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

Họ tên và MSSV: Võ Thành Em b2012081

Nhóm học phần: CT179_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: tuan.thai). (chụp hình minh hoạ).

Khi ta dùng lệnh **sudo tạo user em.vo** tạo user mới thì cần nhập lại mật khẩu sudo

```
[b2012081@localhost ~]$ sudo  adduser em.vo
[sudo] password for b2012081:
```

Dùng lệnh **sudo nano /etc/shadow** để xem chi tiết, Lúc này tài khoản em.vo chưa có cài đặt mật khẩu

```
em.vo:!!:19420:0:99999:7:::
```

Dùng lệnh **sudo paswd em.vo** để cài mật khẩu cho tài khoản em.vo

```
[b2012081@localhost ~]$ sudo passwd em.vo
Changing password for user em.vo.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

Dùng lệnh **sudo nano /etc/shadow** để xem chi tiết, lúc này mật khẩu đã được đặt

```
em.vo:$6$8acdB.dEa0skK.04$8A.zxOPYOVUBDGR/6Lts2/0hfKqlAg3knLZUQ62a2oWPvDdtxcPZ6
```

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.

Khi xem trong thư mục home lệnh **ls /home**

```
[b2012081@localhost ~]$ ls /home
b2012081  em.vo
```

Khi ta dùng lệnh **nano /etc/passwd**

```
b2012081:x:1000:1000:Vo Thanh Em:/home/b2012081:/bin/bash
em.vo:x:1001:1001::/home/em.vo:/bin/bash
```

Khi ta dùng lệnh **nano /etc/group**

```
b2012081:x:1000:
em.vo: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 hoạ).

Lệnh **sudo nano /etc/shadow** xem sử dụng giải **thuật băm là SHA-512 (6)**

```
em.vo:$6$8acdB.dEa0skK.04$8A.zxOPYOVUBDGR/6Lts2/0hfKqlAg3knLZUQ62a2oWPvDdtxcPZ6
```

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

Dùng lệnh **usermod -h** để xem trợ giúp
Dùng lệnh **sudo usermod -e 12/31/2023**

```
[b2012081@localhost ~]$ sudo usermod -e 12/31/2023 em.vo
```

Dùng lệnh **sudo chage -l em.vo** để xem chi tiết

```
[b2012081@localhost ~]$ sudo chage -l em.vo
Last password change                                    : Mar 04, 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).

Dùng lệnh **sudo groupadd di2096a1** để thêm nhóm người dùng là mã lớp và
Để kiểm tra xem đã thêm vào chưa thì dùng lệnh **nano /etc/group**

```
di2096a1:x:1002:
```

Để thêm 1 người dùng vào nhóm ta dùng lệnh **sudo usermod -a -G di2096a1 em.vo**
Và dùng lệnh **groups em.vo** để kiểm tra xem người dùng thuộc nhóm nào

```
[b2012081@localhost ~]$ sudo usermod -a -G di2096a1 em.vo
[sudo] password for b2012081:
[b2012081@localhost ~]$ groups em.vo
em.vo : em.vo di2096a1
```

Dùng lệnh **nano /etc/group** để xem chi tiết

```
em.vo:x:1001:
di2096a1:x:1002:em.vo
```

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

Dùng lệnh **sudo usermod -L em.vo** để khóa tài khoản và
dùng lệnh **sudo nano /etc/shadow** để kiểm tra xem đã khóa chưa **(dấu ! 6 đã khóa tài khoản)**

```
em.vo:!$6$8acdB.dEa0skK.04$8A.zxOPYOVUBDGR/6Lts2/0hf
```

Dùng lệnh **su em.vo** để chuyển tài khoản em.vo để kiểm tra thử

```
[b2012081@localhost ~]$ su em.vo
Password:
su: Authentication failure
```

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

Dùng lệnh **sudo usermod -U em.vo** để mở khóa
Sau đó dùng lệnh **sudo nano /etc/shadow** để kiểm tra xem mất chưa **(dấu ! 6 đã khóa tài khoản)**

```
em.vo:$6$8acdB.dEa0skK.04$8A.zxOPYOVUBDGR/6Lts2/0hfKq
```

Kỹ hơn nữa ta có thể dùng lệnh **su em.vo** để nhập lại mật khẩu

```
[b2012081@localhost ~]$ su em.vo
Password:
[em.vo@localhost b2012081]$
```

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).

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

IMO những ưu điểm chính của sudo so với su là sudo có khả năng ghi nhật ký cao hơn những lệnh đã được chạy và sudo cho phép kiểm soát tốt hơn những gì người dùng có thể làm.

Vì bạn thường phải gọi `sudo`mỗi lần bạn muốn làm điều gì đó đòi hỏi phải có đặc quyền, lý do là bạn sẽ "nghĩ trước khi nhảy", tức là không chỉ dán sudo trước một thứ gì đó mà không suy nghĩ trong giây lát lệnh bạn đang chạy sẽ làm

Với `su`Mặt khác, một khi bạn đang ở, bạn đang ở. Bạn có carte blanche (một giấy phép mở) để làm bất cứ điều gì và tất cả mọi thứ, và lý do là bạn có thể quên trong chốc lát rằng bạn có những đặc quyền và nếu bạn Thật không may mắn, thực thi một cái gì đó sẽ ảnh hưởng nghiêm trọng / làm hỏng hệ thống của bạn - nếu bạn không có đặc quyền su, lệnh sẽ không làm gì nghiêm trọng.

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).

Lệnh exit cho phép ta quay về tài khoản ban đầu

```
[em.vo@localhost b2012081]$ exit
exit
[b2012081@localhost ~]$
```

Để cấp quyền sudo cho tài khoản em.vo ta vào lệnh **sudo nano /etc/sudoers** để xem **nhóm wheel đã có quyền sudo** là thêm người dùng đó vào nhóm wheel
Dùng lệnh **sudo usermod -aG (hoặc -a -G) wheel em.vo**

Và kiểm tra lại bằng lệnh **groups em.vo**

```
[b2012081@localhost ~]$ groups em.vo
em.vo : em.vo wheel di2096a1
```

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

Dùng lệnh **sudo gpasswd -d em.vo** wheel thu hồi quyền sudo

```
[b2012081@localhost ~]$ sudo gpasswd -d em.vo wheel
[sudo] password for b2012081:
Removing user em.vo from group wheel
```

Để kiểm tra lại ta dùng lệnh **groups em.vo**

```
[em.vo@localhost b2012081]$ groups em.vo
em.vo : em.vo di2096a1
```

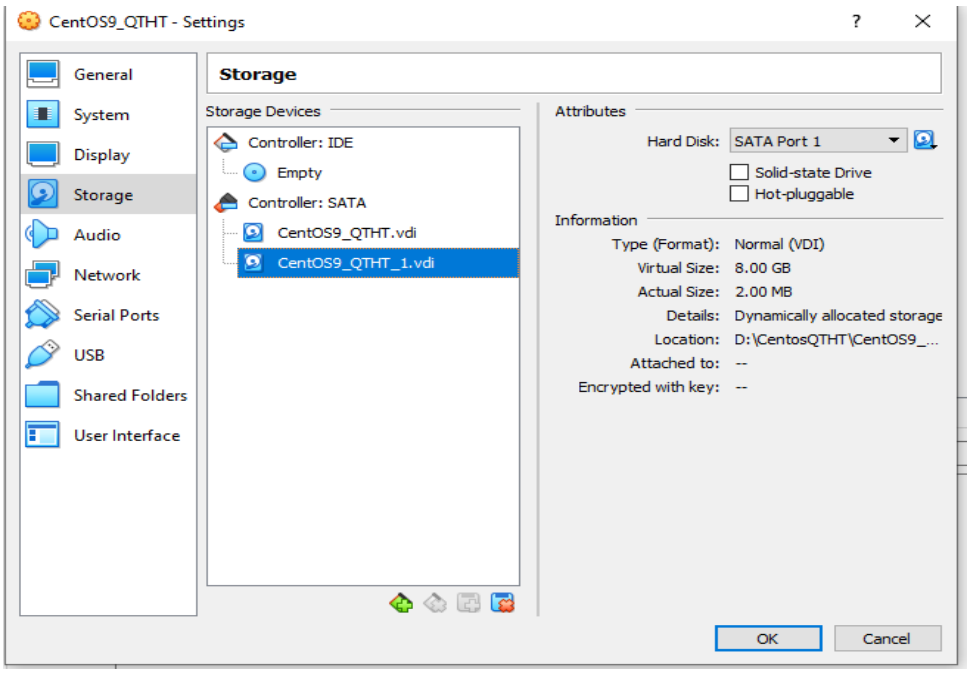
Dùng lệnh su chuyển tài khoản và dùng lệnh sudo nano /etc/shadow nó sẽ báo lỗi vì tài khoản em.vo đã bị thu hồi quyền sudo

```
em.vo 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 hoạ)

Dùng lệnh **sudo fdisk -l** để xem thông tin chi tiết.
Dùng lệnh **sudo fdisk /dev/sdb** vào ổ cứng muốn thao tác. Vào màn hình làm việc fdisk và gõ m để xem trợ giúp. Muốn thực hiện công việc nào đó thì gõ ký tự tương ứng.
Phím n cho phép tạo phân vùng mới**, chưa được lưu vào ổ cứng và để ghi vào thì gõ phím w. fsau đó hệ thống sẽ tự động thoát ra khỏi fdisk**

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

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

Dùng lệnh **sudo fdisk -l** để xem thông tin của phân vùng mới tạo ra là **sdb1**

```
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: 0x3b68a0cc

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

Dùng lệnh **sudo mkfs** để format phân vùng ổ cứng

```
[b2012081@localhost ~]$ sudo mkfs.ext4 /dev/sdb1
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 2096896 4k blocks and 524288 inodes
Filesystem UUID: 9f4f96c7-fe90-4e71-94ff-0e811243ca3d
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 quyền sudo. Mount phân vùng ổ cứng ở 4.2 tới thư mục `/data` (chụp hình minh hoạ)

Dùng lệnh **sudo mkdir /data** (do nằm ở thư mục gốc nên dùng quyền sudo)
Sau đó dùng lệnh **ls /** để liệt kê thư mục đó ra.

```
[b2012081@localhost ~]$ sudo mkdir /data
[b2012081@localhost ~]$ ls /
afs  boot  dev  home  lib64  mnt  proc  run   srv  tmp  var
bin  data  etc  lib   media  opt  root  sbin  sys  usr
```

Dùng lệnh **sudo mount /dev/sdb1 /data** để gắn kết thư mục data đến phân vùng sdb1.

```
[b2012081@localhost ~]$ sudo mount /dev/sdb1 /data
[b2012081@localhost ~]$
```

4.4. Thực hiện lệnh `df -h` để xem kết quả. (chụp hình minh hoạ)
Dùng lệnh sudo df -h để xem kết quả câu 4.3 sau khi phân vùng

```
[b2012081@localhost ~]$ sudo df -h
Filesystem           Size  Used Avail Use% Mounted on
devtmpfs             4.0M     0  4.0M   0% /dev
tmpfs                890M     0  890M   0% /dev/shm
tmpfs                356M  7.3M  349M   3% /run
/dev/mapper/cs-root   17G  5.6G   12G  33% /
/dev/sda1           1014M  367M  648M  37% /boot
tmpfs                178M   96K  178M   1% /run/user/1000
/dev/sdb1            7.8G   24K  7.4G   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`

Dùng lệnh **sudo groupadd nhanvien** tạo nhóm
Sau đó dùng lệnh **sudo usermod -aG** nhanvien em.vo thêm người dùng vào nhóm
Và lệnh **groups em.vo** để kiểm tra xem người dùng đã vào nhóm chưa

```
[b2012081@localhost ~]$ sudo groupadd nhanvien
[b2012081@localhost ~]$ sudo usermod -aG nhanvien em.vo
[b2012081@localhost ~]$ groups em.vo
em.vo : em.vo di2096a1 nhanvien
[b2012081@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 hoạ).

Lệnh chown tên chủ sở hữu : nhóm chủ sở hữu
Dùng lệnh **sudo chown :nhanvien /data** để chuyển nhóm sở hữu.
Sau đó dùng lệnh **ls -l /** để kiểm tra

```
drwxr-xr-x.   3 root nhanvien 4096 Mar  4 22:03 data
```

Phân quyền
Chủ sở hữu có **3 quyền rwx. Dùng số 7** để đại diện cho cả 3 quyền
Còn nhóm sở hữu thì chỉ **có quyền rx thì r = 4 và x=1 => dùng số 5** làm đại diện
Những người khác **không có quyền gì hết thì dùng 0** đại diện

Dùng lệnh **sudo chmod 750 /data** để thay đổi (phân quyền)
Dùng lệnh ls -l / để xem thông tin chi tiết sau khi phân quyền
Nó có 9 bit đại diện cho chủ sỡ hữu 3 bit đầu , nhóm sở hữu 3 bit tiếp theo, và những người khác là 3 bit cuối.

```
drwxr-x---.  3 root nhanvien 4096 Mar  4 22:03 data
```

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 hoạ).

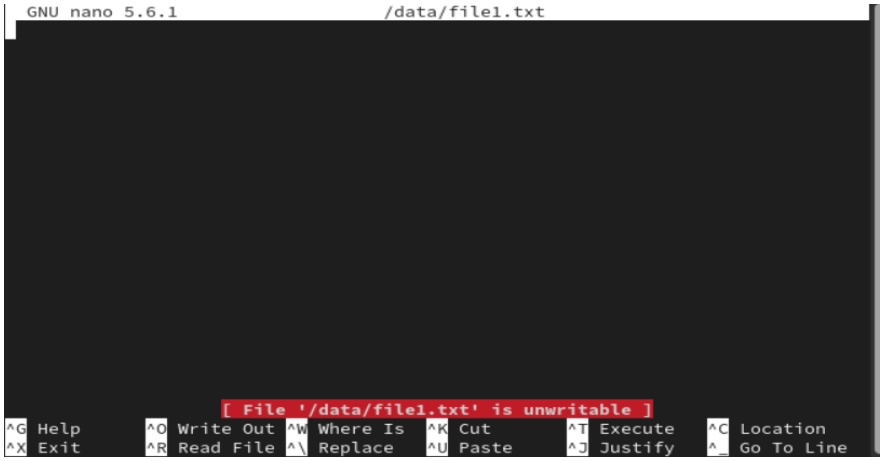
Lệnh **touch hoặc dùng nano** cho phép tạo ra 1 tệp tin rỗng.
Lệnh **sudo nano /data/file1.txt**
Lệnh **sudo ls -l /data** để kiểm tra tệp tin đã được tạo

```
[b2012081@localhost ~]$ sudo ls -l /data
total 16
-rw-r--r--. 1 root root     0 Mar  4 22:43 file1.txt
```

Chuyển quyền su em.vo rồi tạo file2 sẽ bị lỗi (do em.vo chỉ có quyền r-x không có quyên w)

```
[em.vo@localhost b2012081]$ touch /data/file2.txt
touch: cannot touch '/data/file2.txt': Permission denied
```

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).
Dùng lệnh **nano /data/file1.txt** để mở tệp tin và không có quyền thay đổi nội dung tập tin do nó chỉ có quyền r thiếu quyền w



```
[em.vo@localhost b2012081]$ ls -l /data/file1.txt
-rw-r--r--. 1 root root 0 Mar  4 22:43 /data/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 hoạ).

Dùng lệnh **sudo chmod o+w /data/file1.txt** để cấp quyền w (o= other)

```
[b2012081@localhost ~]$ sudo ls -l /data
total 20
-rw-r--rw-. 1 root root    28 Mar  4 22:59 file1.txt
```

Dùng lệnh **su em.vo** chuyển quyền
Sau đó dùng lệnh **nano /data/file1.txt** để thay đổi
Dùng lệnh **cat /data/file1.txt** để xem thay đổi

```
[b2012081@localhost ~]$ su em.vo
Password:
[em.vo@localhost b2012081]$ nano /data/file1.txt
[em.vo@localhost b2012081]$ cat /data/file1.txt
Hey you! are you ok! No ok!
loveSick Dk
```

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 hoạ).

Dùng lệnh **su newuser**
Sau đó dùng lệnh **nano /data/file1.txt** mở tệp tin nó sẽ hiện 1 thông báo lỗi thư mục data không thể truy cập được (do other không có quyền gì cả trên thư mục data , mặc dù có quyền rw- nhưng thiếu quyền x (execute) thì không thể mở lên được)

```
[ Path '/data' is not accessible ]
```

```
[b2012081@localhost ~]$ sudo ls -l /data
total 20
-rw-r--rw-. 1 root root    40 Mar  4 23:09 file1.txt
```

Dùng **lệnh ls -l /** để xem phân quyền người dùng **newuser**

```
drwxr-x---.   3 root nhanvien 4096 Mar  4 22:43 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 hoạ).

Để sử dụng kỹ thuật acl (access control list) thì phải cài đặt gói acl. Do centos 9 đã cài đặt sẵn nên không cần cài đặt vào.

Dùng lệnh **sudo mkdir /report** để tạo thư mục

```
[b2012081@localhost ~]$ sudo mkdir /report
```

Dùng lệnh **sudo groupadd quantri** để tạo nhóm người dùng

```
[b2012081@localhost ~]$ sudo groupadd quantri
```

Dùng lệnh **getfacl /report** để xem phân quyền trên thư mục rreport

```
[b2012081@localhost ~]$ getfacl /report
getfacl: Removing leading '/' from absolute path names
# file: report
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
```

Tương tự khi ta xem thông tin bằng **lệnh ls -l /**

```
drwxr-xr-x.   2 root root        6 Mar  4 23:29 report
```

Để thay đổi quyền trên 1 tệp tin hay thư mục ta dùng lệnh setfacl có 2 tham số cơ bản -m (cho phép thay đổi quyền acl của 1 tệp tin hay thư mục) và -x (cho phép gỡ bỏ acl hay bỏ quyền đã cấu hình trên 1 tệp tin hay thư mục)

ACL entries

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

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

Whitespace between delimiter characters and non-delimiter characters is ignored.

Proper ACL entries including permissions are used in modify and set operations (options **-m**, **-M**, **--set** and **--set-file**). Entries without the *perms* field are used for deletion of entries (options **-x** and **-X**).

*Dùng lệnh **sudo setfacl -m g:quantri:rwx /report** để cấp quyền **rwx** cho nhóm người dùng quantri*

*Dùng lệnh **sudo setfacl -m g:nhanvien:r-x /report** Để cấp quyền **r-x** cho nhóm người dùng nhanvien*

*Dùng lệnh **sudo setfacl -m u:em.vo:--x /report** Để cấp quyền **--x** cho em.vo*

*Dùng lệnh **sudo setfacl -m o:--- /report** Để thay đổi quyền other **---***
*Và lệnh **getfacl /report** để xem thông tin chi tiết*

```
[b2012081@localhost ~]$ sudo setfacl -m o:--- /report
[b2012081@localhost ~]$ getfacl /report
getfacl: Removing leading '/' from absolute path names
# file: report
# owner: root
# group: root
user::rwx
user:em.vo:--x
group::r-x
group:nhanvien:r-x
group:quantri:rwx
mask::rwx
other::---
```

--- Hết ---