

# 知 某局点S5130S-IE SSH登录结合tacacs认证失败案例

Tacacs SSH zhiliao\_l6nhL 2018-09-16 发表

## 组网及说明

不涉及

## 问题描述

客户现场对新接入网络的几台S5130-EI交换机进行SSH管理，结合思科的ACS服务器进行Tacacs认证，目前的故障是可以弹出认证界面，输入用户名和密码提示认证失败

## 过程分析

核实关键配置，没有错误

```
line vty 0 63
authentication-mode scheme
user-role network-admin
user-role network-operator
protocol inbound ssh

domain default enable dji.com
role default-role enable
domain dji.com
authentication login hwtacacs-scheme dji.com
authorization login hwtacacs-scheme dji.com
accounting login hwtacacs-scheme dji.com
hwtacacs scheme dji.com primary authentication 10.10.1.195
primary authorization 10.10.1.195
primary accounting 10.10.1.195 key authentication cipher $c$3$8FWvi1AEOTP+DNY3/iqs7K48i9Wz
Q6ipBg==
key authorization cipher $c$3$7xOJ91M/Cu/WX/hn3/WznfkfVU4GKu1zyQ==
key accounting cipher $c$3$Rw9gTyrrm/MrHjP6QnEskvTlygColtkgBQ==
user-name-format without-domain
nas-ip 10.61.244.13
```

复现问题，采集debug信息分析

```
*Jul 3 09:35:00:186 2018 H3C TACACS/7/EVENT: PAM_TACACS: Dispatching request, Primitive: authentication.
*Jul 3 09:35:00:186 2018 H3C TACACS/7/EVENT: PAM_TACACS: Creating request data, data type: START
*Jul 3 09:35:00:187 2018 H3C TACACS/7/EVENT: PAM_TACACS: Session successfully created.
*Jul 3 09:35:00:187 2018 H3C TACACS/7/EVENT: PAM_TACACS: Getting available server, server-ip=10.10.1.195, server-port=49, VPN instance=--(public).
*Jul 3 09:35:00:188 2018 H3C TACACS/7/EVENT: PAM_TACACS: Connecting to server...
*Jul 3 09:35:05:633 2018 H3C TACACS/7/EVENT: PAM_TACACS: Connection timed out.
%Jul 3 09:35:05:635 2018 H3C SSSH/6/SSHS_LOG: Authentication failed for user rui.chen from 10.61.130.1 port 52841 because of invalid username or wrong password.

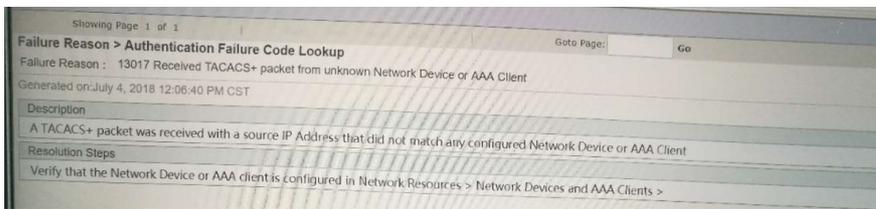
*Jul 3 09:35:05:634 2018 H3C TACACS/7/ERROR: PAM_TACACS: Failed to get available server.
*Jul 3 09:35:05:634 2018 H3C TACACS/7/EVENT: PAM_TACACS: Reply message successfully sent.
*Jul 3 09:35:05:635 2018 H3C TACACS/7/EVENT: PAM_TACACS: Processed authentication reply message, resultCode: 5.
*Jul 3 09:35:05:636 2018 H3C TACACS/7/EVENT: PAM_TACACS: Set status of server to block successfully. serverIP: 10.10.1.195, serverPort: 49.
```

首先上面的日志存在一点乱序，表面上是用户名和密码错误，实际上应该服务器没有回包导致设备认为服务器不可达，并且把服务器状态置为了block，最终SSH登录失败。

在认证失败的时候，在设备上display hwtacacs scheme看到确实是block的状态。

针对这种情况，可以在设备上PING测试服务器地址是否可达，服务器相关端口是否开放。

让现场反馈服务器的报错日志



可以发现服务器收到一个客户端认证请求，但是源地址没有匹配服务器配置的Network Device范围导致被服务器拒绝

#### 解决方法

在服务器端的Network Device内添加进设备的NAS-IP地址解决。

遇到问题不能只看表面现象，要明确排查思路分析问题本质。