某局点S5130-HI ssh登录不上经验案例

SSH 王子腾 2023-04-26 发表

组网及说明

不涉及

问题描述

组网内有几十台S5130-HI，版本为R1120，重启后发现有两台交换机ssh无法登录，**使用正确密码登录后，直接断开链接，没有任何提示，或者在多次尝试登录后，会提示：The server has disconnected with an error. server message reads: A protocol error occurred. Too many authentication failures for xxx(登录使用的账号)。尝试console也无法登录。**

过程分析

1、跟现场确认重启前做过的操作，重启前10天做过如下配置：
password-control enable（改配置之前就开启过此功能）
因开启password-control功能，全局下默认会有一些值，对全局下的值进行修改，该配置做在全局下----------
sys
password-control aging 90 密码过期时间为90
password-control composition type-number 4
password-control length 8
用户组下配置----------
password-control expired-user-login delay 10 times 5 密码过期10天内，允许登录5次
password-control alert-before-expire 7 密码过期7天前用户登录设备会有提醒
password-control login-attempt 5 exceed lock-time 5用户登录设备密码错误5次账号锁定5分钟

2、现场通过日志服务器查看设备日志后，配置没有问题，NTP时间在配置password-control前后也都是同步的。 日志中有报错是密码错误，多次登录后被加黑名单了。跟现场确认报错可能是尝试不同密码登录时报的错。用正确密码登录时依旧登录不上。
syslog.20230328:Mar 28 09:41:25 11.200.199.103 2023 CQB-P-EXF-SW01 %%10PWDCTL/6/ADDBLACKLIST: -DevIP=17.200.128.103; cnaps was added to the blacklist for failed login attempts.
syslog.20230328:Mar 28 09:41:25 11.200.199.103 2023 CQB-P-EXF-SW01 %%10SSHS/6/SSHS_LOG: -DevIP=17.200.128.103; Authentication failed for cnaps from 17.200.157.20 port 46000 because of invalid username or wrong password ssh2.

3、经验证发现，使能password-control，设备重启后，设备启动时间是2013年，用户登录设备，会记录当前的登录时间是2013年，NTP时间同步之后，设备时间是2023年，用户退出再登录时，会判断距离上一次登录的时间，如果超过90天的闲置时间，就不让用户登录设备了，打印**Failed to login because the idle timer expired.** 新版本有优化，建议是升级到R3507P08。 当前版本用SNMP删不掉NTP，所以需要重启跳过配置启动。
[H3C-radius-rad]display password-control
Global password control configurations:
Password control: Enabled (device management users)
Disabled (network access users)
Password aging: Enabled (90 days)
Password length: Enabled (10 characters)
Password composition: Enabled (2 types, 1 characters per type)
Password history: Enabled (max history records:4)
Early notice on password expiration: 7 days
User authentication timeout: 600 seconds
Maximum login attempts: 3
Action for exceeding login attempts: Lock user for 1 minutes
Minimum interval between two updates:24 hours
User account idle time: 90 days

解决方法

重启交换机，进bootware菜单选择跳过配置启动，进入后导出原来配置，重新刷下配置保存，不要配置password-control 。

然后升级版本到R3507P08