CCCSP v15將CCCSP節點連線到SSM

目錄

問題

嘗試將CCCSP節點連線到SSM時，使用者可能會遇到證書信任問題，這會阻止智慧許可註冊成功。此錯誤與Cisco錯誤ID CSCwv41814相關，其中Java證書儲存需要手動更新以信任SSM證書鏈。

環境

- 思科客服中心解決方案平台(CCCSP)版本15（前稱CUSP）
- 需要智慧軟體管理器(SSM)連線
- 用於證書檔案傳輸的SFTP伺服器

解析

SSM憑證信任問題解決方案(CSCwv41814)

如果在連線到SSM時遇到證書信任問題，請按照以下步驟解決Java證書儲存問題。

步驟 1:啟用遠端帳戶訪問：

```
utils remote_account enable
```

步驟 2:建立遠端帳戶進行故障排除：

```
utils remote_account create ciscotac 2
```

步驟 3:導航到Java安全目錄：

```
cd $JAVA_HOME/jre/lib/security
```

步驟 4:透過SFTP將SSM根憑證和中間憑證傳輸到CCCSP系統：

```
sftp root@X.X.X.X
sftp> get sub-root.cer
sftp> get SSM-Root.cer
sftp> exit

# Check if the certificates are there.

[root@hostname security]# ls -ltr
-rw-r--r--. 1 root root  56050 Aug 17 15:55 java.security
-rw-------. 1 root root   2031 Sep  8 13:43 sub-root.cer
-rw-------. 1 root root   1396 Sep  8 13:43 SSM-Root.cer
```

步驟 5:將根證書匯入到Java金鑰庫：

```
$JAVA_HOME/bin/keytool -storetype JKS -import -alias SSM-Root -keystore $JAVA_HOME/jre/lib/security/cac
```

步驟 6:將中間證書匯入到Java金鑰庫：

```
$JAVA_HOME/bin/keytool -storetype JKS -import -alias sub-root -keystore $JAVA_HOME/jre/lib/security/cac
```

步驟 7:重新啟動CCCSP系統以應用更改。

原因

CCCSP v15 CLI限制存在，因為本機crypto key certreq命令未提供將SAN條目新增到CSR的已記錄

方法。當證書中存在SAN時，CCCSP v15使用SAN進行TLS對等驗證；否則，將使用證書公用名(CN)進行驗證。SSM連線問題是由思科錯誤ID CSCwv41814引起的，其中CCCSP上的Java證書儲存不自動信任SSM證書鏈，需要手動匯入根證書和中間證書。

相關內容

- CCCSP 15.0.1 CLI配置指南 — 建立和匯入簽名證書
- 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）。