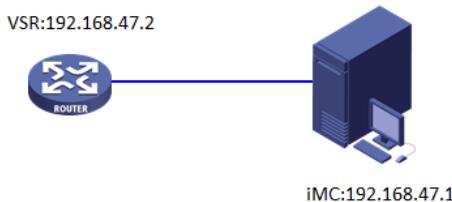


知 iMC V7 TAM结合V7设备进行HWTACACS login认证配置

李树兵 2015-08-19 发表

对需要登录到设备上进行操作的终端用户进行认证、授权以及对终端用户执行的操作进行记录。设备作为HWTACACS的客户端，将用户名和密码发给HWTACACS服务器进行验证，用户验证通过并得到授权之后可以登录到设备上进行操作，HWTACACS服务器上记录用户对设备执行过的命令.并且要求telnet登陆设备的用户不能配置ospf的相关命令。对设备super密码也需要认证。



说明：图中设备VSR1000, version 7.1.049, Release 0204P01
iMC 服务器PLAT 7.1 (E0303), TAM 7.1 (E0302)

1、 路由器配置

开启telnet server服务

telnet server enable

创建HWTACACS方案li

hw tacacs scheme li

配置主认证服务器的IP地址为192.168.47.1, 认证端口号为49

primary authentication 192.168.47.1

配置主授权服务器的IP地址为192.168.47.1, 认证端口号为49

primary authorization 192.168.47.1

配置主计费服务器的IP地址为192.168.47.1, 认证端口号为49

primary accounting 192.168.47.1

配置与认证服务器交互报文时的共享密钥为h3c

key authentication simple h3c

key authorization simple h3c

key accounting simple h3c

配置设备发送HWTACACS报文使用的源地址为192.168.47.2

nas-ip 192.168.47.2

创建ISP域li。

domain li

配置login用户登录认证方法为li方案

authentication login hw tacacs-scheme li local

配置login用户登录授权方法 li方案

authorization login hw tacacs-scheme li local

配置login用户登录计费方法为li方案

accounting login hw tacacs-scheme li local

配置super认证方法为li方案

authentication super hw tacacs-scheme li

配置命令授权方法为li方案

authorization command hw tacacs-scheme li

配置命令统计方法li方案

accounting command hw tacacs-scheme li

user-interface vty 0 4

#配置telnet登陆方式认证为AAA

authentication-mode scheme

配置用户使用VTY用户界面登录设备时，需要服务器授权才能执行命令

command authorization

配置用户使用VTY 用户界面登录设备时，执行的命令需要在HWTACACS服务器上做记录。

command accounting

2、iMC侧配置

配置过程：

1.配置设备类型和设备管理

设备IP地址: 192.168.47.2
共享密钥 *: ***
确认共享密钥 *: ***
认证端口 *: 49
设备区域: MSR
设备类型: MSR
单一连接: 不支持
Watchdog报文: 不支持
描述:

2.配置命令集不能使用ospf命令

命令集名称: ospf
缺省授权方式: 允许
命令集信息

授权	命令行	优先级	修改	删除
拒绝	ospf *	↑↓	☒	✖
拒绝	ospf	↑↓	☒	✖
拒绝	ospf.*	↑↓	☒	✖

共有3条记录。

3.配置Shell profile “456”，设置等级为15 (V7设备的最高权限级别为15)

Shell Profile名称: 456
接入控制列表
授权级别: 15
闲置时长
会话时长
自动执行命令
自定义属性
描述

4、配置授权策略，与之前配置的授权命令集“ospf”和shell profile“456”相关联。

The screenshot shows the 'Modify Authorization Policy' page. At the top, there's a navigation bar with tabs like 'User', 'Business', 'Report', and 'System Management'. Below the navigation is a search bar and a help link. The main area has a title '授权策略信息' (Authorization Policy Information) and a section '基本信息' (Basic Information). It includes fields for '授权策略名' (Policy Name) set to '456', '描述' (Description), and a checkbox for '启用RSA' (Enable RSA). Below this is a table titled '接入授权信息' (Access Authorization Information) with columns: 设备区域 (Device Area), 设备类型 (Device Type), 授权时段 (Authorization Period), Shell Profile, 授权命令集 (Authorization Command Set), 优先级 (Priority), 修改 (Modify), and 删除 (Delete). Two rows are listed: one for '不限' (Unlimited) with 'MSR' type and '456' profile, and another for '不限' with '不限' type and '拒绝' (Reject) profile. At the bottom are '确定' (Confirm) and '取消' (Cancel) buttons.

5. 配置设备用户

The screenshot shows the 'Modify Device User' page. The top navigation bar includes 'Resource', 'User', 'Business', 'Report', 'System Management', and a search bar. The main form contains fields for '帐号名' (Account Name) '123@ii', '用户名' (Username), '登录密码' (Login Password), '登录密码确认' (Login Password Confirmation), '设备用户分组' (Device User Group) '未分组', '分组的授权策略' (Authorization Policy of Group) '不支持命令行访问', '在线数量限制' (Online Quantity Limit) '1', '用户的授权策略' (User Authorization Policy) '456', '失效日期' (Expiration Date), '启用权限提升密码' (Enable Privilege Increase Password) checked, '权限提升密码' (Privilege Increase Password), and '权限提升密码确认' (Privilege Increase Password Confirmation). A note at the bottom says '设备用户自助服务平台的地址为http://IMC主服务器地址:port/imc/noAuth/tam/login.jsp'. At the bottom are '确定' (Confirm) and '取消' (Cancel) buttons.

测试：

```
<H3C>sy
System View: return to User View with Ctrl+Z.
[H3C]ospf 1
[H3C-ospf-1]qu
[H3C]bgp 1
[H3C-bgp]
[H3C-bgp]
[H3C-bgp]qu
[H3C]ospf
System is busy or this command can't be executed because of no such privilege!
[H3C]ospf
System is busy or this command can't be executed because of no such privilege!
[H3C]
[H3C]ospf 1
System is busy or this command can't be executed because of no such privilege!
[H3C]ospf 2
System is busy or this command can't be executed because of no such privilege!
[H3C]ospf 4
System is busy or this command can't be executed because of no such privilege!
[H3C]qu
<H3C>sy
System View: return to User View with Ctrl+Z.
[H3C]bgp 1
[H3C-bgp]qu
[H3C]ospf
System is busy or this command can't be executed because of no such privilege!
[H3C]ospf 1 ?
router-id OSPF Private Router ID
vpn-instance VPN instance
<cr>
[H3C]ospf 1 rou
[H3C]ospf 1 router-id 1.1.1.1
System is busy or this command can't be executed because of no such privilege!
查看日志记录:
```

认证日志:

认证时间 从 2015-07-18 22:19 至 2015-08-18 22:19

认证日志列表

导出日志						
结果	失败原因	登录名	帐号名	认证时间	设备IP地址	详细信息
✓ 成功		123@li	123@li	2015-08-18 22:07:15	192.168.47.2	
✓ 成功		123@li	123@li	2015-08-18 22:04:29	192.168.47.2	
✓ 成功		123@li	123@li	2015-08-18 22:02:29	192.168.47.2	

资源 用户 业务 告警 报表 系统管理

用户 > 设备用户管理 > 日志管理 > 认证日志 > 认证日志详细信息

认证日志详细信息

登录名	123@li
帐号名	123@li
设备用户分组	未分组
认证结果	成功
设备IP地址	192.168.47.2
用户IP地址	192.168.47.1
终端	vty0
认证时间	2015-08-18 22:07:15
动作	登录认证
权限级别	0
认证类型	ASCII认证
服务类型	登录
会话ID	3679816986
序列号	1

授权日志:

禁止使用ospf命令

资源 用户 业务 告警 报表 系统管理

用户 > 设备用户管理 > 日志管理 > 授权日志 > 授权日志详细信息

授权日志详细信息

登录名	123@li
帐号名	123@li
设备用户分组	未分组
授权结果	拒绝
拒绝原因	该命令不允许执行。
授权时间	2015-08-18 22:16:20
Profile属性	
授权级别	15
命令行	ospf 1 router-id 1.1.1.1
策略名称	456
设备IP地址	192.168.47.2
用户IP地址	0.0.0.0
终端	vty0
会话ID	202032866
序列号	1

可以使用其他的命令

资源 用户 业务 告警 报表 系统管理

用户 > 设备用户管理 > 日志管理 > 授权日志 > 授权日志详细信息

授权日志详细信息

登录名	123@li
帐号名	123@li
设备用户分组	未分组
授权结果	允许
授权时间	2015-08-18 22:16:51
Profile属性	
授权级别	15
命令行	display current-configuration
策略名称	456
设备IP地址	192.168.47.2
用户IP地址	0.0.0.0
终端	vty0
会话ID	1946853522
序列号	1

审计日志:

审计日志列表						
导出日志						
登录名	帐号名	命令行	审计类型	审计时间 ▾	设备IP地址	详细信息
123@li	123@li	display current-configuration	命令行结束	2015-08-18 22:16:51	192.168.47.2	
123@li	123@li	quit	命令行结束	2015-08-18 22:16:08	192.168.47.2	
123@li	123@li	bgp 1	命令行结束	2015-08-18 22:16:07	192.168.47.2	
123@li	123@li	system-view	命令行结束	2015-08-18 22:16:05	192.168.47.2	
123@li	123@li	quit	命令行结束	2015-08-18 22:16:04	192.168.47.2	

登陆过程中在设备上debugging hwtacacs all

在设备上的操作如下:

```
<H3C>sy
System View: return to User View with Ctrl+Z.
[H3C]qu
<H3C>sy
System View: return to User View with Ctrl+Z.
```

[H3C]

设备上debug显示的信息:

```
<H3C>debugging hwtacacs all
<H3C>t m
The current terminal is enabled to display logs.
<H3C>t d
The current terminal is enabled to display debugging logs.
<H3C>*Aug 18 22:24:50:207 2015 H3C TACACS/7/EVENT: PAM_TACACS: Processing TACACS
stop-accounting.
*Aug 18 22:24:50:207 2015 H3C TACACS/7/EVENT: PAM_TACACS: Dispatching request, P
rimitive: accounting-stop.
*Aug 18 22:24:50:207 2015 H3C TACACS/7/EVENT: PAM_TACACS: Creating request data,
data type: START
*Aug 18 22:24:50:207 2015 H3C TACACS/7/EVENT: PAM_TACACS: Session successfully c
reated.
*Aug 18 22:24:50:207 2015 H3C TACACS/7/EVENT: PAM_TACACS: Getting available serv
er, server-ip=192.168.47.1, server-port=49, VPN instance=--(public).
*Aug 18 22:24:50:242 2015 H3C TACACS/7/EVENT: PAM_TACACS: Connecting to server..
.
*Aug 18 22:24:50:242 2015 H3C TACACS/7/EVENT: PAM_TACACS: Reply SocketFd receive
d EPOLLOUT event.
*Aug 18 22:24:50:242 2015 H3C TACACS/7/EVENT: PAM_TACACS: Connection succeeded,
server-ip=192.168.47.1, port=49, VPN instance=--(public).
*Aug 18 22:24:50:242 2015 H3C TACACS/7/EVENT: PAM_TACACS: Encapsulating accounti
ng request packet.
*Aug 18 22:24:50:242 2015 H3C TACACS/7/send_packet:
version: 0xc0 type: ACCOUNT_REQUEST seq_no: 1 flag: ENCRYPTED_FLAG
session-id: 0xd4e0bfef
length of payload: 75
flags: STOP
authen_method: NONE authen_service: LOGIN
user_len: 6 port_len: 4 rem_len: 0 arg_cnt: 5
arg0_len: 9 arg1_len: 10 arg2_len: 13 arg3_len: 11
arg4_len: 8
user: 123@li //认证的用户是123@li
port: vty0 //通过vty0登陆
rem_addr:
arg0: task_id=0 arg1: timezOne=0
arg2: service=shell arg3: priv-lvl=15 //服务是shell命令行, 等级为15
arg4: cmd=quit //下发的命令为 quit
*Aug 18 22:24:50:261 2015 H3C TACACS/7/EVENT: PAM_TACACS: Reply SocketFd receive
d EPOLLIN event.
*Aug 18 22:24:50:261 2015 H3C TACACS/7/recv_packet:
version: 0xc0 type: ACCOUNT_REPLY seq_no: 2 flag: ENCRYPTED_FLAG
session-id: 0xd4e0bfef
length of payload: 5
server_msg len: 0 data len: 0 status: STATUS_SUCCESS
```

```
server_msg:  
data:  
*Aug 18 22:24:50:261 2015 H3C TACACS/7/EVENT: PAM_TACACS: Processing accounting  
reply packet.  
*Aug 18 22:24:50:261 2015 H3C TACACS/7/EVENT: PAM_TACACS: Processed accounting-s  
top reply message, resultCode: 0.  
*Aug 18 22:24:50:261 2015 H3C TACACS/7/EVENT: PAM_TACACS: TACACS stop-accounting  
succeeded.  
*Aug 18 22:24:50:261 2015 H3C TACACS/7/EVENT: PAM_TACACS: Reply message successf  
ully sent.  
*Aug 18 22:24:52:881 2015 H3C TACACS/7/EVENT: PAM_TACACS: Processing TACACS auth  
orization.  
*Aug 18 22:24:52:881 2015 H3C TACACS/7/EVENT: PAM_TACACS: Dispatching request, P  
rimitive: authorization.  
*Aug 18 22:24:52:882 2015 H3C TACACS/7/EVENT: PAM_TACACS: Creating request data,  
data type: START  
*Aug 18 22:24:52:882 2015 H3C TACACS/7/EVENT: PAM_TACACS: Session successfully c  
reated.  
*Aug 18 22:24:52:882 2015 H3C TACACS/7/EVENT: PAM_TACACS: Getting available serv  
er, server-ip=192.168.47.1, server-port=49, VPN instance=--(public).  
*Aug 18 22:24:52:882 2015 H3C TACACS/7/EVENT: PAM_TACACS: Connecting to server..  
. .  
*Aug 18 22:24:52:883 2015 H3C TACACS/7/EVENT: PAM_TACACS: Reply SocketFd receive  
d EPOLLOUT event.  
*Aug 18 22:24:52:883 2015 H3C TACACS/7/EVENT: PAM_TACACS: Connection succeeded,  
server-ip=192.168.47.1, port=49, VPN instance=--(public).  
*Aug 18 22:24:52:883 2015 H3C TACACS/7/EVENT: PAM_TACACS: Encapsulating authoriz  
ation request packet.  
*Aug 18 22:24:52:883 2015 H3C TACACS/7/send_packet:  
version: 0xc0 type: AUTHOR_REQUEST seq_no: 1 flag: ENCRYPTED_FLAG  
session-id: 0xe9467887  
length of payload: 61  
authen_method: NONE priv_lv1: 15 authen_type: ASCII authen_service: LOGIN  
user_len: 6 port_len: 4 rem_len: 0 arg_cnt: 3  
arg0_len: 13 arg1_len: 15 arg2_len: 12  
user: 123@li  
port: vty0  
rem_addr:  
arg0: service=shell arg1: cmd=system-view  
arg2: cmd-arg=<cr>  
*Aug 18 22:24:53:010 2015 H3C TACACS/7/EVENT: PAM_TACACS: Reply SocketFd receive  
d EPOLLIN event.  
*Aug 18 22:24:53:010 2015 H3C TACACS/7/recv_packet:  
version: 0xc0 type: AUTHOR_REPLY seq_no: 2 flag: ENCRYPTED_FLAG  
session-id: 0xe9467887  
length of payload: 6  
Status: STATUS_PASS_ADD arg_cnt: 0 server_msg len: 0 data len: 0  
server_msg:  
data:  
*Aug 18 22:24:53:010 2015 H3C TACACS/7/EVENT: PAM_TACACS: Processing authorizati  
on reply packet.  
*Aug 18 22:24:53:010 2015 H3C TACACS/7/EVENT: PAM_TACACS: Reply message successf  
ully sent.  
*Aug 18 22:24:53:010 2015 H3C TACACS/7/EVENT: PAM_TACACS: Processed authorizatio  
n reply message, resultCode: 0.  
*Aug 18 22:24:53:010 2015 H3C TACACS/7/EVENT: PAM_TACACS: TACACS authorization s  
ucceeded.  
*Aug 18 22:24:53:010 2015 H3C TACACS/7/EVENT: PAM_TACACS: Processing TACACS stop  
-accounting.  
*Aug 18 22:24:53:010 2015 H3C TACACS/7/EVENT: PAM_TACACS: Dispatching request, P  
rimitive: accounting-stop.  
*Aug 18 22:24:53:010 2015 H3C TACACS/7/EVENT: PAM_TACACS: Creating request data,  
data type: START  
*Aug 18 22:24:53:011 2015 H3C TACACS/7/EVENT: PAM_TACACS: Session successfully c
```

reated.
*Aug 18 22:24:53:011 2015 H3C TACACS/7/EVENT: PAM_TACACS: Getting available server, server-ip=192.168.47.1, server-port=49, VPN instance=--(public).
*Aug 18 22:24:53:083 2015 H3C TACACS/7/EVENT: PAM_TACACS: Connecting to server..
. .
*Aug 18 22:24:53:083 2015 H3C TACACS/7/EVENT: PAM_TACACS: Reply SocketFd receive d EPOLLOUT event.
*Aug 18 22:24:53:084 2015 H3C TACACS/7/EVENT: PAM_TACACS: Connection succeeded, server-ip=192.168.47.1, port=49, VPN instance=--(public).
*Aug 18 22:24:53:084 2015 H3C TACACS/7/EVENT: PAM_TACACS: Encapsulating accountng request packet.
*Aug 18 22:24:53:084 2015 H3C TACACS/7/send_packet:
version: 0xc0 type: ACCOUNT_REQUEST seq_no: 1 flag: ENCRYPTED_FLAG
session-id: 0xf8fdfd66
length of payload: 82
flags: STOP
authen_method: NONE authen_service: LOGIN
user_len: 6 port_len: 4 rem_len: 0 arg_cnt: 5
arg0_len: 9 arg1_len: 10 arg2_len: 13 arg3_len: 11
arg4_len: 15
user: 123@li
port: vty0
rem_addr:
arg0: task_id=0 arg1: timezOne=0
arg2: service=shell arg3: priv-lvl=15
arg4: cmd=system-view
*Aug 18 22:24:53:153 2015 H3C TACACS/7/EVENT: PAM_TACACS: Reply SocketFd receive d EPOLLIN event.
*Aug 18 22:24:53:153 2015 H3C TACACS/7/recv_packet:
version: 0xc0 type: ACCOUNT_REPLY seq_no: 2 flag: ENCRYPTED_FLAG
session-id: 0xf8fdfd66
length of payload: 5
server_msg len: 0 data len: 0 status: STATUS_SUCCESS
server_msg:
data:
*Aug 18 22:24:53:153 2015 H3C TACACS/7/EVENT: PAM_TACACS: Processing accounting reply packet.
*Aug 18 22:24:53:153 2015 H3C TACACS/7/EVENT: PAM_TACACS: Processed accounting-stop reply message, resultCode: 0.
*Aug 18 22:24:53:153 2015 H3C TACACS/7/EVENT: PAM_TACACS: TACACS stop-accounting succeeded.
*Aug 18 22:24:53:153 2015 H3C TACACS/7/EVENT: PAM_TACACS: Reply message successfully sent.

1. 要特别注意正则表达式的使用，比如限制不能使用ospf的命令，一开始设置的只是 Ospf 和ospf *

但是其他命令，比如 ospf 1 或者 ospf 1 rou 1.1.1.1

类似的命令就不能限制了

这时需要配置 ospf.* 来限制ospf 1或者ospf 1 rou 1.1.1.1 等类似的命令

因为在正则表达式里面“.”代表的是 空格

2. 注意配置

```
# 配置命令授权方法为li方案  
authorization command hwtacacs-scheme li  
# 配置命令统计方法li方案  
accounting command hwtacacs-scheme li
```

这两个命令，否则会出现认证通过了，但是telnet之后提示服务拒绝，无法对设备进行配置。