

## LAB 2

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

**Họ tên và MSSV:** Nguyễn Văn Nhấn - B1809272

**Nhóm học phần:** 02

### 1. Cài đặt CentOS

Thực hiện cài đặt CentOS 6 (hoặc CentOS 7,8) vào máy tính cá nhân (hoặc máy ảo) của bạn (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 masosinhvien (ví dụ: b1801234). (chụp hình minh họa).

```
#adduser bb1809272 && passwd bb1809272
```

```
[root@localhost B1809272]# adduser bb1809272 && passwd bb1809272
Changing password for user bb1809272.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost B1809272]#
```

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.

```
#nano /etc/group
```

```
GNU nano 2.9.8 /etc/group
flatpak:x:978:
colord:x:977:
rpcuser:x:29:
gdm:x:42:
clevis:x:976:
gnome-initial-setup:x:975:
sshd:x:74:
slocate:x:21:
rngd:x:974:
tcpdump:x:72:
B1809272:x:1000:
vboxsf:x:973:
bb1809272:x:1001:
```

```
#ls home
```

```
[root@localhost B1809272]# ls /home
B1809272  bb1809272
[root@localhost B1809272]#
```

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

```
#nano /etc/shadow
```



```
GNU nano 2.9.8 /etc/shadow
gdm:!:18708:::::::
clevis:!:18708:::::::
gnome-initial-setup:!:18708:::::::
sshd:!:18708:::::::
rngd:!:18708:::::::
tcpdump:!:18708:::::::
B1809272:$6$c0sViD8X6r4aDFtC$t3ABQqgXvXkUt0WKYlVIlx5SeAy0paD.0HyXyNvC138KWWw/7RpRY$
vboxadd:!:18708:::::::
bb1809272:$6$B5VL0gb0ULIS3e7i$IQFJZ06GAaF0KGJ.23BkorqViaT0bDX9QZscKA8zPb0Uz1ejdON$
```

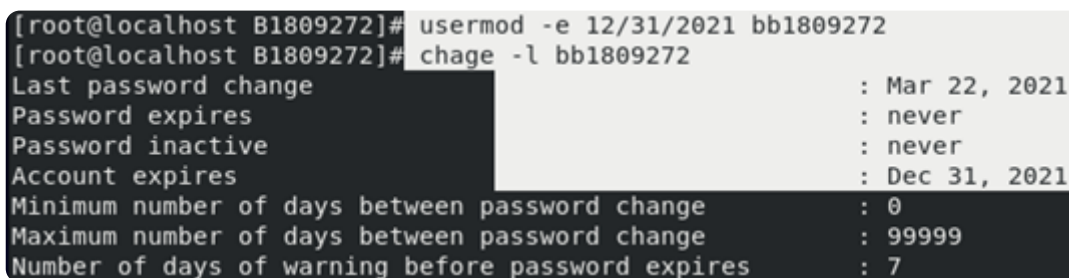
Tài khoản mới tạo sử dụng giải thuật băm : SHA-512 (\$6)

```
$1 = MD5 hashing algorithm.
$2 = Blowfish Algorithm is in use.
$2a = eksblowfish Algorithm
$5 = SHA-256 Algorithm
$6 = SHA-512 Algorithm
```

**2.3.** Thiết lập ngày hết hạn cho tài khoản ở 2.1 là ngày 31/12/2020 (chụp hình minh họa).

```
#usermod -e 12/31/2021 bb1809272
```

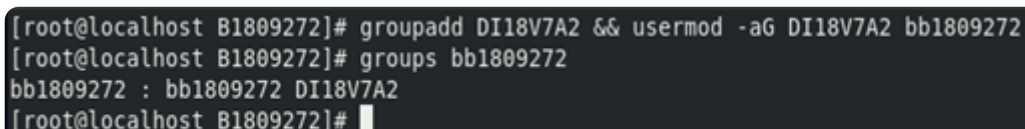
Xem thông tin user: `#chage -l bb1809272`



```
[root@localhost B1809272]# usermod -e 12/31/2021 bb1809272
[root@localhost B1809272]# chage -l bb1809272
Last password change                : Mar 22, 2021
Password expires                    : never
Password inactive                   : never
Account expires                     : Dec 31, 2021
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 họa).

```
#groupadd DI18V7A2 && usermod -aG DI18V7A2 bb1809272
```



```
[root@localhost B1809272]# groupadd DI18V7A2 && usermod -aG DI18V7A2 bb1809272
[root@localhost B1809272]# groups bb1809272
bb1809272 : bb1809272 DI18V7A2
[root@localhost B1809272]#
```

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

```
#usermod -L bb1809272
```

```
[root@localhost B1809272]# usermod -L bb1809272
[root@localhost B1809272]#
```

Trong tập tin **/etc/shadow** mật khẩu thêm "!"

```
bb1809272:!!$B5VL0gb0ULIS3e7i$IQFJZ06GAaF0KGJ.23BkorqViaT0bDX9QZscKA8zPb0Uz1ejd0N$
```

Đăng nhập tài khoản bb1809272: `$su bb1809272`

```
[B1809272@localhost ~]$ su bb1809272
Password:
su: Authentication failure
[B1809272@localhost ~]$
```

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

```
#usermod -U bb1809272
```

```
[root@localhost B1809272]# usermod -U bb1809272
[root@localhost B1809272]#
```

Trong tập tin **/etc/shadow** mật khẩu mất "!"

```
bb1809272:$B5VL0gb0ULIS3e7i$IQFJZ06GAaF0KGJ.23BkorqViaT0bDX9QZscKA8zPb0Uz1ejd0N$
```

Đăng nhập tài khoản bb1809272: `$su bb1809272`

```
[B1809272@localhost ~]$ su bb1809272
Password:
[bb1809272@localhost B1809272]$
```

### 3. Quyền root (Root privilege)

Tìm hiểu và thực hiện các yêu cầu sau:

#### 3.1. Quyền root là gì?

Root là tên người dùng hoặc tài khoản mà theo mặc định có quyền truy cập vào tất cả các lệnh và file trên Linux hoặc hệ điều hành giống Unix khác. Root cũng được gọi là tài khoản root, người dùng root và siêu người dùng.

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

Câu lệnh su đại diện cho quyền hạn cao nhất của người dùng (root user). Nó được thực thi trên hệ thống linux mà không cần bất cứ option nào. Người dùng chỉ cần đơn giản thêm password của tài khoản root. Trên cửa sổ terminal, su cho phép truy cập vào các tài khoản người dùng khác, sử dụng password được yêu cầu. Đó là lý do tại sao su cũng đại diện cho các người dùng thay thế hay người dùng switch. Chỉ đơn giản gõ su, tiếp đó nhập tên tài khoản và password là bạn đã có toàn quyền.

Sudo sử dụng một file config (/etc/sudoers) để xác định quyền của các người dùng khác nhau.

Sau khi so sánh, ta thấy sudo để người dùng sử dụng tài khoản của họ để chạy câu lệnh hệ thống. Su thì bắt buộc người dùng chia sẻ root password với các người dùng khác. Đó chính là lý do tại sao sudo không khởi động bất kì một cửa sổ shell mới nào.

**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).

Tạo và cấp quyền toàn quyền cho nhóm người dùng qtht

```
#groupadd qtht
```

```
[root@localhost B1809272]# groupadd qtht
[root@localhost B1809272]#
```

Cấp quyền trên tập tin: **/etc/sudoers**

Thêm vào dòng: %qtht ALL=(ALL) ALL

```
GNU nano 2.9.8 /etc/sudoers Modified
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, LOCAT$

## 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

## Allows members of the users group to shutdown this system
# %users    localhost=/sbin/shutdown -h now
```

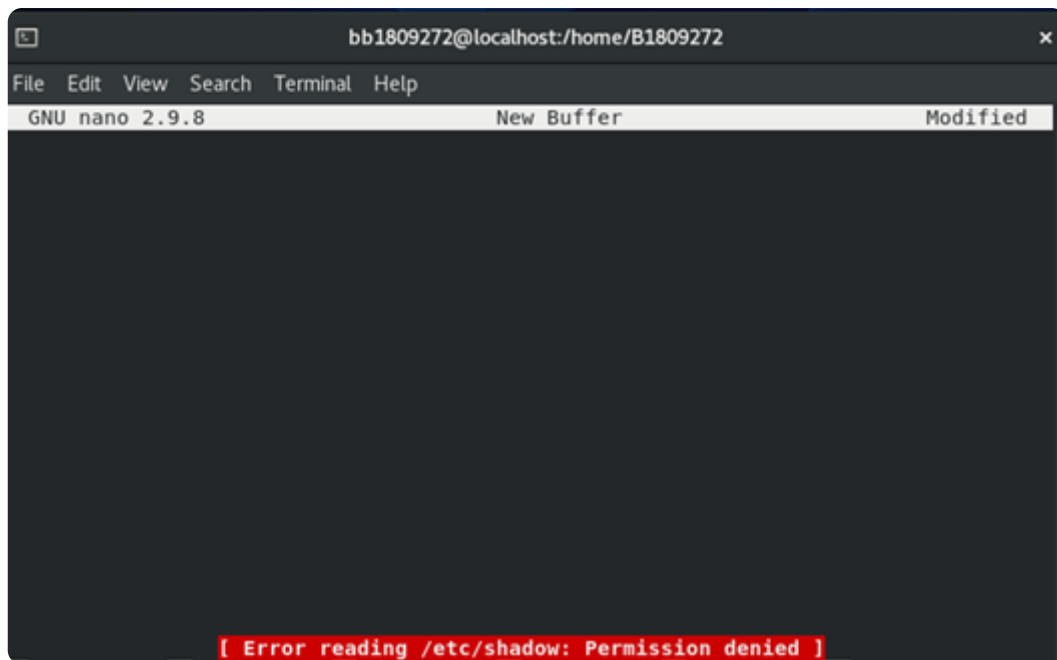
Thêm tài khoản **bb1809272** vào nhóm qtht: #usermod -aG qtht bb1809272

```
[root@localhost B1809272]# usermod -aG qtht bb1809272
[root@localhost B1809272]#
```

Đăng nhập vào tài khoản **bb1809272**: \$su bb1809272

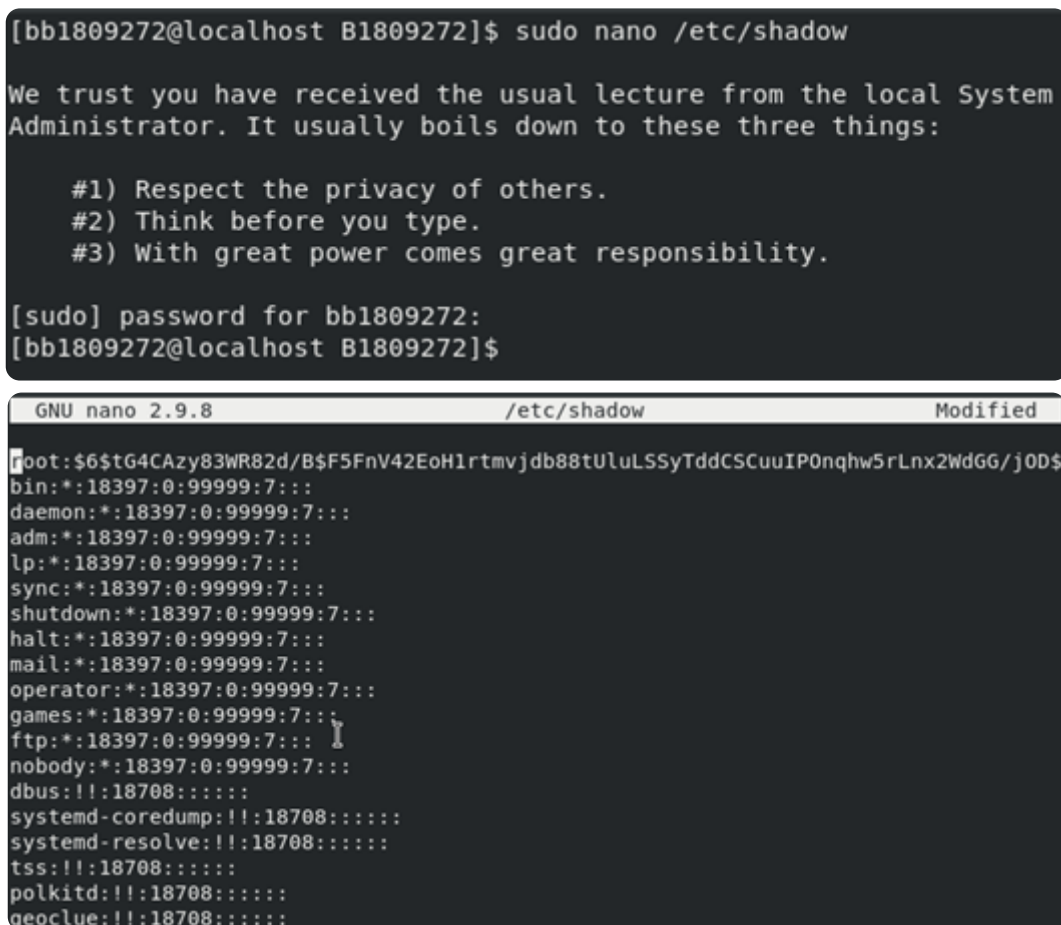
```
[B1809272@localhost ~]$ su bb1809272
Password:
[bb1809272@localhost B1809272]$ S
```

Xem nội dung file **/etc/shadow**: `$nano /etc/shadow`



### Bị từ chối

Xem lại với lệnh `$sudo nano /etc/shadow`



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

Xóa tài khoản **bb1809272** ra khỏi nhóm qtht

```
#gpasswd -d bb1809272 qtht
```

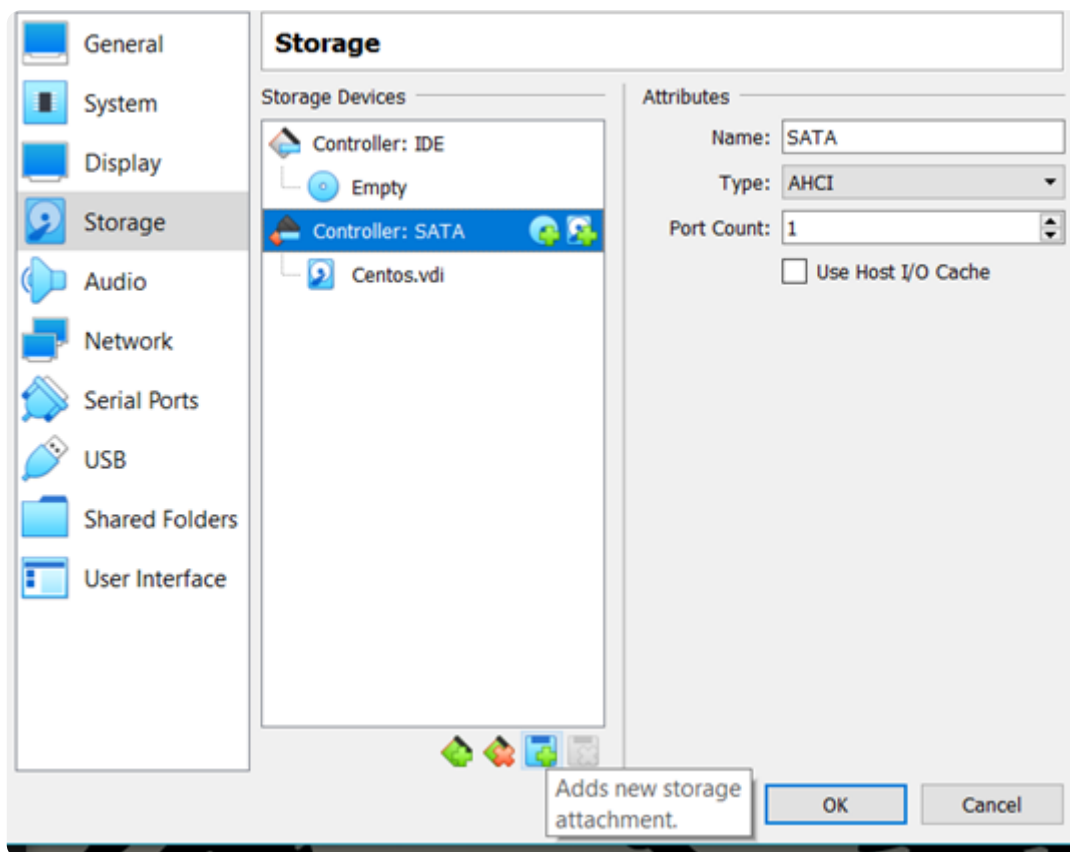
```
[root@localhost B1809272]# gpasswd -d bb1809272 qtht
Removing user bb1809272 from group qtht
[root@localhost B1809272]# groups bb1809272
bb1809272 : bb1809272 DI18V7A2
[root@localhost B1809272]#
```

#### 4. Đĩa và phân vùng ổ cứng

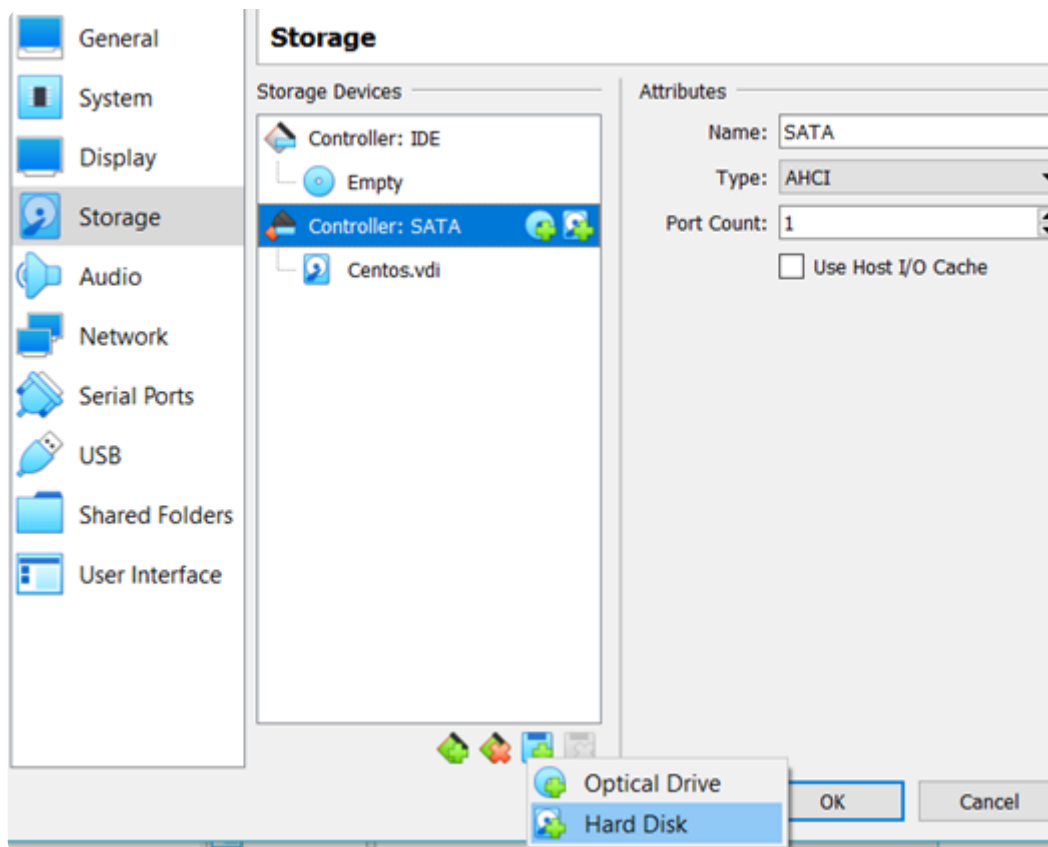
Tìm hiểu và thực hiện các yêu cầu sau:

**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.

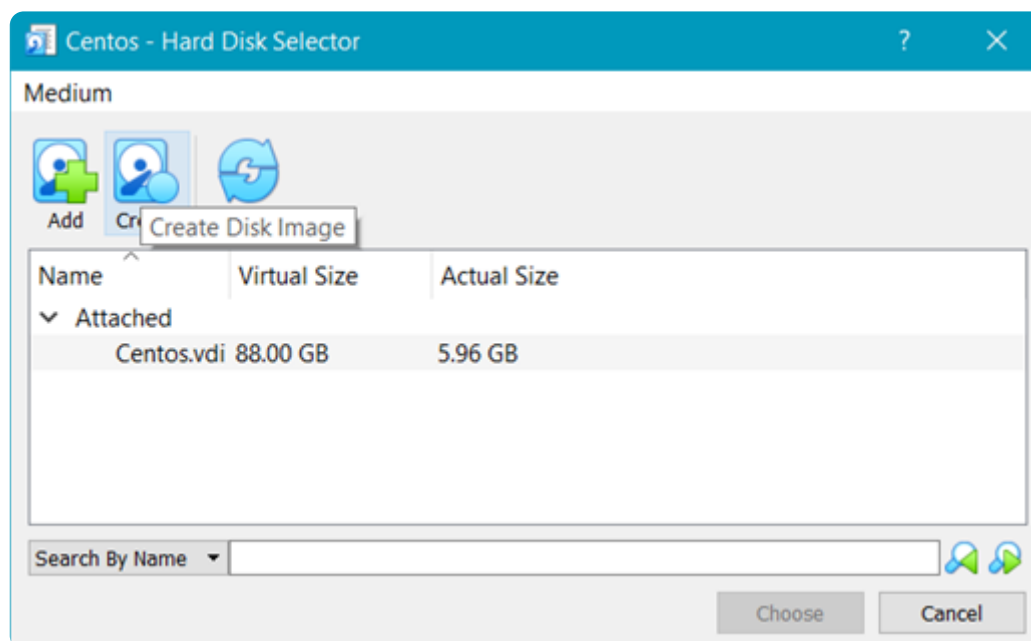
Chọn Adds new storage attachment



Chọn hard disk

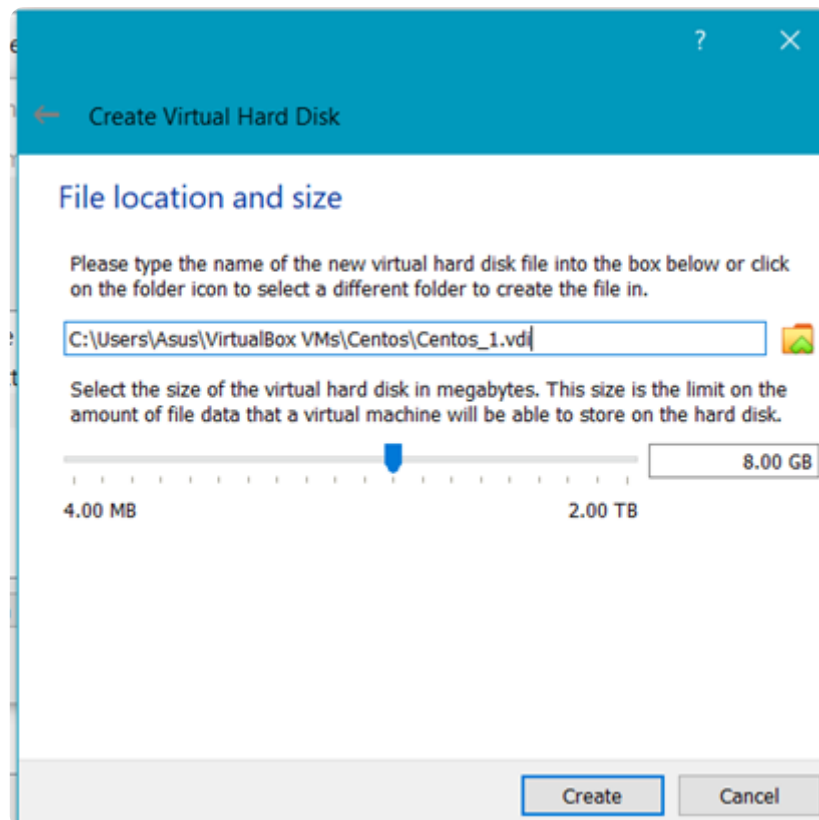


Chọn Create Disk Image

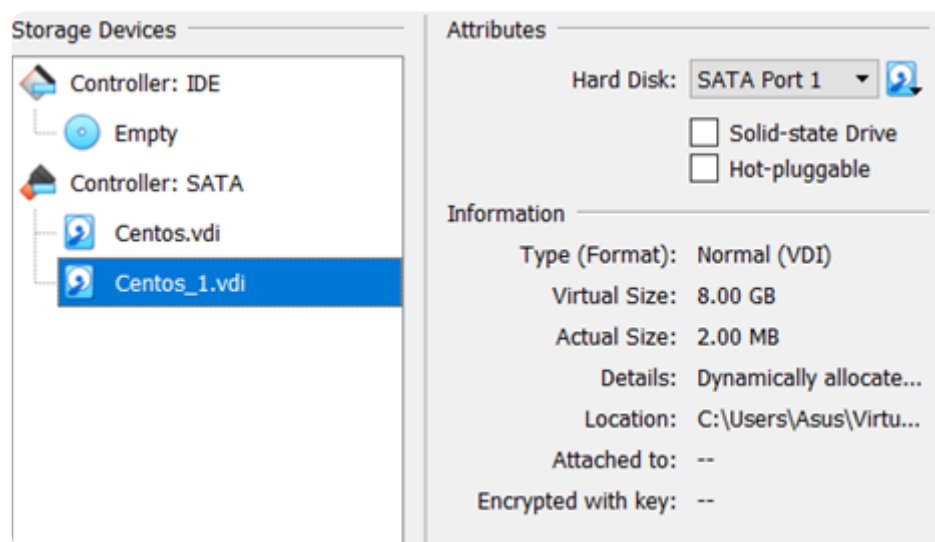


Tạo ổ cứng 8GB





Name	Virtual Size	Actual Size
Attached		
Centos.vdi	88.00 GB	5.96 GB
Not Attached		
Centos_1.vdi	8.00 GB	2.00 MB



**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)

`#fdisk -l` Xem danh sách các thông tin phân vùng ổ cứng



```
[root@localhost B1809272]# fdisk -l
Disk /dev/sdb: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sda: 88 GiB, 94489280512 bytes, 184549376 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x9f7e49c2

Device      Boot    Start        End    Sectors  Size Id Type
/dev/sda1   *         2048     2099199    2097152    1G 83 Linux
/dev/sda2             2099200 184549375 182450176    87G 8e Linux LVM

Disk /dev/mapper/cl-root: 55.8 GiB, 59907244032 bytes, 117006336 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/cl-swap: 4 GiB, 4257218560 bytes, 8314880 sectors
Units: sectors of 1 * 512 = 512 bytes
```

Tạo phân vùng cho ổ cứng: `#fdisk /dev/sdb`

```
[root@localhost B1809272]# fdisk /dev/sdb

Welcome to fdisk (util-linux 2.32.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0xcd8305b8.

Command (m for help):
```

Ý nghĩa các tham số:

**DOS (MBR)**

- a toggle a bootable flag
- b edit nested BSD disklabel
- c toggle the dos compatibility flag

**Generic**

- d delete a partition
- F list free unpartitioned space
- l list known partition types
- n add a new partition
- p print the partition table
- t change a partition type
- v verify the partition table
- i print information about a partition

**Misc**

- m print this menu
- u change display/entry units
- x extra functionality (experts only)

**Script**

- I load disk layout from sfdisk script file
- O dump disk layout to sfdisk script file

**Save & Exit**

- w write table to disk and exit
- q quit without saving changes

**Create a new label**

- g create a new empty GPT partition table
- G create a new empty SGI (IRIX) partition table
- o create a new empty DOS partition table
- s create a new empty Sun partition table

n: tạo phân vùng mới

partition type p: phân vùng chính

w: ghi các thông tin phân vùng ổ đĩa và thoát

```
#fdisk -l
```

Một phân vùng mới **/dev/sdb1** đã được tạo ra

```
[root@localhost B1809272]# fdisk -l
Disk /dev/sdb: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xcd8305b8

Device            Boot  Start        End    Sectors  Size Id Type
/dev/sdb1          1  2048 16777215 16775168   8G 83 Linux

Disk /dev/sda: 88 GiB, 94489280512 bytes, 184549376 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x9f7e49c2

Device            Boot  Start        End    Sectors  Size Id Type
/dev/sda1          *    2048    2099199    2097152   1G 83 Linux
/dev/sda2              2099200 184549375 182450176  87G 8e Linux LVM
```

```
#mkfs.ext4 /dev/sdb1
```

Format phân vùng ổ cứng ext4

```
[root@localhost B1809272]# mkfs.ext4 /dev/sdb1
mke2fs 1.45.6 (20-Mar-2020)
Creating filesystem with 2096896 4k blocks and 524288 inodes
Filesystem UUID: d44d9afe-597f-450a-8230-be15b09e1ced
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

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 tài khoản root. Mount phân vùng ổ cứng ở 4.2 tới thư mục /data (chụp hình minh họa)

```
#mkdir /data && mount /dev/sdb1 /data
```

```
[root@localhost B1809272]# mkdir /data && mount /dev/sdb1 /data
[root@localhost B1809272]#
```

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

```
[root@localhost B1809272]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        1.8G   0    1.8G   0% /dev
tmpfs           1.9G   0    1.9G   0% /dev/shm
tmpfs           1.9G  9.5M    1.9G   1% /run
tmpfs           1.9G   0    1.9G   0% /sys/fs/cgroup
/dev/mapper/cl-root 56G  4.9G   51G   9% /
/dev/mapper/cl-home 28G  361M   27G   2% /home
/dev/sda1       1014M  320M   695M  32% /boot
tmpfs           374M  1.2M   373M   1% /run/user/42
tmpfs           374M  4.6M   370M   2% /run/user/1000
/dev/sdb1       7.9G   36M    7.4G   1% /data
```

## 5. Phân quyền trên hệ thống tập tin

### 5.1. Tạo nhóm người dùng quantri, thêm người dùng ở 2.1 vào nhóm quantri

```
#groupadd quantri && usermod -aG quantri bb1809272
```

```
[root@localhost B1809272]# groupadd quantri && usermod -aG quantri bb1809272
[root@localhost B1809272]# groups bb1809272
bb1809272 : bb1809272 DI18V7A2 quantri
[root@localhost B1809272]#
```

5.2. Chuyển nhóm chủ sở hữu của thư mục **/data** sang quantri. Phân quyền cho thư mục **/data** là chủ sở hữu có toàn quyền read, write và execute, nhóm chủ sở hữu có quyền read và execute, những người khác không có quyền gì (chụp hình minh họa). Chuyển nhóm chủ sở hữu của thư mục **/data** sang **quantri**

```
#chgrp quantri /data
```

```
[root@localhost B1809272]# ls -l / | grep "data"
drwxr-xr-x.  2 root root 4096 Mar 23 04:13 data
[root@localhost B1809272]# chgrp quantri /data
[root@localhost B1809272]# ls -l / | grep "data"
drwxr-xr-x.  2 root quantri 4096 Mar 23 04:13 data
[root@localhost B1809272]#
```

Phân quyền cho thư mục **/data** là chủ sở hữu có toàn quyền read, write và execute, nhóm chủ sở hữu có quyền read và execute, những người khác không có quyền gì

```
#chmod 750 /data
```

```
[root@localhost B1809272]# ls -l / | grep "data"
drwxr-xr-x.  2 root quantri 4096 Mar 23 04:13 data
[root@localhost B1809272]# chmod 750 /data
[root@localhost B1809272]# ls -l / | grep "data"
drwxr-x---.  2 root quantri 4096 Mar 23 04:13 data
[root@localhost B1809272]#
```

5.3. Dùng tài khoản root 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).

```
[root@localhost B1809272]# touch /data/file1.txt
[root@localhost B1809272]# su bb1809272
[bb1809272@localhost B1809272]$ touch /data/file2.txt
touch: cannot touch '/data/file2.txt': Permission denied
[bb1809272@localhost B1809272]$
```

Người dùng bb1809272 không có quyền tạo file trong thư mục /data chỉ root mới có quyền write

```
[root@localhost B1809272]# ls -l / | grep "data"
drwxr-x---. 2 root quantri 4096 Mar 23 04:28 data
[root@localhost B1809272]#
```

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

```
[bb1809272@localhost B1809272]$ cat > /data/file1.txt
bash: /data/file1.txt: Permission denied
[bb1809272@localhost B1809272]$
```

Tài khoản bb1809272 không có quyền thay đổi nội dung tập tin vì chỉ có quyền read

```
[bb1809272@localhost B1809272]$ ls -l /data
total 0
-rw-r--r--. 1 root root 0 Mar 23 04:28 file1.txt
[bb1809272@localhost B1809272]$
```

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

```
[root@localhost B1809272]# ls -l /data/file1.txt
-rw-r--r--. 1 root root 0 Mar 23 04:28 /data/file1.txt
[root@localhost B1809272]# chmod o+w /data/file1.txt
[root@localhost B1809272]# ls -l /data/file1.txt
-rw-r--rw-. 1 root root 0 Mar 23 04:28 /data/file1.txt
[root@localhost B1809272]# cat > /data/file1.txt
thay doi noi dung thanh cong
^Z
[1]+  Stopped                  cat > /data/file1.txt
[root@localhost B1809272]# cat /data/file1.txt
thay doi noi dung thanh cong
[root@localhost B1809272]#
```

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

```
[root@localhost B1809272]# adduser newuser && passwd newuser
Changing password for user newuser.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost B1809272]# su newuser
[newuser@localhost B1809272]$ cat /data/file1.txt
cat: /data/file1.txt: Permission denied
[newuser@localhost B1809272]$ ls -l /data
ls: cannot open directory '/data': Permission denied
[newuser@localhost B1809272]$ su
Password:
[root@localhost B1809272]# ls -l /data
total 4
-rw-r--rw-. 1 root root 29 Mar 23 04:36 file1.txt
[root@localhost B1809272]# ls -l /data/file1.txt
-rw-r--rw-. 1 root root 29 Mar 23 04:36 /data/file1.txt
[root@localhost B1809272]#
```

Người dùng khác không có quyền đọc nội dung trong thư mục /data

```
[root@localhost B1809272]# ls -l / | grep "data"
drwxr-x---. 2 root quantri 4096 Mar 23 04:28 data
[root@localhost B1809272]#
```

--- Hết ---