具有SHA1雜湊不相容的終端DLP證書型自動註冊失敗

目錄

問題

基於證書的自動註冊期間終端DLP註冊失敗，並出現重複的初始化錯誤。註冊過程無法使用客戶端身份證書進行身份驗證，從而導致連續重試嘗試。

在註冊日誌中觀察到以下錯誤消息：

```
[2026-02-05 13:24:58.154989] [info] [AutoEnrollMonitor.cpp:633] Auto-enrollment attempt #5 with enrollm
[2026-02-05 13:24:58.154989] [info] [SSEZtnaEnroller.cpp:185] Processing start event
[2026-02-05 13:24:58.155992] [info] [SSEZtnaEnroller.cpp:205] Starting Enrollment
[2026-02-05 13:24:58.398260] [error] [SSEZtnaEnroller.cpp:335] spIdentities count: 1
[2026-02-05 13:24:58.399259] [error] [SSEZtnaEnroller.cpp:355] None of the 1 user store client certific
[2026-02-05 13:24:58.407289] [info] [SSEZtnaEnroller.cpp:2237] Notifying enrollment completion with res
[2026-02-05 13:24:58.407289] [info] [SSEZtnaEnroller.cpp:2241]
Enrollment Stats
================
Authentication type           : certificate
Bootstrap                     : failure (0.251 sec)
----------------
Overall result                : failure (0.251 sec)
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:214] Notified of enrollment state change to
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:214] Notified of enrollment state change to
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:615] Will retry the enrollment with enrollme
```

其他TLS級別的身份驗證失敗記錄為以下錯誤消息："收到TLS警報：致命的/錯誤的證書。"

環境

- 技術：解決方案支援（SSPT — 需要合約）
- 子技術：安全訪問 — 統一策略（Internet策略、私有策略、DLP策略、RBI、安全配置檔案）
- 軟體版本:ALL

- 身份驗證方法：基於憑證的自動註冊
- 證書儲存：使用者儲存客戶端證書
- 證書雜湊演算法：SHA1（不建議使用）

解析

解決方法涉及使用支援的雜湊演算法重新生成身份證書，並確保正確的證書安裝和配置。

步驟 1:使用支援的雜湊演算法重新生成身份證書

使用SHA256或SHA-3雜湊（而不是棄用的SHA1演算法）生成並重新頒發身份證書。必須使用以下規範建立證書：

- 雜湊演算法：SHA256或SHA-3（不支援SHA1）
- Format:PKCS#12(PFX)格式
- 必填欄位：SAN欄位，帶有為註冊指定的RFC822名稱

步驟 2:在正確的證書儲存中安裝更新的證書

在相應的證書儲存位置安裝新生成的證書：

- 證書儲存位置：使用者/電腦個人>證書儲存
- 證書格式：PKCS#12(PFX)

步驟 3:重新啟動終端以重新觸發身份驗證

安裝更新的證書後，請重新啟動終端系統以重新觸發身份驗證過程，並允許註冊機制檢測新證書。

步驟 4:測試來自非公司網路的身份驗證

要排除邊緣防火牆的SSL檢查或解密干擾，請從非公司網路環境測試身份驗證過程。這有助於隔離可能會干擾註冊過程的潛在網路級證書檢查問題。

步驟 5:重試終端DLP註冊

完成證書替換和系統重新啟動後，再次嘗試終端DLP註冊過程。監視註冊日誌，以驗證身份驗證和註冊成功完成。

原因

註冊失敗是由於在客戶端身份證書中使用SHA1雜湊演算法造成的。SHA1是不再受註冊策略要求支援的過時加密雜湊演算法。註冊系統特別要求證書與現代、安全的演算法（如SHA256或SHA-3）進行雜湊處理，以滿足當前的安全標準和策略合規性。

註冊過程根據註冊選擇策略驗證客戶端證書時，會拒絕使用已棄用的SHA1雜湊演算法的證書，從而導致「1個使用者儲存客戶端證書都不匹配註冊選擇策略」錯誤消息和後續初始化失敗。

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）。