CUCM電話證書問答(LSC/MIC)

目錄

簡介

本文檔包含思科統一通訊管理器(CUCM)電話證書的一些問題和答案。 以下是電話憑證的快速檢視。

製造商安裝證書(MIC):

顧名思義，電話預裝有MIC，管理員無法刪除/修改此功能。證書頒發機構(CA)證書CAP-RTP-001、CAP-RTP-002、Cisco_Manufacturing_CA和Cisco Manufacturing CA SHA2預安裝在CUCM中以信任MIC。由於MIC CA無法重新生成，因此一旦有效性過期，就不能使用MIC。

本地重要證書(LSC):

LSC擁有思科IP電話的公鑰，該公鑰由思科統一通訊管理器證書授權代理功能(CAPF)私鑰簽名。預設情況下未安裝在電話上。管理員對LSC具有完全控制權。可以重新生成CAPF CA證書，從而可以在需要時向電話頒發新的LSC。

電話證書的常見用途是什麼？

以下是電話憑證的一些常見用途

在CAPF和電話之間進行安裝/升級、刪除或故障排除

電話與CAPF建立連線，以安裝/升級、刪除或排除電話上的證書故障。在證書頒發機構代理功能(CAPF)資訊下的身份驗證模式被現有證書（優先於LSC）或現有證書（優先於MIC）設定為時，電話證書用於與CAPF建立連線。

按現有證書（優先於LSC）： 電話使用LSC向CAPF進行身份驗證。如果未安裝LSC，它將使用MIC。如果使用的證書有問題，安裝將失敗，原因為「無效LSC」。例如，CAPF Trust中沒有LSC的已簽名CA。對於此類故障情況，請使用其他證書方法或空字串更新身份驗證模式。

按現有證書（優先到MIC）：電話使用MIC向CAPF進行身份驗證。

在CallManager和電話之間提供傳輸層安全(TLS)連線

電話使用LSC或MIC與CallManager建立TLS連線。CallManager將通過檢查CallManager-trust來驗證電話提供的證書。相應的CAPF證書必須在CallManager-trust中提供，對於LSC和對於MIC的思科製造CA。

在電話和身份驗證伺服器之間進行802.1x身份驗證

CAPF/製造CA證書上傳到身份驗證伺服器，如思科安全訪問控制伺服器(ACS)或身份服務引擎(ISE)。 驗證伺服器會在電話出示其憑證（LSC或MIC）時，使用上傳的憑證對電話進行驗證。

適用於電話與適用於VPN的思科調適型安全裝置(ASA)之間的基於證書的身份驗證

CAPF/製造CA證書在ASA中上傳，當電話出現LIC/MIC時，ASA通過檢查信任對其進行驗證。

存在LSC和MIC時，是否有任何方法為連線顯式選擇LSC或MIC?

沒有選項可以選擇連線是LSC還是MIC。如果安裝了LSC，電話將使用LSC。如果未安裝LSC，電話將使用MIC。

LSC不存在時的控制檯條目：

秒：-PXY_NO_LSC:沒有[SCCP]的LSC，將嘗試MIC

存在LSC時的控制檯條目：

秒：-PXY_CERT_CIPHER:[SCCP]、[TLSv1]、證書[LSC]

只能在CAPF和電話安裝/升級、刪除或故障排除之間選擇LSC或MIC。

在移動到新群集時，安裝了安全配置檔案的LSC電話沒有註冊的原因是什麼？

對於已具有舊群集中的LSC的電話而言，可能會發生這種情況。當MIC和LSC同時存在時，LSC用於建立TLS連線。無法建立TLS，因為新CUCM在其CallManager — 信任中沒有此LSC的CA。

控制檯日誌顯示用於建立TLS的證書。下面的條目顯示使用LSC。

3469不是00:01:31.935298秒：-PXY_CERT_CIPHER:[SCCP]、[TLSv1]、證書[LSC]、密碼[AES256-SHA:AES128-SHA]

SSL3_具有「未知CA」的警報，用於控制檯日誌中的此類失敗案例：-

3486錯誤00:01:31.938954秒：-STATE_SSL3_ALERT:SSL3警報[read]:[fatal]:[未知CA

解決此問題的方法之一是使用非安全配置檔案註冊電話，然後刪除現有的LSC。從新群集安裝LSC，然後使用安全配置檔案註冊電話。也可以使用MIC註冊具有安全配置檔案的電話而不安裝LSC。

電話是否需要安裝LSC才能使用經過身份驗證或加密的安全配置檔案進行註冊？

否。如果未安裝LSC，Phone將使用MIC建立與CUCM的TLS連線。

4878 WRN 15:47:34.756063秒：-PXY_NO_LSC:沒有[SCCP]的LSC，嘗試MIC。

在安裝/升級/刪除LSC時，裝置安全模式是否必須經過身份驗證或加密？

這不是強制性的，可以使用預設標準非安全配置檔案在裝置安全模式中的不安全位置完成此操作。

在電話中安裝LSC時，群集是否必須處於混合模式？

這不是強制性的。即使群集安全模式處於非安全狀態，也可以完成LSC安裝/刪除。

如果電話使用的LSC出現問題，如何快速測試？

通過轉至Phone Admin頁面刪除電話中的LSC。這將強制電話使用MIC。如果使用MIC完全正常，則使用LSC進行故障排除。

如何獲取用於故障排除的電話證書？

在「Device/Phone（裝置/電話）」下將「Certificate Operation（證書操作）」設定為「Troubleshoot（故障排除）」。按儲存然後應用配置。 等待檢視證書操作狀態以排除**成功故障**。從即時監控工具(RTMT)收集**思科證書頒發機構代理功能日誌**。 它包含來自電話的證書。

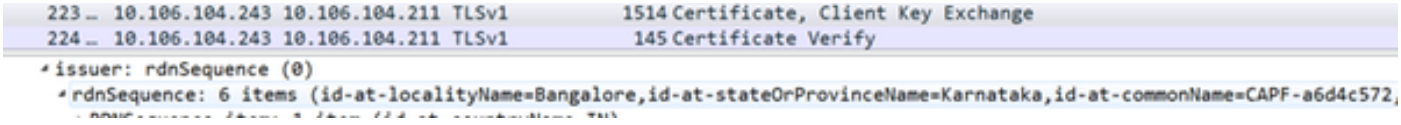
如果電話的LSC或MIC用於與CallManager建立TLS連線，如何從資料包捕獲進行驗證？

收集覆蓋電話重啟的資料包捕獲。

檢查證書、客戶端金鑰交換消息。驗證從IP電話傳送的證書。

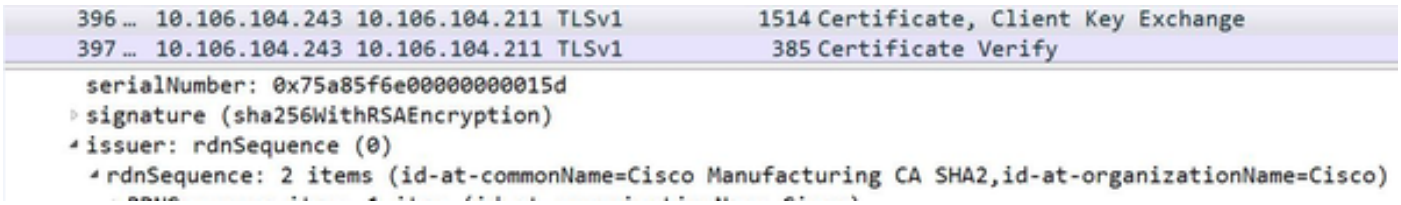
示例LSC:

對於LSC，CAPF CN出現在頒發者欄位中。相應的CAPF根必須在CallManager-trust中。



示例MIC:

對於MIC，在issuer欄位中輸入Cisco Manufacturing CA。CallManager-trust中必須存在相應的根CA。



在證書授權代理功能(CAPF)資訊下，身份驗證模式的意義是什麼？CUCM和電話之間的TLS連線是否有意義？

它只是一種電話和CAPF之間的身份驗證方法，用於安裝/升級/刪除和故障排除操作。它對CUCM和電話之間的TLS連線沒有任何意義。

重新生成CAPF證書後，電話要考慮哪些基本LSC操作？

本節介紹未使用離線CA發出LSC的空閒情況。

與CallManager的TLS連線

從CallManager-trust中刪除以前的CAPF證書之前，請確保在電話上安裝新的LSC。刪除之前的CAPF證書並重新啟動CallManager服務會導致具有此CAPF證書頒發的LSC的電話出現註冊問題。

使用CAPF-Trust的LSC操作

從CAPF-trust中刪除以前的CAPF證書之前，請確保在電話上安裝新的LSC。**Existing Certificate(Precedence to LSC)使用身份驗證模式安裝/刪除**等LSC操作將失敗，並出現錯誤**Invalid LSC**（對於具有此CAPF證書頒發的LSC的電話）。

在電話和身份驗證伺服器之間進行802.1x身份驗證

確保在上傳新的CAPF證書並且電話獲得由新的CAPF頒發的LSC之前，不要從身份驗證伺服器刪除以前的CAPF證書。

在ASA和電話之間

請確保在電話獲取新的LSC並將新的CAPF CA證書上傳到ASA之前，不要從ASA刪除以前的CAPF證書。

有關再生CAPF證書要遵循的步驟，請參閱證書再生。

相關資訊

- Cisco IP電話憑證和安全通訊
- 適用於802.1X的IP電話設計手冊
- 思科統一通訊管理器安全指南