

ISE SFTP RSA金鑰身份驗證超時錯誤

目錄

問題

配置了RSA金鑰身份驗證的SFTP儲存庫在一個ISE節點(ise1)上成功運行，但在運行ISE 3.4的另一個ISE節點(ise2)上失敗。在故障節點上，SSH握手和伺服器驗證成功完成，但公鑰身份驗證未完成，並且SFTP會話超時，並出現「sftp_select Error:逾時！」錯誤消息。

在受影響的ISE節點上嘗試使用show repository SFTP命令列出SFTP儲存庫內容時，出現以下錯誤序列：

```
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
```

這可以防止從受影響的ISE節點使用SFTP儲存庫執行關鍵ISE功能，如備份操作。

環境

- 思科身分識別服務引擎(ISE)版本3.4.0
- 多節點ISE部署，至少有兩個節點 (ise1和ise2)
- 配置了RSA金鑰身份驗證的SFTP儲存庫
- 使用RSA私鑰(/home/admin/.ssh/id_rsa)的SSH基於金鑰的身份驗證
- 可訪問SFTP伺服器

- 已禁用密碼身份驗證(-oPasswordAuthentication=no)

解析

工程小組目前正在調查此案。此問題已升級以進行根日誌分析，以確定受影響的ISE節點上SFTP超時的根本原因。

根據調試輸出，執行下一節中描述的故障排除步驟以收集更多資訊。

步驟 1:驗證節點之間的SFTP儲存庫配置一致性

比較兩個ISE節點上的SFTP儲存庫配置，確保它們相同。

步驟 2:檢查SSH金鑰檔案許可權和所有權

驗證SSH私鑰檔案(/home/admin/.ssh/id_rsa)在受影響的節點上是否具有正確的許可權和所有權。

步驟 3:測試網路連線

確認受影響的ISE節點可以到達埠22上的SFTP伺服器，並且沒有網路級阻止問題。

步驟 4:啟用其他調試

啟用更詳細的SSH/SFTP調試以捕獲有關身份驗證失敗的詳細資訊。

在受影響的節點CLI上：

1. — 使用命令啟用這些調試：

- debug copy 7
- debug transfer 7

2. — 啟用調試後使用show repository xxxxx命令捕獲更多資訊。

步驟 5:比較SSH金鑰指紋

驗證SFTP伺服器上的SSH公鑰是否與受影響ISE節點使用的私鑰相匹配。

通過識別用於在SPAN節點上生成RSA金鑰的正確密碼並重新配置儲存庫設定以與有效憑證保持一致，問題得以解決。

臨時解決方法

建議在CLI上使用ssh-keygen -y -f /home/admin/.ssh/id_rsa手動驗證密碼以確認哪個密碼已成功解鎖私鑰，然後再在GUI中重新應用儲存庫配置。

重新生成RSA金鑰的步驟：

1. — 開啟受影響的節點CLI。
2. — 使用crypto key delete rsa 命令刪除舊的RSA金鑰。
3. — 使用crypto key generate rsa passphrase XXXXXXXXXXXX命令生成具有所需密碼的新RSA金鑰。



附註：密碼必須是13個或更多字元。

-
4. — 使用show crypto key 命令獲取新的RSA公鑰以匯入到其他系統。

原因

使用者錯誤/配置錯誤。調查確定輔助節點上的儲存庫身份驗證失敗是由預期的密碼與用於保護儲存的RSA私鑰的密碼不匹配引起的。這阻止加密子系統成功解密金鑰以簽署SSH身份驗證質詢。

相關內容

- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。