CUCM證書的再生

目錄

簡介

本檔案介紹在Cisco Unified Communications Manager(CUCM)版本8.X和更新版本中重新生成證書的程式。

必要條件

需求

思科建議您瞭解以下主題：

- *即時監控工*具(RTMT)
- CUCM證書

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CUCM 8.X及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文說明如何在Cisco Unified Communications Manager(CUCM)8.X及更新版本中重新生成證書的分步過程。但是，這沒有反映12.0後國際交易日誌恢復的變化情況。

安裝RTMT

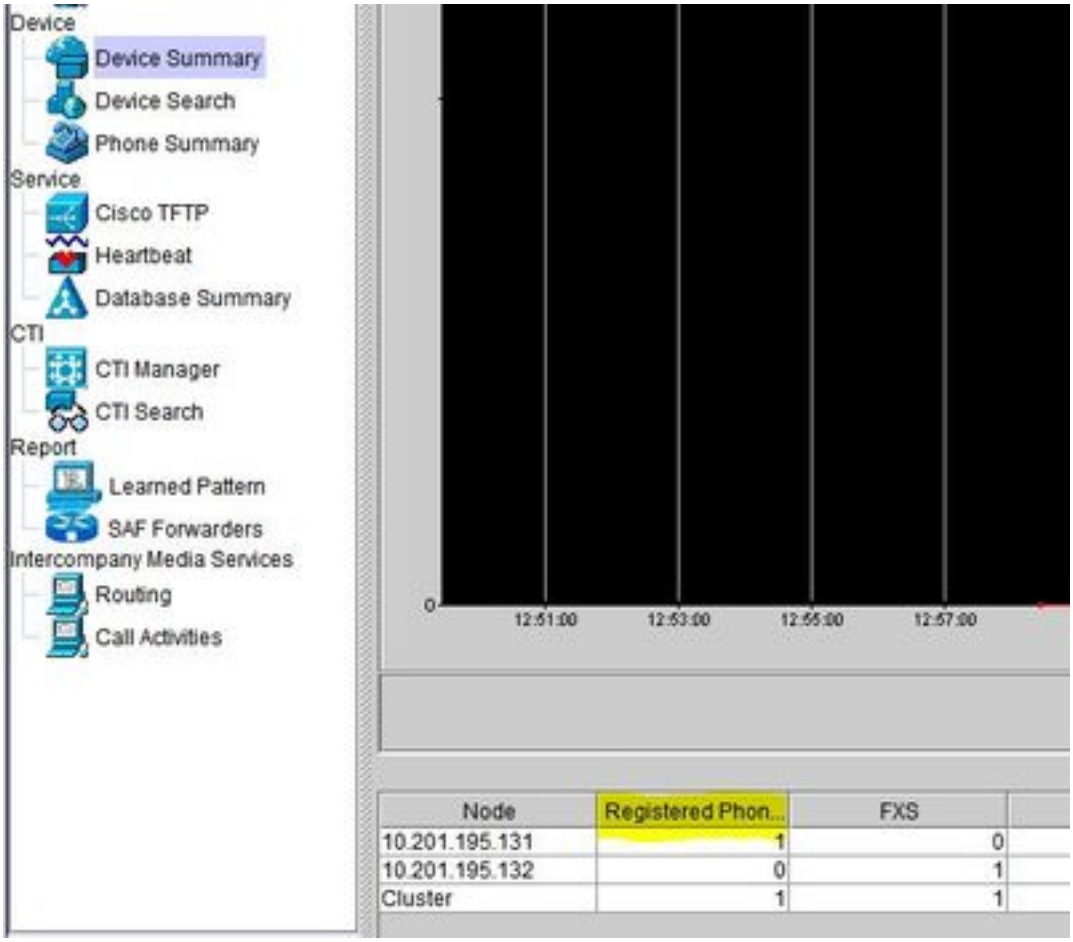
- 從Call Manager下載並安裝RTMT工具。 導航到Call Manager(CM)Administration: **應用程式>外掛>查詢> 思科整合即時監控工具 — Windows >下載** 安裝和啟動

使用RTMT監控端點

- 啟動RTMT並輸入IP地址或完全限定域名(FQDN)，然後輸入使用者名稱和密碼以訪問該工具：
- 選擇**語音/影片頁籤**。選擇**Device Summary**。 此部分標識註冊終端的總數以及每個節點的數量端點重置時監視，以確保在重新生成下一個證書之前進行註冊

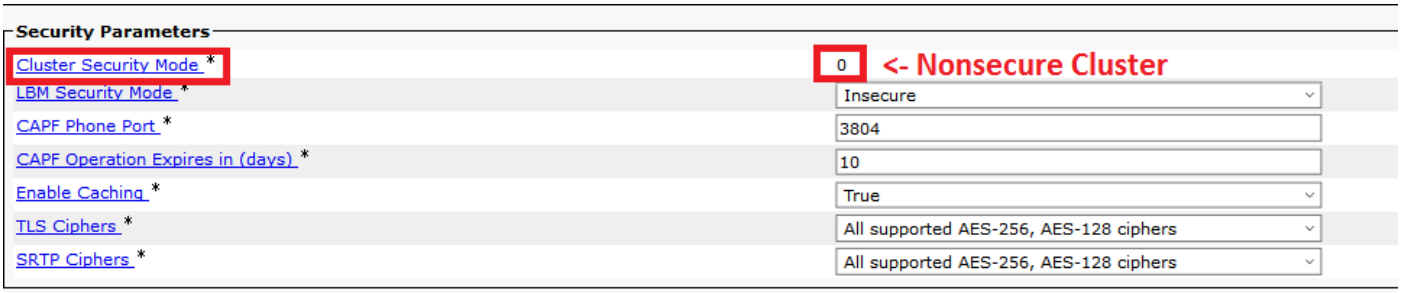
  提示：某些證書的再生過程可能會影響端點。由於需要重新啟動服務和重新啟動電話，請在正常工作時間後考慮一個行動計畫。強烈建議通過RTMT驗證電話註冊。

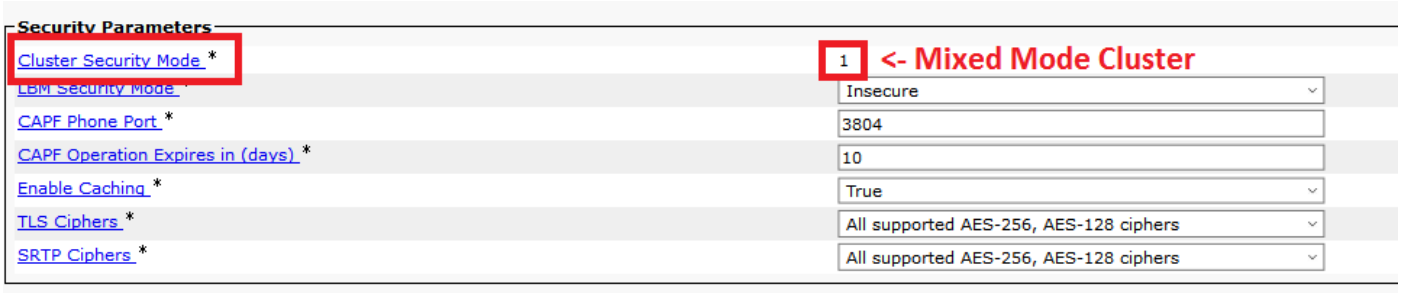
  警告：在此過程之後，當前ITL不匹配的終端可能會出現註冊問題。 在更新過程完成且所有其他電話註冊後，刪除終端上的國際交易日誌是一個典型的最佳做法解決方案。



確定集群是處於混合模式還是非安全模式

- 導航到CM管理。 System > Enterprise Parameters > Security Parameters > Cluster Security Mode





證書儲存的影響

在CUCM群集中更新所有證書對於成功的系統功能至關重要。如果證書過期或無效，可能會嚴重影響系統的正常功能。影響可能因系統設定而異。以下為無效或過期的特定證書的服務清單：

CallManager.pem

- 加密/身份驗證電話未註冊
- 簡單檔案傳輸協定(TFTP)不可信（電話不接受已簽名的配置檔案和/或ITL檔案）
- 電話服務可能受到影響
- 安全作業階段啟始通訊協定(SIP)中繼或媒體資源(會議橋接器、媒體終端點(MTP)、轉碼器等)不註冊或工作。
- AXL請求失敗。

Tomcat.pem

- 電話無法訪問CUCM節點上託管的HTTPs服務，例如公司目錄
- CUCM可能遇到各種Web問題，例如無法從群集中的其他節點訪問服務頁
- 跨群集的分機移動(EM)或分機移動問題
- 單一登入(SSO)
- 如果整合了UCCX(Unified Contact Center Express)，由於CCX 12.5的安全更改，因此需要在UCCX tomcat-trust儲存中上傳CUCM Tomcat證書（自簽名）或Tomcat根和中間證書（CA簽名），因為它會影響Finesse案頭登入。

CAPF.pem

- 電話不對電話VPN、802.1x或電話代理進行身份驗證
- 無法為電話頒發本地重要證書(LSC)證書。
- 加密的配置檔案無效

IPSec.pem

- 災難恢復系統(DRS)/災難恢復框架(DRF)無法正常工作
- 到網關(GW)到其他CUCM群集的IPsec隧道無法正常工作

TVS（信任驗證服務）

預設情況下，信任驗證服務(TVS)是安全性的主要元件。TVS使思科統一IP電話能夠在建立HTTPS時驗證應用伺服器（例如EM服務、目錄和MIDlet）。

TVS提供以下功能：

- 可擴充性 — 要信任的證書數量不會影響思科統一IP電話資源。
- 靈活性 — 信任證書的新增或移除將自動反映在系統中。
- 預設安全 — 非媒體和訊號安全功能是預設安裝的一部分，不需要使用者干預。

ITL和CTL

- ITL包含Call Manager TFTP的證書角色、集群中的所有TVS證書以及運行時的證書授權代理功能(CAPF)。
- CTL包含在同一伺服器上運行的系統管理員安全令牌(SAST)、Cisco CallManager和Cisco TFTP服務的條目、CAPF、TFTP伺服器和Adaptive Security Appliance(ASA)防火牆。CTL中未

引用TVS。

憑證再生程式

附註：在重新生成證書之前，需要開啟並註冊所有端點。否則，未連線的電話要求刪除國際交易日誌。

Tomcat證書

識別是否正在使用第三方證書：

1. 從發佈者開始，依次導航到群集中的每個伺服器（在Web瀏覽器的單獨頁籤中），然後導航到每個訂閱者。 導航至**Cisco Unified OS Administration > Security > Certificate Management > Find**。
   如果Tomcat宣告了系統生成的自簽名證書，請從「描述」列中觀察。如果Tomcat由第三方簽署，請按照提供的連結執行操作，並在Tomcat重新生成後執行這些步驟。第三方簽名證書，請參閱CUCM上傳CCMAdmin Web GUI證書。
2. 選擇**Find**以顯示所有憑證： 選擇**Tomcat pem** Certificate。開啟後，選擇**Regenerate**並等待，直到您看到Success彈出視窗，然後關閉彈出視窗或返回並選擇**Find/List**。
3. 繼續處理每個後續訂閱伺服器，按照步驟2中的相同步驟操作，並在集群中的所有訂閱伺服器上完成。
4. 在所有節點重新生成Tomcat證書後，在所有節點上重新啟動tomcat服務。從發佈者開始，然後是訂閱者。 要重新啟動Tomcat，您需要為每個節點開啟CLI會話並執行命令**utils service restart Cisco Tomcat**。

```
admin:
admin:utils service restart Cisco Tomcat
 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

5.如果適用，CCX環境需要執行以下步驟：

- 如果使用自簽名證書，請將Tomcat證書從CUCM群集的所有節點上傳到Unified CCX Tomcat信任儲存。
- 如果使用CA簽名證書或專用CA簽名證書，請將CUCM的根CA證書上傳到Unified CCX Tomcat信任儲存。
- 按照CCX的證書再生文檔中的說明重新啟動伺服器。

其他參考:

- UCCX解決方案證書管理指南
- Unified CCX運行狀況檢查實用程式

IPSEC憑證

附註：DRF10.X版之前的CUCM/即時消息和線上狀態(IM&P) Master 代理在CUCM Publisher和IM&P Publisher上運行。DRF本地服務分別在訂閱伺服器上運行。 10.X及更高版本，DRF

Master 代理僅在CUCM發佈伺服器上運行，在CUCM訂閱伺服器和IM&P發佈伺服器和訂閱伺服器上運行DRF本地服務。

附註：災難恢復系統使用 Master 代理和本地代理，用於CUCM群集節點之間的資料身份驗證和加密。DRS將IPSec證書用於其公鑰/私鑰加密。請注意，如果從Certificate Management頁面刪除IPSEC truststore(hostname.pem)檔案，則DRS無法按預期工作。如果手動刪除IPSEC信任檔案，則必須確保將IPSEC證書上傳到IPSEC信任儲存。有關詳細資訊，請參閱《思科統一通訊管理器安全指南》中的證書管理幫助頁面。

1. 從發佈者開始，依次導航到群集中的每個伺服器（在Web瀏覽器的單獨頁籤中），然後導航到每個訂閱者。導航至**Cisco Unified OS Administration > Security > Certificate Management > Find**:
   選擇**IPSEC pem** Certificate。開啟後，選擇**Regenerate**並等待，直到您看到Success彈出視窗，然後關閉彈出視窗或返回並選擇**Find/List**。
2. 繼續使用後續使用者；按照步驟1中的相同步驟操作，並在集群中的所有訂閱伺服器上完成。
3. 在所有節點重新生成IPSEC證書後，重新啟動服務。
   導航到Publisher **Cisco Unified Serviceability**。 **Cisco Unified Serviceability > Tools > Control Center - Network Services**。選擇**Restart** on **Cisco DRF** Master服務。服務重新啟動完成後，在發佈器上的**Cisco DRF本地服務**上選擇**Restart**，然後繼續使用訂閱者，然後在**Cisco DRF本地服務**上選擇**Restart**。

發佈器中的IPSEC.pem證書必須有效，並且必須以IPSEC信任儲存形式存在於所有訂閱者中。發佈伺服器中不存在使用者IPSEC.pem證書，因為標準部署中存在IPSEC信任儲存。為了驗證有效性，請將PUB的IPSEC.pem證書中的序列號與SUB中的IPSEC-trust進行比較。它們必須匹配。

CAPF證書

警告：繼續進行之前，請確保已識別群集是否處於混合模式。 請參閱識**別集群是處於混合模式還是非安全模式部分**。

1. 導航至**Cisco Unified CM管理>系統>企業引數**。
   檢查Security Parameters部分，驗證集群安全模式是否設定為0或1。如果值為0，則集群處於非安全模式。如果值為1，則集群處於混合模式，並且需要在重新啟動服務之前更新CTL檔案。請參閱令牌和無令牌連結。
2. 從發佈者開始，依次導航到群集中的每個伺服器（在Web瀏覽器的各個頁籤中），然後導航到每個訂閱者。 導航至**Cisco Unified OS Administration > Security > Certificate Management > Find**。
   選擇**CAPF pem證**書。開啟後，選擇**Regenerate**並等待，直到您看到Success彈出視窗，然後關閉彈出視窗或返回並選擇**Find/List**
3. 繼續使用後續使用者；按照步驟2中的相同步驟操作，並在集群中的所有訂閱伺服器上完成。
   如果群集僅處於混合模式且已重新生成CAPF — 請在繼續下一步之前更新CTL Token - Tokenless。 如果群集處於混合模式，則還需要重新啟動Call Manager服務才能重新啟動其他服務。
4. 所有節點重新生成CAPF證書後，重新啟動服務。
   導航到發佈者**Cisco Unified Serviceability**。 **Cisco Unified Serviceability > Tools > Control Center - Feature Services**。從發佈者開始，在**思科證書頒發機構代理功能服務**上選擇**重新啟動**（僅在活動時）。
5. 導航至**Cisco Unified Serviceability > Tools > Control Center - Network Services**。 從發佈者開

始，然後繼續訂閱者，選擇**Restart** on **Cisco Trust Verification** 。 導航至**Cisco Unified Serviceability > Tools > Control Center - Feature Services**。從發佈伺服器開始，然後繼續使用訂閱伺服器，僅在活動**時重新啟動Cisco TFTP服務**。

6. 重新啟動所有電話： **Cisco Unified CM管理>系統>企業引數**選擇**Reset**，您會看到一個彈出視窗，其中包含**You are about to reset all devices in the system**語句。**此操作無法撤消。繼續？,**選擇**確定，然後選擇重置。**

電話現在已重置。通過RTMT工具監控其操作，以確保重置成功且裝置重新註冊到CUCM。 請等待電話註冊完成，然後再繼續下一個證書。此電話註冊過程可能需要一些時間。請注意，在再生過程之前具有不良ITL的裝置在移除之前不會註冊回集群。

CallManager證書

警告：繼續進行之前，請確保已識別群集是否處於混合模式。請參閱**確定集群是處於混合模式還是非安全模式**部分。

警告：請勿同時重新生成CallManager.PEM和TVS.PEM證書。 這會導致終端上安裝的ITL與不可恢復的不匹配，需要從集群中的所有終端上刪除ITL。完成CallManager.PEM的整個過程，並在電話註冊回後，啟動TVS.PEM的流程。

1. 導航至**Cisco Unified CM管理>系統>企業引數**: 檢查Security Parameters部分，驗證集群安全模式是否設定為0或1。如果值為0，則集群處於非安全模式。如果值為1，則集群處於混合模式，並且需要在重新啟動服務之前更新CTL檔案。請參閱令牌和無令牌連結。
2. 從發佈者開始，依次導航到群集中的每個伺服器（在Web瀏覽器的各個頁籤中），然後導航到每個訂閱者。導航至**Cisco Unified OS Administration > Security > Certificate Management > Find**。
   選擇CallManager pem Certificate。開啟後，選擇**Regenerate**並等待，直到您看到Success彈出視窗，然後關閉彈出視窗或返回並選擇**Find/List**。
3. 繼續使用後續使用者；按照步驟2中的相同步驟操作，並在集群中的所有訂閱伺服器上完成。如果群集僅處於混合模式且已重新生成CallManager證書 — 請在繼續下一步之前更新CTL Token - Tokenless
4. 登入到Publisher Cisco Unified Serviceability: 導航至**Cisco Unified Serviceability > Tools > Control Center - Feature Services**。從發佈伺服器開始，然後繼續訂閱伺服器，在活動**處重新啟動Cisco** CallManager服務。
5. 導航至**Cisco Unified Serviceability > Tools > Control Center - Feature Services**
   從發佈伺服器開始，然後繼續訂閱伺服器，僅在活**動時重新啟動Cisco CTIManager服務**。
6. 導航至**Cisco Unified Serviceability > Tools > Control Center - Network Services**。
   從發佈伺服器開始，然後繼續訂閱伺服器，重新啟動**思科信任驗證服務**。
7. 導航至**Cisco Unified Serviceability > Tools > Control Center - Feature Services**。
   從發佈伺服器開始，然後繼續使用訂閱伺服器，僅在活動**時重新啟動Cisco TFTP服務**。
8. 重新啟動所有電話： **Cisco Unified CM管理>系統>企業引數**選擇**Reset**，您會看到一個彈出視窗，其中包含**You are about to reset all devices in the system**語句。**此操作無法撤消。繼續？,**選擇**確定，然後選擇重置**

電話現在已重置。通過RTMT工具監控其操作，以確保重置成功且裝置重新註冊到CUCM。 請等待電話註冊完成，然後再繼續下一個證書。此電話註冊過程可能需要一些時間。請注意，在再生過程之前存在不良ITL的裝置在ITL被移除之前不會註冊回集群。

TVS證書

警告： 請勿同時重新生成CallManager.PEM和TVS.PEM證書。 這會導致終端上安裝的ITL與不可恢復的不匹配，需要從集群中的所有終端上刪除ITL。

附註：TVS代表Call Manager驗證證書。最後重新生成此證書。

從發佈者開始，依次導航到群集中的每個伺服器（在Web瀏覽器的各個頁籤中），然後導航到每個訂閱者。 導航至**Cisco Unified OS Administration > Security > Certificate Management > Find**:

- 選擇**TVS pem** Certificate。
- 開啟後，選擇**Regenerate**並等待，直到您看到Success彈出視窗，然後關閉彈出視窗或返回並選擇**Find/List**。

1. 繼續使用後續使用者；按照步驟1中的相同步驟操作，並在集群中的所有訂閱伺服器上完成。所有節點重新生成TVS證書後，重新啟動服務： 登入到Publisher **Cisco Unified Serviceability**。 導航至**Cisco Unified Serviceability > Tools > Control Center - Network Services**。在發佈伺服器上，選擇**Restart** on **Cisco Trust Verification Service**。服務重新啟動完成後，繼續與使用者一起並重新啟動**思科信任驗證服務**。
2. 從發佈伺服器開始，然後繼續使用訂閱伺服器，僅在活動時重新啟動**Cisco TFTP服務。**
3. 重新啟動所有電話： **Cisco Unified CM管理>系統>企業引數**。選擇**Reset**，您會看到一個彈出視窗，其中包含**You are about to reset all devices in the system**語句。**此操作無法撤消。繼續？**,選擇**確定，然後選擇重置。**

電話現在已重置。通過RTMT工具監控其操作，以確保重置成功且裝置重新註冊到CUCM。 請等待電話註冊完成，然後再繼續下一個證書。此電話註冊過程可能需要一些時間。請注意，在再生過程之前存在不良ITL的裝置在ITL被移除之前不會註冊回集群。

ITLR恢復證書

附註：當裝置失去其可信狀態時，會使用ITLRecovery證書。證書出現在ITL和CTL中（當CTL提供器處於活動狀態時）。
如果裝置丟失其信任狀態，可以使用**utils itl reset localkey**命令（對於非安全群集）和**utils ctl reset localkey**（對於混合模式群集）命令。請閱讀Call Manager版本的安全指南，熟悉如何使用ITLRecovery證書以及恢復信任狀態所需的流程。
如果群集已升級到支援2048金鑰長度的版本，且群集伺服器證書已重新生成到2048，並且ITLRecovery尚未重新生成且當前金鑰長度為1024，則ITL恢復命令會失敗，並且不使用ITLRecovery方法。

1. 從發佈者開始，依次導航到群集中的每個伺服器（在Web瀏覽器的各個頁籤中），然後導航到每個訂閱者。 導航至**Cisco Unified OS Administration > Security > Certificate Management > Find**:
   選擇**ITLRecovery pem** Certificate。開啟後，選擇**Regenerate**並等待，直到您看到Success彈出視窗，然後關閉彈出視窗或返回並選擇**Find/List**。
2. 繼續使用後續使用者；按照步驟2中的相同步驟操作，並在集群中的所有訂閱伺服器上完成。
3. 在所有節點重新生成ITLRecovery證書後，需要按以下順序重新啟動服務： 如果您處於混合模式 — 繼續之前更新CTL Token - Tokenless。登入到Publisher **Cisco Unified Serviceability**。導航至**Cisco Unified Serviceability > Tools > Control Center - Network Services**。在發佈伺服器上，選擇**Restart** on **Cisco Trust Verification Service**。 服務重新啟動完成後，繼續與使用者一起並重新啟動**思科信任驗證服務**。

4. 從發佈伺服器開始，然後繼續使用訂閱伺服器，僅在活動時重新啟動**Cisco TFTP服務。**
5. 重新啟動所有電話： **Cisco Unified CM管理>系統>企業引數**選擇**Reset**，您會看到一個彈出視窗，其中包含**You are about to reset all devices in the system**語句。**此操作無法撤消。繼續？,**選擇**確定，然後選擇重置。**
6. 現在，手機在重置時上傳新的ITL/CTL。

刪除過期的信任證書

附註：標識需要刪除、不再需要或已過期的信任證書。請勿刪除五個基本憑證，包括CallManager.pem、tomcat.pem、ipsec.pem、CAPF.pem和TVS.pem。可以刪除適當的信任證書。重新啟動的下一個服務旨在清除這些服務中的舊證書的資訊。

1. 導航至**Cisco Unified Serviceability > Tools > Control Center - Network Services。** 從下拉選單中選擇CUCM Publisher。選擇**停止**證書更改通知。對集群中的每個Call Manager節點重複上述操作。如果您有IMP伺服器： 從下拉選單中，逐一選擇您的IMP伺服器，然後選擇**Stop Platform Administration Web Services**和**Cisco Intercluster Sync Agent。**
2. 導航至**Cisco Unified OS Administration > Security > Certificate Management > Find。** 查詢過期的信任證書。(對於10.X及更高版本，可以按「過期」進行過濾。對於低於10.0的版本，您需要手動識別特定證書，如果收到，則需要通過RTMT警報識別這些證書。)同一信任證書可能出現在多個節點中。必須從每個節點單獨刪除它。選擇要刪除的信任證書（取決於您獲得彈出視窗或導航到同一頁上的證書的版本） 選擇**Delete。**(您將看到以「您將永久刪除此證書」開頭的彈出視窗。)選擇**OK。**
3. 對每個要刪除的信任證書重複該過程。
4. 完成後，需要重新啟動與刪除的證書直接相關的服務。在本節中，您無需重新啟動電話。Call Manager和CAPF會對終端產生影響。 Tomcat-trust:通過命令列重新啟動Tomcat服務（請參閱Tomcat部分）CAPF-trust:重新啟動Cisco證書頒發機構代理功能（請參閱CAPF部分）不重新啟動終端。CallManager-trust:CallManager服務/CTIManager（請參閱CallManager部分）不重新啟動端點。 影響端點並導致重新啟動。IPSEC-trust:DRF Master/DRF本地（請參見IPSEC部分）。TVS（自簽名）沒有信任證書。
5. 重新啟動之前在步驟1中停止的服務。

驗證

驗證程式對於此配置不可用。

疑難排解

此配置的故障排除過程不可用。

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）。