從7.4.3升級到7.6.4後FTD管理介面故障

目錄

問題

將思科安全防火牆3130威脅防禦(FTD)高可用性(HA)對從版本7.4.3升級到版本7.6.4後，主裝置在防火牆管理中心(FMC)上的完成率似乎達到99%，並且變得無響應。輔助裝置已成功升級，並在HA對中變為活動狀態。主裝置沒有響應SSH連線，FMC無法與其通訊。

經調查，在FXOS上發現了此嚴重故障：

```
Critical  F1000398 2026-08-14T20:52:06.297     58437 [FSM:FAILED]: out-of-band interface configuration(
```

FTD升級記錄顯示升級實際已順利完成（100%完成），但SFTunnel服務並未正確啟動，導致FTD和FMC之間的通訊無法進行。裝置可以ping通自身、其網關和對等FTD單元，但無法到達位於不同子網上的FMC。

環境

- Cisco安全防火牆3130威脅防禦HA配對
- 原始軟體版本：FTD 7.4.3
- 目標軟體版本：FTD 7.6.4（內部版本69）
- Cisco Firepower可擴展作業系統(FX-OS)v2.16.1（內部版本147）
- 配置了靜態IP地址的管理介面
- 位於FTD管理網路不同子網中的FMC伺服器

解析

在受影響的FTD裝置上完全重新設定管理介面後，問題得以解決。已執行以下步驟：

步驟 1:由於SSH不起作用，請透過主控台存取連線到FTD。

步驟 2:通過檢查升級日誌來驗證升級完成狀態：

```
root@device:/ngfw/var/log/sf/Cisco_FTD_SSP_FP3K_Upgrade-7.6.4# cat status.log
```

步驟 3:確認FXOS上的管理介面故障：

```
device# show fault
```

步驟 4:嘗試通過重新配置管理IP地址進行基本故障排除（這未解決問題）。

步驟 5:執行冷重新啟動（這未解決問題）。

步驟 6:從FTD CLI完全停用management0介面：

```
configure network management-interface disable management0
```

步驟 7:重新啟用management0介面：

```
configure network management-interface enable management0
```

步驟 8:重新配置管理介面的網路設定：

```
configure network ipv4 manual <ip_address> <netmask> <gateway>
```

步驟 9:確認FXOS警報已清除，且FTD現在可以ping通FMC:

```
root@device:/# ping <FMC_IP_address>
```

步驟 10:使用manage_procs.pl指令碼重新啟動SFTunnel服務：

```
manage_procs.pl restart sftunnel
```

步驟 11:驗證SFTunnel連線：

```
root@device:/# sftunnel_status.pl
```

步驟 12:測試故障轉移功能以確保HA操作正常運行。

完成這些步驟後，FTD能夠與FMC正確通訊，並且所有連線和故障轉移測試均成功。然後，可以應用修補程式升級，而不會出現問題。

原因

根本原因是管理介面未能在FTD從7.4.3升級到7.6.4後正確初始化，儘管升級程式已成功完成。帶外管理介面配置有限狀態機(FSM)在升級過程中失敗，導致管理介面無法建立正確的連線。此行為已記錄在Cisco錯誤ID CSCww08417中。

此問題類似於先前報告的思科錯誤ID CSCwj04154和思科錯誤ID CSCwa69303缺陷，但在不同條件下發生。管理介面故障在99%完成時產生了升級失敗的假象，實際上升級已成功完成，但管理連線已斷開。

相關內容

- 思科錯誤ID CSCww08417 - FTD管理介面可能無法升級後啟動

- 思科安全防火牆威脅防禦相容性指南
- 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）。