

Error de tiempo de espera de autenticación de clave RSA SFTP ISE

Contenido

Problema

Un repositorio SFTP configurado con autenticación de clave RSA funciona correctamente en un nodo ISE (ise1), pero falla en otro nodo ISE (ise2) que ejecuta ISE 3.4. En el nodo que falla, el protocolo de enlace SSH y la validación del servidor finalizan correctamente, pero la autenticación de clave pública no finaliza y la sesión SFTP agota el tiempo de espera con un error "sftp_select: tiempo de espera!" .

Al intentar enumerar el contenido del repositorio SFTP mediante el comando show repository SFTP en el nodo ISE afectado, se produce esta secuencia de error:

```
device/admin# show repository SFTP
6 [4005534]:[info] transfer: cars_xfer.c[333] [system]: sftp dir of repository SFTP requested
6 [4005534]:[info] transfer: cars_xfer_util.c[2654] [system]: Server validation successful 10.50.60.200
7 [4005534]:[debug] transfer: sftp_handler.c[1295] [system]: Running sftp command: 10.50.60.200 will.ki
6 [4005534]:[info] transfer: sftp_handler.c[695] [system]: DEBUG: local user: admin UID: 0 sftp_run_par
7 [4005534]:[debug] transfer: sftp_handler.c[705] [system]: fd is:7
7 [4005535]:[debug] transfer: sftp_handler.c[327] [system]: Executing SFTP command: 0 admin /usr/bin/sf
3 [4005534]:[error] transfer: sftp_handler.c[417] [system]: sftp_select Error: timeout!
7 [4005534]:[debug] transfer: sftp_handler.c[1136] [system]: sftp parent status -999
% Failure occurred during request
```

Esto impide el uso del repositorio SFTP del nodo ISE afectado para funciones críticas de ISE, como las operaciones de copia de seguridad.

Entorno

- Cisco Identity Services Engine (ISE) versión 3.4.0
- Implementación de ISE de varios nodos con al menos dos nodos (ise1 e ise2)

- Repositorio SFTP configurado con autenticación de clave RSA
- Autenticación basada en claves SSH mediante clave privada RSA (/home/admin/.ssh/id_rsa)
- Servidor SFTP accesible
- Autenticación de contraseña desactivada (-oPasswordAuthentication=no)

Resolución

Este caso está siendo investigado por el equipo de ingeniería. Se ha derivado el problema para que el análisis del registro raíz determine la causa subyacente del tiempo de espera de SFTP en el nodo ISE afectado.

Según el resultado de la depuración, siga los pasos de solución de problemas descritos en las siguientes secciones para recopilar información adicional.

Paso 1: Verificar la coherencia de la configuración del repositorio SFTP entre nodos

Compare la configuración del repositorio SFTP en ambos nodos ISE para asegurarse de que son idénticos.

Paso 2: Comprobar los permisos y la propiedad del archivo de clave SSH

Verifique que el archivo de clave privada SSH (/home/admin/.ssh/id_rsa) tenga los permisos y la propiedad correctos en el nodo afectado.

Paso 3: Probar conectividad de red

Confirme que el nodo ISE afectado puede alcanzar el servidor SFTP en el puerto 22 y que no hay problemas de bloqueo en el nivel de red.

Paso 4: Habilitar depuración adicional

Habilite una depuración SSH/SFTP más detallada para capturar información detallada sobre la falla de autenticación.

Desde la CLI del nodo afectado:

1.- Habilitar estos debugs con comandos:

- debug copy 7
- debug transfer 7

2.- Utilice el comando `show repository xxxxx` después de habilitar los debugs para capturar más información.

Paso 5: Comparar huellas dactilares de claves SSH

Verifique que la clave pública SSH en el servidor SFTP coincida con la clave privada que está utilizando el nodo ISE afectado.

El problema se resolvió identificando la frase de contraseña correcta utilizada para generar la clave RSA en el nodo SPAN y reconfigurando la configuración del repositorio para alinearla con las credenciales válidas.

Solución alternativa provisional

Se recomienda verificar manualmente la frase de contraseña mediante `ssh-keygen -y -f /home/admin/.ssh/id_rsa` en la CLI para confirmar qué contraseña desbloqueó correctamente la clave privada antes de volver a aplicar la configuración del repositorio en la GUI.

Pasos para regenerar la clave RSA:

1.- Abra el CLI del nodo afectado.

2.- Eliminar la antigua clave RSA con el comando `crypto key delete rsa`.

3.- Generar una nueva clave RSA con la frase de contraseña deseada con el comando `crypto key generate rsa passphrase XXXXXXXXXXXXXXX`.



Nota: La frase de paso debe tener 13 o más caracteres.

4.- Obtener la nueva clave pública RSA para importar al otro sistema con el comando `show crypto key`.

Causa

Error de usuario / Error de configuración. La investigación determinó que el error de autenticación del repositorio en el nodo secundario se debía a una discordancia entre la frase de contraseña esperada y la frase de contraseña utilizada para proteger la clave privada RSA almacenada. Esto evitó que el subsistema criptográfico descifrara correctamente la clave para firmar el desafío de autenticación SSH.

Contenido relacionado

- [Soporte técnico y descargas de Cisco](#)

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).