

實施對CallManager的多SAN Tomcat證書的重複使用

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[重用CallManager的Tomcat證書](#)

[驗證](#)

簡介

本文檔介紹有關如何在CUCM上重新使用CallManager的Multi-SAN Tomcat證書的分步過程。

必要條件

需求

思科建議您瞭解以下主題：

- 思科整合通訊管理員(CUCM)
- CUCM證書
- 身份信任清單(ITL)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CUCM版本15 SU1

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。

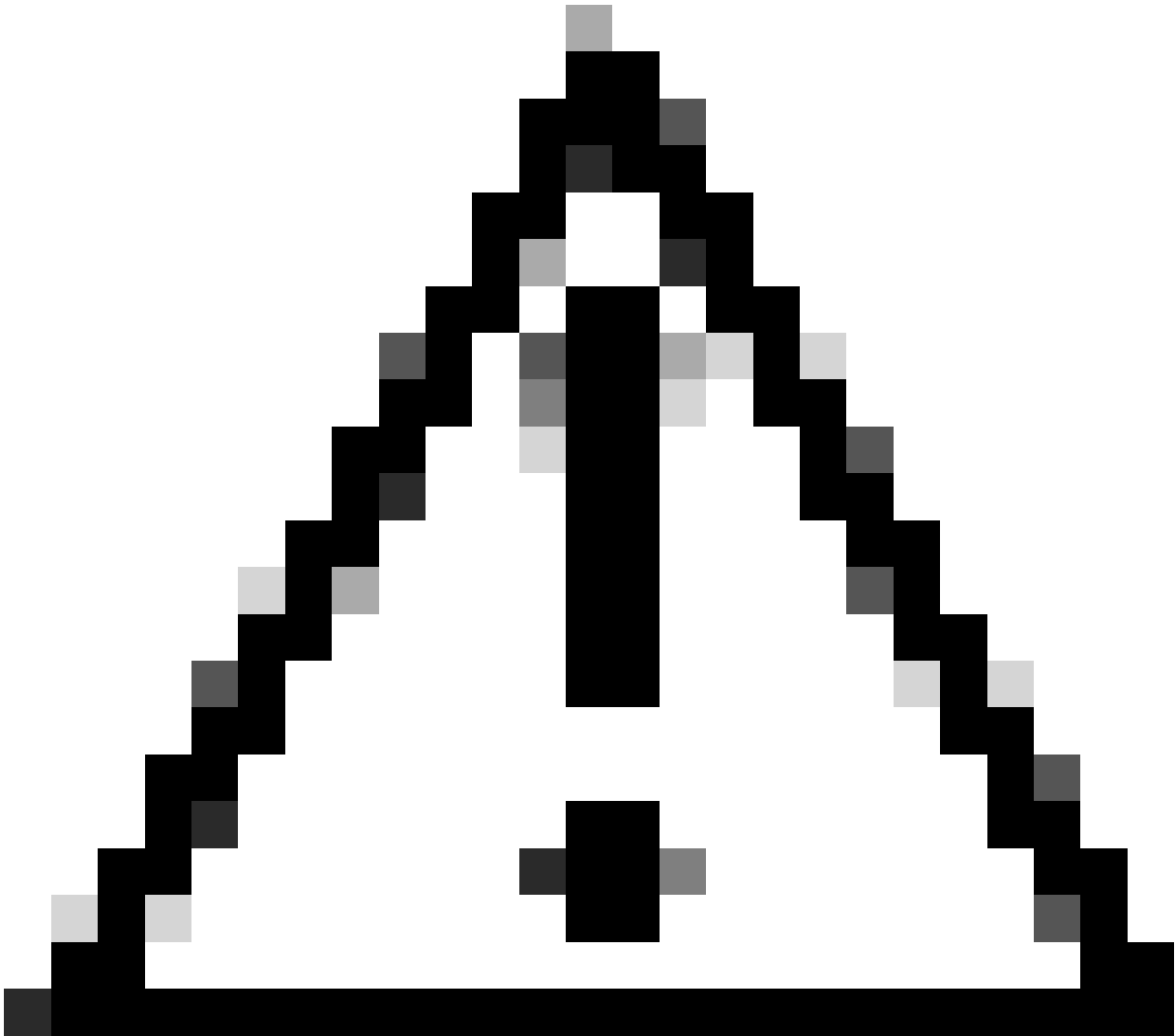
背景資訊

CUCM的早期版本對整個集群的每個服務使用不同的證書，從而增加了證書數量和成本。這包括Cisco Tomcat和Cisco CallManager，它們是在CUCM上運行的關鍵服務，也具有各自的身份證書。

從CUCM版本14開始，增加了一項新功能，以重新使用Multi-SAN Tomcat證書進行CallManager服

務。

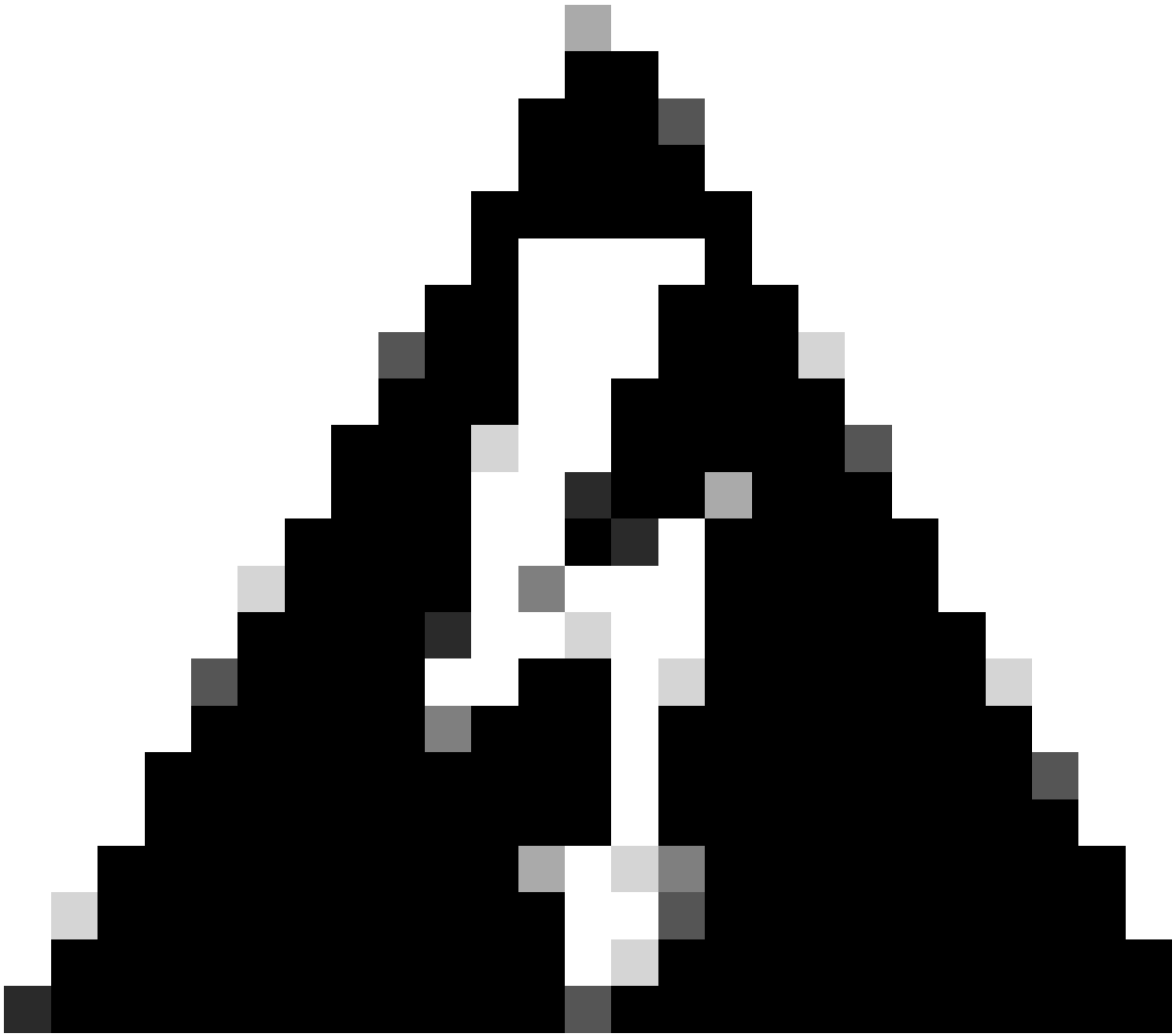
使用此功能的優點是，您可以從CA取得一個憑證，並將其用於多個應用程式。這確保了成本最佳化和管理的減少，並減少了國際交易日誌檔案的大小，從而減少了開銷。



注意：在繼續重新使用配置之前，請確保Tomcat證書為多伺服器SAN證書。Tomcat多SAN證書可以是自簽名或CA簽名。

設定

重用CallManager的Tomcat證書



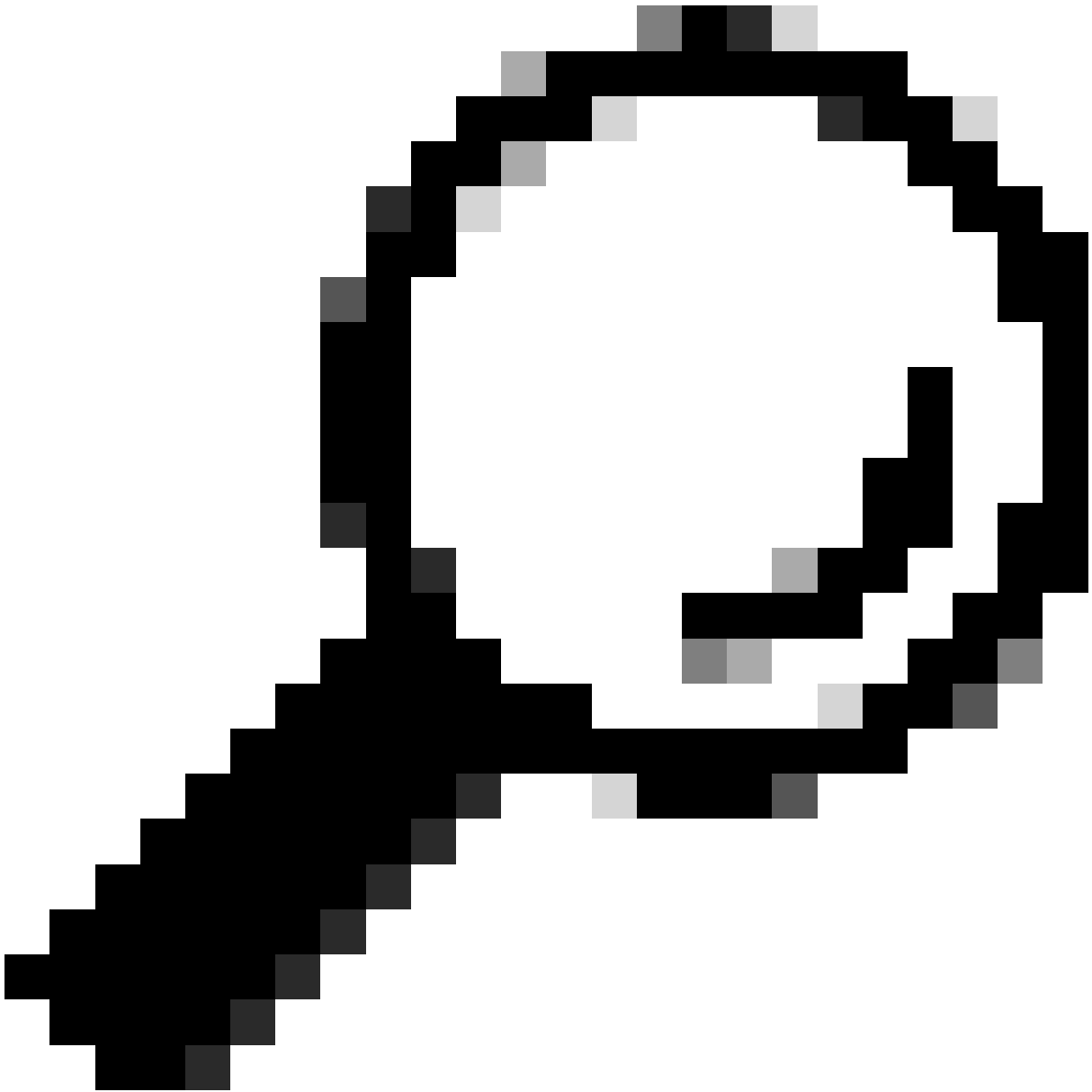
警告：繼續進行之前，請確認叢集處於混合模式或非安全模式。

步驟 1. 導航到Cisco Unified CM管理>系統>企業引數：

檢查Security Parameters部分，並驗證Cluster Security Mode設定為0還是1。如果值為0，則叢集處於非安全模式。如果是1，則叢集處於混合模式，您需要在重新啟動服務之前更新CTL檔案。

步驟 2. 導航到CUCM發佈伺服器，然後導航到思科統一作業系統管理>安全>證書管理。

步驟 3. 將Multi-SAN Tomcat CA Certificate Chain上傳到CallManager Trust儲存。



提示：如果您使用用於Tomcat的自簽名多伺服器SAN證書，則可以跳過此步驟。



在重新使用證書之前，請確保手動將CA證書鏈（簽署tomcat身份證書）上傳到CallManager信任庫。

當您將tomcat證書鏈上傳到CallManager信任時，請重新啟動這些服務。

- CallManager：Cisco HAProxy服務
- CallManager-ECDSA：Cisco CallManager服務和Cisco HAProxy服務

步驟 4. 按一下Reuse Certificate。將會顯示「將Tomcat憑證用於其他服務」頁面。

Use Tomcat Certificate For Other Services

 Finish  Close

Status



Tomcat-ECDSA Certificate is Not Multi-Server Certificate



Tomcat Certificate is Multi-Server Certificate

Source

Choose Tomcat Type*

tomcat

Replace Certificate for the following purpose

CallManager

CallManager-ECDSA

Finish

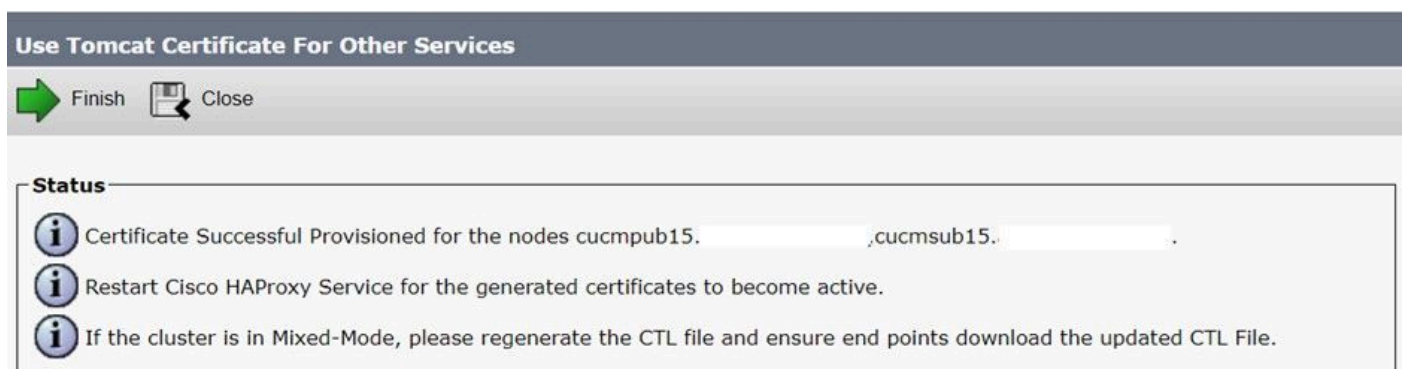
Close

步驟 5. 從Tomcat type 下拉選單中選擇Tomcat或Tomcat-ECDSA。

步驟 6. 在Replace Certificate for the following purpose窗格中，根據之前步驟中選擇的證書選中CallManager或CallManager-ECDSA 覈取方塊。

注意：如果選擇Tomcat作為證書型別，則會啟用CallManager作為替換。如果選擇tomcat-ECDSA作為證書型別，則會啟用CallManager-ECDSA作為替換。

步驟 7. 按一下完成將CallManager證書替換為tomcat多伺服器SAN證書。



Use Tomcat Certificate For Other Services

Finish Close

Status

- Information Certificate Successful Provisioned for the nodes cucmpub15. . . , cucmsub15. . . .
- Information Restart Cisco HAProxy Service for the generated certificates to become active.
- Information If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

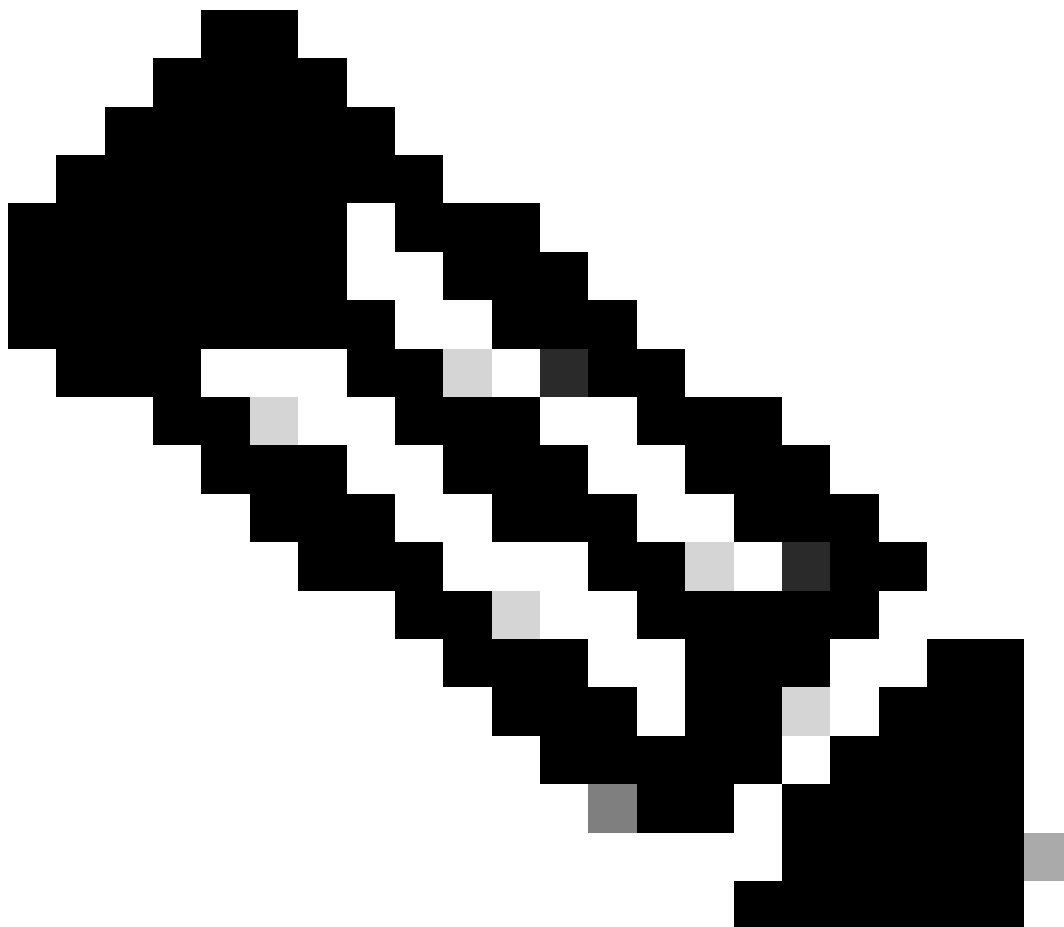
步驟 8. 透過CLI執行utils service restart Cisco HAProxy命令，在集群的所有節點上重新啟動Cisco HAProxy服務。

```
admin:utils service restart Cisco HAProxy
Stopping Cisco HAProxy...

Cisco HAProxy [STOPPED] Service Activated
Starting Cisco HAProxy...
Cisco HAProxy [STARTED]
admin:█
```

步驟 9. 如果集群處於混合模式，請透過CUCM發佈伺服器的CLI運行命令utils ctl update CTLFile更新CTL檔案，然後繼續重置電話以獲取新的CTL檔案。

驗證



注意：重複使用證書時，CallManager證書不會在GUI上顯示。

您可以從CLI運行命令來確認CallManager是否重新使用Tomcat證書。

- show cert list own

```
admin:show cert list own  
  
tomcat/tomcat.pem: Certificate Signed by AKASH-WINSERVLAB-CA  
tomcat-ECDSA/tomcat-ECDSA.pem: Self-signed certificate generated by system  
ipsec/ipsec.pem: Self-signed certificate generated by system  
ITLRecovery/ITLRecovery.pem:  
CallManager-ECDSA/CallManager-ECDSA.pem: Self-signed certificate generated by system  
CallManager/CallManager.pem: Reusing tomcat certificate for CallManager  
TVS/TVS.pem: Self-signed certificate generated by system  
  
admin:█
```


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）。