

# H3C 交换机通过 TACACS+对接 Aruba ClearPass 认证

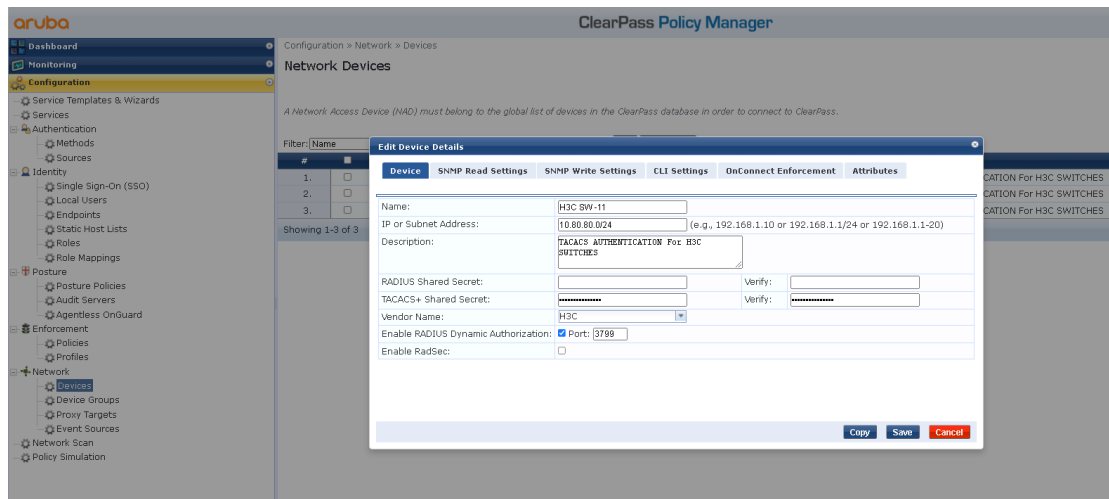
## 1. ClearPass 中添加 Devices

配置路径：

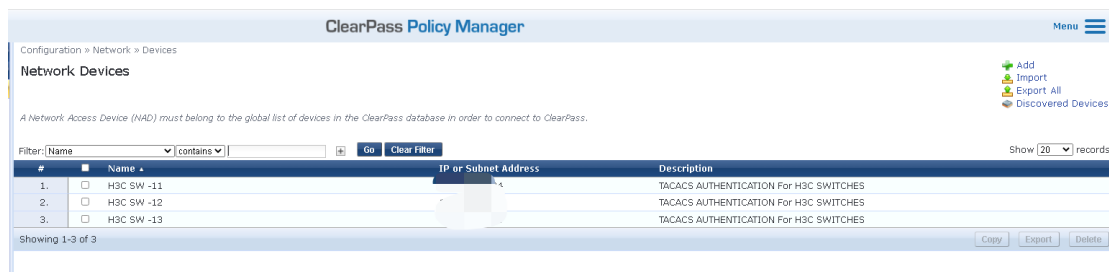
configuration -Network -Devices -Add

说明：

- **Name**：填写设备名称或自己方便记忆的标识
- **IP or Subnet Address**:填写 H3C 交换机的 IP，如有多台可多次添加或添加一个网段
- **TACACS+ Shared Secret**：需要在 H3C 交换机和 ClearPass 保持一致的密钥
- **Vendor Name**：选择 H3C
- **Enable RADIUS Dynamic Authorization**：开启
- **SAVE**



添加完成如下：



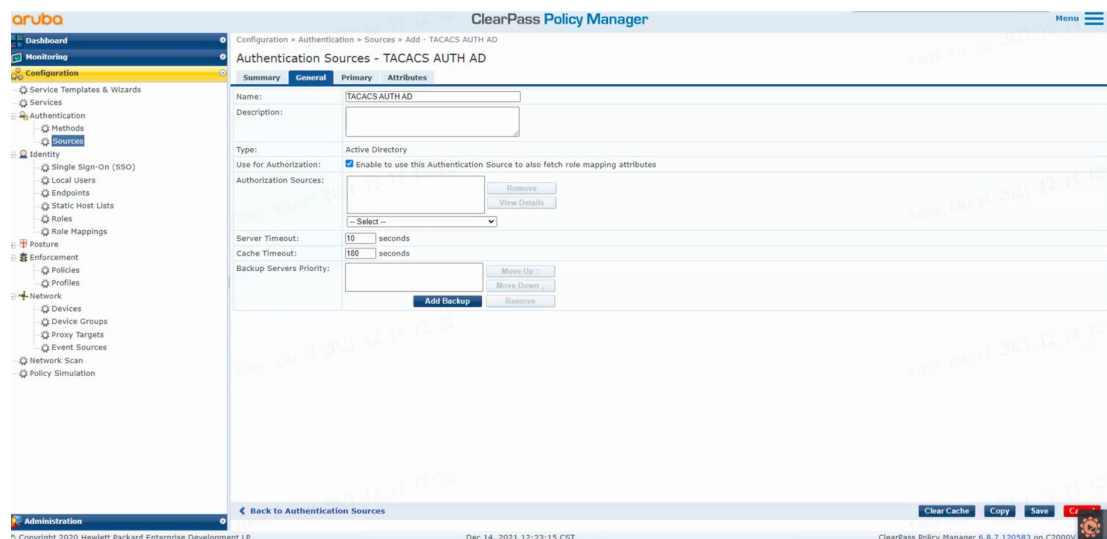
## 2. 创建 Authentication Sources

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，可以点击右侧 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**

The screenshot shows the 'Authentication Sources - TACACS AUTH AD' configuration page in the ClearPass Policy Manager. The page is divided into several sections: Summary, General, Primary, and Attributes. The Primary section is currently active and displays the following configuration details:

Connection Details	
Hostname:	M
Connection Security:	None
Port:	389 (For secure connection, use 636)
Verify Server Certificate:	<input checked="" type="checkbox"/> Enable to verify Server Certificate for secure connection
Bind DN:	(e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)
Bind Password:	*****
NetBIOS Domain Name:	MOS
Base DN:	Search Base Dn
Search Scope:	SubTree Search
LDAP Referrals:	<input type="checkbox"/> Follow referrals
Bind User:	<input checked="" type="checkbox"/> Allow bind using user password
User Certificate:	userCertificate
Always use NetBIOS name:	<input type="checkbox"/> Enable to always use NetBIOS name instead of the domain part in username for authentication

## 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 Role Mapping 使用

SAVE

Configuration > Authentication > Sources > Add

Authentication Sources

Specify filter queries used to fetch authentication and authorization attributes

Filter Name	Attribute Name	Alias Name	Enabled As
1. Authentication	dn	UserDN	-
	department	Department	-
	title	Title	-
	company	company	-
	memberOf	memberOf	Attribute
2. Group	cn	Groups	-
3. Machine	operatingSystem	OperatingSystem	-
4. Onboard Device Owner	memberOf	Onboard memberOf	-
5. Onboard Device Owner Group	cn	Onboard Groups	-

Configure Filter

Please configure base dn first

Configuration Attributes Browse Filter

Filter Name: Authentication

Filter Query: (&(!AccountType=\*) (AuthenticationBaseDn)) (objectClass=users)

Name	Alias Name	Data type	Enabled As
1. dn	UserDN	String	-
2. department	Department	String	-
3. title	Title	String	-
4. company	company	String	-
5. memberOf	memberOf	String	Attribute
6. telephoneNumber	Phone	String	-
7. mail	Email	String	-
8. displayName	Name	String	-
9. accountExpires	Account Expires	Integer4	-
10.			

Save Close

Configuration > Authentication > Sources > Add - TACACS AUTH AD

Authentication Sources - TACACS AUTH AD

Summary General Primary Attributes

Specify filter queries used to fetch authentication and authorization attributes

Filter Name	Attribute Name	Alias Name	Enabled As
1. Authentication	dn	UserDN	-
	department	Department	-
	title	Title	-
	company	company	-
	memberOf	memberOf	Attribute
	telephoneNumber	Phone	-
	mail	Email	-
	displayName	Name	-
	accountExpires	Account Expires	-
	2. Group	cn	Groups
3. Machine	dnsHostName	HostName	-
	operatingSystem	OperatingSystem	-
4. Onboard Device Owner	memberOf	Onboard memberOf	-
5. Onboard Device Owner Group	cn	Onboard Groups	-

Clear Cache Copy Save

### 3. 创建 ClearPass Role

配置路径：

Configuration -Identity -Roles -Add

说明：

ClearPass Role 用于标识一类用户（通过一些特定的属性、条件等区分）

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation options like Dashboard, Monitoring, and Configuration. The main area is titled 'Roles' and shows a list of existing roles. An 'Edit Role' dialog box is open, showing fields for Role ID (3008), Name (SWADMIN), and Description (SW Access). The dialog has 'Save' and 'Cancel' buttons.

#	Name	Description
1.	[AirGroup v1]	Role for an AirGroup protocol version 1 request
2.	[AirGroup v2]	Role for an AirGroup protocol version 2 request
3.	[Aruba TACACS read-only Admin]	Default role for read-only access to Aruba devices
4.	[Aruba TACACS root Admin]	Default role for root access to Aruba devices
5.	[BYOD Operator]	
6.	[Contractor]	
7.	[Device Registration]	
8.	[E-Device]	
9.	[E-Device]	
10.	[E-Device]	
11.	[E-Device]	
12.	[E-Device]	
13.	[E-Device]	
14.	[E-Device]	
15.	[E-Device]	Default role applied during MAC caching
16.	[E-Device]	GT-EMT
17.	[E-Device]	Role for an Android device being provisioned
18.	[Onboard Chromebook]	Role for Chromebook device being provisioned
19.	[Onboard iOS]	Role for an iOS device being provisioned
20.	[Onboard Linux]	Role for Linux device being provisioned
21.	[Onboard macOS]	Role for a macOS device being provisioned
22.	[Onboard Windows]	Role for a Windows device being provisioned

## 4. Role Mapping 配置

配置路径：

Configuration - Identity - Role Mappings - Add

Mapping Rules 配置参数：

Rules Evaluation Algorithm: select first match 评估算法，从头开始

- **Role Mapping Rules:**

**Type** : “ Authorization: TACACS AUTH AD”

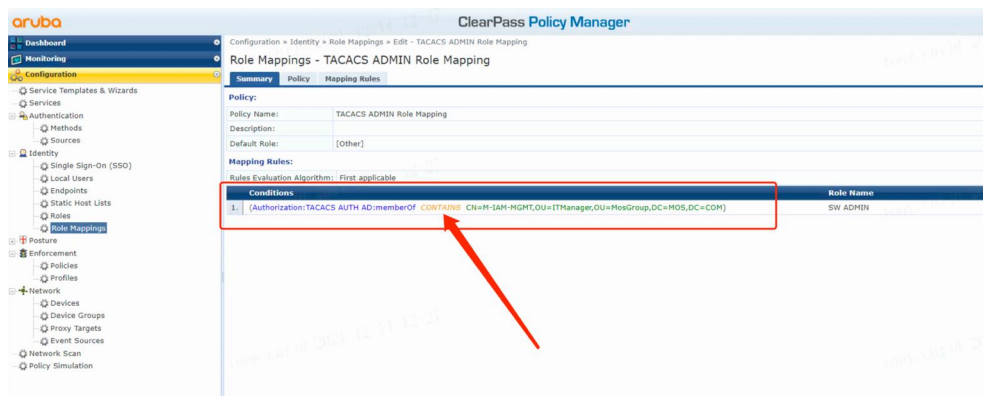
**Name** : “memberOf” 此项参数用于匹配 AD 中特定的部门属性，仅对一类人评估为” SW ADMIN”

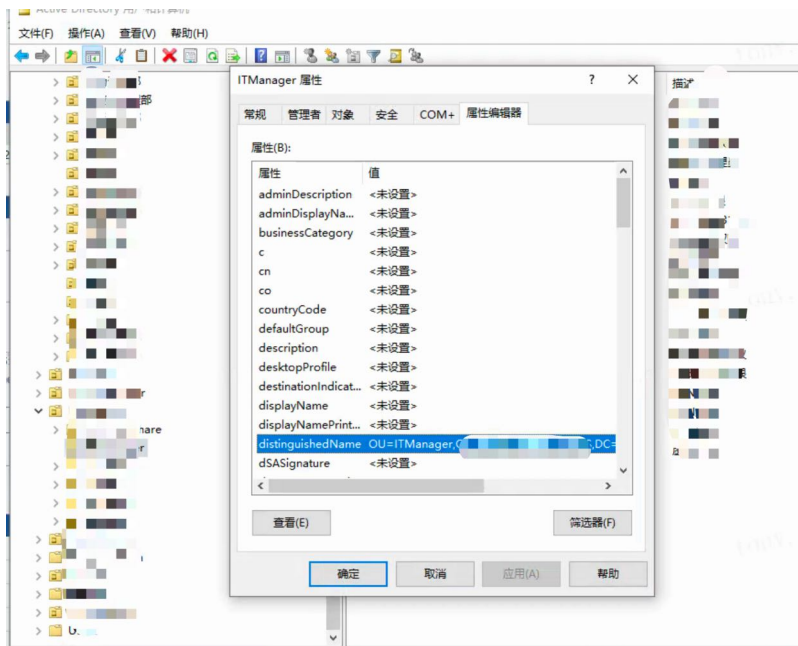
**Operator** : CONTAINS ; 此项参数用于计算公式包含此项属性值，

TIPs : AD 中通过 OU 查询出一个用户的属性，会包含很多属性，因此在此处需要写为 CONTAINS

**Value** : CN=M-IAM-MGMT,OU=ITManager,OU=MosGroup,DC=MOS,DC=COM 此项参数需在 AD 中查找，如下图二

- **SAVE**







## 5. Profile 配置

配置路径：

Configuration - Enforcement - Profiles - Add

参数配置：

- **Template:** TACACS+ Based Enforcement
- **Name:** 填写设备名称或自己方便记忆的标识
- **Description:** 描述/备注
- **Action :** Accept
- **Selected Services:** SHELL
- **Authorize Attribute Status:** ADD
- **Service Attributes:** (此两条 rule 用于返回给 H3C 交换机，因此 network-admin 仅被 H3C 交换机识别)

Type : SHELL、 Name : roels、 Value : network-admin (value 小写)

Type : SHELL、 Name : priv-lvl、 Value : 15

- **Commands :**

Service Type : Shell

Unmatched Commands :  Enable to permit unmatched commands

- **SAVE**

The screenshot shows the 'ClearPass Policy Manager' interface. The left sidebar contains a navigation tree with 'Enforcement' expanded. The main content area displays the configuration for 'Enforcement Profiles - MGMT-H3C-SW TACACS'. The configuration is divided into several sections:

- Profile:** Name: MGMT-H3C-SW TACACS, Description: MGMT-H3C-SW TACACS Profiles, Type: TACACS, Action: Accept, Device Group List: 1. MGMT SW
- Services:** Privilege Level: 15, Selected Services: 1. Shell, Authorize Attribute Status: ADD, Custom Services: -
- Service Attributes:** A table with columns 'Type', 'Name', and 'Value'. It contains two entries:
 

Type	Name	Value
1. Shell	roels	network-admin
2. Shell	priv-lvl	15
- Commands:** Service Type: shell, Unmatched Commands: Permit

## 6. Policies 配置

配置路径：

Configuration - Enforcement - Policies - Add

参数配置：

- **Enforcement:**

Name:

Description:

Enforcement Type: 勾选 TACACS+

Default Profile: [TACACS Deny Profile]

- **Rules:**

Rules Evaluation Algorithm: Select first match

Enforcement Policy Rules:

- 1、 Type : Authentication、 Name : Username、 Operator : EXISTS
- 2、 Type : Tips、 Name : Role、 Operator : EQUALS、 Value : SW ADMIN
- 3、 Enforcement Profiles : MGMT-H3C SW TACACS

- **SAVE**

The screenshot shows the 'ClearPass Policy Manager' interface. The left sidebar contains a navigation menu with categories like Dashboard, Monitoring, Configuration, Service Templates & Wizards, Services, Authentication, Identity, Posture, Enforcement, and Network. The main content area is titled 'Enforcement Policies - TACACS MGMT ACC-For H3C SWs' and has tabs for Summary, Enforcement, and Rules. The 'Rules' tab is selected, showing a table with columns for 'Conditions' and 'Actions'. The first rule is highlighted with a red box, showing conditions: '(Authentication:Username EXISTS )' and '(Tips:Role EQUALS SW ADMIN)'. The action for this rule is 'MGMT-H3C-SW TACACS', indicated by a red arrow.

Conditions	Actions
1. (Authentication:Username EXISTS ) (Tips:Role EQUALS SW ADMIN)	MGMT-H3C-SW TACACS

## 7. Services 配置

配置路径：

Configuration -Services -Add

参数模板关联配置：

- **Service :**

Type: TACACS+ Enforcement

Name:

Description:

Service Rule:

- 1、 Type: Connection、 Name : NAD-IP-Address、 Operator : BEGINS\_WITH、 Value : 10.80.80
- 2、 Type: Connection、 Name : NAD-IP-Address、 Operator : BEGINS\_WITH、 Value : 10.82.0
- 3、 Type: Connection、 Name : NAD-IP-Address、 Operator : BEGINS\_WITH、 Value : 10.81.32
- 4、 Type: Connection、 Name : Protocol、 Operator : EQUALS、 Value : TACACS

- **Authentication:**

Authentication Sources:选择以添加的认证源 AD “TACACS AUTH AD”

- **Roles :**

Role Mapping Policy : “TACACS ADMIN Role Mapping”

- **Enforcement:**

Enforcement Policy: “TACACS MGMT ACC-For H3C SWs”

- **SAVE**

aruba ClearPass Policy Manager Menu

Configuration > Services > Edit - TACACS H3C SWs ACC SERVICE

### Services - TACACS H3C SWs ACC SERVICE

Summary Service Authentication Roles Enforcement

**Service:**

Name: TACACS H3C SWs ACC SERVICE  
 Description: TACACS H3C SWs ACC SERVICE  
 Type: TACACS+ Enforcement  
 Status: Enabled  
 Monitor Mode: Disabled  
 More Options: -

**Service Rule**

Match ANY of the following conditions:

Type	Name	Operator	Value
1. Connection	NAD-IP-Address	BEGINS_WITH	*
2. Connection	NAD-IP-Address	BEGINS_WITH	*
3. Connection	NAD-IP-Address	BEGINS_WITH	*
4. Connection	Protocol	EQUALS	TACACS

**Authentication:**

Authentication Sources: TACACS AUTH AD  
 Strip Username Rules: -

**Roles:**

Role Mapping Policy: TACACS ADMIN Role Mapping

**Enforcement:**

Use Cached Results: Disabled  
 Enforcement Policy: TACACS MGMT ACC-For H3C SWs

## 8. 测试验证-1

**测试方法：**使用在对应 memberOf 属性值的组成员账号登陆 H3C 交换机

**测试结果：**在 ClearPass Tracker 中查看日志信息

**测试结果说明：**

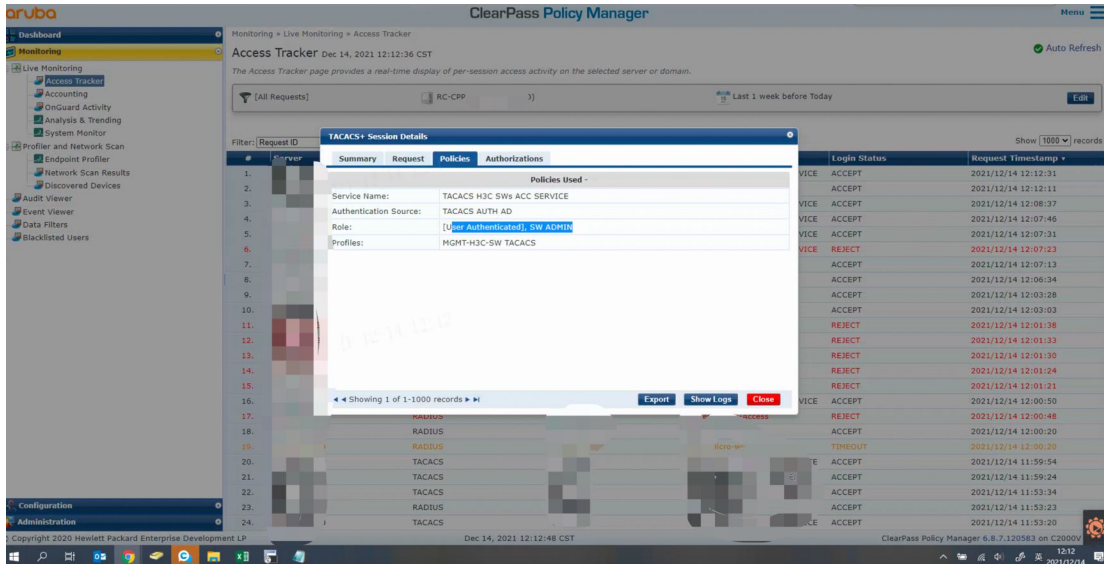
Summary -Status : AUTHEN\_STATUS\_PASS 成功通过认证

The screenshot displays the Aruba ClearPass Policy Manager interface. The main window shows the 'Access Tracker' page with a table of requests. A 'TACACS+ Session Details' pop-up window is open, showing the following information:

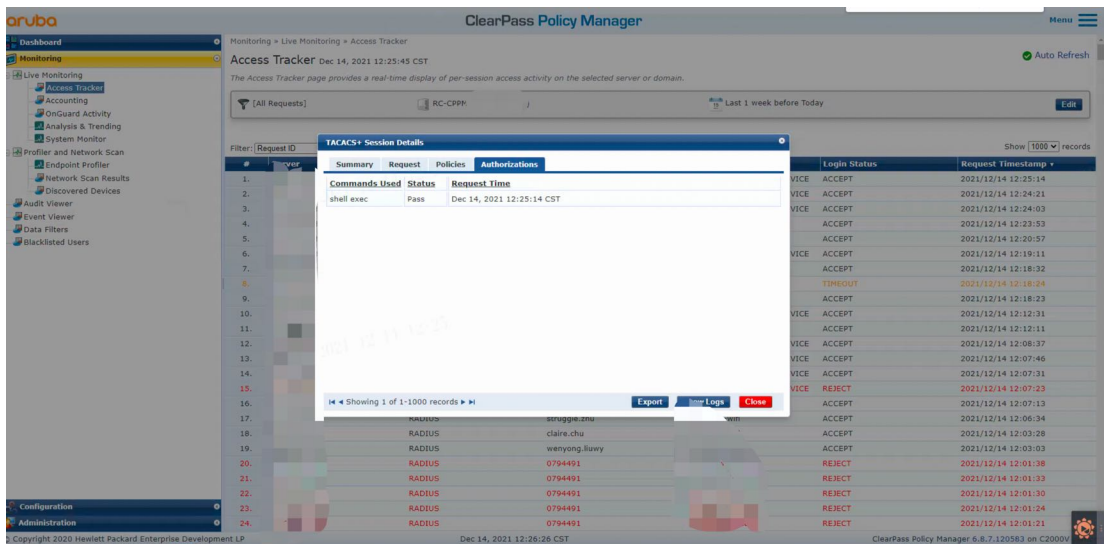
Summary	Request	Policies	Authorizations
Session ID:	T0000047-01-61b81caa		
Username:	ujjd		
Time:	Dec 14, 2021 12:25:14 CST		
Status:	AUTHEN_STATUS_PASS		
Authorizations:	1		

The background table shows a list of requests with columns for #, Server, Request, Policies, Authorizations, Login Status, and Request Time. The status for the selected request is 'ACCEPT'.

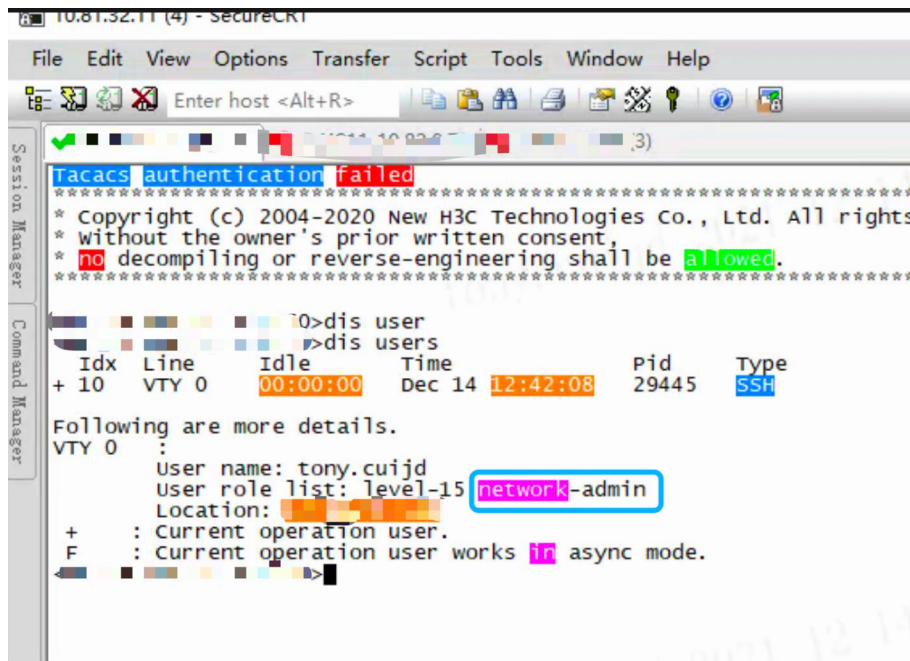
8.1. 日志 Policies -Role : [User Authenticated], SW ADMIN ////该 role 已通过 Role Mapping 获得正确映射关系



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



### 8.3. 交换机查看登陆用户



The screenshot shows a SecureCRT terminal window titled "10.81.32.11 (4) - SecureCRT". The terminal displays the following output:

```
Tacacs authentication failed
*****
* Copyright (c) 2004-2020 New H3C Technologies Co., Ltd. All rights
* without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****

[0]>dis user
[0]>dis users
  Idx  Line  Idle      Time      Pid      Type
+ 10   VTY 0   00:00:00  Dec 14 12:42:08  29445    SSH

Following are more details.
VTY 0 :
      User name: tony.cuijd
      User role list: level-15 network-admin
      Location:
+ : Current operation user.
F : Current operation user works in async mode.
```

## 9. 测试验证-2

测试方法：使用在非对应 memberOf\_属性值的组成员账号登陆 H3C 交换机

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
- Authorizations -Status：Fail ////因无法匹配 SW ADMIN 的角色，授权失败，无法登陆交换机；如下图二所示

The screenshot shows the ClearPass Policy Manager interface. The 'Access Tracker' page displays a list of requests. A red box highlights a specific request with a 'Status' of 'Fail'. The 'TACACS+ Session Details' window is open, showing the 'Authorizations' tab. The 'Role' is listed as '(User Authenticated), (Other)' and the 'Profiles' include '(TACACS Deny Profile)'. The 'Status' is 'REJECT'.

The detailed view of the 'TACACS+ Session Details' window shows the 'Authorizations' tab. The 'Commands Used' table is as follows:

Commands Used	Status	Request Time
	Fail	Dec 14, 2021 12:19:11 CST

At the bottom of the window, it shows 'Showing 6 of 1-1000 records' and buttons for 'Export', 'Show Logs', and 'Close'.