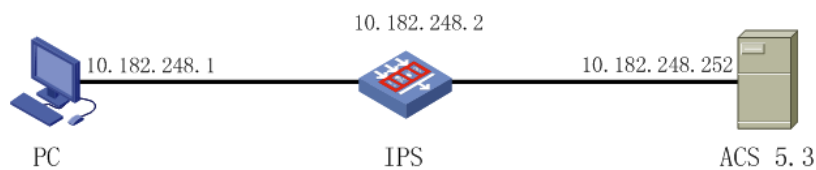


知 IPS结合Cisco ACS做Radius登陆认证配置案例

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：

RADIUS认证配置

全局配置

☒ 使能RADIUS认证

静默时间间隔	5	分钟(0-255)
服务器应答超时时间	3	秒(1-10)
RADIUS报文最大尝试发送次数	20	(1-20)

RADIUS服务器配置

主认证服务器

IPv4地址	10.182.248.252
端口号	1812 (1-65535)
密钥	●●●●●● (1-63 字符)
确认密钥	●●●●●●

2.ACS 5.3配置截图：

1) 添加device group: H3C-IPS

Cisco Secure ACS

Network Resources > Network Device Groups > Device Type > Edit: "Device Type:All Device Types:H3C-IPS"

Device Group - General

Name: H3C-IPS

Description:

Parent: All Device Types [Select]

※ = 必需字段

2) 添加IPS，属于device group: H3C-IPS

The screenshot shows the Cisco Secure ACS interface for configuring a Network Resource named 'IPS'. The left sidebar lists various configuration areas, with 'Network Resources' selected. The main panel shows the configuration for 'IPS' under 'Network Resources > Network Devices and AAA Clients > Edit: "IPS"'. The 'Name' field is 'IPS'. The 'Description' field is empty. Under 'Network Device Groups', the 'Location' is set to 'All Locations' and the 'Device Type' is set to 'All Device Types:H3C-IPS'. Under 'IP Address', the 'Single IP Address' radio button is selected, and the IP is '192.168.0.253'. Under 'Authentication Options', the 'RADIUS' checkbox is checked, and the 'Shared Secret' is 'h3c'. Other options like 'TACACS+', 'CoA port', 'Enable KeyWrap', 'Key Encryption Key', 'Message Authenticator Code Key', and 'Security Group Access (SGA)' are not selected or are empty. A legend at the bottom left indicates that a star icon (*) denotes a required field.

3) 添加identity groups: h3c_ro, 只读帐号属于该分组

The screenshot shows the Cisco Secure ACS interface for creating a new Identity Group named 'h3c_ro'. The left sidebar shows 'Users and Identity Stores' selected, with 'Identity Groups' highlighted. The main panel shows the 'Create' page for 'Identity Groups'. The 'General' tab is active. The 'Name' field is 'h3c_ro'. The 'Description' field is empty. The 'Parent' dropdown is set to 'All Groups'. A legend at the bottom left indicates that a star icon (*) denotes a required field.

4) 添加identity groups: h3c_rw, 读写帐号属于该分组

The screenshot shows the Cisco Secure ACS interface for creating a new Identity Group named 'h3c_rw'. The left sidebar shows 'Users and Identity Stores' selected, with 'Identity Groups' highlighted. The main panel shows the 'Create' page for 'Identity Groups'. The 'General' tab is active. The 'Name' field is 'h3c_rw'. The 'Description' field is empty. The 'Parent' dropdown is set to 'All Groups'. A legend at the bottom left indicates that a star icon (*) denotes a required field.

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。

Cisco Secure ACS

Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: h3cro Status: Enabled

Description:

Identity Group: All Groups:h3c_ro

Password Information

Password must: Contain 4 - 32 characters

Password Type: Internal Users

Password:

Confirm Password:

☐ Change password on next login

Enable Password Information

Password must: Contain 4 - 32 characters

Enable Password:

Confirm Password:

User Information

There are no additional identity attributes defined for user records

= 必需字段

Cisco Secure ACS

Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: h3cnw Status: Enabled

Description:

Identity Group: All Groups:h3c_rw

Password Information

Password must: Contain 4 - 32 characters

Password Type: Internal Users

Password:

Confirm Password:

☐ Change password on next login

Enable Password Information

Password must: Contain 4 - 32 characters

Enable Password:

Confirm Password:

User Information

There are no additional identity attributes defined for user records

= 必需字段

6) 导入我司IPS Radius字典

Cisco Secure ACS

System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA > Create

Name: H3C-IPS

Description:

Vendor ID: 2011

Attribute Prefix:

☐ Use Advanced Vendor Options

= 必需字段

Cisco Secure ACS

System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA > H3C-IPS > Create

General

Attribute: h3c_Exec_Privilege

Description:

RADIUS Configuration

Vendor Attribute ID: 29

Direction: BOTH

Multiple Allowed: False

☒ Include attribute in log

Attribute Type

Attribute Type: Enumeration

ID: 3 Value: Administrator

ID	Value
0	Access
1	Monitor
2	Manager
3	Administrator

Attribute Configuration

☐ Add Policy Condition

Policy Condition Display Name:

☆ = 必需字段

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

Cisco Secure ACS

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

General

Name: H3C-IPS-Level3

Description:

☆ = 必需字段

Cisco Secure ACS

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create

RADIUS Attributes

Attribute	Type	Value
Manually Entered		
Attribute	Type	Value

Add A Edit V Replace A Delete

Dictionary Type: RADIUS-H3C-IPS

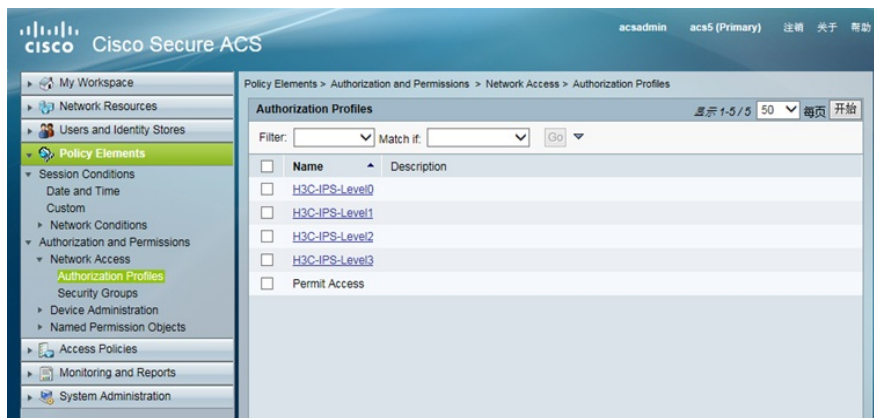
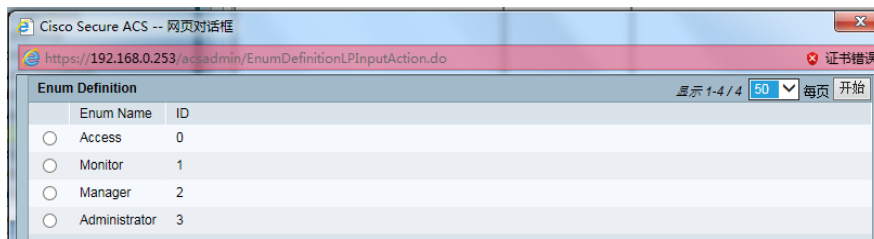
☆ RADIUS Attribute: h3c_Exec_Privilege Select

☆ Attribute Type: Enumeration

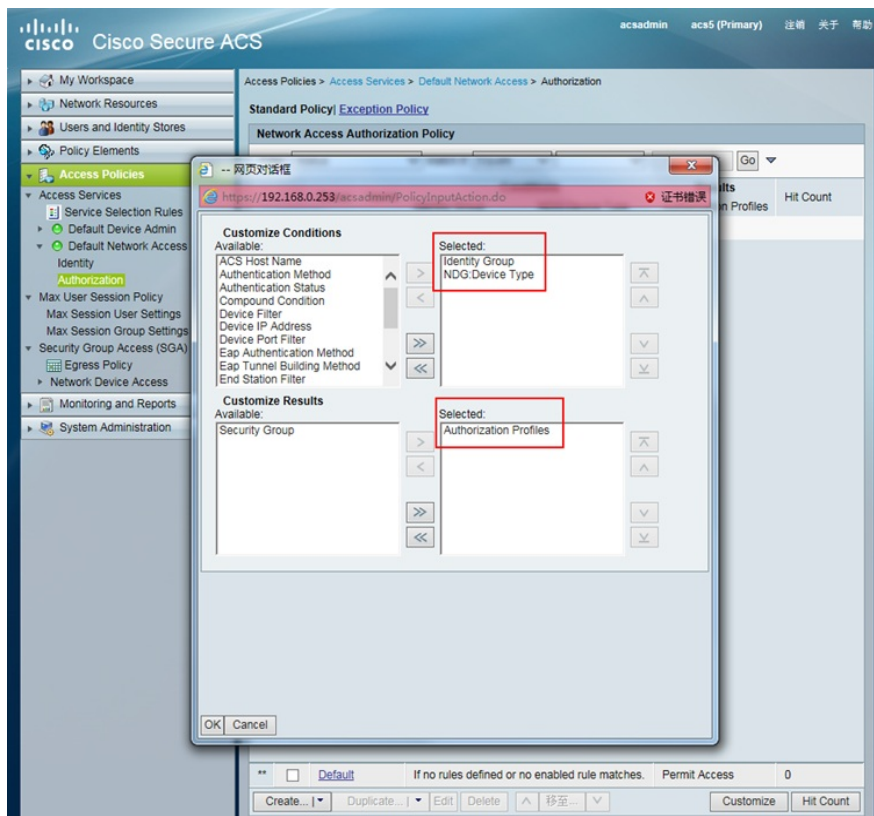
☆ Attribute Value: Static

☆ Administrator Select

☆ = 必需字段



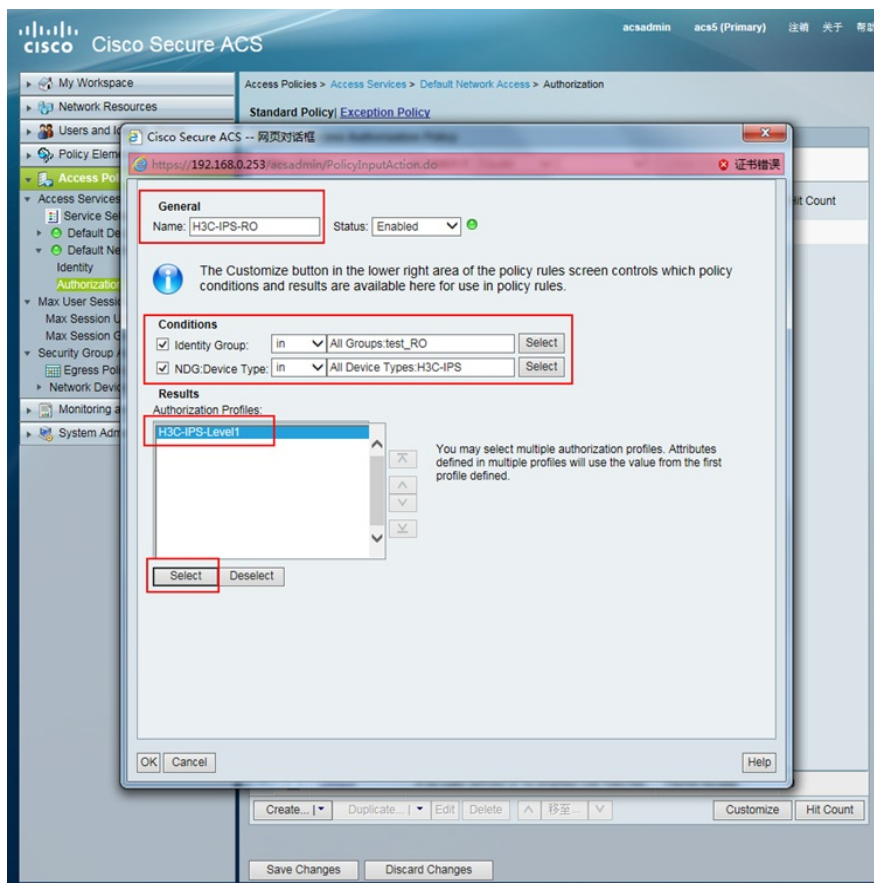
8) 创建authentication policy. customize conditions选择: identity group和device type, customize results选择authorization profiles.



9) 创建authentication policy

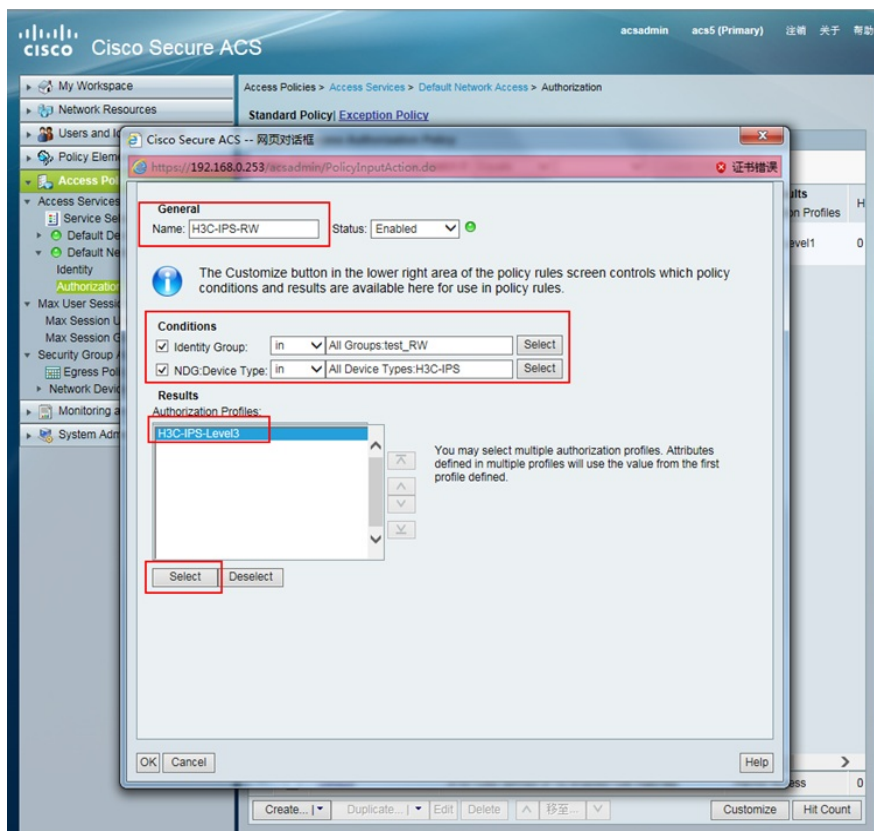
identity group=h3c_ro, device type=H3C-IPS, 授予level1权限。

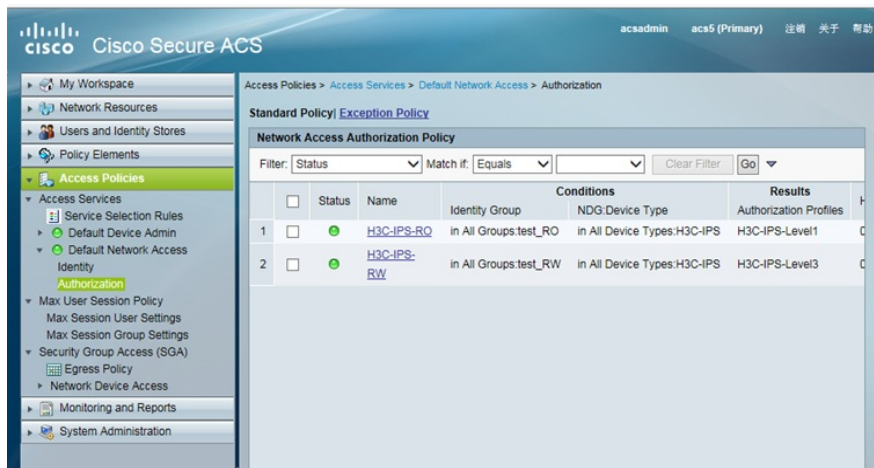
帐号h3cro只有IPS level1权限。



identity 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

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