

知 S7503E-S结合iMC做telnet登录认证EXEC权限下发失败处理经验

Telnet 夏威 2019-11-24 发表

问题描述

S7503E-S结合iMC做telnet登录认证EXEC权限下发失败如何处理?

解决方法

iMC侧给设备管理用户配置的EXEC权限级别是3, 但是认证成功登录设备后发现用户的权限始终为0, iMC侧给设备管理用户下发EXEC权限失败;

```
#<
radius scheme gdtel<
  primary authentication 132.121.84.190<
  primary accounting 132.121.84.190<
  key authentication gdtel2016!<
  key accounting gdtel2016!<
  user-name-format without-domain<
#<
domain gdtel<
  authentication login radius-scheme gdtel<
  authorization login radius-scheme gdtel<
  accounting login radius-scheme gdtel<

<S7503E-S>dis users<
The user application information of the user interface(s):
  ldx UI      Delay  Type  Userlevel<
  51 VTY 1    00:00:12 TEL    0<
Following are more details.<
VTY 1 :<
  User name: login@login<
  Location: 172.16.2.2<
```

将客户的配置在实验室SR6604-X (Version 5.20.106, Release 3303P29) 上测试, 用户的权限为3, iMC侧给设备管理用户下发EXEC权限成功; 尝试在L1000-A (Version 5.20, Ess 7904P02) 测试, 出现了和客户一样的问题, 用户的权限为0, 权限下发失败。

设备侧开启debug radius packet, iMC服务器侧开启抓包, 复现问题。从radius 2号认证响应报文中可以看到已经将EXEC权限级别3下发, iMC服务器侧正常; 设备侧debug信息中, 找到Code=[2]认证响应报文, 没有权限字段[H3C-29 Exec_Privilege], 应该就是设备侧问题, 将radius方案服务类型server-type配置extended再次测试, 发现登录的权限为3, 权限下发成功。EXEC权限级别虽然是我们自己定义的, 对比版本可以看出在V5早期版本仍需要扩展类型, 而V5新版本标准类型就能携带。

No.	Time	Source	Destination	Protocol	Length
1	0.000000	10.88.142.134	10.88.142.171	RADIUS	208
2	0.010859	10.88.142.171	10.88.142.134	RADIUS	86

```
Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: Hangzhou_1d:56:44 (0c:da:41:1d:56:44), Dst: 70:f9:6d:e4:74:f4 (70:f9:6d:e4:74:f4)
Internet Protocol Version 4, Src: 10.88.142.171 (10.88.142.171), Dst: 10.88.142.134 (10.88.142.134)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 4565 (4565)
Radius Protocol
  Code: Access-Accept (2)
  Packet identifier: 0x13 (19)
  Length: 44
  Authenticator: 2e65182adb33af11d8c67147ad7f22da
  [This is a response to a request in frame 1]
  [Time from request: 0.010859000 seconds]
  Attribute Value Pairs
    AVP: l=6 t=Service-Type(6): Login(1)
    AVP: l=6 t=Login-Service(15): Telnet(0)
    AVP: l=12 t=Vendor-Specific(26) v=H3C(25506)
    VSA: l=6 t=Unknown-Attribute(29): 00000003
    Unknown-Attribute: 00000003
```

*Feb 24 12:21:59:713 2017 SZDJG_LB_Sec Blade LB RDS/7/DEBUG: Receive:IP=[10.88.142.171],Code=[2],Length=[44]

*Feb 24 12:21:59:713 2017 SZDJG_LB_Sec Blade LB RDS/7/DEBUG: [6 Service-Type] [6] [1] [15 Login-Service] [6] [0]

//设备识别Code=[2] 认证响应报文中没有权限字段[H3C-29 Exec_Privilege]

*Feb 24 12:21:59:717 2017 SZDJG_LB_Sec Blade LB RDS/7/DEBUG: Recv MSG,[MsgType=Account request Index = 22, ulParam3=0]