

知 S5130S-52P-EI SSH登录不成功

SSH

802.1X

一颗小土豆

2022-03-12 发表

组网及说明

设备型号: S5130S-52P-EI

设备版本: Release 6318P01

组网: 不涉及

问题描述

该局点因为安全性的要求，想要通过SSH登录设备，但是配置好去SSH登录时，发现登录不成功，报错有三种情况，分别见下图：

图一为设备报错服务器密钥和本地缓存密钥不一致。

```
<SD-TA-TSQ-4F>
<SD-TA-TSQ-4F>ssh
Username:
Press CTRL+C to abort.
Connecting to ...
The server's host key does not match the local cached key. Either the server administrator has
changed the host key, or you connected to another server pretending to be this server. Please r
emove the local cached key, before logging in.
<SD-TA-TSQ-4F>
```

图二报用户名和密码错误。

```
<SD-TA-TSQ-4F>ssh ... 5
Username: test
Press CTRL+C to abort.
Connecting to ... port ...
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
test@...: password:
authentication failed
Incorrect username or password, or server configuration error.
%Feb 14 16:21:37:691 2013 SD-TA-TSQ-4F SSHS/6/SSHS_AUTH_PWD_FAIL: Authentication failed for use
r test from ... port 57215 because of invalid username or wrong password.
test@...: password: █
```

过程分析

刚开始的报错是服务器密钥和本地缓存密钥不一致。因此建议现场删除本地的密钥对。命令如下：

1.1.5 public-key local destroy

public-key local destroy命令用来销毁本地非对称密钥对。

【命令】

public-key local destroy { dsa | ecdsa | rsa } [name key-name]

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dsa：本地密钥对类型为DSA。

ecdsa：本地密钥对类型为ECDSA。

rsa：本地密钥对类型为RSA。

name key-name：销毁指定名称的本地非对称密钥对。*key-name*为本地非对称密钥对名称，为1~64个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“_”。如果不指定本参数，则销毁指定类型默认名称的本地非对称密钥对。

【使用指导】

在如下几种情况下，建议用户销毁旧的非对称密钥对，并生成新的密钥对：

- 本地设备的私钥泄露。这种情况下，非法用户可能会冒充本地设备访问网络。
- 保存密钥对的存储设备出现故障，导致设备上没有公钥对应的私钥，无法再利用旧的非对称密钥对进行加解密和数字签名。
- 本地证书到达有效期，需要删除对应的本地密钥对。本地证书的详细介绍，请参见“安全配置指导”中的“PKI”。

修改后再次登录，便报错用户名和密码不匹配（图二）。因此建议现场创建一个新用户测试，但还是不行，如下图：

```
SD-TA-TSQ-3F-110
[~]# config
[~]# local-user test
User added.
[~]# user-manage-test
[~]# user-manage-test service-type telnet
[~]# user-manage-test service-type ssh
[~]# user-manage-test
[~]# user-manage-test pa
[~]# user-manage-test password simple aal23456
[~]# user-manage-test au
[~]# user-manage-test authorization-attribute user-profile
[~]# user-manage-test authorization-attribute user-role network-admin
[~]# user-manage-test quit

[~]# save
[~]#
[~]# aux0-IPAddr=""-user=""; Exit from the system view or a feature view to the user view.

sername: test
ress CTRL+C to abort.
connecting to 76.56.72.4
Feb 17 00:22:02:917 2013 SD-TA-TSQ-3F SSH/6/SSHC_ALGORITHM_MISMATCH: Failed to log in to SSH server 76.56.72.4 because of public key mismatch.
SD-TA-TSQ-3F:Feb 17 00:22:09:935 2013 SD-TA-TSQ-3F IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/27 changed to down.
Feb 17 00:22:09:936 2013 SD-TA-TSQ-3F IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/27 changed to down.
Feb 17 00:22:12:248 2013 SD-TA-TSQ-3F IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/27 changed to up.
Feb 17 00:22:12:250 2013 SD-TA-TSQ-3F IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/27 changed to up.

SD-TA-TSQ-3F-SSH 76.56.72.4
sername: test
ress CTRL+C to abort.
connecting to 76.56.72.4 port 22.
The server is not authenticated. Continue? [y/N]:y
Do you want to save the server public key? [y/N]:n
etc:
's password:
Authentication failed
incorrect username or password, or server configuration error.
Feb 17 00:22:34:237 2013 SD-TA-TSQ-3F SSH/6/SSH_AUTH_PWD_FAIL: Authentication failed for user test from 10.1.1.1 port 2229 because of invalid username or wrong password.
etc:
's password: Feb 17 00:22:43:141 2013 SD-TA-TSQ-3F STP/6/STP_DETECTED_TC: Instance 0 detected a topology change.
```

检查了现场反馈的配置，发现现场配置了默认域：domain default enable AAA，该域是用于802.1x认证的

建议删除该命令后，用户可以正常SSH登录，但是用户无法正常认证上网。

后建议现场在802.1X的接口下配置：**dot1x mandatory-domain AAA**后正常。

解决方法

现场的问题报错其实很明显，按照报错进行针对性排查即可。
但是对于用户名和密码错误的问题还是需要考虑默认域的因素

