CPPM 与多厂家 TACACS 对接

版本:1.0

日期:2025-06-26

目录

版本控制信息

★ 文档属性

属性	内容
项目名称	
文档标题	CPPM 与多厂家对接方案
文档版本号	
版本日期	
作者	胡涤穗
审核人	

★ 文档变更过程

版本	更新日期	更新人	主要更新内容
1.0		胡涤穗	新建

第1章 概述

1.1 文档适用人员

本文档资料主要面向负责“cppm 对接各厂商的 tacacs 测试项目”项目的技术人员，管理人员；上海华讯网络系统有限公司的项目实施小组成员以及方参与者，以便通过参考本文档资料顺利完成测试项目。

第2章 测试需求

2.1 合规检测需求

本次项目意在测试 CPPM 的 tacacs 功能在网络环境中的实现效果。主要包括使用 CPPM 与思科、PA、飞塔、F5、CP、深信服，imperva 等厂商做 tacacs 管理员认证。

2.2 测试接入设备需求

测试设备分为有线和无线接入设备，设备范围以目前产线使用产品为依据包括以下品牌设备：

网络设备：思科、PA、飞塔、F5、CP、深信服，imperva

第3章 测试配置

3.1 CPPM 通用配置

3.1.1 添加设备

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：

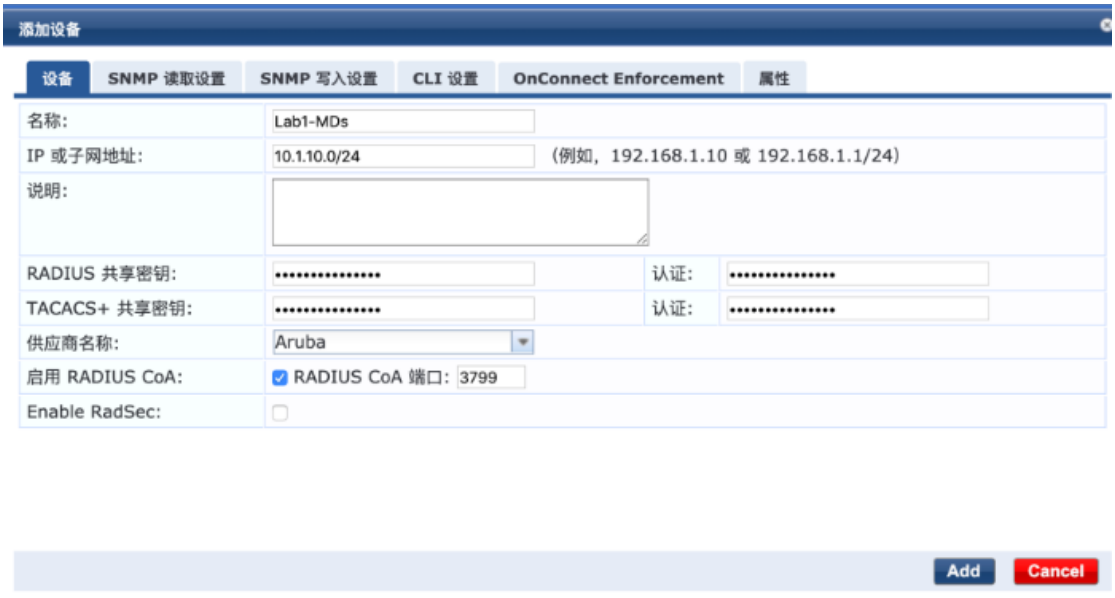
在弹出的对话框中输入以下参数，并点击“保存”

✓ 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



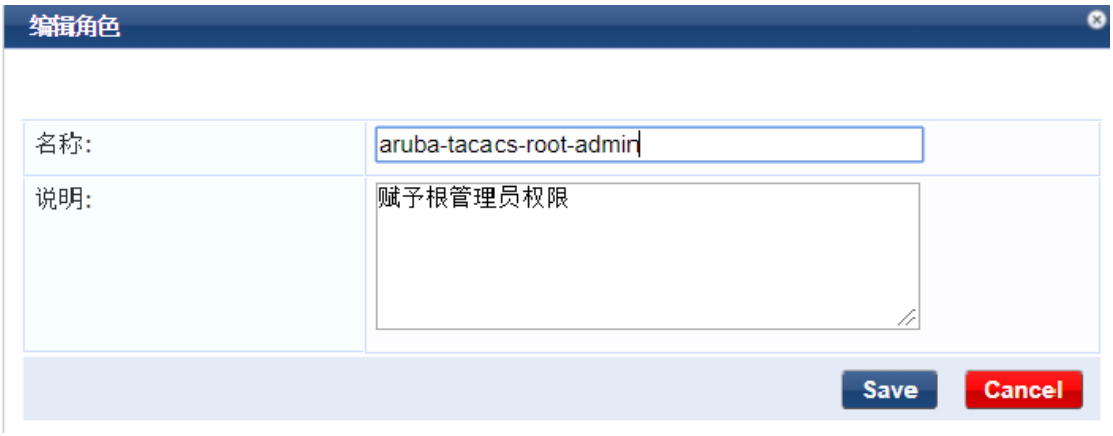
3.1.2 添加本地账号和角色

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：

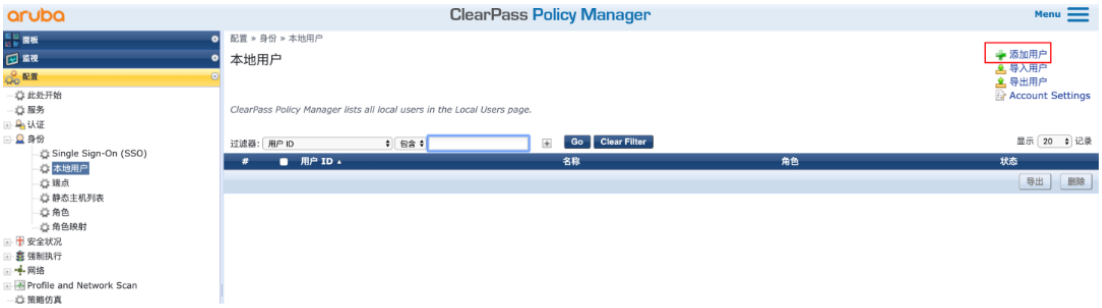
在添加新角色 1 的窗口中，输入下面的参数：

✓名称：aruba-tacacs-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，增加用户账号：



在添加账号的窗口中，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）

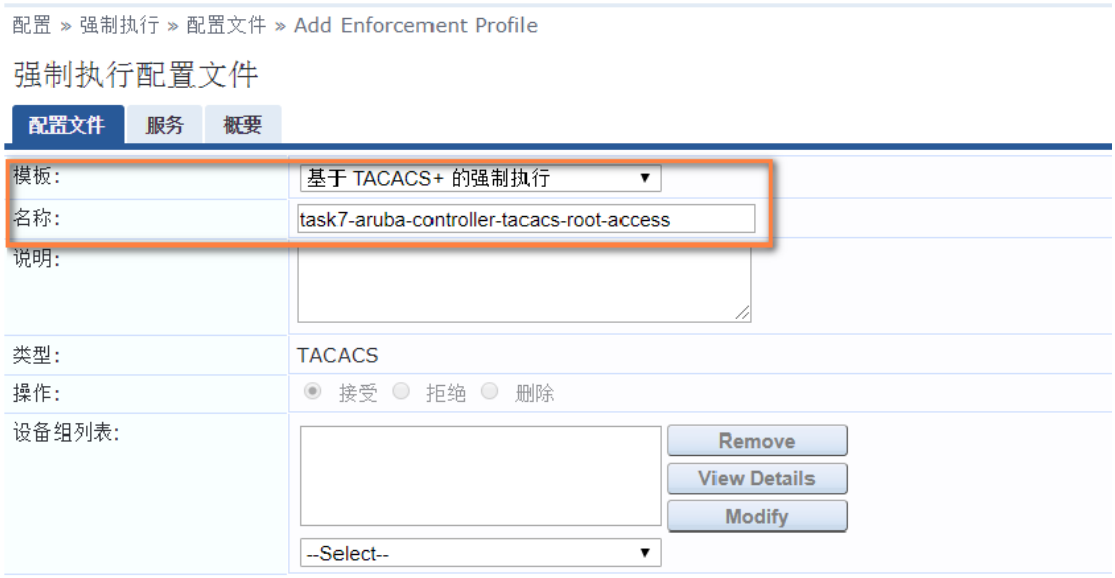
3.1.3 添加认证服务

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：基于 TACACS+的强制执行

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



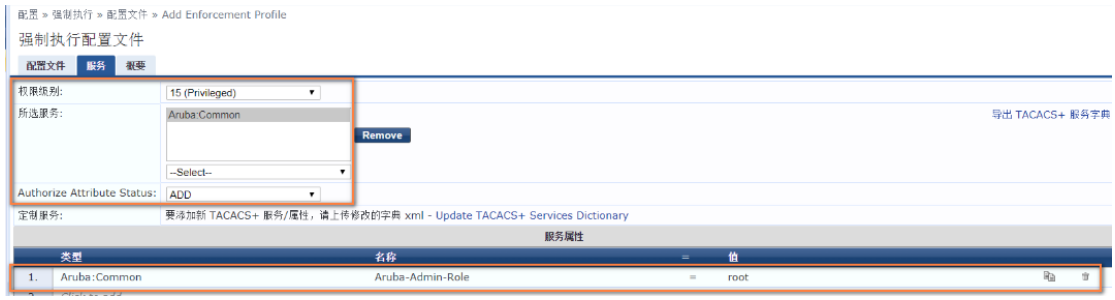
在服务选项卡中，输入下面的参数：

✓ 权限级别： 15(Privileged)

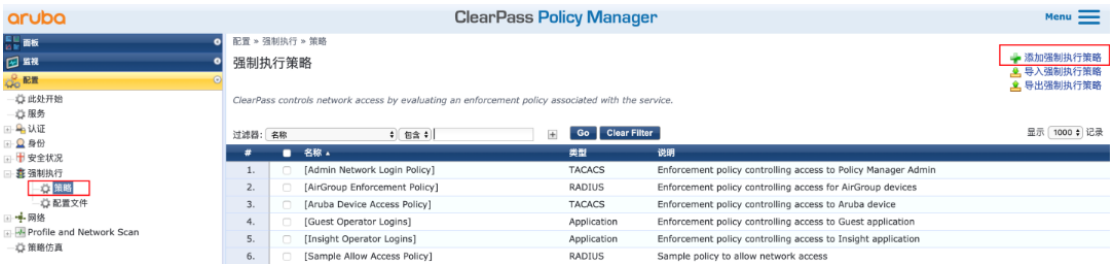
✓ 所选服务： Aruba:Common

✓ 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：



第 2 步：找到 配置 - > 强制执行 - > 策略 ，点击右上角的“添加强制

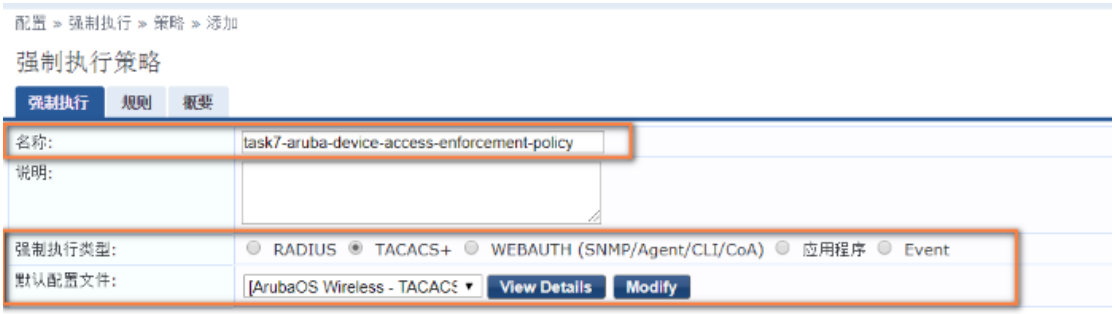
执行策略”按钮，增加一个强制执行策略：

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]（该文件选择适配的对应厂商）



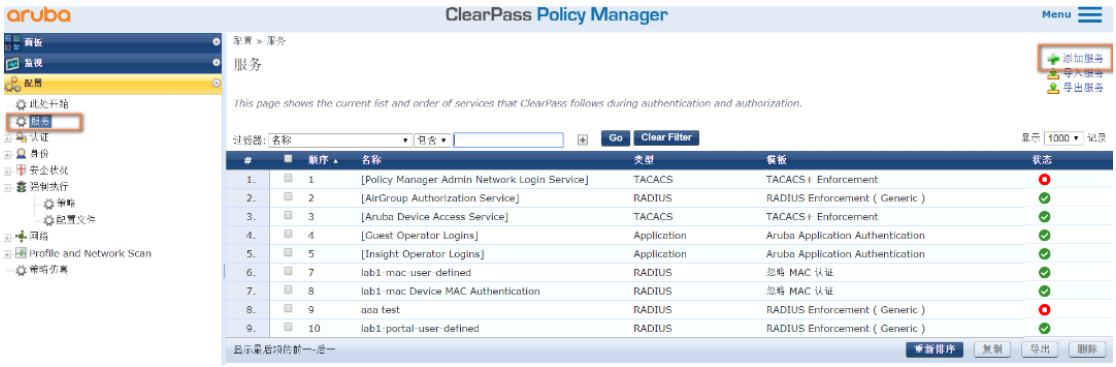
在规则选项卡中，输入下面的参数

✓ 规则：点击“Add Rule”,配置如下

条件是： Tips Role MATCHES_ALL aruba-tacacs-root-admin，[User Authenticated]

✓ 配置文件名：task7-aruba-controller-tacacs-root-access

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



在服务选项卡中，输入下面的参数：

✓ 类型：TACACS+ Enforcement

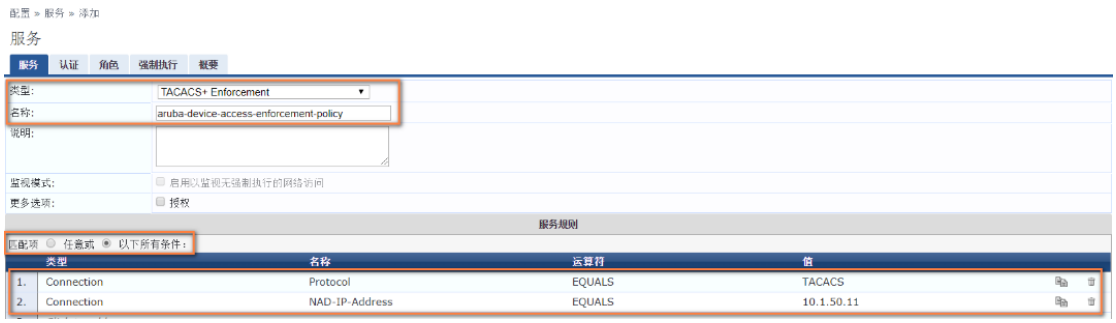
✓ 名称：task7-aruba-device-access-enforcement-policy

✓ 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

✓ 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）

3.2 Cisco

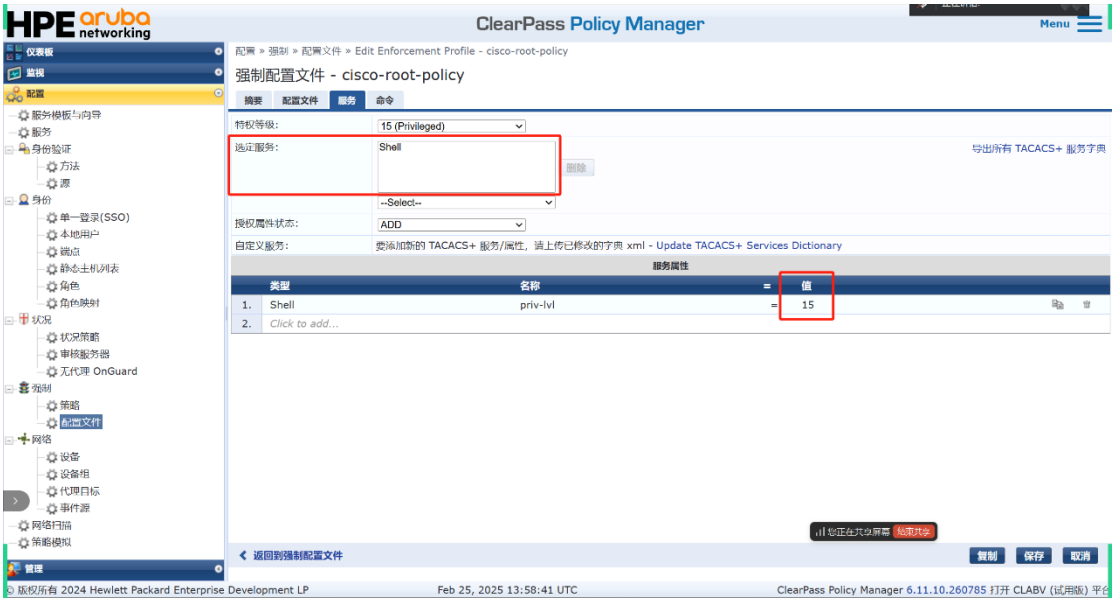
交换机侧命令配置

```
username admin privilege 15 secret 5 $1$aRb8$bt1ydFw.38gOlscjOKmEn1
aaa new-model
!
!
aaa group server tacacs+ cppm
 server-private XXXXXXXX key 7 0207164E09075E731F
 ip tacacs source-interface GigabitEthernet0/7
!
aaa authentication login default group cppm local
aaa authentication enable default group cppm enable
aaa authorization commands 15 default group cppm local
aaa accounting exec default start-stop group cppm
aaa accounting commands 15 default start-stop group cppm
aaa accounting connection default start-stop group cppm
!
!
!
!
!
!
aaa session-id common
tacacs-server directed-request
!
!
!
```

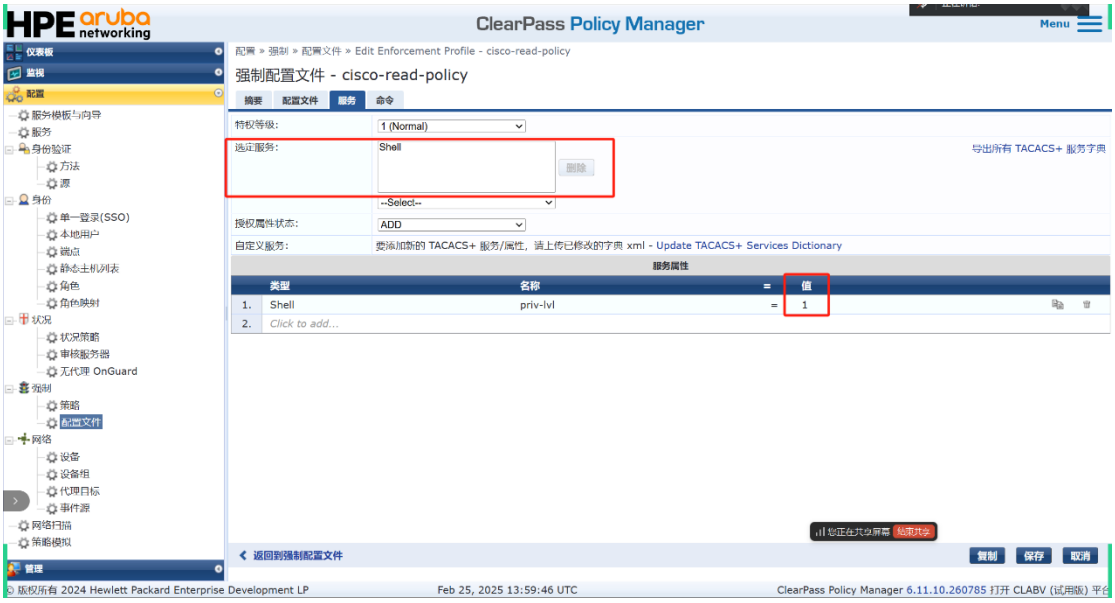
```
line con 0
line vty 0 4
 exec-timeout 30 0
 privilege level 15
 logging synchronous
 transport input telnet ssh
line vty 5 15
!
!
End
```

CPPM 侧配置文件

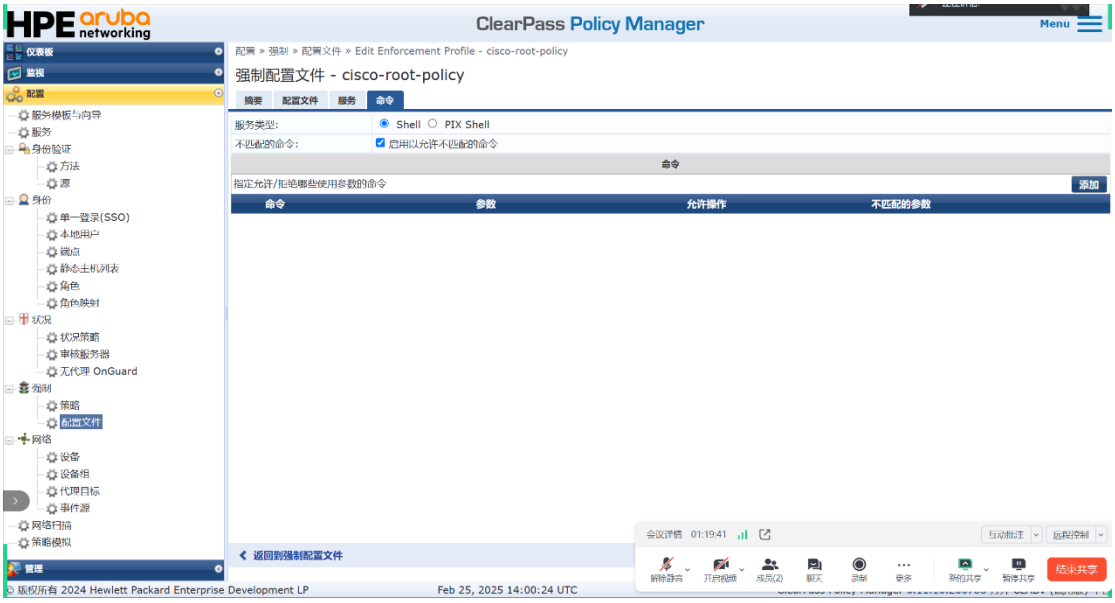
特权等级仅影响登陆时为特权等级或用户层级，实际生效部分为 Shell，root 设置为 15



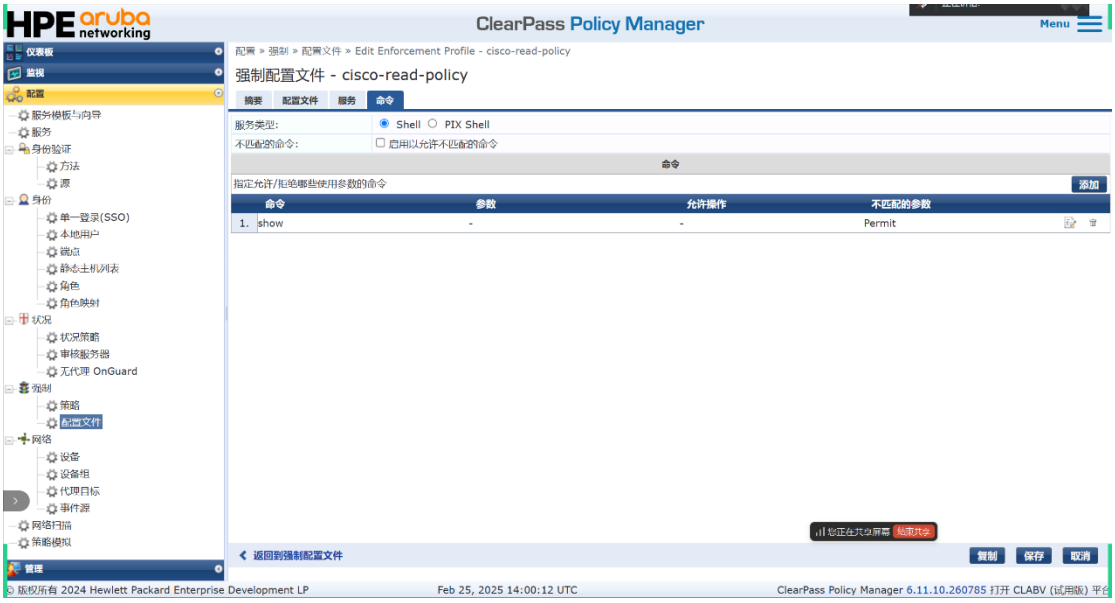
Read 用户设置为 1



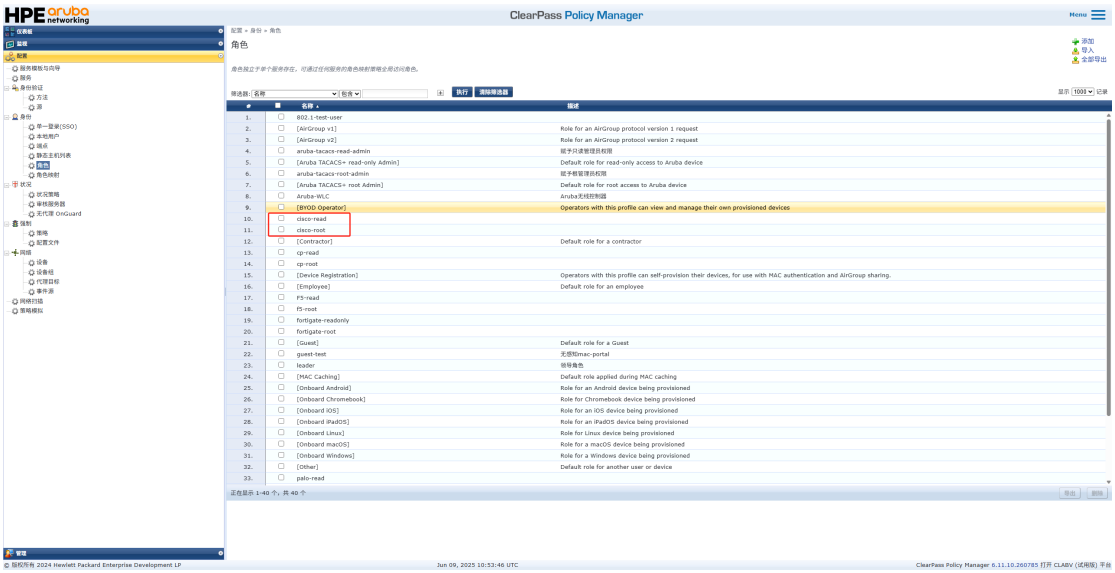
要确保 tacacs 生效，需要再后面勾选启用以允许不匹配命令，这样 CPPM 会放行所有命令



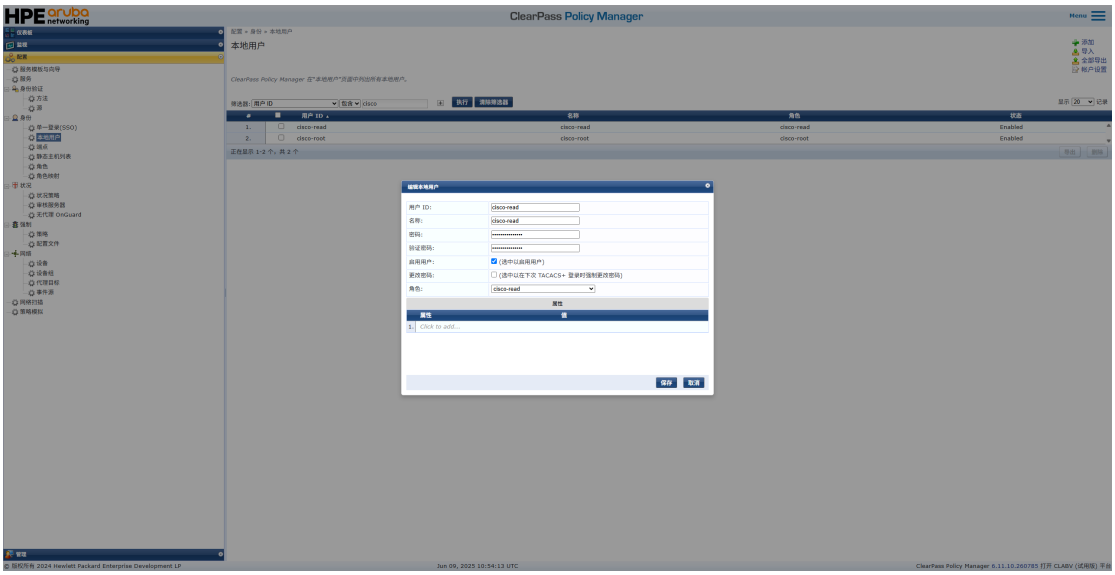
同理，read 用户不需要勾选，在下放单独放行 show 相关命令即可



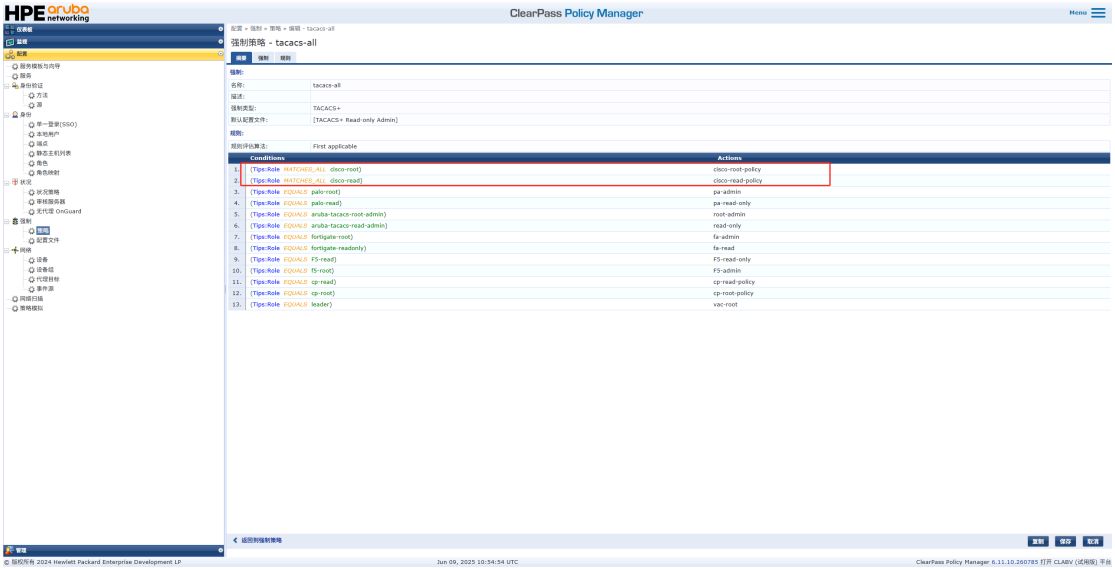
创建对应的相关角色



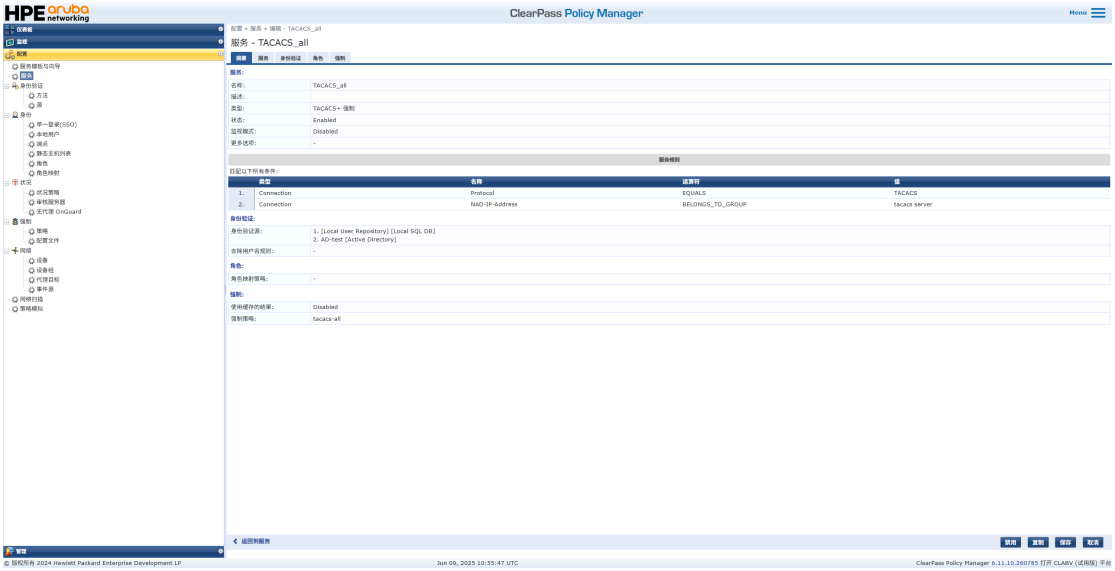
之后创建本地用户并绑定角色

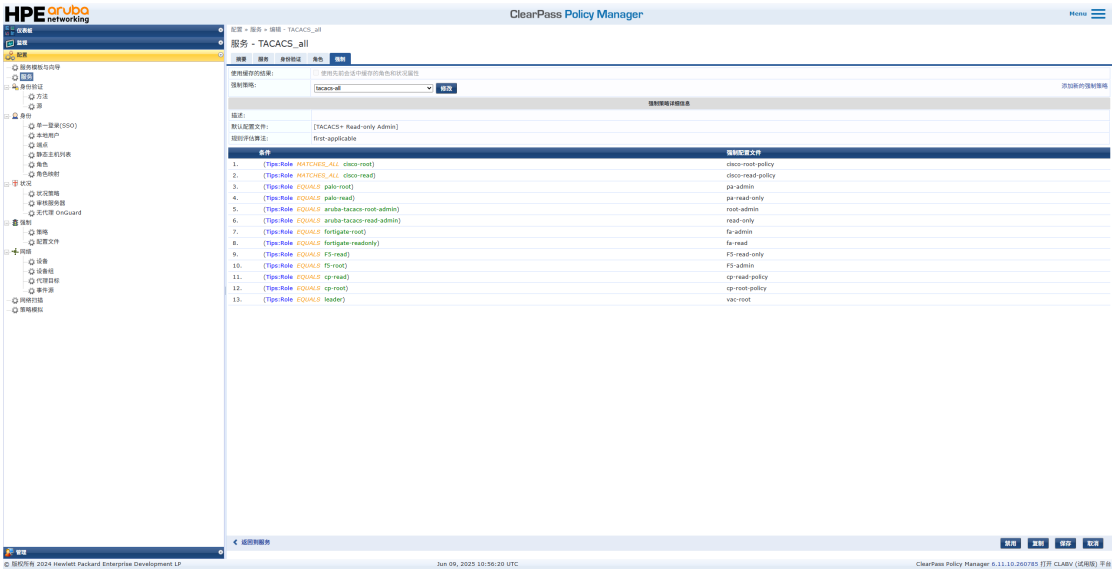


配置策略并将刚刚的角色关联到强制配置文件



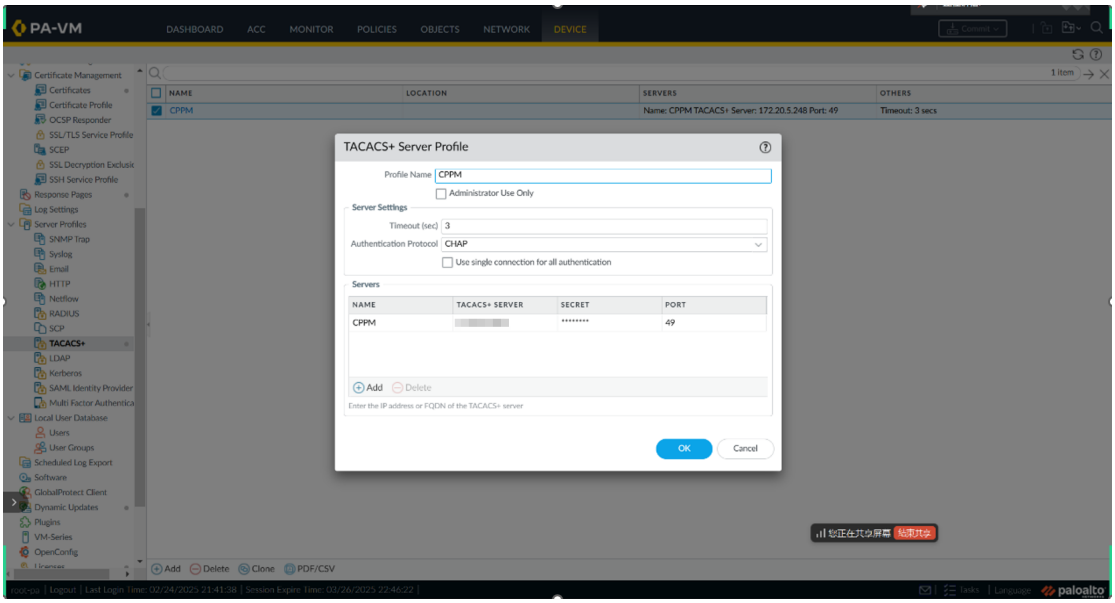
启用 tacacs 服务并调用之前创建的强制策略


HPE aruba networking
ClearPass Policy Manager
Menu
服务 - TACACS_all
概要
服务
身份验证
角色
强制
服务:
名称: TACACS_all
描述:
类型: TACACS+ 强制
状态: Enabled
监视模式: Disabled
更多选项: -
服务规则
匹配以下所有条件:
类型 名称 运算符 值
1. Connection Protocol EQUALS TACACS
2. Connection NAD-IP-Address BELONGS_TO_GROUP tacacs server
身份验证:
身份验证源: 1. [Local User Repository] [Local SQL DB]
2. AD-test [Active Directory]
去除用户名规则: -
角色:
角色映射策略: -
强制:
使用缓存的结果: Disabled
强制策略: tacacs-all
返回到服务
禁用
复制
保存
取消
© 版权所有 2024 Hewlett Packard Enterprise Development LP
Jun 09, 2025 10:55:47 UTC
ClearPass Policy Manager 6.11.10.260785 打开 CLABV (试用版) 平台

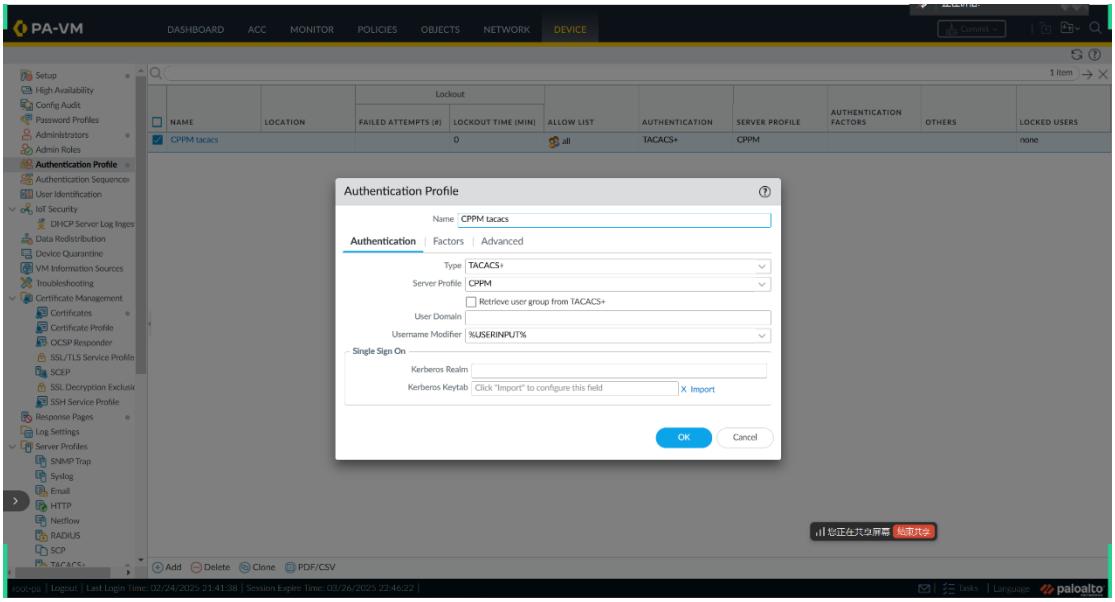

HPE aruba networking
ClearPass Policy Manager
Menu
服务 - TACACS_all
概要
服务
身份验证
角色
强制
使用缓存的结果:
强制策略: tacacs-all
修改
添加新的强制策略
强制策略详细信息
描述:
默认配置文件: [TACACS+ Read-only Admin]
现行评估算法: first-applicable
条件 强制配置文件
1. (Tips:Role MATCHES_ALL cisco-root) cisco-root-policy
2. (Tips:Role MATCHES_ALL cisco-read) cisco-read-policy
3. (Tips:Role EQUALS palo-root) pa-admin
4. (Tips:Role EQUALS palo-read) pa-read-only
5. (Tips:Role EQUALS aruba-tacacs-root-admin) root-admin
6. (Tips:Role EQUALS aruba-tacacs-read-admin) read-only
7. (Tips:Role EQUALS fortigate-root) fa-admin
8. (Tips:Role EQUALS fortigate-readonly) fa-read
9. (Tips:Role EQUALS FS-read) FS-read-only
10. (Tips:Role EQUALS FS-root) FS-admin
11. (Tips:Role EQUALS cp-read) cp-read-policy
12. (Tips:Role EQUALS cp-root) cp-root-policy
13. (Tips:Role EQUALS leader) vac-root
返回到服务
禁用
复制
保存
取消
© 版权所有 2024 Hewlett Packard Enterprise Development LP
Jun 09, 2025 10:56:20 UTC
ClearPass Policy Manager 6.11.10.260785 打开 CLABV (试用版) 平台

3.3 Palo alto

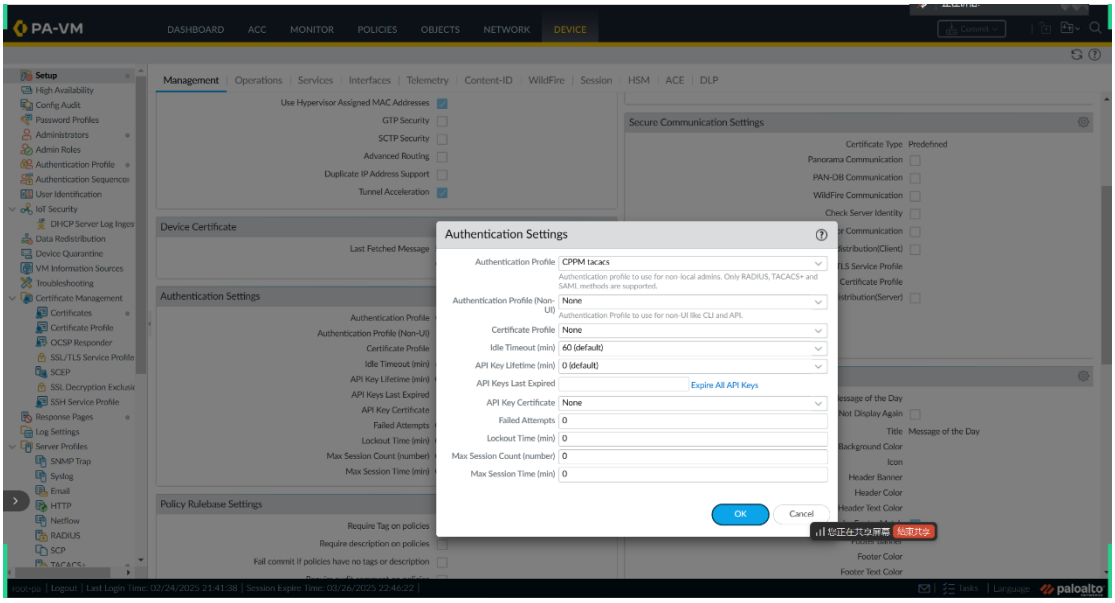
PA 需要在 server profile 中新建 CPPM 的 tacacs



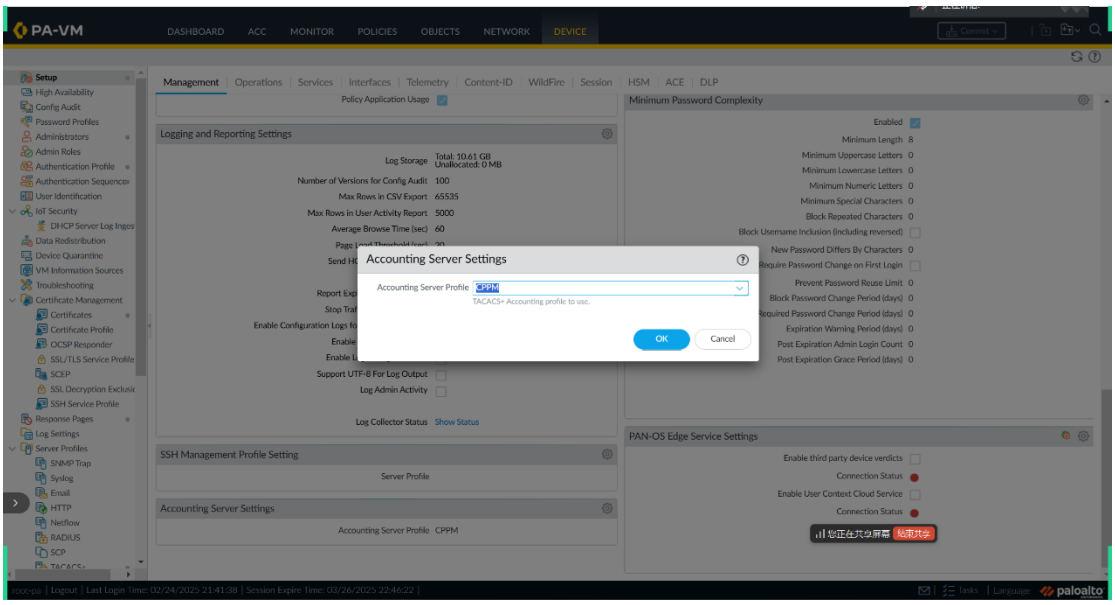
之后在 Authentication profile 中绑定之前创建的 CPPM 文件



在 Setup 层级中调整相关配置，将 Authentication Profile 绑定



Accounting server 设置为之前创建的 CPPM server profile



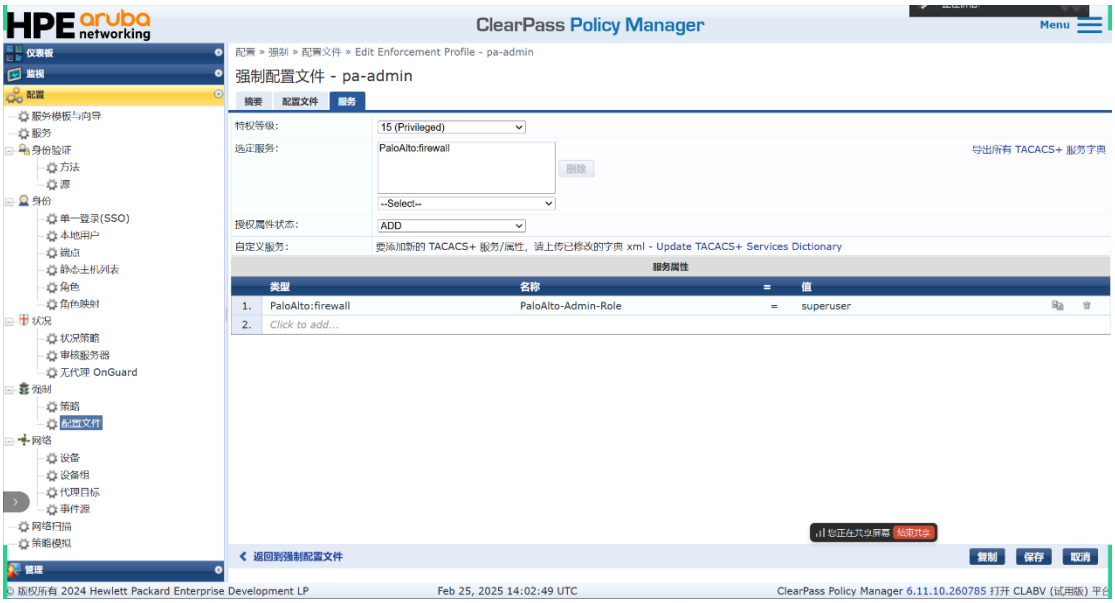
特权等级参数 配置管理员或只读权限均需要配置特权等级为 15

相关特权配置参数

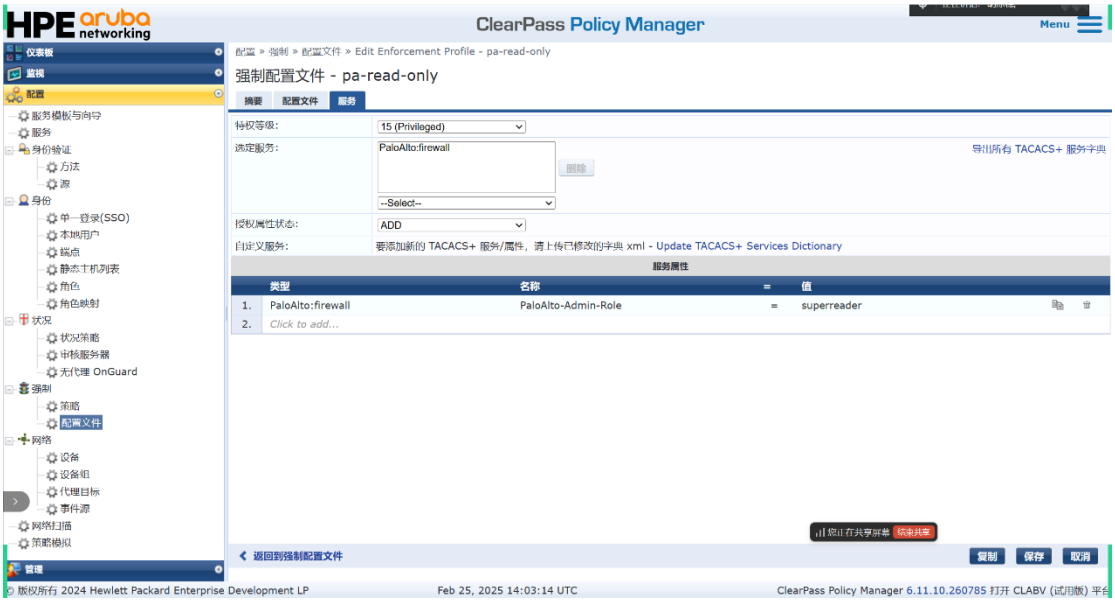
PaloAlto-Admin-Role is the name of the role for the user. It can be the name of a **custom Admin role profile** configured on the firewall or one of the following predefined roles:

- **superuser : Superuser (used in this example)**
- **superreader : Superuser (read-only) (used in this example)**
- deviceadmin : Device administrator
- devicereader : Device administrator (read-only)
- vsysadmin : Virtual system administrator
- vsysreader : Virtual system administrator (read-only)

CPPM 侧配置文件相关需要按照以上参数设定，superuser 为超级管理员



只读用户设置为 Superreader



其余用户创建与策略/服务配置参考思科部分

3.4 飞塔

命令行相关配置

Edited

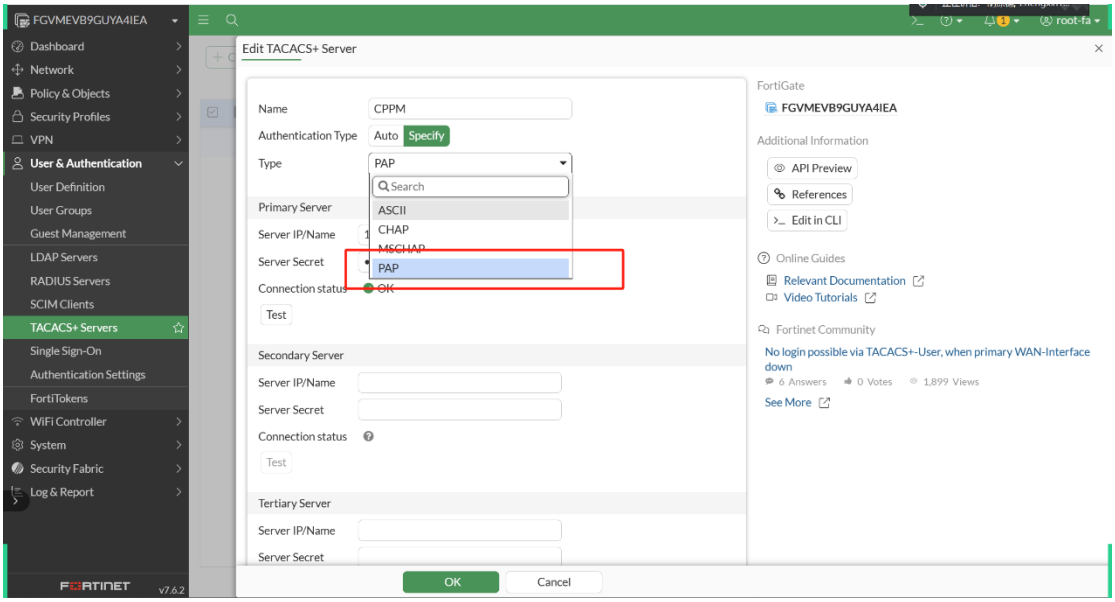
I use the attached Dictionary and Enforcement Profiles. On FortiGate the following is configured:

```
config system accprofile
edit "prof_admin"
set secfabgrp read-write
set ftviewgrp read-write
set authgrp read-write
set sysgrp read-write
set netgrp read-write
set loggrp read-write
set fwgrp read-write
set vpngrp read-write
set utmgrp read-write
set wifi read-write
next
edit "prof_operator"
set secfabgrp read
set ftviewgrp read
set authgrp read
set sysgrp read
set netgrp read
set loggrp read
set fwgrp read
set vpngrp read
```

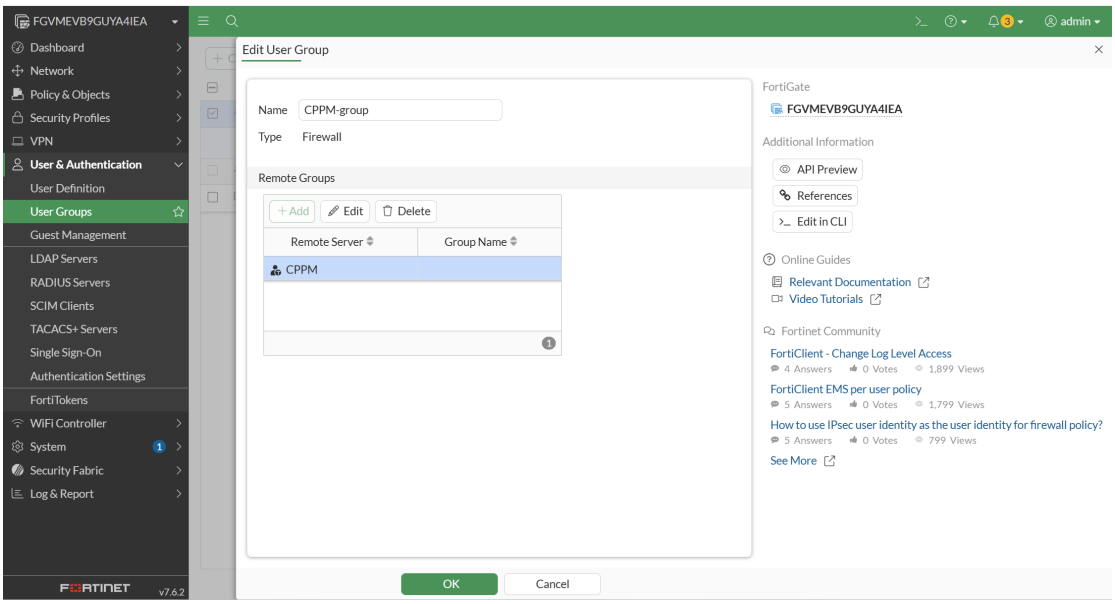
```
set utmgrp read
set wifi read
next
end

...

config system admin
edit "tacacs"
set remote-auth enable
set accprofile "super_admin"
set vdom "root"
set wildcard enable
set remote-group "tacacs"
set accprofile-override enable
next
end

...

config user group
edit "tacacs"
set member "cppm_tacacs"
next
end

...
```

```
config user tacacs+
edit "cppm_tacacs"
set server "XXXXXXXX"
set key ENC K1ZLi0ii7jfeya/jtziqTD/fKLER1k+RdQJxB2aFIisJUbdqlpoJOSLMKP8TK++KEh5LiA34wdLqqCb9nN1cBXMRNEX5Amc1K2Ej1qzYAmIBL9t5Zho7aVZfVP5m/wVC3YP23qM5m5I8Y6QnwHOAJ/NLVO1NCdYZFiH2oBhYDZ5JKh93fy1T6Gp013zMkM6WJtjNEw==
set authen-type ascii
set authorization enable
set source-ip "XXXXXX"
next
End
```

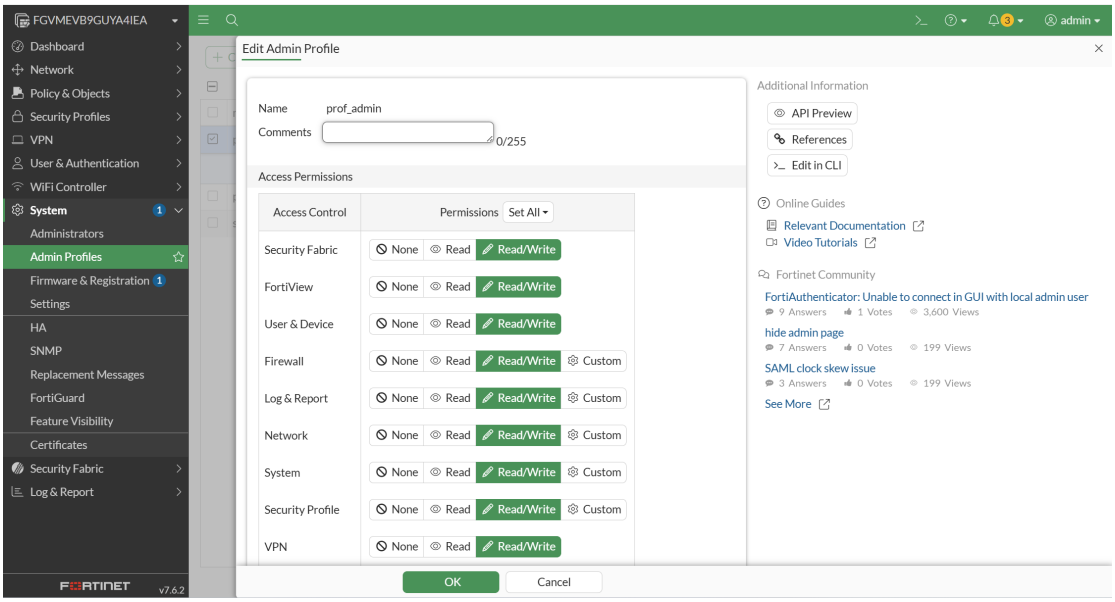
如果采取 WEB 方式，配置需要选择 Tacacs servers，创建服务器对接，需要注意选择 CHAP 会导致 CPPM 上密码错误，在这里要将其改为 PAP 模式



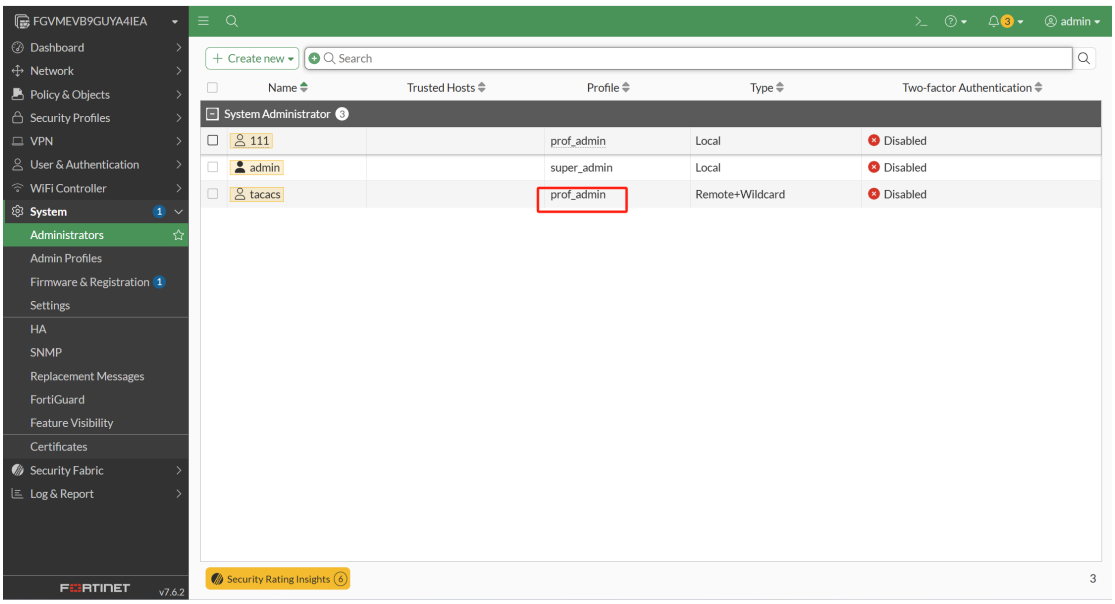
新建 User Group 并绑定 CPPM sever



新建 Profile，一个 root 权限，一个 readonly



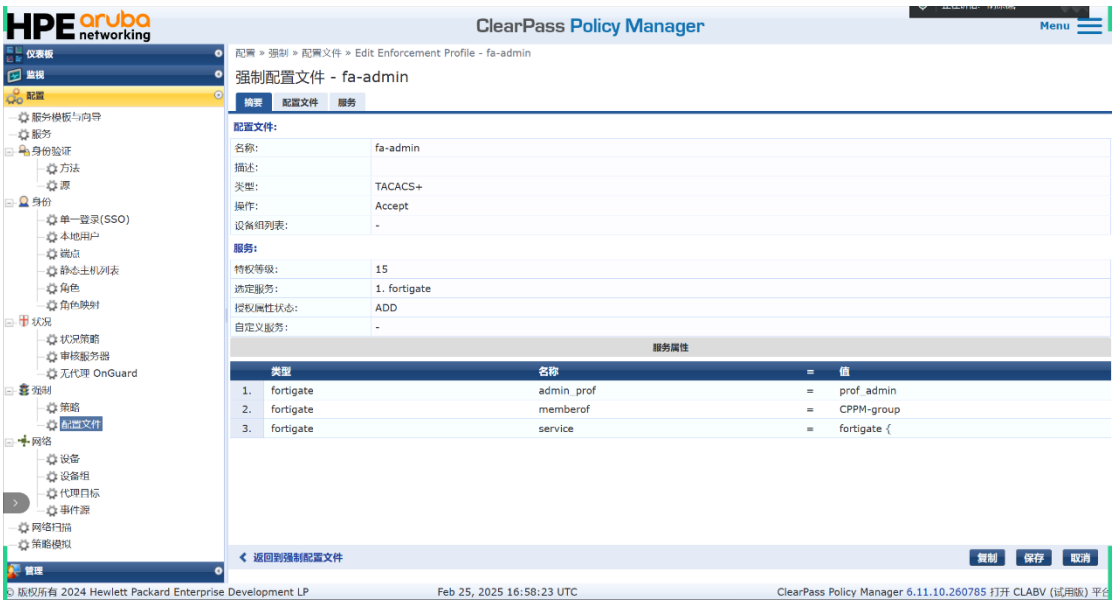
新建 administrator，并且绑定相关的 profile



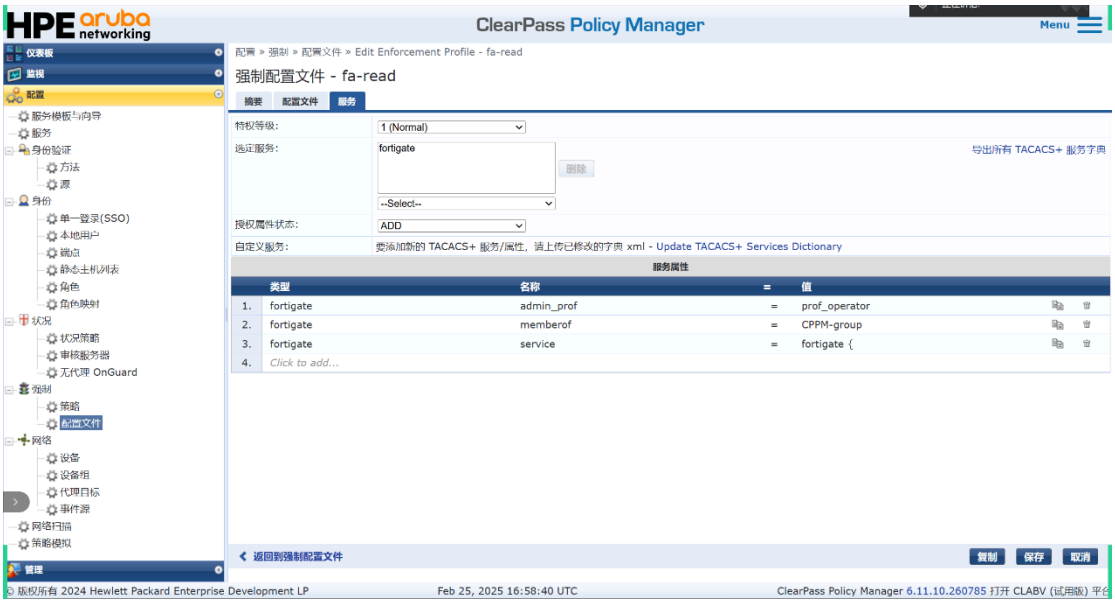
CPPM 相关配置如下图所示

备注：member 与 prof 需要与飞塔实际配置匹配

Root 配置



Readonly 配置



其余用户创建与策略/服务配置参考思科部分

3.5 Check point

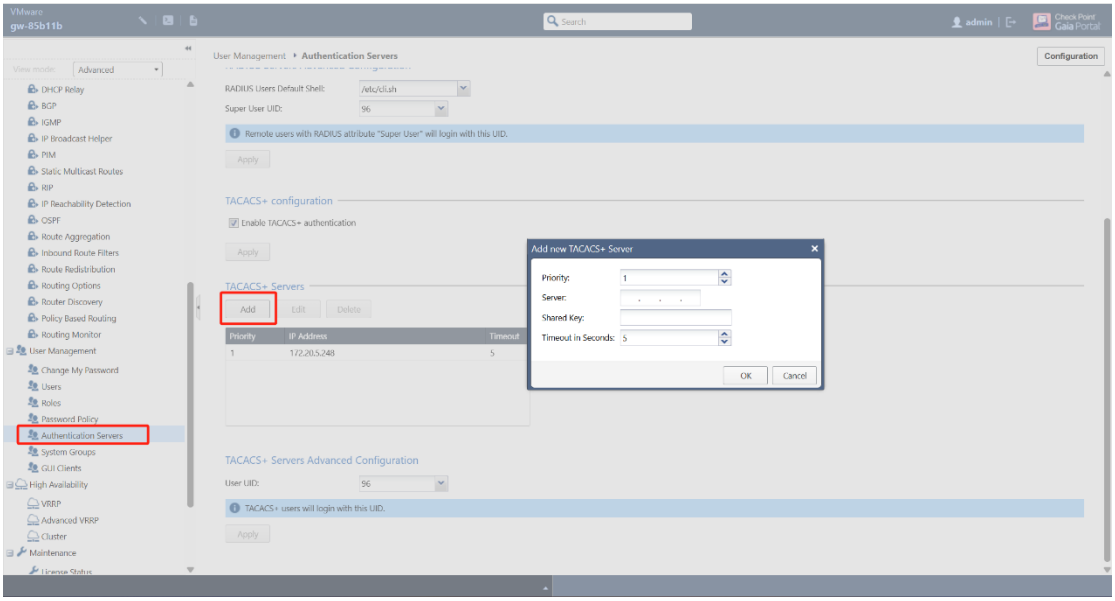
服务配置部分不生效，CP 负责本地授权，CPPM 只负责通过账户认证

Aruba 部分配置文件如下

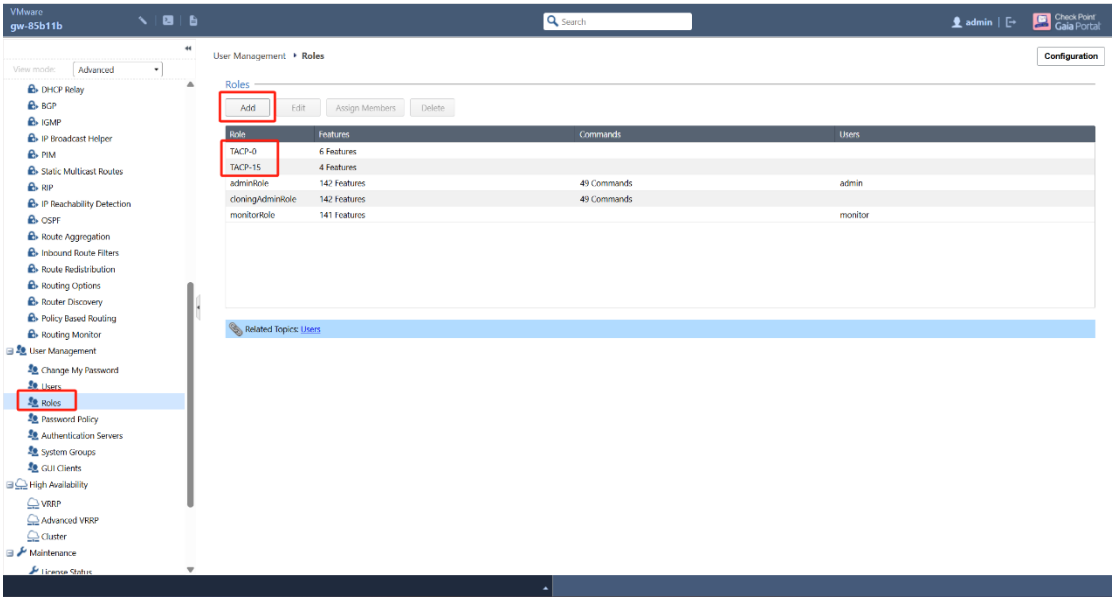
其余用户创建与策略/服务配置参考思科部分

CP 部分配置如下

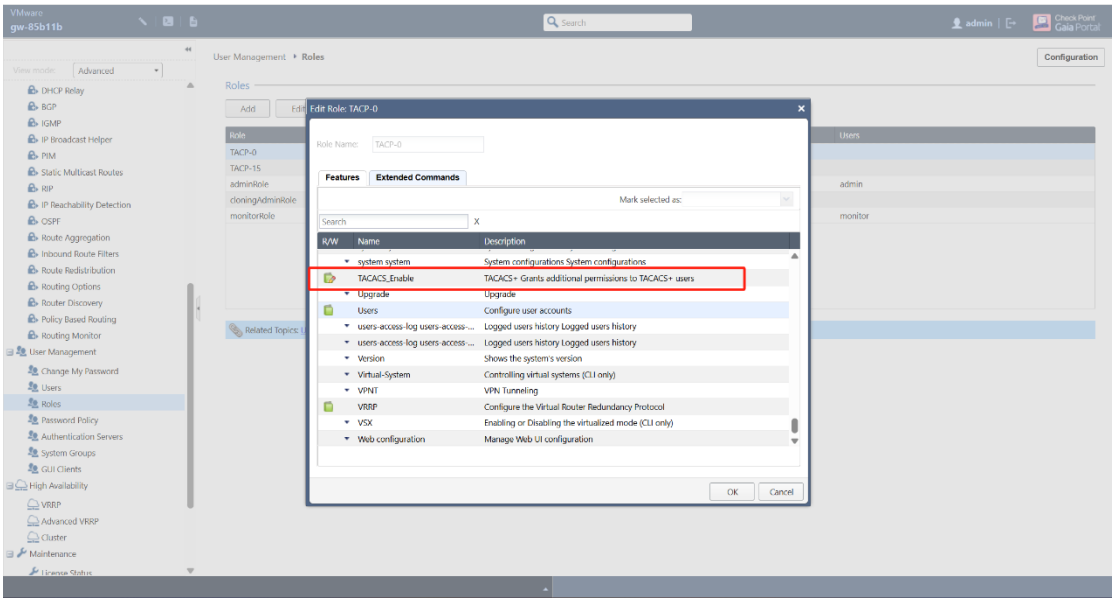
进入 Authentication Servers 添加 CPPM 服务器地址

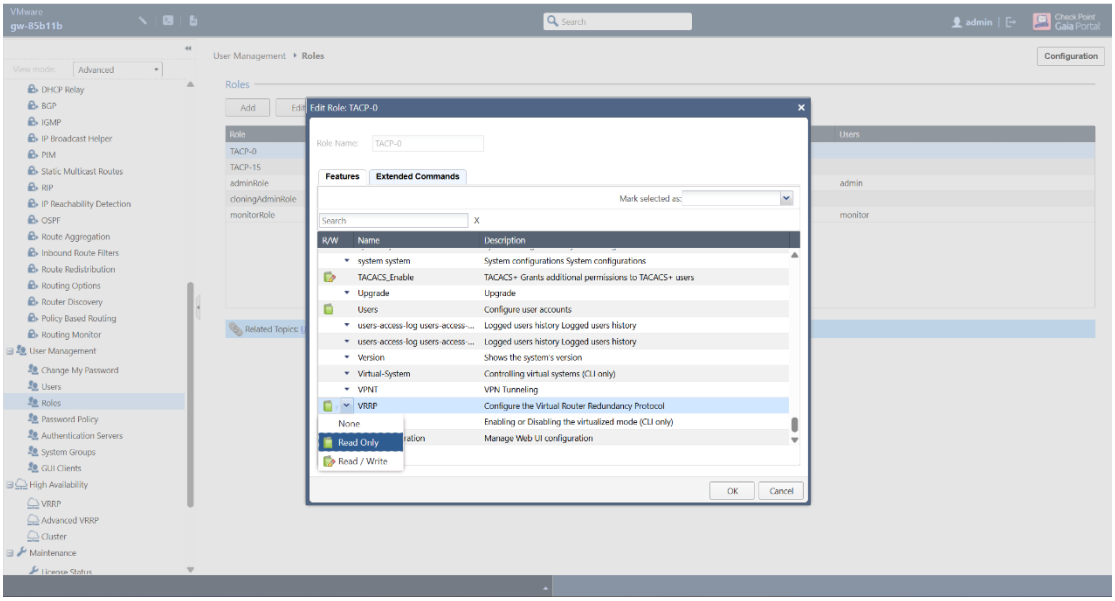


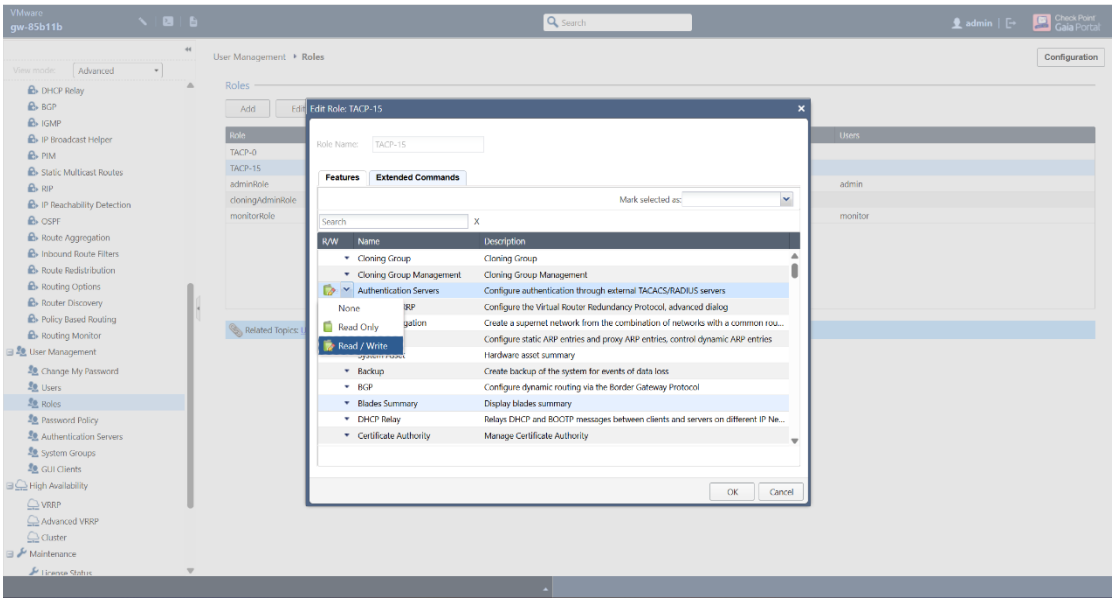
之后再 Role 中创建对应的用户角色，权限按需分配



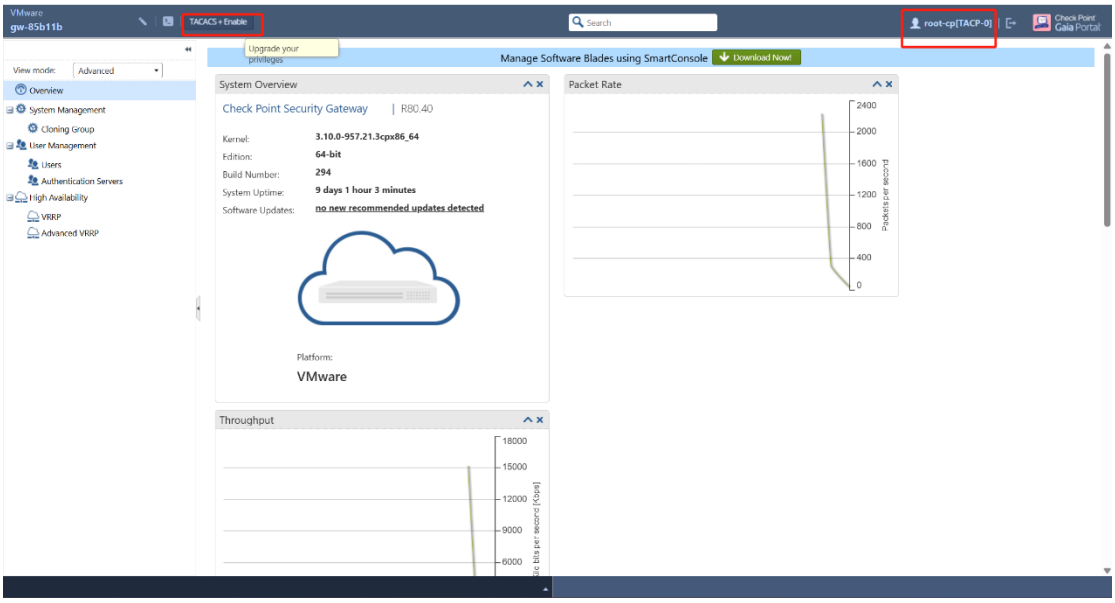
编辑角色，按照 admin 或 readonly 权限分配

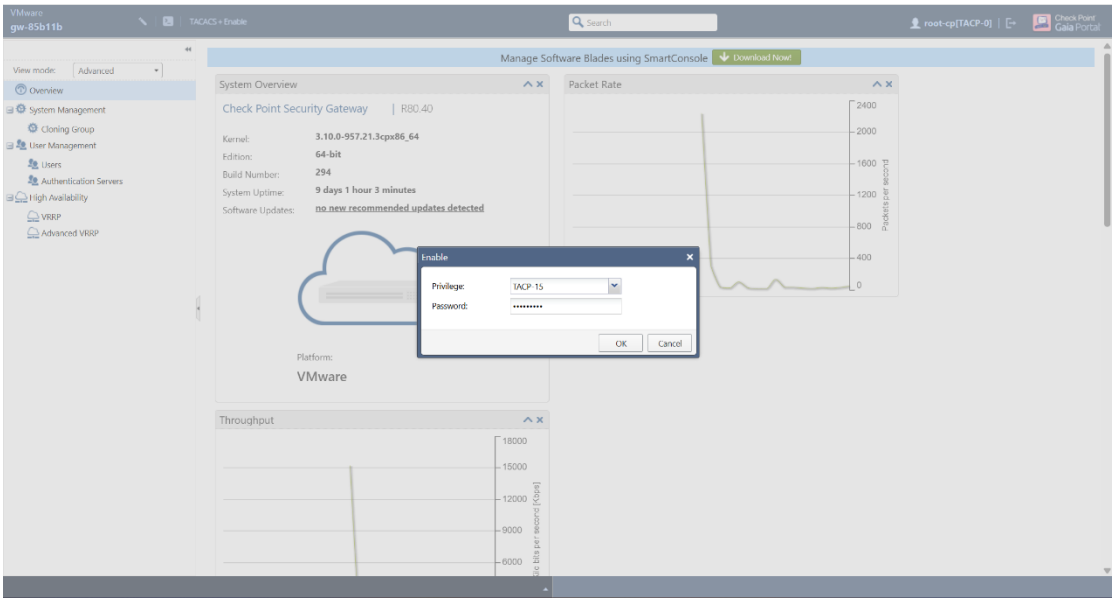

Edit Role: TACP-0
Role Name: TACP-0
Features
Extended Commands
Mark selected as:
R/W
Name
Description
system system
System configurations System configurations
TACACS_Enable
TACACS+ Grants additional permissions to TACACS+ users
Upgrade
Upgrade
Users
Configure user accounts
VRRP
Configure the Virtual Router Redundancy Protocol
VSX
Enabling or Disabling the virtualized mode (CLI only)
Web configuration
Manage Web UI configuration
OK
Cancel

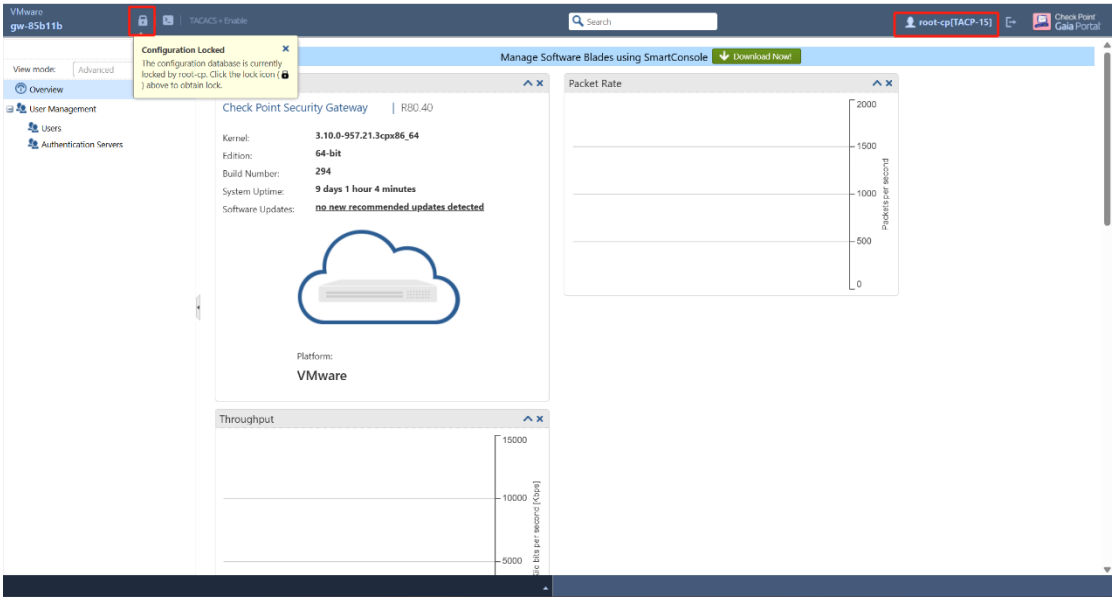

Edit Role: TACP-0
Role Name: TACP-0
Features
Extended Commands
None
Read Only
Read / Write
OK
Cancel



首次登录账户一般默认配置为 readonly，如要提权，需要点击左上角部分选择对应权限的 Role



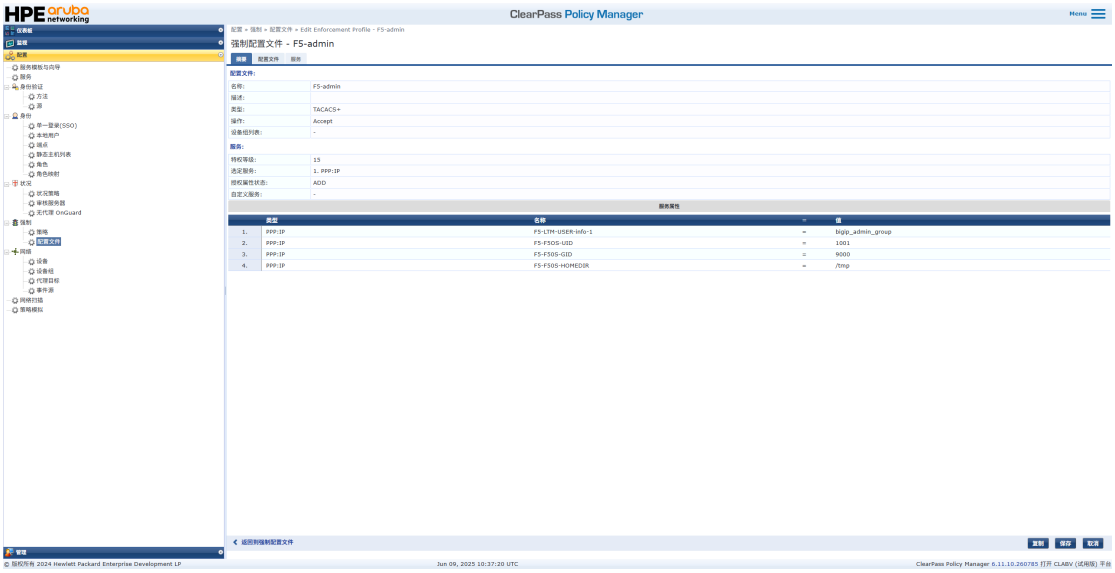

VMware
gw-85b11b
TACACS + Enable
Search
root-cp[TACP-0]
Check Point Gaia Portal
Manage Software Blades using SmartConsole
Download Now!
View mode:
Advanced
Overview
System Management
Cloning Group
User Management
Users
Authentication Servers
High Availability
VRRP
Advanced VRRP
System Overview
Check Point Security Gateway
R80.40
Kernel:
3.10.0-957.21.3cpx86_64
Edition:
64-bit
Build Number:
294
System Uptime:
9 days 1 hour 3 minutes
Software Updates:
no new recommended updates detected
Platform:
VMware
Packet Rate
Packets per second
Enable
Privilege:
TACP-15
Password:
OK
Cancel
Throughput
Kbits per second [Kbps]

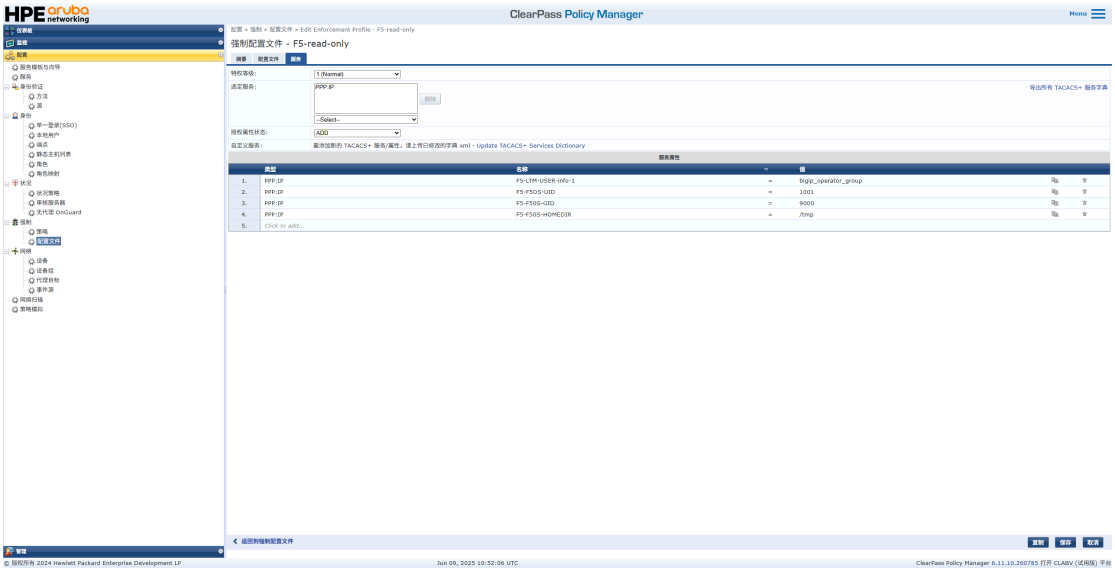

VMware
gw-85b11b
TACACS + Enable
Search
root-cp[TACP-15]
Check Point Gaia Portal
Configuration Locked
The configuration database is currently locked by root-cp. Click the lock icon ( ) above to obtain lock.
Manage Software Blades using SmartConsole
Download Now!
View mode:
Advanced
Overview
User Management
Users
Authentication Servers
Check Point Security Gateway
R80.40
Kernel:
3.10.0-957.21.3cpx86_64
Edition:
64-bit
Build Number:
294
System Uptime:
9 days 1 hour 4 minutes
Software Updates:
no new recommended updates detected
Platform:
VMware
Packet Rate
Packets per second
Throughput
Kbits per second [Kbps]

3.6 F5

Aruba 部分配置如下图所示

注意参数需与 F5 中保持一致

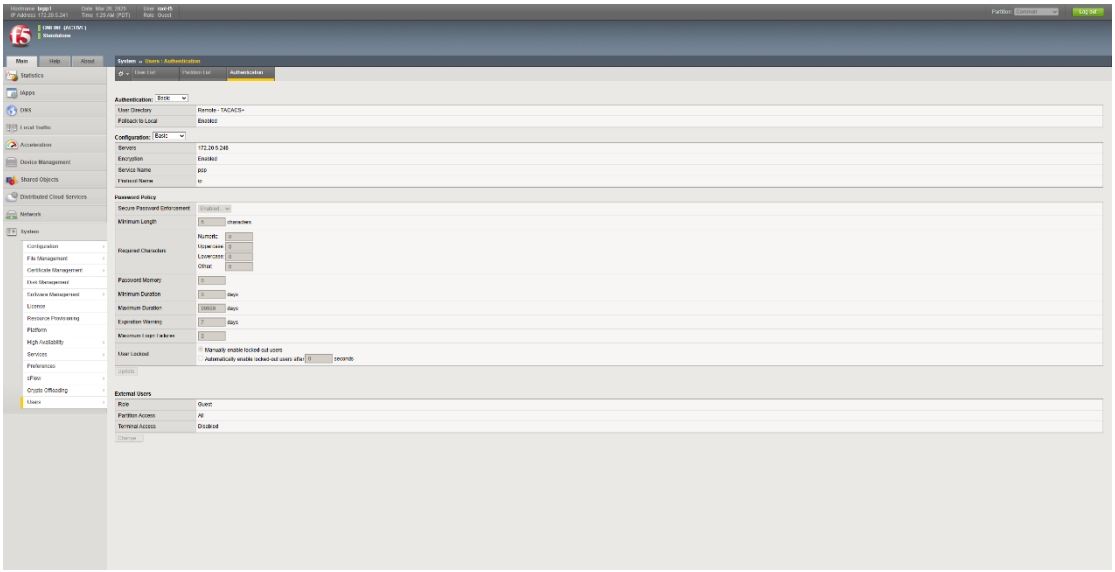




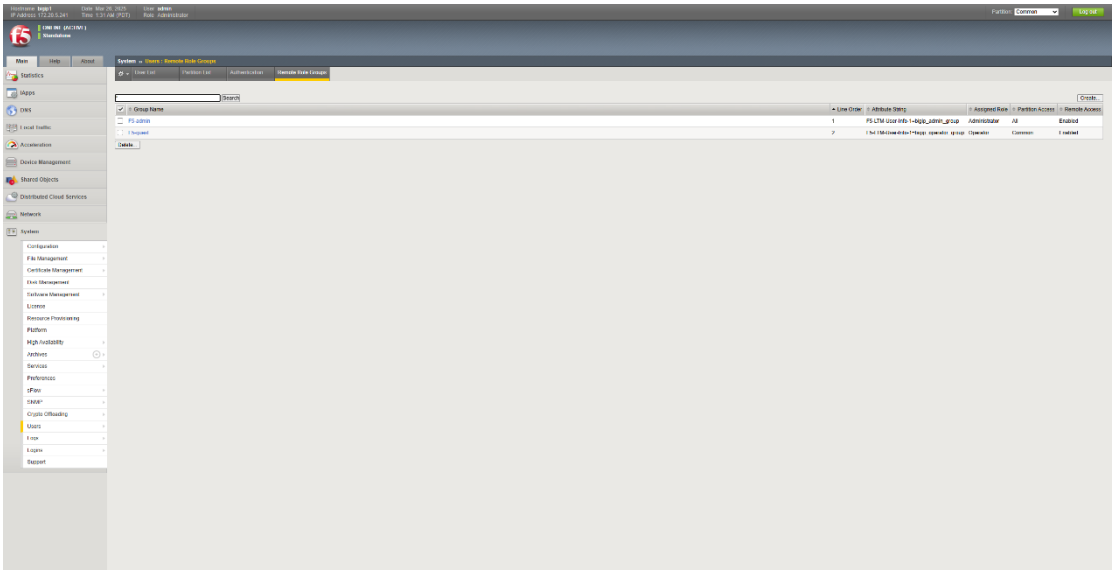
其余用户创建与策略/服务配置参考思科部分

F5 部分配置如下所示

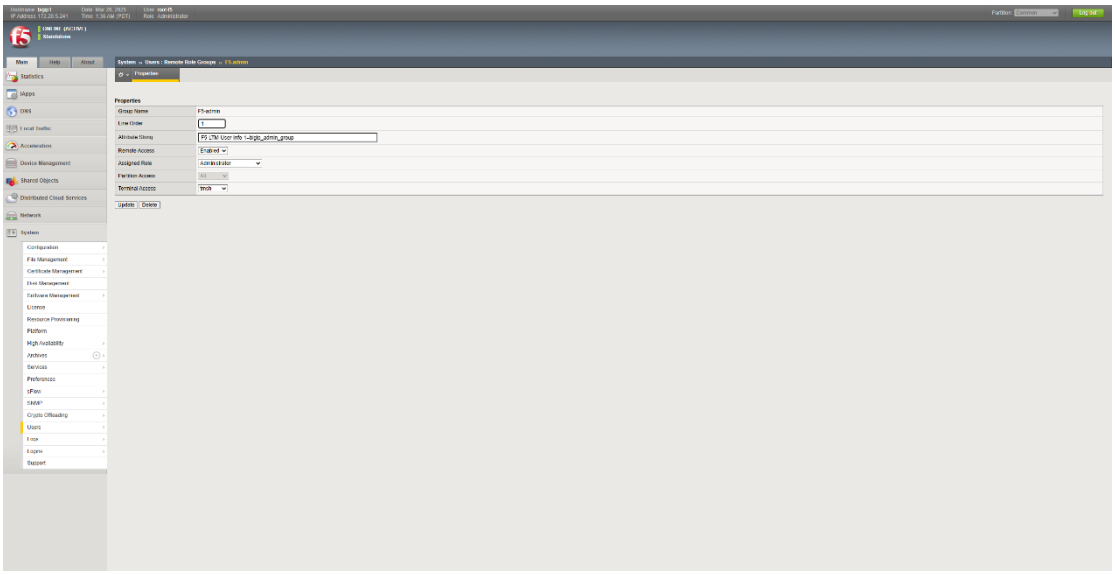
进入 System-user 中启用 Tacacs 服务并添加对应的 CPPM IP 地址



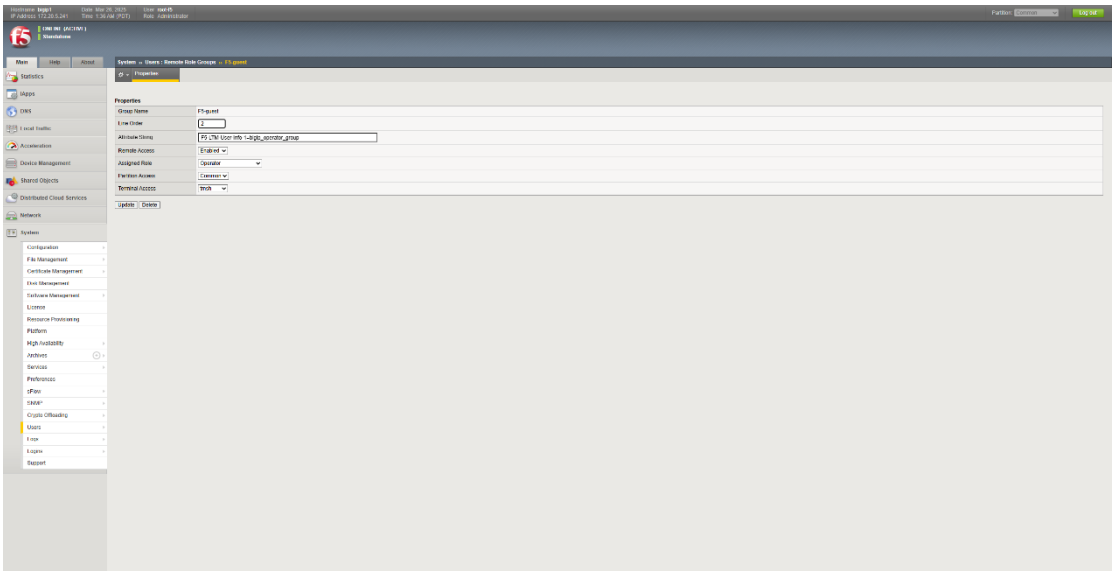
创建 admin 与 readonly 用户组



Admin 部分参数为 F5 LTM USER info 1-bigip_admin_group



Readonly 部分参数为 F5 LTM USER info 1-bigip_operator_group

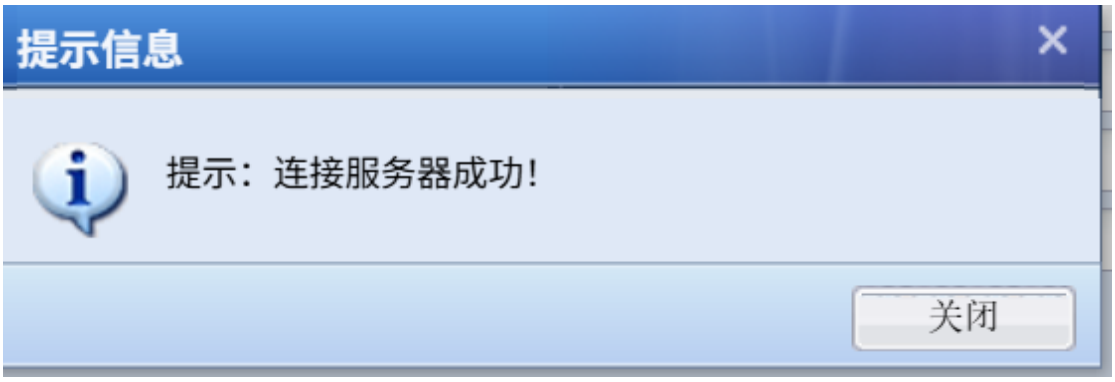


3.7 深信服

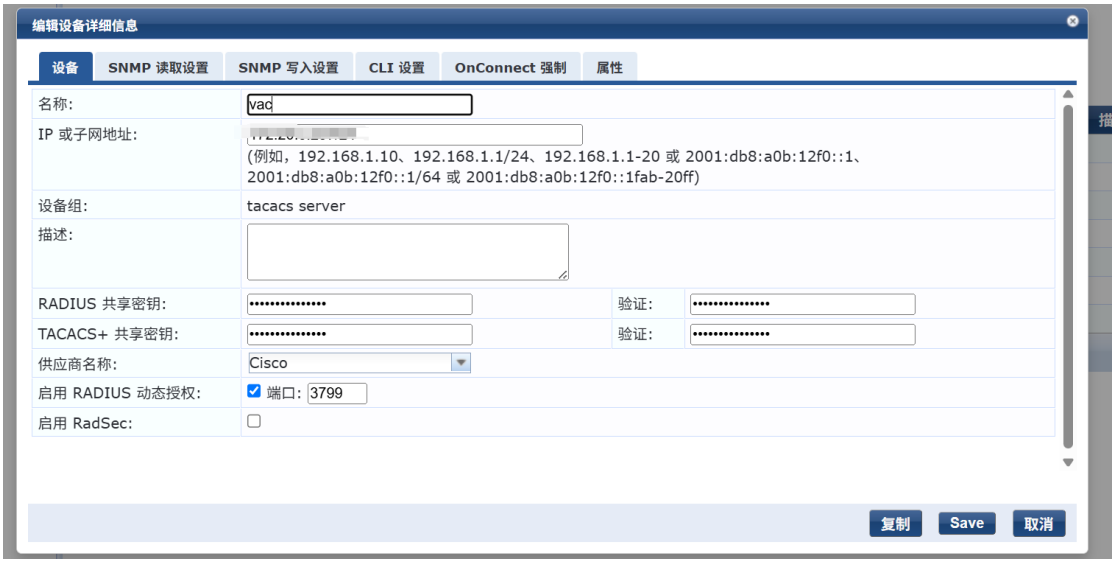
深信服侧配置较简单，选择管理员账号-第三方认证服务器管理

输入对接的 CPPM 地址与密码

点击测试有效性测试连通性

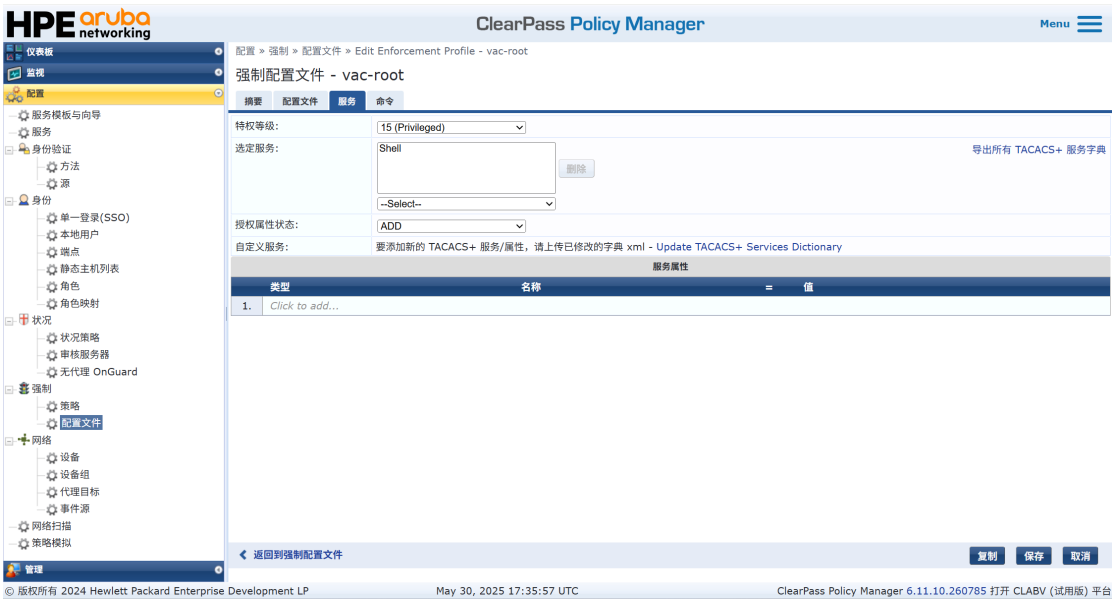


CPPM 侧配置对应 IP，注意供应商没有深信服，随便选即可

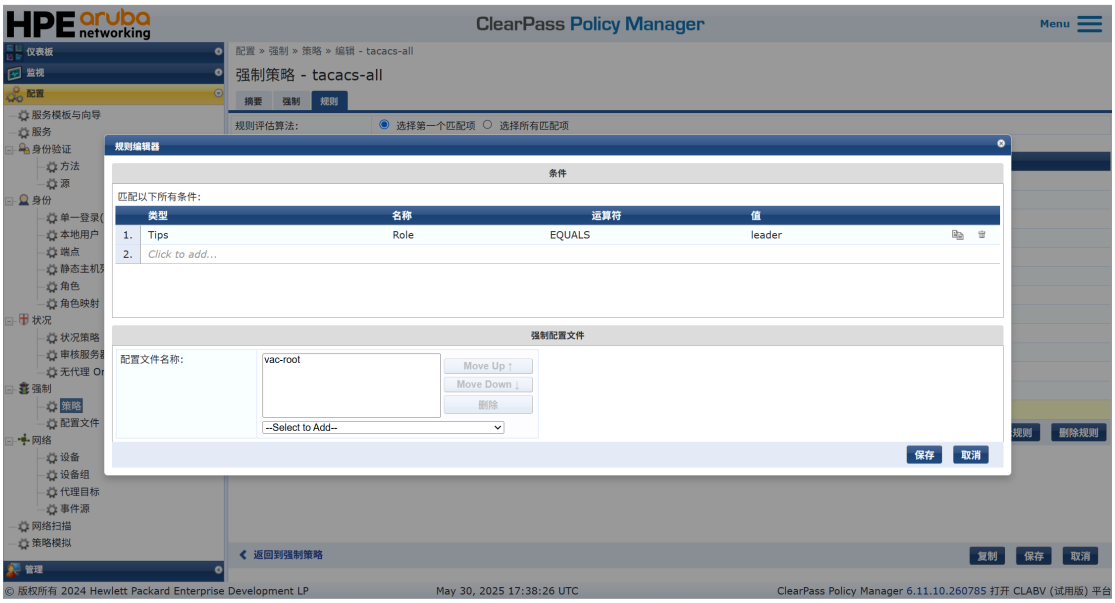


本地用户创建

配置文件中无需做特殊配置，指定为权限 15 即可，read 与 root 权限均指定 15，详细权限分配由深信服侧执行。

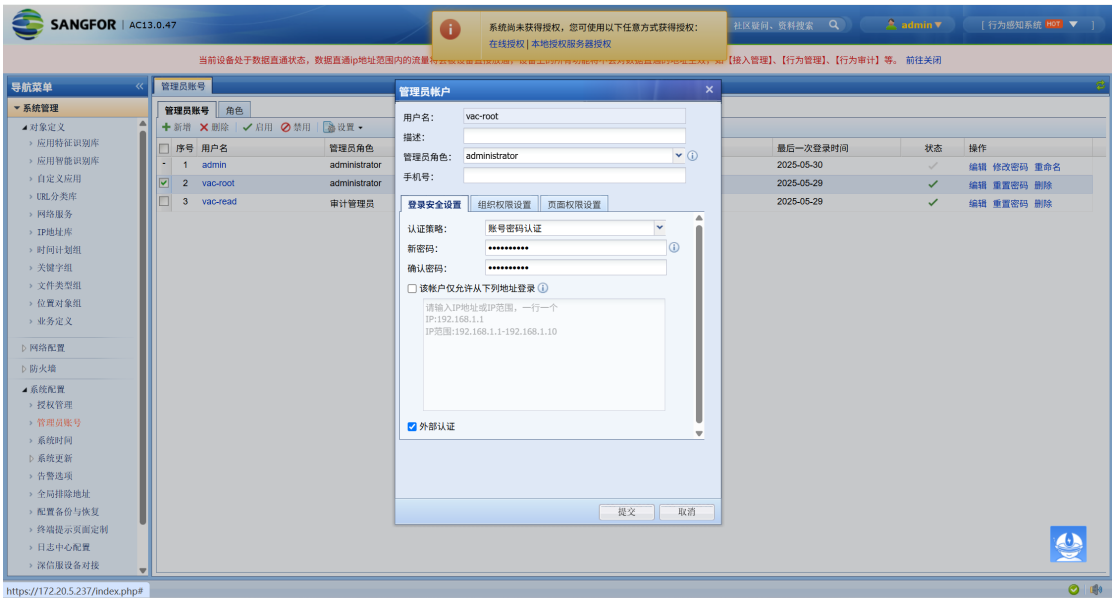


强制策略中添加相关用户及配置绑定

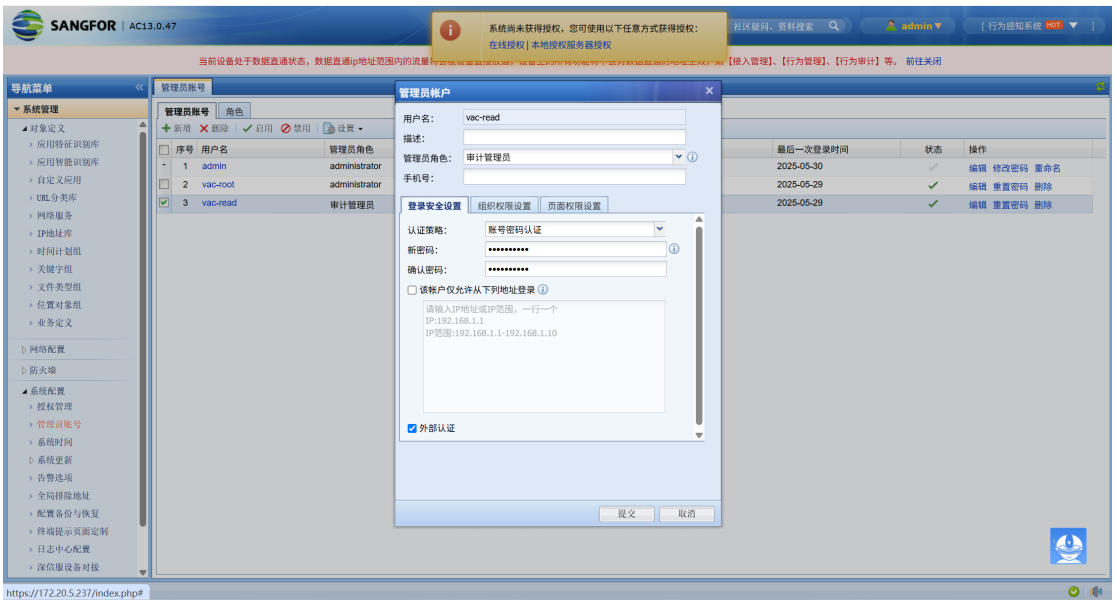


其余用户创建与策略/服务配置参考思科部分

深信服侧新建与 CPPM 侧相同用户并勾选外部认证，切记密码要与 CPPM 不一致



Read 角色设定为审计管理员

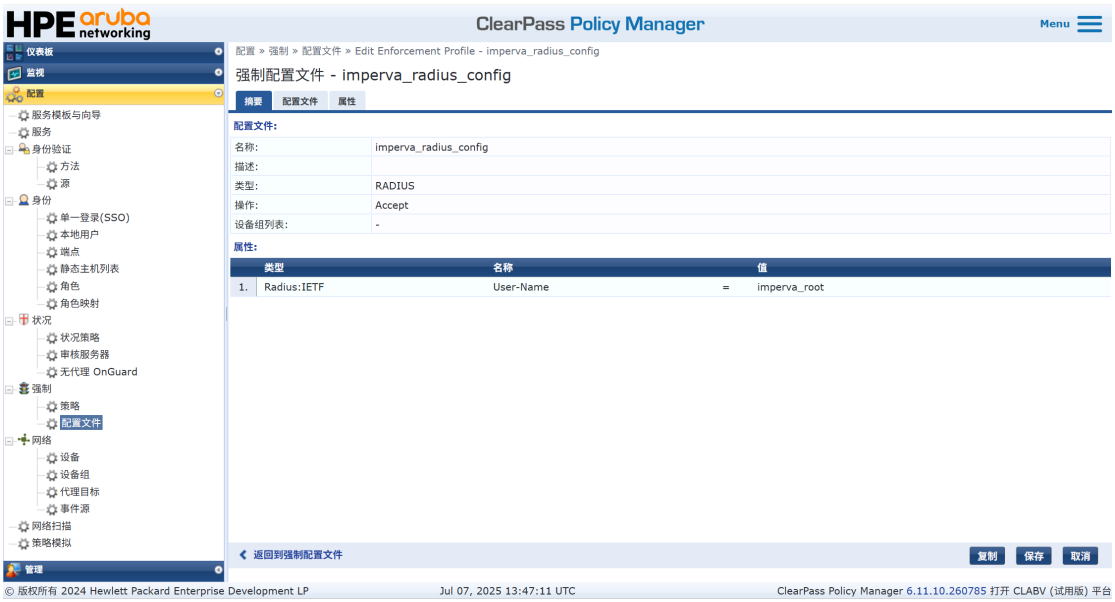


3.8 Imperva

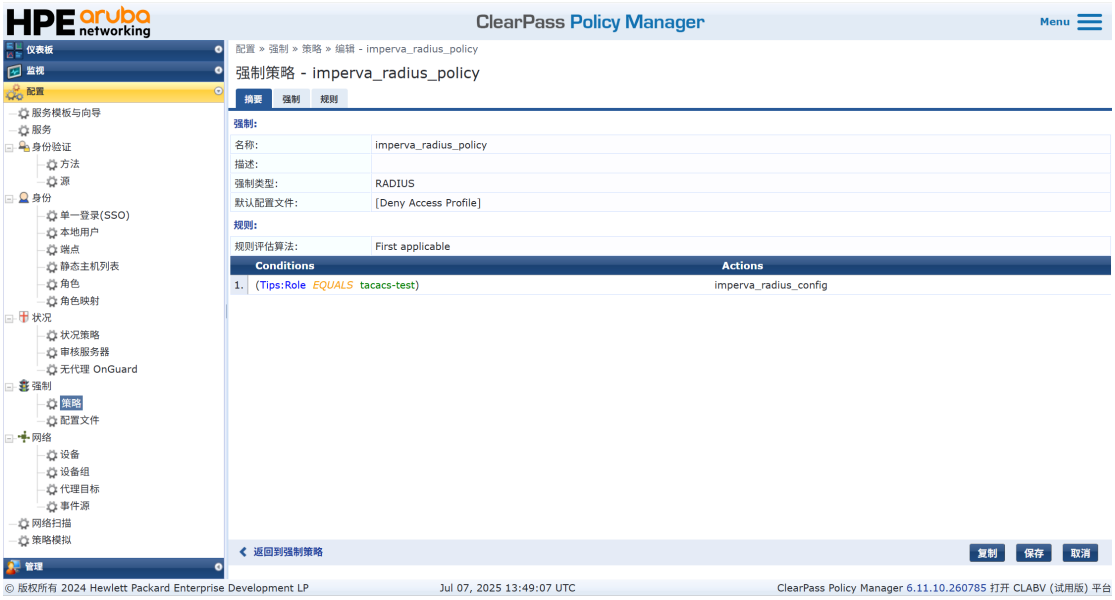
Imperva 部分无法支持 tacacs 服务，只能改为 radius

CPPM 部分配置如下，用户创建等参考基础配置，此处略

强制配置文件如下，下方参数值任意填写，不影响认证流程



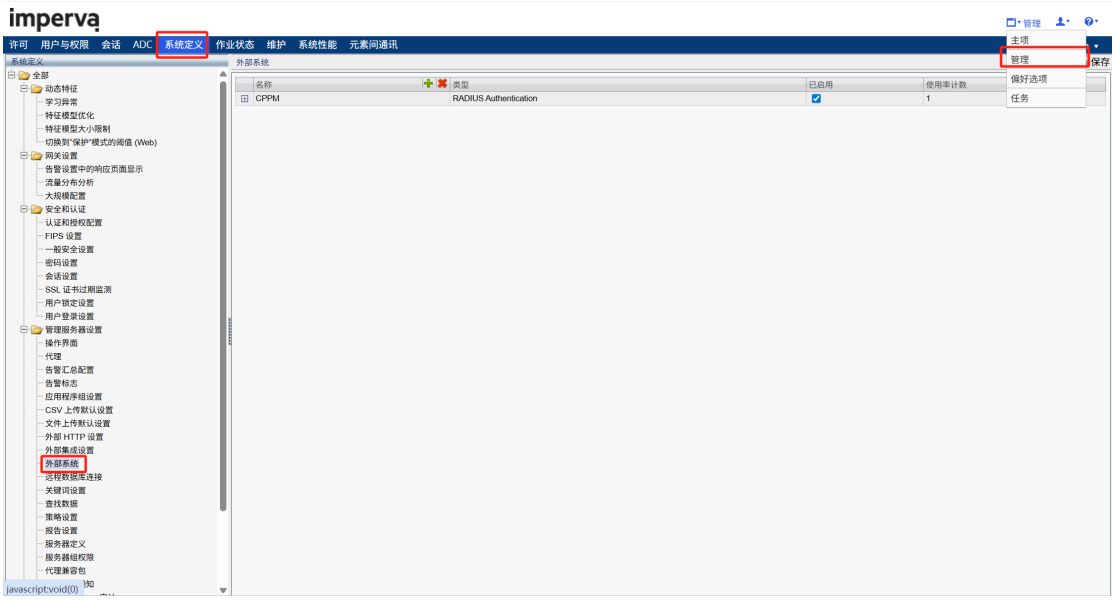
强制策略如下



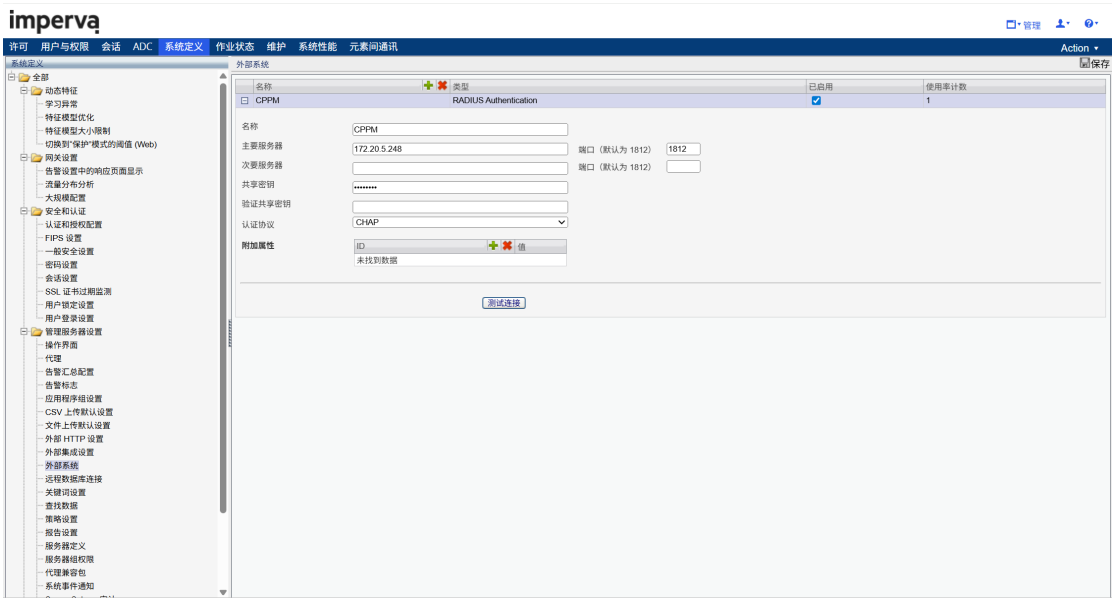
服务部分如下，注意类型需要指定为 radius，另外身份验证部分，认证方式需要与 imperva 相匹配

Imperva 部分配置

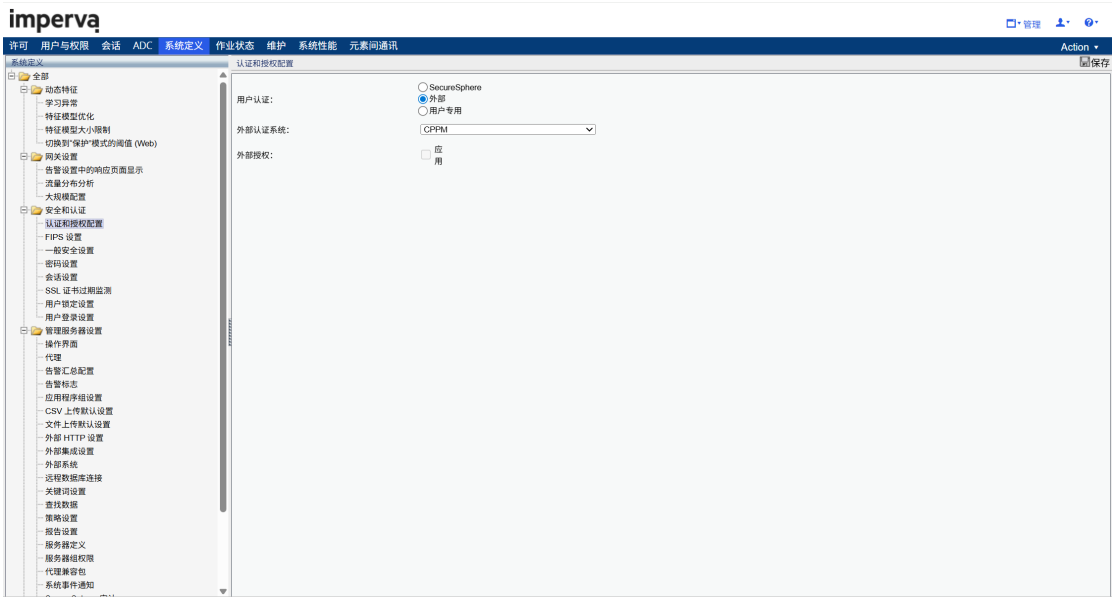
注意，需要先切换到管理部分，默认主页无相关配置内容



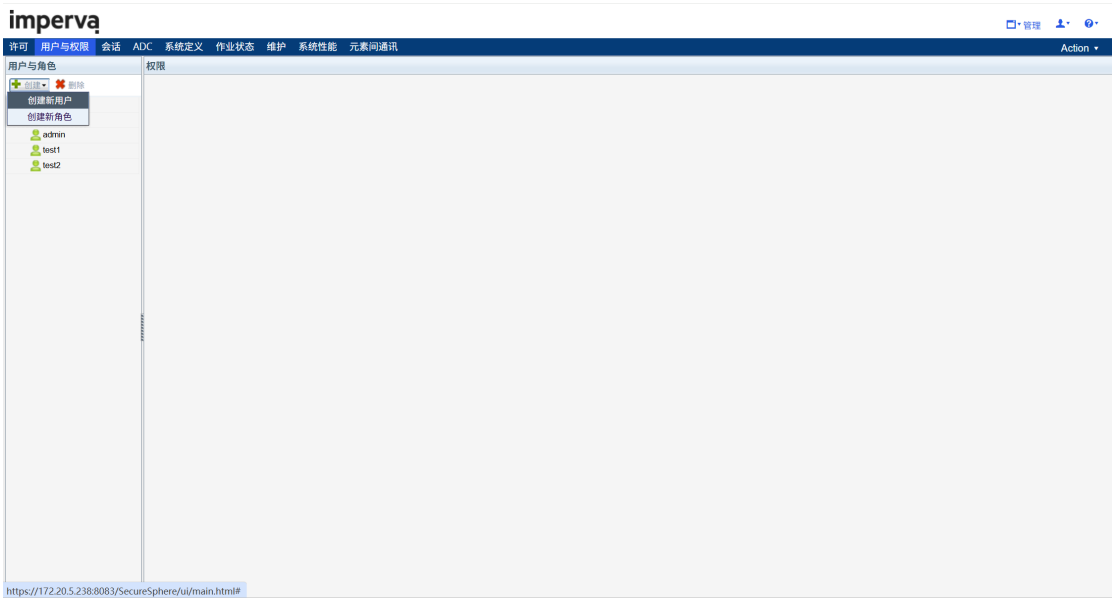
新建 radius 外部服务器，注意认证方式，CPPM 侧服务需要与其相同



认证和授权配置部分切换用户到外部认证



切换到用户与授权，选择创建新用户



由于前面选择了外部认证，这里默认用户认证来源外部，权限按需分配，同时该用户需与 CPPM 内创建用户一致