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

**Thời lượng: 3 tiết**

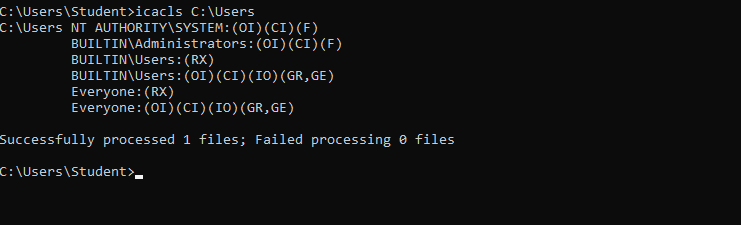
**Nội dung:**

* 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”*

*Các permission trên file/folder trong Windows được xác định bởi các quyền sau đây:*

*Read (Đọc): cho phép người dùng xem nội dung của tệp tin hoặc thư mục.*

*Write (Viết): cho phép người dùng chỉnh sửa nội dung của tệp tin hoặc thư mục.*

*Execute (Thực thi): cho phép người dùng chạy một tệp tin hoặc thực hiện một chương trình.*

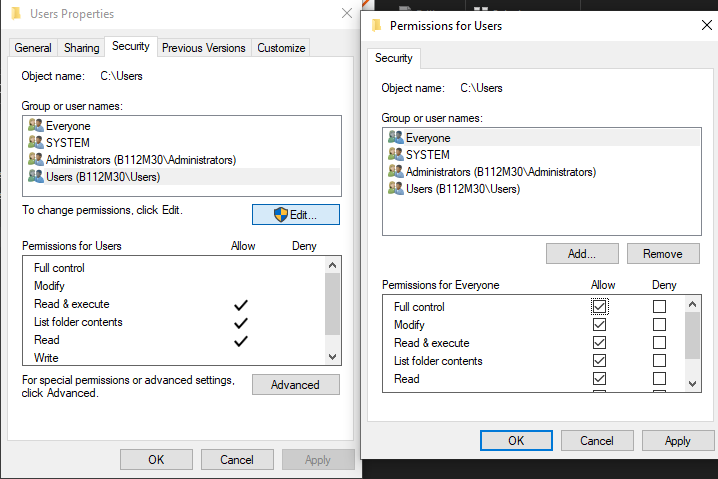
*Delete (Xóa): cho phép người dùng xóa một tệp tin hoặc thư mục.*

*Modify (Thay đổi): cho phép người dùng chỉnh sửa tệp tin hoặc thư mục, bao gồm cả việc thêm hoặc xóa các tệp con và thư mục con.*

*Full Control (Toàn quyền): cho phép người dùng thực hiện tất cả các hoạt động trên tệp tin hoặc thư mục, bao gồm cả việc thay đổi các quyền của tệp tin hoặc thư mục.*

*Những quyền này có thể được gán cho các người dùng cụ thể hoặc cho các nhóm người dùng. Các quyền này có thể được xác định và thay đổi bằng cách sử dụng tính năng Security của Windows. Việc quản lý quyền truy cập sẽ giúp bảo vệ tệp tin và thư mục của bạn khỏi sự truy cập trái phép hoặc sửa đổi từ người dùng không được ủy quyền.*

* 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 o Chỉ được phép đọc
  + Chỉ được phép ghi
  + Full control

*Để thiết lập quyền truy cập cho tài khoản sinhvien trên một thư mục và một file với chủ sở hữu là administrator trên hệ điều hành Windows, chúng ta có thể sử dụng giao diện đồ họa hoặc dòng lệnh.*

*Sử dụng giao diện đồ họa:*

*Chuột phải vào thư mục hoặc file cần thiết lập quyền truy cập.*

*Chọn "Properties" (Tính năng).*

*Chọn tab "Security" (Bảo mật).*

*Nhấp vào nút "Edit" (Sửa).*

*Tại đây, bạn có thể chọn tài khoản sinhvien và thiết lập các quyền truy cập tương ứng. Ví dụ:*

*Được phép đọc/ghi: chọn "Allow" (Cho phép) ở các mục "Read" (Đọc) và "Write" (Ghi).*

*Chỉ được phép đọc: chọn "Allow" ở mục "Read" và "Deny" (Từ chối) ở mục "Write".*

*Chỉ được phép ghi: chọn "Allow" ở mục "Write" và "Deny" ở mục "Read".*

*Full control: chọn "Allow" ở tất cả các mục.*

*Sử dụng dòng lệnh:*

*Mở Command Prompt hoặc PowerShell với quyền Administrator.*

*Sử dụng lệnh icacls để thiết lập quyền truy cập cho thư mục hoặc file. Ví dụ:*

*Được phép đọc/ghi: icacls folder /grant sinhvien:(M)*

*Chỉ được phép đọc: icacls folder /grant sinhvien:(R)*

*Chỉ được phép ghi: icacls folder /grant sinhvien:(W)*

*Full control: icacls folder /grant sinhvien:(F)*

*Ở đây, chúng ta sử dụng tùy chọn /grant để thiết lập quyền truy cập cho tài khoản sinhvien, và sử dụng các tham số (M) (Modify), (R) (Read), (W) (Write), và (F) (Full Control) để thiết lập các quyền tương ứng*

***Được phép đọc/ghi trên folder và file:***

* + *Chọn folder và file cần thiết lập permissions, click chuột phải và chọn Properties.*
  + *Chọn tab Security và click Edit.*
  + *Click Add và nhập tên tài khoản sinhvien vào ô Enter the object names to select.*
  + *Click OK và tại mục Group or user names, chọn tên tài khoản vừa thêm vào.*
  + *Tại mục Permissions for sinhvien, đánh dấu vào Full control, Read và Write.*
  + *Click OK để hoàn thành thiết lập permissions.*
  + *Chỉ được phép đọc trên folder và file:*
  + *Làm tương tự như trên đến bước 4.*
  + *Tại mục Permissions for sinhvien, chỉ đánh dấu vào Read.*
  + *Click OK để hoàn thành thiết lập permissions.*
  + *Chỉ được phép ghi trên folder và file:*
  + *Làm tương tự như trên đến bước 4.*
  + *Tại mục Permissions for sinhvien, chỉ đánh dấu vào Write.*
  + *Click OK để hoàn thành thiết lập permissions.*
  + *Để kiểm tra thiết lập permissions trên folder và file, bạn có thể đăng nhập vào tài khoản sinhvien và thực hiện các hành động đọc, ghi trên folder và file đó. Nếu tài khoản sinhvien được phép đọc và ghi, các hành động này sẽ thành công, ngược lại nếu tài khoản sinhvien chỉ được phép đọc hoặc chỉ được phép ghi thì các hành động đọc hoặc ghi sẽ bị từ chối và trả về thông báo lỗi.*
* *Thực hiện kiểm tra với mỗi thiết lập trên*

**Hướng dẫn**: *Tham khảo <http://www.ntfs.com/ntfs-permissions.htm>*

1. Thiết lập permissions trên một folder :

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

Để thiết lập các quyền truy cập trên một thư mục trên hệ thống của bạn, hãy làm theo các bước sau đây:

*Bước 1: Mở Windows Explorer và tìm thư mục cần thiết lập quyền truy cập.*

*Bước 2: Chuột phải vào thư mục và chọn Properties (Thuộc tính).*

*Bước 3: Chọn tab Sharing (Chia sẻ).*

*Bước 4: Nhấn nút Share (Chia sẻ), chọn "Everyone" trong mục "Type the name of the object to select" (Nhập tên đối tượng để chọn), và sau đó nhấn nút Add (Thêm).*

*Bước 5: Chọn level truy cập bằng cách chọn từ các tùy chọn Read (Đọc), Change (Thay đổi) hoặc Full Control (Toàn quyền).*

*Bước 6: Bấm vào nút Share để hoàn thành chia sẻ folder cho tất cả user trên hệ thống.*

*Bước 7: Quay lại tab Security (Bảo mật) và chọn Edit (Chỉnh sửa).*

*Bước 8: Chọn Add (Thêm) và nhập tên nhóm "abc". Chọn OK.*

*Bước 9: Chọn nhóm "abc" trong danh sách, sau đó chọn tất cả các ô trống phía dưới Quyền (Permission) ngoại trừ ô Đọc & thực thi (Read & execute) và Đọc (Read).*

*Bước 10: Nhấn nút Add (Thêm) và nhập tên nhóm "def". Chọn OK.*

*Bước 11: Chọn nhóm "def" trong danh sách, sau đó chọn các ô Đọc & thực thi (Read & execute) và Ghi (Write) để cho phép nhóm này đọc và ghi vào thư mục.*

*Bước 12: Nhấn nút Add (Thêm) và nhập tên nhóm "administrators". Chọn OK.*

*Bước 13: Chọn nhóm "administrators" trong danh sách, sau đó chọn tất cả các ô phía dưới Quyền (Permission) ngoại trừ ô Toàn quyền (Full Control).*

*Bước 14: Nhấn nút Apply (Áp dụng) và OK để lưu các thay đổi.*

*Bây giờ, các quyền truy cập trên thư mục đã được thiết lập cho các nhóm và người dùng tương ứng.*

**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  *#useradd –c “Nguyen Van A – Server Admin” –g serveradmin -d /home/vana -m 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.

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 NGH**

Phân quyền trên hệ thống tập tin

1. Tạo thư mục tmp dưới thư mục UX và cho nó quyền truy nhập rwxr-x---

* *mkdir -m 750 UX/tmp*

1. Tạo một tệp rỗng có tên wordday dưới tmp (bằng lệnh touch). Cho nó quyền truy nhập rw-r----- và thử đọc nội dung của nó.

* *mkdir -m 750 UX/tmp*
* *touch UX/tmp/wordday*
* *chmod 640 UX/tmp/wordday*
* *cat UX/tmp/wordday*

1. Bỏ quyền đọc (r) của user và thử đọc lại wordday

* *chmod u-r wordday*

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

* *chmod u-w tmp*

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

* *chmod u-r /tmp*
* *ls /tmp*

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

* *chmod u-x tmp/*

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

* *chmod u+rwx tmp/*
* *ls -l tmp/*

1. Thử cho bạn quyền ghi (w) vào thư mục chủ của một thành viên của nhóm của bạn

* *sudo chmod g+w /path/to/directory*

1. Xoá nội dung và bản thân thư mục tmp

* *sudo rm -r /tmpd*