

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

Môn: HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX
BÁO CÁO BÀI THỰC HÀNH SỐ 2

Họ và tên sinh viên:

Trần Đức Minh

Mã số sinh viên:

B20DCAT127

Họ và tên giảng viên:

TS. Đinh Trường Duy

Hà Nội 10/2022

I. Giới thiệu chung

1. Mục đích

- Giúp sinh viên hiểu được cách quản trị một nhóm người dùng trong mạng Lan nội bộ.

2. Yêu cầu

- Sinh viên đã nắm được nội dung lý thuyết.
- Biết cách cấu hình cơ bản: tạo user, password, phân quyền

II. Cơ sở lý thuyết

Máy chủ là thuật ngữ mô tả một máy tính mà kết hợp cả thiết bị phần cứng và phần mềm để xử lý các công việc khác nhau qua môi trường mạng. Về cơ bản máy chủ được thiết kế để cung cấp các dịch vụ và chạy các ứng dụng trong điều kiện tải nặng, thời gian dài và có khả năng chịu lỗi. Thông thường tên máy chủ sẽ gắn với hệ điều hành chạy trên phần cứng máy chủ như máy chủ Windows cho hệ điều hành Microsoft Windows hay máy chủ Linux sử dụng hệ điều hành Linux.

1. Các dịch vụ

Vai trò hay chức năng máy chủ là công việc chủ yếu mà máy chủ sẽ thực hiện. Thực tế, máy chủ có thể đồng thời cung cấp nhiều chức năng hay dịch vụ cho người dùng cũng như là các máy tính khác trong mạng.

Các dịch vụ quan trọng của máy chủ Windows bao gồm:

- Xác thực thư mục động (Active Directory Certificate Services)
- Miền thư mục động (Active Directory Domain Services)
- Liên kết thư mục động (Active Directory Federation Services)
- Thư mục động rút gọn (Active Directory Lightweight Directory Services)

- Quản lý quyền thư mục động (Active Directory Rights Management Services)
- Máy chủ ứng dụng (Application Server)
- Quản lý DHCP (Dynamic Host Configuration Protocol)
- Tên miền DNS (Domain Name System)
- Dịch vụ file
- Dịch vụ ảo hóa Hyper-V
- Truy nhập và chính sách mạng (Network Policy and Access Services)
- In ấn tài liệu (Print and Document Services)
- Dịch vụ đầu cuối (Terminal Services)
- Web (Internet Information Services-IIS)

2. Chuẩn bị cài đặt

Server 2019 cung cấp các phiên bản sau:

- Trung tâm dữ liệu (Datacenter)
- Tiêu chuẩn (Standard)

3. Người dùng và quyền truy nhập

Để sử dụng được máy tính sử dụng hệ điều hành Microsoft Windows, mỗi một người cần phải có tài khoản riêng gọi là tài khoản người dùng. Tài khoản này được sử dụng khi:

Người dùng truy nhập vào mạng

Cho phép người dùng đăng nhập vào máy hay miền thư mục động

Tài khoản cho phép người dùng đăng nhập vào máy tính cụ thể được gọi là tài khoản cục bộ (local account). Tài khoản này chỉ có giá trị đối với một máy tính duy nhất. Khi người dùng muốn sử dụng các tài nguyên trong mạng của một miền (domain) người dùng cần tài khoản miền (domain account). Tài khoản này được tạo trên máy chủ miền và được phép truy nhập vào các tài nguyên của miền. Các thông tin người dùng được lưu trong cơ sở dữ liệu miền và được sao chép tới các máy chủ miền

Để thuận tiện cho việc quản trị, Windows tạo sẵn một số tài khoản như quản trị (Administrator) và khách (Guest). Ngoài ra, các người dùng có vai trò và yêu cầu truy tương tự nhau có thể được xếp vào nhóm người dùng (User group). Điều này giúp cho việc quản trị được dễ dàng và thuận tiện. Tương tự như tài khoản người dùng, nhóm người dùng cũng phân biệt nhóm cục bộ và nhóm miền. Cụ thể như sau:

Nhóm miền cục bộ (Domain local group) tương ứng với nhóm tài khoản ở bất kỳ miền nào có giá trị cục bộ

Nhóm toàn thể (Global group) chứa tài khoản người dùng và nhóm toàn thể khác áp dụng cho một miền cụ thể

Nhóm vạn năng (Universal group) áp dụng cho nhiều miền, chứa các nhóm toàn thể của các miền khác.

Để đơn giản cho công việc quản trị Windows Server cung cấp các nhóm tạo sẵn:

Domain Admins: dùng cho các thành viên làm nhiệm vụ quản trị.

Domain Users: nhóm người dùng miền.

Account Operators: thành viên nhóm có thể tạo, xóa và sửa nhóm và tài khoản người dùng.

Backup Operators: Sao lưu và khôi phục máy chủ miền

Authenticated Users: người dùng hợp lệ

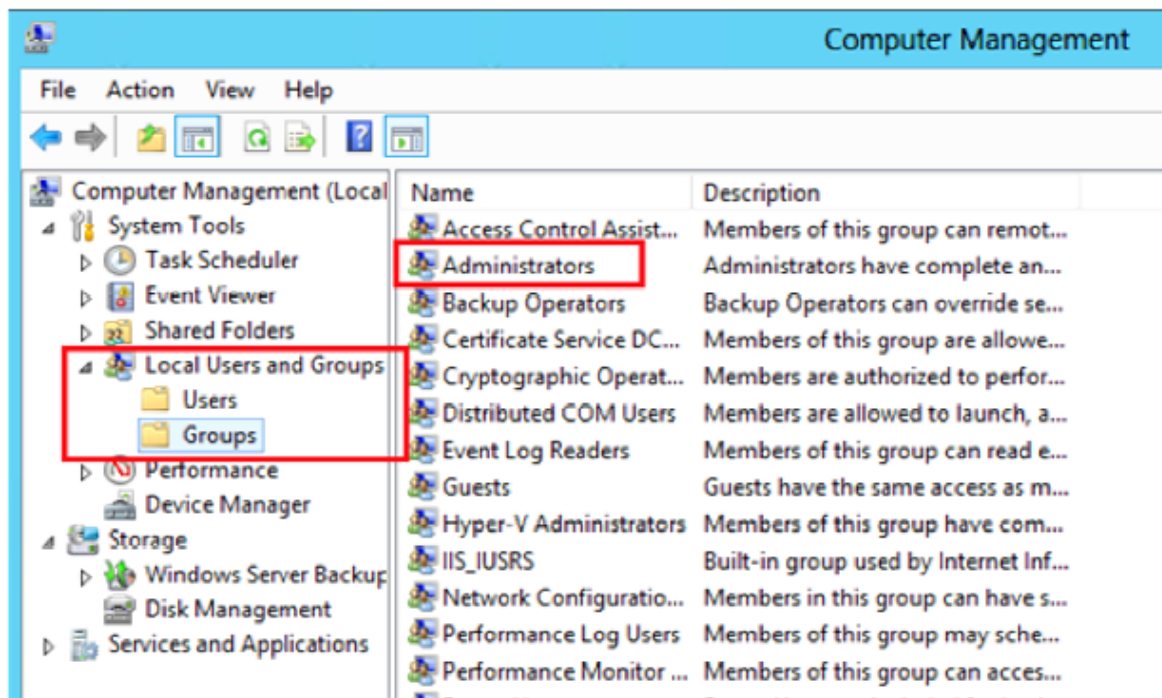
Everyone: bao gồm tất cả các người dùng.

Mỗi tài khoản người dùng cần các thông tin cơ bản sau:

Tên người dùng: được dùng để định danh người sử dụng khi truy nhập vào mạng

Mật khẩu: được gán cho từng tài khoản người dùng và đảm bảo chỉ người dùng được phép mới truy nhập được vào mạng

Các thuộc tính của tài khoản người dùng như họ tên, số điện thoại, thư điện tử.



Với mỗi tài nguyên có kiểm soát truy nhập người dung có thể thực hiện hay cấp các quyền tiêu biểu sau:

Toàn quyền kiểm soát(Full control): bao gồm quyền đọc, ghi, sửa và thực thi đối tượng tài nguyên, thay đổi thuộc tính và quyền, cũng như lấy quyền sở hữu các đối tượng tài nguyên.

Sửa (Modify): cho phép đọc ghi sửa và thay đổi thuộc tính đối tượng tài nguyên.

Đọc (Read): hiển thị dữ liệu, thuộc tính, chủ sở hữu và quyền của các đối tượng tài nguyên.

Ghi (Write): Ghi và thêm dữ liệu vào đối tượng tài nguyên và đọc hay thay đổi các thuộc tính tài nguyên.

4. Chính sách nhóm

Công cụ quản lý nhóm là tính năng quan trọng với Windows cho phép kiểm soát môi trường làm việc với tài khoản người dùng và máy tính.

Các đối tượng chính sách nhóm bao gồm các cài đặt của người dùng và máy tính. Các cài đặt có thể liên quan đến hệ thống (System settings) bao gồm các cài đặt

ứng dụng, màn hình làm việc và các dịch vụ hệ thống. Ngoài ra còn có các cài đặt như:

Cài đặt an ninh (Security settings): cài đặt an ninh mạng, miền và máy tính cục bộ

Cài đặt phần mềm (Software installation settings): Quản lý việc cài đặt phần mềm, cập nhật và gỡ bỏ.

Cài đặt mã (Scripts settings): Các đoạn mã dùng khi máy tính bật và đóng, người dùng đăng nhập hay thoát.

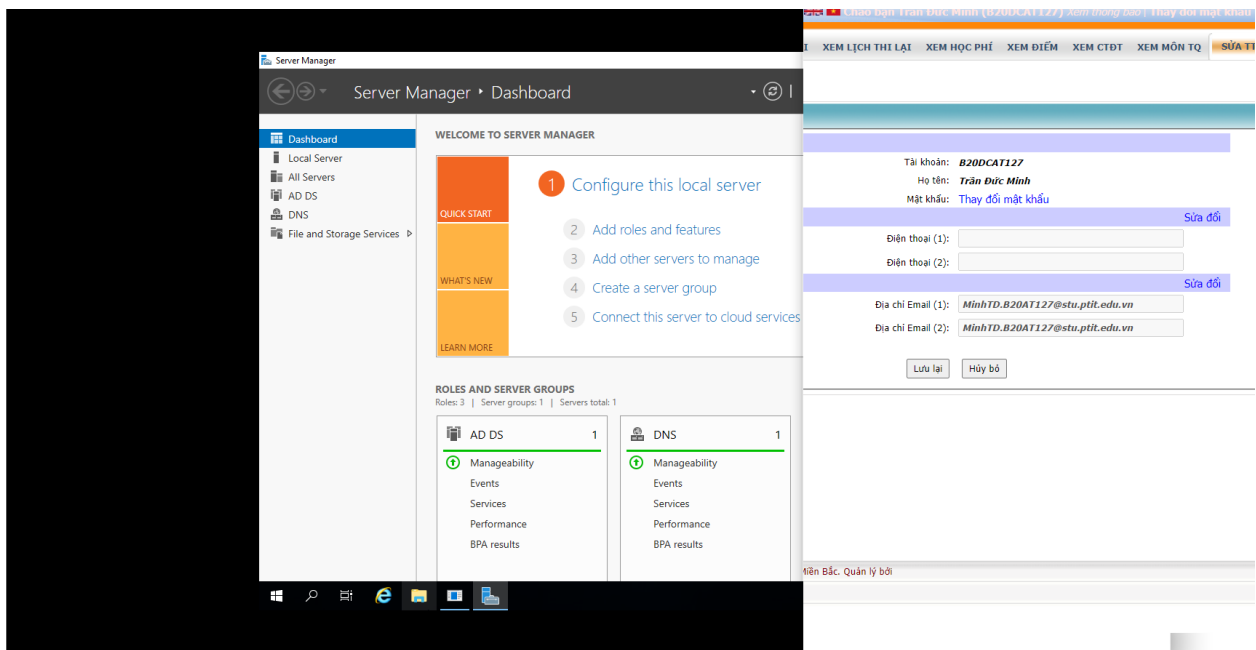
Cài đặt chuyển hướng thư mục (Folder redirection settings): Thư mục của người dùng trên mạng.

Chính sách nhóm có thể sử dụng trong máy tính cụ thể và có giá trị cục bộ dùng để xây dựng các chính sách giám sát việc hoạt động của máy tính như là xác định việc lưu các sự kiện an ninh trong “Event viewer”. Mặt khác, việc xác định người dùng hay nhóm người dùng có đặc quyền gì với máy tính cũng được thiết lập thông qua chính sách nhóm. Tương tự, quản trị hệ thống có thể áp dụng các biện pháp an ninh như cấm hay cho phép các cài đặt an ninh của máy tính, cụ thể thay đổi tên của tài khoản hay truy nhập vào ổ đĩa nhất định.

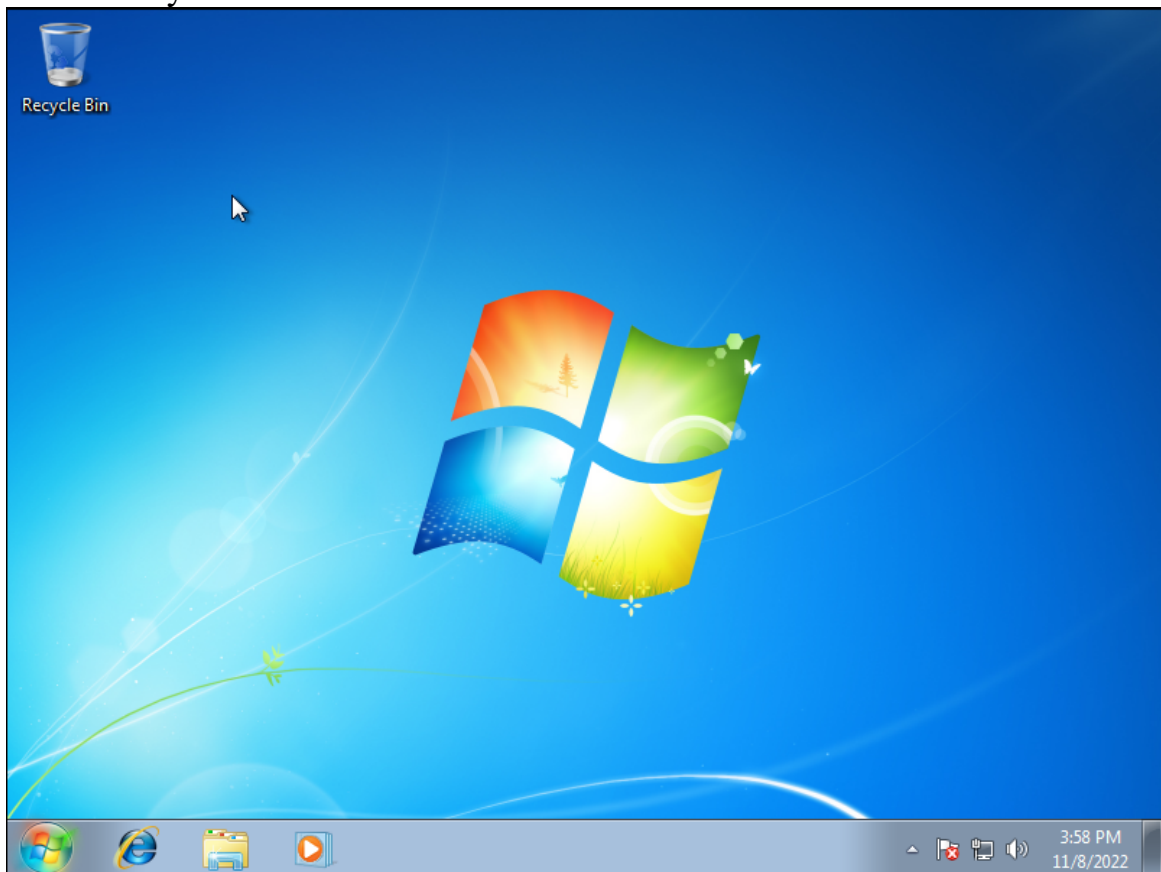
III. Các bước thực hiện

1. Chuẩn bị môi trường

- 1 máy Windows Server đã nâng cấp thành Domain Controller



- 1 máy Windows 7 làm client

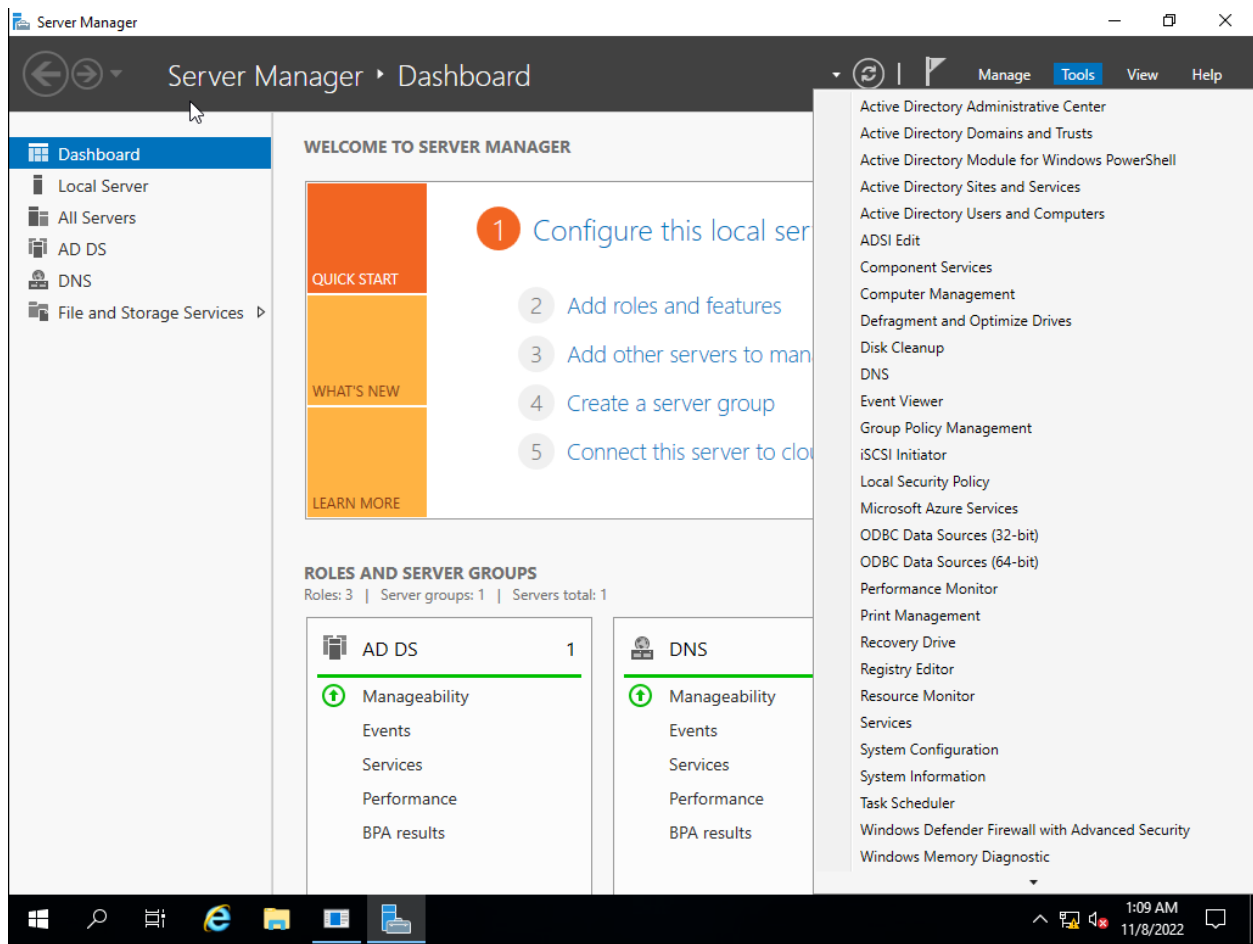


2. Các bước thực hiện

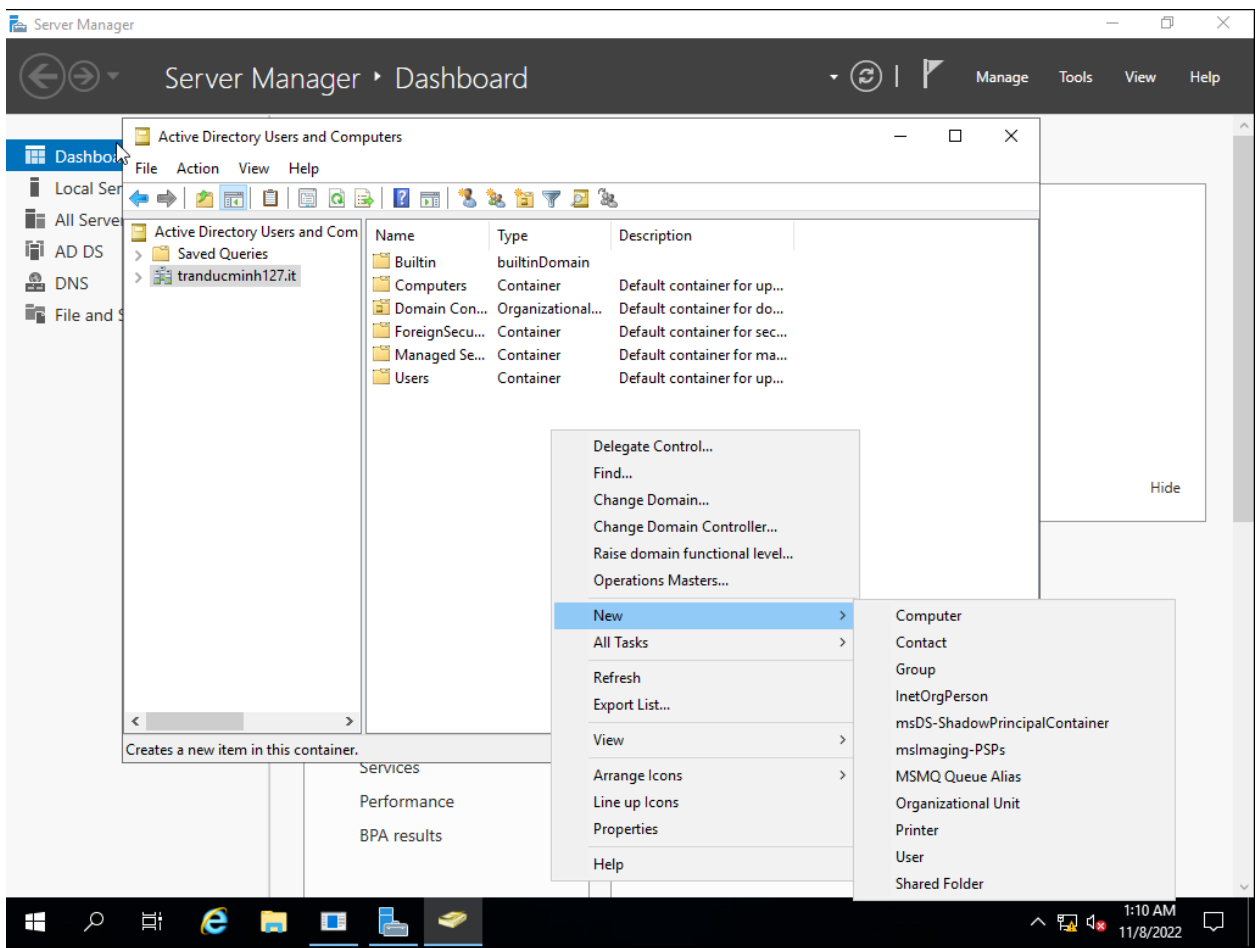
OU: được dùng trong việc quản lý tập trung các client thuộc cùng một domain.

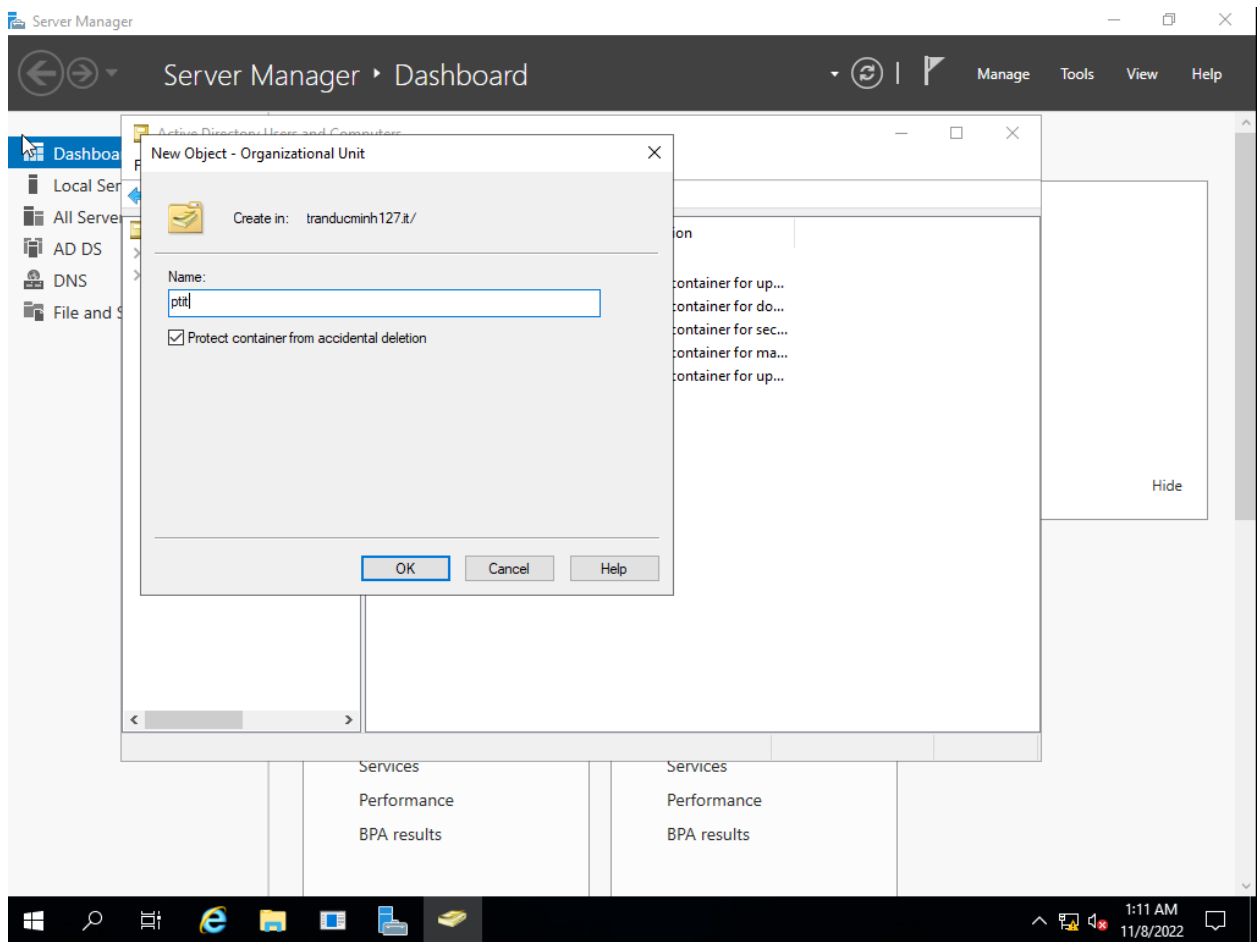
Tạo OU:

- Mở Server Manager chọn Tools



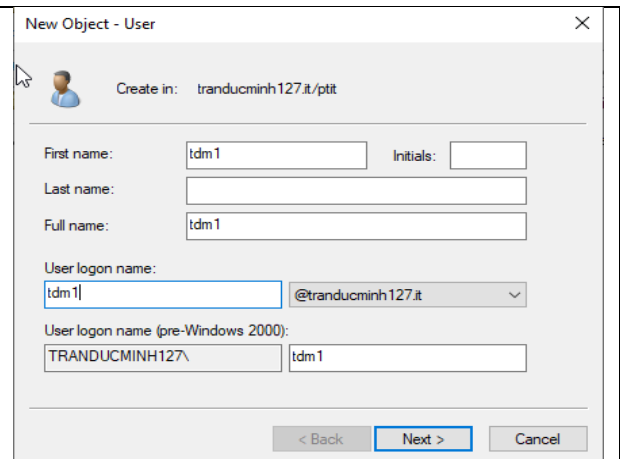
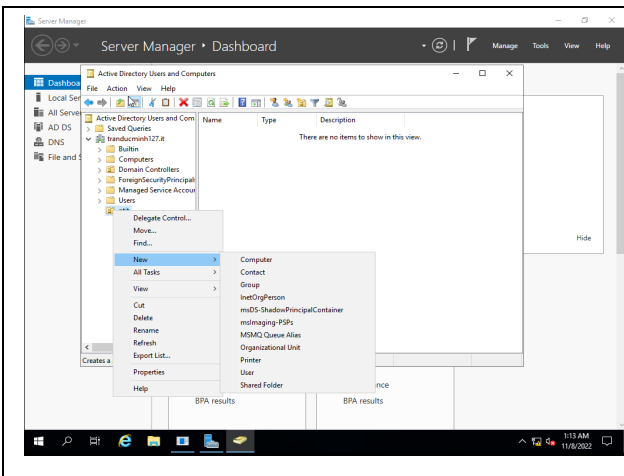
- Sau đó chọn Active Directory Users and Computers → tranducminh127.it, sau đó ấn chuột phải chọn New → Organizational Unit

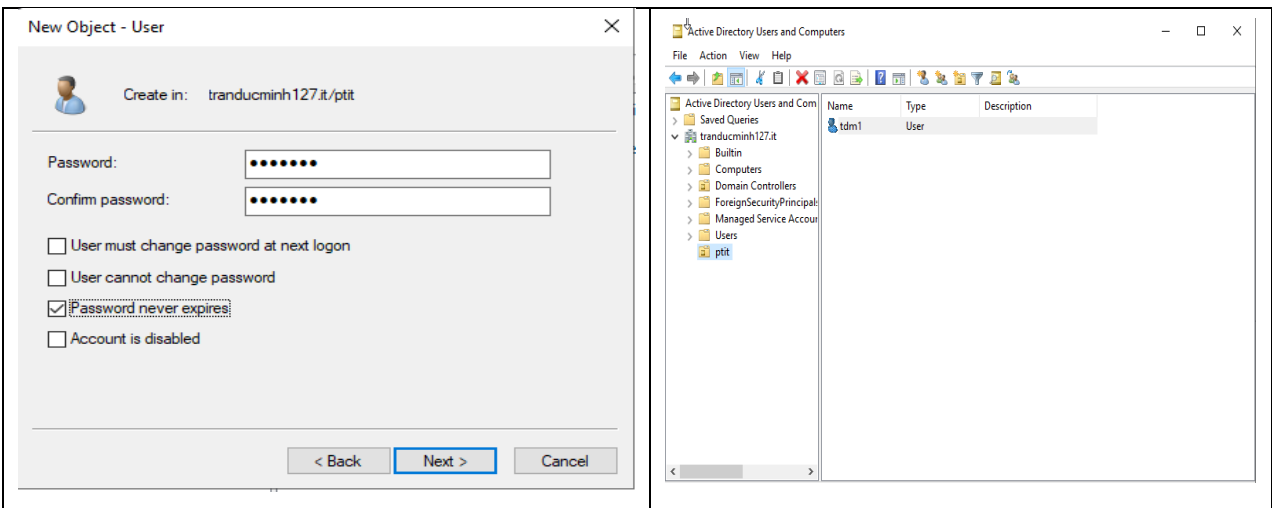




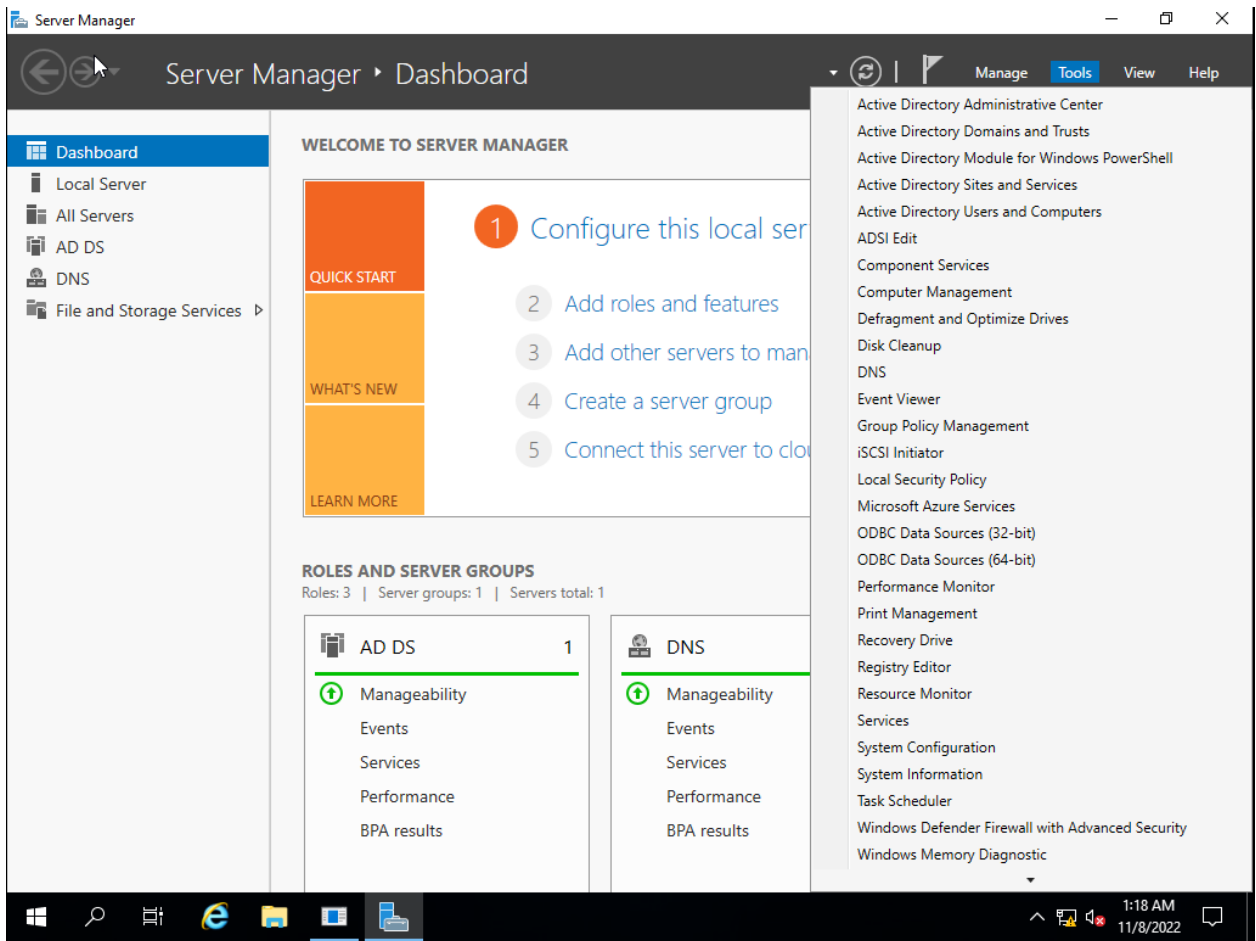
Tạo các user thuộc OU

- Tại OU ptit → chuột phải chọn New → User, Tạo user có tên là tdm1



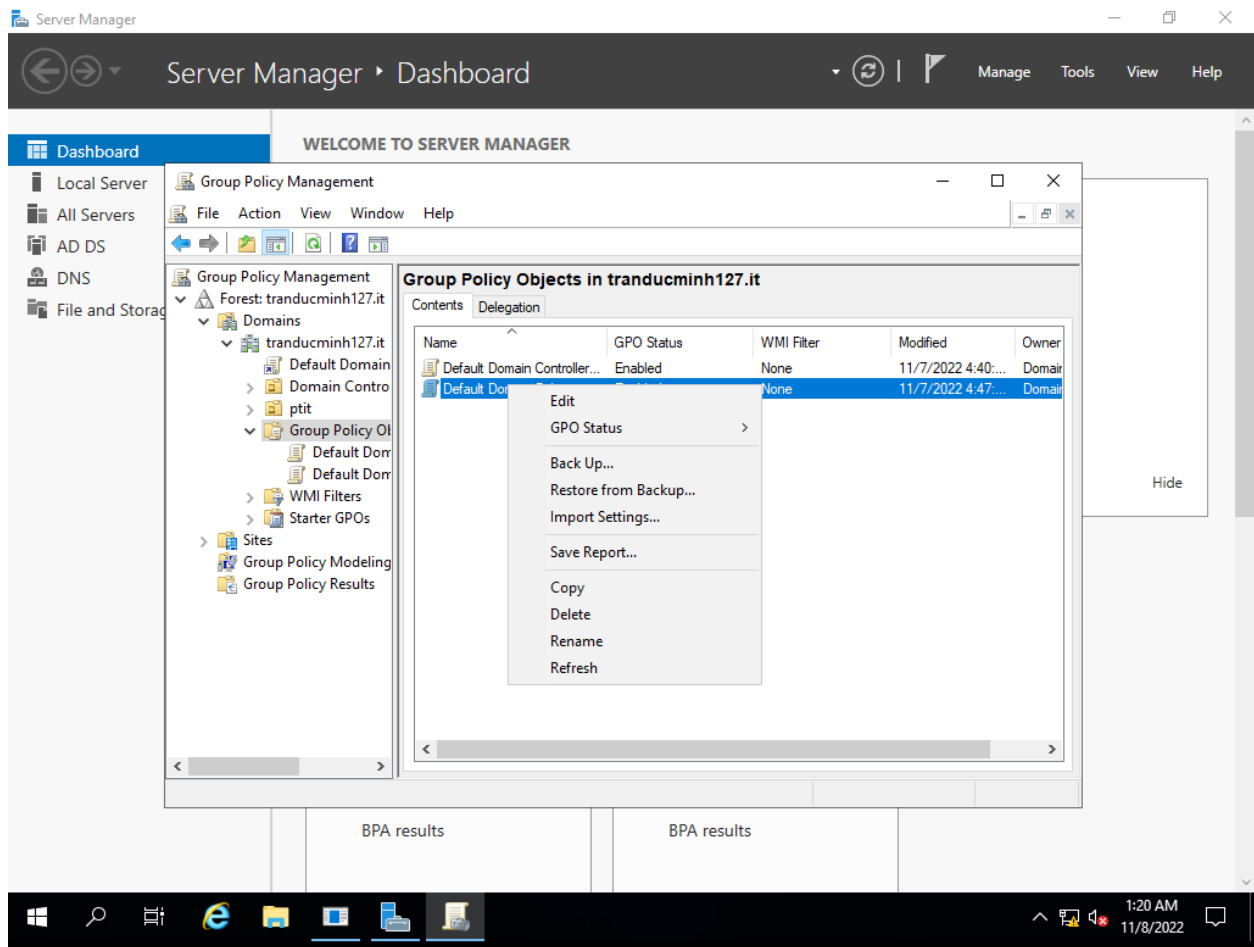


- **Thiết lập chính sách user và password**
 - Trong Server Manager vào Tools chọn Group Policy Management.



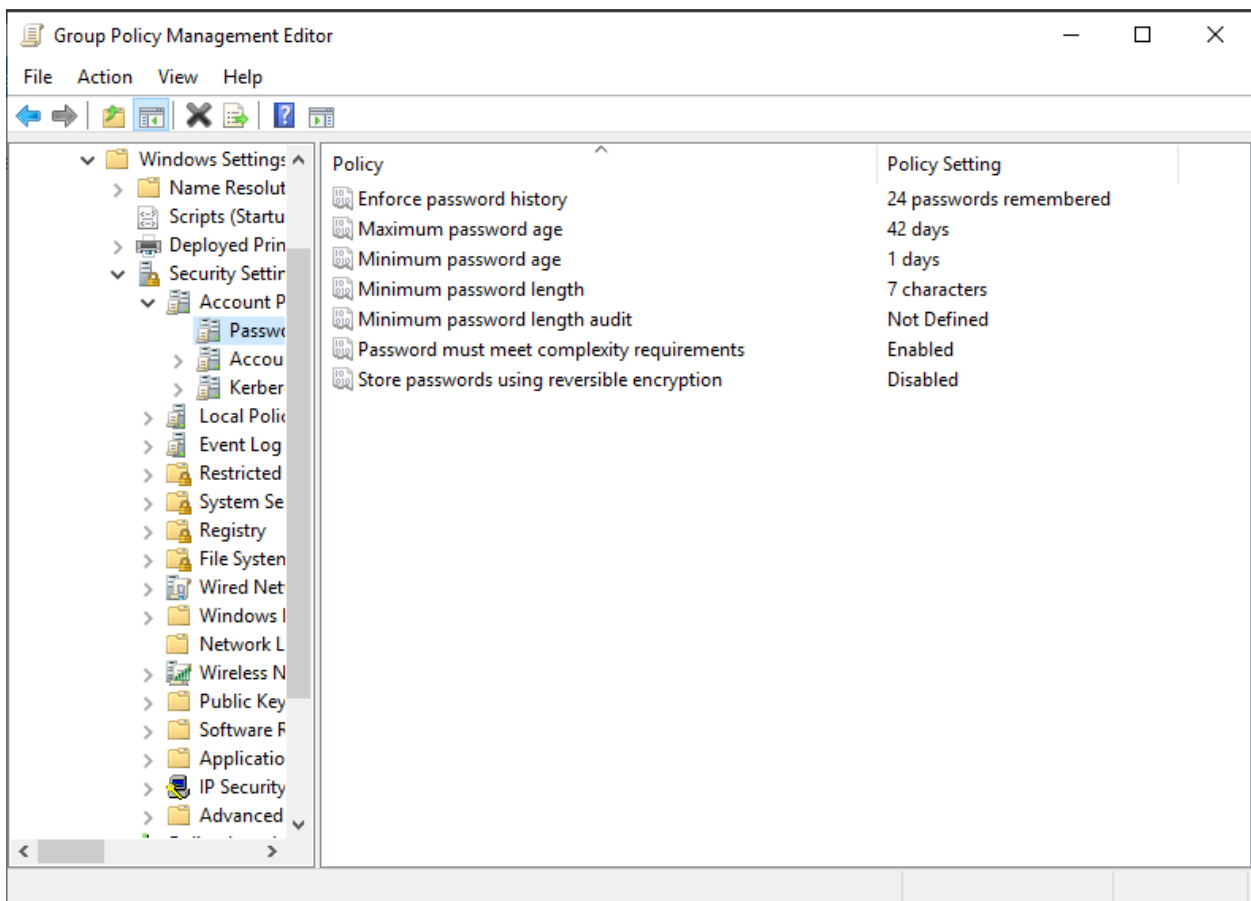
Chính sách password:

- Group Policy Management → Forest → Domains → tranducminh127.it → Group Policy Objects → Default Domain Policy → chuột phải chọn edit.



Tại Group Policy Management Editor:

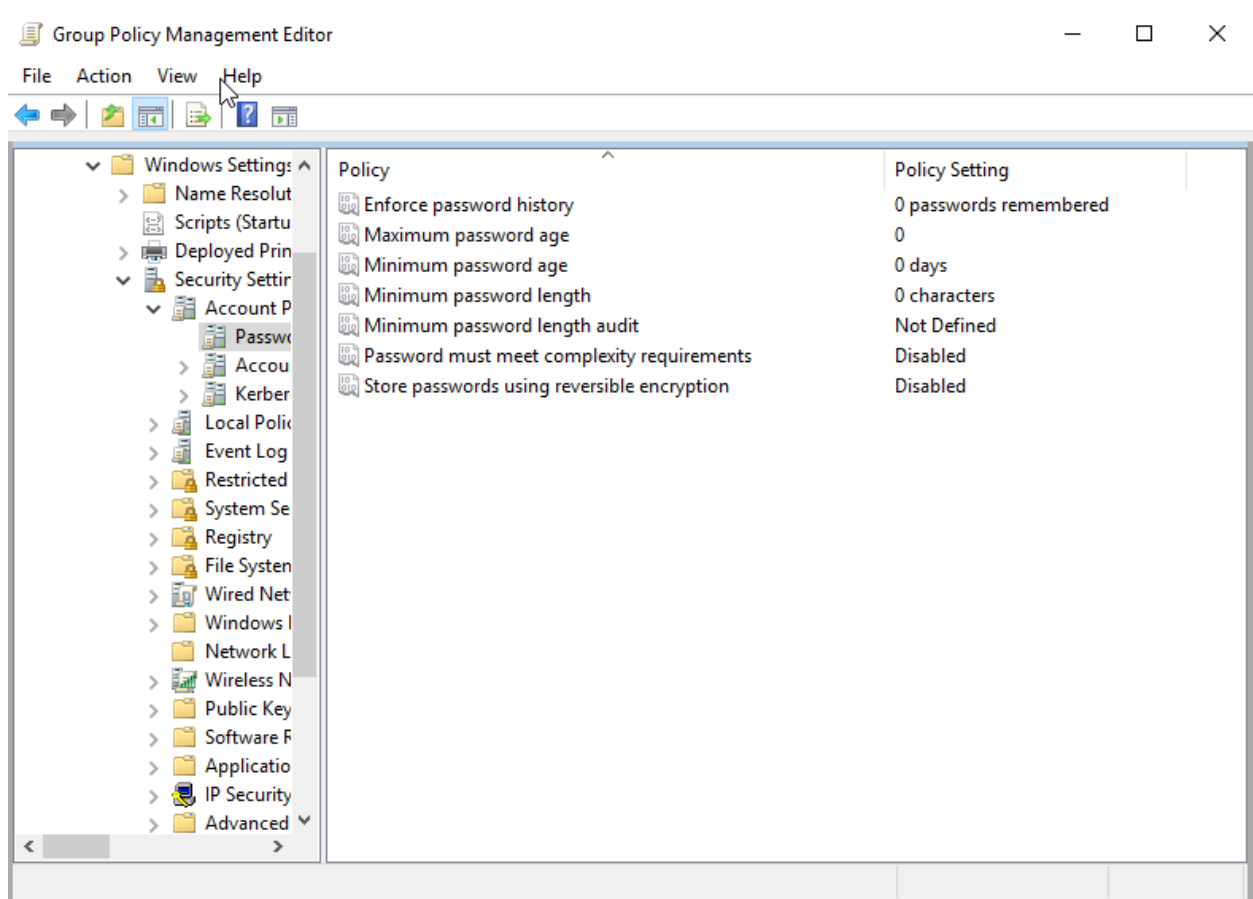
- Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy.



Trong đó:

- Enforce password history: số password hệ thống lưu trữ
- Maximum password age: thời gian có hiệu lực tối đa của một password
- Minimum password age: thời gian có hiệu lực tối thiểu của một password.
- Minimum password length: độ dài tối thiểu của một password
- Password must meet complexity requirements: yêu cầu password phức tạp.
- Store passwords using reversible encryption: độ mạnh của password.

Chỉnh password về dạng không phức tạp, giảm số lượng ký tự và giảm độ mạnh của password.



Lưu chính sách lại:

- cmd → gpupdate /force

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1999]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

Kết quả: tạo user trong OU ptit

New Object - User

Create in: tranducminh127.it/ptit

First name: tdm2 Initials:

Last name:

Full name: tdm2

User login name:
tdm2 @tranducminh127.it

User login name (pre-Windows 2000):
TRANDUCMINH127\ tdm2

< Back Next > Cancel

New Object - User

Create in: tranducminh127.it/ptit

Password:

Confirm password:

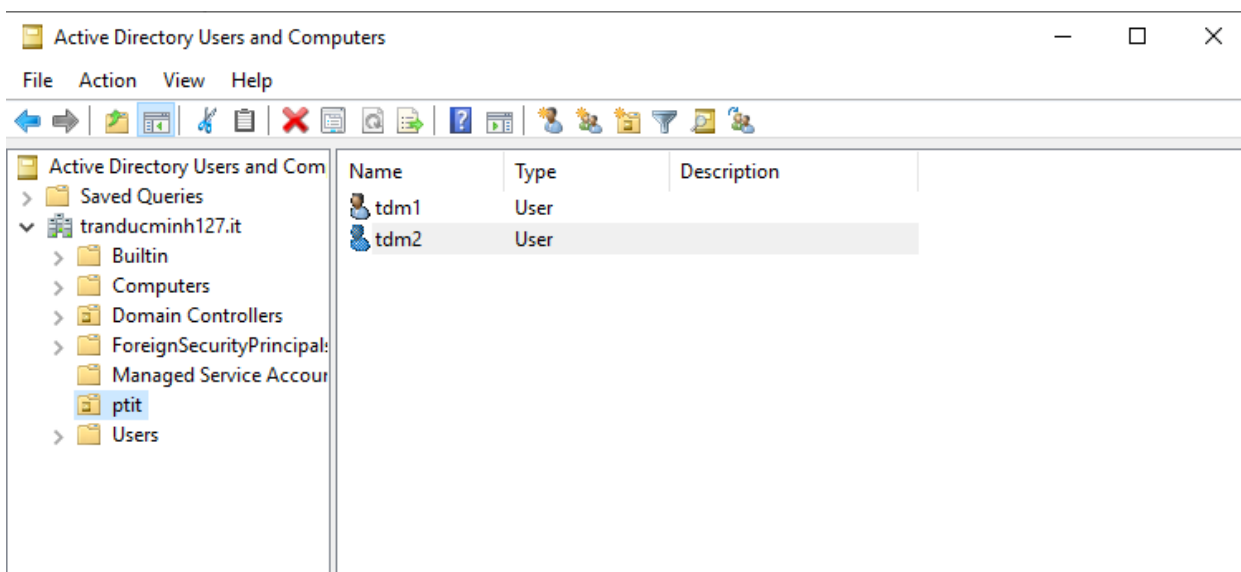
☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

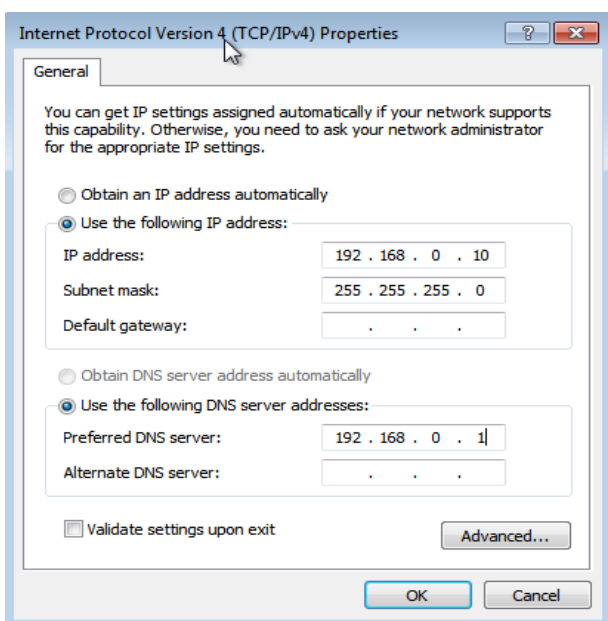
< Back Next > Cancel



- Phân quyền người dùng.

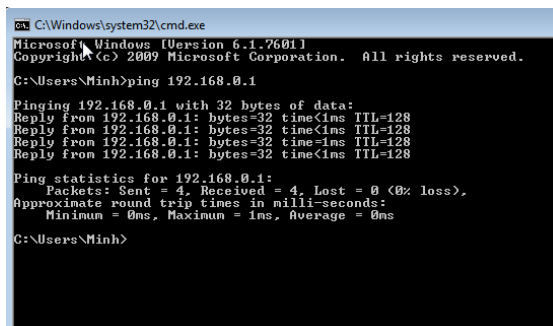
Dùng 1 máy Windows 7 làm máy client, cấu hình join domain để máy Windows 7 trở thành client.

Cấu hình địa chỉ IP cho máy Windows 7, với DNS là IP của máy Windows Server



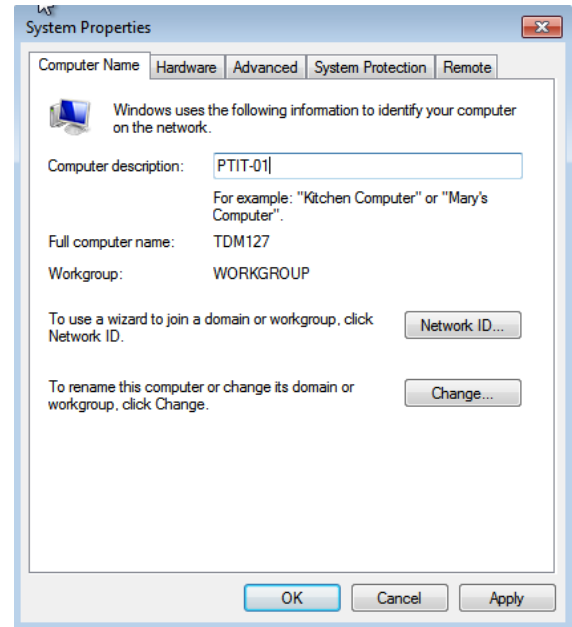
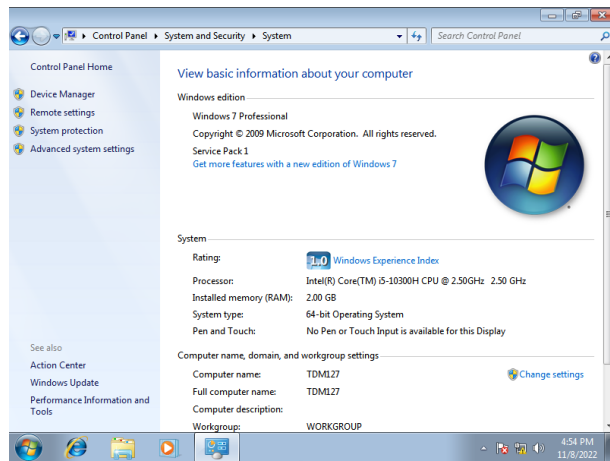
Tại Computer → chuột phải chọn

Kiểm tra sự thông nhau giữa 2 máy Windows 7 với Windows Server 2019

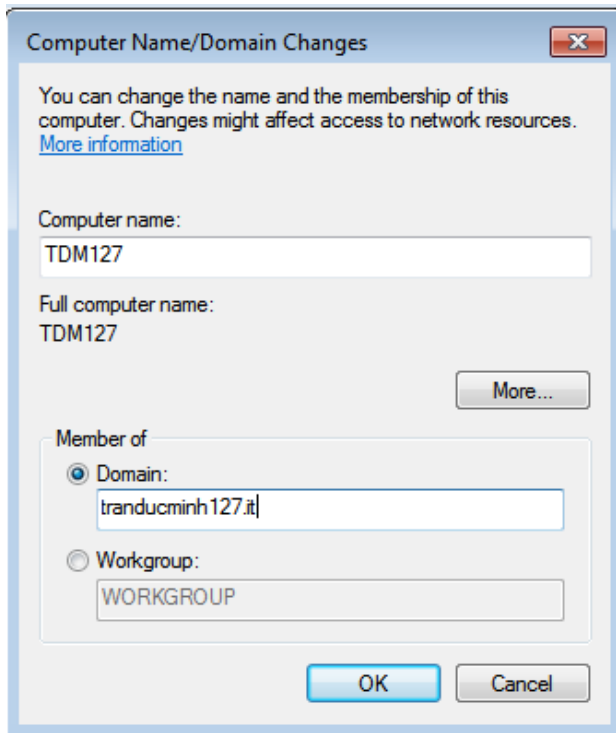


Tại tab Computer Name → change

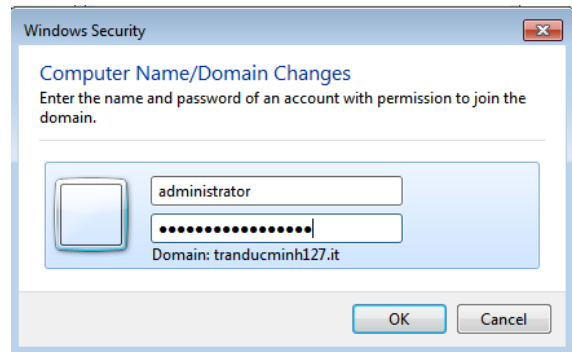
Properties → chọn Advanced system Settings

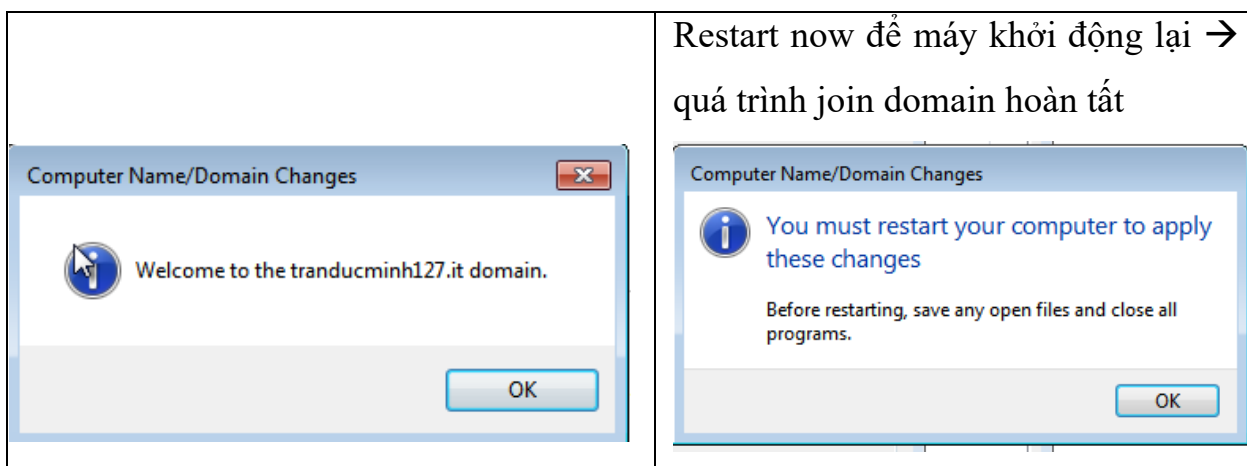


Tại Member of chọn Domain → nhập tên domain muốn join vào → click OK

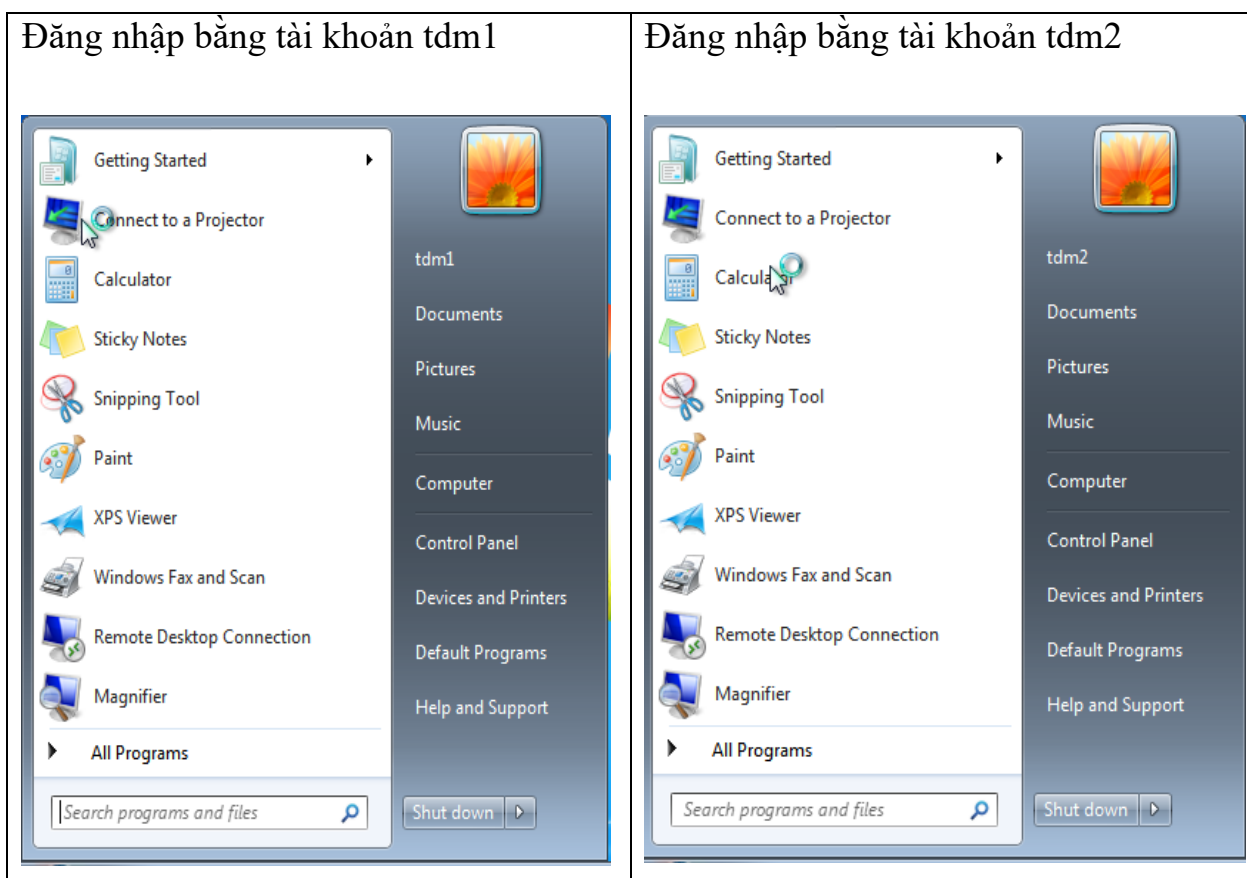


Nhập user và pass của máy domain
Windows Server 2019 → Click Ok





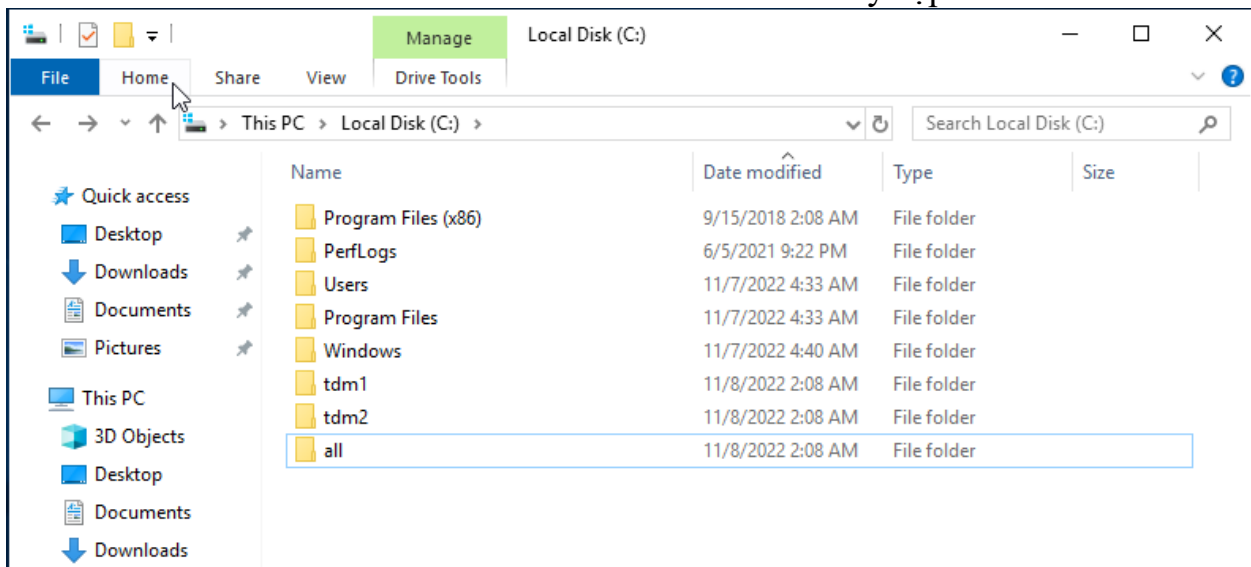
Đăng nhập máy Client bằng user tdm1 và user tdm2 đều được



Phân quyền đăng nhập

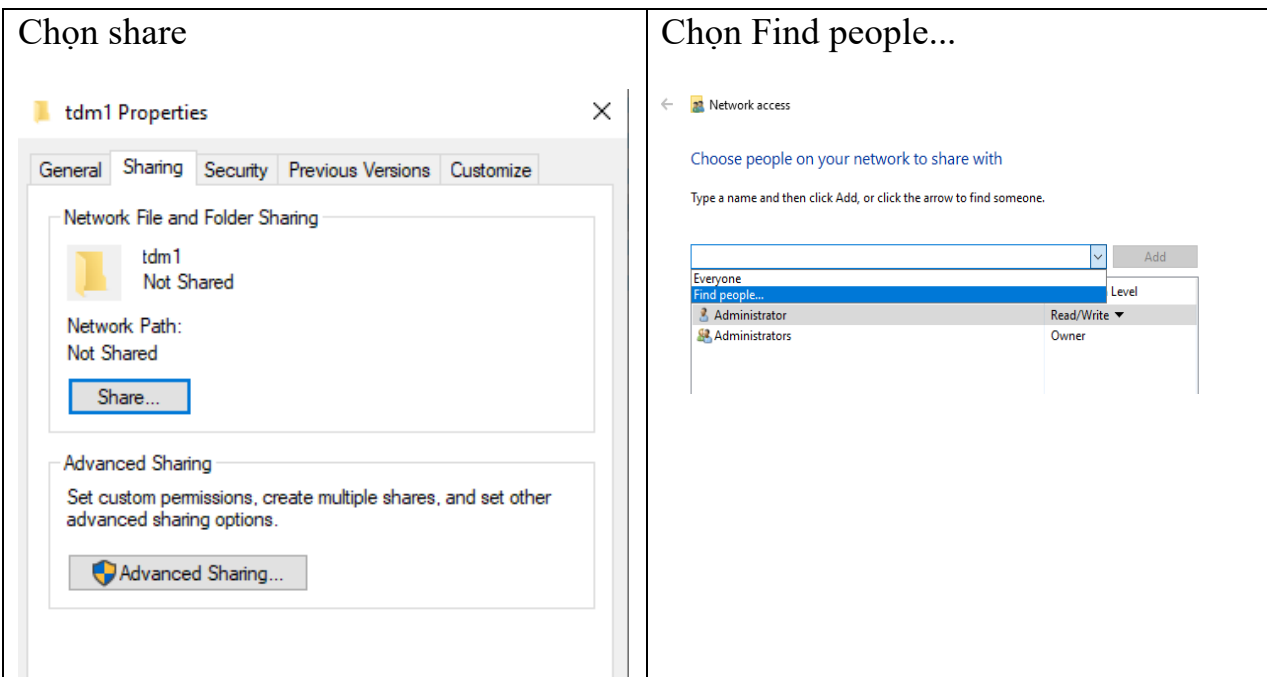
- Tại máy Windows server tạo 3 folder tdm1, tdm2, all
 - o Folder tdm1 chỉ cho user tdm1 truy cập

- Folder tdm2 chỉ cho user tdm2 truy cập
- Folder all cho cả 2 users tdm1 và tdm2 truy cập

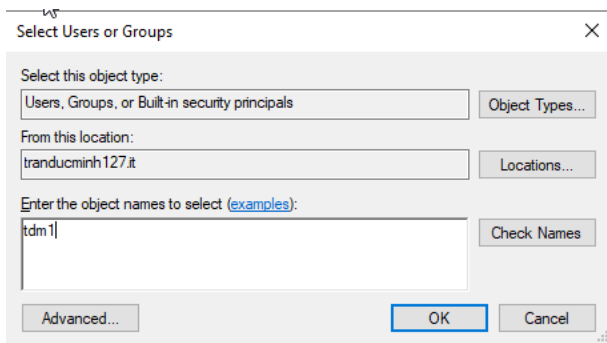


Chia sẻ folder tdm1, và phân quyền chỉ cho user tdm1 được truy cập:

- Ấn chuột phải vào folder tdm1 chọn properties → sharing



Nhập ô check names: tdm1

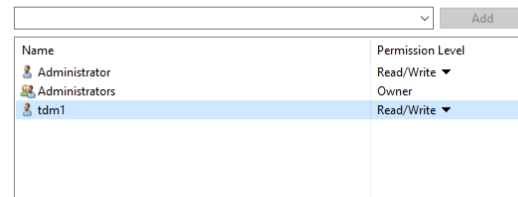


Sau khi tìm ra tài khoản tdm1

→ ấn share → ấn done.

[Choose people on your network to share with](#)

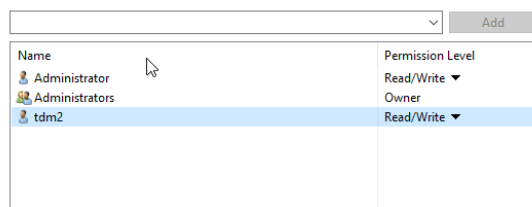
Type a name and then click Add, or click the arrow to find someone.



Tương tự cho folder tdm2

[Choose people on your network to share with](#)

Type a name and then click Add, or click the arrow to find someone.



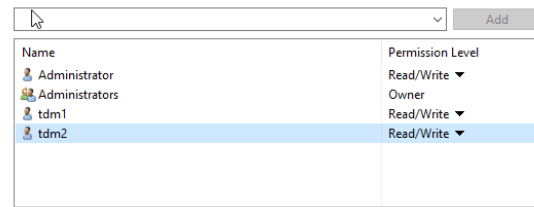
[I'm having trouble sharing](#)

[Share](#) [Cancel](#)

Tương tự cho folder all

[Choose people on your network to share with](#)

Type a name and then click Add, or click the arrow to find someone.

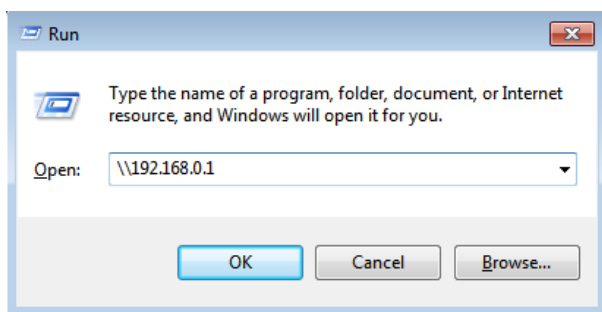


[I'm having trouble sharing](#)

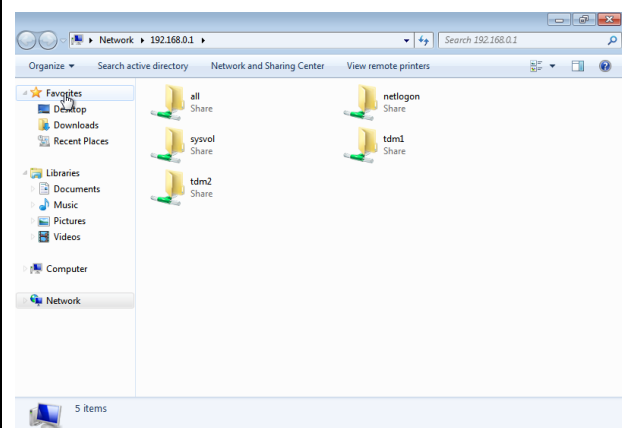
[Share](#) [Cancel](#)

Kiểm tra:

Đăng nhập máy windows 7 bằng user tdm1. Truy nhập vào máy Windows Server

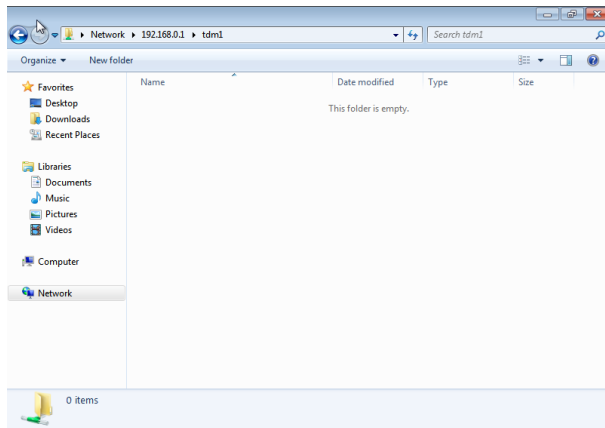


Thấy cả 3 folder được chia sẻ là tdm1, tdm2, all

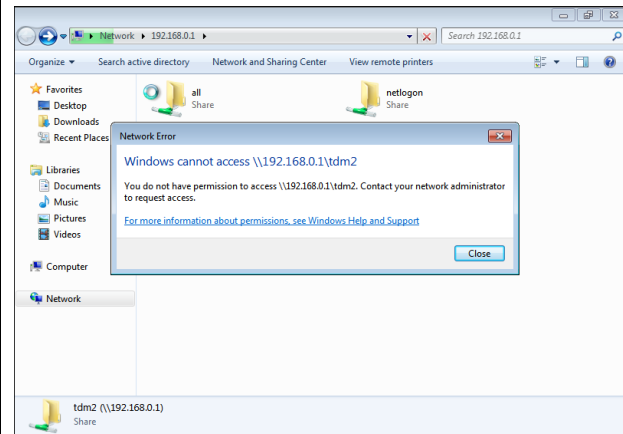


User tdm1 truy cập vào folder tdm1

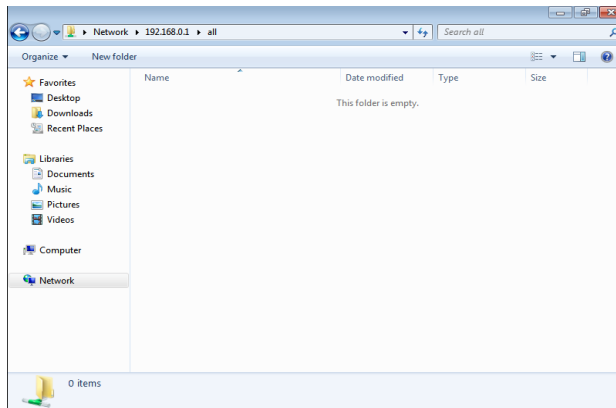
=> ok



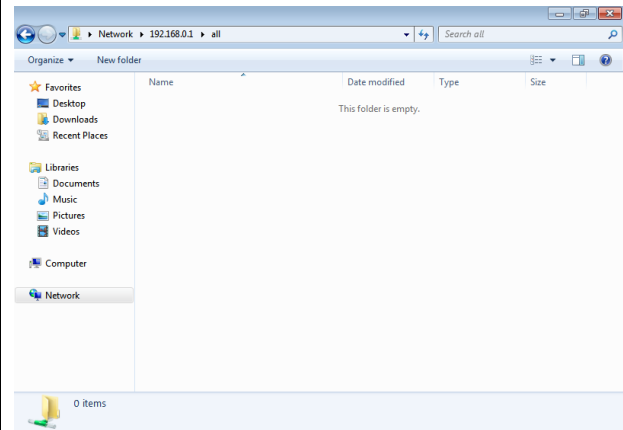
User tdm1 không truy cập được vào folder tdm2



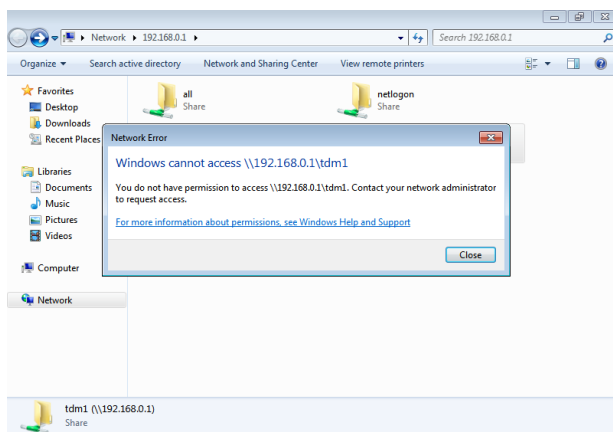
User tdm1 truy cập vào folder all => ok



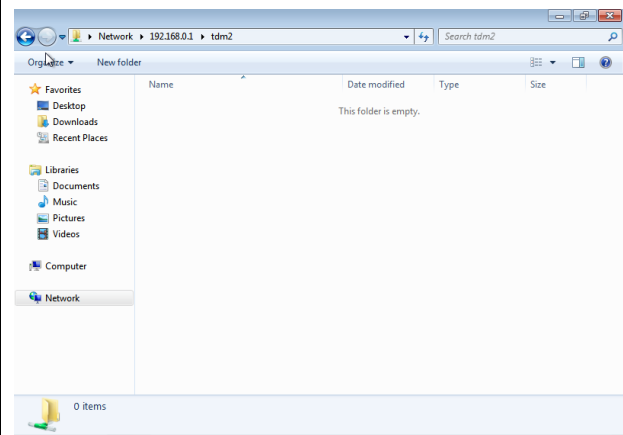
User tdm2 truy cập vào folder all => ok



User tdm2 không truy cập được vào folder tdm1

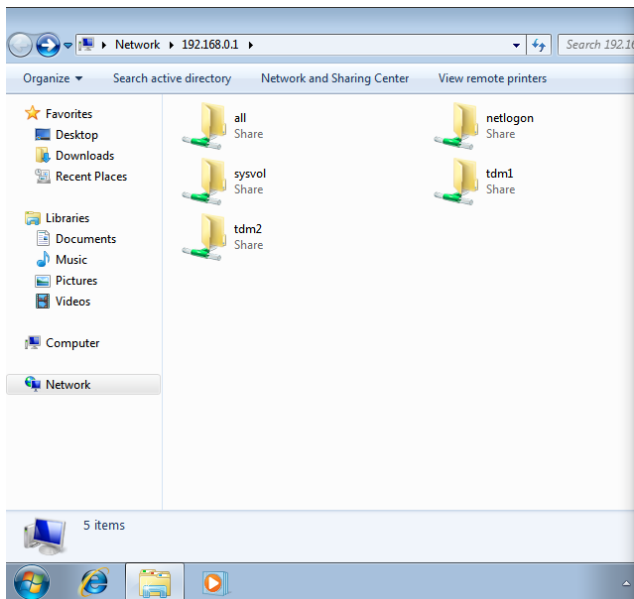


User tdm2 truy cập vào folder tdm2 => ok



III. Kết quả

- Tạo, phân quyền thành công OU, users và chia sẻ thành công tài nguyên.



Tài khoản:	B20DCAT127
Họ tên:	Trần Đức Minh
Mật khẩu:	Thay đổi mật khẩu
	Sửa đổi
Điện thoại (1):	<input type="text"/>
Điện thoại (2):	<input type="text"/>
	Sửa đổi
Địa chỉ Email (1):	<input type="text" value="MinhTD.B20AT127@stu.ptit.edu.vn"/>
Địa chỉ Email (2):	<input type="text" value="MinhTD.B20AT127@stu.ptit.edu.vn"/>
	<input type="button" value="Lưu lại"/> <input type="button" value="Hủy bỏ"/>