Aanmelden probleem oplossen bij ASR5500 wegens ongebruikelijke sessies

Inhoud

Inleiding

Dit document beschrijft hoe u probleemoplossing kunt oplossen wanneer Secure Shell (SSH)-connectiviteit is kwijtgeraakt aan de IPs-beheer van de aggregation services router (ASR 5500/ASR 5000).

Aanmeldingsproblemen met de ASR 5500 knooppunten

U kunt niet inloggen op ASR5500 Packet Core-knooppunten. De SSH-verbinding wordt direct beëindigd zonder de inlogmelding. Telnet-verbindingen vertonen hetzelfde gedrag.

Stappen naar probleemoplossing

Stap 1. Probeer via de console-verbinding in het knooppunt te loggen.

Stap 2. In de meeste gevallen worden er geen specifieke SNMP-trap (Simple Network Management Protocol) uitgegeven die naar de oorzaak van de aansluitingsfout kan wijzen.

Stap 3. De logbestanden met betrekking tot inloggen, die constant op de systeemlogs aanwezig zijn, zijn:

```
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
```

Stap 4. De opdracht **toont de crashlijst met crashes** en geeft de recente crashes weer. Let op dat de items die betrekking hebben op **vpnmgr** vooral belangrijk zijn.

Stap 5. De opdracht **toont taakresources** die er **allemaal** voor zorgen dat de processen van **vpnmgr** en **sshd** niet overdreven zijn. **vpnmgr** is verantwoordelijk voor het beheer van IP-adrespool en voert alle context-specifieke operaties uit. **sshd** ondersteunt beveiligde inloging op de StarOS CLI.

Stap 6. Het opnieuw opstarten van **vpngr-**instantie 1. helpt in sommige gevallen de SSH-verbinding terug te krijgen met een minimaal effect. De verbinding kan echter na een tijdje worden afgesloten.

Stap 7. De MIO-omschakeling lost het probleem op. Houd er rekening mee dat in scenario's waarin een proces een drempelwaarde of een overbelastingsstaat kan bereiken, MIO bounce kan helpen om het proces te ontruimen.

De tijdelijke versie is de MIO-omschakeling. In de volgende sectie wordt gesproken over de stappen voor de analyse van de basisoorzaak.

Root Cause Analysis

1. Gebruik de opdracht **Show beheerders** om het aantal actieve verbindingen op het knooppunt te bepalen. Er is echter mogelijk dat de output te veel actieve sessies vertoont die de verbindingen met het knooppunt hebben verstopt.

Uitvoer van monster:

```
[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. Start deze opdrachten ook uit en graaf in de kwestie. Navigeer naar het debug shell door de verborgen modus.

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

Start deze opdrachten in het debug shell:

```
ps -ef
```

```
setvr 1 bash
netstat -n
```

processen van **ps** - lijsten . Met de opdracht **ps** kunt u technische informatie over de huidige processen in een systeem bekijken en de status ervan controleren.

e - alle processen tonen, ongeacht de gebruiker.

f - show processen in gedetailleerd formaat.

De opdracht **Netstat** is een van de meest handige opties van de opdrachtregel die worden gebruikt om alle socket verbindingen weer te geven die aanwezig zijn in het knooppunt. Het heeft de mogelijkheid om alle tcp- en udp socket verbindingen en de unix-verbindingen op te geven. Deze CLI kan ook worden gebruikt om een lijst op te maken van de mogelijke luisterzakken die nog kunnen wachten tot een verbinding tot stand is gebracht.

Uitvoer van monster:

```
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
```

Volgens het eerder genoemde rapport, voerden servers scripts uit die verbindingen uitbrachten naar de ASR55K box. Deze servers openden veel van deze verbindingen die vast of onklaar waren, maar ze werden nooit gesloten.

Zelfs nadat de TeleTypeWriter (TTY) verbinding werd beëindigd, bleef de TCP verbinding actief op onze gateways.

Als resultaat van deze verbindingen bereikte de ASR5500 het maximum aantal toegestane SSH-verbindingen, waardoor de verbinding met het vakje werd geblokkeerd. Zodra u probeert in te loggen op de servers en de basisprocessen te doden, worden alle verbindingen onmiddellijk vrijgegeven en wordt de SSH onmiddellijk hersteld.

Deze ongebruikte SSH-verbindingen worden ingesteld als geen TeleTypeWriter-verbindingen (noTTY). Zulke noTTY-verbindingen worden gebruikt door programma's die zodanig zijn aangesloten dat hun output niet wordt weergegeven.

Opdrachten zoals SSH admin@asr55k hostname "display versie" maken in de meeste gevallen een noTTY-verbinding in.

Evenzo worden uitspraken als SSH: *@notty geeft aan dat er SSH-telefoons aan onze gateways (GW's) zijn gekoppeld en dat er geen visuele terminal is toegewezen, zoals een shell of pseudo-terminal. Dit kan voorkomen tijdens een verscheidenheid aan script-gerelateerde bewerkingen, vooral bij het gebruik van FTP/Secure Copy (SCP)-verbindingen.

Voorgestelde oplossing

1. Voer een timeout in op de scripts in die gebruikt kunnen worden voor de API servers. Meervoudige SSH-verbindingen die meerdere CLI's uitvoeren, kunnen een congestie van de boodschapper en een aanzienlijk CPU-gebruik op alle sessgmh-processen genereren.
2. Om de probleemoplossing te vergemakkelijken, moet u deze optie configureren:

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

3. Pas deze configuratie op het knooppunt toe. Deze opdracht wordt gebruikt om alle SSH-sessies na 5 minuten te beëindigen. Dit wordt gebruikt als beveiligingsmechanisme tegen de verkoop van de server:

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

Gerelateerde informatie

- CLI-informatie
- Cisco ASR 5000 Series configuratie-handleidingen
- **Technische ondersteuning en documentatie – Cisco Systems**