Radius 奏军 2013-10-31 发表

本文主要讲述 认证的配置方法以7	ComwareV5平台与Cisco ACS 5.2认证服务器通过Radius方式进行 及注意事项。
一、组网需求:	
PC直连S5500 1. PC	-EI, S5500-EI直连Cisco ACS 5.2服务器。
PC使用Windo IP address: 1	ws 7操作系统; 0.1.1.1/24。
2. S5500-EI	
S5500-El使用	软件版本Release 2208;
Vlan10 addres	ss: 10.1.1.254/2l;
Vlan192 addre	əss: 192.168.1.254/24与Server互连接口属vlan192。
3. Cisco ACS 5.2	
IP address: 1	92.168.1.253。
二、组网图:	
10.1	PC S5500-EI ACS 1.1.1/24 Vlan-if 10:10.1.1.254/24 192.168.1.253/24 Vlan-if 192:192.168.1.254/24
三、配置步骤:	
1. PC配置	
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 (0)
	●使用下面的 IP 地址(S): IP 地址(C):
	子阿撞码(0): 255、255、255、0
	默认网关 (0): 10 . 1 . 1 .254
	● 自动赋得 DBS 服务器地址 (B) ● 使用下面的 DBS 服务器地址 (B):
	首选 DNS 服务器 (P):
	週出时验证设置 (L) 高级 (V)
	·····································
	,i
2. 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):

 My Workspace 	Network Resources > Network Device Groups > Location
🔹 😓 Network Resources	Network Device Groups
Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Filter. Match it Go 🐨
B Users and Identity Stores	Beijing
Policy Elements	Hangzhou Hangzhou
Access Policies	
Monitoring and Reports	
System Administration	Create Dopicate Con Delete Pile Operations Export

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 Cli ents):

 My Workspace 	etwork Resources > Network Devices and AAA Clients		
 Wetwork Resources 	Network Devices	展示1-1/1 50	• 每页 开始
Network Device Groups Location Device Type	Filter: • Match if: • 60	NDG:Device Type	Description
B Users and Identity Stores	S5500-EI 192.168.1.254/32 All Locations:Beijing	All Device Types:H3C	
Policy Elements			
Access Policies			
Monitoring and Reports	Country Country Country Country		
System Administration	Coreate Jal. Oxpansion Income Dente The Operations	[Export] [14]]	1 34 1

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。

In contract the second second					
Network Desire Groups	o Name: S	5500-EI			
Location	Description: 1	原华三设备			
Device Type	Network Device	Groups			
Network Devices and AAA Clients	Location	All Locations Beijing		Select	
External RADIUS Servers	Device Type	All Device Types H3C		Select	
Users and Identity Stores	1000				
Policy Elements	IP Address		Authentication Optio	05	
Access Policies	 Single IP A 	Iddress 🕐 IP Range(s)	RADIUS		
Monitoring and Reports	OIP. 192.168.1.	254		400	
System Administration			Shared Secret, 123		
			CoAport 1700		
			Enable KeyWrap		
			Key Encryption H	(ey:	
			Message Authenticator Coo		
			Key Input Forma HEXADECIMAL	t 🔿 ASCII 🛞	
			TrustSec		

3) 配置用户组和用户

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

🕨 😚 My Workspace	Users and Identity Stores > Identity Groups Identity Groups						
Interview Resources							
Given and Identity Stores Identity Groups	Filter: Match if:	• Go •					
Internal Identity Stores Users Hosts	Name Description Valia Groups Identity Group Root	E					
Policy Elements	LSWBJ						
Access Policies							
Monitoring and Reports	Create Duplicate Edit Delete	File Operation: -					
System Administration	< III	+ ne operation. •					

创建用户(Users),设置用户密码,并将用户分配到特定组:

 My Workspace 	Users and Identity Stores > Inter	maildentity Stores > Users > Crea	te
Network Resources	General		
Bigging and Identity Stores Identity Groups Internal Identity Stores Users	Description: Telnet I	Status: User ups:LSWBJ	Enabled 👻 \Theta Select
Hosts Eternal identify Stores LDAP Active Directory RSA SecuritD Token Servers RADIUS Identify Servers Certificate Authorities Certificate Authorities Certificate Authorities	Password Information Password must. • Contain 4 - 32 ch. Password. • Confirm Password.	aracters Enable Pa Password r Enable Password: Confirm Password:	ssword Information nust tain 4 - 32 characters
Policy Elements	Change password	d on next login	
Access Policies	User Information		
Monitoring and Reports	There are no additional	I identity attributes defined for u	ser records
 System Administration 	Submit Cancel		

 My Workspace 	Users an	d Identity Stor	es > Internal identity	Store	is > Users		
Network Resources	Internal Users				2元1-1/1 50 ▼ 毎百 开想		
🔹 🎒 Users and Identity Stores	Filter			- 6 -			
Identity Groups		1 mer		· Match II.		- 00	
 Internal Identity Stores 			Status	User Name		Identity Group	Description
Hosts			0	JuneQ		All Groups:LSWBJ	Telnet User
Policy Elements							
Access Policies	_						
Monitoring and Reports	_	Crea	ate Dup	icate Edit C	elete	Change Pa	ssword File O
System Administration		*					,

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: 2 9, 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。

Network Resources	Gen	eral					
Users and Identity Stores	Attribute: H3C-Exec-Privilege						
Policy Elements							
Access Policies	De	scription.					
Manifering and Reports	RAD	UUS Config	uration		_		
, mormoning and Reports	≓ Ve	ndor Attribu	te ID:	29			
System Administration	Dir	rection:		BOTH			
Dictionaries	Ma	utinia Allowa	ad:	True -			
Protocols	in the	unbie cuowe		ilde e			
* RADIUS		Include att	ribute in log				
RADIUS IETF	Attribute Type						
* RADIUS VSA	Attribute Type: Enumeration						
Cisco							
Cisco Airespace	ID:	3	Value: A	dministrator			
Cisco Aironet							
Cisco BBSM _		Add V	Edit	Replac	eV D	elete	
Cisco VPN 3000/ASA/PIX		ID	Value				
Cisco VPN 5000		0	Access			<u> </u>	
HBC		2	Monitor			E	
Huawei		3	Administr	ator			
Juniper			1.1				
Nortel (Bay)	Attr	ibute Config	uration				
RedCreek	F	Add Police	Condition				
US Robotics		, ridd'r ollog	Containent				
TACACS+	P	olicy Conditi	on Display	Name:			
	$\mathbf{O} = A \mathbf{i}$	Contraction of the					

5) 配置策略元素 创建授权策略:

My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit
• 🐉 Network Resources	Frend Demonstrate Didnin Melbridge
🚳 Users and Identity Stores	General Common Tasks RADIOS Attroutes
Policy Elements	O Name: Level-3
Session Conditions	Description:
Authorization and Permissions	■=必需字段
 Network Access 	Colorado Consul

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。

1 Network Resources	General Common Tasks	RADIUS Attributes	
Busers and Identity Stores	Common Tasks Attributes		
Policy Elements	Attribute	Type	Value
Session Conditions Date and Time Custom Network Conditions Network Access Network Access Network Access Security Groups Device Administration Shell Profiles Command Sets	Manually Entered Attribute Login-Service Service-Type	Type Enumeration Enumeration	Vatue Teinet Login
Named Permission Objects Downloadable ACLs Security Group ACLs Ca Access Policies		Enumeration	Administrator
Monitoring and Reports	Add A Edit V	Replace A Delete	
	Dictionary Type: PAD	NUS-H3C	
 System Administration 	LILEUTINI Y LYDY. DYL		
System Administration	RADIUS Attribute: Attribute Type:		Select
System Administration	RADIUS Attribute: Attribute Type: Attribute Value: Stat	lic	Select

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:

 My Workspace 	Access Policies > Access Services > Create	
Horizon State S	General Allowed Protocols	
B Users and Identity Stores		
Policy Elements	Step 1 - General	
Access Policies		
Access Services Service Selection Rules O Default Device Admin Identity Authorization O Default Network Access	General General Secretaria Description: Access Service Policy Structure Based on service template	Select]
Identity	Based on existing service Default Network Access	Select
TrustSec Access Control Egress Policy Network Device Access	User Selected Service Type Network Access	
Monitoring and Reports	上一步下	一步 Finish 取消
System Administration		

勾选认证协议,这里只需勾选PAP、CHAP即可:



My Workspace	-	Access Policies > Access Services						
+ 😓 Network Resources		Acces	is Services	2	〒1-3/3 50 ▼ 綱西 开始			
Busers and Identity Stores		Filter		a	(GA) ¥			
Policy Elements		T HADY.	- Matchin	11 I.	(m) .			
- 🛃 Access Policies			Name •	Service Type	Included Policies	Description		
Access Services I Service Selection Rules			Default Device Admin	Device Administration	Identity Authorization	Default Device Administration		
O Default Device Admin O Default Network Access	.11	0	Default Network Access	Network Access	Identity Authorization	Default Network Access Ser		
 Login Service Identity Authorization 		а.	Login Service	Network Access	Identity Authorization			
TrustSec Access Control Enrace Policy Monitoring and Reports				-				
System Administration	-	Crea	te, Duplicate [Edit]	Delete	Ŀ	●●页 171 ▶●		

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:

The Customize conditions and Conditions	Status: Enabled Status: Enabled Status: Enabled Status: Enabled Status: Enabled Status: Enable button in the lower right area of the policy rules screen controls which policy results are available here for use in policy rules.
VDG:Location: in	✓ All Locations:Beijing Select
Authorization Profiles:	You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.
Select Deselect	
Cancel	Не
Cancel My Workspace Helwork Resources Users and Identity Stores	He Access Policies > Access Services > Logo Service > Authorization Standard Policy/ Exception Policy Intervid Access Authorization Policy
Cancel Image: Strate Strate Strate Users and Identify Stores Policy Elements	He Access Falces > Access Services > Logo Service > Authorization Standard Policy [Exception Policy Network Access Authorization Policy Filter: Status • Match If: Equals • • Clear Filter: Gg ♥
K Cancel My Workspace My Workspace More and Identify Stores Policy Elements Access Holders Selection Rules O Eduta Univer Access O Eduta Univer Access O Eduta Univer Access Subject Benefit	He Access Falces > Access Services > Logis Service > Authorization Standard Policy Escention Policy Filter: Status + Match R: Equals + Conditions Results Status Name Conditions Results Conditions Results Results H& Count Results I Retend I in All Locations Beijing -AVY- Level-3 0
Cancel My Workspace My Workspace My Norkspace My Nork	He Access Palcels > Access Services > Authorization Standard Policy Escention Policy Network Access Authorization Policy Filter: Status Match & Equals Conditions Results Re

配置服务选择规则,选择已创建的接入服务。



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。

AAA Protocol > RADIUS Authentication

Authentication Status : Pass or Fail Date April 11, 2013 (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterdar | Last 7 Dars | Last 30 Dars) Generated on April 11, 2013 4 22:29 PM UTC Pass X = Fail C = Click for details P =Mouse over item for additional information Logged At RADIUS | NAS Status | Failure | Details | Username | MAC/IP | Access Service | Authentication | Network Device | NAS IP Address April 11, 34 4 22:0 916 PM X Q JuneQ Login Service | PAP_ASCII | S5500-E1 | 192:168.1254 April 11, 34 4 22:0 713 PM X Q JuneQ Login Service | PAP_ASCII | S5500-E1 | 192:168.1254 April 13, 42:20.713 PM X Q JuneQ Login Service | PAP_ASCII | S5500-E1 | 192:168.1254 April 13, 42:20.713 PM X Q JuneQ Login Service | PAP_ASCII | S5500-E1 | 192:168.1254 April 13, 42:20.713 PM X Q JuneQ Login Service | PAP_ASCII | S5500-E1 | 192:168.1254 April 13.42:20.713 PM X Q JuneQ Login Service | PAP_ASCII | S5500-E1 | 192:168.1254 April 13.42:20.713 PM X Q JuneQ Login Service | PAP_ASCII | S5500-E1 | 192:168.1254 April 13.42:20.713 PM X Q JUNEQ | Login Service | PAP_ASCII | S5500-E1 | 192:168.1254 April 12.168.1254

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-Ex ec-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extende d类型;
- 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。