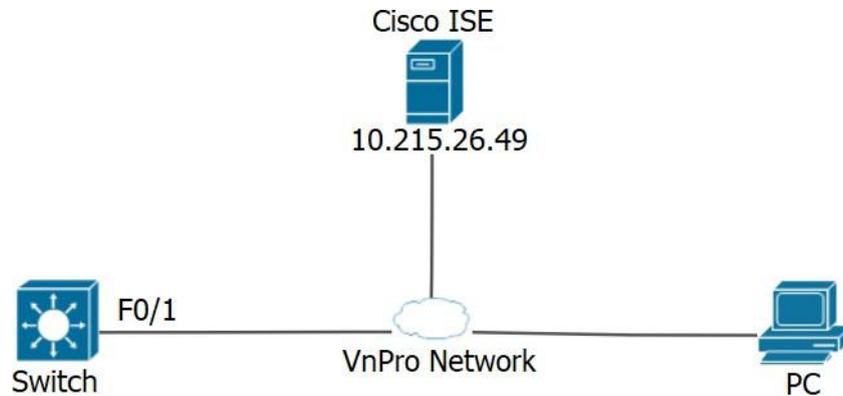


LAB - XÁC THỰC VÀ PHÂN QUYỀN LOGIN BẰNG TACACS+

I. Sơ đồ:



Ta có bảng thông tin như sau:

| Tên thiết bị | Interface | IP/Netmask | Gateway |
|--------------|-----------|--------------|---------|
| Cisco ISE | NIC | 10.215.26.49 | - |
| Switch | F0/1 | DHCP | - |
| PC | NIC | DHCP | - |

II. Yêu cầu:

1. Cấu hình ban đầu

- Thực hiện cấu hình IP cho PC, Switch sao cho switch và PC có thể ping thấy ISE server.

2. Cấu hình TACACS+:

- Tiến hành xác thực và phân quyền privilege cho các user truy cập telnet đến Switch như sau (việc xác thực/phân quyền phải do Cisco ISE kiểm soát):
 - Username: *guest*, password *VnPro@123*, privilege 7
 - Username: *adminvnpro*, password *VnPro@123*, privilege 15
- Cấu hình xác thực local với privilege cho các user như trên để khi hoạt động xác thực với Cisco ISE không thành công, chuyển sang phương thức xác thực/phân quyền local.

III. Thực hiện:

Cấu hình cho Switch

```
Switch(config)#no cdp run  
  
Switch(config)# int f0/1  
  
Switch(config-if)#no switchport  
  
Switch(config-if)# ip address dhcp  
  
Switch(config-if)# no shutdown
```

Cấu hình telnet:

```
Switch(config)# line vty 0 4  
  
Switch(config-line)#transport input telnet
```

Kết nối PC với VnPro Network. Tiến hành ping để kiểm tra kết nối tới ISE Server:

```
C:\Users\hoang>ping 10.215.26.49

Pinging 10.215.26.49 with 32 bytes of data:
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
Reply from 10.215.26.49: bytes=32 time=1ms TTL=61
Reply from 10.215.26.49: bytes=32 time=2ms TTL=61
```

Bật tính năng TACACS+ trên ISE:

Đầu tiên, ta mở trình duyệt và truy cập vào IP 10.215.26.49 (IP của ISE Server).

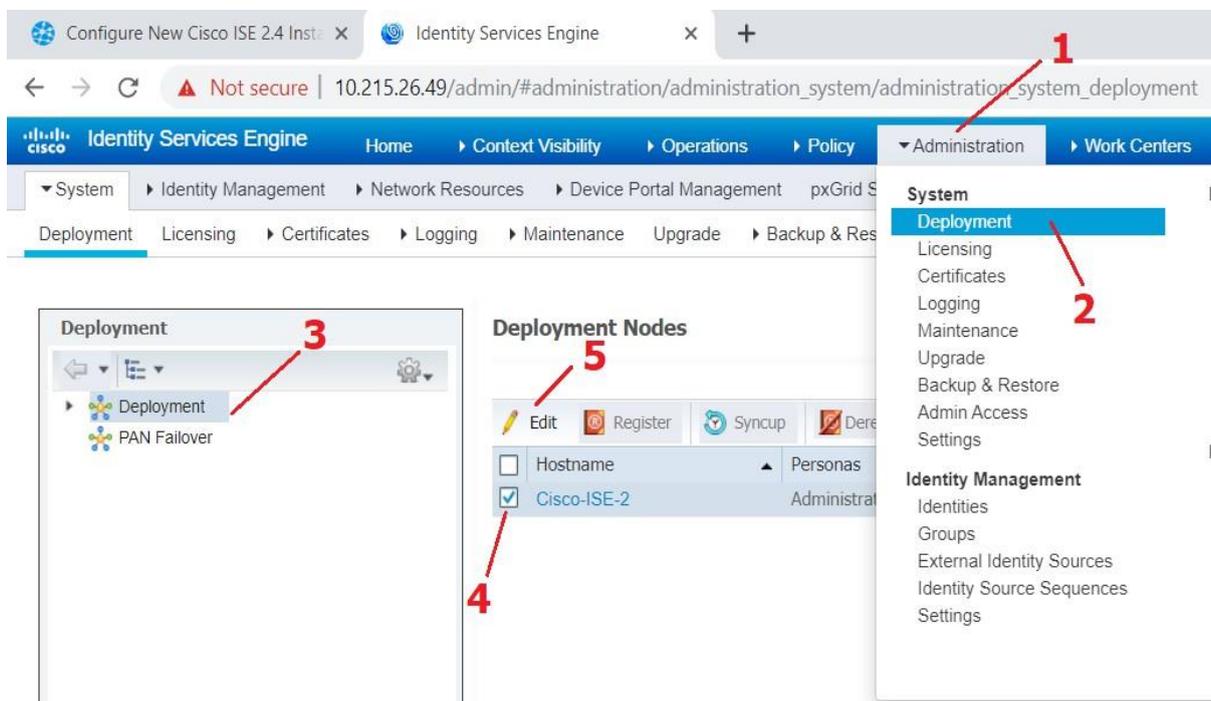
Đăng nhập bằng username và password:

Username: admin

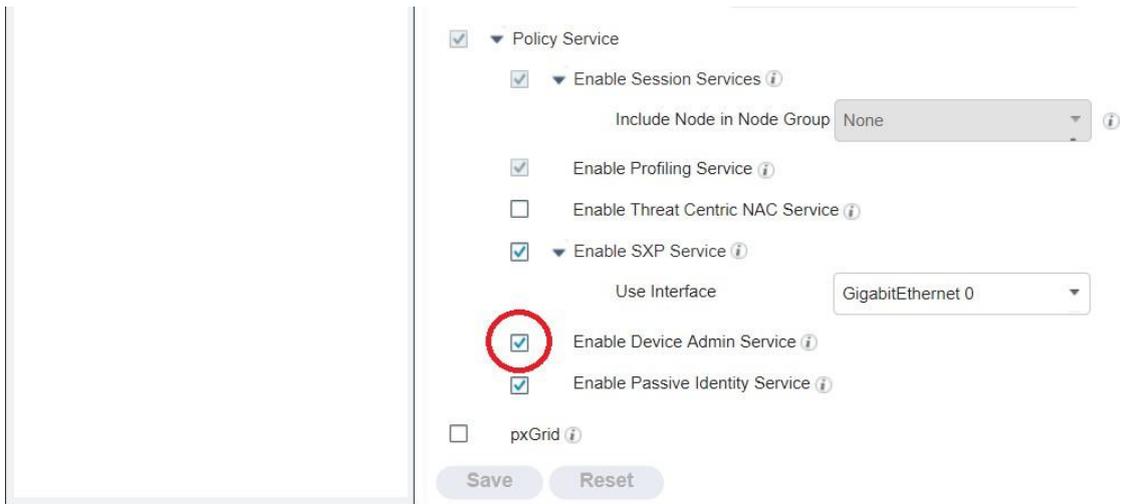
Password: VnPro@123

✓ Vào **Administration** → **Deployment** → Tích chọn hostname của Cisco ISE →

Edit:



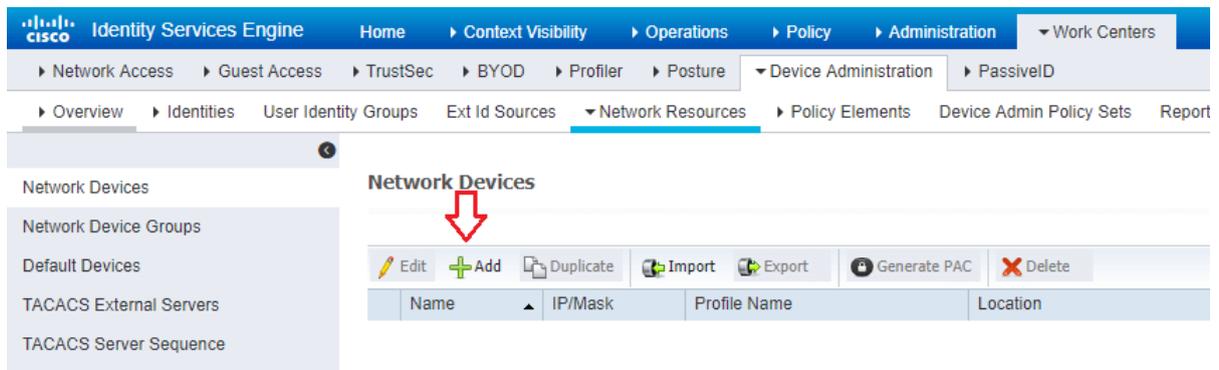
✓ Ở phần Policy Service, chọn **Enable Device Admin Service** và Save lại:



Thêm Switch vào ISE:

✓ Vào **Work Centers** → **Device Administration** → **Network Resources** → **Network Devices** → **Add**:

✓ Nhập tên, và IP của Switch mà ta nhận được từ DHCP do VnPro Network cấp:



✓ Ở phần **TACACS Authentication Settings** ta chỉ định chuỗi **“Shared Secret”** để Switch và ISE giao tiếp với nhau.

✓ Sau đó bấm submit.

✓ **Cấu hình xác thực/phân quyền bằng TACACS+:**

✓ Vào **Work Center → Device Admin Policy Sets:**

✓ Chọn Policy Elements → Result → TACACS Command Sets → Add:

← → ↻ Not secure | 10.215.26.49/admin/#workcenters/workcenter_device_administration/workcenter_device_administration_policy_ele

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

TACACS Command Sets

0 Selected

Refresh + Add Duplicate Trash Edit Import Export

| Name | Description |
|-----------------|---------------------|
| DenyAllCommands | Default Command Set |

✓ Tạo command set cho user *adminvnpro* có thể dùng đầy đủ các lệnh khi telnet:

TACACS Command Sets > CommandSet1

Command Set

Name

Description

Commands

Permit any command that is not listed below

+ Add Trash Edit Move Up Move Down

| Grant | Command | Arguments |
|----------------|---------|-----------|
| No data found. | | |

Cancel Save

✓ Tích chọn “Permit any command that is not listed below” và bấm Save.

- ✓ Ta cũng tạo thêm command set cho user *guest* có privilege là 7, khi user này telnet vào Switch chỉ dùng được lệnh các lệnh *show*:

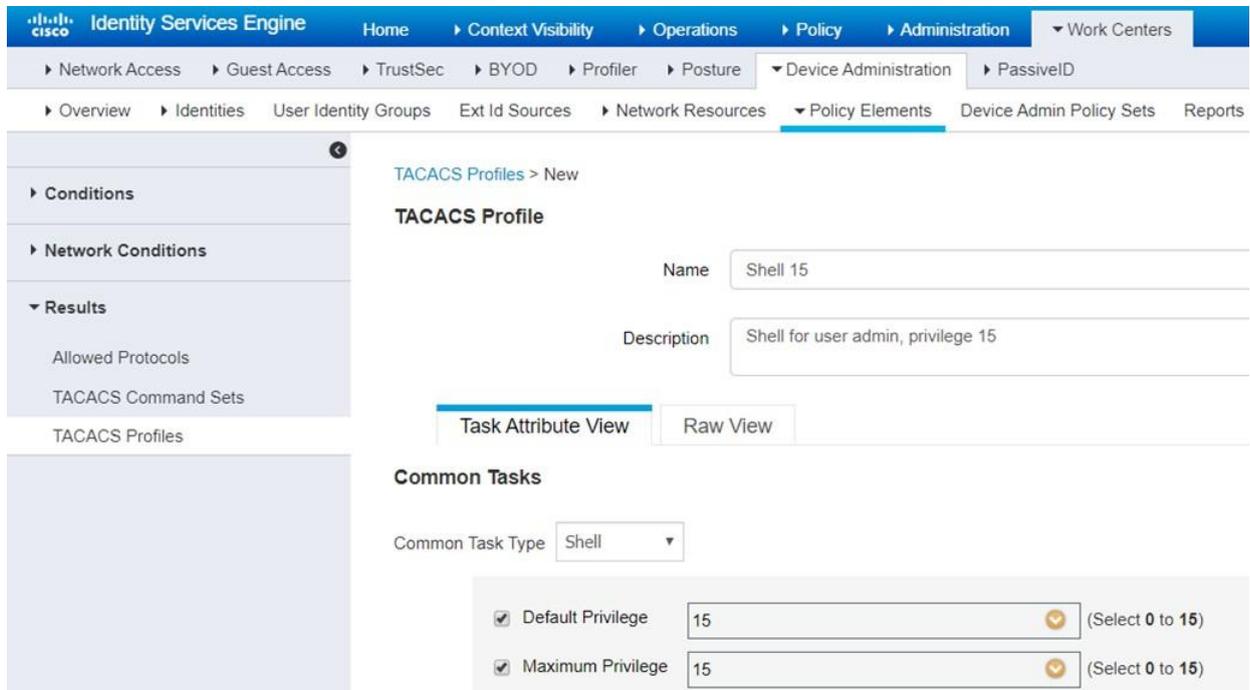
The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassivID > Policy Elements. The main content area is titled 'TACACS Command Sets > CommandSet7'. Under 'Command Set', the 'Name' field is 'CommandSet7' and the 'Description' is 'Privilege level 7 for Guest'. Under 'Commands', there is a checkbox for 'Permit any command that is not listed below' which is unchecked. Below this is a table with columns: Grant, Command, and Arguments. The table contains one entry: PERMIT, show*.

- ✓ Sau đó bấm **Submit**.

- ✓ Tiếp theo, ta vào **TACACS Profiles** → **Add**:

The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassivID > Policy Elements. The main content area is titled 'TACACS Profiles'. It shows '0 Selected' and a toolbar with 'Refresh', '+ Add', 'Duplicate', 'Trash', and 'Edit'. Below the toolbar is a table with columns: Name, Type, and Description. The table contains five entries: Default Shell Profile (Shell), Deny All Shell Profile (Shell), WLC ALL (WLC), and WLC MONITOR (WLC). A red arrow labeled '1' points to the 'TACACS Profiles' link in the left sidebar. Another red arrow labeled '2' points to the '+ Add' button in the toolbar.

✓ Tạo profile cho *adminvnpro* với privilege 15:



The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > Policy Elements > TACACS Profiles > New. The page title is "TACACS Profile".

The configuration fields are as follows:

- Name:** Shell 15
- Description:** Shell for user admin, privilege 15
- Task Attribute View:** Selected
- Common Task Type:** Shell
- Default Privilege:** 15 (Select 0 to 15)
- Maximum Privilege:** 15 (Select 0 to 15)

✓ Profile cho *guest* với privilege 7:

✓ Vào **Administration** → **Groups** → **User Identify Groups** → **Add**:

✓ Tạo 2 group cho user **adminvnpro** và user **guest**:

Identity Services Engine Home ▶ Context Visibility ▶ Operations ▶ Policy ▶ Adm

▶ System ▶ Identity Management ▶ Network Resources ▶ Device Portal Management pxGrid Services

▶ Identities **Groups** External Identity Sources Identity Source Sequences ▶ Settings

Identity Groups

▼

← ▶ [List Icon] [Settings Icon]

- ▶ Endpoint Identity Groups
- ▼ User Identity Groups
 - Admin7
 - ALL_ACCOUNTS (default)

User Identity Groups > **New User Identity Group**

Identity Group

* Name

Description

Identity Services Engine Home ▶ Context Visibility ▶ Operations ▶ Policy ▶ Ad

▶ System ▶ Identity Management ▶ Network Resources ▶ Device Portal Management pxGrid Services

▶ Identities **Groups** External Identity Sources Identity Source Sequences ▶ Settings

Identity Groups

▼

← ▶ [List Icon] [Settings Icon]

- ▶ Endpoint Identity Groups
- ▼ User Identity Groups
 - Admin7
 - ALL_ACCOUNTS (default)

User Identity Groups > **New User Identity Group**

Identity Group

* Name

Description

✓ Vào **Identities** → **Add** → Tạo user *adminvnpro*:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name

Status Enabled

Email

Passwords

Password Type:

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

User Information

Account Options

Account Disable Policy

User Groups

Trong đó:

- **Password Type:** Internal Users
- **User Group:** Group_Admin

Tương tự, ta cũng tạo thêm user **guest** với **User Groups** là Group_Guest:

Network Access User

* Name

Status Enabled

Email

User Groups

✓ Kết quả:

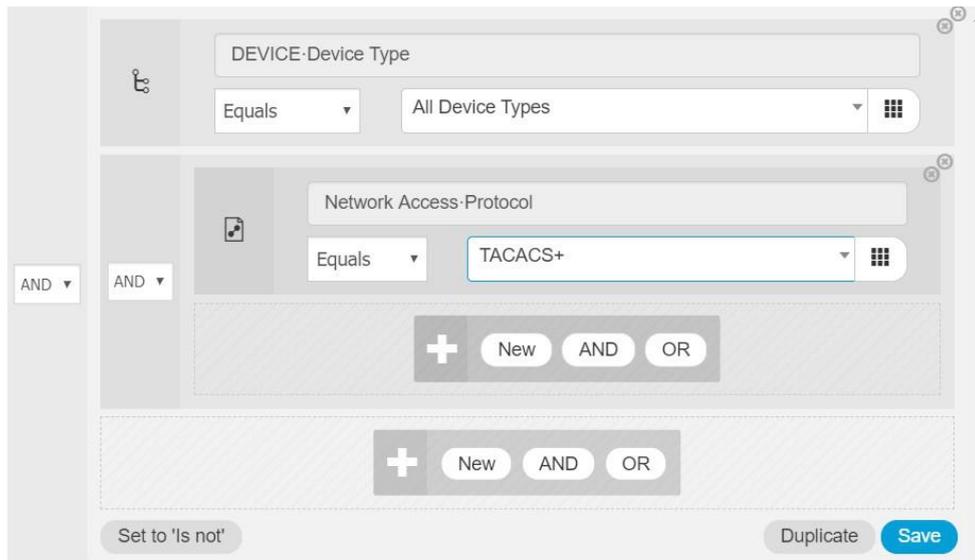
| Status | Name | De... | F. ↓ | Last Na... | E... | User Identity Groups |
|-------------------------------------|------------|-------|------|------------|------|----------------------|
| <input checked="" type="checkbox"/> | adminvnpro | | | | | Group_Admin |
| <input checked="" type="checkbox"/> | guest | | | | | Group_Guest |

✓ Tiếp theo, ta vào **Work Center** → **Device Admin Policy Sets** → **bấm (+)**:

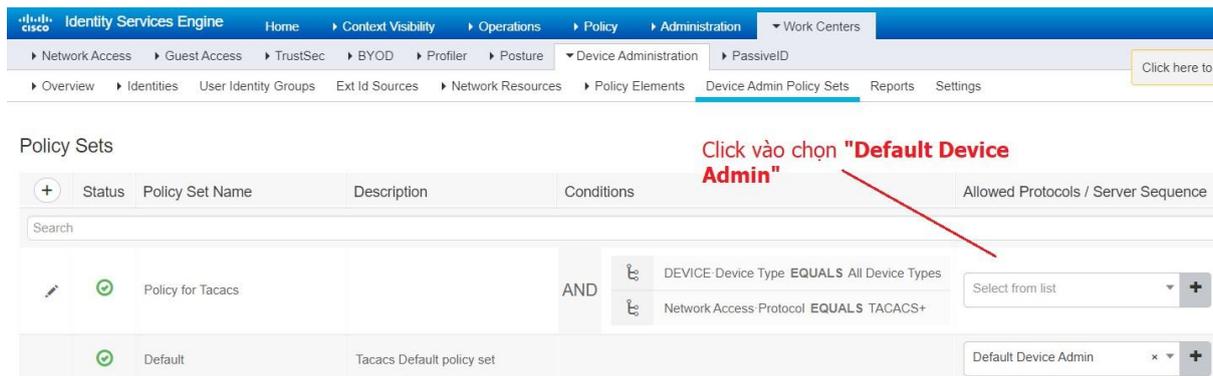
| Status | Policy Set Name | Description | Conditions |
|-------------------------------------|-------------------|---------------------------|------------|
| <input checked="" type="checkbox"/> | Policy for Tacacs | | |
| <input checked="" type="checkbox"/> | Default | Tacacs Default policy set | |

✓ Tạo policy như sau:

✓ Sau khi click “AND” ta chọn “New” và thiết lập như sau:

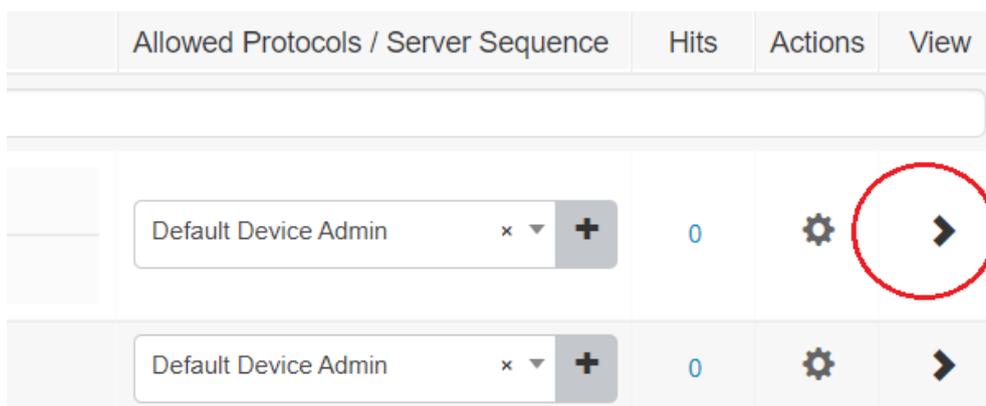


✓ Sau đó bấm “Use”, ta được kết quả:



✓ Sau đó save lại.

✓ Sau đó, ta click vào mũi tên qua phải của policy vừa mới tạo:



✓ Ở phần “Authentication Policy” ta chọn Use: Internal Users:

✓ Tiếp theo, ta cấu hình phần **Authorization Policy**:

✓ Cấu hình conditions như sau:

✓ Sau đó bấm “Use” để quay lại mục **Authorization Policy**, ở mục bên phải, ta chọn command set là “**CommandSet15**” và shell profile là “**Shell 15**”.

| | | | Results | |
|--------|--------------------|--|-------------------|------------------------|
| Status | Rule Name | Conditions | Command Sets | Shell Profiles |
| ✓ | Admin Privilege 15 | IdentityGroup-Name EQUALS User Identity Groups:Group_Admin | * CommandSet15 | Shell 15 |
| ✓ | Default | | * DenyAllCommands | Deny All Shell Profile |

✓ Trong tự vậ, ta cũng tạo **Authorization Policy** cho account *guest*:

IdentityGroup-Name

Equals

* User Identity Groups:Group_Guest

Set to 'Is not' Duplicate Save

+ New AND OR

| | | | Results | | | |
|--------|--------------------|--|-------------------|------------------------|------|---------|
| Status | Rule Name | Conditions | Command Sets | Shell Profiles | Hits | Actions |
| ✓ | Guest Privilege 7 | IdentityGroup Name EQUALS User Identity Groups:Group_Guest | * CommandSet7 | Shell 7 | | ⚙ |
| ✓ | Admin Privilege 15 | IdentityGroup-Name EQUALS User Identity Groups:Group_Admin | * CommandSet15 | Shell 15 | 0 | ⚙ |
| ✓ | Default | | * DenyAllCommands | Deny All Shell Profile | 0 | ⚙ |

Reset Save

✓ Sau đó ta save lại.

Chỉ định TACACS+ Server cho Switch:

```
Switch(config)#aaa new-model  
Switch(config)#tacacs server ISE  
Switch(config)#address ipv4 10.215.27.205  
Switch(config)#key cisco123
```

Cấu hình Switch xác thực với ISE bằng giao thức TACACS+:

Trên Switch, ta dùng các lệnh sau:

```
Switch(config)# aaa new-model  
Switch(config)# aaa group server tacacs+ ISESRV  
Switch(config-sg-tacacs+)# server 10.215.26.49  
Switch(config-sg-tacacs+)# exit  
  
Switch(config)#aaa authentication login VTY group ISESRV local  
Switch(config)#aaa authorization exec VTY group ISESRV local if-authenticated  
  
Switch(config)#aaa accounting exec default start-stop group ISESRV  
  
Switch(config)#aaa accounting commands 1 default start-stop group ISESRV  
  
Switch(config)#aaa accounting commands 15 default start-stop group ISESRV  
  
Switch(config)#aaa accounting network default start-stop group ISESRV
```

```
Switch(config)#aaa accounting connection default start-stop group ISESRV
```

```
Switch(config)#aaa accounting system default start-stop group ISESRV
```

Cấu hình telnet cho Switch:

```
Switch(config)#line vty 0 4
```

```
Switch(config-line)#login authentication VTY
```

```
Switch(config-line)#authorization exec VTY
```

```
Switch(config-line)#exit
```

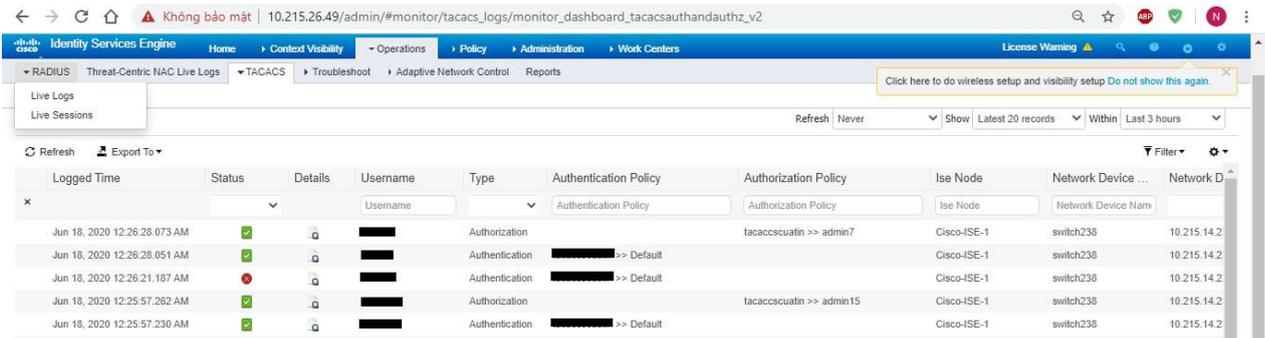
- ✓ Ta dùng PC **telnet** vào Switch thông qua **IP** mà **VnPro network cấp** với username là **adminvnpro** password là **VnPro@123**:

```
CA. Telnet 10.215.24.154
Microsoft Windows [Version 10.0.18363.900]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Jir0w>telnet 10.215.24.154
```

- ✓ Kết quả: Telet thành công:

```
Username:adminvnpro
Password:
Router#
```

- ✓ Gõ “?” để kiểm tra các lệnh user này có thể sử dụng, ta thấy user adminvnpro có thể dùng tất cả các lệnh:
- ✓ Ta kiểm tra **Tacacs+ log** trên cisco ise: **Operation->Tacacs->Live logs** được như sau:



| Logged Time | Status | Username | Type | Authentication Policy | Authorization Policy | Ise Node | Network Device | Network D |
|------------------------------|--------|------------|----------------|-----------------------|-------------------------|-------------|----------------|-------------|
| Jun 18, 2020 12:26:28.073 AM | ✓ | [REDACTED] | Authorization | [REDACTED] | tacaccsuatin >> admin7 | Cisco-ISE-1 | switch238 | 10.215.14.2 |
| Jun 18, 2020 12:26:28.051 AM | ✓ | [REDACTED] | Authentication | [REDACTED] >> Default | | Cisco-ISE-1 | switch238 | 10.215.14.2 |
| Jun 18, 2020 12:26:21.187 AM | ✗ | [REDACTED] | Authentication | [REDACTED] >> Default | | Cisco-ISE-1 | switch238 | 10.215.14.2 |
| Jun 18, 2020 12:25:57.262 AM | ✓ | [REDACTED] | Authorization | [REDACTED] | tacaccsuatin >> admin15 | Cisco-ISE-1 | switch238 | 10.215.14.2 |
| Jun 18, 2020 12:25:57.230 AM | ✓ | [REDACTED] | Authentication | [REDACTED] >> Default | | Cisco-ISE-1 | switch238 | 10.215.14.2 |

✓ Dấu tick màu xanh cho thấy đã pass xác thực nếu màu đỏ là chưa hoàn tất lab

✓ Hoàn tất bài lab.