

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



Họ tên và MSSV: Phạm Minh Sáng

Nhóm học phần: 06

- 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: **tuan.thai**). (chụp hình minh họa).

+Lệnh **sudo adduser sang.pham**

```
[b2110976@localhost ~]$ sudo adduser sang.pham
[sudo] password for b2110976:
[b2110976@localhost ~]$
```

+Lệnh **sudo passwd sang.pham**

```
[b2110976@localhost ~]$ sudo passwd sang.pham
Changing password for user sang.pham.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[b2110976@localhost ~]$
```

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.

+Lệnh **nano /etc/passwd**

```
b2110976:x:1000:1000:Pham Minh Sang:/home/b2110976:/bin/bash
vboxadd:x:978:1::/var/run/vboxadd:/bin/false
sang.pham:x:1001:1001::/home/sang.pham:/bin/bash
```

- 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)
+Lệnh **sudo nano /etc/shadow**

```
b2110976:$6$1/Npk.ZpWoqnCG6b$RPzJQAfPn8BmtNHV9RM2N0AJkDTsEV4uopSbTUJymoVyxNWQHA>
vboxadd:!!:19601:::
sang.pham:$6$QcLlqWU407.7NfNF$v9GnzWki/Iu61i5TQUn8gAs8TPXyULVR/nAUAC5.Yk22suwys>
```

+Mật khẩu vừa tạo cho tài khoản ở câu 2.1 sử dụng giải thuật băm SHA-512
+Dựa vào ký tự (số 6) nằm giữa hai ký tự \$ đầu tiên ngay sau username là ký tự chỉ giải thuật băm

- 2.3.** Thiết lập ngày hết hạn cho tài khoản ở 2.1 là ngày 31/12/2023 (chụp hình minh họa).
+Lệnh **sudo usermod -e 12/31/2023**

```
[b2110976@localhost ~]$ sudo usermod -e 12/31/2023 sang.pham
[sudo] password for b2110976:
[b2110976@localhost ~]$
```

+Xem thông tin chi tiết bằng lệnh **sudo chage -l sang.pham**

```
[b2110976@localhost ~]$ sudo chage -l sang.pham
Last password change                : Sep 12, 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
[b2110976@localhost ~]$
```

- 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).
+Lệnh tạo nhóm **sudo groupadd di21t9a2**

```
[b2110976@localhost ~]$ sudo groupadd di21t9a2
[sudo] password for b2110976:
```

+Đưa tài khoản ở câu 2.1 vào group vừa tạo **sudo usermod -a -G di21t9a2 sang.pham**

```
[b2110976@localhost ~]$ sudo usermod -a -G di21t9a2 sang.pham
[b2110976@localhost ~]$ groups sang.pham
sang.pham : sang.pham di21t9a2
```

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

+Lệnh **sudo usermod -L sang.pham** để khóa tài khoản sang.pham

```
[b2110976@localhost ~]$ sudo usermod -L sang.pham
[b2110976@localhost ~]$ su sang.pham
Password:
su: Authentication failure
[b2110976@localhost ~]$
```

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

+Lệnh **sudo usermod -U sang.pham** để mở khóa tài khoản sang.pham

```
[b2110976@localhost ~]$ sudo usermod -U sang.pham
[b2110976@localhost ~]$ su sang.pham
Password:
[sang.pham@localhost b2110976]$
```

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, truy cập đầy đủ vào tất cả các file và lệnh, có 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).

+sudo cho phép quản trị viên kiểm soát hệ thống các thao tác của người dùng can thiệp đến hệ thống
+sudo giao quyền thực thi với tiêu chí đúng người đúng việc
+sudo thể hiện ưu thế khi thực thi các lệnh từ xa thông qua Telnet/SSH

- 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).

+Các bước cấp quyền sudo cho tài khoản ở 2.1

B1: Thêm người dùng sang.pham vào group wheel

Sudo usermod -aG wheel sang.pham

```
[b2110976@localhost ~]$ sudo usermod -aG wheel sang.pham
[b2110976@localhost ~]$
```

B2: Kiểm tra thông tin nhóm người dùng

Groups sang.pham

```
[b2110976@localhost ~]$ groups sang.pham
sang.pham : sang.pham wheel di21t9a2
[b2110976@localhost ~]$
```

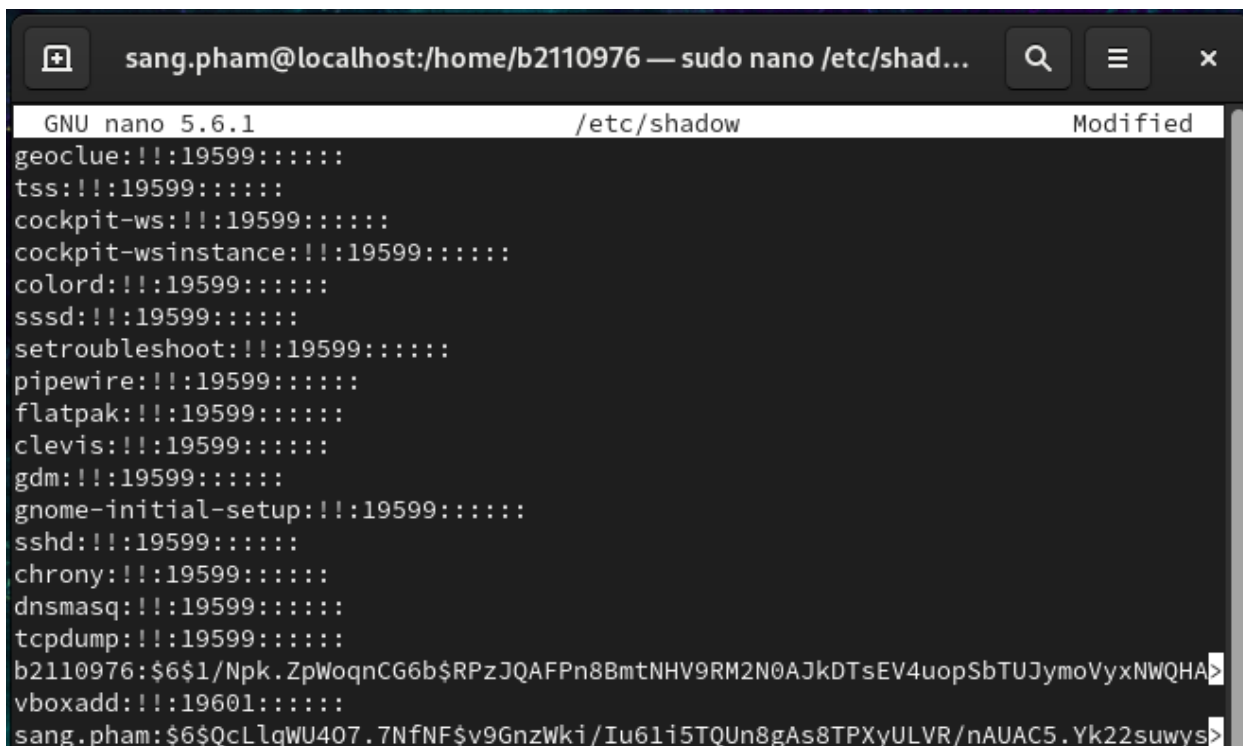
+Ví dụ kiểm chứng: sử dụng lệnh **sudo nano /etc/shadow**

```
[sang.pham@localhost b2110976]$ sudo nano /etc/shadow

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for sang.pham:
[sang.pham@localhost b2110976]$
```



```
GNU nano 5.6.1 /etc/shadow Modified
geoclue:!!:19599::::::
tss:!!:19599::::::
cockpit-ws:!!:19599::::::
cockpit-wsinstance:!!:19599::::::
colord:!!:19599::::::
sssd:!!:19599::::::
setroubleshoot:!!:19599::::::
pipewire:!!:19599::::::
flatpak:!!:19599::::::
clevis:!!:19599::::::
gdm:!!:19599::::::
gnome-initial-setup:!!:19599::::::
sshd:!!:19599::::::
chrony:!!:19599::::::
dnsmasq:!!:19599::::::
tcpdump:!!:19599::::::
b2110976:$6$1/Npk.ZpWoqnCG6b$RPzJQAFPn8BmtNHV9RM2N0AJkDTsEV4uopSbTUJymoVyxNWQHA>
vboxadd:!!:19601::::::
sang.pham:$6$QcLlqWU407.7NfNF$v9GnzWki/Iu61i5TQUn8gAs8TPXyULVR/nAUAC5.Yk22suwys>
```

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

+Lệnh **sudo gpasswd -d sang.pham wheel**

```
[b2110976@localhost ~]$ sudo gpasswd -d sang.pham wheel
[sudo] password for b2110976:
Removing user sang.pham from group wheel
[b2110976@localhost ~]$
```

+Kiểm tra

```
[sang.pham@localhost b2110976]$ sudo nano /etc/shadow
sang.pham is not in the sudoers file. This incident will be reported.
[sang.pham@localhost b2110976]$
```

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)
+Tạo phân vùng
B1: Lệnh **sudo fdisk /dev/sdb**

```
b2110976@localhost:~ — sudo fdisk /dev/sdb
[b2110976@localhost ~]$ sudo fdisk /dev/sdb
[sudo] password for b2110976:

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 0x4730a43d.

Command (m for help):
```

B2: Nhấn `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):
```

B3: Nhấn `p` để tạo phân vùng chính

```
Partition type
  p   primary (0 primary, 0 extended, 4 free)
  e   extended (container for logical partitions)
Select (default p): p
```

B4: Nhấn `1` để tạo ra 1 số lượng phân vùng

```
Partition number (1-4, default 1): 1
First sector (2048-16777215, default 2048):
```

B5: Nhấn Enter để tự tạo sector đầu tiên bằng 2048

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

B6: Nhấn Enter để tự tạo tạo sector cuối cùng bằng 16777215

```
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.
```

B7: Nhấn w để ghi cấu hình vào ổ cứng

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

Kiểm tra lại

```
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  
Disklabel type: dos  
Disk identifier: 0x4730a43d
```

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

+Format phân vùng

Sudo mkfs.ext4

```
[b2110976@localhost ~]$ sudo mkfs.  
mkfs.cramfs  mkfs.ext3    mkfs.fat      mkfs.msdos   mkfs.xfs  
mkfs.ext2    mkfs.ext4    mkfs.minix   mkfs.vfat  
[b2110976@localhost ~]$ sudo mkfs.ext4 /dev/sdb1  
mke2fs 1.46.5 (30-Dec-2021)  
Creating filesystem with 2096896 4k blocks and 524288 inodes  
Filesystem UUID: 79da61d4-5f5f-439c-abc0-be3dac6e521e  
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  
  
[b2110976@localhost ~]$
```

- 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)

+Tạo thư mục /data bằng quyền sudo

Sudo mkdir /data

```
[b2110976@localhost ~]$ sudo mkdir /data
[b2110976@localhost ~]$ ls /
afs  boot  dev  home  lib64  mnt  proc  run  srv  tmp  var
bin  data  etc  lib  media  opt  root  sbin  sys  usr
```

+Mount phân vùng ổ cứng ở 4.2 tới thư mục /data

Sudo mount /dev/sdb1 /data

```
[b2110976@localhost ~]$ sudo mount /dev/sdb1 /data
[b2110976@localhost ~]$
```

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

Sudo df -h

```
[b2110976@localhost ~]$ sudo df -h
[b2110976@localhost ~]$ sudo mount /dev/sdb1 /data
[b2110976@localhost ~]$ sudo 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  4.9G   13G  29% /
/dev/sda1       960M  301M  660M  32% /boot
tmpfs           177M  104K  177M   1% /run/user/1000
/dev/sdb1       7.8G   24K   7.4G   1% /data
[b2110976@localhost ~]$
```

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 người dùng nhanvien

Sudo groupadd nhanvien

```
[b2110976@localhost ~]$ sudo groupadd nhanvien
[b2110976@localhost ~]$
```

+Thêm người dùng ở 2.1 vào nhóm nhanvien

Sudo usermod -aG nhanvien sang.pham

```
[b2110976@localhost ~]$ sudo usermod -aG nhanvien sang.pham
[b2110976@localhost ~]$ groups sang.pham
sang.pham : sang.pham di21t9a2 nhanvien
[b2110976@localhost ~]$
```


- 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).

+Chuyển nhóm chủ sở hữu của thư mục /data sang nhanvien

Sudo chown :nhanvien

```
[b2110976@localhost ~]$ sudo chown :nhanvien /data
[b2110976@localhost ~]$ ls -l /
total 28
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 Aug 30 20:44 boot
drwxr-xr-x.  3 root nhanvien 4096 Sep 13 21:26 data
drwxr-xr-x. 20 root root 3380 Sep 13 21:18 dev
```

+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

Sudo chmod 750

```
[b2110976@localhost ~]$ sudo chmod 750 /data
[b2110976@localhost ~]$ ls -l /
total 28
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 Aug 30 20:44 boot
drwxr-x---.  3 root nhanvien 4096 Sep 13 21:26 data
drwxr-xr-x. 20 root root 3380 Sep 13 21:18 dev
```

- 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).

+Dùng sudo tạo tập tin /data/file1.txt

Sudo touch /data/file1.txt

```
[b2110976@localhost ~]$ sudo touch /data/file1.txt
[b2110976@localhost ~]$ ls -l /data
ls: cannot open directory '/data': Permission denied
[b2110976@localhost ~]$ sudo ls -l /data
total 16
-rw-r--r--. 1 root root    0 Sep 13 21:44 file1.txt
drwx-----. 2 root root 16384 Sep 13 21:26 lost+found
[b2110976@localhost ~]$
```


+Dùng tài khoản 2.1 tạo tập tin /data/file2.txt

Touch /data/file2.txt

```
[sang.pham@localhost b2110976]$ touch /data/file2.txt
touch: cannot touch '/data/file2.txt': Permission denied
[sang.pham@localhost b2110976]$
```

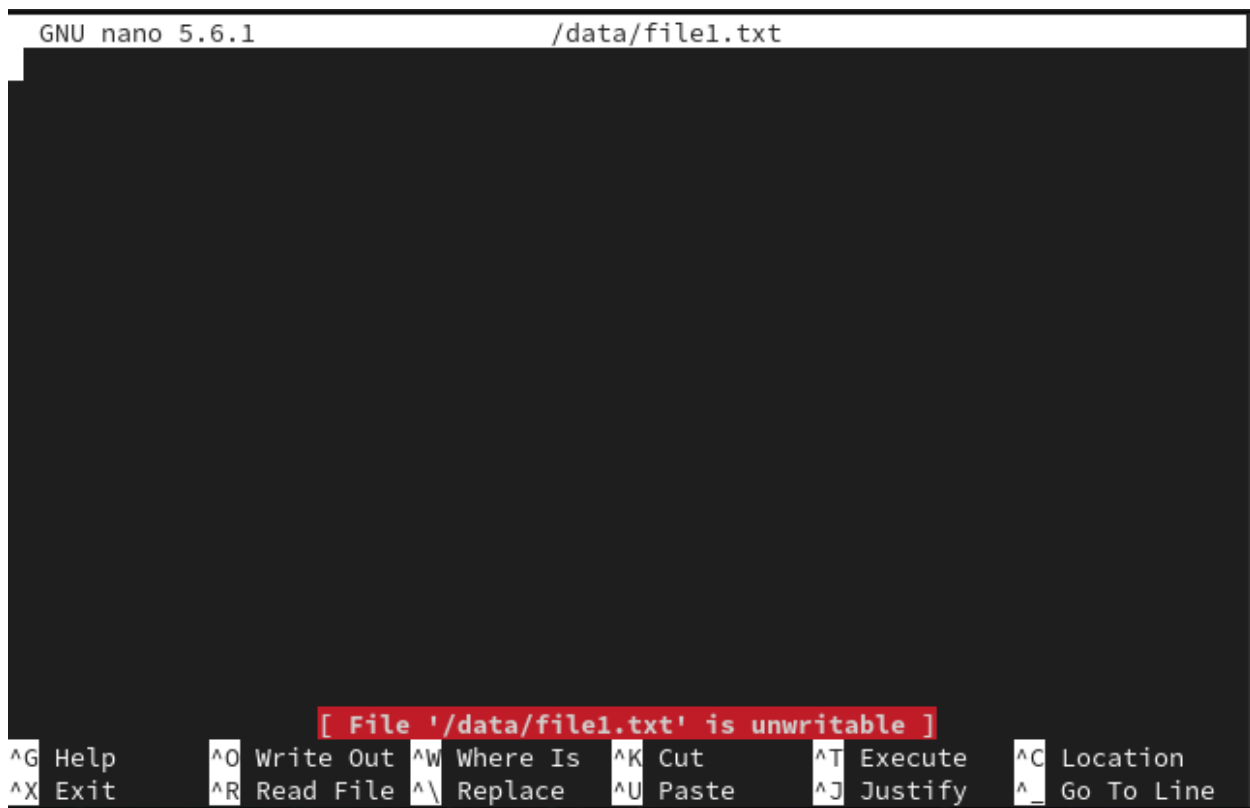
+Kết quả: do tài khoản b2110976 đầu tiên có quyền root nên có thể tạo tập tin /data/file1.txt dễ dàng, trong khi đó tài khoản sang.pham thuộc nhóm nhanvien có quyền nhóm chủ sở hữu là read và excute nên không thể tạo tập tin, ghi dữ liệu vào thư mục /data

- 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).

+Mở tập tin

Nano /data/file1.txt

```
[sang.pham@localhost b2110976]$ nano /data/file1.txt
[sang.pham@localhost b2110976]$
```



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

[ File '/data/file1.txt' is unwritable ]

^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
```

+Thay đổi tập tin

```
GNU nano 5.6.1 /data/file1.txt Modified
quan tri he thong cntt'

[ 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
```

+Kết quả: do người dung sang.pham thuộc nhóm nhanvien có quyền nhóm chủ sở hữu thư mục /data mà nhóm nhanvien chỉ có quyền read và excute nên có thể mở tập tin xem nội dung, tuy nhiên sẽ không có quyền ghi dữ liệu vào tập tin thuộc thư mục /data

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

+Cấp quyền write cho other có thể thay đổi nội dung /data/file1.txt

Sudo chmod o+w /data/file1.txt

```
[b2110976@localhost ~]$ sudo chmod o+w /data/file1.txt
[sudo] password for b2110976:
[b2110976@localhost ~]$ sudo ls -l /data
total 16
-rw-r--rw-. 1 root root    0 Sep 13 21:44 file1.txt
drwx-----. 2 root root 16384 Sep 13 21:26 lost+found
[b2110976@localhost ~]$
```

+Kiểm tra

```
[sang.pham@localhost b2110976]$ nano /data/file1.txt
[sang.pham@localhost b2110976]$ █
```

```
GNU nano 5.6.1 /data/file1.txt Modified
quan tri he thong cntt
```

```
^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
```

```
[sang.pham@localhost b2110976]$ cat /data/file1.txt
quan tri he thong cntt
[sang.pham@localhost b2110976]$ █
```

- 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 một tài khoản mới `newuser`

Sudo adduser newuser

```
[b2110976@localhost ~]$ sudo adduser newuser
[b2110976@localhost ~]$ sudo passwd newuser
Changing password for user newuser.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[b2110976@localhost ~]$ █
```

+Mở tập tin /data/file1.txt bằng tài khoản newuser

```
[newuser@localhost b2110976]$ nano /data/file1.txt
[newuser@localhost b2110976]$
```

The screenshot shows the GNU nano 5.6.1 text editor interface. The title bar at the top indicates the file path is /data/file1.txt. The main editing area is empty. At the bottom, a red error message is displayed: "[Path '/data' is not accessible]". Below the error message, the nano editor's help menu is visible, listing various keyboard shortcuts and their functions: ^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.

+Kết quả: mặc dù tài khoản newuser có quyền other là read và write trên tập tin /data/file1.txt nhưng vẫn không mở được tập tin là do trên thư mục /data người dùng other không có quyền execute. Do đó, newuser không thể mở được tập tin /data/file1.txt

- 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).

+Tạo thư mục /report

Sudo mkdir /report

```
[b2110976@localhost ~]$ sudo mkdir /report
[b2110976@localhost ~]$
```

+Tạo nhóm người dùng quantri

Sudo groupadd quantri

```
[b2110976@localhost ~]$ sudo groupadd quantri
[b2110976@localhost ~]$
```

+Phân quyền trên thư mục /report sao cho nhóm /quantri có quyền read, write và execute

Sudo setfacl -m g:quantri:rwx /report

```
[b2110976@localhost ~]$ sudo setfacl -m g:quantri:rwx /report
[b2110976@localhost ~]$
```

+Nhóm nhanvien có quyền read và execute

Sudo setfacl -m g:nhanvien:r-x /report

```
[b2110976@localhost ~]$ sudo setfacl -m g:nhanvien:r-x /report
[b2110976@localhost ~]$
```

+Người dùng ở 2.1 có quyền execute

Sudo setfacl -m u:sang.pham:--x /report

```
[b2110976@localhost ~]$ sudo setfacl -m u:sang.pham:--x /report
[b2110976@localhost ~]$
```

+Những người khác không có bất kỳ quyền gì cả

Sudo setfacl -m o:--- /report

```
[b2110976@localhost ~]$ sudo setfacl -m o:--- /report
[b2110976@localhost ~]$
```

+Kiểm tra

Getfacl /report

```
[b2110976@localhost ~]$ getfacl /report
getfacl: Removing leading '/' from absolute path names
# file: report
# owner: root
# group: root
user::rwx
user:sang.pham:--x
group::r-x
group:nhanvien:r-x
group:quantri:rwx
mask::rwx
other::---

[b2110976@localhost ~]$
```

--- Hết ---