

H3C 交换机通过 TACACS+对接 Aruba ClearPass 认证

fox210317@sina.com



1. ClearPass 中添加 Devices

配置路径:

configuration -Network -Devices -Add

说明:

- Name:填写设备名称或自己方便记忆的标识
- IP or Subnet Address:填写 H3C 交换机的 IP, 如有多台可多次添加或添加一个网段
- TACACS+ Shared Secret : 需要在 H3C 交换机和 ClearPass 保持一致的密钥
- Vendor Name:选择 H3C
- Enable RADIUS Dynamic Authorization : 开启
- SAVE

aruba		ClearPass Policy Manager						
Dashboard O	Configuration » Net	uration » Network » Devices						
Monitoring 0	Network Devi	ices						
Configuration 0								
- Service Templates & Wizards								
- C Services	A Network Access De	evice (NAD) must belong to the global lis	t of devices in the ClearPass	: database in o	rder to connect to ClearPass.			
🖻 🗣 Authentication								
- 💭 Methods	Filter: Name	Edit Device Details						
- C Sources	#						_	
🖃 🚨 Identity	1. 0	Device SNMP Read Settings	SNMP Write Settings C	LI Settings	OnConnect Enforcement	Attributes	CATION For H3C SWITCHES	
- 🛱 Single Sign-On (SSO)	2						CATION For H3C SWITCHES	
- 🛱 Local Users	2. 0	Name:	H3C SW-11				CATION For USC CHUTCHES	
- C Endpoints	3, 0	IP or Subpet Address	10.00.00.0124	(0.0	102 169 1 10 or 102 169 1 1	(24 or 102 168 1 1 20)	CATION FOR HSC SWITCHES	
- C Static Host Lists	Showing 1-3 of 3	Provideland	10.00.0024	10.9.	192.100.1.10 0/ 192.100.1.5	(/24 0) 192.100.1.1420)		
- O Roles		Description:	SWITCHES	N FOR HSU				
- IQ Role Mappings					1			
e- o Posture		RADIUS Shared Secret:			Verify:			
- I Posture Policies		TACACS+ Shared Secret:			Manify:			
Characters OnGuard		Inchest shared secree.	lung		voluy.			
S & Enforcement		vendor Name:	Hac				-	
- The Policies		Enable RADIUS Dynamic Authorization	on: 🗹 Port: [3799					
- rofiles		Enable RadSec:						
Network								
- Devices								
Device Groups								
- C Proxy Targets								
- C Event Sources						Conv Save Cancel		
- 🛱 Network Scan								
- C Policy Simulation								

添加完成如下:

ClearPass Policy Manager	Menu 💻
Configuration » Network » Devices	
Network Devices A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect	w Add ▲ Import ▲ Export All ♥ Discovered Devices to ClearPass.
Filter: Name 🗸 contains 🗸 👘 Go Clear Filter	Show 20 v records
# Name 🔺 IP or Subnet Addre	ss Description
1. O H3C SW -11	TACACS AUTHENTICATION For H3C SWITCHES
2. 🗆 H3C SW -12	TACACS AUTHENTICATION For H3C SWITCHES
3. 🗆 H3C SW -13	TACACS AUTHENTICATION For H3C SWITCHES
Showing 1-3 of 3	Copy Export Delete



2. 创建 Authentication Sources

配置路径:

Configuration -Authentication -Sources -Add

说明:

- Name : 填写设备名称或自己方便记忆的标识
- Description : 填写描述/备注信息
- **Type**:选择 Active Directory
- Use for Authorization:勾选 (Enable to use this Authentication Source to also fetch role mapping attributes)
- Authorization Sources:如果有除了当前 AD 以外的其他 Authorization Sources, 可以填写,反之则无
- Server Timeout : 10s
- Cache timeout: 36000s, 建议修改为 180s

aruba	ClearPass Policy Manager	Menu
Dashboard O Co	onfiguration » Authentication » Sources » Add - TACACS AUTH AD	10 - 302 A - 12
Monitoring O A	authentication Sources - TACACS AUTH AD	a constant of the
Configuration	Summary General Primary Attributes	
O Services O Service O Service	Sector Views per InCACSA AUTHAD escription: Incacks Authentication per Active Directory active Directory Enable to use this Authentication Source to also fetch role mapping attributes thirding active Directory Incampre verver Timesout: If seconds active Directory Interverver active Directory Interverver active Directory Interverver active Directory If seconds active Directory If seconds active Directory Interverver	(an), cu1)d (2021-12-13-13-
 Q Devices Q Devices Coropp Q Proxy Targets Q Event Sources Q Feet Sources Q Feet Sources Q Policy Simulation 		tuer. en pl 2021, 12.,14.,12
<pre></pre>	Back to Authentication Sources	Clear Cache Copy Save Cr
Administration 0		
5 Copyright 2020 Hewlett Packard Enterprise Development I	LP Dec 14. 2021 12:23:15 CST	ClearPass Policy Manager 6.8.7.120583 on C2000V



2.1. AD 域控服务器信息

说明:

- 在填写完 Bind DN 与 Bind Password 后,可以点右侧 Search Base Dn,如果可以检索 出 OU,则填写的信息可以使用。
- 其他参数保持默认即可
- SAVE

aruba		ClearPass	Policy Manager
Dashboard	• Configuration » Authentica	tion » Sources » Add - TACACS AUTH AD	
Monitoring	 Authentication So 	urces - TACACS AUTH AD	
2 Configuration	Summary General	Primary Attributes	
Comparison of the second	Summary General Hostname: Connection Security: Port: Verify Server Certificate: Bind DN: Bind Password: NetBIOS Domain Name: Base DN: Search Scope: LDAP Referrals: Bind User: User Certificate:	M None V 389 (For secure connection, use 636) Enable to verify Server Certificate for secure conn (e.g. administrator@example.com OR cn=administrator@example.com OR	Connection Details
- Ö Devices	Always use NetBIOS name	Enable to always use NetBIOS name instead of th	ne domain part in username for authentication
Device Groups Device Groups Device Groups Device Fragets Device Scan Device Scan Device Scan	1005-011-04-20		



2.2. Authentication Sources - AD Attributes

说明:此处勾选 memberOf,用于后续通过 AD 中这个属性作为 Role Mapping 使用

SAVE

aruba		ClearPass Po	licy Manager		Menu 🚍
Dashboard O	Configuration » Authentication » Sources » Add				
Monitoring 0	Authentication Sources				
🖧 Configuration 📀	General Primary Attributes Summary	Y			
Configuration Configu	Concert Primary Attorbuts Seminar Concert filter quarks used to forth automotion Filter Name	and automotation attributes attribute Name On department tole concease	Alias Nama Usech Department Itte consarv menberof Please configure base do first ware Pater		ExaMici 46
- ∰ Audit Servers - ∰ Agentiess OnGuard - ■ ■ Enforcement	3. Machine	Filter Query:	countName=+(Authentication:Username})(obje	ctClass=user))	D *
- da Profiles	4. Onboard Device Owner	Name	Alias Name Data type	Enabled As	. De 😰
Hericark Opivica Groups Opivica Groups Opivica Groups Opivica Groups Opivica Groups Opivica Startas Opivica Startas	5. Orboard Device Owner Group	1. dn 4. donytment 3. t2de 4. donytment 5. t2de memberof memberof mei desphoreNumber accountSopres 10. Clob to add	JserfM String Department String fde String member0f in String Phone String mail String Jame String Jame String Jame String	- 57 - 77 - 77 - 77 - 77 - 77 - 77 - 77	
🚰 Administration 🛛 🔍 🛛	C Back to Authentication Sources			Save Close	Next→ Save Cancel

aruba		ClearPass Policy Manag	jer		Menu 🔤
Dashboard	• Configuration » Authentication » Sources » Add - TAC	ACS AUTH AD			1.1.1
Monitoring	 Authentication Sources - TACACS A 	UTH AD			
Configuration	O Summary General Primary Attributes				
- 🛱 Service Templates & Wizards	Specify filter queries used to fetch authentication and	authorization attributes	2010-2010-00	100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100	
- Authentication	Filter Name	Attribute Name	Alias Name	Enabled As	Concession of the local division of the loca
- 🛱 Methods	1.	dn	UserDN		
- O Sources		department	Department		
🖃 🧕 Identity		title	Title		
- C Single Sign-On (SSO)		company	company		- 1 Lan -
- Local Users	Authentication	memberOf	memberOf	Attribute	13 ×
The Static Host Lists		telephoneNumber	Phone	· · · · · · · · · · · · · · · · · · ·	
- D Roles		mail	Email	* 1000 ····	
Role Mappings		displayName	Name		
+ 🖶 Posture		accountExpires	Account Expires		
Enforcement	2. Group	cn	Groups	-	
- 🛱 Policies	3.	dNSHostName	HostName	*	
Profiles	Machine	operatingSystem	OperatingSystem		E ===
- Network		operatingSystemServicePack	OSServicePack		
- I'l Device Groups	4. Onboard Device Owner	memberOf	Onboard memberOf		B
Proxy Targets	5. Onboard Device Owner Group	cn	Onboard Groups		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
- Q Event Sources - Q Network Scan - Q Policy Simulation	Back to Authentication Sources			Clear Cache Copy	Add More Filters
Administration	•			10075	(
A Convrint 2020 Hewlett Parkard Enternrice Devel	Innmant I D	Dec 14 2021 12:28:01 CST		ClearDace Dollov Mananer 6 & 7 12058	3 on C2000V



3. 创建 ClearPass Role

配置路径:

Configuration -Identity -Roles -Add

说明:

ClearPass Role <mark>用于标识一类用户</mark>(通过一些特定的属性、条件等区分)

aruba	ClearPass Policy Manager				licy Manager	
Dashboard O	Configura	tion »	Identity » Roles			
Monitoring O	Roles					
Configuration O						
- Service Templates & Wizards	Roles exi	st inde	pendently of an indivi	dual service and can b	e accessed globally thro	ugh the role-mapping policy of any service.
- C Services						· · · · · · · · · · · · · · · · · · ·
- Motheds	Filter: Na	me	v (contains 🗸	+ Go	Clear Filter
Sources	#		Name 🔺			Description
	1.		[AirGroup v1]			Role for an AirGroup protocol version 1 reque
Single Sign-On (SSO)	2.		[AirGroup v2]			Role for an AirGroup protocol version 2 reque
- O Local Users	3.		[Aruba TACACS rea	d-only Admin]		Default role for read-only access to Aruba de
- 🛱 Endpoints	4.		[Aruba TACACS roo	Admin1		Default role for root access to Aruba device
- 🛱 Static Host Lists	5		[BYOD Operator]	Edit Role		٥,
- 🎝 Roles	6		[Contractor]			
Role Mappings	0.		[Contractor]	Role ID:	3008	
⊕ Posture ■	7.		[Device gistration	Name:	SW ADMIN	
Enforcement	8.		[F	Description:	MGNT SW Access	
- Or Policies	9.	U		Description		
- I Promes	10.					
T Devices	11.		e C-		L	
- Device Groups	12.					
- C Proxy Targets	13.		и е			Save Cancel
Event Sources	14.					
- 🛱 Network Scan	15.		air			Default role applied during MAC caching
- 🛱 Policy Simulation	16.		1			GT-EMT
	17.					Role for an Android device being provisioned
	18.		[Coard Chromeb	ook]		Role for Chromebook device being provisione
	19.		[Onboard iOS]			Role for an iOS device being provisioned
	20.		[Onboard Linux]			Role for Linux device being provisioned
	21.	0	[Onboard macOS]			Role for a macOS device being provisioned
	22.		[Onboard Windows]			Role for a Windows device being provisioned



4. Role Mapping 配置

配置路径:

Configuration - Identity - Role Mappings - Add

Mapping Rules 配置参数:

Rules Evaluation Algorithm: select first match 评估算法,从头开始

Role Mapping Rules:

Type: "Authorization: TACACS AUTH AD"

Name: "memberOf" 此项参数用于匹配 AD 中特定的部门属性, 仅对一类人评估为" SW ADMIN"

Operator: CONTAINS; 此项参数用于计算公式包含此项属性值,

TIPs: AD 中通过 OU 查询出一个用户的属性, 会包含很多属性, 因此在此处需要写为 CONTAINS

Value: <u>CN=M-IAM-MGMT,OU=ITManager,OU=MosGroup,DC=MOS,DC=COM</u>此项 参数需在 AD 中查找,如下图二

• SAVE

ClearPass Policy Manager				
Dashboard	 Configuration » Identity » Role Mappings » Edit - TACACS ADMIN Role Mapping 			
Monitoring	Role Mappings - TACACS ADMIN Role Mapping			
Configuration	O Summary Policy Mapping Rules			
Service Template & Wizards Service Servic	Ownersy Pericy Pericy Hame: TACACS ADM3H Role Happing Description: TACACS ADM3H Role Happing Description: Cother] Mapping Rules: Cother] Conditions TacACS ADM3H Role Mapping CHEM-BAH + MGM1, OU=TManager, OU=MosGroup, DC=MOS, DC=COM)	Role Hame SW ADMIN		



• 🔿 📶 🤞 📋 🗙 🛄 🍳	🚘 🛛 🖬 🕷 🛍 🐨 💆 🍇	1.010
> 🖬 🔰 🖬	ITManager 屬性	? × 描述
	常规 管理者 对象 安全 COM+ 属性编辑器	
	厪性(B):	
	層性 値 adminDescription <未设置> adminDisplayNa <未设置> businessCategory <未设置> c <未设置> cn <未设置> countryCode <未设置> defaultGroup <未设置> defaultGroup <未设置> defaultGroup <未设置> description <未设置> desktopProfile <未设置> desktopProfile <未设置>	
<pre>> inter > inter inte</pre>	displayName <未设置> displayNamePrint <未设置> distinguishedName OU=ITManager.Ç dSASignature <未设置> < < 童舊(E)	▶ ● ● ● ● ●
	确定 取消 应用(A)	報助



5. Profile 配置

配置路径:

Configuration - Enforcement - Profiles - Add

参数配置:

- **Template**: TACACS+ Based Enforcement
- Name: 填写设备名称或自己方便记忆的标识
- **Description**: 描述/备注
- Action : Accept
- Selected Services: SHELL
- Authorize Attribute Status: ADD
- Service Attributes: (此两条 rule 用于返回给 H3C 交换机,因此 network-admin 仅被 H3C 交换机识别)

Type:SHELL、Name:roles、Value:network-admin (value 小写)

Type : SHELL、Name : priv-lvl、Value : 15

Commands :

Service Type : Shell

Unmatched Commands: 勾选 Enable to permit unmatched commands

• SAVE

aruba		Cle	earPass Policy Mana	iger			Menu 🗮
Dashboard	• Configuration » Enforc	ement » Profiles » Edit Enforcement Profile	a - MGMT-H3C-SW TACACS				51 - SUB-
Monitoring	Enforcement Pr	rofiles - MGMT-H3C-SW TAC/	ACS				ront-ronce
Configuration	Summary Profile	Services Commands					
一賞 Service Templates & Wizards 一賞 Services	Profile:						
Authentication	Name:	MGMT-H3C-SW TACACS					
- 🖧 Methods	Description:	MGMT-H3C-SW TACACS Profiles					
- 🛱 Sources	Type:	TACACS					
Q Identity	Action:	Accept					
- 🛱 single sign on (SSO)	Device Group List:	1. MGMT SW					A 14 M2
- Cell Osers	Services:						and all the second second
C Static Host Lists	Privilege Level:	15					A CONTRACTOR OF
- 12 Role Mannings	Selected Services:	1. Shell					
Posture	Authorize Attribute Sta	atus: ADD					
🖃 💈 Enforcement	Custom Services:	-					
Policies Opplies				Service Attributes			
Network	Туре		Name		=	Value	
- Devices	1. Shell		roels		=	network-admin	
- 🛱 Device Groups	2. Shell		priv-lvl		-	15	2 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
🛱 Proxy Targets	Commands:						10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
- C Event Sources	Service Type:	shell					
- Q Network Scan	Unmatched Command	s: Permit					
				Commands			
	Command	Ar	guments	Permit Action	-		nmatched Arguments



6. Policies 配置

配置路径:

Configuration - Enforcement - Policies - Add

参数配置:

Enforcement:

Name:

Description:

Enforcement Type: 勾选 TACACS+

Default Profile: [TACACS Deny Profile]

Rules:

Rules Evaluation Algorithm: Select first match

Enforcement Policy Rules:

- 1. Type : Authentication. Name : Username. Operator : EXISTS
- 2、 Type: Tips、Name: Role、Operator: EQUALS、Value: SW ADMIN
- 3、 Enforcement Profiles : MGMT-H3C SW TACACS
- SAVE

aruba		ClearPass Policy Manager			
Dashboard O	Configuration * Enforcement * Policies * Edit - TACACS MGMT ACC-For H3C SWs				
Monitoring O	Enforcement Po	licies - TACACS MGMT ACC-For H3C SWs			
Sconfiguration	Summary Enforce	ment Rules			
🎝 Service Templates & Wizards 🖧 Services	Enforcement:				
- Authentication	Name:	TACACS MGMT ACC-For H3C SWs			
- 🛱 Methods	Description:				
- 🛱 Sources	Enforcement Type:	TACACS			
🖃 🧕 Identity	Default Profile:	[TACACS Deny Profile]			
🏩 Single Sign-On (SSO) 🎲 Local Users	Rules:				
- 🛱 Endpoints	Rules Evaluation Algori	thm: First applicable			
🛱 Static Host Lists	Conditions		Actions		
- Q Roles	(Authentication:U	sername EXISTS)	MONT HOC SW TACACE		
- 🛱 Role Mappings	AND (Tips:Role	EQUALS SW ADMIN)	HGHT-HSC-SW MCACS		
* Enforcement			1		
Policies					
- Profiles					
- + Network					
- 🛱 Devices					
- 🛱 Device Groups		. en 18			
- 🛱 Proxy Targets					
- 🛱 Event Sources					
- 🛱 Network Scan					
—☆ Policy Simulation					

7. Services 配置

配置路径:

Configuration -Services -Add

参数模板关联配置:

• Service :

Type: TACACS+ Enforcement

Name:

Description:

Service Rule:

- 1、 Type: Connection、Name: NAD-IP-Address、Operator: BEGINS_WITH、Value: 10.80.80
- 2、 Type: Connection、Name: NAD-IP-Address、Operator: BEGINS_WITH、Value: 10.82.0
- 3、 Type: Connection、Name: NAD-IP-Address、Operator: BEGINS_WITH、Value: 10.81.32
- 4、 Type: Connection、Name: Protocol、Operator: EQUALS、Value: TACACS

Authentication:

Authentication Sources:选择以添加的认证源 AD "TACACS AUTH AD"

Roles :

Role Mapping Policy : "TACACS ADMIN Role Mapping"

Enforcement:

Enforcement Policy: "TACACS MGMT ACC-For H3C SWs"

SAVE



aruba		ClearPass Policy	/ Manager	Menu			
Dashboard	 Configuration » Servi 	ces » Edit - TACACS H3C SWs ACC SERVICE					
Monitoring	 Services - TAC 	ACS H3C SWs ACC SERVICE					
Configuration	O Summary Service	e Authentication Roles Enforcement					
- 🛱 Service Templates & Wizards	Service:						
- D Services	Name	TACACE HIS SWE ACC SERVICE					
Authentication	Description:	TACACS HISC SWI ACC SERVICE					
Single Sign-On (SSO)	Tupe:	TACACC+ Enforcement					
- 🛱 Local Users	Casture:	Type: IACACS+ Enforcement					
- 🆧 Endpoints	Monitor Mode:	Disabled					
- 🛱 Static Host Lists	Mere Ontions:	Claubio Claubio					
- Q Roles	Hore options.						
Posture			Service Rule				
3 Binforcement	Match ANY of the follo	wing conditions:					
- 🛱 Policies	Туре	Name	Operator	Value			
- 🛱 Profiles	1. Connection	NAD-IP-Address	BEGINS_WITH				
- +- Network	2. Connection	NAD-IP-Address	BEGINS_WITH	· · ·			
- i Devices	3. Connection	NAD-IP-Address	BEGINS_WITH				
- Device Groups	4. Connection	Protocol	EQUALS	TACACS			
- Contraction Contraction	Authentication:						
🛱 Network Scan	Authentication Source	es: TACACS AUTH AD					
2 Policy Simulation	Strip Username Rules						
	Roles:						
	Role Mapping Policy:	TACACS ADMIN Role Mapping					
	Enforcement:						
	Use Cached Results:	Disabled					
	Enforcement Policy:	TACACS MGMT ACC-For H3C SWs					



8. 测试验证-1

测试方法:使用在对应 memberOf 属性值的组成员账号登陆 H3C 交换机

测试结果:在 ClearPass Tracker 中查看日志信息

测试结果说明:

Summary - Status : AUTHEN_STATUS_PASS 成功通过认证





8.1. **日志 Policies -Role**: [User Authenticated], SW ADMIN ////该 role 已通过 Role Mapping 获 得正确映射关系

aruba		ClearPass P	olicy Manager			Menu
Dashboard	O Monitoring + Live Moni	oring » Access Tracker				
Monitoring	Access Tracker	Dec 14, 2021 12:12:36 CST				🔮 Auto Refresh
Live Monitoring	The Access Tracker pa	e provides a real-time display of per-session access activit	ly on the selected server or domain.			
Access Tracker						
Accounting	T [All Requests]	RC-CPP))		Last 1 week before To	iday	Edit
System Monitor		TACACS+ Session Details		•		at (1000 -)
Profiler and Network Scan	Filter: Request ID					Show 1000 V records
Endpoint Profiler	e Carver	Summary Request Policies Authorizations			Login Status	Request Timestamp *
Network Scan Results Discovered Devices	1	Polici	es Used -	VICE	ACCEPT	2021/12/14 12:12:31
Audit Viewer	2.	Service Name: TACACS H3C SWs ACC SER	VICE		ACCEPT	2021/12/14 12:12:11
Bevent Viewer	3.	Authentication Source: TACACS AUTH AD		VICE	ACCEPT	2021/12/14 12:08:37
Data Filters	4.	Role: [User Authenticated], SW A	DMIN	VICE	ACCEPT	2021/12/14 12:07:46
Blacklisted Users	5.	Profiles: MGMT-H3C-SW TACACS		VICE	ACCEPT	2021/12/14 12:07:31
	0.			VICE	REJECT	2021/12/14 12:07:23
	1.				ACCEPT	2021/12/14 12:07:13
	8.				ACCEPT	2021/12/14 12:06:34
	9.				ACCEPT	2021/12/14 12:03:28
	10.				ACCEPT	2021/12/14 12:03:03
	11.				REJECT	2021/12/14 12:01:38
	12.				REJECT	2021/12/14 12:01:33
	13.				REJECT	2021/12/14 12:01:30
	14.				REJECT	2021/12/14 12:01:24
	15.				REJECT	2021/12/14 12:01:21
	16.	A Showing 1 or 1-1000 records P H	Export	Now Logs Close VIGE	ACCEPT	2021/12/14 12:00:50
		KADIUS		e -access	REJECT	2021/12/14 12:00:48
	18.	RADIUS			ACCEPT	2021/12/14 12:00:20
	20.	TACACS	and the second s	E	ACCEPT	2021/12/14 11:59:54
	21.	TACACS			ACCEPT	2021/12/14 11:59:24
R. m. Ramatan	22.	TACACS		the second s	ACCEPT	2021/12/14 11:53:34
2 Configuration	23.	RADIUS			ACCEPT	2021/12/14 11:53:23
Administration	0 24.) TACACS		CE	ACCEPT	2021/12/14 11:53:20
Copyright 2020 Hewlett Packard Enterprise Develop	pment LP	Dec 14, 2021 12:12:4	8 CST		Cle	arPass Policy Manager 6.8.7.120583 on C2000V
🏽 P 単 📴 🧿 🛹 💽 !	. 1 . 🦪					へ 12:12 へ 10 歳 中 よ 英 <u>2021/12/14</u> 見

8.2. Authorizations - Status : Pass ////获得相关权限授权

aruba		Clearl	Pass Policy Manag	jer		-	Menu 🗮	
Dashboard 0	Monitoring > Live Moni	toring » Access Tracker						
Monitoring O	Access Tracker	Dec 14, 2021 12:25:45 CST					🕑 Auto Refresh	
Live Monitoring	The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.							
Accounting OnGuard Activity Analysis & Trending	T [All Requests]	RC-CPPM		b Last 1 week	k before Tod	ay	Edit	
System Monitor	Filter: Request ID	TACACS+ Session Details			•		Show 1000 V records	
Profiler and Network Scan	* Ever	Summary Request Policies Autho	rizations			Login Status	Request Timestamp *	
	1.				VICE	ACCEPT	2021/12/14 12:25:14	
Discovered Devices	2.	Commands Used Status Request Tim	ie		VICE	ACCEPT	2021/12/14 12:24:21	
Audit Viewer	з.	shell exec Pass Dec 14, 2021	12:25:14 CST		VICE	ACCEPT	2021/12/14 12:24:03	
Event Viewer	4.					ACCEPT	2021/12/14 12:23:53	
Blacklisted Users	5.					ACCEPT	2021/12/14 12:20:57	
	6.				VICE	ACCEPT	2021/12/14 12:19:11	
	7.					ACCEPT	2021/12/14 12:18:32	
	8,						2021/12/14 12:18:24	
	9.					ACCEPT	2021/12/14 12:18:23	
	10.				VICE	ACCEPT	2021/12/14 12:12:31	
	11.					ACCEPT	2021/12/14 12:12:11	
	12.				VICE	ACCEPT	2021/12/14 12:08:37	
	13.				VICE	ACCEPT	2021/12/14 12:07:46	
	14.				VICE	ACCEPT	2021/12/14 12:07:31	
	15.				VICE	REJECT	2021/12/14 12:07:23	
	16.	Id d Showing 1 of 1-1000 records > >I		Export Logs Close		ACCEPT	2021/12/14 12:07:13	
	17.	RADIUS	struggie.znu	WIT		ACCEPT	2021/12/14 12:06:34	
	18.	RADIUS	claire.chu			ACCEPT	2021/12/14 12:03:28	
	19.	RADIUS	wenyong.liuwy			ACCEPT	2021/12/14 12:03:03	
	20.	RADIUS	0794491			REJECT	2021/12/14 12:01:38	
		RADIUS	0794491			REJECT	2021/12/14 12:01:33	
	22.	RADIUS	0794491			REJECT	2021/12/14 12:01:30	
Configuration 0	23.	RADIUS	0794491			REJECT	2021/12/14 12:01:24	
Administration 0	24.	RADIUS	0794491			REJECT	2021/12/14 12:01:21	
Copyright 2020 Hewlett Packard Enterprise Developme	ent LP	Dec 14, 20	21 12:26:26 CST			ClearPass I	Policy Manager 6.8.7.120583 on C2000V	



8.3. 交换机查看登陆用户

IDUBLICATION IN THE PROVINCE INTERPORT OF THE PROVINCE INTERPORT

9. 测试验证-2

测试方法:使用在非对应 memberOf 属性值的组成员账号登陆 H3C 交换机

测试结果:在 ClearPass Tracker 中查看日志信息

测试结果说明:

- Summary Status: AUTHEN_STATUS_PASS 成功通过认证
- Authorizations Status: Fail ////因无法匹配 SW ADMIN 的角色,授权失败,无法登 陆交换机;如下图二所示



Summary Red	quest P	olicies	Authorizations	Alerts	
commands Used	Status Fail	Requi	e <u>st Time</u> 4, 2021 12:19:11	CST	1007-00110 2021-12