

排除FDM上的高可用性配對故障

目錄

問題

在應用同步期間，運行FTD 7.4.2.4的兩台Cisco Firepower 1120裝置之間的高可用性(HA)配對失敗，因為許可證註冊模式不匹配，輔助節點始終進入「失敗」狀態。遇到的特定錯誤消息為：

```
CD App Sync error FDM validation failure License registration mode mismatch between Primary and Secondary
```

show app-sync-history命令顯示以下消息重複失敗：

```
App Sync Status: FAILURE  
Failed Reason: FDM validation failure - License agent compliance mismatch between Primary and Secondary
```

此問題發生在兩個防火牆重設、組態從備份中復原、軟體更新到FTD版本7.4.2.4、VDB和Snort版本更新，以及許可證重新套用新的權杖之後。輔助防火牆仍處於「失敗」狀態，從而防止HA完成並影響防火牆冗餘。

環境

- 為高可用性配置的Cisco Firepower 1120 NGFW裝置
- Firepower威脅防禦(FTD)版本7.4.2.4-9
- Snort檢測引擎：3.1.53.203 - 175
- VDB:425.0
- 地理位置資料庫：2026-03-07-053
- 從智慧許可模式轉換為PLR (永久許可證保留) 模式的裝置

- PLR轉換後嘗試雲連線的主裝置
- 兩台裝置均從備份中恢復

解析

解決方法涉及識別和糾正主裝置和輔助裝置之間的許可證註冊模式不匹配、執行雲註銷以及完成完全部署。

步驟 1:確定許可證註冊模式不匹配

通過檢查應用同步歷史記錄以確認兩台裝置上的許可證註冊模式，瞭解具體的故障原因：

```
show app-sync-history
```

輸出顯示的故障表明：

```
FDM validation failure - License registration mode mismatch between Primary and Secondary node
```

步驟 2:執行雲註銷

從智慧許可模式轉換為PLR模式後，主裝置仍在嘗試雲連線，因此需要註銷雲。

在FDM UI中配置臨時代理（如果沒有配置代理）：

導覽至System Settings > See More > HTTP Proxy索引標籤，並暫時設定虛擬代理[稍後可移除]。

SSH進入FTD裝置並執行聯結器指令碼：

```
ssh admin@<device-ip>
```

```
expert
sudo su
/ngfw/var/sf/bin/connector.sh
```

步驟 3:解決埠8989衝突

如果聯結器指令碼失敗並出現以下錯誤：

```
Error: listen tcp :8989: bind: address already in use
```

使用埠8989 (通常為Cisco Success Network) 識別和終止流程：

```
netstat -tulpn | grep 8989
kill <pid>
```

步驟 4:完成雲註銷

解決埠衝突後重新運行聯結器指令碼：

```
/ngfw/var/sf/bin/connector.sh
```

成功執行必須顯示與以下內容類似的輸出：

```
Starting connector
INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: https_proxy=http://1xx.xx.x
INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: http_proxy=http://1xx.xx.x
```

轉到FDM GUI，「系統設定」>「雲服務」>「雲服務」，然後按一下「取消註冊」選項。驗證裝置是否已從雲服務中註銷。

步驟 5:執行完全部署並恢復HA

在雲註銷後，如果HA配對仍失敗，並且出現相同的許可證不匹配錯誤，請通過FDM介面在活動裝置上執行完全部署。

導覽至Deploy > Deploy Now，然後完成部署過程。

部署完成後，請重試HA形成。裝置必須成功地與已連線介面形成主用 — 備用HA對並處於就緒狀態。

步驟 6:驗證HA狀態

確認成功的HA形成：

```
show failover
```

輸出必須顯示兩個單元處於正確HA狀態，並且同步成功。

原因

根本原因是主Firepower 1120裝置和輔助Firepower裝置之間的許可證註冊模式不匹配。裝置已從智慧許可模式轉換為PLR（永久許可證保留）模式；但是，主裝置繼續嘗試雲連線，導致HA驗證期間許可證代理/匯出合規性狀態不匹配。這導致在應用程式同步期間反復發生FDM/FIM驗證失敗。此外，雲註銷最初被與Cisco Success Network相關的埠8989衝突阻止，該衝突需要解決才能繼續註銷。

相關內容

- [在氣隙網路中應用永久許可證](#)

- [重新映像安全防火牆威脅防禦](#)
- [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）。