



LAB 2 QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG, Ổ CỨNG VÀ HỆ THỐNG TẬP TIN

Họ tên và MSSV: Quách Minh Hón – B2110078

Nhóm học phần: 01

- 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: **bao.quoc**). (chụp hình minh họa).

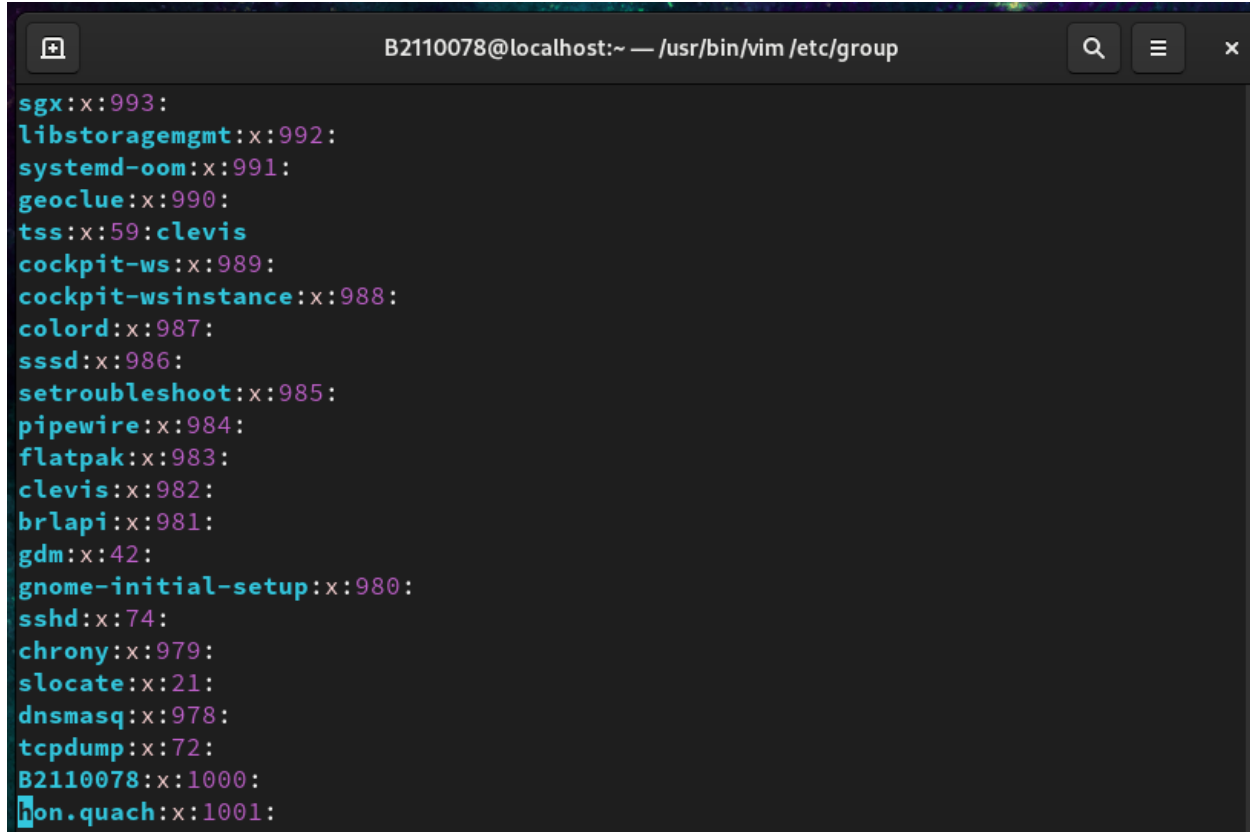
Quan sát để thấy rằng khi một tài khoản mới được tạo, thư mục cá nhân trong `/home` và nhóm cá nhân trong `/etc/group` ứng với tài khoản đó cũng được tạo theo.

```
B2110078@localhost:~ — /usr/bin/vim /etc/passwd
libstoragemgmt:x:992:992:daemon account for libstoragemgmt:/:usr/sbin/nologin
systemd-oom:x:991:991:systemd Userspace OOM Killer:/:usr/sbin/nologin
geoclue:x:990:990:User for geoclue:/var/lib/geoclue:/sbin/nologin
tss:x:59:59:Account used for TPM access:/:sbin/nologin
cockpit-ws:x:989:989:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:988:User for cockpit-ws instances:/nonexisting:/sbin/nologin
colord:x:987:987:User for colord:/var/lib/colord:/sbin/nologin
sssd:x:986:986:User for sssd:/:sbin/nologin
setroubleshoot:x:985:985:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
pipewire:x:984:984:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
flatpak:x:983:983:User for flatpak system helper:/:sbin/nologin
clevis:x:982:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:981:980:/:run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:980:979:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/:sbin/nologin
B2110078:x:1000:1000:Quach Minh Hon :/home/B2110078:/bin/bash
hon.quach:x:1001:1001::/home/hon.quach:/bin/bash
```

38,1

Bot

```
[B2110078@localhost ~]$ ls /home/
B2110078  hon.quach
```



```
sgx:x:993:
libstoragemgmt:x:992:
systemd-oom:x:991:
geoclue:x:990:
tss:x:59:clevis
cockpit-ws:x:989:
cockpit-wsinstance:x:988:
colord:x:987:
sssd:x:986:
setroubleshoot:x:985:
pipewire:x:984:
flatpak:x:983:
clevis:x:982:
brlapi:x:981:
gdm:x:42:
gnome-initial-setup:x:980:
sshd:x:74:
chrony:x:979:
slocate:x:21:
dnsmasq:x:978:
tcpdump:x:72:
B2110078:x:1000:
hon.quach:x:1001:
```

- 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 họa).
- Mật khẩu vừa tạo sử dụng giải thuật băm SHA-512
 - Dựa vào bảng các giải thuật băm trong đường dẫn sau:
[https://en.wikipedia.org/wiki/Crypt_\(C\)#Key_derivation_functions_supported_by_crypt](https://en.wikipedia.org/wiki/Crypt_(C)#Key_derivation_functions_supported_by_crypt)

```

B2110078@localhost:~ — sudo vi /etc/shadow
rtkit:!!:19602::::::
libstoragemgmt:!!:19602::::::
systemd-oom:!!:19602::::::
geoclue:!!:19602::::::
tss:!!:19602::::::
cockpit-ws:!!:19602::::::
cockpit-wsinstance:!!:19602::::::
colord:!!:19602::::::
sssd:!!:19602::::::
setroubleshoot:!!:19602::::::
pipewire:!!:19602::::::
flatpak:!!:19602::::::
clevis:!!:19602::::::
gdm:!!:19602::::::
gnome-initial-setup:!!:19602::::::
sshd:!!:19602::::::
chrony:!!:19602::::::
dnsmasq:!!:19602::::::
tcpdump:!!:19602::::::
B2110078:$6$X$kr1gHd/V.Eb0RrFVG/Ly/st7dW8pHcnp9FR5KN0FNus8IkXWBtEtQBwzdbyjnkMXz4
NLMlBj6CAjIYb7nsITf1:19602:0:99999:7:::
hon.quach:$6$3KouaYxx/0JSIBes$BnhA0Pa8TgEHBvQ03XeXW/2mI6NZpfsSvAjDWy1Xg3vxUZUunf
72aCp6hU9Iho4vEFGeoSpxmcsmlU.mKWkh/.:19616:0:99999:7:::
38,1 Bot

```

- 2.3. Thiết lập ngày hết hạn cho tài khoản ở 2.1 là ngày 31/12/2023 (chụp hình minh hoạ).

```

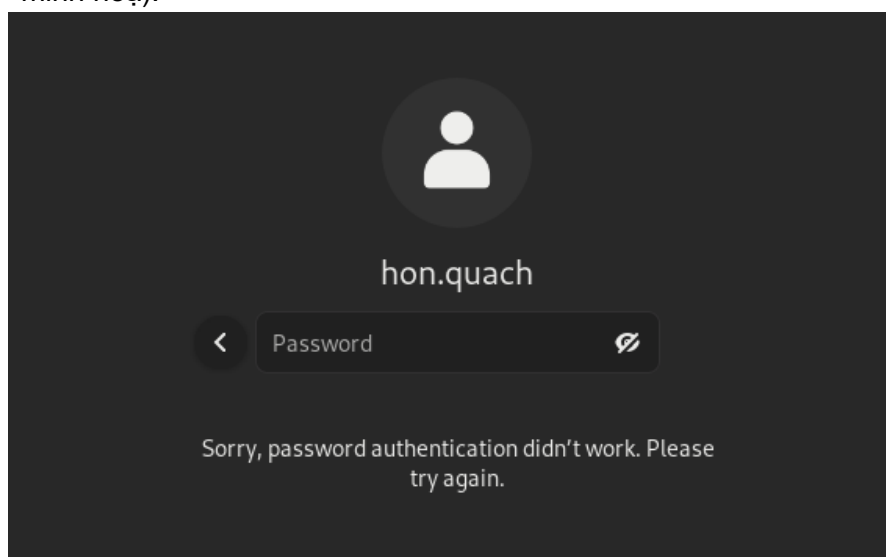
B2110078@localhost:~
[B2110078@localhost ~]$ sudo usermod -e 12/31/2023 hon.quach
[B2110078@localhost ~]$ sudo chage -l hon.quach
Last password change           : Sep 16, 2023
Password expires                : never
Password inactive               : never
Account expires                 : Dec 31, 2023
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

```

- 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 hoạ).

```
B2110078@localhost:~  
[B2110078@localhost ~]$ sudo groupadd CT17901  
[sudo] password for B2110078:  
[B2110078@localhost ~]$ sudo usermod -a -G CT17901 hon.quach  
[B2110078@localhost ~]$ groups hon.quach  
hon.quach : hon.quach CT17901
```

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



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

```
B2110078@localhost:~  
[B2110078@localhost ~]$ sudo usermod -U hon.quach  
  
hon.quach@localhost:~  
[hon.quach@localhost ~]$ groups  
hon.quach CT17901
```

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 các quyền hạn của tài khoản root có trên hệ thống. Tài khoản root là đặc quyền lớn nhất trên hệ thống và có quyền lực tuyệt đối. Nó có quyền truy cập đầy đủ vào tất cả các file và lệnh.
- 3.2. Nêu các ưu điểm của việc dùng `sudo` so với dùng `su` (chuyển sang tài khoản root).

- Không cần phải nhập mật khẩu root
- Kiểm soát chi tiết hơn
- Có thể tùy chỉnh quyền truy cập phức tạp và tùy chỉnh hành vi của các lệnh chạy
- Sử dụng mật khẩu của người dùng thay tài khoản root

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).

```
B2110078@localhost:~  
[B2110078@localhost ~]$ sudo groupadd QTHT  
[sudo] password for B2110078:  
[B2110078@localhost ~]$ sudo visudo /etc/sudoers
```

```
B2110078@localhost:~ — sudo visudo /etc/sudoers  
## Allow root to run any commands anywhere  
root    ALL=(ALL)        ALL  
  
## Allows members of the 'sys' group to run networking, software,  
## service management apps and more.  
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE,  
DRIVERS  
  
## Allows people in group wheel to run all commands  
%wheel   ALL=(ALL)        ALL  
%QTHT    ALL=(ALL)        ALL  
  
## Same thing without a password  
# %wheel   ALL=(ALL)        NOPASSWD: ALL  
  
## Allows members of the users group to mount and unmount the  
## cdrom as root  
# %users   ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom  
:wq
```

```
hon.quach@localhost:/home/B2110078  
[B2110078@localhost ~]$ sudo usermod -a -G QTHT hon.quach  
[sudo] password for B2110078:  
[B2110078@localhost ~]$ groups hon.quach  
hon.quach : hon.quach CT17901 QTHT  
[B2110078@localhost ~]$ su hon.quach  
Password:  
[hon.quach@localhost B2110078]$ sudo vi /etc/passwd
```

```

hon.quach@localhost:/home/B2110078 — sudo vi /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
"/etc/passwd" 38L, 2168B
1,1 Top

```

[hon.quach@localhost B2110078]\$ sudo vi /etc/shadow

```

hon.quach@localhost:/home/B2110078 — sudo vi /etc/shadow
cockpit-ws:!!:19602::::::
cockpit-wsinstance:!!:19602::::::
colord:!!:19602::::::
sssd:!!:19602::::::
setroubleshoot:!!:19602::::::
pipewire:!!:19602::::::
flatpak:!!:19602::::::
clevis:!!:19602::::::
gdm:!!:19602::::::
gnome-initial-setup:!!:19602::::::
sshd:!!:19602::::::
chrony:!!:19602::::::
dnsmasq:!!:19602::::::
tcpdump:!!:19602::::::
B2110078:$6$X$kr1gHd/V.Eb0RrFVG/Ly/st7dW8pHcnp9FR5KN0FNus8IkXWBtEtQBwzdbyjnkMXz4NLMlB
j6CAjIYb7nsITf1:19602:0:99999:7:::
hon.quach:$6$3KouaYxx/0JSIBes$BnhA0Pa8TgEHBvQ03XeXW/2mI6NZpfsSvAjDWy1Xg3vxUZUunf72aCp
6hU9Iho4vEFGeoSpxmcsmlU.mKWkh/.:19616:0:99999:7::19722:
"/etc/shadow" [readonly] 38L, 1266B
38,1 Bot

```

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

```

B2110078@localhost:~
[B2110078@localhost ~]$ sudo gpasswd -d hon.quach QTHT
[sudo] password for B2110078:
Removing user hon.quach from group QTHT
[B2110078@localhost ~]$ groups hon.quach
hon.quach : hon.quach CT17901

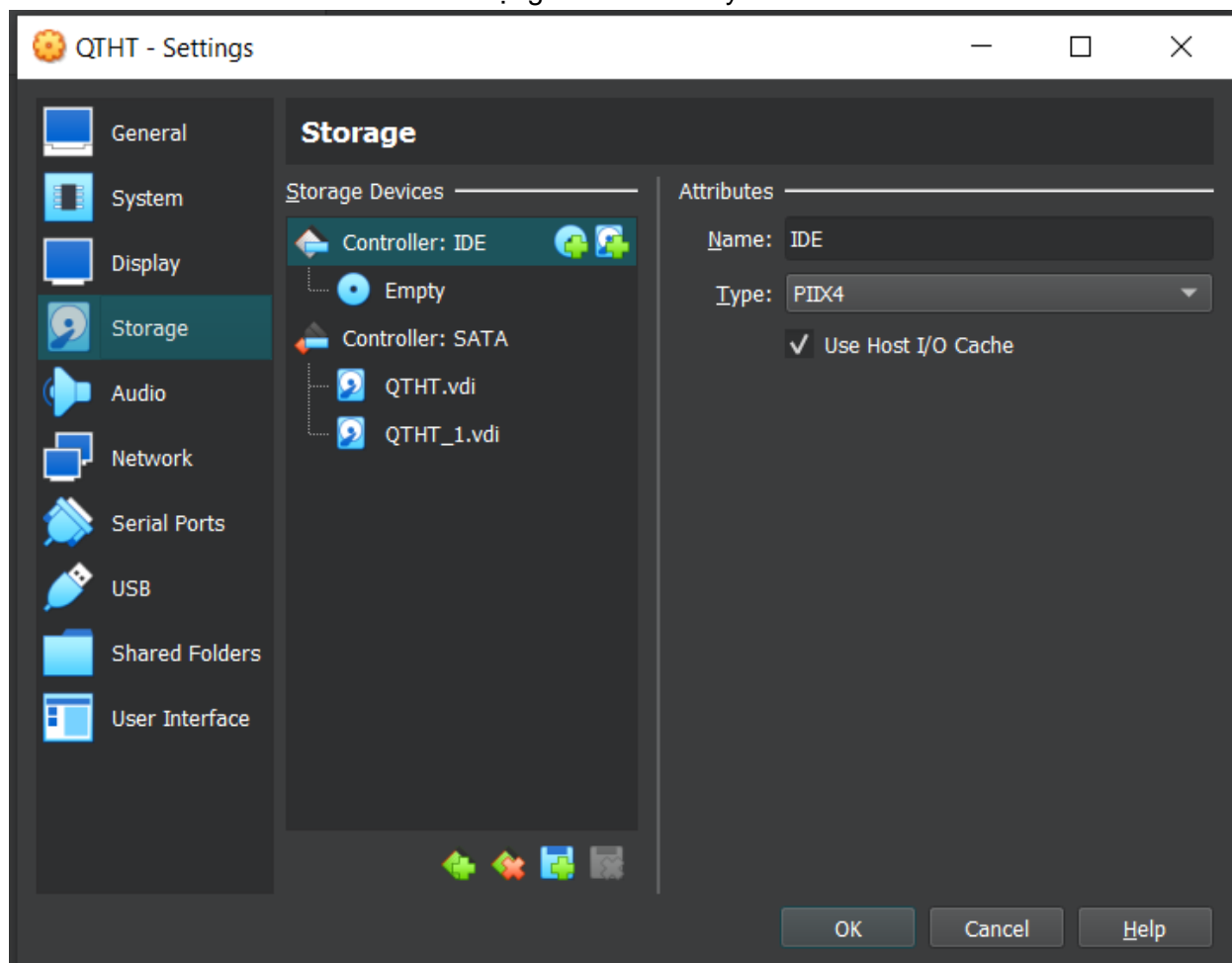
```

```
[B2110078@localhost ~]$ su hon.quach
Password:
[hon.quach@localhost B2110078]$ sudo vi /etc/shadow
[sudo] password for hon.quach:
hon.quach is not in the sudoers file. This incident will be reported.
```

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.



- 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)


```
Command (m for help): n
Partition type
  p   primary (0 primary, 0 extended, 4 free)
  e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-21662223, default 2048): 2048
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-21662223, default 21662223):
10500000
```

Created a new partition 1 of type 'Linux' and of size 5 GiB.

```
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

```
Command (m for help): n
Partition type
  p   primary (1 primary, 0 extended, 3 free)
  e   extended (container for logical partitions)
Select (default p): p
Partition number (2-4, default 2): 2
First sector (105000001-21662223, default 105000096): 105000096
Last sector, +/-sectors or +/-size{K,M,G,T,P} (105000096-21662223, default 21662223): 21662223
```

Created a new partition 2 of type 'Linux' and of size 5.3 GiB.

```
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sdb1		2048	105000000	10497953	5G	83	Linux
/dev/sdb2		105000096	216622223	11162128	5.3G	83	Linux

```
[B2110078@localhost ~]$ sudo mkfs.ext4 /dev/sdb1
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 1312244 4k blocks and 328656 inodes
Filesystem UUID: 1d7f3c15-8345-4560-aa2d-9f2b133780ca
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
```


- 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)

```

B2110078@localhost:~
[B2110078@localhost ~]$ sudo mkdir /data
[sudo] password for B2110078:
[B2110078@localhost ~]$ ls -l /
total 24
dr-xr-xr-x.  2 root root    6 Aug 10  2021 afs
lrwxrwxrwx.  1 root root    7 Aug 10  2021 bin -> usr/bin
dr-xr-xr-x.  5 root root 4096 Sep  8  20:25 boot
drwxr-xr-x.  2 root root    6 Sep 20  21:41 data
drwxr-xr-x. 30 root root 3200 Sep 20  21:21 home

```

```

[B2110078@localhost ~]$ sudo mount /dev/sdb1 /data

```

/dev/mapper/cs-root	/	xfs	defaults	0	0
UUID=90e213dc-1a0f-4ea9-a5f7-a76ad55d2b11	/boot	xfs	defaults	0	0
/dev/mapper/cs-swap	none	swap	defaults	0	0
UUID=1d7f3c15-8345-4560-aa2d-9f2b133780ca	/data	ext4	defaults	0	0

```

[B2110078@localhost ~]$ sudo nano /etc/fstab
[B2110078@localhost ~]$ sudo mount -a
[B2110078@localhost ~]$

```

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

```

[B2110078@localhost ~]$ df -h

```

Filesystem	Size	Used	Avail	Use%	Mounted on
devtmpfs	4.0M	0	4.0M	0%	/dev
tmpfs	882M	0	882M	0%	/dev/shm
tmpfs	353M	5.6M	348M	2%	/run
/dev/mapper/cs-root	17G	5.2G	12G	31%	/
/dev/sda1	960M	407M	554M	43%	/boot
tmpfs	177M	96K	177M	1%	/run/user/1000
/dev/sdb1	4.9G	24K	4.6G	1%	/data

5. Phân quyền trên hệ thống tập tin

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

```

[B2110078@localhost ~]$ sudo groupadd nhanvien
[sudo] password for B2110078:
[B2110078@localhost ~]$ sudo usermod -a -G nhanvien hon.quach
[B2110078@localhost ~]$ groups hon.quach
hon.quach : hon.quach CT17901 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).

```
[B2110078@localhost ~]$ sudo chgrp nhanvien /data
[sudo] password for B2110078:
[B2110078@localhost ~]$ getfacl /data
getfacl: Removing leading '/' from absolute path names
# file: data
# owner: root
# group: nhanvien
user::rwx
group::r-x
other::r-x
```

```
[B2110078@localhost ~]$ sudo chmod 750 /data
[sudo] password for B2110078:
[B2110078@localhost ~]$ getfacl /data
getfacl: Removing leading '/' from absolute path names
# file: data
# owner: root
# group: nhanvien
user::rwx
group::r-x
other::---
```

- 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).

```
[B2110078@localhost ~]$ sudo nano /data/file1.txt
[B2110078@localhost ~]$ sudo cat /data/file1.txt
file 1
[B2110078@localhost ~]$ su hon.quach
Password:
[hon.quach@localhost B2110078]$ sudo nano /data/file2.txt
[sudo] password for hon.quach:
hon.quach is not in the sudoers file. This incident will be reported.
[hon.quach@localhost B2110078]$ nano /data/file2.txt
```

```
GNU nano 5.6.1 /data/file2.txt Modified
file2.txt

[ Error writing /data/file2.txt: Permission denied ]
^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
```

- Có thể tạo file1.txt sử dụng tài khoản B2110078 vì tài khoản đó nằm trong nhóm sudoers.
 - Không thể tạo file2.txt sử dụng tài khoản hon.quach, vì tài khoản hon.quach không nằm trong nhóm nhanvien.
- 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 hoạ).

```
[hon.quach@localhost B2110078]$ nano /data/file1.txt
```

```
GNU nano 5.6.1 /data/file1.txt Modified
lksldkfjlk sdf file 1

[ Error writing /data/file1.txt: Permission denied ]
^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
```

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

```
[B2110078@localhost ~]$ sudo chmod o+w /data/file1.txt
[B2110078@localhost ~]$ sudo ls -l /data/
total 20
-rw-r--rw-. 1 root root      7 Sep 21 15:20 file1.txt
```

```
GNU nano 5.6.1                               /data/file1.txt
file 1
da chinh sua

[ Wrote 2 lines ]
```

```
[hon.quach@localhost B2110078]$ cat /data/file1.txt
file 1
da chinh sua
```

- 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).

```
[B2110078@localhost ~]$ sudo useradd newuser
[sudo] password for B2110078:
[B2110078@localhost ~]$ sudo passwd newuser
[sudo] password for B2110078:
Changing password for user newuser.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[B2110078@localhost ~]$ su newuser
Password:
[newuser@localhost B2110078]$ nano /data/file1.txt
```

```
GNU nano 5.6.1 /data/file1.txt

[ Path '/data' is not accessible ]

^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
```

- 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 hoạ).

```
[B2110078@localhost ~]$ sudo mkdir /report
[B2110078@localhost ~]$ ls /
afs  boot  dev  home  lib64  mnt  proc  root  sbin  sys  usr
bin  data  etc  lib   media  opt  report  run  srv  tmp  var
[B2110078@localhost ~]$ getfacl /report
getfacl: Removing leading '/' from absolute path names
# file: report
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
```

```
[B2110078@localhost ~]$ sudo groupadd quantri
[B2110078@localhost ~]$ sudo setfacl -m g:quantri:rwx /report
[B2110078@localhost ~]$ getfacl /report
getfacl: Removing leading '/' from absolute path names
# file: report
# owner: root
# group: root
user::rwx
group::r-x
group:quantri:rwx
mask::rwx
other::r-x
```

```
[B2110078@localhost ~]$ sudo setfacl -m g:nhanvien:r-x /report
[B2110078@localhost ~]$ getfacl /report
getfacl: Removing leading '/' from absolute path names
# file: report
# owner: root
# group: root
user::rwx
group::r-x
group:nhanvien:r-x
group:quantri:rwx
mask::rwx
other::r-x
```

```
[B2110078@localhost ~]$ sudo setfacl -m u:hon.quach:x /report
[B2110078@localhost ~]$ sudo setfacl -m o:--- /report
[B2110078@localhost ~]$ getfacl /report
getfacl: Removing leading '/' from absolute path names
# file: report
# owner: root
# group: root
user::rwx
user:hon.quach:--x
group::r-x
group:nhanvien:r-x
group:quantri:rwx
mask::rwx
other:---
```

--- Hết ---