

QUẢN TRỊ MẠNG – THỰC HÀNH

01. Cài đặt printer server (1 máy Windows Server 2008 + 1 máy client Windows XP)

- Windows Server 2008:

- + IP address: 192.168.50.1
- + Subnet mask: 255.255.255.0
- + Preferred DNS server: 192.168.50.1

- Windows XP:

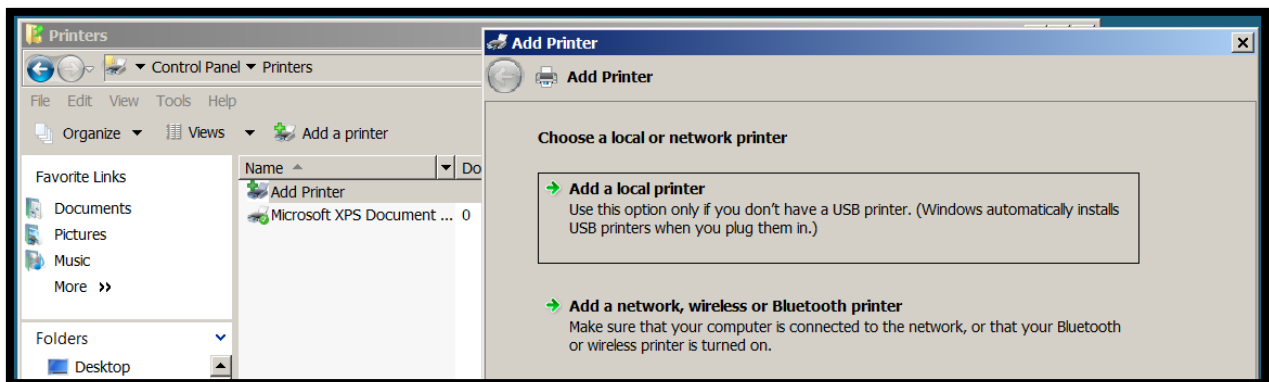
- + IP address: 192.168.50.2
- + Subnet mask: 255.255.255.0
- + Preferred DNS server: 192.168.50.1

The screenshot shows the 'Use the following IP address' section with the following values:
IP address: 192 . 168 . 50 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .
Below this, the 'Obtain DNS server address automatically' option is unselected, and the 'Use the following DNS server addresses' section is selected with the following values:
Preferred DNS server: 192 . 168 . 50 . 1
Alternate DNS server: . . .

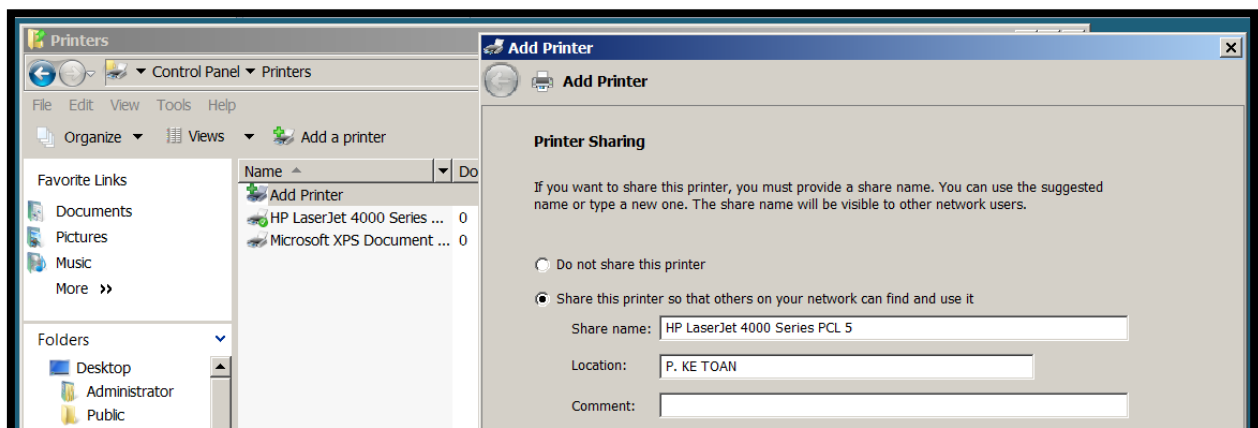
(Yêu cầu các máy phải có cùng card mạng (VMnet 1),
đã tắt tường lửa và có thể ping được cho nhau)

Thực hiện:

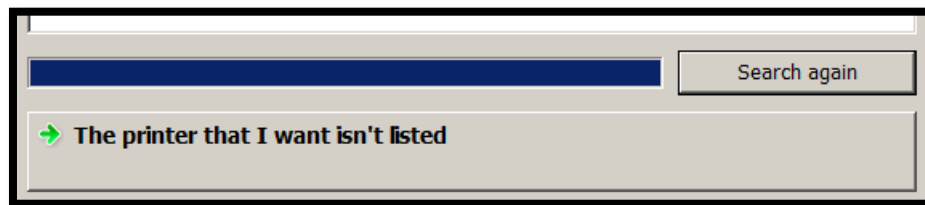
- Windows Server 2008: Control Panel → Printers → Add Printer → Add a local printer



- Use an existing port: LPT1: (Printer Port) → Next → HP LaserJet 4000 Series PCL 5
- Next → Printer name để mặc định → Next → Location: P. KE TOAN → Next → Finish



→ Add Printer (lần 2) → Add a network,... → Stop → The printer that I want isn't listed



→ Add a printer using a TCP/IP address... → Next → Host or IP address: 192.168.50.200

A screenshot of the 'Type a printer hostname or IP address' dialog box. It contains the following fields: 'Device type' set to 'Autodetect', 'Hostname or IP address' set to '192.168.50.200', and 'Port name' set to '192.168.50.200'. At the bottom, there is a checked checkbox labeled 'Query the printer and automatically select the driver to use'.

→ Next → Custom → Next

→ HP Color LaserJet 5500 PCL 6

→ Next → Next

→ Finish (hoàn thành máy in thứ 2)

| | | | |
|-------------|-------------------------------|---|-------|
| Add Printer | | | |
| | HP Color LaserJet 5500 PCL 6 | 0 | Ready |
| | HP LaserJet 4000 Series PCL 5 | 0 | Ready |
| | Microsoft XPS Document Writer | 0 | Ready |

→ Add Printer (lần 3)

→ Add a local printer

→ Create a new port

→ Type of port:

Standard TCP/IP Port

→ Next

A screenshot of the 'Choose a printer port' dialog box. It includes a text box explaining: 'A printer port is a type of connection that allows your computer to exchange information with a printer.' There are two radio buttons: 'Use an existing port:' (selected) with a dropdown menu showing 'LPT1: (Printer Port)', and 'Create a new port:' (unselected). Below the 'Create a new port' option, there is a 'Type of port:' label and a dropdown menu showing 'Standard TCP/IP Port'. A list of port types is displayed below the dropdown: 'Local Port', 'Standard TCP/IP Port' (highlighted), and 'ThinPrint Print Port Monitor for VMWare'.

→ Host or IP address:

192.168.50.201

→ Next

→ Custom

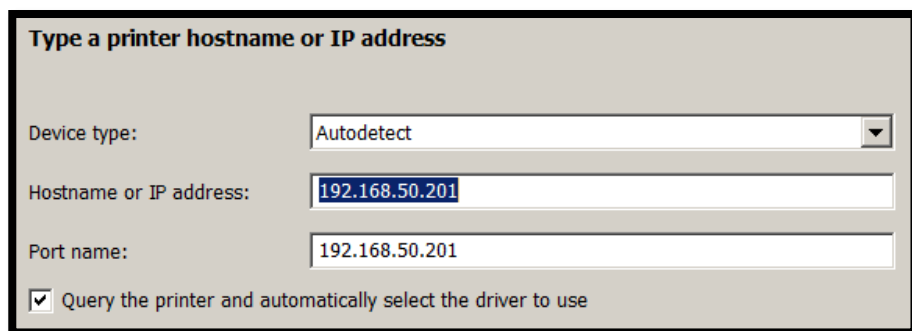
→ Setting

→ SNMP Status Enabled

→ OK → Next

→ HP LaserJet 2200

Series PCL 5 → Next → Next → Next → Finish (hoàn thành máy in thứ 3)



Type a printer hostname or IP address

Device type: Autodetect

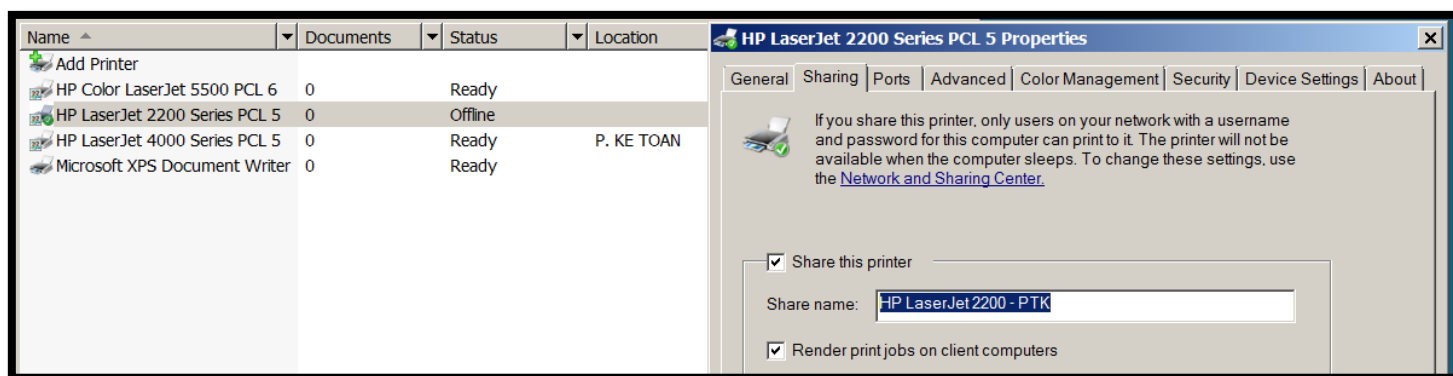
Hostname or IP address: 192.168.50.201

Port name: 192.168.50.201

☒ Query the printer and automatically select the driver to use

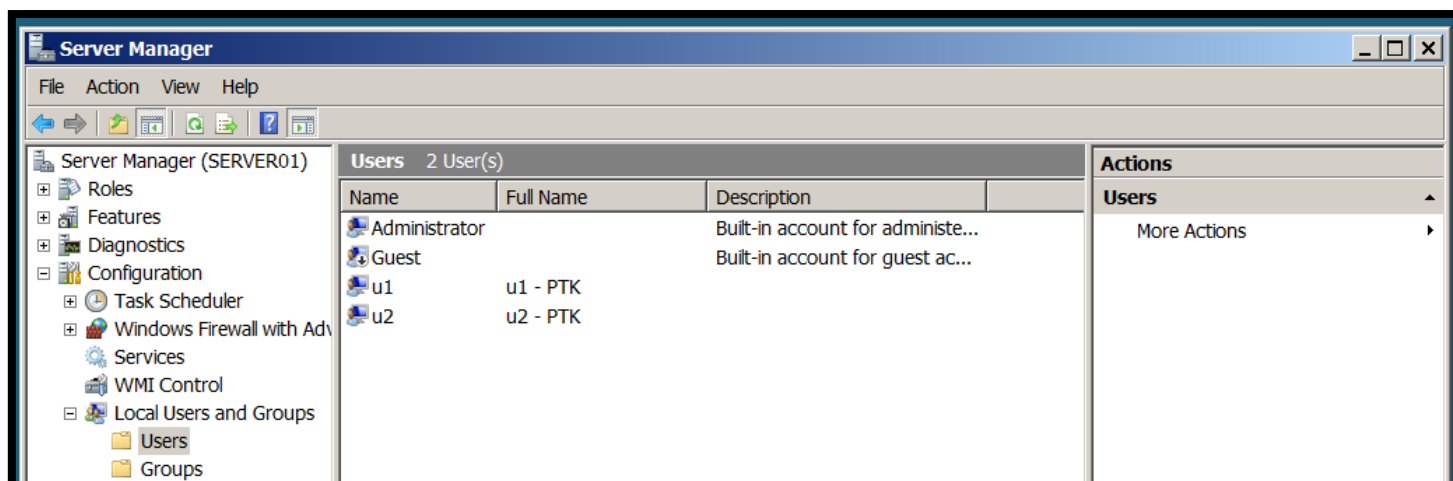
→ Chuột vào HP LaserJet 2200 Series PCL 5 → Properties → Chuyển sang tab Sharing

→ Đổi tên máy thành HP LaserJet 2200 – PTK → OK



→ Tạo 2 user (u1, u2 - PTK) để kiểm tra: Chuột phải vào Computer → Manage (mở Server Manager) → Configuration → Local Users and Groups → Users → New User...

(Lưu ý: phải tạo user có mật khẩu)



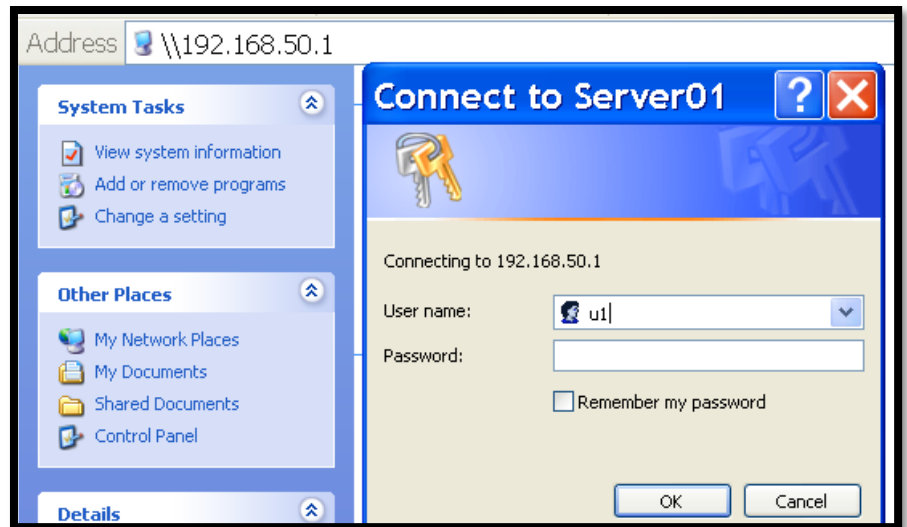
- Windows XP:

Đăng nhập vào máy client

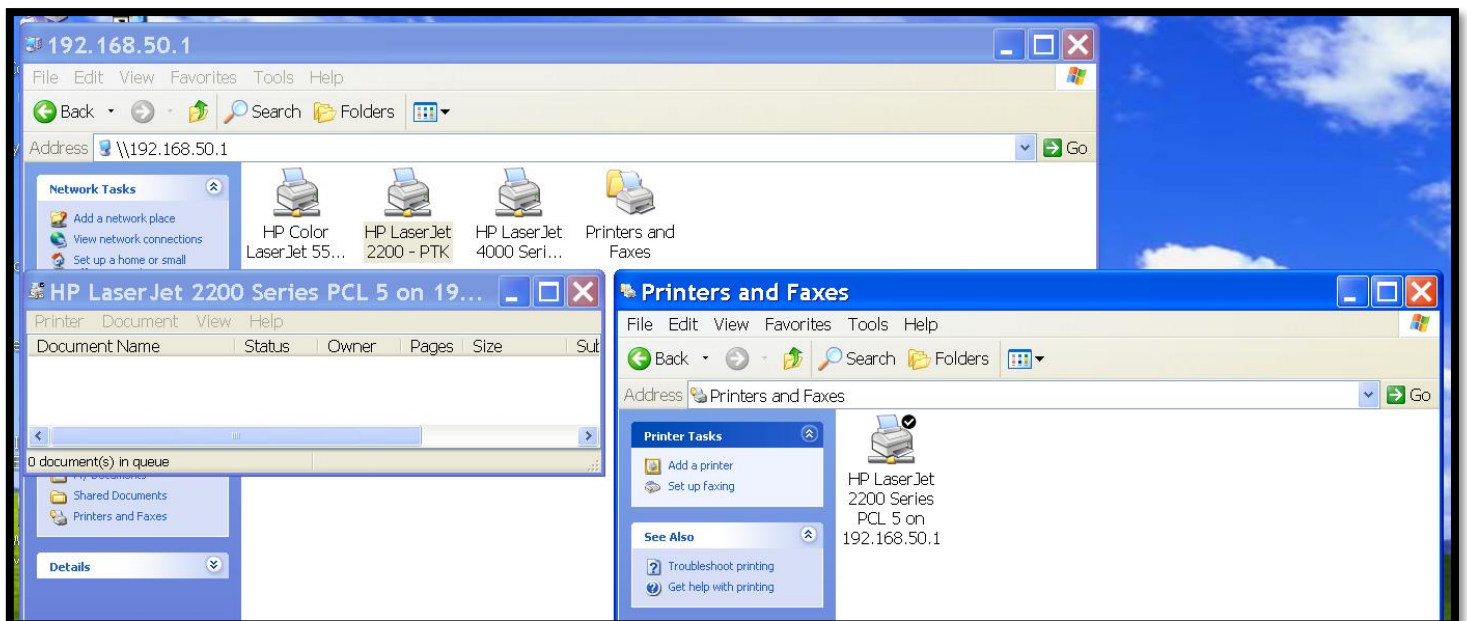
→ Windows Explorer

→ Gõ \\192.168.50.1

→ Lần lượt đăng nhập vào bằng u1 và u2



→ Nhấp đúp vào HP LaserJet 2200 Series PCL 5 → Yes



(Kết quả)

02. Cấu hình group permission (1 máy Windows Server 2008 + 1 máy client Windows XP)

(Yêu cầu các máy phải có cùng card mạng (VMnet 1),
đã tắt tường lửa và có thể ping được cho nhau)

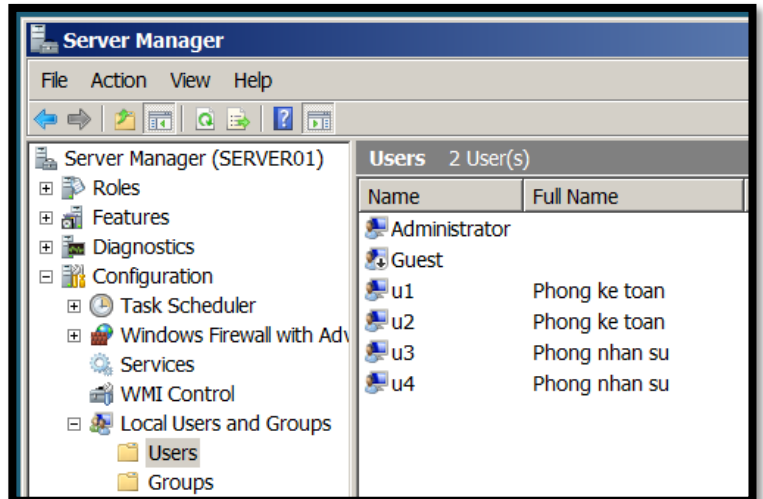
Thực hiện:

- Windows Server 2008:

Tạo ra 4 user (u1, u2, u3 và u4):

- Chuột phải vào Computer
- Manage (mở Server Manager)
- Configuration
- Local Users and Groups
- Users
- New User...

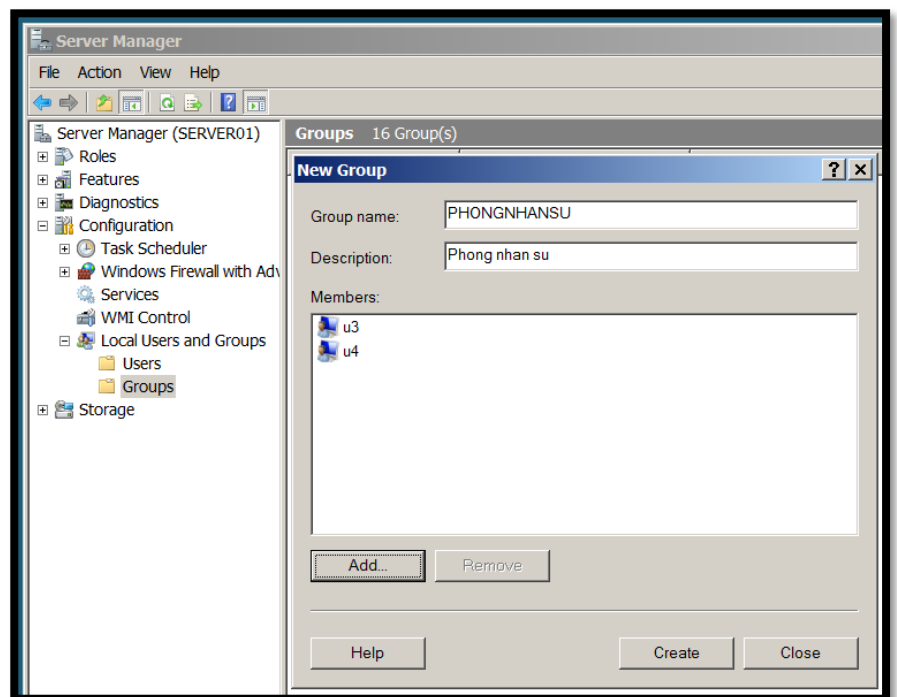
(Lưu ý: phải tạo user có mật khẩu)



Tạo ra 2 group

(PHONGKETOAN và PHONGNHANSU):

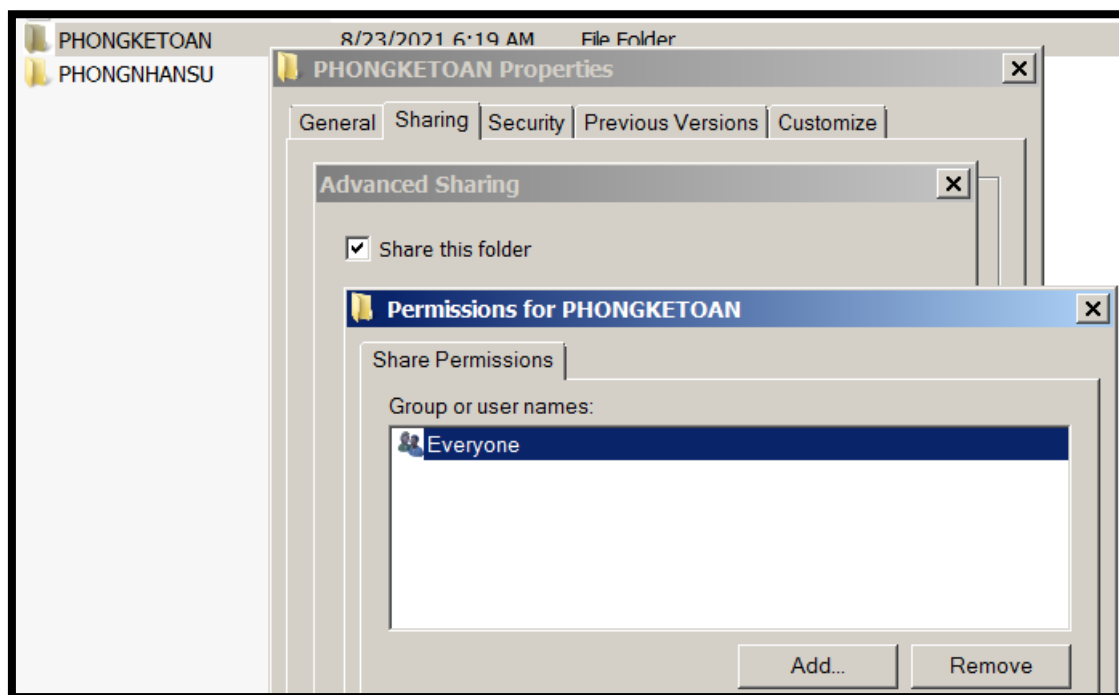
- Chuột phải vào Computer
- Manage (mở Server Manager)
- Configuration
- Local Users and Groups
- Groups
- New Group...
- Tạo các group PHONGKETOAN và PHONGNHANSU



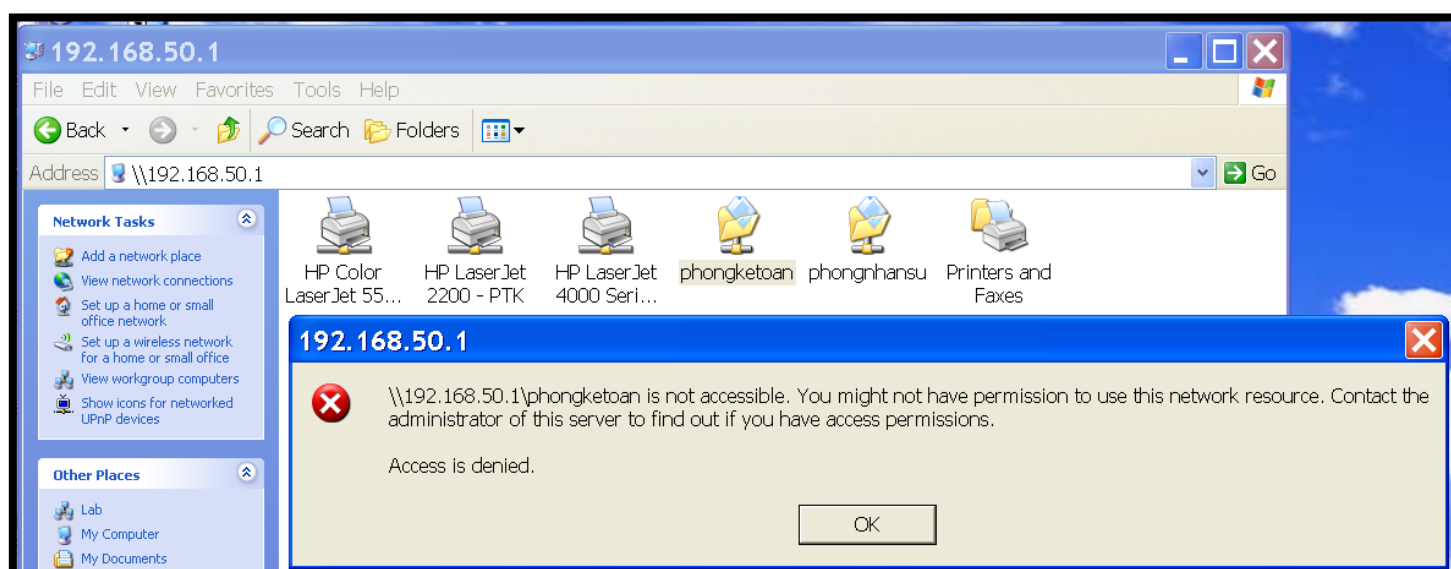
- Thêm u1, u2 vào group PHONGKETOAN → Thêm u3, u4 vào group PHONGNHANSU

Tạo 2 thư mục PHONGKETOAN và PHONGNHANSU trên ổ đĩa C

- Chuột phải vào thư mục PHONGKETOAN → Properties → Chuyển sang tab Sharing
- Advanced Sharing... → Tích chọn “Share this folder” → Permissions
- Remove “Everyone” → Add group PHONGKETOAN vào → Gán quyền Change + Read
- Thực hiện tương tự với PHONGNHANSU



- **Windows XP:** Đăng nhập vào máy client → Windows Explorer → Gõ \\192.168.50.1
→ Lần lượt đăng nhập bằng u1, u2, u3 và u4 để thử nghiệm



(u3 – PHONGNHANSU không có quyền truy cập vào thư mục của PHONGKETOAN)

03. Nâng cấp máy chủ miền (Domain Controller), kết nối máy vào domain, Share & NTFS Permissions (1 máy Windows Server 2008 + 2 máy client Windows XP)

(Yêu cầu các máy phải có cùng card mạng (VMnet 1), đã tắt tường lửa, có thể ping được cho nhau và trỏ DNS về địa chỉ IP của máy Server)

Use the following IP address:

IP address: 192 . 168 . 50 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 50 . 1

Alternate DNS server: . . .

Use the following IP address:

IP address: 192 . 168 . 50 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 50 . 1

Alternate DNS server: . . .

Thực hiện:

- **Windows Server 2008:** Nâng cấp máy chủ miền (Domain Controller)
 - Mở hộp thoại Run → dcpromo → Tích chọn “Use advanced mode installation”
 - Next → Next → Create a new domain...
 - FQDN of the forest root domain: test.pro → Next → Domain NetBIOS name: TEST
 - Next → Forest functional level: Windows Server 2003 → Next → Next → Next
 - Yes → Next
 - Password **(nên đặt đơn giản vì sau khi khởi động lại sẽ phải đổi password mới)**
 - Next → Next → Tích chọn “Reboot on completion”
 - Tiến hành đổi mật khẩu sau khi khởi động lại

Computer name, domain, and workgroup settings

Computer name: Server01

Full computer name: Server01.test.pro

Computer description:

Domain: test.pro

[Change settings](#)

- **Windows XP:** Kết nối máy khách vào Domain Controller
 - My Computer → Properties → Chuyển sang tab Computer Name → Change
 - Domain: test.pro → OK
 - Nhập tài khoản, nếu chưa tạo thì nhập tài khoản administrator của máy server (2008)

- **Windows Server 2008:** Tạo OU (Organizational Unit), Group, user

Tắt tính năng yêu cầu mật khẩu phức tạp:

Administrative Tools → Group Policy Management → Forest: tên domain (test.pro)

→ Domains → Tên domain (test.pro) → Default Domain Policy → OK

→ Chuột phải vào Default Domain Policy → Edit

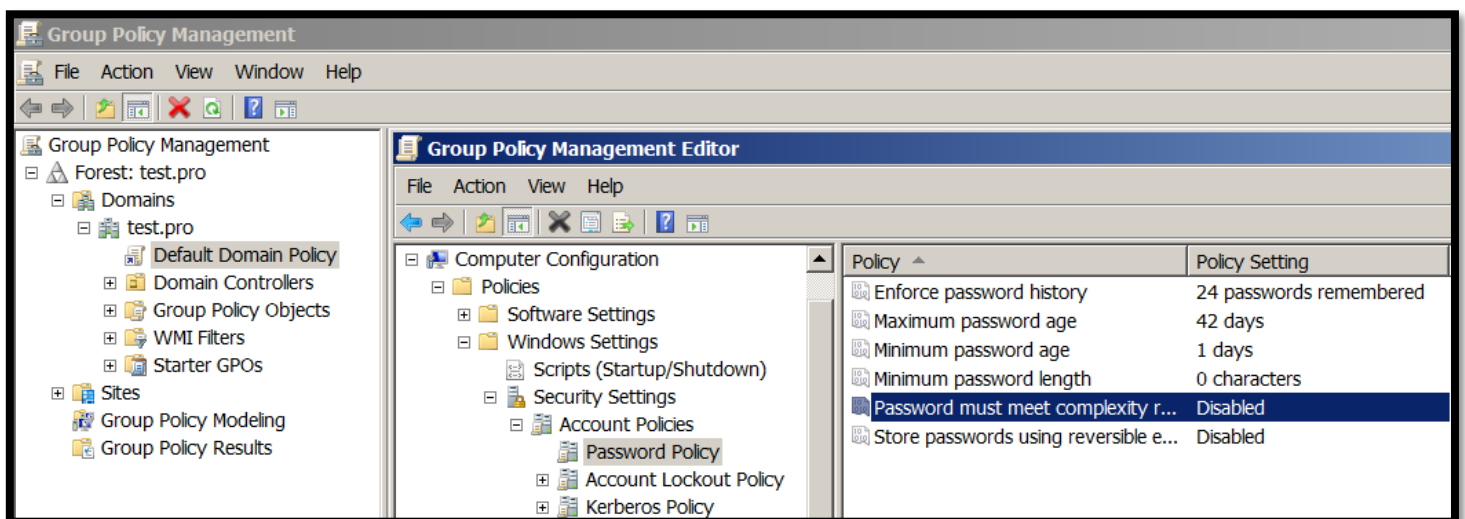
→ Công cụ Group Policy Management Editor sẽ hiện ra → Computer Configuration

→ Policies → Windows Settings → Account Policies → Password Policy

→ Password must meet complexity requirements → Disable

→ Minimum password length có thể chỉnh về 0 characters nếu muốn

→ Mở hộp thoại Run → gpupdate /force



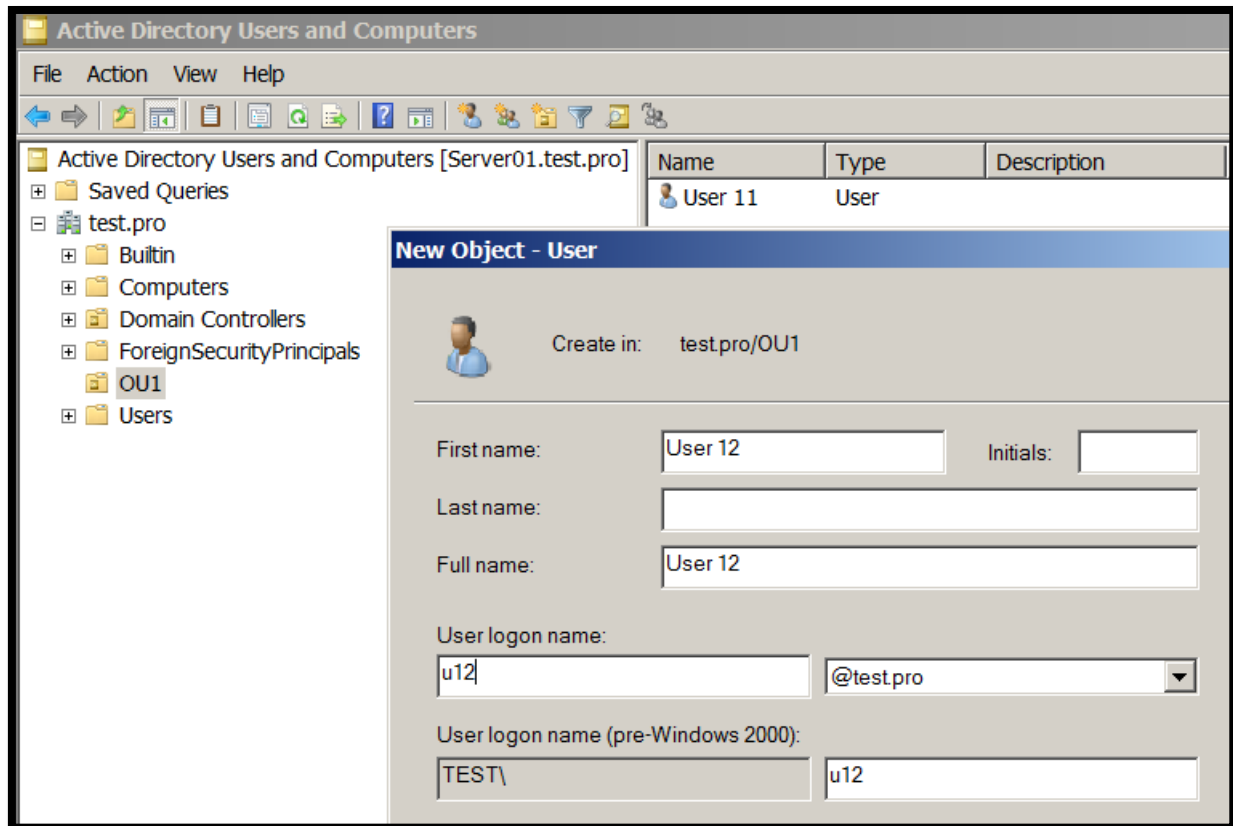
Tạo OU1, OU2, u11, u12, u21, u21:

Administrative Tools → Active Directory Users and Computers

→ Chuột phải vào tên domain (test.pro) → New → Organizational Unit → Tạo OU1

→ Trong OU1, chuột phải → New → User → Tạo u11, u12 thuộc OU1

→ Tương tự với OU2



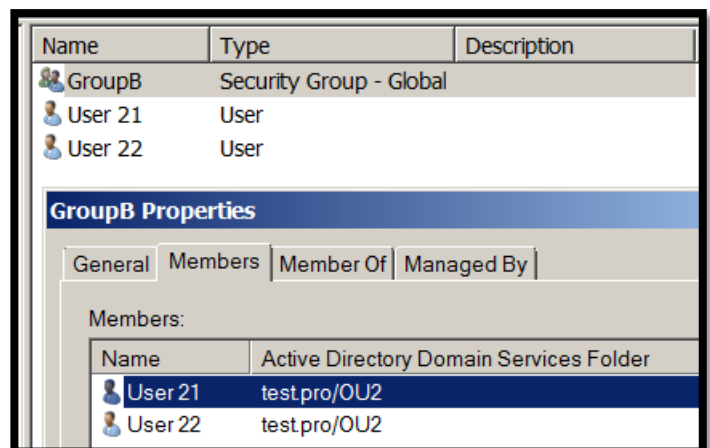
Tạo GroupA, GroupB:

→ Trong OU1, chuột phải

→ New → Group → Tạo GroupA

→ Thêm u11, u12 vào GroupA

→ Tương tự với GroupB



Thêm các Group vào các nhóm của hệ thống (Operators):

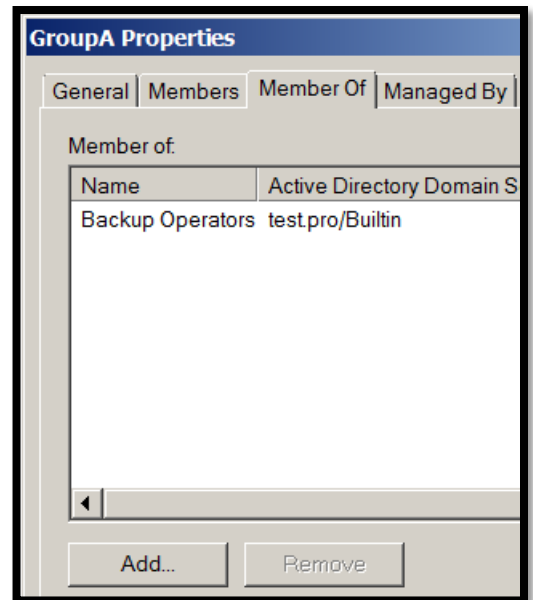
Chuột phải vào GroupA

→ Properties

→ Chuyển sang tab Member Of

→ Add

→ Tương tự với GroupB



Tạo thêm ổ đĩa cho máy Windows Server 2008:

Chuột phải vào tên máy ở ngoài VMware Workstation → Settings... → Add → Hard Disk

→ Next → SCSI (Recommended) → Next → Create a new virtual disk → Next

→ Chọn kích thước tối đa → Split virtual disk into multiple files → Next → Finish

Định dạng cho ổ đĩa vừa tạo: Tại máy Windows Server 2008, chuột phải vào Computer

→ Manage → Storage → Disk management → Initialize Disk: OK

→ Mặc định ổ D: ở máy ảo là ổ đĩa DVD, chuột phải vào ổ D

→ Change Drive Letter and Paths... → Change...

→ Assign the following drive letter: chọn E hoặc bất kỳ ký tự nào khác

(Khuyến cáo: tránh chọn X, Y, Z vì những ổ này dùng cho những việc khác) → Yes

→ Chuột phải ổ đĩa vừa tạo (đang Unallocated) → New Simple Volume... → Next

→ Next → Assign the following drive letter: D hoặc bất kỳ ký tự nào khác mà đề yêu cầu

→ Next → Volume label: Data → Perform a quick format → Next → Finish

Tạo thư mục và gán quyền:

Trong ổ đĩa D, tạo hai thư mục **Applications** và **Public**, trong Public có **Public1** và **Public2**

Thư mục **Applications** và **Public2** gán theo hướng dẫn

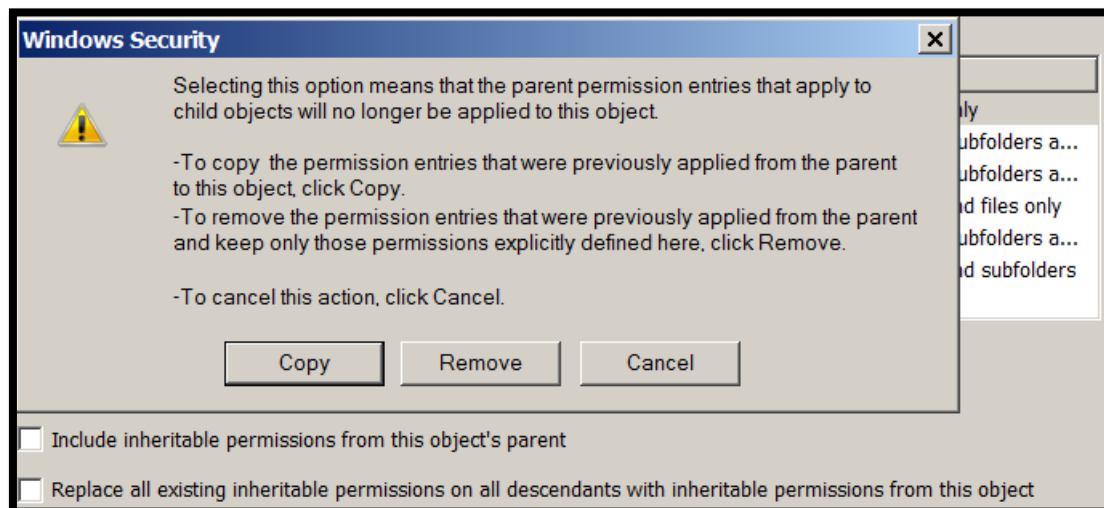
Thư mục **Public**

→ Properties
→ Sharing
→ Advanced Sharing...
→ Tích chọn Share this folder
→ Permissions
→ Thêm quyền Change cho Everyone → OK

→ Chuyển sang tab Security → Edit → Thêm quyền Write cho Users

Thư mục **Public1** → Security → Edit → Add → GroupA
→ Thêm quyền Write cho GroupA → OK

Chỉnh sửa quyền cho Users ở Public1 và Public2: Security → Advanced → Edit
→ Bỏ chọn "Include inheritable permissions from this object's parent" → Copy → OK
→ Edit → Users → Tắt quyền Write của Users để các user chỉ có thể xem nội dung trong **Public1** và **Public2** mà không được phép tạo thư mục mới → OK



- **Windows XP:** Đăng nhập vào các u11, u12, u21 và u22 để kiểm tra quyền.

04. Thiết lập Home Folder - Offline files Windows server, user Domains

(1 máy Windows Server 2008 + 2 máy client Windows XP)

(Cấu hình card mạng, địa chỉ IP, DNS, thêm ổ đĩa, tạo Domain Controller, kết nối máy Client vào Domain và tạo OU, user, group,... tương tự như các bước ở trên)

Thiết lập Home folder:

- **Windows Server 2008:** Tạo thư mục HOME trên ổ đĩa D → Properties → Sharing → Advanced Sharing... → Tích chọn Share this folder → Permissions → Gán Full Control cho Everyone → OK

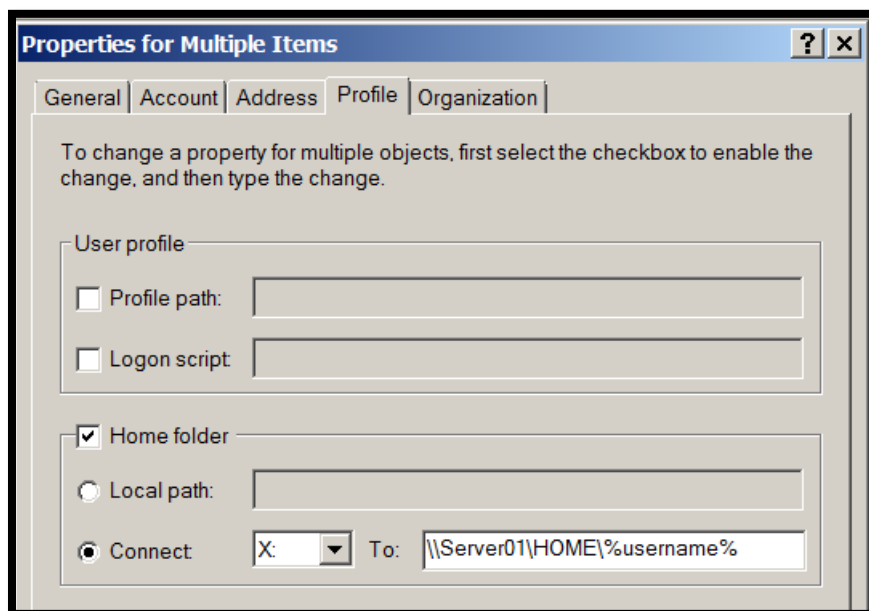
Chuyển sang tab Security → Tắt kế thừa → Xoá Users → Thêm các user được yêu cầu → Gán Full Control cho các user vừa được thêm vào

Administrative Tools → Active Directory Users and Computers

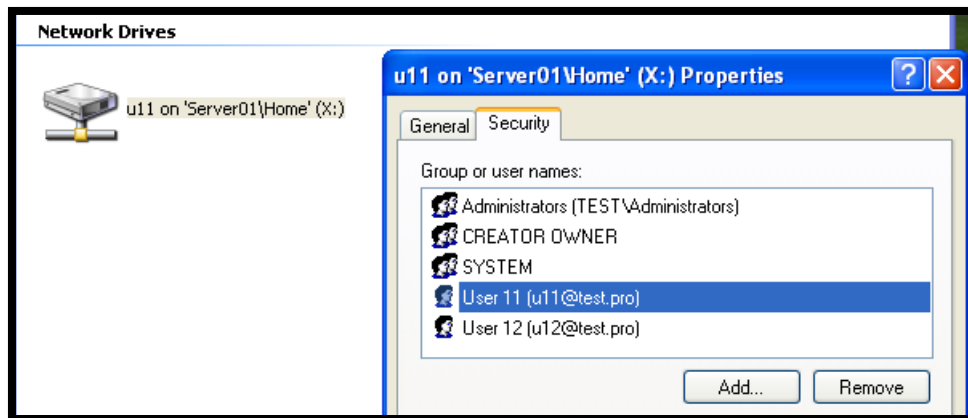
→ Bôi đen các user cần tạo Home folder → Properties → Profile

→ Tích chọn Home folder → Connect → Chọn ổ đĩa để tạo Home folder cho từng user

→ Nhập đường dẫn “\\TÊN SERVER hoặc ĐỊA CHỈ IP\TÊN THƯ MỤC\%username%” để tự động tạo folder cho các user (Ví dụ: \\Server01\HOME\%username%)



- **Windows XP:** Đăng nhập vào các user đã được cấu hình Home folder để kiểm tra xem đã có ổ đĩa mạng Home chưa, tạo và xoá thư mục, tập tin để kiểm tra quyền



(Thiết lập thành công Home folder)

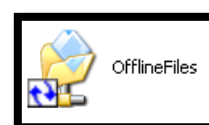
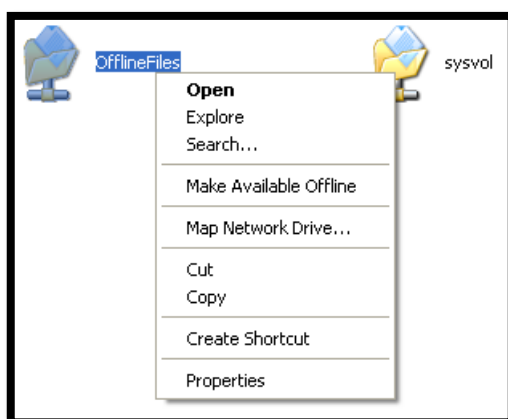
Thiết lập Offline Files:

- **Windows Server 2008:** Tạo thư mục OfflineFiles trên ổ đĩa D → Properties → Sharing → Advanced Sharing... → Tích chọn Share this folder → Permissions → Xoá Everyone → Thêm Domain Users → Gán quyền Change → Thêm các Group → Gán Full Control

Chuyển sang tab Security → Tắt kế thừa → Xoá Users

→ Thêm Domain Users và các Group → Gán Full Control cho các Group

- **Windows XP:** Đăng nhập vào các user đã tạo ở DC → Nhập \\192.168.50.1 → Nhấn chuột phải vào thư mục OfflineFiles → Make Available Offline → Next → Tích chọn "Automatic synchronize..." → Next → Create a shortcut → Finish



(Có thể login bằng tài khoản admin để disable card mạng và dùng 2 máy client để test)

05. Thiết lập roaming profiles, mandatory profile users domain

(1 máy Windows Server 2008 + 2 máy client Windows XP)

(Cấu hình card mạng, địa chỉ IP, DNS, thêm ổ đĩa, tạo Domain Controller, kết nối máy Client vào Domain và tạo OU, user, group,... tương tự như các bước ở trên)

Roaming profile:

- **Windows Server 2008:** Tạo thư mục PROFILES:

Share permission: Domain Users – Full

NTFS permission: Domain Users – Modify

(Nếu không thiết lập hoặc thiết lập thiếu quyền sẽ không thể roaming profiles được)

Administrative Tools

→ Active Directory Users and Computers

→ Bôi đen các user cần

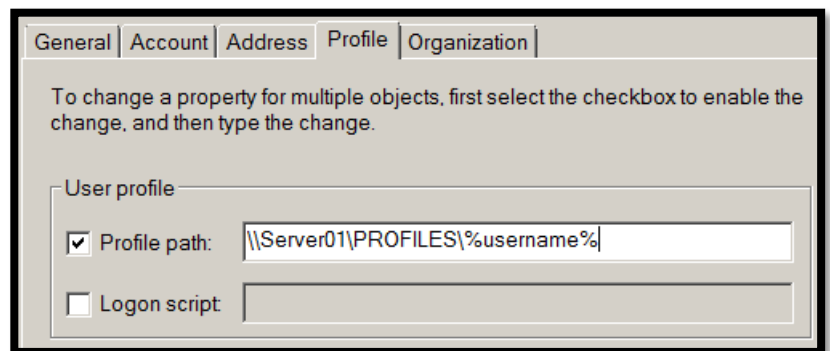
Roaming profile

→ Properties

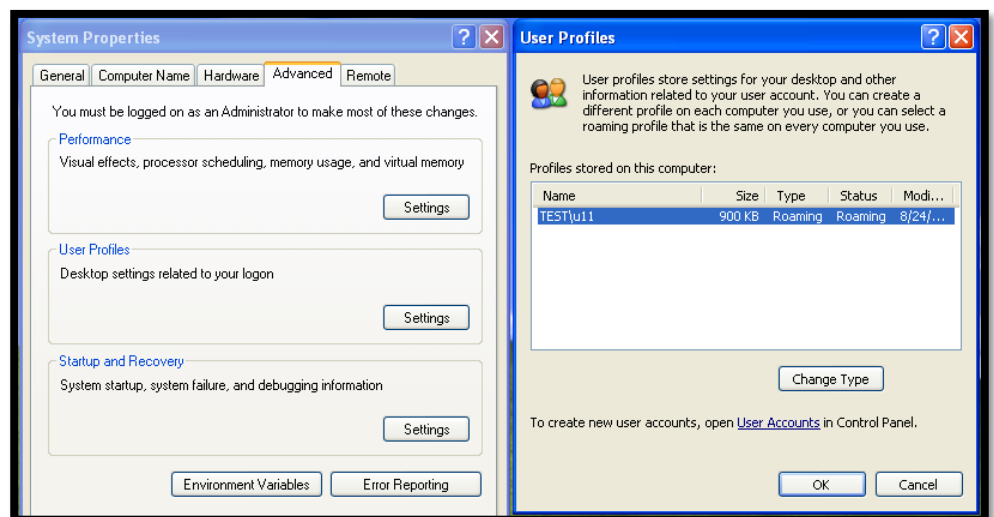
→ Profile

→ User profile

→ Profile path: (Ví dụ: \\Server01\PROFILES\%username%)



- **Windows XP:** Đăng nhập vào user đã được roaming
→ Tạo thư mục, tập tin trong My Documents
→ Đăng xuất
→ Đăng nhập lại để xem loại tài khoản và kiểm tra những thư mục, tập tin



trong My Documents mà user đó đã tạo:

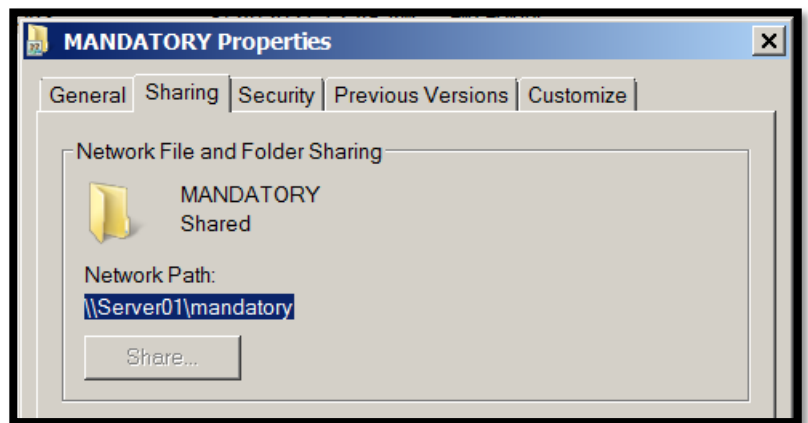
My Computer → Properties → Advanced → User Profiles → Settings → Type, Status

Mandatory profile:

- **Windows Server 2008:** Tạo thư mục MANDATORY:
Share permission: Domain Users – Full
NTFS permission: Domain Users – Modify
- **Windows XP:** Các user cần Mandatory phải từng đăng nhập vào máy Client, nên lấy một user sạch để làm chuẩn

→ Đăng nhập bằng tài khoản admin

→ Sang máy DC sao chép đường dẫn mạng bằng cách vào thư mục MANDATORY → Properties
→ Sharing → Network Path
→ Sao chép đường dẫn mạng “\\Server01\mandatory”



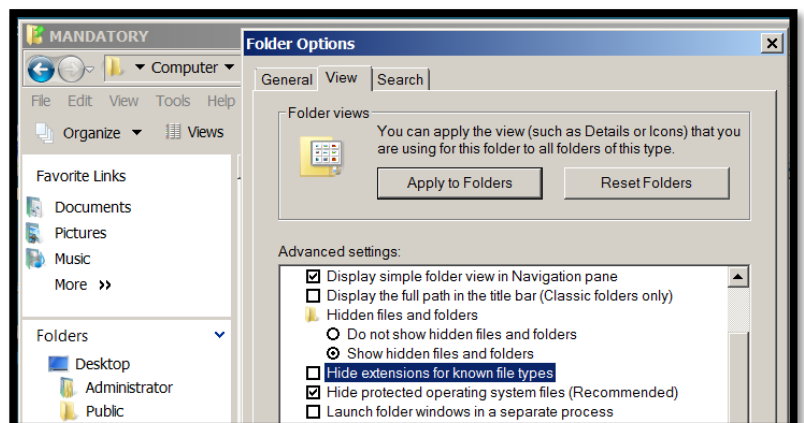
Trở lại máy Client → Mở hộp thoại Run → Dán “\\Server01\mandatory” vào
→ Đăng nhập bằng một user sạch để lấy thông tin mặc định

Tiến hành Mandatory: My Computer → Properties → Advanced → User Profiles
→ Settings → Chọn user đang Roaming → Copy to → Dán “\\Server01\mandatory” vào
→ OK → Yes → OK

- **Windows Server 2008:** Lúc này, trong folder MANDATORY sẽ có profile của user sạch vừa đăng nhập vào

Hiện thư mục ẩn và hiện phần mở rộng của tập tin:

Vào Windows Explorer → Tools
→ Folder Options... → View
→ Chọn “Show hidden files and folders”
→ Bỏ chọn “Hide extensions for known file types”



Vào thư mục MANDATORY → Đổi phần mở rộng ntuser.dat -> ntuser.man → Yes

Roaming tiếp các user khác để thử nghiệm → Đăng nhập các user mới, đã Roaming vào máy Client → Đăng xuất khỏi máy Client

Chiếm lại quyền truy cập vào folder PROFILES (folder lưu thông tin của máy cần Mandatory):

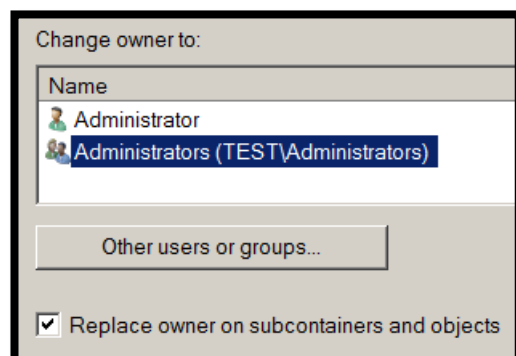
Sang máy DC → Vào thư mục PROFILES

→ Chuột phải vào user mới, đã Roaming

→ Security → Continue → Change owner to:

Administrator (TEST\ Administrators)

→ Tích chọn “Replace owner on subcontainers and objects” → OK → Yes → OK → OK



Vào lại thư mục PROFILES → Security → Thêm user cần Roaming với quyền Full Control

→ Thông tin profile của user này sẽ được hiện ra → Xóa tất cả

→ Sang thư mục MANDATORY để sao chép profile mẫu

→ Dán vào thư mục riêng có tên của user cần Mandatory trong thư mục PROFILES

→ Tích chọn “Do this for the next 3 conflicts” → Copy and Replace

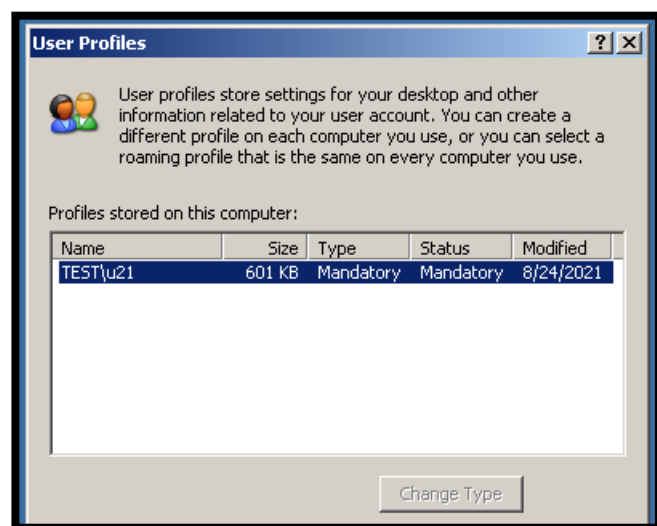
- **Windows XP:** Đăng nhập vào tài khoản của user đã được Mandatory.

Vào My Computer → Properties

→ Advanced → User Profiles → Settings

→ Type, Status

Thử xóa các icon ngoài màn hình desktop và các thư mục trong My Documents, sau đó đăng xuất rồi đăng nhập vào lại để kiểm tra xem đã Mandatory thành công hay chưa

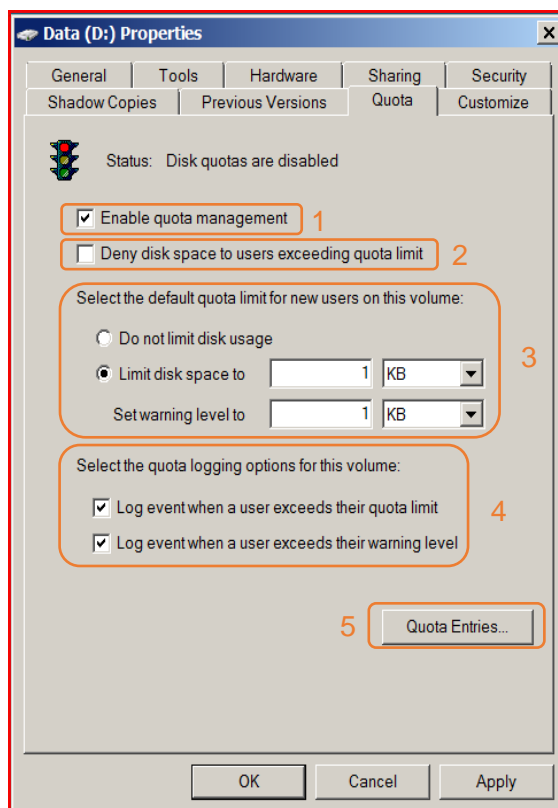


06. Thiết lập hạn ngạch đĩa (Disk Quota), share thư mục, triển khai Group Policy Object (GPO) cho domain users - Triển khai cài đặt phần mềm sử dụng GPO

(1 máy Windows Server 2008 + 1 máy client Windows XP)

- **Windows Server 2008:** Tạo các OU, group, user và thiết lập Home Folder nếu có yêu cầu
→ Nhấn chuột phải vào ổ đĩa cần đặt hạn ngạch sử dụng (Ví dụ: ổ D) → Quota

Cấu hình hạn ngạch sử dụng đĩa (Quota) cho tất cả người dùng: Tại khu vực “Select the default quota limit for new users on this volume” chọn “Limit disk space to”

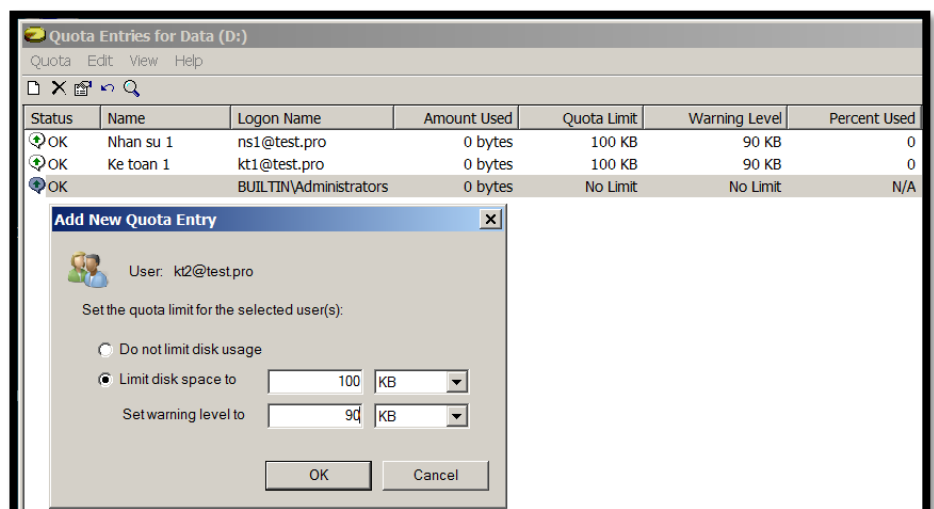


Chú thích:

1. **Enable Quota management:** Đánh dấu Check để bật tất chức năng Disk Quota
2. **Deny disk space to users exceeding quota limit:** Đánh dấu Check để ngăn không cho người dùng chép dữ liệu vào khi dung lượng vượt quá hạn ngạch (Quota) được thiết lập trong mục 3
3. Thiết lập dung lượng mặc định cho người dùng mới và đặt mức cảnh báo:
Limited disk space to: cho phép người dùng sử dụng dung lượng tối đa là bao nhiêu. **Set warning level to:** dung lượng còn lại bao nhiêu thì hiện cảnh báo
4. Thiết lập nhật ký (log) ghi lại quá trình khi vượt quá giới hạn cho phép hoặc vượt cảnh báo.
5. Thiết lập hạn ngạch sử dụng đĩa (Quota) cho từng người dùng.

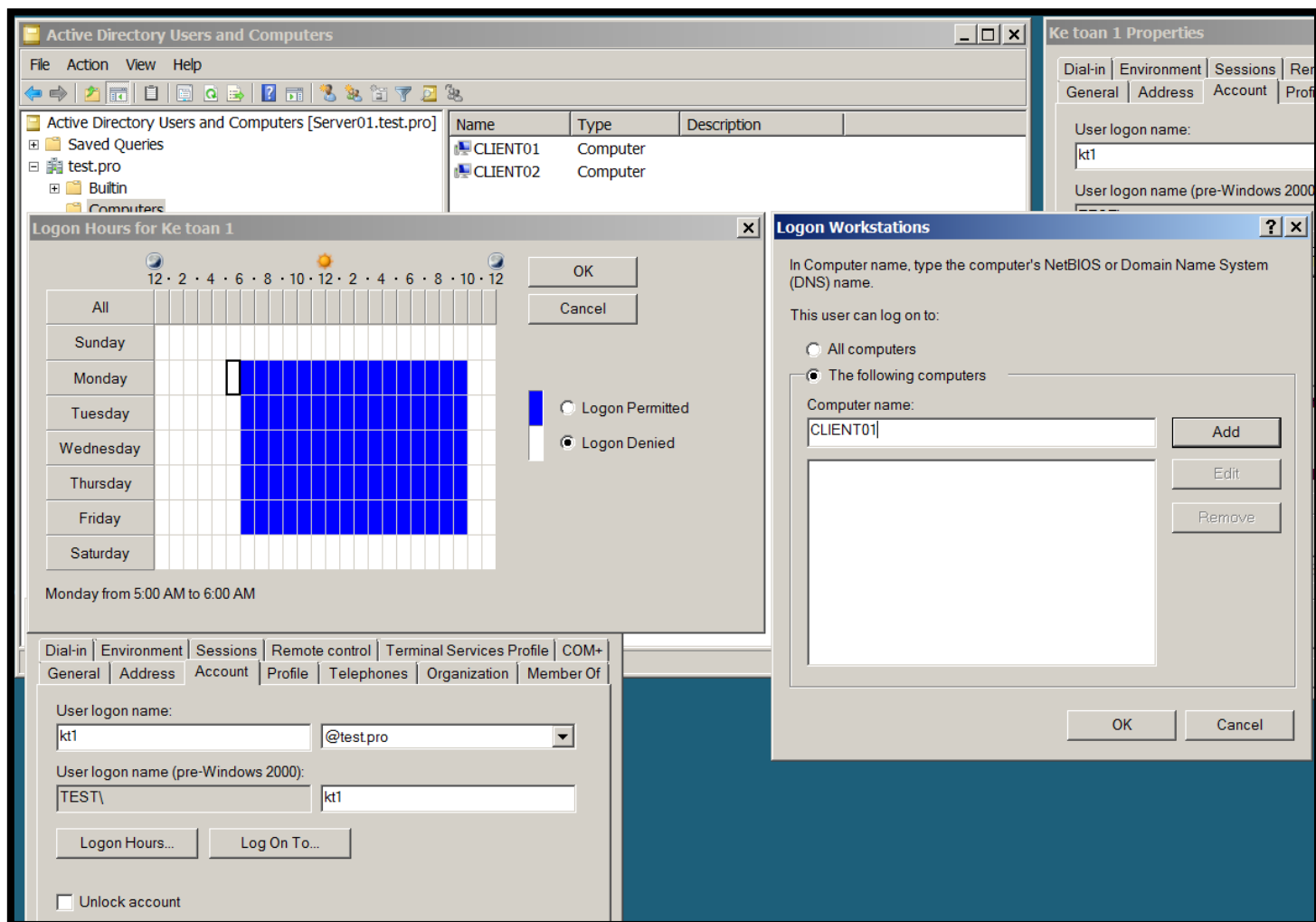
Thiết lập hạn ngạch sử dụng đĩa (Quota) cho từng người dùng:

- Quota Entries...
- Hộp thoại Quota Entries for Data hiện ra
- Quota
- New Quota Entry
- Chọn user
- Limit disk space to
- OK



Thiết lập thời gian và máy tính được phép đăng nhập:

Administrative Tools → Active Directory Users and Computers → Chọn → Properties
→ Account → Logon Hours để chọn thời gian, Log On To để chỉ định máy được phép



Chia sẻ thư mục (Shared Folders) từ máy thật sang máy ảo, ánh xạ (map) thư mục của máy thật thành ổ đĩa mạng của máy ảo:

Chọn máy ảo cần chia sẻ thư mục

→ Settings...

→ Options

→ Shared Folders

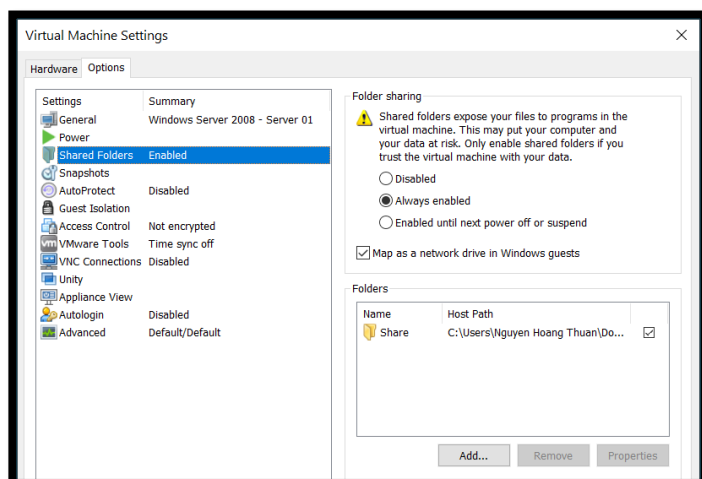
→ Always enabled

→ Map as a network drive in

Windows guests

→ Add...

→ Chọn đường dẫn đến thư mục



Triển khai chính sách nhóm Group Policy Object (GPO):

Tạo thư mục SOFT trên ổ D và copy app vào đây

→ Chia sẻ Share permission cho Domain Users

Bắt đầu thiết lập chính sách

→ Administrative Tools

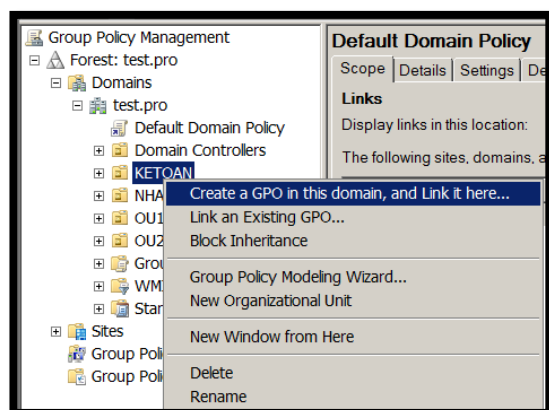
→ Group Policy Management

→ Chọn OU cần áp dụng chính sách

→ Create a GPO in this domain, and Link it here

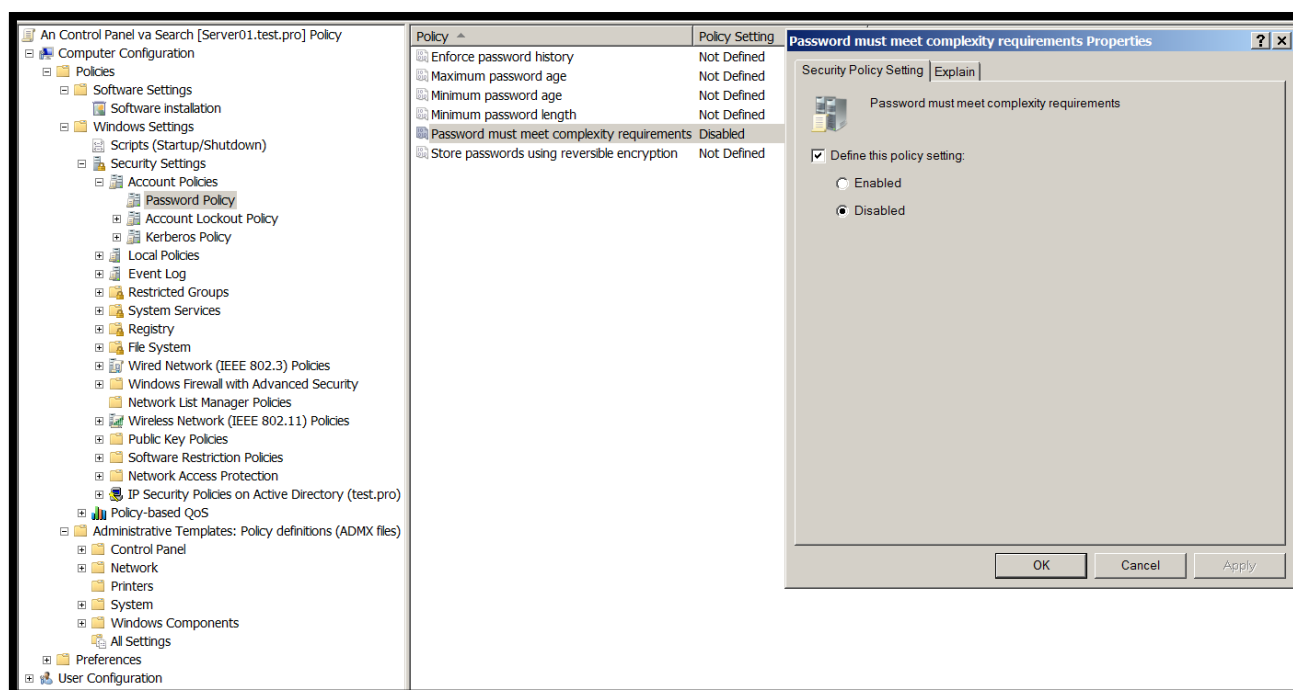
→ Đặt tên cho GPO → OK → Edit

→ Hộp thoại Group Policy Management Editor sẽ được hiện ra



Computer Configuration: Các thay đổi trong phần này sẽ áp dụng cho toàn bộ máy tính trong mạng

User Configuration: Cấu hình chính sách cho các tài khoản trong miền



Software Settings: Chính sách triển khai cài đặt phần mềm xuống Client một cách tự động

Windows Settings: Tại đây, chúng ta có thể tinh chỉnh, áp dụng các chính sách về vấn đề sử dụng tài khoản, quản lý khởi động và đăng nhập trên máy client

Administrative Template: Các chính sách về hệ thống (VD: Control Panel, Desktop)

→ Chọn loại GPO muốn triển khai → Setting → Enabled → gpupdate /force

Ví dụ 1: **Chỉnh sửa các chính sách trong Administrative Template để ngăn không cho Client dùng các chức năng của hệ thống như Control Panel, ẩn icon ngoài Desktop,...**

Sử dụng Group Policy Management để tạo một GPO với chức năng ẩn Control Panel và Search (trong ví dụ này sẽ ẩn đối với OU KETOAN)

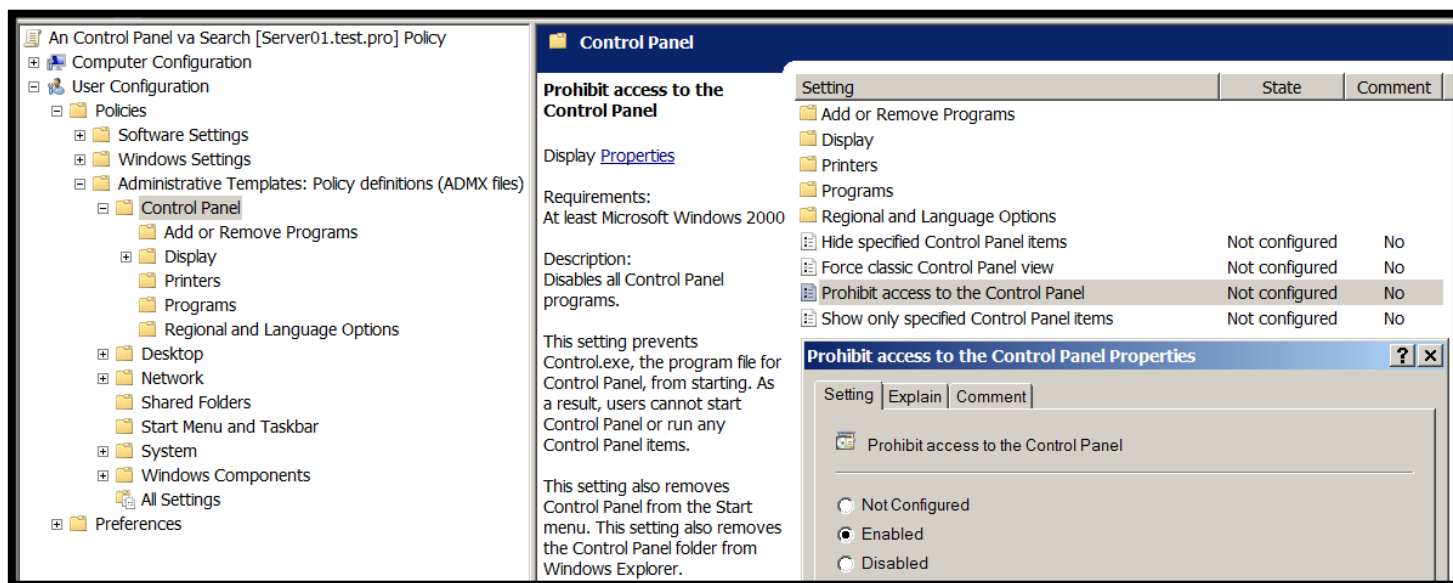
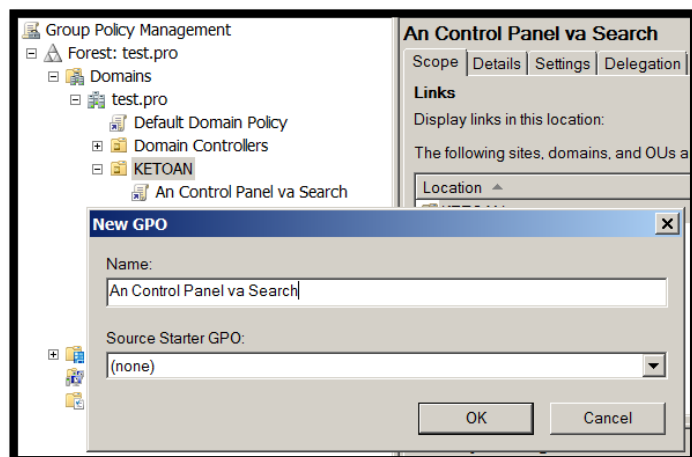
Tại hộp thoại Group Policy Management Editor

→ User Configuration

→ Administrative Template

→ Control Panel

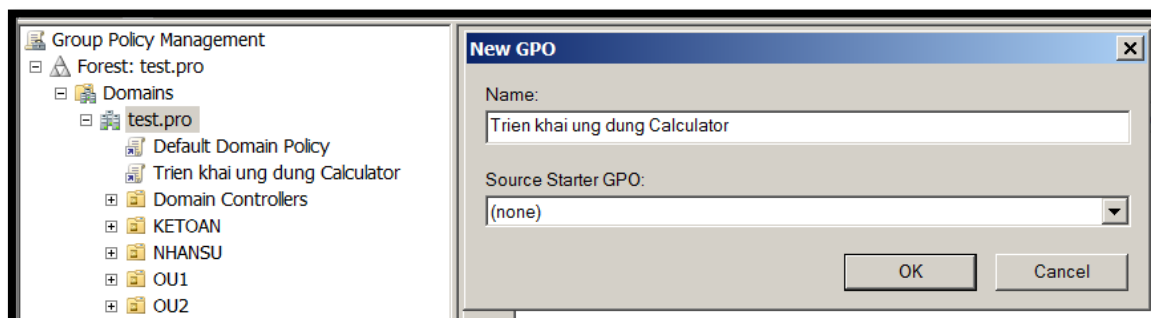
→ Prohibit access to the Control Panel → Enabled → OK → gpupdate /force



Ví dụ 2: **Triển khai ứng dụng**

Group Policy Management → Forest → Domains → Tên Domain (test.pro)

→ Create a GPO in this domain, and Link it here → Đặt tên → OK → Chọn → Edit



Tại hộp thoại Group Policy Management Editor

→ User Configuration

→ Policies

→ Software Settings

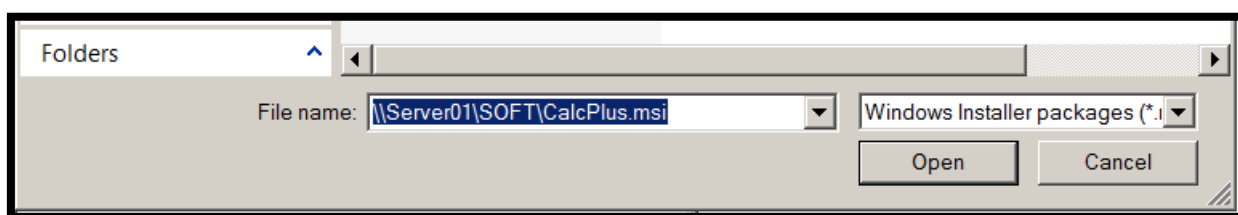
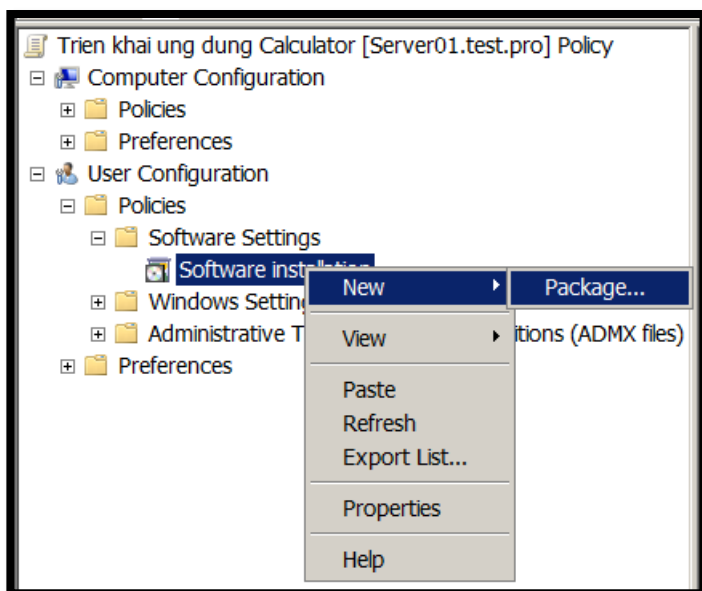
→ Software installation

→ Chuột phải

→ New package

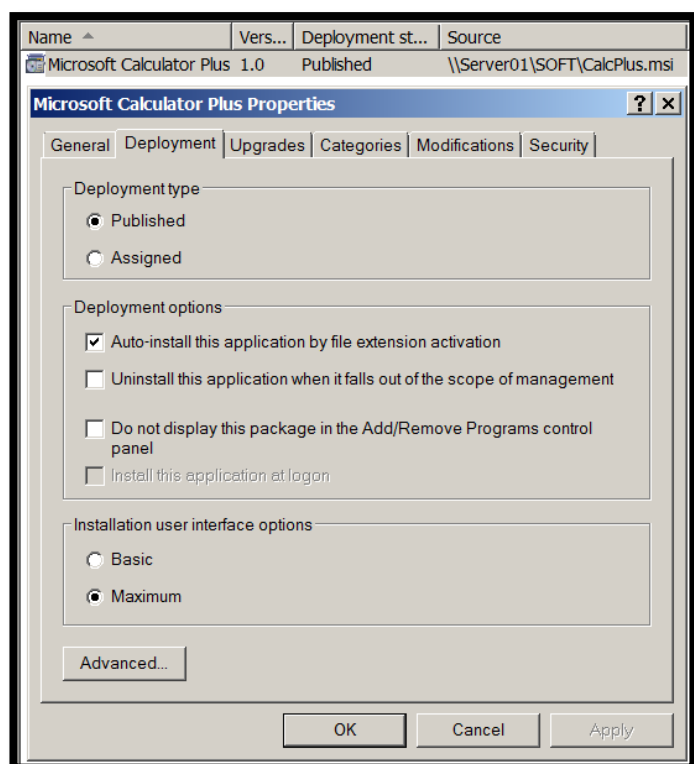
→ Chọn đường dẫn chứa ứng dụng cần được triển khai, hộp thoại chọn đường dẫn sẽ hiện ra (**lưu ý: không được chọn đường dẫn trực tiếp mà phải chọn thông qua File name**), ta

chọn File name: \\Server01\SOFT\CalcPlus.msi --> Open



Published: Ở máy Client, phần mềm sẽ được hiển thị trong danh mục Add New Programs của thành phần Add or Remove Programs trong Control Panel. Người dùng trên máy Client muốn cài đặt phải ấn vào nút Add program thì chương mới trình thực sự được cài đặt. Khi đó, chương trình sẽ thực hiện việc cài đặt phần mềm tự động cho đến khi hoàn thành. Người dùng không thể xóa chương trình

Khi chọn Properties của ứng dụng vừa được triển khai, chuyển sang tab Deployment sẽ thấy dòng "Install this application at logon" đã bị mờ



Assigned: Phần mềm sẽ xuất hiện trong danh mục Program trên thanh Start, khi người dùng chạy thì phần mềm mới được cài đặt. Người dùng có thể không cài gói phần mềm này và xoá đi

Khi chọn Properties của ứng dụng vừa được triển khai, chuyển sang tab Deployment sẽ thấy dòng “Auto-install this application by file extension activation” đã bị mờ

Advanced: Sẽ mở hộp thoại Properties và cho phép chọn thủ công **Published** hoặc **Assigned**, kèm với một số tùy chọn khác trước tiến hành triển khai ứng dụng

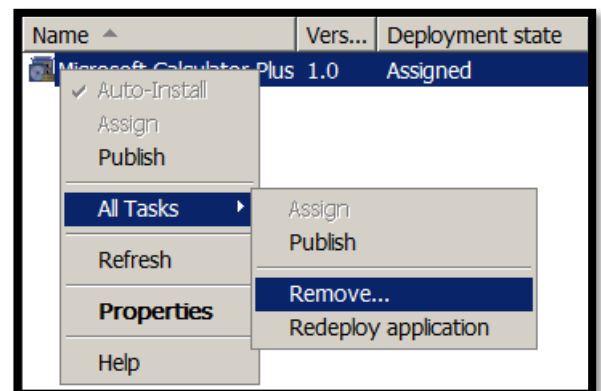
Dùng lệnh “gpupdate /force” để cập nhật chính sách. Ngoài ra, có thể xoá hoặc triển khai lại ứng dụng bằng cách chọn ứng dụng

→ Chuột phải

→ All Tasks

→ Remove... / Redeploy

→ gpupdate /force



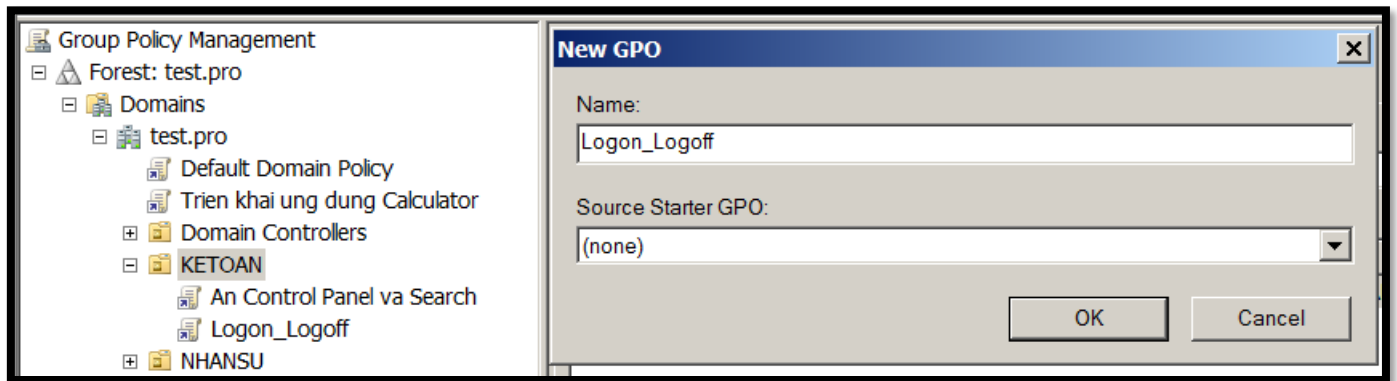
Khi xoá, có thể chọn xoá ngay lập tức hoặc

cho phép người dùng tiếp tục sử dụng nhưng không được cài mới ứng dụng

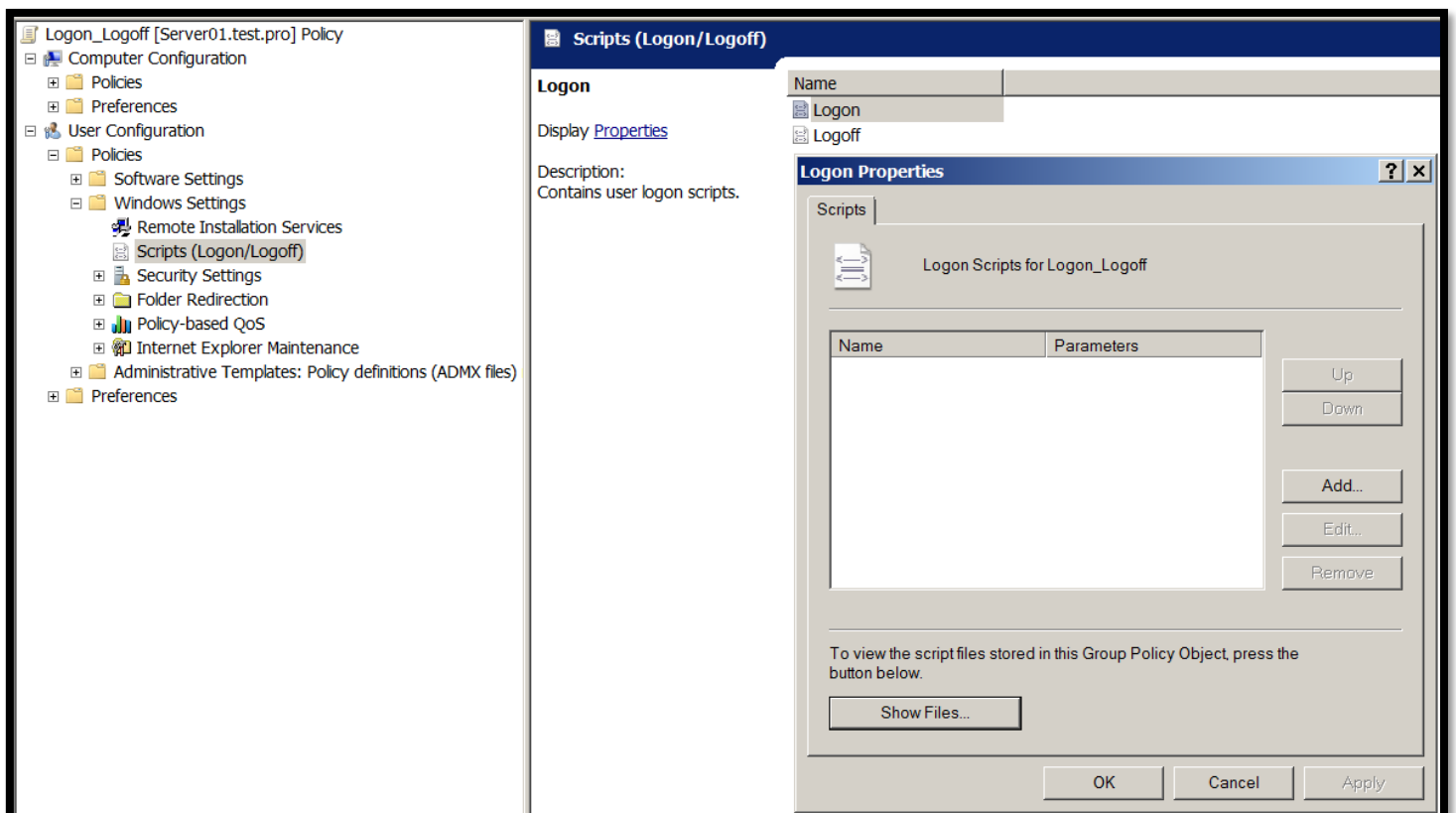
07. Script logon / logoff (1 máy Windows Server 2008 + 1 máy client Windows XP)

Ví dụ 3: Tạo hộp thoại khi đăng nhập và đăng xuất

Tạo GPO "Logon_Logoff" → Edit



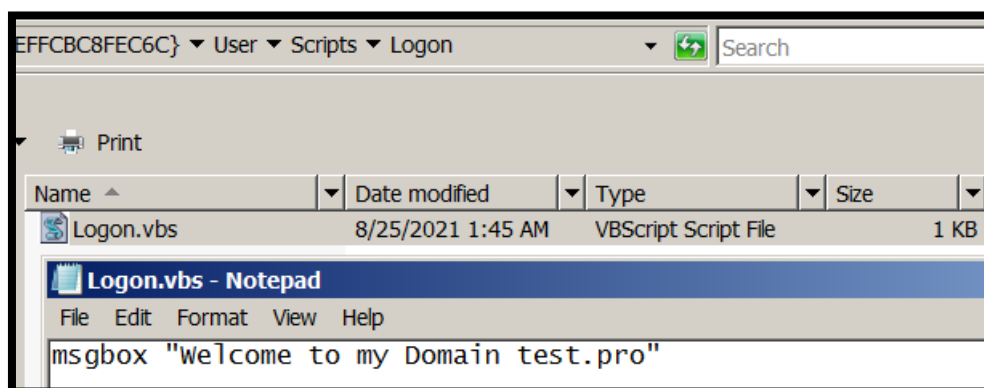
Tại hộp thoại Group Policy Management Editor → User Configuration → Policies
→ Windows Settings → Scripts (Logon/Logoff) → Chọn script Logon
→ Logon Properties sẽ hiện ra → Show Files...



Khi nhấn vào nút Show Files, Windows Explorer sẽ hiện ra

→ Tạo một file text với nội dung: `msgbox "Welcome to my Domain test.pro"`

→ Lưu file lại và đổi tên file cũng như phần mở rộng thành `Logon.vbs` → Yes



Trở lại Logon Properties

→ Add...

→ Hộp thoại Add a Script hiện ra

→ Browse

→ Chọn file Logon.vbs

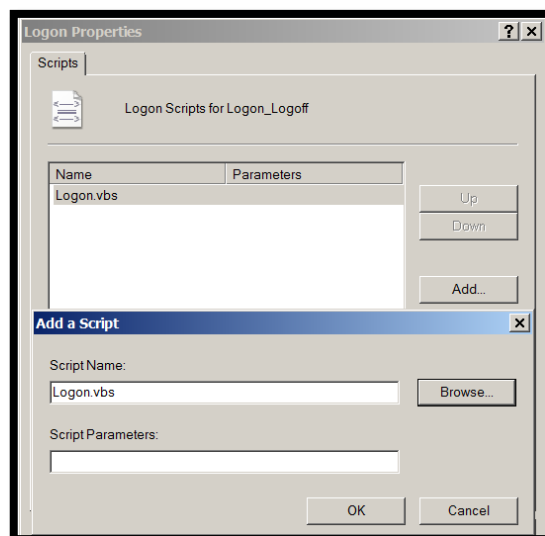
→ OK

→ OK

→ `gpupdate /force`

Làm tương tự với script Logoff.vbs

với nội dung `msgbox "Goodbye..."`



08. Deny App - Cấm sử dụng, thực thi phần mềm dùng GPO

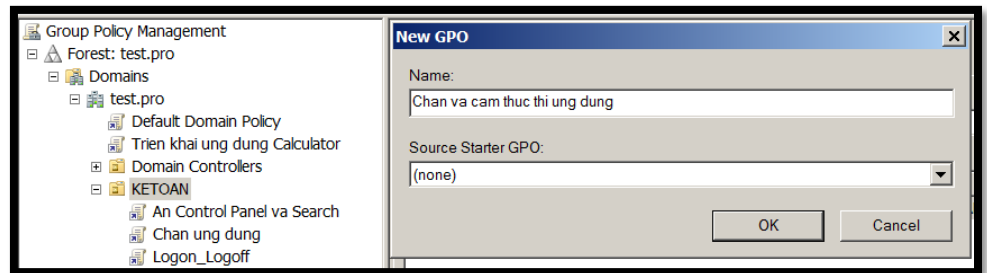
(1 máy Windows Server 2008 + 1 máy client Windows XP)

Ví dụ 4: Cấm sử dụng, thực thi ứng dụng

Tạo GPO

“Chặn ứng dụng”

→ Edit



Tại hộp thoại Group Policy Management Editor

→ User Configuration

→ Policies

→ Windows Settings

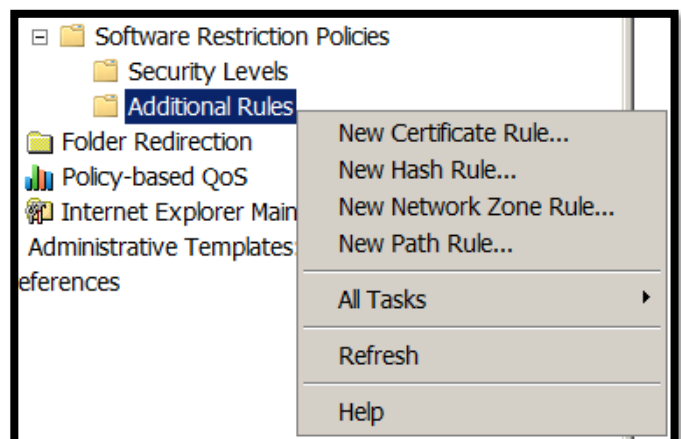
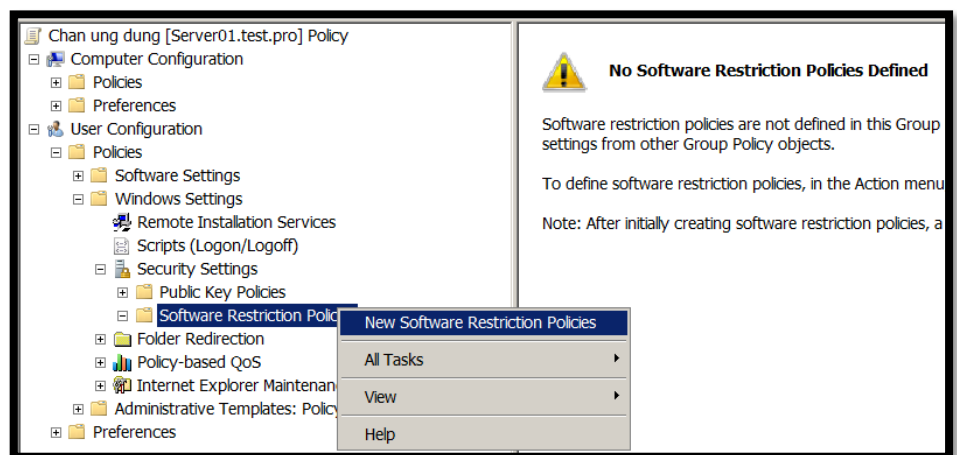
→ Security Settings

→ Software

Restriction Policies

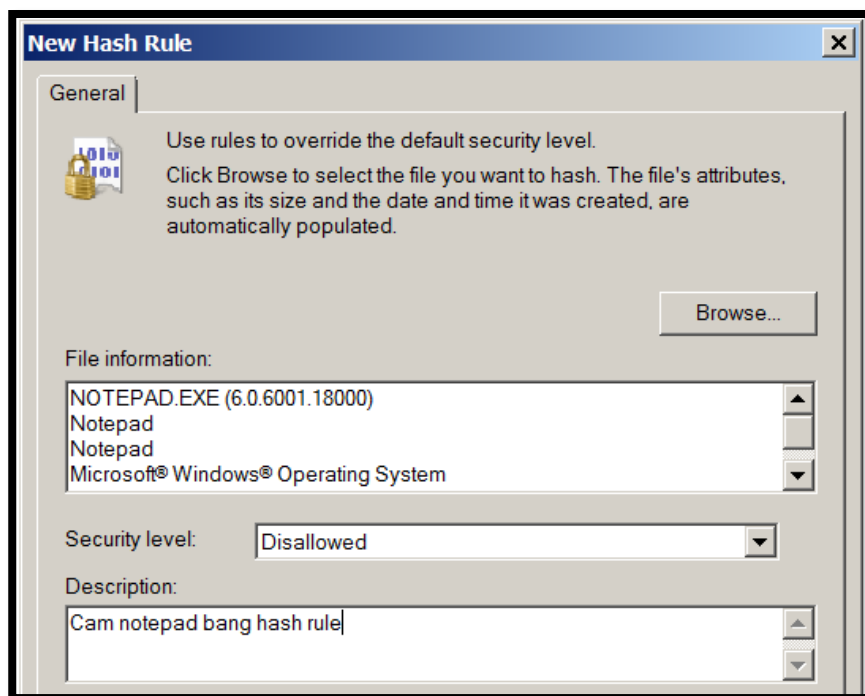
→ New Software

Restriction Policies → Additional Rules

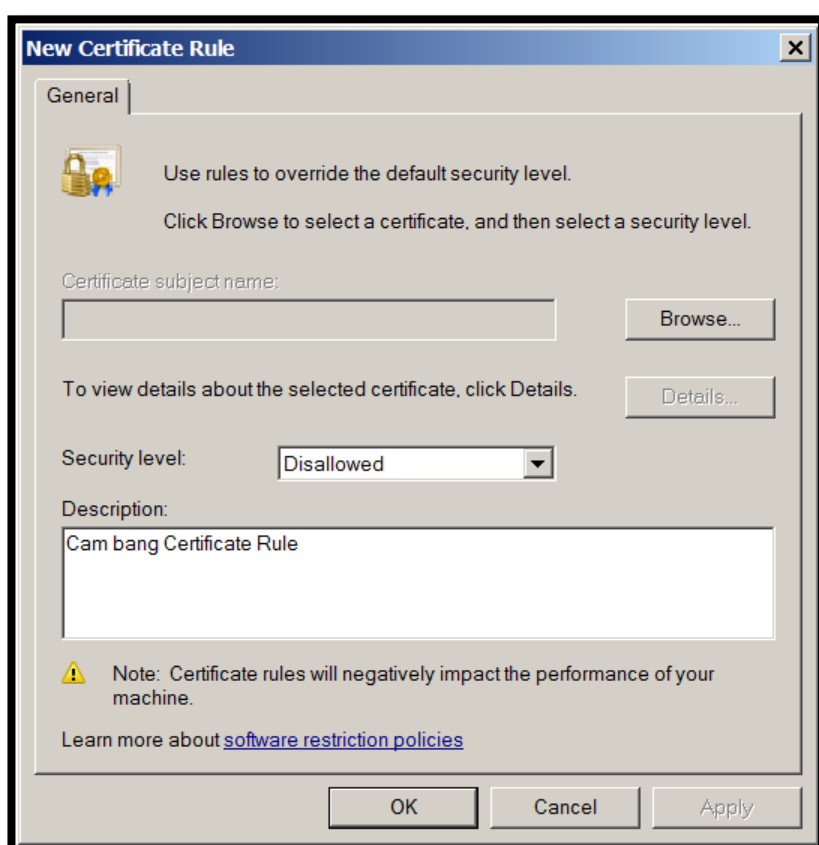


Hash Rule: Windows tạo một hash các file thực thi bằng thuật toán và đảm bảo giá trị hash sinh ra là duy nhất cho mỗi tập tin, giá trị hash của tập tin được lưu trong Software Restriction Policies. Khi người dùng muốn chạy tập tin, hệ thống sẽ so khớp giá trị hash của tập tin với giá trị hash của nó trong Software Restriction Policies, nếu hai giá trị này khớp nhau, luật cấm sẽ được thực thi.

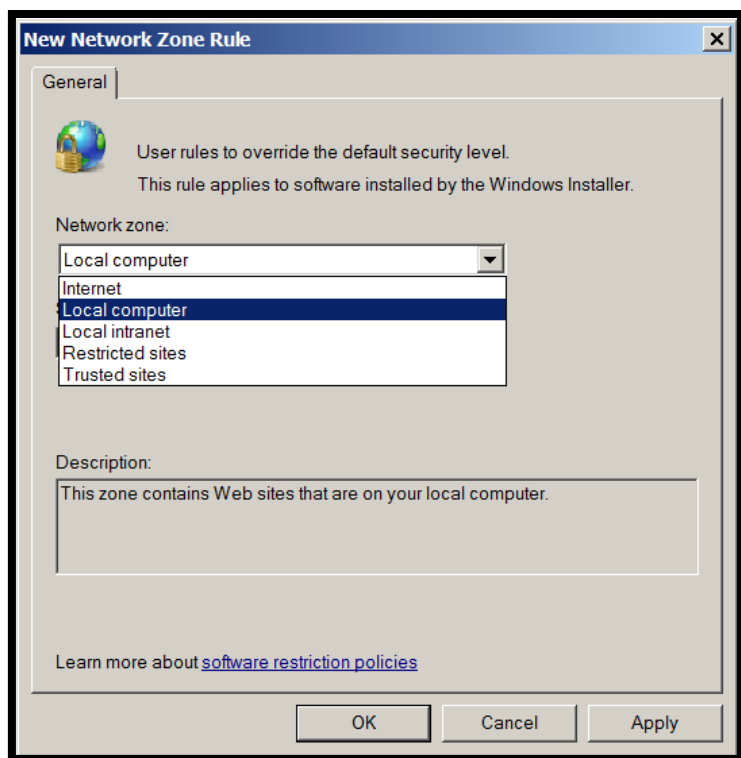
Việc này giúp giá trị hash của tập tin không bị thay đổi dù có thay đổi đường dẫn của tập tin. Tuy nhiên, nếu tập tin bị phá hoại làm thay đổi nội dung của tập tin, dẫn tới giá trị hash bị thay đổi, khi đó, luật trong Software Restriction Policies sẽ không cho chương trình được thực thi



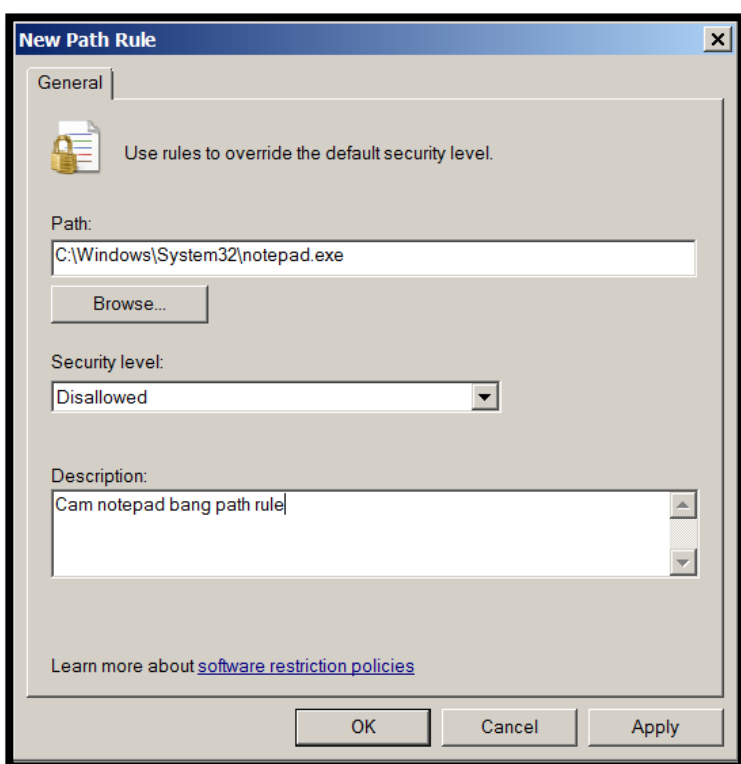
Certificate Rule: cho phép đồng ý hoặc từ chối các ứng dụng dựa vào chứng chỉ số (chữ ký số) của mỗi ứng dụng. Có thể sử dụng certificate rule để cho phép chạy các phần mềm đang bị cấm bởi thiết lập Disallowed. Tuy nhiên, hầu như không ai đánh chữ ký số trên mã ứng dụng của họ. Phạm vi cho phép và cấm quá lớn, khi sử dụng phải tạo thêm một rule riêng với mức ưu tiên cao hơn để khóa một số ứng dụng nào đó không mong muốn



Network Zone Rule: ngăn chặn người dùng download và cài đặt ứng dụng từ Internet, chỉ cho phép người dùng chạy ứng dụng từ các máy nội bộ (file cài đặt phải nằm trên máy nội bộ), local intranet, trusted sites, restricted sites



Path Rule: luật dựa trên vị trí của phần mềm (vị trí của nó trong thiết bị lưu trữ, hoặc thông tin về vị trí được khai báo trong cấu trúc Registry). Có thể sử dụng path rule để cho phép chạy các phần mềm bị cấm bởi thiết lập Disallowed, hoặc cấm chạy các phần mềm do thiết lập Unrestricted. Khi thay đổi vị trí lưu trữ của phần mềm sẽ làm cho luật không còn tác dụng. Ngược lại, nếu dựa vào thông tin vị trí của phần mềm trong Registry sẽ luôn đảm bảo luật được thực thi, vì khi thay đổi vị trí lưu trữ của phần mềm, giá trị trong Registry sẽ được cập nhật tự động



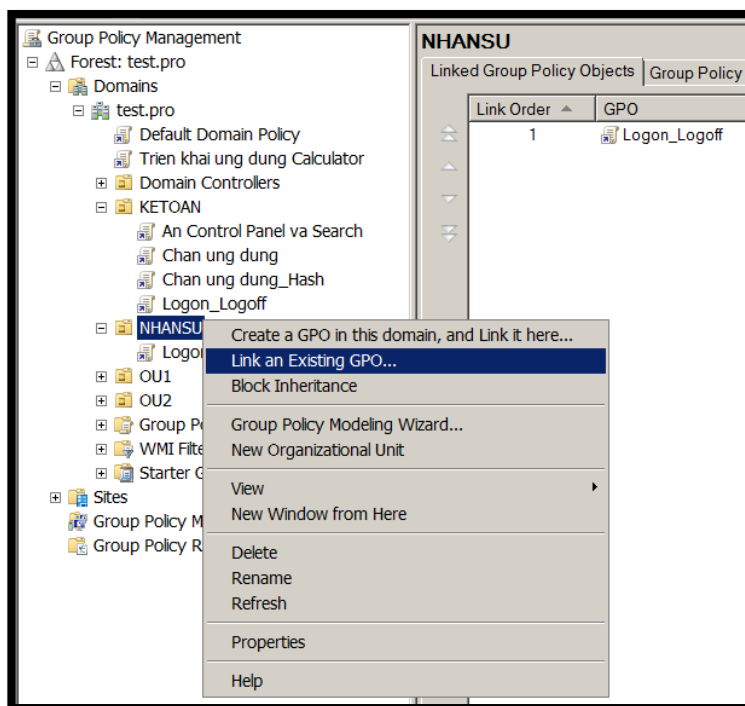
Khi có xung đột giữa các luật, độ ưu tiên:

Hash Rule > Certificate Rule > Network Zone Rule > Path Rule

Sao chép GPO sang một OU mới:

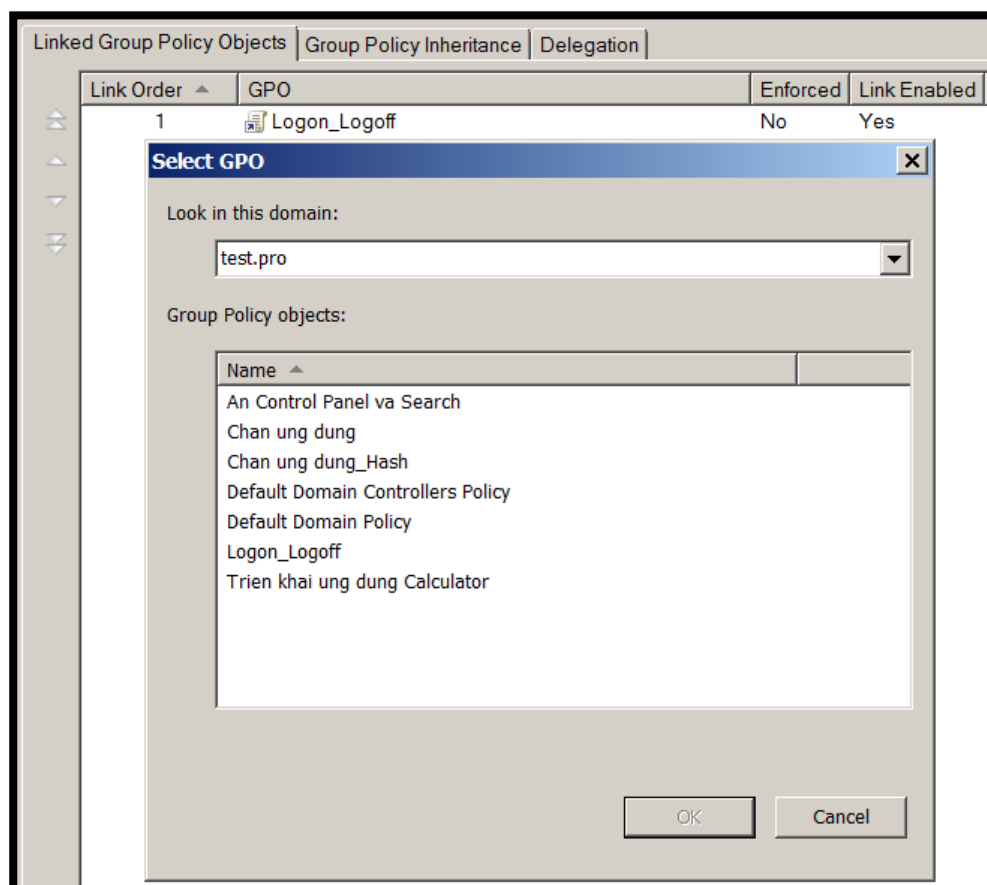
Chọn OU cần sao chép chính sách

→ Link an Existing GPO...



→ Chọn một GPO
đã được tạo

→ OK

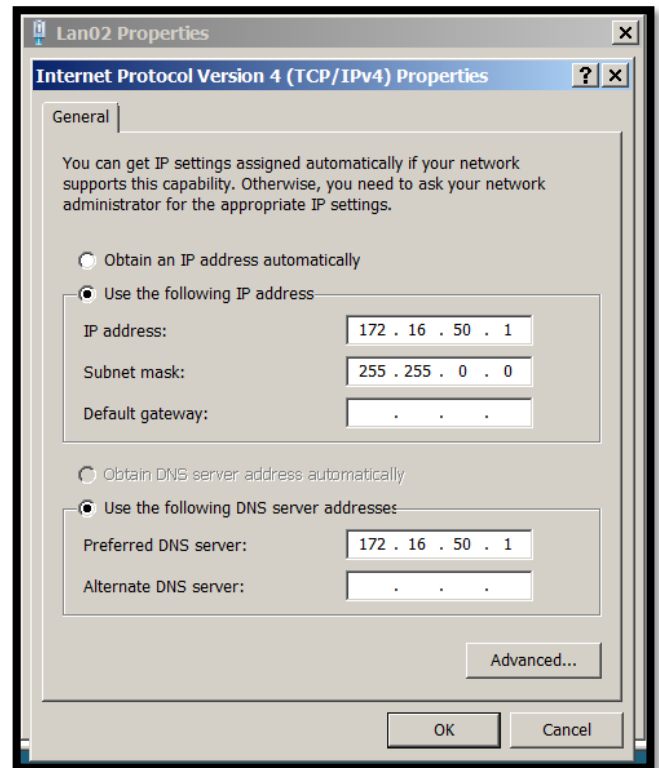
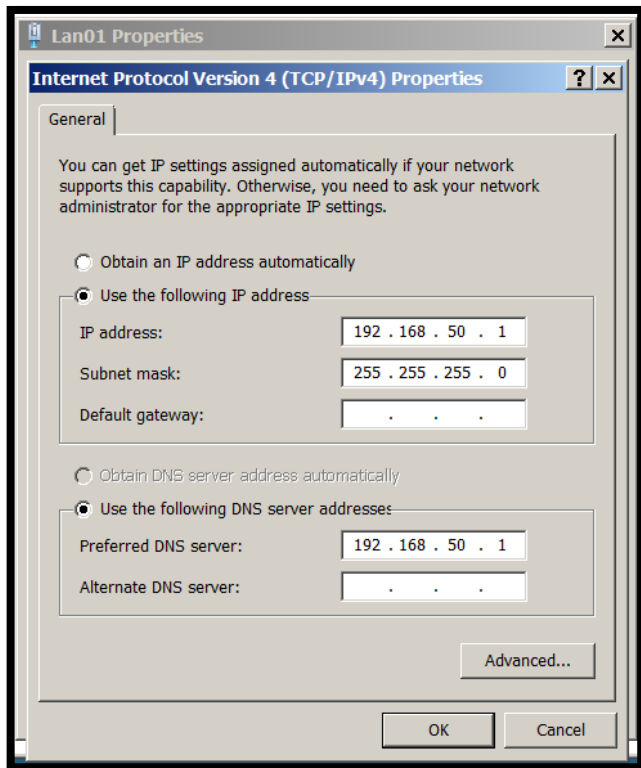


09. Cài đặt, cấu hình dịch vụ DHCP server

(1 máy Windows Server 2008 + 2 máy client Windows XP)

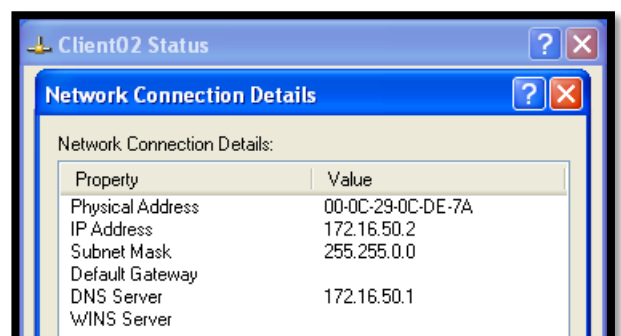
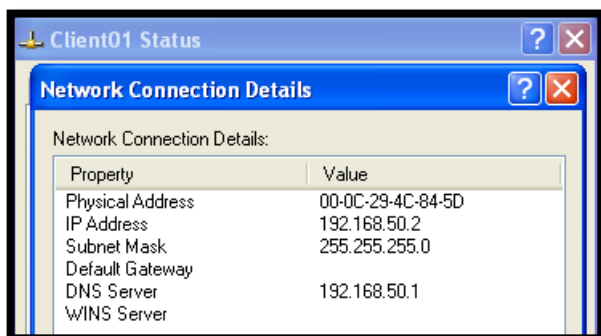
(Cấu hình card mạng, địa chỉ IP, DNS, thêm ổ đĩa, tạo Domain Controller, kết nối máy Client vào Domain và tạo OU, user, group,... tương tự như các bước ở trên)

Tạo thêm card mạng: Virtual Machine Settings → Add → Network Adapter → VMnet2



Client01 phải có cùng lớp mạng (192.168.50.xxx), cùng card mạng (VMnet1) và trỏ DNS về card mạng **Lan01** của **DHCP Server**

Client02 phải có cùng lớp mạng (172.16.50.xxx), cùng card mạng (VMnet2) và trỏ DNS về card mạng **Lan02** của **DHCP Server**



- **Windows Server 2008:**

Administrative Tools

→ Server Manager

→ Add Roles

→ Hộp thoại Add

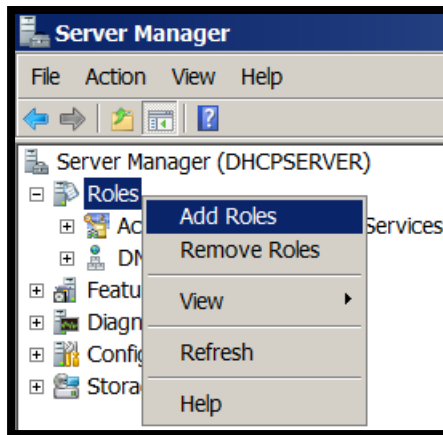
Roles Wizard hiện ra

→ Server Roles

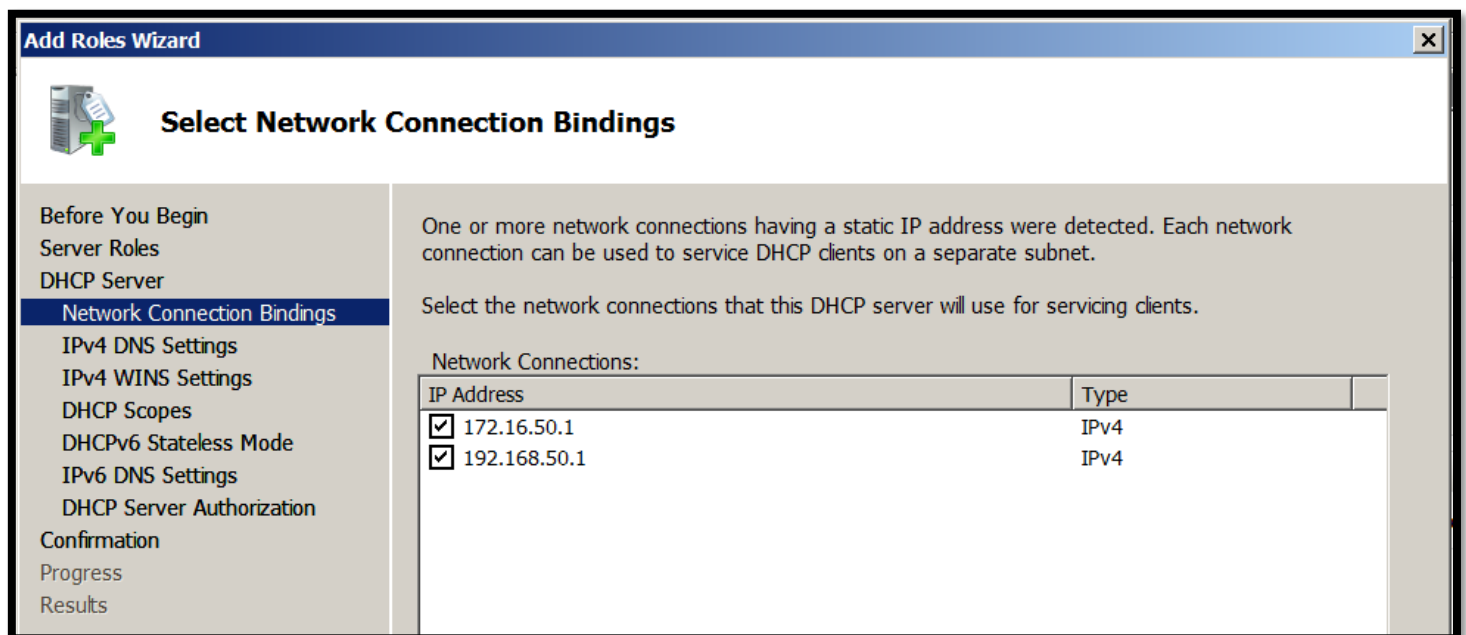
→ DHCP Server

→ Next

→ Next



Network Connection Bindings: Chọn các card mạng muốn dùng làm DHCP Server



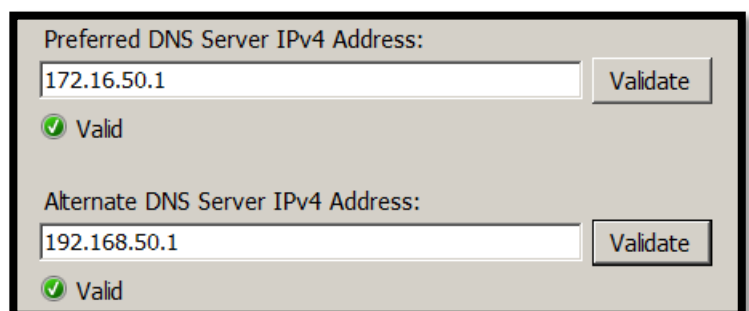
IPv4 DNS Settings:

Nhập địa chỉ của các card mạng

→ Validate

→ Next

→ Next



DHCP Scopes: Add → Nhập dãy địa chỉ mà mình muốn cấp phát cho Client → Next

Add Scope

A scope is a range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.

Scope Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

Default Gateway (optional):

Subnet Type:

☒ Activate this scope

OK Cancel

Add Scope

A scope is a range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.

Scope Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

Default Gateway (optional):

Subnet Type:

☒ Activate this scope

OK Cancel

DHCPv6 Stateless Mode: Tích chọn “Disable DHCPv6 stateless mode for this server”

Before You Begin

Server Roles

DHCP Server

Network Connection Bindings

IPv4 DNS Settings

IPv4 WINS Settings

DHCP Scopes

DHCPv6 Stateless Mode

DHCP Server Authorization

Confirmation

Progress

Results

DHCP Server supports the DHCPv6 protocol for servicing IPv6 clients. Using DHCPv6, clients can automatically configure their own IPv6 addresses using stateless mode, or they can acquire IPv6 addresses in stateful mode from the DHCP server. If routers on your network are configured to support DHCPv6, verify that your selection below matches the router configuration.

Select the DHCPv6 stateless mode configuration for this server.

☐ Enable DHCPv6 stateless mode for this server

IPv6 clients will be automatically configured without using this DHCP server.

☒ Disable DHCPv6 stateless mode for this server

After installing DHCP Server, you can configure the DHCPv6 mode using the DHCP Management console.

DHCP Server Authorization: Use current credentials → Next → Install

Before You Begin

Server Roles

DHCP Server

Network Connection Bindings

IPv4 DNS Settings

IPv4 WINS Settings

DHCP Scopes

DHCPv6 Stateless Mode

DHCP Server Authorization

Confirmation

Progress

Results

Active Directory Domain Services (AD DS) stores a list of DHCP servers that are authorized to service clients on the network. Authorizing DHCP servers helps avoid accidental damage caused by running DHCP servers with incorrect configurations or DHCP servers with correct configurations on the wrong network.

Specify credentials to use for authorizing this DHCP server in AD DS.

☒ Use current credentials

The credentials of the current user will be used to authorize this DHCP server in AD DS.

User Name:

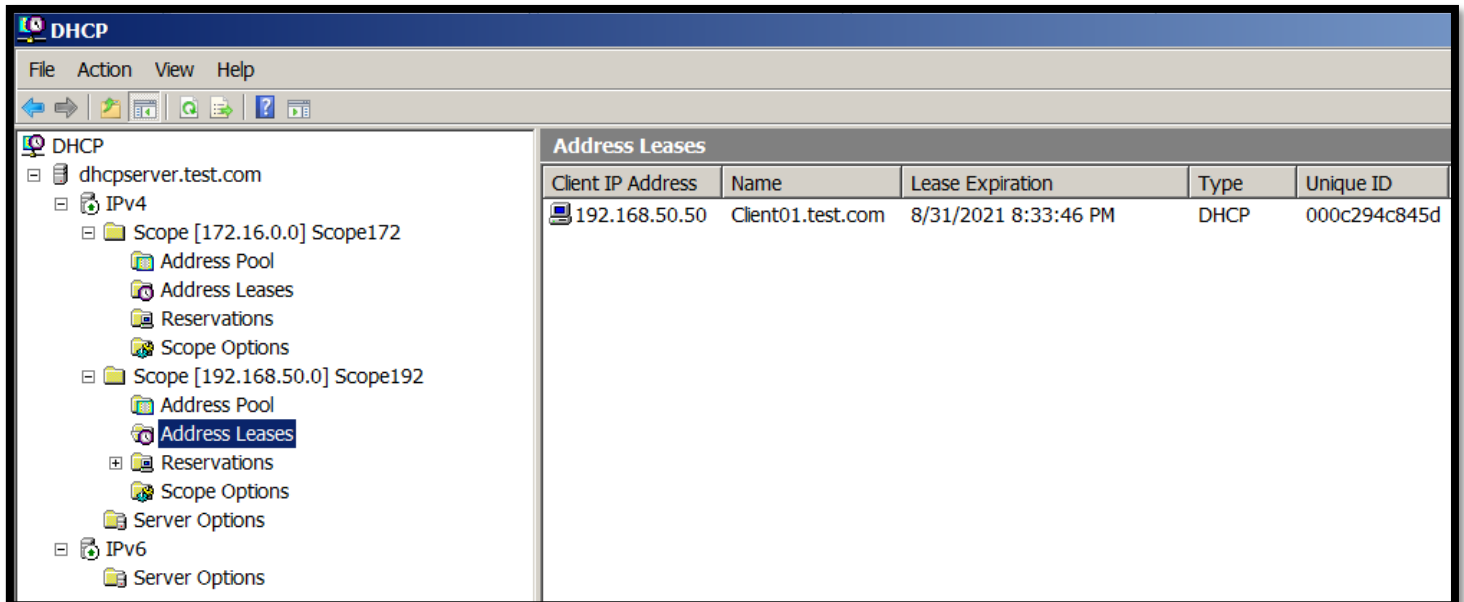
Cấu hình DHCP nâng cao: Administrative Tools → DHCP → Tên DHCP Server → IPv4

Address Pool: loại bỏ một hoặc một dãy địa IP ra khỏi vùng địa chỉ ban đầu

Address Leases: quản lý thời gian có hiệu lực của địa chỉ IP được cấp tự động

Reservations: gán một địa chỉ cố định cho một máy (thường là máy server)

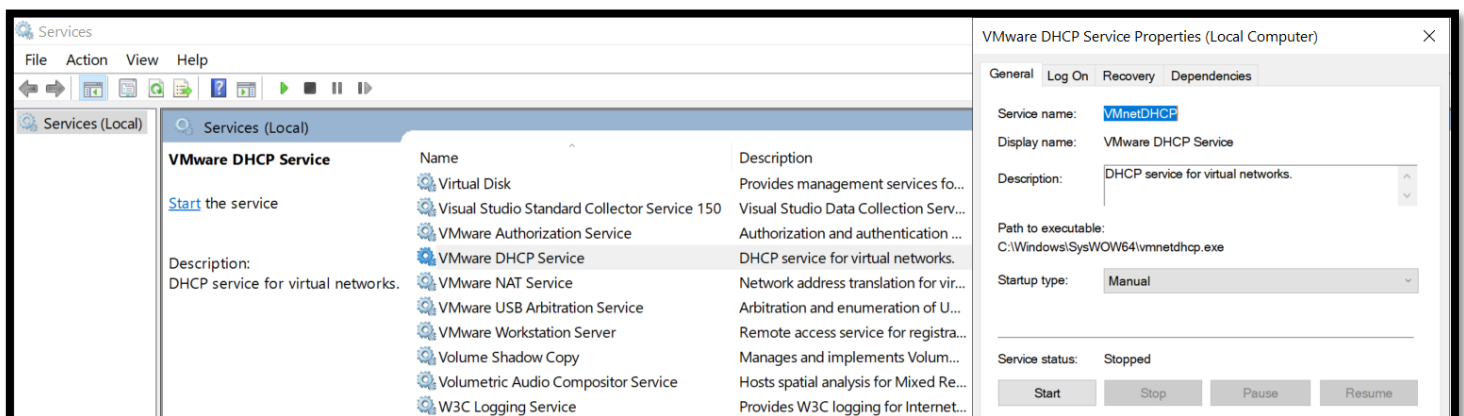
(Sẽ được trình bày và minh họa chi tiết hơn ở Mạng máy tính nâng cao)



Tắt tính năng cấp DHCP tự động của VMware để tránh xung đột với DHCP Server:

Ở máy ngoài (Windows 10) gõ lệnh services.msc để mở Windows Services

→ VMware DHCP Service → Startup type: Manual → Stop → OK



- **Windows XP:** Đăng nhập vào máy Client bằng tài khoản admin → Network Connections → Chuyển sang “Obtain an IP address automatically” và “Obtain DNS server address automatically” để sử dụng IP và DNS được DHCP Server cấp phát tự động
(Dùng các lệnh “ipconfig /release” và “ipconfig /renew” để giải phóng và xin cấp lại IP)

10. Thiết lập, cấu hình FTP (1 máy Windows Server 2008 + 1 máy client Windows XP)

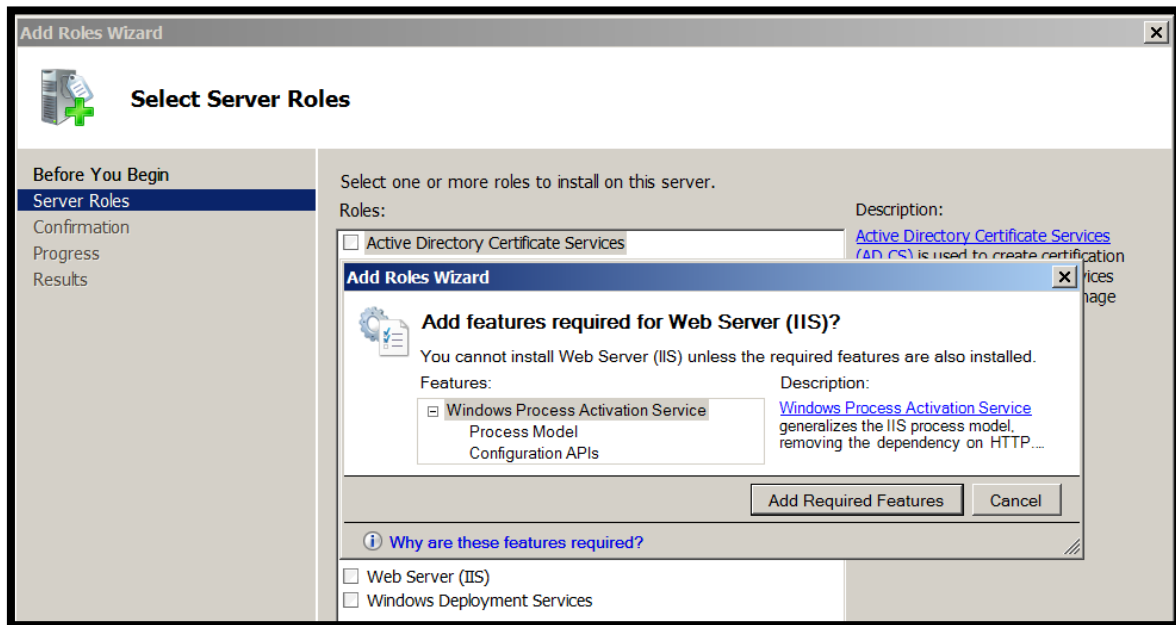
(Cấu hình card mạng, địa chỉ IP, Gateway, DNS, thêm ổ đĩa, tạo Domain Controller, kết nối máy Client vào Domain và tạo OU, user, group,... tương tự như các bước ở trên)

- Windows Server 2008:

Cài đặt Internet Information Services (IIS): Administrative Tools → Server Manager

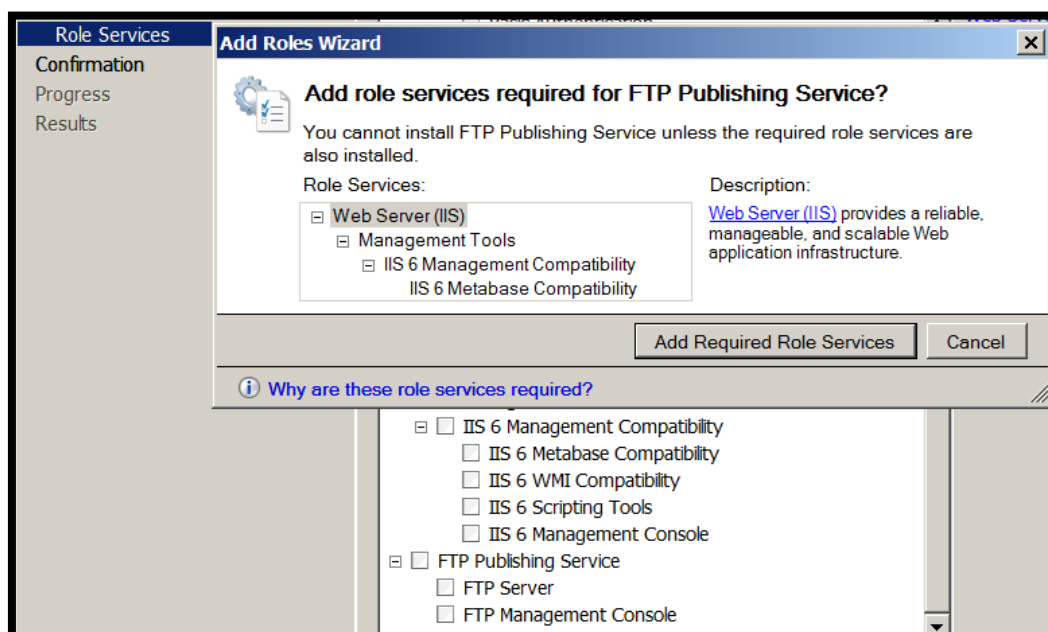
→ Add Roles → Hộp thoại Add Roles Wizard hiện ra → Web Server (IIS)

→ Add Required Features → Next → Next

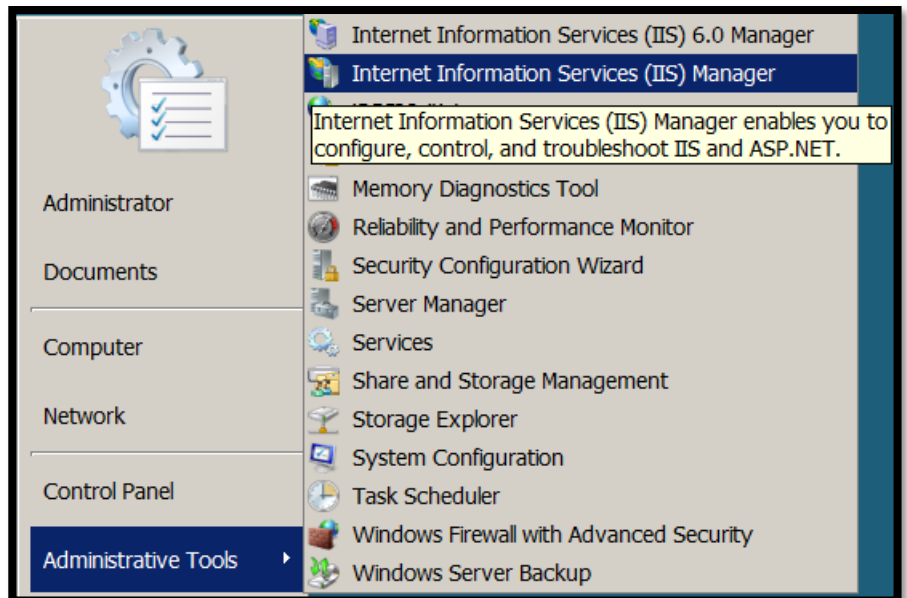


Tại Role Services → Management Tools → Chọn “FTP Publishing Service”

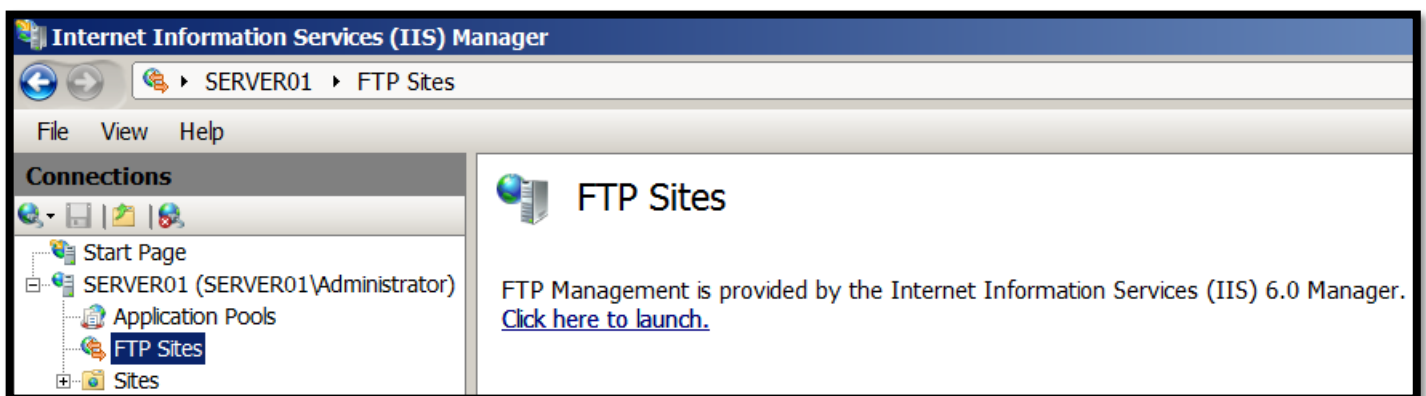
→ Add Required Services → Next → Install



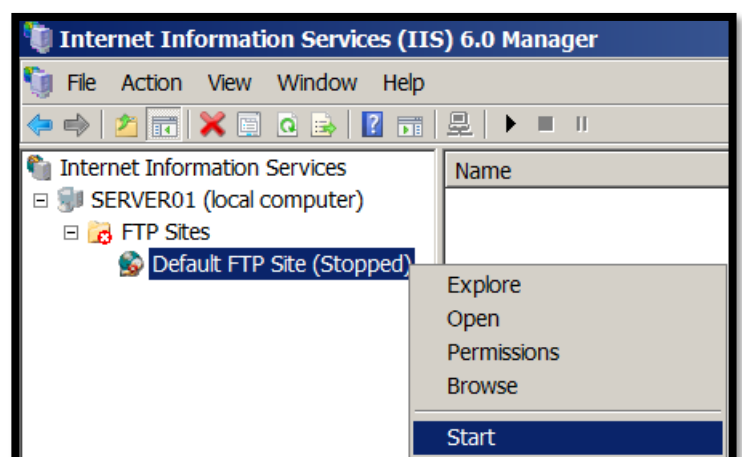
Administrative Tools
→ Internet Information
Services (IIS) Manager



Hộp thoại Internet Information Services (IIS) Manager hiện ra
→ Tên Server → FTP Sites → Click here to launch

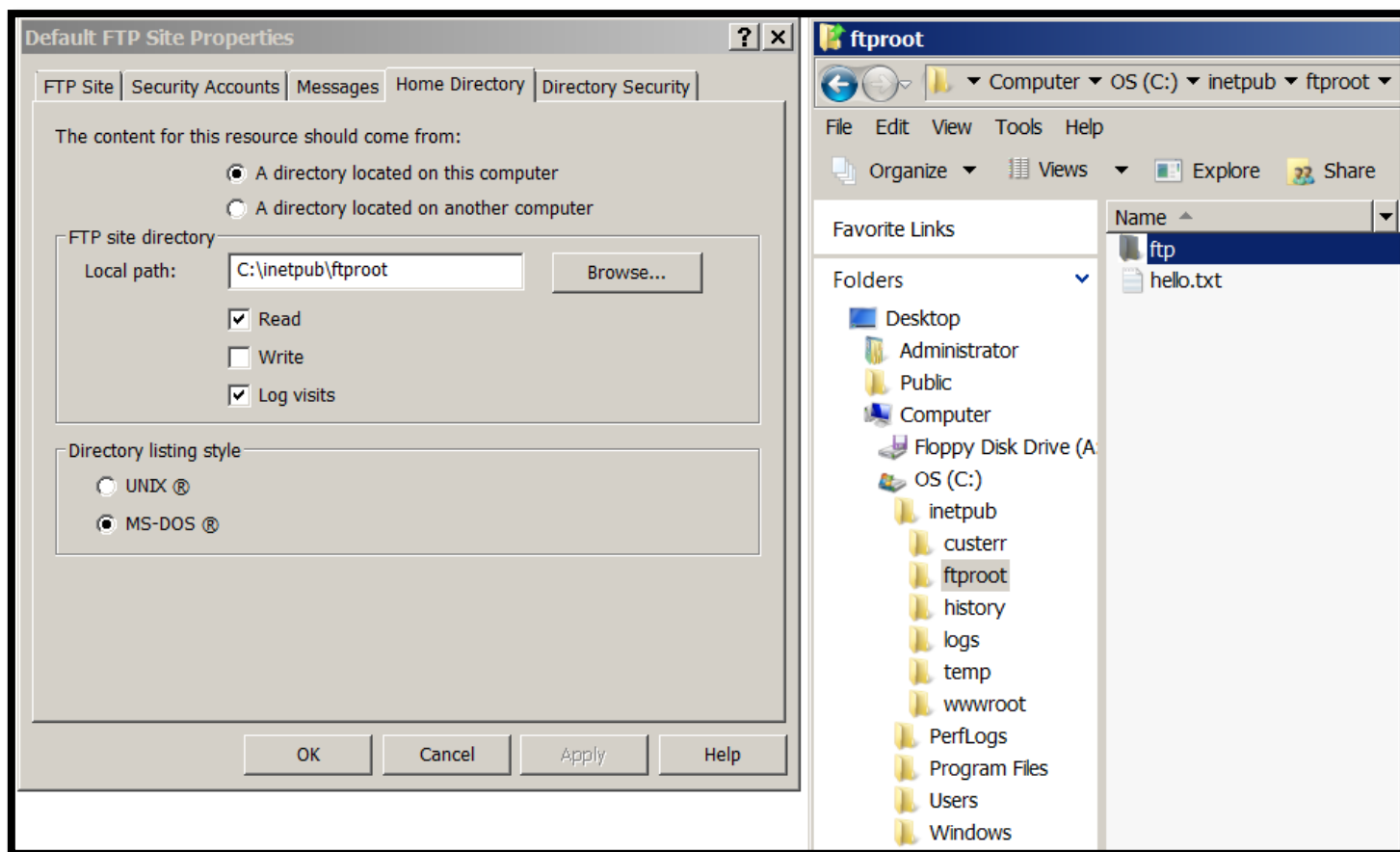


Hộp thoại Internet Information
Services (IIS) 6.0 Manager hiện ra
→ Tên server (local computer)
→ FTP Sites
→ Default FTP Site (Stopped)
→ Start
→ Yes

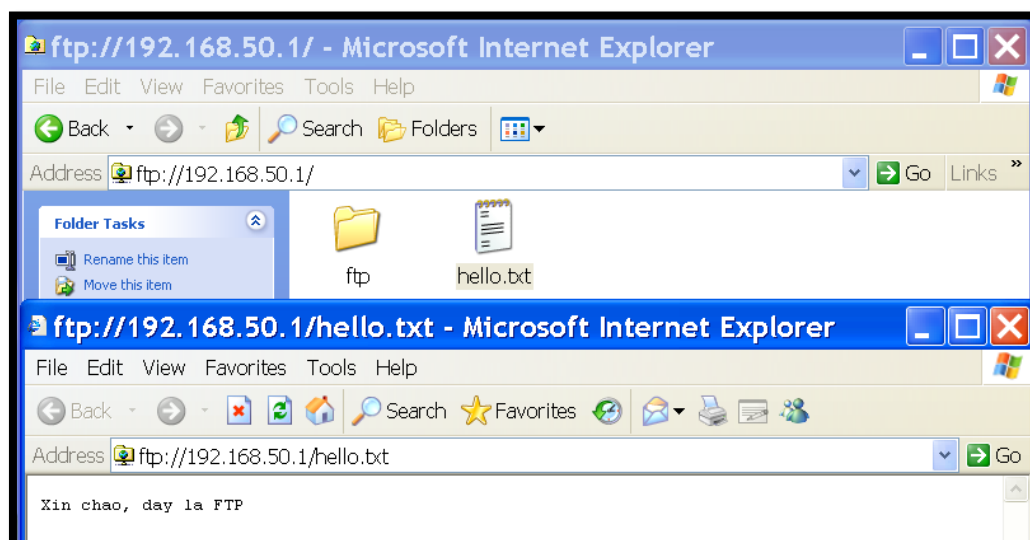


Tạo thư thư mục, tập tin để kiểm tra:

Tìm đường dẫn thư mục mặc định: Default FTP Site → Properties → Home Directory
→ Browse... → Tạo thư mục, tập tin text chứa nội dung và đặt tên tùy ý



- **Windows XP:** Mở trình duyệt Internet Explorer
→ Nhập ftp://TÊN hoặc ĐỊA CHỈ MÁY CHỦ (Ví dụ: ftp://192.168.50.1 | ftp://Server01)
→ Thử xem và xóa thư mục



FTP nâng cao:

Yêu cầu đăng nhập để truy cập FTP:

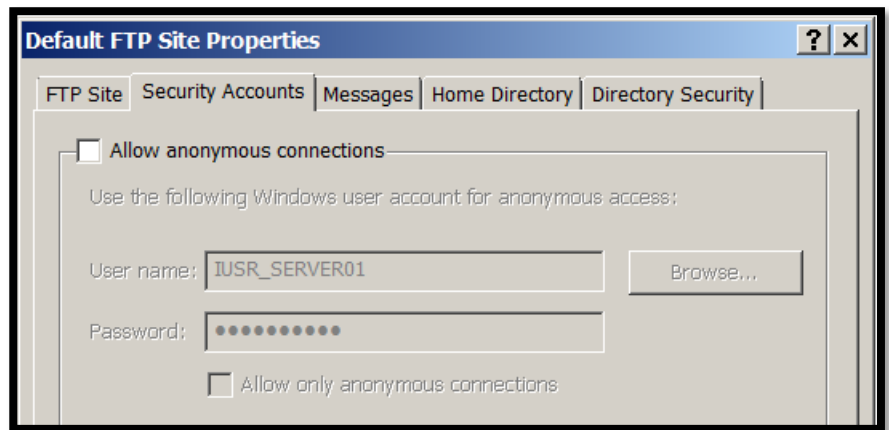
Default FTP Site

→ Properties

→ Security Accounts

→ Bỏ chọn “Allow anonymous connections”

(cần tạo sẵn user có mật khẩu để thử nghiệm trên client)



Tạo một FTP Site riêng:

Tạo sẵn một thư mục chứa FTP Site (Ví dụ: D:\website)

→ Default FTP Site

→ New → FTP Site... → Next

→ Nhập Description (mô tả)

→ Next

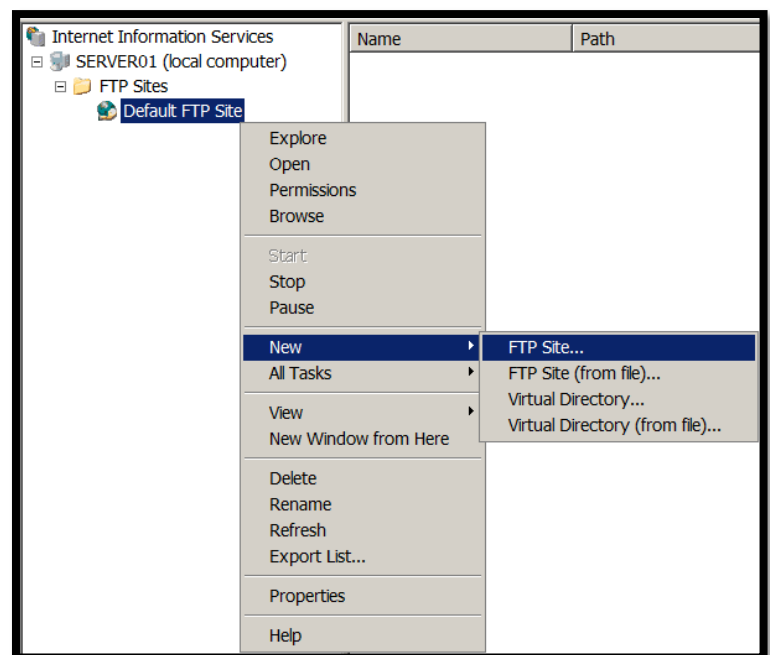
→ Chọn card mạng và port

Enter the IP address to use for this FTP site:

192.168.50.1

Type the TCP port for this FTP site (Default = 21):

5000



→ Next

→ Do not isolate users

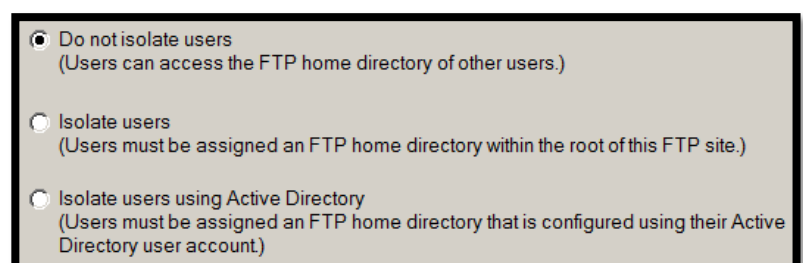
(Không cô lập, cách ly user.

Cô lập user và cô lập bằng AD sẽ được thực hiện ở bài 14, 15)

→ Next

→ Nhập đường dẫn chứa FTP Site (Ví dụ: D:\website) → Next

→ Gán quyền Read/Write (nếu có quyền Write, user sẽ được tạo, xóa) → Finish



Đăng nhập vào máy Client → Nhập ftp://192.168.50.1:5000 (kèm port) để kiểm tra

11. Thiết lập DNS server (1 máy Windows Server 2008 + 1 máy client Windows XP)

(Cấu hình card mạng, địa chỉ IP, Gateway, DNS, thêm ổ đĩa
và tạo OU, user, group,... tương tự như các bước ở trên)

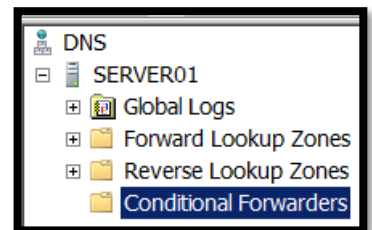
- **Windows Server 2008:** Server Manager → Add Roles → Server Roles → DNS Server
→ Next → Next → Finish

Administrative Tools → DNS

Forward Lookup Zones: phân giải tên máy ra địa chỉ IP

Reverse Lookup Zones: phân giải IP sang tên máy

Conditional Forwarders: là các máy chủ DNS chỉ có nhiệm vụ chuyển tiếp các truy vấn cho các tên miền cụ thể



Phân giải tên máy ra địa chỉ IP:

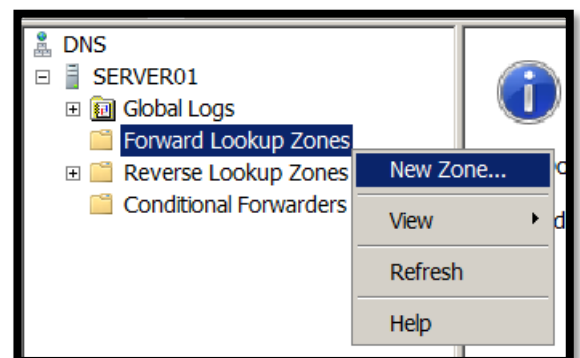
Tên server → Forward Lookup Zones

→ New Zones → Next → Primary Zone

→ Next → Zone name: testdns.com → Next

→ Do not allow dynamic updates → Next

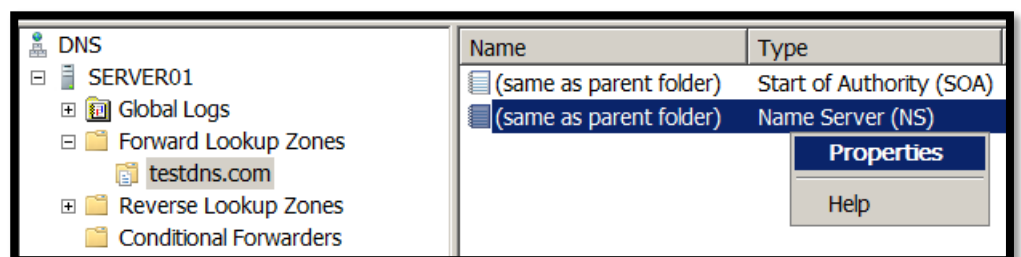
→ Finish



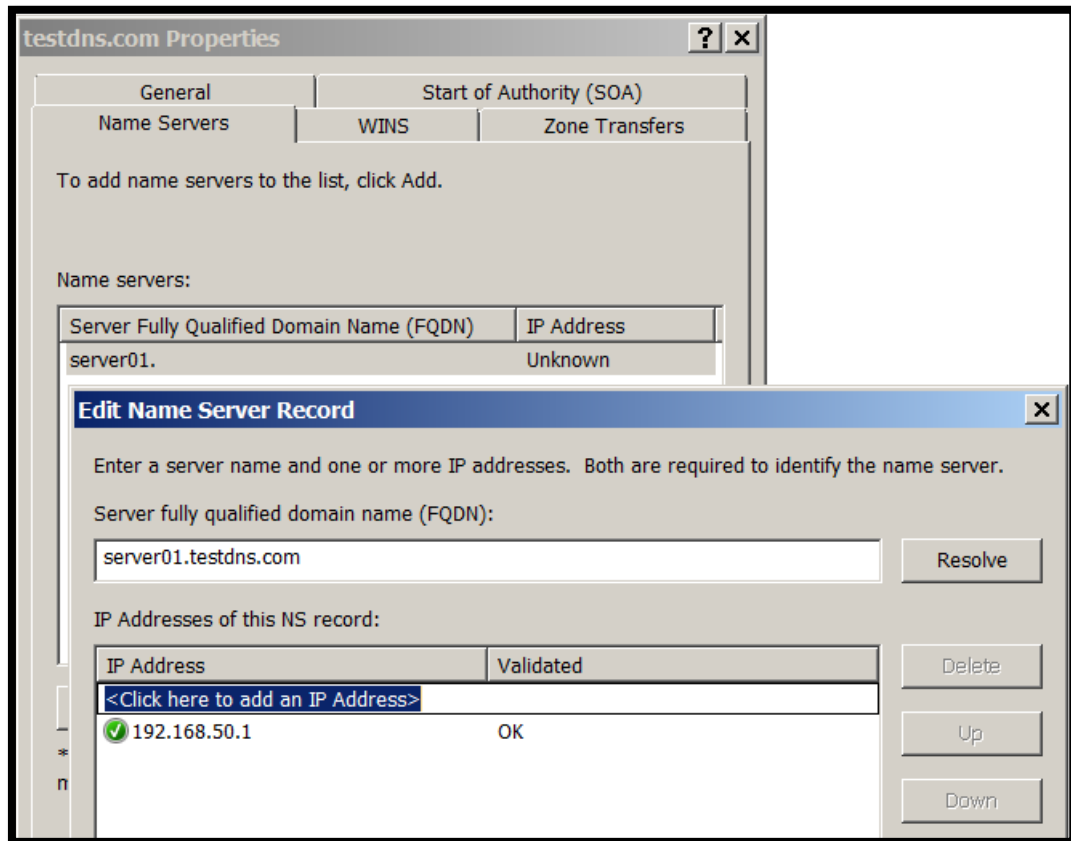
Chọn zone name

(testdns.com)

→ Properties

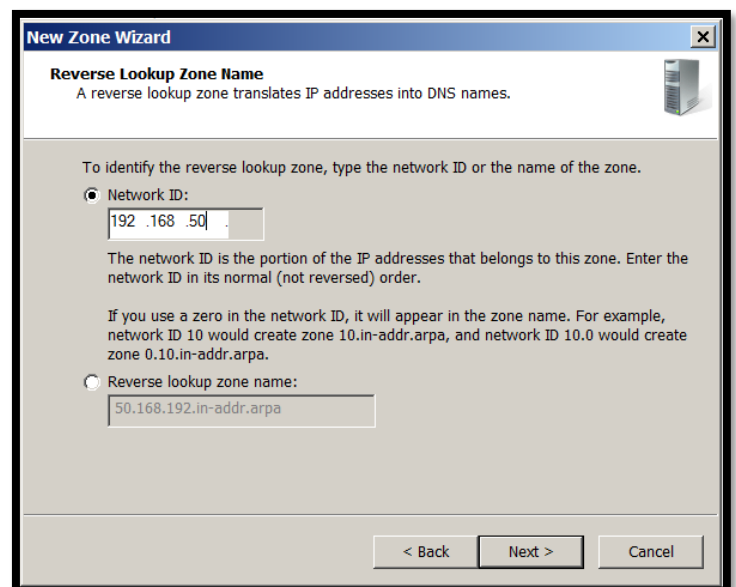


Hộp thoại Properties hiện ra → Name Servers → Server FQDN → Chọn Server
 → Nhập thêm tên domain (testdns.com) → IP Addresses of this NS record
 → Nhập địa chỉ IP của DNS Server → OK



Phân giải IP sang tên máy:

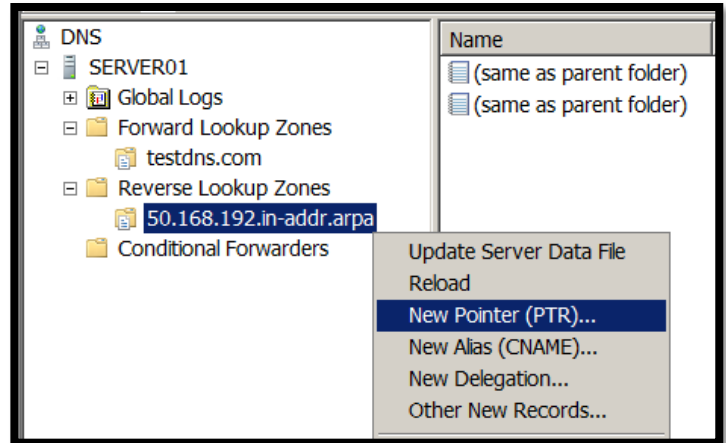
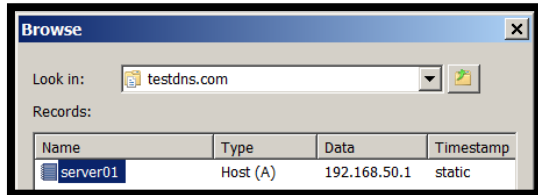
Tên server → Reverse Lookup Zones
 → New Zones → Next
 → Primary Zone → Next
 → IPv4 Reverse Lookup Zone
 → Next
 → Network ID: 192.168.50 (vì đây là địa chỉ mạng lớp C, nếu là lớp B thì sẽ chỉ nhập 172.16)
 → Next
 → Next
 → Do not allow dynamic updates
 → Next → Finish



Thực hiện các bước còn lại giống Forward Lookup Zones

Reverse Lookup Zones

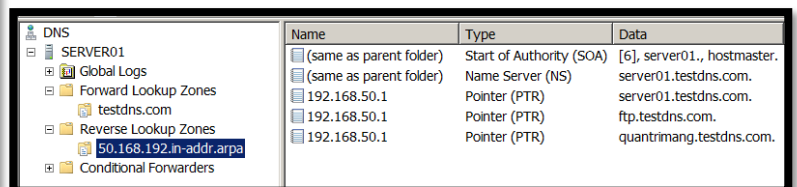
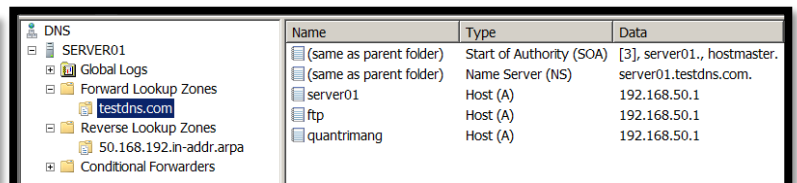
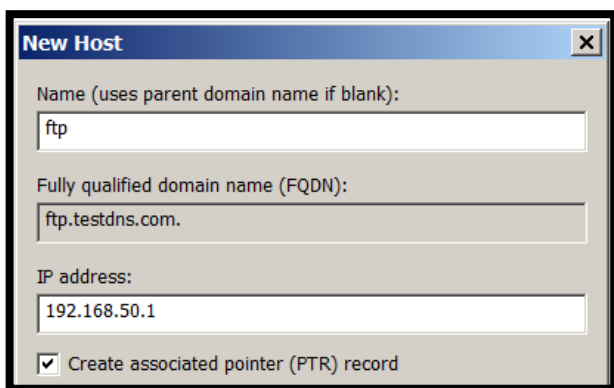
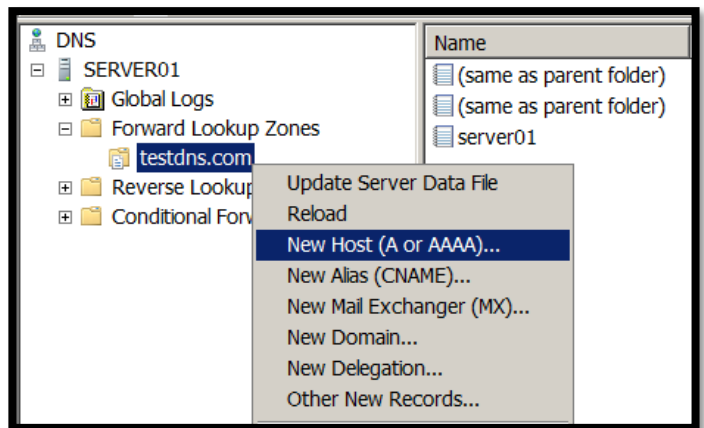
- New Pointer (PTR)...
- Host name → Browse
- Chọn tên của Server
- Forward Lookup Zones
- Chọn tên domain (testdns.com)
- Chọn tên Host(A)



Forward Lookup Zones

- New Host (A or AAAA)...
- Nhập tên Host
- Tích chọn "Create associated pointer (PTR) record"
- Nhập IP address: 192.168.50.1
- Add Host → OK → Done

Có thể nhập thêm Host để test



- **Windows Server 2008:** dùng nslookup để phân giải và lấy thông tin về các máy chủ

```
C:\>nslookup ftp.testdns.com
Server: ftp.testdns.com
Address: 192.168.50.1

DNS request timed out.
timeout was 2 seconds.
Name: ftp.testdns.com
Address: 192.168.50.1
```

```
C:\>nslookup quantrimang.testdns.com
Server: quantrimang.testdns.com
Address: 192.168.50.1

DNS request timed out.
timeout was 2 seconds.
Name: quantrimang.testdns.com
Address: 192.168.50.1
```

```
C:\>nslookup 192.168.50.1
Server: server01.testdns.com
Address: 192.168.50.1

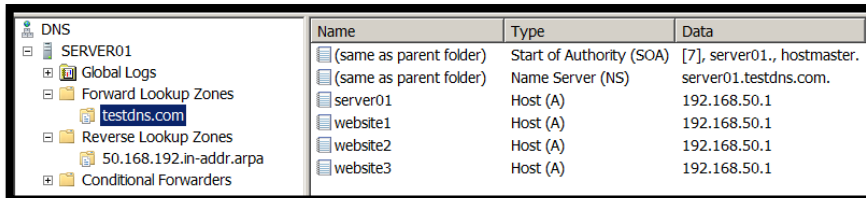
Name: ftp.testdns.com
Address: 192.168.50.1
```

12. Thiết lập Web server (1 máy Windows Server 2008 + 1 máy client Windows XP)

(Cấu hình card mạng, địa chỉ IP, Gateway, DNS, thêm ổ đĩa
và tạo OU, user, group,... tương tự như các bước ở trên)

- Windows Server 2008:

Đã cài đặt, cấu hình FTP, DNS Server và tạo thêm các host website1, website2, website3



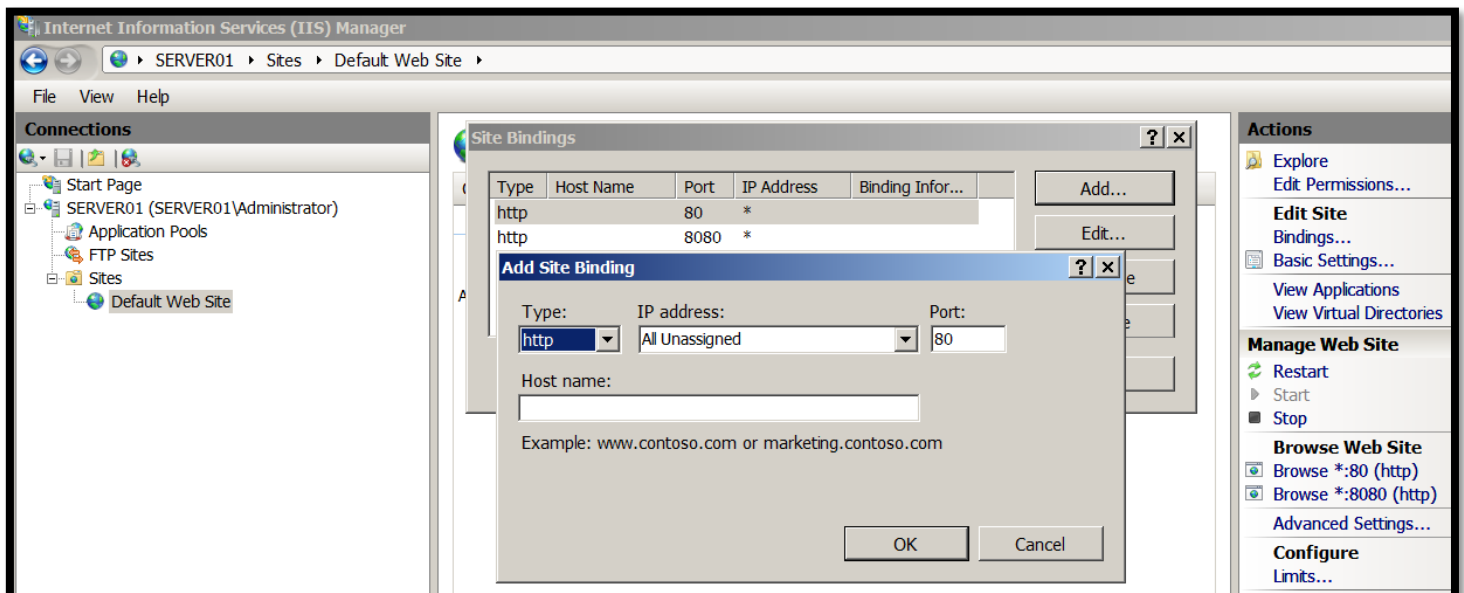
The screenshot shows the DNS console with a tree view on the left and a table of records on the right. The tree view includes SERVER01, Global Logs, Forward Lookup Zones (with testdns.com selected), Reverse Lookup Zones (with 50.168.192.in-addr.arpa selected), and Conditional Forwarders. The table lists records for the selected zones.

| Name | Type | Data |
|-------------------------|--------------------------|-----------------------------|
| (same as parent folder) | Start of Authority (SOA) | [7], server01., hostmaster. |
| (same as parent folder) | Name Server (NS) | server01.testdns.com. |
| server01 | Host (A) | 192.168.50.1 |
| website1 | Host (A) | 192.168.50.1 |
| website2 | Host (A) | 192.168.50.1 |
| website3 | Host (A) | 192.168.50.1 |



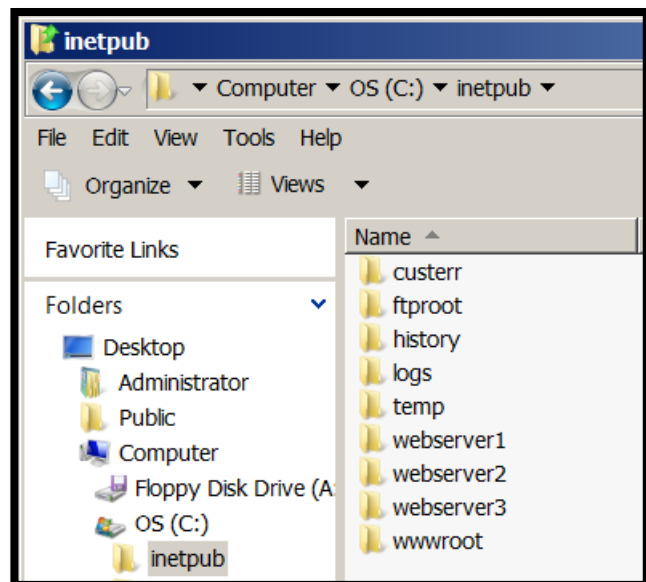
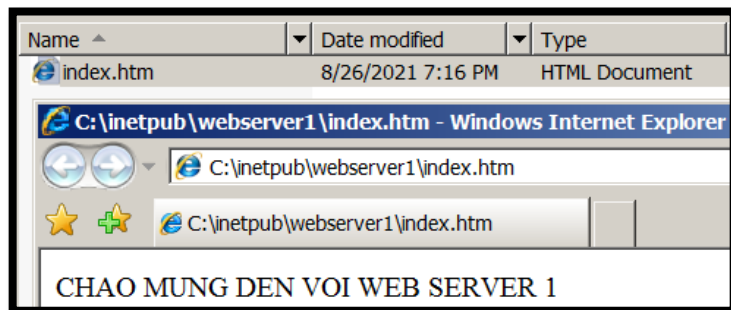
Mở Internet Information Services (IIS) Manager → Tên Server → Sites

→ Default Web Site → Chuột phải, chọn Edit Bindings... (hoặc chọn nút Bindings ở góc trên-bên phải) → Hộp thoại Site Bindings hiện ra → Add → Thêm Port: 8080 → OK



Tạo thư mục (webserver1, webserver2, webserver3) để chứa website trong C:\inetpub

→ Trong mỗi thư mục tạo một file index.htm chứa nội dung của website

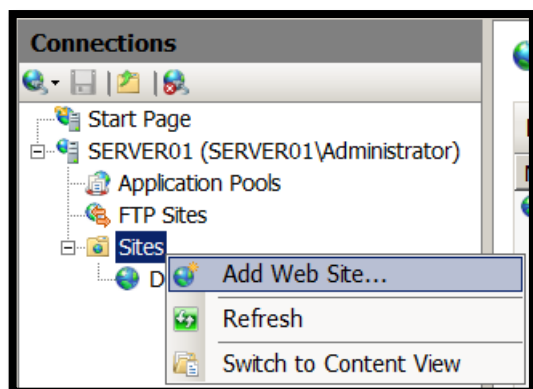
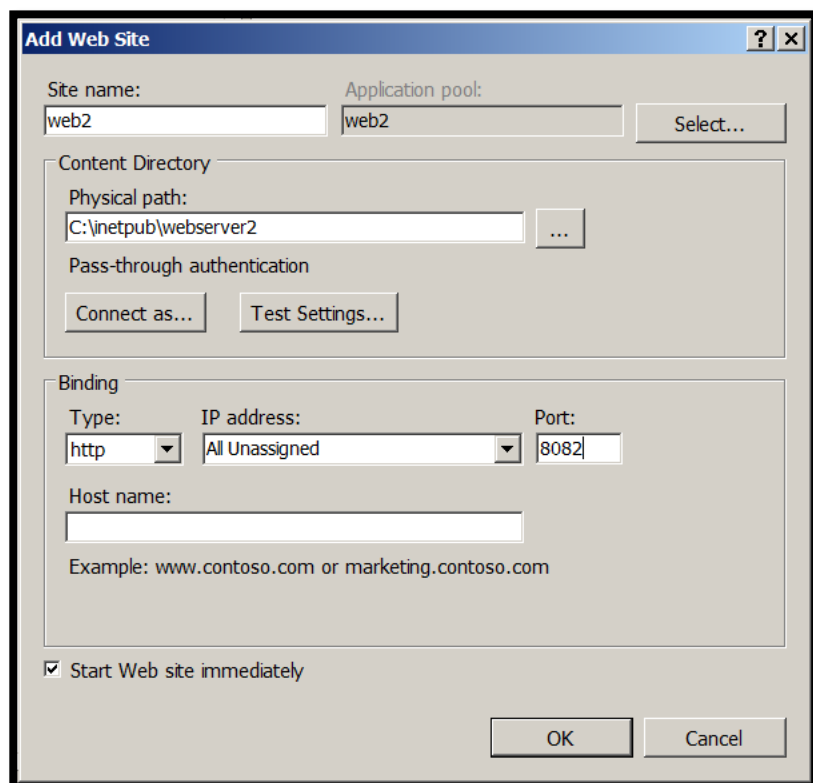


Trở lại Internet Information Services (IIS) Manager

→ Sites → Add Web Site...

→ Site name: web1 (đặt tên tùy thích, không quan trọng)

→ Port: 8082 (tránh chọn trùng với những port của hệ thống)



Cấu hình tường lửa để cho phép toàn bộ truy cập qua mạng:

Administrative Tools

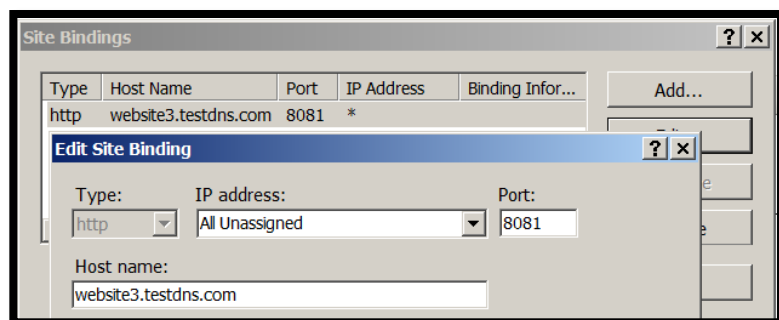
→ Windows Firewall with Advanced Security

→ Inbound Rules → New Rules → Rule Type: Custom

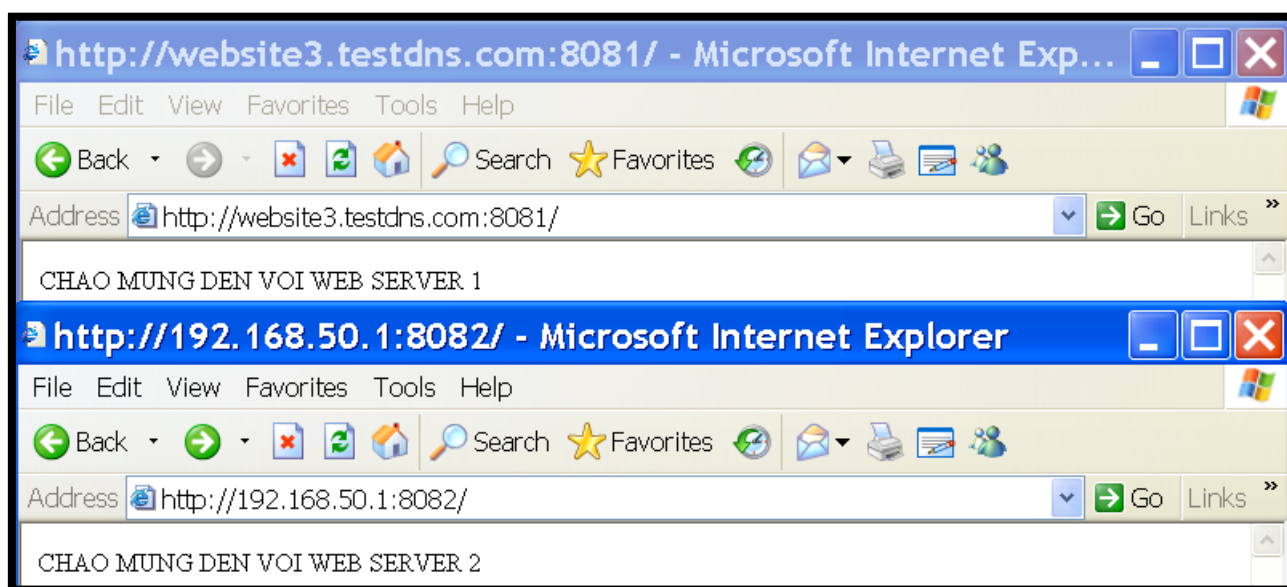
→ Program: All program → Next tất cả → Finish



Thử bind web1 vào website3:



- **Windows XP:** Thử truy cập bằng địa chỉ ip, tên dns và port



Flush DNS:

Hầu hết các hệ điều hành và các DNS client sẽ tự động lưu cache địa chỉ IP và các kết quả DNS gần đây, điều này giúp cho việc truy cập domain nhanh hơn do sử dụng trực tiếp các kết quả DNS trước đó trên máy. Nhưng nếu địa chỉ bị thay đổi (ví dụ: chuyển từ website1.testdns.com sang website3.testdns.com) trước khi cached DNS được cập nhật thì sẽ không thể truy cập vào được trang web

Flush DNS là việc tiến hành xóa bộ nhớ Cache DNS. Khi các Website thay đổi địa chỉ IP hay chuyển sang một máy chủ Web khác mà DNS Cache của bạn chưa kịp cập nhật thì chắc chắn lỗi sẽ xảy ra. DNS Cache sẽ giúp máy tính của bạn cập nhật lại thông tin của trang Web và truy cập thành công vào Website đó.

```
C:\>ipconfig /flushdns  
  
Windows IP Configuration  
  
Successfully flushed the DNS Resolver Cache.
```

13. Thiết lập cấu hình MDAemon Mail Server

(1 máy Windows Server 2008 + 1 máy client Windows XP)

(Cấu hình card mạng, địa chỉ IP, Gateway, DNS, thêm ổ đĩa và tạo OU, user, group,... tương tự như các bước ở trên)

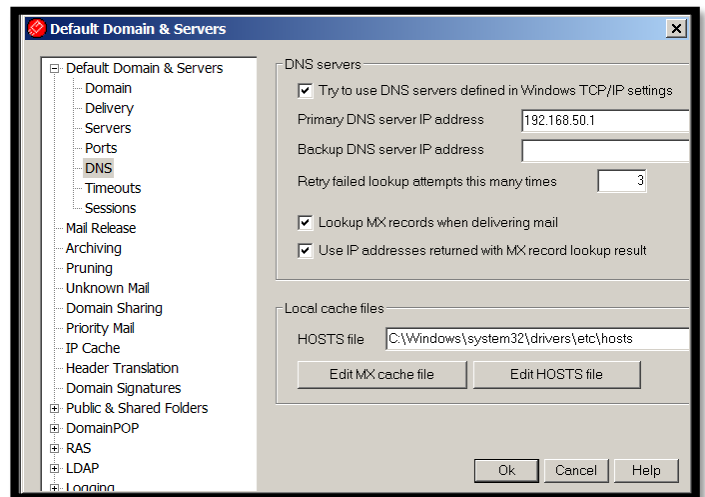
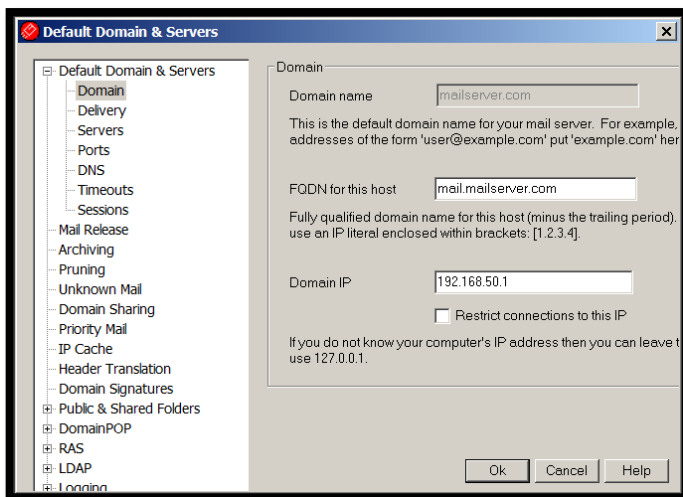
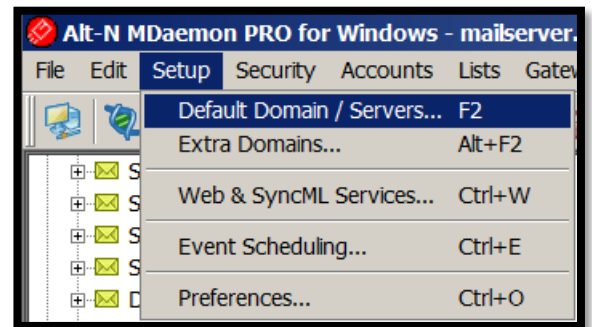
- **Windows Server 2008:** Cài MDAemon Mail Server v10 hoặc v11 (v11 khi cài sẽ yêu cầu kết nối mạng, **chỉnh card mạng sang NAT** (NAT cho phép máy ảo có quyền truy cập vào tài nguyên mạng bằng địa chỉ IP của máy Windows 10 bên ngoài) và IP động để truy cập được mạng và hoàn thành quá trình cài)

Tại giao diện của MDAemon Mail Server

→ Setup → Default Domain / Server...

→ Domain → FQDN for this host: thêm mail vào tên host (ví dụ: mail.mailserver.com)

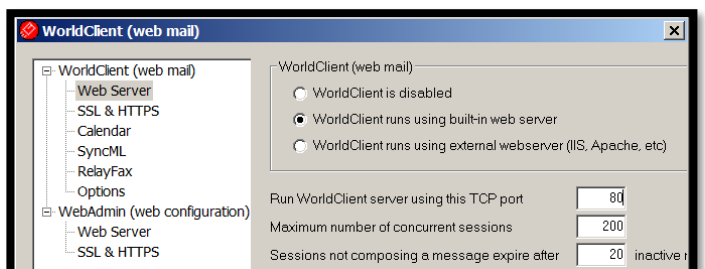
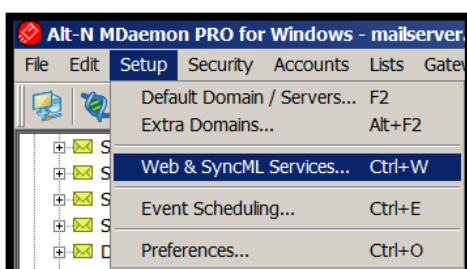
→ DNS → Primary DNS server IP address: nhập địa chỉ IP của máy mail server



Tại giao diện của MDAemon Mail Server

→ Setup → Web & SyncML Services... → Web Server

→ Run WorldClient server using this TCP port: thay 3000 thành 80

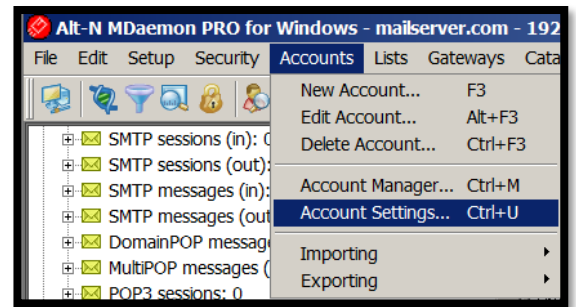


Tắt yêu cầu mật khẩu mạnh khi tạo user:

Accounts → Account Settings...

→ New Account Defaults

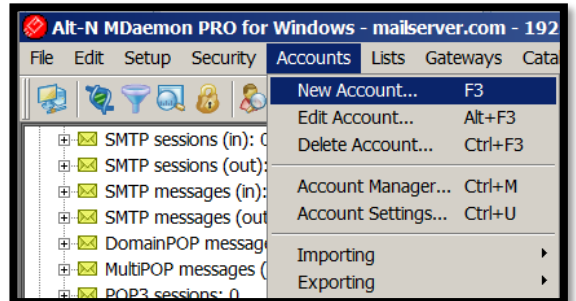
→ Bỏ chọn Require strong passwords



Tạo user: Accounts → New Account...

→ Account Settings → Account

→ Nhập tên người dùng và mật khẩu

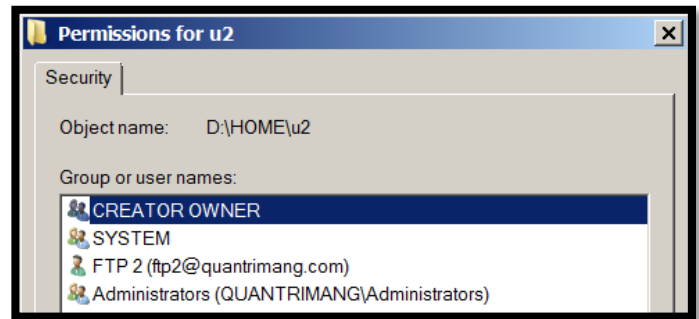
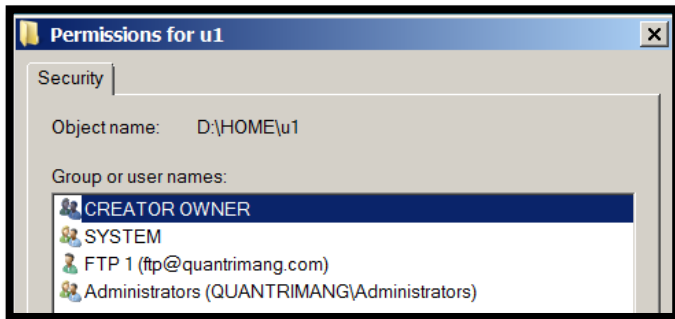


- **Windows XP:**

14. FTP Server, isolate User (1 máy Windows Server 2008 + 1 máy client Windows XP)

(Cấu hình card mạng, địa chỉ IP, Gateway, DNS, thêm ổ đĩa
và tạo OU, user, group,... tương tự như các bước ở trên)

- **Windows Server 2008:** Tạo người dùng, thư mục HOME, trong thư mục HOME chứa các thư mục con cùng tên với tên người dùng, phân quyền cho từng thư mục



Administrative Tools

→ Internet Information Services (IIS) 6.0 Manager

→ Tên Server

→ FTP Sites

→ New

→ FTP Site...

→ Nhập mô tả (tên của FTP)

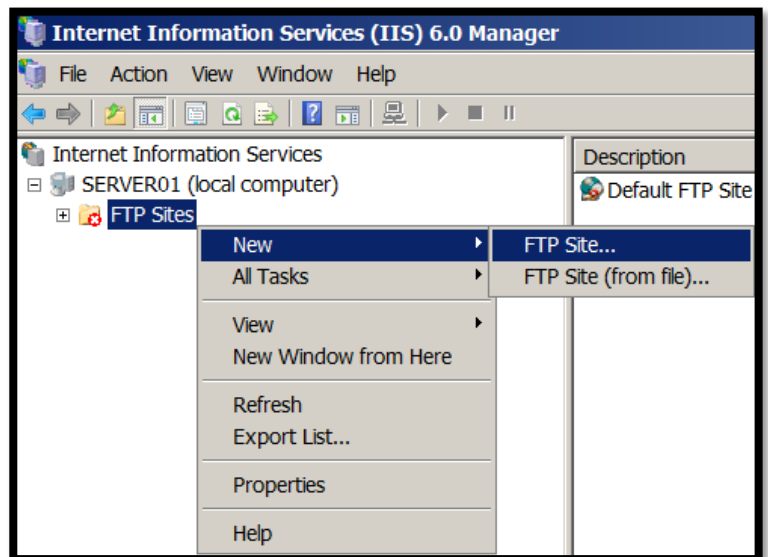
→ Next

→ IP Address and Port Settings: để mặc định

→ Next

→ FTP User Isolation: Isolate users → Next

→ Path: chọn đường dẫn chứa thư mục HOME → Next → Gán quyền Read & Write



- **Windows XP:**

15. Thiết lập FTP Site cách ly user Active Directory

16. Cài đặt, cấu hình DFS server (Distributed File System)

17. Cài đặt Email server - site to site