**LAB 8: QUẢN LÝ USER, GROUP VÀ PHÂN QUYỀN TRONG WINDOWS/LINUX**

**Thời lượng: 3 tiết**

**Nội dung:**

* User và Group
* Tập lệnh quản lý User và Group
* Những file liên quan đến User và Group
* Quyền hạn và các lệnh liên quan đến quyền hạn

**WINDOWS**

1. Phân quyền trong NTFS file system

* Đọc ownership của một file/folder ?
* Khái niệm về permissions trên file/folder trong Windows ?

**Hướng dẫn:** *Tham khảo* ***Help and Support*** *, key “permission”*

* Xem thông tin về permissions của một user account/group trên một file/folder ?
* Thiết lập permissions trên một folder và một file (owner là administrator) sao cho tài khoản sinhvien :
  + Được phép đọc /ghi
  + Chỉ được phép đọc
  + Chỉ được phép ghi
  + Full control
* Thực hiện kiểm tra với mỗi thiết lập trên

**Hướng dẫn**: *Tham khảo* [*http://www.ntfs.com/ntfs-permissions.htm*](http://www.ntfs.com/ntfs-permissions.htm)

1. Thiết lập permissions trên một folder/file :

* Chia sẻ folder cho tất cả user trên 1 hệ thống
* Quyền Read với group abc
* Quyền Write với group def
* Quyền Read & execute với group administrators

**LINUX**

1. **User**

* User là người có thể truy cập đến hệ thống.
* User có **username** và **password**.
* Có hai loại user: **super user** và **regular user**.
* Mỗi user còn có một định danh riêng gọi là **UID**.
* Định danh của người dùng bình thường sử dụng giá trị bắt đầu từ 500.

1. **Group**

* Group là **tập hợp nhiều user** lại.
* Mỗi user luôn là thành viên của một group.
* Khi **tạo một user thì mặc định một group được tạo ra** .
* Mỗi group còn có một định danh riêng gọi là **GID**.
* Định danh của group thường sử dụng giá trị bắt đầu từ 500.

1. **Tập lệnh quản lý User và Group**

|  |  |
| --- | --- |
| Tạo User: | **Cú pháp:** #useradd [option] <username>  -c “Thông tin người dùng”  -d <Thư mục cá nhân>  -m : Tạo thư mục cá nhân nếu chưa tồn tại  -g <nhóm của người dùng>  **Ví dụ:** #**useradd** –c “Nguyen Van A – Server Admin” –g serveradmin vana |
| Thay đổi thông tin cá nhân: | **Cú pháp:** #**usermod** [option] <username>  Những option tương tự **Useradd**  **Ví dụ:** #usermod –g kinhdoanh vana *//chuyển vana từ nhóm server admin sang nhóm kinh doanh.* |
| Xóa người dùng | **Cúpháp** : #**userdel** [option] <username>  **Vídụ :** #userdel –r vana |
| Khóa/Mở khóa người dùng | **passwd –l / passwd –u**  **usermod –L** / **usermod –U**  Trong /etc/shadow có thể khóa tài khoản bằng cách thay từ khóa x bằng từ khóa \*. |
| Tạo nhóm: | **Cú pháp:** #**groupadd** <groupname>  **Ví dụ:** #groupadd serveradmin |
| Xóa nhóm | **Cú pháp:** #**groupdel** <groupname>  **Ví dụ:** #groupdel <serveradmin>  2/4 |
| Xem thông tin về User và Group | **Cú pháp:** #**id** <option> <username>  **Ví dụ:** #id -g vana //xem GroupID của user vana  **Cú pháp:** #**groups** <username>  **Ví dụ:** #groups vana //xem tên nhóm của user vana |

1. **Những file liên quan đến User và Group**

***#/etc/passwd***

Mỗi dòng trong tập tin gồm có 7 trường, được phân cách bởi dấu hai chấm.

***#/etc/group***

Mỗi dòng trong tập tin gồm có 4 trường, được phân cách bởi dấu hai chấm.

***#/etc/shadow***

Lưu mật khẩu đã được mã hóa và chỉ có user root mới được quyền đọc.

1. **Quyền hạn**

Trong Linux có 3 dạng đối tượng :

* Owner (người sở hữu).
* Group owner (nhóm sở hữu).
* Other users (những người khác).

Các quyền hạn :

* Read / r / 4 : cho phép đọc nội dung.
* Write / w / 2 : dùng để tạo, thay đổi hay xóa.
* Execute / x / 1 : thực thi chương trình.

rwx rw- --- khoa.txt

Vídụ : Với lệnh ls –l ta thấy :

[root@task ~]# ls -l

total 32

-rw-------. 1 root root 1416 Jan 10 14:06 anaconda-ks.cfg

-rw-r--r--. 1 root root 15522 Jan 10 14:06 install.log

-rw-r--r--. 1 root root 5337 Jan 10 14:06

install.log.syslog

drwxr-xr-x 6 root root 4096 Feb 9 10:02 softs

Ngoài ra, chúng ta có thể dùng số.

* Vídụ : quyền r, w, x : 4+2+1 = 7
* *Tổ hợp 3 quyền trên có giá trị từ 0 đến 7.*
* 3/4

1. **Các lệnh liên quan đến quyền hạn**

* **Lệnh *Chmod:*** dùng để cấp quyền hạn.

Cú pháp : #**chmod**

*Ví dụ:* #**chmod** 644 baitap.txt *//cấp quyền cho owner có thể ghi các nhóm các chỉ có quyền đọc với file taptin.txt*

* ***Lệnh Chown:*** dùng thay đổi người sở hữu***.***

Cú pháp : #**chown**

* ***Lệnh Chgrp:*** dùng thay đổi nhóm sở hữu***.***

Cú pháp : #**chgrp**

**BÀI TẬP ĐỀ NGHỊ**

Phân quyền trên hệ thống tập tin

1. Tạo thư mục tmp dưới thư mục UX và cho nó quyền truy nhập rwx r-x ---
2. Tạo một tệp rỗng có tên workday dưới tmp (bằng lệnh touch). Cho nó quyền truy nhập rw-r----- và thử đọc nội dung của nó.
3. Bỏ quyền đọc (r) của user và thử đọc lại wordday
4. Bỏ quyền ghi (w) của user của thư mục tmp và thử xoá tệp wordday
5. Bỏ quyền đọc (r) của user của thư mục tmp và thử hiển thị nội dung của nó
6. Bỏ quyền chạy (x) của user của thư mục tmp và thử đi vào thư mục này
7. Trả lại quyền rwx cho user của thư mục tmp
8. Thử cho bạn quyền ghi (w) vào thư mục chủ của một thành viên của nhóm của bạn
9. Xoá nội dung và bản thân thư mục tmp

1. Tạo 2 user **tenSV1** và **tenSV2** (vd: anhminh1, anhminh2)…

2. Tạo thư mục tmp dưới thư mục UX và cho nó quyền truy nhập rwx r-x ---

3. Tạo một tệp có tên workday (nội dung: tên, mssv) dưới tmp (bằng lệnh touch). Cho nó quyền truy nhập rw-r----- (640) và thử đọc nội dung của nó

4. Bỏ quyền đọc (r) của user và thử đọc lại workday

5. Bỏ quyền ghi (w) của user của thư mục tmp và thử xoá tệp workday

6. Bỏ quyền đọc (r) của user của thư mục tmp và thử hiển thị nội dung của nó

7. Bỏ quyền chạy (x) của user của thư mục tmp và thử đi vào thư mục này

8. Trả lại quyền rwx cho user của thư mục tmp

9. Login bằng tkhoa tenSV2, xem nội dung tệp workday

10. Thực hiện lệnh gán quyền để tenSV2 có thể xem được nội dung của tệp workday