

知 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

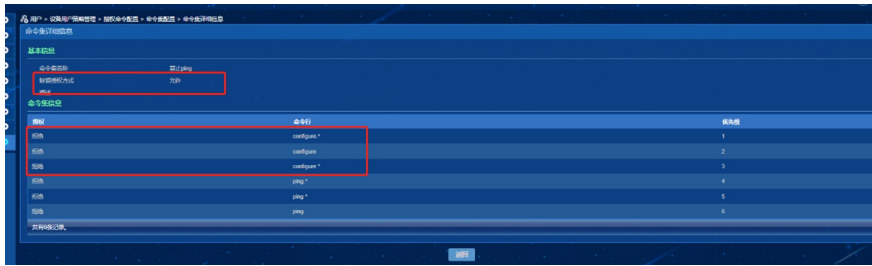
问题描述

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。

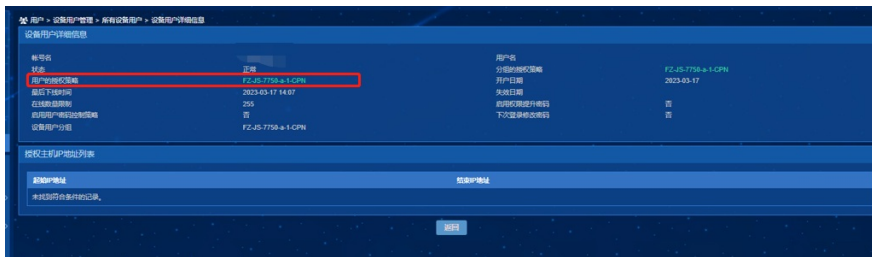
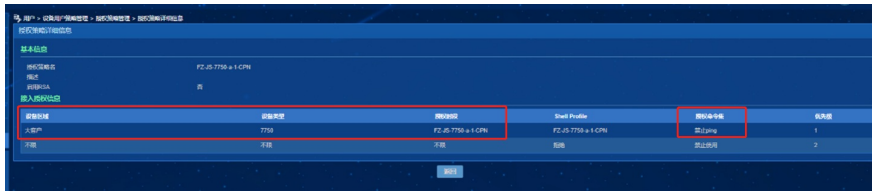
过程分析

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绝，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：

```
16 01 f2 b7 50 22 42 61 f3 b5 22 63 b0
17 e4 2d 61 72 67 3d 69 6e 66 e6 ef
18 2023-03-23 14:52:15.094 ; [DBG] ; [1420] ; chkMsgBody: packet fields
19 PACKET_TYPE = AUTHOR.
20 AUTHOR_AUTHEN_METHOD = TAC_PLUS_AUTHEN_METH_TACACSPLUS.
21 AUTHOR_PRIV_LEVEL = 1.
22 AUTHOR_AUTHEN_TYPE = TAC_PLUS_AUTHEN_TYPE_ASCII.
23 AUTHOR_AUTHEN_SERVICE = TAC_PLUS_SVC_LOGIN.
24 AUTHOR_USER =
25 AUTHOR_PORT = ssh.
26 AUTHOR_FEM_ADDR =
27 AUTHOR_ARG[0] = service=shell.
28 AUTHOR_ARG[1] = cmd=configure.
29 AUTHOR_ARG[2] = cmd-arg=router.
30 AUTHOR_ARG[3] = cmd-arg="Base".
31 AUTHOR_ARG[4] = cmd-arg=info.
32 sock:312, SESSION_ID = 24470.
33
34 2023-03-23 14:52:15.094 ; [HNT] ; [1420] ; pktReader: read-done and dropped [sock:312], port:49
35 2023-03-23 14:52:15.094 ; [DBG] ; [8496] ; procAuthItem: begin.
36 2023-03-23 14:52:15.094 ; [HNT] ; [8496] ; In author packet, the value of arg service is shell.
37 2023-03-23 14:52:15.095 ; [DBG] ; [8496] ; procCmdAuthor: begin.
38 2023-03-23 14:52:15.095 ; [DBG] ; [8496] ; getShellProfileCmdSets: begin.
39 2023-03-23 14:52:15.097 ; [DBG] ; [8496] ; getShellProfileCmdSets: got shell profile id 1 and cmd sets id 1
40 2023-03-23 14:52:15.098 ; [DBG] ; [8496] ; getShellProfileCmdSets: end.
41 2023-03-23 14:52:15.098 ; [DBG] ; [8496] ; procCmdAuthor: CmdResp.succeeded [configure,*], CmdResp.detCmd [configure router "Base" info], match [1]
42 2023-03-23 14:52:15.098 ; [DBG] ; [8496] ; procCmdAuthor: end = cmd upload matched config cmd with result 16.
43 2023-03-23 14:52:15.098 ; [DBG] ; [8496] ; sendAuthorReply: Sent msg content is
44 PACKET_TYPE = AUTHOR_REPLY.
45 [AUTHOR_STATUS = TAC_PLUS_AUTHOR_STATUS_FAIL.
46 AUTHOR_SERVER_MSG = E65049: The command is not allowed to run..
47 AUTHOR_CMD_RESP =
48 AUTHOR_ARG_CNT = 0.
49 SESSION_ID = 24470.
50 ..
```

对应抓包：

2023-03-23 14:52:15.094387	211 36.2	192.16	TACACS+	184 Q: Authorization
2023-03-23 14:52:15.099100	212 192.	36.256	TACACS+	126 R: Authorization

Wireshark · 分组 211 · 服务器响应.pcapng

Encrypted Request

- Decrypted Request
 - Auth Method: TACACSPLUS (0x06)
 - Privilege Level: 1
 - Authentication type: ASCII (1)
 - Service: Login (1)
 - User Len: 11
 - User:
 - Req Len: 11
 - Remaddr Len: 13
 - Arg count: 5
 - Arg[0] length: 13
 - Arg[0] value: service=shell
 - Arg[1] length: 13
 - Arg[1] value: cmd=configure
 - Arg[2] length: 14
 - Arg[2] value: cmd-arg-router
 - Arg[3] length: 14
 - Arg[3] value: cmd-arg="Base"
 - Arg[4] length: 12
 - Arg[4] value: cmd-arg=info

Wireshark · 分组 212 · 服务器响应.pcapng

Frame 212: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF...
Ethernet II, Src: fa:16:3e:0a:d2:58 (fa:16:3e:0a:d2:58), Dst: NewH3To_e: (fa:16:3e:0a:d2:58)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 35.20.1.100
Transmission Control Protocol, Src Port: tacacs (49), Dst Port: 54661 (54661), Seq: 1, A...

TACACS+

- Major version: TACACS+
- Minor version: 0
- Type: Authorisation (2)
- Sequence number: 2
- Session ID: 24470
- Packet length: 48
- Encrypted Reply
- Decrypted Reply
 - Auth Status: FAIL (0x10)
 - Server Msg Length: 42
 - Data length: 0
 - Arg count: 0

0000 74 85 c4 e9 c2 9a fa 16 3e 0a d2 58 08 00 45 00 t.....>X:f
0010 00 70 0b f5 40 00 00 06 00 00 c0 a8 fd 0a 24 fa p-@.....\$.
0020 15 03 00 31 d5 85 e7 5c 9b 73 da 07 0f 3b 00 18 --1...X...<...<
0030 02 01 f8 12 00 00 01 01 08 0a 13 7f 81 0c 08 bf<.....<.....<

该设备为贝尔7750交换机，可能与TAM服务器不匹配，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。

