Configurar y solucionar problemas del repositorio de Azure SFTP Blob Storage en ISE

Contenido

Introducción

Este documento describe cómo configurar Azure Blob Storage como servidor SFTP con autenticación de Infraestructura de clave pública con Identity Services Engine.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento general de ISE
- Configuración del repositorio de ISE
- Autenticación mediante infraestructura de clave pública (PKI)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- ISE 3.3, 3.4, 3.5 VM en Azure
- Suscripción de Azure para acceder a Storage Center

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.

Antecedentes

Como servicio nativo de la nube, el repositorio SFTP de Azure Blob Storage es fácil de implementar e ideal para implementaciones de ISE basadas en Azure. Elimina los problemas de conectividad en las instalaciones, se amplía automáticamente para satisfacer las demandas de almacenamiento fluctuantes y garantiza una alta disponibilidad y durabilidad para grandes conjuntos de datos, al tiempo que elimina la necesidad de una gestión manual de la infraestructura.

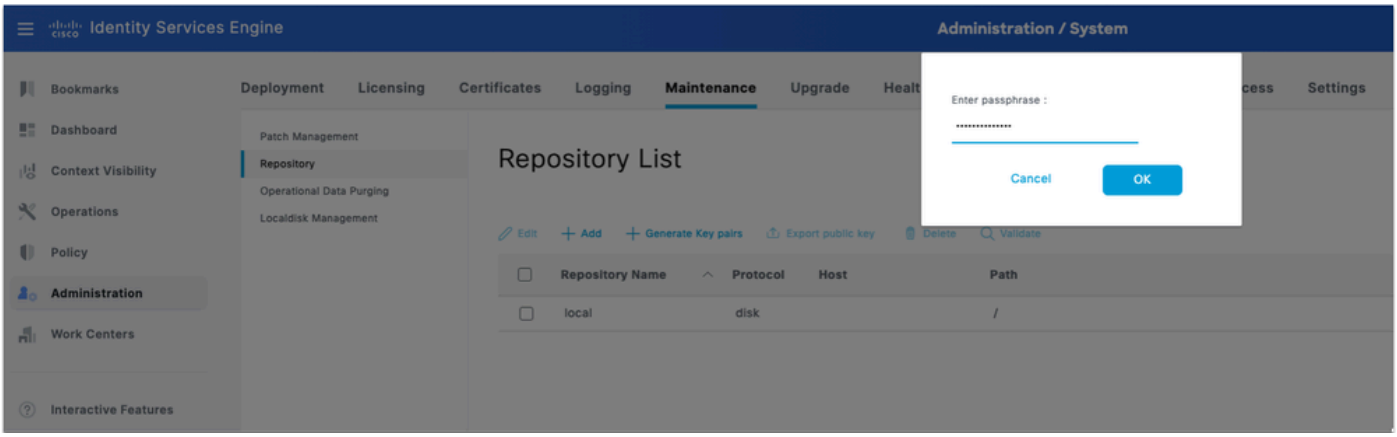
Configurar

Preconfiguración de ISE

1. Generar pares de claves en ISE: Inicie sesión en la GUI del nodo de administración principal. Vaya a Administration > System > Maintenance > Repository.

2. En Lista de repositorios, haga clic en la opción Generar pares de claves.

3. Introduzca la frase de paso (más de 13 caracteres) y haga clic en Aceptar. Esto es necesario para proteger el par de claves.



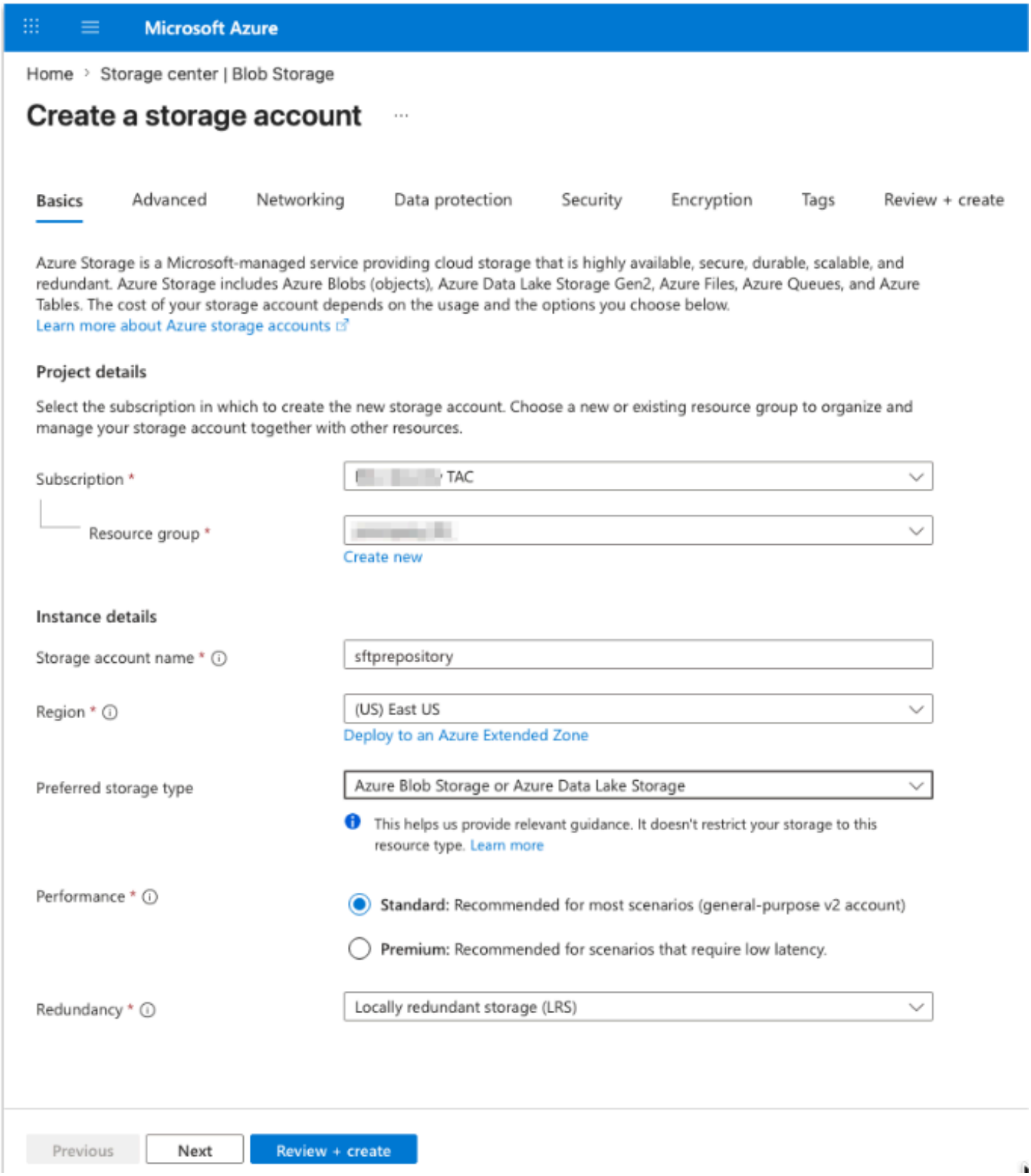
Generar par de claves en ISE

4. Haga clic en Exportar clave pública y descargue la clave id_rsa.pub en su computadora (asegúrese de guardar esto para futuras referencias).

configuración de Azure SFTP

1. Crear y configurar la cuenta de almacenamiento de Azure: Inicie sesión en el Portal de Azure y navegue hasta Cuentas de almacenamiento. En la pestaña Resources, haga clic en Create para crear una nueva cuenta de almacenamiento. Rellene los detalles:

Campo	Valor
Suscripción	Su suscripción a Azure
Grupo de recursos	Seleccionar existente o crear nuevo
Nombre de cuenta de almacenamiento	Debe ser único globalmente
Región	Seleccione su región preferida
Redundancia	Almacenamiento redundante local (LRS): aceptable para entornos de laboratorio/no producción

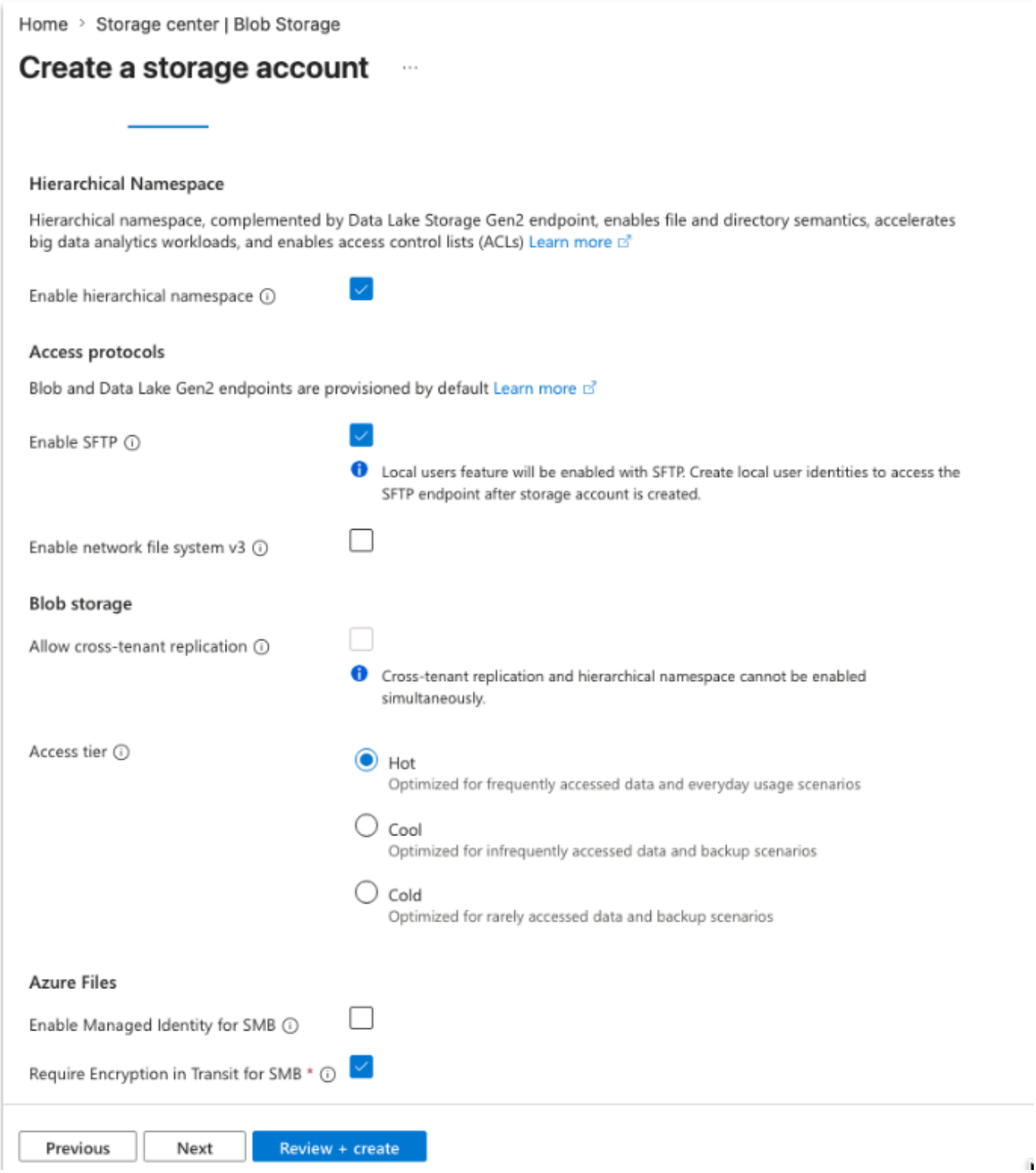


Crear una cuenta de almacenamiento

2. Haga clic en Siguiente y en la pestaña Avanzado, seleccione la casilla de control Activar Espacio de Nombres Jerárquico. Esta opción es obligatoria. SFTP solo se puede habilitar para cuentas de espacio de nombres jerárquico.

3. Active la casilla de verificación Activar SFTP.

4. Deje el resto de las opciones como predeterminado o ajuste según sus requisitos.



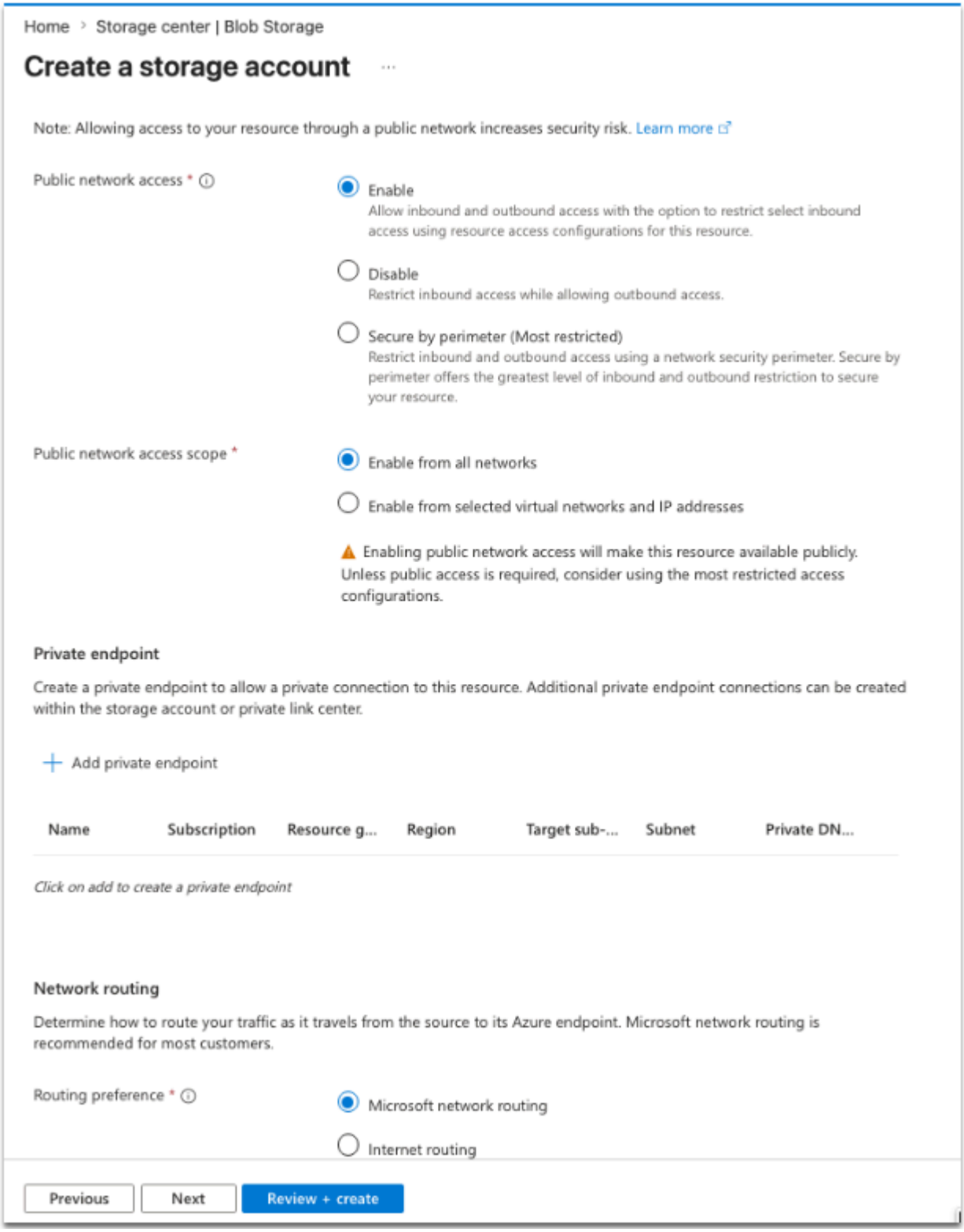
Configurar cuenta de almacenamiento

5. Haga clic en Next para configurar Networking.

6. Establezca Acceso a la red en Habilitar acceso público desde todas las redes.

7. Establezca Routing preference en Microsoft network routing.

Nota: Nota: En entornos de producción, considere la posibilidad de restringir el acceso a intervalos IP específicos (las direcciones IP de los nodos ISE) mediante reglas de firewall en la cuenta de almacenamiento.



8. Haga clic en Next y deje Data protection, Security y Encryption como opción predeterminada. No se requiere ninguna configuración adicional para implementaciones estándar o de laboratorio.

9. Haga clic en Revisar + crear. Una vez superada la validación, haga clic en Create.

10. Espere a que finalice la implementación y, a continuación, haga clic en Ir al recurso.

11. Configure SFTP en la cuenta de almacenamiento de Azure: En la cuenta de almacenamiento recién creada, agregue un contenedor navegando hasta Almacenamiento de datos > Contenedores > Agregar contenedor

12. Proporcione un nombre de contenedor. Haga clic en Crear.

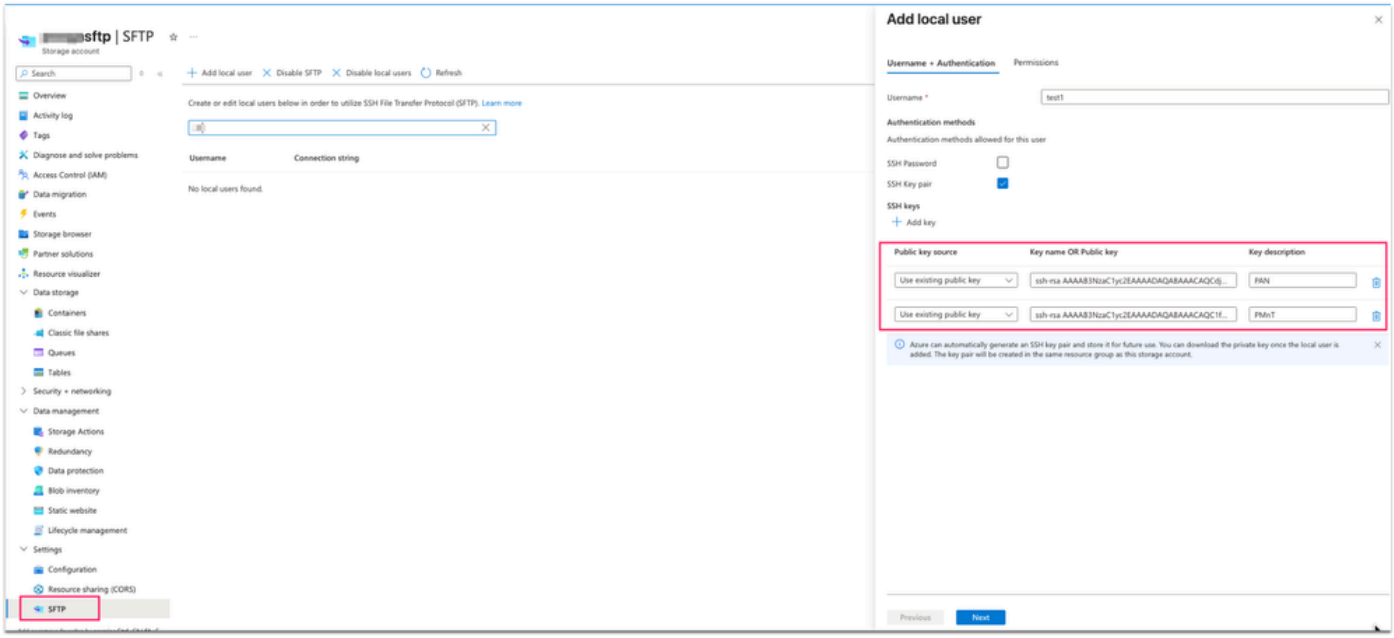
13. Agregue el usuario sftp navegando hasta Settings > SFTP en el menú de la izquierda. Haga clic en Add local user y configure lo siguiente:

Campo	Valor
Nombre de usuario	Un nombre descriptivo
Método de autentificación	Par de claves SSH: NO utilice la contraseña
fuente de clave pública SSH	Utilizar clave existente (generada en el paso 1, la clave id_rsa.pub)

Nota: En una implementación de varios nodos, cuando el PAN principal y el MnT principal son nodos independientes, el archivo id_rsa.pub tiene claves públicas RSA de los nodos PAN principales y del MnT principal.

14. Para utilizar la clave pública existente bajo la opción de claves SSH, abra el archivo id_rsa.pub en un editor de texto de su elección y copie y pegue ambas claves de nodos (empezando con ssh-rsa y terminando con root@your_node_name) por separado haciendo clic en la opción Add key dos veces.

```
Sample key: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCdjUFU6QaMQfxuR/yzbw1QWZ8EwUJjN/C0cNNMlkMOQE9flJQ6GoC
```



Agregando una clave pública en Azure

15. Haga clic en Permisos. Seleccione el contenedor creado inicialmente en este paso y establezca los permisos del contenedor en Lectura, Escritura, Lista, Eliminar y Crear.

16. Establezca el directorio principal en la raíz del contenedor.

17. Guarde el usuario.

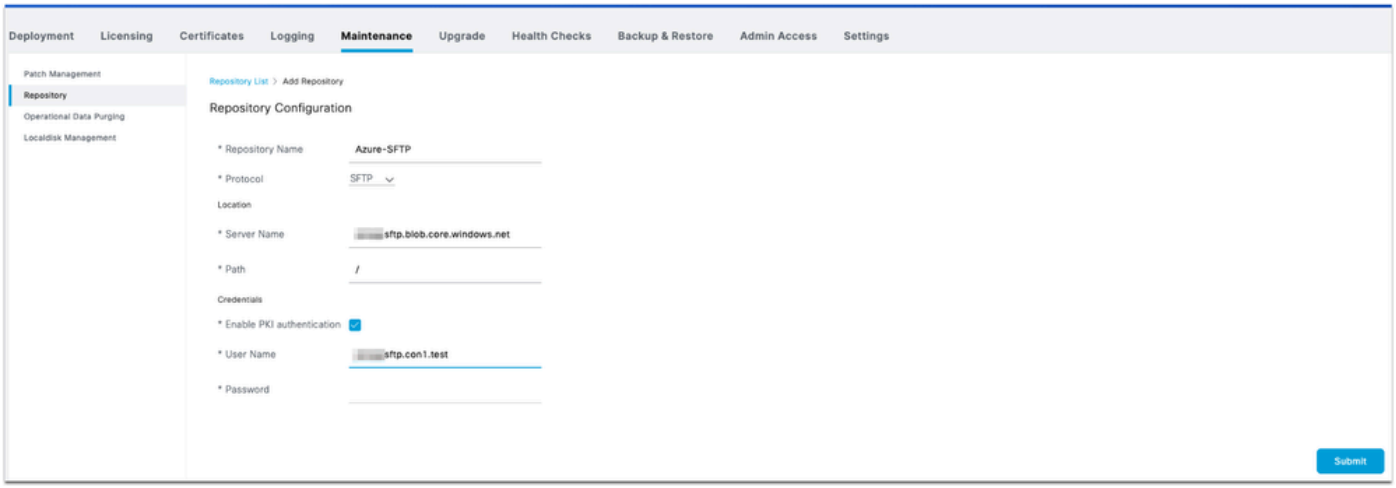
Configuración del repositorio GUI de ISE

1. Vaya a Administración > Sistema > Mantenimiento > Repositorio y haga clic en Agregar. Rellene los campos de la siguiente manera:

Campo	Valor
Nombre del repositorio	Una etiqueta descriptiva (como Azure-SFTP)
Protocolo	SFTP
Nombre del servidor	<storage_account_name>.blob.core.windows.net

Trayecto:	/ (directorio raíz)
Autenticación	PKI
User Name	<storage_account_name>.<container_name>.<sftp_local_username>
Contraseña	Dejar en blanco

2. Haga clic en Enviar para guardar el repositorio.



Configuración del repositorio ISE SFTP

Advertencia: La clave de host del servidor sftp debe agregarse a través de CLI mediante el comando crypto host_key add ejecutable para poder utilizar este repositorio. Asegúrese también de que la cadena de la clave de host coincida con el nombre de host utilizado en la URL de la configuración del repositorio. Para acceder al repositorio habilitado para PKI, genere pares de claves desde la GUI y exporte la clave pública a su máquina local. Copie esta clave pública en el servidor SFTP con PKI activada y agréguela al archivo 'authorized_keys'.

---

3. Inicie sesión en el nodo de administración principal y en el nodo de supervisión principal y agregue la clave de host crypto mediante el comando crypto host_key y host <sftp server>. Asegúrese de que el nodo ISE pueda resolver el nombre de host sftp.

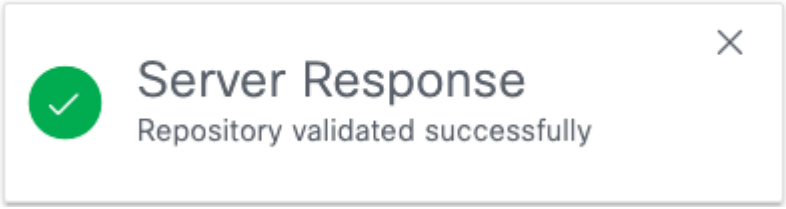
<#root>

```
isenode1/iseadmin#
```

```
crypto host_key add host xxxxxsftp.blob.core.windows.net
```

```
host key fingerprint added
# Host xxxxxsftp.blob.core.windows.net found: line 1
xxxxxsftp.blob.core.windows.net RSA SHA256:sP18dIvbSZgtEa5a2ea+Fy4P54Wd2ocEkToBq6xG74g
```

4. Vuelva a la GUI de ISE en Repositorio, seleccione el repositorio recién creado y haga clic en Validar. Repositorio validado correctamente.



Validación de repositorio satisfactoria

Nota: La opción de validación del repositorio valida la configuración del repositorio sólo en el nodo de administración principal.

Nota: En el caso de un repositorio SFTP creado con una clave pública RSA, los repositorios creados a través de la GUI no se replican en la CLI y los repositorios creados a través de la CLI no se replican en la GUI. Para configurar el mismo repositorio en CLI y GUI, genere claves públicas RSA en CLI y GUI y exporte ambas claves al servidor SFTP.

Configuración del repositorio de ISE CLI

1. SSH en la CLI (interfaz de línea de comandos) del nodo de administración principal. Agregue la clave criptográfica en cada nodo de la implementación en el que desee acceder al repositorio SFTP basado en PKI desde CLI.

2. Genere la clave pública rsa para CLI.

```
isenode1/iseadmin#crypto key generate rsa passphrase <passphrase>
```

3. Exporte el archivo de clave pública generado al repositorio de disco local (cualquier repositorio al que tenga acceso para descargar el archivo).

```
isenode1/iseadmin#crypto key export <give a name for this file> repository <repository name>
```

4. Descargue este archivo del repositorio y ábralo en el editor de texto para copiar la clave pública para el acceso CLI.

5. Cargue la clave pública SSH en Azure, igual que la clave GUI agregada en la pantalla de creación de usuario local de Azure SFTP (desde el paso 3).

6. Haga clic en Agregar clave y Pegue la clave pública SSH completa (en el campo SSH public key).

7. Opcionalmente, proporcione una descripción clave (por ejemplo, ISE-CLI-Key).

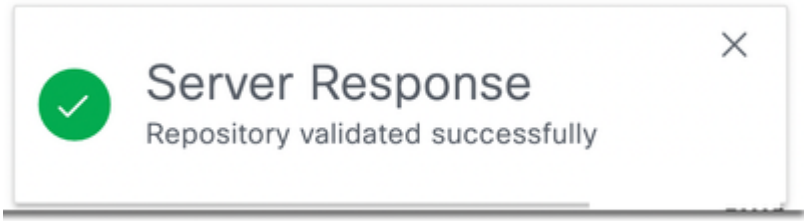
8. Haga clic en Next y en Save.

Verificación

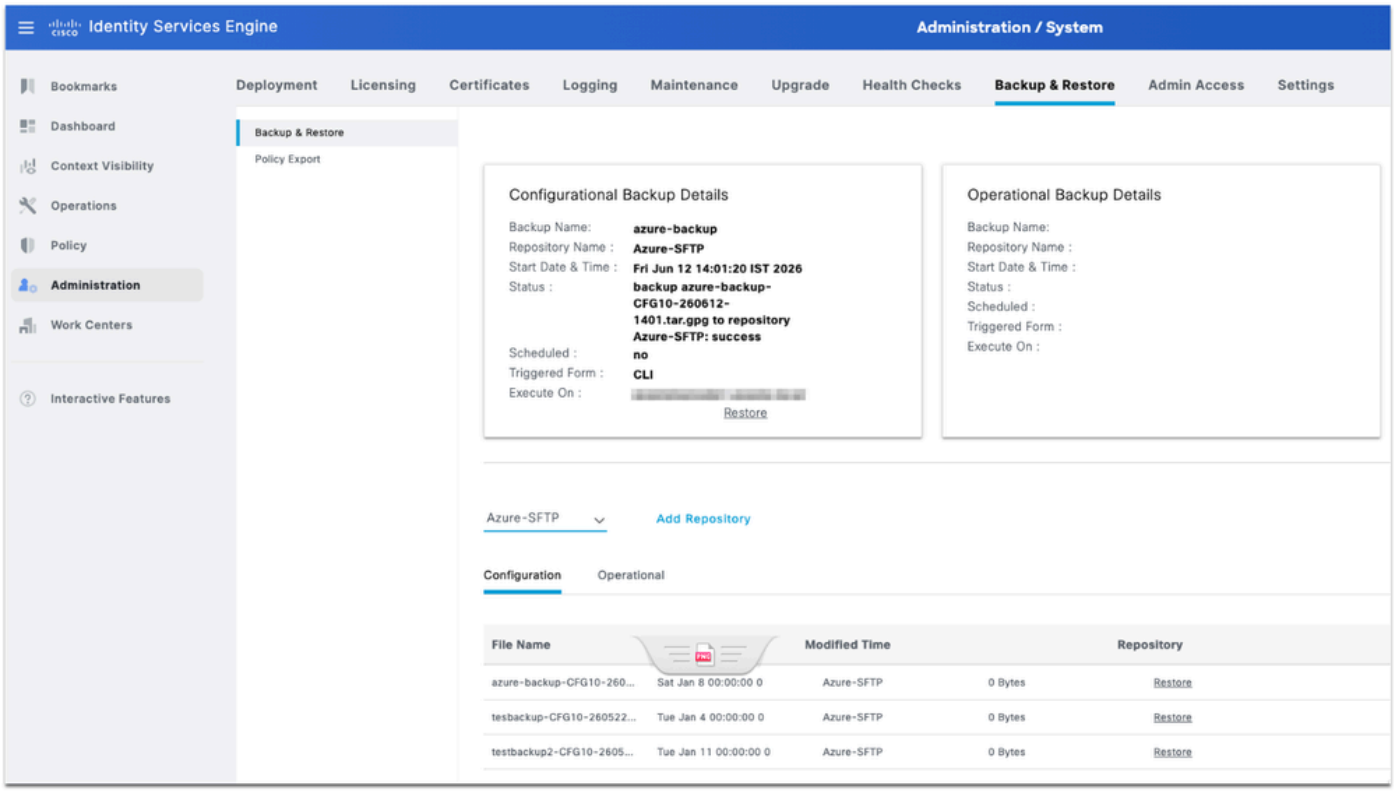
1. Verifique el acceso CLI al repositorio sftp mediante el comando "show repository <Nombre del repositorio>". Muestra los archivos almacenados en este servidor sftp.

```
isenode1/iseadmin#show repository Azure-SFTP
SB-pk-260522-2236.tar.gpg
ops-OPS10-260525-1026.tar.gpg
```

2. Verifique el acceso GUI al repositorio sftp navegando hasta Repositorio y Seleccione el repositorio recién creado y haga clic en Validar. Repositorio validado correctamente.



3. Navegue hasta Administración > Sistema > Copia de Seguridad y Restauración . Realice una copia de seguridad de la configuración y, a continuación, vaya a la parte inferior de esta página, seleccione el repositorio SFTP y, en Configuración, la copia de seguridad reciente estará visible para restaurar.

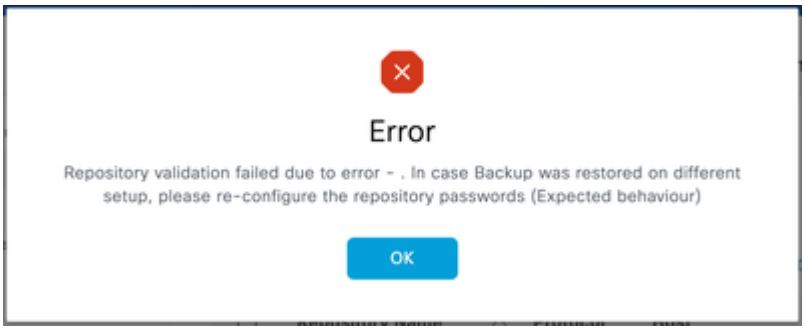


validación del repositorio sftp

Nota: Debido al error cosmético de Cisco IDCSCwu6863, el tamaño de las copias de seguridad en el almacenamiento de Azure se ve aquí como 0 bytes pero no hay impacto funcional. Estas copias de seguridad se pueden restaurar correctamente si es necesario.

Troubleshoot

1. En la GUI de ISE, la validación del repositorio genera este error:



Mensaje de error

Resolución

Compruebe que la clave pública derecha se importa en el servidor SFTP bajo claves SSH (consulte el paso 2 de Configurar SFTP en la cuenta de almacenamiento de Azure). Este error ocurre si el usuario ha generado un nuevo par de claves nuevamente en la GUI después de la validación exitosa del repositorio.

2. Validación de repositorio GUI exitosa pero sin salida del comando show repository <sftp repository>.

Captura de pantalla de error

Resolución

Compruebe que la clave pública RSA generada desde CLI se agrega en la configuración de Azure SSH.

3. Para resolver el problema del repositorio SFTP, habilite el comando debug:

```
isenode1/iseadmin#debug transfer 7
```

```
isenode1/iseadmin#debug transfer 7
isenode1/iseadmin#show repository Azure-SFTP
6 [395485]:[info] transfer: cars_xfer.c[333] [system]: sftp dir of repository Azure-SFTP requested
6 [395485]:[info] transfer: cars_xfer_util.c[2755] [system]: Server validation successful .core.windows.net
7 [395485]:[debug] transfer: sftp_handler.c[1281] [system]: Running sftp command: .blob.core.windows.net *** / ls -l /
6 [395485]:[info] transfer: sftp_handler.c[689] [system]: DEBUG: local user: iseadmin UID: 0 sftp_run_parent FD: 7 remote host: .blob.core.windows
.net remote user: command: ls -l /
7 [395485]:[debug] transfer: sftp_handler.c[699] [system]: fd is:7
7 [395486]:[debug] transfer: sftp_handler.c[327] [system]: Executing SFTP command: 0 iseadmin /usr/bin/sftp -oIdentityFile=/home/iseadmin/.ssh/id_rsa -oUse
rKnownHostsFile=/home/iseadmin/.ssh/known_hosts -oPasswordAuthentication=no .blob.core.windows.net
3 [395485]:[error] transfer: sftp_handler.c[445] [system]: sftp_read Error: read failed
3 [395485]:[error] transfer: sftp_handler.c[914] [system]: sftp_run_parent Error: read(command prompt) failed
7 [395485]:[debug] transfer: sftp_handler.c[1123] [system]: sftp parent status -306
% SSH connect error
```

Registros de depuración

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).