排除由於空閒noTTY會話而導致的ASR5500登入問題

目錄

[簡介](#)
[ASR5500節點的登入問題](#)
[故障排除步驟](#)
[根本原因分析](#)
[建議的解決方案](#)
[相關資訊](#)

簡介

本文描述如何排除當安全外殼(SSH)連線丟失至聚合服務路由器(ASR5500/ASR 5000)的管理IP時的故障。

ASR5500節點的登入問題

您無法登入到ASR5500資料包核心節點。SSH連線會立即終止，而不會出現登入提示。Telnet連線表現出相似的行為。

故障排除步驟

步驟1.嘗試通過控制檯連線登入到節點。

步驟2.在大多數情況下，不會發出可能指向連線失敗原因的特定簡單網路管理協定(SNMP)陷阱。

步驟3.系統日誌中始終存在的與登入相關的日誌為：

```
evlogd: [local-60sec55.607] [tacacs+ 37201 error] [5/0/8908 <vpnmgr:1> authen_events.c:598]
[software internal system critical-info syslog] Authentication failed for user **** on tty
/dev/pts/0, application ssh, remote IP address XX.XX.XX.XX
evlogd: [local-60sec55.623] [cli 30028 debug] [5/0/8908 <vpnmgr:1> luser_auth.c:1448] [context:
local, contextID: 1]  [software internal system syslog] Login attempt failure for user **** IP
address XX.XX.XX.XX - Access type ssh/sftp
evlogd: [local-60sec53.652] [tacacs+ 37201 error] [5/0/8908 <vpnmgr:1> authen_events.c:598]
[software internal system critical-info syslog] Authentication failed for user **** on tty
/dev/pts/0, application ssh, remote IP address XX.XX.XX.XX
evlogd: [local-60sec53.679] [cli 30028 debug] [5/0/8908 <vpnmgr:1> luser_auth.c:1448] [context:
local, contextID: 1]  [software internal system syslog] Login attempt failure for user **** IP
address XX.XX.XX.XX - Access type ssh/sftp#####
evlogd: [local-60sec2.942] [tacacs+ 37201 error] [5/0/8908 <vpnmgr:1> authen_events.c:598]
[software internal system critical-info syslog] Authentication failed for user epcats on tty
/dev/pts/0, application ssh, remote IP address YY.YY.YY.YY
```

步驟4.命令**show crash list all**顯示最近的崩潰，請注意，與**vpnmgr**相關的崩潰尤其重要。

步驟5.命令**show task resources all** 確保**vpnmgr**和**sshd**進程不能處於超狀態狀態。**vpnmgr**負責IP地

址池管理，並執行所有情景特定的操作。**sshd**支援安全登入到StarOS CLI。

步驟6.重新啟動**vpnmgr**例項1.有助於返回SSH連線，在某些情況下產生的影響最小。但是，連線可能會在一段時間後終止。

步驟7. MIO切換解決了問題。請注意，在進程可能達到閾值或過載的情況下，MIO退回可以幫助您清除它。

現有解決方法是MIO切換。下一部分將介紹根本原因分析的步驟。

根本原因分析

1. 使用**show administrators**命令可確定節點上的活動連線數。但是，輸出可能並未顯示過多活動會話，這些會話可能阻塞了到節點的連線。

輸出示例：

```
[local]ASR5500-2# show administrators
Monday September 06 13:15:07 CDT 2021
Administrator/Operator Name    M Type    TTY            Start Time               Mode
Idle

----------------------------- - ------- -------------- ------------------------ ------------ --
--

admin                            admin   /dev/pts/4     Mon Sep 06 13:14:38 2021 Context User 29

admin                            admin   /dev/pts/3     Mon Sep 06 12:21:13 2021 Context User
749

admin                            admin   /dev/pts/2     Thu Sep 02 11:03:57 2021 Context User
342206
[local]ASR5500-2#
```

2. 此外，請執行這些命令並深入瞭解問題。通過隱藏模式導航到debug shell。

```
cli test-command pass <password>
debug shell
```

在debug shell中運行以下命令：

```
ps -ef
setvr 1 bash
netstat -n
```

ps — 列出進程。**ps**命令允許您檢視有關系統上當前進程的技術資訊以及驗證其狀態。

-e — 顯示所有進程，無論使用者是誰。

-f — 以詳細格式顯示進程。

netstat命令是最方便的命令列選項之一，用於顯示節點存在的所有套接字連線。它具有列出所有tcp和udp套接字連線以及unix連線的功能。此CLI還可用於列出可能仍在等待建立連線的偵聽套接字。

輸出示例：

```
ASR5500-2:card5-cpu0# ps -eF

UID        PID  PPID  C    SZ   RSS PSR STIME TTY          TIME CMD

root         1     0  0   511   640   4 Aug20 ?        00:00:13 init [5]

root         2     0  0     0     0   2 Aug20 ?        00:00:00 [kthreadd]

root         3     2  0     0     0   0 Aug20 ?        00:00:00 [ksoftirqd/0]

root         6     2  0     0     0   0 Aug20 ?        00:00:00 [migration/0]

root         7     2  0     0     0   0 Aug20 ?        00:00:01 [watchdog/0]

root         8     2  0     0     0   1 Aug20 ?        00:00:00 [migration/1]

root        10     2  0     0     0   1 Aug20 ?        00:00:00 [ksoftirqd/1]

root        11     2  0     0     0   0 Aug20 ?        00:00:31 [kworker/0:1]

root        12     2  0     0     0   1 Aug20 ?        00:00:00 [watchdog/1]

root        13     2  0     0     0   2 Aug20 ?        00:00:00 [migration/2]

root        15     2  0     0     0   2 Aug20 ?        00:00:00 [ksoftirqd/2]

root        16     2  0     0     0   2 Aug20 ?        00:00:00 [watchdog/2]

root        17     2  0     0     0   3 Aug20 ?        00:00:00 [migration/3]

root        19     2  0     0     0   3 Aug20 ?        00:00:00 [ksoftirqd/3]

root        20     2  0     0     0   3 Aug20 ?        00:00:00 [watchdog/3]

root        21     2  0     0     0   4 Aug20 ?        00:00:00 [migration/4]

root        22     2  0     0     0   4 Aug20 ?        00:00:00 [kworker/4:0]

root        23     2  0     0     0   4 Aug20 ?        00:00:00 [ksoftirqd/4]

……————————————————————

ASR5500-2:card5-cpu0# setvr 1 bash
bash-2.05b# netstat -n

Active Internet connections (w/o servers)

Proto Recv-Q Send-Q Local Address           Foreign Address         State

tcp        0      0 10.201.211.23:22        10.227.230.222:51781    ESTABLISHED

tcp        0      0 10.201.211.23:22        10.24.28.55:49918       ESTABLISHED

tcp        0      0 10.201.211.23:22        10.99.10.148:54915      ESTABLISHED

tcp        0      0 10.201.211.23:22        10.227.230.222:51783    ESTABLISHED

Active UNIX domain sockets (w/o servers)

Proto RefCnt Flags       Type       State         I-Node Path
```

```
unix  2      [ ]         DGRAM                    39221385

unix  2      [ ]         DGRAM                     27056

bash-2.05b# exit
```

根據上述報告，伺服器運行了生成到ASR55K盒連線的指令碼。這些伺服器開啟了許多處於停滯或空閒狀態的連線，但它們從未關閉。

即使TeleTypeWriter(TTY)連線終止，TCP連線仍會在我們的網關上保持活動狀態。

由於這些連線，ASR5500已達到允許的最大SSH連線數，從而妨礙連線到機箱。只要您嘗試登入到伺服器並終止父進程，所有連線就會立即釋放，SSH就會立即恢復。

這些空閒SSH連線建立為沒有TeleTypeWriter(noTTY)連線。這樣noTTY連線由以不顯示其輸出方式連線的程式使用。

SSH admin@asr55k hostname "display version"等命令在大多數情況下會建立noTTY連線。

類似地，語句如SSH:*@notty表示存在到尚未分配可視終端（例如外殼或偽終端）的網關(GW)的SSH登入。這可以在各種與指令碼相關的操作過程中發生，尤其是使用FTP/安全複製(SCP)連線時。

建議的解決方案

1. 對可能用於API伺服器的指令碼實施超時。執行多個CLI的多個SSH連線可能會在所有sessmgr進程上產生信使擁塞和大量的CPU使用率。
2. 為了簡化疑難排解，請設定以下選項：

```
logging filter runtime facility cli level debug critical-info
```

3. 將此配置應用到節點。此命令用於在5分鐘後終止空閒SSH會話。這用作針對伺服器造成的過時會話的保護機制：

```
Exec > Global Configuration > Context Configuration
configure > context context_name
administrator encrypted password timeout-min-absolute 300 timeout-min-idle 300
```

相關資訊

- CLI資訊
- Cisco ASR 5000系列配置指南
- 技術支援與文件 - Cisco Systems