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

BÁO CÁO THỰC HÀNH

BÀI 2: QUẢN TRỊ ACTIVE DIRECTORY TRONG WINDOWS SERVER

Họ và tên: Vũ Thành Long

Mã sinh viên: B21DCAT012

Nhóm: 01

Môn học: Hệ điều hành Windows và Linux/Unix

Giảng viên giảng dạy: Đinh Trường Duy

Bài 2: Quản trị Active Directory trong Windows Server

1 GIỚI THIỆU BÀI THỰC HÀNH

1.1 Mục đích

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

1.2 Yêu cầu

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

1.3 Nhóm thực hành

- ✓ 1 sinh viên.

2 CƠ SỞ LÝ THUYẾT

• Các dịch vụ trong windows server

• Xác thực thư mục động (Active Directory Certificate Services): Dịch vụ tạo và quản lý chứng thực khóa công khai cho hệ thống an ninh dùng công nghệ khóa công khai.

• Miền thư mục động (Active Directory Domain Services): Lưu thông tin về người quản trị, máy tính và các thiết bị khác trong mạng. Ngoài ra, dịch vụ này giúp người quản trị quản lý các thông tin trên an toàn và làm thuận tiện cho việc chia sẻ và phối hợp giữa các người quản trị.

- Liên kết thư mục động (Active Directory Federation Services): Hỗ trợ công nghệ đăng nhập một lần trên Web bằng cách liên kết hay chia sẻ một cách an toàn định danh người dùng, quyền truy nhập giữa các tổ chức với nhau.

- Thư mục động rút gọn (Active Directory Lightweight Directory Services):Dùng để lưu dữ liệu mà không cần dịch vụ miền thư mục động.

- Quản lý quyền thư mục động (Active Directory Rights Management Services):Công nghệ bảo vệ thông tin cho phép các ứng dụng bảo mật thông tin khỏi việc sử dụng trái phép.

• Máy chủ ứng dụng (Application Server): Cung cấp giả pháp hoàn chỉnh cho việc cài đặt và quản lý các ứng dụng doanh nghiệp phân tán: .Net, Web,Message Queuing, COM+... - Quản lý DHCP (Dynamic Host Configuration Protocol): Cho phép máy chủ tự động cấp phát địa chỉ Internet cho các máy tính và thiết bị dùng DHCP và tự động hóa cấu hình (địa chỉ DNS, gateway) các máy tính và thiết bị.

- Tên miền DNS (Domain Name System): Phương pháp tiêu chuẩn liên kết các tên và địa chỉ Internet.

- Dịch vụ file: Cung cấp công nghệ cho việc quản lý lưu trữ, sao lưu, tên miền, tìm kiếm nhanh và truy nhập của người quản trị.

- Dịch vụ ảo hóa Hyper-V: Cho phép tạo và quản lý máy ảo và tài nguyên. Trong đó, mỗi máy ảo cung cấp môi trường thực thi riêng biệt giúp chạy nhiều hệ điều hành đồng thời.

- Truy nhập và chính sách mạng (Network Policy and Access Services): Cho phép người dùng kết nối cục bộ hay từ xa, kết nối các mạng, cho phép quản lý truy nhập tập trung cũng như chính sách cho máy khách. - In ấn tài liệu (Print and Document Services):Giúp quản trị máy in một cách tập trung và cho phép chia sẻ máy in với các người dung trong mạng.

- Dịch vụ đầu cuối (Terminal Services): Cho phép người dùng truy nhập các ứng dụng Windows cài trên máy chủ đầu cuối. Người dùng có thể kết nối tới máychủ đầu cuối để chạy và sử dụng tài nguyên mạng.

- Web (Internet Information Services-IIS): Cho phép chia sẻ thông tin trên mạng Internet và Intranet

• Người dùng và truy nhập

• Để sử dụng được máy tính sử dụng hệ điều hành Microsoft Windows, mỗi một người dùng cần phải có tài khoản riêng còn 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 truy 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 (Active directoryministrator) và khách (Guest). Ngoài ra, các người dùng có vai trò vàyêu 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.

• Tổng quan về Active Directory trên Windows Server

• Active Directory (ACTIVE DIRECTORY) là một kiến trúc độc quyền của Microsoft. Đây là một kiến trúc không thể thiếu được trên Windows Server, được hiểu nôm na là một dịch vụ thư mục. Active Directory là một hệ thống được chuẩn hóa với khả năng quản trị tập trung hoàn hảo về người dùng cũng như các nguồn tài nguyên trong một hệ thống mạng. Active Directory được sử dụng trong mô hình mạng “Server - Client”.

• Active Directory Objects Dữ liệu trong Active Directory như là thông tin users, máy in, server, database, groups, computers và security policies được tổ chức như các objects (đối tượng). Mỗi object có những thuộc tính riêng đặc trưng cho object đó, ví dụ như object user có các thuộc tính liên quan như First Name, Last Name, Logon Name, ... và Computer Object có các thuộc tính như computer name cùng description.

• Active Directory Components

• Trong mô hình mạng doanh nghiệp, các components của Active Directory được sử dụng, áp dụng để xây dựng nên các mô hình phù hợp với nhu cầu các doanh nghiệp. Xét về khía cạnh mô hình kiến trúc của ACTIVE DIRECTORY thì ta phân làm 2 loại làPhysical và Logical.

* Logical Structure: Trong ACTIVE DIRECTORY, việc tổ chức tài nguyên theo cơ chế Logical Structure, được ánh xạ thông qua mô hình domains, OUs, trees và forest. Nhóm các tài nguyên được tổ chức một cách luận lí cho phép bạn dễ dàng truy xuất đến tài nguyên hơn là phải nhớ cụ thể vị trí vật lí của nó.

+Domain: Cốt lõi của kiến trúc tổ chức luận lí trong ACTIVE DIRECTORY chính là Domain, nơi lưu trữ hàng triệu đối tượng (objects). Tất cả các đối tượng trong hệ thống

mạng trong một domain thì do chính domain đó lưu trữ thông tin của các đối tượng. Active Directory được kiến tạo bởi một hay nhiều domain và một domain có thể triển khai trên nhiều physical structure.

+OUs: OU là một container được dùng để tổ chức các đối tượng trong một domain thành các nhóm quản trị luận lí (logical). OUs cung cấp phương tiện thực hiện các tác vụ quản trị trong hệ thống như là quản trị user và resources, đó là những scope đối tượng nhỏ nhất mà bạn có thể ủy quyền xác thực quản trị. OUs bao gồm nhiều đối tượng khác như là user accounts, groups, computers và các OUs khác tạo nên các cây OUs trong cùng một domain. Các cây OUs trong một domain độc lập với kiến trúc các cây Ous thuộc các domain khác

+Trees: Trees là một nhóm các domain được tổ chức theo cấu trúc hình cây với mô hình parent-child ánh xạ từ thực tế tổ chức của doanh nghiệp, tổ chức.

+Forests: Forest là một thuật ngữ được đặt ra nhằm định nghĩa 1 mô hình tổ chức của ACTIVE DIRECTORY, 1 forest gồm nhiều domain trees có quan hệ với nhau, các domain trees trong forest là độc lập với nhau về tổ chức, nghe ra có vẻ mâu thuẫn trong mối quan hệ nhưng ta sẽ dễ hiểu hơn khi mối quan hệ giữa các domain trees là quan hệTrust 2 chiều như các partners với nhau.

*Physical Structure:

- Xét về khía cạnh physical component của AD sẽ gồm 2 phần là Sites và Domain Controllers. Tùy thuộc vào mô hình tổ chức của công ty, người quản trị sẽ phải dùng các components này để thiết kế sao cho phù hợp.

- Sites: Site là một thuật ngữ được dùng đến khi nói về vị trí địa lý của các domain trong hệ thống. Khi hệ thống các domain được phân tán ở những vị trí địa lý, những nơi khác nhau và có quan hệ với nhau thì những nơi đặt các domain

- Domain Controllers: Domain Controller (DC) là 1 máy tính hay server chuyên dụng được setup Windows Server và lưu trữ bản sao của Domain Directory (local domain database). Một domain có thể có 1 hay nhiều domain controller, mỗi domain controller đều có bản sao dữ liệu của Domain Directory. Domain Controller chịu trách nhiệm chứng thực cho users và chịu trách nhiệm đảm bảo các chính sách bảo mật được thực thi. Các chức năng chính của Domain Controller: Mỗi domain controller lưu trữ các bản sao

thông tin của Active Directory cho chính domain đó, chịu trách nhiệm quản lí thông tin và tiến hành đồng bộ dữ liệu với các domain controller khác trong cùng một domain.

+ Domain Controller trong một domain có khả năng tự động đồng bộ dữ liệu với các DC khác trong cùng một domain. Khi bạn thực hiện một tác vụ đối với thông tin lưu trữ trên DC, thì thông tin này sẽ tự động được đồng bộ hóa đến các DC khác. Tuy nhiên để đảm bảo sự ổn định cho hệ thống mạng, chúng ta cần phải có một chính sách hợp lí cho các domain trong việc đồng bộ hóa thông tin dữ liệu với một thời điểm phù hợp.

+ Domain Controller tự động đồng bộ hóa ngay lập tức các thay đổi quan trọng đối với cả domain như disable một user account.

+ Active Directory sử dụng việc đồng bộ hóa dữ liệu theo cơ chế multimaster, nghĩa là không có domain controller nào đóng vai trò là master cả, mà thay vào đó thì tất cả domain controller đều ngang hàng với nhau, mỗi domain controller lưu trữ một bản sao của database hệ thống. Các domain controller lưu trữ các thông tin dữ liệu khác nhau trong một khoảng thời gian ngắn cho đến khi thông tin các domain controller trong hệ thống đều được đồng bộ với nhau, hay nói cách khác là thống nhất dữ liệu cho toàn domain.

+ Mặc dù là Active Directory hỗ trợ hoàn toàn việc đồng bộ dữ liệu theo cơ chế multimaster nhưng thực tế thì không phải lúc nào cũng theo cơ chế này (việc thực thi không được cho phép ở nhiều nơi trong hệ thống mạng trong cùng một thời điểm).Operations master roles là các roles đặc biệt được assigned với 1 hoặc nhiều domain controllers khác để thực hiện đồng bộ theo cơ chế single-master, ta có thể dễ dàng nhận thấy việc thực thi operations của multimaster là sự thực thi của nhiều singlemaster đồng thời.

+ Hệ thống có nhiều hơn một domain hỗ trợ trong trường hợp dự phòng backup domain controller, khi một domain controller có vấn đề xảy ra thì các domain sẽ tự động chạy dự phòng, đảm bảo hệ thống luôn được ổn định.

+ Domain Controller quản lí các vấn đề trong việc tương tác với domain của users, ví dụ xác định đối tượng trong Active Directory hay xác thực việc logon của user.

3 NỘI DUNG THỰC HÀNH

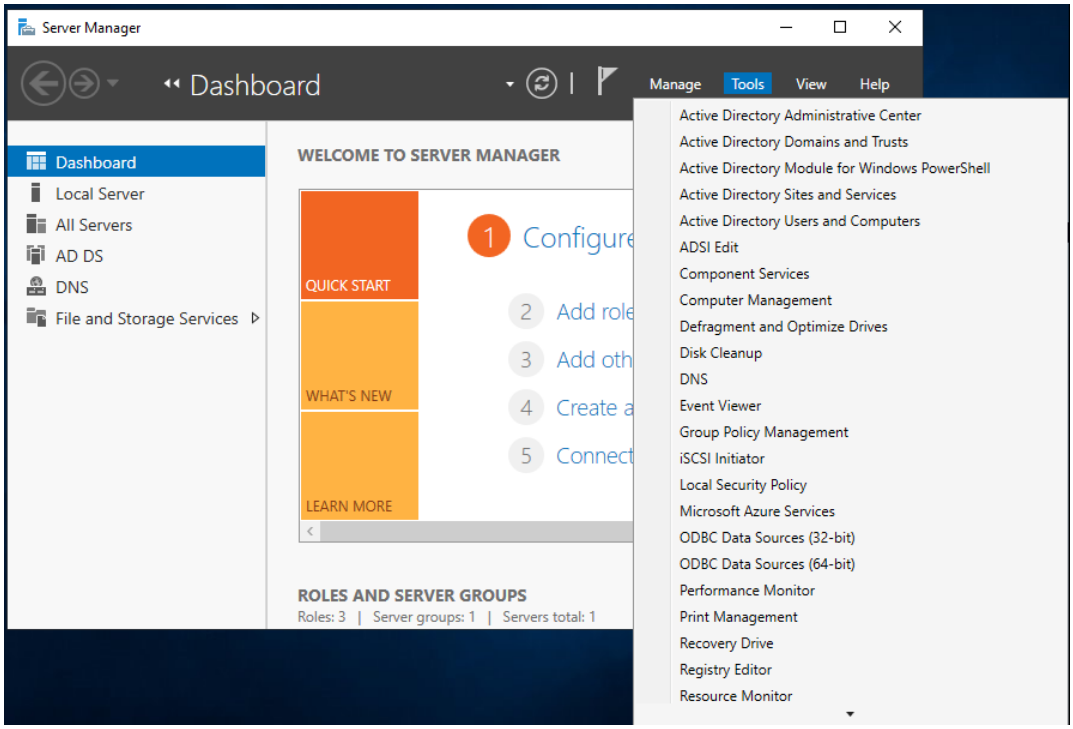
3.1 Chuẩn bị môi trường

- ✓ 1 máy Windows Server đã nâng cấp thành Domain Controller
- ✓ 1 máy Windows 7 làm client

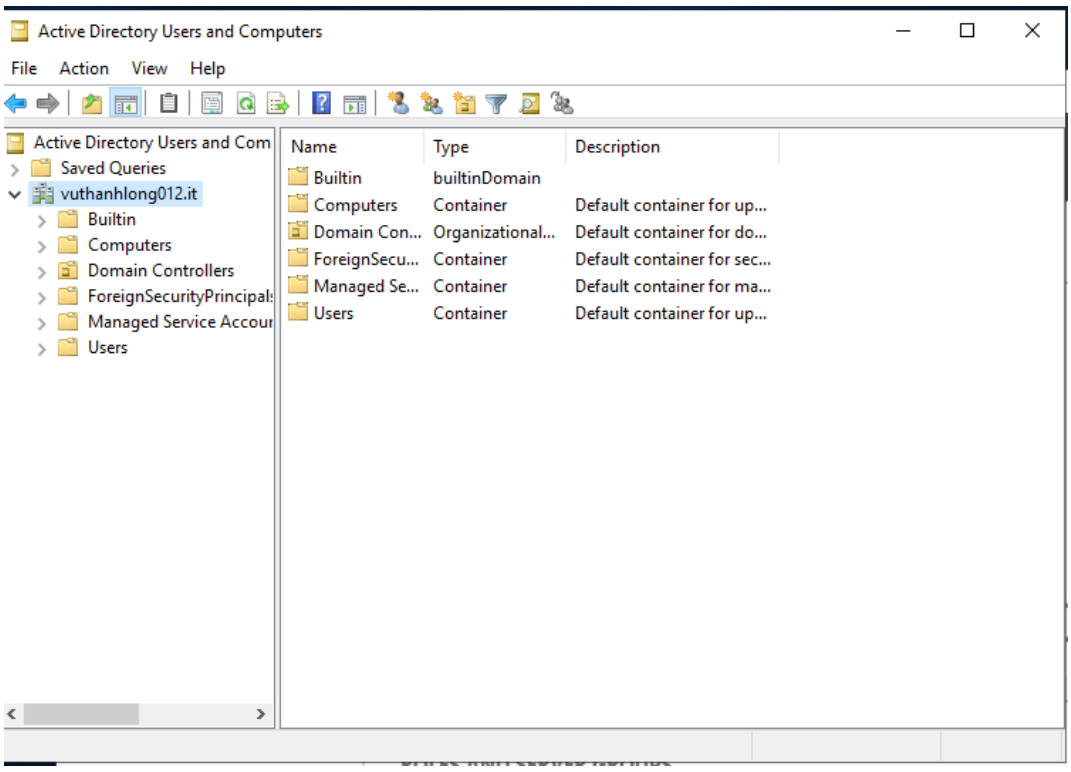
3.2 Các bước thực hiện

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

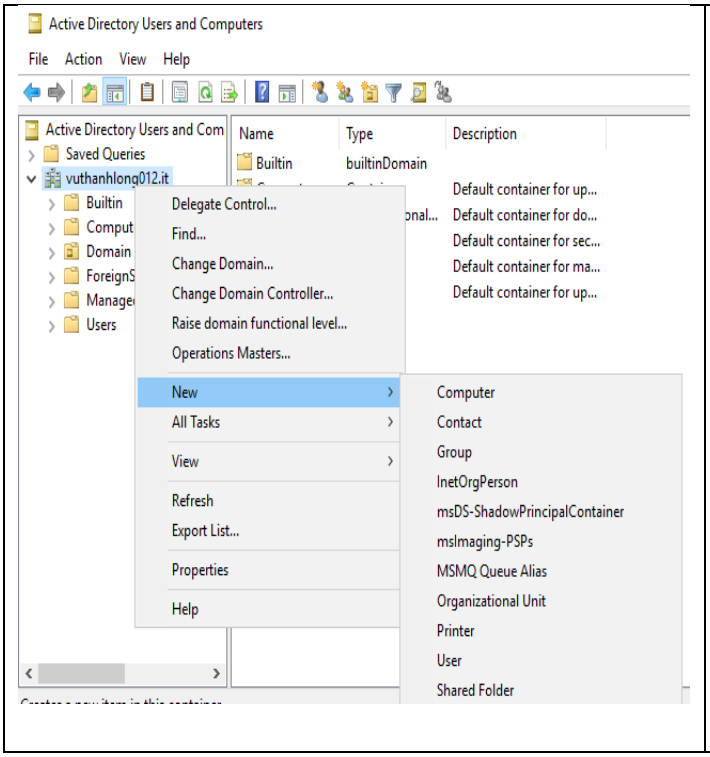
Mở Server Manager chọn Tools

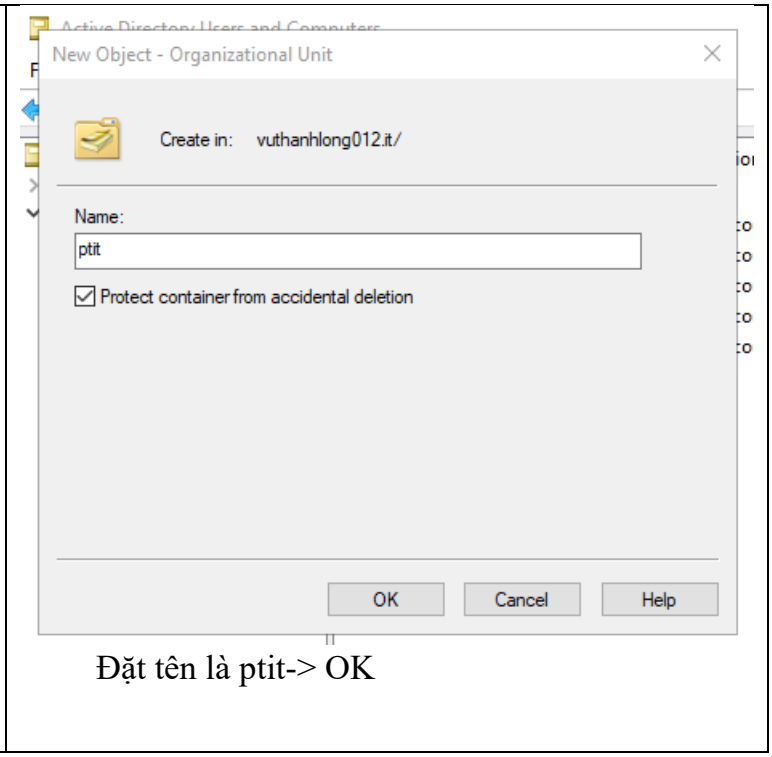


Sau đó chọn Active Directory Users and Computers



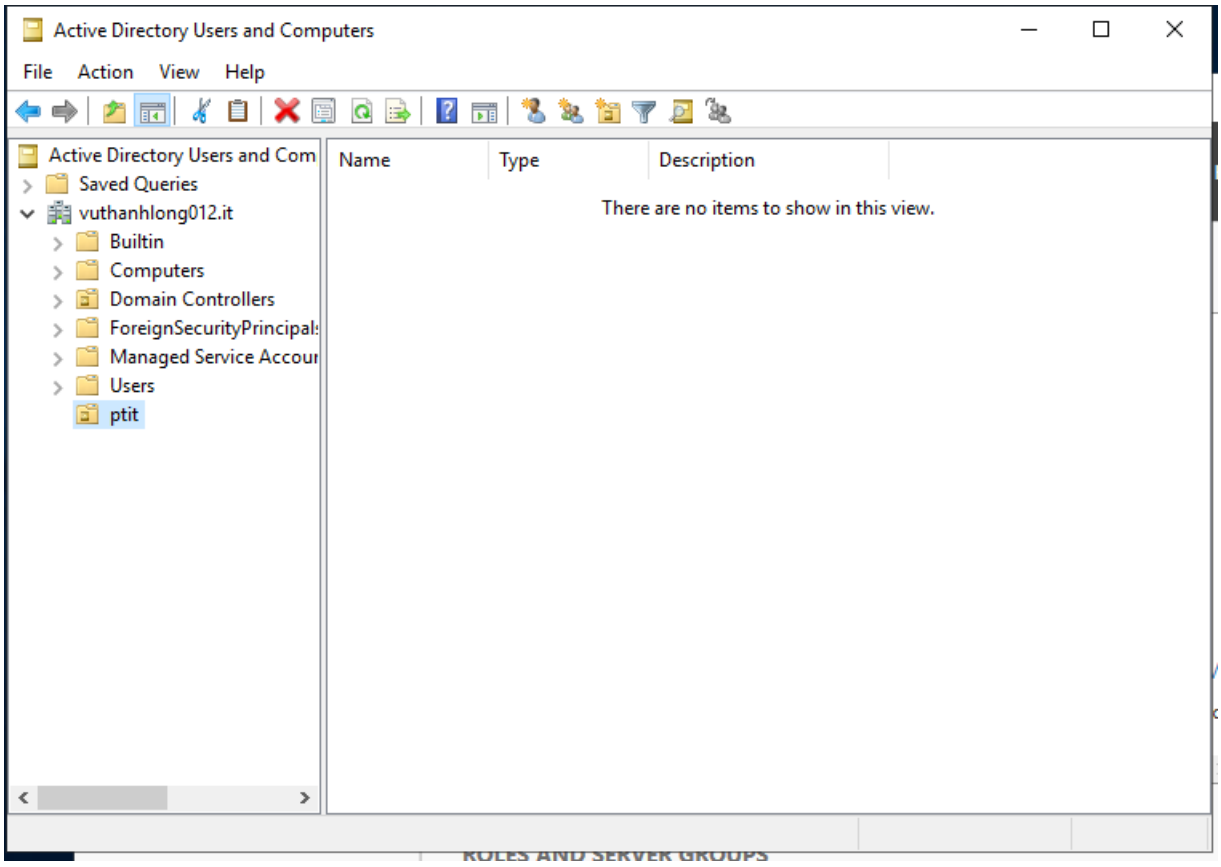
Tạo OU: Active Direstory Users and Computers → vuthanhlong012.it, sau đó ấn chuột phải chọn New → Organizational Unit





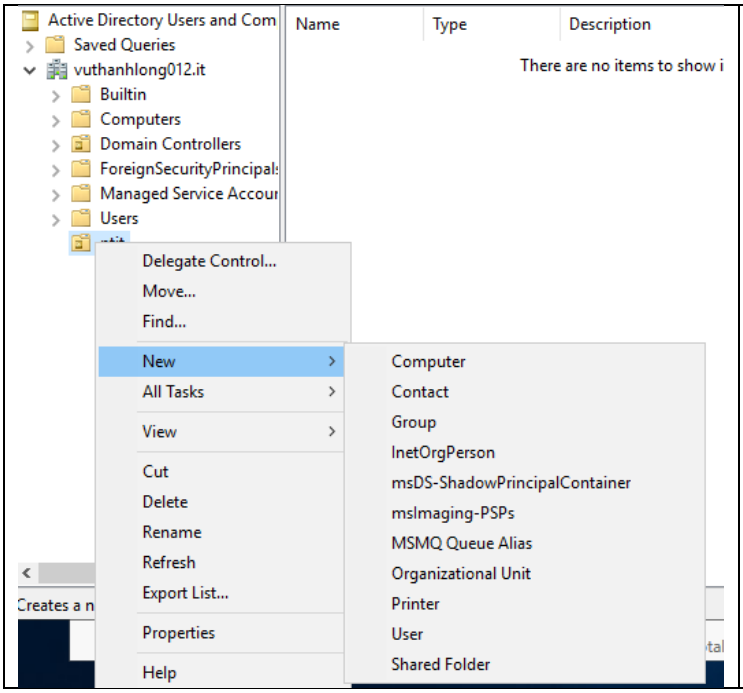
Đặt tên là ptit-> OK

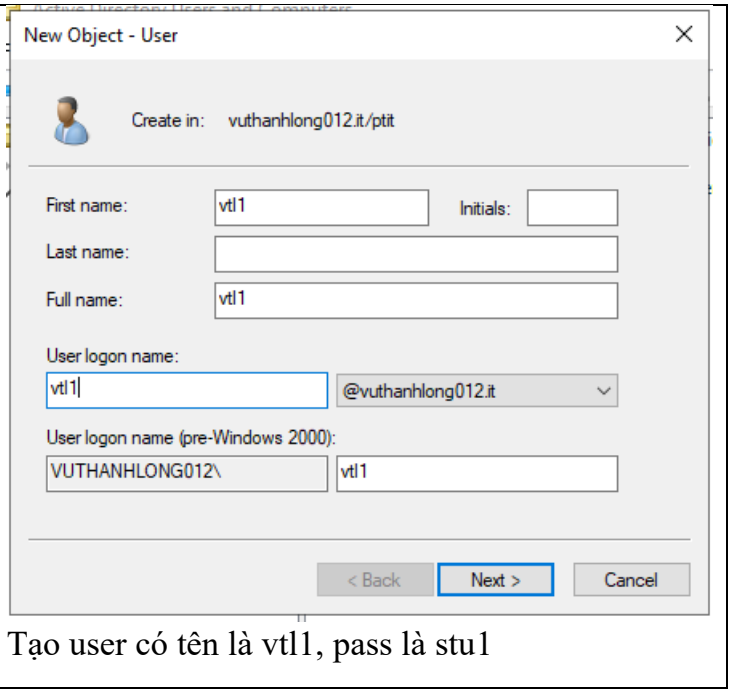
Ta đã thấy OU mới có tên là ptit



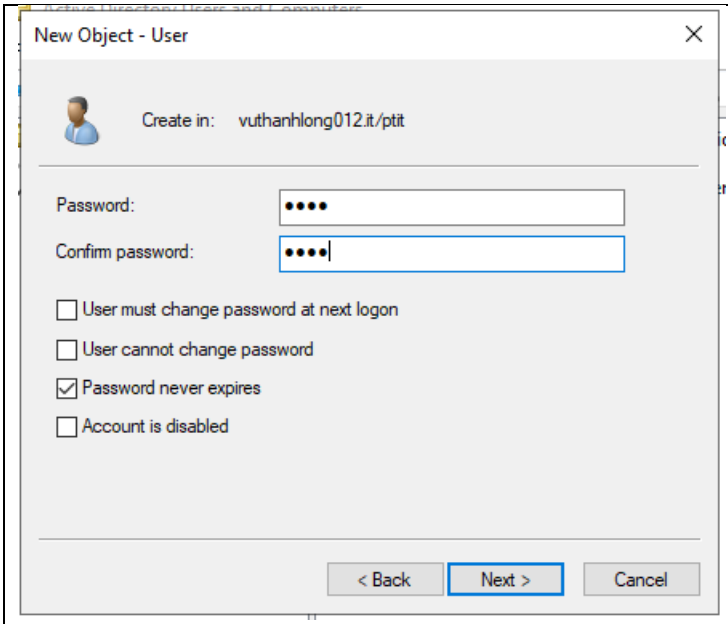
✓ Tạo các user thuộc OU

Tại OU ptit → chuột phải chọn New → User

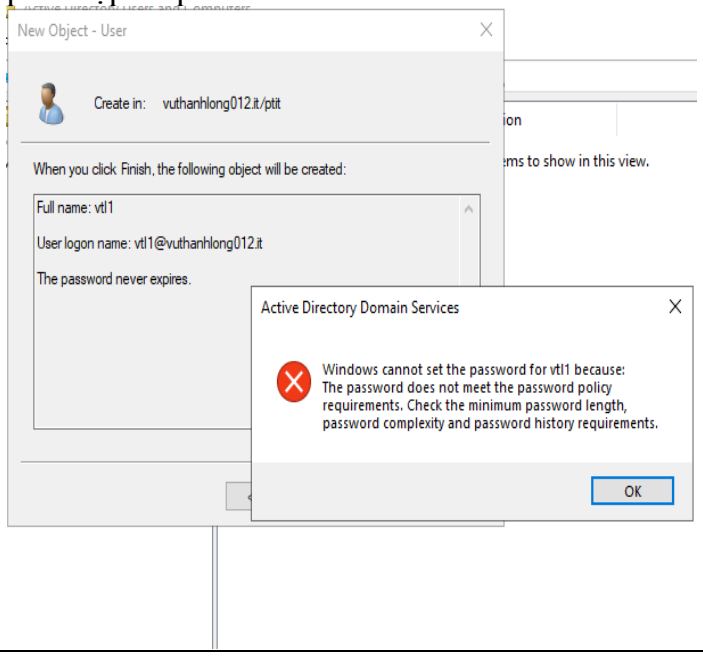


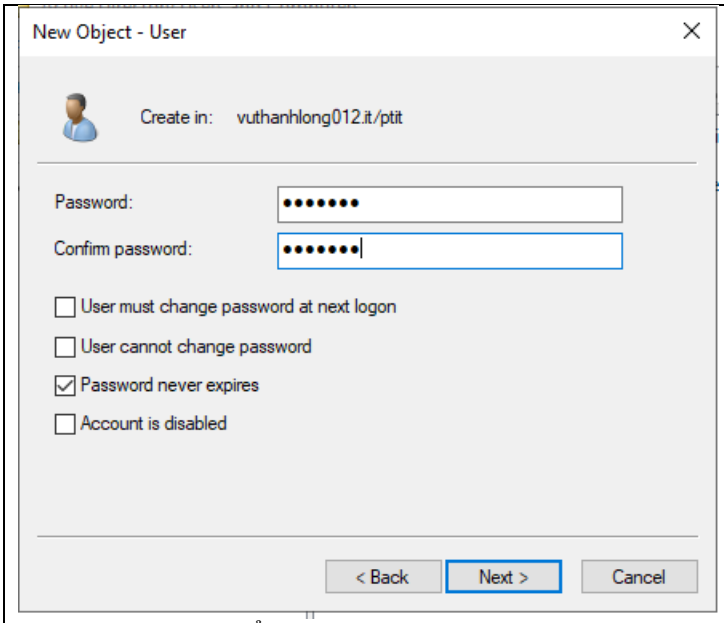


Tạo user có tên là vtl1, pass là stu1

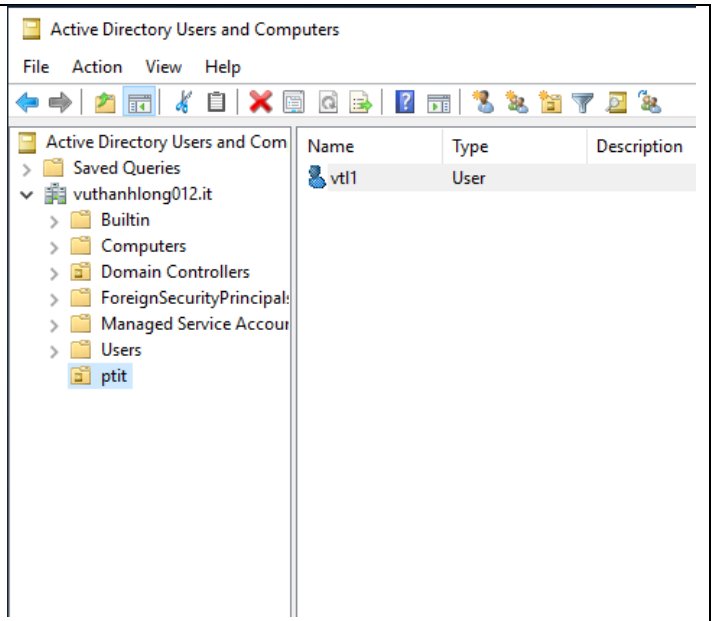


Không đặt được password do yêu cầu pass phải có ít nhất 7 ký tự gồm số, chữ, ký tự đặt biệt, pass phức tạp và phải khỏe.





Ta đặt lại mật khẩu: qtm123!



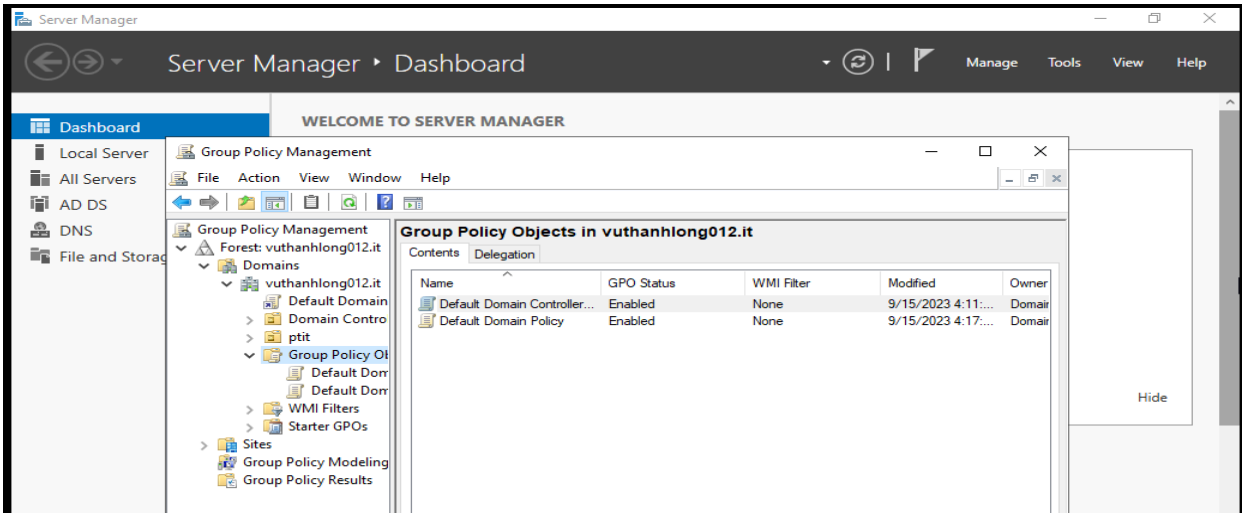
Đã tạo xong user vtl1 thuộc OU ptit

Các lựa chọn cho mật khẩu:

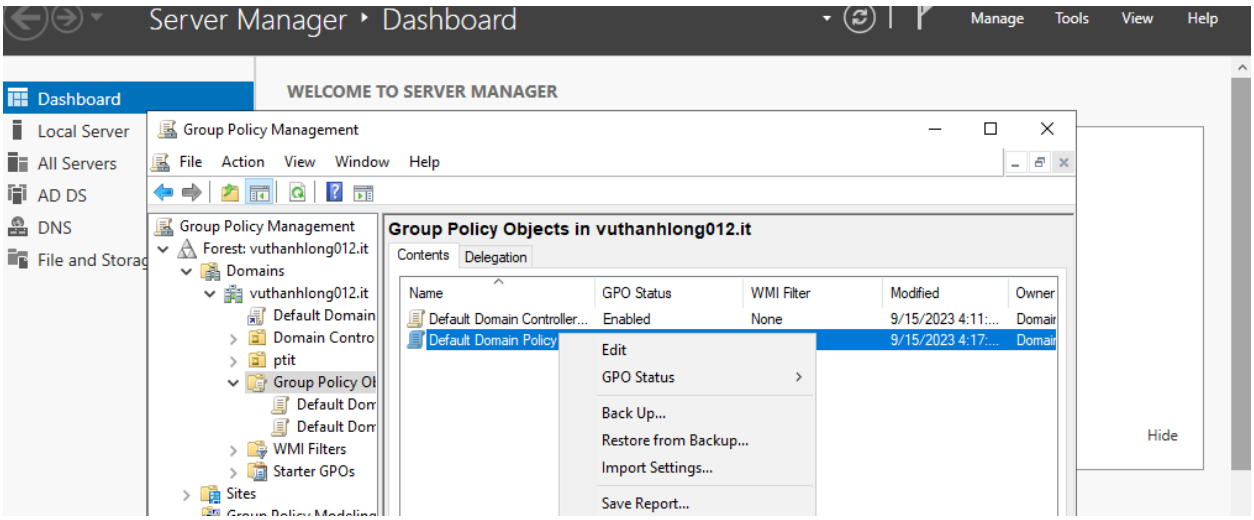
- User must change password at next logon: người dùng phải thay đổi mật khẩu khi đăng nhập vào
- User cannot change password: người dùng không thể thay đổi mật khẩu
- Password never expires: Mật khẩu không bị hết hạn
- Account is disabled: tài khoản bị vô hiệu

Thiết lập chính sách user và password

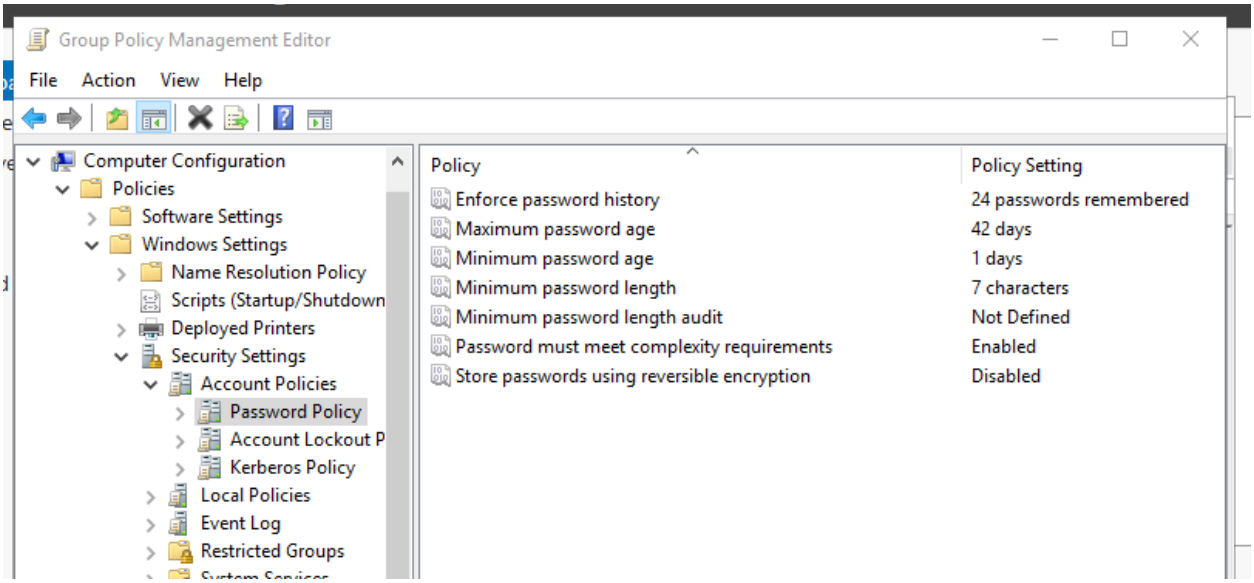
- Trong Server Manager vào Tools chọn Group Policy Management.



- Chỉnh chính sách password: Group Policy Management → Forest → Domains → vuthanhlong012.it → Group Policy Objects → Default Domain Policy → chuột phải chọn edit.

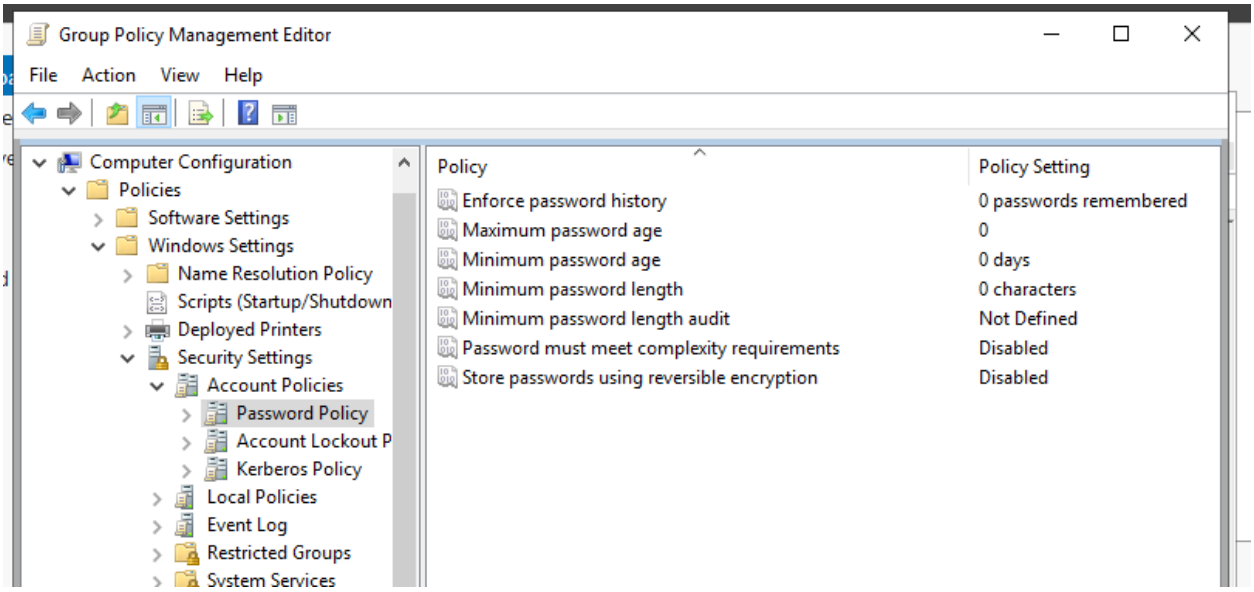


- Tại Group Policy Management Editor: Computer Configuration → Polices → Windows Settings → Security Settings → Account Polices → Password Policy.

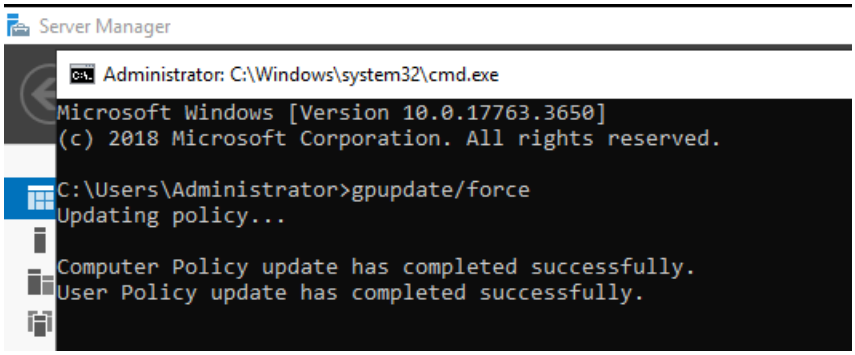


Trong đó:

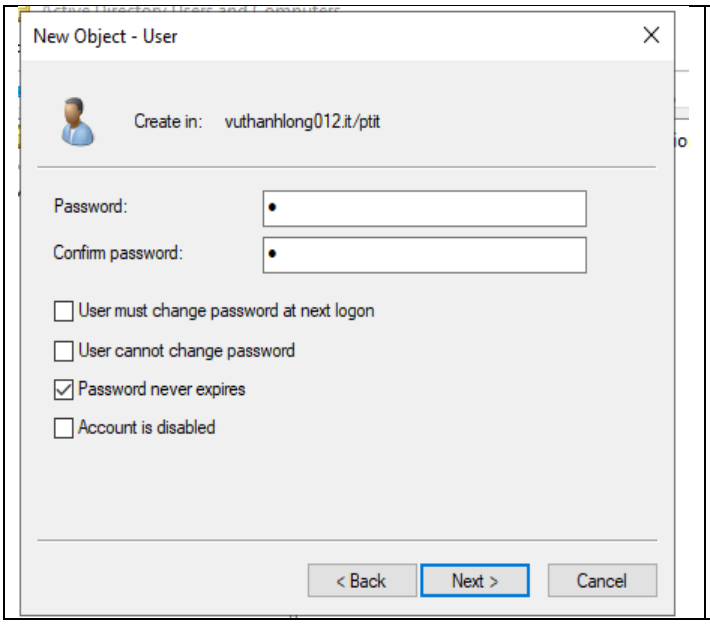
  - **Enforce password history**: số password hệ thống lưu trữ
  - **Maximum password age**: thời gian có hiệu lực tối đa của một password
  - **Minimum password age**: thời gian có hiệu lực tối thiểu của một password.
  - **Minimum password leghth**: độ dài tối thiểu của một password
  - **Password must meet complexity requirement**s: 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.

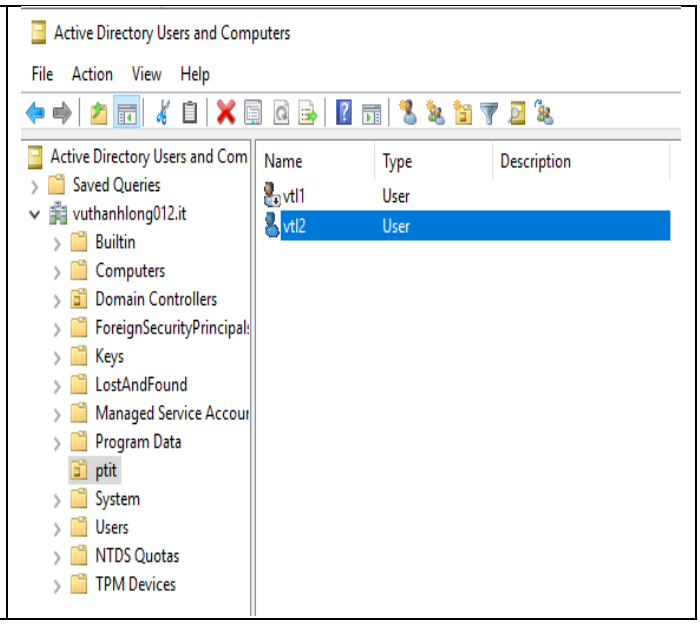


- Lưu chính sách lại: cmd → gpupdate /force.



- Kết quả: tạo user trong OU ptit
  User: vtl2; password: 1 → OK.



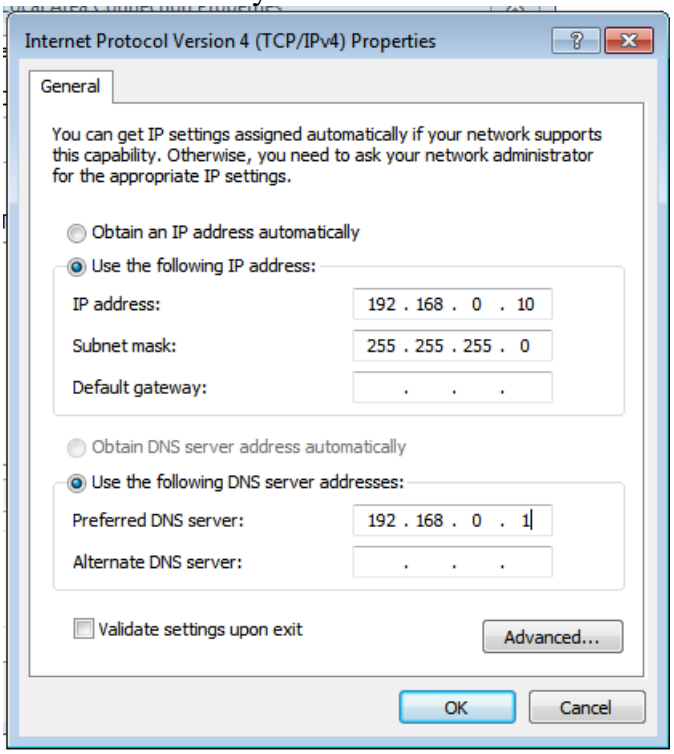


Phân quyền người dùng

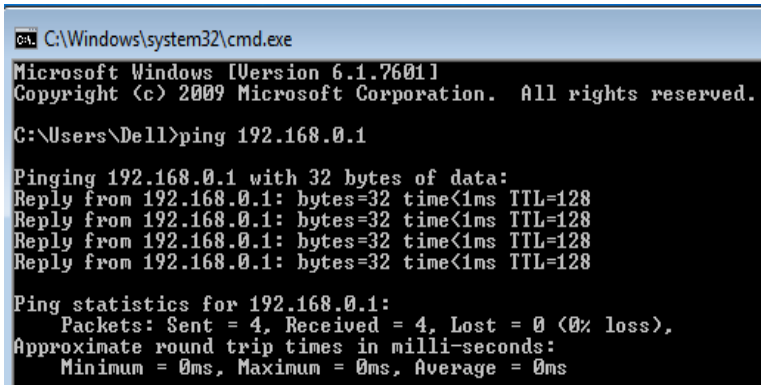
- Dùng 1 máy Windows 7 làm máy client

  Cấu hình join domain để máy Windows 7 trở thành client.

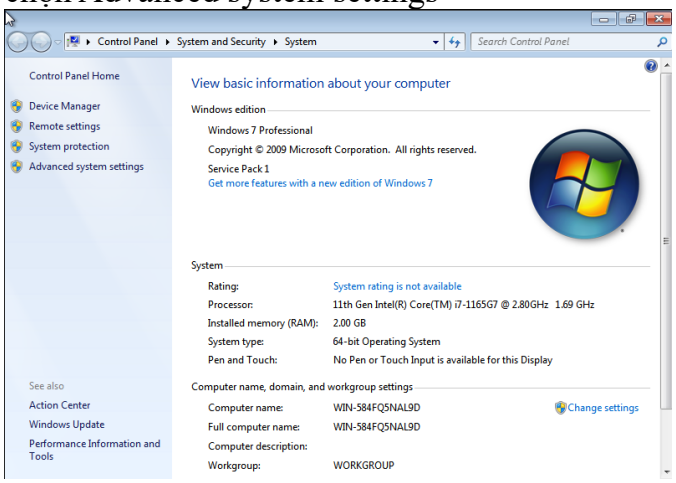
Cấu hình địa chỉ IP cho máy Windows 7, với DNS là IP của máy Windows Server



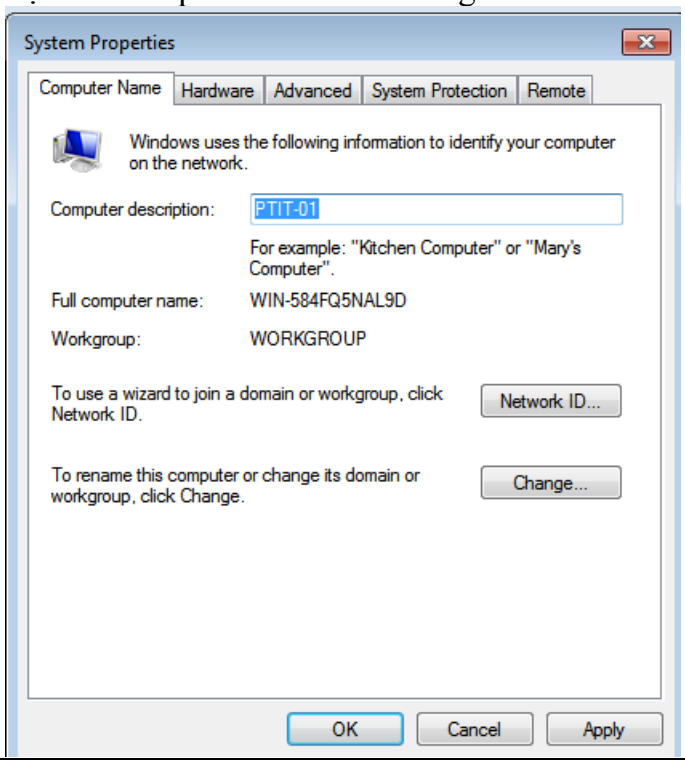
Kiểm tra sự thông nhau giữa 2 máy Windows 7 với Windows Server 2019



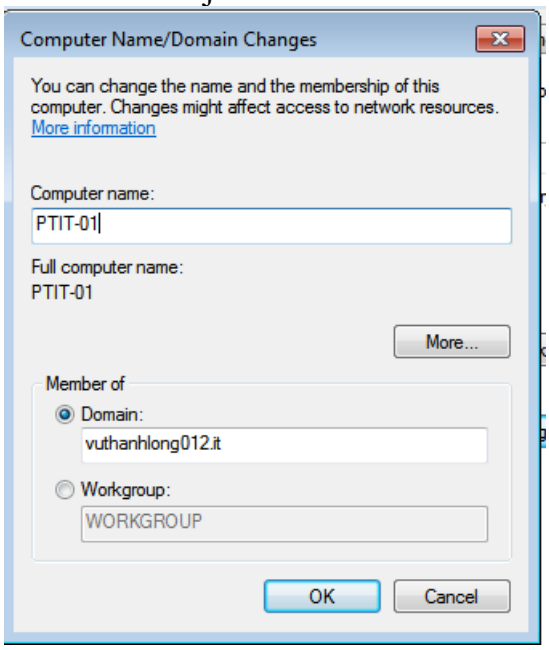
Tại Computer → chuột phải chọn Properties → chọn Advanced system settings



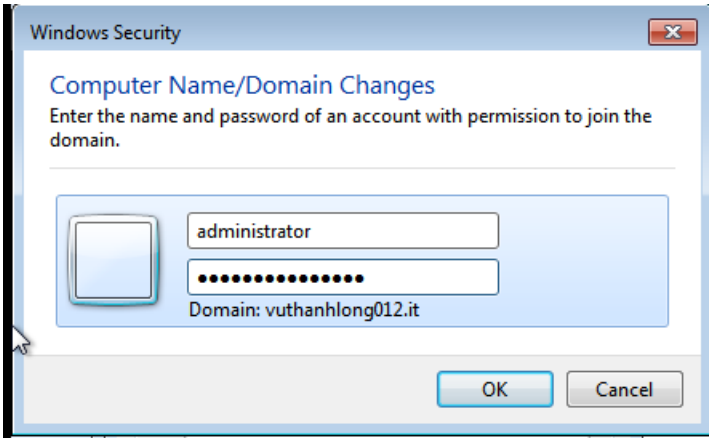
Tại tab Computer Name → change

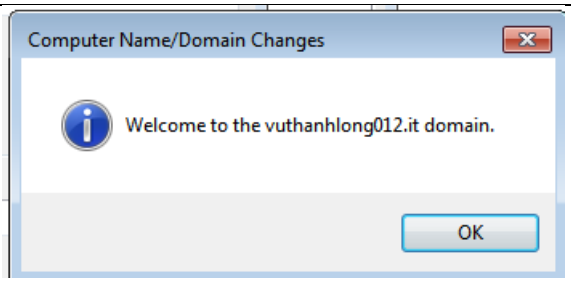


Tại Member of chọn Domain → nhập tên domain muốn join vào → click OK

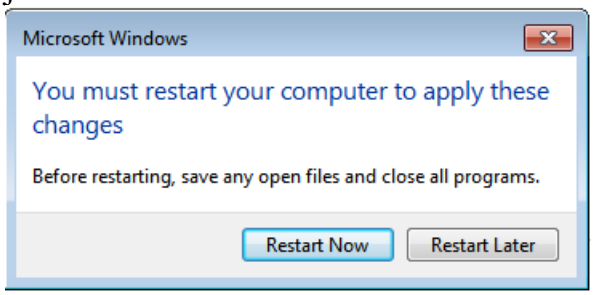


Nhập user và pass của máy domain Windows Server 2019 → Click Ok

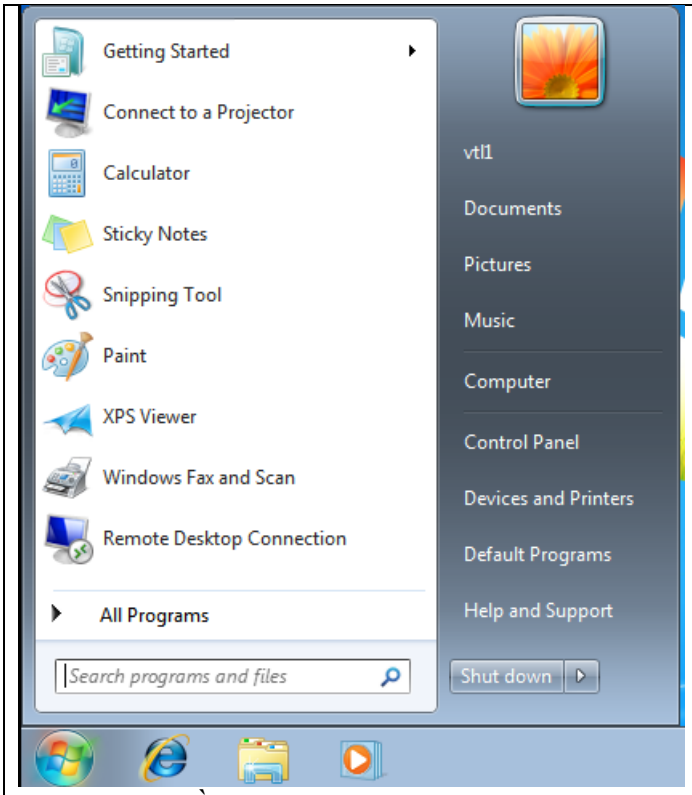




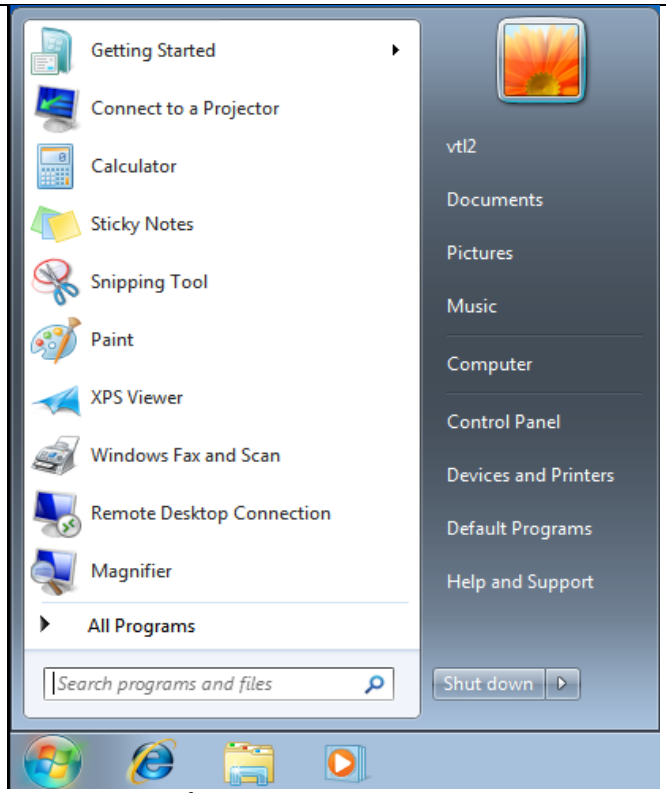
Restart now để máy khởi động lại → quá trình join domain hoàn tất



- Đăng nhập máy Client bằng user vtl1 và vtl2 đều được



Đăng nhập bằng tài khoản vtl1

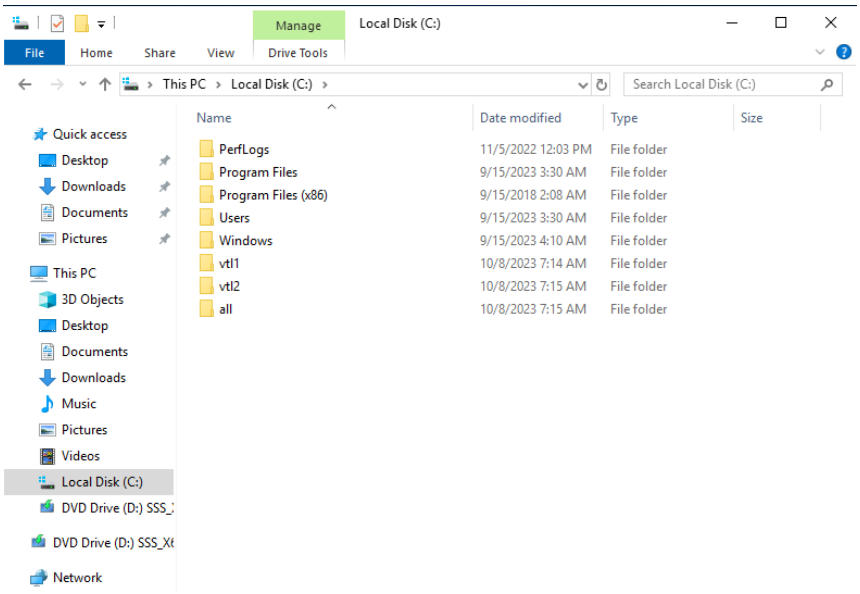


Đăng nhập bằng tài khoản vtl2

- Phân quyền đăng nhập

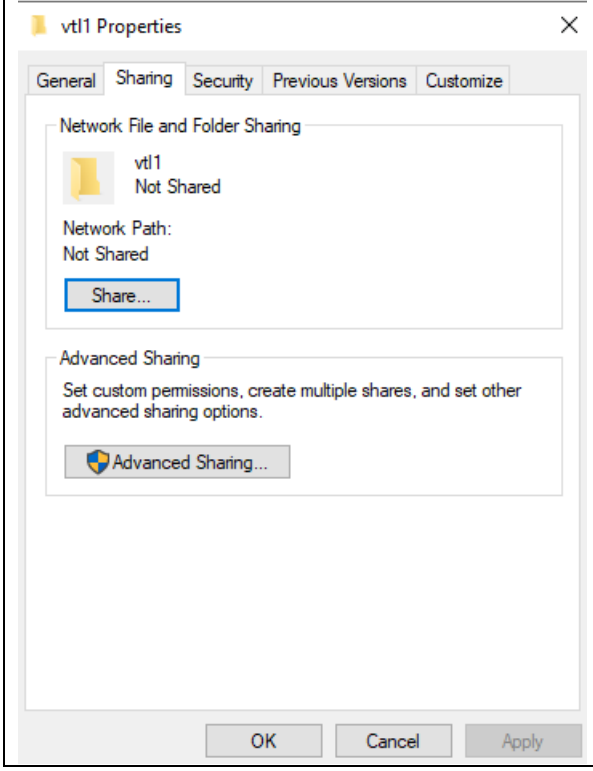
Tại máy Windows server tạo 3 folder vtl1, vtl2, all

- Foder vtl1 chỉ cho user vtl1 truy cập
- Foder vtl2 chỉ cho user vtl2 truy cập
- Foder all cho cả 2 users vtl1 và vtl2 truy cập

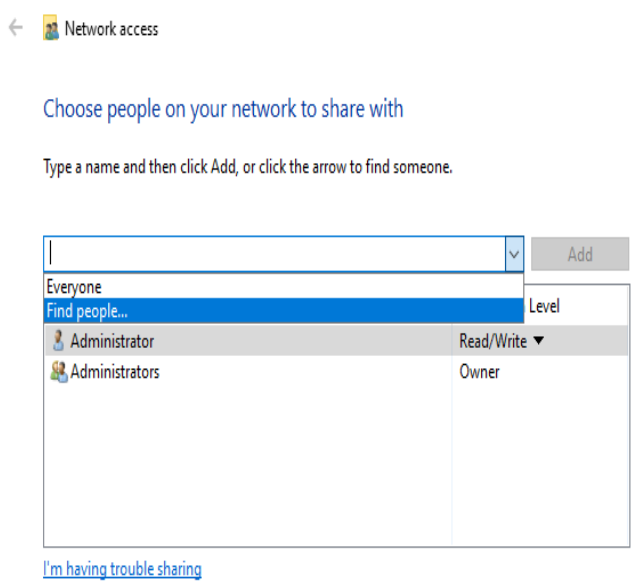


Chia sẻ folder vtl1 và phân quyền chỉ cho user vtl1 được truy cập: ấn chuột phải vào foder vtl1 chọn properties → sharing

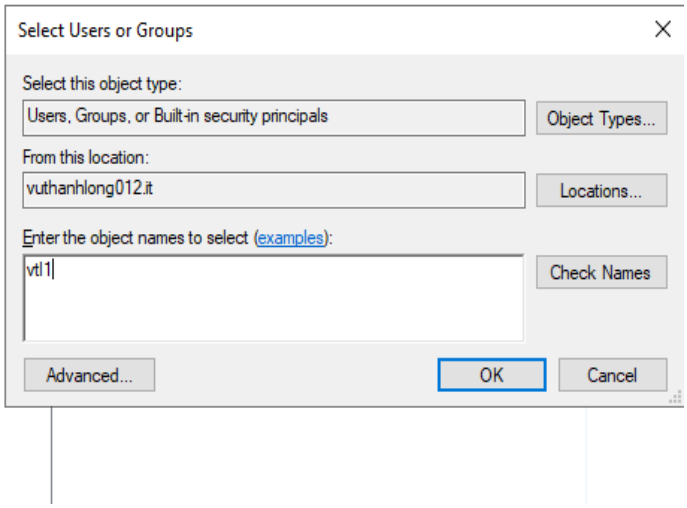
Chọn share



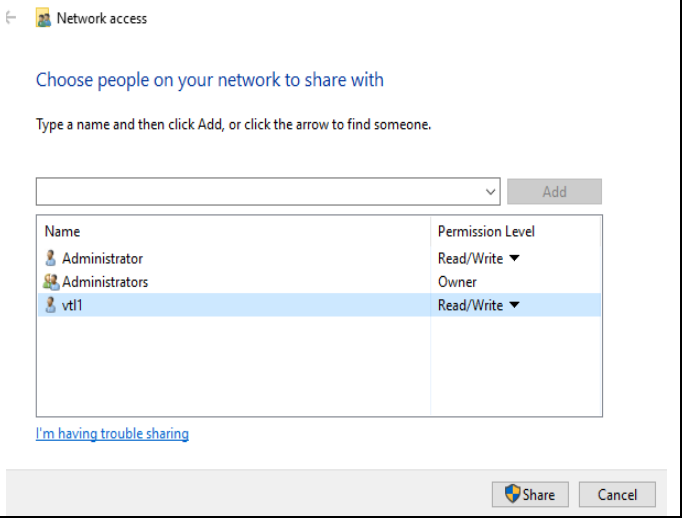
Chọn Find people...



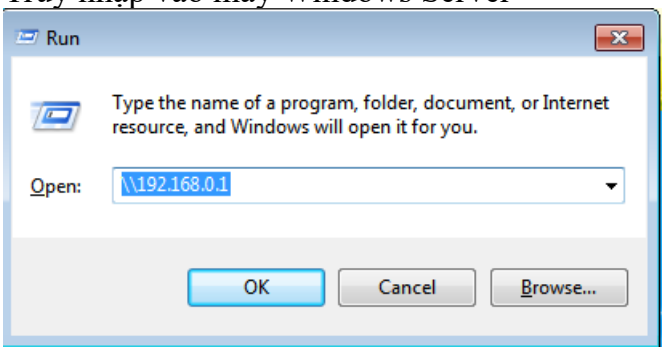
Nhập ô check names: vtl1



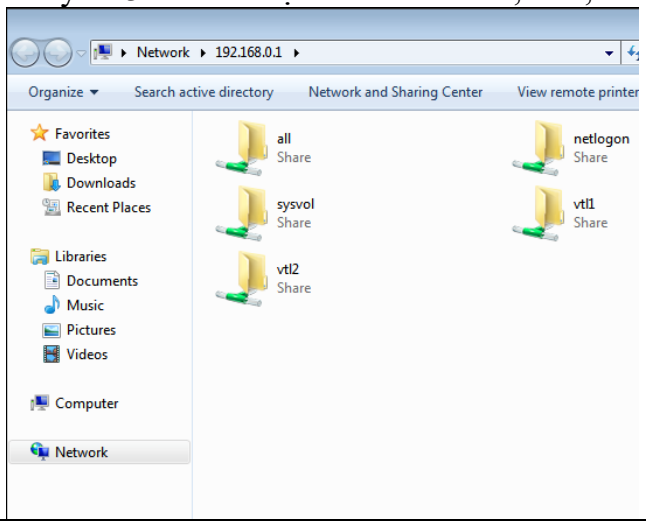
Sau khi tìm ra tài khoản vtl1 → ấn share → ấn done. Làm tương tự cho foder vtl2 và all.



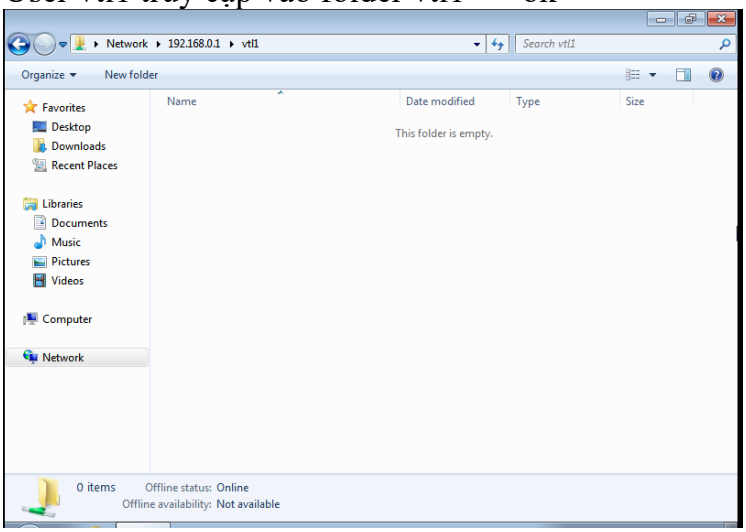
Kiểm tra:
Đăng nhập máy windows 7 bằng user vtl1.
Truy nhập vào máy Windows Server



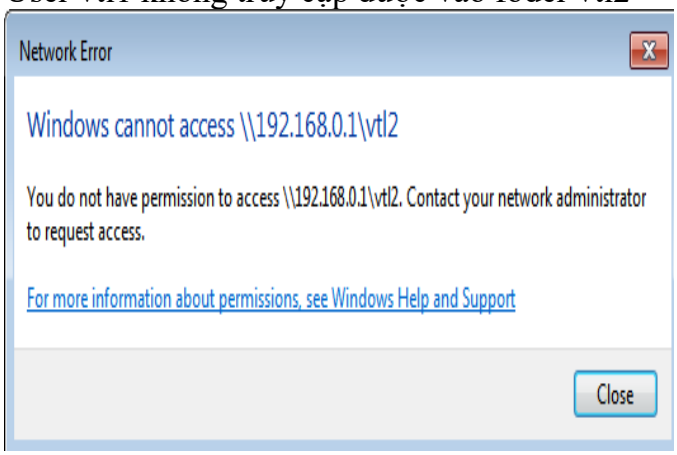
Thấy cả 3 floder được chia sẻ là vtl1, vtl2, all



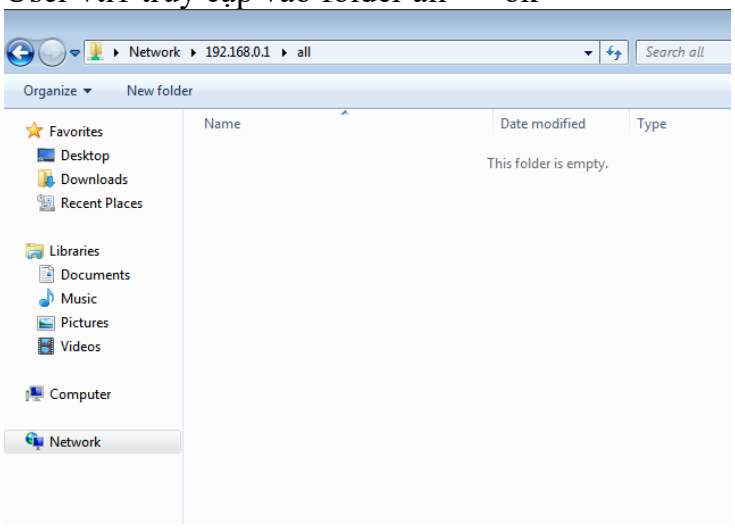
User vtl1 truy cập vào folder vtl1 => ok



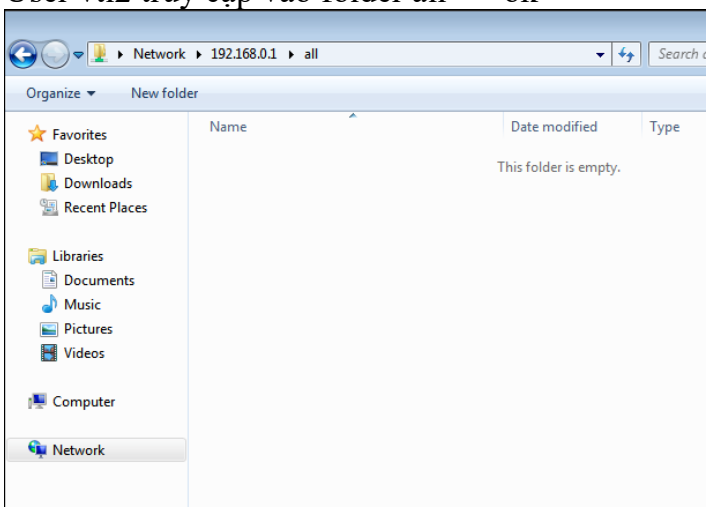
User vtl1 không truy cập được vào foder vtl2



User vtl1 truy cập vào folder all => ok



User vtl2 truy cập vào folder all => ok



3.3 Kết luận

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