使用TACACS帳戶通過SSH進行遠端使用者身份驗證的Nexus 7000系列交換機問題

目錄

簡介

本文提供進行疑難排解和確認Cisco Nexus 7000系列交換器受已知軟體缺陷Cisco bug ID CSCud02139影響所需的步驟。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Nexus 7000 系列交換器
- Cisco Nexus作業系統(NX-OS)版本5.2(5)至5.2(7)（含）
- Cisco NX-OS版本6.0(1)至6.1(3)（含）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

問題

症狀

使用者無法使用TACACS身份驗證遠端登入到Nexus 7000系列交換機虛擬裝置環境(VDC)。

此外，日誌中還會顯示以下消息：

```
n7k-vdc-1# show log last 200 | grep TACACS
2013 May 13 17:17:31 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:17:46 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:18:06 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:18:12 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:18:16 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:20:26 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:20:39 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:21:50 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
2013 May 13 17:22:09 n7k-vdc-1 TACACS-3-TACACS_ERROR_MESSAGE All servers
failed to respond
n7k-vdc-1#
```

狀況

在運行Cisco NX-OS版本5.2(5)和5.2(7)之間以及6.0.1到6.1(3)之間的Nexus 7000系列交換機上遇到此問題。

VDC必須使用TACACS身份驗證，如以下示例：

```
n7k-vdc-1# show run tacacs+

!Command: show running-config tacacs+
!Time: Mon May 13 17:20:57 2013

version 6.1(2)
feature tacacs+

ip tacacs source-interface mgmt0
tacacs-server timeout 30
tacacs-server host 192.0.2.9 key 7 "keypassword"
aaa group server tacacs+ default
server 192.0.2.9
use-vrf management
```

```
n7k-vdc-1# show run aaa

!Command: show running-config aaa
!Time: Mon May 13 17:21:30 2013

version 6.1(2)
aaa authentication login default group default
aaa authorization config-commands default group default
aaa authorization commands default group default
aaa accounting default group default
no aaa user default-role
aaa authentication login error-enable
tacacs-server directed-request
```

疑難排解

1. **確認TACACS伺服器狀態**

   確認Nexus 7000系列交換機能夠通過正確的虛擬路由和轉發(VRF)成功ping TACACS伺服器。確認TACACS伺服器仍能成功驗證其他裝置上的使用者。
2. **檢查身份驗證、授權和記帳(AAA)流程錯誤日誌**

   使用以下命令以檢查AAA流程錯誤日誌：

```
n7k-vdc-1# show system internal aaa event-history errors

1) Event:E_DEBUG, length:54, at 786852 usecs after Mon May 13 17:22:09 2013
[102] All Configured methods failed for default:default

2) Event:E_DEBUG, length:53, at 786796 usecs after Mon May 13 17:22:09 2013
[102] protocol TACACS failed with server group default

3) Event:E_DEBUG, length:54, at 379206 usecs after Mon May 13 17:22:09 2013
[102] All Configured methods failed for default:default

4) Event:E_DEBUG, length:53, at 379172 usecs after Mon May 13 17:22:09 2013
[102] protocol TACACS failed with server group default

5) Event:E_DEBUG, length:54, at 89083 usecs after Mon May 13 17:21:51 2013
[102] All Configured methods failed for default:default

6) Event:E_DEBUG, length:53, at 89051 usecs after Mon May 13 17:21:51 2013
[102] protocol TACACS failed with server group default
```

3. **檢查TACACS+進程錯誤日誌**

   使用以下命令以檢查TACACS+程式錯誤日誌：

```
n7k-vdc-1# show system internal tacacs+ event-history errors

1) Event:E_DEBUG, length:88, at 786728 usecs after Mon May 13 17:22:09 2013
[100] switch_tac_server: Unreachable servers case .setting error code for
aaa session 0
```

```
2) Event:E_DEBUG, length:77, at 786726 usecs after Mon May 13 17:22:09 2013
[100] switch_tac_server: no more server in the server group for
aaa session 0

3) Event:E_DEBUG, length:103, at 786680 usecs after Mon May 13 17:22:09 2013
[100] connect_tac_server: non blocking connect failed, switching server for
aaa session id(0) rtvalue(3)

4) Event:E_DEBUG, length:97, at 786677 usecs after Mon May 13 17:22:09 2013
[100] non_blocking_connect(171): getaddrinfo(DNS cache fail) with retcode:-1
for server:192.0.2.9

5) Event:E_DEBUG, length:62, at 786337 usecs after Mon May 13 17:22:09 2013
[100] tplus_encrypt(655):key is configured for this aaa session.

6) Event:E_DEBUG, length:95, at 786287 usecs after Mon May 13 17:22:09 2013
[100] tplus_make_acct_request(1343):Not calling the name-resolution routine
as rem_addr is empty

7) Event:E_DEBUG, length:63, at 786285 usecs after Mon May 13 17:22:09 2013
[100] tplus_make_acct_request(1308):Accounting userdata&colon;console0

8) Event:E_DEBUG, length:63, at 786266 usecs after Mon May 13 17:22:09 2013
[100] init_tplus_req_state_machine:Global source-interface mgmt0

9) Event:E_DEBUG, length:48, at 785842 usecs after Mon May 13 17:22:09 2013
[100] is_intf_up_with_valid_ip(1129):Port is up.

10) Event:E_DEBUG, length:57, at 785812 usecs after Mon May 13 17:22:09 2013
[100] is_intf_up_with_valid_ip(1126):Proper IOD is found.

11) Event:E_DEBUG, length:52, at 785799 usecs after Mon May 13 17:22:09 2013
[100] Exiting function: get_if_index_from_global_conf

12) Event:E_DEBUG, length:66, at 785797 usecs after Mon May 13 17:22:09 2013
[100] Function get_if_index_from_global_conf: found interface mgmt0

13) Event:E_DEBUG, length:53, at 785783 usecs after Mon May 13 17:22:09 2013
[100] Entering function: get_if_index_from_global_conf

14) Event:E_DEBUG, length:68, at 785781 usecs after Mon May 13 17:22:09 2013
[100] init_tplus_req_state_machine:Falling to globally configured one

15) Event:E_DEBUG, length:79, at 785779 usecs after Mon May 13 17:22:09 2013
[100] init_tplus_req_state_machine:No source-interface configured for this group
```

4. 調試TACACS+身份驗證請求

開啟TACACS+身份驗證請求的調試。AAA調試輸出以下日誌：

```
n7k-vdc-1# debug tacacs+ aaa-request
n7k-vdc-1# show logging logfile last 5
2013 May 13 18:20:26.077572 tacacs: tplus_encrypt(655):key is configured
for this aaa session.
2013 May 13 18:20:26.077918 tacacs: non_blocking_connect(171): getaddrinfo
DNS cache fail) with retcode:-1 for server:192.0.2.9
2013 May 13 18:20:26.077938 tacacs: connect_tac_server: non blocking connect
failed, switching server for aaa session id(0) rtvalue(3)
```

```
2013 May 13 18:20:26.077978 tacacs: switch_tac_server: no more server in the
server group for aaa session 0
2013 May 13 18:20:26.077993 tacacs: switch_tac_server: Unreachable servers
case .setting error code for aaa session 0
```

5. **在TACACS伺服器上執行資料包捕獲**

   TACACS伺服器上的資料包捕獲顯示沒有資料包從VDC到達。

6. **在Nexus 7000系列交換機上執行Ethanalyzer捕獲**

   Ethanalyzer擷取顯示沒有封包輸出到TACACS伺服器。

7. **檢查VDC上的運行進程**

   show proc cpu sort命令顯示TACACSD進程的33個例項（32個已停用）正在運行。

```
n7k-vdc-1# show proc cpu sort | include tacacs
1538 16 16 1014 0.0% tacacsd
1855 16 10 1625 0.0% tacacsd
2163 16 10 1678 0.0% tacacsd
2339 15 23 676 0.0% tacacsd
3820 15 10 1595 0.0% tacacsd
3934 16 13 1272 0.0% tacacsd
4416 25 8 3211 0.0% tacacsd
4470 16 23 734 0.0% tacacsd
5577 26 12 2191 0.0% tacacsd
6592 969767 14589069 66 0.0% tacacs
6934 16 13 1297 0.0% tacacsd
8878 16 13 1252 0.0% tacacsd
8979 16 12 1345 0.0% tacacsd
10153 26 11 2453 0.0% tacacsd
10202 15 8 1888 0.0% tacacsd
10331 26 11 2368 0.0% tacacsd
10482 16 14 1190 0.0% tacacsd
14148 15 11 1433 0.0% tacacsd
14385 14 10 1496 0.0% tacacsd
14402 15 9 1775 0.0% tacacsd
20678 16 9 1785 0.0% tacacsd
20836 16 13 1246 0.0% tacacsd
21257 15 13 1212 0.0% tacacsd
21617 15 9 1749 0.0% tacacsd
22159 15 12 1328 0.0% tacacsd
23776 15 12 1320 0.0% tacacsd
24017 25 9 2788 0.0% tacacsd
29496 15 8 1990 0.0% tacacsd
29972 15 11 1368 0.0% tacacsd
30111 25 9 2847 0.0% tacacsd
30204 15 9 1721 0.0% tacacsd
30409 16 13 1254 0.0% tacacsd
32410 15 8 1876 0.0% tacacsd
```

解決方案

VDC遇到已知的軟體缺陷Cisco錯誤ID CSCud02139。

TACACSD進程產生陷入停滯的子進程。這最多達到32個程式，且無法產生更多程式才能通過驗證。

確認

1. 確認TACACSD有33個例項。您可以使用**show proc cpu sort指令 | grep -c 'tacacsd'**以計數例項。
2. 執行ethanalyzer捕獲，並確認請求沒有離開Nexus 7000系列交換機。
3. 匹配以前的日誌消息。

因應措施

可能發生三種情況。移除所有TACACS配置，並移除和讀取功能和配置。另一種方法是執行Supervisor切換。或者，您可以重新載入VDC。

已解析的版本

- 5.2系列中的NX-OS 5.2(9)及更高版本
- 6.1系列中的NX-OS 6.1(3)版及更高版本

相關資訊

- Cisco Bug Toolkit - Cisco Bug ID CSCud02139
- **虛擬裝置環境技術概述**
- Ethanalyzer:Cisco NX-OS軟體內建資料包捕獲實用程式
- 技術支援與文件 - Cisco Systems

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）。