

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



Họ tên và MSSV: Đỗ Khánh Toàn - B2012046

Nhóm học phần: 07

- 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: **tuân.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.

=>

```
b2012046@vnpt:/home/b2012046

[b2012046@localhost ~]$ su root
Password:
[root@localhost b2012046]# adduser toan.do
[root@localhost b2012046]# passwd toan.do
Changing password for user toan.do.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost b2012046]# nano /etc/passwd
[root@localhost b2012046]# ls /home/
b2012046  toan.do
[root@localhost b2012046]#
```

- 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).

=>

```
b2012046@vnpt:/home/b2012046 — nano /etc/shadow

GNU nano 5.6.1 /etc/shadow
geoclue:!!:19250::::::
tss:!!:19250::::::
cockpit-ws:!!:19250::::::
cockpit-wsinstance:!!:19250::::::
colord:!!:19250::::::
sssd:!!:19250::::::
setroubleshoot:!!:19250::::::
pipewire:!!:19250::::::
flatpak:!!:19250::::::
clevis:!!:19250::::::
gdm:!!:19250::::::
gnome-initial-setup:!!:19250::::::
sshd:!!:19250::::::
chrony:!!:19250::::::
dnsmasq:!!:19250::::::
tcpdump:!!:19250::::::
systemd-oom:!!:19250::::::
b2012046:$6$MHdVnCDkd/H.yyii$fmxzIXU7NLV03pPCY9SLUSiy6RjYP.NGNTua/HZv/F7gHzUc.L
toan.do:$y$j9T$i9y6bijJ4kc44aD5T8/zt0$dt3fIJQq0X45MAxojAobkqjtI8vEB0hFLQfaMj7QN>

^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
```

- 2.3.** Thiết lập ngày hết hạn cho tài khoản ở 2.1 là ngày 31/12/2022 (chụp hình minh hoạ).

=> thiết lập ngày hết hạn cho tài khoản toan.do là ngày 31/12/2022

```
b2012046@vnpt:/home/b2012046
[root@localhost b2012046]# usermod -e 12/31/2022 b2012046
```

Xem lại thông tin ngày hết hạn bằng cách:



```
[root@localhost b2012046]# chage -l toan.do
Last password change           : Sep 19, 2022
Password expires                : never
Password inactive              : never
Account expires                 : Dec 31, 2022
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
[root@localhost b2012046]#
```

- 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).

=> tạo 1 nhóm có tên là mã lớp: DI2095A2

```
[root@localhost b2012046]# groupadd DI2095A2
```

- Sau đó add tài khoản vào bằng cách

```
[root@localhost b2012046]# usermod -a -G DI2095A2 toan.do
```

- Check lại tài khoản toan.do thuộc groups nào bằng cách

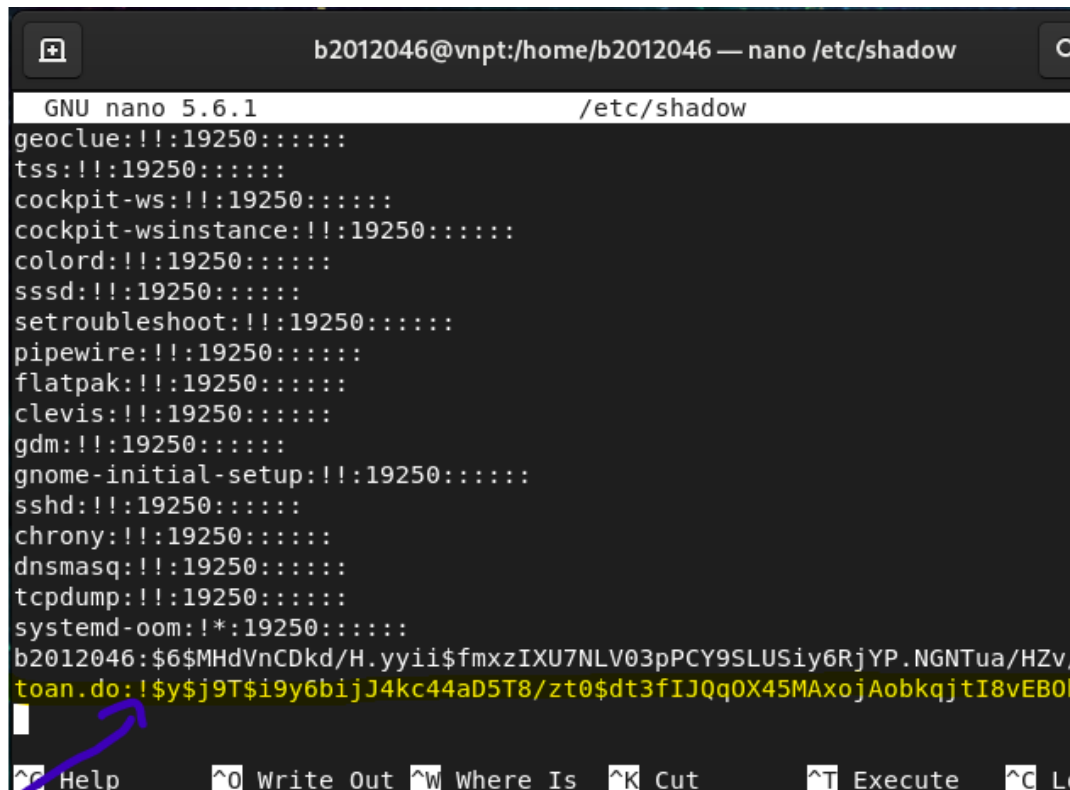
```
[root@localhost b2012046]# groups toan.do
toan.do : toan.do DI2095A2
[root@localhost b2012046]#
```

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

=> khóa 1 tài khoản người dùng là toan.do

```
[root@localhost b2012046]# usermod -L toan.do
```

- Để xem lại tài khoản ta gõ nano /etc/shadow ở đây tìm đến tài khoản toan.do ở phần mã hóa passwd ta thấy dc ở đầu có dấu "!" chứng minh tài khoản này đã được block



```
b2012046@vnpt:/home/b2012046 — nano /etc/shadow
GNU nano 5.6.1 /etc/shadow
geoclue:!!:19250::::::
tss:!!:19250::::::
cockpit-ws:!!:19250::::::
cockpit-wsinstance:!!:19250::::::
colord:!!:19250::::::
sssd:!!:19250::::::
setroubleshoot:!!:19250::::::
pipewire:!!:19250::::::
flatpak:!!:19250::::::
clevis:!!:19250::::::
gdm:!!:19250::::::
gnome-initial-setup:!!:19250::::::
sshd:!!:19250::::::
chrony:!!:19250::::::
dnsmasq:!!:19250::::::
tcpdump:!!:19250::::::
systemd-oom:!!:19250::::::
b2012046:$6$MhdVnCDkd/H.yyii$fmxzIXU7NLV03pPCY9SLUSiy6RjYP.NGNTua/HZV
toan.do:!:5y$j9T$i9y6bijJ4kc44aD5T8/zt0$dt3fIJQq0X45MAxoJAobkqjtI8vEB0
^H Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C L
```

LƯU Ý KHI KHÓA TÀI KHOẢN BẰNG user -L

- Tài khoản chỉ bị khóa khi đăng nhập bằng passwd
 - Trong 1 số trường hợp khác như không nhập passwd vd như chuyển từ tài khoản root sang tài khoản bị khóa thì vẫn có thể vào được
- => Giống như khóa passwd của tài khoản chứ ko khóa tài khoản

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

Lệnh usermod -U “tài khoản cần mở khóa” dùng để mở khóa tài khoản

```
[root@localhost b2012046]# usermod -U toan.do
```

=> như 2.5 khi kiểm tra nano /etc/shadow thì ở tài khoản toan.do passwd sẽ ko còn dấu “!” ở trước, lúc này passwd của tài khoản toan.do đã được mở khóa thành công

3. Quyền root (Root privilege) và sudo

Tìm hiểu và thực hiện các yêu cầu sau:

3.1. Quyền root là gì?

=>

- Root là tên người dùng hoặc là tài khoản theo mặc định có quyền truy cập vào tất cả các lệnh và file trên Linux và hệ điều hành giống Linux hoặc hệ điều hành Unix khác. Root 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)

=>

- Sudo có khả năng xác định các ràng buộc về việc người dùng có thể sử dụng sudo hay không và có thể sử dụng các lệnh nào với nó. Các tập tin có thể chỉnh sửa.
- Ngoài ra sudo còn là nhật kí được lưu giữ cho mọi lệnh, giúp dễ dàng theo dõi những lỗi đã thực hiện và sửa lỗi.
- Sudo không cần chia sẻ mật khẩu vì nó có thể nâng cao các đặc quyền của người dùng cá nhân và cho phép họ có quyền truy cập vào những thứ họ cần
- Các ưu điểm của sudo:
 - o Sudo thường bao gồm 1 lệnh khác trong khi Su thì không
 - o Sudo có các ràng buộc có thể xác định trong khi su thì không
 - o Sudo giữ 1 bản ghi của tất cả các lệnh trong khi Su thì không
 - o Bạn cần chia sẻ mật khẩu với Su nhưng không phải với sudo
 - o Sudo nâng cao các đặc quyền của người dùng trong khi su thì không

.....

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).

```
b2012046@vnpt:/home/b2012046 — sudo nano /etc/sudoers
GNU nano 5.6.1 /etc/sudoers
## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## 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

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)    ALL

## Same thing without a password

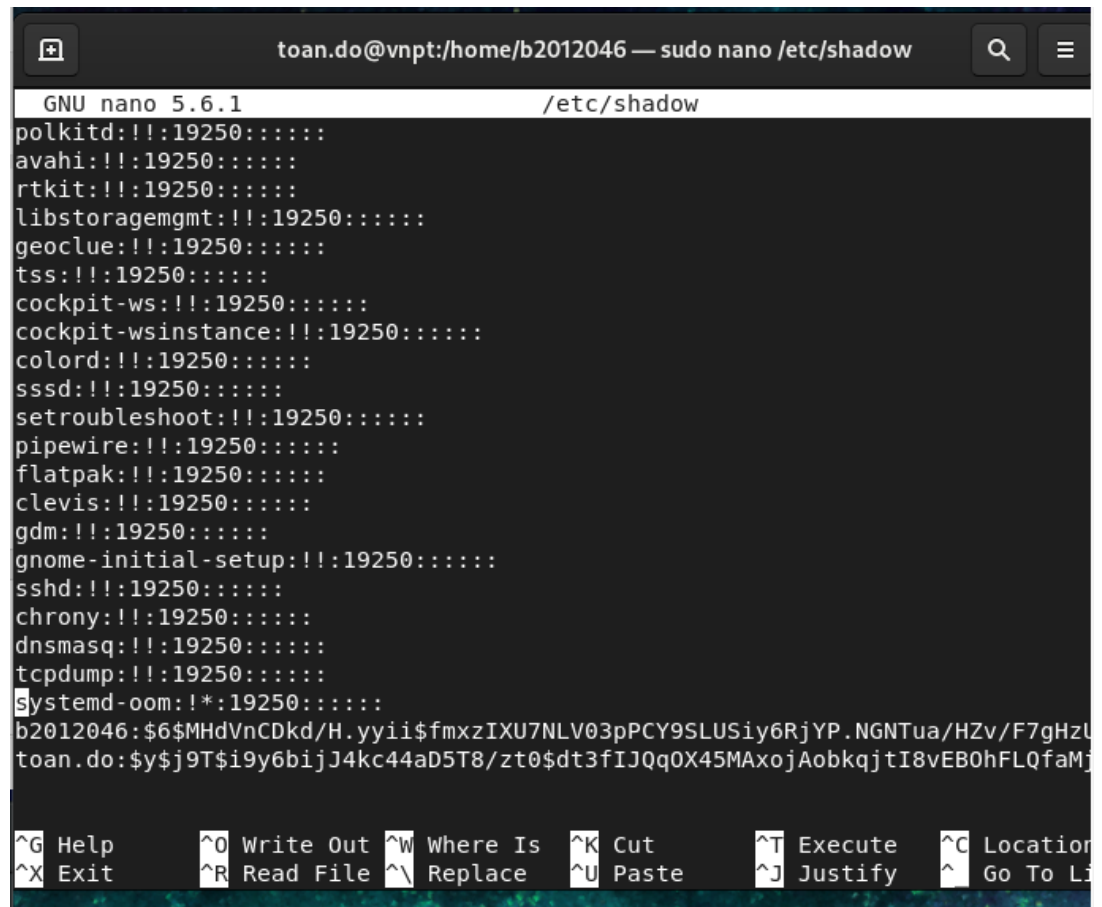
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To L
```

```
[root@localhost b2012046]# sudo nano /etc/sudoers
[root@localhost b2012046]# sudo usermod -aG wheel toan.do
[root@localhost b2012046]# groups toan.do
toan.do : toan.do wheel DI2095A2
[root@localhost b2012046]# su toan.do
[toan.do@localhost b2012046]$
```

1. Kiểm tra root
2. Cấp quyền sudo cho tài khoản toan.do
3. Kiểm tra tài khoản toan.do ở đây có dòng wheel
4. Truy cập vào tài khoản toan.do

```
[toan.do@localhost b2012046]$ sudo nano /etc/shadow
[sudo] password for toan.do:
```

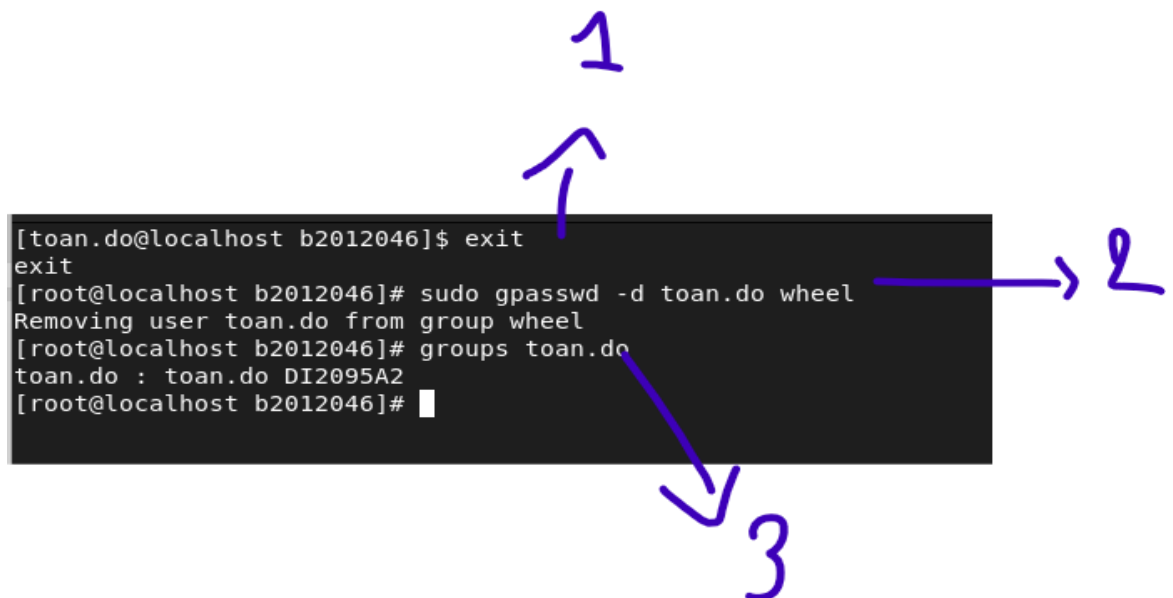
=> truy cập vào shadow bằng tài khoản toan.do



```
toan.do@vnpt:/home/b2012046 — sudo nano /etc/shadow
GNU nano 5.6.1 /etc/shadow
polkitd:!!:19250::::::
avahi:!!:19250::::::
rtkit:!!:19250::::::
libstoragemgmt:!!:19250::::::
geoclue:!!:19250::::::
tss:!!:19250::::::
cockpit-ws:!!:19250::::::
cockpit-wsinstance:!!:19250::::::
colord:!!:19250::::::
sssd:!!:19250::::::
setroubleshoot:!!:19250::::::
pipewire:!!:19250::::::
flatpak:!!:19250::::::
clevis:!!:19250::::::
gdm:!!:19250::::::
gnome-initial-setup:!!:19250::::::
sshd:!!:19250::::::
chrony:!!:19250::::::
dnsmasq:!!:19250::::::
tcpdump:!!:19250::::::
systemd-oom:!!:19250::::::
b2012046:$6$MHDVnCDkd/H.yyii$fmxzIXU7NLV03pPCY9SLUSiy6RjYP.NGNTua/HZv/F7gHzU
toan.do:$y$j9T$i9y6bijJ4kc44aD5T8/zt0$dt3fIJQq0X45MAxojAobkqjtI8vEB0hFLQfaMj
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify  ^_ Go To Li
```

- Ở đây chúng ta đã truy cập và shadow thành công
- Từ thời điểm này tài khoản toan.do có thể thay thế tài khoản root

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



```
[toan.do@localhost b2012046]$ exit
exit
[root@localhost b2012046]# sudo gpasswd -d toan.do wheel
Removing user toan.do from group wheel
[root@localhost b2012046]# groups toan.do
toan.do : toan.do DI2095A2
[root@localhost b2012046]#
```

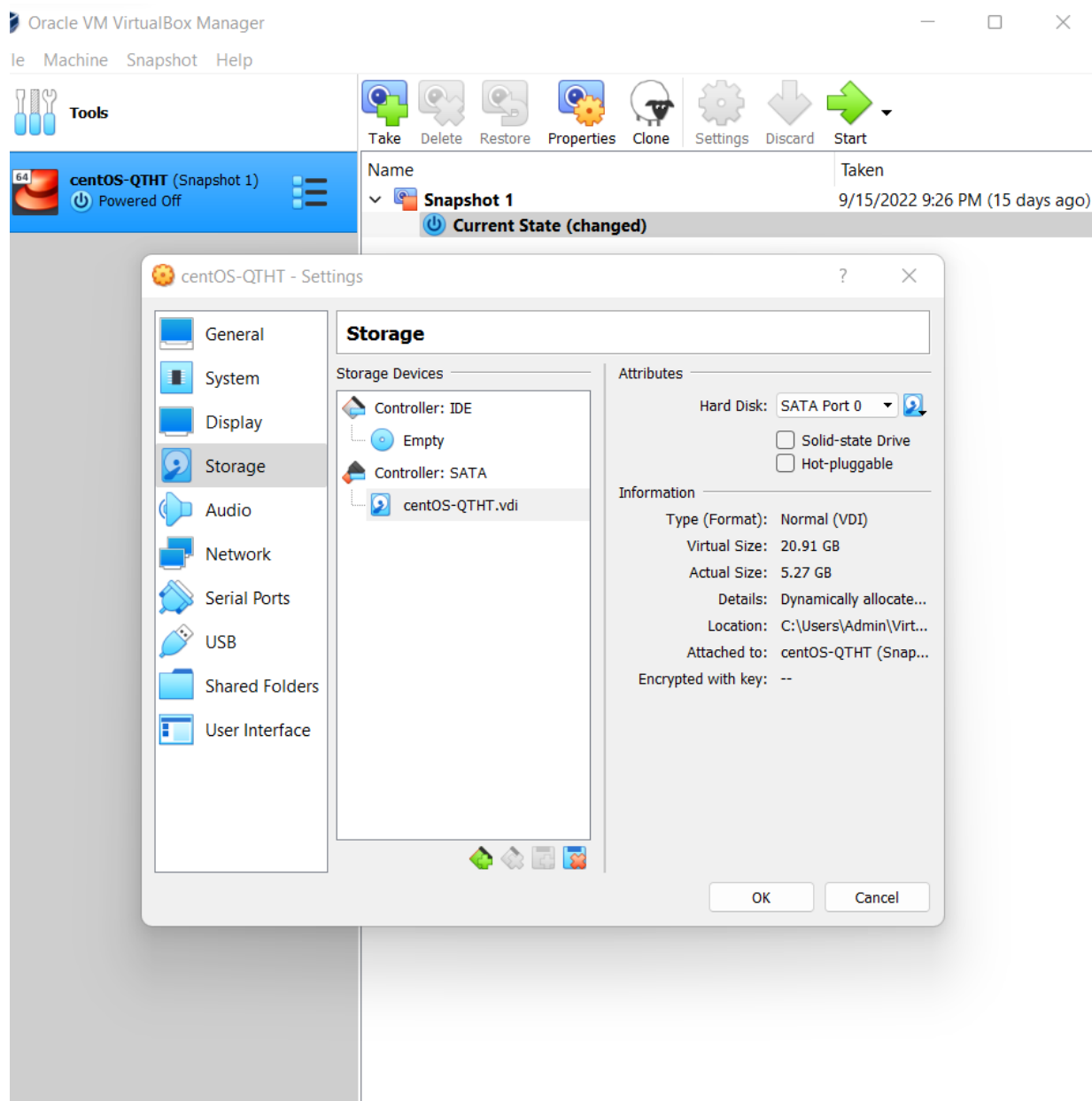
1. Vào tài khoản root để hủy quyền sudo cho tài khoản toan.do

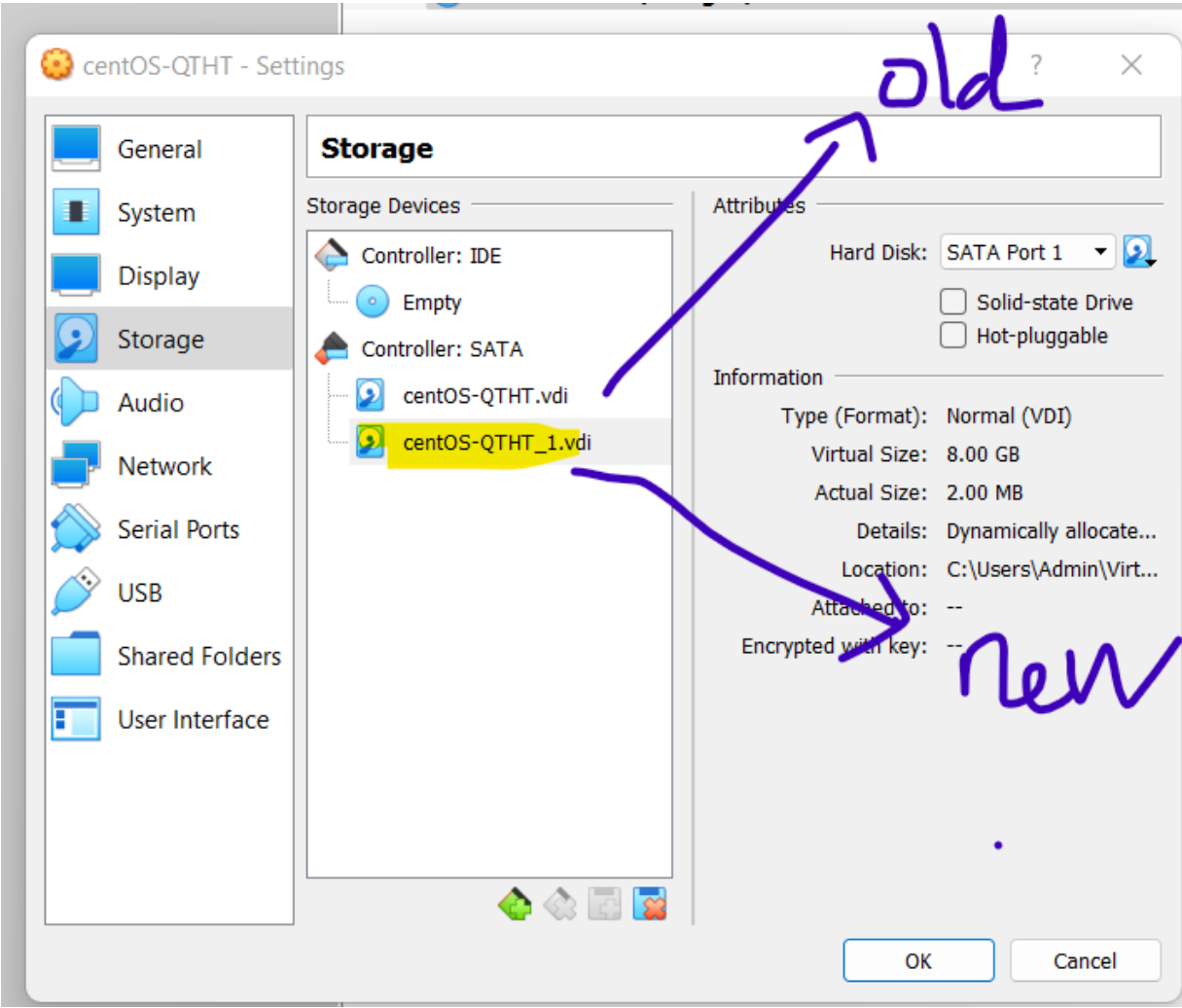
2. Hủy quyền sudo cho tài khoản toan.do
3. Kiểm tra lại bằng groups toan.do
=> ở đây cùng cuối chúng ra sẽ ko thấy wheel vậy chúng ta đã hủy quyền sudo cho tài khoản toan.do thành công

4. Đĩa và phân vùng ổ cứng

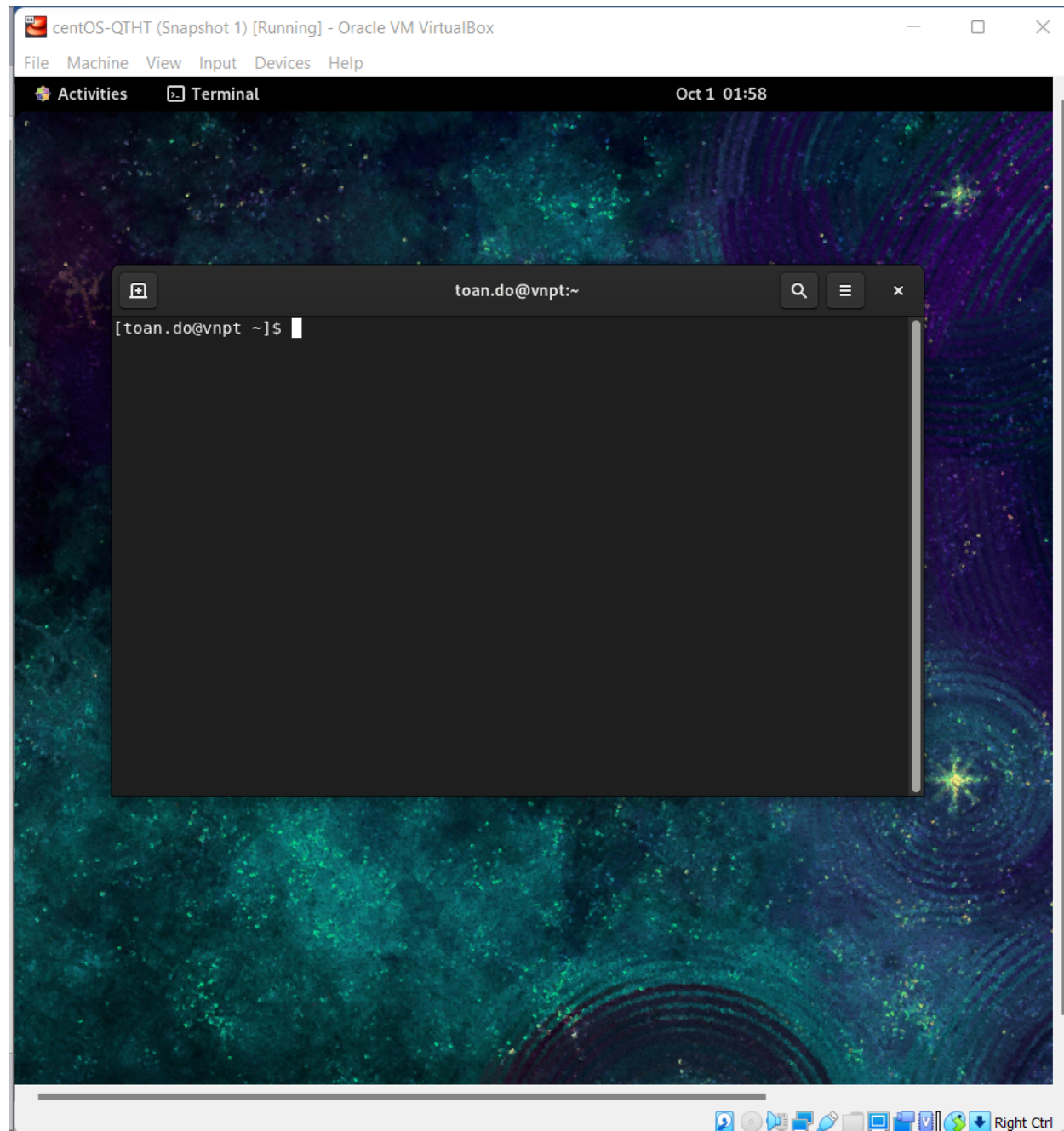
Tìm hiểu và thực hiện các yêu cầu sau:

- 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.





=>



=> tạo thành công

```
[root@vnpt toan.do]# sudo fdisk /dev/sdb
```

```
Welcome to fdisk (util-linux 2.37.4).
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 0x90c07094.
```

```
Command (m for help):
```

- Ở đây gõ phím n để tạo phân vùng mới

```
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):
```

```
First sector (2048-16777215, default 2048): 2048
```

```
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-16777215, default 16777215):
```

```
Created a new partition 1 of type 'Linux' and of size 8 GiB.
```

```
Command (m for help):
```

1. Chọn vùng chính => p
2. Số lượng phân vùng cần tạo => 1
3. Kích thước ổ cứng mặc định => 2048
4. Phân vùng cuối cùng mặc định sector 8Gib

```
Command (m for help): w
```

```
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

=> phân vùng được tạo thành công


- 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)

```
[root@vnpt toan.do]# sudo fdisk -l

Disk /dev/sda: 20.91 GiB, 22450962432 bytes, 43849536 sectors
Disk model: VBOX HARDDISK
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: 0x657c1d5a

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sda1   *        2048     2099199    2097152     1G 83 Linux
/dev/sda2                2099200  43847679  41748480    19.9G 8e Linux LVM

Disk /dev/sdb: 8 GiB, 8589934592 bytes, 16777216 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```



=> ở đây chúng ta sẽ phân vùng cho ổ cứng SDB

```
[root@vnpt toan.do]# sudo mkfs.ext4 /dev/sdb1
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 2096896 4k blocks and 524288 inodes
Filesystem UUID: 70807294-1441-4fb6-ae56-37dc29d7a808
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

[root@vnpt toan.do]#
```

=> thành công

- 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)

```
[root@vnpt toan.do]# sudo mkdir /data
[root@vnpt toan.do]# ls /
afs  boot  dev  home  lib64  mnt  proc  run  srv  tmp  var
bin  data  etc  lib   media  opt  root  sbin  sys  usr
```



=> tạo data trong thư mục gốc

```
[root@vnpt toan.do]# sudo mount /dev/sdb1 /data
```

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

```
[root@vnpt toan.do]# sudo df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M   0    4.0M   0% /dev
tmpfs           886M   0    886M   0% /dev/shm
tmpfs           355M  5.6M   349M   2% /run
/dev/mapper/cs-root 18G   4.3G   14G   24% /
/dev/sda1       1014M  284M   731M   28% /boot
tmpfs           178M  124K   177M   1% /run/user/1001
/dev/sdb1       7.8G   24K    7.4G   1% /data
[root@vnpt toan.do]#
```

5. Phân quyền trên hệ thống tập tin

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

Tạo nhóm `nhanvien`

```
[root@vnpt toan.do]# sudo groupadd nhanvien
```

Thêm người dùng `toan.do` vào nhóm `nhanvien`

```
[root@vnpt toan.do]# sudo usermod -a -G nhanvien toan.do
```

Kiểm tra xem `toan.do` đã thuộc nhóm `nhanvien` chưa

```
[root@vnpt toan.do]# groups toan.do
toan.do : toan.do DI2095A2 nhanvien
[root@vnpt toan.do]#
```


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).

```
toan.do@vnpt:/home/toan.do
[root@vnpt toan.do]# ls -l /
total 28
dr-xr-xr-x.  2 root root   6 Aug  9  2021 afs
lrwxrwxrwx.  1 root root   7 Aug  9  2021 bin -> usr/bin
dr-xr-xr-x.  5 root root 4096 Sep 15 10:15 boot
drwxr-xr-x.  3 root root 4096 Oct  1 02:14 data
drwxr-xr-x. 20 root root 3380 Oct  1 02:09 dev
drwxr-xr-x. 130 root root 8192 Oct  1 02:24 etc
drwxr-xr-x.  4 root root   37 Sep 19 05:56 home
lrwxrwxrwx.  1 root root   7 Aug  9  2021 lib -> usr/lib
lrwxrwxrwx.  1 root root   9 Aug  9  2021 lib64 -> usr/lib64
drwxr-xr-x.  2 root root   6 Aug  9  2021 media
drwxr-xr-x.  2 root root   6 Aug  9  2021 mnt
drwxr-xr-x.  2 root root   6 Aug  9  2021 opt
dr-xr-xr-x. 249 root root   0 Oct  1 01:55 proc
dr-xr-x--.  3 root root  169 Oct  1 02:00 root
drwxr-xr-x. 43 root root 1160 Oct  1 02:14 run
lrwxrwxrwx.  1 root root   8 Aug  9  2021 sbin -> usr/sbin
drwxr-xr-x.  2 root root   6 Aug  9  2021 srv
dr-xr-xr-x. 13 root root   0 Oct  1 01:55 sys
drwxrwxrwt. 14 root root 4096 Oct  1 02:01 tmp
drwxr-xr-x. 12 root root  144 Sep 15 10:04 usr
drwxr-xr-x. 20 root root 4096 Sep 15 10:15 var
[root@vnpt toan.do]#
```

=> chủ sở hữu của data là tài khoản root => vì tạo data bằng sudo

```
[root@vnpt toan.do]# sudo chown :nhanvien /data
```

=> chuyển chủ sang nhanvien



```
[root@vnpt toan.do]# ls -l /
total 28
dr-xr-xr-x.  2 root root      6 Aug  9  2021 afs
lrwxrwxrwx.  1 root root      7 Aug  9  2021 bin -> usr/bin
dr-xr-xr-x.  5 root root 4096 Sep 15 10:15 boot
drwxr-xr-x.  3 root nhanvien 4096 Oct  1 02:14 data
drwxr-xr-x. 20 root root 3380 Oct  1 02:09 dev
drwxr-xr-x. 130 root root 8192 Oct  1 02:24 etc
drwxr-xr-x.  4 root root   37 Sep 19 05:56 home
lrwxrwxrwx.  1 root root      7 Aug  9  2021 lib -> usr/lib
lrwxrwxrwx.  1 root root      9 Aug  9  2021 lib64 -> usr/lib64
drwxr-xr-x.  2 root root      6 Aug  9  2021 media
drwxr-xr-x.  2 root root      6 Aug  9  2021 mnt
drwxr-xr-x.  2 root root      6 Aug  9  2021 opt
dr-xr-xr-x. 249 root root      0 Oct  1 01:55 proc
dr-xr-x-x-.  3 root root  169 Oct  1 02:00 root
drwxr-xr-x. 43 root root 1160 Oct  1 02:14 run
lrwxrwxrwx.  1 root root      8 Aug  9  2021/sbin -> usr/sbin
drwxr-xr-x.  2 root root      6 Aug  9  2021 srv
dr-xr-xr-x. 13 root root      0 Oct  1 01:55 sys
drwxrwxrwt. 14 root root 4096 Oct  1 02:01 tmp
drwxr-xr-x. 12 root root   144 Sep 15 10:04 usr
drwxr-xr-x. 20 root root 4096 Sep 15 10:15 var
[root@vnpt toan.do]#
```

=> chuyển thành công


```
[root@vnpt toan.do]# sudo chmod 750 /data
[root@vnpt toan.do]# ls -l /
total 28
dr-xr-xr-x.  2 root root      6 Aug  9  2021 afs
lrwxrwxrwx.  1 root root      7 Aug  9  2021 bin -> usr/bin
dr-xr-xr-x.  5 root root 4096 Sep 15 10:15 boot
drwxr-xr-x.  3 root nhanvien 4096 Oct  1 02:14 data
drwxr-xr-x. 20 root root 3380 Oct  1 02:09 dev
drwxr-xr-x. 130 root root 8192 Oct  1 02:24 etc
drwxr-xr-x.  4 root root   37 Sep 19 05:56 home
lrwxrwxrwx.  1 root root      7 Aug  9  2021 lib -> usr/lib
lrwxrwxrwx.  1 root root      9 Aug  9  2021 lib64 -> usr/lib64
drwxr-xr-x.  2 root root      6 Aug  9  2021 media
drwxr-xr-x.  2 root root      6 Aug  9  2021 mnt
drwxr-xr-x.  2 root root      6 Aug  9  2021 opt
dr-xr-xr-x. 250 root root    0 Oct  1 01:55 proc
dr-xr-xr-x.  3 root root   169 Oct  1 02:00 root
drwxr-xr-x. 43 root root  1160 Oct  1 02:14 run
lrwxrwxrwx.  1 root root      8 Aug  9  2021/sbin -> usr/sbin
drwxr-xr-x.  2 root root      6 Aug  9  2021 srv
dr-xr-xr-x. 13 root root    0 Oct  1 01:55 sys
drwxrwxrwt. 14 root root 4096 Oct  1 02:52 tmp
drwxr-xr-x. 12 root root   144 Sep 15 10:04 usr
drwxr-xr-x. 20 root root 4096 Sep 15 10:15 var
[root@vnpt toan.do]#
```

- 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).

=>

Tạo tập tin file1.txt

```
[root@vnpt toan.do]# sudo touch /data/file1.txt
[root@vnpt toan.do]#
```

```
[root@vnpt toan.do]# sudo ls -l /data
total 16
-rw-r--r--. 1 root root    0 Oct  1 03:00 file1.txt
drwx-----. 2 root root 16384 Oct  1 02:14 lost+found
[root@vnpt toan.do]#
```

Sau đó

Vào tài khoản toan.do, tạo file2.txt

```
[root@vnpt toan.do]# su toan.do
[toan.do@vnpt ~]$ touch /data/file2.txt
touch: cannot touch '/data/file2.txt': Permission denied
```


Ở đây đương nhiên sẽ báo lỗi vì tài khoản toan.do lúc này ko có quyền tạo

```
[toan.do@vnpt ~]$ ls -l /
total 28
dr-xr-xr-x.  2 root root      6 Aug  9  2021 afs
lrwxrwxrwx.  1 root root      7 Aug  9  2021 bin -> usr/bin
dr-xr-xr-x.  5 root root    4096 Sep 15 10:15 boot
drwxr-x---.  3 root nhanvien 4096 Oct  1 03:00 data
drwxr-xr-x. 20 root root    3380 Oct  1 02:09 dev
drwxr-xr-x. 130 root root    8192 Oct  1 02:24 etc
drwxr-xr-x.  4 root root      37 Sep 19 05:56 home
lrwxrwxrwx.  1 root root      7 Aug  9  2021 lib -> usr/lib
```

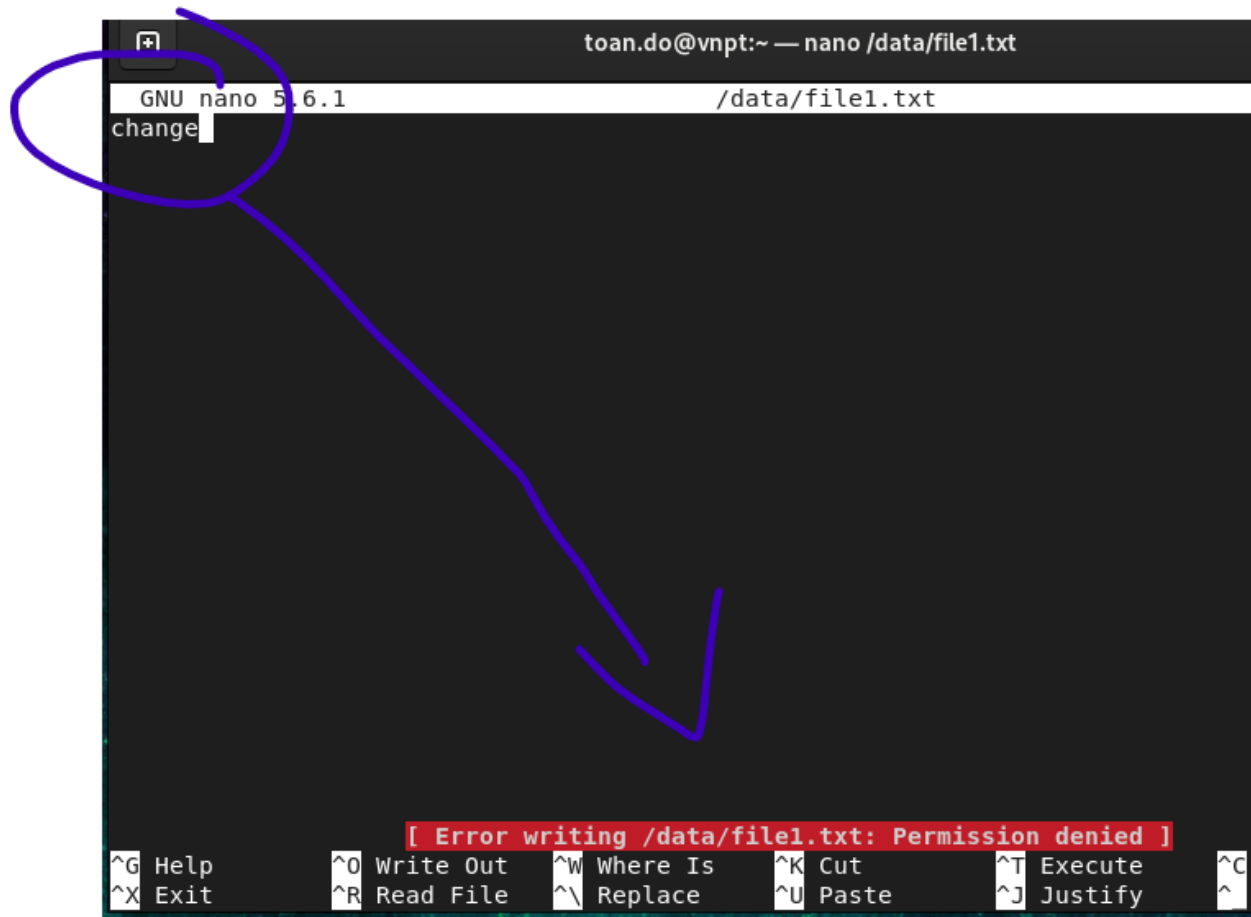
- 5.4. Dùng tài khoản ở 2.1 *mở và thay đổi nội dung* tập tin `/data/file1.txt`, cho biết kết quả (chụp hình minh họa).

=>

Truy cập vào file1.txt bằng cách nano `/data/file1.txt`

The screenshot shows the nano text editor interface. At the top, the title bar reads "toan.do@vnpt:~ — nano /data/file1.txt". Below it, the status bar shows "GNU nano 5.6.1" and the file path "/data/file1.txt". The main editing area is empty. At the bottom, a red error message is displayed: "[File '/data/file1.txt' is unwritable]". Below the error message, the nano editor's command shortcuts are listed: ^G Help, ^O Write Out, ^W Where Is, ^K Cut, ^T Execute, ^C Location, ^X Exit, ^R Read File, ^\ Replace, ^U Paste, ^J Justify, and ^_ Go To Line.

Ở đây tuy nhiên đã vào đc file1.txt nhưng chúng ta có thể xem bên trong mà không thể thay đổi được dữ liệu



```
toan.do@vnpt:~ — nano /data/file1.txt
GNU nano 5.6.1 /data/file1.txt
change

[ Error writing /data/file1.txt: Permission denied ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^
```

Lý do là vì tài khoản toan.do chỉ có quyền read, ko có quyền để thay đổi tập tin

```
[toan.do@vnpt ~]$
[toan.do@vnpt ~]$ ls -l /data/file1.txt
-rw-r--r--. 1 root root 0 Oct  1 03:00 /data/file1.txt
[toan.do@vnpt ~]$
```

Chúng ta chỉ được thay đổi khi cấp quyền cho toan.do hoặc exit vào root chạy chương trình bằng sudo

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

Đầu tiên cần chuyển tài khoản sang tài khoản root để cấp quyền cho toan.do

```
[toan.do@vnpt ~]$ exit
exit
[root@vnpt toan.do]# sudo chmod o+w /data/file1.txt
[root@vnpt toan.do]#
```

Sau đó chúng ra kiểm tra lại



```
[root@vnpt toan.do]# sudo ls -l /data
total 16
-rw-r--rw-. 1 root root    0 Oct  1 03:00 file1.txt
drwx----- 2 root root 16384 Oct  1 02:14 lost+found
[root@vnpt toan.do]#
```

Lúc này đã được cấp quyền thành công
Sau đó chuyển về tài khoản toan.do

```
[root@vnpt toan.do]# su toan.do
[toan.do@vnpt ~]$ nano /data/file1.txt
```


Nhập thông tin cần thay đổi

```
toan.do@vnpt:~ — nano /data/file1.txt
GNU nano 5.6.1 /data/file1.txt
day la file1 do tai khoan toan.do thay doi
[ Wrote 1 line ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Locati
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To
```

Thế là chúng ta đã cấp quyền write cho tài khoản toan.do thành công

- 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).

```
[root@vnpt toan.do]# sudo adduser newuser  
[redacted]  
[redacted]  
[root@vnpt toan.do]# sudo 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@vnpt toan.do]# su newuser  
[newuser@vnpt toan.do]$
```



```
[root@vnpt toan.do]# su newuser
[newuser@vnpt toan.do]$ nano /data/file1.txt
```



```
newuser@vnpt:/home/toan.do — 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
```

LÝ DO:

- Tài khoản newuser có quyền r và w tuy nhiên muốn vào file1.txt thì tài khoản newuser phải đi qua được thư mục data nhưng newuser là các tài khoản khác và nó ko có quyền gì trên thư mục data

```
drwxr-x---
```



- Nếu cố gắng truy cập vào chương trình trong thư mục data cũng ko thể được mặc dù đã có quyền r và w.
- Ở tài khoản toan.do có thể truy cập vào đc file1.txt là vì nó nằm trong nhóm nhân viên

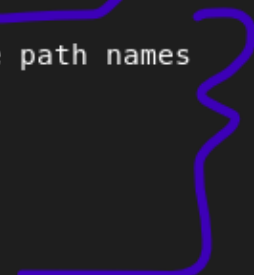
5.7. Dùng quyền sudo tạo thư mục /report và tạo nhóm người dùng quantri. Phân quyền trên thư mục /report sao cho nhóm quantri có quyền read, write và execute, nhóm nhanvien có quyền read và execute, người dùng ở 2.1 có quyền execute, những người khác không có bất kỳ quyền gì cả (chụp hình minh họa).

=>

```
[newuser@vnpt toan.do]$ exit
exit
[root@vnpt toan.do]# sudo mkdir /report
[root@vnpt toan.do]# sudo groupadd quantri
[root@vnpt toan.do]# getfacl /report
getfacl: Removing leading '/' from absolute path names
# file: report
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

[root@vnpt toan.do]#
```

1 2 3



1. Tạo thư mục report
2. Tạo nhóm quantri
3. Kiểm tra quyền của thư mục report

ACL entries

setfacl recognizes the following ACL entry formats (spaces in the following formats are optional, but are included for legibility):

<code>[d[efault]:] [u[ser]:]uid[:perms]</code>	Permissions of the user with user ID <i>uid</i> , or permissions of the file's owner if <i>uid</i> is empty.
<code>[d[efault]:] g[roup]:gid[:perms]</code>	Permissions of the group with group ID <i>gid</i> , or permissions of the owning group if <i>gid</i> is empty.
<code>[d[efault]:] m[ask][:][:perms]</code>	Effective rights mask.
<code>[d[efault]:] o[ther][:][:perms]</code>	Permissions of others.

Bước tiếp theo là cấp quyền rwx cho report

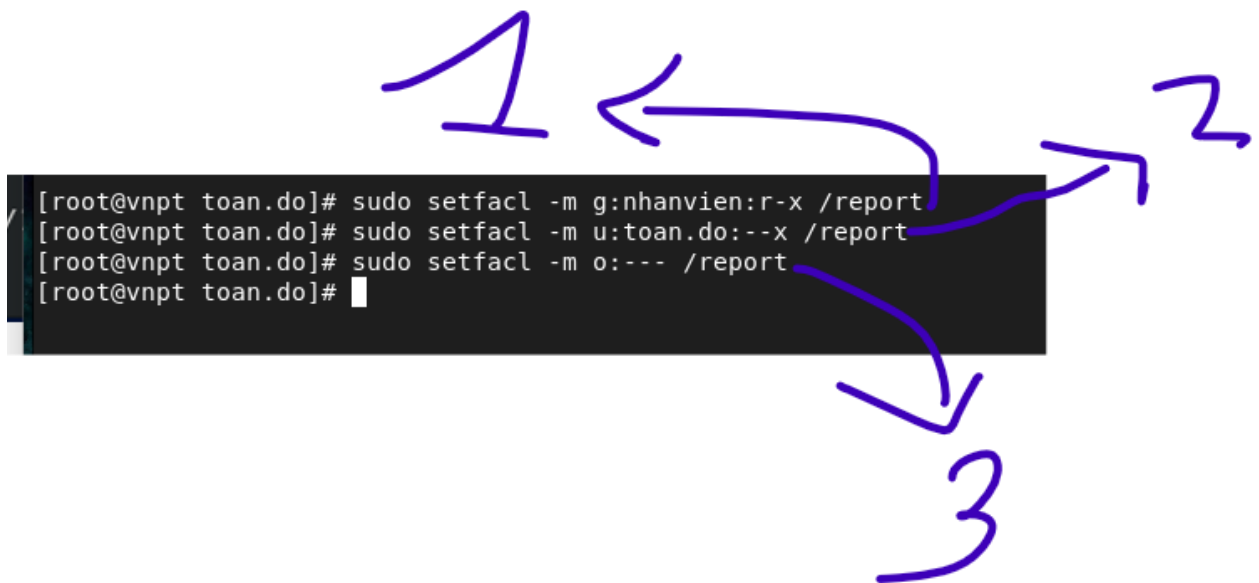
```
[root@vnpt toan.do]# sudo setfacl -m g:quantri:rwx /report
[root@vnpt toan.do]#
```



```
[root@vnpt toan.do]# 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

[root@vnpt toan.do]#
```

Cấp quyền cho quantri thành công



```
[root@vnpt toan.do]# sudo setfacl -m g:nhanvien:r-x /report
[root@vnpt toan.do]# sudo setfacl -m u:toan.do:--x /report
[root@vnpt toan.do]# sudo setfacl -m o:--- /report
[root@vnpt toan.do]#
```

Handwritten annotations: A large '1' with an arrow pointing to the first command, a '2' with an arrow pointing to the second command, and a '3' with an arrow pointing to the third command.

Tương tự như vậy ở đây :

1. Là lệnh cấp quyền r và x cho nhân viên
2. Là lệnh cấp quyền x cho tài khoản toan.do
3. Là lệnh ko cấp quyền nào cả cho các đối tượng khác

KẾT QUẢ:

```
[root@vnpt toan.do]# getfacl /report
getfacl: Removing leading '/' from absolute path names
# file: report
# owner: root
# group: root
user::rwx
user:toan.do:--x
group::r-x
group:nhanvien:r-x
group:quantri:rwx
mask::rwx
other:---
[root@vnpt toan.do]#
```

--- Hết ---