S5560-54C-EI 与思科TACACS做登录认证提示密码错误问题

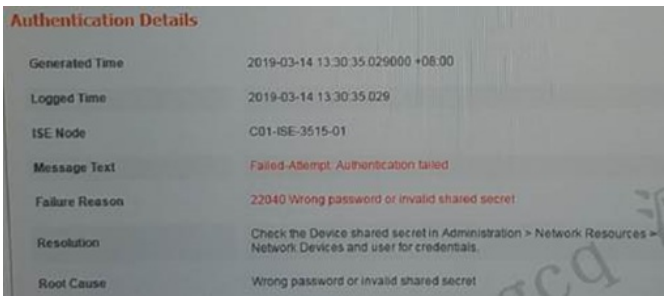
Tacacs 刘嘉炜 2019-04-13 发表

组网及说明

问题描述：

问题描述

S5560-54C-EI 与思科TACACS服务器做登录认证时提示密码错误，网内有一台同配置S7506设备使用TACACS服务器却可以认证成功。下面是TACACS服务器显示S5560-54C-EI的认证结果：



过程分析

过程分析：

1、排查S5560-54C-E配置与认证成功的S7506设置一致。

#

hwtacacs scheme acs

primary authentication 10.100.64.54

primary authorization 10.100.64.54

secondary authentication 10.100.64.57

secondary authorization 10.100.64.57

key authentication cipher c3$vvsSQnmf0+9PaICqhy7DOvSuov+X/ma6XoCO

key authorization cipher c3$R7wMYctGepkcaPkxvbe8O3BnGZty9g1quoBL

user-name-format without-domain

nas-ip 10.118.62.13

#

domain acs

authentication login hwtacacs-scheme acs local

authorization login hwtacacs-scheme acs local

accounting login none

authorization command hwtacacs-scheme acs none

authentication lan-access radius-scheme acs

authorization lan-access radius-scheme acs

accounting lan-access none

#

domain default enable acs

2、通过debugging分析认证失败原因：

Debug信息：

The current terminal is enabled to display debugging logs.

<Y20-BGHJ-HS5560-01>*Mar 14 16:48:48:021 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Processing TACACS authentication.// 处理TACACS认证请求

*Mar 14 16:48:48:021 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Dispatching request, Primitive: authentication.// 分发请求，请求类型为认证

*Mar 14 16:48:48:022 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Creating request data, data type: START// 创建请求数据，数据类型为START

*Mar 14 16:48:48:022 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Session successfully created.// 创建会话成功

*Mar 14 16:48:48:022 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Getting available server, server-ip=10.100.64.54, server-port=49, VPN instance=--(public).// 获取到可用的服务器，服务器IP地址为10.100.64.54，端口号为49，位于公网

*Mar 14 16:48:48:022 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Connecting to server...// 连接服务器

*Mar 14 16:48:48:025 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Reply SocketFd received EPOLLOUT event.// 应答报文套接字接收到EPOLLOUT事件

*Mar 14 16:48:48:025 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Connection

succeeded, server-ip=10.100.64.54, port=49, VPN instance=--(public).// 连接服务器成功，服务器IP地址为10.100.64.54，端口号为49，位于公网
*Mar 14 16:48:48:025 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Encapsulating authentication request packet.// 封装认证请求报文
*Mar 14 16:48:48:025 2019 Y20-BGHJ-HS5560-01 TACACS/7/send_packet:
version: 0xc0 type: AUTHEN_REQUEST seq_no: 1 flag: ENCRYPTED_FLAG
session-id: 0xf0cc92b2
length of payload: 42
action: LOGIN priv_lvl: 0 authen_type: ASCII service: LOGIN
user_len: 4   port_len: 9   rem_len: 12   data_len: 9
user: ping
port: LoopBack0
rem_addr: 10.200.3.154
data: ******
*Mar 14 16:48:48:029 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Reply SocketFd received EPOLLIN event.// 应答报文套接字接收到EPOLLIN事件
*Mar 14 16:48:48:029 2019 Y20-BGHJ-HS5560-01 TACACS/7/recv_packet:
version: 0xc0 type: AUTHEN_REPLY seq_no: 2 flag: ENCRYPTED_FLAG
session-id: 0xf0cc92b2
length of payload: 16
status: STATUS_GETPASS flags: NOECHO
server_msg len: 10 data len: 0
server_msg: password:
data:
*Mar 14 16:48:48:029 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Processing authentication reply packet.// 处理认证回应报文
*Mar 14 16:48:48:030 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Reply message successfully sent.// 成功发送回应消息
*Mar 14 16:48:48:030 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Processed authentication reply message, resultCode: 2.// 处理认证回应数据，回应类型为持续认证
*Mar 14 16:48:48:030 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Creating request data, data type: CONTINUE// 创建持续认证报文并组装发送
*Mar 14 16:48:48:030 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Encapsulating authentication continue request packet.
*Mar 14 16:48:48:030 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Sending authentication continue request packet.
*Mar 14 16:48:48:030 2019 Y20-BGHJ-HS5560-01 TACACS/7/send_packet:
version: 0xc0 type: AUTHEN_CONTINUE seq_no: 3 flag: ENCRYPTED_FLAG
session-id: 0xf0cc92b2
length of payload: 14
user_msg len: ****** data_len: 0 flags: CONTINUE AUTHEN
user_msg: ******
data:
*Mar 14 16:48:48:038 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Reply SocketFd received EPOLLIN event.// 回应报文套接字接收到EPOLLIN事件
*Mar 14 16:48:48:038 2019 Y20-BGHJ-HS5560-01 TACACS/7/recv_packet:
version: 0xc0 type: AUTHEN_REPLY seq_no: 4 flag: ENCRYPTED_FLAG
session-id: 0xf0cc92b2
length of payload: 6
status: STATUS_FAIL flags: ECHO
server_msg len: 0 data len: 0
server_msg:
data:
*Mar 14 16:48:48:038 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Processing authentication reply packet.// 处理认证回应报文
*Mar 14 16:48:48:038 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Reply message successfully sent.// 回应消息发送成功
***Mar 14 16:48:48:039 2019 Y20-BGHJ-HS5560-01 TACACS/7/EVENT: PAM_TACACS: Processed authentication reply message, resultCode: 1.**
%Mar 14 16:48:48:039 2019 Y20-BGHJ-HS5560-01 SSHS/6/SSHS_LOG: Authentication failed for ping from 10.200.3.154 port 61653 ssh2.
//处理了认证回应消息，结果码为0认证成功，1认证失败。说明还是服务器侧与设备密码配置不符，但是和客户反复对比使用的密码都是一致的。
问题还是出在TACACS服务器与密码上，通过抓包分析发现S5560-54C-EI上传密码时所带Payload内

容比正常可上线时多出一个字节（client发送请求时，将pam item封装为item节点的处理中，统一将原始的PAM_STRING类型的item长度也+1--strlen() + 1;），导致上送密码与服务器密码不匹配。
此问题在交换机后续版本中做出下列修改：
在交换机侧将item转换为AVP的处理流程中，统一对数据转换的AVP填充流程做修改，单反PW_STRING类型的属性，均使用传入的length - 1作为AVP的长度以及数据有效长度使用。

解决方法

解决方法：
在交换机版本R1120及之后的版本此问题已经得到解决，因此升级版本后S5560-54C-EI结合思科TACACS登录认证成功。