

Fehler beim Timeout für die ISE-SFTP-RSA-Schlüsselauthentifizierung

Inhalt

Problem

Ein mit RSA-Schlüsselauthentifizierung konfiguriertes SFTP-Repository funktioniert auf einem ISE-Knoten (ise1) erfolgreich, schlägt jedoch auf einem anderen ISE-Knoten (ise2) mit ISE 3.4 fehl. Auf dem ausgefallenen Knoten wird der SSH-Handshake und die Servervalidierung erfolgreich abgeschlossen, die Authentifizierung mit öffentlichem Schlüssel wird jedoch nicht abgeschlossen, und die SFTP-Sitzung wird mit einem Fehler "sftp_select" beendet: Timeout!" fehl.

Wenn Sie versuchen, den Inhalt des SFTP-Repositorys mit dem Befehl `show repository SFTP` auf dem betroffenen ISE-Knoten aufzulisten, tritt diese Fehlersequenz auf:

```
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
```

Dadurch wird verhindert, dass das SFTP-Repository vom betroffenen ISE-Knoten für wichtige ISE-Funktionen wie Sicherungsvorgänge verwendet wird.

Umwelt

- Cisco Identity Services Engine (ISE) Version 3.4.0
- ISE-Bereitstellung mit mehreren Knoten und mindestens zwei Knoten (ise1 und ise2)

- SFTP-Repository mit RSA-Schlüsselauthentifizierung konfiguriert
- Schlüsselbasierte SSH-Authentifizierung mit privatem RSA-Schlüssel (/home/admin/.ssh/id_rsa)
- Zugriff auf SFTP-Server
- Kennwortauthentifizierung deaktiviert (-oPasswordAuthentication=no)

Auflösung

Dieser Fall wird derzeit vom Technikerteam untersucht. Das Problem wurde zur Stammprotokollanalyse eskaliert, um die zugrunde liegende Ursache des SFTP-Timeouts für den betroffenen ISE-Knoten zu ermitteln.

Führen Sie basierend auf der Debugausgabe die in den nächsten Abschnitten beschriebenen Schritte zur Fehlerbehebung aus, um zusätzliche Informationen zu erfassen.

Schritt 1: Überprüfung der Konsistenz der SFTP-Repository-Konfiguration zwischen den Knoten

Vergleichen Sie die SFTP-Repository-Konfiguration auf beiden ISE-Knoten, um sicherzustellen, dass sie identisch sind.

Phase 2: Überprüfen Sie die SSH-Schlüsseldateiberechtigungen und -besitzverhältnisse.

Stellen Sie sicher, dass die Datei mit dem privaten SSH-Schlüssel (/home/admin/.ssh/id_rsa) die richtigen Berechtigungen und Rechte für den betroffenen Knoten hat.

Schritt 3: Testen der Netzwerkverbindung

Vergewissern Sie sich, dass der betroffene ISE-Knoten den SFTP-Server an Port 22 erreichen

kann und keine Blockierungsprobleme auf Netzwerkebene vorliegen.

Schritt 4: Zusätzliches Debuggen aktivieren

Aktivieren Sie ausführlicheres SSH/SFTP-Debugging, um detaillierte Informationen über den Authentifizierungsfehler zu erfassen.

CLI des betroffenen Knotens:

1.- Aktivieren Sie diese Debug-Befehle:

- Debug-Text 7
- Debug-Transfer 7

2.- Verwenden Sie den Befehl `show repository xxxxx` nach dem Aktivieren von Debugs, um weitere Informationen zu erfassen.

Schritt 5: SSH-Schlüssel-Fingerprints vergleichen

Überprüfen Sie, ob der öffentliche SSH-Schlüssel auf dem SFTP-Server mit dem privaten Schlüssel übereinstimmt, der vom betroffenen ISE-Knoten verwendet wird.

Das Problem wurde behoben, indem die richtige Passphrase zum Generieren des RSA-Schlüssels auf dem SPAN-Knoten identifiziert und die Repository-Einstellungen neu konfiguriert wurden, sodass sie mit den gültigen Anmeldedaten übereinstimmen.

Zwischenlösung

Es wird empfohlen, die Passphrase mithilfe von `ssh-keygen -y -f /home/admin/.ssh/id_rsa` in der CLI manuell zu überprüfen, um zu bestätigen, welches Kennwort den privaten Schlüssel erfolgreich entsperrt hat, bevor die Repository-Konfiguration in der GUI erneut angewendet wird.

Schritte zum Neugenerieren des RSA-Schlüssels:

1.- Öffnen Sie die CLI des betroffenen Knotens.

2.- Löschen Sie den alten RSA-Schlüssel mit dem Befehl `crypto key delete rsa`.

3.- Generieren Sie einen neuen RSA-Schlüssel mit der gewünschten Passphrase mit dem Befehl `crypto key generate rsa passphrase XXXXXXXXXXXXXXX`.



Anmerkung: Die Passphrase muss mindestens 13 Zeichen lang sein.

4.- Holen Sie sich den neuen öffentlichen RSA-Schlüssel, der mit dem Befehl `show crypto key` in das andere System importiert werden soll.

Ursache

Benutzerfehler/Konfigurationsfehler. Bei der Untersuchung wurde festgestellt, dass der Fehler bei der Repository-Authentifizierung auf dem sekundären Knoten durch eine Diskrepanz zwischen der erwarteten Passphrase und der Passphrase verursacht wurde, die zum Sichern des gespeicherten privaten RSA-Schlüssels verwendet wurde. Dadurch konnte das kryptografische Subsystem den Schlüssel nicht erfolgreich entschlüsseln, um den SSH-Authentifizierungsproblem zu signieren.

Verwandte Inhalte

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.