對由於證書過期造成的CUCM群集備份故障進行故障排除

目錄

問題

使用災難恢復系統(DRS)的CUCM群集備份失敗。在排除備份故障期間，嘗試從CUCM發佈伺服器訪問IMP節點時遇到證書異常。證書驗證發現群集內的多個證書已過期，包括IMP發佈伺服器和IMP訂閱伺服器節點的Tomcat信任證書。在IMP發佈伺服器上，發現cup、cup-xmpp和tomcat證書已過期，而tomcat證書顯示為CUCM發佈伺服器上舊的多伺服器證書。

環境

- Cisco Unified Communications Manager(CUCM)集群部署
- Cisco Unified IM and Presence(IMP)發佈者和訂閱者節點
- 為群集備份配置的災難恢復系統(DRS)
- 為備份儲存配置的SFTP伺服器
- 多個過期的證書影響群集通訊

解析

要解決由於證書過期而導致的CUCM群集備份故障，請複查以下步驟以續訂必要的證書並重新啟動所需的服務：

步驟 1:在所有群集節點上續訂Tomcat證書和IPsec證書

在群集中的每個節點上續訂Tomcat證書。您可以選擇每個節點的單個自簽名證書，也可以從CUCM

Publisher生成多伺服器tomcat證書並部署到所有節點。

1.在每個節點上導航到OS Administration > Security > Certificate Management，以續訂Tomcat證書。在群集中的每個節點上續訂IPsec證書。

步驟 2:續訂CUP和CUP-XMPP證書

在所有節點上完成Tomcat證書續訂後，繼續續訂受影響的IMP節點上的cup和cup-xmpp證書。

1.導航至Cisco Unified IM and Presence Serviceability > Security > Certificate Management以續訂這些證書。

步驟 3:重新啟動所需的服務

完成證書更新後，重新啟動每個節點指示和需要的服務。系統顯示證書續訂後必須重新啟動哪些服務。

步驟 4:驗證DRF服務狀態

確認DRF主服務正在CUCM發佈伺服器上運行，DRF本地服務正在群集中的所有節點上運行。

1.導航至Cisco Unified Serviceability > Tools > Control Center - Feature Services，以驗證和啟動DRF服務：

- DRF主機必須在CUCM發佈伺服器上運行
- DRF Local必須在所有群集節點上運行

步驟 5:測試手動備份和收集日誌

完成證書續訂和服務重新啟動後，測試手動備份功能並收集RTMT日誌進行分析：

1.導航到Cisco Unified CM管理>系統>備份和恢復>手動備份以啟動測試備份。使用即時監控工具(RTMT)收集以下日誌：

- 來自CUCM發佈伺服器的DRF主日誌
- 來自群集中所有節點的DRF本地日誌

原因

CUCM群集備份失敗是由群集環境中的過期證書引起的。具體而言，IMP發佈伺服器和IMP訂閱伺服器節點的Tomcat信任證書已過期，以及IMP發佈伺服器上的cup、cup-xmpp和tomcat證書。過期的證書阻止了群集節點之間的正確SSL/TLS通訊，這是災難恢復系統(DRS/BARS)成功執行群集範圍的備份操作所必需的。IMP Publisher上的tomcat證書被標識為CUCM Publisher中未正確續訂的舊多伺服器證書。

相關內容

- Cisco Unified IM and Presence配置和管理指南
- 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）。