**LAB 2**

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

| Họ tên và MSSV: Lê Trương Ngọc Duyên B2105569  Nhóm học phần: CT179-06 |
| --- |

*- 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**

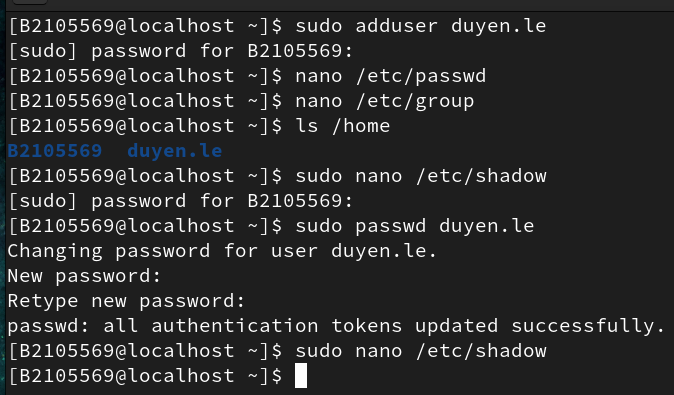
Thực hiện cài đặt CentOS 9 Stream vào máy tính cá nhân (hoặc máy ảo) của bạn nếu cần (KHÔNG cần chụp hình minh họa).

1. **Quản lý tài khoản**

Tìm hiểu và thực hiện các yêu cầu sau:

* 1. Sử dụng lệnh adduservà passwd để tạo một tài khoản mới với tên đăng nhập có dạng **tên.họ** (ví dụ: tuan.thai). (chụp hình minh hoạ).

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



-Dùng lệnh **sudo adduser <tên tài khoản>** để thêm/tạo tài khoản người dùng mới

-Dùng lệnh **sudo passwd <tên tk>** để thay đổi mật khẩu cho tài khoản người dùng hoặc tài khoản nhóm

-Dùng lệnh **nano /etc/passwd** để mở tập tin passwd (không cần dùng quyền sudo)

* x: Thông tin mật khẩu hiện không còn được lưu ở tập tin passwd nữa, mà được thay thế bằng chữ x và thông tin mật khẩu được lưu trữ ở tập tin shadow
* 1001: User ID
* 1001: Group ID
* /home/duyen.le: Đường dẫn đến thư mục cá nhân
* /bin/bash: Login shell



-Dùng lệnh **nano /etc/group** để mở tập tin group (không cần dùng quyền sudo)



-Dùng lệnh **sudo nano /etc/shadow** để mở tập tin shadow xem thông tin mật khẩu (do tập tin shadow chứa thông tin mật khẩu và tài khoản người dùng nên dùng quyền sudo)

* Do tài khoản chưa đặt mật khẩu nên thông tin mật khẩu đang rỗng





* 1. 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).

-Tài khoản mới tạo sử dụng giải thuật băm SHA-512 dựa vào ký tự **6**:



-Dựa vào ký tự 2 dấu **$** đầu tiên ta biết được tài khoản sử dụng giải thuật băm gì

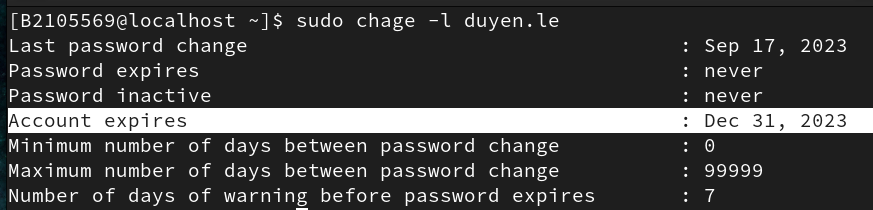
-Một vài giải thuật băm:

* $y$: yescrypt
* $6$: SHA-512
* $1$: MD5
  1. Thiết lập ngày hết hạn cho tài khoản ở 2.1 là ngày 31/12/2023 (chụp hình minh hoạ).

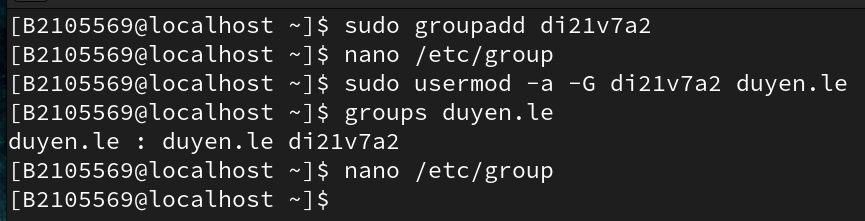
-Dùng lệnh **usermod** với tham số **-e** để thiết lập ngày hết hạn cho tài khoản theo định dạng mm/dd/yyyy:



-Dùng lệnh **sudo chage -l <tên tk>** để xem thông tin của tài khoản:



* 1. 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 <tên nhóm>** để tạo nhóm mới

-Dùng lệnh **sudo usermod -a -G <tên nhóm> <tên ng dùng>** để thêm tài khoản người dùng vào nhóm

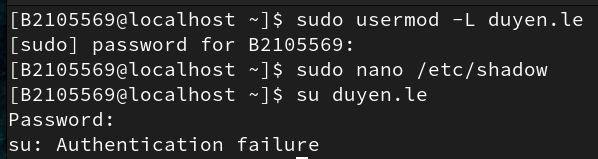
-Dùng lệnh **nano /etc/group** để mở tập tin group

-Dùng lệnh **groups <tên ng dùng>** để kiểm tra 1 người dùng thuộc những nhóm nào



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

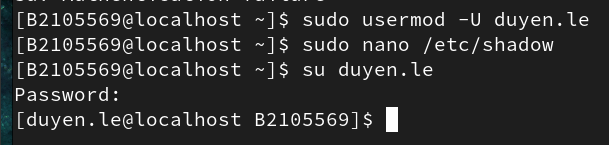


-Dùng lệnh **sudo usermod -L <tên tk>** để khóa tài khoản với tham số **-L** (lock)

-Dùng lệnh **sudo nano /etc/shadow** thì ta thấy mật khẩu của tài khoản có thêm dấu **!**, làm cho mật khẩu của tài khoản bị vô hiệu hóa, dù cho có nhập đúng mật khẩu hay không:



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



-Dùng lệnh **sudo usermod -U <tên tk>** để mở khóa tài khoản với tham số **-U** (unlock)

-Dùng lệnh **sudo nano /etc/shadow** thì ta thấy dấu **!** đã được gỡ bỏ khỏi mật khẩu của tài khoản:



1. **Quyền root (Root privilege) và sudo**

Tìm hiểu và thực hiện các yêu cầu sau:

* 1. Quyền root là gì?

-Quyền root là quyền hạn mà tài khoản root có trên hệ thống. Có quyền truy cập vào tất cả các lệnh và file. Một trong số các quyền hạn của root là khả năng sửa đổi hệ thống theo bất kỳ cách nào mình muốn, cũng như cấp và thu hồi quyền truy cập cho những user khác.

* 1. Nêu các ưu điểm của việc dùng sudo so với dùng su (chuyển sang tài khoản root).

-**sudo** chi tiết và an toàn hơn **su**

* **sudo** chạy một lệnh duy nhất với quyền root. Khi bạn thực thi lệnh **sudo**, hệ thống nhắc bạn nhập mật khẩu tài khoản người dùng hiện tại của bạn trước khi chạy là người dùng root.
* **su** chuyển sang người dùng root - khi bạn thực thi nó mà không có tùy chọn bổ sung. Bạn sẽ phải nhập mật khẩu của tài khoản root.
  1. 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 để cấp quyền sudo cho tài khoản:

+Bước 1: Dùng lệnh **sudo nano /etc/sudoers** để mở tập tin sudoers. Tập tin này dùng để quản lý các quyền sudo trên hệ thống

* Tài khoản root đã có toàn quyền trên hệ thống



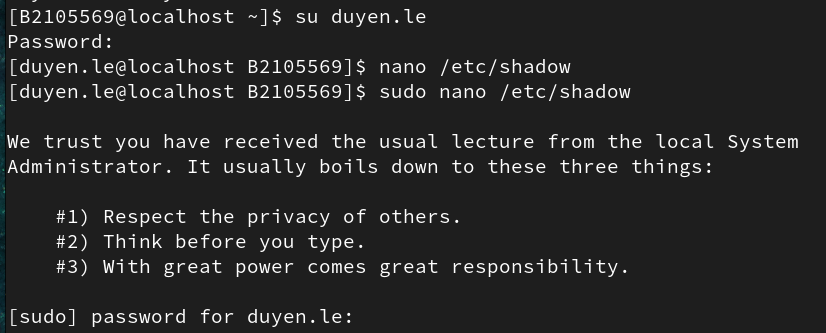
* Cho phép tất cả các người dùng ở trong nhóm wheel thực thi bất kỳ lệnh nào trên hệ thống (**%**<tên nhóm>)
  + Đối với các hệ điều hành Linux thuộc nhóm Red Hat thì thông thường sẽ có 1 nhóm người dùng được tạo sẵn, đó là nhóm wheel



+Bước 2: Dùng lệnh **sudo usermod -aG <tên nhóm có toàn quyền> <tên tk>**

+Bước 3: Dùng lệnh **groups <tên tk>** để kiểm tra tài khoản thuộc những nhóm nào

-Ví dụ kiểm chứng xem tài khoản duyen.le đã thực sự được cấp quyền hay chưa:



* Dùng lệnh **nano /etc/shadow**. Do tập tin shadow chứa thông tin mật khẩu của người dùng nên 1 người dùng thông thường không thể mở tập tin shadow lên được



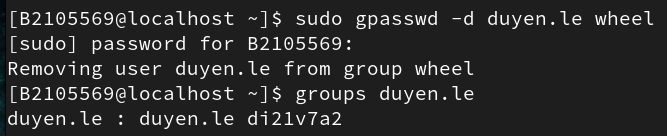
* Vì vậy, để mở được tập tin shadow thì phải dùng quyền sudo cho tài khoản



⇒ Điều này chứng tỏ ta đã cấp được quyền sudo cho tài khoản duyen.le → Từ thời điểm này, tài khoản duyen.le có thể thay thể tài khoản root để thực hiện các thao tác quản trị trên hệ thống

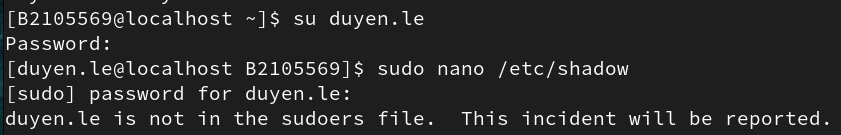
* 1. Thu hồi quyền sudo của một tài khoản ở 2.1 (chụp hình minh họa).

-Để thu hồi quyền sudo của một tài khoản, ta có thể đưa tài khoản đó ra khỏi nhóm có toàn quyền.



* Dùng lệnh **sudo gpasswd -d <tên tk cần xóa khỏi nhóm> <tên nhóm>**
* Kiểm tra lại bằng lệnh **groups**

-Chuyển qua tài khoản duyen.le xem còn thực hiện được quyền sudo hay không



* Lúc này sẽ hiện ra thông báo rằng tài khoản duyen.le không còn trong tập tin sudoers nữa. Sự kiện này sự được báo cáo lên hệ thống. ⇒ Ta đã thu quyền sudo của tài khoản duyen.le và tài khoản này không có quyền sudo nữa.

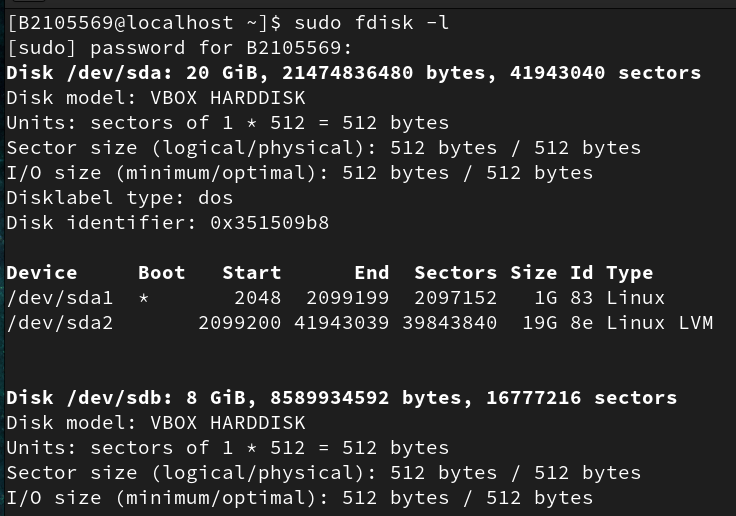
1. **Đĩa và phân vùng ổ cứng**

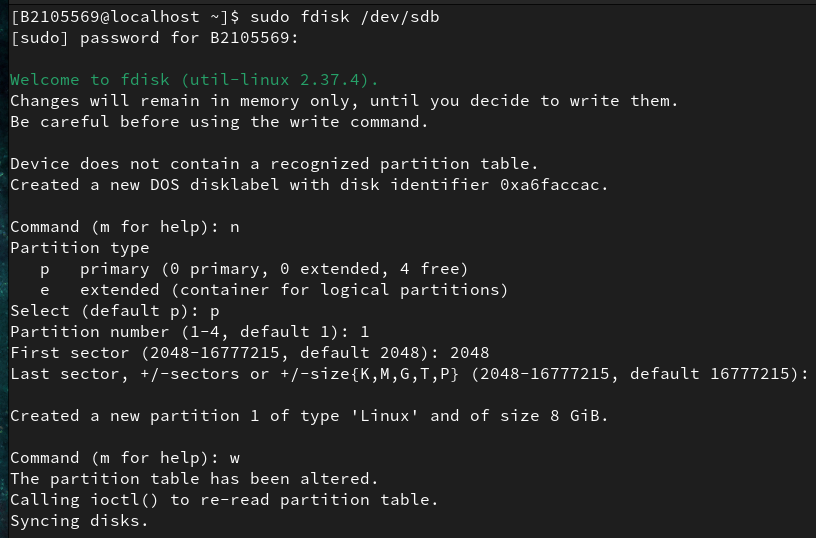
Tìm hiểu và thực hiện các yêu cầu sau:

* 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.
  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)

-Lệnh **fdisk** là tiện ích quản lý phân vùng đĩa cứng trên Linux

* **sudo fdisk -l** : liệt kê các phân vùng ổ cứng trên hệ thống
* **sudo fdisk <đường dẫn ổ cứng>**: phân vùng ổ cứng

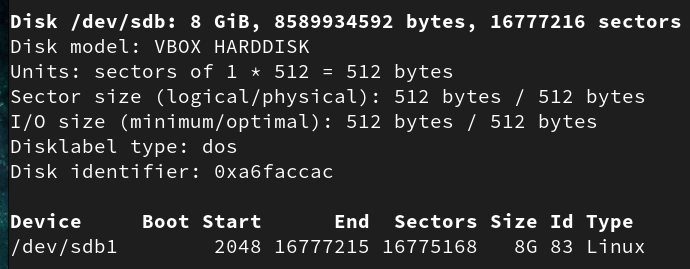




**-sudo fdisk <đường dẫn ổ cứng>**

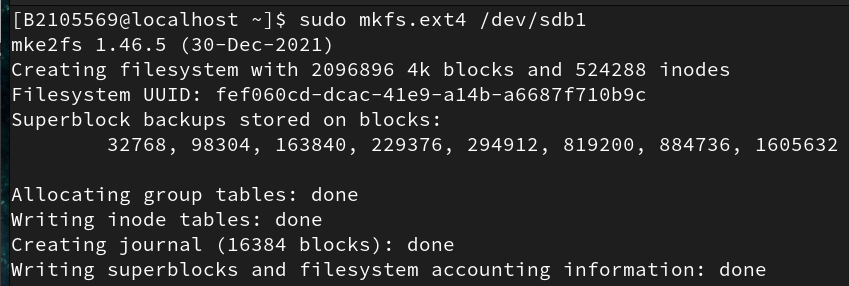
* Gõ **m** để xem hướng dẫn
* Gõ **n** để tạo phân vùng mới
  + Loại phân vùng: p (chính), e (mở rộng)
  + Số phân vùng: 1 - 4
  + Section đầu
  + Section cuối
* Gõ **w** để ghi phân vùng

-Gõ **fdisk -l <đường dẫn ổ cứng>** để kiểm tra

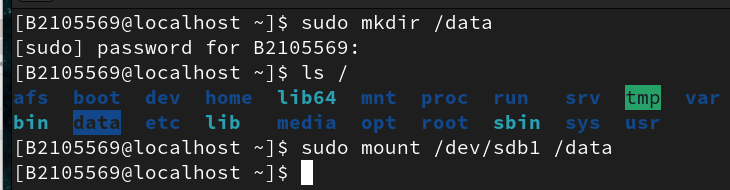


-Lệnh **mkfs** (Makes File System) dùng để định dạng phân vùng ổ cứng

* **sudo mkfs.ext4 <đường dẫn ổ cứng>**: định dạng phân vùng theo chuẩn ext4

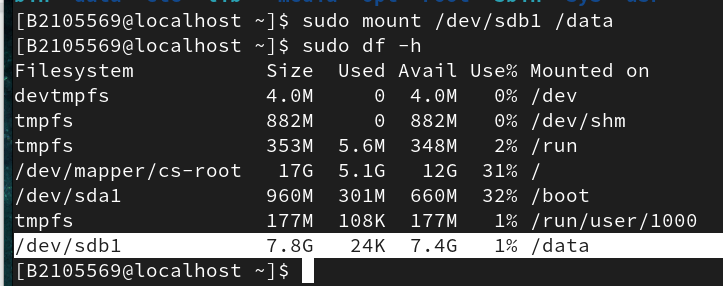


* 1. Tạo thư mục mới có tên /databằng quyền sudo. Mount phân vùng ổ cứng ở 4.2 tới thư mục /data (chụp hình minh hoạ)

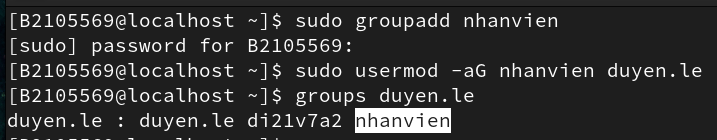


**sudo mount <đường dẫn ổ cứng> <đường dẫn thư mục>**: gắn ổ cứng vào đường dẫn cụ thể

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

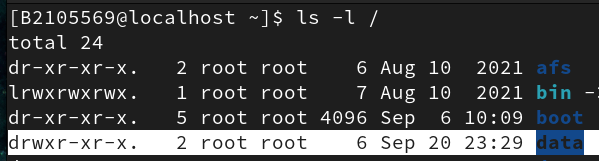


1. **Phân quyền trên hệ thống tập tin**
   1. Tạo nhóm người dùng nhanvien, thêm người dùng ở 2.1 vào nhóm nhanvien



* 1. Chuyển *nhóm chủ sở hữu* của thư mục /datasang 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).

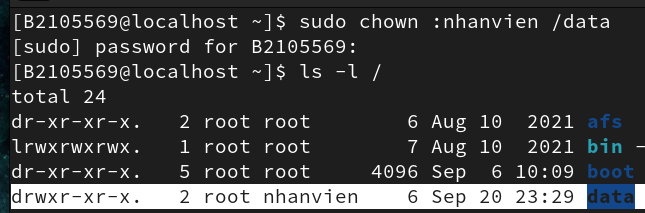
-Do thư mục /data được tạo ra bằng quyền sudo nên chủ sở hữu và nhóm chủ sở hữu đều là tài khoản root



-Lệnh **chown** (Change Owner) dùng để thay đổi chủ sở hữu và nhóm chủ sở hữu của tập tin, thư mục…

* **sudo chown <chủ sở hữu>:<nhóm chủ sở hữu> <tên file>**

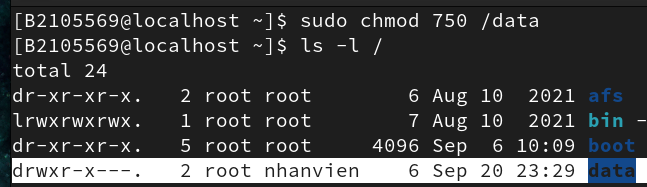
-Chuyển *nhóm chủ sở hữu* của thư mục /datasang nhanvien:



Lệnh **chmod** (Change Mode) dùng để thay đổi quyền truy cập của người dùng tới tập tin, thư mục.

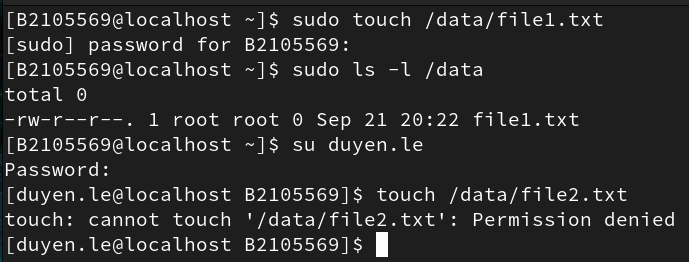
* **chmod <giá trị mode> <tên tập tin>**
  + 777: rwxrwxrwx → Mọi người đều có toàn quyền
  + 755: rwxr-xr-x → Chủ sở hữu toàn quyền, những người còn lại chỉ có quyền đọc và thực thi
  + 750: rwxr-x— → Chủ sở hữu toàn quyền, nhóm người dùng có quyền đọc và thực thi, những người khác không có bất kỳ quyền gì cả
  + 644: rw-r--r– → Chủ sở hữu có quyền đọc viết, những người còn lại chỉ có quyền đọc

-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:



* 1. 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** dùng để tạo tập tin rỗng

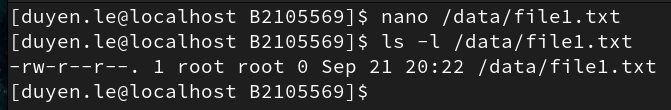


**⇒Kết quả:**

-Dùng lệnh sudo tạo thành công tập tin /data/file1.txt

-Dùng tài khoản duyen.le không thể tạo được tập tin /data/file2.txt

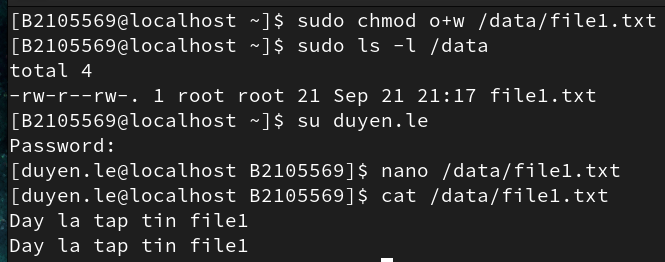
* Vì nhóm người dùng chỉ có quyền read (xem nội dung thư mục) và execute (đi xuyên ngang thư mục), không có quyền write (tạo thư mục con, tập tin) ⇒ Nên khi thực hiện lệnh để tạo tập tin mới thì hệ thống sẽ báo lỗi là quyền bị từ chối
  1. Dùng tài khoản ở 2.1 *mở và thay đổi nội dung* tập tin /data/file1.txt, cho biết kết quả (chụp hình minh hoạ).



**⇒Kết quả:**

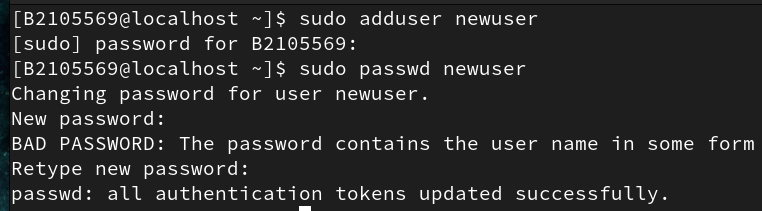
* Do tài khoản duyen.le không có quyền write trên tập tin file1.txt ⇒ Nên không thể thay đổi nội dung tập tin mà chỉ mở được tập tin lên xem nội dung
  1. Cấp quyền cho tài khoản 2.1 có thể thay đổi nội dung tập tin /data/file1.txt (chụp hình minh hoạ).

-Dùng lệnh **sudo chmod o+w <tên tập tin>** để thêm quyền write cho những người khác (other+write)



* 1. 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).

-Tạo thêm một tài khoản mới newuser



-Dùng tài khoản này mở tập tin /data/file1.txt:

* Người dùng newuser (thuộc nhóm những người khác) có quyền read và write. Tuy nhiên, để mở được tập tin file1 lên thì tài khoản newuser phải đi ngang qua thư mục data. Nhưng ta thấy trong thư mục data thì nhóm những người khác không có quyền execute (đi ngang qua thư mục)





⇒ Nên không thể mở tập tin /data/file1.txt

* 1. 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).

-Dùng quyền sudo tạo thư mục /report và tạo nhóm người dùng quantri:



-Áp dụng kỹ thuật **ACL** (Access Control List) dùng để phân quyền cho nhiều nhóm người dùng, nhiều người dùng khác nhau trên một thư mục, tập tin.

-Lệnh **getfacl** dùng để xem các quyền truy cập đầy đủ trên một tập tin, thư mục



-Lệnh **setfacl** dùng để thay đổi quyền truy cập trên một tập tin, thư mục.

+Có 2 tham số cơ bản:

* **-m** (modify): thay đổi quyền của một tập tin, thư mục
* **-x** (remove): gỡ bỏ quyền đã cấu hình trên một tập tin, thư mục

+ Cú pháp: **d: u:<uid>:<quyền> d: g:<gid>:<quyền> d: o:<quyền>**

* d (default): tất cả những thư mục con hoặc tập tin trong thư mục đó sẽ có quyền giống như thư mục đó
* u (user): người dùng
* g (group): nhóm người dùng
* o (other): những người khác

-Dùng lệnh **setfacl** thay đổi cho nhóm quantri có quyền read, write và execute trên thư mục report:



-Dùng lệnh **setfacl** thay đổi cho nhóm nhanvien có quyền read và execute trên thư mục report:



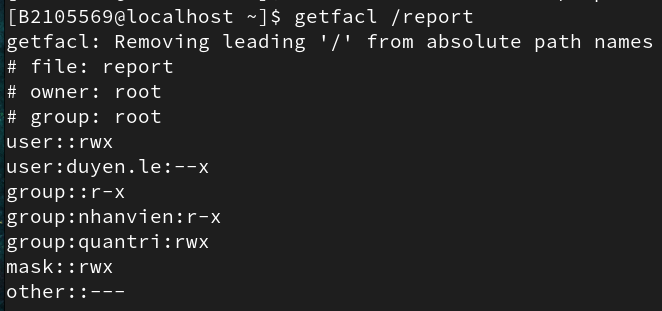
-Dùng lệnh **setfacl** thay đổi cho người dùng duyen.le có quyền execute trên thư mục report:



-Dùng lệnh **setfacl** thay đổi cho những người khác không có quyền gì cả trên thư mục report:



**⇒Kết quả:**



--- Hết ---