解決由於不受支援的GoDaddy R1證書鏈導致的Webex呼叫生存性網關同步失敗

目錄

問題

兩個生存性網關(mcyitsrtr001.centralwire.com和pritsrtr001.centralwire.com)在控制中心中註冊，但無法同步；故障排除重點是mcyitsrtr001.centralwire.com。同步嘗試始終失敗，錯誤消息為：

```
Sync failed due to internal server error (code - 31117)
```

第一次觀察是在2026年8月5日的同步嘗試中。對遙測和Webex後端（網橋）日誌的分析顯示，網關呈現的是GoDaddy R1v1證書鏈（GoDaddy TLS根CA - R1層次結構），而Webex服務不支援該證書鏈，從而導致證書鏈被拒絕和同步失敗。

環境

- 報告了兩個託管網關：mcyitsrtr001.centralwire.com和prtitsrtr001.centralwire.com (故障排除重點是mcyitsrtr001.centralwire.com)
- IOS® XE版本：17.12.6（SGW節點），17.15.06(MGW)
- Webex通話存留閘道(SGW)組態
- 使用R1v1中間CA的GoDaddy TLS證書鏈
- 證書鏈：CN=mcyitsrtr001.centralwire.com → GoDaddy TLS中間CA DV - R1v1 → GoDaddy TLS根CA - R1

解析

通過實施證書交叉簽名工作區來建立受信任的證書路徑解決了此問題。該解決方案涉及安裝GoDaddy R1到G2交叉簽名證書，以將較新的GoDaddy R1層次結構連結到受信任的Go Daddy Root Certificate Authority - G2。



附註：在證書更改期間，crypto pki trustpool import clean命令中斷了網關的NETCONF-YANG/DMI服務，使聯結器暫時離線。無法開啟套接字到192.168.217.55:830)。 這是通過步驟6-7恢復的，是維護的副作用，而不是最初的同步故障。

步驟 1:安裝思科Trustpool捆綁包

安裝包含Go Daddy Root Certificate Authority - G2的Cisco trustpool捆綁包:

```
crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_union.p7b
```

匯入clean將替換整個trustpool — 它可以中斷依賴它的服務（請參閱前面列出的connector-offline註釋）。 請謹慎使用。

步驟 2:驗證G2根證書

確認Go Daddy Root Certificate Authority - G2存在：

```
show crypto pki trustpool | include GoDaddy|Go Daddy
```

步驟 3:刪除自簽名R1信任點

刪除舊的自簽名R1信任點(在提示刪除證書時回答yes):

```
no crypto pki trustpoint GoDaddyRootR1
```

步驟 4:安裝交叉簽名的R1證書

使用交叉簽名的R1證書建立一個新的信任點(Subject:GoDaddy TLS根CA - R1，頒發者：Go Daddy Root Certificate Authority - G2):

```
crypto pki trustpoint GoDaddyCrossR1
enrollment terminal
revocation-check none
exit
crypto pki authenticate GoDaddyCrossR1
<paste cross-signed R1 PEM — Subject: GoDaddy TLS Root CA - R1, Issuer: Go Daddy Root Certificate Autho
quit
yes
```

步驟 5:驗證憑證鏈結

驗證鏈現在是否正確解析：

```
show crypto pki certificates webex-sgw
show crypto pki certificates GoDaddyCrossR1
```

步驟 6:重新啟動NETCONF服務

退回HTTP(S)伺服器和NETCONF-YANG服務（在禁用和啟用之間等待約60秒）：

```
conf t
no netconf-yang
no ip http secure-server
no ip http server
end
```

等待60秒，然後重新啟用：

```
conf t
```

```
ip http server
ip http secure-server
netconf-yang
end
write memory
```

步驟 7:重新載入閘道（如有必要）

如果在服務重新啟動後NETCONF-YANG仍無法正常提供服務，請重新載入路由器以完全重新初始化DMI:

```
reload
```

注意：有可能。此處提到的詳細資訊似乎包含執行後可能會產生重大影響的過程或命令。請確保上述程式或命令已由SME或業務部門在執行或推薦之前進行評估。

步驟 8:驗證解析度

網關重新聯機後，從Control Hub觸發SGW重新同步，並驗證同步是否成功完成，沒有錯誤代碼31117或「Certificate Server Trusted check failed」消息。已確認已解決 — 網關呈現完整枝葉→ R1v1 → R1（頒發者G2）鏈，並且在交叉符號解決方法後成功完成同步。

原因

根本原因確定為證書信任失敗。可生存性網關使用GoDaddy TLS根CA - R1層次結構（具體是GoDaddy TLS中間CA DV - R1v1）呈現證書鏈，該證書鏈未包含在Webex Calling的受信任證書授權清單中。

當Webex後端（掛架）在SIP身份驗證資訊請求期間執行伺服器證書信任檢查時，它無法建立到受信任的根證書的有效證書路徑。這導致出現SunCertPathBuilderException，並出現錯誤「unable to find valid certification path to requested target」，導致HTTP 400響應和同步中斷。

Webex Calling只信任較舊的GoDaddy/Starfield根（例如Go Daddy Root Certificate Authority -

G2），而不信任較新的「GoDaddy TLS」(R1/R1v1)層次結構。

相關內容

- 支援的Webex混合服務證書頒發機構
- GoDaddy證書儲存庫
- 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）。