6900 ssh配合hwtacacs 登录异常

AAA 李敏 2021-12-14 发表

组网及说明

无

问题描述

设备：S6900-54QF-F Release 2612P01

问题描述:

客户设备对接思科的认证系统做管理用户的tacacs认证，查看debug认证授权都已经过了，但是用户端还是ssh登陆不了

```
*Aug  2 11:13:02:301 2021 4F-G10-G11-TOR-IRF TACACS/7/EVENT: PAM_TACACS: Processing authorization reply packet.
*Aug  2 11:13:02:301 2021 4F-G10-G11-TOR-IRF TACACS/7/EVENT: PAM_TACACS: Reply message successfully sent.
*Aug  2 11:13:02:302 2021 4F-G10-G11-TOR-IRF TACACS/7/EVENT: PAM_TACACS: Processed authorization reply message, resultCode: 0.
*Aug  2 11:13:02:302 2021 4F-G10-G11-TOR-IRF TACACS/7/EVENT: PAM_TACACS: TACACS authorization succeeded.
%Aug  2 11:13:02:303 2021 4F-G10-G11-TOR-IRF SSHS/6/SSHS_LOG: Accepted password for xqa1 from 10.46.253.20 port 52355.

%Aug  2 11:13:03:372 2021 4F-G10-G11-TOR-IRF SSHS/6/SSHS_CONNECT: SSH user xqa1 (IP: 10.46.253.20) connected to the server successfully.
%Aug  2 11:13:03:766 2021 4F-G10-G11-TOR-IRF LOGIN/5/LOGIN_FAILED: xqa1 failed to log in from 10.46.253.20.
%Aug  2 11:13:06:777 2021 4F-G10-G11-TOR-IRF SSHS/6/SSHS_DISCONNECT: SSH user xqa1 (IP: 10.46.253.20) disconnected from the server.
```

```
#
hwtacacs scheme acs
primary authentication 10.46.249.35
primary authorization 10.46.249.35
key authentication cipher $c$3$cqZlhf3f9NiIOLljv0OPHDU2zu/IUVrnYJXAH43xVA==
key authorization cipher $c$3$UNQ9cl0uSfQFpJc3zSa4sPLBEuzwGv+wa4WQYpe5ew==
user-name-format without-domain
nas-ip 10.47.139.195
#
radius scheme system
user-name-format without-domain
#
domain idc
authentication login hwtacacs-scheme acs local
authorization login hwtacacs-scheme acs local
#
domain system
#
domain default enable idc
#
role default-role enable
#
#
line vty 0 15
authentication-mode scheme
user-role network-admin
protocol inbound ssh
idle-timeout 1800 0
#
line vty 16 63
authentication-mode scheme
user-role network-admin
protocol inbound ssh
#
```

过程分析

配置少了，domain下只配置了认证和授权，没有配置计费，默认会走本地计费，但是本地没有用户xqa1，计费会失败，登录不了设备。

再加一下下面这个命令试试。

```
accounting login hwtacacs-scheme acs local
#
domain idc
authentication login hwtacacs-scheme acs local
authorization login hwtacacs-scheme acs local
```

解决方法

domain下增加如下配置

```
accounting login hwtacacs-scheme acs local
#
```