由於NCS 1010節點上的CEPKI Trustpool捆綁累積導致恢復時間延長和SSH訪問失敗

目錄

簡介

本文檔介紹由於NCS 1010節點(使用Cisco IOS® XR 24.3.1、25.1.1)上的CEPKI信任池捆綁累積而延長的恢復時間和SSH訪問失敗。

問題

在NCS 1010光纖節點上重新載入路由處理器(RP)後，會觀察到間歇性延長的恢復時間。恢復期間，由於思科嵌入式公鑰基礎設施(CEPKI)初始化延遲，對裝置的SSH訪問失敗。這可以防止受影響節點上的遠端管理和操作任務。系統日誌消息和SSH錯誤表明，SSHD進程在初始化完成之前無法從CEPKI檢索主機金鑰，從而導致SSH登入失敗。SSH訪問的恢復僅在CEPKI完成初始化後觀察到，通常在30-60分鐘之後。此問題與裝置上（尤其是軟體版本24.3.1和25.1.1）上的大量信任池捆綁累積相關。

環境

- 技術：光纖網路
- 產品系列：NCS 1000系列（NCS 1010光纖節點）
- 軟體版本：IOS XR 24.3.1、25.1.1（兩者上都重現問題）
- 元件:路由處理器(RP)、CEPKI、SSHD進程
- 操作功能：Call-Home、智慧許可應用程式
- 近期觀察結果：恢復時間延長、RP重新載入後SSH訪問失敗、高信任池捆綁累積

解析

為了緩解和解決CEPKI初始化延遲和SSH訪問因信任池捆綁累積而導致的故障，請按照上述步驟操作。這些步驟直接源自經過驗證的工程分析和有文檔記錄的解決方案。

1. 檢查Trustpool Bundle Cumulation:

運行這些命令以檢查當前trustpool捆綁狀態和相關證書資訊。提供的資料中沒有示例輸出。

步驟1.檢視詳細的NCS1010技術資訊。

```
show tech ncs1010 detailed
```

步驟2.檢查加密會話詳細資訊。

```
show tech crypto session
```

步驟3.審查CEPKI技術支援資料。

```
show tech-support cepki
```

步驟4.檢視系統資料庫狀態。

```
show tech sysdb
```

步驟5.列出所有已安裝的加密CA證書。

```
show crypto ca certificates
```

步驟6.顯示信任池捆綁詳細資訊。

```
show crypto ca trustpool detail
```

步驟7.顯示trustpool狀態。

```
show crypto ca trustpool
```

步驟8.顯示trustpool策略。

```
show crypto ca trustpool policy
```

2. 受影響版本（24.3.1和25.1.1）的解決方法：

為了清除累積的trustpool捆綁包並強制重新匯入，請依次執行上述命令。此過程刪除之前下載的信任池證書並下載當前捆綁包，有助於緩解初始化延遲。

步驟1.在匯入之前清除信任池證書。

```
crypto ca trustpool import url clean
```

步驟2.匯入信任池捆綁包。

```
crypto ca trustpool import url
```

3. 永久修復（建議升級）：

39205在Cisco IOS XR版本26.1.1中，思科錯誤ID CSCwq下解決了基礎問題.
升級到此版本，以確保系統在下載當前捆綁包之前自動清除以前下載的信任池證書。這將為未來操作保持乾淨且一致的信任池狀態。

4. Call-Home傳輸方法建議：

   請注意，思科已宣佈從Cisco IOS XR 25.3.1版開始的Call-Home傳輸方法的壽命終止(EoL)。強烈建議過渡到智慧許可傳輸方法以保持支援性。如需詳細資訊，請參閱所提供的思科諮詢。

技術指標和日誌：

- 系統日誌：

```
sshd[21897]: main: failed to get keys from cepki
```

- 系統日誌：

```
cepki[274]: certificate database updated
```

- SSH錯誤：

```
ssh: connect to host <node> port 22: Connection refused
```

- 觀察：CEPKI進程在不使用初始化結束(EOI)訊號的情況下重複更新證書。
- 觀察到的Trustpool計數：20次出現「Trustpool:內建，768個「Trustpool:已下載'。

原因

根本原因是裝置上的多個trustpool捆綁包的累積，這些捆綁包由通過Call-Home和智慧許可應用的重複下載觸發。在Cisco IOS XR版本24.3.1和25.1.1中，這些應用程式下載信任池捆綁包而不清除以前儲存的證書，從而導致CEPKI初始化和SSH金鑰檢索延遲。此行為已在Cisco錯誤ID CSCwq39205下解決和修正。
在26.1.1版中，系統現在會在下載新捆綁包之前清除以前的trustpool證書。

相關資訊

- 思科錯誤ID CSCwq39205 — 應清除信任池捆綁包，然後再重新下載
- 思科錯誤ID CSCwq53226 - Call-Home傳輸方法壽命終止建議
- 思科建議：Call-Home遷移至智慧傳輸通知

- 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）。