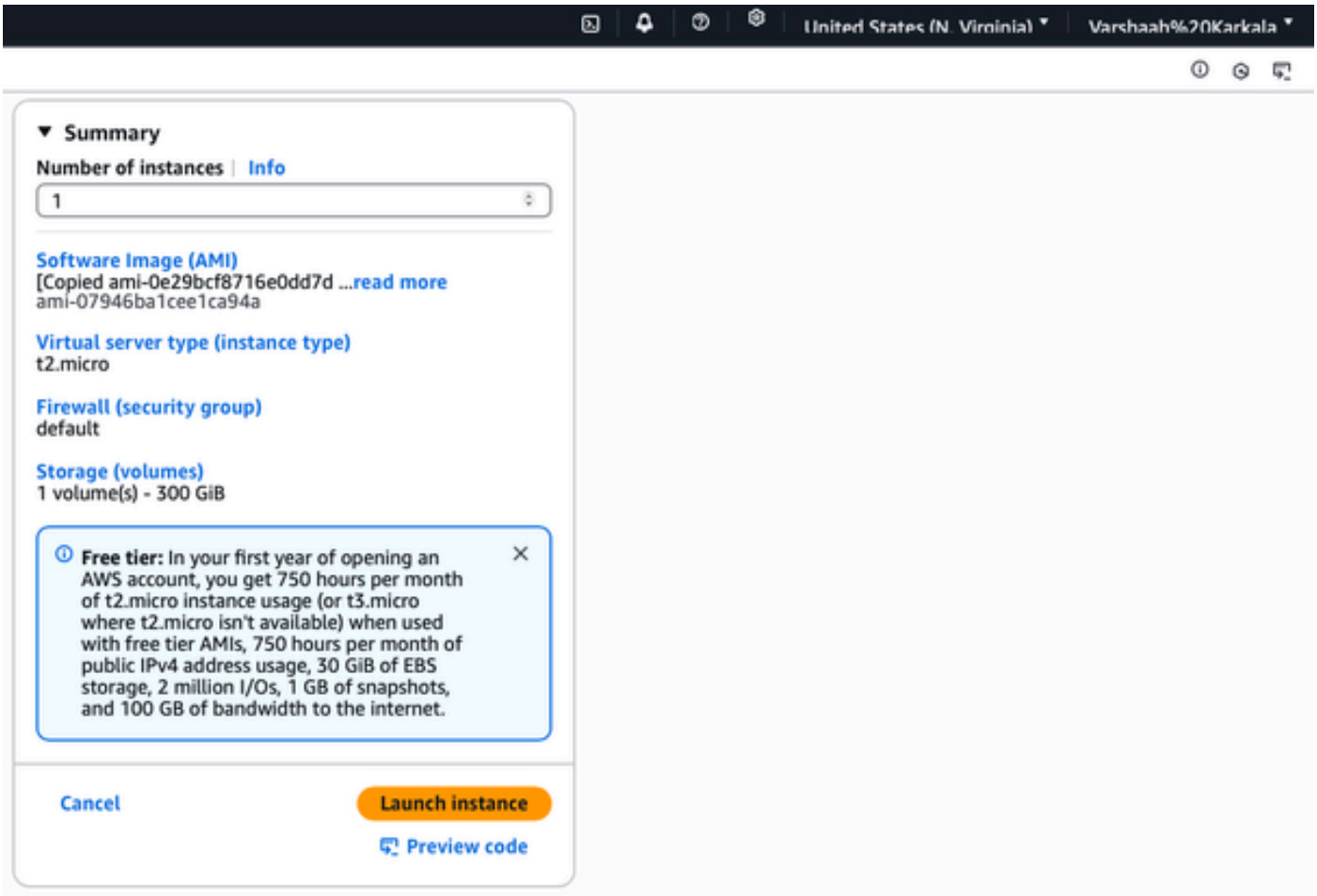
password=Ise@123

ersEnabled=true

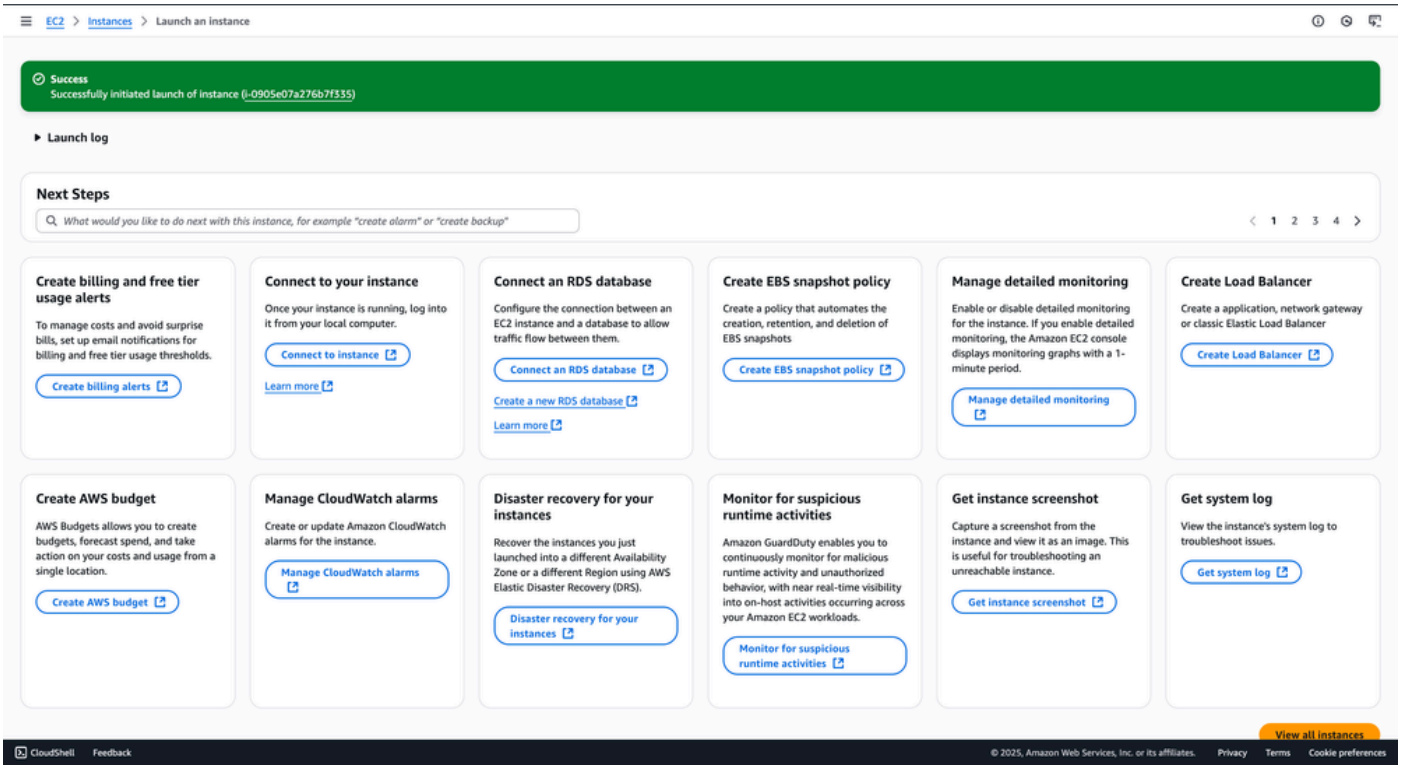


Nota: Asegúrese de que la contraseña cumpla con la política de contraseñas de Cisco ISE.

Una vez introducidos los datos de usuario y completada la configuración, haga clic en Iniciar instancia.



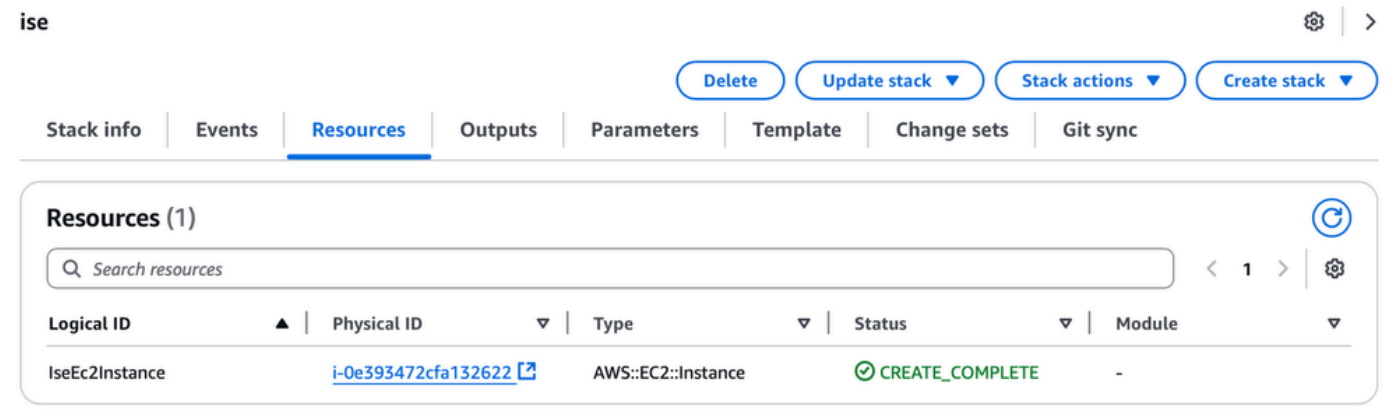
14. Una vez iniciada la instancia, aparece un mensaje de confirmación que indica: 'Se inició correctamente el inicio de la instancia <nombre_instancia>'. Esto indica que el proceso de inicio se ha iniciado correctamente.

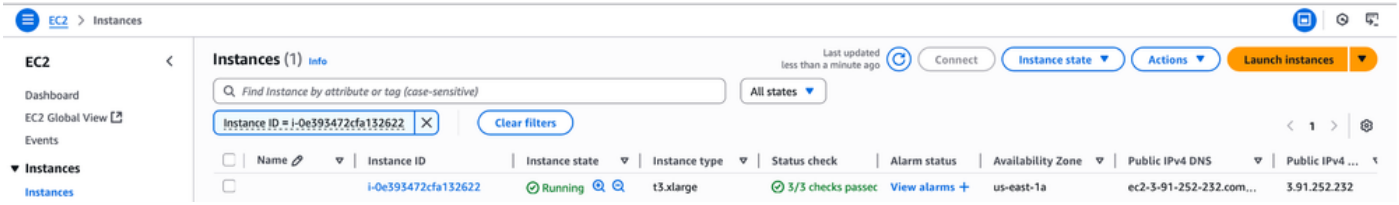


Verificación

Acceder a la instancia de ISE creada con CFT

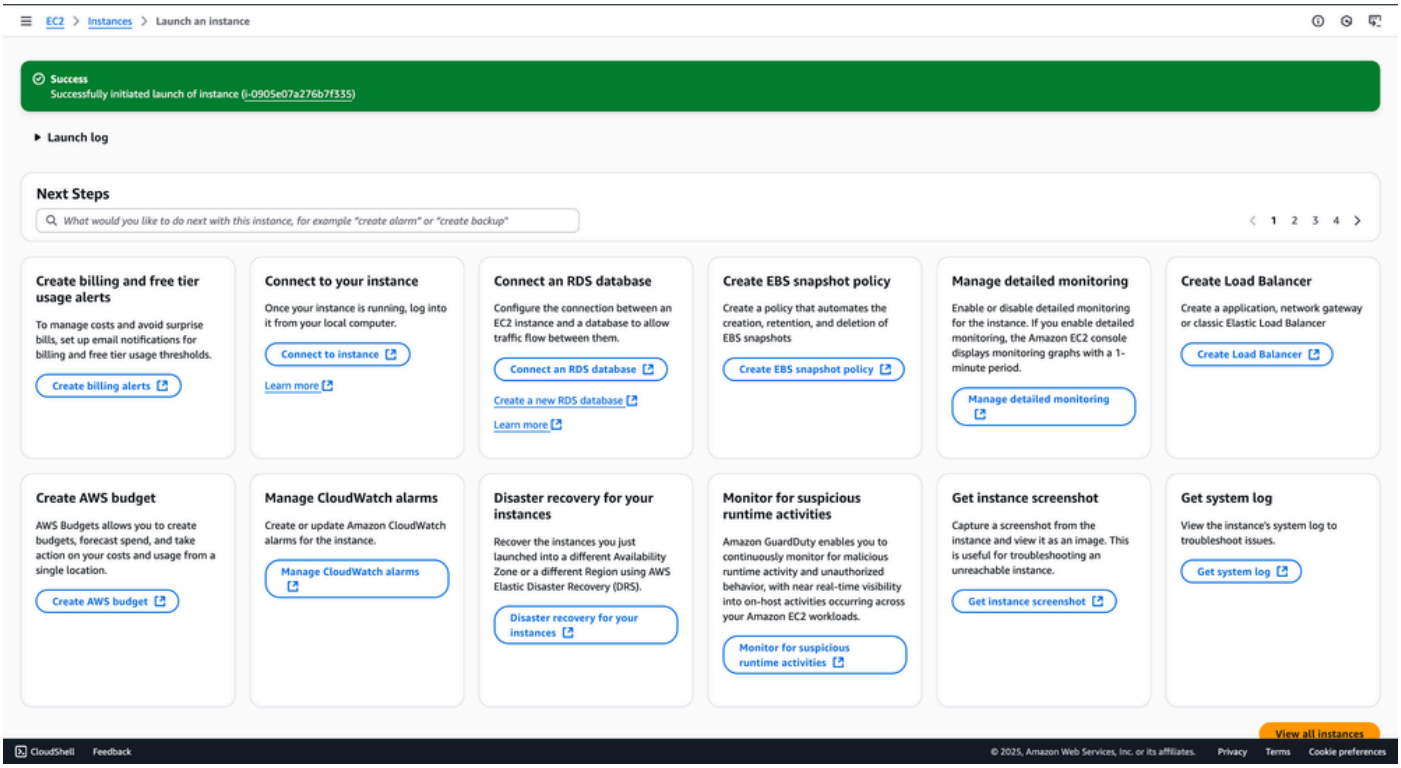
Vaya a la pestaña Resources en su pila de CloudFormation y haga clic en la ID física. Le redirige al panel EC2, donde podrá ver la instancia.

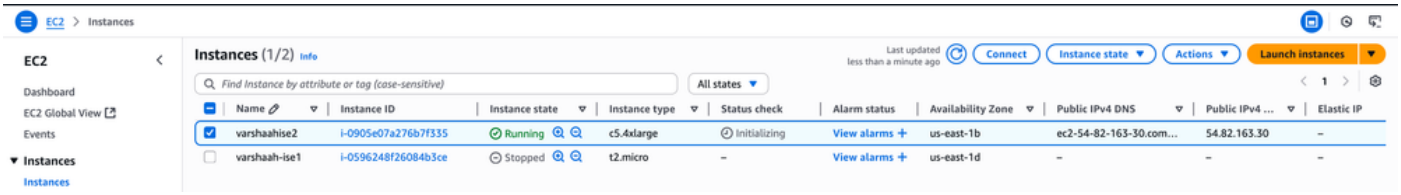




Acceder a la instancia de ISE creada con AMI

Haga clic en Ver todas las Instancias para navegar a la página Instancias EC2. En esta página, compruebe que la Comprobación de Estado aparece cuando se superan las comprobaciones 3/3, indicando que la instancia está activa y en buen estado.





Acceder a la GUI de ISE

El servidor ISE se ha implementado correctamente.

Para acceder a la GUI de ISE, debe utilizar la dirección IP de la instancia en el navegador. Dado que la IP predeterminada es privada, no se puede acceder a ella directamente desde Internet.

Verifique si una IP pública está asociada con la instancia:

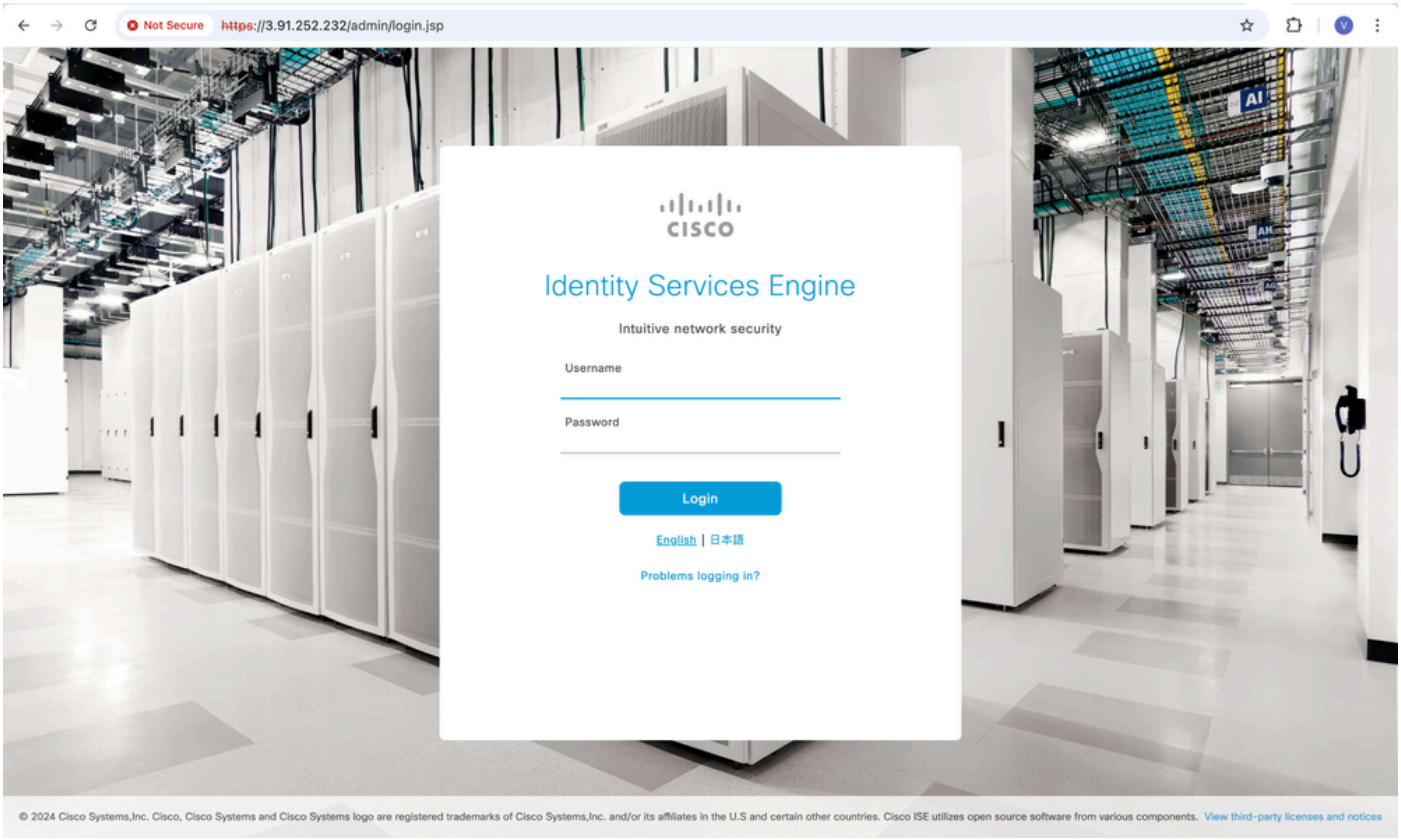
- Navegue hasta EC2 > Instancias y seleccione su instancia.
- Busque el campo Public IPv4 address.

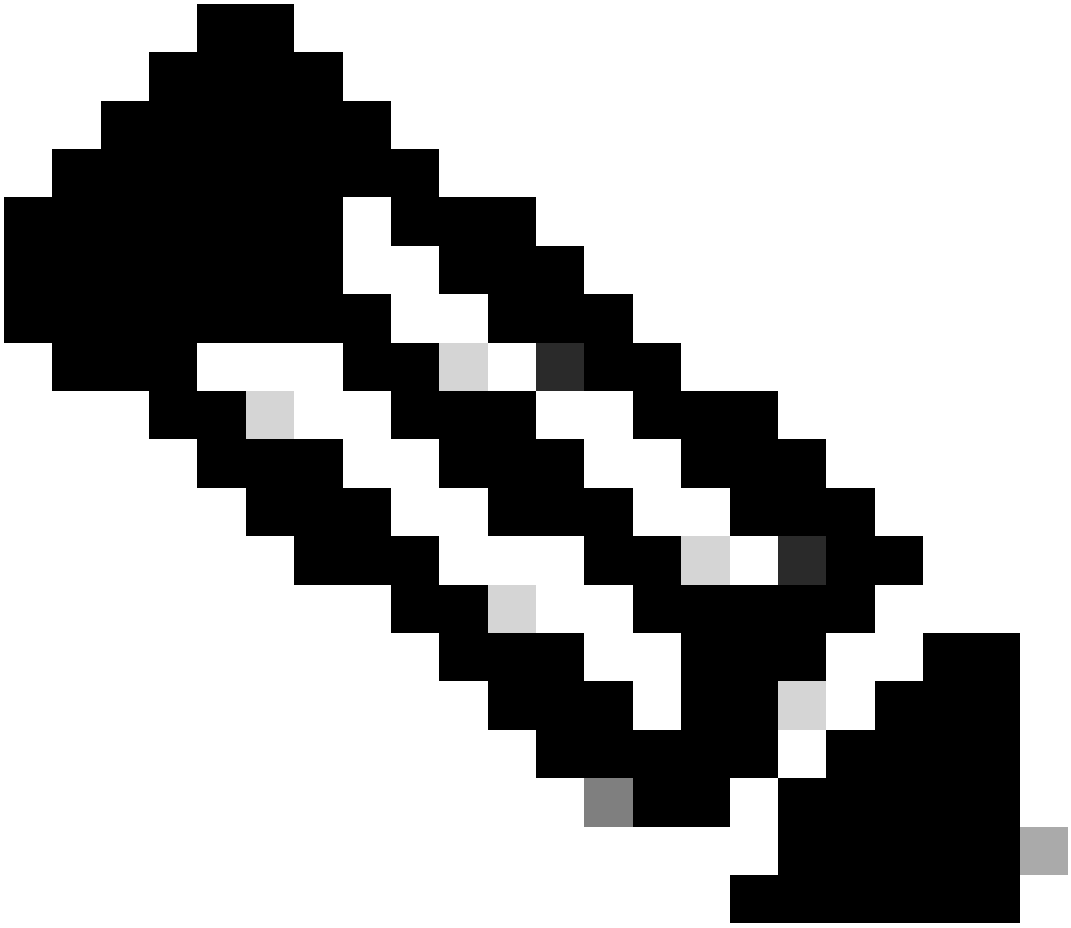
Aquí, podemos ver una dirección IP pública que puede utilizar para acceder a la GUI de ISE.

Abra un explorador compatible (por ejemplo, Chrome o Firefox) e introduzca la dirección IP

pública.

Aparecerá la página de inicio de sesión GUI de ISE.





Nota: Una vez que el acceso SSH pasa a estar disponible, los servicios ISE tardan normalmente entre 10 y 15 minutos más en realizar la transición completa a un estado en ejecución.

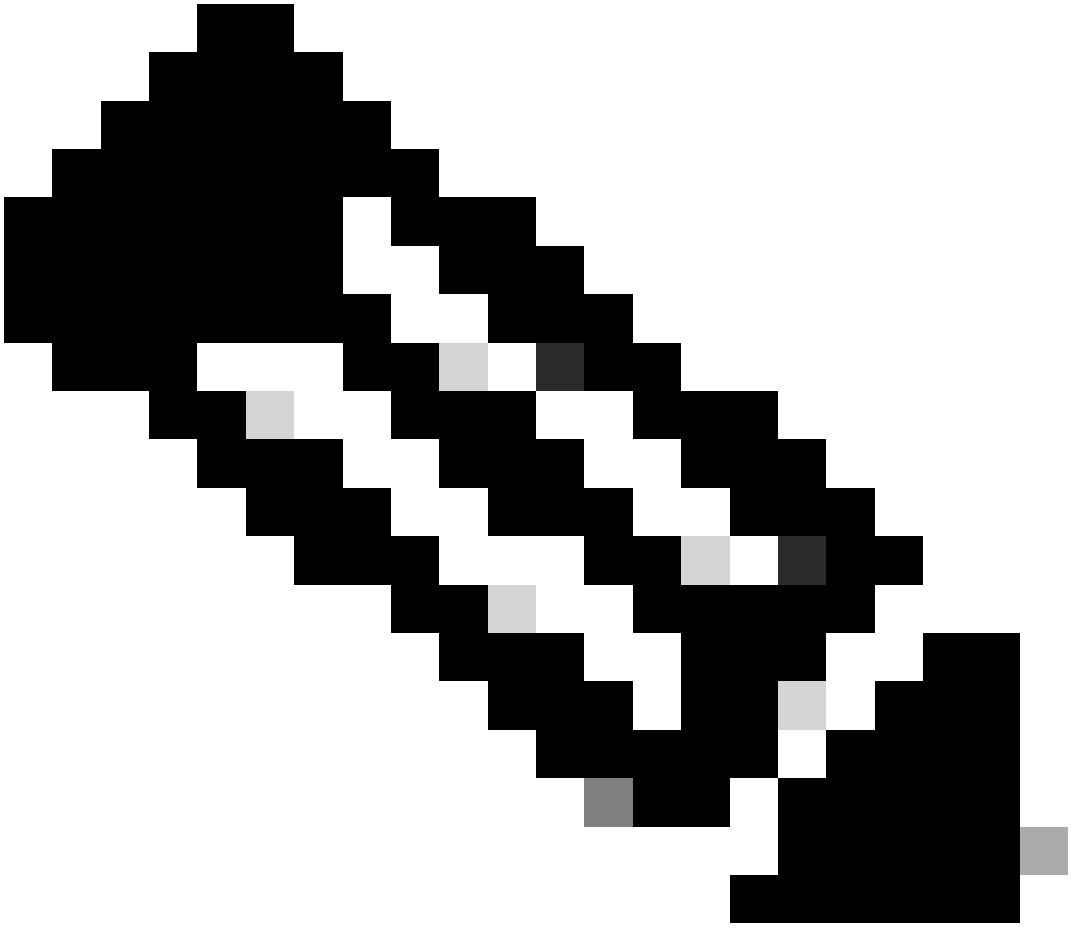
Acceso a CLI a través de SSH desde Terminal

En la consola EC2, seleccione su instancia y haga clic en Connect.

En la pestaña SSH client, siga estos pasos:

- Vaya a la carpeta que contiene el archivo de clave .pem descargado.
- Ejecute estos comandos:

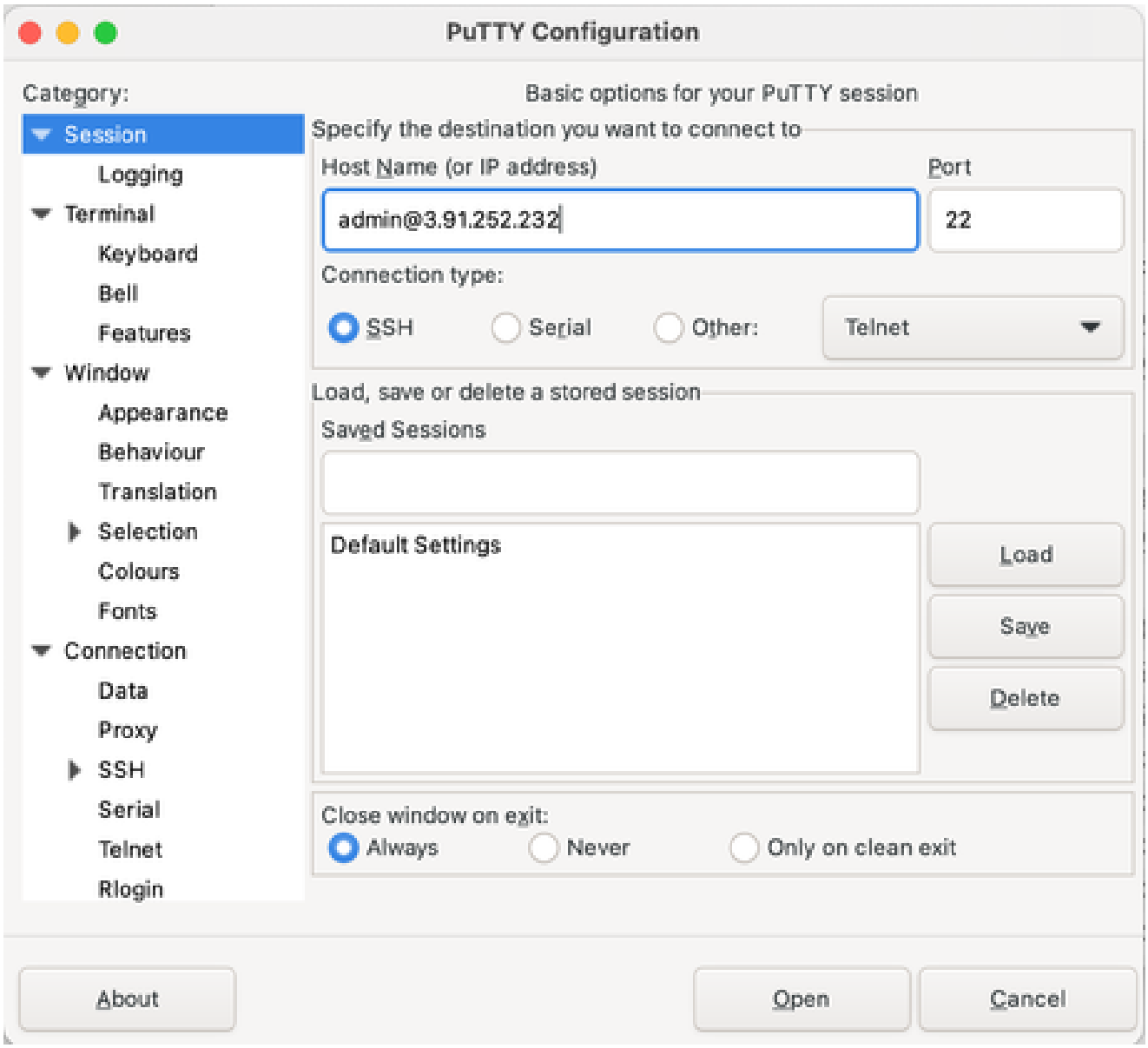
- cd <path-to-key-file>
- chmod 400 <your-key-pair-name>.pem
- ssh -i "<your-key-pair-name>.pem" admin@<public-ip-address>



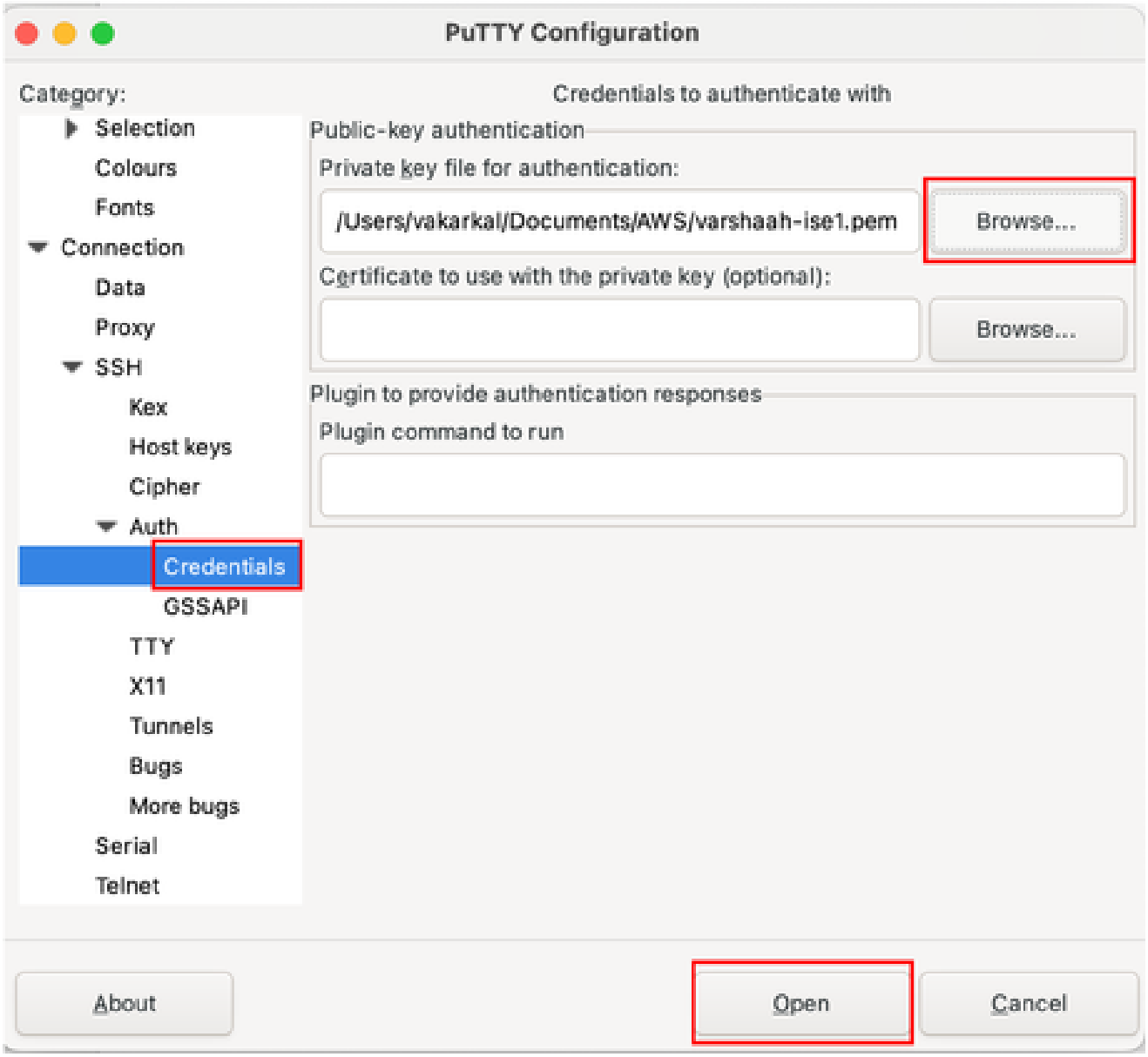
Nota: Utilice admin como usuario de SSH, ya que Cisco ISE desactiva el inicio de sesión raíz mediante SSH.

Acceso a CLI mediante SSH mediante PuTy

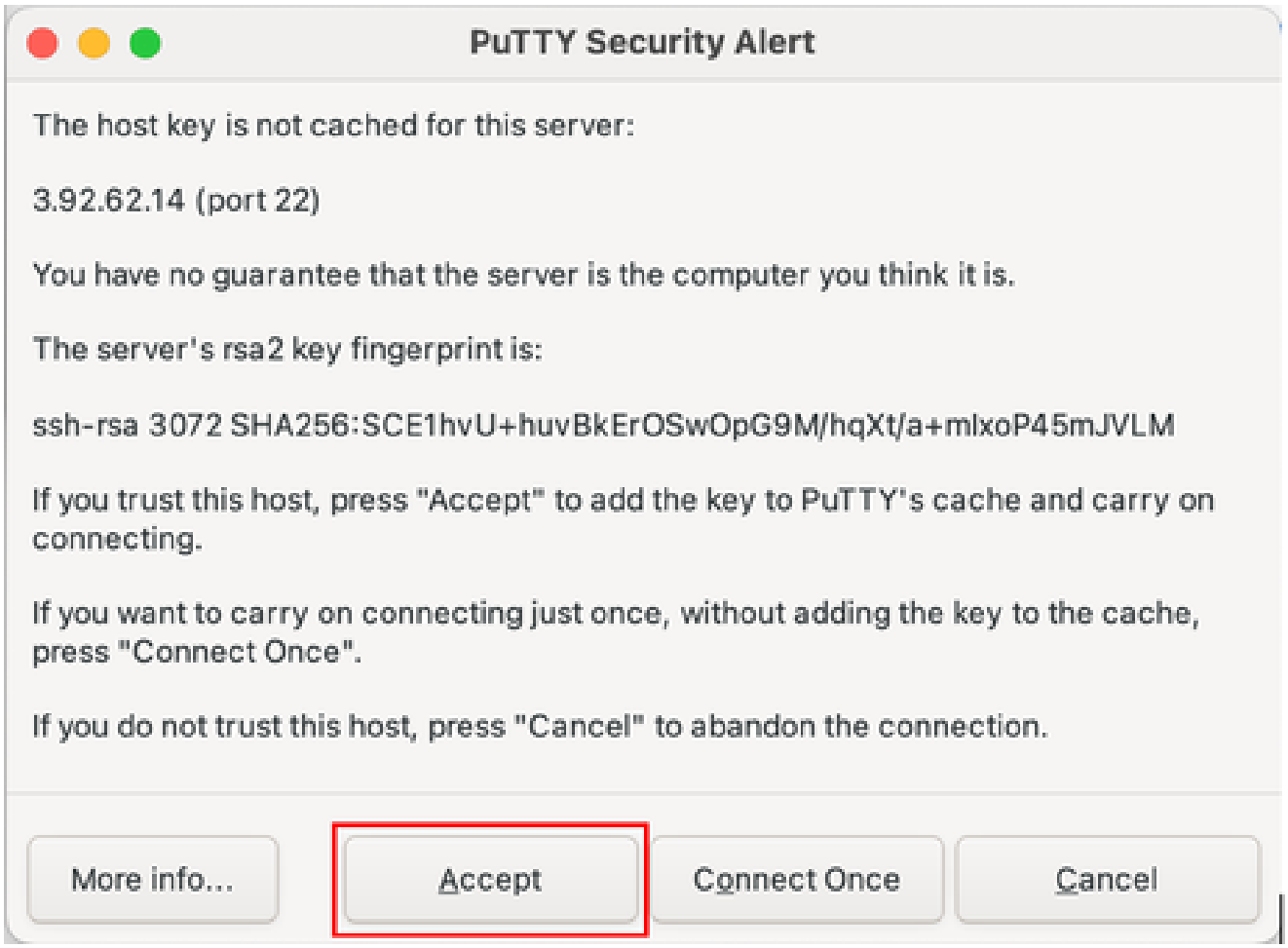
- Abra PuTTY.
- En el campo Host Name, introduzca: admin@<public-ip-address>



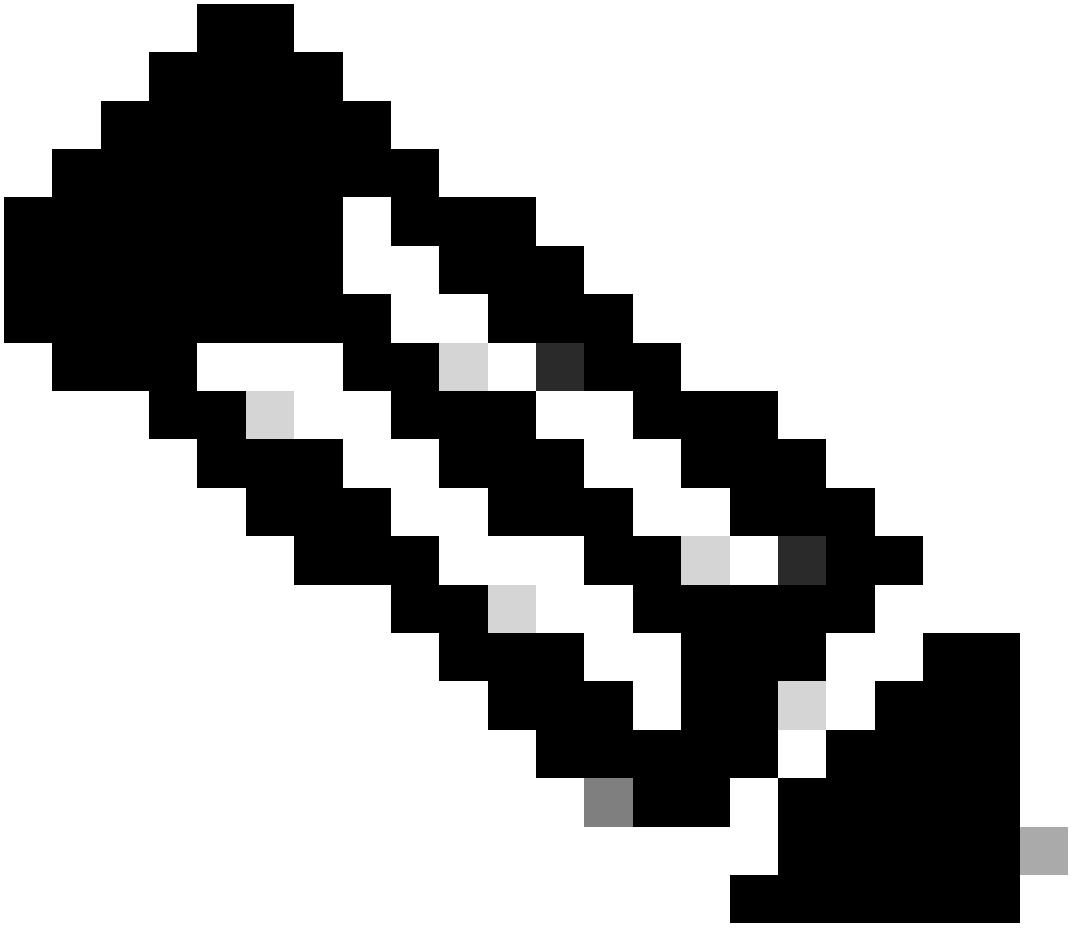
- En el panel izquierdo, navegue hasta Conexión > SSH > Autenticación > Credenciales.
- Haga clic en Browse junto a Private key file for authentication, y seleccione su archivo de clave privada SSH.
- Haga clic en Abrir para iniciar la sesión.



- Cuando se le solicite, haga clic en Accept para confirmar la clave SSH.



- La sesión de PuTTY se conecta ahora a la CLI de ISE.

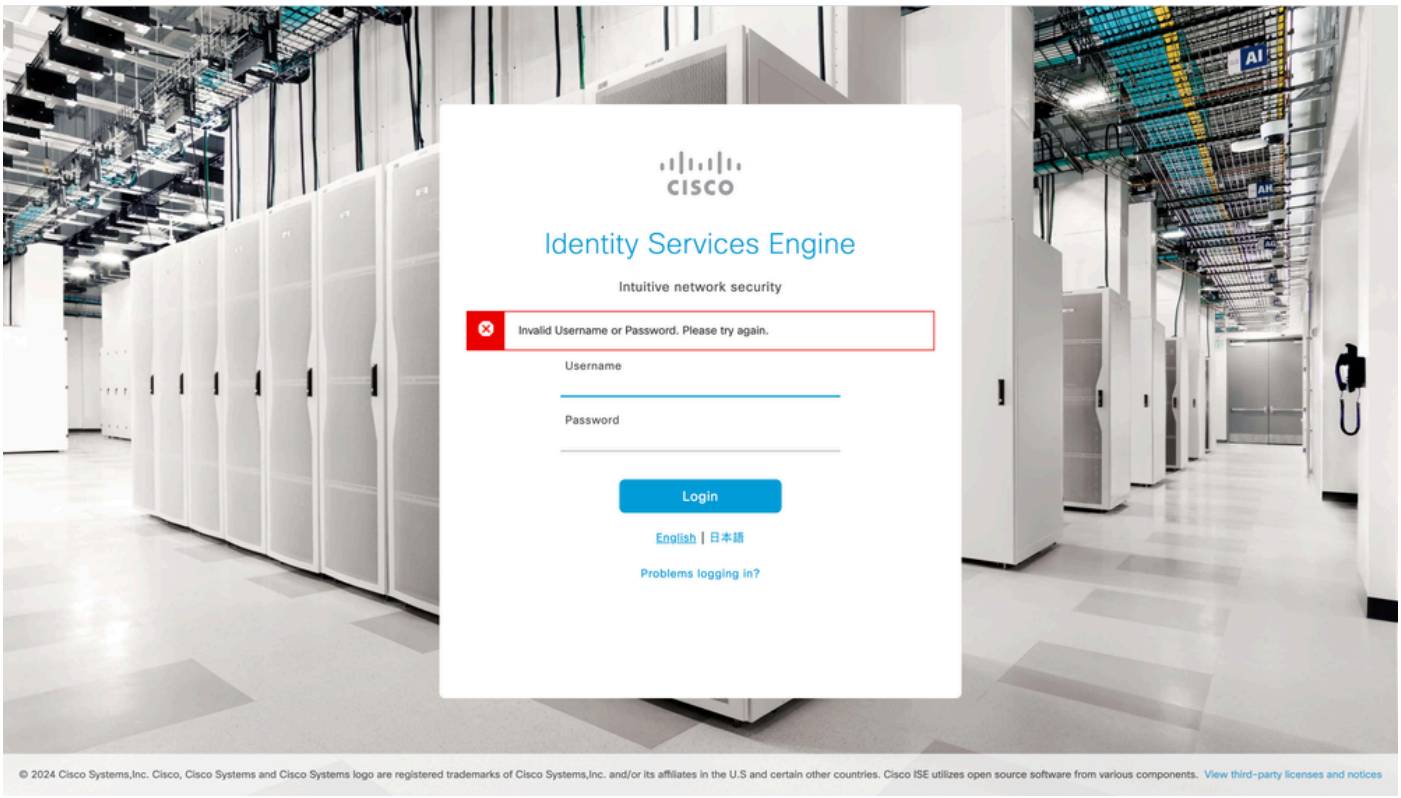


Nota: Puede tardar hasta 20 minutos en que ISE sea accesible a través de SSH. Durante este tiempo, los intentos de conexión pueden fallar con el error: "Permiso denegado (clave pública)."

Troubleshoot

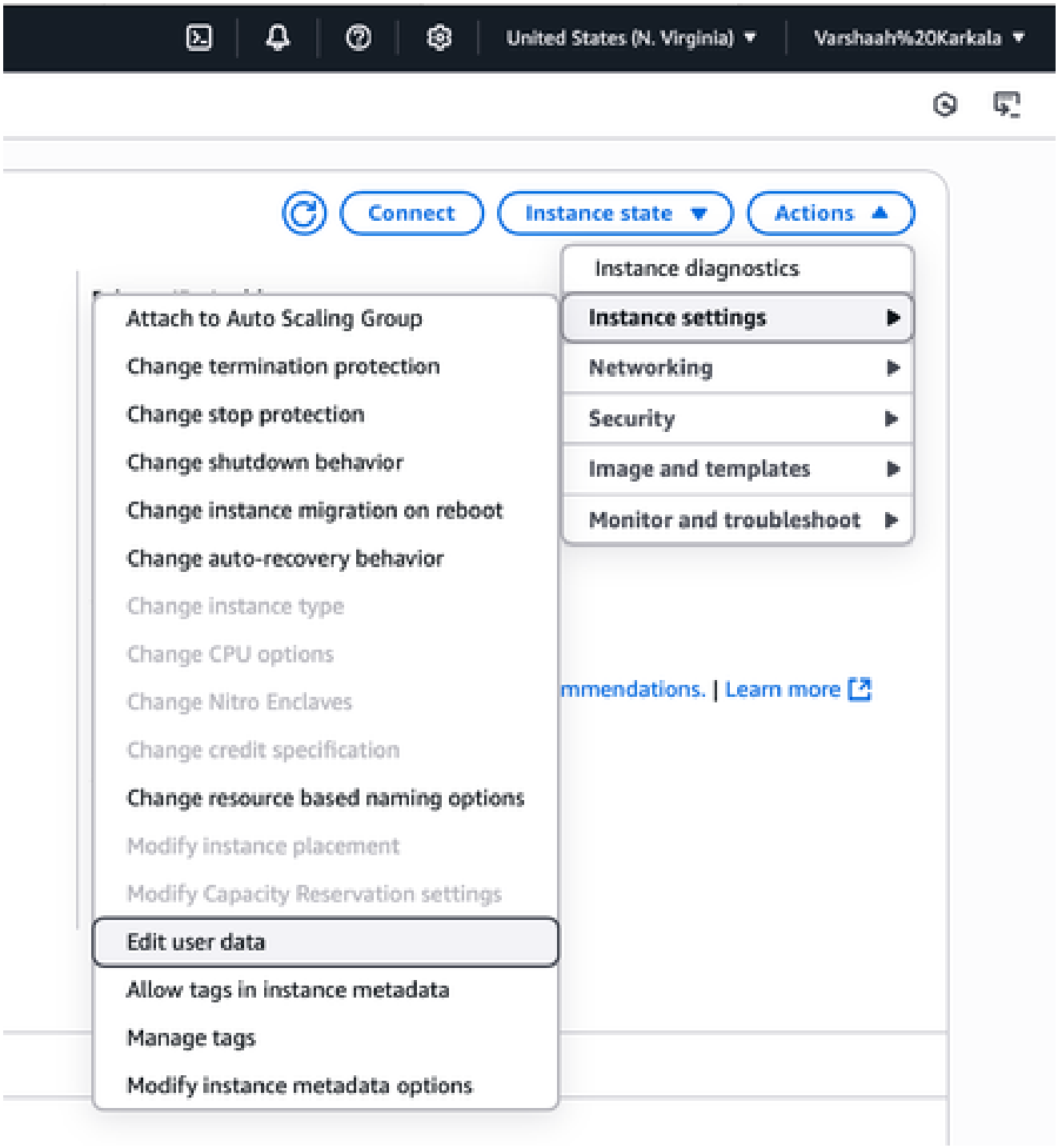
Nombre de usuario o contraseña no válidos

Los problemas de autenticación son causados a menudo por una entrada incorrecta del usuario durante la creación de la instancia. Esto produce un mensaje de error como "Nombre de usuario o Contraseña no válidos. Inténtelo de nuevo." error al intentar iniciar sesión en la GUI.

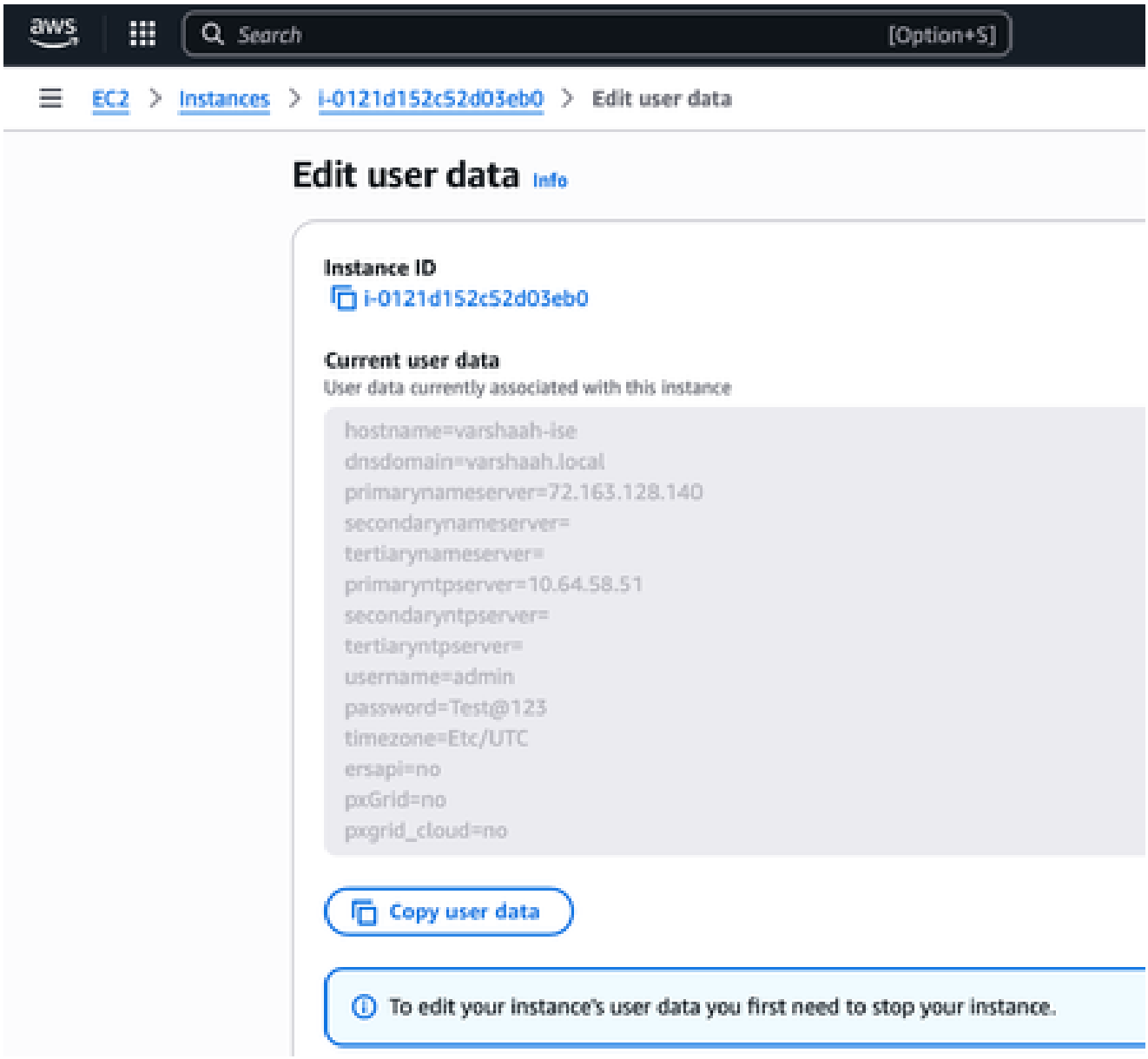


Solución

- En la Consola AWS EC2, navegue hasta EC2 > Instancias > your_instance_id
- Haga clic en Acciones > Configuración de instancia > Editar datos de usuario.



- Aquí puede encontrar el nombre de usuario y la contraseña específicos que se establecieron durante el inicio de la instancia. Estas credenciales se pueden utilizar para iniciar sesión en la GUI de ISE.



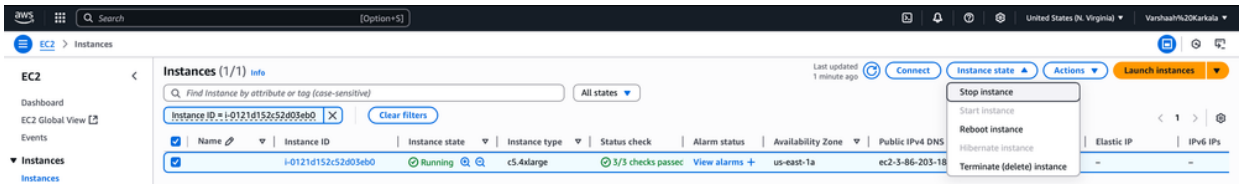
- Verifique el nombre de host y la contraseña al configurar el nombre de host y la contraseña:
  - Hostname
    - Sólo se permiten caracteres alfanuméricos y guiones (-).
    - No debe superar los 19 caracteres.
  - Contraseña
    - Debe cumplir con la política de contraseñas de Cisco ISE.
    - Consulte la Guía de administración oficial de ISE: Política de contraseñas de ISE 3.4: Guía para administradores de Cisco

- Si la contraseña configurada no cumple con la política de contraseñas de ISE, los intentos de inicio de sesión fallarán; incluso con las credenciales correctas.

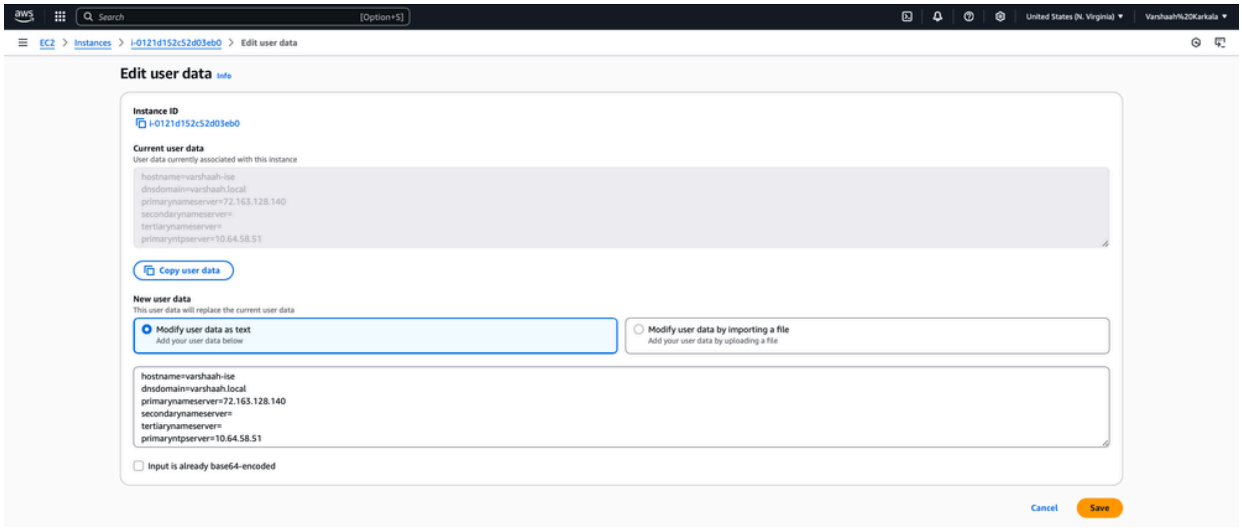
- Si sospecha que la contraseña está mal configurada, siga estos pasos para actualizarla:

    1. En la Consola EC2, vaya a EC2 > Instancias > your_instance_id

    2. Haga clic en Estado de instancia > Detener instancia.



    3. Una vez detenida la instancia, haga clic en Acciones > Configuración de la instancia > Editar datos de usuario.



    4. Modifique la secuencia de comandos de datos de usuario para actualizar la contraseña en consecuencia.

    5. Guarde los cambios y, a continuación, reinicie la instancia mediante Instance state > Start instance.

Defectos conocidos

ID de la falla	Descripción
ID de bug de Cisco 41693	ISE en AWS no puede recuperar los datos del usuario si la versión de metadatos está establecida en "V2 solamente". Solo se admite

	IMDSv1 en las versiones anteriores a ISE 3.4.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).