ComwareV7平台交换机结合CiscoACS5.2进行Radius认证配置及经验总结

Radius 秦军 2013-10-31 发表

ComwareV7平台交换机结合Cisco ACS 5.2进行Radius认证配置及经验总结

一、 组网需求:

PC直连S5820V2，S5820V2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. S5820V2

S5820V2使用软件版本Release 2208P01;

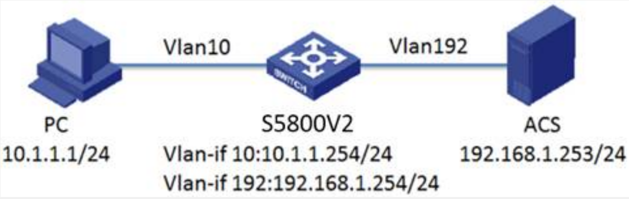
VLAN 10 address：10.1.1.254/24与PC互联接口属VLAN10;

VLAN 192 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。

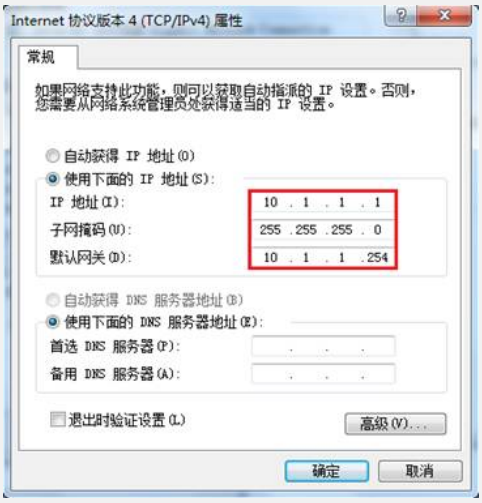
二、 组网图:



三、 配置步骤:

1. PC

配置IP地址:



Internet 协议版本 4 (TCP/IPv4) 属性

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。

○ 自动获得 IP 地址(O)

● 使用下面的 IP 地址(S):

IP 地址(I): 10 . 1 . 1 . 1

子网掩码(U): 255 . 255 . 255 . 0

默认网关(D): 10 . 1 . 1 . 254

○ 自动获得 DNS 服务器地址(B)

● 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P):

备用 DNS 服务器(A):

□ 退出时验证设置(L)

2. S5820V2配置

S5820V2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 Ten-GigabitEthernet1/0/1
 port access vlan 10
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 192
#
user-interface vty 0 15
 authentication-mode scheme
  user-role network-admin
#
radius scheme login
  primary authentication 192.168.1.253
 primary accounting 192.168.1.253
 key authentication cipher 123
 key accounting cipher 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

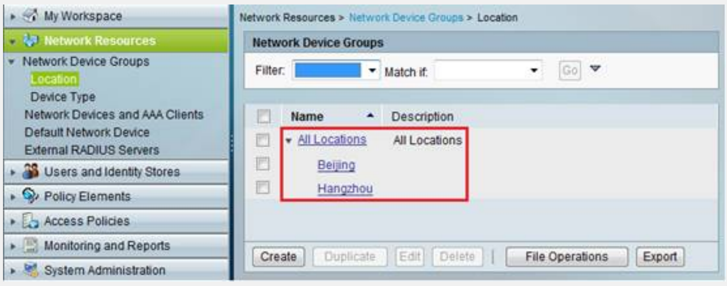
1）通过GUI登录ACS

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

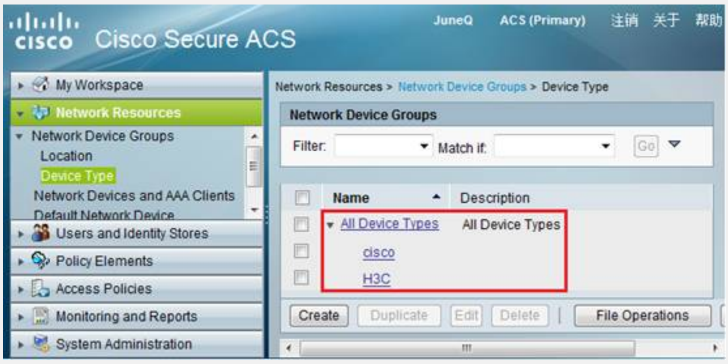
需要预先规划好网络设备组NDG的分配方式，比如按照设备所处位置Location或者设备所属类型Device Type进行规划。

网络资源组>网络设备组NDG下配置位置（Location）：



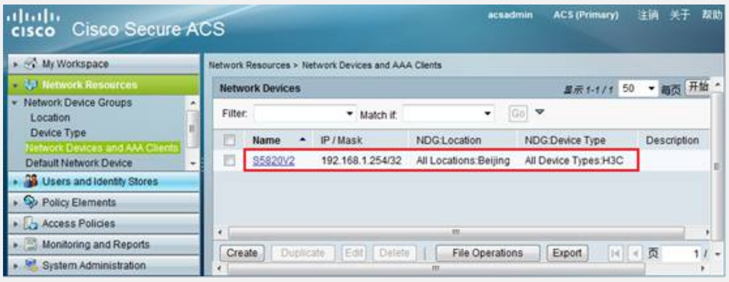
Name	Description
All Locations	All Locations
Beijing	
Hangzhou	

网络资源组>网络设备组NDG下配置设备类型（Device Type）：



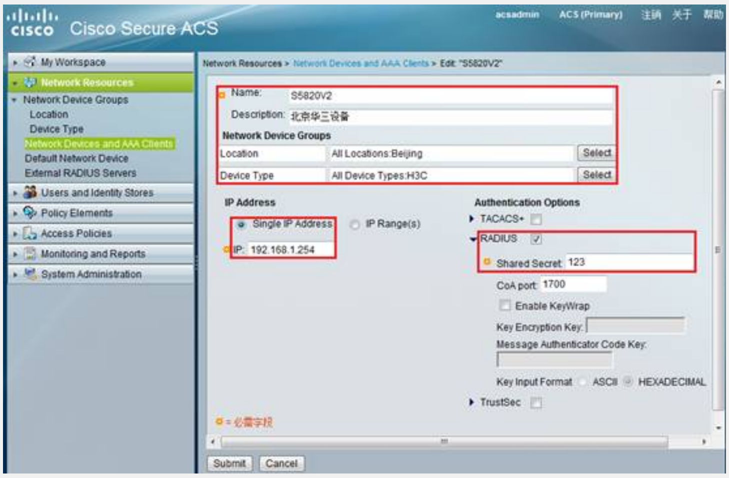
Name	Description
All Device Types	All Device Types
cisco	
H3C	

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）：



Name	IP / Mask	NDG:Location	NDG:Device Type	Description
S5820V2	192.168.1.254/32	All Locations:Beijing	All Device Types:H3C	

将S5820V2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。



Name: S5820V2

Description: 北京华三设备

Network Device Groups

Location: All Locations:Beijing

Device Type: All Device Types:H3C

IP Address

● Single IP Address ○ IP Range(s)

IP: 192.168.1.254

Authentication Options

TACACS+ □

RADIUS ☑

Shared Secret: 123

CoA port: 1700

□ Enable KeyWrap

Key Encryption Key:

Message Authenticator Code Key:

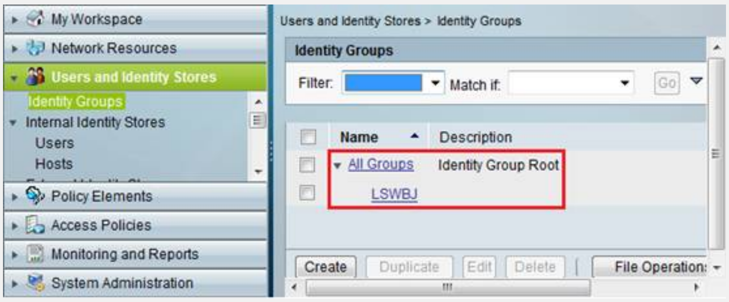
Key Input Format ○ ASCII ● HEXADECIMAL

TrustSec □

= 必需字段

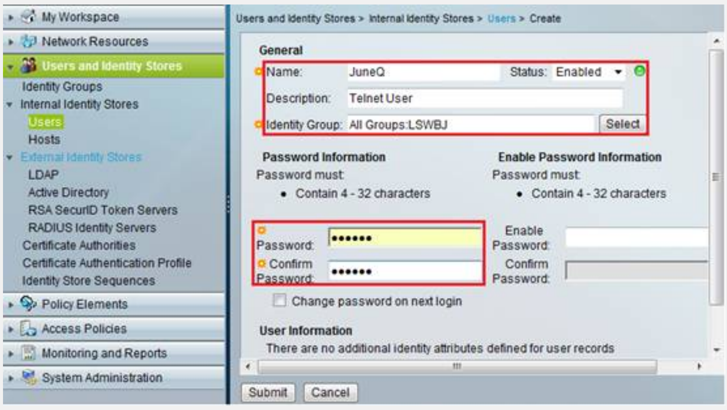
3）配置用户组和用户

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



Name	Description
All Groups	Identity Group Root
LSWBJ	

创建用户（Users），设置用户密码，并将用户分配到特定组：



General

Name: JuneQ Status: Enabled

Description: Telnet User

Identity Group: All Groups:LSWBJ

Password Information
Password must:
- Contain 4 - 32 characters

Enable Password Information
Password must:
- Contain 4 - 32 characters

Password: ••••••

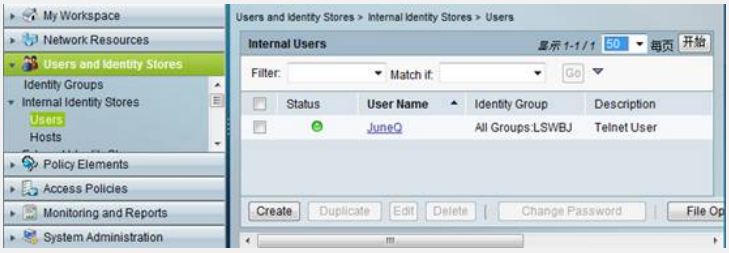
Confirm Password: ••••••

Enable Password:

Confirm Password:

□ Change password on next login

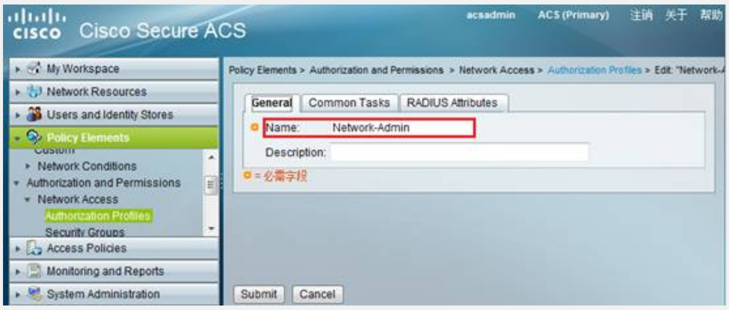
User Information
There are no additional identity attributes defined for user records



Status	User Name	Identity Group	Description
●	JuneQ	All Groups:LSWBJ	Telnet User

4）配置策略元素

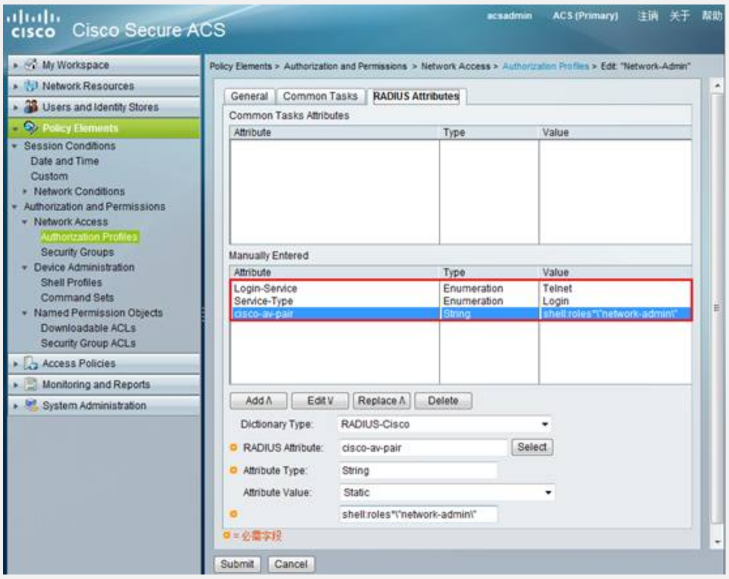
创建授权策略：



Name: Network-Admin

Description:

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-Cisco下的cisco-av-pair，属性填写为shell:roles*\"network-admin\"，或者shell:roles=\"network-admin\"。



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "Network-Admin"

General | Common Tasks | RADIUS Attributes

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
Login-Service	Enumeration	Telnet
Service-Type	Enumeration	Login
cisco-av-pair	String	shell:roles*\"network-admin\"

Dictionary Type: RADIUS-Cisco

RADIUS Attribute: cisco-av-pair

Attribute Type: String

Attribute Value: Static

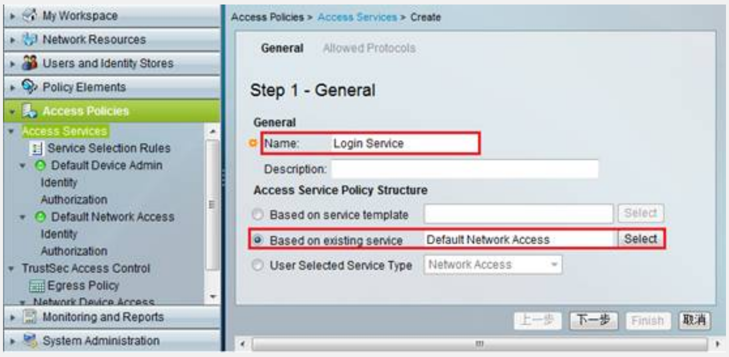
shell:roles*\"network-admin\"

= 必需字段

5）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：



Access Policies > Access Services > Create

Step 1 - General

General

Name: Login Service

Description:

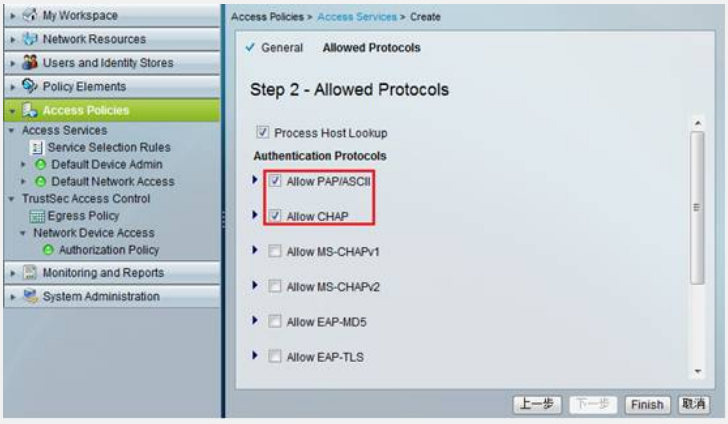
Access Service Policy Structure

○ Based on service template

● Based on existing service: Default Network Access

○ User Selected Service Type: Network Access

勾选认证协议，这里只需勾选PAP、CHAP即可：



Access Policies > Access Services > Create

Step 2 - Allowed Protocols

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII

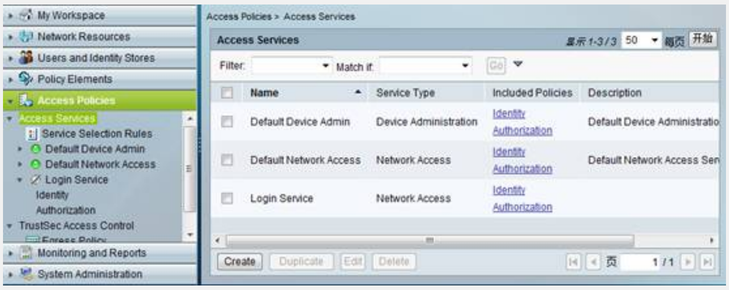
☑ Allow CHAP

☐ Allow MS-CHAPv1

☐ Allow MS-CHAPv2

☐ Allow EAP-MD5

☐ Allow EAP-TLS

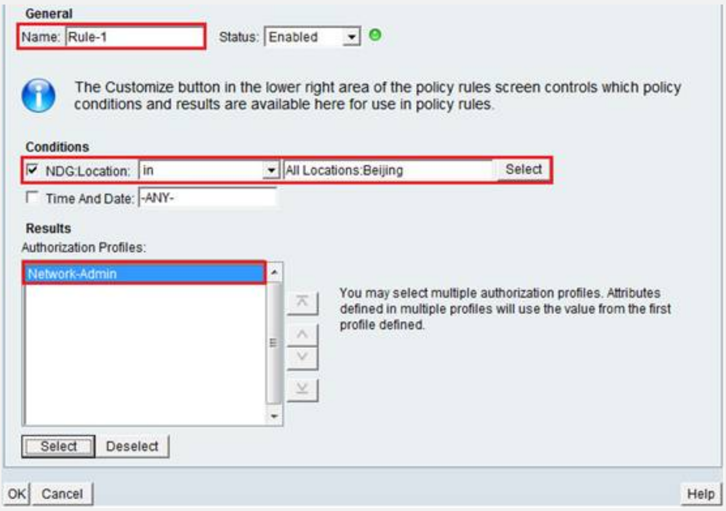


Access Policies > Access Services

Access Services

Name	Service Type	Included Policies	Description
Default Device Admin	Device Administration	Identity Authorization	Default Device Administratio
Default Network Access	Network Access	Identity Authorization	Default Network Access Ser
Login Service	Network Access	Identity Authorization	

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：



General

Name: Rule-1 Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

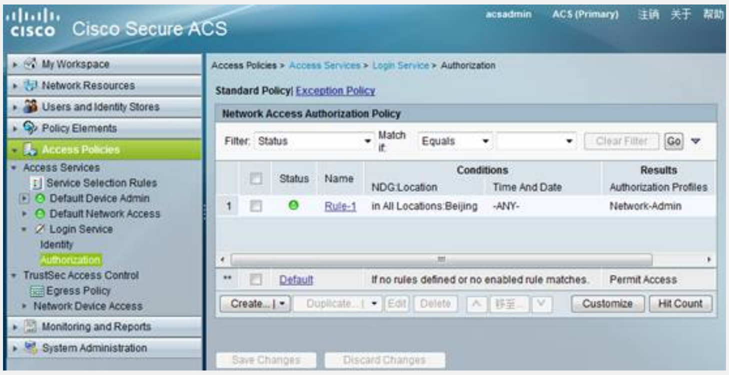
☑ NDG:Location: in All Locations:Beijing

☐ Time And Date: -ANY-

Results

Authorization Profiles: Network-Admin

You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.



Cisco Secure ACS

Access Policies > Access Services > Login Service > Authorization

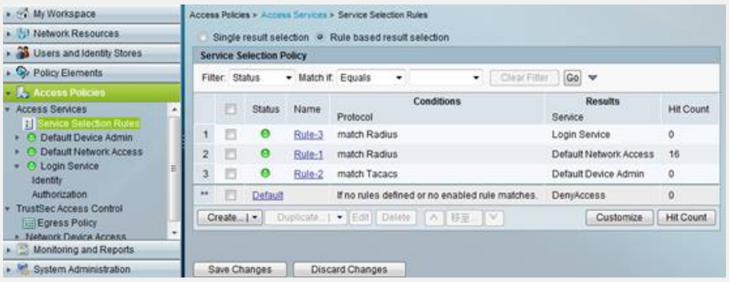
Standard Policy| Exception Policy

Network Access Authorization Policy

Filter: Status Match if: Equals

	☐	Status	Name	Conditions		Results
				NDG:Location	Time And Date	Authorization Profiles
1	☐	●	Rule-1	in All Locations:Beijing	-ANY-	Network-Admin
**	☐		Default	If no rules defined or no enabled rule matches.		Permit Access

配置服务选择规则，选择已创建的接入服务：



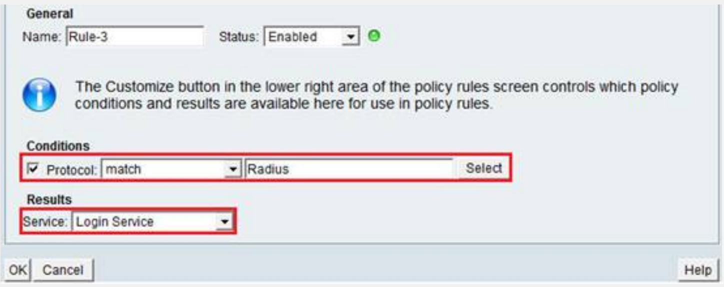
Access Policies > Access Services > Service Selection Rules

○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals

	☐	Status	Name	Conditions	Results	Hit Count
				Protocol	Service	
1	☐	●	Rule-3	match Radius	Login Service	0
2	☐	●	Rule-1	match Radius	Default Network Access	16
3	☐	●	Rule-2	match Tacacs	Default Device Admin	0
**	☐		Default	If no rules defined or no enabled rule matches.	DenyAccess	0



General

Name: Rule-3 Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

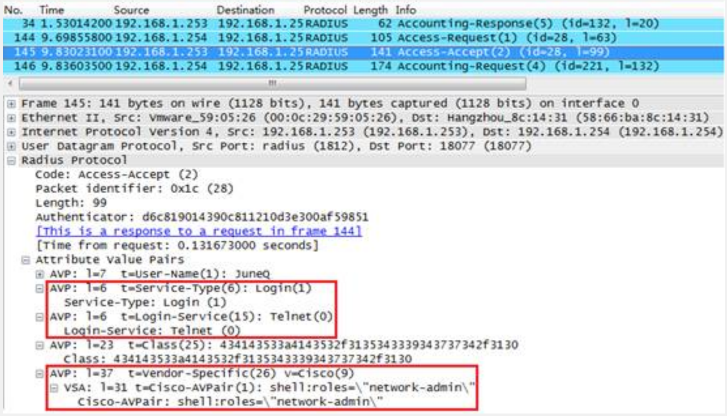
☑ Protocol: match Radius

Results

Service: Login Service

4. 验证

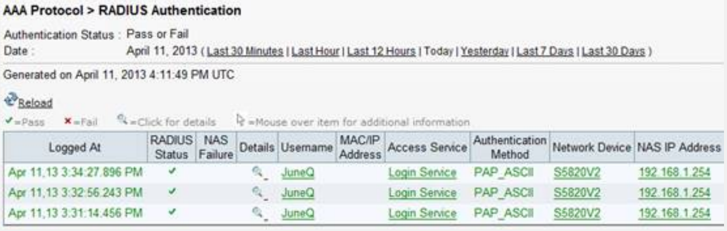
认证时对设备抓包，在获取的Radius Access-Accept报文中可以看到Service-Type、Login-Service、cisco-av-pair等属性。



```
No.  Time        Source         Destination    Protocol Length Info
  34 1.53014200 192.168.1.253  192.168.1.25 RADIUS     62 Accounting-Response(5) (id=132, l=20)
 144 9.69855800 192.168.1.254  192.168.1.25 RADIUS    105 Access-Request(1) (id=28, l=63)
 145 9.83023100 192.168.1.253  192.168.1.25 RADIUS    141 Access-Accept(2) (id=28, l=99)
 146 9.83603500 192.168.1.254  192.168.1.25 RADIUS    174 Accounting-Request(4) (id=221, l=132)

⊞ Frame 145: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface 0
⊞ Ethernet II, Src: Vmware_59:05:26 (00:0c:29:59:05:26), Dst: Hangzhou_8c:14:31 (58:66:ba:8c:14:31)
⊞ Internet Protocol Version 4, Src: 192.168.1.253 (192.168.1.253), Dst: 192.168.1.254 (192.168.1.254)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: 18077 (18077)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x1c (28)
    Length: 99
    Authenticator: d6c819014390c811210d3e300af59851
    [This is a response to a request in frame 144]
    [Time from request: 0.131673000 seconds]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=7  t=User-Name(1): JuneQ
    ⊟ AVP: l=6  t=Service-Type(6): Login(1)
        Service-Type: Login (1)
    ⊟ AVP: l=6  t=Login-Service(15): Telnet(0)
        Login-Service: Telnet (0)
    ⊟ AVP: l=23  t=Class(25): 434143533a4143532f3135343339343737342f3130
        Class: 434143533a4143532f3135343339343737342f3130
    ⊟ AVP: l=37  t=Vendor-Specific(26) v=Cisco(9)
      ⊟ VSA: l=31 t=Cisco-AVPair(1): shell:roles=\"network-admin\"
          Cisco-AVPair: shell:roles=\"network-admin\"
```

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。



AAA Protocol > RADIUS Authentication

Authentication Status : Pass or Fail
Date : April 11, 2013 (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

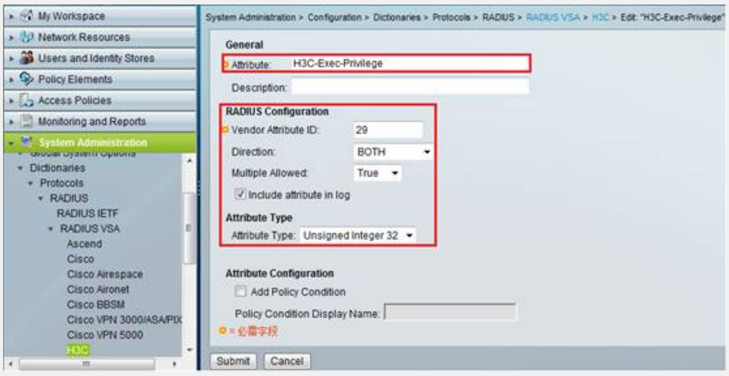
Generated on April 11, 2013 4:11:49 PM UTC

Reload
✓=Pass ✗=Fail =Click for details =Mouse over item for additional information

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address
Apr 11,13 3:34:27.896 PM	✓		🔍	JuneQ		Login Service	PAP_ASCII	S5820V2	192.168.1.254
Apr 11,13 3:32:56.243 PM	✓		🔍	JuneQ		Login Service	PAP_ASCII	S5820V2	192.168.1.254
Apr 11,13 3:31:14.456 PM	✓		🔍	JuneQ		Login Service	PAP_ASCII	S5820V2	192.168.1.254

四、 配置关键点：

1. 配置ACS时必须使用扩展属性cisco-av-pair为用户下发role；
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；
4. 配置cisco-av-pair属性时注意Attribute Value文本框中下发role的格式：shell:roles*\"network-admin\"或shell:roles=\"network-admin\"，注意角色名一定要有双引号，否则设备不识别；
5. 设备支持使用H3C私有属性Exec_Privilege为用户下发登录系统所能访问的命令级别，范围是0-15。通过在RADIUS VSA中添加H3C私有属性，Vendor ID：25506，添加Attribute：H3C-Exec-Privilege，Vendor Attribute ID：29，Attribute Type：Unsigned Integer 32，然后在已创建的授权策略中添加这一属性，并填写授权级别即可实现。



System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA > H3C > Edit: "H3C-Exec-Privilege"

General

Attribute: H3C-Exec-Privilege

Description:

RADIUS Configuration

Vendor Attribute ID: 29

Direction: BOTH

Multiple Allowed: True

☑ Include attribute in log

Attribute Type

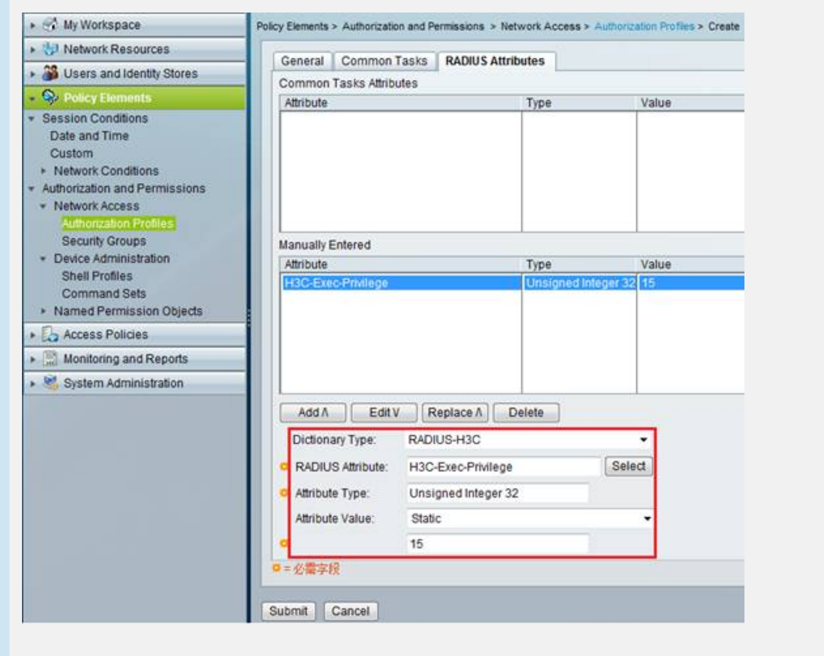
Attribute Type: Unsigned Integer 32

Attribute Configuration

□ Add Policy Condition

Policy Condition Display Name:

= 必需字段



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

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
H3C-Exec-Privilege	Unsigned Integer 32	15

Dictionary Type: RADIUS-H3C

RADIUS Attribute: H3C-Exec-Privilege

Attribute Type: Unsigned Integer 32

Attribute Value: Static

15

= 必需字段