# Restablecer claves SSH para Cisco ISE en VM de Azure

## Contenido


Introducción

- Prerequisites
- Requirements
- Componentes Utilizados

Configurar

Verificación

Troubleshoot


## Introducción

Este documento describe cómo restablecer las claves SSH para las VM de Azure ISE.

### Prerequisites

- Conocimientos básicos de ISE
- Acceso a la consola de ISE a través de Microsoft Azure
- Acceso a la GUI de ISE
- Privilegios para crear nuevos pares de claves en Microsoft Azure

### Requirements

- nodo Cisco ISE

### Componentes Utilizados

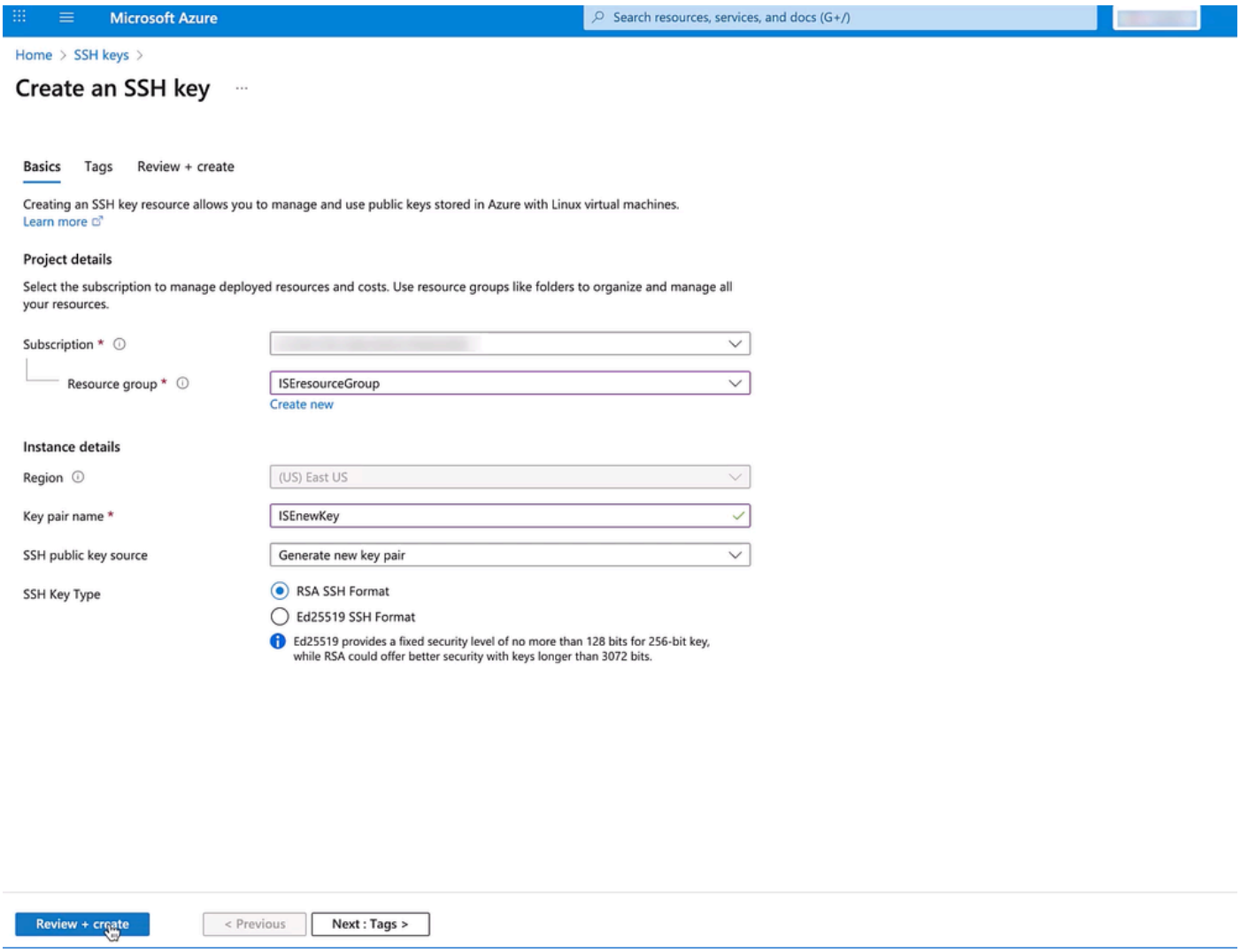
- Cisco ISE 3.3

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.

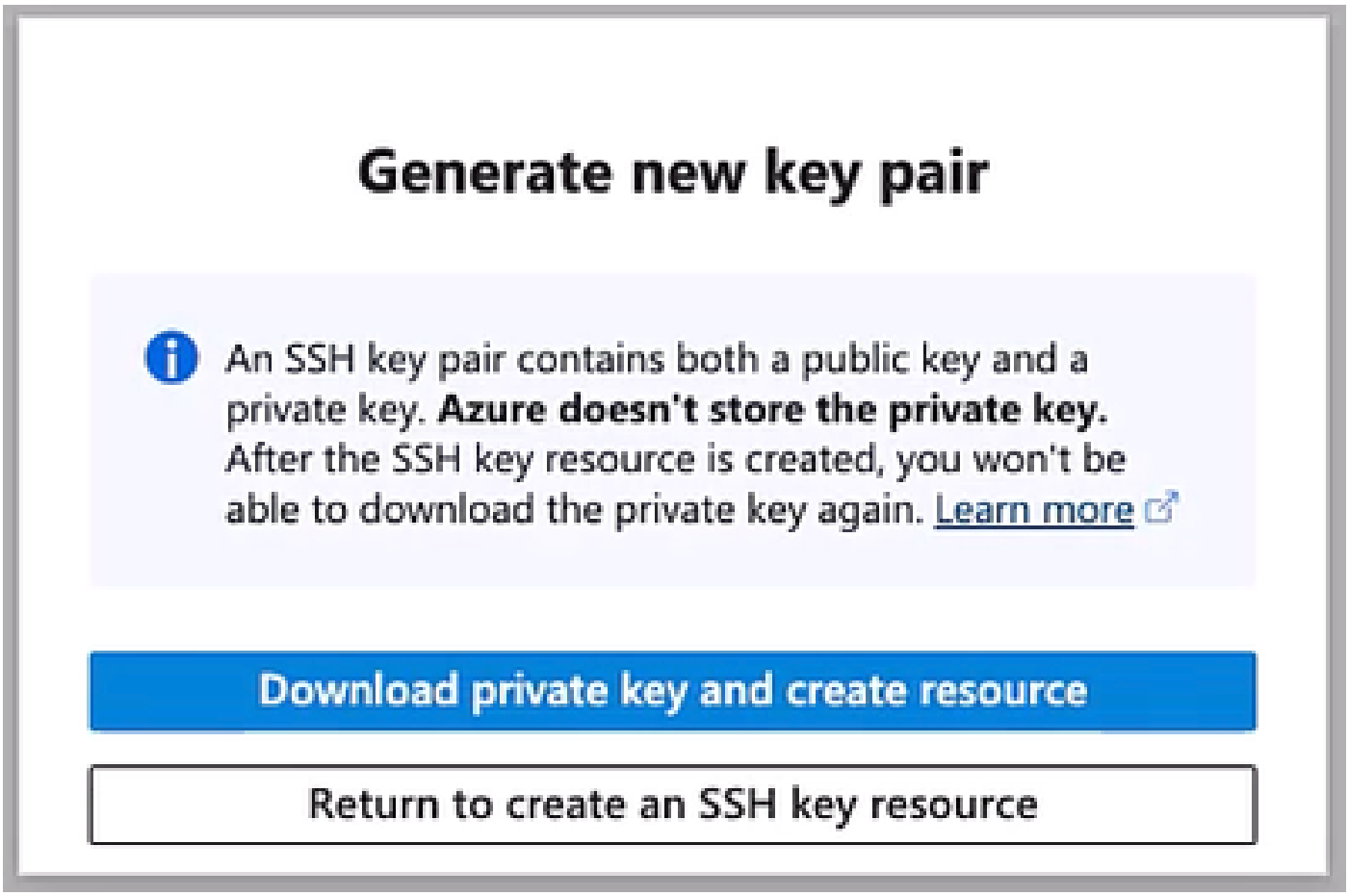
## Configurar

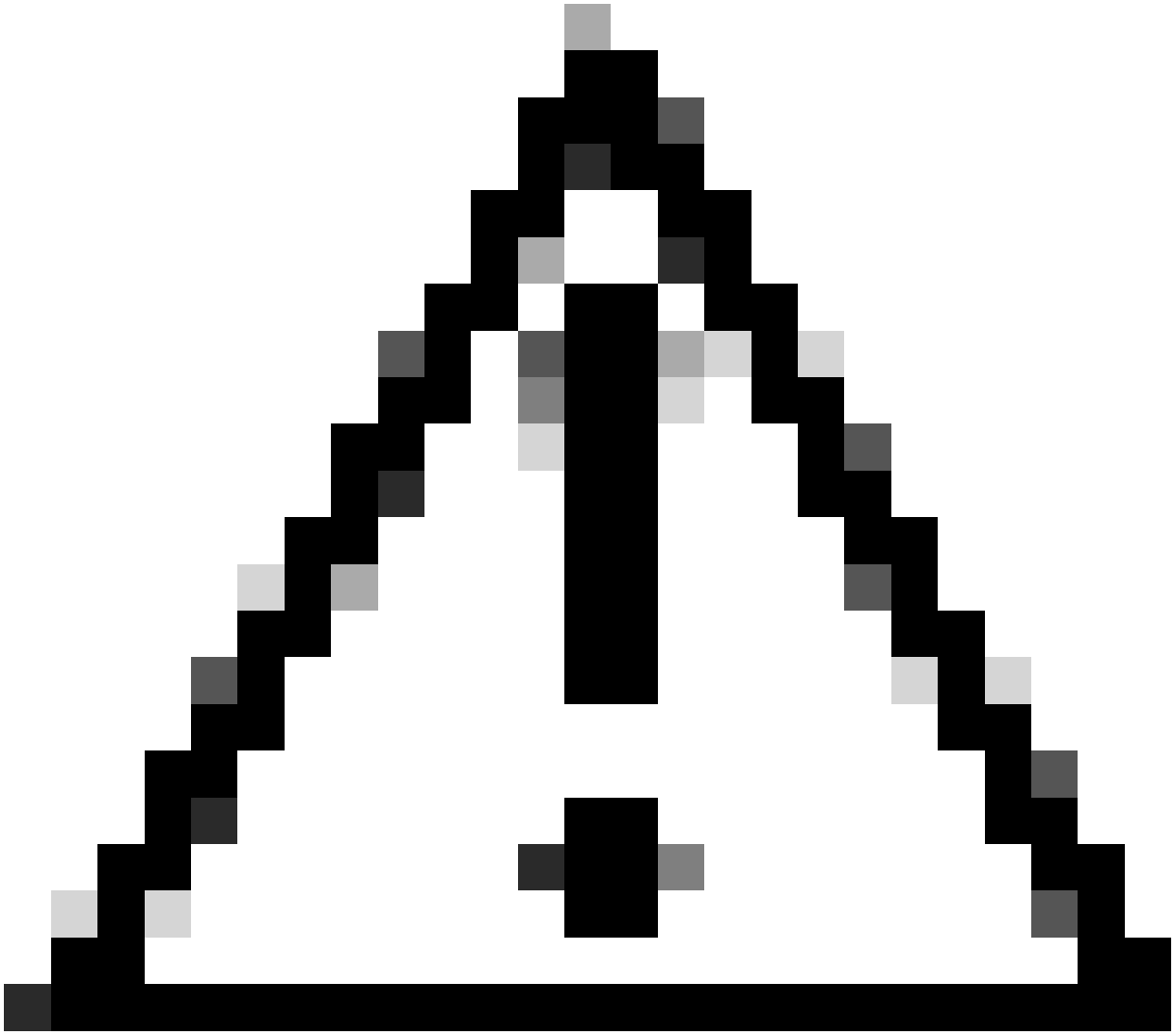
1. En Microsoft Azure, busque el servicio de claves SSH.

2. Haga clic en Create para crear una nueva clave SSH. Seleccione su suscripción y su grupo de recursos. Especifique un nombre personalizado para su nueva clave SSH. Para el campo de origen de clave pública SSH, seleccione la opción Generate new key pair y para SSH Key Type seleccione RSA SSH Format.  Por último, haga clic en Review + Create para validar y crear la clave.



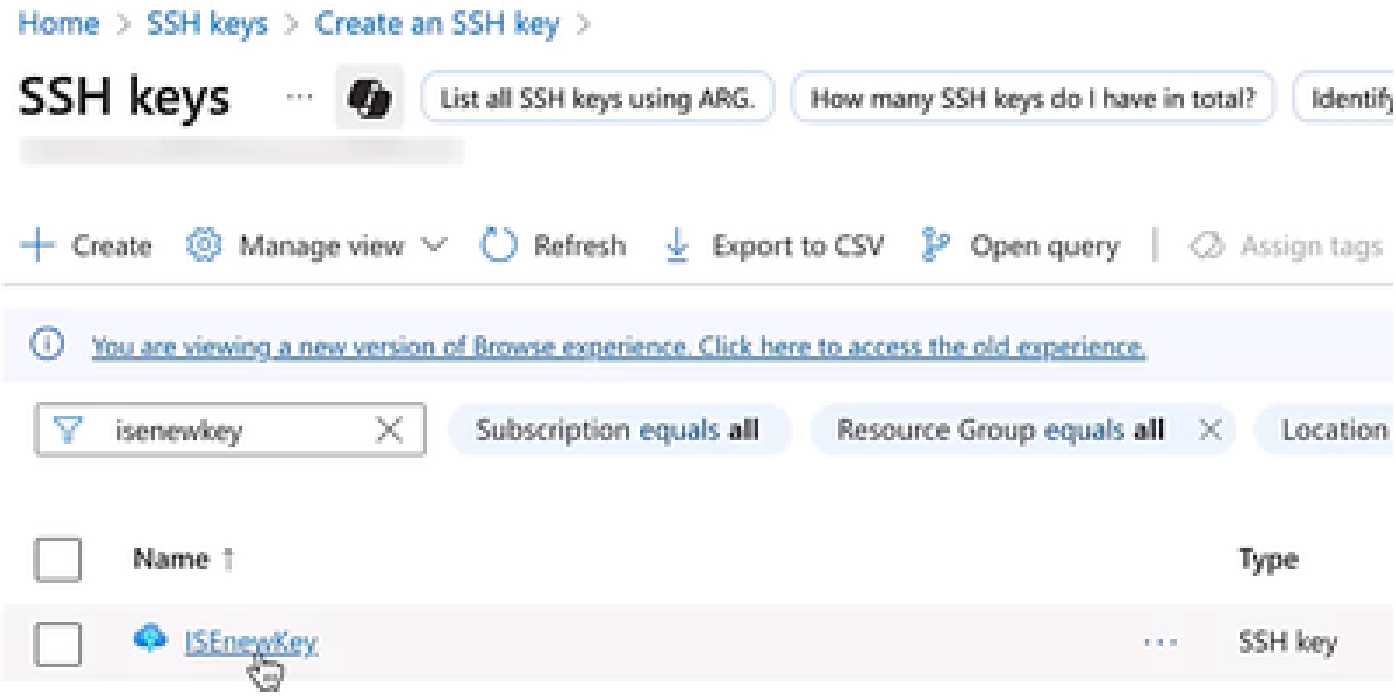
3. Cuando se crea la clave, aparece una nueva ventana. Haga clic en Descargar clave privada y crear recurso.



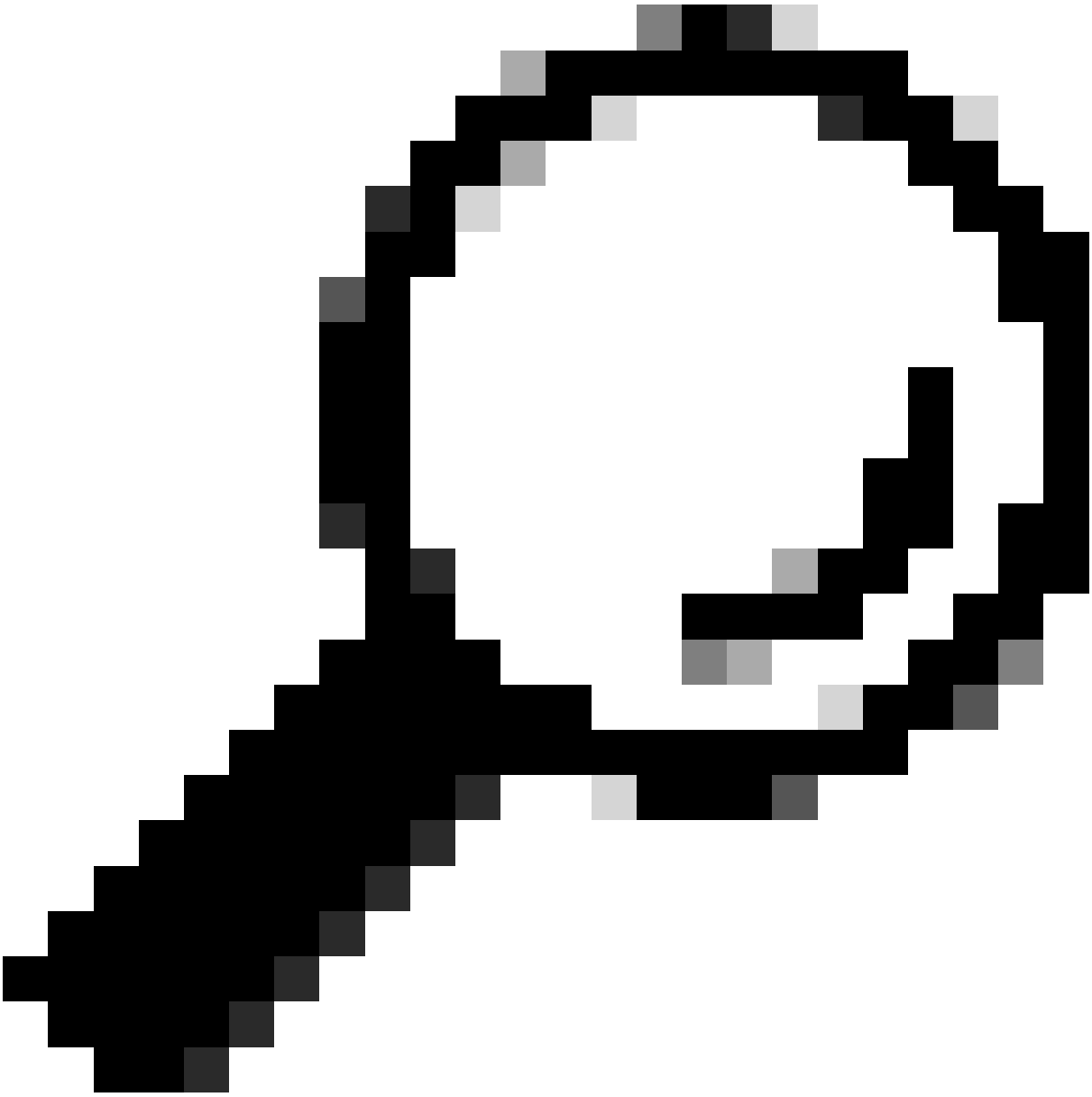


Precaución: Es importante mantener esta clave privada de forma segura, ya que es el único momento en el que Azure le permite descargar esta clave privada. Azure no almacena esta clave privada y no se puede descargar desde ningún otro lugar.

4. Ahora, navegue de nuevo al servicio SSH Keys y busque su clave recién creada y haga clic en ella para ver su descripción general.



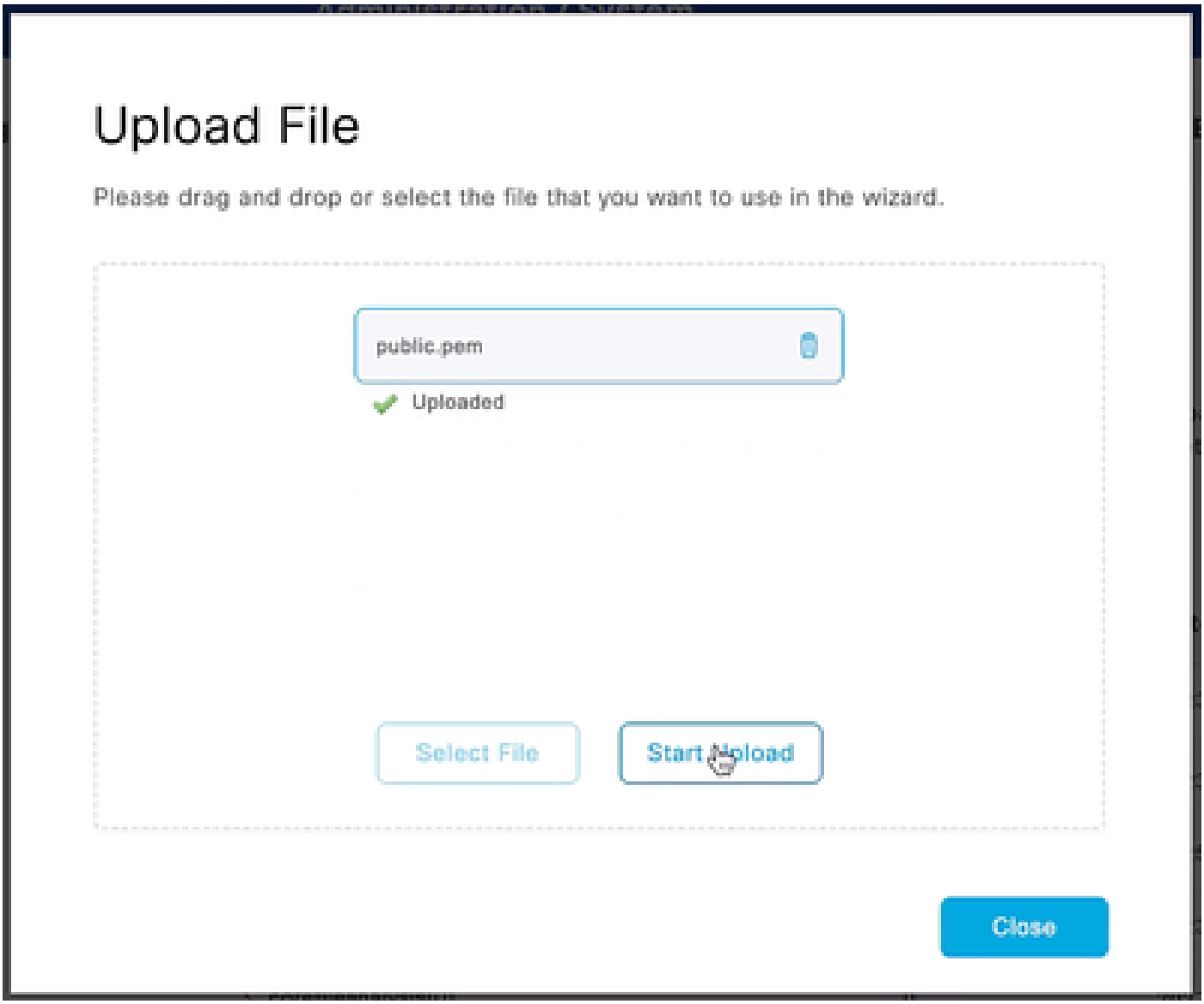

5. En la introducción de la clave, verá la clave pública. Copie este texto y péguelo en un editor de texto para poder guardarlo como un archivo local con la extensión .pem. En esta guía, el archivo se guarda como public.pem .



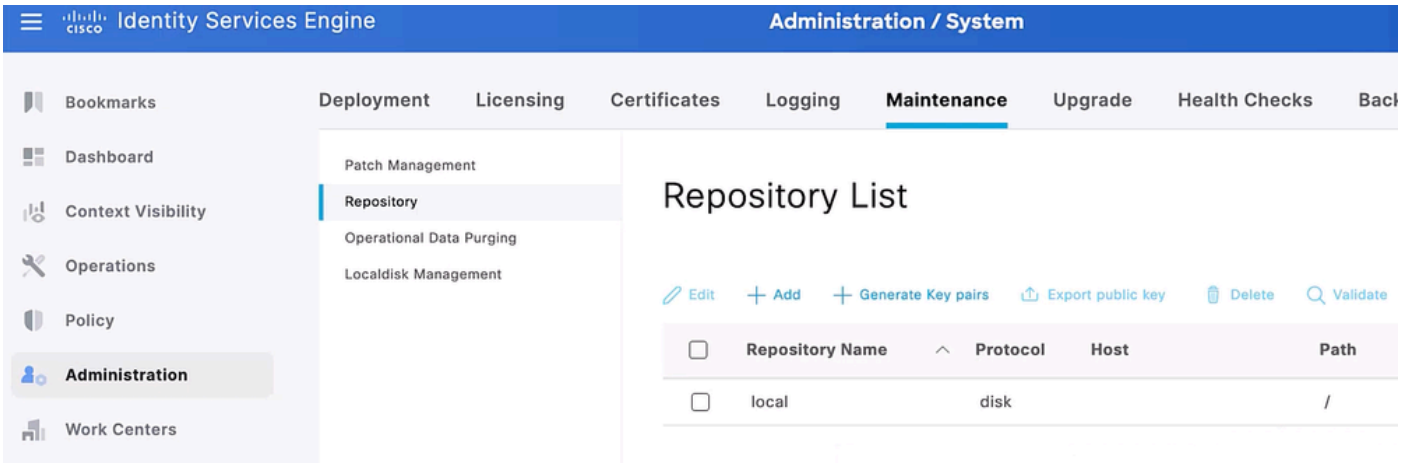
Consejo: Puede hacer clic en el botón Copiar al portapapeles para copiar la cadena de clave pública.

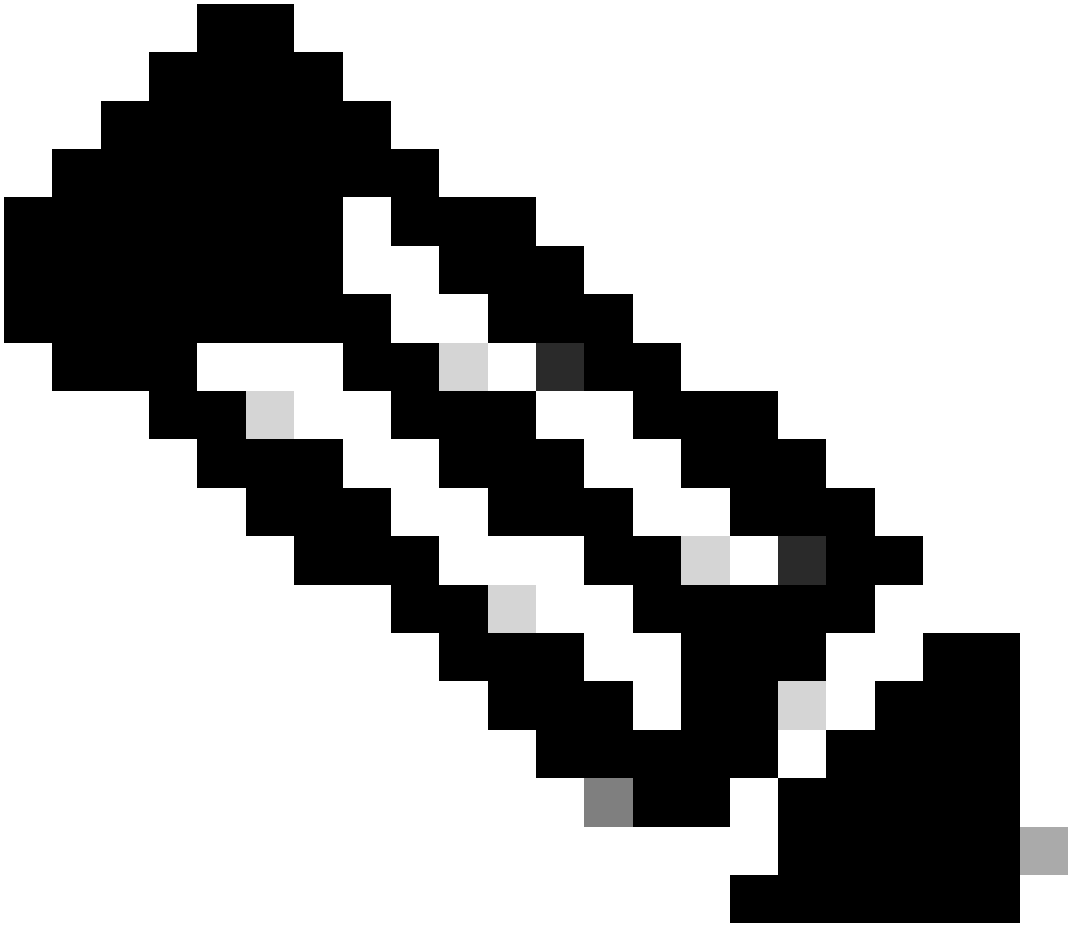
6. Cargue esta clave pública en el disco local de ISE. Para hacerlo, navegue hasta ISE > Administration > System > Maintenance > Local Disk Management. Haga clic en su nombre de host de ISE, haga clic en Cargar y, a continuación, haga clic en Seleccionar archivo y

localice y seleccione la clave pública en su equipo local. Por último, haga clic en Iniciar carga .




7. Cree un repositorio que apunte al disco local de ISE para poder utilizarlo para instalar la clave pública; en este ejemplo, nuestro repositorio se denomina local.

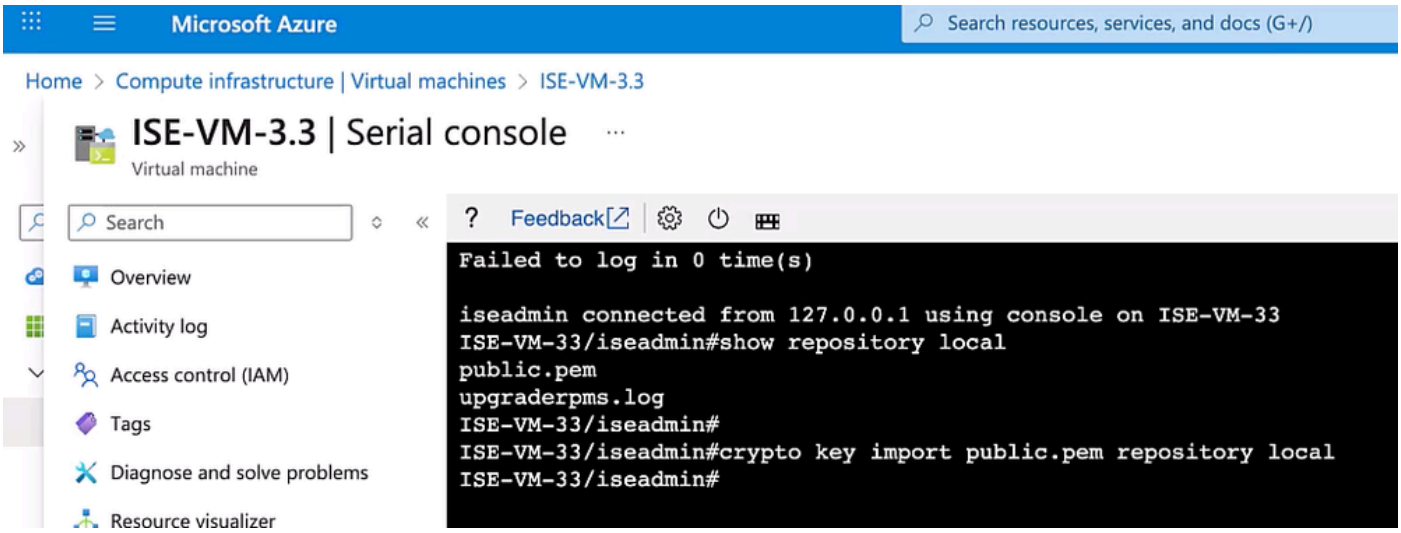




Nota: Si desea poder cargar el archivo de clave pública en un repositorio diferente que ya se haya creado en ISE, no es necesario que sea un disco local.

8. Inicie sesión en ISE Serial Console desde Azure con el nombre de usuario para el que desea restablecer la clave SSH.

9. Compruebe que la clave pública (archivo .pem) está ubicada correctamente en el repositorio e instale la clave con el comando crypto key import { name of the public key file } repository { name of the repository }.




# Verificación

Para conectarse a ISE mediante SSH con los nuevos pares de claves, debe utilizar la clave privada como identificación al iniciar sesión.

1. Asigne los permisos adecuados a la clave privada (la descargada en el paso 3)

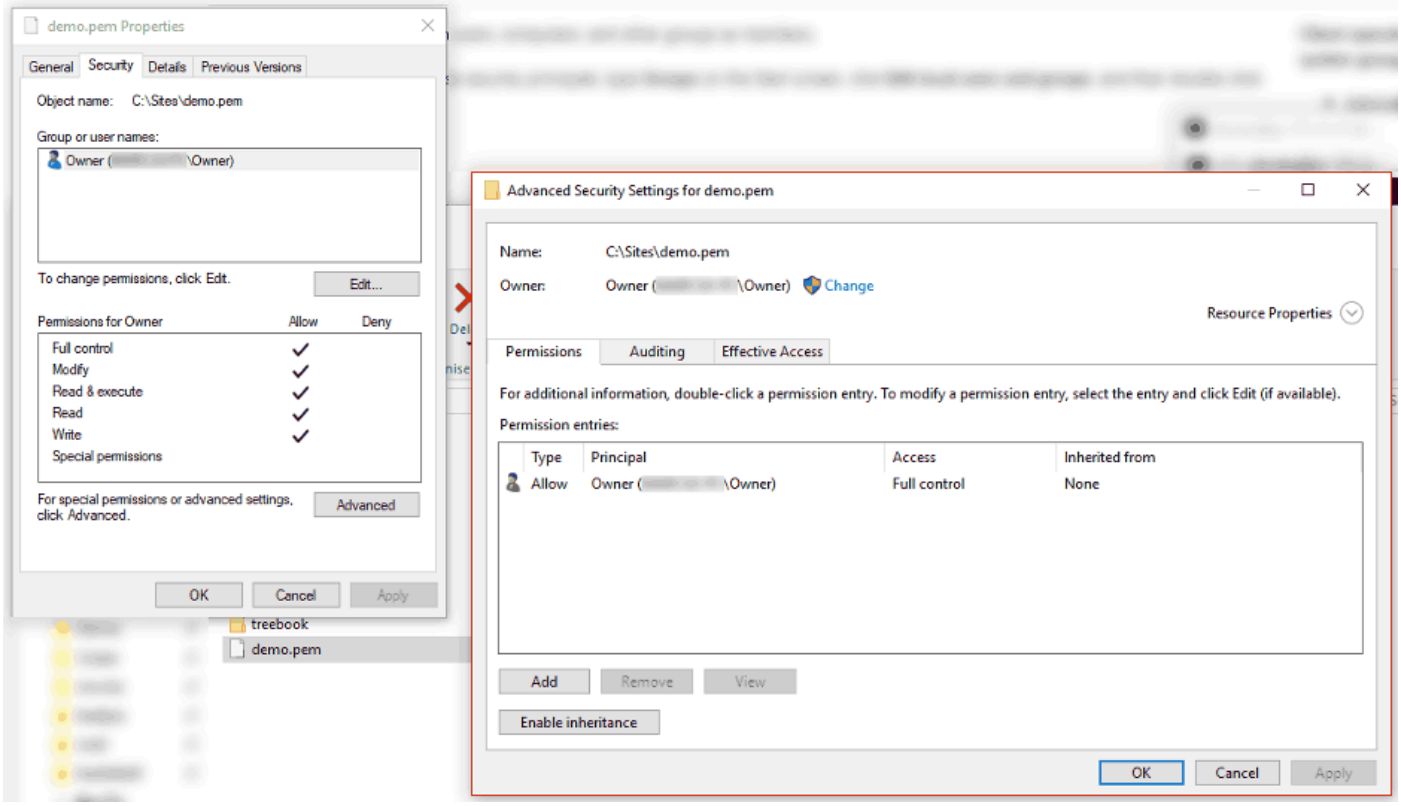
Desde el terminal macOS:

chmod 600 { private key file }

Desde Windows:

Localice el archivo en el Explorador de Windows, haga clic con el botón derecho en él y seleccione Propiedades. Vaya a la pestaña Seguridad y haga clic en Avanzada.

Cambie el propietario, deshabilite la herencia y elimine todos los permisos. A continuación, concédase el control total y guarde los permisos.




2. SSH a ISE mediante la nueva clave privada, el nombre de usuario de ISE y la dirección IP o FQDN de ISE.

Desde el terminal macOS:

ssh -I { private key file } { username }@{ ISE IP o FQDN }

Desde CMD de Windows:

ssh -i "{ private key file }" { username }@{ ISE IP o FQDN }

# Troubleshoot

- Asegúrese de copiar el texto completo del archivo de clave pública en el archivo .pem.
- Asegúrese de que el repositorio contiene el archivo de clave pública.
- Si el comando crypto no puede instalar la clave pública en ISE, genere un ticket con el TAC de Cisco para que la clave se pueda instalar manualmente desde la raíz. El error común para esta operación es "% Error: No se puede actualizar el archivo de clave autorizada."

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).