CVP智慧許可證CSSM證書匯入過程

目錄

問題

CVP呼叫伺服器在SmartAgent日誌中遇到智慧許可「驗證簽名」錯誤。系統要求將CSSM（思科智慧軟體管理器）證書匯入到CVP金鑰庫中，以解決正常授權狀態更新過程中的簽名驗證失敗。如果沒有正確的CSSM證書鏈，CVP將無法使用思科智慧軟體管理器驗證許可事務，從而導致許可合規性問題。

環境

- 思科客戶語音入口網站(CVP)通話伺服器版本12.6.2
- 客服中心軟體 — Packaged Contact Center Enterprise(PCCE)
- CVP服務：Call Server、WSM(Web Service Manager)、VXML Server
- 用於證書管理的Java JCEKS金鑰庫格式
- 智慧許可與思科智慧軟體管理器(CSSM)整合

解析

按照以下詳細步驟將CSSM證書匯入CVP呼叫伺服器金鑰庫。

步驟 1:標識金鑰庫密碼

以管理員身份開啟命令視窗，然後導航到CVP主目錄以解密金鑰庫密碼：

```
cd %CVP_HOME%\bin
DecryptKeystoreUtil.bat
```

記錄此實用程式顯示的口令，因為所有後續的keytool命令都需要該口令。

步驟 2:備份當前金鑰庫

從安全目錄建立現有金鑰庫的備份：

```
cd %CVP_HOME%\conf\security
copy .keystore backup.keystore
```

步驟 3:匯出當前金鑰庫內容

生成金鑰庫中所有當前證書的清單以供參考：

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp.tx
```

檢視生成的檔案以瞭解當前證書清單。

步驟 4:下載CSSM證書

從CVP授權頁面上的傳輸URL獲取所需的CSSM證書鏈。憑證要求取決於憑證型別：

對於CA簽名的證書：以.cer格式單獨下載根證書和中間證書

對於自簽名證書：直接下載CSSM證書

將證書檔案儲存到CVP安全目錄：

```
%CVP_HOME%\conf\security
```

步驟 5:匯入CSSM根證書（CA簽名）

對於CA簽名的證書，請首先匯入根證書：

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

步驟 6:匯入CSSM中間證書（CA簽名）

如果存在中間證書，請使用以下命令將其匯入：

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

步驟 7:匯入自簽名CSSM證書（備選）

對於自簽名證書，請直接匯入CSSM證書：

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

步驟 8:驗證證書匯入

確認金鑰庫中存在新證書：

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp_ne
```

檢視新證書清單以驗證CSSM證書是否已成功匯入。

步驟 9:重新啟動和服務驗證

重新啟動CVP伺服器並記錄重新啟動時間。重新啟動後，確認所有CVP服務都已啟動：

- 通話伺服器
- WSM（Web服務管理器）
- VXML伺服器

在服務啟動後等待約20分鐘，然後繼續驗證。

步驟 10:驗證解決方案

執行以下驗證步驟：

檢查SmartAgent日誌：

導航到C:\Cisco\CVP\logs\WSM，然後按修改日期排序。檢查SmartAgent日誌中最新的15分鐘狀態報告。在重新啟動時間之後，驗證簽名異常必須不再出現。

驗證許可狀態：

訪問CVP許可頁面，確認系統顯示「已註冊」和「合規」狀態且無錯誤。

回滾過程（如果出現問題）

如果在證書匯入過程中遇到問題，請執行以下回滾步驟：

步驟 1:停止所有CVP服務（呼叫伺服器、WSM、VXML）

步驟 2:導航到安全目錄：

```
cd %CVP_HOME%\conf\security
```

步驟 3:刪除已修改的金鑰庫：

```
del .keystore
```

步驟 4:還原備份金鑰庫：

```
rename backup.keystore .keystore
```

步驟 5:重新啟動所有CVP服務

原因

CVP呼叫伺服器金鑰庫不包含驗證來自思科智慧軟體管理器的數位簽章所需的所需CSSM證書鏈。在智慧許可操作期間，CVP嘗試使用基於證書的簽名驗證來驗證許可通訊的真實性。如果Java JCEKS金鑰庫中沒有正確的CSSM證書，則這些簽名驗證嘗試會失敗，從而導致許可事務錯誤和潛在的合規性問題。

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）。