CHƯƠNG 04: QUẢN TRỊ NGƯỜI DÙNG VÀ NHÓM

1. Một số khái niệm

- Để truy nhập vào hệ thống, người dùng phải có một tài khỏan (account).
- Mỗi tài khỏan có một mã nhận diện người dùng (user ID) tương ứng và thuộc về một tài khỏan nhóm khởi nạp nào đó.
- Nhóm người dùng (group) là một quy định logic của một tổ chức người dùng. Mỗi tài khỏan nhóm có một mã số nhận diện nhóm (group ID) tương ứng.

- Trong Linux, tên tài khỏan người dùng và tên tài khỏan nhóm là duy nhất, tuy nhiên user ID và group ID có thể trùng nhau.
- Bất kỳ tập tin nào khi được tạo đều được quy định một tài khỏan người dùng là chủ nhân và một tài khỏan nhóm chủ nhân (là nhóm và người dùng tạo ra tập tin đó), nó cũng được gán các quyền riêng đọc, ghi và thi hành cho chủ nhân, cho các nhóm và người dùng khác có trên hệ thống.
- Các quyền truy nhập trên tập tin có thể được thay đổi bởi root và chủ nhân tập tin.

- **Thư mục chủ (home directory)**
  - Khi thực hiện tạo một tài khỏan người dùng, mặc nhiên Linux tạo một thư mục có tên trùng với tên tài khỏan người dùng đó và đặt trong thư mục /home/. Thư mục được tạo này được gọi là thư mục chủ của người dùng.
  - Một tài khỏan không có thư mục chủ sẽ không đăng nhập được hệ thống. Thư mục chủ của người dùng cho phép người dùng chứa các thông tin riêng trên đó.
  - Mặc nhiên khi thư mục chủ của người dùng được tạo thì nội dung có trong thư mục /etc/skel/ cũng được sao chép vào thư mục chủ đó.

- **Thông tin môi trường làm việc người dùng /etc/skel/**
  - Mỗi khi một người dùng đăng nhập, hai script mô tả môi trường làm việc (profile) được thi hành. Một script mô tả môi trường làm việc của hệ thống (/etc/profile) là giống nhau đối với mọi người dùng, và mỗi người dùng có riêng một script có tên là .bash_profile (đối với shell bash) trong thư mục chủ của người dùng đó.
  - Trong thư mục chủ của người dùng có các tập tin về cấu hình màn hình, các tập tin khởi nạp là .bash_profile, .bash_logout và .bashrc

2. Các lệnh quản trị người dùng

2.1. Tạo tài khỏan người dùng-useradd

2.1.1. Cú pháp

useradd [option] username

trong đó username là tên tài khỏan cần tạo, tên tài khỏan này phải là duy nhất và phải bắt đầu bằng một chữ cái.

2.1.2. Các option

- **-u uid [-o]:** Giá trị nhận diện người dùng (UID). Giá trị này phải là duy nhất (trừ trường hợp sử dụng với lựa chọn **-o**). Giá trị này phải là số dương. Khi không có lựa chọn này uid của tài khỏan được tạo sẽ là số nhỏ nhất lớn hơn 99 và lớn hơn mọi uid của người dùng khác. Giá trị 0-99 được sử dụng cho tài khỏan hệ thống.
- **-g** *group_name***:** Chỉ ra tên tài khỏan nhóm khởi nạp của người dùng. Tên nhóm hay mã số nhóm (GID) phải được tồn tại trước. Nếu không có -g và tên nhóm thì mặc nhiên mỗi tài khỏan được tạo sẽ thuộc về một nhóm có tên trùng với tên tài khỏan.

- **-G *group1[, ...,groupN]***: Cho phép chỉ ra một nhóm group muốn cho người dùng là thành viên.
- **-e *expire_date***: Xác định thời điểm hết hạn sử dụng tài khỏan là *expire_date*. Định dạng ngày tháng là YYYY-MM-DD
- **-s *shell***: Quy định tên *shell* đăng nhập của người dùng, nếu không có lựa chọn này tài khỏan sử dụng shell mặc định của hệ thống
- **-d *home_dir***: Tạo thư mục *home_dir*, thư mục này sẽ là thư mục chủ của người dùng. Trường hợp không có lựa chọn này, mặc định hệ thống sẽ tạo thư mục chủ của người dùng trong thư mục /home/

2.2. Thay đổi mật khẩu tài khỏan- passwd

- Sau khi tạo một tài khỏan người dùng, thao tác tiếp theo là phải tạo mật mã truy nhập cho tài khỏan đó. Linux không cho một tài khỏan không có mật khẩu truy nhập hệ thống. Lệnh passwd cho phép tạo mới hay thay đổi mật mã của một tài khỏan, lệnh này cũng được sử dụng để khóa/mở khóa một tài khỏan.

2.2.1. Cú pháp

passwd [option] [username]

Trong đó username là tên tài khỏan muốn tạo mới hay thay đổi mật khẩu. Trường hợp không có username thì sẽ thực hiện thay đổi mật khẩu cho tài khỏan hiện hành.

2.2.2. Các lựa chọn

- **-l:** Lựa chọn này được sử dụng để khóa tài khỏan. Một tài khỏan bị khóa sẽ có ký tự !! đứng trước chuỗi mật mã đã được mã hóa trong /etc/shadow, tài khỏan bị khóa sẽ không login vào hệ thống được

- **-u [-f]:** Mở khóa một tài khỏan đã bị khóa

  Theo mặc định *passwd* không mở khóa tài khỏan nào không sử dụng mật mã. Lựa chọn **-f** bổ sung cho phép mở khóa tài khỏan không sử dụng mật mã
- **-d**: xóa bỏ mật mã của một tài khỏan
- **--stdin**: Chỉ ra rằng passwd se được đọc từ thiết bị nhập chuẩn, thường dùng với pipeline

  Ví dụ: echo 1234567|passwd user1 --stdin

2.3. Xóa tài khỏan người dùng- userdel

- userdel dùng để xóa tài khỏan người dùng và các tập tin liên quan đến tài khỏan người dùng đó.
- **Cú pháp**

  userdel [-r] username

  – Trong đó ***username*** là tên tài khỏan người dùng muốn xóa.

  – Mặc định khi xóa bỏ tài khỏan người dùng thì các tập tin liên quan đến tài khỏan đó không bị xóa. Lựa chọn **-r** trong trong lệnh này cho phép khi xóa bỏ một tài khỏan thì thư mục chủ của tài khỏan và các tập tin của tài khỏan đó cũng bị xóa .

2.4. Thay đổi thông tin tài khỏan-usermod

2.4.1. Cú pháp

usermod [option] username

Trong đó username là tên tài khỏan muốn thay đổi thông tin.

2.4.2. Các option

- **-L**: Lựa chọn này được sử dụng để khóa tài khỏan. Một tài khỏan bị khóa sẽ có ký tự **!** trước chuỗi mật mã đã được mã hóa trong tập tin /etc/shadow

- **-U**: Mở khóa một tài khoản đã bị khóa
- **-l *login_name***: Thay đổi tên tài khoản từ **username** thành ***login_name***. trường hợp thay đổi tên tài khoản thì tên thư mục chủ của tài khoản đó không thay đổi.
- **-g *initial_group***: Thay đổi nhóm khởi nạp của tài khoản. Tên nhóm ***initial_group*** hay mã số nhóm (GID) phải có trước
- **-e *expire_date***: Thay đổi thời điểm hết hạn của tài khoản là *expire_date*. Định dạng ngày tháng là YYYY-MM-DD

- **-s** *shell*: Thay đổi shell đăng nhập của tài khoản. Nếu shell bỏ trống thì cho phép tài khoản sử dụng shell mặc định của hệ thống.
- **-d *home_dir***: Thay đổi thư mục chủ của tài khoản thành thư mục *home_dir*

2.5. Thay đổi thông tin mặc định khi tạo tài khoản.

- Để có thể thay đổi các thông tin mặc định khi tạo một tài khoản, ta có thể thực hiện sửa đổi thông tin trong tập tin **/etc/login.defs**

- **Tập tin login.defs**
  - Tập tin này xác định những thông tin được gán mặc định cho người dùng khi một tài khỏan được tạo. Định dạng tập tin gồm nhiều khai báo theo cú pháp sau

    lựa chọn giá trị
  - Mỗi khai báo nằm trên một dòng riêng. Dòng có ký tự # đứng đầu dòng là dòng ghi chú. Các lựa chọn khai báo trong tập tin này có thể bao gồm

- **MAIL_DIR /var/spool/mail** Thư mục chứa hộp thư của người dùng. Lựa chọn này bắt buộc phải có.
- **PASS_MAX_DAYS 99999** Số ngày tối đa một mật mã có thể sử dụng.
- **PASS_MIN_DAYS 0** Số ngày tối thiểu cho phép giữa hai lần thay đổi mât mã.
- **PASS_MIN_LEN 5** Chiều dài tối thiểu của mật mã.

- **PASS_WARN_AGE 7** Số ngày sẽ xuất hiện thông báo trước khi một mật mã hết hạn sử dụng.
- **UID_MIN 500** Số giá trị tối thiểu của userID được sinh ra khi tạo tài khỏan mới.
- **UID_MAX 60000** Số giá trị tối đa của userID được sinh ra khi tạo tài khỏan.
- **GID_MIN 500** Số giá trị tối thiểu của groupID được sinh ra khi tạo group mới.

- **GID_MAX 60000** Giá trị tối đa của GroupID được phát sinh tự động khi khai báo tài khỏan nhóm mới.
- **USERDEL_CMD /usr/sbin/userdel_local**
  Nếu được định nghĩa, lệnh này sẽ được thi hành khi xóa bỏ một tài khỏan người dùng. Nó sẽ loại bỏ tất cả các công việc in ấn, cron...đang thi hành của tài khỏan bị xóa bỏ.
- **CREATE_HOME yes** nếu lựa chọn này có giá trị là **yes** thì mỗi khi tạo ra tài khỏan mới, thư mục chủ của tài khỏan người dùng đó

3. Các lệnh quản trị nhóm

3.1. Tạo tài khoản nhóm- groupadd

3.1.1. Cú pháp

groupadd [option] group_name

3.1.2. Lựa chọn

- Trong đó ***group_name*** là tên nhóm muốn tạo. Trên một máy tính tên nhóm phải là duy nhất. Các lựa chọn sau
- **-g gid [-o]:** Xác định mã nhận diện groupID. Giá trị này phải là duy nhất (Trừ trường hợp với lựa chọn **-o**). Giá trị này phải là một số nguyên dương. Giá trị mặc định của số nhỏ nhất lớn hơn 500 và lớn hơn mọi GID của nhóm khác hiện có.

3.2. Xóa tài khoản nhóm-groupdel

- Lệnh **groupdel** cho phép xóa các tài khoản nhóm cùng tất cả các mục từ tham chiếu tới tài khoản nhóm bị xóa đó.
- **Cú pháp**

  groupdel group_name

  trong đó group_name là tên tài khoản nhóm muốn xóa.

Chú ý:

- Không thể xóa được các tài khoản nhóm còn có chứa các tài khoản người dùng.
- Danh sách các group chứa trong file **/etc/group**

3.3. Thay đổi thông tin tài khỏan nhóm-groupmod

3.3.1. Cú pháp

groupmod [option] group_name

trong đó group_name là tên tài khỏan nhóm cần thay đổi thông tin

3.3.2. Option

- **-g gid [-o]** Xác định mã nhận diện tài khỏan nhóm (GID). Giá trị này phải duy nhất (trừ trường hợp sử dụng với lựa chọn **-o**), giá trị này phải là một số dương.

- **-n *other_name***: Thay đổi tên nhóm từ group_name thành *other_name*; tên nhóm phải duy nhất trên hệ thống.

3.4. Xem thông tin nhận diện tài khỏan-id

- Lệnh **id** cho biết thông tin nhận diện tài khỏan người dùng bao gồm UID và GID thật (real) và một hay nhiều GID thực tế (effective).
- Một tài khỏan người dùng luôn có một UID và một GID tương ứng (GID này chính là mã nhận diện tài khỏan nhóm khởi nạp của người dùng)

- Một tài khỏan người dùng có thể có nhiều GID thực tế. Các GID thực tế là mã nhận diện các tài khỏan nhóm mà tài khỏan người dùng là thành viên của chúng.

3.4.1. Cú pháp

id [option]username

Trong đó username là tên tài khỏan người dùng muốn xem thông tin. Trường hợp không chỉ ra username lệnh **id** sẽ cho biết thông tin về tài khỏan người dùng hiện hành.

- Khi thi hành lệnh id mà không chỉ ra bất kỳ một lựa chọn nào, lệnh id sẽ hiển thị tất cả các UID và GID có liên quan đến tài khỏan muốn xem thông tin.

3.4.2. Option

- **-g**: Chỉ hiển thị GID thật của tài khỏan
- **-u**: Chỉ hiển thị UID thật của tài khỏan
- **-G**: Chỉ hiển thị danh sách tất cả các GID của các nhóm mà tài khỏan là thành viên.

3.5. Lệnh su

3.5.1. Để tạm thời trở thành người dùng khác, ta sử dụng lệnh su

3.5.2. Cú pháp

su [-] [username]

- Lệnh **su** khi thực hiện không có đối số cho phép ta chuyển sang người dùng root

- Khi thi hành lệnh **su**, hệ thống sẽ xuất hiện lời nhắc yêu cầu nhập mật mã của tài khỏan username, ngọai trừ khi ta đăng nhập với quyền root.
- Lệnh **su** chỉ thực hiện thay đổi tài khỏan hiện hành để có được quyền truy nhập của tài khỏan username. Phần lớn các biến môi trường sẽ giữ nguyên.
- Tuy nhiên nếu thi hành lệnh **su** với option **'-'** thì xem như ta đăng nhập vào hệ thống với tài khỏan username.

3.6. Thay đổi chủ nhân tập tin- chown

3.6.1. Cú pháp

chown [option] owner [:[group]] file

3.6.2.Các diễn giải

- Trong đó **owner** là tên tài khỏan người dùng sẽ là chủ nhân mới của tập tin, **group** là tên nhóm sẽ là nhóm chủ nhân mới của tập tin

- Nếu đối số của lệnh chown chỉ có **owner** thì chỉ có chủ nhân tập tin thay đổi, nhóm chủ nhân không thay đổi.
- Nếu sau tên **owner** có dấu **:** mà không có tên **group** thì **owner** sẽ là chủ nhân mới của tập tin và nhóm của tập tin sẽ thay đổi thành nhóm đăng nhập của **owner** đó.
- Nếu lệnh có đầy đủ cả **owner** và **group** cách nhau : thì chủ nhân và nhóm của tập tin đều thay đổi.
- Nếu chỉ có tên **group** đi sau dấu **:** thì chỉ có nhóm của tập tin thay đổi, trường hợp này tương tự như **chgrp**

3.6.3. Option

- **-R**: Thay đổi chủ nhân cho cả các thư mục con và các tập tin có trong đó
- **--dereference**: Thay đổi chủ nhân tập tin mà symbolic link chỉ đến, thay vì thay đổi chủ nhân của symbolic link.
- **-h**: Thay đổi chủ nhân của symbolic link mà không thay đổi chủ nhân của tập tin mà symbolic link chỉ đến.
- **-v**: Hiển thị các thông điệp hệ thốngkhi thực hiện chuỗi xử lý mỗi tập tin.

3.7. Thay đổi nhóm chủ nhân tập tin-chgrp

3.7.1. Cú pháp

chgrp [option] group file

Trong đó group là nhóm chủ nhân mới của tập tin và file là tập tin ta muốn thay đổi nhóm chủ nhân.

3.7.2. Các option

- **-R**: Thay đổi nhóm chủ nhân cho tất cả các thư mục con và các tập tin có trong đó

- **--dereference**: Thay đổi nhóm chủ nhân tập tin mà symbolic link chỉ đến, thay vì thay đổi nhóm chủ nhân của symbolic link.
- **-h**: Thay đổi nhóm chủ nhân của symbolic link và không thay đổi nhóm chủ nhân của tập tin mà symbolic link chỉ đến
- **-v**: Hiển thị các thông điệp hệ thống khi thực hiện xử lý mỗi tập tin.

3.8. Các tập tin có liên quan: /etc/passwd và /etc/shadow

- Khi một tài khoản người dùng được ấn định một mật mã, mật mã này sẽ được mã hóa bằng một giá trị được phát sinh một cách ngẫu nhiên gọi là salt. Giá trị salt sau đó sẽ được lưu cùng với mật mã đã được mã hóa
- Khi người dùng đăng nhập hệ thống và cung cấp một mật mã, mật mã vừa nhập vào sẽ được mã hóa bằng giá trị salt, giá trị salt này được lấy ra từ mật mã đã được mã hóa của tài khoản đã lưu trữ trước đó. Hệ thống thực hiện so sánh kết quả thu được với mật mã đã được mã hóa của tài khoản. Nếu chúng giống nhau thì người dùng được xác thực

- Thông tin người dùng bao gồm cả mật mã được lưu trữ trong tập tin **/etc/passwd**. Mật mã được lưu trữ trong một dạng định dạng đã được mã hóa.
- Tập tin **/etc/passwd** chứa thông tin UID và GID, những thông tin này được sử dụng bởi chương trình hệ thống. Do vậy tập tin **/etc/passwd** phải để trong tình trạng cho các chương trình và ứng dụng đều có khả năng đọc được. Do đó không an tòan.

- Để giải quyến vấn đề này, Linux có chứa thêm gói ***shadow suite***. Shadow suite chuyển các mật mã đã được mã hóa vào tập tin /etc/shadow. Tập tin **/etc/shadow** là tập tin chỉ cho phép root truy nhập.
- Một mục từ trong **/etc/passwd** có định dạng sau

username: passwd: UID:GID:full_name:directory:shell

- Một mục từ trong tập tin **/etc/shadow** có định dạng

username:passwd:last:min:max:warn:inact:expire:reserved

- **Trong đó**
  - **usename**: tên tài khỏan
  - **passwd**: Mật mã đã được mã hóa
  - **last**: Thời điểm tính từ 1/1/70 mật mã đã thay đổi lần cuối
  - **min**: Số ngày tối thiểu trước khi mật mã bị đổi
  - **max**:Số ngày tố đa sử dụng mật mã
  - **warn**: Số ngày báo trước khi mật mã hết hạn
  - **inact**: Số ngày sau khi hết hạn sử dụng tài khỏan sẽ bị vô hiệu
  - **expire**: Ngày tài khỏan vô hiệu tính từ 1/1/70
  - **reserved**: trường dự phòng

- Tài khỏan bị khóa có dấu **!** Trước mật mã
- Tài khỏan có **!!** Trước mật mã là tài khỏan không có mật mã và không đăng nhập hệ thống được.
- Tài khỏan có * ở trường passwd sẽ không được đăng nhập hệ thống

3.9.Lệnh gpasswd

3.9.1. Thêm một user vào một group

3.9.2. Cú pháp

gpasswd [option] username groupname

3.9.3. Option

- **-a:** Thêm user vào group
- **-d:** Xóa user ra khỏi group