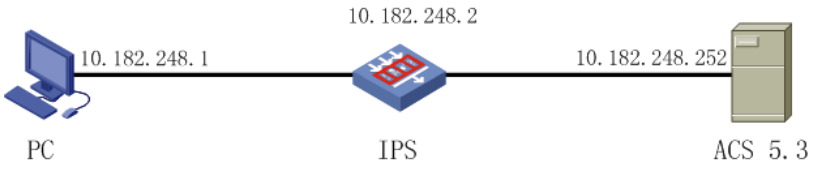
IPS结合Cisco ACS做Radius登陆认证配置案例

认证 王晓辉 2015-10-16 发表

通过Radius认证功能，IPS可以结合第三方AAA服务器进行登陆认证。本文以Cisco ACS 5.3为例，介绍了如何利用ACS对IPS进行Radius登陆认证。

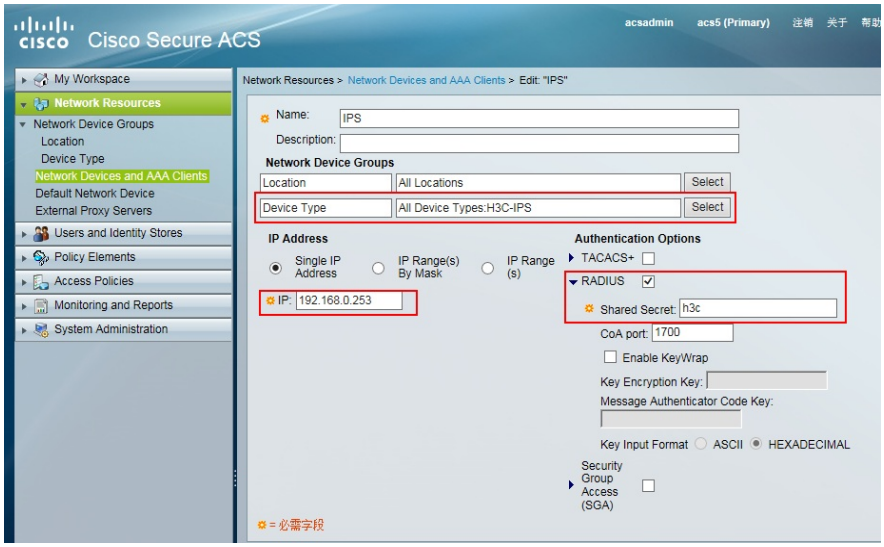


1.IPS Radius配置截图：

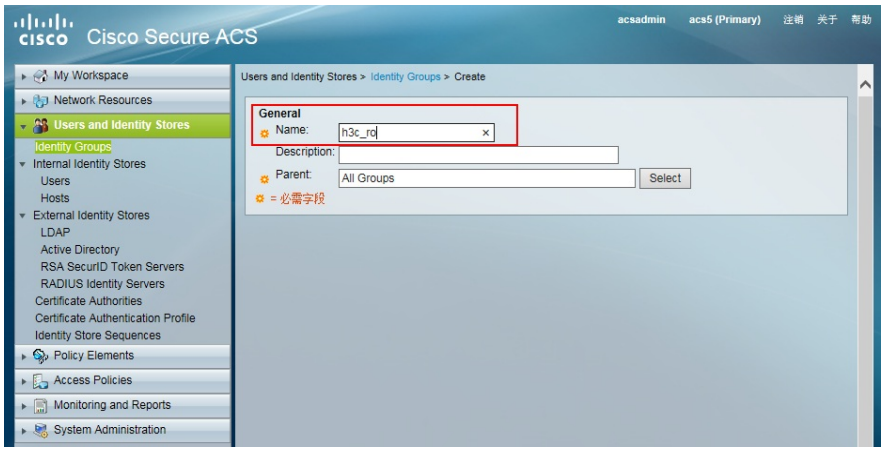
2.ACS 5.3配置截图：

1）添加device group：H3C-IPS

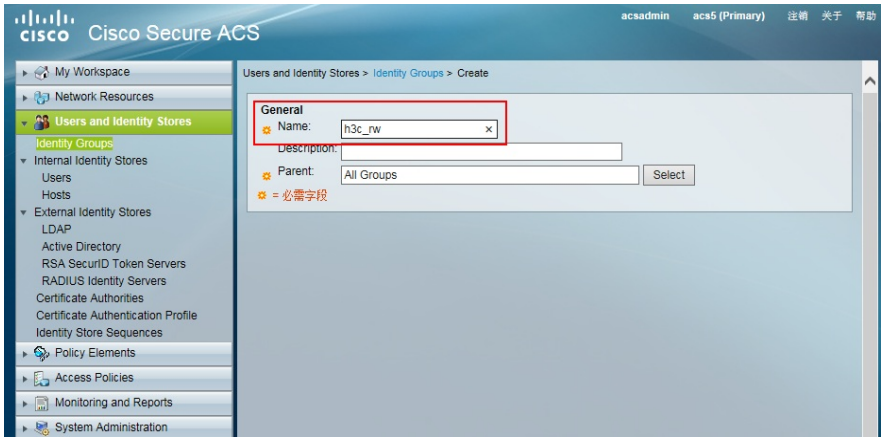
2）添加IPS，属于device group：H3C-IPS



3）添加identity groups：h3c_ro，只读帐号属于该分组

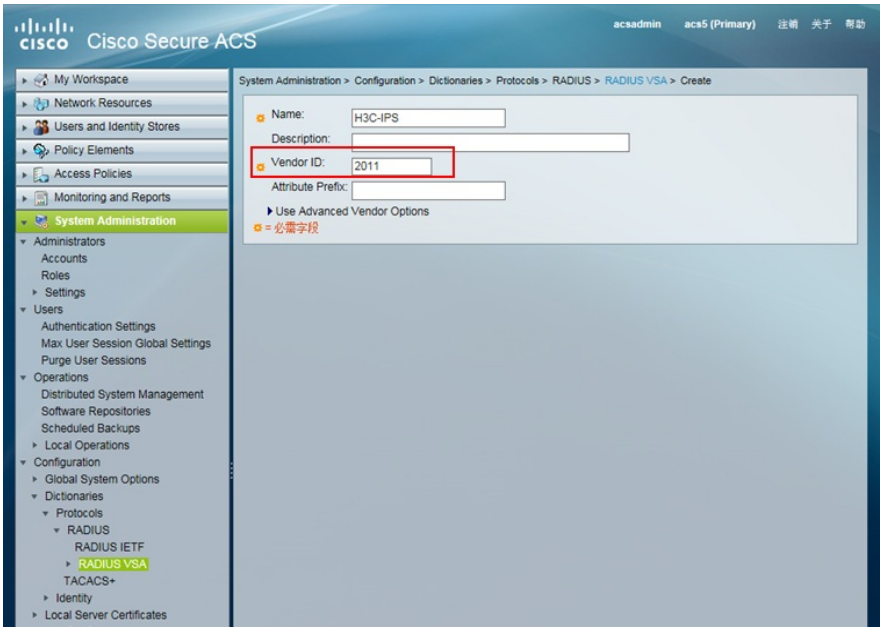


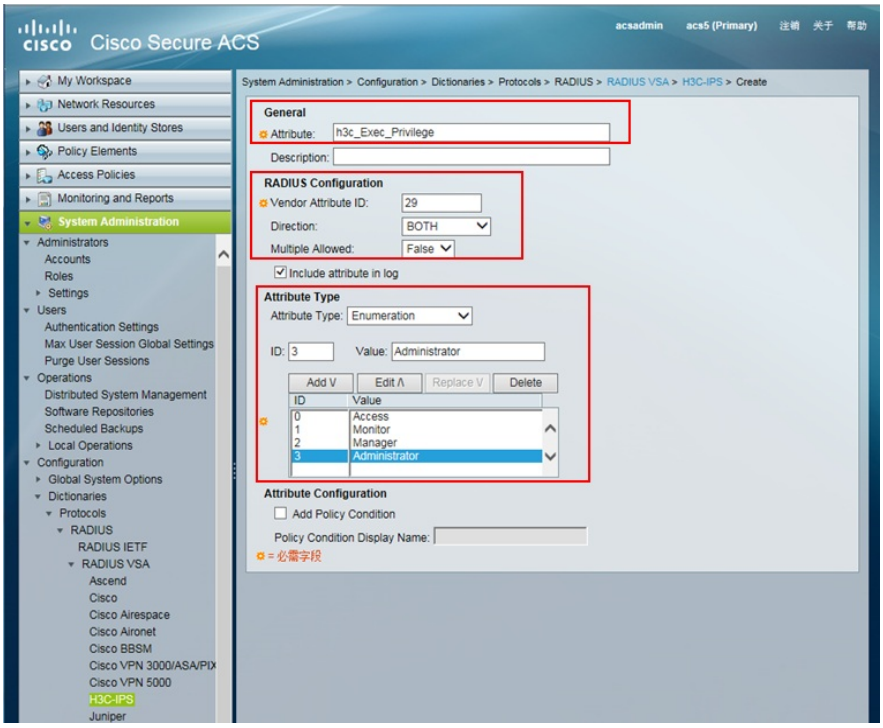
4）添加identity groups：h3c_rw，读写帐号属于该分组



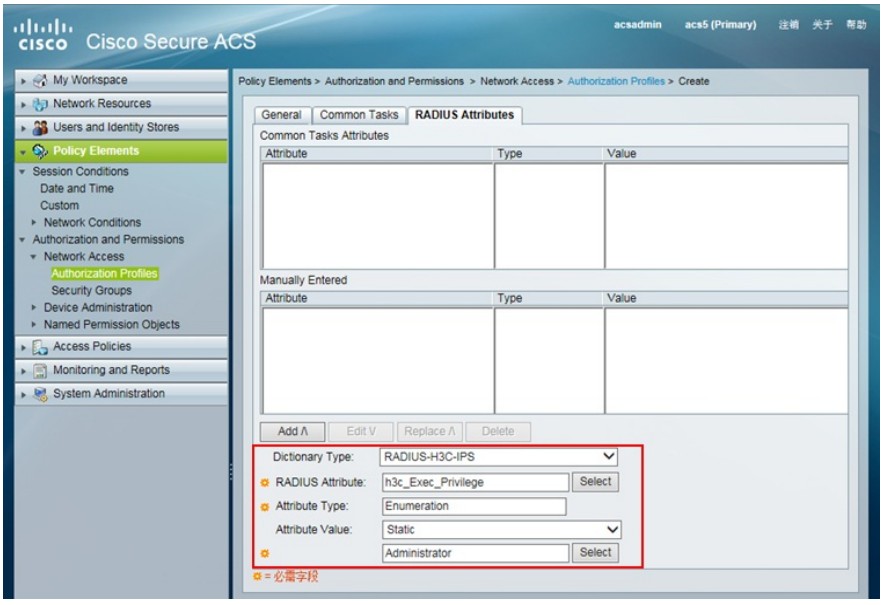
5）添加users：h3cro，只读权限，属于分组h3c_ro。h3crw，只读权限，属于分组h3c_rw。

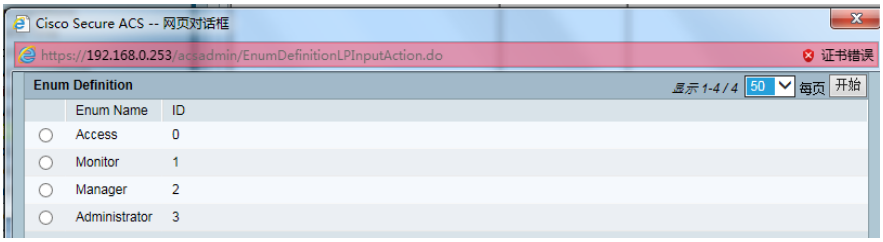
6）导入我司IPS Radius字典

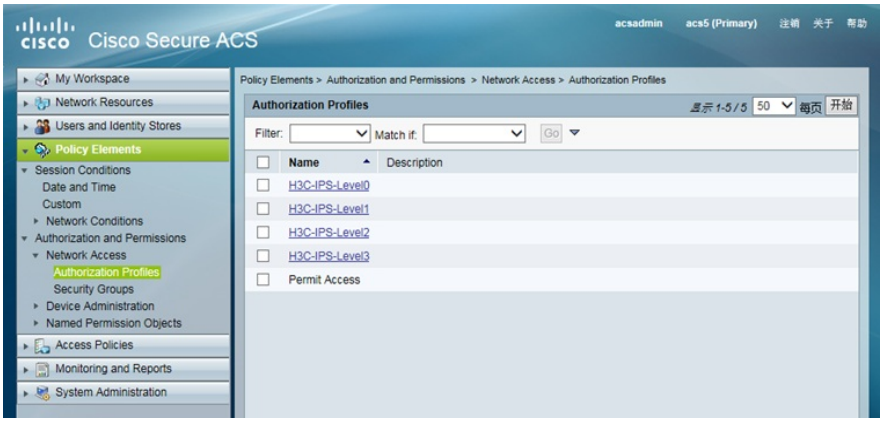




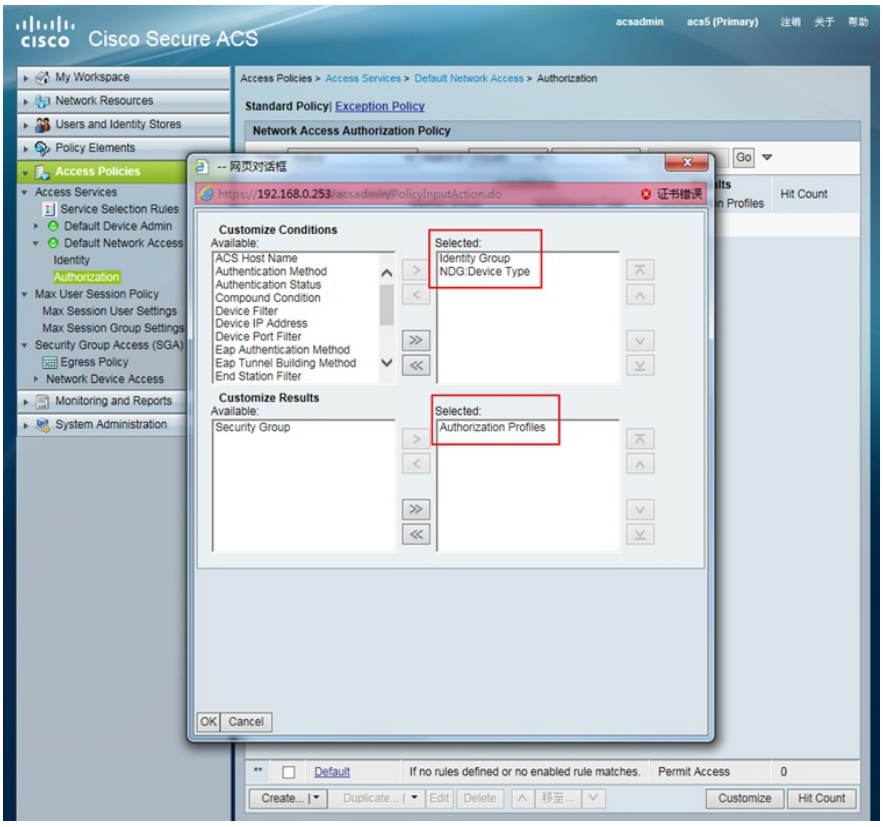
7）创建authorization profiles，分别创建4个授权文件，对应IPS的0-3级权限







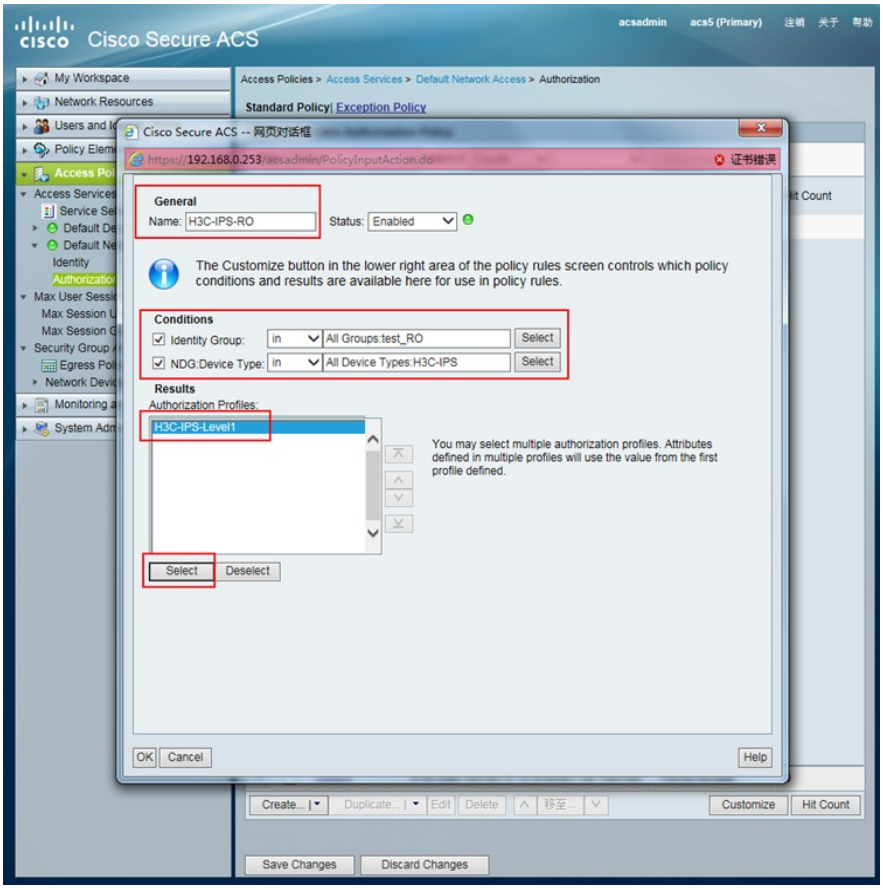
8）创建authentication policy。customize conditions选择：identity group和device type，customize results选择authorization profiles。



9）创建authentication policy

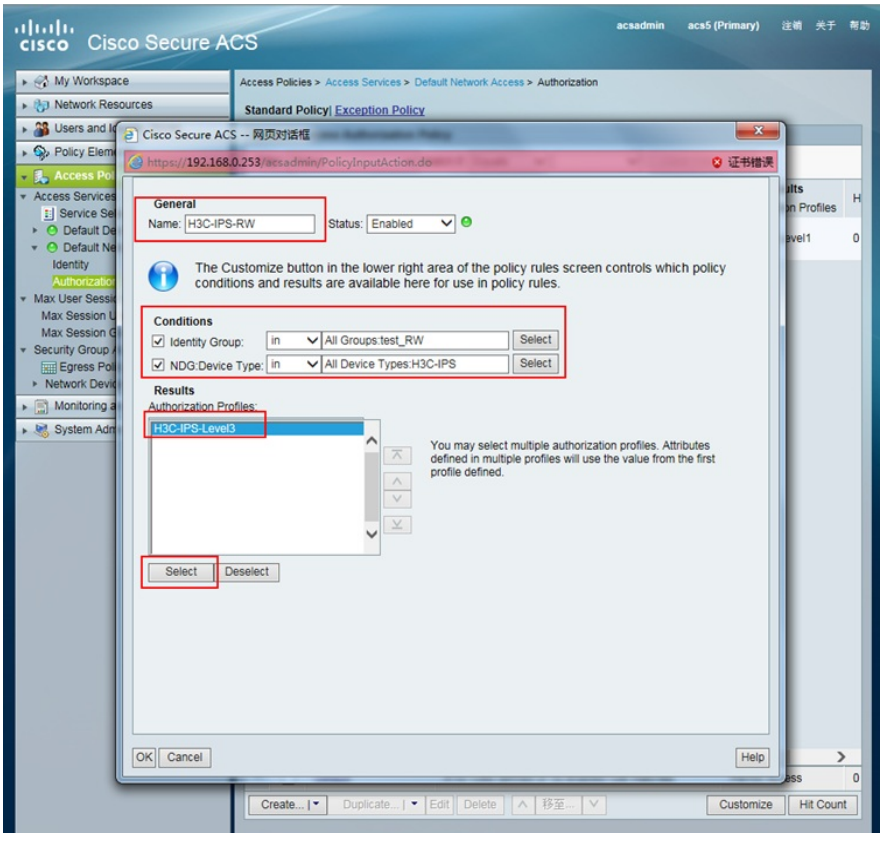
identify group=h3c_ro，device type=H3C-IPS，授予level1权限。

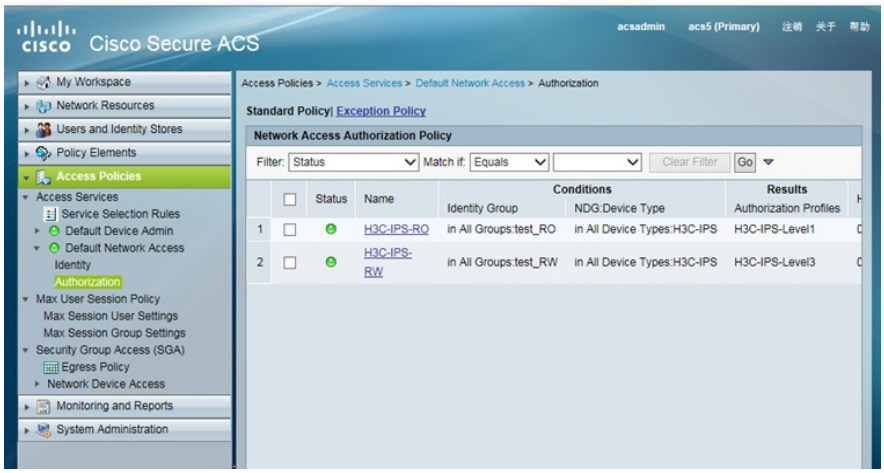
帐号h3cro只有IPS level1权限。



identify group=h3c_rw，device type=H3C-IPS，授权level3权限。

帐号h3crw拥有IPS最高权限。





3.最终结果:

1）帐号h3cro登陆，拥有level1权限

2）帐号h3crw登陆，拥有level3权限

用户名	级别	登录时间	最近访问时间	登录地址	认证方式	语言
h3crw	LEVEL3	2014-12-09 16:38:07	2014-12-09 16:38:18		RADIUS	中文
h3cro	LEVEL1	2014-12-09 16:37:29	2014-12-09 16:38:03		RADIUS	中文

强制退出

一、 IPS Radius私有属性信息

[User Defined Vendor]

Name=H3C

IETF Code=2011

VSA 29=h3c_Exec_Privilege

[h3c_Exec_Privilege]

Type=INTEGER

Profile=IN OUT

Enums=h3c_Exec_Privilege-Values

[h3c_Exec_Privilege-Values]

0=Access

1=Monitor

2=Manager

3=Administrator