BÀI THỰC HÀNH SỐ 1

Quản lý và phân quyền tài khoản người dùng trên hệ điều hành Linux

Mục đích:

Công việc quản lý các tài khoản và phân quyền truy cập có ý nghĩa quan trọng trên các hệ thống máy tính có nhiều đối tượng dùng chung, đặc biệt là các máy chủ cung cấp dịch vụ. Nội dung bài thực hành này giới thiệu các thao tác quản lý tài khoản và phân quyền truy cập cho các tài khoản này trên hệ điều hành Linux CentOS 6.4.

Môi trường thực hành:

- Hệ điều hành: Linux CentOS 6.4
- Trình duyệt Web: Mozilla Firefox

I. Hướng dẫn chung

1. Quản lý tài khoản người dùng trên hệ điều hành CentOS 6.4

1.1. Quản lý tài khoản người dùng

Hệ điều hành CentOS 6.4 cung cấp một số lệnh để thực hiện quản lý tài khoản người dùng như sau:

- Thêm một tài khoản mới:

useradd *new_account_name*

Ví dụ lệnh sau tạo tài khoản có tên là là **test**

useradd *test*

- Thiết lập mật khẩu cho tài khoản:

passwd *account_name*

Ví dụ lệnh sau đặt mật khẩu cho tài khoản **test**:

passwd *test*

Sau đó nhập mật khẩu mà ta muốn đặt cho tài khoản.

- Thêm nhóm người dùng mới:

groupadd *new_group_name*

Ví dụ lệnh sau tạo nhóm có tên là là **student**

groupadd *student*

- Thêm tài khoản vào một nhóm:

usermod -aG *group_name account_name*

Ví dụ lệnh sau thêm người dùng **test** vào nhóm **student**

usermod -aG *student test*

- Liệt kê tất cả các nhóm người dùng:

getent group

- Xem danh sách người dùng trong một nhóm:

getent group *group_name*

Ví dụ lệnh sau xem danh sách người dùng trong nhóm student:

getent group *student*

- Xóa tài khoản người dùng:

userdel *account_name*

Để xóa cả dữ liệu của tài khoản đó, thay lệnh trên bằng **userdel -r *account_name***

Ví dụ lệnh sau thực hiện xóa tài khoản **test**

userdel *test*

hoặc để xóa cả dữ liệu trong thư mục người dùng: **userdel -r *test***

- Xóa nhóm người dùng

groupdel *group_name*

Ví dụ lệnh sau xóa nhóm có tên là **student:**

groupdel *student*

1.2. Thay đổi mật khẩu tài khoản đang sử dụng

- Bước 1: Đăng nhập với tài khoản cần thay đổi mật khẩu

- Bước 2: Mở cửa sổ Terminal và thực hiện lệnh **passwd**

Điền mật khẩu đang sử dụng và mật khẩu mới.

2. Phân quyền trong hệ điều hành họ Unix/Linux

2.1. Giới thiệu chung

Các hệ điều hành họ Unix/Linux cài đặt ma trận điều khiển truy cập theo danh sách ACL. Trên mỗi tài nguyên của hệ thống, có 3 dạng tài khoản được phân quyền:

- Owner: tài khoản sở hữu
- Group: nhóm sở hữu
- Others: các tài khoản khác (không phải là tài khoản sở hữu và không nằm trong nhóm sở hữu)

Trên mỗi tài nguyên, người dùng có 3 quyền truy cập là Đọc (r), Ghi (w) và Thực thi(x). Trong thông tin phân quyền của một tài nguyên, mỗi quyền này thể hiện bởi 1 bit với giá trị 0 nếu không có quyền và 1 nếu có quyền. Như vậy thông tin phân quyền trên file, thư mục có 10 bit:

- Bit 1: File(hiển thị **–**) hay thư mục(hiển thị **d**).
- Bit 2, 3, 4: Quyền truy cập cho tài khoản sở hữu
- Bit 5, 6, 7: Quyền truy cập cho nhóm sở hữu
- Bit 8, 9, 10: Quyền truy cập cho tài khoản khác

Ví dụ 1 110 100 000

Khi bỏ qua bit đầu tiên, thông tin phân quyền này có hai cách biểu diễn:

- Chuỗi số: mỗi số là giá trị thập phân của 3 bít phân quyền tương ứng với mỗi loại người dùng. Ví dụ chuỗi 754 cho biết thông tin phân quyền như sau:
  - Owner: Đọc, Ghi, Thực thi($7 = 111_{(2)}$)
  - Group: Đọc, Thực thi ($5 = 101_{(2)}$)
  - Others: Đọc ($4 = 100_{(2)}$)
- Chuỗi ký tự: mỗi ký tự là từ viết tắt cho quyền được cấp hoặc ký tự **–** nếu quyền đó không được cấp. Như vậy thông tin phân quyền cho mỗi loại người dùng gồm có 3 ký tự. Ví dụ với chuỗi số 754 thì chuỗi ký tự tương ứng là rwxr-xr--

  Biểu diễn đầy đủ: 10 ký tự:

  - Ký tự đầu tiên: File (‘-‘), thư mục (‘d’)
  - 9 ký tự tiếp theo: Biểu diễn quyền truy cập

Các lệnh cơ bản được sử dụng để phân quyền trong Unix/Linux bao gồm:

- Lệnh thay đổi sở hữu:

  chown -R *Tên_người_dùng:Tên_nhóm Đường_dẫn_file_hoặc_thư_mục*

  Trong đó tùy chọn –R được sử dụng nếu muốn lệnh này tác động tới tất cả các file và thư mục con cháu trong thư mục đó. Ví dụ, lệnh để đổi sở hữu toàn bộ thư mục /var/test tới người dùng test và nhóm student như sau:

  chown -R test:student /var/test

- Lệnh phân quyền:

  chmod -R *Chuỗi_số_phân_quyền Đường_dẫn_file_hoặc_thư_mục*

Trong đó tùy chọn –R được sử dụng nếu muốn lệnh này tác động tới tất cả các file và thư mục con cháu trong thư mục đó. Ví dụ, lệnh để đổi phân quyền toàn bộ thư mục /var/test thành 754 như sau:

chmod -R 754 /var/test

- Lệnh xem thông tin phân quyền: **ls –la Đường_dẫn_thư mục**

  Lệnh này hiển thị thông tin phân quyền của tất cả các file và thư mục có trong thư mục đó. Ví dụ dưới đây cho biết kết quả thực hiện lệnh này:

```
[root@localhost /]# ls -la /var/local
total 16
drwxr-xr-x.  4 root root 4096 Aug  6 05:34 .
drwxr-xr-x. 22 root root 4096 Dec  8  2016 ..
drwxr-xr-x.  2 root root 4096 Aug  6 05:31 Test
```

Trong đó:

total: số block trên ổ đĩa để lưu trữ thư mục
Hai dòng đầu tiên: thông tin của thư mục được đề cập(.) và thư mục cha(..)
Các dòng tiếp theo: thông tin của file và thư mục con
Cấu trúc mỗi dòng thông tin gồm có:
Phân quyền Số liên kết Tài khoản sở hữu Nhóm sở hữu Kích thước Thời gian tạo Tên file/thư mục
Trong ví dụ trên, Test là thư mục (ký tự đầu tiên trong thông tin phân quyền là d) với quyền cho các loại người dùng là rwxr-xr-x hay dưới dạng số là 755.

2.2. Thay đổi mặt nạ umask

Giá trị mặt nạ umask được sử dụng để thiết lập chính sách phân quyền mặc định cho file và thư mục được tạo ra. Chuỗi số thể hiện phân quyền mặc định như sau:

- Phân quyền trên file: 666 – umask

- Phân quyền trên thư mục: 777 – umask

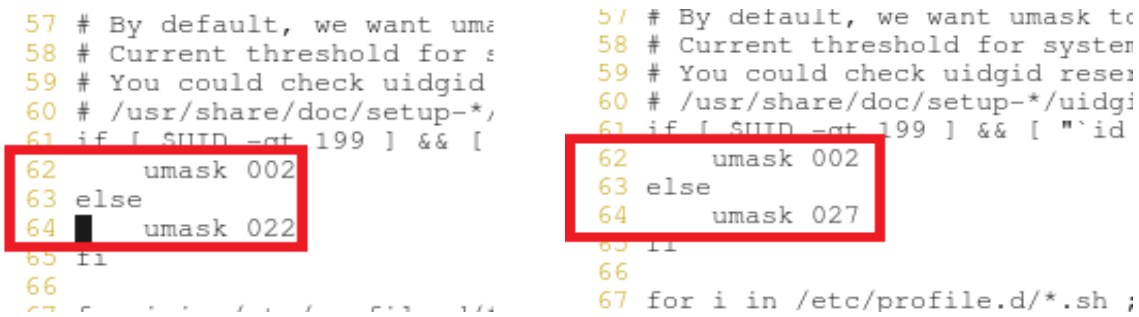
Để nâng cao độ an toàn bảo mật cho hệ thống file, chúng ta cần thay đổi giá trị UMASK là 027.

Cách 1: Sửa trong file hệ thống /etc/profile

- **Bước 1:** Mở cửa sổ Terminal

- **Bước 2:** Thực hiện lệnh sudo gedit /etc/profile. Điền mật khẩu tài khoản đang sử dụng nếu được yêu cầu.

- **Bước 3:** Sửa giá trị umask ở dòng 62 từ 022 thành 027



- **Bước 4:** Lưu file và đóng cửa sổ chương trình soạn thảo.

Cách 2: Sử dụng lệnh umask

Thực hiện lệnh sau trên cửa sổ dòng lệnh

umask 0027

II. Nội dung thực hành

Khởi động máy ảo CentOS và đăng nhập tài khoản root với mật khẩu 123456

1. Thay đổi giá trị mặt nạ umask

Thực hiện thay đổi giá trị mặt nạ umask theo hướng dẫn ở phần I.

2. Quản lý tài khoản người dùng

Câu hỏi 1: Tạo 2 nhóm có tên là customer và staff

Câu hỏi 2: Tạo 3 tài khoản người dùng mới là alice, bob và charlie. Đặt mật khẩu tùy ý cho các tài khoản này.

Câu hỏi 3: Thêm tài khoản alice và charlie vào nhóm staff. Thêm tài khoản bob vào nhóm customer.

3. Phân quyền tài khoản

- **Bước 1:** Mở cửa sổ Terminal và thực hiện lệnh **cd /** để chuyển thư mục làm việc vào thư mục gốc.
- **Bước 2:** Mở cửa sổ Terminal và thực hiện lệnh sau để tạo thư mục /data

  mkdir data

- **Bước 3:** Thực hiện lệnh **ls -l | grep data** để xem phân quyền trên thư mục vừa tạo

```
[root@localhost /]# ls -l | grep data
drwxr-x---.   2 root root    6 Aug 13 00:41 data
```

Từ kết quả hiển thị ta có thể thấy thư mục này của tài khoản **root** và nhóm root. Có thể thấy giá trị phân quyền trên thư mục là 750 = 777 – 027, trong đó 027 là giá trị umask mà chúng ta vừa thiết lập ở trên.

- **Bước 4:** Tạo thư mục con **backup** trong thư mục data bằng lệnh sau:

  mkdir /data/backup

- **Bước 5:** Tạo các file **allow.txt** và **restrict.txt** bằng các lệnh sau:

  touch /data/allow.txt

  touch /data/restrict.txt

- **Bước 6:** Thực hiện lệnh **ls -l /data** để xem thông tin phân quyền trên các file và thư mục trong thư mục **/data**

```
[root@localhost data]# ls -l /data
total 0
-rw-r-----. 1 root root 0 Aug 13 01:11 allow.txt
drwxr-x---. 2 root root 6 Aug 13 01:12 backup
-rw-r-----. 1 root root 0 Aug 13 01:11 restrict.txt
```

Câu hỏi 4: Các file và thư mục ở trên thuộc sở hữu của tài khoản nào?

Câu hỏi 5: Tài khoản root có quyền gì trên các file và thư mục?

Câu hỏi 6: Các tài khoản alice, bob và charlie có quyền gì trên các file và thư mục?

Câu hỏi 7: Thực hiện lệnh thay đổi quyền sở hữu toàn bộ thư mục **/data** cho người dùng **alice** và nhóm **staff**

Câu hỏi 8. Xem lại thông tin phân quyền trên thư mục /data và các file bên trong bằng lệnh:

ls -l /data

Tài khoản alice có các quyền gì trên các file và thư mục trong thư mục data.

Câu hỏi 9. Tài khoản bob có quyền gì trên các file và thư mục trong thư mục data.

Câu hỏi 10. Tài khoản charlie có quyền gì trên các file và thư mục trong thư mục data.

Câu hỏi 11. Đăng nhập bằng tài khoản bob và kiểm tra tài khoản này có thể thực hiện được những thao tác nào trên thư mục /data?

- Truy cập vào thư mục /data
- Đọc file allow.txt và restrict.txt bằng lệnh **gedit allow.txt** và **gedit restrict.txt**
- Thay đổi nội dung của file allow.txt và restrict.txt
- Xóa file allow.txt
- Truy cập thư mục /data/backup
- Tạo thư mục mới với tên nào đó
- Tạo file mới với tên nào đó

Câu hỏi 12. Đăng nhập bằng tài khoản charlie và kiểm tra tài khoản này có thể thực hiện được những thao tác nào?

- Truy cập vào thư mục /data
- Đọc file allow.txt và restrict.txt bằng lệnh **gedit allow.txt** và **gedit restrict.txt**
- Thay đổi nội dung của file allow.txt và restrict.txt
- Xóa file allow.txt
- Truy cập thư mục /data/backup
- Tạo thư mục mới với tên nào đó
- Tạo file mới với tên nào đó

Câu hỏi 13. Đăng nhập bằng tài khoản alice và kiểm tra tài khoản này có thể thực hiện được những thao tác nào?

- Truy cập vào thư mục /data
- Đọc file allow.txt và restrict.txt bằng lệnh **gedit allow.txt** và **gedit restrict.txt**
- Thay đổi nội dung của file allow.txt và restrict.txt
- Xóa file allow.txt
- Truy cập thư mục /data/backup
- Tạo thư mục mới với tên nào đó
- Tạo file mới với tên nào đó

Câu hỏi 14. Thực hiện các lệnh để cấp quyền truy cập sau cho bob mà không làm thay đổi quyền truy cập của alice và charlie trên thư mục này:

- Truy cập thư mục /data
- Đọc file allow.txt