



22162029 Le Quang Trong Nghia Lab4 ACCESS CONTROL

An toàn thông tin (Trường Đại học Sư phạm Kỹ Thuật Thành phố Hồ Chí Minh)



Scan to open on Studocu

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HCM
KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN AN TOÀN THÔNG TIN**

□□□



HCMUTE

**BÁO CÁO BÀI THỰC HÀNH
LAB 04: ACCESS CONTROL**

GVHD: HUỲNH NGUYỄN CHÍNH

MÃ HP: INSE330380_23_2_03

SINH VIÊN THỰC HIỆN:

STT	HỌ VÀ TÊN	MSSV
1	Lê Quang Trọng Nghĩa	22162029

TP.HCM, 3/2024

MỤC LỤC

1. Tổng quan.....	1
2. Thực hành	2

1. Tổng quan

Access Control (Kiểm soát truy cập) đề cập đến khả năng người dùng truy cập vào một đối tượng cụ thể và có thể sửa đổi nó. Về mặt hệ điều hành, *Access Control* đề cập đến khả năng người dùng đọc, ghi hoặc thực thi một tệp hoặc thư mục nhất định. Mục tiêu của bài lab này là để ta nghiên cứu khung kiểm soát truy cập cho các nền tảng dựa trên *Microsoft Windows* và *UNIX – 7*.

2. Thực hành

2.1. Sử dụng lệnh *chmod* trên *LINUX*

Permission Bits											
Extra			Owner			Group			Others		
su	sg	t	r	w	x	r	w	x	r	w	x

su: Set-UID, **sg**: Set-GID, **t**: sticky

- Một số tùy chọn của *chmod* command:

```
$chmod u+w = add write to *user*
$chmod g-rw = remove read and write from *group*
$chmod o-rwx = remove read, write and execute from *other*
$chmod a+w = add write to *all*
$chmod a-wx = remove write and execute from *all*

$ chmod -R 755 myfolder
```

Lưu ý: -R. Nó cho phép bạn sửa đổi các đối tượng **một cách đệ quy**, thay đổi quyền trên tất cả các đối tượng trong một thư mục và các thư mục con của nó.

- *Linux file system permissions*:

Bước 1: Tạo 3 tài khoản người dùng: trongnghia, quangminh, baophuc
Password: user123

```
nghia@nghia-2602: ~  
nghia@nghia-2602:~$ sudo adduser trongnghia  
info: Adding user 'trongnghia' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group 'trongnghia' (1004) ...  
info: Adding new user 'trongnghia' (1004) with group 'trongnghia (1004)' ...  
info: Creating home directory '/home/trongnghia' ...  
info: Copying files from '/etc/skel' ...  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: password updated successfully  
Changing the user information for trongnghia  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] y  
info: Adding new user 'trongnghia' to supplemental / extra groups 'users' ...  
info: Adding user 'trongnghia' to group 'users' ...  
nghia@nghia-2602:~$
```

```
nghia@nghia-2602: ~  
info: Adding user 'trongnghia' to group 'users' ...  
nghia@nghia-2602:~$ sudo adduser quangminh  
[sudo] password for nghia:  
info: Adding user 'quangminh' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group 'quangminh' (1005) ...  
info: Adding new user 'quangminh' (1005) with group 'quangminh (1005)' ...  
info: Creating home directory '/home/quangminh' ...  
info: Copying files from '/etc/skel' ...  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: password updated successfully  
Changing the user information for quangminh  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] y  
info: Adding new user 'quangminh' to supplemental / extra groups 'users' ...  
info: Adding user 'quangminh' to group 'users' ...  
nghia@nghia-2602:~$
```

```
nghia@nghia-2602: ~  
info: Adding new user 'quangminh' to supplemental / extra groups 'users' ...  
info: Adding user 'quangminh' to group 'users' ...  
nghia@nghia-2602:~$ sudo adduser baophuc  
info: Adding user 'baophuc' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group 'baophuc' (1006) ...  
info: Adding new user 'baophuc' (1006) with group 'baophuc (1006)' ...  
info: Creating home directory '/home/baophuc' ...  
info: Copying files from '/etc/skel' ...  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: password updated successfully  
Changing the user information for baophuc  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n] y  
info: Adding new user 'baophuc' to supplemental / extra groups 'users' ...  
info: Adding user 'baophuc' to group 'users' ...  
nghia@nghia-2602:~$
```

Bước 2: Tạo 3 files hoặc folders

- Chuyển qua user trongnghia và tạo folder với tên trongnghiafolder có permission như sau:

```
trongnghia@nghia-2602: ~  
nghia@nghia-2602:~$ sudo su - trongnghia  
trongnghia@nghia-2602:~$ mkdir trongnghiafolder  
trongnghia@nghia-2602:~$ ls -l  
total 4  
drwxrwxr-x 2 trongnghia trongnghia 4096 Mar 22 23:35 trongnghiafolder  
trongnghia@nghia-2602:~$
```

- Chuyển qua user quangminh và tạo folder với tên quangminhfolder có permission như sau:

```
nghia@nghia-2602:~$ sudo su - quangminh  
quangminh@nghia-2602:~$ mkdir quangminhfolder  
quangminh@nghia-2602:~$ ls -l  
total 4  
drwxrwxr-x 2 quangminh quangminh 4096 Mar 22 23:41 quangminhfolder  
quangminh@nghia-2602:~$
```

- Chuyển qua user baophuc và tạo folder với tên baophucfolder có permission như sau:

```
nghia@nghia-2602:~$ sudo su - baophuc  
baophuc@nghia-2602:~$ mkdir baophucfolder  
baophuc@nghia-2602:~$ ls -l  
total 4  
drwxrwxr-x 2 baophuc baophuc 4096 Mar 22 23:42 baophucfolder  
baophuc@nghia-2602:~$
```

Bước 3: Sử dụng lệnh chmod để thay đổi quyền đối với các tệp hoặc thư mục này:

Permission Bits											
Extra			Owner			Group			Others		
su	sg	t	r	w	x	r	w	x	r	w	x

Mỗi quyền truy cập trong hệ thống Unix/Linux được biểu thị bằng một số octal 3-bit như sau:

- Quyền đọc (read) được biểu thị bằng 4 (100 trong hệ thống octal).
- Quyền ghi (write) được biểu thị bằng 2 (010 trong hệ thống octal).
- Quyền thực thi (execute) được biểu thị bằng 1 (001 trong hệ thống octal).

Khi bạn kết hợp các quyền truy cập lại với nhau, bạn sẽ có các con số octal tương ứng. Ví dụ :

- Quyền read và write là $4 + 2 = 6$ (110 trong hệ thống octal).

- Quyền read và execute là $4 + 1 = 5$ (101 trong hệ thống octal).
- Quyền read, write và execute là $4 + 2 + 1 = 7$ (111 trong hệ thống octal).

3.1. Thay đổi quyền với trongnghiafolder

Lúc đầu trongnghiafolder có các quyền đối với Owner là toàn quyền, Group là toàn quyền và Others chỉ có quyền read và execute.

Tiến hành thay đổi, ta có permission Owner là toàn quyền, Group và Others chỉ có quyền read và execute:

Extra			Owner			Group			Others		
su	sg	t	r	w	x	r	w	x	r	w	x
0	0	0	1	1	1	1	0	0	1	0	0

➔ Chmod 754 trongnghiafolder

```

nghia@nghia-2602:~$ sudo su - trongnghia
trongnghia@nghia-2602:~$ chmod 744 trongnghiafolder
trongnghia@nghia-2602:~$ ls -l
total 4
drwxr--r-- 2 trongnghia trongnghia 4096 Mar 22 23:35 trongnghiafolder
trongnghia@nghia-2602:~$

```

3.2. Thay đổi quyền với quangminhfolder

Lúc đầu quangminhfolder có các quyền đối với Owner là toàn quyền, Group là toàn quyền và Others chỉ có quyền read và execute.

Tiến hành thay đổi, ta có permission Owner là toàn quyền, Group có quyền read và execute và Others chỉ có quyền read:

Extra			Owner			Group			Others		
su	sg	t	r	w	x	r	w	x	r	w	x
0	0	0	1	1	1	1	0	1	1	0	0

➔ Chmod 754 quangminhfolder

```

nghia@nghia-2602:~$ sudo su - quangminh
quangminh@nghia-2602:~$ chmod 754 quangminhfolder
quangminh@nghia-2602:~$ ls -l
total 4
drwxr-xr-- 2 quangminh quangminh 4096 Mar 22 23:41 quangminhfolder
quangminh@nghia-2602:~$

```

3.3. Thay đổi quyền với baophucfolder

Lúc đầu baophucfolder có các quyền đối với Owner là toàn quyền, Group là toàn quyền và Others chỉ có quyền read và execute.

Tiến hành thay đổi, ta có permission Owner, Group và Others chỉ có quyền read và write:

Extra			Owner			Group			Others		
su	sg	t	r	w	x	r	w	x	r	w	x
0	0	0	1	1	0	1	1	0	1	1	0

→ Chmod 666 baophucfolder

```
ngghia@ngghia-2602:~$ sudo su - baophuc
baophuc@ngghia-2602:~$ chmod 666 baophucfolder
baophuc@ngghia-2602:~$ ls -l
total 4
drw-rw-rw- 2 baophuc baophuc 4096 Mar 22 23:42 baophucfolder
baophuc@ngghia-2602:~$
```

2.2. Sử dụng NTFS permission trên Windows

Bước 1: Tạo 3 tài khoản người dùng: *Alice, John, Julie*:

Tạo folder: Data

Tạo 3 folder ở phía MS window để liên kết với Domain trongnghia.vn

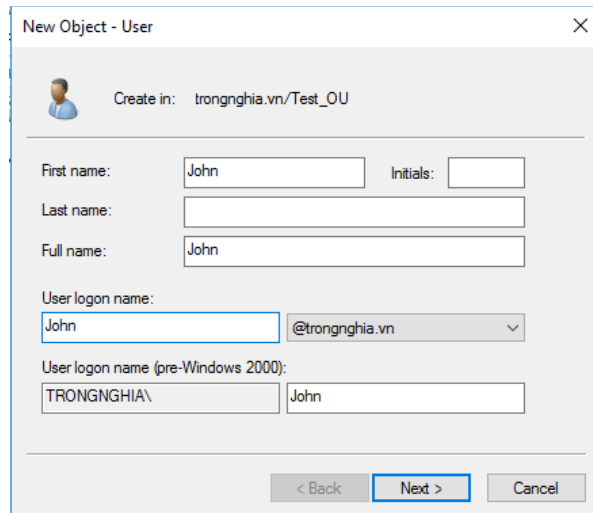
o *Alice*:

The screenshot shows the 'New Object - User' dialog box with the title bar 'New Object - User' and a close button. The 'Create in:' field is set to 'trongnghia.vn/Test_OU'. The 'First name' field contains 'Alice', and the 'Initials' field is empty. The 'Last name' field is empty. The 'Full name' field contains 'Alice'. The 'User login name' field contains 'Alice' and the domain dropdown is set to '@trongnghia.vn'. The 'User login name (pre-Windows 2000)' field contains 'TRONGNGHIA\Alice'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

The screenshot shows the 'New Object - User' dialog box with the title bar 'New Object - User' and a close button. The 'Create in:' field is set to 'trongnghia.vn/Test_OU'. The 'Password' field is masked with dots, and the 'Confirm password' field is also masked with dots. Below the password fields, there are four checkboxes: 'User must change password at next login', 'User cannot change password', 'Password never expires', and 'Account is disabled'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

The screenshot shows the 'New Object - User' dialog box with the title bar 'New Object - User' and a close button. The 'Create in:' field is set to 'trongnghia.vn/Test_OU'. The text 'When you click Finish, the following object will be created:' is displayed above a text box. The text box contains the following information: 'Full name: Alice' and 'User login name: Alice@trongnghia.vn'. At the bottom, there are buttons for '< Back', 'Finish', and 'Cancel'.

○ John:



New Object - User

Create in: trongnghia.vn/Test_OU

First name: John Initials:

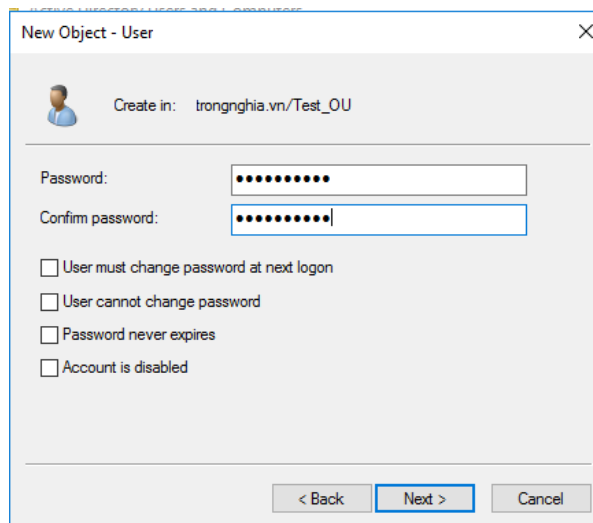
Last name:

Full name: John

User logon name: John @trongnghia.vn

User logon name (pre-Windows 2000): TRONGNGHIA\ John

< Back Next > Cancel



New Object - User

Create in: trongnghia.vn/Test_OU

Password:

Confirm password:

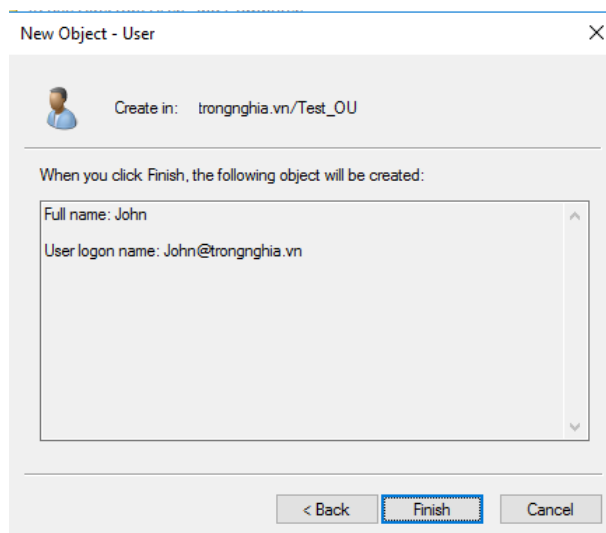
☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back Next > Cancel



New Object - User

Create in: trongnghia.vn/Test_OU

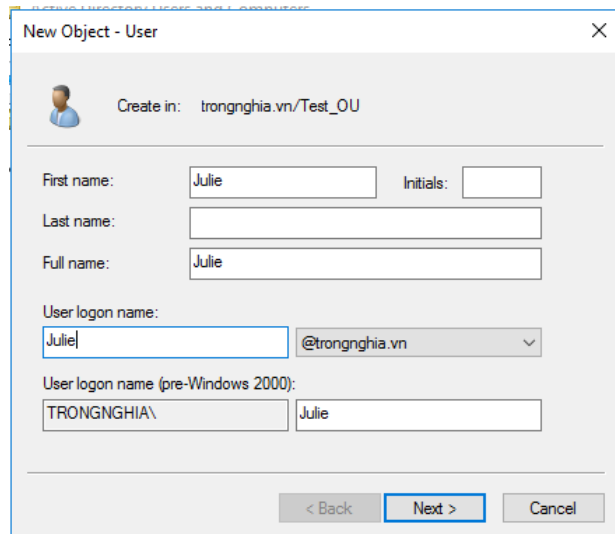
When you click Finish, the following object will be created:

Full name: John

User logon name: John@trongnghia.vn

< Back Finish Cancel

○ Julie:



New Object - User

Create in: trongnghia.vn/Test_OU

First name: Julie Initials:

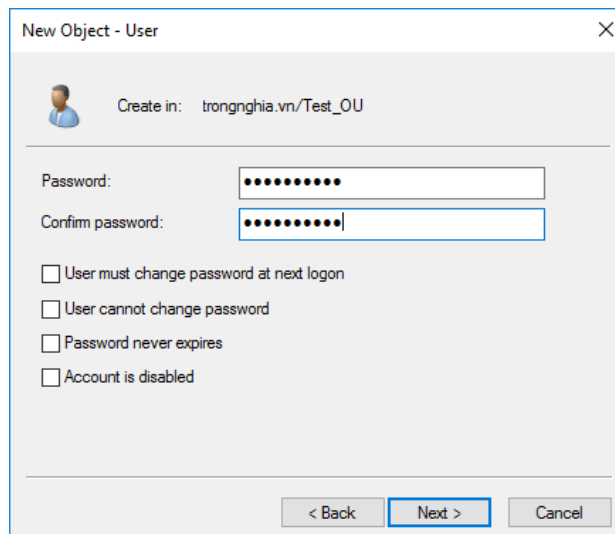
Last name:

Full name: Julie

User logon name: Julie @trongnghia.vn

User logon name (pre-Windows 2000): TRONGNGHIA\ Julie

< Back Next > Cancel



New Object - User

Create in: trongnghia.vn/Test_OU

Password:

Confirm password:

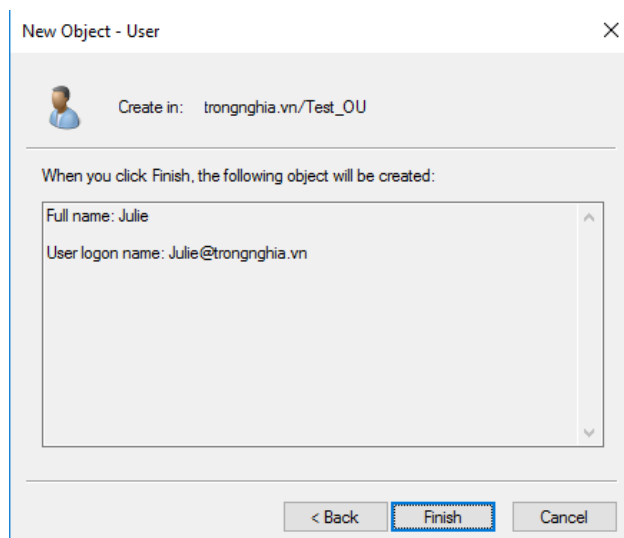
☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back Next > Cancel



New Object - User

Create in: trongnghia.vn/Test_OU

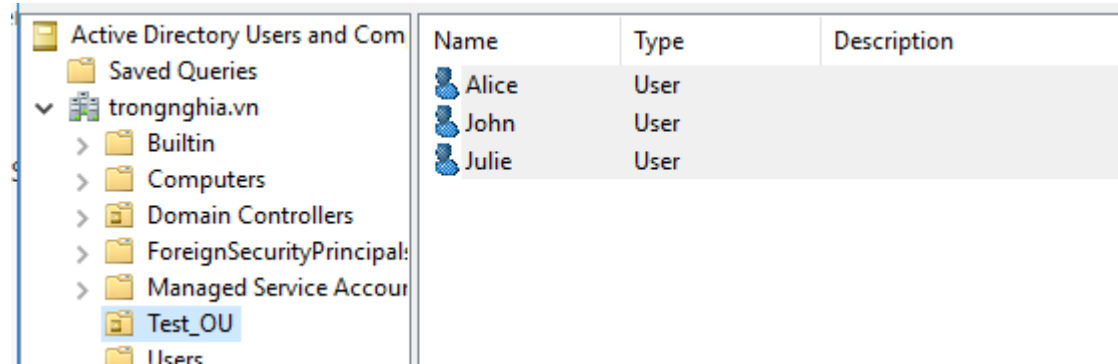
When you click Finish, the following object will be created:

Full name: Julie

User logon name: Julie@trongnghia.vn

< Back Finish Cancel

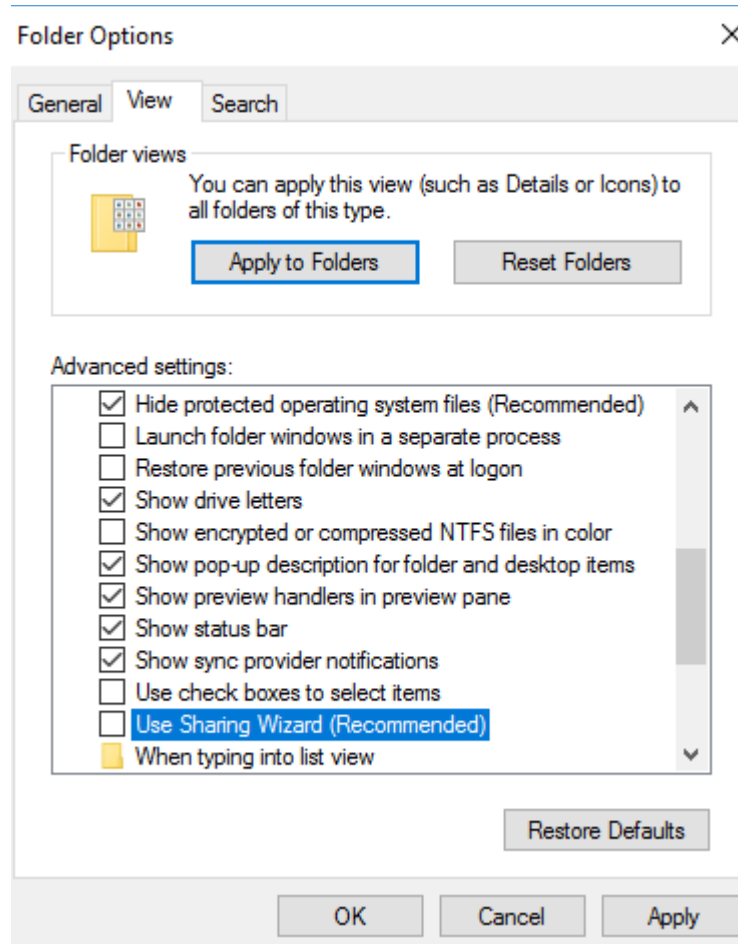
Tạo thành công 3 user ở WinXP



Name	Type	Description
Alice	User	
John	User	
Julie	User	

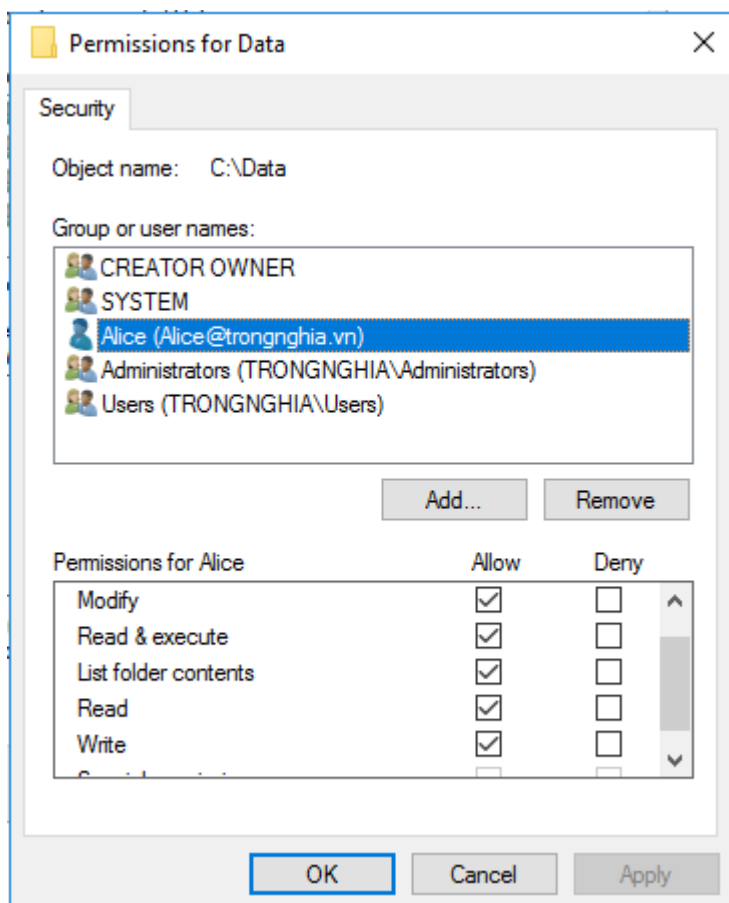
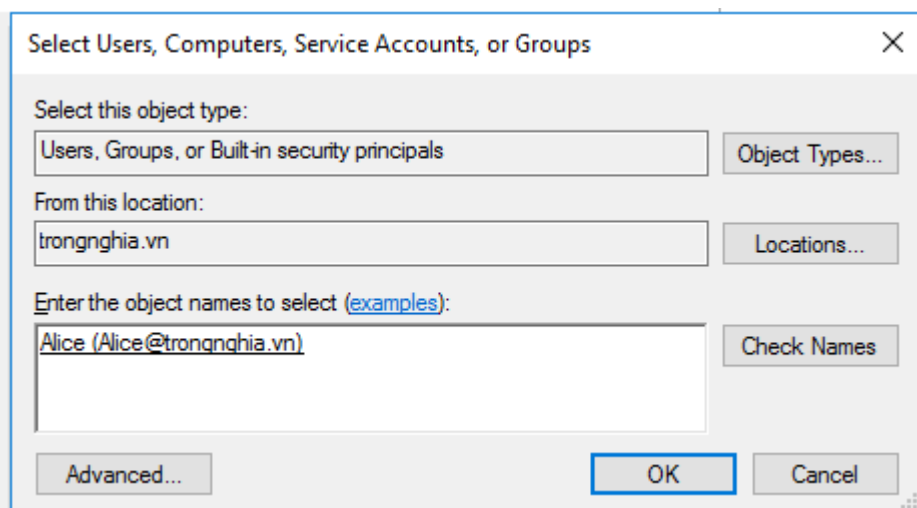
Trước khi có NTFS permission on Windows

Ta cần tắt tính năng quyền đơn giản khi chia sẻ file trên Windows

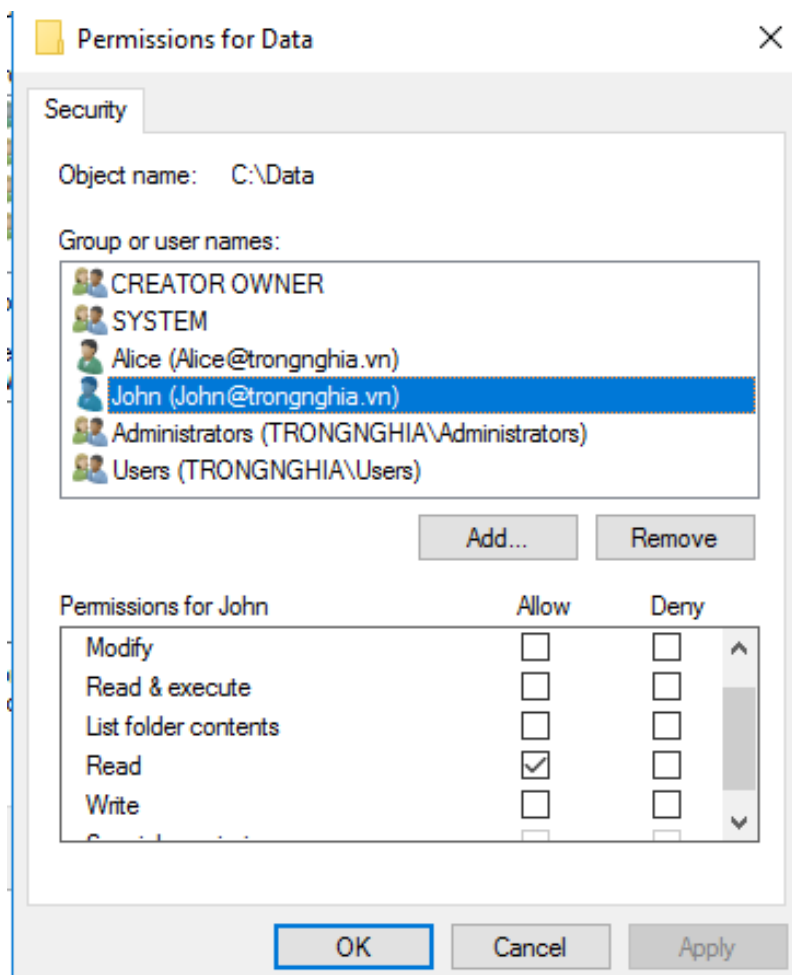
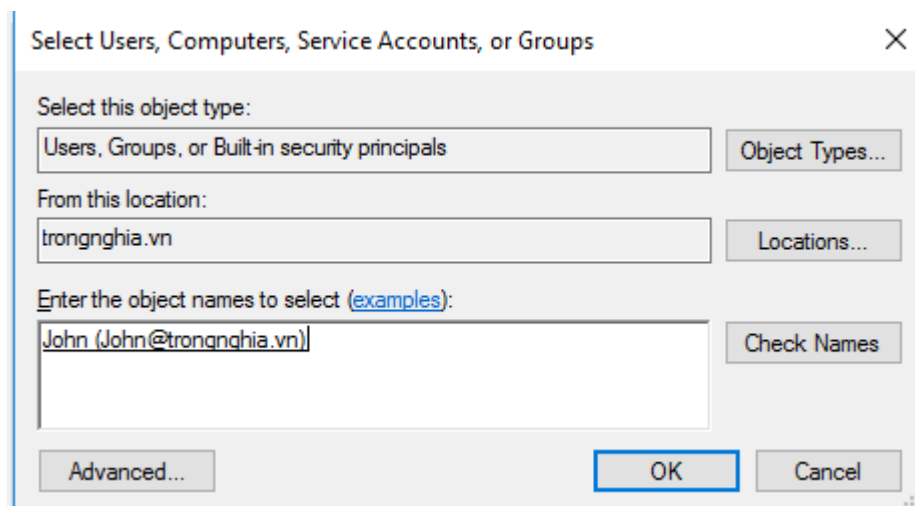


Bước 2: Tạo 1 thư mục *Data* và thiết lập quyền *NTFS* cho thư mục *Data*:

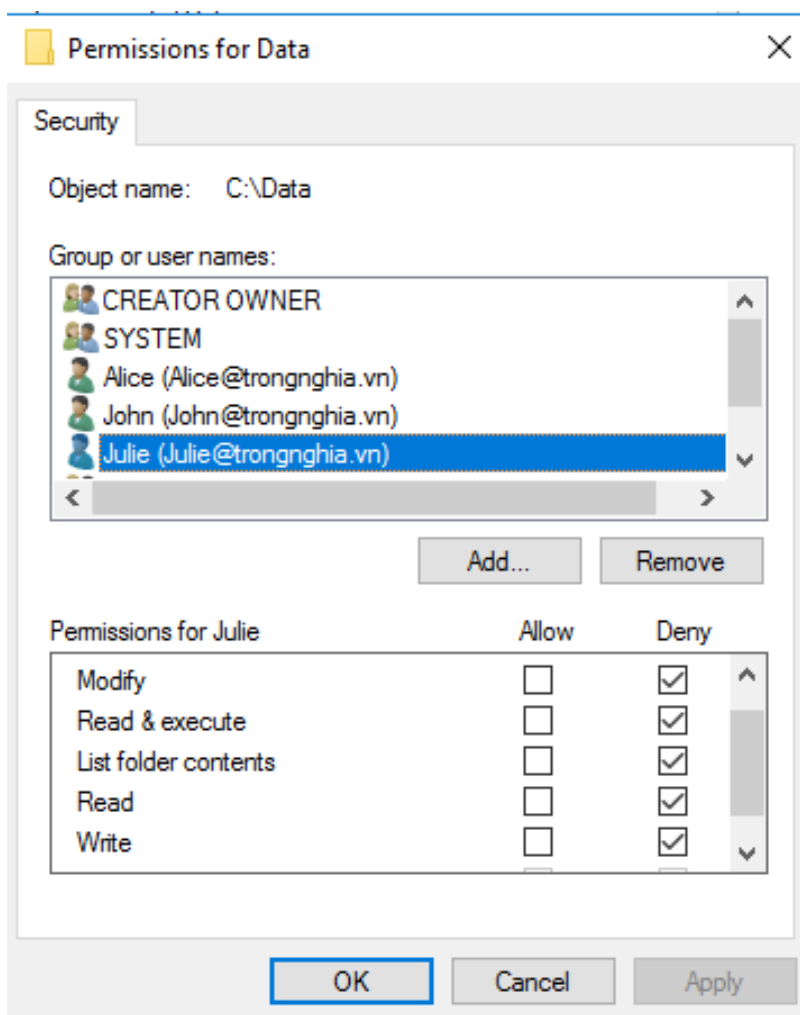
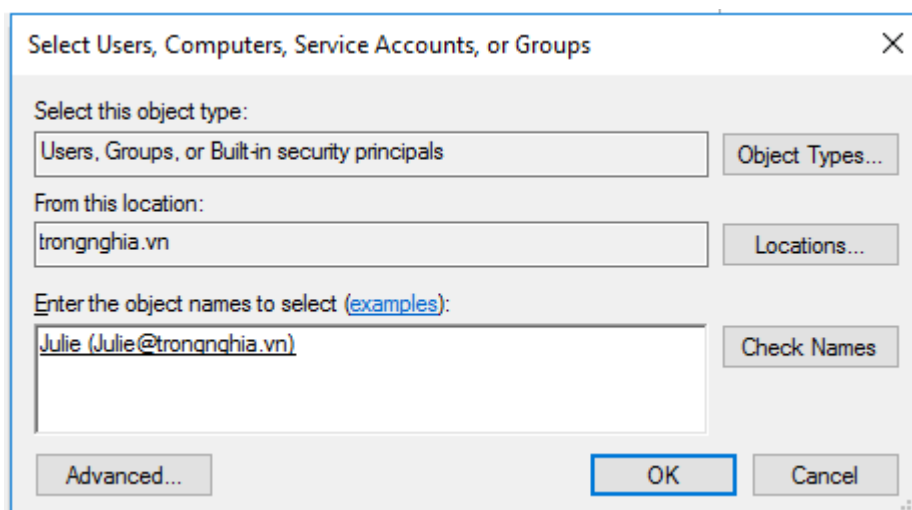
- Alice có toàn quyền đối với thư mục *Data*



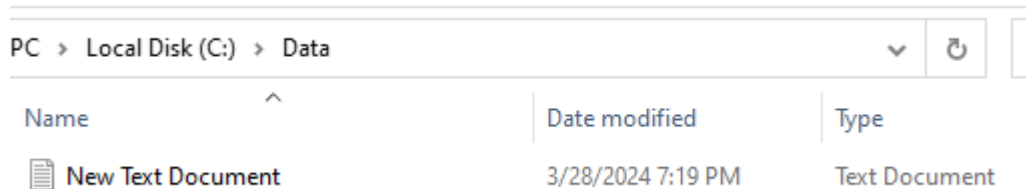
- John chỉ có quyền đọc trên thư mục Data



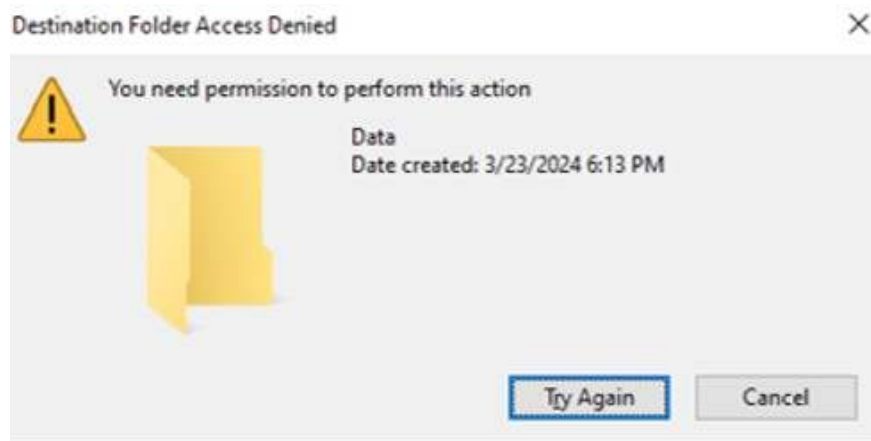
- Julie không có quyền nào trên thư mục Data



- *Alice*: Đọc được thư mục Data cũng như có thể ghi, sửa và xóa các tệp (Tạo folder hay file New Text Document)



- *John*: Chỉ đọc được các tệp và thư mục trong Data, không thực hiện được ghi, xóa chỉnh



- *Julie*: Không thể mở thư mục Data, sẽ nhận thông báo lỗi:

