iMC TAM tacacs认证授权命令集未生效问题

iMC 高洋 2023-03-28 发表

组网及说明

不涉及

告警信息

不涉及

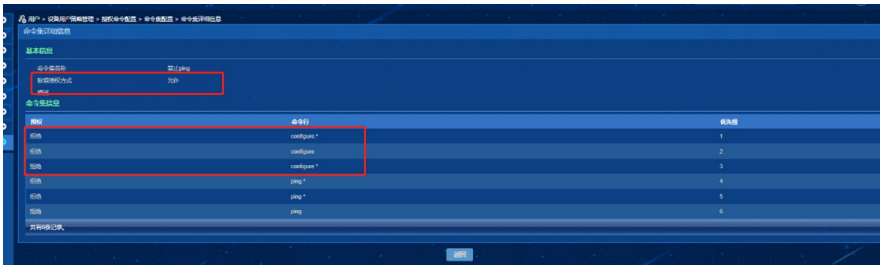
问题描述

现场想实现某个设备用户禁止输入configure命令。现场根据认证手册进行配置之后登录该设备用户还是可以执行configure命令。

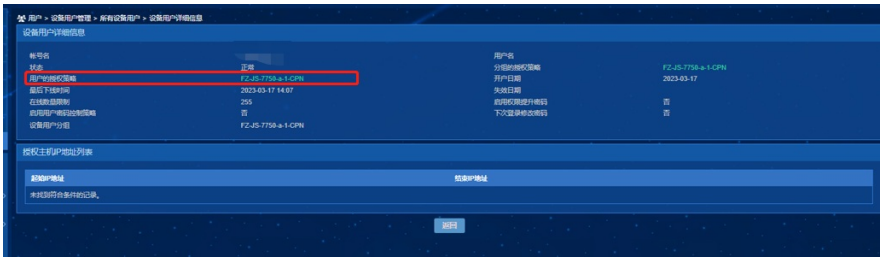
过程分析

1、查看具体的命令集配置，看是否配置错误；

现场配置如图，configure相关命令配置的均为拒接，配置没有问题；



2、检查授权命令集是否被授权策略引用，检查登录的设备是否满足设备区域、设备类型、授权时段等信息，检查设备用户是否引用了该授权策略。



3、查看授权日志，发现日志显示授权命令集已经生效，命令已经拒绝；

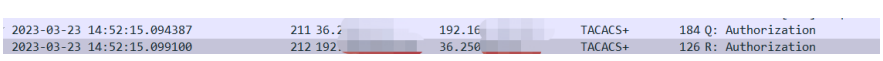
4、分析tam debug日志和抓包，用户登录后，从抓包和日志来看TAM服务器已经拒绝了configure命令。需要设备厂商的同事看下为什么没生效。

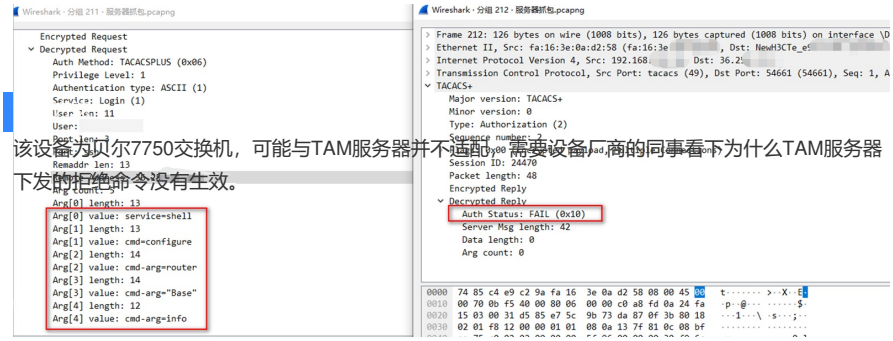
对应tacacs日志：

```
64 2d 61 72 67 3d 69 6e 66 6f
2023-03-23 14:52:15.094 ; [DBG] ; [1420] ; chkMsgBody: packet fields
PACKET_TYPE = AUTHOR.
AUTHOR_AUTHEN_METHOD = TAC_PLUS_AUTHEN_METH_TACACSPLUS.
AUTHOR_PRIV_LEVEL = 1.
AUTHOR_AUTHEN_TYPE = TAC_PLUS_AUTHEN_TYPE_ASCII.
AUTHOR_AUTHEN_SERVICE = TAC_PLUS_SVC_LOGIN.
AUTHOR_USER =
AUTHOR_PORT = ssh.
AUTHOR_REM_ADDR =
  AUTHOR_ARG[0] = service=shell.
  AUTHOR_ARG[1] = cmd=configure.
  AUTHOR_ARG[2] = cmd-arg=router.
  AUTHOR_ARG[3] = cmd-arg="Base".
  AUTHOR_ARG[4] = cmd-arg=info.
sock:312, SESSION_ID = 24470.

2023-03-23 14:52:15.094 ; [HNT] ; [1420] ; pktReader: read-done and dropped [sock:312],  port:49]
2023-03-23 14:52:15.094 ; [DBG] ; [8496] ; procAuthorItem: begin.
2023-03-23 14:52:15.094 ; [HNT] ; [8496] ; In author packet, the value of arg service is shell.
2023-03-23 14:52:15.095 ; [DBG] ; [8496] ; procCmdAuthor: begin.
2023-03-23 14:52:15.095 ; [DBG] ; [8496] ; getShellProfIdCmdSetsId: begin.
2023-03-23 14:52:15.097 ; [DBG] ; [8496] ; getShellProfIdCmdSetsId: got shell profile id 1 and cmd sets id 1
2023-03-23 14:52:15.097 ; [DBG] ; [8496] ; getShellProfIdCmdSetsId: end.
2023-03-23 14:52:15.098 ; [DBG] ; [8496] ; procCmdAuthor: CmdRsp.srcCmd [configure.*], CmdRsp.dstCmd [configure router "Base" info], match [1]
2023-03-23 14:52:15.098 ; [DBG] ; [8496] ; procCmdAuthor: end - cmd upload matched config cmd with result 16.
2023-03-23 14:52:15.098 ; [DBG] ; [8496] ; sendAuthorReply: Sent msg content is
PACKET_TYPE = AUTHOR_REPLY.
AUTHOR_STATUS = TAC_PLUS_AUTHOR_STATUS_FAIL.
AUTHOR_SERVER_MSG = E65049: The command is not allowed to run..
AUTHOR_DATA = .
AUTHOR_ARG_CNT= 0.
SESSION_ID = 24470.
```

对应抓包：





该设备为贝尔7750交换机，可能与TAM服务器并不适配，需要设备厂商的同事看下为什么TAM服务器下发的拒绝命令没有生效。