Aruba Hand-On Lab Guider

ClearPass - Basic Configuration

2019.10.28

V 1.2

Jihu Sun

Zhengxin Yang

Jinghao Ma

目录

1 LAB 拓扑环境和设备登录信息

1.1 Lab 内容简介

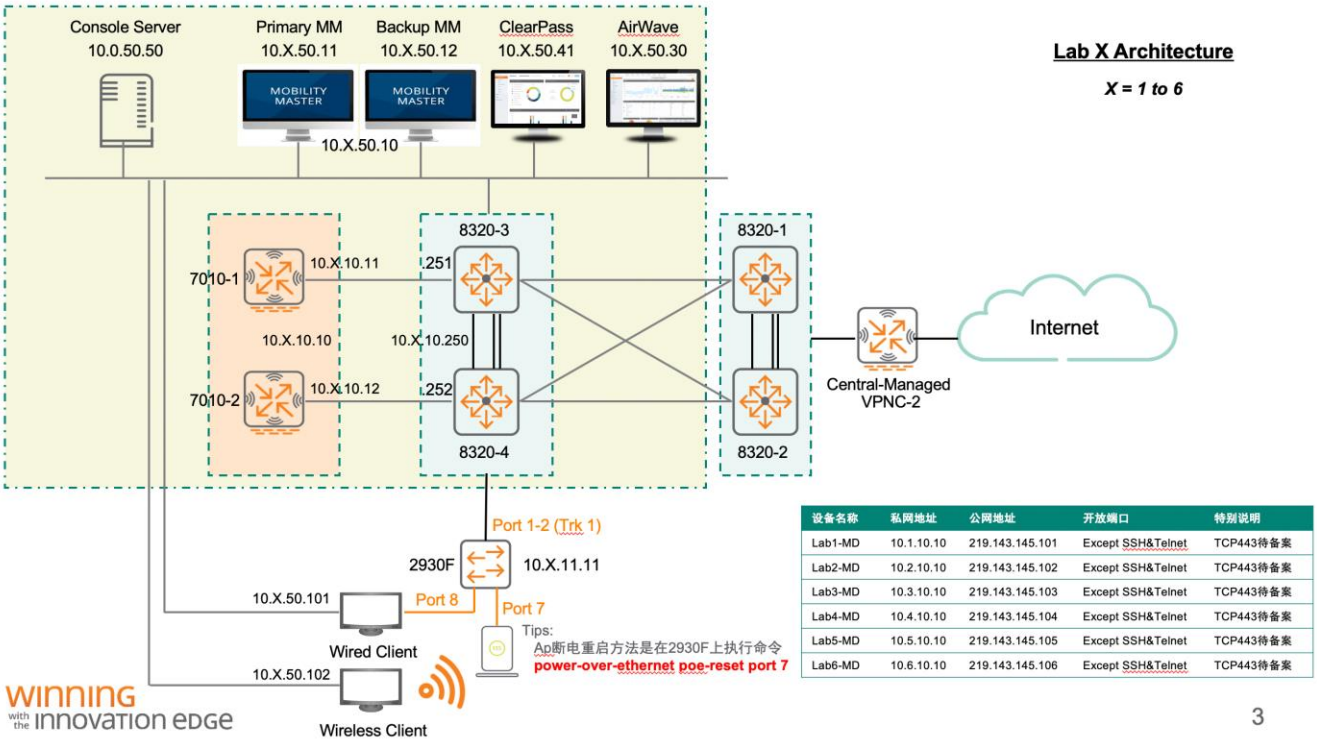
本次lab所有内容为远程操作，涉及配置Aruba MM、Controller、ClearPass产品，给初步接触Aruba ClearPass产品的SE熟悉ClearPass工作流程和基本操作。本次lab内容包括：创建一个简单的认证服务、Aruba控制器集成ClearPass实现Mac认证、Portal认证、802.1X认证、Mac + Portal无感知认证、访客自注册认证、Tacacs+认证、ClearPass Insight操作、ClearPass认证基本问题诊断以及ClearPass集群操作。

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）



设备名称	私网地址	公网地址	开放端口	特别说明
Lab1-MD	10.1.10.10	219.143.145.101	Except SSH&Telnet	TCP443待备案
Lab2-MD	10.2.10.10	219.143.145.102	Except SSH&Telnet	TCP443待备案
Lab3-MD	10.3.10.10	219.143.145.103	Except SSH&Telnet	TCP443待备案
Lab4-MD	10.4.10.10	219.143.145.104	Except SSH&Telnet	TCP443待备案
Lab5-MD	10.5.10.10	219.143.145.105	Except SSH&Telnet	TCP443待备案
Lab6-MD	10.6.10.10	219.143.145.106	Except SSH&Telnet	TCP443待备案

3

1.3 Lab 设备 VLAN 和 IP 信息

设备信息				
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	

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
ClearPass	https	10.X.50.41	admin	aruba123
	ssh		appadmin	aruba123
AirWave	https	10.X.50.30	admin	admin
	ssh		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

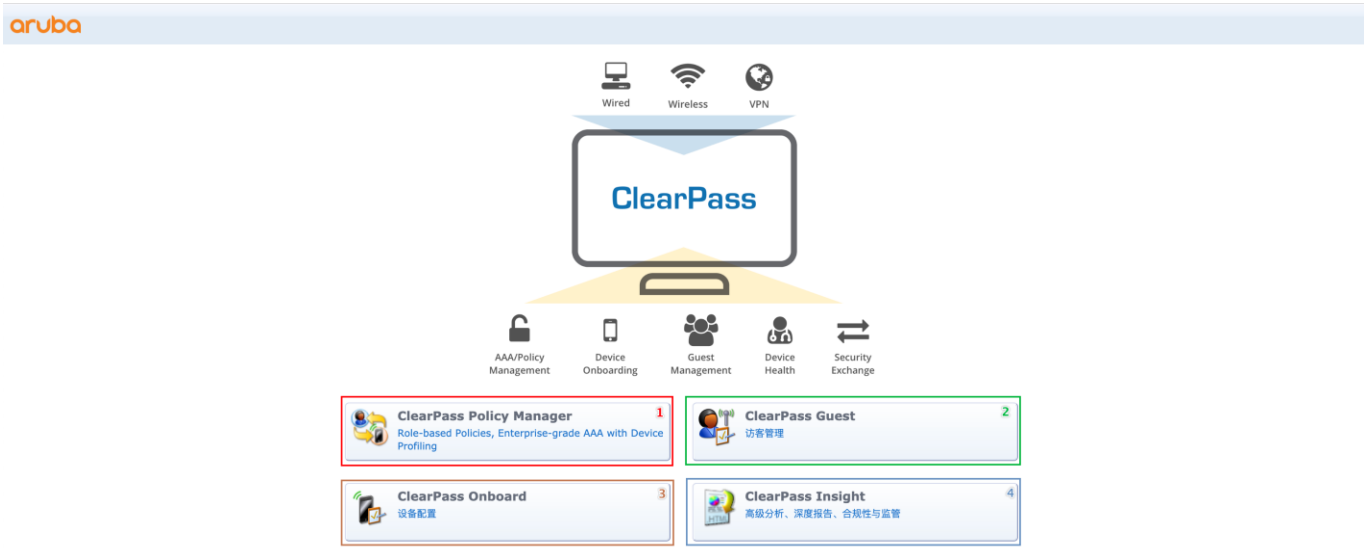
- 配置无线控制器：
  - 初始化MD1和MD2
  - 配置Cluster
  - 配置Radius服务器指向CPPM（10.X.50.41）
- 配置ClearPass：配置一条认证服务用于aaa test

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



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”

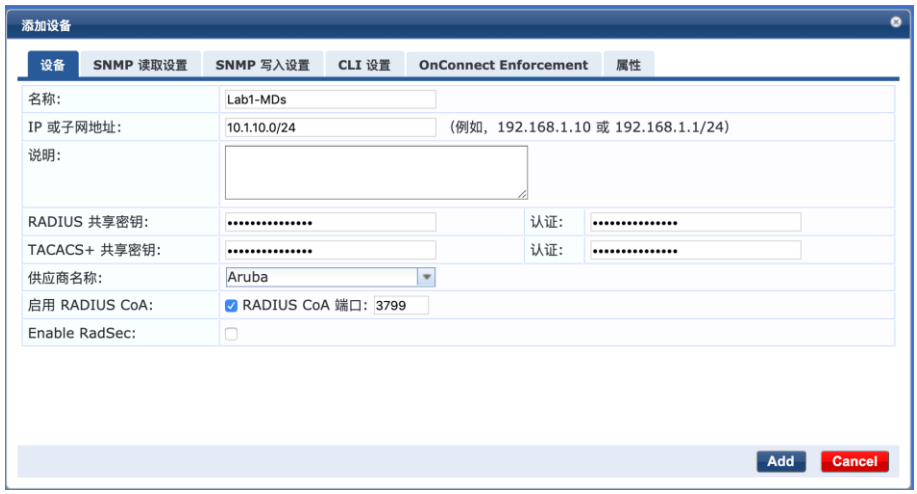
- ✓ 用户名：admin
- ✓ 密码：aruba

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：

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



2.3.3 添加服务器参数

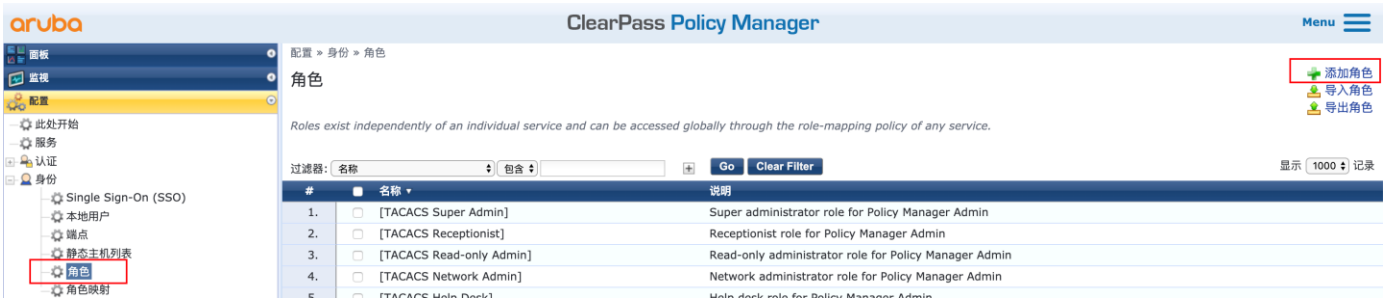
第1步：找到 管理 - > 服务器管理器 - > 服务器配置，点击右侧 服务器“LabX-CPPM-1” （X：1…6）

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“

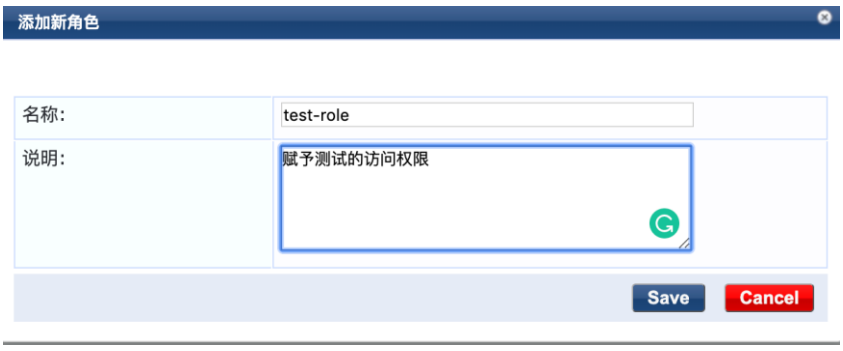
2.3.4 添加本地账号和角色

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：

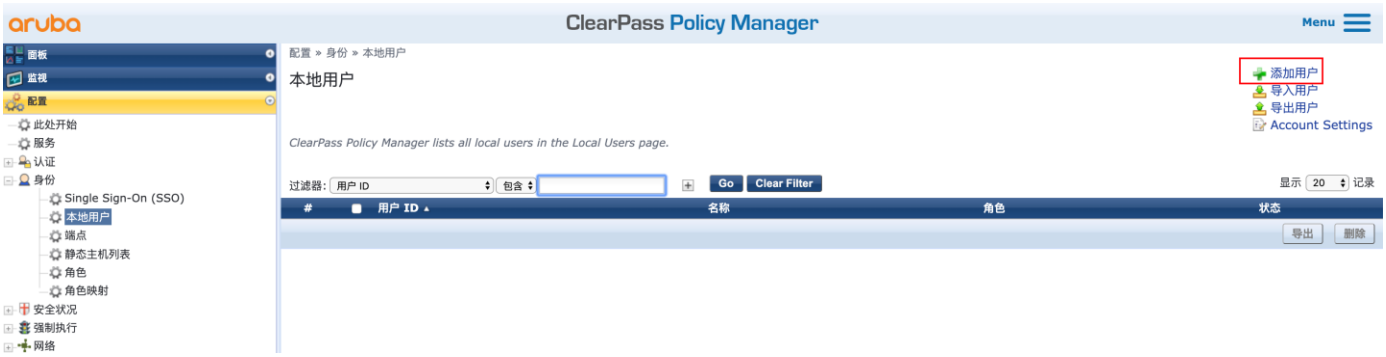


在弹出的添加角色窗口中输入下面参数，点击“save”：

- ✓ 名称：test-role
- ✓ 说明：赋予测试的访问权限



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

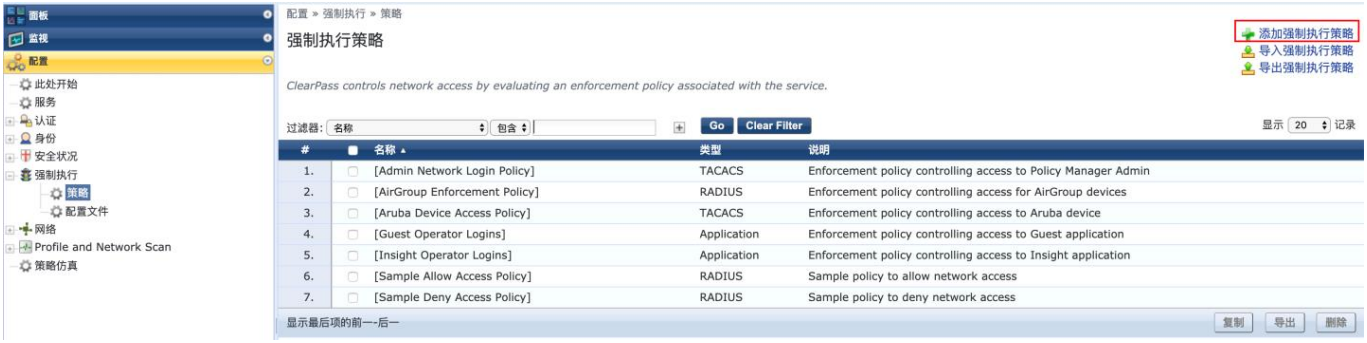


在弹出的添加角色窗口中输入下面参数，点击“save”：

- ✓ 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）

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：



在“服务”选项卡中配置如下参数：

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

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]

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

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”

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

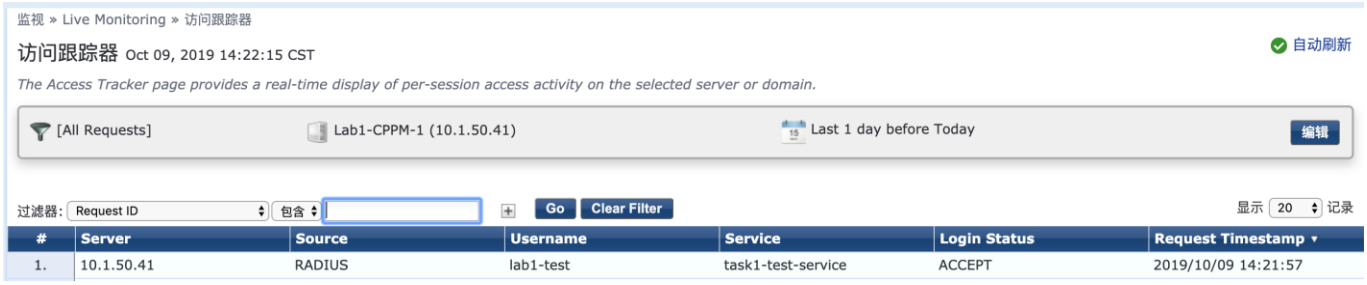
```
(Lab1-MM-1) ^[mm] (config) #write memory
Saving Configuration...
Configuration Saved.
```

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：



NOTE

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

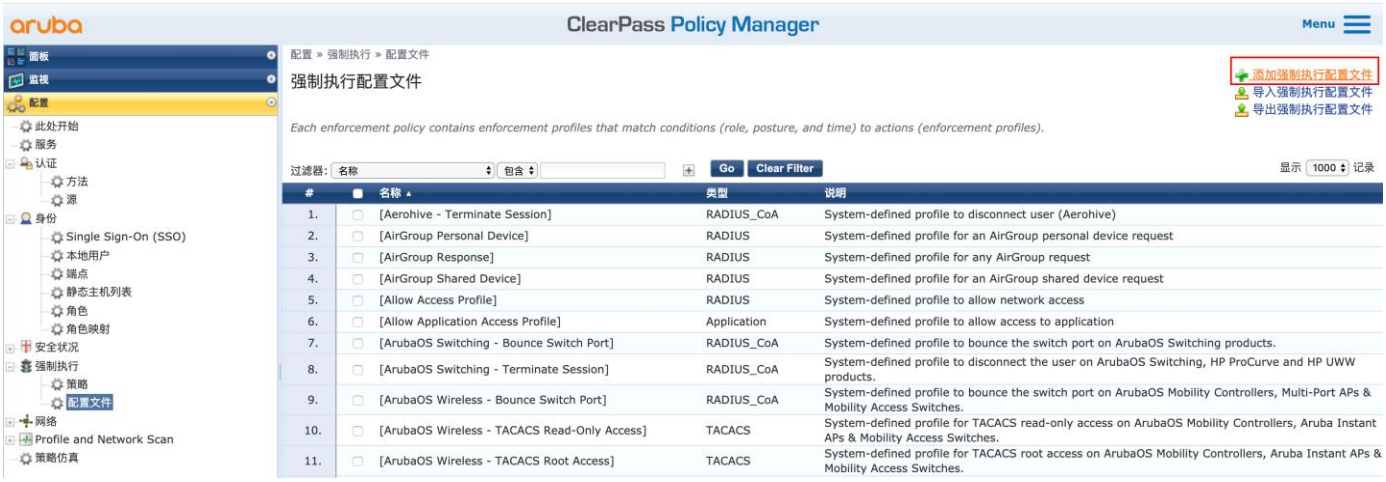
在弹出的添加角色窗口中输入下面参数，点击“save”：

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

添加完成后，状态如下：

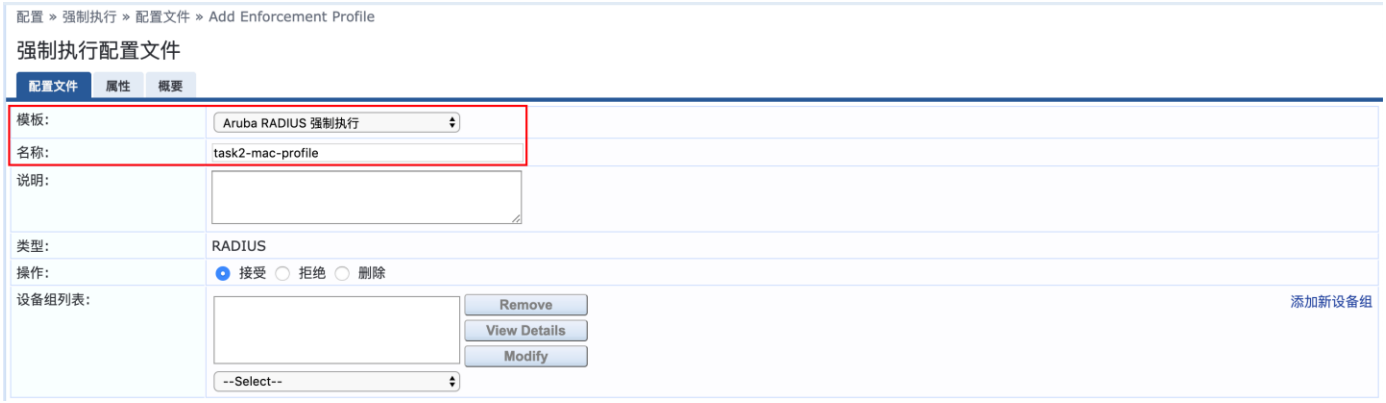
3.3.2 添加认证服务

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**：



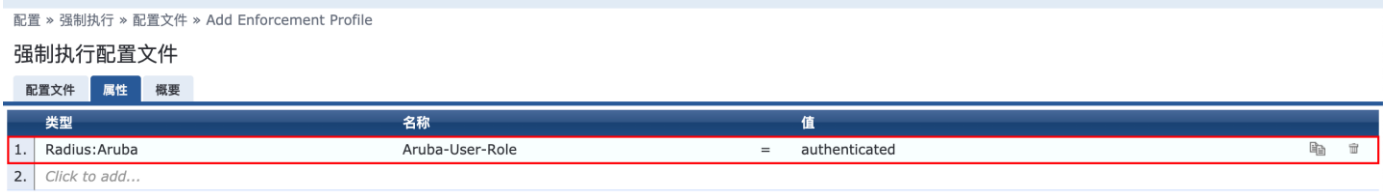
在“配置文件”选项卡中输入下面参数：

- ✓ 模板：Aruba Radius 强制执行
- ✓ 名称： task2-mac-profile



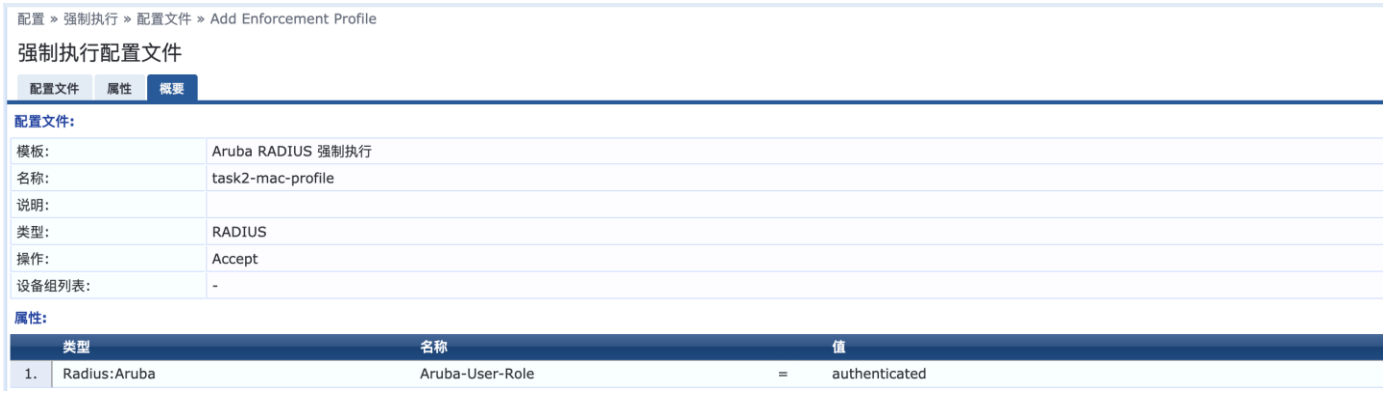
在“属性”选项卡中输入下面参数：

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

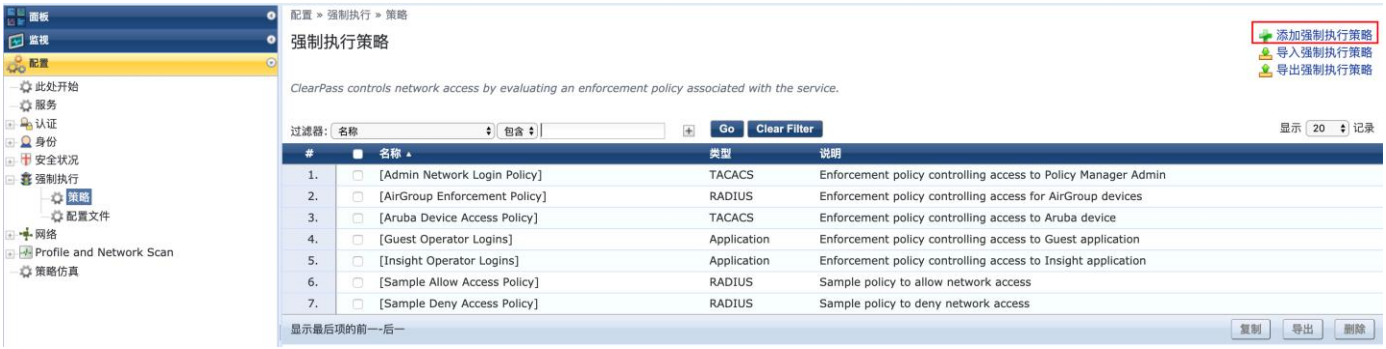


在“概要”选项卡中对配置进行总览：

- ✓ 概要： 点击“保存”



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：

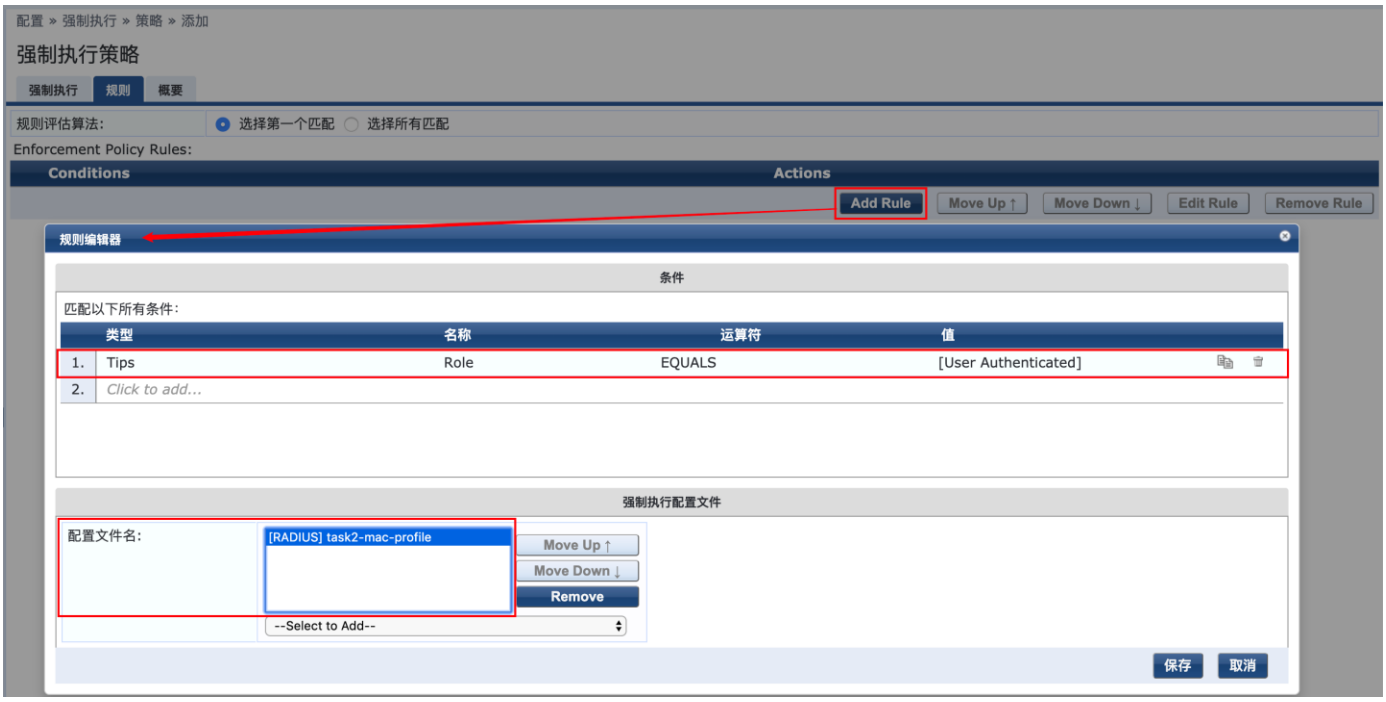


在“强制执行”选项卡中输入下面参数：

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

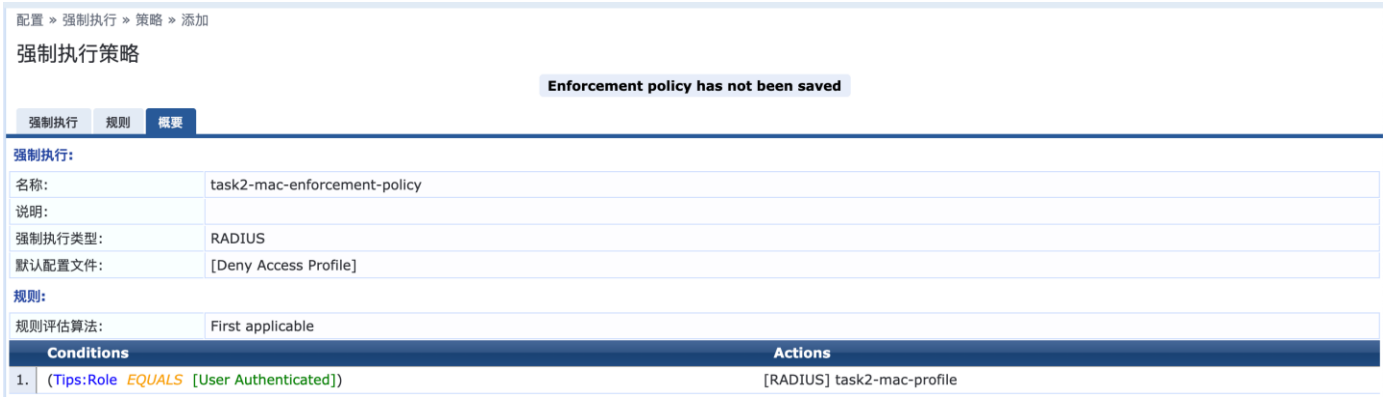
在“规则”选项卡中点击“Add Rule”：

- ✓ 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)*

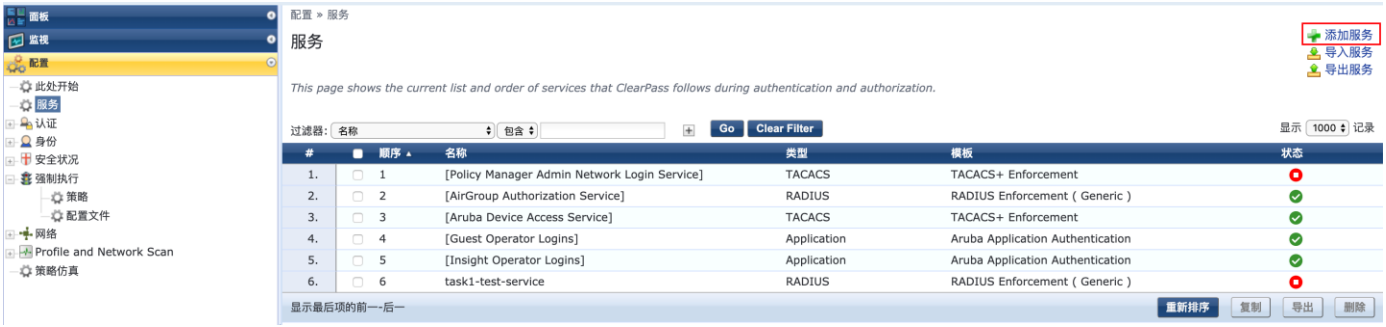


在“概要”选项卡中对配置进行总览：

✓ 概要：查看配置总览，并点击“保存”



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：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）

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]

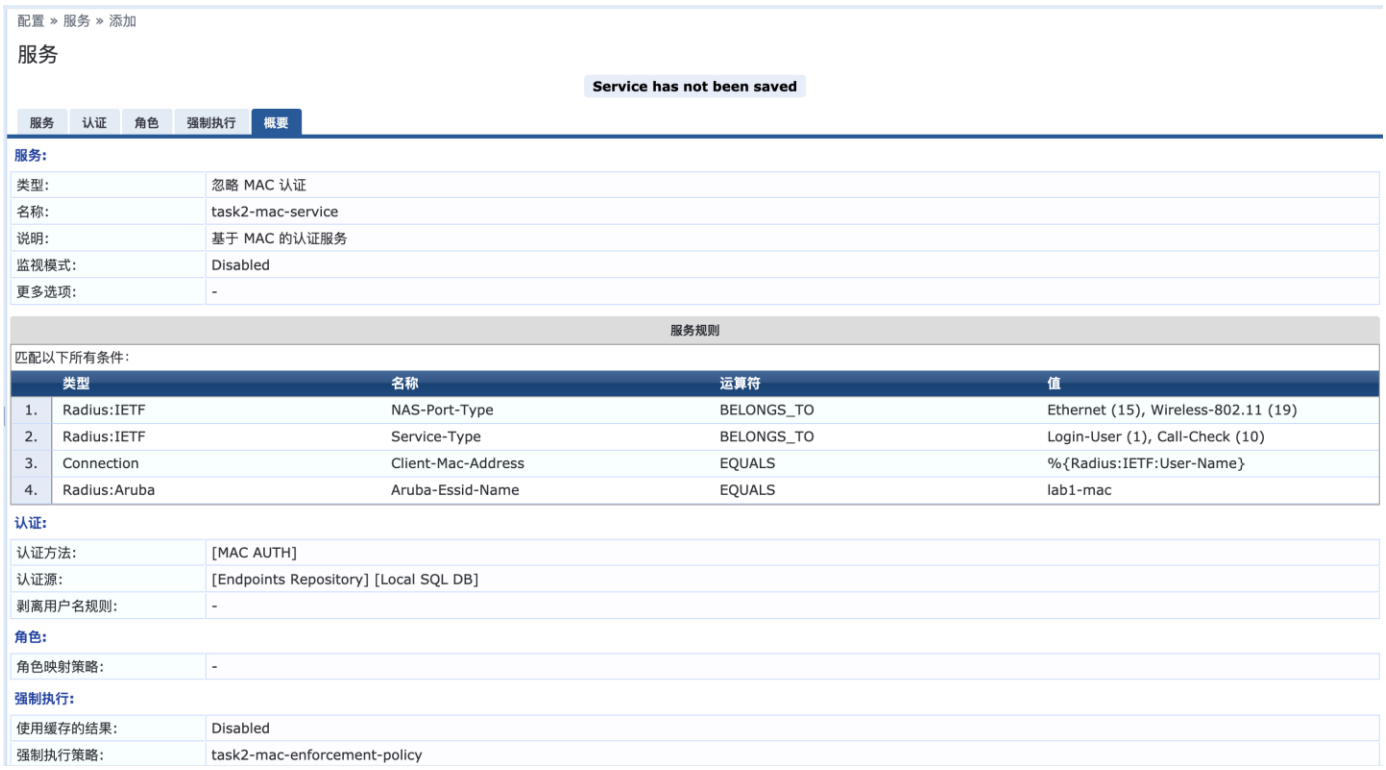
在“角色”选项卡中，暂时不做任何配置*（详细内容可以参考高级介绍部分）*：

- ✓ 角色映射策略：空

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)*

在“概要”选项卡中对配置进行总览，并点击保存：



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.
```

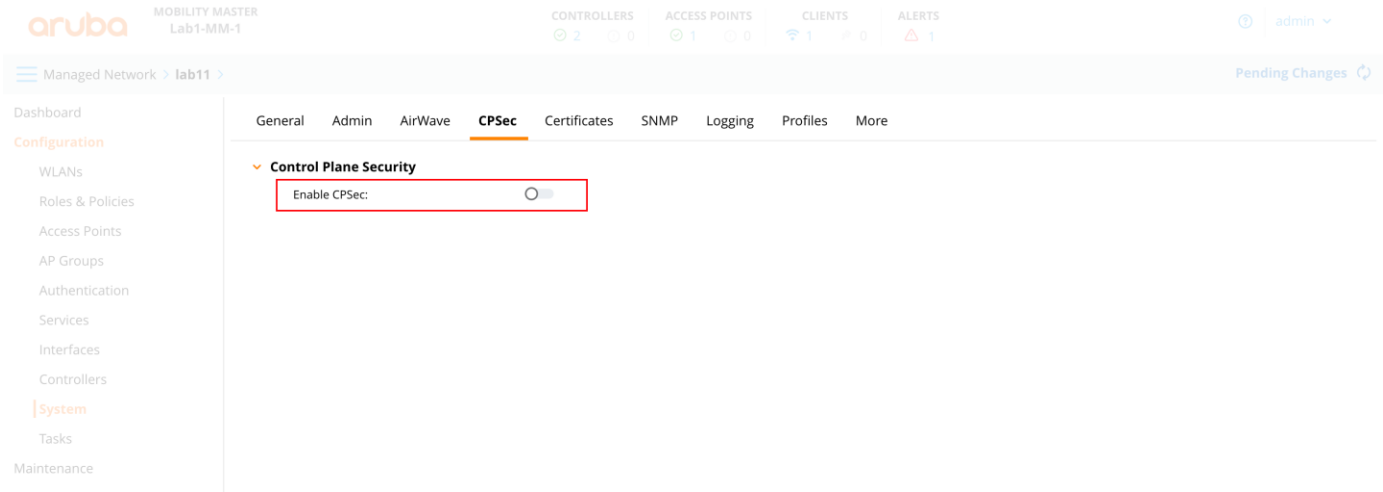
第4步: 查看开启 PEF 功能结果

```
(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

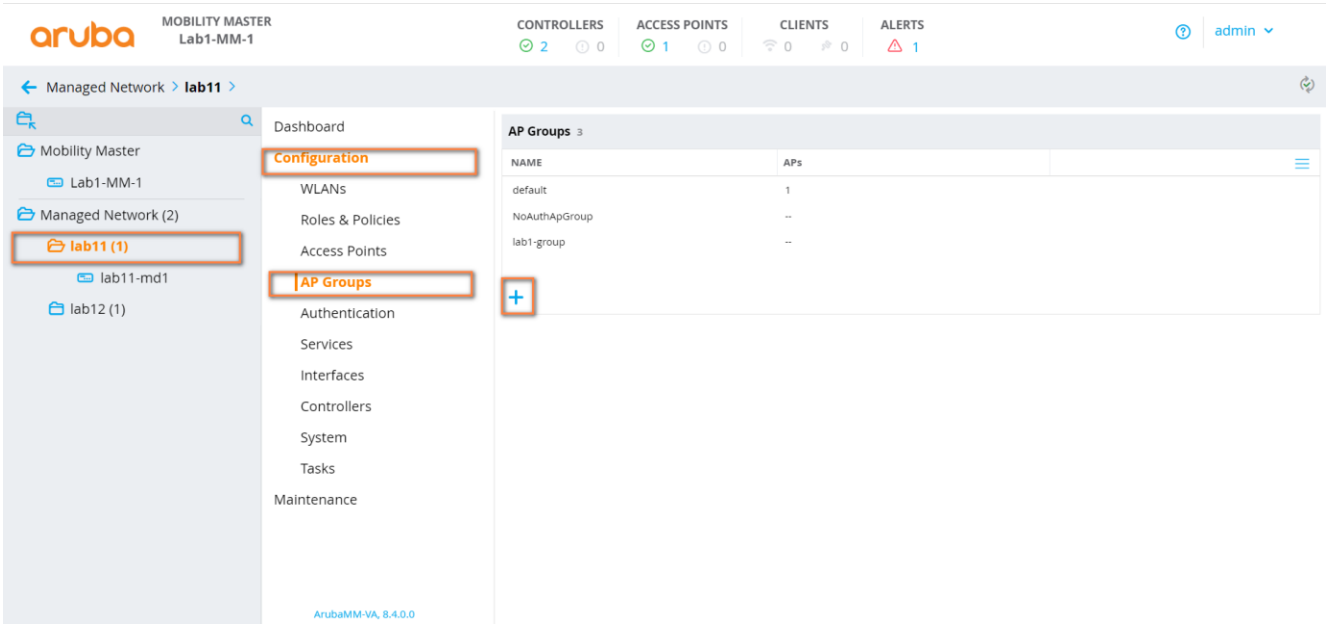
第1步: 使用Web 方式登录到Mobility Master（10.X.10.11），找到Managed Networks -> labX -> Configuration -> System（X： 1 ·····6）

✓ 关闭 Enable CPSec



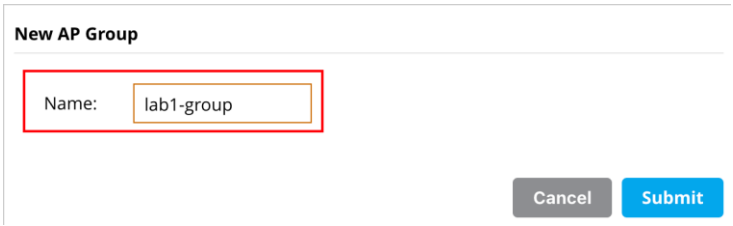
3.4.3 添加 AP-Group

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”



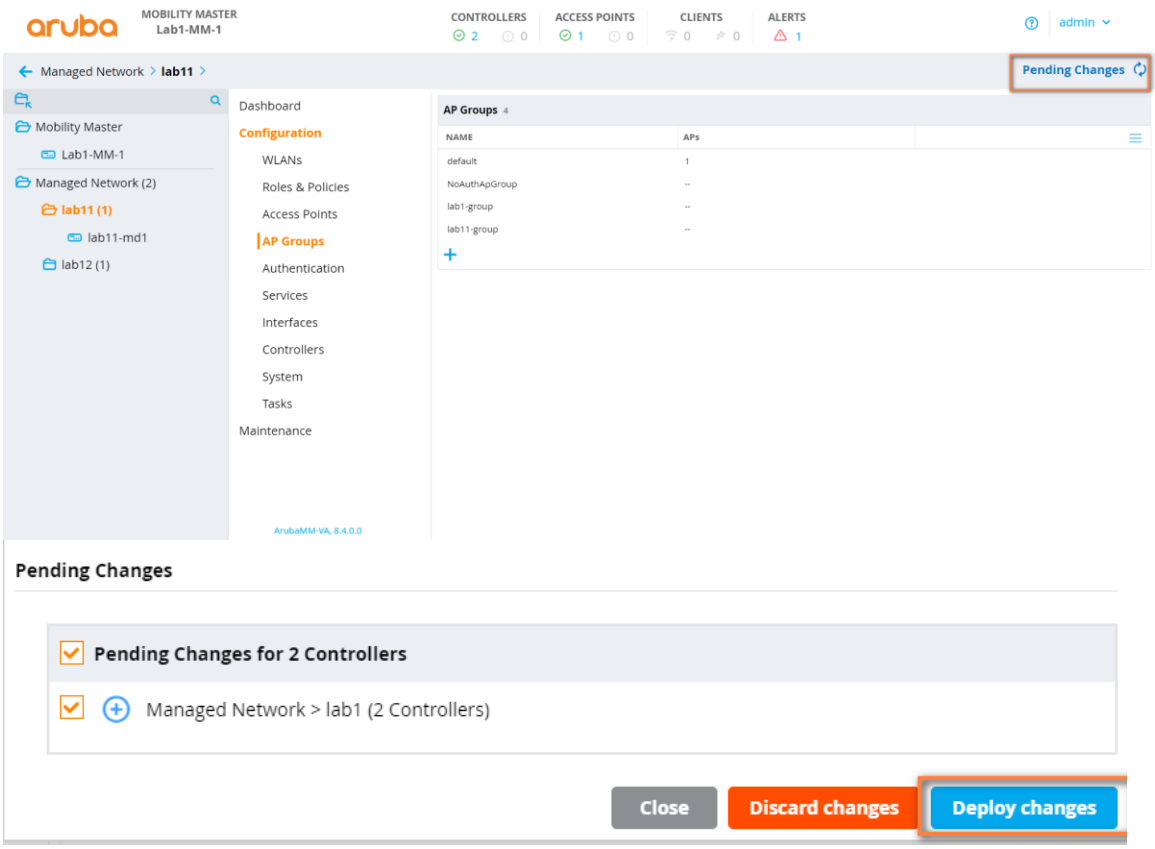
第3步：在弹出的窗口的输入以下参数，并点击“Submit”提交配置

- ✓ Name： labX-group (X : 1····6)



第4步：配置保存并同步给md设备

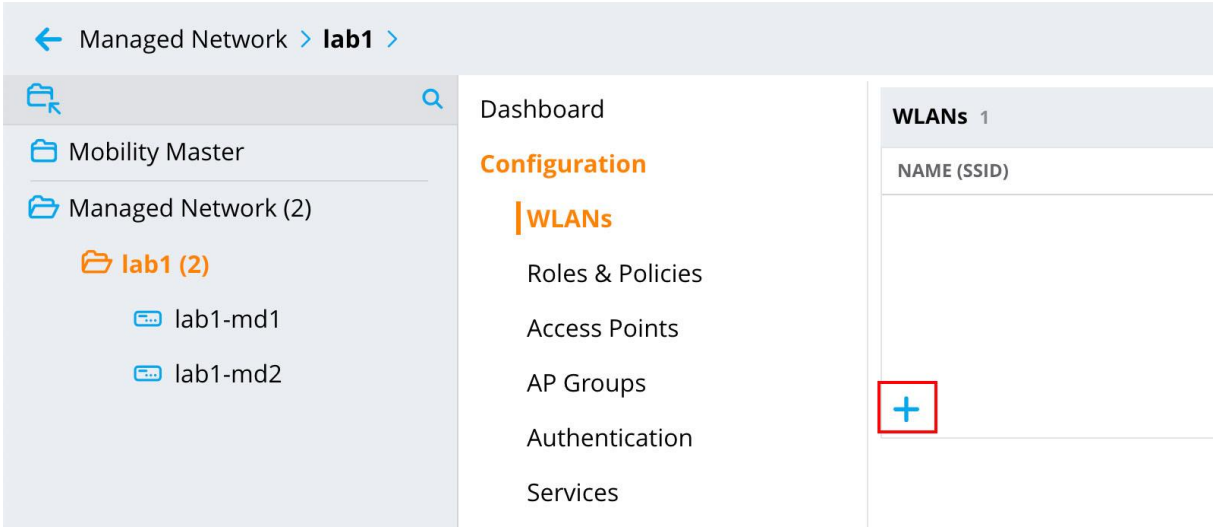
- ✓ 1、Pending Changes： 点击该按钮（右上角提示）
- ✓ 2、Deploy changes： 点击该按钮



3.4.4 添加无线信号

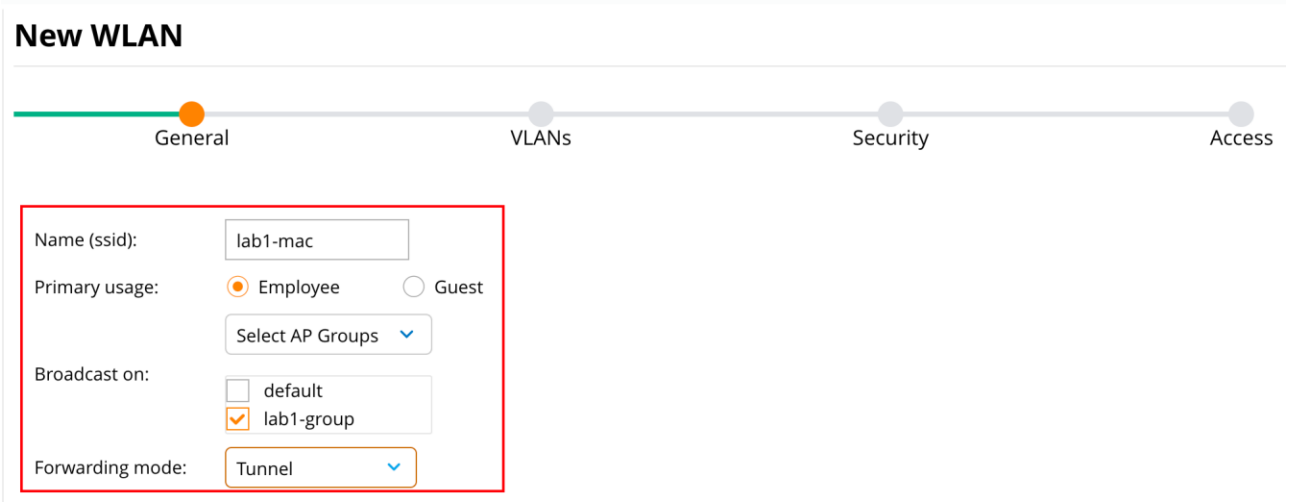
第1步: 使用 Web 方式登录到 Mobility Master (10.X.10.11)，找到 Managed Networks - > labX -> Configuration -> WLANs（X： 1 ·····6），点击“+”进入创建一个新的无线配置向导

配置一个 SSID: labX-mac (X : 1 • • • • • • 6)



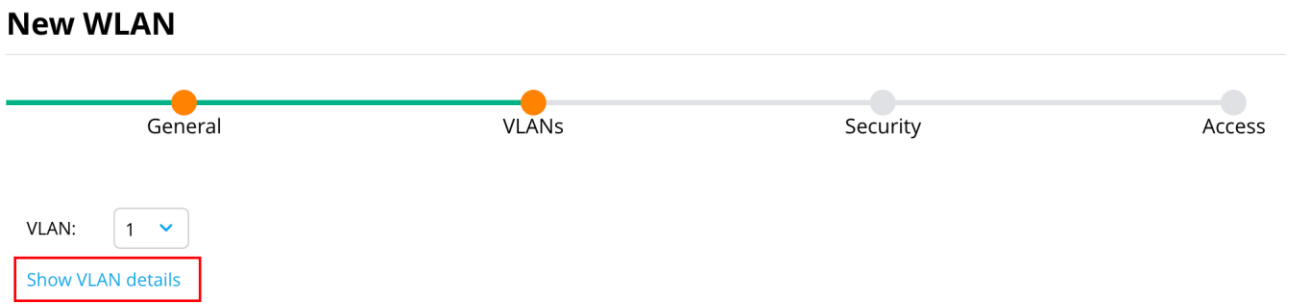
第2步：在“General”选项卡中配置如下参数

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



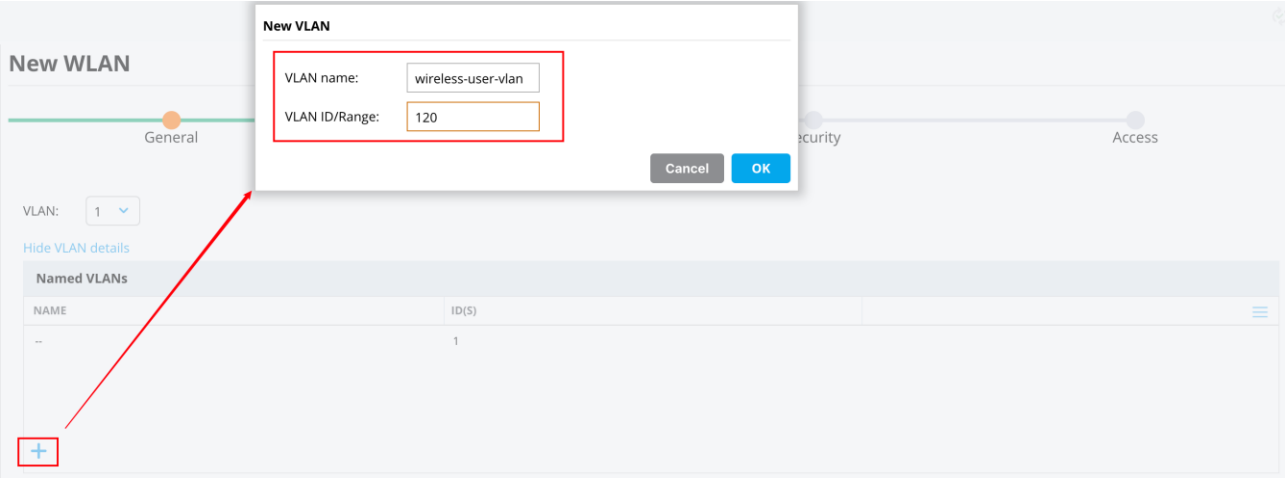
第3步：在“VLANs”选项卡中，点击“Show VLAN details”，进入 VLAN 配置向导

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 。



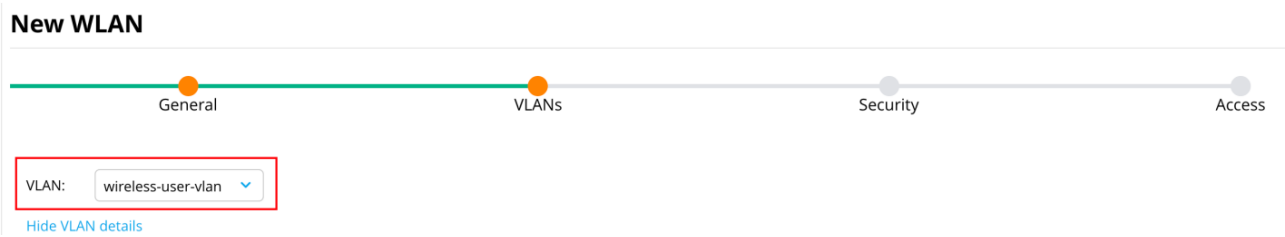
第4步：点击下面的“+”，增加一个无线业务 VLAN，配置参数如下，点击“OK”：

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



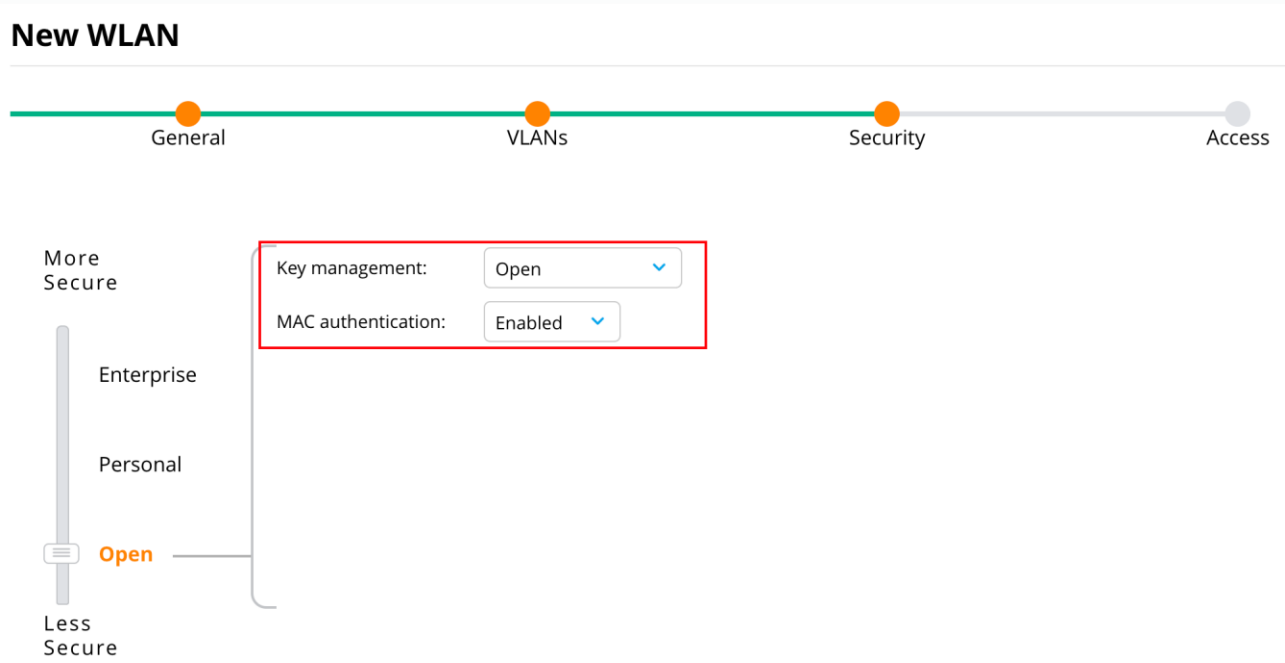
第5步：将 VLAN 的参数选择为“wireless-user-vlan”*(既上一步中创建的 vlan name)*：

- ✓ VLAN：wireless-user-vlan



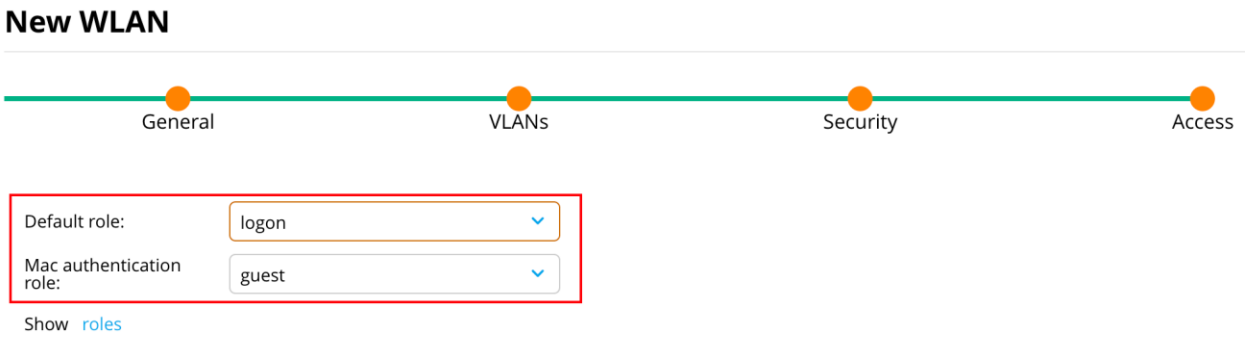
第6步：在“Security”选项卡中配置如下参数

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



第7步：在“Access”选项卡中配置如下参数并点击“Finish”

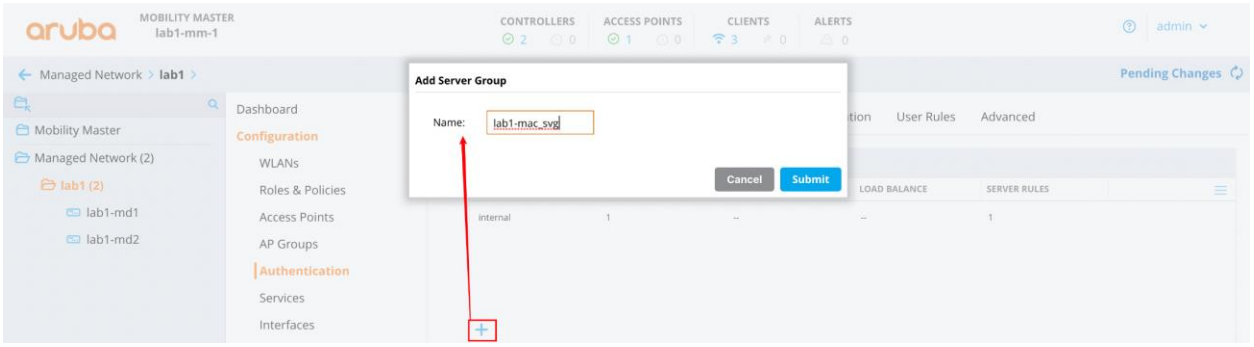
✓ Mac authentication role：guest *(测试阶段注意观察一下通过 mac 认证的终端实际获取到的 role？)*



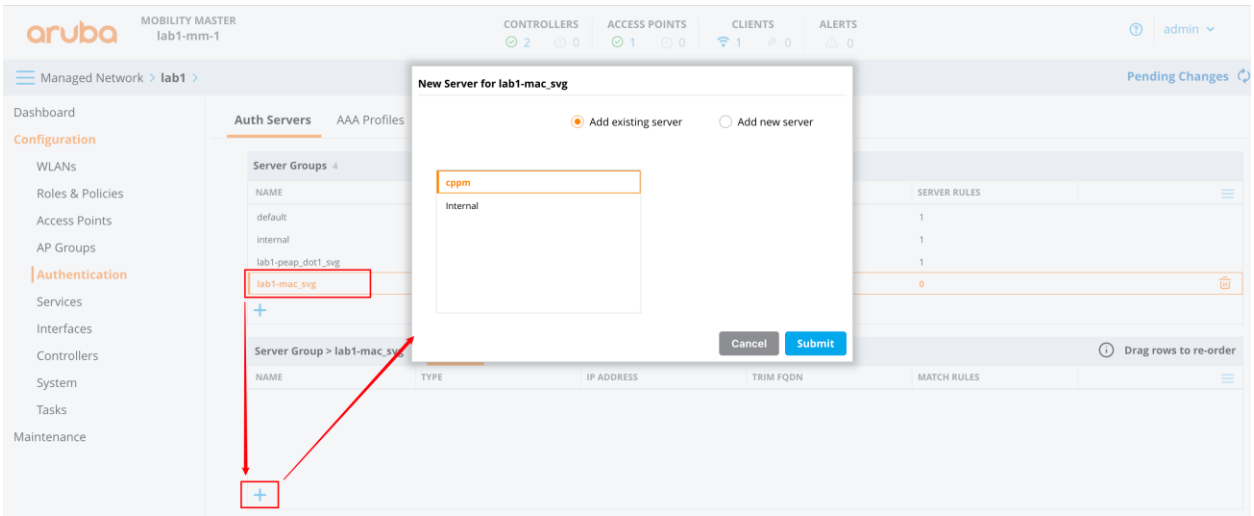
3.4.5 添加认证和计费服务器

第1步：找到 Managed Networks - > labX -> Configuration -> Authentication->Auth Servers（X：1 ·····6）,点击“+”

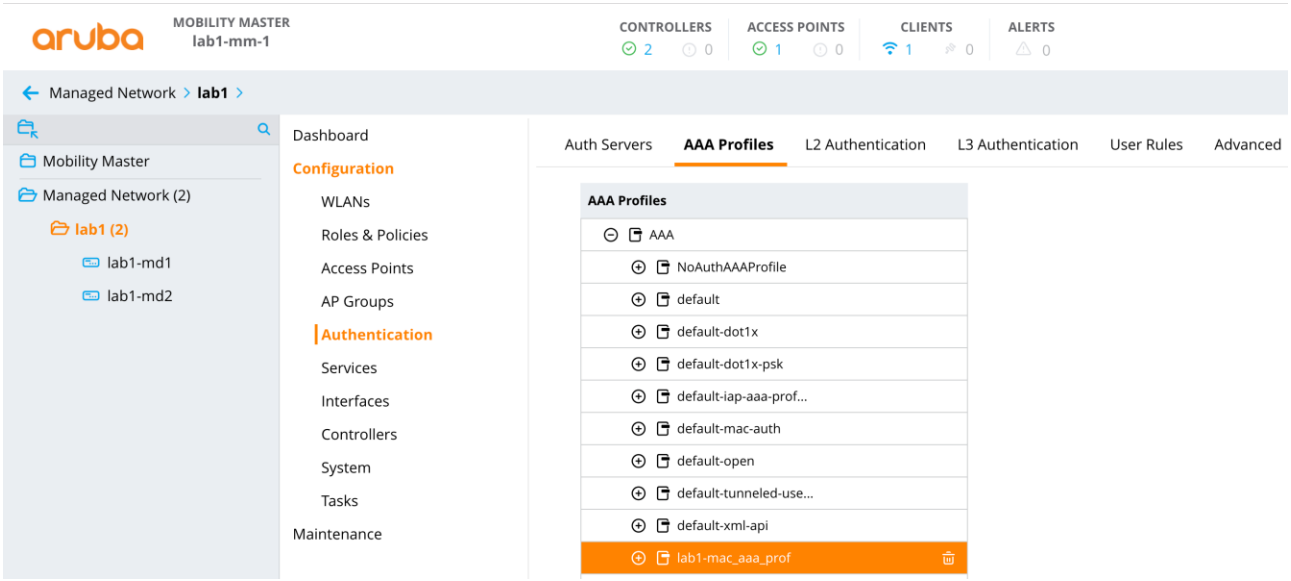
✓ 在弹出的选项卡中输入“labX-mac_svg” （X： 1 ·····6）



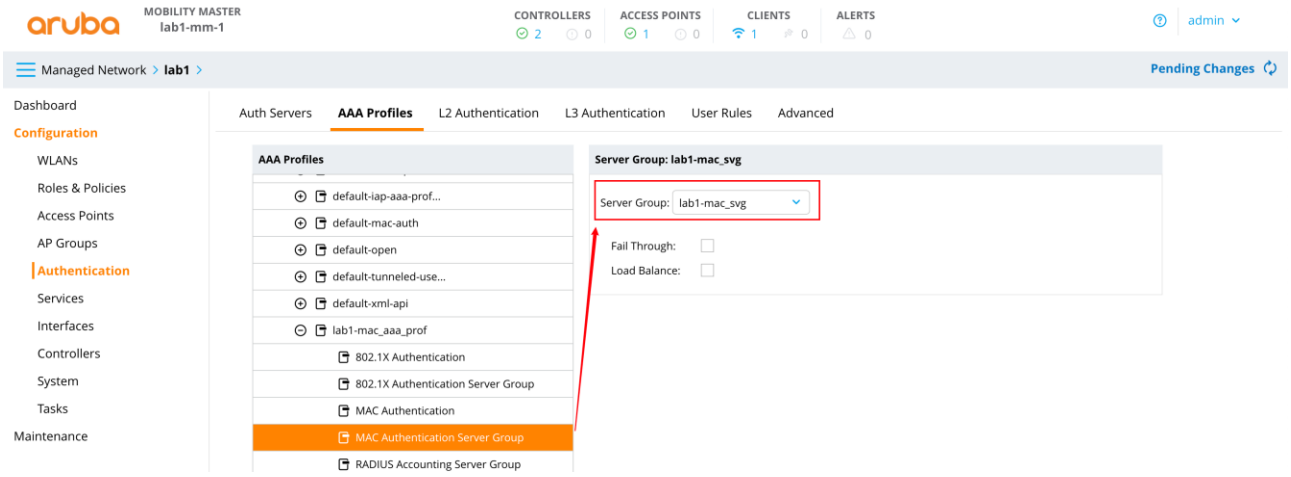
第2步：点击新建的 Server Group： “lab1-mac_svg”，点击下方的“+”添加 radius server，在弹出的选项卡中选中“cppm”，并点击“**Submit**”



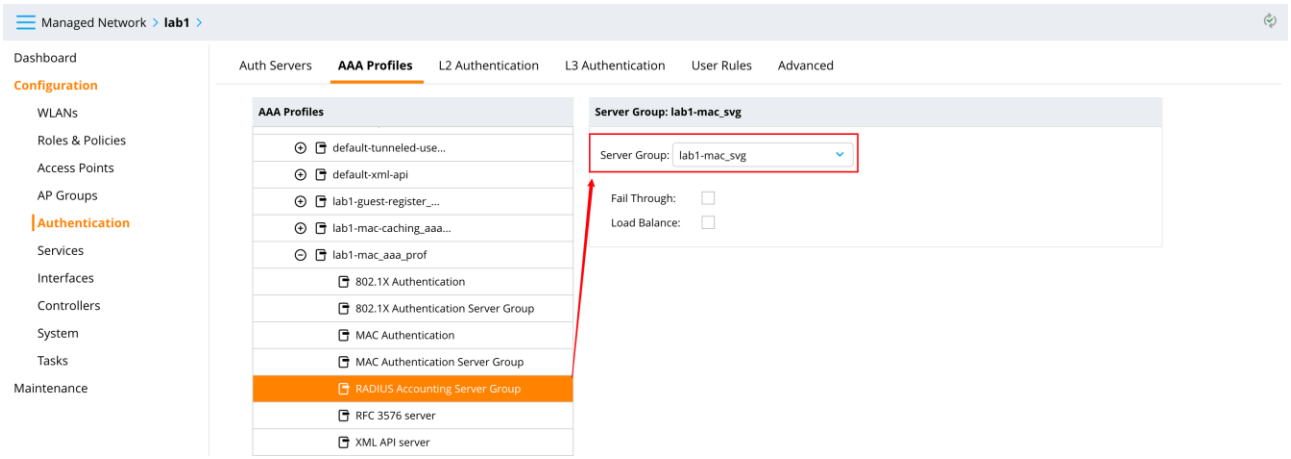
第3步：找到 Managed Networks - > labX -> Configuration -> Authentication -> AAA Profile（X：1 ·····6），找到 labX-mac_aaa_prof（X：1 ·····6）：



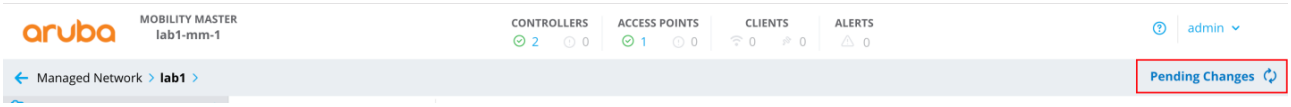
✓ 修改“MAC Authentication Server Group”为“labX-mac_svg”(X:1·····6)，并点击“**Submit**”



✓ 修改“Radius Accounting Server Group”为“labX-mac_svg”(X:1·····6)，并点击“**Submit**”



第4步：点击右上角“Pending Changes”保存配置



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

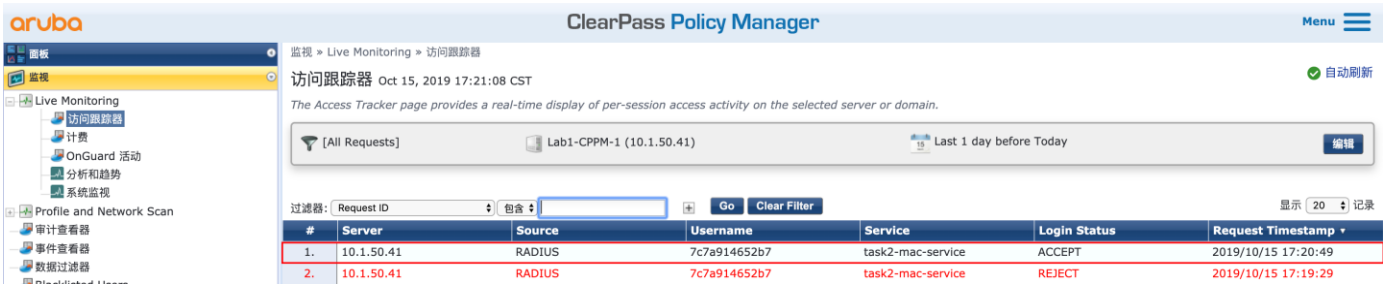
第2步：SSH登录到MM：10.X.10.50（X：1···6），查看当前用户所在MD

```
(lab1-md1) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP            MAC            Name         Role          Age(d:h:m)  Auth  VPN link  AP name          Roaming   Essid/Bssid/Phy                Profile
me  User Type
----------    ------------       ------       ----          ----------  ----  --------  -------          -------   ---------------                -------
--  ----------
10.1.20.102  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
    WIRELESS
```

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。

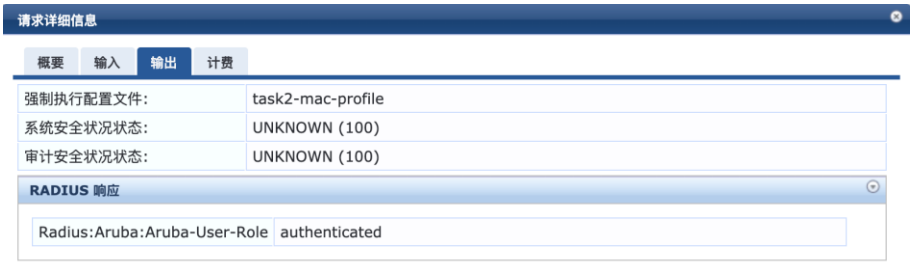
✓ 此时我们看到用户mac认证成功



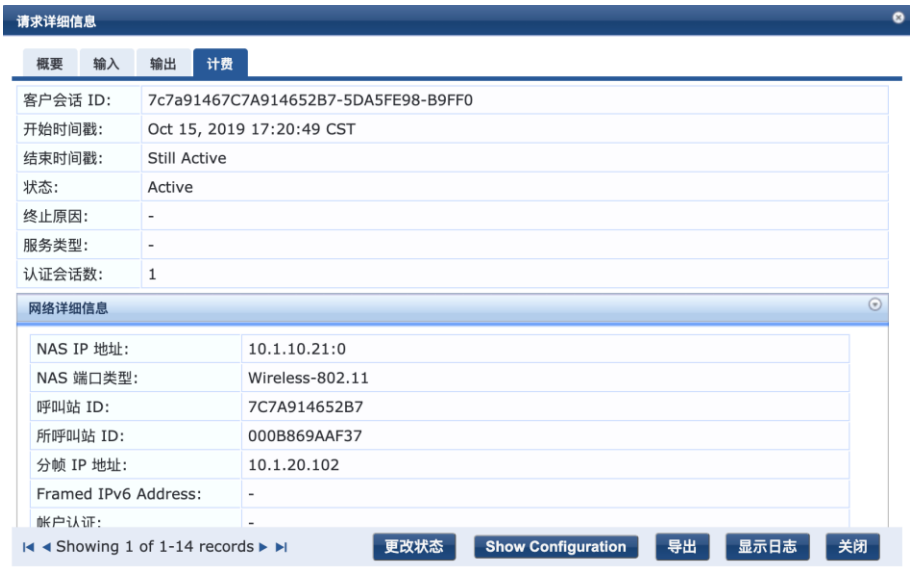
✓ 点击认证成功的记录，在“概要”选项卡中查看信息，如下图：

✓ 点击“输入”选项卡中查看认证请求信息，如下图：

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



✓ 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
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:
-
Showing 1 of 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）

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

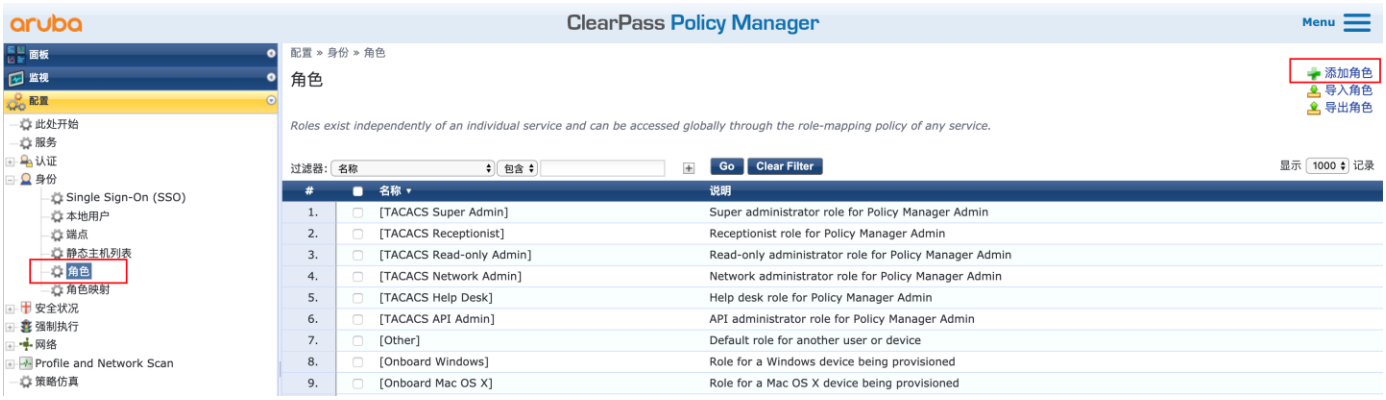
4.3 ClearPass 配置

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）

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：



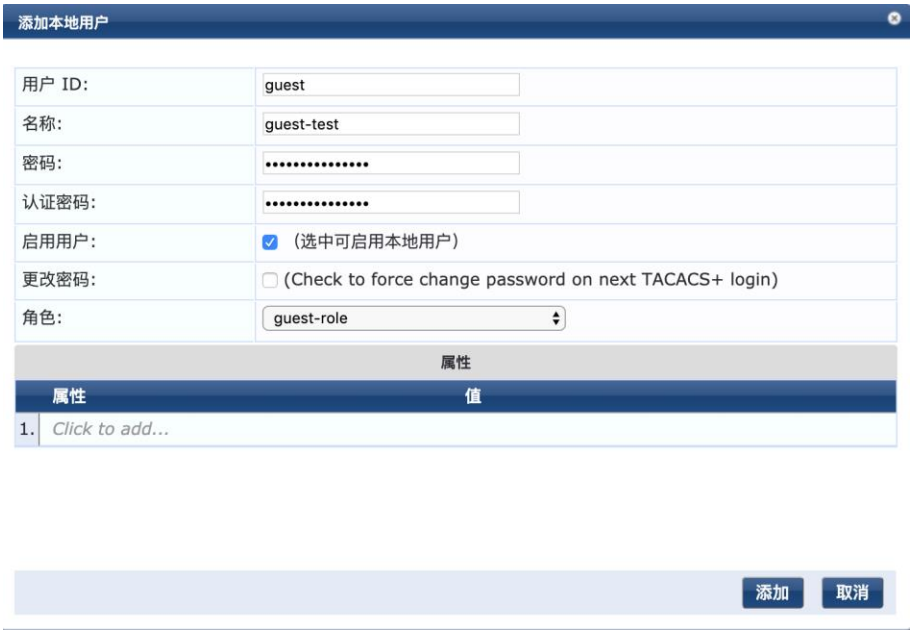
在弹出的添加角色窗口中输入下面参数，点击“save”：

- ✓ 名称：guest-role
- ✓ 说明：赋予访客的访问权限

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

在弹出的添加角色窗口中输入下面参数，点击“save”：

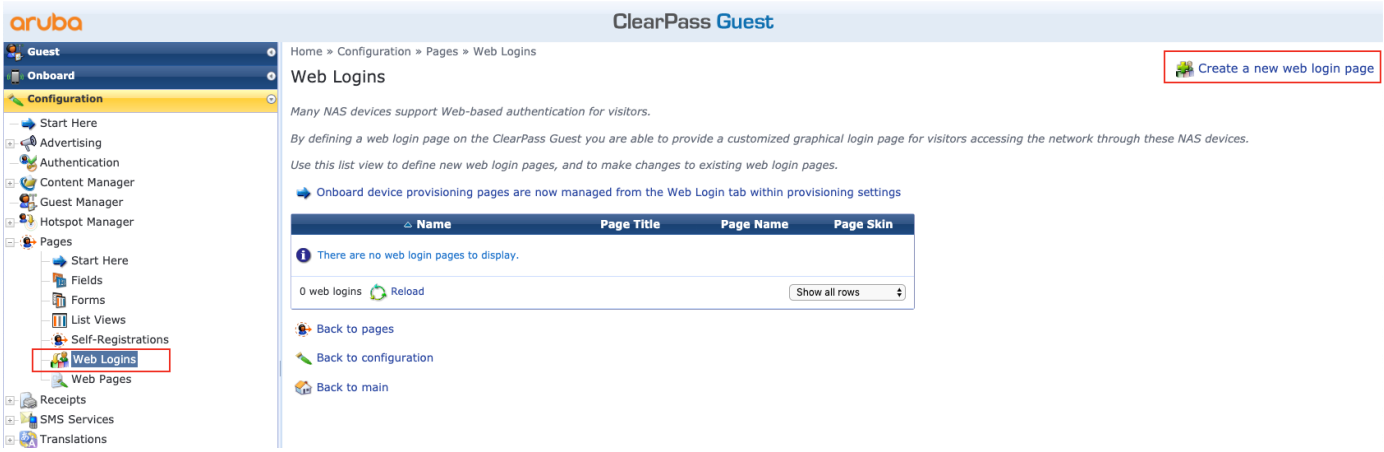
- ✓ 用户ID：guest（即用户的登录账号）
- ✓ 名称：guest-test （即该账号的别名，只是一个标签）
- ✓ 密码：aruba123（即用户的登录账号）
- ✓ 认证密码：aruba123（即重复输入一次登录密码）
- ✓ 启用用户：☑ （勾选）
- ✓ 角色：guest-role （该角色在第一步中创建的）



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）

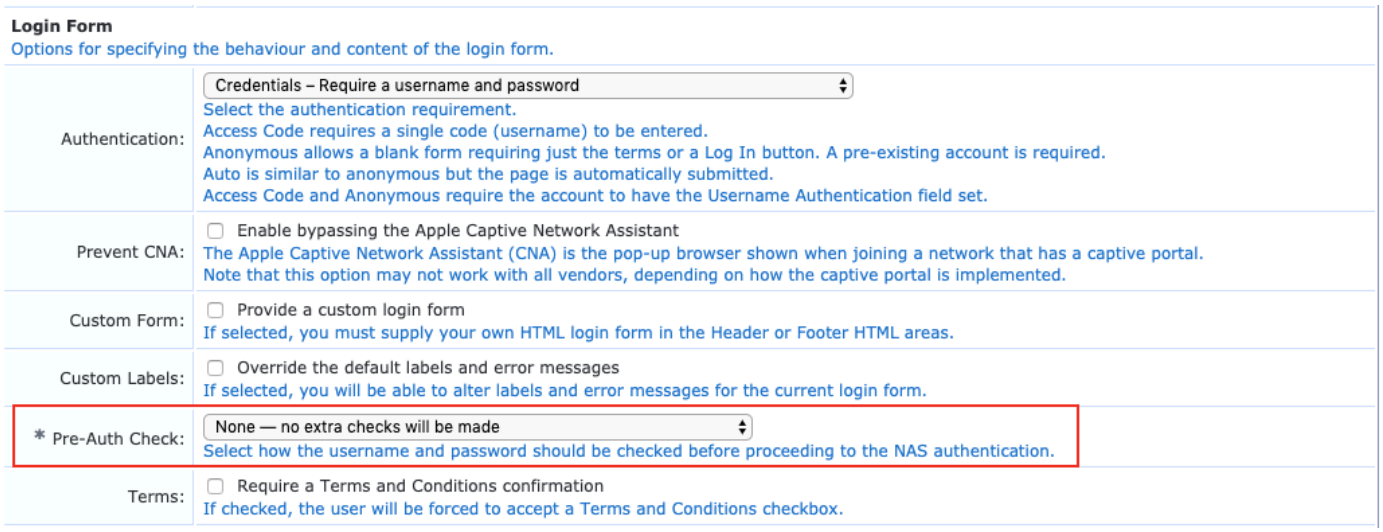
第2步：找到Configuration » Pages » Web Logins，点击右侧的“Create a new web login page”按钮，新增一个访客登录页面：



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”

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



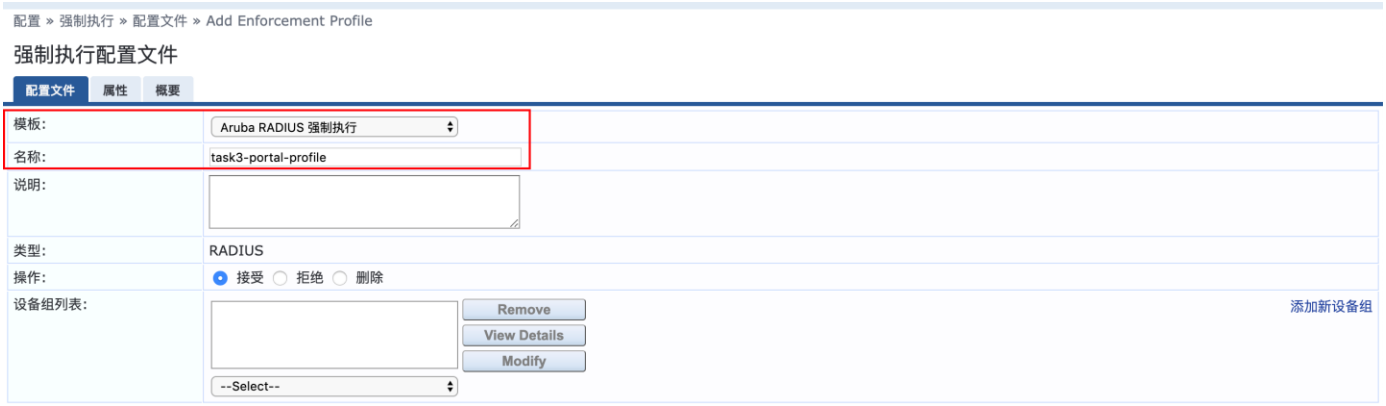
✓ 点击“**Save Changes**”按钮保配置

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：

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

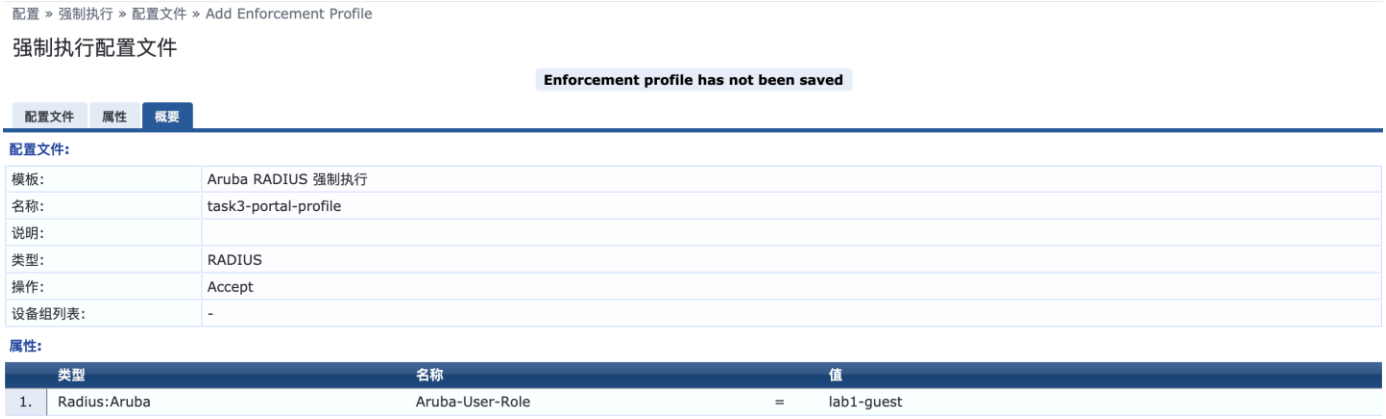


在“属性”选项卡中输入下面参数：

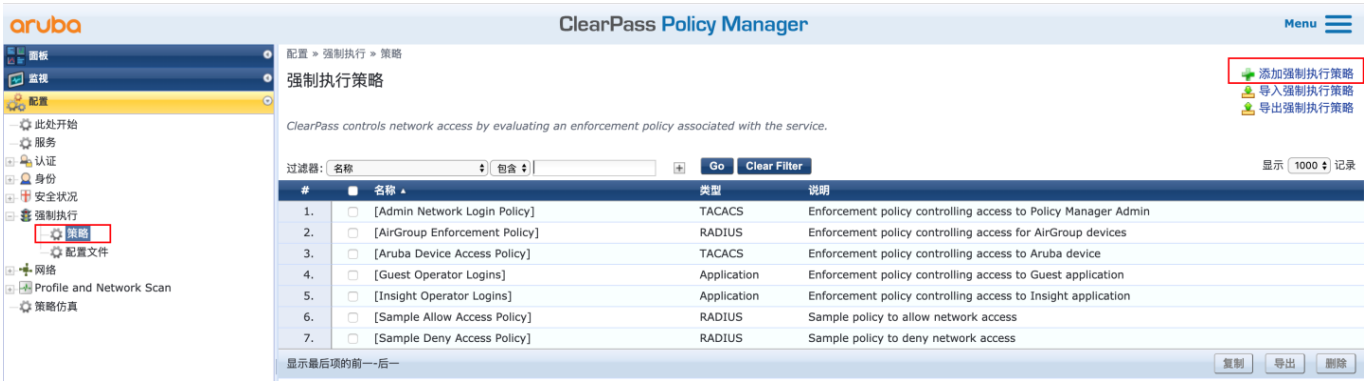
- ✓ 属性： Radius:Aruba Aruba-User-Role lab1-guest

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”



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：

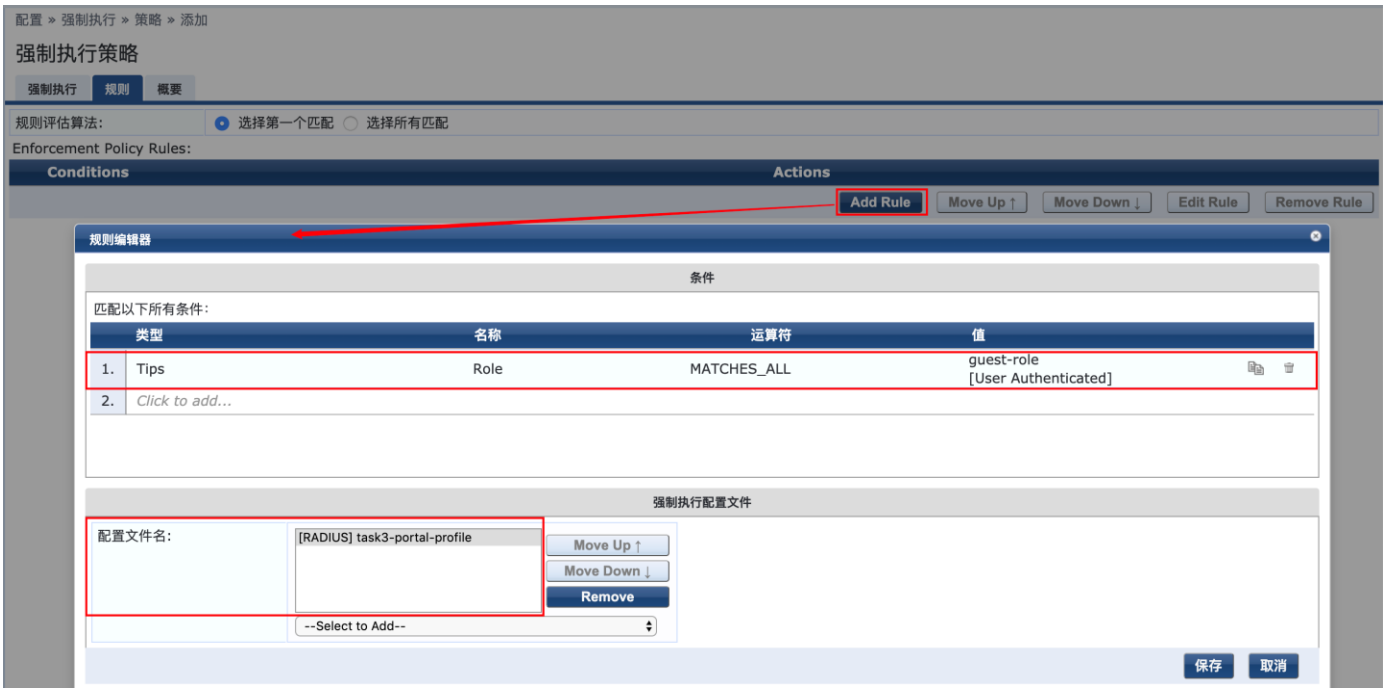


在 “强制执行” 选项卡中输入下面参数：

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

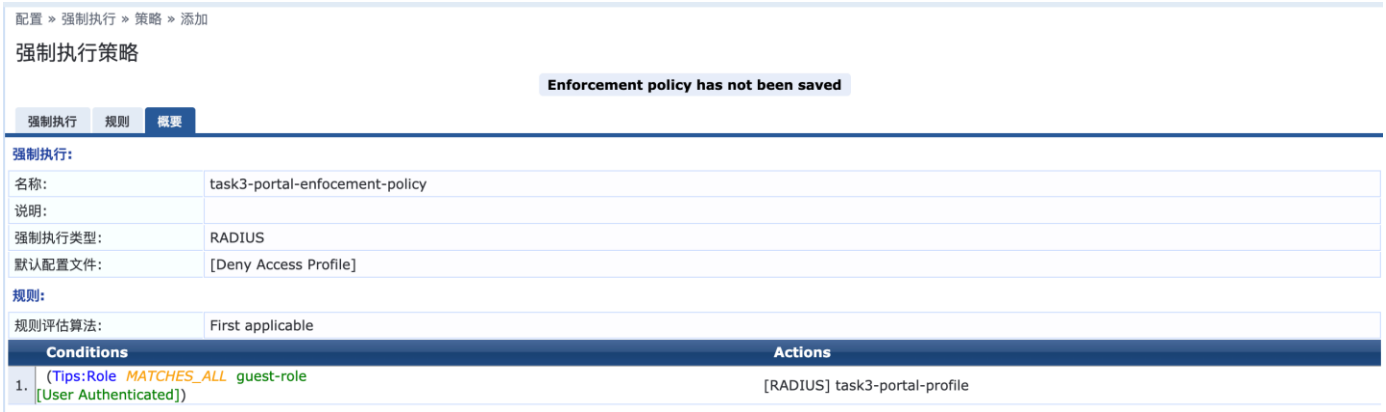
在 “规则” 选项卡中输入下面参数：

- ✓ 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)*



在“概要”选项卡中对配置进行总览：

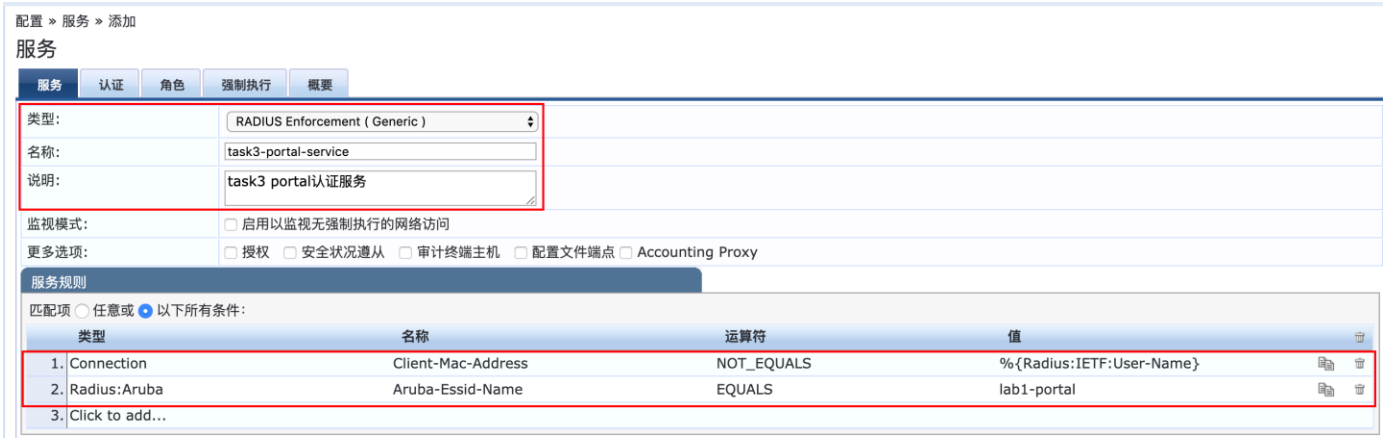
- ✓ 概要：查看配置总览，点击“保存”按钮



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）



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]

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

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)*

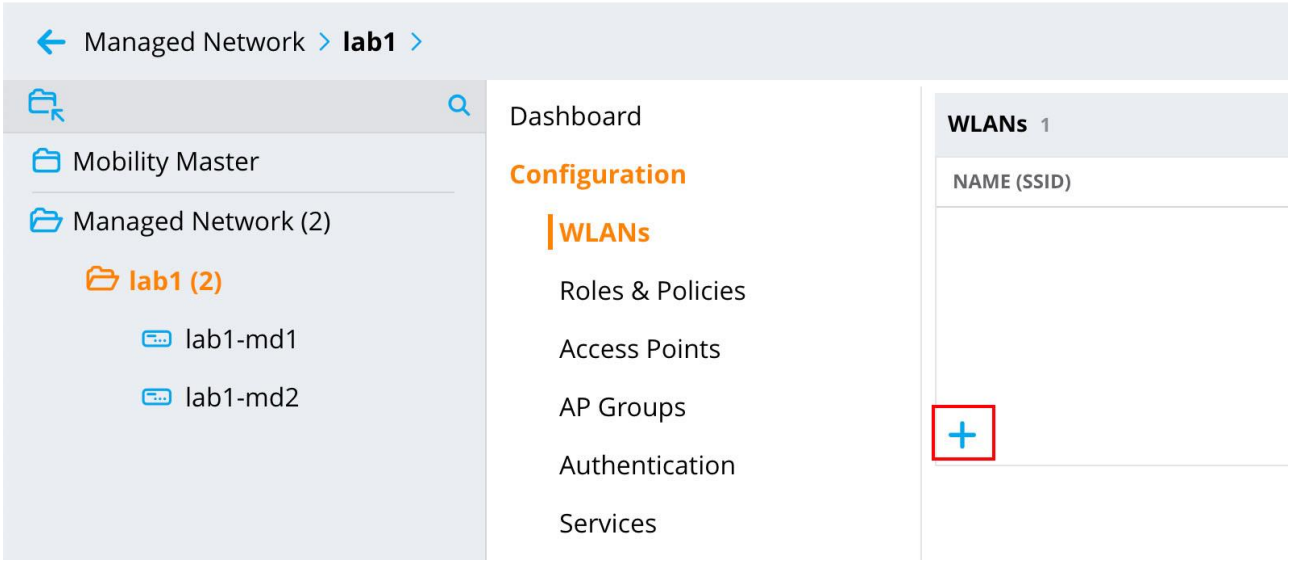
在“概要”选项卡中对配置进行总览：

✓ 概要：查看配置总览，点击“保存”按钮

4.4 控制器配置

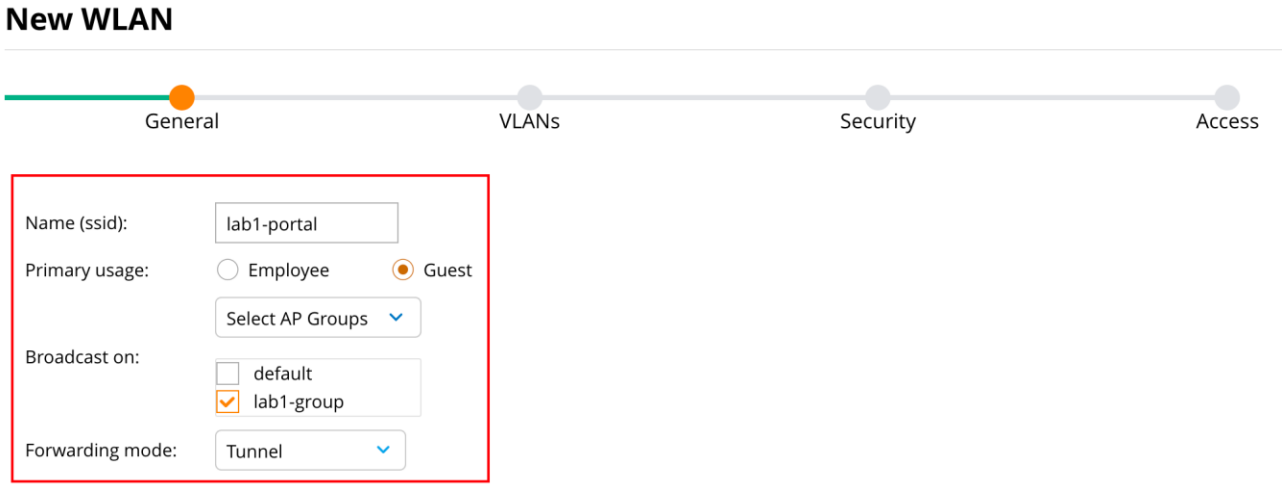
4.4.1 添加无线信号

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



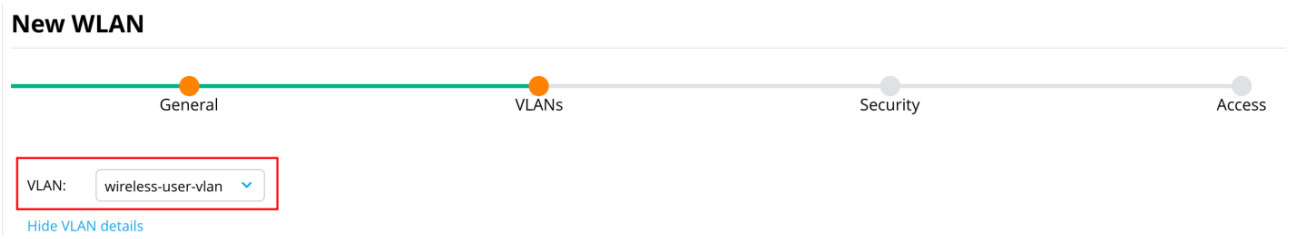
第2步：配置 SSID 名称、主要用途、在哪个 AP-Group 广播、转发模式

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



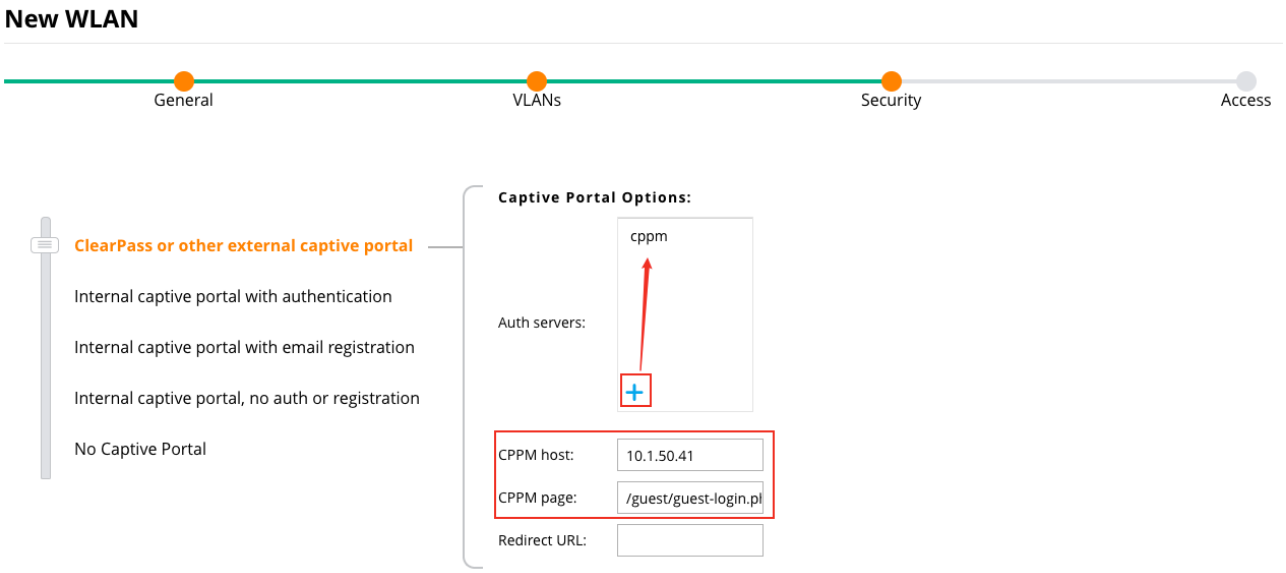
第3步：配置 VLAN

- ✓ VLAN：wireless-user-vlan

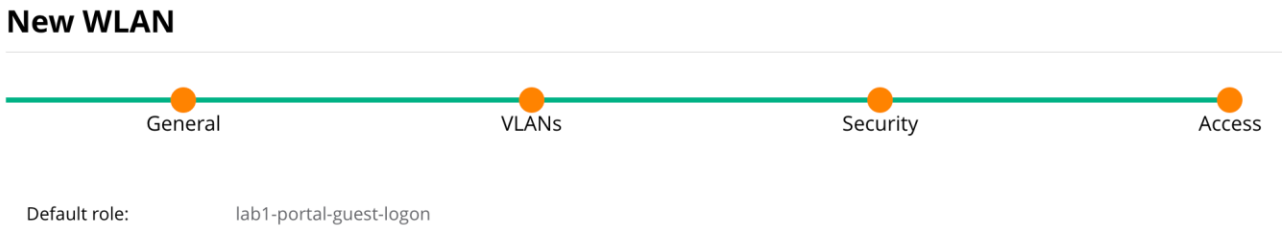


第4步：配置 portal 认证方式

- ✓ 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*）



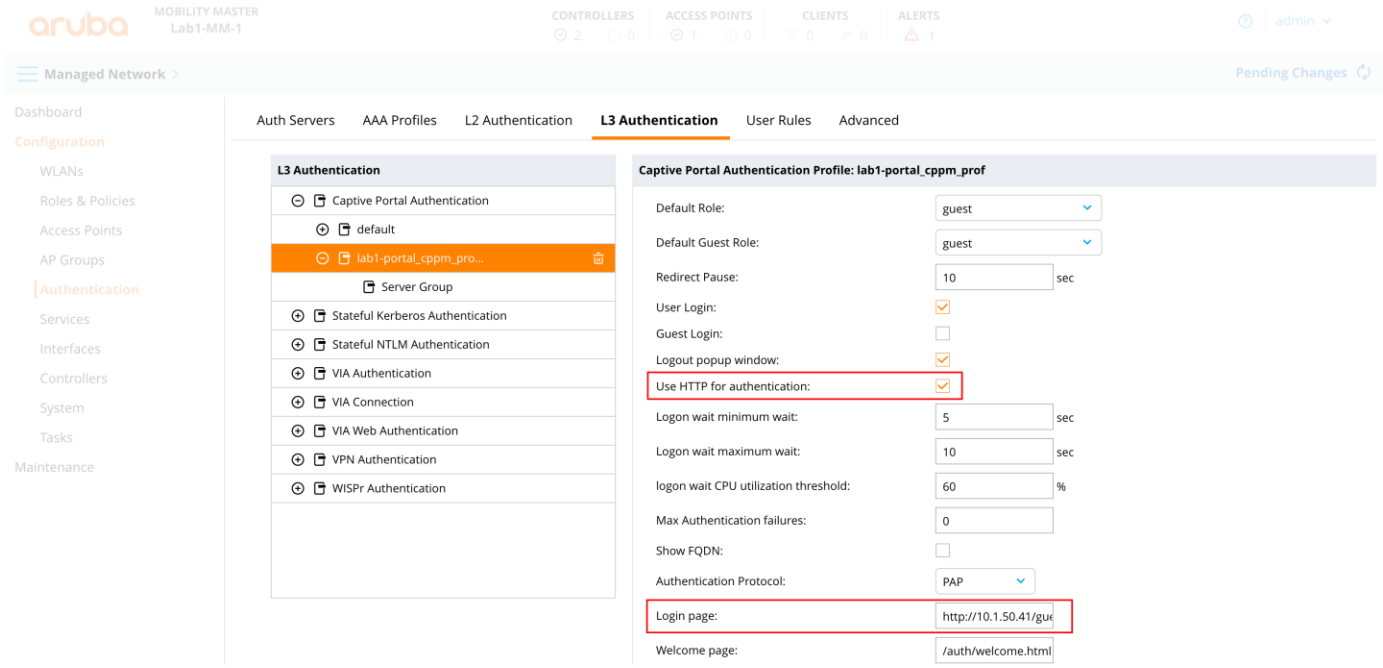
第5步：完成向导配置



4.4.2 修改 portal 认证配置

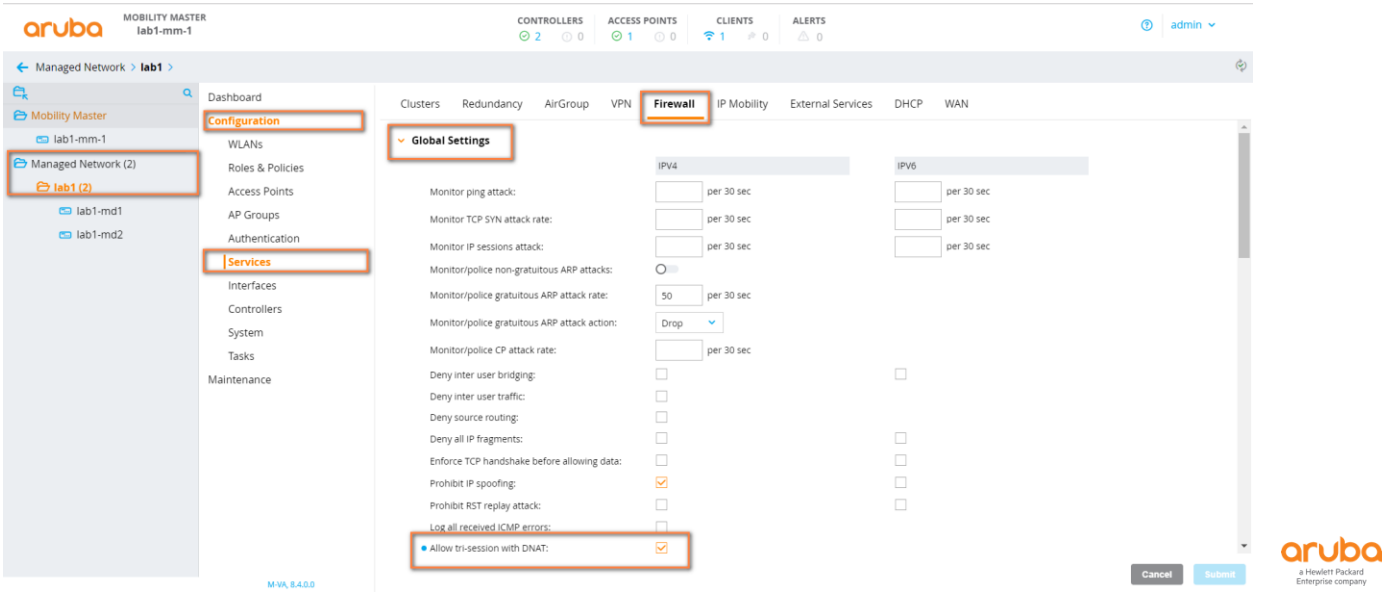
找到Managed Network - > labX -> Configuration -> Authentication -> L3 Authentication 点击“Captive Portal Authentication”，选中“labX-portal_cppm_prof” （X： 1 ·····6），修改如下参数

- ✓ 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）

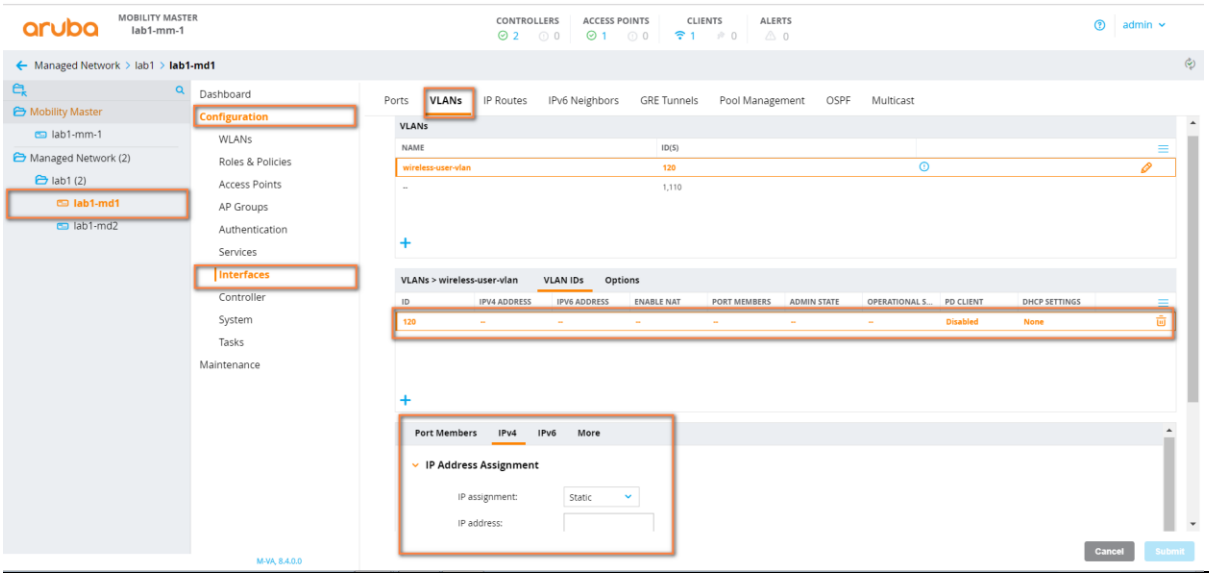


4.4.3 添加 Portal 重定向

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）



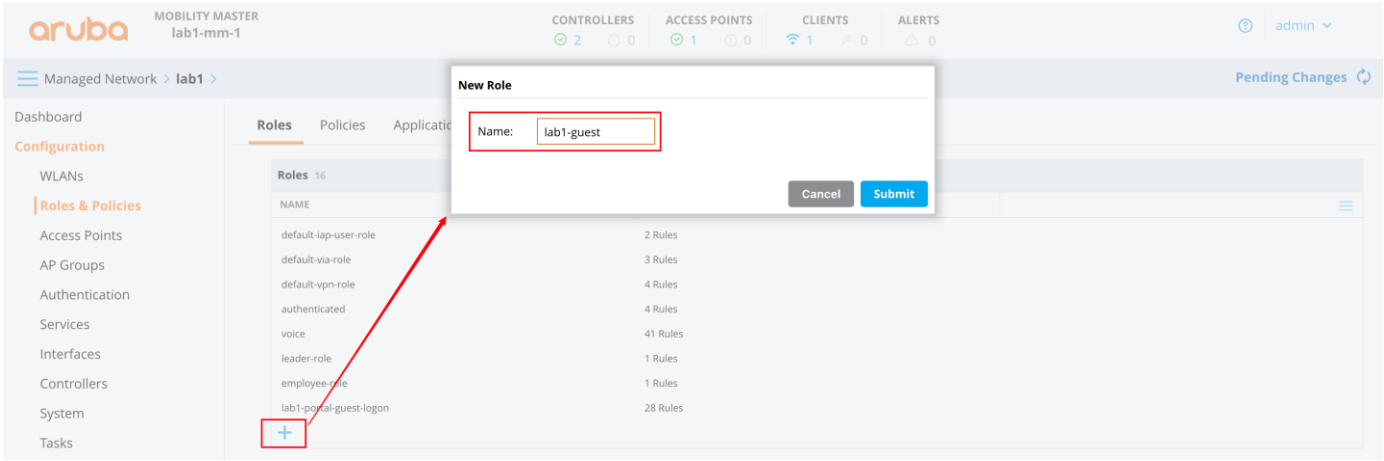
或者找到 Managed Network - > labX （X： 1 ·····6） -> labX-md1 /labX-md2（X： 1 ·····6） -> Configuration -> Interface -> VLANs, 点击“wireless-user-vlan -> VLAN ID 120”给控制器无线用户 VLAN：X20（X： 1 ·····6）配置三层接口 IPv4 地址，保证无线用户能够正常弹出 Portal 页面。



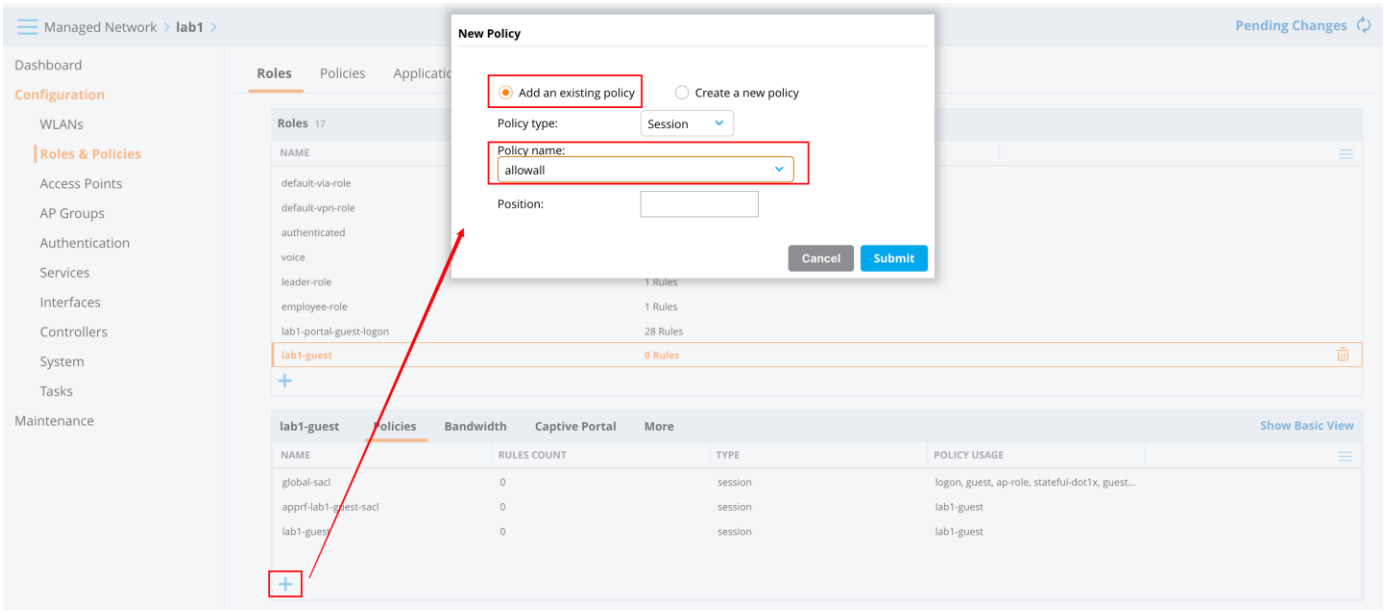
NOTE 需要对集群中的每台 md 分别进行配置,不同的 md 接口 IP 地址不同。

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）。

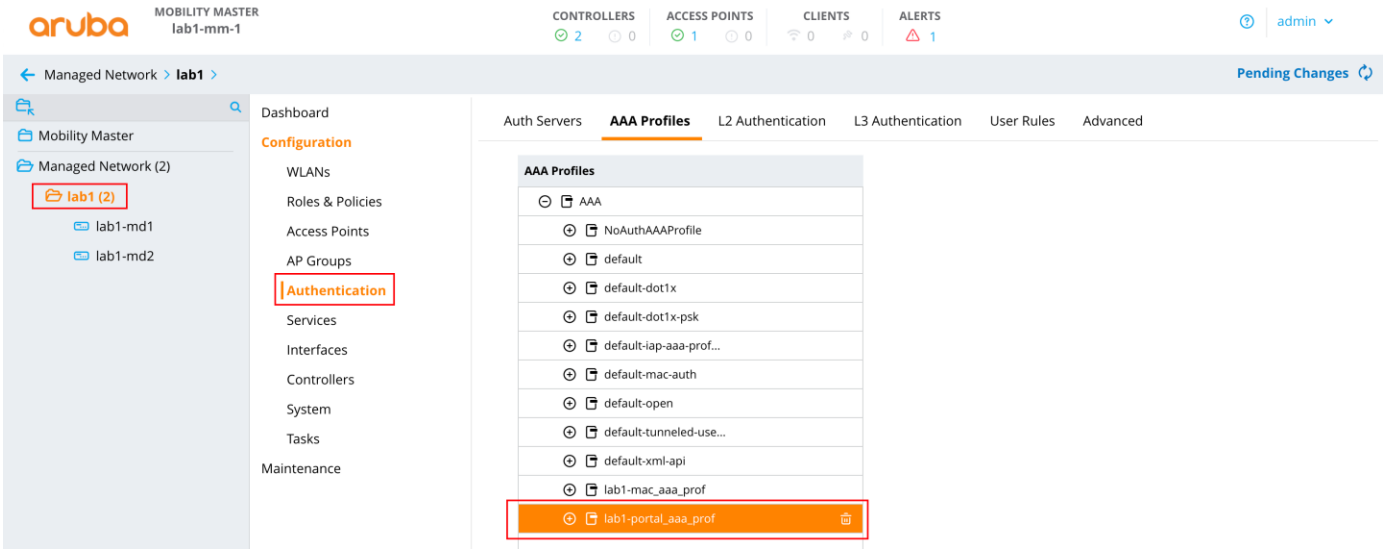


选中新建的role“labX-guest”，点击下方的“+”给这个role增加一个“allowall”的policy

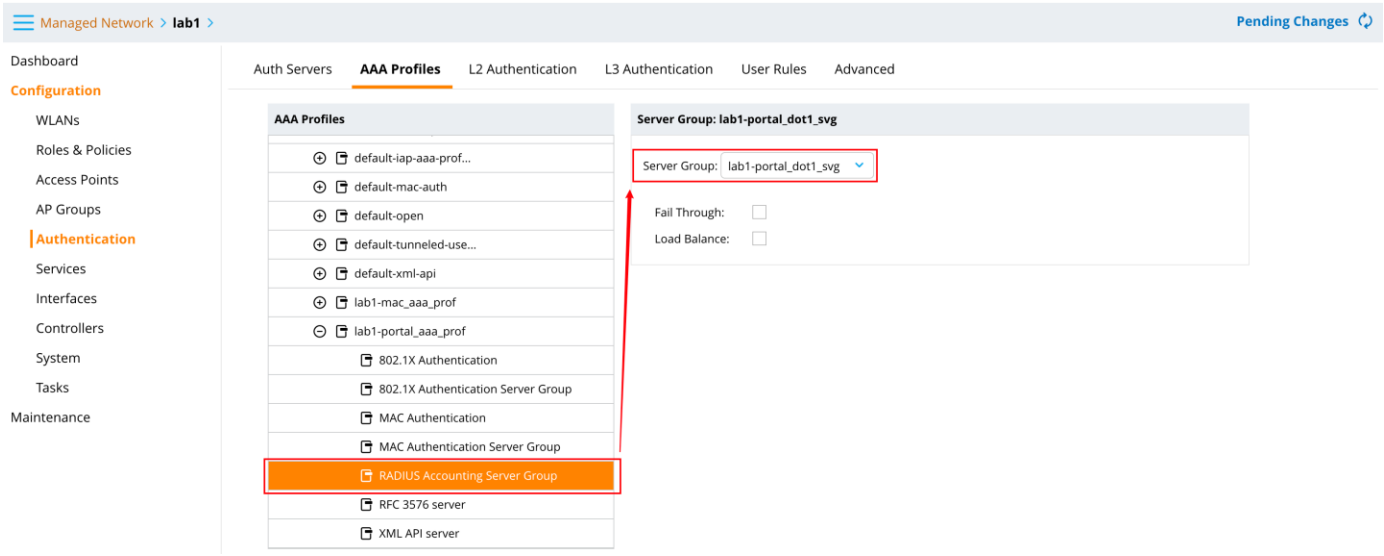


4.4.5 添加计费

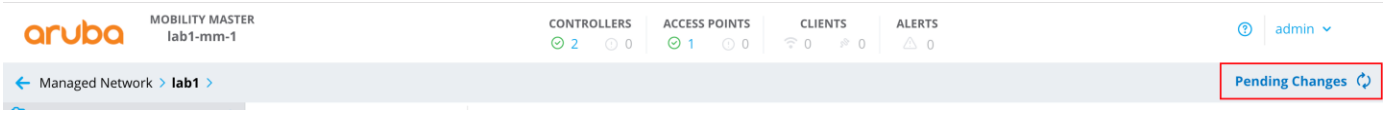
第1步: 找到 Managed Networks - > labX -> Authentication，在右侧的“AAA Profile”列表中找到“lab1-portal_aaa_prof“



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



第2步：点击右上角“Pending Changes”保存配置



4.5 验证结果

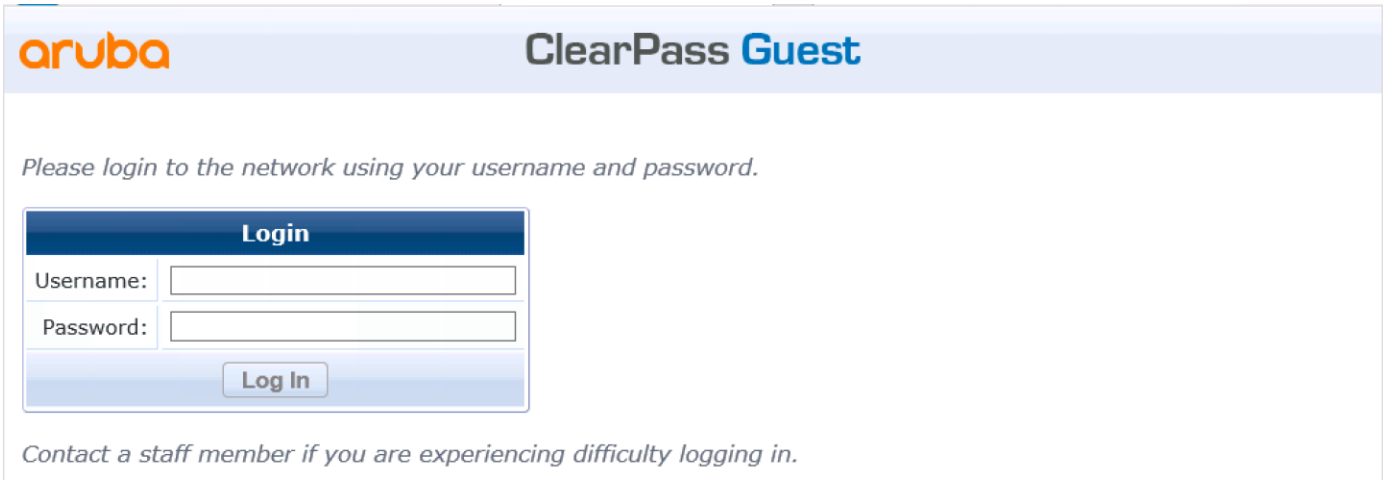
第1步：远程登录到 Wi-Fi 测试客户端 10.X.50.102，连接到 SSID：labX-portal。（X：1…6）

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 on number of users. Please be patient ....

Users
-----
    IP            MAC            Name     Role                 Age(d:h:m)  Auth  VPN link  AP name          Roaming   Essid/Bssid/Phy                 Profile             Forward mode  Type   Host
 Name  User Type
---------  ------------  ------  ----  ---------  ----  --------  -------  -------  ---------------  -------  ------------  ----  ----
10.1.20.102  7c:7a:91:46:52:b7           lab1-portal-guest-logon  00:00:00                94:b4:0f:c1:3f:e0  Wireless  lab1-portal/94:b4:0f:93:fe:11/a-VHT  lab1-portal_aaa_prof  tunnel        Win 8
       WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/171 Free:2/170 Dyn:3 AllocErr:0 FreeErr:0
```

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。

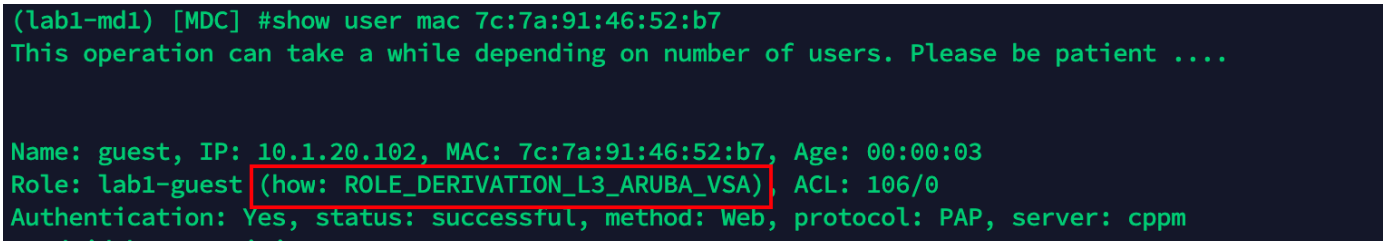
- ✓ 用户名：guest
- ✓ 密码：aruba123



第4步：远程登录到无线控制器，（X：1…6）

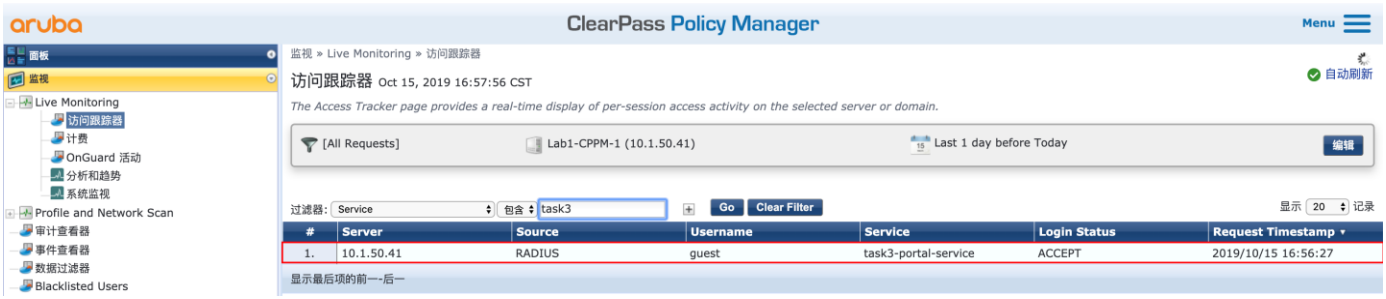
✓ 查看用户在 MD 上的状态：Name（用户名）、Role（角色）、Auth（认证方式）

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



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

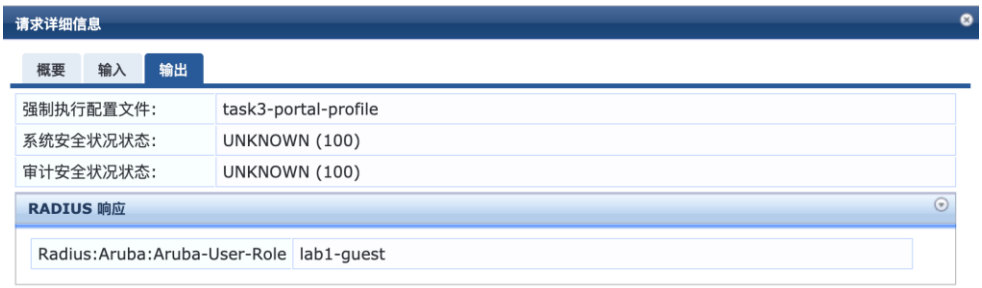
✓ 看到认证成功记录



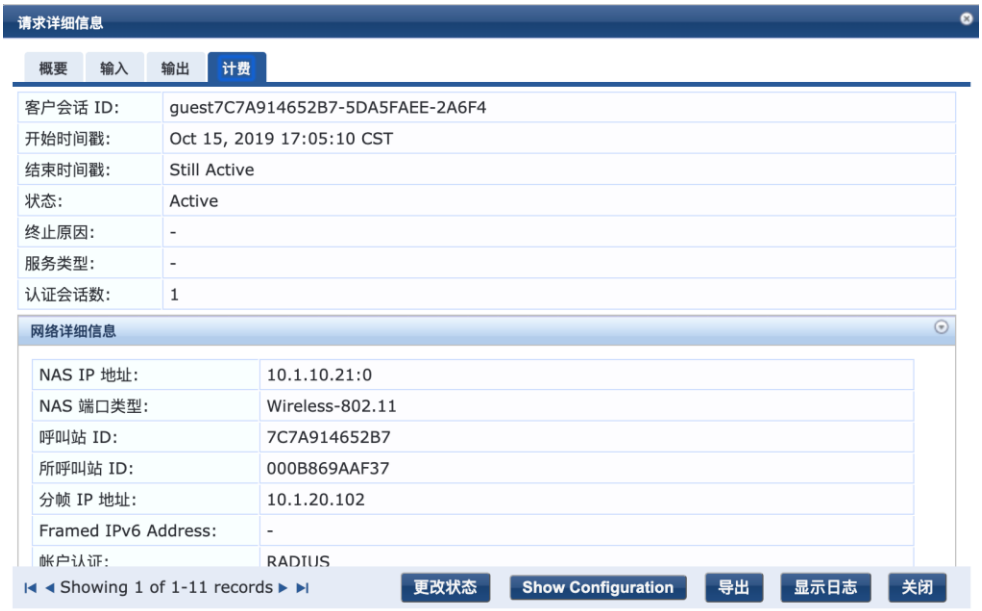
✓ 点击这条认证记录，查看“概要”选项卡内容，观察，可以看到哪些信息

✓ 点击“输入”选项卡内容，观察，可以看到哪些 radius 信息

✓ 点击“输出”选项卡内容，观察，可以看到哪些 radius 信息



✓ 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: _____

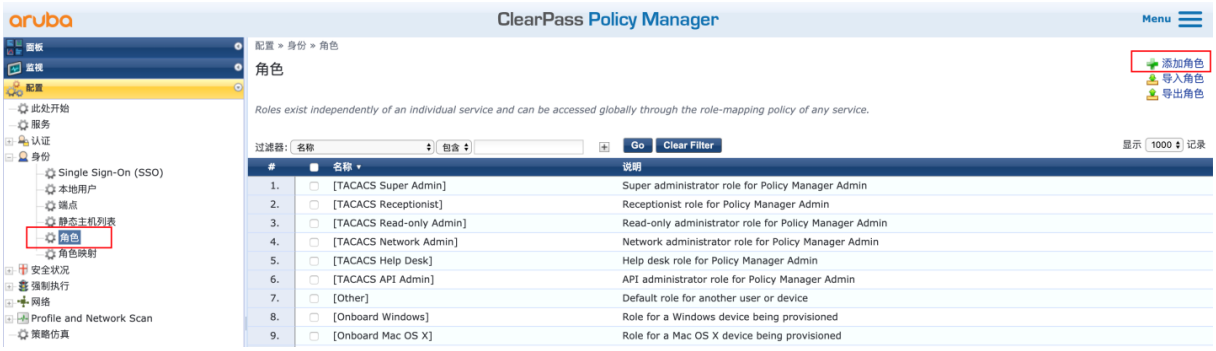
✓ 针对802.1x认证的用户，我们设计两种类型的用户，例如领导和普通员工，利用Radius的授权功能，返回什么样属性给到控制器，从而实现不同的访问权限?

答案: _____

5.3 ClearPass 配置

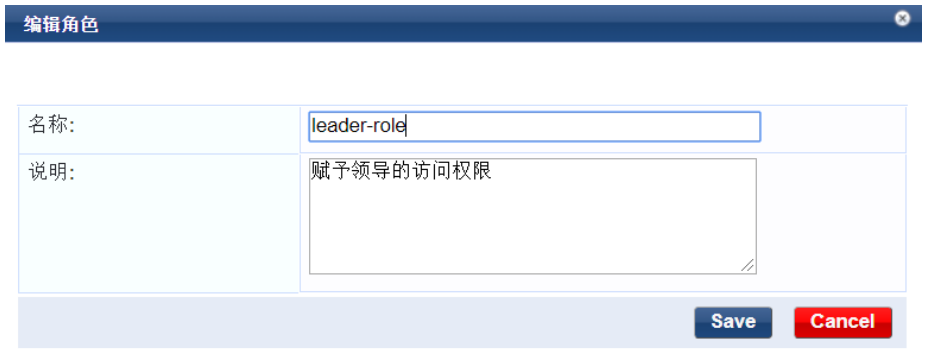
5.3.1 添加本地账号和角色

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:



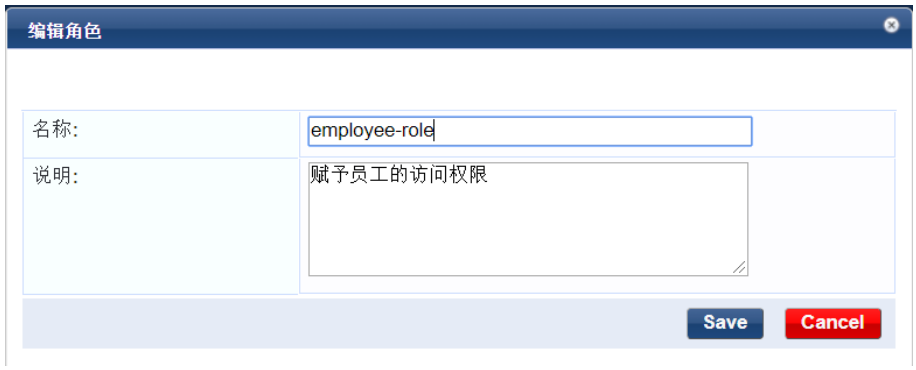
在添加新角色1的窗口中，输入下面的参数：

- ✓ 名称：leader-role
- ✓ 说明： 赋予领导的访问权限

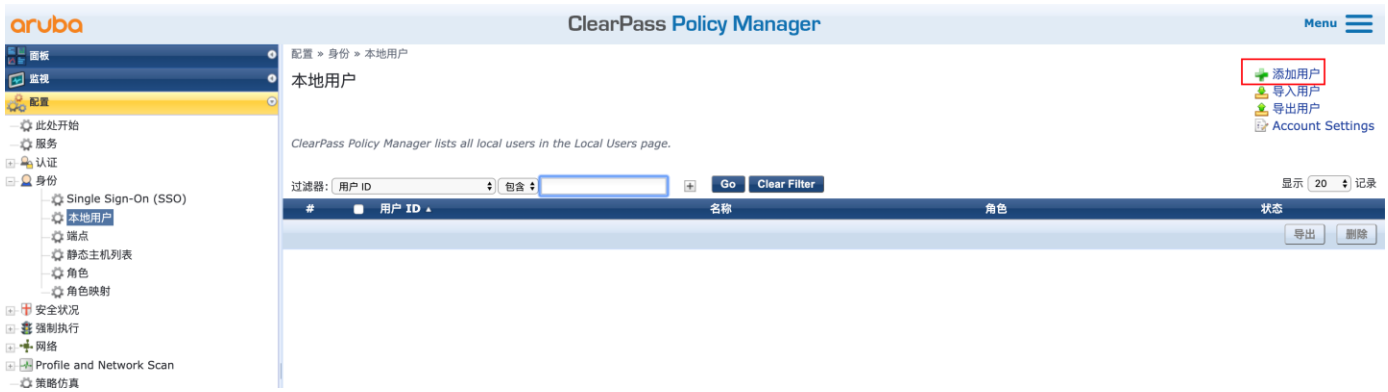


在添加新角色2的窗口中，输入下面的参数：

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

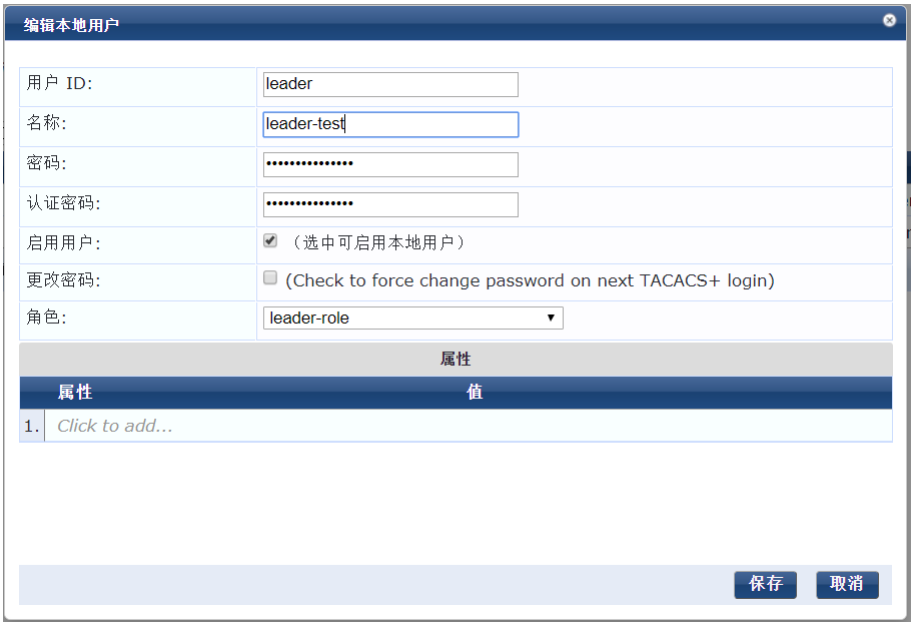


第2步：找到 配置 - > 身份 - >本地用户，点击右上角的“添加用户”按钮，增加两个用户账号：



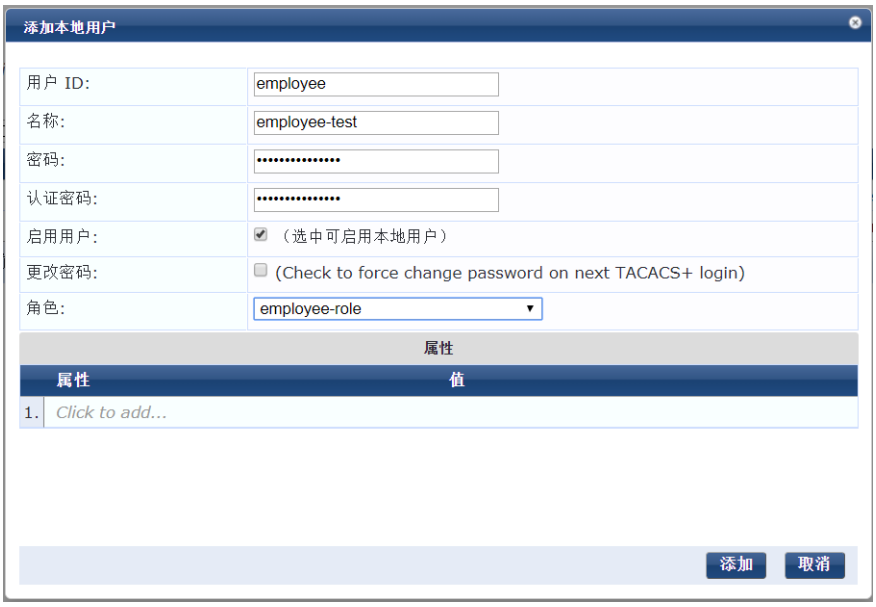
在添加账号1的窗口中，输入下面的参数：

- ✓ 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）

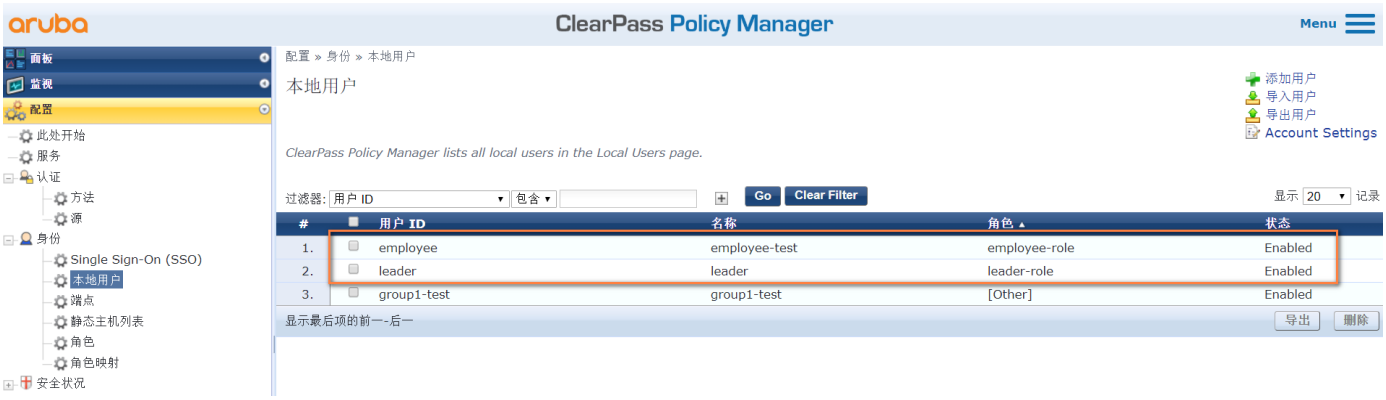


在添加账号2的窗口中，输入下面的参数：

- ✓ 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）



配置总览：

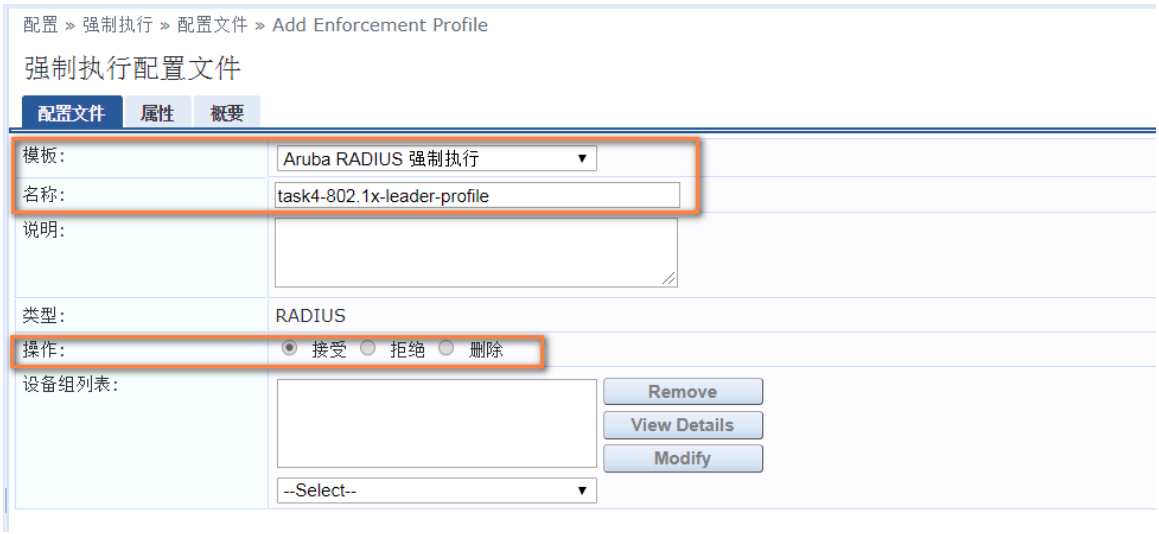


5.3.2 添加认证服务

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：

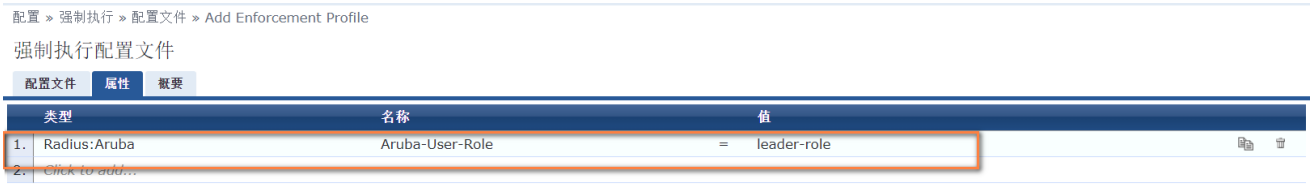
在配置文件（第一个）选项卡中，输入下面的参数：

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



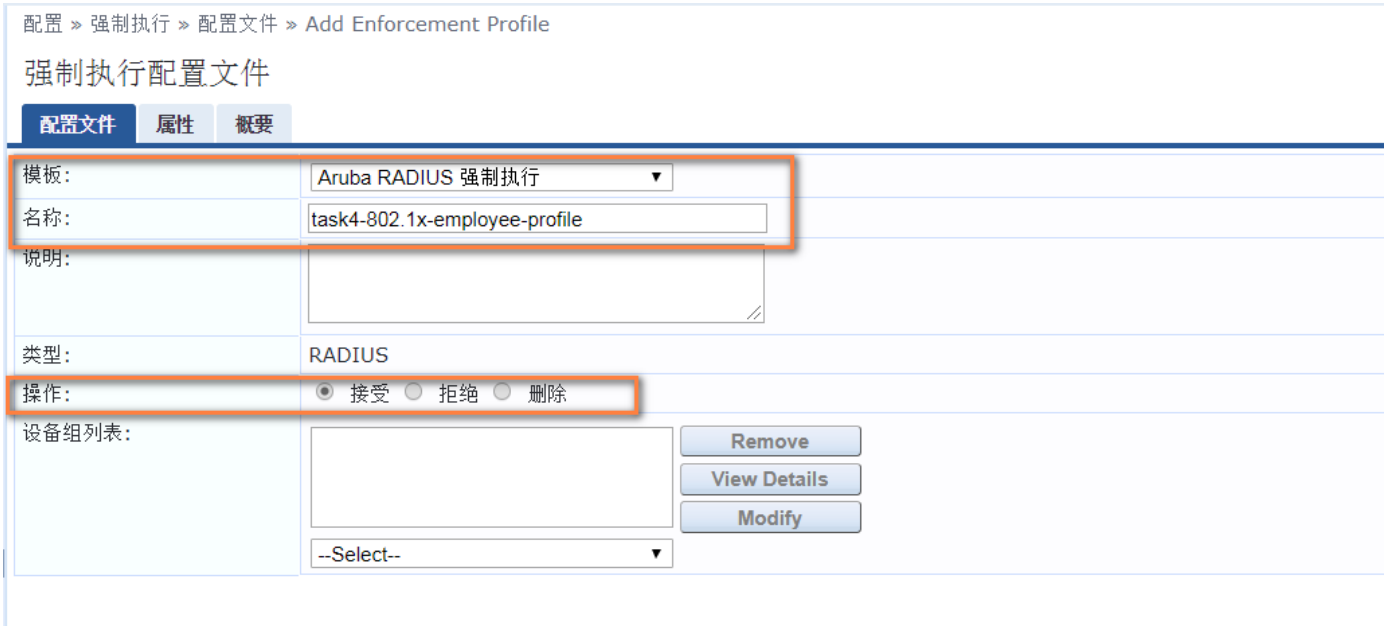
在属性选项卡中，输入下面的参数：

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



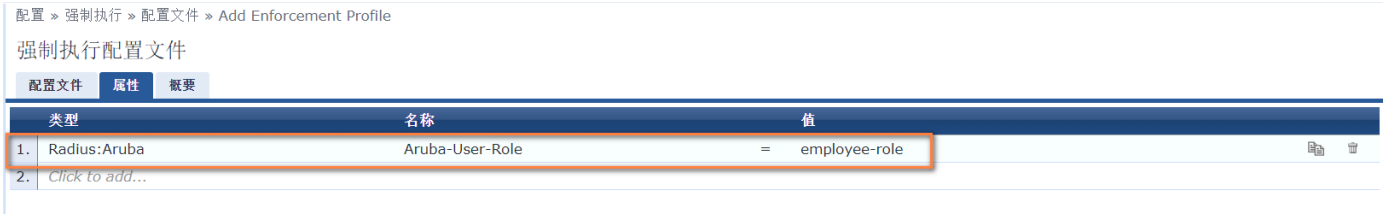
在配置文件（第二个）选项卡中，输入下面的参数：

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

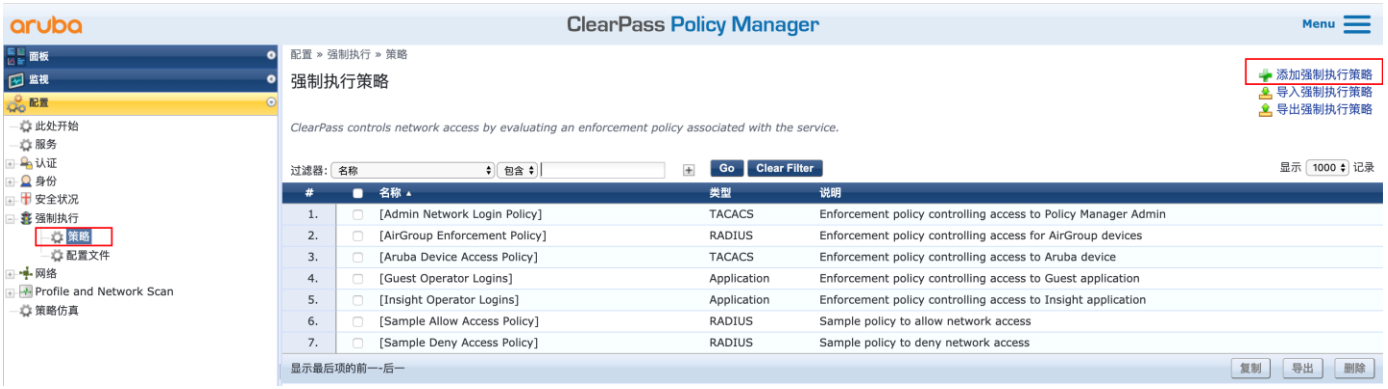


在属性选项卡中，输入下面的参数：

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

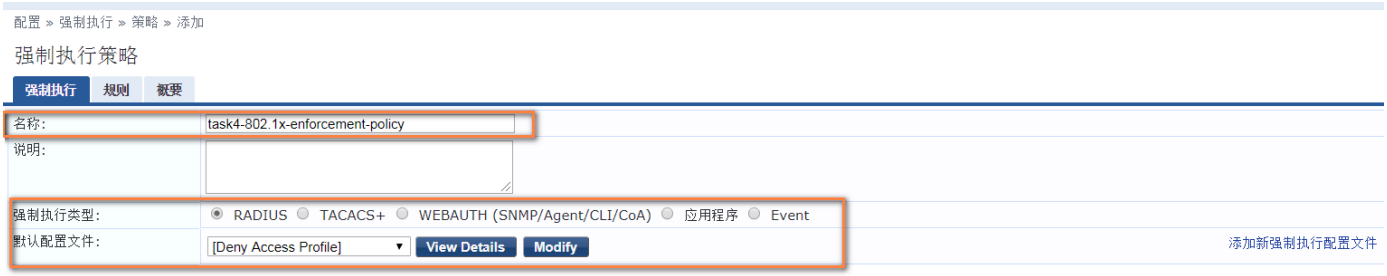


第2步：找到 配置 - > 强制执行 - > 策略，点击右上角的“添加强制执行策略”按钮，增加一个强制执行策略：



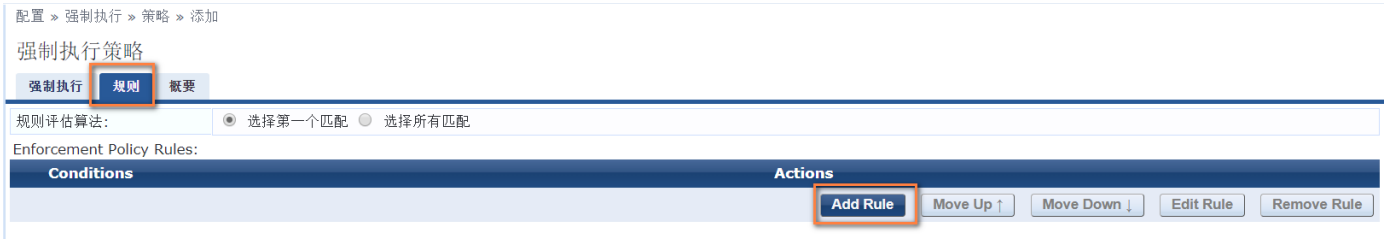
在强制执行选项卡中，输入下面的参数：

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



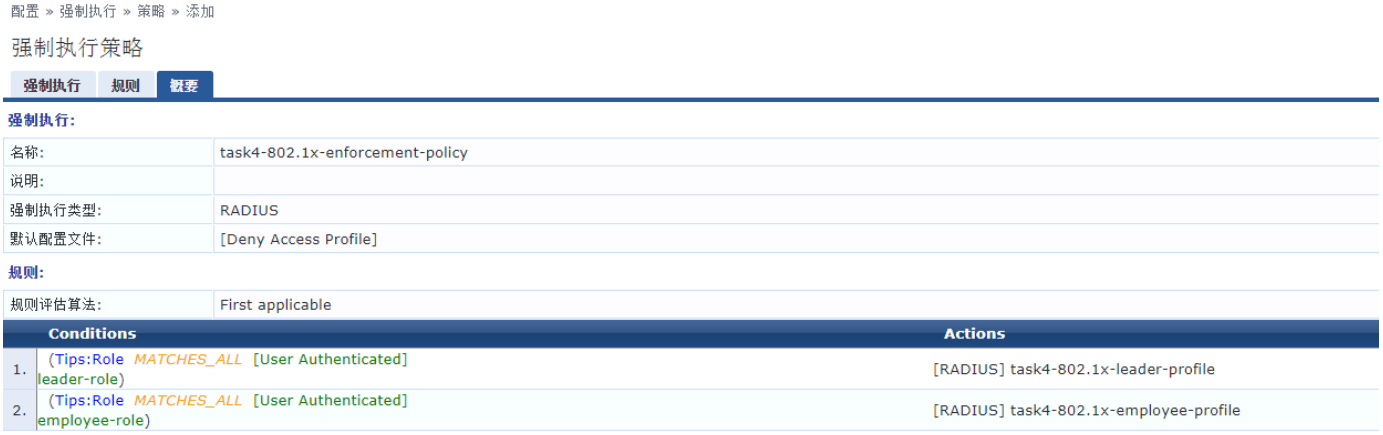
在规则选项卡中，输入下面的参数：

- ✓ 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

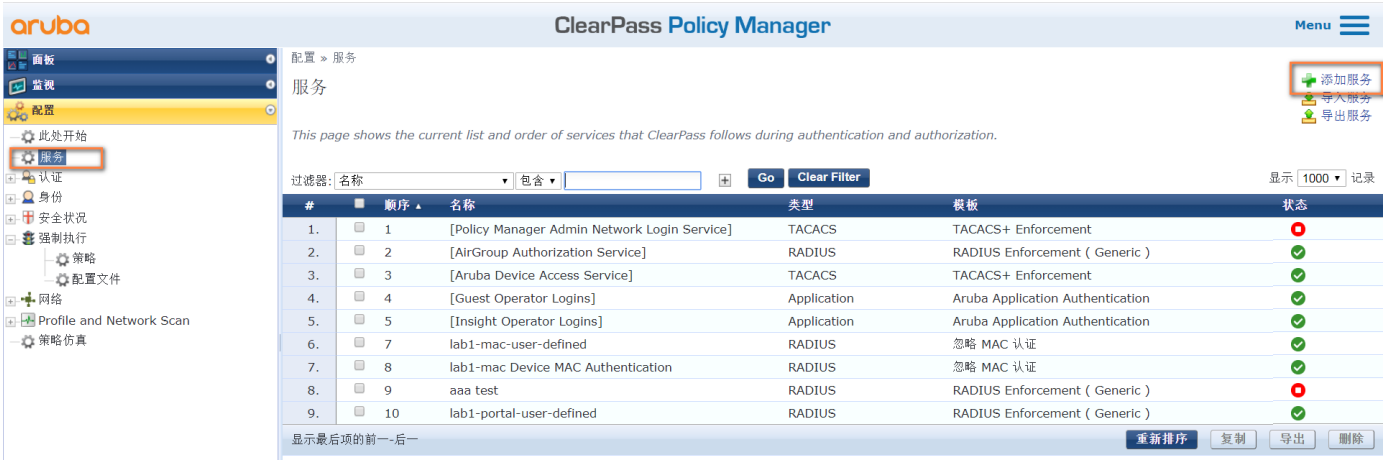


  - ■ 再添加第二个规则条件是 Tips Role MATCHES_ALL employee-role，[User Authenticated]
  - ■ 配置文件名： task4-802.1x-employee-profile

在概要选项卡中，对整体配置进行总览：



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：



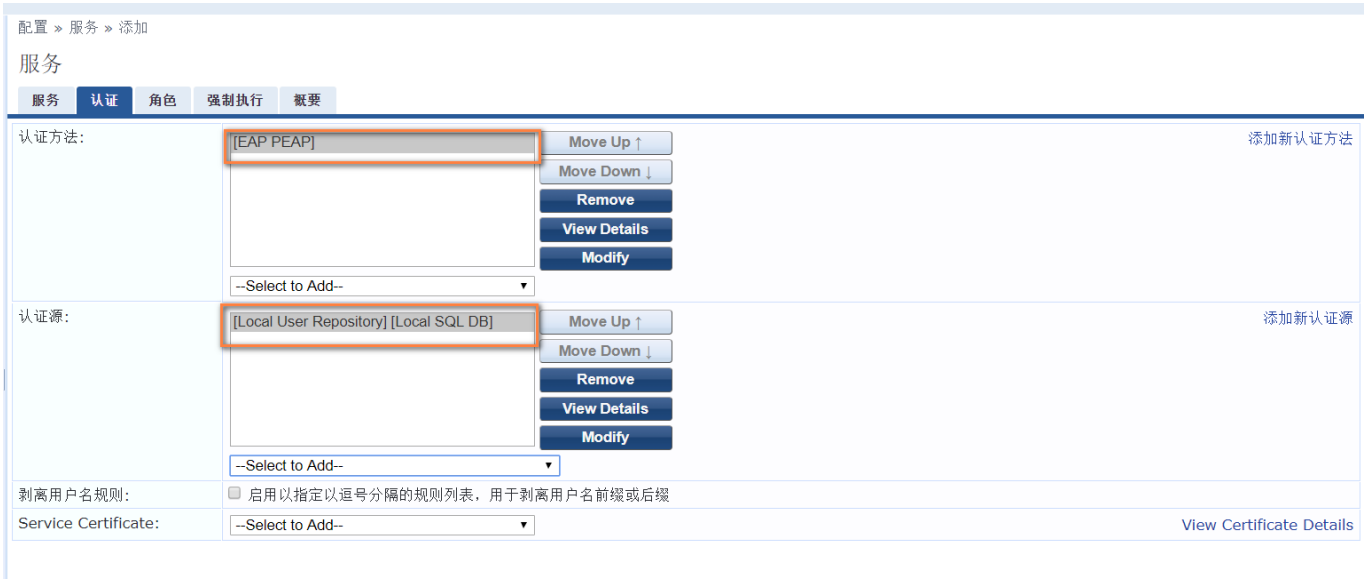
在服务选项卡中，输入下面的参数：

- ✓ 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）

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]



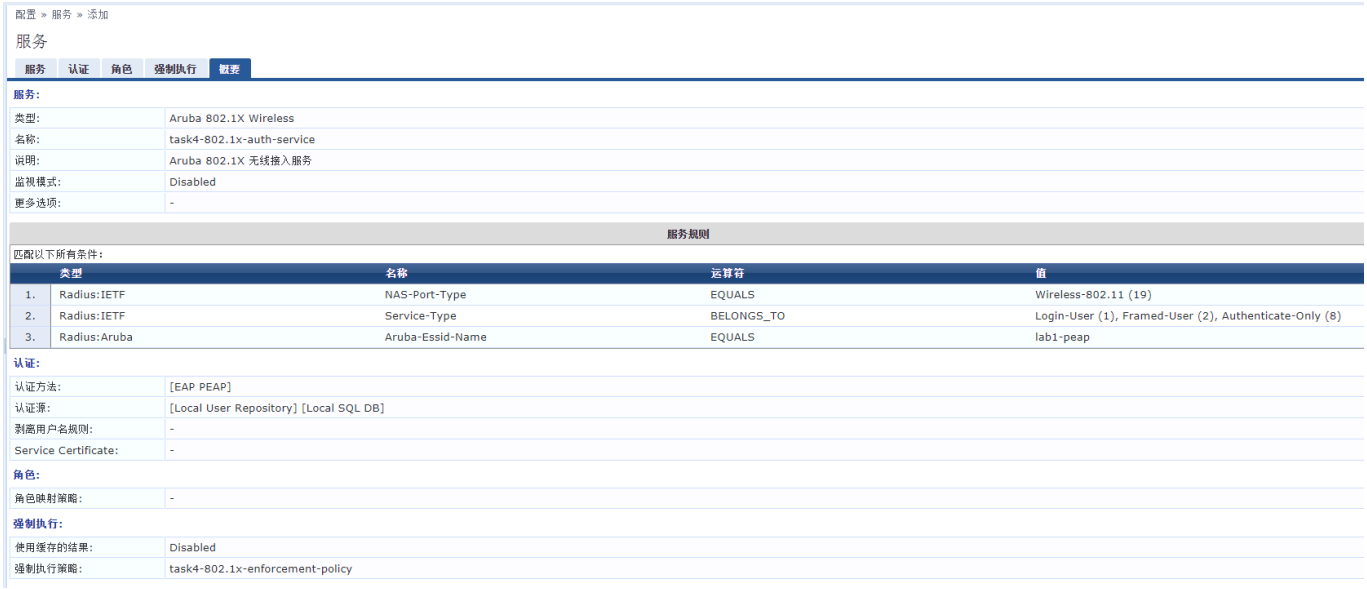
在角色选项卡中，暂时不做任何配置（详细内容可以参考高级介绍部分）

- 1、角色映射策略： 空

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）*

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 | 概要

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
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.	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	lab1-peap

认证：

认证方法：	[EAP PEAP]
认证源：	[Local User Repository] [Local SQL DB]
剥离用户名规则：	-
Service Certificate:	-

角色：

角色映射策略：	-

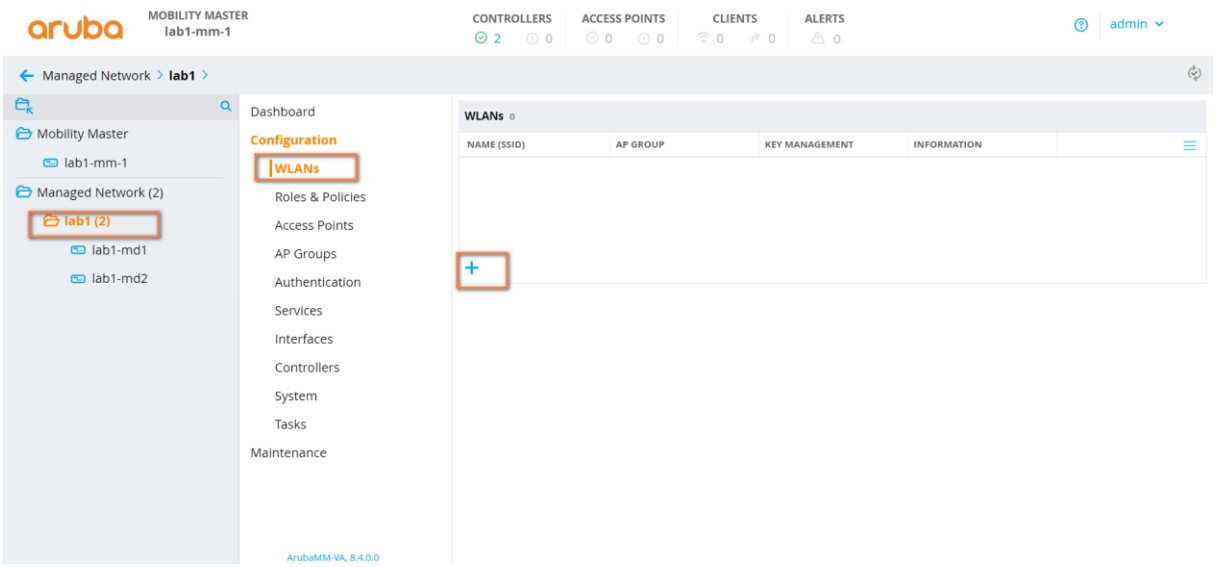
强制执行：

使用缓存的结果：	Disabled
强制执行策略：	task4-802.1x-enforcement-policy

5.4 控制器配置

5.4.1 添加无线信号

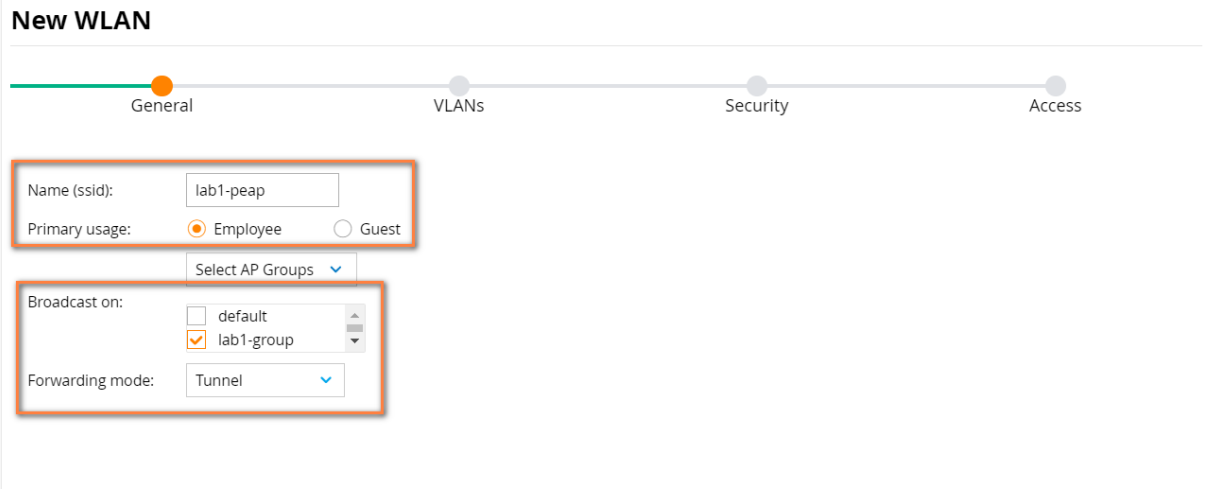
第1步：使用 Web 方式登录到 Mobility Master (10.X.50.11) （X： 1 ·····6），找到 Managed Network - > labX （X： 1 ·····6） -> Configuration -> WLANs 点击“+”进入创建一个新的无线配置向导



第2步：General 常规选项设置

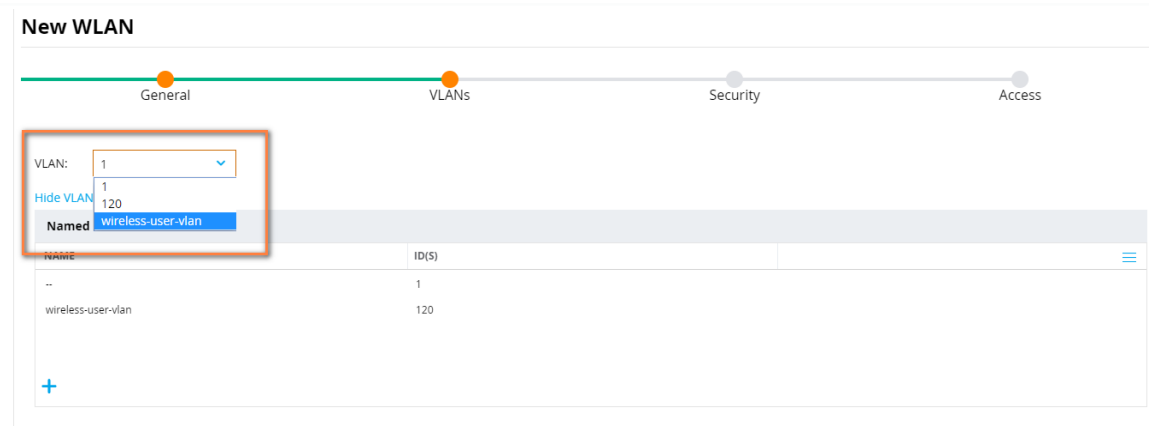
- ✓ 1、Name(ssid)： labX-peap （X： 1 ·····6）
- ✓ 2、Primary usage: Employee

- ✓ 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



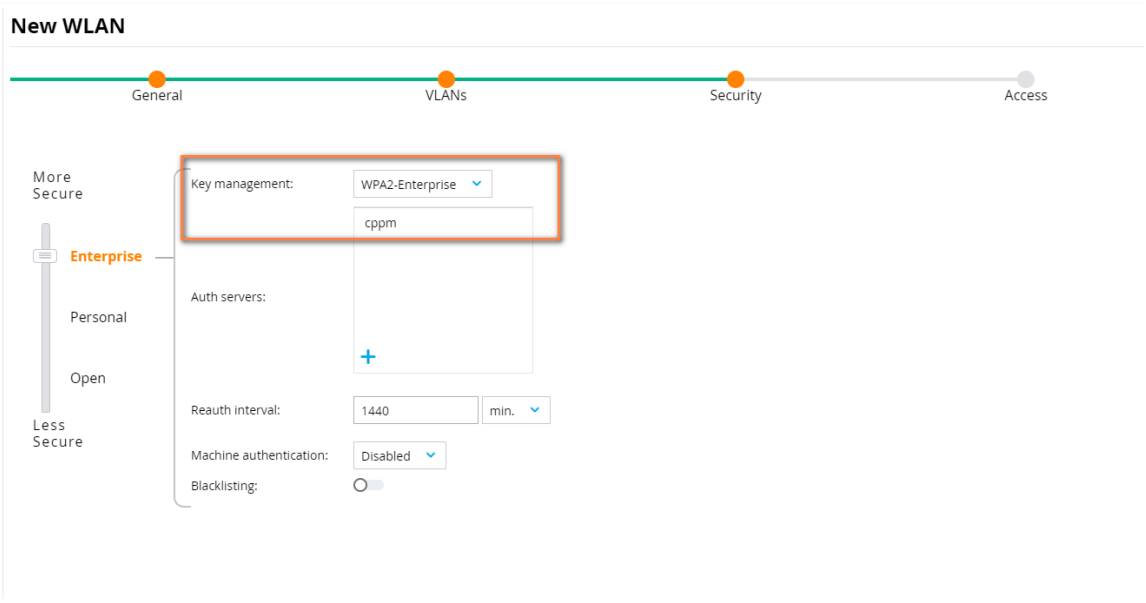
第3步: 配置用户的 VLAN

- ✓ VLAN： wireless-user-vlan



第4步: 安全选项设置

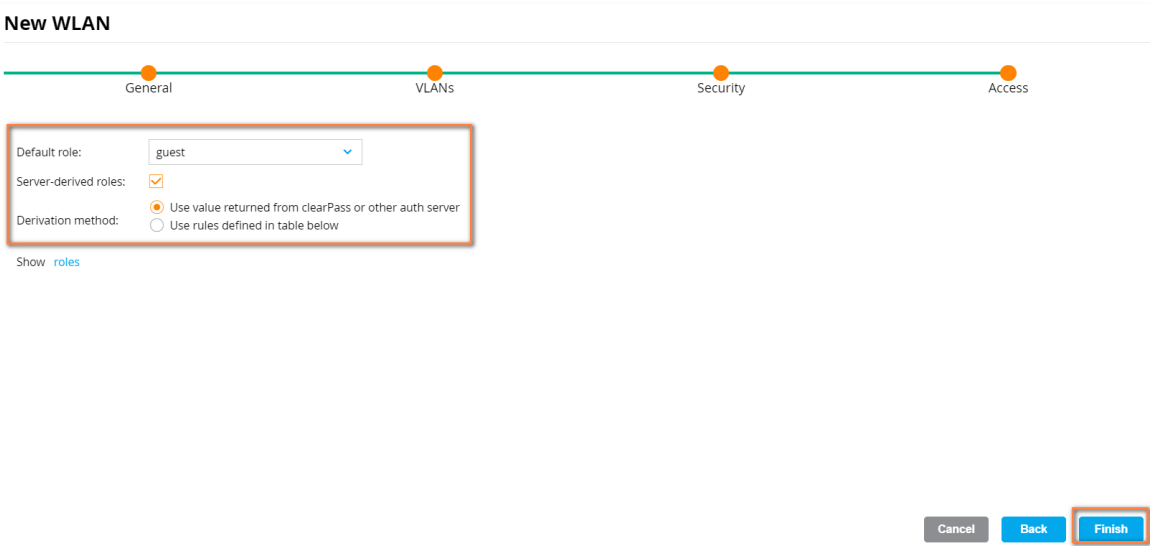
- ✓ 1、Key management： WPA2-Enterprise， 采用WPA2的企业认证方式
- ✓ 2、Auth server： cppm ， 即选择之前lab中创建好的RADIUS(cppm)认证服务器



第5步：访问权限设置

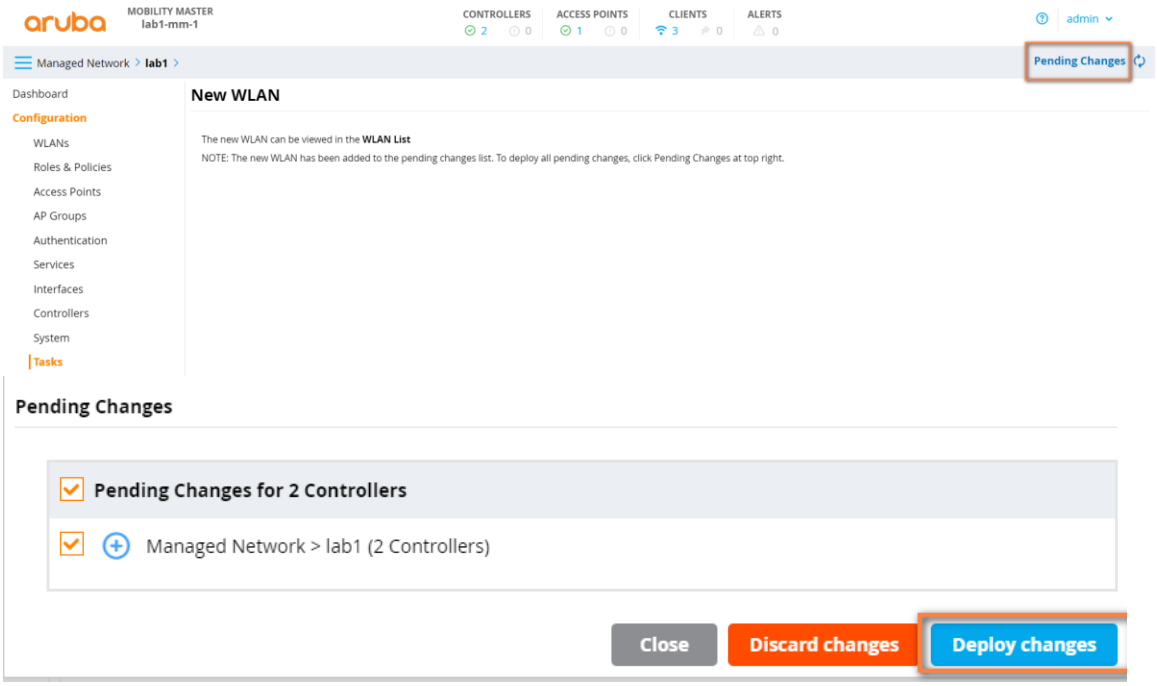
- ✓ 1、Default role： guest
- ✓ 2、Server-derived roles： 勾选
- ✓ 3、Derivation method： Use value returned from clearpass or other auth server
- ✓ 4、Finish：最后点击该按钮，完成配置

NOTE 在向导中，默认给予 802.1x 认证后的角色是 guest，我们可以采用 RADIUS（CPPM）的授权，返回 Aruba 的 VSA 属性给到控制器，从而用户认证后分配更高阶的角色（即该指派的角色优先级要高于原来的 guest 角色），从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。



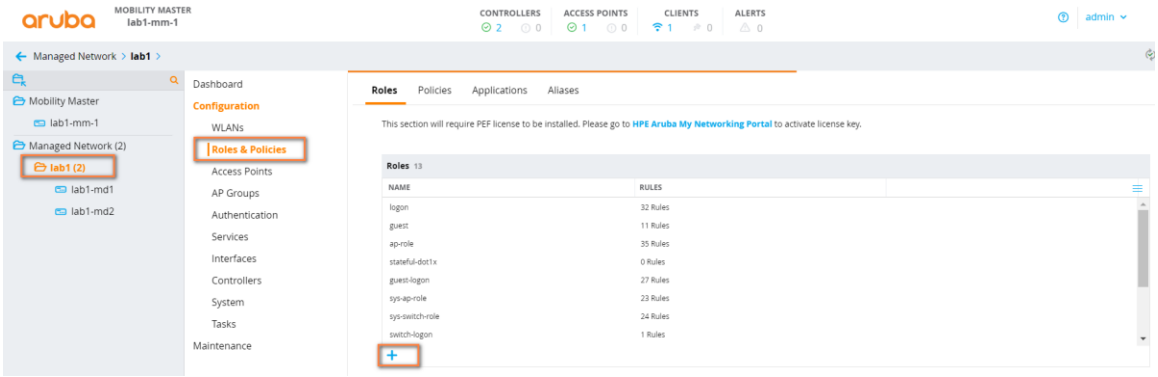
第6步：配置保存并同步给 md 设备

- ✓ 1、Pending Changes： 点击该按钮
- ✓ 2、Deploy changes： 点击该按钮

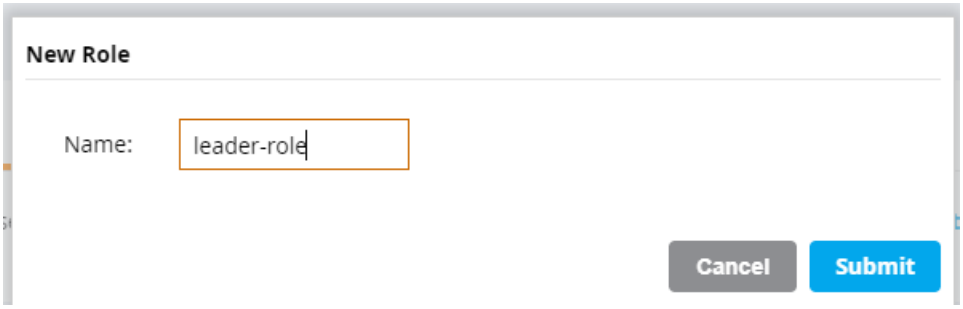


5.4.2 添加角色

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（leader-role 和 employee-role）。

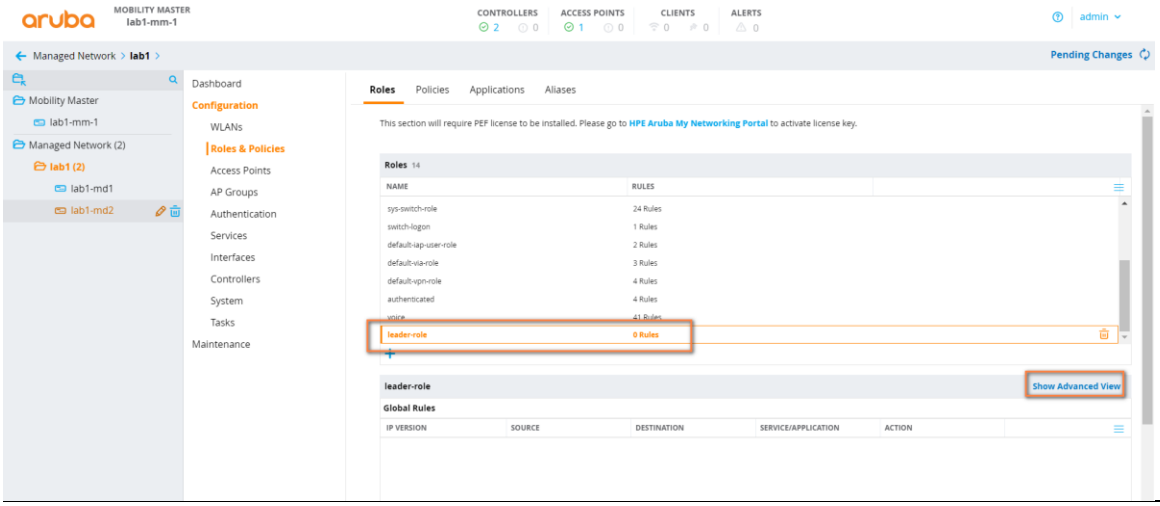


- ✓ Name： leader-role， 新建一个领导的角色

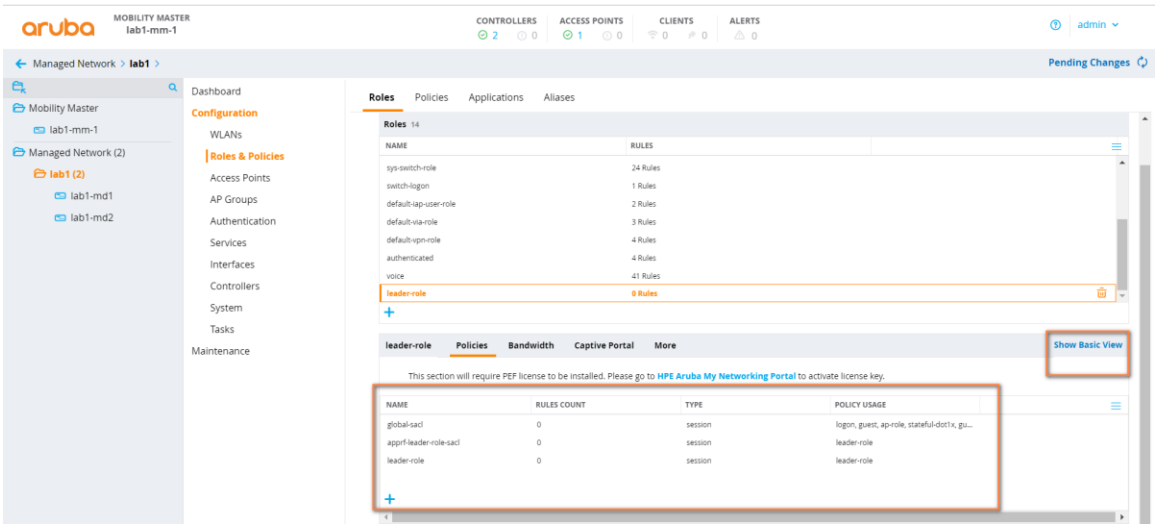


✓ 1、在roles里面，选择上一步创建好的leader-role

✓ 2、再点击右下角的show Advanced View



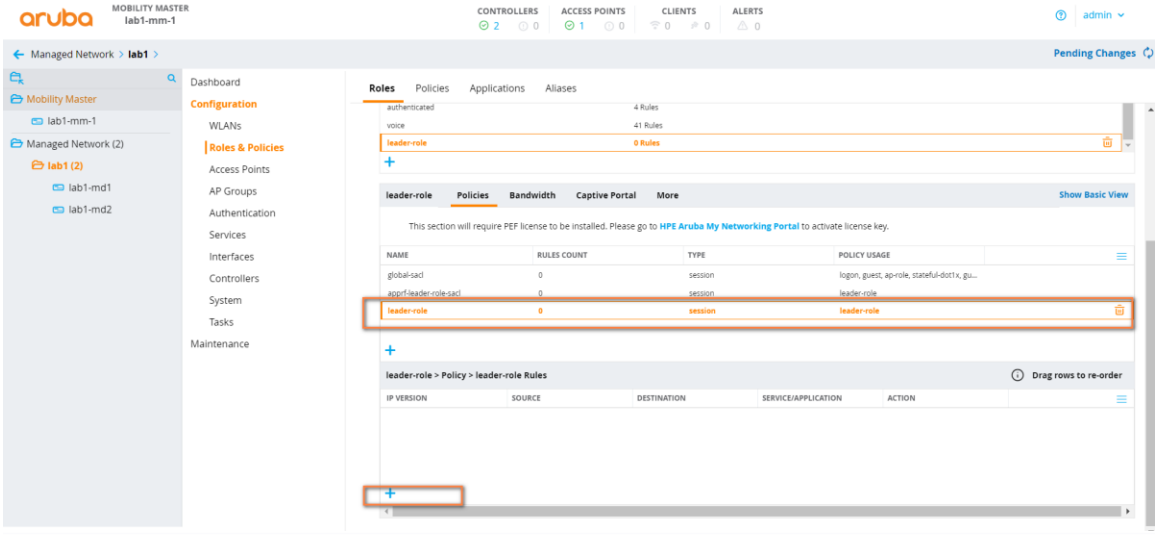
NOTE 需要事先在右上角的蓝色字体 admin 的下拉列表中选择 preferences， 勾选 show advanced profiles

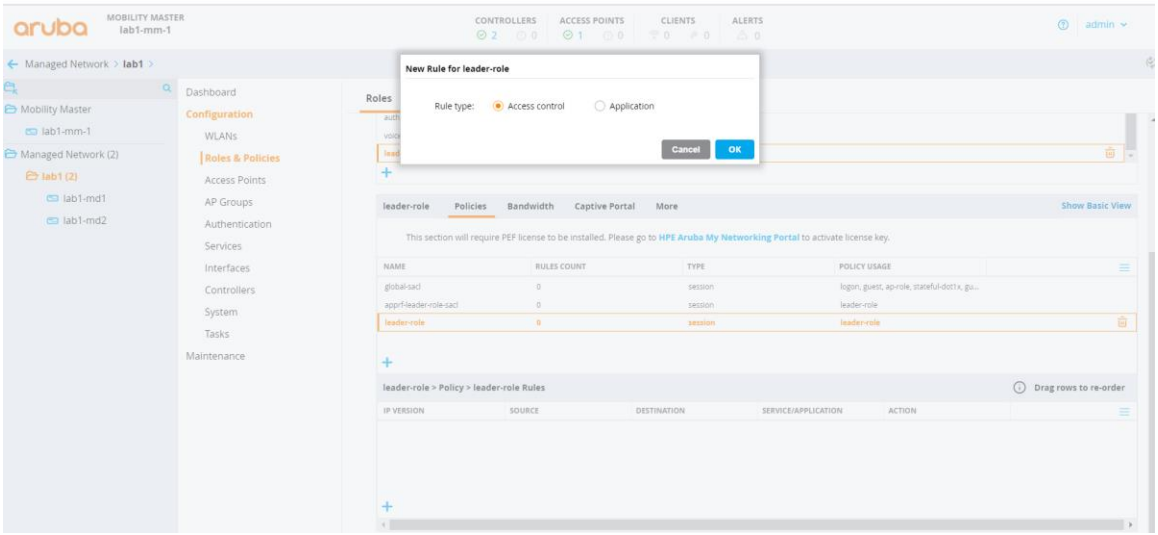


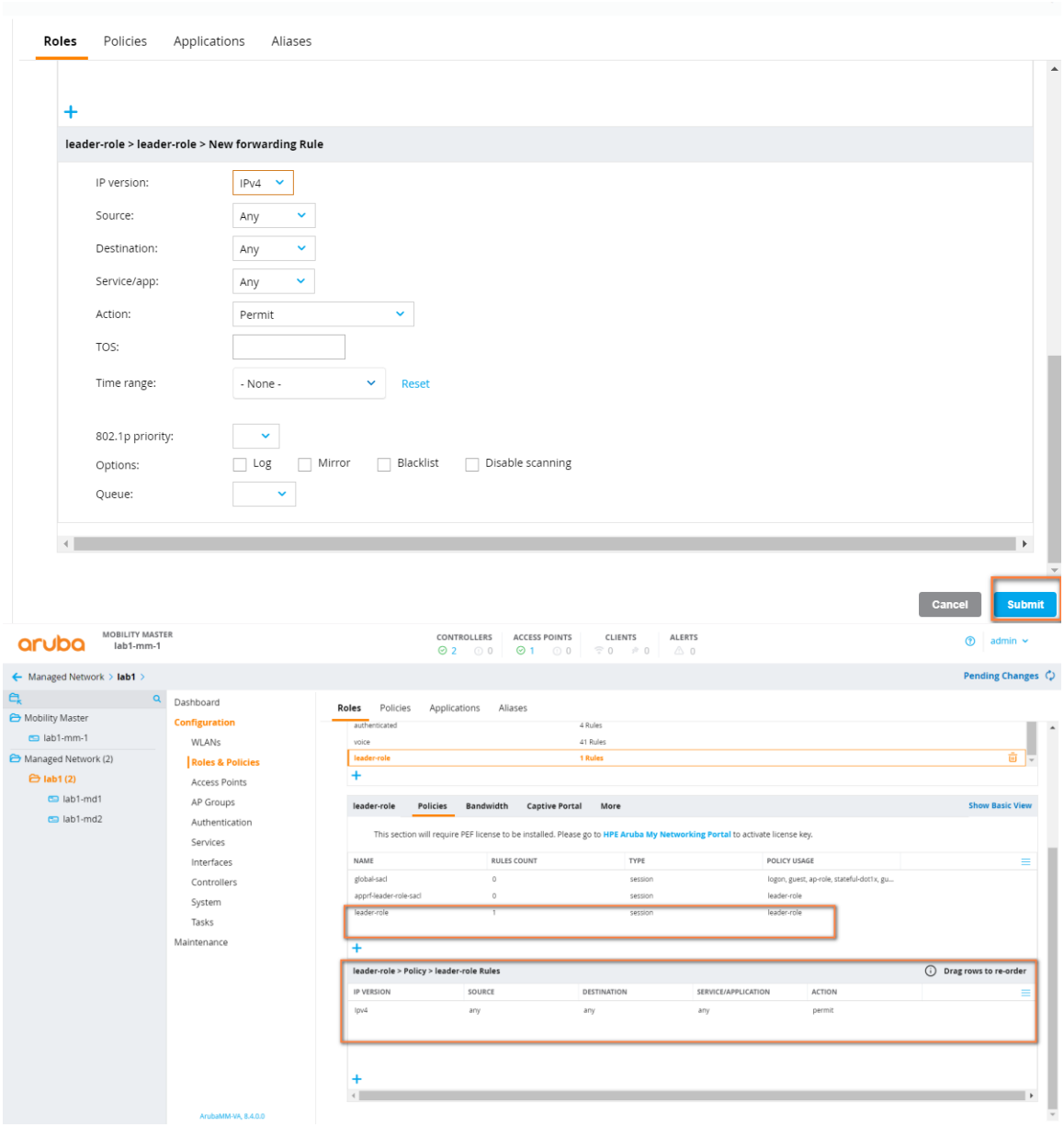
✓ 1、在policies窗口里面，选中并点击leader-role

✓ 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



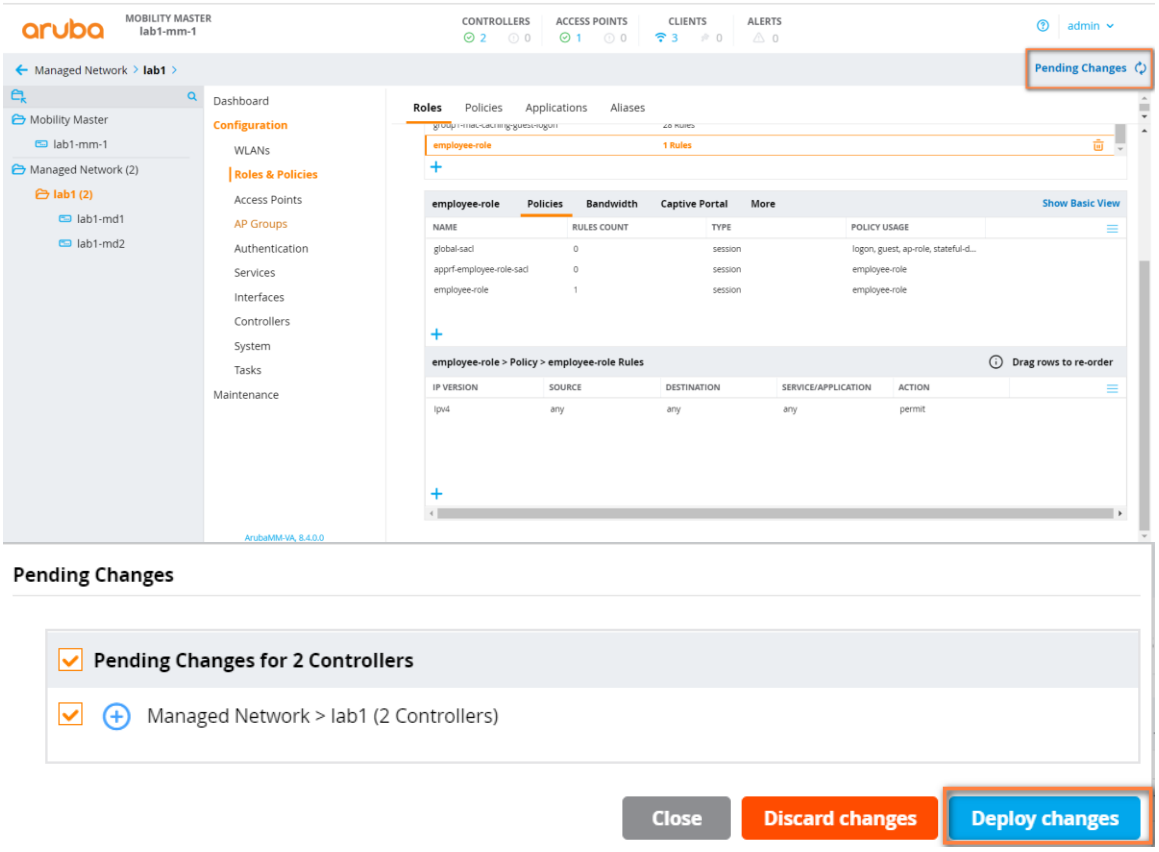




第2步:　采用上面同样的方法，我们再创建另外一个角色 employee-role，两种角儿之间我们可以设置不同的访问策略，从而设定两种不同的访问权限。

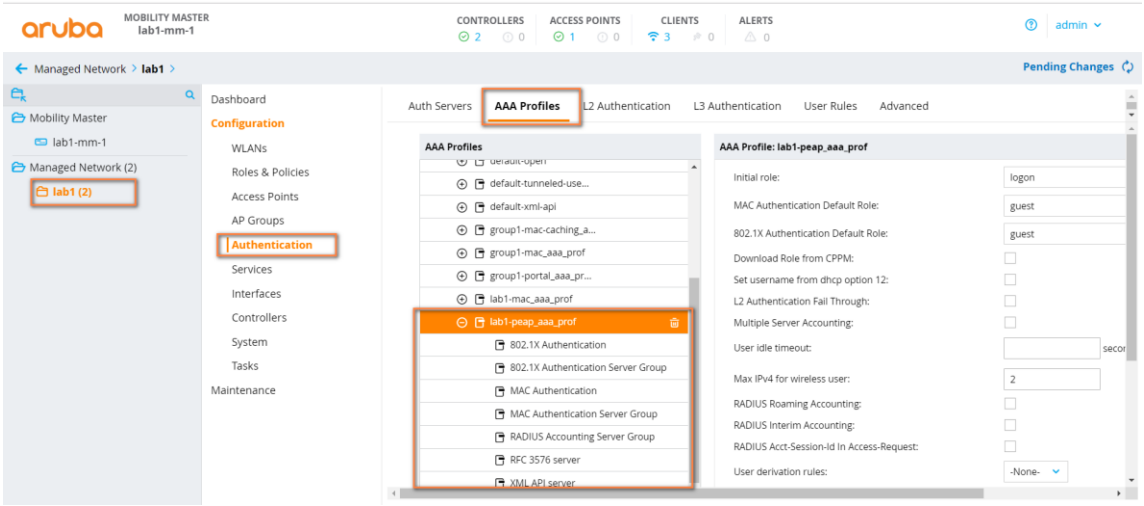
第3步:　配置保存并同步给 md 设备

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

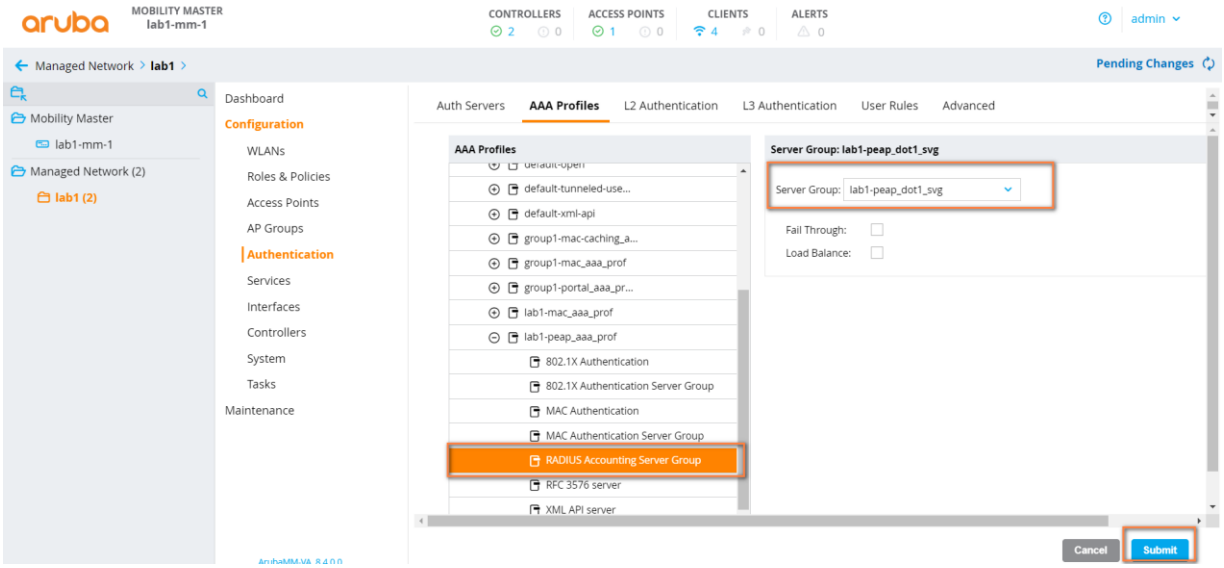


5.4.3 添加计费

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“+”展开所有的配置项

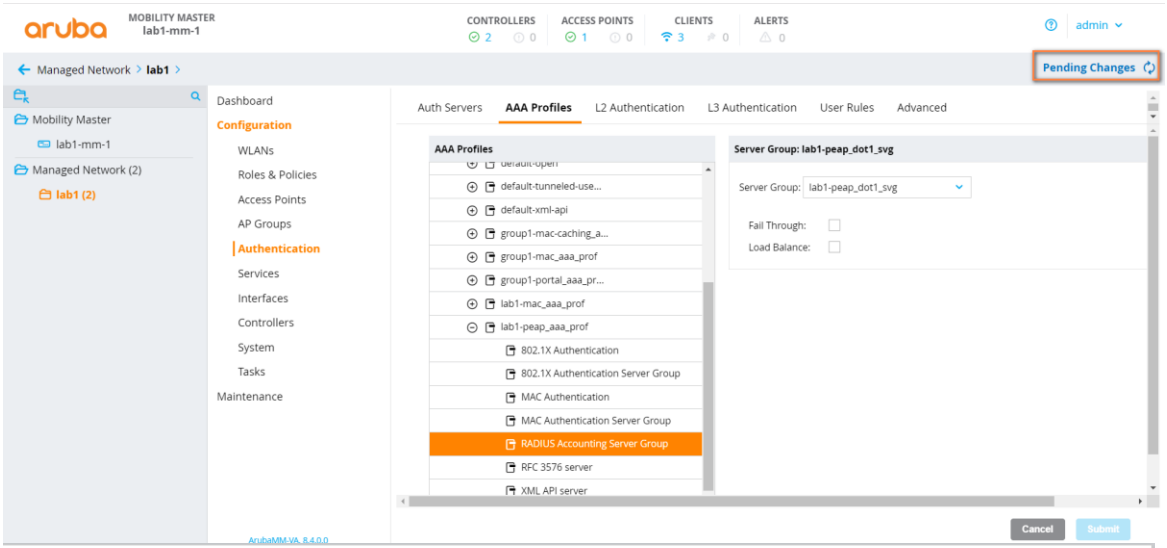


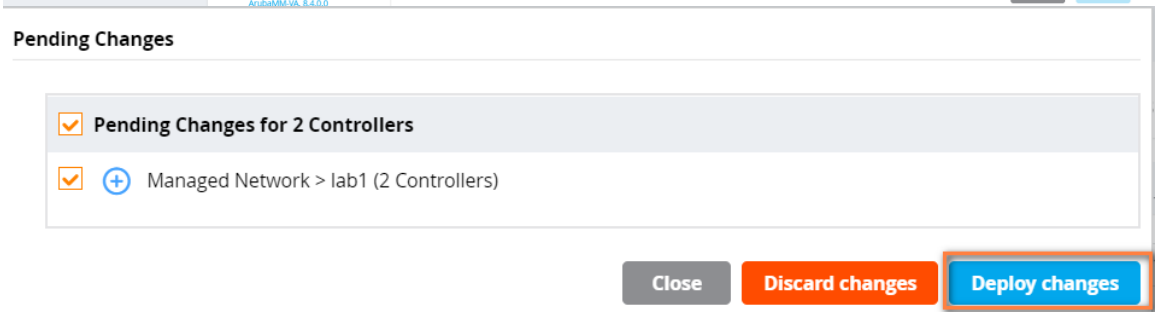
第2步： 选择 RADIUS Accounting Server Group，在右边配置窗口中，从 Server Group 下拉列表中选择之前向导已经创建的 labX-peap-dot1_svg. 点击右下角的 Submit 按钮。



第3步： 配置保存并同步给 md 设备

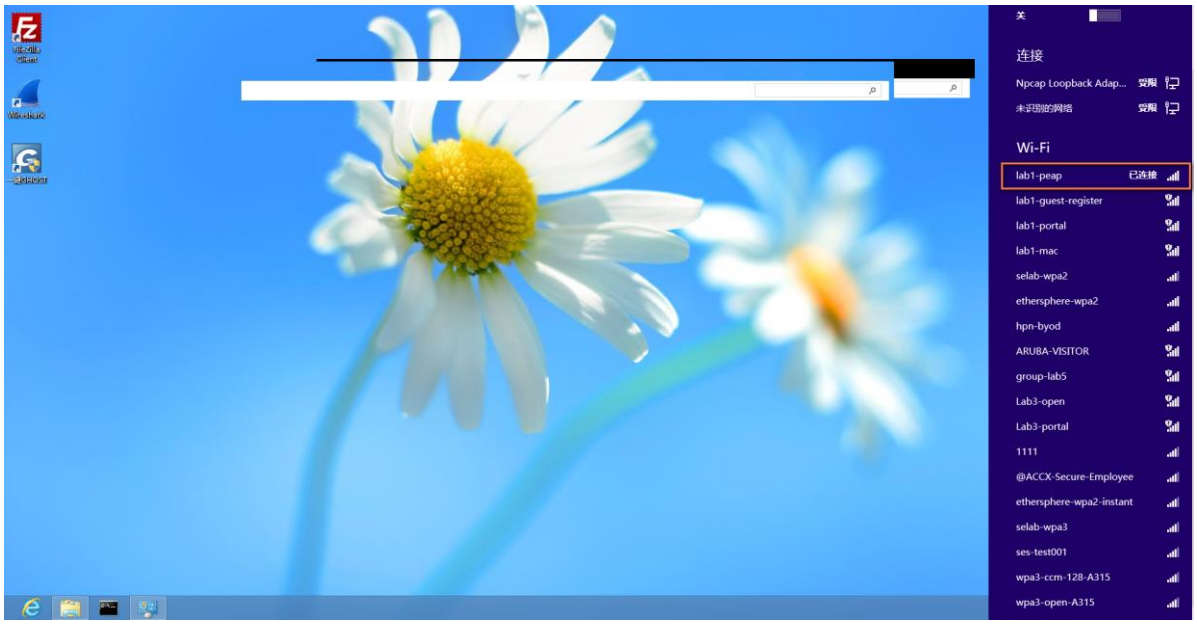
- ✓ 1、Pending Changes： 右上角点击该按钮
- ✓ 2、Deploy changes ： 点击该按钮





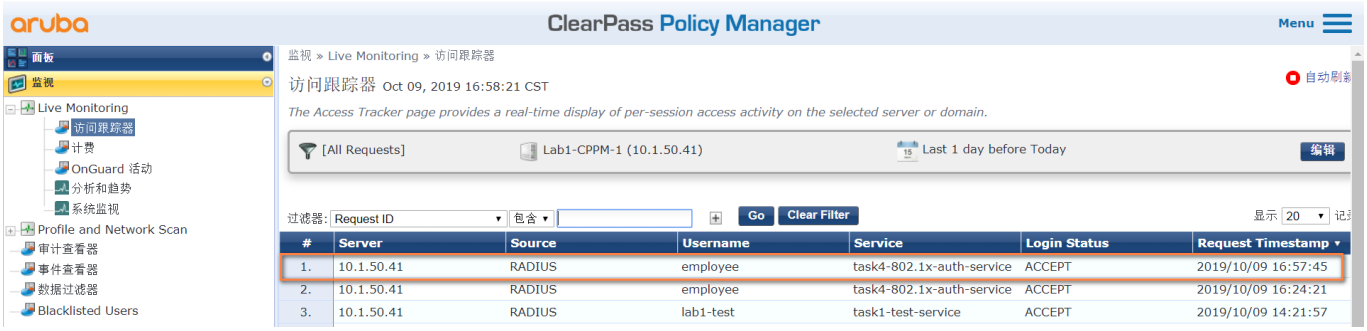
5.5 验证结果

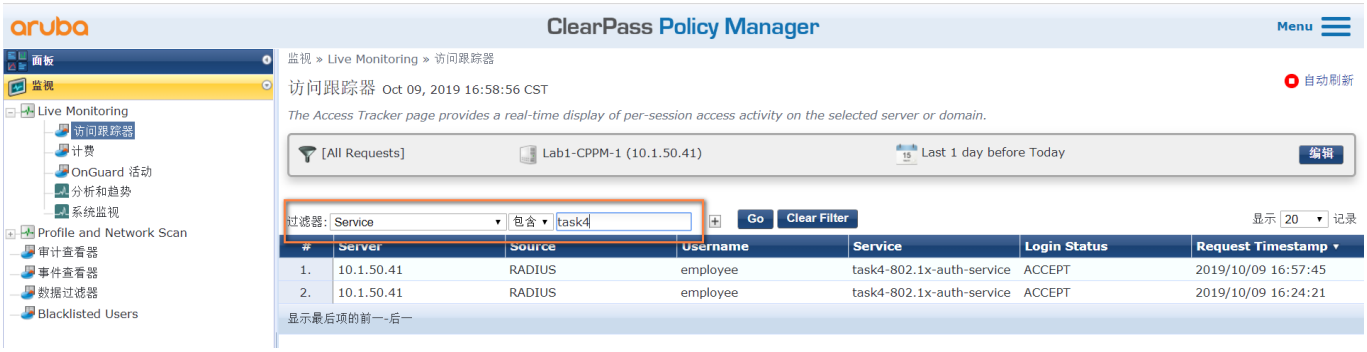
5.5.1 终端上的关联和登录记录



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。

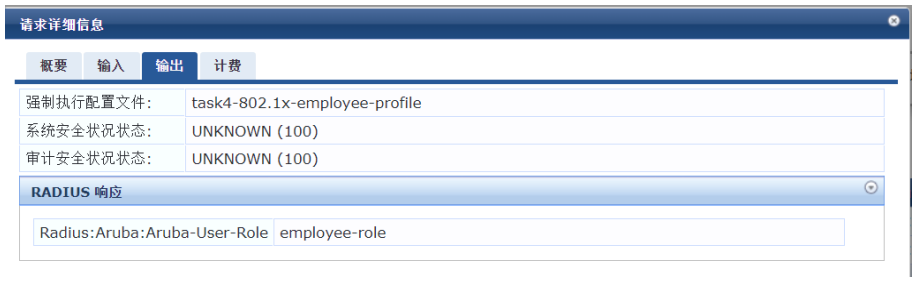




✓ 点击这条认证记录，查看“概要”选项卡内容，观察，可以看到哪些信息

✓ 点击“输入”选项卡内容，观察，可以看到哪些信息

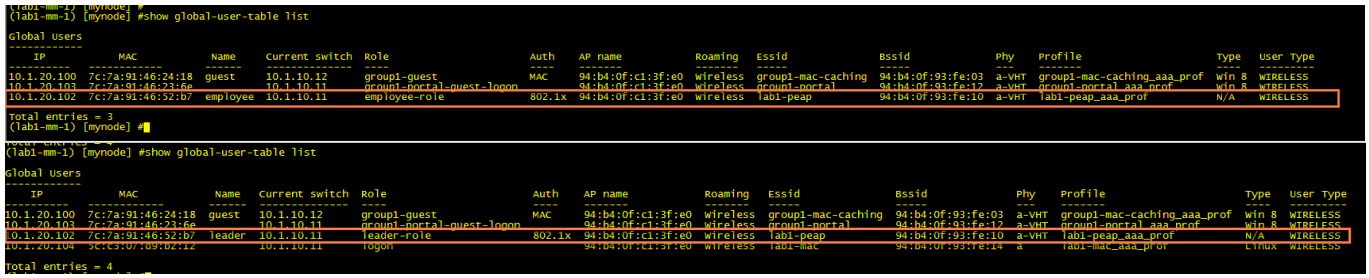
✓ 点击“输出”选项卡内容，观察，可以看到哪些信息



✓ 点击“计费”选项卡内容，观察，可以看到哪些信息

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

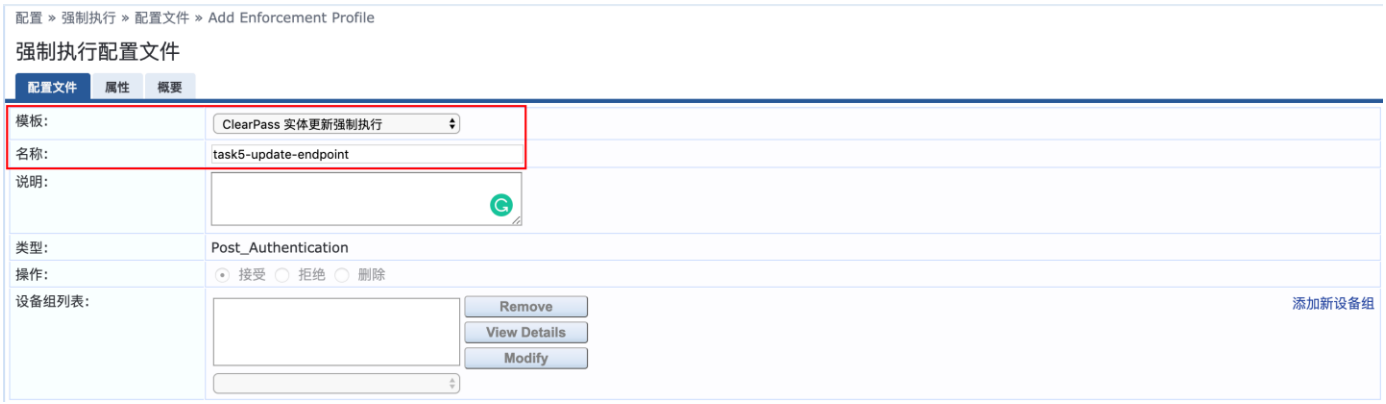
6.3.2 添加 mac caching 认证服务

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

✓ 名称：task5-update-endpoint



在“属性”选项卡中输入下面参数：

✓ 属性：

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

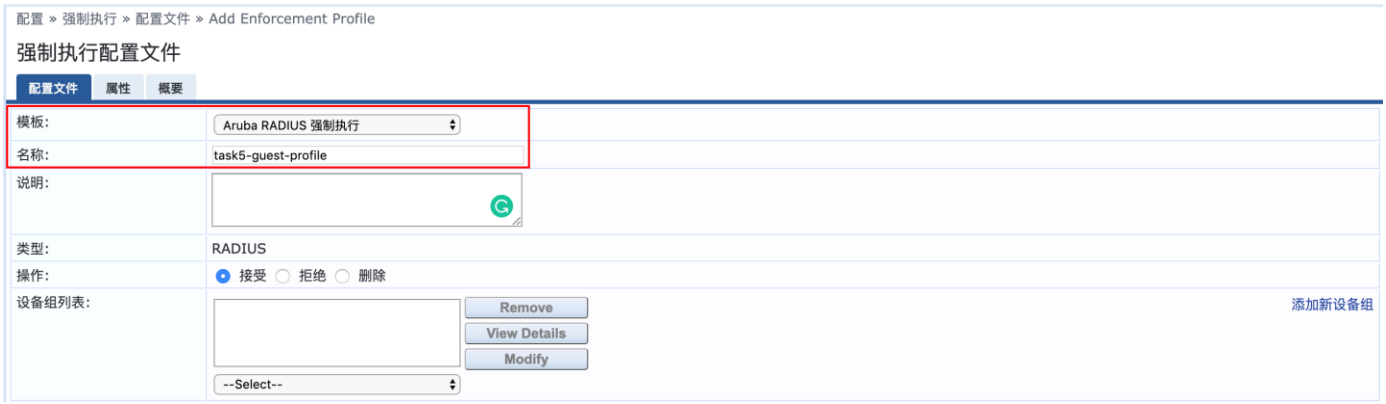
在“概要”选项卡中对配置进行总览：

✓ 概要：查看配置总览，并点击“保存”

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

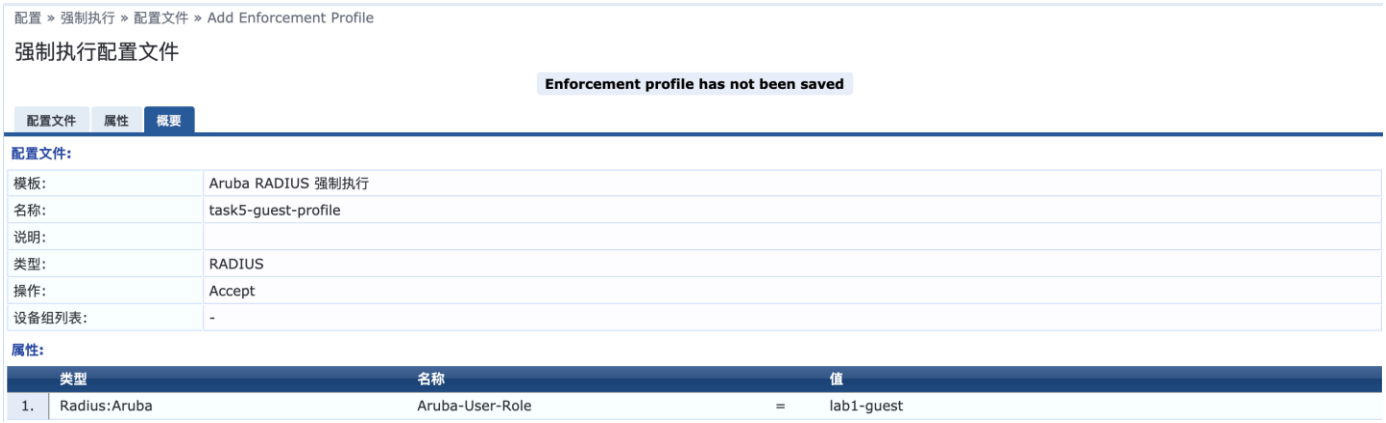


在“属性”选项卡中输入下面参数：

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

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”



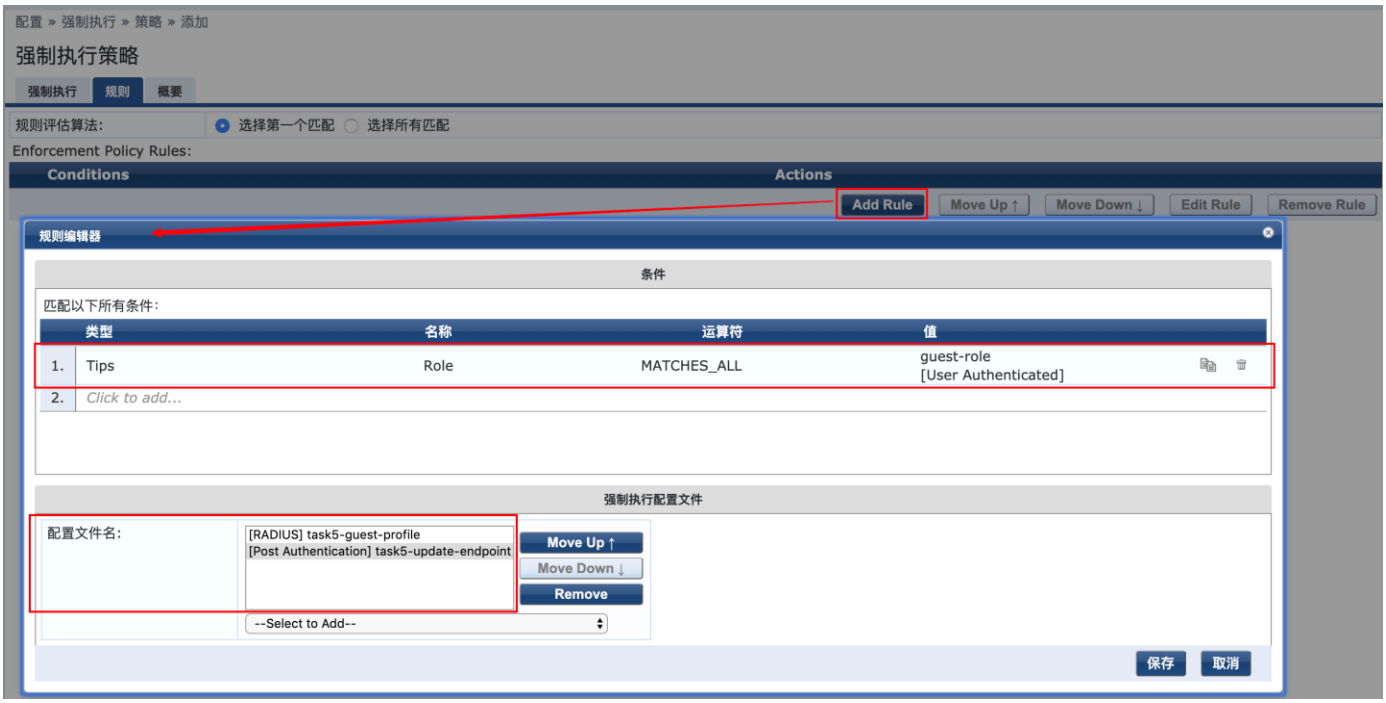
第3步：找到 配置 - > 强制执行 - > 策略，点击右侧的“添加强制执行策略”按钮，增加一个强制执行策略：

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]

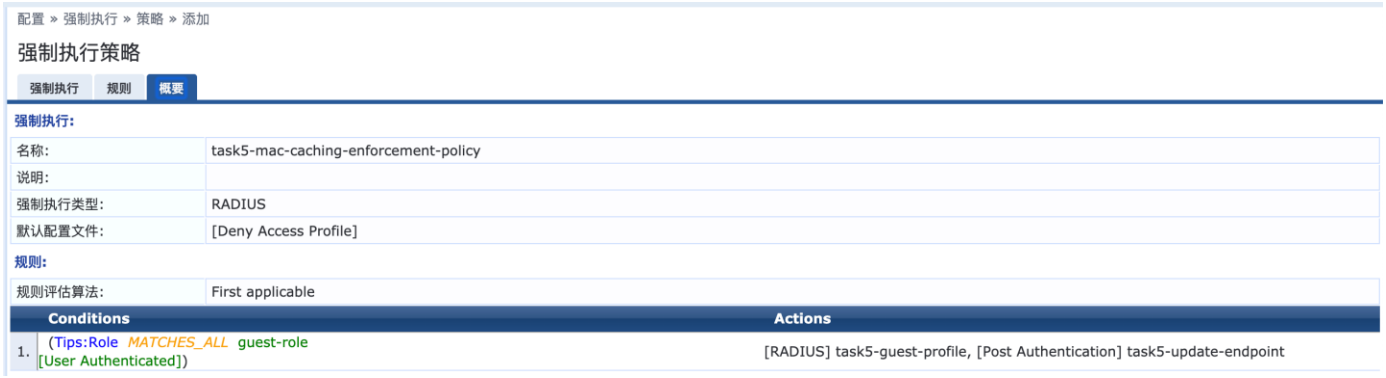
在“规则”选项卡中输入下面参数：

- ✓ 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)*



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”



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：

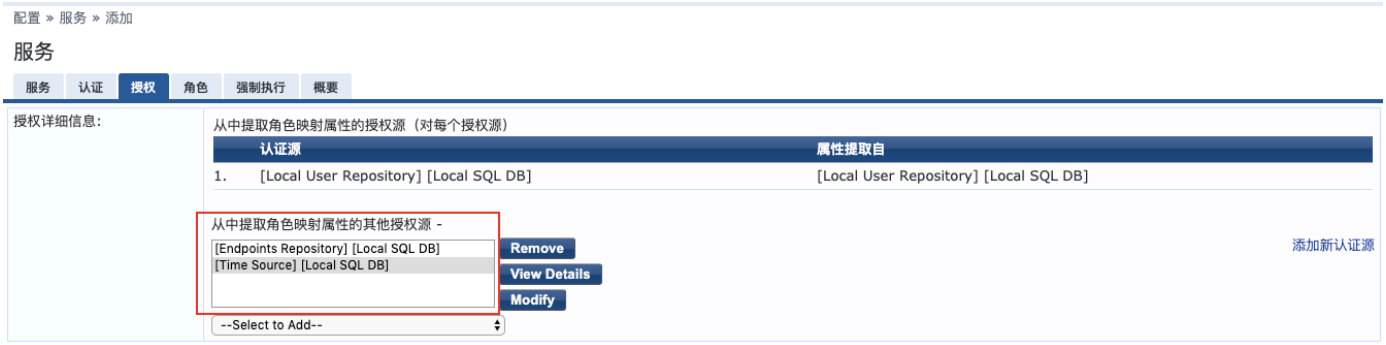
- ✓ 类型选择：RADIUS Enforcement (Generic)
- ✓ 名称填写：task5-mac-caching-service
- ✓ 更多选项：授权（开启）
- ✓ 服务规则：
  - ■ 1、Connect Client-Mac-Address NOT_EQUALS %{Radius:IETF:User-Name}
  - ■ 2、Radius:Aruba Aruba-Essid-Name EQUALS labX-mac-caching （X：1……6）

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]

在“授权”选项卡中配置如下参数：

- ✓ “[Endpoint Repository][Local SQL DB]”
- ✓ “[Time Source][Local SQL DB]”



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）*：

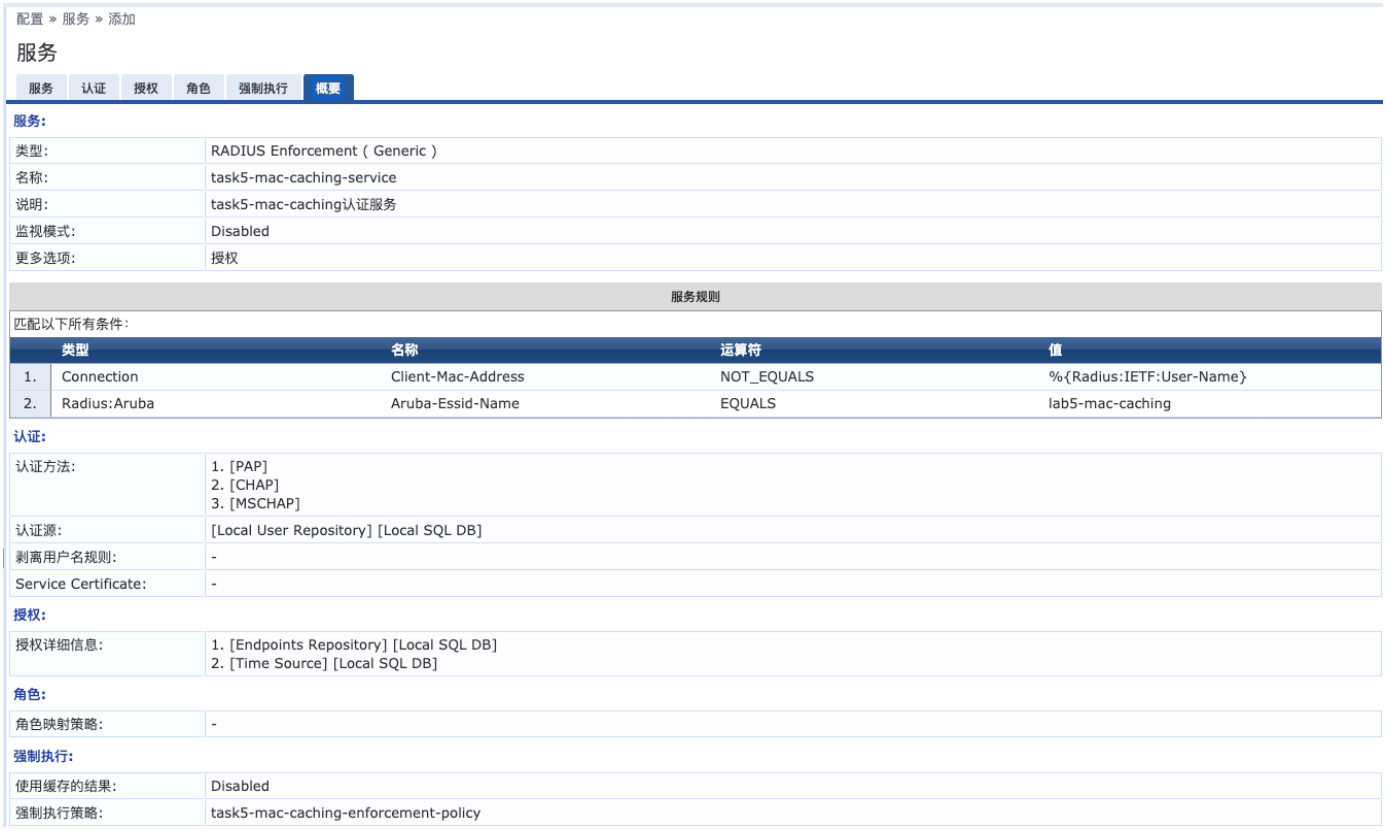
- ✓ 角色映射策略：空

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)*

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

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-service
说明：	task5-mac-caching认证服务
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.	Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}
2.	Radius:Aruba	Aruba-Essid-Name	EQUALS	lab5-mac-caching

认证：

认证方法：	1. [PAP] 2. [CHAP] 3. [MSCHAP]
认证源：	[Local User Repository] [Local SQL DB]
剥离用户名规则：	-
Service 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：	-

强制执行：

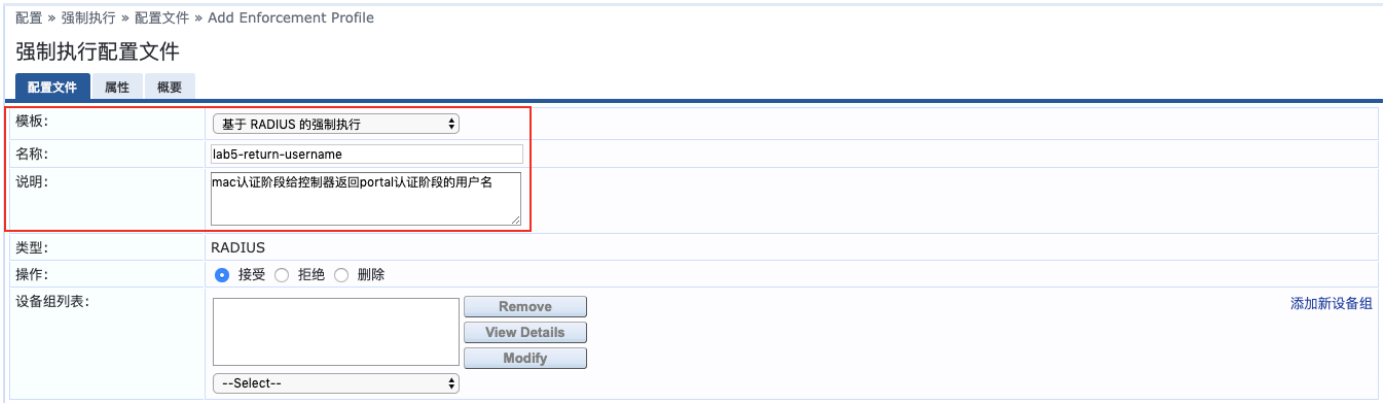
使用缓存的结果：	Disabled
强制执行策略：	task5-mac-caching-enforcement-policy

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：

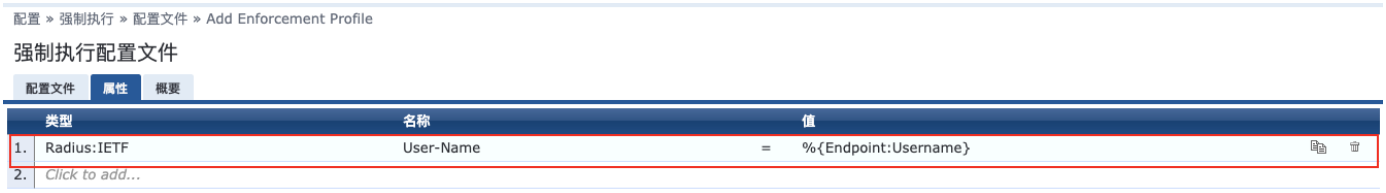
在“配置文件”选项卡中输入下面参数：

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



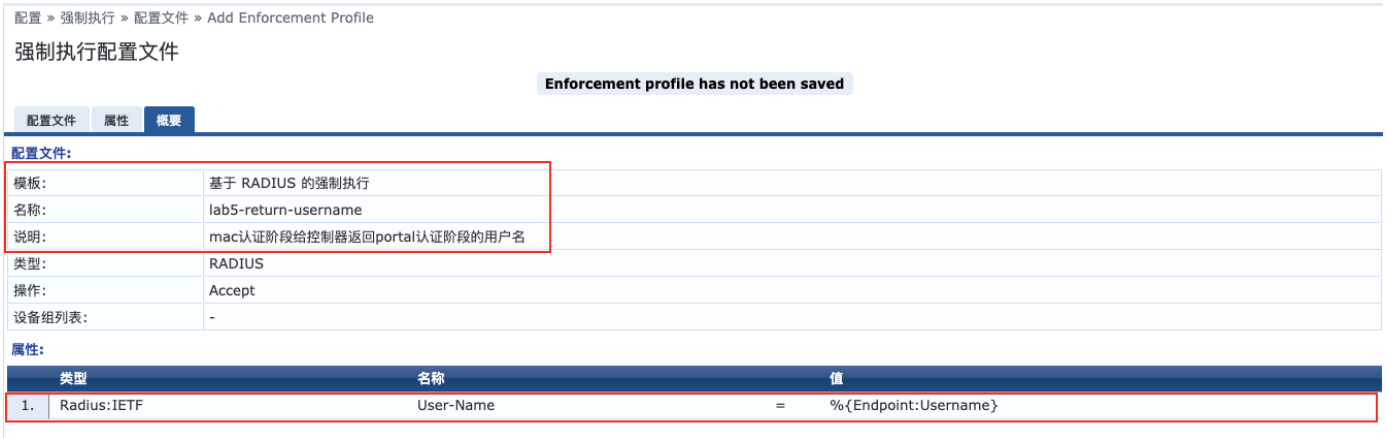
在“属性”选项卡中输入下面参数：

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



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”



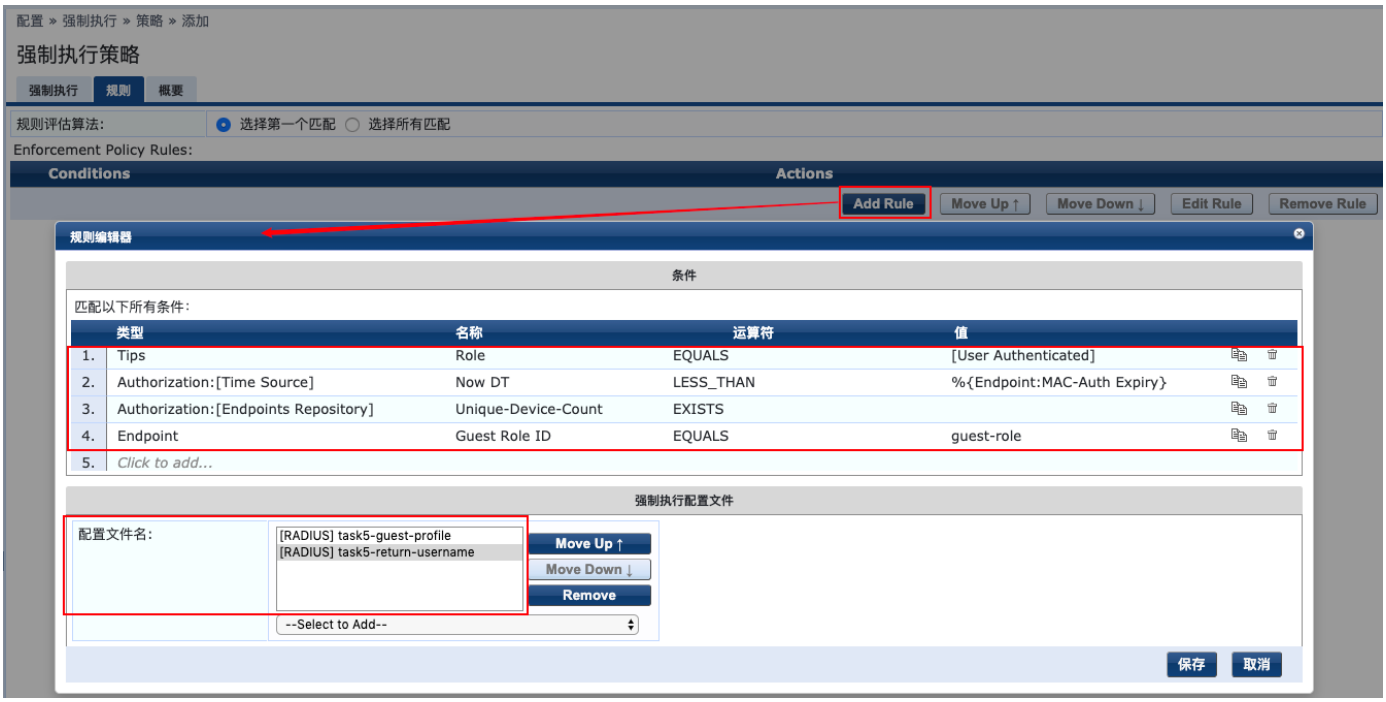
第2步：找到 配置 - > 强制执行 - > 策略，点击右侧的“添加强制执行策略”按钮，增加一个强制执行策略：

在“强制执行”选项卡中输入下面参数：

- ✓ 名称： task5-mac-enforcement-policy

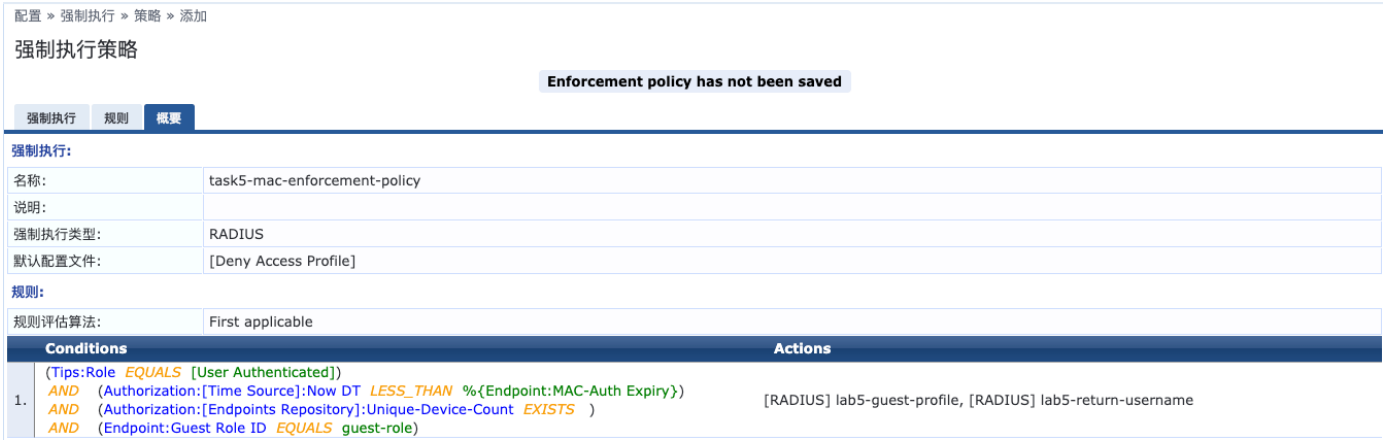
在“规则”选项卡中输入下面参数：

- ✓ 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)*



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



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

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]

在“授权”选项卡中配置如下参数：

- ✓ “[Endpoint Repository][Local SQL DB]”
- ✓ “[Time Source][Local SQL DB]”

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

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)*

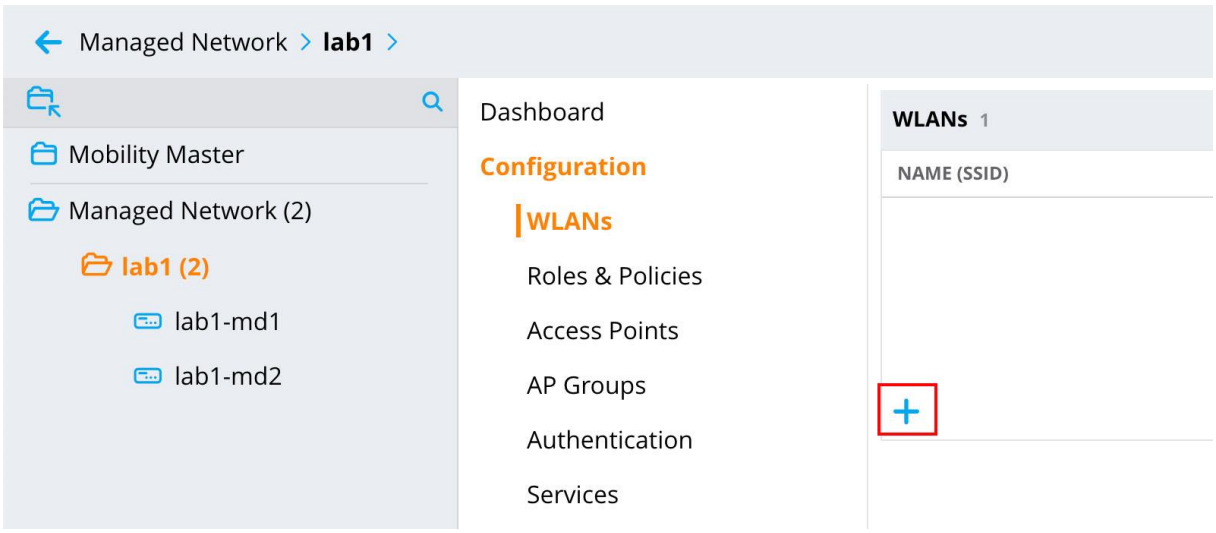
在“概要”选项卡中对配置进行总览：

✓ 概要：查看配置总览，点击“保存”按钮

6.4 控制器配置

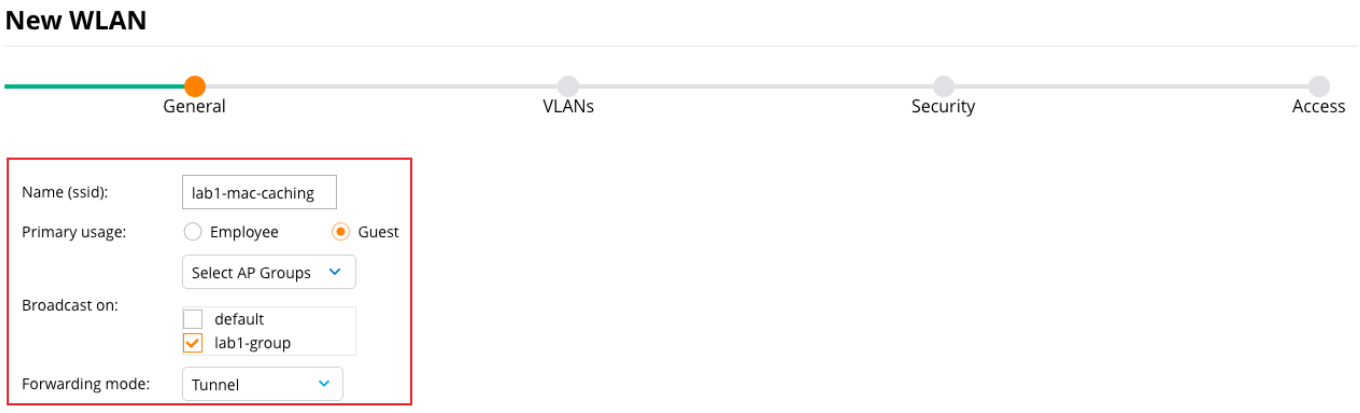
6.4.1 添加无线信号

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



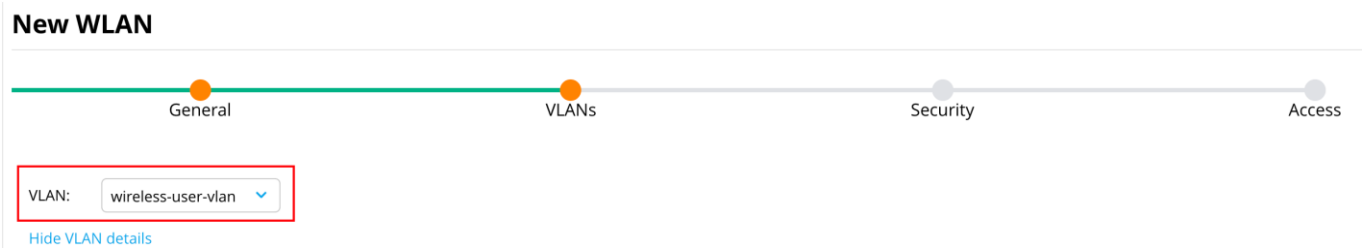
第2步：配置 SSID 名称、主要用途、在哪个 AP-Group 广播、转发模式

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



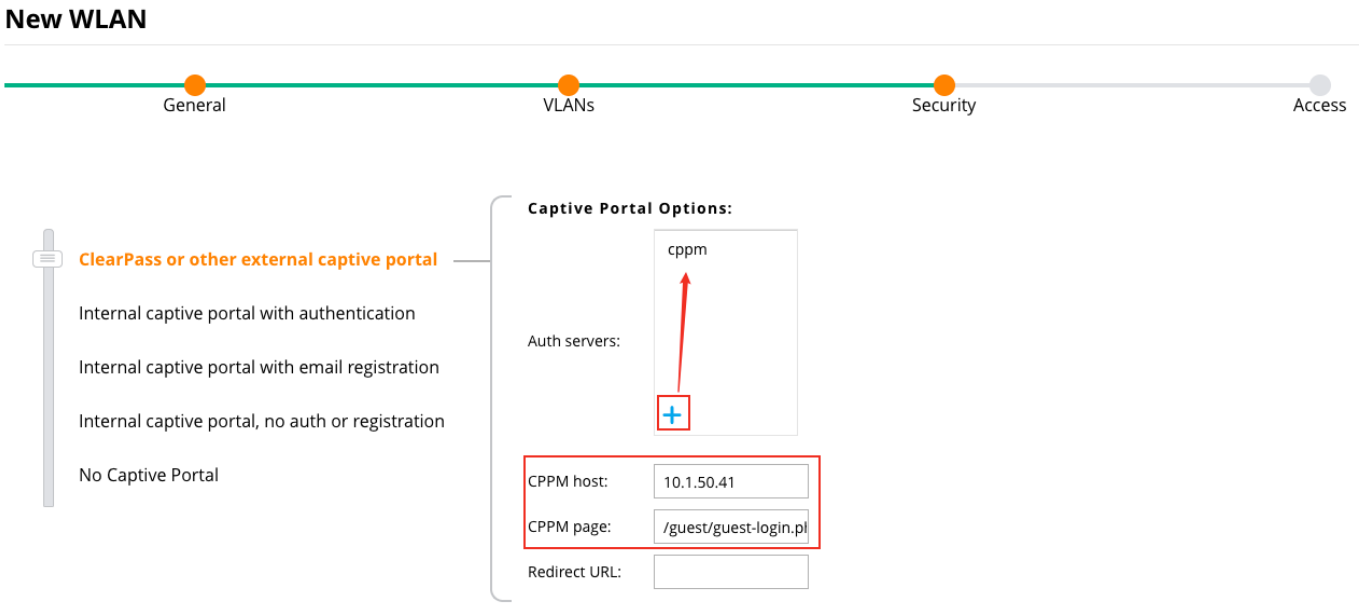
第3步：配置 VLAN

- ✓ VLAN：wireless-user-vlan

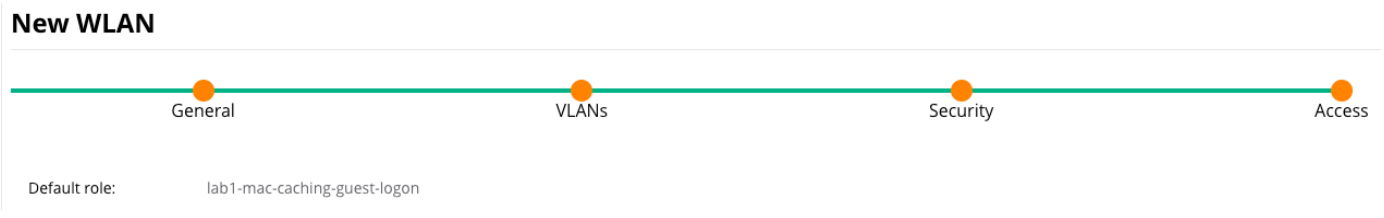


第4步：配置 portal 认证方式

- ✓ 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*）



第5步：完成向导配置



6.4.2 修改 portal 认证配置

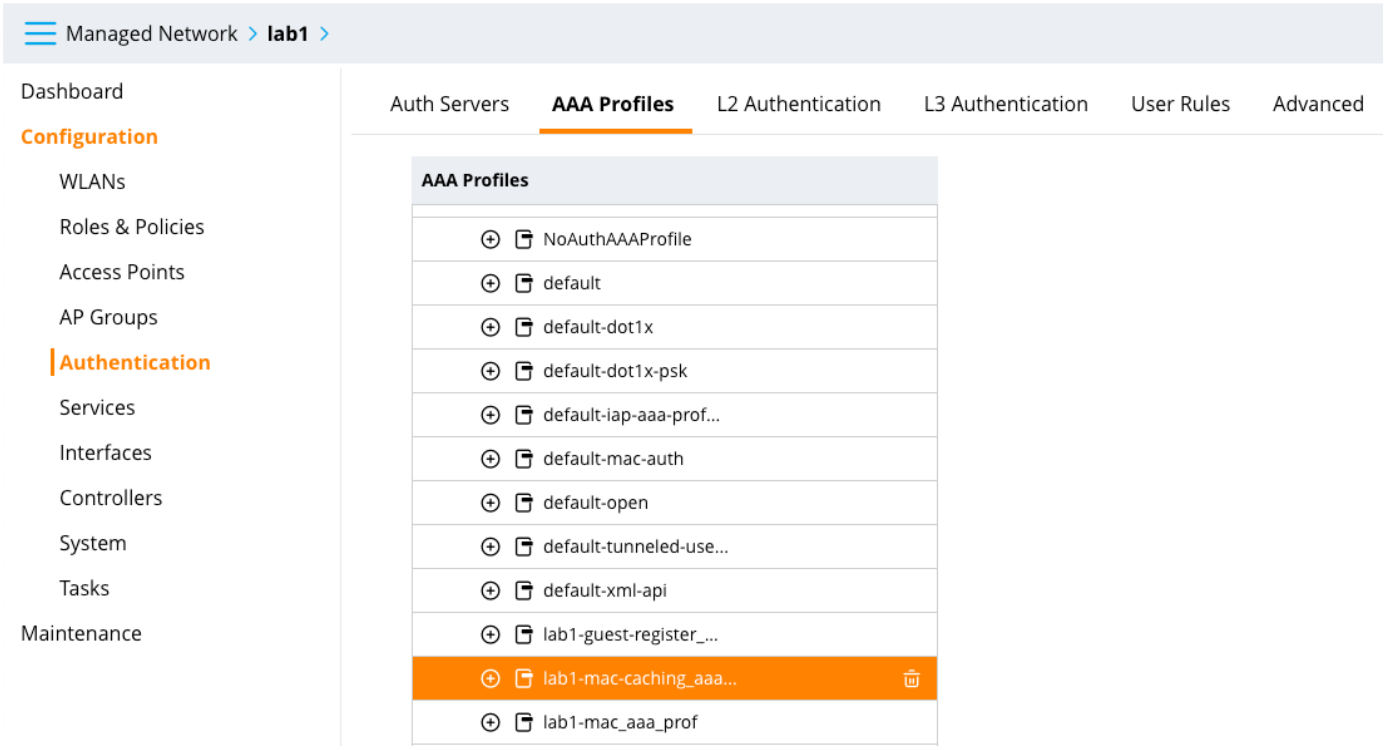
找到Managed Network - > labX -> Configuration -> Authentication -> L3Authentication 点击“Captive Portal Authentication”，选中“labX-mac-caching_cppm_prof” （X： 1 ·····6），修改如下参数

- ✓ 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）

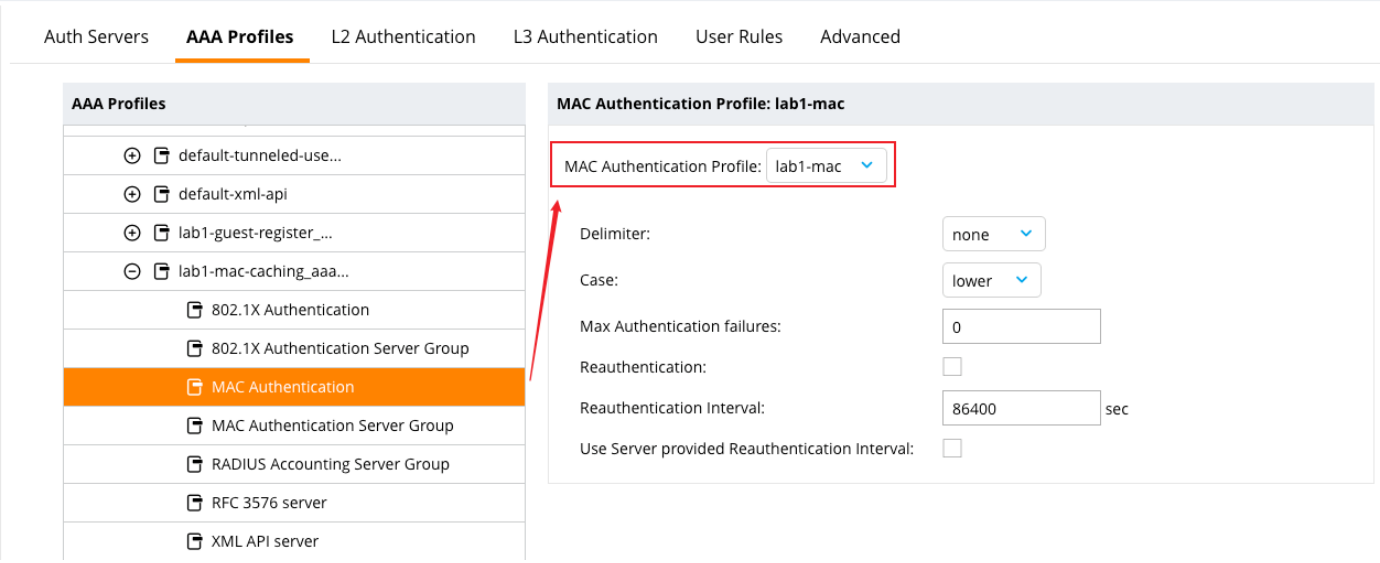
(配置截图略，详见4.4.2)

6.4.3 添加 MAC 认证

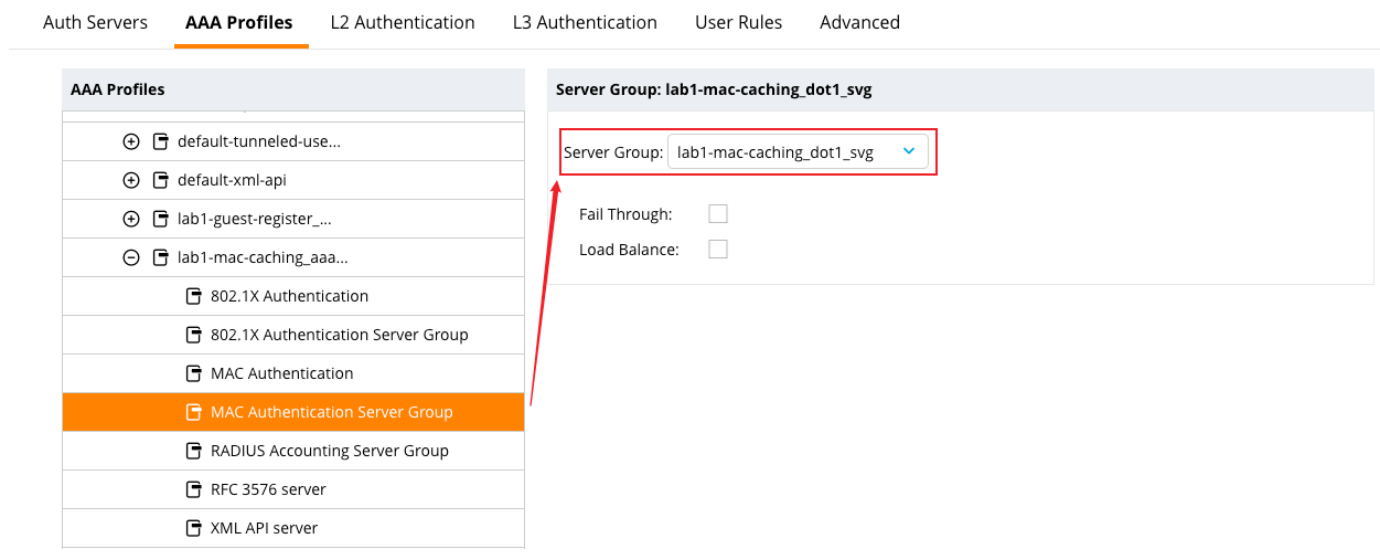
第1步: 找到 Managed Networks - > labX -> Configuration -> Authentication，在右侧点击“AAA Profile”，找到“AAA Profile: labX-mac-caching_aaa_prof” （X： 1 ·····6）



第2步: 修改 MAC Authentication Profile 为“labX-mac” （X：1···6），点击右下角“**Submit**”

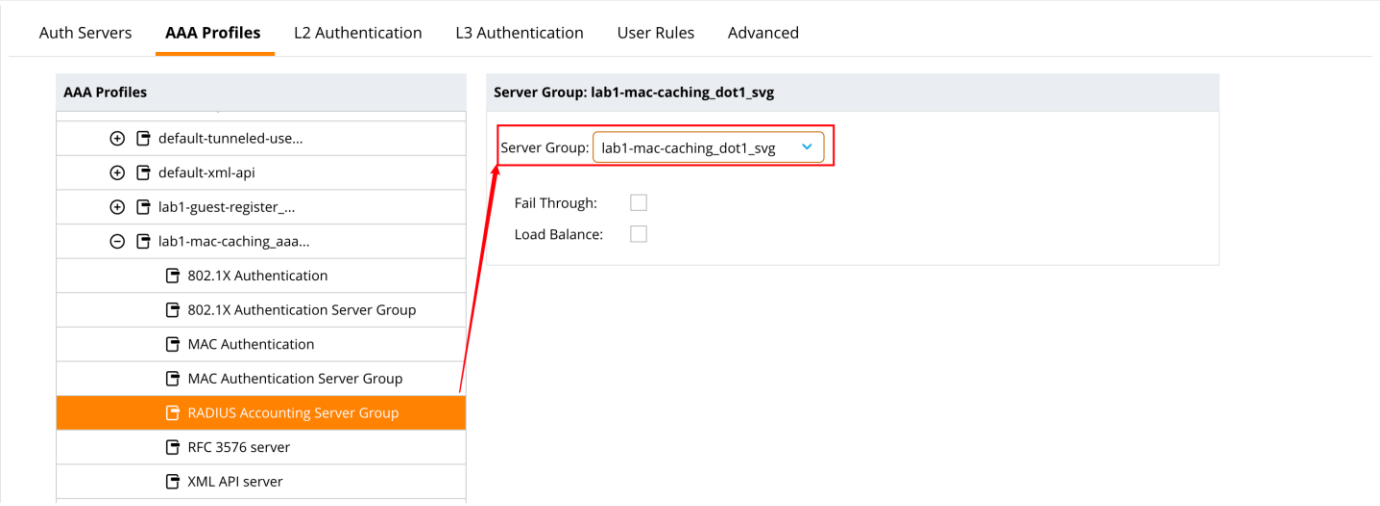


第3步：修改 MAC Authentication Server Group 为“labX-mac-caching_dot1_svg” （X：1…6），点击右下角“**Submit**”

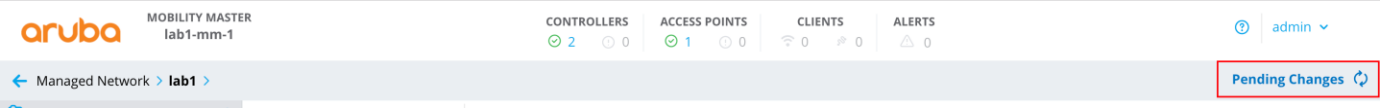


6.4.4 添加计费

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



第2步：点击右上角“Pending Changes”保存配置



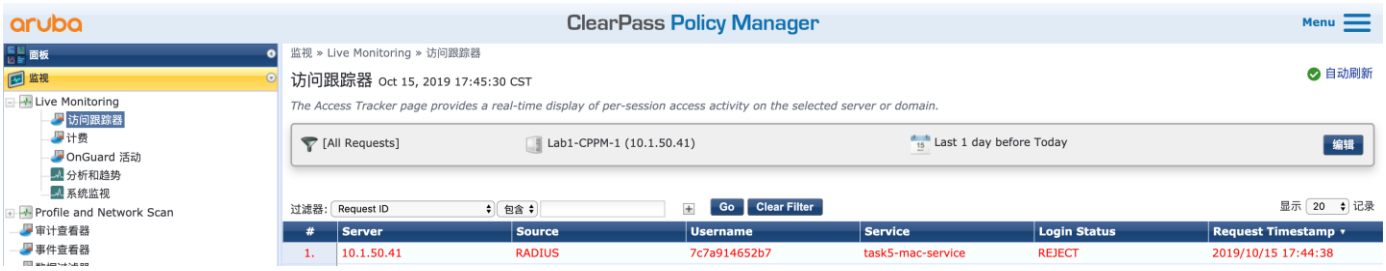
6.5 验证结果

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

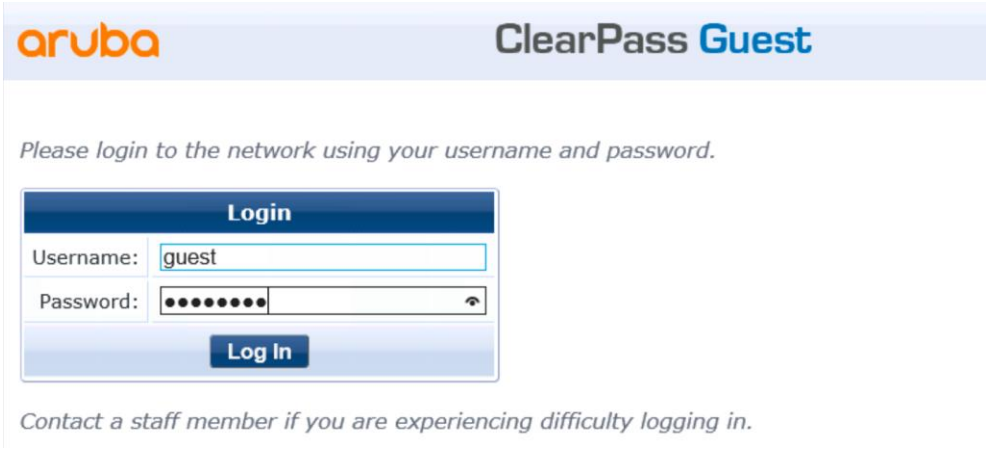
第2步：登录到 ClearPass，找到 监控 - > Live Monitoring - > 访问跟踪器，查看认证记录（1/3），

- ✓ 此时我们发现匹配到了task5-mac-service，认证失败

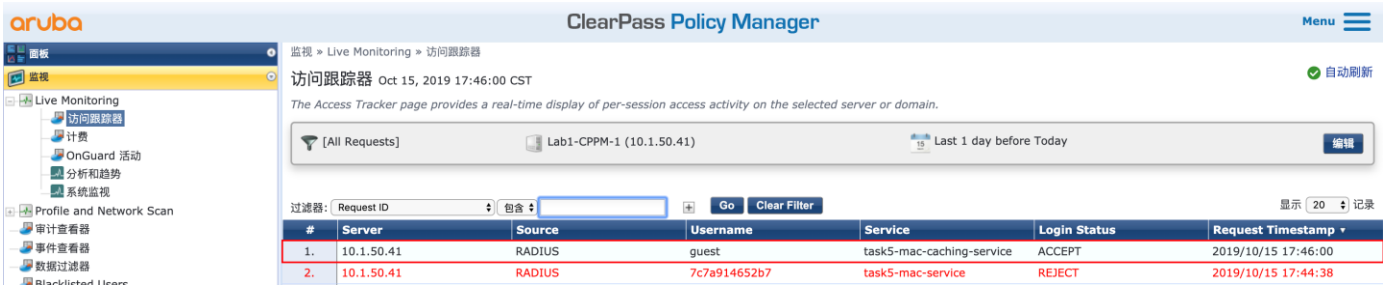


第3步：远程登录到测试终端 10.X.50.102（X：1…6），打开浏览器

- ✓ 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。



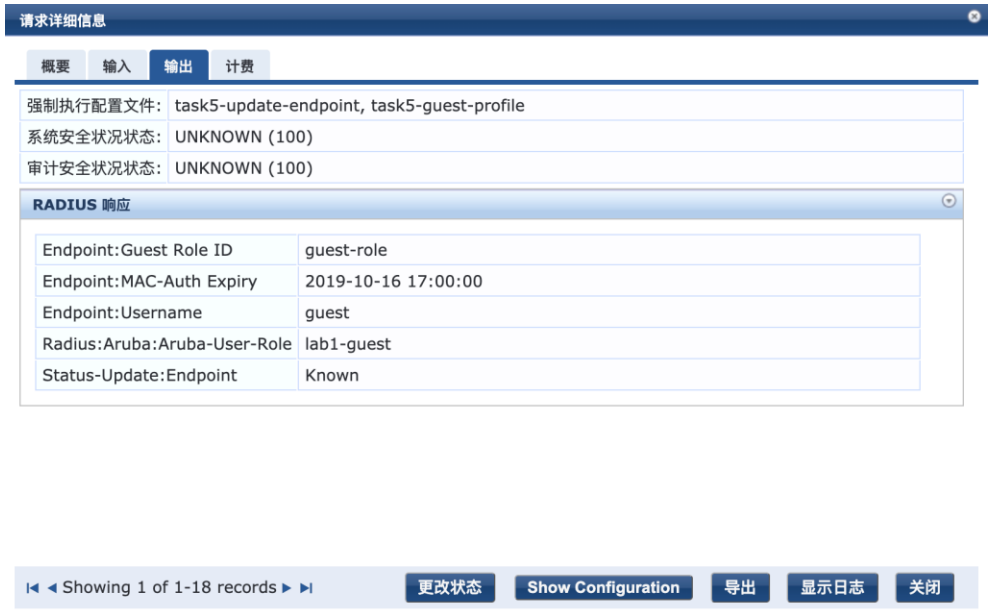
- ✓ 登录到ClearPass，找到 监控 - > Live Monitoring - > 访问跟踪器，查看认证记录（2/3），此时我们发现匹配到task5-mac-caching-service，认证成功。



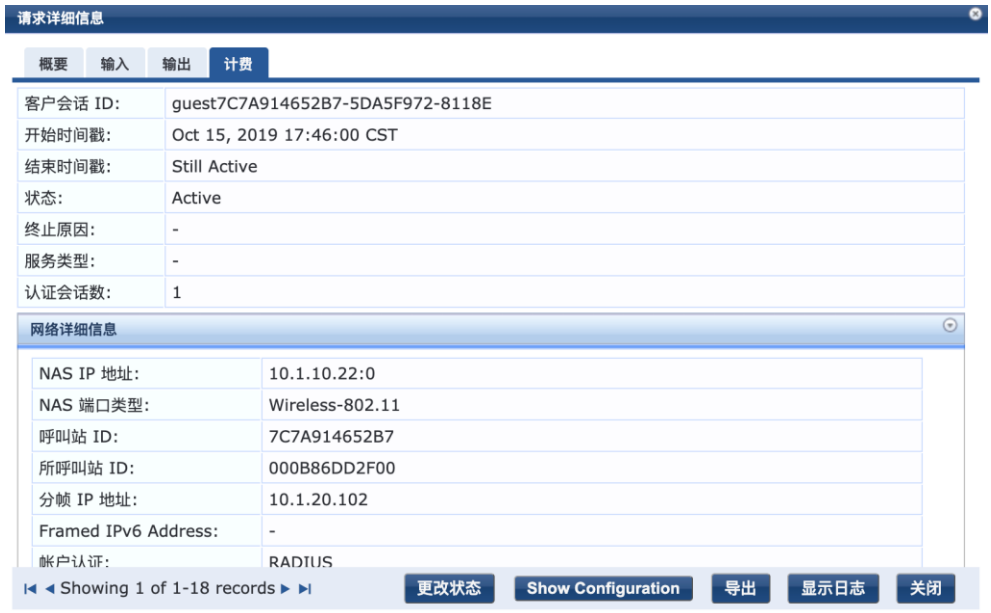
- ✓ 点击认证成功记录，在“概要“选项卡中观察，看看能看到哪些信息。

✓ 在“输入“选项卡中观察，看看能看到哪些信息。

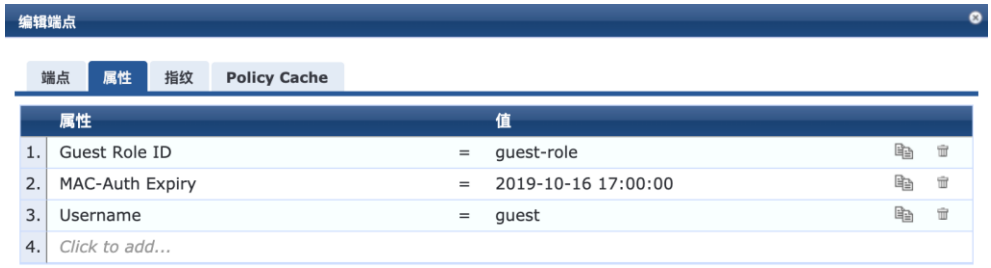
✓ 点击“输出“选项卡，并观察，看看能看到哪些信息。



✓ 点击“计费“选项卡，并观察，看看能看到哪些信息。



✓ 登录到 CPPM，找到 配置 - > 端点，点击“属性”，查看终端属性



✓ 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            MAC            Name    Role        Age(d:h:m)  Auth  VPN link  AP name
me  User Type
----------   ------------       ------  ----        ----------  ----  --------  -------
--  ---------
10.1.20.102  7c:7a: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 global-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
```

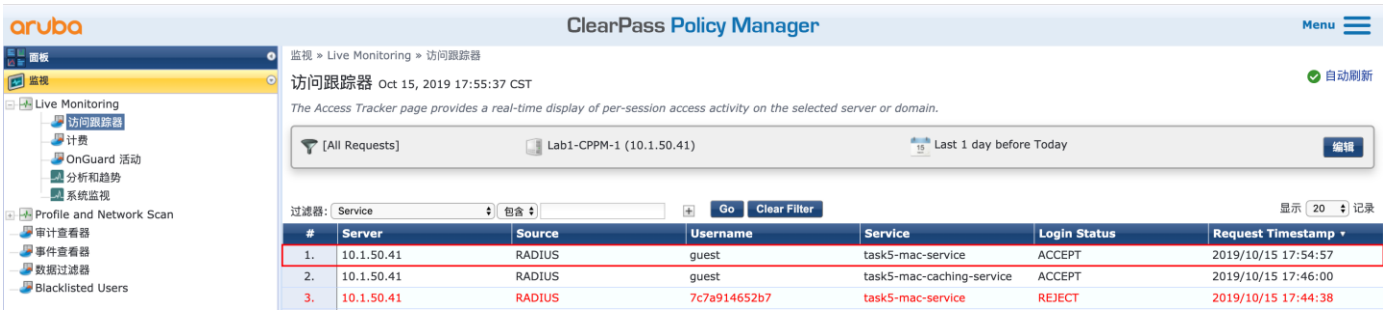
✓ 登录到用户所在控制器10.1.10.11，将用户下线。

```
(lab1-mm-1) [mynode] #logon 10.1.10.11


(lab1-md1) [MDC] #aaa user delete mac 7c:7a:91:46:52:b7
1 users deleted
```

✓ 通过“show user”查看用户在线状态

```
(lab1-md1) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP              MAC              Name      Role         Age(d:h:m)  Auth  VPN link  AP name
me  User Type
----------    ------------       ------    ----         ----------  ----  --------  -------
--  ---------
10.1.20.102   7c:7a:91:46:52:b7  guest     lab1-guest   00:00:00    MAC             94:b4:0f:c1:3f:e0
    WIRELESS
```

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

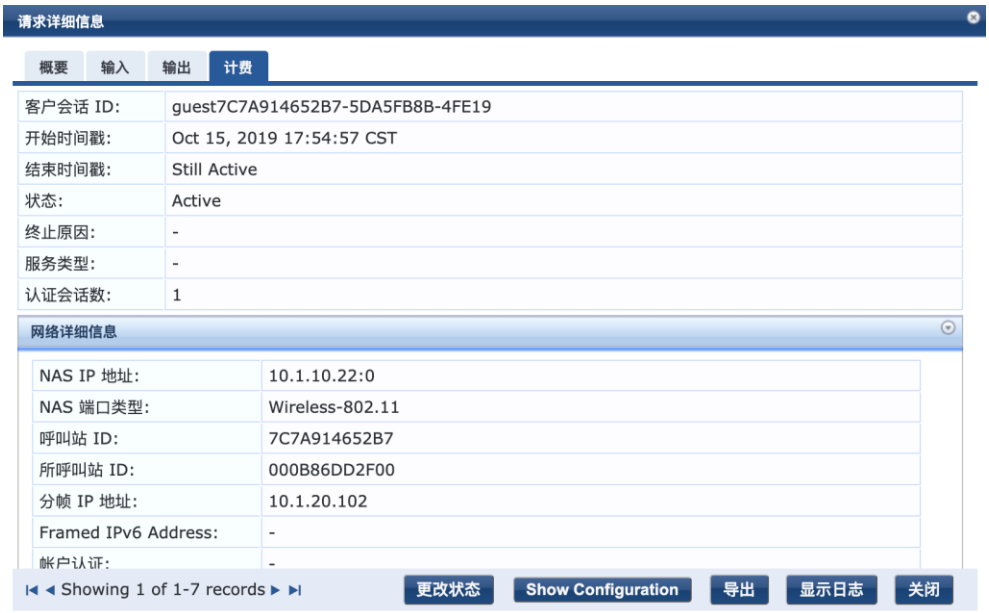


✓ 点击这条认证记录，查看“概要”选项卡，看看有哪些信息

✓ 查看“输入”选项卡，观察获取到的radius信息

✓ 查看“输出”选项卡，观察ClearPass向控制器返回到radius信息

✓ 查看“计费”选项卡，观察radius计费信息



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： _____

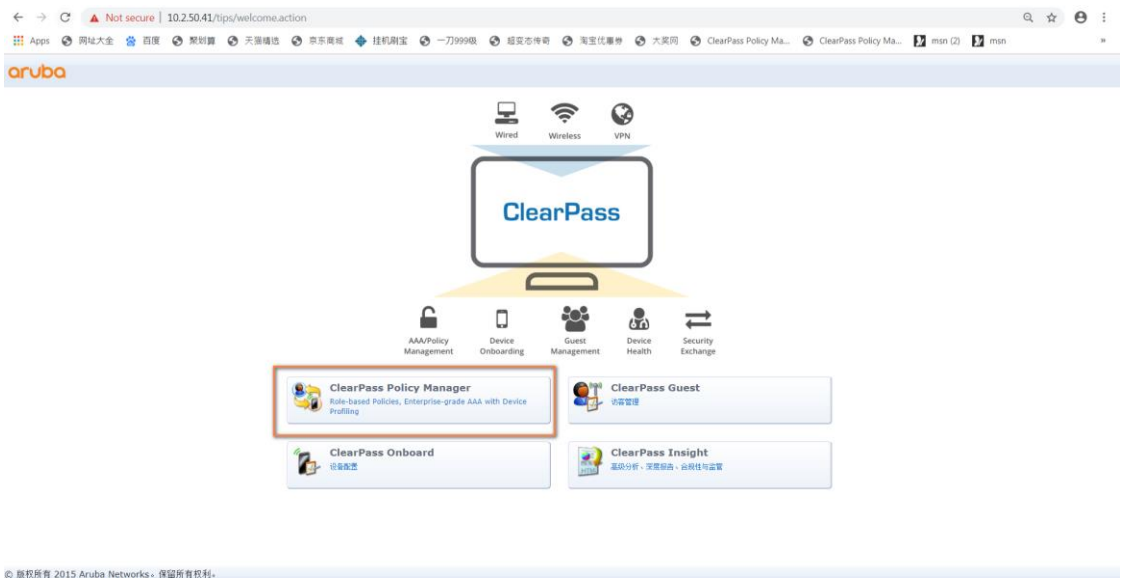
✓ 针对访客自注册认证，我们需要思考下，你对该认证方式的完整流程熟悉吗?

答案： _____

7.3 ClearPass 配置

7.3.1 添加 SMTP 信息

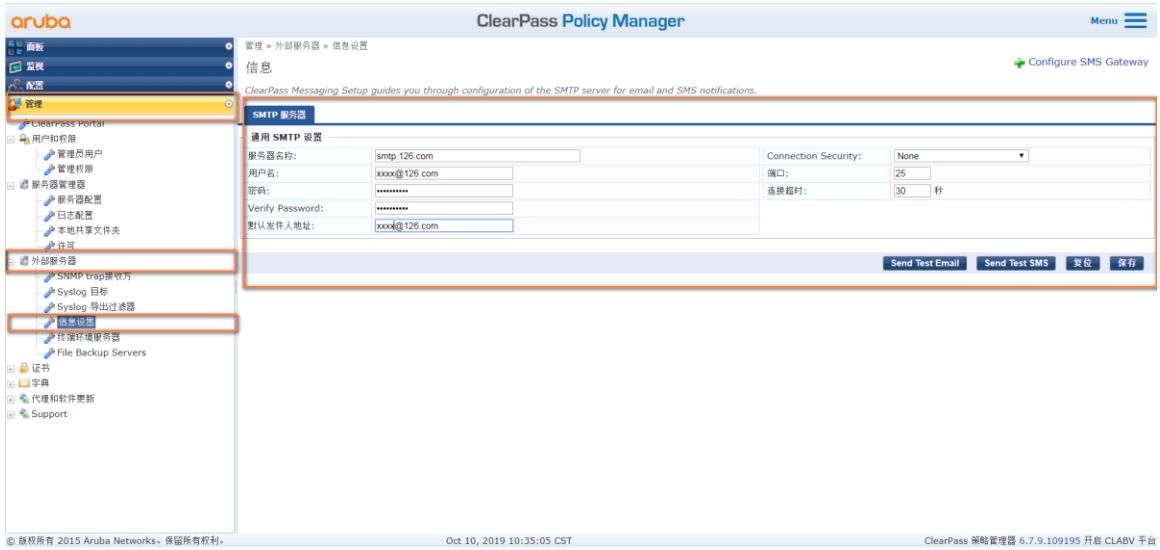
第1步: 通过网页浏览器来访问ClearPass的管理IP(10.X.50.41) （X ： 1 ·····6），从而进入到welcome行动页面，点击ClearPass Policy Manager 模块，从而进入到策略管理页面。

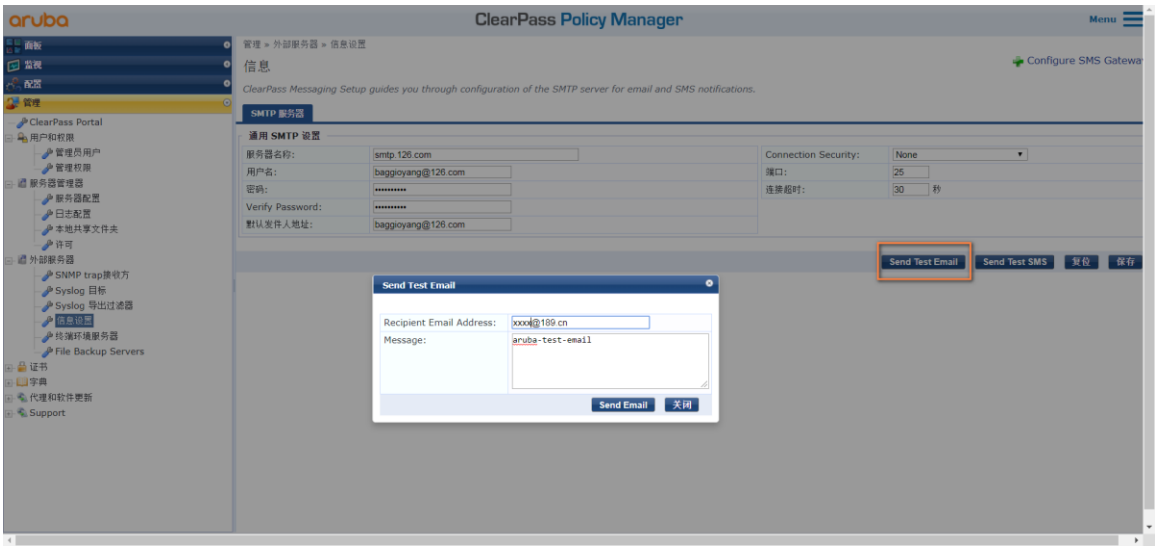


第2步：在策略管理页面中，打开 管理 - > 外部服务器- > 信息设置，在右边的SMTP服务器中配置相应的SMTP设置，点击 保存按钮，点击 Send Test Email 测试SMTP服务器是否设置成功，在 Send Test Email 窗口输入收件人Email地址和测试内容，点击 Send Email，当提示 Successfully sent test email to 表示发送成功。

在SMTP配置窗口中，输入下面的参数：

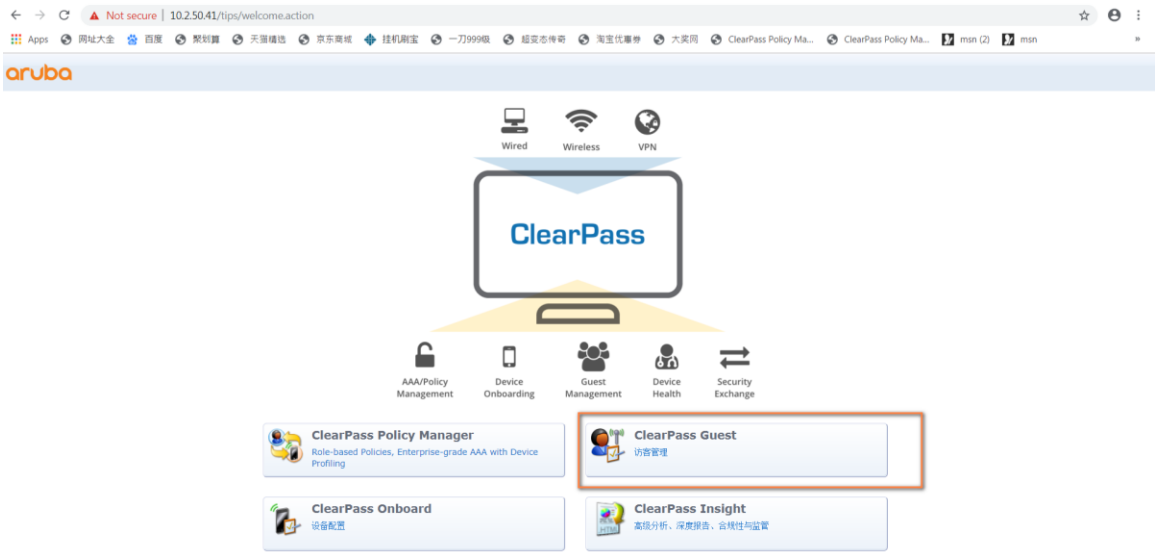
- ✓ 服务器名称：smtp.126.com（这里就是管理员的SMTP服务器地址）
- ✓ 用户名： 邮箱登录账号
- ✓ 密码：邮箱登录密码
- ✓ 默认发件人地址：用来发邮件的地址





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。



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：

在页面的基本属性中，输入下面的参数：

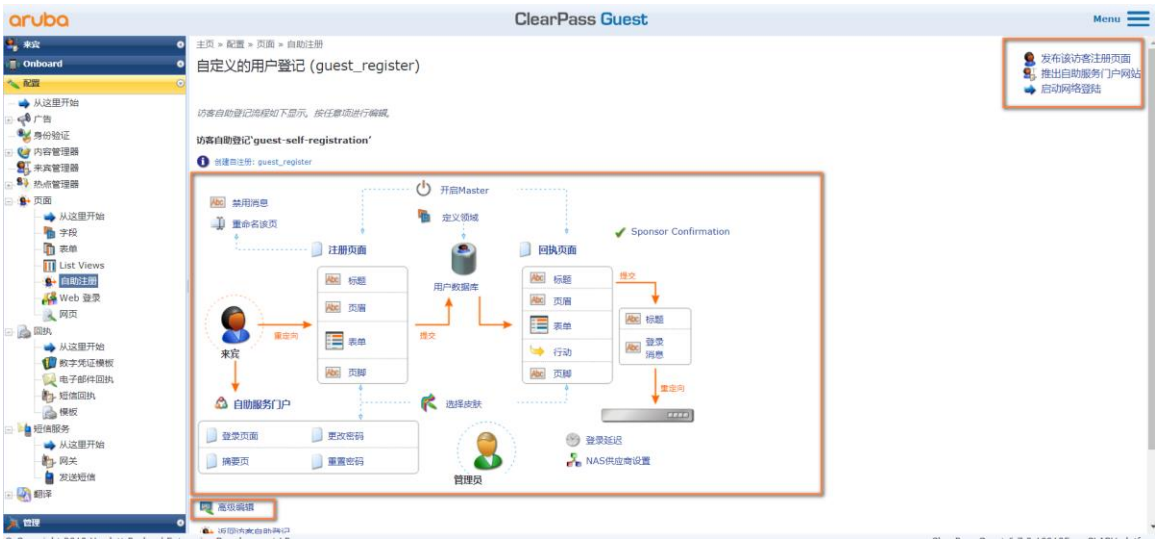
- ✓ 名字： guest-self-registration （即该访客自注册页面的配置名称）
- ✓ 注册页面：guest_register （即该访客自注册页面的URL后缀名称guest_register.php）
- ✓ 保存更改：点击保存

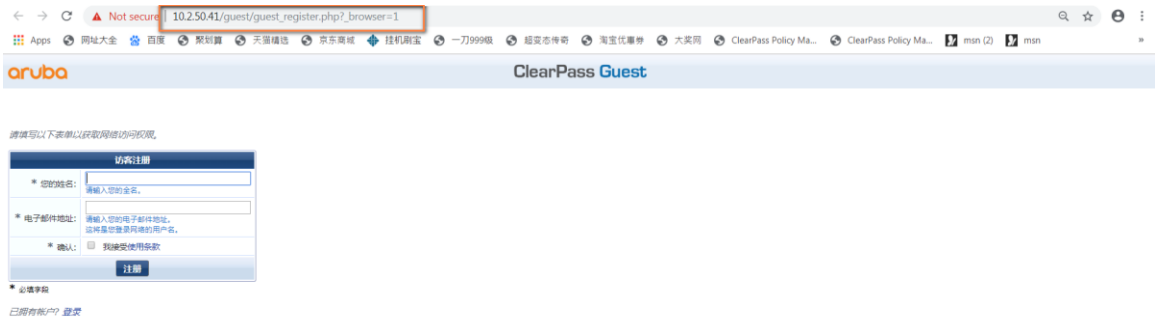
在自定义的用户登记中，可以看到ClearPass内置的自注册流程图介绍：

- ✓ 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



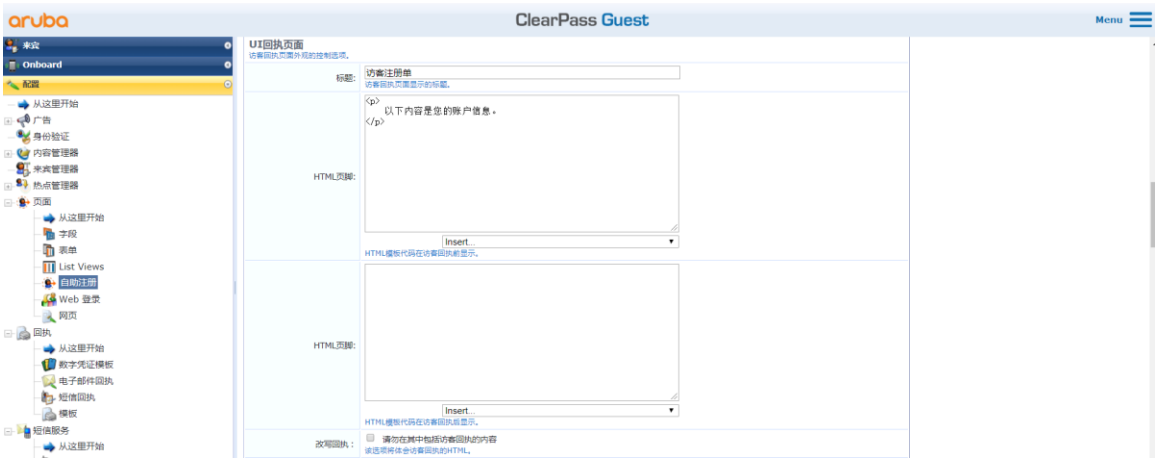


✓ 基本属性部分：相关内容之前步骤已经配置好，皮肤可以选择自己喜欢的页面风格，本次手册以默认皮肤为参考使用

✓ 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

✓ 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

✓ 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



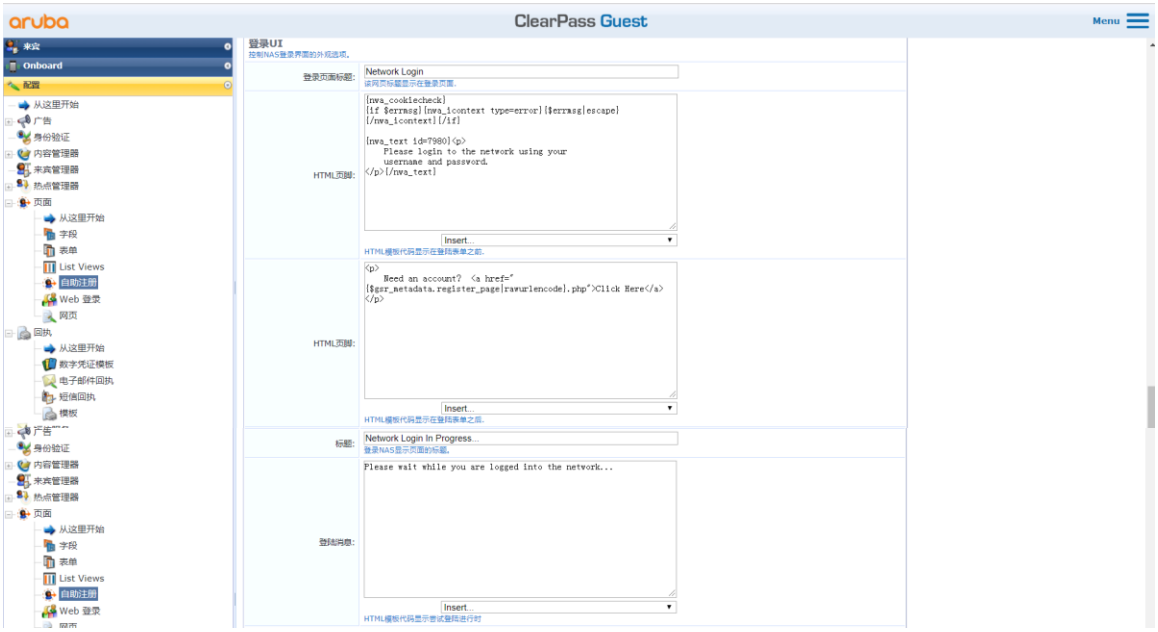
✓ 回执操作部分：可以在这里设置回执内容的如何发布，可以采用下载、打印、邮件以及短信等方式将访客账号和密码告知给访客人员， 本次手册我们采用邮件方式来告知。

✓ 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。

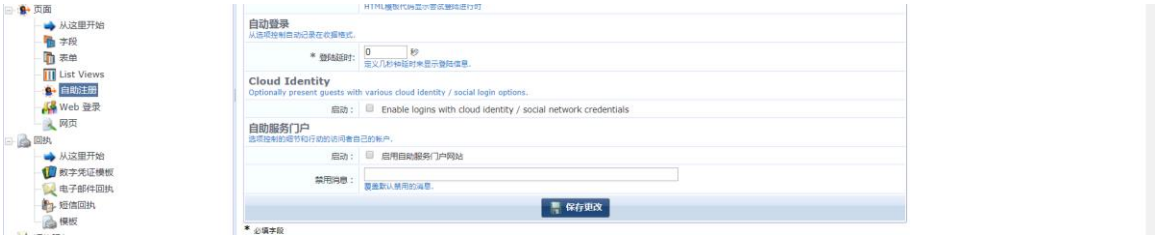
✓ 登录部分：可以在这里设置登录页面的相关内容，这里的登录页面是该自注册页面自动生成的，用于该自注册页面和登录页面的自动跳转使用。安全登录设置为通过HTTP发送明文密码（因为我们本次实验会采用ClearPass的自签证书，所以统一用HTTP发送明文。如果需要更安全的HTTPS发送密文，请事先准备好商业签发的Public 证书）。 默认网址即设置访客认证后的欢迎页面的URL，勾选覆盖目标.

✓ 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。

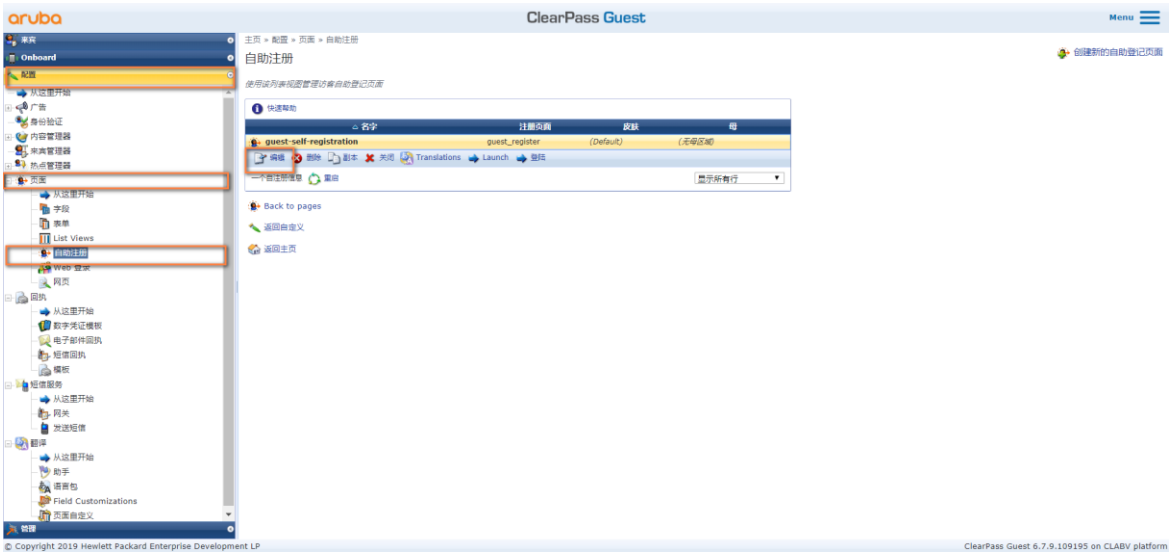
✓ 登录UI部分：可以在这里设置登录页面的提示内容以及自动跳转到自注册页面的的超链接URL



✓ 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。

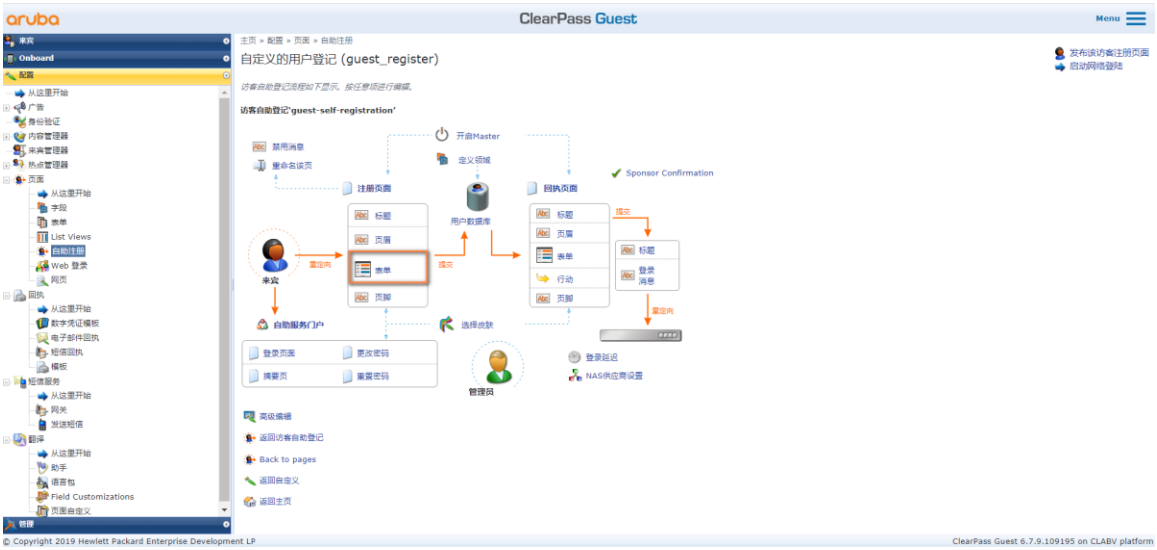


第4步：在【访客管理页面】中，找到 配置 - > 页面 - > 自助注册 ， 点击访客自注册页面guest-self-registration，进入到编辑按钮，点击进入到编辑状态。



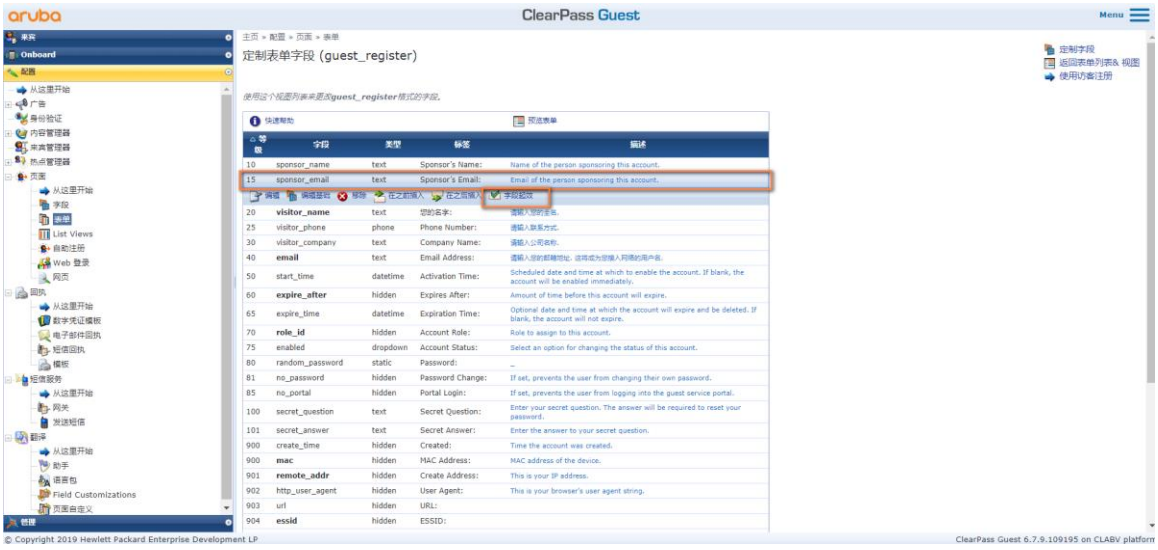
在【自定义的用户登记】中，可以看到ClearPass内置的自注册流程图介绍：

- ✓ 表单：进入到注册页面的表单编辑



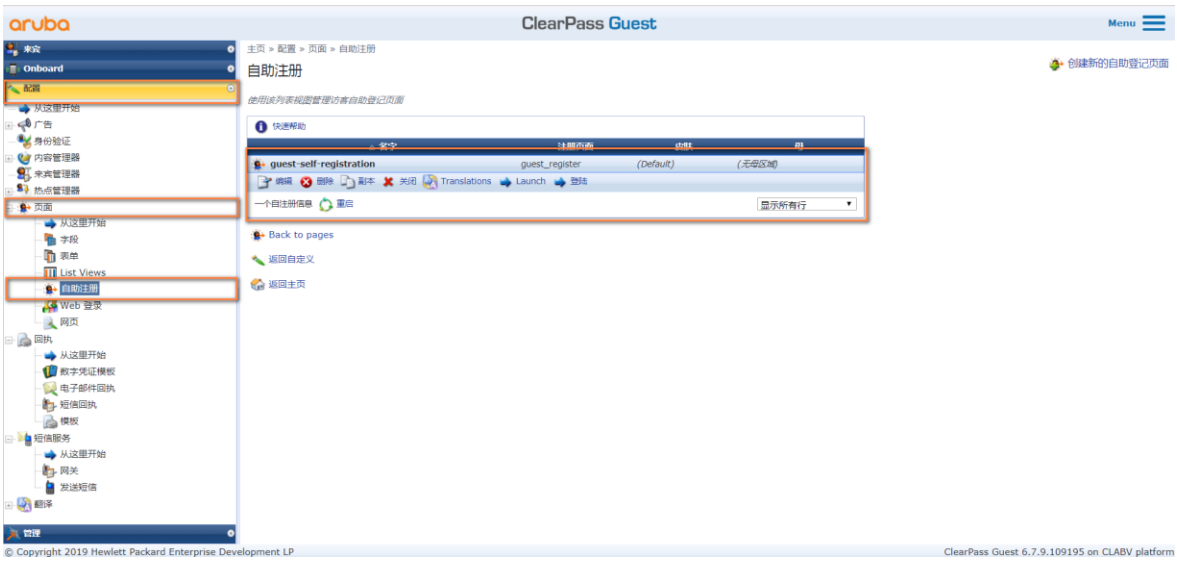
在【定制表单字段】中，可以看到访客自注册页面中表单各字段内容：

- ✓ sponsor_email：将该字段启用



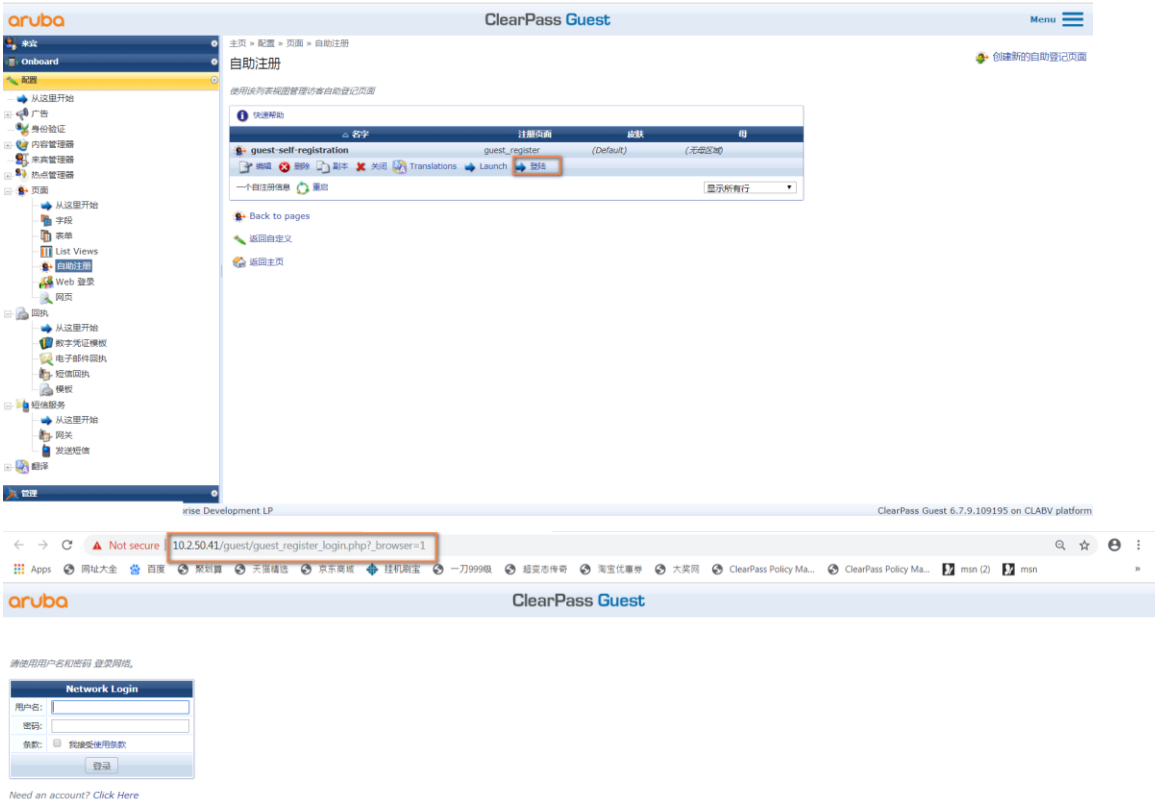
7.3.3 添加访客 portal 登录页面

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：

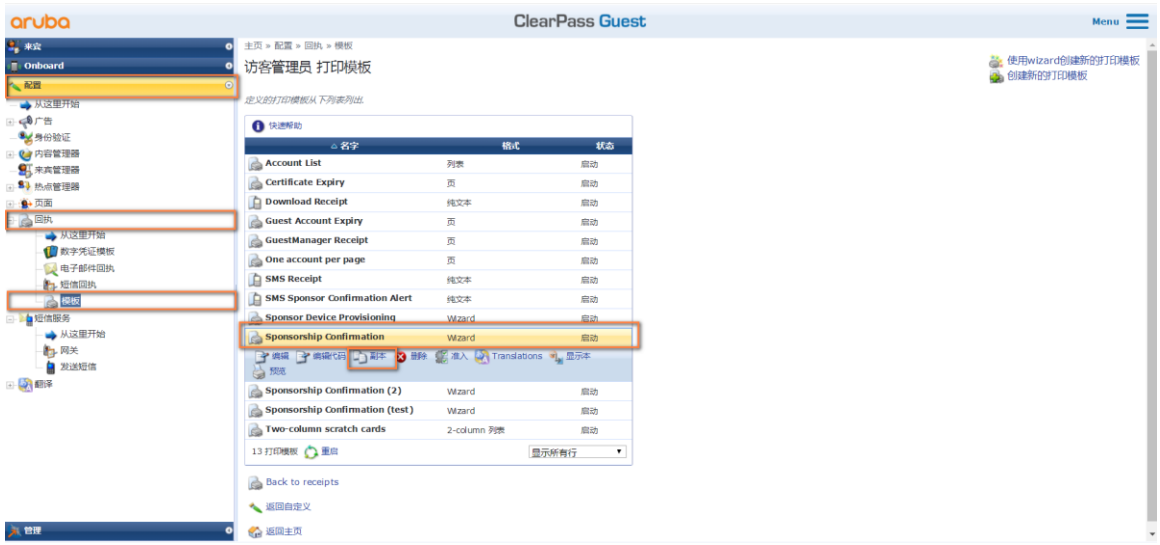
http://10.2.50.41/guest/guest_register_login.php?_browser=1



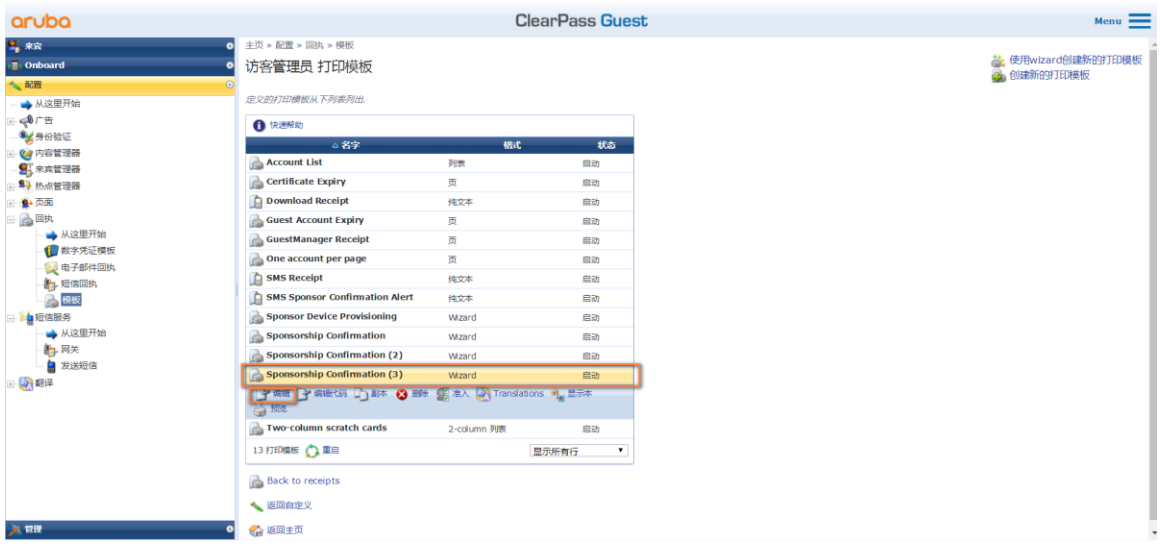
7.3.4 修改联系人邮件确认收据

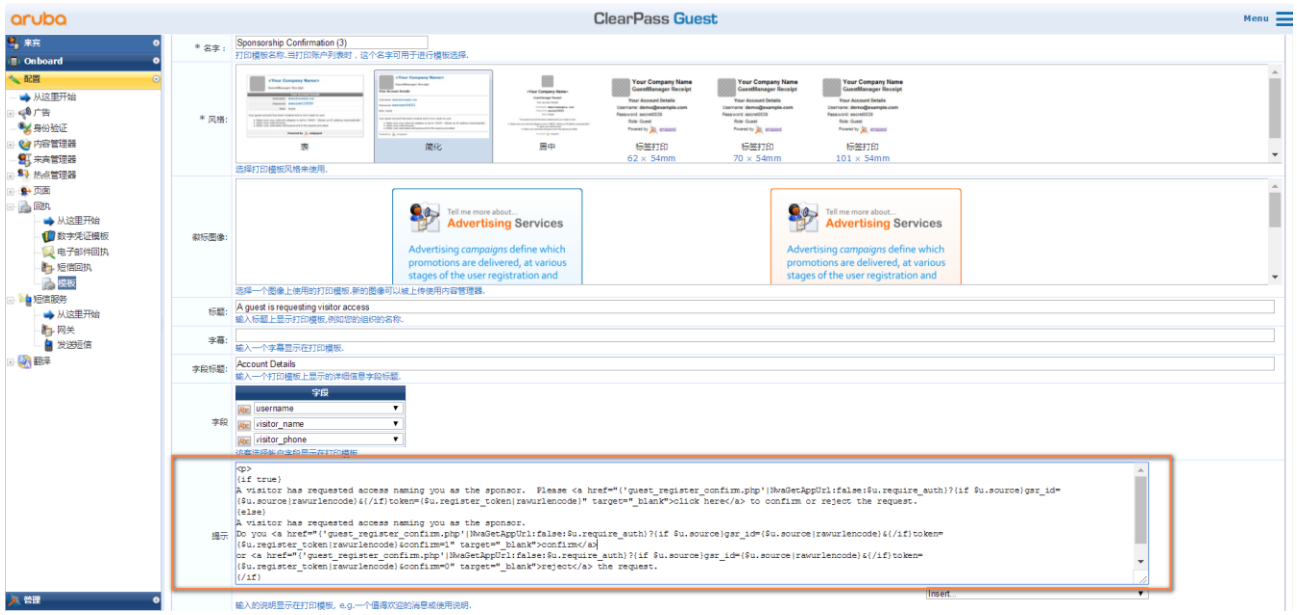
第1步：在访客管理页面中，找到 配置 - > 回执 - > 模板 ，点击“Sponsorship Confirmation ”，在下面的菜单中点击副本按钮，对系统默认的联系人确认邮件模板进行复制（这里必须是先点击下Sponsorship Confirmation 字体后，才会出现下面一行的编辑、编辑代码、副本、删除等菜单按钮）：

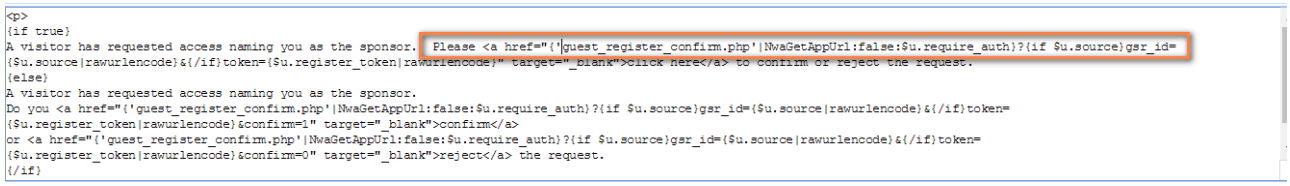
NOTE 当然你也可以直接在 Sponsorship Confirmation 系统默认的模板中直接修改。



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：







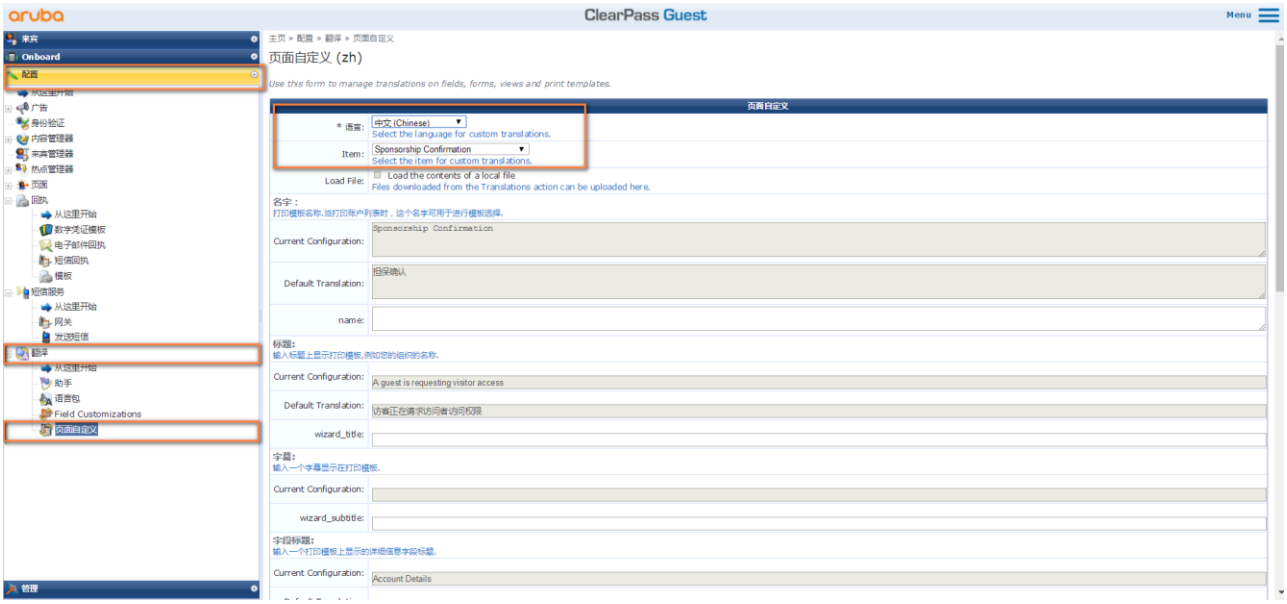
对提示栏目中的代码进行下面的修改，这样可以保证当联系人收到该邮件确认函后，点击Click Here能够通过IP地址访问该ClearPass，而不是默认的通过主机名方式来访问(前提是该网络中并没有实现域名的解析)。

我们需要在guest_register_confirm.php 前面增加 http://x.x.x.x/guest/ (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)

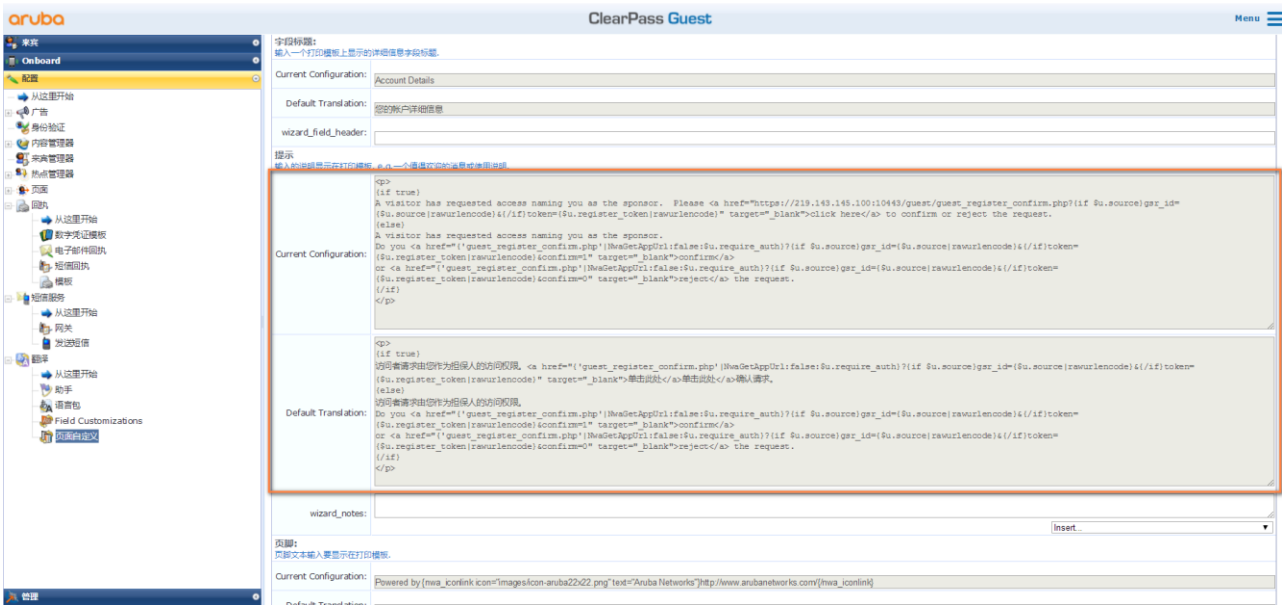
NOTE 由于 ClearPass 具有自动语言翻译包功能，当前我们修改的模板，仅仅是针对英文版本的浏览器生效，也就是如果客户采用英文语言的浏览器访问了自注册页面并发送账号批准申请，那么该代码是生效的。而针对中文语言的浏览器，我们还需要设置下中文语言包的代码修改，请继续。

```
<p>
{if true}
A visitor has requested access naming you as the sponsor.  Please <a href="{'http://10.1.50.41/guest/guest_register_confirm.php'|NwaGetAppUrl:false:$u.require_auth}?{if
$u.source}gsr_id={$u.source|rawurlencode}&{/if}token={$u.register_token|rawurlencode}" target="_blank">click here</a> to confirm or reject the request.
{else}
A visitor has requested access naming you as the sponsor.
Do you <a href="{'guest_register_confirm.php'|NwaGetAppUrl:false:$u.require_auth}?{if $u.source}gsr_id={$u.source|rawurlencode}&{/if}token=
{$u.register_token|rawurlencode}&confirm=1" target="_blank">confirm</a>
or <a href="{'guest_register_confirm.php'|NwaGetAppUrl:false:$u.require_auth}?{if $u.source}gsr_id={$u.source|rawurlencode}&{/if}token=
{$u.register_token|rawurlencode}&confirm=0" target="_blank">reject</a> the request.
{/if}
</p>
```

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：

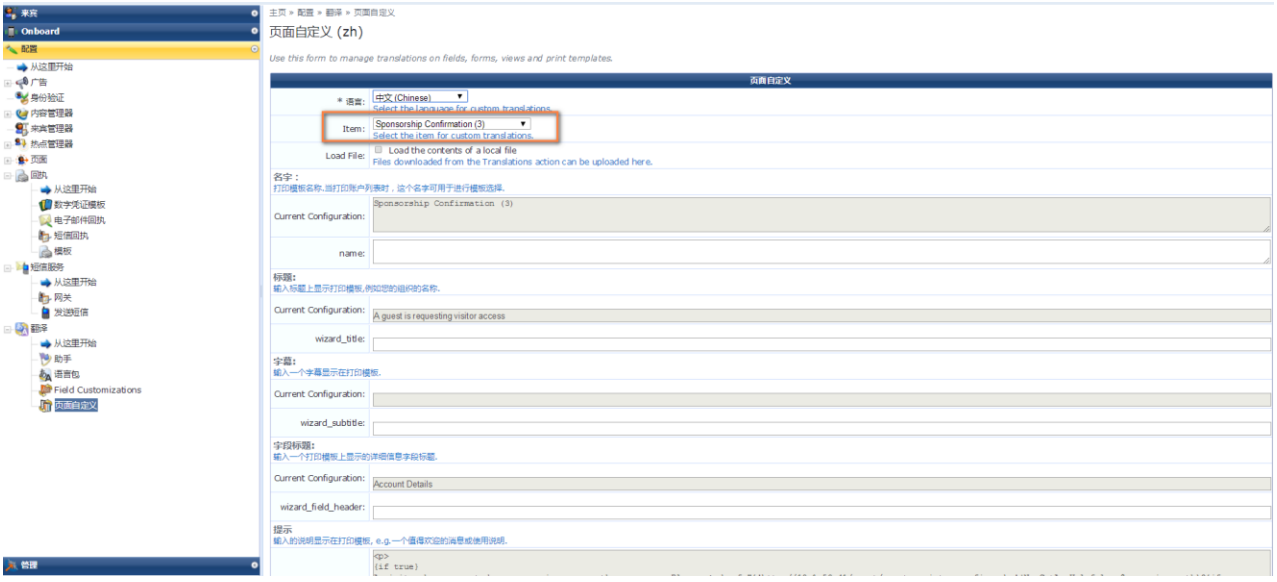


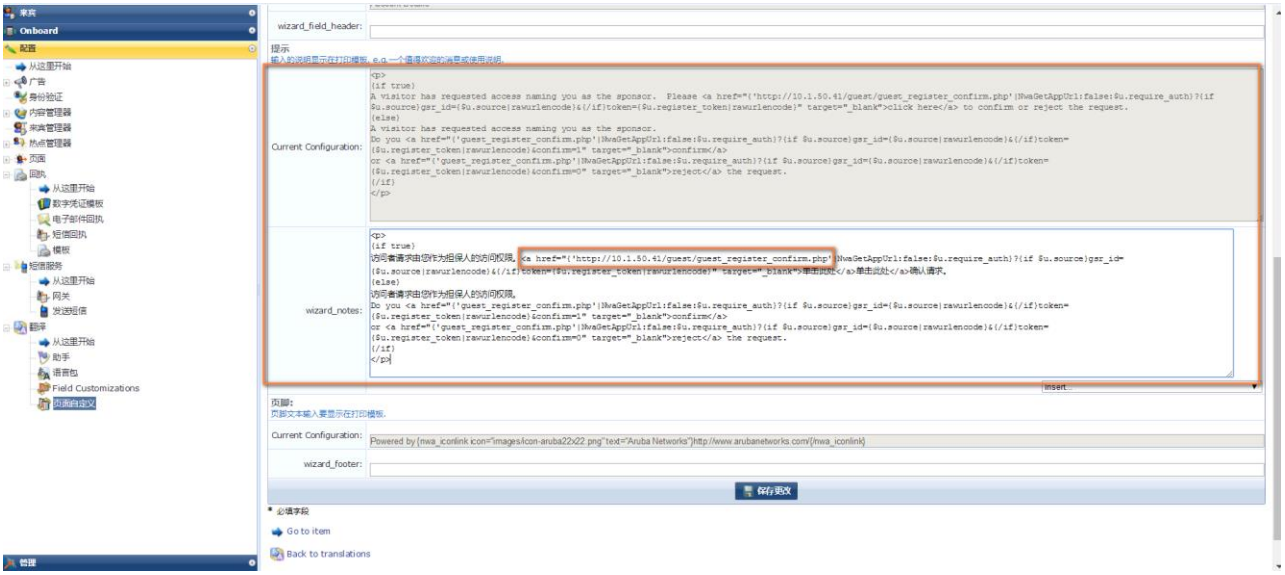
NOTE 你会发现在中文语言翻译包里面，系统默认并没有对修改的 URL 进行翻译和变更，所以我们需要继续修改联系人确认邮件模板。



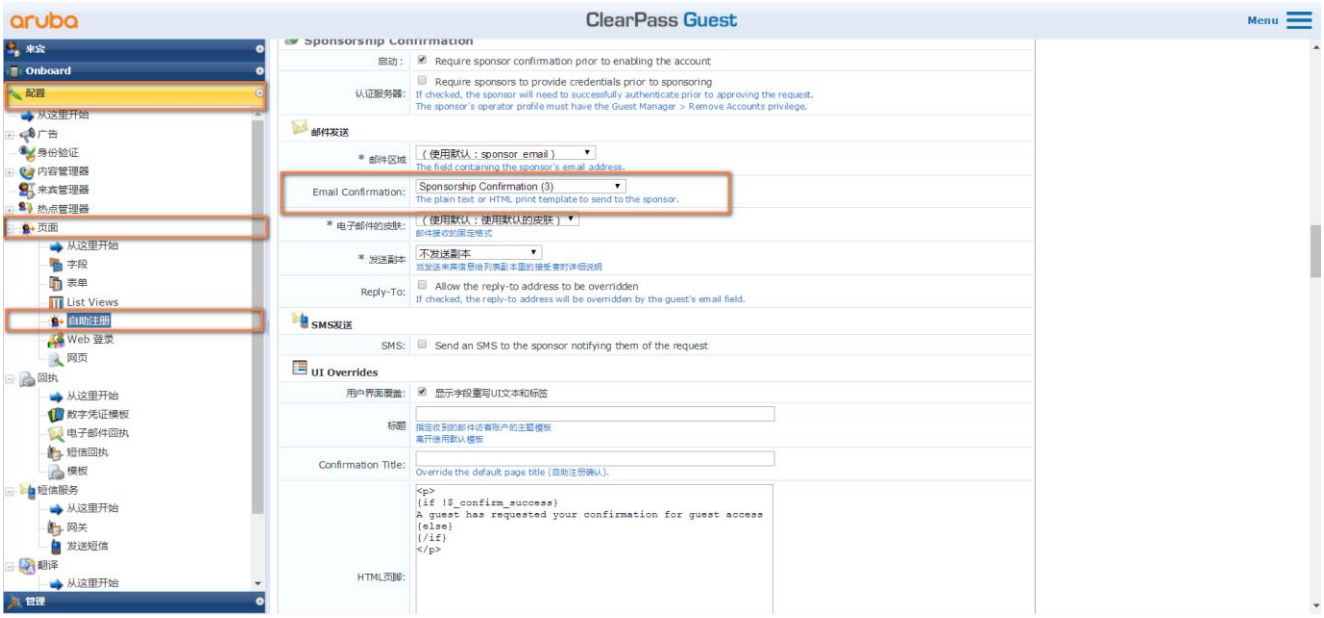
将Default Translation 里面的内容拷贝到文本文件中，并继续在guest_register_confirm.php 前面增加 http://x.x.x.x/guest/ (x.x.x.x即ClearPass的管理IP地址，可以是本地IP，也可以是对应的公网IP)，留作备用。

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。



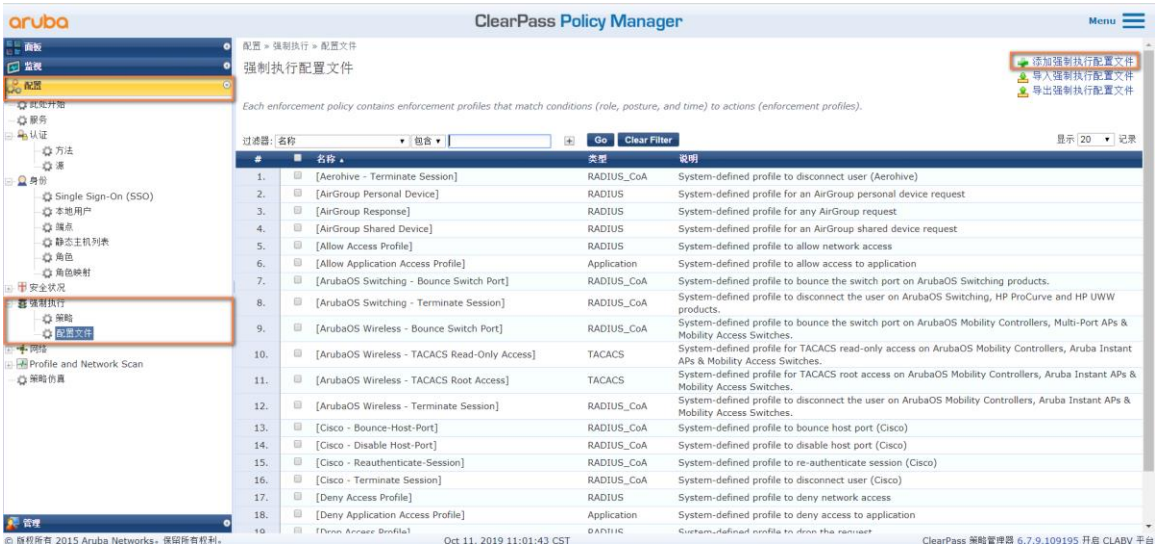


第4步: 回到之前步骤7.3.2中的访客portal自注册页面，在之前创建的自注册页面的高级编辑中，在Sponsorship Confirmation 部分中，修改Email Confirmation 选择Sponsorship Confirmation(3)，最后点击保存修改按钮.



7.3.5 添加认证服务

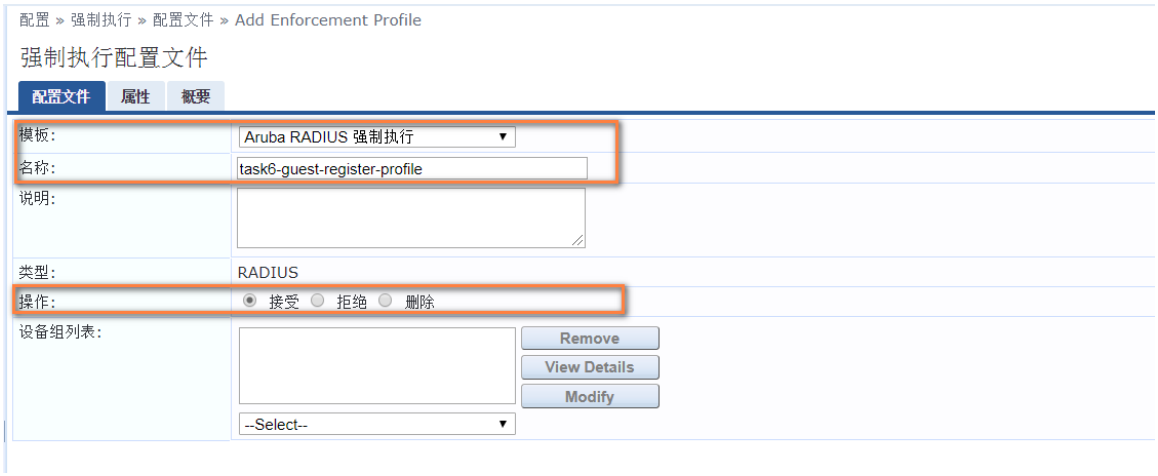
第1步：找到 配置 - > 强制执行 - > 配置文件，点击右上角的“添加强制执行配置文件”按钮，增加一个强制执行配置文件：



在配置文件选项卡中，输入下面的参数：

- ✓ 模板：Aruba RADIUS 强制执行

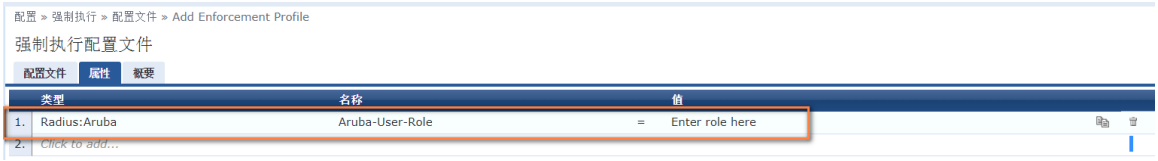
- ✓ 名称： task6-guest-register-profile
- ✓ 操作： 接受



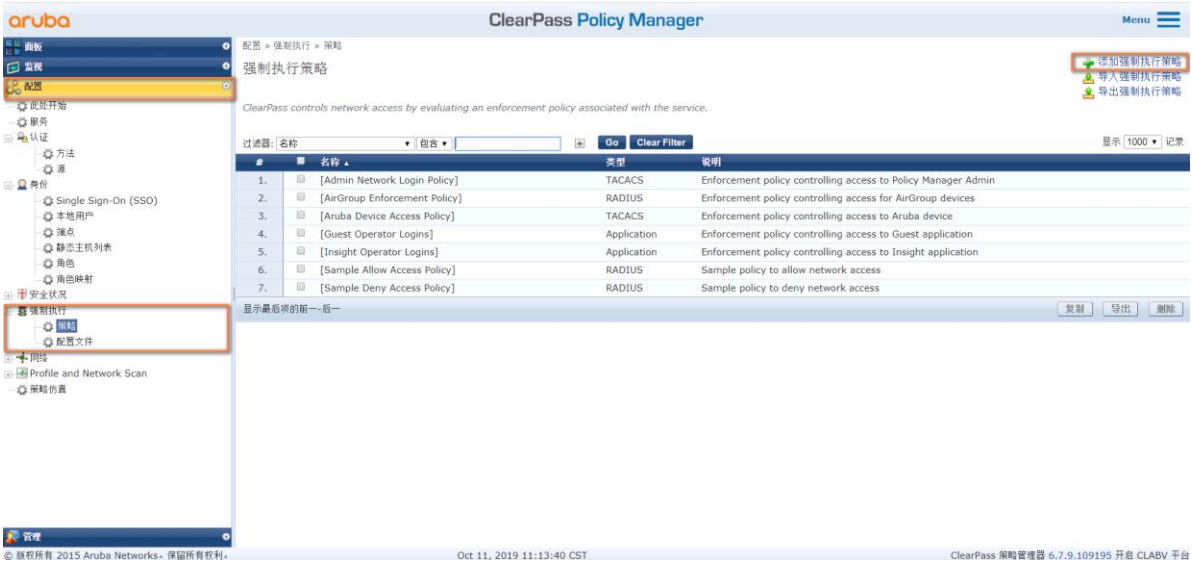
在属性选项卡中，输入下面的参数：

- ✓ 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

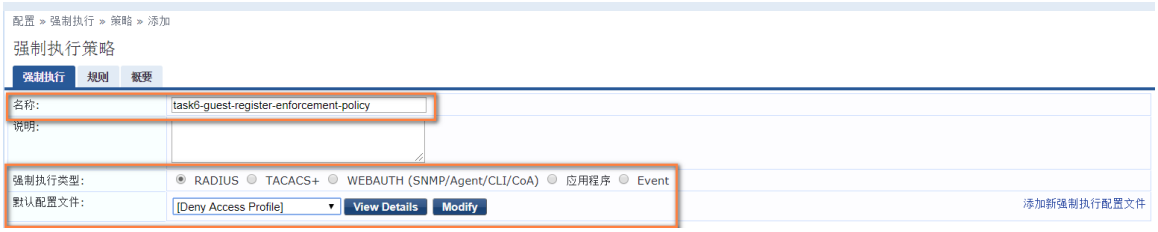


第2步：找到 配置 - > 强制执行 - > 策略 ， 点击右上角的 “添加强制执行策略” 按钮，增加一个强制执行策略：



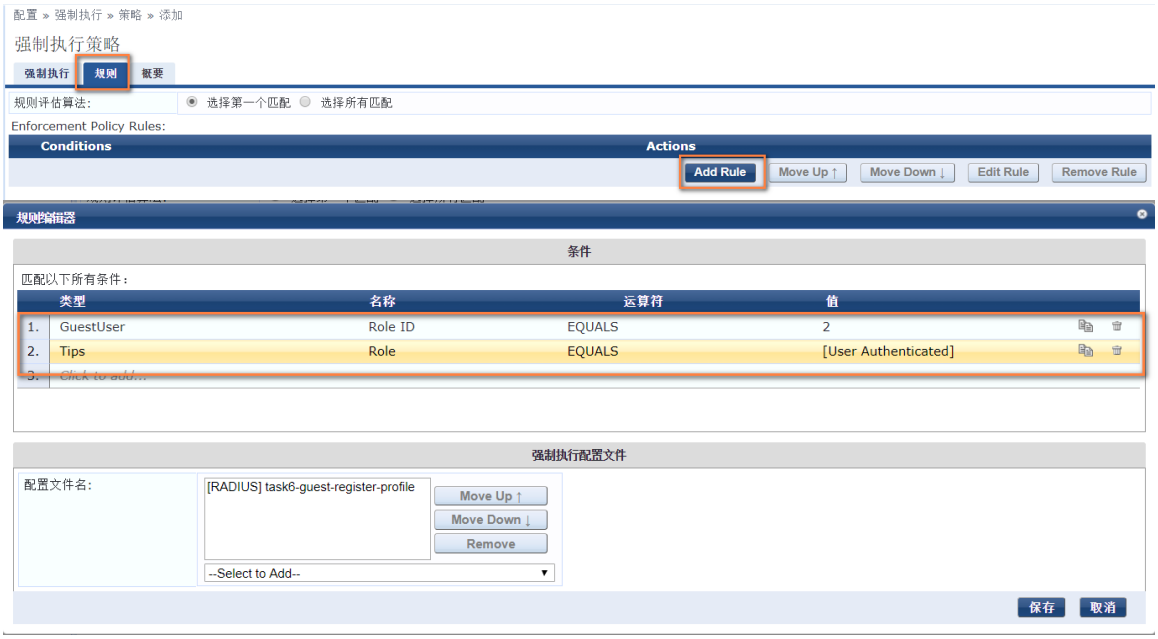
在强制执行选项卡中，输入下面的参数：

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



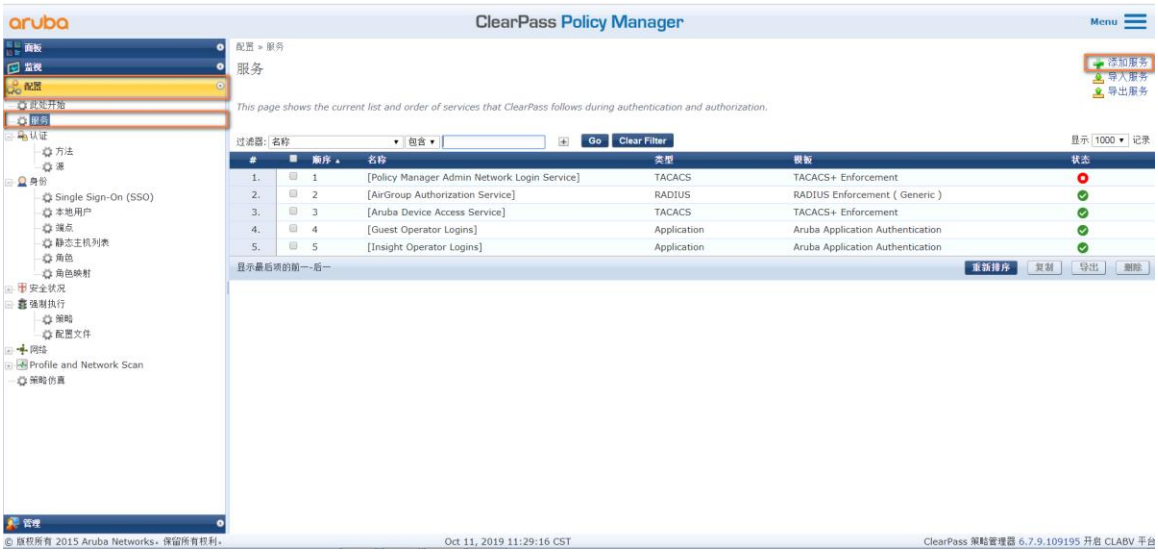
在规则选项卡中，输入下面的参数：

- ✓ 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



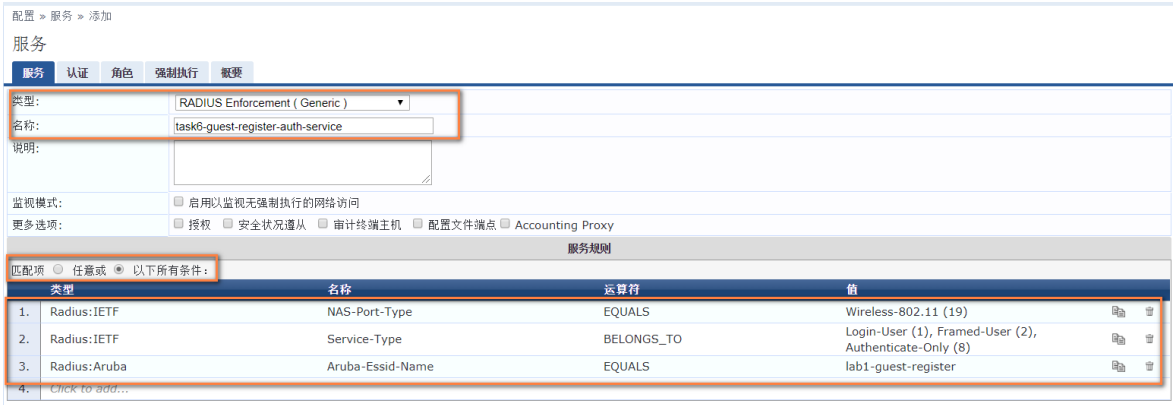
在概要选项卡中，对整体配置进行总览：

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：



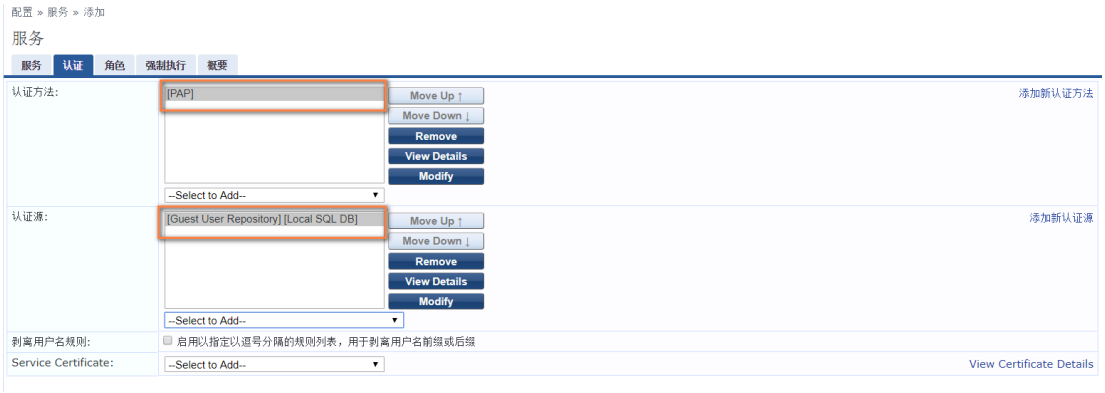
在服务选项卡中，输入下面的参数：

- ✓ 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）



在认证选项卡中，输入下面的参数：

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



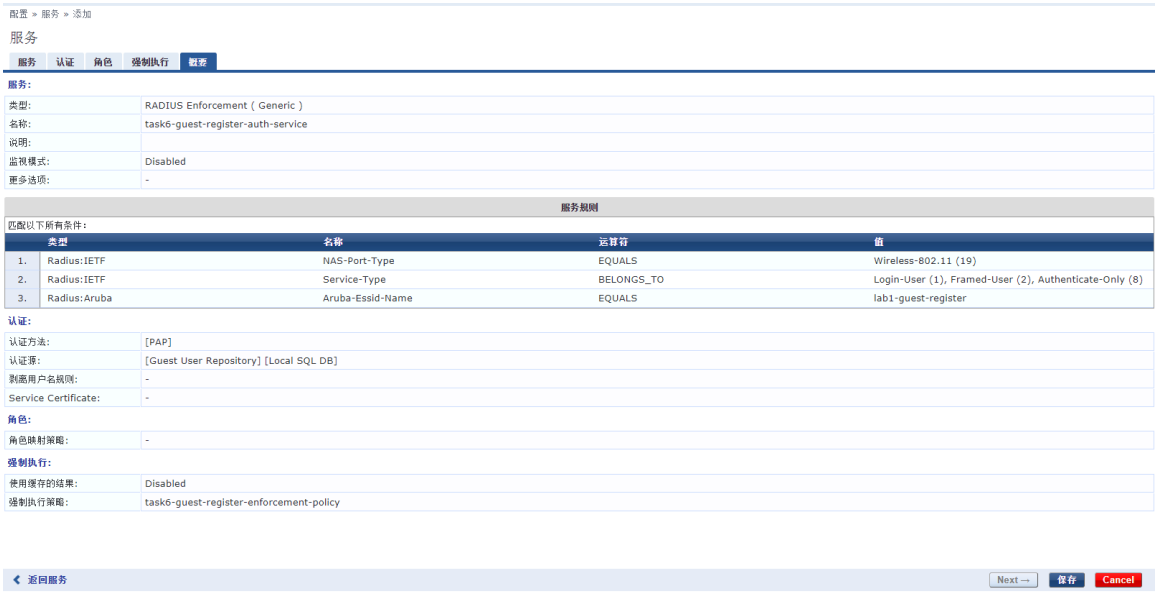
在角色选项卡中，暂时不做任何配置（详细内容可以参考高级介绍部分）

- ✓ 角色映射策略： 空

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*）

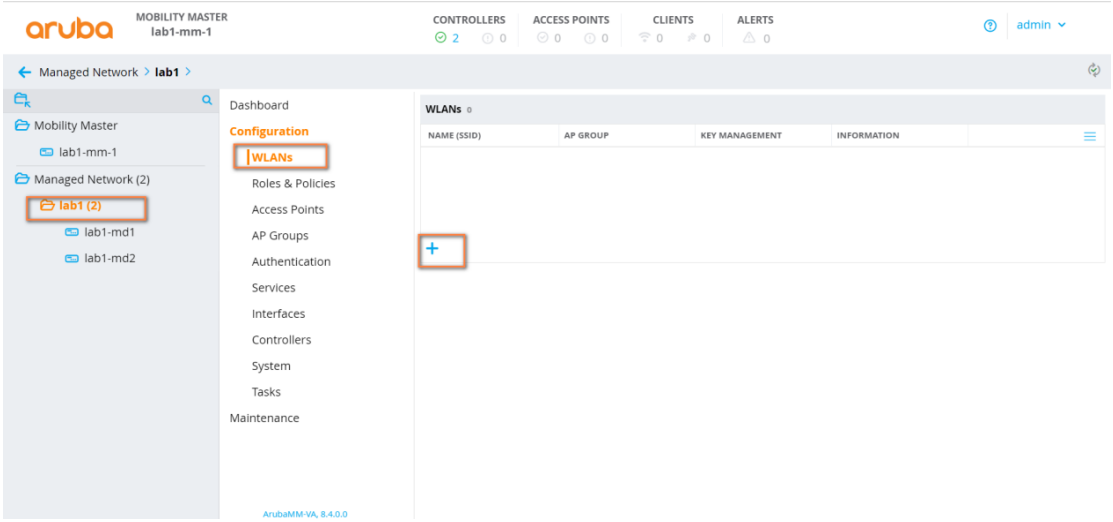
在概要选项卡中，对配置进行总览：



7.4 控制器配置

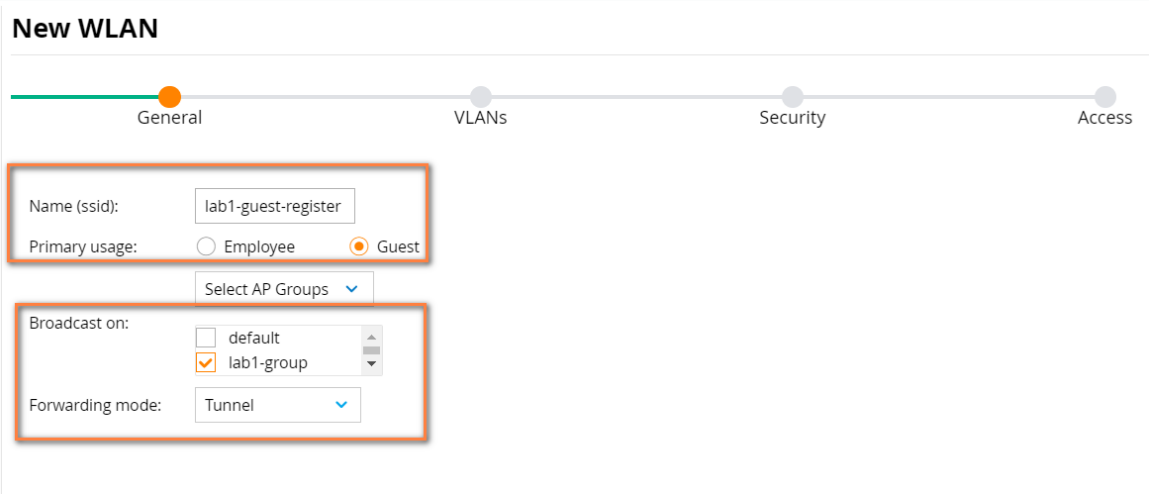
7.4.1 添加无线信号

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



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



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。

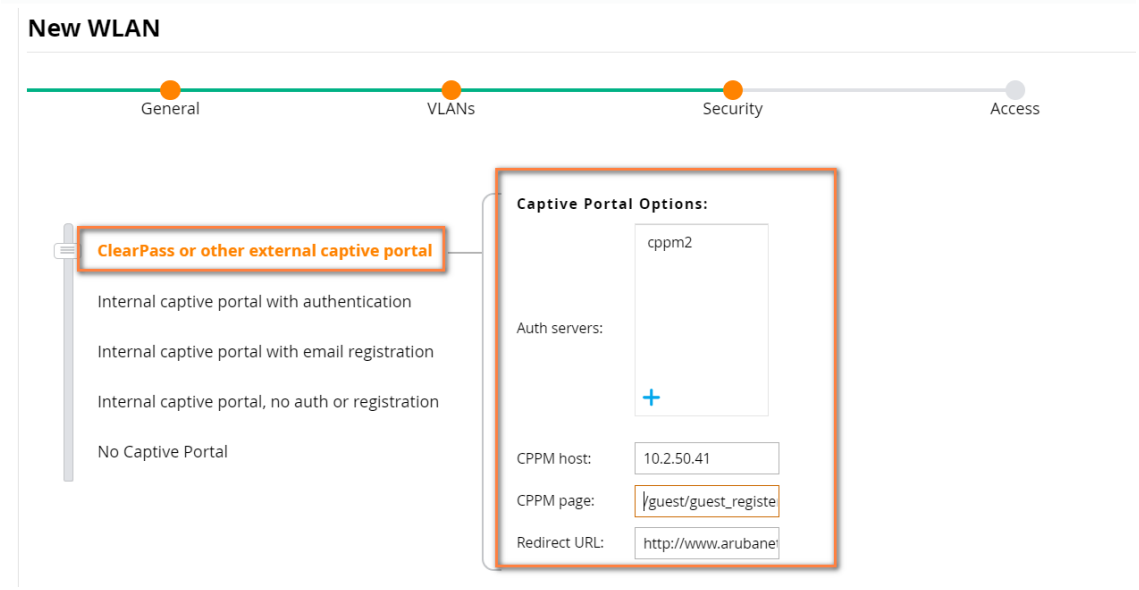
第4步：安全选项设置

- 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https://clearpass-ip 前缀，且是https://开头的。初始化向导后，补全的URL是

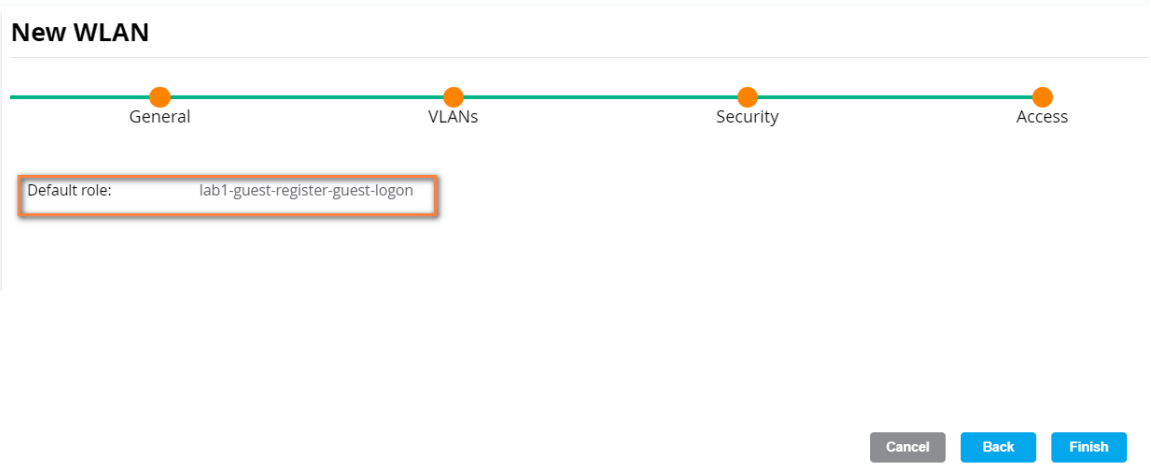
https://10.2.50.41/guest/guest_register_login.php?_browser=1，该URL就是captive portal profile中的Login page

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



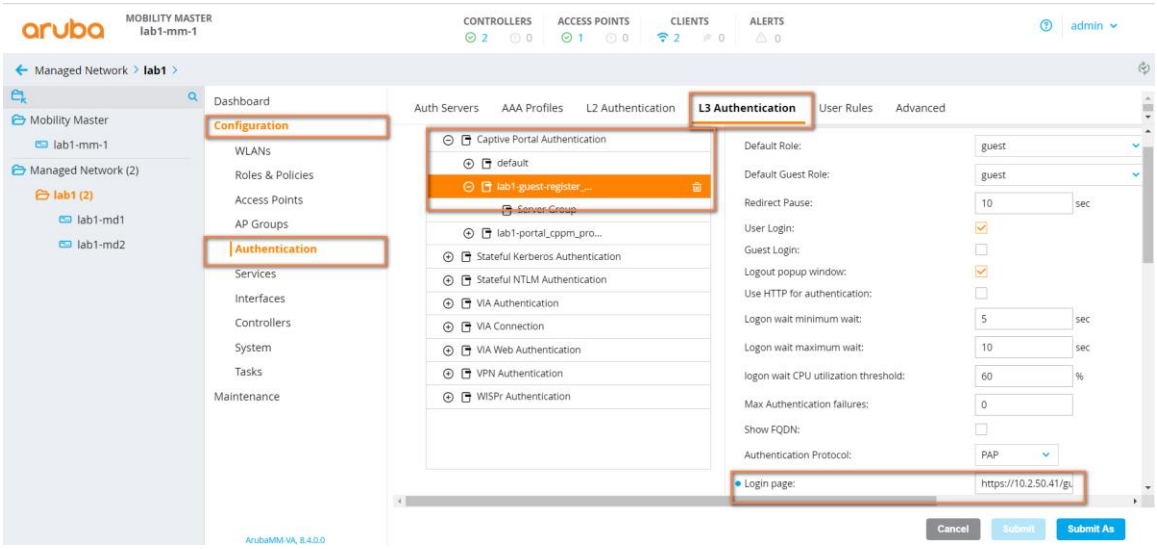
第5步：访问权限设置

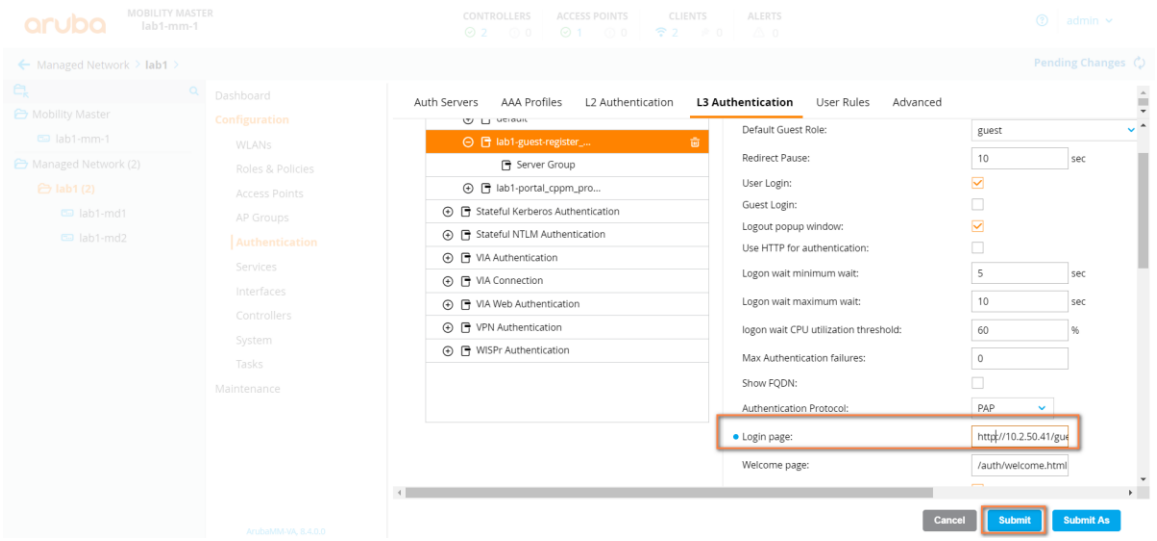
- 1、Default role： lab1-guest-register-guest-logon （向导自动创建好的，就是Portal认证前的角色，对应到aaa profile中的initial role）
- 2、Finish： 点击右下角的Finish 蓝色按钮，完成向导配置



第6步：更改 Captive Portal Authentication 配置，Managed Network - > labX （X： 1 ·····6） -> Configuration -> Authentication -> L3 Authentication ->Captive Portal Authentication ->labx-guest-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

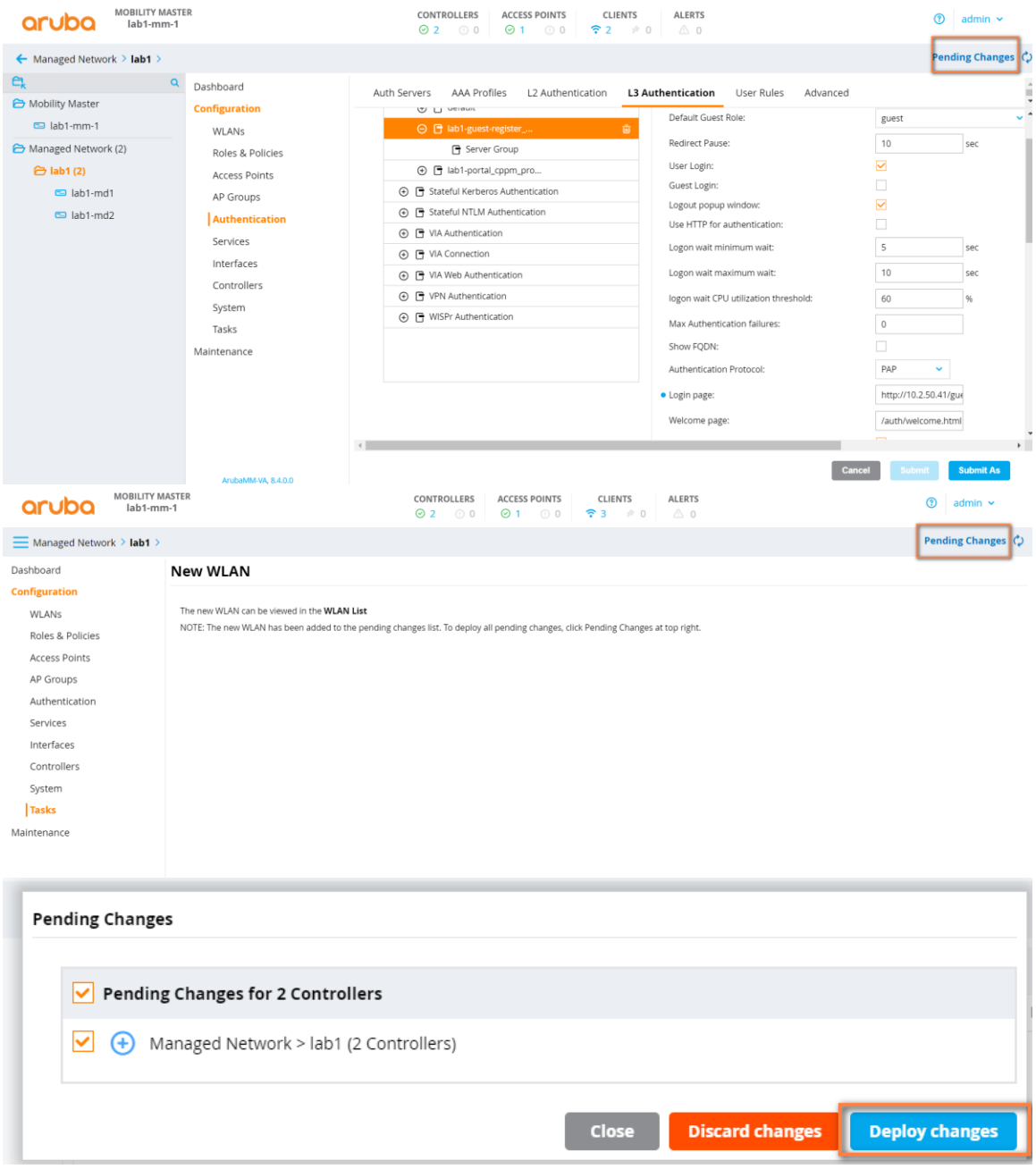
书告警提示，最后点击 Submit 按钮提交配置更改。（因为默认 aruba clearpass 采用的是自签服务器证书，如果需要 https 的安全跳转，强烈建议使用商业签发证书导入到 clearpass 中使用）。





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

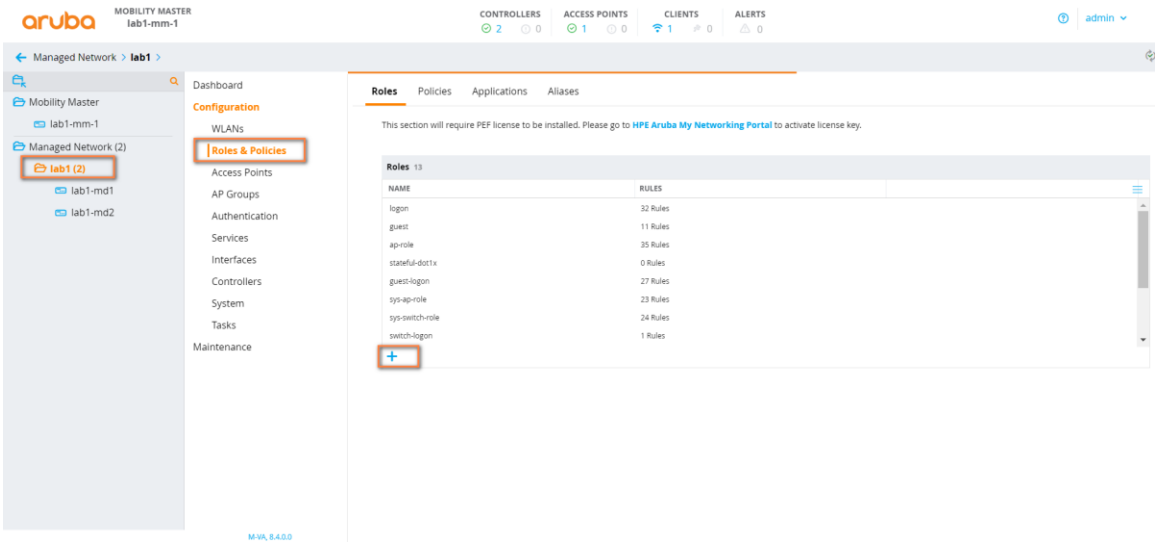


7.4.2 添加 Portal 重定向

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）。

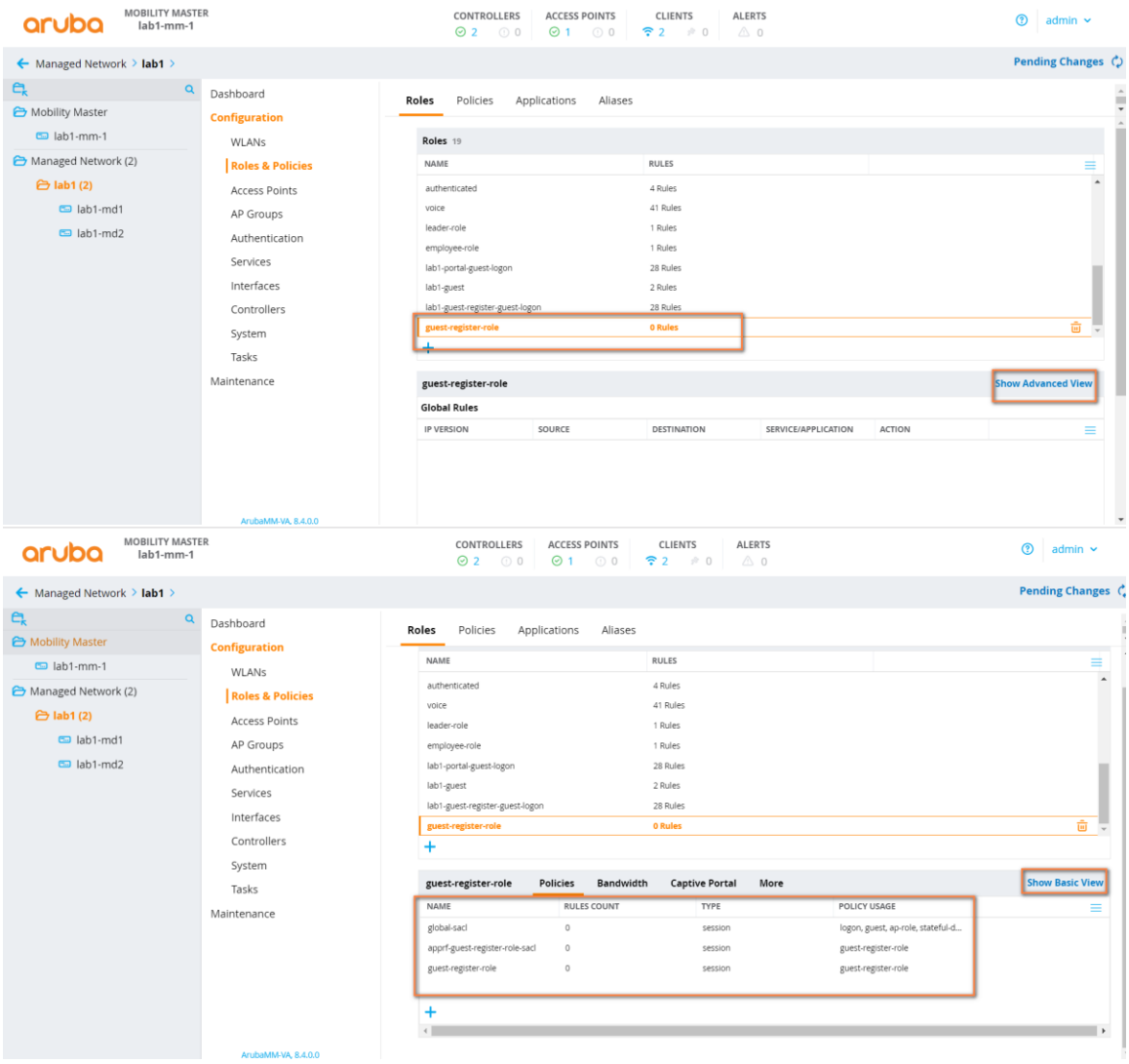


✓ Name： guest-register-role， 新建一个访客Portal认证后获得的role

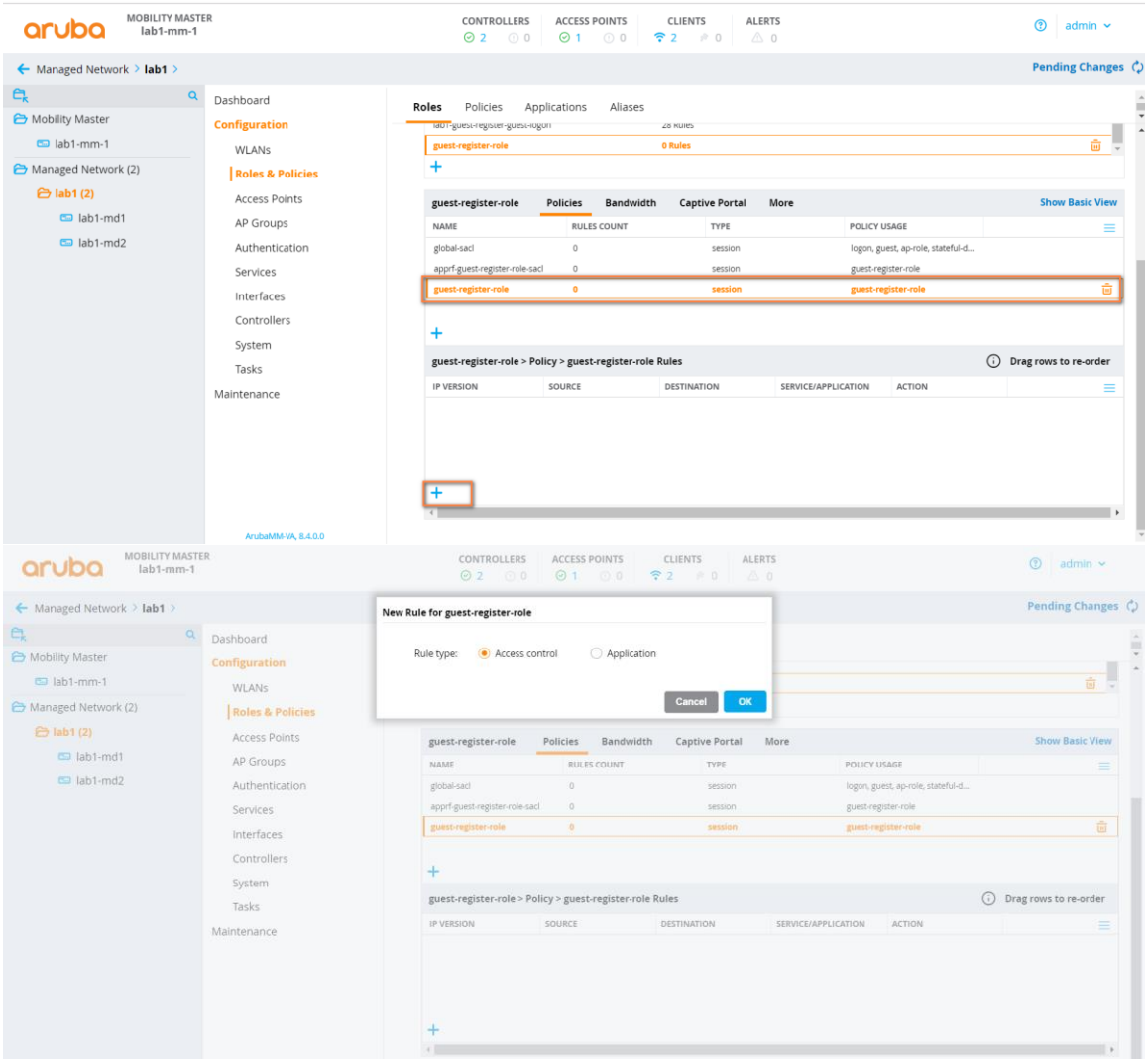
✓ 1、在roles里面，选择上一步创建好的guest-register-role

✓ 2、再点击右下角的show Advanced View

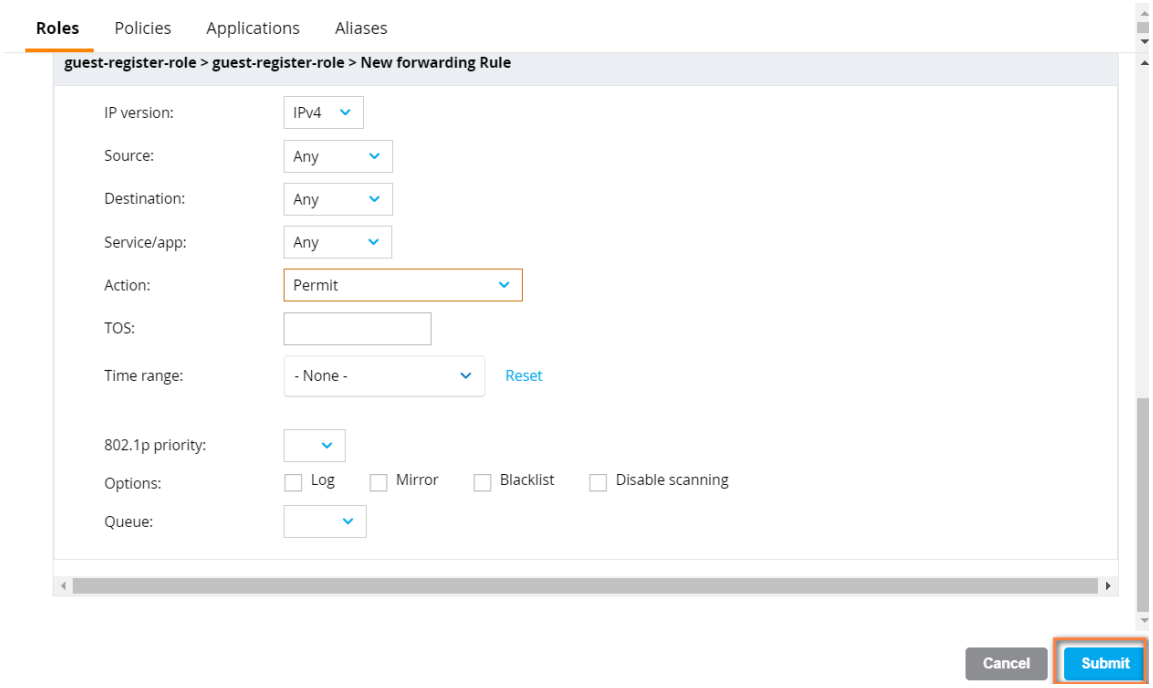
NOTE 需要事先在右上角的蓝色字体admin的下拉列表中选择preferences， 勾选 show advanced profiles



- ✓ 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

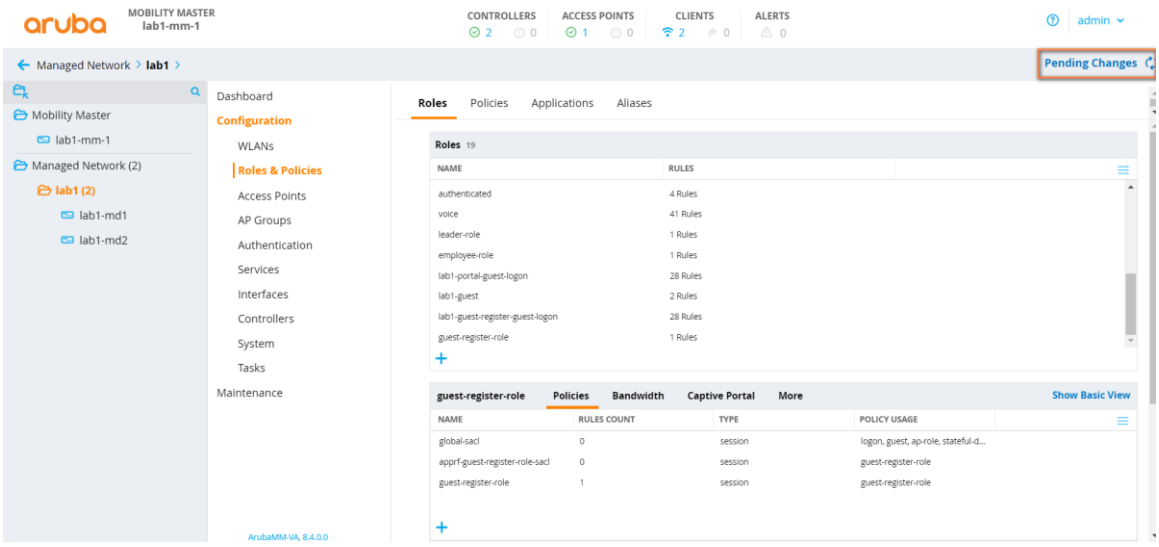


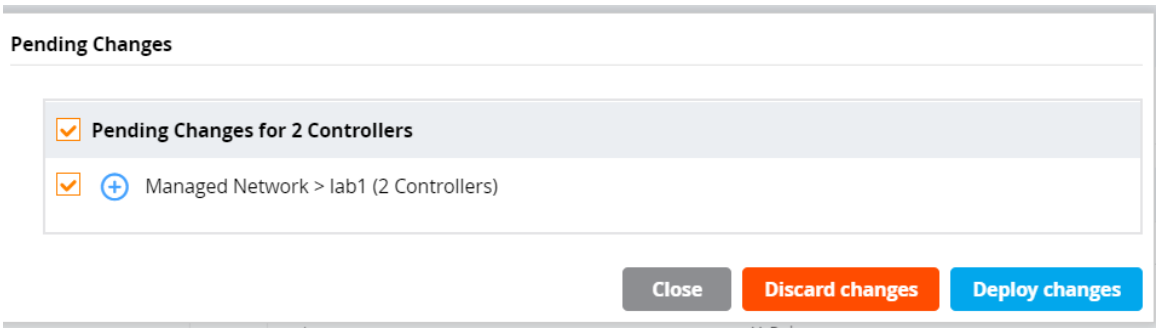
NOTE 如果这里无法看到Submit变成蓝色背景，请在Action 里面切换下动作，然后再重新选择Permit，这样Submit按钮会变成蓝色背景。



第2步:　配置保存并同步给md设备

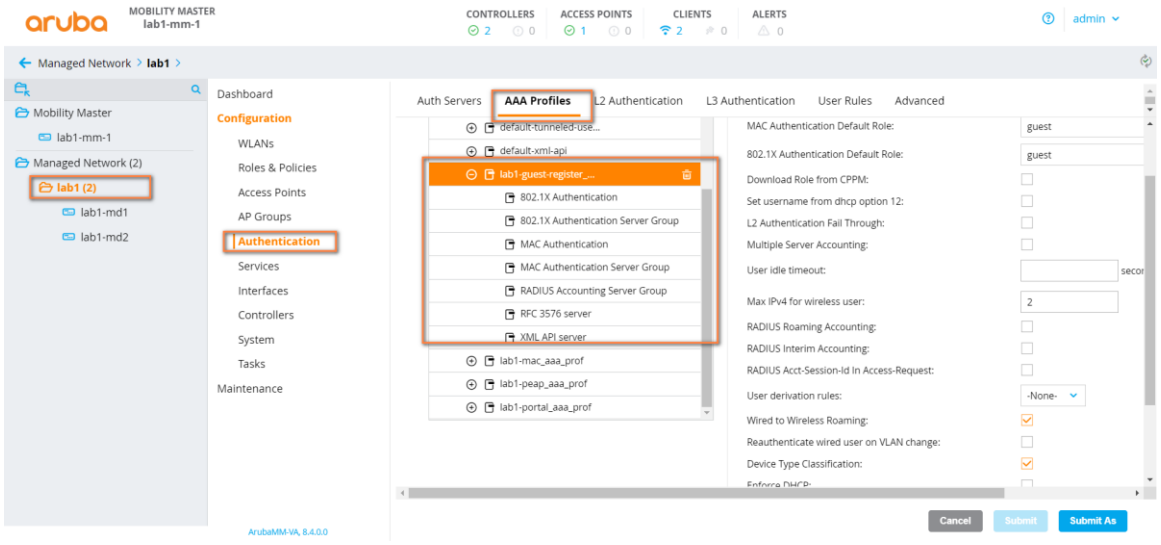
- 1、Pending Changes：　右上角点击该按钮
- 2、Deploy changes：　点击该按钮



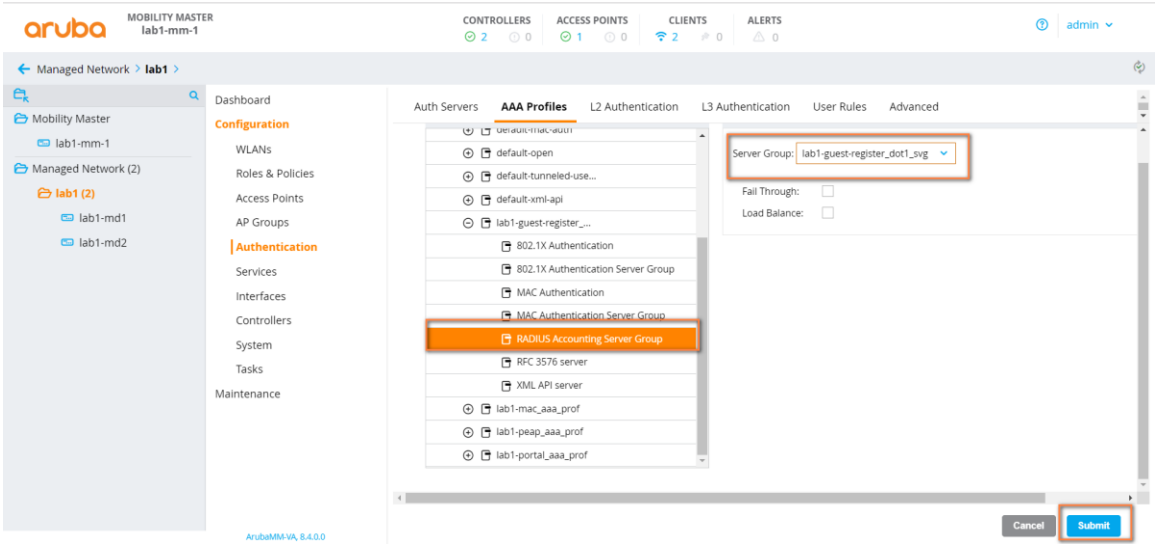


7.4.4 添加计费

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.

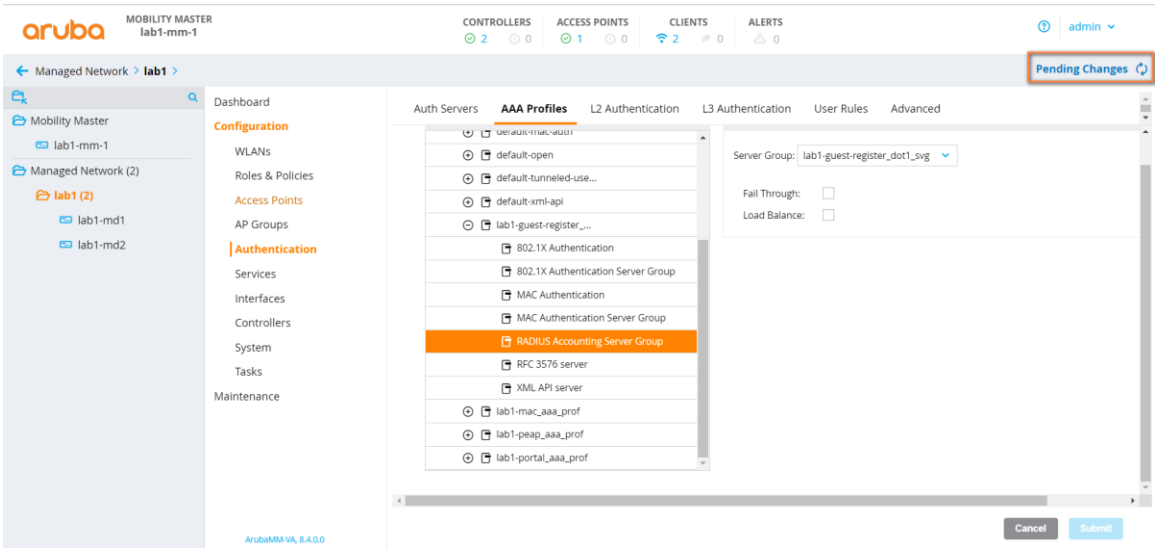


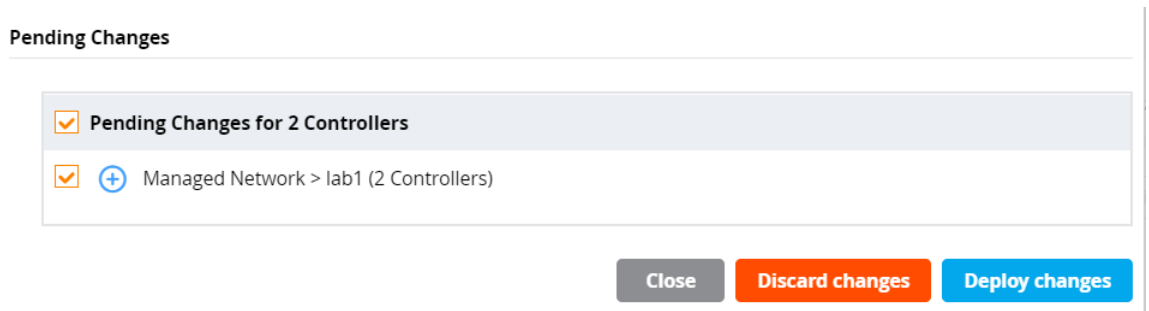
第2步: 选择 RADIUS Accounting Server Group，在右边配置窗口中，从 Server Group 下拉列表中选择之前向导已经创建好的 labX-guest-register_dot1_svg （X： 1 ·····6）. 点击右下角的 Submit 按钮。



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

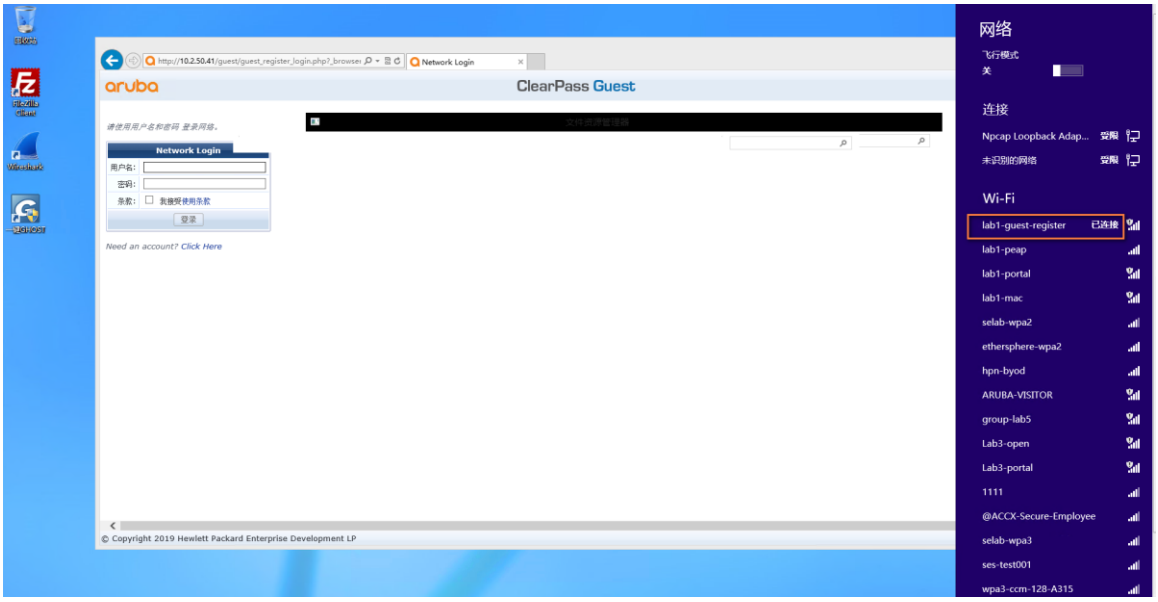


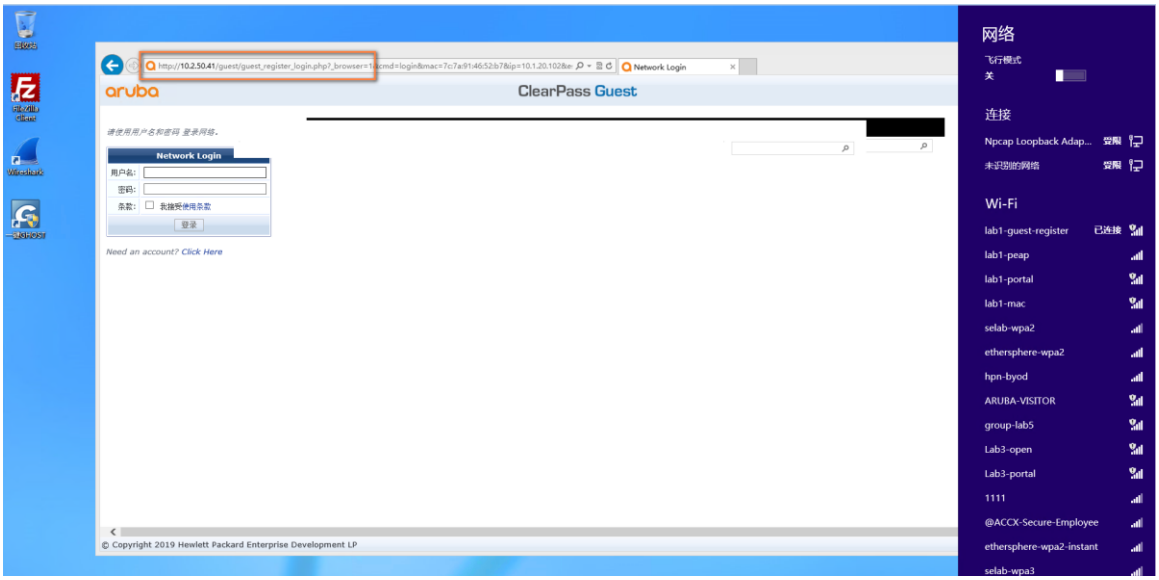


7.5 验证结果

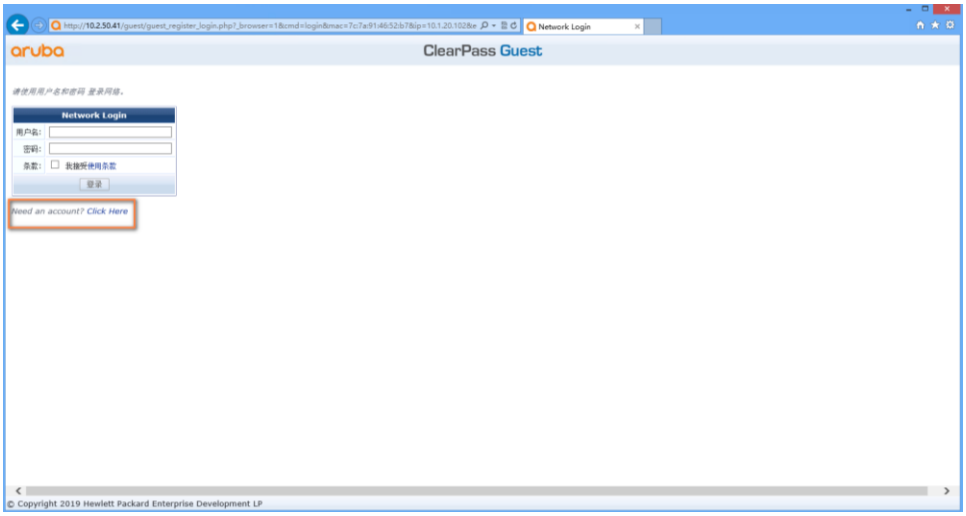
7.5.1 终端侧的无线关联和访客自注册

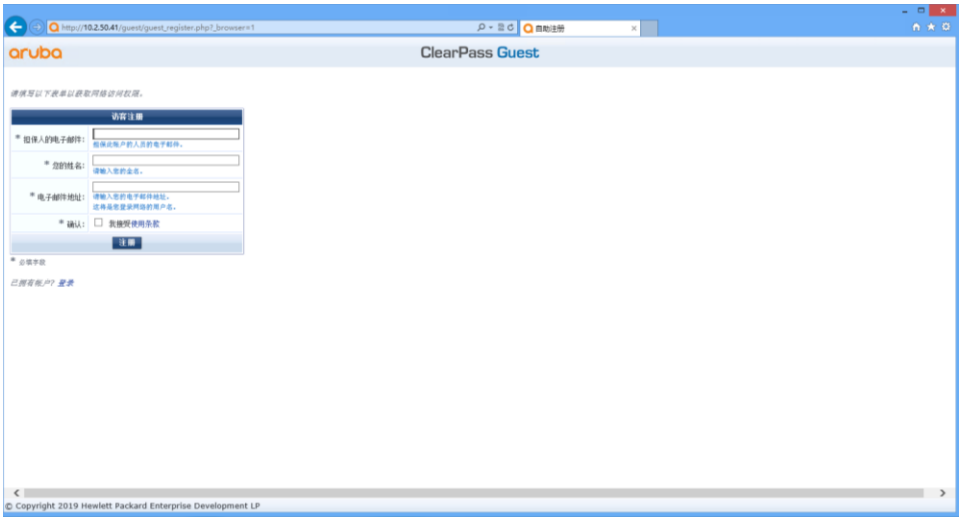
我们在测试终端上，关联到打开浏览器输入任何网址，被重定向到ClearPass 的Guest登录页面上。

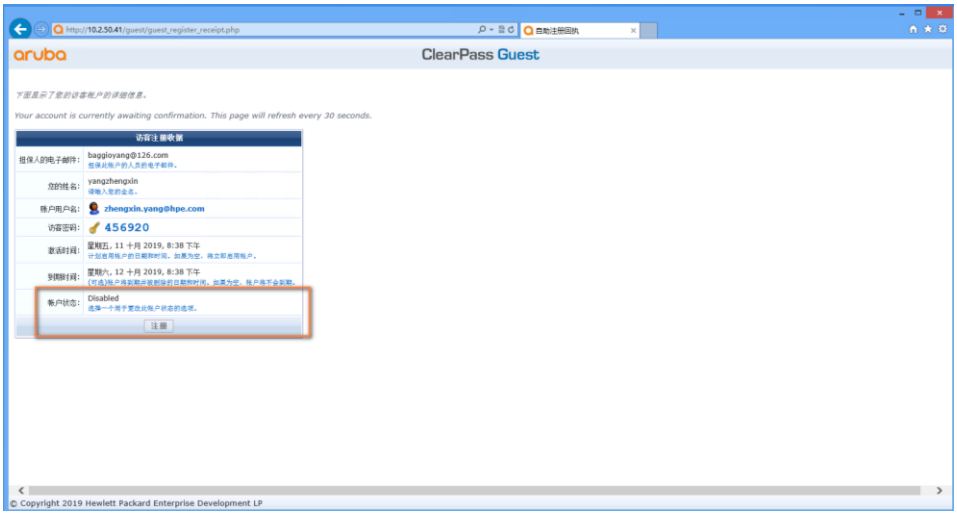




点击Click Here，进入到自注册页面。

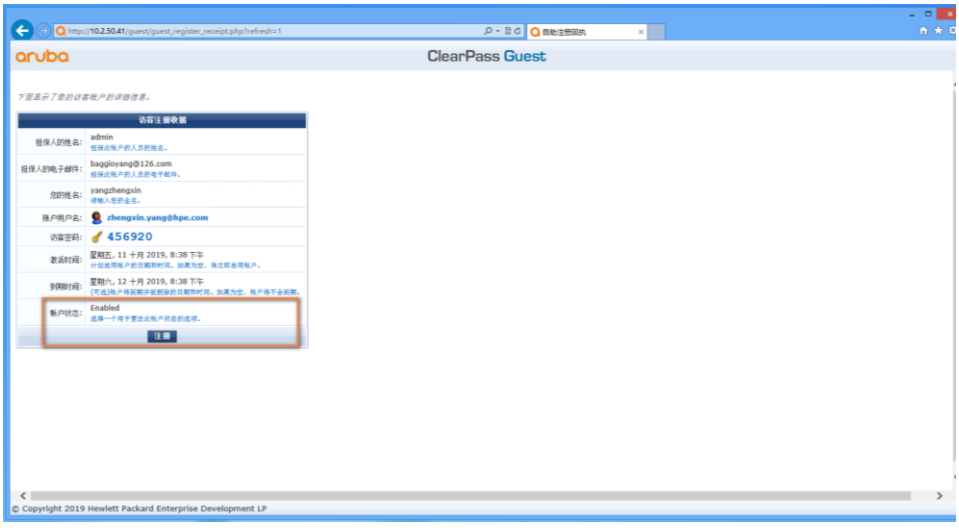


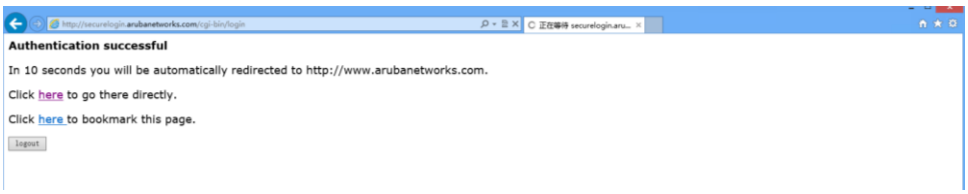




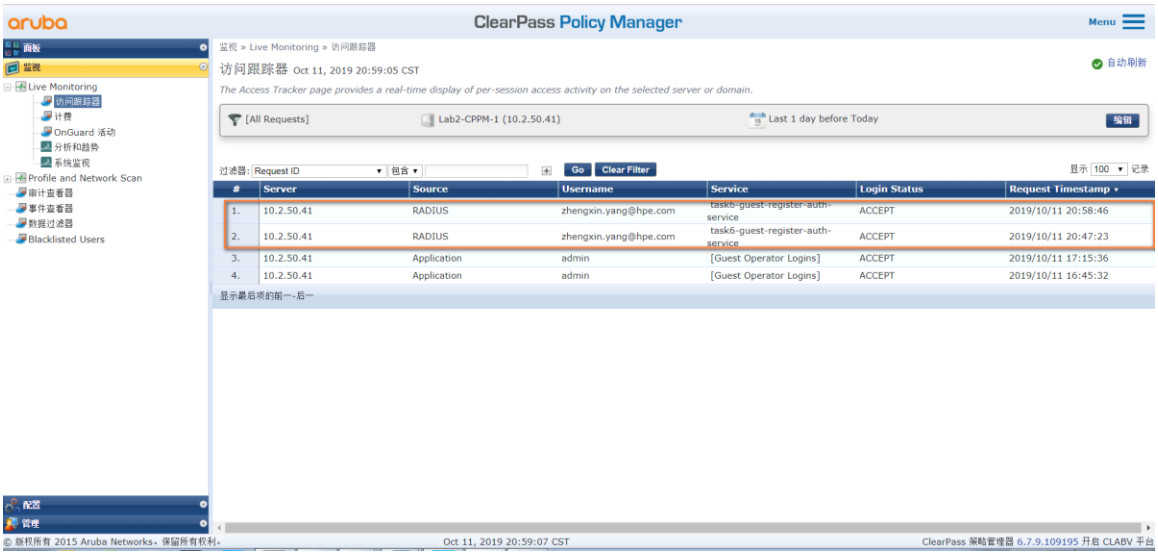
接着联系人会收到该访客自注册的申请批复邮件，需要联系人批准下。

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。





7.5.2 CPPM 上查看认证记录

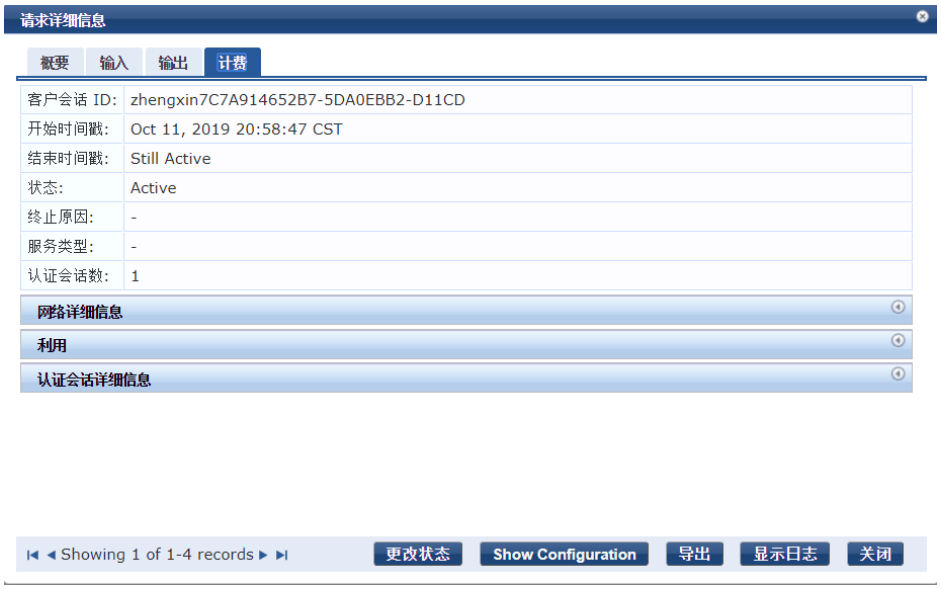


✓ 点击认证成功记录，在“概要“选项卡中观察，看看能看到哪些信息。

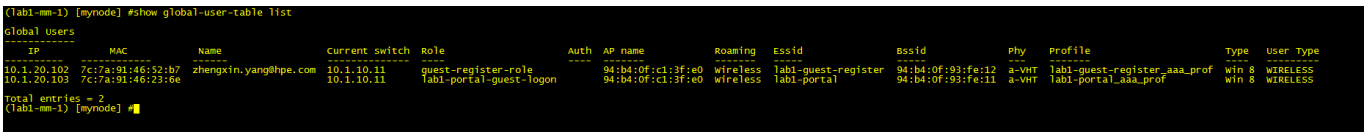
✓ 点击“输入“选项卡中观察，看看能看到哪些信息。

✓ 点击“输出“选项卡中观察，看看能看到哪些信息。

✓ 点击“计费“选项卡中观察，看看能看到哪些信息。



7.5.3 控制器上查看认证记录



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: _____

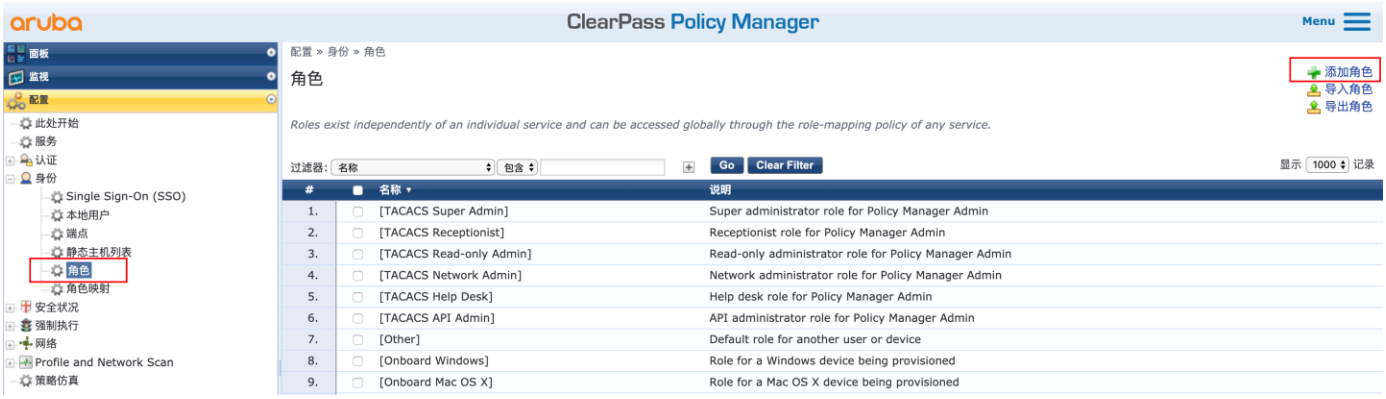
8.3 ClearPass 配置

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。

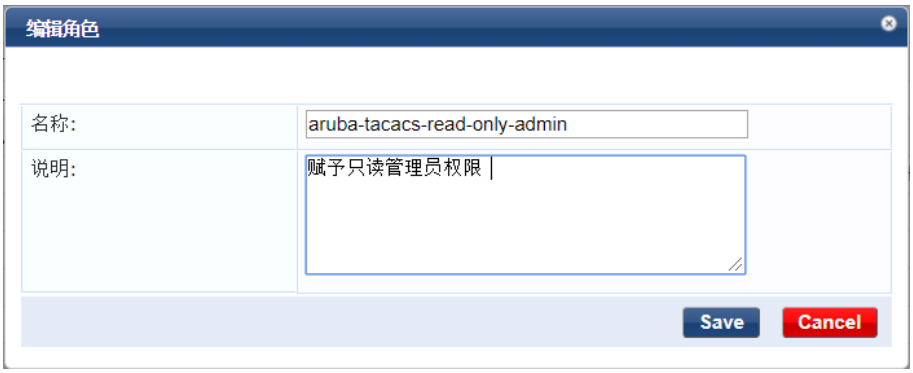
8.3.2 添加本地账号和角色

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:



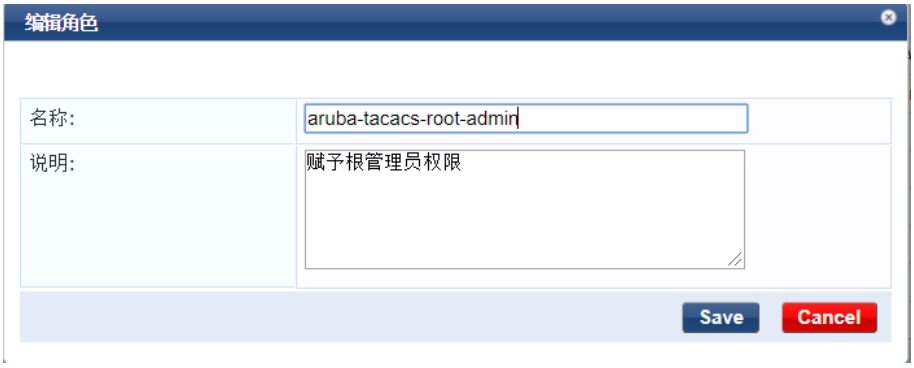
在添加新角色1的窗口中，输入下面的参数：

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

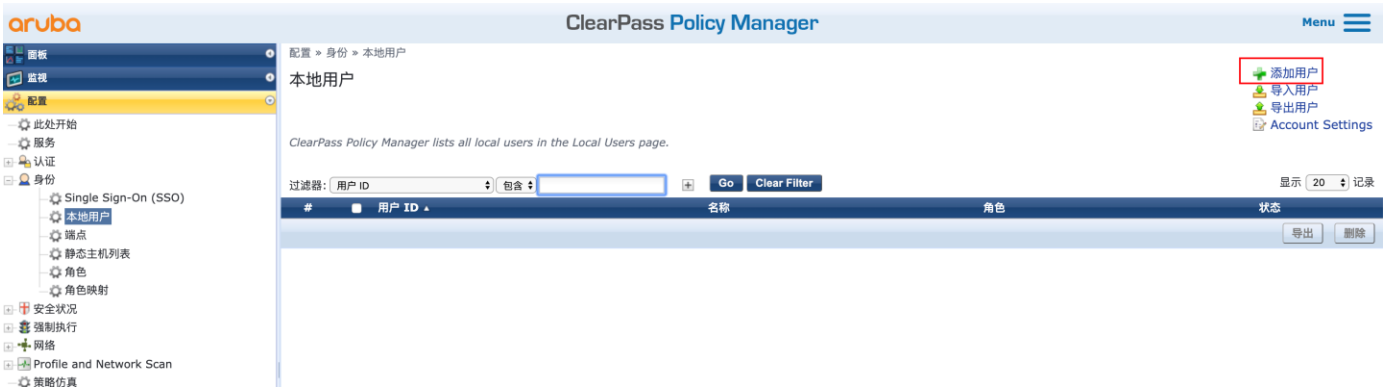


在添加新角色2的窗口中，输入下面的参数：

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



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：



在添加账号1的窗口中，输入下面的参数：

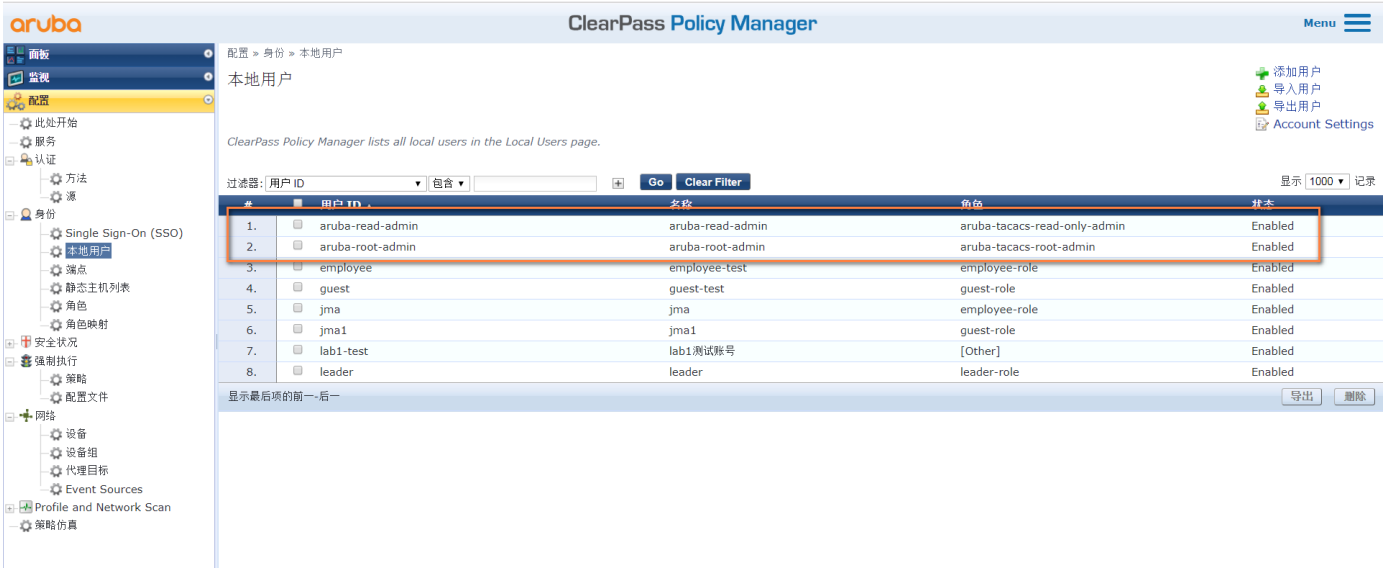
- ✓ 用户ID：aruba-read-admin （即用户的登录账号）

- ✓ 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）

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）

配置总览：

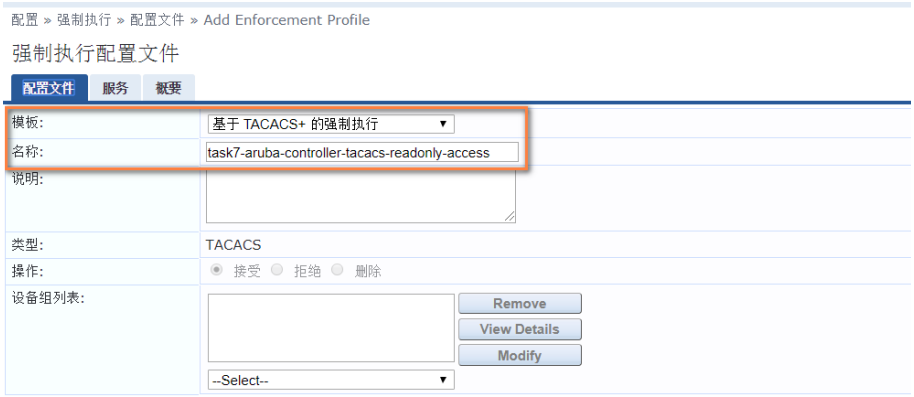


8.3.3 添加认证服务

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：

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

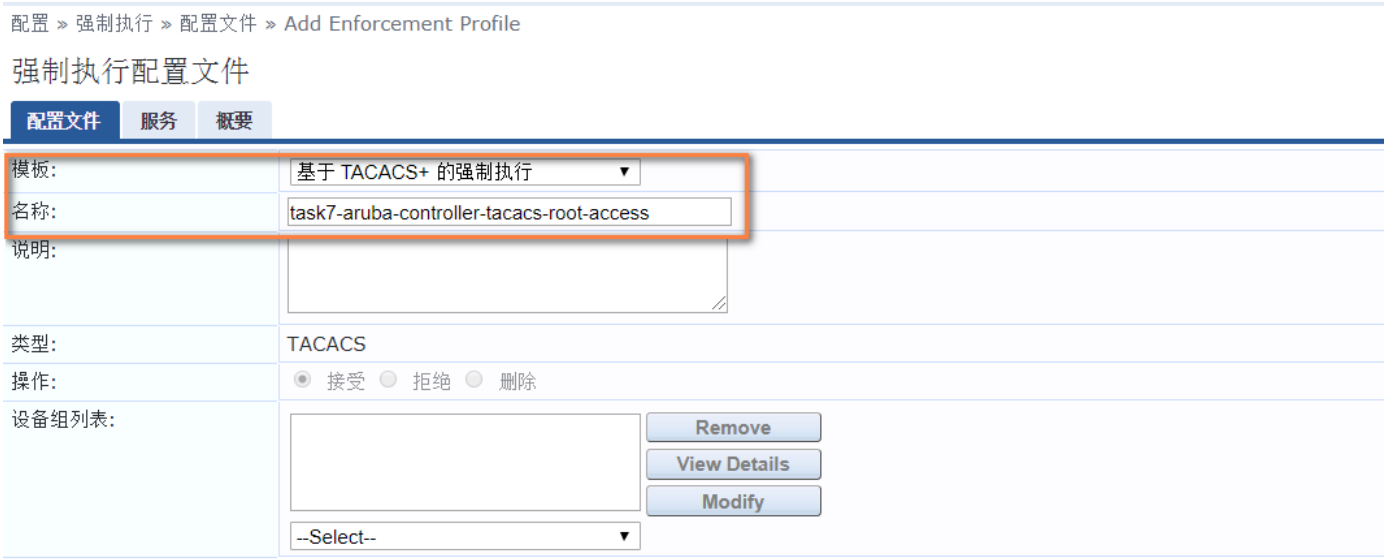


在服务选项卡中，输入下面的参数：

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

在配置文件（第二个）选项卡中，输入下面的参数：

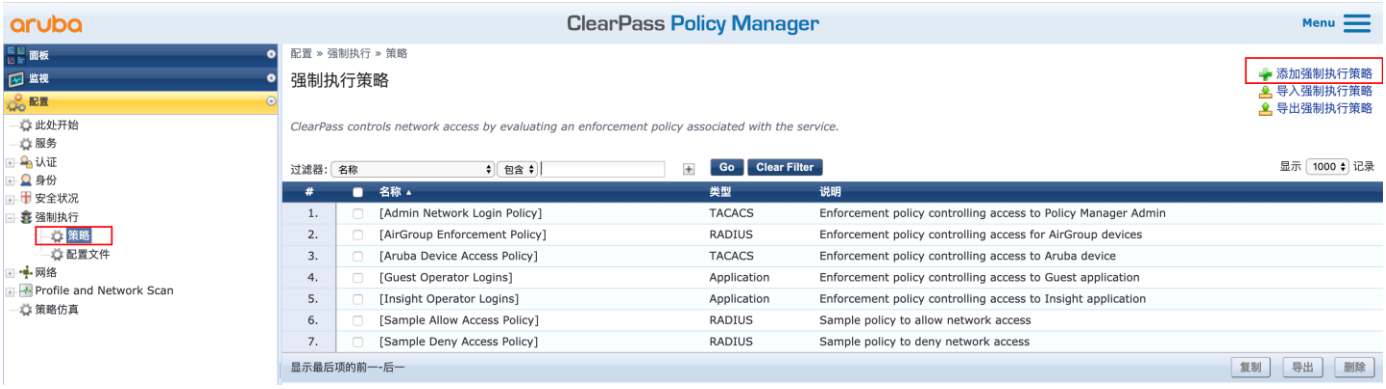
- ✓ 模板：基于TACACS+的强制执行
- ✓ 名称： task7-aruba-controller-tacacs-root-access



在服务选项卡中，输入下面的参数：

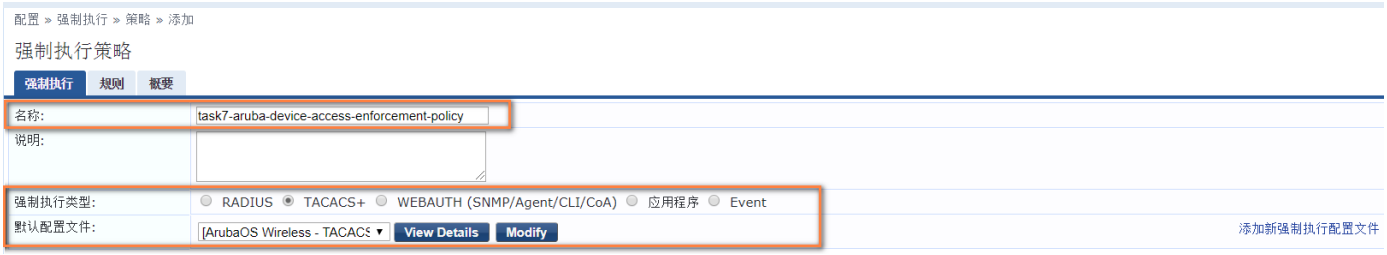
- ✓ 权限级别： 15(Privileged)
- ✓ 所选服务： Aruba:Common
- ✓ Authorize Attribute Status： ADD
- ✓ Aruba:Common Aruba-Admin-Role = root

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：



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]

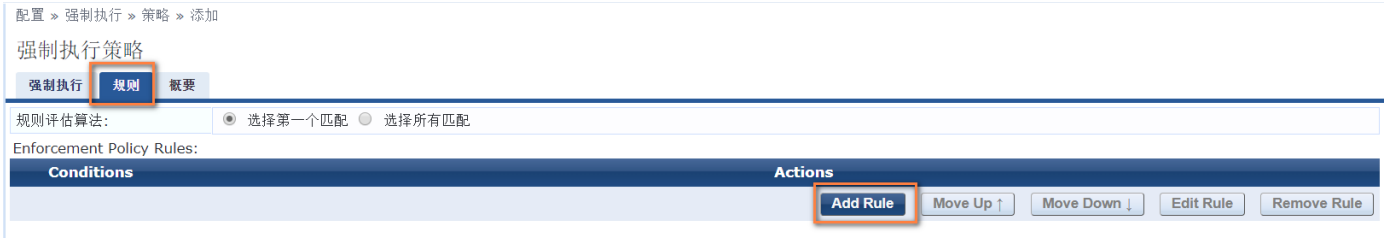


在规则选项卡中，输入下面的参数：

- ✓ 规则：点击“Add Rule”,配置如下：

添加第一个规则

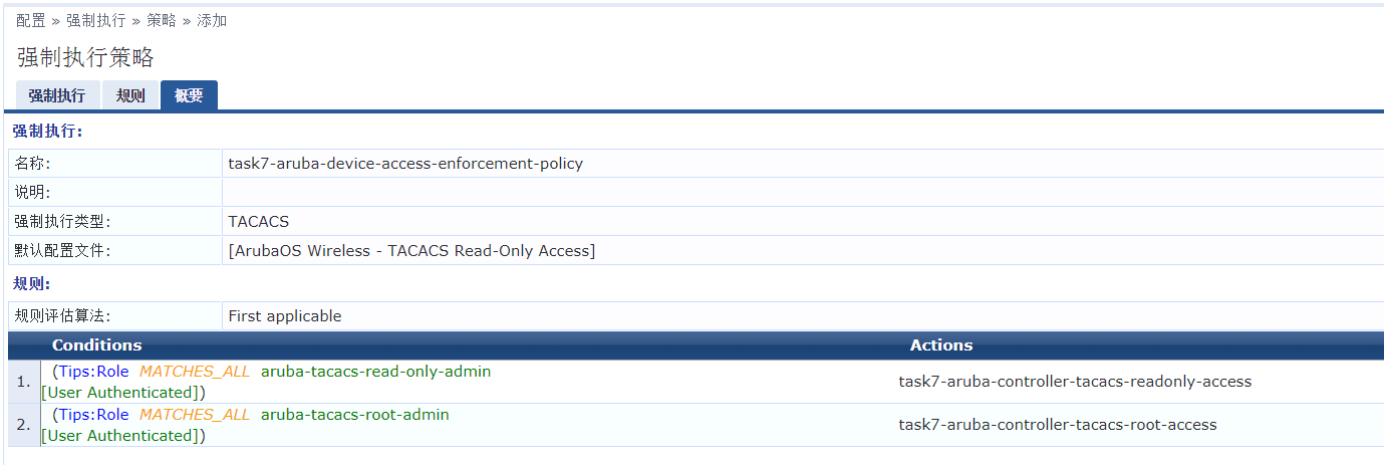
- ✓ 条件是： Tips Role MATCHES_ALL aruba-tacacs-read-only-admin，[User Authenticated]
- ✓ 配置文件名： task7-aruba-controller-tacacs-readonly-access



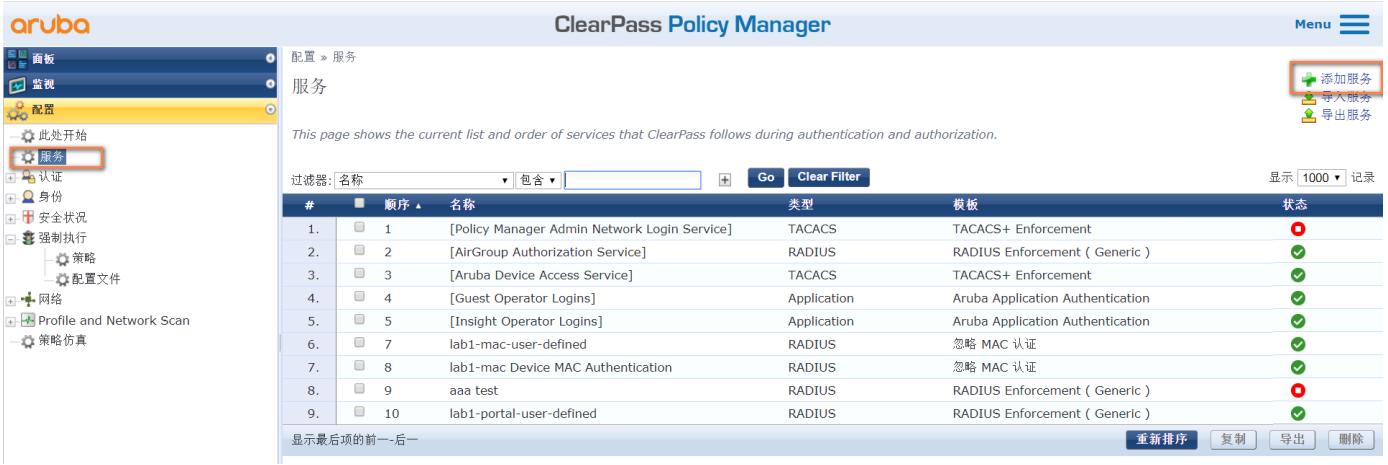
再添加第二个规则

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

在概要选项卡中，对整体配置进行总览：

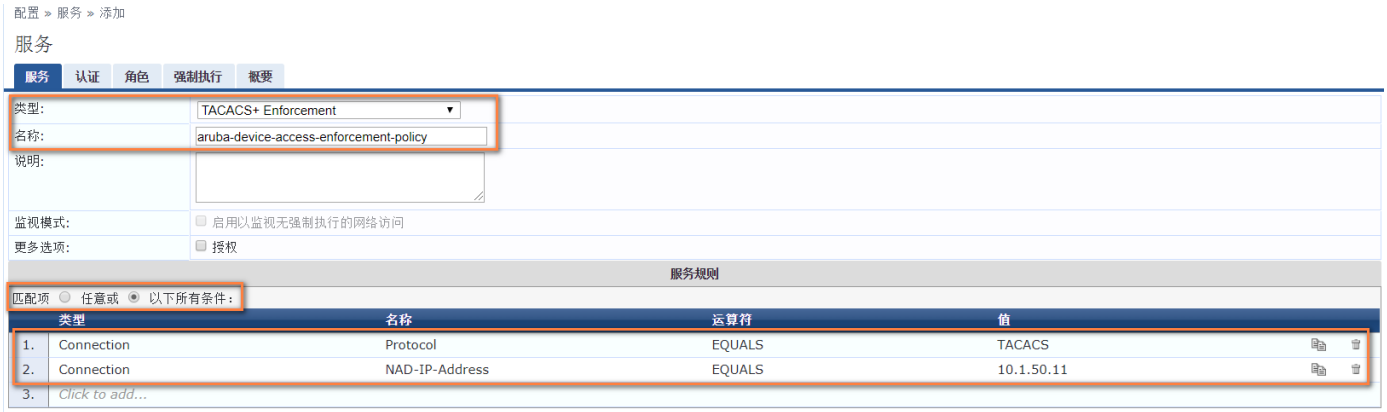


第3步：找到 配置 - > 服务 ， 点击右上角的 “添加服务” 按钮，增加一个服务：



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）



在认证选项卡中，输入下面的参数：

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

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

在强制执行选项卡中，输入下面的参数：

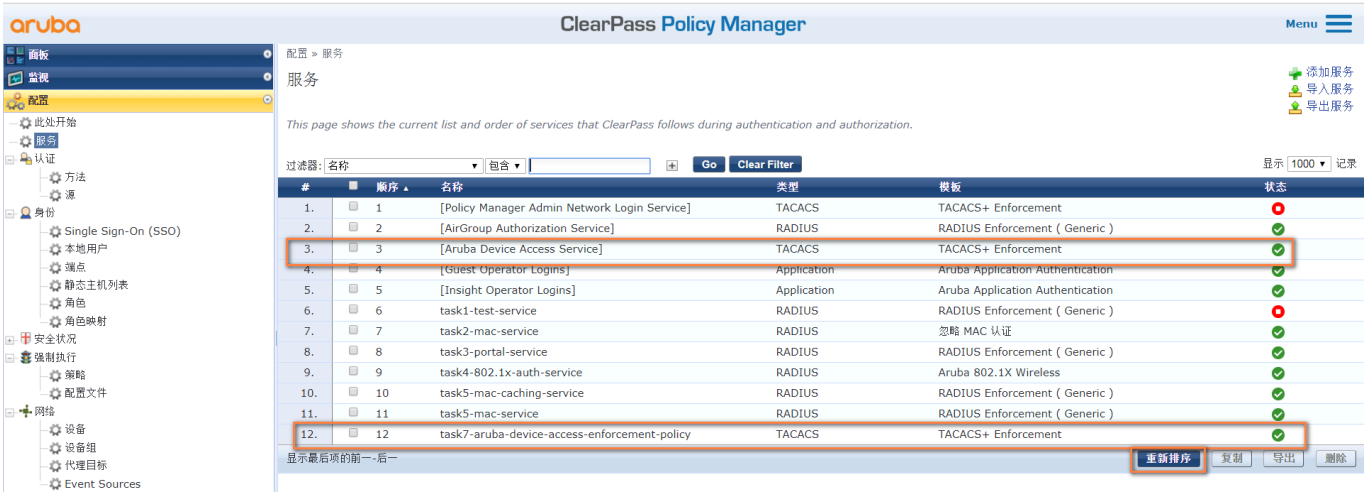
- ✓ 强制执行策略： task7-aruba-device-access-enforcement-policy （*即第2步中创建的强制执行策略*）

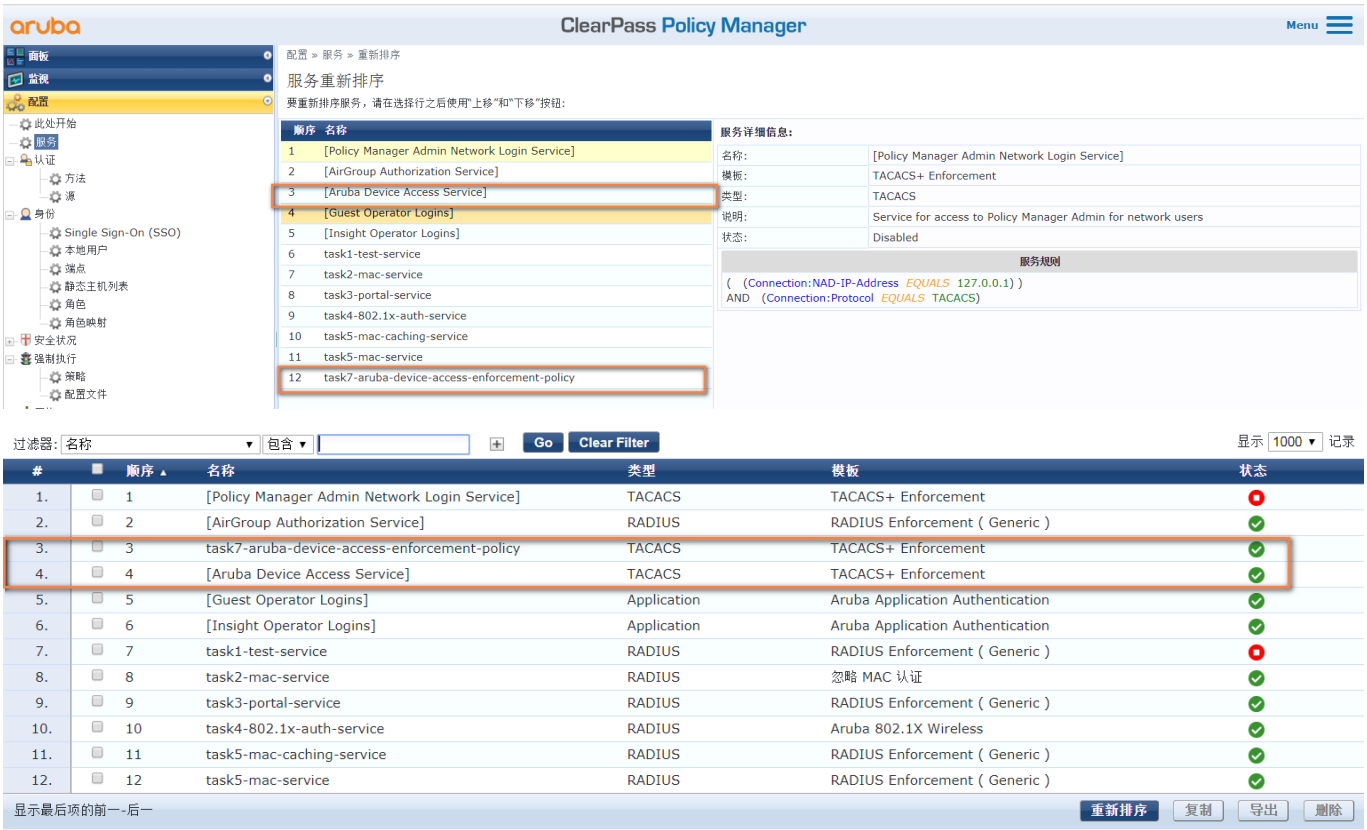
在概要选项卡中，对配置进行总览：

第4步：找到 配置 - > 服务 ，将刚才创建的认证服务调整优先级：

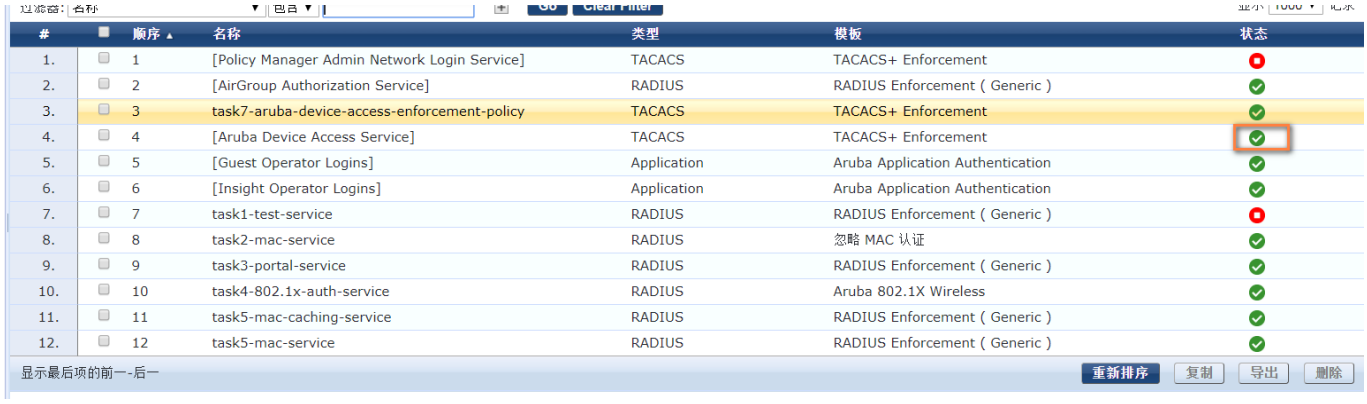
ClearPass系统安装好后，默认就会在服务中添加了一个 Aruba Device Access Service 服务，该服务的匹配规则是空的，也即是任何aruba的tacacs请求服务都会优先击中这条 service（从上至下的优先匹配原则）。

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
ClearPass Policy Manager
Menu
面板
监视
配置
此处开始
服务
认证
方法
源
身份
Single Sign-On (SSO)
本地用户
端点
静态主机列表
角色
角色映射
安全状况
强制执行
策略
配置文件
网络
设备
设备组
代理目标
Event Sources
配置 » 服务
服务
添加服务
导入服务
导出服务
This page shows the current list and order of services that ClearPass follows during authentication and authorization.
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
2. 2 [AirGroup Authorization Service] RADIUS RADIUS Enforcement (Generic)
3. 3 [Aruba Device Access Service] TACACS TACACS+ Enforcement
4. 4 [Guest Operator Logins] Application Aruba Application Authentication
5. 5 [Insight Operator Logins] Application Aruba Application Authentication
6. 6 task1-test-service RADIUS RADIUS Enforcement (Generic)
7. 7 task2-mac-service RADIUS 忽略 MAC 认证
8. 8 task3-portal-service RADIUS RADIUS Enforcement (Generic)
9. 9 task4-802.1x-auth-service RADIUS Aruba 802.1X Wireless
10. 10 task5-mac-caching-service RADIUS RADIUS Enforcement (Generic)
11. 11 task5-mac-service RADIUS RADIUS Enforcement (Generic)
12. 12 task7-aruba-device-access-enforcement-policy TACACS TACACS+ Enforcement
显示最后项的前一-后一
重新排序 复制 导出 删除

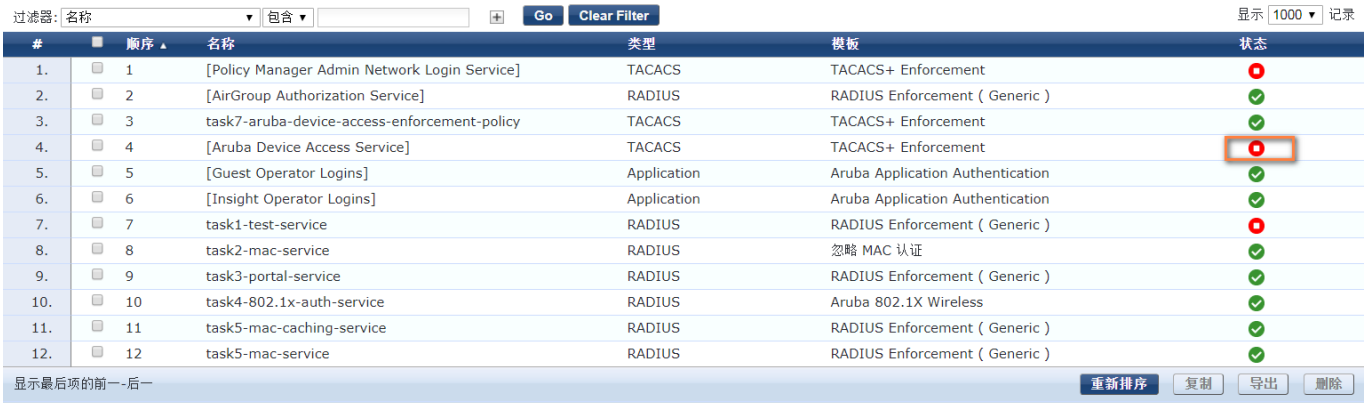

aruba
ClearPass Policy Manager
Menu
面板
监视
配置
此处开始
服务
认证
方法
源
身份
Single Sign-On (SSO)
本地用户
端点
静态主机列表
角色
角色映射
安全状况
强制执行
策略
配置文件
配置 » 服务 » 重新排序
服务重新排序
要重新排序服务，请在选择行之后使用"上移"和"下移"按钮:
顺序 名称
1 [Policy Manager Admin Network Login Service]
2 [AirGroup Authorization Service]
3 [Aruba Device Access Service]
4 [Guest Operator Logins]
5 [Insight Operator Logins]
6 task1-test-service
7 task2-mac-service
8 task3-portal-service
9 task4-802.1x-auth-service
10 task5-mac-caching-service
11 task5-mac-service
12 task7-aruba-device-access-enforcement-policy
服务详细信息:
名称: [Policy Manager Admin Network Login Service]
模板: TACACS+ Enforcement
类型: TACACS
说明: Service for access to Policy Manager Admin for network users
状态: Disabled
服务规则
((Connection:NAD-IP-Address EQUALS 127.0.0.1))
AND (Connection:Protocol EQUALS TACACS)
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
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
5. 5 [Guest Operator Logins] Application Aruba Application Authentication
6. 6 [Insight Operator Logins] Application Aruba Application Authentication
7. 7 task1-test-service RADIUS RADIUS Enforcement (Generic)
8. 8 task2-mac-service RADIUS 忽略 MAC 认证
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)
显示最后项的前一-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。



#		顺序 ▲	名称	类型	模板	状态
1.		1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	
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	
5.		5	[Guest Operator Logins]	Application	Aruba Application Authentication	
6.		6	[Insight Operator Logins]	Application	Aruba Application Authentication	
7.		7	task1-test-service	RADIUS	RADIUS Enforcement (Generic)	
8.		8	task2-mac-service	RADIUS	忽略 MAC 认证	
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)	

显示最后项的前一-后一　　重新排序　复制　导出　删除



过滤器: 名称 ▾ 包含 ▾ Go Clear Filter　　显示 1000 ▾ 记录

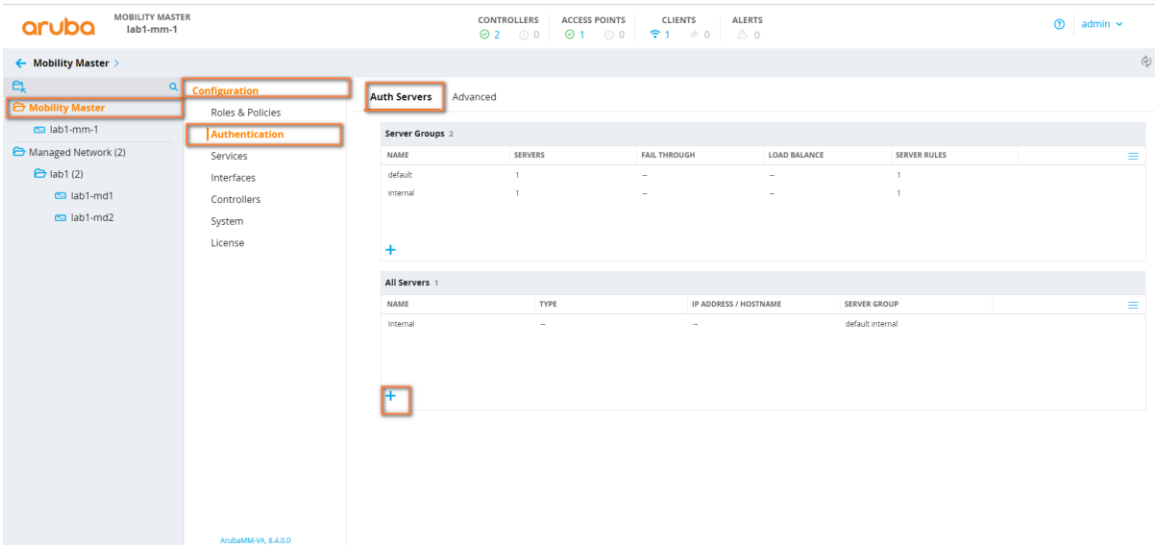
#		顺序 ▲	名称	类型	模板	状态
1.		1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	
2.		2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	
3.		3	task7-aruba-device-access-enforcement-policy	TACACS	TACACS+ Enforcement	
4.		4	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	
5.		5	[Guest Operator Logins]	Application	Aruba Application Authentication	
6.		6	[Insight Operator Logins]	Application	Aruba Application Authentication	
7.		7	task1-test-service	RADIUS	RADIUS Enforcement (Generic)	
8.		8	task2-mac-service	RADIUS	忽略 MAC 认证	
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)	

显示最后项的前一-后一　　重新排序　复制　导出　删除

8.4 控制器配置

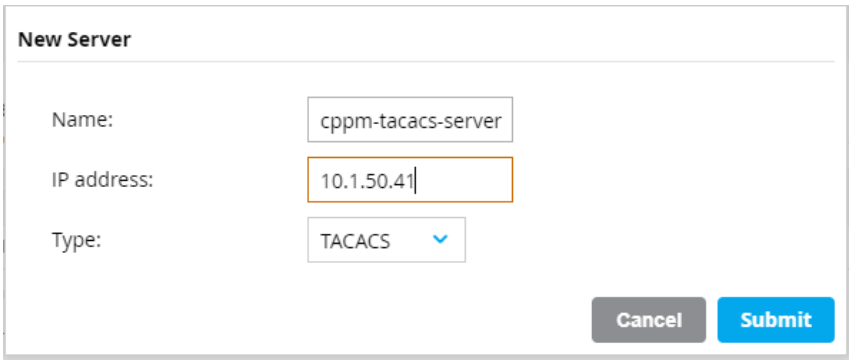
8.4.1 添加 TACACS 服务器和服务器组

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。



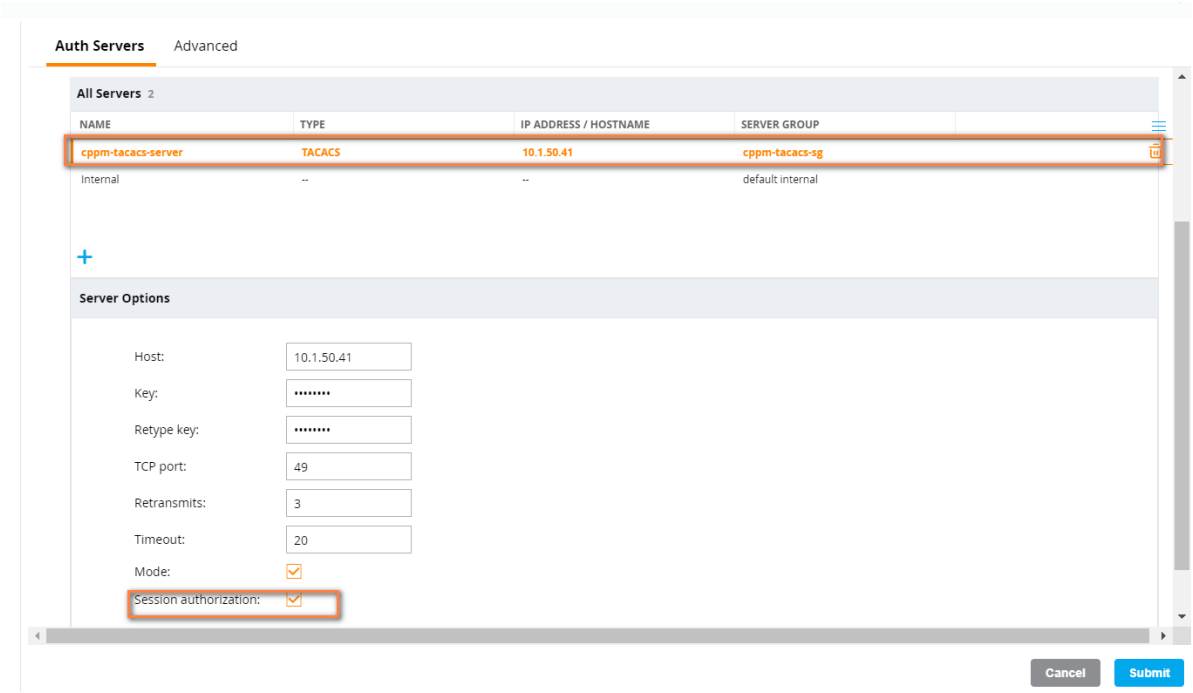
在 New Server 窗口中设置：

- ✓ 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

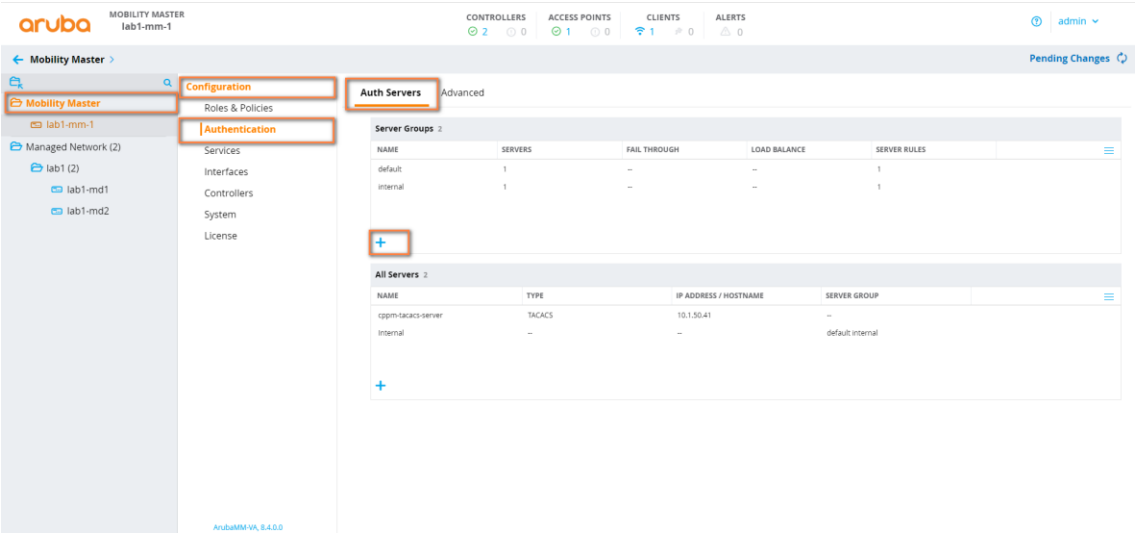


点击刚才创建好的auth server： cppm-tacacs-server，进入到认证服务器的编辑窗口，

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

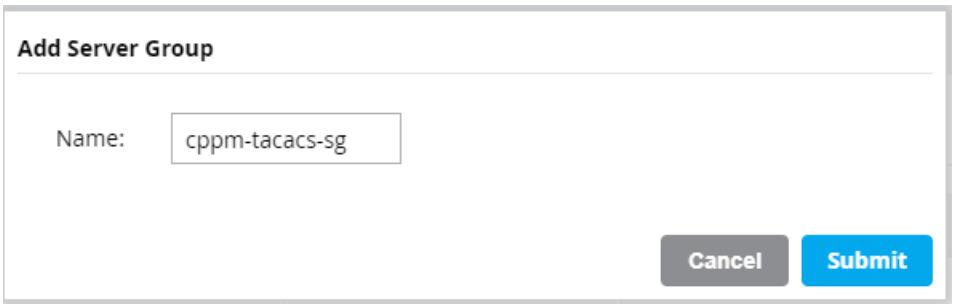


第2步：点击 Server Groups 下的“+”进入创建一个新的认证服务器组。

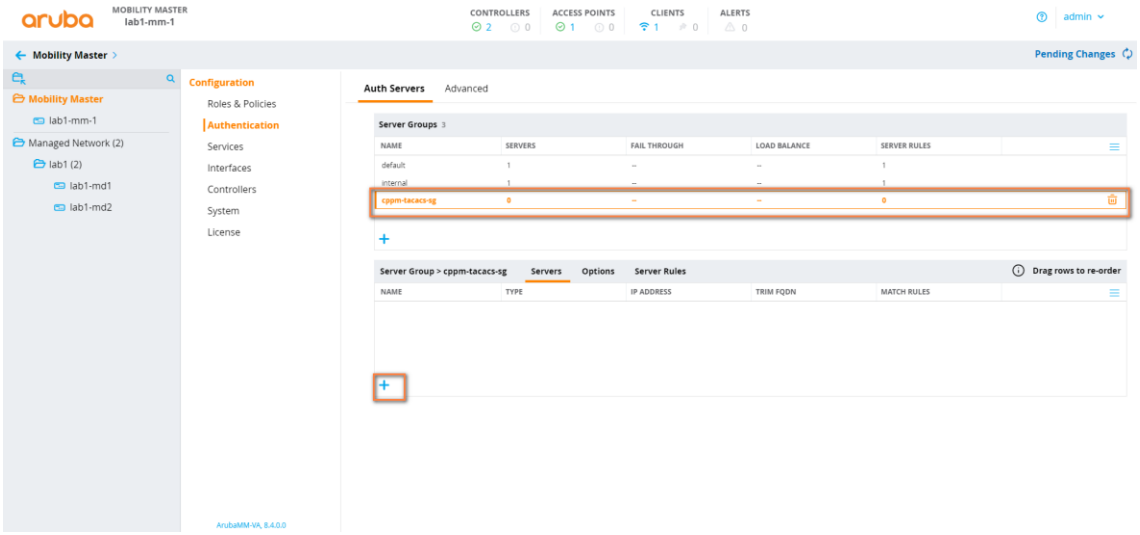


在 Add Server Group 窗口中设置：

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

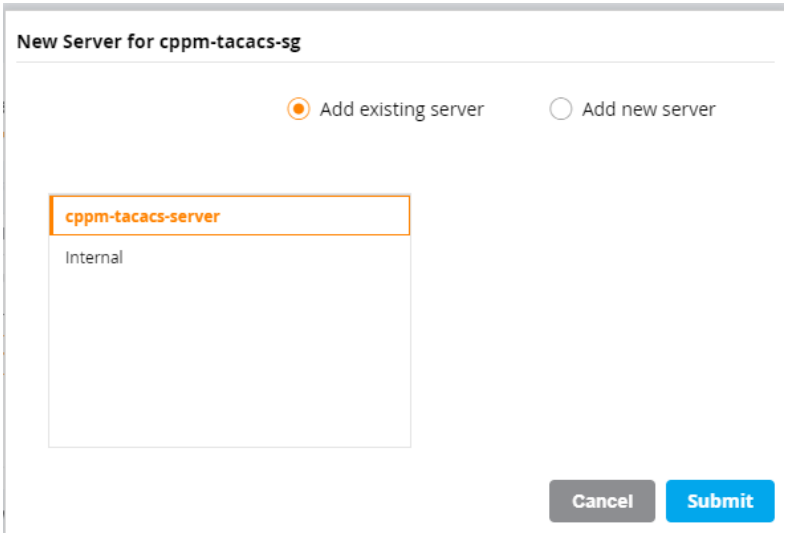


在 Server Groups 下点击 cppm-tacacs-sg, 在 Servers 选项卡窗口下半部分，出现 server group 的编辑界面。 点击下面的“+”进入到认证服务器组编辑窗口。



在认证服务器组的编辑窗口，选择添加已存在的认证服务器。

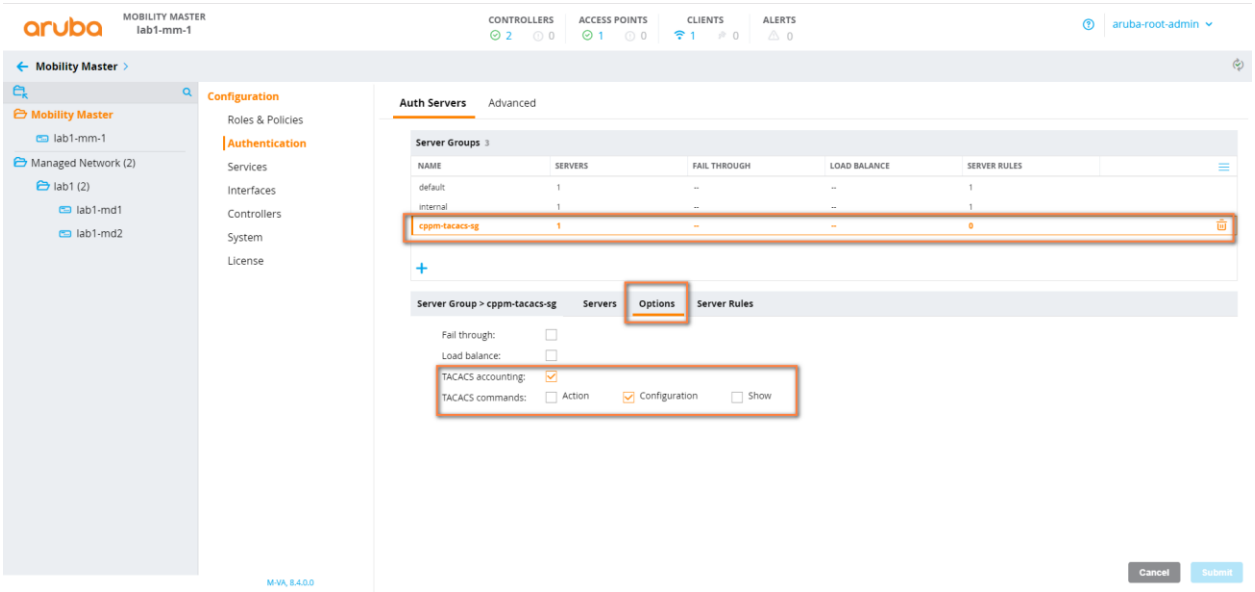
- Add existing server： cppm-tacacs-server
- Submit: 点击提交配置



在 Server Groups 下点击 cppm-tacacs-sg，继续在 Options 选项卡窗口下设置：

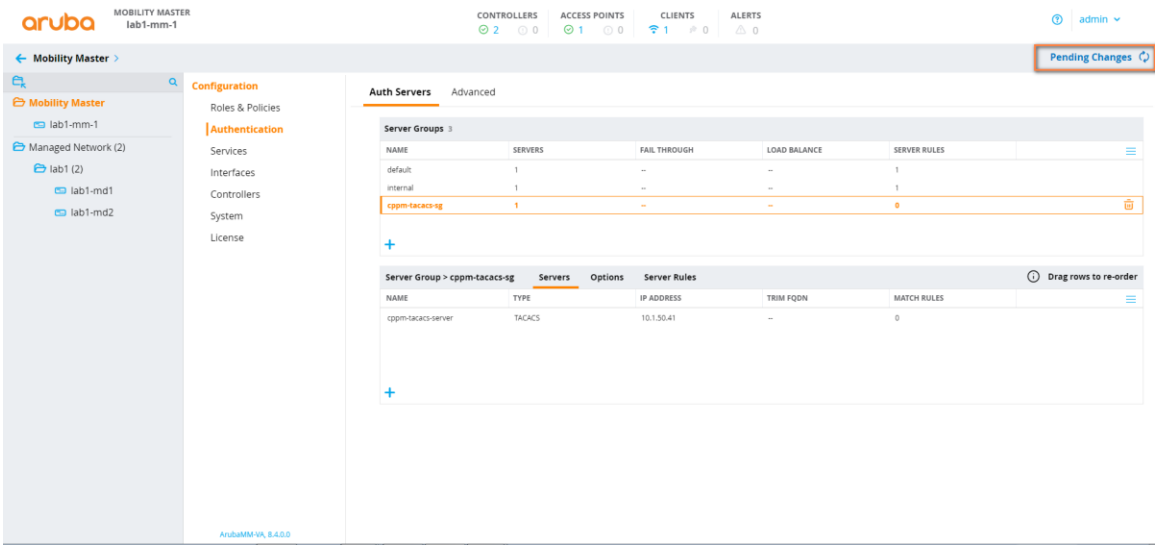
- 1、TACACS accounting： 勾选

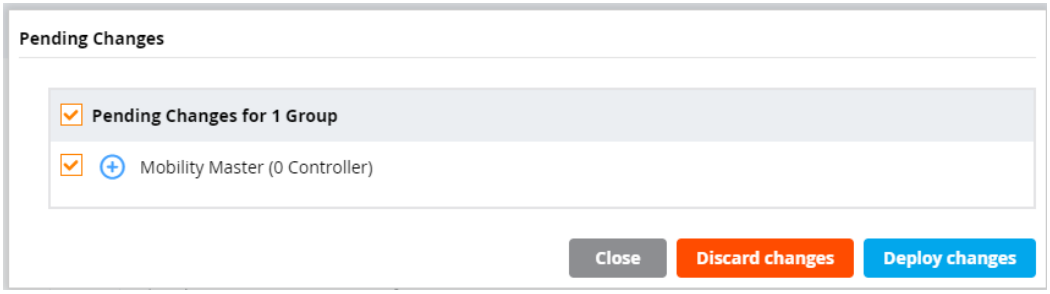
- 2、TACACS command： Configuration
- 3、Submit: 点击提交配置



第3步： 配置保存并同步给 md 设备

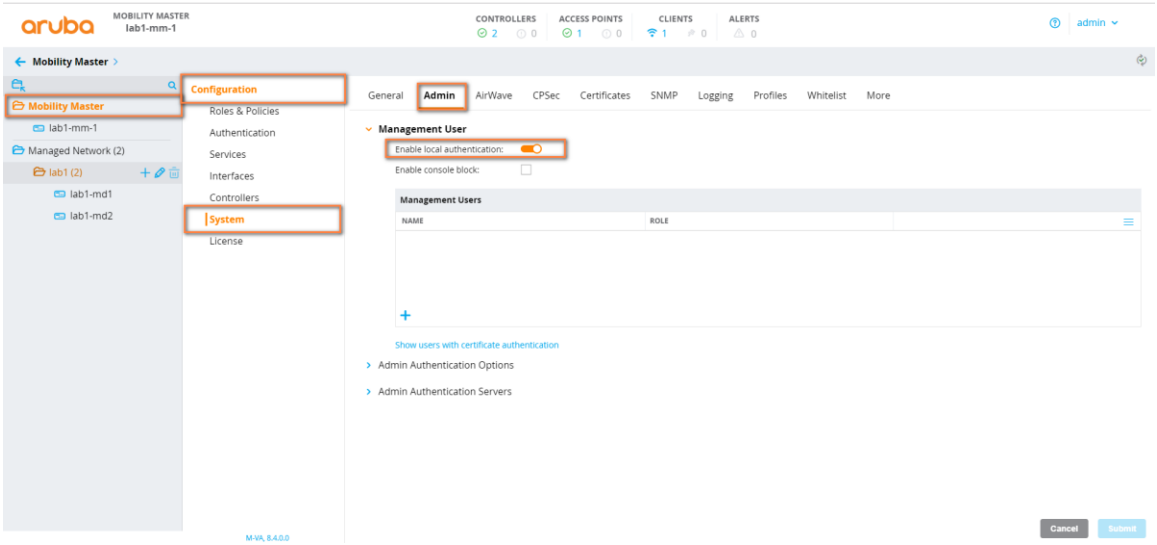
- 1、Pending Changes： 右上角点击该按钮
- 2、Deploy changes： 点击该按钮



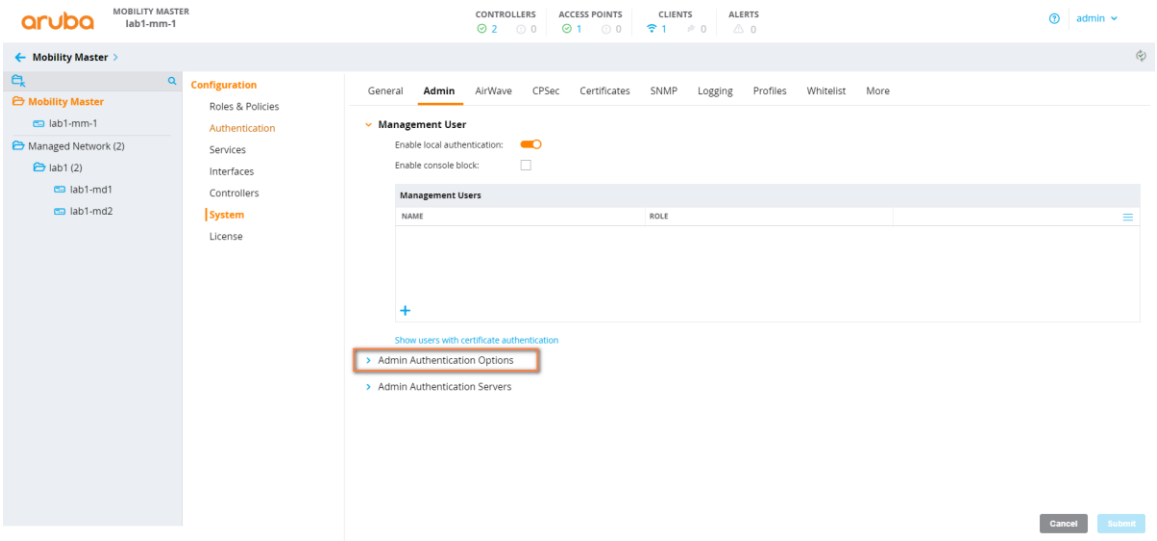


8.4.2 添加管理员的认证

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。

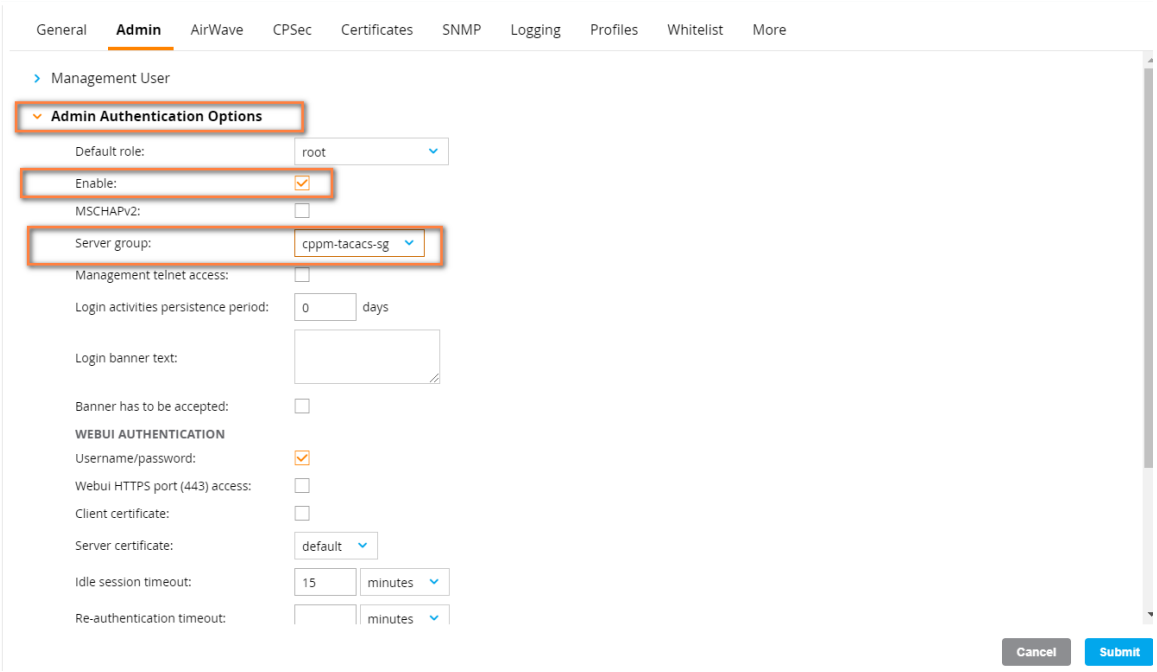


第2步：在该页面下，继续点击 Admin Authentication Option。



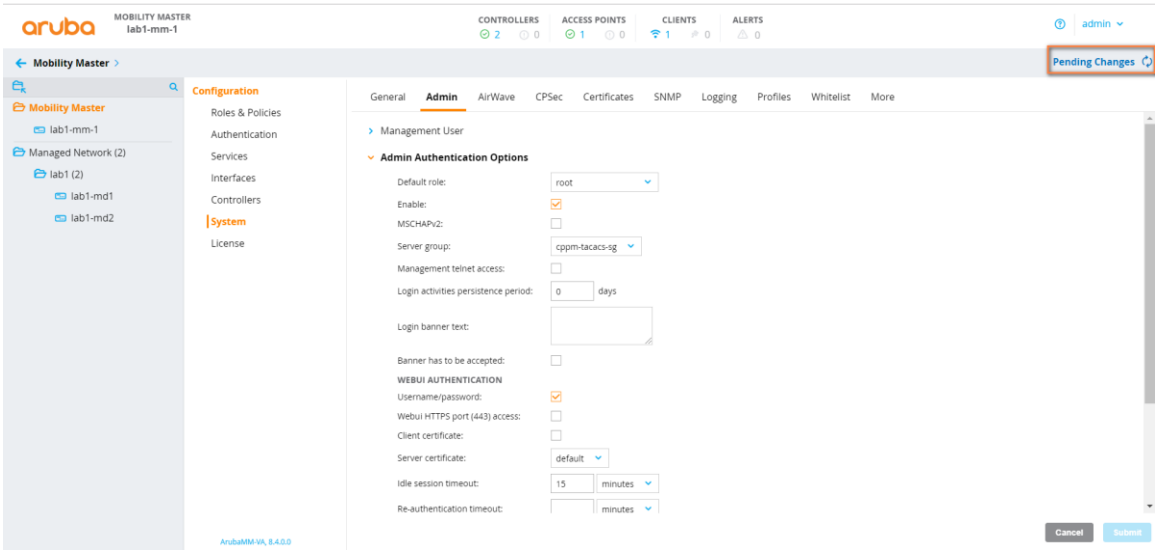
在 Admin Authentication Option 窗口下设置：。

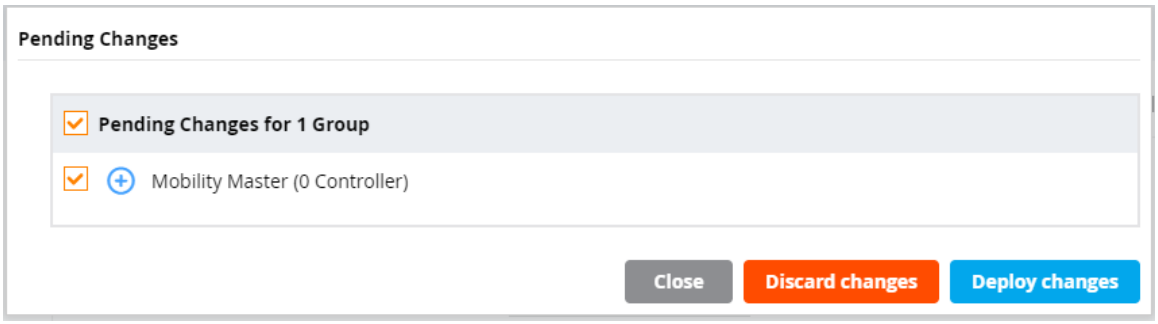
- ✓ 1、Enable：勾选 （必须勾选，这样控制器才会优先使用外置的认证服务器对管理员账号进行认证）
- ✓ 2、Server Group: 选择之前步骤中创建的cppm-tacacs-sg
- ✓ Submit: 点击提交配置



第3步:　配置保存并同步给 md 设备

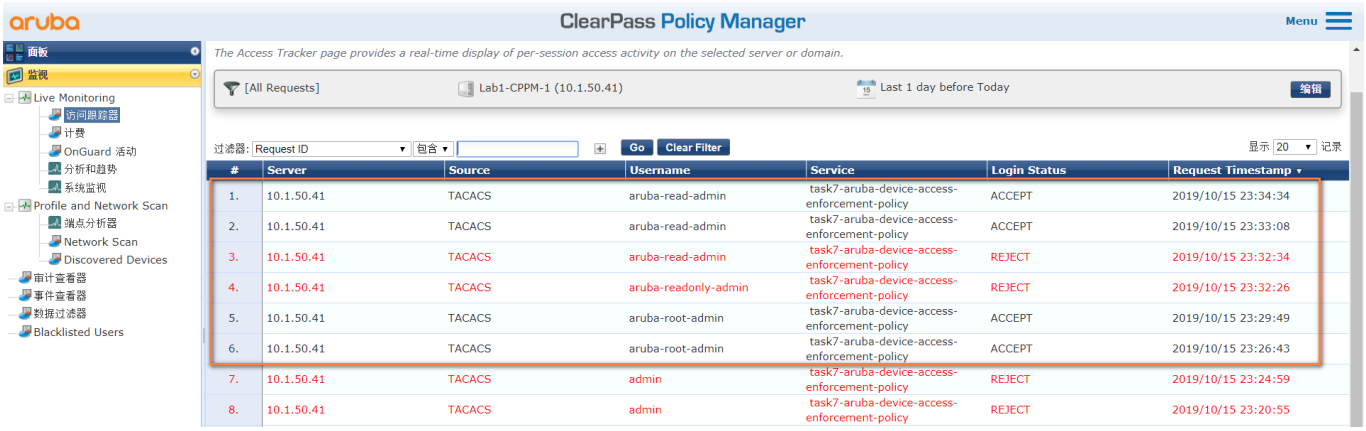
- Pending Changes：　右上角点击该按钮
- Deploy changes：　点击该按钮



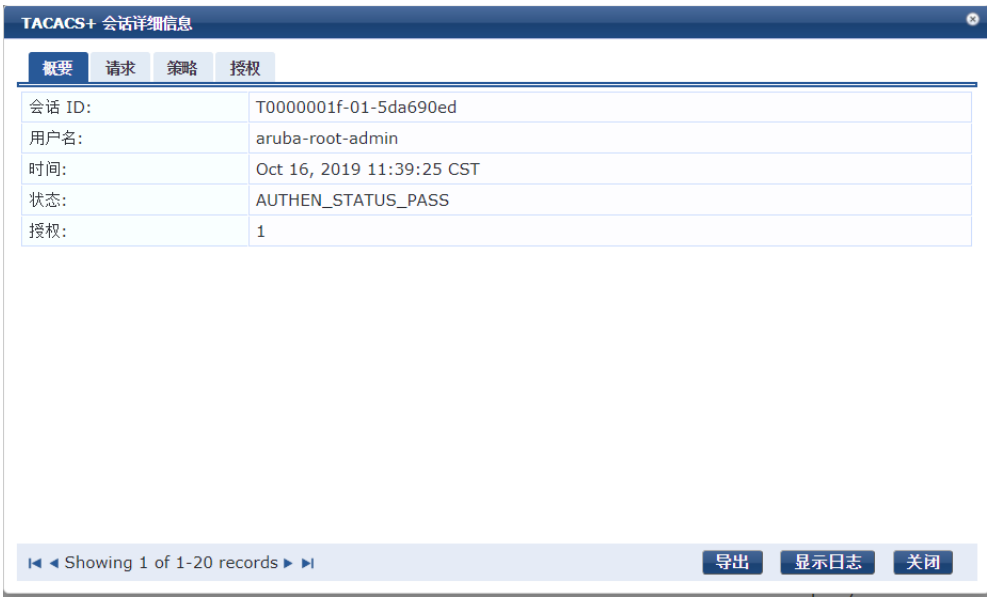


8.5 验证结果

8.5.1 CPPM 上查看认证记录

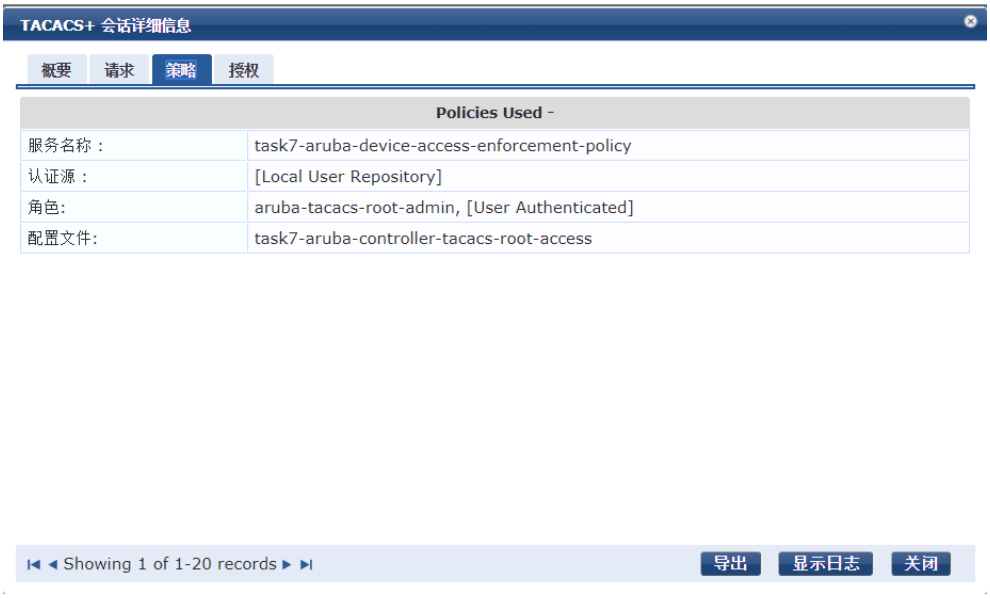


✓ 点击认证成功记录，在“概要“选项卡中观察，看看能看到哪些信息。

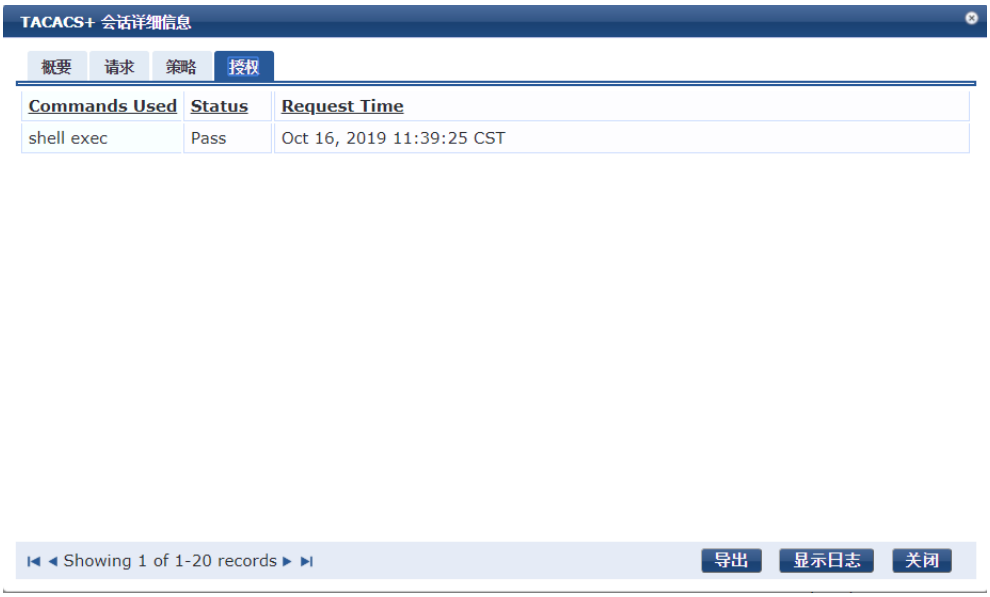


✓ 点击 “请求“选项卡中观察，看看能看到哪些信息。

✓ 点击 “策略“选项卡中观察，看看能看到哪些信息。

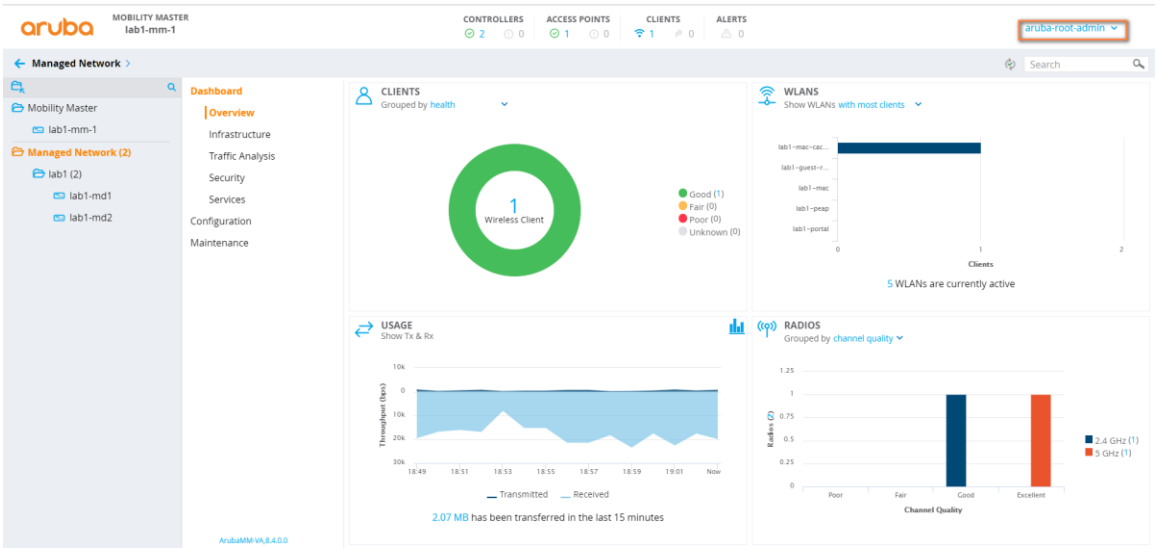


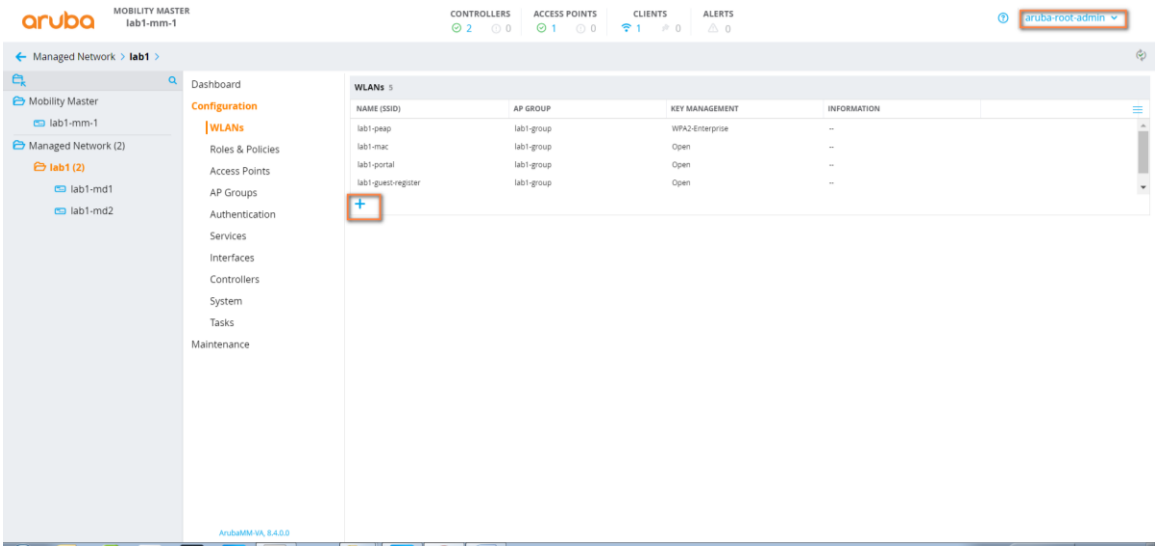
✓ 点击 “授权“选项卡中观察，看看能看到哪些信息。

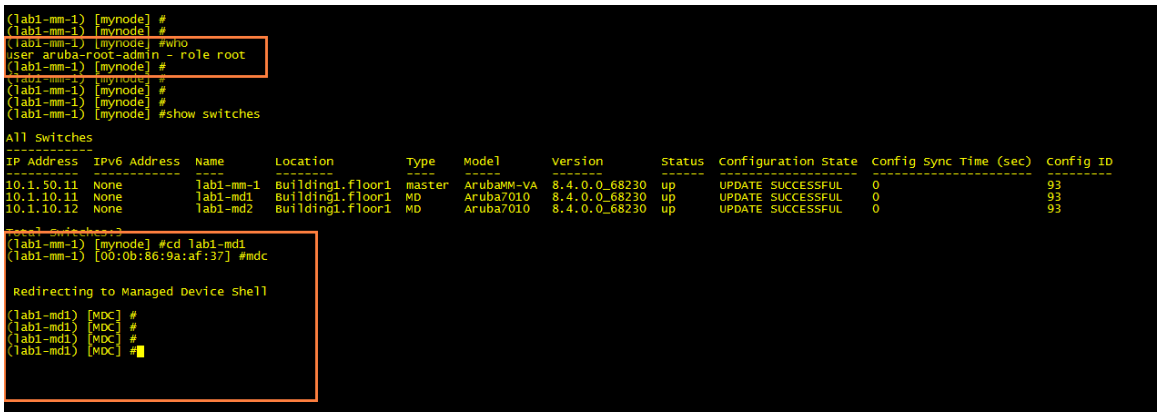


8.5.2 控制器上查看认证记录

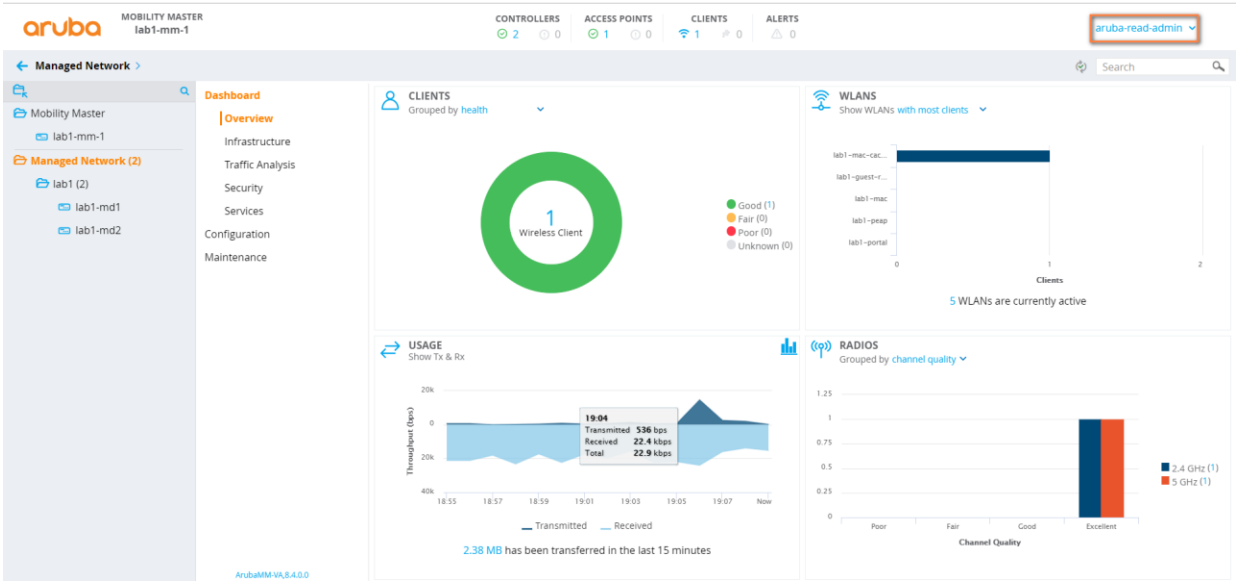
MM控制器可以使用ClearPass上的aruba-root-admin账号登录，而且aruba-root-admin账号可以对控制器进行配置更改和操作。

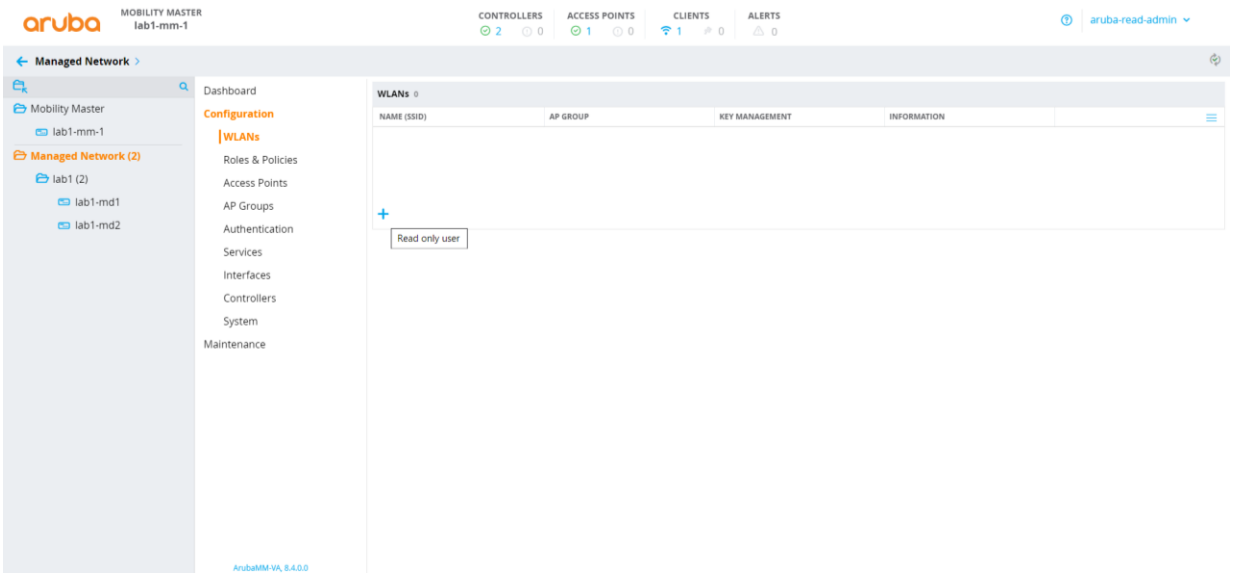






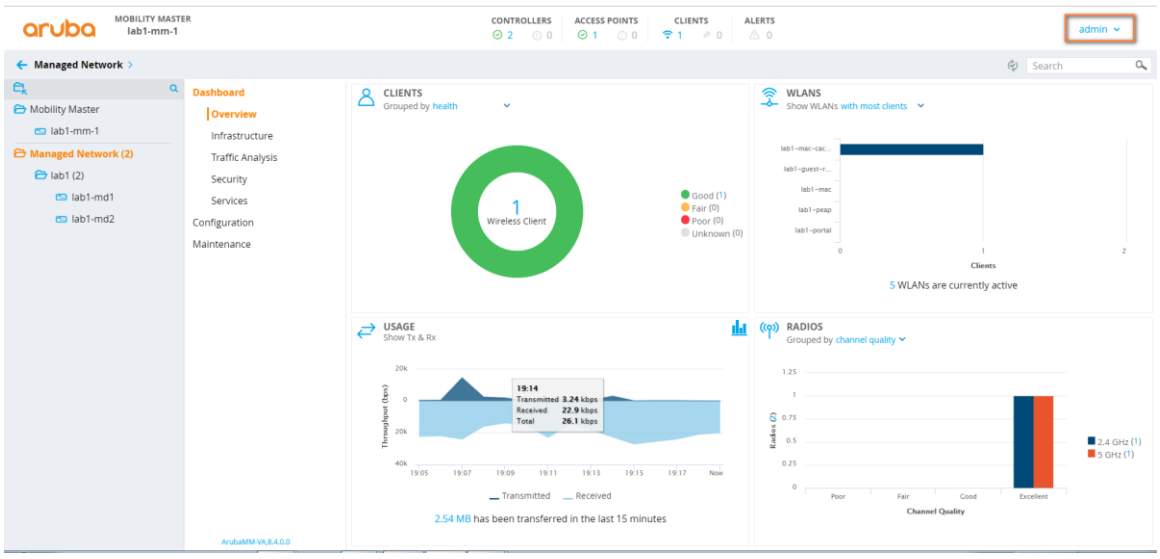
MM控制器可以使用ClearPass上的aruba-read-admin账号登录，而且aruba-read-admin账号不可以对控制器进行配置更改和操作。

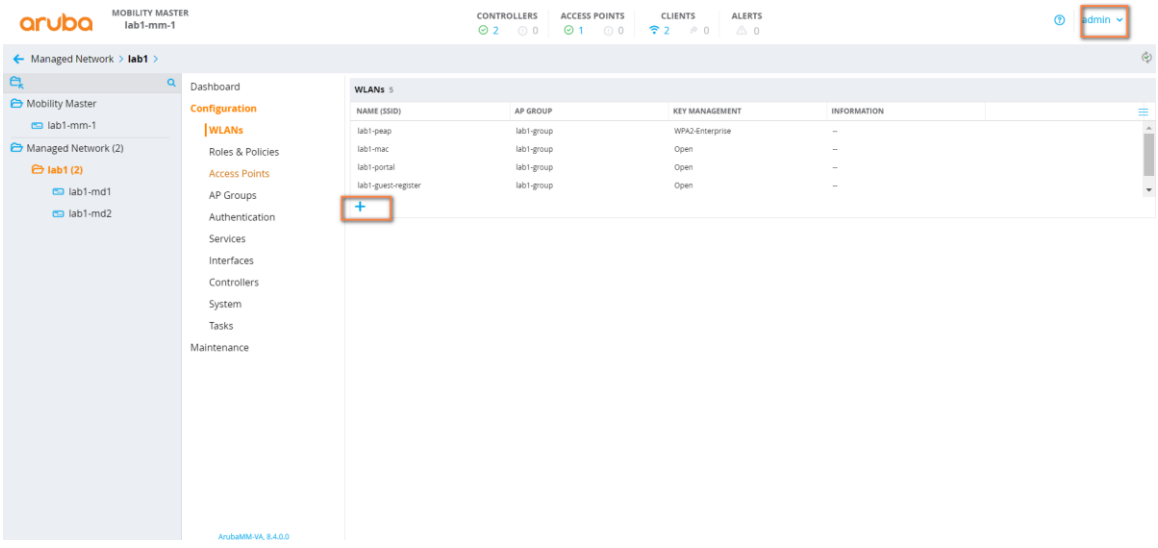





```
(lab1-mm-1) [mynode] #
(lab1-mm-1) [mynode] #who
User aruba-read-admin - role read-only
(lab1-mm-1) [mynode] #
(lab1-mm-1) [mynode] #
(lab1-mm-1) [mynode] #show switches

All Switches
------------
IP Address  IPv6 Address  Name       Location          Type    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
10.1.10.11  None          lab1-md1   Building1.floor1  MD      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    0                       93

Total Switches:3
(lab1-mm-1) [mynode] #cd lab1-md1
(lab1-mm-1) [00:0b:86:9a:af:37] #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(lab1-mm-1) [00:0b:86:9a:af:37] (config) #mdc
Error:You do not have permission to execute this command
(lab1-mm-1) [00:0b:86:9a:af:37] (config) #
(lab1-mm-1) [00:0b:86:9a: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。






```
(lab1-mm-1) [mynode] #
(lab1-mm-1) [mynode] #
(lab1-mm-1) [mynode] #
(lab1-mm-1) [mynode] #
(lab1-mm-1) [mynode] #who
user admin - role root
(lab1-mm-1) [mynode] #
(lab1-mm-1) [mynode] #
(lab1-mm-1) [mynode] #
(lab1-mm-1) [mynode] #show switches

All Switches
------------
IP Address  IPv6 Address  Name       Location          Type    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                       94
10.1.10.11  None          lab1-md1   Building1.floor1  MD      Aruba7010   8.4.0.0_68230  up      UPDATE SUCCESSFUL    0                       94
10.1.10.12  None          lab1-md2   Building1.floor1  MD      Aruba7010   8.4.0.0_68230  up      UPDATE SUCCESSFUL    0                       94

Total Switches:3
(lab1-mm-1) [mynode] #cd lab1-md1
(lab1-mm-1) [00:0b:86:9a:af:37] #mdc


 Redirecting to Managed Device 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

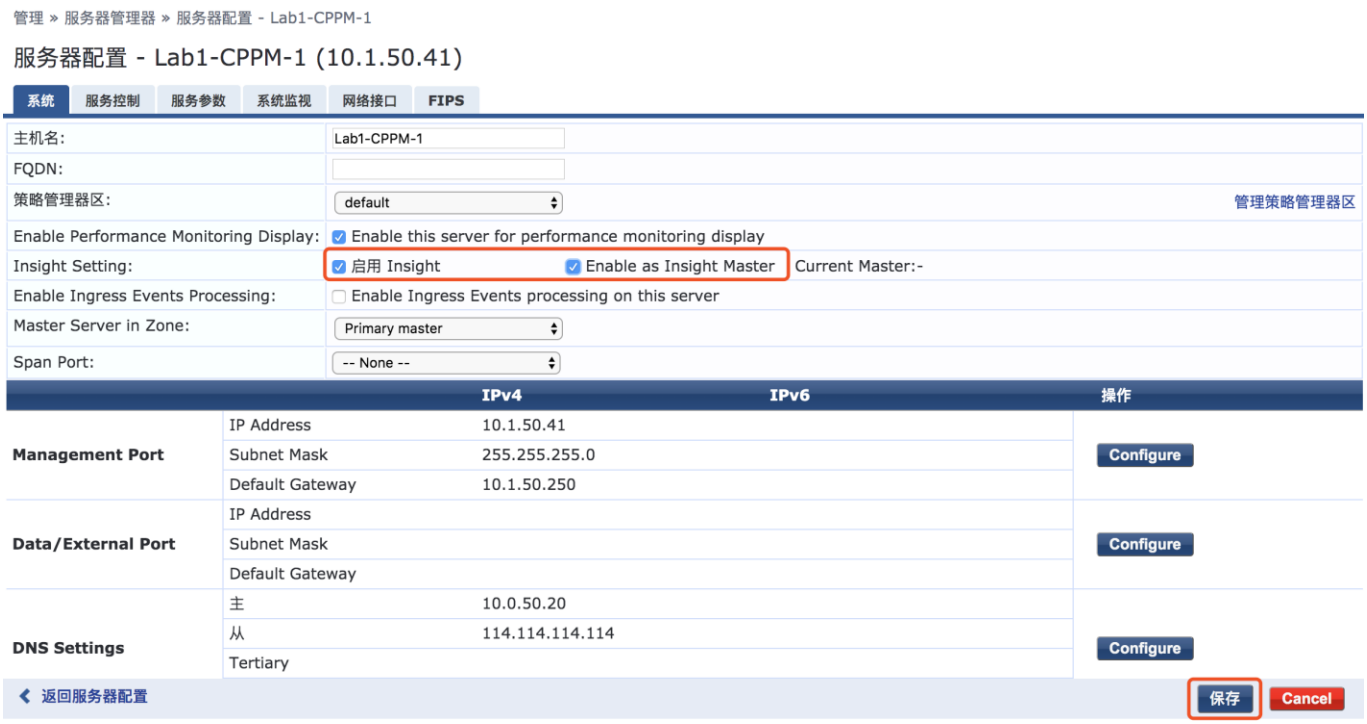
- ✓ ClearPass自带的Insight模块，可以实现自定义报表和自定义告警功能，可以每天、每周、每月自动生成报表，同时可以通过Email的方式自动向指定的管理员邮箱发送报表内容和告警信息
- ✓ 配置步骤如下：
  - 1、开启Insight功能；
  - 2、创建Insight Report，把当天LabX所有控制器发起的Radius认证记录生成报表；
  - 3、创建Insight Alert，当同一终端5分钟内认证失败次数超过3次时，产生告警。

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。

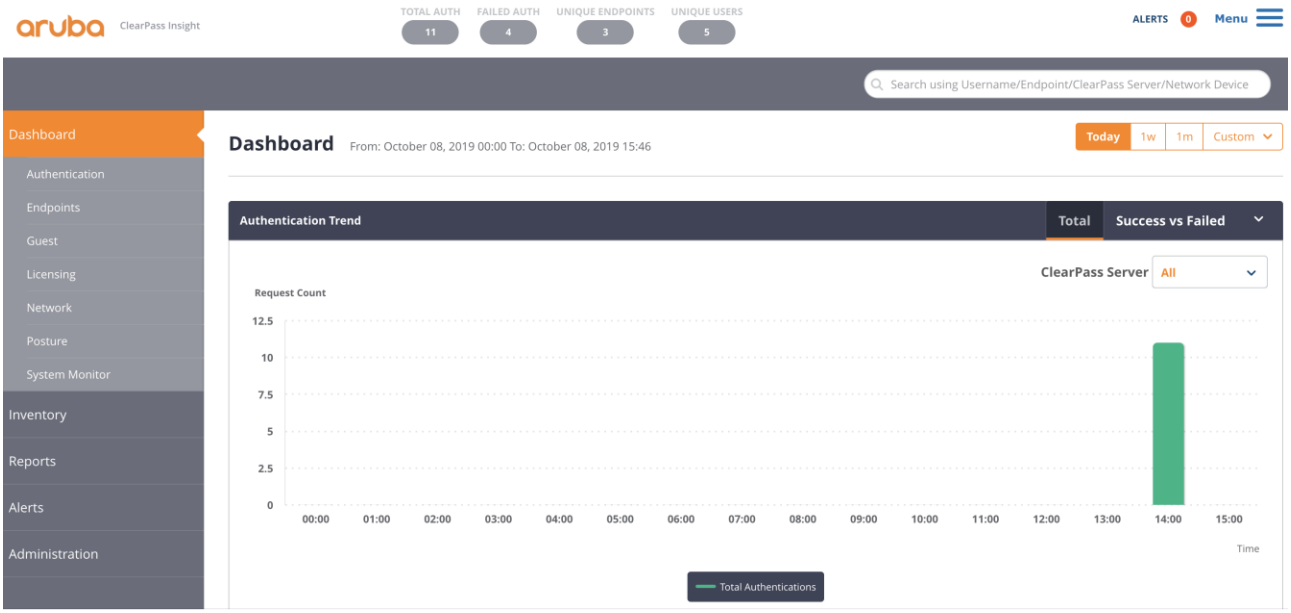
第2步：在 服务器配置 界面中，勾选 启用 Insight 和 Enable as Insight Master，点击 保存 。



9.3.2 进入 Insight 界面

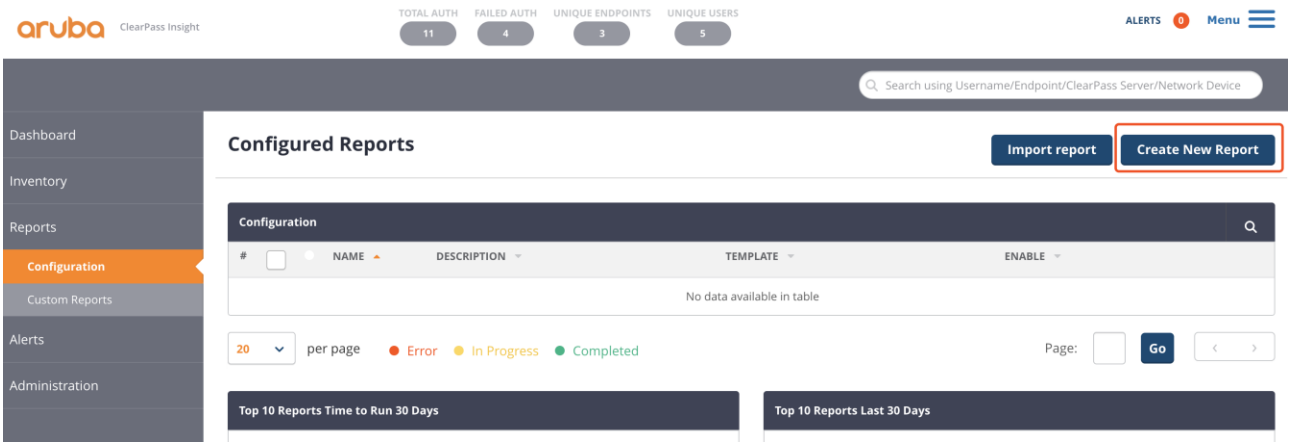
第1步：在ClearPass Policy Manager中，打开 面板 ，在右边 Quick Links 中点击 ClearPass Insight ，进入 ClearPass Insight 界面。

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。



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。

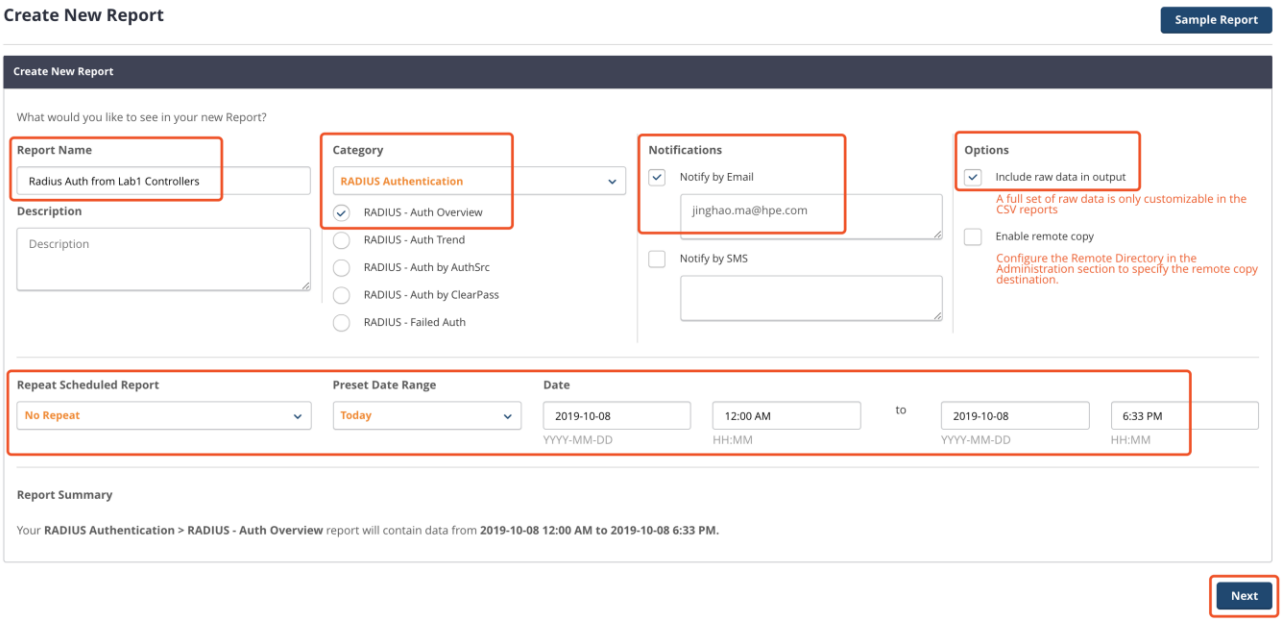


第2步：在 Create New Report 界面，设置以下内容：

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

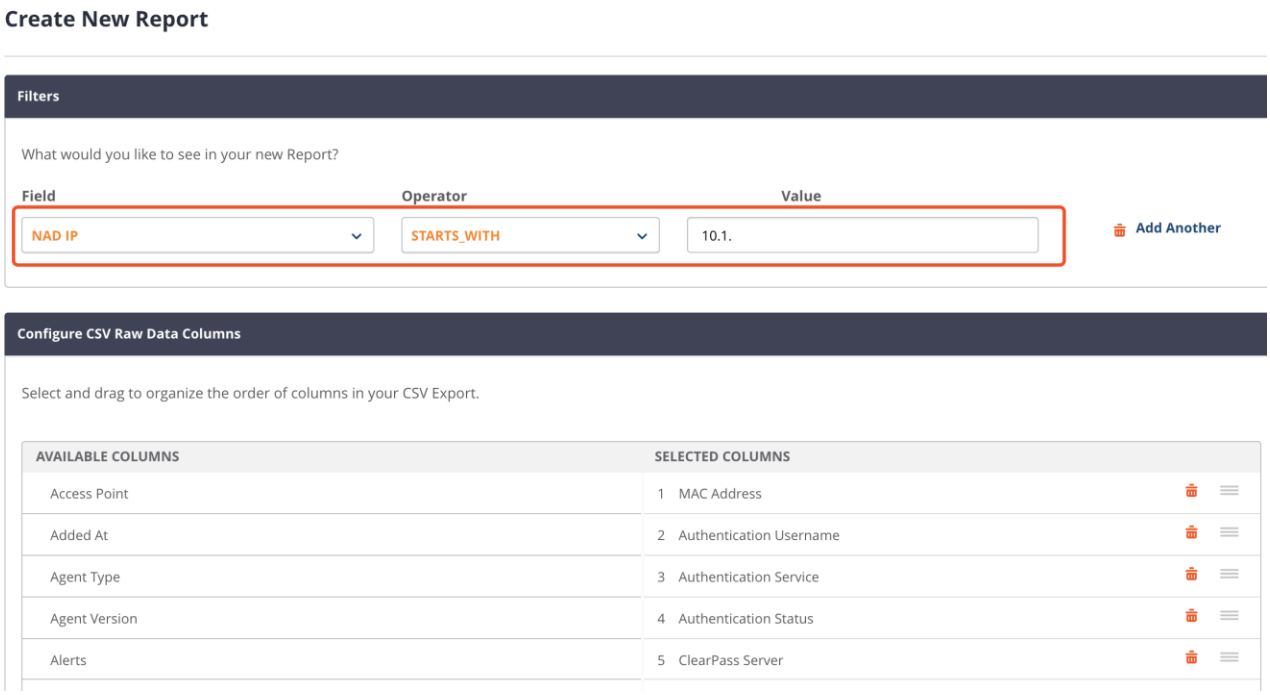
- ✓ **Notifications**：如需通过Email发送Report，需要勾选 Notify by Email 并在下方输入框中填写 收件人邮箱 。必须先在ClearPass Policy Manager中设置好SMTP，才可以勾选Notify by Email，否则无法勾选Notify by Email，设置SMTP方法请参考第7章 访客自注册中的SMTP设置内容
- ✓ **Options**：勾选 Include raw data in output ，勾选此项会同时生成CSV格式的详细report记录
- ✓ **Repeat Scheduled Report**：选择 No 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

点 Next 进入下一步

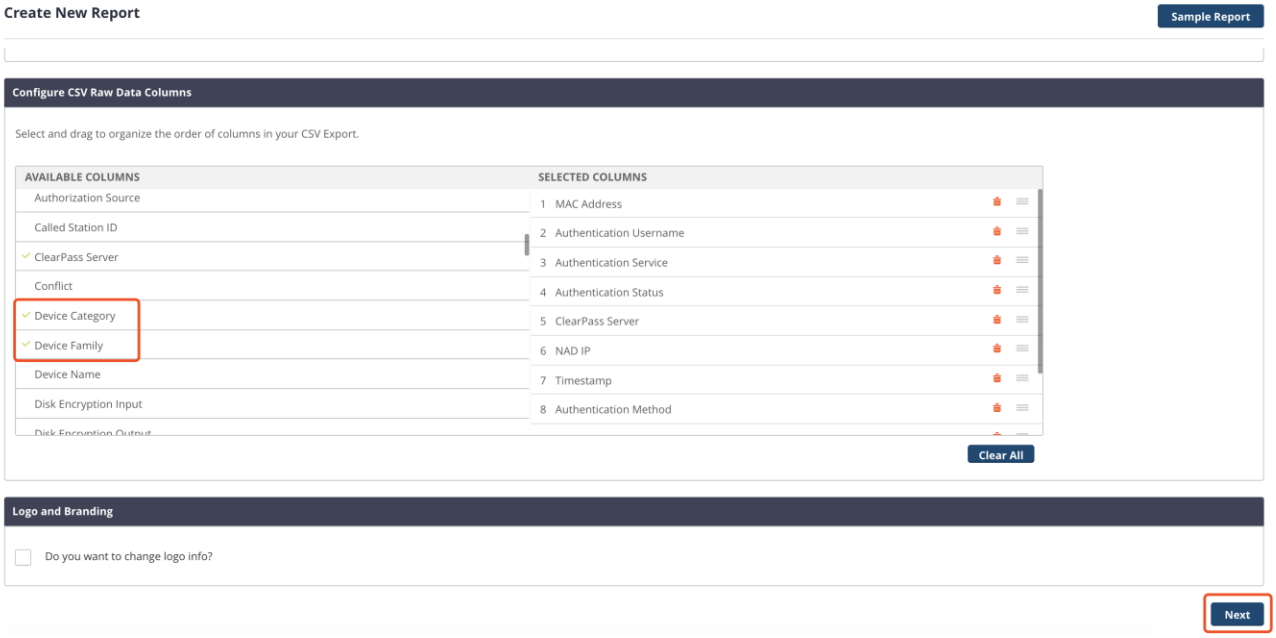


第3步：通过 Filters 设置过滤规则，设置内容如下：

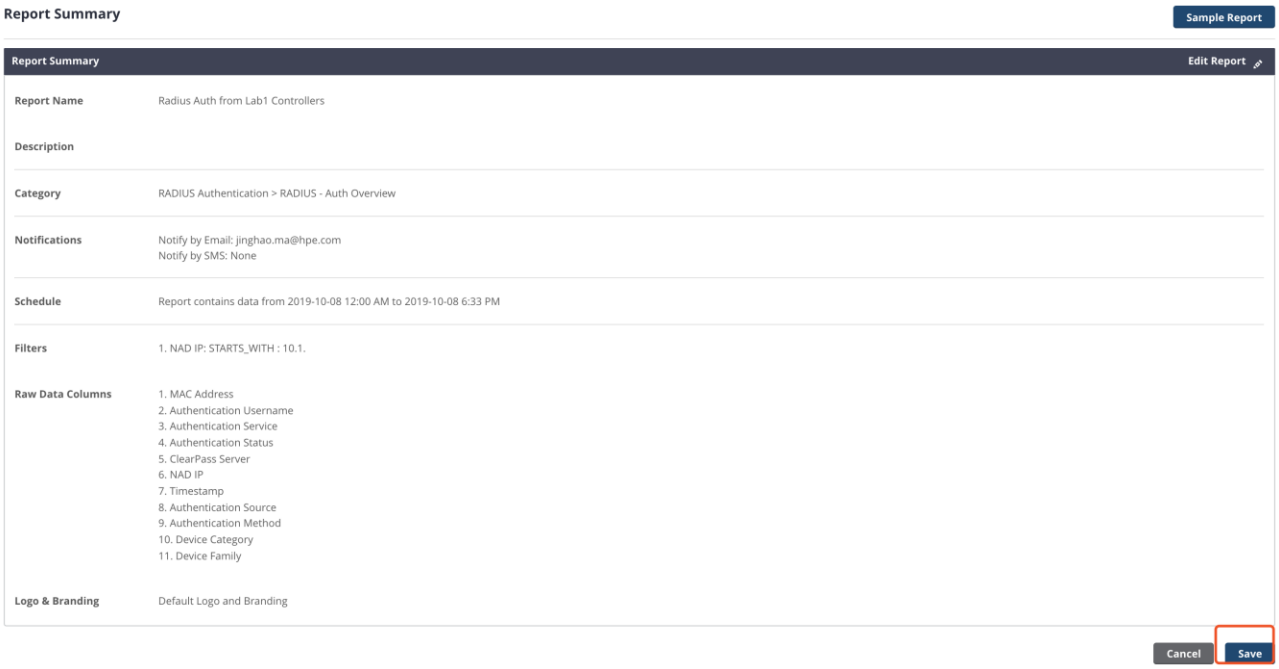
- ✓ NAD IP　STARTS_WITH　　10.X.



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

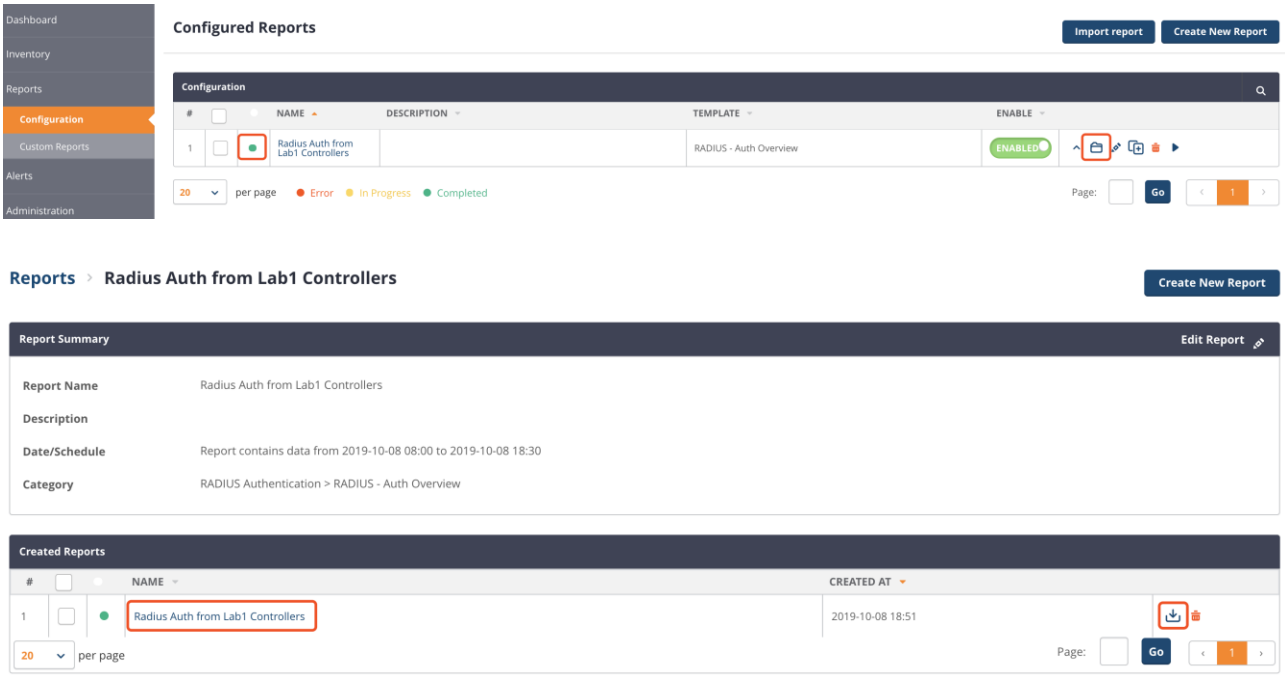


确认Report Summary内容无误后，点击 Save 保存



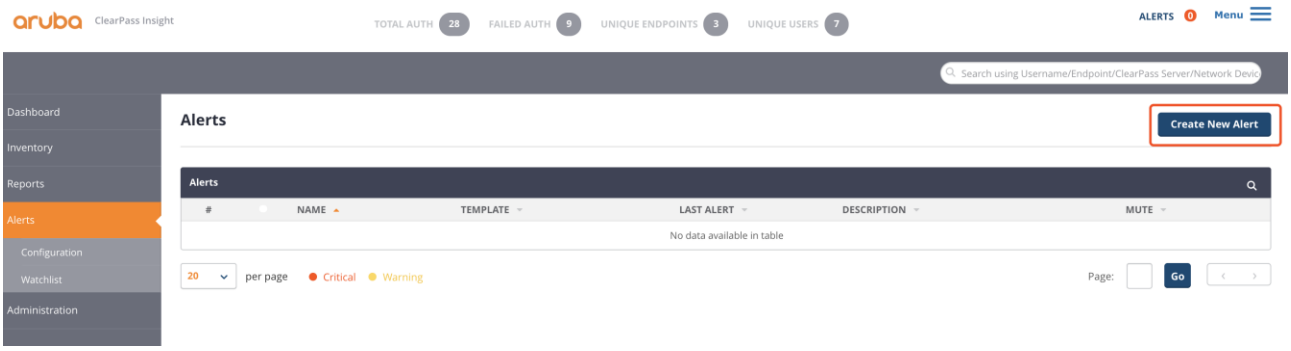
第4步：打开 Reports - > Configuration，查看刚才创建的Report状态，

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



9.3.4 添加 Insight Alert

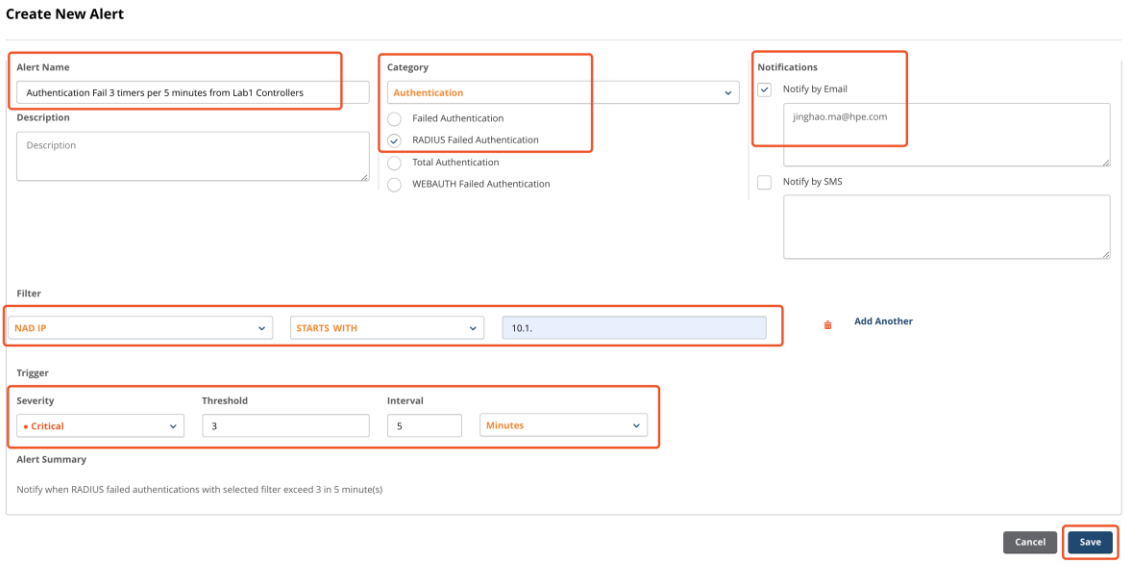
第1步：在ClearPass Insight中，打开 Alerts ，点击右边的 Create New Alert 按钮，进入 Create New Alert 界面。



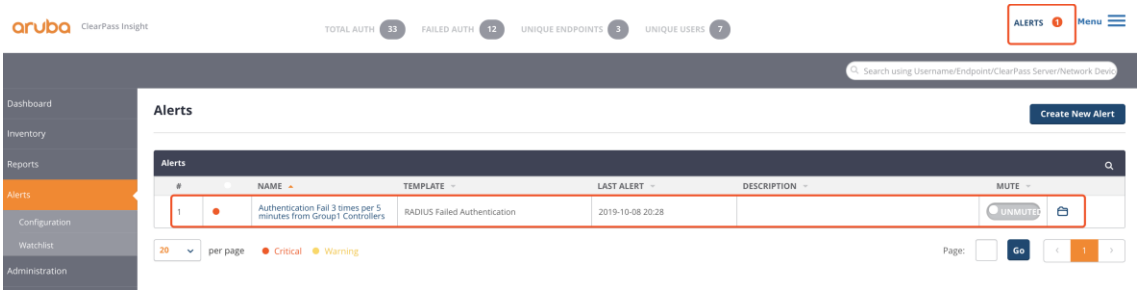
第2步：在 Create New Alert 界面，设置以下内容：

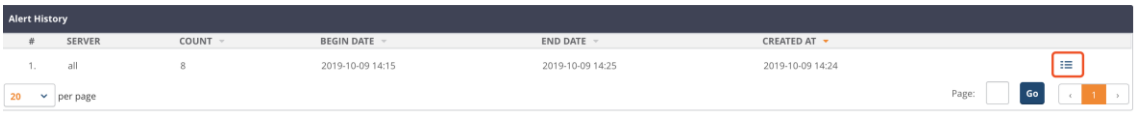
- ✓ **Alert Name：** Authentication Fail 3 timers per 5 minutes from LabX Controllers
- ✓ **Category：** Authentication ，勾选 RADIUS Failed Authentication
- ✓ **Notifications：**如需通过Email发送Report，需要勾选 Notify by Email 并在下方输入框中填写 收件人邮箱 。必须先在ClearPass Policy Manager中设置好SMTP，才可以勾选Notify by Email，否则无法勾选Notify 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

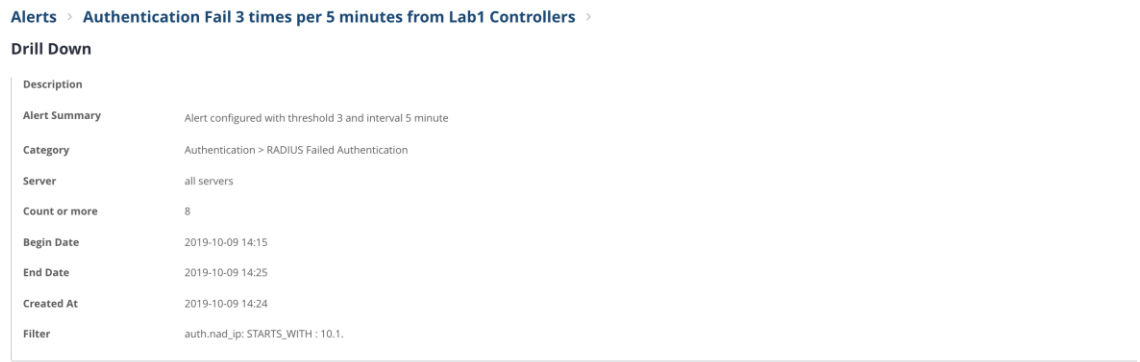
点 Save 保存

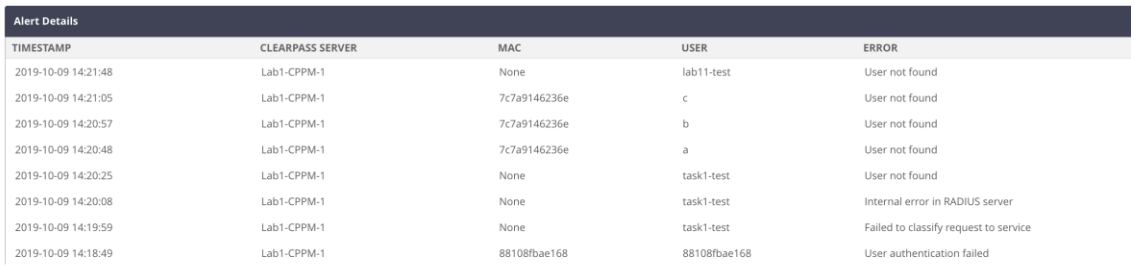


第3步：通过远程桌面登录相应 LabX 的 Wireless Client（10.X.50.102，用户名：lab，密码：Aruba123!），断开其无线网络连接，重新连接到前面章节创建的Portal认证无线网络 labX-portal ，在弹出的Portal页面输入错误的账号密码，5分钟内连续输入超过3次错误账号密码，等待大概5分钟后，观察Insight右上角的 ALERTS 计数，如下图显示 ①，点击后显示Alerts记录，在Alert Name上点击进入，查看 Alert History 记录，点右边的 浏览 按钮显示 Alert Details ，可查看具体的认证终端Mac和用户名。









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。

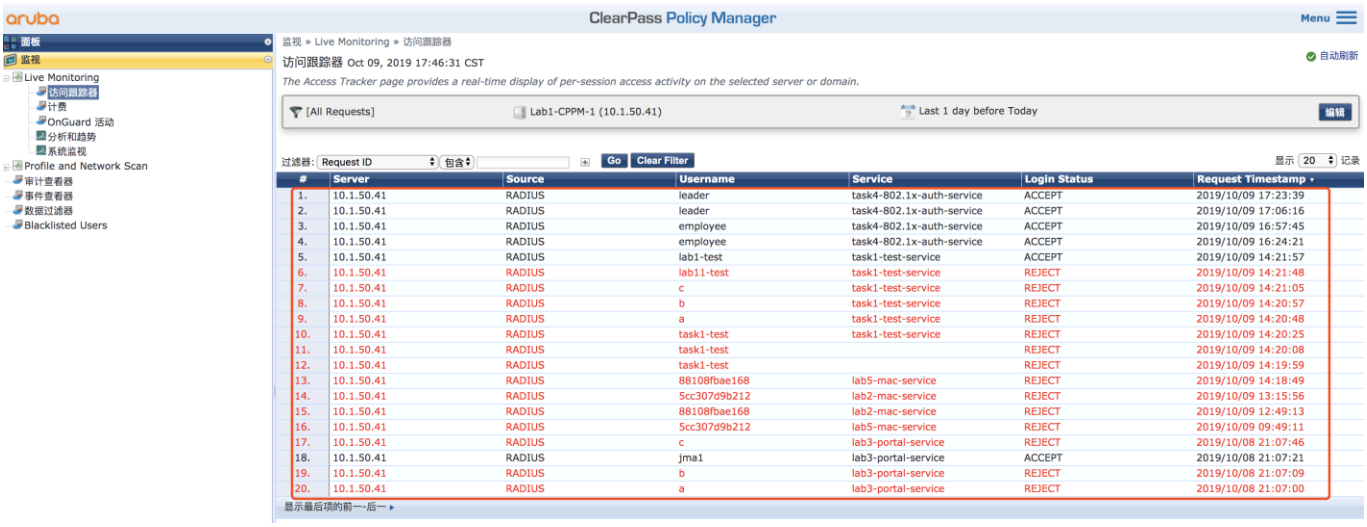
10.2 实现思路

- ✓ 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

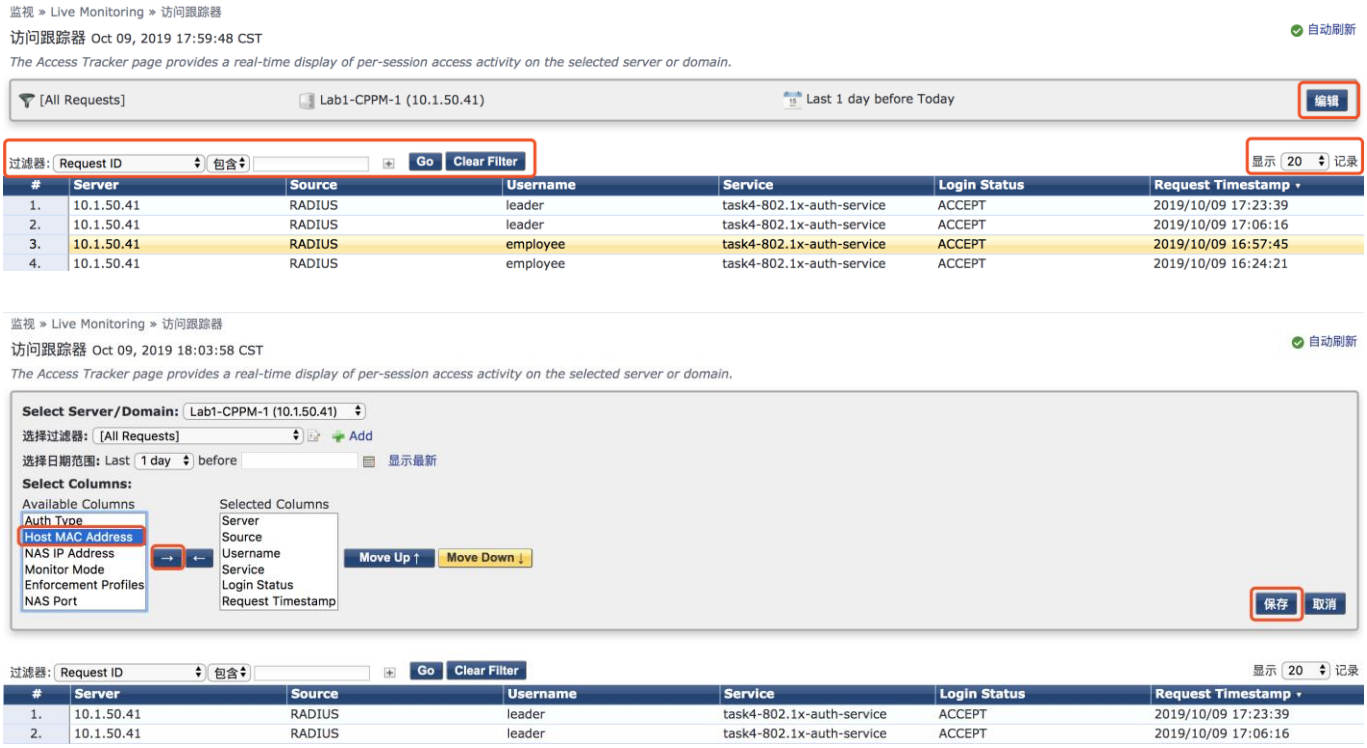
10.3.1 访问跟踪器过滤和查看认证记录

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。



#	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
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	a	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

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。



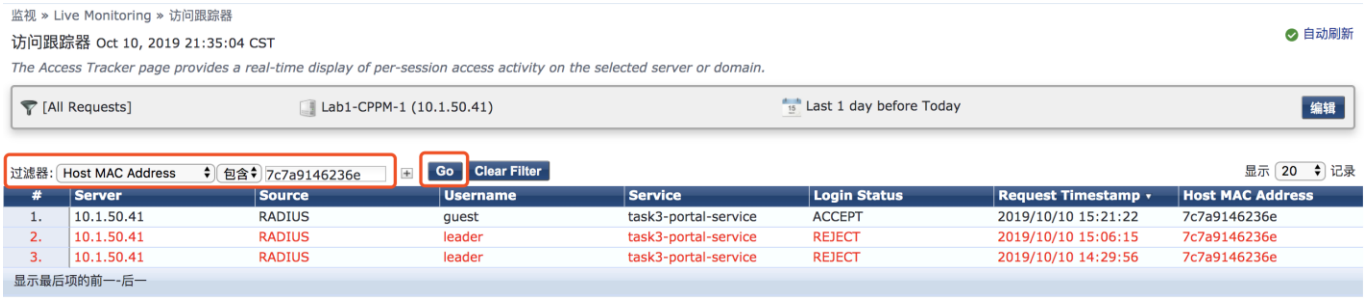
第3步：通过远程桌面登录相应 LabX 的 Wireless Client（10.X.50.102，用户名：lab，密码：Aruba123!），将无线网络连接到 labX-mac 后，重新连接到Portal认证无线网络 labX-portal，在弹出的Portal页面输入 账号：leader，密码：aruba 进行认证，提示认证失败，再输入 账号：leader，密码：

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：

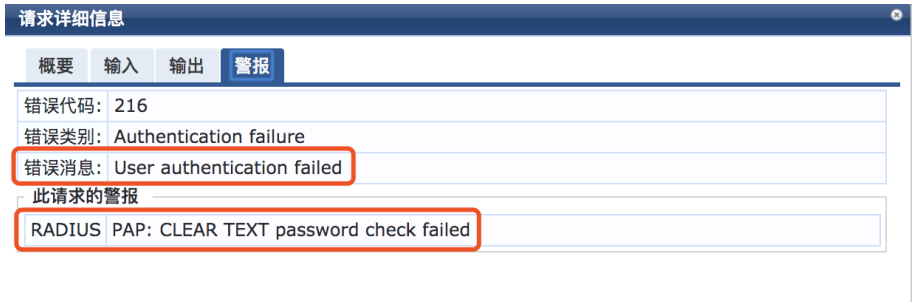
- ✓ Host MAC Address 包含 <终端的MAC>

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。

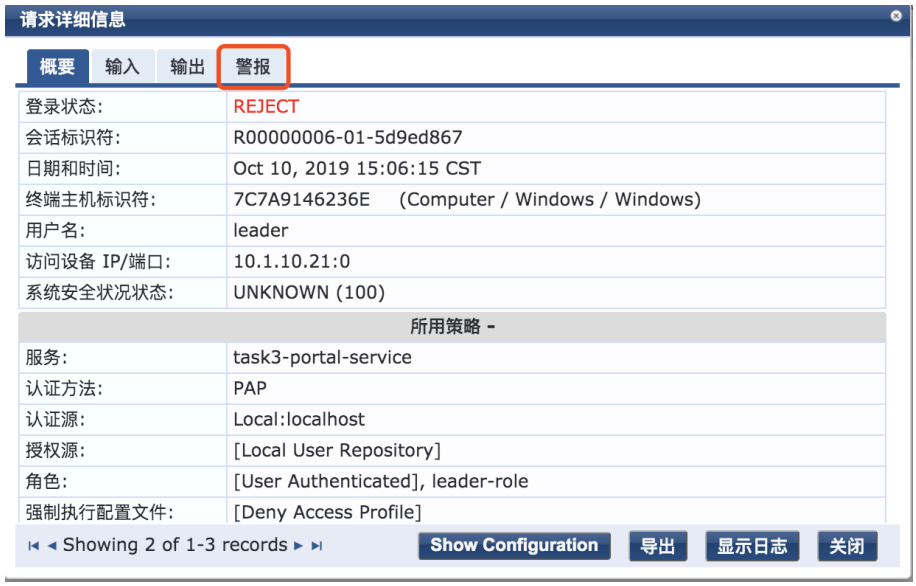


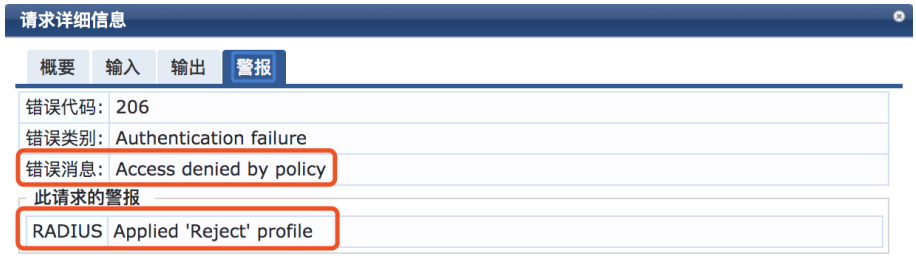
10.3.2 通过访问跟踪器分析认证失败原因

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。

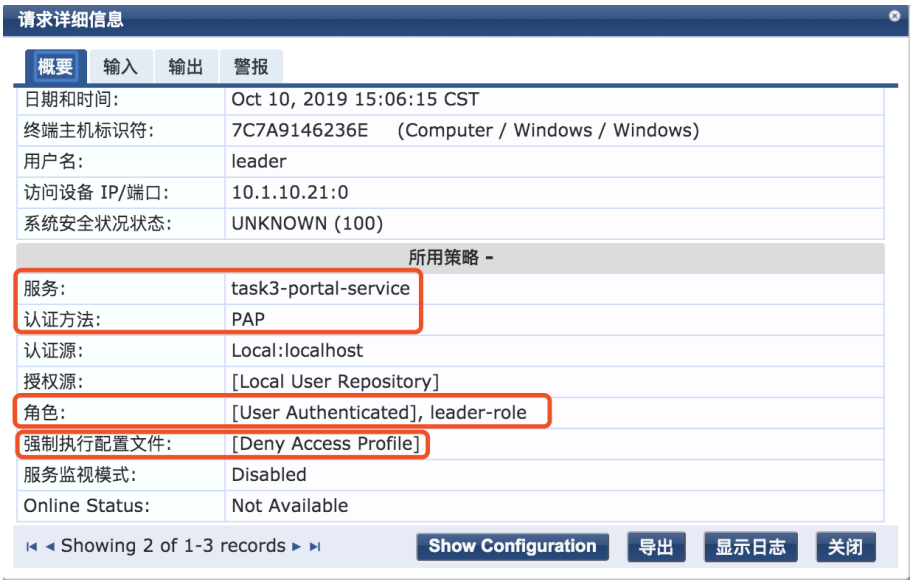


第2步：在9.3.1章节中过滤的认证记录中，点击第二条通过用户名leader认证失败的记录（即编号为2的认证记录），进入 请求详细信息 显示框，点击上方的 警报 按钮，显示 错误消息：Access denied by policy，此请求的警报 RADIUS Applied 'Reject' profile，提示应用了Reject的Profile，被策略拒绝。





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。



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guest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：_____。

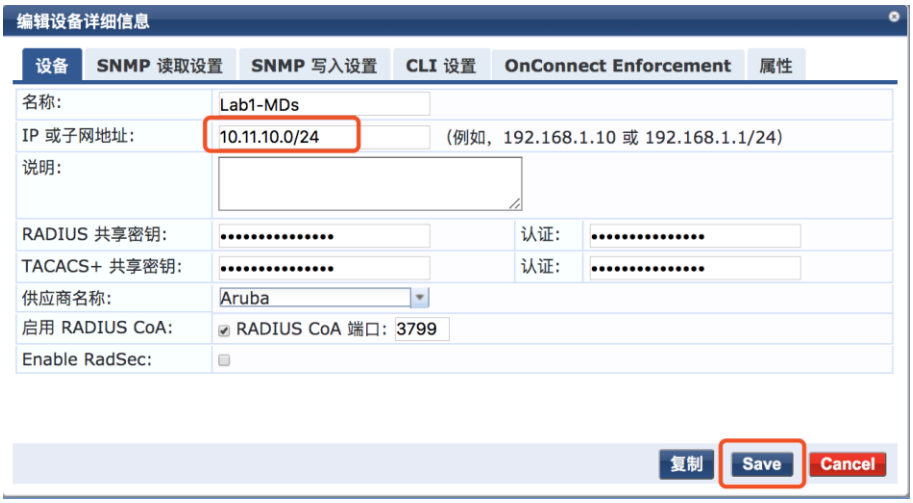
更复杂的认证失败原因需要结合 请求详细信息 中的 输入 中的 RADIUS请求、计算属性、授权属性 ，以及 服务 中的 授权、角色、强制执行 等配置来综合分析。

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。

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。

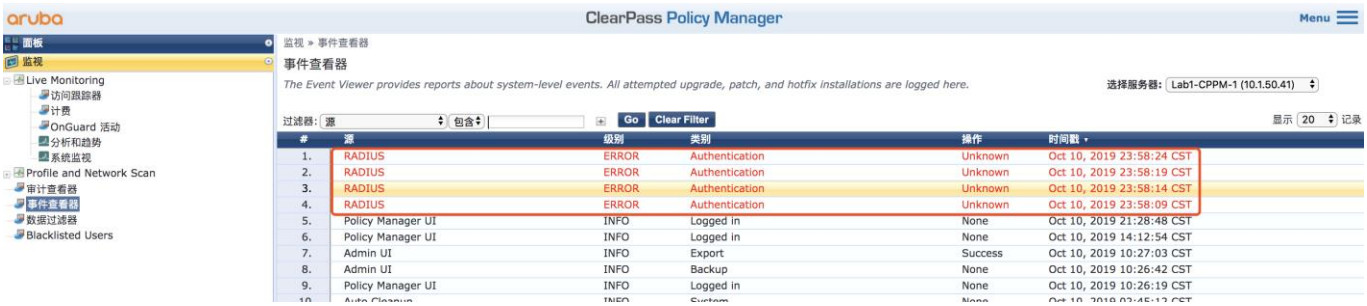


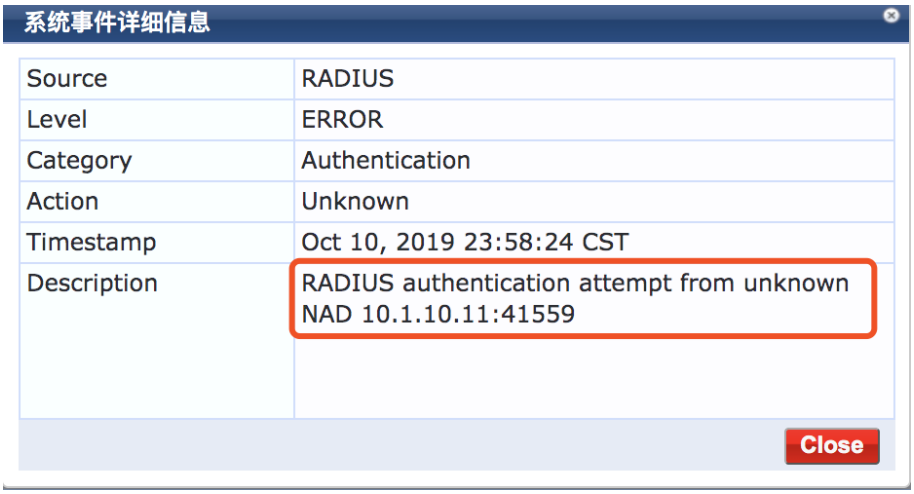
第3步：在第1步中弹出的Portal认证页面中输入 账号：guest-test，密码：aruba123 进行认证，认证失败，提示 Auth server timeout ，在ClearPass访问跟踪器中过滤 Username 包含 guest-test 的认证记录，提示 没有与指定过滤标准匹配的结果 ，说明访问跟踪器没有该认证记录，原因可能有两种：

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。

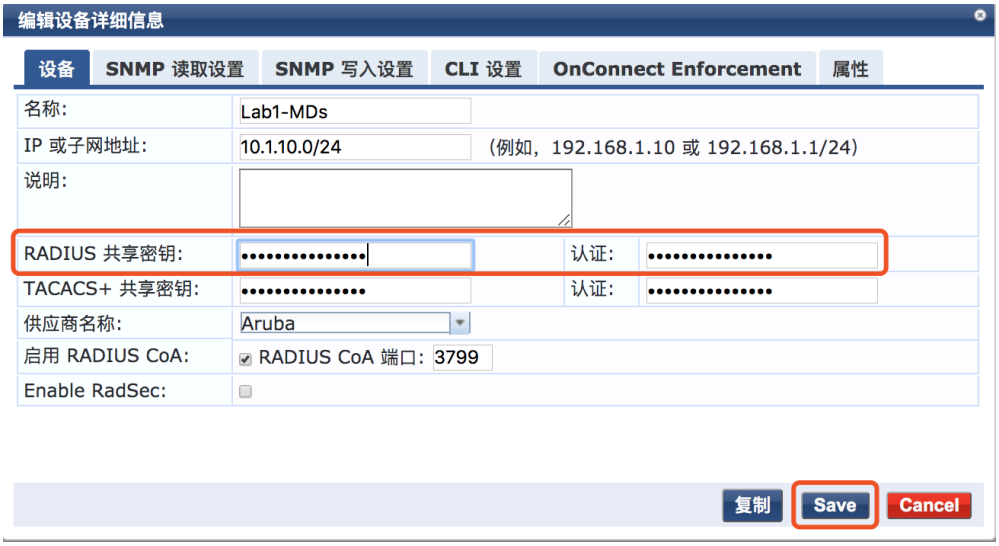
第4步：在ClearPass Policy Manager中，打开 监视 - > 事件查看器 ，在右边可以看到4条 RADIUS ERROR 事件，时间与通过guest-test账号认证的时间一致，点开一条查看 系统事件详细信息 ，查看 Description RADIUS authentication attempt from unknown NAD 10.X.10.11:41559 ，提示收到未知NAD 10.X.10.11的RADIUS认证请求，于是定位到问题是该NAD未添加到网络设备列表，前往网络设备中将IP或子网地址还原。

✓ 请大家讨论事件查看器中为什么是4条RADIUS ERROR记录?



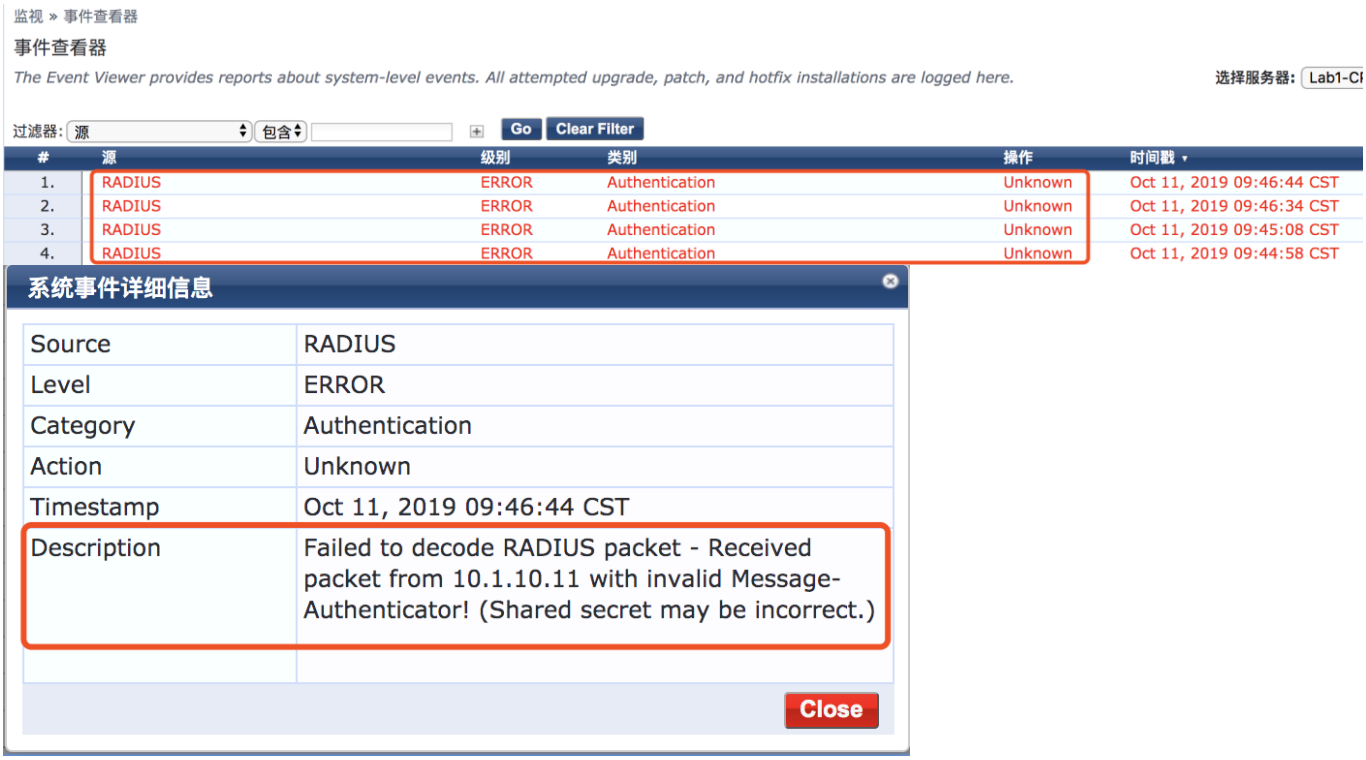


第5步：在ClearPass Policy Manager中，打开 配置 - > 网络 - > 设备，在右边点击网络设备名称 LabX-MDs，在弹出的 编辑设备详细信息 显示框中将 RADIUS共享密钥 修改为：test123 ，点 Save 按钮保存。



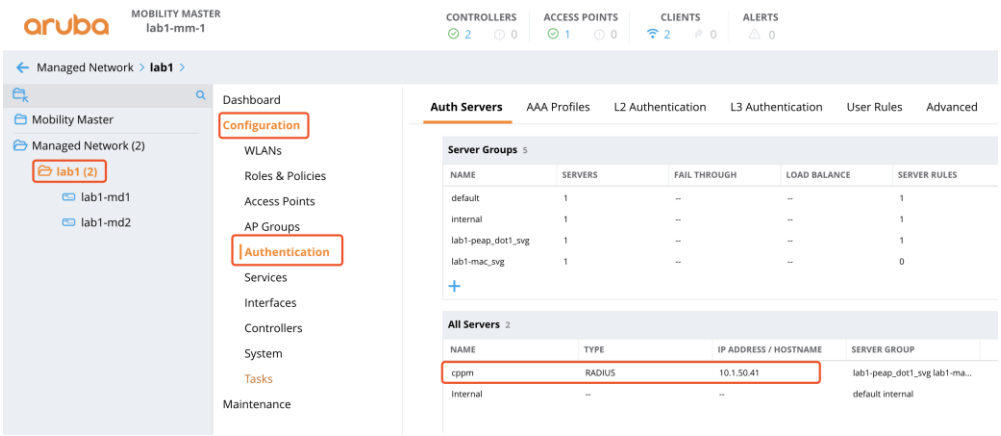
第6步：在 Wireless Client 的Portal认证页面中输入 账号：guest-test，密码：aruba123 进行认证，认证失败，提示 Auth server timeout ，在ClearPass访问跟踪器中过滤 Username 包含 guest-test 的认证记录，提示 没有与指定过滤标准匹配的结果 ，说明访问跟踪器没有该认证记录。

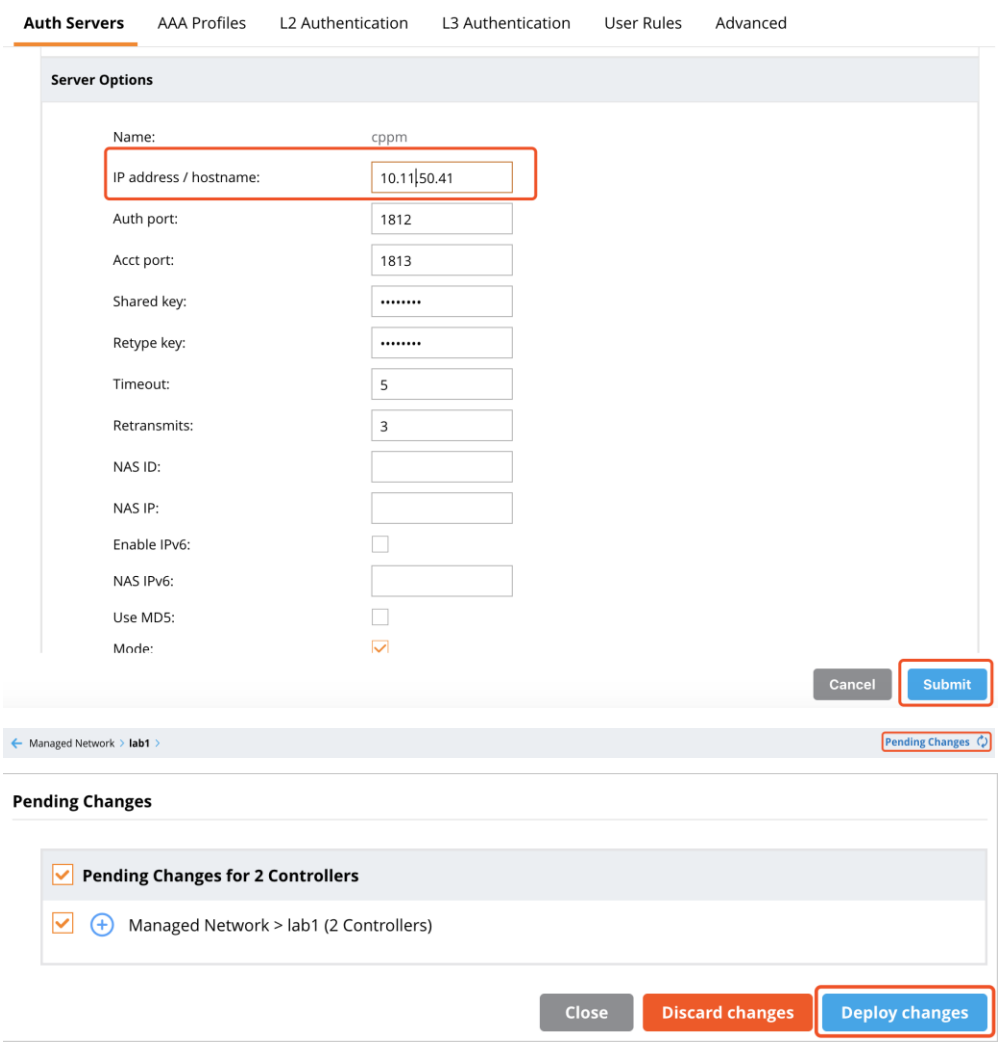
第7步：在ClearPass Policy Manager中，打开 监视 - > 事件查看器 ，在右边可以看到4条 RADIUS ERROR 事件，时间与通过guest-test账号认证的时间一致，点开一条查看 系统事件详细信息 ，查看 Description Failed to decode RADIUS packet - Received packet from 10.1.10.11 with invalid Message-Authenticator! (Shared secret may be incorrect.) ，提示共享密钥可能不正确，前往网络设备中将RADIUS共享密钥还原。



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。

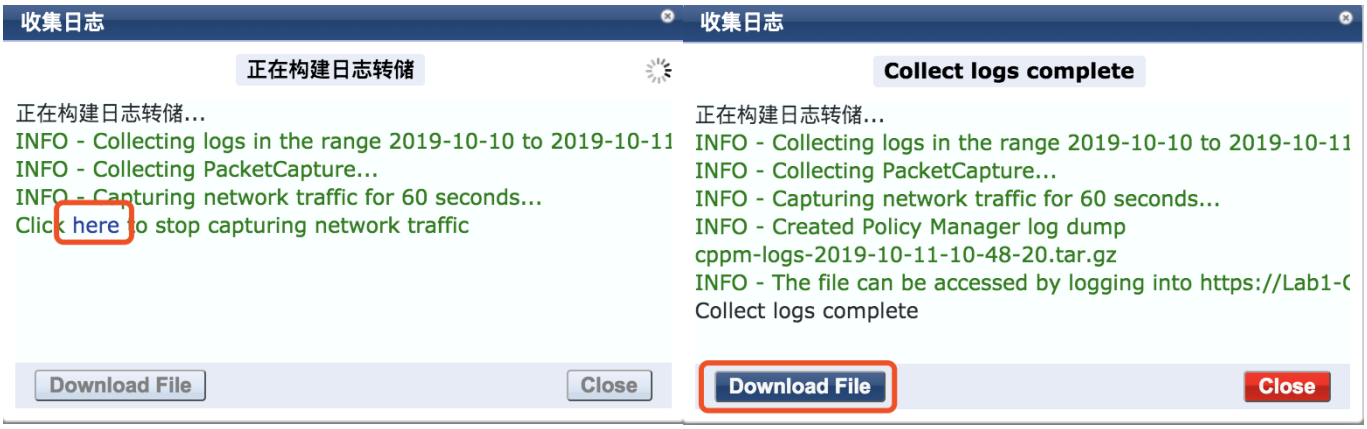




第2步：在ClearPass Policy Manager中，打开 管理 - > 服务器管理器 - > 服务器配置，在右边点击服务器下方的 收集日志 按钮，在弹出的 收集日志 显示框中 勾选捕获网络数据包，取消其它日志的勾选，点 Start 开始抓包。

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?



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。

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。

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。

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。

11.3.2 添加 Virtual IP

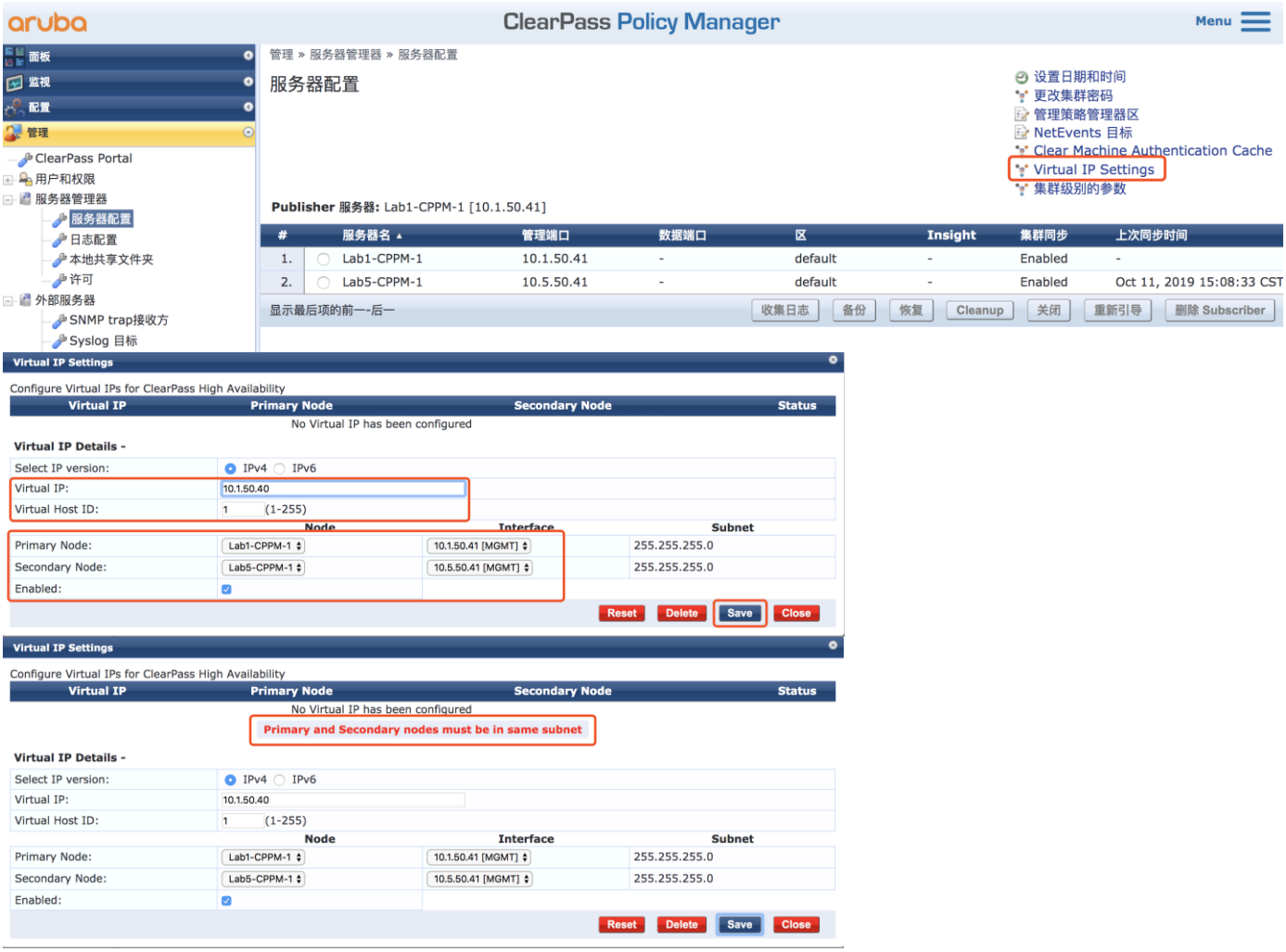
ClearPass要实现认证的冗余备份，除了建立Cluster集群架构外，还需要配置Virtual IP（VRRP），前提是配置Virtual IP的多台ClearPass需要在一个子网网段，本实验采用的Lab中ClearPass都位于不同的子网网段，所以无法配置Virtual IP，以下步骤作为在实际部署环境中配置Virtual IP的参考。

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 。



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

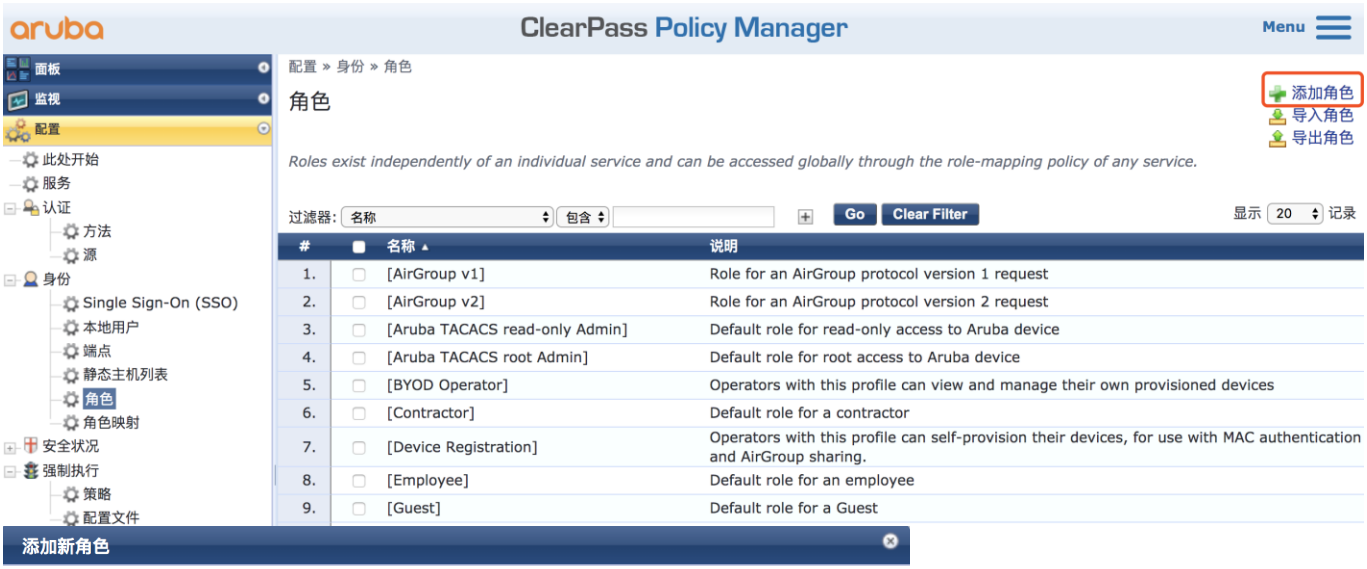
第1步：分别登录Publisher和Subscriber，在ClearPass Policy Manager的 面板 中的 集群状态 下都可以看到两台ClearPass，一个是Publisher，一个是Subscriber，状态都是OK。

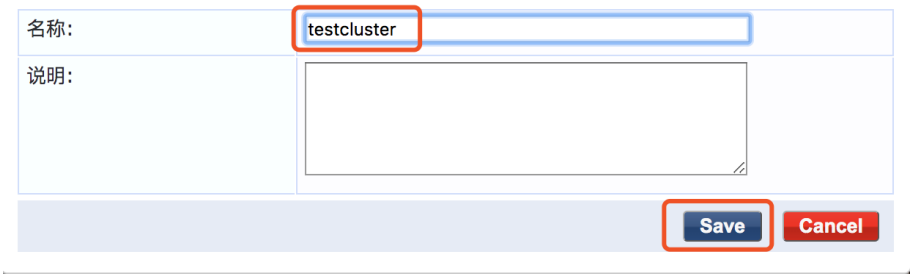
第2步：分别登录Publisher和Subscriber，在ClearPass Policy Manager中，打开 管理 - > 服务器管理器 - > 许可，确认License许可数量是否合并，检查服务器平台License以及应用程序License是否都是激活状态。（本实验Lab中安装的ClearPass为Demo版本，不必确认License数量是否合并）

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 。

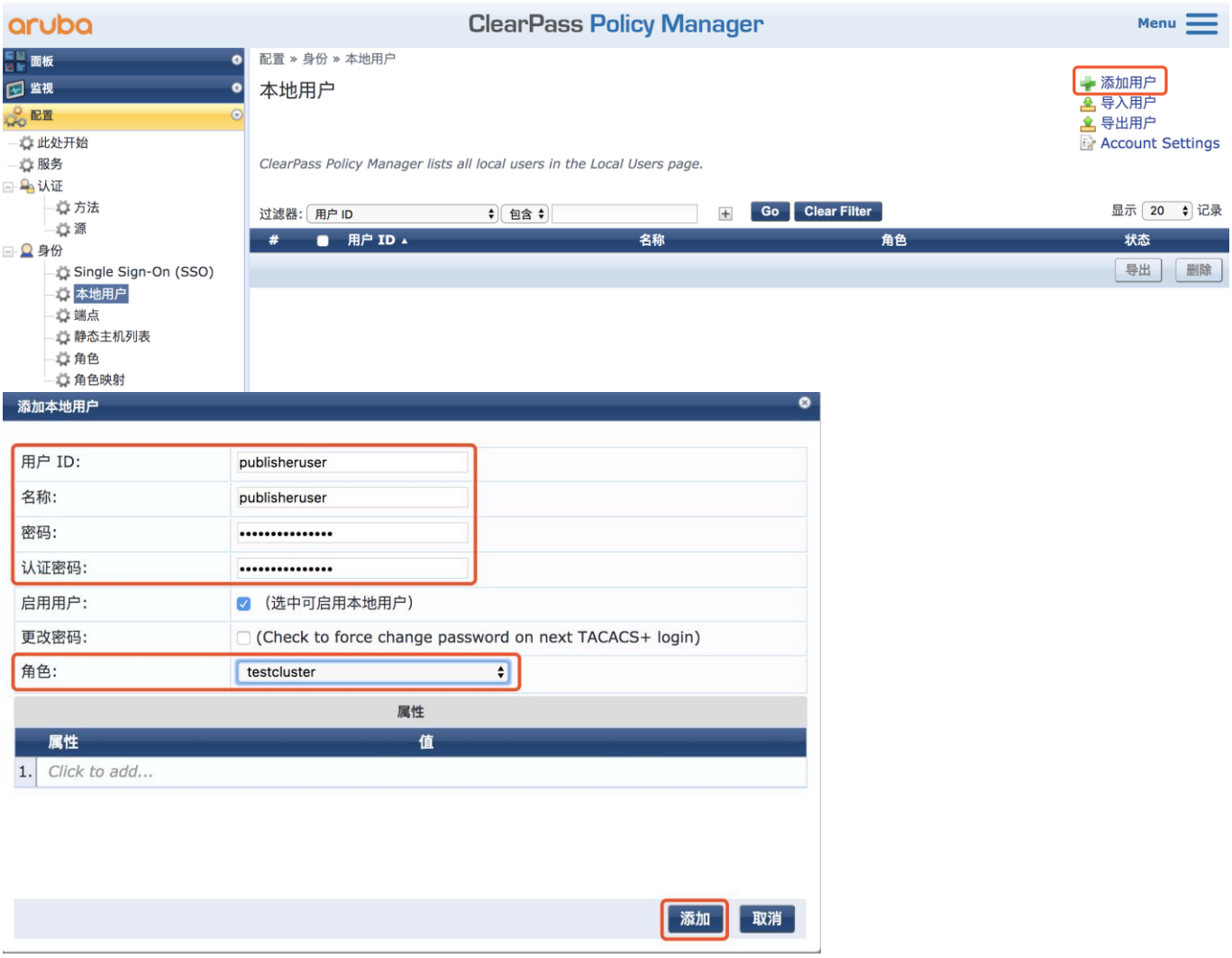




第2步：打开 配置 - > 身份 - > 本地用户，点击右上角的 添加用户 链接，在弹出的 添加本地用户 对话框中输入以下内容：

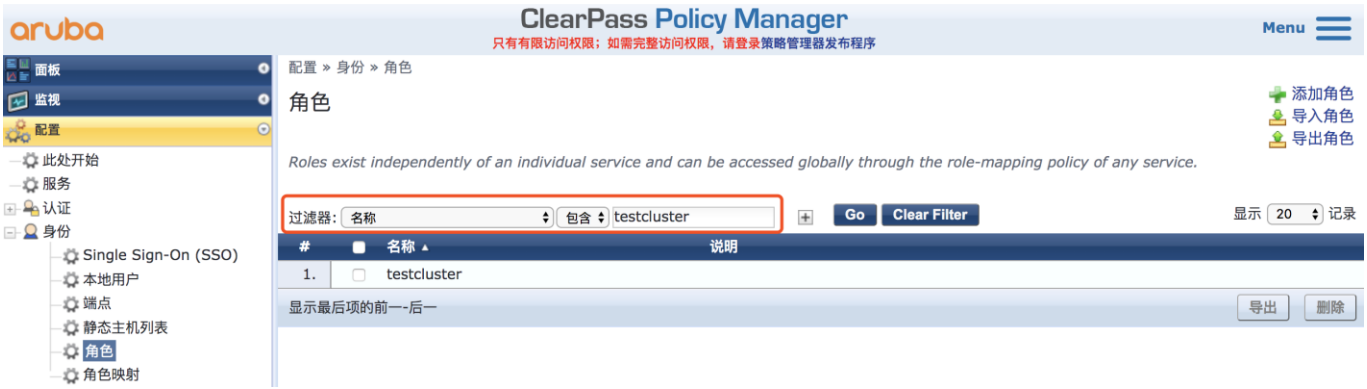
- ✓ 用户ID：publisheruser
- ✓ 名称：publisheruser
- ✓ 密码：aruba123
- ✓ 认证密码：aruba123
- ✓ 角色：testcluster

点 添加 按钮。

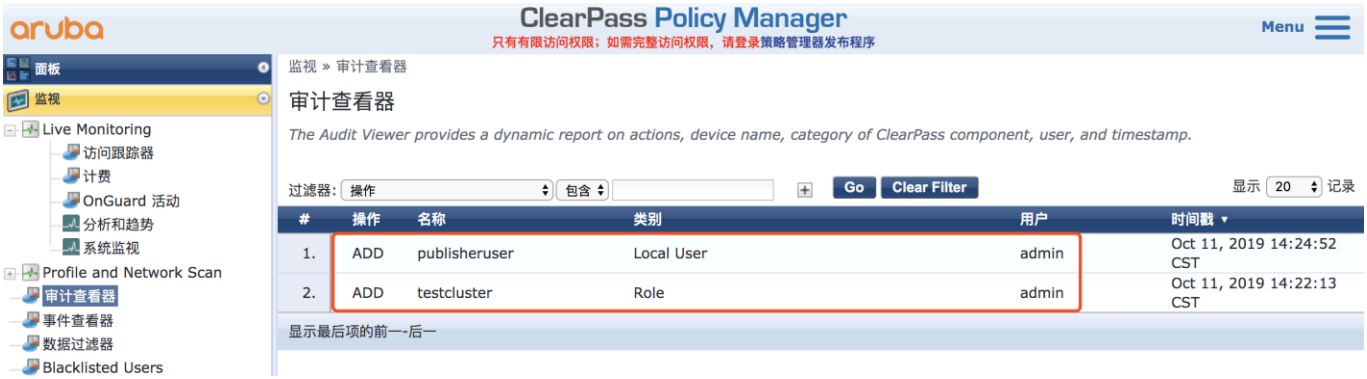


第3步：登录Subscriber，在ClearPass Policy Manager中，打开 配置 - > 身份 - > 角色，在右边的过滤器中输入：名称 包含 testcluster，点 Go 按钮进行过滤，可以看到Subscriber上自动创建了testcluster角色。

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。



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。



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

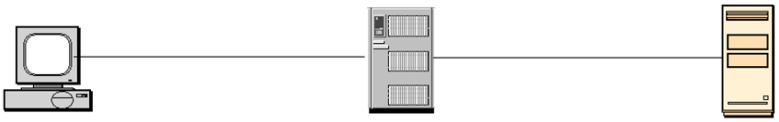
✓ 首先我们需要思考下,在当前的无线网络接入认证方式中，哪一种是最安全的接入认证方式?

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



用户 Login登录　　NAS（RADIUS Client）　　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

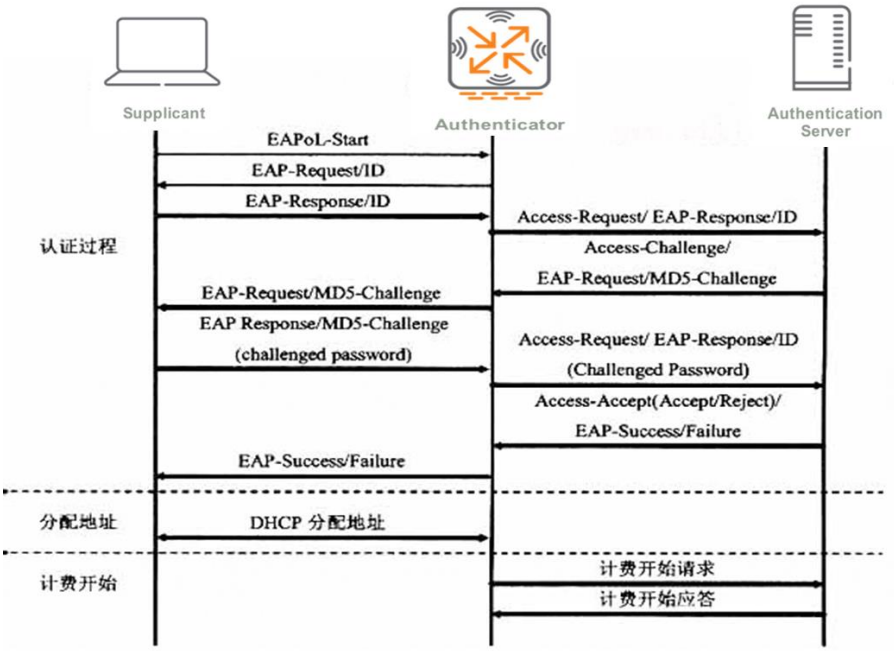
RADIUS
Combines authentication & authorization.
Encrypts only the password.
Requires each network device to contain authorization configuration.
No command logging.
Minimal vendor support for authorization.
UDP- Connectionless UDP ports 1645/1646, 1812/1813
Designed for subscriber AAA

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？

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：

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）

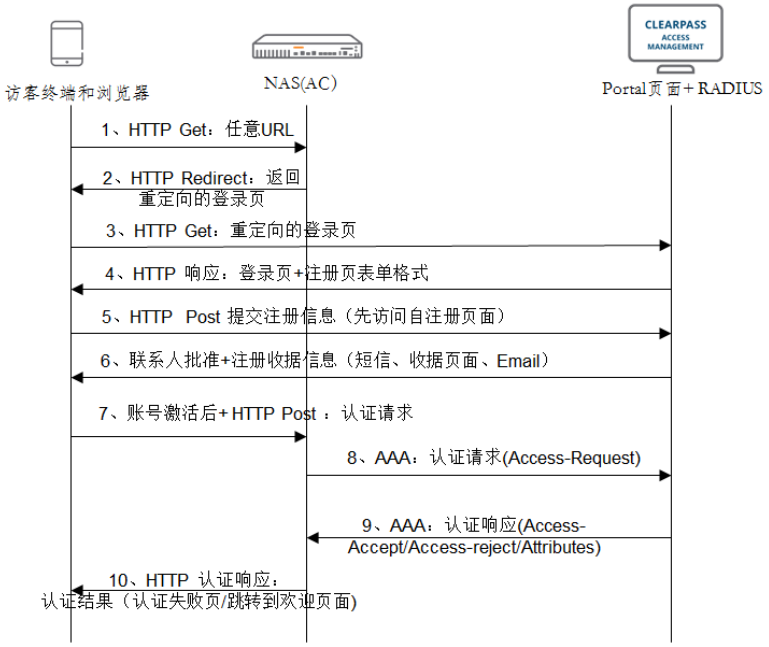
有三个网元部分:

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

Aruba的访客用户自注册认证流程



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?

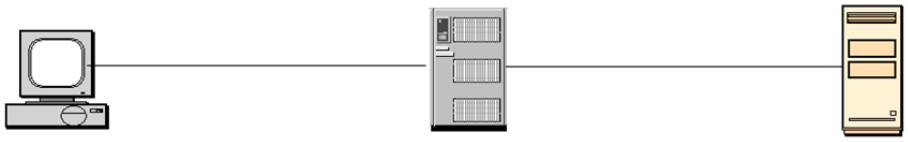
答案：TACACS+认证

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（TACACS Client）** **TACACS 服务器**

通常对TACACS协议的服务端口号是TCP 49

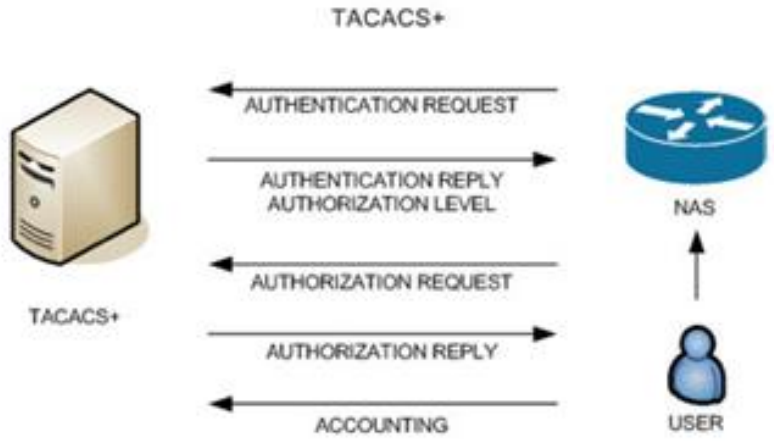
TACACS+
Separates all 3 elements of AAA, making it more flexible.
Encrypts the username and password.
Central management for authorization configuration.
Full command logging.
Supported by most major vendors.
TCP- Connection oriented TCP port 49
Designed for administrator AAA

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）