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

fox210317@sina.com

需求：

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

实现思路：

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

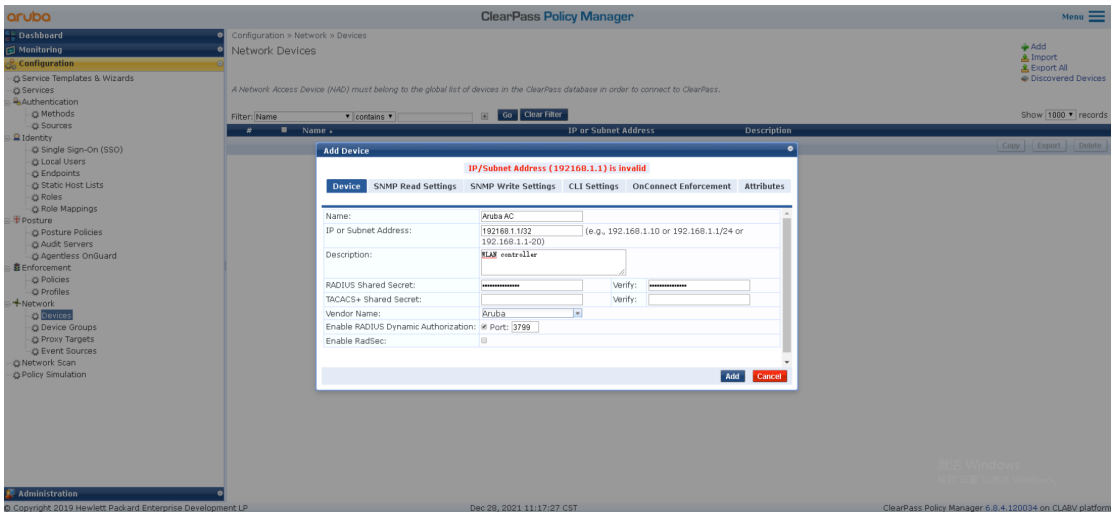
1. ClearPass 中添加 Devices

配置路径：

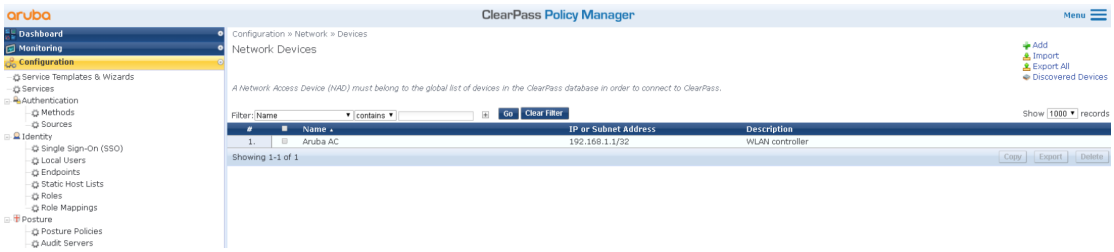
configuration -Network -Devices -Add

说明：

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



添加完成如下：



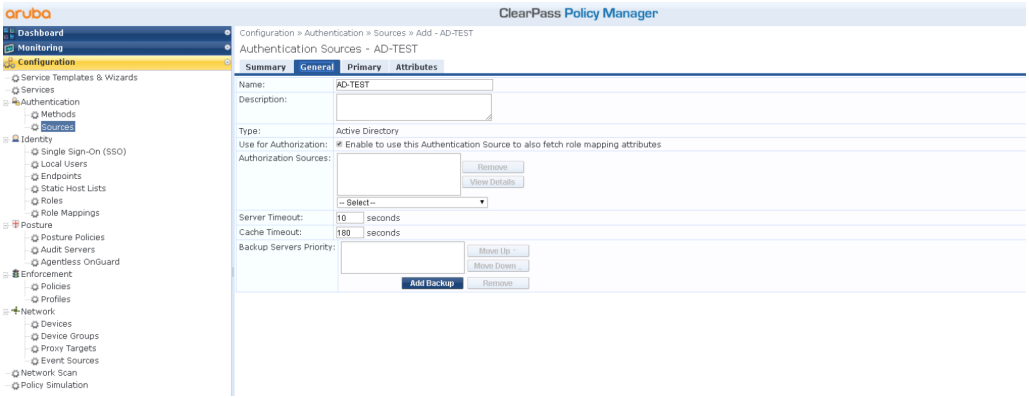
2. 创建 Authentication Sources

配置路径：

Configuration -Authentication -Sources -Add

说明：

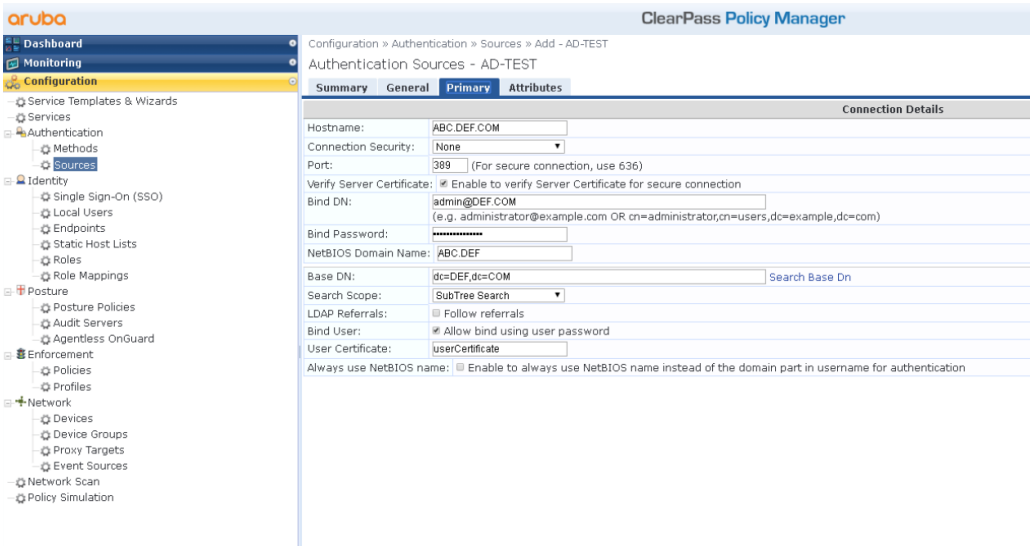
- **Name**：填写设备名称或自己方便记忆的标识
- **Description**：填写描述/备注信息
- **Type**：选择 Active Directory
- **Use for Authorization:**勾选（Enable to use this Authentication Source to also fetch role mapping attributes）
- **Authorization Sources**:如果有除了当前 AD 以外的其他 Authorization Sources，可以填写，反之则无
- **Server Timeout**：10s
-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



2.1. AD 域控服务器信息

说明：

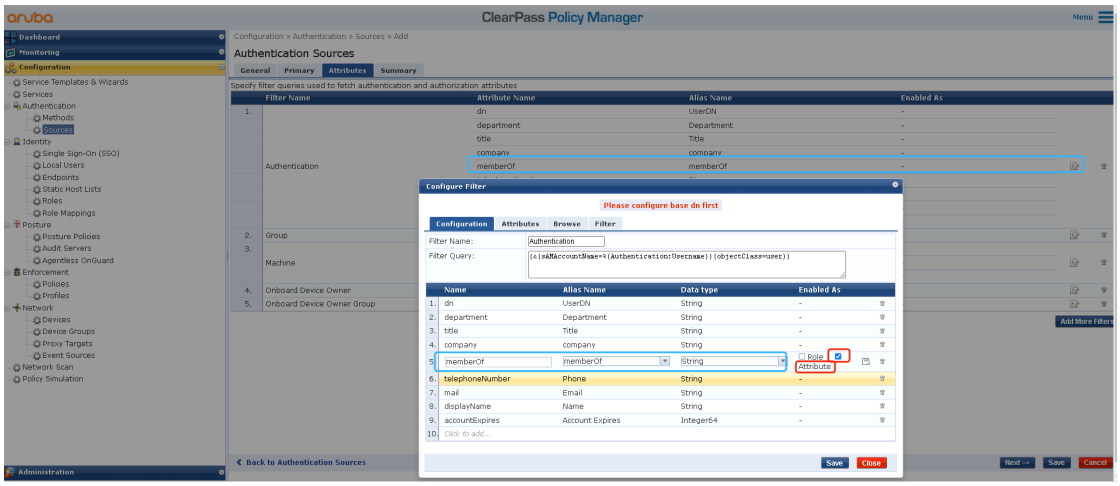
- 在填写完 Bind DN 与 Bind Password 后，可以点右侧 Search Base Dn，如果可以检索出 OU，则填写的信息可以使用。
- 其他参数保持默认即可
- **SAVE**



2.2. Authentication Sources -AD Attributes

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

SAVE



3. Profile 配置

3.1. Return Aruba-User-Role Profile 配置

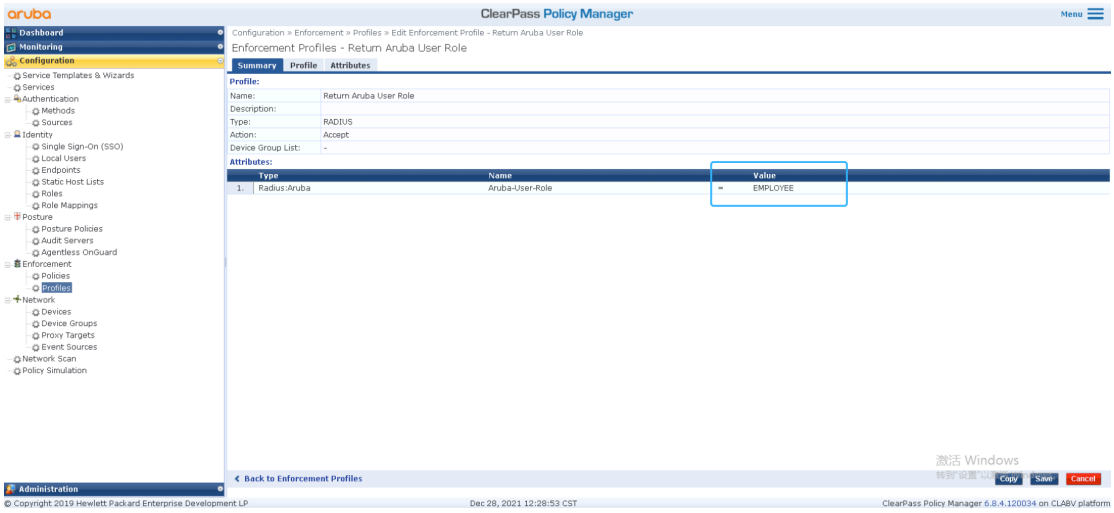
配置路径：

Configuration -Enforcement -Profiles -Add

参数配置：

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

SAVE



3.2. Enforcement Profiles – Device Count Profile 配置

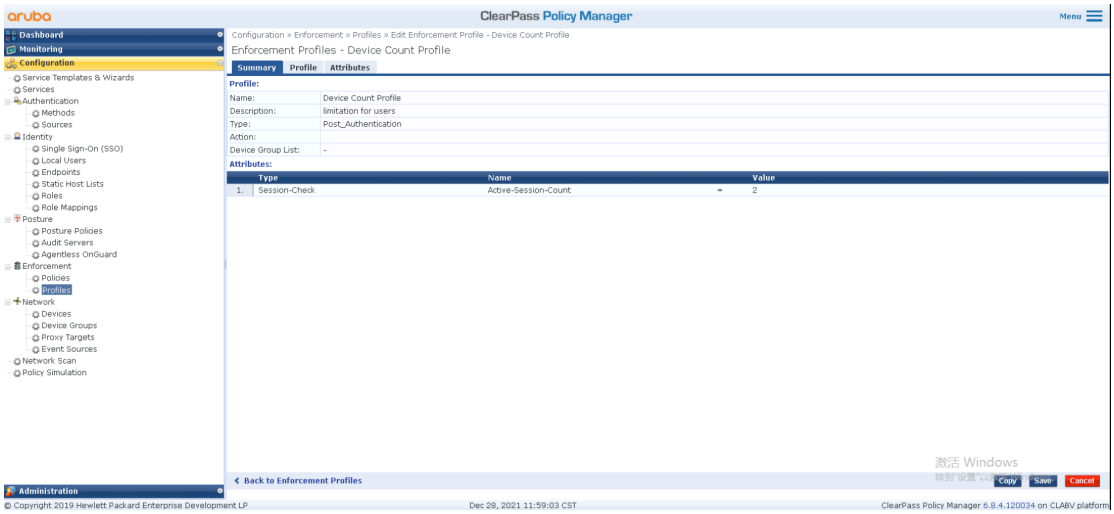
配置路径：

Configuration -Enforcement -Profiles -Add

参数配置：

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

SAVE



TIPs:

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

4. Policies 配置

配置路径：

Configuration -Enforcement -Policies -Add

参数配置：

- **Enforcement**:
  - **Name**: ARUBA-WLAN-802.1X
  - **Description**:
  - **Enforcement Type**: 勾选 RADIUS
  - **Default Profile**: OTHER DENY
- **Rules**:（同理写 rule 1-3）
  - **Rules Evaluation Algorithm**: Select first match
  - **Enforcement Policy Rules**:

    1、 Type：Authorization: GM-AD、Name：UserDN、Operator：CONTAINS、VALUE: OU=MOS,DC=MOS,DC=COM

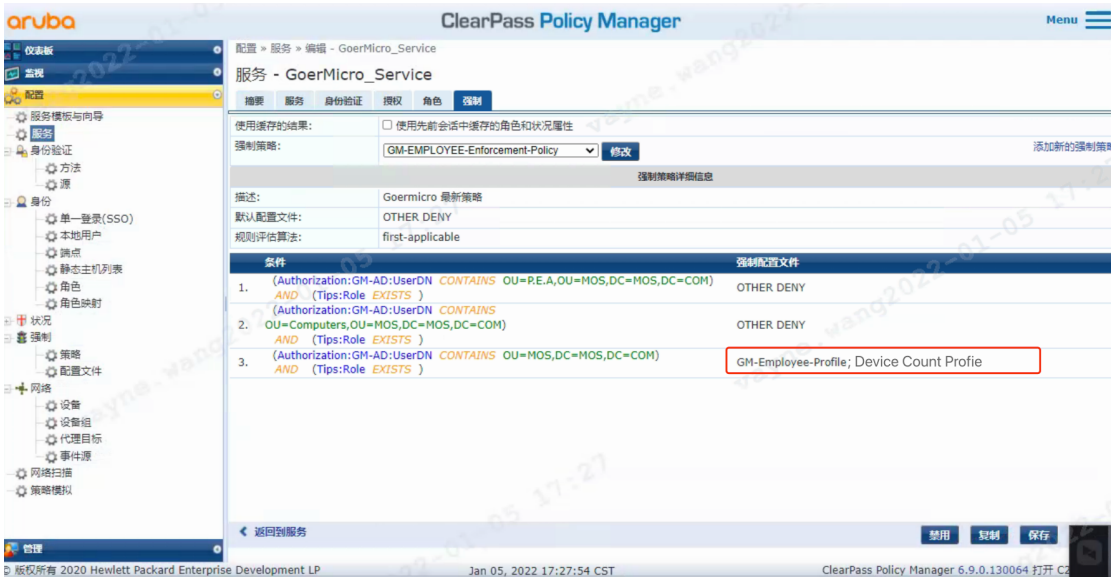
    2、 Type：Tips、Name：Role、Operator：EXISTS

    3、 Enforcement Profiles（调用 3.1、3.2）：

    3.1. Return Aruba User Role

    3.2. Device Count Profile

    4、 SAVE



5. Services 配置

配置路径：

Configuration -Services -Add

参数模板关联配置：

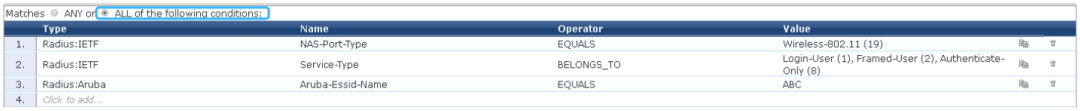
- **Service**：

  Type: Aruba 802.1X Wireless

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

  Description: Aruba 802.1X Wireless Access Service

  Service Rule:



- **Authentication**:

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

- **Authorization:**

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

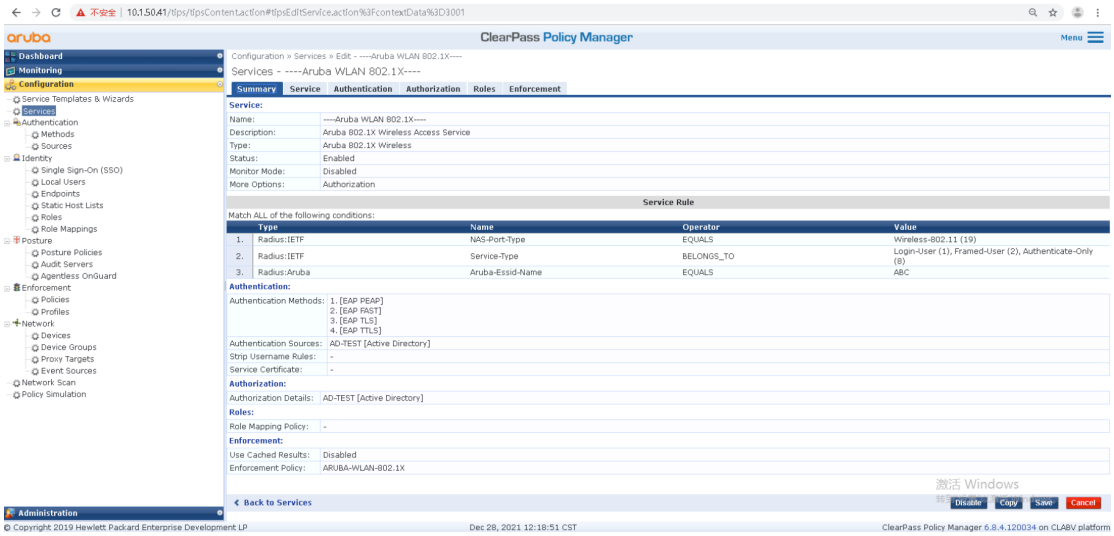
  GM-AD [Active Dictory]

- **Roles**：空
- **Enforcement**:

  Enforcement Policy: “ARUBA-WLAN-802.1X”

- **SAVE**

  下图为实验环境模拟，请忽略 AD-TEST（同 GM-AD）



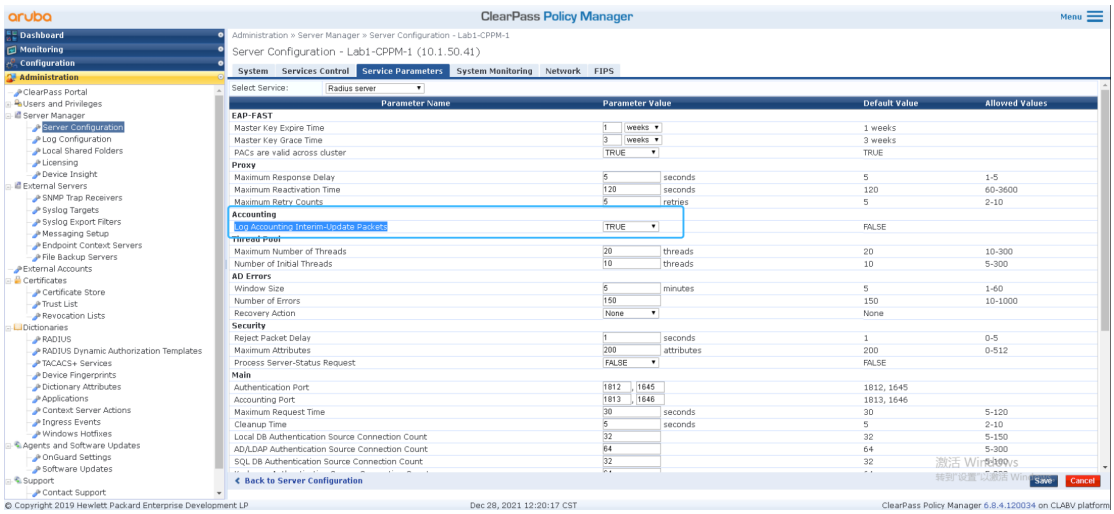
6. ClearPass 开启 RADIUS ACCOUNTING

配置路径：

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

Select Service : RADIUS SERVER

Accounting Log Accounting Interim-Update Packets : **TRUE**



7. 无线控制器开启 ACCOUNTING

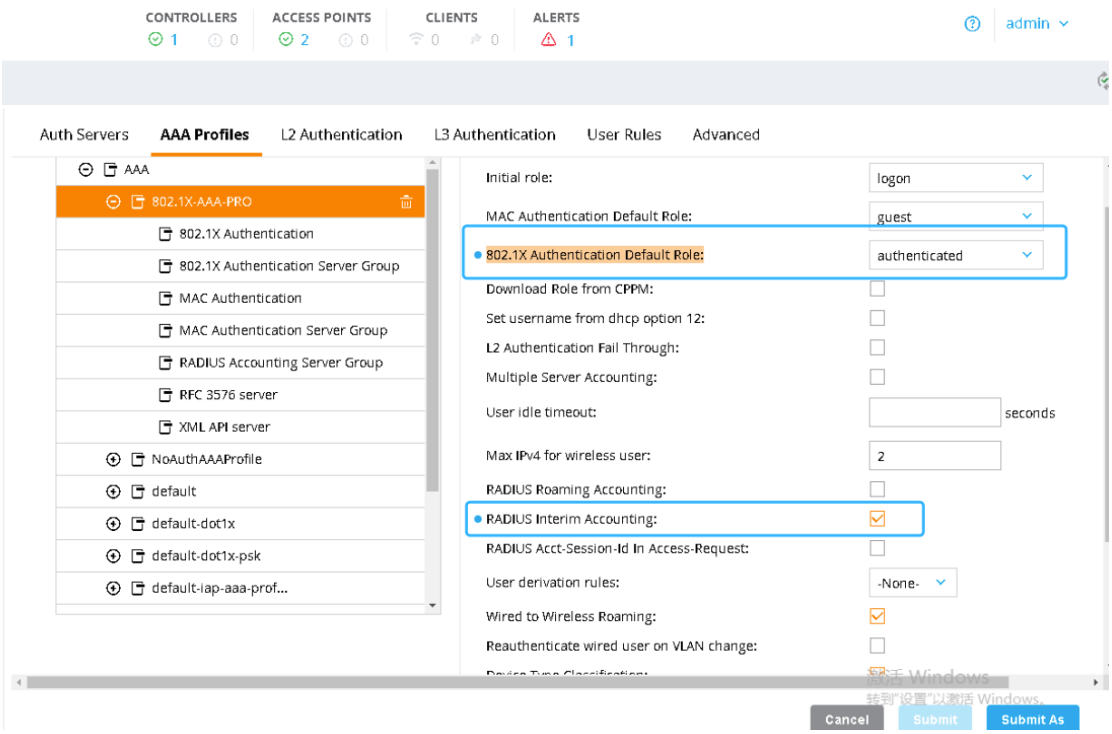
7.1. 修改 802.1x authentication default role & 开启 Accounting

说明：

在 ClearPass 通过 VSA（Return User Role 的方式）返回给 Aruba 无线控制器 user-role 时，此处 AAA Profile 写的 802.1X Authentication Default Role 为 authenticated 会被 ClearPass 返回的 EMPLOYEE 覆盖

Role Derivation Sequence：

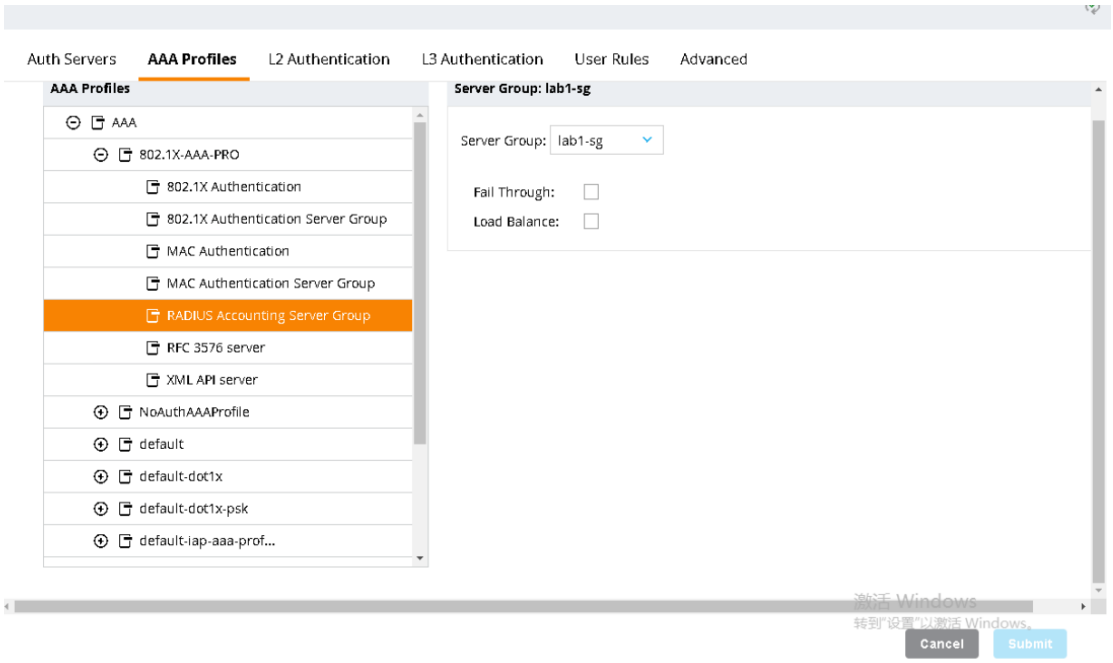
VSA > SDR > UDR > Default Role.



7.2. AAA Profile 调用 RADIUS ACCOUNTING SERVER-GROUP

说明：

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



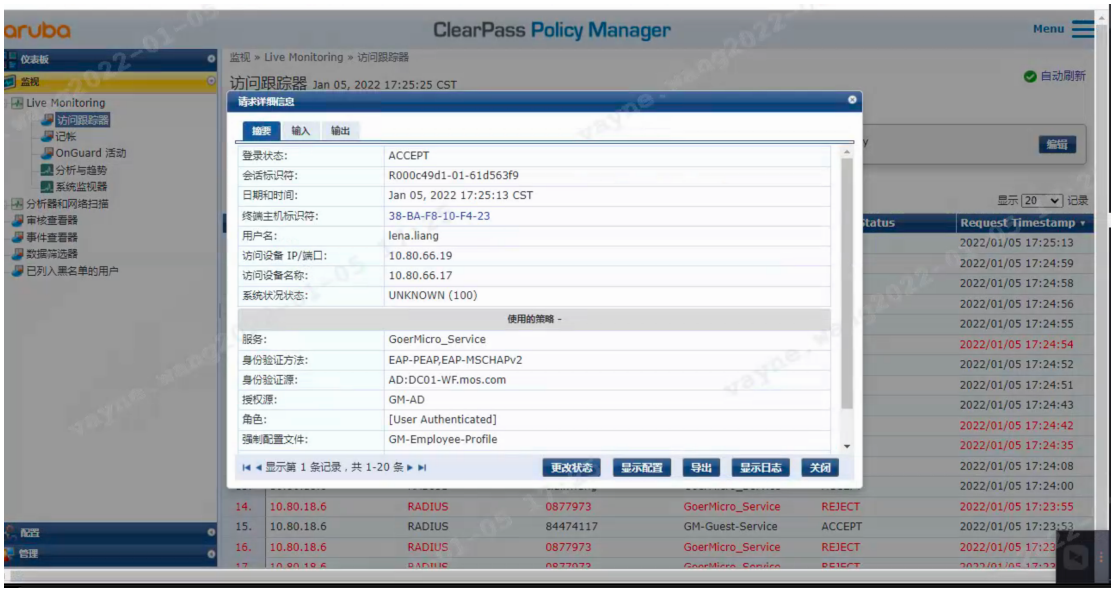
8. 测试验证-1

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

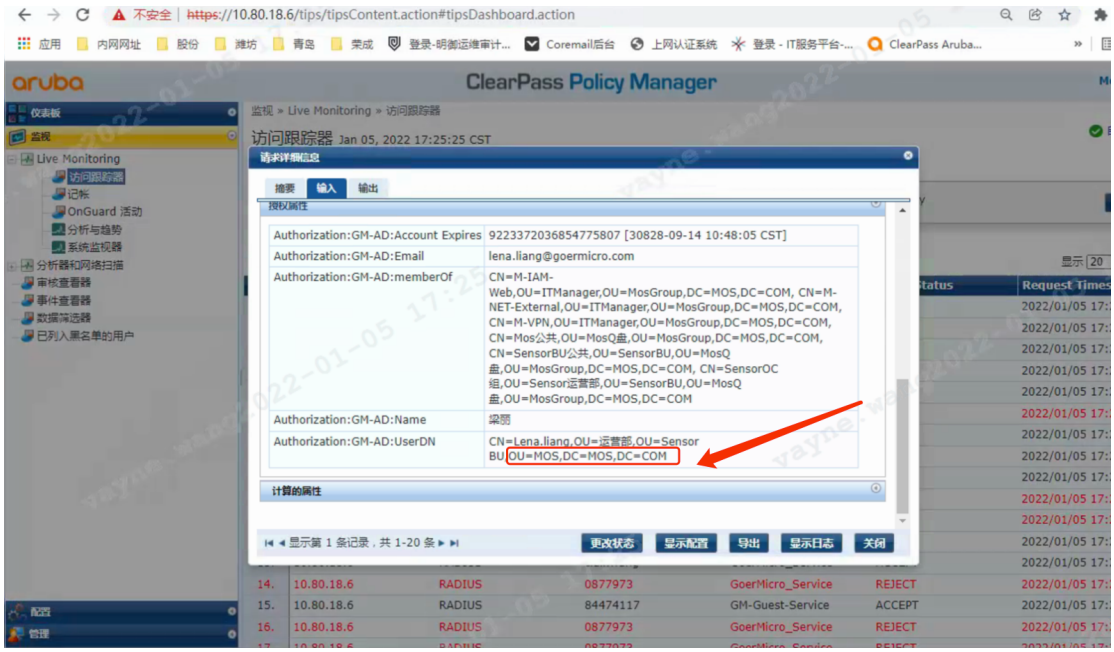
测试结果：在 ClearPass Tracker 中查看日志信息

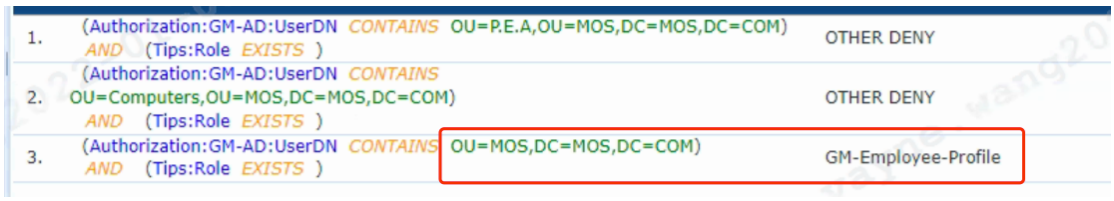
测试结果说明：

Summary -Status：AUTHEN_STATUS_PASS 成功通过认证（ACCEPT）



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





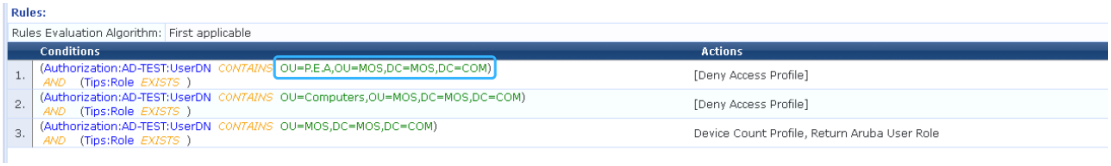
9. 测试验证-2

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

测试结果：在 ClearPass Tracker 中查看日志信息

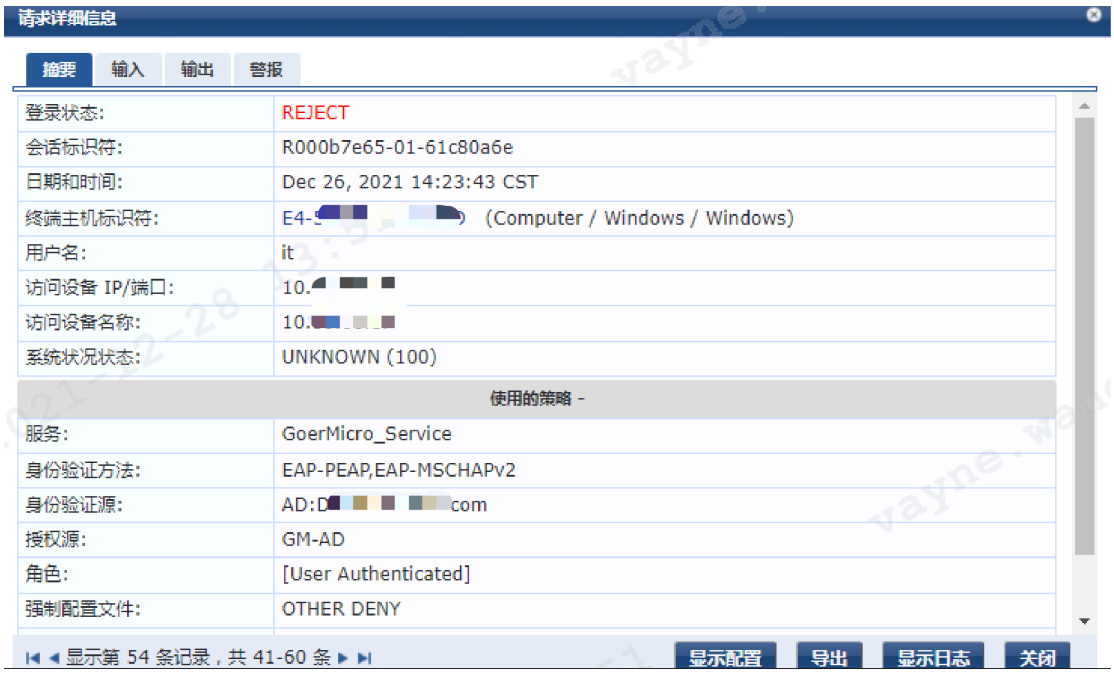
测试结果说明：

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



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

- 登陆状态：REJECT
  强制配置文件： "OTHER DENY"



RADIUS 请求

授权属性

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

9.2. 使用非 AD 内的设备登陆

配置文件为 OTHER DENY

请求详细信息

摘要 输入 输出 警报

日期和时间:	Jan 05, 2022 17:30:44 CST
终端主机标识符:	B2-2、 _2
用户名:	@goermicro.com
访问设备 IP/端口:	10
访问设备名称:	10、 .7
系统状况状态:	UNKNOWN (100)
使用的策略 -	
服务:	GoerMicro_Service
身份验证方法:	EAP
身份验证源:	None
授权源:	GM-AD
角色:	-
强制配置文件:	OTHER DENY
服务监视器模式:	Disabled
在线状态:	不可用

显示第 2 条记录，共 1-20 条

显示配置 导出 显示日志 关闭

Authorization：GM-AD：UserDN 为空