某局点S10508设备命令行认证慢问题处理经验案例

AAA 孟普 2018-01-30 发表

某局点对设备的管理要求比较高，对所有设备的命令行输入都会进行HWTACACS认证，其他设备在输入命令时认证返回都很快速，但是核心交换机S10508设备每输入一条命令后都需要比较久的时间认证，客户明显感觉到输入一条命令回车后的卡顿现象。

无

1.通过S10508debug查看命令行认证过程：
*Dec 6 11:56:45:027 2016 HS105-IRF01 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Processing authorization reply packet.
*Dec 6 11:56:45:027 2016 HS105-IRF01 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Reply message successfully sent.
*Dec 6 11:56:45:027 2016 HS105-IRF01 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Processing TACACS authorization.
*Dec 6 11:56:45:027 2016 HS105-IRF01 TACACS/7/EVENT: -MDC=1; PAM_TACACS: TACACS authorization succeeded.
*Dec 6 11:56:45:028 2016 HS105-IRF01 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Processing TACACS stop-accounting.
*Dec 6 11:56:45:028 2016 HS105-IRF01 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Session successfully created.
*Dec 6 11:56:45:028 2016 HS105-IRF01 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Getting available server, server-ip=99.XXX.XXX.111, server-port=49, VPN instance=--(public).
*Dec 6 11:56:45:218 2016 HS105-IRF01 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Connecting to server...
System View: return to User View with Ctrl+Z.
[HS105-IRF01]*Dec 6 11:56:45:419 2016 HS105-IRF01 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Reply SocketFd received EPOLLOUT event.
*Dec 6 11:56:45:419 2016 HS105-IRF01 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Connection succeeded, server-ip=99.xxx.xxx.111, port=49, VPN instance=--(public).
*Dec 6 11:56:45:419 2016 HS105-IRF01 TACACS/7/EVENT: -MDC=1; PAM_TACACS: Encapsulating accounting request packet.
*Dec 6 11:56:45:419 2016 HS105-IRF01 TACACS/7/send_packet: -MDC=1;
version: 0xc0 type: ACCOUNT_REQUEST seq_no: 1 flag: ENCRYPTED_FLAG

通过debug查看正常设备命令行认证过程：
Jan 1 02:44:46:493 2013 H3C TACACS/7/EVENT: PAM_TACACS: Processing authorization reply packet.
*Jan 1 02:44:46:493 2013 H3C TACACS/7/EVENT: PAM_TACACS: Reply message successfully sent.
*Jan 1 02:44:46:494 2013 H3C TACACS/7/EVENT: PAM_TACACS: Processing TACACS authorization.
*Jan 1 02:44:46:494 2013 H3C TACACS/7/EVENT: PAM_TACACS: TACACS authorization succeeded.
*Jan 1 02:44:46:494 2013 H3C TACACS/7/EVENT: PAM_TACACS: Processing TACACS stop-accounting.
*Jan 1 02:44:46:494 2013 H3C TACACS/7/EVENT: PAM_TACACS: Session successfully created.
*Jan 1 02:44:46:494 2013 H3C TACACS/7/EVENT: PAM_TACACS: Getting available server, server-ip=99.xxx.xxx.111, server-port=49, VPN instance=--(public).
*Jan 1 02:44:46:494 2013 H3C TACACS/7/EVENT: PAM_TACACS: Connecting to server...
*Jan 1 02:44:46:495 2013 H3C TACACS/7/EVENT: PAM_TACACS: Reply SocketFd received EPOLLOUT event.
*Jan 1 02:44:46:495 2013 H3C TACACS/7/EVENT: PAM_TACACS: Connection succeeded, server-ip=99.xxx.xxx.111, port=49, VPN instance=--(public).
*Jan 1 02:44:46:495 2013 H3C TACACS/7/EVENT: PAM_TACACS: Encapsulating accounting request packet.
*Jan 1 02:44:46:495 2013 H3C TACACS/7/send_packet:
version: 0xc0 type: ACCOUNT_REQUEST seq_no: 1 flag: ENCRYPTED_FLAG
session-id: 0xdeb0aa88
length of payload: 81

flags: STOP
authen_method: NONE authen_service: LOGIN
user_len: 6   port_len: 4   rem_len: 0   arg_cnt: 5
arg0_len: 9   arg1_len: 10   arg2_len: 13   arg3_len: 10
arg4_len: 15
user: 203161
port: vty0

发现S105确实比其他设备命令行认证的时间更长
2.查看设备配置
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
 command authorization
 command accounting
##
hwtacacs scheme cmbyyzx
 primary authentication 99.xxx.xxx.111
 primary authorization 99.xxx.xxx.111
 primary accounting 99.xxx.xxx.111
 secondary authentication 99.xxx.xxx.130
 secondary authorization 99.xxx.xxx.130
 secondary accounting 99.xxx.xxx.130
 key authentication cipher c3$lIFQVQ9mJunMCFu5sSBnjmnmD9ZQ1pY=
 key authorization cipher c3$VgCt71oOfIjMuo4RmfQzPfanuC2KUHM=
 key accounting cipher c3$9mIZBlwPq6ZCLhYItTe+yIRTTo8dDaQ=
 user-name-format without-domain
 nas-ip 99.xxx.xxx.3
#
domain system
 authentication login hwtacacs-scheme cmbyyzx local
 authorization login hwtacacs-scheme cmbyyzx local
 accounting login hwtacacs-scheme cmbyyzx local
 authorization command hwtacacs-scheme cmbyyzx local
 accounting command hwtacacs-scheme cmbyyzx
#
 domain default enable system
3.测试设备到服务器的延迟情况，发现延迟很小
<HS105-IRF01>ping -a 99.xxx.xxx.3 99.xxx.xxx.111
Ping 99.xxx.xxx.111 (99.xxx.xxx.111) from 99.xxx.xxx.3: 56 data bytes, press CTRL_C to break
56 bytes from 99.xxx.xxx.111: icmp_seq=0 ttl=126 time=2.361 ms
56 bytes from 99.xxx.xxx.111: icmp_seq=1 ttl=126 time=2.273 ms
56 bytes from 99.xxx.xxx.111: icmp_seq=2 ttl=126 time=1.929 ms
56 bytes from 99.xxx.xxx.111: icmp_seq=3 ttl=126 time=2.116 ms
56 bytes from 99.xxx.xxx.111: icmp_seq=4 ttl=126 time=2.046 ms
--- Ping statistics for 99.xxx.xxx.111 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.929/2.145/2.361/0.155 ms
<HS105-IRF01>
<HS105-IRF01>
<HS105-IRF01>ping -a 99.xxx.xxx.3 99.xxx.xxx.130
Ping 99.xxx.xxx.130 (99.xxx.xxx.130) from 99.xxx.xxx.3: 56 data bytes, press CTRL_C to break
56 bytes from 99.xxx.xxx.130: icmp_seq=0 ttl=59 time=42.697 ms
56 bytes from 99.xxx.xxx.130: icmp_seq=1 ttl=59 time=42.427 ms
56 bytes from 99.xxx.xxx.130: icmp_seq=2 ttl=59 time=42.418 ms
56 bytes from 99.xxx.xxx.130: icmp_seq=3 ttl=59 time=42.303 ms
56 bytes from 99.xxx.xxx.130: icmp_seq=4 ttl=59 time=42.265 ms
--- Ping statistics for 99.xxx.xxx.130 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 42.265/42.422/42.697/0.151 ms
4.hwtacacs scheme视图下配置primary accounting 时，默认情况下每次计费都会使用一个新的TCP连接。

为了增加认证计费的效率，可以配置上single-connection参数，使得所有与主HWTACACS计费服务器交互的计费报文使用同一个TCP连接。如果未指定本参数，则表示每次计费都会使用一个新的TCP连接。

primary accounting { host-name | ipv4-address | ipv6 ipv6-address } [port-number | key { cipher | simple } string | single-connection | vpn-instance vpn-instance-name] *
配置single-connection参数后可节省TCP连接资源，但有些HWTACACS服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置single-connection参数，以提高性能和效率。