解決由登入阻止安靜模式導致的IOS XE裝置上的間歇性SSH訪問故障

目錄

問題

運行IOS XE軟體的裝置出現間歇性SSH訪問故障。有時會接受SSH連線，有時會以不一致的模式被拒絕。對裝置的控制檯訪問不會受到影響。對於失敗的SSH會話，在受影響的裝置上執行的資料包捕獲會確認裝置本身在收到客戶端的TCP SYN後立即傳送TCP RST資料包，甚至在SSH會話開始協商之前。啟用debug ip tcp transactions 指令後，以下偵錯輸出說明了TCP RST行為：

```
Aug 21 19:46:04.697: Reserved port 0 in Transport Port Agent for TCP IP type 0
Aug 21 19:46:04.697: TCP: sending RST, seq 0, ack 1013312911
Aug 21 19:46:04.697: TCP: sent RST to 10.x.x.x:43266 from 10.x.x.x:22
Aug 21 19:46:04.698: Released port 0 in Transport Port Agent for TCP IP type 0 delay 0
Aug 21 19:46:04.698: TCP0: state was LISTEN -> CLOSED [0 -> UNKNOWN(0)]
Aug 21 19:46:04.698: TCB destroyed
```

驗證以下專案，以排除它們作為起作用的原因：

- 使用命令show ip ssh確認裝置上已啟用SSH。
- 使用命令show tcp brief確認TCP埠22正在監聽IOSd進程。
- show ip traffic或debug ip error命令輸出中沒有「no port」錯誤
- 未完全衝減VTY行；show line的命令輸出沒有顯示所有線路忙。
- 刪除VTY線路上的任何訪問類配置後，問題仍然存在。

裝置日誌記錄緩衝區顯示大量重複的身份驗證失敗，以及處於活動狀態的安靜模式：

```
Aug 21 12:24:32: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: test_user] [Source: LOCAL] [localport:
Aug 21 12:24:32: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failures is 0 secs, [user: tes
```

出現故障時的show login輸出顯示SSH出現故障時裝置處於靜默模式。

環境

- 平台:Cisco Catalyst 9500系列交換器（核心交換器和管理式交換器堆疊）
- SSH已啟用，用於遠端訪問裝置
- 裝置上的登入塊配置處於活動狀態：login block-for 120 attempts 3 within 60

解析

此問題是由大量失敗的身份驗證嘗試持續觸發Login Block quiet模式功能引起的。要解決此問題，請為受信任的SSH管理裝置使用安靜模式訪問類ACL。

使用安靜模式受信任IP訪問類ACL配置登入塊

配置登入塊功能並實施安靜模式訪問類ACL（訪問控制清單）。 此ACL允許受信任的管理主機和子網繞過靜默模式強制執行，同時對於所有其他源，登入塊保護保持活動狀態。

1.定義允許受信任的管理主機和子網的命名擴展ACL。以下示例允許兩個特定的跳轉主機IP和一個/22管理子網。調整條目以匹配環境中的受信任管理源：

```
device# configure terminal
device(config)# ip access-list extended quietmode_trusted_ip
device(config-ext-nacl)# 10 permit ip host <trusted_host_1_ip> any
device(config-ext-nacl)# 20 permit ip host <trusted_host_2_ip> any
device(config-ext-nacl)# 30 permit ip <subnet_address> <wildcard_mask> any
device(config-ext-nacl)# exit
```

對於ACL條目構造：

- 使用host關鍵字，後跟單個IP地址，以允許特定管理主機（例如，跳轉伺服器）。

- 要允許整個子網，請指定網路地址，後跟相應的萬用字元掩碼。

2.將ACL套用到安靜模式訪問類，這樣，即使安靜模式處於活動狀態，也允許與ACL匹配的源連線：

```
device(config)# login quiet-mode access-class quietmode_trusted_ip
device(config)# end
```

3.如果刪除了login block-for 配置命令，請重新啟用：

```
device# configure terminal
device(config)# login block-for 120 attempts 3 within 60
device(config)# end
```

4.儲存配置：

```
device# write memory
```

5.監視系統日誌，觀察安靜模式是否繼續被觸發，以及當前登入模式：

```
device# show logging
device# show login
```

解決持續身份驗證失敗的根本原因

上述基於ACL的解決方法可解決症狀（安靜模式阻止的SSH），但無法解決根本原因，即反複身份驗證失敗的數量較多。這些故障會持續觸發安靜模式。為了充分解決這一問題，需要研究和解決頻繁的認證問題。

原因

間歇性SSH訪問失敗是由大量反複失敗的身份驗證嘗試導致IOS-XE Login Block功能進入安靜模式造成的。login block-for配置示例：

```
login block-for 120 attempts 3 within 60
```

此配置指示IOS XE裝置進入靜默模式，並在60秒視窗中檢測到3次或更多失敗的登入嘗試時，在120秒內阻止所有新的登入連線。大量失敗的身份驗證嘗試持續觸發登入安靜模式。安靜模式實施是全域性性的，適用於為SSH配置的所有VTY線路和所有TCP埠。當靜默模式處於活動狀態時，裝置在收到來自靜默模式訪問類ACL未明確允許的任何源的新TCP SYN資料包後立即傳送TCP RST資料包，從而阻止建立SSH會話。

相關內容

- Cisco IOS-XE安全配置指南：登入增強功能（login block-for和quiet-mode access-class）
- 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）。