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

Thời lượng: 3 tiết

(Tham khảo:

https://drive.google.com/file/d/10FWwdvgpg_VnaYjIY77dzet3W78OvUWV/view)

Nội dung:

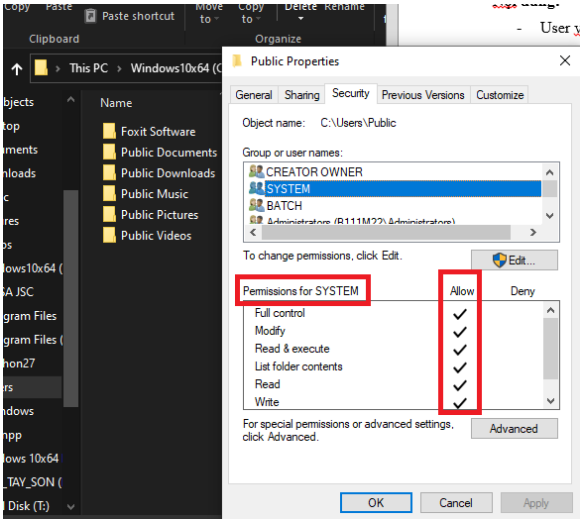
- User và Group
- Tập lệnh quản lý User và Group
- Những file liên quan đến User và Group
- Quyền hạn và các lệnh liên quan đến quyền hạn

WINDOWS

1. Phân quyền trong NTFS file system

- **Đọc ownership của một file/folder ?**

+ Trên hệ điều hành Windows, để xem quyền sở hữu của một tập tin hoặc thư mục, bạn có thể mở Windows Explorer, chuột phải vào tập tin hoặc thư mục đó, chọn "Properties" và chuyển đến tab "Security". Trên đó, bạn sẽ thấy danh sách các người dùng và nhóm được cấp quyền truy cập vào tập tin hoặc thư mục đó, và bạn có thể kiểm tra quyền của từng người dùng hoặc nhóm bằng cách nhấp chuột vào tên của họ.



- **Khái niệm về permissions trên file/folder trong Windows ?**

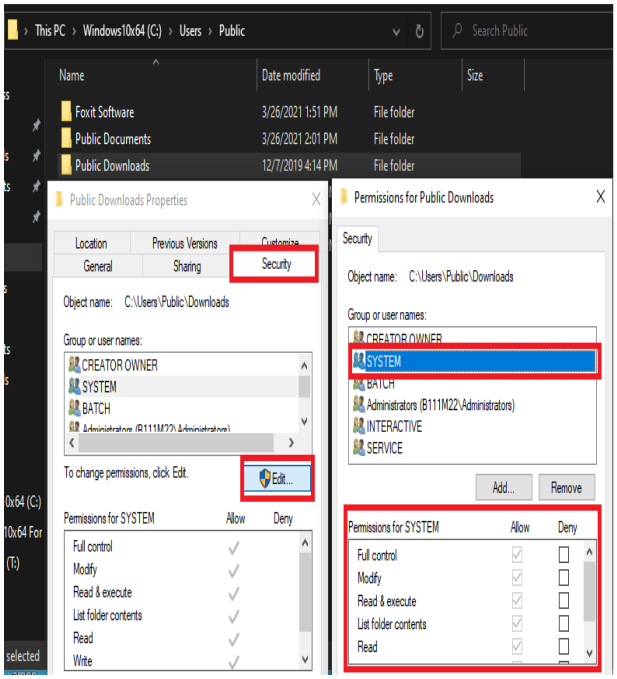
+ Trên Windows, quyền truy cập vào tập tin hoặc thư mục được xác định bởi permissions. Các quyền này được phân loại thành 3 nhóm chính: Read (đọc), Write (ghi) và Execute (thực thi). Mỗi nhóm này lại được chia thành các quyền chi tiết khác nhau, ví dụ như quyền đọc, quyền ghi, quyền thay đổi quyền truy cập, quyền chạy chương trình, v.v.

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

- **Xem thông tin về permissions của một user account/group trên một file/folder ?**

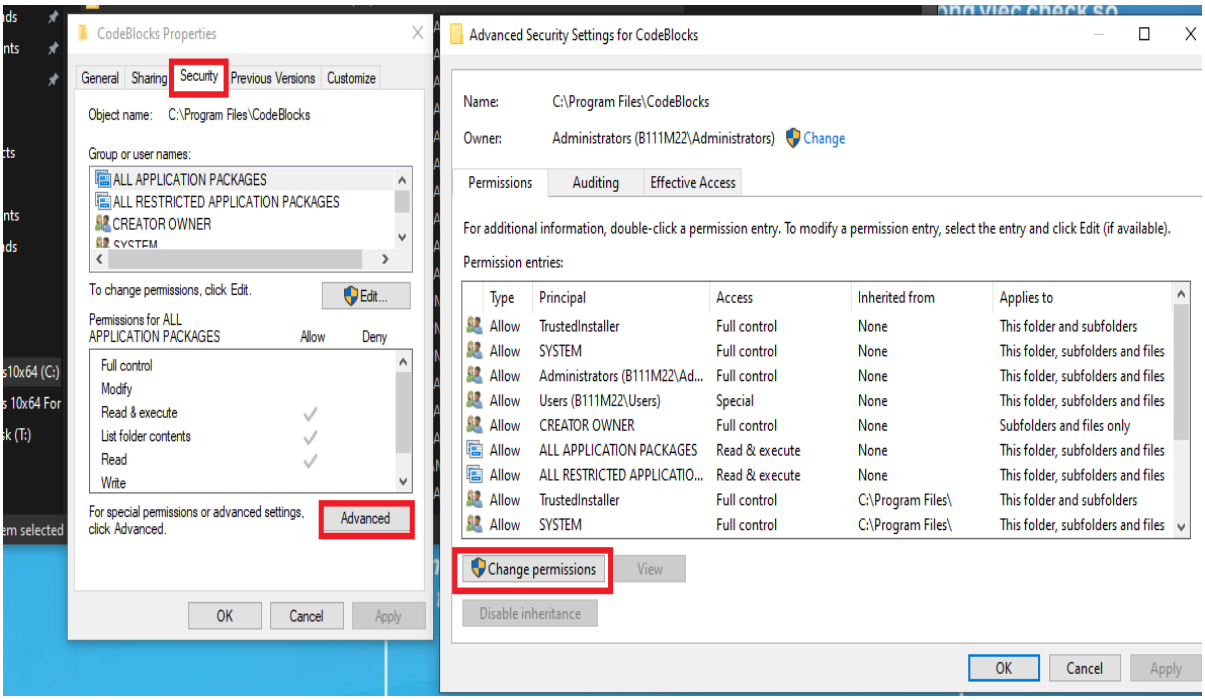
+ Để xem thông tin về quyền truy cập của một user account hoặc group trên một file hoặc thư mục cụ thể trên Windows, bạn có thể làm theo các bước sau:

1. Chuột phải vào file hoặc thư mục đó và chọn Properties.
2. Chuyển đến tab Security.
3. Ở đây, bạn sẽ thấy danh sách các user và group, và các quyền tương ứng của họ.
4. Nếu bạn muốn xem chi tiết hơn về các quyền đó, bạn có thể chọn một user hoặc group cụ thể và nhấp vào nút Edit. Tại đây, bạn có thể xem các quyền chi tiết được cấp cho user hoặc group đó trên file hoặc thư mục đó.

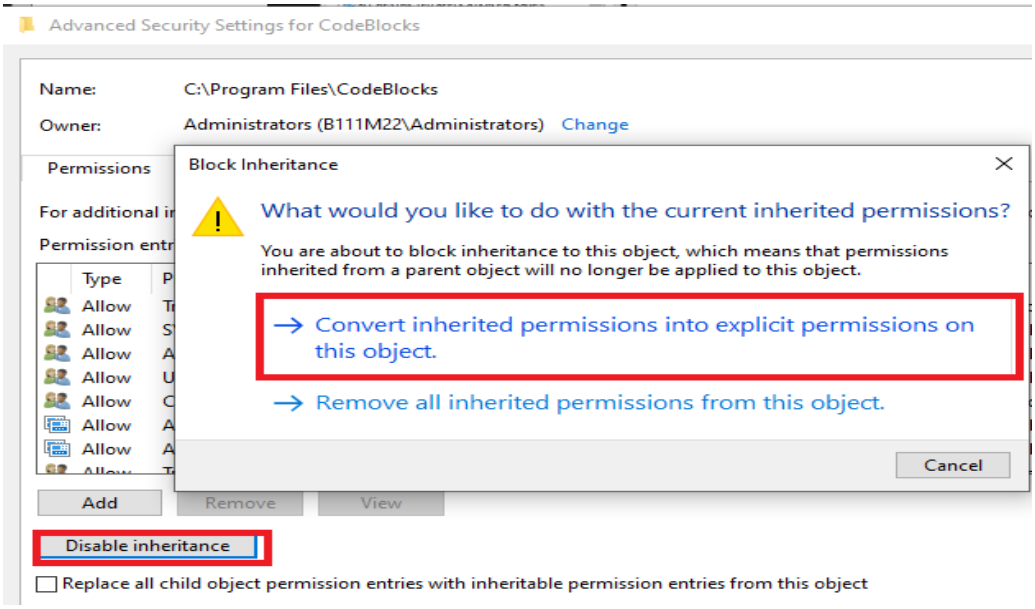


- **Thiết lập permissions trên một folder và một file (owner là administrator) sao cho tài khoản sinhvien :**

1.Nhấn Propertile chọn tab security rồi nhấn advanced rồi chọn Change permisions

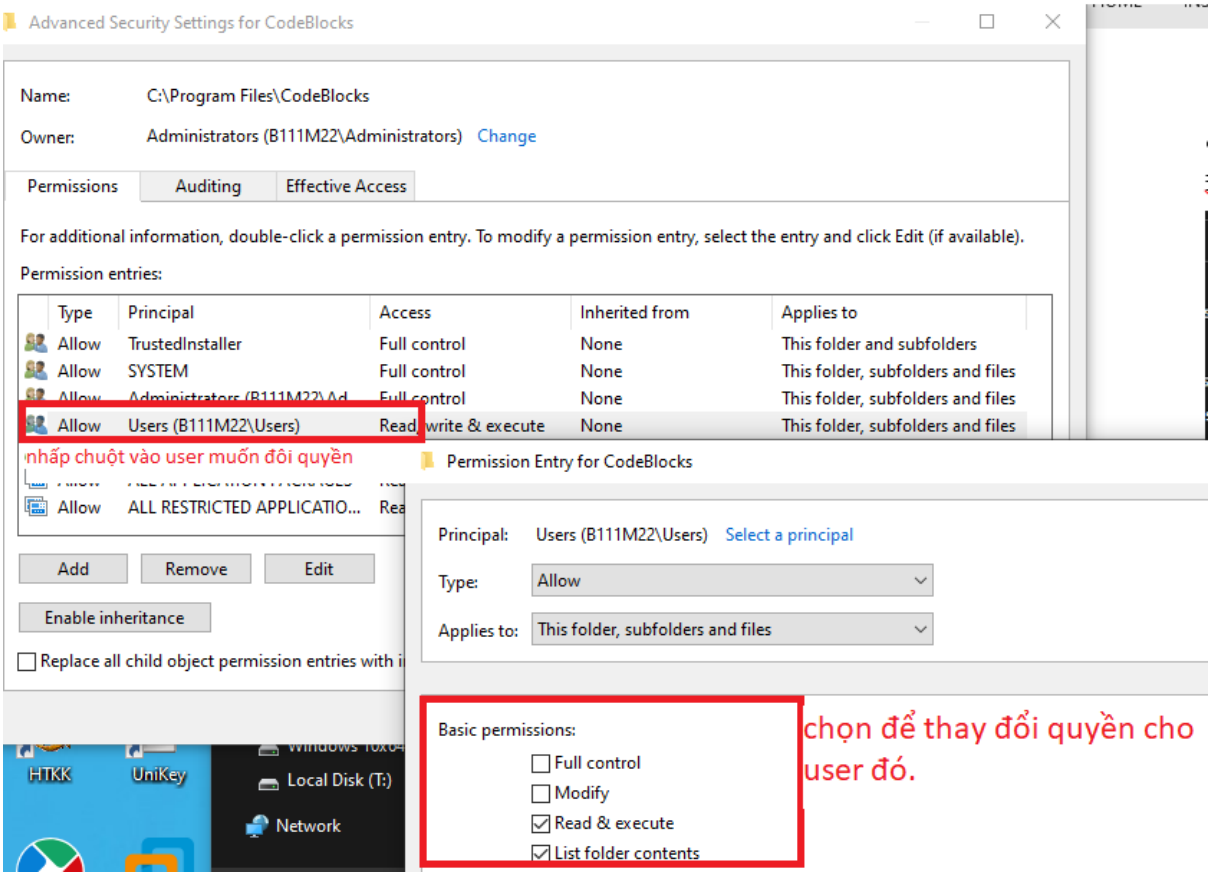


2.Nhấn Disable inheritance để dừng việc chia sẻ quyền hiện tại , rồi chọn Convert inhertited ….

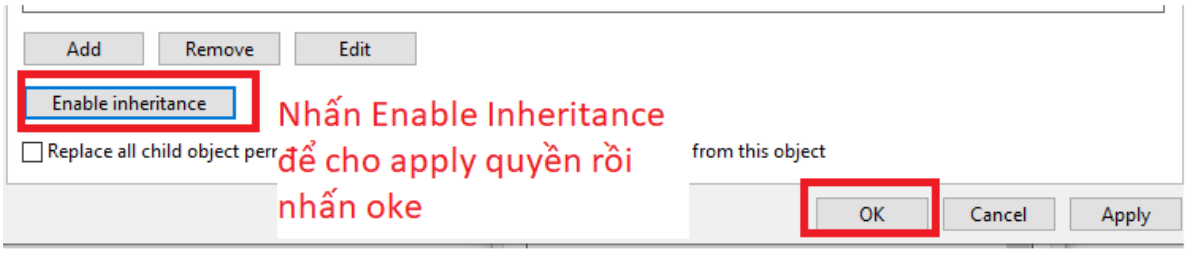


3.Nhấp chuột vào user muốn đổi quyền, ở đây ta chọn user sinhvien (student)

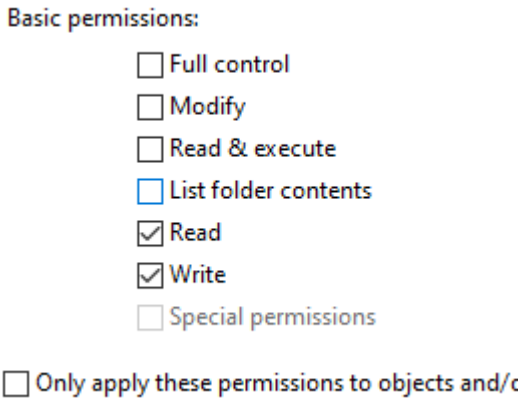
Sau đó chọn quyền muốn phân cho user rồi nhấn OK.



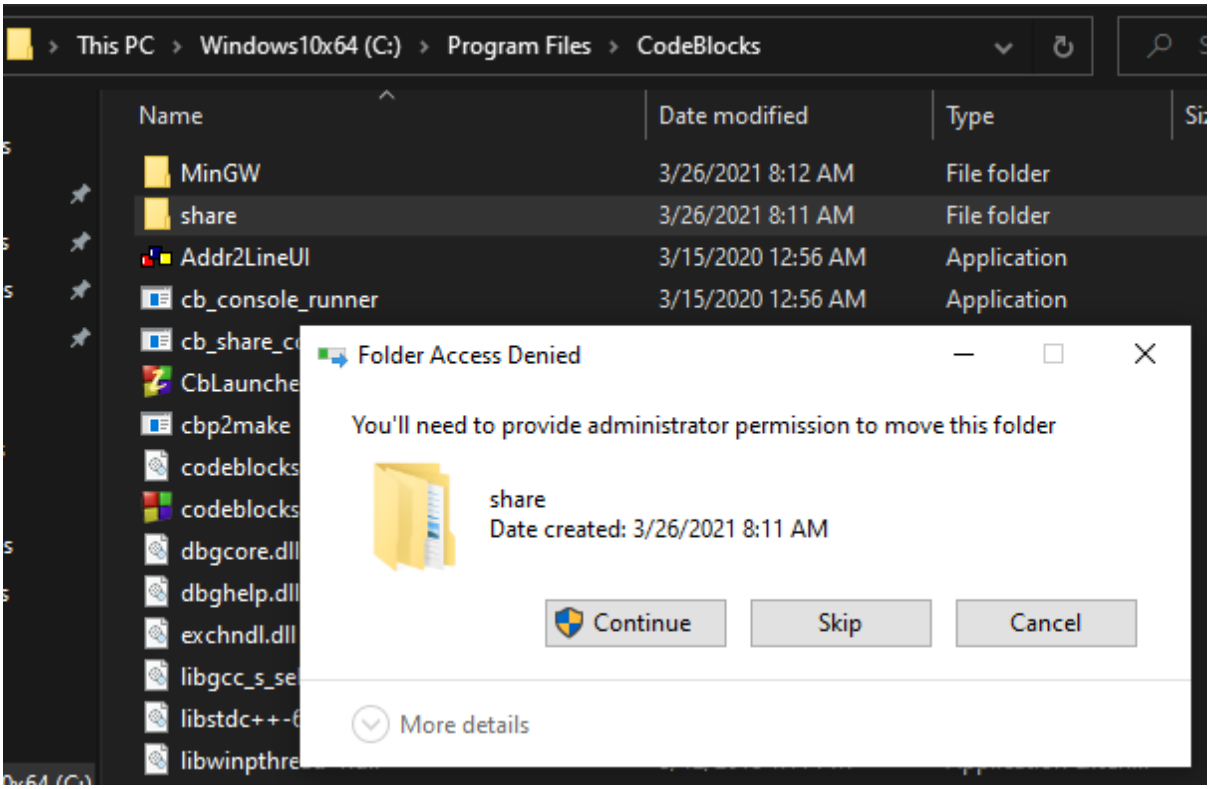
4.Sau cùng nhất Enable inhertitance rồi nhấn apply và OK



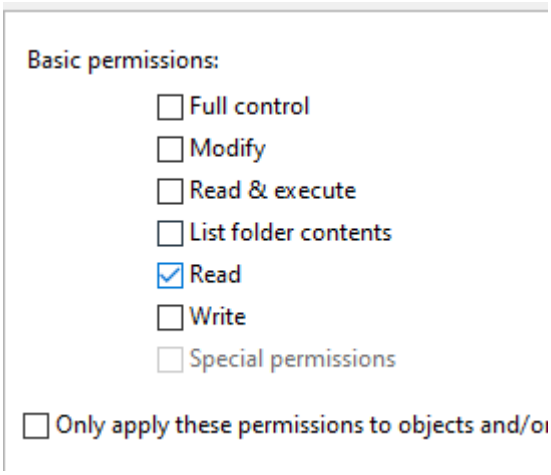
- **Được phép đọc /ghi**



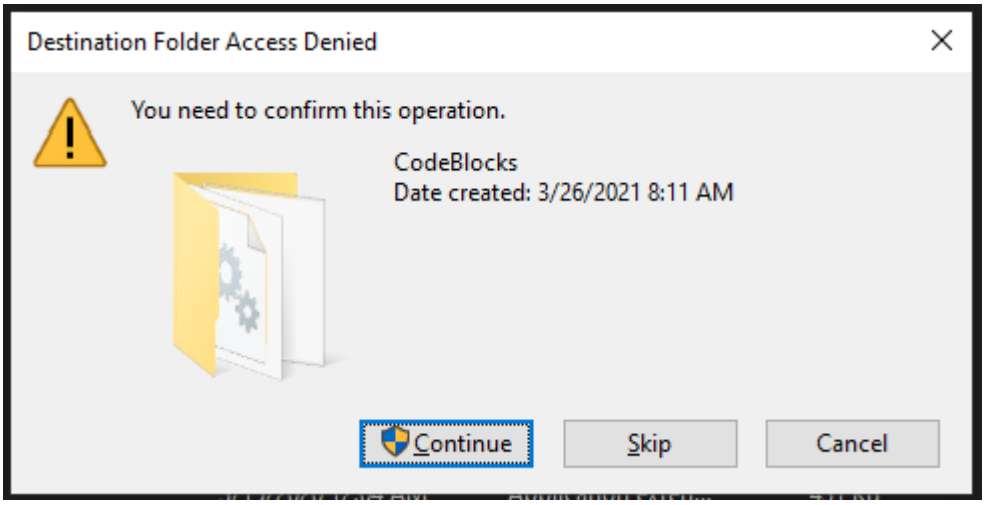
Được phép được đọc/ ghi nên không thể di chuyển được



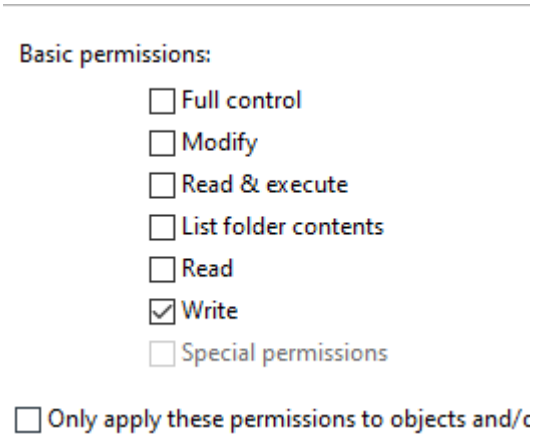
○ Chỉ được phép đọc



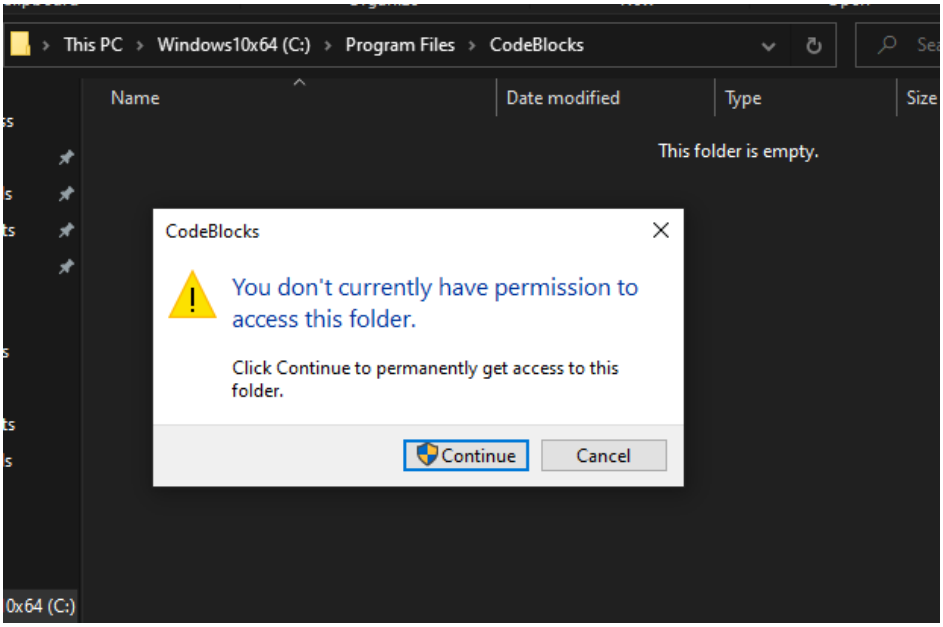
Chỉ được phép đọc nên không thể ghi hay thực thi như tạo file/floder mới



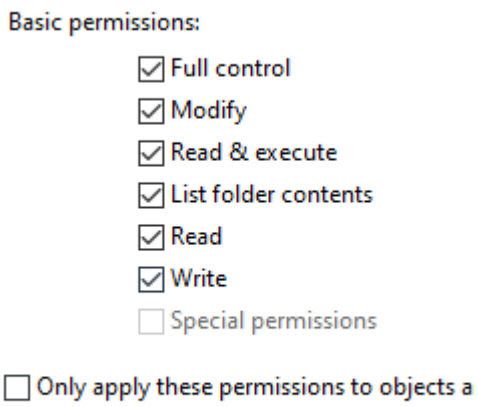
○ Chỉ được phép ghi



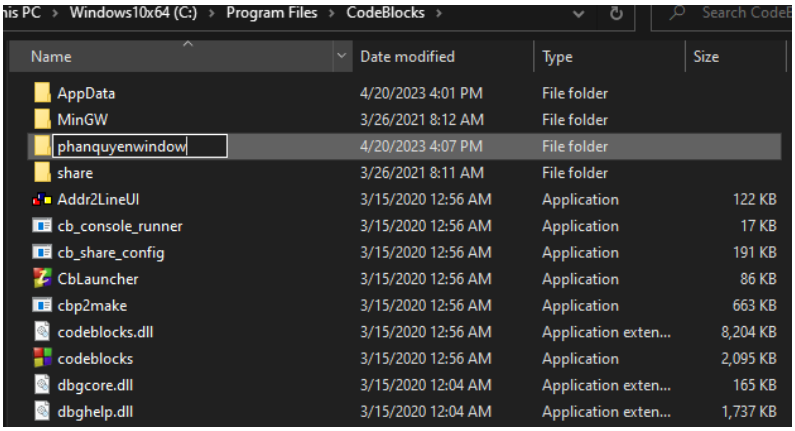
Chỉ được phép ghi nên không thể đọc được file nào hết trong floder đã phân quyền



- **Full control**



Do được phần full control nên ta có tất cả các quyền trên folder này. Có thể thêm sửa xóa, đọc, viết, di chuyển, copy,..



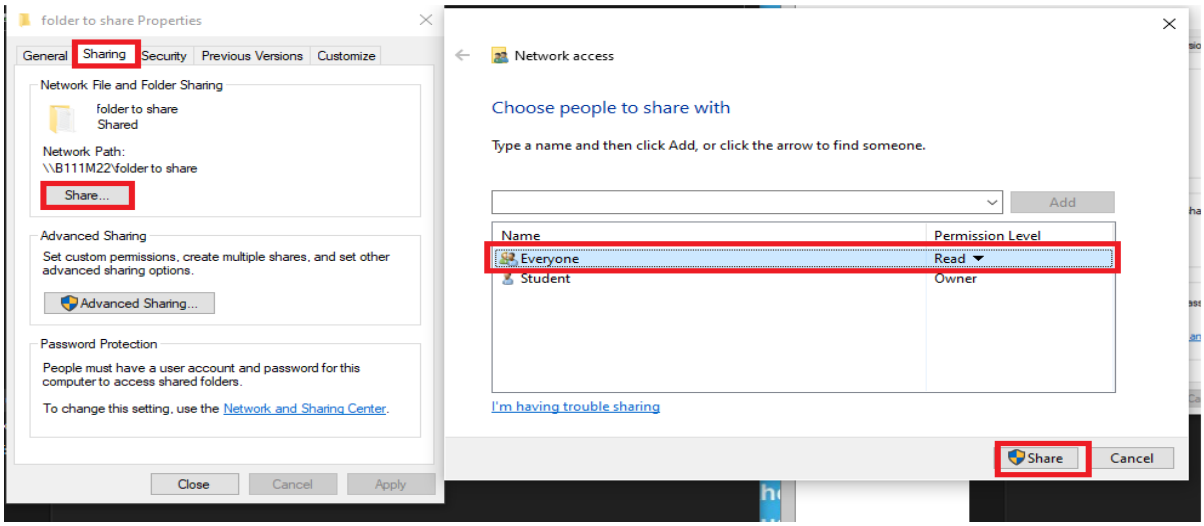
- Thực hiện kiểm tra với mỗi thiết lập trên

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

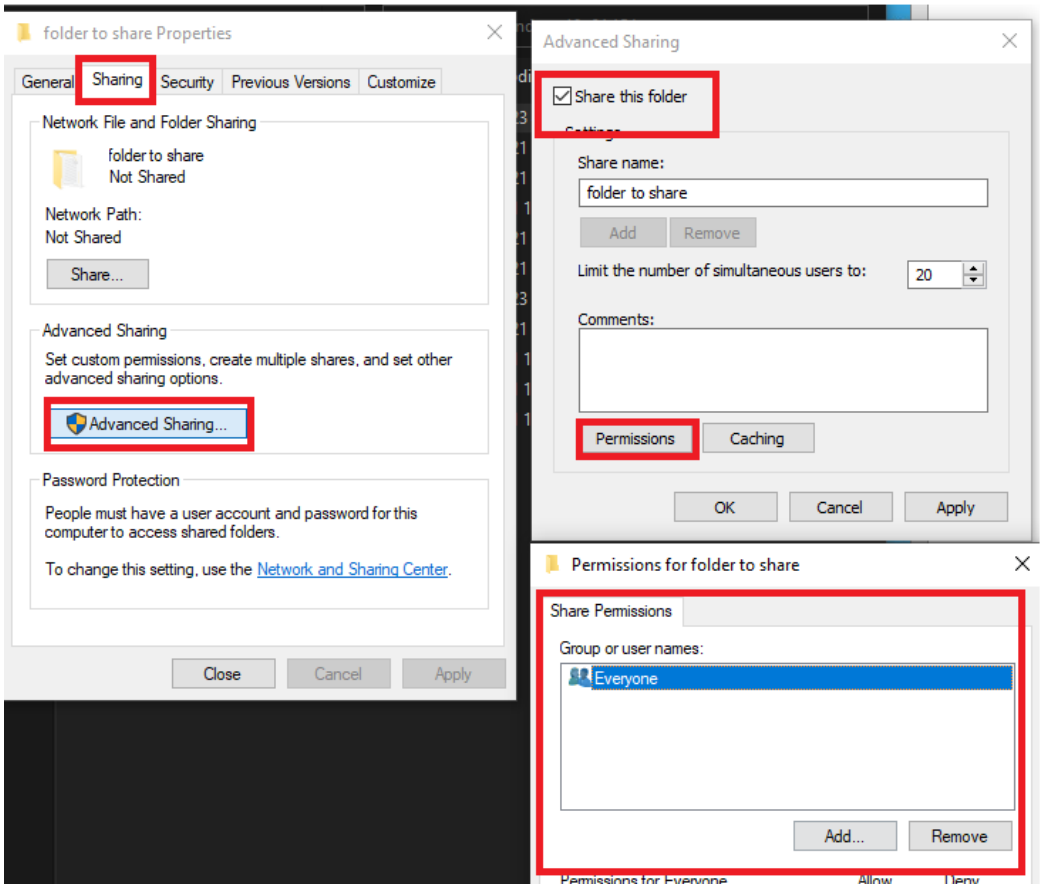
2. Thiết lập permissions trên một folder :

- Chia sẻ folder cho tất cả user trên 1 hệ thống

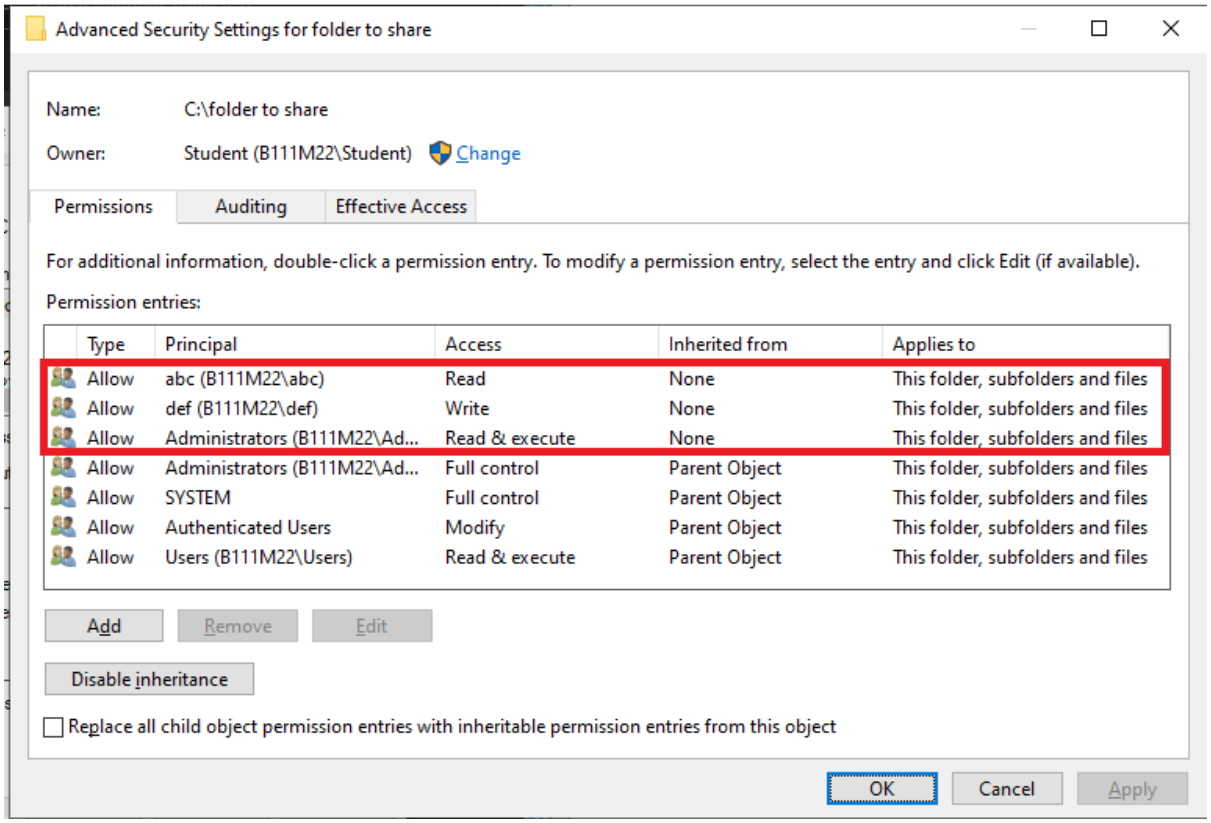
Cách 1:



Hoặc cách 2:



- Quyền Read với group abc
- Quyền Write với group def
- Quyền Read & execute với group administrators



LINUX

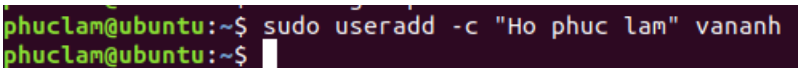
1. User

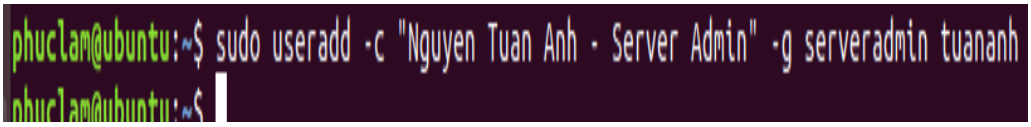
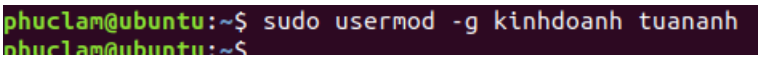
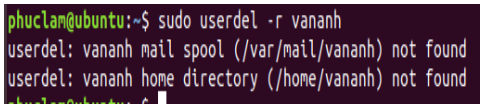
- User là người có thể truy cập đến hệ thống.
- User có **username** và **password**.
- Có hai loại user: **super user** và **regular user**.
- Mỗi user còn có một định danh riêng gọi là **UID**.
- Định danh của người dùng bình thường sử dụng giá trị bắt đầu từ 500.

2. 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.

3. Tập lệnh quản lý User và Group

<table>
<tr><td>Tạo User:</td><td>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
 


</td></tr>
<tr><td>Thay đổi thông tin cá nhân:</td><td>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.
 
</td></tr>
<tr><td>Xóa người dùng</td><td>Cúpháp : #userdel [option] <username>
Vídụ : #userdel –r vana
 
</td></tr>
</table>

Khóa/Mở khóa người dùng	**passwd –l / passwd –u**
	`phuclam@ubuntu:~$ sudo passwd -l quangminh`
	`passwd: password expiry information changed.`
	`phuclam@ubuntu:~$ sudo passwd -u quangminh`
	`passwd: password expiry information changed.`
	usermod –L / usermod –U
	`phuclam@ubuntu:~$ sudo usermod -L quangminh`
	`phuclam@ubuntu:~$ sudo usermod -U quangminh`
	`phuclam@ubuntu:~$`
	Trong /etc/shadow có thể khóa tài khoản bằng cách thay từ khóa x bằng từ khóa *.
	-L : là Lock khóa user lại
	-U : là Unlock để mở user.

Tạo nhóm:	**Cú pháp: #groupadd** <groupname> **Ví dụ:** #groupadd serveradmin `phuclam@ubuntu:~$ sudo groupadd serveradmin`
Xóa nhóm	**Cú pháp: #groupdel** <groupname> **Ví dụ:** #groupdel <serveradmin> `phuclam@ubuntu:~$ sudo groupdel serveradmin`

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
	`phuclam@ubuntu:~$ id -g tuananh`
	`1005`
	`phuclam@ubuntu:~$ groups tuananh`
	`tuananh : kinhdoanh`
	`phuclam@ubuntu:~$`

4. 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.

```
phuclam@ubuntu:~$ sudo cat /etc/passwd
phuclam:x:1000:1000:hophuclam,,,:/home/phuclam:/bin/bash
hoangthuan:x:1001:1001:huynhhoangthuan,01,0,0,0:/home/hoangthuan:/bin/bash
vantam:x:1002:1002:tm,s,s,s,s:/home/vantam:/bin/bash
tuananh:x:1004:1005:Nguyen Tuan Anh - Server Admin:/home/tuananh:/bin/sh
quangminh:x:1003:1003:bui quang minh,1,2,3,4:/home/quangminh:/bin/bash
```

#/etc/group

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

```
phuclam@ubuntu:~$ sudo cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,phuclam
```

```
phuclam:x:1000:
sambashare:x:126:phuclam
hoangthuan:x:1001:
vantam:x:1002:
serveradmin:x:1004:
kinhdoanh:x:1005:
quangminh:x:1003:
phuclam@ubuntu:~$
```

#/etc/shadow

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

```
phuclam@ubuntu:~$ sudo -i
root@ubuntu:~# cat /etc/shadow
root:!:19458:0:99999:7:::
daemon:*:18295:0:99999:7:::
```

```
phuclam:$1$Qm1qNdtx$jw6Oeg66PrhMG09JyZIoP/:19458:0:99999:7:::
hoangthuan:$6$wyYkreXX$lIRBqLhciGUz8GBDy9rDevCHPoX6jbF2DeFcYiVk0jf9t3g/W2RkQPPD2DFu0Tq7FsJjdX5Ufw
lnsF3I92RSY.:19460:0:99999:7:::
vantam:$6$sLWHlKfa$F26sgi0IjgxW3QqMZ6QgO4v3igILpIHnvZLUJuaj1chltOssP5FOs00mc3P9ZZCwwJJGo45A4OTlcx
f/Qyt9Y/:19460:0:99999:7:::
tuananh:!:19468:0:99999:7:::
quangminh:$6$wKFrQWYX$Vh6x/0b5cONAJA7QZ6PU9j23w9ba3uI0BOnHBjx8fyVXz7/jsWdckfwES.DSoafvjPwgTI8zE8R
S5XKcG/d0F/:19468:0:99999:7:::
root@ubuntu:~#
```

5. 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@ubuntu:~# ls -l
total 8
-rwx---r-- 1 root root   15 Apr 12 23:05 hello.txt
drwx------ 6 root root 4096 Apr 11 03:53 snap
root@ubuntu:~#
```

```
[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
```

```
root@ubuntu:~# ls -la
total 36
drwx------  5 root root 4096 Apr 12 23:05 .
drwxr-xr-x 28 root root 4096 Apr 20 07:35 ..
-rw-------  1 root root 1040 Apr 12 23:10 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Feb  3  2020 .cache
-rwx---r--  1 root root   15 Apr 12 23:05 hello.txt
drwxr-xr-x  3 root root 4096 Apr 12 23:05 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  6 root root 4096 Apr 11 03:53 snap
root@ubuntu:~#
```

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.*

6. 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*

```
root@ubuntu:~# chmod 644 hello.txt
root@ubuntu:~# ls -la
total 36
drwx------  5 root root 4096 Apr 12 23:05 .
drwxr-xr-x 28 root root 4096 Apr 20 07:35 ..
-rw-------  1 root root 1040 Apr 12 23:10 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Feb  3  2020 .cache
-rw-r--r--  1 root root   15 Apr 12 23:05 hello.txt
```

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

  Cú pháp : #**chown**

  sudo chown [tên user mới]:[tên group mới] [đường dẫn đến file/thư mục]

```
root@ubuntu:~# chown vantam:phuclam /
```

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

  Cú pháp : #**chgrp**

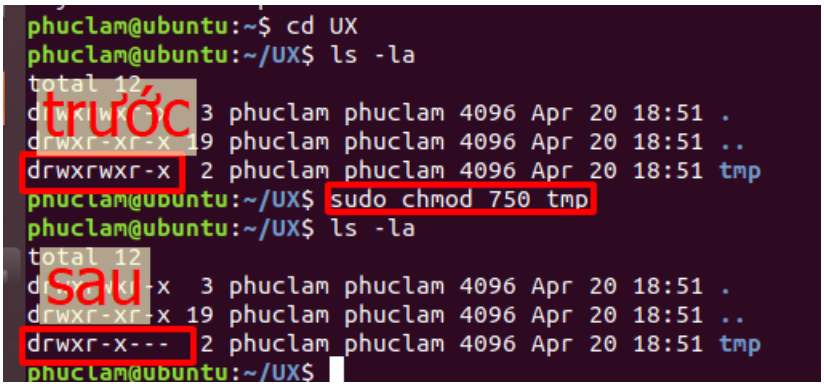
  sudo chgrp users file.txt

```
root@ubuntu:~# chgrp hoangthuan hello.txt
root@ubuntu:~#
```

BÀI TẬP ĐỀ NGHỊ

Phân quyền trên hệ thống tập tin

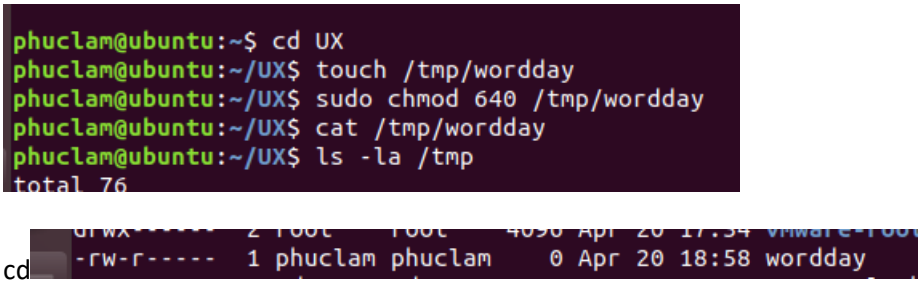
1. Tạo thư mục tmp dưới thư mục UX và cho nó quyền truy nhập rwxr-x---




```
sudo mkdir /UX/tmp
sudo chmod 750 /UX/tmp
```

2. 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.

Vì do tệp wordday rỗng nên khi đọc sẽ không hiển thị gì trên màn hình.




```
sudo touch /UX/tmp/wordday
sudo chmod 640 /UX/tmp/wordday
cat /UX/tmp/wordday
```

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

chmod u-r wordday

cat wordday

```
sudo chmod 600 /UX/tmp/wordday
cat /UX/tmp/wordday
```
Sẽ có thông báo lỗi "Permission denied".

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

chmod u-w /UX/tmp

rm /UX/tmp/wordday

```
sudo chmod -w /UX/tmp
rm /UX/tmp/wordday
```
Sẽ có thông báo lỗi "Permission denied".

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

```
sudo chmod -r /UX/tmp
ls /UX/tmp
```
Sẽ có thông báo lỗi "Permission denied".

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

```
sudo chmod -x /UX/tmp
cd /UX/tmp
```
Sẽ có thông báo lỗi "Permission denied".

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

```
sudo chmod 700 /UX/tmp
```

8. Thử cho bạn quyền ghi (w) vào thư mục chủ của một thành viên của nhóm của bạn
   sudo chown phuclam /UX/tmp
9. Xoá nội dung và bản thân thư mục tmp

sudo chmod g+w /UX/tmp