ComwareV5平台交换机通过CiscoACS5.2 Radius认证配置总结

Radius **秦军** 2013-10-31 发表

ComwareV5平台交换机通过Cisco ACS 5.2认证配置总结

本文主要讲述ComwareV5平台与Cisco ACS 5.2认证服务器通过Radius方式进行Telnet认证的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 address：10.1.1.1/24。

2. S5500-EI

S5500-EI使用软件版本Release 2208；

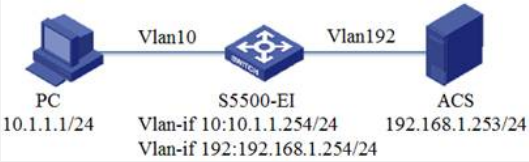
Vlan10 address：10.1.1.254/2l;

Vlan192 address：192.168.1.254/24与Server互连接口属vlan192。

3. Cisco ACS 5.2

IP address：192.168.1.253。

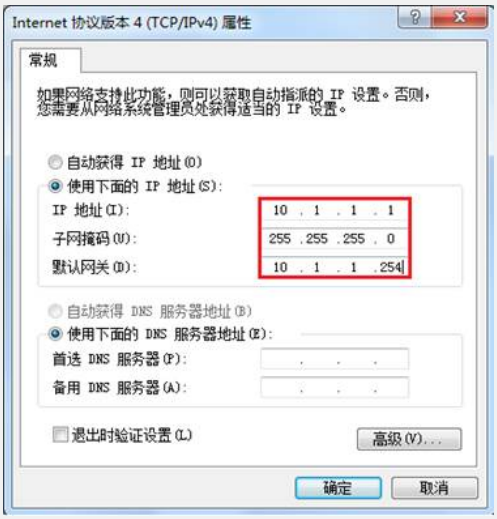
二、组网图：



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 192
#
interface Vlan-interface10
 ip address 10.1.1.254 255.255.255.0
#
interface Vlan-interface192
 ip address 192.168.1.254 255.255.255.0
#
interface GigabitEthernet1/0/23
 port access vlan 10
#
interface GigabitEthernet1/0/24
 port access vlan 192
#
user-interface vty 0 15
 authentication-mode scheme
#
radius scheme login
 server-type extended
 primary authentication 192.168.1.253
 primary accounting 192.168.1.253
 key authentication 123
 key accounting 123
 user-name-format without-domain
 nas-ip 192.168.1.254
#
domain system
 authentication login radius-scheme login
 authorization login radius-scheme login
 accounting login radius-scheme login
 #
```

3. Cisco ACS5.2配置

3.1命令行配置

Cisco ACS配置
interface GigabitEthernet 0 ip address 192.168.1.253 255.255.255.0 no shutdown ! ip default-gateway 192.168.1.254

3.2 Web页面配置

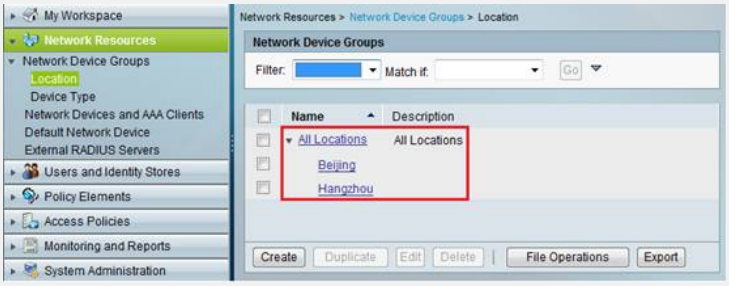
1）通过GUI登录ACS

通过IE浏览器键入https://192.168.1.253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。

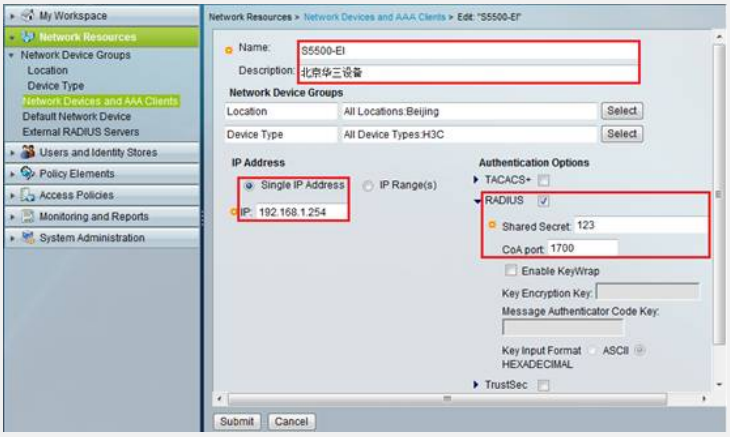
网络资源组>网络设备组NDG下配置位置（Location）：



网络资源组>网络设备组NDG下配置设备类型（Device Type）：

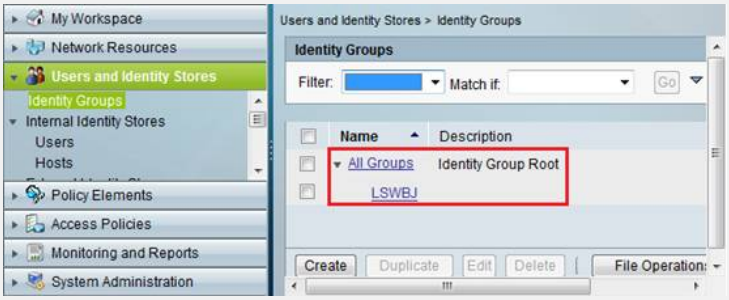
网络资源组>网络设备组NDG下配置网络设备和AAA客户端（Network Devices and AAA Clients）：

将S5500-EI分配到指定站点、设备类型组，指定设备的IP地址，选择Radius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。

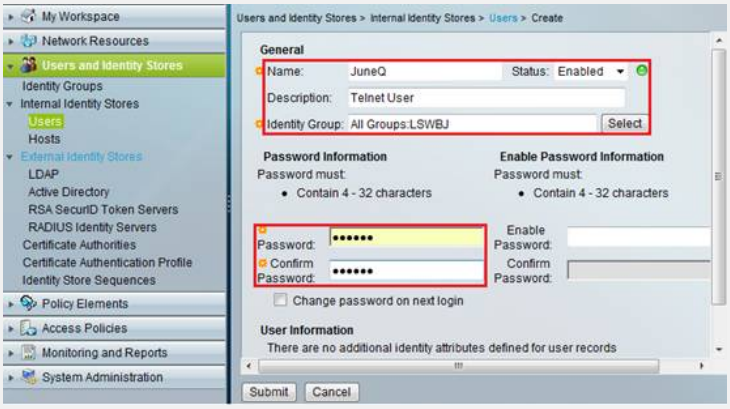


3）配置用户组和用户

创建身份组（Identity Groups），并分配到All Groups组中：

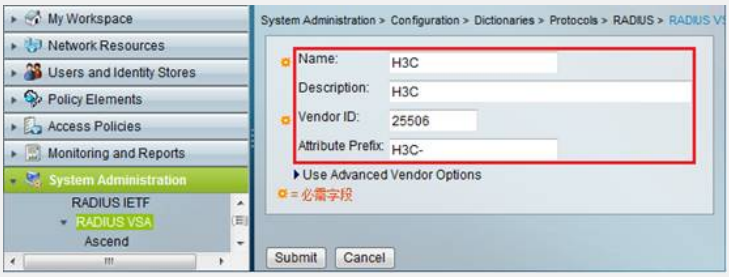


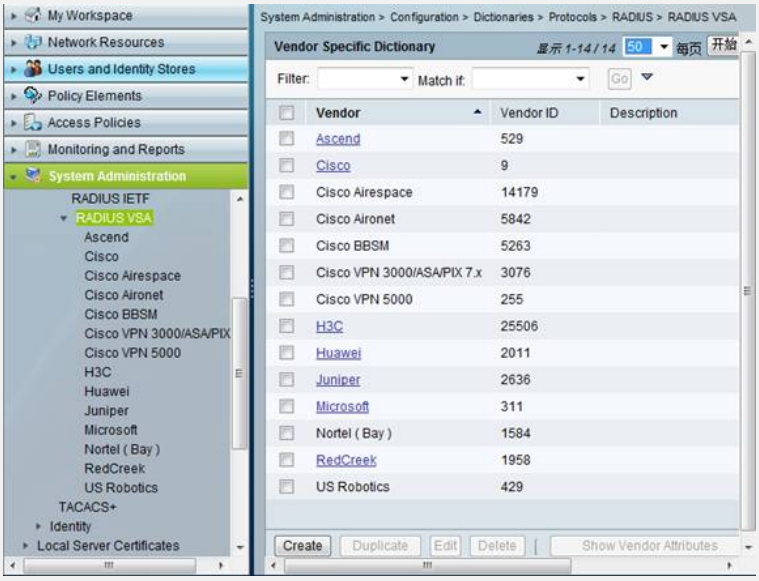
创建用户（Users），设置用户密码，并将用户分配到特定组：



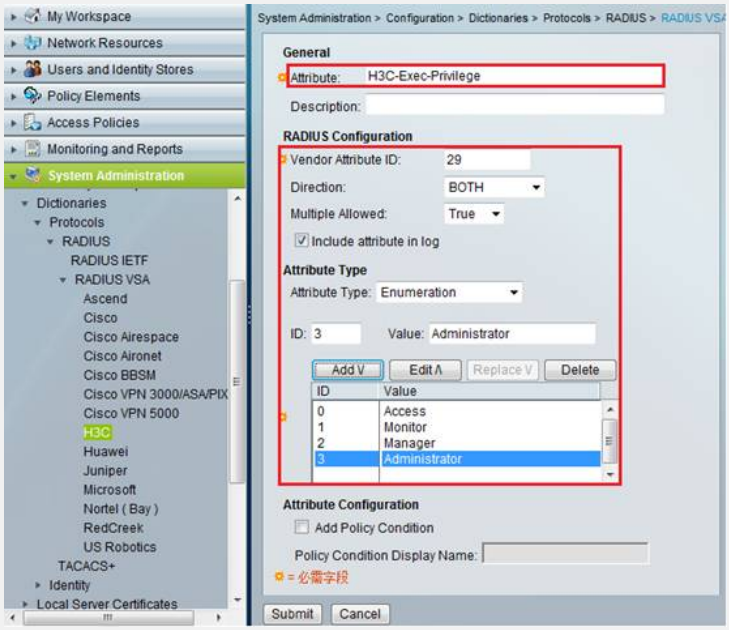
4）创建H3C私有属性

导入H3C字典，新建Radius VSA（Vendor-Specific-Attributes），Name：H3C，Vendor ID：25506，Attribute Prefix：H3C-：





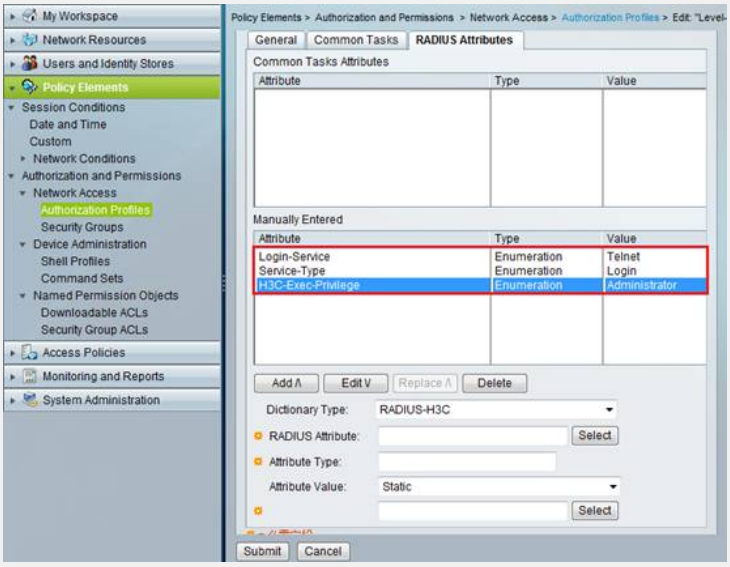
定义EXEC用户优先级扩展属性，Attrbute：H3C-Exec-Privilege，Vendor Attribute ID：29，Direction：BOTH，Multiple Allowed：True，Attribute Type：Enumeration，同时添加ID值分别为0、1、2、3的权限级别属性。



5）配置策略元素

创建授权策略：

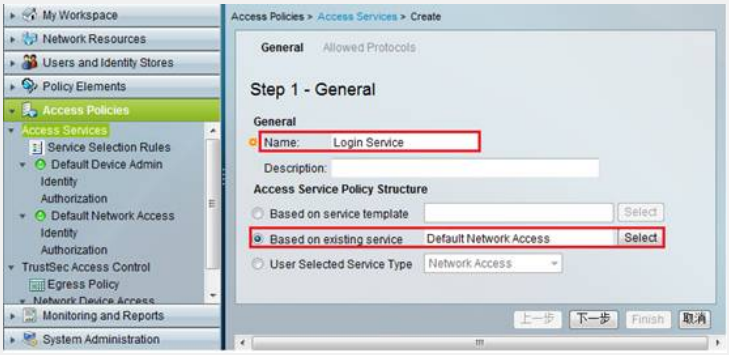
添加Radius属性，主要包含三个属性：RADIUS-IEIF下的Login-Service，Enum Name选择Telnet；RADIUS-IEIF下的Service-Type，Enum Name选择Login；RADIUS-H3C下的H3C-Exec-Privilege，Enum Name选择Administrator。



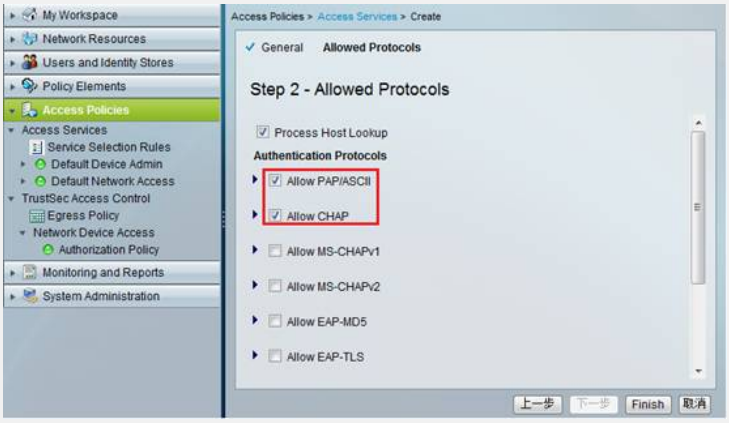
6）配置接入访问策略

缺省情况下存在设备管理和网络接入控制两个默认访问策略。

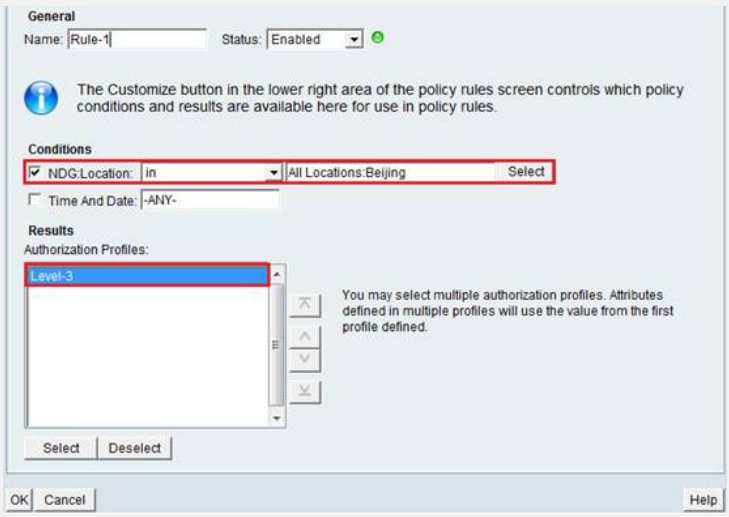
创建接入服务，可以基于已存在的服务进行配置：

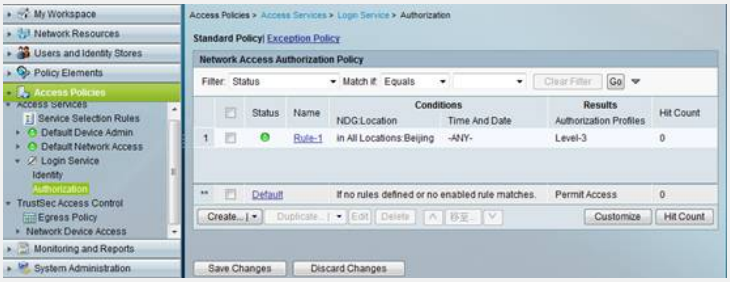


勾选认证协议，这里只需勾选PAP、CHAP即可：



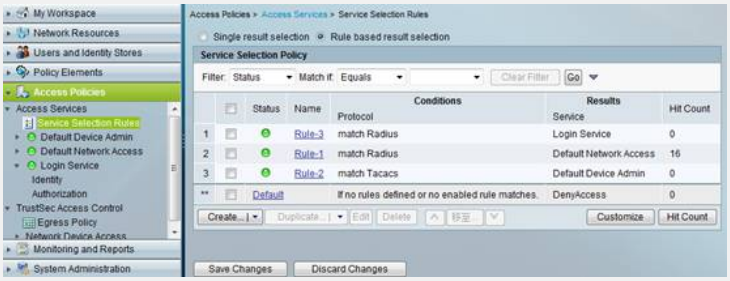
在接入服务中配置授权操作，创建授权规则，选择NDG位置以及授权策略：





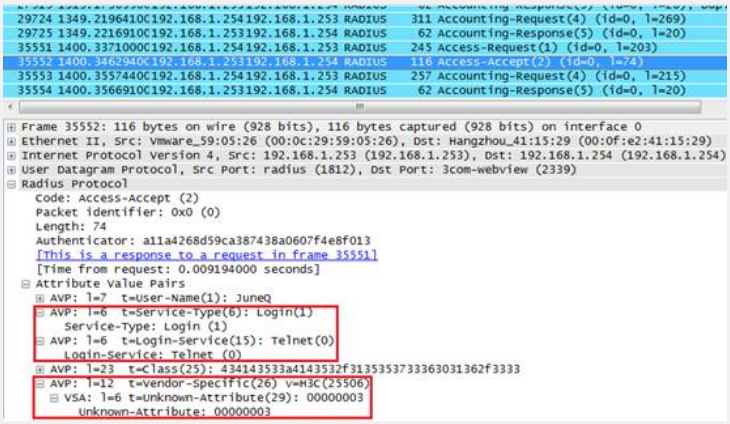
配置服务选择规则，选择已创建的接入服务。

接入策略>接入服务>服务选择规则，创建服务选择策略，选择匹配Radius协议时使用的接入服务：



4. 验证

认证时对设备抓包，在获取的Radius Access-Accept报文中可以看到Service-Type、Login-Service、Exec-Privilege等属性。



在监控与报告中可以获取详细的日志信息，以便认证失败时进行排查。

四、配置关键点：

1. 配置ACS时必须定义扩展属性H3C-Exec-Privilege为用户下发权限，也可以使用Huawei定义的扩展属性，Vendor ID：2011，属性名称hw_Exec_Privilege，定义方法与H3C-Exec-Privilege完全相同；
2. 在设备侧配置Radius Scheme时，需要将设备支持的RADIUS服务器类型设置为extended类型；
3. 配置服务选择规则，注意调整准则的先后顺序，按照从上到下的顺序对协议类型进行匹配。