H3C S3600 与ACS配合在远程认证通信失败后不能成功转本地认证故障排除一例

赵国卫 2008-06-13 发表

H3C S3600 与ACS配合在远程认证通信失败后不能成功
转本地认证故障排除一例

一、 组网：

无

二、 问题描述：

某网络在使用H3C S3600与ACS配合做tacacs认证时，发现在远程到ACS认证通信失败的情况下，tacacs并未如预想的那样转到本地认证成功，造成管理用户无法正常登录设备。

三、 过程分析：

在交换机上开启如下debug:

<H3C>debugging hwtacacs all

<H3C>debugging local-server private

发现debug信息中有如下内容

*0.86152099 H3C SC/8/SC_GENERAL::- 1 -Recv MSG,[MsgType=Authen ack success Index= 71, ulParam3=2185366660] --------**表示认证成功**

*0.86152216 H3C TAC/8/Event:- 1 -TAC_MESSAGE for AAA->TAC:

*0.86152299 H3C TAC/8/Event:- 1 -
UserID=71 AuthorType=4 AuthenMethod=6 AuthenType=1 AuthenService=1 PrivLevel=0 TemplateNum=0 ArgNum=2 UserName=test@3900 PortName=vty0 Service=shell Protocol=cmd* RemAddress=1.1.1.1

*0.86152586 H3C TAC/8/Event:- 1 -Tac receive 3 message, but cannot find according session.

*0.86152682 H3C TAC/8/Event:- 1 - hwtacacs create new session :session id: 18114, user id: 71, server ip: 1.1.1.4

*0.86152832 H3C TAC/8/Event:- 1 -version:c0 type:AUTHOR_REQUEST
seq_no:1 flag:ENCRYPTED_FLAG session_id:46c2 length:47
authen_method:AUTHEN_METH_PLUS priv_lvl:VISIT
authen_type:AUTHEN_TYPE_ASCII authen_service:AUTHEN_SVC_LOGIN
user len:9 port len:4 rem_addr len:7 arg_cnt:2
arg1 len:13 arg2 len:4 user:test@3900 port:vty0 rem_addr:1.1.1.1
arg1 :service=shell arg2 :cmd*

*0.86153332 H3C TAC/8/Event:- 1 -statics: transmit flag:1, server flag: 1,packet flag: 0xff

*0.86156285 H3C TAC/8/Event:- 1 -statics: transmit flag:3, server flag: 1,packet flag: 0xff

*0.86156383 H3C TAC/8/Event:- 1 -No useful server.

*0.86156432 H3C TAC/8/Event:- 1 - hwtacacs session is deleted due to expiration:session id: 18114, user id: 71, server ip: 1.1.1.4

*0.86156599 H3C SC/8/SC_GENERAL::- 1 -Recv MSG,[MsgType=Author ack reject Index= 71, ulParam3=2185746340]----------表示授权被拒绝

*0.86156716 H3C SC/8/SC_GENERAL::- 1 -Recv MSG,[MsgType=Leaving request Index =71, ulParam3=0]

从上述debug信息可以看到，是在授权阶段出错了。进一步查看配置发现:

```
hwtacacs scheme acs
 primary authentication 1.1.1.4
 primary authorization 1.1.1.4
 key authentication h3c
 key authorization h3c
#
domain 3600
 authentication hwtacacs-scheme acs local
 authorization hwtacacs-scheme acs
 accounting none
domain system
```

该配置当中，将认证/授权/计费分别指定，这种情况下三者分别按照自己的配置生效，只有认证能够在本地进行认证，授权还是到远端认证因此被拒绝。

四、 解决方法：

问题已经明确，修改配置可以解决，修改后的配置如下:

```
hwtacacs scheme acs
 primary authentication 1.1.1.4
 primary authorization 1.1.1.4
 key authentication h3c
 key authorization h3c
#
domain 3600
 scheme hwtacacs-scheme acs local
 accounting none
```

这样认证和授权都会成功。

注意：如果要在远程认证通信失败的情况下转本地认证，只能采用scheme hwtacacs-scheme的方式来配置不能认证/授权分开配置。