

ClearPass 通过 AD userDN 属性实现 802.1x 认证准入

fox210317@sina.com

需求:

 需通过 WLAN 对接 AD 实现 802.1X PEAP 认证,同时要限制 AD 中不同部门的准入, 以及每个账号登陆设备的数量。

实现思路:

- ClearPass 的 Policy 可以通过 Authorization: AD userDN "xxxx"并返回给无线控制器准入信息。
- 通过 Profile 中 Post_Authentication 返回无线控制器 Active-Session-Count=2
- 不使用 clearpass role-mapping 功能,某些客户对于 role-mapping 的配置逻辑理解
 不够深入



1. ClearPass 中添加 Devices

配置路径:

configuration -Network -Devices -Add

说明:

- Name : ARUBA AC
- IP or Subnet Address:填写无线控制器的 IP,如有多台可多次添加或添加一个网段
- RADIUS Shared Secret:需要在 Aruba 无线控制器和 ClearPass 保持一致的密钥
- Vendor Name:选择 Aruba
- Enable RADIUS Dynamic Authorization : 开启
- SAVE

aruba	ClearPass Policy Manager	Menu 🗮
Dashboard O	Configuration » Network » Devices	
🖬 Monitoring 🛛 🔹 🛛	Network Devices	Add
😤 Configuration 💿		Evport All
- @ Service Templates & Wizards		Discovered Devices
- Ø Services	A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.	
🗉 🖶 Authentication		
- 🗘 Methods	Filter: Name	Show 1000 Trecords
-Ø Sources	# 🖩 Name 🖌 IP or Subnet Address Description	
🗈 🖴 Identity		Conv Export Delete
-Q Single Sign-On (SSO)	Add Device C	Contra Contract
- Endosinte	IP/Subnet Address (192168.1.1) is invalid	
- in Static Host Lists	Davice SNMD Read Settings SNMD Write Settings CLT Settings OnConnect Enforcement Attributes	
- in Roles	Severe steamy steamy steamy car sectings on connect and connect and the	
C Role Mappings		
∋ ⊕ Posture	Name: Aruba AC	
- @ Posture Policies	IP or Subnet Address: 192168.1.1/32 (e.g., 192.168.1.1/0 or 192.168.1.1/24 or	
–iQ Audit Servers	192.168.1.1-20)	
- @ Agentless OnGuard	Description:	
e Enforcement		
- Q Policies	RADIUS Shared Secret: Verify:	
	TACACS+ Shared Secret: Verify:	
- Devices	Vendor Name: Aruba *	
Device Groups	Enable RADIUS Dynamic Authorization: # Port: 3799	
- © Proxy Targets	Enable RadSec:	
- 🛱 Event Sources		
- 💭 Network Scan		
- © Policy Simulation	Add Cancel	
		識法 Windows
		16 회 없을 NUBLE Windows,
🐉 Administration 🔹 🔍 🛛		
© Copyright 2019 Hewlett Packard Enterprise Development	ent LP Dec 28, 2021 11:17:27 CST ClearPass Po	licy Manager 6.8.4.120034 on CLABV platform

添加完成如下:

aruba		ClearPass Policy Manager		Menu 🗮
Dashboard Monitoring Monitoring	Configuration » Network » Devices Network Devices A Network Access Device (NAD) must belong to the akibal li	st of devices in the ClearRess database in order to connect to ClearRess		 Add & Import
BAuthentication Q Methods Q Sources Be Identity Q Single Sign-On (SSO) C Local Vers	Filter: Name	Go Clear Filter IP or Subnet Address 192.168.1.1/32	Description WLAN controller	Show 1000 V records
- © Endpoints - © Static Host Lists - © Roles - © Roles ■ ¹⁸ Posture - © Abla Servers - © Audit Servers				



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
Dashboard O Configurati	on » Authentication » Sources » Add - AD-TEST
Monitoring • Authenti	cation Sources - AD-TEST
& Configuration Summary	General Primary Attributes
Gervice Templates & Wizards Gervices Authentication Gervices Authentication Gervices	AD-TEST
- Q Sources Type:	Active Directory
O Single Sign-On (SSO) Use for Aut O Local Users Authorizatio D Endpoints O Static Host Lists O Relies	nonzation: M Enable to use this Authentication Source to also fetch role mapping attributes I Bernave View Details - Select -
- Q Role Mappings Server Time	aout: 10 seconds
Desture Policies Cache Time	aut: 180 seconds
Audit Servers Backup Ser Agentless OnGuard	vers Priority: Move Up -
a Benforcement - → Policies	Add Backup Remove
⊉ Profiles ⊒ +Network	
O Devices O Device Groups O Prove Torops O Prove Torops O Prove Tources O Levent Sources O Aletwork Soan O Policy Simulation	



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 O	Configuration » Authen	tication » Sourc	es » Add - A	D-TEST	
🖅 Monitoring 🔹 💿	Authentication So	urces - AD-1	EST		
🝰 Configuration 💿	Summary General	Primary	Attributes		
– 🛱 Service Templates & Wizards	Gammary General		Terroutes		Connection Datails
- 🛱 Services	Lie also a second				Connection Details
🖙 🖴 Authentication	Hostname:	ABC.DEF.COM			
- 🛱 Methods	Connection Security:	None	۲		
- 🗘 Sources	Port:	389 (For se	cure connect	ion, use 636)	
E SIdentity	Verify Server Certificate	: 🗹 Enable to v	erify Server	Certificate for secure connection	
-@ Single Sign-On (SSO)	Bind DN:	admin@DEF.CO	M		
- 🛱 Local Users		(e.g. administr	,dc=example,dc=com)		
- O Endpoints	Bind Password:				
Q: Static Host Lists 🛱 Roles	NetBIOS Domain Name:	ABC.DEF			
🛱 Role Mappings	Base DN:	dc=DEF,dc=COM			Search Base Dn
🖃 🖶 Posture	Search Scope:	SubTree Search	•		
- Posture Policies	LDAP Referrals:	Follow referred	als		
- Q Audit Servers	Bind User:	Allow bind us	sing user pa	ssword	
- g Agentiess UnGuard	User Certificate:	userCertificate			
- Belicies	Always use NetBIOS na	me: 🗆 Enable f	o always us	e NetBIOS name instead of the doma	in part in username for authentication
- Profiles					
- + Network					
- ä Devices					
- Device Groups					
Proxy Targets					
- D Event Sources					
- @ Network Scan					
- O Policy Simulation					

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<mark>作为授权使用</mark>



SAVE



3. Profile 配置

3.1. Return Aruba-User-Role Profile 配置

配置路径:

Configuration - Enforcement - Profiles - Add

参数配置:

- **Template**: Aruba RADIUS Enforcement
- Name: Return Aruba User Role
- Description: 描述/备注
- Action : Accept
- Service Attributes: (此条 rule 用于返回给 Aruba 无线控制器,因此 EMPLOYEE 仅被 Aruba 无线控制器识别)
 - Type: RADIUS: Aruba、Name: Aruba-User-Role、Value: EMPLOYEE (大小 写需要与 Aruba Controller 一致)

SAVE

aruba		ClearPass Polic	cy Manager			Menu
Dashboard •	Configuration » Enforce	ement » Profiles » Edit Enforcement Profile - Return Aruba User F	Role			
🖬 Monitoring 🔹 🔹	Enforcement Prof	iles - Return Aruba User Role				
🝰 Configuration 💿	Summary Brofile	Attributor				
Gervice Templates & Wizards Miservices	Profile:	Actiones				
Authentication	Name:	Return Aruba User Role				
- 🔅 Methods	Description:					
- @ Sources	Type:	RADIUS				
🖃 🚨 Identity	Action:	Accept				
-@ Single Sign-On (SSO)	Device Group List:	- · · · · · · · · · · · · · · · · · · ·				
- @ Local Users	Attributes:					
- p Endpoints	Type	Name		Value		
- g Static Host Lists	1. Radius:Aruba	Aruba-User-Role		 EMPLOYEE 		
- C Role Mappings						
- 🛱 Posture Policies						
- @ Audit Servers						
- @ Agentless OnGuard						
⊴-8 Enforcement						
- @ Policies						
-O Profiles						
G-						
- 🛱 Devices						
-g Device Groups						
- C Proxy Targets						
- g Event Sources						
-grondy sindadan						
					396年 Windows	
					DXIA WINGOVS	
	K Back to Enforcement	ent Profiles			转到"设置"以为"Copy"的Sa	Cancel
Administration o						



3.2. Enforcement Profiles - Device Count Profile 配置

配置路径:

Configuration - Enforcement - Profiles - Add

参数配置:

- **Template**: Session Restrictions Enforcement
- Name: Device Count Profile
- **Description**: 描述/备注
- **Type**: Post_Authentication (无法变更)
- Action: accept (无法变更)
- Service Attributes:
 - Type : Session-Check、Name : Active-Session-Count、Value : 2

SAVE

aruba			ClearPass Policy Manager		Menu 🗮
📲 Dashboard	 Configuration » Enf 	proement » Profiles » Edit Enforcem	ent Profile - Device Count Profile		
Monitoring	 Enforcement Pr 	ofiles - Device Count Profi	e		
& Configuration	Summary Prof	ile Attributes			
Zerafiyarada Z	Summary Prof Summary Prof Profile: Name: Oescription: Type: Addon: Device Group List: Type 1. Session-Che	Onlies - Device Count Profile Entributes Perice Count Profile Imitation for users Post_uberroration -	e Name Active-lession-Count	Value - 2	
Pretvork Overs Overs	< Back to Enforce	ment Profiles			激活 Windows 時間 2011 Copy Sow Careet
🚰 Administration	•				
© Copyright 2019 Hewlett Packard Enterprise Develo	opment LP		Dec 28, 2021 11:59:03 CST		ClearPass Policy Manager 6.8.4.120034 on CLABV platform

TIPs:

以上创建的2条 Profile, 需要同时调用在 Policies	s 一个 rule 中使用;
针对不同的 Role (Aruba Controller Role) 需要写	多条 Profile rule.



4. Policies 配置

配置路径:

Configuration - Enforcement - Policies - Add

参数配置:

- Enforcement:
 - Name: ARUBA-WLAN-802.1X
 - Description:
 - Enforcement Type: 勾选 RADIUS
 - Default Profile: OTHER DENY
- Rules: (同理写 rule 1-3)
 - Rules Evaluation Algorithm: Select first match
 - Enforcement Policy Rules:
 - 1、 Type: <u>Authorization: GM-AD</u>、Name: <u>UserDN</u>、Operator: <u>CONTAINS</u>、 VALUE: <u>OU=MOS,DC=MOS,DC=COM</u>
 - 2、 Type: Tips、Name: Role、Operator: EXISTS
 - 3、 Enforcement Profiles (调用 3.1、3.2) :
 - 3.1. Return Aruba User Role
 - 3.2. Device Count Profile
 - 4、 SAVE

aruba		ClearPass Po	olicy Manager		Menu
· 仪表板 0	配置 » 服务 » 编辑 - GoerM	licro_Service			
Ø ≦#O Ø Ø Ø Ø	服务 - GoerMicro	Service			
。 総置 ・	摘要 服务 身份验证	授权 角色 强制			
- 静服务模板与向导	使用缓存的结果:	□ 使用先前会话中缓存的角色和状况厚			
	强制策略:	GM-EMPLOYEE-Enforcement-Policy	✔ 修改		添加新的强制策略
			强制策略详细信息		
	描述:	Goermicro 最新策略			
↓单—登录(SSO)	默认配置文件:	OTHER DENY			
· 章本地用户	规则评估算法:	first-applicable			
- 登 调点 - 凸 静态主机列表	条件			强制配置文件	<i>.</i>
- 2 角色	1. (Authorization:GM AND (Tips:Bole	-AD:UserDN CONTAINS OU=P.E.A,(OU=MOS,DC=MOS,DC=COM)	OTHER DENY	
_☆ 角色映射	(Authorization:GM	-AD:UserDN CONTAINS			
 中状況 二 書 福制 	2. OU=Computers,OU=	MOS,DC=MOS,DC=COM)		OTHER DENY	
→☆ 策略 → ○ 配置文件	3. (Authorization:GM- AND (Tips:Role	-AD:UserDN CONTAINS OU=MOS,C EXISTS)	DC=MOS,DC=COM)	GM-Employee-Profile; Device Count Pro	ofie
 → 网络 ○ 设备 ○ 设备 ○ 设备 ○ 代理目标 ○ 代理目标 ○ 代理目标 ○ 同端扫描 ○ 同端扫描 ○ 預時機以 					
					100
o (11)	< 巡回到服务			魏用	复制 保存



5. Services 配置

配置路径:

Configuration -Services -Add

参数模板关联配置:

• Service :

Type: Aruba 802.1X Wireless

Name: ----Aruba WLAN 802.1X----

Description: Aruba 802.1X Wireless Access Service

Service Rule:

Match	es 🔍 ANY or 💌 ALL of the following conditions:]					
	Туре	Name	Operator	Value		
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	助	8
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate- Only (8)	B	*
з.	Radius:Aruba	Aruba-Essid-Name	EQUALS	ABC	89	8
4.	Click to add					

Authentication:

Authentication Sources:选择以添加的认证源 AD "GM-AD"

• Authorization:

Additional authorization sources from which to fetch role-mapping attributes -

GM-AD [Active Dictory]

- Roles : 空
- Enforcement:

Enforcement Policy: "ARUBA-WLAN-802.1X"

SAVE

下图为实验环境模拟,请忽略 AD-TEST(同 GM-AD)



uba			ClearPass Policy Manag	er	Menu				
Dashboard	 Configuration » Set 	ervices » EditAruba WLAN 802.1							
Ionitoring	Services	Aruba WI AN 802.1X							
onfiguration	Cummon Co	wice Authentication Authorization	ion Polor Enforcement						
Service Templates & Wizards	Service:	vice Addientication Addioniza	ton Koles Emorcement						
Authentication	Name:	Aruba WLAN 802.1X							
- ä Methods	Description:	Aruba 802.1X Wireless Access 9	ervice						
O Sources	Type:	Aruba 802.1X Wireless							
dentity	Status:	Enabled							
Ø Single Sign-On (SSO)	Monitor Mode:	Disabled							
- 🛱 Local Users	More Options:	Authorization							
- 🛱 Endpoints									
- 🛱 Static Host Lists		Service Rule							
- 🛱 Roles	Match ALL of the fo	llowing conditions:							
🛱 Role Mappings	Туре		Name	Operator	Value				
osture	1. Radius:IET	-	NAS-Port-Type	EQUALS	Wireless-802.11 (19)				
- Q Posture Policies	Radius:IETI	-	Service-Type	BELONGS_TO	(R)				
- D Audic Servers	3. Radius:Aru	ba	Aruba-Essid-Name	EOUALS	ABC				
-g Agendess Onduard	Authentication:								
(h Dolicier	Aught and in shire Mark	hada: 1 (CAD DCAD)							
© Profiles Network	Addentication Me	2. [EAP FLS] 3. [EAP TLS] 4. [EAP TTLS]							
- Devices	Authentication Sou	arces: AD-TEST [Active Directory]							
- D Proxy Targets	Strip Username Ru	les: -							
A Event Sources	Service Certificate:	-							
letwork Scan	Authorization:								
Policy Simulation	Authorization Deta	ils: AD-TEST [Active Directory]							
	Roles:								
	Role Manning Polic	W1 -							
	Enforcement:								
	Use Cached Result	s: Disabled							
	Enforcement Policy	ARUBA-WLAN-802.1X							
	and a second for the party				激活 Windows				
					and la TTTTTG OTTO				

6. ClearPass 开启 RADIUS ACCOUNTING

配置路径:

Administration – Server Manager – 选择配置的这台 CPPM – Service Parameters –

Select Service : RADIUS SERVER

Accounting Log Accounting Interim-Update Packets : TRUE

aruba			ClearPass	Policy Ma	nager				Menu 🗮
E Dashboard	 Administration » Server Ma 	nager » Server Configuration - L	ab1-CPPM-1						
Monitoring	Sonyor Configuration	- Lab1-CDDM-1 (10.1.50	41)						
Configuration	e Server configuration	- Eab1-CFFM-1 (10.1.50.	41)						
Administration	System Services Con	trol Service Parameters S	ystem Monitoring	Network F	IPS				
	Select Service: R	adius server 🔻							A
- Proceeding and Devidence		Daxameter Mame			Davamo	tor Val		Default Value	Allowed Valuer
Gerver Manager	EAD-EAST	Parameter Name			Parame	ter vai	ue	Default value	Allowed Values
- A Server Configuration	Mactar Kay Evoira Tima				1 144	nake v		1 wooks	
- 2 Log Configuration	Master Key Grace Time				3 144	ooks v		2 weeks	
Local Shared Folders	PACe are valid across dud	tar			TRUE	•		TRUE	
- Dicensing	Provy	(6)			more			TROL	
Device Insight	Maximum Response Delay				5		saconde	5	1.5
External Servers	Maximum Reactivation Tim				120		records	120	60.2600
- SNMP Trap Receivers	Maximum Retry Counts	0			6	_	retries	5	2-10
- P Syslog Targets	Accounting				~		i cones	5	2-10
- P Syslog Export Filters	Log Accounting Interim Lin	date Darkete			TRUE	•		EAL CE	
- Je Messaging Setup		Gate Petrols			more			THESE	
- P Endpoint Context Servers	Maximum Number of Three				20		threads	20	10-200
- Pile Backup Servers	Number of Initial Threads	103			10		threads	10	5-300
- PExternal Accounts	AD Errors						0110005	10	0 000
E 🐱 Certificates	Window Site				5		minuter	6	1.60
Certificate Store	Number of Errors				160		111110/03	150	10-1000
- JP Trust List	Recovery Action				None			None	10-1000
- / Revocation Lists	Security				reone			Tear Inc	
- Ulctionaries	Reject Darket Delay				1		seconds	1	0.5
A PADIUS A PADIUS A paper of the prime of th	Maximum Attributes				200		attributer	200	0.512
aTACACC - Comises	Dropace Service Status Per	avect			EALOE	•	accibuces	ENICE	0.011
Device Eingergrints	Main	fnear			TALUL			THESE	
Dictionary Attributes	Authentication Bort				1812	1645		1012 1645	
Applications	Accounting Port				1912	1646		1012, 1646	
Context Server Actions	Maximum Request Time				30	1040	seconds	20	5,120
Ingress Events	Cleanun Time				5		seconds	50	3-10
Windows Hotfixes	Local DB Authentication Sc	aurce Connection Count			32	_	accontas	32	5-150
- Agents and Software Updates	ADA DAR Authentication Sc	aurce Connection Count			64			64	5-200
- P OnGuard Settings	SOL DB Authentication Sol	urse Connection Count			32	_		20	2012年 11/1:15:300 10
- P Software Updates	and a second second second					_			
🕾 🗞 Support	Configuration	uration							转到 吸血 以應口 K 應口 K m Cancel
- P Contact Support	-								
Copyright 2019 Hewlett Packard Enterprise Develop	ment LP		Dec 28, 2021 12:	20:17 CST				ClearPass	Policy Manager 6.8.4.120034 on CLABV platform

7. 无线控制器开启 ACCOUNTING

7.1. 修改 802.1x authentication default role & 开启 Accounting

说明:

在 ClearPass 通过 VSA (Return User Role 的方式) 返回给 Aruba 无线控制器 user-role

时, 此处 AAA Profile 写的 802.1X Authentication Default Role 为 authenticated 会被

ClearPass 返回的 EMPLOYEE 覆盖

Role Derivation Sequence :

	CONTROLLERS ACCESS PO ⊙ 1 ○ 0 ⊙ 2 ○	INTS CLIE	NTS ALERTS № 0 🛆 1	0	admin 🗸
Auth Servers	AAA Profiles L2 Authe	ntication L3	Authentication User Rules Advanced		
ΘĒA4	AA	Î	Initial role:	logon	~
Θ	302.1X-AAA-PRO	ŵ	MAC Authentication Default Role:	guest	~
	802.1X Authentication 802.1X Authentication Service	er Group	802.1X Authentication Default Role:	authenticated	~
	MAC Authentication		Download Role from CPPM:		
	MAC Authentication Serve RADIUS Accounting Server	Group Group	Set username from dhcp option 12: L2 Authentication Fail Through: Multiple Server Accounting:		
	RFC 3576 server XML API server	- 1	User idle timeout:		seconds
⊕ [NoAuthAAAProfile		Max IPv4 for wireless user:	2	
⊕ [default		RADIUS Roaming Accounting:		
⊕ [default-dot1x		RADIUS Interim Accounting:		
•	default-dot1x-psk		RADIUS Acct-Session-Id In Access-Request:		
⊕ [🖥 default-iap-aaa-prof		User derivation rules:	-None- 🗡	
		·	Wired to Wireless Roaming:		
			Reauthenticate wired user on VLAN change:		
			Device The Classifications	State and a second second	



φ.

7.2. AAA Profile 调用 RADIUS ACCOUNTING SERVER-GROUP

说明:

如不调用 RADIUS ACCOUNTING SERVER-GROUP,则 ClearPass 无法收到 Accounting 报文

AAA Profiles Server Group: lab1-sg	
⊙ 📑 802.1X-AAA-PRO	~
🕞 802.1X Authentication Fail Through:	
802.1X Authentication Server Group Load Balance:	
G MAC Authentication	
MAC Authentication Server Group	
🕞 RADIUS Accounting Server Group	
🕞 RFC 3576 server	
TXML API server	
⊕	
⊕ default ■	
④ ☐ default-iap-aaa-prof	
¥	
	激活 Windows



8. 测试验证-1

测试方法:使用在对应 UserDN 属性值的组成员账号连接 ARUBA WLAN

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 (ACCEPT)

aruba		ClearPas	s Policy Mana	ger		Menu 🚞
	^{监视 »} Live Monitoring » 访 访问跟踪器 Jan 05, 20	问跟踪器 22 17:25:25 CST		and the second		● 自动刷新
Live Monitoring 》访问跟踪器 》记帐	请求详细信息 接要 输入 输出		423		• •	
—————————————————————————————————————	登录状态:	ACCEPT				2014
分析与趋势	会话标识符:	R000c49d1-01-61d563f9)			
	日期和时间:	Jan 05, 2022 17:25:13	CST			显示 20 ✔ 记录
	终端主机标识符:	38-BA-F8-10-F4-23			tatus	Request Timestamn *
₩ 事件查看器	用户名:	lena.liang			tutus	2022/01/05 17:25:13
	访问设备 IP/端口:	10.80.66.19				2022/01/05 17:23:15
	访问设备名称:	10.80.66.17			1000	2022/01/05 17:24:58
	系统状况状态:	UNKNOWN (100)			10000	2022/01/05 17:24:56
		便	用的策略 -			2022/01/05 17:24:55
	服务:	GoerMicro Service			- 1 C	2022/01/05 17:24:54
	身份验证方法:	EAP-PEAP.EAP-MSCHAPv	2			2022/01/05 17:24:52
	身份验证源:	AD:DC01-WF.mos.com				2022/01/05 17:24:52
	授权源:	GM-AD				2022/01/05 17:24:51
	角色:	[User Authenticated]				2022/01/05 17:24:43
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	强制配置文件:	GM-Employee-Profile				2022/01/05 17:24:42
					·	2022/01/05 17:24:35
	▲ 显示第1 策记家,共	1-20 荼▶▶	更改状态显示	和置 导出 显示日志	关闭	2022/01/05 17:24:08
						2022/01/05 17:24:00
	14. 10.80.18.6	KADIUS	0877973	Goermicro_Service	REJECT	2022/01/05 17:23:55
A22 0	15. 10.80.18.6	KADIUS	844/411/	GM-Guest-Service	ACCEPT	2022/01/05 17:23:53
(1) 合理 (1)	16. 10.80.18.6	RADIUS	0877973	GoerMicro_Service	REJECT	2022/01/05 17:23
1 de la companya	17 110 00 10 6	DAMAGE	10 77672	Georgiano Consico	DETERT	30333003 /ns 17-32



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



1.	(Authorization:GM-AD:UserDN CONTAINS OU=P.E.A,OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS)	OTHER DENY	20
2.	(Authorization:GM-AD:UserDN CONTAINS OU=Computers,OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS)	OTHER DENY	
3.	(Authorization:GM-AD:UserDN CONTAINS OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS)	GM-Employee-Profile	



9. 测试验证-2

测试方法:使用在非对应 UserDN 属性值的组成员账号连接 ARUBA WLAN

测试结果:在 ClearPass Tracker 中查看日志信息

测试结果说明:

CN=it,OU=P.E.A,OU=MOS,DC=MOS,DC=COM 匹配情况如下图所示

Rul	95:	
Rul	es Evaluation Algorithm: First applicable	
	Conditions	Actions
1.	(Authorization:AD-TEST:UserDN CONTAINS OU=P.E.A.,OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS)	[Deny Access Profile]
2.	(Authorization:AD-TEST:UserDN CONTAINS OU=Computers,OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS)	[Deny Access Profile]
з.	(Authorization:AD-TEST:UserDN CONTAINS OU=MOS,DC=MOS,DC=COM) AND (Tips:Role EXISTS)	Device Count Profile, Return Aruba User Role

9.1. 使用 Rule 1 对应的 OU, 获取 Deny Access Profile 的权限

登陆状态:	REJEC	T.
强制配置文	件:	" <mark>OTHER DENY</mark> "

摘要 输入 输出 警訊	E JOY	
	REJECT	
会话标识符:	R000b7e65-01-61c80a6e	
日期和时间:	Dec 26, 2021 14:23:43 CST	
终端主机标识符:	E4- 💶 📁 (Computer / Windows / Windows)	
用户名:	it	
访问设备 IP/端口:	10.4	
访问设备名称:	10.	
系统状况状态:	UNKNOWN (100)	
	使用的策略 -	
服务:	GoerMicro_Service	7
身份验证方法:	EAP-PEAP,EAP-MSCHAPv2	
身份验证源:	AD:D	
授权源:	GM-AD	
角色:	[User Authenticated]	
强制配置文件:	OTHER DENY	

a Hewlett Packard Enterprise company

RADIUS 请求		۲
授权属性		۲
Authorization:GM-AD:Account Expires	9223372036854775807 [30828-09-14 10:48:05 CST]	
Authorization: GM-AD: Email	it@goermicro.com	
Authorization:GM-AD:memberOf	CN=M-IAM-MGMT,OU=ITManager,OU=MosGroup,DC=MOS,DC=COM	
Authorization:GM-AD:Name	it	
Authorization:GM-AD:UserDN	CN=it,OU=P.E.A,OU=MOS,DC=MOS,DC=COM	

9.2. 使用非 AD 内的设备登陆

配置文件为 <mark>OTHER DENY</mark>

请求详细信息				0
摘要 輸入 輸出	警报	133		
日期和时间:	Jan 05,	2022 17:30:44 CST		
终端主机标识符:	B2-2	_2		
用户名:		@goermicro.com		
访问设备 IP/端口:	10			_
访问设备名称:	10.	.7		
系统状况状态:	UNKNO	WN (100)		
		使用的策略 -		
服务:	GoerMi	cro_Service		
身份验证方法:	EAP			
身份验证源:	None			11
授权源:	GM-AD			
角色:	-			
强制配置文件:	OTHER	DENY		
服务监视器模式:	Disable	d		
在线状态:	不可用			v
◄ ■示第 2 条记录,共	1-20 条 🕨		示配置 导出 显示日志	关闭



Authorization:GM-AD:UserDN 为<mark>空</mark>

请求详细信息	
摘要 输入 輸出 警报	123
用户名: / ng@goermicro.com	
终端主机标识符: B2-26	
访问设备 IP/端口: 10.8	
RADIUS 请求	
授权属性	
Authorization:GM-AD:UserDN	
计算的属性	
24	

强制配置文件:	OTHER DENY	
系统状况状态:	UNKNOWN (100)	
审核状况状态;	UNKNOWN (100)	