NHẤT NGHỆ

TRUNG TÂM ĐÀO TẠO CNTT NHẤT NGHỆ
ĐỐI TÁC ĐÀO TẠO CỦA MICROSOFT TẠI VIỆT NAM
105 Bà Huyện Thanh Quan, Quận 3, TP.HCM
Tel: 08.39322.735 – 0913.735.906
Website: www.nhatnghe.com

Microsoft Partner

QUẢN TRỊ MẠNG *Microsoft*

LAB MCSA 2012

WINDOWS SERVER 2012

MÔN 70-410

MỤC LỤC

LOCAL USERS – LOCAL GROUPS

CÁC BƯỚC TRIỂN KHAI:

*** Phần 1: Thực hiện trên Window Server 2012**

1. Tắt User Account Control (UAC)
2. Tạo Local User Account
3. Cấu hình Log on tự động bằng account định sẵn
4. Tạo local group account
5. Network access

*** Phần 2: Thực hiện trên Windows 8.1**

1. Tạo Local User và Group
2. Tham khảo các Option khi nhấn Ctrl + Alt + Del
3. Enabled Account Administrator
4. Tham khảo các Option của User Account
5. Cho máy tính tự động log on với account định sẵn

A- CHUẨN BỊ

Mô hình bài lab bao gồm 2 máy

- PC01: Windows Server 2012 R2
- PC02: Windows Server 2012 R2
- 2 máy tắt firewall. Kiểm tra bằng lệnh Ping giữa 2 máy

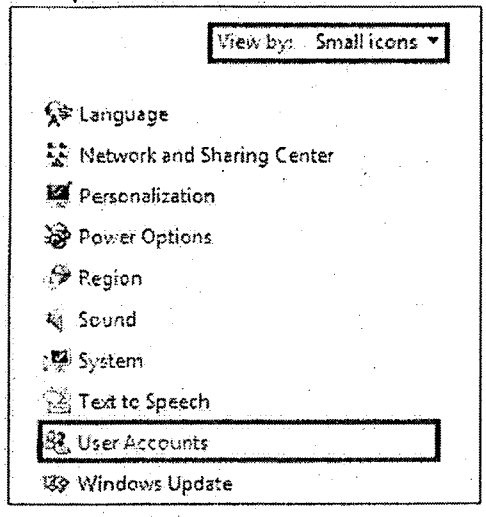
B- THỰC HIỆN

* Phần 1: Thực hiện trên Window Server 2012

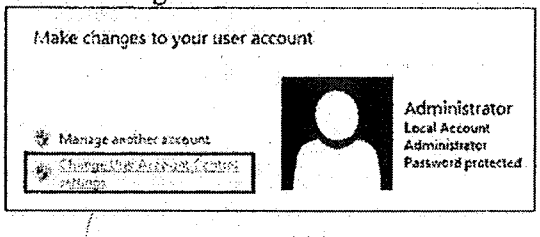
1. Tắt User Account Control (UAC)

B1 - Nhấn tổ hợp phím ⊞ + X → chọn Control Panel hoặc nhấn phím P

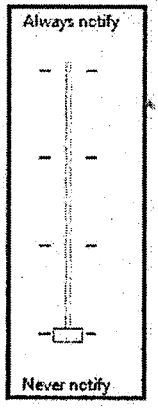
B2 - Ở mục View By → chọn Small icons → chọn User Accounts



B3 - Nhấn vào mục Change User Account Control settings



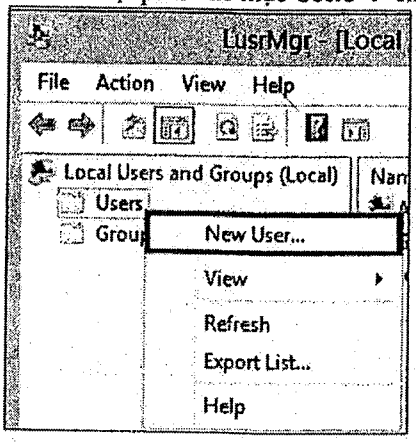
B4 - Cuộn thanh cuộn xuống cuối cùng Never Notify và nhấn OK. Sau đó khởi động lại máy để thay đổi có hiệu lực.



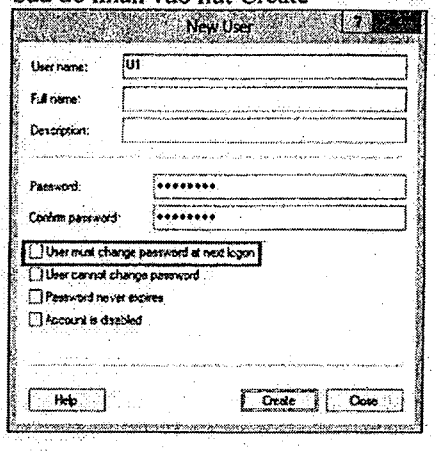
2. Tạo Local User Account

B1 - Mở chương trình Local Users and Groups bằng cách nhấn tổ hợp phím ⊞ + R → gõ lệnh lusrmgr.msc

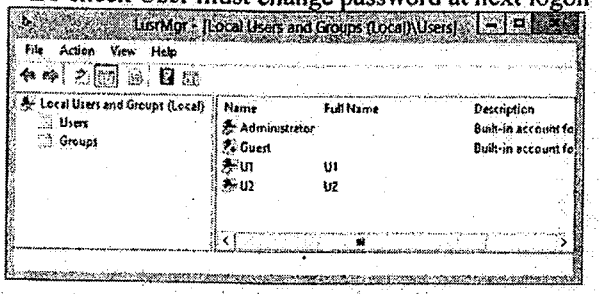
B2 - Chuột phải vào mục Users → chọn New User.



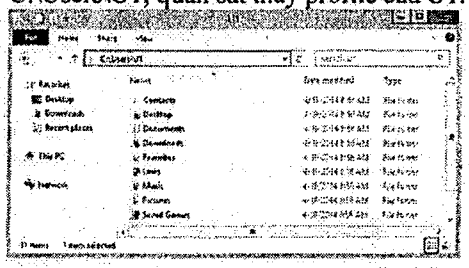
B3 - Điền vào các thông tin sau:
+ Username : U1
+ Password và Confirm password : P@ssword
+ Bỏ check User must change password at next logon
Sau đó nhấn vào nút Create



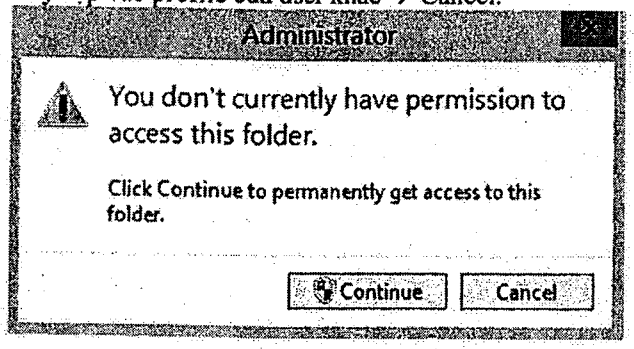
B4 - Tương tự tạo thêm user U2 với các thông số sau
+ Username : U2
+ Password/Confirm password : P@ssword
+ Bỏ check User must change password at next logon



B5 - Log on user U1. Truy cập vào thư mục C:\Users\U1, quan sát thấy profile của U1.



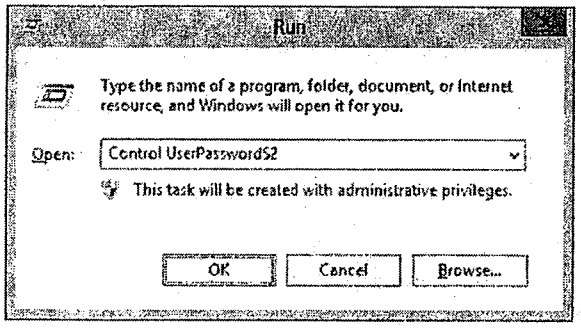
B6 - Tiếp theo thử truy cập thư mục C:\Users\Administrator, sẽ thấy báo lỗi không có quyền truy cập vào profile của user khác → Cancel.



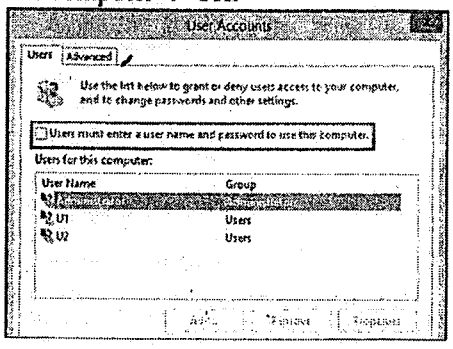
3. Cấu hình Log on tự động bằng account định sẵn

B1 - Log on bằng account Administrator, nhấn Ctrl + Alt + Del →chọn Change Password. Đổi mật khẩu thành P@ssword456

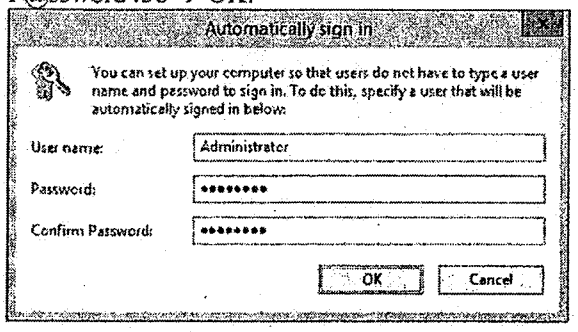
B2 - Nhấn tổ hợp phím ⊞ + R, gõ lệnh Control UserPasswords2



B3 - Ở mục Users for this computer → chọn Administrator. Sau đó bỏ check ở ô Users must enter a user name and password to use this computer → OK.



B4 - Nhập vào mật khẩu của account Administrator: P@ssword456 → OK.



B5 - Kiểm tra : Khởi động lại máy. Máy tính tự động đăng nhập bằng account Administrator, không hỏi password

4. Tạo local group account

B1 - Nhấn tổ hợp phím ⊞ + R, gõ lệnh lusrmgr.msc

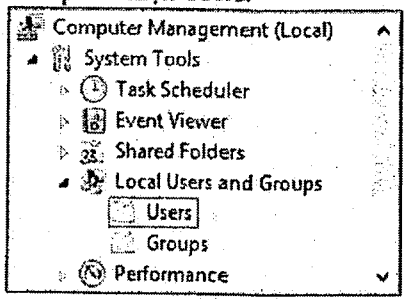
*** Phần 2: Thực hiện trên Windows 8.1**

Chuẩn bị: Ghost máy PC01 bản Windows 8.1

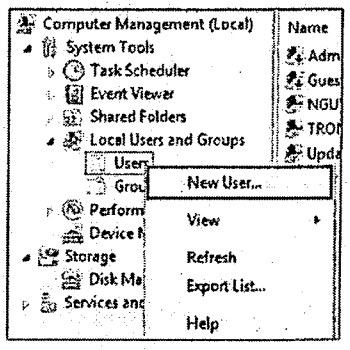
1. Tạo Local User và Group

B1 - Mở File Explorer, chuột phải vào This PC → chọn Manage

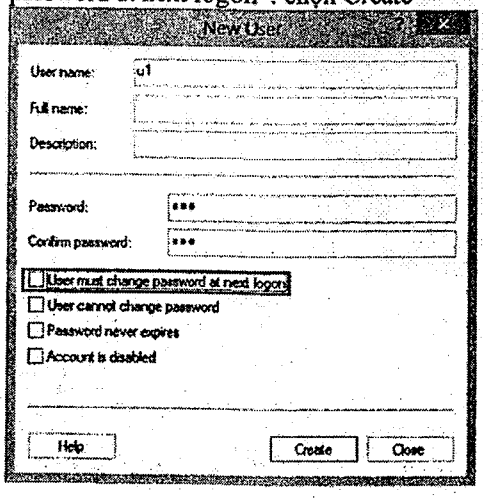
B2 - Ở khung bên trái, bung mục Local Users and Groups → chọn Users.



B3 - Chuột phải vào Users → New User

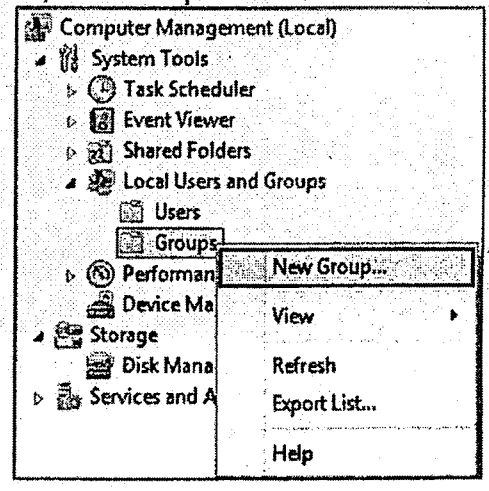


B4 - Trong cửa sổ New User, khai báo các thông tin:
+ User name: u1
+ Password: 123
+ Confirm Password: 123
+ Bỏ dấu check trước dòng "User must Change password at next logon", chọn Create



B5 - Log Off. Quan sát thấy đã có thêm user account mới trong phần log on.

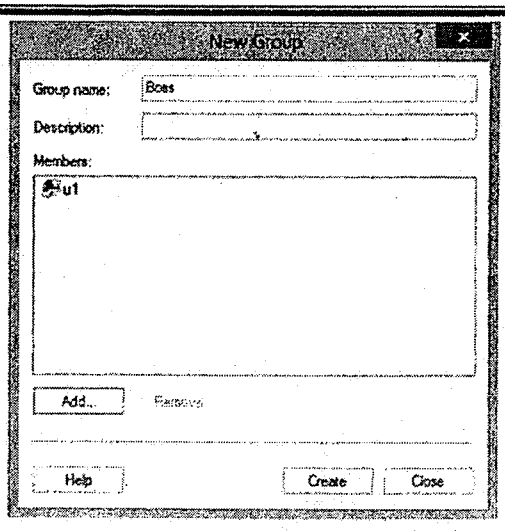
B6 - Tiếp theo chuột phải lên mục Groups → chọn New Group



B7 - Trong cửa sổ New Group, ở mục Group Name, bạn đặt tên group là: Boss → Add

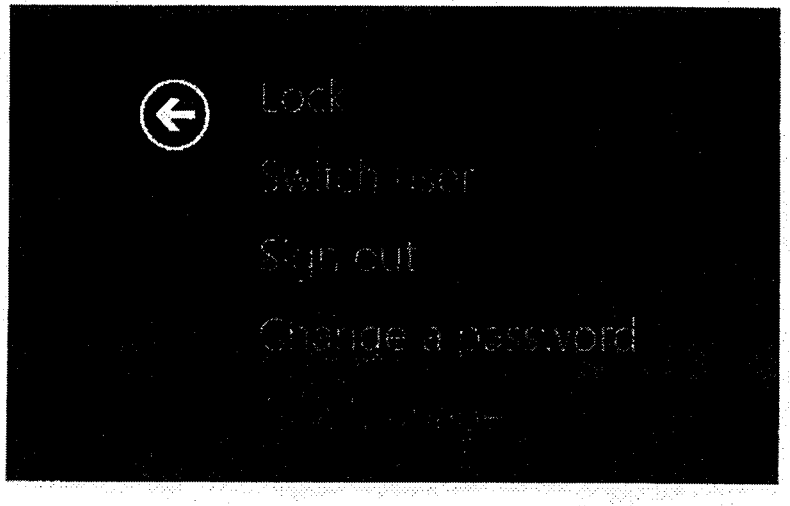
B8 - Nhập vào u1 → Checks Name → OK

B9 - Quan sát thấy user u1 đã được thêm vào group Boss → Create.



2. Tham khảo các Option khi nhấn Ctrl + Alt + Del

- Nhấn tổ hợp phím Ctrl + Alt + Delete.



- Quan sát thấy các tùy chọn:

+ Lock: Khóa máy tính

+ Switch User: Chuyển qua môi trường làm việc của user khác mà không tắt session hiện tại

+ Sign out: Chuyển qua môi trường làm việc của user khác và tắt session hiện tại

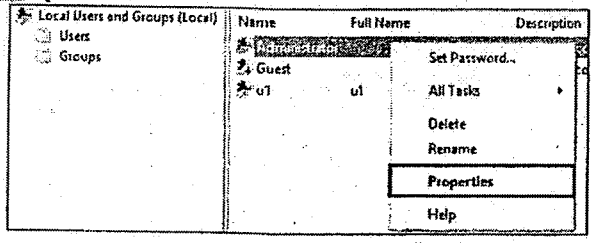
+ Task Manager: Dùng để xem các thông số performance của máy tính

3. Enabled Account Administrator

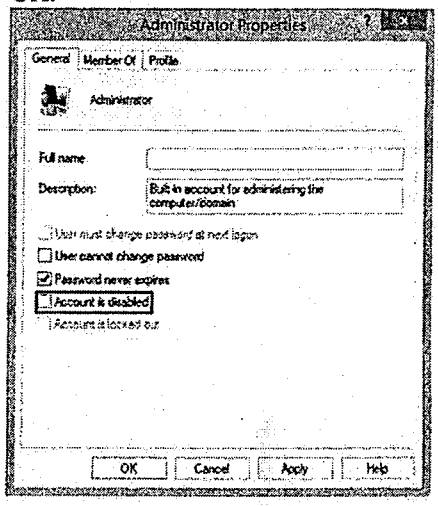
B1 - Mở File Explorer, chuột phải vào This PC → chọn Manage

B2 - Ở khung bên trái, bung mục Local Users and Groups → chọn Users.

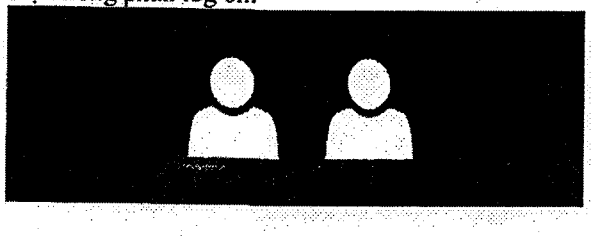
B3 - Chuột phải lên account "Administrator"→ chọn Properties.



B4 - Bỏ check "Account is disabled" → OK.



B5 - Log off và quan sát account Administrator đã xuất hiện trong phần log on.



4. Tham khảo các Option của User Account

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Account is disabled
- ☐ Account is locked out

+ User must change password at next logon : User phải đổi password trong lần log on đầu tiên

+ User cannot change password: User không có quyền đổi password

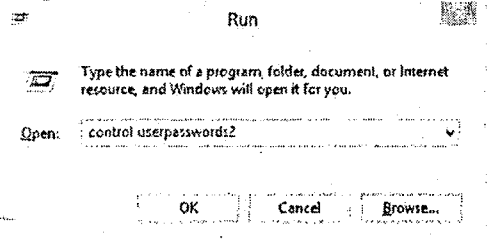
+ Password nerver expires: Password của user không bao giờ bị hết hạn

+ Account is disabled: Vô hiệu hóa Account

+ Account is locked out: Account tạm thời bị khóa

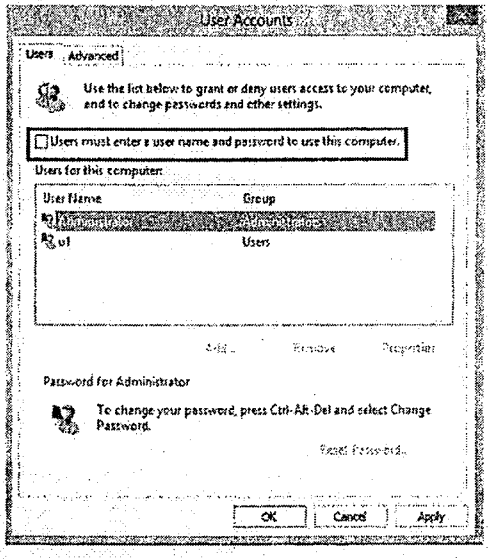
5. Cho máy tính tự động log on với account định sẵn

B1 - Gõ tổ hợp phím: ⊞ + R, nhập lệnh control userpasswords2



B2 - Bỏ check " Users must enter a username and paswword to use this computer"

B3 - Ở mục "Users for this computer"→ chọn Administrator



B4 - Kiểm tra : Khởi động lại máy. Máy tính tự động đăng nhập bằng account Administrator, không hỏi password.

LOCAL POLICY

CÁC BƯỚC TRIỂN KHAI:

1. Cấu hình Local Policy

a. Điều chỉnh policy Computer Configuration

b. Điều chỉnh policy User Configuration

2. Cấu hình Local User Policy

A- CHUẨN BỊ

- Mô hình bài lab bao gồm 1 máy Windows Server 2012 R2

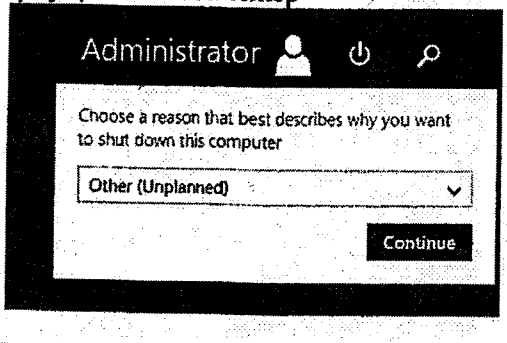
- Tạo user Teo, Password: P@s

B- THỰC HIỆN

1. Cấu hình Local Policy

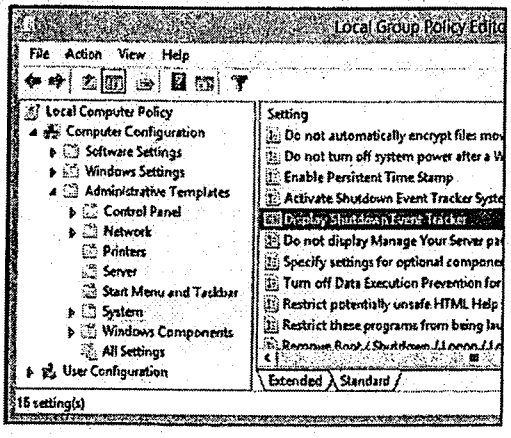
a. Điều chỉnh policy Computer Configuration

B1 - Log on vào máy bằng account Administrator. Nhấn phím ⊞, chọn biểu tượng Turn Off → Shut down. Xuất hiện bảng Shutdown Event Tracker. Nhấn phím ⊞ để quay lại màn hình Desktop



B2 - Nhấn tổ hợp phím ⊞ + R, gõ lệnh Gpedit.msc

B3 - Lần lượt mở theo đường dẫn: Local Computer Policy → Computer Configuration → Administrative Templates → System. Ở khung bên phải nhấn double click vào Display Shutdown Event Tracker.



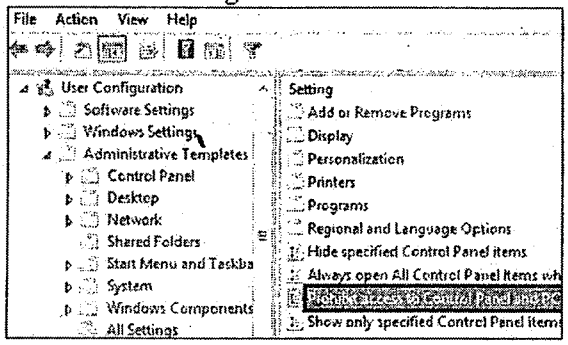
B4 - Chọn Disabled → OK

B5 - Thử kiểm tra nhấn phím ⊞, chọn biểu tượng Turn Off → Shut down → Không thấy xuất hiện bảng Shutdown Event Tracker nữa.

b. Điều chỉnh policy User Configuration

B1 - Mở Control Panel → Truy cập thành công.

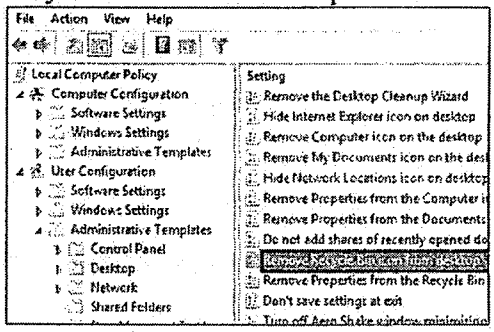
B2 - Lần lượt mở theo đường dẫn: Local Computer Policy → User Configuration → Administrative Templates → Control Panel. Ở khung bên phải, nhấn double click vào Prohibit access to Control Panel and PC Settings.



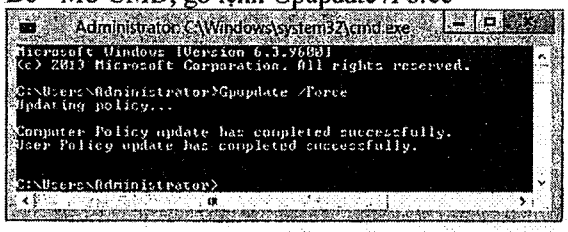
B3 - Chọn Enabled → OK

B4 - Kiểm tra: Truy cập vào Control Panel, xuất hiện thông báo lỗi chặn truy cập.

B5 - Quay lại cửa sổ Local Group Policy Editor. Mở theo đường dẫn Local Computer Policy → User Configuration → Administrative Templates → Desktop. Ở khung bên phải, nhấn double click Remove Recycle Bin icon from Desktop → Enabled.

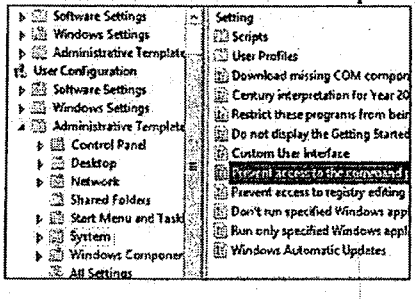


B6 - Mở CMD, gõ lệnh Gpupdate /Force

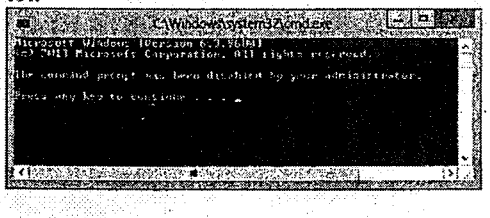


B7 - Kiểm tra: Log off và log on lại máy sẽ thấy mất biểu tượng Recycle Bin trên desktop.

B8 - Quay lại cửa sổ Local Group Policy Editor. Mở theo đường dẫn Local Computer Policy → User Configuration → Administrative Templates → System. Ở khung bên phải, nhấn double click vào Prevent access to the command prompt → Enabled



B9 - Truy cập thử vào CMD sẽ thấy bị báo lỗi.

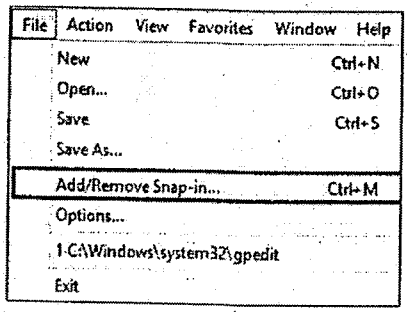


B10 - Sau khi thực hiện xong, trả các policy vừa thiết lập về mặc định như lúc đầu.

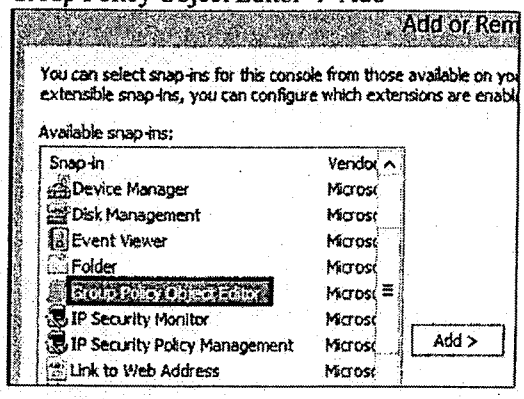
2. Cấu hình Local User Policy

B1 - Nhấn tổ hợp phím ⊞ + R, gõ lệnh MMC

B2 - Cửa sổ Console 1, vào menu File → Add/Remove Snap-in… hoặc nhấn tổ hợp phím Ctrl + M



B3 - Ở khung Available snap-ins bên trái, chọn Group Policy Object Editor → Add

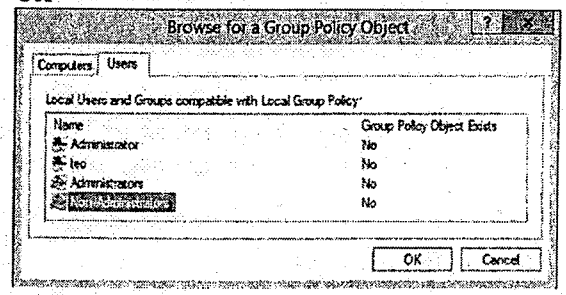


B4 - Nhấn Finish

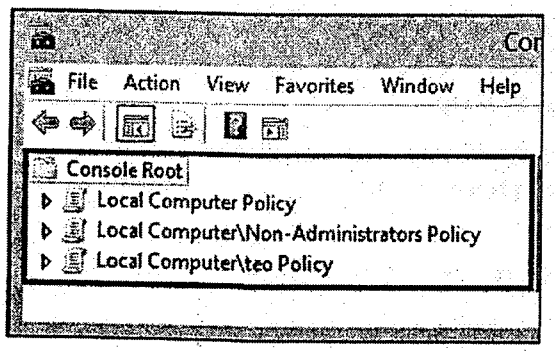
B5 - Tiếp tục vào menu File, chọn Add/Remove Snap-in… → Group Policy Object Editor → Add

B6 - Nhấn nút Browse

B7 - Qua tab Users → chọn Non-Administrators → OK

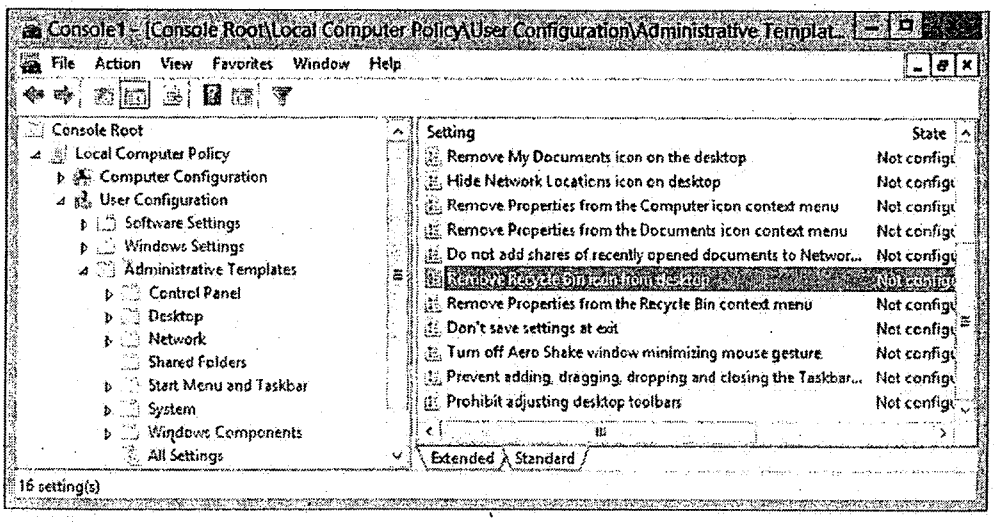


B8 - Tương tự, vào menu File, chọn Add/Remove Snap-in… → Group Policy Object Editor → Add → Browse → Qua tab Users, chọn User Teo. Quan sát thấy có 3 policy vừa add ứng với từng đối tượng: Computer Policy, Non-Administrators Policy và Teo Policy



*** TH1: Chỉnh Local Computer Policy xóa Recycle Bin trên Desktop**

- Mở theo đường dẫn: Local Computer Policy → User Configuration → Administrative Templates → Desktop. Ở khung bên phải, nhấn double click Remove Recycle Bin icon from Desktop → Enabled.



- Kiểm tra: Log on User Teo, kiểm tra thấy biểu tượng Recycle Bin bị mất trên Desktop

*** TH2: Chỉnh Non-Administrators Policy không xóa Recycle Bin trên Desktop**

- Log on Administrator. Mở theo đường dẫn: Local Computer\Non-Administrators Policy → User Configuration → Administrative Templates → Desktop. Ở khung bên phải, nhấn double click Remove Recycle Bin icon from Desktop → Disabled.

- Kiểm tra: Log on User Teo, kiểm tra thấy biểu tượng Recycle Bin **KHÔNG** bị mất trên Desktop

*** TH3: Chỉnh Teo Policy xóa Recycle Bin trên Desktop**

- Log on Administrator. Mở theo đường dẫn: Local Computer\teo Policy → User Configuration → Administrative Templates → Desktop. Ở khung bên phải, nhấn double click Remove Recycle Bin icon from Desktop → Disabled

- Kiểm tra: Log on User Teo, kiểm tra thấy biểu tượng Recycle Bin bị mất trên Desktop

LOCAL SECURITY POLICY

CÁC BƯỚC TRIỂN KHAI:

1. Password Policy

2. Account Lockout Policy

3. User Rights Assignment

4. Network Access

A- CHUẨN BỊ

- Mô hình bài lab bao gồm 2 máy

* PC01: Windows Server 2012 R2

* PC02: Windows Server 2012 R2

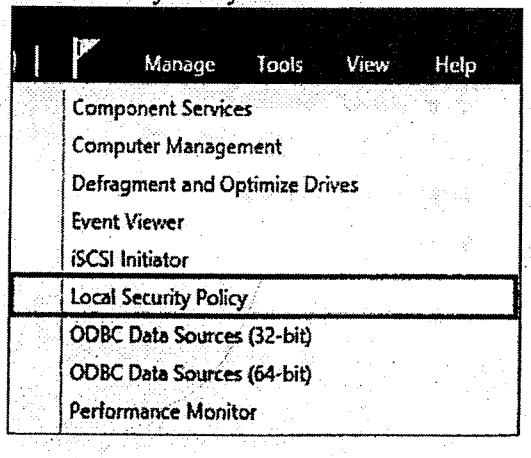
- 2 máy tắt Firewall → Kiểm tra đường truyền bằng lệnh PING

B- THỰC HIỆN

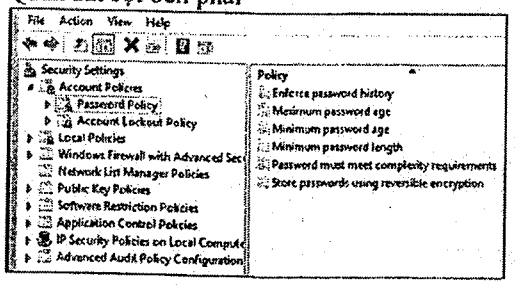
1. Password Policy (Thực hiện trên PC01)

B1 - Log on Administrator → Tạo user bằng password : 123 → báo lỗi không thể tạo được do không thỏa yêu cầu về độ phức tạp của password

B2 - Mở Server Manager, vào menu Tools → Local Security Policy



B3 - Mở Account Polices → Password Policy. Quan sát cột bên phải



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

+ Maximum password age : Thời gian sử dụng tối đa của 1 password (khuyên dùng: 42)

+ Minimum password age : Thời gian sử dụng tối thiểu của 1 password (khuyên dùng: 1)

+ Minimum password length : Độ dài tối thiểu của 1 password (khuyên dùng: 7)

+ Password must meet complexity requirements: Yêu cầu password phức tạp (khuyên dùng: Enabled)

→ Chỉnh password policy :

B4 - Password must meet complexity requirements → Chọn Disabled

B5 - Các password policy còn lại chỉnh giá trị về 0 → OK

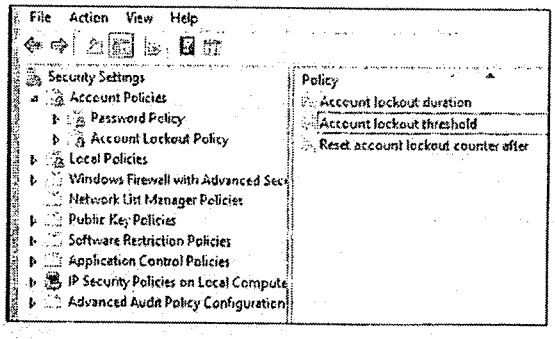
B6 - Mở CMD → gõ lệnh Gpupdate /Force

B7 - Kiểm tra: Tạo account U1 với password : 123 → Tạo thành công

2. Account Lockout Policy

B1 - Mở Local Security Policy. Truy cập theo đường dẫn Account Policies → Account Lockout Policy

B2 - Quan sát các policy bên phải
+ Account lockout duration: Thời gian account bị khóa
+ Account lockout threshold : Số lần nhập sai password trước khi account bị khóa
+ Reset account lockout counter after : thời gian chuyển bộ đếm về giá trị 0
- Điều chỉnh thông số các policy :
+ Account lokout threshold : 3
+ Account lockout duration : 30
+ Reset account lockout counter after : 30



B3 - Kiểm tra: Đăng nhập sai password 3 lần → không thể đăng nhập tiếp. Chờ sau 30 phút → có thể đăng nhập lại.

3. User Rights Assignment

Yêu cầu:

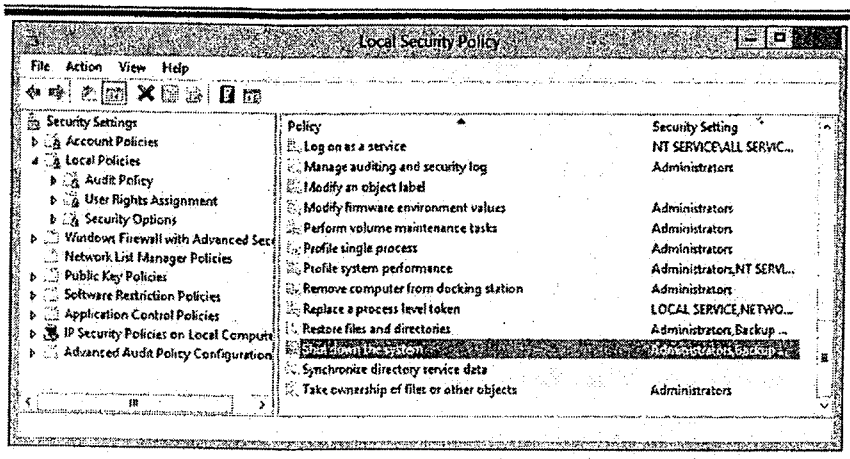
+ Log on bằng quyền U1 → shut down máy tính → không được

+ Thay đổi ngày giờ hệ thống → không được

B1 - Log on Administrator → Mở local security policy → Local Policies → User Rights Assignment → cột bên phải: Quan sát 2 policy

+ Change the system time: Cho phép user/group có quyền thay đổi ngày giờ hệ thống

+ Shutdown the system: Cho phép user/group có quyền tắt máy



B2 - Điều chỉnh thông số policy

+ Change the system time: Đưa group Users vào

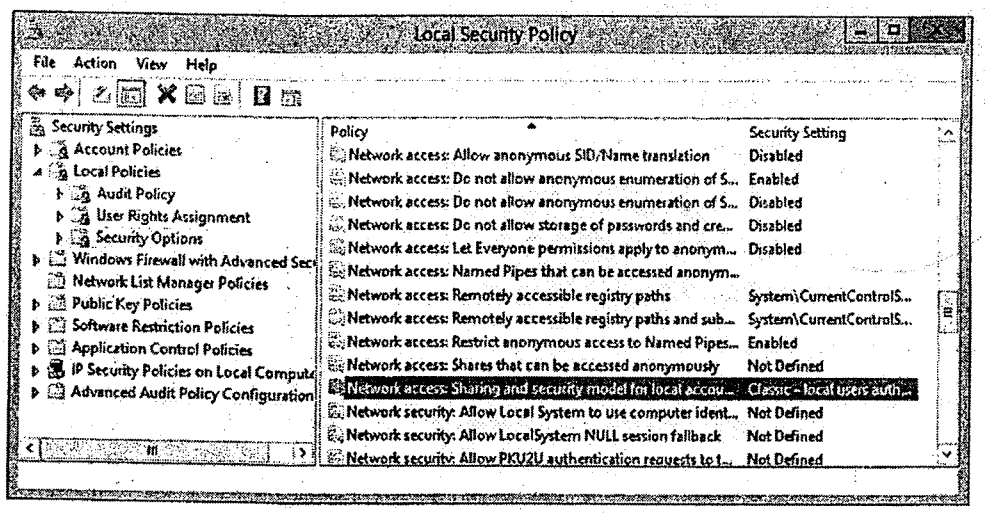
+ Shutdown the system: Đưa group Users vào

B3 - Kiểm tra : Log on U1 → Shut down thử → thành công. Thay đổi ngày giờ hệ thống → thành công

4. Network Access

*** Trường hợp 1: Classic**

- Mở Local Security Policy → Local Policy → Security Options → Double click Network access : Sharing and security model for local account. (Mặc định Windows Server chạy Classic).



a. Classic: 2 máy cùng password (Thực hiện trên cả 2 máy)

- Đổi password administrator là 123

- Thực hiện truy cập bằng URL từ Máy PC01 qua Máy PC02 và ngược lại

- Tại PC02 : Nhấn tổ hợp phím ⊞ + R, gõ \\PC01 → truy cập thành công mà không hỏi username và password

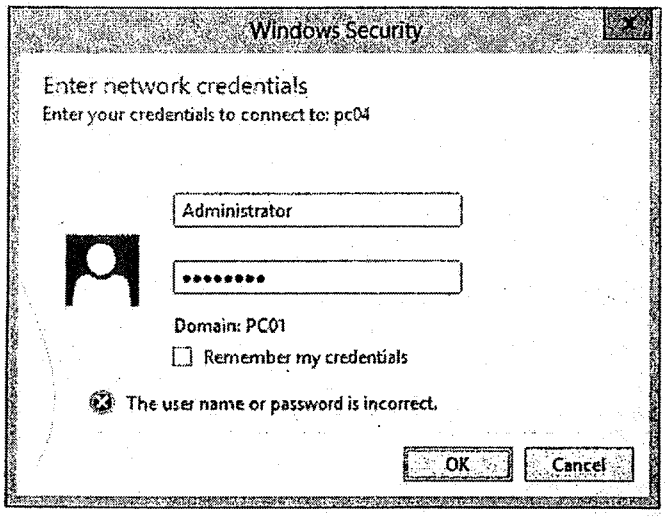
- Nhận xét : Khi truy cập vào PC02 nếu account dùng để log on trên Máy PC01 trùng user name và password với 1 account trên máy PC 02 , thì khi network access sẽ không bị hỏi username và password

b. Classic: 2 máy khác password (Thực hiện trên cả 2 máy)

- Đổi password administrator Máy PC01 thành 123 , password administrator Máy PC02 thành 456 → Log on vào PC01 bằng account administrator

- Thực hiện truy cập bằng URL từ Máy PC01 qua Máy PC02 và ngược lại

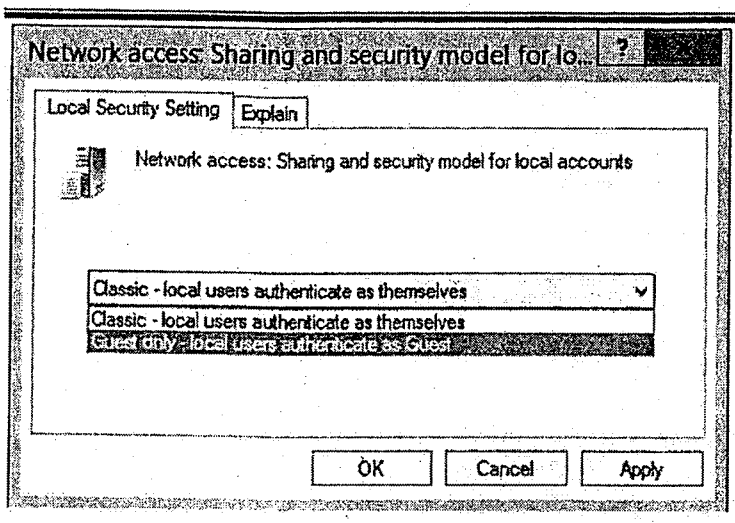
- Tại PC01 : Nhấn tổ hợp phím ⊞ + R, gõ \\PC02 → Hiện thông báo đòi User name and password → Khai báo username và password Máy PC02 → OK → Truy cập thành công qua PC02



*** Trường hợp 2: Guest only** (Thực hiện trên cả 2 máy)

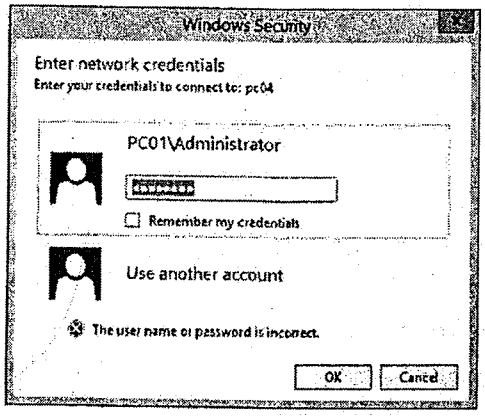
- Máy PC02: Enabled user Guest.

- Mở Local Security Policy → Local Policy → Security Options → Double click Network access: Sharing and security model for local account → Guest only – local users authenticate as Guest.



- PC01 truy cập vào PC02: Không hỏi username, password. Mặc định chứng thực bằng account Guest.

- PC02: Disabled account Guest. PC01 truy cập vào PC02 sẽ bị hỏi User name và password , tuy nhiên dù nhập account Administrator cũng không thể truy cập được vì chỉ có thể truy cập bằng bằng account Guest (Đã bị disable).



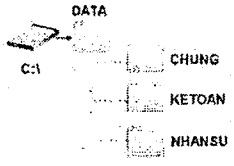
NTFS

CÁC BƯỚC TRIỂN KHAI

1. Phân quyền thư mục bằng Standard Permission
2. Phân quyền thư mục bằng Special Permission
3. Take OwnerShip
4. Xét quyền khi di chuyển dữ liệu

A- CHUẨN BỊ

- Mô hình bài lab bao gồm 1 máy sử dụng bản ghost Windows Server 2012 R2
- Tạo cây thư mục như trong hình:



- 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

B- THỰC HIỆN

1. 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:

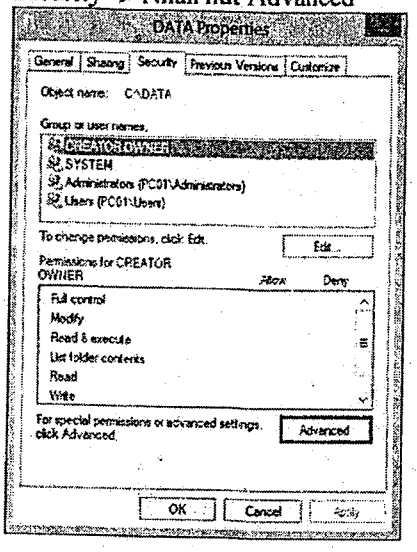
+ Group Ketoan có quyền ***Full****. Group Nhansu* ***không có quyền***

- Trên thư mục Nhansu:

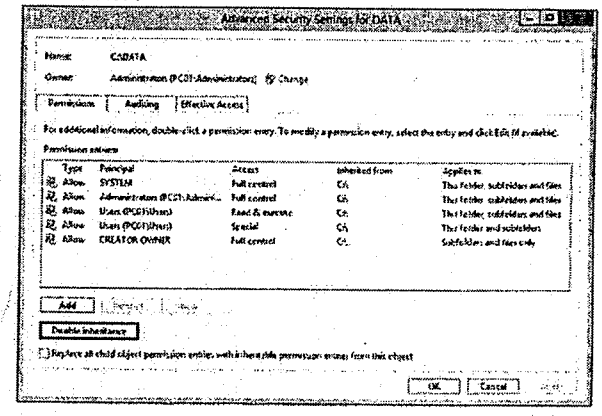
+ Group Nhansu có quyền ***Full****. Group Ketoan* ***không có quyền***

a. Phân quyền trên thư mục DATA

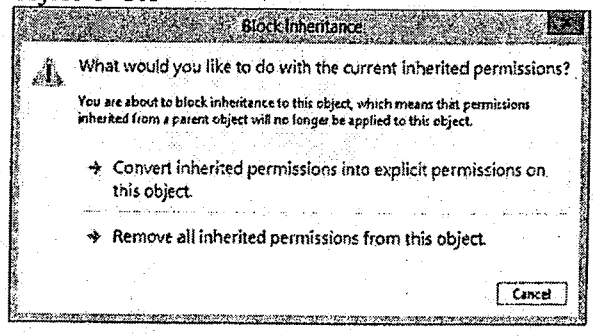
B1 - Chuột phải lên thư mục DATA → Chọn Properties → Qua tab Security → Nhấn nút Advanced



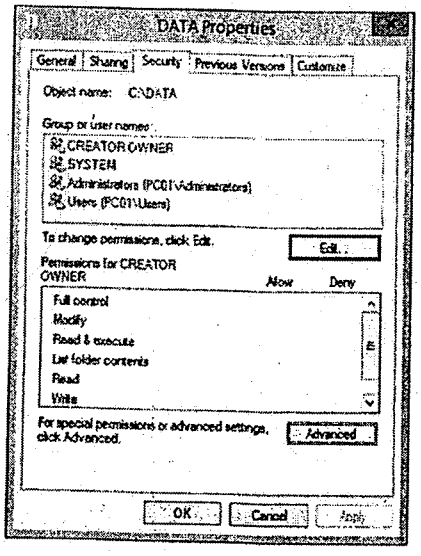
B2 - Trong tab Permissions → Chọn Disable Inheritance



B3 - Trong cửa sổ Block Inheritance, chọn Convert inherited permissions into explicit permissions on this object → OK

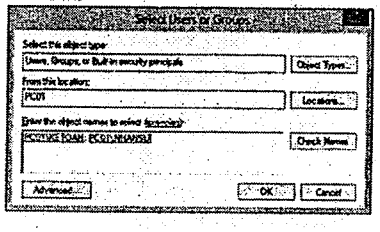


B4 - Quay lại cửa sổ DATA Properties → nhấn nút Edit

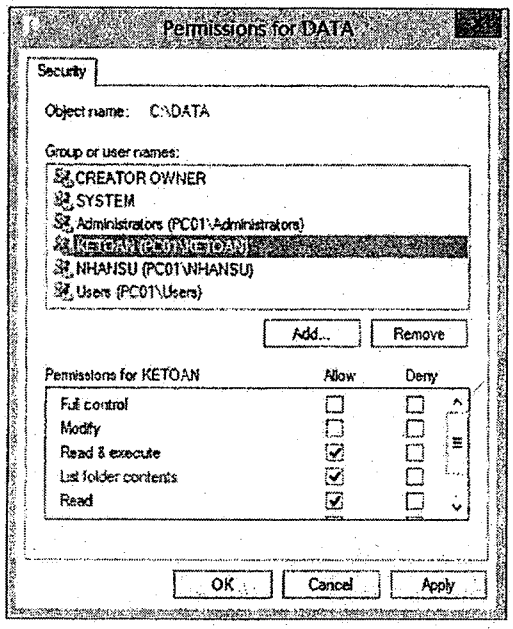


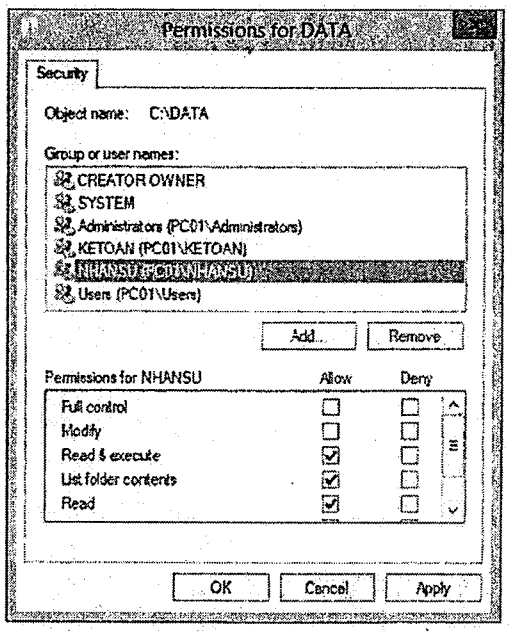
B5 - Cửa sổ Permissions for DATA → nhấn nút Add

B6 - Nhập vào: ketoan;nhansu → Chọn Check Names → OK

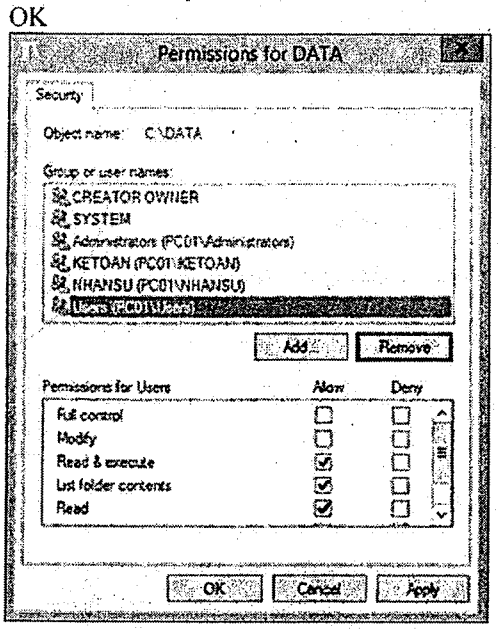


B7 - Quan sát 2 group KETOAN và NHANSU → có 3 quyền Allow: Read & excute, List folder contents, Read.





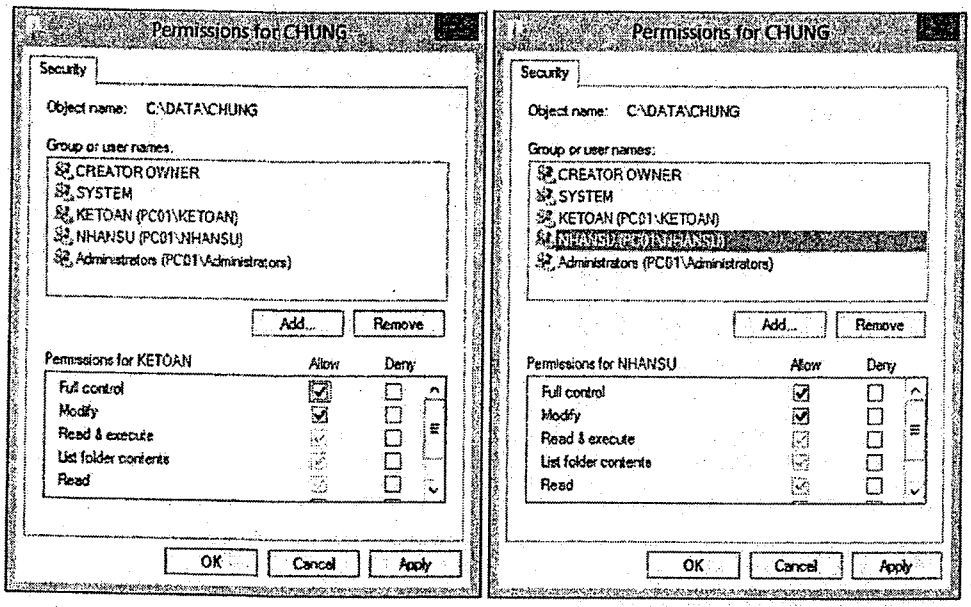
B8 - Chọn Group Users → Remove → OK → OK



B9 - Kiểm tra:
+ Lần lượt log on vào máy bằng quyền KT1, NS1 → Mở thư mục C:\DATA → truy cập thành công
+ Tạo Folder bất kì → xuất hiện báo lỗi không có quyền.

b. Phân quyền cho thư mục Chung

B1 - Log on Administrator → Chuột phải lên thư mục Chung, chọn Properties → Tab Security → Chọn Edit → Lần lượt chọn từng group KeToan và NhanSu → Chọ quyền Allow Full Control → 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 kì trong thư mục Chung → thành công

c. Phân quyền cho thư mục KETOAN

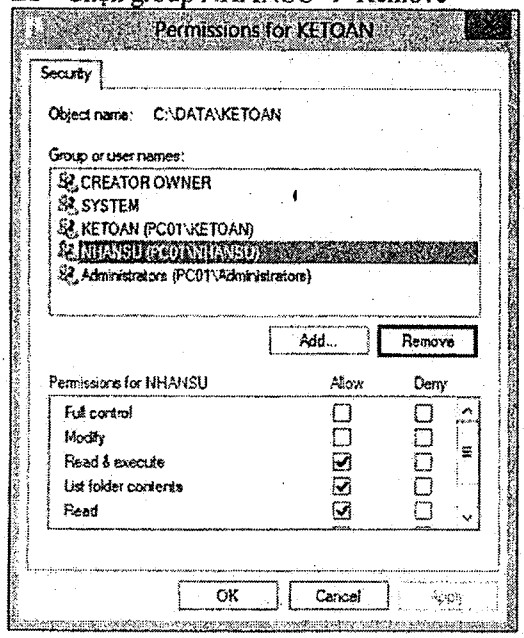
B1 - Chuột phải lên thư mục KETOAN → Chọn Properties → Qua tab Security → Chọn Advanced

B2 - Trong tab Permissions → Chọn Disable Inheritance

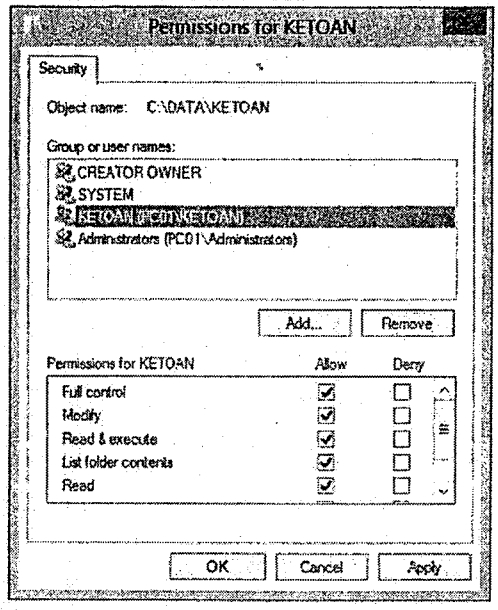
B3 - Trong cửa sổ Block Inheritance, chọn Convert inherited permissions into explicit permissions on this object → OK

B4 - Cửa sổ KETOAN Properties → Chọn Edit

B5 - Chọn group NHANSU → Remove



B6 - Chọn Group KETOAN → Chọn Allow Full Control → OK → OK



B7 - 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 kì trong thư mục KETOAN → thành công

d. Phân quyền cho thư mục NHANSU

B1 - Chuột phải lên thư mục NHANSU → Chọn Properties → Qua tab Security → Chọn Advanced

B2 - Trong tab Permissions → Chọn Disable Inheritance

B3 - Trong cửa sổ Block Inheritance, chọn Convert inherited permissions into explicit permissions on this object → OK

B4 - Cửa sổ NHANSU Properties → Chọn Edit

B5 - Chọn group KETOAN → Remove

B6 - Chọn Group NHANSU → Chọn Allow Full Control → OK → OK

B7 - 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

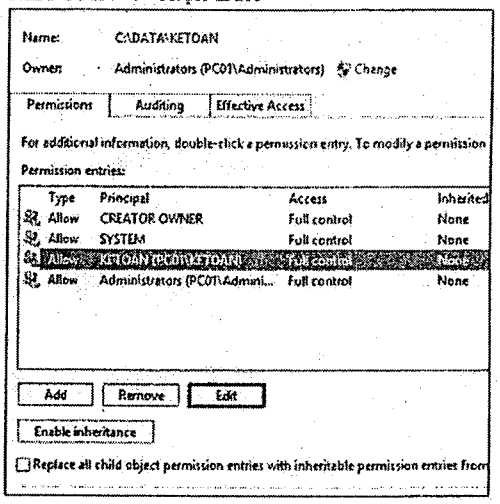
+ User NS1 tạo , xóa file, folder bất kì trong thư mục NHANSU → thành công

2. Phân quyền thư mục bằng Special Permission

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

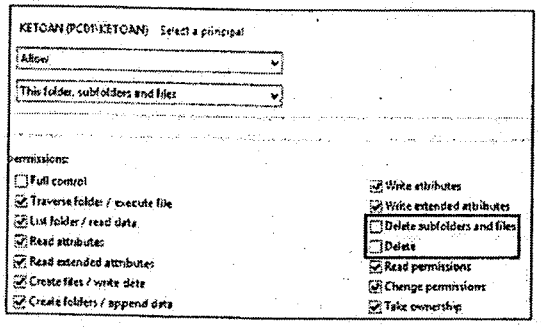
B1 - Chuột phải lên thư mục KETOAN → Chọn Properties → Qua tab Security → nhấn vào nút Advanced

B2 - Trong tab Permissions → chọn Group KETOAN → chọn Edit



B3 - Trong cửa sổ Permission Entry for KETOAN, nhấn vào liên kết Show advanced permissions.

B4 - Ở mục Allow, tắt dấu chọn ở ô Delete subfolders and files và Delete → Chọn OK 4 lần



B5 - Kiểm tra :

+ Lần lượt log on bằng KT1 và KT2 → truy cập vào thư mục KeToan

+ KT1 tạo file KT1.txt , KT2 tạo file KT2.txt

- Log on bằng KT1 → xóa file KT2.txt → báo lỗi không có quyền xóa . Xóa file KT1.txt → thành công

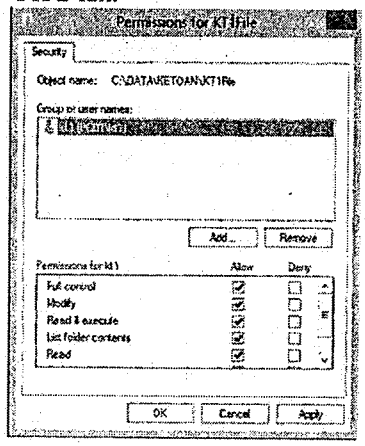
- Log on bằng KT2 → xóa file KT1.txt → báo lỗi không có quyền xóa . Xóa file KT2.txt → thành công

3. Take Owner Ship

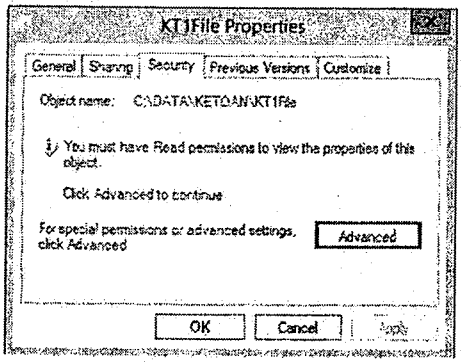
B1 - Log on KT1, truy cập vào folder KETOAN → tạo folder KT1file

B2 - Phân quyền NTFS trên thư mục KT1file. Chuột phải thư mục KT1File → Chọn Properties → Qua tab security → Chọn Advanced → Disable Inheritance

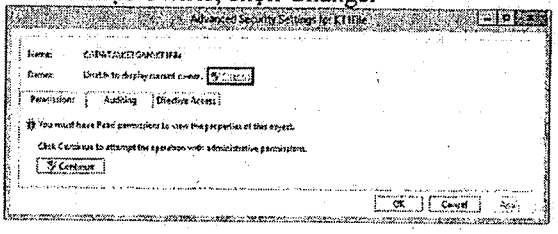
B3 - Tab Security → chọn Edit → Remove tất cả các object, ngoại trừ KT1 (Full Control) → nhấn OK 2 lần.



B4 - Log on Administrator, truy cập vào folder KETOAN. Truy cập vào folder KT1file bị báo lỗi không thể truy cập → Chuột phải lên folder KT1file, chọn Properties → Qua tab Security, chọn Advanced

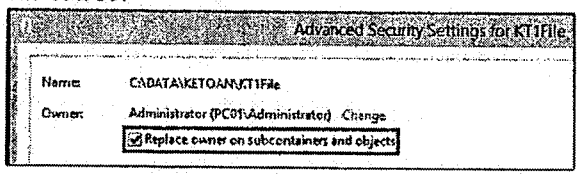


B5 - Ở mục Owner, chọn Change.



B6 - Nhập vào Administrator → Check Names → OK

B7 - Đánh dấu chọn vào ô Replace owner on subcontainers and object → Yes→ OK → OK đóng các cửa sổ.



B8 - Kiểm tra: Chuột phải vào folder KT1file, quan sát thấy Administrator đã có quyền Full Control

4. Xét quyền khi di chuyển data trên cùng Partition

a. Copy

- Trong ổ C tạo 1 folder tên là A
- Chuột phải lên C:\DATA chọn Copy → Mở thư mục A → chuột phải chọn Paste

- Kiểm tra quyền của thư mục C:\A\DATA → các quyền NTFS bị thay đổi

b. Move

- Trong ổ C tạo 1 folder tên là B

- Chuột phải lên C:\DATA chọn Cut → Mở thư mục B → chuột phải chọn Paste

- Kiểm tra quyền của thư mục C:\A\DATA → các quyền NTFS không bị thay đổi

** Nhận Xét :*

- Khi di chuyển dữ liệu trong cùng partition → quyền của data không bị thay đổi.

- Khi copy dữ liệu vào nơi khác cùng partition thì quyền của data vừa copy bị thay đổi phụ thuộc vào nơi đến.

SHARE PERMISSION – ACCESS BASE EMULATION (ABE)

CÁC BƯỚC TRIỂN KHAI

1. Share một Folder
2. Thực hiện Share Ẩn
3. Map Network Drive
4. Share 1 folder với nhiều tên
5. Quản lý các Shared Resources
6. Access Base Emulation

A- CHUẨN BỊ

- Mô hình bài lab bao gồm 2 máy:

+ PC01: Windows Server 2012 R2

+ PC02: Windows 8.1 Enterprise

- PC01 tạo account u1 với password là P@ssword ,

- PC01 tạo folder ThucTap trong ổ C:. Trong thư mục ThucTap tạo 2 folder DuLieu và BiMat

- Trong các folder tạo file Abc.txt với nội dung tùy ý

- Trên 2 máy tắt Firewall, UAC, và kiểm tra đường truyền bằng lệnh Ping

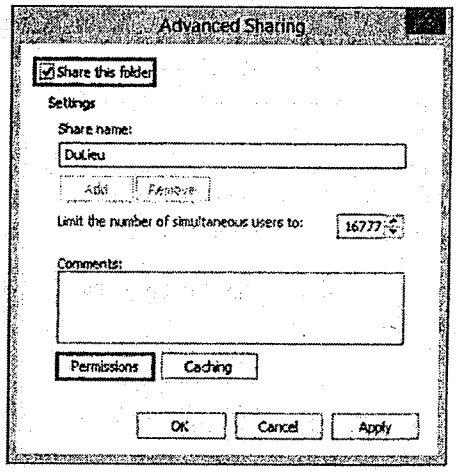
B- THỰC HIỆN

1. Share một Folder (Thực hiện trên PC01)

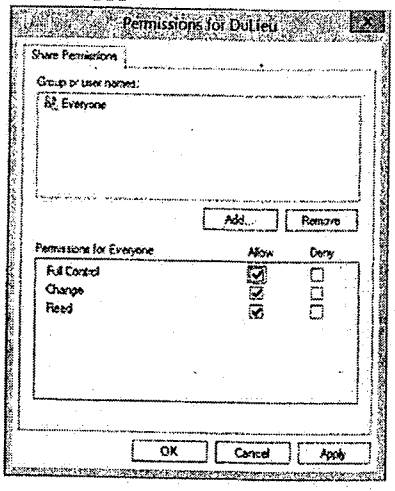
B1 - Chuột phải lên folder DULIEU chọn Share with → Advanced sharing…

B2 - Ở tab Sharing → Nhấn vào nút Advanced Sharing…

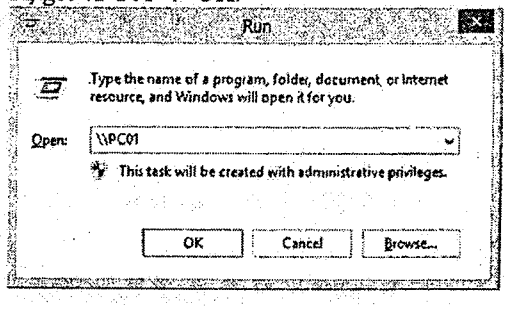
B3 - Đánh dấu chọn vào ô Share this folder → Click vào Permissions



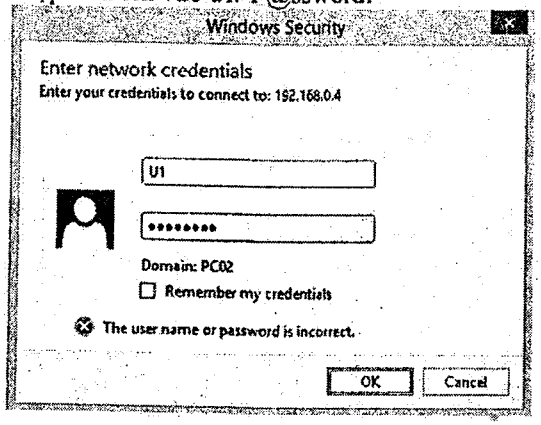
B4 - Check vào Allow Full Control → OK → OK → OK



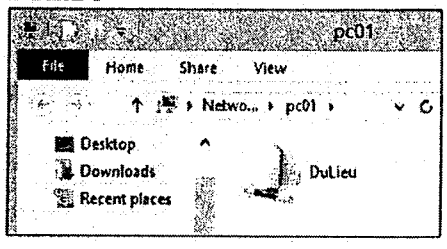
B5 - Qua máy PC02, nhấn tổ hợp phím ⊞ + R, gõ: \\PC01 → OK.



B6 - Hộp thoại yêu cầu chứng thực khi đăng nhập → Điền vào u1/ P@ssword.



B7 - Truy cập thành công thấy Folder DULIEU

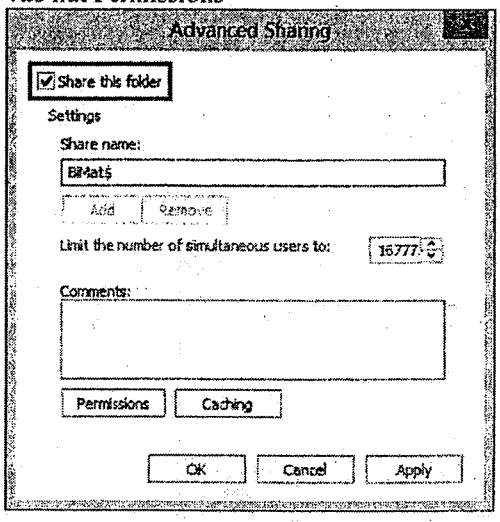


2. Share ẩn một folder (Thực hiện tại máy PC01)

B1 - Chuột phải thư mục BIMAT → Chọn Share with → Advanced Sharing

B2 - Ở tab Sharing → Nhấn vào nút Advanced Sharing…

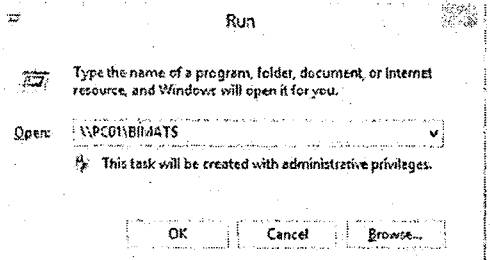
B3 - Đánh dấu chọn vào ô Share this folder. Ở mục Share Name, nhập vào BiMat$ → Nhấn vào nút Permissions



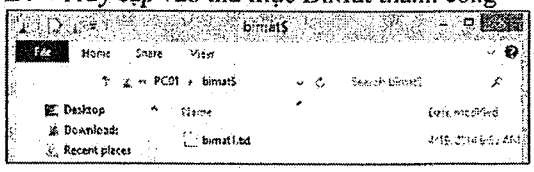
B4 - Check vào Allow Full Control → OK → OK → Close

B5 - Tại máy PC02 nhấn tổ hợp phím ⊞ + R, gõ: \\PC01 → OK → Truy cập vào không thấy folder BIMAT.

B6 - Tắt cửa sổ File Explorer → Truy cập lại \\PC01\BIMAT$



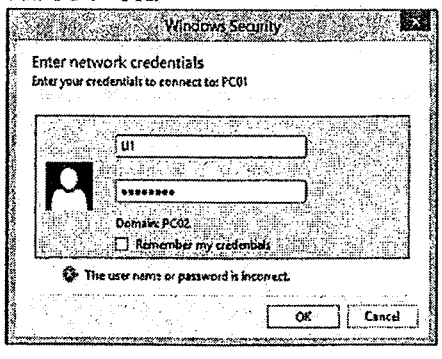
B7 - Truy cập vào thư mục BiMat thành công



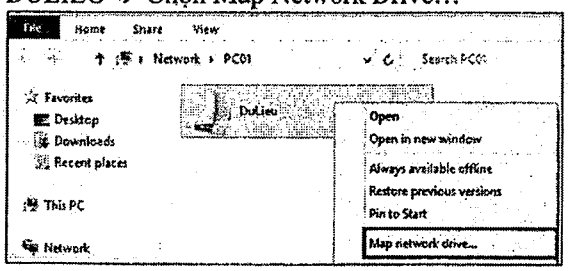
3. Map Network Drive

B1 - Qua máy PC02 → truy cập network access vào máy PC01.

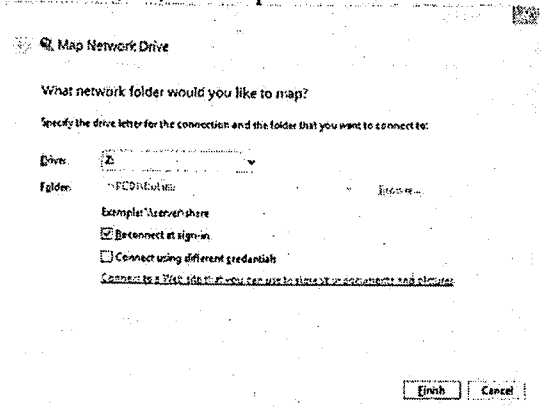
B2 - Hộp thoại yêu cầu chứng thực khi đăng nhập → Điền vào Username và Password của U1→ OK.



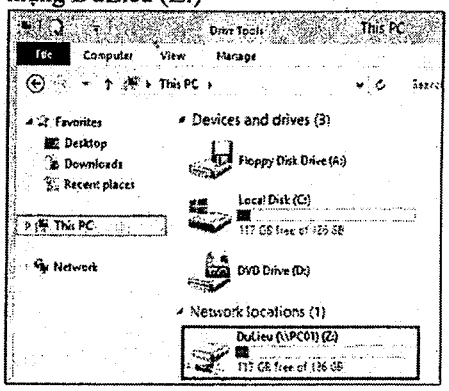
B3 - Tại màn hình truy cập, chuột phải lên folder DULIEU → Chọn Map Network Drive…



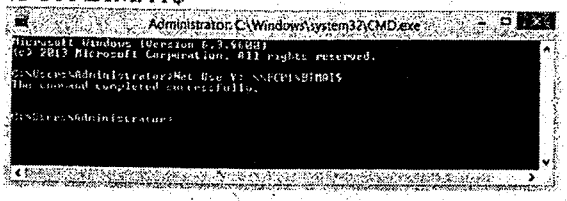
B4 - Để mặc định các options → Nhấn Finish.



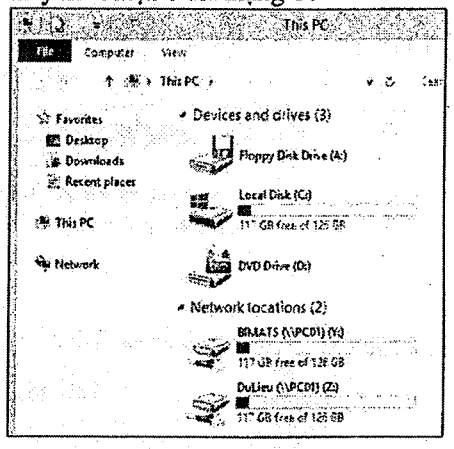
B5 - Mở Computer kiểm tra đã có ổ đĩa mạng DuLieu (Z:)



B6 - Mở CMD, gõ lệnh Net use Y: \\PC01\BIMAT$

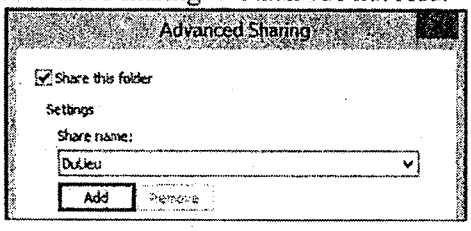


B7 - Kiểm tra trên PC02 mở File Explorer thấy xuất hiện ổ đĩa mạng Y:

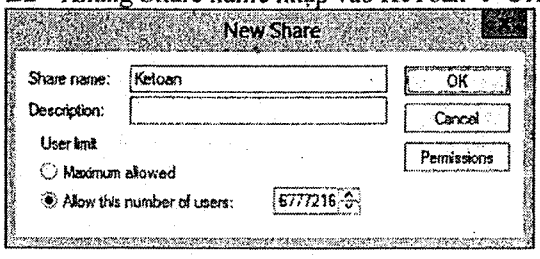


4. Share 1 folder với nhiều tên (Thực hiện trên PC01)

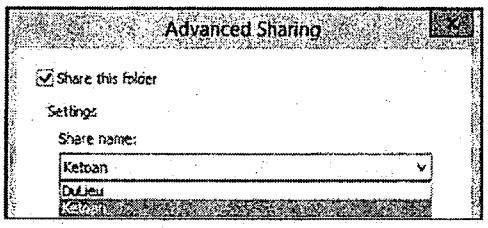
B1 - Chuột phải lên folder DULIEU → Share with → Chọn Advanced sharing...→ Advanced sharing → Nhấn vào nút Add.



B2 - Khung Share name nhập vào KeToan → OK.

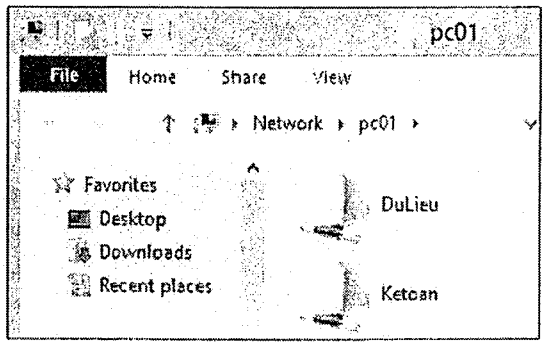


B3 - Kiểm tra trong hộp thoại Advanced Sharing, phần Share name có 2 tên DuLieu và KeToan.



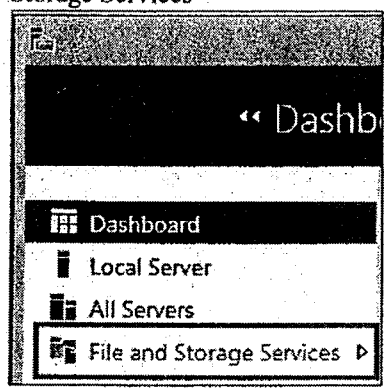
B4 - Nhấn vào nút Permission → Phân quyền lại với Everyone → Full Control → OK → Close

B5 - Máy PC02 truy cập server kiểm tra kết quả thấy có 2 folder được share với tên KeToan , DuLieu

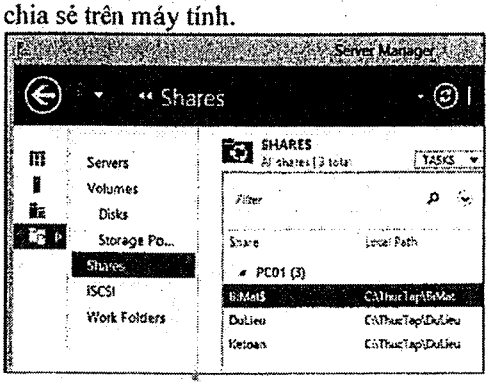


5. Quản lý các Share Resources (Thực hiện trên máy PC01)

B1 - Mở Server Manager → chọn File and Storage Services



B2 - Ở khung bên trái chọn Shares → Quan sát bên tay phải: các dữ liệu hiện đang được chia sẻ trên máy tính.



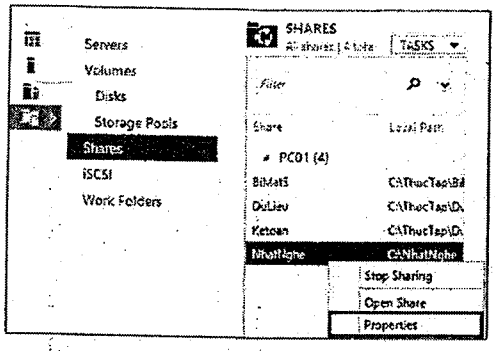
6. Access Base Emulation

B1 - Tạo Folder C:\Nhat Nghe

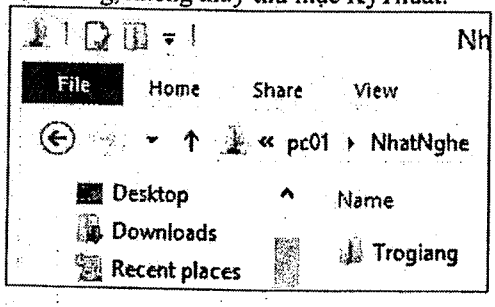
B2 - Trong C:\Nhat Nghe tạo 2 thư mục : Kythuat và TroGiang

B5 - Tạo User u2/ password: P@ssword

B6 - Mở Server Manager → File and Storage Services → Shares → Chuột phải lên C:\NhatNghe → Properties



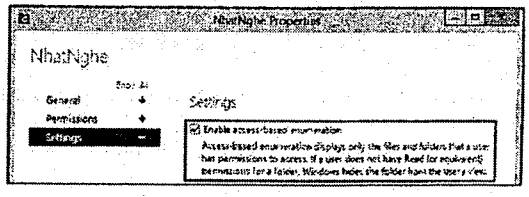
B9 - Tương tự PC02 truy cập network Access vào PC01 bằng quyền U2: Truy cập thư mục Nhất Nghệ quan sát thấy chỉ thấy thư mục TroGiang, không thấy thư mục KyThuat.



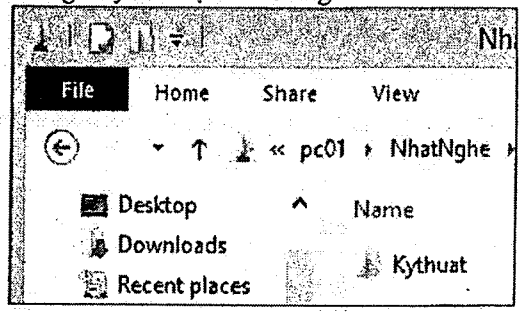
B3 - Share Full thư mục C:\Nhat Nghe

B4 - Phân quyền NTFS :
+ U1 có toàn quyền trên thư mục KyThuat, U2 không có quyền
+ U2 có toàn toàn quyền trên thư mục TroGiang, U1 không có quyền

B7 - Chọn Settings → đánh dấu chọn vào ô Enable access-based enumeration → OK → OK



B8 - Kiểm tra : PC02 truy cập network Access vào PC01 bằng quyền U1: Truy cập thư mục Nhất Nghệ quan sát chỉ thấy thư mục Kythuat, không thấy thư mục TroGiang



DOMAIN

CÁC BƯỚC TRIỂN KHAI

1. Nâng cấp Domain Controller

2. Join máy Workstation vào Domain

3. Cấu hình Policy trên máy Domain Controller

a. Cấu hình cho phép đặt password đơn giản

b. Cấu hình cho phép Group Users được log on trên DC

4. Tạo Domain Group và Domain User

5. Cài Remote Server Administrator Tools cho máy Client

A- CHUẨN BỊ

- Mô hình bài lab bao gồm 2 máy:

+ PC01: Windows Server 2012 R2

+ PC02: Windows 8.1 Enterprise

- Chỉnh password account Administrator cho cả 2 máy là 123

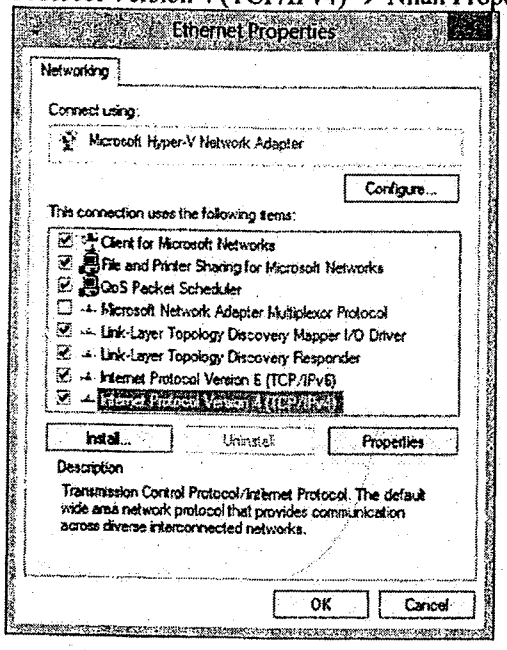
- Disable card CROSS. Gỡ bỏ Protocol TCP/IP IPv6 trên card LAN

- Kiểm tra 2 máy liên lạc với nhau bằng lệnh PING

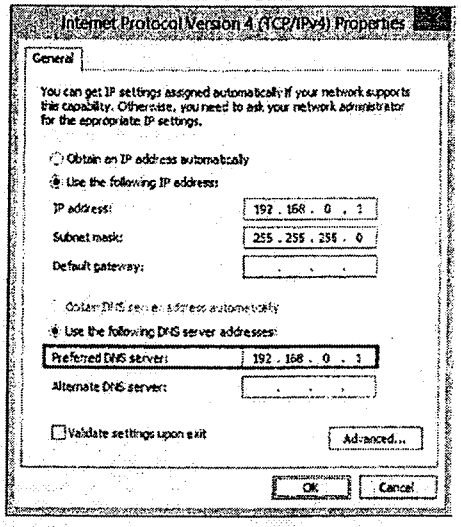
B- THỰC HIỆN

1. Nâng cấp Domain Controller (Thực hiện tại PC01)

B1 - Mở Control Panel → Network and Sharing Center, chọn Change Adapter Settings. Chuột phải lên card LAN, chọn Properties → Chọn Internet Protocol Version 4 (TCP/IPv4) → Nhấn Properties.



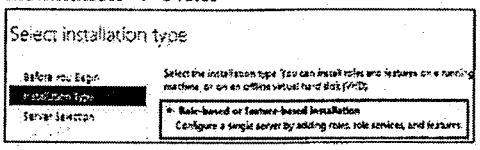
B2 - Ở mục Preferred DNS server, trỏ về IP của chính mình → OK.



B3 - Mở Server Manager, vào menu Manage, chọn Add Roles and Features

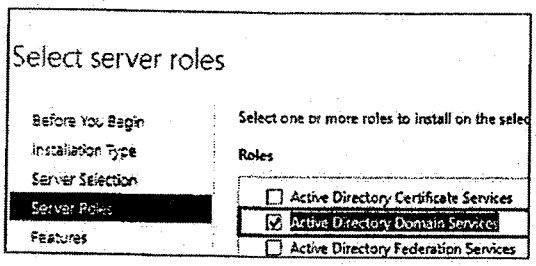
B4 - Màn hình Welcome → Next

B5 - Màn hình Select installation type → chọn Role-based or feature-based installation → Next



B6 - Màn hình Select destination server, giữ nguyên như mặc định → Next

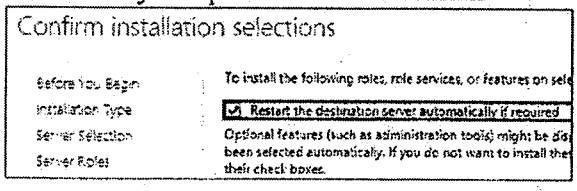
B7 - Màn hình Select server roles, đánh dấu chọn vào ô Active Directory Domain Services



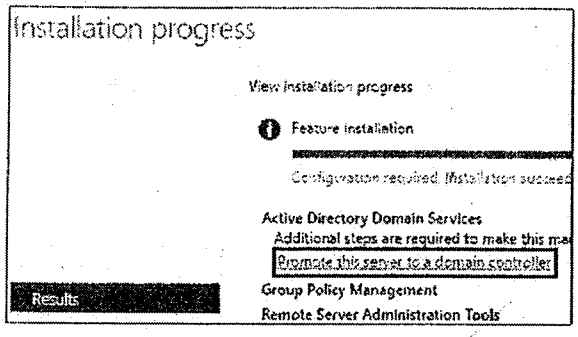
B8 - Cửa sổ Add Roles and Features Wizard → nhấn vào nút Add Features → Next

B9 - Màn hình Select features, giữ nguyên như mặc định → Next

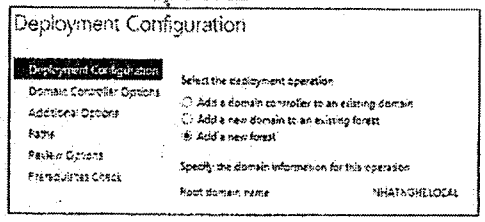
B10 - Màn hình Confirm installation selections, đánh dấu chọn vào ô Restart the destination server automatically if required → Nhấn nút Install



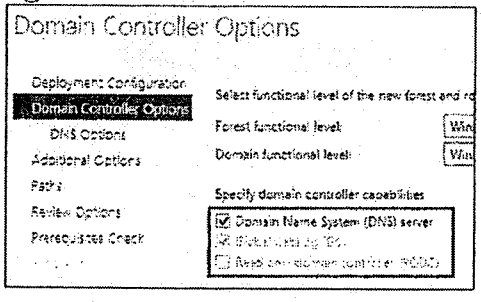
B11 - Quá trình cài đặt diễn ra. Sau khi cài đặt xong, nhấn vào mục Promote this server to a domain controller



B12 - Màn hình Deployment Configuration, chọn Add a new forest. Ở mục Root domain name, đặt tên: NHATNGHE.LOCAL



B13 - Màn hình Domain Controller Options, ở mục Specify domain controller capabilities, đánh dấu chọn vào ô Domain Name System (DNS) server. Ở mục Type the Directory Services Restore Mode (DSRM) password, nhập vào mật khẩu P@ssword → Next



B14 - Các bước còn lại, nhấn Next theo mặc định. Màn hình Prerequisites Check, khi nhận được thông báo All prerequisites check passed successfully nghĩa là quá trình kiểm tra điều kiện để lên DC đã thành công → nhấn nút Install để bắt đầu cài đặt

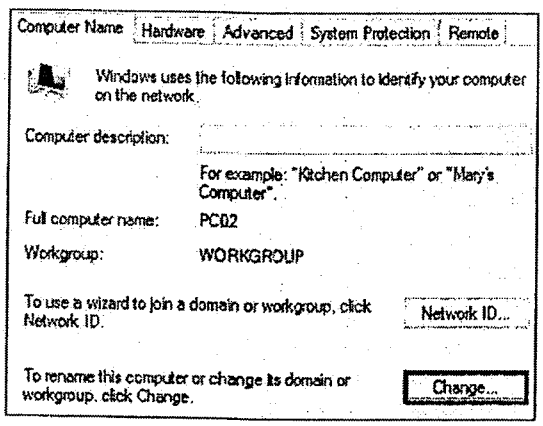
2. Join máy Workstation vào Domain (Thực hiện trên PC02)

B1 - Mở Control Panel → Network and Internet → Network And Sharing Center → Change adapter settings → Disable card Cross

B2 - Chuột phải card Lan → Properties. Bỏ dấu check Internet Protocol Version 6 (TCP/IPv6). → chọn Internet Protocol Version 4 (TCP/IPv4) → chọn Properties

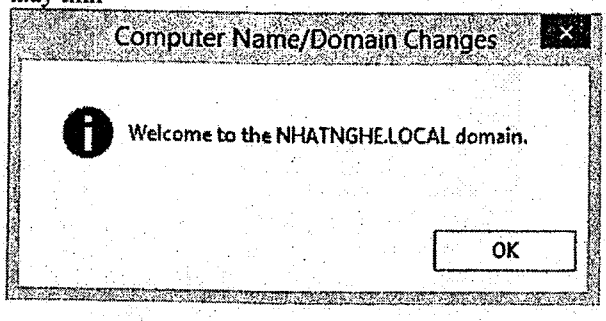
B4 - Nhấn tổ hợp phím ⊞ + R, gõ lệnh Sysdm.cpl

B5 - Trong tab Computer Name, nhấn Change

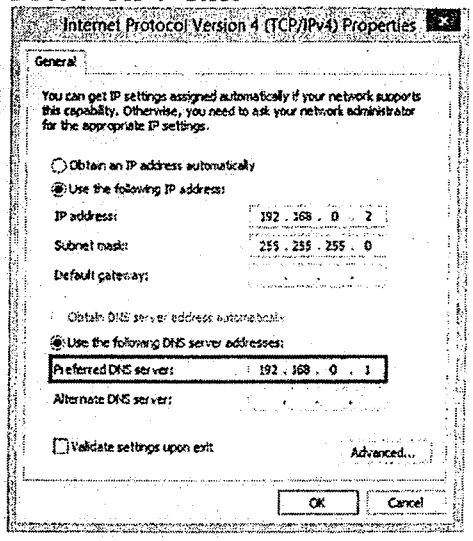


B7 - Cửa sổ Windows Security, nhập vào Username và password: Administrator/123

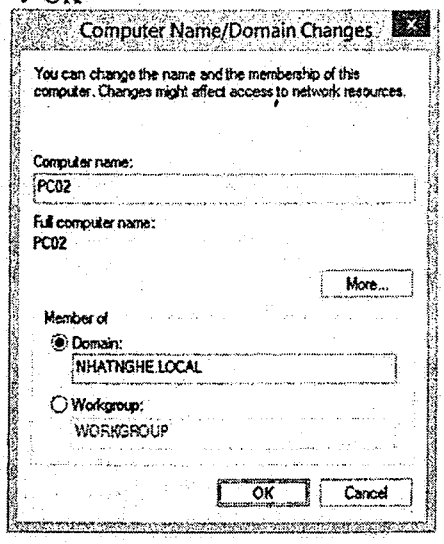
B8 - Quá trình join domain thành công, khởi động lại máy tính



B3 - Chỉnh Preferred DNS server về IP Máy PC01→ OK → Close



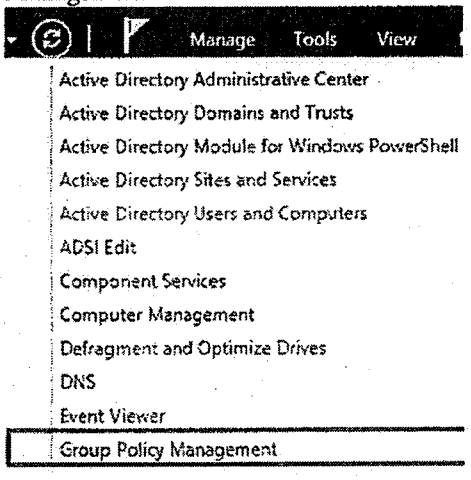
B6 - Ở mục Member of → chọn Domain, sau đó gõ tên domain NHATNGHE.LOCAL → OK



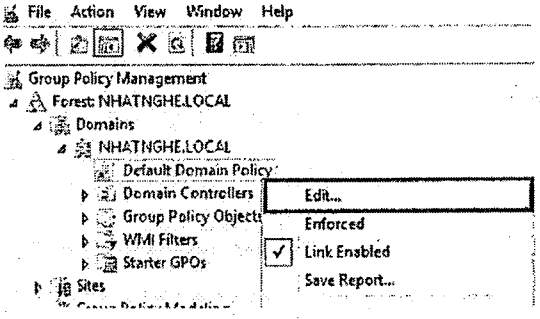
3. Cấu hình Policy trên máy Domain Controller

a. Cấu hình cho phép đặt password đơn giản

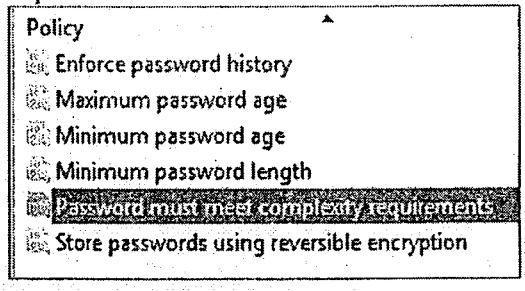
B1 - Quay lại máy PC01, mở Server Manager. Vào menu Tools, chọn Group Policy Management.



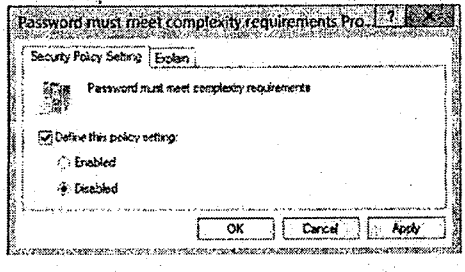
B2 - Lần lượt bung các mục Forest: NHATNGHE.LOCAL → Domains → NHATNGHE.LOCAL → Chuột phải Default Domain Policy, chọn Edit



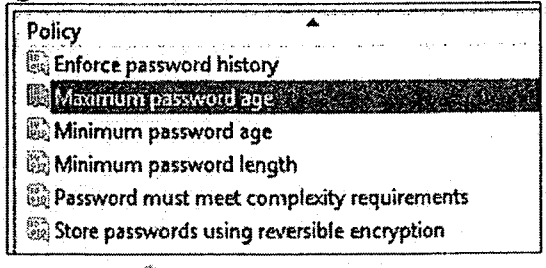
B3 - Lần lượt mở theo đường dẫn Computer Configuration → Windows Settings → Security Settings → Account Policy → Password Policy → double click vào Password must meet complexity requirements



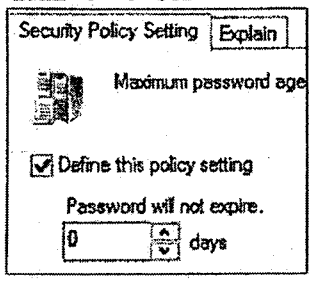
B4 - Chọn Disabled → OK



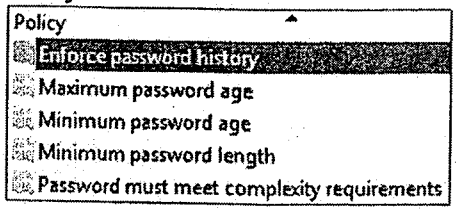
B5 - Quay lại cửa sổ Group Policy Management Editor, nhấn double click vào Maximum password age



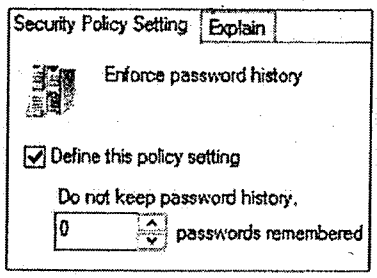
B6 - Ở mục Password will not expire, sửa giá trị thành "0" → OK



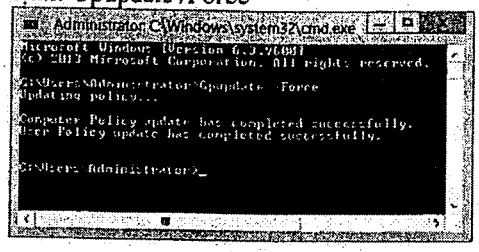
B7 - Quay lại cửa sổ Group Policy Management Editor, nhấn double click vào Enforce password history



B8 - Ở mục Do not keep passwords remember, sửa giá trị thành "0" → OK

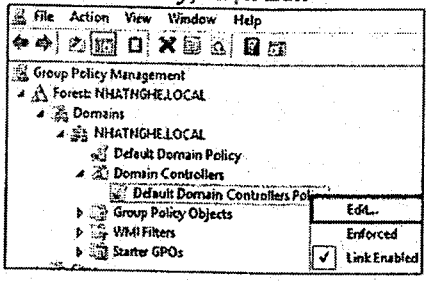


B9 –Sau khi chỉnh policy xong, mở CMD, gõ lệnh: Gpupdate /Force

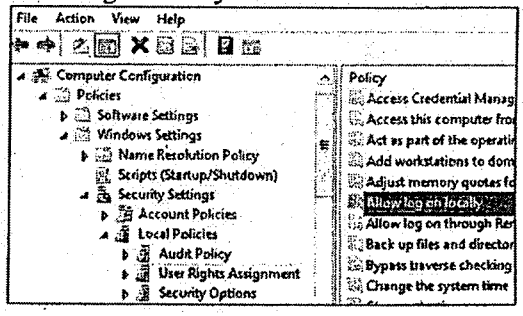


b. Cấu hình cho phép Group Users được log on trên DC

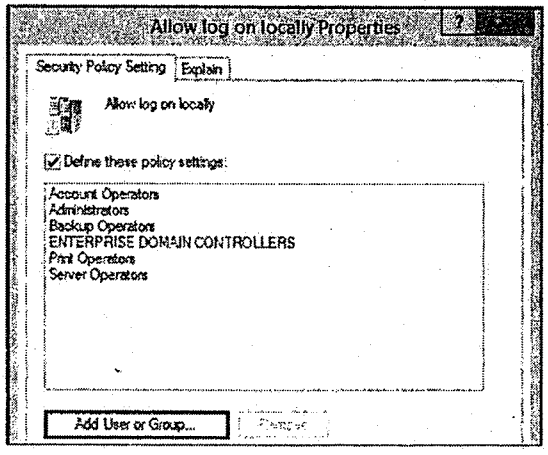
B1 - Lần lượt bung các mục Forest: NHATNGHE.LOCAL → Domains → NHATNGHE.LOCAL → Domain Controllers → Chuột phải Default Domain Controller Policy, chọn Edit

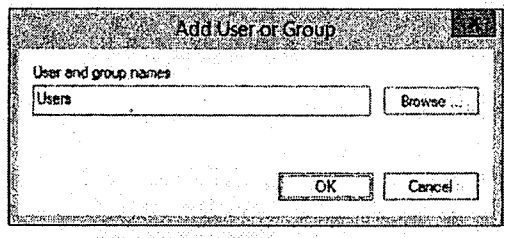


B2 - Mở theo đường dẫn sau Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment → double click vào mục Allow log on locally



B3 - Nhấn vào nút Add User or Group → nhập vào Users → OK → OK

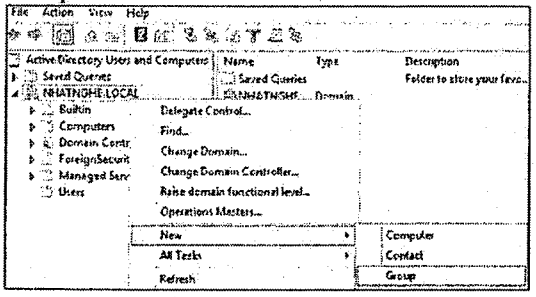




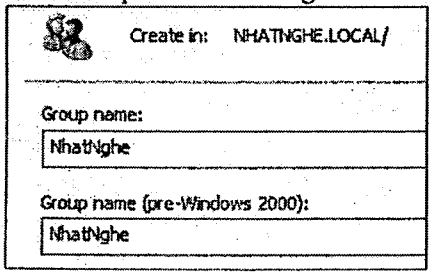
B4 - Sau khi chỉnh policy xong, mở CMD, gõ lệnh: Gpupdate /Force

4. Tạo Domain Group và Domain User

B1 - Mở Active Directory Users and Computers. Chuột phải NHATNGHE.LOCAL → New → Group

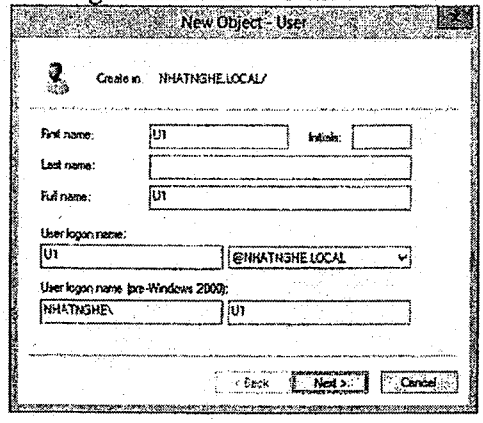


B2 - Group name : Nhat Nghe → OK



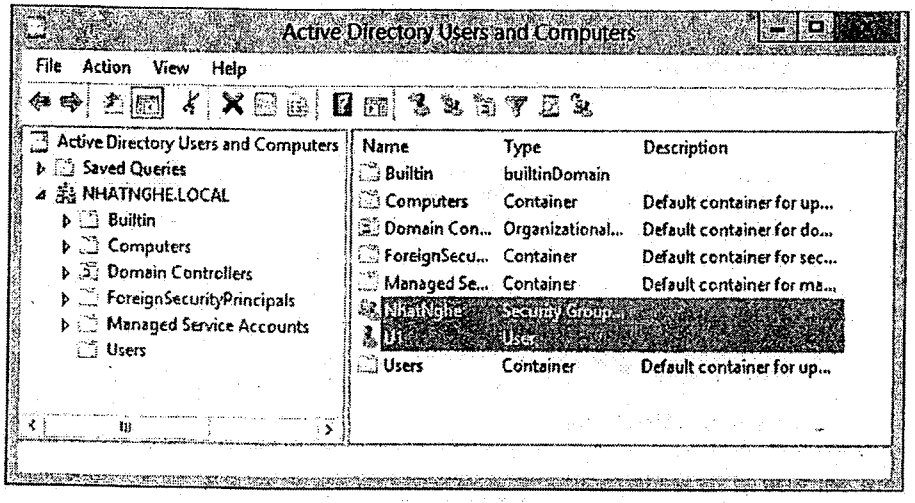
B3 - Chuột phải NHATNGHE.LOCAL → New → User

B4 - Full name : U1
User logon name : U1 → Next



B5 - Password/Confirm password: 123
Bỏ dấu chọn ở ô User must Change password at Next logon → Next

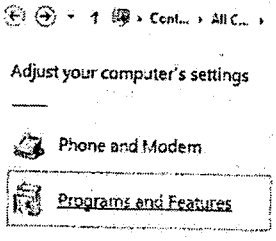
B6 - Quan sát thấy Domain Group và Domain User vừa tạo



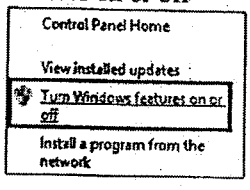
5. Cài Remote Server Administrator Tools cho máy Client (Thực hiện trên PC02)

B1 - Log on NHATNGHE\Administrator. Truy cập Server, chép source Windows8.1-KB2693643-x64 vào ổ C: và chạy file này để cài đặt

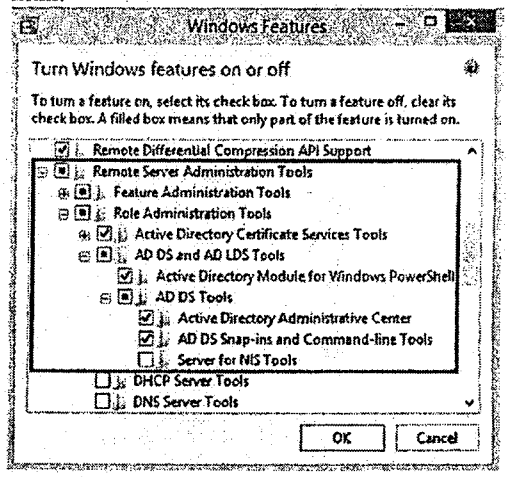
B2 - Mở Control Panel, chọn Program and Features



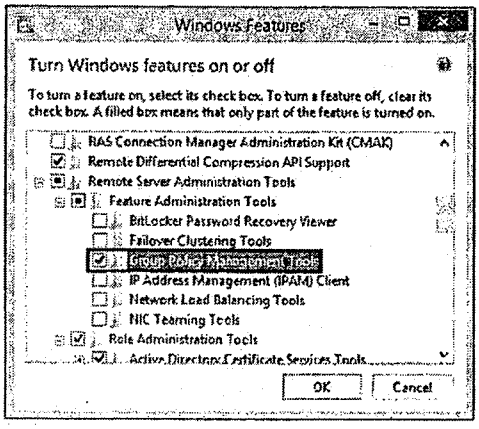
B3 - Ở góc bên trái, chọn Turn Windows features on or off



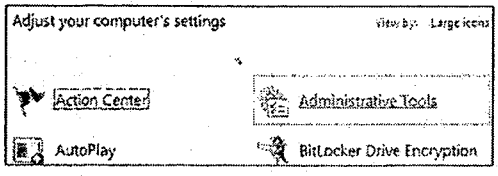
B4 - Đánh dấu chọn vào các mục như trong hình.



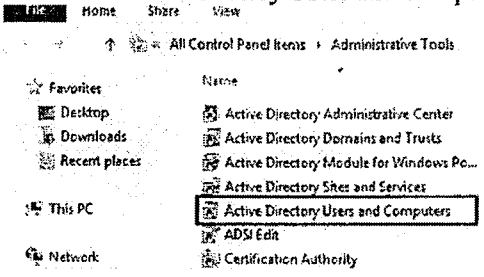
B5 - Chọn Group Policy Management Tools → OK → Close



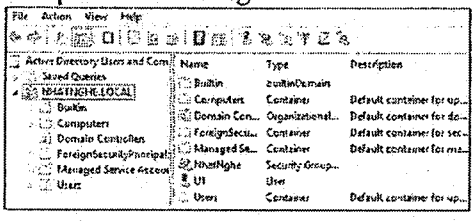
B6 - Mở Control Panel, chọn Administrative Tools



B7 - Mở Active Directory Users and Computers



B8 - Truy cập vào Active Directory Users and Computers thành công



B9 - Kiểm tra:
+ Trên PC02 tạo user U2, password 123 → tạo thành công
+ Trên PC01, mở AD kiểm tra thấy có user U2

DELEGATE – DOMAIN USERS, GROUPS, COMPUTERS

CÁC BƯỚC TRIỂN KHAI

1. Delegate

a. Delegate cho Group

b. Delegate cho User

2. Domain Users

a. Tạo – Sử dụng User Template

b. Làm việc với Multi Users

c. Xem toàn bộ thuộc tính của User

3. Domain Computers

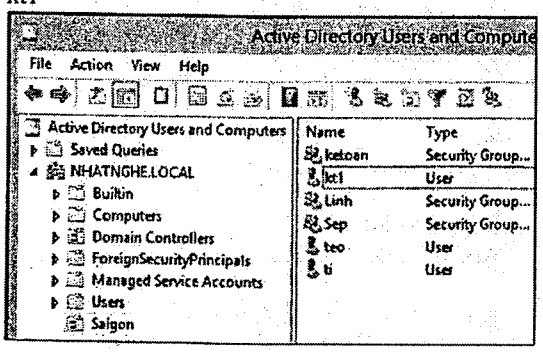
A- CHUẨN BỊ

- Mô hình bài lab bao gồm 2 máy

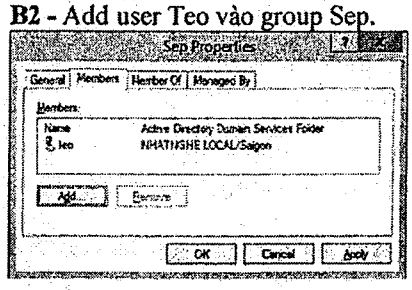
+ PC01: Windows Server 2012 R2 DC (Domain: NHATNGHE.LOCAL)

+ PC02: Windows 8.1 Enterprise Stand Alone

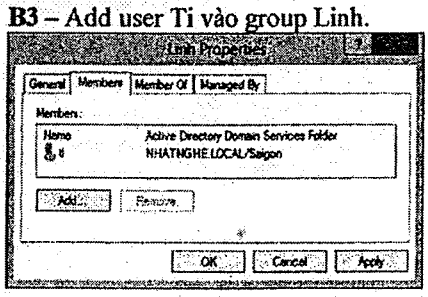
B1 - Trên PC01, tạo OU SaiGon. Trong OU Saigon, tạo 3 group Sep, Linh, Ketoan. Tạo 3 user teo, ti và ktl



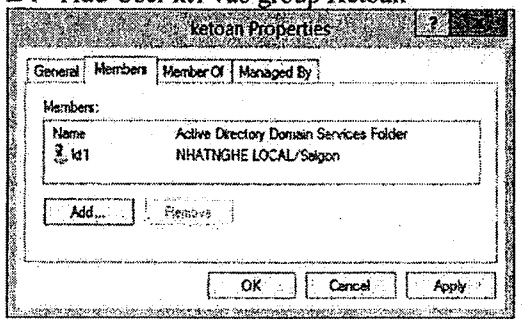
B2 - Add user Teo vào group Sep.



B3 – Add user Ti vào group Linh.



B4 - Add User kt1 vào group Ketoan



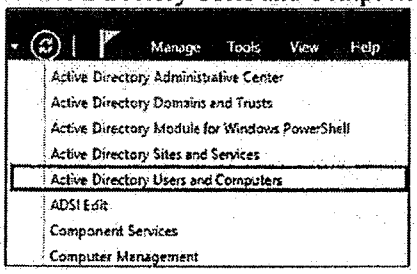
B- THỰC HIỆN

1. Delegate

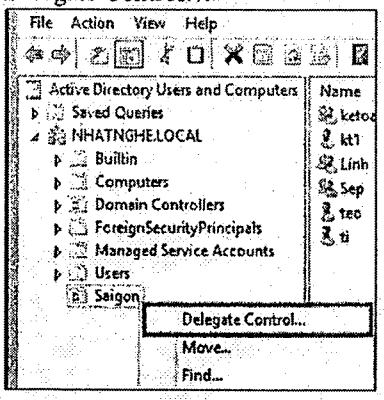
a. Delegate cho Group

Uỷ quyền cho các thành viên trong group Sep được phép tạo mới, xóa và chỉnh sửa thông tin user trong OU SaiGon

B1 - Mở Server Manager → menu Tools → chọn Active Directory Users and Computers

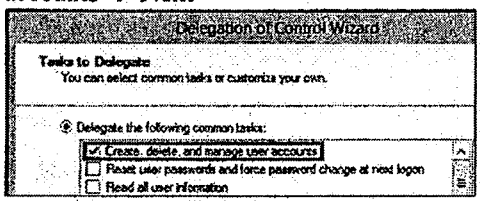


B2 - Chuột phải vào OU Saigon → chọn Delegate Control…



B3 - Màn hình Welcome → chọn Next

B5- Chọn Create, delete, and manage user accounts → Next

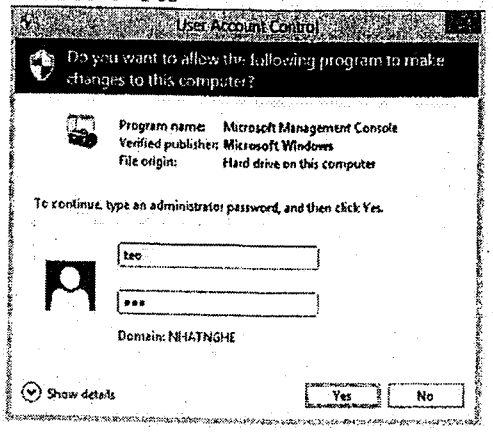


B4 - Màn hình Users and Groups → nhấn Add, gõ Sep → Check Names → Next

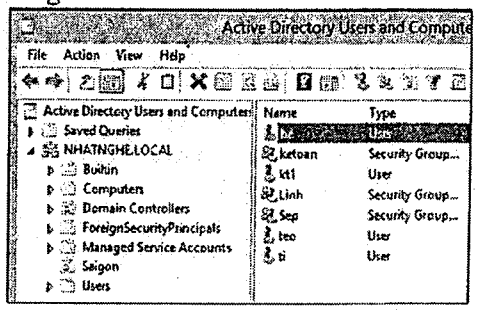
B6 - Màn hình Completing → Finish

B7 - Kiểm tra, trên PC01, log off Administrator, log on Teo. Nhấn tổ hợp phím ⊞ + R, gõ DSA.MSC.

B9 - Màn hình UAC, gõ username và password của Teo → Yes



B10 - Tạo mới User be → Kiểm tra tạo thành công

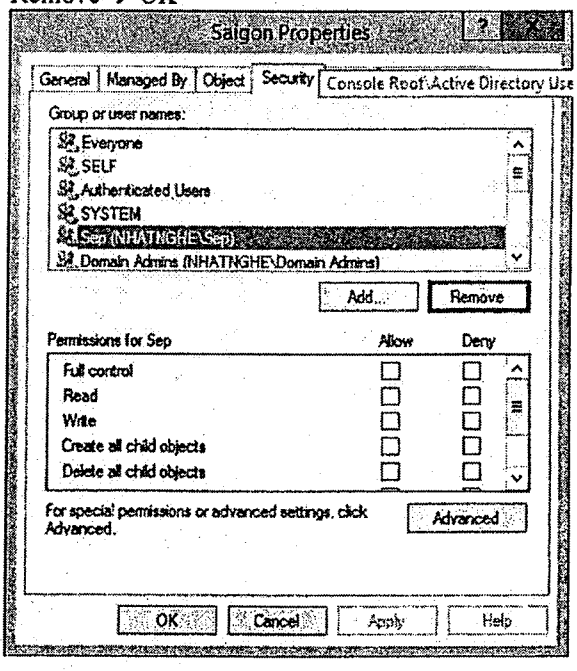


b. Delegate cho User

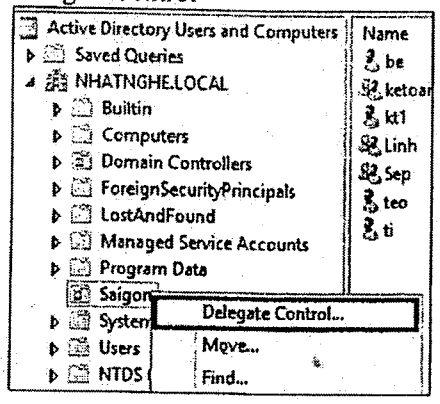
Uỷ quyền cho user kt1 được phép Reset Password và đọc thông tin tài khoản user trong OU SaiGon

B1 - Log on Administrator. Mở Active Directory Users and Computers → chuột phải vào OU Saigon → chọn Properties

B2 - Qua tab Security → chọn Group Sep → Remove → OK



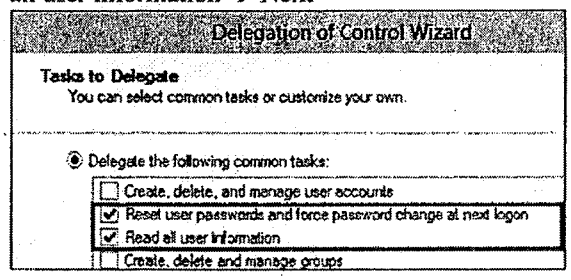
B3 - Chuột phải vào OU Saigon → chọn Delegate Control



B4 - Màn hình Welcome → chọn Next

B5 - Màn hình Users and Groups, nhấn Add → nhập vào user kt1 → Check Names → OK → Next

B6 - Đánh dấu chọn vào 2 ô Reset user passwords and force password change at next logon và ô Read all user information → Next

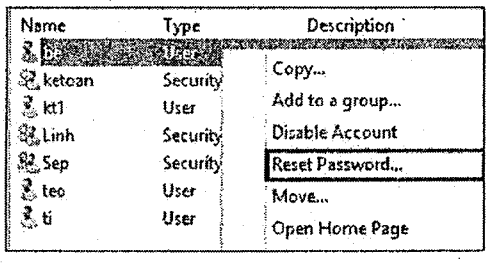


B7 - Màn hình Completing → Finish

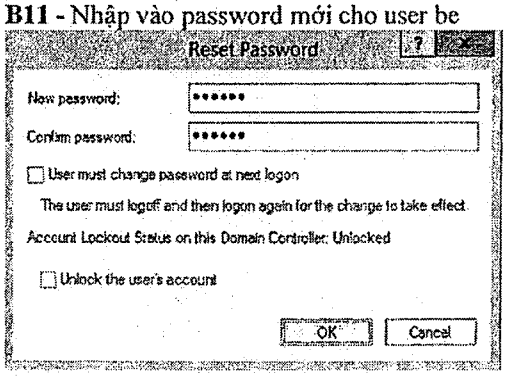
B8 - Kiểm tra, trên PC01, log off Administrator, log on KT1. Nhấn tổ hợp phím ⊞ + R, gõ DSA.MSC.

B9 - Màn hình UAC, gõ username và password của kt1 → Yes

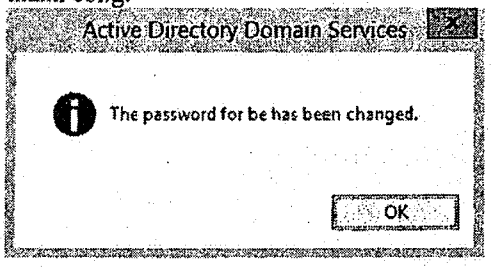
B10 - Chuột phải vào user be → chọn Reset Password



B11 - Nhập vào password mới cho user be



B12 - Quan sát thấy thay đổi password thành công.

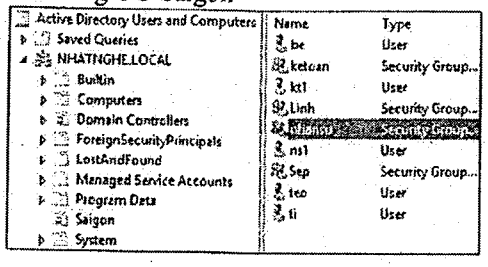


2. Domain Users

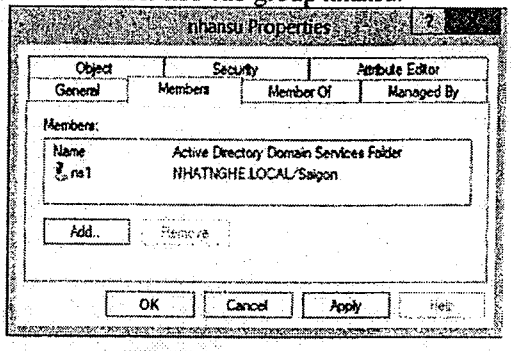
a. Tạo – Sử dụng User Template

B1 - Log on Administrator, mở File Explorer → Trong ổ C: tạo 2 folder Homes và Profiles. Share 2 thư mục này với quyền: Everyone - Full Control

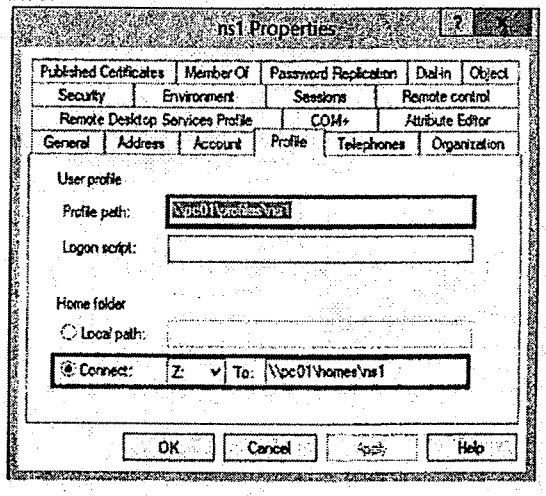
B2 - Mở Active Directory Users and Computers. Tạo thêm group nhansu và user ns1 trong OU Saigon



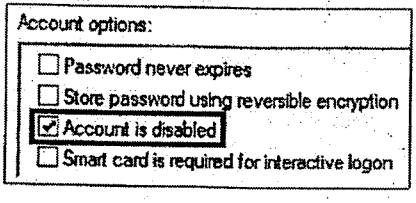
B3 - Add user ns1 vào group nhansu.



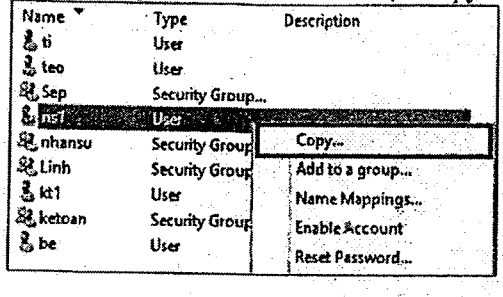
B4 - Tạo Roaming Profile và Home Folder cho ns1.



B5 - Qua tab Account → phần Account options → đánh dấu chọn vào ô Account is disabled → OK



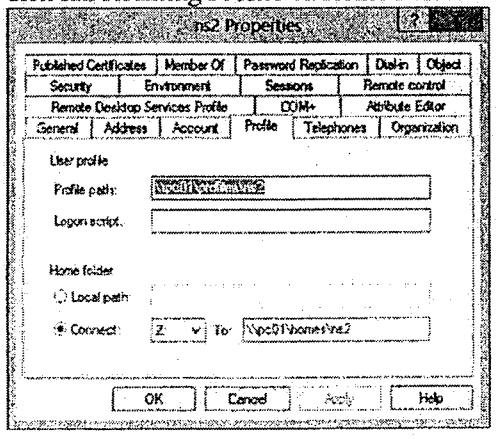
B6 - Chuột phải vào user ns1 → chọn Copy



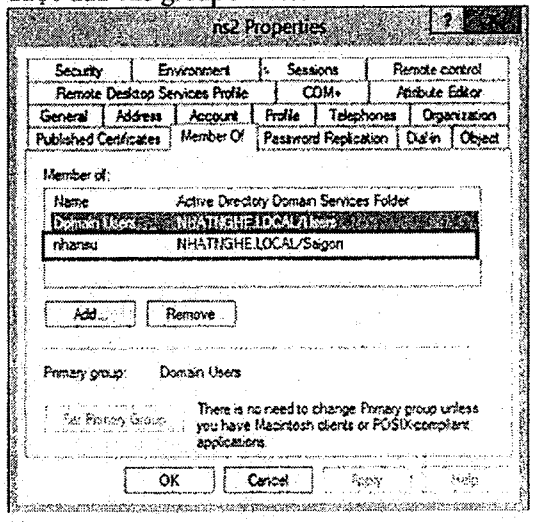
B7 - Full Name: ns2 → User logon name: ns2 → nhấn Next

B8 - Gõ 123 trong 2 phần Password và Confirm password → Bỏ dấu chọn Account is disabled → Next → Finish

B9 - Chuột phải vào user ns2 vừa tạo → chọn Properties →Qua tab Profile, thấy đã được điền sẵn Roaming Profile và Home Folder.



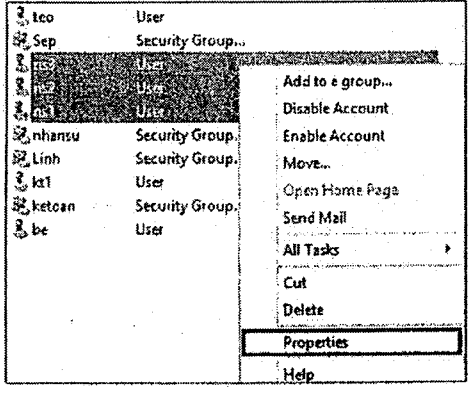
B10 - Qua tab Member of → thấy user ns2 đã được add vào group Nhansu



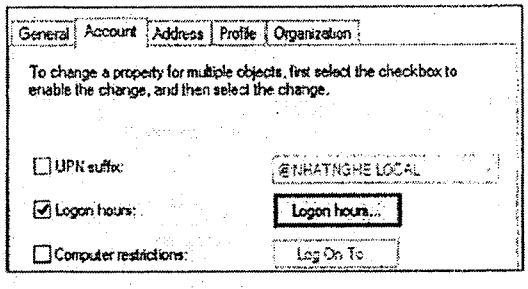
B11 - Thực hiện tương tự để copy NS1 thành account NS3/password 123

b. Làm việc với Multi Users

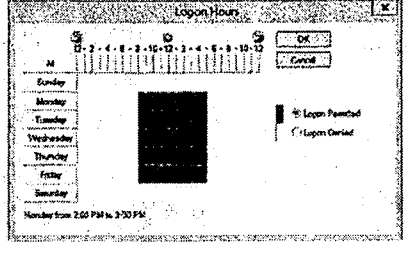
B1 - Giữ phím CTRL, lần lượt click chuột chọn cả 3 user ns1, ns2 và ns3 → Chuột phải chọn Properties.



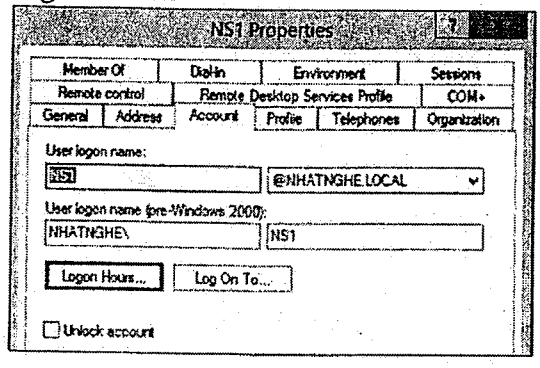
B2 - Qua tab Account → Đánh dấu chọn trước dòng Logon hours → Nhấn vào nút Logon hours



B3 - Tô xanh vùng từ 8h – 5h / Sunday - Friday → Chọn OK → OK



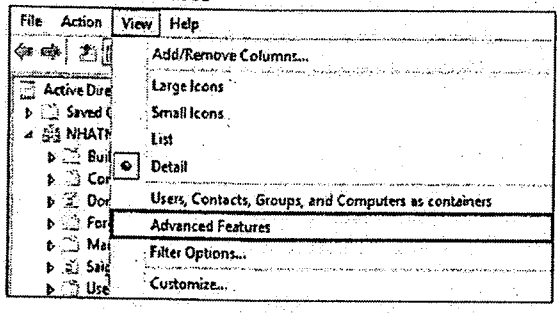
B4 - Kiểm tra : lần lượt mở Properties của cả 3 user: ns1, ns2, ns3 → Qua tab Account → Chọn Logon Hours…



B5 - Quan sát thấy cả 3 user account ns1, ns2, ns3 đều được chỉnh thời gian được phép đăng nhập vào máy tính.

c. Xem toàn bộ thuộc tính của User

B1 - Tại chương trình Active Directory Users and Computers → Chọn Menu View → Chọn Advanced Features



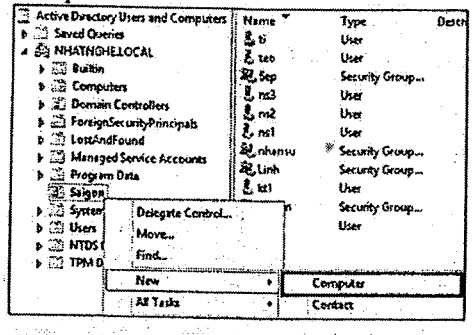
B2 - Chuột phải vào user ns3 → Chọn Properties

B3 - Chọn Tab Attribute Editor → Tìm đến mục homeDirectory và ProfilePath → Quan sát thấy giá trị trong 2 dòng này giống trong tab Profile

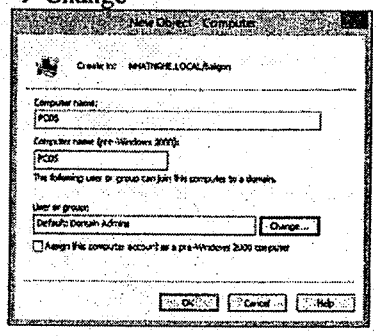
Nhận xét : Mọi thuộc tính của user account đều có thể được xem và chỉnh sửa tại Attribute Editor

3. Domain Computers

B1 - Chuột phải vào OU Saigon → Chọn New → Computer

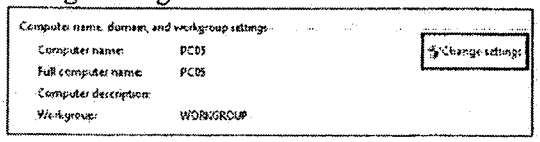


B2 - Mục Computer Name: nhập vào PC05 → Change

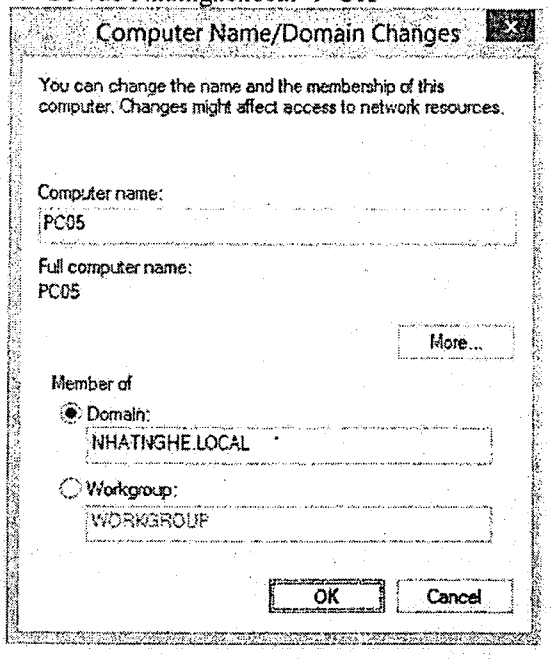


B3 - Nhập vào user ns2 → Check Names → OK 2 lần

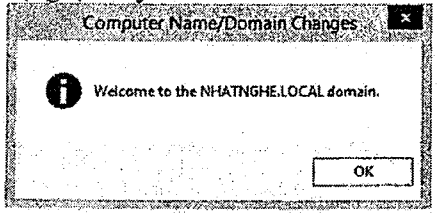
B5 - Kiểm tra: Trên PC05, log on Administrator. Mở File Explorer → Chuột phải vào This PC → Chọn Properties. Ở mục Computer Names, chọn Change settings



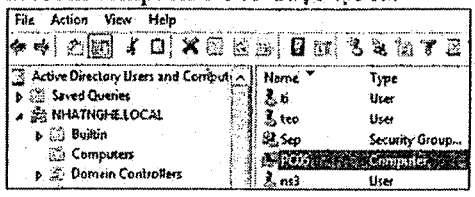
B7 - Trong phần Member of: Chọn mục Domain → Gõ vào Nhatnghe.local → OK



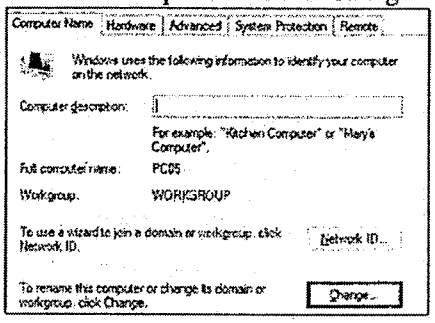
B9 - Join Domain thành công → OK → Khởi động lại máy tính



B4 - Quan sát thấy trong OU SaiGon có account computer PC05 được tạo ra.



B6 – Tab Computer Name → Change



B8 - Hiện bảng Windows Security → Gõ ns2 với password 123 → OK

B10 - Kiểm tra: Trên PC01 mở Active Directory Users and Computers → Mở Container Computers → Quan sát không có computer account được tạo ra.

Nhận xét : Nếu trên Active Directory Users and Computers đã tạo trước computer account trùng tên với máy client trước khi client join domain, thì khi máy client join vào domain, hệ thống sẽ không tạo ra thêm computer account nữa và sẽ sử dụng computer account đã tạo trước đó.

GROUP POLICY MANAGEMENT

CÁC BƯỚC TRIỂN KHAI

1. Tạo và link Policy vào OU
2. Block Inheritance cho OU
3. Enforce Policy
4. Chỉnh order cho Policy
5. Security Filtering
6. Xem các setting của policy
7. Modeling Wizard
8. Item Level Targetting
9. Disable một phần của policy
10. Khảo sát nơi chứa policy templates

A- CHUẨN BỊ

Mô hình bài lab bao gồm 2 máy

+ PC01 : Windows Server 2012 R2 – DC (Domain: NHATNGHE.LOCAL)

+ PC02 : Windows 8.1 – Join Domain

- PC01 :

* Chỉnh Policy password đơn giản

* Chỉnh Policy cho phép group Users có quyền log on locally

* Tạo OU Cha. Trong OU Cha, tạo OU Con

* Trong OU Cha tạo user u1, u2. Trong OU Con tạo user u3, u4

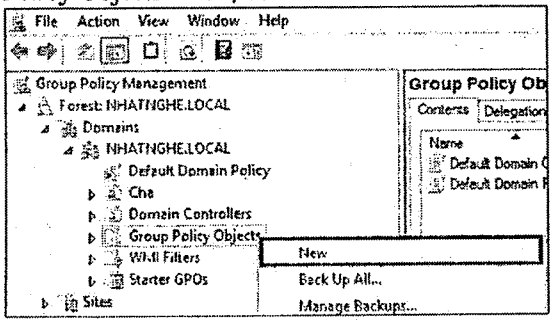
* Trong Domain Nhatnghe.local tạo group TEST, add 2 user u1 và u3 vào group

B- THỰC HIỆN

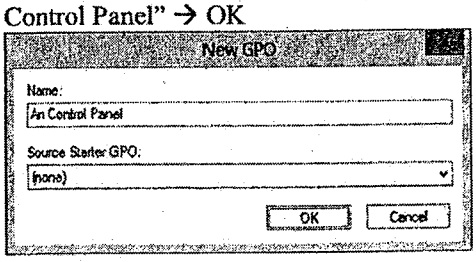
1. Tạo và link Policy vào OU (Thực hiện trên máy PC01)

B1 - Mở Server Manager → vào menu Tools → Group Policy Management

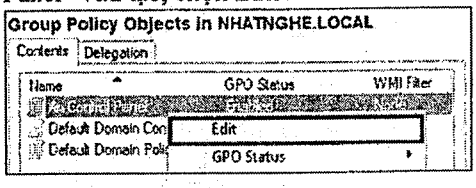
B2 - Bung Forest → Domains → NHATNGHE.LOCAL → Chuột phải vào Group Policy Objects → chọn New.



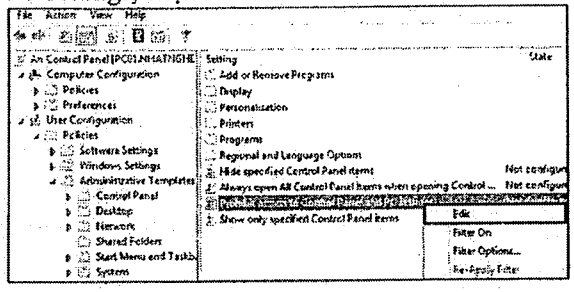
B3 - Đặt tên cho GPO ở khung name "Ẩn Control Panel" → OK



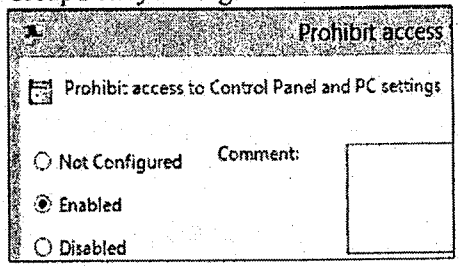
B4 - Chuột phải vào GPO "Ẩn Control Panel" vừa tạo, chọn Edit



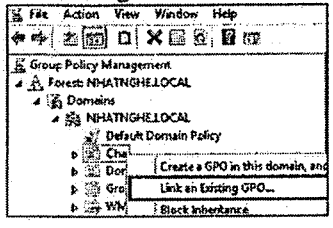
B5 - Bung mục User Configuration → Policies → Administrative Templates → Control Panel, chuột phải vào Prohibit access to the Control Panel and PC settings, chọn Edit.



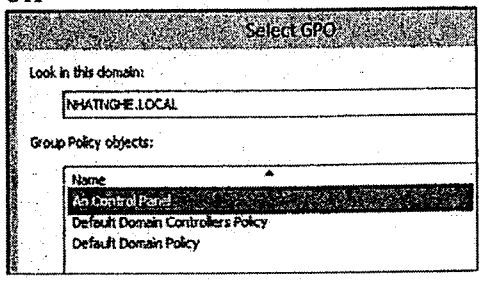
B6 - Chọn Enabled → OK → Đóng cửa sổ Group Policy Management Editor



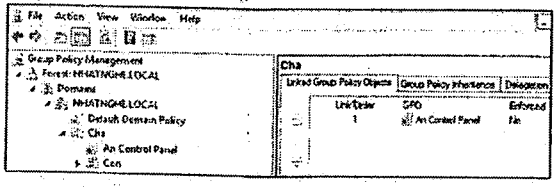
B7 - Quay trở lại màn hình Group Policy Management, chuột phải vào OU Cha, chọn Link an Existing GPO…



B8 - Chọn GPO "Ẩn Control Panel" → OK



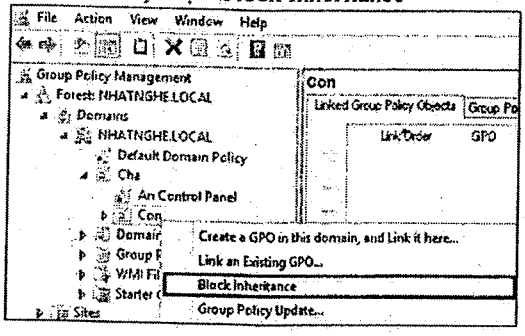
B9 - Quan sát thấy GPO "Ẩn Control Panel" đã được link vào OU Cha



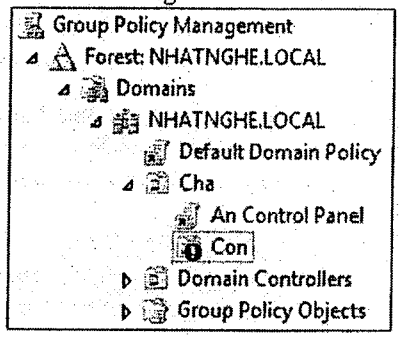
B10 - Kiểm tra: Trên PC02, log on lần lượt vào các user u1, u2, u3, u4 → Bị mất Control Panel

2. Block Inheritance cho OU (Thực hiện trên máy PC01)

B1 - Mở Group Policy Management, chuột phải vào OU Con, chọn Block Inheritance



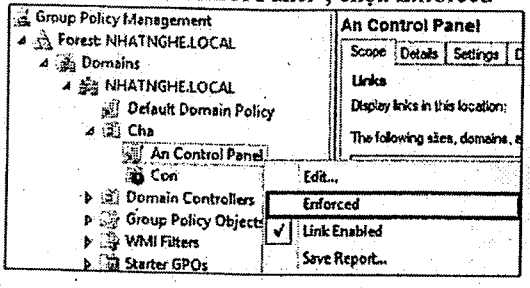
B2 - Quan sát OU Con, thấy có biểu tượng dấu chấm than



B3 - Kiểm tra: Trên máy PC02, lần lượt log on user u3, u4 → sẽ thấy có Control Panel

3. Enforce Policy (Thực hiện trên máy PC01)

B1 - Mở Group Policy Management, chuột phải vào GPO "Ẩn Control Panel", chọn Enforced

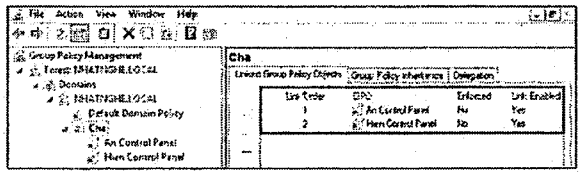


B2 - Trên máy PC02, log on user u3, u4 → sẽ thấy bị mất Control Panel

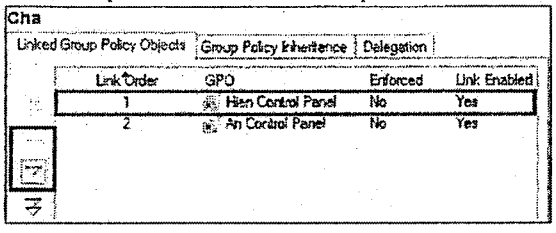
4. Chỉnh order cho Policy (Thực hiện trên máy PC01)

B1 - Mở Group Policy Management, tắt Enforce Policy và Block Inheritance trên OU Cha và OU Con.

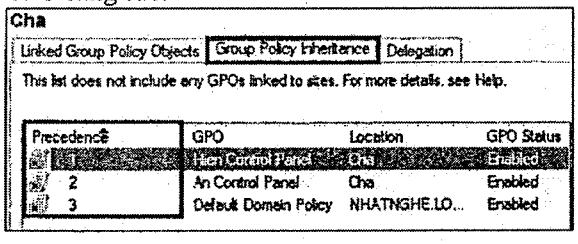
B2 - Tạo thêm GPO "Hiện Control Panel", link GPO này vào OU Cha. Như vậy lúc này OU Cha có 2 GPO "Ẩn Control Panel" và "Hiện Control Panel".



B3 - Nhấn vào OU Cha, ở góc trái dùng 2 biểu tượng mũi tên Move Up và Move Down, di chuyển GPO "Hiện Control Panel" lên vị trí đầu tiên.



B4 - Qua tab Group Policy Inheritance, chú ý mục Precedent, Precedence càng nhỏ thì độ ưu tiên của GPO càng cao.



B5 - Kiểm tra: Trên máy PC02, log on user u3, u4 → sẽ thấy Control Panel

Nhận xét:

** Trong cùng 1 OU nếu áp chung 2 policy (không Enforce) thì policy nào có giá trị Link Order nhỏ thì sẽ có độ ưu tiên cao hơn*

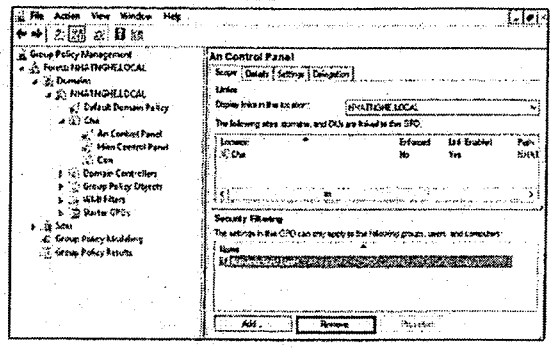
** Trong cùng 1 OU nếu áp chung 2 policy (cả 2 policy đều Enforce) thì policy nào có giá trị Link Order nhỏ thì sẽ có độ ưu tiên cao hơn*

** Trong cùng 1 OU nếu áp chung 2 policy (1 policy Enforce và 1 policy không Enforce) thì policy Enforce sẽ có độ ưu tiên hơn*

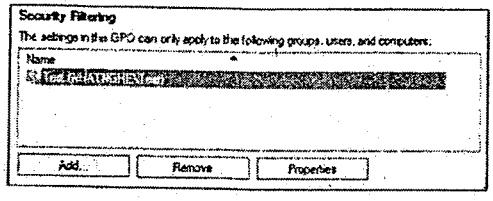
5. Security Filtering (Thực hiện trên máy PC01)

B1 - Mở Group Policy Management → Chuyển policy "Ẩn Control Panel" lên Link Order bằng 1

B2 - Chọn GPO"Ẩn Control Panel", bên dưới mục Security Filtering, chọn vào group Authenticated Users → Remove → OK



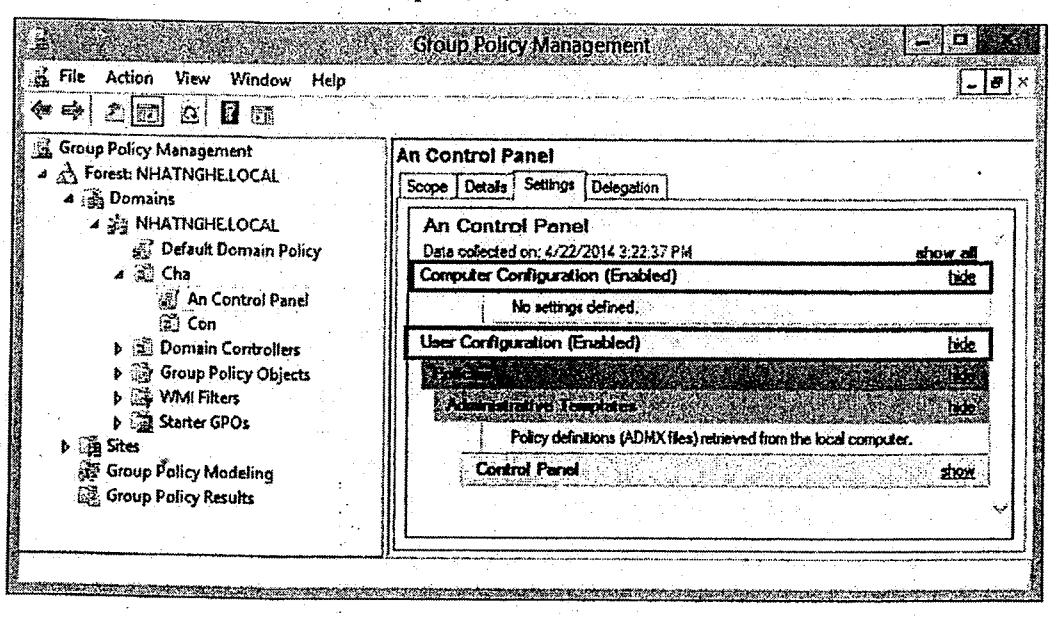
B3 - Quay trở lại màn hình Security Filtering, chọn Add → Add Group Test vào → OK



B4 - Kiểm tra: Trên máy PC02:
+ Log on user U1, U3 → mất Control Panel
+ Log on user U2, U4 → hiện Control Panel

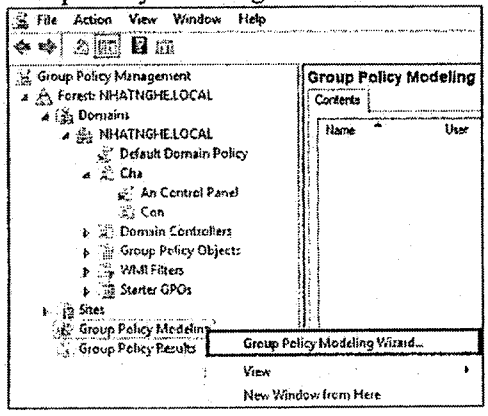
6. Xem các Setting của GPO (Thực hiện trên máy PC01)

- Mở Group Policy Management, chọn GPO "Ẩn Control Panel", qua tab Settings → Add → Add → Close → Quan sát các thiết lập được tạo ra trên GPO

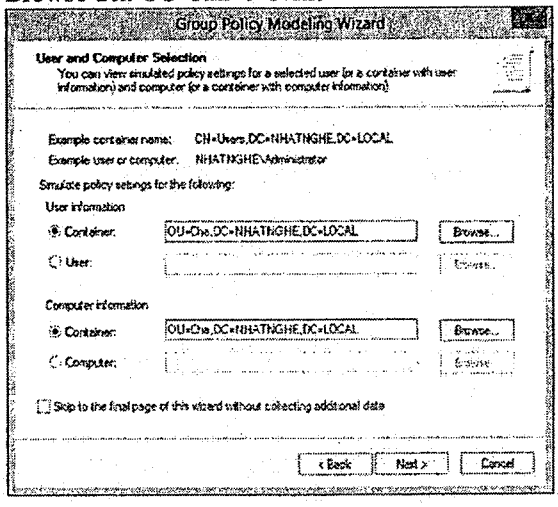


7. Modeling Wizards (Thực hiện trên máy PC01)

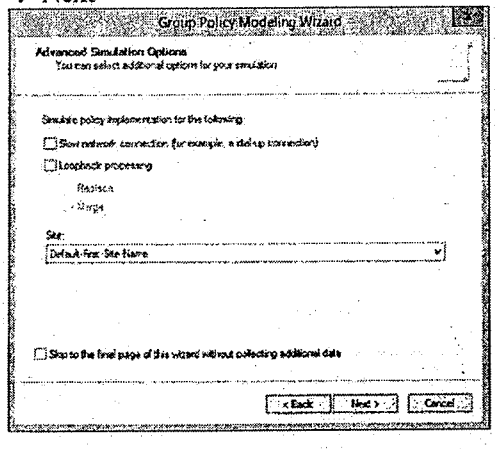
B1 - Mở Group Policy Management, chuột phải vào Group Policy Modeling, chọn Group Polciy Modeling Wizard…



B2 - Các bước đầu tiên nhấn Next theo mặc định. Màn hình User and Computer Selection → Để xem OU Cha bị áp policy gì, trong 2 phần User Information và Computer Information, chọn Browse đến OU Cha → Next



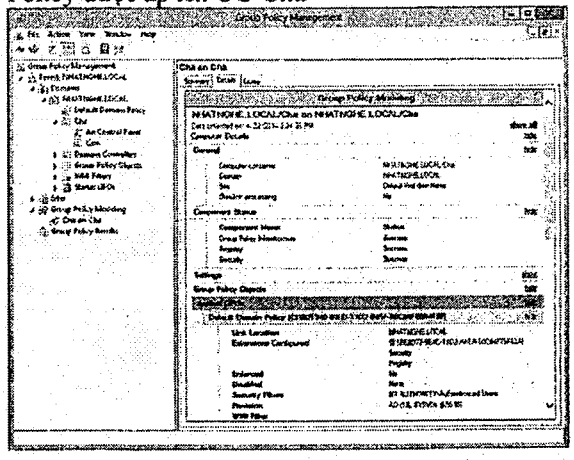
B3 - Màn hình Advanced Simulation Options → Chọn Default-First-Site-Name → Next



B4 - Màn hình Computer Security Groups, chọn Authenticated Users → Next

B5 - Các bước còn lại nhấn Next theo mặc định → Màn hình Completing…→ Finish

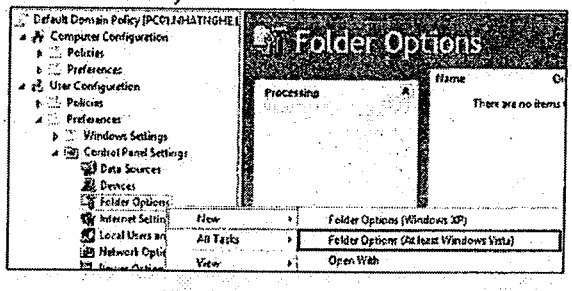
B6 - Quan sát thấy bảng báo cáo chi tiết về các Policy được áp lên OU Cha



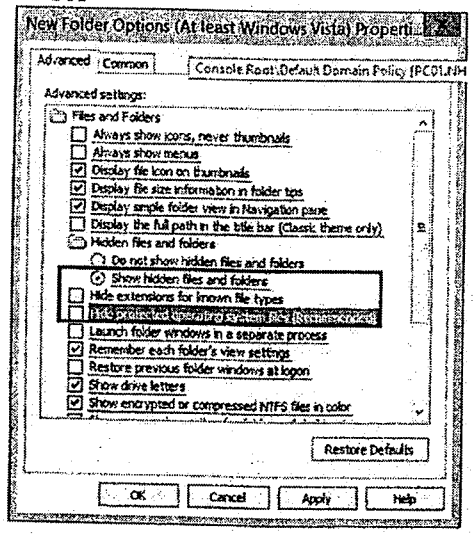
8. Item Level Targeting (Thực hiện trên máy PC01)

B1 - Mở Group Policy Management, chuột phải vào Default Domain Policy, chọn Edit…

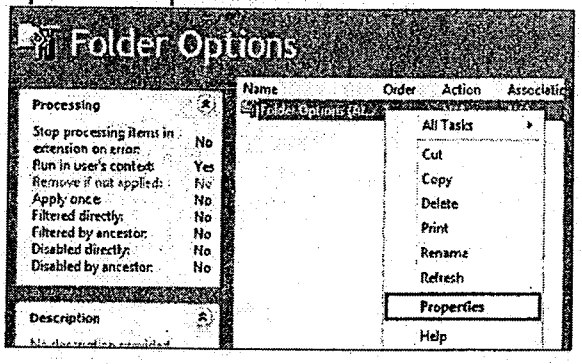
B2 - Bung mục User Configuration → Preferences → Control Panel Settings, chuột phải vào Folder Options, chọn New → Folder Options (at least Windows Vista)



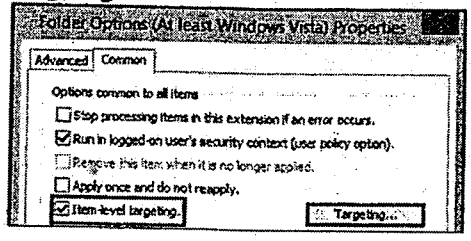
B3 - Mục Hidden files and folders, chọn Show hidden files and folders. Tắt dấu check ở 2 mục:
+ Hide extensions for known file types
+ Hide protected operating system files (Recommended)
→ OK



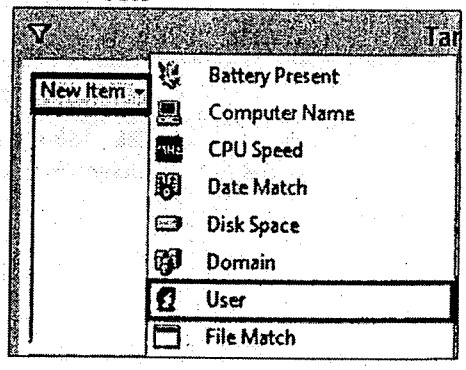
B4 - Ở khung bên phải → Chuột phải vào Folder Options → Properties



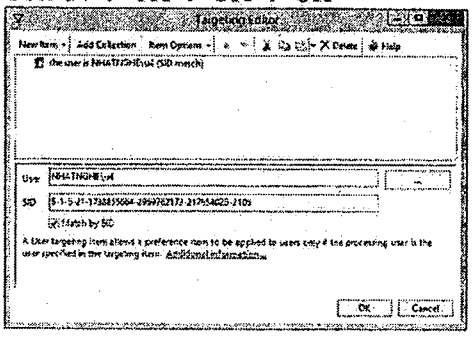
B5 - Qua tab Common, đánh dấu check vào mục Item-level targeting → chọn Targeting…



B6 - Tại màn hình Targeting Editor → Chọn New Item → User



B7 - Trong mục User → Browse → Add User u4 → OK → OK → OK



B8 - Kiểm tra: Trên máy PC02
+ Log on user u4 → Mở File Explorer, kiểm tra thấy các file ẩn xuất hiện và hiển thị đuôi file.
+ Log on user u3 → Mở File Explorer, không thấy các file ẩn.

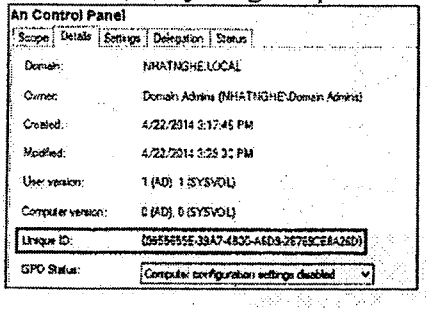
9. Disable một phần của policy

Đôi khi ta chỉ sử dụng một phần trong của GPO (ví dụ User Configuration), để tăng tốc quá trình xử lý GPO, ta nên tắt những phần không dùng đến.

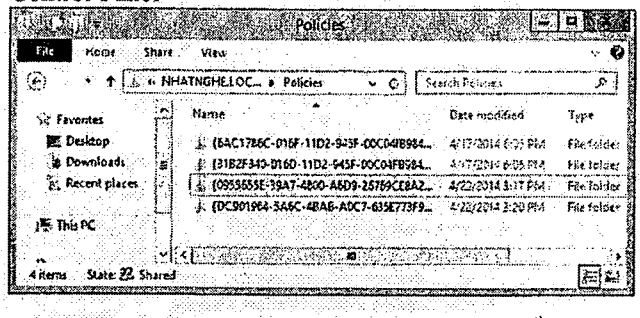
- Mở Group Policy Management, chọn GPO "Ẩn Control Panel" → Details , ở mục GPO Status, chọn Computer Configuration settings disabled → OK

10. Khảo sát nơi chứa policy templates

B1 - Mở Group Policy Management, chọn GPO "Ẩn Control Panel". Qua tab Details, chú ý dòng Unique ID



B2 - Truy cập vào ổ C:\Windows\SYSVOL\SYSVOL\nhatnghe.local\Policies, sẽ thấy có thư mục giống Unique ID của policy "Ẩn Control Panel"



B3 - Mở thư mục trùng với Unique ID → User → sẽ thấy có file Registry.pol. Thông tin về Policy được lưu vào file này.

B4 - Mở file Registry.pol bằng Notepad quan sát nội dung bên trong

GPO CENTRAL STORE & SECURITY FILTERING

CÁC BƯỚC TRIỂN KHAI

1. Tạo Central Store

2. Tạo GPO

a. Tạo Starter GPO

b. Tạo GPO từ Starter GPO

c. Kiểm tra

3. Security Filtering

A- CHUẨN BỊ

Mô hình bài lab bao gồm 2 máy:

+ PC01: Windows Server 2012 R2 - DC (Domain:NHATNGHE.LOCAL)

+ PC02: Windows 8.1 Enterprise đã join domain

- Trên PC01 tạo group IT và user Teo. Add Teo làm thành viên của Group IT.

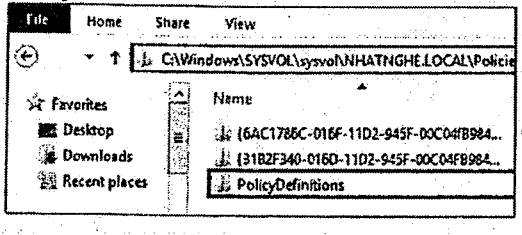
- Chỉnh password đơn giản và cho phép User Account Log On Locally

B- THỰC HIỆN

1. Tạo Central Store (Thực hiện trên máy PC01)

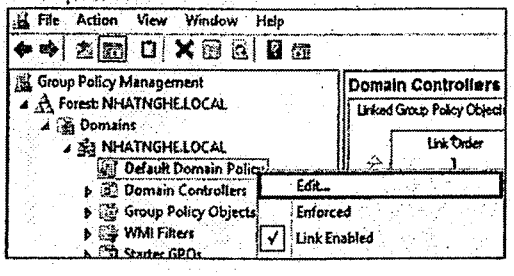
B1 - Mở File Explorer, truy cập vào đường dẫn C:\Windows\PolicyDefinitions. Chọn toàn bộ tập tin và thư mục có trong folder này → chuột phải nhấn Copy

B2 - Truy cập vào đường dẫn C:\Windows\SYSVOL\sysvol\NHATNGHE.LOCAL\Policies → Tạo mới Folder, đặt tên PolicyDefinitions

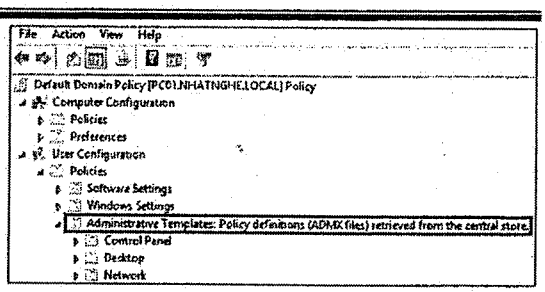


B3 - Nhấn Double Click vào folder PolicyDefinitions vừa tạo → chuột phải chọn Paste

B4 - Kiểm tra: Mở Group Policy Management Editor. Chuột phải vào Default Domain Policy → chọn Edit



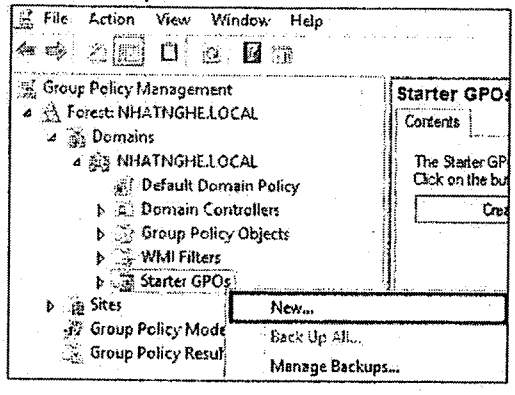
B5 - Bung mục User Configuration → Policies. Quan sát thấy mục Administrative Templates: Policy definitions (ADMX files) retrieved from the Central Store" → Đóng cửa sổ lại



2. Tạo GPO

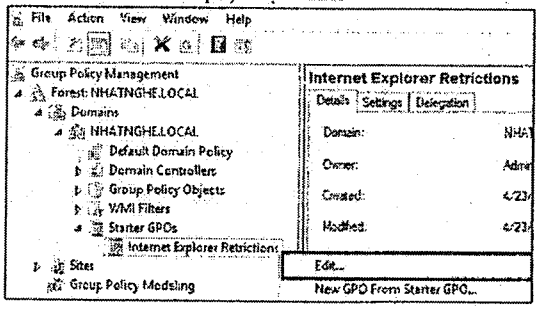
a. Tạo Starter GPO

B1 - Quay lại Group Policy Management Editor. Mở theo đường dẫn Forest: NHATNGHE.LOCAL → Domains → NHATNGHE.LOCAL. Chuột phải vào Starter GPOs → chọn New

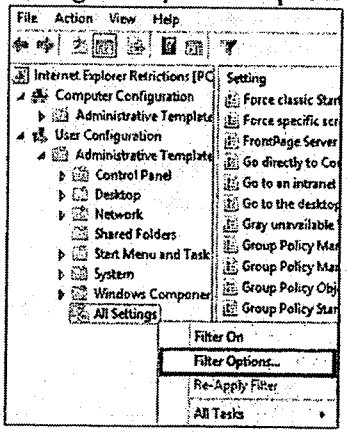


B2 - Ở mục Name, đặt tên là Internet Explorer Restricitions → OK

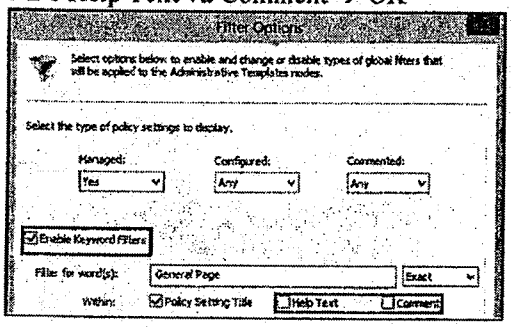
B3 - Chuột phải vào GPO Internet Explorer Restricitions vừa tạo, chọn Edit



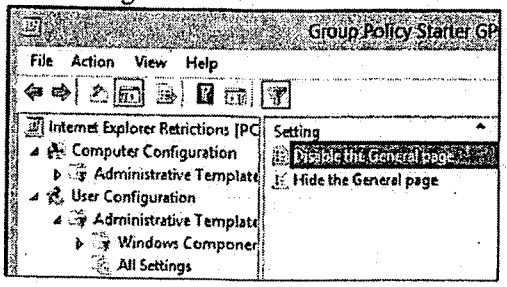
B4 - Mở theo đường dẫn User Configuration → Administrative Templates, chuột phải vào All Settings → chọn Filter Options



B5 - Đánh dấu chọn vào Enable Keyword Filters. Mục Filter for word(s), gõ vào General Page. Khung kế bên, chọn Exact. Bỏ dấu chọn ở 2 ô Help Text và Comment → OK



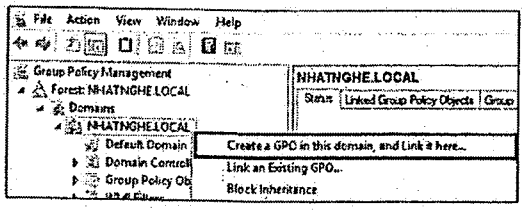
B6 - Double click vào mục Disable the General Page



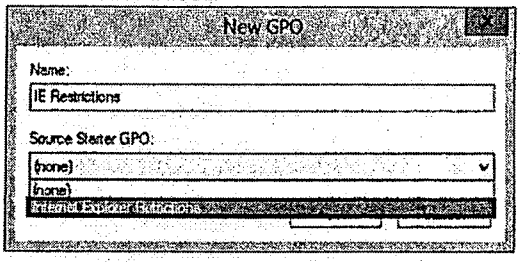
B7 - Chọn Enabled → OK

b. Tạo GPO từ Starter GPO

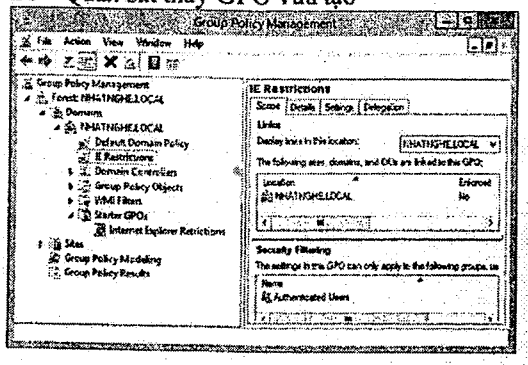
B1 - Quay lại cửa sổ Group Policy Managent Editor, chuột phải vào NHATNGHE.LOCAL → chọn Create a GPO in this domain, and Link it here.



B2 - Ở mục Name, đặt tên IE Restrictions. Ở mục Soure Starter GPO, chọn Internet Explorer Restrictions → OK.



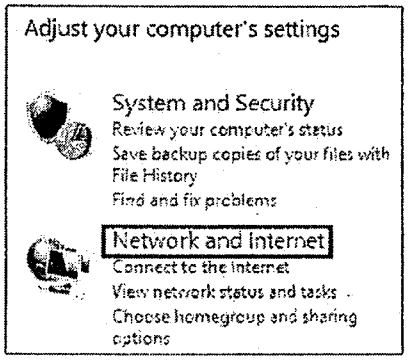
B3 - Quan sát thấy GPO vừa tạo



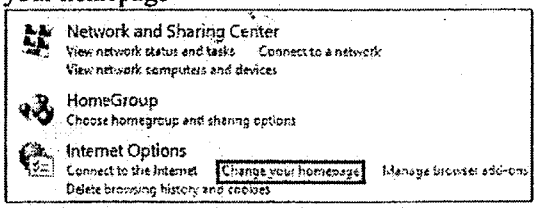
c. Kiểm tra

B1 - Trên máy PC02, log on user Teo

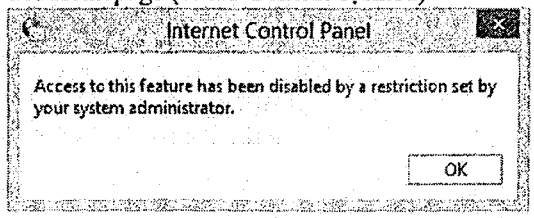
B2 - Mở Control Panel → chọn Network and Internet



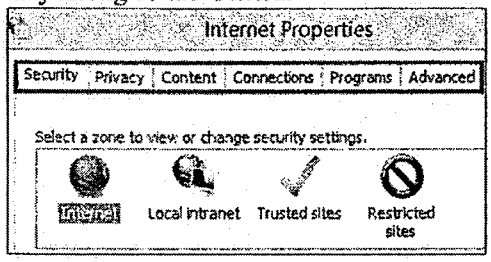
B3 - Ở mục Internet Options → chọn Change your homepage



B4 - Quan sát thấy báo lỗi không cho phép thay đổi Homepage (vì tab General bị khóa)

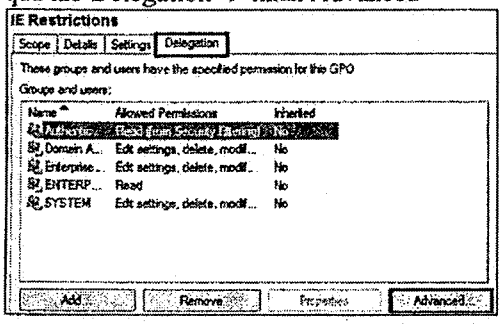


B5 - Tiếp theo mở Internet Options, quan sát thấy không có tab General



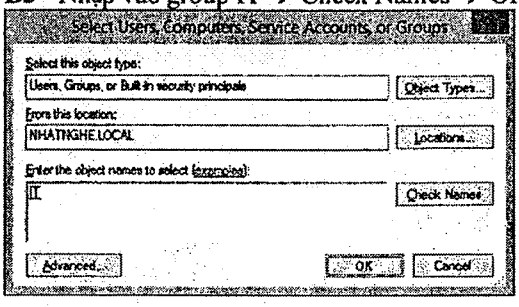
3. Security Filtering (Thực hiện trên máy PC01)

B1 - Qua máy PC01, quay lại Group Policy Management. Chọn vào policy IE Restriction, qua tab Delegation → nhấn Advanced

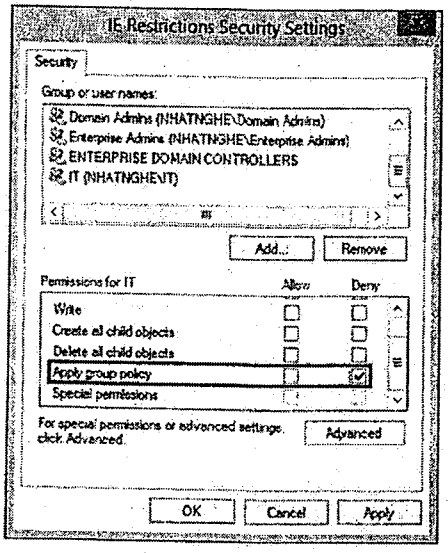


B2 - Nhấn nút Add

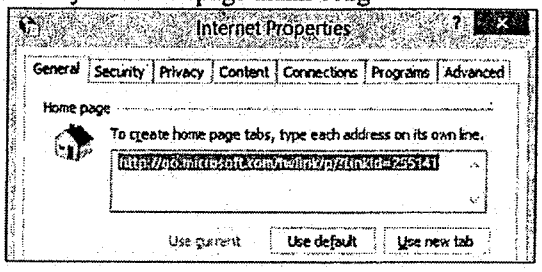
B3 - Nhập vào group IT → Check Names → OK



B4 - Tìm đến mục Apply Group Policy → đánh dấu chọn vào Deny → Apply → OK → Yes



B5 - Kiểm tra: Qua máy PC02, log on user Teo. Mở Internet Options, quan sát thấy có tab General và thay đổi Homepage thành công



GPO FINE-GRAINED PASSWORD POLICY

CÁC BƯỚC TRIỂN KHAI

1. Cấu hình Fine-Grained Password Policy

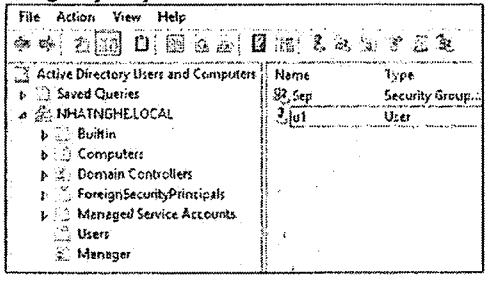
2. Kiểm tra

A- CHUẨN BỊ

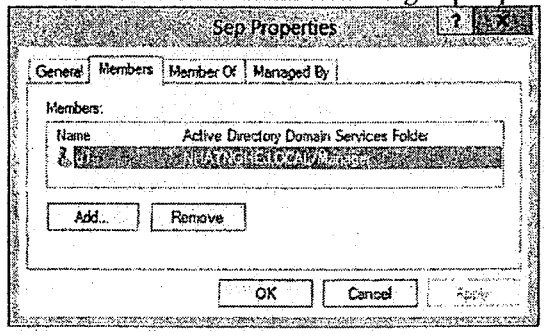
Mô hình bài lab bao gồm 1 máy:

+ PC01: Windows Server 2012 R2 DC (Domain: NHATNGHE.LOCAL)

B1 - Tạo OU Manager. Trong OU Manager, tạo group Sep và user U1.



B2 - Add User U1 là thành viên của group Sep.

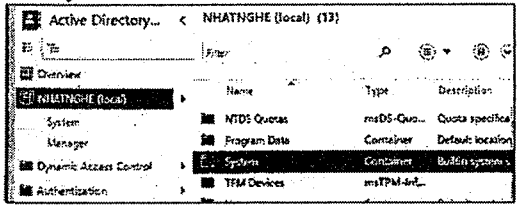


B- THỰC HIỆN

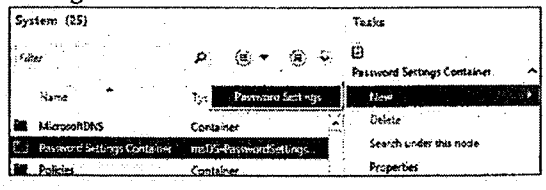
1. Cấu hình Fine-Grained Password Policy

B1 - Mở Server Manager → menu Tools → chọn Active Directory Administrative Center.

B2 - Ở khung bên trái → chọn NHATNGHE (local) → ở khung Details, nhấn double click vào System.



B3 - Ở khung Details, chuột phải vào Password Settings Container →chọn New → Password Settings



B4 - Màn hình Create Password Settings: Manager PSO → Khai báo các thông tin sau:

+ Name: ManagerPSO

+ Precedence: 10

+ Minimum password length: 15

+ Number of passwords remembered: 20

+ User must change the password after (days): 30

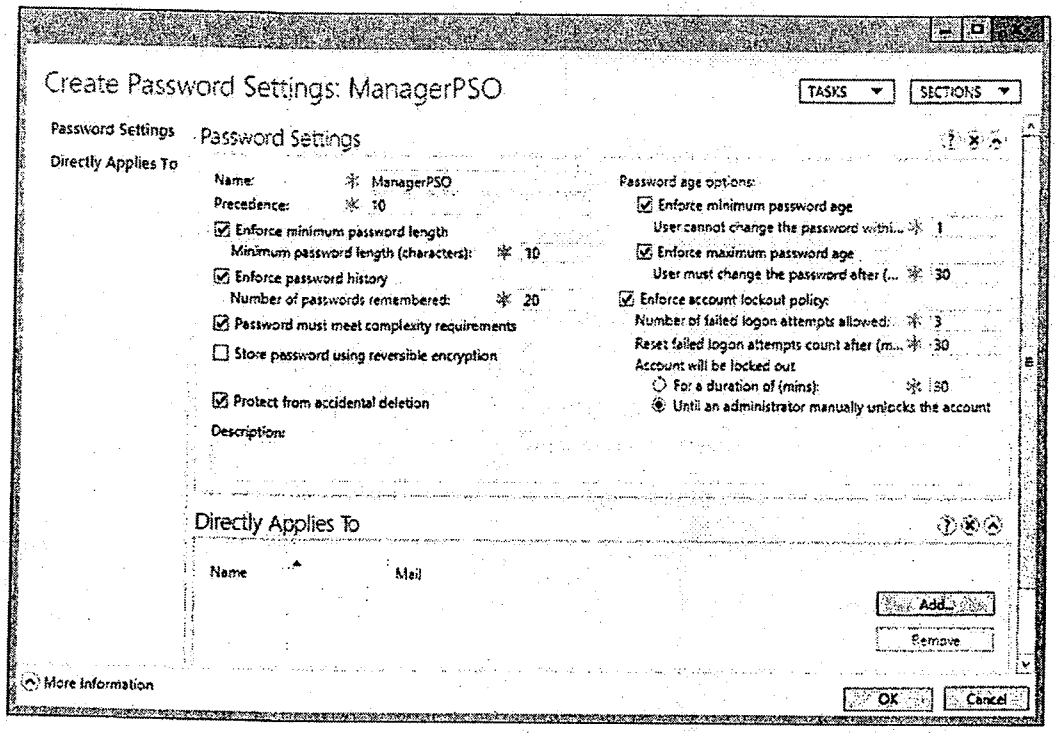
+ Đánh dấu chọn vào ô Enforce account lockout policy

+ Number of failed logon attempts allowed: 3

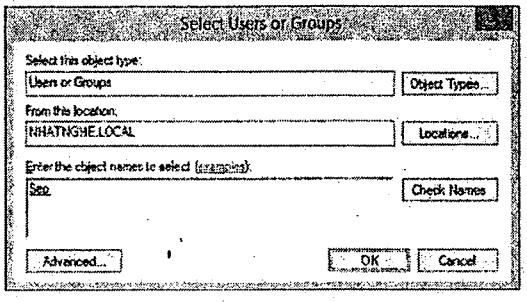
+ Reset failed logon attempts count after(mins): 30

+ Chọn ô Until an administrator manually unlocks the account

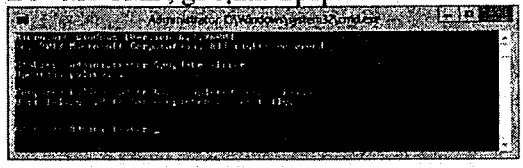
+ Ở khung Direct Apply To → nhấn Add



B5 - Nhập vào Sep → Check Names → OK → OK

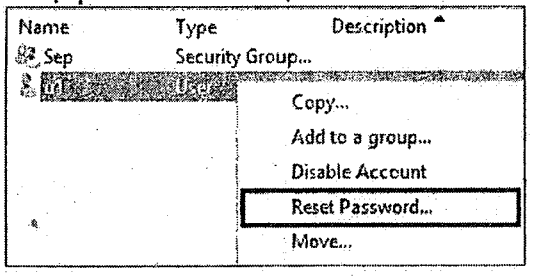


B6 - Mở CMD, gõ lệnh: Gpupdate /Force

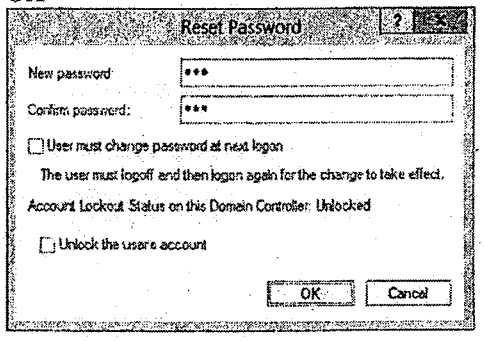


2. Kiểm tra

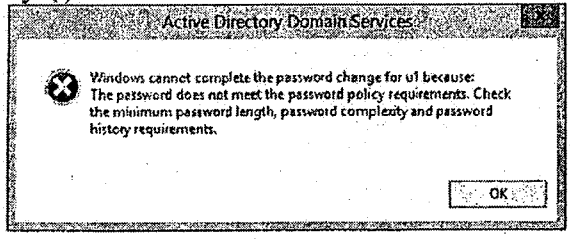
B1 - Mở Active Directory Users and Computers → Chuột phải user U1 → chọn Reset Password.



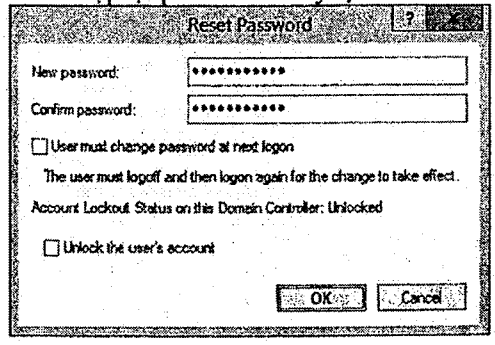
B2 - Nhập password chỉ 3 ký tự, vd: 123 → OK



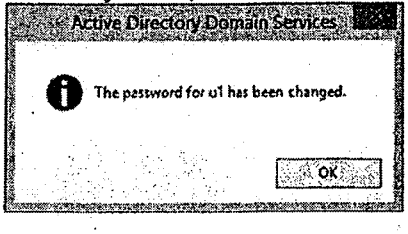
B3 - Hộp thoại báo lỗi không đáp ứng yêu cầu chính sách bảo mật (phải đặt mật khẩu tối thiểu 10 ký tự) → OK.



B4 - Nhập lại password 10 ký tự → OK



B5 - Thay đổi mật khẩu cho user thành công.



GPO ADMINISTRATIVE TEMPLATES – DEPLOY SOFTWARE – FOLDER REDIRECTION

CÁC BƯỚC TRIỂN KHAI

1. Cấu hình Administrative Templates

2. Cấu hình Deploy Software

3. Cấu hình Folder Redirection

A- CHUẨN BỊ

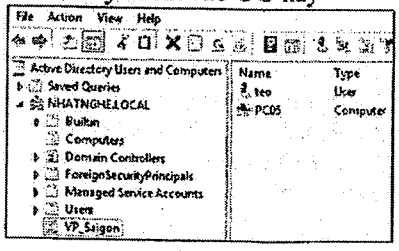
- Mô hình bài lab bao gồm 2 máy

+ PC01: Windows Server 2012 R2 DC (Domain: NHATNGHE.LOCAL)

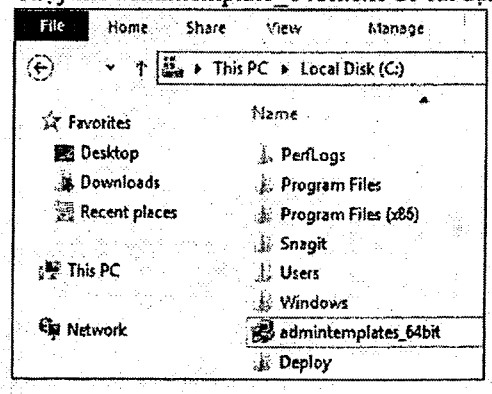
+ PC05: Windows 8.1 Enteprise đã join domain

B1 - Trên máy PC01, tạo thư mục C:\SaiGon. Share Everyone – Full Control

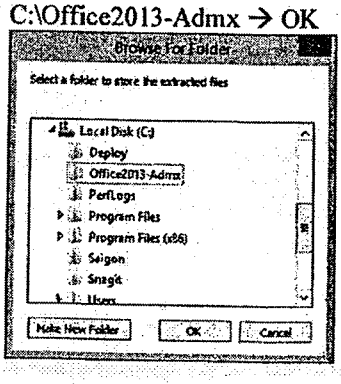
B2 - Tạo OU VP_SaiGon, tạo user Teo và move máy client vào OU này



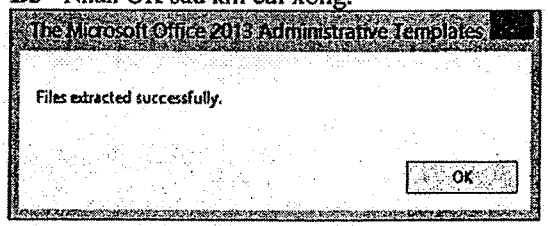
B3 - Truy cập vào Server, copy source cài đặt Office 2013 Administrative Templates (ADMX). Chạy file admintemplate_64bit.exe để cài đặt



B4 - Chọn Make New Folder → tạo thư mục C:\Office2013-Admx → OK



B5 - Nhấn OK sau khi cài xong.



B6 - PC05 cài đặt Microsoft Office 2013

B- THỰC HIỆN

1. Cấu hình Administrative Templates (Thực hiện trên máy PC01)

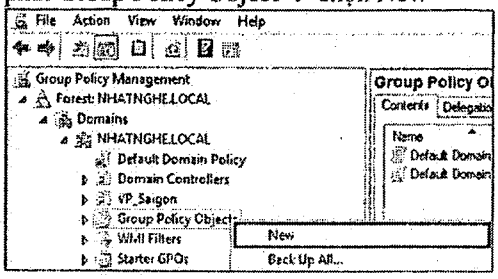
B1 - Mở File Explorer, truy cập vào đường dẫn C:\Office2013-Admx\admx\en-us → Quét chọn toàn bộ, chuột phải nhấn Copy

B2 - Mở theo đường dẫn C:\Windows\PolicyDefinitions\en-US, chuột phải chọn Paste

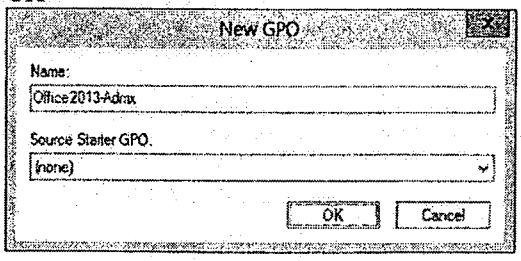
B3 - Quay lại đường dẫn, C:\Office2013-Admx\admx → Quét chọn toàn bộ file *.admx, chuột phải nhấn Copy.

B4 - Mở theo đường dẫn C:\Windows\PolicyDefinitions, chuột phải chọn Paste.

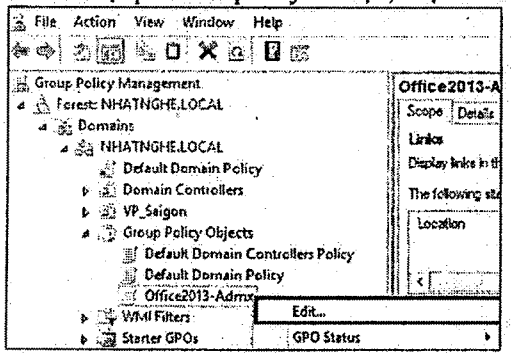
B5 - Mở Group Policy Management → chuột phải Group Policy Object → chọn New



B6 - Ở mục Name, đặt tên Office2013-Admx → OK

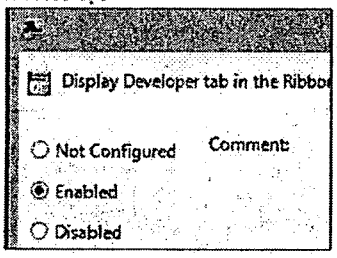


B7 - Chuột phải vào policy vừa tạo, chọn Edit

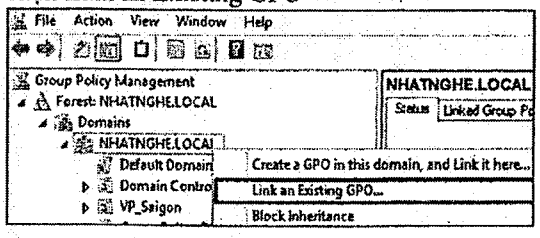


B8 - Bung theo đường dẫn User Configuration → Policies → Administrative Templates → Microsoft Word 2013→ Word Options → Customize Ribbon, double click vào mục Display Developer tab in the Ribbon

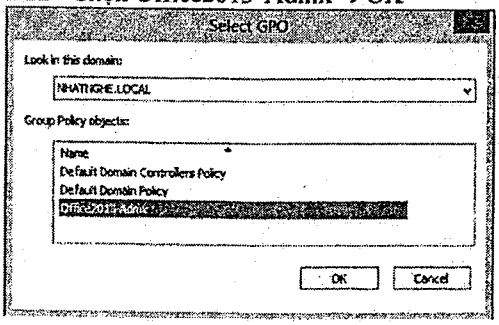
B9 - Chọn Enabled → OK → Đóng cửa sổ Group Policy Management Editor lại



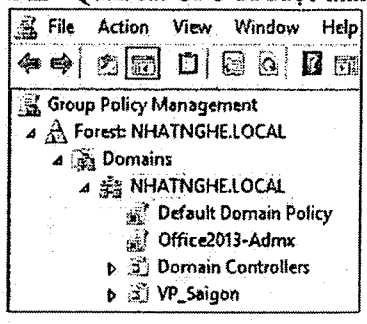
B10 - Chuột phải vào NHATNGHE.LOCAL, chọn Link an Existing GPO



B11 - Chọn Office2013-Admx →OK

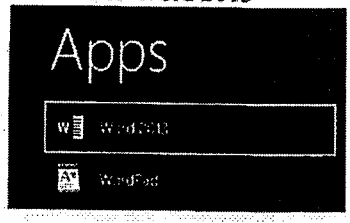


B12 - Quan sát GPO đã được link

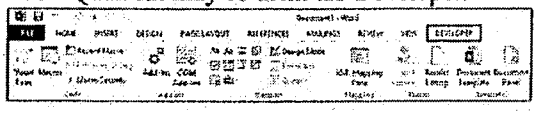


B13 - Mở CMD, gõ lệnh Gpupdate /Force

B14 - Kiểm tra: Trên máy PC05, log on user Teo → Mở Word 2013

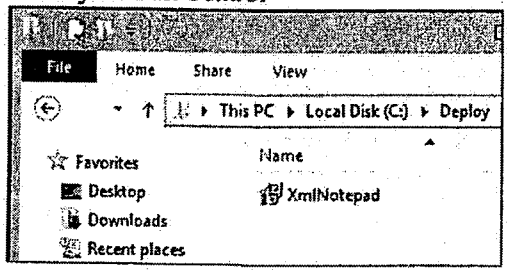


B15 - Quan sát thấy có thêm tab Developer.

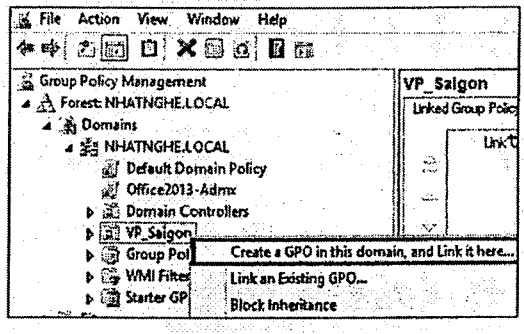


2. Deploy Software (Thực hiện trên máy PC01)

B1 - Truy cập vào Server, copy file XmlNotepad.msi vào C:\Deploy. Share Folder – Everyone Full Control

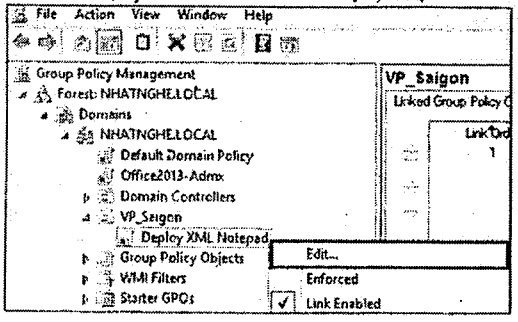


B2 - Mở Group Policy Management, chuột phải vào OU VP_SaiGon → chọn Create a GPO in this domain and Link it here

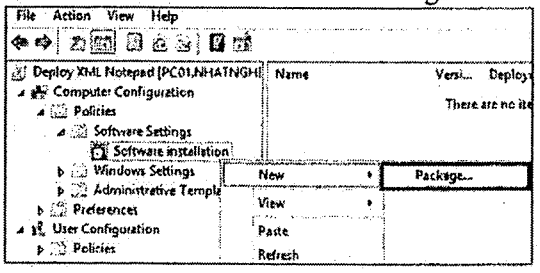


B3 - Ở mục Name, đặt tên Deploy XML Notepad → OK

B4 - Chuột phải vào GPO vừa tạo, chọn Edit.

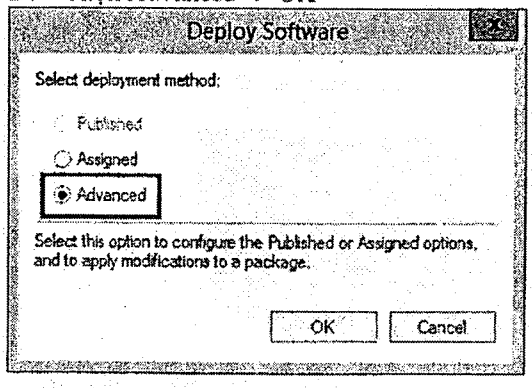


B5 - Mở theo đường dẫn Computer Configuration → Policies → Software Settings, chuột phải Software installation → New → Package

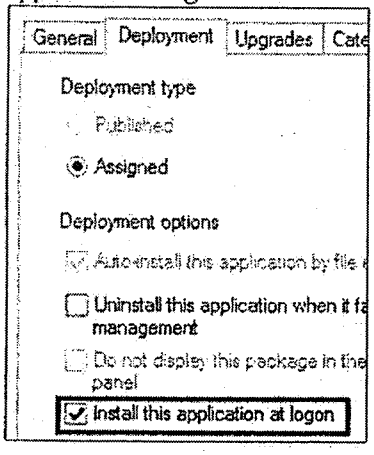


B6 - Trỏ đường dẫn \\pc01\Deploy\XMLNotepad.msi → Open

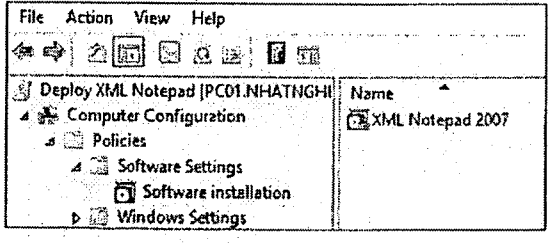
B7 - Chọn Advanced → OK



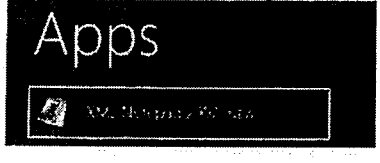
B8 - Đánh dấu chọn vào ô Install this application at logon → OK



B9 - Quan sát thấy Software Installation vừa tạo.



B10 - Kiểm tra:
+ Qua máy PC05, Restart lại máy.
+ Log on Administrator, mở CMD, gõ lệnh Gpupdate /Force → Restart lại máy
+ Log on Teo, quan sát thấy máy Client đã được cài đặt XMLNotepad

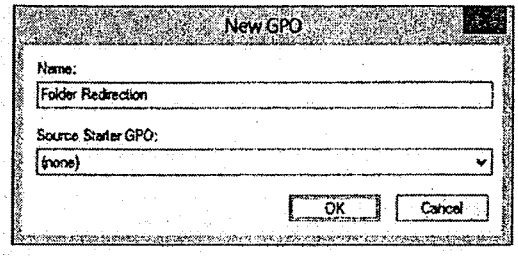


3. Cấu hình Folder Redirection (Thực hiện trên máy PC01)

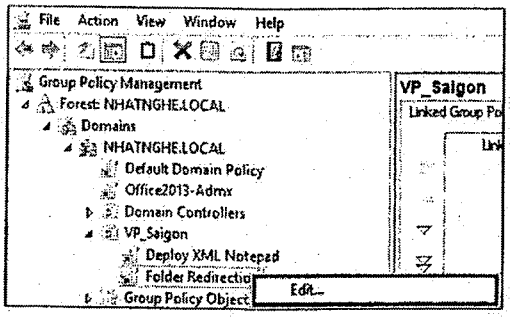
B1 - Mở File Explorer, tạo thư mục C:\FolderRedir. Share Everyone – Full Control

B2 - Mở Group Policy Management, chuột phải OU VP_SaiGon → chọn Create a GPO in this domain and Link it here.

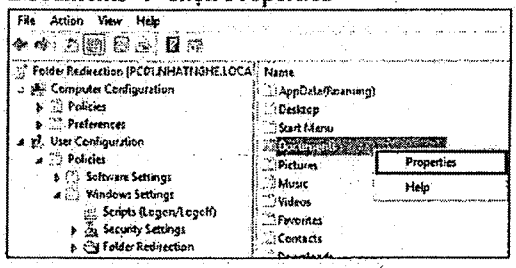
B3 - Ở mục Name, đặt tên Folder Redirection → OK



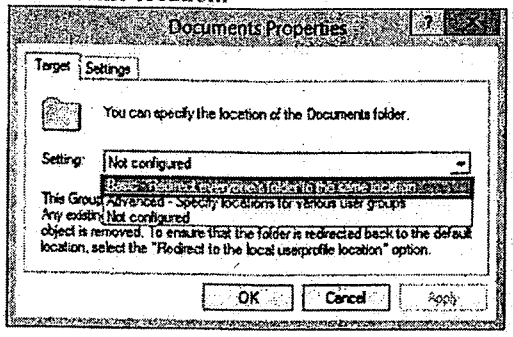
B4 - Chuột phải vào GPO vừa tạo → chọn Edit



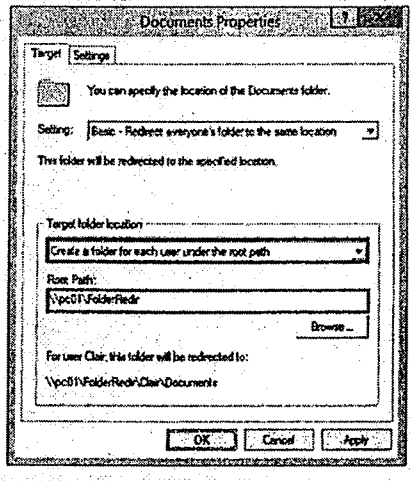
B5 - Mở theo đường dẫn User Configuration → Policies → Windows Settings → Folder Redirection. Ở khung bên phải, chuột phải vào Documents → chọn Properties



B6 - Chọn Basic – Redirect everyone's folder to the same location.

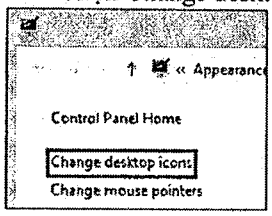


B7 - Ở mục Target Folder Location → chọn Create a folder for each user under the root path. Ở mục Root Path → gõ \\pc01\FolderRedir → OK → Yes

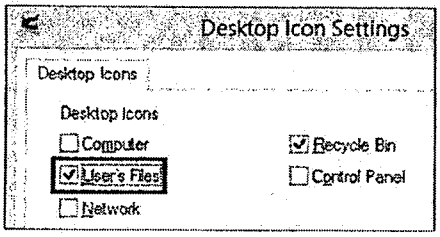


B8- Kiểm tra:
+ Qua máy PC05, Restart lại máy.
+ Log on Administrator, mở CMD, gõ lệnh Gpupdate /Force → Restart lại máy
+ Log on Teo, chuột phải vào Desktop → chọn Personalize

B9 - Chọn Change desktop icons

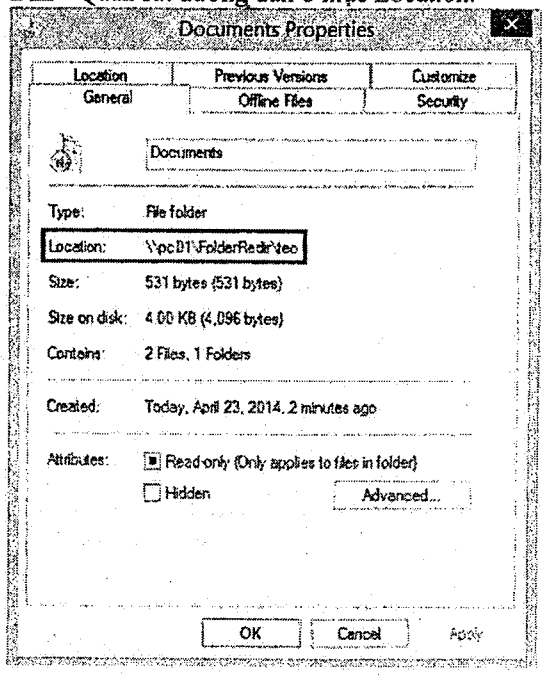


B10 - Đánh dấu chọn vào ô User's Files → OK



B11 - Double click vào folder Teo trên Desktop. Chuột phải vào Documents → chọn Properties

B12 - Quan sát đường dẫn ở mục Location.



GPO SECURE MEMBER SERVER – AUDITING – APPLOCKER – ADVANCED FIREWALL

CÁC BƯỚC TRIỂN KHAI

1. Sử dụng Group Policy để bảo mật Member Servers

2. Auditing

a. Giám sát truy cập File hệ thống

b. Giám sát User Log on trên domain

3. Cấu hình Applocker Policy

4. Cấu hình Windows Firewall

A- CHUẨN BỊ

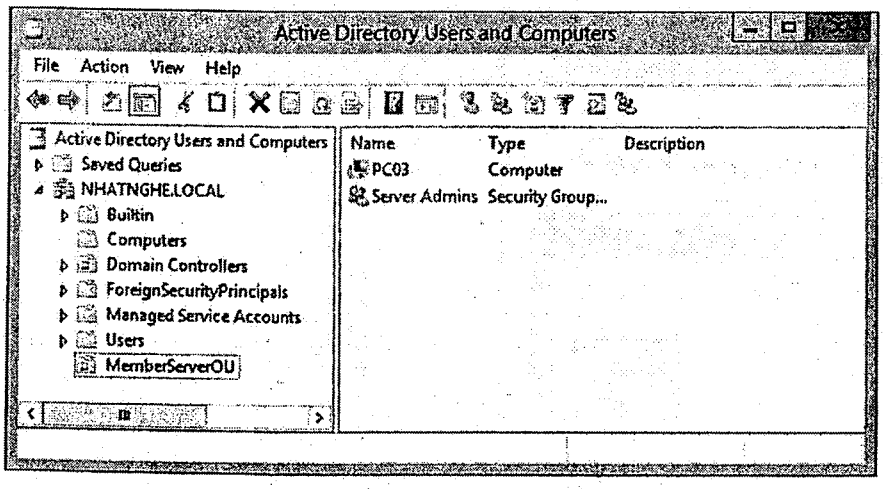
Mô hình bài lab bao gồm 2 máy:

+ PC01: Windows Server 2012 R2 DC

+ PC03: Windows Server 2012 R2 đã join domain

+ PC05: Windows 8.1 Enterprise đã join domain

- Trên PC01, tạo OU MemberServerOU, move Computer PC03 vào OU này và tạo thêm Group Server Admins

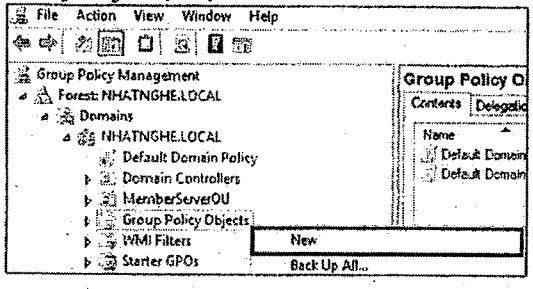


- Tạo User Teo.

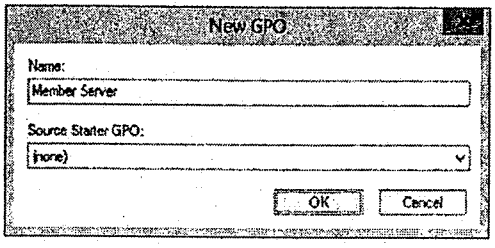
B- THỰC HIỆN

1. Sử dụng Group Policy để bảo mật Member Servers (Thực hiện trên PC01)

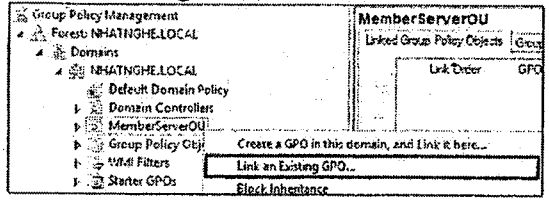
B1 - Mở Group Policy Management → Bung Forest: NHATNGHE.LOCAL →Domains → NHATNGHE.LOCAL. Chuột phải vào Group Policy Objects, chọn New.



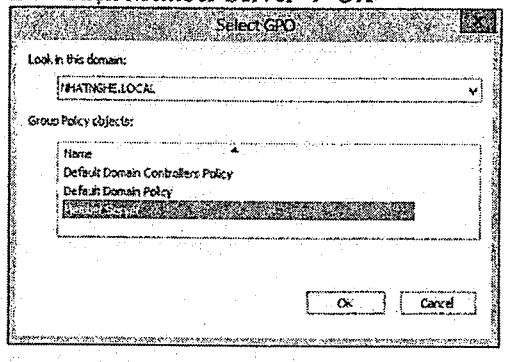
B2 - Ở mục Name, đặt tên Member Server → OK



B3 - Chuột phải vào OU MemberServerOU, chọn Link an Existing GPO.



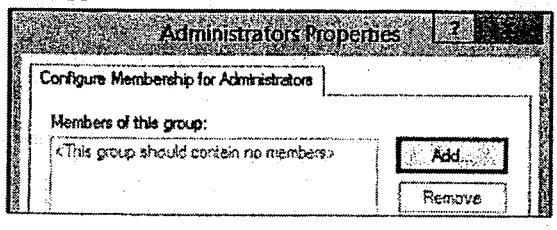
B4 - Chọn Member Server → OK



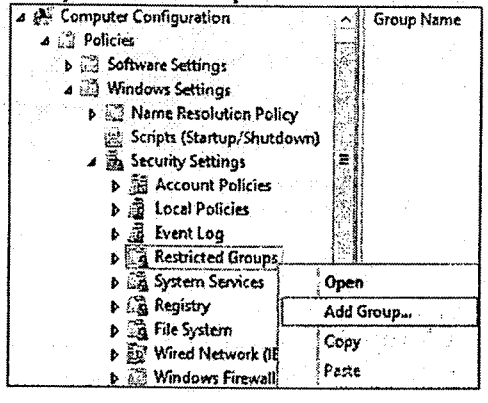
B5 - Chuột phải vào Default Domain Policy → chọn Edit

B7 - Nhấn Browse, nhập vào Administrators → Check Names → OK

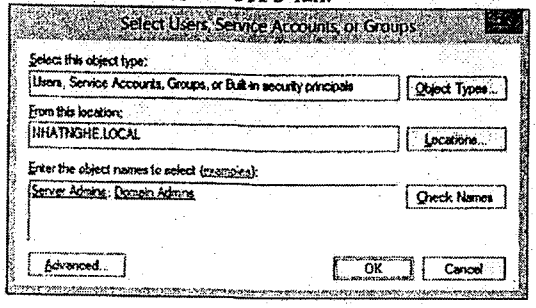
B8 - Khung Members of this group → Add → Browse



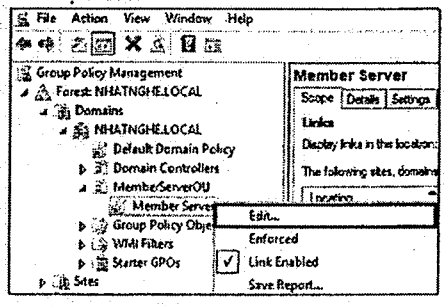
B6 - Mở theo đường dẫn Computer Configuration → Windows Settings → Security Settings. Chuột phải vào Restricted Groups → Add Group



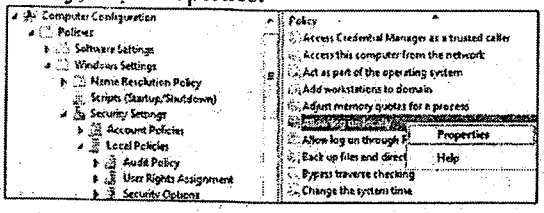
B9 - Nhập vào: Server Admins, Domain Admins → Check Names → OK 3 lần.



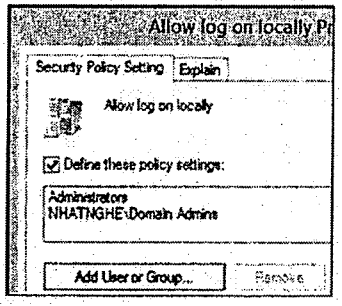
B10 - Chuột phải vào GPO Member Server → chọn Edit



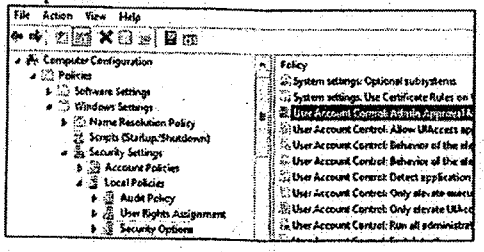
B11 - Mở theo đường dẫn Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment. Chuột phải vào Allow log on locally, chọn Properties.



B12 - Nhấn vào nút Add User or Group → Nhập vào Administrators, Domain Admins → Check Names → OK → OK



B13 - Tiếp tục ở khung bên trái → chọn Security Options. Khung bên phải → Double click vào User Account Control: Admin Approval Mode for the Built-in Administrator account, chọn Properties

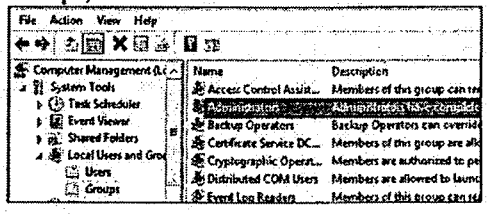


B14 - Chọn Enabled → OK

B15 - Kiểm tra: Trên máy PC03, log on Administrator. Mở CMD, gõ lệnh Gpupdate /force

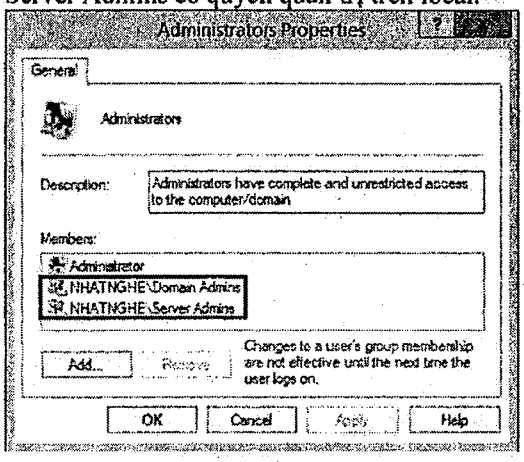
B16 - Mở Server Manager, vào menu Tools → chọn Computer Management

B17 - Bung mục Local Users and Groups → Groups, double click vào Administrators



B19 - Log off Administrators, log on bằng user Teo.

B18 - Quan sát thấy nhóm Domain Admins và Server Admins có quyền quản trị trên local.

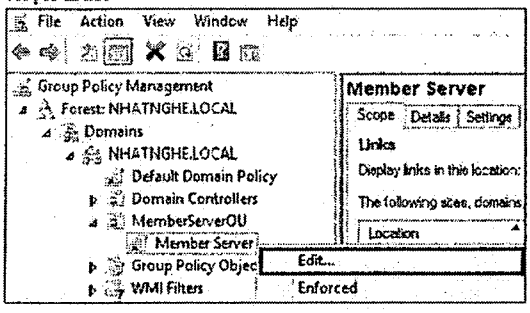


B20 - Quan sát thấy user Teo không được phép log on trên máy PC03 được.

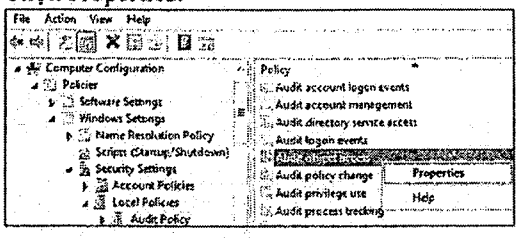
2. Auditing

a. Giám sát truy cập File hệ thống

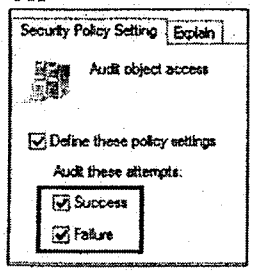
B1 - Chuột phải vào GPO Member Server → chọn Edit



B2 - Mở theo đường dẫn Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy. Chuột phải vào Audit object access → Chọn Properties.



B3 - Đánh dấu chọn vào ô Define these policy settings, sau đó chọn 2 ô Success và Failure → OK

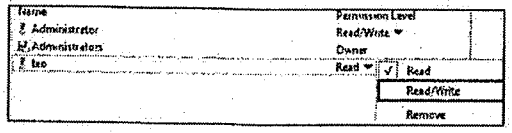


B4 - Qua máy PC03, mở File Explorer, tạo thư mục C:\Data. Chuột phải vào thư mục Data → chọn Share with → Specific people.

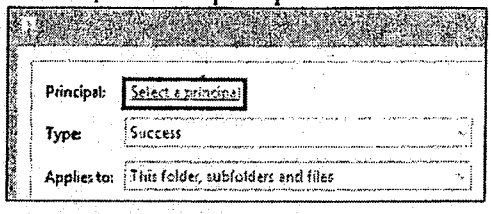
B6 - Chuột phải vào thư mục Data → chọn Properties → Nhấn Advanced

B7 - Qua tab Auditing → Nhấn Add

B5 - Share user Teo → Read/Write → Share → Done

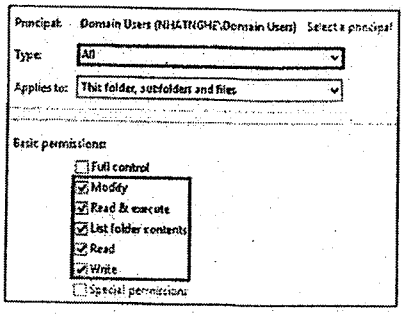


B8 - Chọn Select a principal



B9 - Nhập vào Domain Users → Check Names → OK

B10 - Ở mục Type → chọn All. Ở mục Basic permissions → Đánh dấu chọn vào ô Write → OK 3 lần

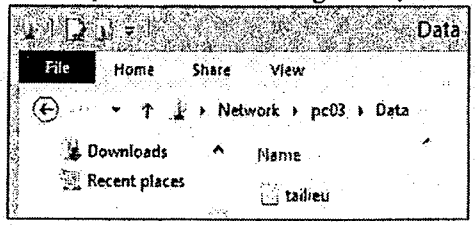


B11 - Mở CMD, gõ lệnh: Gpupdate /force

B12 - Kiểm tra: Trên PC05, log on Administrator → Mở CMD, gõ lệnh Gpupdate /force

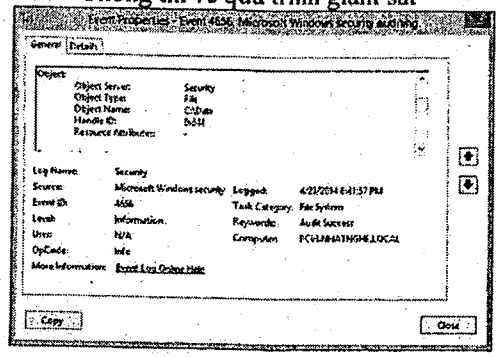
B13 - Log off Administrator, log on user Teo. Nhấn tổ hợp phím ⊞ + R, gõ \\pc03

B14 - Tạo file tailieu.txt trong thư mục Data

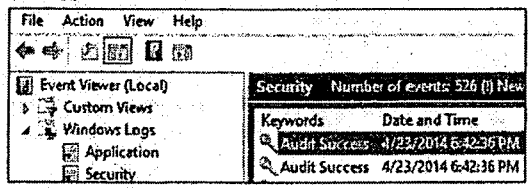


B15 - Qua máy PC03, mở Server Manager → menu Tools → chọn Event Viewer

B17 - Thông tin về quá trình giám sát



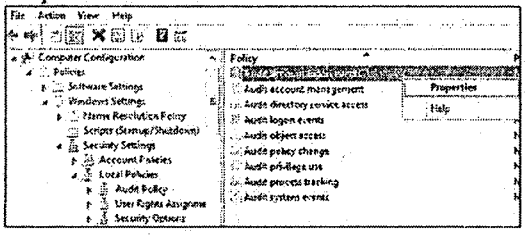
B16 - Ở khung bên trái chọn Windows Logs → Security. Nhấn double click vào event Audit Sucess



b. Giám sát User Log on trên domain (Thực hiện trên máy PC01)

B1 - Mở Group Policy Management → Chuột phải vào Default Domain Policy → chọn Edit

B2 - Mở theo đường dẫn Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy. Chuột phải vào Audit account log on events → Chọn Properties.



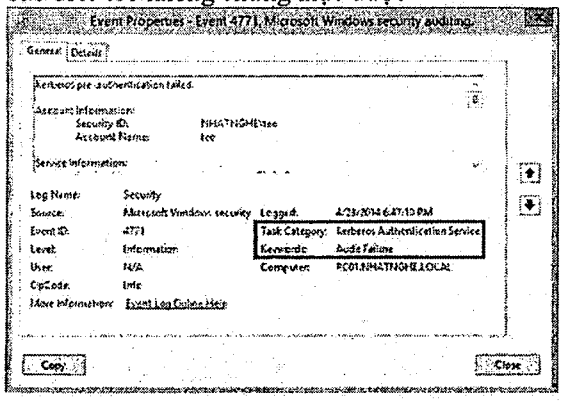
B3 - Đánh dấu chọn vào ô Define these policy settings, sau đó chọn 2 ô Success và Failure → OK

B4 - Mở CMD, gõ lệnh Gpupdate /Force

B5 - Kiểm tra: Trên máy PC05, log on Administrator. Mở CMD, gõ lệnh Gpupdate /Force

B6 - Log off Administrator, log on user Teo (cố tình nhập mật khẩu sai)

B7 - Qua máy PC01, mở Event Viewer → chọn Windows Logs → Securities. Quan sát thấy event báo user teo không chứng thực được

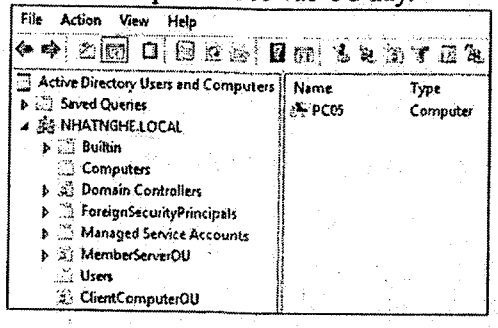


B8 - Qua máy PC05, log on user Teo, nhập đúng mật khẩu

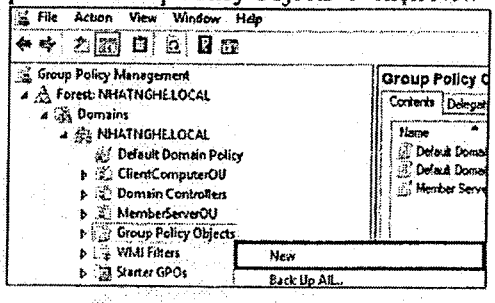
B9 - Qua máy PC01, kiểm tra Event Viewer, thấy event Audit Success do user Teo đăng nhập thành công.

3. Cấu hình Applocker Policy (Thực hiện trên PC01)

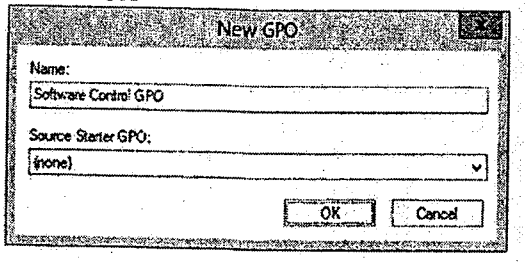
B1 - Mở Active Directory Users and Computers, tạo OU ClientComputerOU, sau đó move computer PC05 vào OU này.



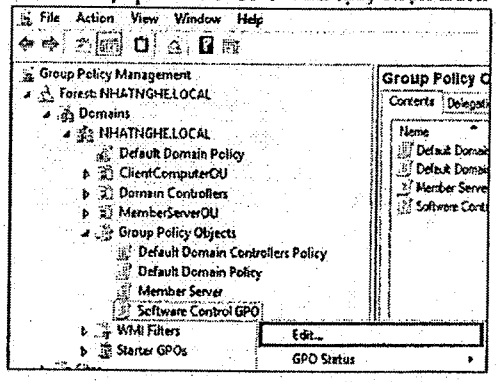
B2 - Mở Group Policy Management → Chuột phải vào Group Policy Objects → chọn New



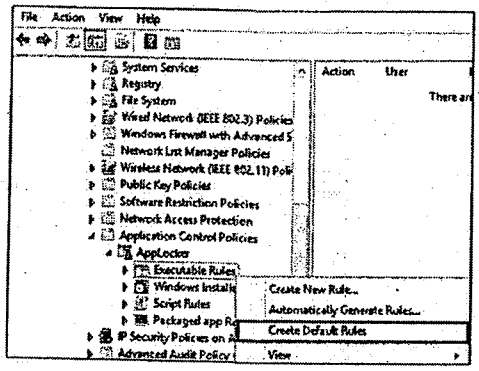
B3 - Ở mục Name, đặt tên Software Control GPO → OK



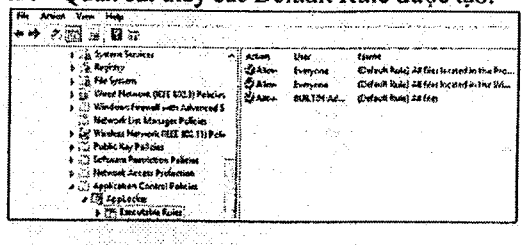
B4 - Chuột phải vào GPO vừa tạo, chọn Edit.



B5 - Mở theo đường dẫn: Computer Configuration → Policies → Windows Settings → Security Settings → Application Control Policies → AppLocker. Chuột phải vào Executable Rules → chọn Create Default Rules

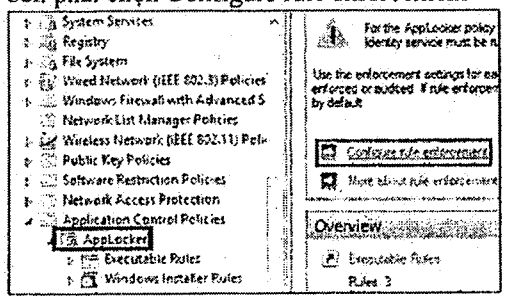


B6 - Quan sát thấy các Default Rule được tạo.

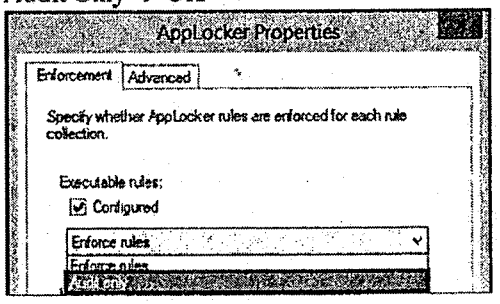


B7 - Thực hiện tương tự tạo Default Rule cho Windows Installer Rules, Script Rules, và Package App Rules.

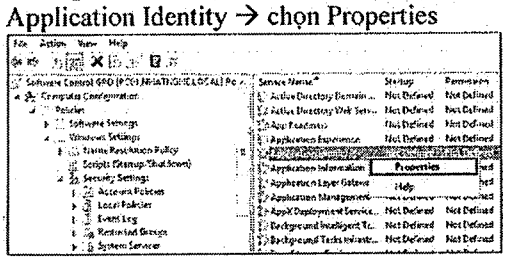
B8 - Nhấn chuột vào AppLocker → Ở khung bên phải chọn Configure rule enforcement



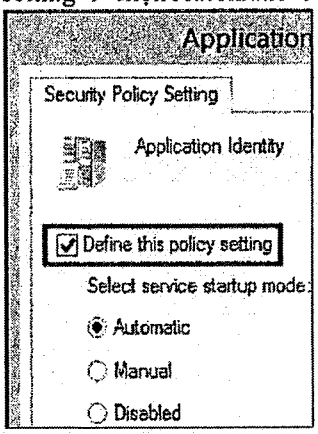
B9 - Đánh dấu chọn vào Configured → chọn Audit Only → OK



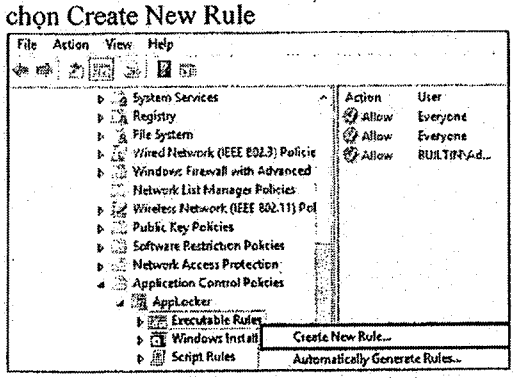
B10 - Mở theo đường dẫn Computer Configuration → Policies → Windows Settings → Security Settings. Chuột phải vào Application Identity → chọn Properties



B11 - Đánh dấu chọn vào ô Define this policy setting → chọn Automatic → OK

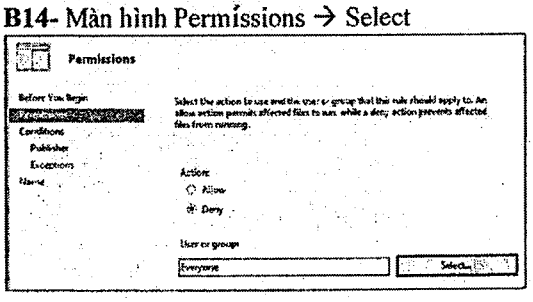


B12 - Chuột phải vào Executable Rules → chọn Create New Rule



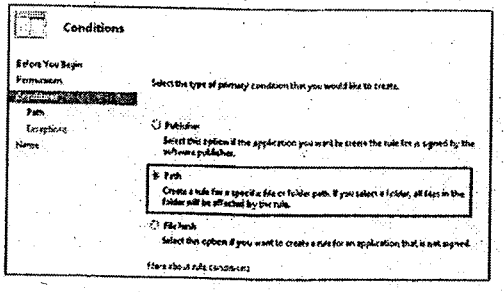
B13 - Màn hình Before you begin → Next

B14- Màn hình Permissions → Select

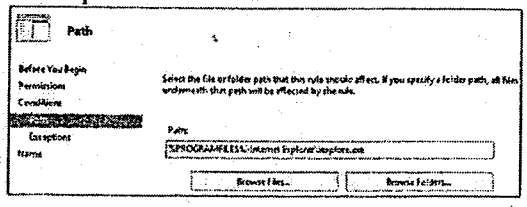


B15 - Nhập vào user Teo → Check Names → OK → Next

B16 - Màn hình Conditions → chọn Path → Next

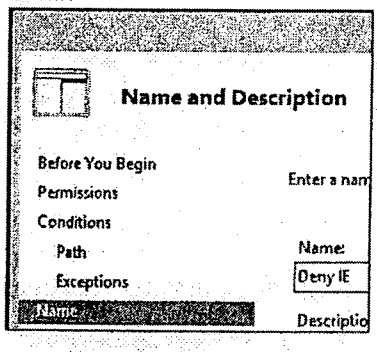


B17 - Nhấn Browse Files và trỏ đường dẫn đến file iexplore.exe → Next

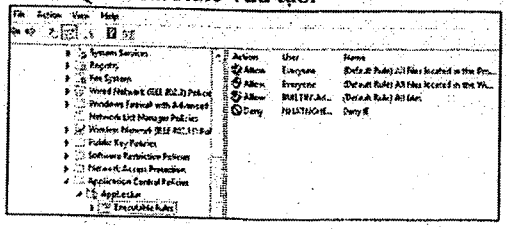


B18 - Màn hình Exceptions → Next

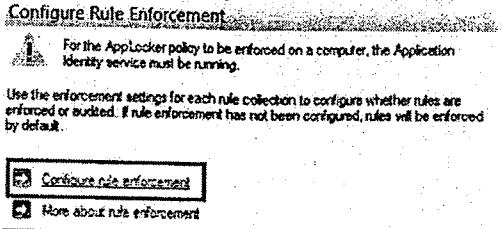
B19 - Màn hình Name → đặt tên Deny IE → Create



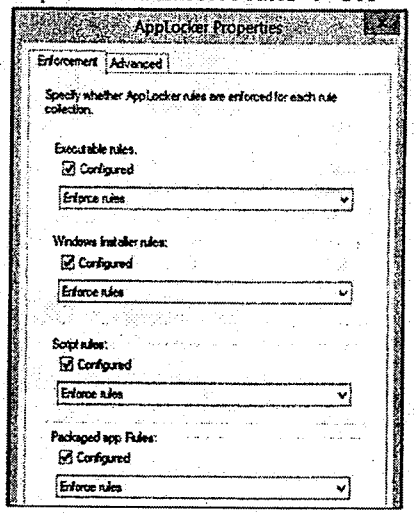
B20 - Quan sát Rule vừa tạo.



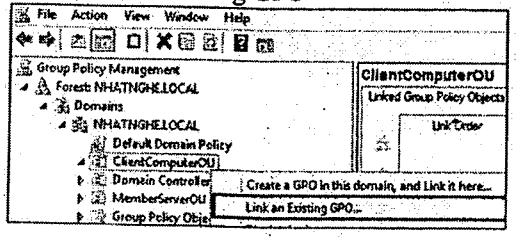
B21 - Ở khung bên trái chọn AppLocker → nhấn vào mục Configure rule enforcement



B22 - Đánh dấu chọn vào các ô Configured → chọn tất cả là Enforce rules → OK

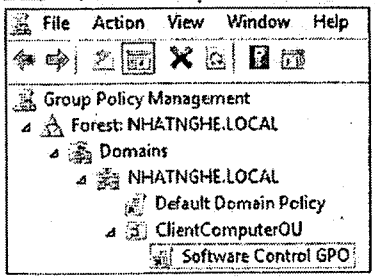


B23 - Chuột phải vào ClientComputer OU → chọn Link an Existing GPO



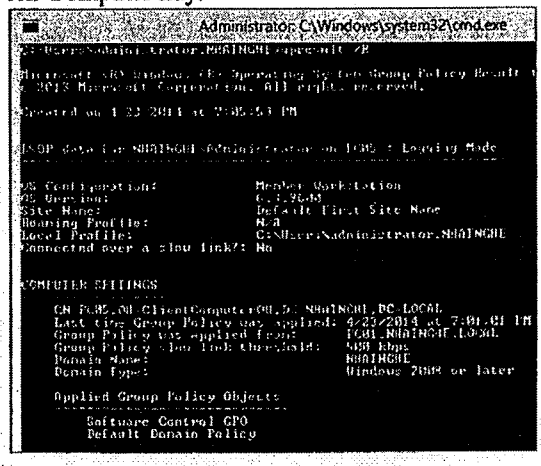
B24 - Chọn Software Control GPO vừa tạo → OK

B25 - GPO đã được link vào OU.

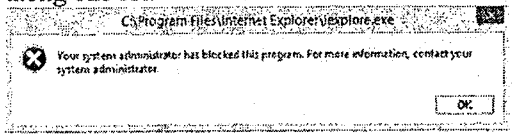


B26 - Mở CMD, gõ lệnh Gpupdate /Force

B27 - Kiểm tra: Trên PC05, log on user Teo, mở CMD, gõ lệnh Gpresult /R để kiểm tra policy áp lên Computer này.

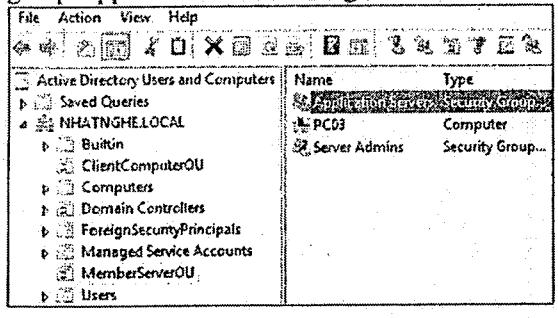


B28 - Mở Internet Explorer → nhận được thông báo lỗi.



4. Cấu hình Windows Firewall (Thực hiện trên PC01)

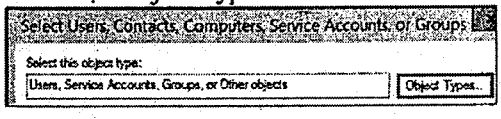
B1 - Mở Active Directory Users and Computers, tạo group Application Servers trong MemberServerOU.



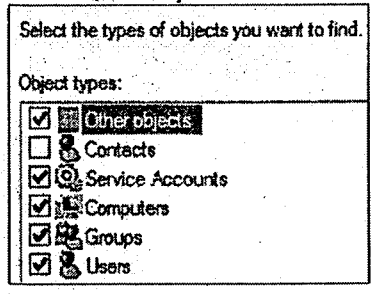
B2 - Chuột phải vào group Application Servers → chọn Properties

B3 - Qua tab Members → Add

B4 - Chọn Object Types



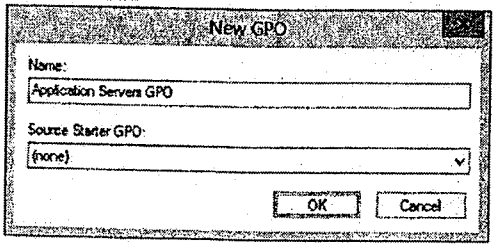
B5 - Chọn Computers → OK 3 lần.



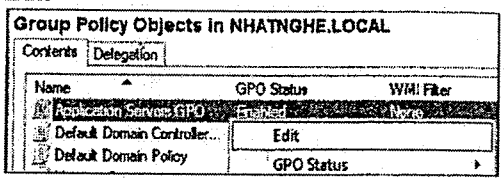
B6 - Nhập vào PC03 → Check Names → OK → OK

B7 - Mở Group Policy Management, chuột phải vào Group Policy Objects → New

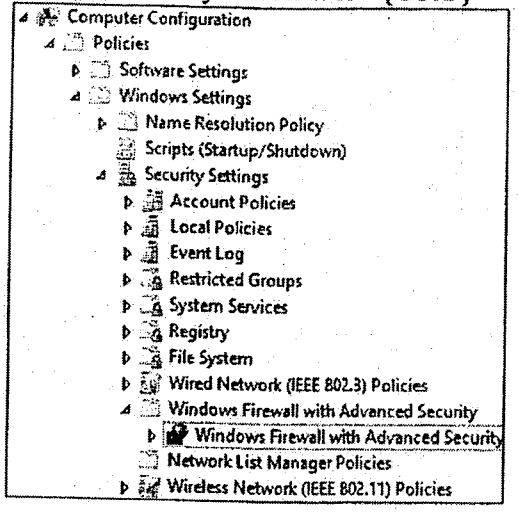
B8 - Ở mục Name, đặt tên là Application Servers GPO → OK



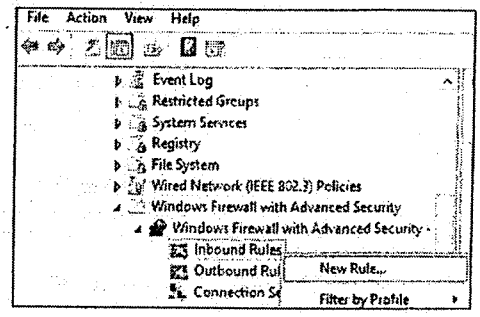
B9 - Chuột phải vào GPO vừa tạo → chọn Edit



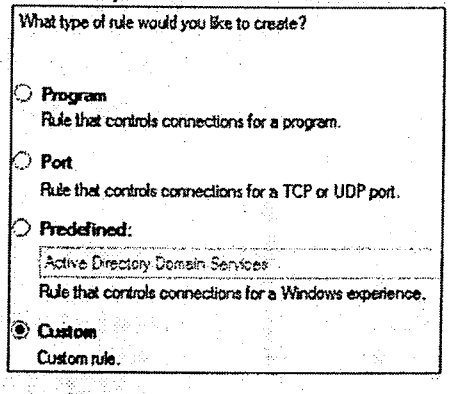
B10 - Mở theo đường dẫn Computer Configuration → Policies → Windows Settings → Security Settings → Windows Firewall with Advanced Security. Nhấn vào Windows Firewall with Advanced Security - LDAP://CN={GUID}



B11 - Chuột phải vào Inbound Rules → New Rule

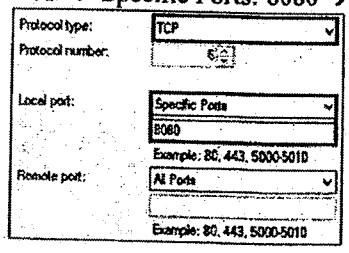


B12 - Chọn Custom → Next



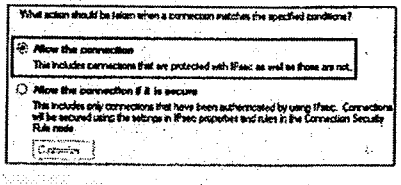
B13 - Màn hình Program → Next

B14 - Màn hình Protocol and Ports → Mục Protocol: TCP → Specific Ports: 8080 → Next

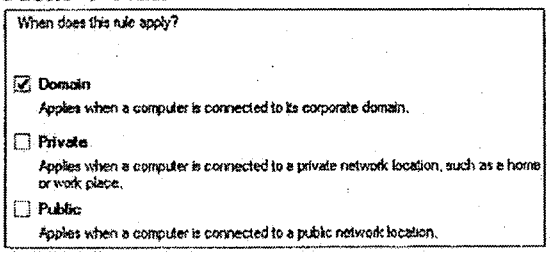


B15 - Màn hình Scope → Next

B16 - Màn hình Action → chọn Allow the connection → Next

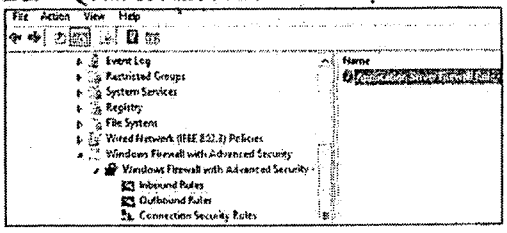


B17 - Màn hình Profile, bỏ dấu chọn ở ô Private và Public → Next

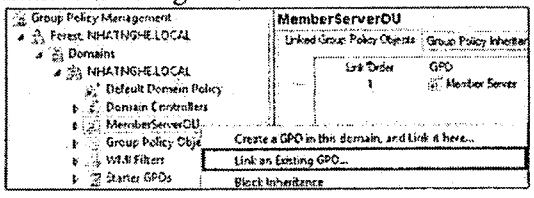


B18 - Màn hình Name, đặt tên Application Server Department Firewall Rule → Finish

B19 - Quan sát Inboud Rule vừa tạo.

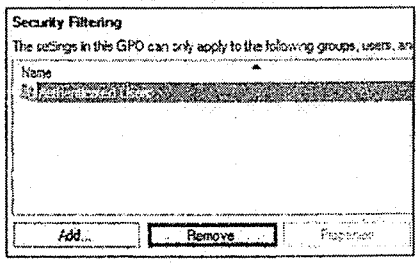


B20 - Chuột phải vào MemberServerOU → chọn Link an Existing GPO



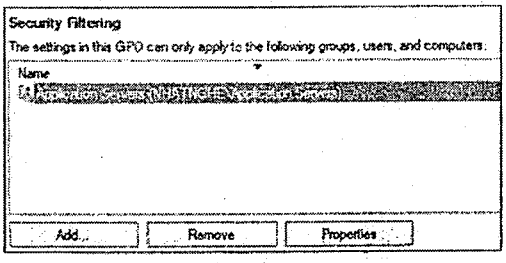
B21 - Chọn Application Servers GPO → OK

B22 - Ở khung Security Filtering ở góc cuối cùng bên phải → chọn Authenticated Users → Remove → OK → Add



B23 - Nhập vào Application Servers → OK

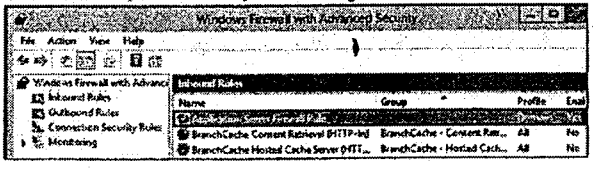
B24 – Quan sát group Application Servers đã được thêm vào



B25 - Kiểm tra: Qua máy PC03, mở CMD, gõ lệnh Gpupdate /force

B26 - Mở Server Manager, vào menu Tools → chọn Windows Firewall with Advanced Security

B27 - Quan sát thấy Application Server Firewall Rule đã được kích hoạt trên máy PC03



DISTRIBUTED FILE SYSTEM

CÁC BƯỚC TRIỂN KHAI

1. Cài Distributed File System role service trên các file server

2. Tạo NameSpace & chỉ định các NameSpace Server

3. Tạo Replication Group

4. Chỉ định Replicate và publish trong NameSpace

5. Thử nghiệm Failover

A- CHUẨN BỊ

Mô hình bài lab bao gồm 03 máy:

- PC01: Windows Server 2012 R2 - DC (Domain: NHATNGHE.LOCAL)

- PC03 và PC04: Windows Server 2012 R2 đã join domain, tạo thư mục DATA và share full thư mục DATA trên ổ C:

- PC05: Windows 8.1 Enterprise đã join domain.

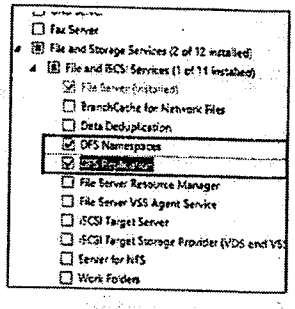
- Log on Domain Admin trên 3 máy PC01, PC03 và PC04

B- THỰC HIỆN

1. Cài Distributed File System role service trên PC03 và PC04

B1 - Mở Server Manager, vào menu Manage → Add Roles and Features.

B2 - Nhấn Next theo mặc định. Màn hình Server Roles → đánh dấu chọn vào 2 ô DFS Namespaces và DFS Replication → Next → Next



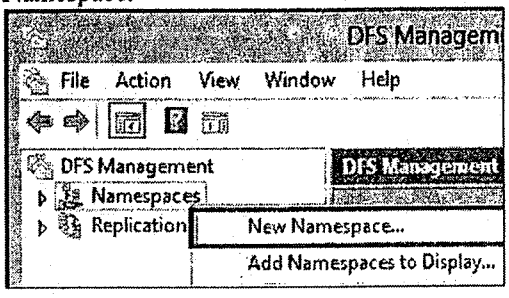
B3 - Màn hình Confirmation → đánh dấu chọn vào ô Restart the destination server automatically if required → Install → Close

2. Tạo NameSpace & chỉ định các NameSpace Server

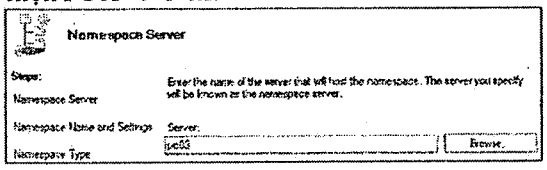
a. Tạo NameSpace HoSo (Thực hiện trên PC03)

B1 - Mở Server Manager, vào menu Tools → DFS Management

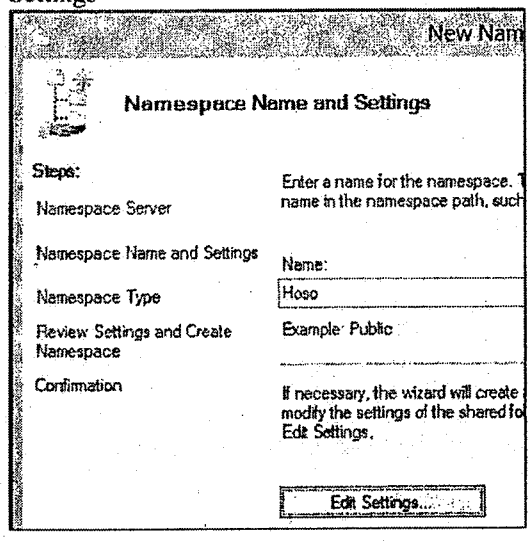
B2 - Chuột phải Namespaces → chọn New Namespace.



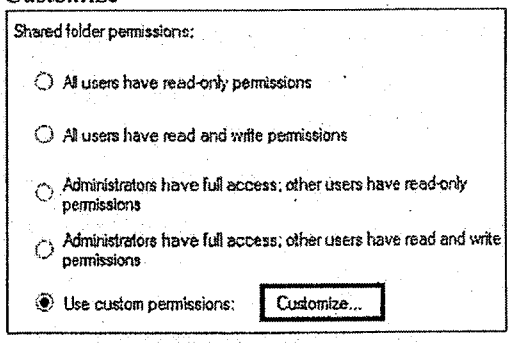
B3 - Màn hình Namespace Server → Browse → chọn PC03 → Next



B4 - Màn hình Namespace Name and Settings → Điền vào ô Name : HoSo → Chọn Edit Settings

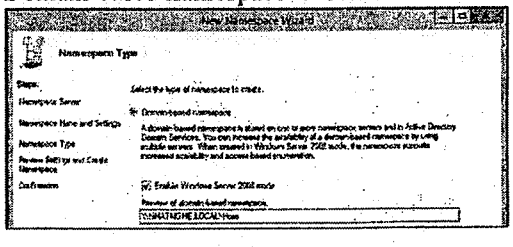


B5 - Chọn Use custom permissions → chọn Customize



B6 - Cho Group Everyone quyền Full Control → OK → OK → Next

B7 - Hộp thoại Namespace Type → Chọn Domain-based namespace → Next

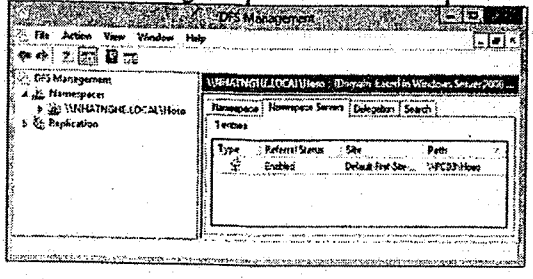


B8 - Hộp thoại Review Settings and Creat Namespace → Chọn Create

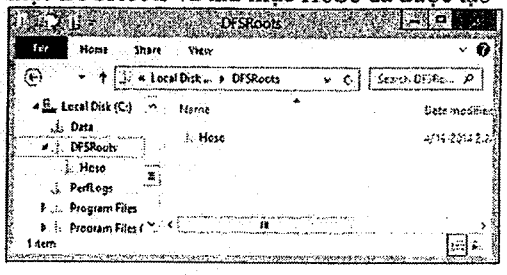
B9 - Hộp thoại Confirmation → Close

b. Kiểm tra kết quả trên PC03

B1 - Quan sát trong DFS, qua tab Namespace Servers → khung bên phải đã có Name Space

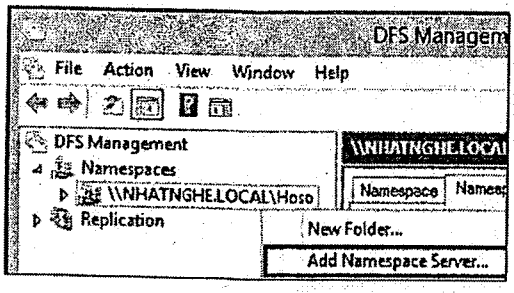


B2 - Mở Computer → Quan sát thấy có thư mục DFSRoots và thư mục HoSo đã được tạo

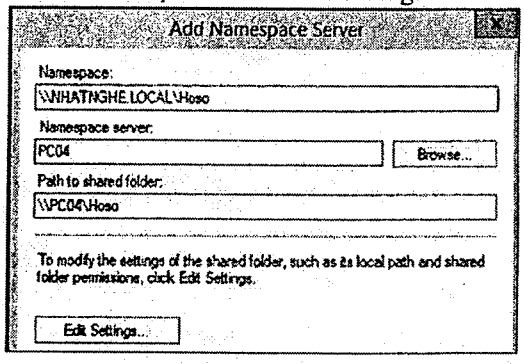


c. Tạo thêm NameSpace Server PC04 trên PC03

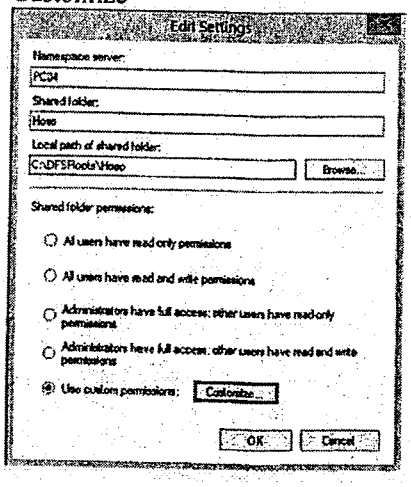
B1 - Mở DFS → Chuột phải \\NhatNghe.local\HoSo → Add Namespace Server



B2 - Hộp thoại Namespace Server → Chọn Browse → Chọn PC04 → Edit Settings

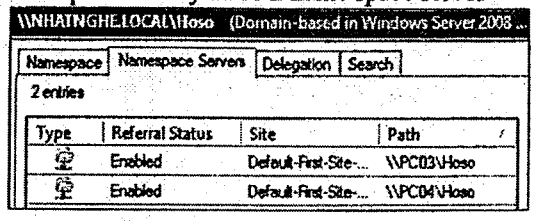


B3 - Chọn Use custom permissions → Customize



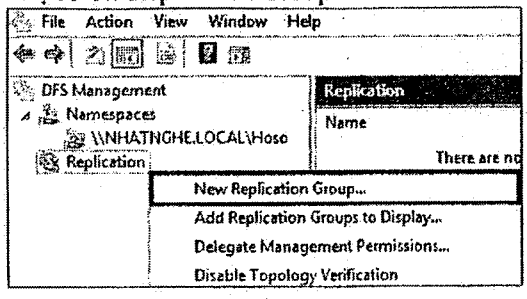
B4 - Cho Group Everyone quyền Full Control → OK → OK

B5 - Quan sát: Kiểm tra trên cả 2 server → Mở DFS quan sát thấy đã có 2 name space server

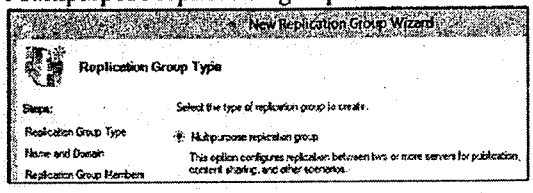


3. Tạo Replication Group (Thực hiện trên máy PC03)

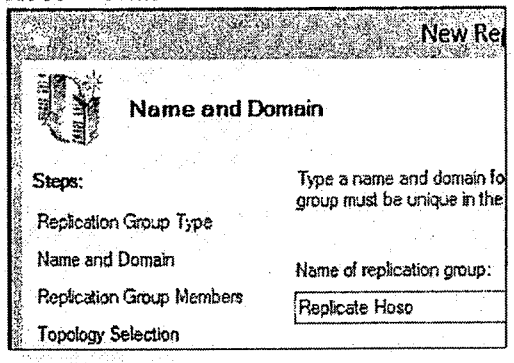
B1 - Chuột phải lên Replication Group → Chọn New Replication Group



B2 - Màn hình Replication Group Type → chọn Multipurpose replication group → Next

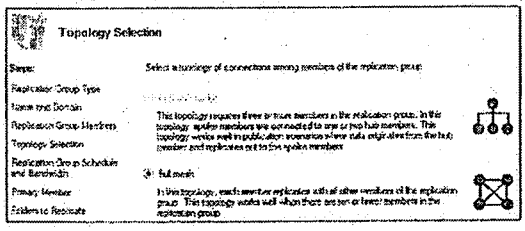


B3 - Đặt tên Replication group là: Replicate HoSo → Next

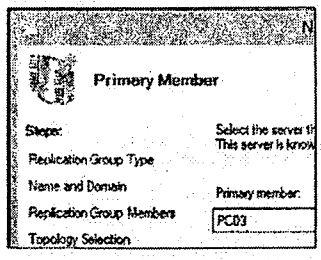


B4 - Màn hình Replication Group Members → Chọn Add → Chọn PC03, PC04 → OK → Next

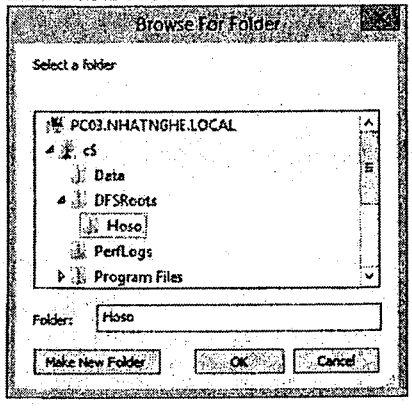
B5 - Màn hình Topology Selection → Chọn Full mesh → Next → Next



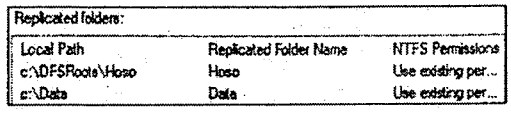
B6 - Màn hình Primary Member → Chọn PC03 → Next



B7 - Màn hình Folders to Replicate → Chọn Add → Browse → chọn thư mục DFSRoots\HoSo → OK → OK

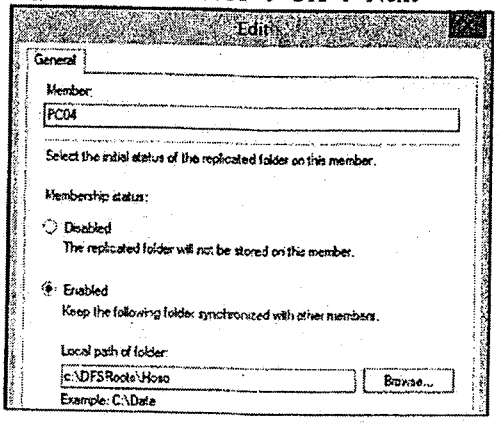


B8 - Thực hiện add tiếp thư mục C:\DATA → OK → OK → Next



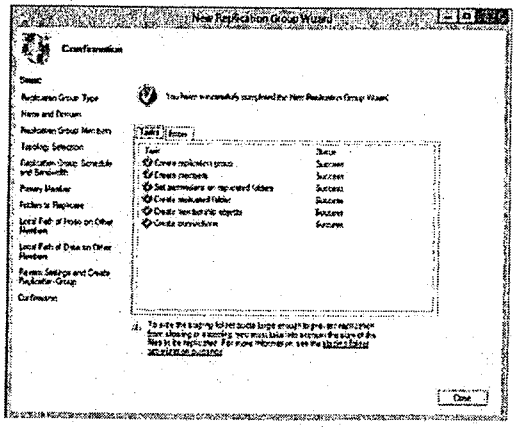
B9 - Màn hình Local Path of HoSo on Other Member → Chọn Edit

B10 - Chọn Enabled → Browse → chỉ đến thư mục: DFS Roots/Hoso → OK → Next



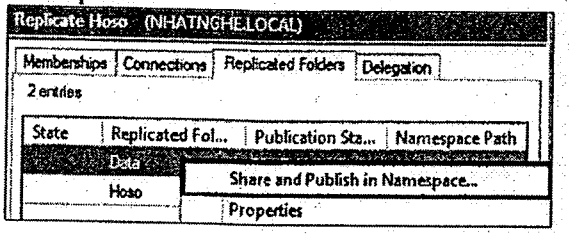
B11 - Màn hình Local Path of DATA on Other Member → Chọn Edit → Chọn Enabled → Browse → chỉ đến thư mục: C:\DATA → OK → Next

B12 - Màn hình Review Settings → Create → Close

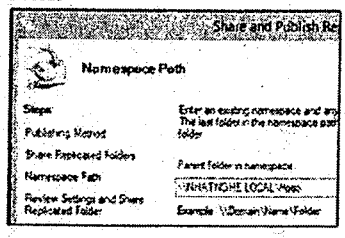


4. Chỉ định Replicate và Publish trong NameSpace

B1 - Ở khung bên trái chọn Replicate HOSO. Ở khung bên phải, chọn tab Replicated Folder → Chuột phải lên Data → Chọn Share and Publish in Namespace



B2 - Màn hình Namespace Path → Browse → chọn \\NHATNGHE.LOCAL\HoSo --> Next



B3 - Màn hình Review Settings → Share → Close

B4 - Thực hiện trên cả 2 member server (PC03 và PC04). Nhấn tổ hợp phím ⊞ + R, gõ Services.msc

B5 - Chuột phải DFS Replication, chọn Restart.

B6 - Kiểm tra: Trên máy PC05, truy cập \\Nhatnghe.Local\HoSo

B7 - Quan sát thấy có thư mục Data

B8 - Tạo 1 file bất kì trong thư mục HoSo và thư mục Data

B9 - Mở thư mục HoSo và Data của cả 2 máy PC03 và PC04 → kiểm tra trong thư mục HoSo đều có file được tạo từ máy Client

5. Thử nghiệm Failover

- PC05 truy cập: \\Nhatnghe.local\HoSo, tạo các file WordPad BaoCaoKeToan & TuyenDung
- Tắt PC03. PC05 truy cập: \\Nhatnghe.local\HoSo, tạo file Kiemtra.txt
- Bật PC03, tắt PC04. PC05 truy cập: \\Nhatnghelocal\HoSo, tạo file Kiemtra2.txt
- Bật PC04. PC05 truy cập: \\Nhatnghe.local\HoSo, truy cập được đủ 4 file đã tạo.

BITLOCKER

CÁC BƯỚC TRIỂN KHAI

1. Triển khai BitLocker bằng Group Policy

2. Kích hoạt BitLocker cho ổ đĩa

3. Di chuyển ổ đĩa sang máy khác và kiểm tra

A- CHUẨN BỊ

Mô hình bài lab bao gồm 2 máy

+ PC01: Windows Server 2012 R2 DC (Domain: NHATNGHE.LOCAL).

+ PC03: Windows Server 2012 (đã join domain). Trên máy PC03 phải có ít nhất 2 ổ cứng và được định dạng là NTFS.

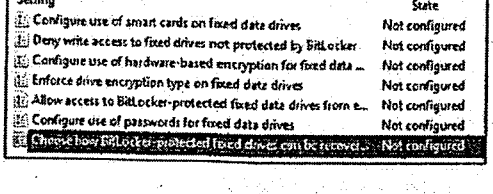
B- THỰC HIỆN

1. Triển khai BitLocker bằng Group Policy (Thực hiện trên máy PC01)

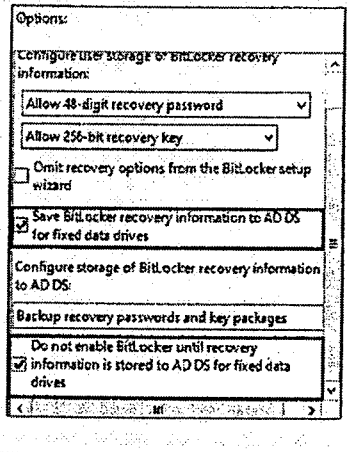
B1 - Mở Server Manager → menu Tools → chọn Group Policy Management

B2 - Mở theo đường dẫn: Forest: NHATNGHE.LOCAL → Domains → NHATNGHE.LOCAL, Chuột phải Default Domain Policy → chọn Edit

B3 - Mở theo đường dẫn: Computer Configuration → Policies → Administrative Templates → Windows Components → BitLocker Drive Encryption → Fixed Data Drives → nhấn double click vào policy: Choose how BitLocker-protected fixed drives can be recovered setting.



B4 - Chọn Enabled → Đánh dấu chọn vào 2 ô: Save BitLocker recovery information to AD DS for fixed data drives và ô Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives → OK

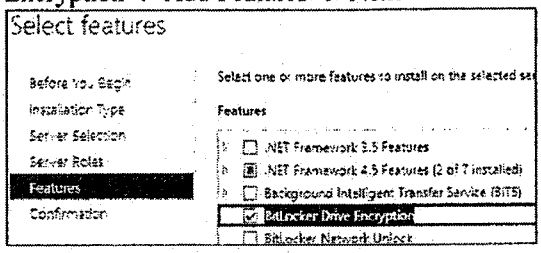


B5 - Qua máy PC03, log on NHATNGHE\Administrator. Mở CMD, gõ lệnh Gpupdate /Force. Sau đó Restart lại máy PC03

2. Kích hoạt BitLocker cho ổ đĩa (Thực hiện trên máy PC03)

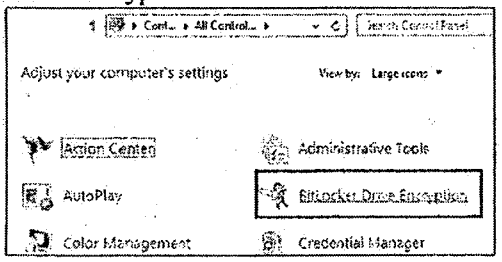
B1 - Mở Server Manager → menu Manage → chọn Add Roles and Features

B2 - Nhấn Next theo mặc định. Màn hình Features → đánh dấu chọn vào ô BitLocker Drive Encryption → Add Features → Next

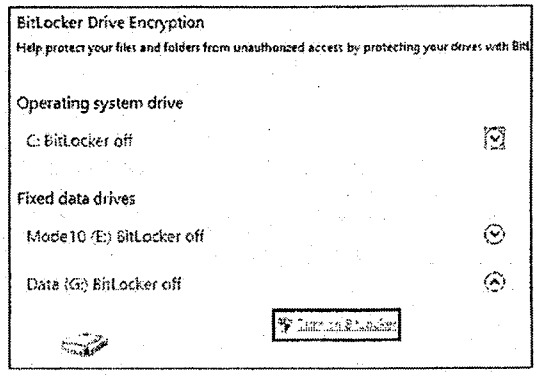


B3 - Màn hình Confirmation → đánh dấu chọn vào ô Restart the destination server automatically if required → Install → Close

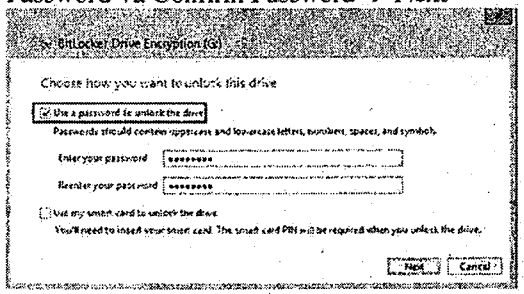
B4 - Mở Control Panel → chọn BitLocker Drive Encryption



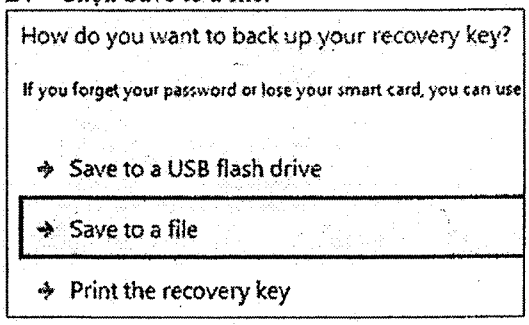
B5 - Chọn ổ đĩa muốn bảo mật → Nhấn Turn on BitLocker.



B6 - Đánh dấu chọn vào ô Use a password to unlock the drive → Nhập vào mật khẩu ở 2 ô Password và Confirm Password → Next

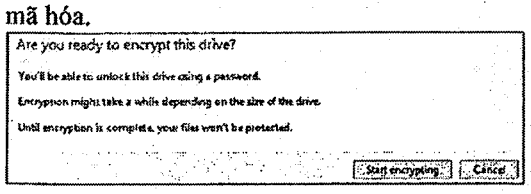


B7 - Chọn Save to a file.

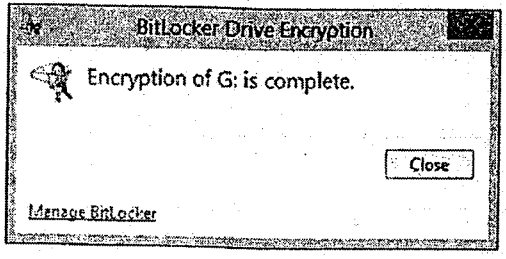


B8 - Trỏ đường dẫn đến nơi lưu khóa giải mã → Save → Yes

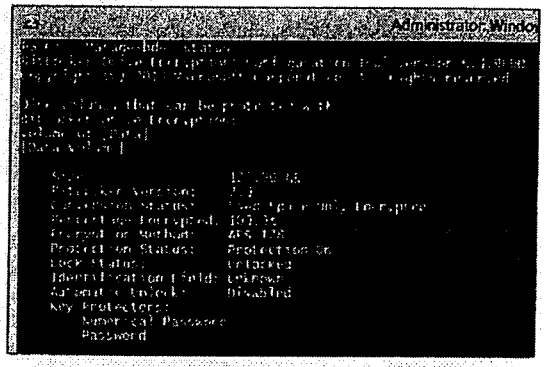
B9 - Nhấn vào nút Start encrypting để bắt đầu mã hóa.



B10 - Sau khi mã hóa thành công → nhấn Close.



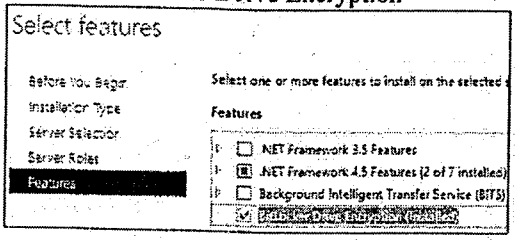
B11 - Mở Windows PowerShell, gõ lệnh Manage-bde –status. Quan sát thấy ổ đĩa được bảo vệ bằng BitLocker, dòng Protection Status hiển thị Protection On.



3. Di chuyển ổ đĩa sang máy khác và kiểm tra

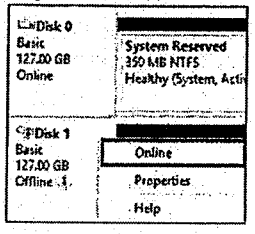
B1 - Gỡ bỏ ổ cứng bảo mật trên máy PC03 và gắn vào máy PC01.

B2 - Trên máy PC01, mở Server Manager → cài Features BitLocker Drive Encryption

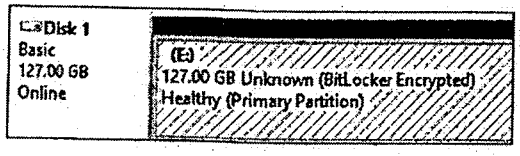


B3 - Nhấn tổ hợp phím ⊞ + R, gõ lệnh diskmgmt.msc

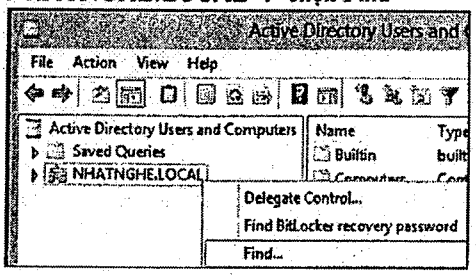
B4 - Chuột phải vào đĩa mới được gắn vào → chọn Online



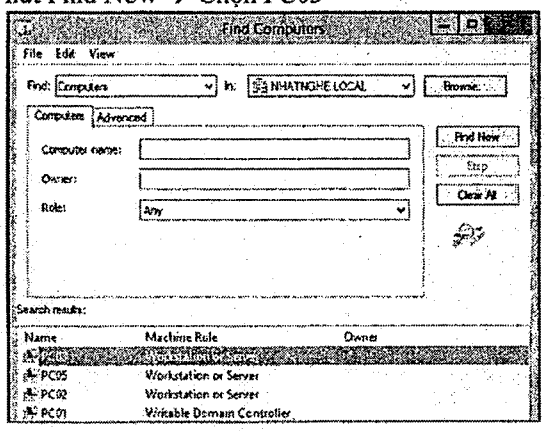
B5 - Quan sát thấy ổ đĩa vẫn được bảo vệ bằng BitLocker



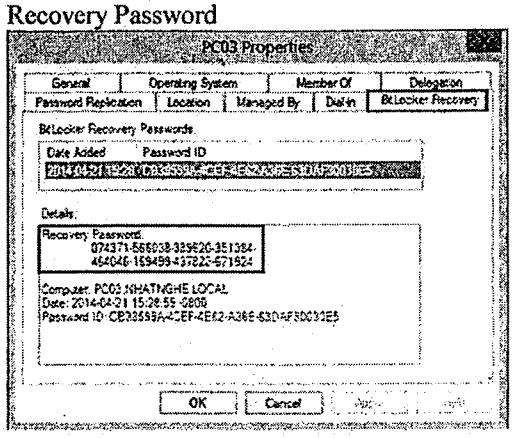
B6 - Mở Active Directory Users and Computers → Chuột phải vào NHATNGHE.LOCAL → chọn Find



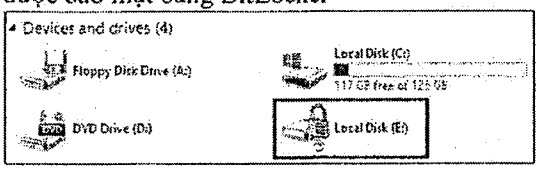
B7 - Ở mục Find → chọn Computers → nhấn nút Find Now → Chọn PC03



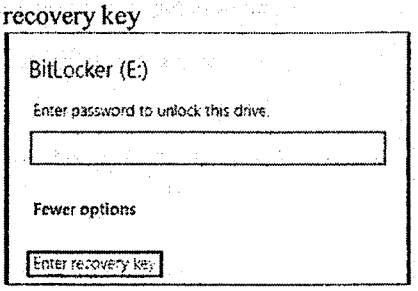
B8 - Qua tab BitLocker Recovery → Ở khung Details, copy toàn bộ nội dung ở dòng Recovery Password



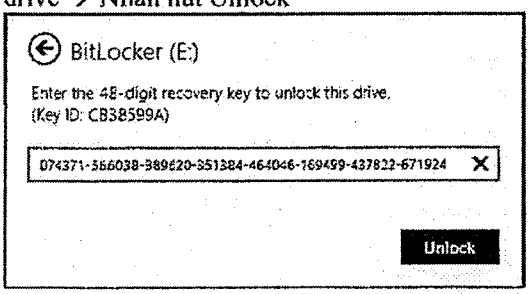
B9 - Mở File Explorer, double click vào ổ đĩa được bảo mật bằng BitLocker



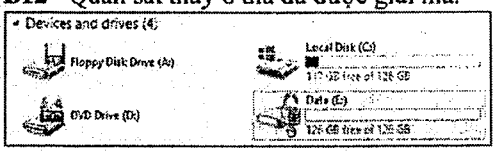
B10 - Chọn More options → Nhấn Enter recovery key



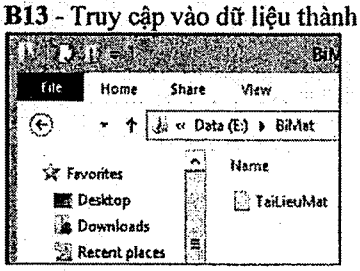
B11 - Dán toàn bộ nội dung vừa copy vào khung Enter the 48-digit recovery key to unlock this drive → Nhấn nút Unlock



B12 - Quan sát thấy ổ đĩa đã được giải mã.



B13 - Truy cập vào dữ liệu thành công.



FILE SERVER RESOURCE MANAGER

CÁC BƯỚC TRIỂN KHAI

1. Cài đặt File Server Resource Mananger

2. Tạo giới hạn 5MB

3. Cấm sao chép tất cả các file trừ file *.exe vào thư mục BaoCao

4. Kiểm tra

A- CHUẨN BỊ

- Mô hình bài lab gồm 2 máy :

+ PC01: Ghost Windows Server 2012 R2

+ PC02: Ghost Windows Server 2012 R2

- PC01: Tạo thư mục C:\BaoCao, Share: Full Control

- PC01: Tạo user U1/123

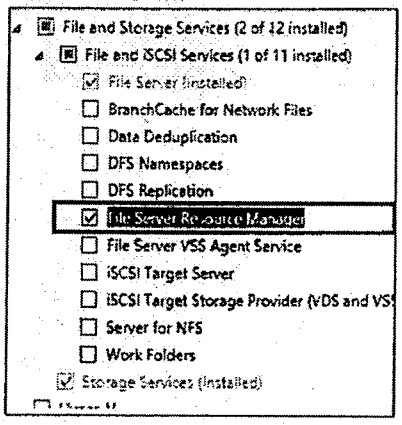
- PC02: Đổi password Administrator thành 123

B- THỰC HIỆN

1. Cài đặt File Server Resource Manager (Thực hiện trên PC01)

B1 - Mở Server Manager → menu Manage → chọn Add Roles and Features

B2 - Các bước đầu tiên nhấn Next theo mặc định. Màn hình Server Roles → đánh dấu chọn vào ô File Server Resource Manager → Add Features → Next → Next

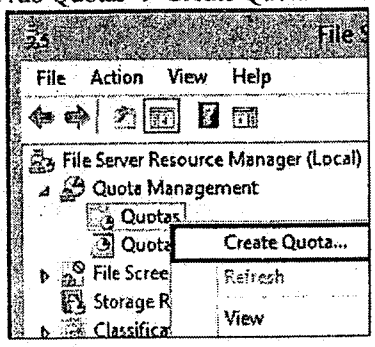


B3 - Màn hình Confirmation → Đánh dấu chọn vào ô Restart the destination server automatically if required → Install → Close

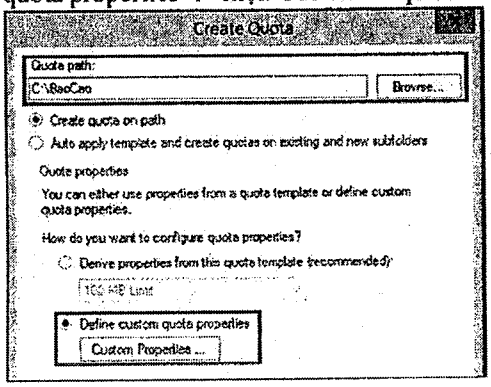
2. Tạo giới hạn 5MB

B1 - Sau khi cài đặt xong, vào menu Tools → chọn File Server Resource Manager

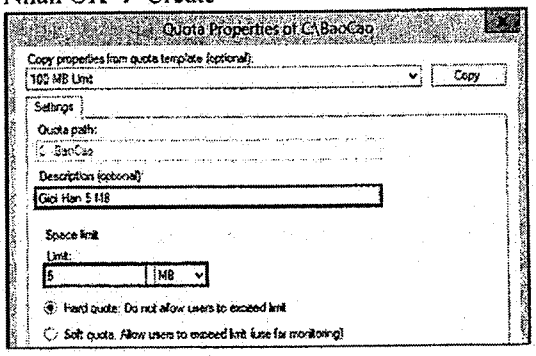
B2 - Bung mục Quota Management, chuột phải vào Quotas → Create Quota



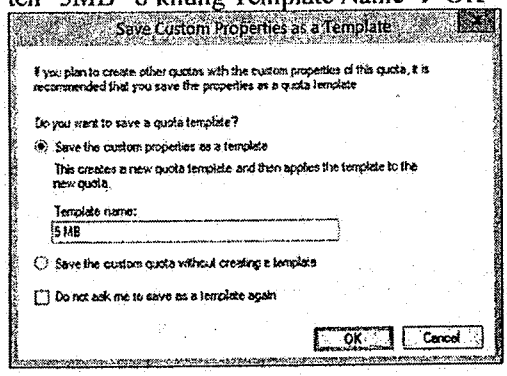
B3 - Mục Quota path, Browse đến đường dẫn C:\BaoCao. Bên dưới chọn Define custom quota properties → chọn Custom Properties…



B4 - Trong hộp thoại Quota Properties
+ Mục Label: đặt tên Giới hạn 5 MB
+ Mục Limit: 5 MB
Nhấn OK → Create

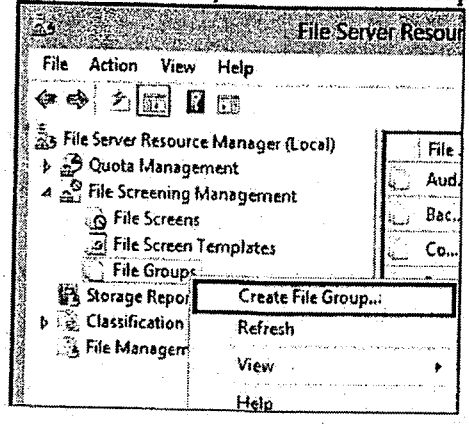


B5 - Hộp thoại yêu cầu Save Template, đặt tên "5MB" ở khung Template Name → OK

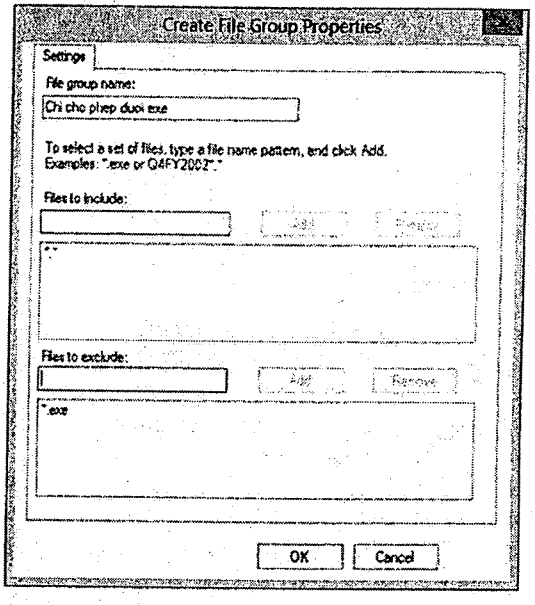


3. Cấm sao chép tất cả các file trừ file *.exe vào thư mục BaoCao

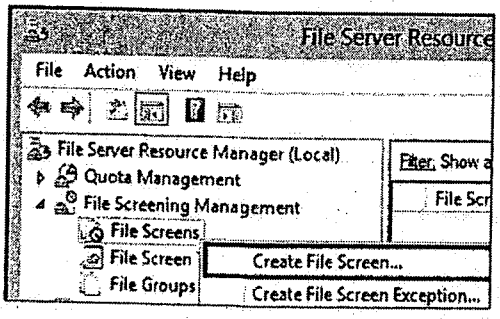
B1 - Mở File Server Resource Manager → Bung mục File Screening Management, chuột phải vào File Groups → Create File Group…



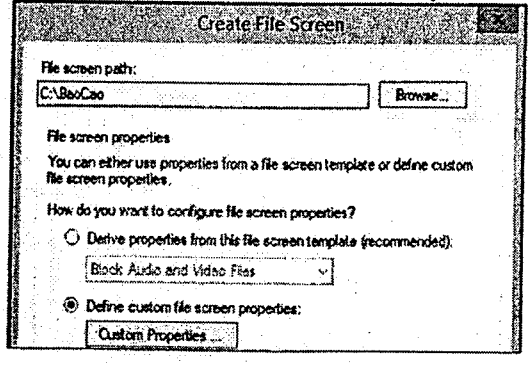
B2 - Trong hộp thoại Create File Group
+ File Group Name: Chỉ cho phép đuôi exe
+ Files to include: nhập *.*
+ Files to exclude: nhập *.exe
Nhấn OK



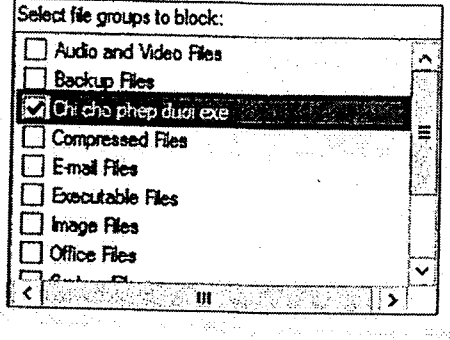
B3 - Chuột phải vào File Screens → Create File Screen…



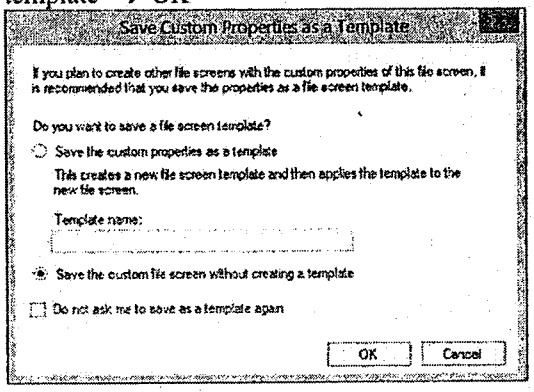
B4 - Mục File screen path, Browse đến đường dẫn C:\BaoCao. Bên dưới chọn Define custom file screen properties, chọn Custom Properties…



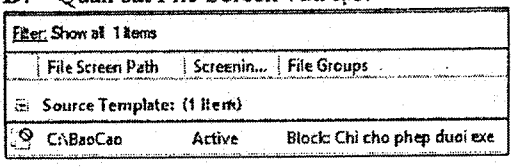
B5 - Ở mục File Groups, đánh dấu chọn vào ô "Chỉ cho phép đuôi exe" → OK → Create



B6 - Hộp thoại yêu cầu Save Template, chọn "Save the custom file screen without creating a template" → OK



B7 - Quan sát File Screen vừa tạo.

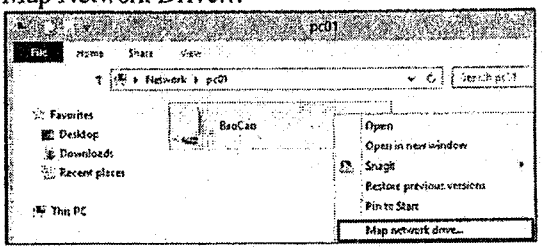


4. Kiểm tra

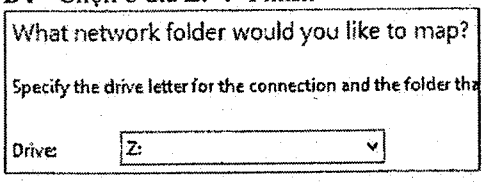
B1 - Log on Administrator ở máy PC02. Nhấn tổ hợp phím ⊞ + R, gõ \\PC01

B2 - Hộp thoại yêu cầu xác thực quyền, nhập vào u1 và password 123

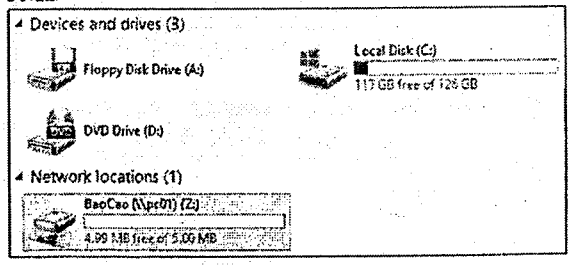
B3 - Chuột phải vào thư mục BAO CAO → chọn Map Network Drive…



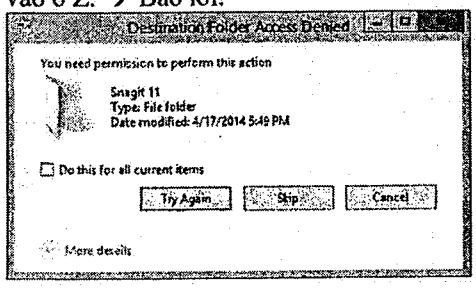
B4 - Chọn ổ đĩa Z: → Finish



B5 - Quan sát ổ đĩa Z:, tổng cộng dung lượng là 5MB



B6 - Copy thử tập tin hoặc thư mục bất kỳ vào ổ Z: → Báo lỗi.



B7 - Chép thử file *.exe vào ổ Z: → Copy thành công.

WORK FOLDERS

CÁC BƯỚC TRIỂN KHAI

1. Cài đặt Role Work Folders
2. Tạo Sync Share
3. Enable SMB Access
4. Tạo GPO phân quyền Domain Users làm Local Administrator trên các máy Client
5. Tạo GPO tự động cấu hình WorkFolders
6. Tạo GPO tự động chạy Script trên các máy Client
7. Kiểm tra

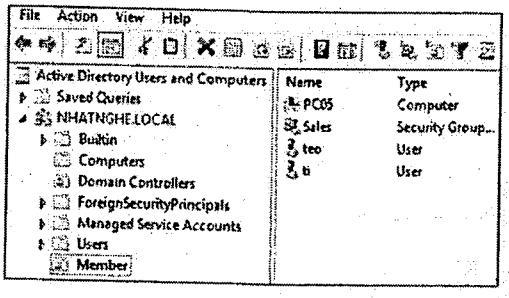
A- CHUẨN BỊ

Mô hình bài lab bao gồm 2 máy:

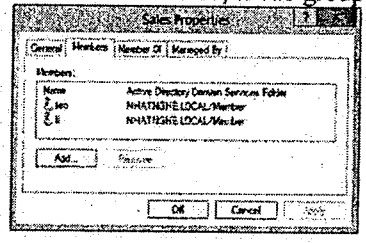
+ PC01: Windows Server 2012 R2 DC (Domain: NHATNGHE.LOCAL)

+ PC05: Windows 8 Enterprise 8.1 đã join domain

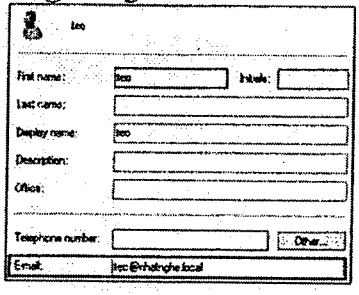
B1 - Trên PC01, tạo OU Member. Move PC05 vào OU Member. Tạo user teo, ti và group Sales.



B2 - Add 2 user teo, ti vào group Sales



B3 - Chuột phải user Teo, chọn Properties. Tab General → Mục Email, điền vào teo@nhatnghe.local



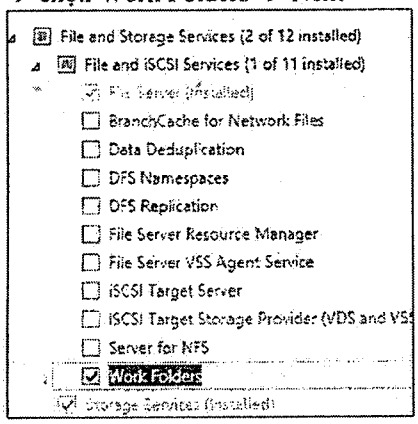
B4 - Thực hiện tương tự khai báo email cho user Ti

B- THỰC HIỆN

1. Cài đặt Role Work Folders (Thực hiện trên PC01)

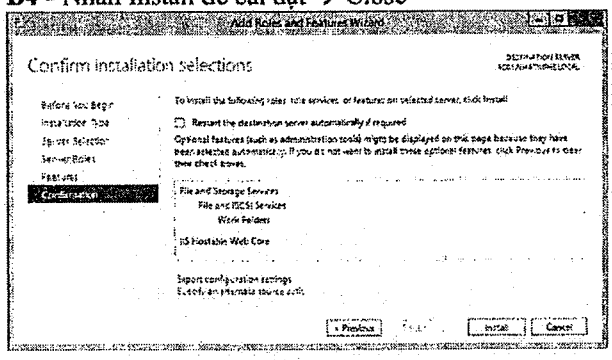
B1 - Mở Server Manager → menu Manage → chọn Add Roles and Features

B2 - Các bước đầu tiên nhấn Next theo mặc định. Màn hình Select Server Roles → chọn Work Folders → Next



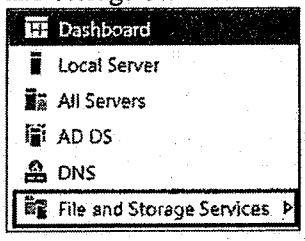
B3 - Chọn Add Features → Next

B4 - Nhấn Install để cài đặt → Close

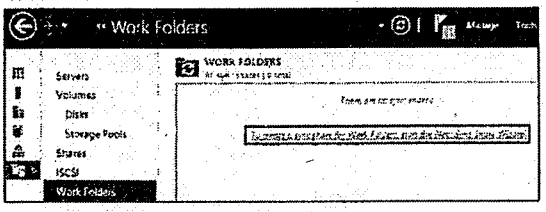


2. Tạo Sync Share (Thực hiện trên PC01)

B1 - Quay lại Server Manager → chọn File and Storage Services

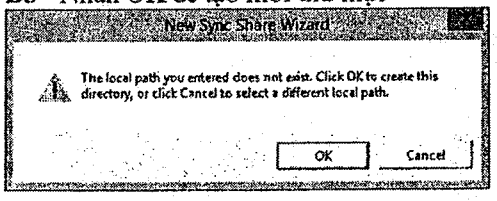


B2 - Chọn Work Folders → To create a sync share for Work Folders, start the New Sync Share Wizard.

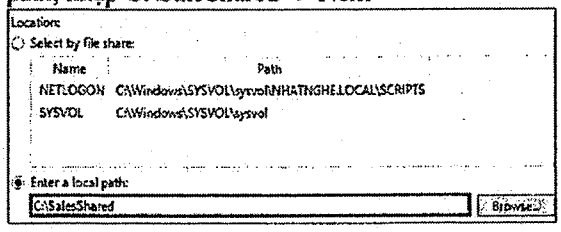


B3 - Màn hình Before you begin → Next

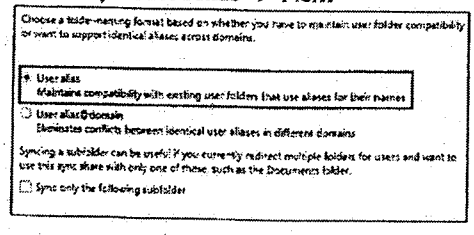
B5 - Nhấn OK để tạo mới thư mục



B4 - Màn hình Server and path → Enter a local path, nhập C:\SaleShared → Next

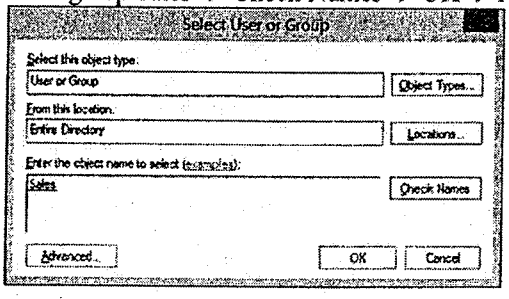


B6 - Chọn User Alias → Next

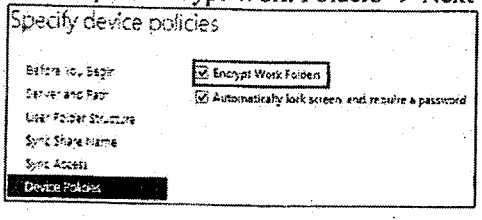


B7 - Màn hình Sync Share Name → giữ nguyên như mặc định → Next

B8 - Màn hình Sync Access → nhấn Add → Chọn thêm group Sales → Check Names → OK → Next

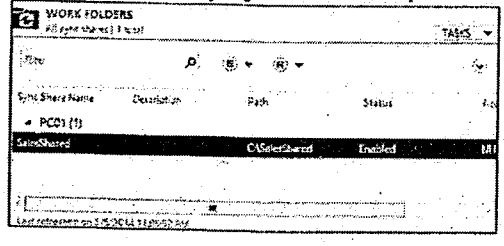


B9 - Chọn ô Encrypt Work Folders → Next



B10 - Màn hình Confirmation → Create → Close

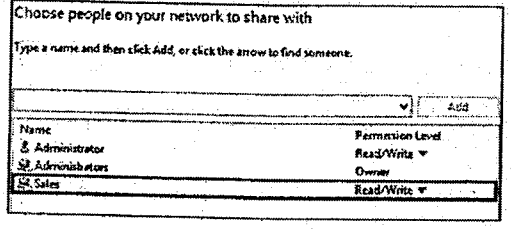
B11 - Quan sát thấy SyncShare vừa tạo.



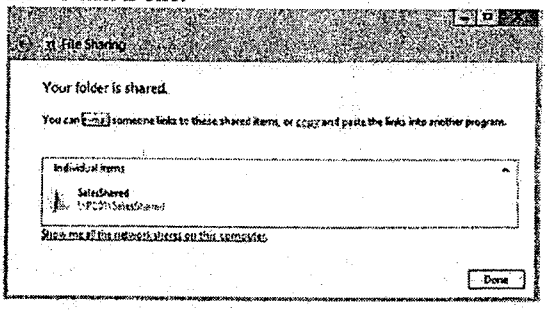
3. Enable SMB Access (Thực hiện trên máy PC01)

B1 - Mở File Explorer → Chuột phải vào C:\SaleShared → Share with → Specific people

B2 - Add group Sales → Phân quyền Read/Write → Share → Done



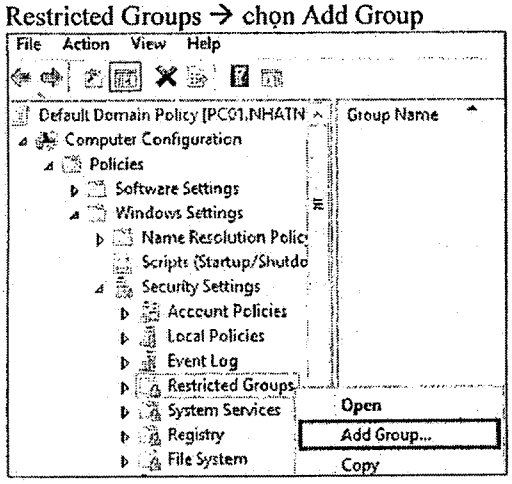
B3 - Nhấn Done.



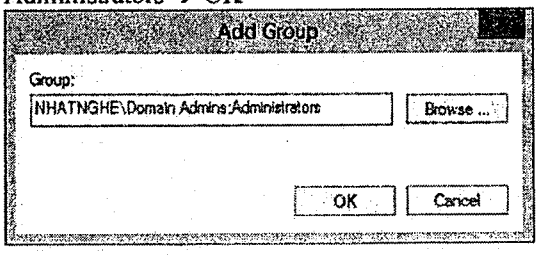
4. Tạo GPO phân quyền Domain Users làm Local Administrator trên các máy Client (Thực hiện trên máy PC01)

B1 - Mở Group Policy Management → Chuột phải vào Default Domain Policy → chọn Edit

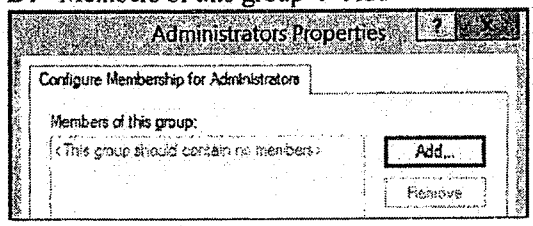
B2 - Bung theo đường dẫn: Computer Configuration → Policies → Windows Settings → Security Settings. Chuột phải vào Restricted Groups → chọn Add Group



B3 - Nhấn Browse, nhập vào Domain Admins và Administrators → OK

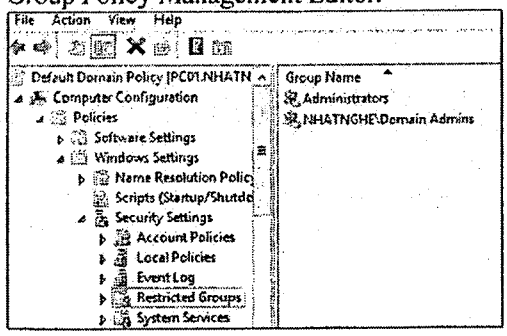


B4 - Members of this group → Add

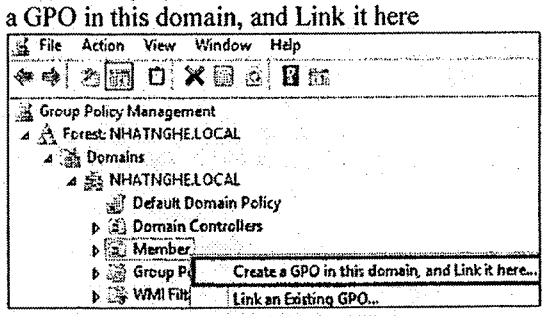


B5 - Nhập vào group Sales → Check Names → OK 3 lần

B6 - Quan sát thấy group Sales đã được thêm vào nhóm Administrators → Đóng cửa sổ Group Policy Management Editor.

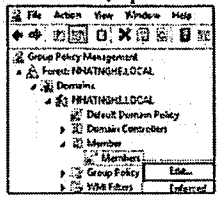


B7 - Chuột phải vào OU Member → chọn Create a GPO in this domain, and Link it here

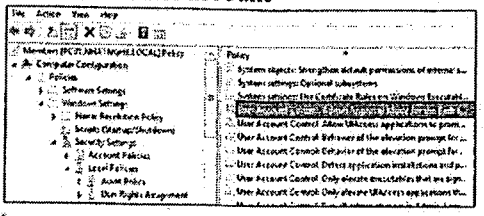


B8 - Ở mục Name, đặt tên Members → OK

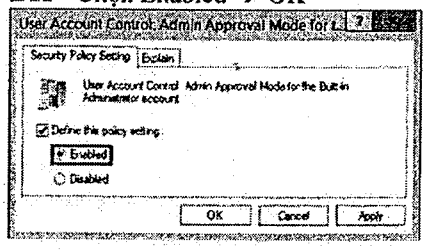
B9 - Chuột phải vào GPO Members → chọn Edit



B10 - Mở theo đường dẫn Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options, khung bên phải nhấn double click vào mục User Account Control: Admin Approval Mode for the Built-in Administrator account



B11 - Chọn Enabled → OK

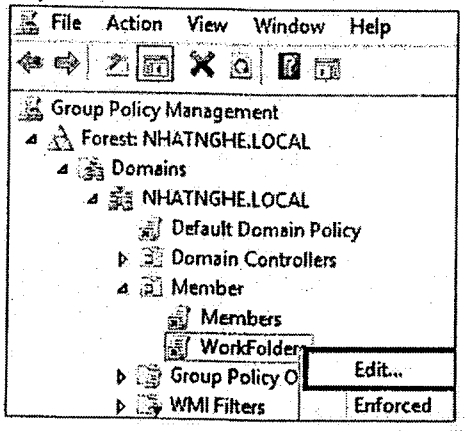


B12 - Mở CMD, gõ lệnh Gpupdate /Force

5. Tạo GPO tự động cấu hình WorkFolders (Thực hiện trên máy PC01)

B1 – Quay lại Group Policy Management. Chuột phải vào OU Member → chọn Create a GPO in this domain, and Link it here

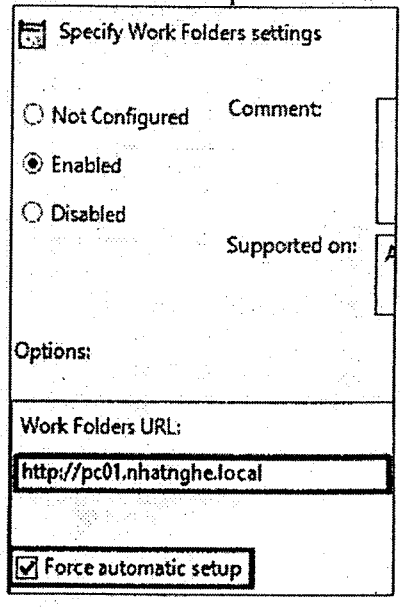
B3 - Chuột phải vào GPO WorkFolders → chọn Edit



B4 - Mở theo đường dẫn: User Configuration → Policies → Administrative Templates → Windows Components → Work Folders, nhấn double click vào mục Specify Work Folders settings

B2 - Ở mục Name, đặt tên WorkFolders → OK

B5 - Chọn Enabled. Ở mục Work Folders URL, nhập vào: http://pc01.nhatnghe.local → Chọn ô Force automatic setup → OK



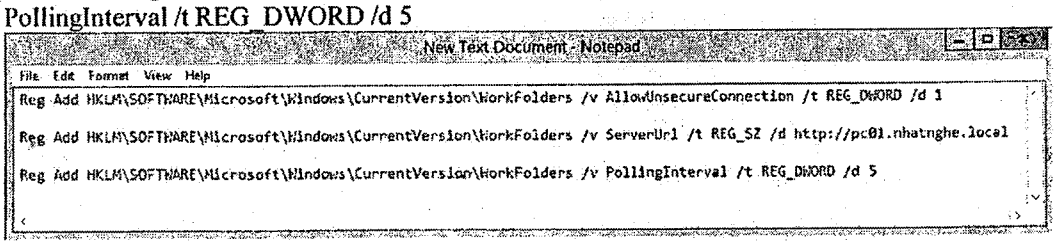
6. Tạo GPO tự động chạy Script trên các máy Client (Thực hiện trên PC01)

B1 - Mở Notepad, lần lượt nhập 3 lệnh sau:

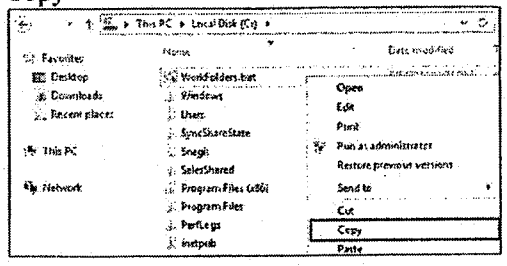
+ Lệnh 1: Reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WorkFolders /v AllowUnsecureConnection /t REG_DWORD /d 1

+ Lệnh 2: Reg add HKLM\Software\Microsoft\Windows\CurrentVersion\WorkFolders /v ServerUrl /t REG_SZ /d http://pc01.nhatnghe.local

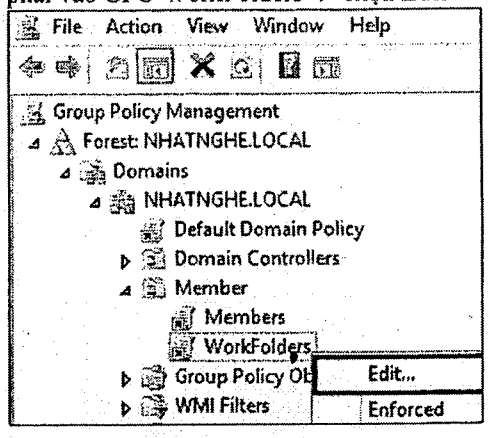
+ Lệnh 3: Reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WorkFolders /v PollingInterval /t REG_DWORD /d 5



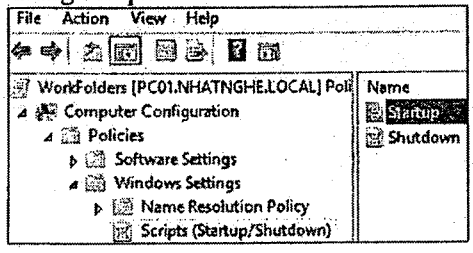
B2 - Lưu lại thành file WorkFolders.bat. Chuột phải vào file WorkFolders.bat → chọn Copy



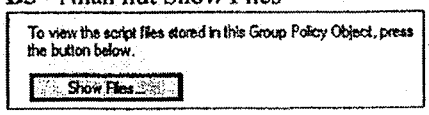
B3 – Quay lại Group Policy Management. Chuột phải vào GPO WorkFolders → chọn Edit



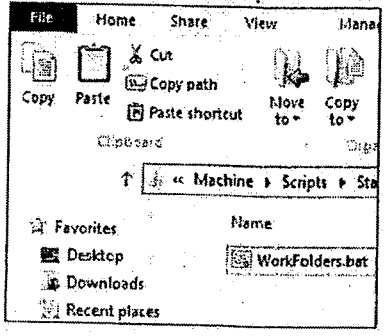
B4 - Mở theo đường dẫn: Computer Configuration → Policies → Windows Settings → Scripts (Startup/Shutdown), khung bên phải nhấn double click vào Startup



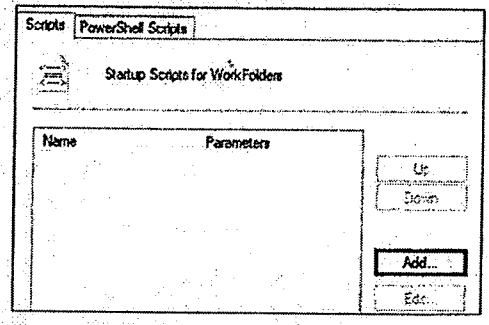
B5 - Nhấn nút Show Files



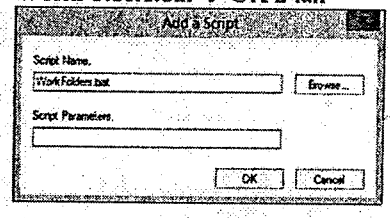
B6 - Chuột phải chọn Paste. Quan sát thấy file WorkFolders.bat đã được dán vào.



B7 - Nhấn nút Add



B8 - Nhấn nút Browse và trỏ đường dẫn đến file WorkFolders.bat → OK 2 lần

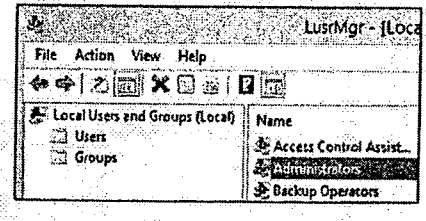


B9 - Mở CMD, gõ lệnh Gpupdate /Force

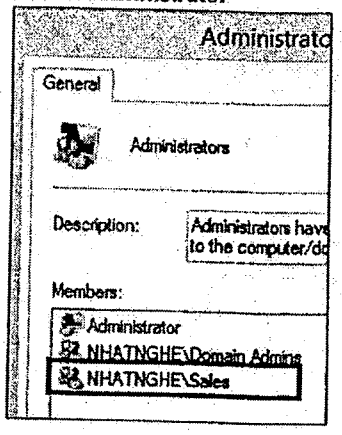
7. Kiểm tra (Thực hiện trên máy PC05)

B1 - Log on user Ti, nhấn tổ hợp phím ⊞ + R, gõ lệnh LusrMgr.msc → OK

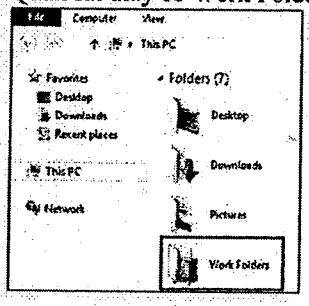
B2 - Ở khung bên trái, chọn Groups → Double click vào Administrators



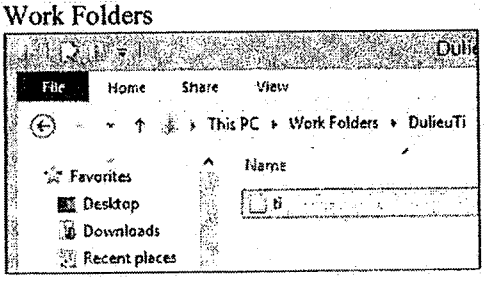
B3 - Quan sát thấy Group Sales nằm trong Local Administrator



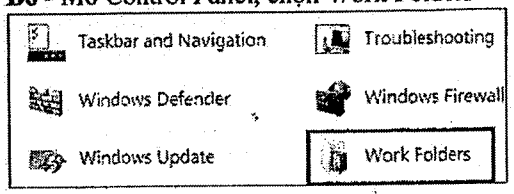
B4 - Mở File Explorer → nhấn vào This PC → Quan sát thấy có Work Folders



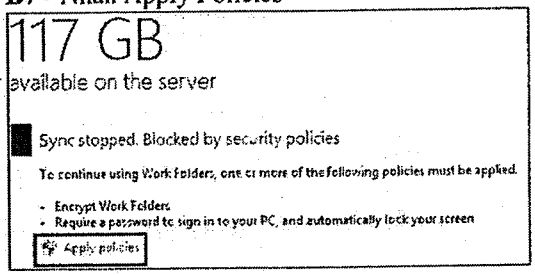
B5 - Mở Notepad, tạo file ti.txt và lưu vào Work Folders



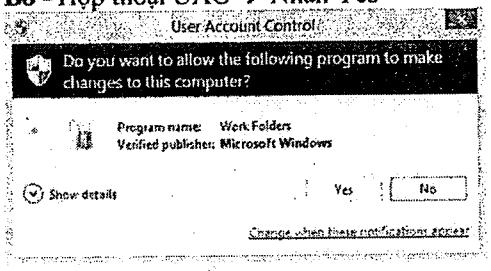
B6 - Mở Control Panel, chọn Work Folders



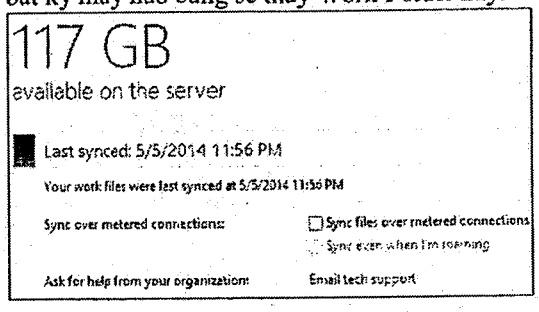
B7 - Nhấn Apply Policies



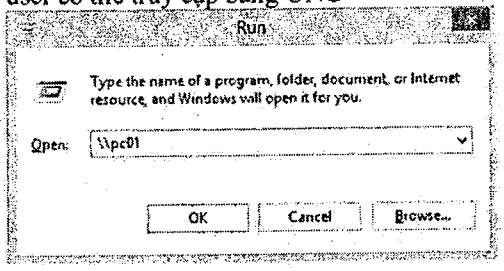
B8 - Hộp thoại UAC → Nhấn Yes



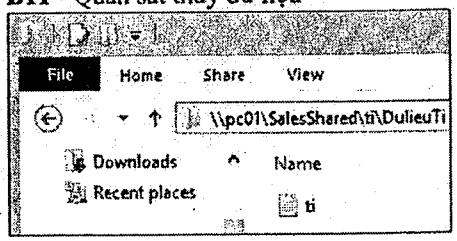
B9 - Dữ liệu được đồng bộ hóa. User Ti ngồi ở bất kỳ máy nào cũng sẽ thấy Work Folder này.



B10 - Ngoài ra, do SMB được enabled nên user có thể truy cập bằng UNC



B11 - Quan sát thấy dữ liệu



PRINTER

CÁC BƯỚC TRIỂN KHAI

1. Local Printer
2. Network Printer
3. Map Printer
4. Phân quyền
5. Printer pooling
6. Available Time
7. Spool folder
8. Priority
9. Additional Driver
10. Deploy Printer

A- CHUẨN BỊ

- Mô hình bài lab bao gồm 2 máy

+ PC01: Windows Server 2012 R2 DC (Domain: NHATNGHE.LOCAL)

+ PC02: Windows Server 2012 R2 – Join Domain

- Trên máy PC01

+ Tạo 3 user: KT1, NS1, U1. Tạo 2 group: KeToan và NhanSu

+ Add user KT1 vào group KeToan, add user NS1 vào group NhanSu

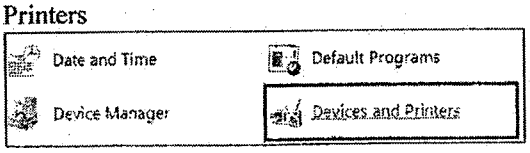
+ Chỉnh Policy Log on Locally: cho phép group Users có quyền log on vào PC01

+ Giả sử đã có 1 máy in HP có IP 192.168.7.150

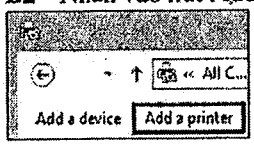
B- THỰC HIỆN

1. Local Printer (Thực hiện trên máy PC01)

B1 - Mở Control Panel → chọn Devices and Printers

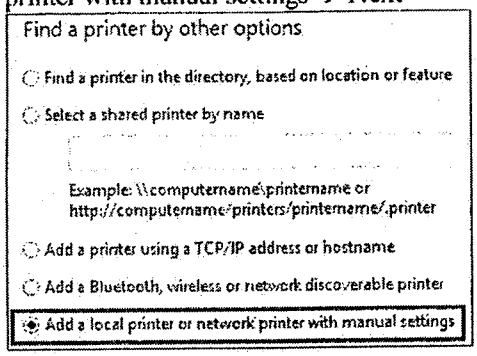


B2 - Nhấn vào nút Add a Printer.



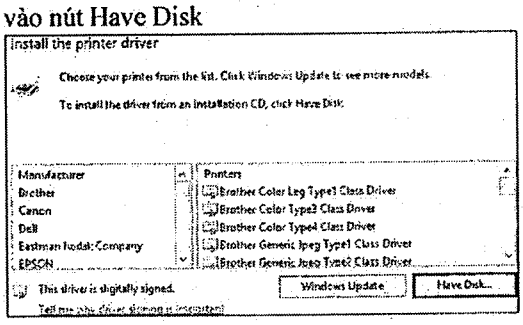
B3 - Màn hình Add Printer → Next

B4 - Chọn Add a local printer or network printer with manual settings → Next



B5 - Màn hình Choose a printer port, giữ nguyên như mặc định → Next

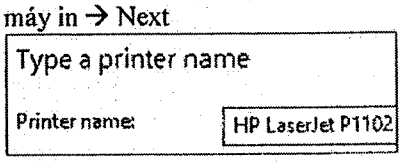
B6 - Màn hình Install the printer driver → nhấn vào nút Have Disk



B7 - Nhấn vào nút Browse → trỏ đường dẫn đến thư mục driver của máy in → OK

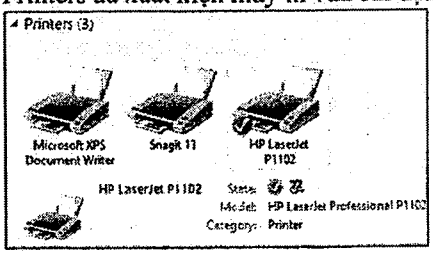
B8 - Chọn đúng model máy in của mình → Next

B9 - Màn hình Type a printer name, đặt tên cho máy in → Next



B10 - Màn hình Printer Sharing, giữ nguyên mặc định Share this printer so that others on your network can find and use it → Next

B11 - Nhấn Finish → Quan sát trong phần Printers đã xuất hiện máy in vừa cài đặt.

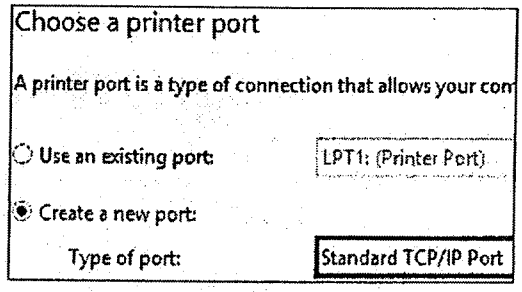


2. Network Printer (Thực hiện tại máy PC01)

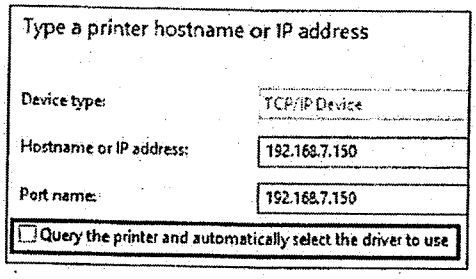
B1 - Mở Control Panel → Devices and Printers → nhấn Add a Printer → Next

B2 - Chọn Add a local printer or network printer with manual settings → Next

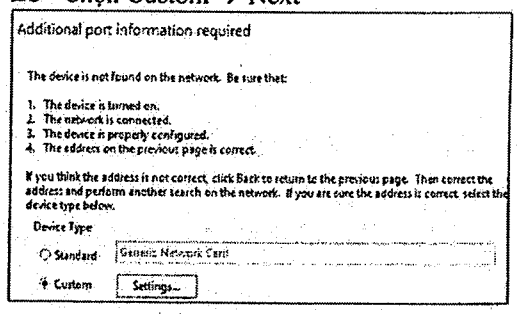
B3 - Màn hình Choose a printer port → Chọn Create a new port → Chọn dạng Standard TCP/IP Port → Next



B4 - Khai báo các thông số sau
+ Hostname or IP address: 192.168.7.150
+ Port name: 192.168.7.150
+ Bỏ dấu chọn trước dòng Query the printer and automatically select the driver to use → Next



B5 - Chọn Custom → Next

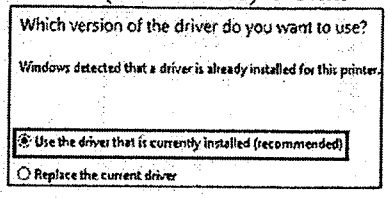


B6 - Màn hình Install the printer driver → nhấn vào nút Have Disk

B7 - Nhấn vào nút Browse → trỏ đường dẫn đến thư mục driver của máy in → OK

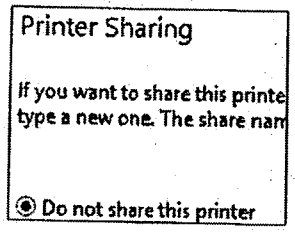
B8 - Chọn model máy in của mình → Next

B9 - Chọn Use the driver that is currently installed (recommened) → Next

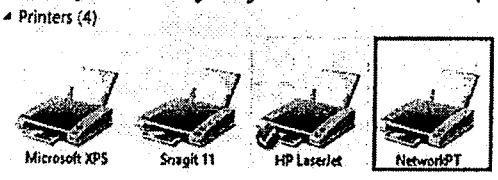


B10 - Trong mục Printer name → điền vào: NetworkPT → Next

B11 - Chọn Do not share this printer → Next → Finish



B10 - Quan sát thấy máy in NetworkPT vừa tạo.

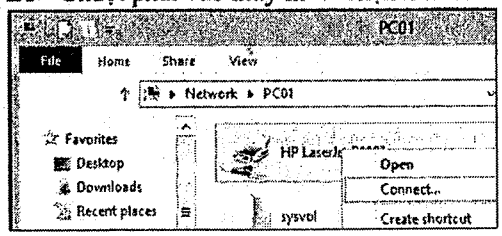


3. Map Printer

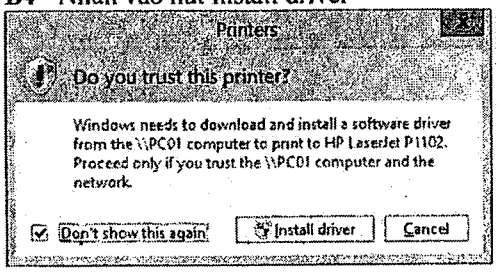
B1 - Trên PC01, xóa máy in NetworkPT

B2 - Qua máy PC02, log on Administrator → Truy cập vào máy PC01.

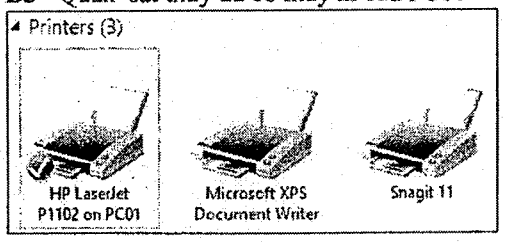
B3 - Chuột phải vào máy in → chọn Connect



B4 - Nhấn vào nút Install driver



B5 - Quan sát thấy đã có máy in của PC01



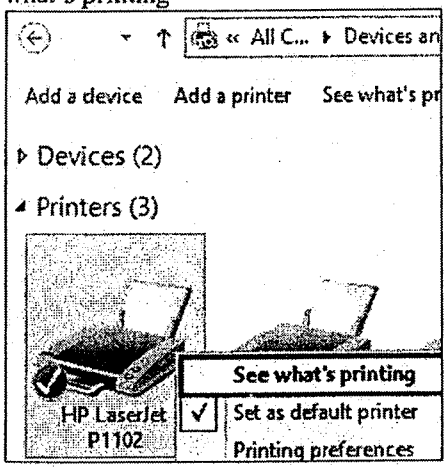
4. Phân quyền (Thực hiện trên PC01)

+ U1 không có quyền in

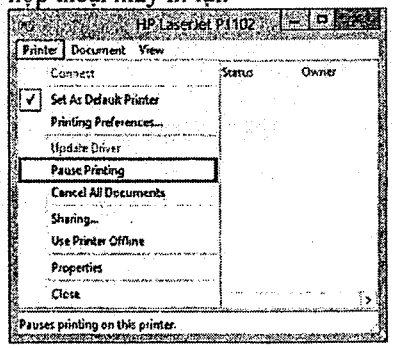
+ Group KeToan có quyền in và quản lý document

+ Group NhanSu có quyền in và chỉ xóa được document do mình tạo ra

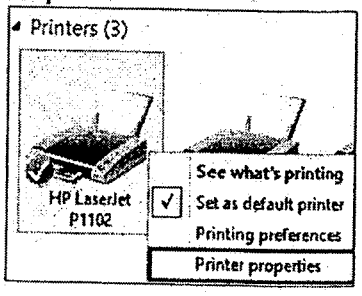
B1 - Chuột phải lên máy in → Chọn See what's printing



B2 - Hộp thoại máy in xuất hiện → Vào menu Printer → Chọn Pause Printing → Sau đó đóng hộp thoại máy in lại.

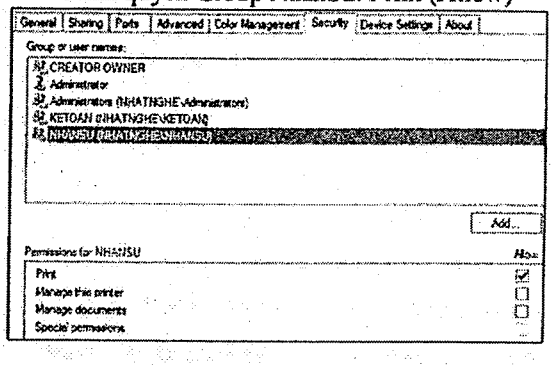


B3 - Chuột phải lên máy in → Chọn Printer Properties

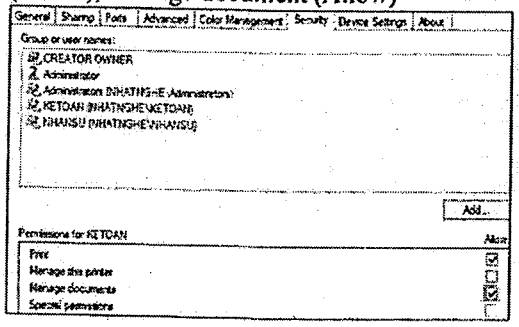


B4 - Tại tab Security → Remove các group ngoại trừ 2 group Administrators và Creator Owner , add thêm 2 group KeToan và NhanSu vào

B5 - Phân quyền Group NhanSu: Print (Allow)



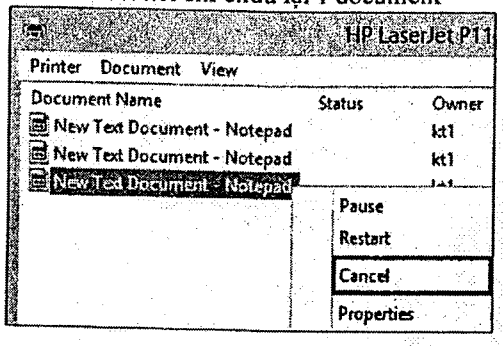
B6 - Phân quyền group KeToan: Print (Allow), Manage document (Allow)



B7 - Kiểm tra: Log on KT1: Mở Notepad soạn nội dung bất kì và gửi lệnh in 3 lần

B8 - Mở Control Panel → Devices and Printers → Double click vào máy in → Double Click See what's printing → Chuột phải lên các document đang có chọn cancel để hủy lệnh in → Hộp thoại cảnh báo chọn Yes → Cancel thành công

B9 - Cancel hết chỉ chừa lại 1 document



B10 - Log on NS1 → Mở notepad soạn nội dung bất kì và gửi lệnh in 3 lần

B11 - Mở Control Panel → Devices and Printers → Double click vào máy in Lexmark → Double Click See what's printing → Chuột phải lên các document đang có của user NS1 chọn cancel để hủy lệnh in → Hộp thoại cảnh báo chọn Yes → Cancel thành công

B12 - Chọn Cancel document của user KT1 → Không thể thực hiện

B13 - Log on U1: Mở Notepad → in thử → không thấy máy in do không có quyền in.

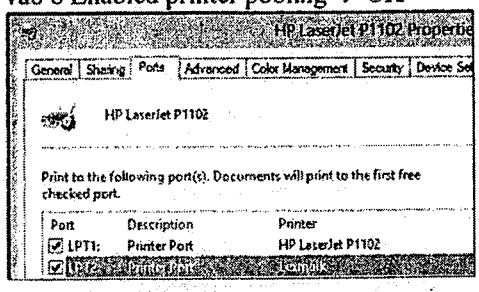
5. Printer pooling (Thực hiện trên PC01)

Mục đích: Tạo ra 1 printer sử dụng chung 2 máy in vật lý

B1 - Thực hiện các thao tác giống phần 1 để add thêm printer Lexmark trên port LPT2

B2 - Trong phần Printers → Chuột phải lên máy in HP → Chọn Printer Properties

B3 - Trong tab Ports → Đánh dấu chọn vào 2 mục: LPT1 và LPT2 → Sau đó đánh dấu chọn vào ô Enabled printer pooling → OK



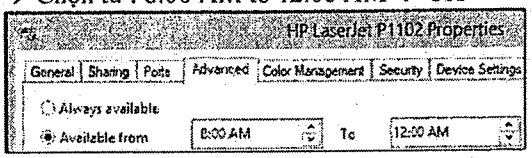
6. Available Time (Thực hiện trên PC01)

B1 - Mở phần Devices and Printers → Chuột phải lên máy in HP → Chọn Printer Properties.

B3 - Kiểm tra: PC02: Log on administrator điều chỉnh giờ hệ thống là 16:00 PM

B4 - Log on KT1: Mở notepad → in thử → không thể in được

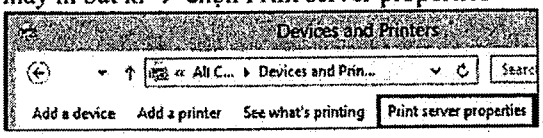
B2 - Qua tab Advanced → Chọn Available from → Chọn từ : 8:00 AM to 12:00 AM → OK



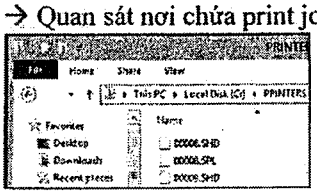
7. Spool folder (Thực hiện tại PC01)

Mục đích: Thay đổi nơi lưu các print job

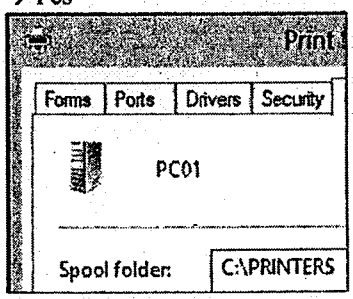
B1 - Trong phần Devices and Printers → Chọn máy in bất kì → chọn Print server properties



B3 - Kiểm tra: Trong ổ C: có thư mục Printers → Quan sát nơi chứa print job



B2 - Qua tab Advanced → đổi đường dẫn "Spool folder" → "C:\PRINTERS" → OK →Yes

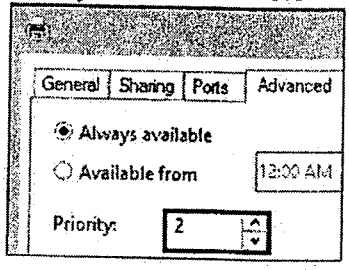


8. Priority (Thực hiện tại PC01)

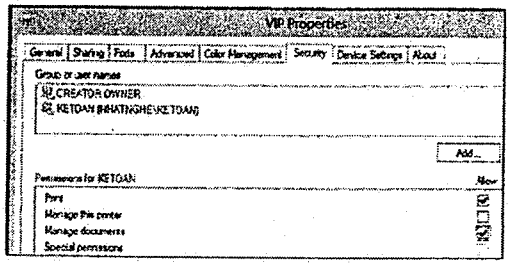
B1 - Thực hiện giống phần 1 để tạo 1 printer mới đặt tên là VIP

B2 - Tại mục Printers → Chuột phải lên Printer VIP → Chọn Printer Properties

B4 - Qua tab Advanced → Trong phần Priority → điền số 2 → OK



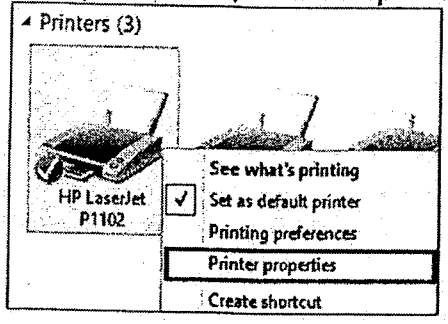
B3 - Trong tab security phân quyền cho group KeToan



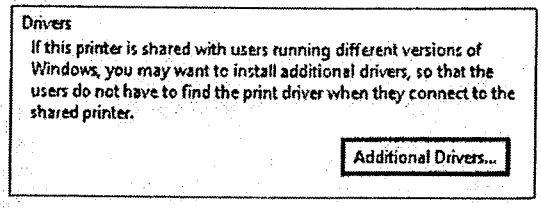
9. Additional Driver

PC01: Add thêm driver dành cho Windows 8

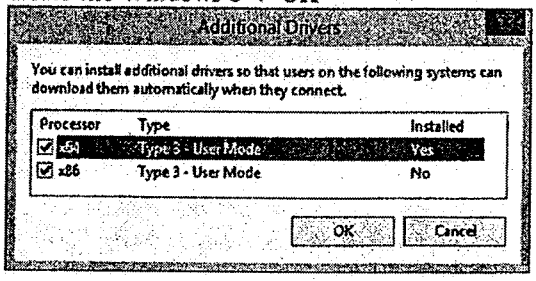
B1 - Mở Devices and Printers → Chuột phải lên máy in HP → chọn Printer Properties



B2 - Qua tab Sharing → Nhấn vào nút Additional Drivers



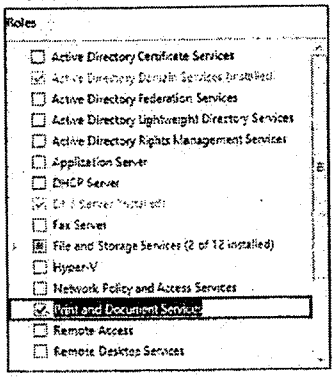
B3 - Đánh dấu chọn vào ô x86 để add thêm phần driver cho Windows 8 → OK



10. Deploy Printer (Thực hiện tại PC01)

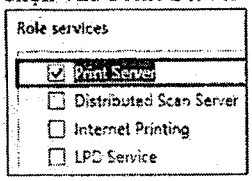
B1 - Mở Server Manager → Menu Manage → Add Roles and Features

B2 - Các bước đầu tiên, nhấn Next theo mặc định → Màn hình Server Roleș → Chọn Print and Document Services



B3 - Chọn Add Features → Next theo mặc định

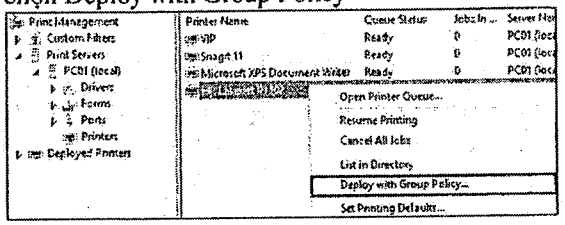
B4 - Màn hình Role Services → đánh dấu chọn vào Print Server → Next



B5 - Màn hình Confirmation → Đánh dấu chọn vào ô Restart the destination server automatically if required → Nhấn Install → Close

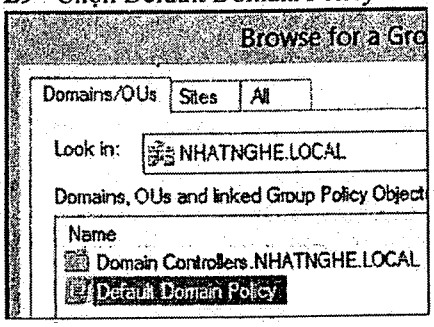
B6 - Mở Server Manager → menu Tools → Print Management

B7 - Bung mục Print Servers → PC01 → Printers → Khung bên phải chuột phải vào máy in HP → chọn Deploy with Group Policy

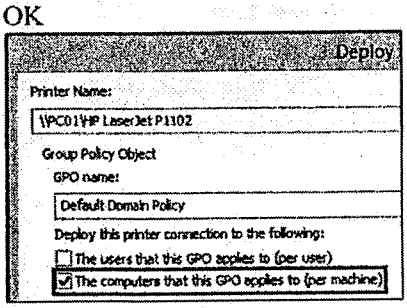


B8 - Ở mục GPO Name → Nhấn Browse

B9 - Chọn Default Domain Policy → OK



B10 - Đánh dấu chọn trước ô The computers that the GPO applies to (per machine) → Chọn Add → OK



B11 - Màn hình cảnh báo chọn OK

B12 - Kiểm tra: Trên máy PC02: log on Administrator → xóa các máy in đã cài đặt → Restart lại máy

B13 - Vào lại phần Printers → Quan sát thấy có máy in HP đã được cài đặt lại

MONITORING

CÁC BƯỚC TRIỂN KHAI

1. Tạo Data Collector Set

2. Lập lịch chạy Data Collector Set

A- CHUẨN BỊ

Mô hình bài lab bao gồm 1 máy Windows Server 2012 R2

- Tắt User Account Control

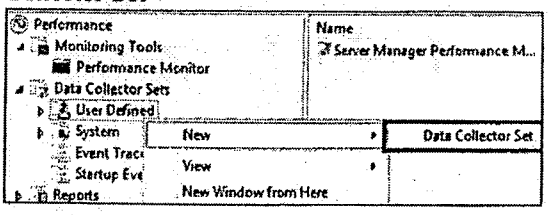
- Log on Administrator

B- THỰC HIỆN

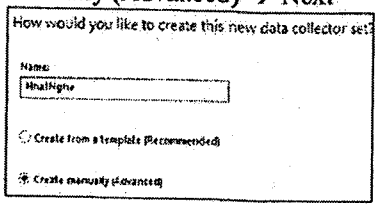
1. Tạo Data Collector Set

B1 - Mở Server Manager → menu Tools → chọn Performance Monitor

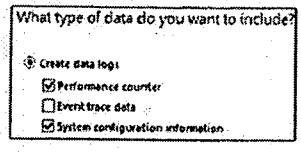
B2 - Chuột phải lên User Defined → New → Data Collector Set



B3 - Đặt tên là NhatNghe → Chọn Create manually (Advanced) → Next

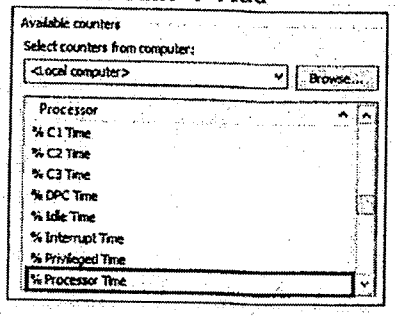


B4 - Chọn Create data logs → Đánh dấu chọn vào 2 ô Performance counter và System Configuration Information → Next

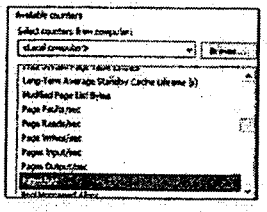


B5 - Nhấn nút Add

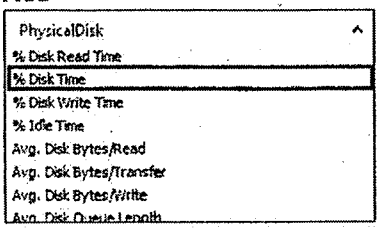
B6 - Bung phần Processor → Chọn % Processor Time → Add

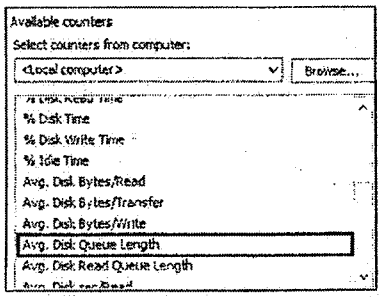


B7 - Bung phần Memory → Chọn Pages/sec → Add

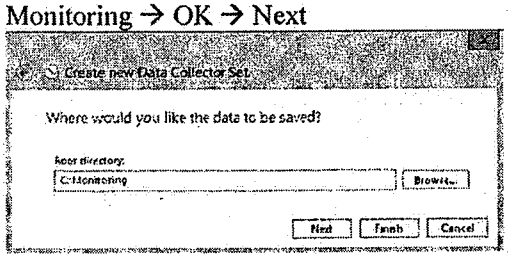


B8 – Bung phần Physical Disk → Chọn % Disk Time và Avg. Disk Queu Length → Add

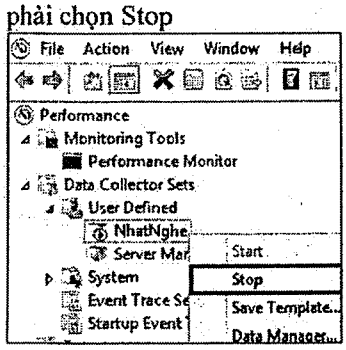




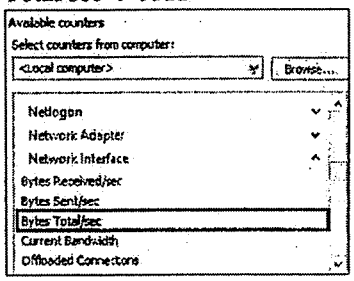
B11 - Chọn Browse → Make New Folder → Monitoring → OK → Next



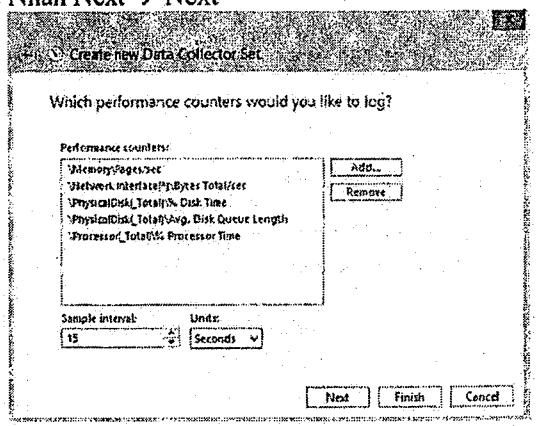
B14 - Sau khi Start khoảng 5 phút → Chuột phải chọn Stop



B9 - Bung phần Network Interface → Chọn Bytes Total/sec → Add

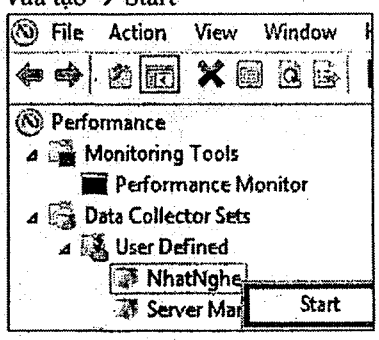


B10 - Kiểm tra các counter đã Add → OK → Nhấn Next → Next

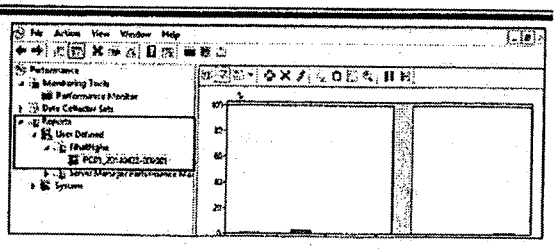


B12 - Nhấn Finish

B13 - Chuột phải lên Data Collector Nhat Nghe vừa tạo → Start

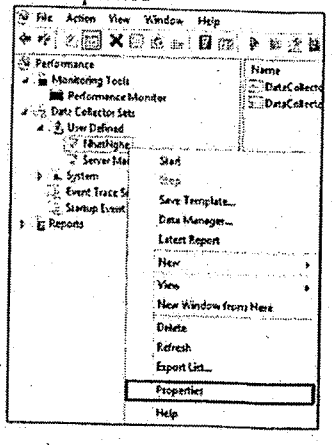


B15 - Mở Report → User Defined → NhatNghe → 0001 : Quan sát các chỉ số đã được lưu lại của Processor, Memory, Physical Harkdisk, Network Interface

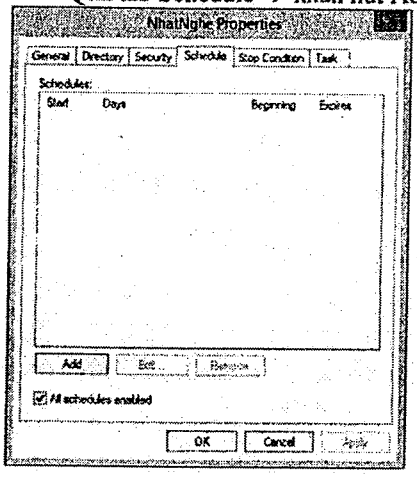


2. Lập lịch chạy Data Collector Set

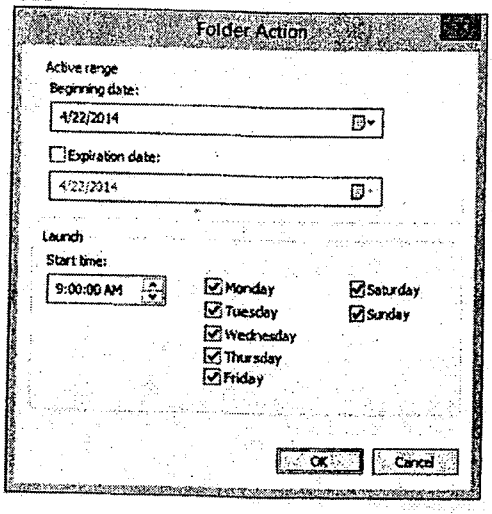
B1 - Mở theo đường dẫn Data Collector Sets → User Defined → Chuột phải vào NhatNghe → Properties



B2 - Qua tab Schedule → nhấn nút Add



B3 - Khai báo lịch chạy của chương trình → OK



BACKUP & SHADOW COPY

CÁC BƯỚC TRIỂN KHAI

1. Cài đặt Windows Server Backup
2. Backup - Recovery File
3. Backup – Recovery System State
4. Lập lịch backup
5. Shadow Copy

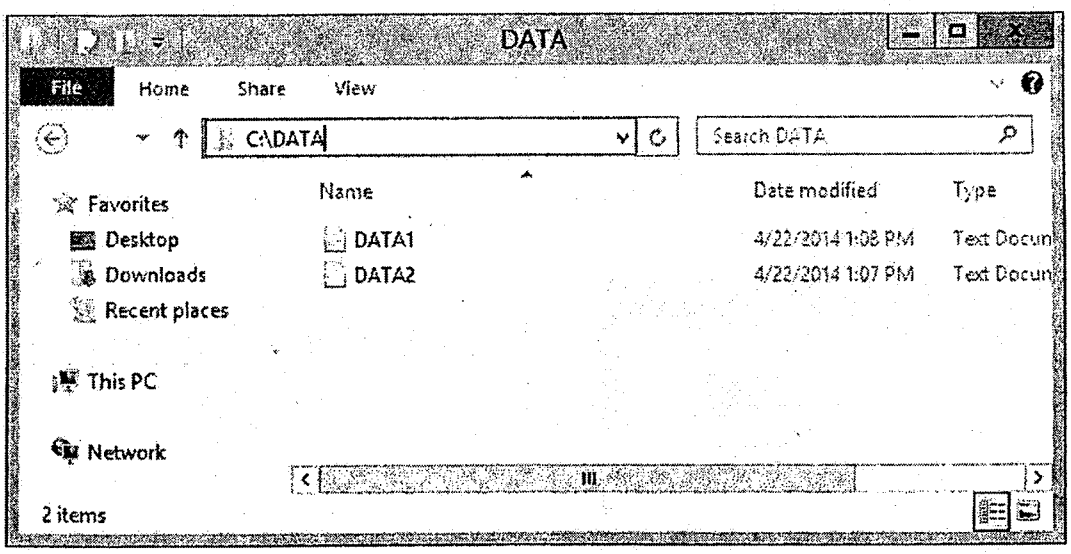
A- CHUẨN BỊ

Mô hình bài lab bao gồm 2 máy:

+ PC01: Windows Server 2012 R2 – DC (Domain: NHATNGHE.LOCAL)

+ PC03: Windows Server 2012 R2

- PC01: Tạo thư mục C:\DATA. Trong DATA tạo 2 file: DATA1.TXT và DATA2.TXT



- PC01: Tạo user U1/password: 123

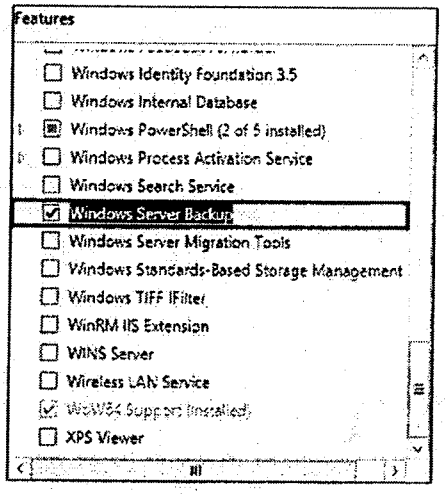
- PC03: Tạo 2 thư mục Backup và BackupSystem trong ổ C:, Share full cả 2 thư mục

B- THỰC HIỆN

1. Cài đặt Windows Server Backup (Thực hiện trên máy PC01)

B1 - Mở Server Manager → Menu Manage → Add Roles and Features

B2 - Các bước đầu tiên nhấn Next theo mặc định. Màn hình Features → đánh dấu chọn vào ô Windows Server Backup → Next → Install → Close

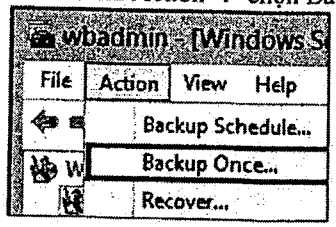


2. Backup - Recovery File (Thực hiện trên máy PC01)

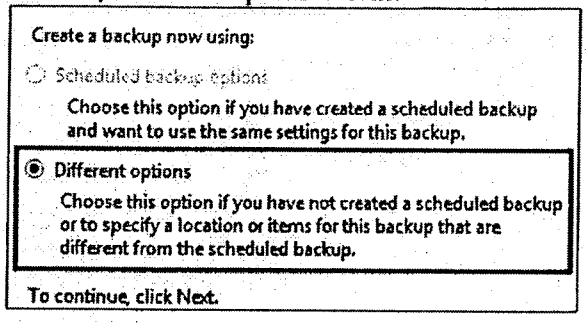
a. Backup File

B1 - Mở Server Manager → menu Tools → chọn Windows Server Backup

B2 - Menu Action → chọn Backup Once



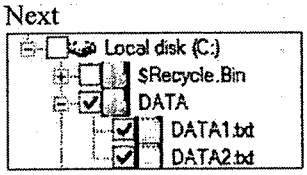
B3 - Chọn Different options → Next



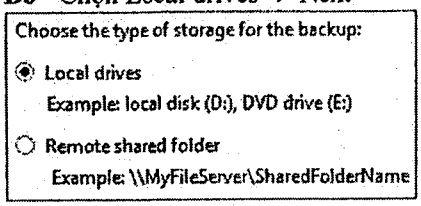
B3 - Chọn Custom → Next

B4 - Nhấn vào nút Add Items

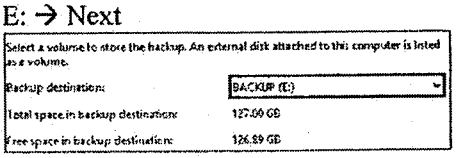
B5 - Chọn vào thư mục DATA → OK → Next



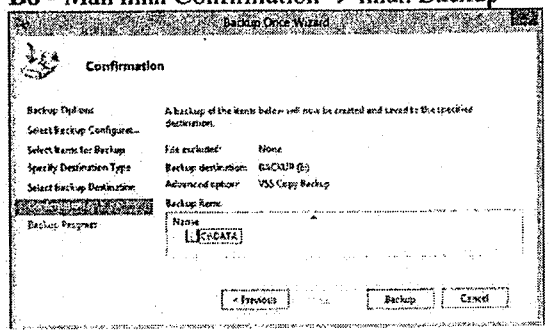
B6 - Chọn Local drives → Next



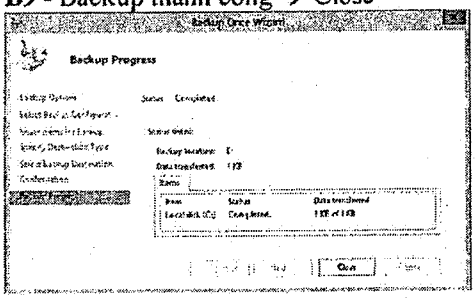
B7 - Ở mục Backup Destination → chọn ổ E: → Next



B8 - Màn hình Confirmation → nhấn Backup



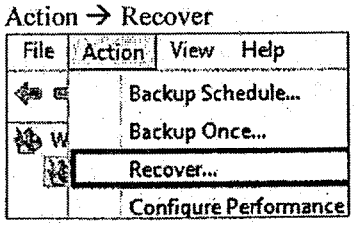
B9 - Backup thành công → Close



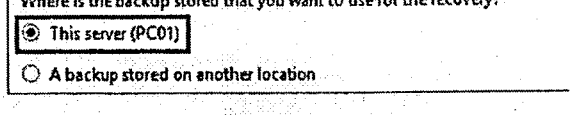
b. Recovery File

B1 - Xóa thư mục C:\DATA

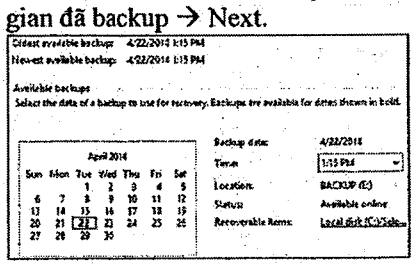
B2 - Mở Windows Server Backup → Menu Action → Recover



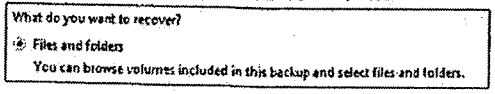
B3 - Chọn This server (PC01) → Next



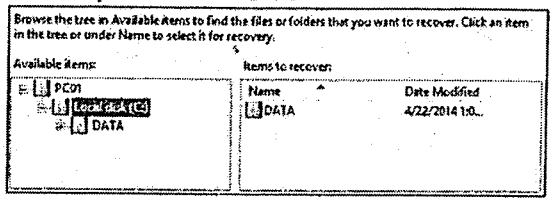
B4 - Màn hình Select Backup Date, chọn thời gian đã backup → Next.



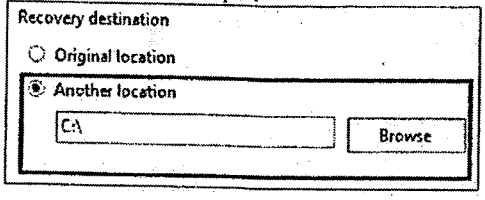
B5 - Chọn Files and Folders → Next



B6 - Chọn ổ đĩa C: → Next



B7 - Chọn Another location → Browse đến thư mục muốn khôi phục → Next



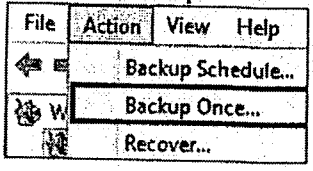
B8 - Nhấn nút Recover để khôi phục → Close

B9 - Kiểm tra: PC01 mở ổ C: quan sát thư mục DATA đã được phục hồi.

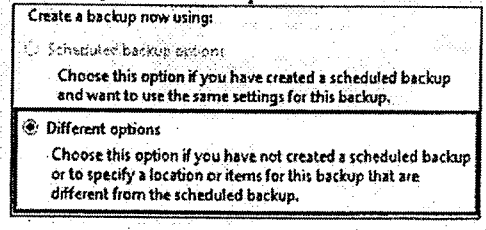
3. Backup- Recovery SystemState

a. Backup SystemState

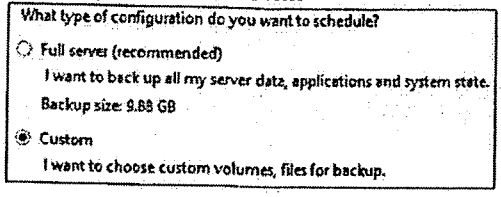
B1 - Mở Window Server Backup → Menu Action → Backup Once



B2 - Chọn Different options → Next

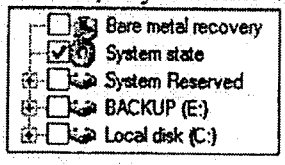


B3 - Chọn Custom → Next

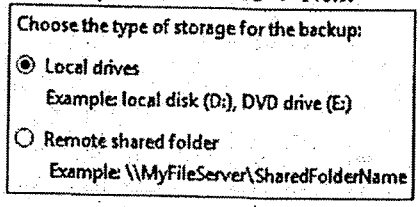


B4 - Nhấn vào nút Add Items

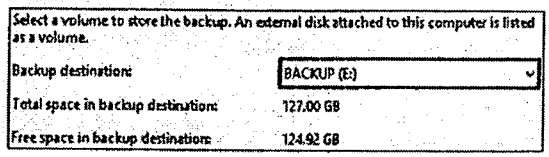
B5 - Chọn System state → OK → Next



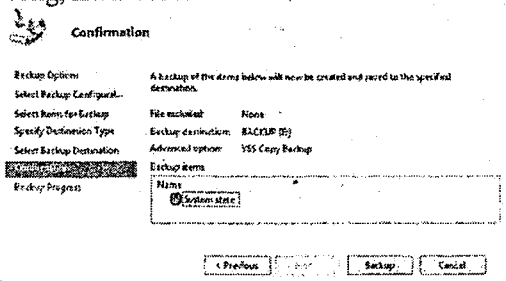
B6 - Chọn Local drives → Next



B7 - Ở mục Backup Destination → chọn ổ E: → Next



B8 - Nhấn Backup → Sau khi backup thành công, nhấn Close

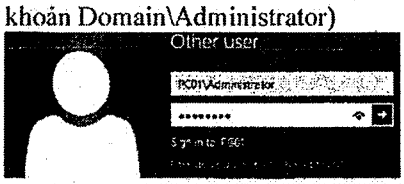


b. Recovery System State

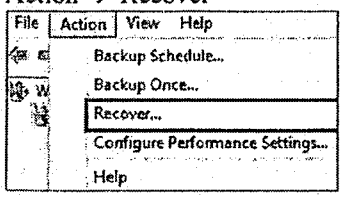
B1 - PC01 : xóa user U1

B2 - Khởi động lại máy , nhấn F8 liên tục → Tại màn hình Boot Option → Chọn Directory Services Repair Mode

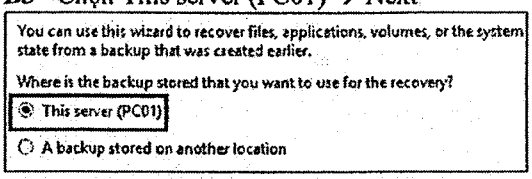
B3 - Log on bằng account Local Administrator (Lưu ý: không log on bằng tài khoản Domain\Administrator)



B4 - Mở Windows Server Backup → Menu Action → Recover

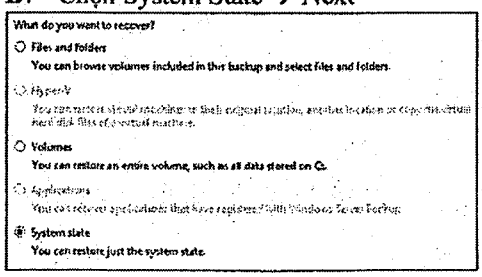


B5 - Chọn This server (PC01) → Next



B6 - Màn hình Select Backup Date, chọn thời gian đã backup → Next.

B7 - Chọn System State → Next



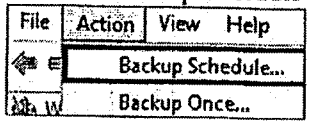
B8 - Hộp thoại cảnh báo → nhấn OK

B9 - Các bước còn lại nhấn Next theo mặc định. Màn hình Confirmation → Recover → Yes → Restart

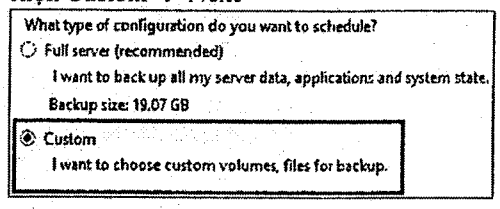
B10 - Kiểm tra : Account U1 đã được khôi phục.

4. Lập Lịch Backup

B1 - Mở Windows Server Backup → menu Action → Backup Schedule



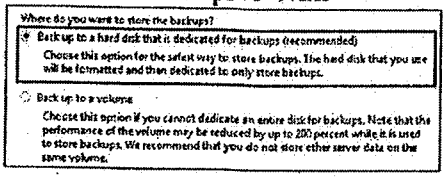
B2 - Màn hình Select Backup Configuration, chọn Custom → Next



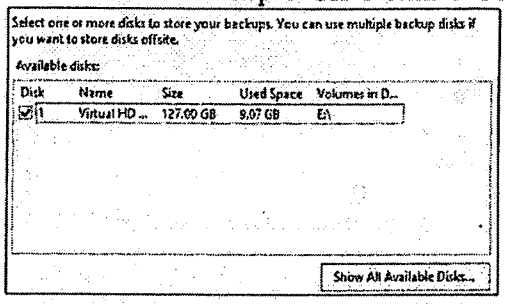
B3 - Nhấn Add Items, chọn đối tượng muốn tự động backup, VD: System State → OK → Next

B4 - Chọn lựa thời gian tự động backup → Next

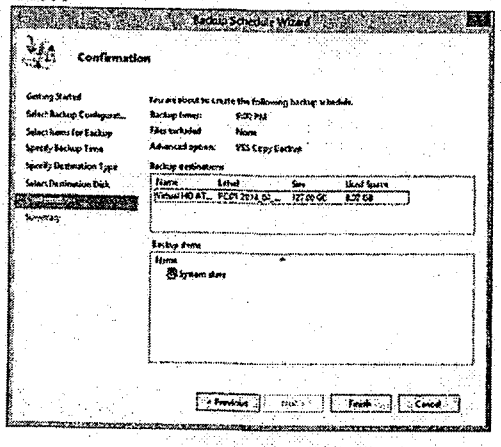
B5 - Chọn Backup to a hard disk that is dedicated for backups → Next



B6 - Nhấn Show All Available Disks → Chọn ổ đĩa muốn lưu file backup → OK → Next → Yes



B7 - Lập lịch backup thành công → Finish → Close

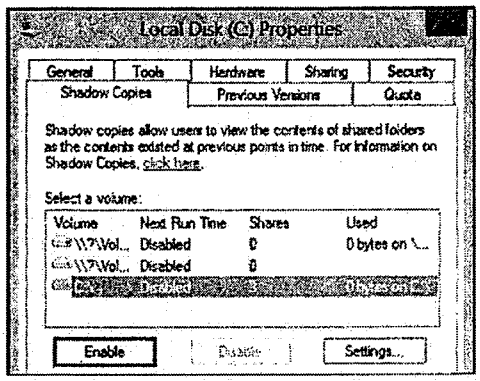


5. Shadow Copy (Thực hiện trên PC01)

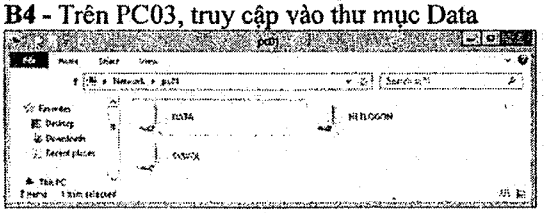
B1 - Tạo folder C:\ Data & Share everyone allow full control

B2 - Mở File Explorer → Chuột phải vào ổ C: → chọn Properties

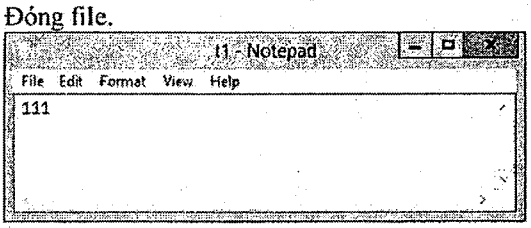
B3 - Qua tab Shadow Copies → Chọn Enable → Yes



B4 - Trên PC03, truy cập vào thư mục Data

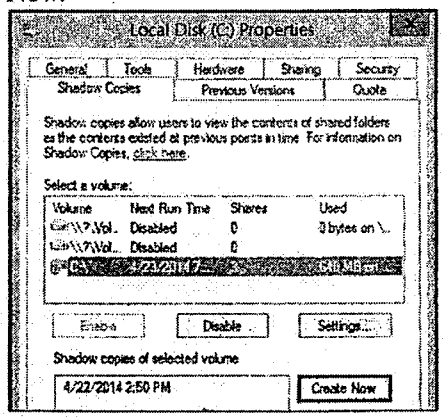


B5 - Tạo file T1.txt nội dung "111" → Save → Đóng file.

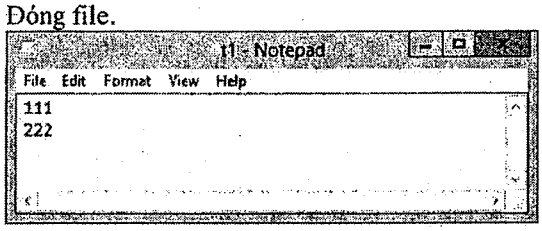


B6 - Trên PC01, mở File Explorer → Chuột phải lên C: → Properties.

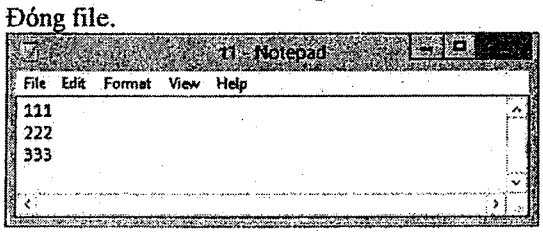
B7 - Qua tab Shadow Copies → nhấn Create Now.



B8 - Trên PC03, truy cập vào thư mục Data và thêm vào file T1.txt nội dung "222" → Save → Đóng file.

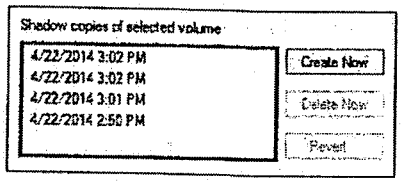


B9 - Trên PC03: Truy cập vào thư mục Data và thêm vào file T1.txt nội dung "333" → Save → Đóng file.



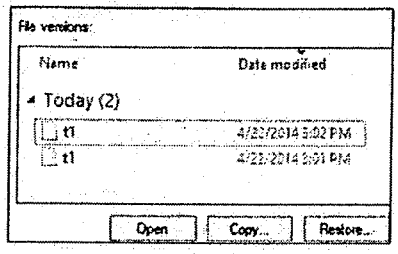
B10 - Trên PC01: Chuột phải vào ổ C: → Properties → Qua tab Shadow Copies → Chọn Create Now để tạo thêm nhiều Shadow Copies.

B11 - Quan sát thấy các Shadow Copies đã tạo → OK

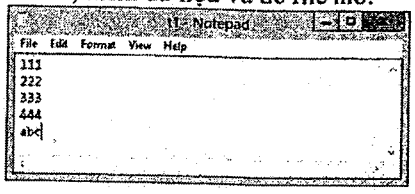


B12 - Trên PC03 → Properties file T1.txt

B13 - Qua tab Previous Versions → Thấy có các File version. Muốn khôi phục lại version nào, nhấn chọn vào version đó → nhấn nút Restore



B14 - Bên cạnh đó Shadows copies còn có khả năng backup "OPEN FILE". Trên PC03, mở file T1.txt, thêm dữ liệu và để file mở.

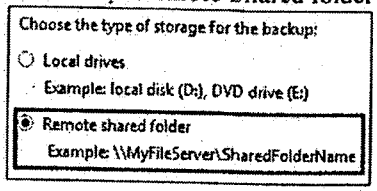


B15 - Trên PC01: Backup folder DATA bằng cách mở chương trình Windows Server Backup → Action → Backup One.

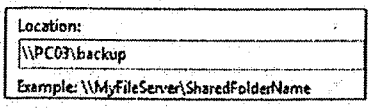
B16 - Các bước đầu tiên nhấn Next theo mặc định → Màn hình Select Backup Configuration → Chọn Custom→ Next.

B17 - Chọn Add Items → Đánh dấu chọn vào DATA → OK → Next

B18 - Chọn Remote Shared folder → Next



B19 - Location nhập: \\PC03\Backup → Next.



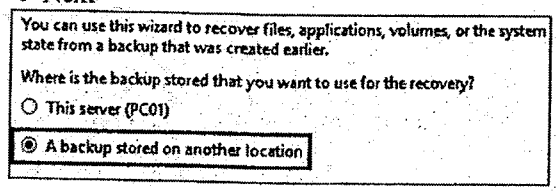
B20 - Nhập vào username: Administrator và password của PC03

B21 - Nhấn Backup → Close

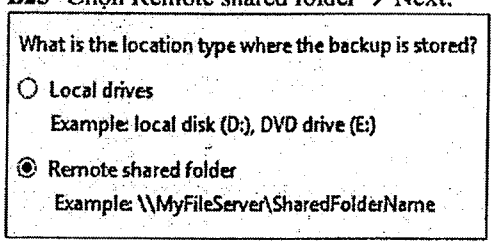
B22 - Trên PC01: Restore dữ liệu backup vào ổ C:

B23 - Mở chương trình Windows Server Backup → Action → Recover

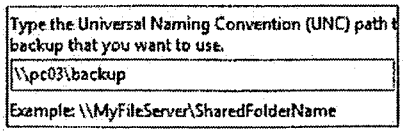
B24 - Chọn A backup stored on another location → Next



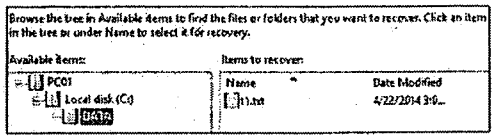
B25- Chọn Remote shared folder → Next.



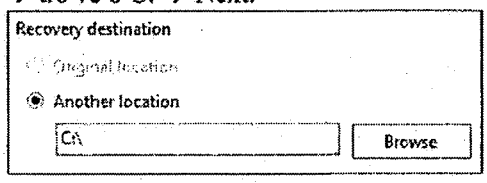
B26 - Nhập vào đường dẫn: \\pc03\backup → Next.



B27 - Các bước còn lại nhấn Next theo định. Màn hình Select Items to Recover → chọn Data → Next.

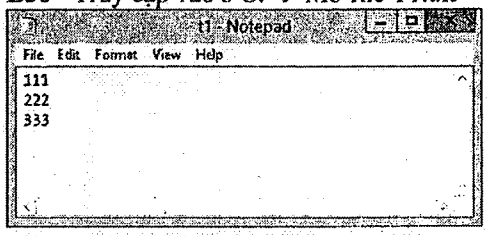


B28 - Mục Recover destination → Chọn Browse → trỏ về ổ C: → Next.



B29 - Chọn Recover

B30 - Truy cập vào ổ C: → Mở file T1.txt



** Nhận xét: Có thể thấy rằng trong thời điểm backup diễn ra, dù file T1.txt đang được mở (open file) nhưng chương trình backup đã tự động backup phiên bản mới nhất trong các previous version.*

HYPER-V

CÁC BƯỚC TRIỂN KHAI

1. Cài đặt Hyper-V

2. Khảo sát Hyper-V

a. Tạo Switch ảo (Virtual Switch)

b. Tạo đĩa cứng ảo (Virtual Hard Disk)

c. Xem thông tin đĩa cứng ảo (Inspect Disk)

d. Chỉnh sửa đĩa cứng ảo

e. Tạo máy ảo (Virtual Machine)

f. Tạo Diffrerencing Disk

g. Tạo Snapshot (Backup trạng thái máy ảo)

h. Khôi phục Snapshot (Restore máy ảo)

A- CHUẨN BỊ

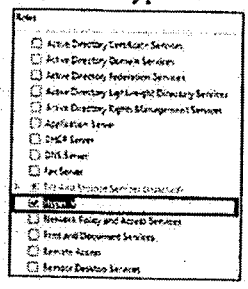
Mô hình bài lab bao gồm 1 máy Windows Server 2012 R2 Stand Alone

B- THỰC HIỆN

1. Cài đặt Hyper-V

B1 - Trên Server Manager, vào menu Manage, chọn Add Roles and Features

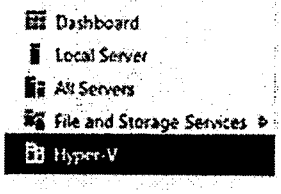
B2 – Các bước tiếp theo nhấn Next theo mặc định. Màn hình Server Roles → đánh dấu chọn vào Hyper-V.



B3 - Nhấn Add Features → Next → Next. Các bước còn lại nhấn Next theo mặc định.

B4 - Màn hình Confirm Installation Selections → đánh dấu chọn vào ô Restart the destination server automatically if required → Install → Yes

B5 - Quá trình cài đặt sẽ diễn ra. Sau khi cài xong kiểm tra sẽ thấy Role Hyper-V.



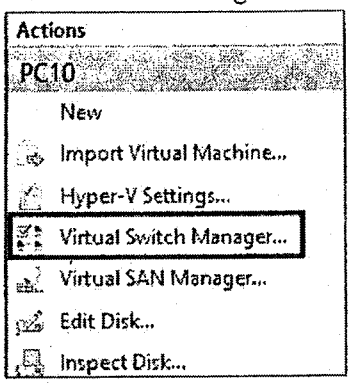
2. Khảo sát Hyper -V

- Máy được cài đặt Hyper-V gọi là Host Hyper V.

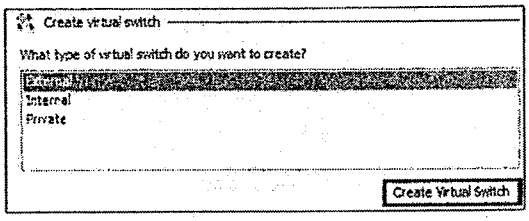
- Virtual Switch của Hyper-V gọi là Switch ảo, bản thân máy Host có thể đảm nhận vai trò Switch ảo.

a. Tạo Switch ảo (Virtual Switch)

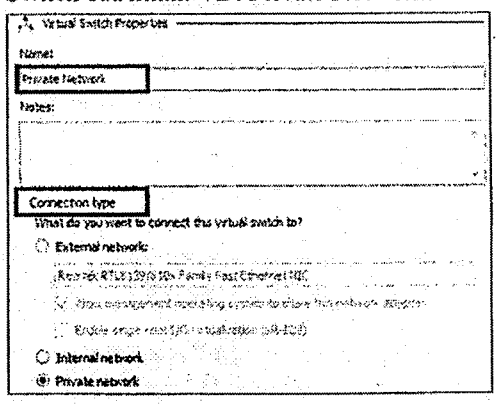
B1 - Mở Hyper-V Manager → Ở khung Actions nằm ở góc phải → nhấn vào mục Virtual Switch Manager.



B2 - Để tạo Switch ảo → nhấn vào Create Virtual Switch.



B3 - Ở mục Connection type, chọn dạng Virtual Switch muốn tạo → Ở mục Name, đặt tên cho Switch của mình. VD: Private Network.



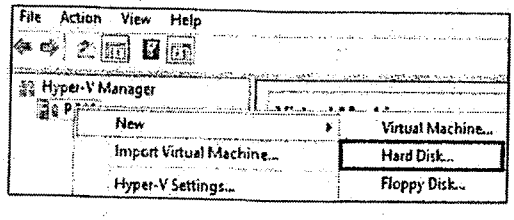
B4 - Tương tự tạo thêm Internal Network và External Network.

b. Tạo đĩa cứng ảo (Virtual Hard Disk)

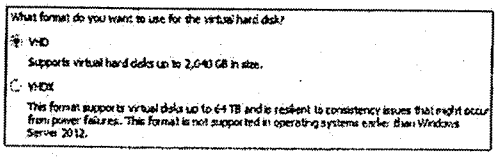
*Đĩa cứng ảo (Virtual Hard Disk): là file có đuôi *.vhd (trên Windows Server 2008) hoặc *.vhdx (chỉ có trên Windows Server 2012).*

B1 - Tạo folder C:\VM, sau đó lần lượt tạo thêm các thư mục VM1, VM2, VM3 trong C:\VM

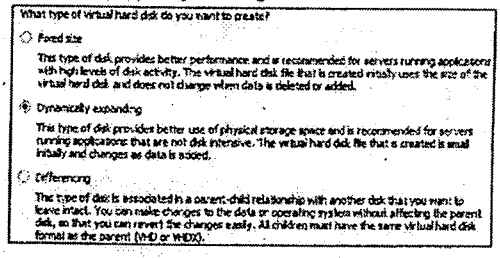
B2 - Quay lại Hyper-V Manager, chuột phải lên tên máy tính → chọn New → chọn Hard Disk…



B3 - Màn hình Choose Disk Format → VHD → Next

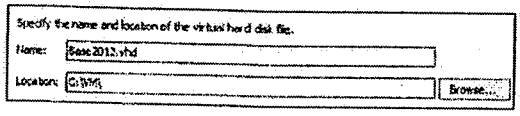


B4 - Màn hình Choose Disk Type → chọn Dynamically expanding → Next

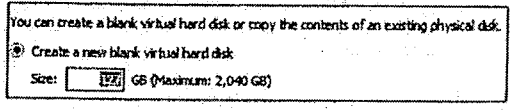


B5 - Màn hình Specify Name and Location, ở mục Name → đặt tên cho ổ cứng là Base2012.vhd.

B6 - Tiếp theo ở mục Location → nhấn Browse → trỏ đường dẫn đến thư mục C:\VM\ để lưu ổ cứng ảo



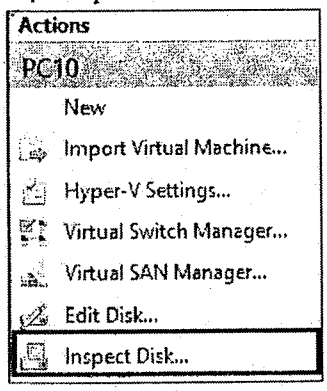
B7 - Màn hình Configure Disk → chọn Create a new blank virtual hard disk. Ở mục Size → nhập vào dung lượng đĩa cứng ảo → Next



B8 - Màn hình Completing the New Virtual Hard Disk Wizard → kiểm tra lại thông tin về đĩa cứng ảo → nhấn Finish.

c. Xem thông tin đĩa cứng ảo (Inspect Disk)

B1 - Sau khi tạo xong, để xem thông tin đĩa cứng ảo, trong cửa sổ Hyper-V Manager → ở khung Action nằm ở góc phải → nhấn vào mục Inspect Disk.



B2 - Tiếp theo trỏ đường dẫn đến đĩa cứng ảo mà bạn muốn xem thông tin. Chương trình sẽ hiển thị thông tin chi tiết về đĩa như:

+ Format: Định dạng đĩa cứng ảo: vhd hay vhdx

+ Type: Loại đĩa cứng ảo: Dynamically expanding, Differencing hay Fixed Size

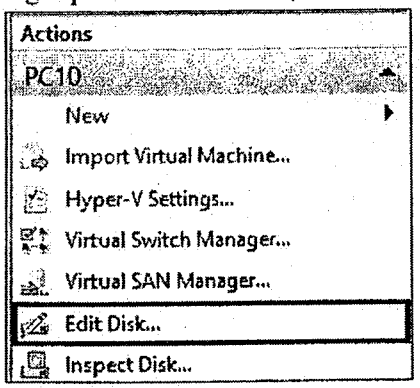
+ Location: Nơi chứa đĩa cứng ảo

+ Current File Size: Kích thước dung lượng đĩa hiện tại

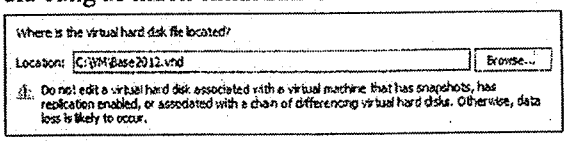
+ Maximum Disk Size: Dung lượng tối đa của đĩa

d. Chỉnh sửa đĩa cứng ảo

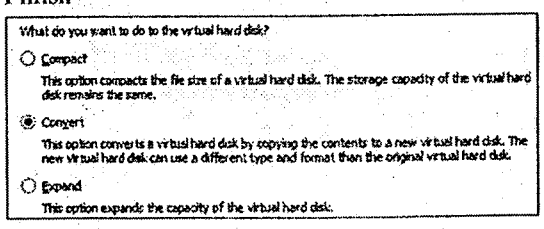
B1 - Để chỉnh sửa đĩa cứng ảo, trong cửa sổ Hyper-V Manager → ở khung Action nằm ở góc phải → nhấn vào mục Edit Disk.



B2 - Màn hình Locate Virtual Hard Disk, ở mục Location → nhấn nút Browse → trỏ đường dẫn đến đĩa cứng ảo muốn chỉnh sửa → nhấn Next.



B3 - Màn hình Choose Action → Chọn Convert → Finish



+ Compact: Tăng vùng trống còn lại trên đĩa, không thay đổi dung lượng tối đa. VD: Đĩa tối đa 127 GB, đã dùng 100 GB, như vậy vùng trống còn 27GB. Chức năng Compact là nó sẽ sắp xếp đĩa (defragment disk) ở vùng đã dùng (100 GB) để tăng dung lượng cho vùng trống (27 GB). Đây được gọi là chức năng chống phân mảnh trên đĩa cứng ảo.

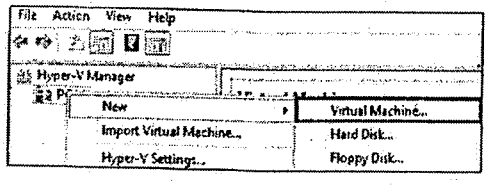
+ Convert: Để chuyển đổi qua lại giữa định dạng vhd và vhdx. Chương trình sẽ tạo ra 1 file mới với định dạng mà bạn muốn chuyển đổi (không xóa file cũ).

+ Expand: Nới rộng dung lượng tối đa của đĩa cứng ảo.

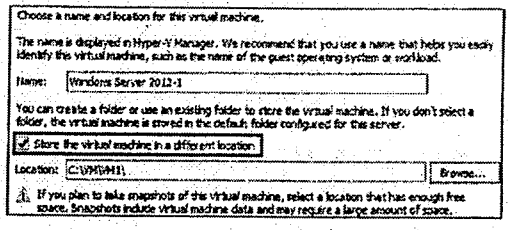
e. Tạo máy ảo (Virtual Machine)

Chuẩn bị: file ISO cài đặt Windows Server 2012

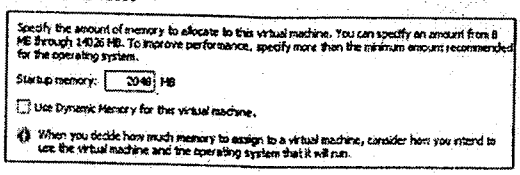
B1 - Chuột phải lên Host → chọn New → chọn Virtual Machine…



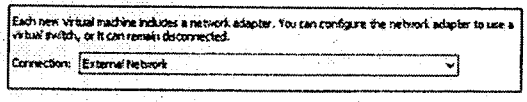
B2 - Màn hình Specify Name and Location, ở mục Name →đặt tên cho máy ảo của mình: Windows Server 2012-1 → Đánh dấu chọn vào ô Store the virtual machine in a different location → Nhấn nút Browse và trỏ đường dẫn đến C:\VM\VM1 → Next.



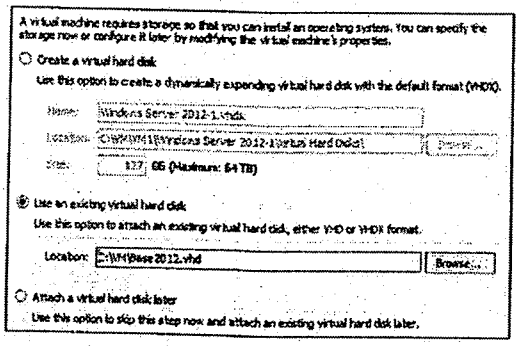
B3 - Màn hình Assign Memory, ở mục Startup memory → thiết lập RAM cho máy ảo : 2048 MB → Next



B4 - Màn hình Configure Networking, ở mục Connection → chọn Virtual Switch đã tạo: External Network.

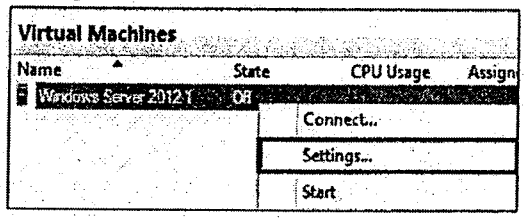


B5 - Màn hình Connect Virtual Hard Disk → chọn Use and existing virtual hard disk → nhấn nút Browse và trỏ đường dẫn đến đĩa cứng ảo đã tạo → Next

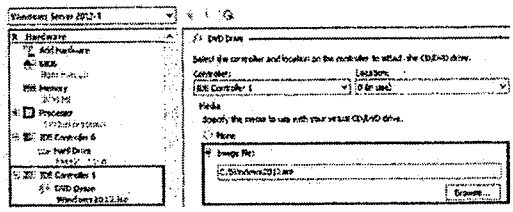


B6 - Sau khi tạo xong → nhấn nút Finish

B7 - Chuột phải lên máy ảo vừa tạo → chọn Settings.



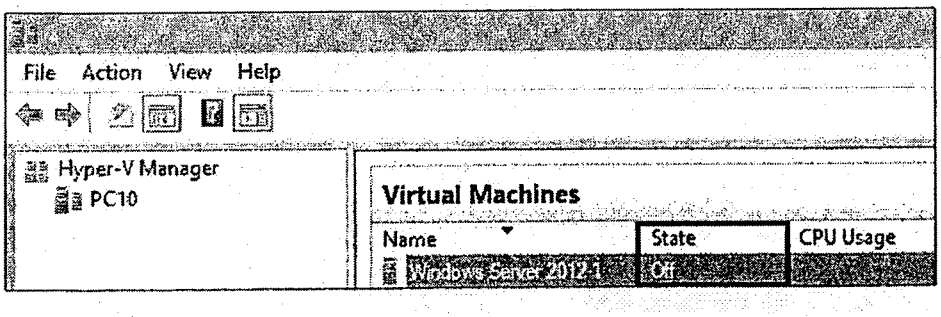
B8 - Ở cột bên trái → chọn DVD. Sau đó ở khung bên phải → chọn Image File và trỏ đường dẫn đến file ISO cài đặt Windows Server 2012 → nhấn Apply → OK.



B9 - Chuột phải vào máy ảo vừa tạo → chọn Start, sau đó nhấn double click vào máy ảo và bắt đầu cài Windows Server 2012 (cài phiên bản Windows DataCenter 2012 with GUI)

*** Một số phím tắt trên máy ảo**

- Ctrl + Alt + End (thay thế Ctrl + Alt + Delete)
- Ctrl+ Alt + Pause (Break) (Phóng to toàn màn hình)
- Để Shutdown máy ảo chuột phải vào máy ảo → chọn Shutdown.
- Quan sát sẽ thấy cột State ở máy ảo là Off nghĩa là quá trình tắt máy thành công.



f. Tạo Differencing Disk

B1 - Quay lại Hyper-V Manager → chuột phải lên Host → chọn New → chọn Hard Disk.

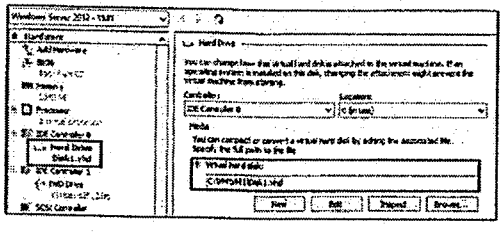
B2 - Màn hình Choose Disk Format → chọn định dạng đĩa cứng ảo là VHD → Next

B4 - Màn hình Specify Name and Location → ở mục Name, đặt tên cho đĩa cứng ảo: Disk1.vhd. Ở mục Location → nhấn vào Browse và trỏ đường dẫn đến thư mục C:\VM\VM1.

B6 - Màn hình Summary → kiểm tra lại thông tin → nhấn nút Finish

B7 - Chuột phải vào máy ảo, chọn Settings.

B8 - Ở cột bên trái, tìm đến mục Hard Drive → Ở khung bên phải, mục Virtual hard disk → nhấn nút Browse và trỏ đường dẫn đến đĩa cứng ảo Disk1.vhd vừa mới tạo → nhấn nút Apply → OK.

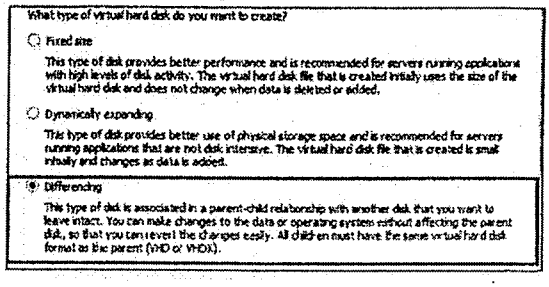


B11 - Khởi động máy ảo, chép dung lượng bất kỳ vào. Sau đó kiểm tra lại dung lượng của ổ đĩa ảo (Disk 1) sẽ thấy tăng lên, ổ đĩa Base ko thay đổi (Cấu trúc của Differencing).

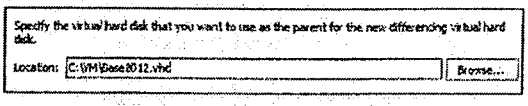
Disk 1: 285,496 KB

Disk Base: 8,409,356 GB

B3 - Màn hình Choose Disk Type → chọn loại đĩa cứng là Differencing → Next



B5 - Màn hình Configure Disk → nhấn nút Browse → trỏ đường dẫn đến đĩa Parent (hay còn gọi là đĩa Base)



B9 - Chuột phải vào máy ảo, chọn Start. Kiểm tra thấy máy ảo khởi động Windows thành công.

B10 - Tắt máy ảo, dùng tính năng Inspect Disk, ghi chú lại dung lượng của đĩa Base và đĩa cứng ảo của máy ảo 1

Disk 1: 332 KB

Disk Base: 8,409,356 GB

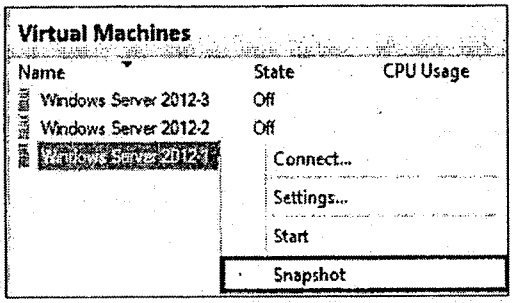
B12 - Tương tự tạo thêm Disk2.vhd và Disk3.vhd (Dạng đĩa Differencing) cùng gắn vào 1 đĩa Base duy nhất. Tạo 2 máy ảo VM2 và VM3, máy ảo sẽ sử dụng ổ đĩa tương ứng. Khởi động cả 3 máy cùng lúc. Như vậy chứng minh được 1 đĩa base xài được cho nhiều differencing.

Lưu ý: Không thay đổi kích thước đĩa Base khi sử dụng Differencing.

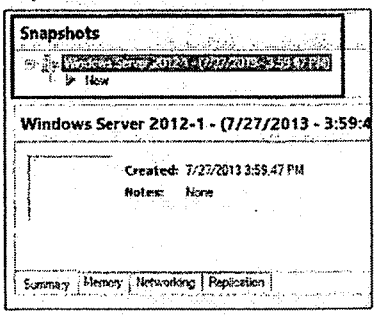
g. Tạo Snapshot (Backup trạng thái máy ảo):

Snapshot máy ảo: Trả máy ảo về tình trạng như lúc ban đầu

B1 - Chuột phải vào máy ảo muốn Backup → chọn Snapshot.

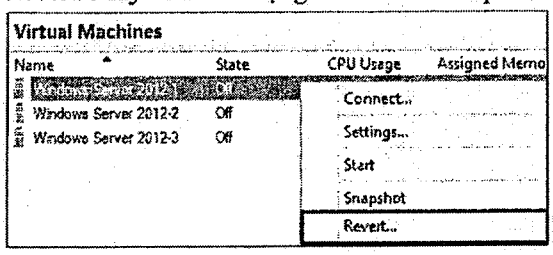


B2 - Quan sát Snapshot vừa tạo ở khung Snapshot (có thể tạo nhiều Snapshot). Muốn đổi tên Snapshot → chuột phải vào Snapshot → chọn Rename.

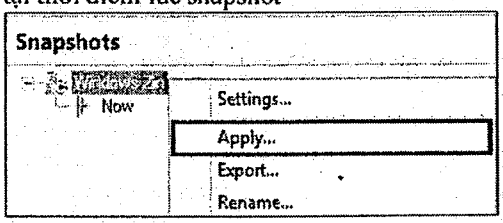


h. Khôi phục Snapshot (Restore máy ảo)

- Cách 1: Chuột phải vào máy ảo → chọn Revert. Máy ảo trả về trạng thái trước 1 snapshot.



- Cách 2: Chuột phải vào Snapshot cần khôi phục → chọn Apply. Máy ảo sẽ được trả lại tại thời điểm lúc snapshot



LOCAL STORAGE – PHẦN 1

CÁC BƯỚC TRIỂN KHAI

1. Basic Disk

a. Primary Partition

b. Extended - Logical Partition

2. Dynamic Disk

a.Chuyển disk sang dynamic

b. Mirror

c. Spanned

d. Striped

e. Raid 5

A- CHUẨN BỊ

- 1 máy ảo Windows Server 2012 R2 có 3 HDD:

* HDD 0 (15GB) : có 1 partition Windows (7 GB)

* HDD 1 (15GB) : trống

* HDD 2 (15Gb) : trống

- Gắn Disk0 và Disk1 vào máy ảo

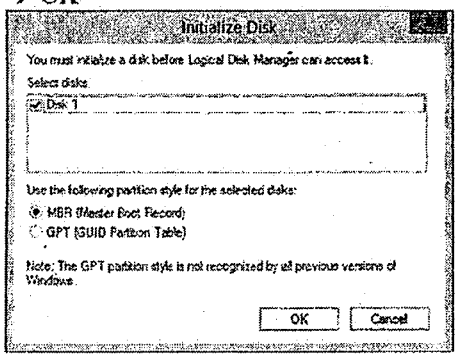
B- THỰC HIỆN

1. Basic Disk

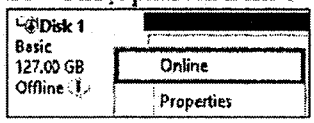
a. Primary Partition

B1 - Nhấn tổ hợp phím ⊞ + R, gõ lệnh Diskmgmt.msc

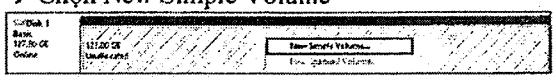
B2 - Cửa sổ Initialize Disk → Chọn Disk 1 → OK



B3 - Chuột phải lên Disk 1 → Chọn Online

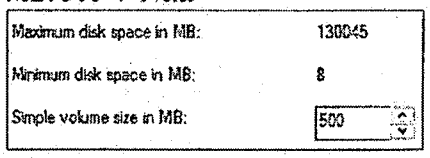


B4 - Chuột phải lên vùng Unallocated của Disk1 → Chọn New Simple Volume

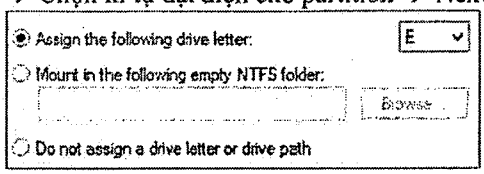


B5 - Màn hình Welcome → nhấn Next

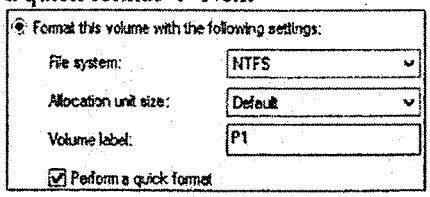
B6 - Màn hình Specify Volume Wizard → Chọn dung lượng partition trong Simple volume size in MB: 500 → Next



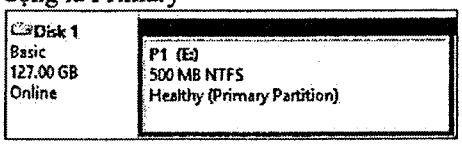
B7 - Màn hình Assign Drive Letter or Path → Chọn kí tự đại diện cho partition → Next



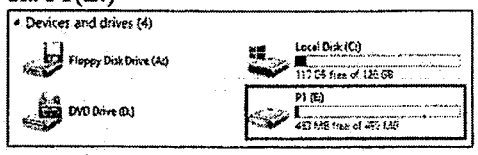
B8 - Màn hình Format Partition → Chọn tên nhãn đĩa trong phần Volume label: P1 → Chọn Perform a quick format → Next



B9 - Chọn Finish. Quan sát tạo partition thành công. Loại partition được chọn tự động là Primary



B10 - Mở File Explorer, quan sát thấy có thêm ổ đĩa P1(E:)



B11 - Thực hiện lại các bước trên tạo thêm 2 partition dung lượng 500 MB với tên lần lượt P2, P3

b. Extended - Logical Partition

- Thực hiện lại các bước giống phần a. để tạo ra partition dung lượng 100 MB, đặt tên là P4

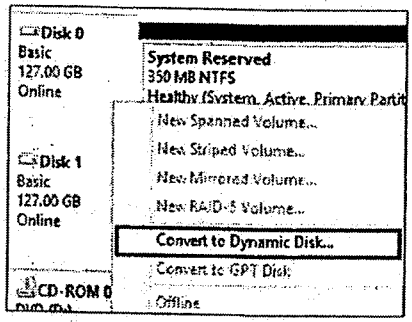
+ Quan sát thấy partition P4 được chọn tự động là Logical

+ Logical Partition được bao bọc bởi Extended Partition

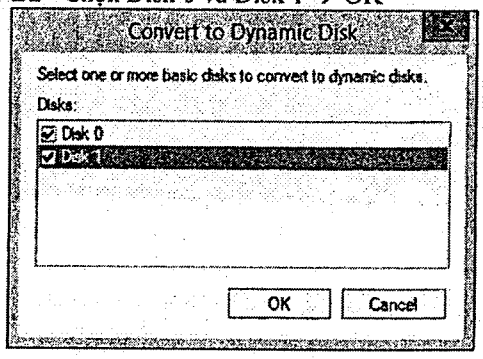
2. Dynamic Disk

a. Chuyển disk sang dynamic

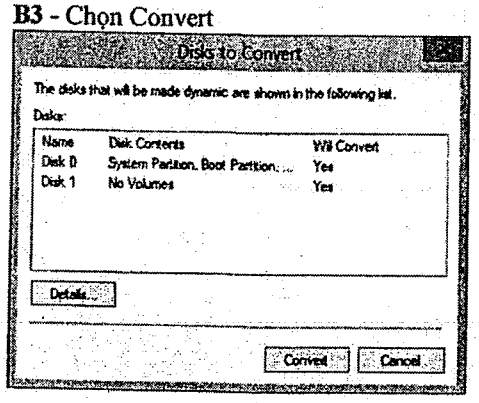
B1 - Mở Disk Management → Chuột phải lên Disk1 → Chọn Convert to Dynamic Disk



B2 - Chọn Disk 0 và Disk 1 → OK

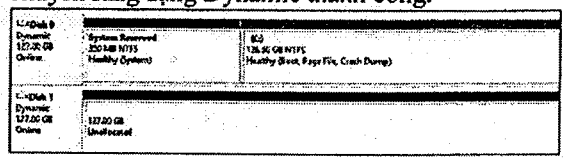


B3 - Chọn Convert



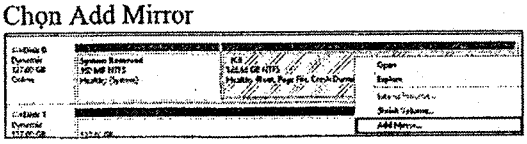
B4 - Màn hình cảnh báo → Chọn Yes

B5 - Quan sát thấy Disk 0 và Disk 1 đã được chuyển sang dạng Dynamic thành công.

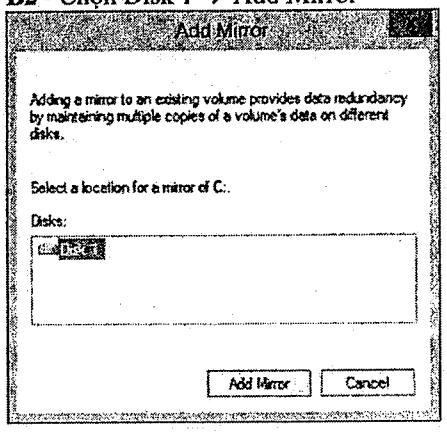


b. Mirror

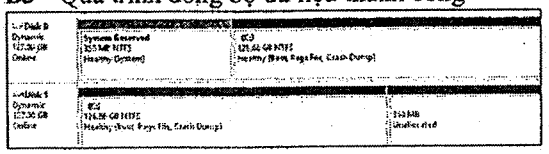
B1 - Chuột phải lên partition chứa hệ điều hành → Chọn Add Mirror



B2 - Chọn Disk 1 → Add Mirror

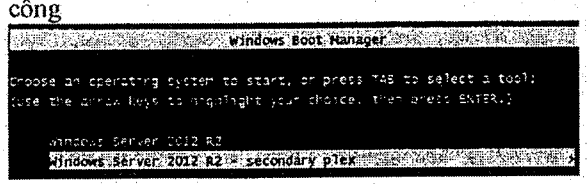


B3 - Quá trình đồng bộ dữ liệu thành công



B4 - Kiểm tra: Gỡ disk 0 ra khỏi máy ảo → Khởi động máy ảo.

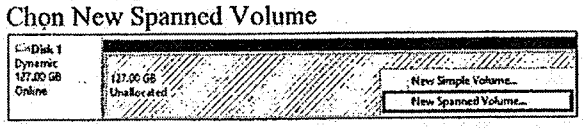
B5 - Chọn Microsoft Windows Server 2012 R2 – secondary plex → Khởi động vào Windows thành công



3. Spanned

B1 - Gắn Disk0 vào máy ảo. Vào Disk Management → Chuột phải lên disk 1 chọn Remove Mirror

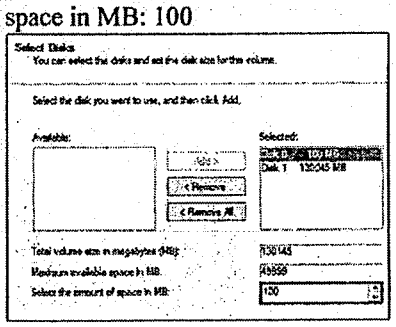
B2 - Chuột phải lên vùng Unallocated tên disk0 → Chọn New Spanned Volume



B3 - Màn hình Welcome → Chọn Next

B4 - Màn hình Select Disks → khung bên trái chọn Disk1 → Chọn Add. Sau đó chọn Disk 0 → Add

B5 - Chọn Disk0 → Select the amount of space in MB: 100



B6 - Chọn Disk1 → Select the amount of space in MB: 200 → Next

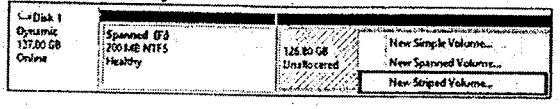
B7 - Màn hình Assign Drive Letter or Path → Next

B8 - Đặt tên partition là Spanned → Đánh dấu chọn vào ô Perform a quick format → Next → Finish

B9 - Kiểm tra: Mở File Explorer thấy xuất hiện Spanned Partition có dung lượng là 300 MB

d. Striped

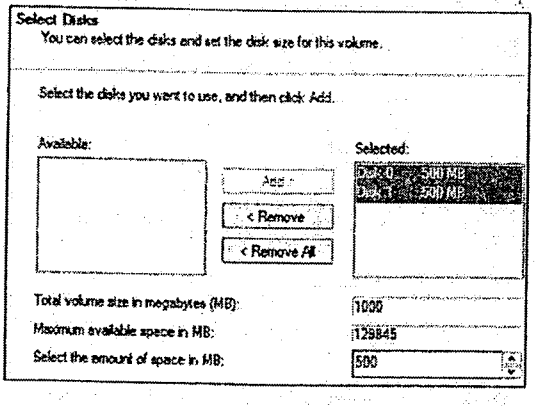
B1 - Chuột phải lên vùng unallocated của disk0 → Chọn New striped volume



B2 - Màn hình Welcome → chọn Next

B3 - Màn hình Select Disk → khung bên trái chọn Disk 1 → Add. Sau đó chọn Disk 0 → Add

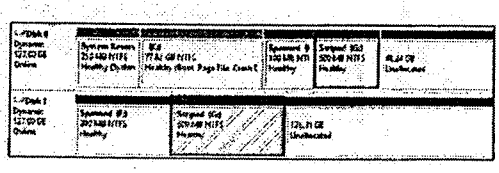
B4 - Chọn dung lượng sẽ lấy để tạo partition trên 2 ổ đĩa vật lí : Select the amount of space in MB : 500 → Next



B5 - Chọn ký tự ổ đĩa G: → Next

B6 - Đặt tên partition là Striped → Chọn ô Perform a quick format → Next → Finish

B7 - Quan sát tạo partition thành công (phần vùng màu xanh)



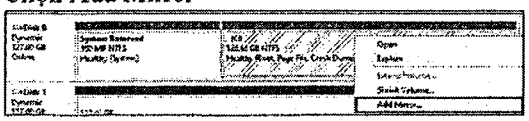
B8 - Kiểm tra: Mở File Explorer, kiểm tra dung lượng Striped partition vừa tạo: 1000 MB

e. Raid 5

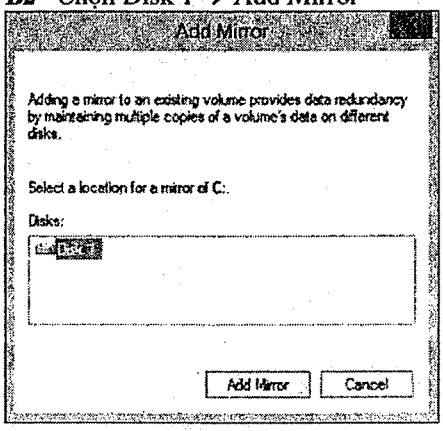
- Xóa hết các partition đã tạo (trừ partition chứa hệ điều hành)
- Gắn đĩa số 3 vào máy ảo

b. Mirror

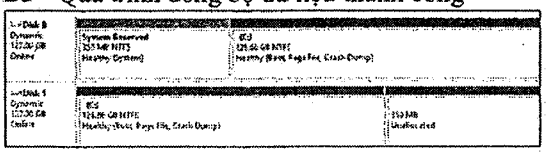
B1 - Chuột phải lên partition chứa hệ điều hành → Chọn Add Mirror



B2 - Chọn Disk 1 → Add Mirror

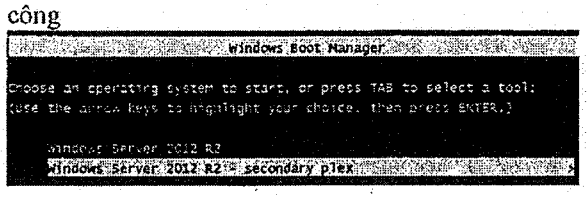


B3 - Quá trình đồng bộ dữ liệu thành công



B4 - Kiểm tra: Gỡ disk 0 ra khỏi máy ảo → Khởi động máy ảo.

B5 - Chọn Microsoft Windows Server 2012 R2 – secondary plex → Khởi động vào Windows thành công



3. Spanned

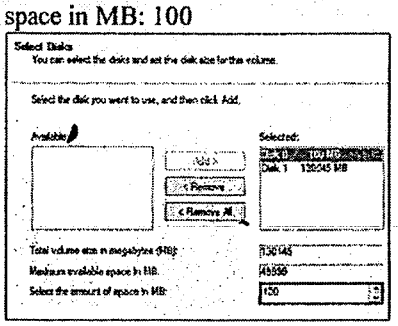
B1 - Gắn Disk0 vào máy ảo. Vào Disk Management → Chuột phải lên disk 1 chọn Remove Mirror

B2 - Chuột phải lên vùng Unallocated tên disk0 → Chọn New Spanned Volume

B3 - Màn hình Welcome → Chọn Next

B4 - Màn hình Select Disks → khung bên trái chọn Disk1 → Chọn Add. Sau đó chọn Disk 0 → Add

B5 - Chọn Disk0 → Select the amount of space in MB: 100



B6 - Chọn Disk1 → Select the amount of space in MB: 200 → Next

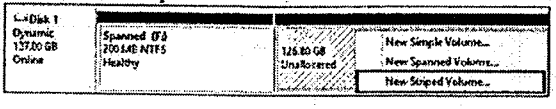
B7 - Màn hình Assign Drive Letter or Path → Next

B8 - Đặt tên partition là Spanned → Đánh dấu chọn vào ô Perform a quick format → Next → Finish

B9 - Kiểm tra: Mở File Explorer thấy xuất hiện Spanned Partition có dung lượng là 300 MB

d. Striped

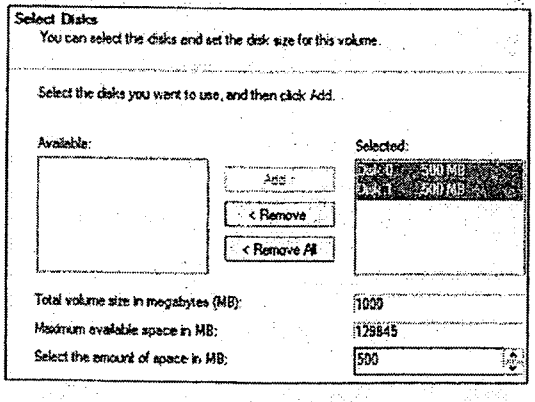
B1 - Chuột phải lên vùng unallocated của disk0 → Chọn New striped volume



B2 - Màn hình Welcome → chọn Next

B3 - Màn hình Select Disk → khung bên trái chọn Disk 1 → Add. Sau đó chọn Disk 0 → Add

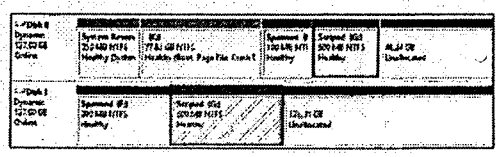
B4 - Chọn dung lượng sẽ lấy để tạo partition trên 2 ổ đĩa vật lí : Select the amount of space in MB : 500 → Next



B5 - Chọn ký tự ổ đĩa G: → Next

B6 - Đặt tên partition là Striped → Chọn ô Perform a quick format → Next → Finish

B7 - Quan sát tạo partition thành công (phần vùng màu xanh)



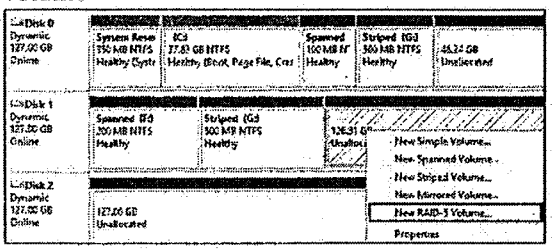
B8 - Kiểm tra: Mở File Explorer, kiểm tra dung lượng Striped partition vừa tạo: 1000 MB

e. Raid 5

- Xóa hết các partition đã tạo (trừ partition chứa hệ điều hành)

- Gắn đĩa số 3 vào máy ảo

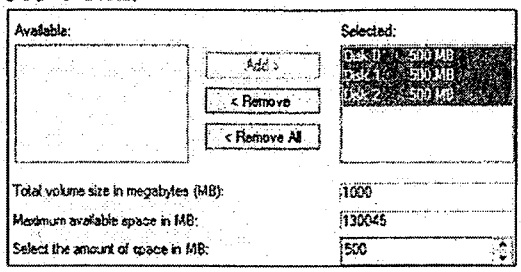
B1 - Khởi động máy ảo → Vào Disk Management → Chuột phải lên vùng Unallocated trên disk1 → Chọn New RAID-5 volume



B2 - Màn hình Welcome → Chọn Next

B3 - Màn hình Select Disks → Khung bên trái chọn Disk1 và Disk2 → Add

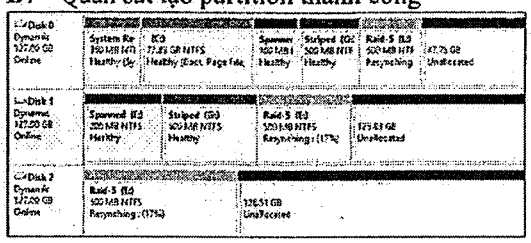
B4 - Chọn dung lượng partition trên cả 3 disk: 500 → Next



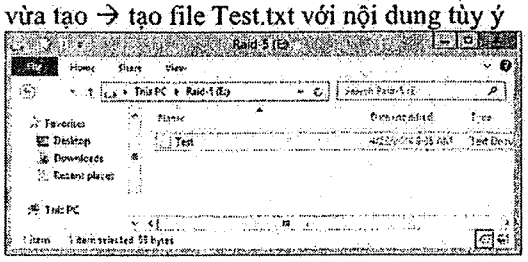
B5 - Chọn ký tự ổ đĩa G: → Next

B6 - Đặt tên partition là Raid-5 → Đánh dấu chọn vào ô Perform a quick format → Next → Finish

B7 - Quan sát tạo partition thành công



B8 - Kiểm tra: Mở File Explorer → Mở partition vừa tạo → tạo file Test.txt với nội dung tùy ý



B9 - Tắt máy ảo, gỡ Disk1 ra khỏi máy ảo

B10 - Khởi động máy ảo → vẫn truy xuất được file

Lưu ý: sau khi gắn trả Disk 1 về máy ảo : Mở Disk Management → Chuột phải lên partition của RAID – 5 → Chọn Reactive để đồng bộ dữ liệu lại.

LOCAL STORAGE – PHẦN 2

CÁC BƯỚC TRIỂN KHAI

1. Tạo Storage Pool

2. Tạo Virtual Disk

3. Tạo Volume

4. Kiểm tra

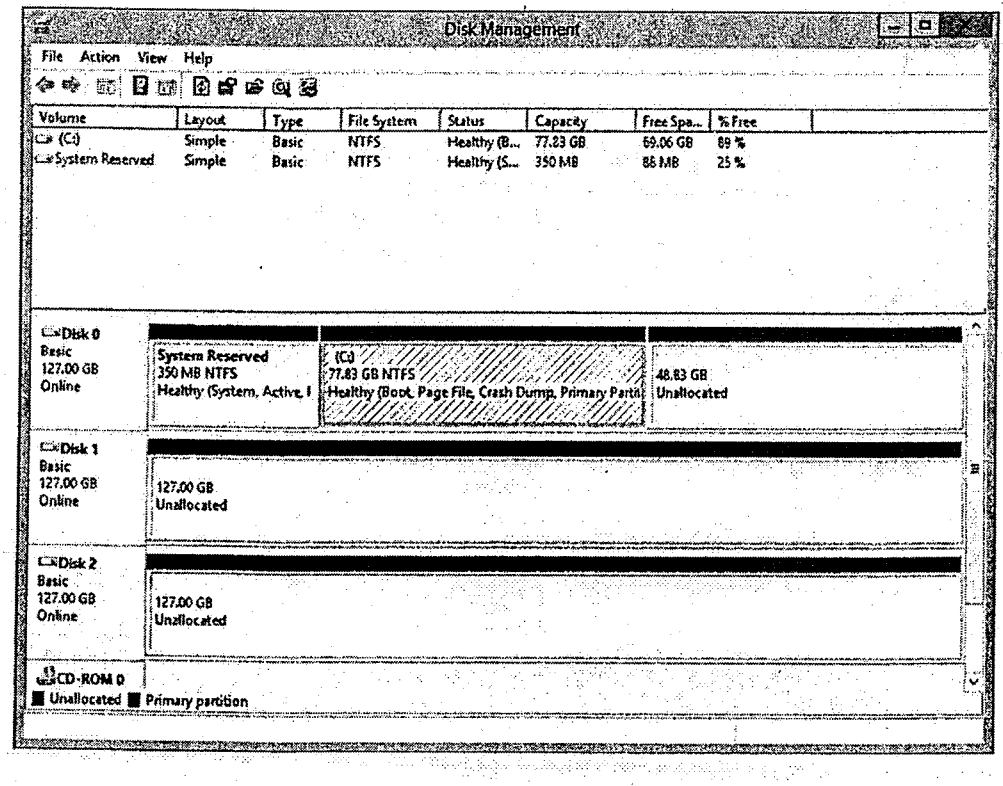
A- CHUẨN BỊ

Mô hình bài lab bao gồm 2 máy

- PC01: Windows Server 2012 R2

- PC02: Windows 8.1

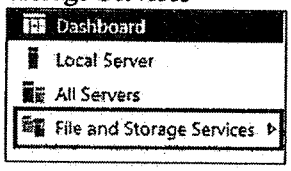
- Gắn thêm 2 đĩa cứng ảo Disk1 và Disk2 vào máy PC01



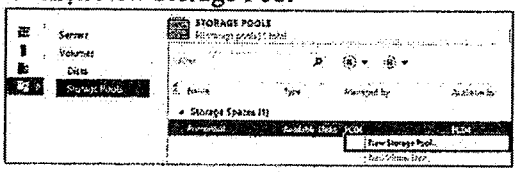
B- THỰC HIỆN

1. Tạo Storage Pool

B1 - Mở Server Manager → chọn File and Storage Services

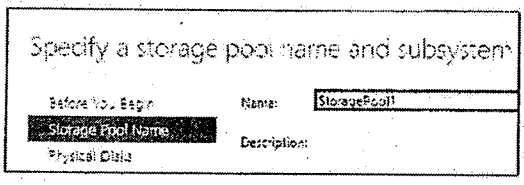


B2 - Trong khung Server nằm ở góc trái → chọn Storage Pools → Chuột phải vào khoảng trống → chọn New Storage Pool

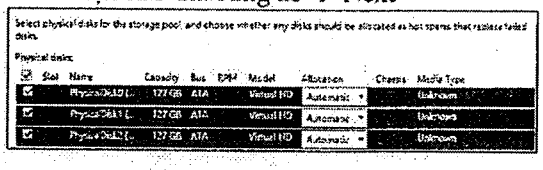


B3 - Màn hình Before you begin → Next

B4 - Ở khung Name, đặt tên: StoragePool1 → Next



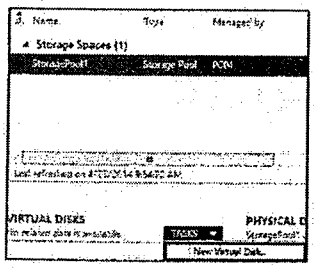
B5 - Chọn cả 3 đĩa cứng ảo → Next



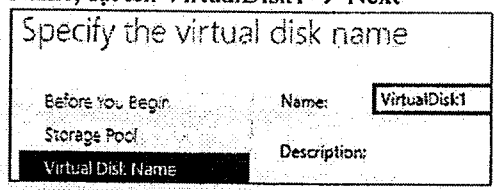
B6 - Nhấn Create để tạo mới → Close.

2. Tạo Virtual Disk

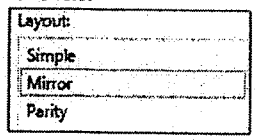
B1 - Chọn Storage Pool 1 → Ở khung Virtual Disks → menu Tasks → chọn New Virtual Disk



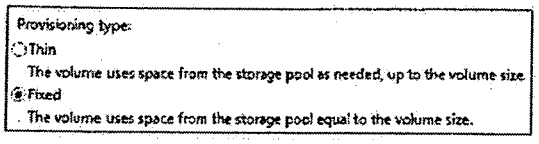
B2 - Các bước đầu tiên nhấn Next theo mặc định → Màn hình Virtual Disk Name → ở mục Name, đặt tên VirtualDisk1 → Next



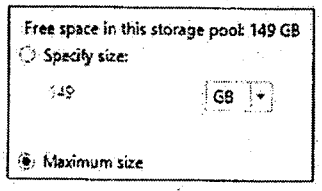
B3 - Màn hình Storage Layout → chọn Mirror → Next



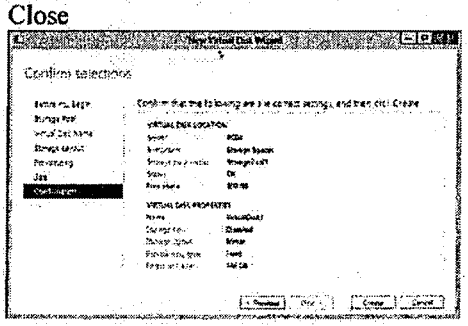
B4 - Màn hình Provisioning → chọn Fixed → Next



B5 - Màn hình Size → chọn Maximum size → Next

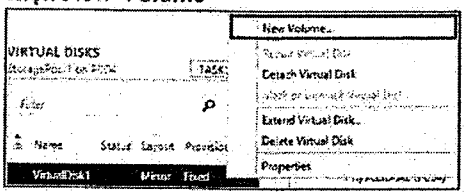


B6 - Màn hình Confirmation → Create → Close



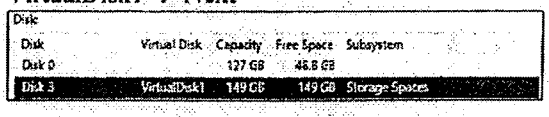
3. Tạo Volume

B1 - Chuột phải vào VirtualDisk1 vừa tạo → chọn New Volume

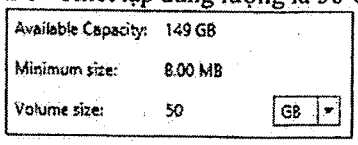


B2 - Màn hình Before you begin → Next

B3 - Màn hình Server and Disk → chọn VirtualDisk1 → Next

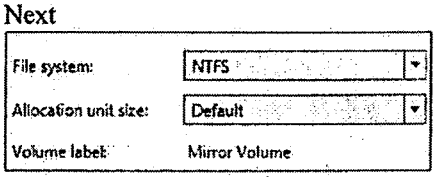


B4 - Thiết lập dung lượng là 50 GB → Next



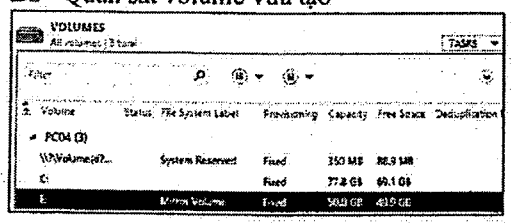
B5 - Màn hình Drive Letter or folder, chọn ký tự ổ đĩa → Next

B6 - Đặt tên cho Volume là: Mirror Volume → Next



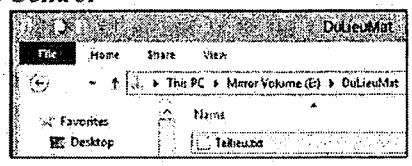
B7 - Màn hình Confirmation → nhấn Create → Close

B8 - Quan sát volume vừa tạo



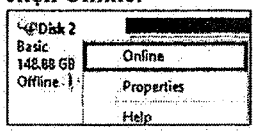
4. Kiểm tra

B1 - Mở File Explorer, tạo thư mục DuLieuMat trên volume vừa tạo, sau đó tạo file Tailieu.txt trong thư mục này. Share Everyone – Full Control

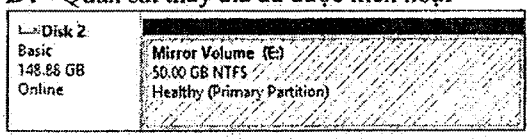


B2 - Gỡ Disk 1 ra khỏi máy ảo

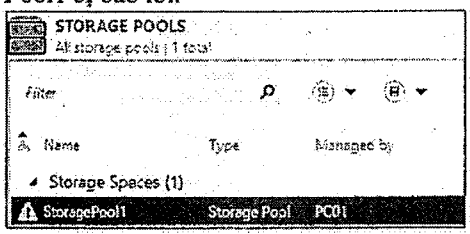
B3 - Khởi động lại máy, vào Disk Management → chuột phải vào Disk 2 → chọn Online.



B4 - Quan sát thấy đĩa đã được kích hoạt



B5 - Mở Server Manager → chọn File and Storage Services → kiểm tra thấy Storage Pool1 bị báo lỗi.



B6 - Trên máy PC02 → truy cập vào máy PC01 → Dữ liệu vẫn đọc bình thường.