Công ty An ninh mạng Viettel

Báo cáo về User/Group Management

Sinh viên: Nguyễn Đan Trường

*MỤC LỤC*

[Chương 1. Quản lý user account 3](#_Toc151393392)

[1. Quản trị tài khoản người dùng 3](#_Toc151393393)

[2. Tạo tài khoản người dùng 9](#_Toc151393394)

[3. Group 12](#_Toc151393395)

[Chương 2. Phân quyền trong tập tin và thư mục 13](#_Toc151393396)

[1. Các quyền trong Linux 13](#_Toc151393397)

[Chương 3. Sudo command và Bash shell enviroment 17](#_Toc151393398)

[1. Chuyển đổi người dùng với lệnh su 17](#_Toc151393399)

[2. Cấp quyền thực thi với sudo 17](#_Toc151393400)

[3. Bash Shell enviroment 19](#_Toc151393401)

# Quản lý user account

## Quản trị tài khoản người dùng

Có 2 loại tài khoản:

* Tài khoản root: có quyền quản trị cáo nhất trong hệ thống, được phép làm mọi việc mà không bị kiểm soát
* Các tài khoản thông thường được tạo ra cho các mục đích:
  + Cung cấp tài khoản truy nhập cho người sử dụng hệ thống
  + Cung cấp tài khoản dùng bởi các dịch vụ hệ thống như http, samba, mysql….

Chú ý: tránh làm việc dưới tài khoản của root cho các công việc thông thường hằng ngày với Linux, mỗi user có một định danh duy nhất gọi là UID

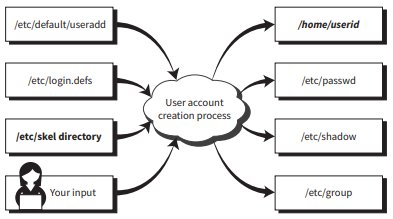
Quản lý người dùng hệ thống bằng lệnh

* useradd: tạo user mới
* usermod: chỉnh sửa thông tin user.
* userdel -r: xóa user khỏi hệ thống
* passwd: đổi mật khẩu, chính sách thay đổi mật khẩu
* groupadd: tạo group mới
* groupdel: xóa group khỏi hệ thống
* groupmod: chỉnh sửa thông tin group.

Mỗi user thuộc ít nhất một group. Mỗi group cũng có một định danh duy nhất là GID

Mỗi users cần có những thông tin: tên user, UID, tên group, GID, home directory... Linux quản lý thông tin bằng file text. Có thể chỉnh sửa thông tin của users bằng công cụ, hoặc sửa trực tiếp bằng text file.

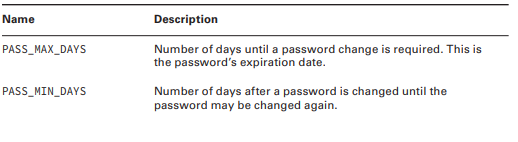
**Configuring Use Account**

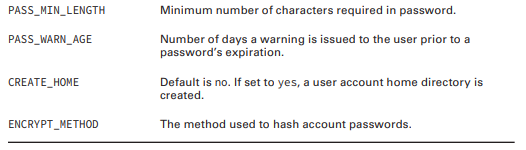
****

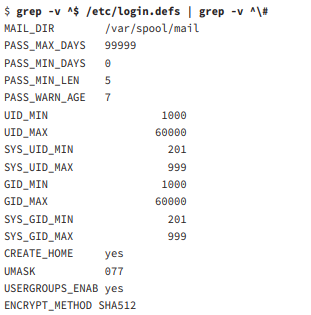
Khi muốn thêm một user mới vào hệ thống:

* Các file được đọc: */etc/default/useradd, /etc/login.defs,* ***/etc/skel directory***
* Các file đượ ghi vào: ***/home/userid****, /etc/password, /etc/shadow, /etc/group*

File */etc/login.defs*: định nghĩa liên quan đến những cài đặt mặc định của người dùng



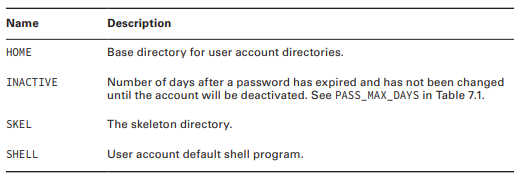




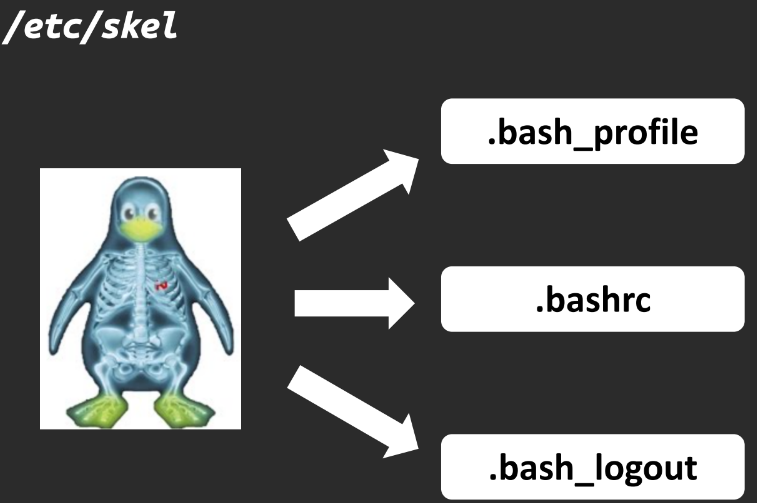
File */etc/default/useradd*: định nghĩa những chỉ dẫn tiếp theo trong việc tạo tài khoản

|  |  |
| --- | --- |
|  |  |

Đây là những cài đặt cho một user khi mới được add vào hệ thống.



Thư mục */etc/skel*: chứa các file mẫu, sẽ được copy vào thư mục người dùng khi người dùng đó được tạo ra

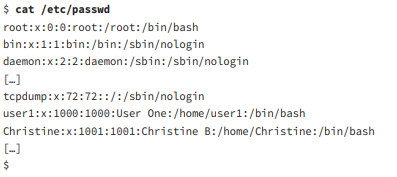


.profile: khởi tạo thiết lập tự đông các biến môi trường khi người dùng tạo phiên làm việc (login vào hệ thống)

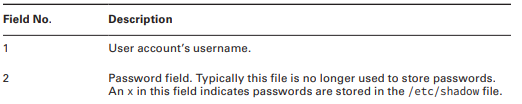
.bashrc: tệp cấu hình cho shell Bash, chứa các cài đặt môi trường và lệnh được thực hiện mỗi khi bạn mở một cửa sổ terminal

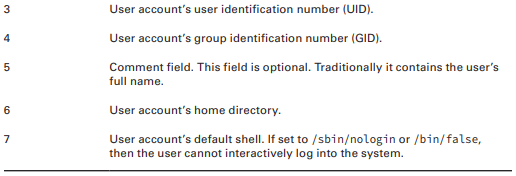
.bash\_logout: thiết lập các lệnh, cấu hình thực thi khi người dùng thoát khỏi phiên làm việc

File */etc/passwd*: gồm các dòng lưu thông tin người dùng, tất cả các user đều có thể đọc file

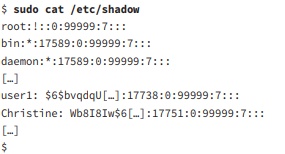


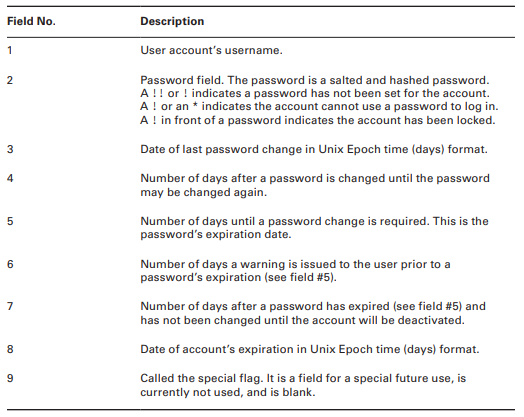
Mỗi dòng tương ứng với một user và bao gồm 7 trường thông tin ngăn cách nhau bởi dấu “:” :





File */etc/shadow*: lưu password của các user nhưng chỉ duy nhất user root có quyền đọc/ghi vào file này





Trường số 2 lưu thông tin password đã được mã hóa bằng các thuật toán như MD5, SHA-1, SHA-2, …

Ký tự “$” trước mật khẩu đã được mã hóa cho biết mật khẩu này được băm theo thuật toán nào.

Trường mật khẩu trong file /etc/shadow có cấu trúc dạng ***$id$salt$hash***

***id=1*** mật khẩu được mã hóa bằng thuật toán ***MD5***

***id=2*** mật khẩu được mã hóa bằng thuật toán ***blowfish*** (thuật toán mã hóa đối xứng, dùng khóa nào để mã hóa dữ liệu thì dùng chính khóa đó để giải mã)

***id=2a*** mật khẩu được mã hóa bằng thuật toán ***eksblowfish***

***id=5*** mật khẩu được mã hóa bằng thuật toán ***SHA-256***

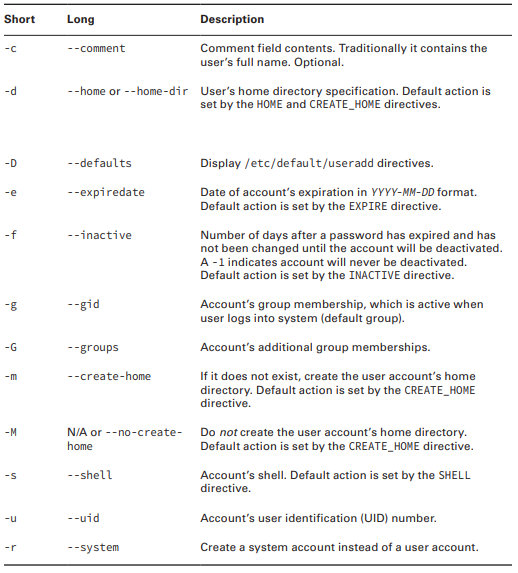
***id=6*** mật khẩu được mã hóa bằng thuật toán ***SHA-512***

***salt***: 8 characters

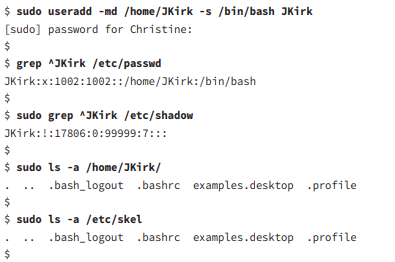
* Mật khẩu của user sẽ được hash với giá trị salt ngẫu nhiên. Giá trị salt và mật khẩu đã được hash sẽ được lưu trong file /etc/shadow
* Khi user login vào hệ thống thì giá trị salt sẽ được lấy ra và dùng để hash mật khẩu. Nếu giá trị mật khẩu hash trong file /etc/shadow và giá trị vừa được hash trùng nhau thì user được xác thực.

## Tạo tài khoản người dùng

Khi thêm một user account vào hệ thống có thể thêm các tùy chọn để thay đổi những cấu hình mặc địch khi một user được tạo ra:

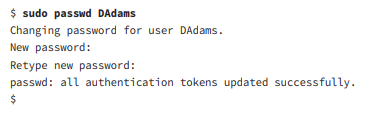


Trên đây là các option của lênh useradd.



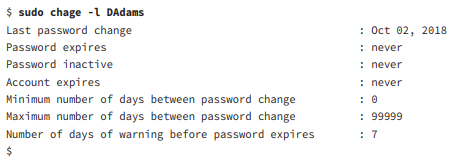
**Quản lý password**

Thay đổi password của user:

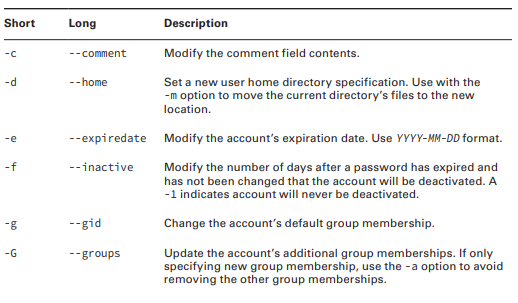
****

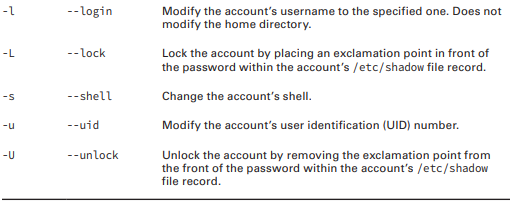
Xem thông tin trạng thái password cả user:

****

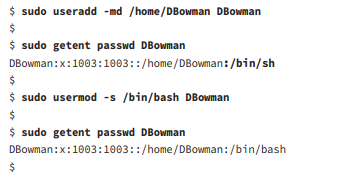
****

**Modify account bằng công cụ usermod**

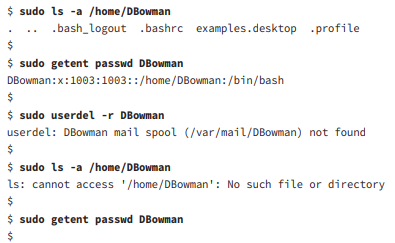








**Xóa account với công cụ userdel**



## Group

Trong Linux, các user được tổ chức thành các nhóm (group) để quản lý và kiểm soát quyền truy cập vào tệp tin, thư mục và tài nguyên hệ thống. Mỗi người dùng có thể thuộc nhiều nhóm và thông thường, một nhóm có thể chứa nhiều người dùng.

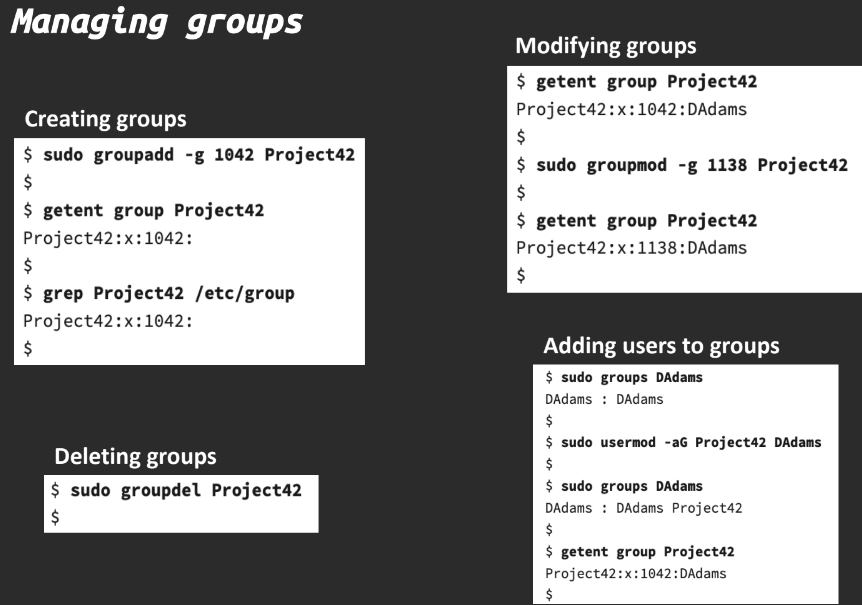
Các tệp tin và thư mục trên hệ thống Linux thường được gán quyền truy cập dựa trên người dùng và nhóm. Một nhóm có thể được gán làm chủ sở hữu của một tập tin hoặc thư mục, cho phép tất cả các thành viên trong nhóm có quyền truy cập đến tệp tin hoặc thư mục đó.

Nhóm cũng được sử dụng để chia sẻ tài nguyên giữa các thành viên trong nhóm một cách thuận tiện.

**Mối quan hệ giữa user – group**

* Mỗi user được gán vào ít nhất một group chính khi được tạo ra. Group chính này thường trùng với tên người dùng.
* User có thể thuộc nhiều nhóm bổ sung khác nhau.
* Khi một người dùng tạo tệp tin và thư mục, nó sẽ được gán một nhóm chủ sở hữu. Các thành viên trong nhóm chủ sở hữu có quyền đọc, ghi và thực thi tệp hoặc thư mục đó.

**Quản lý group**



# Phân quyền trong tập tin và thư mục

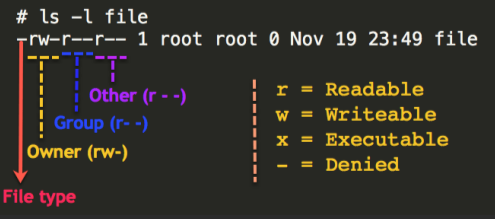
## Các quyền trong Linux

Trong Linux có 3 quyền và 2 nhóm quyền có thể được gán quyền được phân chia như sau:

* Quyền đọc: r (read) hay 4
* Quyền ghi: w (write) hay 2
* Quyền thực thi: x (excute) hay 1

Các quyền được áp dụng trên 3 nhóm người dùng, kí hiệu bằng 2 ký tự: u, g, o

* u = owner user = chủ sở hữu
* g = group = những người có cùng nhóm với chủ sở hữu
* o = others = tất cả những người khác



Quyền truy cạp có thể thiết lập theo 2 dạng với lện *chmod*:

* Mode ký hiệu (symbolic): *chmod [augo] +-= [rwx] filename*

*u (user), g (group), o (other), a (all), + thêm quyền , - bớt quyền*

* Mode dùng số bát phân (octal): *chmod [0-7][0-7][0-7] filename*

Chỉ những người sở hữu file mới có thể thay đổi được mức đặc quyền đối với file

*# chmod 777 filename*

*# chmod g-w,o+r filename*

*# chmod a+r filename*

*# chmod og-x filename*

*# chmod u+rwx filename*

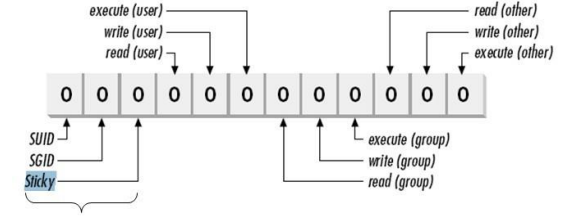
Quyền thực thi (x) đối với thư mục tức là bạn có thể truy cập (cd,ls) vào thư mục đó.

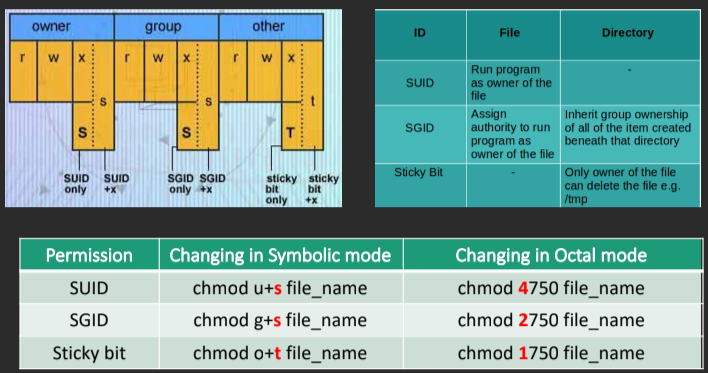
**Default permission**

Ta có thể thiết lập quyền deafult cho các file hoặc thư mục được tạo ra bởi hệ thống bằng công cụ umask



**Các quyền đặc biệt**

****

****

**SUID**

Khi một tệp thực thi được đặt quyền SUID, nó sẽ chạy với quyên của chủ sở hữu tệp.

Một số ví dụ:

* Thay đổi mật khẩu sử dụng lênh “passwd”. Khi người dùng muốn thay đổi mật khẩu của mình họ cần có quyền ghi vào tập “/etc/passwd”. Tuy nhiên, không phải tất cả người dùng đều có quyền ghi vào tệp tin. Do đó, lệnh “passwd” có quyền SUID để chạy với quyên chủ sở hữu (root) cho phép thay đổi mật khẩu



* Lệnh Ping cũng sử dụng quyền SUID để gửi gói tin ICMP mà không cần đặc quyền root



**SGID**

Khi một tệp thực thi được đặt quyền SGID, nó sẽ chạy với quyền của group owner.

Khi một thư mục được đặt quyền SGID, tất cả các tệp tin và thư mục mới tạo ra trong thư mục đó sẽ kế thừa group owner chứ không phải nhóm tạo ra nó.

Một số ví dụ:

* Khi bạn muốn đảm bảo tất cả các tệp tin và thư mục mới tạo ra trong thư mục chia sẻ đó thuộc cùng một nhóm.

**Sticky bit**

Khi một thư mục có quyền sticky bit, người dùng chỉ có thể xóa hoặc di chuyển các tệp tin của chính họ trong thư mục đó.

Một số ví dụ:

* Thư mục /tmp: có quyền sticky bit để ngăn chặn người dùng xóa tệp tin của người khác trong thư mục chung sử dụng.



Mặc định khi khi user tạo ra một tệp mới thì group owner là primary group của user đó. Ta có thể thay đổi owner và group owner bằng các lệnh:

*chown [option] new\_owner file*

*chgrp [option] new\_group file*

Có thể thay đổi cả owner và group owner bằng câu lệnh:

*chown user:group file.txt*

# Sudo command và Bash shell enviroment

## Chuyển đổi người dùng với lệnh su

Mỗi một user được tạo trên hệ thống đều phải có một UID. Hệ điều hành sẽ quản lý tài khoản người dùng thông qua UID, còn user name chỉ là tên gọi giúp con người dễ dàng phân biệt các user.

Tài khoản quản trị root được Linux tự động tạo ra với UID = 0. Có thể chỉnh sửa UID của một user về 0 để có quyền hạng ngang bằng root => để leo thang đặc quyền cho một user thông thường.

Lệnh su (super user) trên linux có chức năng yêu cầu chọn tài khoản root để chuyển đổi. Nếu không được chỉ định, lệnh sẽ yêu cầu chọn tài khoản root để chuyển đổi.

*$ su - root*

Trong trường hợp muốn chuyển đổi sang một tài khoản khác không phải root ta dùng lệnh:

*$ su – user\_name*

## Cấp quyền thực thi với sudo

Lệnh **sudo** (**SuperUser DO) là một thay thế nâng cao và nhiều ưu điểm hơn cơ chếu chuyển sang người dùng khác bằng lênh su. Trong đó ưu điểm lớn nhất là cho phép người dùng quản trị kiểm soát được các thao tác của người dùng có can thiệp đến hệ thống.**

**Lệnh sudo cho phép cung cấp đặc quyền root thực hiện một số lệnh thay vì tất cả các lệnh. Các khai báo cho user được làm gì? Được cấu hình trong file */etc/sudoers***

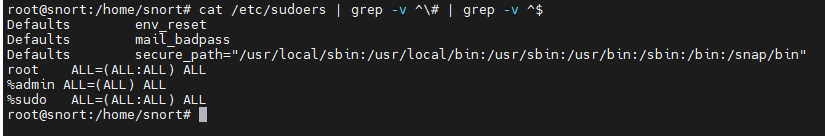




Sudo là một lệnh dạng SUID -> mọi user đều có quyền chạy lệnh này

Lệnh được thực hiện qua sudo đều được ghi log vào file /var/log/secure (Redhat/Fedora/CentOS) hoặc /var/log/auth.log (Ubuntu/Debian)

**Cú pháp /etc/sudoers**

****

USER MACHINE=(TARGET-USERS) COMMANDS

* USER: người sử dụng được quyền thực thi, Các user được phân cách nhau bằng dấu phẩy “,”
* MACHINE: máy mà quyền thực thi được áp dụng lên
* TARGET-USERS: người dùng cho mượn quyền thực thi, nếu tham số này không tồn tại người dùng sudo sẽ chạy với quyền root.
* COMMANDS: lệnh mà người dùng sudo được quyền thực thi. Các lệnh phân cách nhau bằng dầu phẩy “,”

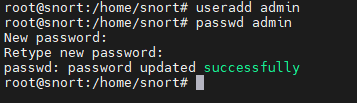
Nếu cấp quyền cho group, tham số USER được thay bằng %GROUP

Từ khóa ALL có nghĩa là tất cả các user, tất cả các nhóm, tất cả các lệnh, tất cả các máy.

Nếu thiết lập dài hơn 1 dòng, có thể dùng dấu “\” để viết tiếp xuống dòng tiếp theo

Từ khóa NOPASSWD cung cấp khả năng thực thi lệnh mà không yêu cầu nhập password.

VD: thực hiện tạo user admin



Khi dùng lệnh sudo, mật khẩu của root được giữ bí mật. Nếu kiểm soát vấn đề ủy quyền thông qua sudo không chặt chẽ thì normal user dễ dàng chiếm quyền điều khiển hệ thống với đặc quyền root

Cho phép user admin sudo lênh su

Thêm dòng ***admin ALL=/bin/su*** ở cuối file /etc/sudoers

Login với user admin, sau đó gõ lệnh ***sudo su - root*** rồi cung cấp mật khẩu của user admin là có quyền root mà không cần biết mật khẩu root



Password mà user admin nhập vào không phải là password root, điều này khiến cho người quản trị root biết được các hoạt động của admin.

## Bash Shell enviroment

Biến môi trường trong Bash Shell là các biến có ảnh hưởng đến muốn trường làm việc của shell và các tiền trình con. Các biến môi trường thường được sử dụng để lưu trữ thông tin đường dẫn, ngôn ngữ, biến đếm, và nhiều thông tin khác.

Để xem tất cả các biến môi trường hiện tại sử dụng lệnh: “**env**”

Xem một biến môi trường cụ thể: “**echo $TEN\_BIEN**”

Đặt giá trị cho một biến môi trường: “**TEN\_BIEN=giatri**” và “**export TEN\_BIEN**”

Xóa một biến môi trường: “**unset TEN\_BIEN**”

Một số biến môi trường phổ biến:

* **PATH**: chứa đường dẫn các thư mục nơi hệ thống sẽ tìm khiếm các tệp thực thi
* **HOME**: chứa đường dẫn đến thư mục home của người dùng hiện tại
* **USER**: chứa tên người dùng hiện tại
* **PS1**: định dạng của dòng lệnh
* **LANG và LC\_\***: cài đặt ngôn ngữ và định dạng vùng của hệ thống

Lưu ý rằng việc sử dụng **export** làm cho biến chỉ là biến môi trường trong quá trình thực hiện của shell hiện tại và của các tiến trình con tạo ra từ nó. Khi bạn tắt shell hoặc mở một shell mới, bạn cần xuất biến môi trường lại nếu bạn muốn nó có hiệu lực. Điều này thường được thực hiện trong các tệp cấu hình như **.bashrc** hoặc **.bash\_profile**.

**Setting Enviroment Variable at login**

**Login shell** là phiên shell bắt đầu bằng việc xác thực người dùng. Nếu bạn bắt đầu một phiên shell mới từ trong phiên đã xác thực thì một phiên **non-login shell** sẽ được bắt đầu.

Khi một phiên login shel được bắt đầu, nó sẽ đọc chi tueets cấu hình từ tệp /etc/profile trước tiên. Sau đó, nó sẽ tìm đến tệp cấu hình shell login trong thư mục chính của người dùng để lấy chi tết cấu hình dành riêng cho người dùng.

Nó thực hiện đọc các tệp ~/.bash\_profile, ~/.bash\_login và ~/.profile

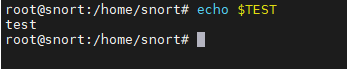
Ngược lại một phiên được xác định là non-login shell sẽ đọc file /etc/bash.bashrc và sau đó là tệp ~/.bashrc

Bạn muốn thiết lập các biến môi trường dành riêng cho người dùng và thường muốn các cài đặt có sẵn trong cả 2 phiên login shell và non-login shell. Nơi xác định các biến môi trường là ~/.bashrc:

*$vim ~/.bashrc*

Thêm dòng: *export MY\_VARIABLE="MyValue"*

Chạy lại tệp caais hình: *source ~/.bashrc*



Sau khi login lại ta thấy biến môi trường vẫn còn tồn tại.