

CLISH Ping/Traceroute長時間運行期間鎖定和部署停滯

目錄

問題

在Cisco Secure Firewall Firepower平台 (7.6.4、7.7和10.0.0版) 上，當對同一裝置啟用多個SSH會話時，使用CLISH CLI在一個會話中執行長時間運行的命令 (如連續ping) 會阻止其他CLI命令在其他會話或CLISH中完成。例如，如果管理員在一個SSH CLISH會話中啟動連續ping並嘗試在另一個CLISH會話中執行show命令，則後續命令將掛起，直到長時間運行的命令完成或中止。在某些版本中，無法中止該長時間運行的ping。CLISH，導致CLISH或部署鎖定。直接使用專家模式或LINA引擎(通過系統支援diagnostic-cli)允許在不發生此阻止行為的情況下運行。

環境

- 思科安全防火牆Firepower硬體平台：1000、1200和4200系列
- 軟體版本：7.6.4、7.7、10.0.0
- 多個SSH會話 (相同或不同的使用者) 連線到同一裝置
- CLISH CLI介面
- 專家模式和LINA診斷CLI用法
- 使用命令進行測試：ping、traceroute、show sip、show ip、show conn、show xlate
- 在FPR1010、FPR1200和FPR4200裝置上重現的問題
- 相關缺陷：CSCws82823、CSCwb84748

解析

問題顯示以下症狀：

- 使用不同的或相同的使用者憑證建立到裝置的兩個SSH會話。
- 在作業階段1中，從FTD CLISH提示中，執行長時間執行、且重複計數較高的執行ping。

```
> ping 1.1.1.1 repeat 2000
```

注意：如果進行測試，請使用較小的計數數字嘗試此操作，例如2000可能需要幾個小時才能完成。

注意：CLISH中的ping/traceroute不會顯示任何通常在LINA CLI中直接看到的進度字元。

- 在作業階段2中，嘗試在CLISH中執行另一個LINA命令，例如「show sip」。

```
> show sip
```

- Session 2中的命令不會完成，直到Session 1中的ping完成或被中止。

此解決方案可用：

- 使用Ctrl+C中止初始延長命令，以避免CLISH鎖定和部署停滯。
- 在受影響的版本中，Ctrl+C或關閉SSH會話無法中止CLISH中長時間運行的ping。
- 如果嘗試操作，後端程式將繼續執行，CLISH對其他LINA命令保持鎖定狀態。
- 如果發現FTD處於這種狀態，或懷疑是FTD已透過停滯的長時間ping進入這種狀態，則需要重新啟動FTD才能復原。
- 要避免CLISH/部署鎖定，請直接使用LINA引擎運行LINA命令。此方法不會顯示有缺陷的行為。

```
> system support diagnostic-cli  
firepower# ping 1.1.1.1 repeat 2000
```

- 通過LINA診斷CLI執行的命令不會阻止其他會話中的CLISH或部署進程。但是，系統支援diagnostic-cli只允許每個會話有一個CLI使用者。

其他注意事項和意見：

- - Traceroute指令通常可在CLISH中中止，但可能會導致其他作業階段中的新LINA指令發生臨時停滯（約3分鐘）。
 - 如果長時間運行的ping在CLISH中處於活動狀態，則從Secure Firewall Management Center或Device Manager啟動的部署操作可能會被延遲或阻止，因為這兩個進程都使用同步方法並等待完成（最長10分鐘）。
 - 這種阻塞行為是為同步過程操作設計的；然而，無法中止是由於缺陷引起的。

原因

根本原因是一個缺陷(Cisco錯誤ID CSCws82823)，該缺陷無意中從CLISH中的某些CLI命令中刪除了所需的代碼，從而使LINA引擎無法正確識別和管理長時間運行的命令。這導致Ctrl+C中止功能丟失，並導致CLISH鎖定，阻止其他命令和部署操作，直到長時間運行的命令完成。阻塞行為是因為CLISH命令處理的同步性質。

相關內容

- [思科安全防火牆威脅防禦命令參考：使用命令列介面\(CLI\)](#)
- [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）。