ComwareV5平台交换机结合CiscoACS 5.2进行TACACS认证配置及经验总结

Tacacs 秦军 2014-03-05 发表

ComwareV5平台交换机结合CiscoACS 5.2进行TACACS认证配置及经验总结

本文主要讲述ComwareV5平台交换机与Cisco ACS 5.2认证服务器通过TACACS方式进行Telnet认证、授权和计费配置方法以及注意事项。

一、组网需求：

PC直连S5500-EI，S5500-EI直连Cisco ACS 5.2服务器。

1. PC

PC使用Windows 7操作系统，IP地址：10.1.1.1/24。

2. S5500-EI

S5500-EI使用软件版本Release 2220P02；

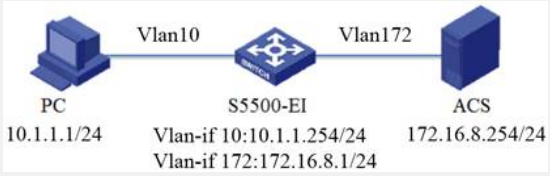
Vlan-if 10 IP地址：10.1.1.254/24，用于与PC互联；

Vlan-if 172 IP地址：172.16.8.1/24，用于与ACS服务器互联。

3. Cisco ACS 5.2

IP address：172.16.8.254。

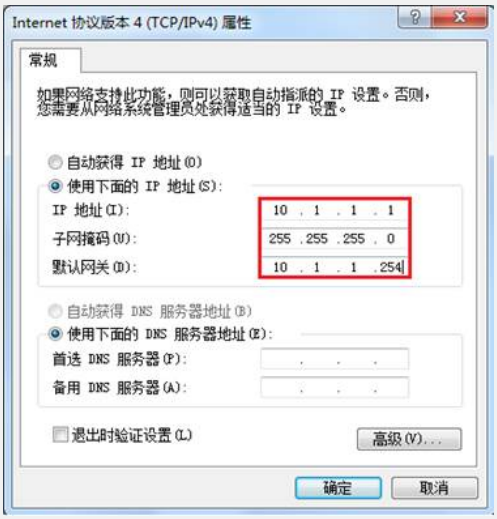
二、组网图：



三、配置步骤：

1. PC配置

配置IP地址：



2. S5500-EI配置

S5500-EI配置

```
telnet server enable
#
vlan 10
#
vlan 172
#
interface Vlan-interface10
 ip address 10.1.1.254 255.255.255.0
#
interface Vlan-interface172
 ip address 172.16.8.1 255.255.255.0
#
interface GigabitEthernet1/0/23
 port access vlan 10
#
interface GigabitEthernet1/0/24
 port access vlan 172
#
user-interface vty 0 15
 authentication-mode scheme
 command authorization  //使能命令行授权功能，如果不需要服务器对命令行做授权，则无需配置
 command accounting  //使能命令行计费功能，如果不需要服务器对命令行做计费，则无需配置。
#
hwtacacs scheme login
 primary authentication 172.16.8.254
 primary authorization 172.16.8.254
 primary accounting 172.16.8.254
 nas-ip 172.16.8.1
 key authentication 123456
 key authorization 123456
 key accounting 123456
 user-name-format without-domain
#
domain system
 authentication login hwtacacs-scheme login
 authorization login hwtacacs-scheme login
 accounting login hwtacacs-scheme login
 authorization command hwtacacs-scheme login
 accounting command hwtacacs-scheme login
#
```

3. Cisco ACS5.2配置

3.1命令行配置

Cisco ACS配置
interface GigabitEthernet 0 ip address 172.16.8.254 255.255.255.0 no shutdown ! ip default-gateway 172.16.8.1

3.2 Web页面配置

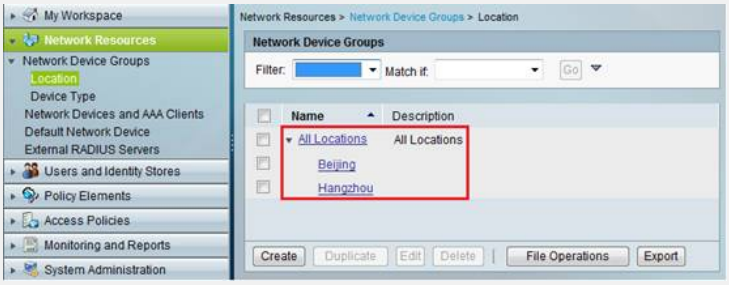
1）通过GUI登录ACS

通过IE浏览器键入https://172.16.8.254登录ACS WEB页面。

2）配置网络资源

需要预先规划好网络设备组NDG的分配方式，比如按照设备所处位置（Location）或者设备所属类型（Device Type）进行规划。

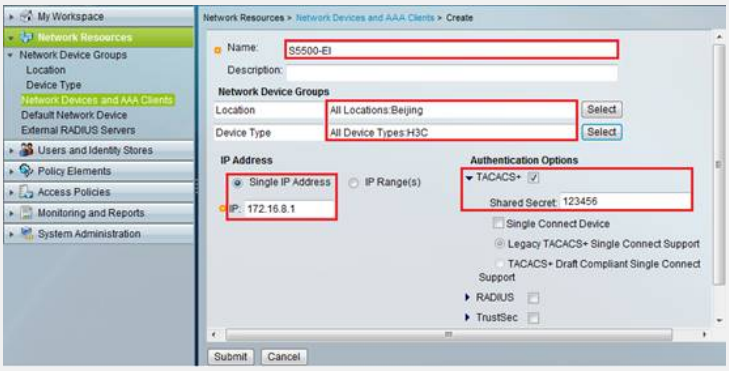
网络资源组（Network Device Groups）>网络设备组（Network Device Groups）>位置（Location）视图下创建新的位置：



网络资源组（Network Device Groups）>网络设备组（Network Device Groups）>设备类型（Device Type）视图下创建新的设备类型：

网络资源组（Network Device Groups）>网络设备组（Network Device Groups）>网络设备和AAA客户端（Network Devices and AAA Clients）视图下创建网络设备（Network Devices）：

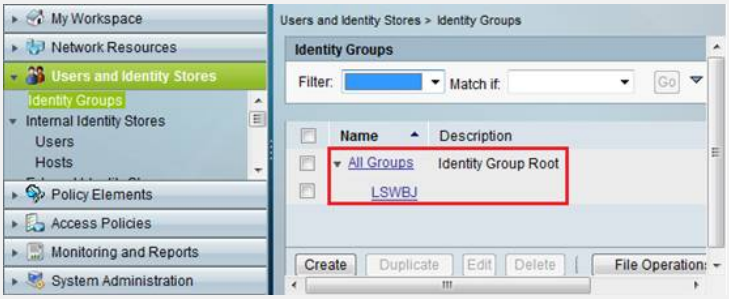
将新创建的设备分配到指定位置（Location）、设备类型（Device Type），指定设备的IP地址，选择TACACS+协议，配置共享密钥，必须保证此密钥与设备上设置的共享密钥完全一致。



创建完成后返回网络设备列表：

3）配置用户组和用户

用户与身份库（Users and Identity Stores）>身份组（Identity Groups）视图下创建新的身份组，并分配到All Groups组中：

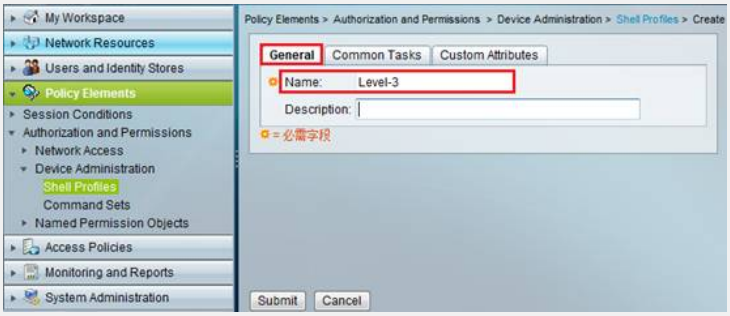


用户与身份库（Users and Identity Stores）> 内部身份库（Internal Identity Stores）>用户（Users）视图下创建新用户，设置用户密码，并将用户分配到特定组：

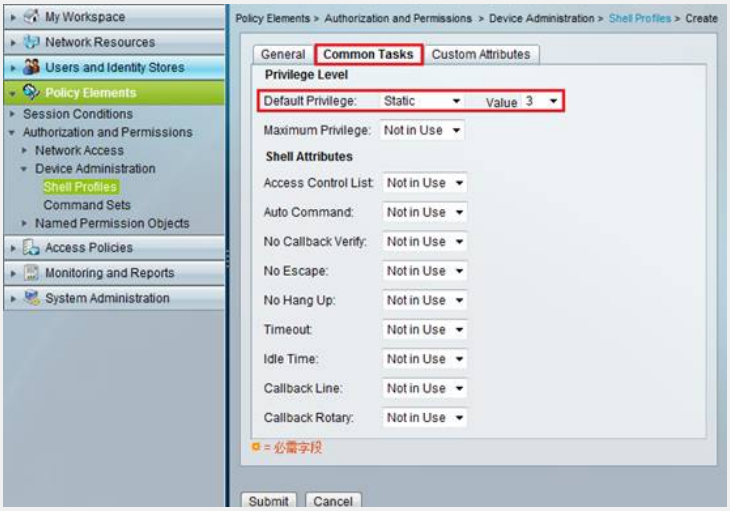
创建完成后返回内部用户列表：

4）配置策略元素

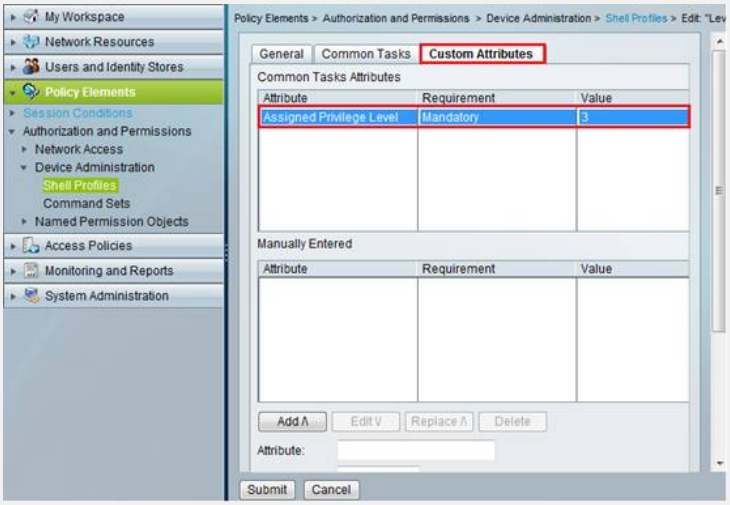
策略元素（Policy Elements）>授权与权限（Authorization and Permissions）>设备管理（ Device Administration）> Shell Profiles视图下创建授权策略，其中Permit Access是缺省的授权策略，这里再定义一个授权级别为三级的授权策略。



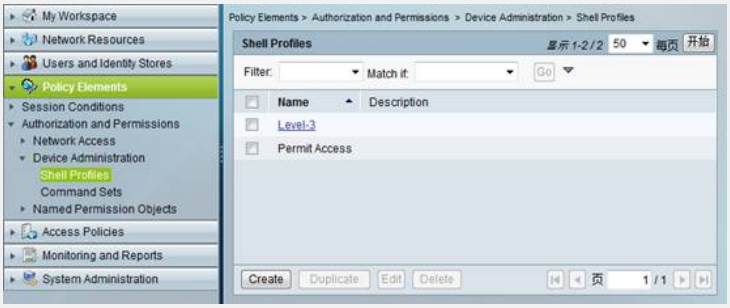
定义授权级别为三级：



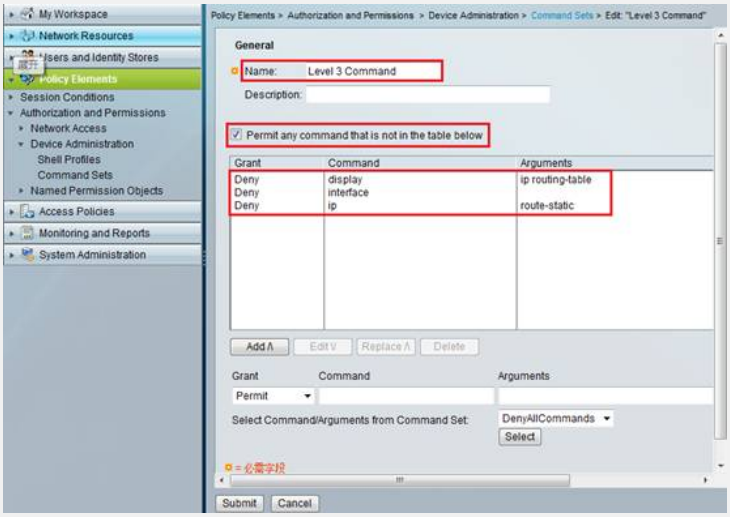
这时在定制属性中可以看到名称为Assigned Privilege Level，属性值为3的属性：



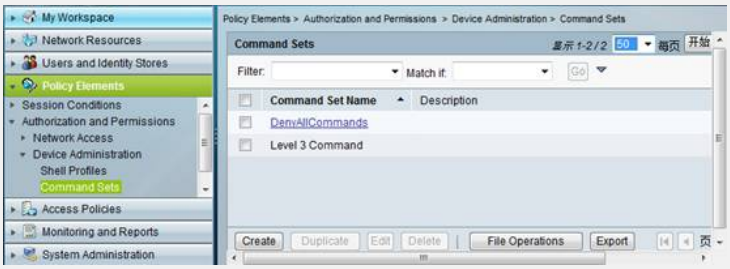
配置完成后返回Shell Profiles列表：



如果要对命令进行授权，在设备授权操作中配置授权命令集。策略元素（Policy Elements）>授权与权限（Authorization and Permissions）>设备管理（ Device Administration）> 授权命令集（Command Sets）视图下创建授权命令集，这里创建三级授权所使用的授权命令集，除了不允许查看路由表、进入接口视图、添加静态路由以外，允许其他所有的三级权限命令。其中DenyAllCommands是缺省的命令集。



配置完成后返回授权命令集列表：



5）配置接入服务

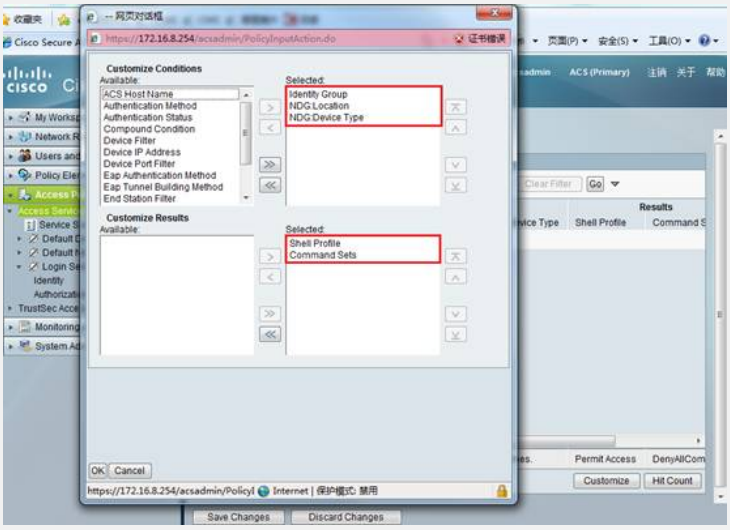
接入策略（Access Policies ）>接入服务（Access Services）视图下创建新的接入服务。缺省情况下存在设备管理（Default Device Admin）和网络接入控制（Default Network Access）两个默认的访问策略。

创建接入服务时，可以基于已存在的访问策略进行配置：

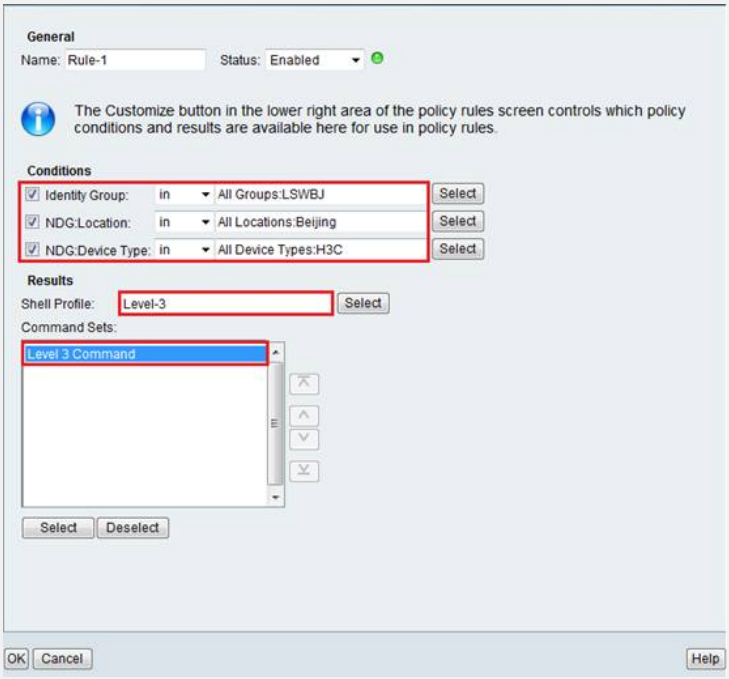
点击“下一步”，勾选允许的认证协议，这里只需勾选PAP、CHAP即可：

配置完成后，返回接入服务列表：

在接入服务（Access Services）中配置授权操作，单击接入服务“Login Service”对应的“Authorization”。首先选择定制方式（Customize），选择使用这一接入服务的身份组（Identity Group）、位置（NDG Location）以及设备类型（NDG Device Type），并对认证成功的用户按照Shell Profile和授权命令集，为认证用户下发授权级别以及对命令做授权：



然后创建授权规则，选择用户组、NDG位置、NDG设备类型，以及Shell Profile和授权命令集：



配置完成后返回授权策略列表：

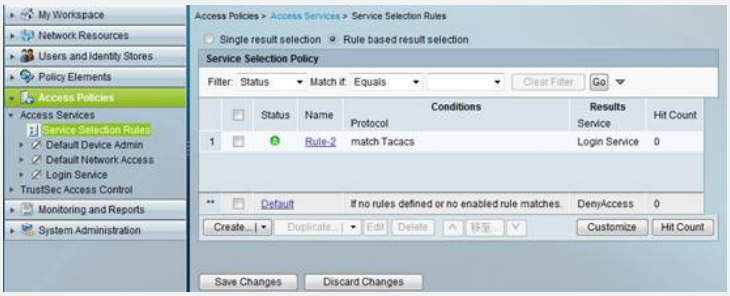
单击“Save Changes”保存配置。

6）配置服务选择规则

配置服务选择规则，选择已创建的接入服务。

接入策略（Access Policies ）>接入服务（Access Services）>服务选择规则（Service Selection Rules）视图下，创建服务选择策略，选择匹配TACACS协议时所使用的接入服务：

配置完成后，返回服务选择策略列表：



单击“Save Changes”保存配置。

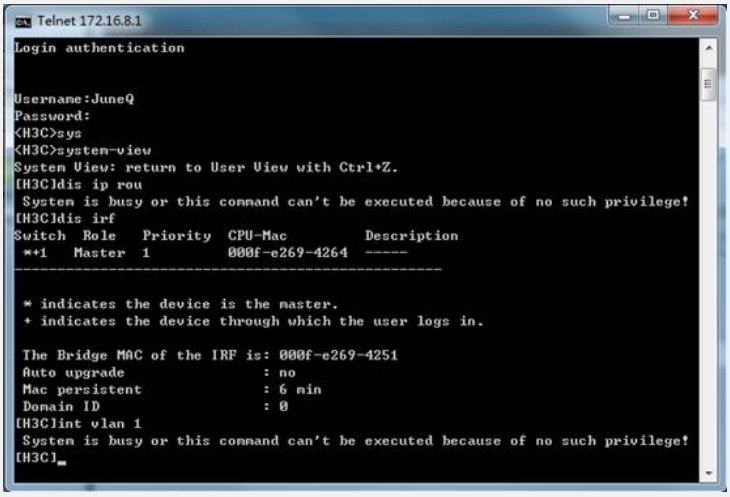
4. 验证

Telnet登录设备后，查看用户的授权级别为三级：

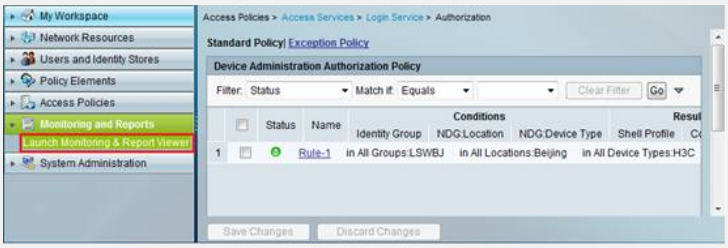
```
display users
The user application information of the user interface(s):
  Idx UI      Delay    Type Userlevel
F 0   AUX 0   00:00:00      3
  25  VTY 0   00:00:26 TEL  3


Following are more details.
VTY 0    :
        User name: JuneQ
        Location: 10.1.1.1
 +    : Current operation user.
 F    : Current operation user work in async mode.
```

分别测试授权和未授权的命令：

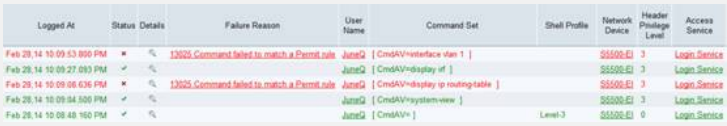


通过ACS的监控功能，查看登录用户的认证、授权、计费的记录：

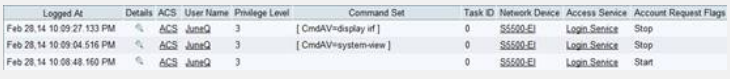


查看TACACS协议的认证、授权、计费的记录信息：

查看TACACS授权记录，可以看到认证成功后调用的Shell Profile对用户下发授权级别，以及对于命令授权成功、未授权的记录信息：



如果没有配置命令行授权功能，则当前用户执行的每一条命令都会发送到HWTACACS服务器上做记录；如果配置了命令行授权功能，则当前用户执行的并且授权成功的命令都会发送到HWTACACS服务器上做记录。这里在开启命令行授权的情况下，查看TACACS计费记录，只记录了授权成功的命令行：



四、配置关键点：

1. HWTACACS认证、授权、计费报文的共享密钥必须与ACS侧TACACS+的共享密钥一致；
2. 默认情况下，在配置接入服务的授权项时，只能按照Shell Profile下发授权，如果要调用授权命令集对每条命令做授权服务，则首先要在定制方式中选择授权命令集（Command Sets）；
3. 配置服务选择策略时，如果存在多条策略，注意调整策略的先后顺序，按照从上到下的顺序对协议类型进行匹配。