

BÀI TẬP THỰC HÀNH

BÀI 1: LOCAL USER ACCOUNT & GROUP ACCOUNT

Giới thiệu: Thông thường một máy tính không phải lúc nào cũng chỉ có một người nào đó sử dụng duy nhất mà trên thực tế ngay cả máy trong gia đình chúng ta đôi khi vẫn có ít nhất từ 2-3 người sử dụng. Tuy nhiên nếu tất cả mọi người đều sử dụng chung một tài khoản thì những dữ liệu riêng tư của người này người kia hoàn toàn có thể xem được.

Nhưng nếu máy tính là máy chung của công ty và vấn đề đặt ra là ta không muốn tài liệu của người dùng này người dùng kia có thể xem tùy tiện được. Vậy cách tốt nhất là cấp cho mỗi nhân viên một máy nhất định và yêu cầu họ đặt **password** lên máy của mình, nhưng như thế thì rất tốn kém và không được ưa chuộng. Chính vì thế người quản trị mạng sẽ sử dụng công cụ **Local Users and Groups** để tạo các tài khoản người dùng trên cùng một máy, khi đó dữ liệu của người này người kia không thể truy cập được.

Local User - Để tạo được User local bạn phải có quyền ngang hàng với Administrator của hệ thống.

1. Tạo Local user account

B1: Mở chương trình **Local user and group**

- **Start** chọn **programs** chọn **Administrative tools** chọn **Computer Management** chọn **Local user and group**

- Cách 2: Vào **Start** chọn **run** gõ lệnh **lusrmgr.msc**

B2: Click phải chuột vào user chọn **New user**



B3: Điền các thông số:

A screenshot of the 'New User' dialog box in Windows XP. It contains the following fields and options:

- User name: SV1
- Full name: Nguyen Van Nam
- Description: Lop Truong
- Password: [masked with dots]
- Confirm password: [masked with dots]
- Four unchecked checkboxes at the bottom:
 - ☐ User must change password at next logon
 - ☐ User cannot change password
 - ☐ Password never expires
 - ☐ Account is disabled

- user name: **SV1**
- Full name: Nguyen Van Nam

- Description: Lop Truong
- Password: abc@123
- Confirm Password: abc@123
- Bỏ dấu check trước dòng **user must chang password at next logon** chọn **Create**

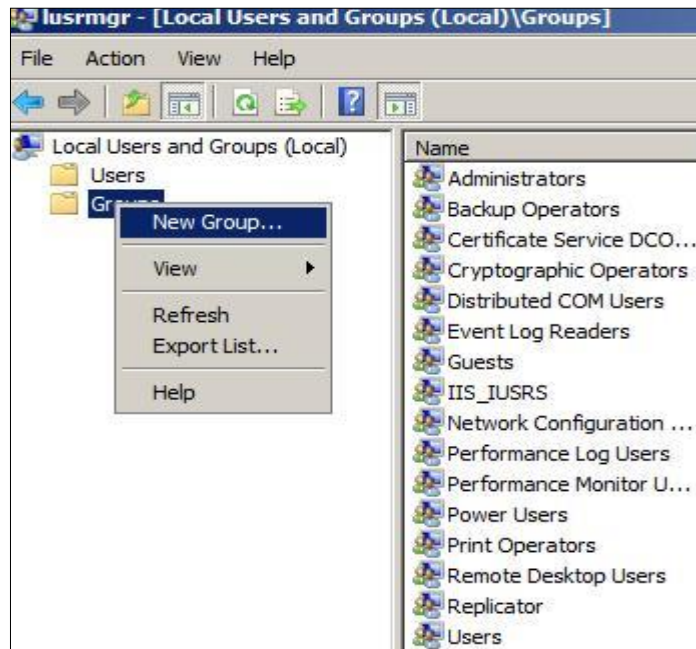
B5: Làm các bước trên tạo user **SV1,SV2,SV3**

B6: Log on vào user SV1

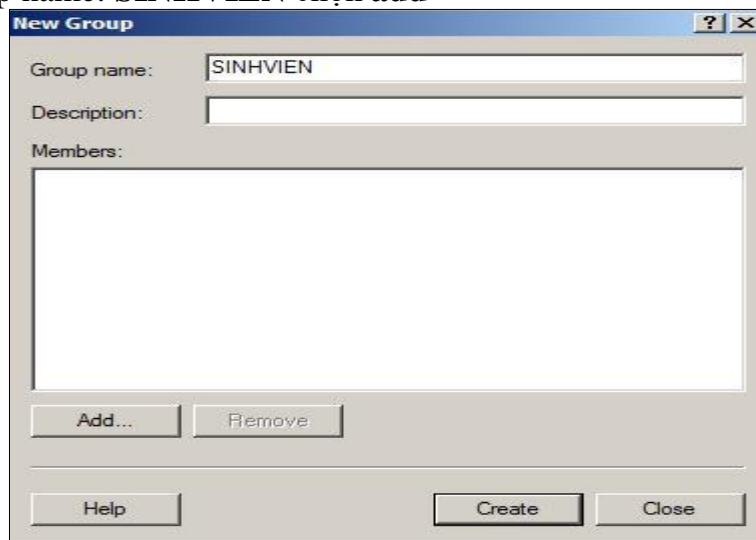
2. Tạo Local Group Account

B1: Vào **Start** chọn **run** gõ lệnh **lusrmgr.msc**

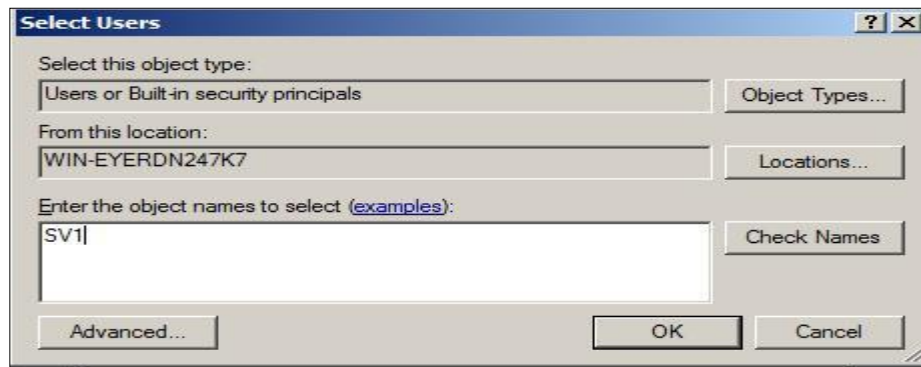
B2: Click phải chuột vào **Group** chọn **New group**



B3: Group name: **SINHVIEN** chọn **add**



B4: Hộp thoại **New group** chọn **add** gõ **SV1** chọn **Check name** chọn **ok**



B5: Quan sát thấy user **SV1** đã được **add** vào **Group SINHVIEN**

B6: Làm các bước trên tạo **Group GIAOVIEN** và add các user **GV1, GV2** vào

BÀI 2: LOCAL SECURITY POLICY

1. Password policy

B1: Log on bằng **administrator**

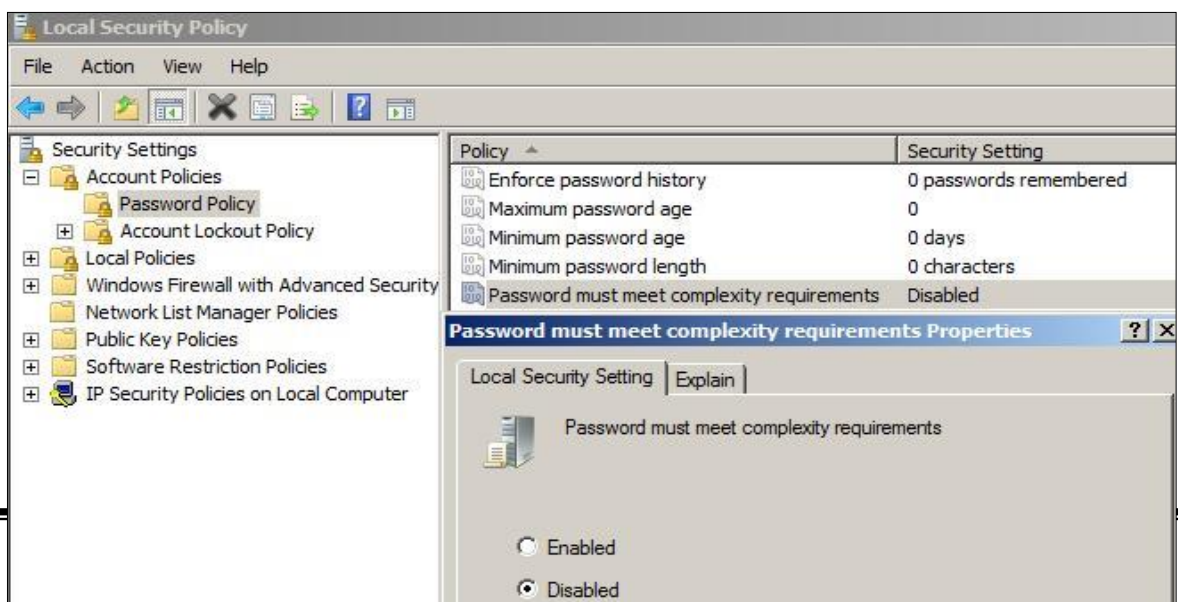
Tạo 1 user **U4** và password là : **123**

Báo lỗi không thể tạo được do không thỏa yêu cầu về độ phức tạp của password

B2: Vào **start** chọn **program** chọn **Administrative Templates** chọn **Local Security policy**

B3: Mở Account polices chọn password policy

Quan sát cột bên phải



B4:

Enforce password history: Số password hệ thống lưu trữ (khuyến dùng: 24)

Maximun password age: Thời gian hiệu lực tối đa của 1 password (khuyến dùng : 42)

Minimun password age: Thời gian hiệu lực tối thiểu của 1 password (khuyến dùng : 1)

Minimun password length: Độ dài tối thiểu của 1 password (khuyến dùng 7)

Password must meet complexity requirements: Yêu cầu password phức tạp (khuyến dùng: enable)

Chỉnh password policy:

- **Password must meet complexity requirements** chọn **disable**
- Các password policy còn lại chỉnh giá trị về **0** chọn **OK**
- Gõ lệnh **Gpupdate/Force**

Kiểm tra: tạo user **U4** với password **123** thành công

2. Account Lockout policy

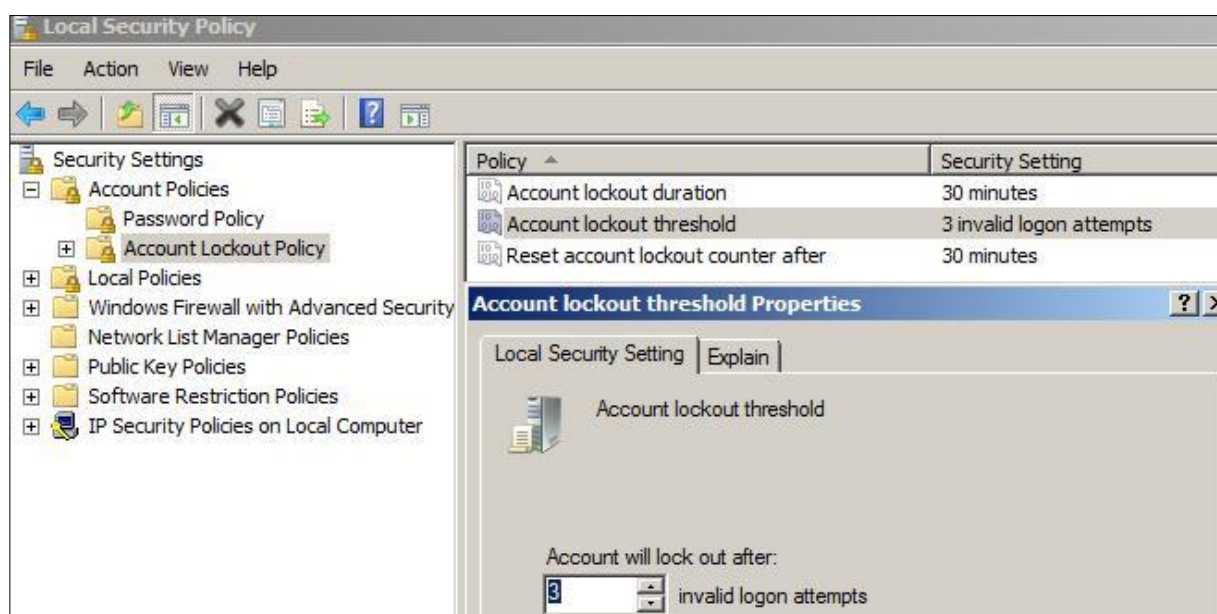
B1: Mở local security policy

B2: theo đường dẫn **Account policies** chọn **Account lockout policy**

- Quan sát các policy bên phải **Account lockout threahold** số lần nhập sai password trước khi account bị khóa
- **Account lockout duration:** Thời gian account bị khóa
- **Reset Account lockout counter after:** thời gian khởi động lại bộ đếm

B3: Chỉnh policy:

- **Account lockout threahold : 3**
- **Account lockout duration: 30**
- **Reset Account lockout counter after: 30**



Kiểm tra:

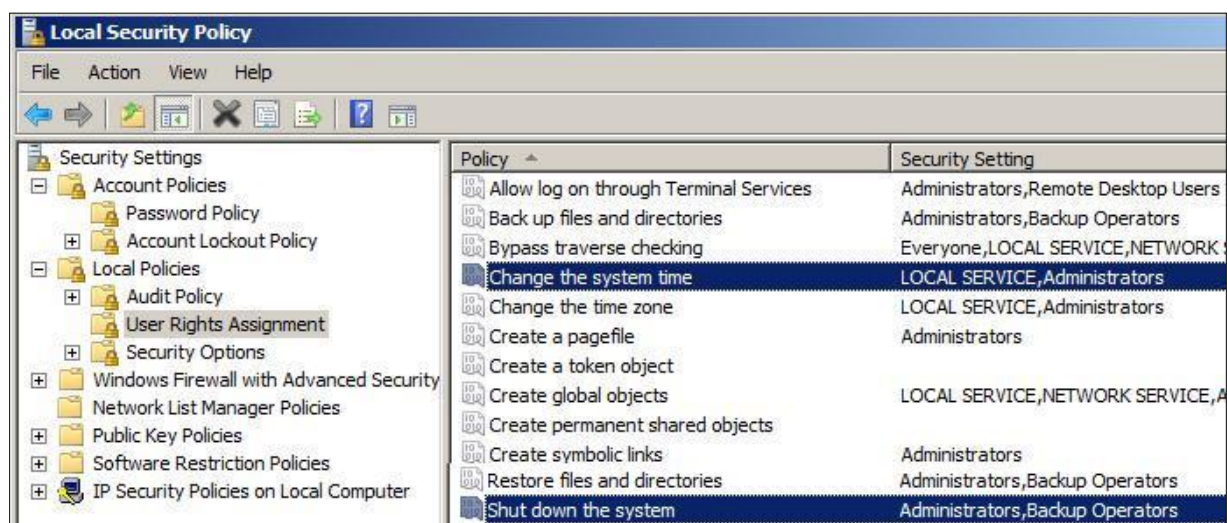
- Đăng nhập thử sai password **4** lần không thể đăng nhập được tiếp
- Chờ sau **30** phút có thể đăng nhập lại

3. user rights assignment

B1: - Log on bằng quyền U4 shut down Máy tính không được
 - Thay đổi ngày giờ hệ thống không được

B2: Log on bằng **administrator** mở **local security policy** chọn **local policies** chọn **user rights assignment** cột bên phải quan sát thấy có 2 policy.

- **Change the system time** : cho phép 1 user có quyền thay đổi ngày giờ hệ thống
- **Shutdown the system**: cho phép 1 user có quyền tắt máy



B3: Chỉnh policy:

- **Change the system time**: Đưa group users vào
- **Shutdown the system**: Đưa group user vào policy

Kiểm tra:

- Log on **U4** Shut down thử thành công
- Thay đổi ngày giờ hệ thống thành công

BÀI 3: SHARE PERMISSION

Việc chia sẻ các tài nguyên trên mạng là điều không thể thiếu trong bất kỳ hệ thống mạng nào, tuy nhiên việc chia sẻ này còn tùy thuộc vào nhu cầu người sử dụng & ý đồ của nhà quản trị mạng, ví dụ trong công ty chúng ta có nhiều phòng ban và các phòng ban trong công ty có nhu cầu chia sẻ tài nguyên cho nhau tuy nhiên nhà quản trị mạng muốn không phải phòng ban nào cũng có thể truy cập vô tư các dữ liệu của phòng ban khác.

Chẳng hạn các nhân viên trong phòng kinh doanh thì có thể truy cập dữ liệu của phòng mình và phòng kỹ thuật thoải mái, nhưng với các nhân viên trong phòng kỹ thuật chỉ được phép truy cập tài nguyên trong phòng mình mà thôi và không được phép truy cập các tài liệu từ phòng kinh doanh. Tính năng **Sharing and Security..** sẽ giúp ta giải quyết các yêu cầu trên.

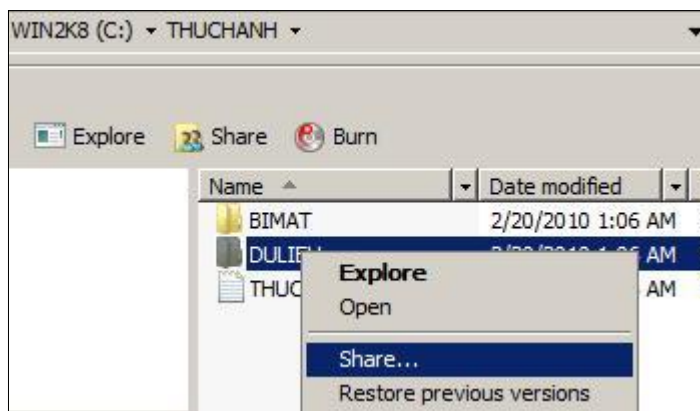
Chuẩn bị:

- Mô hình bài Lab gồm 2 máy
 - + **SERVER1** Windows Server 2019
 - + **CLIENT 1** Windows 7
- **PC01** Tạo 2 account **U1** và **U2** với password là :**123**
- Tạo Folder **THUCHANH** trong ổ đĩa **C**, trong thư mục **THUCHANH** tạo 2 Folder là **DULIEU** và **BIMAT**
- Trong các thư mục tạo file **thuchanh.txt** nội dung tùy ý
- Mở **windows explore** chọn **Tool** chọn **folder options** chọn **View** bỏ dấu chọn trước dòng **User Sharing Wizard**
- Trên 2 máy tắt **Firewall**, **UAC** và chương trình Virus. Kiểm tra đường truyền bằng lệnh **Ping**

Thực hiện:

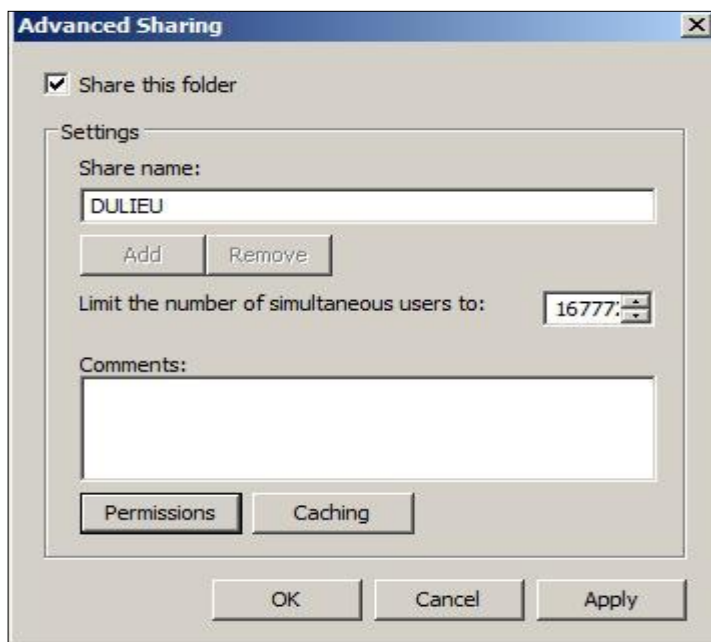
1. Share một Folder

B1: Vào thư mục gốc ổ đĩa **C** chọn Folder **DULIEU** Click chuột phải lên folder **DULIEU** chọn **Share**

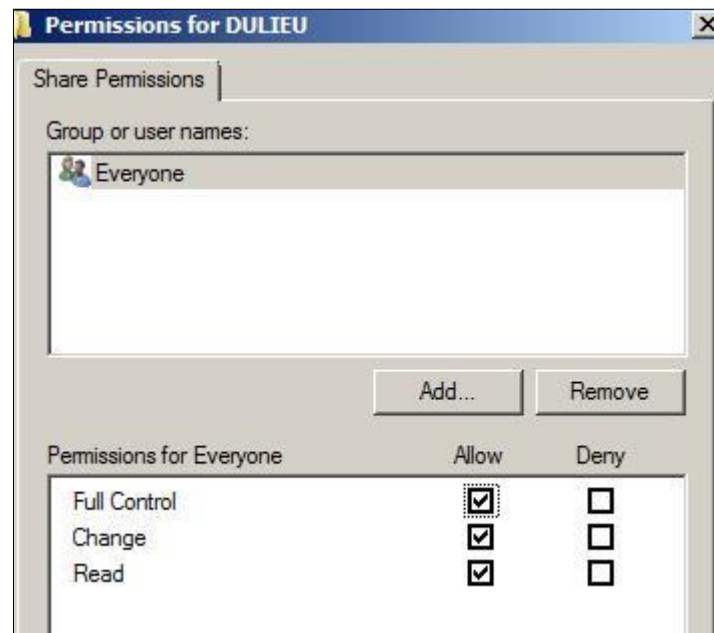


B2: Tại tab Share Click vào **Advanced Sharing....**

- Đánh dấu check vào **share this folder** click vào **Permissions**



Phía trên chọn **Everyone** phía dưới check vào **Allow full control** chọn **OK**



B3: Tại máy **CLIENT 1** chọn Menu **Start** chọn **Run** gõ: [\\SERVER1](#) (Tên máy của server) chọn **OK**

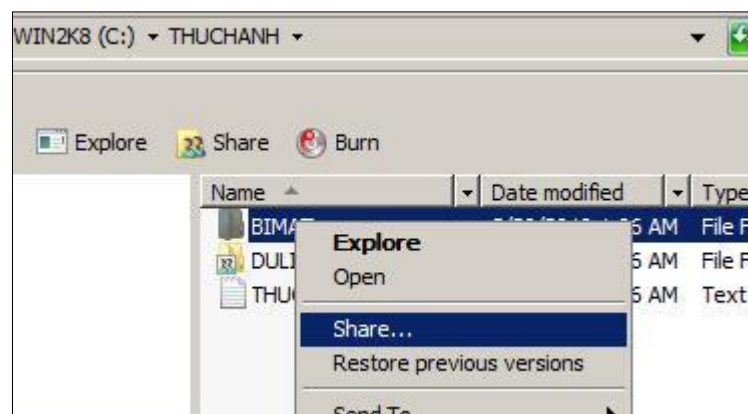
Hộp thoại yêu cầu chứng thực khi đăng nhập điền vào **user name: U1** và **Password 123**

Truy cập thành công thấy Folder **DULIEU**

2. Share ẩn một folder

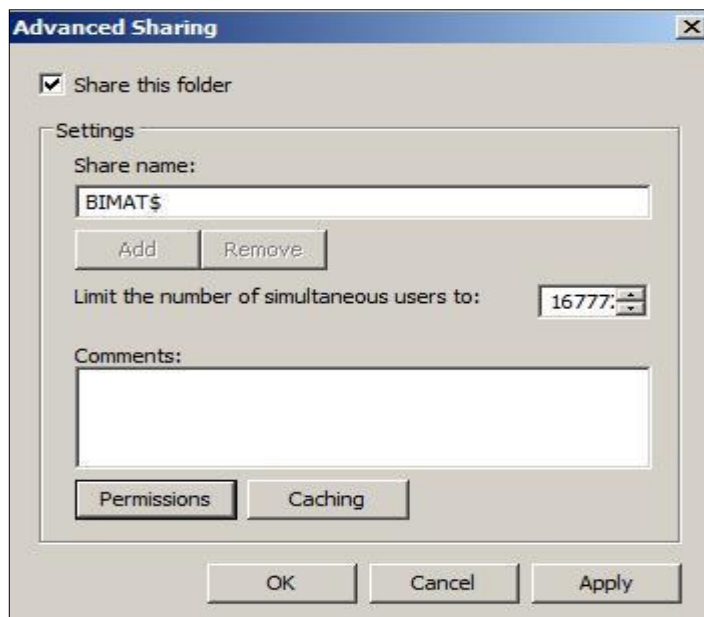
Thực hiện trên **PC01**:

B1: Click chuột phải lên folder **BIMAT** chọn **Share**

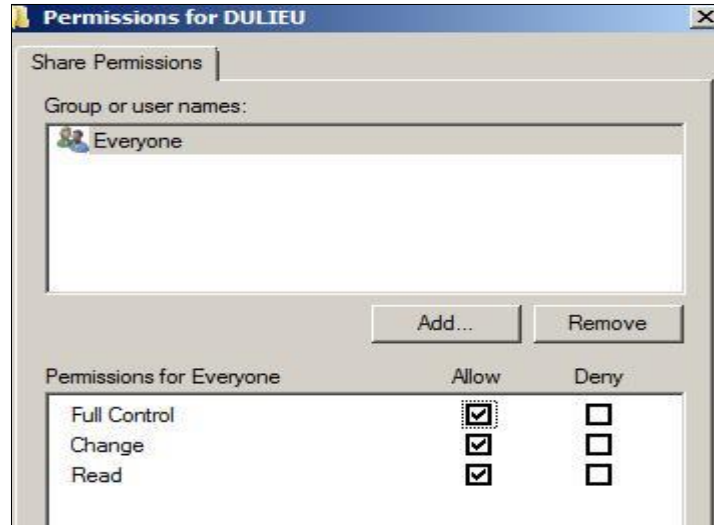


B2: Tại tab Sharing Click chọn vào **Advanced Sharing....**

- Đánh dấu check vào **share this folder**
- **Khung Share name** Thêm vào **BIMAT\$** Chọn vào **Permissions**

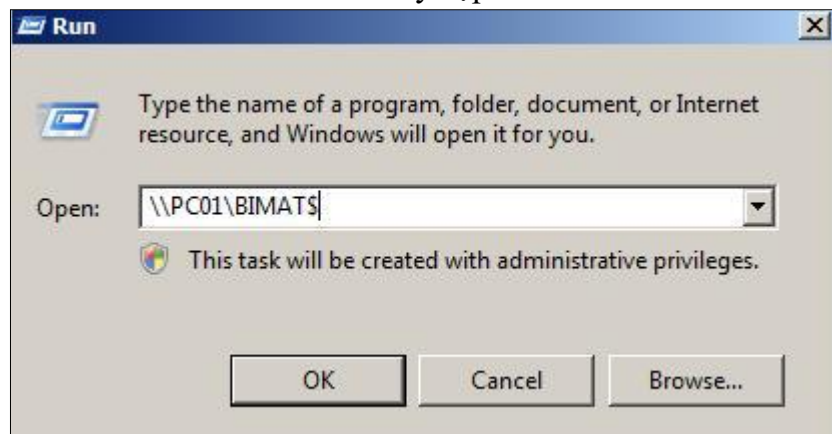


Phía trên chọn **Everyone** phía dưới check vào **Allow full control** chọn **OK**



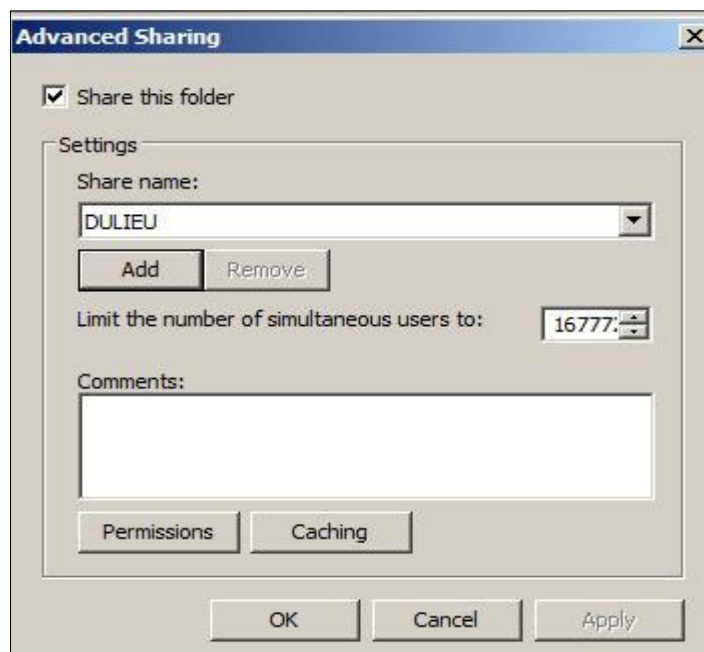
B3: Tại máy PC02 chọn menu **Start** chọn **Run** nhập vào [\\server1](#) (tên máy server) truy cập vào không thấy folder **BIMAT**

- Tắt cửa sổ explorer truy cập lại PC01 **Start** chọn **Run** nhập vào `\\server1\BIMAT$`
Gõ user name: U1 và Password 123 Truy cập vào Folder **BIMAT** thành công

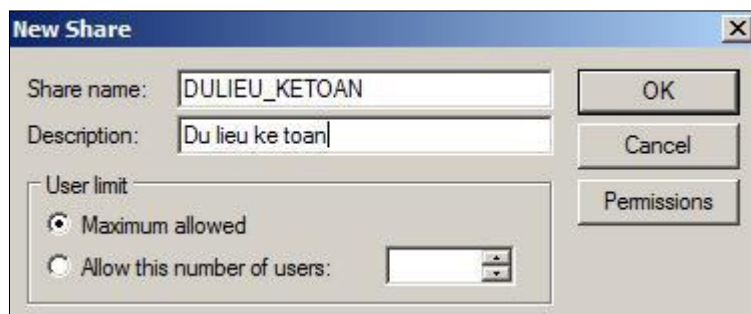


3. Share một folder với nhiều tên

B1: Click chuột phải lên folder **DULIEU** chọn **Share** chọn **Advanced Sharing....**
Click vào **Add**.



B2: Khung **share name** nhập vào **DULIEU_KETOAN** Chọn **Ok**



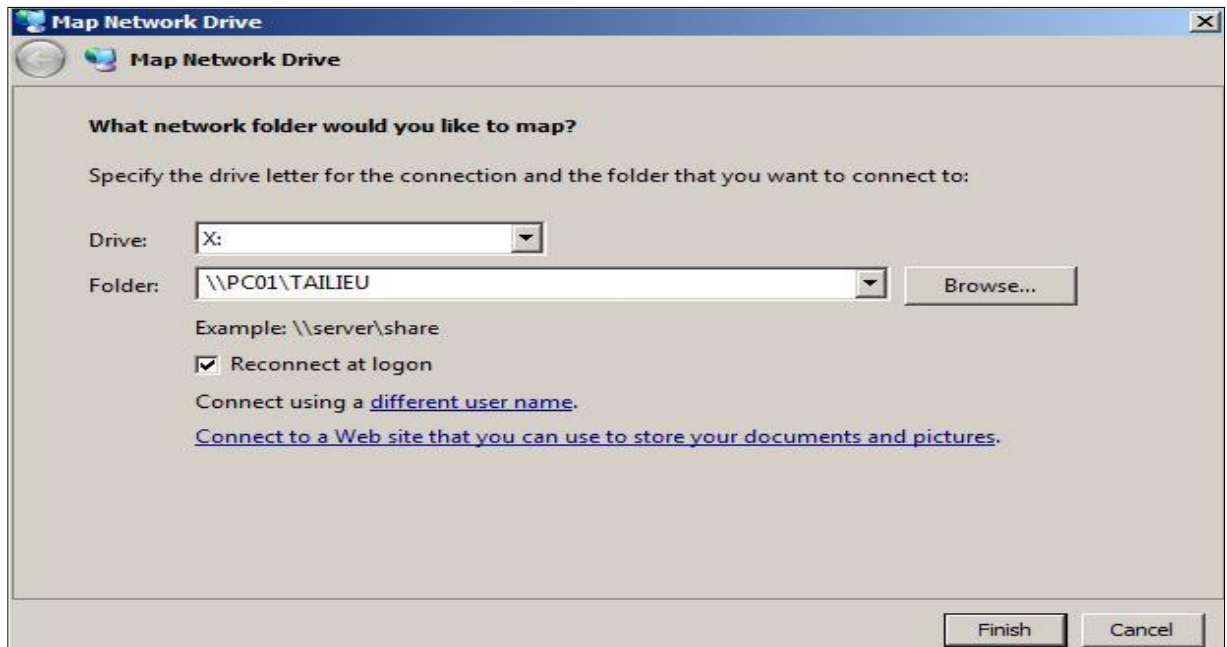
B3: Kiểm tra trong hộp thoại **Advanced Sharing**, phần **Share name** có 2 tên **DULIEU** Và **DULIEU_KETOAN**

4. Gán tên ổ đĩa mạng để truy cập các shared folder

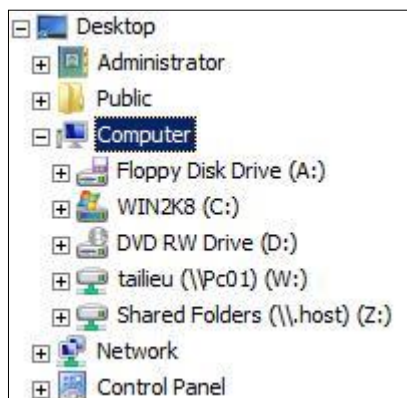
B1: Share thư mục **TAILIEU** trên đĩa **C**

B2: Click chuột vào folder **TAILIEU** chọn vào **Tool** Chọn vào **Map network drive..**

- **Driver:** Chọn tên ổ đĩa
- **Folder:** gõ vào **\\tên PC\tên thư mục Share** sau đó chọn **Finish**

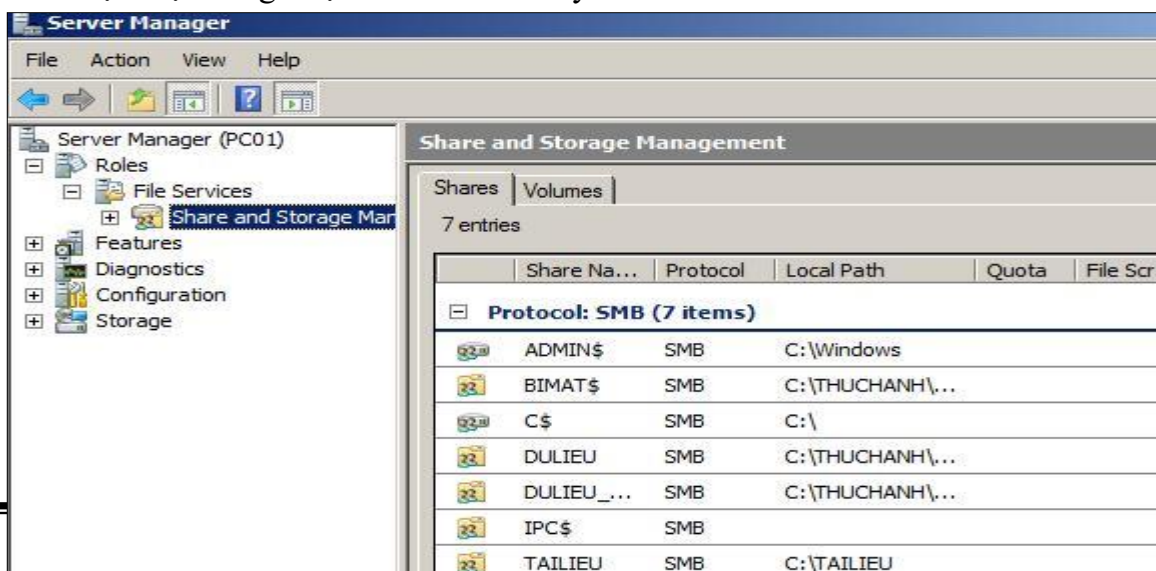


B3: Mở Windows explore kiểm tra đã có ổ đĩa mạng **DULIEU(W)**



5. Quản lý các Share Resources

Click chuột phải lên biểu tượng **Computer** ngoài **Desktop** Chọn **Manage** chọn vào **Role** chọn vào **file services** chọn vào **share and storage management** Quan sát bên tay phải các dữ liệu hiện đang được chia sẻ trên máy tính

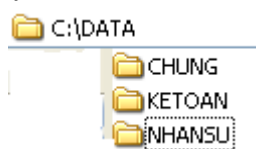


BÀI 4: NTFS PERMISSION

Như chúng ta đã biết khi chia sẻ tài nguyên qua mạng (Share) User sẽ chịu tác động của **Permission** có quyền hay bị giới hạn quyền do **Administrator** phân quyền. Nhưng nó chỉ có tác dụng nếu User đó từ máy **Client** truy cập vào còn nếu User đó ngồi trên **Server** thì mọi tác động của **Share Permission** hoàn toàn vô nghĩa, vì thế để giới hạn quyền của User tại local người ta sử dụng **NTFS Permission** Khi đó khi User truy cập vào một tài nguyên nào đó đó mạng sẽ chịu tác động của 2 Permission là **Share Permission & NTFS Permission** Trong khi đó nếu truy cập tại local sẽ chỉ chịu tác động của **NTFS Permission** .

Điều kiện để sử dụng **NTFS Permission** là **Partition** của bạn phải được format định dạng file system là **NTFS**.

Chuẩn bị: Tạo cây thư mục như hình dưới



- Tạo 2 Group: **KETOAN, NHANSU**
- Tạo 2 User : **KT1, KT2** Add 2 user này vào Group **KETOAN**
- Tạo 2 User : **NS1, NS2** Add 2 user này vào Group **NHANSU**

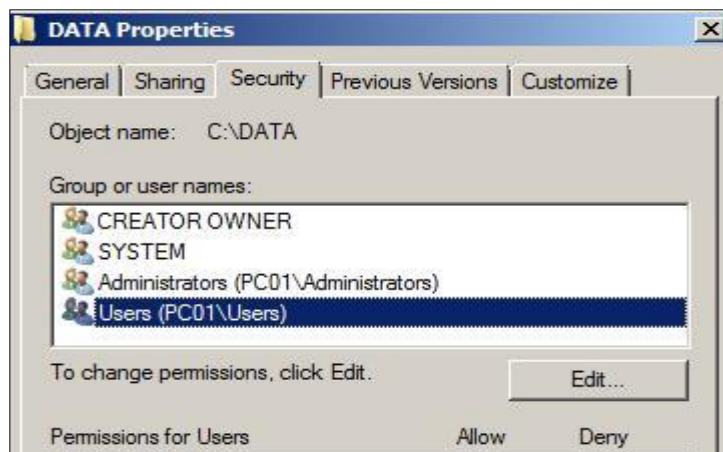
Phân quyền thư mục bằng Standard Permission

Phân quyền cho các **Group** như sau

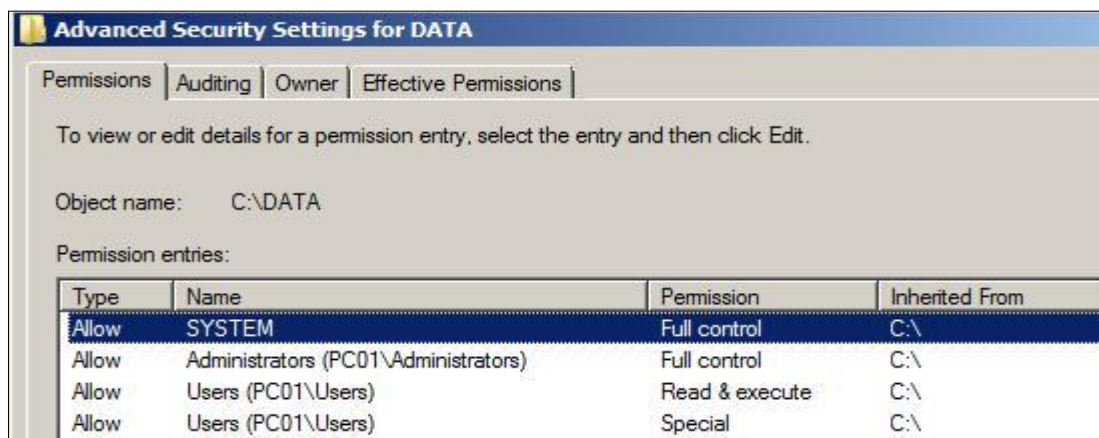
- Trên thư mục **Data**:
 - + Group **Ketoan** và **Nhansu** có quyền **Read**
- Trên thư mục **Chung**:
 - + Group **Ketoan** và **Nhansu** có quyền **Full**
- Trên thư mục **Ketoan**:
 - + Group **Ketoan** có quyền **Full**
 - + Group **Nhansu** không có quyền
- Trên thư mục **Nhansu**:
 - + Group **Nhansu** có quyền **Full**
 - + Group **Nhansu** không có quyền

1. Phân quyền trên thư mục DATA

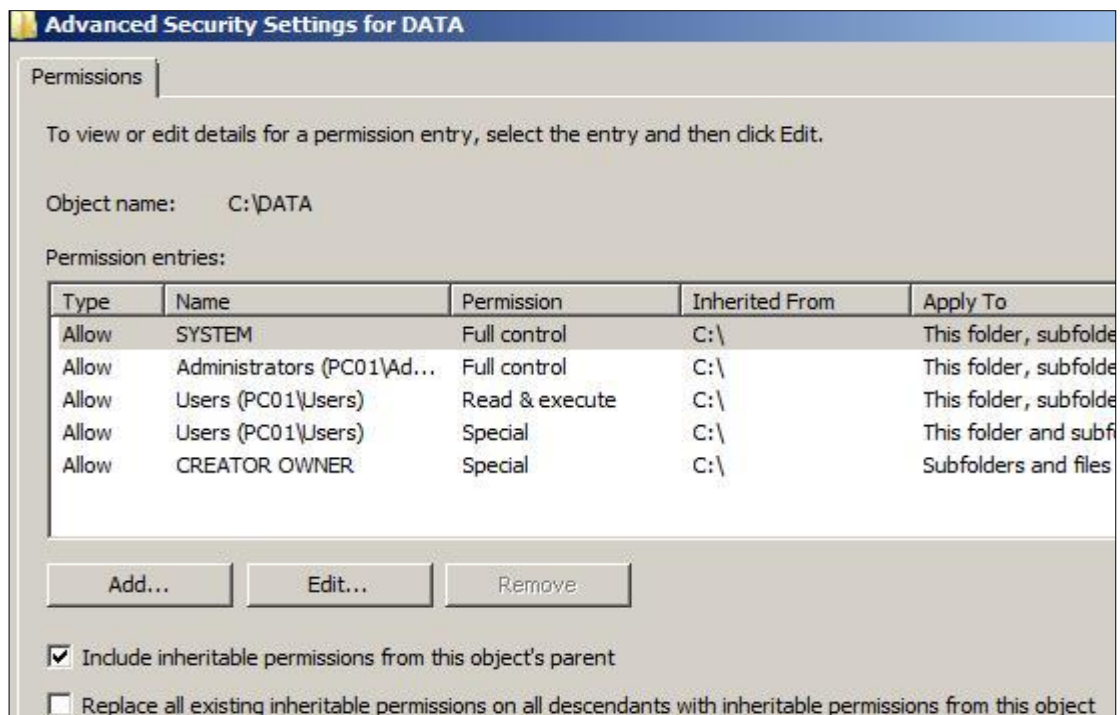
B1: Click chuột phải lên thư mục **DATA** chọn **Properties** qua tab **Security** chọn **Advanced**



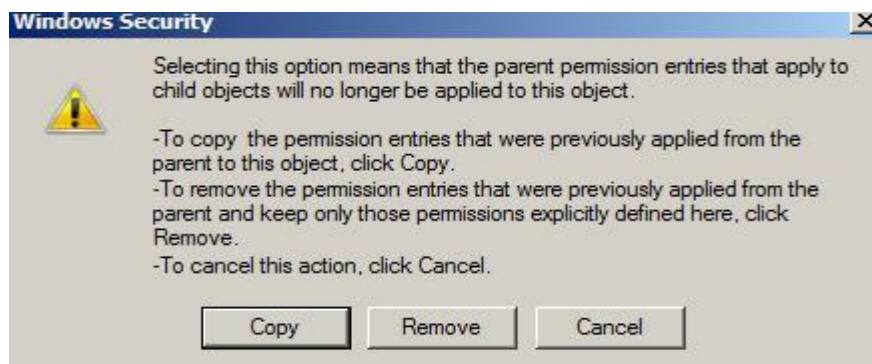
B2: Trang tab **Permissions** chọn **Edit**



B3: Bỏ dấu check trước dòng **Include inheritable permissions from this object's parent**



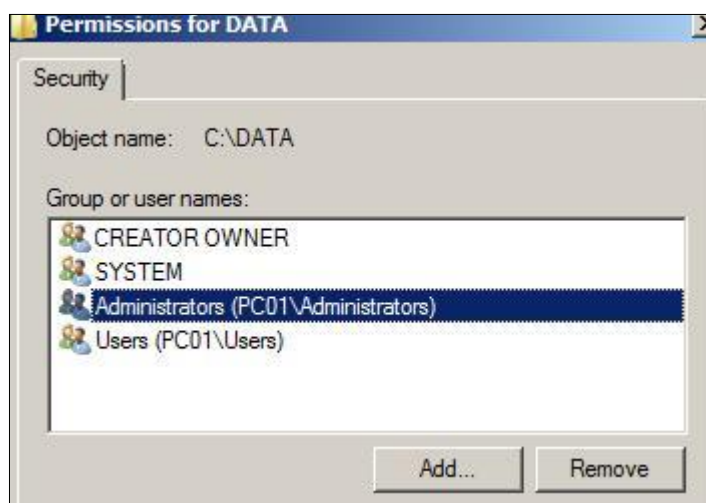
B4: Màn hình **Windows security** chọn **copy** chọn **OK-OK**



B5: Tại màn hình **DATA properties** chọn **Edit**



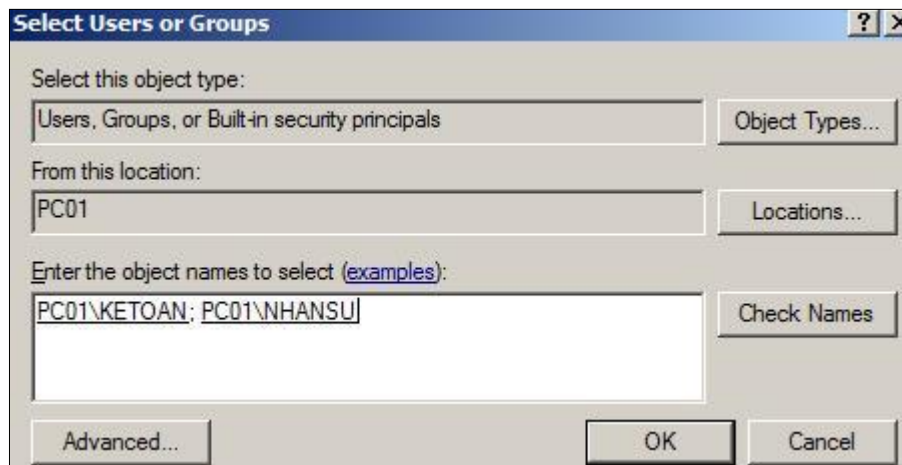
B6: Màn hình **Permissions for DATA** chọn **Add**



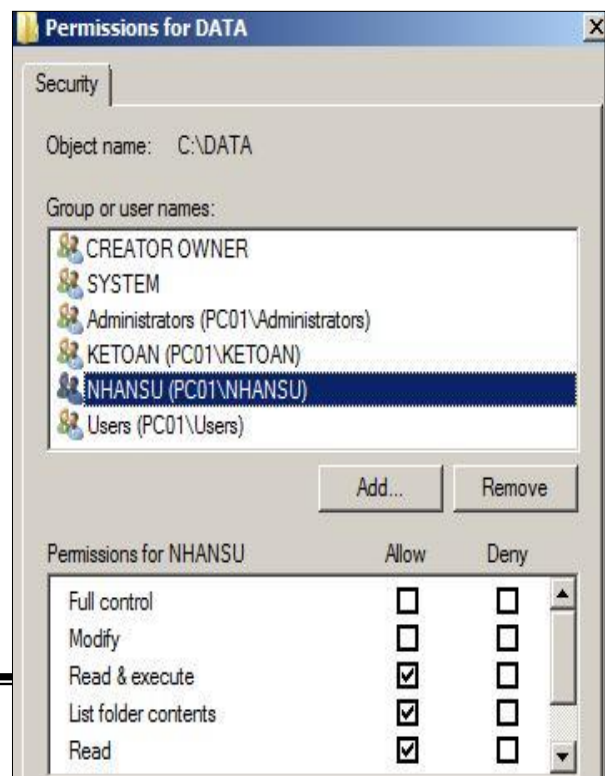
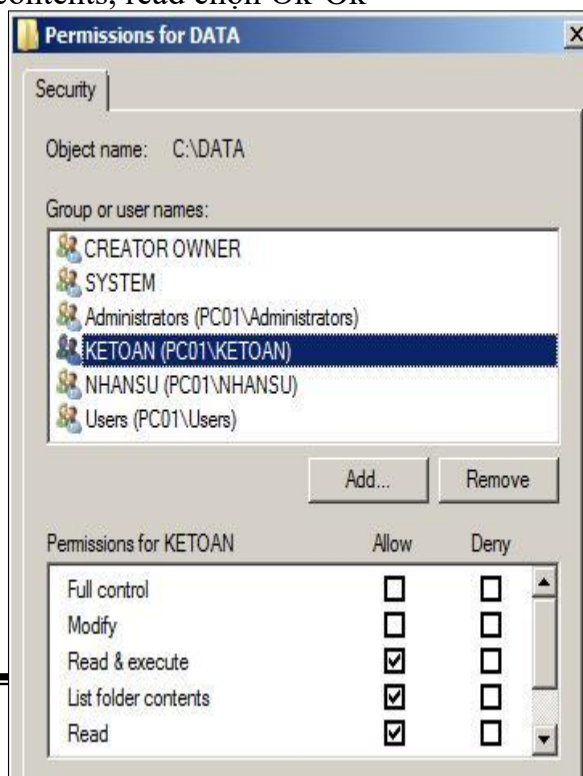
B7: Trong khung **Enter the object names to select** gõ **KETOAN ; NHANSU** Chọn **check names**



B8: Quan sát thấy **KETOAN** Và **NHANSU** đã được gạch chân xác định group **KETOAN** Và **NHANSU** có tồn tại chọn **OK**



Quan sát thấy **KETOAN** và **NHANSU** có 3 quyền Allow: Read & excute, List folder contents, read chọn Ok-Ok

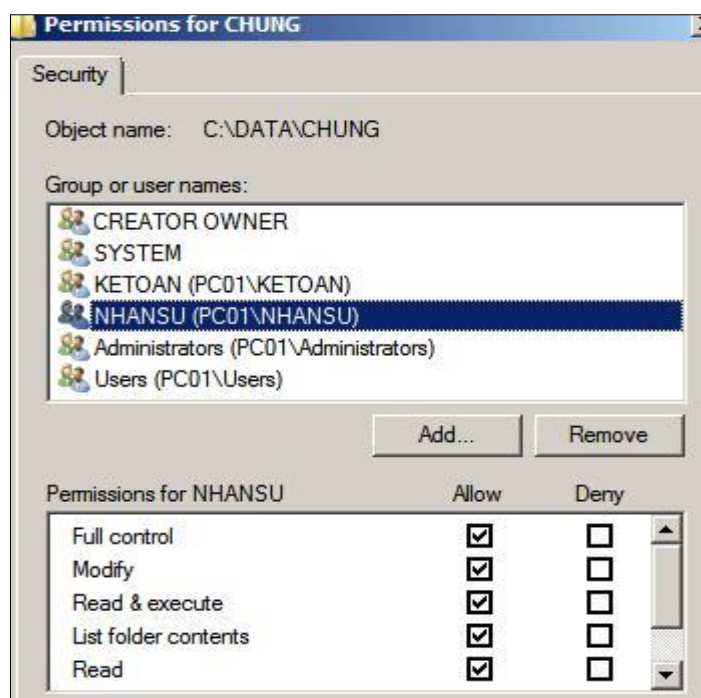
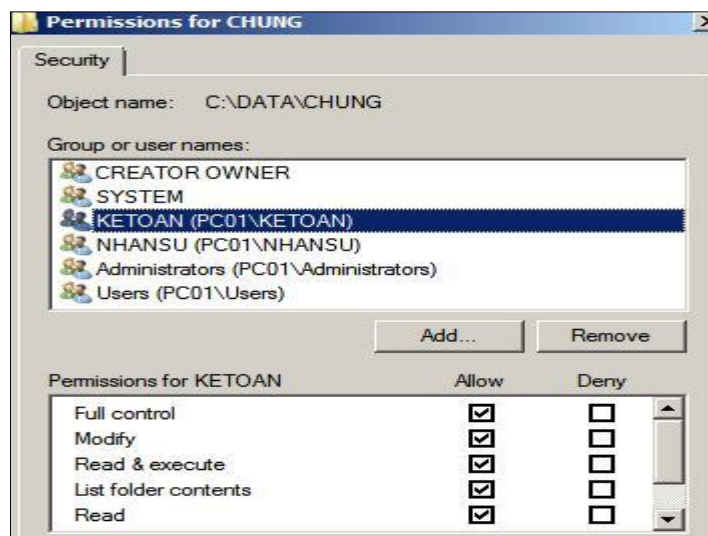


Kiểm tra:

- Lần lượt log on vào máy bằng quyền **KT1,NS1** mở thư mục **c:\DATA** truy cập thành công
- Tạo Folder bất kỳ xuất hiện thông báo lỗi không có quyền

2. Phân quyền cho thư mục Chung

B1: Log on **Administrator** click chuột phải lên thư mục chung chọn **Properties** qua tab **security** chọn **Edit** Lần lượt chọn từng Group **Ketoan** và **Nhansu** cho quyền **Allow full control** chọn Ok-OK

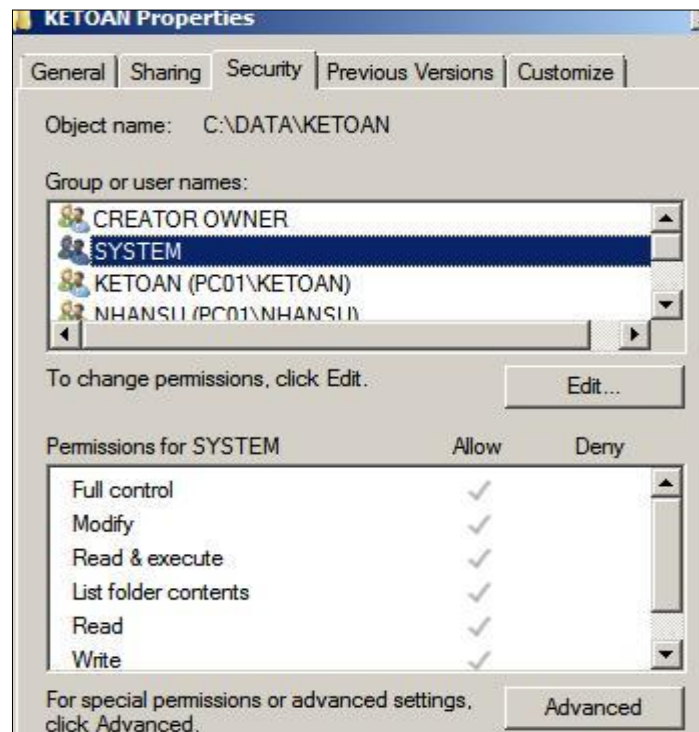


B2: Kiểm tra:

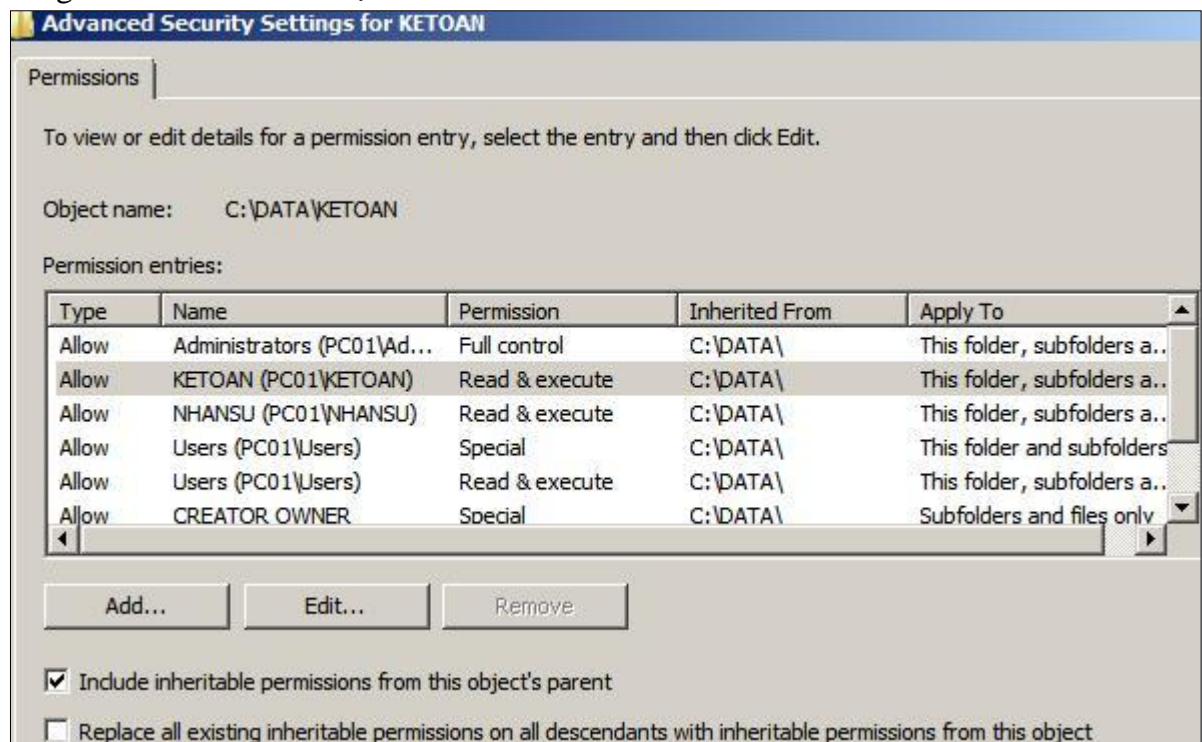
- Lần lượt log on vào bằng **KT1, NS1** truy cập vào thư mục **Chung** truy cập thành công
- Tạo xóa, folder bất kỳ trong thư mục **chung** thành công

3. Phân quyền cho mục KETOAN

B1: Click chuột phải lên thư mục **KETOAN** chọn **Properties** qua tab **security** chọn **advanced**

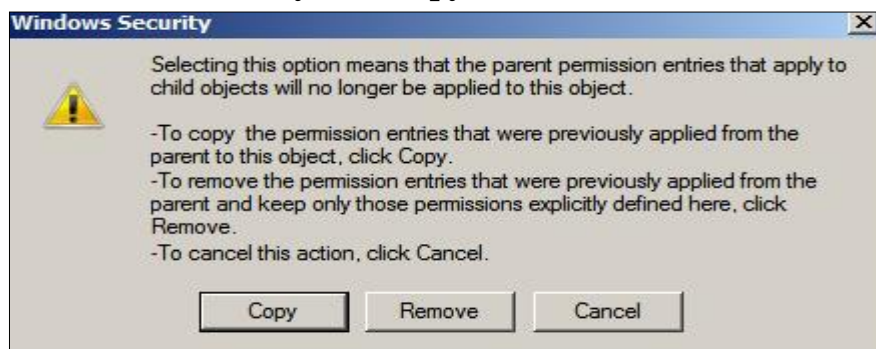


B2: Trong tab **Permissions** chọn **Edit**

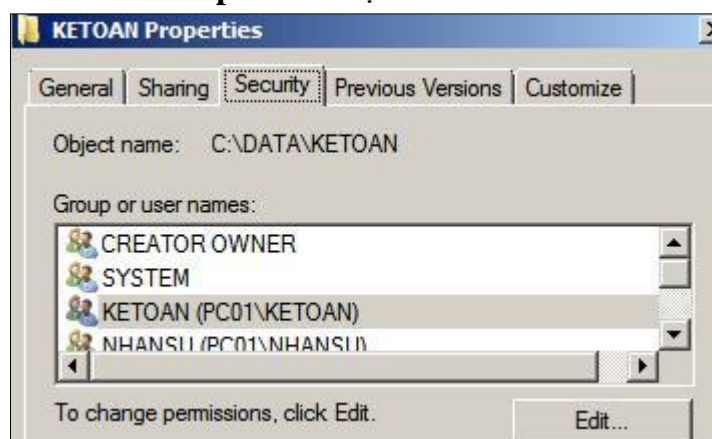


B3: Bỏ dấu check trước dòng **Include inheritable permissions from this object's parent**

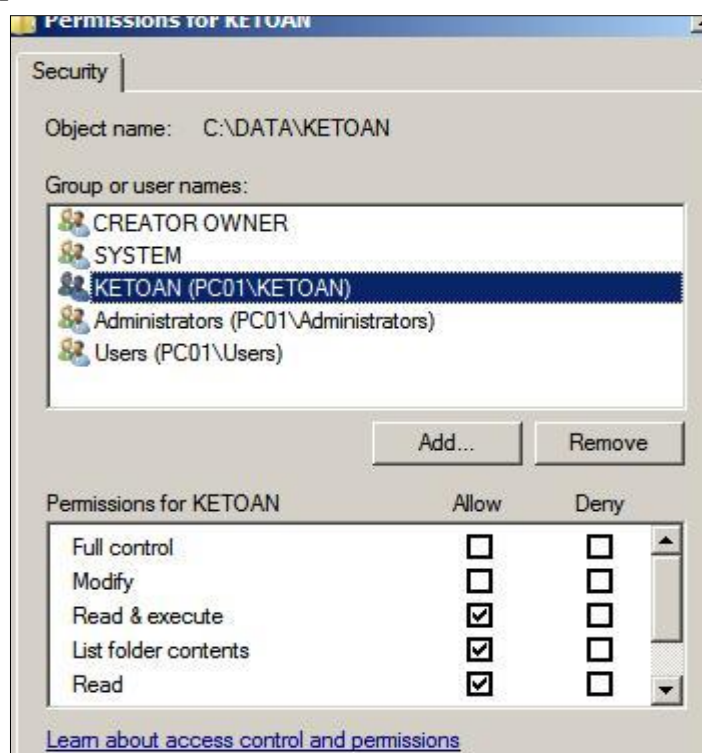
B4: Màn hình **Windows security** chọn **copy** chọn **OK-OK**



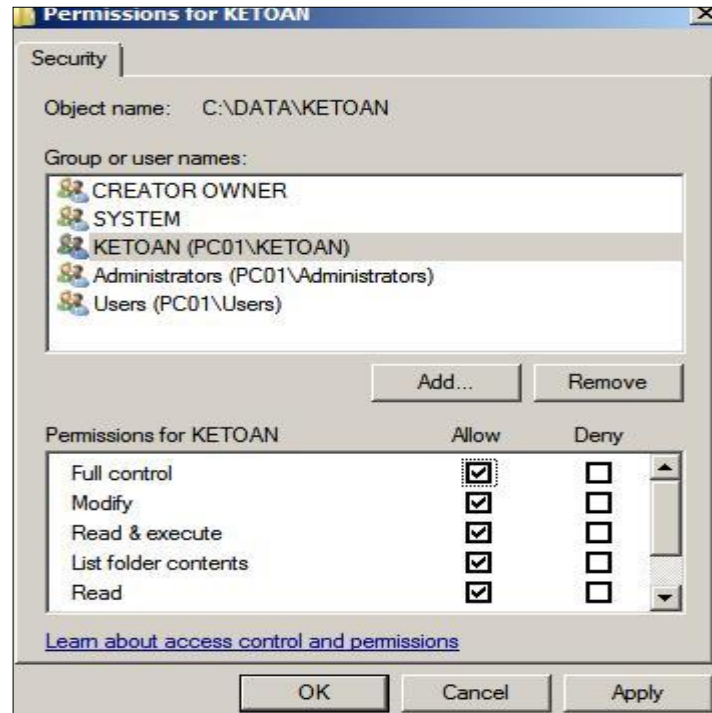
B5: Tại màn hình **KETOAN Properties** chọn **Edit**



B6: Chọn Group **NHANSU** chọn **Remove**



B7: Chọn Group **KETOAN** chọn **allow full control** chọn **ok-ok**

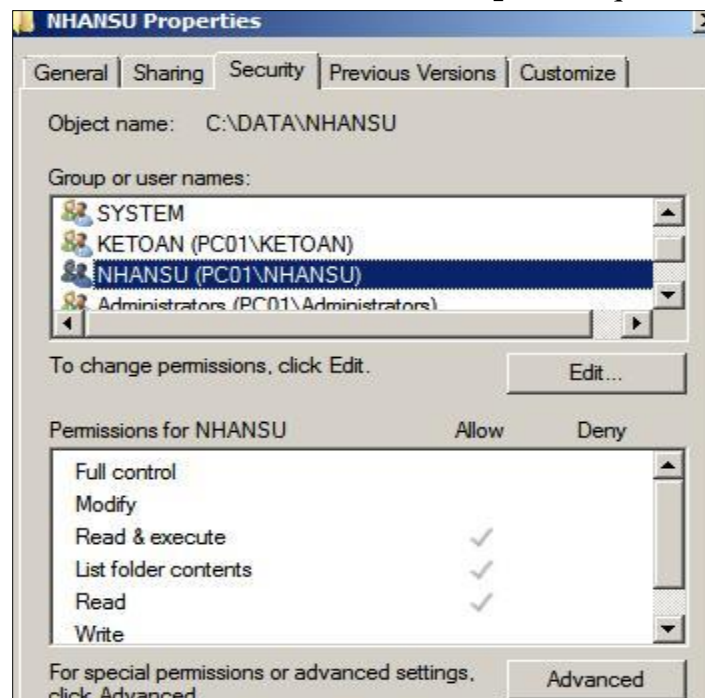


Kiểm tra:

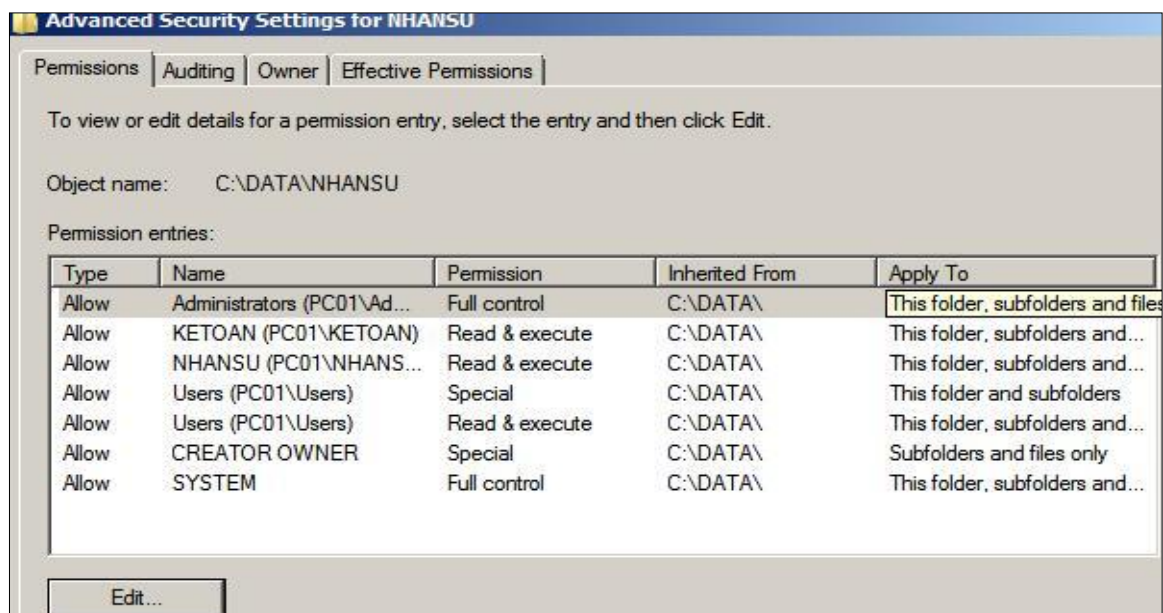
- Lần lượt log on vào bằng **KT1**, **NS1** truy cập vào thư mục **KETOAN** chỉ có **KT1** truy cập thành công, còn **NS1** không truy cập được.
- User **KT1** Tạo, xóa file, folder bất kỳ trong thư mục **KETOAN** thành công

4. Phân quyền trên thư mục NHANSU

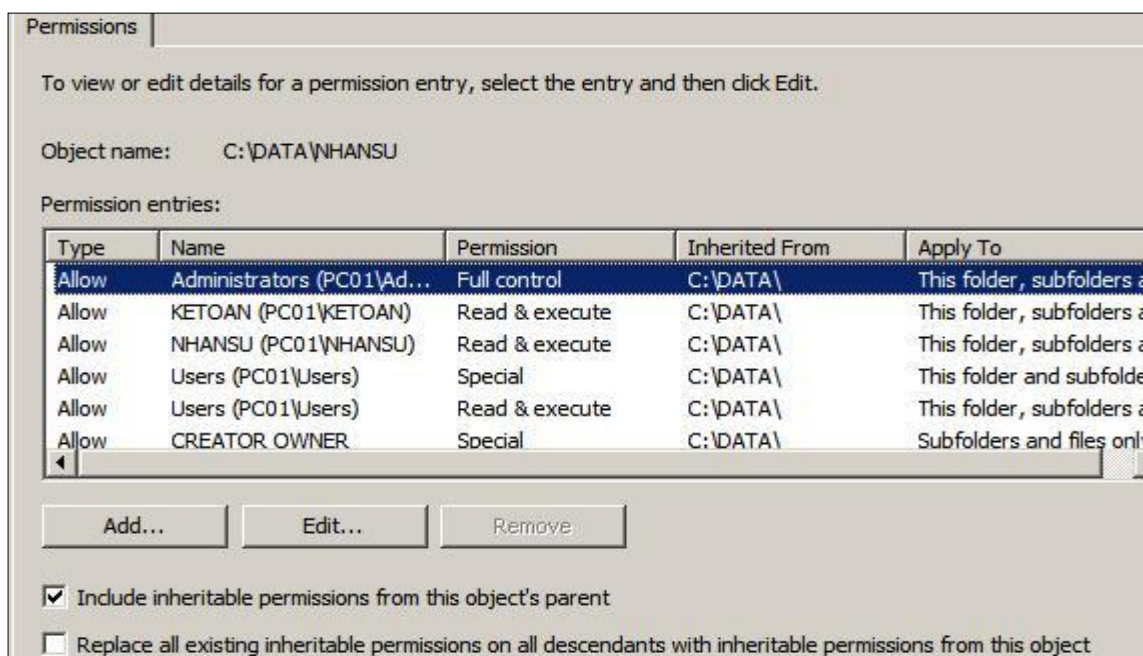
B1: Click chuột phải lên thư mục **NHANSU** chọn **Properties** qua tab **security** chọn **advanced**



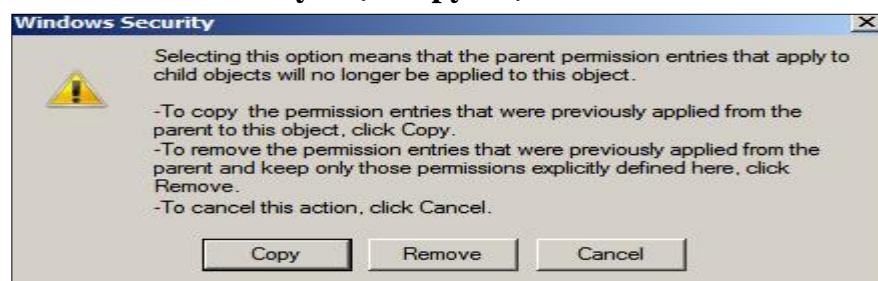
B2: Trong tab **Permissions** chọn **Edit**



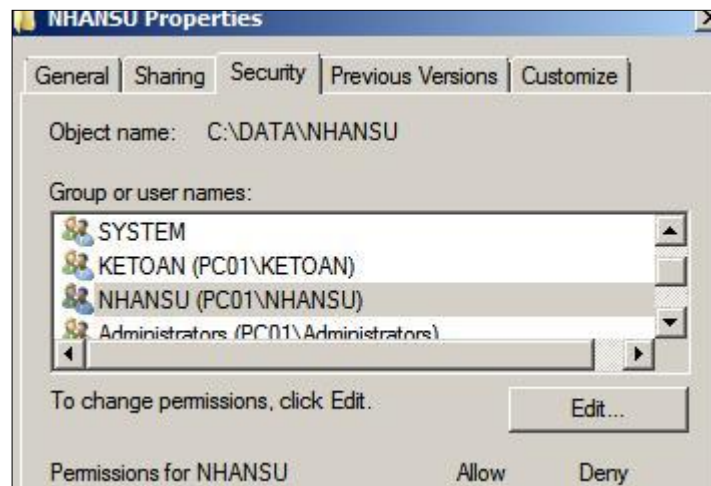
B3: Bỏ dấu check trước dòng **Include inheritable permissions from this object's parent**



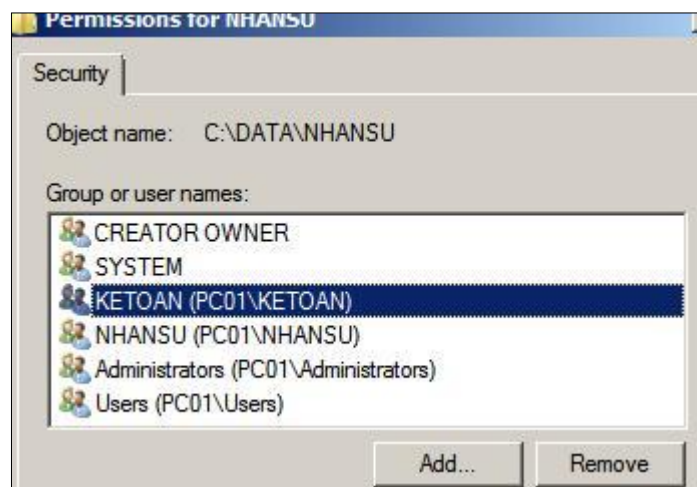
B4: Màn hình **Windows security** chọn **copy** chọn **OK-OK**



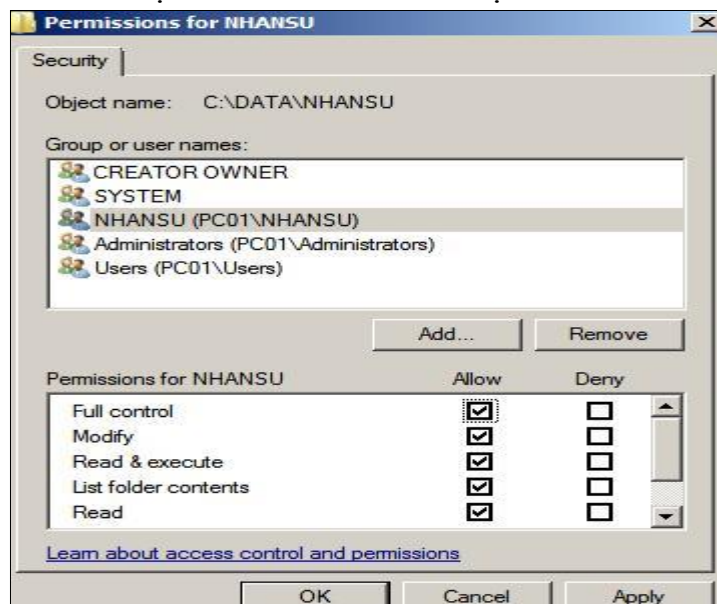
B5: Tại màn hình **NHANSU Properties** chọn **Edit**



B6: Chọn Group **KETOAN** chọn **Remove**



B7: Chọn Group **NHANSU** chọn **allow full control** chọn **ok-ok**



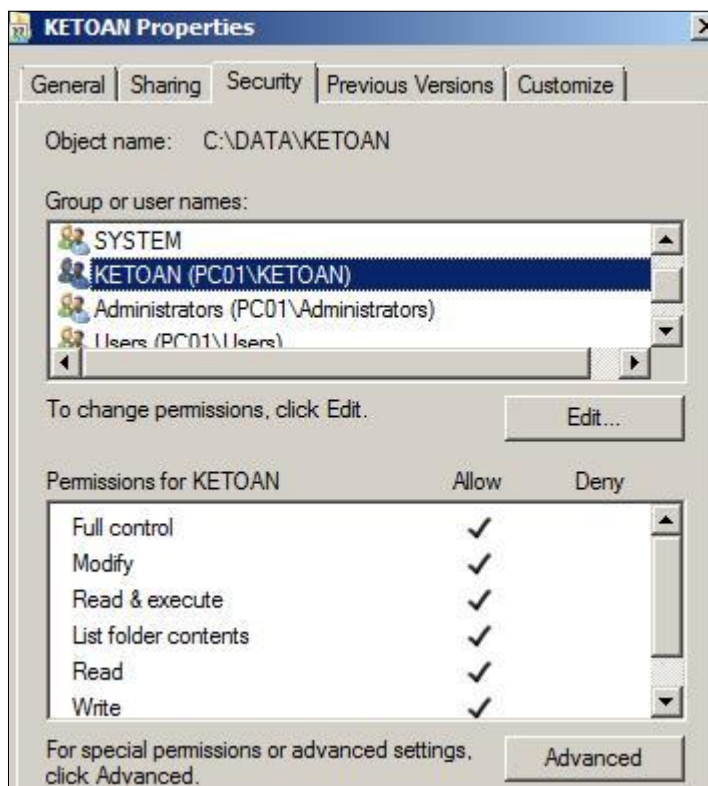
Kiểm tra:

- Lần lượt log on vào bằng **KT1**, **NS1** truy cập vào thư mục **NHANSU** chỉ có **NS1** truy cập thành công, còn **KT1** không truy cập được.
- User **NS1** Tạo, xóa file, folder bất kỳ trong thư mục **NHANSU** thành công

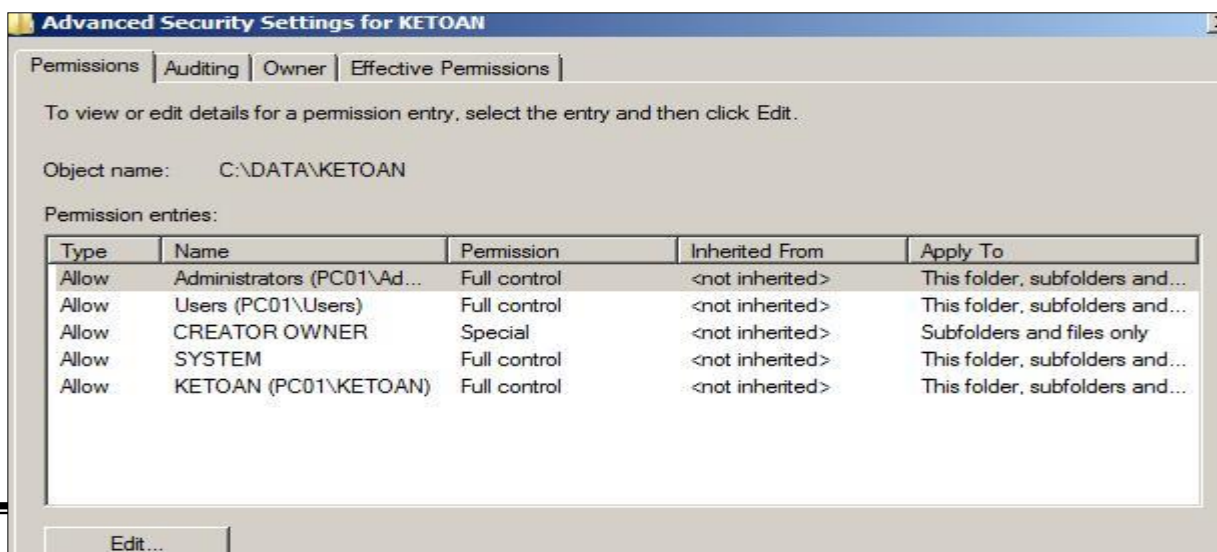
Phân quyền thư mục bằng Special Permission

Phân theo yêu cầu: File do user nào tạo ra User đó mới xóa được

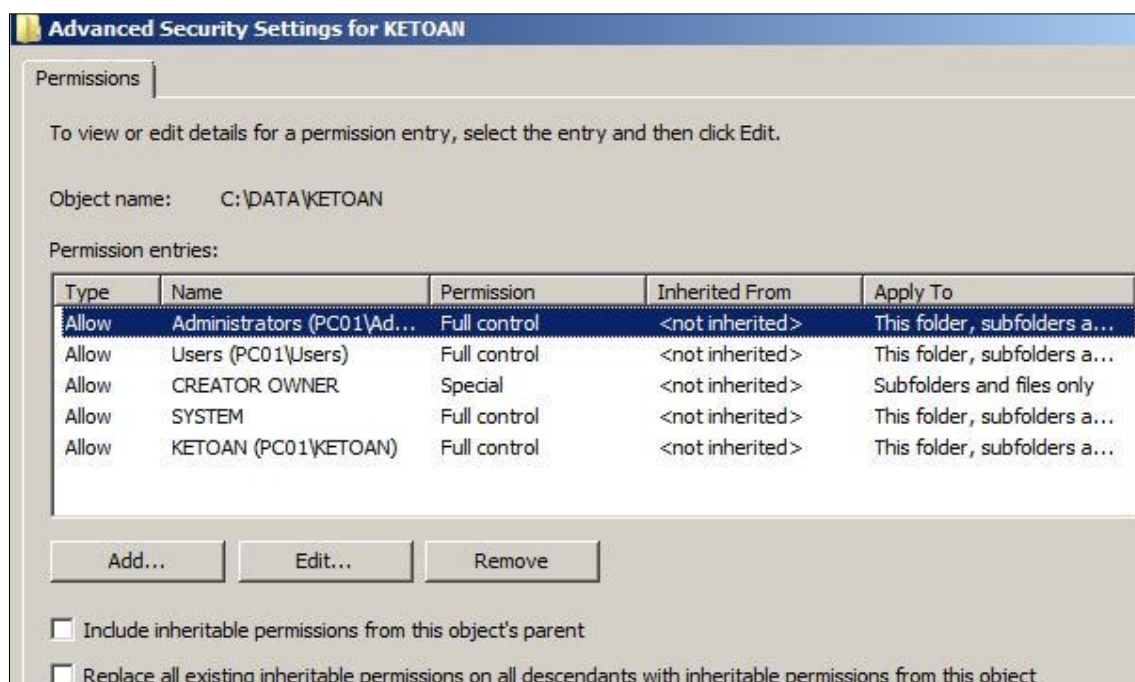
B1: Click chuột phải lên thư mục **KETOAN** chọn **Properties** qua tab **security** chọn **advanced**



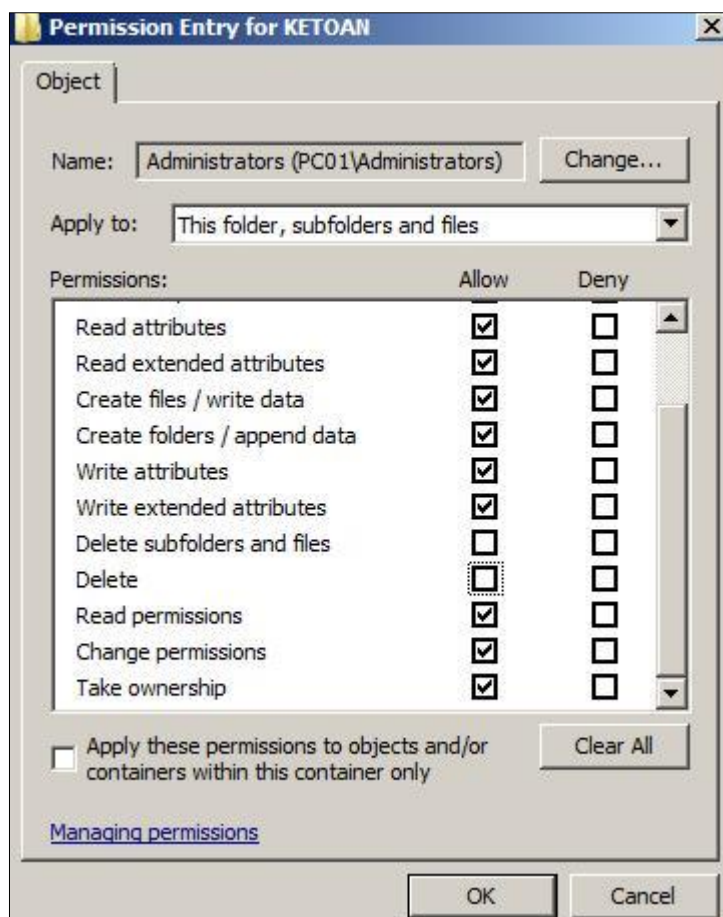
B2: Trong tab **Permissions** chọn Group **KETOAN** Chọn **edit**



B3: Tại màn hình **advanced security Setting for KETOAN**, Chọn group **KETOAN** chọn **edit**



B4: Ở mục **Allow**, tắt dấu check ở **Delete subfolders and file** và **delete** chọn ok 3 lần



B5: Kiểm tra:

- Lần lượt log on vào bằng **KT1**, **KT2** truy cập vào thư mục **KETOAN**
- **KT1** tạo file **KT1.txt**
- **KT2** tạo file **KT2.txt**
- Log on **KT1** xóa file **KT2.txt** báo lỗi không có quyền xóa. Xóa file **KT1.txt** thành công.
- Log on **KT2** xóa file **KT1.txt** báo lỗi không có quyền xóa. Xóa file **KT2.txt** thành công.

BÀI 5: DOMAIN

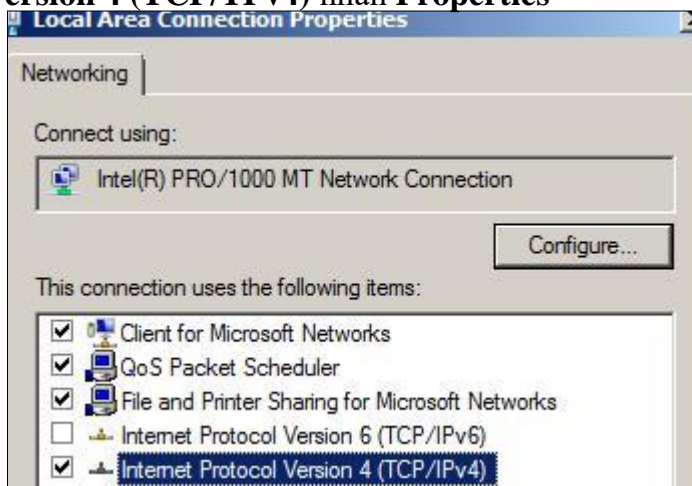
Trong các bài trước chúng ta đã học về các vấn đề như tạo user Account trên server. Hãy tưởng tượng trong công ty bạn có khoảng 5 máy tính với mỗi máy chúng ta sẽ tạo các User Account cho nhân viên truy cập. Tuy nhiên nếu người dùng đăng nhập vào máy 1 để làm việc sau đó anh ta sang máy thứ 2 làm việc thì mọi tài nguyên do anh ta tạo trên máy 1 hoàn toàn độc lập với máy 2 và thậm chí với từng máy Admin phải tạo các User Account giống nhau anh ta mới truy cập được, mọi chuyện sẽ không trở nên quá rắc rối nếu công ty chúng ta có chừng ấy máy. Nhưng nếu công ty bạn có khoảng 100 máy thì mọi chuyện lại khác, vấn đề đặt ra là chả lẽ mỗi máy Admin phải ngồi tạo **100 Account** để nhân viên truy cập? và vì mỗi máy độc lập với nhau việc tìm lại dữ liệu trên máy mà ta từng ngồi làm việc trước đó là cực kỳ khó khăn.

Do đó **Windows** đã có tính năng là **Domain Controller (DC)** giúp ta giải quyết rắc rối trên. Điều kiện để có một **DC** là bạn phải trang bị một máy **Server** riêng được gọi là máy **DC** các máy còn lại được gọi là máy **Client**, cả hệ thống được gọi là **Domain** Khi đó Administrator chỉ việc tạo User Account ngay trên máy **DC** mà thôi nhân viên công ty dù ngồi vào bất cứ máy nào trên **Domain** đều có thể truy cập vào **Account** của mình mà các tài nguyên anh ta tạo trước đó đều có thể dễ dàng tìm thấy.

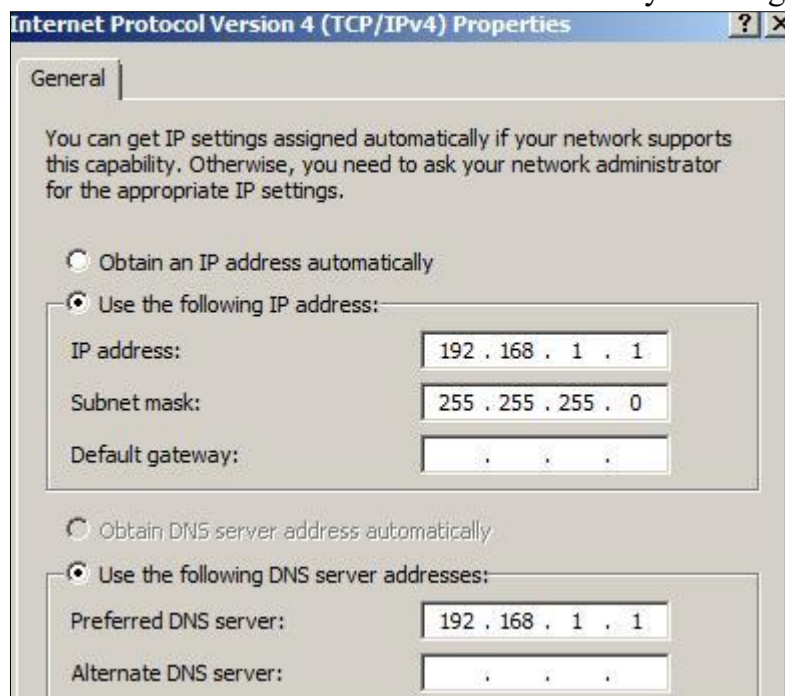
1. Nâng cấp Domain Controller

B1: Chỉnh IP

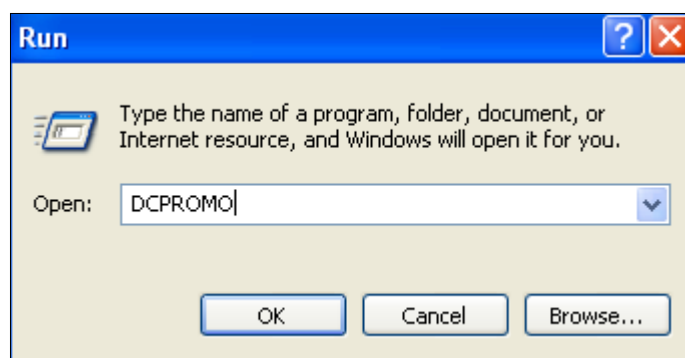
- Menu **start** chọn **setting** chọn **network Connections** click chuột phải vào **card** mạng Lan chọn **Properties** bỏ dấu check **internet Protocol Version 6 (TCP/IPv6)** chọn **internet Protocol Version 4 (TCP/IPv4)** nhấn **Properties**



B2: Điều chỉnh **Preferred DNS server** về IP của chính số máy mình ngồi chọn **OK**



B3: Vào menu **Start** chọn **Run** đánh lệnh **DCPROMO**



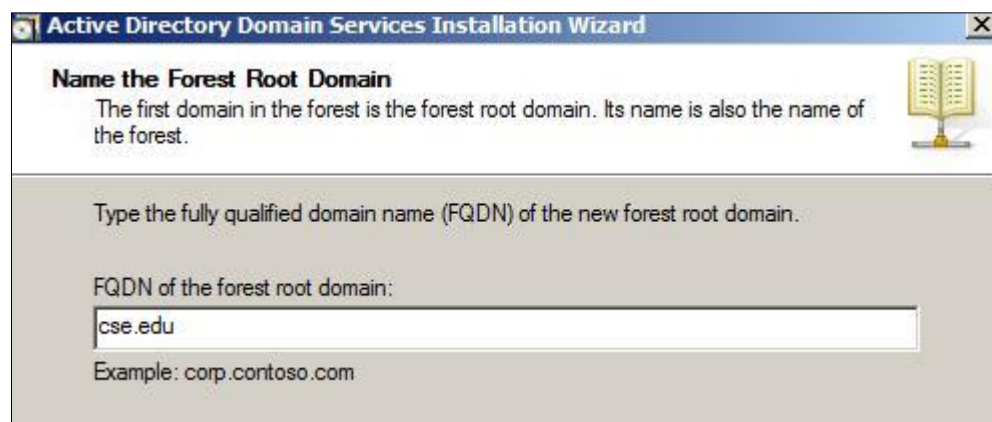
B4: Màn hình **Welcome to the Active Directory Domain Services Installation wizard** chọn **user advanced mode Installation** chọn **next**



B5: Màn hình **Choose a Deployment configuration** chọn **Create a new domain in a new forest**



B6: Màn hình **Name the forest root Domain** gõ tên domain **cse.edu** chọn **next**



B7: Màn hình **Domain NetBIOS name** chọn **next**



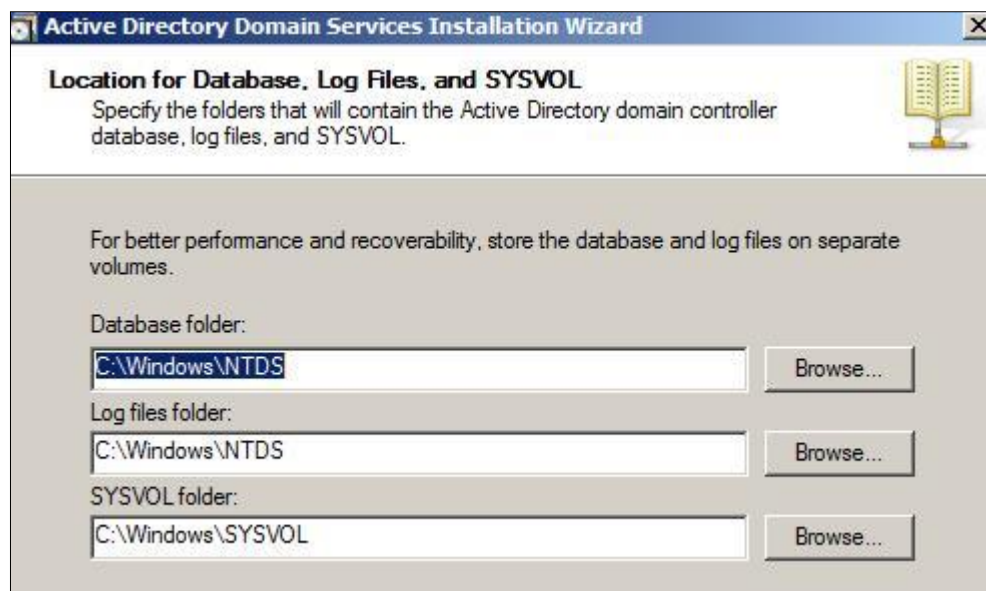
B8: Màn hình **Set Forest Functional Level** Chọn **windows server 2008** chọn **next**



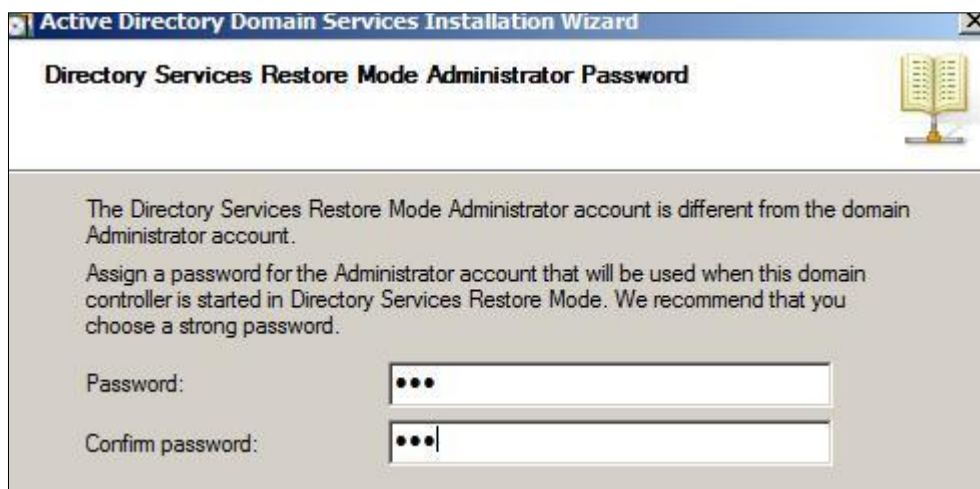
B9: Màn hình **additional Domain Controller Options** chọn **next**



B10: Màn hình **Location for database, log files, and SYSVOL** chọn **next**



B11: Màn hình **Directory Services Restore mode Administrator password** gõ **abc@123** Chọn next



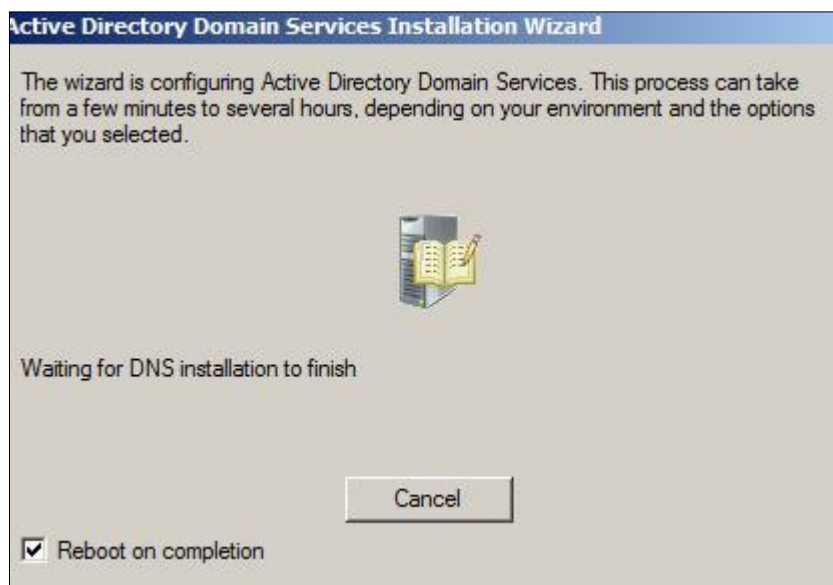
The screenshot shows the 'Active Directory Domain Services Installation Wizard' window. The title bar reads 'Active Directory Domain Services Installation Wizard'. The main heading is 'Directory Services Restore Mode Administrator Password'. Below the heading, there is an icon of an open book. The text explains that the Directory Services Restore Mode Administrator account is different from the domain Administrator account and asks the user to assign a password. It recommends a strong password. There are two input fields: 'Password:' and 'Confirm password:'. Both fields have three dots indicating masked text.

B12: Màn hình **summary** chọn next



The screenshot shows the 'Active Directory Domain Services Installation Wizard' window. The title bar reads 'Active Directory Domain Services Installation Wizard'. The main heading is 'Summary'. Below the heading, there is an icon of an open book. The text says 'Review your selections:' followed by a list of configuration options: 'Configure this server as the first Active Directory domain controller in a new forest.', 'The new domain name is cse.edu. This is also the name of the new forest.', 'The NetBIOS name of the domain is CSE', 'Forest Functional Level: Windows Server 2008', and 'Domain Functional Level: Windows Server 2008'.

B13: Màn hình **Active Directory Doamin services Installation**



The screenshot shows the 'Active Directory Domain Services Installation Wizard' window. The title bar reads 'Active Directory Domain Services Installation Wizard'. The text explains that the wizard is configuring Active Directory Domain Services and that the process can take from a few minutes to several hours, depending on the environment and options selected. There is an icon of a server rack. Below the icon, the text says 'Waiting for DNS installation to finish'. At the bottom, there is a 'Cancel' button and a checkbox labeled 'Reboot on completion' which is checked.

B14: Màn hình **Completing Active Directory Domain Services Installation Wizard** **Finish** chọn **Restart**

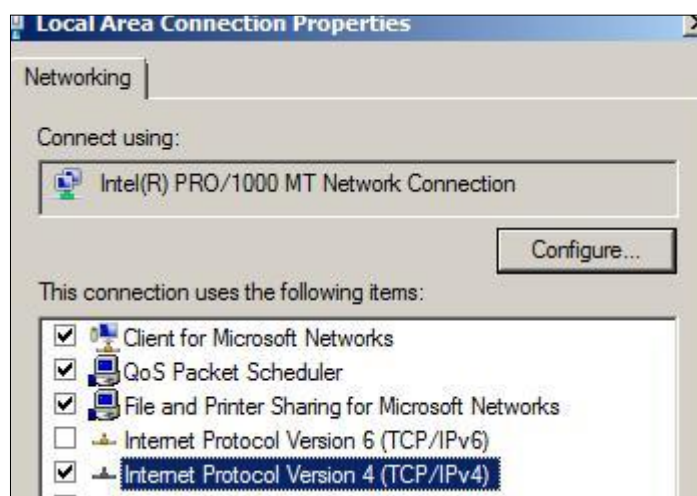
2. Join các máy Workstation vào Domain

Sau khi nâng cấp máy Server lên DC bây giờ ta tiến hành Join tất cả các máy Client vào Domain. Lợi ích của việc **Join** vào **Domain** này là rất nhiều trong bài này không thể nói hết được nhưng cứ hiểu một cách nôm na rằng join vào **Domain** rồi mọi máy **Client** không cần tạo User gì cả mà chỉ cần dùng các User **Account** mà ta đã tạo trên DC mà vẫn có thể truy cập vào máy một cách ngon lành. Cách Join như sau:
Vào **TCP/IP** chỉnh **DNS** là **IP** của máy **DC**

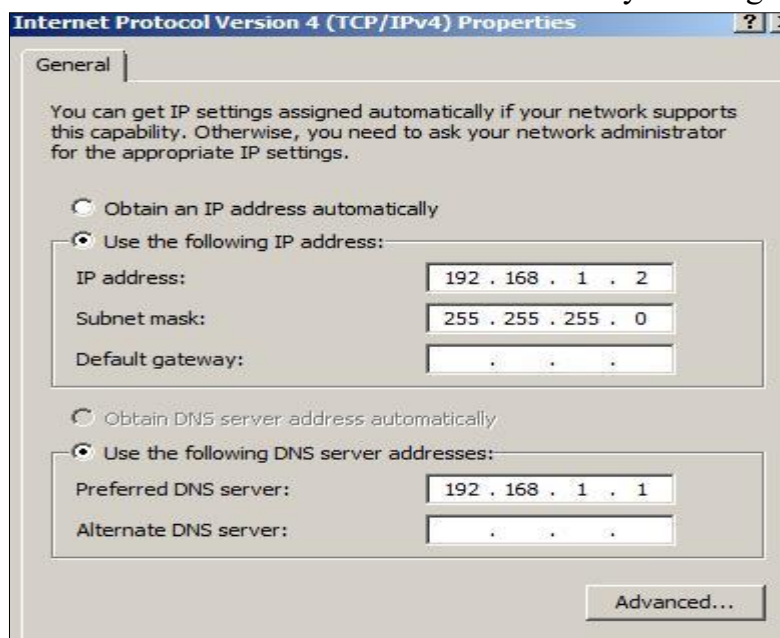
Thực hiện trên PC2 : Windows server 2008

B1: Chỉnh IP

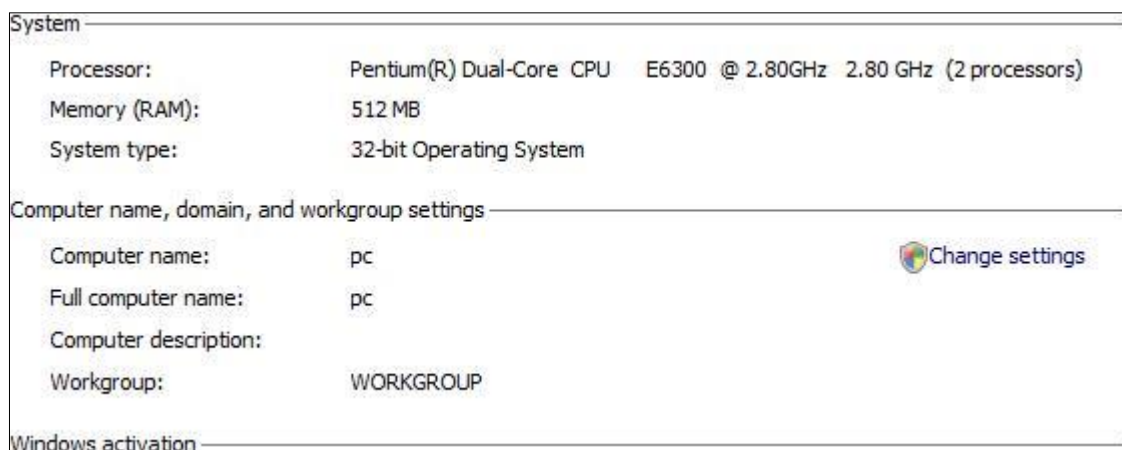
- Menu **start** chọn **setting** chọn **network Connections** click chuột phải vào **card** mạng Lan chọn **Properties** bỏ dấu check **internet Protocol Version 6 (TCP/IPv6)** chọn **internet Protocol Version 4 (TCP/IPv4)** nhấn **Properties**



Điều chỉnh **Preferred DNS server** về IP của chính số máy mình ngồi chọn **OK**



B2: Click chuột phải vào **Computer** chọn **Properties** Trong phần **Computer name, domain, and workgroup setting** chọn **Change setting**



- Trong phần **Member of** chọn **domain** điền tên domain **cse.edu** chọn **ok**



- Điền **Username** và **Password: administrator** và **Password: 123**

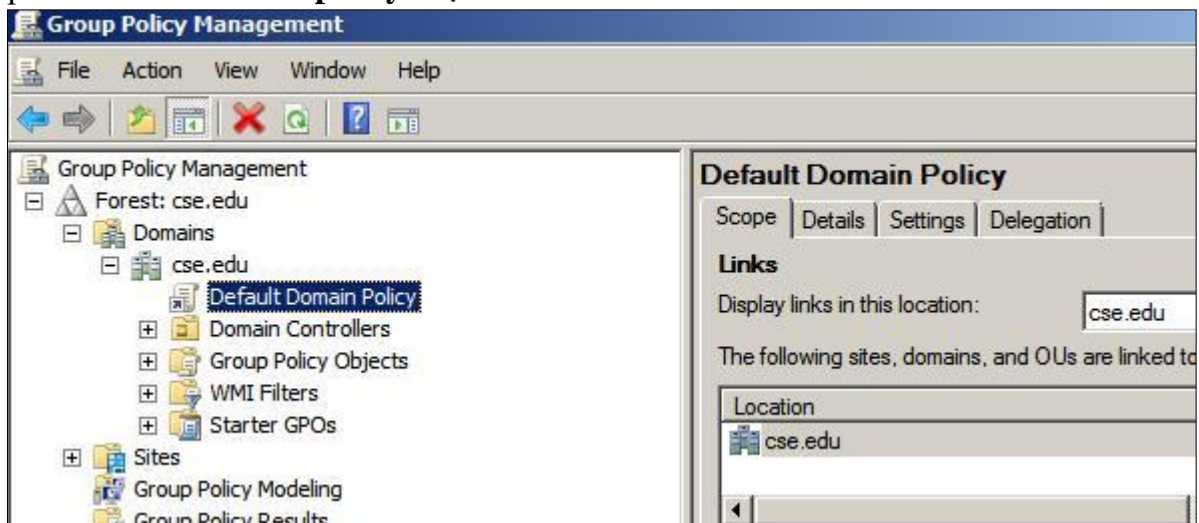
3. Khảo sát các policy trên máy Domain Controller

Một số thay đổi khi nâng cấp lên máy Domain Controller

- Quan sát trong **Server Manager** không còn **Local Users and Group**
- Mở **Active Directory users and computer** Vào **Start** chọn **Program** chọn **Administrative tools** chọn **Active Directory users and computer** Quan sát

- **Chỉnh policy cho phép đặt password đơn giản**

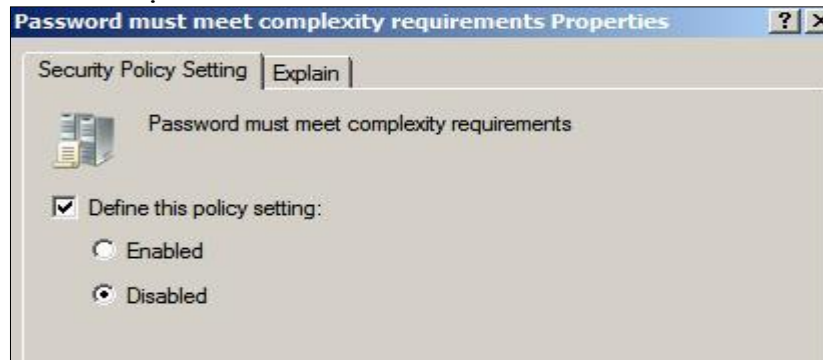
B1: Vào **Start** chọn **Program** chọn **Administrative tools** chọn **Group policy Management** chọn **Forest** chọn **cse.edu** chọn **Domain** chọn **cse.edu** click chuột phải **Default domain policy** chọn **Edit**



B2: Theo đường dẫn **Computer Configuration** chọn **policies** chọn **Windows setting** chọn **security setting** chọn **Account policy** chọn **Password policy** Double click vào **Password must meet complexity requirements**



B3: Chọn **Disable** chọn **OK**



B4: Màn hình **Group policy management Editor** Double click vào **Maximum password age** chọn **Properties**

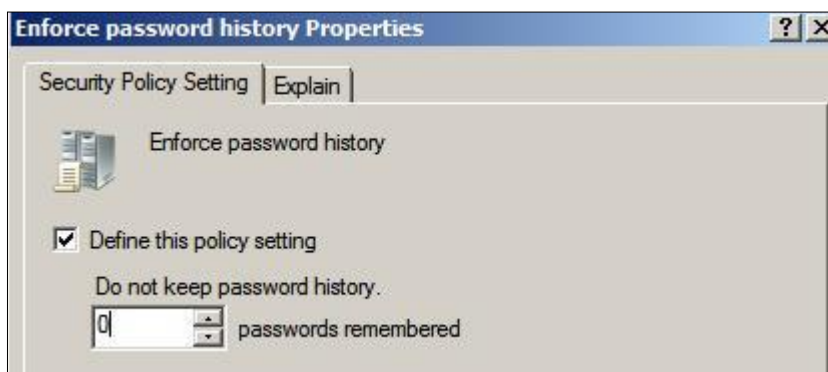
Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

B5: Gõ **0** vào dòng



Màn hình **Group policy management Editor** Double click vào **Enforce password history** chọn properties

Gõ **0** vào dòng **Do not keep passwords remember**



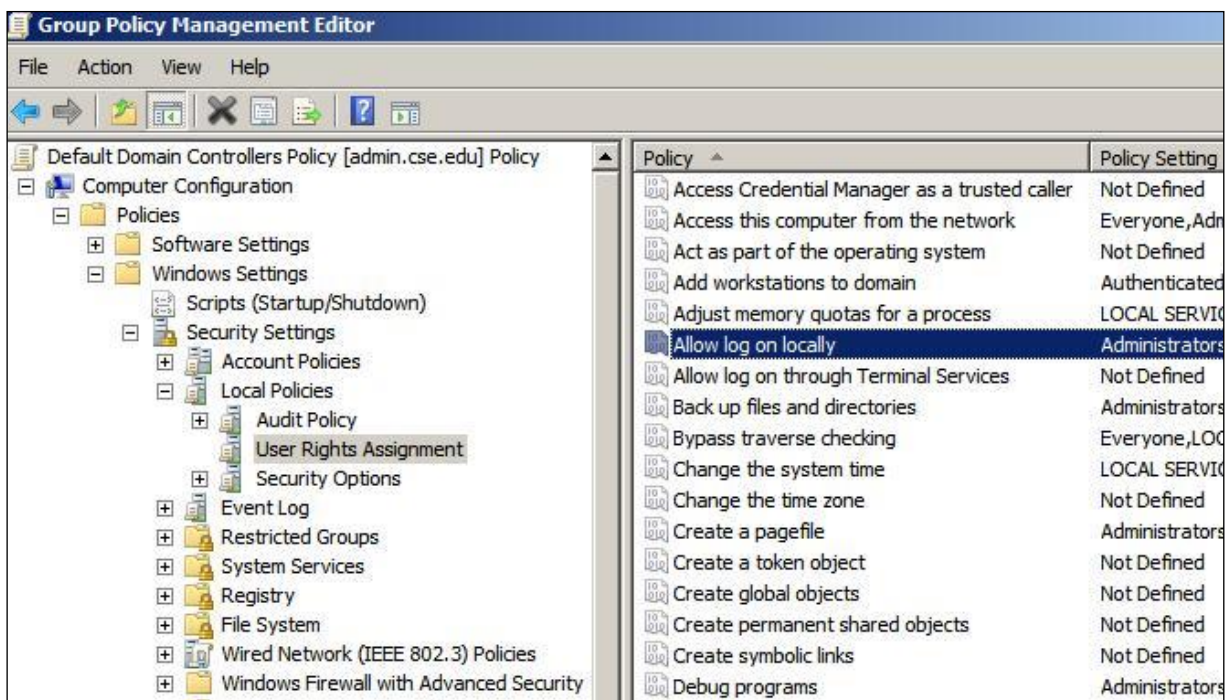
Vào **Start** chọn **Run** gõ **CMD** chọn **Ok** Gõ **GPUPDATE/FORCE** Enter

- **Điều chỉnh cho phép Group Users Logon trên máy DC**

B1: Vào **Start** chọn **Program** chọn **Administrative tools** chọn **Group policy Management** chọn **Forest** chọn **cse.edu** chọn Domain chọn **cse.edu** click chuột phải **Default domain Controller policy** chọn **Edit**

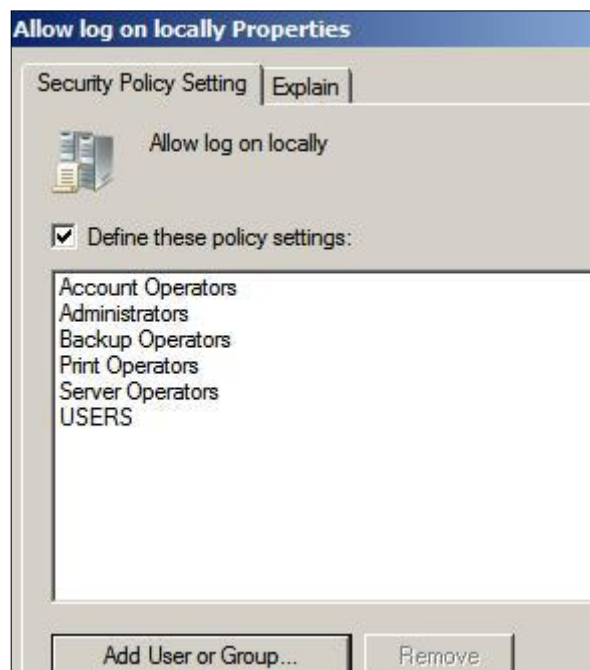
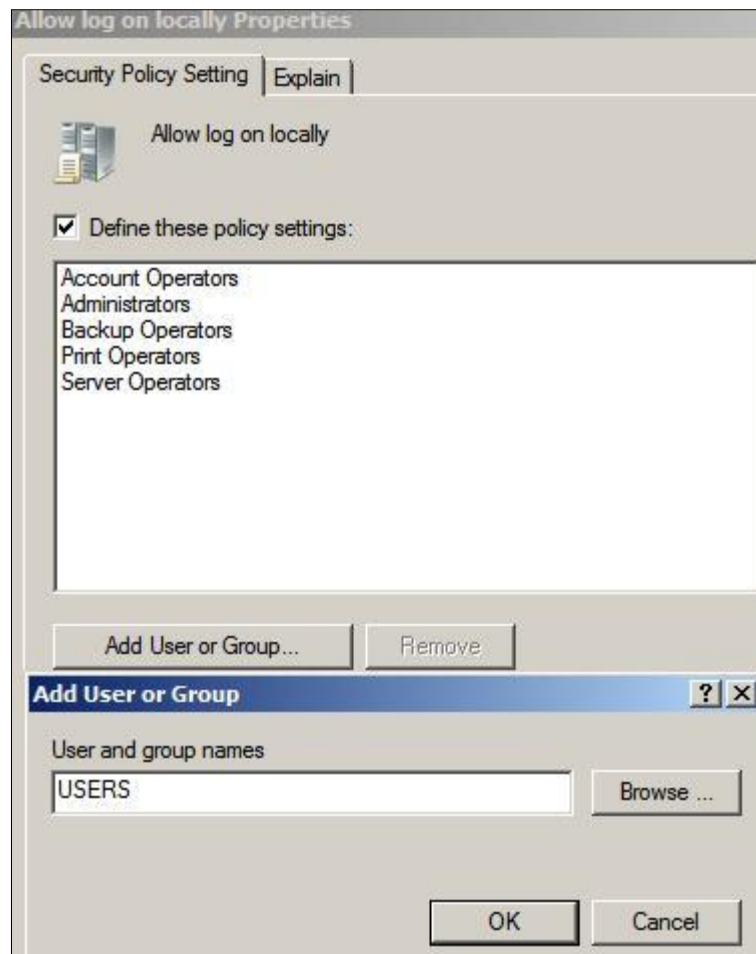


B2: Theo đường dẫn **Computer Configuration** chọn **policies** chọn **Windows setting** chọn **security setting** chọn **Local policy** chọn **user right assignment**



B3: Hộp thoại **Allow log on locally** chọn **Properties** chọn **Add user or Group**

B4: Gõ vào **Users** chọn **Ok**- **Ok**



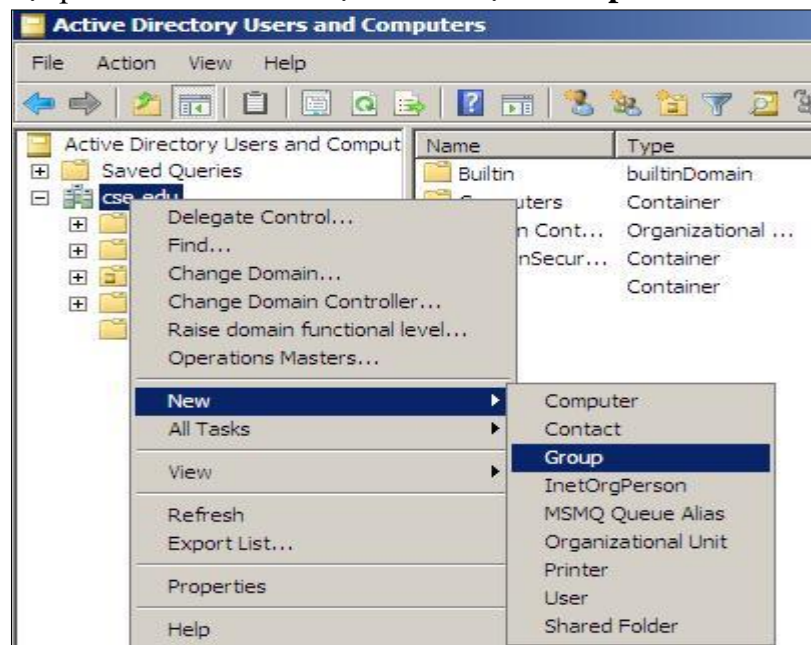
Vào **Start** chọn **Run** gõ **CMD** chọn **Ok** Gõ **GPUPDATE/FORCE** Enter

4. Tạo Domain Group

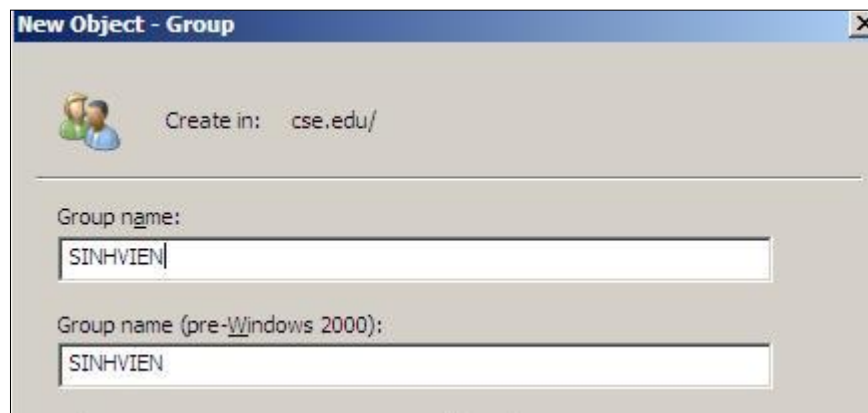
B1: Mở Active Directory Users and Computer



B2: Nhấp chuột phải vào **cse.edu** chọn **New** chọn **Group**

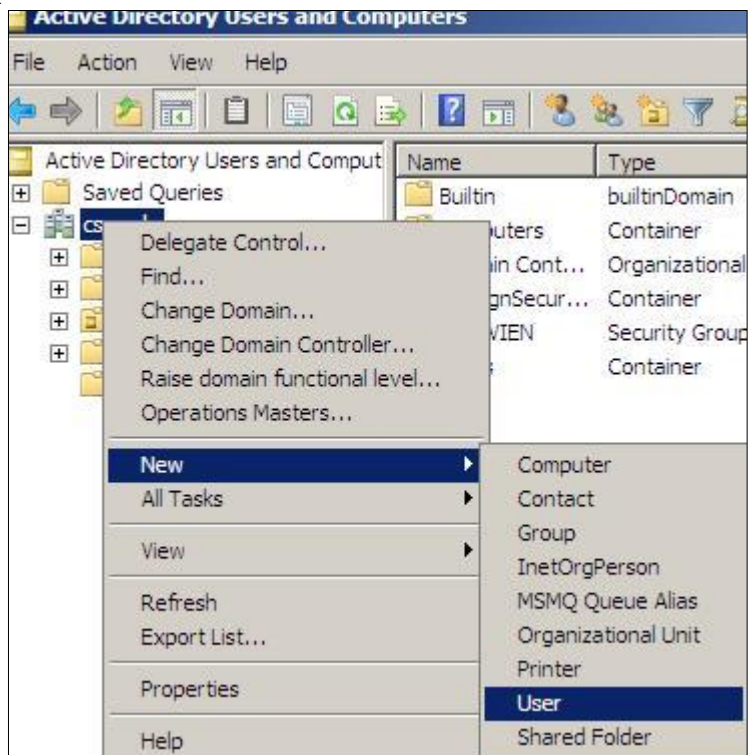


B3: Group name: **SINHVIEN** chọn **Ok**



5. Tạo Domain User

B1: Mở **Active Directory Users and Computer** Nhấp chuột phải vào **cse.edu** chọn **New** chọn **User**

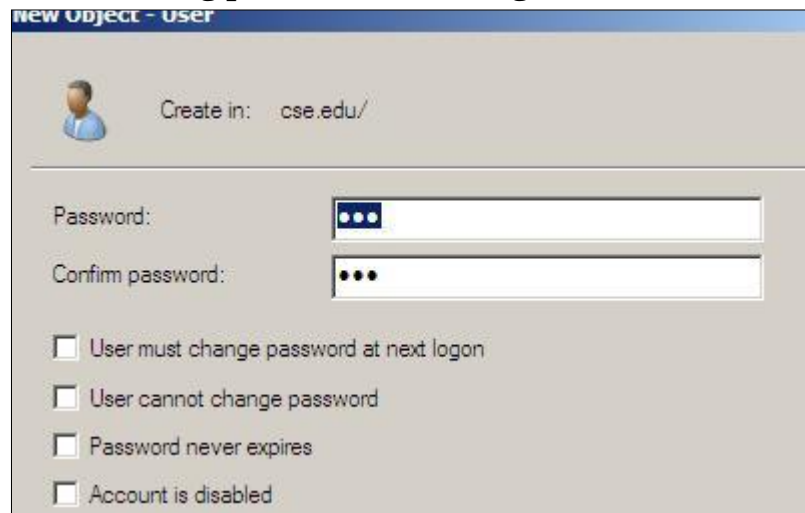


- B2:
- First name : Nguyen Van
 - Last name : Nam
 - Full name : Nguyen Van Nam
 - **User logon name: SV1** chọn **Next**

The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: cse.edu/'. Below this, there are several input fields: 'First name:' with 'Nguyen Van', 'Initials:' (empty), 'Last name:' with 'Nam', and 'Full name:' with 'Nguyen Van Nam'. Further down, 'User logon name:' has 'SV1' in the text box and '@cse.edu' in the dropdown menu. Below that, 'User logon name (pre-Windows 2000):' has 'CSE\' in the text box and 'SV1' in the adjacent text box. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- B3: - Password : 123
- Confirm password : 123

Bỏ dấu check **User must chang password at next logon** chọn **next**



Quan sát thấy User vừa tạo



BÀI 6: ORGANIZATIONAL UNIT (OU) DELEGATE CONTROL

Trong bài này chúng ta cần có một máy **DC** và một máy **Client** đã **join** vào **domain**. Như chúng ta đã biết ở các bài trước để tạo một **User Admin** phải vào **Active Directory Users & Computers** để tạo. Nhưng vấn đề sẽ trở nên khó khăn hơn với một công ty lớn đến vài trăm thậm chí vài ngàn nhân viên, như vậy người quản trị mạng phải tạo, xóa, disable các Account rất mất công.

Vì vậy Windows có một tính năng rất hay là **Organizational Unit (OU)** giúp giảm tải công việc cho người quản trị mạng bằng cách Ủy quyền cho một User nào đó có quyền thay thế anh ta trong việc quản lý các **User Account** nhưng với quyền hạn chế hơn. Ví dụ anh quản trị mạng sẽ ủy quyền cho User SV1 có quyền tạo, xóa, disable các Account chung Group với anh ta nhưng không có quyền với các Group khác. Trước tiên **Administrator** sẽ tạo các **Organizational Unit** và gán quyền cho một User nào đó bằng cách mở **Active Directory Users & Computers** ra nhấp phải vào domain chọn **New -> Organizational Unit**.

Chuẩn bị: Mô hình bài Lab gồm 2 máy

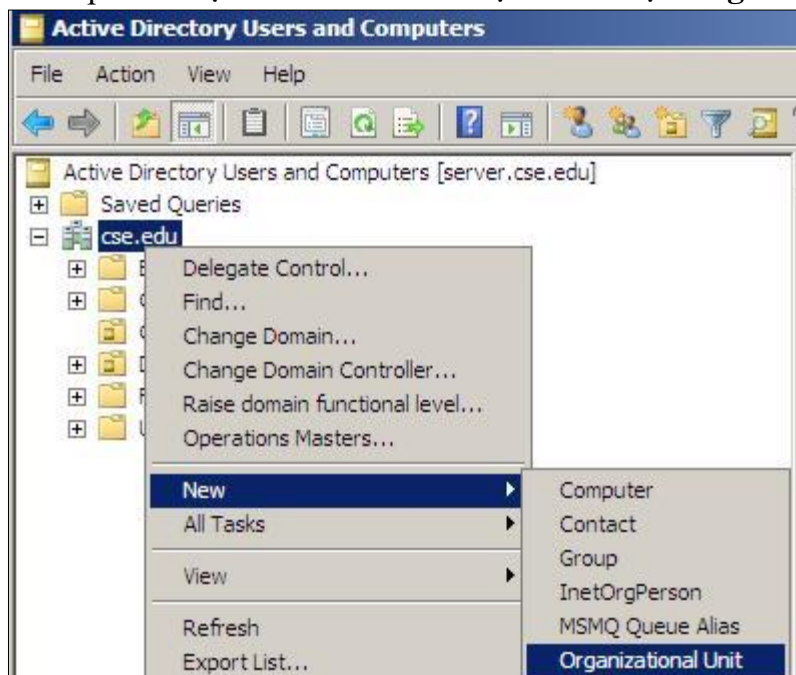
PC1: Windows server 2008 chỉnh password policy đơn giản

PC2: Windows server 2008, Join domain

Thực hiện: Trên máy PC1

1. Tạo OU:

B1: **Start** chọn **Program** chọn **administrative tool** chọn **Active Directory user and computer** click phải chuột vào **CSE.EDU** chọn **New** chọn **Organizational Unit**

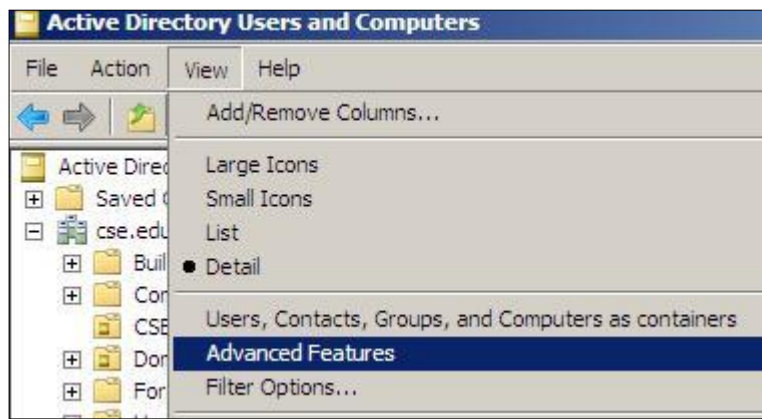


B2: Ở mục **name** nhập vào **OU** ví dụ: **PHONGDAOTAO** sau đó chọn **OK**

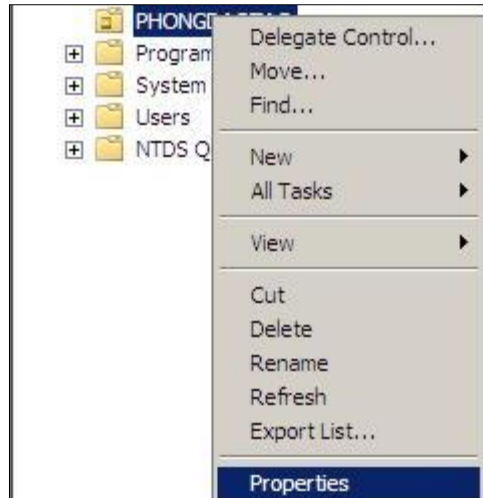


2. Xóa OU

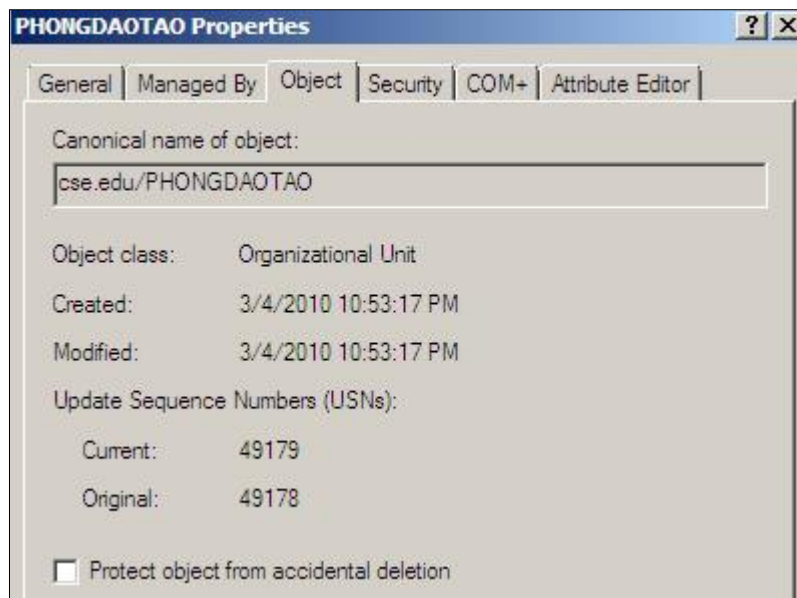
B1: Vào **View** chọn **advanced Features**



B2: Click phải chuột vào **PHONGDAOTAO** chọn **properties**

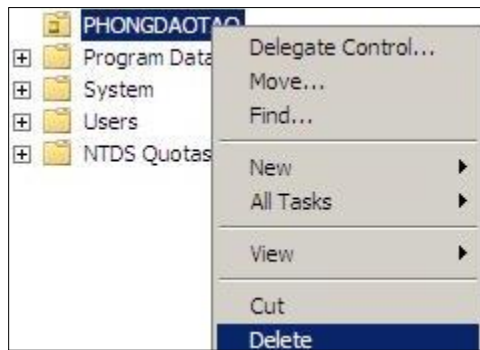


B3: Qua tab **Objects** tắt dấu check **Protect object from accidental deletion** sau đó chọn **Ok**



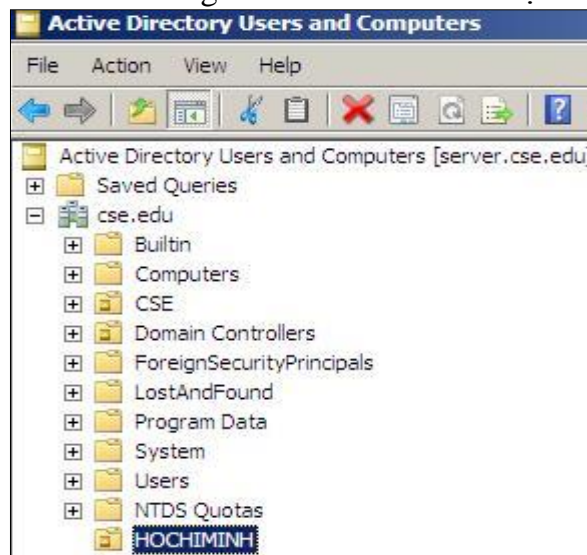
B4: chuột phải vào OU **PHONGDAOTAO** chọn **Delete**

- Hộp thoại cảnh báo chọn Yes
- OU **PHONGDAOTAO** đã được xóa thành công

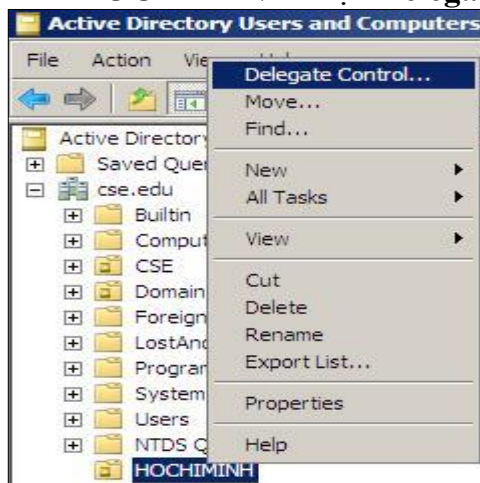


3. Ủy quyền cho User trên OU

B1: Tạo OU **HOCHIMINH** trong OU **HOCHIMINH** tạo user **quan1**



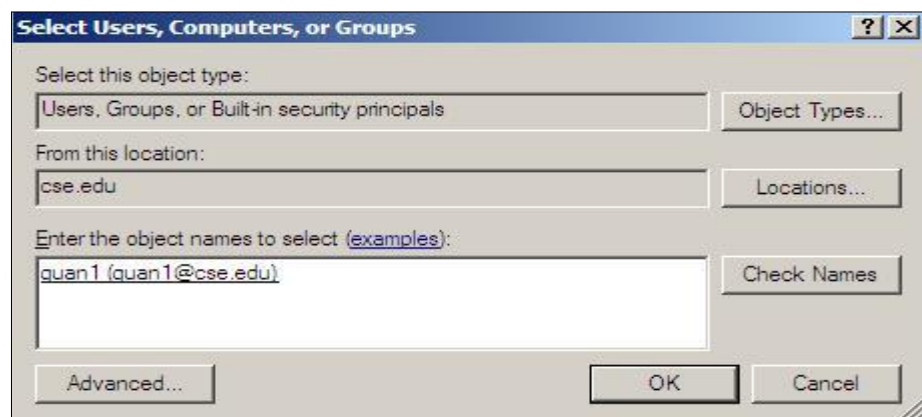
B2: Click chuột phải vào OU **HOCHIMINH** chọn **Delegate control...**



B3: Màn hình **Welcome** chọn **Next** trong màn hình **Selected users and group** chọn **add**



B4: Nhập vào user **quan1** chọn **check names** sau đó chọn **ok** chọn **next**



B5: Trong màn hình **Tasks to Delegate** đánh dấu check vào **Create, delete and manage user accounts** chọn **next**

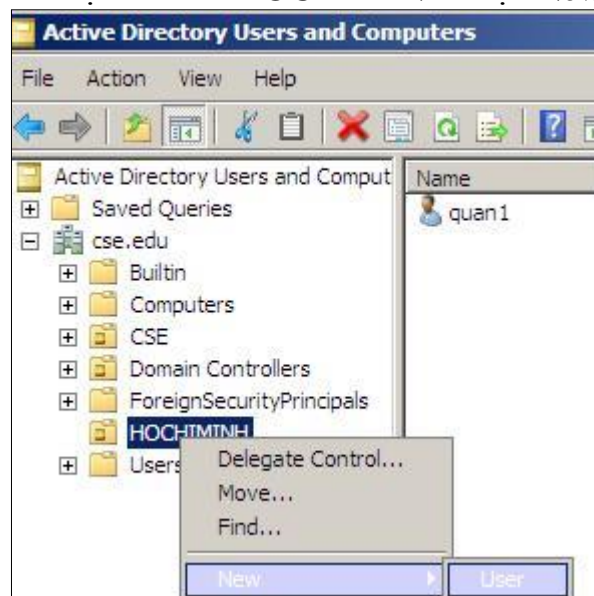


B6: Màn hình **Completing** chọn **Finish**

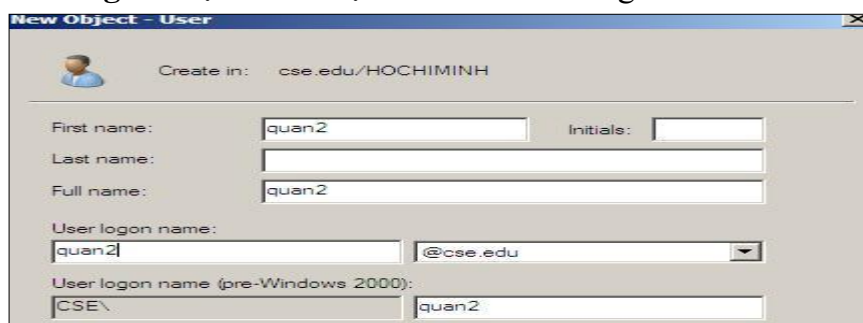


B7: Kiểm tra trên máy PC2

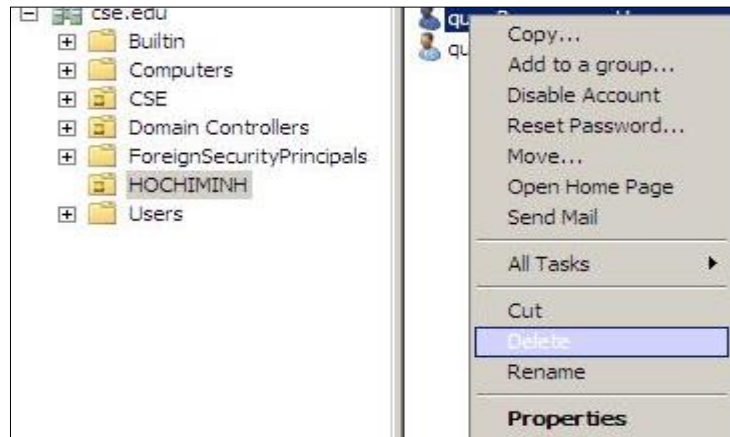
Log on user **quan1** trên máy PC2 mở **Administrative tool** chọn **Active Directory user and computer** click phải chuột vào OU **HOCHIMINH** chọn **New** chọn **user**



B8: Trong cửa sổ **new Object** chọn **user** tạo user **quan2** chọn **next** trong ô **Password** và **Confirm password** điền **abc@123** bỏ dấu check tại dòng **user must change password at next logon** chọn **next** chọn **Finish** thành công.



B9: Tạo thêm user **quan3** sau đó click chuột phải user **quan3** chọn **delete** xóa thành công **quan3**



B10: Click chuột phải vào **Container users** thử tạo 1 user mới không xuất hiện menu tạo user



Kết luận: User **quan1** chỉ được tạo, xóa, quản lý user trên OU **HOCHIMINH**

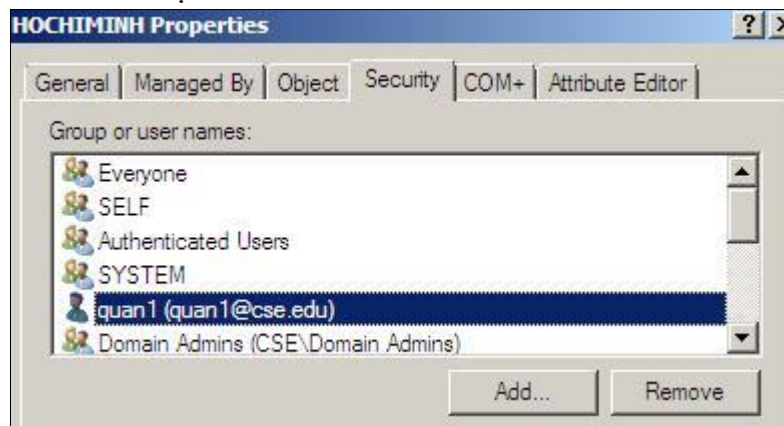
4. Trúcc quyền user trên OU

Máy PC1

B1: Log on administrator Mở **Active administrative tool** chọn **Active Directory user and computer** click phải chuột vào OU **HOCHIMINH** chọn **Properties**

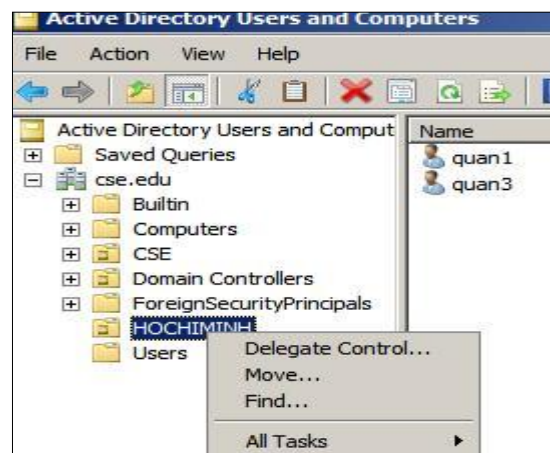


B2: Trong màn hình **HOCHIMINH** chọn **Properties**, qua tab **Security** chọn vào user **quan1** chọn **Remove** chọn **OK**

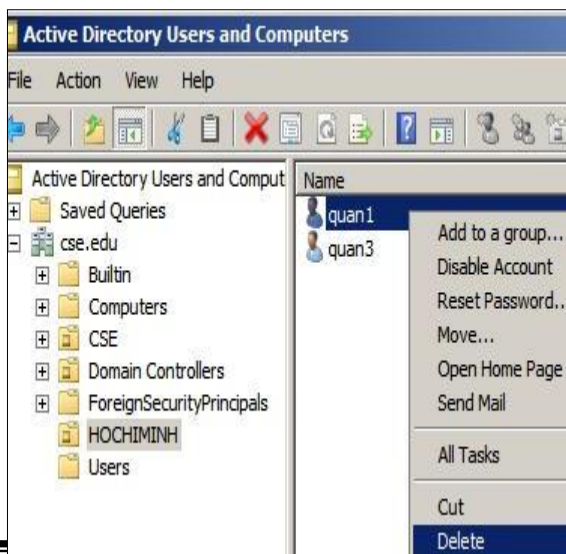


B3: Kiểm tra trên máy PC2

Log on User **quan1** mở **Active Directory user and computer** click phải vào OU **HOCHIMINH** Tạo user mới **không** tạo được



- Click chuột phải vào user **quan1**, chọn **Delete**
- Bảng báo lỗi sẽ xuất hiện thông báo user **quan1** **không** có quyền.



BÀI 7: ỨNG DỤNG GPO

Là một người quản trị mạng ngoài việc quản lý máy Server ra thì còn cả khối việc với các máy Client nữa. Trong đó có việc cài hoặc gỡ bỏ một số software ở các máy Client.

Ví dụ công ty bạn có 2 phòng ban đó là phòng **KETOAN** & **NHANSU** mỗi phòng có **20 máy**, vì 2 phòng ban này có công việc khác nhau nên trên các máy Client này phần mềm được cài lên cũng khác nhau. Tôi lấy ví dụ phòng **NHANSU** thì cần chương trình **Acrobat Rerader** trong khi đó phòng **KETOAN** thì cần có **Bitdefender Anti Virus**.

Chả lẽ với **40 máy** trên ta phải đi từng máy cài thêm software hay sao... thật là quá cực nhọc & nhàm chán. Vì thế Windows server đã thiết kế sẵn cho người quản trị mạng tính năng **Software Deployment** để giúp bạn giải quyết vấn đề nay giản trên.

Nhưng trước thời **Windows 2000** Microsoft chưa thiết kế các tính năng này nên các file setup thường có đuôi là ***.exe**, ***.com**, ***.bat...** các đuôi này không hỗ trợ Software Deployment, cho nên từ khi cho ra mắt Windows 2000 Microsoft cho giới thiệu một định dạng mới với phần mở rộng là ***.msi**, định dạng mới này nhanh chóng được các hãng phần mềm hưởng ứng và phát triển rộng rãi hiện nay. Nói tóm lại điều kiện cần để chạy **Software Deployment** là Software đó phải **hỗ trợ định dạng *.msi**

Nhân tiện đây cũng nói cho bạn đọc biết thêm đối với các phần mềm chỉ có đuôi ***.exe** thì hiện nay trên thị trường có rất nhiều công cụ giúp ta chuyển đổi chúng thành ***.msi** các bạn có thể search bất cứ đâu trên Net

Chuẩn bị:

PC1: Windows server 2008-DC

PC2: Windows server 2008 hoặc Winxp hoặc Windows 2003 Join Domain

PC1: tạo các OU **KETOAN**, OU **NHANSU**, OU **CLIENTS** trong OU **KETOAN** Tạo các user **kt1**, **kt2**

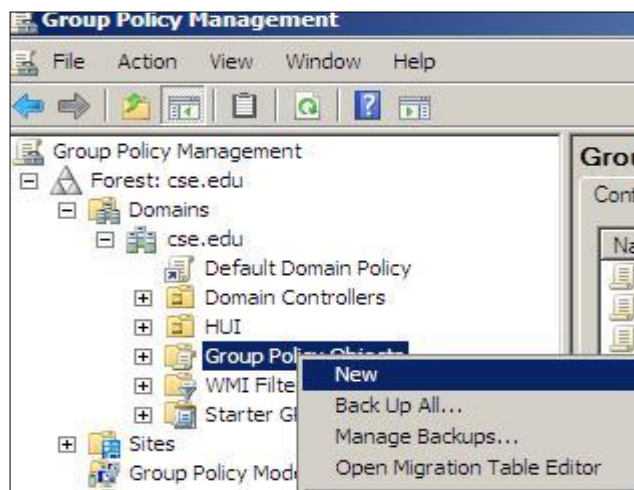
- Tạo thư mục **Softs** trong ổ đĩa **C** chép 2 thư mục **COSMO1** và **COSMO2** vào trong thư mục **softs** , **Share** thư mục **Softs** quyền **Everyone-Full control**

Thực hiện:

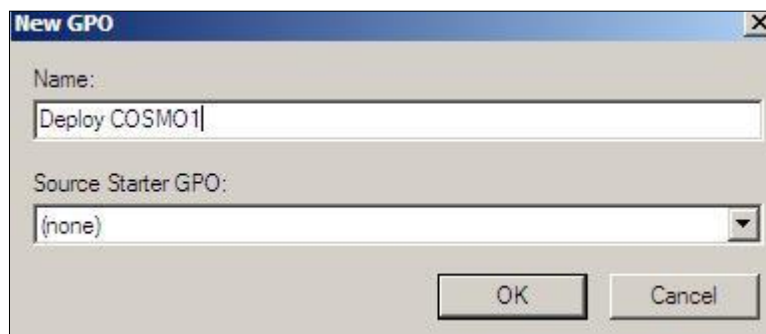
1. Deploy Software trên User:

Thực hiện trên PC1:

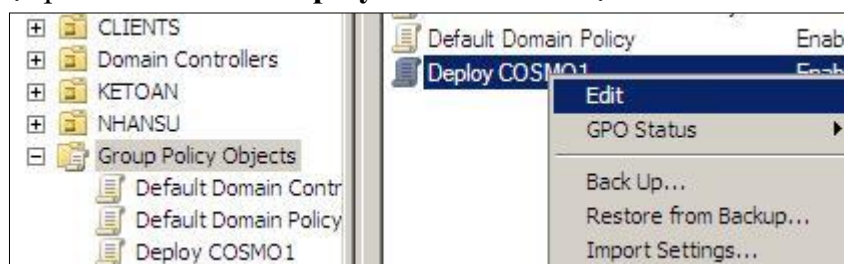
B1: Mở **Group policy management** click chuột phải vào **Group policy Object** chọn **New**



B2: Đặt tên **GPO** là **Deploy COSMO1**



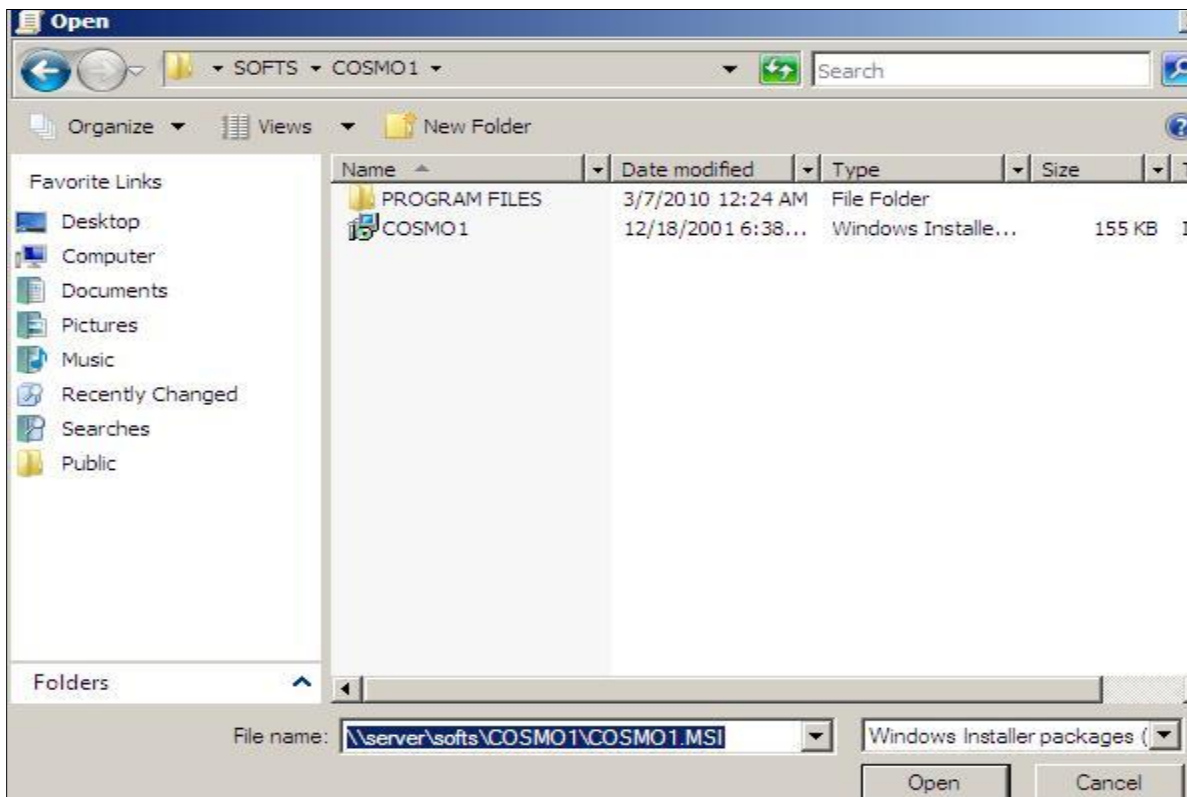
B3: click chuột phải vào **GPO “Deploy COSMO1”** chọn **Edit**



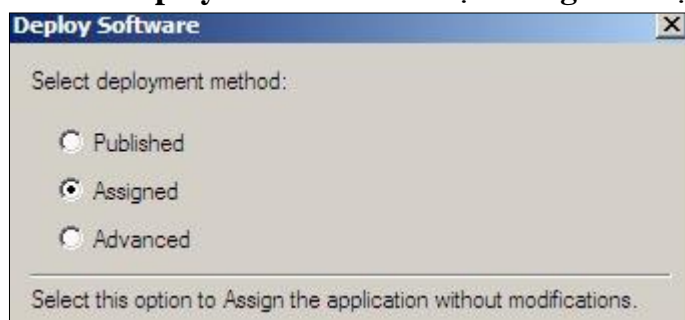
B4: Bung mục **User configuration** chọn **Policies** chọn **Software settings** click phải chuột vào **Software Installation** chọn **New** chọn **Package...**



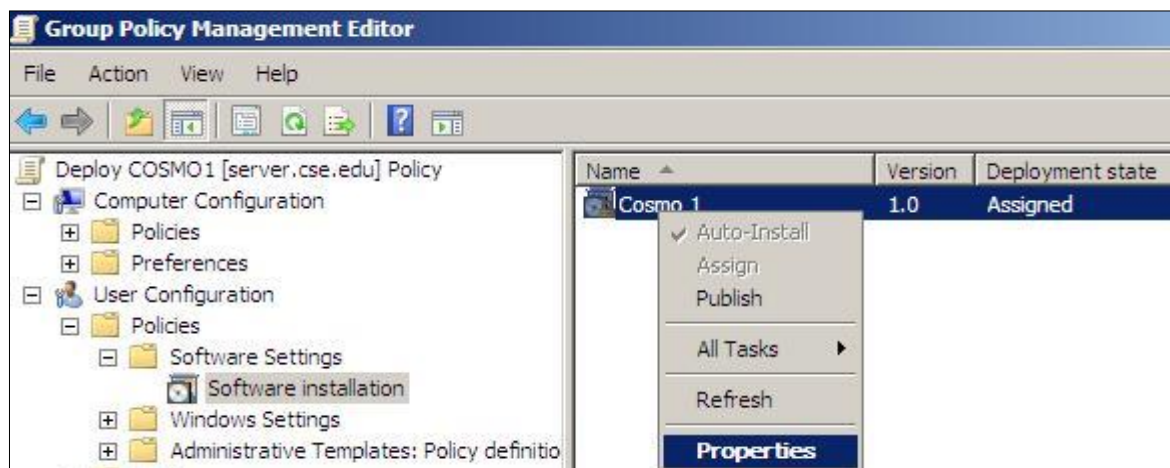
B5: Ở khung File name nhập vào
\\Server\Softs\cosmo1\ cosmo1.msi chọn vào **Open**



B6: Màn hình **Select Deployment method** chọn **Assigned** chọn **ok**



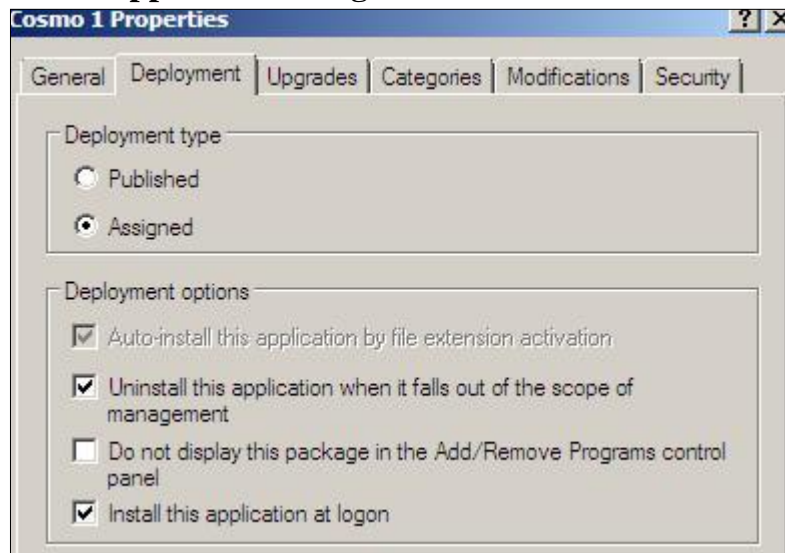
B7: Click chuột phải vào **Cosmo1** vừa tạo, chọn **Properties**



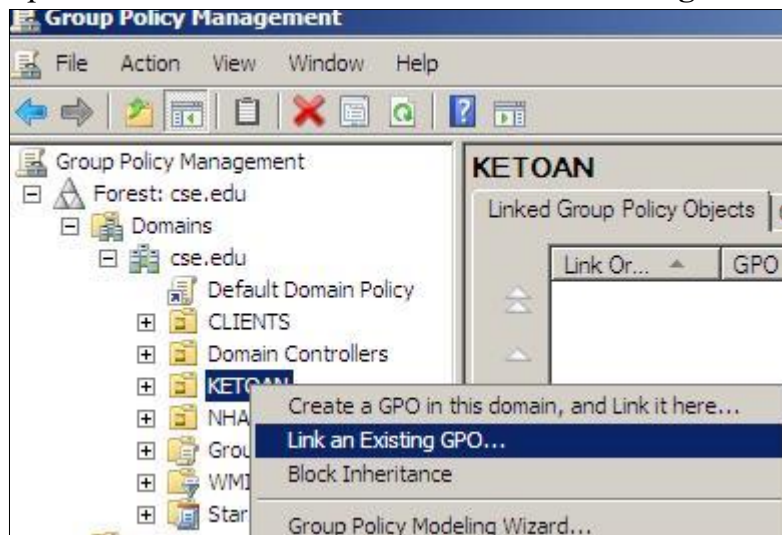
B8: Qua tab **Deployment** ở mục **Deployment options** đánh dấu chọn vào 2 dòng

- **Uninstall this application when....**
- **Install this application at logon**

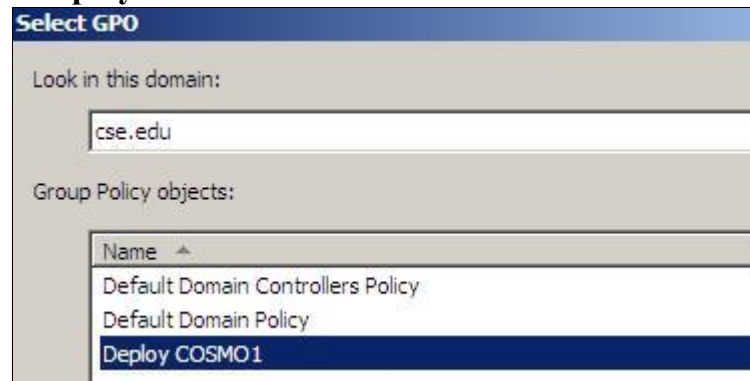
Chọn



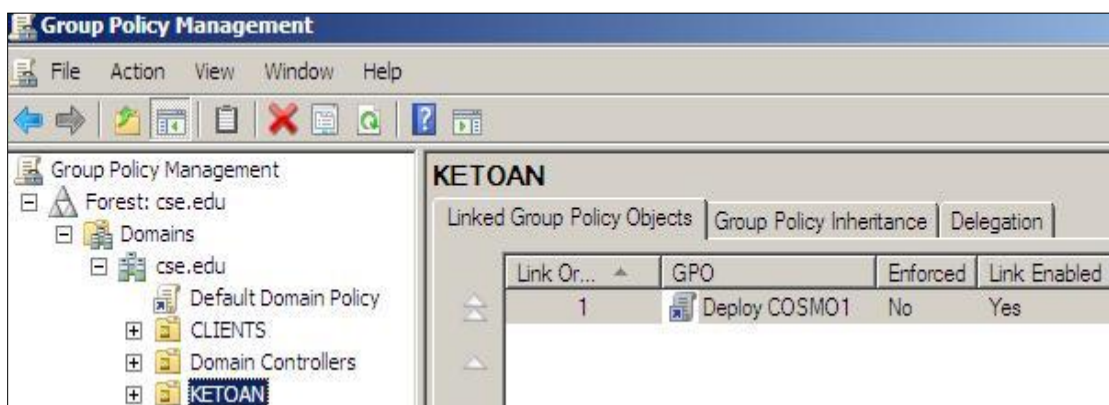
B9: Click chuột phải vào OU **KETOAN** chọn **Link an Existing PGO...**



B10: Chọn **GPO” Deploy COSMO1”**



B11: Quan sát thấy Ou **KETOAN** đã có GPO ” **Deploy COSMO1”**



B12: Kiểm tra trên **PC2**:

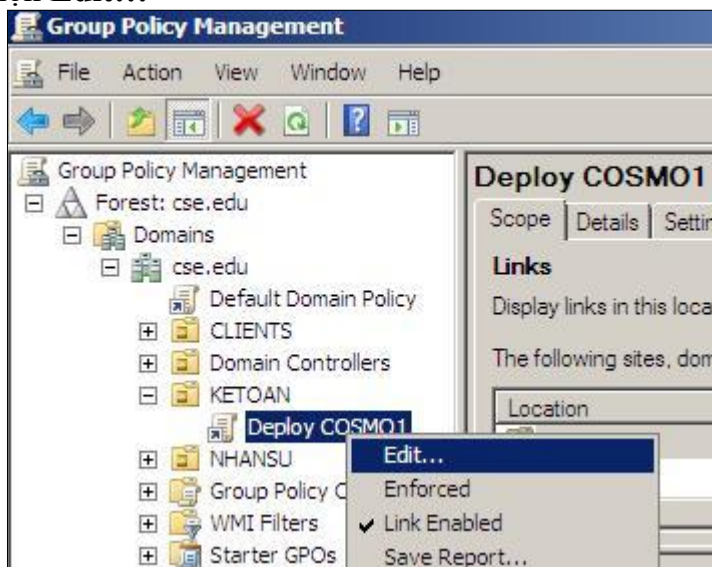
Log on **KT1** quan sát thấy có phần mềm **COSMO1 V1.0**

B13: trên **PC2** log on Administrator mở Windows explorer vào thư mục **C:\Program\File\COSMO1** xóa một vài file **dll** bất kỳ để giả lập chương trình bị lỗi . Chạy thử chương trình COSMO báo lỗi không thể chạy chương trình.

B14: **PC2** Log off và Logon **KT1** chạy thử chương trình **COSMO** thành công chương trình đã tự động sửa lỗi.

2. Upgrade phần mềm bằng Deploy Software

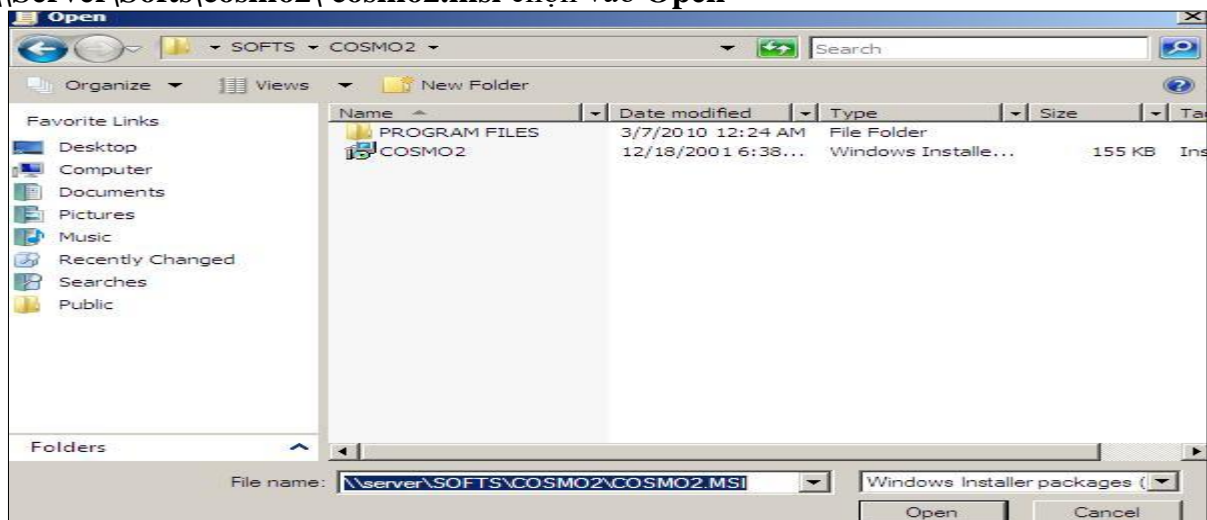
B1: **PC1**: Mở **Group policy management** click chuột phải vào GPO “**Deploy COSMO1**” chọn **Edit...**



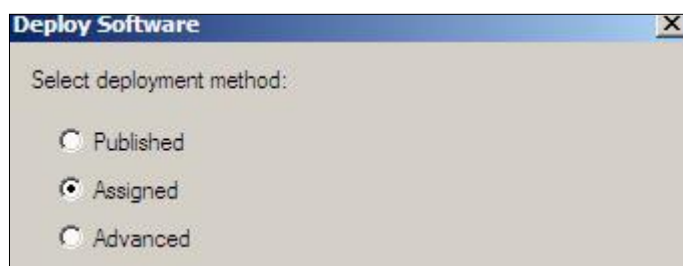
B2: Bung mục **User configuration** chọn **Policies** chọn **Software settings** click phải chuột vào **Software Installation** chọn **New** chọn **Package...**



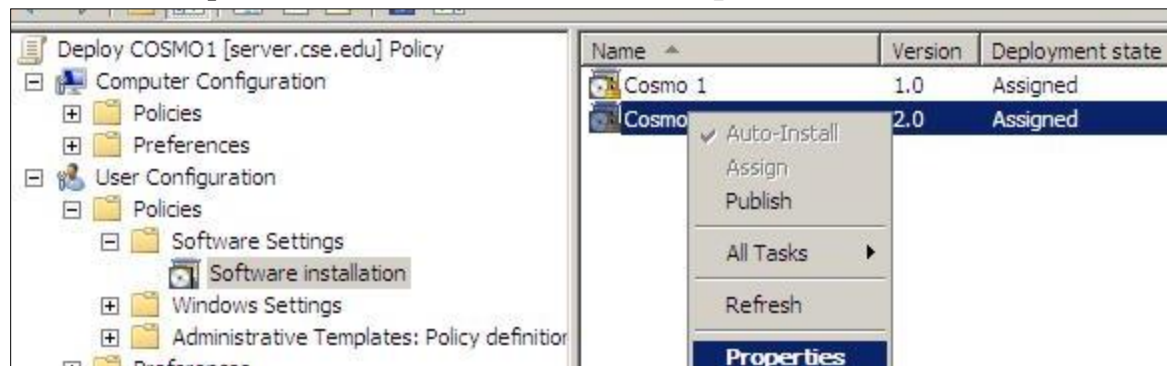
B3: Ở khung File name nhập vào
 \\Server\Softs\cosmo2\ cosmo2.msi chọn vào Open



B4: Màn hình Select Deployment method chọn Assigned chọn ok

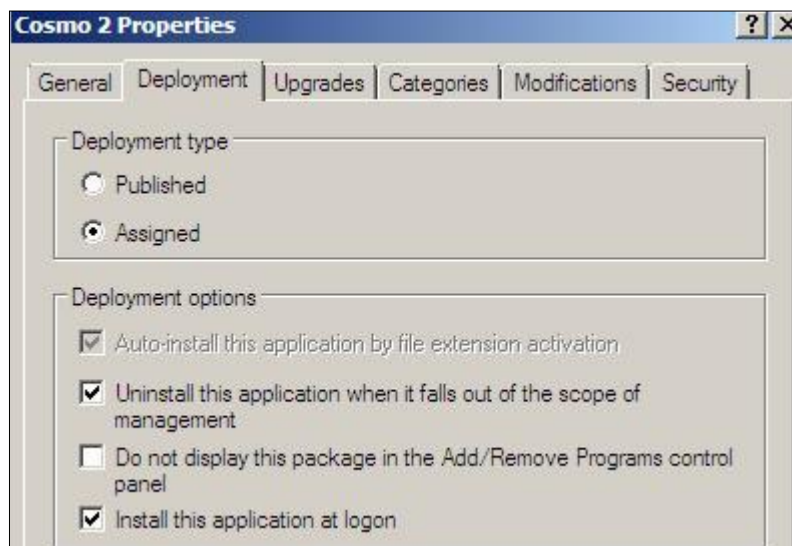


B5: click chuột phải vào Cosmo2 vừa tạo, chọn Properties

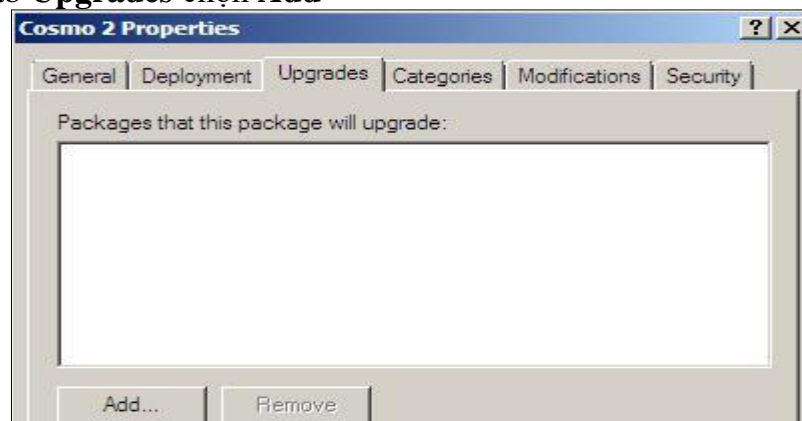


- B6: Qua **tab Deployment** ở mục **Deployment options** đánh dấu chọn vào 2 dòng
- **Uninstall this application when....**
 - **Install this application at logon**

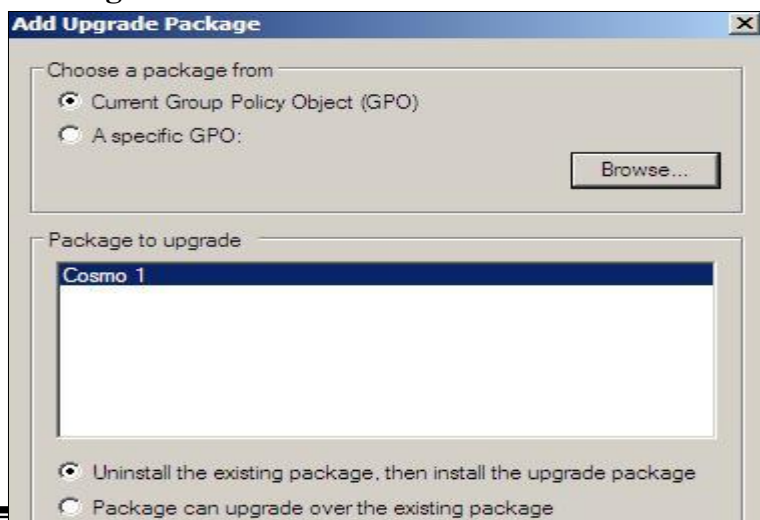
Chọn **OK**



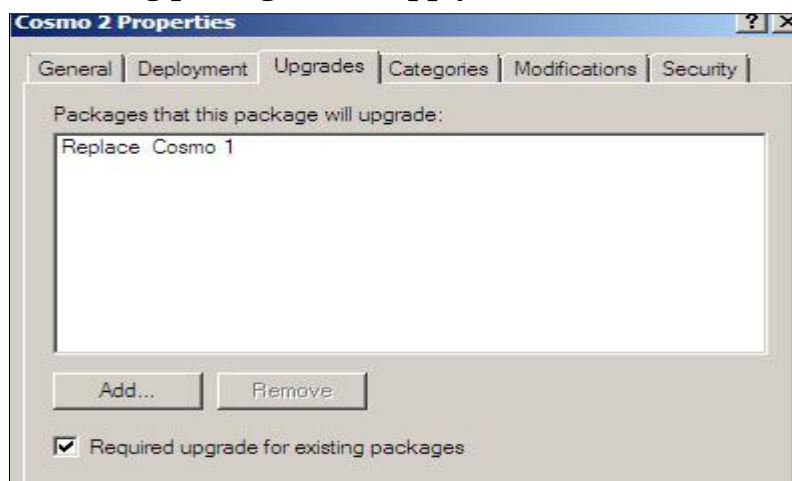
- B7: Qua tab **Upgrades** chọn **Add**



- B8: Chọn mục **A specific GPO** và **Browse** đến **GPO Deploy COSMO** bên dưới chọn **Uninstall the existing...**



B9: trở lại hộp thoại COSMO 2 chọn **Properties** đánh dấu chọn vào mục **Required upgrade for existing packages** chọn **apply** chọn



B10: Kiểm tra trên máy **PC2**:

Log on Kt1 quan sát thấy có chương trình **COSMO** đã được **upgrade lên phiên bản v2.0**

B11: Trên **PC1** Move user kt1 vào **OU NHANSU**

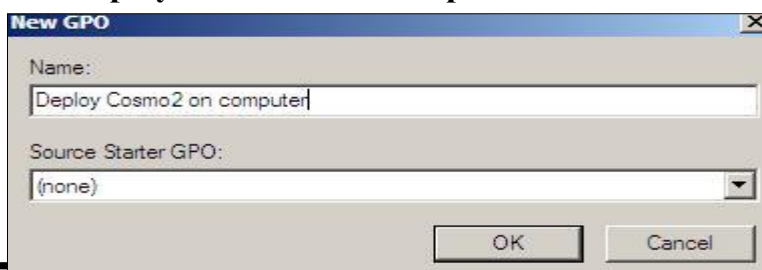
B12: Trên **PC2** logon kt1 chương trình **Cosmo** đã tự động Remove

3. Deploy software trên Computer

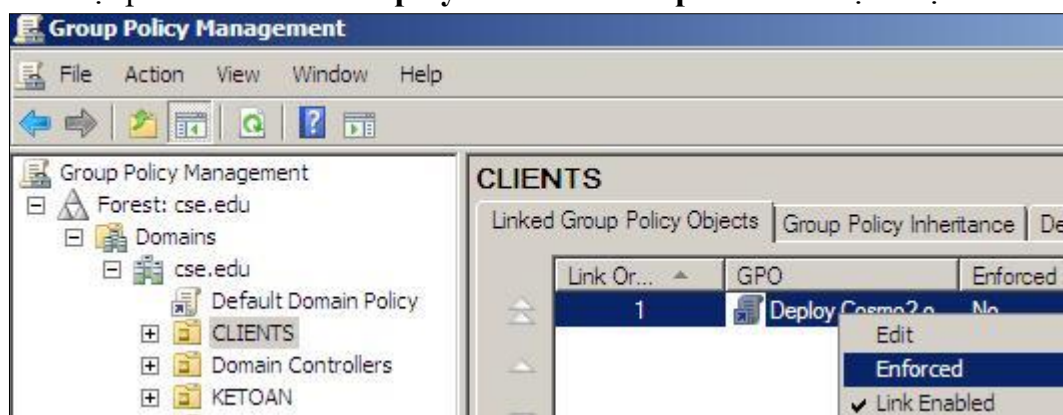
B1: Mở **Group policy Management** Chuột phải vào **Ou Clients**, chọn **Create a GPO in this domain, and Link it here...**



B2: Đặt tên **GPO “Deploy COSMO2 on computer”**



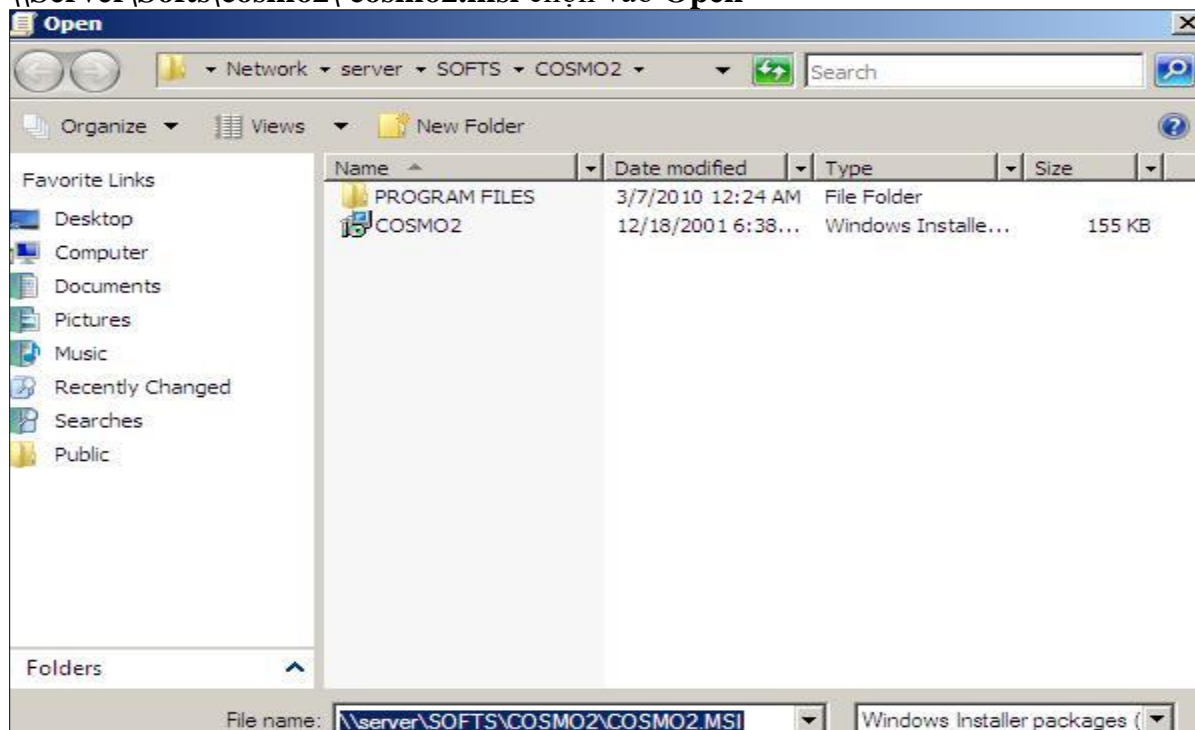
B3: Click chuột phải vào **GPO “Deploy cosmo on computer”** vừa tạo chọn **Edit**



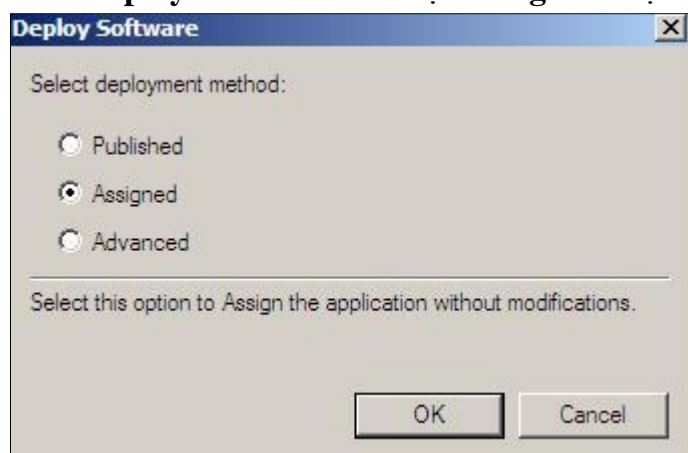
B4: Bung mục **Computer configuration** chọn **Policies** chọn **Software settings** click phải chuột vào **Software Installation** chọn **New** chọn **Package...**



B5: Ở khung File name nhập vào **\\Server\Softs\cosmo2\ cosmo2.msi** chọn vào **Open**



B6: Màn hình **Select Deployment method** chọn **Assigned** chọn **ok**



B7: **Kiểm tra:**

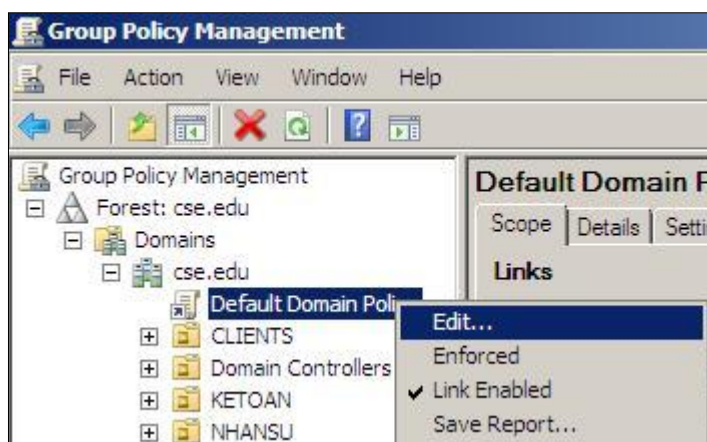
Trên **PC2**, lần lượt logon các user **Administrator** , **KT1**, **KT2** đều thấy có phần mềm **COSMO** đã được cài đặt.

3. Một số Policy

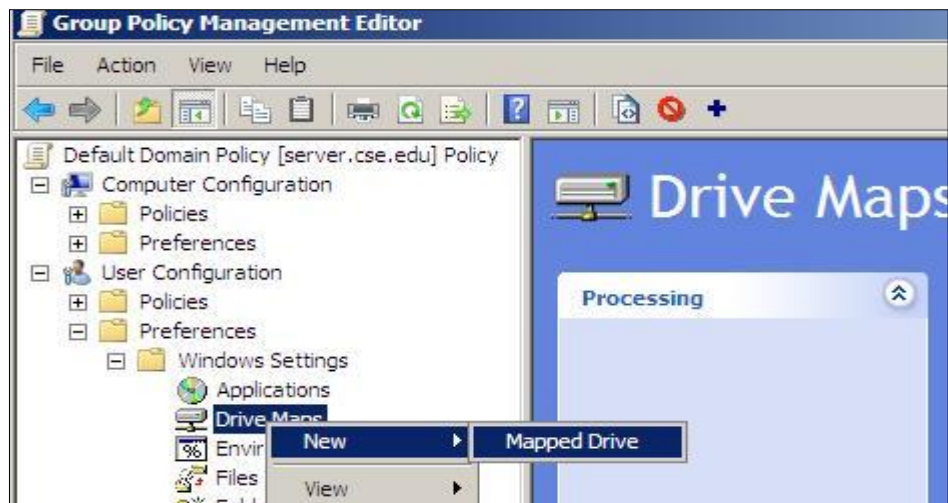
A. **Map tạo ổ đĩa mạng cho Client Thực hiện trên PC1**

Tạo một thư mục tên là **TaiLieu** trong ổ đĩa **C Share** quyền **Everyone- Full Control**

B1: Log on Administrator Mở **Group policy Management** click chuột phải lên **Default Domain Policy** chọn **Edit**



B2: Mở theo đường dẫn: Chọn **User Configuration** chọn **Preferences** chọn **Windows settings** click chuột phải lên **Driver Map** chọn **New** chọn **Mapped Driver**



B3:

- Action: Chọn **Create**
- Location: **\\Server\TaiLieu**
- **Chọn dòng : Reconnect**
- Driver Letter: Chọn user chọn ổ **Z** chọn **OK**

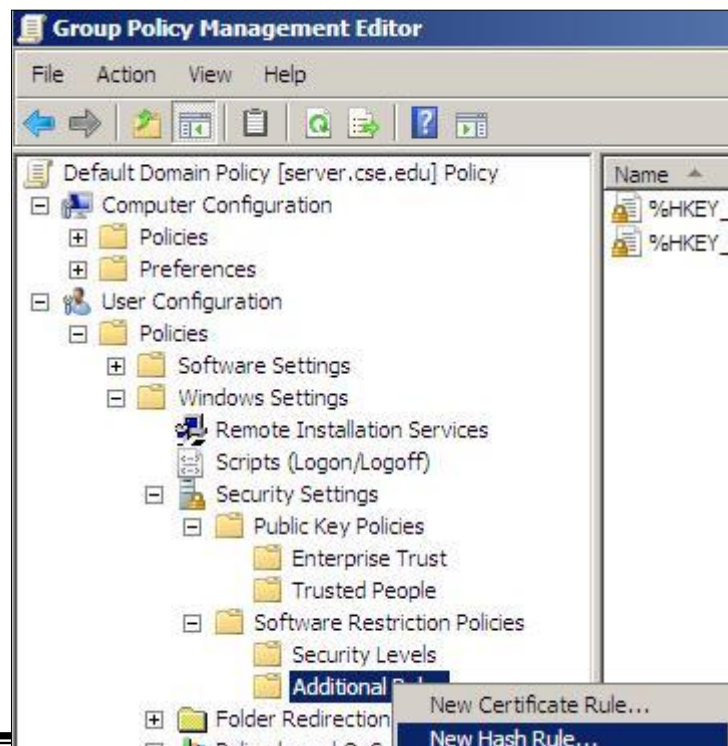
Kiểm tra:

PC2: Lần lượt log on bằng các user Mở **My Computer** đều có ổ đĩa mạng **Z:\TaiLieu**

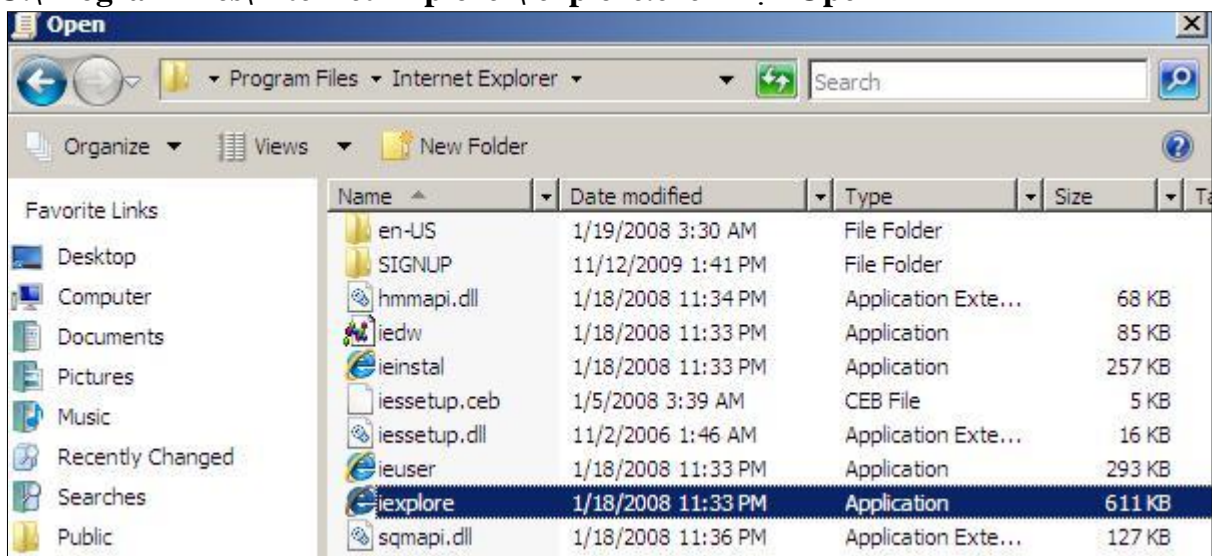
B. Software Restriction- Thực hiện trên PC1

Cấm sử dụng một phần mềm

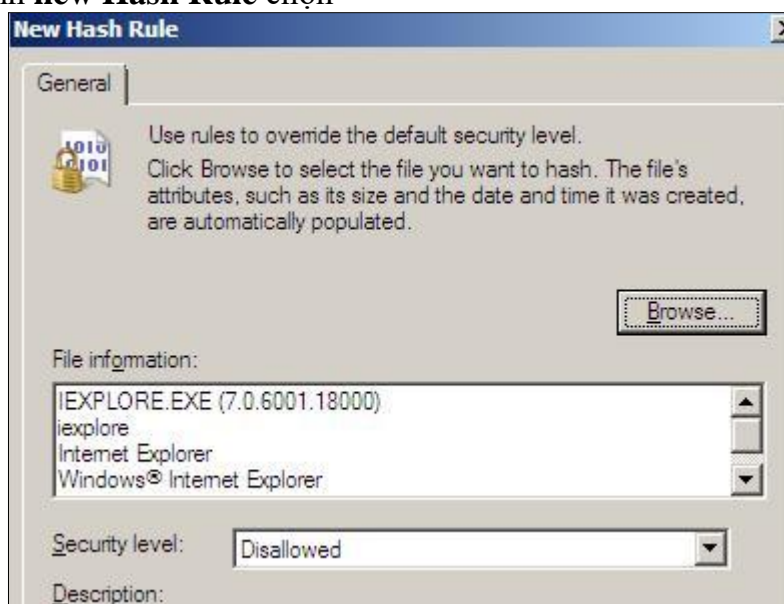
B1: Log on Administrator Mở **Group policy Management** Chọn **Edit** chọn **Default Domain Policy** truy cập theo đường dẫn: **user configuration** chọn **Policies** chọn **Windows setting** chọn **security setting** click chuột phải chọn **New Software Restriction polici** Sau đó click chuột phải lên **Additional Rules** chọn **New Hash Rule**



B2: Màn hình **New Hash Rule** chọn **Browse** chỉ đường dẫn đến:
C:\ProgramFiles\Internet Explorer\iexplore.exe chọn **Open**



B3: Màn hình **new Hash Rule** chọn



B4: **Kiểm tra:**

PC2: Log on bằng account **KT1** Mở chương trình **Internet Explorer** Báo lỗi không thể truy cập.

BÀI 8: WINDOWS SERVER BACKUP

Khi làm công tác quản trị mạng vấn đề an toàn dữ liệu luôn được chúng ta chú trọng với các công việc đảm bảo cho chúng luôn ở mức độ an toàn cao. Không may một ngày nào đó cả hệ thống bị nhiễm virus trầm trọng, phòng chứa server rủi ro xảy ra hoả hoạn... những gì còn lại bây giờ là một hệ thống với dữ liệu bị tàn phá nặng nề hoặc mọi thứ đã biến thành tro khi cháy nổ xảy ra. Chính vì thế Windows khuyến cáo bạn nên sao lưu dự phòng dữ liệu sang một nơi khác vị trí địa lý với nơi đặt server và nếu tốt hơn là sao lưu dự phòng với tần suất mỗi ngày một lần là tốt hơn cả.

Nhưng hãy tượng tượng xem không lẽ mỗi ngày ta phải sao lưu cả hệ thống hàng chục thậm chí hàng trăm **GB** ra đĩa và đem cất đi, ngày qua ngày thì chi phí cho ta đầu tư để dự phòng dữ liệu có lẽ là một con số khổng lồ mà với qui mô nhỏ may ra còn kham nổi, nhưng với những công ty có đến hàng trăm máy thì e ra có vẻ kinh khủng quá

Chuẩn bị:

PC1: Windows server 2008

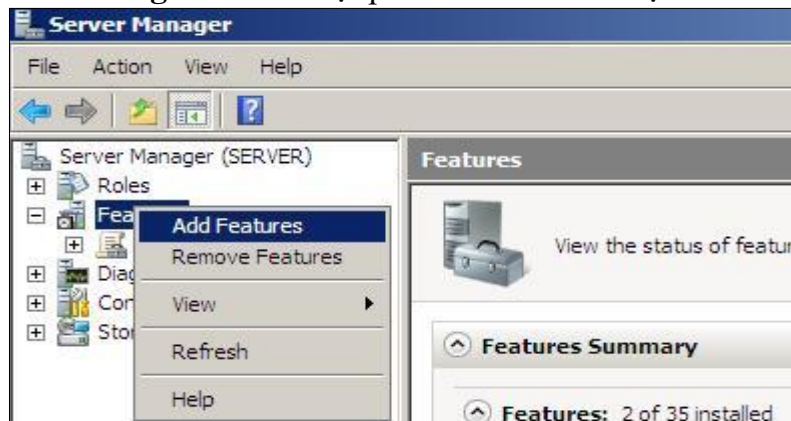
PC2: Windows server 2008

PC2: Tạo User **U1** password **123** . Tạo và Share thư mục **BACKUP** trên ổ **C** phân quyền cho **U1** quyền **Everyone- Full control** trên thư mục này.

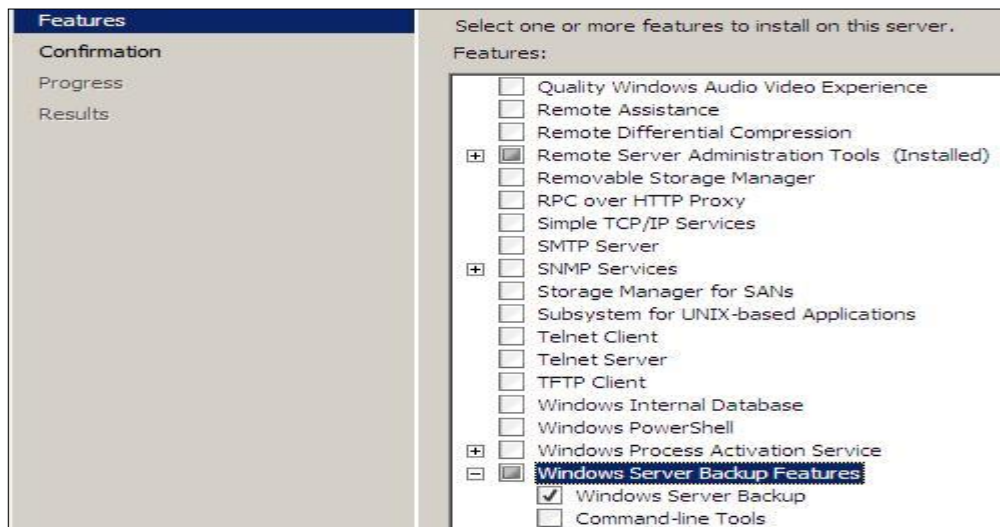
Thực hiện: Trên PC1

1. BACKUP

B1: Mở **server manager** click chuột phải lên **Feature** chọn **Add Features**



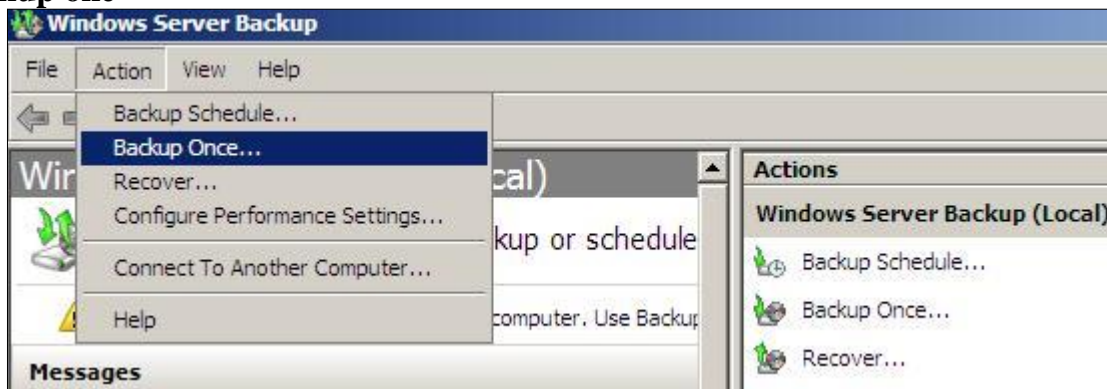
B2: Màn hình **Welcom** chọn **next** chọn **Windows server backup Features** chọn **next** chọn **Install**



B3: Tạo thư mục **C:\DATA** và 2 File text tên **Dulieu1.txt** và **Dulieu2.txt**



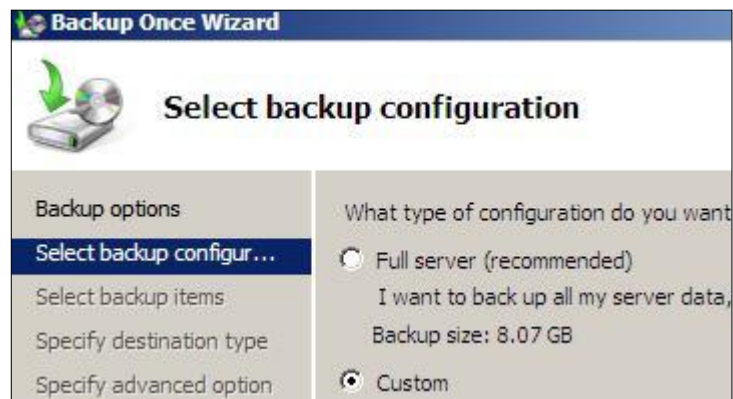
B4: Mở **Windows server backup** trong **Administrative tools** khung **Action** chọn **Backup one**



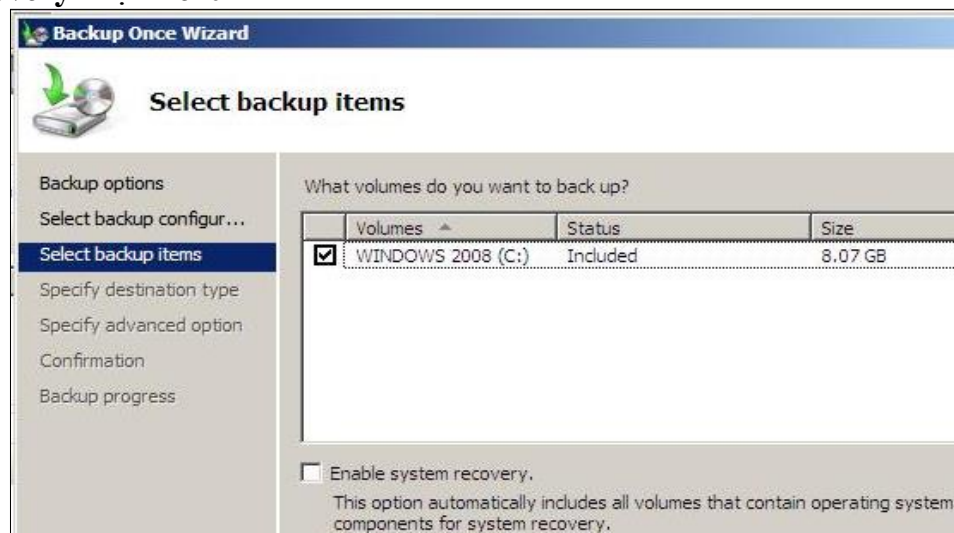
B5: Cửa sổ **Backup Options** chọn **Different Options** chọn **next**



B6: Hộp thoại **Select Backup configuration** chọn **Custom** chọn **Next**



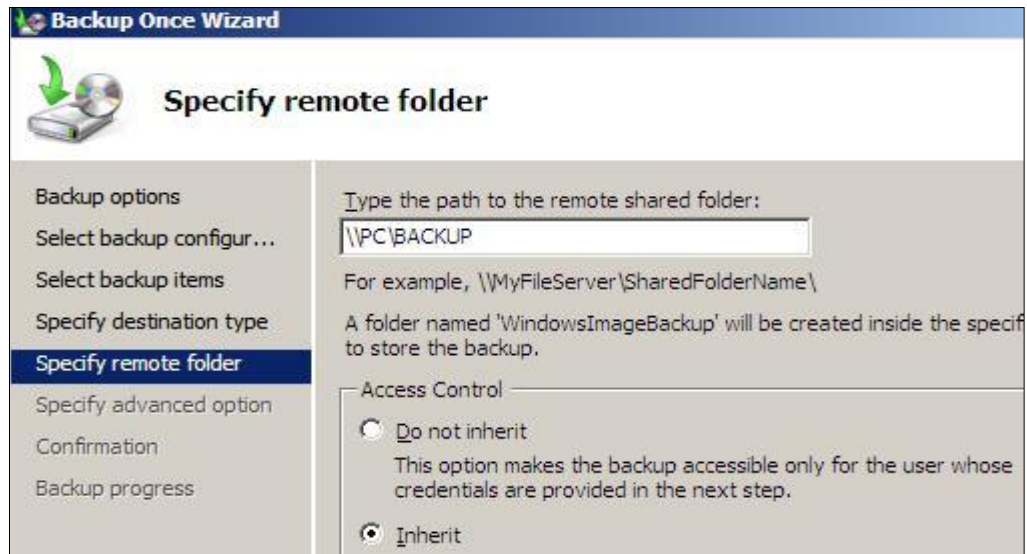
B7: Hộp thoại **Select backup items** Chọn **Server(C)** Bỏ dấu check trước dòng **Enable system recovery** chọn **next**



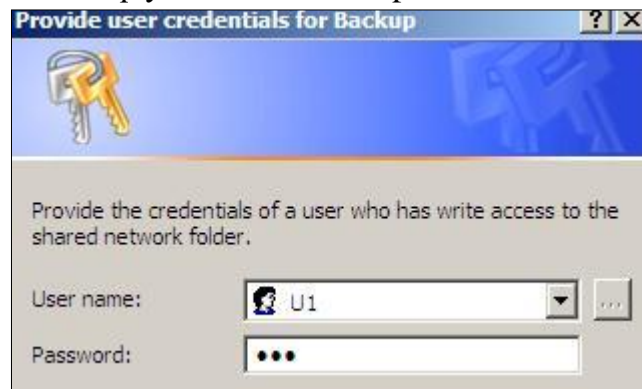
B8: Hộp thoại **Specify destination type** chọn **Remote shared folder** chọn



B9: Trong phần **Type the path to the Remote shared folder** gõ **\\PC2\BACKUP**
Chọn **Do not inherit** chọn **next**



B10: Hộp thoại xác nhận quyền: điền vào **U1** password **123** chọn **OK**

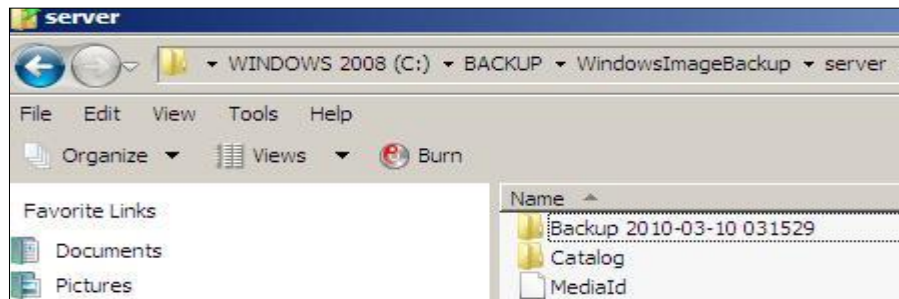


B11: Hộp thoại **Specify advanced option** chọn **vss copy backup (recommended)** chọn **next** chọn **next**



B12: Chọn **Backup** sau khi Backup xong chọn **Close**

B13: Trên **PC2** mở thư mục **BACKUP** chọn **WindowsImageBackup** chọn **PC1** Quan sát nơi chứa các file backup từ **PC1**

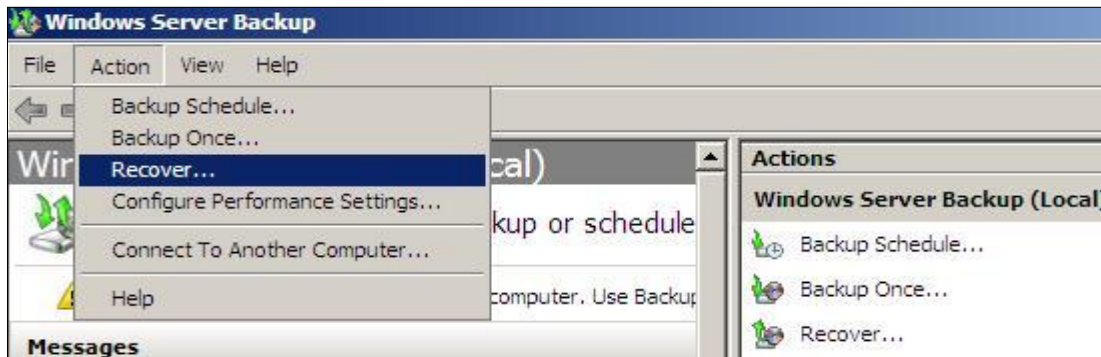


2. RECOVER

Trước khi Restore giả lập mất dữ liệu bằng cách **PC1** xóa thư mục **DATA**

Tiến hành khôi phục dữ liệu

B1: Trong chương trình **Windows server Backup** trong khung **Action** chọn **Recover**

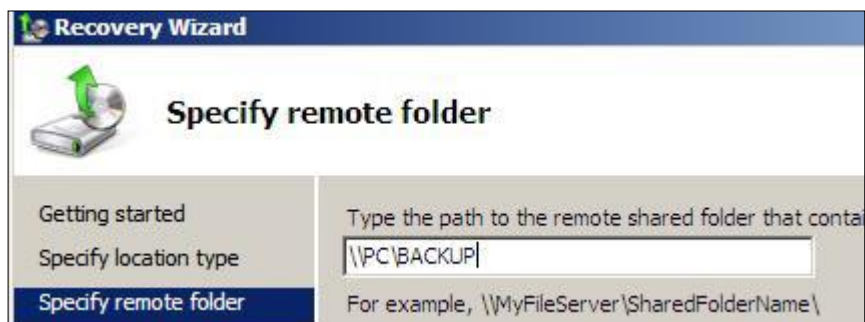


B2: Hộp thoại **Getting started** chọn **Another server** chọn **next**

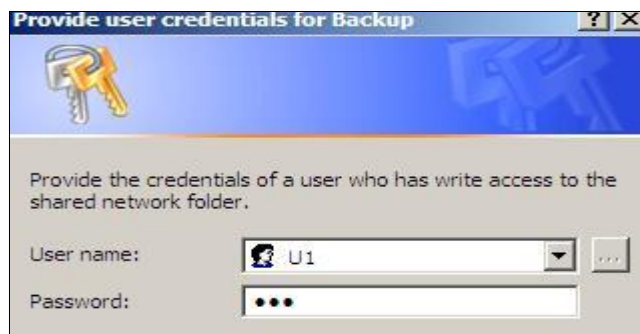


B3: **Specify remote folder** gõ **\\PC2\BACKUP** chọn **Next**





B4: Điền **username** và **password** của U1 chọn **Ok**



B5: **Select backup date** chọn **next**



B6: **Select recovery type** chọn **Files and folders** chọn **next**



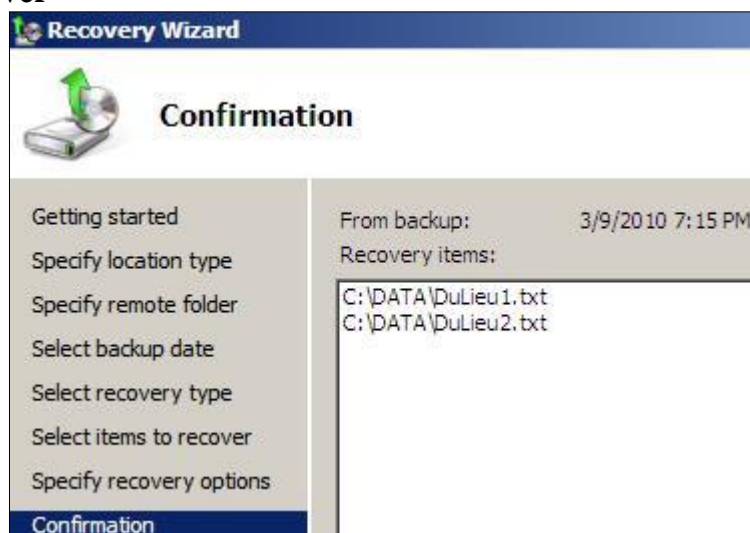
B7: **Select Items to recover** chọn thư mục **DATA** chọn **next**



B8: Specify recovery options giữ mặc định chọn next



B9: chọn **Recover**



Kiểm tra trên **PC1**: Sau khi Recover hoàn tất , mở ổ C quan sát thấy Folder **DATA** và các File trong **DATA** đã được khôi phục.