**LAB 2**

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

|  |
| --- |
| Họ tên và MSSV: **Lê Tuấn Đạt - B2113328**  Nhóm học phần: **CT17906** |

* *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.* Hình minh hoạ chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.
* *Video hướng dẫn ở cuối bài.*

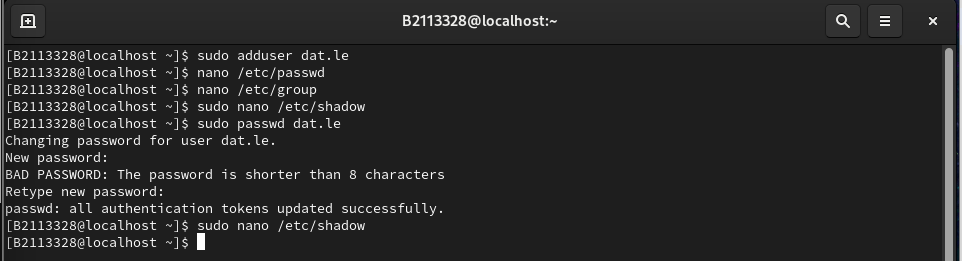
1. **Cài đặt CentOS**

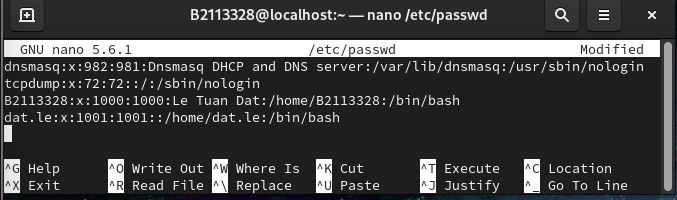
Thực hiện cài đặt CentOS 9 Stream vào máy tính cá nhân (hoặc máy ảo) của bạn nếu cần (KHÔNG cần chụp hình minh họa).

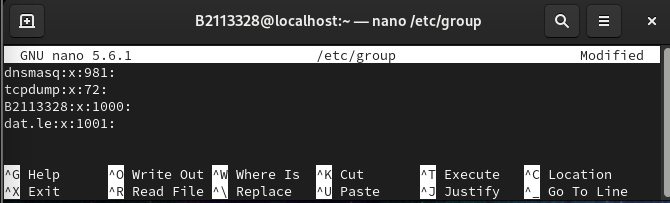
1. **Quản lý tài khoản**

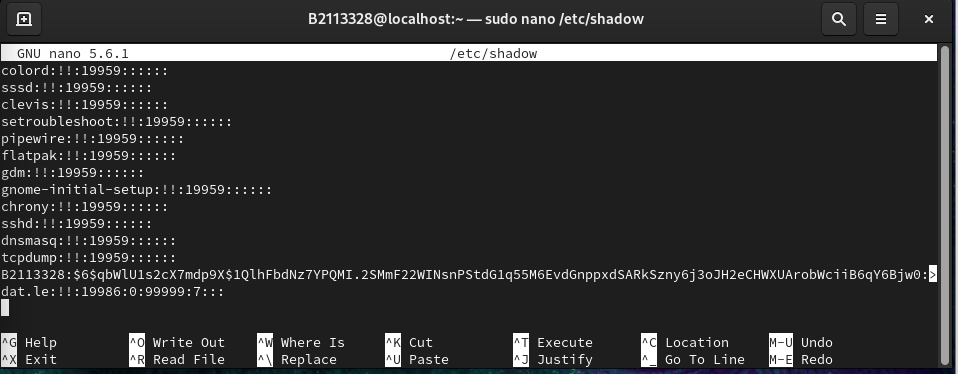
Tìm hiểu và thực hiện các yêu cầu sau:

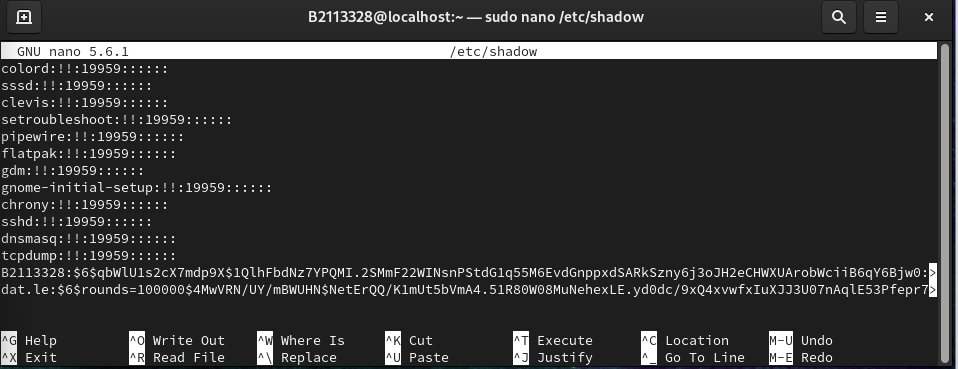
* 1. Sử dụng lệnh adduservà passwd để tạo một tài khoản mới với tên đăng nhập có dạng **tên.họ** (ví dụ: tuan.thai). (chụp hình minh hoạ).







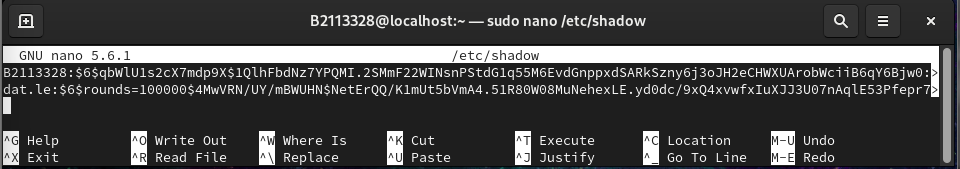




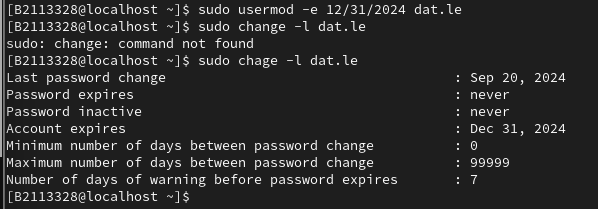
Quan sát để thấy rằng khi một tài khoản mới được tạo, thư mục cá nhân trong /home và nhóm cá nhân trong/etc/groupứng với tài khoản đó cũng được tạo theo.

* 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).

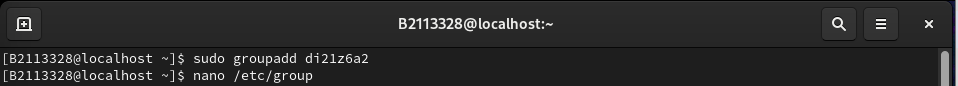
- Giải thuật băm được sử dụng cho tài khoản mới tạo là: SHA-512. Do giữa 2 dấu ‘$’ bên phải tên user có số id là 6.

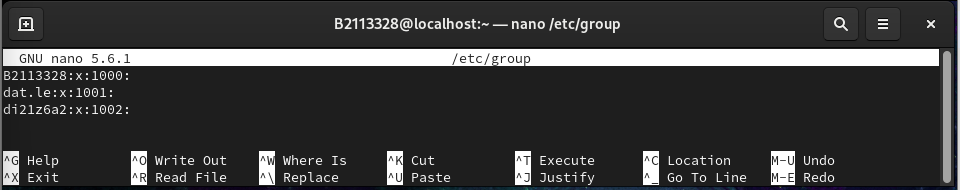


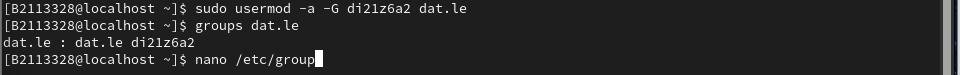
* 1. Thiết lập ngày hết hạn cho tài khoản ở 2.1 là ngày 31/12/2024 (chụp hình minh hoạ).

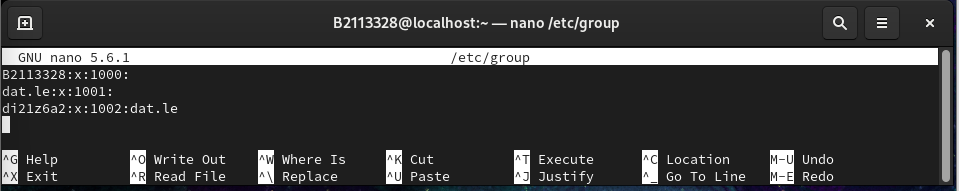


* 1. Tạo một nhóm người dùng với tên nhóm là mã lớp của bạn. Thêm tài khoản ở 2.1 vào nhóm vừa tạo (chụp hình minh hoạ).

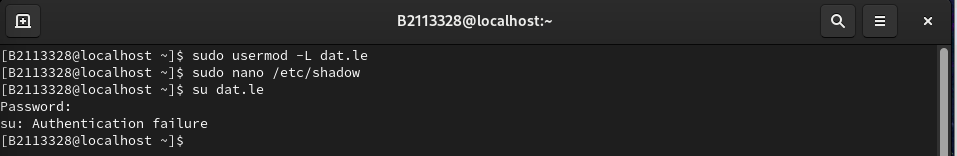


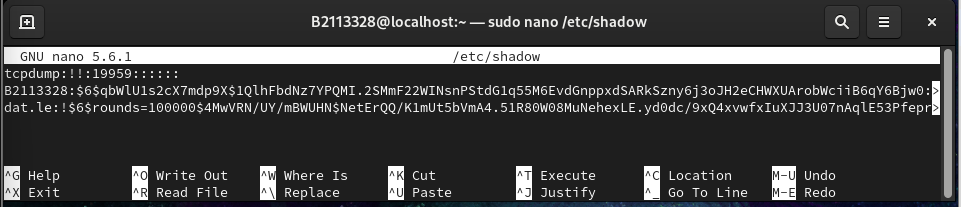




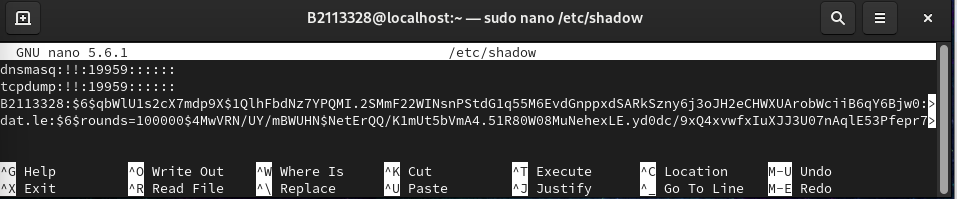


* 1. Thực hiện khóa tài khoản ở 2.1, sau đó đăng nhập thử và quan sát (chụp hình minh hoạ).





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





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 cao nhất trong hệ điều hành Linux. Tài khoản root có toàn quyền kiểm soát hệ thống và thực hiện các thay đổi quan trọng khác. Đây là tài khoản có quyền cao nhất và không bị giới hạn bởi các cơ chế bảo mật thông thường của hệ điều hành.

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

- Sử dụng **sudo** không yêu cầu phải chia sẻ mật khẩu root, thay vào đó, chỉ cần mật khẩu cá nhân của người đó.

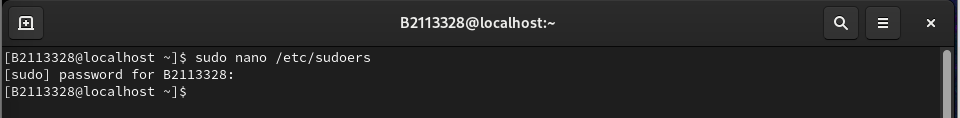
- Do **sudo** là giới hạn của **su**, **sudo** cho phép chúng ta cấp quyền chỉ đối với các lệnh cụ thể mà không cần phải chuyển sang quyền root hoàn toàn. Người dùng chỉ có thể thực thi các lệnh họ được phép mà không có quyền truy cập toàn bộ hệ thống.

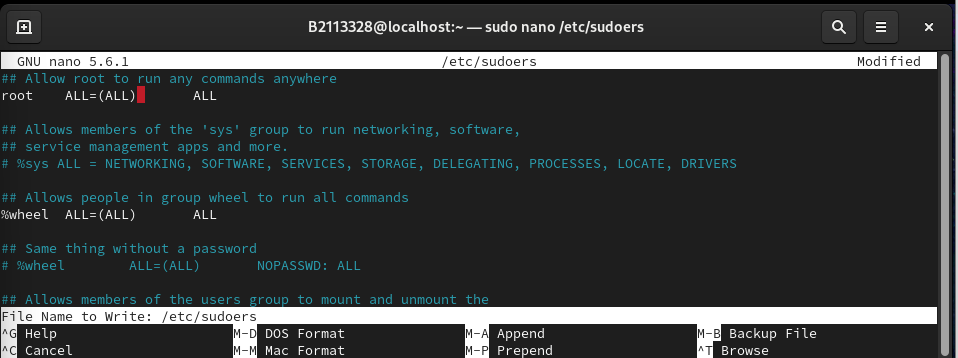
- Các lệnh thực thi bằng **sudo** đều được ghi lại (Logs), giúp quản trị viên theo dõi và kiểm soát hoạt động người dùng.

- Sudo thường chỉ có hiệu lực trong khoảng thời gian ngắn (thường là 5-15 phút), sau đó người dùng sẽ phải nhập lại mật khẩu để tiếp tục sử dụng **sudo**. Điều này giảm thiểu rủi ro rằng ai đó có quyền truy cập trái phép vào máy khi người dùng tạm vắng mặt.

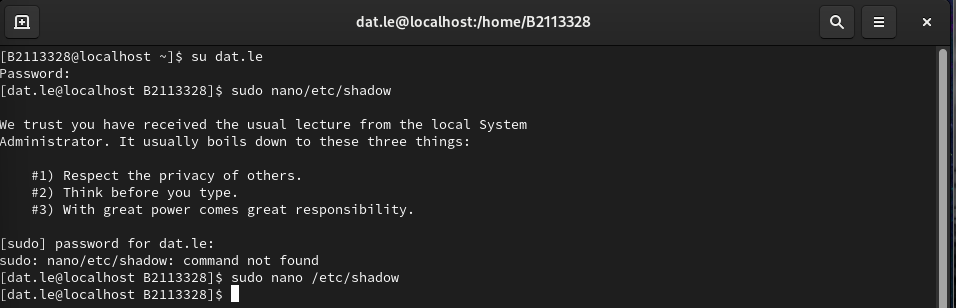
- **sudo** cho phép quản trị viên hệ thống tùy chỉnh và phân quyền cho từng người dùng trong file cấu hình **/etc/sudoers**, mà không cần cấp quyền root hoàn toàn.

* 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).

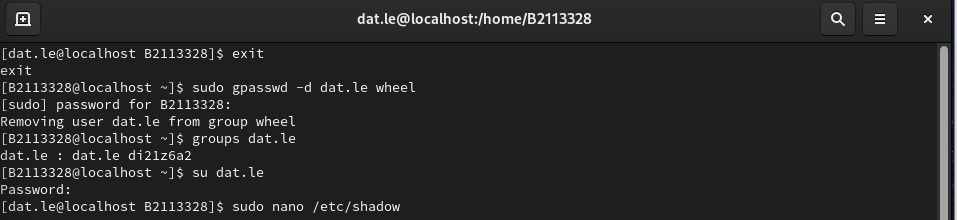








* 1. Thu hồi quyền sudo của một tài khoản ở 2.1 (chụp hình minh họa).

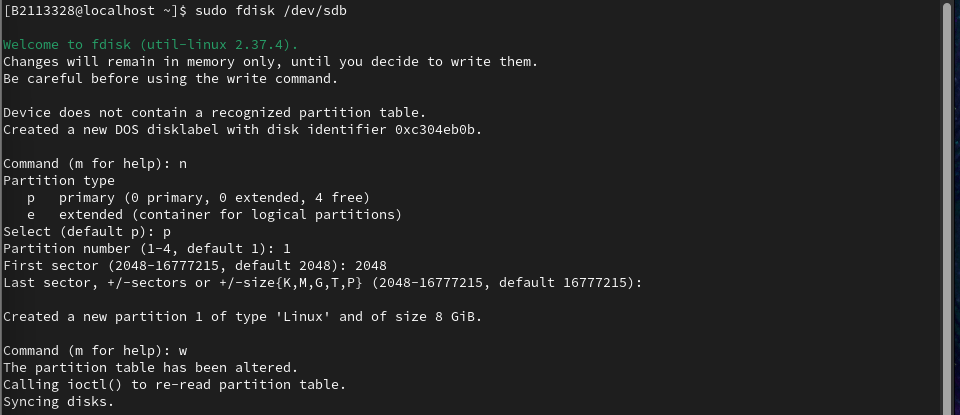




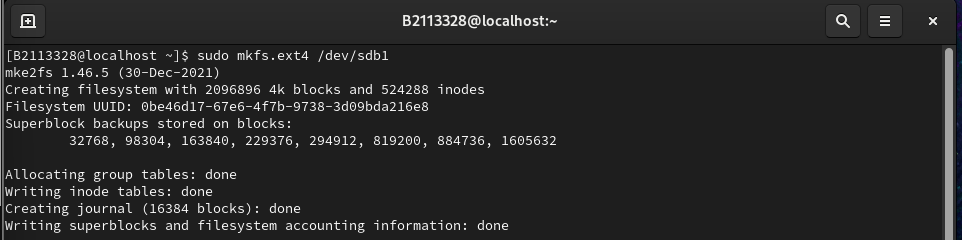
1. **Đĩa và phân vùng ổ cứng**

Tìm hiểu và thực hiện các yêu cầu sau:

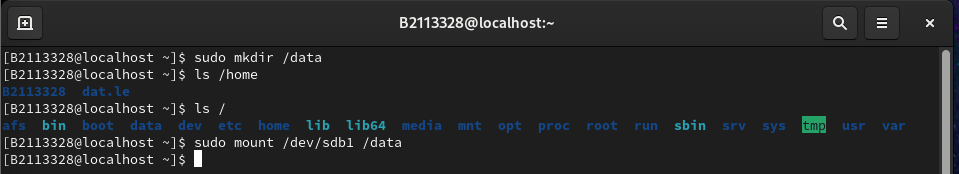
* 1. Thêm một ổ cứng vào máy ảo CentOS. Nếu đã cài CentOS trực tiếp vào máy tính cá nhân thì có thể sử dụng 1 USB để thay thế.
  2. Sử dụng lệnh fdisk và mkfs để tạo và format một phân vùng trên ổ cứng vừa mới thêm ở 4.1 (chụp hình minh hoạ)



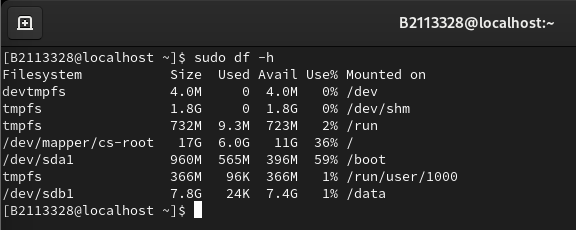




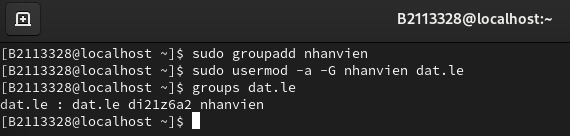
* 1. Tạo thư mục mới có tên /databằng quyền sudo. Mount phân vùng ổ cứng ở 4.2 tới thư mục /data (chụp hình minh hoạ)



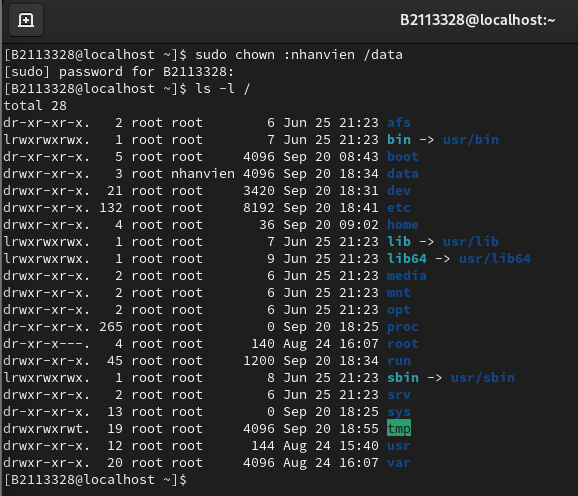
* 1. Thực hiện lệnh df -h để xem kết quả. (chụp hình minh hoạ)

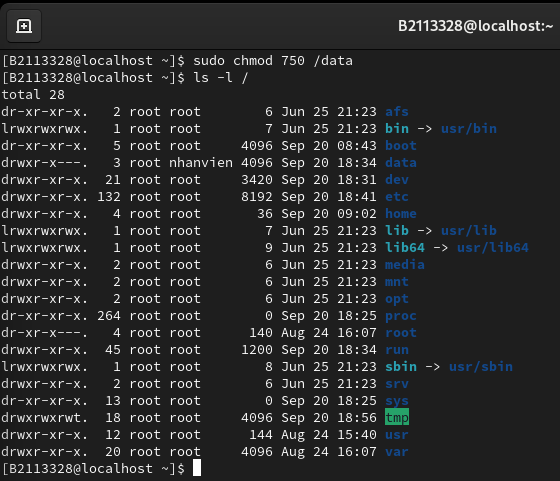


1. **Phân quyền trên hệ thống tập tin**
   1. Tạo nhóm người dùng nhanvien, thêm người dùng ở 2.1 vào nhóm nhanvien

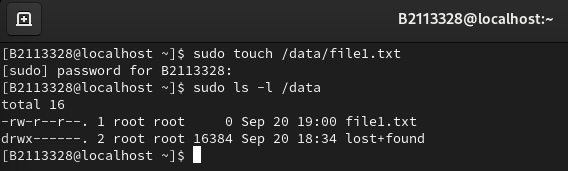


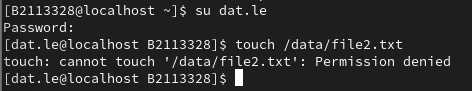
* 1. Chuyển *nhóm chủ sở hữu* của thư mục /datasang nhanvien. Phân quyền cho thư mục /data là chủ sở hữu có quyền read, write và execute, nhóm chủ sở hữu có quyền read và execute, những người khác không có bất kỳ quyền gì cả (chụp hình minh hoạ).



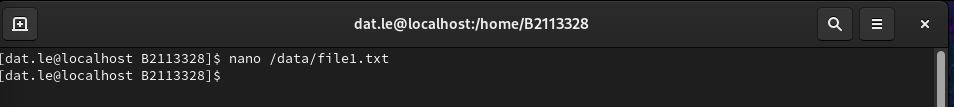


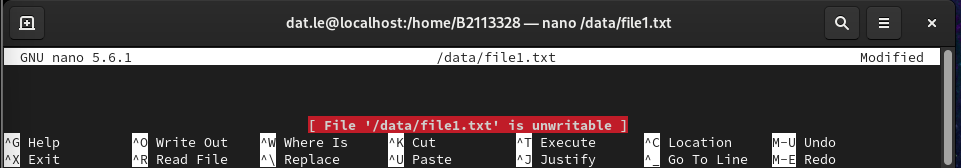
* 1. Dùng quyền sudo tạo tập tin /data/file1.txt. Sau đó dùng tài khoản ở 2.1 tạo tập tin /data/file2.txt. Quan sát và cho biết kết quả trong 2 trường hợp (chụp hình minh hoạ).



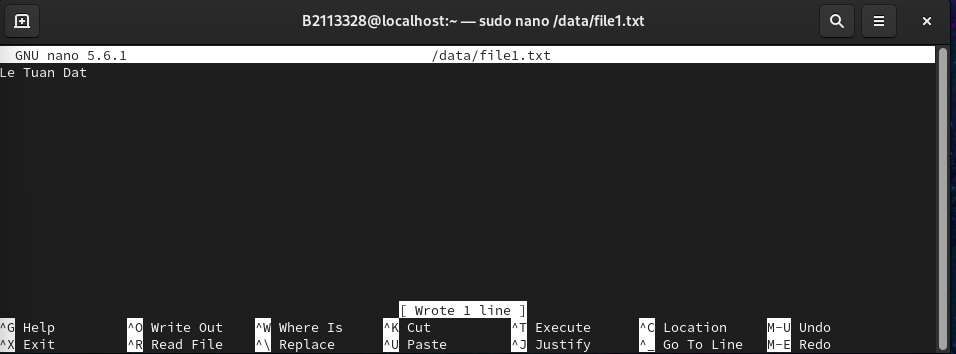


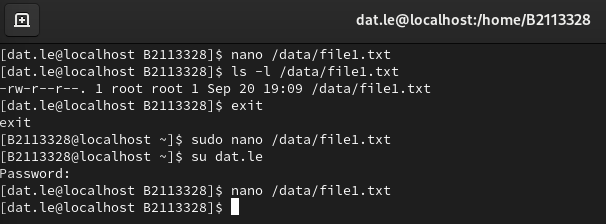
* 1. Dùng tài khoản ở 2.1 *mở và thay đổi nội dung* tập tin /data/file1.txt, cho biết kết quả (chụp hình minh hoạ).

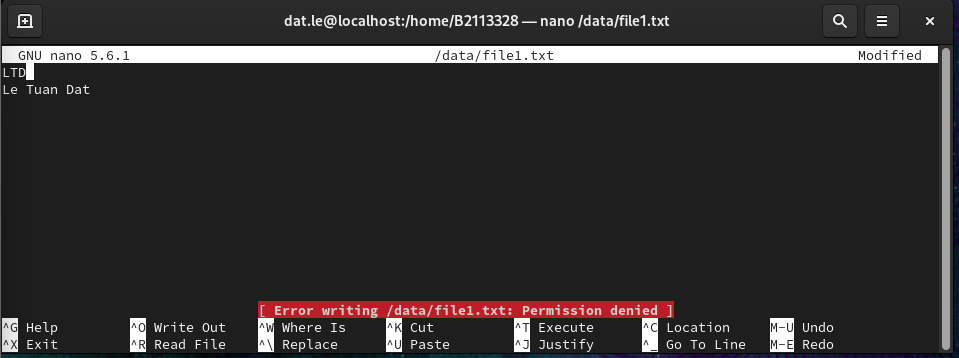




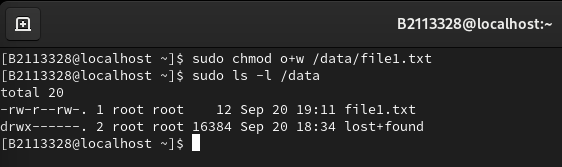


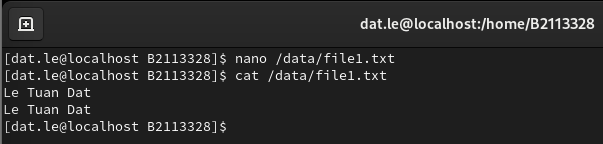




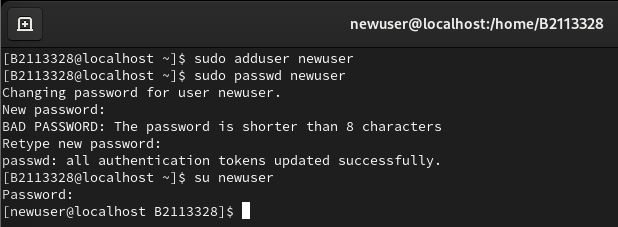


* 1. Cấp quyền cho tài khoản 2.1 có thể thay đổi nội dung tập tin /data/file1.txt (chụp hình minh hoạ).

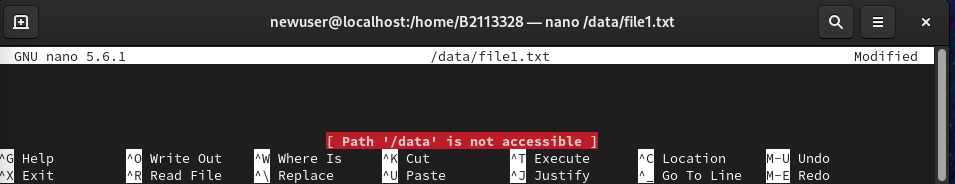




* 1. Tạo thêm một tài khoản mới newuser, dùng tài khoản này mở tập tin /data/file1.txt, cho biết kết quả (chụp hình minh hoạ).

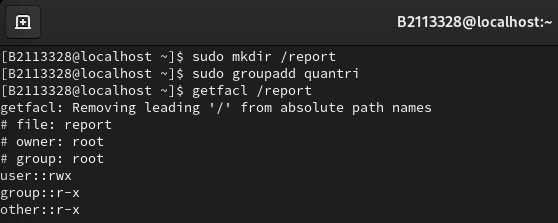


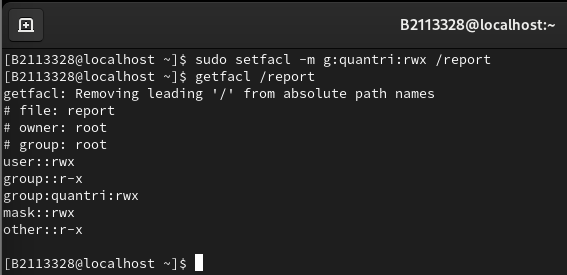


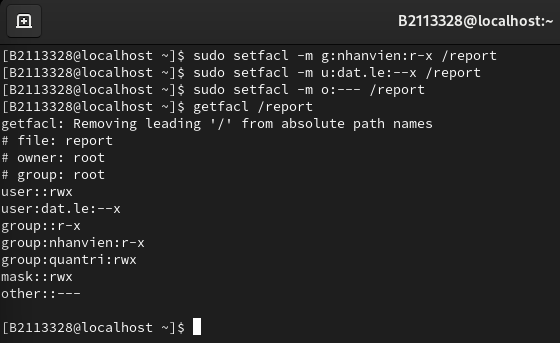


* 1. Dùng quyền sudo tạo thư mục /report và tạo nhóm người dùng quantri. Phân quyền trên thư mục /report sao cho nhóm quantri có quyền read, write và execute, nhóm nhanvien có quyền read và execute, người dùng ở 2.1 có quyền execute, những người khác không có bất kỳ quyền gì cả (chụp hình minh hoạ).

=> (Sử dụng ACL - Access Control List)







--- Hết ---