

Errore di timeout dell'autenticazione della chiave RSA ISE SFTP

Sommario

Problema

Un repository SFTP configurato con l'autenticazione a chiave RSA funziona correttamente su un nodo ISE (ise1) ma non su un altro nodo ISE (ise2) che esegue ISE 3.4. Sul nodo in cui si è verificato l'errore, l'handshake SSH e la convalida del server sono stati completati correttamente, ma l'autenticazione a chiave pubblica non si conclude e la sessione SFTP scade con un "errore sftp_select: timeout!" x

Quando si cerca di elencare i contenuti del repository SFTP usando il comando `show repository SFTP` sul nodo ISE interessato, si verifica questa sequenza di errore:

```
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
```

Ciò impedisce l'uso del repository SFTP dal nodo ISE interessato per funzioni ISE critiche, come le operazioni di backup.

Ambiente

- Cisco Identity Services Engine (ISE) versione 3.4.0
- Implementazione ISE a più nodi con almeno due nodi (ise1 e ise2)

- Repository SFTP configurato con autenticazione della chiave RSA
- Autenticazione basata su chiave SSH con chiave privata RSA (/home/admin/.ssh/id_rsa)
- Server SFTP accessibile
- Autenticazione password disabilitata (-oPasswordAuthentication=no)

Risoluzione

Il caso è attualmente sotto indagine da parte della squadra di ingegneri. Il problema è stato segnalato per l'analisi del log radice per determinare la causa sottostante del timeout SFTP sul nodo ISE interessato.

In base all'output del comando debug, eseguire la procedura di risoluzione dei problemi descritta nelle sezioni seguenti per raccogliere ulteriori informazioni.

Passaggio 1: Verifica della coerenza della configurazione del repository SFTP tra i nodi

Confrontare la configurazione del repository SFTP su entrambi i nodi ISE per assicurarsi che siano identici.

Passaggio 2: Verifica delle autorizzazioni e della proprietà del file di chiave SSH

Verificare che il file della chiave privata SSH (/home/admin/.ssh/id_rsa) disponga delle autorizzazioni e della proprietà corrette sul nodo interessato.

Passaggio 3: Verifica connettività di rete

Confermare che il nodo ISE interessato possa raggiungere il server SFTP sulla porta 22 e che non vi siano problemi di blocco a livello di rete.

Passaggio 4: Abilita debug aggiuntivo

Abilitare il debug SSH/SFTP più dettagliato per acquisire informazioni dettagliate sull'errore di autenticazione.

Dalla CLI del nodo interessato:

1.- Abilitare questi debug con i comandi:

- copia di debug 7
- trasferimento di debug 7

2.- Utilizzare il comando `show repository xxxxx` dopo aver abilitato i debug per acquisire ulteriori informazioni.

Passaggio 5: Confronta impronte digitali della chiave SSH

Verificare che la chiave pubblica SSH sul server SFTP corrisponda alla chiave privata utilizzata dal nodo ISE interessato.

Il problema è stato risolto identificando la passphrase corretta utilizzata per generare la chiave RSA sul nodo SPAN e riconfigurando le impostazioni del repository in modo da allinearle con le credenziali valide.

Soluzione provvisoria

Si consiglia di verificare manualmente la passphrase utilizzando `ssh-keygen -y -f /home/admin/.ssh/id_rsa` sulla CLI per confermare la password che ha sbloccato correttamente la chiave privata prima di riapplicare la configurazione del repository nella GUI.

Passaggi per rigenerare la chiave RSA:

1.- Aprire la CLI del nodo interessato.

2.- Eliminare la vecchia chiave RSA con il comando `crypto key delete rsa`.

3.- Generare una nuova chiave RSA con la passphrase desiderata con il comando `crypto key generate rsa passphrase XXXXXXXXXXXXX`.



Nota: La passphrase deve contenere almeno 13 caratteri.

4.- Ottenere la nuova chiave pubblica RSA da importare nell'altro sistema con il comando `show crypto key`.

Causa

Errore utente / Errore di configurazione. L'indagine ha determinato che il guasto di autenticazione del repository sul nodo secondario è stato causato da una mancata corrispondenza tra la passphrase prevista e la passphrase utilizzata per proteggere la chiave privata RSA archiviata. Il sottosistema di crittografia non è stato in grado di decrittografare correttamente la chiave per firmare la richiesta di autenticazione SSH.

Contenuto correlato

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).