

Aruba Hand-On Lab Guider

ClearPass - Basic Configuration

2019.10.28

V 1.2

Jihu Sun

Zhengxin Yang

Jinghao Ma

目录

<u>1</u> L	AB 拓扑环境和设备登录信息	<u></u>	<u>7</u>
1.1	LAB 内容简介		7
1.2	LAB 设备及拓扑	•••••	7
1.3	LAB 设备 VLAN 和 IP 信息	•••••	8
1.4	LAB 设备登录账号和密码	••••••	9
<u>2</u> <u>T</u>	ASK1: 创建一个最简单的认证服务	<u></u>	10
2.1	用户需求		10
2.2	实现思路	•••••	10
2.3	CLEARPASS 配置	•••••	10
2.3.1	登录 CLEARPASS		10
2.3.2	添加网络设备		11
2.3.3	添加服务器参数		12
2.3.4	添加本地账号和角色	•••••	13
2.3.5	添加认证服务		14
2.4	控制器配置		16
2.5	验证结果	•••••	17
<u>3 T</u>	ASK2: ARUBA 控制器集成	<u></u>	18
3.1	用户需求		18
3.2	实现思路	•••••	18
3.3	CLEARPASS 配置	•••••	18
3.3.1	添加本地账号		18
3.3.2	添加认证服务		19
3.4	控制器配置	•••••	25
3.4.1	开启 PEF 功能	••••••	25
3.4.2	关闭 CPSEC	26	
3.4.3	添加 AP-GROUP	27	a Hewlett Packard Enterprise company

3.4.4	添加无线信号	
3.4.5	添加认证和计费服务器	
3.5	验证结果	33
<u>4 T/</u>	ASK3: ARUBA 控制器集成 CPPM 实现 PORTAL 认证	37
4.1	用户需求	37
4.2	实现思路	37
4.3	CLEARPASS 配置	38
4.3.1	取消内置的 HTTP 到 HTTPS 的跳转	
4.3.2	添加本地账号和角色	
4.3.3	添加 PORTAL 登录页面	
4.3.4	添加认证服务	41
4.4	控制器配置	47
4.4.1	添加无线信号	
4.4.2	修改 PORTAL 认证配置	
4.4.3	添加 Portal 重定向	
4.4.4	添加角色	
4.4.5	添加计费	51
4.5	验证结果	52
<u>5 T/</u>	ASK4: ARUBA	56
5.1	用户需求	56
5.2	实现思路	56
5.3	CLEARPASS 配置	56
5.3.1	添加本地账号和角色	
5.3.2	添加认证服务	
5.4	控制器配置	66
5.4.1	添加无线信号	
5.4.2	添加角色	
5.4.3	添加计费	73
5.5	验证结果	orubo
		a Hewlett Packard Enterprise company

5.5.1	终端上的关联和登录记录	75
5.5.2	2 CPPM 上查看认证记录	75
5.5.3	9 控制器上查看认证记录	77
<u>6 T</u>	ASK5: ARUBA <mark>控制器集成 CPPM 实现无感知认证(</mark> MAC + PORTAL)	78
6.1	用户需求	78
6.2	实现思路	78
6.3	CLEARPASS 配置	78
6.3.1	- 添加 Portal 登录页面	
6.3.2	2 添加 мас саснілд 认证服务	79
6.3.3	8 添加 мас 认证服务	85
6.4	控制器配置	91
6.4.1	· 添加无线信号	91
6.4.2	2 修改 PORTAL 认证配置	92
6.4.3	8 添加 MAC 认证	93
6.4.4	~	94
6.4.4 6.5	· 添加订费	94 9 5
6.4.4 6.5	· 添加订费	94
6.4.4 6.5 <u>7</u> <u>T</u>	¹ 添加订费 验证结果 ASK6:ARUBA 控制器集成 CPPM 实现访客自注册认证	
6.4.4 6.5 <u>7</u> <u>T</u>	[。]	
6.4.4 6.5 <u>7</u> <u>T</u> 7.1	[、]	
6.4.4 6.5 <u>7</u> <u>T</u> 7.1 7.2	 添加订费 验证结果 TASK6:ARUBA 控制器集成 CPPM 实现访客自注册认证 用户需求 实现思路 	
6.4.4 6.5 7 <u>T</u> 7.1 7.2 7.3	添加订费 验证结果 在SK6:ARUBA 控制器集成 CPPM 实现访客自注册认证 用户需求 成正名野ASS 配置 CLEARPASS 配置	
6.4.4 6.5 7 <u>T</u> 7.1 7.2 7.3 7.3.1	 添加订安 验证结果 TASK6:ARUBA 控制器集成 CPPM 实现访客自注册认证 用户需求 取现思路 CLEARPASS 配置 添加 SMTP 信息 	
6.4.4 6.5 7 <u>T</u> 7.1 7.2 7.3 7.3.1 7.3.2	 添加口安 验证结果 ASK6:ARUBA 控制器集成 CPPM 实现访客自注册认证 用户需求 实现思路 交现思路 CLEARPASS 配置 添加 SMTP 信息 添加访客 PORTAL 自注册页面 	
6.4.4 6.5 7.1 7.1 7.3 7.3.1 7.3.2 7.3.3	 添加订费	
6.4.4 6.5 7.1 7.2 7.3.1 7.3.2 7.3.3 7.3.4	 添加订费	
6.4.4 6.5 7 <u>T</u> / 7.1 7.3 7.3.1 7.3.2 7.3.3 7.3.4 7.3.5	 添加订费	
6.4.4 6.5 7 <u>T</u> 7.1 7.2 7.3.1 7.3.2 7.3.3 7.3.4 7.3.5 7.4	 添加订费	
6.4.4 6.5 7.1 7.2 7.3.1 7.3.2 7.3.3 7.3.4 7.3.5 7.4 7.4.1	 添加正按	
6.4.4 6.5 7.1 7.2 7.3 7.3.1 7.3.2 7.3.3 7.3.4 7.3.5 7.4 7.4.1 7.4.2	 添加口子母	
6.4.4 6.5 7 <u>T</u> . 7.1 7.2 7.3.1 7.3.2 7.3.3 7.3.4 7.3.5 7.4 7.4.1 7.4.2 7.4.3	 添加口按	

7.4.4	4 添加计费	
7.5	验证结果	
7.5.1	1 终端侧的无线关联和访客自注册	
7.5.2	2 CPPM 上查看认证记录	
7.5.3	3 控制器上查看认证记录	
<u>8 T</u>	TASK7: ARUBA	
8.1	用户需求	141
8.2	实现思路	141
8.3	CLEARPASS 配置	141
8.3.1	1 添加 NAS CLIENT	
8.3.2	2 添加本地账号和角色	
8.3.3	3 添加认证服务	
8.4	控制器配置	154
8.4.1	1 添加 TACACS 服务器和服务器组	
8.4.2	2 添加管理员的认证	
8.5	验证结果	
8.5.1	1 CPPM 上查看认证记录	
8.5.2	2 控制器上查看认证记录	
<u>9 T</u>	TASK8: INSIGHT 实现自动生成报表及告 警	
9.1	用户需求	
9.2	实现思路	
9.3	CLEARPASS 配置	
9.3.1	1 开启 INSIGHT 功能	
9.3.2	2 进入 INSIGHT 界面	
9.3.3	3 添加 Insight Report	
9.3.4	4	
<u>10</u>	<u>TASK9: CPPM 认证基本问题诊断</u>	

10.1	用户需求174
10.2	实现思路174
10.3	CLEARPASS 认证问题诊断174
10.3.1	访问跟踪器过滤和查看认证记录174
10.3.2	通过访问跟踪器分析认证失败原因176
10.3.3	通过事件查看器分析认证失败原因180
10.3.4	通过 CLEARPASS 抓包分析认证失败原因183
<u>11 T</u>	ASK10: CLEARPASS 集群管理186
11.1	用户需求186
11.2	实现思路186
11.3	CLEARPASS CLUSTER 集群配置
11.3.1	开启 CLUSTER 集群186
11.3.2	添加 VIRTUAL IP188
11.4	验证结果189
11.4.1	检查 CLEARPASS 集群状态189
11.4.2	检查配置同步
<u>12</u>	付录194
12.1	Тазк1 实现思路
12.2	Тазк2 实现思路
12.3	Таѕк3 实现思路
12.4	Таsк4 实现思路
12.5	Таѕк5 实现思路
12.6	Таѕк6 实现思路
12.7	Таѕк7 实现思路



1 LAB 拓扑环境和设备登录信息

1.1 Lab 内容简介

本次lab所有内容为远程操作,涉及配置Aruba MM、Controller、ClearPass产品,给初步接触Aruba ClearPass产品的SE熟悉ClearPass工作流程和基本操作。本次lab内容包括:创建一个简单的认证服务、Aruba 控制器集成ClearPass实现Mac认证、Portal认证、802.1X认证、Mac + Portal无感知认证、访客自注册认证、Tacacs+认证、ClearPass Insight操作、ClearPass认证基本问题诊断以及ClearPass集群操作。

通过本次lab的练习,你应该能对ClearPass工作原理有所了解,并且能够熟悉并独立完成Aruba控制器集成 ClearPass实现常用的几种无线认证。掌握ClearPass认证基本问题的故障排查方法。

本次lab主要以ClearPass的配置为主,但同时涉及到Aruba Controller的配置,因此你应该对Aruba Controller OS8的配置有一定的了解。

1.2 Lab 设备及拓扑

- ♦ 6台Mobility Master (每组1台MM)
- ♦ 12台Mobility Controller (每组2台MC)
- ♦ 6套ClearPass (每组1套CPPM)
- ♦ 6套Airwave (每组1套AMP)
- ♦ 6台Switch (每组1台接入交换机)
- ♦ 6颗Access Point (每组1颗AP)
- ◆ 6台无线客户端 (每组1台无线客户端)
- ◆ 6台有线客户端 (每组1台有线客户端)
- ♦ Console 服务器一套 (共用)





1.3 Lab 设备 VLAN 和 IP 信息

·····································									
Device	VLAN	IP	Mask	Default GTW					
MM-1	X50	10.X.50.11	255.255.255.0	10.X.50.250					
MM-2	X50	N/A	N/A	N/A					
MD-1	X10	10.X.10.11	255.255.255.0	10.X.10.250					
MD-2	X10	10.X.10.12	255.255.255.0	10.X.10.250					
MD-VRRP	X50	10.X.10.10	255.255.255.0	10.X.10.250					
MD1-COA	X50	10.X.10.21	255.255.255.0	10.X.10.250					
MD2-COA	X50	10.X.10.22	255.255.255.0	10.X.10.250					
Wireless User	X20								
Wired User 1	X21								
Wired User 2	X22								
ClearPass	X50	10.X.50.41	255.255.255.0	10.X.50.250					
Wired Client		10.X.50.101	255.255.255.0						
Wireless Client		10.X.50.102	255.255.255.0						

a Hewlett Packard Enterprise company

1.4 Lab 设备登录账号和密码

Device	Method	IP Address	Account	Password
Console Server	https	10.0.50.50	访客账号	访客密码
8320-3	telnet	10.0.50.50:10833	访客账号	访客密码
8320-4	telnet	10.0.50.50:10834	访客账号	访客密码
5406-1	telnet	10.0.50.50:10541	admin	aruba123
5406-2	telnet	10.0.50.50:10542	admin	aruba123
ClearDess	https	10 \ 50 41	admin	aruba123
ClearPass	ssh	10.X.50.41	appadmin	aruba123
A : J A /	https	10 1 50 20	admin	admin
Airwave	ssh	10.X.50.30	ampadmin	ArubaSELab
MM-1	https/ssh	10.X.50.11	admin	aruba123
MM-2 (NA)	https/ssh	10.X.50.12		
7010-1	telnet	10.0.50.50:20X01	admin	aruba123
7010-2	telnet	10.0.50.50:20X02	admin	aruba123
2930F	telnet	10.0.50.50:20X03	manager	aruba123
Wired Client	RDP	10.X.50.101	lab	Aruba123!
Wireless Client	RDP	10.X.50.102	lab	Aruba123!



2 TASK1: 创建一个最简单的认证服务

2.1 用户需求

配置ClearPass认证服务:只要通过aaa test测试通过即可

2.2 实现思路

答案详见附录

✓ ClearPass如何处理一个radius认证请求?

答案: ______

- ✓ 你需要了解的几个问题:
 - MM1的IP地址: _____
 - CPPM的IP地址: _____
 - Radius共享密码:
 - MD测试radius命令是什么:______

✓ 配置步骤

- 配置无线控制器:
 - ◆ 初始化MD1和MD2
 - ◆ 配置Cluster
 - ◆ 配置Radius服务器指向CPPM (10.X.50.41)
- 配置ClearPass: 配置一条认证服务用于aaa test

2.3 ClearPass 配置

2.3.1 登录 ClearPass

第1步: 登录 到ClearPass的WebUI: https://10.X.50.41 (X: 1…6)

- ✓ 1、ClearPass Policy Manager: 策略管理模块
- ✓ 2、ClearPass Guest: 访客模块
- ✓ 3、ClearPass Onboard: Onboard 模块
- ✓ 4、ClearPass Insight: Insight 模块



aruba	
	ClearPass
	AAA/Policy Management Onboarding Guest Device Security Health Health Exchange
	ClearPass Policy Manager 1 Rele-based Policies, Enterprise-grade AAA with Device Profiling 比容智道
	ClearPass Onboard 3 设备配置 3

第2步: 点击ClearPass Policy Manager链接, 进入策略管理模块页面

也可以通过https://10.X.50.41/tips (X: 1…6),直接跳转到此页面,输入用户名、密码,点击"登录"

- ✓ 用户名: admin
- ✓ 密码: aruba

aruba	ClearPass Policy Manage
	Admin Login
	用户名:
	密码: 音录

2.3.2 添加网络设备

第1步:找到 配置 - > 网络 - > 设备,点击右侧 "添加设备"按钮,添加控制器,如下图所示:

aruba		ClearPass Po	licy Manager		Menu 🗮
ि हे क्र 0 ि इस 0 स्र 0 स्र 0	配置 » 网络 » 设备 网络设备				 ● 添加设备 全,导入设备 全,导入设备 全,导出设备
- ↓ mx2+141 - ↓ m85 - ↓ ↓ - ↓ ↓ ↓ - ↓ ↓ ↓ - ↓ ↓ ↓ - ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	A Network Access Device (NAD) must belong 过滤器: 名称	to the global list of devices i	in the ClearPass database in ord	er to connect to ClearPass.	 ➡ Discovered Devices 显示 20 € 记录
● 套 國助時行 ● 4	# ■ <u>~</u> 19) A		12 晚于两地址	1469 3	Copy 导出 翻除

在弹出的对话框中输入以下参数,并点击"保存"

- ✓ 名称: LabX-MDs (X:1…6)
- ✓ IP: 10.X.10.0/24 (X:1…6)
- ✓ RADIUS 共享密钥: aruba123
- ✓ TACACS+共享密码: aruba123

添加设备						8
设备 SNMP 读取设置	SNMP 写入设置	CLI 设置	OnConnect Enf	orcemer	nt 属性	
名称:	Lab1-MDs					
IP 或子网地址:	10.1.10.0/24		(例如,192	.168.1.1	10 或 192.168.1.1/24)	
说明:				*		
RADIUS 共享密钥:	•••••			认证:	••••••	
TACACS+ 共享密钥:				认证:	••••••	
供应商名称:	Aruba		•			
启用 RADIUS CoA:	🗹 RADIUS CoA	端口: 3799				
Enable RadSec:						
					Add	Cancel

2.3.3 添加服务器参数

第1步: 找到 管理 - > 服务器管理器 - > 服务器配置, 点击右侧 服务器 "LabX-CPPM-1" (X: 1…6)

aruba		ClearPass P	olicy Manager				Menu 🗮
■ ● 面板 0	管理 » 服务器管理器 » 服务器配置						
 □ 监视 ● ● ● ● ■ ● 	服务器配置					 ④ 设置日期和时间 ● 更改集群密码 ● 管理策略管理器区 	
2 管理 •						NetEvents 目标	the strength of the
 —						* Clear Machine Au * Virtual IP Setting を主成 Subscriber	s
→	Publisher 服务器: Lab1-CPPM-1 [10.1.	50.41]				〒 未存+4X701019 2X	
→ 本地共享文件夹	# 服务器名▲	管理端口	数据端口	×	Insight	集群同步	上次同步时间
<i>🍌</i> 许可	1. Lab1-CPPM-1	10.1.50.41	-	default	Enabled	Enabled	-
	显示最后项的前一-后一				收集日志 备份	恢复 Cleanup	关闭重新引导

第2步:在弹出的窗口中,点击"服务参数"选项卡,

 ✓ 选择服务: "Radius server"下的, Log Accounting Interim-Update Packets 参数选择"TRUE",并点击 "保存"



管理 » 服务器管理器 » 服务器配置 - Lab1-CPPM-1							
服务器配置 - Lab1-CPPM-1 (10.1.50.41)							
系统 服务控制 服务参数 系统监视 网络接口 FIPS							
选择服务: Radius server 🔶							
参数名	参数值	默认值	允许的值				
EAP-FAST							
Master Key Expire Time	1 weeks \$	1 weeks					
Master Key Grace Time	3 weeks \$	3 weeks	3 weeks				
PACs are valid across cluster	TRUE	TRUE					
Proxy							
Maximum Response Delay	5 seconds	5	1-5				
Maximum Reactivation Time	120 seconds	120	60-3600				
Maximum Retry Counts	5 retries	5	2-10				
Accounting							
Log Accounting Interim-Update Packets	TRUE 🔶	FALSE					
Thread Pool							
Maximum Number of Threads	20 threads	20	10-300				
Number of Initial Threads	10 threads	10	5-300				

2.3.4 添加本地账号和角色

第1步:找到 配置 - > 身份 - > 角色 ,点击右上角的"添加角色"按钮,增加一个角色:

ClearPass Po				icy Manager	Menu 🗮
■ ■ 面板	配置 » 身份	份 » 角色			
医遊視・	角色				▲ 添加角色
					▲ 导出角色
一章 此处开始 一章 服务	Roles exis	ist independently of an individual ser	rvice and can be accessed glo	pally through the role-mapping policy of any service.	
	过滤器: 名	名称 🕴 包含 🕯	+	Go Clear Filter	显示 1000 🛟 记录
□ Q 身份 Single Sign-On (SSQ)	#	□ 名称 ▼		说明	
—————————————————————————————————————	1.	[TACACS Super Admin]		Super administrator role for Policy Manager Admin	
— 🖧 端点	2.	[TACACS Receptionist]		Receptionist role for Policy Manager Admin	
	3.	[TACACS Read-only Admin]		Read-only administrator role for Policy Manager Admin	
	4.	[TACACS Network Admin]		Network administrator role for Policy Manager Admin	
一口 角色映射	5	ITACACE Hale Deck1		Help deck role for Balicy Manager Admin	

在弹出的添加角色窗口中输入下面参数, 点击 "save":

- ✓ 名称: test-role
- ✓ 说明:赋予测试的访问权限

添加新角色	•
名称:	test-role
说明:	赋予测试的访问权限 ()
	Save Cancel

第2步: 找到 配置 - > 身份 - >本地用户,点击右上角的"添加用户"按钮,增加一个用户账号



aruba		ClearPass Policy Manager		Menu 🗮
E■ 面板 0	配置 » 身份 » 本地用户			
E型 単税 ● ● ● ●	本地用户			 → 添加用户 ▲ 导入用户 ▲ 导入用户 ▲ 导出用户
	ClearPass Policy Manager lists all local users in the	Local Users page.		P Account Settings
□ 身份	过滤器: 用户 ID 🕴 包含 🗘	🛨 Go Clear Filter		显示 20 🛟 记录
- ○ Single Sign-On (SSO) - ○ 本地用户 - ○ 端点 - ○ 静态主机列表 - ○ 静态主机列表	# 1 户 ID 。	名称	角色	状态
→ □ 用日映射 ● 〒 安全状況 ● 書 强制执行 ● ◆ 网络				

在弹出的添加角色窗口中输入下面参数, 点击 "save":

- ✓ 用户ID: labX-test (X: 1…6) (即用户的登录账号)
- ✓ 名称: labX测试账号 (X: 1…6) (即该账号的别名,只是一个标签)
- ✓ 密码: aruba123 (即用户的登录账号)
- ✓ 认证密码: aruba123 (即重复输入一次登录密码)
- ✓ 启用用户: ☑ (勾选)
- ✓ 角色: test-role (该角色在第一步中创建的)

添加本地用户			۰
用户 ID:	lab1-test		
名称:	lab1测试账号		
密码:			
认证密码:			
启用用户:	☑ (选中可启用本地用户)	
更改密码:	Check to force characteristic	nge password on next TACA	CS+ login)
角色:	test-role	\$	
	II	性	
属性		值	
1. Click to add			
			添加取消

2.3.5 添加认证服务

第1步:找到配置 -> 服务,点击右侧 "添加服务"按钮添加一个服务:



 回 重板 (回 重視 20 重視 20 重視 20 重視 20 重視 20 重視 20 重視 	● 配置 » 例 ● 强制排 ● ClearPas	 RE ■ 强制执行 > 策略 Gall执行策略 ClearPass controls network access by evaluating an enforcement policy associated with the service. 					* *	添加强制执行策略 导入强制执行策略 导出强制执行策略
	过滤器:(#	名称	\$)[包含 \$) 名称 ▲	ŧ	Go Clear Filte 类型	rr 1988		显示 20 🛊 记录
中 安全状况	1.	0	[Admin Network Login Policy]		TACACS	Enforcement policy controlling access to Policy Manager Admin		
	2.		[AirGroup Enforcement Policy]		RADIUS	Enforcement policy controlling access for AirGroup devices		
心 配置文件	3.		[Aruba Device Access Policy]		TACACS	Enforcement policy controlling access to Aruba device		
∃ ➡ 网络	4.		[Guest Operator Logins]		Application	Enforcement policy controlling access to Guest application		
Profile and Network Scan	5.		[Insight Operator Logins]		Application	Enforcement policy controlling access to Insight application		
一 禄 束 眙 15 具	6.		[Sample Allow Access Policy]		RADIUS	Sample policy to allow network access		
	7.		[Sample Deny Access Policy]		RADIUS	Sample policy to deny network access		
	显示最后	项的前-	后-				复制	

在"服务"选项卡中配置如下参数:

- ✓ 类型: RADIUS Enforcement (Generic)
- ✓ 名称: task1-test-service

配置 » 服务 » 添加							
服务							
服务认证角色强制	期执行 概要						
类型:	RADIUS Enforcement (Generic)						
名称:	task1-test-service						
说明:							
监视模式:	□ 启用以监视无强制执行的网络访问						
更多选项:	□ 授权 □ 安全状况遵从 □ 审计终端主机 □ 配置文件端点 □ Accounting Proxy						
服务规则							
匹配项 🔿 任意或 💿 以下所有条件:							
类型	名称						
1. Click to add							

在"认证"选项卡中配置如下参数:

- ✓ 1、认证方法: [PAP]、 [MSCHAP]
- ✓ 2、认证源: [Local User Repository][Local SQL DB]

配置 » 服务 » 添加			
服务			
服务 认证 角色 强制	执行 概要		
认证方法:	[PAP] [MSCHAP]	Move Up ↑ Move Down ↓ Remove View Details Modify	添加新认证方法
N L MPNEE .	Select to Add]	
IV IF 38:	[Local User Repository] [Local SQL DB]	Move Up ↑ Move Down ↓ Remove View Details Modify	漆加新心证源
	Select to Add	•	
剥离用户名规则:	🗆 启用以指定以逗号分隔的规则列表,用于剥离	离用户名前缀或后缀	
Service Certificate:	Select to Add 🛟)	View Certificate Details



在"角色"选项卡中,暂时不做任何配置(详细内容可以参考高级介绍部分):

✓ 角色映射策略:空

配置 » 服务 » 添加			
服务			
服务认证 角色 强制	制执行 概要		
角色映射策略:	Select	Modify	添加新角色映射策略
		角色映射策略详细信息	
说明:	-		
默认角色:	-		
规则评估算法:	-		
条件		角色	

第2步: 点击"强制执行"选项卡, 配置"强制执行", 选择强制执行策略, 如下图所示, 并点击"保存"

配置 » 服务 » 添加		
服务		
服务认证角色强	期待 概要	
使用缓存的结果:	□ 使用从上一会话中缓存的角色和安全状况属性	
强制执行策略:	[Sample Allow Access Policy]	添加新强制执行策略
	强制执行策略详细信息	
说明:	Sample policy to allow network access	
默认配置文件:	[Allow Access Profile]	
规则评估算法:	evaluate-all	
条件		强制执行配置文件
1. (Date:Day-of-Wee Sunday)	BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday,	[Allow Access Profile]

2.4 控制器配置

使用 SSH 方式登录到 Mobility Master (10.X.10.11) 第1步:在 Mobility Master (MM)上进入 /md/labX 配置路径 (X: 1……6)

(Lab1-MM-1) [mynode] #cd /md/lab1

(Lab1-MM-1) [lab1] #

第2步: 进入配置模式

(Lab1-MM-1) [lab1] #configure terminal

Enter Configuration commands, one per line. End with CNTL/Z

(Lab1-MM-1) [lab1] (config) #

第3步: 增加一个新的 radius 认证服务器 "cppm"

(Lab1-MM-1) [lab1] (config) #aaa authentication-server radius cppm

(Lab1-MM-1) ^[lab1] (RADIUS Server "cppm") #host 10.1.50.41

(Lab1-MM-1) ^[lab1] (RADIUS Server "cppm") #key aruba123



第4步:保存配置

(Lab1-MM-1) ^[mm] (config) #write memory

Saving Configuration...

Configuration Saved.

2.5 验证结果

第1步: 登录到 MD1, 使用 aaa test 命令测试
(Lab1-MM-1) [lab1] (config) #logon 10.1.10.11
(LAB1-MD1) [MDC] #aaa test-server pap cppm lab1-test aruba123
Authentication Successful

第2步:登录到 CPPM 查看认证记录:

监视 » Liv	e Monitoring » 访问题	眼器						
访问跟	访问跟踪器 Oct 09, 2019 14:22:15 CST 📀 自动刷新							
The Acces	s Tracker page prov	ides a real-time display of per-s	ession access activity on the sele	ected server or domain.				
TAII	[] [All Requests] [] Lab1-CPPM-1 (10.1.50.41) [] Last 1 day before Today [] [] Lab1							
过滤器: F	lequest ID	\$ 包含 \$	🕂 🛛 Go 🗌 Clear Filte	3		显示 20 🔶 记录		
#	Server	Source	Username	Service	Login Status	Request Timestamp 🔹		
1.	10.1.50.41	RADIUS	lab1-test	task1-test-service	ACCEPT	2019/10/09 14:21:57		
NOTI	如果 aaa test 结果是 "Authentication failed"可能是什么问题? (1、用户名或密码错误。2、没有匹配到 service) 如果 aaa test 结果是 "AAA server timeout"可能是什么问题? (1、radius 服务器网络不可达。2、radius 共享密钥不匹配)							



3 TASK2: ARUBA 控制器集成 CPPM 实现 MAC 认证

3.1 用户需求

用户希望针对无线覆盖区域内的一批IOT设备实现基于mac地址的访问接入控制,并且给予特定的访问权限

3.2 实现思路

答案详见附录

✓ MAC认证时,我们并没有手动输入用户名和密码,那他的用户名和密码是什么?

答案:_____

✓ ClearPass如何匹配一个MAC认证请求:

答案:

✓ ClearPass可以用哪个认证源来做MAC认证

答案: ______

- ✓ 配置步骤
 - 配置CPPM认证服务:配置一个MAC认证服务
 - 无线控制器配置:
 - ◆ 配置一个SSID: labX-mac,并启用MAC认证,
 - ◆ 认证服务器指向CPPM IP:10.X.50.41, (X: 1…6)
 - ◆ 认证成功后通过ClearPass返回role: authenticated

3.3 ClearPass 配置

3.3.1 添加本地账号

第1步: 找到 配置 - > 身份 - >端点 , 点击右上角的"添加端点"按钮 , 增加一个用户账号

aruba			ClearPas	s Policy Manager			Menu 📕
■ ■ 面板 ● ■ 面板	配置》身份》端。	ġ.					➡ 添加端点
	端只						 ▲ 导入端点 ▲ 导出所有端点
	This page auton etc.).	natically lists all auth	enticated endpoints. An endp	oint device is an Internet-capable hardwa	are device on a TCP/IP netwo	rk (e.g. laptops, smart phor	nes, tablets,
□ ♀ 身份	过滤器: MAC 地址	£ \$	包含 \$	Go Clear Filter			显示 20 🛊 记录
— O Single Sign-On (SSO)	# •	MAC 地址 ▲	主机名	类别	OS 系列	状态	已分析
	1.	000c29c4a049	Lab1-CPPM-1	Server	ClearPass	Unknown	Yes
	显示最后项的前一	-后-		认证记录 Bulk Up	date Bulk Delete Triş	gger Server Action Upda	te Fingerprint)

在弹出的添加角色窗口中输入下面参数, 点击 "save":

- ✓ MAC地址: 7c7a914652b7
- ✓ 状态:选择"已知客户端"

添加端点	
	7-7-0440501-7
MAC 地址	/c/a914652b/
1元1月:	
状态	● 已知客户端 ○ 未知客户端 ○ 已禁用客户端
	属性
属性	值
1. Click to add	



添加完成后,状态如下:

aruba			ClearPas	s Policy Manager			Menu 🗮
■ ■版	配置 » 身 端点 This pag etc.).	予份 » 端点 ge automatically lists all a	uthenticated endpoints. An endp	pint device is an Internet-capable hardwar	e device on a TCP/IP ne	twork (e.g. laptops, smart phones,	 ➡ 添加端点 ▲ 导入端点 ▲ 导出所有端点 tablets,
□ ♀ 身份	过滤器:	MAC 地址	♦ 包含 ♦	Go Clear Filter			显示 20 🛊 记录
- ② Single Sign-On (SSO)	#	■ MAC 地址 ▲	主机名	类别	OS 系列	状态	已分析
	1.	000c29c4a049	Lab1-CPPM-1	Server	ClearPass	Unknown	Yes
→ 静态主机列表	2.	7c7a914652b7				Known	No
	显示最后	项的前一-后一		认证记录 Bulk Upda	te Bulk Delete	Trigger Server Action Update F	ingerprint 导出 删除

3.3.2 添加认证服务

第1步: 找到 配置 - > 强制执行 - > 配置文件 , 点击右侧的 "添加强制执行配置文件"按钮 , 增加一



个**强制执行配置文件**:

aruba			ClearPass	Polic	cy Manager	Menu 🗮
三 山 面板	● 配置 » 引	量制执行	i » 配置文件			
国際	 强制拐 	丸行面	出置文件			· 添加强制执行配置文件
2 RH	0					▲ 导入强制执行配置文件 全 导出强制执行配置文件
- 🛟 此处开始 - 🙄 服务	Each en	forcen	nent policy contains enforcement profiles that match o	condition	s (role, posture, and	time) to actions (enforcement profiles).
回 🗣 认证	过滤器:	名称	◆ 包含 ◆	+	Go Clear Filter	显示 1000 😜 记录
	#		名称 ▲	\$	类型	说明
□ ♀ 身份	1.	0	[Aerohive - Terminate Session]	F	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)
- 🛱 Single Sign-On (SSO)	2.	0	[AirGroup Personal Device]	F	RADIUS	System-defined profile for an AirGroup personal device request
一心 本地用户	3.	0	[AirGroup Response]	F	RADIUS	System-defined profile for any AirGroup request
一章 端点	4.	0	[AirGroup Shared Device]	F	RADIUS	System-defined profile for an AirGroup shared device request
一心 静态主机列表	5.	0	[Allow Access Profile]	F	RADIUS	System-defined profile to allow network access
一 4 用巴	6.	0	[Allow Application Access Profile]	ŀ	Application	System-defined profile to allow access to application
→ 中安全状况	7.	0	[ArubaOS Switching - Bounce Switch Port]	F	RADIUS_CoA	System-defined profile to bounce the switch port on ArubaOS Switching products.
■ 書 强制执行	8.	0	[ArubaOS Switching - Terminate Session]	F	RADIUS_CoA	System-defined profile to disconnect the user on ArubaOS Switching, HP ProCurve and HP UWW products.
一章 配置文件	9.	0	[ArubaOS Wireless - Bounce Switch Port]	F	RADIUS_CoA	System-defined profile to bounce the switch port on ArubaOS Mobility Controllers, Multi-Port APs & Mobility Access Switches.
→ 一 网络 → Profile and Network Scan	10.	0	[ArubaOS Wireless - TACACS Read-Only Access]	1	ACACS	System-defined profile for TACACS read-only access on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches.
一心 策略仿真	11.	0	[ArubaOS Wireless - TACACS Root Access]	1	ACACS	System-defined profile for TACACS root access on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches.

在"配置文件"选项卡中输入下面参数:

✓ 模板: Aruba Radius 强制执行

✓ 名称: task2-mac-profile

配置 » 强制执行 » 配置文件 »	Add Enforcement Profile
强制执行配置文件	
配置文件 属性 概要	
模板:	Aruba RADIUS 强制执行 🗘
名称:	task2-mac-profile
说明:	
类型:	RADIUS
操作:	 ● 接受 ○ 拒绝 ○ 删除
设备组列表:	Remove 添加新设备组 View Details Modify

在"属性"选项卡中输入下面参数:

✓ 属性: Radius:Aruba Aruba-User-Role authenticated

配置 » 强制执行 » 配置文件 » Add Enforcement Profile							
强制执行配置文件							
配置文件 属性 概要							
	夕秒		Jai				
	白柳						
1. Radius:Aruba	ㅋゕ Aruba-User-Role	=	authenticated	Đ	Ť		

在"概要"选项卡中对配置进行总览:

✓ 概要: 点击"保存"



配置 » 强制执行 » 配置文件 »	Add Enforcement Profile		
强制执行配置文件			
配置文件 属性 概要			
配置文件:			
模板:	Aruba RADIUS 强制执行		
名称:	task2-mac-profile		
说明:			
类型:	RADIUS		
操作:	Accept		
设备组列表:	-		
属性:			
类型	名称		值
1. Radius:Aruba	Aruba-User-Role	=	authenticated

第2步: 找到 配置 - > 强制执行 - > 策略 , 点击右侧的 "添加强制执行策略"按钮 , 增加一个强制执行策略:

■■ 面板 図 = 面板 回 監視 ² 2 配置	● ^{配置 »} ● 强制打	^{虽制执行} 丸行第	ī» 策略 5 88				*	添加强制 导入强制	执行策略 执行策略
- 章 此处开始 - 章 服务	ClearPa	ss cont	trols network access by evaluating an enforcement poli	cy ass	ociated with the se	rvice.		守山独制	执行束略
	过滤器:	名称	\$ 包含 \$	+	Go Clear Filter			显示 20	+ 记录
□ 〒 安全状况	#		名称 ▲		类型	说明			
■ 靠强制执行	1.	0	[Admin Network Login Policy]		TACACS	Enforcement policy controlling access to Policy Manager Admin			
	2.	0	[AirGroup Enforcement Policy]		RADIUS	Enforcement policy controlling access for AirGroup devices			
心 配置文件	3.	0	[Aruba Device Access Policy]		TACACS	Enforcement policy controlling access to Aruba device			
□ + 网络	4.	0	[Guest Operator Logins]		Application	Enforcement policy controlling access to Guest application			
Profile and Network Scan	5.	0	[Insight Operator Logins]		Application	Enforcement policy controlling access to Insight application			
一章 策略仿具	6.	0	[Sample Allow Access Policy]		RADIUS	Sample policy to allow network access			
	7.	0	[Sample Deny Access Policy]		RADIUS	Sample policy to deny network access			
	显示最后	项的前	后-				复制	导出	删除

在"强制执行"选项卡中输入下面参数:

- ✓ 名称: task2-mac-enforcement-policy
- ✓ 默认配置文件: [Deny Access Profile]

配置 » 强制执行 » 策略 » 添加	1	
强制执行策略		
强制执行 规则 概要		
名称:	task2-mac-enforcement-policy	
说明:	0	
强制执行类型:	● RADIUS ○ TACACS+ ○ WEBAUTH (SN	MP/Agent/CLI/CoA) 〇 应用程序 〇 Event
默认配置文件:	[Deny Access Profile] View Details	Modify 添加新强制执行配置文件

在"规则"选项卡中点击"Add Rule":

- ✓ 在规则编辑器中配置一条规则如下图所示,并点击"保存"
 - 条件: Tips Role EQUALs [User Authenticated]
 - 配置文件名: task2-mac-profile (在第1步中创建的配置文件)



配置 »	强制	执行 » 策略 » 添加	1					
强制	执行	f策略						
强制技	执行	规则概要						
规则评	估算法	± :	● 选择第一个匹配 ○ 选择所有匹配					
Enforo	emen	t Policy Rules:						
с	Condit	tions			Actions			
					Add Rule	Move Up ↑ Move Down ↓	Edit Rule Rem	nove Rule
	规则编	辑器					•	
				条件				
	匹配	以下所有条件:						
		类型	名称		运算符	值		
	1.	Tips	Role	EQUALS		[User Authenticated]	Ba 🕆	
	2.	Click to add						
				强制执行配置文件	ŧ			
	配置	文件名:	[RADIUS] task2-mac-profile	Move Up ↑ Move Down ↓ Remove				
			Select to Add				保存取消	

在"概要"选项卡中对配置进行总览:

✓ 概要:查看配置总览,并点击"保存"

配置 » 强制执行 » 策略 » 添加 强制执行策略	ba
	Enforcement policy has not been saved
强制执行规则概要	
强制执行:	
名称:	task2-mac-enforcement-policy
说明:	
强制执行类型:	RADIUS
默认配置文件:	[Deny Access Profile]
规则:	
规则评估算法:	First applicable
Conditions	Actions
1. (Tips:Role EQUALS [User Authenticated]) [RADIUS] task2-mac-profile



第3步: 找到 配置 - > 服务 , 点击右侧的 "添加服务" 按钮 , 增加一个服务 :

□ 重数 0 □ 広我 0 ○ 記録 0 ○ 記録 0	配置» 服务	服务 ge sho	ws the curre	int list and order of services that ClearPass fo	llows during authentication and authorization.			 添加服务 亭入服务 亭入服务 亭出服务
	过滤器: #	名称	順序 ▲	 ◆ 包含 ◆ 名称 	+ Go Clear Filter 类型	模板	显: 状	示 1000 🛊 记录
 □ 套 强制执行 	1.		1	[Policy Manager Admin Network Login Serv	ice] TACACS	TACACS+ Enforcement	(D
- 🖧 策略	2.	0	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	(9
	3.	0	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	(9
● • • 网络	4.		4	[Guest Operator Logins]	Application	Aruba Application Authentication	(2
Profile and Network Scan A 等較在有	5.		5	[Insight Operator Logins]	Application	Aruba Application Authentication	(9
₩ 東昭辺具	6.		6	task1-test-service	RADIUS	RADIUS Enforcement (Generic)	(D
	显示最后	与项的前	—-后一				重新排序 复制	

在"服务"选项卡中配置如下参数:

- ✓ 类型选择: 忽略MAC认证
- ✓ 名称填写: task2-mac-service
- ✓ 服务规则中添加:
 - Radius:Aruba Aruba-Essid-Name EQUALS labX-mac (X: 1……6)

配置	記里》服务》添加						
服务	务						
服务	服务 认证 角色 强制执行 概要						
类型:	型: 忽略 MAC 认证 🗘						
名称:		task2-mac-service					
说明:		基于 MAC 的认证服务	G				
监视模式:							
更多边	先项:	□ 授权 □ 审计终端主机 □ 配置文件	端点 🗌 Accounting Proxy				
			1	服务规则			
匹配功	页 🔵 任意或 💿 以下所有	有条件:					
	类型	名称		运算符	值		
1.	Radius:IETF	NAS-Port-	-Туре	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)	₿ <u>₿</u>	Ť
2.	Radius:IETF	Service-T	уре	BELONGS_TO	Login-User (1), Call-Check (10)	Ē	Ť
3.	Connection	Client-Ma	c-Address	EQUALS	%{Radius:IETF:User-Name}	Ē	Ť
4.	Radius:Aruba	Aruba-Ess	sid-Name	EQUALS	lab1-mac	ĒÐ	Ť
5.	Click to add						

在"认证"选项卡中配置如下参数:

- ✓ 1、认证方法: [MAC AUTH]
- ✓ 2、认证源: [Endpoint Repository][Local SQL DB]



五栗 、 四水 、 沃 林			
ബ 重 » 服 穷 » 渝 加			
服务			
服务认证角色强制	执行 概要		
认证方法:	[MAC AUTH]	Move Up↑ 添加新认i	正方法
		Move Down ↓	
		Remove	
		View Details	
		Modify	
	Select to Add 💠	•	
认证源:	[Endpoints Repository] [Local SQL DB]	Move Up ↑ 添加新订	人证源
		Move Down ↓	
		Remove	
		View Details	
		Modify	
	Select to Add	•	
剥离用户名规则:	🗆 启用以指定以逗号分隔的规则列表,用于剥离	」离用户名前缀或后缀	

在"角色"选项卡中,暂时不做任何配置(详细内容可以参考高级介绍部分):

✓ 角色映射策略:空

配置 » 服务 » 添加			
服务			
服务认证 角色 强制	利执行 概要		
角色映射策略:	Select	Modify	添加新角色映射策略
		角色映射策略详细信息	
说明:	-		
默认角色:	-		
规则评估算法:	-		
条件		角色	

在"强制执行"选项卡中,配置如下参数:

✓ 强制执行策略: task2-mac-enforcement-policy(即前面步骤中创建的强制执行策略)

配置 » 服务 » 添加						
服务						
服务认证角色强制	期 一概要					
使用缓存的结果:	□ 使用从上一会话中缓存的角色和安全状况属性					
强制执行策略:	task2-mac-enforcement-policy	添加新强制执行策略				
	强制执行策略详细信息					
说明:						
默认配置文件:	[Deny Access Profile]					
规则评估算法:	first-applicable					
条件		强制执行配置文件				
1. (Tips:Role EQUALS	[User Authenticated])	task2-mac-profile				



在"概要"选项卡中对配置进行总览,并点击保存:

配置 »	配置 » 服务 » 添加						
服务	ī						
	Service has not been saved						
012 Az	80.47 21.37 da.da. 300 millio (C. 100 millio)						
服务	1入1业 用巴 强调	明执行 做要					
服务:							
类型:		忽略 MAC 认证					
名称:		task2-mac-service					
说明:		基于 MAC 的认证服务					
监视模	[式:	Disabled					
更多选	项:	-					
			服务规则	1			
匹配以	下所有条件:						
	类型	名称		运算符	值		
1.	Radius:IETF	NAS-F	Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)		
2.	Radius:IETF	Servic	се-Туре	BELONGS_TO	Login-User (1), Call-Check (10)		
3.	Connection	Client	-Mac-Address	EQUALS	%{Radius:IETF:User-Name}		
4.	Radius:Aruba	Aruba	a-Essid-Name	EQUALS	lab1-mac		
认证:	认证:						
认证方法: [MAC AUTH]							
认证源	认证源: [Endpoints Repository] [Local SQL DB]		QL DB]				
剥离用户名规则: -							
角色:							
角色映射策略: -							
强制执	行:						
使用缓	存的结果:	Disabled					
强制执	行策略:	task2-mac-enforcement-policy					

3.4 控制器配置

3.4.1 开启 PEF 功能

第1步: 使用 SSH 方式登录到 Mobility Master (10.X.10.11), 在 Mobility Master (MM) 上进入 /mm 配置路 径 (X: 1·····6)

(Lab1-MM-1) [mynode] #cd /mm

(Lab1-MM-1) [mm] #

第2步:进入配置模式

(Lab-1-MM-1) [mm] #configure terminal

Enter Configuration commands, one per line. End with CNTL/Z

(Lab-1-MM-1) [mm] (config) #

第3步: 开启 PEF 功能

(Lab-1-MM-1) [mm] (config) #license-pool-profile-root

(Lab-1-MM-1) ^[mm] (License root(/) pool profile) #pefng-licenses-enable

Please ensure to add licenses before enabling feature bit.



(Lab-1-MM-1) ^[mm] (License root(/) pool profile) #!

(Lab-1-MM-1) ^[mm] (config) #

(Lab-1-MM-1) ^[mm] (config) #write memory

Saving Configuration...

Configuration Saved.

第4步: 查看开启 PEF 功能结果

(Lab-5-MM-1) [mm] (config) #show license-pool-profile-root

License root(/) pool profile

-----Parameter Value
----enable PEFNG feature Enabled

enable RFP feature Disabled

enable ACR feature Disabled

enable WebCC feature Disabled

3.4.2 关闭 CPSec

第1步: 使用Web 方式登录到Mobility Master (10.X.10.11), 找到Managed Networks - > labX -> Configuration -> System (X:1……6)

✓ 关闭 Enable CPSec

Managed Network > lab1	1>		
	General Admin AirWave CPSec C	Certificates SNMP Logging Profiles More	
	 Control Plane Security 		
Roles & Policies	Enable CPSec:		
Access Points			
AP Groups			
Authentication			
Tasks			
Maintenance			



3.4.3 添加 AP-Group

第2步: 使用Web 方式登录到Mobility Master (10.X.10.11), 找到Managed Networks - > labX -> Configuration -> AP Groups (X:1……6),点击 "+" 创建一个新的 "AP Group"

ALAPTOR MOBILITY MASTI Lab1-MM-1	ER	CONTROLLERS ACCESS POINTS ◎ 2 ○ 0 ◎ 1 ○ 0	CLIENTS ALERTS	⑦ admin ✓
Managed Network > lab11 >				(¢)
€ ,	Dashboard	AP Groups 3		
🔁 Mobility Master	Configuration	NAME	APs	=
📼 Lab1-MM-1	WLANs	default	1	
🔁 Managed Network (2)	Roles & Policies	NoAuthApGroup	84	
🗁 lab11 (1)	Access Points	lab1-group	-	
🖾 lab11-md1	AP Groups			
🗀 lab12 (1)	Authentication	<u>+</u>		
	Services			
	Interfaces			
	Controllers			
	System			
	Tasks			
	Maintenance			
	Wantenance			
	ArubaMM-VA, 8.4.0.0			

第3步: 在弹出的窗口的输入以下参数, 并点击 "Submit" 提交配置

✓ Name : labX-group (X : 1…6)

N	ew AP Gro	up				
	Name:	lab1-group				
				Cancel	Submit	
				Cancel	Submit	

第4步: 配置保存并同步给md设备

- ✓ 1、Pending Changes: 点击该按钮 (右上角提示)
- ✓ 2、Deploy changes: 点击该按钮



ALADIA MOBILITY MASTE Lab1-MM-1	ER	CONTROLLERS	ACCESS POINTS	CLIENTS 〒 0 ₱ 0	ALERTS	? admin ~
← Managed Network > lab11 >						Pending Changes 🗘
€ <mark>,</mark> Q	Dashboard	AP Groups 4				
🔁 Mobility Master	Configuration	NAME		APs		=
📼 Lab1-MM-1	WLANs	default		1		
🔁 Managed Network (2)	Roles & Policies	NoAuthApGroup				
🔁 lab11 (1)	Access Points	lab1-group				
📼 lab11-md1	AP Groups	lab11-group				
🗀 lab12 (1)	Authentication	+				
	Services					
	Interfaces					
	Controllers					
	System					
	Tasks					
	Maintenance					
	ArubaMM-VA, 8.4.0.0					
Pending Changes						
Rending Chang	tos for 2 Controllors					
	ses for 2 controllers					
🗹 🕂 Managed	Network > lab1 (2 Cont	rollers)				
				lose	Discard changes	Deploy changes

3.4.4 添加无线信号

第1步: 使用 Web 方式登录到 Mobility Master (10.X.10.11), 找到 Managed Networks - > labX -> Configuration -> WLANs (X : 1 ····6), 点击 "+"进入创建一个新的无线配置向导 配置一个 SSID: labX-mac (X : 1 • • • • • 6)

Managed Network > lab1 >		
€ , Q	Dashboard	WLANs 1
🗀 Mobility Master	Configuration	NAME (SSID)
🗁 Managed Network (2)	WLANs	
🗁 lab1 (2)	Roles & Policies	
📼 lab1-md1	Access Points	
📼 lab1-md2	AP Groups	
	Authentication	+
	Services	

第2步:在 "General" 选项卡中配置如下参数

- ✓ Name (ssid): labX-mac (X : 1…6)
- ✓ Primary usage: Employee
- ✓ Broadcast on: lab1-group
- ✓ Forwarding mode: Tunnel

Gene	ral	VLANs	Security	Acces
Name (ssid):	lab1-mac			
Primary usage:	● Employee	st		
	Select AP Groups 💙			
Broadcast on:	default lab1-group 			
Forwarding mode:	Tunnel 🗸			

第3步:在"VLANs"选项卡中,点击"Show VLAN details",进入 VLAN 配置向导

NOTE 在向导中,此时由于还没有为该无线用户创建好 VLAN ID x20,所以在 VLAN 下拉列表中是无法选择 VLAN X20 的,因此我们需要新增该 VLAN ID X20。

New WLAN

•			
General	VLĀNs	Security	Access
VLAN: 1 💙			
Show VLAN details			

第4步: 点击下面的"+",增加一个无线业务 VLAN, 配置参数如下, 点击"OK":

- ✓ VLAN name: wireless-user-vlan
- ✓ VLAN ID/Range: X20 (X: 1…6)

	New VLAN	
New WLAN	VLAN name: wireless-user-vlan VLAN ID/Range: 120	
VLAN: 1 V Hide VLAN details		
NAME NAME	ID(S)	
-	1	

第5步:将 VLAN 的参数选择为 "wireless-user-vlan" (既上一步中创建的 vlan name):

✓ VLAN: wireless-user-vlan

New WLAN			
General	VLANS	Security	Access
VLAN: wireless-user-vlan			
第6步:在"Security"选项卡中	中配置如下参数		

- ✓ Key Management: open
- ✓ MAC authentication: Enable

New WLAN

General		VLANs	Secur	ity	Access
More Secure	Key management: MAC authentication:	Open 🗸]		
Enterprise	L		1		
Personal					
Open					
Less Secure					

第7步:在 "Access" 选项卡中配置如下参数并点击 "Finish"

✓ Mac authentication role: guest (测试阶段注意观察一下通过 mac 认证的终端实际获取到的 role?)

New WLAN

Genera	I	VLANS	Security	Access
Default role:	logon	~		
Mac authentication role:	guest	~		
Show roles				

3.4.5 添加认证和计费服务器

第1步: 找到 Managed Networks - > labX -> Configuration -> Authentication->Auth Servers (X:

- 1 ……6) ,点击"+"
- ✓ 在弹出的选项卡中输入 "labX-mac_svg" (X:1…6)

Aruba MOBILITY MAST	ER		CONTROLLERS	ACCESS POINTS	CLIENTS ALER	TS 0		③ admin ↔
← Managed Network > lab1 >		Add Server	Group					Pending Changes $ \diamondsuit $
Mobility Master Managed Network (2)	Dashboard Configuration WLANs	Name:	lab1-mac_svg]	Cancel Submit	tion User Rules	Advanced	
 lab1-md1 lab1-md2 	Roles & Policies Access Points AP Groups Authentication Services Interfaces		internal	1		LOAD BALANCE	SERVER RULES	

第2步: 点击新建的 Server Group: "lab1-mac_svg",点击下方的"+"添加 radius server,在弹出的选项 卡中选中"cppm",并点击"**Submit**"

aruba	MOBILITY MASTER lab1-mm-1	CONTROLLERSACCESS POINTSCLIENTSALERIImage: Original controlImage: Original c	rs 0	admin ~
Managed Networ	k > lab1 >	New Server for lab1-mac_svg		Pending Changes $ \phi $
Dashboard Configuration	Auth Servers AAA Profiles	Add existing server Add new server		
WLANS Roles & Policies Access Points AP Groups Authentication	Server Groups 4 NAME default internal lab1-peap_doc1_svg	cppm Internal	SERVER RULES	
Services Interfaces Controllers	+ Server Group > lab1-mac_sy	Cancel Submit		 Drag rows to re-order
System Tasks Maintenance	NAME +	TYPE IP ADDRESS TRIM FQDN	MATCH RULES	

第3步: 找到 Managed Networks - > labX -> Configuration -> Authentication -> AAA Profile (X: 1 ·····6), 找到 labX-mac_aaa_prof (X: 1 ·····6):

	BILITY MASTI ab1-mm-1	ER	CONTROLLERS ACCESS POINTS CLIENTS ALERTS ∅ 2 0 ∅ 1 0 〒 1 ∅ 0 △ 0	
← Managed Network > I	lab1 >			
€ _k	۹	Dashboard	Auth Servers ΔΔΔ Profiles 1.2 Authentication 1.3 Authentication	Liser Rules Advanced
🚞 Mobility Master		Configuration		Auvanceu
合 Managed Network (2)		WLANs	AAA Profiles	
🗁 lab1 (2)		Roles & Policies		
📼 lab1-md1		Access Points	One State Sta	
📼 lab1-md2		AP Groups	⊕ ☐ default	
		Authentication	⊕ G default-dot1x	
		Services	 → G default-dot1x-psk 	
		Interfaces		
		Controllere	⊕ ☐ default-mac-auth	
		Controllers	default-open	
		System		
		Tasks		
		Maintenance		
	L AUT MASTER IIM-1	entication Server ($\begin{array}{c c c c c c c c c c c c c c c c c c c $	9)、开 只击
Managed Network > lab1 >	•			Pending Changes $ column{0}{\rm Q} $
Dashboard	Auth S	ervers AAA Profiles L2 Authenticati	n L3 Authentication User Rules Advanced	
Configuration				
WLANs	AAA	A Profiles	Server Group: lab1-mac_svg	
Roles & Policies		④	Server Group: lab1-mac_svg 🗸	
AP Groups		default-mac-auth	Fail Through:	
Authentication		default-tuppeled-use	Load Balance:	
Services		G default-xml-api		
Interfaces				
Controllers		802.1X Authentication		
System		802.1X Authentication Server Group		
Tasks		MAC Authentication		
Maintenance		MAC Authentication Server Group		

✓ 修改"Radius Accounting Server Group"为"labX-mac_svg"(X:1・・・・6), 并点击"Submit"

Managed Network > lab1 >			Ŷ
Dashboard	Auth Servers AAA Profiles 12 Authentication	3 Authentication Liser Rules Advanced	
Configuration			
WLANs	AAA Profiles	Server Group: lab1-mac_svg	
Roles & Policies			
Access Points	🕀 🖻 default-xml-api	server Group: Tab I-mac_svg	
AP Groups		Fail Through:	
Authentication	⊕ ☐ lab1-mac-caching_aaa	Load Balance:	
Services	⊖ 🕒 lab1-mac_aaa_prof		
Interfaces	802.1X Authentication		
Controllers	802.1X Authentication Server Group		
System	MAC Authentication		
Tasks	MAC Authentication Server Group		
Maintenance	🕞 RADIUS Accounting Server Group		
	🕞 RFC 3576 server		
	XML API server		
第4步:点击右上角	"Pending Changes"保存	字配置	
Orubo Mobility Master Iab1-mm-1	CONTROLL © 2	ERS ACCESS POINTS CLIENTS ALERTS ① ○ ○ 1 ○ 0 0 △ 0 △ ○<	admin 🗸
Managed Network > lab1 >		Pendi	ng Changes 🗘

3.5 验证结果

第1步:远程桌面到10.X.50.102 (X:1…6),搜索无线信号SSID: labX-mac(X:1…6),点击连接

第2步: SSH登录到MM: 10.X.10.50 (X: 1…6), 查看当前用户所在MD

(lab1-md1) [M This operation	IDC] #show user on can take a while	depending on	number of users	. Please be	patien	t				
Users										
IP me User Type	MAC	Name	Role	Age(d:h:m)	Auth	VPN link	AP name	Roaming	Essid/Bssid/Phy	Profile
10.1.20.102 WIRELESS	7c:7a:91:46:52:b7	7c7a914652b7	authenticated	00:00:00	MAC		94:b4:0f:c1:3f:e0	Wireless	lab1-mac/94:b4:0f:93:fe:14/a-VHT	lab1-mac_aaa_prof

思考 在控制器配置第 5 步,配置的 Mac authentication role 是 guest,为什么测试结果是: authenticated?

第3步: 登录到CPPM, 找到 监控 - > Live Monitoring - > 访问跟踪器查看认证记录。

✓ 此时我们看到用户mac认证成功



aruba			ClearPa	ss Policy Manager	r		Menu 🗮
 ■ 面板 ● ■ 些 ● 	^{监视»U} 访问距	ive Monitoring » 访 艮踪器 Oct 15, 20	问跟踪器 19 17:21:08 CST				⊘ 自动刷新
■ Live Monitoring ●	The Acc	ess Tracker page p	rovides a real-time display of per-ses	ssion access activity on the sele	cted server or domain.	efore Today	編報
系统监视 ☞	过滤器:〔 #	Request ID Server	\$〕包含 € Source	🛨 Go Clear Filter Username	Service	Login Status	显示 20 🛟 记录 Request Timestamp +
	1. 2.	10.1.50.41 10.1.50.41	RADIUS RADIUS	7c7a914652b7 7c7a914652b7	task2-mac-service task2-mac-service	ACCEPT REJECT	2019/10/15 17:20:49 2019/10/15 17:19:29

✓ 点击认证成功的记录,在"概要"选项卡中查看信息,如下图:

请求详细信息	
概要 输入 输出 计	十费
会话标识符:	R0000021-01-5da58f71
日期和时间:	Oct 15, 2019 17:20:49 CST
终端主机标识符:	7C7A914652B7 (SmartDevice / Android / Android)
用户名:	7c7a914652b7
访问设备 IP/端口:	10.1.10.21:0
系统安全状况状态:	UNKNOWN (100)
	所用策略 -
服务:	task2-mac-service
认证方法:	MAC-AUTH
认证源:	Local:localhost
授权源:	[Endpoints Repository]
角色:	[User Authenticated]
强制执行配置文件:	task2-mac-profile
服务监视模式:	Disabled
Online Status:	📀 Online
I < Showing 1 of 1-14 re	cords ▶ ▶ 更改状态 Show Configuration 导出 显示日志 关闭

✓ 点击"输入"选项卡中查看认证请求信息,如下图:



概要 输入 输出	计费		
用户名:	7c7a914652	267	
冬端主机标识符:	7C7A91465	2B7 (SmartDevice / Android / Android)	
访问设备 IP/端口:	10.1.10.21:	0	
RADIUS 请求			
Radius:Aruba:Aruba	-AP-Group	lab1-group	
Radius:Aruba:Aruba	-Essid-Name	lab1-mac	
Radius:Aruba:Aruba-Location-Id		94:b4:0f:c1:3f:e0	
Radius:IETF:Called-	Station-Id	000B869AAF37	
Radius:IETF:Calling-	-Station-Id	7C7A914652B7	
Radius:IETF:NAS-IP	-Address	10.1.10.21	
Radius:IETF:NAS-Po	ort	0	
Radius:IETF:NAS-Po	ort-Type	19	
Radius:IETF:Service	-Type	10	
Radius:IETF:User-Na	ame	7c7a914652b7	

✓ 在"输出"选项卡中查看ClearPass返回给控制器的radius属性,如下图:

请求详细信息	
概要 输入 输出 计费	
强制执行配置文件:	task2-mac-profile
系统安全状况状态:	UNKNOWN (100)
审计安全状况状态:	UNKNOWN (100)
RADIUS 响应	\odot
Radius:Aruba:Aruba-User-I	Role authenticated

✓ 在"计费"选项卡中查看计费相关信息,如下图:



请求详细信息	
概要 输入	输出 计费
客户会话 ID:	7c7a91467C7A914652B7-5DA5FE98-B9FF0
开始时间戳:	Oct 15, 2019 17:20:49 CST
结束时间戳:	Still Active
状态:	Active
终止原因:	-
服务类型:	-
认证会话数:	1
网络详细信息	0
NAS IP 地址:	10.1.10.21:0
NAS 端口类型:	Wireless-802.11
呼叫站 ID:	7C7A914652B7
所呼叫站 ID:	000B869AAF37
分帧 IP 地址:	10.1.20.102
Framed IPv6	ddress: -
帐户认证:	
Showing 1	f 1-14 records ▶ ▶ 更改状态 Show Configuration 导出 显示日志 关闭


4 TASK3: ARUBA 控制器集成 CPPM 实现 PORTAL 认证

4.1 用户需求

客户希望针对无线用户实现WEB认证的方式接入无线,并给用户授予用户特定的访问权限。Web认证页面需要 外置并能够客户定制化。

4.2 实现思路

答案详见附录

✓ ClearPass的WEB认证登录页面是如何将用户名和密码送到Aruba控制器的。

答案: ____

✓ ClearPass如何匹配一个Portal认证请求:

答案: ____

- ✓ 配置步骤:
 - ClearPass配置
 - ◆ 配置portal认证登录页面
 - ◆ 配置一个Portal认证服务
 - 无线控制器:
 - ◆ 配置一个SSID:**labX-portal**,并启用Portal认证,
 - ◆ 认证服务器指向CPPM_IP:10.X.50.41,
 - ◆ Portal认证前role: labX-portal-guest-logon,成功后获得role: labX-guest (X: 1…6)

ClearPass web 登录页面默认使用的 http post action url 是: http://securelogin.arubanetworks.com/cgi-

NOTE bin/login,此 API 同时支持 Aruba 控制和 IAP,另外 Aruba 控制还支持另一个 http post API: http://securelogin.arubanetworks.com/auth/index.html/u



4.3 ClearPass 配置

4.3.1 取消内置的 HTTP 到 HTTPS 的跳转

在访客管理页面中,找到配置->身份验证,将安全设置项取消(因为默认ClearPass的内置页面的HTTP访问请求,都会被自动跳转到HTTPs上,为了避免证书告警提示问题,我们取消内部的HTTP到HTTPs的自动跳转)

aruba	ClearPass Guest	Menu
💐 #22 🔰	◎ 主页 » 配置 » 身份验证	
Onboard C	◎ 身份验证	
▲ 配置	Use this page to modify authentication settings for ClearPass Guest.	
→ 📢 广告	Authentication Settings	
 · · · · · · · · · · · · · · ·	助志授収: 送送一个新开/重新授収的信息到NAS 全局新开时自动效送通用/角色成合约改变。	
 ■ ■ ● ●	NAS类型: Aruba Networks (RFC 3576 support) * 通照网络能入影务器的就认类型。	
● 页面	RFC-3576 Bind Address: 102.50.41 Force a specific bind address for RFC-3576 requests. This may be needed in an AirGroup environment.	
	* Internal Auth Type: Controls the RADIUS authentication type used for internal RADIUS authentication requests.	
— 順 表単 — III List Views	安全: ◎ 为客人要求HTTPS访问 安全: 如果勾测此现,由客人划起的HTTP均同律求持续转到使用HTTPS来代替,	
— 🌸 自助注册 — 🕵 Web 登录		
- <u>2</u> 网页		
→ 从这里开始 - 1 数字凭证模板	公 返回主页	
- 父 电子邮件回执		
₩ 2010,001%		
▶ № 短信服务		
	6	

4.3.2 添加本地账号和角色

第2步:找到配置 -> 身份 -> 角色,点击右上角的"添加角色"按钮,增加一个角色:

aruba			ClearPass	cy Manager	Menu 🗮	
	配置»∮	∲份 » 角	1色			
☑ 监视 ○	角色					🚽 添加角色 😫 导入角色
🖧 Rêlît 🔍 🔍						👱 导出角色
一尊 此处开始	Roles ex	list ind	lependently of an individual service and can be access	ed glob	ally through the role-mapping policy of any service.	
- 尊服务						
	过滤器:	名称	\$ 包含 \$	+	Go Clear Filter	显示 1000 🛊 记录
□ 呈 身份 □ ☆ Single Sign-On (SSO)	#		名称 ▼		说明	
	1.		[TACACS Super Admin]		Super administrator role for Policy Manager Admin	
- 🖧 端点	2.		[TACACS Receptionist]		Receptionist role for Policy Manager Admin	
→ 静态主机列表	3.		[TACACS Read-only Admin]		Read-only administrator role for Policy Manager Admin	
一章 角色	4.		[TACACS Network Admin]		Network administrator role for Policy Manager Admin	
- 森 角色映射	5.		[TACACS Help Desk]		Help desk role for Policy Manager Admin	
● ① 女主状パ	6.		[TACACS API Admin]		API administrator role for Policy Manager Admin	
□ 4 August 1	7.		[Other]		Default role for another user or device	
Profile and Network Scan	8.		[Onboard Windows]		Role for a Windows device being provisioned	
一心 策略仿真	9.		[Onboard Mac OS X]		Role for a Mac OS X device being provisioned	

在弹出的添加角色窗口中输入下面参数, 点击 "save" :

- ✓ 名称: guest-role
- ✓ 说明:赋予访客的访问权限



添加新角色		8
名称:	guest-role	
说明:	赋予访客的访问权限 ⑤	
	Save	incel

第3步: 找到 配置 - > 身份 - >本地用户,点击右上角的"添加用户"按钮,增加一个用户账号

aruba	Cle	ClearPass Policy Manager								
■ 面板 O	配置 » 身份 » 本地用户									
🕑 监视 🛛 🛛 🛛	本地用户			→ 添加用户						
20 RE 📀				 シーマスカード 全、号出用户 						
一尊 此处开始										
	ClearPass Policy Manager lists all local users in the Loca	al Users page.								
□ ♀ ♀ 分	(対線路・田白 ID ▲ 句令 ▲	Go Clear Filter		显示 1000 🛊 记录						
_☆ Single Sign-On (SSO) _☆ 本地用户	# 用户ID▲	名称	角色	大态 Seebled						
	1. add-test	IdD1测证,赋亏	[Other]	Enabled						
一項 静念王机列表 一造 角角	显示最后项的前一-后一			「「「」」 「「」」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「						
▲ 角色映射										
→ 🖶 安全状况										
■ 臺强制执行										
 ● ● Profile and Network Scan ● ↓ 策略仿真 										

在弹出的添加角色窗口中输入下面参数, 点击 "save":

- ✓ 用户ID: guest (即用户的登录账号)
- ✓ 名称: guest-test (即该账号的别名,只是一个标签)
- ✓ 密码: aruba123 (即用户的登录账号)
- ✓ 认证密码: aruba123 (即重复输入一次登录密码)
- ✓ 启用用户: ☑ (勾选)
- ✓ 角色: guest-role (该角色在第一步中创建的)



泰加本地用户		
用户 ID:	guest	
名称:	guest-test	
密码:		
认证密码:		
启用用户:	☑ (选中可启用本地用户)	
更改密码:	Check to force change	e password on next TACACS+ login)
角色:	guest-role	•
	属性	E
属性		值
1. Click to add		

添加	取消

4.3.3 添加 portal 登录页面

- 第1步: 登录到ClearPass Guest管理页面: https://10.X.50.41/guest/guest_index.php (X: 1----6)
- 第2步: 找到Configuration » Pages » Web Logins,点击右侧的 "Create a new web login page" 按钮,新 增一个访客登录页面:

aruba		ClearPas	s Guest							
💱 Guest 🛛 0	Home » Configuration » Pages » Web Log	jins								
📳 Onboard 🛛 🛛	Web Logins						🚔 Create a new web login page			
🔨 Configuration 📀	Many NAS devices support Web-based a	thentication for visitors								
🛶 Start Here	Harry Wild devices support web-based at	internication for visitors.								
🖭 📢 Advertising	By defining a web login page on the Clea	By defining a web login page on the ClearPass Guest you are able to provide a customized graphical login page for visitors accessing the network through these NAS devices.								
- 🎭 Authentication	Use this list view to define new web login	Use this list view to define new web login pages, and to make changes to existing web login pages.								
🖃 🥶 Content Manager	Ophoard device provisioning pages a	are now managed from the Web I	onin tab within provi	isioning settings						
- 🕵 Guest Manager	- onboard device provisioning pages (ogin coo maini provi	Storing Sectings						
🗈 靲 Hotspot Manager	🛆 Name	Page Title	Page Name	Page Skin						
E- 😫 Pages										
	There are no web login pages to display									
- Mi Fields	0 web logins (Reload		Sho	wall rows						
- m Forms				•	J					
List Views	🛞 Back to pages									
- Self-Registrations	Pack to configuration									
- A web Logins										
web Pages	🍪 Back to main									
E Receipts										
E Sms Services										

第3步: 在弹出的页面配置里配置访客登录页面的相关参数如下

- ✓ Name: guest-login (ClearPass中登录页面的名称)
- ✓ Page Name: guest-login (登录页面url: http:// 10.1.50.41/guest/guest-login.php)
- ✓ 安全登录:在下拉菜单中选中"通过HTTP发送明文密码"



	Web Login Editor
* 名字:	guest-login 键入网页登陆页面名称
页面名称:	guest-login 输入此Web登录页的名称. 该网站的登录将可从 "page_name.php"
描述:	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
*供应商设置:	Aruba Networks \$ 选择一个预定义组设置符合标准网络配置。
Login Method:	Controller-initiated — Guest browser performs HTTP form submit Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
* 地址:	securelogin.arubanetworks.com 在此输入供应商产品的IP地址或者主机名。
安全登录:	 通过HTTP发送明文密码 ◆ 为该网站登录过程选择一个安全选项为该网站登录过程.
Dynamic Address:	The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.

✓ Pre-Auth Check: None-no extra checks will be made

Login Form Options for specifying the behaviour and content of the login form. Credentials – Require a username and password \$ Select the authentication requirement. Access Code requires a single code (username) to be entered. Authentication: Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field set. Enable bypassing the Apple Captive Network Assistant Prevent CNA: The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented. Provide a custom login form Custom Form: If selected, you must supply your own HTML login form in the Header or Footer HTML areas. Override the default labels and error messages Custom Labels: If selected, you will be able to alter labels and error messages for the current login form. None — no extra checks will be made \$ * Pre-Auth Check: Select how the username and password should be checked before proceeding to the NAS authentication. Require a Terms and Conditions confirmation Terms: If checked, the user will be forced to accept a Terms and Conditions checkbox.

✓ 点击 "Save Changes" 按钮保配置

4.3.4 添加认证服务

第1步: 找到 配置 - > 强制执行 - > 配置文件 , 点击右侧的 "添加强制执行配置文件"按钮 , 增加一个强制执行 配置文件:

aruba		ClearPass Policy Manager					
■ 面板 ■ 面板 ■ 监視	配置 » ·	置 > 强制执行 > 配置文件 R 出 は / 石 P 等 で 化					
記量 一章 此处开始	Each ei	the neuronal sector contains enforcement profiles that match conditions (role, posture, and time) to actions (enforcement profiles).					
- ☆ 服务 - ♣ 认证 - ▲ 身份	过滤器:	名称	♦ 包含 <>)	÷	Go Clear Filte		显示 100 🛟 记录
🕞 🖶 安全状况	#	-	名称 🔺		类型	说明	
····································	1.		[Aeronive - Terminate Session]		RADIUS_COA	System-defined profile to disconnect user (Aeronive)	
	2.	0	[AirGroup Personal Device]		RADIUS	System-defined profile for an AirGroup personal device request	
- 章 配置文件	3.	0	[AirGroup Response]		RADIUS	System-defined profile for any AirGroup request	
	4.	0	[AirGroup Shared Device]		RADIUS	System-defined profile for an AirGroup shared device request	
Profile and Network Scan	5.	0	[Allow Access Profile]		RADIUS	System-defined profile to allow network access	
一种原始加州	6.	0	[Allow Application Access Profile]		Application	System-defined profile to allow access to application	

在"配置文件"选项卡中输入下面参数:

- ✓ 模板: Aruba Radius 强制执行
- ✓ 名称: task3-portal-profile

配置 » 强制执行 » 配置文件 »	Add Enforcement Profile
强制执行配置文件	
配置文件 属性 概要	
模板:	Aruba RADIUS 强制执行
名称:	task3-portal-profile
说明:	
类型:	RADIUS
操作:	● 接受 ○ 拒绝 ○ 删除
设备组列表:	Remove 添加新设备组 View Details Modify

在"属性"选项卡中输入下面参数:

✓ 属性: Radius:Aruba Aruba-User-Role lab1-guest

2置 » 强制执行 » 配置文件 » Add Enforcement Profile							
强制执行配置文件							
配置文件 属性 概要							
类型	名称		值				
1. Radius:Aruba	Aruba-User-Role	=	lab1-guest	Ē	Ť		
2 Cliels to add							

在"概要"选项卡中对配置进行总览:

✓ 概要:查看配置总览,并点击"保存"



配置 » 强制执行 » 配置文件 » Add Enforcement Profile 强制执行配置文件 Enforcement profile has not been saved 配置文件 属性 概要 配置文件: 模板: Aruba RADIUS 强制执行 名称: task3-portal-profile 说明: 类型: RADIUS 操作: Accept 设备组列表: 属性: 类型 名称 值 1. Radius:Aruba Aruba-User-Role lab1-guest

第2步: 找到 配置 - > 强制执行 - > 策略 , 点击右侧的 "添加强制执行策略" 按钮 , 增加一个强制执行策略:

aruba			(ClearPass Pol	icy Manager		Menu 🗮
5世 面板 	• 配置 »	强制执行	亍»策略				
医 监视	强制	执行贫	き略				🚽 添加强制执行策略
26 RH	2						会 导入强制执行策略 会 导出强制执行策略
一章 此处开始	ClearP	ass cor	trols network access by evaluating ar	n enforcement policy ass	sociated with the serv	vice.	
— 〇 服务							
	过滤器	: 名称	\$ 句念 \$	+	Go Clear Filter		显示 1000 记录
	#		名称 🖌		类型		
★ ① 安主状況	1.		[Admin Network Login Policy]		TACACS	Enforcement policy controlling access to Policy Manager Admin	
	2.	0	[AirGroup Enforcement Policy]		RADIUS	Enforcement policy controlling access for AirGroup devices	
心 配置文件	3.		[Aruba Device Access Policy]		TACACS	Enforcement policy controlling access to Aruba device	
● ➡ 网络	4.		[Guest Operator Logins]		Application	Enforcement policy controlling access to Guest application	
Profile and Network Scan	5.		[Insight Operator Logins]		Application	Enforcement policy controlling access to Insight application	
一發 東哈10具	6.	0	[Sample Allow Access Policy]		RADIUS	Sample policy to allow network access	
	7.		[Sample Deny Access Policy]		RADIUS	Sample policy to deny network access	
	显示最	后项的前	一-后一				复制导出删除

在"强制执行"选项卡中输入下面参数:

- ✓ 名称: task3-portal-enfocement-policy
- ✓ 默认配置文件: [Deny Access Profile]

配置 » 强制执行 » 策略 » 添加	1		
强制执行策略			
强制执行规则概要			
名称:	task3-portal-enfocement-policy		
说明:			
强制执行类型:	SADIUS ○ TACACS+ ○ WEBAUTH (SNM)	MP/Agent/CLI/CoA) 🔿 应用程序 🔵 Event	
默认配置文件:	[Deny Access Profile] View Details	Modify	添加新强制执行配置文件

在"规则"选项卡中输入下面参数:

- ✓ Conditions: 点击 "Add Rule ", 配置如下,
 - 条件: Tips Role MATCHES_ALL guest-role & [User Authenticated]
 - 配置文件名: task3-portal-profile (在第1步中创建的配置文件)



配置 » 强制	山执行 »	策略 » 添力	0						
强制执行	行策 暗	\$							
强制执行	规则	概要							
规则评估算	法:		 选择第一个匹配 〇 选择所有匹配 						
Enforceme	ent Poli	cy Rules:							
Cond	litions				Actions				
						Add Rule Move Up ↑	Move Down ↓	Edit Rule	Remove Rule
	规则编	串器							•
					条件				- 84
	匹配以	「下所有条件	:						
		类型	名和	R	运算符	值			
	1.	Tips	Rol	e	MATCHES_ALL	guest-ro [User Au	le thenticated]		÷
	2.	Click to a	dd						
									_
				强制	則执行配置文件				
	配置;	文件名:	[RADIUS] task3-portal-profile	Move Up ↑					
				Remove					
			Select to Add	\$					
								保存工	(消)

在"概要"选项卡中对配置进行总览:

✓ 概要:查看配置总览,点击"保存"按钮

配置 » 强制执行 » 策略 » 添加 强制执行策略	配置 » 强制执行 » 策略 » 添加 品目 11 分子等 PS					
Enforcement policy has not been saved						
强制执行 规则 概要 强制执行:						
名称:	task3-portal-enfocement-policy					
说明:						
强制执行类型:	RADIUS					
默认配置文件:	[Deny Access Profile]					
规则:						
规则评估算法:	First applicable					
Conditions	Actions					
1. [User Authenticated])	ALL guest-role [RADIUS] task3-portal-profile					

第3步:找到配置 - > 服务,点击右侧的"添加服务"按钮,增加一个服务:

在"服务"选项卡中配置如下参数:

- ✓ 类型选择: RADIUS Enforcement (Generic)
- ✓ 名称填写: task3-portal-service
- ✓ 服务规则:
 - 1、Connect Client-Mac-Address NOT_EQUALS %{Radius:IETF:User-Name}
 - 2、Radius:Aruba Aruba-Essid-Name EQUALS labX-portal (X: 1……6)



配置»服务»添加 服务				
服务 认证 角色	强制执行 概要			
类型:	RADIUS Enforcement (Generic)			
名称:	task3-portal-service			
说明:	task3 portal认证服务			
监视模式:	□ 启用以监视无强制执行的网络访问			
更多选项:	□ 授权 □ 安全状况遵从 □ 审计终端主机 □ 配置文件端点	Accounting Proxy		
, 服务规则				
匹配项 🔵 任意或 💿 以下所有新	条件:			
类型	名称	运算符	值	Î
1. Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}	Ē t
2. Radius:Aruba	Aruba-Essid-Name	EQUALS	lab1-portal	B =
3. Click to add				

在"认证"选项卡中配置如下参数:

- ✓ 1、认证方法: [PAP] 、[CHAP]、 [MSCHAP]
- ✓ 2、认证源: [Local User Repository][Local SQL DB]

配置 » 服务 » 添加		
服务		
服务认证 角色 强制	执行 概要	
认证方法:	[PAP] [CHAP] [MSCHAP]	Move Up↑ 添加新认证方法 Move Down↓ Remove View Details Modify
	Select to Add	
认证源:	[Local User Repository] [Local SQL DB]	Move Up↑ Move Down↓ Remove View Details Modify
	Select to Add	
剥离用户名规则:	□ 启用以指定以逗号分隔的规则列表,用于剥离	第 用户名前缀或后缀
Service Certificate:	Select to Add	View Certificate Details

在"角色"选项卡中,暂时不做任何配置(详细内容可以参考高级介绍部分):

✓ 角色映射策略:空

配置 » 服务 » 添加			
服务			
服务认证 角色 强制	則执行 概要		
角色映射策略:	Select	Modify	添加新角色映射策
		角色映射策略详细信息	
说明:	-		
默认角色:	-		
规则评估算法:	-		
条件			角色

在"强制执行"选项卡中,配置如下参数:

✓ 强制执行策略: task3-mac-enforcement-policy (即前面步骤中创建的强制执行策略)



配置 » 服务 » 添加				
服务				
服务认证角色强	則执行 概要			
使用缓存的结果:	□ 使用从上一会话中缓存的角色和安全状况属性			
强制执行策略:	task3-portal-enfocement-policy Modify	添加新强制执行策略		
	强制执行策略详细信息			
说明:				
默认配置文件:	[Deny Access Profile]			
规则评估算法:	first-applicable			
条件 强制执行配置文件				
1. (Tips:Role MATCH [User Authenticated]	ES_ALL guest-role	task3-portal-profile		

在"概要"选项卡中对配置进行总览:

✓ 概要:查看配置总览,点击"保存"按钮

配置»服务»添加				
服务				
		Service has not been sa	ved	
服务 计证 角色	深刻执行 掷页			
服务:				
类型:	RADIUS Enforcement (Generic)			
名称:	task3-portal-service			
说明:	task3 portal认证服务			
监视模式:	Disabled			
更多选项:	-			
		服务规则		
匹配以下所有条件:				
类型	名称	运算符		值
1. Connection	Client-Mac-	Address NOT_EC	UALS	%{Radius:IETF:User-Name}
2. Radius:Aruba	Aruba-Essid	-Name EQUALS	í	lab1-portal
认证:				
认证方法:	1. [PAP] 2. [CHAP] 3. [MSCHAP]			
认证源:	[Local User Repository] [Local SQL DE]		
剥离用户名规则:	-			
Service Certificate:	-			
角色:				
角色映射策略:	-			
强制执行:				
使用缓存的结果:	Disabled			
强制执行策略:	task3-portal-enfocement-policy			



4.4 控制器配置

4.4.1 添加无线信号

第1步: 使用 Web 方式登录到 Mobility Master (10.X.10.11), 找到 Managed Networks - > labX -> Configuration -> WLANs (X : 1 ·····6), 点击 "+"进入创建一个新的无线配置向导

Managed Network > lab1 >		
€ <mark>,</mark> Q	Dashboard	WLANs 1
🗎 Mobility Master	Configuration	NAME (SSID)
🗁 Managed Network (2)	WLANs	
🗁 lab1 (2)	Roles & Policies	
📼 lab1-md1	Access Points	
📼 lab1-md2	AP Groups	
	Authentication	
	Services	
 第2步:配置 SSID 名称、主要用途、在 ✓ Name (ssid): labX-portal (X ✓ Primary usage: Guest ✓ Broadcast on: lab1-group ✓ Forwarding mode: Tunnel 	哪个 AP-Group 广播、转发模式 : 16)	
-		

New WLAN

Gene	ral	VLANs	Security	Access
Name (ssid): Primary usage:	lab1-portal	lest		
Broadcast on:	Select AP Groups V default lab1-group			
Forwarding mode:	Tunnel 🗸			

第3步: 配置 VLAN



✓ VLAN: wireless-user-vlan

New WLAN General VLANs Security Access VLAN: wireless-user-vlan ~ Hide VLAN details 第4步: 配置 portal 认证方式

- - ✓ Auth servers: cppm
 - ✓ CPPM host: 10.X.50.41 (X: 1…6)
 - ✓ CPPM page: /guest/guest-login.php (在4.3.3第3步中创建的页面)

New WLAN

General	VLANs		Security	Access
ClearPass or other external captive portal — Internal captive portal with authentication Internal captive portal with email registration Internal captive portal, no auth or registration	Captive Porta	cppm		
No Captive Portal	CPPM host: CPPM page: Redirect URL:	10.1.50.41 /guest/guest-login.pl		

第5步:完成向导配置







4.4.2 修改 portal 认证配置

找到Managed Network - > labX -> Configuration -> Authentication -> L3 Authentication 点击 "Captive Portal Authentication",选中 "labX-portal_cppm_prof" (X:1……6),修改如下参数

- ✓ Use HTTP for authentication: 启用
- ✓ Login page: http://10.X.50.41/guest/guest-login.php (X:1…6) (https 修改为 http)

Managed Netw	rk >			
	Auth Servers AAA Profiles L2 Authentication L	3 Authentication User Rules Advanced		
	L3 Authentication	Captive Portal Authentication Profile: lab1-port	al_cppm_prof	
Roles & Policies	⊖ 🖻 Captive Portal Authentication	Default Role:	guest 🗸	
Access Points	④	Default Guest Role:	guest v	
AP Groups	ා 🕞 🕞 lab1-portal_cppm_pro 💼	beladie odese kole.	guest	
	G Server Group	Redirect Pause:	10 sec	
	⊕ ☐ Stateful Kerberos Authentication	User Login:		
		Guest Login:		
	⊕	Logout popup window:		
		Use HTTP for authentication:		
	↔ 🕒 VIA Web Authentication	Logon wait minimum wait:	5 sec	
	OP VPN Authentication	Logon wait maximum wait:	10 sec	
	⊕ 🕒 WISPr Authentication	logon wait CPU utilization threshold:	60 %	
		Max Authentication failures:	0	
		Show FODN:		
		Authentication Protocol		
		Addienteddon riotocol.		
		Login page:	http://10.1.50.41/gue	
		Welcome page:	/auth/welcome.html	

4.4.3 添加 Portal 重定向

找到 Managed Network - > labX (X: 1 ·····6) -> Configuration -> Services -> Firewall 点击 "Global Settings", 找到 Allow tri-session with DNAT 并勾选。(强烈推荐采用该方法设置)

			•••			
ALCONO MOBILITY MASTE Iab1-mm-1	ER	CONTROLLERSACCESS☉2①0○1	CLIENTS CLIENTS ○ 0 〒 1 0	ALERTS		admin ~
Managed Network > lab1 >						(¢)
€ <mark>,</mark>	Dashboard	Clusters Redundancy AirGroup VPN	Firewall IP Mobility	External Services D	HCP WAN	
🔁 Mobility Master	Configuration					
🖾 lab1-mm-1	WLANs	 Global Settings 				i i
Managed Network (2)	Roles & Policies		IPV4	1	PV6	
🔁 lab1 (2)	Access Points	Monitor ping attack:	per 30 sec		per 30 sec	
🖾 lab1-md1	AP Groups	Monitor TCP SYN attack rate:	per 30 sec		per 30 sec	
lab1-md2	Authentication	Monitor IP sessions attack:	per 30 sec		per 30 sec	
	Services	Monitor/police non-gratuitous ARP attacks:	0			
	Interfaces	Monitor/police gratuitous ARP attack rate:	50 per 30 sec			
	Controllers	Monitor/police gratuitous ARP attack action:	Drop 👻			
	System	Monitor/police CP attack rate:	per 30 sec			
	Maintenance	Deny inter user bridging:				
	maintenance	Deny inter user traffic:				
		Deny source routing:				
		Deny all IP fragments:				
		Enforce TCP handshake before allowing data:				
		Prohibit IP spoofing:				
		Prohibit RST replay attack:				
		Log all received ICMP errors:				
		 Allow tri-session with DNAT: 				•
						Cancel Submit
	M-VA, 8.4.0.0					

或者找到 Managed Network - > labX (X : 1 ····6) -> labX-md1 /labX-md2 (X : 1 ····6) -> Configuration -> Interface -> VLANs, 点击 "wireless-user-vlan -> VLAN ID 120" 给控制器无线用户 VLAN: X20 (X : 1 ····6) 配置三层接口 IPv4 地址, 保证无线用户能够正常弹出 Portal 页面。

ALCODO MOBILITY MAST Iab1-mm-1	TER	$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	(?) admin ~
Managed Network > lab1 > lab	1-md1		Ŷ
€ <mark>k</mark> Q	Dashboard	Ports VIANS IP Routes IPv6 Neighbors GRF Tunnels Pool Management OSPF Multicast	
🔁 Mobility Master	Configuration	in Koutes in Volkeignbors Cite formen agement. Corr inditidast	
🖘 lab1-mm-1	WLANs	NAME ID/S	_
🔁 Managed Network (2)	Roles & Policies	wireless-user-vlan 120 0	
🔁 lab1 (2)	Access Points	- 1,110	
🖾 lab1-md1	AP Groups		
lab1-md2	Authentication		
	Services	+	
	Interfaces	VLANs > wireless-user-vlan VLAN IDs Options	
	Controller	ID IPV4 ADDRESS IPV6 ADDRESS ENABLE NAT PORT MEMBERS ADMIN STATE OPERATIONAL S	PD CLIENT DHCP SETTINGS
	System	120	Disabled None 🔟
	Tasks		
	Maintenance		
		+	
		Port Members IPv4 IPv6 More	
		V IP Address Assignment	
		IP assignment: Static 💙	
		IP address:	
	M-VA 8.4.0.0		Cancel Submit

NOTE 需要对集群中的每台 md 分别进行配置,不同的 md 接口 IP 地址不同。

4.4.4 添加角色

第1步: 找到 Managed Networks - > labX -> Roles & Policies 点击右侧的 "+" 按钮, 新增一个 role:

labX-guest (X: 1....6) 。

	ILITY MASTER b1-mm-1			CONTROLLERS ACCESS POIN ○ 2 ○ 0 ○ 1 ○	NTS CLIENTS ALER	0	admin ~
Managed Network > Ia	ab1 >		New Role				Pending Changes 🤇
Dashboard Configuration	R	oles Policies Applicat	Name:	lab1-guest			
WLANs		Roles 16					
Roles & Policies		NAME			Cancel		
Access Points		default-iap-user-role		2 Rules			
AP Groups		default-via-role		3 Rules			
Authentication		default-vpn-role		4 Rules			
Services		authenticated		4 Rules			
Interfaces		voice		41 Rules			
Controllors		leader-role		1 Rules			
Controllers		lah1-norral-guest-logon		78 Pules			
System		+		20 Hule3			
Tasks	[Ŧ					

选中新建的role "labX-guest",点击下方的 "+" 给这个role增加一个 "allowall" 的policy



Managed Network > lab1 >	N	ew Policy			Pending Changes 🗘
Dashboard Configuration	Roles Policies Applicatio	Add an existing polic	Create a new policy		
WLANs	Roles 17	Policy type:	Session 💙		
Roles & Policies	NAME	Policy name:	· · · · · · · · · · · · · · · · · · ·		
Access Points	default-via-role	allowall	•		
AP Groups	default-vpn-role	Position:			
Authentication	authenticated		_		
Services	voice leader-role		Car 1 Rules	incel Submit	
Interfaces	employee-role		1 Rules		
Controllers	lab1-portal-guest-logon		28 Rules		
System	lab1-guest		0 Rules		
Tasks	+				
Maintenance	lab1-guest olicies Ban	width Captive Portal	More		Show Basic View
	NAME	RULES COUNT	TYPE	POLICY USAGE	
	global-sacl	0	session	logon, guest, ap-role, stateful-dot1x, guest	
	apprf-lab1-griest-sacl	0	session	lab1-guest	
	lab1-gues	0	session	lab 1-guest	

4.4.5 添加计费

第1步: 找到 Managed Networks - > labX -> Authentication, 在右侧的 "AAA Profile" 列表中找到 "lab1-portal_aaa_prof"

Aruba Mobility Masti lab1-mm-1	ER	CONTROLLERS ACCESS POINTS CLIENTS ALERTS ∅ 2 0 ∅ 1 0 № 0 ▲ 1	⑦ admin ✓
Managed Network > lab1 >			Pending Changes 🗘
 Managed Network > Iab1 > Mobility Master Managed Network (2) Iab1(2) Iab1-md1 Iab1-md2 	Dashboard Configuration WLANs Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers System Tasks	AAA Profiles L2 Authentication L3 Authentication User Rules Advanced AAA Profiles C T AAA C T NoAuthAAAProfile C T default C T default. C T default.dot1x C T default.dot1x.psk C T default.dot1x.psk C T default.ap-aaa-prof C T default.open C T default.tunneled.use C T defaul	renuing changes (φ
		 Iab1-mac_aaa_prof	

配置 "RADIUS Accounting Server Group"为 "labX-portal_dot1_svg" (X: 1…6)



Managed Network > lab1 >			Pending Changes 🗘
Dashboard	Auth Servers AAA Profiles 12 Authentication	13 Authentication User Rules Advanced	
Configuration			
WLANs	AAA Profiles	Server Group: lab1-portal_dot1_svg	
Roles & Policies	⊕ ☐ default-iap-aaa-prof		
Access Points	⊕	Server Group: lab1-portal_dot1_svg	
AP Groups	⊕	Fail Through:	
Authentication	④	Load Balance:	
Services	⊕		
Interfaces	Iab1-mac_aaa_prof		
Controllers	⊖ 📑 lab1-portal_aaa_prof		
System	802.1X Authentication		
Tasks	802.1X Authentication Server Group		
Maintenance	MAC Authentication		
	MAC Authentication Server Group		
	🖻 RADIUS Accounting Server Group		
	RFC 3576 server		
	XML API server		
第2步:点击右上角	"Pending Changes" 保存	配置	
ALDO ADDO ADDILITY MASTER Iab1-mm-1	CONTR © 2	OLLERS ACCESS POINTS CLIENTS ALERTS ○ 0 ○ 1 ○ 0 ○ 0 △ 0	⑦ admin ✓
Managed Network > lab1 >			Pending Changes 🗘

4.5 验证结果

第1步: 远程登录到 Wi-Fi 测试客户端 10.X.50.102, 连接到 SSID: labX-portal。(X: 1…6)

第2步: SSH登录到MD: 10.X.10.11/10.X.10.12 (X: 1…6),查看当前用户在MD上的Role。

(lab1-md1) [MDC] #show user This operation can take a while	depending	g on number of users. Plea	ise be patien	t	ell					
Users										
IP MAC	Name	Role	Age(d:h:m)		VPN link	AP name	Roaming		Forward mode	Host
Name User Type										-
10.1.20.102 7c:7a:91:46:52:b7 WIRELESS		lab1-portal-guest-logon	00:00:00					lab1-portal_aaa_prof		
User Entries: 1/1 Curr/Cum Alloc:1/171 Free:2/17	0 Dyn:3 Al									

第3步: 远程登录到 Wi-Fi 测试客户端 10.X.50.102(X: 1…6),打开浏览器,在弹出的录页面中输入账号、密码进行验证。

- ✓ 用户名: guest
- ✓ 密码: aruba123

aruba	ClearPass Guest
Please login to the network using your use	ername and password.
L a cin	
Lõgin	
Username:	
Password:	
Log In	

第4步:远程登录到无线控制器, (X: 1…6)

✓ 查看用户在 MD 上的状态: Name (用户名) 、Role (角色) 、Auth (认证方式)

(lab1-md1) [This operation	MDC] #show user on can take a while	e dependin	g on number o								
Users											
IP ype		Name	Role	Auth	VPN link	AP name	Roaming		Forward mode	Host Name	User T
10.1.20.102 SS		guest	lab1-guest	Web				lab1-portal_aaa_prof			WIRELE
User Entries Curr/Cum Al	: 1/1 loc:1/171 Free:2/1	70 Dyn:3 A	llocErr:0 Fre								

✓ 通过 show user mac <mac>命令查看用户 role 是如何获取的。

(lab1-md1) [MDC] #show user mac 7c:7a:91:46:52:b7 This operation can take a while depending on number of users. Please be patient
Name: guest, IP: 10.1.20.102, MAC: 7c:7a:91:46:52:b7, Age: 00:00:03 Role: lab1-guest (how: ROLE_DERIVATION_L3_ARUBA_VSA) ACL: 106/0 Authentication: Yes, status: successful, method: Web, protocol: PAP, server: cppm

第5步: 登录到 ClearPass, 找到 监控 - > Live Monitoring - > 访问跟踪器

✓ 看到认证成功记录

aruba		ClearPass Policy Manager Mer							
8월 面板 ●	监视 » L	ive Monitoring » រ៉	方问跟踪器				0		
😰 监视 📀	访问跟		019 16:57:56 CST				📀 自动刷新		
 Live Monitoring 参加銀線器 	The Acc	ess Tracker page	provides a real-time display of per-sess	ion access activity on the s	elected server or domain.				
2 计费 2 计费 2 OnGuard 活动 2 分析和趋势	T [A	ll Requests]	📑 Lab1-CPPM-1 (10.:	1.50.41)	15 Last 1 day bef	ore Today	編辑		
→ ■ 系統监视 ● → Profile and Network Scan	过滤器:	Service	♦ 包含 ♦ task3	🖶 Go Clear Fi	lter		显示 20 ¢ 记录		
→ 审计查看器	#	Server	Source	Username	Service	Login Status	Request Timestamp •		
— 🥔 事件查看器 — 🚇 数据过滤器 — 🖉 Blacklisted Users	1. 显示最后	10.1.50.41 项的前一-后一	RADIUS	guest	task3-portal-service	ACCEPT	2019/10/15 16:56:27		



请求详细信息	
概要 输入 输出 计	费
会话标识符:	R000001e-01-5da58bc6
日期和时间:	Oct 15, 2019 17:05:10 CST
终端主机标识符:	7C7A914652B7 (SmartDevice / Android / Android)
用户名:	guest
访问设备 IP/端口:	10.1.10.21:0
系统安全状况状态:	UNKNOWN (100)
	所用策略 -
服务:	task3-portal-service
认证方法:	PAP
认证源:	Local:localhost
授权源:	[Local User Repository]
角色:	[User Authenticated], guest-role
强制执行配置文件:	task3-portal-profile
服务监视模式:	Disabled
Online Status:	🛇 Online
I ◄ Showing 1 of 1-11 rec	zords ▶ ▶ 更改状态 Show Configuration 导出 显示日志 关闭

点击这条认证记录, 查看"概要"选项卡内容, 观察, 可以看到哪些信息 \checkmark

点击"输入"选项卡内容,观察,可以看到哪些 radius 信息 \checkmark

有水详细信息		
概要输入	俞出 计费	
用户名:	guest	
终端主机标识符:	7C7A914652B7	(SmartDevice / Android / Android)
访问设备 IP/端口:	10.1.10.21:0	
RADIUS 请求		G
Radius Aruba A	ruba-AP-Group	lah1-group
Radius:Aruba:A	ruba-Device-Type	Win 8
Radius:Aruba:A	ruba-Essid-Name	lab1-portal
Radius:Aruba:A	ruba-Location-Id	94:b4:0f:c1:3f:e0
Radius:IETF:Ca	lled-Station-Id	000B869AAF37
Radius:IETF:Ca	lling-Station-Id	7C7A914652B7
Radius:IETF:Fra	med-IP-Address	10.1.20.102
Radius:IETF:NA	S-IP-Address	10.1.10.21
Radius:IETF:NA	S-Port	0
Radius:IETF:NA	S-Port-Type	19
Radius IFTE Se	rvice-Tvne	1
I < Showing 1 of	1-11 records ► ►	更改状态 Show Configuration 导出 显示日志 关闭

✓ 点击"输出"选项卡内容,观察,可以看到哪些 radius 信息

请求详细信息		8
概要 输入 输出		
强制执行配置文件:	task3-portal-profile	Τ
系统安全状况状态:	UNKNOWN (100)	
审计安全状况状态:	UNKNOWN (100)	
RADIUS 响应	6	0
Radius:Aruba:Aruba-	User-Role lab1-guest	



青求详细信息					
概要 输入	输出计费				
客户会话 ID:	guest7C7A	914652B7-5DA5FAEE-2A6F4			
开始时间戳:	Oct 15, 20	19 17:05:10 CST			
结束时间戳:	Still Active				
状态:	Active				
终止原因:	-				
服务类型:	-				
认证会话数:	1				
网络详细信息		\odot			
NAS IP 地址:		10.1.10.21:0			
NAS 端口类型	:	Wireless-802.11			
呼叫站 ID:		7C7A914652B7			
所呼叫站 ID:		000B869AAF37			
分帧 IP 地址:		10.1.20.102			
Framed IPv6	Address:	-			
帐户认证:		RADIUS			
I Showing 1	of 1-11 recor	ds ►► 更改状态 Show Configuration 导出 显示日志 关闭			

✓ 点击"计费"选项卡内容,观察,可以看到哪些 radius 信息



5 TASK4: ARUBA 控制器集成 CPPM 实现 802.1X 认证

5.1 用户需求

用户希望在无线覆盖的区域实现最安全的接入认证方式,保证接入的同时可以给不同的用户进行授权,并给予不同的网络访问权限,包括接入策略的细化以及对用户接入VLAN的区别控制等。

5.2 实现思路

答案详见附录

✓ 首先我们需要思考下,在当前的无线网络接入认证方式中,哪一种是最安全的接入认证方式?

答案:_____

✓ 针对该认证方式,我们需要思考下还需要为无线网络新增什么网元,即需要针对无线网络来设计什么样的认证服务器呢?

答案:

✓ 针对该认证服务器,我们需要思考下,你对该认证方式的完整流程熟悉吗?

答案:

✓ 针对802.1x认证的用户,我们设计两种类型的用户,例如领导和普通员工,利用Radius的授权功能,返回什么样属性给到控制器,从而实现不同的访问权限?

答案: ______

5.3 ClearPass 配置

5.3.1 添加本地账号和角色

第1步:找到 配置 - > 身份 - > 角色 , 点击右上角的"添加角色"按钮 , 增加两个角色:

aruba			ClearPass	o Pol	icy Manager	Menu 🗮
	配置»!	ŀ份 » 角	 音色			
₩ 监视 0	角色					🚽 添加角色
26 RE O						 基 守八用巴 全 导出角色
一章 此处开始	Roles ex	kist ind	lependently of an individual service and can be acces	sed glol	bally through the role-mapping policy of any service.	
- 登服务						
□ ♣ 认证	过滤器:	名称	♦ 包含 ♦	+	Go Clear Filter	显示 1000 🛊 记录
→ 呈身份 → 二章 Single Sign-On (SSO)	#		名称 •		说明	
	1.		[TACACS Super Admin]		Super administrator role for Policy Manager Admin	
一章 端点	2.		[TACACS Receptionist]		Receptionist role for Policy Manager Admin	
	3.		[TACACS Read-only Admin]		Read-only administrator role for Policy Manager Admin	
一章 角色	4.		[TACACS Network Admin]		Network administrator role for Policy Manager Admin	
	5.		[TACACS Help Desk]		Help desk role for Policy Manager Admin	
○ ① 女主状元	6.		[TACACS API Admin]		API administrator role for Policy Manager Admin	
□ → 网络	7.		[Other]		Default role for another user or device	
Profile and Network Scan	8.		[Onboard Windows]		Role for a Windows device being provisioned	
一心 策略仿真	9.		[Onboard Mac OS X]		Role for a Mac OS X device being provisioned	



在添加新角色1的窗口中, 输入下面的参数:

- ✓ 名称: leader-role
- ✓ 说明: 赋予领导的访问权限

编辑角色		8
名称:	leader-role	
说明:	赋予领导的访问权限 //	
	Save Cancel	

在添加新角色2的窗口中, 输入下面的参数:

- ✓ 名称: employee-role
- ✓ 说明: 赋予员工的访问权限

编辑角色		8
名称:	employee-role	
说明:	赋予员工的访问权限	
	Save	Cancel

第2步: 找到 配置 - > 身份 - >本地用户,点击右上角的"添加用户"按钮,增加两个用户账号:

aruba	(ClearPass Policy Manager		Menu
■ 面板 •	配置 » 身份 » 本地用户			
₩ 监视	本地用户			→ 添加用户
🝰 RE 📀				▲ 导出用户
一尊 此处开始				Account Settings
— 🔅 服务	ClearPass Policy Manager lists all local users in the	Local Users page.		
⊞- 🖴 认证				
	过滤器: 用户 ID 🔶 包含 🗘	🛨 Go Clear Filter		显示 20 🛟 记录
- C Single Sign-On (SSO)	# ■ 用户 ID ▲	名称	角色	状态
→ 🖶 安全状况				
→ 晝 强制执行				
→ 网络				
Profile and Network Scan				
一心 策略仿真	0			



在添加账号1的窗口中,输入下面的参数:

- ✓ 用户ID: leader (即用户的登录账号)
- ✓ 名称: leader-test (即该账号的别名,只是一个标签)
- ✓ 密码: aruba123 (该账号的登录密码)
- ✓ 认证密码: aruba123 (即重复输入一次登录密码)
- ✓ 启用用户: enable (勾选)
- ✓ 角色: leader-role (该角色在第一步中创建的)

编辑本地用户	0
用户 ID:	leader
名称:	leader-test
密码:	
认证密码:	
启用用户:	☑ (选中可启用本地用户)
更改密码:	\square (Check to force change password on next TACACS+ login)
角色:	leader-role
	属性
属性	值
1. Click to add	
	保存 取消

在添加账号2的窗口中, 输入下面的参数:

- ✓ 用户ID: employee (即用户的登录账号)
- ✓ 名称: employee-test (即该账号的别名,只是一个标签)
- ✓ 密码: aruba123 (该账号的登录密码)
- ✓ 认证密码: aruba123 (即重复输入一次登录密码)
- ✓ 启用用户: enable (勾选)
- ✓ 角色: employee-role (该角色是在第一步中创建的)



添加本地用户		8
用户 ID:	employee	
名称:	employee-test	
密码:		
认证密码:		
启用用户:	✓ (选中可启用本地用户)	
更改密码:	$\hfill\square$ (Check to force change password on next TACACS+ login)	
角色:	employee-role v	
	属性	
属性	值	
1. Click to add		
	添加取消	

配置总览:

aruba		ClearPass Policy Manager		Menu 🗮
■ 面転	配置 » 身份 » 本地用户 本地用户 ClearPass Policy Manager lists all lo	cal users in the Local Users page.		 ♣ 添加用户 ▲ 导入用户 ▲ 导出用户 ▲ 导出用户 ➡ Account Settings
 ➡ 认证 ☆ 方法 ☆ 源 ■ 2 身份 	过滤器: 用户 ID # 用户 ID	● Go Clear Filter 名称	角色 ▲	显示 20 ▼ 记录 状态
 ↓ Single Sign-On (SSO) ↓ 講響用戶 ↓ 講応主机列表 ↓ 前応 ↓ 前 	2. leader 3. group1-test 显示最后项的前一-后一	leader group1-test	leader-role [Other]	Enabled Enabled 原出 删除

5.3.2 添加认证服务

第1步: 找到 配置 - > 强制执行 - > 配置文件,点击右上角的"添加强制执行配置文件"按钮,增加两个强制执行配置文件:

aruba			Clear	Pass Po	icy Manage	er	Menu
19月1日 西板	◎ 配置 > 强制执行 > 配置文件						
	 强制拐 	强制执行配置文件					
28 RH	•						每八独制执行配置文件
	Each en	oforcem	ent policy contains enforcement profiles that	t match conditi	ons (role, posture,	and time) to actions (enforcement profiles).	
□ ♣ 认证	过滤器:	名称	\$ 包含 \$	+	Go Clear Filt	er	显示 100 🗘 记录
■ ■ 野切	#		名称 🔺		类型	说明	
3 强制执行	1.	0	[Aerohive - Terminate Session]		RADIUS_CoA	System-defined profile to disconnect user (Aerohive)	
□ 策略	2.	0	[AirGroup Personal Device]		RADIUS	System-defined profile for an AirGroup personal device request	
一章 配置文件	3.	0	[AirGroup Response]		RADIUS	System-defined profile for any AirGroup request	
□ ÷ 网络	4.	0	[AirGroup Shared Device]		RADIUS	System-defined profile for an AirGroup shared device request	
Profile and Network Scan	5.	0	[Allow Access Profile]		RADIUS	System-defined profile to allow network access	
	6.	O	[Allow Application Access Profile]		Application	System-defined profile to allow access to application	

在配置文件(第一个)选项卡中,输入下面的参数:

- ✓ 模板: Aruba RADIUS 强制执行
- ✓ 名称: task4-802.1x-leader-profile
- ✓ 操作: 接受

配置 » 强制执行 » 配置文件	» Add Enforcement Profile
强制执行配置文件	
配置文件 属性 概要	
模板:	Aruba RADIUS 强制执行 ▼
名称:	task4-802.1x-leader-profile
说明:	
类型:	RADIUS
操作:	● 接受 ○ 拒绝 ○ 删除
设备组列表:	Remove
	View Details
	Modify
	Select

在属性选项卡中, 输入下面的参数:

✓ 属性: Radius:Aruba Aruba-User-Role leader-role

酉	置 » 强制执行 » 配置文件 » Add Enforcement Profile					
5	a制执行配置文件					
	配置文件 属性 概要					
-						
	· · · · · · · · · · · · · · · · · · ·	名称	值	1		
1	类型 Radius:Aruba	名称 Aruba-User-Role =	值 = lead	ader-role	E	è t

在配置文件(第二个)选项卡中,输入下面的参数:

- ✓ 模板: Aruba Radius 强制执行
- ✓ 名称: task4-802.1x-employee-profile
- ✓ 操作: 接受



配置 » 强制执行 » 配置文件 »	Add Enforcement Profile
强制执行配置文件	
配置文件 属性 概要	
模板:	Aruba RADIUS 强制执行 ▼
名称:	task4-802.1x-employee-profile
说明:	
类型:	RADIUS
操作:	● 接受 ○ 拒绝 ○ 删除
设备组列表:	Remove View Details Modify

在属性选项卡中, 输入下面的参数:

✓ 属性: Radius:Aruba Aruba-User-Role leader-role

配	置 » 强制执行 »	記置文件	» Add Enforcement Profile				
强	制执行配置	文件					
Ē	2置文件 属性	概要					
	类型		名称		值		
1.	Radius:Aruba		Aruba-User-Role	=	employee-role	₿ <u></u>	Ť
2.	Click to add						

第2步: 找到 配置 - > 强制执行 - > 策略 , 点击右上角的"添加强制执行策略"按钮 , 增加一个强制执行策略:

aruba			ClearPass Po	licy Manage	n	Menu
■ 面板 •	配置 »	强制执行	» 策略			
「「」」」「「」」」「」」」「」」」」」」	强制	丸行策	略			🚽 添加强制执行策略
26 RH 🔹 📀						子/通利执行東略 全导出强制执行策略
一章 此处开始	ClearPa	iss con	trols network access by evaluating an enforcement policy as	sociated with the se	rvice.	
▶ ♣ 从业	过滤器:	名称	◆ 包含 ◆ +	Go Clear Filte	r	显示 1000 🛊 记录
	#		名称 ▲	类型	说明	
- 3 强制执行	1.		[Admin Network Login Policy]	TACACS	Enforcement policy controlling access to Policy Manager Admin	
一章 策略	2.	0	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices	
- 心 配置文件	3.		[Aruba Device Access Policy]	TACACS	Enforcement policy controlling access to Aruba device	
e •••• 网络	4.		[Guest Operator Logins]	Application	Enforcement policy controlling access to Guest application	
→ → → Frome and Network Scan	5.		[Insight Operator Logins]	Application	Enforcement policy controlling access to Insight application	
M. WARDAN	6.	0	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access	
	7.		[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access	
	显示最后	后项的前	后			复制导出删除



在强制执行选项卡中, 输入下面的参数:

- ✓ 名称: task4-802.1x-enforcement-policy
- ✓ 强制执行类型: RADIUS
- ✓ 默认配置文件: [Deny Access Profile]

配置 » 强制执行 » 策略 » 添加	Ω	
强制执行策略		
强制执行 规则 概要		
名称:	task4-802.1x-enforcement-policy	
说明:		
	//	
强制执行类型:	● RADIUS ◎ TACACS+ ◎ WEBAUTH (SNMP/Agent/CLI/CoA) ◎ 应用程序 ◎ Event	
默认配置文件:	[Deny Access Profile] View Details Modify	添加新强制执行配置文件

在规则选项卡中, 输入下面的参数:

- ✓ 规则: 点击 "Add Rule",配置如下:
 - 添加第一个规则条件是 Tips Role MATCHES_ALL leader-role, [User Authenticated]
 - 配置文件名: task4-802.1x-leader-profile

配置 » 强制执行 » 策略 » 添加	ha			
强制执行策略				
强制执行 规则 概要				
规则评估算法:	◉ 选择第一个匹配 ◎ 选择所有匹配			
Enforcement Policy Rules:				
Conditions		Acti	ons	
			Add Rule Move Up ↑ Move Down ↓	Edit Rule Remove Rule
规则编辑器				8
		条件		
匹配以下所有条件:				
类型	名称	运算符	值	
1. Tips	Role	MATCHES_ALL	leader-role [User Authenticated]	Pa úr
2. Click to add				
		强制执行配置文件		
配置文件名:	[RADIUS] task4-802 1x-leader-profile			
		Move Up ↑		
		Move Down ↓		
		Remove		
	Select to Add	*		
				保存取消

■ 再添加第二个规则条件是 Tips Role MATCHES_ALL employee-role, [User Authenticated]

aruba

■ 配置文件名: task4-802.1x-employee-profile

aruba

規则编辑器				¢
		条件		
匹配以下所有条件:				
类型	名称	运算符	值	
1. Tips	Role	MATCHES_ALL	employee-role [User Authenticated]	È t
		强制执行配置文件		
配置文件名:	[RADIUS] task4-802.1x-employee-profile	love Up ↑		
	Mo	ve Down ↓		
	F	Remove		
	Select to Add	T		

在概要选项卡中,对整体配置进行总览:

配置 » 强制执行 » 策略 » 添加

强制执行策略		
强制执行 规则 概要		
强制执行:		
名称:	task4-802.1x-enforcement-policy	
说明:		
强制执行类型:	RADIUS	
默认配置文件:	[Deny Access Profile]	
规则:		
规则评估算法:	First applicable	
Conditions		Actions
1. (Tips:Role MATCHES leader-role)	S_ALL [User Authenticated]	[RADIUS] task4-802.1x-leader-profile
2. (Tips:Role MATCHES	<u>ALL</u> [User Authenticated]	[RADIUS] task4-802.1x-employee-profile

第3步:找到 配置 - > 服务,点击右上角的"添加服务"按钮,增加一个服务:

aruba				ClearPass Poli	cy IV	lanager		Menu
■ 面板 O	配置 »	服务						
2 监视 0	服务							🚽 添加服务
🔏 配置 💿								圣 守八服分 2 导出服务
一尊 此处开始	This pa	age sho	ows the cu	rrent list and order of services that ClearPass	follows	during authentication	and authorization.	
☆ 服务								
Ⅲ — — — 认证	过滤器:	名称		▼ 包含 ▼	+	Go Clear Filter		显示 1000 • 记录
	#		顺序 ▲	名称		类型	模板	状态
王·丁 女全状位	1.		1	[Policy Manager Admin Network Login Serv	/ice]	TACACS	TACACS+ Enforcement	0
	2.		2	[AirGroup Authorization Service]		RADIUS	RADIUS Enforcement (Generic)	O
	3.		3	[Aruba Device Access Service]		TACACS	TACACS+ Enforcement	
➡ ➡ 网络	4.		4	[Guest Operator Logins]		Application	Aruba Application Authentication	0
🕢 🛃 Profile and Network Scan	5.		5	[Insight Operator Logins]		Application	Aruba Application Authentication	0
一口 策略仿真	6.		7	lab1-mac-user-defined		RADIUS	忽略 MAC 认证	
	7.		8	lab1-mac Device MAC Authentication		RADIUS	忽略 MAC 认证	
	8.		9	aaa test		RADIUS	RADIUS Enforcement (Generic)	0
	9.		10	lab1-portal-user-defined		RADIUS	RADIUS Enforcement (Generic)	
	显示最片	后项的首	前一-后一				重新排	序 复制 导出 删除

在服务选项卡中, 输入下面的参数:

✓ 类型: Aruba 802.1X Wireless

- ✓ 名称: task4-802.1x-auth-service
- ✓ 匹配项:以下所有条件
- ✓ 服务规则:
 - 1、Radius:IETF NAS-Port-Type EQUALS Wireless-802.11 (19)
 - 2、Radius:IETF Service-Type BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8)
 - 3、Radius:Aruba Aruba-Essid-Name EQUALS labX-peap (X: 1……6)

服务 Wa 角色 强制执行	
联务 认证 角色 强制执行 振要 类型: Aruba 802.1X Wireless 名称: Iask4-802.1x-auth-service 说明: Aruba 802.1X 无线接入服务	
类型: Aruba 802.1X Wireless ▼ 名称: task4-802.1x-auth-service 说明: Aruba 802.1X 无线接入服务	
名称: task4-802.1x.auth-service 说明: Aruba 802.1X 无线接入服务	
说明: Aruba 802.1X 无线接入服务	
监视模式: 📃 启用以监视无强制执行的网络访问	
更多选项: 🛛 授权 🗋 安全状况遵从 📄 审计终端主机 📄 配置文件端点 🗎 Accounting Proxy	
服务规则	
匹配项 🔘 任意或 🖲 以下所有条件:	
1. Radius:IETF NAS-Port-Type EQUALS Wireless-802.11 (19)	1 1
2. Radius:IETF Service-Type BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8)	1 T
3. Radius:Aruba Aruba-Essid-Name EQUALS Iab1-peap) 🗇

在认证选项卡中, 输入下面的参数:

- ✓ 1、认证方法: [EAP PEAP]
- ✓ 2、认证源: [Local User Repository][Local SQL DB]



an en la vala			
配直 » 脉夯 » 添加			
服务			
服务 认证 角色	强制执行 概要		
认证方法:	[EAP PEAP]	Move Up ↑	添加新认证方法
		Move Down ↓	
		Remove	
		View Details	
		Modify	
	Select to Add	•	
认证源:	[Local User Repository] [Local SQL DB]	Move Up ↑	添加新认证源
	-	Move Down ↓	
1		Remove	
		View Details	
		Modify	
	Select to Add	v	
剥离用户名规则:	🔲 启用以指定以逗号分隔的规则列表,用于	F剥离用户名前缀或后缀	
Service Certificate:	Select to Add	v	View Certificate Details

在角色选项卡中,暂时不做任何配置(详细内容可以参考高级介绍部分)

■ 1、角色映射策略: 空

配置 » 服务 » 添加			
服务			
服务 认证 角色	强制执行 概要		
角色映射策略:	Select	Modify	添加新角色映
		角色映射策略详细信息	
说明:	-		
默认角色:	-		
规则评估算法:	-		
条件		角色	

在强制执行选项卡中, 输入下面的参数:

■ 1、强制执行策略: task4-802.1x-enforcement-policy (即第2步中创建的强制执行策略)

配置 » 服务 » 添加		
服务		
服务 认证 角色 强	制执行 极要	
使用缓存的结果:	□ 使用从上一会话中缓存的角色和安全状况属性	
强制执行策略:	task4-802.1x-enforcement-policy Modify	添加新强制执行策略
	强制执行策略详细信息	
说明:		
默认配置文件:	[Deny Access Profile]	
规则评估算法:	first-applicable	
条件		强制执行配置文件
1. (Tips:Role MATCHE leader-role)	ES_ALL [User Authenticated]	task4-802.1x-leader-profile
2. (Tips:Role MATCHE employee-role)	ES_ALL [User Authenticated]	task4-802.1x-employee-profile

在概要选项卡中,对配置进行总览:

证 角色				
证 角色				
	强制执行 概要			
	Aruba 802.1X Wireless			
	task4-802.1x-auth-service			
	Aruba 802.1X 无线接入服务			
	Disabled			
	-			
			服务规则	
条件:				
2		名称	运算符	<u>á</u>
dius:IETF		NAS-Port-Type	EQUALS	Wireless-802.11 (19)
dius:IETF		Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
dius:Aruba		Aruba-Essid-Name	EQUALS	lab1-peap
	[EAP PEAP]			
	[Local User Repository] [Lo	ocal SQL DB]		
则:	-			
tificate:	-			
:	-			
:果:	Disabled			
:	task4-802.1x-enforcement	-policy		
	R件: ius:IETF ius:IETF ius:Aruba 이: ificate:	Aruba 802.1x Wireless task4-802.1x-auth-service Aruba 802.1x 无线输入服务 Disabled - - - - - - - - - - #: Disabled task4-802.1x-enforcement	Aruba 802.1X Wireless task4-802.1x-auth-service Aruba 802.1X 无线推入服务 Disabled	Aruba 802.1X Wireless task4-802.1X-auth-service Aruba 802.1X 系统输入服务 Disabled

5.4 控制器配置

5.4.1 添加无线信号

第1步: 使用 Web 方式登录到 Mobility Master (10.X.50.11) (X:1……6),找到 Managed Network ->

labX (X:1……6) -> Configuration -> WLANs 点击 "+" 进入创建一个新的无线配置向导

ALCONDO MOBILITY MASTI Iab1-mm-1	ER	CONTROLLERS ACC	CLIENTS	ALERTS		admin	-
← Managed Network > lab1 >							¢)
€ <mark>,</mark> Q	Dashboard	WLANs o					
🔁 Mobility Master	Configuration	NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION		=
📼 lab1-mm-1	WLANS						
Managed Network (2)	Roles & Policies						
🔁 lab1 (2)	Access Points						
📼 lab1-md1	AP Groups	—					
📼 lab1-md2	Authentication						
	Services						
	Interfaces						
	Controllers						
	System						
	Tasks						
	Maintenance						
	ArubaMM-VA, 8.4.0.0						
至步: General 常规	见选项设置						
✓ 1、Name(s	sid): labX-pea	ap (X:1	6)				
✓ 2、Primary	usage: Employ	ee					



- ✓ 3、Broadcast on: Select AP Groups-->labX-group (X:1……6) (前面的task中已经创建了该ap group)
- ✓ 4、Forwarding mode : Tunnel

New WLAN

Gene	eral	VLANs	Security	Access
Name (ssid):	lab1-peap			
Primary usage:	🖲 Employee 🛛 🔾 Gi	uest		
	Select AP Groups 💙			
Broadcast on:	default 🔺]		
	Tuppel			

第3步: 配置用户的 VLAN

✓ VLAN : wireless-user-vlan

New WLAN			
General	VLANS	Security	Access
VLAN: 1 V Hide VLAN 1 120 Named Wireless-user-vlan			
NAME	ID(S)		=
	1		
wireless-user-vlan	120		
+			

第4步:安全选项设置

- ✓ 1、Key management: WPA2-Enterprise, 采用WPA2的企业认证方式
- ✓ 2、Auth server: cppm , 即选择之前lab中创建好的RADIUS(cppm)认证服务器

G	ieneral	VLANS	Security	Access
re ure	Key management:	WPA2-Enterprise 💙		
Enterprise		cppm		
Personal	Auth servers:			
0		+		
Open				
	Reauth interval:	1440 min. 💙		
s ure	Reauth interval: Machine authenticatio	1440 min. V		
s ure	Reauth Interval: Machine authenticatic Blacklisting:	1440 min. V Disabled V		
。 ure :访问 、	Reauth Interval: Machine authenticatic Blacklisting: 时权限设置 1、Default r	ole: guest		
s ure : 访问 ✓ ✓	Reauth Interval: Machine authenticatic Blacklisting: 和权限设置 1、Default r 2、Server-de	ole: guest erived roles: 勾选		
s ure :: 访问 ✓ ✓	Reauth Interval: Machine authenticatic Blacklisting: 1、Default r 2、Server-de 3、Derivatio	ole: guest erived roles: 勾选 on method: Use val	lue returned from cle	earpass or other auth server

而实现不同用户可以具有不同的角色,不同的角色具有不同的访问权限。

lew WLAN				
G	eneral	VLANS	Security	Acc
Default role:	guest			
Server-derived roles:				
Derivation method:	 Use value returned from clearPass Use rules defined in table below 	or other auth server		





√ 2	、Deploy changes:	点击该按钮		
	IASTER m-1	CONTROLLERS ACCESS POINTS ⊙ 2 ○ 0 ⊙ 1 ○ 0 주	CLIENTS ALERTS 3 № 0 △ 0	3 admin ~
Managed Network > lab1 >				Pending Changes $ \diamondsuit $
Dashboard	New WLAN			
Configuration WLANs Roles & Policles Access Points AP Groups Authentication Services Interfaces Controllers System	The new WLAN can be viewed in the WLAN List NOTE: The new WLAN has been added to the pending ch	anges list. To deploy all pending changes, click Per	nding Changes at top right.	
Pending Changes	banges for 2 Controllers			
Man	naged Network > lab1 (2 Contro	llers)		
		Clo	Discard change	Deploy changes

第6步: 配置保存并同步给 md 设备

✓ 1、Pending Changes: 点击该按钮

5.4.2 添加角色

第1步: 使用 Web 方式登录到 Mobility Master (10.X.50.11) (X: 1 ·····6),找到 Managed Network - >

labX (X:1……6) -> Configuration -> Roles & Policies 点击"+"进入创建两个新的角色(leaderrole 和 employee-role)。

ALCONO MOBILITY MAST Iab1-mm-1	ER	CONTRO ② 2	ACCESS POINTS CLIENTS ALERTS ○ 0 ○ 1 ○ 0 〒 1 ∅ 0 △ 0	⑦ admin ∽
← Managed Network > lab1 >				¢.
Mobility Master Salab1-mm-1 Managed Network (2)	Dashboard Configuration WLANs Roles & Policies	Roles Policies Application	ons Allases se to be installed. Please go to HPE Aruba My Networking Portal to activate license key.	
c) lab1-md1 c) lab1-md2	Access Points AP Groups Authentication Services Interfaces Controllers System Tasks Maintenance	NAKE logon guest stanfuldott k guesklogon ysysopole ysjsansch-naje sattsh-logon	RULES 32 Rules 35 Rules 0 Rules 27 Rules 28 Rules 24 Rules 1 Rules	
✓ N	lame: lead	ーー ler-role, 新	建一个领导的角色	

a Hewlett Packard Enterprise company

New Role					
Name:	leader-role				
			Can	cel Submit	
√ 1	l、在roles里面	ā,选择上一步创建	建好的leader-r	ole	
√ 2	2、再点击右下	角的show Advan	ced View		
	ster 1	CONTROLLERS A ⊘ 2 ○ 0 0	CCESS POINTS CLIENTS AI ☉ 1 ○ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	LERTS	(?) admin ~
Managed Network > lab1 >					Pending Changes 🗘
Mobility Master I ab1-mm-1 Managed Network (2) Data Lab1 (2) I ab1-md1	Dashboard Configuration WLANs Roles & Policies Access Points AP Groups	Roles Policies Applications Allas This section will require PEF license to be installe Roles 14 NAME	es ed. Please go to HPE Aruba My Networking RULES	Pertal to activate license key.	=
📼 lab1-md2 🥔 (Authentication Services Interfaces Controllers System Tasks Maintenance	yp-antich-tole santch-tole default-sa-poser-tole default-sa-pose-tole aufento-sant-tole santon santon santon santon	24 Rules 1 Rules 2 Rules 3 Rules 4 Rules 4 Rules 41 Rules 0 Rules		• •
		leader-role Global Rules IP VERSION SOURCE	DESTINATION	SERVICE/APPLICATION ACTION	Show Advanced View

NOTE 需要事先在右上角的蓝色字体 admin 的下拉列表中选择 preferences , 勾选 show advanced profiles

aruba Iab1-mm-	iter 1		OLLERS ACCESS POINTS ○ 0 ○ 1	CLIENTS ALERTS		admin ~
← Managed Network > lab1 >						Pending Changes
	Dashboard	Roles Policies Applicati	ons Aliases			
 Mobility Master Iab1-mm-1 	Configuration	Roles 14				
C Managed Network (2)	Roles & Policies	NAME		RULES		=
🔁 lab1 (2)	Access Points	sys-switch-role switch-logon		24 Rules 1 Rules		Î
lab1-md1	AP Groups	default-iap-user-role		2 Rules		
La 1801-1102	Authentication	default-via-role default-vpn-role		3 Rules 4 Rules		
	Interfaces	authenticated		4 Rules		
	Controllers	leader-role		0 Rules		
	System	+				
	Maintenance	leader-role Policies	Bandwidth Captive Porta	i More		Show Basic View
		This section will require P	EF license to be installed. Please	e go to HPE Aruba My Networkir	ng Portal to activate license key.	
		NAME	RULES COUNT	TYPE	POLICY USAGE	=
		global-sacl	0	session	logon, guest, ap-role, stateful-dot1x, gu	
		apprf-leader-role-sacl leader-role	0	session session	leader-role leader-role	
		+				

- ✓ 1、在policies窗口里面,选中并点击leader-role
- ✓ 2、进入到Rules窗口, 点击 "+"来新增规则。



✓ 3、Rule type: Access control,新增一个permit all的策略(具体的访问权限可以后期根据实际 环境的需求来进行编辑和修改),最后点击 Submit按钮

aruba	lab1-mm-1		(
 Managed Netwo 	ork > lab1 >						Pending Change
7	Q Das	hboard	Roles Policies An	nlications Aliases			
Mobility Master	Cor	figuration	authenticated	photosis mases	4 Rules		
🗂 lab1-mm-1		WLANs	voice		41 Rules		
Managed Netwo	rk (2)	Roles & Policies	leader-role		0 Rules		Ū .
🔁 lab1 (2)		Access Points	+				
📼 lab1-m	id1	AP Groups					at the second second
📼 lab1-m	d2	Authentication	leader-role Policie	es Bandwidth Captive Po	rtal More		Show Basic View
		Sanisas	This section will re	quire PEF license to be installed. Ple	ase go to HPE Aruba My Networking	Portal to activate license key.	
		Jet vices	NAME	RULES COUNT	TYPE	POLICY IISAGE	-
		Controllors	global-sarl	0	session	logon quest an-role stateful-dot1x qu	
		Controllers	apprf-leader-role-sacl	0	session	leader-role	
		System	leader-role	0	session	leader-role	Ū
		Tasks					
	Mai	intenance	+				
			leader-role > Policy > le	ader-role Rules			Drag rows to re-order
			IP VERSION	SOURCE	DESTINATION SEE	VICE/APPLICATION ACTION	
			+				
	MOBILITY MASTER		(+	ONTROLLERS ACCESS POINT	S CLIENTS ALERTS		() admin v
aruba	MOBILITY MASTER lab1-mm-1			ONTROLLERS ACCESS POINT	S CLIENTS ALERTS) admin ~
Aruba Managed Networ	MOBILITY MASTER lab1-mm-1 rk > lab1 >		New Rule for lead	ONTROLLERS ACCESS POINT 2 0 0 0 1 0 0 er-role	S CLIENTS ALERTS		 admin ~
Managed Networ	MOBILITY MASTER lab1-mm-1 rk > lab1 > Q Dast	iboard	New Rule for lead	ONTROLLERS ACCESS POINT 2 0 1 0 er-role Access control Application Application	S CLIENTS ALERTS		(i) admin ~
Managed Networ	MOBILITY MASTER lab1-mm-1 rk > lab1 > Cont	iboard Inguration	Roles Rule type:	ONTROLLERS ACCESS POINT 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	s CLIENTS ALERTS		 admin ~
Managed Networ Mobility Master	MOBILITY MASTER lab1-mm-1 rk > lab1 > Cont Cont	iboard Iguration WLANS	Roles Rule type:	ONTROLLESS ACCESS FOINT D 2 0 0 0 1 0 0 er-role • Access control 0 Ap	s CLIENTS ALERTS) admin ~
Managed Networ Mobility Master Dab1-mm-1 Managed Network	MOBILITY MASTER lab1-mm-1 rk > lab1 > Con k (2)	iboard Iguration WLANS Roles & Policies	Roles Rule type:	ONTROLLERS 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	s CLIENTS ALERTS S S 0 P 0 & 0 plication Gancel OK) () admin ~
Managed Networ Mobility Master Diab1-mm-1 Managed Network Diab1 (2)	MOBILITY MASTER lab1-mm-1 rk > lab1 > Con k (2)	ibbard Alguration WLANS Boles & Policies Access Polints	Roles Roles Rule type: +	ONTROLLERS 2 0 0 0 1 0 0 er-role Access control Ap	S CLIENTS ALERTS CLIENTS ALERTS Plication Cancel OK		() admin ~
Managed Network	MOBILITY MASTER lab1-mm-1 rk > lab1 > Con k(2) k(2)	ibbard figuration WLANs Boles & Policies Access Polints AP Groups	New Rule for lead	onrholles Access Point 2 2 0 0 0 1 0 0 arrole ● Access control Ap 5 Bandwidth Captive Po	s CLIENTS ALERTS proton Gancel OK rtal More		 admin ~ admin ~ admin ~
Managed Network Sabl-mm-1 Managed Network Sabl-md Sabl-md Sabl-md Sabl-md	MOBILITY MASTER Iab1-mm-1 rk > Iab1 > Con k (2) 11 12 (0) (1) (1) (1) (1) (2) (2) (2) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4	iboard Iguration WLANs Roles & Policies Access Points AP Groups Authentication	Roles Role S Rule type: add role role role role role role role role	onrraolless Access Ponrr 2 0 0 0 1 0 0 errole Access control Ap 4 Access control Ap	s CLIENTS ALERTS) () admin ~ () () () () () () () () () ()
Managed Networ Mobility Master Silab 1-mm-1 Managed Network Anaged Network Silab 1-md Silab 1-md	MobilLity MASTER lab1-mm-1 rk > lab1 > Q Dast k (2) 11 2	iboard Nguration WLANs Roles & Policies Access Politics AP Groups Authentication Services	Roles Rule type: add valo type teaden-role Policie This section will rec	onmaolles Access Point a 2 0 0 0 1 0 0 errole errole Access control Ap a Bandwidth Captive Po puire PEP license to be installed. Pie	S CLIENTS ALERTS D T 0 P 0 0 0 0 plication Cancel OK rtal More ase go to HPL Aruba My Networking	Portal to activate license key.) (1) admin ~ (2) (2) (3) (3) (4) (4) (4) (4) (5) (4) (5) (4) (5) (4) (5) (5) (4) (5) (5) (5) (5) (5) (5) (5) (5
Managed Networ Mobility Master Bab1-mm-1 Managed Network Bab1 (2) Bab1 (2) Bab1-md	MOBILITY MASTER Iab1-mm-1 Ick - Iab1	Ibbard Inguration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces	Roles Auto Built type: Auto Frei Headen-role Rollcie This section will rec NAME	ONTROLLES ACCESS POINT 2 0 0 1 01 errole • Access control Ap 5 Bandwidth Captive Po pure PCF locence to be installed. Pie RULES COUNT	s CLIENTS ALERTS plication Cancel OK rtal More TYPE	Potal to activate license key.	 admin ~ admin ~ Show Basic View
Managed Networ Mobility Master I ab1-mm-1 Managed Networl I ab1-md I ab1-md	MOBILITY MASTER lab1-mm-1 rk > lab1 - 0 k (2) l l l l l l	Ibbard figuration WLANs Bodes & Policies Access Points AP Groups Authentication Services Interfaces Controllers	New Rule for lead Roles Rule type: add Factor Header-role Policie This section will rec RAME globalicad	ONTROLLERS ACCESS POINT C C C C C C C C C C C C C C C C C C C	S CLIENTS ALERTS D D D O O O O pS(ction Cancel OK rtal More ase go to HPE Aruba My Networking TYPE Settion	Portal to activate license key. Poucer usaas keyn, guest, ayreik, szaetűd-dette, gu-	 admin ~ admin ~ Show Basic View
Managed Networ Mobility Master I lab I-mm-1 Managed Networ I lab I-md I lab I-md	MOBILITY MASTER Iab1-mm-1 Con k(2) k(2) k(2) k(3) k(3	ibbard figuration WLANs Boles & Policies Access Polints Authentication Services Interfaces Controllers System	Roles Roles Rule type: audi voite + Feader-role Rule type: type type type Rule type: type type type type type type type type	ONTROLLERS ACCESS POINT Control Contr	s CLIENTS ALERTS TO PO Cancel OK rtal More Type sesson sesson	Perfail to activate license key.	admin ~
Anaged Networ Aobiity Master Calabi-mm-1 Anaged Networ Calabi-md Calabi-md	MobilLITY MASTER lab1-mm-1 rk > lab1 > Q Dast (Con k (2) 11 12	Iboard Aguration WLANs Boles & Policies Access Politics Access Politics Authentication Services Interfaces Controllers System Tasks	Roles Roles Rule type: action visit visit reader-role Rule type: This section will read NAME gogSalsard soprificader-role-action leader-role	antraolLERS access Point arrole arrole arrole and antrole and antrole and antrole and antrole	S CLIENTS ALERTS CLIENTS ALERTS CLIENTS O CO CLIENTS O CLIENTS O CLIE	Pertal to activate license key. Pouce USAGE keyen pert sponde, standul-detix, pu- kedercele kedercele	admin ~
Aruba Managed Networ Abbility Master El lab1-mm-1 Anaged Network El lab1-md El lab1-md	MOBILITY MASTER Iab1-mm-1 rk > lab2 (k (2) 11 12 2 Main Main	Ibbard Bguration WLANs Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers System Tasks tenance	Roles Auto Built type: Auto Built type: Built type: This section will rec NAME global and global and Built type: This section will rec NAME global and Built type: This section will rec NAME global and Built type: This section will rec NAME global and based collected	Access Pointr Access Pointr Access Pointr Access control Access cont	s CLIENTS ALERTS plication Cancel OK rtal More ase go to HPE Avuba My Networking session session	Pertal to activate license key. Postal to activate license key. Postal constraints standard destx ga Isaber-rele Isaber-rele Isaber-rele	 admin ~ admin ~ Show Basic Vie =
Aruba Managed Networ Mobility Master I ab1-mm-1 Managed Networ I ab1-md I ab1-md I ab1-md	MOBILITY MASTER Iab1-mm-1 rk > Iab1 Con K(2) I1 I2 Mar	Ibbard Alguration Michael Michael Michael Michael Access Points Ar Groups Authentication Services Services Controllers System Tasks teenance	Roles Roles Roles Rule type: add Face Packet Rule type: This section will rec Rules SportFace Packet SportFace Packet SportFace Rule type: Rule	ONTROLLERS 2 00 0 1 0 0 errole • Access control Ap • Acces	S CLIENTS ALERTS pReation Cancel OK real More set go to HPE Aruba My Networking FUTE Settion Settion	Portal to activate license key. Poucy URAB license key. Poucy URAB license key. Inder-celle Isadervole	 admin ~ admin ~ Show Basic View admin ~
tobility Master bility Master bility Master bility Master bib1-mm-1 lanaged Network bib1-md bib1-md	K(2) Dast kk(2) K(2) K(2) K(2) K(2) K(2) K(2) K(2) K	ibbard figuration MLANS Bolicies Access Points Access Poi		ONTROLLERS ACCESS POINT acroie Access control Acc	S CLIENTS ALERTS Pleation Cancel OK Trai More Trae Session Session Session Session	Pertal to activate license key. Potcer state login, giert, aperia, stateful destir, giu- lasteride lasteride lasteride	 admin ~ admin ~ Shew Basic View
Aruba Managed Networ Mobility Master I lab1-mm-1 Managed Networl I lab1-md I lab1-md	MOBILITY MARTER Iab1-mm-1 (k J bat) (k (2) (k (2) (k (2) (k (2) (k (2) (k (2) (k (2) (k	ibbard figuration WLANS Books & Policies Access Points Access Points Ac	Kove Rule for lead Roles	ONTROLLERS ACCESS POINT 2 2 0 0 ACCESS CONTrol A P Access Contro	S CLIENTS ALERTS Protocol Cancel OK rtal More season seas	Pertail to activate license key.	admin ~ admin ~ Show Basic View Show Basic View C Drag rows to re-order C Drag rows to re-order
Managed Networ Mobility Master (a) Jab1-mm-1 Managed Networ (c) Jab1-md (c) Jab1-md	MOBILITY MASTER Iab1-mm-1 rk > lab1 > (k (2) 11 12 2 4 4 4 4 4 4 4 4 4 4 4 4 4	ibbard Bguration WLNS Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers System Tasks System Tasks	Roles Auto Auto Auto Auto Auto Auto Auto Auto	ONTROLLESS 2 0 0 0 1 0 0 errole errole Access control Ap advervele Rules Source	S CLIENTS ALERTS pication Cance OK rtal More ase go to HPT Aruba My Networking TYPE session ses	Pertail to activate license key. Pertail to activate license key. Issue perta area in standard destr. ga Issue role Issue role Issue role	admin ~



+			
leader-role > lead	er-role > New forwarding R	tule	
IP version:	IPv4 💙		
Source:	Any		
Destination:	Anv		
Destination.	City		
Service/app:	Any 🗸		
Action:	Permit	•	
TOS:			
Time range:	Nees		
nme range:	- None -	 Keset 	
902 1p			
ouz. ip priori	y	Nieror Dischlarsonning	
Options:	Log	Mirror Biackiist Disable scanning	
Queue:	✓		
•			
MOBILITY MASS Iab1-mm-1	18	CONTROLLERS ACCESS POINTS CLIENTS ALERTS	Cancel Sul
MOBILITY MASS Lab1-mm-1 aged Network > Lab1 >	ER	CONTROLLERS ACCESS POINTS CLIENTS ALERTS \odot 2 \odot 0 \odot 1 \odot 0 \odot 0 ρ 0 Δ 0	Cancel Su admin Pending Char
MOBILITY MASS lab1-mm-1 aged Network > lab1 >	ER Dashboard	CONTROLLERS ACCESS POINTS CLIENTS ALERTS ② 2 ○ 0 ○ 1 ○ 0 ○ 0 ○ 0 ○ 0 ○ 0 ○ 0 ○ 0 ○ 0	Cancel Su admin Pending Char
MOBILITY MASS Iab1-mm-1 aged Network > Iab1 >	ER Dashboard Configuration	CONTROLLERS ACCESS POINTS CLIENTS ALERTS Image: Original Control Image: Original Control Image: Original Control Image: Original Control Roles Policies Applications Allases authenticated 4 Rules	Cancel Su admin Pending Char
MOBILITY MASS Iab1-mm-1 aged Network > Iab1 > Q ity Master ab1-mm-1 ged Network (2)	TR Dashboard Configuration WLANS Boles & Policies	CONTROLLERS ACCESS POINTS CLENTS ALERTS Image: Control of the second sec	Cancel Su admin Pending Char
MOBILITY MASS Iab1-mm-1 aged Network > Iab1 > Q ity Master ab1-mm-1 ged Network (2) ab1(2)	TR Dashboard Configuration WLANS Roles & Policies Access Polits	CONTROLLERS ACCESS POINTS CLENTS ALERTS Image: State of the stat	Cancel Su (*) admin Pending Char (*)
MOBILITY MASS Iab1-mm-1 aged Network > Iab1 > (ty Master Ib1-mm-1 ged Network (2) Ib1(2) Iab1-md1	TR Dashboard Configuration WLANS Roles & Policies Access Polints AP Groups	CONTROLLERS ACCESS POINTS CLIENTS ALERTS Image: Control of the state of the s	Cancel Su () admin Pending Char () Show Basic Vin Show Basic Vin
MOBILITY MASS Iab1-mm-1 Iab1-mm-1 iged Network > Iab1 > Q ity Master ib1-mm-1 ged Network (2) ib1(2) iab1-md1 iab1-md1	ER Dashboard Configuration WLANS Roles & Policies Access Points A Corsups Authentication	CONTROLLERS ACCESS POINTS CLIENTS ALERTS © 2 0 © 1 0 © 0 0 Roles Policies Applications Allases Auflenciated 4 Rules 0 Isaderrole 1 Rules Isaderrole 1 Rules Isaderrole 1 Rules This section will require PEF license to be installed. Please go to HPE Aruba My Networking Portal to activate license key.	Cancel Su () admin Pending Char () Show Basic Vin
MOBILITY MASS Idb1-mm-1 Idb1-mm-1 idb1-mm-1 idb1-mm-1 idb1-mm-1 idb1-mm-1 idb1-mm1 idb1-mm1 idb1-mm1 idb1-mm1 idb1-mm2	ER Dashboard Configuration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces	CONTROLLERS ACCESS POINTS CLIENTS ALERTS © 2 0 © 1 0 © 0 P 0 0 Roles Policies Applications Allases addrenicated 4 Rules isaderrole 1 Rules isaderrole 1 Rules the 1 Rules	Cancel Su () admin Pending Char Show Basic Vin
MOBILITY MASS Idb1-mm-1 aged Network > Idb1 > V ty Master Ib1-mm-1 ged Network (2) Ib1-md1 Iab1-md1 Iab1-md2	ER Dashboard Configuration WLANS Plotes & Policies Access Points AP Groups Authentication Services Interfaces Controllers	CONTROLLERS ACCESS POINTS CLIENTS ALERTS © 2 0 © 1 0 © 0 P 0 0 Roles Policies Applications Allases addreticated 4 Rules 0 tadderrole 1 Rules + Isaderrole 1 Rules + Isaderrole 1 Rules + • Instantonic Replications to be installed. Please go to HPE Aruba My Networking Portal to activate license key. NAME RULES COUNT TYPE Policy Usadet globalizad 0	Cancel Su () admin Pending Char Show Basic Vin Show Basic Vin
MOBILITY MASS Idb1-mm-1 aged Network > Idb1 > V ty Master Ib1-mm-1 ged Network (2) bb1(2) ida1-md1 iab1-md2	ER Dashboard Configuration WLANS Plotes & Policies Access Points A Groups Authentication Services Interfaces Controllers System	CONTROLLERS ACCESS POINTS CLIENTS ALERTS © 2 0 © 1 0 © 0 P 0 0 Roles Policies Applications Allases saffericated 4 Rules 0 taddercale 1 Rules	Cancel Su () admin Pending Char Show Basic Vin Show Basic Vin Show Basic Vin
MOBILITY MASS Idb1-mm-1 aged Network > Idb1 > V ty Master Ib1-mm-1 ged Network (2) bb1 (2) ida1-md1 iab1-md1 iab1-md2	ER Dashboard Configuration WLANS Plotes & Policies Access Points AP Groups Authentication Services Interfaces Controllers System Tasks Multinenzee	CONTROLLERS ACCESS POINTS CLIENTS ALERTS © 2 0 © 1 0 © 0 P 0 0 Roles Policies Applications Allases addreticated 4 Rules 0 tadderrole 1 Rules + Isaderrole 1 Rules + Isaderrole 1 Rules + Isaderrole 1 Rules + Isaderrole 1 Rules + Isaderrole 1 Rules + Isaderrole 1 Rules + Isaderrole 1 Rules + Isaderrole 1 Sesson Isaderrole 1 Sesson Isaderrole 1 Sesson	Cancel Su () admin Pending Char Show Basic Viv
MOBILITY MASS Mobility Masser Ib1-mm-1 ged Network (2) Ib1-mm1 ib1-mm1 ib1-mm1 ib1-mm1 ib1-mm1 ib1-mm1	ER Dashboard Configuration WLANS Roles & Policies Access Points A Coroups Authentication Services Interfaces Controllers System Tasks Maintenance	CONTROLLERS ACCESS POINTS CLIENTS ALERTS © 2 0 © 1 0 © 0 P 0 0 0 Roles Policies Applications Allases Automiciand 4 Rules 0 satisficand 4 Rules 0 issderrole 1 Rules issderrole 1 Rules This section will require PEF license to be installed. Please go to HPE Aruba My Networking Portal to activate license key. NAME RULES COUNT issderrole 0 isseland 0	Cancel Su () admin Pending Char Show Basic Vice ()
MOBILITY MASS aged Network > lab1 > ity Masser ab1-mm-1 ged Network (2) ab1(2) lab1-md1 lab1-md2	ER Dashboard Configuration WLANS Roles & Policies Access Points A Groups Authentication Services Interfaces Controllers System Tasks Maintenance	CONTROLLERS ACCESS POINTS CLIENTS ALERTS © 2 0 © 1 0 © 0 P 0 © 0 Roles Policies Applications Allages Automiciand 4 Rules 0 satisficand 4 Rules issderrole 1 Rules issderrole 1 Rules the 1 issderrole 1 Rules issderrole 1 Rules issderrole 1 Rules issderrole 1 issderrole 9 Rules Count issderrole 1 issderrole 1 isselerole 1	Cancel Su () admin Pending Char Show Basic Via () Show Basic Via () () () () () () () () () ()
MOBILITY MASS aged Network > lab1 > work > lab1 ity Masser ab1-mm1 ged Network (2) ab1(2) lab1-md1 lab1-md2	ER Dashboard Configuration WLANS Roles & Policies Access Points A Coroups Authentication Services Interfaces Controllers System Tasks Maintenance	CONTROLLERS ACCESS POINTS CLIENTS ALERTS © 2 0 © 1 0 © 0 P 0 0 0 Roles Policies Applications Allases submicicated 4 Rules 0 statescare 1 Rules isaderrole 1 Rules + • Statescare • This section will require PEF license to be installed Please go to HPI Aruba My Networking Portal to achivate license key. NAME Rules count sesson login pars, parsis, stateful-detri, gu- lasederole Isaderrole 1 Isaderrole 1 Isaderrole 1 Isaderrole 1	Cancel Su () admin Pending Char Show Basic Vice Control of the second secon

第2步: 采用上面同样的方法,我们再创建另外一个角色 employee-role,两种角儿之间我们可以设置不同的访问策略,从而设定两种不同的访问权限。

- 第3步: 配置保存并同步给 md 设备
 - ✓ 1、Pending Changes: 右上角点击该按钮
 - ✓ 2、Deploy changes: 点击该按钮
| aruba | MOBILITY MASTI
lab1-mm-1 | ER | CONTROLL
⊙ 2 (| ERS ACCESS POINTS ○ ○ 1 ○ 0 | CLIENTS ALER
〒 3 ₱ 0 △ | o o | admin ~ |
|-------------------------------------|-----------------------------|---------------------|----------------------|---|---------------------------|-----------------------------------|-------------------------|
| Managed Network | ork > lab1 > | | | | | | Pending Changes 🕻 |
| Ê₽, | ۹ | Dashboard | Roles Policies | Applications Aliases | | | |
| 🔁 Mobility Master | | Configuration | group r-mac-caching- | guesciugun | 20 MURS | | |
| 🖾 lab1-mm-1 | | WLANs | employee-role | | 1 Rules | | <u>.</u> . |
| Managed Network | rk (2) | Roles & Policies | + | | | | |
| 🔁 lab1 (2) | | Access Points | employee-role | Policies Bandwidth | Captive Portal Mor | re | Show Basic View |
| 😑 lab1-md | ±1 | AP Groups | NAME | RULES COUNT | TYPE | POLICY USAGE | |
| 🖘 lab1-md | 12 | Authentication | global-sacl | 0 | session | logon, guest, ap-role, stateful-d | |
| | | Services | apprf-employee-role | -sad 0 | session | employee-role | |
| | | Interfaces | employee-role | 1 | session | employee-role | |
| | | Controllers | | | | | |
| | | System | + | | | | |
| | | Tasks | employee-role > F | olicy > employee-role Rules | | | i Drag rows to re-order |
| | | Maintenance | IP VERSION | SOURCE | DESTINATION | SERVICE/APPLICATION ACTION | = |
| | | | Ipv4 | any | any | any permit | |
| | | ArubaMM-VA, 8.4.0.0 | +
< | | | | |
| ending Ch | anges | | | | | | |
| Per | nding Ch | anges for 2 Control | lers | | | | |
| | D Maria | | 2 controllers) | | | | |
| | | | | | Close | Discard changes | Deploy changes |

5.4.3 添加计费

第1步: 使用 Web 方式登录到 Mobility Master (10.X.50.11) (X:1…6), 找到 Managed Network - > labX (X:1…6) -> Configuration -> Authentication -> AAA Profiles 选项卡,点击 AAA 前面的 "+"展开所有的 AAA Profile,找到之前向导已经生成的 labX-peap_aaa_prof,点击 前面的 "+"展开所

有的配置	置项			
	.ITY MASTER 11-mm-1	CONTROLLERS ACCESS POINTS CLIENT ∅ 2 0 ∅ 1 0 ? 3	ALERTS	admin ~
🗲 Managed Network > la	b1 >			Pending Changes 🗘
C Mobility Master	Q Dashboard	Auth Servers AAA Profiles L2 Authentication	L3 Authentication User Rules Advanced	×
🖾 lab1-mm-1	WLANs	AAA Profiles	AAA Profile: lab1-peap_aaa_prof	
Managed Network (2)	Roles & Policies	G default-tunneled-use	Initial role:	logon
(1) HUT (2)	Access Points	default-xml-api default-xml-api	MAC Authentication Default Role:	guest
	AP Groups		802.1X Authentication Default Role:	guest
	Authentication		Download Role from CPPM:	
	Services		Set username from dhcp option 12:	
	Interfaces	⊕ ☐ lab1-mac_aaa_prof	L2 Authentication Fail Through:	
	Controllers	\ominus 🕞 lab1-peap_aaa_prof 👘	Multiple Server Accounting:	
	System	802.1X Authentication	User idle timeout:	secor
	Tasks	802.1X Authentication Server Group	Max IPv4 for wireless user:	2
	Maintenance	MAC Authentication	PADIUS Posming Accounting	•
		MAC Authentication Server Group	RADIUS Interim Accounting:	
		RADIUS Accounting Server Group	RADIUS Arct-Session-Id In Arcess-Request:	
		RFC 3576 server	User derivation rules:	-None-
		R XML API server	Oser derivatori rules.	-ivone-

第2步: 选择 RADIUS Accounting Server Group,在右边配置窗口中,从 Server Group 下拉列表中选择之前 向导已经创建的 labX-peap-dot1_svg. 点击右下角的 Submit 按钮。





5.5 验证结果

5.5.1 终端上的关联和登录记录



5.5.2 CPPM 上查看认证记录

第1步: 找到 监视 - > Live Monitoring - > 访问跟踪器, 查看近期的认证记录。 如果认证记录较多的话,我们可以采用过滤条件来查询。

aruba			ClearPas	s Policy Manag	ger		Menu 🔜
■■ 而板	● 监视 »	Live Monitoring »	访问跟踪器				
₩ 监视	 访问 	跟踪器 Oct 09, 2	019 16:58:21 CST				自动刷新
□	The Ac	ccess Tracker page	provides a real-time display of per	-session access activity	on the selected server or domain.		
_	? [[All Requests]	Lab1-CPPM-1 (10).1.50.41)	Last 1 day befor	re Today	编辑
	过滤器:	Request ID	▼ 包含 ▼	+ Go	Clear Filter		显示 20 🔻 记:
➡ ➡ Profile and Network Scan	#	Server	Source	Username	Service	Login Status	Request Timestamp 🔹
	1.	10.1.50.41	RADIUS	employee	task4-802.1x-auth-service	ACCEPT	2019/10/09 16:57:45
数据过滤器	2.	10.1.50.41	RADIUS	employee	task4-802.1x-auth-service	ACCEPT	2019/10/09 16:24:21
	3.	10.1.50.41	RADIUS	lab1-test	task1-test-service	ACCEPT	2019/10/09 14:21:57
Cruba 重数 変数 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	● ^{监视 »} ● 访问] The Ac	Live Monitoring » à 跟踪器 Oct 09, 2 ccess Tracker page	ClearPas 防问跟踪器 019 16:58:56 CST provides a real-time display of per	s Policy Manag	ger		Menu 🔜 O 自动刷新
- 學 访问跟踪器 - 學 计费 - 學 OnGuard 活动 - ₽ 分析和趋势	?	All Requests]	Lab1-CPPM-1 (10	0.1.50.41)	Last 1 day befor	re Today	编辑
	过滤器:	Service	▼ 包含 ▼ task4		Clear Filter		显示 20 🔻 记录
Profile and Network Scan	L	Server	Source	Username	Service	Login Status	Request Timestamp 🔹
— ● 中丁旦有益 — ■ 車件査差哭	1.	10.1.50.41	RADIUS	employee	task4-802.1x-auth-service	ACCEPT	2019/10/09 16:57:45
	2.	10.1.50.41	RADIUS	employee	task4-802.1x-auth-service	ACCEPT	2019/10/09 16:24:21
Blacklisted Users	显示最	后项的前一-后一					
	111-13 1960						

✓ 点击这条认证记录,查看"概要"选项卡内容,观察,可以看到哪些信息



请求详细信息					
概要 输入 输出	计费				
登录状态:	ACCEPT				
会话标识符:	R00000051-01-5d9da109				
日期和时间:	Oct 09, 2019 16:57:45 CST				
终端主机标识符:	7C7A914652B7 (Computer / Windows / Windows)				
用户名:	employee				
访问设备 IP/端口:	10.1.10.21:0				
系统安全状况状态:	UNKNOWN (100)				
	所用策略 -				
服务:	task4-802.1x-auth-service				
认证方法:	EAP-PEAP				
认证源:	Local:localhost				
授权源:	[Local User Repository]				
角色: [User Authenticated], employee-role					
强制执行配置文件: task4-802.1x-employee-profile					
服务监视模式:	<u>á视模式:</u> Disabled				
Online Status:	🖸 Online				
Showing 1 of 1-2	Precords ▶ ▶ 更改状态 Show Configuration 导出 显示日志	关闭			

✓ 点击"输入"选项卡内容,观察,可以看到哪些信息

概要 输入 输出 计费		
用户名:	employee	
冬端主机标识符:	7C7A914652B7 (Computer / Windows / Windows)	
方问设备 IP/端口:	10.1.10.21:0	
RADIUS 请求		
Radius:Aruba:Aruba-AP-Group	lab1-group	
Radius:Aruba:Aruba-Essid-Name	lab1-peap	
Radius:Aruba:Aruba-Location-Id	94:b4:0f:c1:3f:e0	
Radius:IETF:Called-Station-Id	000B869AAF37	
Radius:IETF:Calling-Station-Id	7C7A914652B7	
Radius:IETF:Framed-MTU	1100	
Radius:IETF:NAS-Identifier	10.1.10.11	
Radius:IETF:NAS-IP-Address	10.1.10.21	
Radius:IETF:NAS-Port	0	
Radius:IETF:NAS-Port-Type	19	
Padius: IETE: Sorvico-Typo	2	

✓ 点击"输出"选项卡内容,观察,可以看到哪些信息



i求详细信息 🔹 🔍						
概要 输入 输出	计费					
强制执行配置文件:	task4-802.1x-employee-profile					
系统安全状况状态:	UNKNOWN (100)					
审计安全状况状态:	UNKNOWN (100)					
RADIUS 响应	\odot					
Radius:Aruba:Aruba	a-User-Role employee-role					

✓ 点击"计费"选项卡内容,观察,可以看到哪些信息

概要 输入	、输出	计费	
客户会话 ID:	employ	ee7C7A914652B7-5D9E1038-DAA60	
干始时间戳:	Oct 09	2019 16:57:46 CST	
吉束时间戳:	Still Ac	ive	
犬态:	Active		
冬止原因:	-		
服务类型:	-		
人证会话数:	1		
网络详细信息			∍
NAS IP 地址	::	10.1.10.21:0	
NAS 端口类	型:	Wireless-802.11	
呼叫站 ID:		7C7A914652B7	
所呼叫站 ID	:	000B869AAF37	
分帧 IP 地址:		10.1.20.102	
Framed IPv6 Address:		-	
帐户认证:		-	

5.5.3 控制器上查看认证记录

第1步: 通过 SSH 登录到 labX 的 mm 控制器上,采用 show global-user-table list 可以查看当前所有的关联 用户列表,可以查看当前用户的认证账号,认证后的角色,采用的认证方法,获取的 IP,终端的 MAC 地 址、当前关联的 AP-Name, ESSID 等



6 TASK5: ARUBA 控制器集成 CPPM 实现无感知认证 (MAC + PORTAL)

6.1 用户需求

用户希望访客用户通过portal认证的方式接入无线网络,并给予访客访问权限。为了提高访客使用无线网络的体验,只需要用户在第一次连接无线的时候使用用户名和密码进行web认证登录,之后将采用MAC无感知认证的方式接入网络。为了对MAC认证终端进行管理,要求MAC认证用户在控制器上显示portal认证登录的用户名。

6.2 实现思路

答案详见附录

✓ ClearPass针同一个SSID既有MAC认证,又有Portal认证,如何匹配到一个正确的认证请求:

答案:_____

✓ ClearPass上有两条MAC认证服务,如何匹配到一个正确的认证请求:

答案: ____

- ✓ 配置步骤:
 - ClearPass配置
 - ◆ 配置一个portal认证登录页面
 - ◆ ClearPass配置一个MAC Caching认证服务,用来匹配portal认证请求,并更新Endpoint数据库
 - ◆ ClearPass配置一个MAC认证服务,用来匹配mac认证请求,利用MAC caching认证阶段更新的 Endpoint数据库进行无感知认证,并返回缓存的用户名
 - 无线控制器配置:
 - ◆ 配置一个SSID: labX-mac-caching,并启用MAC认证和Portal认证,
 - ◆ 认证服务器指向CPPM IP:10.X.50.41。
 - ◆ Portal认证前role: **labX-mac-caching-guest-logon**,成功后获得role: **guest**
 - ◆ Mac认证后获得role: guest (X: 1…6)

6.3 ClearPass 配置

6.3.1 添加 Portal 登录页面

Portal页面配置公用lab3的guest-login 页面,这里不再重复 \checkmark

6.3.2 添加 mac caching 认证服务

第1步: 找到 配置 - > 强制执行 - > 配置文件 , 点击右侧的 "添加强制执行配置文件"按钮 , 增加一个强制执行 配置文件:

在"配置文件"选项卡中输入下面参数:

- 模板: ClearPass 实体更新强制执行 \checkmark
- 名称: task5-update-endpoint \checkmark

配置 > 强制执行 > 配置文件 > Add Enforcement Profile					
强制执行配置文件					
配置文件 属性 概要					
模板:	ClearPass 实体更新强制执行 🗘				
名称:	task5-update-endpoint				
说明:	©				
类型:	Post_Authentication				
操作:	⊙ 接受 ○ 拒绝 ○ 删除				
设备组列表:	Remove 添加新设备组 View Details Modify				

在"属性"选项卡中输入下面参数:

配置 » 强制执行 » 配置文件 » Add Enforcement Profile

 \checkmark 属性:

强制执行配置文件

- 1. Endpoint Username
- 2. Endpoint Guest Role ID =
- 3. Endpoint MAC-Auth Expiry
- 4. Status-Update Endpoint
- %{Authentication:Username}
- guest-role
- = %{Authorization:[Time Source]:One Day DT}
- =
- Known

=

配置文件 属性 概要 类型 名称 偱 Endpoint %{Authentication:Username} 1. Username ĥ 2. Endpoint Guest Role ID Ē ŵ quest-role Ē ŵ 3. Endpoint MAC-Auth Expiry %{Authorization:[Time Source]:One Day DT} Status-Update Ē ŵ Endpoint Known Click to add... 5.

在"概要"选项卡中对配置进行总览:

概要: 查看配置总览, 并点击"保存" \checkmark



配置 » 强制执	配置 » 强制执行 » 配置文件 » Add Enforcement Profile							
强制执行	强制执行配置文件							
配置文件	配置文件 属性 概要							
配置文件:								
模板:		ClearPass 实体更新强制执行						
名称:		lab5-update-enpoint						
说明:		lab5更新endpoint数据库配置文件						
类型:		Post_Authentication						
操作:		Accept						
设备组列表:		-						
属性:								
类型		ŧ	名称		值			
1. Endpo	oint	ι	Username	=	%{Authentication:Username}			
2. Endpo	oint	0	Guest Role ID	=	%{GuestUser:Role ID}			
3. Endpo	oint	Ν	MAC-Auth Expiry	=	%{Authorization:[Time Source]:One Day DT}			
4. Status	is-Update	E	Endpoint	=	Known			

第2步: 找到 配置 - > 强制执行 - > 配置文件 , 点击右侧的 "添加强制执行配置文件"按钮 , 增加第二个强制执行配置文件:

在"配置文件"选项卡中输入下面参数:

- ✓ 模板: Aruba Radius 强制执行
- ✓ 名称: task5-guest-profile

配置 » 强制执行 » 配置文件 »	Add Enforcement Profile						
强制执行配置文件	强制执行配置文件						
配置文件 属性 概要							
模板:	Aruba RADIUS 强制执行						
名称:	task5-guest-profile						
说明:	C						
类型:	RADIUS						
操作:	● 接受 ○ 拒绝 ○ 删除						
设备组列表:	Remove 添加新设备组 View Details Modify Select ↓						

在"属性"选项卡中输入下面参数:

✓ 属性: Radius:Aruba Aruba-User-Role labX-guest (X: 1…6)

配調	記置 » 强制执行 » 配置文件 » Add Enforcement Profile						
强	强制执行配置文件						
Ā	配置文件 属性 概要						
	業型 名称 値						
1.	Radius:Aruba	Aruba-User-Role	=	lab1-guest		Ť	
2	Click to add						

在"概要"选项卡中对配置进行总览:

✓ 概要:查看配置总览,并点击"保存"



配置》强	配置 » 强制执行 » 配置文件 » Add Enforcement Profile							
强制执	虽制执行配置又件							
				Enforcement profile ha	as not been	ı sav	red	
配置文件	属性	概要						
配置文件:								
模板:			Aruba RADIUS 强制执行					
名称:			task5-guest-profile					
说明:								
类型:			RADIUS					
操作:			Accept					
设备组列表	₹:		-					
属性:								
类	¥			名称			值	
1. Ra	dius:Aru	ba		Aruba-User-Role	=		lab1-guest	

第3步: 找到 配置 - > 强制执行 - > 策略 , 点击右侧的 "添加强制执行策略"按钮 , 增加一个强制执行策略:

在"强制执行"选项卡中输入下面参数:

- ✓ 名称: task5-mac-caching-enforcement-policy
- ✓ 默认配置文件: [Deny Access Profile]

配置 » 强制执行 » 策略 » 添加	ha	
强制执行策略		
强制执行规则概要		
名称:	task5-mac-caching-enforcement-policy	
说明:	©	
强制执行类型:	O RADIUS ○ TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ 应用程序 ○ Event	
默认配置文件:	[Deny Access Profile]	添加新强制执行配置文件

在"规则"选项卡中输入下面参数:

- ✓ Conditions: 点击 "Add Rule ", 配置如下参数, 并点击 "保存"
 - 条件: Tips Role MATCHES_ALL guest-role & [User Authenticated]
 - 配置文件名: task5-portal-profile (在第1步中创建的配置文件)



配置»引	虽制执行 » 策略	• 添加						
强制热	执行策略							
强制执	行规则	E						
规则评估	。 算法:	● 选择第一个匹配 ○ 选择所有匹配						
Enforce	ment Policy R	es:						
Co	nditions			Actions				
				Add Rule	Move Up ↑	Move Down ↓	Edit Rule	Remove Rule
规则	编辑器							•
			条件					
π			2011					
20A	3以下所有家件· 类型	名称	运算符		值			
	Ting	Bala	MATCHES ALL	ç	guest-role		Pa, #	1
1.	Tips	KUIE	MATCHES_ALL	[User Authenticated	d]		
2.	Click to ad	••						-
			强制执行配置文件					
配	置文件名:	[RADIUS] task5-guest-profile [Post Authentication] task5-update-endpo Select to Add	nt Move Up ↑ Move Down ↓ Remove					
						保存	ア 取消	

在"概要"选项卡中对配置进行总览:

✓ 概要:查看配置总览,并点击"保存"

配置 » 强制执行 » 策略 » 添加	添加	
强制执行策略		
强制执行规则概要		
强制执行:		
名称:	task5-mac-caching-enforcement-policy	
说明:		
强制执行类型:	RADIUS	
默认配置文件:	[Deny Access Profile]	
规则:		
规则评估算法:	First applicable	
Conditions	Actions	
1. [User Authenticated])	ES_ALL guest-role [RADIUS] task5-guest-profile, [Post Authent	ication] task5-update-endpoint

第4步:找到配置 - > 服务,点击右侧的"添加服务"按钮,增加一个服务:

在"服务"选项卡中配置如下参数:

- ✓ 类型选择: RADIUS Enforcement (Generic)
- ✓ 名称填写: task5-mac-caching-service
- ✓ 更多选项:授权(开启)
- ✓ 服务规则:
 - 1、Connect Client-Mac-Address NOT_EQUALS %{Radius:IETF:User-Name}
 - 2、Radius:Aruba Aruba-Essid-Name EQUALS labX-mac-caching (X: 1……6)



配置 » 服务 » 添加				
服务				
服务认证授权角	色 强制执行 概要			
类型:	RADIUS Enforcement (Generic)			
名称:	task5-mac-caching-service			
说明:	task5-mac-caching认证服务			
	G			
监视模式:	□ 启用以监视无强制执行的网络访问			
更多选项:	☑ 授权 🗌 安全状况遵从 🗌 审计终端主机 🗌 配	置文件端点 🗌 Accounting Proxy		
		服务规则		
匹配项 🔘 任意或 💿 以下戶	所有条件:			
类型	名称	运算符	值	
1. Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}	
2. Radius:Aruba	Aruba-Essid-Name	EQUALS	lab5-mac-caching	Ba 🗇
3. Click to add				

在"认证"选项卡中配置如下参数:

- ✓ 1、认证方法: [PAP]、 [CHAP]、[MSCHAP]
- ✓ 2、认证源:[Local User Repository][Local SQL DB]

配置 » 服务 » 添加			
服务			
服务 认证 授权 角色	图 强制执行 概要		
认证方法:	[PAP] [CHAP] [MSCHAP]	Move Up ↑ Move Down ↓ Remove View Details Modify	添加新认证方法
	Select to Add		
认证题:	[Local User Repository] [Local SQL DB]	Move Up↑ Move Down↓ Remove View Details Modify	添加新认证源
	Select to Add	•	
剥离用户名规则:	 启用以指定以逗号分隔的规则列表,用于剥 	离用户名前缀或后缀	
Service Certificate:	Select to Add 🛟)	View Certificate Details

在"授权"选项卡中配置如下参数:

- ✓ "[Endpoint Repository][Local SQL DB]"
- ✓ "[Time Source][Local SQL DB]"



配置 »丿	服务 » 添	加						
服务								
服务	认证	授权	角色	强制执行	概要			
授权详细	暗息:			从中提取角色	映射属性]授权源(对每个授权源)		
				认证波	l		属性提取自	
				1. [Loca	l User R	pository] [Local SQL DB]	[Local User Repository] [Local SQL DB]	
				从中提取角色 [Endpoints Re [Time Source] Select to A	映射属性的 pository] [Local SC	其他授权源 - .ccal SQL DB] .DB] View Details Modify		添加新认证源

在"角色"选项卡中,暂时不做任何配置(详细内容可以参考高级介绍部分):

✓ 角色映射策略:空

配置 » 服务 » 添加			
服务			
服务认证 角色 强震	則执行 概要		
角色映射策略:	Select +	Modify	添加新角色映射策略
		角色映射策略详细信息	
说明:	-		
默认角色:	-		
规则评估算法:	-		
条件			角色

在"强制执行"选项卡中,配置如下参数:

✓ 强制执行策略:在强制执行策略下拉菜单中找到lab5-mac-caching-enfocement-policy" (即前面步骤 中创建的强制执行策略)

配置 » 服务 » 添加					
服务					
服务 认证 授权 角柱	色 强制执行 概要				
使用缓存的结果:	□ 使用从上一会话中缓存的角色和安全状况属性				
强制执行策略:	task5-mac-caching-enforcement-policy Image: Modify	添加新强制执行策略			
	强制执行策略详细信息				
说明:					
默认配置文件:	[Deny Access Profile]				
规则评估算法:	first-applicable				
条件	条件 强制执行配置文件				
1. (Tips:Role MATCH [User Authenticated]	ES_ALL guest-role]) task5-guest-profile, task5-update-endpoint				

在"概要"选项卡中对配置进行总览:

✓ 概要:查看配置总览,点击"保存"按钮



配置 »	配置 » 服务 » 添加						
服务							
服务	认证	授权	角色	强制执行 概要			
服务:							
类型: RADIUS Enforcement (Generic)							
名称:				task5-mac-caching-s	ervice		
说明:				task5-mac-cachingù	证服务		
监视模	式:			Disabled			
更多选	项:			授权			
						服务规则	
匹配以	下所有条件	:					
	类型				名称	运算符	值
1.	Connecti	on			Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}
2.	Radius:A	ruba			Aruba-Essid-Name	EQUALS	lab5-mac-caching
认证:							
认证方	法:			1. [PAP] 2. [CHAP] 3. [MSCHAP]			
认证源	:			[Local User Reposito	ry] [Local SQL DB]		
剥离用	户名规则:			-			
Servio	e Certifica	ate:		-			
授权:							
授权详	细信息:			 [Endpoints Repos [Time Source] [Lo 	tory] [Local SQL DB] ical SQL DB]		
角色:							
角色映	射策略:			-			
强制执	7 :						
使用缓	存的结果:			Disabled			
强制执	行策略:			task5-mac-caching-	enforcement-policy		

6.3.3 添加 mac 认证服务

第1步: 找到 配置 - > 强制执行 - > 配置文件,点击右侧的"添加强制执行配置文件"按钮,增加一个强制执行 配置文件:

在"配置文件"选项卡中输入下面参数:

- ✓ 模板:基于radius的强制执行
- ✓ 名称: task5-return-username



配置 » 强制执行 » 配置文件 »	Add Enforcement Profile
强制执行配置文件	
配置文件 属性 概要	
模板:	基于 RADIUS 的强制执行 🗘
名称:	lab5-return-username
说明:	mac认证阶段给控制器返回portal认证阶段的用户名
类型:	RADIUS
操作:	 ● 接受 ○ 拒绝 ○ 删除
设备组列表:	Remove 添加新设备组 View Details Modify

在"属性"选项卡中输入下面参数:

✓ 属性: Radius:IETF User-Name = %{Endpoint:Username}

配置 » 强制执行 » 配置文件 » Add Enforcement Profile					
强制执行配置文件					
配置文件 属性 概要					
类型	名称		<u>ش</u>		
类型 1. Radius:IETF	名称 User-Name	=	值 %{Endpoint:Username}	Ē	Ť

在"概要"选项卡中对配置进行总览:

✓ 概要:查看配置总览,并点击"保存"

配置 » 强制执行 » 配置文件 » Add Enforcement Profile					
强制执行配置文件					
		Enforcement profile has not been say	ved		
配置文件 属性 概要					
配置文件:		_			
模板:	基于 RADIUS 的强制执行				
名称:	lab5-return-username				
说明:	mac认证阶段给控制器返回portal认证阶段的用户名				
类型:	RADIUS	-			
操作:	Accept				
设备组列表:	-				
属性:					
类型	名称		值		
1. Radius:IETF	User-Name	=	%{Endpoint:Username}		

第2步: 找到 配置 - > 强制执行 - > 策略 , 点击右侧的 "添加强制执行策略"按钮 , 增加一个强制执行策略:

在"强制执行"选项卡中输入下面参数:

✓ 名称: task5-mac-enforcement-policy

配置 » 强制执行 » 策略 » 添加	R置 » 强制执行 » 策略 » 添加						
强制执行策略	强制执行策略						
强制执行 规则 概要							
名称:	task5-mac-enforcement-policy						
说明:							
强制执行类型:	SADIUS ○ TACACS+ ○ WEBAUTH (SNI)	MP/Agent/CLI/CoA) 🔿 应用程序 🔿 Event					
默认配置文件:	[Deny Access Profile] View Details	Modify	添加新强制执行配置文件				

在"规则"选项卡中输入下面参数:

- ✓ Conditions: 点击 "Add Rule ", 配置参数如下, 并点击保存
 - 条件:
 - 1.Tips Role EQUAL [User Authenticated]
 - ◆ 2.Authorization:[Time Source] Now DT LESS_THAN %{Endpoint:MAC-Auth Expiry}
 - ◆ 3.Authorization:[Endpoints Repository] Unique-Device-Count EXISTS
 - ◆ 4.Endpoint Guest Role ID EQUALS guest-role
 - 配置文件名:
 - ◆ task5-guest-profile (在第1步中创建的配置文件)
 - ◆ task5-return-username (在第1步中创建的配置文件)

» 强制执	1行»策略»添加									
山执行的	策略									
执行	规则概要									
平估算法:	: 选择第一	-个匹配 🔘 选择所有匹配								
cement	Policy Rules:									
Conditi	ions				Actions					
						Add Rule	Move Up ↑	Move Down ↓	Edit Rule	Remo
规则编	鳥輯器 ←									8
					条件					
元配	以下所有条件:				2011					
Eard	类型		名称		运算符		值			
1.	Tips		Role		EQUALS		[User Authen	ticated]	Ē	8
2.	Authorization: [Time Sour	rce]	Now DT		LESS_THAN		%{Endpoint:	MAC-Auth Expiry}		Ť
3.	Authorization: [Endpoints	Repository]	Unique-Devi	ice-Count	EXISTS					Ť
4.	Endpoint		Guest Role I	(D	EQUALS		guest-role			Ť
5.	Click to add									
				强制	 执行配置文件					
配置	宜文件名: [R [R	ADIUS] task5-guest-profile ADIUS] task5-return-userna	me	Move Up ↑ Move Down ↓ Remove						
	-	-Select to Add		\$						
									保存 面	∀消
									49	1112 I

在"概要"选项卡中对配置进行总览:

✓ 概要:查看配置总览,点击"保存"按钮

配置	配置 » 强制执行 » 策略 » 添加						
强制	强制执行策略						
				Enforcement policy has not been saved			
强制	山执行	规则	概要				
强制拔	行:						
名称:				task5-mac-enforcement-policy			
说明:							
强制拐	机行类型	:		RADIUS			
默认曹	记置文件			[Deny Access Profile]			
规则:							
规则议	平估算法	::		First applicable			
	Conditions Actions						
1.	(Tips:Role EQUALS [User Authenticated]) AND (Authorization:[Time Source]:Now DT LESS_THAN %{Endpoint:MAC-Auth Expiry})) AND (Authorization:[Endpoint:Repository]:Unique-Device-Count EXISTS) AND (Endpoint:Guest Role ID EQUALS guest-role) [RADIUS] lab5-guest-profile, [RADIUS] lab5-return-username						

第3步:找到配置 - > 服务,点击右侧的"添加服务"按钮,增加一个服务:

在"服务"选项卡中配置如下参数:

- ✓ 类型选择: RADIUS Enforcement (Generic)
- ✓ 名称填写: lab5-mac-service
- ✓ 服务规则:

配置 » 服务 » 添加

- 1、Connect Client-Mac-Address EQUALS %{Radius:IETF:User-Name}
- 2、Radius:Aruba Aruba-Essid-Name EQUALS labX-mac-caching (X: 1……6)

服务	5				
服务	务 认证 授权 角色	e 强制执行 概要			
类型:	:	RADIUS Enforcement (Generic)			
名称:	:	lab5-mac-service			
说明:	:	lab5 mac认证服务 G			
监视相	模式:	□ 启用以监视无强制执行的网络访问			
更多词	选项:	☑ 授权 □ 安全状况遵从 □ 审计终端主机 □ 酮	置文件端点 🗌 Accounting Proxy		
			服务规则		
匹配功	项 🔘 任意或 💿 以下所	有条件:			
	类型	名称	运算符	值	
1.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}	i i
2.	Radius:Aruba	Aruba-Essid-Name	EQUALS	group1-mac-caching	E T
3.	Click to add				

在"认证"选项卡中配置如下参数:

- ✓ 1、认证方法: [MAC AUTH]
- ✓ 2、认证源: [Endpoint Repository][Local SQL DB]



記録。 昭冬 & 沃 山							
服务							
服务 认证 角色 强制 认证方法:	JI执行 概要 [MAC AUTH]	Move Up↑ 添加新认证 Move Down↓ Remove View Details	方法				
	CSelect to Add	Modify					
1A 1E 38 :	[Endpoints Repository] [Local SQL DB]	Move Up ↑ 添加新心 Move Down ↓ Remove View Details Modify	证源				
	Select to Add	\$					
剥离用户名规则:	启用以指定以逗号分隔的规则列表,用于剥离	离用户名前缀或后缀					
Service Certificate:	Select to Add	View Certificate De	tails				

在"授权"选项卡中配置如下参数:

- ✓ "[Endpoint Repository][Local SQL DB]"
- ✓ "[Time Source][Local SQL DB]"

配置 »	服务 » 添	加					
服务							
服务	认证	授权 🧌	色	强制执行	概要		
授权详细	田信息:		Ж	中提取角色明	映射属性	的授权源(对每个授权源)	
				认证源		属性提取自	
			1.	[Endp	oints R	pository] [Local SQL DB] [Endpoints Repository] [Local SQL DB]	_
) [E [T	中提取角色的 ndpoints Rep ime Source] -Select to Ac	<u>映射属性</u> oository] [Local SC	<u>ol其他授权源</u> - [Local SQL DB] LL DB] View Details Modify	源

在"角色"选项卡中,暂时不做任何配置(详细内容可以参考高级介绍部分):

✓ 角色映射策略:空

配置 » 服务 » 添加			
服务			
服务认证 角色 强制	制执行 概要		
角色映射策略:	Select	Modify	添加新角色映射策略
		角色映射策略详细信息	
说明:	-		
默认角色:	-		
规则评估算法:	-		
条件		角色	

在"强制执行"选项卡中,配置如下参数:

✓ 强制执行策略:在强制执行策略下拉菜单中找到task5-mac-enfocement-policy" (即前面步骤中创建的 强制执行策略)

配置 » 服务 » 添加					
服务					
服务 认证 授权 角色 强制执行 概要					
使用缓存的结果: 🗌 使用从上一会话中缓存的角色和安全状况属性					
强制执行策略: task5-mac-enforcement-policy \$ Modify	添加新强制执行策略				
强制执行策略详细信息					
说明:					
默认配置文件: [Deny Access Profile]					
规则评估算法: first-applicable					
条件 强制执行配置文件					
(Tips:Role EQUALS [User Authenticated]) AND (Authorization:[Time Source]:Now DT LESS_THAN %{Endpoint:MAC-Auth Expiry}) AND (Authorization:[Endpoints Repository]:Unique-Device-Count EXISTS) AND (Endpoint:Guest Role ID EQUALS guest-role)	lab5-guest-profile, lab5-return-username				

在"概要"选项卡中对配置进行总览:

✓ 概要:查看配置总览,点击"保存"按钮

配置 »	配置 » 服务 » 添加							
服务	服务							
	Service has not been saved							
服务	认证 授权	角色	强制执行概要					
服务:								
类型:		F	ADIUS Enforcement (Generic)					
名称:		t	ask5-mac-service					
说明:		t	ask5-mac认证服务					
监视模	式:	[Disabled					
更多选	项:	ł	受权					
				服务规则				
匹配以	下所有条件:							
	类型		名称	运算符	(ii			
1.	Connection		Client-Mac-Addr	ess EQUALS	%{Radius:IETF:User-Name}			
2.	Radius:Aruba		Aruba-Essid-Nar	ne EQUALS	lab1-mac-caching			
认证:								
认证方	法:	[MAC AUTH]					
认证源	:	[Endpoints Repository] [Local SQL DB]					
剥离用	户名规则:	-						
Servio	e Certificate:	-						
授权:								
授权详	细信息:	1	[Endpoints Repository] [Local SQL DB] 2. [Time Source] [Local SQL DB]					
角色:								
角色映	射策略:	-						
强制执	;							
使用缓	存的结果:	[Disabled					
强制执	行策略:	t	ask5-mac-enforcement-policy					



6.4 控制器配置

6.4.1 添加无线信号

第1步: 使用 Web 方式登录到 Mobility Master (10.X.10.11), 找到 Managed Networks - > labX -> Configuration -> WLANs (X : 1 ·····6), 点击 "+"进入创建一个新的无线配置向导

Dashboard	WLANs 1
Configuration	NAME (SSID)
WLANs	
Roles & Policies	
Access Points	
AP Groups	
Authentication	+
Services	
	Dashboard Configuration WLANs Roles & Policies Access Points AP Groups Authentication Services

第2步:配置 SSID 名称、主要用途、在哪个 AP-Group 广播、转发模式

- ✓ Name (ssid): labX-mac-caching(X : 1…6)
- ✓ Primary usage: Guest
- ✓ Broadcast on: lab1-group
- ✓ Forwarding mode: Tunnel

New WLAN

(General	VLANs	Security	
Name (ssid):	lab1-mac-caching			
Primary usage:	🔵 Employee 🛛 💿 Guest			
	Select AP Groups 💙			
Broadcast on:	│ default ✔ lab1-group			
Forwarding mode:	Tunnel 🗸			

第3步: 配置 VLAN

✓ VLAN: wireless-user-vlan



New WLAN									
General	VLANS	Security	Access						
VLAN: wireless-user-vlan VLAN details									

第4步:配置 portal 认证方式

- ✓ Auth servers: cppm
- ✓ CPPM host: 10.X.50.41 (X: 1…6)
- ✓ CPPM page: /guest/guest-login.php (在4.3.3 第3步中创建的页面)

New WLAN

General	VLANs		Security	Access
ClearPass or other external captive portal —— Internal captive portal with authentication Internal captive portal with email registration Internal captive portal, no auth or registration	Captive Porta	cppm		
No Captive Portal	CPPM host: CPPM page: Redirect URL:	10.1.50.41 /guest/guest-login.pl		

第5步:完成向导配置



6.4.2 修改 portal 认证配置

找到Managed Network - > labX -> Configuration -> Authentication -> L3Authentication 点击 "Captive Portal Authentication",选中 "labX-mac-caching cppm prof" (X:1……6),修改如下参数

- ✓ Use HTTP for authentication: 启用
- ✓ Login page: http://10.X.50.41/guest/guest-login.php (X:1…6) (https 修改为 http)

(配置截图略, 详见4.4.2)

6.4.3 添加 MAC 认证

第1步: 找到 Managed Networks - > labX -> Configuration -> Authentication, 在右侧点击 "AAA Profile", 找到 "AAA Profile: labX-mac-caching aaa prof" (X:1……6)

Managed Network > lab1 >						
Dashboard	Auth Servers	AAA Profiles	L2 Authentication	L3 Authentication	User Rules	Advanced
Configuration						
WLANs	AAA Profiles					
Roles & Policies	⊕ ⊟	NoAuthAAAProfile				
Access Points	⊕ ⊟	default				
AP Groups	⊕ ⊟	default-dot1x				
Authentication	⊕ ⊟	default-dot1x-psk				
Services	⊕ ⊟	default-iap-aaa-pro	f			
Interfaces	⊕ □	default-mac-auth				
Controllers	÷ 🖬	default-open				
System	⊕ ⊟	default-tunneled-us	se			
Tasks	⊕ ⊟	default-xml-api				
Maintenance	⊕ ⊟	lab1-guest-register_				
	⊕ ⊡	lab1-mac-caching_a	iaa	ش		
	⊕ ⊟	lab1-mac_aaa_prof				

第2步:修改 MAC Authentication Profile为"labX-mac"(X:1…6),点击右下角"Submit"



AAA Profiles	MAC Authentication Profile: lab1-mac	
G default-tunneled-use default-xml-api	MAC Authentication Profile: lab1-mac 💙	
 →	Delimiter:	none 💙
⊖ 🖻 lab1-mac-caching_aaa	Case:	lower 💙
802.1X Authentication	Max Authentication failures:	0
🕒 802.1X Authentication Server Group	Reauthentication:	
MAC Authentication	Reputhentication Interval:	26400
MAC Authentication Server Group	Readification interval.	80400 Sec
RADIUS Accounting Server Group	Use Server provided Reauthentication Interval:	

第3步: 修改 MAC Authentication Server Group 为 "labX-mac-caching_dot1_svg" (X: 1…6), 点击右 下角 "**Submit**"

Auth Servers AAA Profiles L2 Authentication	L3 Authentication User Rules Advanced
AAA Profiles	Server Group: lab1-mac-caching_dot1_svg
⊕	Server Group: lab1-mac-caching_dot1_svg 💙
\ominus 📑 default-xml-api	1
	Fail Through:
⊖ 🕒 lab1-mac-caching_aaa	Load Balance:
802.1X Authentication	
802.1X Authentication Server Group	
MAC Authentication	
🕒 MAC Authentication Server Group	
🖻 RADIUS Accounting Server Group	
RFC 3576 server	
TXML API server	

6.4.4 添加计费

第1步:修改"RADIUS Accounting Server Group"为"labX-mac-caching_dot1_svg"(X: 1…6),点击 右下角"**Submit**"

uth Servers AAA Profiles L2 Authentication	L3 Authentication User Rules Advanced
AAA Profiles	Server Group: lab1-mac-caching_dot1_svg
⊕	Server Group: lab1-mac-caching dot1_svg
④	
	Fail Through:
⊖ 🖪 lab1-mac-caching_aaa	Load Balance:
802.1X Authentication	
802.1X Authentication Server Group	
MAC Authentication	
MAC Authentication Server Group	
📑 RADIUS Accounting Server Group	
🕞 RFC 3576 server	
TXML API server	

第2步: 点击右上角 "Pending Changes" 保存配置

aruba	MOBILITY MASTER lab1-mm-1	CONTROLLERS ACCESS POINTS CLIENTS ALERTS ∅ 2 0 ∅ 1 0 😤 0 ǿ 0 △ 0	③ admin ∽
Managed Network	< > lab1 >		Pending Changes 🗘
~			

6.5 验证结果

第1步: 远程登录到测试终端 10.X.50.102(X: 1…6),终端连接到 SSID: lab1-mac-caching

✓ 登录到无线控制器,通过show user命令,观察无线控制器上终端状态

(lab1-md2) [MDC] This operation ca	#show user an take a while	depending	on number of users. Please be	e patient							
Users											
		waa de	0-2-			1000 (S.S.S.	10			B	·
de Type Host I	Name User Type	Name	KOLE	Age(d:n:m)	Auth	VPN LINK	AP name	Roaming			Porward mo
CONTRACTOR OF STREET											
											Strengt Com
10.1.20.102 7c:	7a:91:46:52:b7		lab1-mac-caching-guest-logon				94:b4:0f:c1:3f:e0		lab1-mac-caching/94:b4:0f:93:fe:13/a-VHT	lab1-mac-caching_aaa_prof	tunnel

第2步: 登录到 ClearPass, 找到 监控 - > Live Monitoring - > 访问跟踪器, 查看认证记录 (1/3),

✓ 此时我们发现匹配到了task5-mac-service,认证失败



aruba			Clear	Pass Policy Manage	r		Menu 🗮	
■ 面板 ■ 型規	2 単数 2 送税 × Live Monitoring × 访问跟踪器 1 访问跟踪器 Oct 15, 2019 17:45:30 CST							
→ Live Monitoring 小学订回照算器 - 学订费 - 学可局Guard 活动 - 型 分析和趋势	The Acc	cess Tracker page provide All Requests]	es a real-time display of per	-session access activity on the sele (10.1.50.41)	ected server or domain.	fore Today	编辑	
系统监视 글 → Profile and Network Scan → 学审计查看器	过滤器: #	Request ID Server	¢ 包含 ↓ Source	Go Clear Filter	Service	Login Status	显示 20 🔹 记录 Request Timestamp 🔹	
	1.	10.1.50.41	RADIUS	7c7a914652b7	task5-mac-service	REJECT	2019/10/15 17:44:38	

- 第3步: 远程登录到测试终端 10.X.50.102 (X: 1…6) , 打开浏览器
 - ✓ 输入任意URL,在弹出的登录页面中输入用户名:guest,密码:aruba123,点击登录。

arub	a	ClearPass Guest
Please logi	n to the network usina your user	name and password.
	Login	
Username:	guest	

Contact a staff member if you are experiencing difficulty logging in.

Log In

 ✓ 登录到ClearPass, 找到 监控 - > Live Monitoring - > 访问跟踪器, 查看认证记录 (2/3), 此时我们 发现匹配到task5-mac-caching-service, 认证成功。

aruba			ClearPas	s Policy Manage	r		Menu 🔜
6 ■ 面板 0	监视 » L	ive Monitoring » 访	问跟踪器				
😰 监视 📀	访问跟	退踪器 Oct 15, 20:	19 17:46:00 CST				📀 自动刷新
	The Acc	ess Tracker page p	rovides a real-time display of per-session	on access activity on the sele	ected server or domain.		
·····································	T [A	ll Requests]	Lab1-CPPM-1 (10.1	.50.41)	15 Last 1 day before	e Today	编辑
- 🔜 系统监视 🗉 🛃 Profile and Network Scan	过滤器:〔	Request ID	♦ 包含 ♦	Go Clear Filter	2		显示 20 🛟 记录
	#	Server	Source	Username	Service	Login Status	Request Timestamp 🔹
—— 🎩 事件查看器	1.	10.1.50.41	RADIUS	guest	task5-mac-caching-service	ACCEPT	2019/10/15 17:46:00
	2.	10.1.50.41	RADIUS	7c7a914652b7	task5-mac-service	REJECT	2019/10/15 17:44:38

✓ 点击认证成功记录,在"概要"选项卡中观察,看看能看到哪些信息。

8

请求详细信息			
概要 输入 输出 计	费		
会话标识符:	R0000025-01-5da59558		
日期和时间:	Oct 15, 2019 17:46:00 CST		
终端主机标识符:	7C7A914652B7 (SmartDevice / Android / Android)		
用户名:	guest		
访问设备 IP/端口:	10.1.10.22:0		
系统安全状况状态:	UNKNOWN (100)		
	所用策略 -		
服务:	task5-mac-caching-service		
认证方法:	PAP		
认证源: Local:localhost			
授权源: [Local User Repository], [Endpoints Repository], [Time Source]			
角色:	[User Authenticated], guest-role		
强制执行配置文件:	task5-update-endpoint, task5-guest-profile		
服务监视模式:	Disabled		
Online Status:	Online		
I ◄ Showing 1 of 1-18 reco	ords ▶ ▶ 更改状态 Show Configuration 导出 显示日志 关闭		

✓ 在"输入"选项卡中观察,看看能看到哪些信息。

请求详细信息

户名:	guest		
端主机标识符:	7C7A914652B7	(SmartDevice / Android / Android)	
问设备 IP/端口:	10.1.10.22:0		
RADIUS 请求			
Radius:Aruba:A	ruba-AP-Group	lab1-group	
Radius:Aruba:A	ruba-Device-Type	Win 8	
Radius:Aruba:A	ruba-Essid-Name	lab1-mac-caching	
Radius:Aruba:A	ruba-Location-Id	94:b4:0f:c1:3f:e0	
Radius:IETF:Ca	lled-Station-Id	000B86DD2F00	
Radius:IETF:Calling-Station-Id		7C7A914652B7	
Radius:IETF:Fra	amed-IP-Address	10.1.20.102	
Radius:IETF:NA	S-IP-Address	10.1.10.22	
Radius:IETF:NA	S-Port	0	
Radius:IETF:NA	S-Port-Type	19	
Radius IFTF Se	rvice-Tvne	1	

✓ 点击"输出"选项卡,并观察,看看能看到哪些信息。



概要 输入 输出 计费 强制执行配置文件: task5-update-endpoint, task5-guest-profile 系统安全状况状态: UNKNOWN (100) 审计安全状况状态: UNKNOWN (100) Thtge UNKNOWN (100) Endpoint:Guest Role ID guest Radius:Aruba:Aruba-User-Role Iab1-guest Status-Undate:Endpoint Known	ず求详细信息			
强制执行配置文件: task5-update-endpoint, task5-guest-profile 系统安全状况状态: UNKNOWN (100) 审计安全状况状态: UNKNOWN (100) C C Endpoint:Guest Role ID guest-role Endpoint:MAC-Auth Expiry 2019-10-16 17:00:00 Endpoint:Username guest Radius:Aruba:Aruba-User-Role lab1-guest Status-Undate:Endpoint Known	概要 输入	输出计费		
系统安全状况状态: UNKNOWN (100) 审计安全状况状态: UNKNOWN (100) RADIUS 响应 Endpoint:Guest Role ID guest-role Endpoint:MAC-Auth Expiry 2019-10-16 17:00:00 Endpoint:Username guest Radius:Aruba:Aruba-User-Role lab1-guest Status-Lindate:Endpoint Known	强制执行配置文件:	task5-update-e	ndpoint, task5-guest-profile	
审计安全状况状态: UNKNOWN (100) RADIUS 响应 Endpoint:Guest Role ID Endpoint:MAC-Auth Expiry 2019-10-16 17:00:00 Endpoint:Username guest Radius:Aruba:Aruba-User-Role lab1-guest Status-Indate:Endpoint Known	系统安全状况状态:	UNKNOWN (10	0)	
RADIUS 响应 Image: Constraint of the second seco	审计安全状况状态:	UNKNOWN (10	0)	
Endpoint:Guest Role ID guest-role Endpoint:MAC-Auth Expiry 2019-10-16 17:00:00 Endpoint:Username guest Radius:Aruba:Aruba-User-Role lab1-guest Status-Undate:Endpoint Known	RADIUS 响应			◙
Endpoint:MAC-Auth Expiry 2019-10-16 17:00:00 Endpoint:Username guest Radius:Aruba-User-Role lab1-guest Status-Undate:Endpoint Known	Endpoint:Guest	Role ID	guest-role	
Endpoint:Username guest Radius:Aruba:Aruba-User-Role lab1-guest Status-Undate:Endpoint Known	Endpoint:MAC-Auth Expiry		2019-10-16 17:00:00	
Radius:Aruba:Aruba-User-Role lab1-guest	Endpoint:Username		guest	
Status-Indate-Endpoint Known	Radius:Aruba:Aruba-User-Role		lab1-guest	
Status opurce intomi	Status-Update:	Endpoint	Known	

I ◄ Showing 1 of 1-18 records ► ►I

更改状态 Show Configuration 导出 显示日志 关闭

8

✓ 点击"计费"选项卡,并观察,看看能看到哪些信息。 请求详细信息

概要 输入	输出 计费						
客户会话 ID:	guest7C7A	914652B7-5DA5F972-8118E					
开始时间戳:	Oct 15, 201	19 17:46:00 CST					
结束时间戳:	结束时间戳: Still Active						
状态:	Active						
终止原因:	-						
服务类型:	-						
认证会话数:	1						
网络详细信息		Θ					
NAS IP 地址:		10.1.10.22:0					
NAS 端口类型:		Wireless-802.11					
呼叫站 ID:		7C7A914652B7					
所呼叫站 ID:		000B86DD2F00					
分帧 IP 地址:		10.1.20.102					
Framed IPv6 A	ddress:	-					
帐户认证:		RADIUS					
I ◄ Showing 1 of	f 1-18 record	Is ► ► 更改状态 Show Configuration 导出 显示日志 关闭					



	✓ 登录到 CPPM,找到 配置 -	>	端点,	点击	"属性"	,	查看终端属性	Ē
编辑	端点							8
1	端点 属性 指纹 Policy Cache							
	属性		值					
1.	Guest Role ID	=	guest-ro	ole				Ť
2.	MAC-Auth Expiry	=	2019-10	0-16 17:0	0:00			Ť
3.	Username	=	guest					Ť
4.	Click to add							

✓ 登录到用户所在MD: 10.X.10.11/10.X.10.12 (X: 1…6) , 通过show user命令查看用户状态

(lab1-md1) [MDC] #show user This operation can take a while depending on number of users. Please be patient										
Users										
IP me User Type	МАС	Name	Role	Age(d:h:m)	Auth	VPN link	AP name			
 10.1.20.102 7c:7	a:91:46:52:b7	guest	 lab1-guest	00:00:14	 Web		 94:b4:0f:c1:3f:e0			
WIRELESS										

第4步:验证无感知认证,SSH 登录到 MM: 10.X.50.11 (X: 1…6)

✓ 查看当前用户在那台控制器上:

(lab1-mm-1)	[mynode] #show glob	al-user-	table list			
Global Users						
IP	MAC	Name	Current switch	Role	Auth	AP name
10.1.20.102	7c:7a:91:46:52:b7	guest	10.1.10.11	lab1-guest		94:b4:0f:c1:3f:e0
✓ 登录到	用户所在控制器10.1.10).11,将用	目户下线。			
(lab1-mm-1)	[mynode] #logon 10.1	.10.11				
(lab1-md1) [M	IDC] #aaa user delet	e mac 70	c:7a:91:46:52:b7			

1 users deleted

✓ 通过 "show user" 查看用户在线状态



(la Thi	b1-md1) [l s operatio	MDC] #show user on can take a while	e dependin	g on number c	of users. Ple	ase be	e patient .	
Use	rs							
me	IP User Type	MAC e	Name	Role	Age(d:h:m)	Auth	VPN link	AP name
 10.	 1.20.102 WIRELESS	 - 7c:7a:91:46:52:b7	guest	 lab1-guest	00:00:00	MAC		 94:b4:0f:c1:3f:e0
	✓ 登录到	到ClearPass,找到 <u>出</u>		e Monitoring	y - > 访问跟 跟	;器, ī	查看认证记录	录(3/3),此时我们

发现匹配到task5-mac-service,认证成功。

aruba				Menu					
E = 面板	当視 > Live Monitoring > 访问跟踪器 う 访问跟踪器 Oct 15, 2019 17:55:37 CST								
 ■ Live Monitoring ■ 計過設算器 ■ 计费 ■ OnGuard 活动 ■ 分析和趋势 	The Acc	xess Tracker page provides a	real-time display of per-session a	access activity on the selected se	erver or domain.	P Today	编辑		
- ■ 系统监视	过滤器:[#	Service Server	● 包含 争 Source	Go Clear Filter Username	Service	Login Status	显示 20 🛟 记录 Request Timestamp +		
—學事件查看器 —學數据过滤器 —學 Blacklisted Users	1. 2. 3.	10.1.50.41 10.1.50.41 10.1.50.41	RADIUS RADIUS RADIUS	guest guest 7c7a914652b7	task5-mac-service task5-mac-caching-service task5-mac-service	ACCEPT ACCEPT REJECT	2019/10/15 17:54:57 2019/10/15 17:46:00 2019/10/15 17:44:38		

✓ 点击这条认证记录, 查看"概要"选项卡, 看看有哪些信息

请求详细信息

概要 输入 输出 计野	男
登录状态:	ACCEPT
会话标识符:	R0000026-01-5da59771
日期和时间:	Oct 15, 2019 17:54:57 CST
终端主机标识符:	7C7A914652B7 (SmartDevice / Android / Android)
用户名:	guest
访问设备 IP/端口:	10.1.10.22:0
系统安全状况状态:	UNKNOWN (100)
	所用策略 -
服务:	task5-mac-service
认证方法:	MAC-AUTH
认证源:	Local:localhost
授权源:	[Endpoints Repository], [Time Source]
角色:	[User Authenticated]
强制执行配置文件:	task5-guest-profile, task5-return-username
服务监视模式:	Disabled
I ≤ Showing 1 of 1-7 record	rds ▶ ▶ 更改状态 Show Configuration 导出 显示日志 关闭

✓ 查看"输入"选项卡,观察获取到的radius信息



城安 那八 制 五	ΗЩ				
护名:	guest				
§端主机标识符:	7C7A914652B7	(SmartDevice)	/ Android / Android)		
问设备 IP/端口:	10.1.10.22:0				
RADIUS 请求					
受权属性					
Authorization:[Endpoi	nts Repository]:Uniq	ue-Device-Count	1		
Authorization:[Time S	ource]:Now DT		2019-10-15 17:00:00)	
Authorization:[Time S	ource]:One Day DT		2019-10-16 17:00:00)	
Authorization: [Time S	ource]:One Month D	т	2019-11-15 17:00:00)	
Authorization:[Time S	ource]:One Week D	Г	2019-10-22 17:00:00)	
Authorization: [Time S	ource]:Six Months D	т	2020-04-15 17:00:00)	
计算属性					
Endpoint Attributes ◄ Showing 1 of 1-7 re	ecords ► ►I	更改状态	Show Configuration	导出 显示日志	关闭
■ Showing 1 of 1-7 re ✓ 查看 "输 求洋细信息	ecords▶▶ 出"选项卡,	_{更改状态} 观察ClearF	Show Configuration Pass向控制器返	^{导出 显示日志} 回到radius信息	关闭
Endpoint Attributes ◀ Showing 1 of 1-7 re ✓ 查看 "输 求详细信息 概要 输入 輸出	ecords▶▶ 出"选项卡, ^{计费}	_{更改状态} 观察ClearF	Show Configuration Pass向控制器返	^{导出 显示日志} 回到radius信息	关闭 見
Endpoint Attributes ✓ 查看 "输 求详细信息 概要 输入 输出 副执行配置文件: task5	ecords ▶ ► 出"选项卡, 计费 -guest-profile, task5	更改状态 观察ClearF	Show Configuration Pass向控制器返	导出 显示日志 回到radius信息	关闭 J
 ▲ Showing 1 of 1-7 re ✓ 查看 "输 水详细信息 概要 输入 输出 副执行配置文件: task5 系统安全状况状态: UNKK 	ecords ▶ ▶I 出"选项卡, 计费 i-guest-profile, task5 NOWN (100)	更改状态 观察ClearF	Show Configuration Pass向控制器返	^{导出 显示日志} 回到radius信息	关闭
■ Showing 1 of 1-7 re ✓ 査看 "输 水洋細信息 概要 輸入 輸出 副执行配置文件: task5 系統安全状況状态: UNKM 計安全状況状态: UNKM	ecords ▶ ►I 出"选项卡, 计费 i-guest-profile, task5 NOWN (100) NOWN (100)	更改状态 观察ClearF	Show Configuration PASS向控制器返	导出 显示日志 回到radius信息	Ki ka
 ▲ Showing 1 of 1-7 re ✓ 查看 "输 ★ 增加 ★ 输出 株要 输入 输出 翻执行配置文件: task5 系详细信息 就详细信息 就详细信息 取详细信息 取详细信息 取计组合表 取计组合表 取计组合表 取计组合表 取计组合表 取时目示 取时目示 	acords ► ►I 出"选项卡, 计费 5-guest-profile, task5 NOWN (100) NOWN (100)	更改状态 观察ClearF	Show Configuration Pass向控制器返	导出 显示日志 回到radius信息	R 天 見
A Showing 1 of 1-7 re ✓ 査看 "输 求详細信息 概要 输入 输出 副期执行配置文件: task5 系统安全状况状态: UNKM 同计安全状况状态: UNKM RADIUS 响应 Radius:Aruba:Aruba-U Radius:IETF:User-Nar	ecords ► ►I 估出"选项卡, 计费 5-guest-profile, task5 NOWN (100) NOWN (100) User-Role lab1-gues me guest	更改状态 观察ClearF	Show Configuration Pass向控制器返	导出 显示日志 回到radius信息	关闭 見
Endpoint Attributes ▲ Showing 1 of 1-7 re ✓ 查看 "输 求详细信息 概要 输入 输出 副执行配置文件: task5 系统安全状况状态: UNKM RADIUS 响应 Radius:Aruba:Aruba-U Radius:IETF:User-Nar ✓ 查看 "计	ecords ► ►I 出"选项卡, 计费 5-guest-profile, task5 NOWN (100) User-Role lab1-gues me guest 安"选项卡,	更改状态 观察ClearF return-username tt 	Show Configuration Pass向控制器返 。	导出 显示日志 回到radius信息	关闭 引 。

概要 输入	输出 计费		
客户会话 ID:	guest7C7A	914652B7-5DA5FB8B-4FE19	1
开始时间戳:	Oct 15, 20	19 17:54:57 CST	
结束时间戳:	Still Active		
状态:	Active		
终止原因:	-		
服务类型:	-		
认证会话数:	1		
网络详细信息		0	
NAS IP 地址:		10.1.10.22:0	1
NAS 端口类型:		Wireless-802.11	
呼叫站 ID:		7C7A914652B7	
所呼叫站 ID:		000B86DD2F00	
分帧 IP 地址:		10.1.20.102	
Framed IPv6 A	ddress:	-	
帐户认证:		-	
I < Showing 1 o	of 1-7 records	S ▶ ▶ 更改状态 Show Configuration 导出 显示日志 关闭	



7 TASK6:ARUBA 控制器集成 CPPM 实现访客自注册认证

7.1 用户需求

客户希望在无线覆盖的区域实现便捷的访客接入,IT管理人员无需事先创建访客账号,而是让访客能够现场通过 提交相关的访客信息来完成自注册的方式获得账号和密码,在该访客账号激活前,需要事先经过审核人的批准后 才能被激活和使用,从而确保真实的访客来使用无线网络。

7.2 实现思路

答案详见附录

✓ 首先我们需要思考下,访客的自注册应该采用哪种认证方式

答案:______

✓ 针对该认证方式,我们需要思考下还需要为无线网络新增什么网元,即需要针对无线网络来设计什么样的认证服务器呢?

答案:

✓ 针对访客自注册认证,我们需要思考下,你对该认证方式的完整流程熟悉吗?

答案:______

7.3 ClearPass 配置

7.3.1 添加 SMTP 信息

第1步:通过网页浏览器来访问ClearPass的管理IP(10.X.50.41) (X:1……6),从而进入到welcome行动页面, 点击ClearPass Policy Manager 模块,从而进入到策略管理页面。



← → C ▲ Not secure 10.2.50.41/tips/welcome.action 器 Apps ● 网址大全 ※ 百度 ● 聚划算 ● 天漫唱选 ● 京	东商城 🐟 挂机剧宝 🚱 —77999级	· ③ 超变态传奇 ④) 淘宝优惠券 🕝 大3	(何) 🚱 ClearPass Policy Ma	ClearPass Policy Ma	msn (2)	M msn	Q \$	0
ruba						-			
		Clear	es VPN						
_	AAA/Policy Management	Device G Onboarding Mana	uest Device regement Health	Security Exchange					
2	ClearPass Policy Manager Role-based Policies, Enterprise-grade AA Profiling	A with Device	ClearPass	Guest					

第2步: 在策略管理页面中, 打开 管理 - > 外部服务器- > 信息设置, 在右边的SMTP服务器中配置相应的SMTP 设置, 点击 保存按钮, 点击 Send Test Email 测试SMTP服务器是否设置成功, 在 Send Test Email 窗口 输入收件人Email地址和测试内容, 点击 Send Email, 当提示 Successfully sent test email to 表示发送成 功。

在SMTP配置窗口中, 输入下面的参数:

- ✓ 服务器名称: smtp.126.com (这里就是管理员的SMTP服务器地址)
- ✓ 用户名: 邮箱登录账号
- ✓ 密码:邮箱登录密码

© 版权所有 2015 Aruba Networks。保留所有权利。

✓ 默认发件人地址:用来发邮件的地址

aruba		Clea	rPass Policy Mana	ager			Menu 📃
■	管理 » 外卸服务器 » 信息	投置					
🖬 监視 🔹 🔹	信息					👘 Configu	re SMS Gateway
<u>k</u> ne 🔹 🔍	ClearPass Messaging Se	tup quides you through configurati	ion of the SMTP server for email	and SMS notifications.			
2 管理 🔹	CMTD EXT						
Je ClearPass Portal	SHITP BOYIG						
🖃 🖴 用户和权限	通用 SMTP 设置						
	服务器名称:	smtp.126.com		Connection Security:	None	•	
── 管理权限	用户名:	xxxx@126.com		端口:	25		
□ · · · · · · · · · · · · · · · · · · ·	密码:			连接超时:	30 秒		
- → 服务器配置	Verify Password:						
	默认发件人地址:	xxxxd@126.com	1				
● 体理 中枢代学文 肝大							
1 個 外部勝等器	1				Sand Test Empil	Sand Test SMS	有片 月方
- P SNMP trap接收方					Send lest Linal	Send lest sms	34.122 14/19
- A Syslog 目标							
→ P Syslog 导出过滤器							
- 🎤 信息设置	1						
- ♪终端环境服务器	1						
- Je File Backup Servers							
▶ 🛄 字典							
🗈 🐔 代理和软件更新							
🗈 🐔 Support							
© 節权所有 2015 Aruba Networks。保留所有权利。		Oct 10, 2019	10:35:05 CST		ClearPass	等略管理器 6.7.9.1091	95 开启 CLABV 平台



aruba		Clea	arPass Policy Manager			Menu 🚍
-	○ 管理 » 外部服务器 » 信息	设置				
₩ 监視	• 信息					🛉 Configure SMS Gatewa
d. 822	O ClearPase Messaring S		tion of the SMTP server for email and St	15 notifications		
2月 管理 (1)	Charle Bite 7	cap galacs you an ough conngare				
P ClearPass Portal	SMIP BOIRS					
🖃 💊 用户和权限	· 通用 SMTP 设置 —					
→ 管理员用户	服务器名称:	smtp.126.com		Connection Security:	None	•
	用户名:	baggioyang@126.com		9異口:	25	
□ ····································	密码:			连接超时:	30 秒	
▲ □====================================	Verify Password:					
→ 本地共享文件夹	默认发件人地址:	baggioyang@126.com				
글 續 外部服务器					Send Test Email	Send Test SMS 复位 保存
— 🥜 SNMP trap接收方		Cond Test Freed				
- A Syslog 目标		Send Test Email				
		Recipient Email Address:	xxxx@189.cn			
→ ジ環环現版分益 由 Eile Backup Sequere		Message:	aruba-test-email			
一 一 一 File backup servers						
				4		
→ 代理和软件更新						
🕞 🐁 Support			Send Email 天日			

7.3.2 添加访客 portal 自注册页面

第1步:通过网页浏览器来访问ClearPass的管理IP(10.X.50.41) (X:1……6),从而进入到welcome行动页面, 点击ClearPass Guest 模块,从而进入到访客管理页面。





aruba	ClearPass Guest	Menu
*** 0 ** 以次四五台 ** バスの当話 ** (第二会) ** (*******************	王 (二) 、 未来 访客性理長 が客水 戸管理 使用以下指令去看達信付短期指約条用一級(二) 砂(三) 新聞の時間を近一一書絵(四) 砂(三) 新聞の時間を近一一書絵(四) 砂(三) 新聞の時間を用し、一日前の間間に見一点になる。 砂(三) 新聞の時間の時間の時間の一点のなるためまたのは時齢を知知ったのであり、 御覧の「小酒家」のなながのは時齢を知知ったのであり、 御覧の「小酒家」のななながのは時を発見ないたの時かを発見いた。 御覧の「小酒家」のなななたのは時を発見ないたの時か。 御覧の「小酒家」のなななたのは時を発見ないたの時か。 御覧の「小酒家」のなななたのは時を発見ないたの時か。 御覧の「小酒家」のなななたのはなかたの時を発見ないたの時か。 御覧の「小酒家」のなななたのはなかたの時を発見ないたの意か。 御覧の「小酒家」のなななたのはなかたの時を発見ないためまた。 むかまた 本	
ill Onboard の へ AZ の 文 AZ の 文 AZ の	(加加)(10) (加加)(10) (加加)(10) (加加)(10) (加加)(10) (加加)(10) (加加)(10) (10) (加加)(10) (10) (10) (10) (10) (10) (10) (10) (10) (10) (10) (10) (10) (10) (10) (10) (10) (10)	

第2步: 在访客管理页面中, 找到 配置 - > 身份验证 , 将安全设置项取消 (参考之前的步骤4.3.1) 第3步: 在访客管理页面中, 找到 配置 - > 页面 - > 自助注册 , 点击右上角的 "创建新的自助登记页面" 按钮,

增加一个新的访客自注册页面:

aruba		ClearPass Guest	:		Menu 🗮
💐 *x;: 🔹 🛛 🖉	主页 » 配置 » 页面 » 自助注册				
📳 Onboard 🔹 💿	自助注册				创建新的自助登记页面
	使用该列表视图管理访客自助登记页面				
- ** 身份验证		壮雄西面	中社	151	
● 🥶 内容管理器 - ST 来寫管理器	Guest Self-Registration Default settings for visitor self-registration.	guest_register	(Default)	•9 (无母区域)	
 \$ \$	一个自注册信息 🗘 重启			显示所有行	
从这里开始	Back to pages				
- % 字段 - % 表单	🔨 返回自定义				
List Views	公 返回主页				
- <mark>M</mark> Web 登录					
_ ➡ 从这里开始					
- 1 数字凭证模板					
- 😥 电子邮件回执					
10- 短信回执					
- 🛃 模板					
□- ▶ 短信服务					
- → 从这里开始					
<u>) ≈ ≈</u> 0					
 ● 日子部件回路 ● 日信回路 ● 日信回券 ● 和信服券 ● 人这里开始 ● Copyright 2019 Hewlett Packard Enterprise 	2 Development LP				LlearPass Guest 6.7.9.109195 on CLABV platform

在页面的基本属性中, 输入下面的参数:

- ✓ 名字: guest-self-registration (即该访客自注册页面的配置名称)
- ✓ 注册页面: guest_register
- (即该访客自注册页面的URL后缀名称guest_register.php)
- ✓ 保存更改:点击保存



aruba		ClearPass Guest
*s; 0	主页 » 配置 »	页面 » 自助注册
Onboard O	自定义的月	护登记 (new)
- 配置		
- 🛶 从这里开始	使用该表格创造	新的访客自助登记项。
一 📌 广告		自定义的用户登记
- 🔧 身份验证	基本属性	
	功者目的登记的者	中球中球地域。 quest-self-registration
	* 名字:	305150119月300001 約入回285日計算河市的名称。 法名称位置理具可用
- 🛶 从这里开始	描述:	
— 🛅 字段		对读自助登记进行评论,评论内容仅管理员可见。
- 🛅 表单	启动:	✓ 允许访客自助登记
List Views	* 注册页面:	guest_register
- 9+ 目前推动		(非木本 - 单个)
	家长:	字段和文本将使用父的价值,除非重写。 只需体改一个字段的值要盖父。
- 🛃 回执		Require operator credentials prior to registering the guest
→ 从这里开始	认让服务器:	If checked, access to this registration page will require operator credentials. The sponsor's operator profile must have the Guest Manager > Create New Guest Account privilege.
- 11 数字凭证模板	热区;	□ 为热区事项准备自主注册
		如要求支付豐強則勾选此道
- A 模板		保存更改保存后继续
□ ≥ 2 短信服务	* 必填字段	
- → 从这里开始	🌸 返回访客自	助豐记
	Back to r	ages
© Copyright 2019 Hewlett Packard Enterprise	e Development I	p

在自定义的用户登记中,可以看到ClearPass内置的自注册流程图介绍:

✓ 发布该访客注册页面:点击,浏览器自动跳转到访客自注册页面上,同时会有页面的URL显示,该
 URL的后缀就是前面步骤中的注册页面的内容。那么这里创建好的访客自注册页面的URL就是:

http://10.2.50.41/guest/guest_register.php?_browser=1

✓ 高级编辑:进入到高级编辑窗口

aruba	ClearPass Guest	Menu 💻
♀ 未完 ■ Onboard ◇ 祝聞	 • 主□ × 範圍 × 貢勵 × 負励注册 自定义的用户登记 (guest_register) 	发布该访客注册页面 推出自助服务门户网站 启动网络登陆
 → 从这里开始 ◆ 广告 ◆ 劳份验证 ◆ 内容管理器 ● ◆ 内容管理器 	i方書自然登记信用知 T 显示。 終任重切進行時間。 IS者自動登记 ² guest-self-registration' ● 新聞面主用: guest_register	
	Sponsor Confirmation Sponsor Confirma	
● 月关 ● 发送短信 ● 影送短信 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	■ 勝要页 ■ 重要性的 管理版 和名供総合设置	



$\leftarrow \ \ \rightarrow \ \ G$	A Not secure	10.2.50.41/	guest/guest_re	gister.php?_br	owser=1									Q 🕁	Θ	:
Apps 🕥	网址大全 😤 百度	😧 聚划算	天猫精造	京东商城	💠 挂机刷宝	④ 一刀999级	超变态传奇	③ 淘宝优惠券	🕑 大奖网	ClearPass Policy Ma	ClearPass Policy Ma	🐓 msn (2)	🐓 msn			39
aruba							ClearPa	iss Guest								
请填写以下表单以	《获取网络访问权限。															
	访客注册															
* 您的姓名:	清输入您的全名。															
* 电子邮件地址:	请输入您的电子邮件地站 这将是您登录网络的用F	t. *8.														
* 确认:	□ 我接受使用条款															
	注册															
* 必填字段																
已拥有帐户? 登录	t in the second s															

✓ 基本属性部分:相关内容之前步骤已经配置好,皮肤可以选择自己喜欢的页面风格,

aruba		ClearPass Guest	Menu
¥ 未完 0 ■ Onboard 0	主页 > 配置 > 页面 > 自助注 白完 V 的田白登记(部 (nuest-self-registration)	← 返回编辑访客自助登记
▲ 配置 ● → 从这里开始	他用该表情来改变访客自助量	IB/guest-self-registration,	
→ ● 广告 - ● 号份验证	基本属性	CONTRACTOR STREET	
 ● 内容室理論 - ● 未真管理器 ■ ● 热点管理器 	* 名字:	<mark>guest sold solgistador</mark> 総入会社成品を登记者的名称。協名的仅管理员可见。	
→ ● 页面 - → 从这里开始 - ● → 以这里开始	描述:	对正在处理记录行评论、评论内容的管理历习及。	
— 🋅 表单 — 🎹 List Views	* 注册页面:	guest_register 编入访客登记页面的基本网页名。	
- ● 自助注册 	* 用户数据库:	ClearPass Policy Manager 自动起星功者等户功能由该服务管理者开启。	
- <u>2</u> 网页	* 皮肤:	(武以) • 遗择晶构登记河面的成块。	
□ □□□ □□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□	Prevent CNA:	Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not netw kit all a vendors, depending on how the captive portal is implemented.	
- 😥 电子邮件回执	Advertising:	Enable Advertising Services content	
- 10- 短信回执 	Translations:	Skip automatic translation handling Many fields and pages have translations available under 配置 > 副译 > Page Customizations. Select this option to keep all text as default.	

本次手册以默认皮肤为参考使用

 ✓ 访问控制部分:可以在这里设置自注册页面的访问权限,能否访问到该页面的源IP地址的黑白名单, 能够访问到该页面的时间表

aruba		ClearPass Guest	Menu 🗮
9 *x 0	访问控制 控制进入注册页面。		
Dobbard O 《配置 O	认证服务器:	Require operator credentials prior to registering the guest If checked, access to this registration page will require operator credentials. The sponsor's operator profile must have the Guest Hamager > Create New Guest Account privilege.	
	允许访问:	A. IP的地址公司后行独立作利用。	
	被拒绝的访问:	A 为10%社会长后登记使人对称.	
- 10 字段 10 本的	* 拒绝的行为:	发进HTTP 404没有找到状态▼ 选择系统调查到一个不被允许的课来。	
■ List Views ● List Views ● 经助注册 ● 经 Web 登录	场间时间:	成入一个时间和相信,自注而自同。相行一个谨慎。 例如,"日子"的选择时间的分词编定已使可能描述。	

✓ UI注册页面部分:可以在这里设置注册前的页面内容,相关的提示文字以及返回到登录页面的超链接
 URL等

aruba		ClearPass Guest	Menu
Si 未完 O ■ Onboard O	UI注册页面 访客注册页面外观的控制选项。		
へ 起資 📀	标题:	(討會注册) 培養 聖尼页面上显示的标题。	
	HTML2388:	(p) 論完成以下內容以着加則後访问。 (p) (p) (p) (p) (p) (p) (p) (p)	
● 雪子 ● 二 ● 末年 ● 11 Ust Views ● 11 Ust V	HTMLEIM	[if f gram_methates may locals, methated (a)- bineasy hows an account? Or & barder' [fear_methates register_mage]rewurlencode]_login.php?Sign Inc(a)- (p)/(1f) [insert	
	改写表格:	□ 请勿在其中包括访客登记类指的内容 督派HTML表示思项	

✓ UI回执页面部分:可以在这里设置注册成功后的页面内容,相关的提示文字等

aruba		ClearPass Guest
Signation Control C	UI回执页面 访客回执页面外观的控制运项。 标题:	10/m1注册单 专案指示项型 57-54-52
◆ 从这里开始 ◆ 小於理形始 ◆ 小於管理器 ◆ 小於管理器 ◆ 小於管理器 ◆ 小於管理器 ◆ 小於管理器 ◆ 小於管理器 ◆ 小說里开始 ◆ 小說里开始 ◆ 小說里开始 ◆ 小說里开始 ◆ 小說里用一	HTML598:	(P) 以下内容差念的等户性意。 (/p) INTML展示代表式的考虑的思想表示.
List Views List Views 成功 成成	HTML3508:	Insert.
- → 从这里开始	改寫證执:	■ 译勿在其中包括功者因此的内容 该还供将体金访者因此的HTML,

✓ 回执操作部分:可以在这里设置回执内容的如何发布,可以采用下载、打印、邮件以及短信等方式将访客账号和密码告知给访客人员,本次手册我们采用邮件方式来告知。

aruba		ClearPass Guest	Menu 🗮
💐 米定 🛛 o 👖 Onboard 🛛 o	回执操作 为自助登记的访客提供收益。		*
ペ 配置 ○	23T		
	启动:	□ 允许访睿回执的下载	
	🍓 ¥JEp		
- 5 身份验证	启动:	息用春户回达打印窗口	
	1000 400		
	ND9+AUX		
	后动:	思是自动通过电子邮件发送客户収益	
→ → 从这里开始	* 邮件区域	(使用默认:email) ▼ 该本和包含该都经产的电子部件地址。	
- 🏪 字段 - 🛅 表单	标题	Aruba访書自注册账号通知 描述反影的邮件访赛用户的主要模拟 属于把图影以编集	
- III List Views - ● 自助注册	* 收至旧的邮件	(使用戰以: GuestManager Receipt) ▼ 生成却件数编时使用绝文本或HTML打印模板。	
- 👫 Web 登录 - 🔍 阿页	* 电子邮件的皮肤:	(使用数认:使用数认的皮肤) ▼ 邮件振攻的展走格式	
□- 🚵 回执 -→ 从这里开始	* 发送副本	(使用默认:使用Bcc;如果激送给访客)▼ 当发递来宾信思给列表副本量的接受者时详细说明	
10 数字凭证模板 15 电子邮件回执	复制到	default 一个可语的其利米宾班卢信誉的部件清单的将被发送	
	Reply-To:	Allow the reply-to address to be overridden If checked, the reply-to address will be overridden by the sponsor_email field. Leave unchecked to use the global from address.	
🖃 🎽 短信服务	SMSWIE		
→ 从这里开始	启动:	禁止发送的SMS客户收益	
		Prove Marca	
	Sponsorship Con	firmation	
	启动:	Require sponsor confirmation prior to enabling the account	
注意 0	Download Pass Options for downloading a gue	ist receipt as a pass for use with Apple Passbook.	
Copyright 2019 Hewlett Packard Enterprise Devel	lopment LP		ClearPass Guest 6.7.9.109195 on CLABV platform


✓ Sponsorship Confirmation部分:可以在这里设置是否启用基于联系人的审核批准,联系人的邮箱地址 字段设置,是否向联系人发送短消息告知,是否允许联系人重新设定访客的角色和到期时间等。

aruba		ClearPass Guest	Menu 🗮
ey externat	Sponsorship Con	firmation	•
Onboard	6 启动:	Require sponsor confirmation prior to enabling the account	
▲ Kai	 认证服务器: 	Require sponsors to provide credentials prior to sponsoring If checked, the sponsor will need to successfully authenticate prior to approving the request. The sponsor's operator profile must have the Guest Manager > Remove Accounts privilege.	
- 😽 身份验证	100年发送		
·····································	* 邮件区域	(使用默认: sponsor email)	
● [■] 热点管理器	Email Confirmation:	Sponsorship Confirmation The plain text or HTML print template to send to the sponsor.	
- → 从这里开始 - → A 20	* 电子邮件的皮肤:	(使用默认:使用默认的按缺) · · · · · · · · · · · · · · · · · · ·	
	* 发送副本	不发送副本 ■ 当发递来真体是给到表副本量的接受者引连相说明	
	Reply-To:	Allow the reply-to address to be overridden If checked, the reply-to address will be overridden by the guest's email field.	
🥵 Web 登录	MS发送		
	SMS:	Send an SMS to the sponsor notifying them of the request	
- 📸 回外 - 🛶 从这里开始	UI Overrides		
- 🕼 数字凭证模板	用户界面覆盖:	显示字段重写UI文本和标签	
	S Account Overrides		
一個、短目回列	Role Override:	(No override) Change the guest's role upon a successful confirmation from the sponsor, to Enforcement on the first sector area more write for exercises to be undefined automatically.	
- ▶ 12 短旗級务 - → 从这里开始 - → 网关 - → 发送短信	Extend Expiration:	And constructions many concerning LOB Fore Frame must exist for sessions to be updated automatically.	
금 😪 超译)) 법명 © Convright 2019 Haudatt Packard Enternric	0 Te Davielonment I P	Extend the account's explanation time, Lawse blank to use the original explanation time. Torier a single values to automatically adjust the time. Enter a single values (2), 20, 6, er 37. Example values (2), 20, 6, er 37.	ClastPare Guet 5.7.9.109105 on CLABV platform

✓ 登录部分:可以在这里设置登录页面的相关内容,这里的登录页面是该自注册页面自动生成的,用于该 自注册页面和登录页面的自动跳转使用。安全登录设置为通过HTTP发送明文密码(因为我们本次实验会 采用ClearPass的自签证书,所以统一用HTTP发送明文。如果需要更安全的HTTPS发送密文,请事先准 备好商业签发的Public 证书)。默认网址即设置访客认证后的欢迎页面的URL,勾选覆盖目标.

aruba		ClearPass Guest	Menu
¥ 未完 ■ Onboard	● 登录 ● Options controlling logging in f	for self-registered guests.	
100 × 100		允许访客登录一台网络接入服务器 •	
从这里开始	* 供应商设置:	Aruba Networks T 思择一个预定义组设置符合标准网络配置。	
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	Login Method:	Controller-initiated — Guest browser performs HTTP form submit Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.	
	* IPHEIL:	securelogin arubanetworks.com 存在的入供应意符是的IP的地域意志机会。	
□ ● 页面	安全登录:	通过HTTP发送明文密码 * 为该网站登录过程法师一个安全选项为该网站数录过程。	
→ M38組7788 - 100 -	Dynamic Address:	The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used meners the parameter is not available or fails the requirements below.	
- III List Views	Security Hash:	Do not check – login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.	
- 🥵 Web 登录 - 🔍 阿页	取入目标 控制目标客户法经常需定会到设备	á,	
 回执 → 从这里开始 	* 默认网址:	http://www.arubanetworks.com wi.likusupuru建在考察声频。 编编你在梁凯亚上下时y/TPI任何外部间。	
WW 数子先延模板 QQ 电子邮件回执	覆盖目标:	2 强强的所有本中国的振动目标 如果思惑,有个国的影响的目标将被置置,不论它的强。	

✓ 登录表项和Post-Authentication部分:可以在这里设置登录页面的表单相关内容,即登录账号和登录 密码的标签内容的定制设置。同时可以设置预认证成功后的相关动作,可以做健康检测和更新为已知状态的endpoint。

aruba		ClearPass Guest	Menu
🗣 未完 📳 Onboard	○ 登录表项 造项控制登录NAS的形式出现	Namazari en l'enzantinazion l'ortenaggian ("Lis Europes")	
< ▲ 配置	O 目定义表单:	■ 標便自由文型要素单 若违指统项,您必须提供您的HTML页量或页脚区域的整要素单。	
- ➡ 从这里开始 ■ ◀ 广告	自定义标签:	重期就认為签約期決保應 如果选择。你將該勢投受当該的量要果单約签約購換保證。	
- No 身份验证 - No 内容管理器	Pre-Auth的检查:	Local — match a local account Select how the username and password should be checked before proceeding to the NAS authentication.	
 来宾管理器 新杰管理器 	Username Authentication:	Only require a username for authentication if set, the password field will not be displayed. forly accounts with the Username Authentication flag set on their account can login.	
● ● 页面	是数:	条款和条件要求确认 如果告中,用户件能治接受良新和良件奠括框。	
· 李段 四 李台	Post-Authentication Actions to perform after a succ	cessful pre-authentication.	
List Views	Health Check:	Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.	
Web 登录	Update Endpoint:	Mark the user's MAC address as a known endpoint If selected, the endpoint's attributes will also be updated with other details from the user account.	

✓ 登录UI部分:可以在这里设置登录页面的提示内容以及自动跳转到自注册页面的的超链接URL

aruba		ClearPass Guest	Menu
🥰 ¥2 0	登录UI 控制NAS登录界面的外观透现。		
Onboard O	登录页面标题:	Network Login 结网因标题显示在登录页面。	
→ 从这里开始 ◆ 人这里开始 ◆ 小宫告 ◆ 小宫告 ◆ 小宫告語 ◆ 小宫告語 ◆ 小宫告語 ◆ 小宫告 ◆	HTMLEIJ#:	[mm_codischedd] [if ferma[sontext type=error][#ernsg[escape] //ws_tontext]//if] [mm_text 1d=7800]©> Fleese login to the network using your unername and password.	
		Insert T HTML模板代码型示在登録录单之前。	
- Ⅲ List Views - ■ ■加速節 - ● ● 200連節 - ● ● 秋空登交 - ● ● 秋空型で - ● ● 秋空型で - ● ● 秋空里が始 - ● ● 秋空里が - ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	HTMLZEBU:	(Q) Meed an account? (a href=" [Eggr_metadata.register_page]rwwwiencode].php">Click Here(/a> (/p) /msert	
·····································		HTML欄板代码显示在臺灣表筆之順。	
— 😼 身份验证	和示服团:	Network Login in Progress 登录NAS显示页面的标题。	
 ● properties ● 大田田 ● 大田田 ● 大田 ● 大田<	型地有意:	Please wait while you are logged into the network	
— 🚜 Web 登录		Inset ▼	

✓ 自动登录, 社交账号集成以及自助服务门户部分: 这部分内容基本默认即可, 针对自助服务门户部分,
 关闭启用自助服务门户网站, 最后点击保存更改按钮, 完成本次访客自注册页面的设置。

- 9 0 0 0	HTML模拟CUB型示器运输组合约
→ 从这里开始	自动整果从运用控制自动记录在你编奏式。
一 天单	* 植物植物: 0 砂 完义几秒中国时来显示物把库里。
	Cloud Identity Optionally present guests with various cloud identity / social login options.
- Meb 登录	启动: 📃 Enable logins with cloud identity / social network credentials
- 🔍 阿页 - 🚵 回执	自動服务门户 地域是480回时和行政的回用者自己的来产。
	启动: 🔲 启用自动服务门户网站
1 数字凭证模板 2 电子邮件回执	禁锢時意: 要重取以所用的调意。
新 短信回执	- 幕 保存更改
Line texts	* 心理学校

第4步: 在【访客管理页面】中, 找到 配置 - > 页面 - > 自助注册 , 点击访客自注册页面guest-selfregistration,进入到编辑按钮,点击进入到编辑状态。

aruba		ClearF	ass Guest			Menu 🗮
祭 来宾	主页 > 配置 > 页面 > 自助注册					
Onboard O	自助注册					👙 创建新的自助登记页面
A28 0						
- 🍑 从这里开始	使用读列表视图管理访客自助登记页面					
日本の方法	 快速報助 					
- 🔧 鼻份验证	△ 名字	注册页页	皮肤	8		
● 🥶 内容管理器	guest-self-registration	guest_register	(Default)	(无母区域)		
	🕞 編載 🔕 影除 🗋 副本 🗶 关闭 💭 Tra	nslations 📥 Launch 📸 塑质				
▶ ■ 熱点管理器					-	
2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				显示所有行	•	
→ 从这里升始	Back to pages					
List Views	🔨 返回自定义					
	公司 适回主页					
A Web WW						
- 😥 网页						
- 🔁 RA						
- 🛶 从这里开始						
- 🇊 数字凭证模板						
- 😥 电子邮件回热						
短信回执						
- 品 模板						
□- ▶ / 短信服务						
- ➡ 从这里开始						
1 0- 网关						
□ 】 发送短信						
— ➡ 从这里升始						
- V 約子 約 (正要約)						
Field Customizations						
前面面自安文	1					
	1					
Copyright 2019 Hewlett Packard Enterprise Developm	nent LP					ClearPass Guest 6.7.9.109195 on CLABV platform

在【自定义的用户登记】中,可以看到ClearPass内置的自注册流程图介绍:

✓ 表单:进入到注册页面的表单编辑

aruba	ClearPass Guest	Menu
Signation (1997) (19977) (19977) (19977) (1997) (1997) (1997) (1997) (1997) (±须。w≣。y页案 elwit统 自定义的用户登记 (guest_register)	发布该访查注册页面 面动网络登陆
▲ 2篇 ○ - → 从这里开始 ▲ - 《 方 告 - 《 方 告 - 《 方 合正理論 - 》 方容理論 - 》 方容理論 - 》 方容理 - 》 方容 - 》 方容 - 》	は命命総理記原理が子型で、你注意理定行機構、 的名称範囲をないますelf registration' 一個 単分記用用 単 単分記用用 単 単分記用用	
● ★ 从这里开始 ● 字段 ● 词章 ● Ust Views ● Ust Views ● Kolling ● Web 登去 ● KNS		
 → 風助, → 从这里开始 → 数本失过课版 → 经考益计量助, → 短语意助, → 短语意助, 		
□ · · · · · · · · · · · · · · · · · · ·		
● 対理程度 ● 秋島里开始 ● 秋島里开始 ● 秋島里开始 ● 秋島 ● Field Customizations ● Field Customizations	 • 英国大学 和学校(中国) • 英国大学 和学校(中国) • Back to pages • 新聞主要() • 新聞主要() 	
Copyright 2019 Hewlett Packard Enterprise Developme	ent LP ClearPass Gu	est 6.7.9.109195 on CLABV platform

在【定制表单字段】中,可以看到访客自注册页面中表单各字段内容:

✓ sponsor_email: 将该字段启用

ba				ClearPass Guest	
	 主页 > 配置 > 页面 > 表示 				
and	○ 定到表前字段 (n)	ect register	-)		📲 定制字目
	0 AE1034X++ J +X (90	cor_register	0		- 近回天日
2 8 1.00					- CEASVON
io.a./ no	使用这个提图列赛来更改要	uest_register///言	C129:#112.		
- 6)验证	A chierman			271/0 vet 00	
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	U Haberto	1000000	100.000		
本管理器	10 10 10 10 10 10 10 10 10 10 10 10 10 1	20 Miles	6 535	編述	
白管理器	10 sponsor name	text	Sponsor's Name:	Name of the person sponsoring this account.	
2	15 sponsor email	text	Sponsor's Email:	Email of the person sponsoring this account.	
➡ 从这里开始	·> ## ₩ #####	🛪 89 🔸 EZO	植入 一 在之后输入	学校起版	
事 李段	20 visitor name	text	想的名字:	市場入業が主要	
	25 visitor phone	phone	Phone Number:	連邦となるため	
List Views	30 visitor company	text	Company Name:	· · · · · · · · · · · · · · · · · · ·	
+ 自助注册	40 email	text	Email Address:	情報人間的影響ない、は国家大学課人目的が用点を	
🙀 Web 登录 🔍 网页	50 start_time	datetime	Activation Time:	Scheduled date and time at which to enable the account. If blank, the	
	50 expire after	hidden	Expires After:	Amount of time before this account will expire.	
▶ 从这里开始 ● 数字体证明版	65 expire_time	datetime	Expiration Time:	Optional date and time at which the account will expire and be deleted. If blank, the account will not expire.	
m Zat/t Eth	70 role id	hidden	Account Role:	Role to assign to this account.	
19月11日11日	75 enabled	dropdown	Account Status:	Select an option for changing the status of this account.	
福振	80 random_passwo	d static	Password:	-	
服务	81 no_password	hidden	Password Change:	If set, prevents the user from changing their own password.	
从这里开始	85 no_portal	hidden	Portal Login:	If set, prevents the user from logging into the guest service portal.	
▶ 网关	100 secret question	text	Secret Question:	Enter your secret question. The answer will be required to reset your	
发送短信			Count Longer	password.	
	101 secret_answer	text	Secret Answer:	Enter the answer to your secret question.	
从这里开始	you create_time	nidden	Created:	time the account was created.	
》助手:	900 mac	nidden	MAL ADDRESS:	MAL address of the device.	
A 语言包	901 remote_addr	nidden	Create Address:	This is your IP address.	
Field Customizations	902 http_user_agent	nidden	User Agent:	This is your browser's user agent string,	
页面自定义	A03 nu	nidden	UKL:		

7.3.3 添加访客 portal 登录页面

第1步: 在访客管理页面中, 找到 配置 - > 页面 - > 自助注册 , 点击 "guest-self-registration" 对之前创建的 访客自注册页面进行编辑(这里必须是先点击下guest-self-registration 字体后, 才会出现下面一行的编辑、 删除、副本、关闭等菜单按钮):

第 來完 0 主页 » 配置 » 页面 » 自助注册
onboard o 自助注册
● V 内容管理器 August college (postul) (元何行時)
- Starting And Anticipation A
● ● 页面 显示所有行 ●
Juženným Radio Parister a se
- 🍟 字段 🔭 Dack to pages
List Views 公司 按照中面
- 1 7. 短 信 国执
- 🛶 从这里开始
- В р. Ю́Х
🎽 发送短信

第2步:点击自注册页面guest-self-registration下的登录按钮,可以自动跳转到相对应的登录页面URL上,此时 记住该登录页面的URL,并复制和粘贴到一个文本文件中,留作后期在控制器上配置captive portal profile 中的login url使用。那么这里系统自动创建好的访客登录页面的URL就是:

http://10.2.50.41/guest/guest_register_login.php?_browser=1

aruba		ClearPass C	Guest			Ме	enu 📕	
북 米文 이 I Onboard 이 入記법 이	主页 » 配置 » 页面 » 自助注册 自助注册					🍦 创建新的自同	助登记页面	
- 🛶 从这里开始	使用该列表视图管理访客自助登记页面							
	① 快速帮助							
	△名字	注册页面	建設	8				
- 4. 来宾管理器	guest-self-registration	guest_register	(Default)	(元母宮城)				
→ \$ 热点管理器								
□ ● 页面				显示所有行				
- 19 字段	🌸 Back to pages							
- 👔 表単	🔨 返回自定义							
List Views	🐔 返回主页							
- 18 Web 70 0	(B) summer							
- 2 网页								
 一品 四邦, 								
→ 从这里开始								
御 短信回执								
🛃 模板								
▶ 发送短信								
▶ 管理 •								
rise Dev	elopment LP				ClearPass Gu	est 6.7.9.109195 on CLA	BV platform	
$\leftarrow \rightarrow C$ A Not secure 10.2.50.41	/guest/guest_register_login.php?_browser=1						0. 1	0:
👯 Apps 📀 网址大全 🎂 百度 📀 聚频算	▲ 受 天湿精造 ③ 京东商城 ◆ 挂机刷宝 ④	-刀999版 📀 超变态传奇	③ 淘宝优惠券 (📀 大奖网 🔇 ClearPass Policy Ma.	📀 ClearPass Policy Ma	📝 msn (2) 📝 msn		30
on the		ClearDa	ee Gueet					
		GlearFa	iss Ouest					
清使用用户名和密码 登录网络。								
Network Login								
用户名:								
密码:								
条款: 🗎 找接受使用条款								
登录								
Need an economia Click Harr								
nieed an accountr Glick Here								

7.3.4 修改联系人邮件确认收据

- 第1步: 在访客管理页面中, 找到 配置 > 回执 > 模板 , 点击 "Sponsorship Confirmation", 在下面的菜 单中点击副本按钮, 对系统默认的联系人确认邮件模板进行复制(这里必须是先点击下Sponsorship Confirmation 字体后, 才会出现下面一行的编辑、编辑代码、副本、删除等菜单按钮):
- NOTE 当然你也可以直接在 Sponsorship Confirmation 系统默认的模板中直接修改。



aruba			ClearPass Gues
S #g 0 ■ Onboard 0	主页 » 配置 » 回执 » 機板 访客管理员 打印模板		
	定义的打印模板从下列表列出。		
 ■ ● 广告 ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	()快速解助		
→ 🥶 内容管理器	△ 名字	- Alexandrian Contraction of Contrac	C #53
	Certificate Expiry	万	启动
 □ - · · · · · · · · · · · · · · · · · ·	Download Receipt	纯文本	启动
日間回規	Guest Account Expiry	页	启动
 → 从这里开始 ● 数字体运进机 	🍰 GuestManager Receipt	页	启动
	🚵 One account per page	页	启动
短信回执	SMS Receipt	纯文本	启动
	SMS Sponsor Confirmation Alert	纯文本	启动
	Sponsor Device Provisioning	Wizard	启动
	Sponsorship Confirmation	Wizard	
2013年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日		S ALX WITTANS	abons 🦏 💷 ग्रा
	Sponsorship Confirmation (2)	Wizard	启动
	Sponsorship Confirmation (test)	Wizard	启动
	Two-column scratch cards	2-column 列表	启动
	13 打印機板 🖒 重启		显示所有行
	Back to receipts		
	🔦 返回自定义		
<u>〕 管理</u> の	🏠 返回主页		

第2步:对系统新增的联系人确认邮件模板Sponsorship Confirmation(3)进行编辑:

aruba			ClearPass <mark>Gue</mark> s
📲 xg 🛛 🔍 0	主页 » 配置 » 回执 » 模板		
📳 Onboard 🛛 🛛 🛛	访客管理员 打印模板		
🔨 配置 💿			
— 🛶 从这里开始	定义的打印模板从下列表列出。		
	(1) 快速帮助		
- 🤹 身份验证	△名字	俗	い 状态
	Account List	列表	启动
	Certificate Expiry	页	启动
回 — · · · · · · · · · · · · · · · · · ·	Download Receipt	纯文本	启动
- 🔒 回执	Guest Account Expiry	页	启动
- 🛶 从这里开始	GuestManager Receipt	页	启动
- 1 数字先证模板	One account per page	页	启动
	SMS Receipt	纯文本	启动
	SMS Sponsor Confirmation Alert	纯文本	启动
□ ≥	Sponsor Device Provisioning	Wizard	启动
	Sponsorship Confirmation	Wizard	启动
- 約 -	Sponsorship Confirmation (2)	Wizard	启动
	Sponsorship Confirmation (3)	Wizard	启动
19 19 19 19 19 19 19 19 19 19 19 19 19 1		鑦 准入 💽 Trans	lations 🔌 显示本
	B Two-column scratch cards	2-column 列表	启动
	13 打印機板 🖒 重启		显示所有行 ▼
	Back to receipts		
	🔨 返回自定义		
) 🕅 📜 🖉	🏠 返回主页		





{if true}

A visitor has requested access naming you as the sponsor. Please click nere to confirm or reject the request. {else}

(else)
A visitor has requested access naming you as the sponsor.
Do you <a href="('guest_register_confirm.php'|NwaGetAppUrl:false:\$u.require_auth)?(if \$u.source)gsr_id=(\$u.source|rawurlencode)&(/if)token=
(\$u.register_token|rawurlencode)&confirm=1" target="_blank">confirm
or <a href="('guest_register_confirm.php'|NwaGetAppUrl:false:\$u.require_auth)?(if \$u.source)gsr_id=(\$u.source|rawurlencode)&(/if)token=
(\$u.register_token|rawurlencode)&confirm=0" target="_blank">confirm
(\$u.source)gsr_id=(\$u.source)rawurlencode)&confirm=0" target="_blank">confirm
(\$u.register_token|rawurlencode)&confirm=0" target="_blank")

{/if}

对提示栏目中的代码进行下面的修改,这样可以保证当联系人收到该邮件确认函后,点击Click Here能够通过IP 地址访问该ClearPass,而不是默认的通过主机名方式来访问(前提是该网络中并没有实现域名的解析)。

我们需要在quest register confirm.php 前面增加 http://x.x.x.x/quest/ (x.x.x.x即ClearPass的管理IP地址, 可 以是本地IP,也可以是对应的公网IP)

由于 ClearPass 具有自动语言翻译包功能,当前我们修改的模板,仅仅是针对英文版本的浏览器生效,也就是如果 NOTE 客户采用英文语言的浏览器访问了自注册页面并发送账号批准申请,那么该代码是生效的。而针对中文语言的浏览 器,我们还需要设置下中文语言包的代码修改,请继续。





第3步: 在访客管理页面中, 找到 配置 - > 翻译 - > 页面自定义 , 语言选择 "中文(Chinese)" , Item选择 Sponsorship Confirmation (即系统原始文件名) , 对中文语言包的确认邮件模板进行查看:

aruba		ClearPass Guest	Menu
🗣 жд 🔹 O	主页 > 配置 > 翻译 > 页面	自定义	
📳 Onboard 🛛 🔍 O	页面自定义 (zh)		
< 配置 💿			
➡ 从这里开始	Use this form to manage	e translations on nelos, torms, views and print templates.	
- 😽 身份验证	* 语言:	中文 Chinese _ V	
● 🥶 内容管理器		Steps: Use an judge to Custom Carissianovs.	
	Item:	Select the item for custom translations.	
	Load File:	Load the contents of a local file The action can be velocited here	
	名宝·	Pres dominated in on the management action can be uprovided in a c.	
→ 从这里开始	打印模板名称,当打印账户列	(表时,这个名字可用于进行模倣选择。	
🗊 数字凭证模板		Sponsorship Confirmation	
- 100 电子邮件回执	Current Configuration:		
		ingent i	
一般权	Default Translation:		
	name:		
- 2 发送短信	42.00.		
- 🛃 翻平	1008: 输入标题上显示打印模板。例	收回题的最高级东南。	
→ 从这里开始	Ourrent Configuration:		
- 💛 助手	contraite configuration	A guest is requesting visitor access	
· A 培言包	Default Translation:	法案に対象が方向後近回り	
an Field Customizations			
	wizard_title:		
	字墓: 输入一个字幕显示在打印模	8.	
	Current Configuration:		
	wizard_subtitle:		
	字段标题: 输入一个打印模板上显示的	1. (半母在君子兵行题:	
	Current Configuration:	Account Details	

NOTE 你会发现在中文语言翻译包里面,系统默认并没有对修改的 URL 进行翻译和变更,所以我们需要继续修改联系人确认邮件模板。



aruba	ClearPass Guest					
来実 0 ■ Onboard 0	字段标题: 输入一个打印模板上显示的	洋總國尊和防藏。				
< 配置 ○	Current Configuration:	Account Details				
— 🛶 从这里开始 ∋ 📢 广告	Default Translation:	(201m)户洋和图象				
	wizard_field_header:					
	提示 输入的说明显示在打印模板	。 ,A.A.一个通道官会的道思对他们问题。				
◆ 於西田道谷 ◆ 方面 ◆	Current Configuration:	<pre>qp (df true) A visitor has requested access naming you as the sponsor. Flease <a &u.source)gsr_id="(&u.source)resultencede)#(/if)token=<br" ("quest_register_confirm.php?newheakeepporlfalse:#u.require_muit)?(if="" href="https://19.143.145.10010043/quest/quest_register_confirm.php?if &u.source)gsr_id=
(ds.source)resultancede)#(//1f)token=(ds.register_token)resultancede)* targets*_black=visito & to confirm or reject the request.
A visitor has requested access naming you as the sponsor.
Do you ca href*">(ds.reqister_confirm.php?NewHeakeEppOrlfalse:#u.require_muit)?(if &u.source)gsr_id=(&u.source)resultencede)#(/if)token= (cs.reqister_confirm.php?NewHeakEppOrlfalse:#u.require_muit)?(if &u.source)gsr_id=(&u.source)resultencede)#(/if)token= (request_confirmeurlencede)confirm="" target="black=yrequire_muit)?(if &u.source)gsr_id=(&u.source)resultencede)#(/if)token= (request_confirmeurlencede)confirm="" target="black=yrequire_muit)?(if &u.source)gsr_id=(&u.source)resultencede)#(/if)token= (request_confirmeurlencede)confirm="" target="black=yrequire_muit). (request_confirmeurlencede)confirm="" target="black=yrequire_muit] (request_confirmeurlencede)confirm="" target="black=yrequire_muit] (request_confirmeurlencede)confirm="" target="black=yrequire_muit] (request_confirmeurlencede)confirm="" target="black=yrequire_muit] (request_confirmeurlencede)confirm="" target="black=yrequire_muit] (request_confirmeurlencede)confirm="" target="black=yrequire_muit] (request_confirmeurlencede)confirm="" target="black=yrequest_confirmeurlencede)confirm="" target="black=yrequest_confirmeurlencede)confirm="" target="black=yrequest_confirmeurlencede)confirm="" target="black=yrequest_confirmeurlencede)confirm="" target="black=yrequest_confirmeurlencede]confirm=" target="black=yrequest_confirmeurlencede]confirm=" target="black=yrequest_confirmeurlencede]confirm=" target="black=yrequest_confirmeurlencede]confirm=" target="black=yreq</pre>				
- ● 第2885年 ● 第2885年 - ● 从送至开始 - ● 約年 - ● 約年 - ● 約年 - ● 新年 - ● Field Customizations - ② ● Field Customizations	Default Translation:	GD- (はfrom) 認想業者和URPが法規人が法規例人が法規例の認識。ca href**('guest_register_confirm.php' hadetAppUrlifiles(fu.register_utent))(if fu.source)ger_id*(fu.source)ger_id*	h			
	wizard_notes:		li.			
	页脚: 页脚:	Inset.	۲			
	Current Configuration:	we∽ Powerd by (nwa_icoriink icon="imagesicon-aruba22o22 png" text="Aruba Networks"}http://www.arubanetworks.com?[hwa_iconiink]				
<u>) N MIE</u> 0	Dofault Translations					

将 Default Translation 里面的内容拷贝到文本文件中,并继续在guest_register_confirm.php 前面增加 http://x.x.x.yguest/ (x.x.x.x即ClearPass的管理IP地址,可以是本地IP,也可以是对应的公网IP),留作备用。

将Item重新选择Sponsorship Confirmation(3)--即之前创建的,在提示部分中的wizard_notes文本框中贴入前 面文本文件修改好的代码,最后点击保存修改按钮。

💐 来宾 🛛 🛛 🛛 🖉	主页。 乾證 > 翻译 > 页面自见义
📳 Onboard 🔹 🔍	页面自定义 (zh)
< 配置 •	Line this form to manage translations on Relde forms, views and wrint termolates
— 🛶 从这里开始	Ger na rutt vorteinege Geraedonis on neway kunnay heitra eray preti tempietea.
	百角自定义
- 😽 身份 验证	* _{语言:} 中文 (Chinese) ▼
🗈 🍲 内容管理器	Select the language for outtom transitions
- 1957 宋宾管理器	Item: [Sponsorship Confirmation (3) •
 約点管理器 	Jest the restrict of a local file
(a) (a) (b) (b) (b) (b) (b) (b) (b) (b) (b) (b	Lead File: File solution the Translations action can be uploaded here.
- 🔂 QM.	名字:
	打印機板名称。当打印账户列表时,这个名字可用于进行模拟选择。
1 数字凭证模板	Sponsorship Confirmation (3)
	Current Configuration:
	name:
- 🛶 从这里开始	1998年 第二次時上三世元打印機應,例如2893頃(1993年)。
- b , 网关	
● 发送短信	Current Connguration: A guest is requesting visitor access
	ward hite
→ 从这里开始	
「入は目記」	周/一 / 今後四次任210萬的·
Field Customizations	Current Configuration:
	wizard_subtite:
	字段标题:
	編入一个打印機應上显示的洋畑信息字段标题.
	Current Configuration:
	Account Datails
	wizard_field_header:
	握示
	輸入的洗明显示在打印模板。e.g.一个值得实验的消息或她用说明。
in water of	
<u>~</u>	



	0	Laster () state	_
	wizard field header:		
N CHIDOARD	· 提示		_
→ 从这里开始	編入80次時間17月1日開版	● Q 一「 量像水量的過程表現用説明. 	-
	Current Configuration:	<pre>qup (qp) (lst tune) As source(partid=(as comer naming you as the sponsor. Planes (s href=""""""""""""""""""""""""""""""""""""</pre>	
	wizard_notes:	yr (1 f tan) MSΦαβμάθητΜΒΑ,ΔΕΔΕΝΟΘΟΑ, (* bref*"("brep//]0.1.50.41/gwer/gwer_register_confirm.pp") MSΦαβμάθητΜΒΑ,ΔΕΔΕΝΟΘΟΑ. (*.sounoeiterwarlencode) 4//1f Swameferu.eggsconfirm.com (*.sounoeiterwarlencode) 4000000000000000000000000000000000000	
Field Customizations		insert	
(m) 更新自己义	(只開: 页部文本输入要显示在打印)	dara.	
	Current Configuration:	Powered by (mwa_iconfink icon="imagesicon-anubat2:x22 png" text="Avuba Networks")http://www.arubanetworks.com/(hwa_iconfink)	
	wizard_footer:		
		曹 保存要文	
	* 必填字段		
	🛶 Go to item		
<u>〕</u> 《理	• Back to translations		

第4步:回到之前步骤7.3.2中的访客portal自注册页面,在之前创建的自注册页面的高级编辑中,在 Sponsorship Confirmation 部分中,修改Email Confirmation 选择Sponsorship Confirmation(3),最后点击 保存修改按钮.

aruba		ClearPass Guest	Menu 🚍
🤐 来宜	o sponsorsnip com	Irmation	
Ophoard	启动:	Require sponsor confirmation prior to enabling the account	
	• 认证服务器:	Require sponsors to provide credentials prior to sponsoring if diveked, the sponsor will need to successfully authenticate prior to approving the request. The sponsor's operator profile must have the Guest Manager > Remove Accounts privilege.	
→ 八2里开始 → 《◎广告	₩ 邮件发送		
- No 身份验证	* 創件区域	(使用訳认: sponsor email)	
· · · · · · · · · · · · · · · · · · ·	Email Confirmation:	Sponsorship Confirmation (3) The plain text or HTML print template to send to the sponsor.	
· (1) 页面	* 电子邮件的皮肤:	(使用默认:使用默认的皮肤) ▼ 邮供你的周短循环	
- → 从这里开始 - 100 字段	* 发送副本	不发送副本 ● 11世送 未完成 登場列表面は重約1件研究時	
— 🚮 表単 — III List Views	Reply-To:	Allow the reply-to address to be overridden If checked, the reply-to address will be overridden by the guest's email field.	
- 19 自助注册	SMS发送		
Web 登录	SMS:	Send an SMS to the sponsor notifying them of the request	
	UI Overrides		
	用户界面覆盖:	☑ 显示字段重写UI文本和听签	
↓ 数字凭证模板 → Q 电子邮件回执	标题	指型改变的)的体征 有效产的注意 模拟 氧开使用数以 模拟	
	Confirmation Title:	Override the default page title (面助注册确认).	
● ● ● ● ● ○	HTMLZEW:	<pre>cp> (if 15_confirm_success) A guest has requested your confirmation for guest access (else) (/if)</pre>	

Aruba Hands-On Lab Guider: ClearPass

7.3.5 添加认证服务

第1步: 找到 配置 - > 强制执行 - > 配置文件 , 点击右上角的 "添加强制执行配置文件"按钮 , 增加一个强制执行配置文件:

aruba	ClearPass Policy Manager					
- AN	0 配置 > 强制执行 > 配置文件					
	强制排	丸行面	置文件		■ 添加强制执行配置文件 ● 导入强制执行配置文件	
20 配置	Ð				2 导出强制执行配置文件	
Q 武处开始	Each en	forcem	ent policy contains enforcement profiles that match co	nditions (role, posture,	and time) to actions (enforcement profiles).	
- 尊服务						
袖状证	过滤器:	名称	• 包含 •	🖶 Go Clear Filt	ter 显示 20 • 记录	
- 12 万法			名称。	类型	说明	
日本で	1.	0	[Aerohive - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)	
Single Sign-On (SSO)	2.		[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request	
- 叠 本地用户	3.		[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request	
- 尊 端点	4.	10	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request	
	5.		[Allow Access Profile]	RADIUS	System-defined profile to allow network access	
→◎ 角色	6.	8	[Allow Application Access Profile]	Application	System-defined profile to allow access to application	
	7.		[ArubaOS Switching - Bounce Switch Port]	RADIUS_CoA	System-defined profile to bounce the switch port on ArubaOS Switching products.	
■ ● ※主秋元 ■ ■ 磁制执行	8.		[ArubaOS Switching - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect the user on ArubaOS Switching, HP ProCurve and HP UWW products.	
- Q 第略 - Q 配置文件	9.	0	[ArubaOS Wireless - Bounce Switch Port]	RADIUS_CoA	System-defined profile to bounce the switch port on ArubaOS Mobility Controllers, Multi-Port APs & Mobility Access Switches.	
· •• 网络 · ··································	10.	8	[ArubaOS Wireless - TACACS Read-Only Access]	TACACS	System-defined profile for TACACS read-only access on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches.	
- 众 策略仿真	11.	8	[ArubaOS Wireless - TACACS Root Access]	TACACS	System-defined profile for TACACS root access on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches.	
	12.	8	[ArubaOS Wireless - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect the user on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches.	
	13.		[Cisco - Bounce-Host-Port]	RADIUS_CoA	System-defined profile to bounce host port (Cisco)	
	14.		[Cisco - Disable Host-Port]	RADIUS_CoA	System-defined profile to disable host port (Cisco)	
	15.		[Cisco - Reauthenticate-Session]	RADIUS_CoA	System-defined profile to re-authenticate session (Cisco)	
	16.	8	[Cisco - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Cisco)	
	17.	8	[Deny Access Profile]	RADIUS	System-defined profile to deny network access	
T 00:0	18.	. 🕀	[Deny Application Access Profile]	Application	System-defined profile to deny access to application	
	10	- 61	IDron Accase Drofila1	DADTHS	Suptamudafinad nonfile to dron the request	

在配置文件选项卡中, 输入下面的参数:

✓ 模板: Aruba RADIUS 强制执行



- ✓ 名称: task6-guest-register-profile
- ✓ 操作: 接受

配置 » 强制执行 » 配置文件 »	Add Enforcement Profile
强制执行配置文件	
配置文件 属性 概要	
模板:	Aruba RADIUS 强制执行 ▼
名称:	task6-guest-register-profile
说明:	
类型:	RADIUS
操作:	● 接受 ● 拒绝 ● 删除
设备组列表:	Remove
	View Details
	Modify
	Select 🔻

在属性选项卡中, 输入下面的参数:

✓ 属性: Radius:Aruba Aruba-User-Role guest-register-role

NOTE 该角色就是当访客认证通过后, CPPM 返回的认证后的角色授权

配置 » 强制执行 » 配置文件 » Add Enfo	rcement Profile		
强制执行配置文件			
配置文件 屍性 概要			
类型	名称	<u> </u>	
类型 1. Radius:Aruba	名称 Aruba-User-Role	11 = Enter role here	Ba 11

第2步: 找到 配置 - > 强制执行 - > 策略 , 点击右上角的"添加强制执行策略"按钮 , 增加一个强制执行策略:

aruba		Cle	arPass Policy N	lanager	Menu 🗮
_ 向 板	○ 配置 » 强制执行	» %站			
- - 1 12 - 12 - 12 - 12 - 12 - 12 - 12 -	• 品制执行等	11久			🖕 漆加强制执行策略
NR.	0 1300117(1) X				导入强制执行策略
0 10 10 10 10 10 10 10 10 10 10 10 10 10					2. 导出强制执行策略
4 8.8.77 M	ClearPass contr	ols network access by evaluating an enfor	cement policy associated wil	th the service.	
₩ 26.71 局は正					
前方法	过滤器: 名称	 包含 	🛨 Go C	lear Filter	显示 1000 • 记录
0 2		名存▲	类型	说明	
2 与份	1. 💷	[Admin Network Login Policy]	TACACS	Enforcement policy controlling access to Policy	Manager Admin
Single Sign-On (SSO)	2.	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGn	oup devices
- 尊 本地用户	3. 🗐	[Aruba Device Access Policy]	TACACS	Enforcement policy controlling access to Aruba	device
- 🗘 端点	4. 🗊	[Guest Operator Logins]	Applicat	ion Enforcement policy controlling access to Guest	application
一尊 静态主机列表	5. 🗐	[Insight Operator Logins]	Applicat	ion Enforcement policy controlling access to Insigh	t application
一心 角色	6. 🗉	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access	
一〇二角色映射	7.	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access	
▼ 安至状况 ● 按到時間		- 6-			(日本) (日本) (日本)
↓ 回題 ↓ 配置文件 ▲ 四時 ■ Profile and Network Scan ◎ 策略仿真					
5 Anna					

在强制执行选项卡中, 输入下面的参数:

- ✓ 名称: task6-guest-register-enforcement-policy
- ✓ 强制执行类型: RADIUS
- ✓ 默认配置文件: [Deny Access Profile]

配置»强制执行»策略»添	ta da	
强制执行策略		
强制执行 规则 概要		
名称:	task6-guest-register-enforcement-policy	
说明:		
强制执行类型:	● RADIUS ◎ TACACS+ ◎ WEBAUTH (SNMP/Agent/CLI/CoA) ◎ 应用程序 ◎ Event	
默认配置文件:	[Deny Access Profile] View Details Modify	添加新强制执行配置文件

在规则选项卡中, 输入下面的参数:

- ✓ 规则: 点击 "Add Rule",配置如下:
 - 添加第一个规则条件是 GuestUser Role ID EQUALS 2
 - 添加第二个规则条件是 Tips Role EQUALS [User Authenticated]
 - 配置文件名: task6-guest-register-profile

配置 »	强制执行»策略»添加	D								
强制	执行策略									
强制挂	执行 规则 概要									
规则评	估算法:	◉ 选择第一个匹配 ◎ 选择所有匹配								
Enforce	ement Policy Rules:									
C	onditions			Acti	ons					
					Add Rule	Move Up ↑ Mo	ove Down ↓	Edit Rule	Remov	e Rule
规则指	細器	- <u>Al</u> itan iling - Ali								0
				条件						
匹配じ	以下所有条件:									
	类型	名称		运算符		值				
1.	GuestUser	Role ID		EQUALS		2			ĒÐ	Ť
2.	Tips	Role		EQUALS		[User Aut	henticated]		B)	÷
- 3.	Click to add									
			22.441	长和平文件						
			124(10)1/							
配置:	文件名:	[RADIUS] task6-guest-register-profile	Move Up ↑ Move Down ↓ Remove							
		Select to Add	٣							
								保	F N	消

在概要选项卡中,对整体配置进行总览:

配置»强制执行»策略» 品制力行等政	添加
强制执行 规则 概	8
强制执行:	
名称:	task6-guest-register-enforcement-policy
说明:	
强制执行类型:	RADIUS
默认配置文件:	[Deny Access Profile]
规则:	
规则评估算法:	First applicable



	Conditions	Actions
1.	(GuestUser:Role ID EQUALS 2) AND (Tips:Role EQUALS [User Authenticated])	task6-guest-register-profile

第3步:找到配置 - > 服务,点击右上角的"添加服务"按钮,增加一个服务:

aruba				ClearPass Policy	Manager		Menu
直接	0 配置 > 1	很劳					
1 11 12	 服务 						👍 添加服务
	0						▲ 导入服务
○ 武处开始	This nai	ae shows	the current list and order of se	rvices that ClearPass follows during	n authentication and authoriza	tion	· +- L1/107
3 服务		, contraction		nees onee orean ass renorms during			
14.认证	过滤器:	名称	▼ 包含 ▼	Go Go	Clear Filter		显示 1000 • 记
一樽 方法			新序 名容		类型	根板	状态
	1.	0	[Policy Manager Ad	min Network Login Service]	TACACS	TACACS+ Enforcement	0
The Single Sign-On (SSO)	2.		2 [AirGroup Authoriza	ition Service]	RADIUS	RADIUS Enforcement (Generic)	0
	3.	0 :	3 [Aruba Device Acce	ss Service]	TACACS	TACACS+ Enforcement	0
-◎ 端点	4.		Guest Operator Lo	gins]	Application	Aruba Application Authentication	0
一心 静态主机列表	5.	0.1	5 [Insight Operator L	ogins]	Application	Aruba Application Authentication	0
一章 角色	8-2-2-6	100.00	e -			20 AC	the devided to the matter
書 强制执行 ↓ 前略 ↓ 前感 ■ Profile and Network Scan ↓ 新略仿真							
= 日本 版权所有 2015 Aruba Networks。保留所有权:	利.		00	t 11, 2019 11:29:16 CST		ClearPass 領略管	理器 6.7.9.109195 开启 CLABV

在服务选项卡中, 输入下面的参数:

- ✓ 类型: RADIUS Enforcement (Generic)
- ✓ 名称: task6-guest-register-auth-service
- ✓ 匹配项:以下所有条件
- ✓ 服务规则:
 - 1、 Radius:IETF NAS-Port-Type EQUALS Wireless-802.11 (19)
 - 2、Radius:IETF Service-Type BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8)
 - 3、Radius:Aruba Aruba-Essid-Name EQUALS labX-guest-register (X: 1……6)

配置	»服务 » 漆加						
服务	z,						
服	§ 认证 角色 强	制执行 概要					
类型:		RADIUS Enforcement (Ge	eneric) 🔻				
名称:		task6-guest-register-auth-se	ervice				
说明:			li				
监视机	莫式:	■ 启用以监视无强制执行的	网络访问				
更多	先项:	■ 授权 🔲 安全状况遵从	■ 审计终端主机 ■ 配置文件端点 ■ Accounting P	Proxy			
_			服务	5规则			
匹配马	页 🔍 任意或 🖲 以下所	有条件:					
	类型		名称	运算符	值		
1.	Radius:IETF		NAS-Port-Type	EQUALS	Wireless-802.11 (19)		Û
2.	Radius:IETF		Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	Ħħ	÷
3.	Radius:Aruba		Aruba-Essid-Name	EQUALS	lab1-guest-register	ĒÐ	Û
4	1 1100 10 200						_

在认证选项卡中, 输入下面的参数:



✓ 1、认证方法: [PAP]

v	认证源: [Guest User Repository][Local SQL DB]	
配置»服务»添加 服务		
服务 认证 角色	ī	
认证方法:	AP Move Up 1 Move Down j Remove View Detalls Modify	

\checkmark	2、	认证源:	[Guest User Repository][Local SQL DB]
--------------	----	------	---------------------------------------

认证方法:	[PAP]	Move Up ↑	添加新认证方法
		Move Down ↓	
		Remove	
		View Details	
		Modify	
	-Select to Add		
认证源:	[Guest User Repository] [Local SQL DB]	Move Up ↑	添加新认证源
		Move Down ↓	
		Remove	
		View Details	
		Modify	
	Select to Add]	
剥离用户名规则:	□ 启用以指定以逗号分隔的规则列表,用于剥离	户名前缀或后缀	
Service Certificate:	Select to Add		View Certificate Details

在角色选项卡中,暂时不做任何配置(详细内容可以参考高级介绍部分)

✓ 角色映射策略: 空

配置 » 服务 » 添加			
服务			
服务 认证 角色 •	强制执行 概要		
角色映射策略:	Select V	Modify	添加新角色映射策
		角色映射策略详细信息	
说明:	-		
默认角色:	-		
规则评估算法:	-		
条件			角色

在强制执行选项卡中, 输入下面的参数:

✓ 强制执行策略: task6-guest-register-enforcement-policy (即第2步中创建的强制执行策略)

配置 » 服务 » 添加		
服务		
服务认证角色强	NULL NULL NULL NULL NULL NULL NULL NULL	
使用缓存的结果:	◎ 使用从上一会话中缓存的角色和安全状况属性	
强制执行策略:	task6-guest-register-enforcement-policy Modify	添加新强制执行策略
	强制执行策略详细信息	
说明:		
默认配置文件:	[Deny Access Profile]	
规则评估算法:	first-applicable	
条件	强制执行配置文件	
1. (GuestUser:Role I	EQUALS 2) task6-guest-register-profile	

在概要选项卡中,对配置进行总览:

配置 »	服务 » 添加				
服务					
服务	认证 角色	强制执行 数据			
服务:					
类型:		RADIUS Enforcement (Generic)			
名称:		task6-guest-register-auth-service			
说明:					
监視模	式:	Disabled			
更多迭	项:	-			
				服务规则	
匹配以	下所有条件:				
	类型		名称	运算符	值
1.	Radius:IETF		NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF		Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
з.	Radius: Aruba		Aruba-Essid-Name	EQUALS	lab1-guest-register
认证:					
认证方	法:	[PAP]			
认证源	:	[Guest User Repository] [Local SC	(LDB]		
剥离用	户名规则:	-			
Servio	e Certificate:	-			
角色:					
角色映	射策略:	-			
强制执	行:				
使用缓	存的结果:	Disabled			
强制执	行策略:	task6-guest-register-enforcement	-policy		
< 返	回服务				Next→ 保存 Cancel

7.4 控制器配置

7.4.1 添加无线信号

第1步: 使用 Web 方式登录到 Mobility Master (10.X.50.11) (X:1……6),找到 Managed Network ->

labX (X:1……6) -> Configuration -> WLANs 点击 "+" 进入创建一个新的无线配置向导

		-					
Aruba MOBILITY MASTI Iab1-mm-1	ER	CONTROLLERS ACC ⊙ 2 ① 0 ⊙	CESS POINTS CLIENT	S ALERTS		⑦ admin ∨	
Managed Network > lab1 >							Ş
€ <mark>k</mark> Q	Dashboard	WLANs o					
🔁 Mobility Master	Configuration	NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION		
📼 lab1-mm-1	WLANs						
🔁 Managed Network (2)	Roles & Policies						
🗁 lab1 (2)	Access Points						
📼 lab1-md1	AP Groups						
📼 lab1-md2	Authentication	!					
	Services						
	Interfaces						
	Controllers						
	System						
	Tasks						
	Maintenance						

第2步: General 常规选项设置

- ✓ Name(ssid): labX-guest-register (X : 1 ·····6)
- ✓ Primary usage: Guest
- ✓ Broadcast on: Select AP Groups-->labX-group (X: 1 ……6) (前面的task中已经创建了该ap group)
- ✓ Forwarding mode : Tunnel



New WLAN				
Gene	ral	VLANs	Security	Access
Name (ssid):	lab1-guest-register	Guet		
Thinkiy usage.	Select AP Groups 👻	Guest		
Broadcast on:	default ↓ ✔ lab1-group ↓			
Forwarding mode:	Tunnel 🗸			

第3步:配置用户的 VLAN

✓ VLAN : wireless-user-vlan

NOTE 在向导中,如果此时先前的task中已经创好了无线用户的VLAN ID,那么我们可以在VLAN的下拉列表中直接选择需要的VLAN,这里我们选择wireless-user-vlan。

General VLANs Security Access	New WLAN					
/LAN: wireless-user-vlan	General	VLANs	Security	Access		
	N: wireless-user-vlan 🗸					

第4步:安全选项设置

- 1、clearpass or other external captive portal: 选中
- 2、Auth servers: cppm , 即选择之前lab中创建好的RADIUS(cppm)认证服务器
- 3、CPPM host: 10.X.50.41 (X:1……6),该地址是让系统自动生成访客认证前角色中的白名 单访问策略,即无需认证就可以访问到的资源。
- 4、CPPM page: /guest/guest_register_login.php?_browser=1,该page是在先前cppm上已 经创建好的登录页面链接的一部分,即访客被重定向到的登录页面做自注册和认证。

NOTE 这里不需要输入完整的http://开头的URL,仅仅是IP地址后的部分。这样向导会自动补全<u>https://clearpass-ip</u>前 缀,且是https://开头的。初始化向导后,补全的URL是



https://10.2.50.41/guest/guest_register_login.php?_browser=1,该URL就是captive portal profile中的Login page

	5、Redirect URL:	http://www.arubanetworks.com,	该URL即访客认证后获得的欢迎页面链接
--	-----------------	-------------------------------	---------------------

General	VLANS		Security	Acces
	ſ	Captive Porta	l Options:	
ClearPass or other external	captive portal		cppm2	
Internal captive portal with au	uthentication			
Internal captive portal with er	nail registration	Auth servers:		
nternal captive portal, no aut	h or registration		+	
No Captive Portal		CPPM host:	10.2.50.41	
		CPPM page:	/guest/guest_registe	
		Redirect URL:	http://www.arubane	

第5步:访问权限设置

- 1、Default role: lab1-guest-register-guest-logon (向导自动创建好的,就是Portal认证前的 角色,对应到aaa profile中的initial role)
- 2、Finish: 点击右下角的Finish 蓝色按钮,完成向导配置

New WLAN			
General	VLANS	Security	Access
Default role: lab1-guest	register-guest-logon		

第6步: 更改 Captive Portal Authentication 配置, Managed Network - > labX (X : 1 ····6) -> Configuration -> Authentication -> L3 Authentication ->Captive Portal Authentication -> labxguest-register_cppm_prof (X : 1 ·····6). 在 Login page 中的 https 更改为 http, 避免页面跳转时的证

Back

Cancel

书告警提示,最后点击 Submit 按钮提交配置更改。(因为默认 aruba clearpass 采用的是自签服务器证书,如果需要 https 的安全跳转,强烈建议使用商业签发证书导入到 clearpass 中使用)。

rubo MOBILITY I Iab1-m	MASTER m-1	CONTROLLERSACCESS POINTSCLO2OO1O7	ALERTS	③ admin ~
Managed Network > lab1 >	£			
	Q Dashboard			
lobility Master	Configuration	Auth Servers AAA Profiles L2 Authentication	L3 Authentication User Rules Advance	d
Iab1-mm-1	WIANC	Captive Portal Authentication	Default Role:	guest
anaged Network (2)	Roles & Policies	🕀 🖻 default	Default Guest Role:	guest
∋ lab1 (2)	Access Points	⊖ ☐ lab1-guest-register	Dedicert Davisor	10
🖾 lab1-md1	AP Groups	G Server Group	lies Lodes	sec
lab1-md2	Authentication	⊕ lab1-portal_cppm_pro	User Login:	
	Services	Stateful Kerberos Authentication	Logout popup window:	
	Interfacer	G Stateful NTLM Authentication	Use HTTP for authentication:	
	Controllers	VIA Authentication	Logon wait minimum wait:	5 sec
	Controllers	VIA Connection	Leave whit enables on white	10
	Taska	VIA Web Authentication	Logon wait maximum wait.	io sec
	IdSKS	PVN Authentication	logon wait CPU utilization threshold:	60 %
	Maintenance	G WisPr Authentication	Max Authentication failures:	0
			Show FQDN:	
			Authentication Protocol:	PAP
	ArubaMM VA, E.4.0.0 MASTER Imr-1	CONTROLLERS ACCESS POINTS CLI © 2 0 0 0 1 0 0 7 2	Login page: Login page: ALERTS ALE	https://10.250.41/gu Cancel Submit Submit As @ admin ~
MOBILITY Jab5-m Managed Network > Jab1 >	ArubaMM VA, 8400 MASTER	CONTROLLERS ACCESS POINTS CLI	Login page: ALERTS ALERTS O 0 1 1 20 10	https://10.2.50.41/gu Cancel Submit As @ admin ~ Pending Change
MOBILITY lab1-m	Arabaketwik 8.400 MASTER 9 Dashboard	CONTROLLERS ACCESS POINTS CL © 2 0 0 0 1 0 0 7 2 Auth Servers AAA Profiles L2 Authentication	Login page: ALERIS O	Cancel Submit As
Anaged Network > Tab1 > oblity Master	ArabaMMWA 8.400 MASTER 9 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	CONTROLLERS ACCESS POINTS CL CONTROLLERS ACCESS POINTS CL CONTRO	Login page: ALERIS O	Cancel Submit As
MOBILITY: Iab1-m Anaged Network > Iab1 > oblity Master D Iab1-mm-1	ArubaMMVA, 8.400 MASTER P Dashboard Configuration WLANS	CONTROLLERS ACCESS POINTS CL © 2 00 0 1 00 0 2 Auth Servers AAA Profiles L2 Authentication © 1 versure © 1 tub guest-register	Login page: ALERTS O	Attps://10.2.50.41/gu
CUDO MOBILITY lab1-m tanaged Network > lab1 > obility Master lab1-mm-1 anaged Network (2)	ArubaMMWA, 8.4.0.0 MASTER P P Dashboard Configuration WLANS Roles & Policies	CONTROLLERS ACCESS POINTS CL © 2 00 01 00 0 2 Auth Servers AAA Profiles L2 Authentication © 1 ubl guest-register © 1 ubl guest-register © 2 ubl guest-register © 3 bit server for up	Login page: ALERTS O O Con C	Cancel Submit As Submit As Pending Chang d guest 10 sec
MOBILITY lab1-m bility Master lab1-mm-1 anaged Network (2) bility (2) bi	ArubaMM.VA, E.4.00 MASTER Pashboard Configuration VULANS Roles & Policies Access Points	CONTROLLERS ACCESS POINTS CL © 2 00 01 00 0 2 Auth Servers AAA Profiles L2 Authentication © 1 ubl-guart-register © 1 ubl-guart-register © 1 ubl-poral.cpm.pro © 1 Stardel Kennes Authentication		Cancel Submit As Cancel Submit As Pending Chang d guest 10 sec U
Amobility Iabt-mini-1 Amaged Network 2 Iabt 3 Iabt-mm-1 Amaged Network (2) 5 Iabt (2) C Iabt md1	ArubaMMVA, E4.00 MASTER Immiliar Obshiboard Configuration VULANS Roles & Policies Access Points A P Groups	Auth Servers AAA Profiles L2 Authentication		Cancel Submit As Cancel Submit As Pending Change guest 10 sec V
Amaged Network 2 lab1 3 anaged Network 2 lab1 3 anaged Network (2) 5 lab1 (2) C lab1-md1 C lab1-md2	AubaMAW, E.4.00 MASTER Dashboard Configuration WLANs Roles & Policies Access Points AP Groups Authentication	Auth Servers AAA Profiles L2 Authentication		Cancel Submit As Cancel Submit As Pending Chang d guest 10 sec V U
Amaged Network > lab1 = bility Master anaged Network (2) bility Lab1-mm-1 anaged Network (2) bility Lab1-mm-1 bility Lab1-m	AubaMAW, 8.400 MASTER Dashboard Configuration WILANs Roles & Policies Access Points Access Points Access Points Access Points Access Points Services	Auth Servers AAA Profiles L2 Authentication Contractions AAA Profiles L2 Authentication Contractions Contractio		Cancel Submit As Cancel Submit As Pending Change d guest 10 sec V 5 sec
Annaged Network > lab1 : billity Master billity Master bill	AubaMAW, 8.400 MASTER Dashboard Configuration WLANs Roles Polities Acces Polities Acces Polities Acces Polities Authentication Services Interfaces	Auth Servers AAA Profiles L2 Authentication Image: Contract Content Co		https://10.2.50.41/gu Cancel Submit As @ admin ~ Pending Change d guest 10 sec ~ 5 sec 10 sec
Annaged Network > lab1 : bility Master bility Mas	AutoMMM, 2.000 MASTER MASTER Configuration VULANS Roles & Polices AC Groups AC Groups AC Groups Authentication Services Interfaces Controllers	Auth Servers AAA Profiles L2 Authentication		https://10.2.50.41/gi Cancel Submit As @ admin ~ Pending Change d guest 10 sec > 5 5 5 60 94, 00
Anaged Network > lab1 > ability Master bility Master lab1-mm-1 anaged Network (2) lab1-m1 c lab1-m1 c lab1-m1	AutoMMAX, 2.000 MASTER MASTER	CONTROLLERS ACCESS POINTS CL Q 2 Q 1 Q 2 Q 2 Auth Servers AAA Profiles L2 Authentication Q 1 University Q 1 Q 2 Auth Servers AAA Profiles L2 Authentication Q 1 University Q 1 Q 2 Q 1 University Q 2 Q 2 Q 1 Q 2 Q 2 Q 2 Auth Servers AAA Profiles L2 Authentication Q 1 University Q 2 Q 2 Q 1 University Q 2 Q 2 Q 1 University L2 Authentication Q 2 Q 1 University Q 2 Q 2 Q 1 University L2 Authentication Q 2 Q 1 University University Q 2 Q 1 University Q 2 Q 2 Q 2 Q 1 University Stateful Kerberos Authentication Q 2 Q 1 Q 2 Q 2 Q 2 Q 2 Q 2 Q 1 VN Authentication Q 2 <td< td=""><td></td><td>Cancel Submit As Cancel Submit As Pending Change d guest 10 sec 5 sec 10 sec 60 %</td></td<>		Cancel Submit As Cancel Submit As Pending Change d guest 10 sec 5 sec 10 sec 60 %
Anaged Network > lab1 > oblity Master lab1-mm-1 anaged Network (2) lab1-md1 anaged Network (2) lab1-md1 anaged Network (2) lab1-md1	AubaMMAX, 8.400 MASTER MASTER P Dashboard Configuration VULN's Roles & Policies Access Policies Acce	CONTROLLESS ACCESS POINTS CL O 2 O 0 1 O 0 2 Auth Servers AAA Profiles L2 Authentication O 1 Bub Lysees register Stateful Kerbers Authentication O 1 Stateful Kerbers Authentication O 1 Stateful Kerbers Authentication O 1 VA Neb Authentication O 1 VA Neb Authentication O 1 VPN Authentication	Login page: ALERTS O ALERTS ALERTS O ALERTS O ALERTS ALERTS	https://10.2.50.41/gu Cancel Submit As Image: Concelling Change Image: Concel
Anaged Network > labt > Anaged Network > labt > obility Master I labt-mm-1 anaged Network (2) I labt-md1 I labt-md2	AubaMMAX, 8.400 MASTER MASTER P Dashboard Configuration VULNS Roles & Policies Access Polints ACCess P	CONTROLLESS ACCESS POINTS CL Q 2 Q 2 Q 1 Q 2 Auth Servers AAA Profiles L2 Authentication Q 1 Q 1 Q 2 Auth Servers AAA Profiles L2 Authentication Q 1 Q 1 Q 2 Q 1 University Q 2 Q 1 Q 1 Q 2 Q 1 Q 1 Q 2 Q 2 Q 1 Q 2 Q 2 Q 2 Q 2 Q 2 Auth Servers AAA Profiles L2 Authentication Q 1 Q 10 Q 2 Q 1 University Q 2 Q 1 University Q 2 Q 1 University Q 2 Q 1 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2		https://10.2.50.41/gu Cancel Submit As @ admin ~ Pending Change d guest 10 10 sec V 5 sec 10 sec 0 % 0 % 0 %
Anaged Network > lab1 > ability Master bility Mas	AutoMMAX, 2.000 MASTER MASTER Configuration VULNS Roles & Politics Access Points A Coroups Autoentication Services Interfaces Controllers System Tasks Maintenance	CONTROLLERS ACCESS POINTS CL Q 2 Q 1 Q 2 Q 2 Auth Servers AAA Profiles L2 Authentication Q 1 University Q 2 Q 2 Auth Servers AAA Profiles L2 Authentication Q 1 University Q 2 Q 2 Q 1 University Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Auth Servers AAA Profiles L2 Authentication Q 2 Q 1 University Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2	Login page: ALERTS	https://10.2.50.41/gu Cancel Submit As @ admin ~ Pending Change d guest 10 sec 9 10 sec 9<
Anaged Network > labt > Anaged Network > labt > obility Master is labt-mm-1 anaged Network (2) is labt-md1 is labt-md1 is labt-md2	AutoMMAX, 2.000 MASTER Configuration VVLNS Roles & Policies Access Polints Access Polints Access Polints Access Polints Controllers Services Interfaces Controllers System Tasks Maintenance	CONTROLLERS ACCESS POINTS CL Q 2 Q 1 Q 2 Q 2 Auth Servers AAA Profiles L2 Authentication Q 1 Q 1 Q 2 Vernine Q 2 Q 2 Q 1 Q 2 Q 2 Q 2 Q 2 Q 2 Auth Servers AAA Profiles L2 Authentication Q 1 Q 1 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Auth Servers ALA Profiles L2 Authentication Q 1 Q 1 Q 2 Q 2 Q 1 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 Q 2 <td>Login page: ALERTS ALERTS</td> <td>https://10.2.50.41/gi Cancel Submit As Cancel Submit As @ admin ~ Pending Change d guest 10 sec 9 5 5 9 <tr< td=""></tr<></td>	Login page: ALERTS	https://10.2.50.41/gi Cancel Submit As Cancel Submit As @ admin ~ Pending Change d guest 10 sec 9 5 5 9 <tr< td=""></tr<>

第7步: 配置保存并同步给 md 设备

- 1、Pending Changes: 点击右上角的该按钮
- 2、Deploy changes : 点击该按钮



aruba MOBILITY Iab1-n	MASTER 1m-1	CONTROLLERS ACCESS POINTS CLIEM	ALERTS	(?) admin ~
Managed Network > lab1	>			Pending Changes
A	0			
C Mobility Master	Dashboard	Auth Servers AAA Profiles L2 Authentication	L3 Authentication User Rules Advance	ed
	Configuration		Default Guest Role:	guest 🗸
	WLANs	O 🗗 lab1-guest-register	Redirect Pause:	10 sec
Managed Network (2)	Roles & Policies	G Server Group	liter Legin	
🗁 lab1 (2)	Access Points	Iab1-portal_cppm_pro	Guest Login:	
🖾 lab1-md1	AP Groups	Stateful Kerberos Authentication	Logout popup window:	
🖘 lab1-md2	Authentication	Stateful NTLM Authentication	Use HTTP for authentication:	
	Services	VIA Authentication	Logon wait minimum wait:	5 500
	Interfaces	VIA Connection	Logon Harcininian Harc	5
	Controllers	VIA Web Authentication	Logon walt maximum wait:	10 sec
	System	OPN Authentication	logon wait CPU utilization threshold:	60 %
	Tacke	⊕ WISPr Authentication	Max Authentication failures:	0
	Malatarara		Show FQDN:	
	Walltenatice		Authentication Protocol:	
			 Login page: 	http://10.2.50.41/gue
			Welcome page:	/auth/welcome.html
		4		•
				Cancel Submit Submit As
MODILITY	ArubaMM-VA, 8.4.0.0			
aruba lab1-m	im-1	CONTROLLERS ACCESS POINTS CLIENT	ALERTS	admin ~
_				
Managed Network > lab1 >				Pending Changes C
Dashboard	New WLAN			
Configuration				
WLANs	The new WLAN can be viewed in the W	LAN List		
Roles & Policies	NOTE: The new WLAN has been added	to the pending changes list. To deploy all pending changes, click Pending C	hanges at top right.	
Access Points				
Access Points				
AP Groups				
Authentication				
Services				
Interfaces				
Controllers				
System				
Tasks				
Maintenance				
mannenance				
Pending Change	es			
Rendin	a Changes for 2 Cont	rallars		
🔽 Pendin	g Changes for 2 Contr	rollers		
🖌 Pendin	g Changes for 2 Conti	rollers		
 ✓ Pendin ✓ (+) M 	g Changes for 2 Cont i Nanaged Network > lab	r ollers 1 (2 Controllers)		
✓ Pendin✓ ↔ M	g Changes for 2 Contr Nanaged Network > lab	rollers 1 (2 Controllers)		
✓ Pendin✓	ig Changes for 2 Conti Managed Network > lab	r ollers 1 (2 Controllers)		
✓ Pendin ✓ ↔ M	ig Changes for 2 Conti Managed Network > lab	rollers 1 (2 Controllers)		
✓ Pendin✓ ✓	ig Changes for 2 Conti Janaged Network > lab	rollers 1 (2 Controllers)	Discard changes	Doploy chapter
✓ Pendin✓ ✓ ✓ ♦	i g Changes for 2 Conti /lanaged Network > lab	rollers 1 (2 Controllers) Clos	e Discard changes	Deploy changes

7.4.2 添加 Portal 重定向

内容请参考前面4.4.3章节相关配置。

7.4.3 添加角色

```
第1步: 使用 Web 方式登录到 Mobility Master (10.X.50.11) (X:1……6), 找到 Managed Network - > labX (X:1……6) -> Configuration -> Roles & Policies 点击 "+" 进入创建一个新的角色 (guest-register-role)。
```

AND		CONTROLLERS ACCESS POINTS ∅ 2 0 ∅ 1 0	CLIENTS ALERTS	٢	admin 🗸	
Managed Network > lab1 >						¢
Managed Network > 1801 > C Dat Mobility Master Cor Iab1-mm-1 Managed Network (2) Iab1-md1 Iab1-md2	shiboard nfiguration WLANS Roles & Policies Access Points Ar Groups Authentication Services Interfaces Controllers System Tasks aintenance	Policies Applications Allases tion will require PEP license to be installed. Please go to 13 - dotts -	HPT Aruba My Networking Pertal to activate license key. RULES 23 Rules 23 Rules 23 Rules 23 Rules 23 Rules 23 Rules 23 Rules 14 Rules 14 Rules			
	M-VA, 8.4.0.0					

- ✓ Name:
- guest-register-role, 新建一个访客Portal认证后获得的role

New Role	
Name:	guest-register-role
	Cancel Submit
✓	1、在roles里面,选择上一步创建好的guest-register-role
\checkmark	2、再点击右下角的show Advanced View

NOTE 需要事先在右上角的蓝色字体admin的下拉列表中选择preferences, 勾选 show advanced profiles



	m-1				ⓓ admin ▾
← Managed Network > lab1 >					Pending Changes 🗘
C Mobility Master	Q Dashboard	Roles Policies Applications	Aliases		į.
lab1-mm-1	Configuration				
Managed Network (2)	WLANs	Roles 19			
	Roles & Policies	NAME	RULES		=
(2)	Access Points	authenticated	4 Rules		
lab1-md1	AP Groups	voice leader role	41 Rules		
📼 lab1-md2	Authentication	employee-role	1 Rules		
	Services	lab1-portal-guest-logon	28 Rules		
	Interfaces	lab1-guest	2 Rules		
	Controllers	lab1-guest-register-guest-logon	28 Rules		
	System	guest-register-role	0 Rules		<u>.</u>
	Tasks	L+			
	Maintenance				Charles Advanced March
	Walliterialite	guest-register-role			Show Advanced View
		Global Rules			
		IP VERSION SOURCE	DESTINATION SERVIC	E/APPLICATION ACTION	
	ASTER	CONTROLLERS ACCESS PO	INTS CLIENTS ALERTS		
arupo lab1-m	MASTER m-1	CONTROLLERS ACCESS PO	INTS CLIENTS ALERTS ○ 0 ○ 2 ▷ 0 △ 0		admin ~
Managed Network > lab1 >	AASTER m-1	$\begin{array}{c} \text{CONTROLLERS} \\ \bigcirc 2 \\ \bigcirc 0 \\ \end{array} \begin{array}{c} \text{ACCESS PO} \\ \bigcirc 1 \\ \hline \end{array}$	INTS CLIENTS ALERTS ○ 0		 admin ~ Pending Changes (
Kanaged Network > lab1 >	AASTER m-1 Dashboard	CONTROLLERS ACCESS PO	INTS CLIENTS ALERTS		③ admin ~ Pending Changes (
Konstant And Andrew Andre	Q Dashboard Configuration	CONTROLLERS ACCESS PO © 2 0 0 0 1 0 Roles Policies Applications	INTS CLIENTS ALERTS ○ 0		③ admin ~ Pending Changes (
Konstant And Antiperson Anti	Q Dashboard Configuration	CONTROLLERS ACCESS PO © 2 0 0 0 1 0 Roles Policies Applications NAME	INTS CLIENTS ALERTS ○ 0		admin Pending Changes C
Managed Network > lab1 > Managed Network > lab1 > Mobility Master Iab1-mm-1 Managed Network (2)	Q Dashboard Configuration WLANS Dask & Policies	CONTROLLERS ACCESS PO © 2 0 0 0 1 0 Roles Policies Applications NAME authenticated	INTS CLIENTS ALERTS ○ 0		admin ~ Pending Changes (
Managed Network > lab1 > Managed Network > lab1 > Mobility Master alab1-mm-1 Managed Network (2) Alab1 (2)	Configuration WLANS Roles & Policies Accord Policies	CONTROLLERS ACCESS PO 2 0 0 0 1 0 Roles Policies Applications NAME authenticated voice	INTS CLIENTS ALERTS 0 •		③ admin ~ Pending Changes ()
Kanaged Network > lab1 > Managed Network > lab1 > Mobility Master Silab1-mm-1 Managed Network (2) Plab1(2) Silab1.mm1	AASTER m-1 Dashboard Configuration WLANs Roles & Policies Access Points	CONTROLLERS ACCESS PO © 2 0 0 0 1 0 Roles Policies Applications NAME authenticated voice leaderrole	INTS CLIENTS ALERTS 0 ? 2 0 0 0 Allases RULES 4 1 <td></td> <td>admin ~ Pending Changes ()</td>		admin ~ Pending Changes ()
Kanaged Network > lab1 > lab1 Managed Network > lab1 > lab1 Managed Network (2) P lab1 (2) Blab1-mm-1	AASTER m-1 Dashboard Configuration WLANs Roles & Policies Access Points AP Groups	CONTROLLERS ACCESS PO ○ 2 ○ 0 ○ 1 ○ Roles Policies Applications NAME authenticated voice leader-role employee-role	INTS CLIENTS ALERTS 0 ? 2 0 0 0 Allases RULES 4 1 <td></td> <td>admin ~ Pending Changes (</td>		admin ~ Pending Changes (
Kanaged Network > lab1 > Managed Network > lab1 > Mobility Master Solution Managed Network (2) Solution lab1-mm1 lab1-mm1 lab1-md1 lab1-md2	AASTER m-1 Dashboard Configuration WLANs Roles & Policies Access Points ACcess Points AP Groups Authentication	CONTROLLERS ACCESS PO 2 0 0 0 1 0 Roles Policies Applications NAME authenticated voice leader-role employee-role tabi-portal guest-logon	INTS CLIENTS ALERTS O O O O O O O O O O O O O O O O O O O		admin ~ Pending Changes (
Kanaged Network > lab1 > Managed Network > lab1 > Mobility Master Si lab1-mm-1 Managed Network (2) Si lab1-md1 Si lab1-md2	Configuration ULANS Roles & Policies ACcess Points ACcess Points ACcess Points ACcess Points Services	CONTROLLERS ACCESS PO 2 0 0 0 1 0 Roles Policies Applications NAME authenticated voice lieader-role employee-role liabi-portal-guest.logon labi-guest	INTS CLIENTS ALERTS 0 ? 2 0 0 0 Aliases 4 8 1		3 admin ~ Pending Changes (
Kanaged Network > lab1 > Managed Network > lab1 > Mobility Master iab1-mm-1 Managed Network (2) iab1-md1 iab1-md2	C Dashboard Configuration WLANs Roles & Policies Access Points A Afroug Authentication Services Interfaces	CONTROLLERS ACCESS PO ⊘ 2 ○ 0 0 ∞ 1 0 Roles Policies Applications NAME authenticated voice leader-role leader-role leabi-guest-logon labi-guest-sologon	INTS CLIENTS ALERTS O O P 2 P 0 A O		ending Changes (
Kanaged Network > lab1 - mir Managed Network > lab1 - mir Managed Network (2) Deltab1 (2) Deltab1 (2) Deltab1 (2) Deltab1 - md1 Deltab1 - md2	AASTER m-1 Dashboard Configuration VLANs Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers	CONTROLLERS ACCESS PO ⊘ 2 ○ 0 0 ∞ 1 0 Roles Policies Applications NAME authenticated voice leader-role labi-guest-register-guest-logon labi-guest-register-guest-logon	INTS CLIENTS ALERTS O O P 2 P 0 A O		ending Changes (
Kanaged Network > lab1 - mir Managed Network > lab1 - mir Managed Network (2) Iab1 (2) Iab1 (2) Iab1 - md1 Iab1-md2	AASTER m-1 Dashboard Configuration VLANs Roles & Policies Access Points A Croups Authentication Services Interfaces Controllers System	CONTROLLERS ACCESS PO ⊘ 2 ○ 0 0 ∞ 1 0 Roles Policies Applications NAME authenticated voice leader-role leader-role leader-role leb1-guest-register-guest-logon Lguest-register-role ↓	INTS CLIENTS ALERTS O O P 2 P 0 O O O		ending Changes (
Kanaged Network > lab1 > Mobility Master lab1-mm-1 Managed Network (2) P lab1 (2) lab1-md1 lab1-md2	AASTER m-1 Dashboard Configuration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers System Tacks	CONTROLLERS ACCESS PO 2 0 0 0 1 0 Roles Policies Applications NAME authenticated voice leader-role employee-role lab1-portal guest-logon lab1-portal guest-logon guest-register-role + guest-register-role Policies	INTS CLIENTS ALERTS O Q 2 0 0 0 0 0		ending Changes (
Kanaged Network > lab1 > Mobility Master State = Mobility Master State = Managed Network (2) State = lab1-mm1 Iab1-md1 Iab1-md2	AASTER m-1 Dashboard Configuration WLANs Roles & Policies ACcess Points AP Groups Authentication Services Interfaces Controllers System Tasks Mitheman	CONTROLLERS ACCESS PO ⊘ 2 ○ 0 0 ∞ 1 0 Roles Policies Applications NAME authenticated voice leader-role leader-role lab1-portal-guest-logon Lab1-portal-guest-logon Lab1-portal-guest-logon Lab1-portal-guest-logon Lab1-portal-guest-logon Lab1-portal-guest-logon Lab1-portal-guest-logon	INTS CLIENTS ALERTS CLIENTS ALERTS A	POLICY USAGE	admin ~ Pending Changes (
Kanaged Network > lab1 > Managed Network > lab1 > Mobility Master Solution Managed Network (2) Solution lab1-md1 Solution lab1-md2	AASTER M-1 Dashboard Configuration VILANS Notes & Policies Access Points A Access Points Authentication Services Interfaces Controllers System Tasks Maintenance	CONTROLLERS ACCESS PO ② 2 ○ 0 ○ 1 Roles Policies Applications NAME authenticated voice isader-role employee-role lab1-guest lab1-guest-register-role guest-register-role Policies NAME RULES co jobal-sacd 0	INTS CLIENTS ALERTS 0 0 2 0 0 1 10 10 10 10 10 10 10 10 10 10 10	POLICY USAGE logor, guest, ap-role, stateful-d	ending Changes ()
Kanaged Network > lab1 - mir Managed Network > lab1 - mir Managed Network (2) Deltab1 (2) Deltab1 (2) Deltab1 (2) Deltab1 - mir	AASTER MAASTER Configuration VLANs Roles & Policies Access Points A Coups Authentication Services Interfaces Controllers System Tasks Maintenance	CONTROLLERS ACCESS PO ② 2 ○ 0 ○ 1 Roles Policies Applications NAME authenticated voice leader-role leader-role leader-role leader-role leader-role leader-role leader-role leader-role leader-role leader-role leader-role leader-role guest-register-role Policies NAME RULES or global-sad	INTS CLIENTS ALERTS O ALERTS ALERTS ALERTS ALIASS A	POLICY USAGE logon guest, aprole, stateful-d guest-register-role	ending Changes (Pending Changes ()))))))))))))))))))
Kanaged Network > lab1 - mir Managed Network > lab1 - mir Managed Network (2) Deltab1 (2) Deltab1 (2) Deltab1 - mid Deltab1 - mid Deltab1 - mid	AASTER M-1 Dashboard Configuration VILANS Roles & Policies A Access Points A P Groups A Athentication Services Interfaces Controllers System Tasks Maintenance	CONTROLLERS ACCESS PO ② 2 ○ 0 ○ 1 Roles Policies Applications NAME authenticated voice leader-role leader-role leader-role leader-role leader-role leader-role guest-register-role Policies NAME RULES of global-sacl global-sacl 0 guest-register-role 0	NTS CLENTS ALERTS 0 2 0 0 0 Allases 0 0 0 0 0 Allases 4 1 0 0 0 0 4 Rules 4 1 0	POLICY USAGE logors guest, aprole, stateful.d guest-register-role guest-register-role	ending Changes (Pending Changes ()))))))))))))))))))
Anaged Network > lab1 - mi Managed Network > lab1 - mi Managed Network (2) Def lab1 (2) lab1-md1 lab1-md2	AASTER MAASTER AASTER Dashboard Configuration WLANS Notes & Policies A Access Points A ACCESS POINTS	CONTROLLERS ACCESS PO ② 2 ○ 0 ○ 1 Roles Policies Applications NAME authenticated voice Isader-role Isader-role Policies NAME RULES of on oper-role-said on	INTS CLIENTS ALERTS 0 ALERTS ALERTS 2 0 0 ALERTS Allases RULES 4 Rules 4 Rules 4 Rules 2 Rules	POLICY USAGE logon, guest, ap-role, stateful-d guest-register-role guest-register-role	ending Changes (Pending Changes ()
Kanaged Network > lab1 - mir Managed Network > lab1 - mir Managed Network (2) P lab1 (2) lab1-md1 lab1-md2	AASTER MAASTER Configuration VILANS Roles & Policies Access Points A P Groups Authentication Services Interfaces Controllers System Tasks Maintenance	CONTROLLERS ACCESS PO ② 2 ○ 0 ○ 1 Roles Policies Applications NAME authenticated voice leader-role employee-role lab1-portal-guest-logon lab1-portal-guest-logon lab1-portal-guest-logon lab1-portal-guest-logon guest-register-role Policies NAME RULES of 0 guest-register-role 0 guest-register-role 0 guest-register-role 0 H Exet-register-role	INTS CLIENTS ALERTS O O P 2 P 0 A O ALERTS Allases RULES ARUES ARUES ARUES BRUES BR	POLICY USAGE logon, guest, aprole, stateful-d guest-register-role guest-register-role	ending Changes (Pending Changes ()
Anaged Network > lab1 - mi Managed Network > lab1 - mi Managed Network (2) Del lab1 (2) lab1-md1 lab1-md2	AASTER m-1 Dashboard Configuration WLANs Roles & Policies ACcess Points AP Groups Authentication Services Interfaces Controllers System Tasks Maintenance	CONTROLLERS ACCESS PO ② 2 ○ 0 ○ 1 Roles Policies Applications NAME authenticated voice leader-role employee-role lab1-portal-guest-logon lab1-guest-register-role bb1-guest-register-role • make RULES of Quest-register-role	INTS CLIENTS ALERTS O ALERTS A	POLICY USAGE logon, guest, ap-role, stateful.d guest-register-role guest-register-role	Show Basic View

- ✓ 1、在policies窗口里面,选中并点击guest-register-role
- ✓ 2、进入到Rules窗口,点击"+"来新增规则。
- ✓ 3、Rule type: Access control, 新增一个permit all的策略(具体的访问权限可以后期根据 实际环境的需求来进行编辑和修改),最后点击 Submit按钮





NOTE 如果这里无法看到Submit变成蓝色背景,请在Action 里面切换下动作,然后再重新选择Permit,这样Submit按钮 会变成蓝色背景。



IP version:	IPv4 🗸	
Source:	Any 🗸	
Destination:	Any 🗸	
Service/app:	Any 🗸	
Action:	Permit 👻	
TOS:		
Time range:	- None - 🗸 Reset	
802.1p priority:	~	
Options:	Log Mirror Blacklist Disable scanning	
Queue:	·	

第2步: 配置保存并同步给md设备

- 1、Pending Changes: 右上角点击该按钮
- 2、Deploy changes : 点击该按钮

aruba lab1-mm-1	ER	CONTROLLERS	ACCESS POINTS	CLIENTS	ALERTS 0		admin ~
Managed Network > lab1 >							Pending Changes 🖧
Ck Q C→ Mobility Master	Dashboard Ro	oles Policies Appl	ications Aliases				
🖘 lab1-mm-1	WLANs	Roles 19					
Managed Network (2)	Roles & Policies	NAME		RULES			≡
🔁 lab1 (2)	Access Points	authenticated		4 Rules			*
🖾 lab1-md1	AP Groups	voice		41 Rules			
lab1-md2	Authentication	leader-role		1 Rules			
	Services	employee-role		1 Rules			
	Interfaces	lab1-guest		2 Rules			
	Controllers	lab1-guest-register-guest-logor	n	28 Rules			
	System	guest-register-role		1 Rules			*
	Tasks	+					
	Maintenance	guest-register-role	Policies Bandwid	th Captive Por	rtal More		Show Basic View
		NAME	RULES COUNT	TYPE		POLICY USAGE	=
		global-sacl	0	sessio	on	logon, guest, ap-role, stateful-d	
		apprf-guest-register-role-sacl	0	sessio	n	guest-register-role	
		guest-register-role	1	sessio	on	guest-register-role	
	ArubaMM-VA, 8.4.0.0	+					



Pending Changes	
✓ Pending Changes for 2 Controllers	
Managed Network > lab1 (2 Controllers)	
	Close Discard changes Deploy changes

7.4.4 添加计费

第1步:使用 Web 方式登录到 Mobility Master (10.X.50.11) (X:1…6),找到 Managed Network ->

labX (X:1……6) -> Configuration -> Authentication -> AAA Profiles 选项卡,点击 AAA 前面的

"+" 展开所有的 AAA Profile,找到之前向导已经生成的 labX-guest_register_aaa_prof (X:

1 ……6), 点击前面的"+"展开所有的配置项.

ALITY MASTI Iab1-mm-1	ER	CONTROLLERS ACCESS POINTS CLIENT ⊙ 2 ○ 0 ⊙ 1 ○ 0 ? 2	ALERTS № 0 △ 0	admin ~
Managed Network > lab1 >				Ŷ
Ck Q	Dashboard	Auth Servers AAA Profiles L2 Authentication	L3 Authentication User Rules Advanced	
lab1-mm-1	Configuration WLANs	default-tunneled-use	MAC Authentication Default Role:	guest
Managed Network (2)	Roles & Policies	 G G lab1-guest-register 	802.1X Authentication Default Role: Download Role from CPPM:	guest
🖾 lab1-md1	Access Points AP Groups	802.1X Authentication 802.1X Authentication Server Group	Set username from dhcp option 12:	
🖴 lab1-md2	Authentication	MAC Authentication	Multiple Server Accounting:	
	Services Interfaces	MAC Authentication Server Group RADIUS Accounting Server Group	User idle timeout:	secor
	Controllers	RFC 3576 server	Max IPv4 for wireless user: RADIUS Roaming Accounting:	2
	System Tasks	XML API server Iab1-mac_aaa_prof	RADIUS Interim Accounting:	
	Maintenance	lab1-peap_aaa_prof lab1-portal aaa prof	User derivation rules:	-None- 💙
			Wired to Wireless Roaming: Reauthenticate wired user on VLAN change:	
			Device Type Classification:	
		4	Cancel	Submit Submit As
	ArubaMM-VA, 8.4.0.0			

第2步: 选择 RADIUS Accounting Server Group,在右边配置窗口中,从 Server Group 下拉列表中选择之前 向导已经创建好的 labX-guest-register_dot1_svg (X:1……6).点击右下角的 Submit 按钮。



arupa lab1-mm-1		$ \bigcirc 2 \bigcirc 0 \bigcirc 1 \bigcirc 0 \bigcirc 2 \not 0 \bigcirc 1 \bigcirc 0 $	admin ~
← Managed Network > lab1 >			Ċ
Check Control Solution Instant Control Instant	shboard nfiguration WLANs Roles & Policies Access Polints AP Groups Authentication Services Interfaces Controllers System Tasks intenance	Auth Servers AAA Profiles L2 Authentication L3 Authentication Userver Group: Lab1-guest-registerdot1_svg Image: Control of the server Group Image: Control of the server Group Fail Through: Load Balance: Image: Control of the server Group Image: Control of the server Group Image: Control of the server Group Image: Control of the server XML API server Image: Control of the server Group Image: Control of the server XML API server Image: Control of the server Group Image: Control of the server XML API server Image: Control of the server Group Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server Image: Control of the server<	Cancel

- 第3步: 配置保存并同步给 md 设备
 - ✓ 1、Pending Changes: 右上角点击该按钮
 - ✓ 2、Deploy changes : 点击该按钮

ALCONDO MOBILITY MASTE Iab1-mm-1	R	CONTROLLERSACCESS POINTSCLIENTSALERTS \odot 2 \odot 0 \odot 1 \odot 0 $夺$ 2 $≠$ 0 \bigtriangleup 0	admin ~
← Managed Network > lab1 > Charlen Constraints (Constraints) ← Mobility Master ← lab1-mm-1 ← Managed Network (2) ← lab1 (2)	Dashboard Configuration WLANs Roles & Policies Access Points	Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced Image: Construction of the server Group: Image: Construction of the serve	Pending Changes 💠
 lab1-md1 lab1-md2 	AP Groups Authentication Services Interfaces Controllers System Tasks Maintenance	Cad Balance: Cad Balance: Cad	,
Pending Changes Pending Cha Pending Cha Hending Cha Hending Cha	anges for 2 Controlle ed Network > lab1 (2	rs Controllers)	Cancel Statemat
		Close Discard changes De	ploy changes

7.5 验证结果

7.5.1 终端侧的无线关联和访客自注册

我们在测试终端上,关联到打开浏览器输入任何网址,被重定向到ClearPass的Guest登录页面上。



点击Click Here, 进入到自注册页面。



Co D http://10.2.50.41/guest/guest_register_login.php7_browser=18cmd	i=login8mac=7c7a914652:b78bjp=10.1.20.1028te ρ - ≣ ¢ Ο Network Login ×	×
aruba	ClearPass Guest	
オピス用ルータルロード 上の月日 Network Login 第日: 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本		
<		>
Copyright 2019 Hewlett Packard Enterprise Development LP		
C () () http://10.2.50.41/guest/guest_register.php?_browsers1	P = 20 Q 自動注册 ×	×
aruba	ClearPass Guest	
BIRJ 2014 7-0171: BIRJ 2014 6-1 Control - Control -		•
		- 🗆 🗙
C http://10.2.50.41/guest/guest_register_receipt.php		n * a
アヨスタブなからなたかりは彼なま。 Tour account is currently availing confirmation. This page will refresh (every 30 seconds.	
Copyright 2019 Hewlett Packard Enterprise Development LP		>

接着联系人会收到该访客自注册的申请批复邮件,需要联系人批准下。



■ 中国电信 4G		21:11			● ♥ 7	0% 🔳
く收件箱			Æ	Ũ		\sim
Wireless a zhengxin.y	ccess re ang@hp	quest e.cor	fron n	ı:		
我 20:3 发至 我	7 详情					
zhengxin.ya	ang@hpe	e.com				
	aruba	Clea	irPass	Guest		
用户名: zhen 全名: yangzh 电话: 访问者请求由/	gxin.yang engxin 密作为担保人	@hpe. 的访问机	com 又限。单	击此处单	自击此处	·确
技术支持: O Aruba	Networks					
© Copyright 2019	Aruba, a Hewlett Pa	ackard Enterp	prise compa	iny.		
© Copyright 2019	Aruba, a Hewlett Pa	ackard Enter	prise compa	iny.		
© Copyright 2019	Aruba, a Hewlett Pa	ackard Enterg 邮件已结	prise compa ft束	iny.		
© Copyright 2019	Aruba, a Hewlett P4	ackard Enterg 邮件已结	prise compu	iny.		

等待联系人批准后,该页面的账号变成激活状态后,就可以登录认证了。

			×
🗧 😑 🖸 http://10.2	2.50.41/guest/guest_register_receipt.php?refresh=1	,○ - 目 C Q 目動注册回抗 ×	n 🛪 🛙
aruba		ClearPass Guest	
「面显示了您的说客帐」	户的详细信息。		
	访音注册收据		
担保人的姓名: adr	min 宋史殊户的人首的姓名。		
保人的电子邮件: bag	ggioyang@126.com 吴近班户的人员的电子邮件。		
您的姓名: yar	ngzhengxin 喻入志的全名。		
账户用户名: 🙎	zhengxin.yang@hpe.com		
访喜密码: 🥑	456920		
激活时间: 星期 计划	期五,11 十月 2019,8:38 下午 18月晚户的日期和时间。如果为空,希立即自局晚户。		
9(期时间: 星前 (可)	現六,12 十月 2019,8:38 下午 送)後戶得到期井被到除的日期即时间,如果为空,後戶得不会到期。		
新户状态: Ena 45	abled 第一个用于更改此版户状态的选项。		
	10		
-			
			>
opyright 2019 Hev	wlett Packard Enterprise Development LP		
🕘 💋 http://secu	relogin.arubanetworks.com/cgi-bir/login	・ ○ × □ × ○ 正在等待 securelogin.aru_ ×	
hentication	successful		
0 seconds yo	ou will be automatically redirected to	http://www.arubanetworks.com.	
k <u>here</u> to go t	there directly.		
k <u>here</u> to boo	okmark this page.		
k <u>here</u> to boo	okmark this page.		
k <u>here t</u> o boo ^{sut}	okmark this page.		
k <u>here</u> to boo	kmark this page.		

7.5.2 CPPM 上查看认证记录



A							_
aruba			Clea	arPass Policy Manag	er		Menu
	监视 »	Live Monitoring » 访问	同眼踪器				
💼 监视 📀	访问	跟踪器 Oct 11, 201	9 20:59:05 CST				📀 自动刷新
Live Monitoring	The Ac	cess Tracker page pr	ovides a real-time display of per-se	ession access activity on the selecte	d server or domain.		
	T (All Requests]	Lab2-CPPM-1	Lab2-CPPM-1 (10.2.50.41)		ore Today	強領
	过速器:	Request ID	• 句含 •	Go Clear Filter			显示 100 ▼ 记录
Profile and Network Scan		Server	Source	Username	Service	Login Status	Request Timestamp *
	1.	10.2.50.41	RADIUS	zhengxin.yang@hpe.co	tasko-guest-register-auth- service	ACCEPT	2019/10/11 20:58:46
	2.	10.2.50.41	RADIUS	zhengxin.yang@hpe.co	task6-guest-register-auth- service	ACCEPT	2019/10/11 20:47:23
	3.	10.2.50.41	Application	admin	[Guest Operator Logins]	ACCEPT	2019/10/11 17:15:36
	4.	10.2.50.41	Application	admin	[Guest Operator Logins]	ACCEPT	2019/10/11 16:45:32
	显示最优	后项的前一-后一					
e a a a a a a a a a a a a a a a a a a a							
2 管理 0	4						•
© 版权所有 2015 Aruba Networks。保留所有权	利。		Oct 11, 2019	20:59:07 CST		ClearPa	ass 策略管理器 6.7.9.109195 开启 CLABV 平台

✓ 点击认证成功记录,在"概要"选项卡中观察,看看能看到哪些信息。

请求详细信息		8					
概要 输入 输出 计	费						
登录状态:	ACCEPT	-					
会话标识符:	R0000001-01-5da07c86						
日期和时间:	Oct 11, 2019 20:58:46 CST						
终端主机标识符:	7C7A914652B7 (Computer / Windows / Windows)						
用户名:	zhengxin.yang@hpe.com						
访问设备 IP/端口:	10.1.10.21:0						
系统安全状况状态:	JNKNOWN (100)						
	所用策略 -						
服务:	task6-guest-register-auth-service						
认证方法:	PAP						
认证源:	Local:localhost						
授权源:	[Guest User Repository]						
角色:	[Guest], [User Authenticated]						
强制执行配置文件:	task6-guest-register-profile						
服务监视模式:	Disabled	-					
I ◄ Showing 1 of 1-4 recor	rds ► ► 更改状态 Show Configuration 导出 显示日志 关闭						



✓ 点击"输入"选项卡中观察,看看能看到哪些信息。

请求详细信息	8
概要 输入 输出 计费	
用户名: zhengxin.yang	@hpe.com
终端主机标识符: 7C7A914652B	7 (Computer / Windows / Windows)
访问设备 IP/端口: 10.1.10.21:0	
RADIUS 请求	\odot
Radius: Aruba: Aruba-AP-Group	lah1-group
Radius:Aruba:Aruba-Device-Type	Win 8
Radius:Aruba:Aruba-Essid-Name	lab1-guest-register
Radius:Aruba:Aruba-Location-Id	94:b4:0f:c1:3f:e0
Radius:IETF:Called-Station-Id	000B869AAF37
Radius:IETF:Calling-Station-Id	7C7A914652B7
Radius:IETF:Framed-IP-Address	10.1.20.102
Radius:IETF:NAS-IP-Address	10.1.10.21
Radius:IETF:NAS-Port	0
Radius:IETF:NAS-Port-Type	19
Radius:IETF:Service-Type	1
I ◄ Showing 1 of 1-4 records ► ►	更改状态 Show Configuration 导出 显示日志 关闭

✓ 点击"输出"选项卡中观察,看看能看到哪些信息。

请求详细信息		8
概要 输入 输出	计费	
强制执行配置文件:	task6-guest-register-profile	
系统安全状况状态:	UNKNOWN (100)	
审计安全状况状态:	UNKNOWN (100)	
RADIUS 响应		
Radius:Aruba:Aruba	-User-Role guest-register-role	
I ≤ Showing 1 of 1-4	records▶▶↓ 更改状态 Show Configuration 导出 显示日志	关闭



✓ 点击"计费"选项卡中观察,看看能看到哪些信息。

请求详细信息		8
概要 输入	、 輸出 計費	
客户会话 ID:	zhengxin7C7A914652B7-5DA0EBB2-D11CD	
开始时间戳:	Oct 11, 2019 20:58:47 CST	
结束时间戳:	Still Active	
状态:	Active	
终止原因:	-	
服务类型:	-	
认证会话数:	1	
网络详细信息		۲
利用		٩
认证会话详细	信息	•

I ◄ Showing 1 of 1-4 records ► ►I	更改状态	Show Configuration	导出	显示日志	关闭
------------------------------------	------	--------------------	----	------	----

7.5.3 控制器上查看认证记录

(lab1-mm-1)	[mynode] #show glob	al-user-table list											
Global Users													
IP 10.1.20.102 10.1.20.103	MAC 7c:7a:91:46:52:b7 7c:7a:91:46:23:6e	Name zhengxin.yang@hpe.com	Current switch 10.1.10.11 10.1.10.11	Role guest-register-role lab1-portal-guest-logon	Auth	AP name 94:b4:0f:c1:3f:e0 94:b4:0f:c1:3f:e0	Roaming Wireless Wireless	Essid lab1-guest-register lab1-portal	Bssid 94:b4:0f:93:fe:12 94:b4:0f:93:fe:11	Phy a-VHT a-VHT	Profile lab1-guest-register_aaa_prof lab1-portal_aaa_prof	Type Win 8 Win 8	USER Type WIRELESS WIRELESS
Total entrie (lab1-mm-1)	s = 2 [mynode] #												



8 TASK7: ARUBA 控制器集成 CPPM 实现 TACACS+认证

8.1 用户需求

用户希望针对aruba的所有无线设备提供管理员账号的集中认证和授权管理,保障了管理员账号的安全,同时也 控制了不同身份的账号具有不同的设备管理权限等。

8.2 实现思路

✓ 首先我们需要思考下,在当前的管理员集中认证机制中,哪一种是最常用的认证方式?

答案:

✓ 针对该认证方式,我们需要思考下还需要为无线网络新增什么网元,即需要针对无线网络来设计什么样的认证服务器呢?

答案:

✓ 针对TACACS认证的用户,我们设计两种类型的用户,例如根管理员和只读管理员,利用TACACS的授权功能,返回什么样属性给到控制器,从而实现不同的管理员访问权限?

答案: _____

8.3 ClearPass 配置

8.3.1 添加 NAS Client

参考第二章节中的网络设备配置,其中MM控制器需要设置 TACACS共享密钥。

8.3.2 添加本地账号和角色

第1步:找到配置 -> 身份 -> 角色,点击右上角的"添加角色"按钮,增加两个角色:

aruba	ClearPass Policy Manager Menu				Menu 🗮	
■ ■ 面板 の 気 監想	配置 > 身份 > 角色				🚽 添加角色	
	用巴 <u>・</u> ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・				👱 导入角色 🚖 导出角色	
	Roles e	Roles exist independently of an individual service and can be accessed globally through the role-mapping policy of any service.				
● → 以业 ● 身份	过滤器: #	名称	 ◆ 〔包含 ◆ 〕 名称 ▼ 	+	Go Clear Filter 说明	显示 1000 🛊 记录
	1.		[TACACS Super Admin]		Super administrator role for Policy Manager Admin	
- 🗘 端点	2.		[TACACS Receptionist]		Receptionist role for Policy Manager Admin	
静态主机列表	3.		[TACACS Read-only Admin]		Read-only administrator role for Policy Manager Admin	
	4.		[TACACS Network Admin]		Network administrator role for Policy Manager Admin	
	5.		[TACACS Help Desk]		Help desk role for Policy Manager Admin	
	6.		[TACACS API Admin]		API administrator role for Policy Manager Admin	
→ → 网络	7.		[Other]		Default role for another user or device	
Profile and Network Scan	8.		[Onboard Windows]		Role for a Windows device being provisioned	
一心 策略仿真	9.		[Onboard Mac OS X]		Role for a Mac OS X device being provisioned	

在添加新角色1的窗口中,输入下面的参数:

- ✓ 名称: aruba-tacacs-read-only-admin
- ✓ 说明: 赋予只读管理员权限

编辑角色		8
名称:	aruba-tacacs-read-only-admin	
说明:	赋予只读管理员权限 //	
	Save Cancel	

在添加新角色2的窗口中, 输入下面的参数:

- ✓ 名称: aruba-tacacs-root-admin
- ✓ 说明: 赋予根管理员权限

编辑角色		8
名称:	aruba-tacacs-root-admin	
说明:	赋予根管理员权限	
	Save	el

第2步: 找到 配置 - > 身份 - >本地用户,点击右上角的"添加用户"按钮,增加两个用户账号:

aruba	CI	earPass Policy Manager		Menu 🗮
■■ 面板 0	配置 » 身份 » 本地用户			
□ 監視 0 ○ 配置 ○ ○ 此处开始 ○ 用条	本地用户 ClearPage Policy Manager lists all local users in the Lo	ral lifeers page		 → 添加用户 ▲ 导入用户 ▲ 导出用户 ☆ Account Settings
→最 地理	ClearPass Foncy manager lists an local users in the Lo	car osers page.		
 ● ● 身份 - ② Single Sign-On (SSO) - ③ 添加用户 - ○ 端底点 - ③ 静态主机列表 - ○ 角色 - ○ 角色 - ○ 角色 	过滤器:〔用户ID	★ Go Clear Filter 名称	角色	显示〔20 €) 记录 犹然 号出〕 劉陰〕

在添加账号1的窗口中, 输入下面的参数:

✓ 用户ID: aruba-read-admin (即用户的登录账号)

- ✓ 名称: aruba-read-admin-test (即该账号的别名,只是一个标签)
- ✓ 密码: aruba123 (该账号的登录密码)
- ✓ 认证密码: aruba123 (即重复输入一次登录密码)
- ✓ 启用用户: enable (勾选)
- ✓ 角色: aruba-tacacs-read-only-admin (该角色是在第一步中创建的)

编辑本地用户		8			
用户 ID:	aruba-read-admin				
名称:	aruba-read-admin-test				
密码:					
认证密码:					
启用用户:	☑ (选中可启用本地用户)				
更改密码:	\square (Check to force change password on next TACACS+ login)				
角色:	aruba-tacacs-read-only-admin 🔹				
属性					
属性	值				
1. Click to add					



在添加账号2的窗口中, 输入下面的参数:

- ✓ 用户ID: aruba-root-admin (即用户的登录账号)
- ✓ 名称: aruba-root-admin-test (即该账号的别名,只是一个标签)
- ✓ 密码: aruba123 (该账号的登录密码)
- ✓ 认证密码: aruba123 (即重复输入一次登录密码)
- ✓ 启用用户: enable (勾选)
- ✓ 角色: aruba-tacacs-root-admin (该角色是在第一步中创建的)



编辑本地用户		8
用户 ID:	aruba-root-admin	
名称:	aruba-root-admin	
密码:		
认证密码:	•••••	
启用用户:	✓ (选中可启用本地用户)	
更改密码:	$\hfill\square$ (Check to force change password on next TACACS+ login)	
角色:	aruba-tacacs-root-admin •	
	属性	
属性	值	
1. Click to add		
		_
	保存取消	

配置总览:

aruba			ClearPass Policy Manager		Menu 🚍				
■ ■ 面板 ●	配置 ≥ 身份 ≥ 本地用户								
🕑 监视 🔹 💿	本地用	本地用户							
· 配置 · · · · · · · · · · · · · · · · · ·									
一章 此处开始		S Acount Settings							
一口 服务	ClearPas	ClearPass Policy Manager lists all local users in the Local Users page.							
🖃 🗣 认证									
一口 方法	过滤器:月	用户ID ▼ 包含▼	Go Clear Filter		显示 1000 ▼ 记录				
—————————————————————————————————————	#	∎ щето.		角色	<u>**</u>				
→ 量 対加 A Single Sign On (SSO)	1.	aruba-read-admin	aruba-read-admin	aruba-tacacs-read-only-admin	Enabled				
- A single sign-on (330)	2.	aruba-root-admin	aruba-root-admin	aruba-tacacs-root-admin	Enabled				
- 4 端点	3.	employee	employee-test	employee-role	Enabled				
静态主机列表	4.	guest	guest-test	guest-role	Enabled				
	5.	🔍 jma	jma	employee-role	Enabled				
一口 角色映射	6.	🔲 jma1	jma1	guest-role	Enabled				
→ 〒 安全状況	7.	lab1-test	lab1测试账号	[Other]	Enabled				
- 警 独耐执行 - 答 鉴 除	8.	leader	leader	leader-role	Enabled				
	显示最后耳	项的前一-后一			《創账 出 出 記				
□ + 网络									
— 🛟 设备组									
- C Event Sources									
Profile and Network Scan A 勞敗佐吉									
一編集中的四個									

8.3.3 添加认证服务

第1步: 找到 配置 - > 强制执行 - > 配置文件,点击右上角的"添加强制执行配置文件"按钮,增加两个强制执行配置文件:
aruba		ClearPass Policy Manager							
● 画版 ■ 監視 ● 配置 ● 配置 ● の記念を	● 配重 » 引 ● 强制拼 ● Each en	制执行 1行面	>> 配置文件 置文件 ent policy contains enforcement profiles that match condi- tion and the profiles and the pr	ions (role, posture, an	d time) to actions (enforcement profiles).	 → 添加强制执行配置文件 ▲ 导入强制执行配置文件 ▲ 导出强制执行配置文件 			
→ 4 (A) → 4 (A) → 2 身份 → 年本全球2	过滤器: (#	名称	 ◆ 包含 ◆ 	Go Clear Filter 类型	说明	显示 100 🛟 记录			
● 文 Secolo ● 教師版行 ● 和言文件 ● 一種文件 ● 一種文件 ● 一種文件	1. 2. 3. 4. 5.		[Aerohive - Terminate Session] [AirGroup Personal Device] [AirGroup Response] [AirGroup Shared Device] [Ailow Access Profile]	RADIUS_CoA RADIUS RADIUS RADIUS RADIUS	System-defined profile to disconnect user (Aerohive) System-defined profile for an AlrGroup personal device request System-defined profile for an AlrGroup shared device request System-defined profile for allow network access				
一發東始加具	6.		[Allow Application Access Profile]	Application	System-defined profile to allow access to application				

在配置文件(第一个)选项卡中,输入下面的参数:

✓ 模板:基于TACACS+的强制执行

✓ 名称: task7-aruba-controller-tacacs-readonly-access

在服务选项卡中, 输入下面的参数:

- ✓ 权限级别: 15(Privileged)
- ✓ 所选服务: Aruba:Common
- ✓ Authorize Attribute Status: ADD
- ✓ Aruba:Common Aruba-Admin-Role = read-only



配置 » 强制执行 » 配置文件 »	Add Enforcement Profile				
强制执行配置文件					
配置文件 服务 概要					
权限级别:	15 (Privileged)				
所选服务:	Aruba:Common				导出 TACACS+ 服务字典
		Remove			
	Select				
Authorize Attribute Statues					
Authorize Attribute Status:	ADD				
定制服务:	要添加新 TACACS+ 服务/属性,请上传修	改的字典 xml - Update TACACS+ Services Dictionary			
		服务属性			
类型		名称		值	
1. Aruba:Common		Aruba-Admin-Role	=	read-only	
2. Click to add					

在配置文件(第二个)选项卡中,输入下面的参数:

- ✓ 模板:基于TACACS+的强制执行
- ✓ 名称: task7-aruba-controller-tacacs-root-access

配置 » 强制执行 » 配置文件 »	Add Enforcement Profile
强制执行配置文件	
配置文件 服务 概要	
模板:	基于 TACACS+ 的强制执行 ▼
名称:	task7-aruba-controller-tacacs-root-access
说明:	
类型:	TACACS
操作:	● 接受 ● 拒绝 ● 删除
设备组列表:	Remove View Details Modify

在服务选项卡中, 输入下面的参数:

- ✓ 权限级别: 15(Privileged)
- ✓ 所选服务: Aruba:Common
- ✓ Authorize Attribute Status: ADD
- ✓ Aruba:Common Aruba-Admin-Role = root



配置 » 强制执行 » 配置文件 »	Add Enforcement Profile				
强制执行配置文件					
配置文件 服务 概要					
权限级别:	15 (Privileged)				
所选服务:	Aruba:Common				导出 TACACS+ 服务字典
		Remove			
	Select				
Authorize Attribute Status:					
定制服务:	要添加新 TACACS+ 服务/属性,请上传	修改的字典 xml - Update TACACS+ Services Dict	tionary		
		服务属性			
类型		名称	=	值	
1. Aruba:Common		Aruba-Admin-Role	=	root	Ba 6
2. Click to add					

第2步: 找到 配置 - > 强制执行 - > 策略 , 点击右上角的"添加强制执行策略"按钮 , 增加一个强制执行策略:

aruba			Menu				
E ■ 面板 0	配置 »	强制执行	» 策略				
🕑 监视 🛛 🛛 🛛	强制	丸行策	略				🚽 添加强制执行策略
🭰 R 🖩 💿							会 导入强制执行策略
一章 此处开始	ClearPa	ass cont	rols network access by evaluating an enfor	cement policy as	sociated with the ser	vice.	
🕞 🗣 认证	\\ → 連縄・	夕段	1 旬令 1	+	Go Clear Filter		显示 1000 🗧 记录
	A2.86101	-14100	(BE V)		446.001	N nD	
🖅 📅 安全状况	#		名称▲		突型	说明	
□ 晝 强制执行	1.		[Admin Network Login Policy]		TACACS	Enforcement policy controlling access to Policy Manager Admin	
一尊 策略	2.		[AirGroup Enforcement Policy]		RADIUS	Enforcement policy controlling access for AirGroup devices	
一章 配置文件	3.		[Aruba Device Access Policy]		TACACS	Enforcement policy controlling access to Aruba device	
→ ● 网络	4.		[Guest Operator Logins]		Application	Enforcement policy controlling access to Guest application	
M Profile and Network Scan A 等略化声	5.		[Insight Operator Logins]		Application	Enforcement policy controlling access to Insight application	
一分束的四具	6.	0	[Sample Allow Access Policy]		RADIUS	Sample policy to allow network access	
	7.		[Sample Deny Access Policy]		RADIUS	Sample policy to deny network access	
	显示最原	5项的前-	后一				复制 导出 删除

在强制执行选项卡中, 输入下面的参数:

- ✓ 名称: task7-aruba-device-access-enforcement-policy
- ✓ 强制执行类型: TACACS
- ✓ 默认配置文件: [ArubaOS Wireless TACACS Read-Only Access]

配置 » 强制执行 » 策略 » 添加	n de la constante de	
强制执行策略		
强制执行规则概要		
名称:	task7-aruba-device-access-enforcement-policy	
说明:		
强制执行类型:	◎ RADIUS ● TACACS+ ◎ WEBAUTH (SNMP/Agent/CLI/CoA) ◎ 应用程序 ◎ Event	
默认配置文件:	[ArubaOS Wireless - TACACS View Details Modify	添加新强制执行配置文件

在规则选项卡中, 输入下面的参数:

✓ 规则: 点击 "Add Rule",配置如下:

添加第一个规则



- ✓ 条件是: Tips Role MATCHES_ALL aruba-tacacs-read-only-admin, [User Authenticated]
- ✓ 配置文件名: task7-aruba-controller-tacacs-readonly-access

配置》强制执行》策略》添加	1			
迟到场 <i>行华</i> 政	4			
姐前执行東略				
强制执行 规则 概要				
规则评估算法:	● 选择第一个匹配 ◎ 选择所有匹配			
Enforcement Policy Rules:				
Conditions		Actions	7	
		Add Rule	Move Up ↑ Move Down ↓ Edit Rule	Remove Rule
			-	
规编辑器				6
		条件		
匹配以下所有条件:				
类型	名称	运算符	值	
1. Tips	Role	MATCHES_ALL	aruba-tacacs-read-only-admin	Pa T
2 Click to add			[User Authenticated]	
2. Click to aud				
		强制执行配置文件		
配置文件名:	task7-aruba-controller-tacacs-readonly-access			
		Move Up ↑		
		Move Down ↓		
		Remove		
	Select to Add	T		
				de me sik

再添加第二个规则

- ✓ 条件是: Tips Role MATCHES_ALL aruba-tacacs-root-admin, [User Authenticated]
- ✓ 配置文件名: task7-aruba-controller-tacacs-root-access



规则的	補器				6
			条件		
匹配	以下所有条件:				
	类型	名称	运算符	值	
1.	Tips	Role	MATCHES_ALL	aruba-tacacs-root-admin [User Authenticated]	Pa t
2.	Click to add				
			强制执行配置文件		
配置	文件名:	task7-aruba-controller-tacacs-root-access	Move Lip 1		
			Move Op		
			Remove		
			Tremove		
		Select to Add	T		

在概要选项卡中,对整体配置进行总览:

配置 » 强制执行 » 策略 » 添加						
强制执行策略						
强制执行规则权要						
强制执行:						
名称:	task7-aruba-device-access-enforcement-policy					
说明:						
强制执行类型:	TACACS					
默认配置文件:	[ArubaOS Wireless - TACACS Read-Only Access]					
规则:						
规则评估算法:	First applicable					
Conditions		Actions				
1. [Tips:Role MATCHES_ALL aruba-tacacs-read-only-admin task7-aruba-controller-tacacs-readonly-access [User Authenticated]) task7-aruba-controller-tacacs-readonly-access						
2. [User Authenticated])	ALL aruba-tacacs-root-admin	task7-aruba-controller-tacacs-root-access				

第3步:找到配置 - > 服务,点击右上角的"添加服务"按钮,增加一个服务:

aruba				Menu					
■ 面板 0	配置»,	服务							
₩ 监视 0	服务							🚽 添加服务	
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2								 二 守八服労 全 导出服务 	
	This pa	This page shows the current list and order of services that ClearPass follows during authentication and authorization.							
■☆ 服务									
🗉 🗣 认证	过滤器:	名称		▼ 包含 ▼	+ Go	Clear Filter		显示 1000 ▼ 记录	
	#		顺序 ▲	名称		类型	模板	状态	
➡ ① 女主状况	1.		1	[Policy Manager Admin Network Login Service	æ]	TACACS	TACACS+ Enforcement	0	
「「「「「「「「「「」」」の「「「」」」の「「「」」」の「「「」」」の「「「」」」の「「」」の「「」」の「「」」の「「」」の「」」。」。	2.		2	[AirGroup Authorization Service]		RADIUS	RADIUS Enforcement (Generic)	0	
□ 配置文件	3.		3	[Aruba Device Access Service]		TACACS	TACACS+ Enforcement	0	
글 ┿ 网络	4.		4	[Guest Operator Logins]		Application	Aruba Application Authentication	0	
💀 💀 Profile and Network Scan	5.		5	[Insight Operator Logins]		Application	Aruba Application Authentication	0	
一〇 策略仿真	6.		7	lab1-mac-user-defined		RADIUS	忽略 MAC 认证	Ø	
	7.		8	lab1-mac Device MAC Authentication		RADIUS	忽略 MAC 认证	Ø	
	8.		9	aaa test		RADIUS	RADIUS Enforcement (Generic)	0	
	9.		10	lab1-portal-user-defined		RADIUS	RADIUS Enforcement (Generic)	0	
	显示最周	后项的育	前一-后一				重新排序	复制 导出 删除	

a Hewlett Packard Enterprise company

在服务选项卡中, 输入下面的参数:

- ✓ 类型: TACACS+ Enforcement
- ✓ 名称: task7-aruba-device-access-enforcement-policy
- ✓ 匹配项:以下所有条件
- ✓ 服务规则:
 - 1、Connection Protocol EQUALS TACACS
 - 2、Connection NAD-IP-Address EQUALS 10.X.50.11 (X:1……6即 MM的IP地址)

配置	» 服务 » 添加											
服务	<u>हे</u> क्र											
服务	5 认证 角色 强	制执行 概要										
类型: TACACS+ Enforcement T												
名称:		aruba-device-access-enforcement-policy										
说明:												
监视相	莫式:	■ 启用以监视无强制执行的网络访问										
更多i	先项:	□ 授权										
			服务规则									
匹配功	🖲 🗍 任意或 🖲 以下所	有条件:										
	类型	名称	运算符	值								
1.	Connection	Protocol	EQUALS	TACACS	Eg ú							
2.	Connection	NAD-IP-Address	EQUALS	10.1.50.11	Ba ti							
3.	Click to add											

在认证选项卡中, 输入下面的参数:

✓ 认证源: [Local User Repository][Local SQL DB]

配置 » 服务 » 添加			
服务			
服务认证角色强	制执行 概要	_	
认证源:	[Local User Repository] [Local SQL DB]	Move Up ↑ Move Down ↓ Remove View Details Modify	汤》加新认证 源
	Select to Add	•	
剥离用户名规则:	□ 启用以指定以逗号分隔的规则列表,用于剥离	阉用户名前缀或后缀	

在角色选项卡中,暂时不做任何配置(详细内容可以参考高级介绍部分)

✓ 角色映射策略:空

配置 » 服务 » 添加		
服务		
服务认证角色 强	制約行 板要	
角色映射策略:	─_Select Modify 添加新角色®	A 射策略
	角色映射策略详细信息	
说明:	-	
默认角色:	-	
规则评估算法:	-	
条件	角色	

a Hewlett Packard Enterprise company

在强制执行选项卡中, 输入下面的参数:

 ✓ 强制执行策略: task7-aruba-device-access-enforcement-policy (即第2步中创建的强制执行策 略)

配置 »	服务 » 添	加		
服务				
服务	认证	角色	强制执行 概要	
使用缓	存的结果:		■ 使用从上一会话中缓存的角色和安全状况属性	
强制执行	亍策略:		task7-aruba-device-access-enforcement-policy V Modify	添加新强制执行策略
			强制执行策略详细信息	
说明:				
默认配.	置文件:		[ArubaOS Wireless - TACACS Read-Only Access]	
规则评	估算法:		first-applicable	
	条件		强制执行配置文件	
1.	(Tips:F	Role MA	IATCHES_ALL aruba-tacacs-read-only-admin task7-aruba-controller-tacacs-readonly-access	
2.	(Tips:F	Role MA	ATCHES_ALL aruba-tacacs-root-admin task7-aruba-controller-tacacs-root-access cated])	

在概要选项卡中,对配置进行总览:

强制执行策略: task7-aruba-device-access-enforcement-policy

配置 »	置 > 服务 > 添加							
服务	r							
服务	认证	角色	强制执行 概要					
服务:								
类型:			TACACS+ Enforcement					
名称:			aruba-device-access-enford	ement-policy				
说明:								
监视横	! ग्र :		Disabled					
更多选	项:		-					
					服务规则			
匹配以	下所有条件	÷:						
	类型			名称	运算符	值		
1.	Connect	tion		Protocol	EQUALS	TACACS		
2.	Connect	tion		NAD-IP-Address	EQUALS	10.1.50.11		
认证:								
认证源	i:		[Local User Repository] [Lo	cal SQL DB]				
剥离用]户名规则:		-					
角色:								
角色映	射策略:		-					
强制执	(行:							
使用缓	存的结果:		Disabled					

第4步: 找到 配置 - > 服务 , 将刚才创建的认证服务调整优先级:

ClearPass系统安装好后,默认就会在服务中添加了一个 Aruba Device Access Service 服务,该服务的匹配规则 是空的,也即是任何aruba的tacacs请求服务都会优先击中这条 service (从上至下的优先匹配原则)。

我们可以把之前新建的task7-aruba-device-access-enforcement-policy顺序调整到Aruba Device Access Service之前,

aruba	a		ClearPass Polic	y Manager		Menu 💻
■■ 面板		 ● 配置 » 服务 				
😥 监视		 服务 				
🖧 配置		•				□ 3/100/2 ▲ 导出服务
	ń	This page shows the curre	nt list and order of services that ClearPass follows d	uring authentication and auth	norization.	
————————————————————————————————————						
-07	万法	过滤器:名称		Go Clear Filter	111 Jun	±7 1000 ▼ 1C×
-Q 3	<u>ą</u>	# ■ 顺序 ▲	古桜 [Deling Managers Admin Natural: Login Convice]	突型	役似 TACACE: Enforcement	π
	in alla Gina (250)		[Policy Manager Admin Network Login Service]	RADIUS	RADIUS Enforcement (Ge	peric)
-0.4	single sign-on (SSO) s地用户	3. 3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	
-0.9	憲法	4. 4	[Guest Operator Logins]	Application	Aruba Application Authent	Ication
一段前	静态主机列表	5. 5	[Insight Operator Logins]	Application	Aruba Application Authent	ication 🥑
-Q: #	自色 6.6.1.1.1	6. 🗖 6	task1-test-service	RADIUS	RADIUS Enforcement (Ge	neric)
⊡ 🕆 安全状》	R	7. 7	task2-mac-service	RADIUS	忽略 MAC 认证	0
🖃 🤹 强制执行	Ŧ	8. 8	task3-portal-service	RADIUS	RADIUS Enforcement (Ge	neric) 📀
-Q 8	() 開始	9. 9	task4-802.1x-auth-service	RADIUS	Aruba 802.1X Wireless	0
一口目	化面叉件	10. 10	task5-mac-caching-service	RADIUS	RADIUS Enforcement (Ge	neric)
_Q 8	2番		task7-mac-service	TACACS	TACACS+ Enforcement	
- 🗘 i	设备组		task/-aruba-device-access-eniorcement-policy	TACACO	TACACOT Enforcement	无知此在 有相 日中 副除
-Q f	代理目标	亚小眼眉类时间一周				王初孙//
127 E	vent Sources					
orubo	2		ClearPass Polic	v Manager		Menu 💻
三		 配置 » 服务 » 重新排序 		, ,		
「「「「「「」」「「」」		 B&重新排序 				
2 配置		○ 要重新排席服务, 请在洗择行	之后傅田"上移"和"下移"按钮·			
	÷					
一〇 服务		東戶 名称	min Natwork Login Sanvical	服务详细信息:		
🖃 🖴 认证		2 [AirGroup Authoriz:	ation Service]	名称:	[Policy Manager Admin Network Login	Service]
- Q 7	5法 =	3 [Aruba Device Acce	ss Service]	候版:	TACACS+ Enforcement	
	7	4 [Guest Operator Lo	gins]	央型: 说明:	Service for access to Policy Manager A	dmin for network users
- 🛱 S	iingle Sign-On (SSO)	5 [Insight Operator L	ogins]	状态:	Disabled	
Q 4	*地用户	6 task1-test-service			服务规则	
- 2 3	≝点 ▲本主和 別表	7 task2-mac-service		((Connection:NAD-IP-A	Address EQUALS 127.0.0.1))	
- 2 角	A L 10/2020 角色	8 task3-portal-servic	e	AND (Connection:Protoc	col EQUALS TACACS)	
	角色映射	9 task4-802.1x-auth	service			
→ 🕆 安全状》	R -	10 task5-mac-caching	service			
□- 28 独司执1 → 23 分	丁 新路	12 task7-aruba-device	-access-enforcement-policy			
-Q 8	2.置文件		access enforcement poncy	1		
•						
过滤器: 4	当称	▼ 包含 ▼	🛨 🛛 Go 🔹 Clear Filter			显示 1000 ▼ 记录
#	■ 顺序 ▲	名称	类型	模板		状态
1.	1	[Policy Manager Admin Network	Login Service] TACACS	TACA	ACS+ Enforcement	0
2.	2	[AirGroup Authorization Service]	RADIUS	RAD	IUS Enforcement (Generic)	O
3.	3	task7-aruba-device-access-enfor	cement-policy TACACS	TACA	ACS+ Enforcement	O
4.	4	[Aruba Device Access Service]	TACACS	TACA	ACS+ Enforcement	O
5.	5	[Guest Operator Logins]	Application	Arub	a Application Authentication	S
6.	6	[Insight Operator Logins]	Application	Arub	a Application Authentication	O
7.	7	task1-test-service	RADIUS	RADI	IUS Enforcement (Generic)	0
8.	8	task2-mac-service	RADIUS	忽略	MAC 认证	O
9.	9	task3-portal-service	RADIUS	RADI	IUS Enforcement (Generic)	O
10.	10	task4-802.1x-auth-service	RADIUS	Arub	a 802.1X Wireless	O
11.	11	task5-mac-caching-service	RADIUS	RADI	IUS Enforcement (Generic)	O
12.	12	task5-mac-service	RADIUS	RADI	IUS Enforcement (Generic)	O
显示最后耳	顷的前一-后一					重新排序 复制 导出 删除



或者将已有的Aruba Device Access Service 给关闭掉。点击下状态按钮√,就会变成停止按钮,表示该service被关闭 掉了。

111%器: 1	当和小			ritter		MEAN TOOD + NEWS
#		顺序 ▲	名称	类型	模板	状态
1.		1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	0
2.		2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	\bigcirc
3.		3	task7-aruba-device-access-enforcement-policy	TACACS	TACACS+ Enforcement	0
4.		4	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	0
5.		5	[Guest Operator Logins]	Application	Aruba Application Authentication	0
6.		6	[Insight Operator Logins]	Application	Aruba Application Authentication	
7.		7	task1-test-service	RADIUS	RADIUS Enforcement (Generic)	0
8.		8	task2-mac-service	RADIUS	忽略 MAC 认证	S
9.		9	task3-portal-service	RADIUS	RADIUS Enforcement (Generic)	
10.		10	task4-802.1x-auth-service	RADIUS	Aruba 802.1X Wireless	
11.		11	task5-mac-caching-service	RADIUS	RADIUS Enforcement (Generic)	
12.		12	task5-mac-service	RADIUS	RADIUS Enforcement (Generic)	S
显示最后	页的前一	后一			重新排序	导出删除

过滤器:	名称		▼ 包含 ▼ Go Clear	Filter		显示 1000 ▼ 记录
#		顺序 ▲	名称	类型	模板	状态
1.		1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	0
2.		2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	
3.		3	task7-aruba-device-access-enforcement-policy	TACACS	TACACS+ Enforcement	
4.		4	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	0
5.		5	[Guest Operator Logins]	Application	Aruba Application Authentication	I
6.		6	[Insight Operator Logins]	Application	Aruba Application Authentication	 Image: A start of the start of
7.		7	task1-test-service	RADIUS	RADIUS Enforcement (Generic)	0
8.		8	task2-mac-service	RADIUS	忽略 MAC 认证	\bigcirc
9.		9	task3-portal-service	RADIUS	RADIUS Enforcement (Generic)	
10.		10	task4-802.1x-auth-service	RADIUS	Aruba 802.1X Wireless	
11.		11	task5-mac-caching-service	RADIUS	RADIUS Enforcement (Generic)	I
12.		12	task5-mac-service	RADIUS	RADIUS Enforcement (Generic)	
显示最后	项的前-	后一			重新排序	日 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一



8.4 控制器配置

8.4.1 添加 TACACS 服务器和服务器组

第1步: 使用 Web 方式登录到 Mobility Master (10.X.50.11) (X:1…6), 找到 Mobility Master ->

Configuration -> Authentication -> Auth Servers 点击 All Servers 下的 "+" 进入创建一个新的认证 服务器。

ALIAN MOBILITY MAST	ER		CONTROLLERS ACCESS ⊙ 2 ○ 0 ⊙ 1	POINTS CLIENTS ⊙ 0 중 1 ₱ 0	ALERTS		(?) admin ~
🔶 Mobility Master >							Ŷ
€ , q	Configuration	Auth Servers Ad	vanced				
🔁 Mobility Master	Roles & Policies						
📼 lab1-mm-1	Authentication	Server Groups 2					
Managed Network (2)	Services	NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES	=
🔁 lab1 (2)	Interfaces	default	1	-	-	1	
📼 lab1-md1	Controllers	internal	1		-	1	
📼 lab1-md2	System						
	License	+					
		All Servers 1					
		NAME	TYPE	IP ADDRESS	/ HOSTNAME SER	RVER GROUP	=
		Internal	-	-	def	fault internal	
		+					

在 New Server 窗口中设置:

- ✓ Name(ssid): cppm-tacacs-server
- ✓ IP address/hostname: 10.X.50.41 (X:1…6,每组CPPM的各自管理IP地址)
- ✓ Type: TACACS
- ✓ Submit: 点击提交配置

New Server	
Name:	cppm-tacacs-server
IP address:	10.1.50.41
Туре:	TACACS 💙
	Cancel Submit

点击刚才创建好的auth server: cppm-tacacs-server, 进入到认证服务器的编辑窗口,

- ✓ 1、Key和Retype Key: aruba123
- ✓ 2、Session authorization: 勾选
- ✓ 2、Submit: 点击提交配置



All Servers 2				
NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP	
cppm-tacacs-server	TACACS	10.1.50.41	cppm-tacacs-sg	
Internal			default internal	
+				
Server Options				
Host:	10.1.50.41			
Key:	••••••			
Retype key:				
TCP port:	49			
Petransmits	2			
Reconstruct.	5			
Timeout:	20			
Mode:				
Session authorization	n: 🗹			

第2步: 点击 Server Groups 下的 "+"进入创建一个新的认证服务器组。

ALITY MASTE Iab1-mm-1	R		CONTROLLERS ACCESS POI ∅ 2 0 ∅ 1 0	NTS CLIENTS 0 ? 1 ₽ 0	ALERTS 0		admin ~
🔶 Mobility Master >							Pending Changes 🗘
€ <mark>k</mark> Q	Configuration	Auth Servers	lvanced				
🔁 Mobility Master	Roles & Policies						
🖾 lab1-mm-1	Authentication	Server Groups 2					
Managed Network (2)	Services	NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES	=
🔁 lab1 (2)	Interfaces	default	1	-	-	1	
📼 lab1-md1	Controllers	internal	1	-	-	1	
lab1-md2	System						
	License	+					
		All Servers 2					
		NAME	TYPE	IP ADDRES	S / HOSTNAME	SERVER GROUP	=
		cppm-tacacs-server	TACACS	10.1.50.41		-	
		Internal	-	-		default internal	
		+					
	Andrew 8400						

在 Add Server Group 窗口中设置:

- ✓ Name(ssid): cppm-tacacs-sg
- ✓ Submit: 点击提交配置



Add Server (Froup		
Name:	cppm-tacacs-sg		
		Cancel	Submit

在 Server Groups 下点击 cppm-tacacs-sg, 在 Servers 选项卡窗口下半部分,出现 server group 的编辑界 面。点击下面的"+"进入到认证服务器组编辑窗口。

Mobility Master > wobility Master alabimm-1 whanged Network (2) labi-md1 labi-md2	Configuration Roles & Policies Authentication Services Controllers System License 经期的编辑窗 Add existin Submit: 点言	Auth Servers Advanced Server Groups 3 Navit Genetic Commentacing F Transf Tran	serves 1 ● Setg Servers Options TYPE □ 口 つ つ つ つ つ つ の つ の つ の つ の つ の つ の の の の の の の の の の の の の	FAIL THROUGH - - - - D ADDRESS (证服务器, ACCS-SERVER	СОЛ ВИЛИЛСЕ - - - Т ТВИМ РОСИ - Т ТВИМ РОСИ - - - - - - - - - - - - -	SRIVER RULES 1 1 1 0 MATCH RULES	Pending Change
bobility Masser lab1-mm-1 fanaged Network (2) lab1-md1 lab1-md2 Lab1-md2 Lab1-md2 Lab1-md2	Configuration Reles & Policies Authentication Services Interfaces Controllers System License ·红的编辑窗 Add existin Submit: 点言	Auth Server Groups 3 NAME default permit server Group > cepm-tacact NAME 中 口,选择添加已 g server: cp 击提交配置	serves 1 3-4g Servers Options Type □存在的认 opm-taca	TAIL THROUGH - - - - - - - - - - - - - - - - - - -	0 0 0	SERVER RULES	Drag rows to re-ard
lobility Master latanaged Network (2) lata1(2) lata1(2) lata1(2) lata1(2) lata1-md1 lata1-md2 lata1-md	Roles & Policies Authentication Services Controllers System License 建的编辑窗 Add existin Submit: 点音	■ Control Co	serves 1 3-3g servers options 7777 ○ 3-3g Servers options 7777 ○ 3-3g Servers options	FAIL THEOUGH - - - - D ADDRESS UIT服务器。 ACCS-SETVER	C C C C C C C C C C C C C C C C C C C	SERVER RULIS	Orag rows to re-ard
alaagad Network (2) alab 1 (2) □ lab 1 (2) □ lab 1-md 2 □ lab 1-md 2 □ lab 1-md 2 ■ ■ ■ ■ ■ ■ ■	Authentication Services Interfaces Controllers System License 纪的编辑窗 Add existin Submit: 点音	server Groups 3 NAAE getant reterrid commentations reterrid commentations reterrid commentations reterrid	servers 1 ● Seg Servers Options TYPE □ 口 つ つ つ の つ の の の の の の の の の の の の の	Rall TraditionUder 	COAD BALANCE 	SRIVER RULES 1 1 1 0 0 MATCH RULES	Drag rows to re-ord
anaged Network (2) ⇒ lab1 (2) ■ lab1-md1 ■ lab1-md2 ■ lab1-md2 ■ ■ ■ ■ ■	Services Interfaces Controllers System License 组的编辑窗 Add existin Submit: 点司	naat eduction enternation (□ppretectoring + Server Group > cppre-tacacci naat + = = = = g server: cp 击提交配置	servers 	PALT HIROUGH - - - ■ P ADDRESS ↓ 证服务器. ACCS-SERVER	UDAD BALANCE	SRIVER RULES 1 1 3 0 MATCH RULES	Orag rows to re-ord
Lie Labi-md1 ● Labi-md1 ● Labi-md2 ● Labi-md2	Interfaces Controllers System License 组的编辑窗 Add existin Submit: 点音	ordenti 「oppmetacere ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	t seg <u>servers</u> option Troe □存在的认 opm-taca	- - P ADDRESS ↓证服务器- ACS-Server		1 0 MATCH RULES	() Drag rows to re-ord
L	Controllers System License 组的编辑窗 Add existin Submit: 点司	「comtracting ↓ Server Group > cppm-tacact NAATE ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	。 ™ ™ 」 了存在的认 opm-taca	s Server Rules ⊯ ADDRESS \\ \\ ↓ 证服务器 ACS-Server	- TRIM FQON	0 MATCH RULES	① Drag rows to re-ord
认证服务器 ■ ■ ■	Juense License 组的编辑窗 Add existin Submit: 点司	+ Server Group > cppm+tacact NAATE 1 1 1 1 1 5 5 5 5 5 5 5 5 5 5 5 5 5	3-sg <u>servers</u> option ™ □存在的认 opm-taca	s Server Rules ⊮ ADDRESS \\\UILTUR务器 ACS-Server	TRIM FQON	MATCH RULES	① Drag rows to re-ord
认证服务器 ■ ■ ew Server for o	2000年10月1日 组的编辑窗 Add existin Submit: 点音	+ Server Group > cppm-tacact NAME + 口,选择添加已 g server: cp 击提交配置	3-se <u>servers</u> option ™ □存在的认 ppm-taca	s Server Rules ⊮ ADDRESS \\\\UILTUR务器 ACCS-SERVER	TRIM FQON	MATCH RULES	Orag rows to re-ord
认证服务器 ■ ■ ew Server for o	组的编辑窗 Add existin Submit: 点音	Server Group > cppm-tacact NAME 一,选择添加已 g server: cp 击提交配置	⊴存在的认 ppm-taca	s Server Rules PADDRESS 认证服务器 ACCS-SERVER	тим лоом Ф	MATCH RULES	Orag rows to re-ord
认证服务器 ■ ■ ■	组的编辑窗 Add existin Submit: 点音	□,选择添加E g server: cp 击提交配置	⊡存在的认 opm-taca	₩ADDRESS \证服务器 ACS-Server	TRIM PQON	MATCH RULES	
认证服务器 ■ w Server for o	2000年10月1日 组的编辑窗 Add existin Submit: 点音	➡ 口,选择添加E g server: cp 击提交配置	∃存在的认 opm-taca	\证服务器 acs-server	0		
人证服务器 ■ w Server for o	/////////////////////////////////////	➡ □,选择添加E g server: cp 击提交配置	∃存在的认 ppm-taca	\证服务器 acs-server	0		
认证服务器 ■ ■ w Server for o	组的编辑窗 Add existin Submit: 点音	E □,选择添加E g server: cp 击提交配置	∃存在的认 ppm-taca	\证服务器 acs-server	0		
认证服务器 ■ ≝w Server for o	www.coo 组的编辑窗 Add existin Submit: 点音	口,选择添加已 g server: cp 击提交配置	己存在的认 ppm-taca	\证服务器 acs-server	0		
认证服务器 ■ ■	24的编辑窗 Add existin Submit: 点音	口,选择添加E g server: cp 击提交配置	己存在的认 ppm-taca	\证服务器 acs-server	o		
认证服务器 ■ ■ w Server for o	组的编辑窗 Add existin Submit: 点च	口,选择添加E g server: cp 击提交配置	已存在的认 ppm-taca	\证服务器 acs-server	0		
人证服务器 ■ ■ w Server for o	组的编辑窗 Add existin Submit: 点च	口,选择添加E g server: cp 击提交配置	己存在的认 p pm-taca	\证服务器 acs-server	0		
人证服务器 ■ ■ w Server for o	组的编辑窗 Add existin Submit: 点च	口,选择添加E g server: cp 击提交配置	己存在的认 ppm-taca	\证服务器 acs-server	0		
人证服务器 ■ ■ w Server for o	组的编辑窗 Add existin Submit: 点च	口,选择添加已 g server: cp 击提交配置	己存在的认 p pm-taca	\证服务器 acs-server	0		
认证服务器 ■ ■ w Server for o	组的编辑窗 Add existin Submit: 点音	口,选择添加已 g server: cp 击提交配置	己存在的认 ppm-taca	、证服务器 acs-server	0		
小 Ш 加 分 奋 ■ w Server for (组的编辑函 Add existin Submit: 点音	口,远痒祢加口 g server: cp 击提交配置	_1手往的び ppm-taca	化止服分奋。 ACS-Server	0		
ew Server for d	Add existin Submit: 点音	g server: cµ 击提交配置	ppm-taca	acs-server			
ew Server for o	Submit: 点音	g server. c _r 击提交配置	ppin-tace	acs-server			
ew Server for o	Submit: 点语	击提交配置					
ew Server for o	Sinnans 光云	古促父郎直					
ew Server for (
ew Server for o							
	ppm-tacacs-sg						
	~						
	۲	Add existing server	🔾 Add	d new server			
cppm-tacacs	server						
Internal							
			Cane	cel Subm	it		
			Canc				
~ ~							
Server Gr			2 × 1		nnc 语頭・	卡窗口卜设	置.
	oups 下点击	🕆 cppm-tacac	ːs-sg,继	续在 Optio	加了起火		- <u></u> •



aruba

■ 2、TACACS command: Configuration

■ 3、Submit: 点击提交配置

	/ASTER m-1	col O	ACCESS POIN 2 0 0 1 0	rs clients 0	ALERTS		aruba-root-admin v
← Mobility Master >							Ŷ
Ch.	Q Configuration	Auth Servers Ad	vanced				
Mobility Master	Roles & Policies						
Managed Network (2)	Authentication	Server Groups 3	SERVERS	FAIL THROUG	H LOAD	BALANCE SERVER R	ULES =
🔁 lab1 (2)	Interfaces	default	1	**	**	1	
🖘 lab1-md1	Controllers	internal cppm-tacacs-sg	1	-	-	0	۵.
😑 lab1-md2	System						
	License	+		_			
		Server Group > cpp	m-tacacs-sg Servers	Options Server Rul	es		
		Fail through:					
		Load balance:	nting:				
		TACACS comm	ands: Action	Configuration	Show		
	MVA 8400						Cancel Submit
ちった。 副空	四方并同止级	md :r/z					
お3ず: 111自	脉行开问亚纪	mu 设备					
•	1、Pendin	a Changes	: 右上角	点击该按	钘		
•	2、Deploy	/ changes :	点击该投	钳			
	TER	CONT	OLLERS ACCESS POINTS	CLIENTS ALE	RTS		⑦ admin ∽
	ı	⊘ 2	⊙ 0 ⊘ 1 ⊙ 0	? 1 № 0 △	0		
C Mobility Master >	Configuration						Pending Changes Q
Hobility Master	Roles & Policies	Auth Servers Advanced					
lab1-mm-1 Managed Network (2)	Authentication	Server Groups 3					
ab1 (2)	Services	default	SERVERS		LOAD BALANCE	SERVER RULES	
📼 lab1-md1	Controllers	internal	1		-	1	<u></u>
📼 lab1-md2	System	cppm-tacacs-sg	1	-	-	•	
	License	+					
		Server Group > cppm-tacacs	sg Servers Options	Server Rules			(i) Drag rows to re-order
		NAME copm-tacacs-server	TYPE TACACS	IP ADDRESS 10.1.50.41	TRIM FQDN	MATCH RULES	=
		+					
	ArubaMM-VA, 8.4.0.0						
Beer diamont							
Pending Changes							
Pending C	hanges for 1 Group						
	0 · · · · · · · · ·						
🗹 🕣 Mob	ility Master (0 Controlle	er)					
				_			
			Close	Disca	rd changes	Deploy change	25

8.4.2 添加管理员的认证

第1步: 使用 Web 方式登录到 Mobility Master (10.X.50.11) (X:1••••6), 找到 Mobility Master -> Configuration -> System -> Admin 确保 Enable local authentication 是开启的。

-	•	•	
	ER	CONTROLLERS ACCESS POINTS CLIENTS ALERTS \odot 2 \odot 0 \odot 1 \odot 0 $夺$ 1 ϕ 0 \bigtriangleup 0	admin ~
🔶 Mobility Master >			Ŷ
e , a	Configuration	General Admin AirWave CPSec Certificates SNMP Logging Profiles Whitelist More	
🔁 Mobility Master	Roles & Policies		
🗂 lab1-mm-1	Authentication	V Management User	
Managed Network (2)	Services	Enable local authentication:	
🔁 lab1 (2) 🛛 🕂 🖉 🛅	Interfaces	Enable console block:	
📼 lab1-md1	Controllers	Management Users	
📼 lab1-md2	System	NAME ROLE	=
	License	+ Show users with certificate authentication 3 Admin Authentication Options 3 Admin Authentication Servers	
			Cancel Submit

第2步:在该页面下,继续点击 Admin Authentication Option。

ALCONO AND ALL	R	CONTROLLERS ACCESS POINTS ⊙ 2 ○ 0 ⊙ 1 ○ 0	CLIENTS ALERTS	(?) admin ~
🗧 Mobility Master >				Ŷ
Mobility Master Ibil-mm-1 Managed Network (2) Ibil (2) Ibil (2) Ibil-md1 Ciabi-md2	Configuration General Roles & Policies Manaj Authentication En Services En Interfaces Manaj Controllers Manaj License Manaj Services Services Authentication Services Jost Admin Admin	Admin Al/Wave CPSec Certificates rement User Image: Comparison of the compari	SNIMP Logging Profiles Whitelist More	

在 Admin Authentication Option 窗口下设置: 。

- ✓ 1、Enable: 勾选 (必须勾选,这样控制器才会优先使用外置的认证服务器对管理员账号进行认证)
- ✓ 2、Server Group: 选择之前步骤中创建的cppm-tacacs-sg
- ✓ Submit: 点击提交配置



General Admin AirWave C	PSec Certificates SN	NMP Logging	Profiles	Whitelist	More
> Management User					
 Admin Authentication Options 					
Default role:	root 🗸				
Enable:					
MSCHAPv2:					
Server group:	cppm-tacacs-sg 💙				
Management telnet access:					
Login activities persistence period:	0 days				
Login banner text:					
Banner has to be accepted:					
WEBUI AUTHENTICATION					
Username/password:					
Webui HTTPS port (443) access:					
Client certificate:					
Server certificate:	default 💙				
Idle session timeout:	15 minutes 💙				
Re-authentication timeout:	minutes 🗸				
					Cancel

第3步: 配置保存并同步给 md 设备

- Pending Changes: 右上角点击该按钮
- Deploy changes : 点击该按钮

Aruba MOBILITY MASTE Iab1-mm-1	R	CONTROLLERS ⊘ 2 ① 0	ACCESS POINTS CLIENTS ALERTS ○ 1 0 ? 1 № 0	(?) admin ~
🔶 Mobility Master >				Pending Changes 🗘
€ <mark>k</mark> Q	Configuration	General Admin AirWave C	"PSec Certificates SNMP Logging Profiles Whitelist More	
🔁 Mobility Master	Roles & Policies		and contracts areas and contracts there	
📼 lab1-mm-1	Authentication	 Management User 		
Managed Network (2)	Services	 Admin Authentication Options 		
🔁 lab1 (2)	Interfaces	Default role:	root	
🖾 lab1-md1	Controllers	Enable:		
🕒 lab1-md2	System	MSCHAPv2:		
	License	Server group:	cppm-tacacs-sg 👻	
		Management telnet access:		
		Login activities persistence period:	0 days	
		Login banner text:		
		Banner has to be accepted:		
		WEBUI AUTHENTICATION		
		Username/password:		
		Webui HTTPS port (443) access:		
		Client certificate:		
		Server certificate:	default 👻	
		Idle session timeout:	15 minutes 💙	
		Re-authentication timeout:	minutes 👻	-
	ArthaMMAVA 8400			Cancel Submit



Per	nding Changes			
	✓ Pending Changes for 1 Group			
	Mobility Master (0 Controller)			
		Close Discard ch	hanges Deploy changes	

8.5 验证结果

8.5.1 CPPM 上查看认证记录

aruba			Clea	rPass Policy Mana	ger		Menu 🗮
<mark>■</mark> 面板 0	The Acce	ess Tracker page	provides a real-time display of per-session acc	ess activity on the selected serve	er or domain.		^
監视 Compared Live Monitoring Jon Live Monitoring Jon Live Monitoring	T [A	ll Requests]	📑 Lab1-CPPM-1 (10.1.50	0.41)	15 Last 1 day before	e Today	编辑
_❷ 计费 _❷ OnGuard 活动	过滤器: [Request ID	▼ 包含 ▼	Go Clear Filter			显示 20 🔹 记录
	#	Server	Source	Username	Service	Login Status	Request Timestamp 🔹
—————————————————————————————————————	1.	10.1.50.41	TACACS	aruba-read-admin	task7-aruba-device-access- enforcement-policy	ACCEPT	2019/10/15 23:34:34
□□□□ 端点分析器	2.	10.1.50.41	TACACS	aruba-read-admin	task7-aruba-device-access- enforcement-policy	ACCEPT	2019/10/15 23:33:08
- Joseph Vetwork Scan - Joseph Vetwork Devices	з.	10.1.50.41	TACACS	aruba-read-admin	task7-aruba-device-access- enforcement-policy	REJECT	2019/10/15 23:32:34
—— 🖉 审计查看器 — 🎩 事件查看器	4.	10.1.50.41	TACACS	aruba-readonly-admin	task7-aruba-device-access- enforcement-policy	REJECT	2019/10/15 23:32:26
—————————————————————————————————————	5.	10.1.50.41	TACACS	aruba-root-admin	task7-aruba-device-access- enforcement-policy	ACCEPT	2019/10/15 23:29:49
	6.	10.1.50.41	TACACS	aruba-root-admin	task7-aruba-device-access- enforcement-policy	ACCEPT	2019/10/15 23:26:43
	7.	10.1.50.41	TACACS	admin	task7-aruba-device-access- enforcement-policy	REJECT	2019/10/15 23:24:59
	8.	10.1.50.41	TACACS	admin	task7-aruba-device-access- enforcement-policy	REJECT	2019/10/15 23:20:55

✓ 点击认证成功记录,在"概要"选项卡中观察,看看能看到哪些信息。

TACACS+ 会话详细信息	
被要 请求 策略 授	权
会话 ID:	T000001f-01-5da690ed
用户名:	aruba-root-admin
时间:	Oct 16, 2019 11:39:25 CST
状态:	AUTHEN_STATUS_PASS
授权:	1
I ◄ Showing 1 of 1-20 reco	ords ▶ ▶ 导出 显示日志 关闭



۲

ACACS+ 会话详细信息				-
概要 请求 策略 授	权			
月户名:	aruba-root-adm	n		1 🔺
è话 ID:	T0000001f-01-5	da690ed		
1间:	Oct 16, 2019 11	:39:25 CST		
:态)	AUTHEN_STATU	5_PASS		
「求类型:	TACACS_AUTHE	NTICATION		
1息:	-			
客户端 IP:	10.1.50.11:tty0			
远程 IP:	10.20.2.182			
计算属性			\odot	
Authentication:Full-Userr	name	aruba-root-admin		
Authentication:Full-Userr	name-Normalized	aruba-root-admin		
Authentication:Source		[Local User Repository]		
Authentication:Status		User		
Authentication: TacacsAuthenService		AUTHEN_SVC_LOGIN		-
I	ords 🕨 🕨		导出 显示日志 关闭	

✓ 点击"请求"选项卡中观察,看看能看到哪些信息。

✓ 点击"策略"选项卡中观察,看看能看到哪些信息。

TACACS+ 会话详细信息

概要 请求 策略 授权

Policies Used -					
服务名称:	task7-aruba-device-access-enforcement-policy				
认证源:	[Local User Repository]				
角色:	aruba-tacacs-root-admin, [User Authenticated]				
配置文件:	task7-aruba-controller-tacacs-root-access				

I⊲ ⊲ Showing 1 of 1-20 records ► ►I

导出 显示日志 关闭



✓ 点击"授权"选项卡中观察,看看能看到哪些信息。

TACACS	+ 会话详	田信息	Į,			8
概要	请求	箣	峈	授权		
Comma	ands Us	sed	Sta	<u>itus</u>	Request Time	
shell ex	ec		Pas	s	Oct 16, 2019 11:39:25 CST	

I ◄ Showing 1 of 1-20 records ► ►	日本

8.5.2 控制器上查看认证记录

MM控制器可以使用ClearPass上的aruba-root-admin账号登录,而且aruba-root-admin账号可以对控制器进行配置更改和操作。





aruba lab1-mm-1	R	co	NTROLLERS ACC 2 ○ 0 ⊘	CLIEN	nts ALI ⊯0 ∆	erts	① aru	ba-root-admin 👻
Managed Network > lab1 >								Ŷ
C , Q	Dashboard	WLANS 5						
🔁 Mobility Master	Configuration	NAME (SSID)	AP GROUI	P	KEY MANAGE	EMENT INFORMATI	ON	+
📼 lab1-mm-1	WLANs	lab1-peap	lab1-grou	P	WPA2-Enterp	orise		A.
Managed Network (2)	Roles & Policies	lab1-mac	lab1-grou	Р	Open			
🔁 lab1 (2)	Access Points	lab1-portal	lab1-grou	P	Open			
📼 lab1-md1	AP Groups	lab1-guest-register	lab1-grou	P	Open			*
📼 lab1-md2	Authentication	+						
	Services							
	Interfaces							
	Controllers							
	System							
	Tasks							
	Maintenance							
	indirice for the							
	ArubaMM-VA, 8.4.0.0							
		111 <u> </u>						
(]ab1-mm-1) [mynode] #								
(lab1-mm-1) [mynode] # (lab1-mm-1) [mynode] #wh	10 _							
user aruba-root-admin - (lab1-mm-1) [mvnode] #	role root							
(labi-mm-i) [mynode] #								
(lab1-mm-1) [mynode] #	ou suitshas							
(Tabi-mm-i) [mynode] #Sr	low switches							
All Switches								
IP Address IPv6 Address	Name Location	Туре	Model	Version	Status	Configuration State	Config Sync Time (sec)	Config ID
10.1.50.11 None	lab1-mm-1 Building1	floor1 master	ArubaMM-VA	8.4.0.0_68230	up	UPDATE SUCCESSFUL	0	93
10.1.10.12 None	lab1-md2 Building1	floor1 MD	Aruba7010	8.4.0.0_68230	up	UPDATE SUCCESSFUL	ŏ	93
Total Switches:3								
(lab1-mm-1) [mynode] #cc (lab1-mm-1) [00:0b:86:9a	a:af:37] #mdc							
Redirecting to Managed	Device Shell							
(lab1-md1) [MDC] #								
(lab1-md1) [MDC] #								
(Tabl-mdl) [MDC] #								

MM控制器可以使用ClearPass上的aruba-read-admin账号登录,而且aruba-read-admin账号不可以对控制器进行 配置更改和操作。



aruba lab1-mn	n-1		CONTROLLERS	ACCESS POINTS	CLIENTS 1 ≠ 0	ALERTS		•	aruba-read-admin 🐱	
Managed Network >									6	t)
e,	Q Dashboard	WLANS 0								
🔁 Mobility Master	Configuration	NAME (SSID)	AP (ROUP	KEY N	MANAGEMENT	NFORMATION			
🖘 lab1-mm-1	WLANs									
🔁 Managed Network (2)	Roles & Policies									
🔁 lab1 (2)	Access Points									
🗂 lab1-md1	AP Groups									
🗂 lab1-md2	Authentication	T								
	Services	Read only user								
	Interfaces									
	Controllers									
	System									
	Maintenance									
	4mh-144 VA 8400									
	Hubanin VA, 64.00	1								
(lab1-mm-1) [mynode] # (lab1 mm 1) [mynode] #										
(lab1-mm-1) [mynode] #w user aruba-read-admin -	who - role read-only									
(lab1-mm-1) [mynode] #	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,									
(lab1-mm-1) [mynode] # (lab1-mm-1) [mynode] #	show switches									
All Switches										
IP Address IPv6 Addres	S Name Location	туре	Model	Version	Status	Configuration State	Config Sync Time (s	ec)	Config ID	
10.1.50.11 None 10.1.10.11 None	lab1-mm-1 Building1 lab1-md1 Building1	floor1 master	ArubaMM-VA Aruba7010	8.4.0.0_68230	up	UPDATE SUCCESSFUL	0		93	
10.1.10.12 None	lab1-md2 Building1	floor1 MD	Aruba7010	8.4.0.0_68230	up	UPDATE SUCCESSFUL	ŏ		93	
Total Switches:3	rd labt mdt									
(lab1-mm-1) [00:0b:86:9	9a:af:37] #configure ter	minal d with CNTL (7								
(labt an 1) [00.0b 05.0	nmanus, one per tine. En									
Error:You do not have p	permission to execute th	is command								
(lab1-mm-1) [00:0b:86:9 (lab1-mm-1) [00:0b:86:9	Da:af:37] (config) # Da:af:37] (config) #									

MM控制器仍然可以继续使用本地的admin账号登录,且可以对控制器进行配置更改和操作。





	/ MASTE mm-1	R					LERS ACCE	ESS POINTS	CLIEN	ALERTS			۲	admin 🗸	
Managed Network > lab1	>														¢
e,	Q	Dashboard		WI ANE 5											
🔁 Mobility Master		Configuration		NAME (SSIC))	A	AP GROUP		KE	Y MANAGEMENT		INFORMATION			-
📼 lab1-mm-1		WLANs		lab1-peap		1	lab1-group		WF	PA2-Enterprise		-			-
Managed Network (2)		Roles & Po	licies	lab1-mac		l.	lab1-group		Op	ien .		-			
🔁 lab1 (2)		Access Poi	nts	lab1-portal		L.	lab1-group		Op	ien .		-			. 1
📼 lab1-md1		AP Groups		lab1-guest-	register	h.	lab1-group		Op	ien		-			-
📼 lab1-md2		Authentica	ition	+											
		Services													
		Interfaces													
		Controller	5												
		System													
		Tasks													
		Maintenance													
		ArubaMM-	/A. 8.4.0.0												
(lab1-mm-1) [mynode] (lab1-mm-1) [mynode] (lab1-mm-1) [mynode] (lab1-mm-1) [mynode] (lab1-mm-1) [mynode] (lab1-mm-1) [mynode] (lab1-mm-1) [mynode] (lab1-mm-1) [mynode]	# # # #who pt #														
(lab1-mm-1) [mynode]	#														
(labl-mm-1) [mynode]	#shov	v switches													
All Switches															
IP Address IPv6 Addr	ess	Name	Location	т, –	ype	Model	Version		Status	Configuration	State	Config Sync Time (sec)	Contig ID		
10.1.50.11 None 10.1.10.11 None 10.1.10.12 None		lab1-mm-1 lab1-md1 lab1-md2	Building1.f Building1.f Building1.f	loor1 m loor1 M loor1 M	aster D D	ArubaMM-VA Aruba7010 Aruba7010	8.4.0.0 8.4.0.0 8.4.0.0	_68230 _68230 _68230	up up up	UPDATE SUCCESS UPDATE SUCCESS UPDATE SUCCESS	SFUL SFUL SFUL	0 0 0	94 94 94		
Total Switches:3 (lab1-mm-1) [mynode] (lab1-mm-1) [00:0b:86	#cd :9a:a	lab1-md1 af:37] #mdc													
Redirecting to Manag	jed De	evice Shell													
(lab1-md1) [MDC] # (lab1-md1) [MDC] # (lab1-md1) [MDC] # (lab1-md1) [MDC] # (lab1-md1) [MDC] #															



9 TASK8: INSIGHT 实现自动生成报表及告警

9.1 用户需求

用户需要统计每天的无线网络认证情况(认证次数、成功次数、失败次数等),认证的终端数量及用户数量,以 及不同终端类型的终端数量,希望能够自动生成报表,以便于了解网络使用情况。

同时,当有终端连续多次认证失败时,系统自带产生告警提示,避免有用户暴力破解员工密码。

9.2 实现思路

- ✓ ClearPass自带的Insight模块,可以实现自定义报表和自定义告警功能,可以每天、每周、每月自动生成报表,同时可以通过Email的方式自动向指定的管理员邮箱发送报表内容和告警信息
- ✓ 配置步骤如下:
 - 1、开启Insight功能;
 - 2、创建Insight Report,把当天LabX所有控制器发起的Radius认证记录生成报表;
 - 3、创建Insight Alert,当同一终端5分钟内认证失败次数超过3次时,产生告警。

9.3 ClearPass 配置

9.3.1 开启 Insight 功能

第1步: 在ClearPass Policy Manager中, 打开 管理 - > 服务器管理器 - > 服务器配置, 点击右边的服务器, 进入 服务器配置 界面。



第2步:在服务器配置界面中,勾选启用 Insight 和 Enable as Insight Master,点击保存。

管理 » 服务器管理器 » 服务器配置 - Lab1-CPPM-1

服务器配置 - Lab1-CPPM-1 (10.1.50.41)

系统	服务控制	服务参数	系统监视	网络接口	FIPS					
主机名:				Lab1-CPPM-	·1					
FQDN:										
策略管理署	器区:			default		\$				管理策略管理器区
Enable P	erformanc	e Monitorin	g Display:	🗹 Enable t	his serve	er for performance mo	nitoring display			
Insight S	Setting:			☑ 启用 Insi	ght	🗹 Enable a	s Insight Master	Current Master:-		
Enable Ir	ngress Eve	nts Process	sing:	🗆 Enable I	ngress E	events processing on the	nis server			
Master S	erver in Z	one:		Primary ma	aster	\$				
Span Por	t:			None		\$				
						IPv4	IF	Pv6	操作	
		IF	P Address			10.1.50.41				
Manage	ment Por	t S	ubnet Mask	< C		255.255.255.0			Configure	
		D	efault Gate	way		10.1.50.250				
		IF	9 Address							
Data/Ex	ternal Po	ort S	ubnet Mask	c					Configure	
		D	efault Gate	way						
		主				10.0.50.20				
DNS Set	tinas	Ж				114.114.114.114			Configure	
	lingo	Te	ertiary						comgaro	
< 返回服	服务器配置								¢.	存 Cancel

9.3.2 进入 Insight 界面

第1步: 在ClearPass Policy Manager中, 打开 面板, 在右边 Quick Links 中点击 ClearPass Insight, 进入 ClearPass Insight 界面。

□□ 雨垢 ○	次念	土机名	Zone
		Lab1-CPPM-1 (10.1.50.41)	default
警报 最近的警报	System CPU L	Jtilization	0
• 所有请求 所有策略管理器请求的趋势	100 —		
● 应用程序 启动其他 ClearPass 应用程序	Centage		
验证状态 成功和失败验证的趋势	B er		
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	14	4:00 14:05 14:10 14:15 14:20 Time (mins)	14:25
设备类别 设备类别		🔶 System 🔶 User 🖶 IO Wait 📥 Idle	
设备系列 设备系列	Quick Links		0
2 Endpoint Profiler Summary	☆ 开始配置策■	各	
Endpoint profiling details	🌣 管理服务		
~ 生败验证	冯 访问跟踪器		
國國 跟踪最近失败的验证	🔜 分析和趋势		
■ 健康状态	🗘 网络设备		
建康和不健康请求的趋势	📲 服务器管理器		
最新验证 最新验证	🥵 ClearPass (Guest	
🖌 监视 🔹 💿	ClearPass (Onboard	
<i>总</i> 配置 0	ClearPass 1	Insight	
	The areas a clear Pass I	Extensions	



第2步:由于刚开启Insight,还没有认证记录,所以Insight界面显示TOTAL AUTH为0,通过远程桌面登录相应 LabX 的 Wireless Client (10.X.50.102,用户名: lab,密码: Aruba123!),断开其无线网络连接,重新连 接到前面章节创建的无线网络(例如 labX-peap),并通过ClearPass完成认证。这样Insight就会产生记录, 查看Insight界面是否有认证记录。

ClearPass Insight			11	FAILED AUTH	UNIQUE	3	UNIQUE 5	USERS						AL	ERTS 0	Menu	=
										Q Se	arch using	Username/	'Endpoint/Cl	learPass Ser	ver/Netwo	ork Device	
Dashboard	Dashb	oard From:	October 08, 201	9 00:00 To: O	ctober 08, i	2019 15:46								Today 1	w 1m	Custon	n 🗸
Authentication																	
Endpoints	Authent	ication Trend											Tota	al Succ	ess vs Fa	ailed	~
Guest																	
Licensing													ClearP	ass Servei	All		•
Network	Reque:	st Count															
Posture	12.5																
System Monitor	10																
Inventory	7.5																
Reports	2.5																
Alerts	0	00:00 01:	00 02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	
Administration							_									Tin	ne
							-	Total Authen	tications								

9.3.3 添加 Insight Report

第1步:在ClearPass Insight中,打开 Reports - > Configuration,点击右边的 Create New Report 按钮,进入 Create New Report 界面。

ClearPass Insight	TOTALAUTH FAILED AUTH UNIQUE ENDPOINTS UNIQUE U	iers	ALERTS 🧿 Menu 🗮
		Q Search using Use	rname/Endpoint/ClearPass Server/Network Device
Dashboard	Configured Reports		Import report Create New Report
Inventory			
Reports	Configuration		٩
Configuration	# NAME A DESCRIPTION ~	TEMPLATE ~	ENABLE -
Custom Reports	No da	ta available in table	
Alerts	20 v per page • Error • In Progress • Completed		Page: Go <>
Administration	Top 10 Reports Time to Run 30 Days	Top 10 Reports Last 30 Days	

第2步:在 Create New Report 界面,设置以下内容:

- ✓ **Report Name:** Radius Auth from LabX Controllers
- ✓ Category: RADIUS Authentication, 勾选 RADIUS-Auth Overview



- ✓ Notifications: 如需通过Email发送Report, 需要勾选 Notify by Email 并在下方输入框中填写 收 件人邮箱。必须先在ClearPass Policy Manager中设置好SMTP, 才可以勾选Notify by Email, 否则无法勾选Notify by Email, 设置SMTP方法请参考第7章 访客自注册中的SMTP设置内容
- ✓ Options: 勾选 Include raw data in output , 勾选此项会同时生成CSV格式的详细report记录
- ✓ Repeat Scheduled Report:选择 No Repeat,由于实验时间的限制,这里选择No Repeat,如
 需周期性自动生成报告,可选择 Daily、Weekly、Monthly
- ✓ Preset Date Range:设置报告运行的时间期间,选择 Today,从0点开始到当前时间

						54	пріс кероі
Create New Report							
What would you like to see in your new Report?							
Report Name Radius Auth from Lab1 Controllers Description Description	Category RADIUS Authentication RADIUS - Auth Overview RADIUS - Auth Overview RADIUS - Auth by AuthSrc RADIUS - Auth by AuthSrc RADIUS - Auth by ClearPass RADIUS - Failed Auth	~	Notifications Notify by Email jinghao.ma@hpe.com Notify by SMS	*	Options Include raw dat A full set of raw CSV reports Enable remote a Configure the I Administration destination.	a in output w data is only customi: copy Remote Directory in th section to specify the	zable in the ne : remote coj
Repeat Scheduled Report	Preset Date Range	Date		to			
No Repeat	▼ Today ▼	2019-10-08 YYYY-MM-DD	HH:MM	Y	2019-10-08 /YYY-MM-DD	6:33 PM HH:MM	
Report Summary Your RADIUS Authentication > RADIUS - Auth I	Overview report will contain data from 2019-	10-08 12:00 AM to 201	9-10-08 6:33 PM.				

第3步:通过 Filters 设置过滤规则,设置内容如下:

✓ NAD IP STARTS_WITH 10.X.



点 Next 讲入下一步

Create New Report

Operator	Value	
STARTS_WITH	✓ 10.1.	📅 Add Another
your CSV Export.		
	SELECTED COLUMNS	
	1 MAC Address	.
	2 Authentication Username	=
	3 Authentication Service	.
	4 Authentication Status	=
	5 ClearPass Server	=
	Operator STARTS_WITH your CSV Export.	Operator Value STARTS_WITH 10.1. your CSV Export. SELECTED COLUMNS 1 MAC Address 2 Authentication Username 3 Authentication Status 4 Authentication Status 5 ClearPass Server

编辑CSV中记录的内容,在 AVAILABLE COLUMNS 中勾选需要的内容,如: Device Category、Device Family 等,点击 Next 进入下一步

Create New Report			Sample Report
Configure CSV Raw Data Columns			
Select and drag to organize the order of columns in your CSV Exp	port.		
AVAILABLE COLUMNS	SELECTED COLUMNS		
Authorization Source	1 MAC Address	• =	
Called Station ID	2 Authentication Username	• =	
✓ ClearPass Server	3 Authentication Service	• =	
Conflict	4 Authentication Status	• =	
✓ Device Category	5 ClearPass Server	• =	
✓ Device Family	6 NAD IP	• =	
Device Name	7 Timestamp	• =	
Disk Encryption Input	8 Authentication Method	= =	
Disk Encryption Output		÷ =	
		Clear All	
Logo and Branding			
Do you want to change logo info?			
			Next

确认Report Summary内容无误后,点击 Save 保存



aruba

Report Summary Sample Report Report Summary Edit Report 🔊 Report Name Radius Auth from Lab1 Controllers Description Category RADIUS Authentication > RADIUS - Auth Overview Notifications Notify by Email: jinghao.ma@hpe.com Notify by SMS: None Schedule Report contains data from 2019-10-08 12:00 AM to 2019-10-08 6:33 PM Filters 1. NAD IP: STARTS_WITH : 10.1. Raw Data Columns 1. MAC Address 2. Authentication Username Authentication Osernia
 Authentication Service
 Authentication Status 5. ClearPass Server 6. NAD IP 7. Timestamp 8. Authentication Source 9. Authentication Method 10. Device Category 11. Device Family Logo & Branding Default Logo and Branding Cancel Save

第4步: 打开 Reports - > Configuration, 查看刚才创建的Report状态,

Report Name前面的圆点表示状态,黄色表示正在运行,刷新页面,绿色表示运行完成。如果勾选了 Notify by Email ,运行完成后会自动发送指定的邮箱,点击Report后面的 文件夹 按钮进入 Created Reports 页面,点击 Report Name查看,或者点后面的 下载 按钮下载Report内容

Dashboard	Configured Reports				Import report Create New	w Report
Inventory						
Reports	Configuration					٩
Configuration	# NAME •	DESCRIPTION ~	TEMPLATE ~	EN	ABLE -	
Custom Reports	1 Radius Auth from Lab1 Controllers		RADIUS - Auth Overview	EN	IABLED 🔨 🦳 🕯 🕨	
Alerts	20 v per page • Error • In	Progress Completed			Page; Go <	1 >
Administration		riogram e compress				
Reports > Radius	Auth from Lab1 Controll	ers			Create New	Report
Report Summary					Edit Rep	ort 🔊
Report Name	Radius Auth from Lab1 Controlle	rs				
Description						
Date/Schedule	Report contains data from 2019	10-08 08:00 to 2019-10-08 18:30				
Category	RADIUS Authentication > RADIUS	- Auth Overview				
Created Reports						
# NAM	E 👻			CREATED AT 🝷		
1 🗌 🖲 Radiu	us Auth from Lab1 Controllers			2019-10-08 18:51	<u>ن</u> ش	
20 🗸 per page					Page: Go <	1 >

9.3.4 添加 Insight Alert

第1步:在ClearPass Insight中,打开 Alerts,点击右边的 Create New Alert 按钮,进入 Create New Alert 界面。

ClearPass Insig	ht	TOTAL AUTH 28 FAILED AUTH 9	UNIQUE ENDPOINTS 3 UNIQUE US	ers 7	ALERTS 🗿 Menu 🗮
					Q. Search using Username/Endpoint/ClearPass Server/Network Devic
Dashboard	Alerts				Create New Alert
Inventory					
Reports	Alerts				۹
Alerts	# NAME 🔺	TEMPLATE ~	LAST ALERT	DESCRIPTION -	MUTE ~
			No data available in table		
Configuration Watchlist	20 v per page • Critical	Warning			Page: Go <>
Administration					

第2步:在 Create New Alert 界面,设置以下内容:

- ✓ Alert Name: Authentication Fail 3 timers per 5 minutes from LabX Controllers
- ✓ Category: Authentication, 勾选 RADIUS Failed Authentication
- ✓ Notifications: 如需通过Email发送Report,需要勾选 Notify by Email 并在下方输入框中填写 收 件人邮箱。必须先在ClearPass Policy Manager中设置好SMTP,才可以勾选Notify by Email,否则无法勾选Notify by Email,设置SMTP方法请参考第7章 访客自注册中的SMTP设置内容
- ✓ Filter: 设置 NAD IP STARTS_WITH 10.X.
- ✓ **Trigger:** 设置 Critical 3 5 Minutes

点 Save 保存

Create New Alert

Alert Name	Category		Notifications
Authentication Fail 3 timers per 5 minutes from Lab1 Controllers	Authentication	~	Notify by Email
Description	Failed Authentication		jinghao.ma@hpe.com
Description	RADIUS Failed Authentication		
	Total Authentication		
4	WEBAUTH Failed Authentication		Notify by SMS
			li li
Filter			
NAD IP STARTS WITH	∽ 10.1.		a Add Another
			_
Trigger			
Severity Threshold	Interval		
• Critical v 3	5 Minutes	~	
Alert Summary			
Notify when RADIUS failed authentications with selected filter exceed 3 in 5 minute	(s)		
			Cancel



第3步:通过远程桌面登录相应 LabX 的 Wireless Client (10.X.50.102,用户名: lab,密码: Aruba123!),断 开其无线网络连接,重新连接到前面章节创建的Portal认证无线网络 labX-portal,在弹出的Portal页面输 入错误的账号密码,5分钟内连续输入超过3次错误账号密码,等待大概5分钟后,观察Insight右上角的 ALERTS 计数,如下图显示 ①,点击后显示Alerts记录,在Alert Name上点击进入,查看 Alert History 记 录,点右边的 浏览 按钮显示 Alert Details,可查看具体的认证终端Mac和用户名。

ClearPass Insig	ht	TOTAL AUTH	33 FAILED AUTH 12 UNIQ	UE ENDPOINTS 3 UNIQUE US	ers 7	ALERTS 1 Menu
						Q. Search using Username/Endpoint/ClearPass Server/Network D
ard	Alerts					Create New A
у						create new A
	Alerts					
		NAME 🔺	TEMPLATE ~	LAST ALERT	DESCRIPTION ~	MUTE ~
turation	1 •	Authentication Fail 3 times per 5 minutes from Group1 Controllers	RADIUS Failed Authentication	2019-10-08 20:28		
list	20 y per page	Critical Warning				Page: Go (1
ration	per propri					
a dauth an ti						
s > Authentic	ation Fall 3 times	s per 5 minutes fror	n Lab1 Controllers			Create New Al
Summary						Edit Alert
Name	Authentication Fail 3 t	imes per 5 minutes from Lab1	Controllers			
ription						
Summary	Alert configured with t	threshold 3 and interval 5 minu	ute			
egory	Authentication > RADI	IUS Failed Authentication				
istory						
SERVER	COUNT -	BEGIN DATE		END DATE 👻	CREATED AT 🝷	
all	8	2019-10-09 14:1	5	2019-10-09 14:25	2019-10-09 14:24	
✓ per page						Page: Go 🦂 1
II Down						
scription						
rt Summary	Alert configured	d with threshold 3 and inter	val 5 minute			
egory	Authentication	> RADIUS Failed Authentica	tion			
ver	all servers					
nt or more	8					
in Date	2019-10-09 14:1	15				
Date	2019-10-09 14:2	25				
ated At	2019-10-09 14:2	24				
er	auth pad in: CT	ARTS WITH 10.1				
	aaaaaaa_p. 30					
t Details						
STAMP		CLEARPASS SERVER	MAC	l	JSER	ERROR
-10-09 14:21:48		Lab1-CPPM-1	None	I	ab11-test	User not found
9-10-09 14:21:05		Lab1-CPPM-1	7c7a914	16236e c		User not found
9-10-09 14:20:57		Lab1-CPPM-1	7c7a914	16236e k	0	User not found
9-10-09 14:20:48		Lab1-CPPM-1	7c7a914	16236e a	a	User not found
9-10-09 14:20:25		Lab1-CPPM-1	None	t	ask1-test	User not found
9-10-09 14:20:08		Lab1-CPPM-1	None	t	ask1-test	Internal error in RADIUS server
9-10-09 14:19:59		Lab1-CPPM-1	None	t	ask1-test	Failed to classify request to service
19-10-09 14:18:49		Lab1-CPPM-1	88108ft	ae168 8	38108fbae168	User authentication failed



10 TASK9: CPPM 认证基本问题诊断

10.1 用户需求

用户希望能够针对认证失败原因进行快速的诊断和定位,而不是像传统的方式在网络中进行复杂的抓包分析。

10.2 实现思路

- ✓ ClearPass自带的 访问跟踪器 详细记录了每一次认证的相关信息,包括 RADIUS请求报文信息、ClearPass 计算属性、ClearPass授权属性、终端属性、RADIUS响应信息、认证失败的错误信息 等,查询到对应终端/ 用户的认证记录即可快速的定位认证问题
- ✓ 认证问题排查步骤如下:
 - 1、查看 ClearPass访问跟踪器,过滤相应的认证记录,是否有对应的认证记录存在;
 - 2、如果存在对应的认证记录,查看认证记录的 认证失败告警信息及其他信息,即可排查认证失败原因;
 - 3、如果不存在对应的认证记录,一是可能ClearPass未收到认证请求,二是可能ClearPass收到了认证 请求,但是NAS设备未添加到ClearPass的网络设备列表中或者共享密钥不一致。

10.3 ClearPass 认证问题诊断

10.3.1 访问跟踪器过滤和查看认证记录

第1步: 在ClearPass Policy Manager中,打开 监视 - > Live Monitoring - > 访问跟踪器,右边会显示认证记录,黑色为认证成功的记录,红色为认证失败的记录,点击某一条认证记录可以查看详细的认证信息,分别点击上方的 概要、输入、输出、警报 等按钮,查看详细信息。

aruba			Cle	arPass Policy Manager			Menu
	○ 监视 » L	.ive Monitoring » 값	问跟踪器				
■ 监視	 访问跟 	腔器 Oct 09 2019	17:46:31 CST				自动刷新
- A Live Monitoring	The Act	and Tracker page	wouldoo a waal timo dianlay of pay coopia	a needed activity on the colorted conve	r or domain		
➢ 访问跟踪器 ➢ 计费		Il Requests]	Lab1-CPPM-1 (10	0.1.50.41)	ir or domain.	e Today	编辑
- MonGuard 活动							
分析和趋势							
一國永統溫代 	过滤器:	Request ID		o Clear Filter			显示 20 🗘 记录
→ 一部 审计查看器	#	Server	Source	Username	Service	Login Status	Request Timestamp +
→ 事件查看器	1.	10.1.50.41	RADIUS	leader	task4-802.1x-auth-service	ACCEPT	2019/10/09 17:23:39
	2.	10.1.50.41	RADIUS	leader	task4-802.1x-auth-service	ACCEPT	2019/10/09 17:06:16
Blacklisted Users	3.	10.1.50.41	RADIUS	employee	task4-802.1x-auth-service	ACCEPT	2019/10/09 16:57:45
	4.	10.1.50.41	RADIUS	employee	task4-802.1x-auth-service	ACCEPT	2019/10/09 16:24:21
	5.	10.1.50.41	RADIUS	lab1-test	task1-test-service	ACCEPT	2019/10/09 14:21:57
	6.	10.1.50.41	RADIUS	lab11-test	task1-test-service	REJECT	2019/10/09 14:21:48
	7.	10.1.50.41	RADIUS	c	task1-test-service	REJECT	2019/10/09 14:21:05
	8.	10.1.50.41	RADIUS	b	task1-test-service	REJECT	2019/10/09 14:20:57
	9.	10.1.50.41	RADIUS	а	task1-test-service	REJECT	2019/10/09 14:20:48
	10.	10.1.50.41	RADIUS	task1-test	task1-test-service	REJECT	2019/10/09 14:20:25
	11.	10.1.50.41	RADIUS	task1-test		REJECT	2019/10/09 14:20:08
	12.	10.1.50.41	RADIUS	task1-test		REJECT	2019/10/09 14:19:59
	13.	10.1.50.41	RADIUS	88108fbae168	lab5-mac-service	REJECT	2019/10/09 14:18:49
	14.	10.1.50.41	RADIUS	5cc307d9b212	lab2-mac-service	REJECT	2019/10/09 13:15:56
	15.	10.1.50.41	RADIUS	88108fbae168	lab2-mac-service	REJECT	2019/10/09 12:49:13
	16.	10.1.50.41	RADIUS	5cc307d9b212	lab5-mac-service	REJECT	2019/10/09 09:49:11
	17.	10.1.50.41	RADIUS	c	lab3-portal-service	REJECT	2019/10/08 21:07:46
	18.	10.1.50.41	RADIUS	jma1	lab3-portal-service	ACCEPT	2019/10/08 21:07:21
	19.	10.1.50.41	RADIUS	b	lab3-portal-service	REJECT	2019/10/08 21:07:09
	20.	10.1.50.41	RADIUS	a	lab3-portal-service	REJECT	2019/10/08 21:07:00



请求详细信息	0			
概要 输入 输出	计费			
登录状态:	ACCEPT			
会话标识符:	R00000053-01-5d9da71b			
日期和时间:	Oct 09, 2019 17:23:39 CST			
终端主机标识符:	7C7A914652B7 (Computer / Windows / Windows)			
用户名:	leader			
访问设备 IP/端口:	10.1.10.21:0			
系统安全状况状态:	UNKNOWN (100)			
	所用策略 -			
服务:	task4-802.1x-auth-service			
认证方法:	EAP-PEAP			
认证源:	Local:localhost			
授权源:	[Local User Repository]			
角色:	[User Authenticated], leader-role			
强制执行配置文件:	task4-802.1x-leader-profile			
I < Showing 1 of 1-20	records ▶ ▶ 更改状态 Show Configuration 导出 显示日志 关闭			

第2步: 在 访问跟踪器 上方功能区,可以通过左侧的 过滤器 来过滤想要查看的认证记录,可以通过右边的 显示 记录数下拉框 修改每页显示的认证记录数量,通过右上角 编辑 按钮,可以修改显示的内容,以及修改显示 的记录天数。在 Available Columns 中选择 Host MAC Address,点击 右箭头,点保存,这时会在访问 跟踪器中显示终端MAC地址。

[All Requests]	Lab1-CPPN	I-1 (10.1.50.41)	1 day before	e Today	
器: Request ID	♦ 包含	. Go Clear Filter			显示 20
# Server	Source	Username	Service	Login Status	Request Timestamp +
10.1.50.41	RADIUS	leader	task4-802.1x-auth-service	ACCEPT	2019/10/09 17:23:39
. 10.1.50.41	RADIUS	leader	task4-802.1x-auth-service	ACCEPT	2019/10/09 17:06:16
10.1.50.41	RADIUS	employee	task4-802.1x-auth-service	ACCEPT	2019/10/09 16:57:45
10.1.50.41	RADIUS	employee	task4-802.1x-auth-service	ACCEPT	2019/10/09 10:24:21
10.1.50.41	RADIUS	empioyee	task4-802.1X-autn-service	ACCEPT	2019/10/09 16:24:21
10.1.50.41	RADIUS 访问跟踪器	empioyee	task4-ou2.1x-auth-service	ACCEPT	2019/10/09 16:24:21
10.1.50.41 Live Monitoring > 很踪器 Oct 09, 20 ccess Tracker pag	RADIUS 访问跟踪器 19 18:03:58 CST e provides a real-time display of per-	employee	ver or domain.	ACCEPT	2019/10/09 16:24:21
10.1.50.41 Live Monitoring > 很踪器 Oct 09, 20 cccess Tracker pag ect Server/Dom	RADIUS 访问跟踪器 19 18:03:58 CST e provides a real-time display of per- iin: Lab1-CPPM-1 (10.1.50.41) 年	employee	ver or domain.	ACLEPI	2019/10/09 16:24:21
10.1.50.41 Live Monitoring > 很踪器 Oct 09, 20 cccess Tracker pag ect Server/Dom 过滤器: [All Require	RADIUS 访问跟踪器 19 18:03:58 CST # provides a real-time display of per- in: Lab1-CPPM-1 (10.1.50.41)	employee	ver or domain.		2019/10/09 16:24:21
10.1.50.41 Live Monitoring > 很踪器 Oct 09, 20 cccess Tracker page ect Server/Dom 过滤器: [All Requi 日期范围: Last 10	RADIUS 访问跟踪器 19 18:03:58 CST # provides a real-time display of per- tim: Lab1-CPPM-1 (10.1.50.41)	employee session access activity on the selected ser 显示最新	ver or domain.		2013/10/03 10:24:21
10.1.50.41 Live Monitoring > 很踪器 Oct 09, 20 cccess Tracker pag act Server/Dom 过滤器: [All Requind 日期范围: Last 1 (1 ect Columns:	RADIUS 访问跟踪器 19 18:03:58 CST # provides a real-time display of per- iin: [Lab1-CPPM-1 (10.1.50.41)	employee session access activity on the selected ser 显示最新	ver or domain.		2013/10/03 15:24:21
10.1.50.41 Live Monitoring o 段踪器 Oct 09, 20 cccess Tracker pag ect Server/Dom 过滤器: 〔All Requi 日期范围: Last 〔d ect Columns: lable Columns	RADIUS 访问跟踪器 19 18:03:58 CST # provides a real-time display of per- in: Lab1-CPPM-1 (10.1.50.41) \$ts] \$ts] \$ @ Add ay \$ before	employee session access activity on the selected ser 显示最新	ver or domain.		2019/10/09 15:24:21
10.1.50.41 Live Monitoring A 現踪器 Oct 09, 20 cccess Tracker pag act Server/Dom 过滤器: [All Requi 日期范围: Last 10 ect Columns: ilable Columns	RADIUS 访问跟踪器 19 18:03:58 CST # provides a real-time display of per- in: Lab1-CPPM-1 (10.1.50.41)	employee session access activity on the selected ser 显示最新	ver or domain.		2019/10/09 15:24:21
10.1.50.41 Live Monitoring of 很踪器 Oct 09, 20 cccess Tracker pag ect Server/Dom 过滤器: [All Requi 日期范围: Last 11 ect Columns: liable Columns h Type	RADIUS 访问跟踪器 19 18:03:58 CST a provides a real-time display of per- tim: Lab1-CPPM-1 (10.1.50.41) (stsj) (employee session access activity on the selected ser 显示最新	ver or domain.	ACLEPI	2019/10/09 15:24:21

过滤器:	Request ID 🗘 包含 🗘	💮 Go Clear Fi	iter			显示 20 🗘 记录
#	Server	Source	Username	Service	Login Status	Request Timestamp +
1.	10.1.50.41	RADIUS	leader	task4-802.1x-auth-service	ACCEPT	2019/10/09 17:23:39
2.	10.1.50.41	RADIUS	leader	task4-802.1x-auth-service	ACCEPT	2019/10/09 17:06:16

第3步:通过远程桌面登录相应 LabX 的 Wireless Client (10.X.50.102,用户名: lab,密码: Aruba123!),将 无线网络连接到 labX-mac 后,重新连接到Portal认证无线网络 labX-portal,在弹出的Portal页 面输入 账号: leader,密码: aruba 进行认证,提示认证失败,再输入 账号: leader,密码: aruba123 进行认证,仍然提示认证失败,再输入 账号:guest, 密码: aruba123 进行认证,认证成功, 记录终端MAC地址。

第4步:在 过滤器 中设置过滤器内容如下:

✓ Host MAC Address 包含 <终端的MAC>

点 Go 按钮进行过滤,下方会显示过滤的认证记录,能看到最近的三次认证记录,两次Username为leader认证 失败,一次Username为guest认证成功。

监视》L 访问跟 The Acc	ive Monitoring » 访问 踪器 Oct 10, 2019 : ess Tracker page pr	可跟踪器 21:35:04 CST rovides a real-time display of per	-session access activity on th	e selected server or domain.			⊘ 自动刷新
💎 [AI	Requests]	Lab1-CPPM	-1 (10.1.50.41)		Last 1 day before Toda	ау	编辑
过滤器:〔	Host MAC Address	◆ 包含◆ 7c7a9146236e	Go Clear Filter				显示 20 🗘 记录
过滤器:〔 #	Host MAC Address	◆ 包含◆ 7c7a9146236e Source	⊕ Go Clear Filter Username	Service	Login Status	Request Timestamp •	显示 20 🗘 记录 Host MAC Address
过滤器:〔 # 1.	Host MAC Address Server 10.1.50.41	◆ 包含◆ 7c7a9146236e Source RADIUS	€ Go Clear Filter Username guest	Service task3-portal-service	Login Status ACCEPT	Request Timestamp • 2019/10/10 15:21:22	显示 20 ◆ 记录 Host MAC Address 7c7a9146236e
过滤器:(# 1. 2.	Host MAC Address Server 10.1.50.41 10.1.50.41	◆〔包含◆〕7c7a9146236e Source RADIUS RADIUS	€ Go Clear Filter Username guest leader	Service task3-portal-service task3-portal-service	Login Status ACCEPT REJECT	Request Timestamp • 2019/10/10 15:21:22 2019/10/10 15:06:15	显示 20 ◆ 记录 Host MAC Address 7c7a9146236e 7c7a9146236e
过滤器:(# 1. 2. 3.	Host MAC Address Server 10.1.50.41 10.1.50.41 10.1.50.41	◆ 包含◆ 7c7a9146236e Source RADIUS RADIUS RADIUS	Go Clear Filter Username guest leader leader	Service task3-portal-service task3-portal-service task3-portal-service	Login Status ACCEPT REJECT REJECT	Request Timestamp • 2019/10/10 15:21:22 2019/10/10 15:06:15 2019/10/10 14:29:56	显示 20

10.3.2 通过访问跟踪器分析认证失败原因

第1步:在9.3.1章节中过滤的认证记录中,点击第一条通过用户名leader认证失败的记录(即编号为3的认证记录),进入请求详细信息显示框,点击上方的警报按钮,显示错误消息:User authentication failed,此 请求的警报 RADIUS PAP: CLEAR TEXT password check failed,提示密码校验失败,也就是密码错误。

请求详细信息	0
概要 输入 输出	警报
登录状态:	REJECT
会话标识符:	R0000005-01-5d9ecfe4
日期和时间:	Oct 10, 2019 14:29:56 CST
终端主机标识符:	7C7A9146236E (Computer / Windows / Windows)
用户名:	leader
访问设备 IP/端口:	10.1.10.21:0
系统安全状况状态:	UNKNOWN (100)
	所用策略 -
服务:	task3-portal-service
认证方法:	PAP
认证源:	Local:localhost
授权源:	-
角色:	-
强制执行配置文件:	[Deny Access Profile]
I ◄ Showing 3 of 1-3	records ▶ ▶ Show Configuration 导出 显示日志 关闭



请求详细值	言息							8
概要	输入	输出	警报					
错误代码	: 216							Γ
错误类别	: Auth	enticat	ion failure					
错误消息	: User	auther	ntication failed					
此请求的	的警报							
RADIUS	S PAP:	CLEAR	R TEXT passwor	d check failed				

第2步:在9.3.1章节中过滤的认证记录中,点击第二条通过用户名leader认证失败的记录(即编号为2的认证记录),进入请求详细信息显示框,点击上方的警报按钮,显示错误消息:Access denied by policy,此 请求的警报 RADIUS Applied 'Reject' profile,提示应用了Reject的Profile,被策略拒绝。

请求详细信息	
概要 输入 输出	警报
登录状态:	REJECT
会话标识符:	R0000006-01-5d9ed867
日期和时间:	Oct 10, 2019 15:06:15 CST
终端主机标识符:	7C7A9146236E (Computer / Windows / Windows)
用户名:	leader
访问设备 IP/端口:	10.1.10.21:0
系统安全状况状态:	UNKNOWN (100)
	所用策略 -
服务:	task3-portal-service
认证方法:	PAP
认证源:	Local:localhost
授权源:	[Local User Repository]
角色:	[User Authenticated], leader-role
强制执行配置文件:	[Deny Access Profile]
Showing 2 of 1-3	records ► ► Show Configuration 导出 显示日志 关闭

请求详细信息	•
概要 输入	、 输出 警报
错误代码: 20	16
错误类别: Au	ithentication failure
错误消息: Ac	cess denied by policy
此请求的警报	
RADIUS Ap	plied 'Reject' profile

第3步:分析应用Reject Profile的原因,查看 请求详细信息的概要部分,检查服务、认证方法、认证源、授权源 是否正确,检查角色(此角色为ClearPass分配角色,并非无线控制器中的角色),[User Authenticated]角色表示用户账号密码校验成功,同时分配了 leader-role 角色。

请求详细信息							
概要 输入 输出	警报						
日期和时间:	Oct 10, 2019 15:06:15 CST						
终端主机标识符:	7C7A9146236E (Computer / Windows / Windows)						
用户名:	leader						
访问设备 IP/端口:	10.1.10.21:0						
系统安全状况状态:	UNKNOWN (100)						
	所用策略 -						
服务:	task3-portal-service						
认证方法:	PAP						
认证源:	Local:localhost						
授权源:	[Local User Repository]						
角色:	[User Authenticated], leader-role						
强制执行配置文件:	[Deny Access Profile]						
服务监视模式:	Disabled						
Online Status:	Not Available						
I ≤ Showing 2 of 1-3 records ► ► Show Configuration 导出 显示日志 关闭							

第4步: 在 配置 - > 服务 中检查对应的服务 task3-portal-service 里面 强制执行 的配置:

默认配置文件:

[Deny Access Profile] ,当下方条件无一匹配时会应用默认配置文件,在 配置 - > 强制执行 - > 服务 中查看 [Deny Access Profile] 的配置,该配置文件为系统自定义的RADIUS Reject配置文件;

规则评估算法:

- ✓ first-application,优先匹配规则,一旦有条件匹配以后,强制执行结束,不再校验后面的条件;
- ✓ evaluate-all,匹配所有规则,所有条件都会校验,所有匹配的条件后方的强制执行配置文件都会执行;

条件和强制执行配置文件:

(Tips:Role MATCHES_ALL guest-role [User Authenticated]) task3-portal-profile ,

- ✓ Tips:Role 表示ClearPass分配角色,
- ✓ MATCHES_ALL 表示匹配后面所有值,当ClearPass同时分配了 guest-role 和 [User Authenticated] 角色
 时,执行 task3-portal-profile 配置文件,

在 配置 - > 强制执行 - > 服务 中查看 task3-portal-profile 的配置,该配置文件为RADIUS Accept配置文件,同时发送Radius:Aruba属性Aruba-User-Role=lab1-guest,即给Aruba无线控制器下发User-Role(此role为无线控制器中的角色);

第二条通过用户名leader认证失败的记录中, ClearPass分配了 [User Authenticated] 和 lead-role 角色, 不匹配条件, 所以执行了默认配置文件 [Deny Access Profile] 策略。

✓	请检查通过用户名gu	est认证成功的认证记录中,ClearPass分配角色:	, 强制执行配置
	文件:	,用户在Aruba无线控制器获取的角色:	e a Hewlett Packard

更复杂的认证失败原因需要结合 请求详细信息 中的 输入 中的 RADIUS请求、计算属性、授权属性 ,以及 服务 中的 授权、角色、强制执行 等配置来综合分析。

如果Aruba无线控制器中用户获取的role与ClearPass下发的Aruba-User-Role不一致,需要检查Aruba-User-Role名称与Aruba无线控制器中定义的role名称是否一致,AOS6.x版本中role区分大小写,需要与Aruba-User-Role名称完全一致,AOS8.x版本中role不区分大小写。

配置 » 服务 » 编辑 - task3-portal-service 服务 - task3-portal-service 概要 服务 认证 角色 强制执行 ■ 使用从上一会话中缓存的角色和安全状况属性 使用缓存的结果: 强制执行策略: task3-portal-enfocement-policy Modify 强制执行策略详细信息 说明: 默认配置文件: [Deny Access Profile] 规则评估算法: first-applicable 强制执行配置文件 条件 (Tips:Role MATCHES_ALL guest-role 1. task3-portal-profile [User Authenticated]) 配置 » 强制执行 » 配置文件 » Edit Enforcement Profile - [Deny Access Profile] 强制执行配置文件 - [Deny Access Profile] 概要 配置文件 属性 配置文件: 名称: [Deny Access Profile] 说明: System-defined profile to deny network access 类型: RADIUS 操作: Reject 设备组列表: _ 属性: 类型 名称 配置 » 强制执行 » 配置文件 » Edit Enforcement Profile - task3-portal-profile

强制执行配置文件 - task3-portal-profile

概要	配置文件	属性		
配置文(#:			
名称:		task3-por	al-profile	
说明:				
类型:		RADIUS		
操作:		Accept		
设备组织	列表:	-		
属性:				
	类型		名称	值
1.	Radius:Arub	ba	Aruba-User-Role =	lab1-guest

10.3.3 通过事件查看器分析认证失败原因

- 第1步:通过远程桌面登录相应 LabX 的 Wireless Client (10.X.50.102,用户名: lab,密码: Aruba123!)将 无线网络连接到 labX-mac 后,重新连接到Portal认证无线网络 labX-portal,弹出Portal认证页面。
- 第2步:在ClearPass Policy Manager中,打开配置 -> 网络 -> 设备,在右边点击网络设备名称 LabX-MDs, 在弹出的 编辑设备详细信息 显示框中将 IP 或子网地址 修改为:10.1X.10.0/24,点 Save 按钮保存。

aruba							ClearPas	ss Policy Manager		
1000 - 10000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1		 配置 > 	> 网络 > 设备	ŕ						
🖸 监视		网络	设备							
🖧 配置		•								
—♀ 服务 □		A Net	work Access	s Device	(NAD) must belong to	the globa	I list of device	es in the ClearPass databas	e in order to connect to ClearPass.	
 方法		>+>#=					Go	Cloar Filtor		
二 源		过滤器	*(名称	夕称 .			÷ 60	TD就之网地址	送明	
□ ♀ 身份		#		古你▲ Lab1-MD	s			10.1.10.0/24	17.1H	
- Q Single Sign-On (SS - Q 本地用户	50)	显示量	最后项的前—-	后—	<u> </u>			10111010, 11		
- 🗘 端点			K/H-X+313	/1						
→ 静态主机列表										
■ 冊 安全状况										
🖃 🔹 强制执行										
→ 卆 策略 → - □ 澤 立 供										
- 🎝 设备										
- 🗘 设备组										
- Q 代理目标										
Profile and Network Sca	an									
─☆ 策略仿真										
编辑设备详细信息							0			
设备 SNMP 读取设	置 SNMP 写入设	置 CLI	【 设置 0	nConn	ect Enforcement	属性				
名称:	Lab1-MDs									
IP 或子网地址:	10.11.10.0/24		(例如,19	92.168.	1.10 或 192.168.1.1	/24)				
说明:										
			/.	2						
RADIUS 共享密钥:	•••••			认证:	•••••					
TACACS+ 共享密钥:	•••••			认证:	•••••					
供应商名称:	Aruba	•								
启用 RADIUS CoA:	☑ RADIUS CoA 端	□: 3799)							
Enable RadSec:										
					复制	Save	Cancel			

第3步:在第1步中弹出的Portal认证页面中输入 账号:guest-test,密码:aruba123 进行认证,认证失败,提示 Auth server timeout,在ClearPass访问跟踪器中过滤 Username 包含 guest-test 的认证记

录,提示 没有与指定过滤标准匹配的结果,说明访问跟踪器没有该认证记录,原因可能有两种:
一是ClearPass未收到认证请求;二是ClearPass收到认证请求,但是未处理,不处理的原因可能是因为NAS 设备不在网络设备列表中,或者共享密钥不一致。ClearPass收到不在网络设备列表中的NAS设备发起的 RADIUS请求,或者共享密码不一致,都会在监视 - > 事件查看器中记录,可以通过事件查看器确认。

监视 » Live Monitoring »	访问跟踪器					▲ 白动同族
访问跟踪器 Oct 11, 20	19 00:18:16 CST					♥ 日本川利利
			没有与指定过滤标准匹配的	告果		
The Access Tracker page	e provides a real-time display of per-	session access activity or	the selected server or doma	in.		
Tall Requests]	📑 Lab1-CPPM-	1 (10.1.50.41)		🔠 Last 1 day before Today		编辑
		_				
过滤器: Username	◆ 包含◆ guest-test	Go Clear Filter				显示 20 🗘 记录
# Server	Source	Username	Service	Login Status	Request Timestamp 🔹	Host MAC Address

- 第4步: 在ClearPass Policy Manager中, 打开 监视 > 事件查看器, 在右边可以看到4条 RADIUS ERROR 事件, 时间与通过guest-test账号认证的时间一致, 点开一条查看 系统事件详细信息, 查看 Description RADIUS authentication attempt from unknown NAD 10.X.10.11:41559, 提示收到未知 NAD 10.X.10.11的RADIUS认证请求, 于是定位到问题是该NAD未添加到网络设备列表, 前往网络设备中将IP或 子网地址还原。
- ✓ 请大家讨论事件查看器中为什么是4条RADIUS ERROR记录?

aruba				ClearPass	Policy Manager			Menu 🗮
	 监视 » 導 	件查看器						
1 监视	9 事件香	盲 器						
. Hive Monitoring	The Eve	nt Viewer provides n	enorts about system	level events All attempt	d upgrade patch and hotfix installation	is are longed here	进择服务器· lab1	CPPM-1 (10 1 50 41)
➡访问跟踪器	The Life	it frenci provideo i	epones about system	rever events. An accompt	a apgrade, pater, and notix instanced	is are rogged here.	2114/02/97/821 (2001	0111011(10:100:41)
─────────────────────────────	attabag.	10	* (mo *)	Go Cl	ar Filtor			局示 20 ♣ 记录
- OnGuard 活动	LI ASER.	28		40.94	*9	场.45	时间翻。	100 (100 - 100 K
■分析和證券	1	RADIUS		ERROR	Authentication	Linknown	Oct 10, 2019 23-58-24 CST	1
→ ■ 永玑监视 → ■ Profile and Network Scan	2	RADIUS		FRROR	Authentication	Unknown	Oct 10, 2019 23:58:19 CST	
→ ■ 审计查看器	3.	RADIUS		ERROR	Authentication	Unknown	Oct 10, 2019 23:58:14 CST	
事件查看器	4.	RADIUS		ERROR	Authentication	Unknown	Oct 10, 2019 23:58:09 CST	
■数据过滤器	5.	Policy Manager L	II	INFO	Logged in	None	Oct 10, 2019 21:28:48 CST	,
Blacklisted Users	6.	Policy Manager L	IL	INFO	Logged in	None	Oct 10, 2019 14:12:54 CST	
	7.	Admin UI		INFO	Export	Success	Oct 10, 2019 10:27:03 CST	
	8.	Admin UI		INFO	Backup	None	Oct 10, 2019 10:26:42 CST	
	9.	Policy Manager L	JI	INFO	Logged in	None	Oct 10, 2019 10:26:19 CST	
	10	Auto Classico		TNEO	Cuetom	None	0++ 10 2010 02-4E-12 CCT	
系统事件详细信息	D	DIUC				8		
Source	R/	ADIUS						
Level	EF	ROR						
Category	Αι	uthenticat	tion					
Action	Ur	nknown						
Timestamp	00	t 10, 20	19 23:58	:24 CST				
Description	RA NA	ADIUS au AD 10.1.1	thenticat	ion attemp 559	from unknown			
					Close			



第5步:在ClearPass Policy Manager中,打开配置 -> 网络 -> 设备,在右边点击网络设备名称 LabX-MDs, 在弹出的 编辑设备详细信息 显示框中将 RADIUS共享密钥 修改为:test123,点 Save 按钮保存。

编辑设备	详细信息							
设备	SNMP 读取设言	置 SNMP 写入设置	CLI 设置	OnConr	nect Enforcement	属性		
名称:		Lab1-MDs						
IP 或子网	网地址:	10.1.10.0/24	(例如,	192.168	.1.10 或 192.168.1.1	/24)		
说明:								
RADIUS	5 共享密钥:	•••••		认证:	•••••			
TACACS	6+ 共享密钥:	•••••		认证:	•••••			
供应商名	術:	Aruba	•					
启用 RA	DIUS CoA:	☞ RADIUS CoA 端口:	3799					
Enable	RadSec:							
					复制	Save		

第6步:在 Wireless Client 的Portal认证页面中输入 账号:guest-test,密码:aruba123 进行认证,认证失败, 提示 Auth server timeout,在ClearPass访问跟踪器中过滤 Username 包含 guest-test 的认证记录,提示 没有与指定过滤标准匹配的结果,说明访问跟踪器没有该认证记录。

监视 » Live Monitoring » 访	问跟踪器				
访问跟踪器 Oct 11, 2019	09:45:55 CST				
			没有与指定过滤标准匹配的	结果	
The Access Tracker page p	rovides a real-time display of p	per-session access activity on t	he selected server or doma	in.	
💎 [All Requests]	Lab1-CPI	PM-1 (10.1.50.41)		Last 1 day before Today	
过波器· Ilsername	▲ 句令▲ quast tast	Go Clear Filter			
# Server	Source	Username	Service	Login Status	Re

第7步: 在ClearPass Policy Manager中, 打开 监视 - > 事件查看器, 在右边可以看到4条 RADIUS ERROR 事件, 时间与通过guest-test账号认证的时间一致, 点开一条查看 系统事件详细信息, 查看 Description Failed to decode RADIUS packet - Received packet from 10.1.10.11 with invalid Message-Authenticator! (Shared secret may be incorrect.), 提示共享密钥可能不正确, 前往网络设备中将 RADIUS共享密钥还原。



监视 » 事件查看器			
事件查看器			
The Event Viewer provides repo	rts about system-level events. All attempted upgrade, patch, and hotfix installations a	re logged here.	选择服务器: Lab1-Ci
过滤器: 源 🗘	包含◆ Go Clear Filter		
# 源	级别	操作	时间戳 ▼
1. RADIUS	ERROR Authentication	Unknown	Oct 11, 2019 09:46:44 CST
2. RADIUS	ERROR Authentication	Unknown	Oct 11, 2019 09:46:34 CST
3. RADIUS	ERROR Authentication	Unknown	Oct 11, 2019 09:45:08 CST
4. RADIUS	ERROR Authentication	Unknown	Oct 11, 2019 09:44:58 CST
系统事件详细信息	0		
Source	RADIUS		
Level	ERROR		
Category	Authentication		
Action	Unknown		
Timestamp	Oct 11, 2019 09:46:44 CST		
Description	Failed to decode RADIUS packet - Received packet from 10.1.10.11 with invalid Message- Authenticator! (Shared secret may be incorrect.)		
	Close		

10.3.4 通过 ClearPass 抓包分析认证失败原因

第1步: 通过WebUI登录相应 LabX 的 MM (10.X.50.11,用户名: admin,密码: aruba123),打开 Managed Networks - > labX - > Configuration - > Authentication,在 All Servers 中点击 cppm, 在下方的 Server Options 中将 IP address / hostname 修改为 10.1X.50.41,点击 Submit 按钮提交,点 击右上角出现的 Pending Changes,在弹出的 Pending Changes 提示框中点击 Deploy changes,下发 配置到控制器。

ALDO MOBILITY MAST lab1-mm-1	ER	CONTROLLERS ⊘ 2 ① 0	ACCESS POINTS ○ 1 ○ 0	CLIENTS	ALERTS	
Managed Network > lab1 >						
 Mobility Master Mobility Master Managed Network (2) Iab1 (2) Iab1-md1 Iab1-md2 	Dashboard Configuration WLANS Roles & Policies Access Points AP Groups [Authentication Services Interfaces	Auth Servers Server Groups NAME default internal lab1-pesp.dot1, lab1-mac_svg +	AAA Profiles 1 5 5 1 1 3 5 9 9 1 1 1 1	L2 Authentication FAIL THROUG - - - -	L3 Authentication	User Rules Advanced
	Controllers System Tasks Maintenance	All Servers 2 NAME cppm Internal	TYPE RADIUS 	10 10	ADDRESS / HOSTNAME	SERVER GROUP lab1-peap_dot1_svg lab1-ma default internal



Auth Serv	AAA Profiles	L2 Authentication	L3 Authentication	User Rules	Advanced	
Server	Options					
	Name:	cppm				
	IP address / hostname:	10.11	0.41			
	Auth port:	1812				
	Acct port:	1813				
	Shared key:					
	Retype key:					
	Timeout:	5				
	Retransmits:	3				
	NAS ID:					
	NAS IP:					
	Enable IPv6:					
	NAS IPv6:					
	Use MD5:					
	Mode:					Cancel
 Managed Netw 	vork > lab1 >					Pending Changes 🗘
Pending Cl	hanges					
🗹 Pe	ending Changes for 2	Controllers				
	Managed Network	< > lab1 (2 Controllers	;)			
				ose Dis	card chang <u>es</u>	Deploy changes

第2步: 在ClearPass Policy Manager中,打开管理 - > 服务器管理器 - > 服务器配置,在右边点击服务器下方的 收集日志 按钮,在弹出的 收集日志 显示框中 勾选捕获网络数据包,取消其它日志的勾选,点 Start 开始抓包。

aruba		ClearPass Policy Manager Menu						
● 医転 ● 〇 互相 ● ○ E型 ● ● 日本印名S Portal ● 用分和収現 ● 用分和収現 ● 品分表型理想 ● 月分和収現 ● 品名記量	管理 > 服 服务器翻 Publishe	券器管理器 > 服务器配置 2置 ar服券器: Lab1-CPPM-1 [10.1.50.41]					 ② 设置日期和时间 ▼ 建改集群密码 ◎ 管理策略管理器区 ○ NetEvents 目标 マ Clear Machine A * Virtual IP Setting ◆ 生成 Subscriber * 集群级别的参数 	uthentication Cache 35
	# 1. 显示最后I	服务器名 ▲ Lab1-CPPM-1 页的前一-后一	管理端口 10.1.50.41	数据端口 -	⊠ default	Insight Enabled 【收集日志】 备份	集群同步 Enabled 恢复 Cleanup	上次同步时间 - 关闭 重新引导

收集日志
输出文件名(将添加 .tar.gz 扩展名)
收集以下日志
□ 系统日志
□ 所有策略管理器服务的日志
☑ 捕获网络数据包 转储持续时间: 60 secs.
□ 来自策略管理器服务的诊断转储
Back up ClearPass configuration data
Logs from Performance Metrics
□ 选择日期范围
截止到现在的天数 1
yyyy-mm-dd 格式的开始日期
yyyy-mm-dd 格式的截止日期
Advanced Options for Packet Capture
Start Cancel

- 第3步:在 Wireless Client 的Portal认证页面中输入 账号:guest-test,密码:aruba123 进行认证(注意:上 一步设置的抓包时间为60秒,所以要在60秒内完成认证),认证失败,提示 Auth server timeout。在 ClearPass的 收集日志 显示框中点 here 停止抓包,随后点击 Download File 下载抓包文件,解压后通过 Wireshark打开,过滤radius报文,可以确认ClearPass未收到radius报文,或者未收到本次认证的radius报 文,前往MM将Radius Server cppm 的IP address / hostname 还原为 10.X.50.41。
- ✓ 请大家讨论除了以上Radius Server中IP配置错误以外,还有什么情况会导致ClearPass收不到RADIUS认证 请求?

收集日志		8	◎
	正在构建日志转储		Collect logs complete
正在构建日志转储 INFO - Collecting log INFO - Collecting Pac INFO - Canturing net Click here to stop ca	is in the range 2019-10-10 cketCapture twork traffic for 60 seconds pturing network traffic	to 2019-10-11	正在构建日志转储 INFO - Collecting logs in the range 2019-10-10 to 2019-10-11 INFO - Collecting PacketCapture INFO - Capturing network traffic for 60 seconds INFO - Created Policy Manager log dump cppm-logs-2019-10-11-10-48-20.tar.gz INFO - The file can be accessed by logging into https://Lab1-C Collect logs complete
Download File		Close	Download File Close



11 TASK10: CLEARPASS 集群管理

11.1 用户需求

用户希望安装多台认证服务器,实现认证系统的冗余备份以及负载分担,避免单台认证系统宕机后导致全网无法 认证,同时多台认证服务器实现集中配置和管理,避免配置的不一致,并实现数据库的自动同步,避免每台单独 添加用户账号。

11.2 实现思路

- ✓ ClearPass支持Cluster集群架构,多台ClearPass可以实现统一管理和统一配置,多台之间数据库自动同步, 所有配置统一在Publisher节点上完成,自动同步到所有Subscriber节点。
- ✓ 本实验需要两组LabX来配合完成,请按照分配的搭档来配合完成,需要商量谁是Publisher谁是Subscriber

11.3 ClearPass Cluster 集群配置

11.3.1 开启 Cluster 集群

开启Cluster集群只需要在Subcriber节点配置,Publisher节点请跳过10.3.1章节,直接进入10.3.2章节。

以下步骤仅限于Subscriber节点:

第1步: WebUI登录作为Subscriber节点的ClearPass, 在ClearPass Policy Manager中, 打开 管理 - > 服务器 管理器 - > 服务器配置, 点击右上角的 生成 Subscriber 链接。

aruba			ClearPass P	olicy Manager				Menu 🗮
E ■ 面板 図 単現 永、記量 3 ● 管理	o ^{管理 »} ● 服务· ●	服务器管理器 » 服务器配置 器配置					设置日期和时间 更改集群密码 管理策略管理器区 NetEvents 目标	
	Publi	sher 服务器: Lab5-CPPM-1 [1	0.5.50.41]			8 8 9	Clear Machine A Virtual IP Settin 生成 Subscriber 集群级别的参数	gs
→ 本地共享文件夹 → 许可	#	服务器名 ▲ Lab5-CPPM-1	管理端口 10.5.50.41		⊠ default	Insight -	集群同步 Enabled	上次同步时间
 → ↓ 1 шчжуры → ↓ 2*# ◆ ↓ 2*# ◆ ▲ 代理和软件更新 ◆ ▲ Support 	显示最	后项的前一-后一				<u>收</u> 栗日志 备份 恢	E Cleanup	关闭重新引导

第2步: 在弹出的 添加 Subscriber 节点 对话框中输入如下内容:

- ✓ Publisher IP: 10.X.50.41 (作为Publisher节点的ClearPass IP)
- ✓ Publisher 密码: aruba123 (作为Publisher节点的ClearPass 的appadmin密码)
- ✓ 点 Save 按钮保存, ClearPass开始加入Cluster集群。



添加 Subscriber 节点		8
Publisher IP	10.1.50.41	
Publisher 密码	••••••	

🗌 在此操作之后恢复本地日志数据库 🗌 在此操作之前不备份现有数据库

WARNING:

- Configuration changes will be blocked on the publisher during initial cluster sync as part of this operation.
- 将删除此服务器上的所有应用程序许可证。请联系技术支持以添加和激活这些 许可证。



第3步:等待ClearPass加入Cluster集群完成后,会提示 Make subscriber complete,点 Close 按钮关闭窗口。

Make subscriber complete. Re-login after sometime INFO - 10.1.50.41: - Backup databases for AppPlatform INFO - 10.1.50.41: - Backup databases for PolicyManager INFO - 10.1.50.41: - Backup extensions
INFO - 10.1.50.41: - Backup databases for AppPlatform INFO - 10.1.50.41: - Backup databases for PolicyManager INFO - 10.1.50.41: - Backup extensions
INFO - Config database lock released INFO - Subscriber now replicating from publisher 10.1.50.41 INFO - Retaining local node certificate INFO - Subscriber replication and node setup complete INFO - Notify publisher that adding subscriber is complete INFO - Subscriber added successfully INFO - Restarting Policy Manager admin server Make subscriber complete. Re-login after sometime Close

第4步: 等待一会时间后,重新登录作为Subscriber节点的ClearPass WebUI,看到提示 只有有限访问权限;如 需完整访问权限,请登录策略管理器发布程序,表示该ClearPass服务器是Subscriber,完整访问权限需要 登录Publisher。



ClearPass Policy Manager 只有有限访问权限;如需完整访问权限,请登录策略管理器发布程序

Admin Login					
用户名:	admin				
密码:	•••••				
登录					

11.3.2 添加 Virtual IP

ClearPass要实现认证的冗余备份,除了建立Cluster集群架构外,还需要配置Virtual IP (VRRP),前提是配置 Virtual IP的多台ClearPass需要在一个子网网段,本实验采用的Lab中ClearPass都位于不同的子网网段,所以无 法配置Virtual IP,以下步骤作为在实际部署环境中配置Virtual IP的参考。

第1步: 登录Publisher, 在ClearPass Policy Manager中, 打开 管理 - > 服务器管理器 - > 服务器配置, 点击 右上角的 Virtual IP Settings 链接, 在弹出的 Virtual IP Settings 对话框中输入以下内容:

- ✓ Virtual IP: 10.X.50.40
- ✓ Virtual Host ID: 1 (VRRP ID, 不要与子网中其他VRRP ID冲突)
- ✓ Primary Node: LabX-CPPM-1 (选择Publisher节点)
 - Interface: 10.X.50.41 [MGMT] (选择管理口)
- ✓ Secondary Node: LabX-CPPM-1 (选择Subscriber节点)
 - Interface: 10.X.50.41 [MGMT] (选择管理口)

点 Save 按钮保存。

由于本实验Lab中两台ClearPass不在一个子网网段,所以Virtual IP无法配置成功,提示 Primary and Secondary nodes must be in same subnet。

aruba		ClearPa	iss Policy Mana	iger			Menu 🗮
こ 見 面板	 管理 » 服务器管理器 » 朋 	3 务器配置					
	0 服务界积器					④ 设置日期	和时间
	加劳奋的里					🚏 更改集群	摔密码
						📴 管理策略	Y管理器区
↓ 管理	•					NetEve	nts 目标
- JearPass Portal					1	* Virtual	IP Settings
						*** 集群级别	山的参数
- ■ 服务器管理器	Publisher 服务器: Lab	1-CPPM-1 [10.1.50.41]					
	# 服务器名▲	管理端口	数据端口	X	Insight	集群同步	上次同步时间
	1 Lab1-CPPN	1-1 10.1.50.41	1 -	default	-	Enabled	-
一 本地共享文件关 一 净 许可	2 ClabE-CPPA	1 10.5.50.41	1 -	default		Enabled	Oct 11 2010 15:09:22 CET
□	Z. CLabs-CPP	1-1 10.5.50.4	-	delault	-	Enabled	000 11, 2019 15:08:55 CS1
— A SNMP trap接收方	显示最后项的前一-后一			收集日志备份	恢复 Cleanup	关闭	重新引导 删除 Subscriber
→ Syslog 目标							
Virtual IP Settings				•			
Configure Virtual IPs for ClearPass High	Availability						
Virtual IP	Primary Node	Secondary I	Node	Status			
	No Virtual IP has bee	n configured					
Virtual IP Details -							
Select IP version:	o IPv4 ○ IPv6						
Virtual IP: 1	0.1.50.40						
Virtual Host ID: 1	(1-255)						
Derimony Nodes	Node		Subn	et			
Primary Node:	Labi-CPPM-1 C	10.1.50.41 [MGM1] \$	255.255.255.0				
Secondary Node:	Lab5-CPPM-1 C	10.5.50.41 [MGM1] \$	255.255.255.0				
Enabled:	<i>.</i>						
			Reset Delete Sa	Close			
Virtual IP Settings				•			
Configure Virtual IPs for ClearPass High	Availability						
Virtual IP	Primary Node	Secondary I	Node	Status			
	No Virtual IP has bee	n configured					
	Primary and Secondary	nodes must be in same subnet					
Virtual IP Details -							
Select IP version:	o IPv4 ○ IPv6						
Virtual IP: 1	0.1.50.40						
Virtual Host ID: 1	(1-255)						
Primary Made	Node	Interface	Subr	et			
Primary Node:	Lab1-CPPM-1 \$	10.1.50.41 [MGMT] \$	255.255.255.0				
Secondary Node:	Lab5-CPPM-1 \$	10.5.50.41 [MGMT] \$	255.255.255.0				
Enabled:							
			Reset Delete Sa	Close			

第2步:当Virtual IP配置成功后,需要在MM中将认证Radius Server的IP改为上一步配置的Virtual IP。本实验忽略此步骤。

11.4 验证结果

11.4.1 检查 ClearPass 集群状态

第1步: 分别登录Publisher和Subscriber, 在ClearPass Policy Manager的 面板 中的 集群状态 下都可以看到两 台ClearPass, 一个是Publisher, 一个是Subscriber, 状态都是OK。

aruba		ClearPass	Policy Manager			Menu 📃
	-					Default
● 警报 最近的警报	集群状态					٥
所有请求 所有策略管理器请求的趋势	状态 の	主机名 Lab1-CPPM-1 (10.1.50.41)	Zone default	服务器角色 Publisher Subscriber	Last Replication	OK
◎ 应用程序 启动其他 ClearPass 应用程序		Laus-CFFFF1 (10.3.30.41)	deradic	Subscriber	04(11, 2019 13:30:32 (3)	ŬK.
發展 10 10 10 10 10 10 10 10 10 10 10 10 10	System CPU Utiliz	tion	● Re	equest Processing Time		•
3. 集群状态 当项 监测整个集群的状态	100					
♀ 设备类别	50 50	•			No Activity	
♀ 设备系列	.	13:25 13:30 13:35 13:40	13:45			
Endpoint Profiler Summary Endpoint profiling details		Time (mins)			Policy Manager	
会 失败验证 跟踪最近失败的验证					, only Munugur	

第2步: 分别登录Publisher和Subscriber, 在ClearPass Policy Manager中, 打开管理 - > 服务器管理器 - > 许可,确认License许可数量是否合并,检查服务器平台License以及应用程序License是否都是激活状态。 (本实验Lab中安装的ClearPass为Demo版本,不必确认License数量是否合并)

aruba			ClearPass Policy Manager Menu 🚍						
計 面板 ☑ 监視 《 配置 》管理		● 管理 ● 许可 ● 7700	L > 服务器管理器 > 许可 可	s artivated for the ClearPass cluste	r A ClearPass Platform license i	s required for every r	product instance.	◆ 添加许可证	
-	Portal 章 配置	许集群	可证概要 服务器 应用程序						
 ク日志記 ク本地共 グド回 分部服务器 クSNMP 	置 享文件夹 trap提收方		许可证类型 1 Onboard 2 OnGuard 3 Access	総 10 10 10	0 0 0	已用计数 0 0 0		史新子 2019/10/11 13:45:05 2019/10/11 13:45:05 2019/10/11 13:45:05	
许可证概	要 服务器 应用程序		产品	许可证 类刑	持续时间		激活状态	添加的许可证已自用	
1 2	10.1.50.41 10.5.50.41		ClearPass Platf ClearPass Platf	orm Permanent orm Permanent	- - 103401[0]		Activated Activated	Mar 14, 2019 21:25:31 CST Mar 14, 2019 21:38:51 CST	

许可证	概要 服务器 应用程序					
#	产品	许可证类型	端点数	持续时间	激活状态	添加的许可证已启用
1	OnGuard	Permanent	100	-	Activated	Mar 14, 2019 21:27:07 CST
2	Onboard	Permanent	100	-	Activated	Mar 14, 2019 21:26:42 CST
3	Access	Permanent	100	-	Activated	Mar 14, 2019 21:26:04 CST

11.4.2 检查配置同步

通过在publisher上添加一个账号,在subscribe节点上查看配置是否同步。

第1步: 登录Publisher, 在ClearPass Policy Manager中, 打开 配置 - > 身份 - > 角色, 点击右上角的 添加角色 链接, 在弹出的 添加新角色 对话框中输入 名称: testcluster, 点 Save 按钮保存。

aruba		ClearPass Policy Manager					
■■面板	配置 »	身份 >	▶ 角色				
₩ 监视	角色				🚽 添加角色		
- 🌣 此处开始	Roles exist independently of an individual service and can be accessed globally through the role-mapping policy of any service.						
——————————————————————————————————————							
□- ♀ 认证	过滤器	: 名称	\$ (包含 \$)	🕂 Go Clear Filter	显示 20 🛟 记录		
一, 万法	#		名称 ▲	说明			
□ 身份	1.		[AirGroup v1]	Role for an AirGroup protocol version 1 request			
— Single Sign-On (SSO)	2.		[AirGroup v2]	Role for an AirGroup protocol version 2 request			
	3.		[Aruba TACACS read-only Admin]	Default role for read-only access to Aruba device			
	4.		[Aruba TACACS root Admin]	Default role for root access to Aruba device			
一 印 静态主机列表	5.		[BYOD Operator]	Operators with this profile can view and manage their own provisioned	devices		
☆ 角色映射	6.		[Contractor]	Default role for a contractor			
	7.		[Device Registration]	Operators with this profile can self-provision their devices, for use with and AirGroup sharing.	MAC authentication		
□ 著 强制执行	8.		[Employee]	Default role for an employee			
→ ^東 □ □ □ 配置文件	9.		[Guest]	Default role for a Guest			
添加新角色				•			

名称:	testcluster
说明:	
	Save

第2步:打开 配置 - > 身份 - > 本地用户,点击右上角的 添加用户 链接,在弹出的 添加本地用户 对话框中输入 以下内容:

- ✓ 用户ID: publisheruser
- ✓ 名称: publisheruser
- ✓ 密码: aruba123
- ✓ 认证密码: aruba123
- ✓ 角色: testcluster

点 添加 按钮。



a Hewlett Packard Enterprise company

■ 正 ● 日本 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	aruba		ClearPass Policy Mar	nager	Menu 🗮
● 方法 ● 方法 ● 方法 ● 日户 10 • 包含 ● Clear Filter 日元 20 • 0 ● 日戸 10 • 包含 ● Clear Filter 日元 20 • 0 ● 本語戸 ● ○ 角合 ○ ○ 角合を発射 ● 日戸 10 • 0 名称 角色 久古 ● ○ 角合を発射 ● 加加本地用户 ● 「日戸 10: publisheruser ● ● ○ 角合を発射 ● ● ● ● ○ 自然を見対し、 ● ● ● ● ○ 自然を見対し、 ● ● ● ● ● ● ● ● ● ● ● <td> ■ 面板 ■ 监視 ● 配置 ● 心此处开始 - 心 肌务 </td> <td> 配置»身份»本地用户 本地用户 ClearPass Policy Manager lists all </td> <td>l local users in the Local Users page.</td> <td></td> <td> → 添加用户 ▲ 导入用户 ▲ 导出用户 ▲ 导出用户 ☆ Account Settings </td>	 ■ 面板 ■ 监視 ● 配置 ● 心此处开始 - 心 肌务 	 配置»身份»本地用户 本地用户 ClearPass Policy Manager lists all 	l local users in the Local Users page.		 → 添加用户 ▲ 导入用户 ▲ 导出用户 ▲ 导出用户 ☆ Account Settings
資稅色 資稅色 済加支地用户 第加支地用户 日户 ID: publisheruser 名称: publisheruser 密码: ····································	 → 认证 ☆ 方法 ☆ 源 ● 身份 → Single Sign-On (SSO) → ⁵ 本地用户 → ⁵ 端点 → 静态主机列表 	过滤器: 用户 ID ▲	◆〔包含 ◆〕 名称	● Go Clear Filter 角色	显示 20 t) 记录 状态 导出 删除
山山 山山 认证密码: ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	○角色 ●角色映射 添加本地用户 用户 ID: 名称: 変品・	publisheruser publisheruser		•	
启用用户: ☑ (选中可启用本地用户) 更改密码: (Check to force change password on next TACACS+ login) 角色:	出吗. 认证密码:				
更改密码: (Check to force change password on next TACACS+ login) 角色: testcluster + 属性 值 1. Click to add	启用用户:	🛛 (选中可启用本地用户)			
属性 属性 1. Click to add	更改密码: 角色:	 (Check to force change pass testcluster 	sword on next TACACS+ login)		
	属性 1. Click to add	属性			

第3步: 登录Subscriber, 在ClearPass Policy Manager中, 打开 配置 - > 身份 - > 角色, 在右边的过滤器中输入: 名称 包含 testcluster, 点 Go 按钮进行过滤,可以看到Subscriber上自动创建了testcluster角色。 打开 配置 - > 身份 - > 本地用户, 在右边可以看到Subscriber上也自动创建了publisheruser用户。

aruba	ClearPass Policy Manager 只有有限访问权限;如需完整访问权限,请登录策略管理器发布程序	Menu 🗮
■ 面板 ○ 図 監視 ○ 20 配置 ○ - ☆ 此处开始	配置 » 身份 » 角色 角色 Roles exist independently of an individual service and can be accessed globally through the role-mapping policy of any service.	- ᡎ 添加角色 - ▲ 导入角色 - ▲ 导出角色
→ 御 以证 ● 量 以证 ■ 量 身份 ▲ Single Sign-On (SSO)	过滤器: 名称 ◆ 包含 ◆ testcluster ● Go Clear Filter # ● 名称 ▲ 说明	显示 20 记录
→ 本地用户 → 端点 → 静态主机列表 → <u>角色</u> → 角色映射	显示最后项的前一-后一	創體
		aruba

aruba	Clear _{只有有限访问权限}	Pass Policy Manager 建: 如需完整访问权限,请登录策略管理器发布	程序	Menu
■面板	配置 » 身份 » 本地用户			
医 监视 0	本地用户			🚽 添加用户
<mark>்</mark> 能置 ○				▲ 导八用尸
一〇 此处开始				📴 Account Settings
——————————————————————————————————————	ClearPass Policy Manager lists all local use	rs in the Local Users page.		
∃- ♣ 认证				
□- 👤 身份	过滤器: 用户 ID 🔶 包含	•	Go Clear Filter	显示 20 ᅌ 记录
Single Sign-On (SSO)	# ■ 用户 ID ▲	名称	角色	状态
—↓ 本地用厂 —↓ 端点	1. Dublisheruser	publisheruser	testcluster	Enabled
→ 静态主机列表	显示最后项的前一-后一			导出删除
——————————————————————————————————————				

第4步: 分别登录Publisher和Subscriber, 在ClearPass Policy Manager中, 打开 监视 - > 审计查看器, 在右 边可以看到都有创建了testcluster Role和publisheruser Local User的事件记录。

aruba		ClearPass Policy Manager 只有有限访问权限;如開完整访问权限,请登录策略管理器发布程序						
■■面板	监视 »	审计查看器	l P					
🗾 监视 💿	审计	审计查看器						
 Live Monitoring 参访问跟踪器 	The Au	udit Viewei	r provides a dynamic	report on actions, device name, cat	tegory of ClearPass component, user,	and timestamp.		
— Je 计费 □ Imp Guard 活动	过滤器	: 操作	\$	包含 🗧	Go Clear Filter	显示 20 ᅌ 记录		
→ OffGuard Ab) → Aff和趋势	#	操作	名称	类别	用户	时间戳 ▼		
▲ 系统监视	1.	ADD	publisheruser	Local User	admin	Oct 11, 2019 14:24:52 CST		
Hereit Profile and Network Scan □	2.	ADD	testcluster	Role	admin	Oct 11, 2019 14:22:13 CST		
—— 🥜 事件查看器 —— 🖉 数据过滤器	显示最	后项的前一一	-后一					

12 附录

12.1 Task1 实现思路

✓ ClearPass如何处理一个radius认证请求

答案:

	认证过程	描述	
1	RADIUS 认证请求	网络访问服务器(NAS)将RADIUS访问请求发送到ClearPass,然后评估请求并识 别RADIUS连接属性。	
2	服务匹配	ClearPass根据标识的RADIUS连接属性,该请求将被匹配到ClearPass不同的服务。	
3	认证方法	ClearPass尝试使用预定义的认证方法(按优先级顺序)对用户进行身份验证	
4	认证源	与用户协商身份验证方法后,ClearPass根据预定义的身份认证源(按优先级顺序) 对用户进行身份验证	
5	角色映射 (可选)	在角色映射策略中定义ClearPass的角色,基于多种信息源,包括RADIUS连接属性,身份验证源或授权属性。	
6	强制执行策略	强制执行策略是根据ClearPass定义的规则(包括Radius连接属性、身份认证源或者 授权属性)将强制执行配置文件应用到认证请求。	
7	强制执行配置文件	强制配置文件是控制网络访问的基础(给NAS设备返回具体的Radius的属性)。一个强制执行策略可以调用多个强制执行配置文件。	

- ✓ 你需要了解的几个问题:
 - MM1的IP地址: 10.X.50.11
 - CPPM的IP地址: 10.X.50.41
 - Radius共享密码: aruba123
 - MD测试radius命令是什么: aaa test-server pap <radius-server> <username> <password>

12.2 Task2 实现思路

✓ MAC认证时,我们并没有手动输入用户名和密码,那他的用户名和密码是什么?

答案: 用户名和密码都是终端的MAC地址

✓ ClearPass如何匹配一个MAC认证请求:

答案: 通过"服务规则"匹配Radius认证请求报文的用户名和终端的MAC地址是否相同来区分;或者在控制器 上针对mac认证的radius server配置一个特定的nas-id,通过"服务规则"匹配nas-id来区分。

✓ ClearPass可以用哪个认证源来做MAC认证

答案: "本地用户"、"端点"、"静态主机列表"、"第三方认证源"

12.3 Task3 实现思路

✓ MAC认证时,我们并没有手动输入用户名和密码,那他的用户名和密码是什么?

答案: 用户名和密码都是终端的MAC地址

✓ ClearPass如何匹配一个MAC认证请求:

答案: 通过"服务规则"匹配Radius认证请求报文的用户名和终端的MAC地址是否相同来区分;或者在控制器 上针对mac认证的radius server配置一个特定的nas-id,通过"服务规则"匹配nas-id来区分。

✓ ClearPass可以用哪个认证源来做MAC认证

答案: "本地用户"、"端点"、"静态主机列表"、"第三方认证源"

12.4 Task4 实现思路

✓ 首先我们需要思考下,在当前的无线网络接入认证方式中,哪一种是最安全的接入认证方式?

答案: 802.1x认证 (EAP-PEAP)

是否应用802.1x或者选择哪一种EAP验证类型,取决于公司所需的安全级别和所需的额外管理功能,大家可以去参考各种EAP类型的功能和说明,这里不再详细介绍,本次我们会采用最常用的、最灵活部署的EAP-PEAP类型(不需要证书)。

✓ 针对该认证方式,我们需要思考下还需要为无线网络新增什么网元,即需要针对无线网络来设计什么样的认证服务器呢?

答案: RADIUS 服务器

通常对RADIUS协议的服务端口号是 UDP 1812/1813 或者是1645/1646

RADIUS

Combines authentication & authorization.

Encrypts only the password.

Requires each network device to contain authorization configuration.

No command logging.

Minimal vendor support for authorization.

UDP- Connectionless

UDP ports 1645/1646, 1812/1813

Designed for subscriber AAA

有三个网元部分:

- 1. 请求者(用户)-运行的1x认证软件的无线客户端
- 2. 验证者(NAS)-Wi-Fi 接入点和无线控制器,作为 NAS 设备
- 3. 验证服务器-一个验证数据库,通常是一个 RADIUS 服务器

✓ 针对该认证服务器,我们需要思考下,你对该认证方式的完整流程熟悉吗?

答案: 802.1x的认证流程





✓ 针对802.1x认证的用户,我们设计两种类型的用户,例如领导和普通员工,利用Radius的授权功能,返回什 么样属性给到控制器,从而实现不同的访问权限?

<u>答案:返回aruba-user-role属性给到控制器,我们设计两种role, 一个是leader-role,一个是</u> employee-role

12.5 Task5 实现思路

✓ ClearPass针同一个SSID既有MAC认证,又有Portal认证,如何匹配到一个正确的认证请求:

<u>答案:通过"服务规则"匹配认证的用户名和终端的 MAC 地址是否相同来区分,相同是 MAC 认证;不相同</u> 则是 Portal 认证。

✓ ClearPass上有两条MAC认证服务,如何匹配到一个正确的认证请求:

答案: 通过"服务规则"匹配认证的用户名和终端的MAC地址是否相同来区分是否是MAC认证;通过匹配认证 请求的radius属性Aruba-Essid-Name来区分不同的SSID送上来的认证请求。

12.6 Task6 实现思路

✓ 首先我们需要思考下,访客的自注册应该采用哪种认证方式

答案: Portal认证 (也可以结合mac caching)

是否应用mac caching,需要结合用的实际需求,因为Portal认证的用户存在超时下线的情况,即如果有一段时间没有网络通讯的话,该终端会被无线系统自动超时下线,默认是5分钟。通常我们会强烈建议使用该功能,保证访客在账号的有效期内,都会自动关联无线网络并获得访客访问权限,而无需重复地进行Portal认证。

✓ 针对该认证方式,我们需要思考下还需要为无线网络新增什么网元,即需要针对无线网络来设计什么样的认证服务器呢?

答案: Portal页面服务器和RADIUS服务器 (通常两者可以合二为一)

有三个网元部分:

- 1. 验证者(NAS)-Wi-Fi 接入点和无线控制器,作为 NAS 设备
- 2. Portal 页面服务器,即提供 web 页面服务,用于页面的登录和自注册使用
- 3. 验证服务器-一个验证数据库,通常是一个 RADIUS 服务器
- ✓ 针对访客自注册认证,我们需要思考下,你对该认证方式的完整流程熟悉吗?

答案:具有访客自注册的Portal认证流程



12.7 Task7 实现思路

✓ 首先我们需要思考下,在当前的管理员集中认证机制中,哪一种是最常用的认证方式?

答案: TACACS+认证

RADIUS结合了身份验证和授权。RADIUS 服务器向客户端发送的访问接受数据包中包含授权信息。这样就 很难分离身份验证和授权。TACACS+使用分离 AAA 的 AAA 体系结构。这就使独立的身份验证解决方案仍 然可使用 TACACS+ 进行授权和记帐。例如,使用 TACACS+,就可以使用 Kerberos 身份验证 和 TACACS+授权和记帐。NAS 在 Kerberos 服务器上经过身份验证后,它可以从 TACACS+ 服务器请求授 权信息,而不必重新验证身份。NAS会通知 TACACS+ 服务器,它已经在 Kerberos 服务器上成功通过身份 验证,然后服务器就会提供授权信息。

会话期间,如果需要进行额外的授权检查,则接入服务器会与 TACACS+服务器进行核对,确定是否授予了 用户使用特定命令的权限。这样可以更好地控制用户能够在接入服务器上执行的命令,同时将授权机制与身 份验证机制分离。

✓ 针对该认证方式,我们需要思考下还需要为无线网络新增什么网元,即需要针对无线网络来设计什么样的认证服务器呢?

答案: TACACS+认证服务器 (ClearPass默认内置就支持)



用户 Login 登录 NAS(T/

NAS (TACACS Client)

TACACS 服务器

通常对TACACS协议的服务端口号是TCP 49

TACACS+		
Separates all 3 elements of AAA, making it more flexible.		
Encrypts the username and password.		
Central management for authorization configuration.		
Full command logging.		
Supported by most major vendors.		
TCP- Connection oriented TCP port 49		
Designed for administrator AAA		

有三个网元部分:

- 1. 请求者(用户)-运行的 SSH/Telnet 远程控制的无线客户端
- 2. 验证者(NAS)-Wi-Fi 接入点和无线控制器,作为 NAS 设备
- 3. 验证服务器-一个验证数据库,通常是一个 TACACS+服务器

✓ 针对该认证服务器,我们需要思考下,你对该认证方式的完整流程熟悉吗?

答案: TACACS+的认证流程





✓ 针对TACACS认证的用户,我们设计两种类型的用户,例如根管理员和只读管理员,利用TACACS的授权功能,返回什么样属性给到控制器,从而实现不同的管理员访问权限?

答案: 返回aruba-admin-role属性给到控制器,我们设计两种role,一个是read-only(只读权限),一个是 root(根权限)