Họ và tên: Nguyễn Minh Mạnh

Link source code: [Bài tập tuần 2](https://github.com/minhmannh2001/VCS_Intern/tree/main/exercise2)

**Lý thuyết**

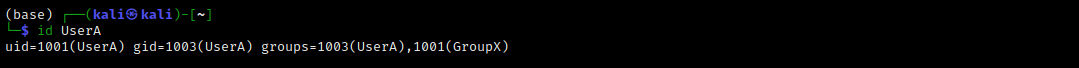
1. **Quản lý User và Group trong hệ điều hành Ubuntu**

Hệ điều hành Ubuntu cho phép nhiều người dùng hoạt động trên hệ thống thông qua một hệ thống quản lý người dùng và nhóm người dùng.

Người dùng là một thực thể trong hệ điều hành Ubuntu. Mỗi người dùng có thể thực hiện các thao tác với file và thực hiện các câu lệnh của hệ thống. Mỗi người dùng được gán với một ID duy nhất, không bị trùng với các người dùng khác trong hệ thống.

Các thông tin liên quan đến người dùng được lưu trong file **/etc/passwd**. Để xem thông tin về các người dùng trong hệ thống, có thể sử dụng các lệnh **less, more**, **cat** để hiển thị nội dung trong file. Hoặc sử dụng câu lệnh **id** kèm theo các câu lệnh chỉnh sửa thông tin để lấy ra nội dung cần thiết.

Dưới dây chúng ta sử dụng lệnh **id** để xem các thông tin về người dùng UserA

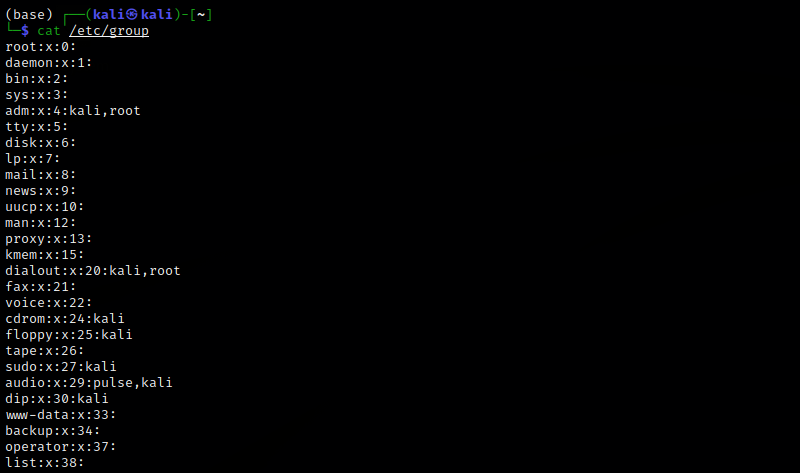


Trong Linux, group là một nhóm những người dùng có chung một số đặc điểm. Mục đích của group là để thiết lập một tập các đặc quyền bao gồm quyền đọc, viết và thi hành cho một tài nguyên trong hệ thống. Từ đó chia sẻ đặc quyền này giữa các người dùng trong cùng một nhóm.

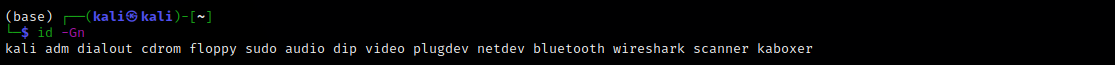
Có 2 loại group trong hệ điều hành Ubuntu:

* Primary group (Nhóm chính): là group được tự động gán với một file mới được tạo ra bởi người dùng. Thông thường, group này có tên trùng với tên của người dùng. Mỗi người dùng chỉ được phép phân vào một primary group duy nhất.
* Secondary group (Nhóm bổ sung): được dùng để cấp tập quyền cho nhóm người dùng. Không bắt buộc người dùng luôn phải thuộc vào 1 secondary group.

Các thông tin liên quan đến group được lưu trong file **/etc/group**. Để liệt kê danh sách các group trong hệ thống, ta sử dụng các câu lệnh **less**, **cat**, **more** để hiển thị nội dung của file **/etc/group**. Có thể sử dụng thêm các câu lệnh **awk**, **cut** để chỉnh sửa thông tin trước khi in ra.

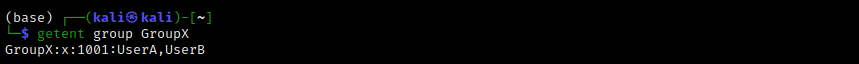


Hoặc sử dụng lệnh **id [user\_name]** để hiển thị thông tin liên quan đến người dùng, trong đó có cả thông tin về group.

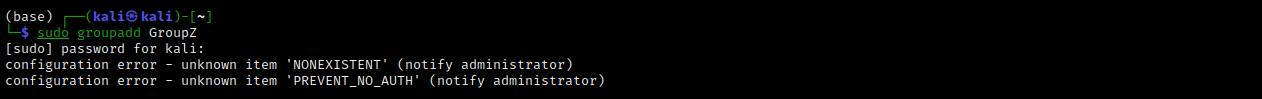


Trong đó, nhóm đầu tiên là nhóm chính (primary group)

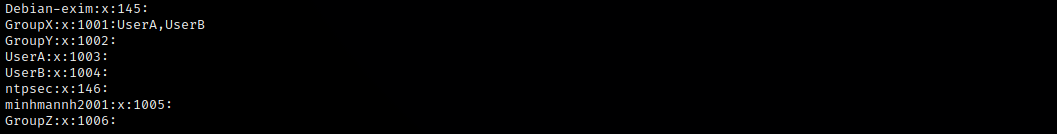
Để hiển thị danh sách người dùng của một group trong hệ thống, ta sử dụng câu lệnh **getent** **group [group\_name]**.



Để tạo một nhóm mới trong hệ thống, ta sử dụng câu lệnh **groupadd** với các tham số phù hợp.



Kiểm tra lại trong file **/etc/group** ta thấy GroupZ đã được thêm vào hệ thống với group ID là 1006.

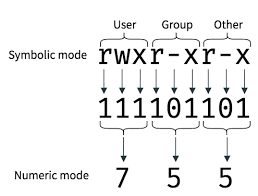


1. **Phân quyền sử dụng file trong hệ điều hành Ubuntu**

Trong hệ điều hành Ubuntu, mọi tài nguyên đều được xử lý như là một file. Mỗi file khi được tạo ra đều được gắn liền với một người dùng sở hữu nó (owner) và nhóm của người dùng sở hữu nó (group).

Các cờ phân quyền của file, folder.

Mỗi file đều có các quyền đọc (read), quyền chỉnh sửa (write) và quyền thực thi (execute). Các thông tin này được lưu trữ lại bởi file descriptor tương ứng với nó. Cụ thể, hệ thống sẽ lưu trữ thông tin này dưới dạng cờ bit phân quyền như sau:



Ở dạng symbolic mode (thân thiện với người dùng), ta có một dãy gồm 9 ký tự được chia thành 3 nhóm như sau: người sở hữu file (user), nhóm của người sở hữu file (group) và nhóm những người dùng khác (other). Với ý nghĩa của mỗi ký tự như sau:

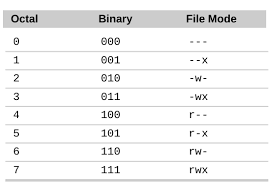
* r - quyền đọc file/quyền xem danh sách các file hoặc subfolder trong folder
* w - quyền ghi vào file/quyền tạo, xóa file hoặc subfolder mới trong folder hiện tại
* x - quyền thực thi file/quyền thay đổi địa chỉ thư mục đang làm việc hiện tại đối với folder

Ký hiệu - (hyphen) thể hiện rằng người dùng tương ứng với nhóm quyền đấy sẽ không có quyền ở vị trí của ký hiệu - (hyphen).

Ví dụ như hình bên trên, ta thấy ở nhóm quyền của Group, ở vị trí của quyền ghi (write permission), ta thấy có ký hiệu - (hyphen). Vì vậy, đối với những người dùng có cùng nhóm với người sở hữu (owner), họ sẽ không có quyền ghi vào trong file này.

Thực chất, máy tính lưu các quyền này dưới dạng dãy các bit (cờ phân quyền). Bao gồm dãy 10 bit. Vị trí đầu tiên đánh dấu liệu file có phải là một folder hay không. Bản chất của folder vẫn được lưu trữ như là một file trong hệ điều hành Ubuntu. Tuy nhiên nó có các thuộc tính đặc biệt hơn so với một file nên ta phân biệt với file để dễ thao tác. Nếu là một folder thì bit này sẽ được đánh dấu là 1. Hoặc ngược lại. Tương tự đối với các quyền còn lại, theo thứ tự từ trái qua phải sẽ là quyền đọc, quyền ghi và quyền thực thi. Lặp lại đối với hai nhóm: người dùng cùng nhóm với chủ sở hữu và nhóm các người dùng khác. Tại mỗi quyền, nếu nó được cung cấp đối với file, thì sẽ có ký hiệu là 1, ngược lại nếu không được cung cấp quyền thì sẽ có ký hiệu là 0.

Ngoài ra, ta có thể biểu diễn cờ dưới dạng số nguyên như sau:



Với quyền đọc (read permission) tương ứng với giá trị 4, quyền ghi (write permission) tương ứng với giá trị 2, quyền thực thi (execution permission) tương ứng với giá trị 1.

Một file nếu có đầy đủ các quyền đọc, ghi và thực thi sẽ có giá trị tương ứng là 7 = 4 + 2 + 1. Do đó, với các số từ 0 đến 7, ta có thể biểu diễn được sự phân quyền đối với một file.

Ngoài những cờ cơ bản trên, ta còn có một số loại cờ khác như cờ UID, cờ GID, cờ Sticky Bit và cờ Conditional Execute.

Ý nghĩa của các cờ trên như sau:

|  |  |  |
| --- | --- | --- |
| Cờ | File | Folder |
| Set UID | File có cờ này cho phép tất cả người dùng quyền thực thi file như là người sở hữu. | Cờ này không có tác dụng đối với folder. |
| Set GID | File có cờ này cho phép tất cả người dùng quyền thực thi file như là người dùng cùng nhóm với người sở hữu. | Đối với folder có cờ này, khi người dùng tạo file trong folder này. Các file sẽ được tự động gán cho nhóm người dùng tương ứng với nhóm người dùng của folder. |
| Sticky Bit | Cờ này không có tác dụng đối với file. | Khi cờ này được bật, hệ thống sẽ ngăn chặn những người dùng không phải chủ sở hữu xóa các file trong folder. |
| Conditional Execution | Chỉ khi quyền thực thi đã được trao cho ít nhất 1 trong 3 nhóm người dùng thì hệ thống mới cho phép thêm quyền thực thi vào file này. | Cho phép xem danh sách các file trong folder. |

Các lệnh thao tác để điều chỉnh phân quyền trong hệ điều hành Ubuntu

Để thay đổi chế độ phân quyền đối với file trong hệ thống, ta sử dụng các câu lệnh sau:

**chmod +rwx filename** để bật tất cả các quyền đối với file **filename**

**chmod -rwx directoryname** để tắt tất cả các quyền đối với folder **directoryname**

**chmod +x filename** để bật quyền thực thi đối với file **filename**

**chmod -wx filename** để tắt các cờ ứng với quyền viết và quyền thực thi đối với file **filename**

Lưu ý rằng câu lệnh trên chỉ thay đổi các quyền đối với chủ sở hữu của file.

Để thay đổi chế độ phân quyền đối với file trong hệ thống cho người dùng cùng group với chủ sở hữu và những người dùng khác ta thêm các **option g** đối với group hoặc **option o** đối với những người dùng khác.

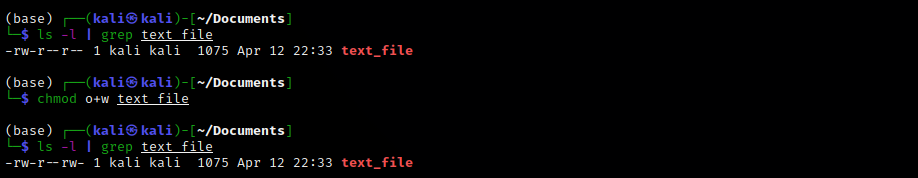
**chmod g+w filename**

**chmod g-wx filename**

**chmod o+w filename**

**chmod o-rwx foldername**

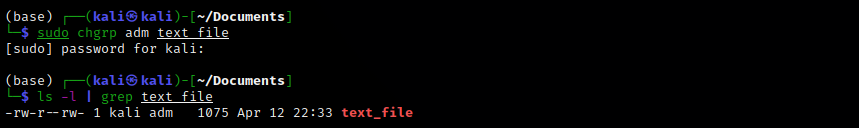
Để thay đổi chế độ phân quyền đối với file cho tất cả người dùng, sử dụng **option a**.



Để thay đổi nhóm người dùng của file trong hệ thống Ubuntu, ta sử dụng câu lệnh **chgrp** như sau:

**chrgp groupname filename**

**chrgp groupname foldername**

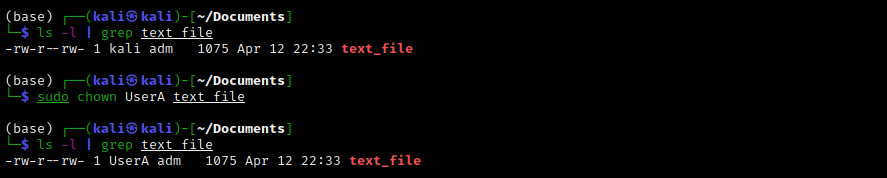
****

Lưu ý rằng các nhóm **groupname** phải tồn tại, nếu không sẽ gây ra lỗi.

Để thay đổi quyền sở hữu đối với file trong hệ điều hành Ubuntu, ta sử dụng câu lệnh **chown**:

**chown username filename**

**chown username foldername**

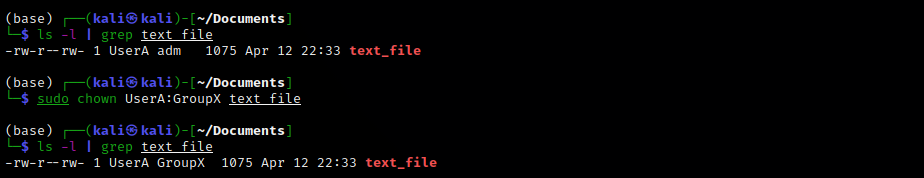
****

Các câu lệnh trên chỉ thay đổi quyền sở hữu đối với folder, chủ sở hữu của các file và subfolder bên trong không thay đổi. Ta thêm **option -R** để thực hiện đệ quy câu lệnh đối với các file và subfolder bên trong.

**chown -R username filename**

Kết hợp thay đổi người sở hữu và nhóm của người sở hữu trong một câu lệnh như sau:

**chown -R username:groupname filename**

****

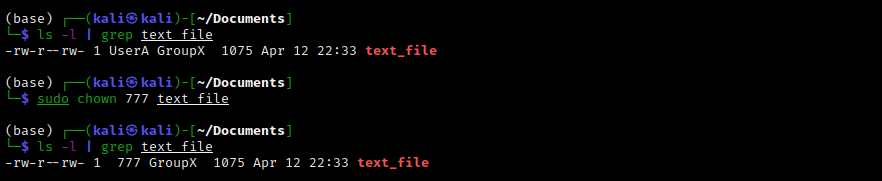
Thay đổi chế độ phân quyền sử dụng các mã số nguyên (numeric code) tương ứng

Ví dụ:

**chmod 777 foldername** sẽ cấp quyền đọc, viết, thực thi cho tất cả người dùng trong hệ thống

**chmod 700** **foldername** sẽ chỉ cấp quyền đọc, viết, thực thi cho người sở hữu, tất cả những người dùng còn lại không có quyền đối với folder này.

**chmod 327** **foldername** sẽ cấp quyền ghi và thực thi cho người sở hữu, quyền ghi cho nhóm của người sở hữu và tất cả các quyền đối với những người dùng còn lại.



1. **Khái niệm real user id và effective user id của một process**

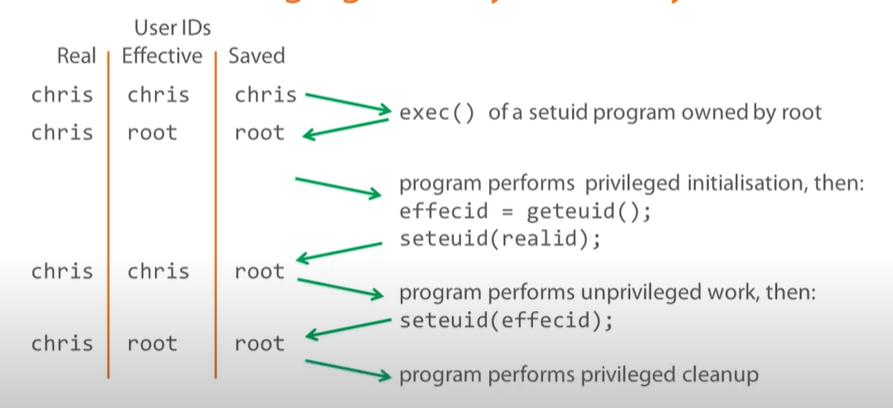
Mỗi process khi khởi chạy đều gắn liền với một bộ UIDs xác định để kiểm tra xem process trên có thể thực hiện những tác vụ nào, hợp pháp hay là không.

real user id: đây chính là UserID của người dùng đã khởi chạy process này. Nó xác định phạm vi mà chương trình có thể thực hiện, những file nào mà chương trình có quyền tiếp cận.

effective user id: Thông thường, nó chính là real user id. Tuy nhiên nó có thể thay đổi để cho phép những người dùng thông thường có thể mượn đặc quyền root để tiếp cận các file mà chỉ người dùng root mới có quyền tiếp cận. Máy tính sẽ kiểm tra thông tin trường này để xác định xem bạn có thể làm được những gì. Đây là một cơ chế bảo mật của Linux, cho phép người dùng bình thường có thể thực hiện một vài công việc như là người dùng root nhưng lại không cho họ quyền root thực sự.

saved user id: Khi một chương trình chạy với đặc quyền root, nó sẽ cần chuyển về các đặc quyền thấp hơn để thực hiện các tác vụ, điều này có thể thực hiện bằng cách thay đổi về đặc quyền của người dùng thông thường.

Khi ta chuyển đổi đặc quyền, effective user id sẽ được chuyển về giá trị tương ứng với đặc quyền thấp hơn và giá trị cũ của effective user id sẽ được lưu trữ trong trường saved user id, để có thể chuyển đổi lại đặc quyền root khi công việc hoàn tất.



Hình trên minh họa việc chuyển đổi đặc quyền trong chương trình chạy dưới quyền root. Ban đầu người khởi tạo là người dùng thông thường chris, sau đấy, vì chương trình đang bật cờ setuid nên các trường effective uid và saved uid sẽ được chuyển thành giá trị của người dùng root. Sau đấy để thực hiện công việc có đặc quyền thấp hơn, ta thay đổi effective uid về giá trị ban đầu bằng cách gán effective uid bằng giá trị của real uid. Khi thực hiện xong, ta gán lại giá trị saved uid vào effective uid. Khi này chương trình lại có thể thực hiện với đặc quyền root.

1. **Khái niệm cờ setuid và cờ setgid của file binary.**

Như trình bày ở bảng trên.