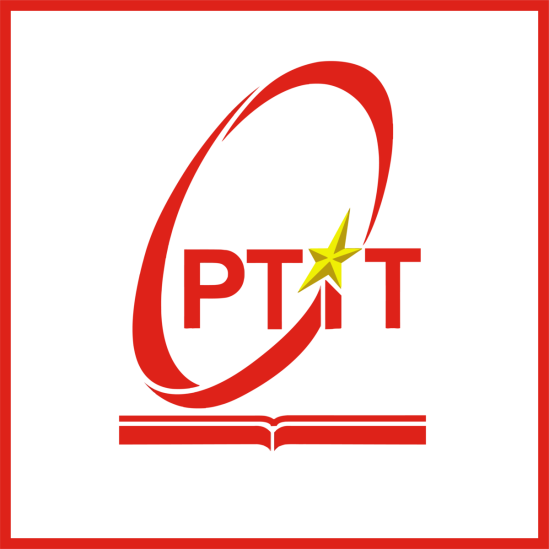
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN 1**



Môn: HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

**BÁO CÁO BÀI THỰC HÀNH SỐ 2**

Họ và tên sinh viên:

Đỗ Tiến Sĩ

Mã số sinh viên:

B20DCAT153

Họ và tên giảng viên:

TS. Đinh Trường Duy

I. Giới thiệu chung

1. Mục đích

- Hiểu được cách quản trị một nhóm người dùng trong mạng Lan nội bộ.

- Biết cách cấu hình cơ bản: tạo user, password, phân quyền.

2. Mô tả lý thuyết

2.1. Người dùng (user) và quyền 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.

• 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.

• “Active Directory Users and Computers” cung cấp chức năng quản lý các máy tính và người dùng, nhóm, đơn vị tổ chức trong miền.

• Mỗi tài khoản người dùng cần cung cấp 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 mới được truy nhập vào mạng.

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

• Với mỗi tài nguyên có quyền kiểm soát truy nhập người dùng 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. 2.2. Chính sách nhóm

• Công cụ quản trị nhóm là tính năng quan trọng với Windows cho phép kiểm soát môi trường làm việc với tài khoản người dùng và máy tính. Ngoài ra, quản trị chính sách nhóm cho phép quản lý và cấu hình tập trung với hệ điều hành ứng dụng và các cài đặt của người dùng giúp đơn giản hóa công việc quản trị.

• Chính sách nhóm xây dựng dựa trên các đối tượng chính sách nhóm GPO (Group policy objects). Đây là tập hợp các hướng dẫn cấu hình mà máy tính có thể áp dụng cho miền, vị trí (site) hay ở cấp độ thấp hơn. Mặc dầu, việc áp dụng các chính sách nhóm làm thay đổi danh mục đăng ký (Registry) song việc này vẫn dễ dàng hơn nhiều so với việc sửa đổi bằng tay.

• 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 cài đặt ứng dụng, màn hình làm việc và các dịch vụ hệ thống. Ngoài ra còn có thể là 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. 2.3. Tổ chức thư mục động

• Về mặt lô-gíc thư mục động bao gồm

+ Đơn vị tổ chức (Organizational Units): là các đối tượng bên trong một miền cho phép bố trí và nhóm các tài nguyên lại để làm thuận tiện cho công việc quản trị và cho phép ủy thác (delegate) và quyền quản trị.

+ Miền (Domain) là đơn vị lô-gíc các máy tính và tài nguyên mạng xác định ranh giới an ninh. Miền sử dụng một cơ sở dữ liệu miền động đơn lẻ để chia sẻ thông tin chung về an ninh và người dùng cho phép quản lý tập trung toàn bộ người dùng, nhóm và tài nguyên mạng. Một cơ quan hay doanh nghiệp có thể có nhiều miền tương ứng với cơ cấu tổ chức.

+ Cây (Tree) chứa một hay nhiều miền dùng chung không gian định danh gốc. Có thể hình dung cây tập hợp các miền chia sẻ không gian tên Internet như fit.ptit.edu.vn. Rừng (Forest) chứa một hay nhiều cây và không gian định danh có thể tách biệt. Miền đầu tiên trong rừng được gọi là miền gốc của rừng (forest root domain).

+ Quan hệ tin cậy (Trust relationship) cho phép người dùng từ các miền khác nhau sử dụng tài nguyên mạng của các miền.

• Đơn vị tổ chức OU (Organizational Units) trợ giúp việc sắp xếp các đối tượng trong miền và giảm thiểu số miền cần thiết. Đây là phần tử nhỏ nhất mà người quản trị có thể cài đặt các chính sách nhóm hay ủy thác quyền quản trị. Đơn vị tổ chức có thể lưu trữ người dùng, nhóm, máy tính và các đơn vị tổ chức khác. Các đơn vị tổ chức tạo trước (như máy tính, người dùng) thì không thể gán quyền hay chính sách nhóm.

 • Trong thư mục động, các đối tượng chính là tập được đặt tên riêng biệt chứa đựng các thuộc tính hay đặc tính thể hiện tài nguyên mạng của thư mục động. Các đối tượng phổ biến trong thư mục động là máy tính, người dùng, nhóm. Mỗi đối tượng được gắn số duy nhất gọi là GUID (Globally unique identifier) hay định danh an ninh (Security identifier).

• Tài khoản người dùng trong thư mục động, còn gọi là tài khoản người dùng miền, được lưu trong máy chủ miền cho phép người dùng truy nhập tới các tài nguyên bên trong một miền miễn là người dùng đó có đủ quyền phù hợp. Liên kết với tài khoản người dùng là danh sách thư mục và dữ liệu về môi trường làm việc của người dùng và cài đặt ứng dụng.

• Tài khoản ứng với máy tính cung cấp công cụ để theo dõi và giám sát việc truy nhập của máy tính vào mạng và tài nguyên của miền và tương ứng duy nhất với một máy tính.

• Để người dùng và máy tính có thể truy nhập được các tài nguyên của miền, người dùng và máy tính cần phải thực hiện thao tác gia nhập miền. Nói cách khác, người quản trị miền cần phải thêm máy tính vào trong danh sách quản lý của miền.

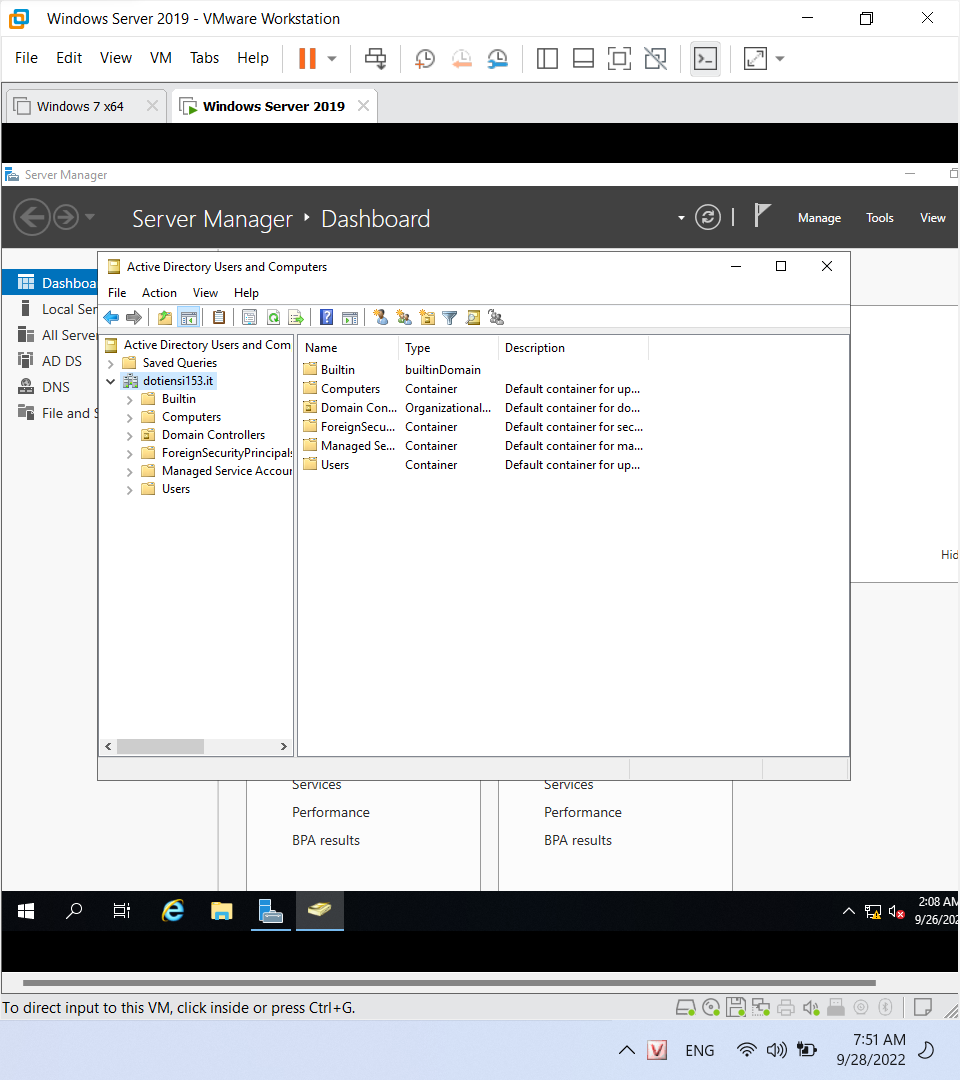
II. Các bước thực hiện.

1. Tạo Organizational Unit (OU)

* OU được dung trong việc quản lý tập trung các client thuộc cùng 1 domain.
* Cách thực hiện:

- Mở Server Manager → Tools → Active Directory Users and Computers.

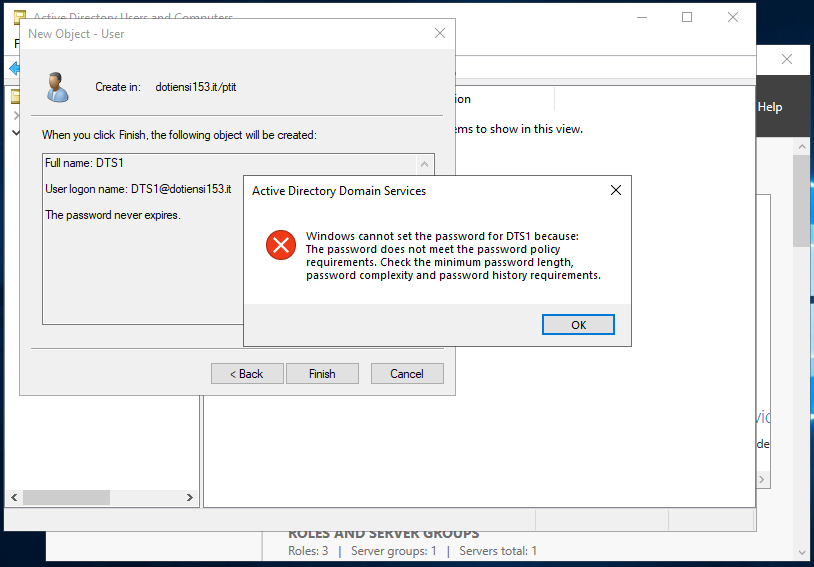
- Tạo OU: Active Directory Users and Computers → nguyenthiyen205.it, sau đó ấn chuột phải chọn New → Organizational Unit.



Đặt tên ptit là ok:

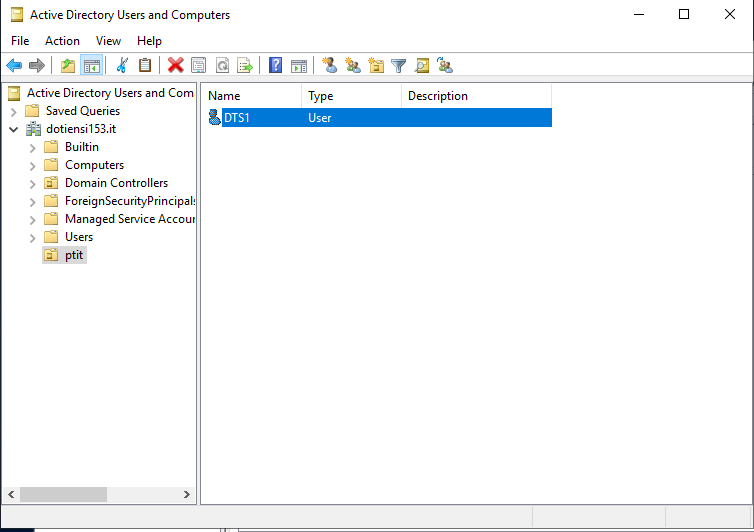
|  |
| --- |
| https://lh3.googleusercontent.com/ed7Vt46Px2XcuqrmwJTvM51KTU37L71zcpWBkcZTg0hbz2PyIZ4baitnchLQ_GD8-QSPY8_PyVDHW6wFsBKXmvUkk0kbfzRn3OB9aQK24VyrJxrvyAiPxZgh4WO48n7nXFPRFQMN8FjgE8RRZb67LrRKcP1Bqub7j94596ypkTakoVb1SoRIaCZBUQ8NP---xymxLQ |

1. **Tạo các user thuộc OU**

Cài user1 tên là DTS1 và pass dts1. Ta không đặt được là vì phải yêu cầu là phải có 7 kí tự gồm chữ, số , kí tự đặc biêt, pas phức tạp và khỏe.

|  |  |
| --- | --- |
| https://lh6.googleusercontent.com/J9g91BYcsK7nCD3l5Es8T98igQ56o2FffmidAgJ7yRJSr8O5mEZhn8cO_4xi7RdSqQ3SK-T-JmcUrC8DQFL8k2pP3L8o_Jn1eBEc74a7ZADGHe5BLgWiQXZKzIm8oiRVOWpKYwfEDqU38uz6s1kPBzg5zW55jVQyfrSyDbkBbP6TOTsaYrfJgQrY8WdRdfrHwF1a8Q | 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 bao giờ bị hết hạn.  - **Account is disable:** tài khoản bị vô hiệu |

Đổi lại mk là qtm123! Thì ok .

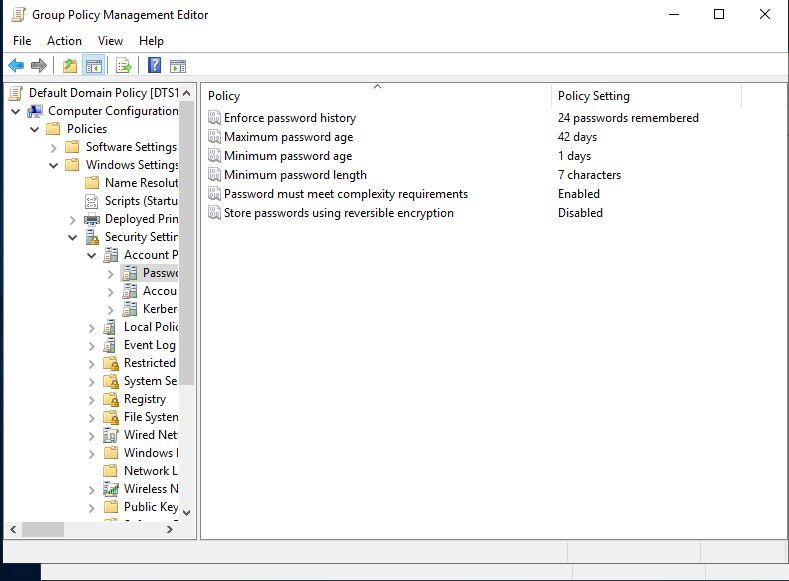


1. **Chính sách đổi mật khẩu**

Thực hiện theo các bước mà đã hướng dẫn, ta truy cập được vào trình thay đổi.

|  |  |
| --- | --- |
| - Chỉnh chính sách password: Group Policy Management → Forest → Domains → dotiensi153.it → Group Policy Objects → Default Domain Policy → chuột phải chọn edit. | https://lh6.googleusercontent.com/DwtotrQStZEDbD44s5X8qaFtKj3cXZPIB48LNv42eXOxE3gLpRz9UBcVIcv6x2Wvd1f-xpoJmlrlndslvUbjmPPM1vK-5AbyU126RkQ2cLlMbW-nBYgAfoisyJT0GJBFXSNKf1NCHUIpEyKpu9mjRMZAG3nCSg57YzFME7p3rV6tWbBwJLUqpBLMEfjSHu80RsTIZQ |

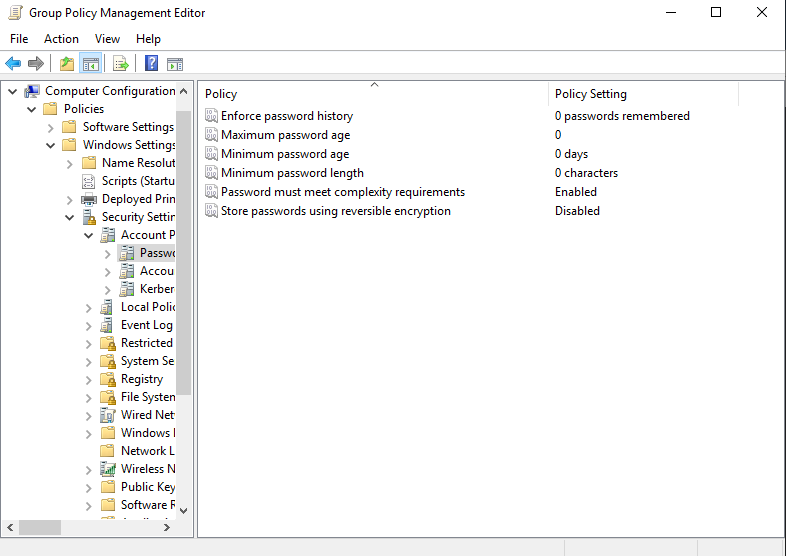
- Chỉnh password về dạng không phức tạp, giảm số lượng ký tự và giảm độ mạnh của password.

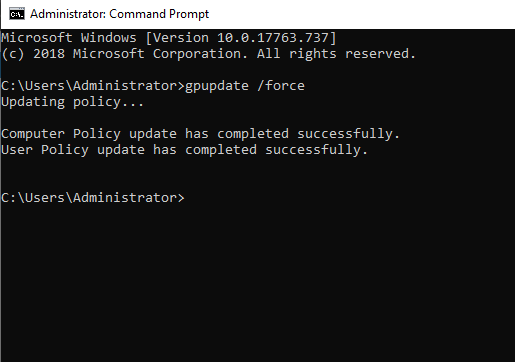


Trong đó:

* 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 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

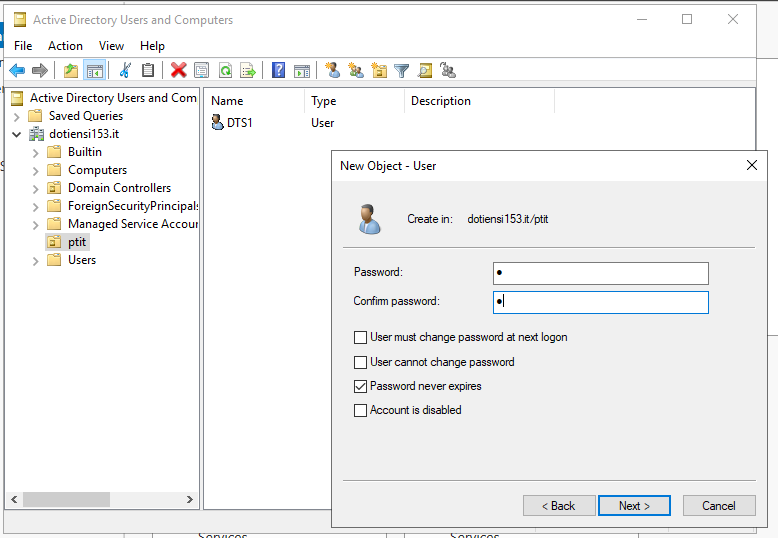
của password.

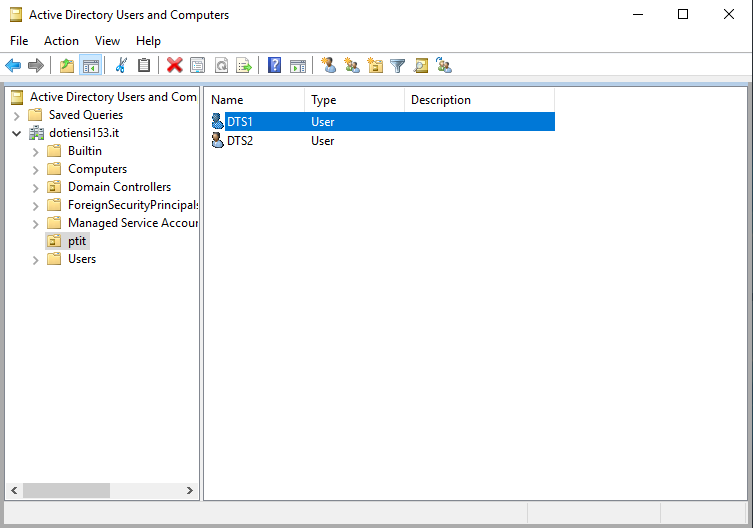
* Chỉnh password về dạng không phức tạp, giảm số lượng ký tự và giảm độ mạnh của password.
* Lưu lại chính sách: cmd → gpupdate/force



Kết quả: thay đổi chính sách mật khẩu thành công.

Tạo user DTS2 với mk là 1

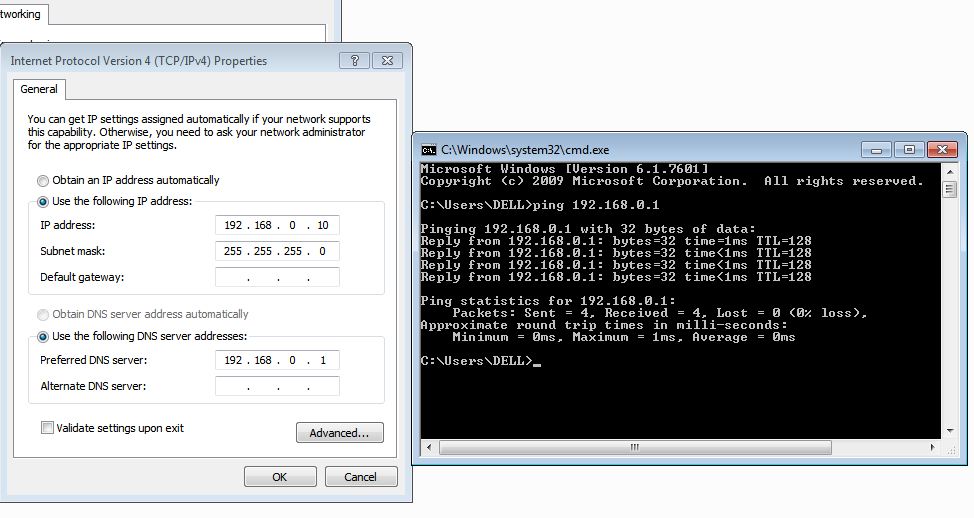


Tạo thành công user2 DTS2.

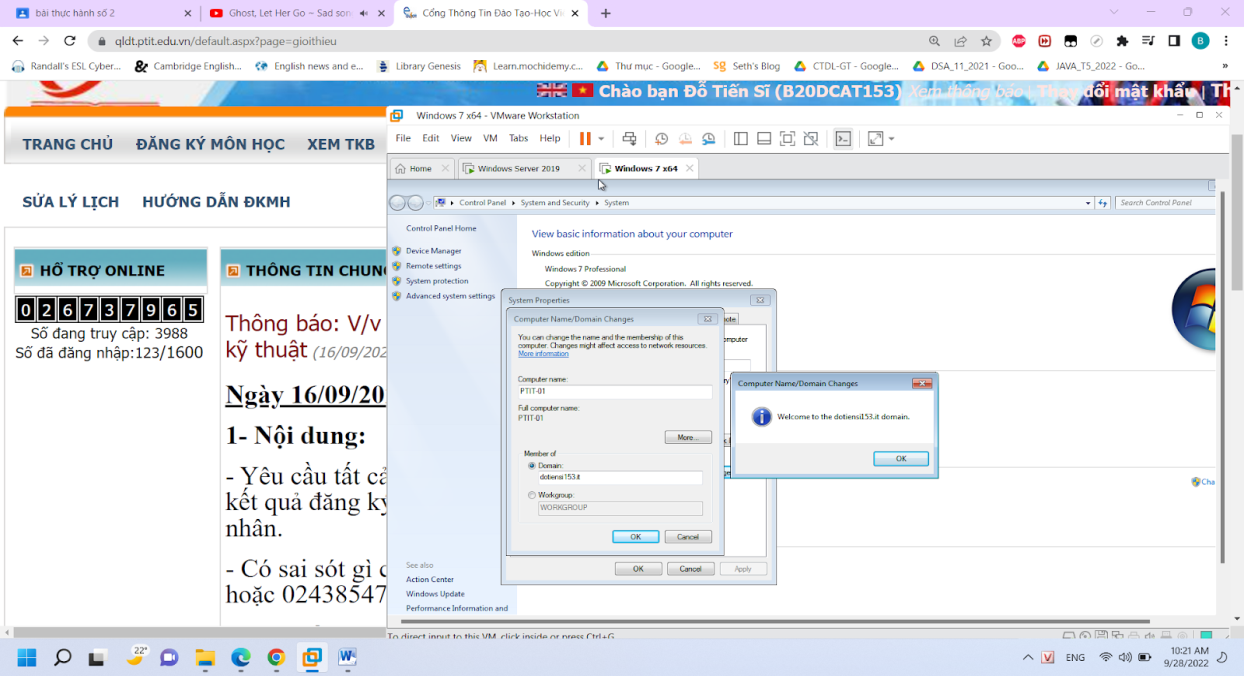
**3. Phân quyền người dùng.**

\* Dùng máy Windows 7 làm máy client. Cấu hình join domain để máy Windows 7 trở thành client.

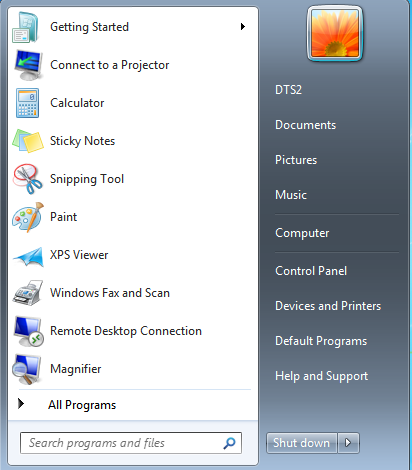
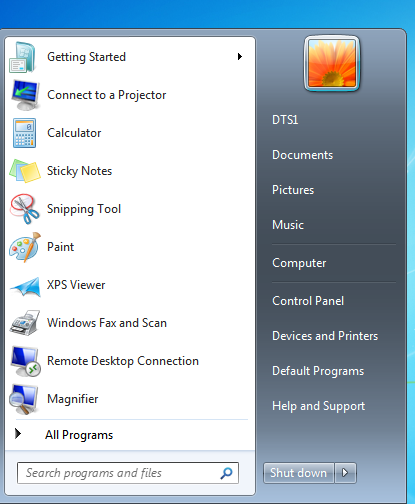
- Cấu hình địa chỉ IP cho máy Windows 7, với DNS là IP của máy Windows Server và kiểu tra liên thong của 2 máy win7 và win server 2019



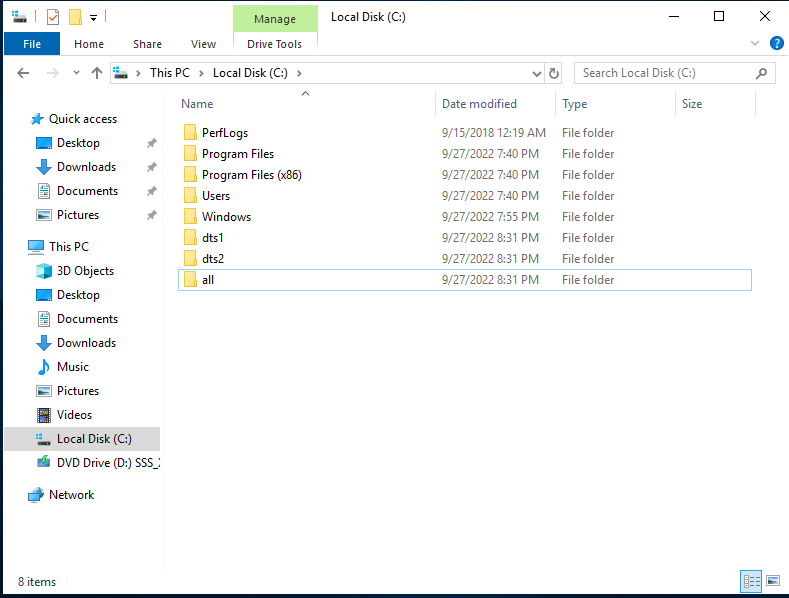
* Tham gia đăng nhập Domain dotiensi153.it thành công.



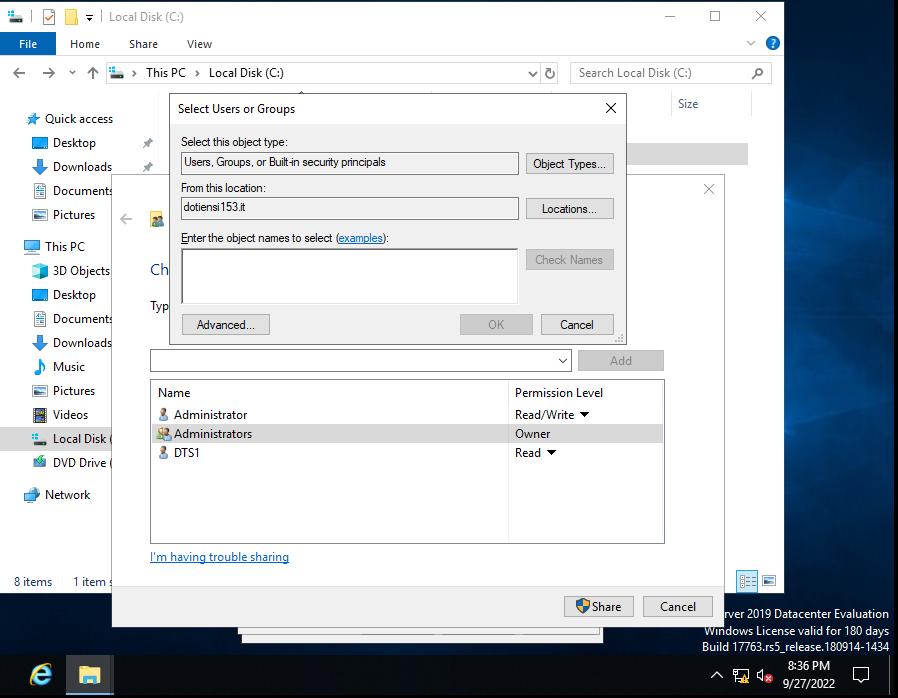
* Đăng nhập DTS1 và DTS2



* Phân quyền đăng nhập  
  tạo ra 3 tệp DTS1, DTS2, ALL
* Phân quyền dts1 cho user DTS1 sử dụng
* Phân quyền dts2  cho user DTS2 sử dụng
* Phân quyền all cho user DTS1 , DTS2 sử dụng.



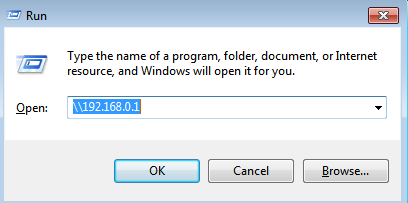
* Share quyền tệp dts1 cho DTS1



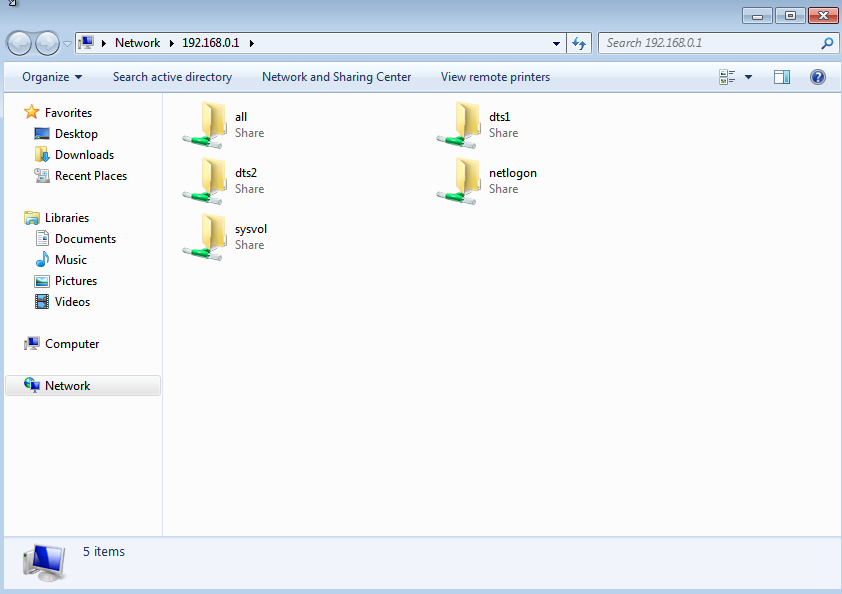
- Tương tự cho dts2 và all

**4. kiểm tra**

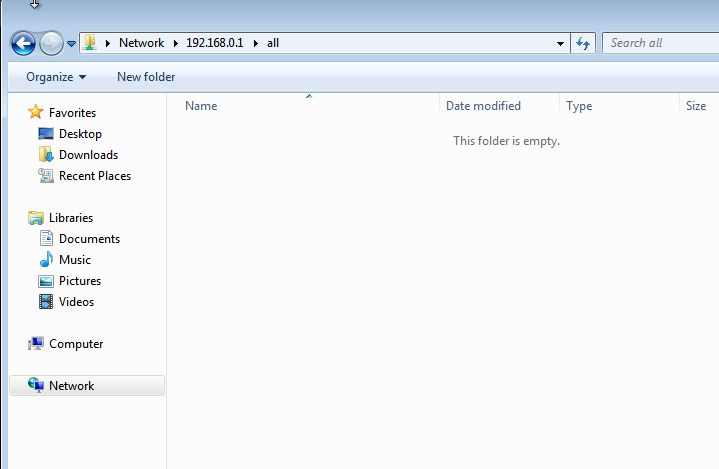
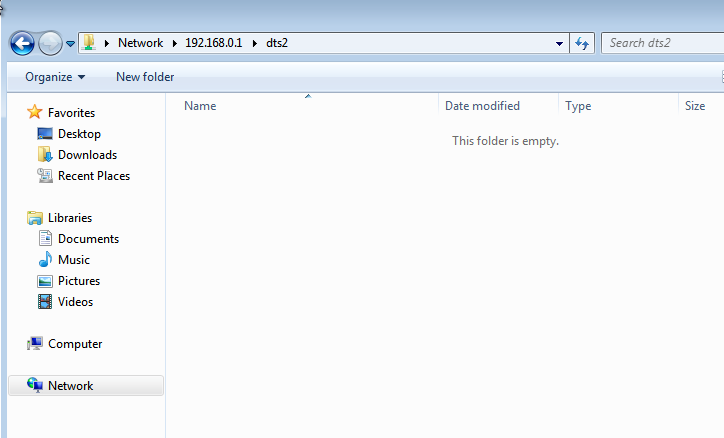
* VÀO DTS2 và run



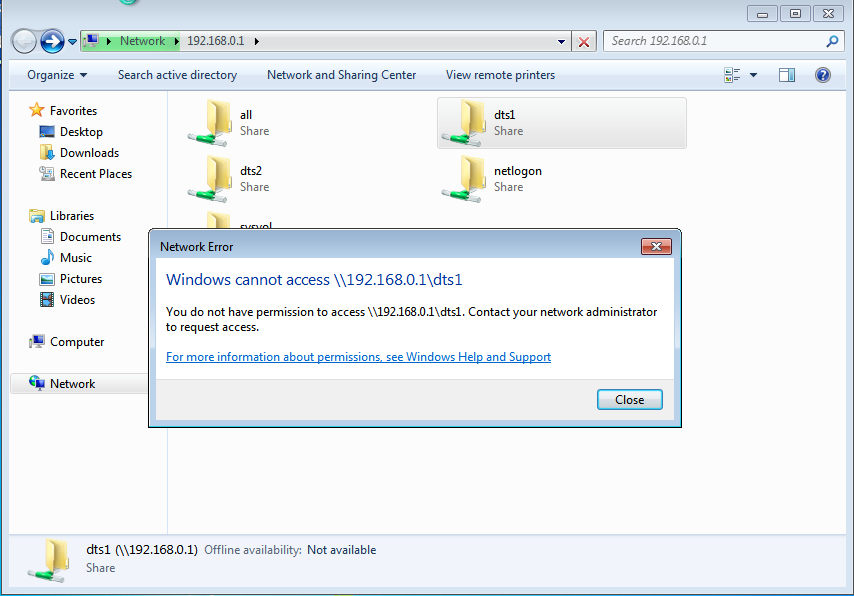
* Các tệp mà có



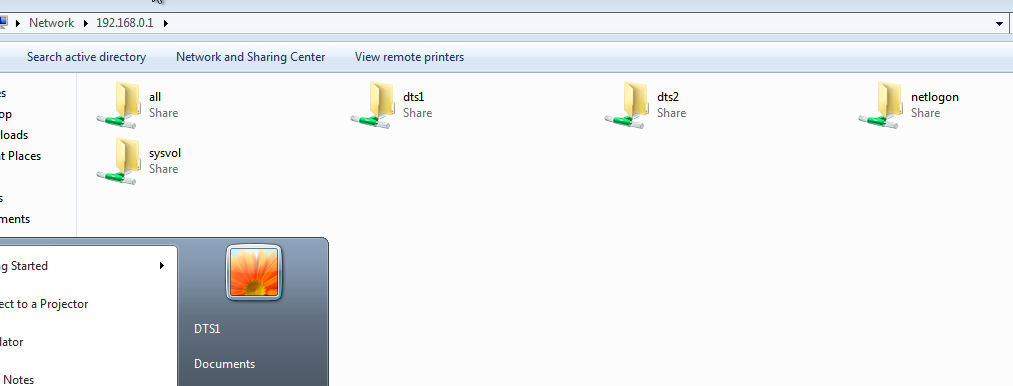
* User DTS2 vào dts2 và all thì ok.



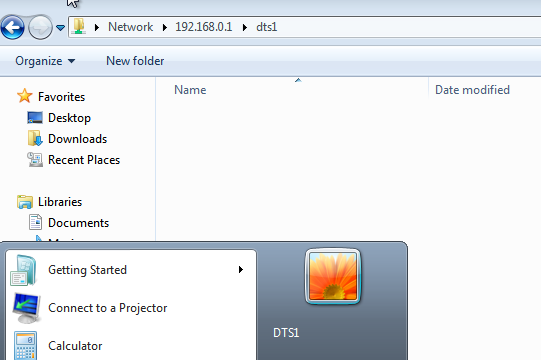
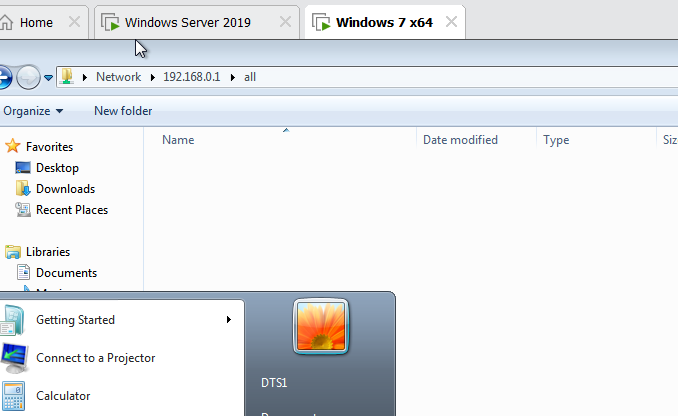
* DTS2 không truy cập vào dts1 được vì không được cấp quyền truy cập



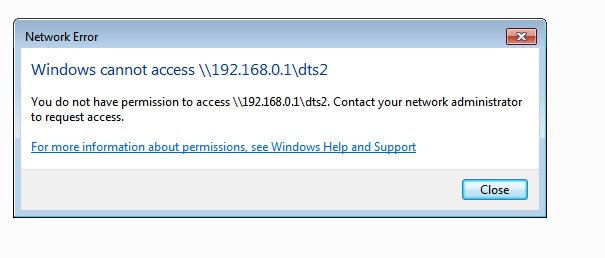
* Ta kiểm tra với user DTS1



* Tham gia thành công



* User DTS1 vào folder dst1 và all ok và không truy cập được vào folder dts2:



Kết quả: Tạo, phân quyền thành công OU, users và chia sẻ thành công tài nguyên