

# 排除因空闲noTTY会话而导致的ASR5500登录问题

## 目录

[简介](#)

[ASR5500节点的登录问题](#)

[故障排除的步骤](#)

[根本原因分析](#)

[建议的解决方案](#)

[相关信息](#)

## 简介

本文档介绍如何对汇聚服务路由器(ASR5500/ASR 5000)的管理IP丢失安全外壳(SSH)连接时的场景进行故障排除。

## ASR5500节点的登录问题

您无法登录ASR5500数据包核心节点。SSH连接立即终止，且没有登录提示。Telnet连接表现出类似的行为。

### 故障排除的步骤

步骤1.尝试通过控制台连接登录到节点。

步骤2.在大多数情况下，未发出任何可能指向连接故障原因的特定简单网络管理协议(SNMP)陷阱。

步骤3.与登录相关的日志（经常出现在系统日志中）包括：

```
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
```

步骤4.命令show crash list all显示最近的崩溃，请注意，与vpnmgr相关的崩溃尤其重要。

步骤5.命令show task resources all可确保vpnmgr 和sshd 进程不能处于过度状态。vpnmgr负责IP地

址池管理并执行所有情景特定操作。sshd支持安全登录StarOS CLI。

步骤6.重新启动vpmngr实例1。有助于在某些情况下以最小影响恢复SSH连接。但是，连接可能会在一段时间后终止。

步骤7. MIO切换解决了问题。请注意，在进程可能达到阈值或过载状态的情况下，MIO退回可以帮助清除它。

解决方法是MIO切换。下一节介绍根本原因分析的步骤。

## 根本原因分析

1. 使用show administrators命令可确定节点上的活动连接数。但是，输出中可能未显示过多活动会话，这些会话可能会阻塞到节点的连接。

示例输出：

```
[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，执行这些命令并深入探讨问题。通过隐藏模式导航到调试外壳。

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

在debug shell中运行以下命令：

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

**ps** — 列出进程。ps命令允许您查看有关系统上当前进程的技术信息并验证其状态。

**-e** — 显示所有进程，而不考虑用户。

**-f** — 以详细格式显示进程。

**netstat** 命令是最方便的命令行选项之一，用于显示存在于节点的所有套接字连接。它能够列出所有tcp和udp套接字连接以及unix连接。此CLI还可用于列出可能仍等待连接建立的侦听套接字。

示例输出：

```
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
```

根据前面提到的报告，服务器运行的脚本导致连接到ASR55K机箱。这些服务器打开了许多处于停滞或空闲状态的连接，但它们从未关闭。

即使在TeleTypeWriter(TTY)连接终止后，TCP连接仍在网关上处于活动状态。

由于这些连接，ASR5500达到了允许的最大SSH连接数，妨碍了与机箱的连接。一旦您尝试登录到服务器并终止父进程，所有连接都会立即释放，SSH会立即恢复。

这些空闲SSH连接将建立为无TeleTypeWriter(noTTY)连接。这样的noTTY连接由连接的程序使用，以使其输出不显示。

在大多数情况下，SSH admin@asr55k主机名“显示版本”等命令会建立noTTY连接。

同样，SSH语句：\*@notty表明有SSH登录到我们的网关(GW)，但尚未分配可视终端，例如外壳或伪终端。这可能发生在各种与脚本相关的操作中，特别是在使用FTP/安全复制(SCP)连接时。

## 建议的解决方案

1. 对可用于API服务器的脚本实施超时。执行多个CLI的多个SSH连接可能会在所有会话管理器进程上生成Messenger拥塞和显着的CPU使用率。
2. 为了简化故障排除，请配置以下选项：

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

3. 将此配置应用于节点。此命令用于在5分钟后终止空闲SSH会话。这用作防止服务器导致的过时会话的保护机制：

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

## 相关信息

- [CLI信息](#)
- [Cisco ASR 5000系列配置指南](#)
- [技术支持和文档 - Cisco Systems](#)