N7k tacacs以及认证失败案例分析

目录

硬件平台

N7K-C7010 / N7K-SUP1

软件版本

NXOS-6.1(2)

案例介绍

用户配置了AAA 以及tacacs+认证，以前一直运行正常，某一天突然远程登录失败，但从console可以登录（console口本地认证）。基本配置如下：

```
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 tacacs+
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 authentication login console local
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
```

问题分析思路

从现象来看，基本可以肯定问题出现在AAA TACACS+认证这一块，到底是什么原因导致认证失败呢？是N7K工作不正常，还是认证主机有问题?基本查错过程如下：

查看log信息，显示tacacs server没有响应。

```
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
```

从console口登录N7K后，ping 认证主机，没有问题，说明IP连通性并没有问题。

在tacacs server端抓包，可以抓到ping报文，但抓不到tacacs认证报文，说明问题还是出现在N7K端。

用N7K内置的ethanalyzer工具，抓从CPU发出到management接口的报文，也抓不到tacacs报文，说明该报文根本就没有出CPU，问题可能出现在tacacs进程上。

查看tacacs process，发现有多个tacacs进程。

```
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
```

Debug tacacs aaa-request 显示一些具体的失败信息：

```
n7k-vdc-1# debug tacacs+ aaa-request
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
```

用如上信息在TAC case库里查找，发现匹配一个software bug：

CSCud02139
The tacacsd process spawns child processes which get stuck. This reaches a maximum of 32 processes and it is unable to spawn any more to pass the authentication.

该bug将在如下版本中解决。

5.2(9)及更高
6.1(3)及更高

有3种临时解决方案：

1. 去掉相关AAA/tacacs+配置，重启tacacs+ feature，然后再重新加上相关配置
2. 如果双引擎，可以做一次引擎切换
3. 重启该VDC。

问题总结

当N7K出现和认证服务器的通讯问题时，我们可以先借助于抓包定位是哪端的问题，然后通过debug信息及进程信息，收集到认证失败的具体原因，这些原因对我们最终找到root cause非常重要。

经验总结

无。

相关命令

```
show log last 200 | grep TACACS
show run tacacs+
show run aaa
show system internal aaa event-history errors
show system internal tacacs+ event-history errors
show proc cpu sort | include tacacs
ethanalyzer local interface mgmt display-filter 'tcp.port == 49'
debug tacacs+ aaa-request
```