



## LAB 2

### QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG, Ổ CỨNG VÀ HỆ THỐNG TẬP TIN

Họ tên và MSSV: Trương Đặng Trúc Lâm B2111933

Nhóm học phần: M03

- Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.

- Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết.

#### 1. Cài đặt CentOS

Thực hiện cài đặt CentOS 9 Stream vào máy tính cá nhân (hoặc máy ảo) của bạn **nếu cần** (KHÔNG cần chụp hình minh họa).

#### 2. Quản lý tài khoản

Tìm hiểu và thực hiện các yêu cầu sau:

**2.1.** Sử dụng lệnh `adduser` và `passwd` để tạo một tài khoản mới với tên đăng nhập có dạng **tên.họ** (ví dụ: **luan.thai**). (chụp hình minh họa).

Quan sát để thấy rằng khi một tài khoản mới được tạo, thư mục cá nhân trong `/home` và nhóm cá nhân trong `/etc/group` ứng với tài khoản đó cũng được tạo theo.

```
B2111933@localhost:~  
[B2111933@localhost ~]$ sudo adduser lam.truong  
[sudo] password for B2111933:  
[B2111933@localhost ~]$ ls /home  
B2111933 lam.truong  
[B2111933@localhost ~]$
```

Tạo tài khoản bằng quyền **sudo adduser <tên tài khoản>**. VD: **sudo adduser lam.truong**

```
B2111933@localhost:~ — nano /etc/passwd

GNU nano 5.6.1 /etc/passwd
geoclue:x:996:992:User for geoclue:/var/lib/geoclue:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
cockpit-ws:x:995:991:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:994:990:User for cockpit-ws instances:/nonexisting:/sbin/nologin
colord:x:993:989:User for colord:/var/lib/colord:/sbin/nologin
sssd:x:992:988:User for sssd:/:/sbin/nologin
setroubleshoot:x:991:987:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
pipewire:x:990:986:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
flatpak:x:989:985:User for flatpak system helper:/:/sbin/nologin
clevis:x:988:984:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:987:982:/:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:986:981:/:/var/lib/chrony:/sbin/nologin
dnsmasq:x:985:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
systemd-oom:x:978:978:systemd Userspace OOM Killer:/usr/sbin/nologin
B2111933:x:1000:1000:Truong Dang Truc Lam:/home/B2111933:/bin/bash
lam.truong:x:1001:1001:/:/home/lam.truong:/bin/bash

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

Ta có thể xem thông tin các tài khoản qua tập tin **/etc/passwd** hoặc **/etc/group** (mật khẩu đã được thay bằng ký tự “x”, thông tin mật khẩu được lưu trong tập tin **shadow**)

```
B2111933@localhost:~ — sudo nano /etc/shadow

GNU nano 5.6.1 /etc/shadow
flatpak:!!:19395:::::::
clevis:!!:19395:::::::
gdm:!!:19395:::::::
gnome-initial-setup:!!:19395:::::::
sshd:!!:19395:::::::
chrony:!!:19395:::::::
dnsmasq:!!:19395:::::::
tcpdump:!!:19395:::::::
systemd-oom:!*:19395:::::::
B2111933:$6$j0HG5l0.53LkN/Qf$EDQ7pVnAfDvHmi65Z96AP4lU.H.KIbapUDSmZY8igdVyqq
lam.truong:!!:19402:0:99999:7:::

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Do tập tin **/etc/shadow** chứa thông tin mật khẩu người dùng nên ta dùng lệnh **sudo** để mở. (ta có thể thấy tài khoản **lam.truong** chưa được tạo mật khẩu)

```
B2111933@localhost:~  
[B2111933@localhost ~]$ sudo passwd lam.truong  
Changing password for user lam.truong.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[B2111933@localhost ~]$
```

Ta gõ lệnh **sudo passwd <tên tài khoản>** để cập nhật mật khẩu cho tài khoản chỉ định.

**2.2.** Mở file `/etc/shadow` và cho biết mật khẩu bạn vừa tạo cho tài khoản mới sử dụng giải thuật băm nào? Dựa vào đâu để biết điều đó? (chụp hình minh hoạ).

```
B2111933@localhost:~ — sudo nano /etc/shadow  
GNU nano 5.6.1 /etc/shadow  
flatpak:!:19395:!:19395:!:19395:!  
clevis:!:19395:!:19395:!:19395:!  
gdm:!:19395:!:19395:!:19395:!  
gnome-initial-setup:!:19395:!:19395:!:19395:!  
sshd:!:19395:!:19395:!:19395:!  
chrony:!:19395:!:19395:!:19395:!  
dnsmasq:!:19395:!:19395:!:19395:!  
tcpdump:!:19395:!:19395:!:19395:!  
systemd-oom:!:19395:!:19395:!:19395:!  
B2111933:$6$j0HG5l0.53LkN/Qf$EDQ7pVnAfDvHmi65Z96AP4lU.H.KIbapUDSmZY8igdVyqqOS7p  
lam.truong:$6$Jo1aaPgHJpptpABe$kNuPhsKnruZ2C8eP8i69/6xrIjplmuE70jzJ60XDuMng2iXp  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

Ta dùng lệnh **sudo** để mở tập tin `/etc/shadow` và thấy mật khẩu đã được tạo cho **lam.truong**.  
(ký tự ở giữa hai dấu “\$” ở đầu mật khẩu là ký tự tượng trưng cho giải thuật băm)

Scheme id	Schema	Example
	DES	Kyq4bCxaK3kbg
—	BSDi	_EQ0.,jzh5VeUyoSqLupI
1	MD5	\$1\$etNnh7FA\$0lM7e1jE/B7F134XVnkb81
2, 2a, 2x, 2y, 2b	bcrypt	\$2a\$10\$VihI0oFSHqg061L4wzE//e.77dAQ6qntF/1dT7bqCrVtquInMy2q1
3	NTLASH	\$3\$5846F7eae8fb117ad06bd83007586c
5	SHA-256	\$5\$9ks3nWqv31FX.F\$gdEoLpScRsn/hW3uxdzfz2Loov1zeF4vJLomTRFD
6	SHA-512	\$6\$qqE2letU\$wMPRI.PVczjzeMvgjiA8LLy2nOyZbf7Amj3qIL978oi8gbMySdKZ7uepq9tmMQXyTirS12Pin.2Q/6Xscao0
7	scrypt	\$7\$DU....2Q0obwLh1n8qvQ16s1sA0/\$sHay3j/7Bdcu04131Ax1wCo9e5X518TcInCwyID1218
md5	Solaris MD5	\$md5,pounds=5000\$GUBv0xjJ\$5\$SugIsvdJ1TV0Yxv7HBVn0
sha1	PBKDF1 with SHA-1	\$sha1\$40000\$jtnX3nZ2\$H8NaIrkT4u8I2o5rs18Kxj5jNq1q
ily	gost-yescrypt	\$gy\$JCT\$H87v.7RupQLba8FDjN5k1\$vgq57k20ZwhFbAJVBye2vaA7ex/1VtU3a5fmL8wv/26
yr	yescrypt	\$y\$9T\$F53x5fExrKuPp53xLKQ...1\$X3DX8P04c7o.9agCG0G317fhZg05qC.S15rd.8hAtQ7
8 (Cisco)	PBKDF2 with SHA256	\$8\$mTj4RZG8H9ZD0k\$e1Y/asfm8kD3iDmkBe3hD2r4scA/0oW55V7os.O91u.
8 (JunOS)	PBKDF2	\$8\$crypt-algo\$hash-algo\$iterations\$salt\$iv\$tag\$encrypted \$8\$aes256-gcm\$mac-sha2-256\$100\$y/4mC4YDLU\$FzYDI4jjN5YCyQsVLSaf8A\$1lu4jLcZarD9YnyD/HeJua\$okh8lc0cGak5qYv0uv

Ta có thể

thấy mật khẩu của tài khoản **lam.truong** sử dụng giải thuật băm **SHA-512**. (\$6\$)  
**2.3.** Thiết lập ngày hết hạn cho tài khoản ở 2.1 là ngày 31/12/2022 (chụp hình minh hoạ).

```

B2111933@localhost:~
[B2111933@localhost ~]$ sudo usermod -e 12/31/2023 lam.truong
[B2111933@localhost ~]$ sudo chage -l lam.truong
Last password change                : Feb 14, 2023
Password expires                     : never
Password inactive                    : never
Account expires                     : Dec 31, 2023
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
[B2111933@localhost ~]$

```

Lệnh **usermod -e <tháng>/<ngày>/<năm> <tên tài khoản>** cho phép ta thiết lập ngày hết hạn cho tài khoản. Ta có thể xem thông tin phía trên bằng lệnh **chage -l <tên tài khoản>**.  
 Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ

2.4. Tạo một nhóm người dùng với tên nhóm là mã lớp của bạn. Thêm tài khoản ở 2.1 vào nhóm vừa tạo (chụp hình minh họa).

```
B2111933@localhost:~  
[B2111933@localhost ~]$ sudo groupadd DI21V7F3  
[sudo] password for B2111933:  
[B2111933@localhost ~]$ nano /etc/group
```

Ta dùng lệnh **groupadd <tên nhóm>** để tạo một nhóm người dùng.  
(tiến hành kiểm tra tập tin **/etc/group** xem nhóm người dùng trên đã được tạo hay chưa)

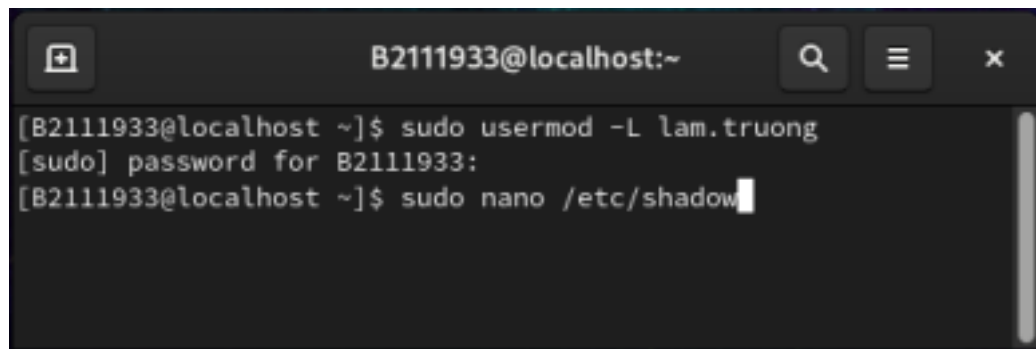
```
B2111933@localhost:~  
[B2111933@localhost ~]$ sudo usermod -a -G DI21V7F3 lam.truong  
[sudo] password for B2111933:  
[B2111933@localhost ~]$ groups lam.truong  
lam.truong : lam.truong DI21V7F3  
[B2111933@localhost ~]$
```

Lệnh **usermod -a -G <tên nhóm> <tên tài khoản>** dùng để thêm tài khoản vào nhóm chỉ định. Ta kiểm tra tài khoản hiện đang nằm trong nhóm nào với lệnh **groups <tên tài khoản>**.

```
B2111933@localhost:~ — nano /etc/group  
GNU nano 5.6.1 /etc/group  
dnsmasq:x:980:  
tcpdump:x:72:  
sgx:x:979:  
systemd-oom:x:978:  
B2111933:x:1000:  
lam.truong:x:1001:  
DI21V7F3:x:1002:lam.truong  
  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

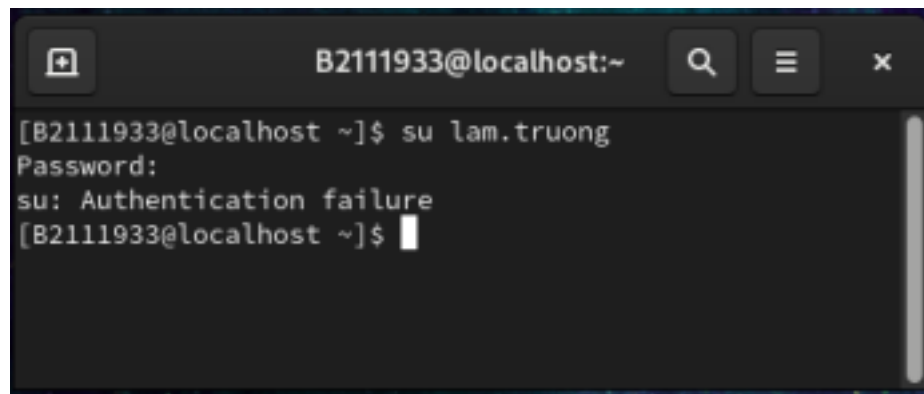
Kiểm tra lại thông tin nhóm người dùng bằng công cụ **nano**.

**2.5.** Thực hiện khóa tài khoản ở 2.1, sau đó đăng nhập thử và quan sát (chụp hình minh họa).



```
B2111933@localhost:~  
[B2111933@localhost ~]$ sudo usermod -L lam.truong  
[sudo] password for B2111933:  
[B2111933@localhost ~]$ sudo nano /etc/shadow
```

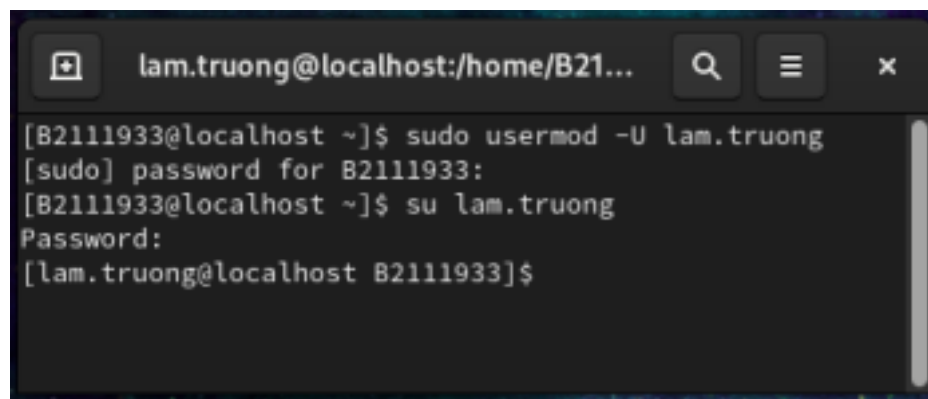
Lệnh **usermod -L <tên tài khoản>** cho phép ta khóa tài khoản.  
(ta có thể truy cập tập tin **/etc/shadow** để kiểm tra mật khẩu)



```
B2111933@localhost:~  
[B2111933@localhost ~]$ su lam.truong  
Password:  
su: Authentication failure  
[B2111933@localhost ~]$
```

Ta dùng lệnh **su <tên tài khoản>** để chuyển sang tài khoản chỉ định.  
Có thể thấy dù nhập đúng mật khẩu ta vẫn không thể truy cập tài khoản đã bị khóa.

**2.6.** Mở khóa tài khoản ở 2.1 (chụp hình minh họa).



```
lam.truong@localhost:/home/B21...  
[B2111933@localhost ~]$ sudo usermod -U lam.truong  
[sudo] password for B2111933:  
[B2111933@localhost ~]$ su lam.truong  
Password:  
[lam.truong@localhost B2111933]$
```

Lệnh **usermod -U <tên tài khoản>** cho phép ta mở khóa tài khoản.  
Giờ đây ta có thể truy cập tài khoản trên vì nó đã được mở khóa.

### 3. Quyền root (Root privilege) và sudo

Tìm hiểu và thực hiện các yêu cầu sau:

#### 3.1. Quyền root là gì?

Quyền **root** là quyền hạn mà tài khoản root có trên hệ thống. Tài khoản **root** là đặc quyền lớn nhất trên hệ thống và có quyền lực tuyệt đối đối với nó (tức là truy cập đầy đủ vào tất cả các file và lệnh). Một trong số các quyền hạn của **root** là khả năng sửa đổi hệ thống theo bất kỳ cách nào bạn muốn, cũng như cấp và thu hồi quyền truy cập (nghĩa là khả năng đọc, sửa đổi và thực thi các file và thư mục cụ thể) cho những user khác, kể cả mặc định dành riêng cho **root**.



#### 3.2. Nếu các ưu điểm của việc dùng **sudo** so với dùng **su** (chuyển sang tài khoản root).

Khái niệm **sudo**: **sudo** là một chương trình cho các hệ điều hành tương tự Unix. **sudo** cho phép user chạy chương trình với những đặc quyền bảo mật của user khác trong hệ điều hành Linux. Tức là, **sudo** cho phép thành viên nào đó có thể thực hiện lệnh trong hệ thống dưới quyền của thành viên khác và không cần cấp quyền đặc biệt.

##### Điểm khác biệt giữa **su** và **sudo**:

-**su** mang đến tính năng khởi động một cửa sổ mới của quyền root. Với các bảng phân phối Linux, người dùng có thể đăng nhập với tư cách người sử dụng root bằng cách gõ lệnh **su**. Sau đó, người dùng nhập tài khoản, mật khẩu của tài khoản root và truy cập bằng tài khoản của người dùng khác trên cửa sổ terminal.

-**sudo** chỉ chạy dòng lệnh khi được root cho phép. Tức là, khi chạy **sudo**, bạn cần nhập thông tin về tài khoản, mật khẩu mới có thể chạy câu lệnh như người dùng root. Bên cạnh đó, để xác nhận quyền của các user, **sudo** còn dùng file config (/etc/ sudoers).

Các ưu điểm của việc dùng **sudo** so với **su**:

-Sự khác biệt chính giữa hai loại này là mật khẩu họ yêu cầu: trong khi '**sudo**' yêu cầu mật khẩu người dùng hiện tại, **su** yêu cầu bạn nhập mật khẩu người dùng root. **sudo** là một sự thay thế tốt hơn giữa hai bên liên quan đến an ninh.

-Hành vi mặc định của lệnh **su** có khả năng gây nguy hiểm cho khả năng người dùng có thể quên thực tế rằng họ đang làm việc với quyền root và có thể vô tình thực hiện một số thay đổi không thể phục hồi.

-Mặc dù các lệnh chạy qua **sudo** được thực thi như người dùng đích (theo mặc định là root), chúng được gắn thẻ với tên người dùng của sudoer. Nhưng trong trường hợp **su**, không thể theo dõi trực tiếp những gì người dùng đã làm sau khi họ muốn vào tài khoản root.

-Lệnh **sudo** linh hoạt hơn nhiều ở chỗ bạn thậm chí có thể giới hạn các lệnh mà bạn muốn sudo-ers có quyền truy cập.

**3.3.** Mô tả các bước (chụp hình minh họa) để cấp quyền sudo cho tài khoản ở 2.1. Sau đó cho một ví dụ để kiểm chứng xem tài khoản này đã thực sự được cấp quyền hay chưa (chụp hình minh họa).

*Chúng ta không nên trực tiếp cấp quyền **sudo** cho từng người dùng.*

*Chúng ta nên thêm người dùng vào nhóm có quyền **sudo**.*

Ta lần lượt thực hiện các bước sau:

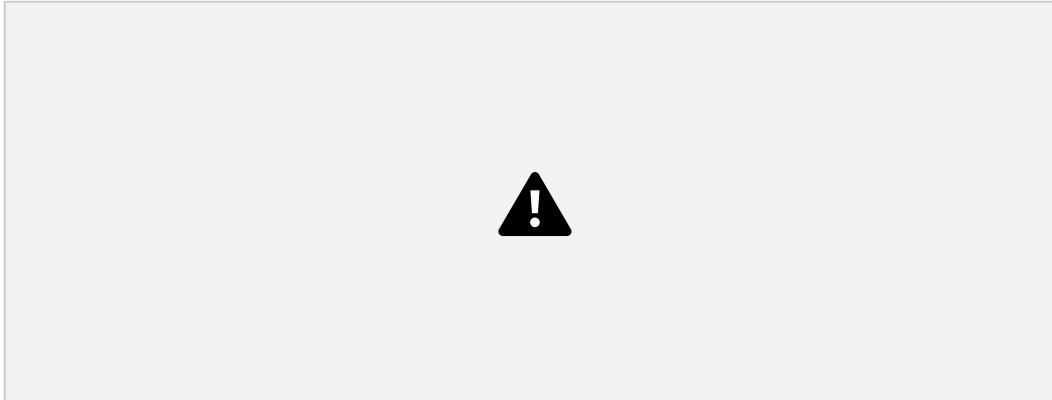
Bước 1: Kiểm tra nhóm người dùng có quyền sudo.



Đối với các hệ điều hành Linux thuộc nhánh phân phối Red Hat, thông thường sẽ có nhóm người dùng "wheel" được tạo sẵn và cấu hình có toàn quyền trên hệ thống.

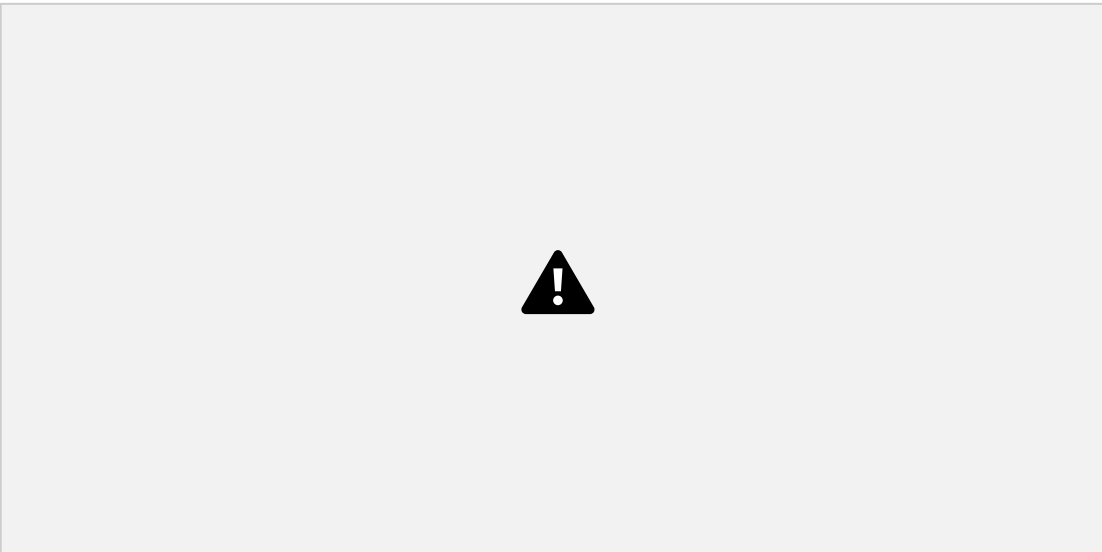


## Bước 2: Thêm người dùng vào nhóm có quyền **sudo**



Sử dụng lệnh **usermod -a -G <tên nhóm> <tên người dùng>** để thêm người dùng vào nhóm. Ta có thể kiểm tra lại kết quả bằng lệnh **groups <tên người dùng>**.

## Bước 3: Kiểm chứng xem tài khoản đã thực sự được cấp quyền hay chưa.



Ta tiến hành đăng nhập vào tài khoản chỉ định và thực hiện một lệnh bất kỳ cần quyền **sudo**. Có thể thấy trong lần đầu tiên người dùng chỉ định thực hiện quyền **sudo**, hệ thống sẽ gửi những thông báo nhắc nhở ta nên sử dụng quyền **sudo** một cách cẩn thận.

Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ

### **3.4.** Thu hồi quyền sudo của một tài khoản ở 2.1 (chụp hình minh họa).



Ta dùng lệnh **gpasswd -d <tên người dùng> <tên nhóm>** để xóa người dùng khỏi nhóm.



Ta tiến hành kiểm tra kết quả bằng cách đăng nhập tài khoản vừa bị xóa khỏi nhóm trên và thực hiện lệnh bất kỳ cần quyền **sudo**. Có thể thấy thông báo rằng tài khoản không có quyền **sudo**.

#### 4. Đĩa và phân vùng ổ cứng

Tìm hiểu và thực hiện các yêu cầu sau:

- 4.1. Thêm một ổ cứng vào máy ảo CentOS. Nếu đã cài CentOS trực tiếp vào máy tính cá nhân thì có thể sử dụng 1 USB để thay thế.

#### Các bước thêm một ổ cứng vào máy ảo CentOS:

**Bước 1:** Trước tiên ta phải tắt máy ảo.



Ta có thể tắt máy ảo với lệnh **shutdown now**.

Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ

**Bước 2:** Truy cập mục **Settings... → Storage**.



Ta click chuột phải vào máy ảo và chọn **Settings...**



Tiếp theo ta truy cập mục **Storage**.

**Bước 3:** Tiến hành thêm ổ cứng.



Chọn **Add hard disk**

Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ



Create → Chọn VDI → Next → Chọn Dynamic... → Next → Chọn 8gb → Create → Chọn.



Ổ cứng vừa tạo.

#### **Bước 4:** Khởi động lại máy ảo.

Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ

**4.2.** Sử dụng lệnh `fdisk` và `mkfs` để tạo và format một phân vùng trên ổ cứng vừa mới thêm ở 4.1 (chụp hình minh họa)

##### **1. Tạo ổ cứng**



ên máy ảo.

Sau đó ta dùng lệnh **fdisk <tên phân vùng>** để tiến hành phân vùng ổ đĩa.



Gõ phím **n** để tạo ra một phân vùng.

Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ

*Vậy là chúng ta đã tạo ra một phân vùng. Tuy nhiên, thông tin tạo phân vùng ấy vẫn chưa được ghi vào ổ cứng. Vì thế ta phải gõ phím 'w' để ghi phân vùng trên vào trong ổ cứng.*



*Phân vùng được tạo thành công.*



*Dùng lệnh **fdisk -l** để kiểm tra kết quả.*

## 2. Định dạng ổ cứng



Ta dùng lệnh `mkfs.ext4 <tên phân vùng>` để định dạng phân vùng trên theo chuẩn 4.

Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ

**4.3.** Tạo thư mục mới có tên `/data` bằng quyền **sudo**. Mount phân vùng ổ cứng ở 4.2 tới thư mục `/data` (chụp hình minh họa)

***Mount phân vùng ổ cứng ở 4.2 tới thư mục `/data` có nghĩa là dữ liệu trong thư mục `/data` sẽ được ghi vào phân vùng ổ cứng ở 4.2.***



Ta tiến hành tạo thư mục **/data** bằng quyền sudo, sau đó ta mount phân vùng ở **4.2** tới thư mục **/data** với cú pháp **mount <tên phân vùng> <tên thư mục>**.

**4.4.** Thực hiện lệnh **df -h** để xem kết quả. (chụp hình minh họa)



## **5. Phân quyền trên hệ thống tập tin**

**5.1.** Tạo nhóm người dùng **nhanvien**, thêm người dùng ở 2.1 vào nhóm **nhanvien**



Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ

Ta tạo nhóm **nhanvien** và thêm **người dùng ở 2.1** vào nhóm **nhanvien**.

**5.2.** Chuyển *nhóm chủ sở hữu* của thư mục **/data** sang **nhanvien**. Phân quyền cho thư mục **/data** là chủ sở hữu có quyền read, write và execute, nhóm chủ sở hữu có quyền read và execute, những người khác không có bất kỳ quyền gì cả

(chụp hình minh họa).



Do thư mục **/data** được tạo bằng quyền **sudo** nên chủ sở hữu hiện tại là **root**.



Dùng lệnh **chown :<tên nhóm> <tên thư mục>** để chuyển quyền sở hữu thư mục cho nhóm.



**chmod <1><2><3> <tên thư mục>** dùng để phân quyền cho thư mục chỉ định. **<1>** là quyền của chủ sở hữu. ( read + write + execute = 4 + 2 +1 = 7)

**<2>** là quyền của nhóm sở hữu. (read + execute = 4 + 1 = 5)

Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ

**<3>** là quyền của người khác. (không có quyền gì cả thì ta nhập 0)

**5.3. Dùng quyền sudo** tạo tập tin `/data/file1.txt`. Sau đó dùng tài khoản ở 2.1 tạo



tập tin `/data/file2.txt`. Quan sát và cho biết kết quả trong 2 trường hợp (chụp hình minh họa).



Lệnh **`sudo touch <tên tập tin>`** chắc chắn sẽ thành công do ta được cấp quyền **`sudo`**.



Có thể thấy thư mục **`/data`** thuộc quyền sở hữu của nhóm **`nhanvien`**. Do nhóm **`nhanvien`** không có quyền **`write`** nên ta không thể tạo tập tin hay thư mục khác trong thư mục **`/data`**.  
Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ

**5.4.** Dùng tài khoản ở 2.1 *mở và thay đổi nội dung* tập tin `/data/file1.txt`, cho biết kết quả (chụp hình minh họa).



Ta dùng công cụ **nano** để mở tập tin **file1.txt** và nhận thấy không thể thay đổi nội dung tập tin.



Tương tự câu **5.3**, do không có quyền **write** nên ta không thể ghi lại tập tin **file1.txt**.

**5.5.** Cấp quyền cho tài khoản 2.1 có thể thay đổi nội dung tập tin `/data/file1.txt` (chụp hình minh họa).



Ta quay về tài khoản có quyền **sudo** và dùng lệnh **chmod o+w <tên tập tin>** để  
Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ

cấp quyền **write** lên tập tin chỉ định cho nhóm “**người khác**”.



Đăng nhập **tài khoản 2.1** để kiểm tra kết quả.

**5.6.** Tạo thêm một tài khoản mới `newuser`, dùng tài khoản này mở tập tin `/data/file1.txt`, cho biết kết quả (chụp hình minh họa).



Tạo tài khoản **newuser** và đặt mật khẩu.



Dùng công cụ **nano** để mở tập tin **file1.txt** và ta nhận thông báo “**không thể truy cập**”.

***Ta quay về tài khoản có quyền sudo để kiểm tra.***

Quản trị hệ thống (CT179) - Khoa CNTT&TT - Đại học Cần Thơ



Ta thấy rằng nhóm “**người khác**” có quyền **write** trên tập tin **file1.txt**. Tuy nhiên trong thư mục **/data**, nhóm “**người khác**” lại không được cấp quyền gì cả (**không có quyền execute**) nên ta không thể đi ngang thư mục **/data**, dẫn đến việc không thể truy cập tập tin **file1.txt**. Tài khoản **lam.truong** thuộc nhóm **nhanvien** nên có quyền đi ngang thư mục **/data**.

**5.7. Dùng quyền sudo** tạo thư mục `/report` và tạo nhóm người dùng `quantri`. Phân quyền trên thư mục `/report` sao cho nhóm `quantri` có quyền `read`, `write` và `execute`, nhóm `nhanvien` có quyền `read` và `execute`, người dùng ở 2.1 có quyền `execute`, những người khác không có bất kỳ quyền gì cả (chụp hình minh họa).

Ta sử dụng kỹ thuật **ACL** để tiến hành phân quyền cho nhiều người dùng hay nhiều nhóm người dùng khác nhau trên một thư mục hay tập tin.





Đối với hệ điều hành **CentOS 9**, gói **acl** đã được cài đặt sẵn.



Ta tiến hành tạo thư mục **/report** và tạo nhóm người dùng **quantri**.  
Lệnh **getfacl <tên thư mục>** cho phép ta xem các quyền trên thư mục chỉ định



Ta sử dụng lệnh **setfacl -m g:quantri:rwX /report** để phân quyền trên thư mục **/report** sao cho nhóm **quantri** có quyền **read, write và execute**.



Tương tự ta dùng lệnh **setfacl -m g:nhanvien:r-x /report** để phân quyền cho nhóm **nhanvien**.



Lệnh **setfacl -m u:lam.truong:--x /report** dùng để phân quyền **execute** cho **người dùng 2.1**.  
Lệnh **setfacl -m o:--- /report** sẽ điều chỉnh sao cho nhóm “**người khác**” không có quyền gì cả.

--- Hết ---