TRƯỜNG CAO ĐẲNG NGHỀ CÔNG NGHIỆP HÀ NỘI

Chủ biên: Trần Thị Ngân

Đồng tác giả: Dương Ngọc Việt

GIÁO TRÌNH

CHUYÊN ĐỀ (DOMAIN SERVER)

Hà Nội – 2013

Tuyên bố bản quyền

Địa chỉ liên hệ:

Trường Cao đẳng nghề Công nghiệp Hà Nội.

131 – Thái Thịnh – Đống Đa – Hà Nội

Điện thoại: (84-4) 38532033

Fax: (84-4) 38533523

Website: www.hnivc.edu.vn

MỞ ĐẦU : GIỚI THIỆU WINDOWS SERVER 2008

I. GIỚI THIỆU VỀ WINDOWS SERVER 2008

Microsoft Windows Server 2008 là thế hệ kế tiếp của hệ điều hành Windows Server, có thể giúp các chuyên gia công nghệ thông tin có thể kiểm soát tối đa cơ sở hạ tầng của họ và cung cấp khả năng quản lý và hiệu lực chưa từng có, là sản phẩm hơn hẳn trong việc đảm bảo độ an toàn, khả năng tin cậy và môi trường máy chủ vững chắc hơn các phiên bản trước đây.

Windows Server 2008 cung cấp những giá trị mới cho các tổ chức bằng việc bảo đảm tất cả người dùng đều có thể có được những thành phần bổ sung từ các dịch vụ từ mạng. Windows Server 2008 cũng cung cấp nhiều tính năng vượt trội bên trong hệ điều hành và khả năng chuẩn đoán, cho phép các quản trị viên tăng được thời gian hỗ trợ cho các doanh nghiệp.

Windows Server 2008 được thiết kế để cung cấp cho các tổ chức có được nền tảng sản xuất tốt nhất cho ứng dụng, mạng và các dịch vụ web từ nhóm làm việc đến những trung tâm dữ liệu với tính năng động, tính năng mới có giá trị và những cải thiện mạnh mẽ cho hệ điều hành cơ bản.

Cải thiện hệ điều hành cho máy chủ Windows.Thêm vào tính năng mới, Windows Server 2008 cung cấp nhiều cải thiệm tốt hơn cho hệ điều hành cơ bản so với hệ điều hành Windows Server 2003.

Những cải thiện có thể thấy được gồm có các vấn đề về mạng, các tính năng bảo mật nâng cao, truy cập ứng dụng từ xa, quản lý role máy chủ tập trung, các công cụ kiểm tra độ tin cậy và hiệu suất, nhóm chuyển đổi dự phòng, sự triển khai và hệ thống file.

1. Tính năng vượt trội

Microsoft Windows Server 2008 là hệ điều hành máy chủ windows thế hệ tiếp theo của hãng Microsoft.

Các tính năng được cải thiện mạnh mẽ so với phiên bản 2003:

+ An toàn bảo mật.
+ Truy cập ứng dụng từ xa.
+ Quản lý server tập trung.
+ Các công cụ giám sát hiệu năng và độ tin cậy.
+ Failover clustering và hệ thống file.

➔Hỗ trợ trong việc kiểm soát một cách tối ưu hạ tầng máy chủ, đồng thời tạo nên một môi trường máy chủ an toàn, tin cậy và hiệu quả hơn trước rất nhiều.

2. Các phiên bản cùa Windows Server 2008

- Windows Server 2008 Standard Edition
- Windows Server 2008 Enterprise Edition
- Windows Server 2008 Datacenter Edition
- Windows Web Server 2008

3. Yêu cầu phần cứng để cài đặt Windows Server 2008

Dưới đây là bảng yêu cầu phần cứng để cài đặt windows server 2008:

Category	Minimum / Recommended Requirements
Processor	• Minimum: 1GHz (x86 processor) or 1.4GHz (x64 processor) • Recommended: 2GHz or faster **Note:** For Itanium based systems an Intel Itanium 2 processor is required.
Memory	• Minimum: 512MB RAM • Recommended: 2GB RAM or greater • Maximum (32-bit systems): 4GB (Standard) or 64GB (Enterprise and Datacenter) • Maximum (64-bit systems): 32GB (Standard) or 2TB (Enterprise, Datacenter and Itanium-Based Systems)
Available Disk Space	• Minimum: 10GB • Recommended: 40GB or greater **Note:** Systems with RAM in excess of 16GB will require greater amounts of disk space to accommodate paging, hibernation, and dump files
Drive	DVD-ROM drive
Display and Peripherals	• Super VGA or greater-resolution monitor (800x600) • Keyboard • Microsoft Mouse or compatible pointing device

II. CÁC TÍNH NĂNG CỦA WINDOWS SERVER 2008

1. Công cụ quản trị Server Manager

Server Manager là một giao diện điều khiển được thiết kế để tổ chức và quản lý một server chạy hệ điều hành Windows Server 2008. Người quản trị có thể sử dụng Server Manager với những nhiều mục đích khác nhau.

- Quản lý đồng nhất trên một server
- Hiển thị trạng thái hiện tại của server
- Nhận ra các vấn đề gặp phải đối với các role đã đoợc cài đặt một cách dễ dàng hơn
- Quản lý các role trên server, bao gồm việc thêm và xóa role
- Thêm và xóa bỏ các tính năng
- Chẩn đoán các dấu hiệu bất thường
- Cấu hình server: có 4 công cụ (Task Scheduler, Windows Firewall, Services và WMI Control).
- Cấu hình sao lưu và lưu trữ: các công cụ giúp bạn sao lưu và quản lý ổ đĩa là Windows Server Backup và Disk Management đều nằm trên Server Manager.

2. Windows Server Core

- Server Core là một tính năng mới trong Windows Server 2008. Nó cho phép có thể cài đặt với mục đích hỗ trợ đặc biệt và cụ thể đối với một số role.
- Tất cả các tương tác với Server Core được thông qua các dòng lệnh.

Server Core mang lại những lợi ích sau:

+Giảm thiểu được phần mềm, vì thế việc sử dụng dung lượng ổ đĩa cũng được giảm. Chỉ tốn khoảng 1GB khi cài đặt.

+ Bởi vì giảm thiểu được phần mềm nên việc cập nhật cũng không nhiều.

+ Giảm thiểu tối đa những hành vi xâm nhập vào hệ thống thông qua các port được mở mặc định.

+ Dễ dàng quản lý.

- Server Core không bao gồm tất cả các tính năng có sẵn trong những phiên bản cài đặt Server khác. Ví dụ như .NET Framework hoặc Internet Explorer.

3. PowerShell

- PowerShell là một tập hợp lệnh. Nó kết nối những dòng lệnh shell với một ngôn ngữ script và thêm vào đó hơn 130 công cụ dòng lệnh(được gọi là cmdlets).Hiện tại, có thể sử dụng PowerShell trong:

+ Exchange Server

+ SQL Server

+ Terminal Services

+ Active Directory Domain Services.

+ Quản trị các dịch vụ, xử lý và registry.

- Mặc định, Windows PowerShell chưa được cài đặt. Tuy nhiên bạn có thể cài đặt nó một cách dễ dàng bằng cách sử dụng công cụ quản trị Server Manager và chọn Features > Add Features

4. Windows Deloyment Services.

- Windows Deployment Services được tích hợp trong Windows Server 2008 cho phép bạn cài đặt hệ điều hành từ xa cho các máy client mà không cần phải cài đặt trực tiếp. WDS cho phép bạn cài đặt từ xa thông qua Image lấy từ DVD cài đặt. Ngoài ra, WDS còn hỗ trợ tạo Image từ 1 máy tính đã cài đặt sẵn Windows và đầy đủ các ứng dụng khác.

- Windows Deployment Serviece sử dụng định dạng Windows Image (WIM). Một cải tiến đặc biệt với WIM so với RIS là WIM có thể làm việc tốt với nhiều nền tảng phần cứng khác nhau.

5. Terminal Services.

- Terminal Services là một thành phần chính trên Windows Server 2009 cho phép user có thể truy cập vào server để sử dụng những phần mềm.

- Terminal Services giúp người quản trị triển khai và bảo trì hệ thống phần mềm trong doanh nghiệp một cách hiệu quả. Người quản trị có thể cài đặt các chương trình phần mềm lên Terminal Server mà không cần cài đặt trên hệ thống máy client, vì thế việc cập nhật và bảo trì phần mềm trở nên dễ dàng hơn.

- Terminal Services cung cấp 2 sự khác biệt cho người quản trị và người dùng cuối :

- Dành cho người quản trị: cho phép quản trị có thể kết nối từ xa hệ thống quản trị bằng việc sử dụng Remote Desktop Connection hoặc Remote Desktop.

- Dành cho ngọời dùng cuối: cho phép người dùng cuối có thể chạy các chương trình từ Terminal Services server.

6. Network Access Protection

- Network Access Protection (NAP) là một hệ thống chính sách thi hành (Health Policy Enforcement) được xây dựng trong các hệ điều hành Windows Server 2008.
- Cơ chế thực thi của NAP:

+ Kiểm tra tình trạng an toàn của client.

+ Giới hạn truy cập đối với các máy client không an toàn.

+ NAP sẽ cập nhật những thành phần cần thiết cho các máy client không an toàn, cho đến khi client đủ điều kiện an toàn.Cho phép client kết nối nếu client đã thỏa điều kiện.

+ NAP giúp bảo vệ hệ thống mạng từ các client.

+ NAP cung cấp bộ thư viên API (Application Programming Interface), cho phép các nhà

quản trị lập trình nhằm tăng tính bảo mật cho mình

7. Read-Only Domain Controllers

- Read-Only Domain Controller (RODC) là một kiểu Domain Controller mới trên Windows Server 2008.Với RODC, doanh nghiệp có thể dễ dàng triển khai các Domain Controller ở những nơi mà sự bảo mật không được đảm bảo về bảo mật. RODC là một phần dữ liệu của Active Directory Domain Services.
- Vì RODC là một phần dữ liệu của ADDS nên nó lưu trữ mọi đối tượng, thuộc tính và các chính sách giống như domain controller, tuy nhiên mật khẩu thì bị ngoại trừ.

8. Công nghệ Failover Clustering.

- Clustering là công nghệ cho phép sử dụng hai hay nhiều server kết hợp với nhau để tạo thành một cụm server để tăng cường tính ổn định trong vận hành.Nếu server này ngưng hoạt động thì server khác trong cụm sẽ đảm nhận nhiệm vụ mà server ngưng hoạt động đó đang thực hiện nhằm mục đích hoạt động của hệ thống vẫn bình thường. Quá trình chuyên giao gọi là fail-over.

Những phiên bản sau hỗ trợ:

. Windows Server 2008 Enterprise

. Windows Server 2008 Datacenter

. Windows Server 2008 Itanium

9. Windows Firewall with Advance Security

- Windows Firewall with Advance Security cho phép người quản trị có thể cấu hình đa dạng và nâng cao để tăng cường tính bảo mật cho hệ thống.
- Windows Firewall with Advance Security có những điểm mới:

+ Kiểm soát chặt chẽ các kết nối vào và ra trên hệ thống (inbound và outbound)

+ IPsec được thay thế bằng khái niệm Connection Security Rule, giúp bạn có thể kiểm soát và quản lý các chính sách, đồng thời giám sát trên firewall. Kết hợp với Active Directory.

+ Hỗ trợ đầy đủ IPv6.

III. MỘT SỐ TÍNH NĂNG MỚI CỦA WINDOWS SERVER 2008

1. Công nghệ ảo hóa Hyper-V

Hyper-V là công nghệ ảo hóa server thế hệ mới của Microsoft, sự thay đổi lớn nhất mà Microsoft mang lại so với phiên bản Windows Server 2003. Hyper-V hoạt động trên nền hệ điều hành 64-bit. Với Hyper-V, người sử dụng có thể sở hữu một nền tảng ảo hóa linh hoạt, bảo mật, tối đa hiệu suất và tiết kiệm chi phí:

+ Hyper-V có thể thích nghi với doanh nghiệp lớn với hàng nghìn máy tính hoặc các doanh nghiệp nhỏ hay văn phòng chi nhánh. Hyper-V hỗ trợ bộ nhớ ảo lên đến 64GB, đa bộ vi xử lý.

+ Khả năng bảo mật giống như các server vật lý. Kết hợp các cộng cụ bảo mật Windows Firewall, Network Access Protection…do đó tính bảo mật tốt như môi trường thật.

+ Hyper-V giúp khai thác tối đa hiệu suất sử dụng phần cứng server. Bằng việc hợp nhất server, cho phép một server vật lý có thể đóng nhiều vai trò của nhiều server. Từ đó, tiết kiệm được chi phí từ các khoảng mua server, điện, không gian và bảo trì. Hyper-V chỉ có thể hỗ trợ đến 32 bộ vi xử lý.

2. Processor Compatibility Mode

- Cho phép di trú các máy ảo sang một máy chủ vật lý khác với một phiên bản CPU khác (nhưng không phải là CPU của nhà sản xuất khác). Trước đây, để chuyển một máy ảo Hyper-V sang một phần cứng khác, các CPU phải giống nhau, điều đó yêu cầu người dùng thường phải mua lại phần cứng mới.

3. File Classification Infrastructure

- FCI là một tính năng built-in cho phép các chuyên gia CNTT phân loại và quản lý dữ liệu trong các máy chủ file. Dữ liệu có thể được phân loại với tác động doanh nghiệp mức thấp, cao hoặc trung bình, sau đó người dùng có thể backup các dữ liệu quan trọng nhất dễ dàng hơn và hiệu quả hơn.

4. Quản lý trong ỗ đĩa và file:

- Cung cấp khả năng thay đổi kich thước phân vùng.
- Shadow Copy hỗ trợ ổ đĩa quang, ổ đĩa mạng.
- Distributed File System được cải tiến.
- Cải tiến Failover Clustering.
- Internet Storage Naming Server cho phép đăng ký, hủy đăng ký tập trung và truy xuất tới các ổ đĩa cứng iSCS.

5. Cải tiến giao thức và mã hóa

- Hỗ trợ mã hóa 128 và 256 bit cho giao thức chứng thực Keberos.
- Hàm API mã hóa mới hỗ trợ mã hóa vòng elip và cải tiến quản lý chứng chỉ.
- Giao thức VPN mới Secure Socket Tunneling Protocol.
- AuthIP được sử dụng trong mạng VPN Ipsec.
- Giao thức Server Message Block 2.0 cung cấp các cải tiến trong truyền thông.

6. Một số tính năng khác

- Windows Deployment Services thay thế cho Automated Deployment Services và Remote Installation Services.
- IIS 7 thay thế IIS 6, tăng cường khả năng bảo mật, cải tiến công cụ chuẩn đoán, hỗ trợ quản lý.
- Có thành phần "Desktop Experience" cung cấp khả năng cải tiến giao diện.

IV. CÁC LỢI ÍCH CỦA WINDOWS SERVER 2008

Windows Server 2008 mang đến lợi ích trong bốn lĩnh vực:Web, Ảo hóa, Bảo mật, Nền tảng vững chắc cho các hoạt động của tổ chức

1. Web

-Windows Server 2008 cung cấp một nền tảng đồng nhất để triển khai dịch vụ Web nhờ tích hợp IIS7.0,ASP.NET,Windows Communication Foundation và Microsoft Windows SharePoint Services.

- Lợi ich của IIS 7.0:

+ Tinh năng phân tích
+ Quản trị hiệu quả.
+ Nâng cao tính bảo mật.
+ Giảm chi phí hỗ trợ.
+ Giao diện thân thiện và tiện dụng
+ Hỗ trợ việc sao chép giữa các site.
+ Copy dễ dàng các thiết lập của trang web giữa các máy chủ web khác nhau mà không cần phải thiết lập gì thêm.
+ Chính sách phân quyền quản trị các ứng dụng và các site rõ ràng

2. Ảo hóa :

- Phiên bản 64 bit của Windows Server 2008 được tích hợp sẵn công nghệ ảo hóa hypervisor :

+ Cho phép máy ảo tương tác trực tiếp với phần cứng máy chủ hiệu quả hơn.
+ Có khả năng ảo hóa nhiều hệ điều hành khác nhau trên cùng 1 phần cứng máy chủ sẽ làm giảm chi phí, tăng hiệu suất sử dụng phần cứng, tối ưu hóa hạ tầng, nâng cao tính sẵn sàng của máy chủ.
+ Tiết kiệm chi phí mua sắm bản quyền phần mềm.
+ Tich hợp và tập trung các ứng dụng phục vụ cho việc truy cập từ xa một cách dễ dàng bằng cách sử dụng Terminal Services.

3. Bảo mật:

- Các tính năng an ninh bao gồm: Network Access Protection, Read-Only Domain Controller, BitLocker, Windows Firewall… cung cấp các mức bảo vệ chưa từng có cho hệ thống mạng, dữ liệu và công việc của tổ chức.

3.1. Network Access Protection (NAP):

- NAP dùng để thiết lập chính sách mạng đối với các máy trạm khi máy trạm đó muốn kết nối váo hệ thống mạng của tổ chức. Yêu cầu an ninh đối với máy trạm được kết nối với hệ thống mạng:
- Đã cài đặt phầm mềm diệt virus.
- Đã cập nhật phiên bản mới.
- Đã cài đặt các bản và lỗi hệ thống hoặc đã cài đặt phần mềm firewall.

3.2. Read-Only Domain Controller (RODC):

Là một kiểu Domain Controller (DC).
- RODC chứa một bản sao các dữ liệu "chỉ đọc" của dữ liệu Active Directory (AD).
- User không thẻ ghi trực tiếp vào RODC.
- RODC không chứa thông tin về mật khẩu trong AD, mà chỉ caching các users được phép sử dụng ở đó.

➔ RODC thích hợp cho việc triển khai ở các chi nhánh, nơi có điều kiện bảo mật kém cũng như trình độ của nhân viên IT còn hạn chế.

3.3. BitLocker:

Bảo vệ an toàn cho máy chủ, máy trạm, máy tính di động.
- Mã hóa nội dung của ổ đĩa nhằm ngăn cản
- Nâng cao khả năng bảo vệ dữ liệu: kết hợp chức năng mã hóa tập tin hệ thống và kiểm tra tinh toàn vẹn của các thành phần khi boot.
- Toàn bộ tập tin hệ thống được mã hóa, gồm cả file swap và file hibernation.

3.4. Windows Firewall:

- Ngăn chặn các lưu lượng mạng theo cấu hình và các ứng dụng dạng chạy để bảo vệ mạng khỏi các chương trình và người dùng nguy hiểm.
-Hỗ trợ ngăn chặn các thông tin vào và ra.
- Sử dụng MMC snap-in (Windows Firewall with Adbanced Security) để đơn giản hóa việc cấu hình, quản trị.

V. Các Phiên bản của Windows Server 2008

Windows Server 2008: ứng dụng cho các trung tâm data lớn, ứng dụng nghiệp vụ riêng,... khả năng mở rộng cao cho tới 64 bộ xử lý.

Windows Server 2008 Standard Edition

Windows Server 2008 Standard là một trong những phiên bản ít tốn kém nhất của các phiên bản khác nhau có sẵn. Windows Server 2008 Stardard hỗ trợ tới 4GB RAM và 4 bộ vi xử lý.

Chủ yếu nhắm mục tiêu và các doanh nghiệp vừa và nhỏ. Chỉ có thể nâng cấp lên Windows Server 2008 Standard từ Windows 2000 Server và Windows Server 2003 Standard Edition.

Windows Server 2008 Enterprise Edition

- Windows Server 2008 Enterprise Edition cung cấp chức năng lớn hơn và có khả năng mở rộng hơn so với bản tiêu chuẩn. Cũng như phiên bản Standard Edition thì

phiên bản Enterprise cũng có cả hai phiên bản 32-bit và 64-bit. Hỗ trợ 8 bộ xử lý và lên tới 64GB bộ nhớ RAM trên hệ thống 32-bit và 2TB RAM trên hệ thống 64-bit.
- Các tính năng khác của ấn bản Doanh nghiệp bao gồm hỗ trợ Clustering đến 8 nút và Active Directory Federated Services (AD FS).
- Các phiên bản Windows Server 2000, Windows 2000 Advanced Server, Windows Server 2003 Standard Edition và Windows Server 2003 Enterprise Edition đều có thể được nâng cấp lên Windows Server 2008 Enterprise Edition.

Windows Server 2008 Datacenter Edition

- Phiên bản Datacenter đại diện cuối cùng của loạt sản phẩm máy chủ Windows 2008 và mục tiêu là nhiệm vụ quan trọng đòi hỏi các doanh nghiệp ổn định và mức độ thời gian hoạt động cao. Windows Server 2008 phiên bản Datacenter là liên hệ chặt chẽ với các phần cứng cơ bản thông qua việc thực hiện tùy chỉnh Hardware Abstraction Layer (HAL).
- Windows server 2008 Datacenter cũng hỗ trợ hai phiên bản 32 bit và 64 bit. Nó hỗ trợ 64GB bộ nhớ RAM trên nền 32 bit và lên tới 2TB RAM trên nền 64 bít. Ngoài ra phiên bản này còn hỗ trợ tối thiểu là 8 bộ vi xử lý và tối đa là 64.
- Để nâng cấp lên phiên bản này thì phải là các phiên bản Datacenter 2000 và 2003.

Windows Web Server 2008

- Windows Web Server 2008 là một phiên bản của Windows Server 2008 được thiết kế chủ yếu cho mục đích cung cấp các dịch vụ web. Nó bao gồm Internet Information Services (IIS) 7,0 cùng với các dịch vụ liên quan như Simple Mail Transfer Protocol (SMTP) và Telnet. Nó cũng có các phiên bản 32-bit và 64-bit, phiên bản và hỗ trợ lên đến 4 bộ vi xử lý. RAM được giới hạn 4GB và 32GB trên 32-bit và 64-bit hệ thống tương ứng.
- Windows Web Server 2008 thiếu nhiều tính năng hiện diện trong các phiên bản khác như phân nhóm,mã hóa ổ đĩa BitLocker, Multi I/O,Windows Internet Naming Service (WINS),Removable Storage Management và SAN Management.

CHƯƠNG 1 : CÀI ĐẶT WINDOWS SERVER 2008

I. YÊU CÀU PHẦN CỨNG

Phần cứng	Yêu cầu tối thiểu	Đề nghị
Bộ vi xử lý	1 Ghz (x86), 1,4 Ghz (x64)	2Ghz hoặc lớn hơn
RAM	512MB RAM	2GB
Dung lượng trống	15GB	40GB

II. CÀI ĐẶT WINDOWS SERVER 2008

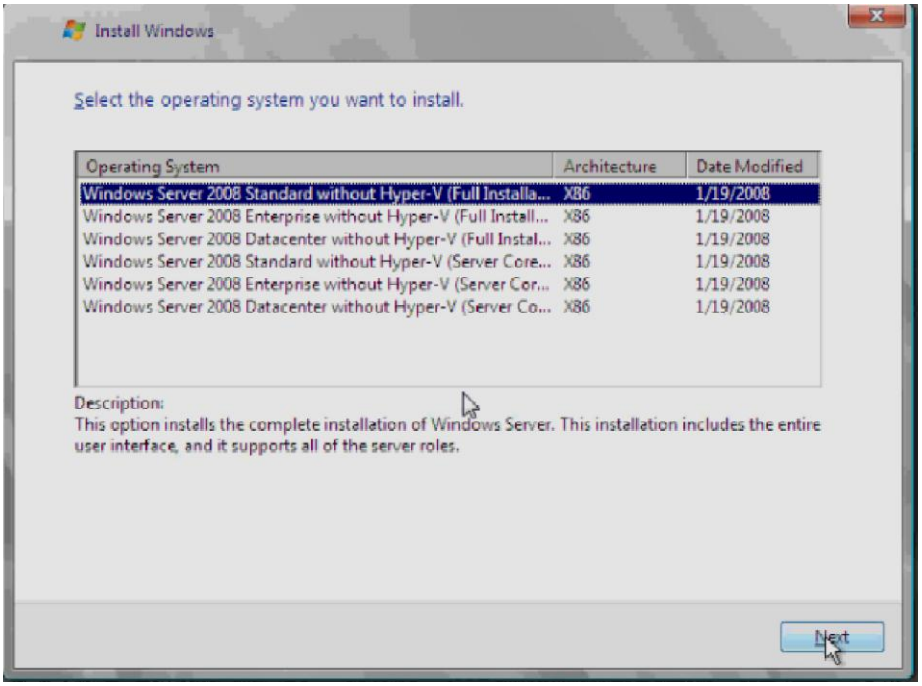
Đặt đĩa CD vào ổ đĩa, khởi động lại máy tính và bắt đầu tiến hành quá trình cài đặt.

Language to installk : ngôn ngữ bạn muốn hiển thị.

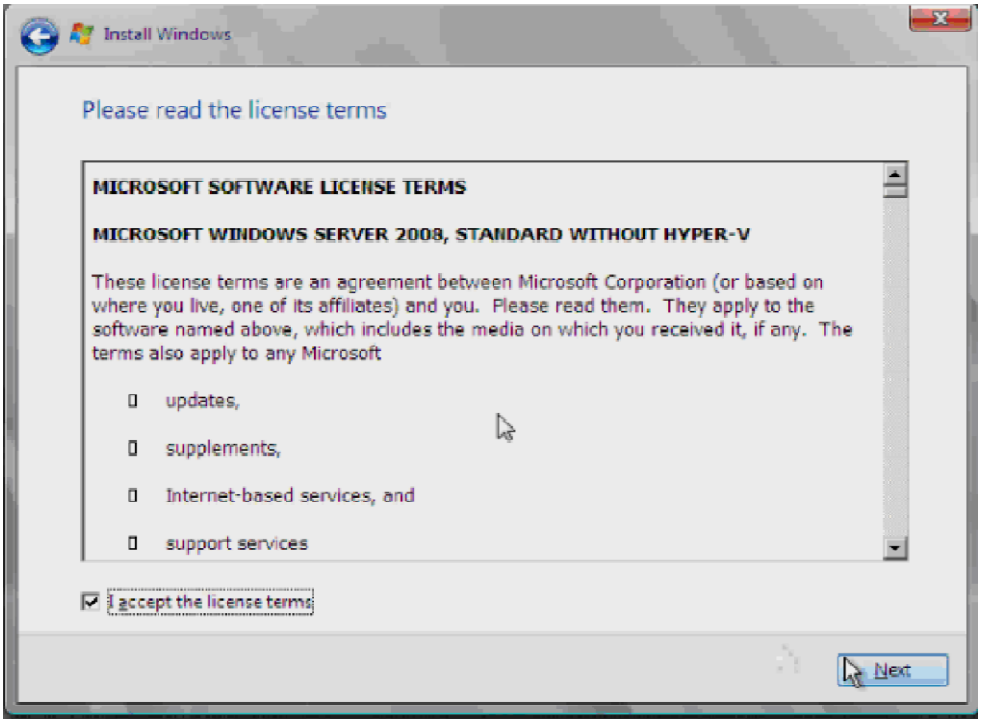
Time and currency format : định dạng thời gian và tiền tệ.

Keyboard or input method : định dạng bàn phím và phương thức nhập chữ.Sau khi lựa chọn, click **Next** để tiếp tục cài đặt

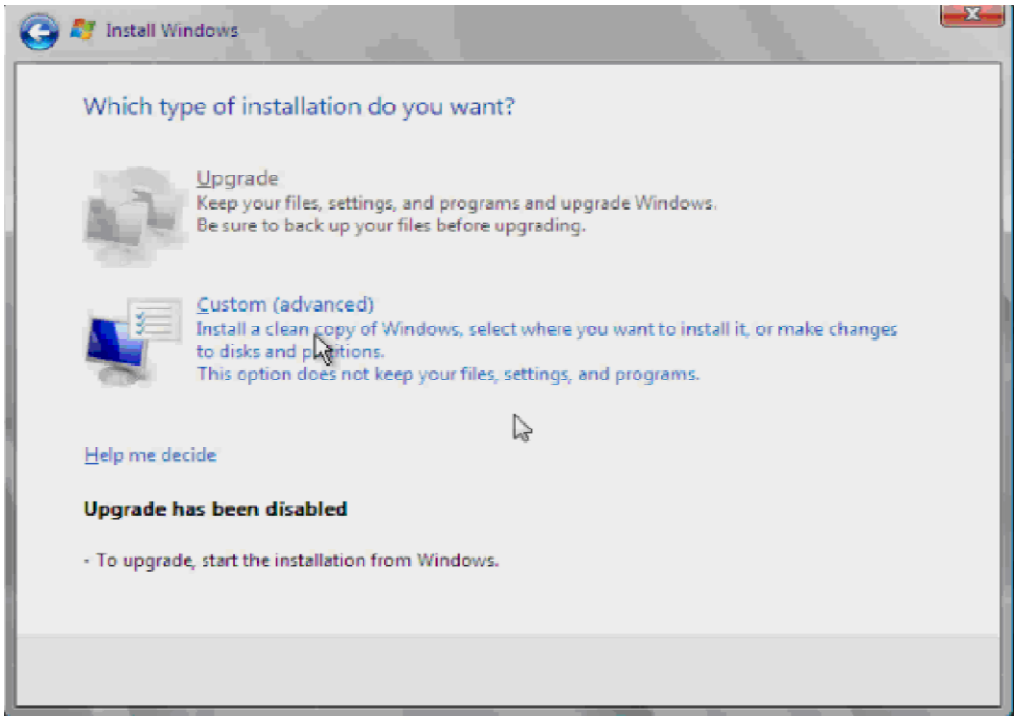
Click **Install now** để bắt đầu cài đặt.



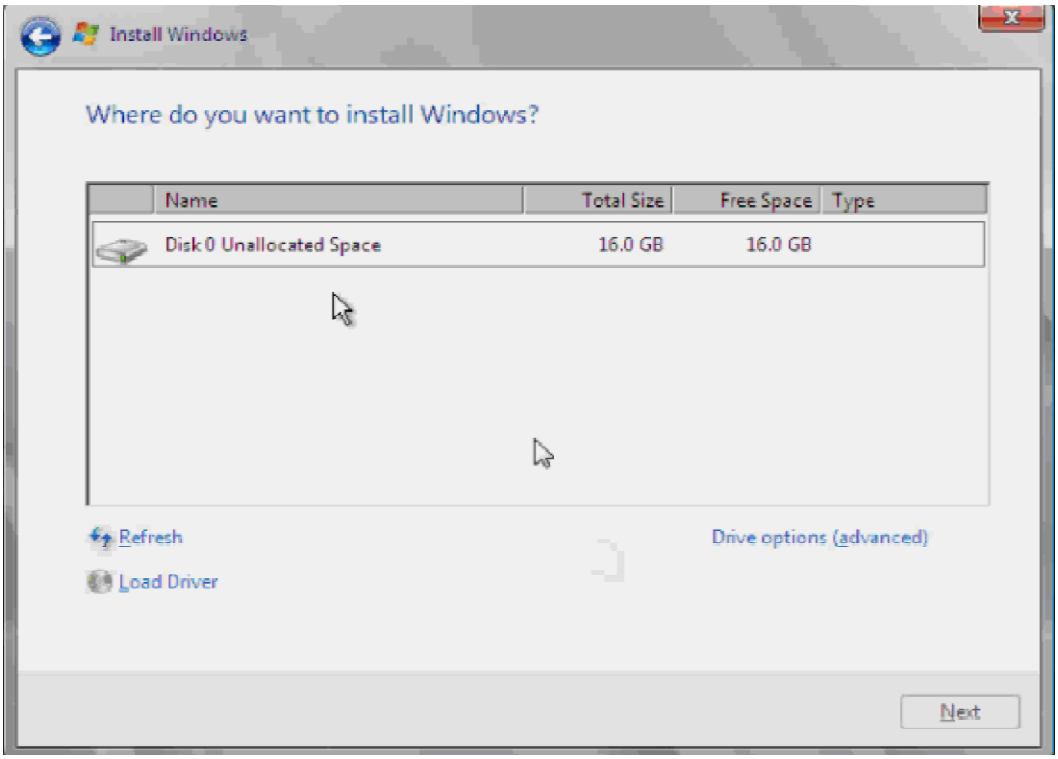
Lựa chọn phiên bản Windows Server thích hợp, ở đây chúng ta chọn phiên bản Windows Server Standard without Hyper-V. Click **Next** để tiếp tục.



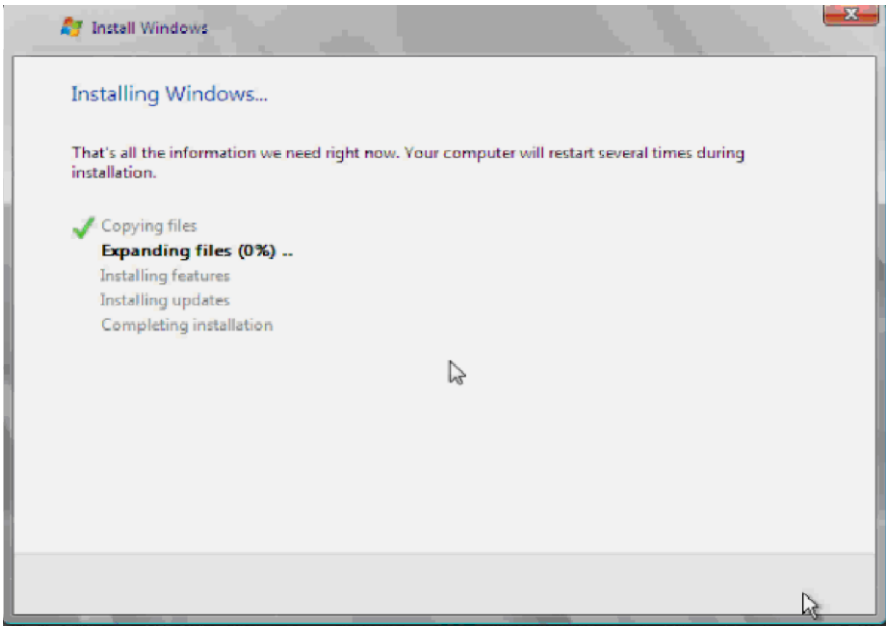
Tại bảng MICROSOFT PRE-RELEASE SOFTWARE LICENSE TERMS là những điều khoản sử dụng sản phẩm của Microsoft. Đánh dấu chọn **vào I accept the license terms** để chấp nhận những điều khoản đó và click **Next** để tiếp tục.



Chọn **Custom (advaneced)** để tiến hành cài đặt tùy chọn.

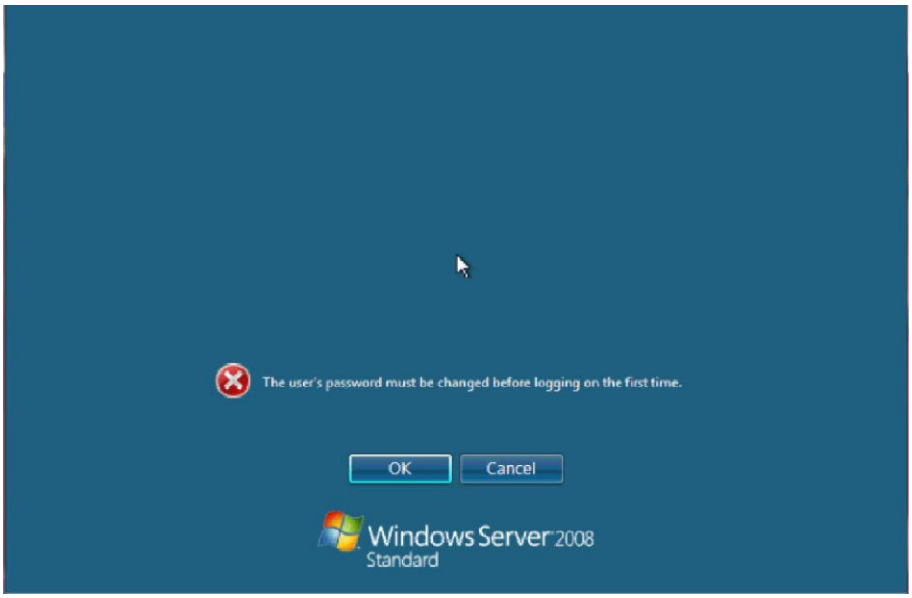


Tiếp theo là chọn ổ đĩa để cài dặt Windows. Tiếp tục click **Next** sau khi đã chọn ổ đĩa cài đặt.



Đợi cho đến khi hoàn tất cài đặt Windows Server 2008

Sau khi hệ thống hoàn tất cái đặt sẽ tự động đăng nhập vời tài khoản Administrator, tuy nhiên mật khẩu đang ở trạng thái trống (blank) vì thế cần phải thiết lập mật khẩu ở lần đăng nhập đầu tiên.

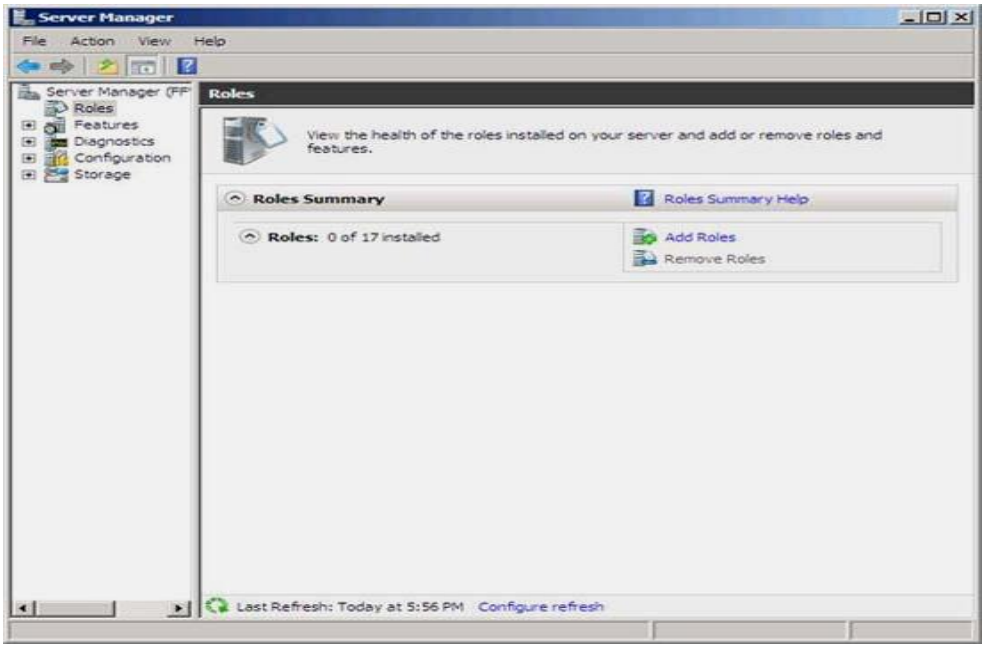


Click OK để tiến hành thay đổi mật khẩu.Sau đó đăng nhập vào bằng mật khẩu vừa thay đổi.

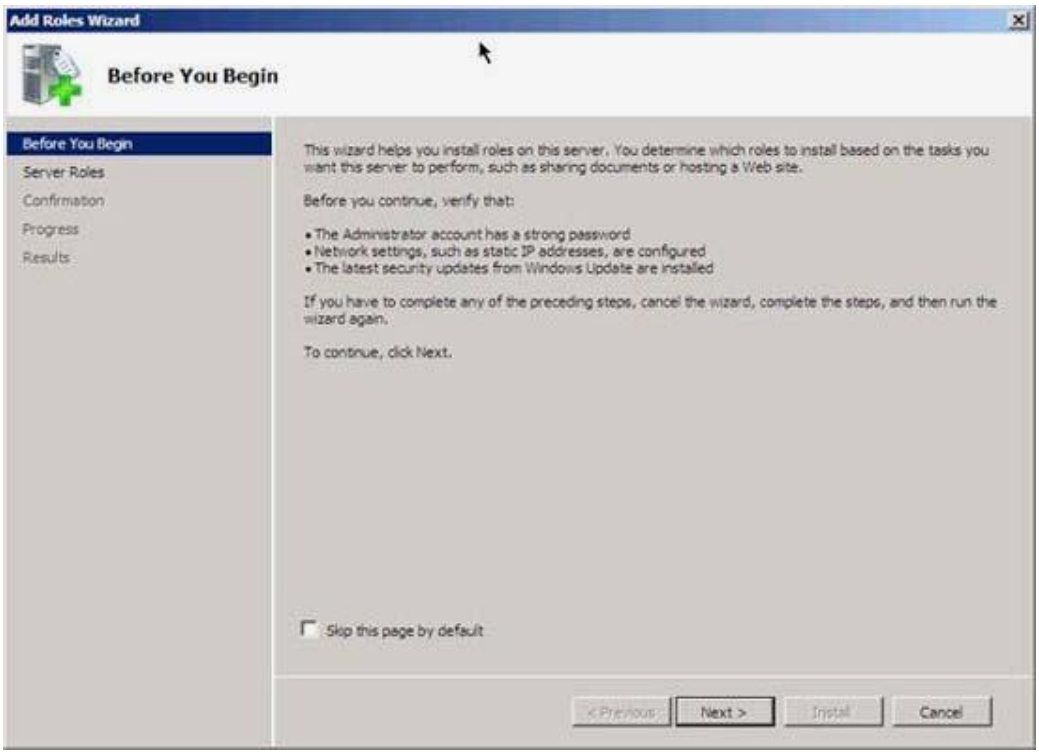
Đến đây quá trình cài đặt kết thúc.

I. TẠO DỰNG DOMAIN CONTROLLER

Giống như Windows Server 2003 sẽ vẫn cần chạy **dcpromo** từ nhắc lệnh **Run,** tuy nhiên cần phải cài đặt **Active Directory Domain Controller** role, đầu tiên bạn cài đặt role, sau đó chạy **dcpromo**.Vào **Server Manager ➔ Roles ➔ Add Roles**



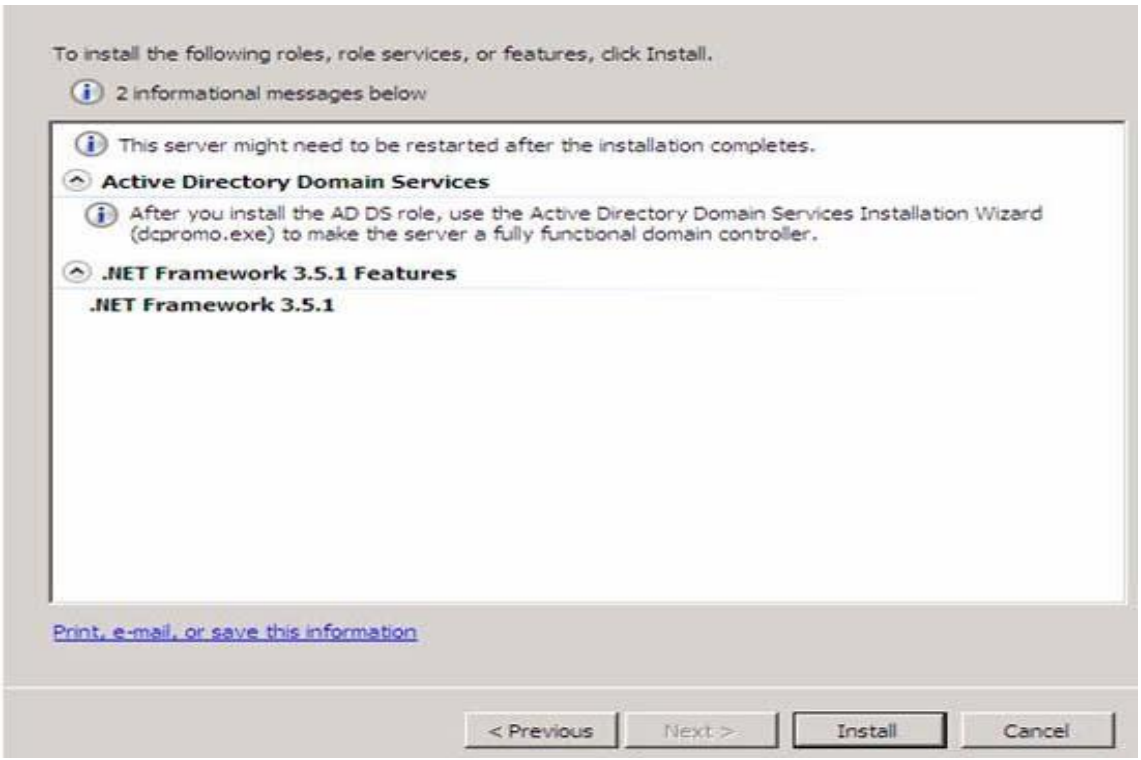
Xuất hiện trang **Before You Begin**, nhấn **Next** để tiếp tục.



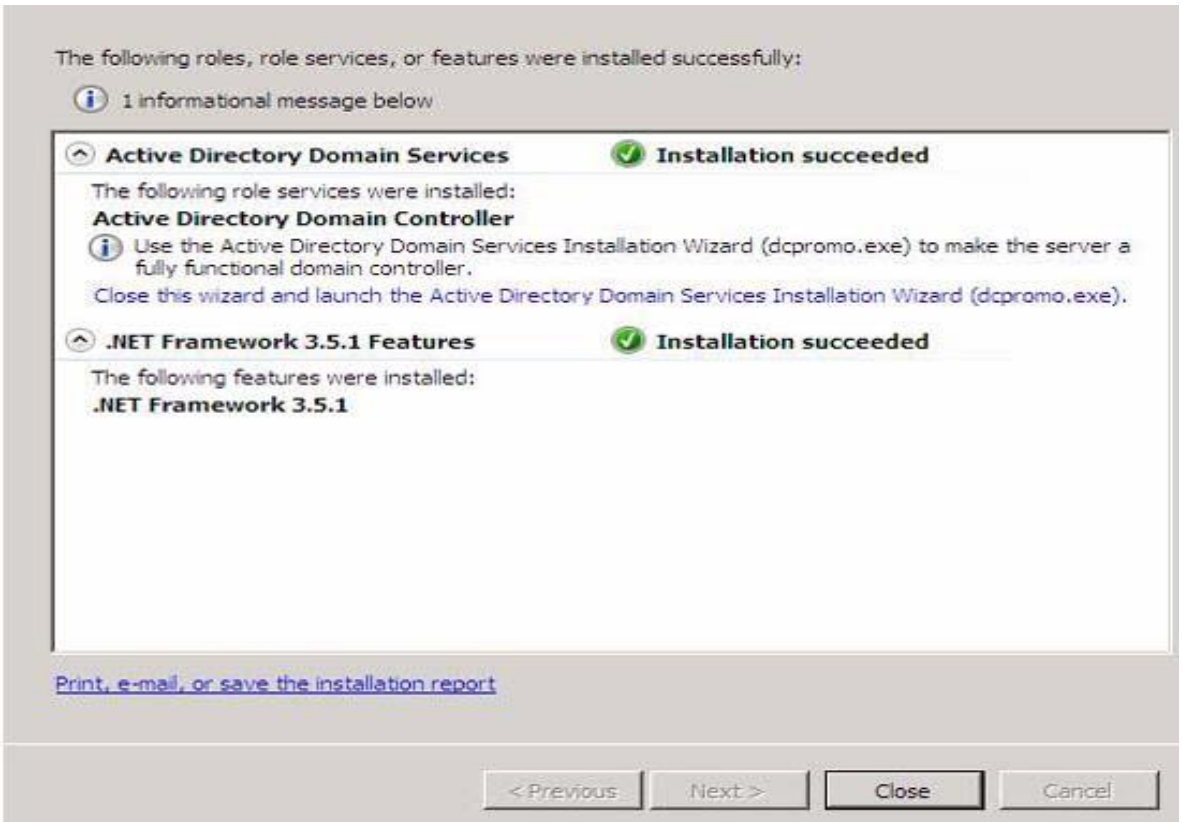
Chọn **Active Directory Domain Services ➔Add Required Features** để cài đặt thêm các tính năng này với Active Directory Server Role.

Sau khi chọn Active Directory DC Server Role, bạn sẽ thấy các thông tin về Server Role.

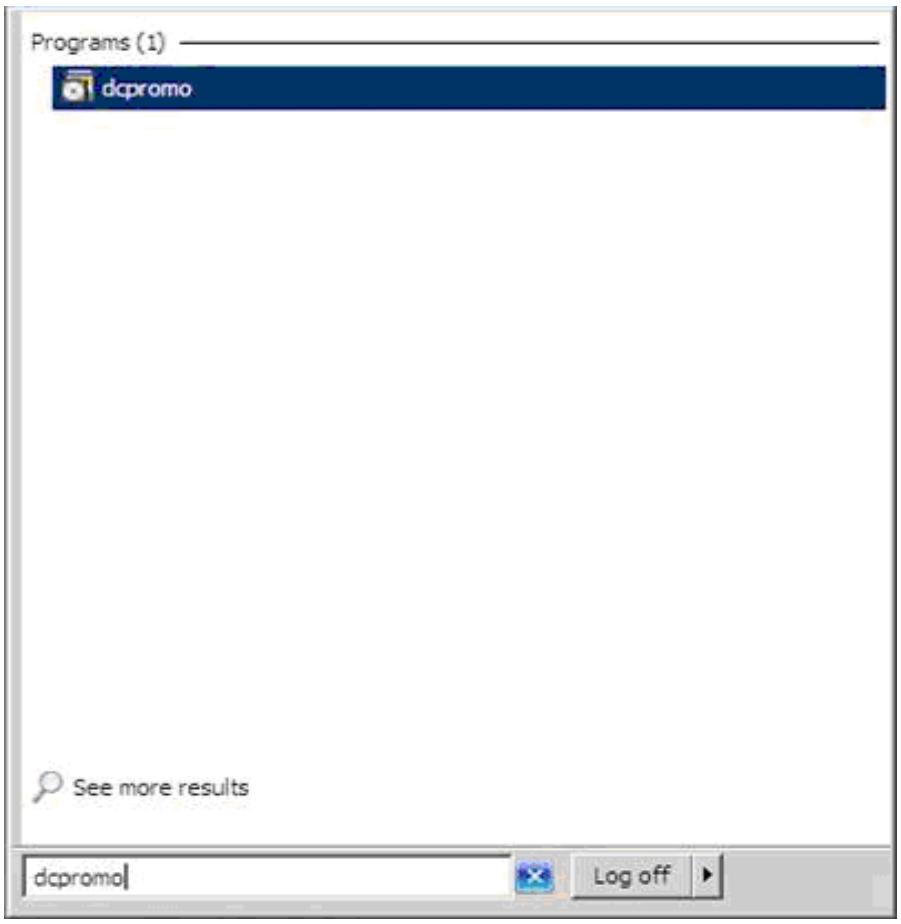
Kích **Install** để cài đặt các file yêu cầu nhằm chạy **dcpromo**



Cài đặt được thực hiện thành công. Kích **Close**.



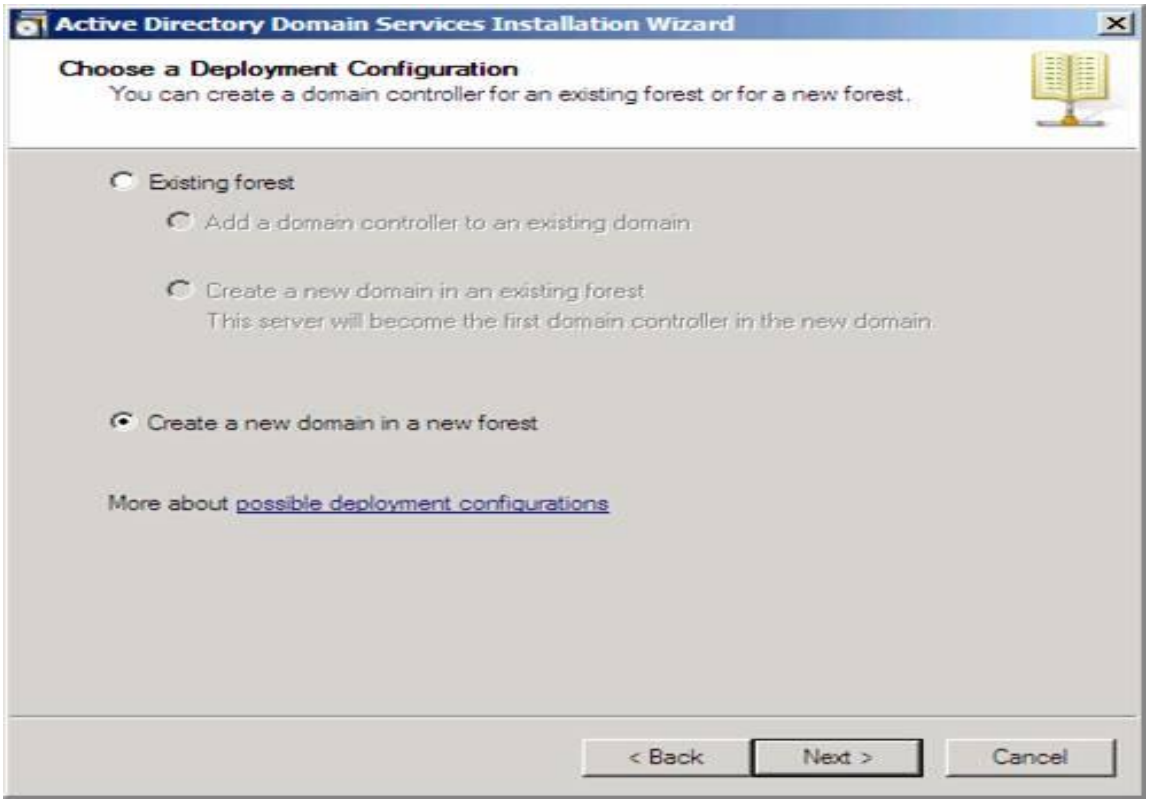
Lúc này vào menu **Start**, đánh **dcpromo** vào hộp tìm kiếm. Kích **dcpromo**.



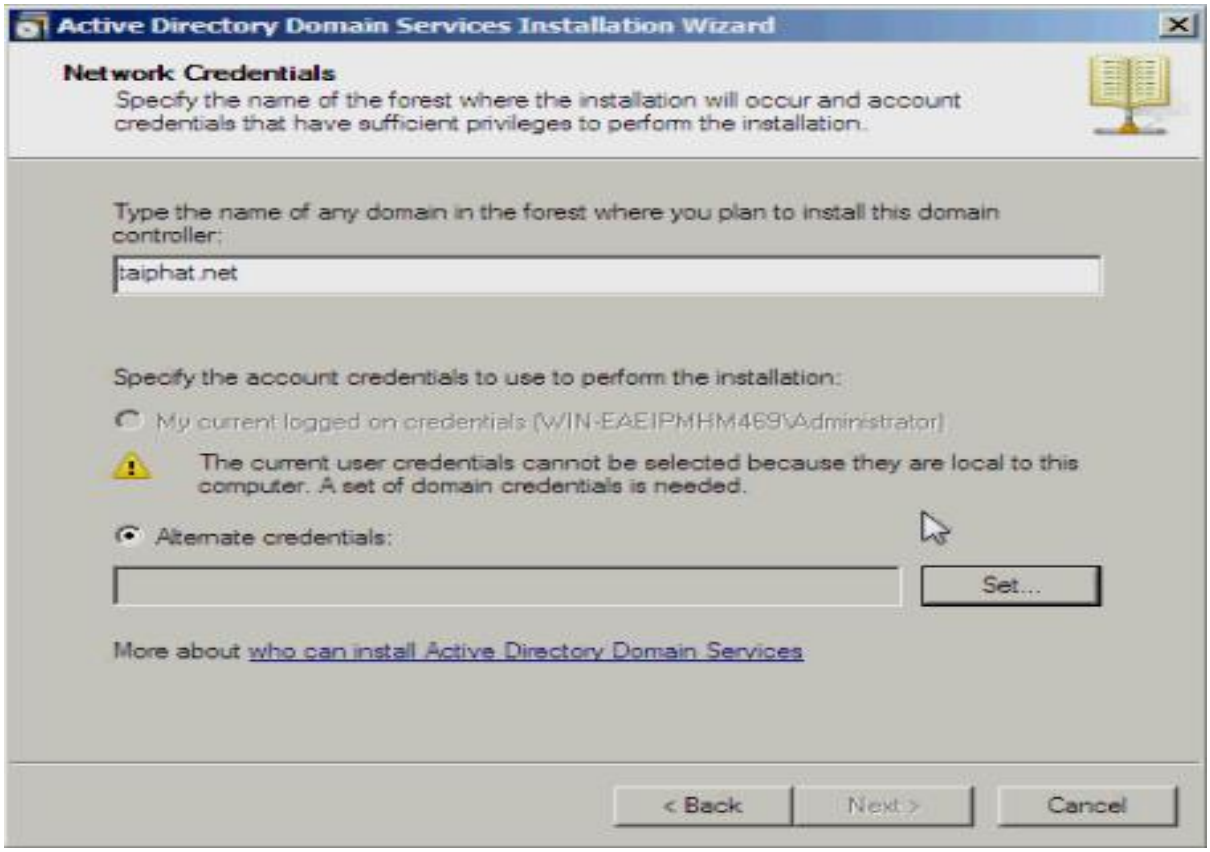
Thao tác này sẽ khởi chạy **Welcome to the Active Directory Domain Service Installation Wizard**. Kích **Next**.

Sau đó tiếp tục nhấn **Next.**

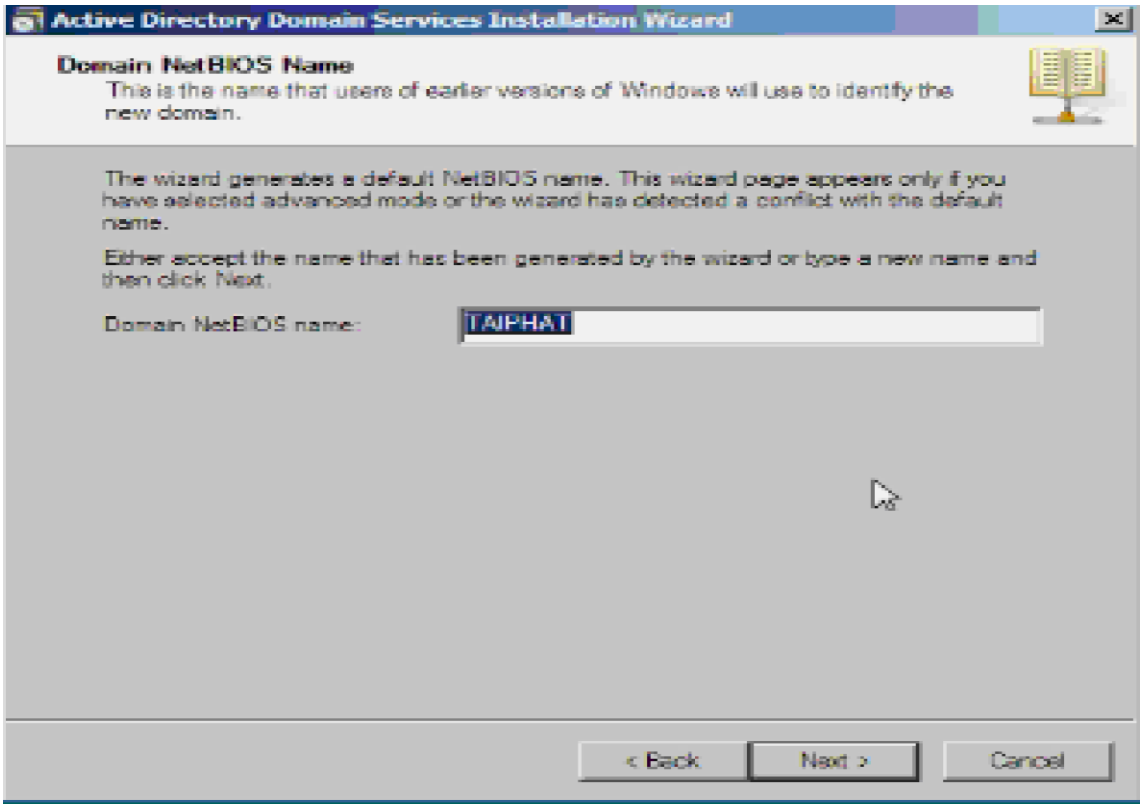
Trong trang **Choose a Deployment Configuration ➔Create a new domain in a new forest.**.



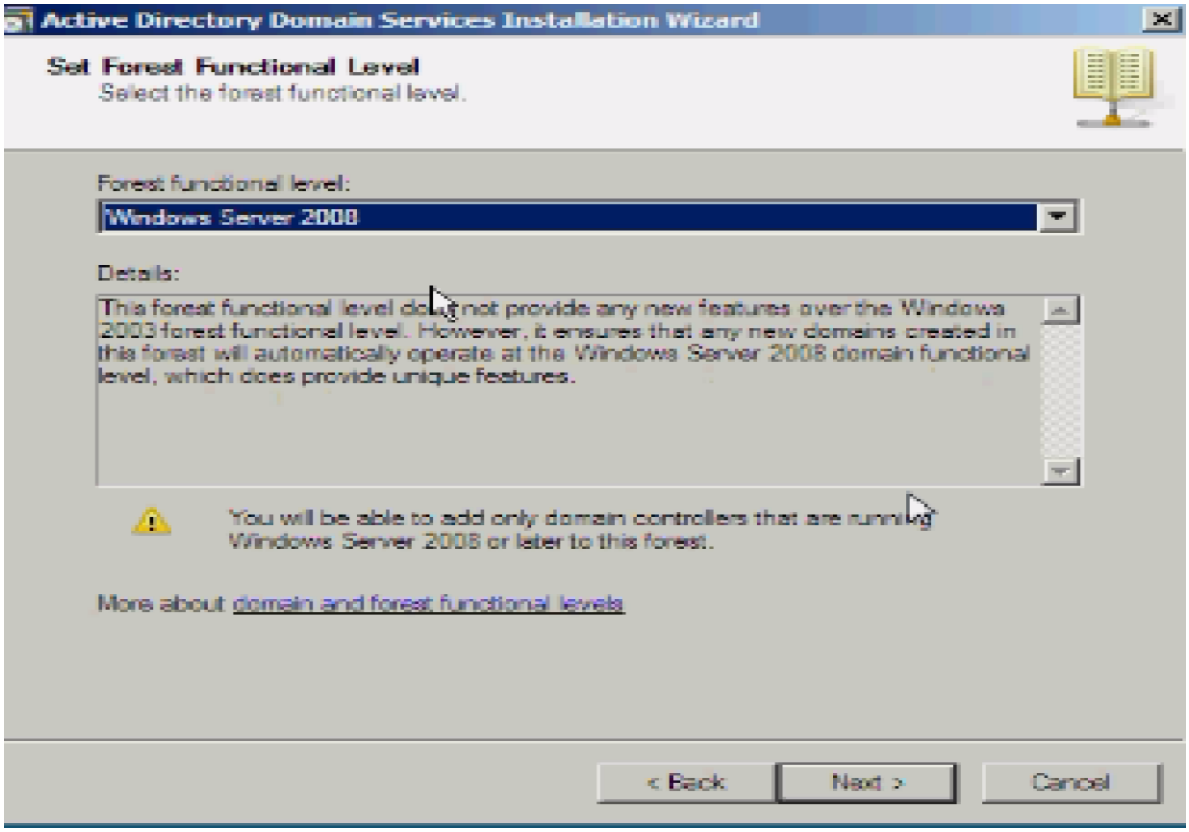
Trong trang **Name the Forest Root Domain**, nhập vào tên của miền trong hộp nhập liệu **FQDN of the forest room domain.**Nhấn **Next** để tiếp tục.



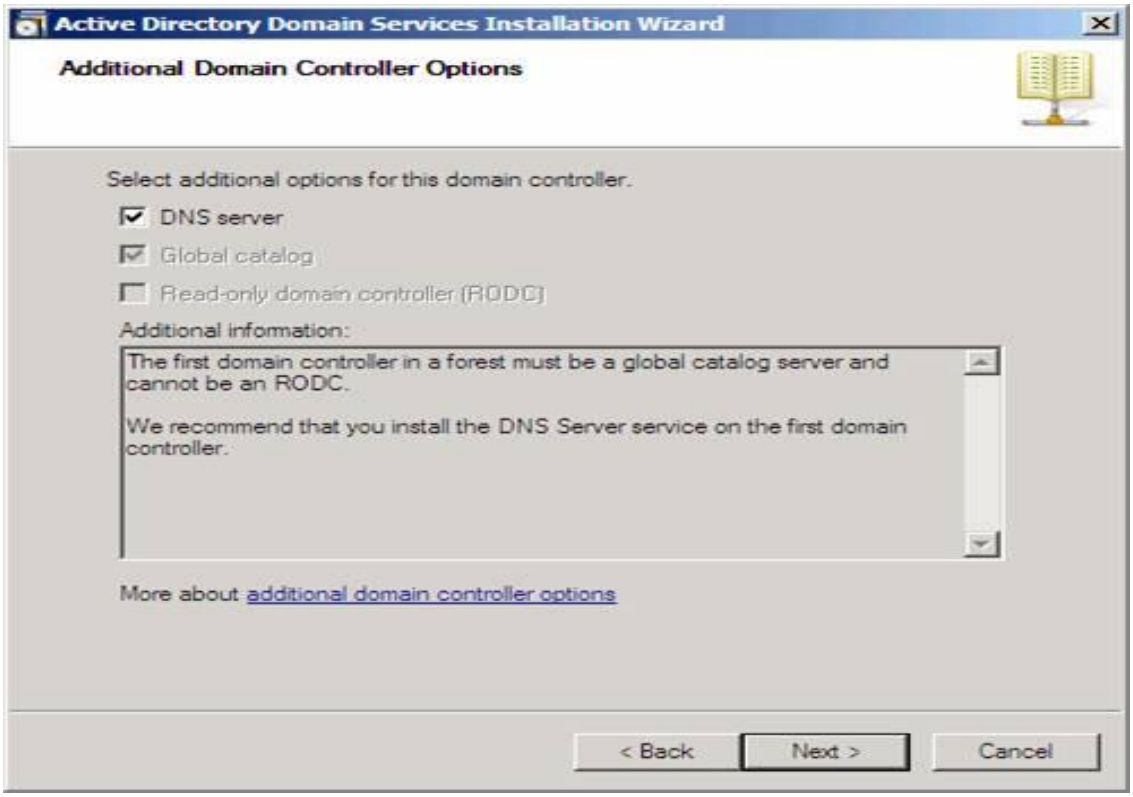
Nhấn **Next** để tiếp tục.



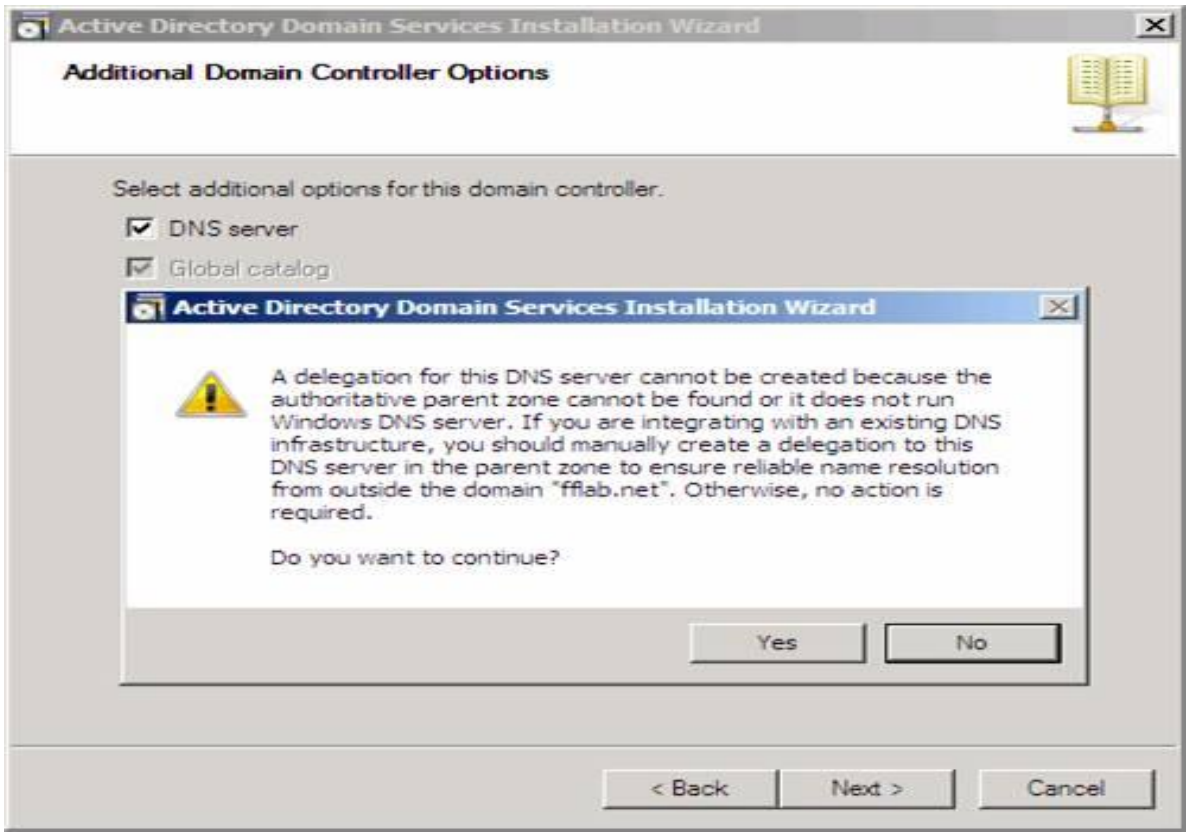
Trong trang **Set Forest Functional Level**, chọn Windows Server 2008. Nhấn **Next** để tiếp tục.



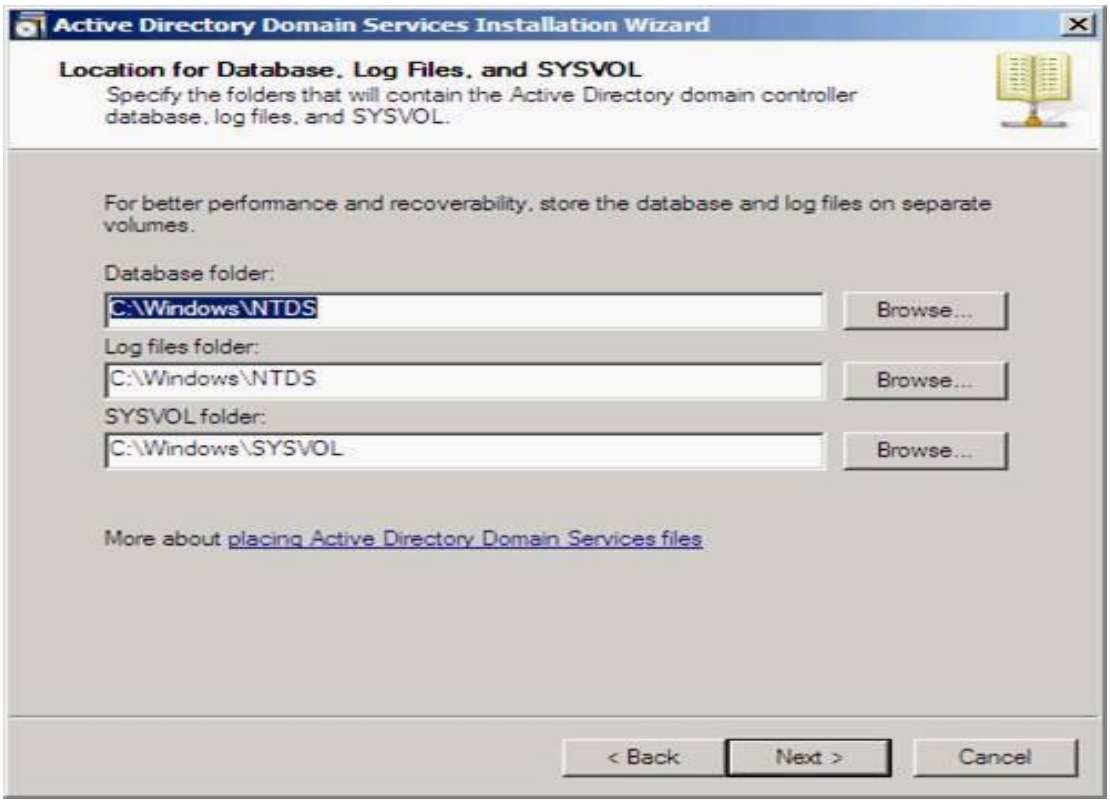
Trong trang **Additional Domain Controller Options**, Chọn **DNS server** và kích **Next**.



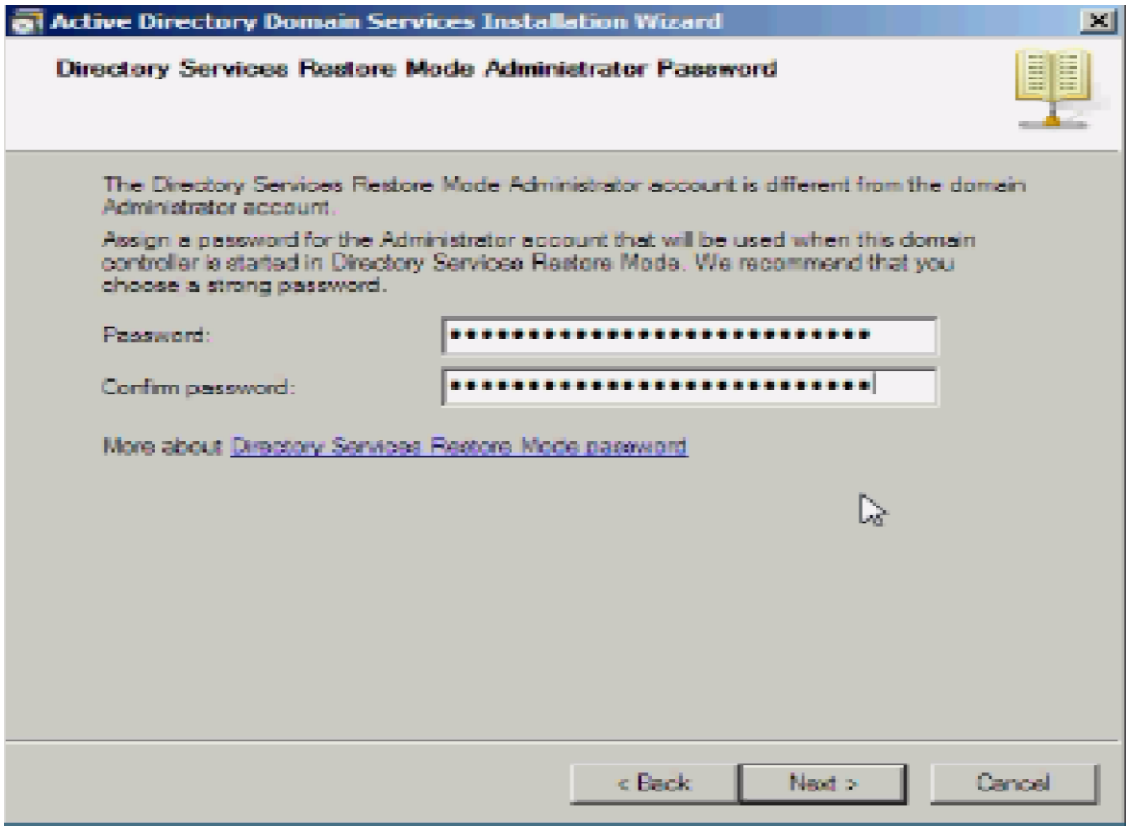
Một hộp thoại sẽ xuất hiện nói răng không thể tạo đại biểu cho máy chủ DNS này vì không thể tìm thấy vùng xác thực hoặc nó không chạy Windows DNS server. Lý do cho điều này là vì đây là DC đầu tiên trên mạng. Nhấn **Next** để tiếp tục.



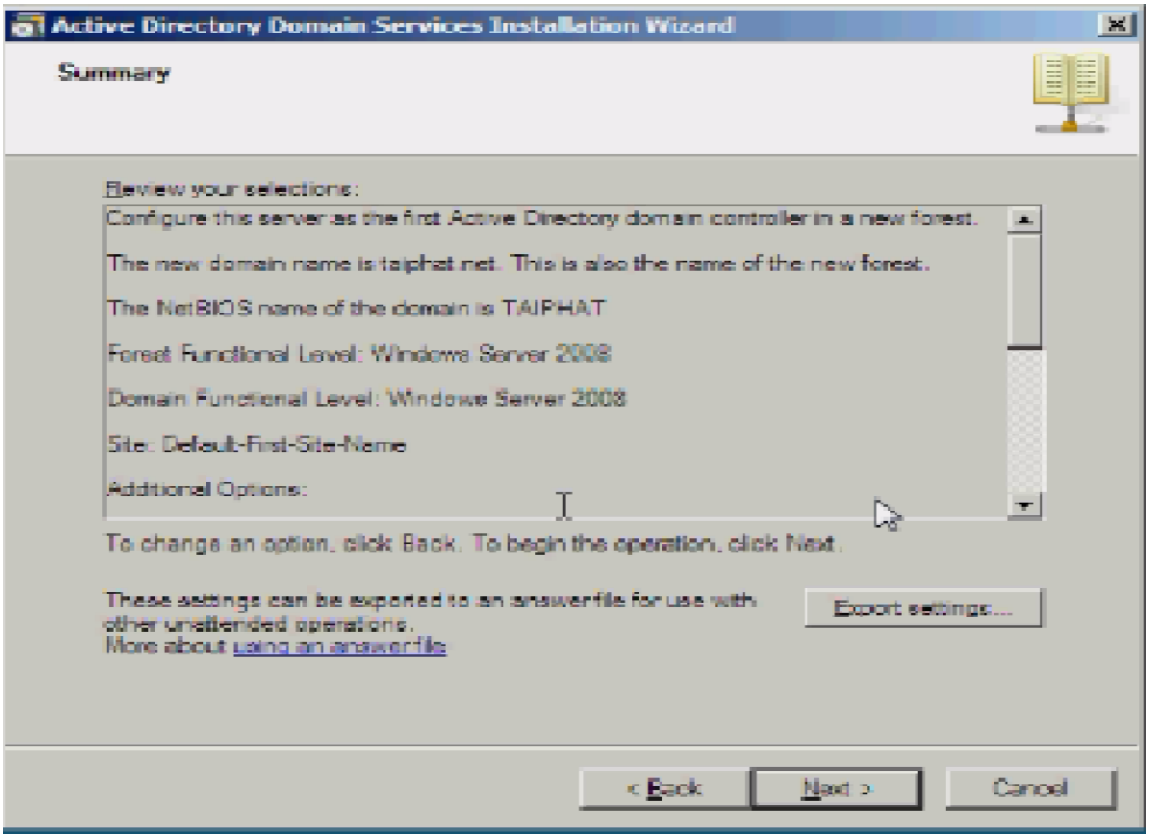
Để lại thư mục Database, Log Files và SYSVOL ,kích **Next.**



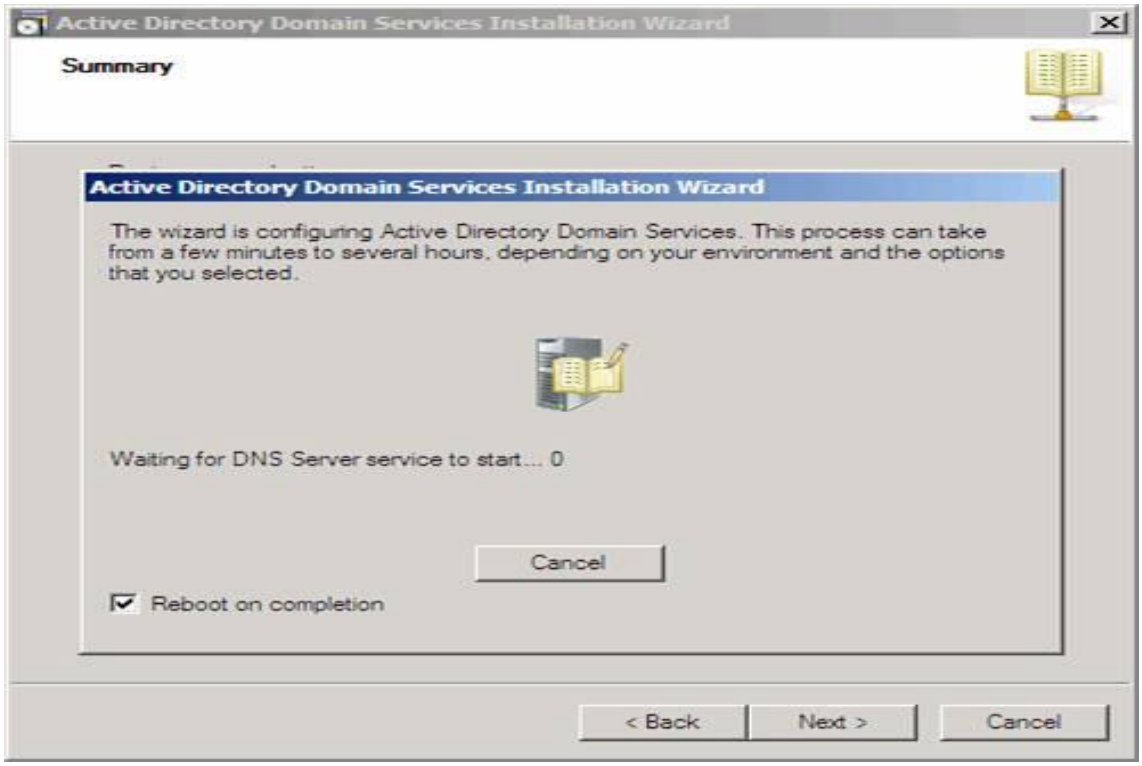
Trong **Directory Service Restore Mode Administrator Password**, nhập một mật khẩu mạnh vào các hộp nhập liệu **Password** và **Confirm password.**



Xác nhận các thông tin trên trang **Summary** và kích **Next**.



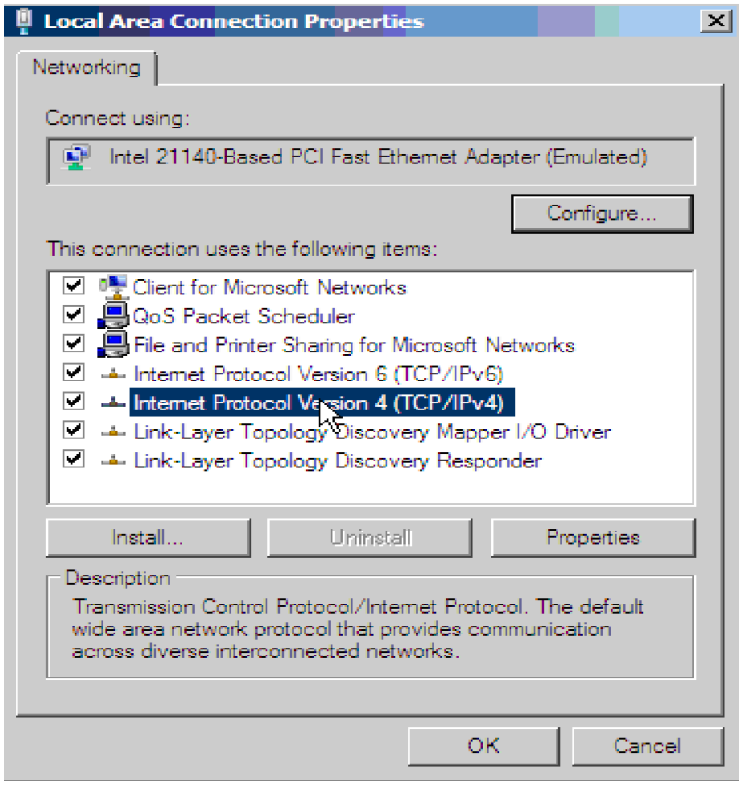
Active Directory sẽ cài đặt. Đặt một dấu kiểm vào hộp chọn **Reboot on completion** để máy tính sẽ tự động khởi động lại khi cài đặt DC được hoàn tất.



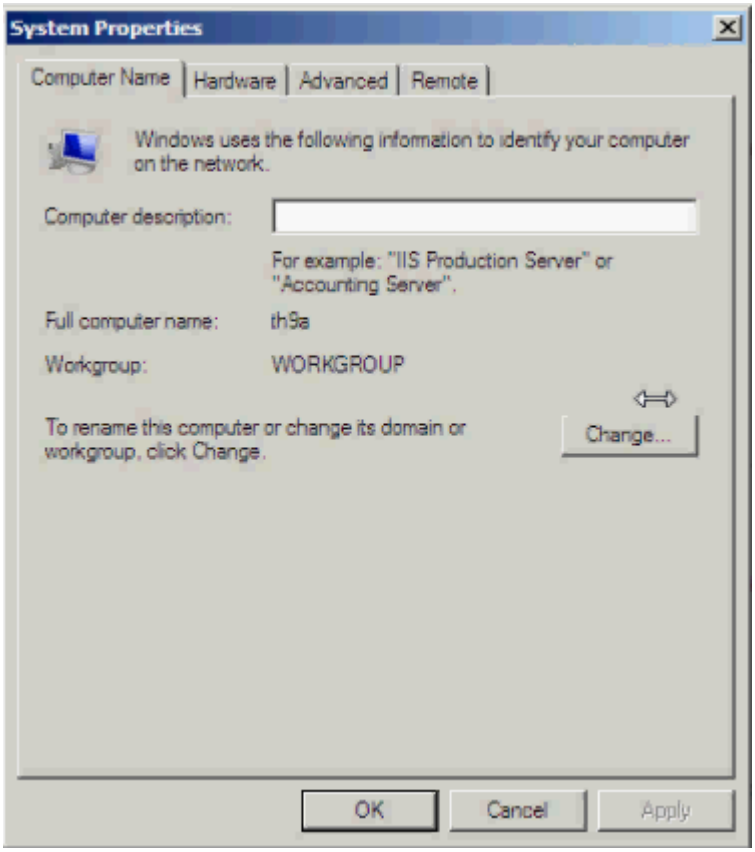
. Cài đặt sẽ hoàn tất khi đăng nhập.

II. ĐĂNG NHẬP MÁY CLIENT VÀO DOMAIN

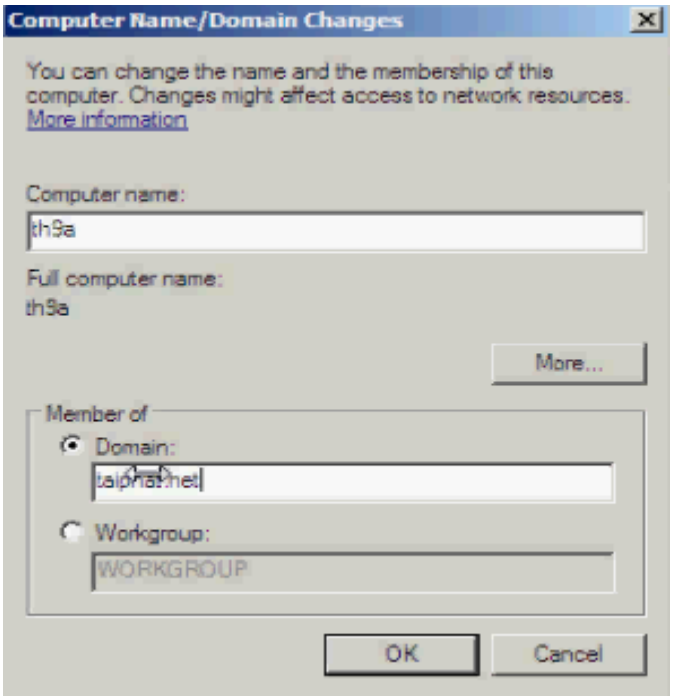
Đặt địa chỉ IP.Click phải vào **My Network places** ➔**Properties**.Chọn **Manager network connections**➔Click phải vào biểu tượng card mạng chọn **Properties**.Chọn **Internet Protocol Version 4 (TCP/IPv4)** ➔**Properties**



Click phải My Computer ➔Properties ➔Change Settings.
Nhấn nút Change.

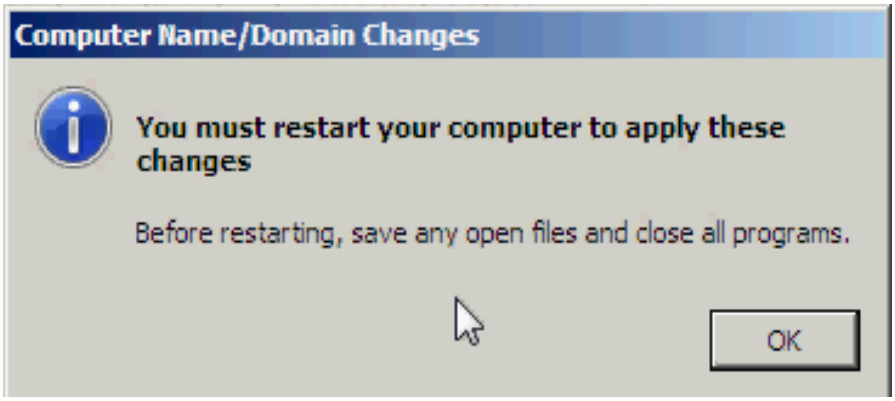


Chọn Domain ➔Nhập tên domain



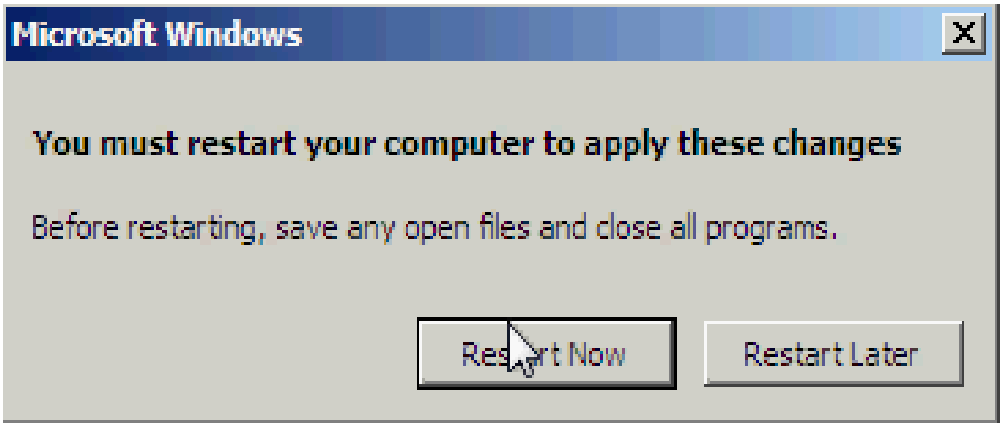
Công việc thành công.

Nhấn **OK** để chấp nhận Restart máy.



Nhấn **Close.**

Nhấn **Restart Now.**



Sau khi restart, log on vào domain Administrator➔ máy tính đã trở thành 1 client của domain taiphat.net.

CHƯƠNG 3 : XÂY DỰNG CÁC DỊCH VỤ

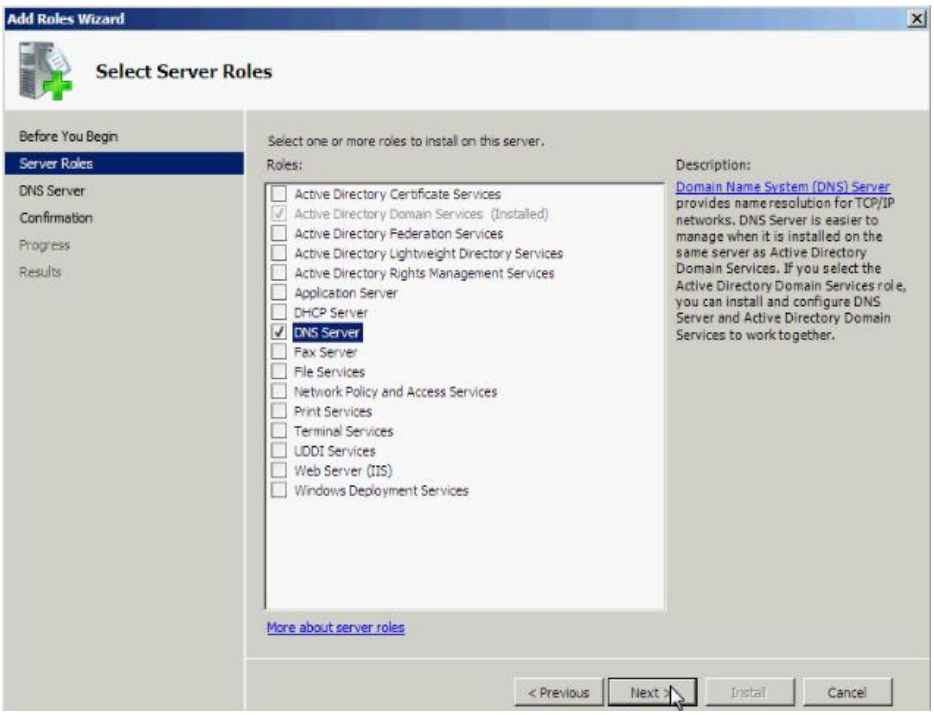
I. DỊCH VỤ DNS

1. Giới thiệu về DNS

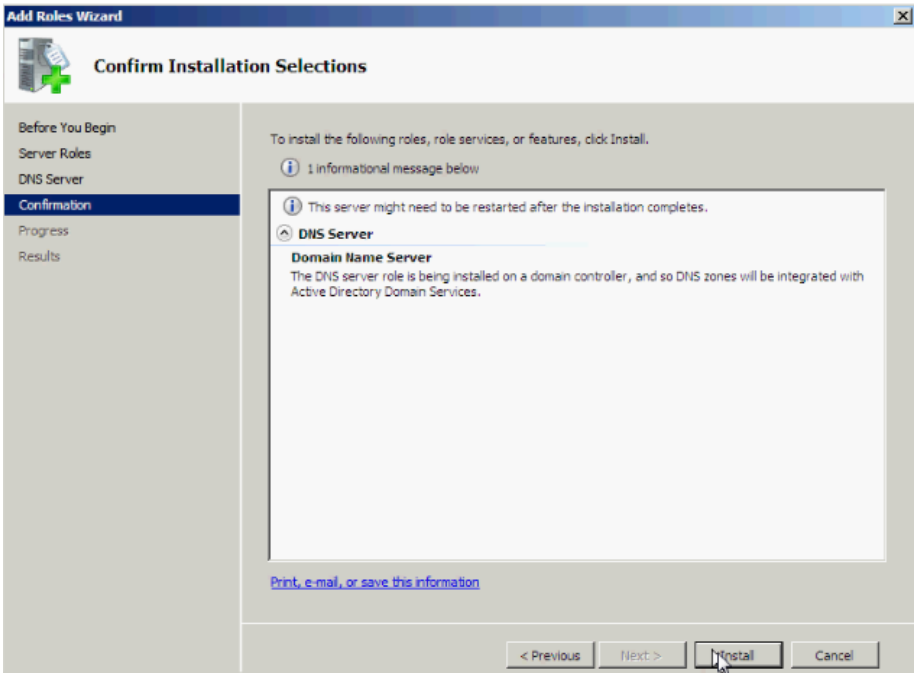
DNS (Domain Name System) Server là máy chủ được dùng để phân giải domain thành địa chỉ IP và ngược lại. Về cách thức hoạt động, DNS Server lưu trữ một cơ sở dữ liệu bao gồm các bản ghi DNS và dịch vụ lắng nghe các yêu cầu.Khi máy client gửi yêu cầu phân giải đến, DNS Server tiến hành tra cứu trong cơ sở dữ liệu và gửi kết quả tương ứng về máy client.

2. Cài đặt DNS

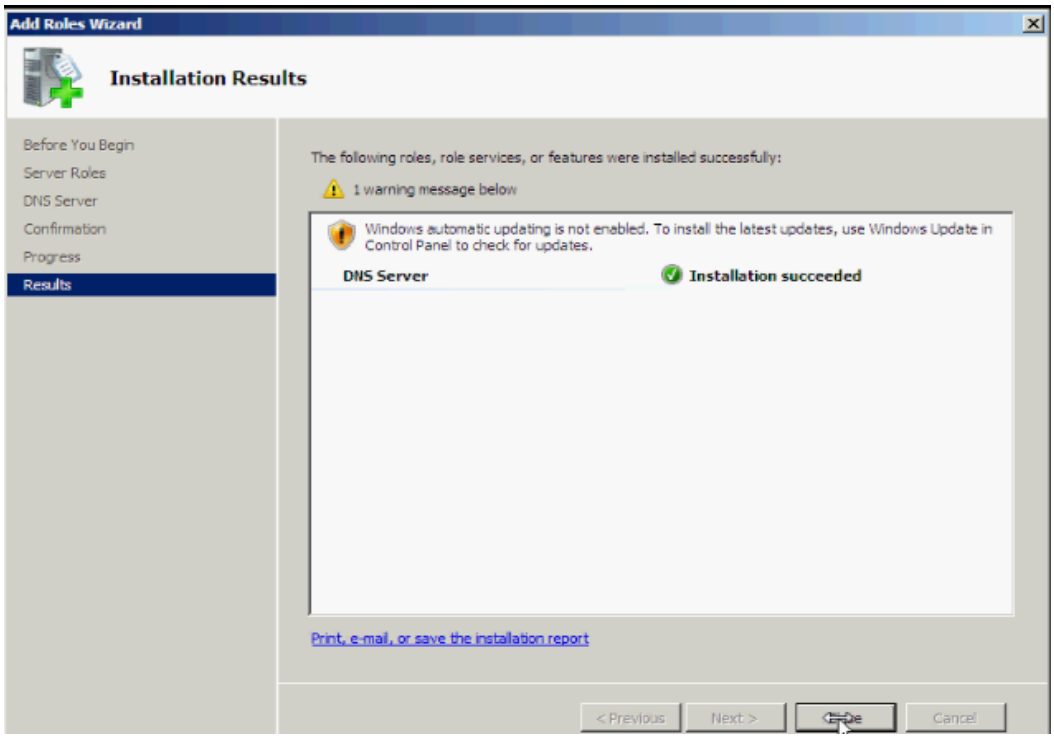
Vào Server Manager ➔ Roles ➔Add Roles.Tại bảng Select Server Roles, chọn DNS Server



- Sau đó nhấn **Next** để tiếp tục
- Chọn **Instal**. Tại bảng **Confirm Installation Selections** xác nhận việc cài đặt.

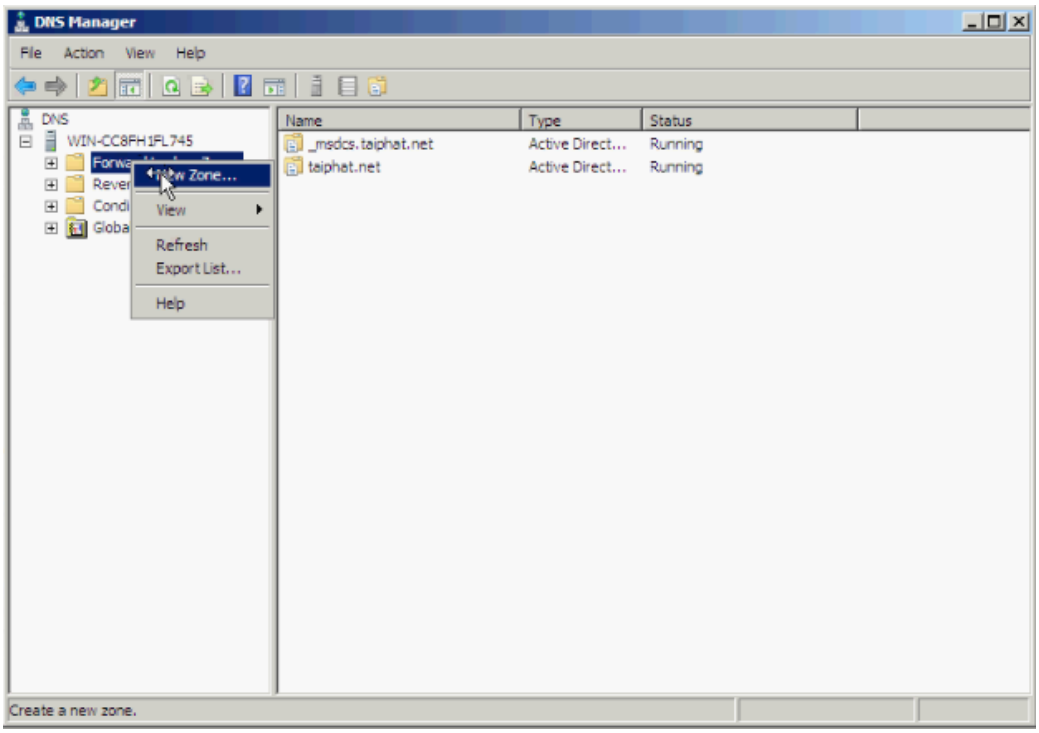


- Chọn **Close** để hoàn tất cài đặt.



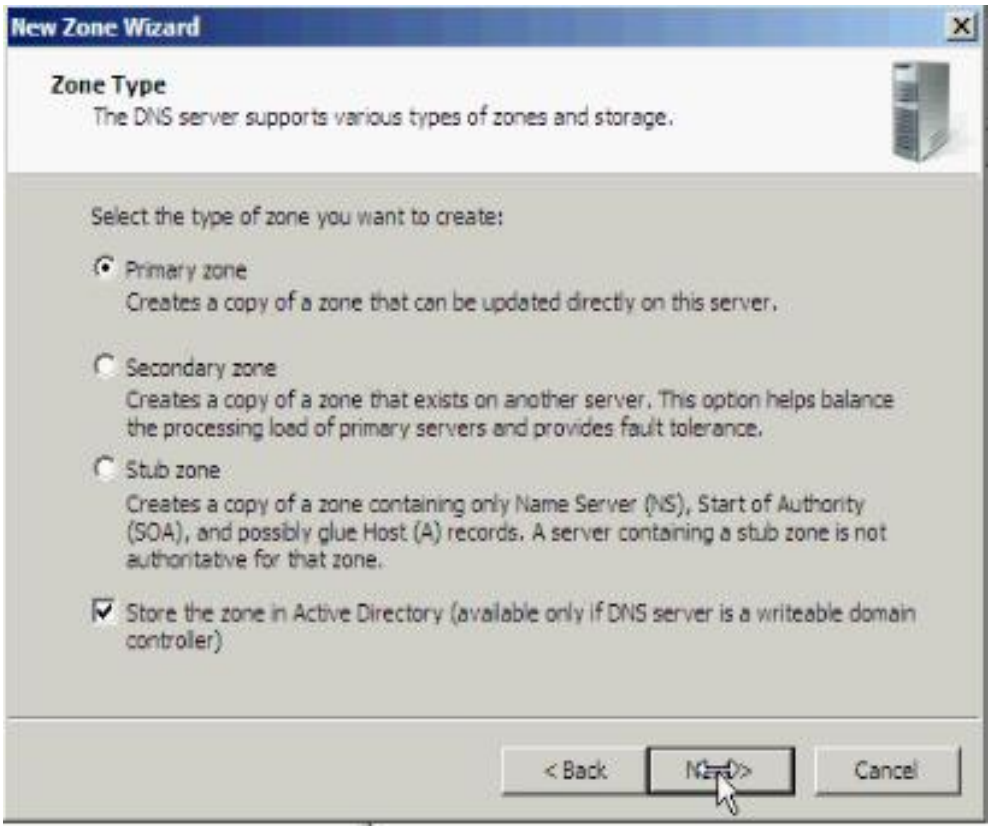
3. Cấu hình DNS

- Đối với DNS Server,thông thường nên xây dựng đồng thời hai hệ thống là DNS Server chính (Primary) và DNS Server dự phòng (Secondary) dùng chung một cơ sở dữ liệu. Với phương pháp này,sẽ hạn chế khả năng dịch vụ DNS bị ngưng khi có sự cố xảy ra trên hệ thống.
- Vào **Start ➔Administrative Tools ➔DNS.**
- Nhấp chuột phải vào **Forward Lookup Zones** và chọn **New Zone.**

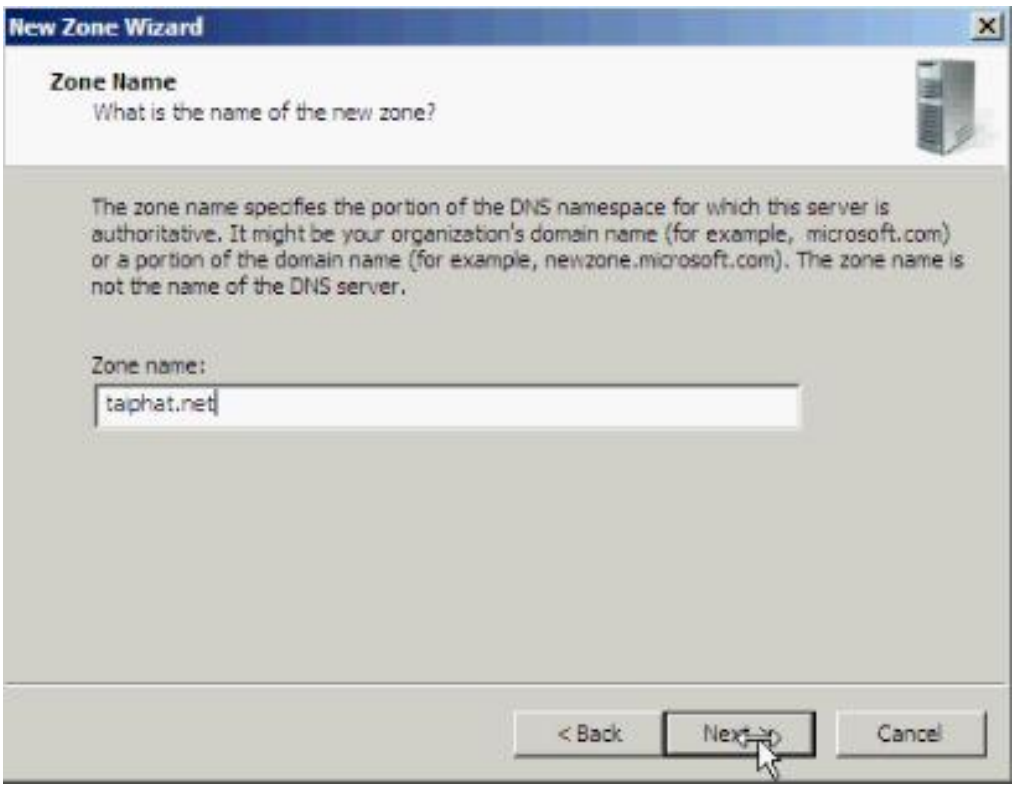


- Tại bảng **Welcome to the New Zone Wizard** ,chọn **Next.**

- Tại bảng **Zone Type chọn Primary zone** để cấu hình DNS Server chính.

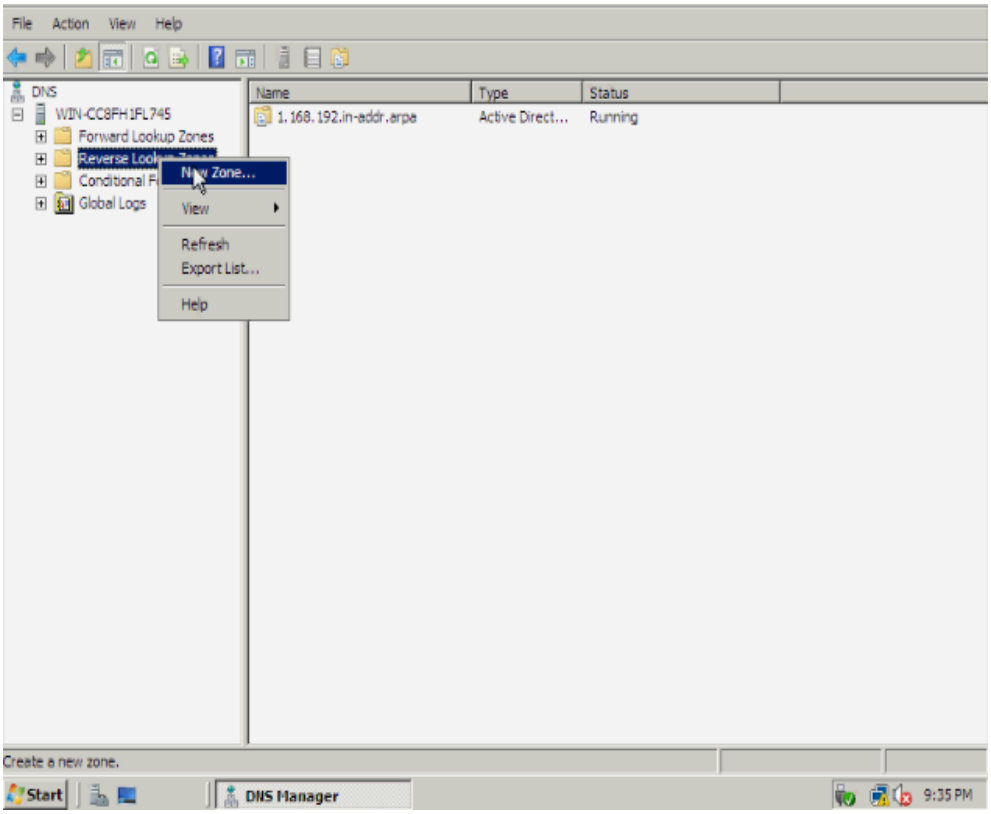


- Chọn Next. Tại bảng **Zone Name** gõ tên domain vào.

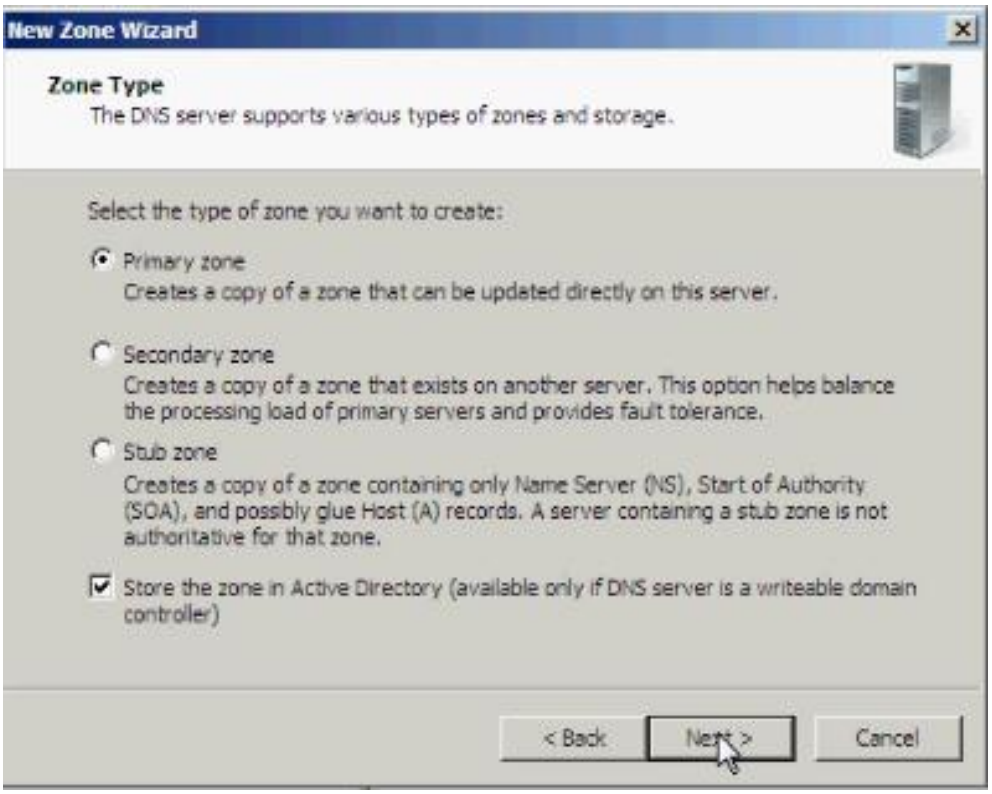


- Chọn **Next**. Tại bảng **Zone File**, để mặc định. Chọn **Next**.

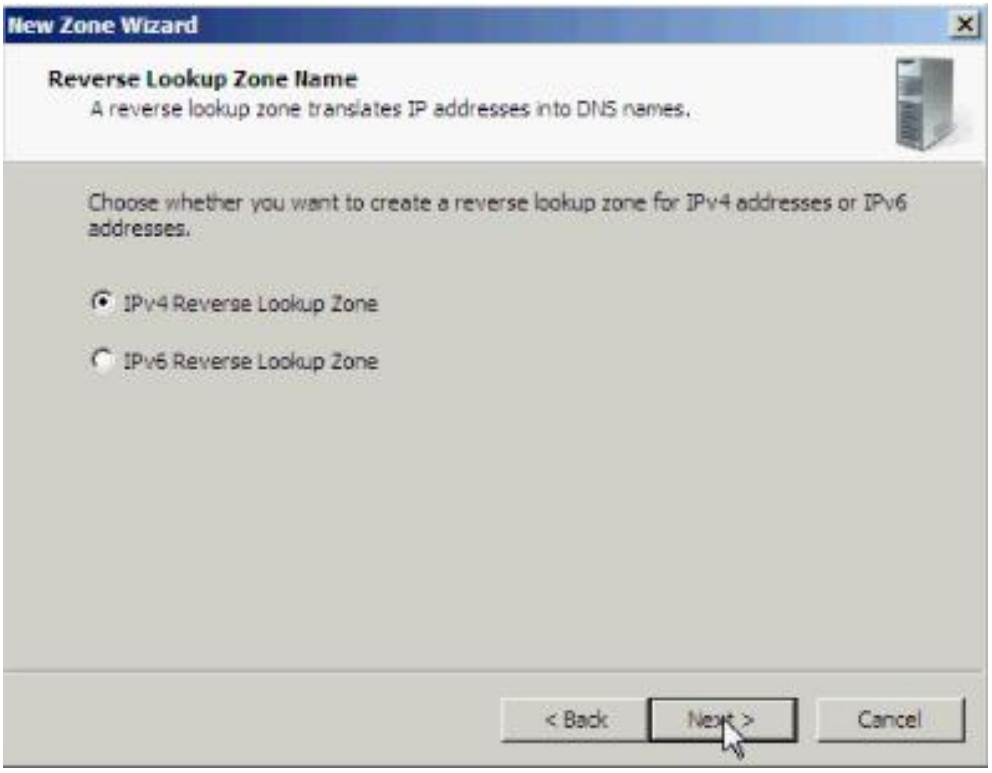
- Chọn **Next.** Tại bảng **Completing the New Zone Wizard** xem lại thông tin.
- Sau đó chọn **Finish** để hoàn tất.
- Nhấp chuột phải vào Reverse **Lookup Zones và chọn New Zone.**



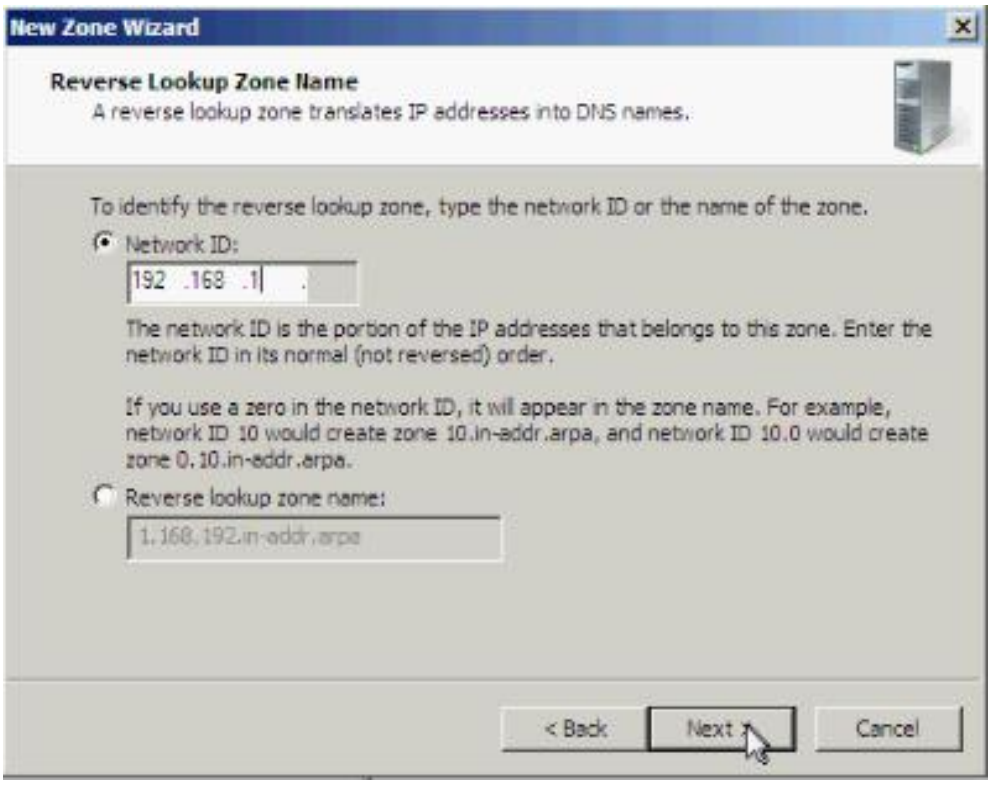
- Tại bảng **Welcome to the New Zone Wizard** chọn **Next**.
- Tại bảng Zone Type chọn Primary zone để cấu hình chức năng reverse cho DNS Server chính.



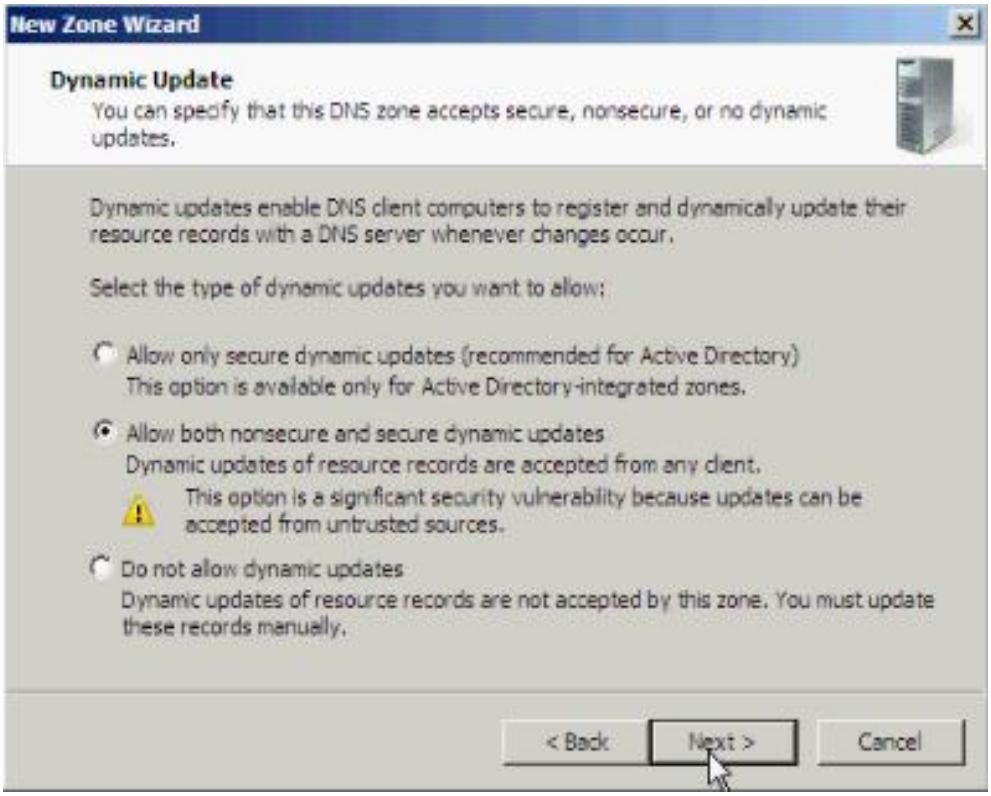
- Chọn Next.Tại bảng Reverse Lookup Zone Name chọn kiểu IP cần phân giải. Ở đây chọn IPv4.



- Chọn Next. Điền Network ID và chọn Next.

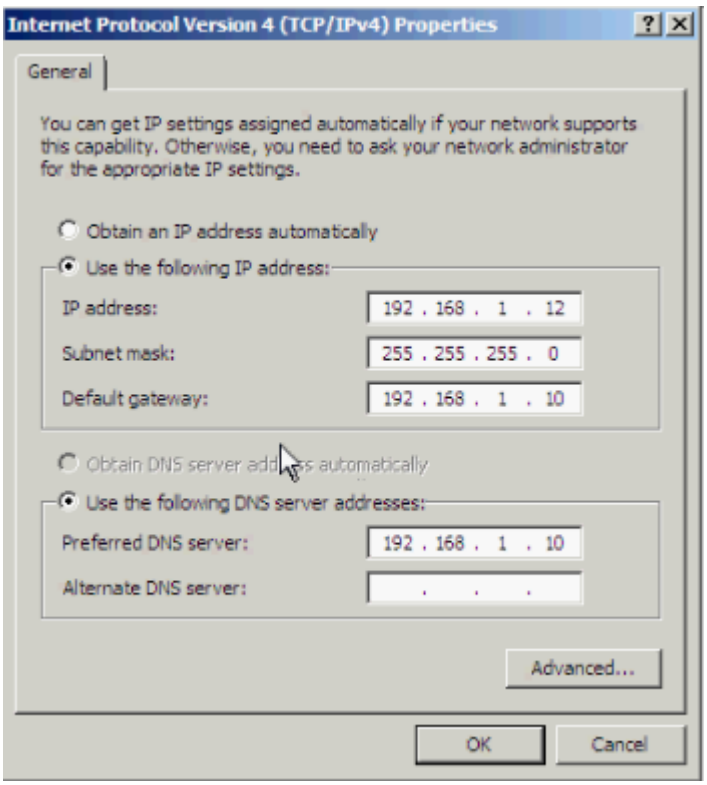


- Tại bảng Zone File để mặc định. Chọn Next.
- Tại bảng Dynamic Update chọn Allow both nonsecure dynamic updates.



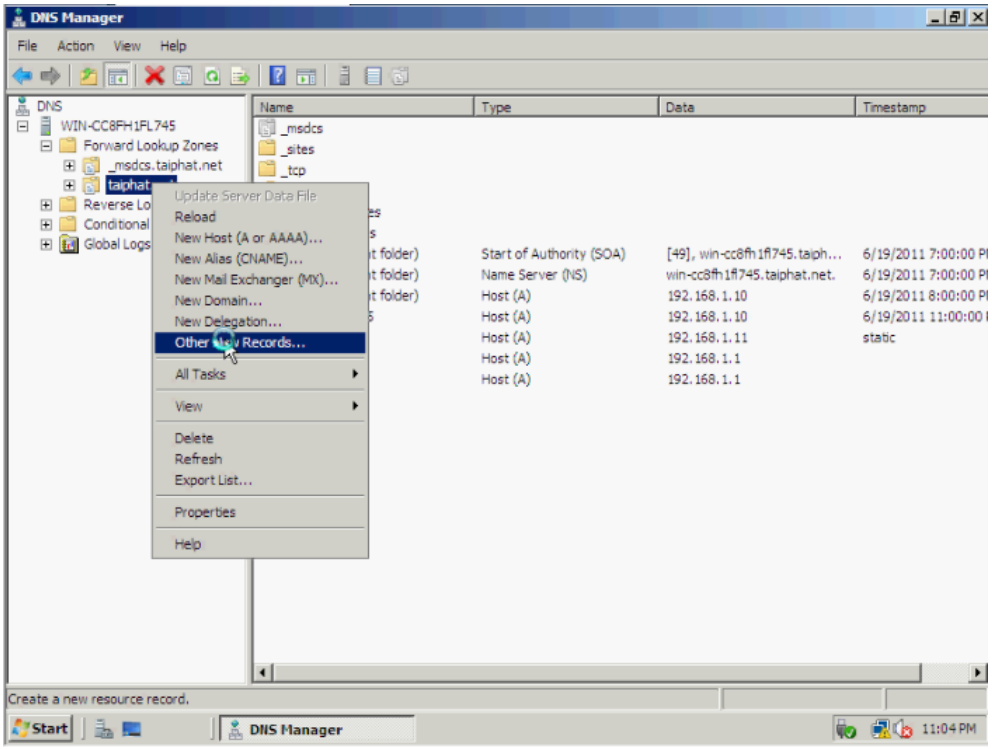
- Chọn Next và xem lại thông tin thiết lập, và sau đó chọn Finish để kết thúc.

4. Cấu hình địa chỉ DNS Server trên máy Client



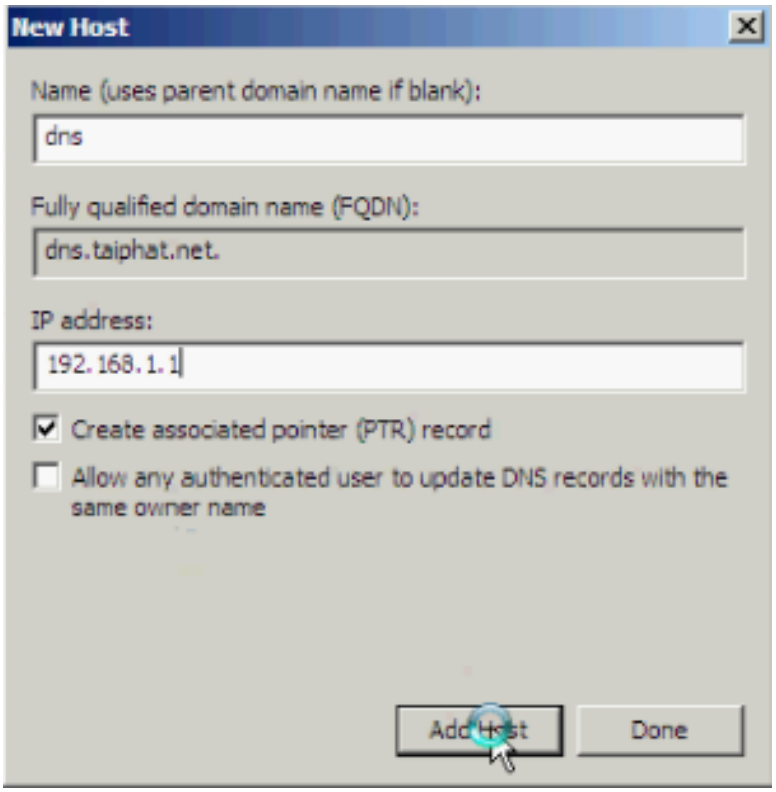
5. Bổ sung các bản ghi DNS vào DNS Server

- Nếu muốn tạo các record khác.Nhấp chuột phải vào zone và chọn Other New Records.



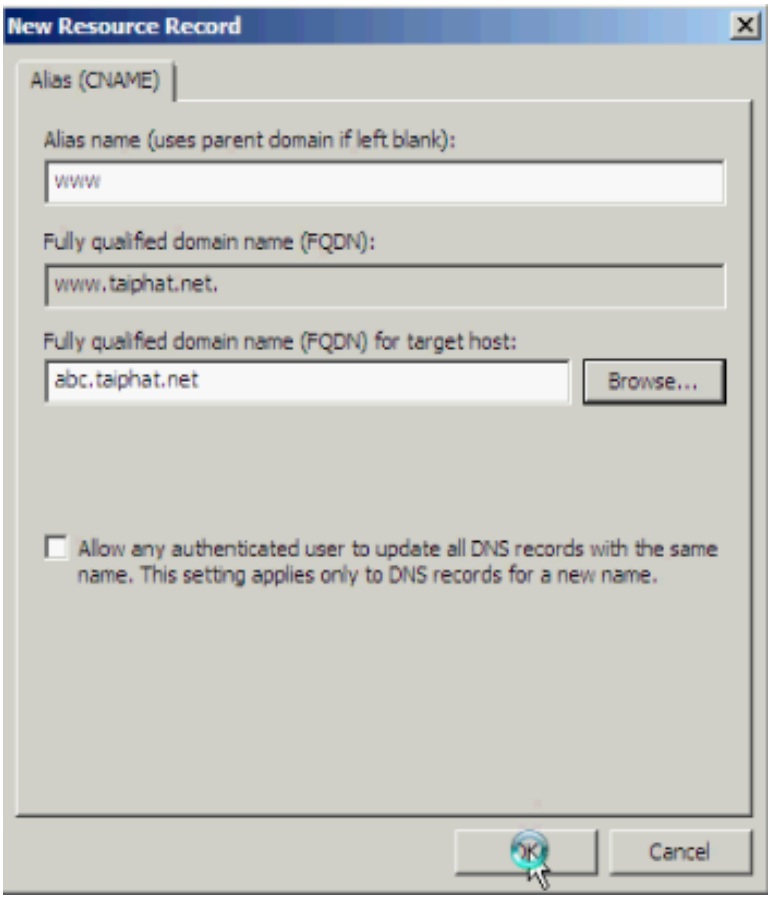
- Vào Start ➔Administrative Tools ➔DNS. Nhấp chuột phải vào zone và chọn New

- Gõ tên host vào mục Name, gõ địa chỉ IP vào mục IP address. Nếu muốn tạo ra một bản ghi DNS phân giải ngược tương ứng thì đánh dấu chọn Create associated pointer (PTR) record.

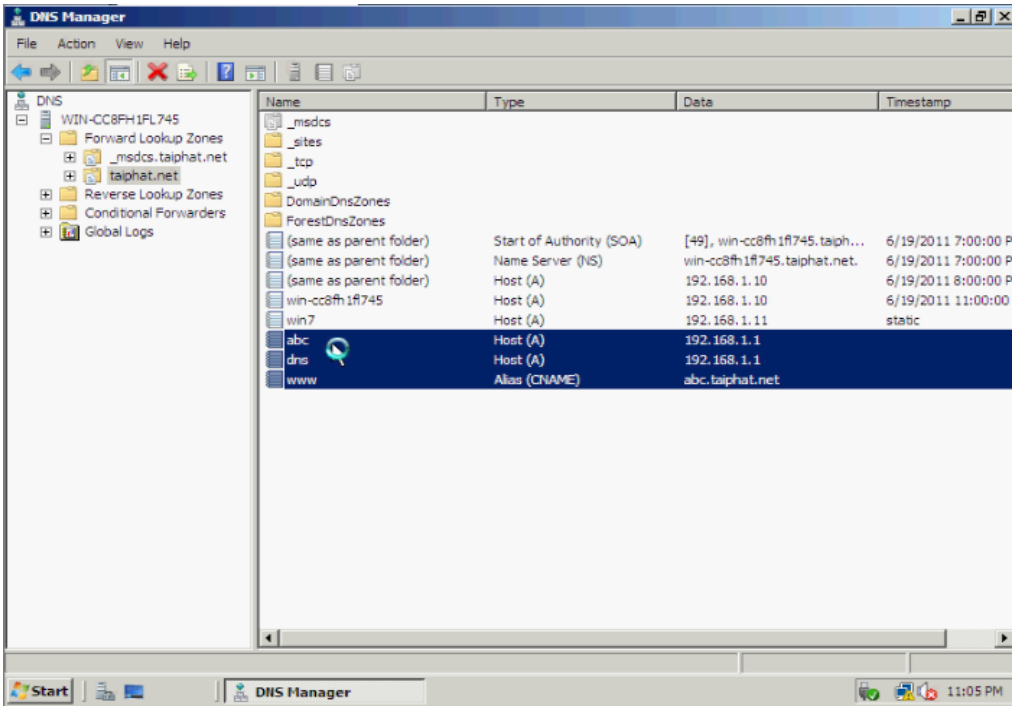


- Sau đó chọn Add Host.Xuất hiện thông báo thành công.

Chọn OK. Bảng New Host tiếp tục xuất hiện, chọn Done để kết thúc tạo bản ghi. Để tạo một bản ghi Alias, nhấp chuột phải vào zone và chọn New Alias (CNAME). Tương tự như trên, điền các thông tin vào. Tại mục Fully qualified domain name (FQDN) for target host, nếu bạn không nhớ, chọn Browse để tìm tên máy cần thết.



- Sau khi đã điền thông tin đầy đủ. Chọn OK để hoàn tất.



II. DỊCH VỤ DHCP

1. Giới thiệu dich vụ DHCP

- Dịch vụ DHCP cho phép chúng ta cấp động các thông số cấu hình mạng cho các máy trạm.(client).

- Cơ chế sử dụng các thông số mạng được cấp phát động có ưu điểm hơn so với cơ chế khai báo tĩnh các thông số mạng như:

Khắc phục được tình trạng đụng địa chỉ IP và giảm chi phí quản trị cho hệ thống mạng.Giúp cho các nhà cung cấp dịch vụ (ISP) tiết kiệm được số lượng địa chỉ IP thật (Public IP).Phù hợp cho các máy tính thường xuyên di chuyển qua lại giữa các mạng.Kết hợp với hệ thống mạng không dây (Wireless) cung cấp các điểm Hotspot như: nhà ga, sân bay, trường học…

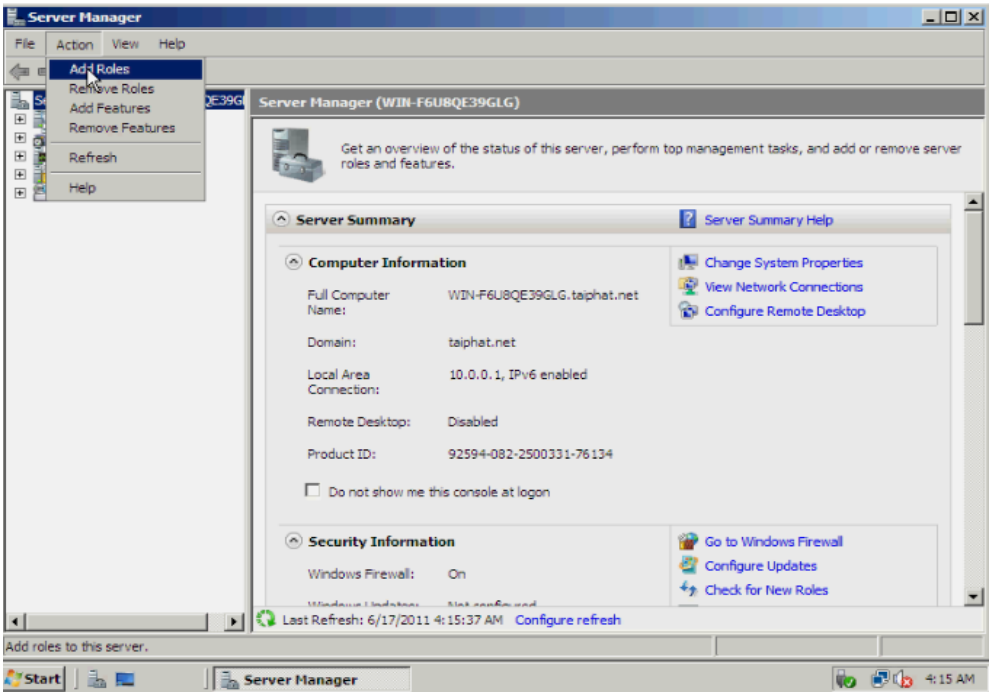
2. Hoạt động của giao thức

Giao thức DHCP làm việc theo mô hình client/server.Khi máy client khởi động, máy sẽ gửi broadcast gói tin DHCPDISCOVER, yêu cầu một server phục vụ mình. Gói tin này cũng chứa địa chỉ MAC của máy client.Các máy Server trên mạng khi nhận được gói tin yêu cầu đó, nếu còn khả năng cung cấp địa chỉ IP, đều gửi lại cho máy Client gói tin DHCPOFFER, đề nghị cho thuê một địa chỉ IP trong một khoản thời gian nhất định, kèm theo là một subnet mask và địa chỉ của Server.

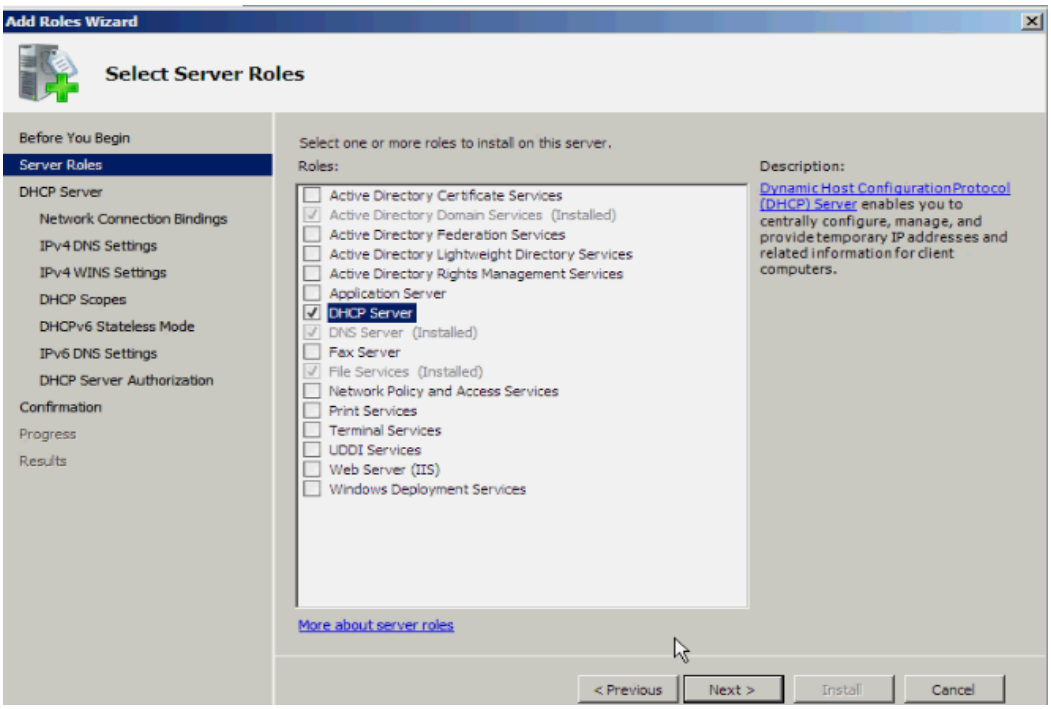
3. Cài đặt trên Windows Server 2008

3.1. Trên máy Server

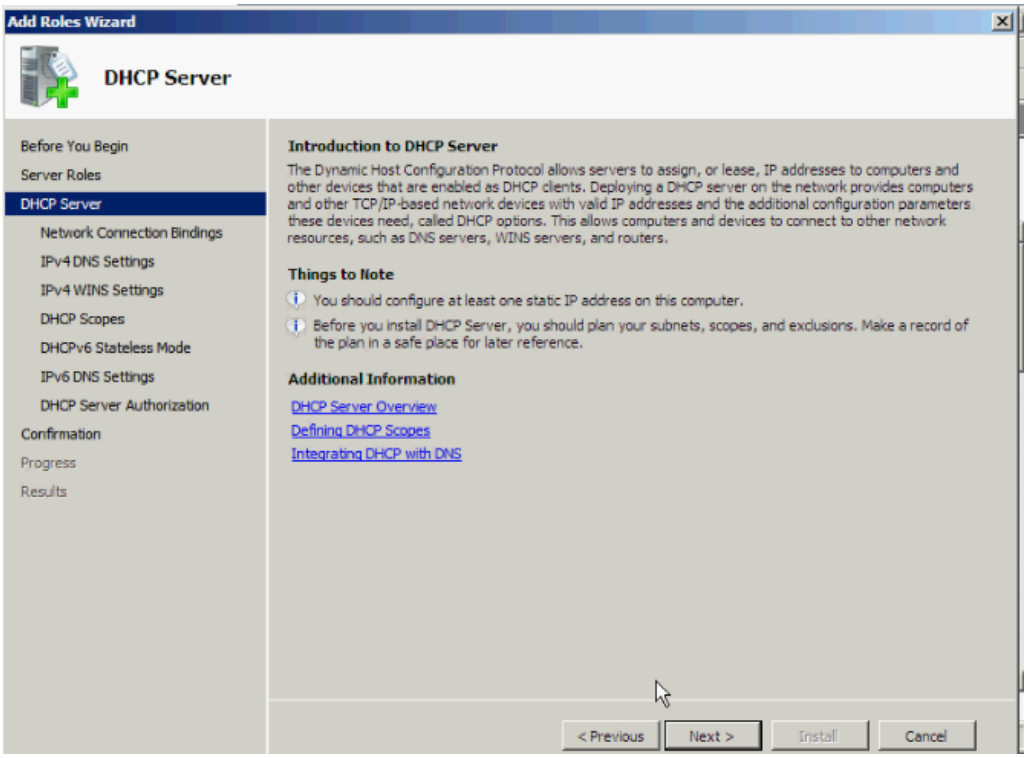
- Vào **Server Manger ➔ Roles ➔Add Roles.**



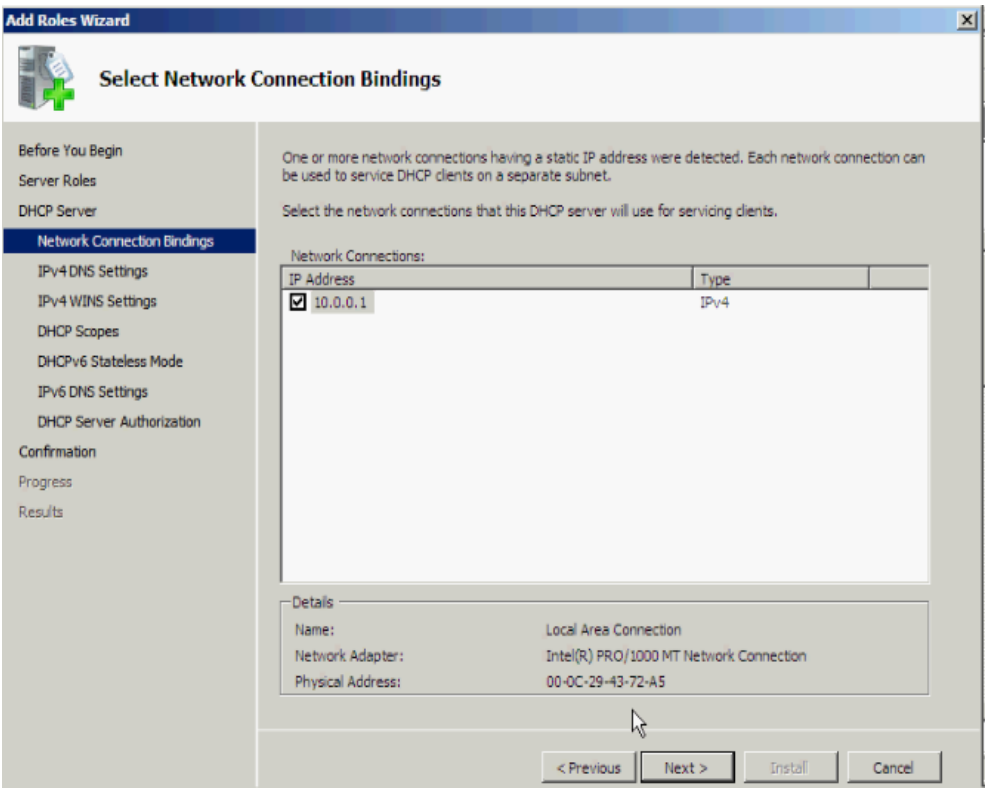
- Nhấn **Next** ➔trong mục **Roles** chọn "**DHCP Server**". Nhấn **Next.**



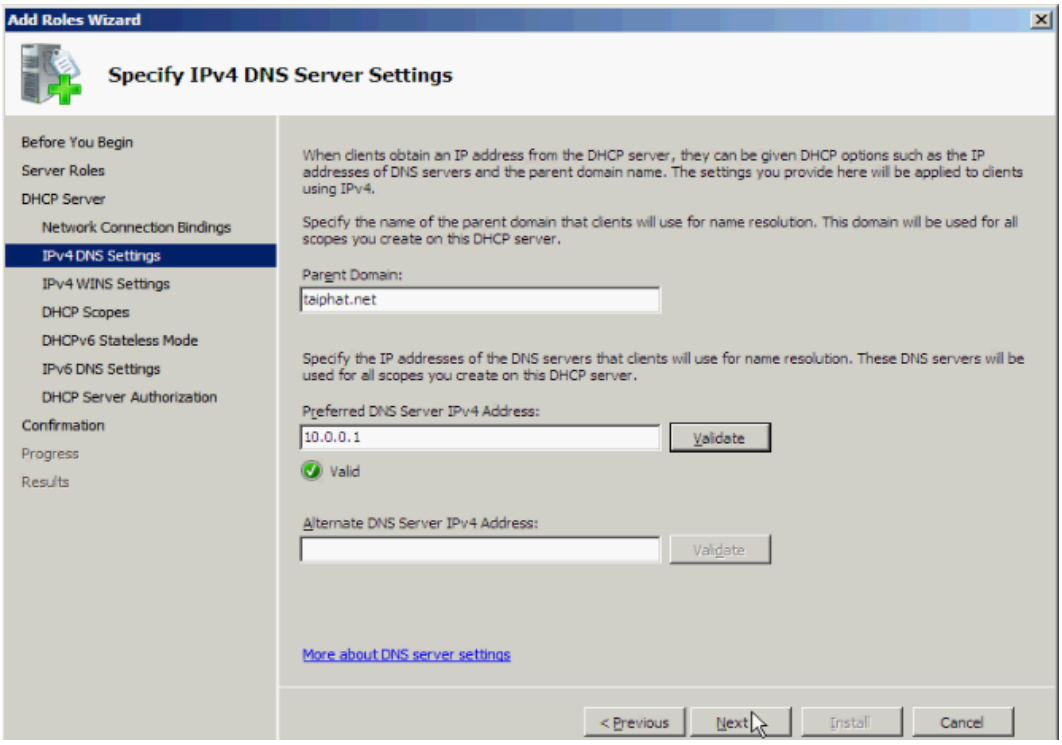
- Trong bảng này giới thiệu về DHCP và các điểm cần lưu ý **Things to Note**. Tiếp tục nhấn Next.



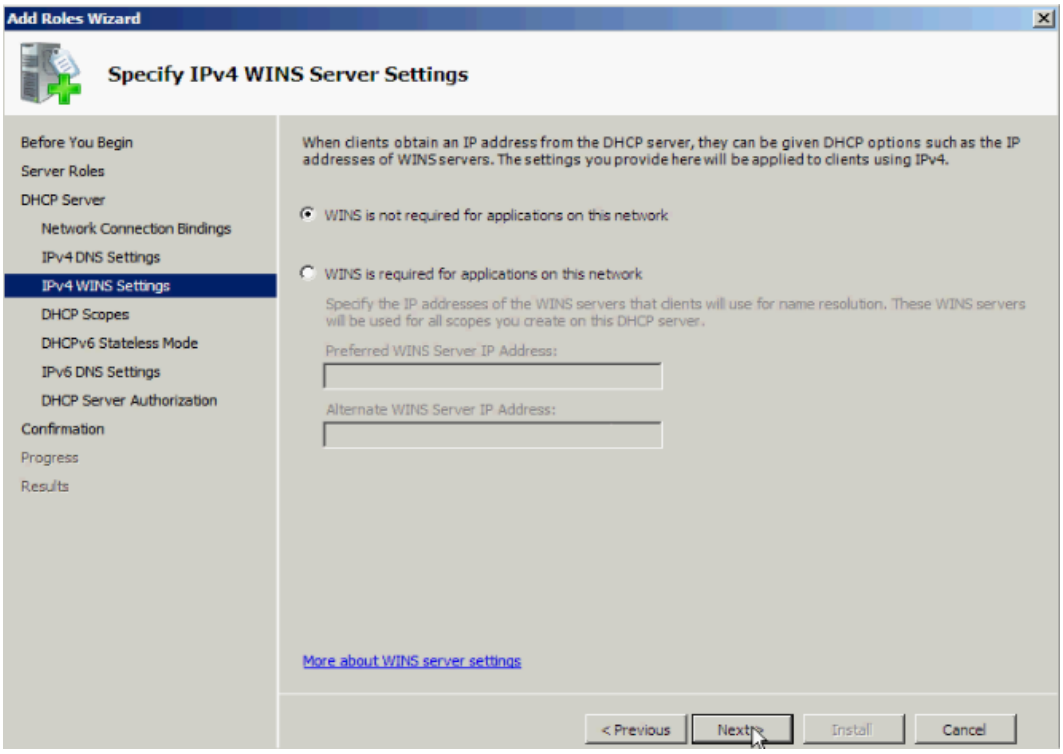
- Chọn card mạng sử dụng dịch vụ này ở đây chúng ta chỉ có một card mạng nên tiếp tục nhấn Next nhấn **Next.**



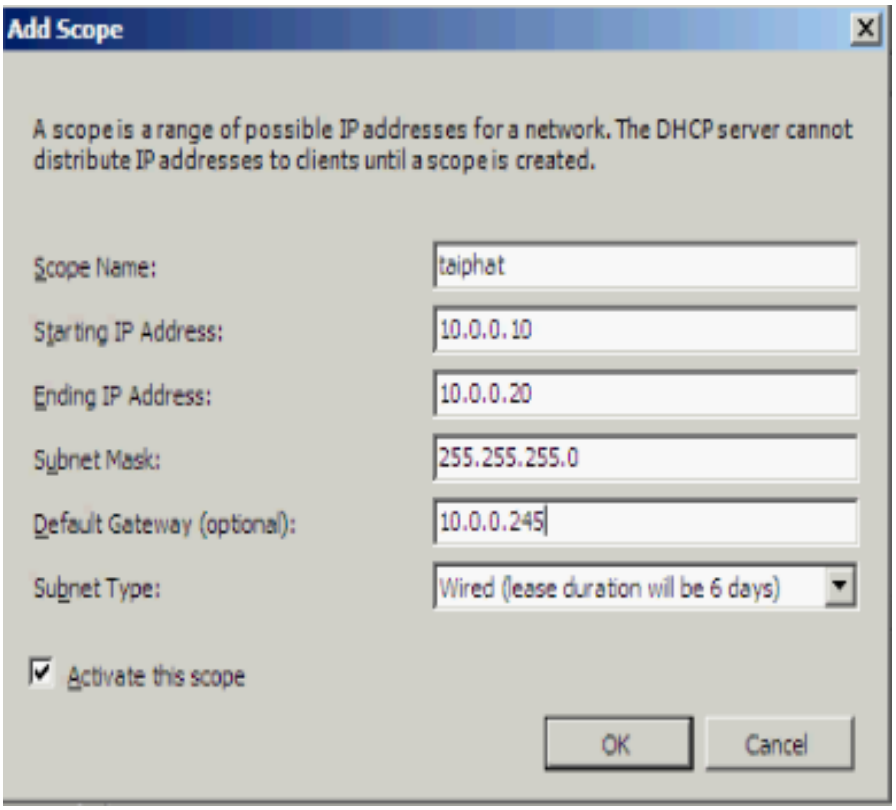
- Trong mục "**Parent Domain**" điền tên domain và điền IP DNS server ở mục "**Preferred DNS**…" và nhấn **Validate** để kiểm tra và xác nhận tồn tại và tiếp tục nhấn **Next**.

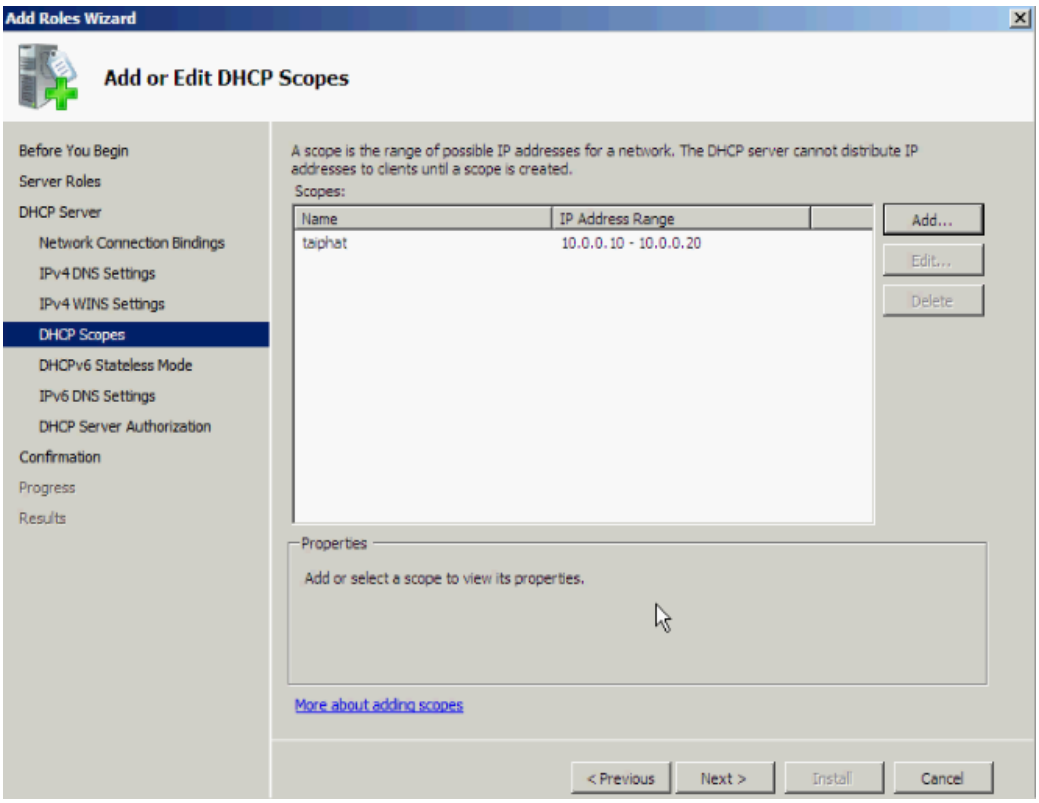


- Tiếp tục nhấn **Next**.

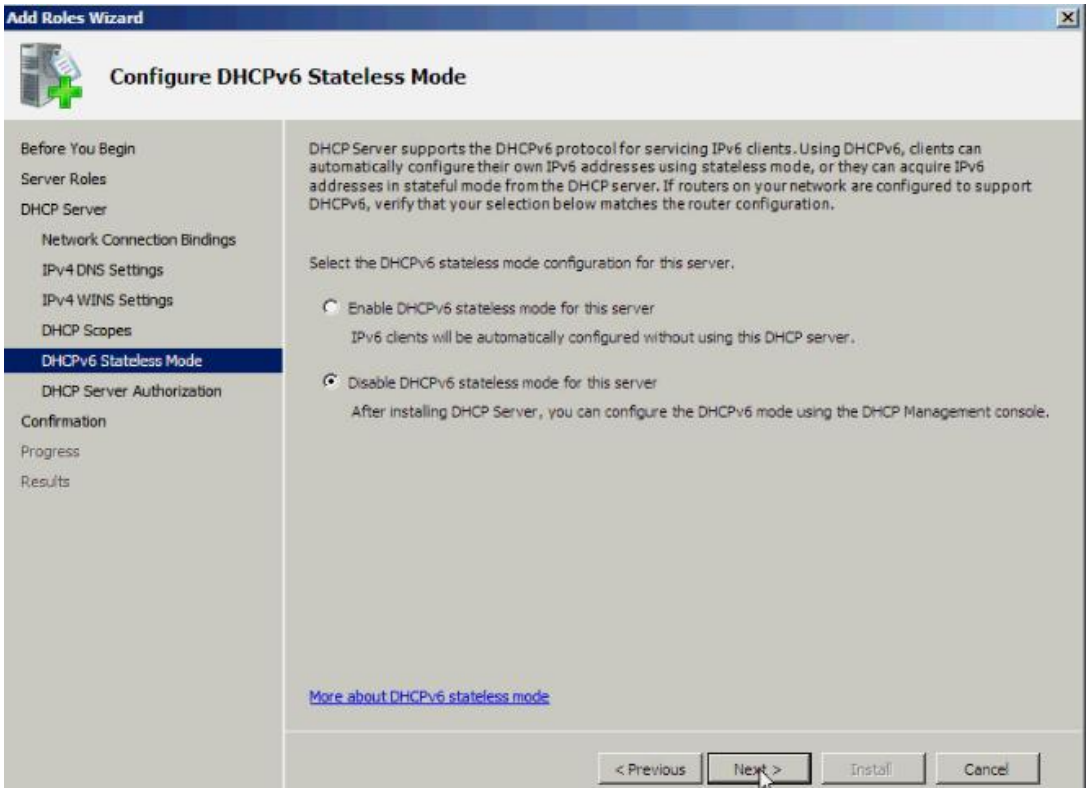


- Ở bảng **Add or Edit DHCP Scopes**, nhấn **Add** để thêm **scope**, điền thông tin scope cần add và nhấn **OK**.

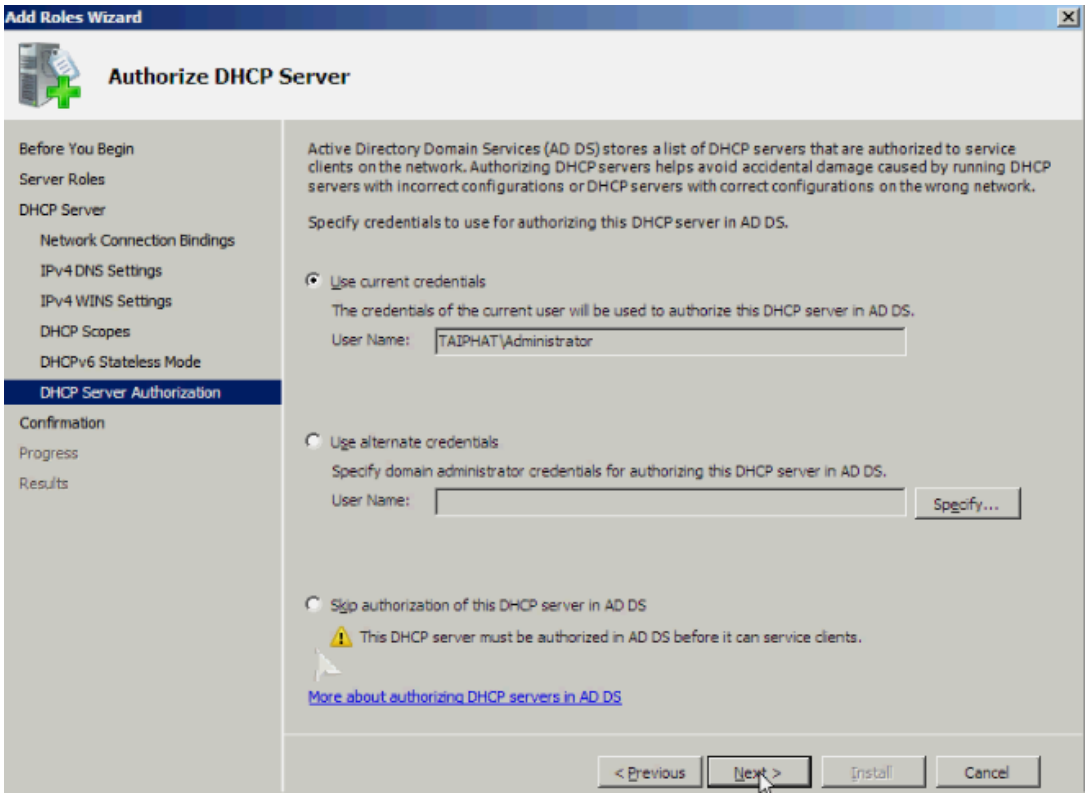




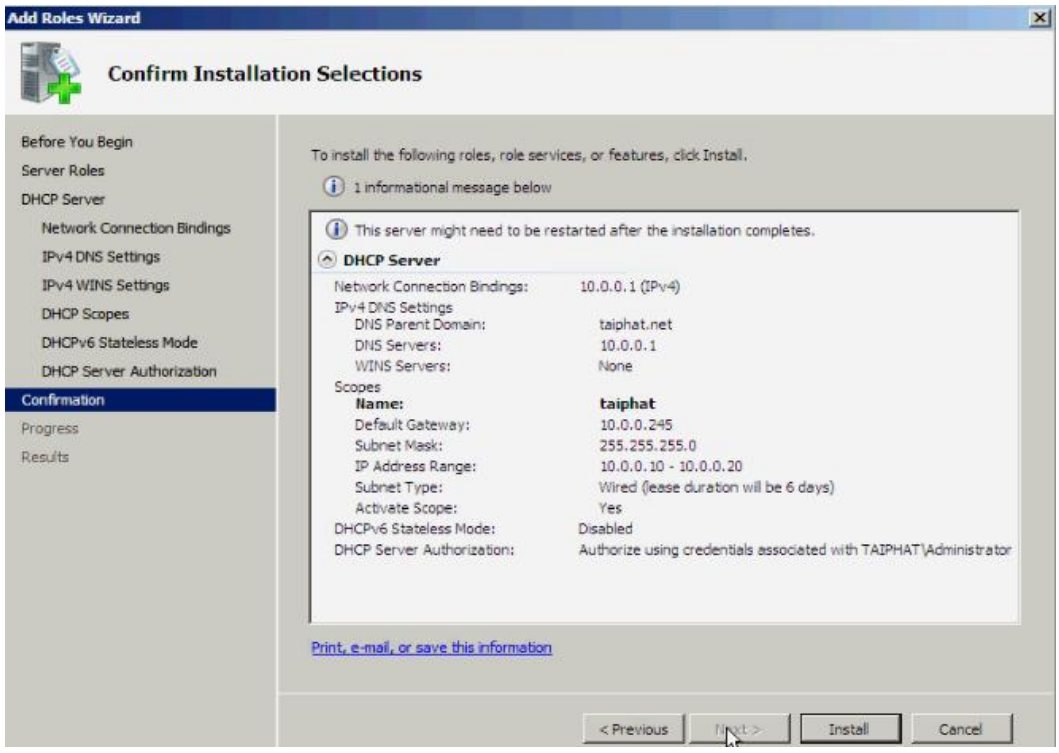
- Nhấn **Next** và Tắt chức năng IPv6 ở đây chúng ta không sử dụng IPv6, chọn "**Disable IPv6 Stateless mode…**" và **Next**.



- Chọn user có quyền Author➔ **Next**.

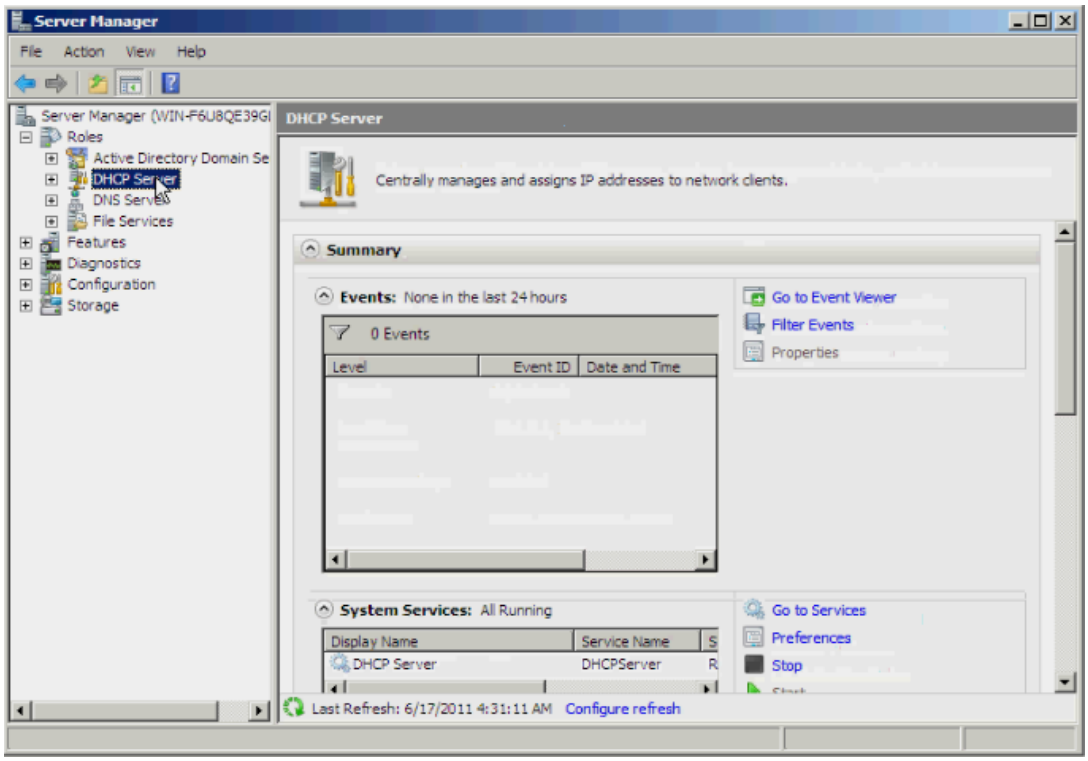


- Xác nhận lại thông tin trước khi cài đặt dịch vụ DHCP.



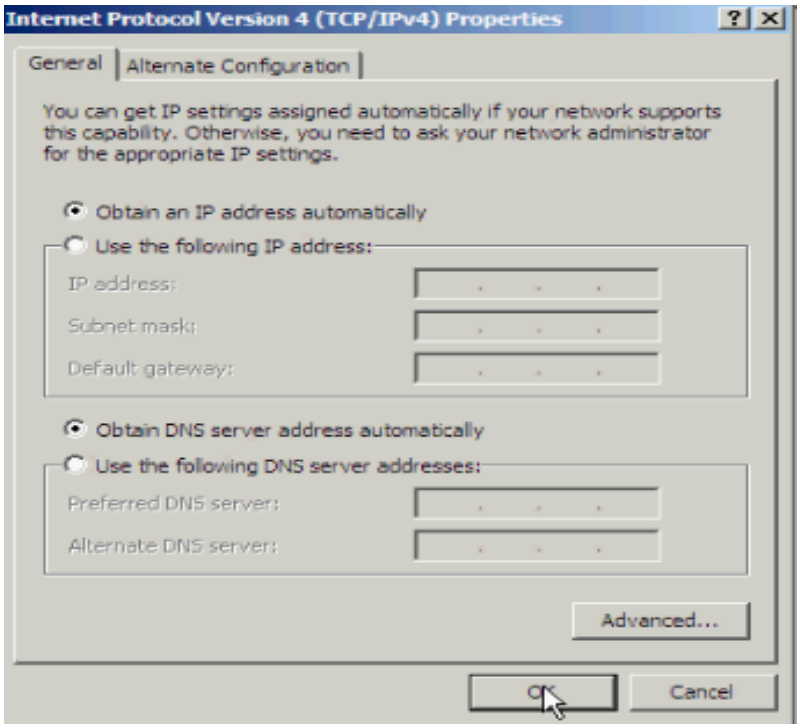
- Nhấn **Install** để tiến hành cài đặt.
- Cài đặt Role hoàn tất, và nhấn **Close**

Kiểm tra lại hệ thống.



3.2 Trên máy Client

- Ở máy client cấu hình TCP/IPv4 cho nhận IP động.

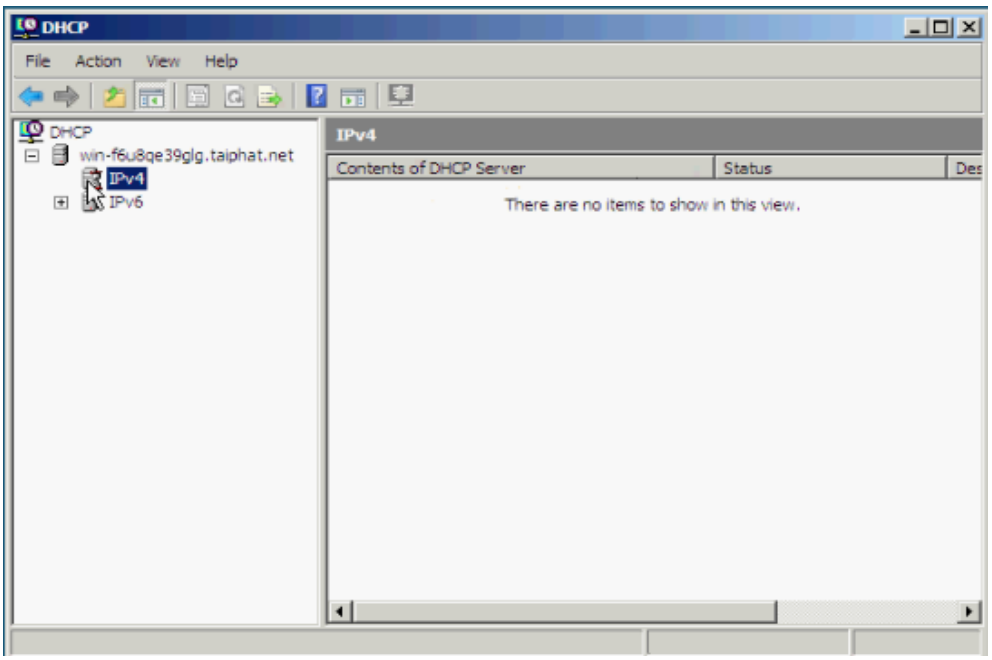


- Mở Command Prompt, nhập lệnh ipconfig /release (xóa IP động hiện tại) và nhập tiếp lệnh ipconfig /renew (yêu cầu cấp IP động mới) để kiểm tra việc cấp phát ip động của DHCP.

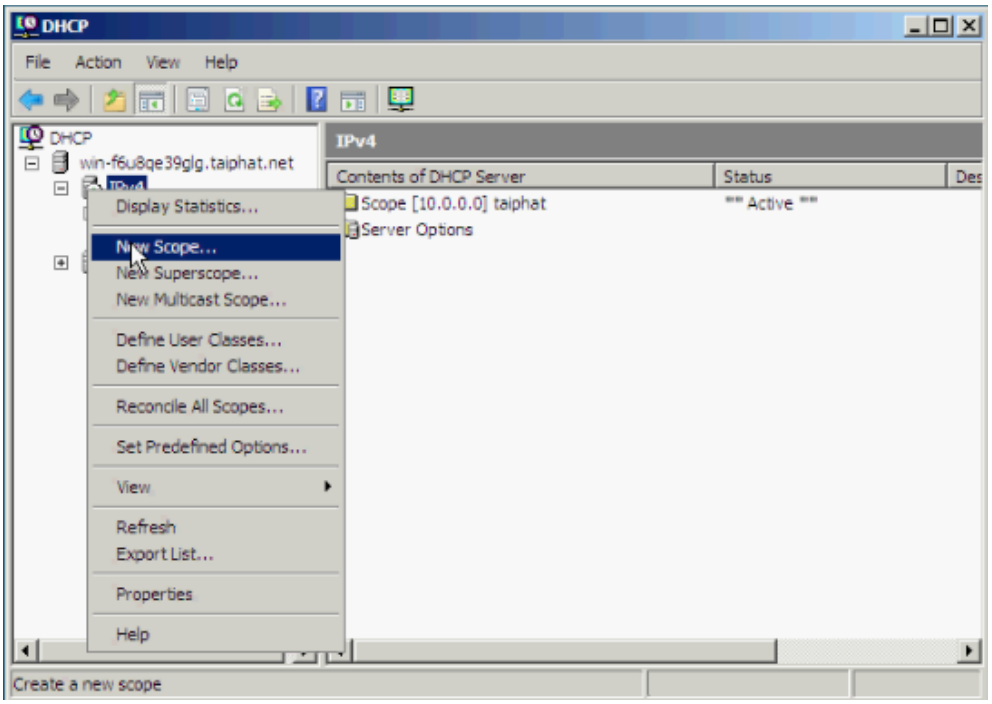
4. Cấu hình DHCP

4.1. Tạo Scope

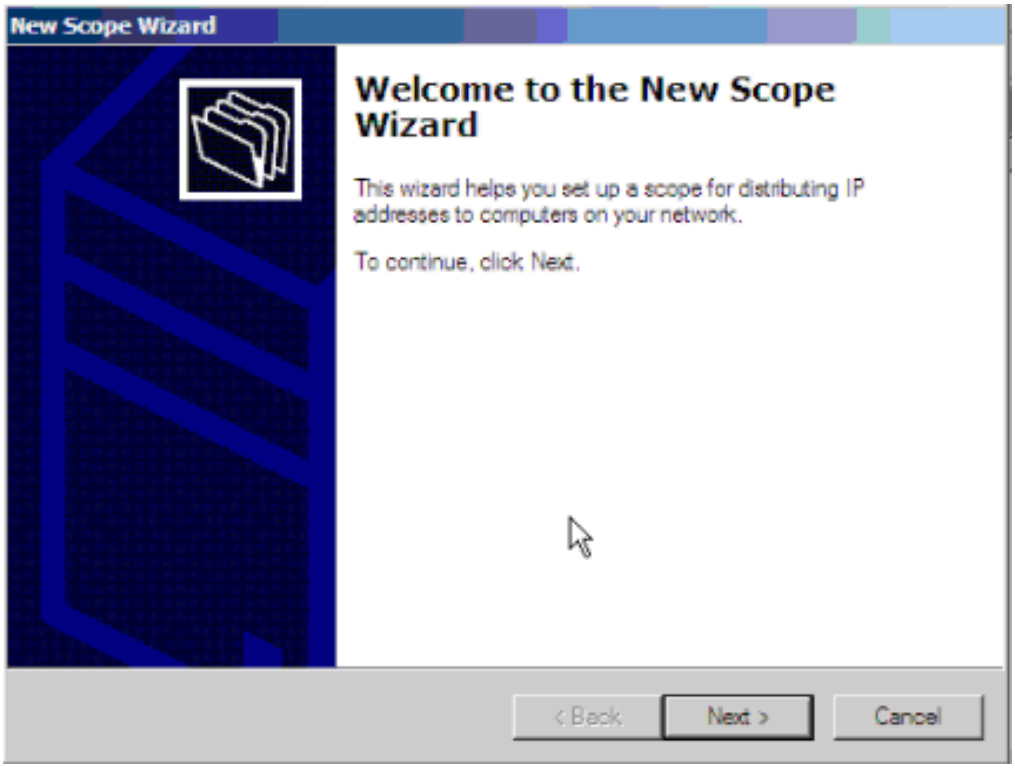
- Vào **Administrative Tools ➔DHCP**.



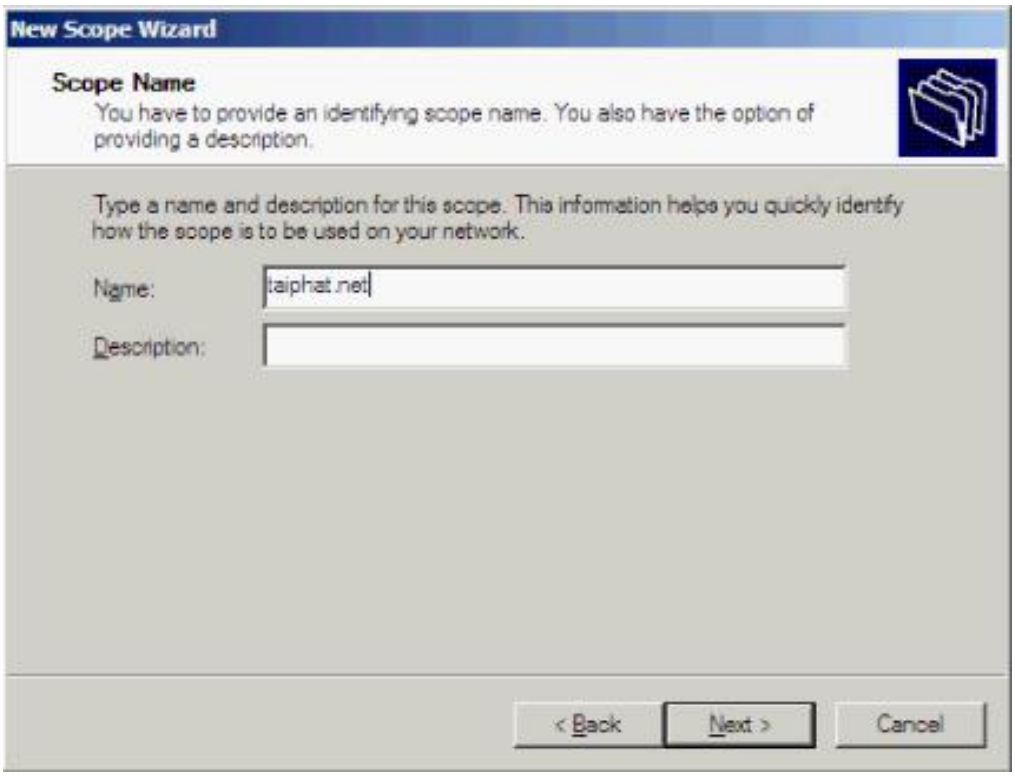
- Nhấn chuột phải vào **IPv4** và **New Scope**.



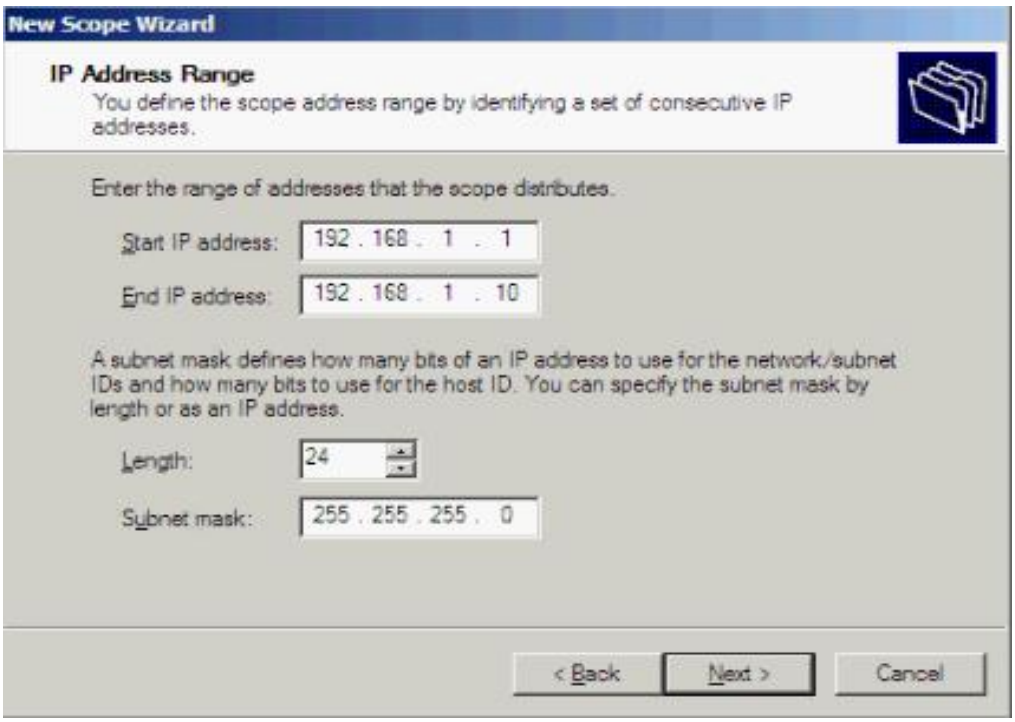
- Hộp thoại **New Scope** hiện ra và **Next**.



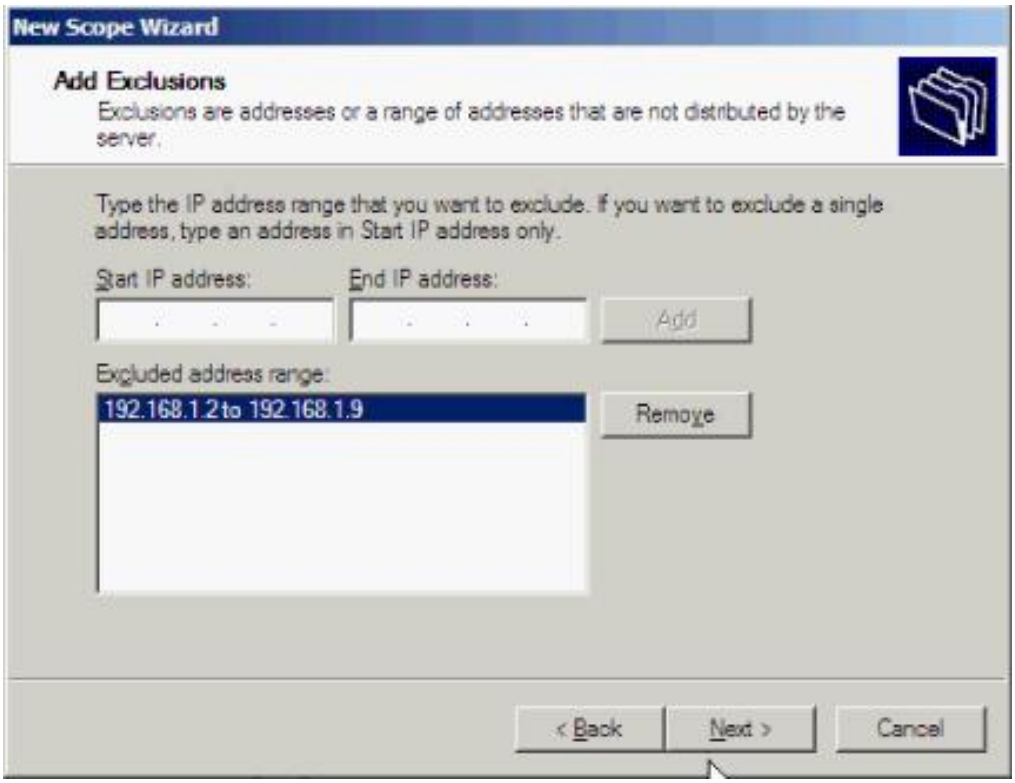
- Hộp thoại **Scope Name** và Điền tên của scope vào mục **Name** và nhấn **Next**.



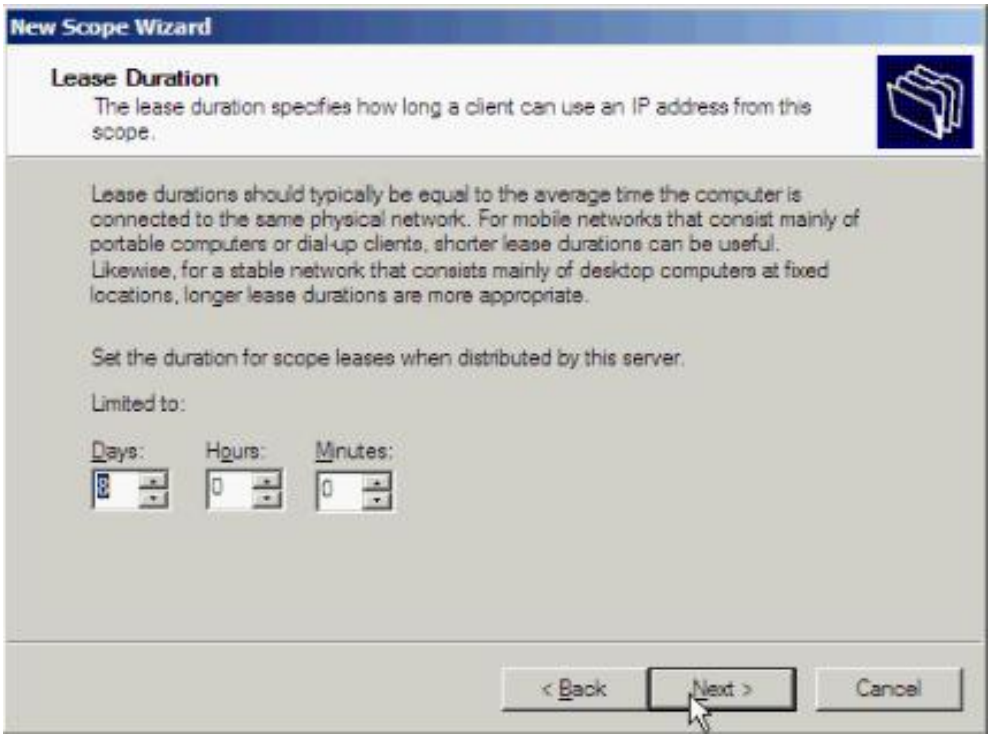
- Hộp thoại **IP Address Range**, điền thông số range IP cấp phát và subnet mask➔ **Next**.



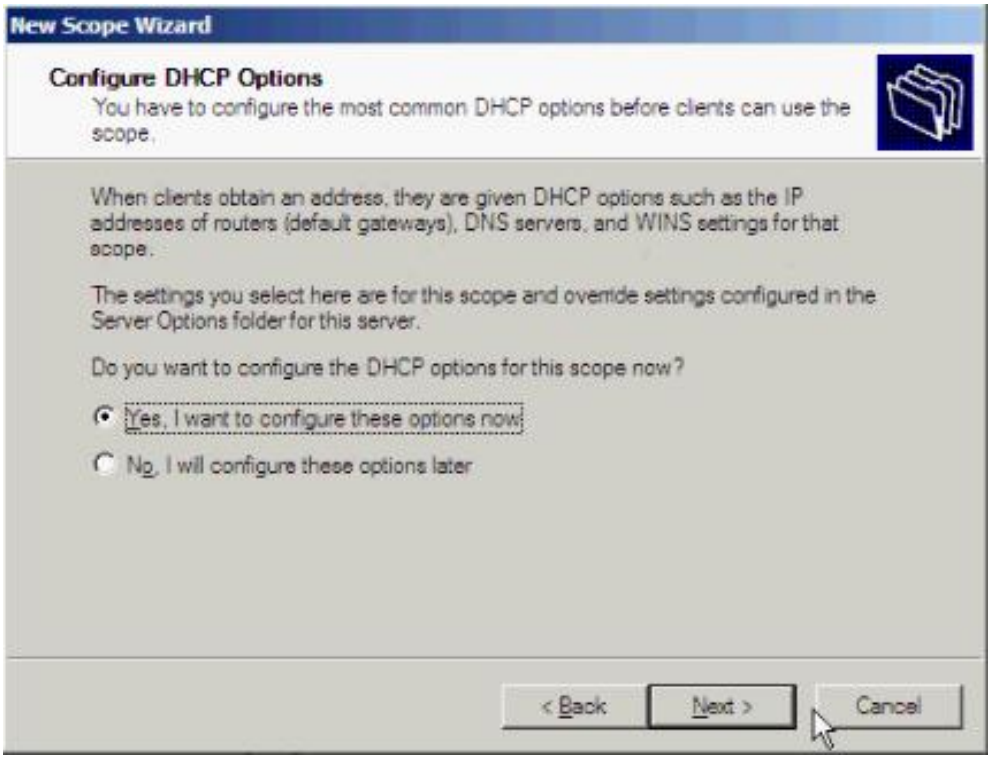
- Hộp thoại **Add Exclusions**: nhập range ip đặc biệt không dùng để cấp phát ➔**Add** ➔**Next**.



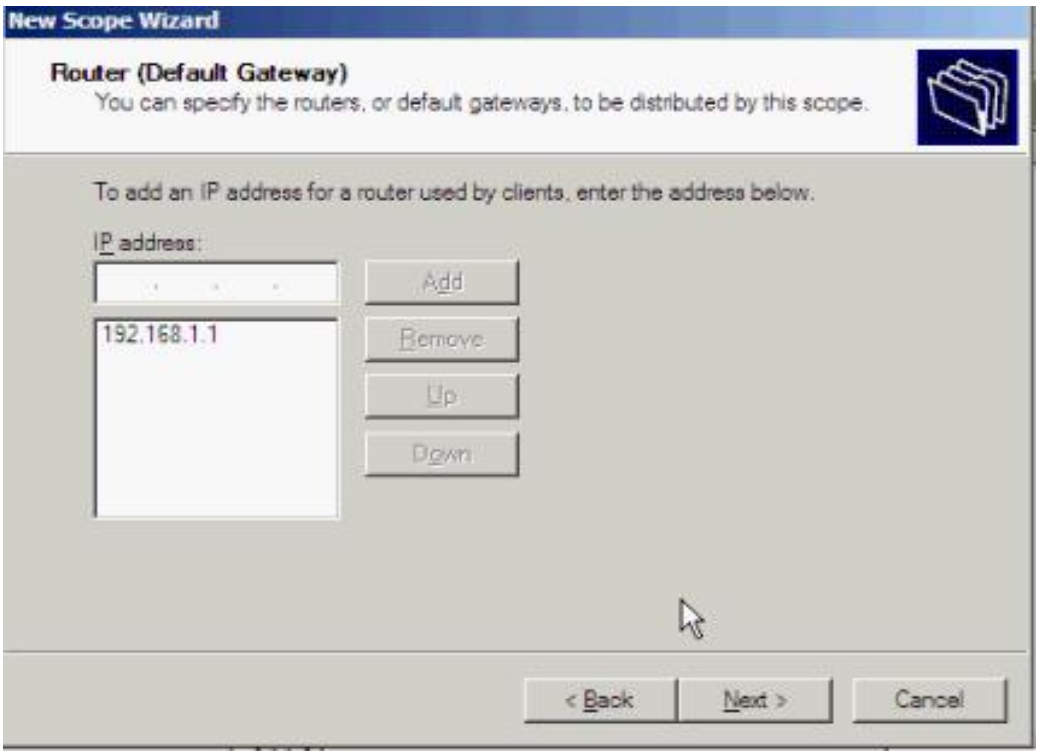
- Hộp thoại **Lease Duration**: thời gian thuê địa chỉ IP mặc định là 8 ngày.



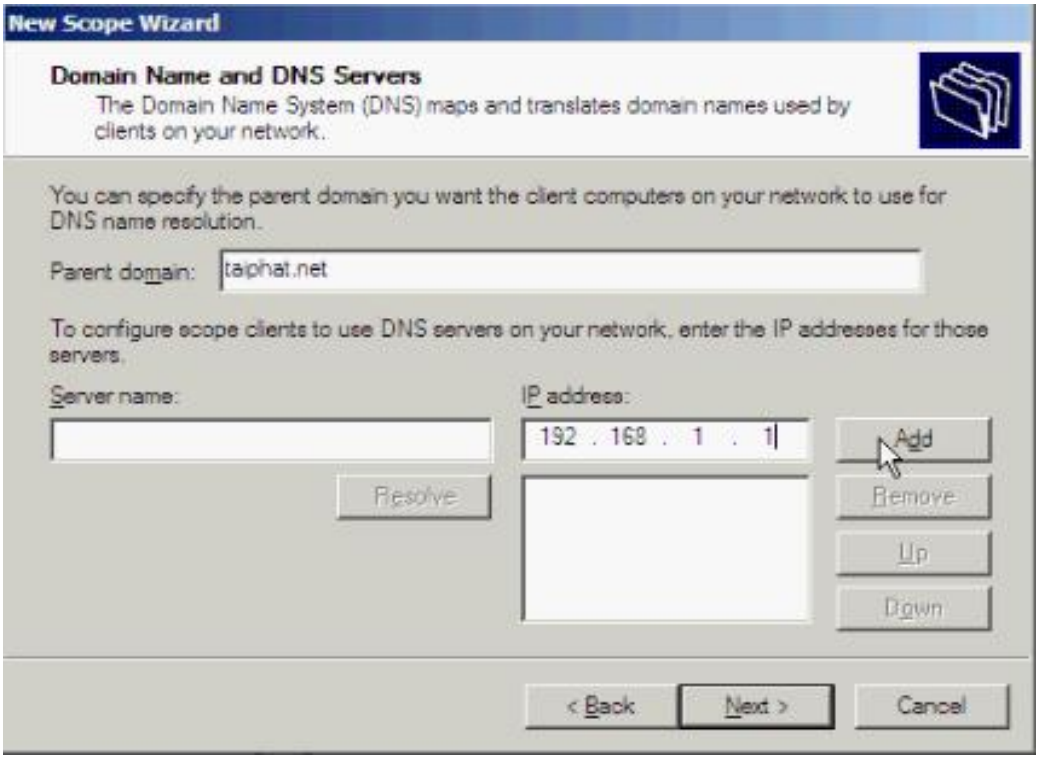
- Hộp thoại **Configuration DHCP Options** yêu cầu chúng ta cấu hình thông số dịch vụ của scope ngay bây giờ hoặc để sau. Ở đây ta chọn **Yes, I want to config these options now** và nhấn **Next**.



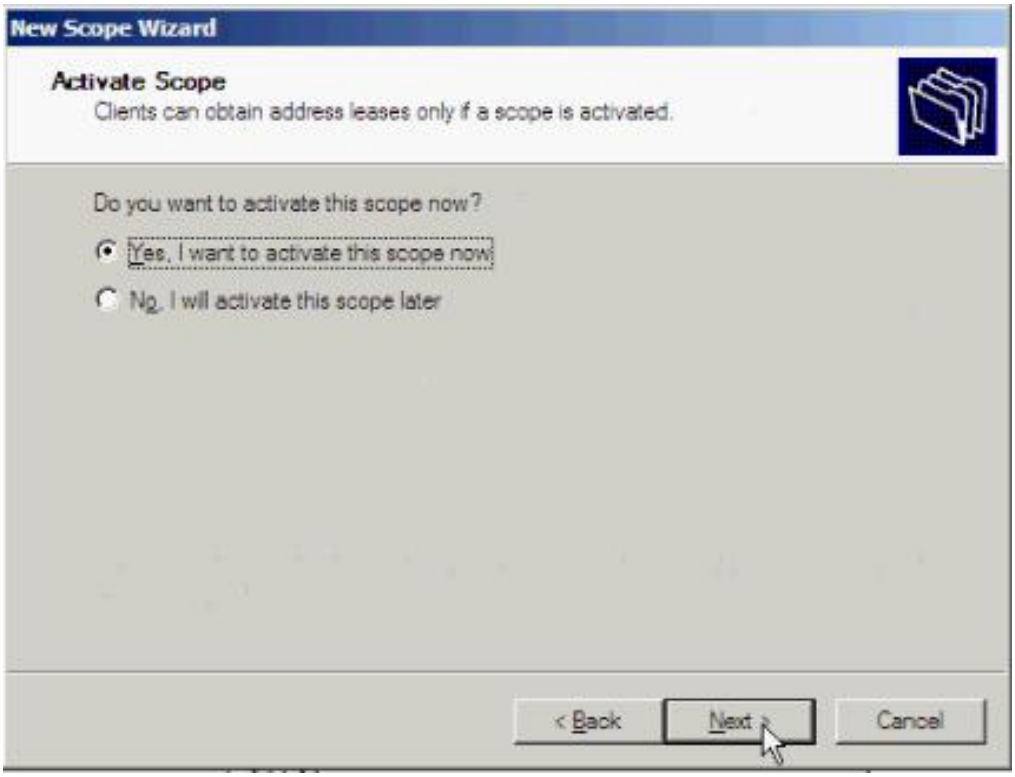
- Hộp thoại **Router (Default gateway):** nhập địa chỉ default gateway của scope này rồi nhấn Add và Next.



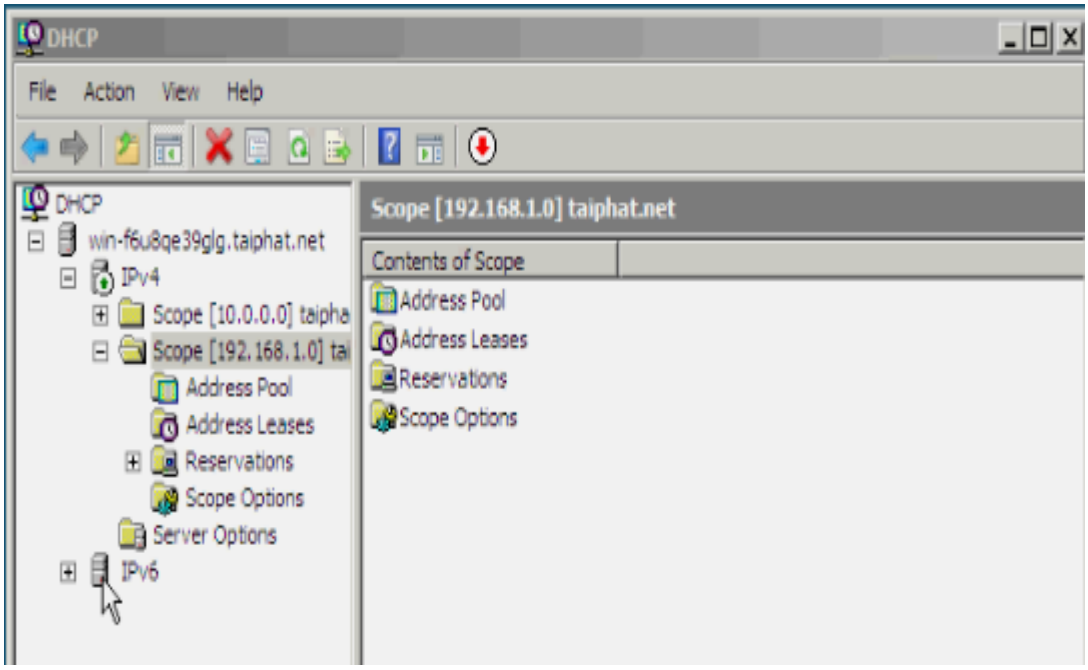
- Hộp thoại **Domain Name và DNS server** : điền tên domain, phần IP Address điền IP DNS server



- Nhấn **Next** để tiếp tục.
- Hộp thoại **Active Scope** chọn **active scope** và nhấn **Next.**

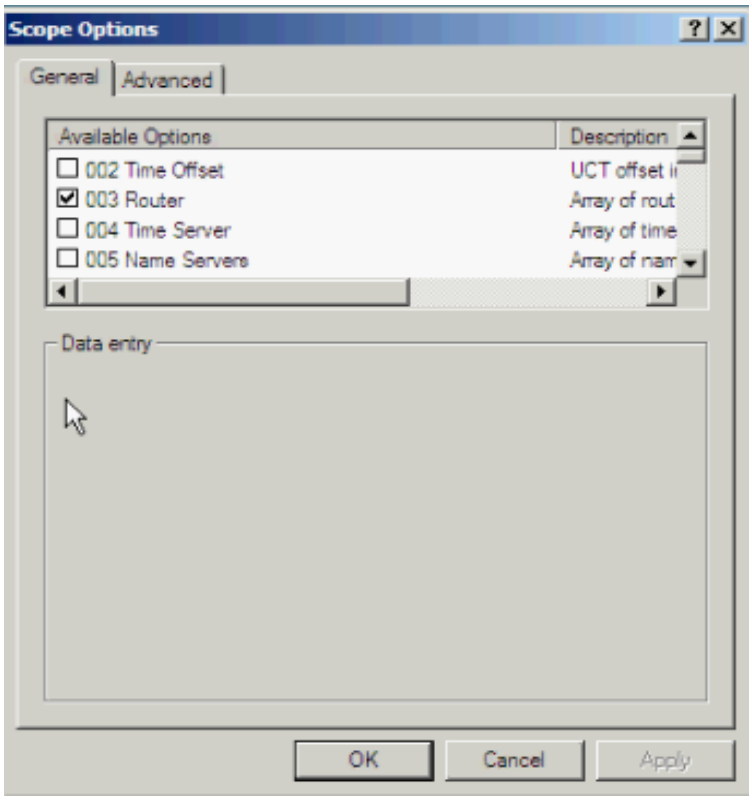


- Sau đó nhấn Finish để kết thúc.
- Xem kết quả scope 192.168.1.0 đã được tạo:

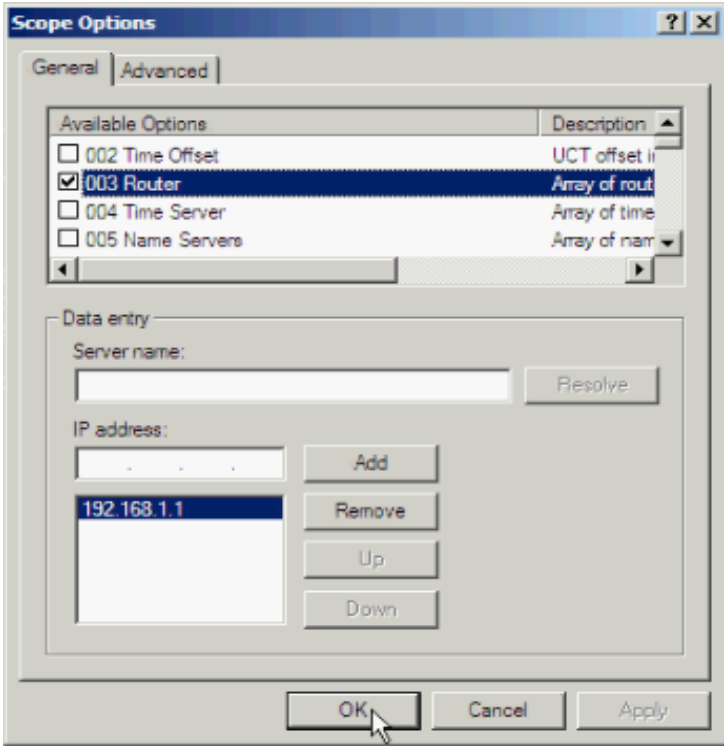


4.2. Thay đổi options của Scope

- Xổ scope cần thao tác và chuột phải **scope options ➔Configure Options**.
- Hộp thoại Scope Options hiện ra, ở trường Available Options là những thuộc tính sẵn sàng mà chúng ta có thể thay đổi với những thuộc tính đã stick là những thuộc tính đã được cấu hình trước đó.



- Chúng ta sẽ thử cấu hình default gateway lại cho scope này, chọn **Router**. Router Options hiện ta cho chúng ta thêm xóa và edit với những thuộc tính khác cũng vậy.

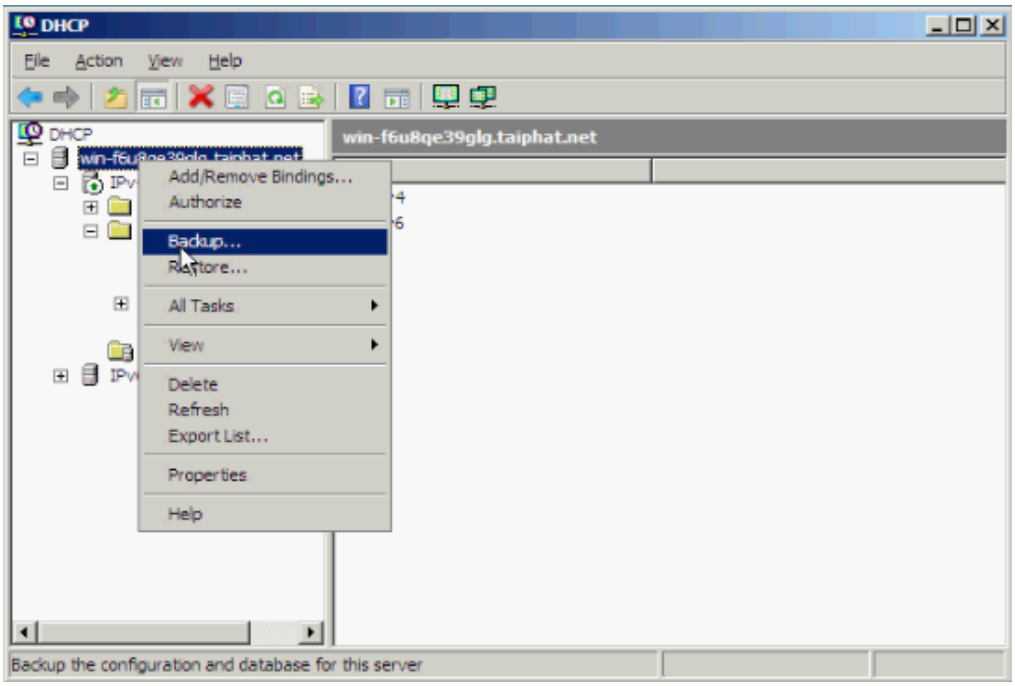


4.3. Thay đổi Server options

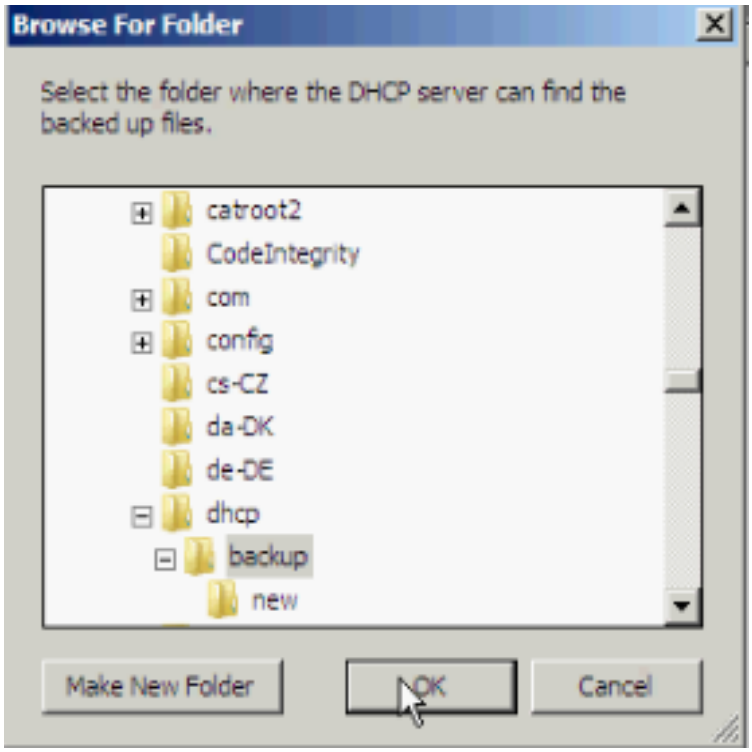
- Chuột phải **Server options ➔Configure Options**.
- Cũng như cách thức thay đổi thuộc tính của scope options chỉ khác là những thuộc tính thay đổi ở đây sẽ áp cho tất cả các scope của server.

5. Backup DHCP Server

- Vào Administrative Tools là DHCP. Nhấn chuột phải tên máy và **Backup**…



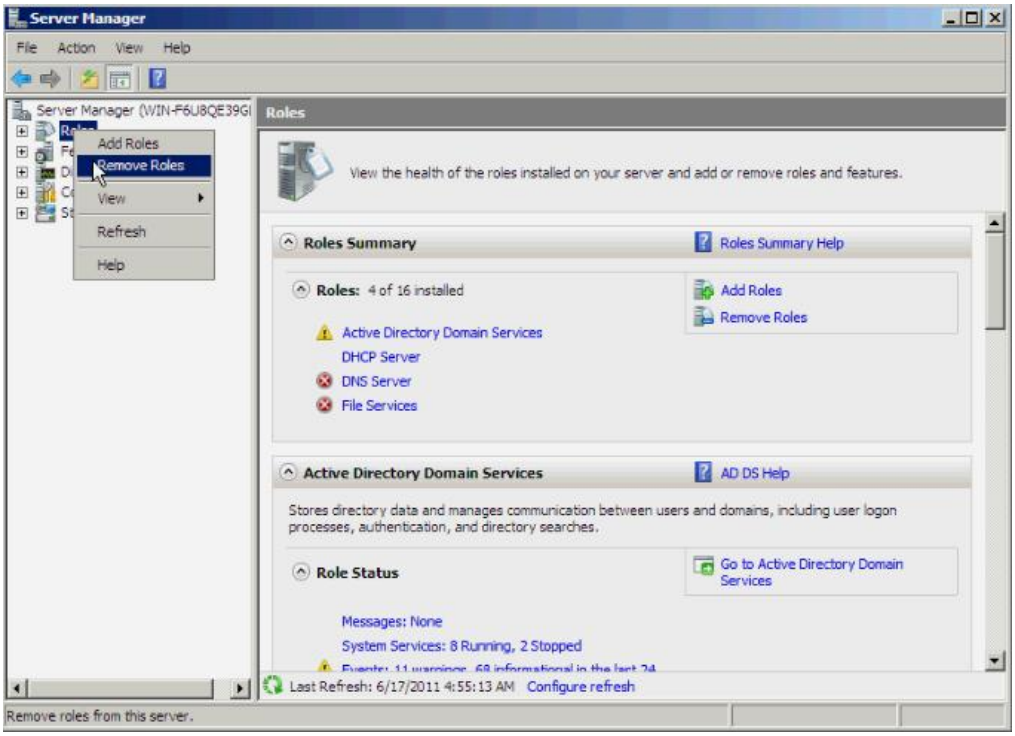
- Hộp thoại **Browse For Folder** hiện ra yêu cầu chọn nơi cất file backup, mặc định là trong **C:\Windows\system32\dhcp\backup.**



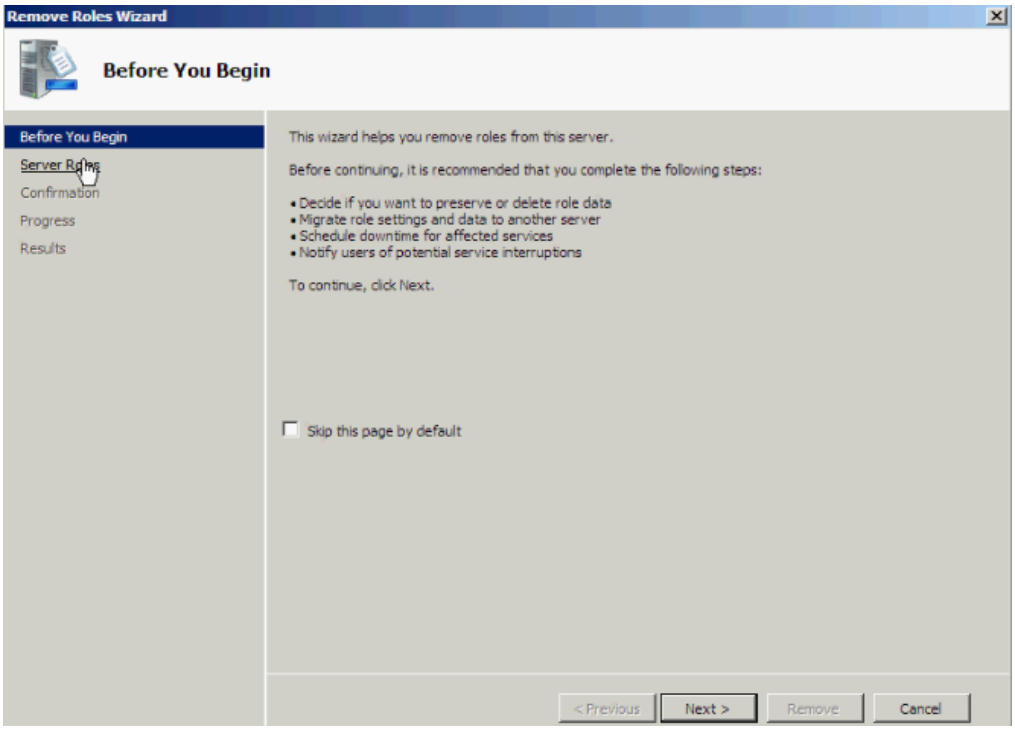
- Chúng ta để mặc định và **OK** kết thúc quá trình backup vào thư mục chứ bakup kiểm tra.

6. Remove DHCP Server

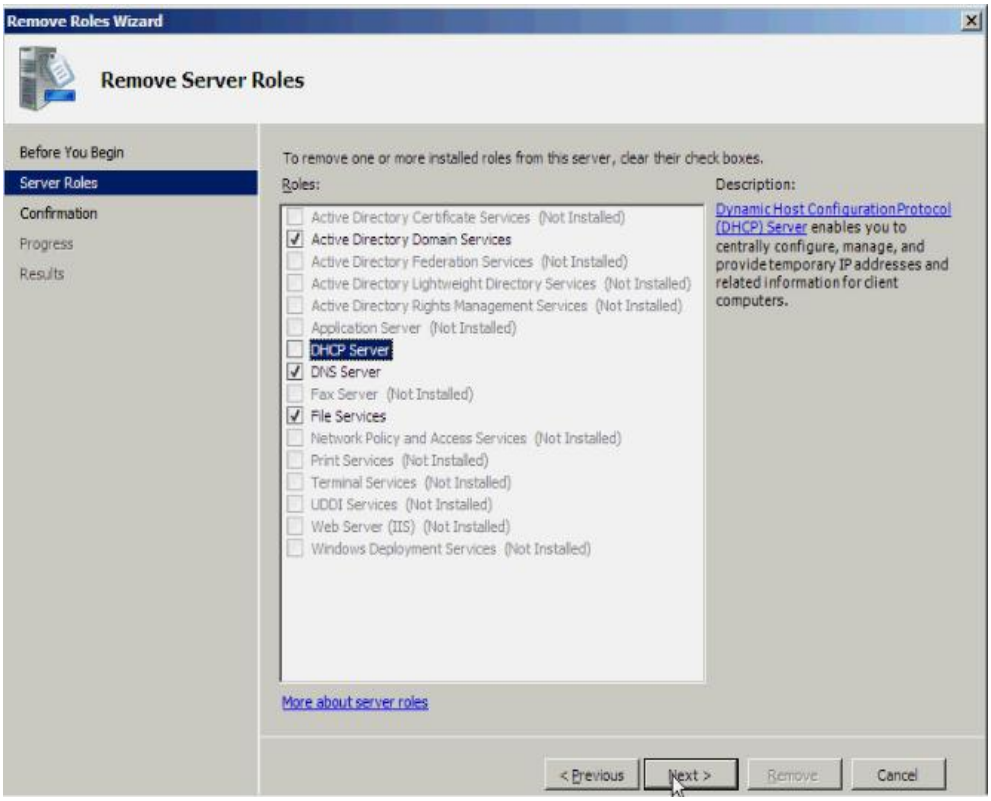
- Vào **Server Manager➔ Roles ➔** Chọn **Remove roles**.



- Hộp thoại **Remove Roles Wizard** hiện ra và nhấn **Next**.



- Bỏ dấu stick dịch vụ **DHCP** và **Next**, sau đó chọn **Remove** để xóa dịch vụ **DHCP**



- Sau đó Restart lại hệ thống.

III.DỊCH VU THƯ MỤC (Directory Services)

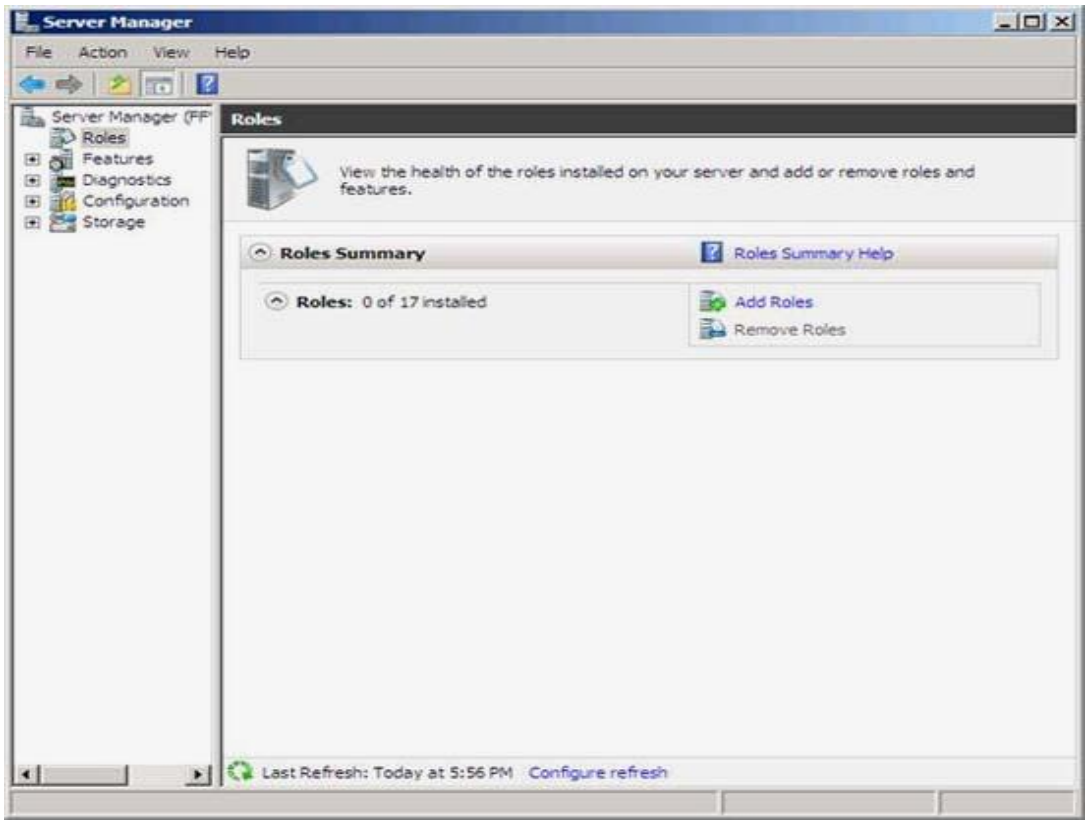
1. Chuẩn bị

Thiết lập địa chỉ IP cho card mạng của server hoặc bạn có thể thiết lập địa chỉ IP của các DNS Server trong hệ thống. Nếu muốn cài đặt một Read-Only Domain Controller,bạn phải chuẩn bị forest bằng lệnh adprep /rodcprep.Xây dựng các DNS Server trong hệ thống mạng nếu có, trong quá trình cài đặt AD DS sẽ có cài đặt DNS Server.

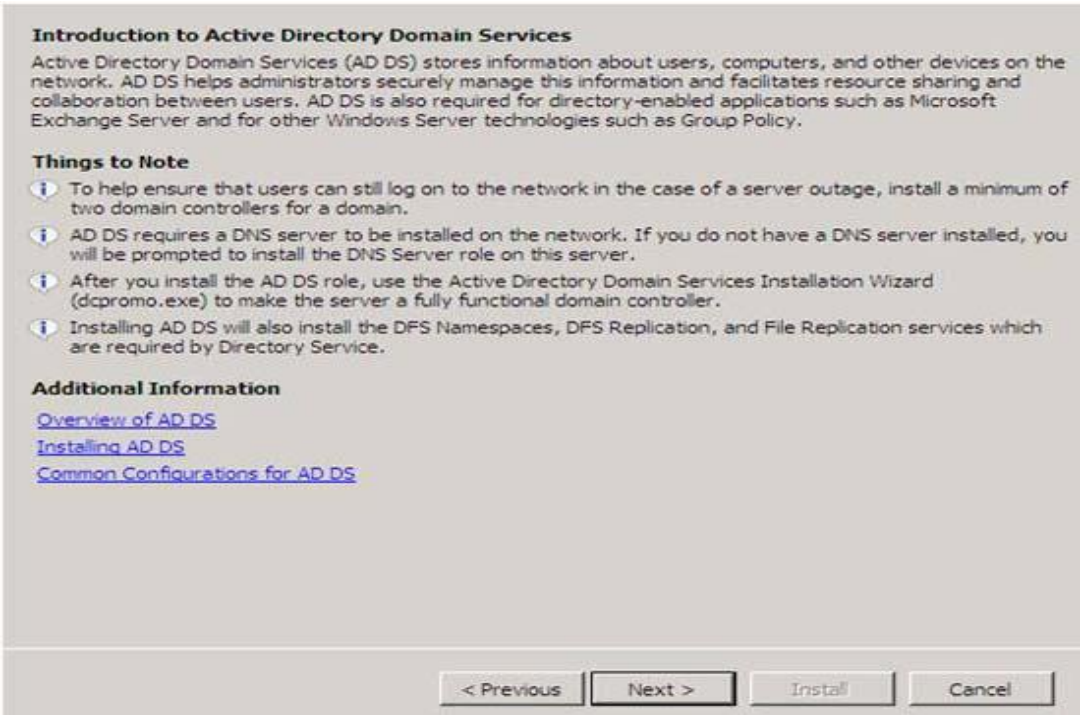
2. Cấu hình

2.1 Trên máy Server

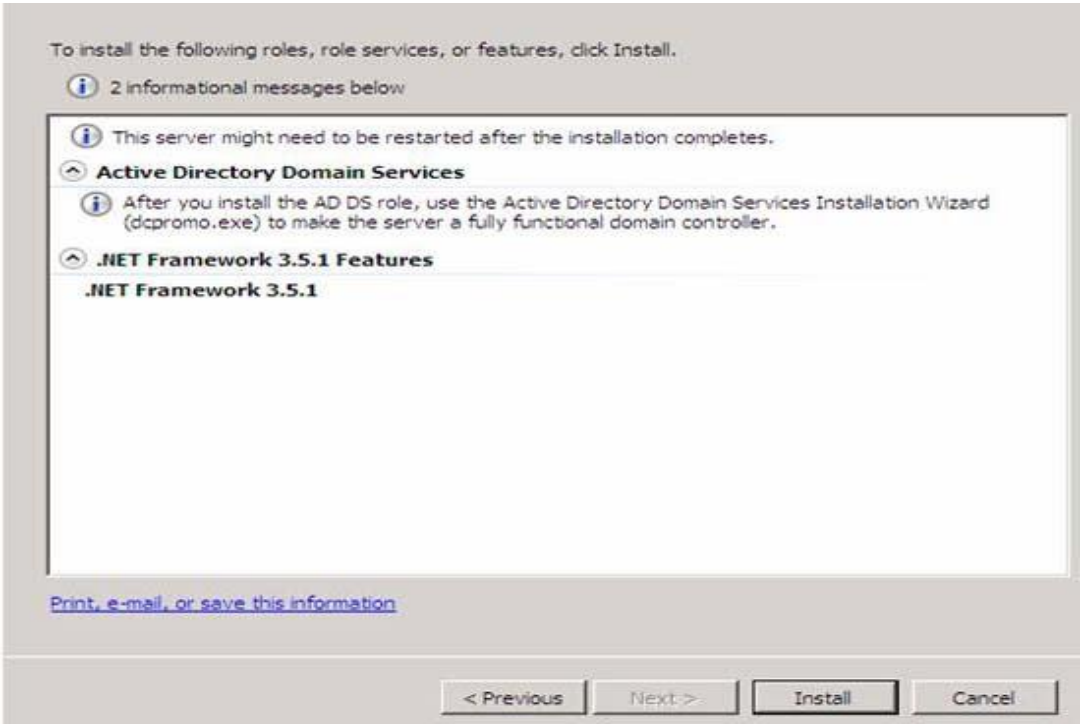
- Vào **Adminstrator Tool** chọn **Server Manager**
- Trong mục **Roles** chọn **Add roles**.



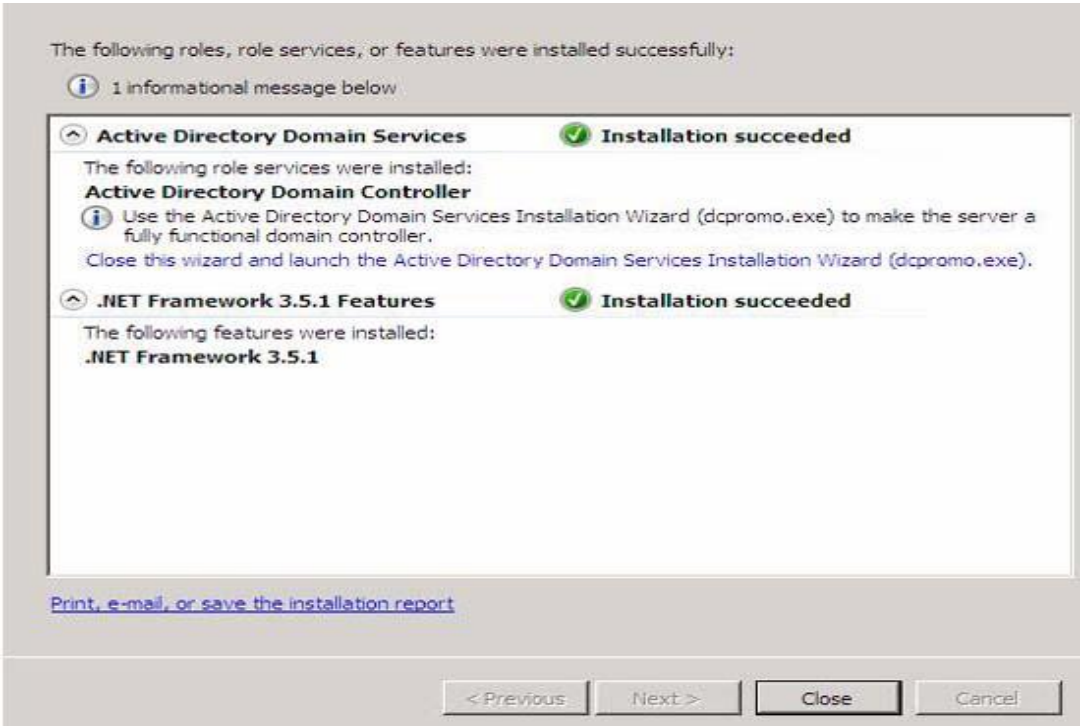
- Nhấn **Next**, mục này mô tả về AD DS và những chú ý **Things to Note**.



- Tiếp tục Next, mục này xác nhận lần cuối trước khi cài đặt dịch vụ.



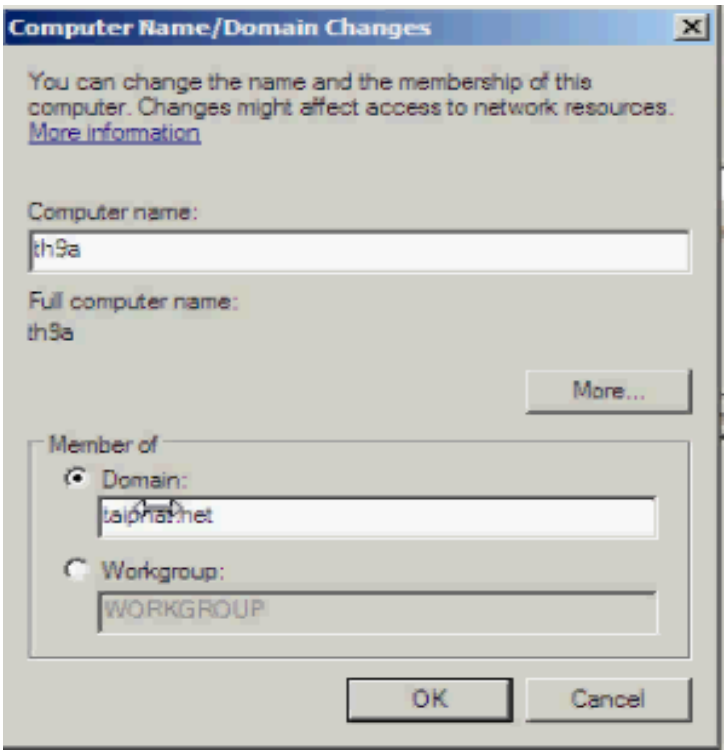
- Quá trình cài đặt thành công. Click Close.



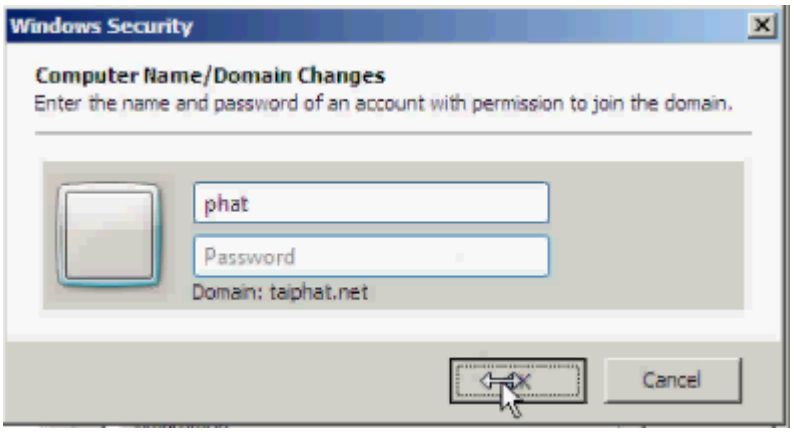
- Tiến trình cài đặt dịch vụ kết thúc sẽ hiện ra câu thông báo yêu cầu nâng cấp lên domain bằng lệnh dcpromo như Windows Server 2003.

2.1. Cho Client vào Domain

Computer Name: đánh tên máy vào đây nếu muốn đổi tên ở đây chọn là **th9a**.



- Tiếp theo stick vào phần Domain nhập tên Domain ,ở đây Domain có tên là **taiphat.net.**
- Nhấn **OK** hệ thống check DNS server DC của domain **taiphat.net**, bảng thông báo hiện ra yêu Xác nhận hoàn tất.



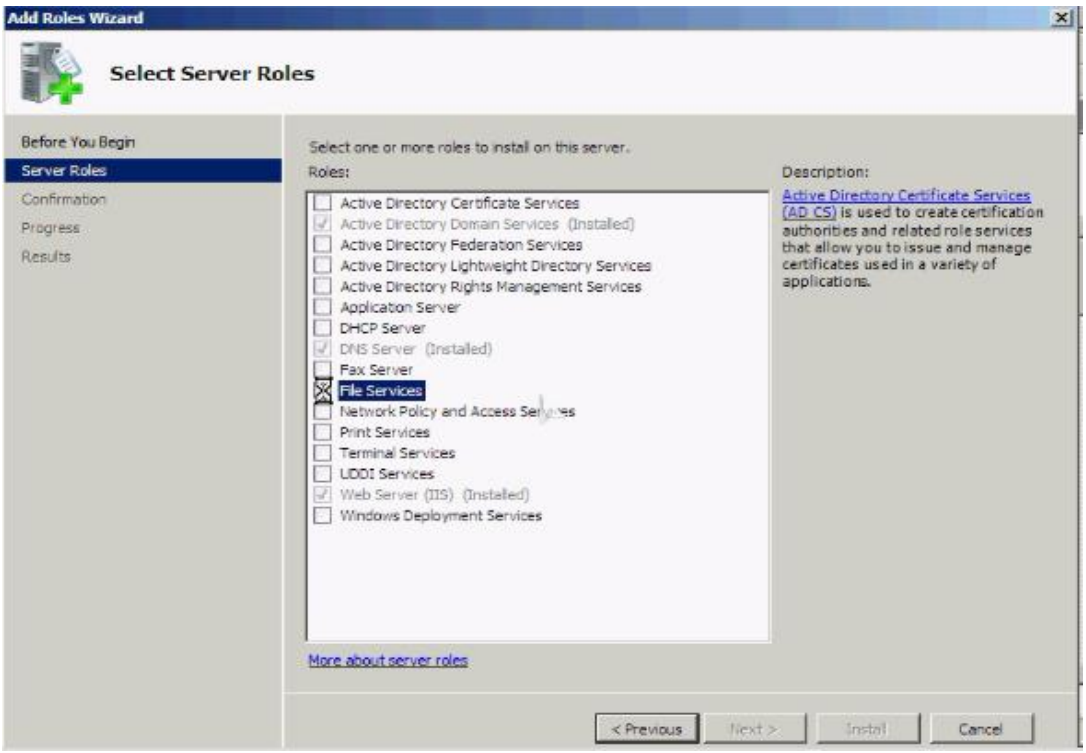
- Tiếp theo chọn OK và sau đó được yêu cầu **Restart** lại hệ thống.

IV. DỊCH VỤ TẬP TIN (File Services)

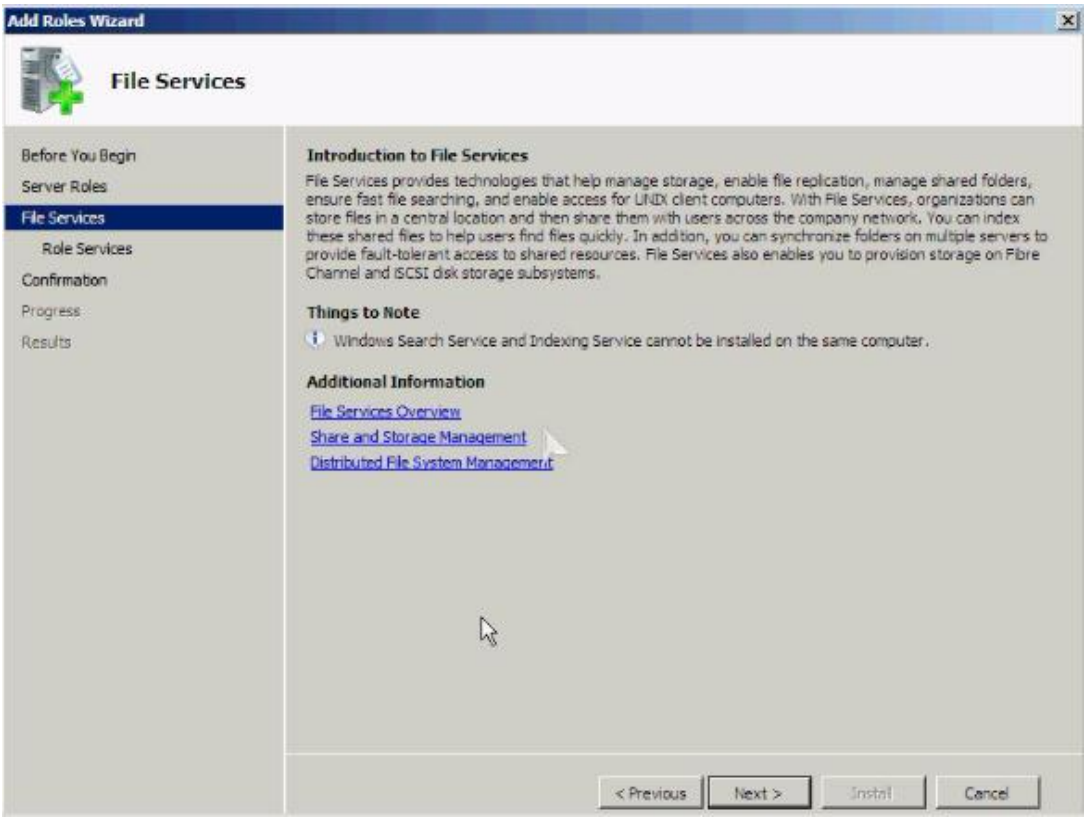
1. Triển khai File Sevices

File Server Resource Manager là một tập hợp các công cụ cho phép người quản trị có thể điều khiển và quản lý dữ liệu trên các server chạy hệ điều hành Windows Server 2008 một cách hiệu quả.Với công cụ này, có thể cấu hình quota trên cả ổ đĩa và thư mục,ngăn cấm sao chép những định dạng mà bạn chỉ định,đồng thời xuất ra các báo cáo giám sát hoạt động của người dùng trên không gian lưu trữ.

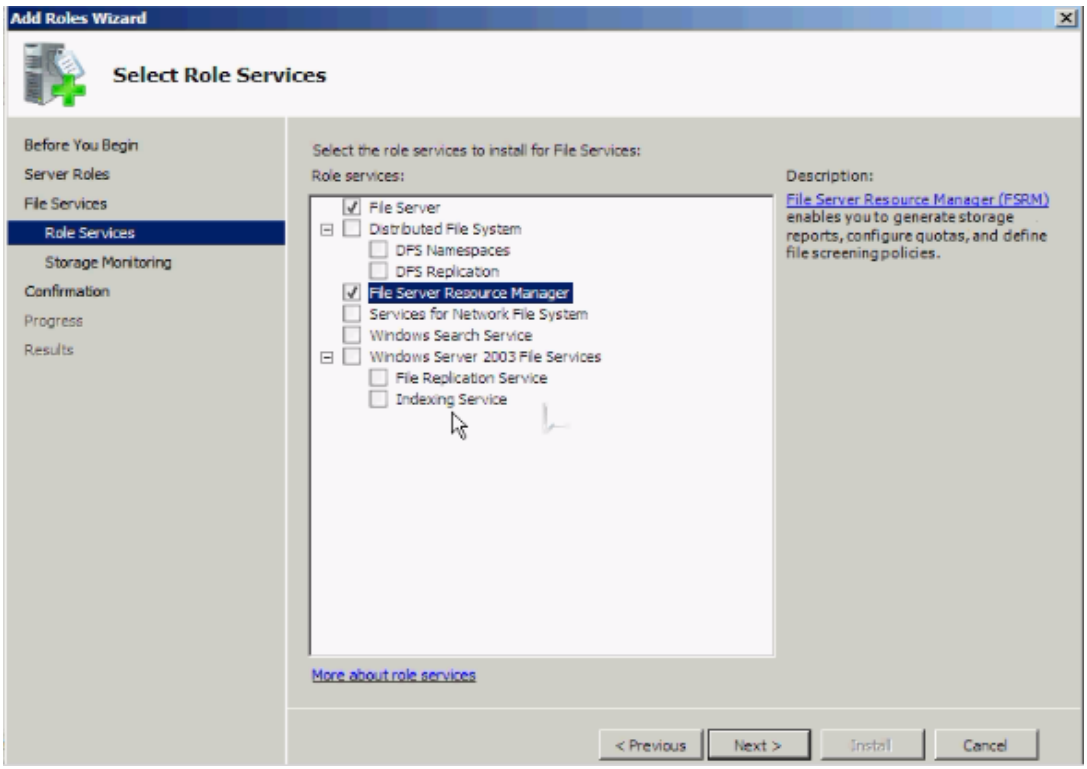
- Để cài đặt dịch vụ **File Services** vào **Server Manager ➔Roles ➔Add Roles**
- Tại bảng **Select Server Roles**,chọn **File Services.**



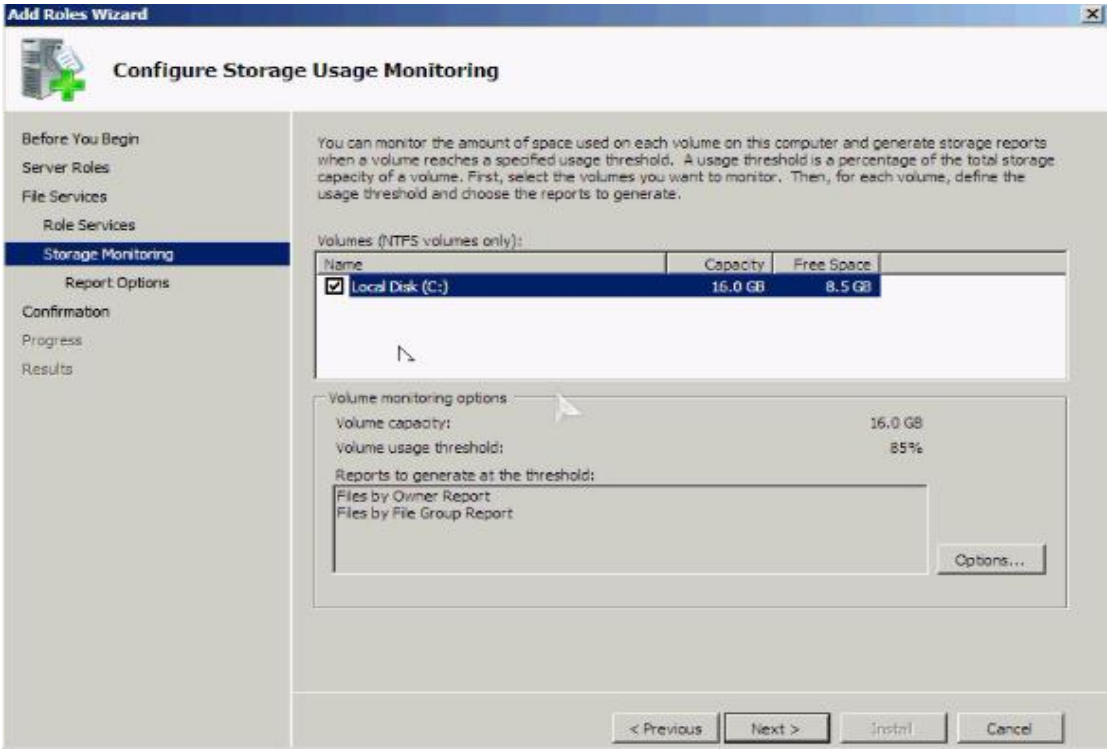
- Chọn **Next**. Tại bảng **File Services** ,xem giới thiệu thông tin về dịch vụ **File Services**



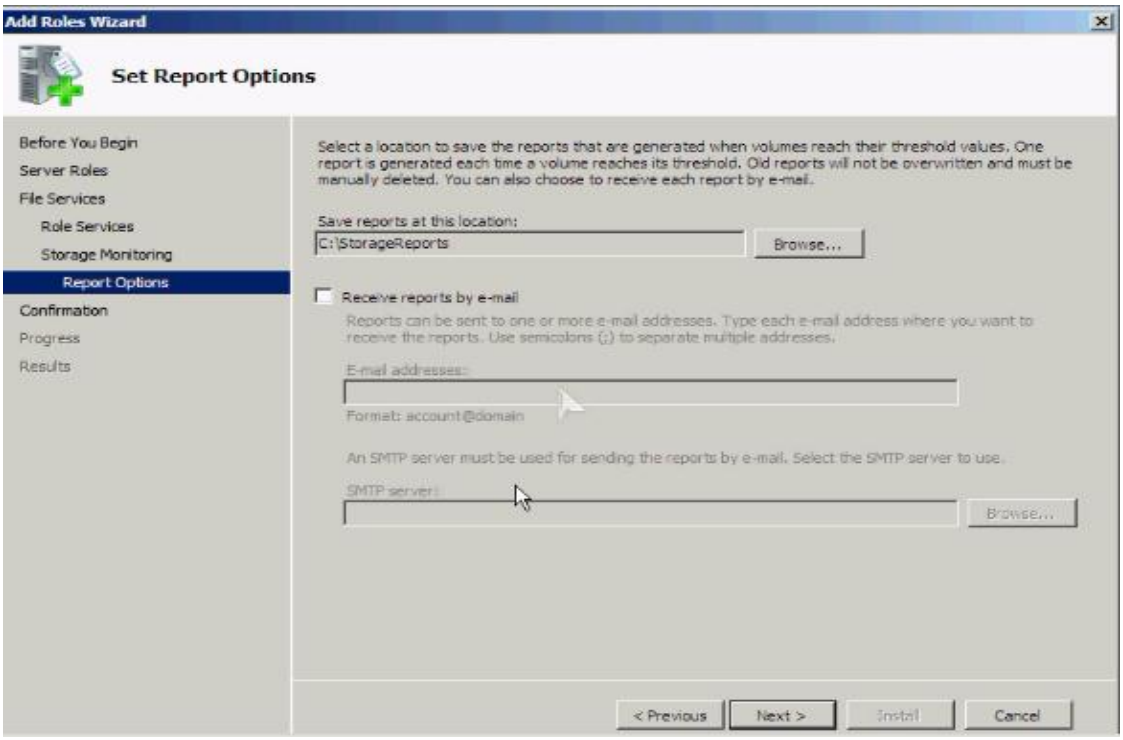
- Chọn **Next**. Tại bảng **Select Role Services** chọn **File Server Resource Manager**.



- Chọn **Next**. Tại bảng **Configure Storage Usage Monitoring** ,chọn ổ đĩa cần theo dõi.



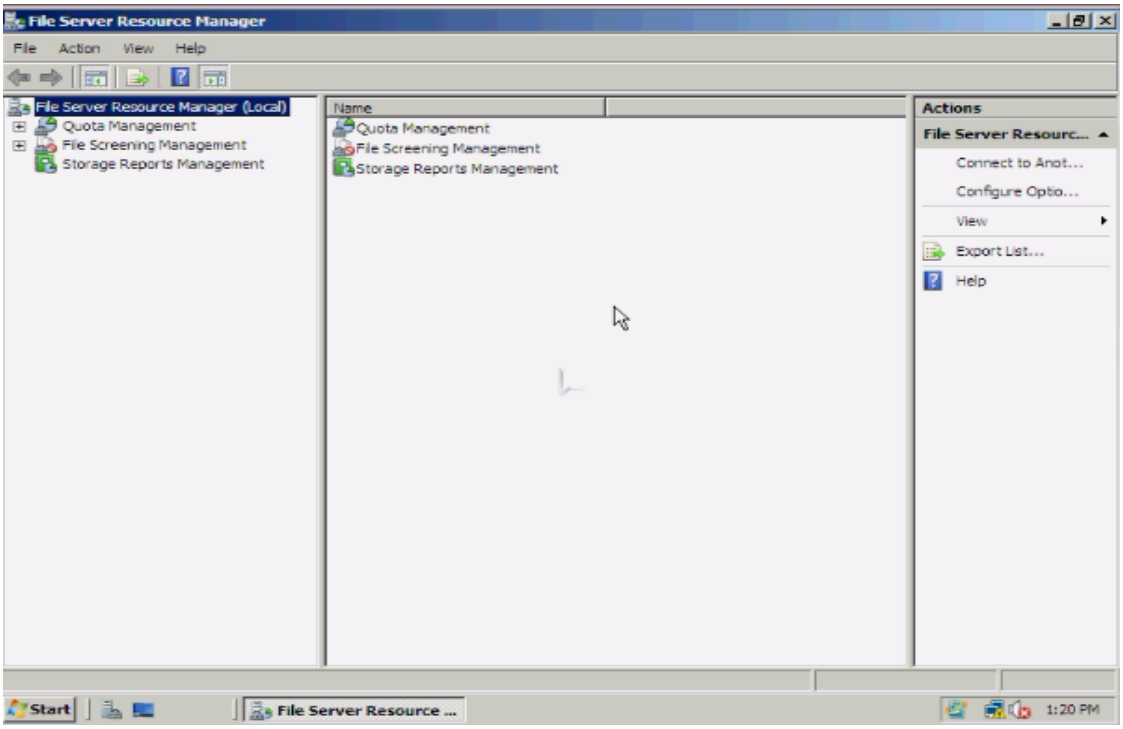
- Chọn **Next**. Tại bảng **Set Report Options**, thay đổi các tùy chọn liên quan đến báo cáo sẽ xuất ra như vị trí lưu trữ báo cáo,gửi báo cáo qua email.



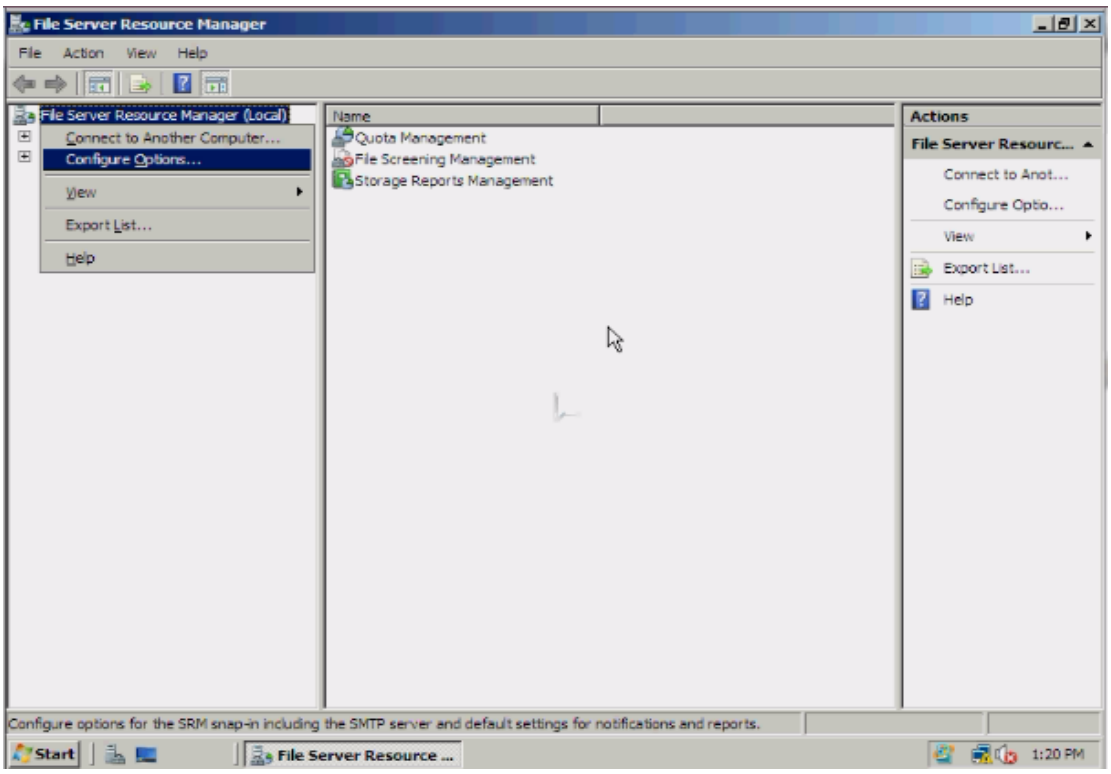
- Chọn **Next**. Tại bảng **Confirm Installation Selections**, xem lại các thiết lập, sau đó chọn **Install**.

- Sau khi cài đặt hoàn tất.Chọn **Close**.

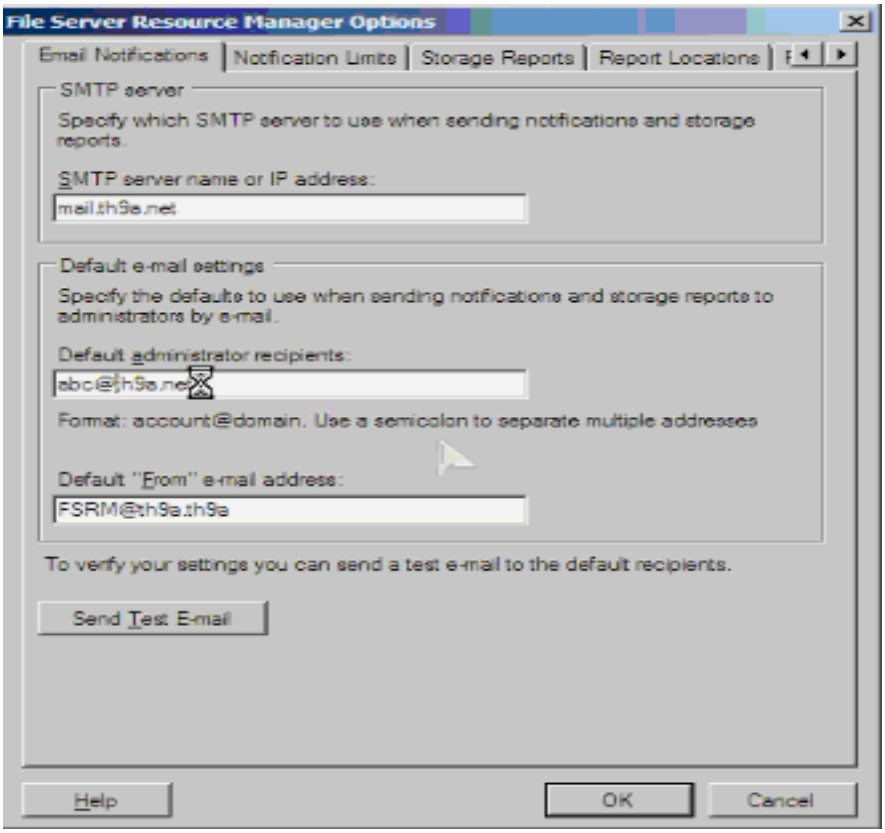
- Để mở **File Server Reource Manager** vào **Start → Administrative Tools → File Server Resource Manager**.



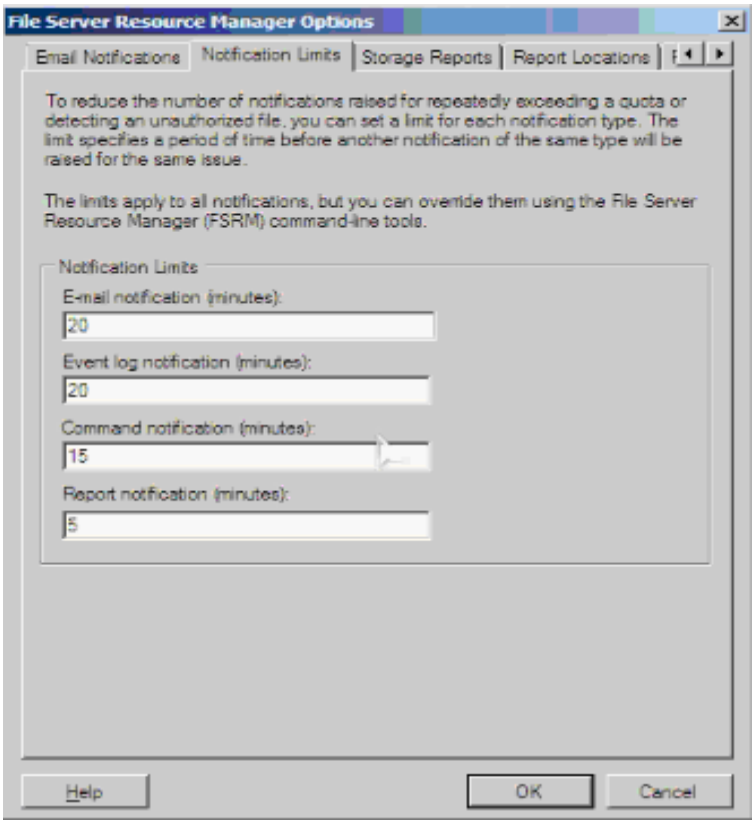
- Tại đây có 3 thành phần chính là **Quota**,**File Screening**,**Storage Report** .Để cấu hình các tùy chọn trên **File Server Resource Manager** nhấp chuột phải vào **File Server Resource Manager** (Local) và chọn **Configure Options**.



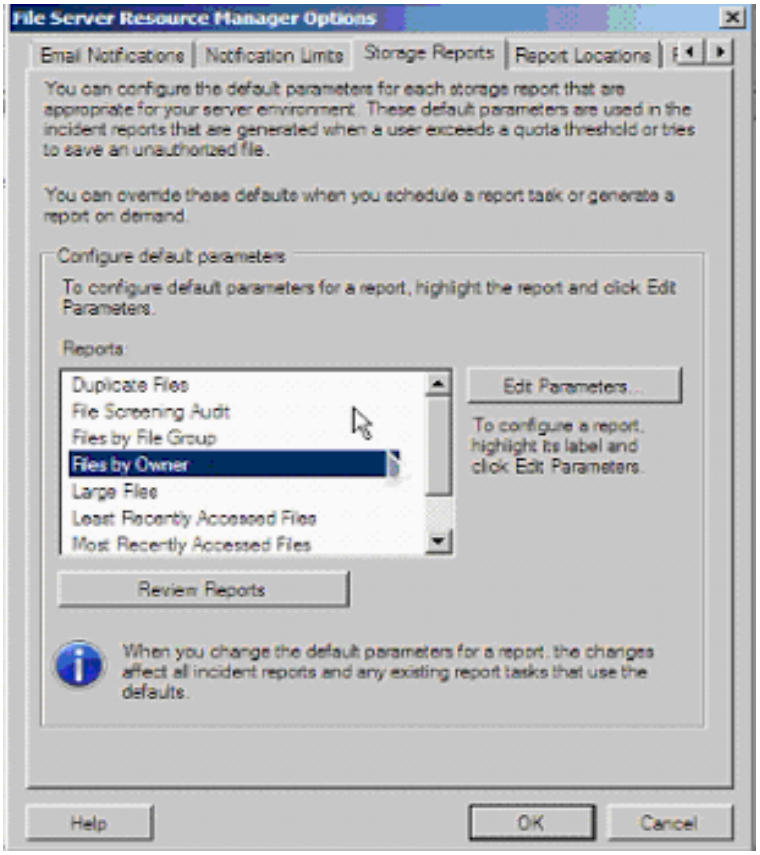
Tại tab **Email Notification**, nhập thông tin về **Mail Server** và địa chỉ email của người nhận để hệ thống gửi thông tin cảnh báo và các báo cáo.



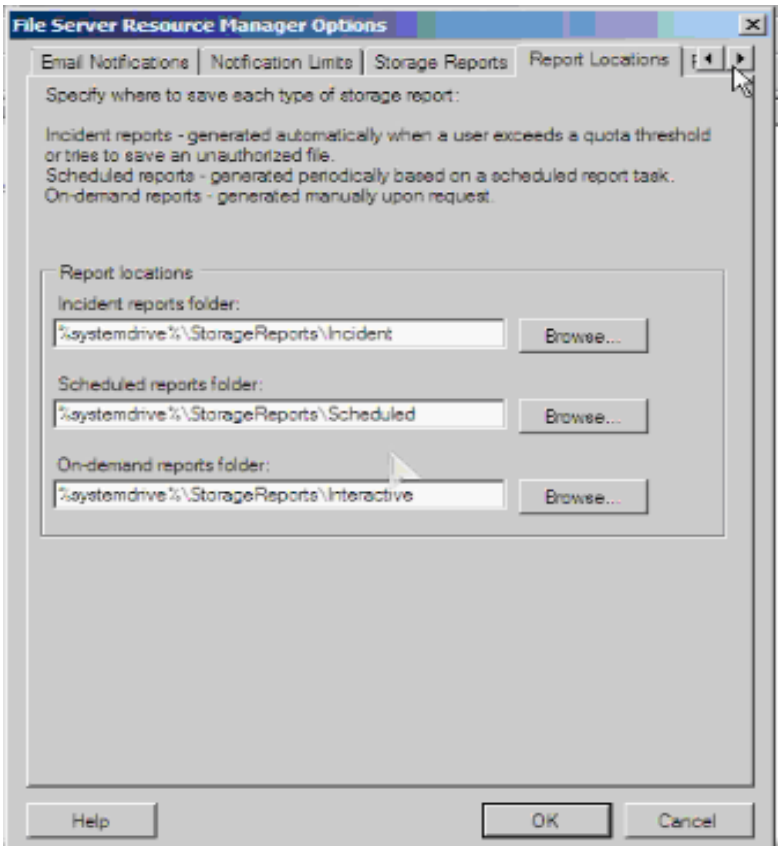
Ở tab **Notification Limits**, bạn có thể giới hạn số lượng thông tin cảnh báo gửi về.



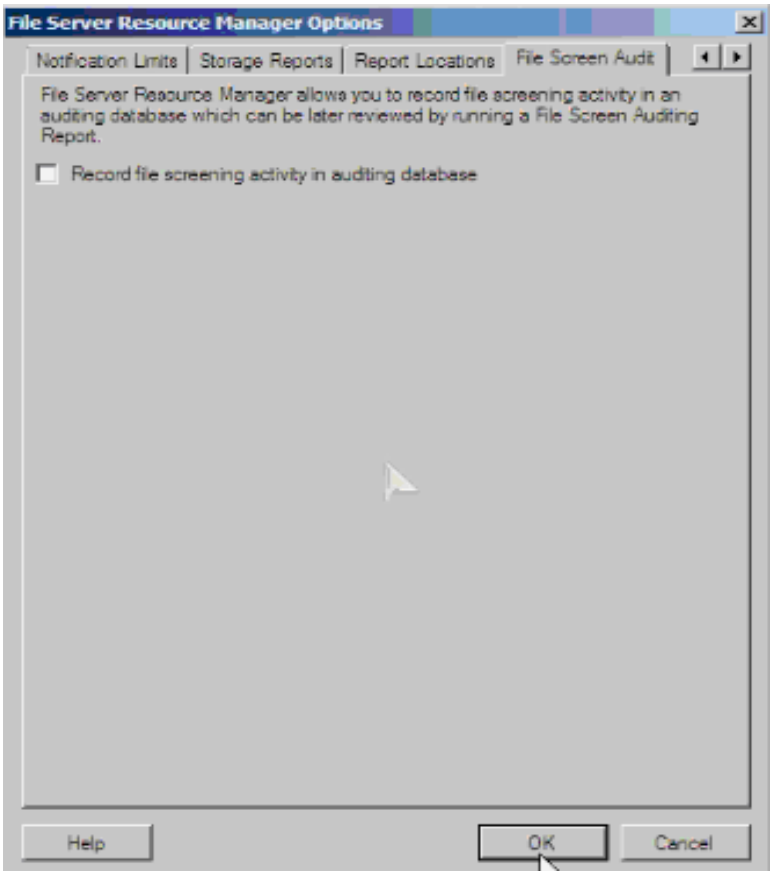
Tại tab **Storage Reports** có thể thiết lập những thông số mặc định trong các báo cáo sẽ xuất ra.Ở mỗi report có thể chỉnh lại bằng cách chọn **Edit Parameters**.



Tại tab **Report Locations** cho phép thiết lập vị trí lưu trữ các báo cáo.



Tại tab **File Screen Audit** cho phép thiết lập bản ghi về file screen trên audit.



Chọn **OK** để hoàn tất các thiết lập.

2. Quản lý File Screen

File Screen là công cụ dùng để ngăn chặn người sử dụng lưu trữ một số file không được phép lên ổ đĩa hoặc thư mục được cấp.

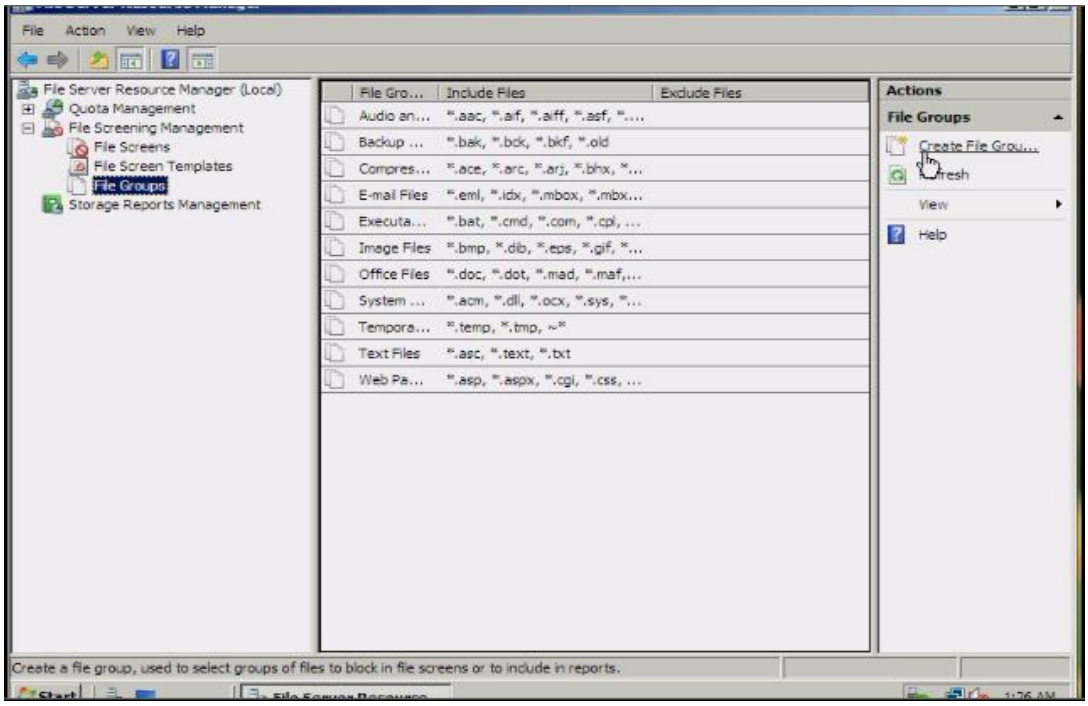
Khi tạo một file screen,có thể chọn một trong 2 hình thức:

- Active Screening : không cho phép người sử dụng lưu trữ các loại file không được phép lên server
- Passive Screening : cho phép người sử dụng lưu trữ các loại file không được phép lên server,đồng thời đưa ra các cảnh báo cần thiết để phục vụ cho mục đích kiểm soát.

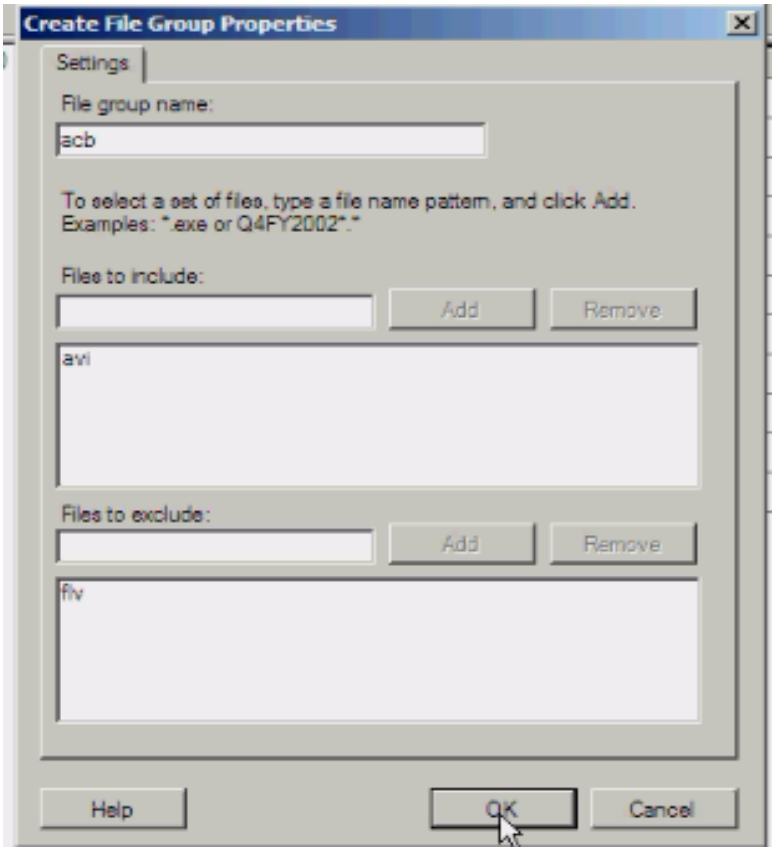
Chú ý : với các file đã tồn tại trong ổ đĩa hoặc thư mục trước khi file screen được tạo ra,người sử dụng hoàn toàn có thể truy cập được,cho dù các file đó thuộc vào danh sách các loại file bị cấm.

❖ **Các bước cài đặt File Screen**

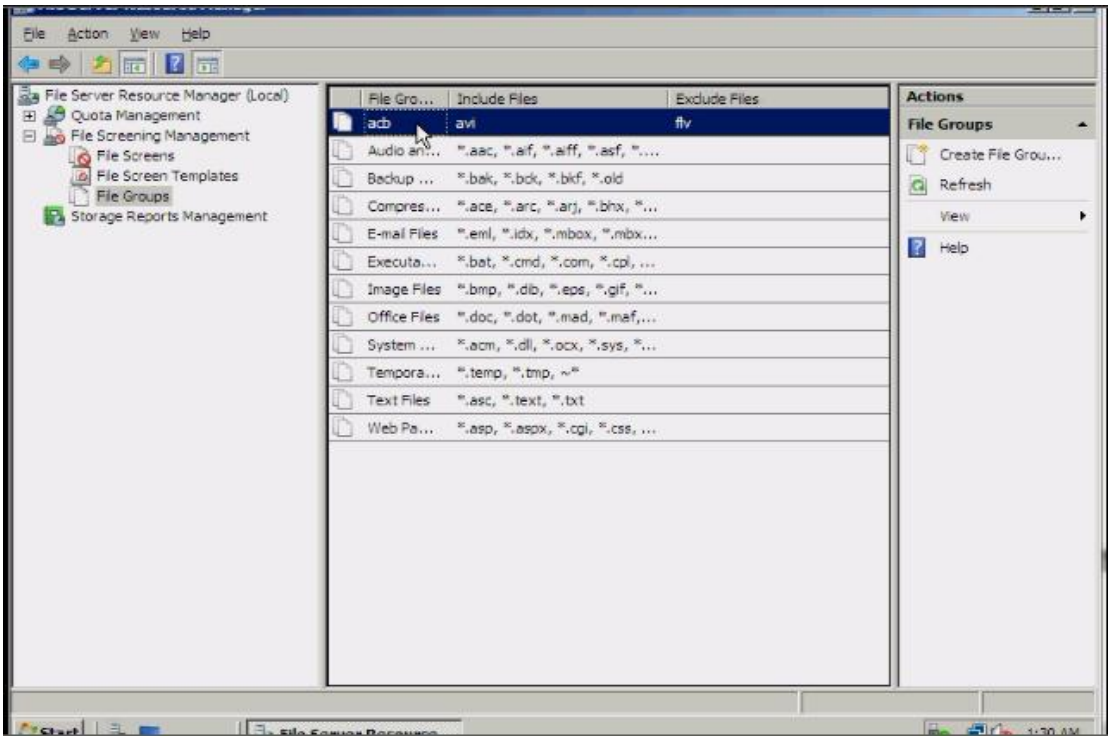
- Để tạo một file group,vào **Start➔Administrative Tools➔File Server Resource Manager** Click vào **File Screening Management** .Nhấp chuột phải vào **File Groups** chọn **Create File Group.**



- Tại bảng Create File Group Properties,nhập tên file của file group vào mục File group name.
- Nhập định dạng file vào và chọn Add,hoặc bỏ thì chọn Remove. File to include : bao gồm các loại file thuộc groupFile to exclude : bao gồm các loại file không thuộc group.



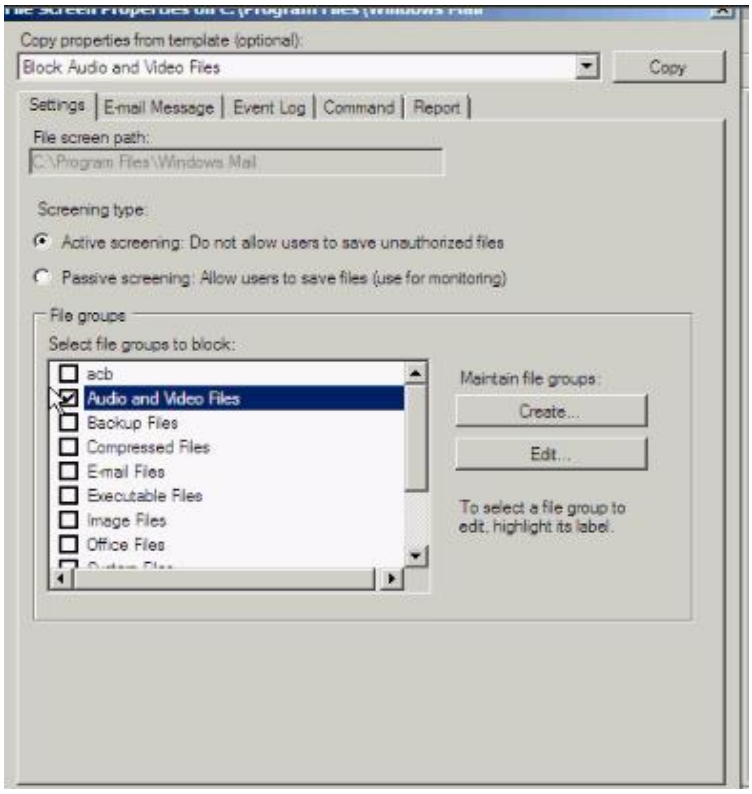
Chọn **OK** để hoàn tất.Lúc này group đã xuất hiện tại bảng



- Để tạo một **file screen**,tại **File Server Resource Manager**.Nhấp chuột phải vào **File Screens** và chọn **Create File Screen**

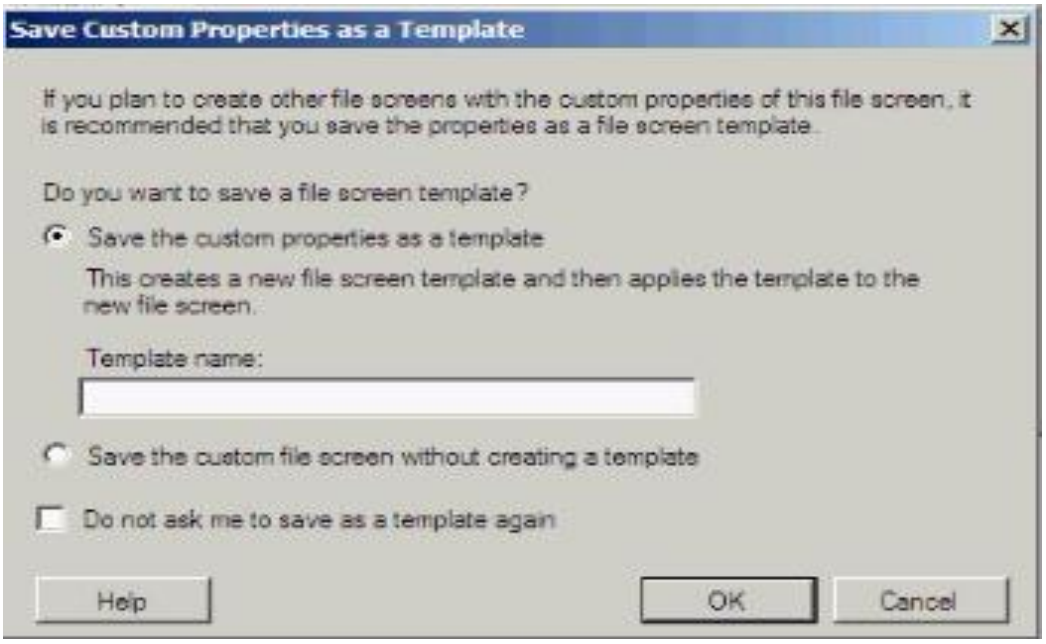
- Tại bảng **Create File Screen**,tại mục **File screen path**,chọn đường dẫn thư mục sẽ áp dụng **file screen**.Ở mục **How do you want to configure file screen properties**,chọn **Derive properties from this file screen template** để sử dụng các template sẵn có trên hệ thống.

- Nếu muốn thiết lập các thuộc tính riêng biệt do mình tự định nghĩa,chọn **Define custom file screen properties**,sau đó click chọn **Custom Properties.**
- Tại bảng **File Screen Properties** ,nếu muốn copy các thuộc tính từ một template trên hệ thống, chọn một template từ danh sách Copy properties from template và chọn **Copy**
- Ở mục **Screening type**,chọn **Active screening hoặc Passive screening**.
- Ở mục **File group**,chọn các file group tương ứng với file screen.

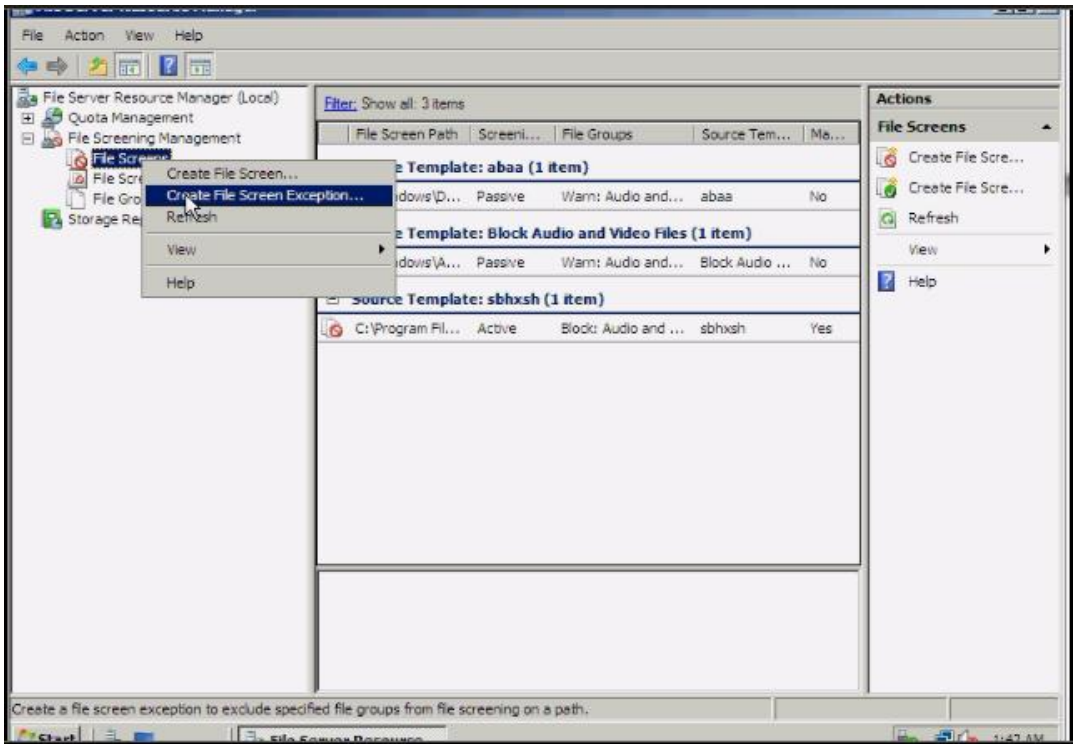


- Sau khi thiết lập xong chọn **OK** .

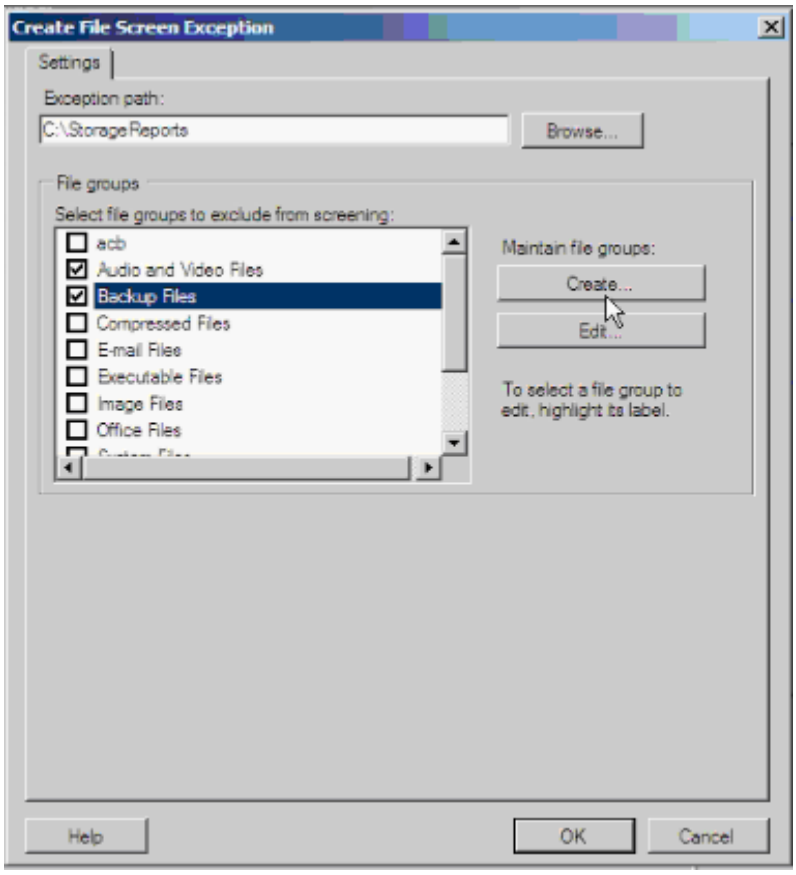
- Sau đó chọn **Create** .Tại bảng **Save Custom Properties as a Template**,đánh dấu chọn **Save the custom properties as a template** và nhập tên template vào mục **Template name➔OK**.



- Để tạo một **file screen exception** ,nhấp chuột phải vào **Files Screen** và chọn **Create File Screen Exception.**



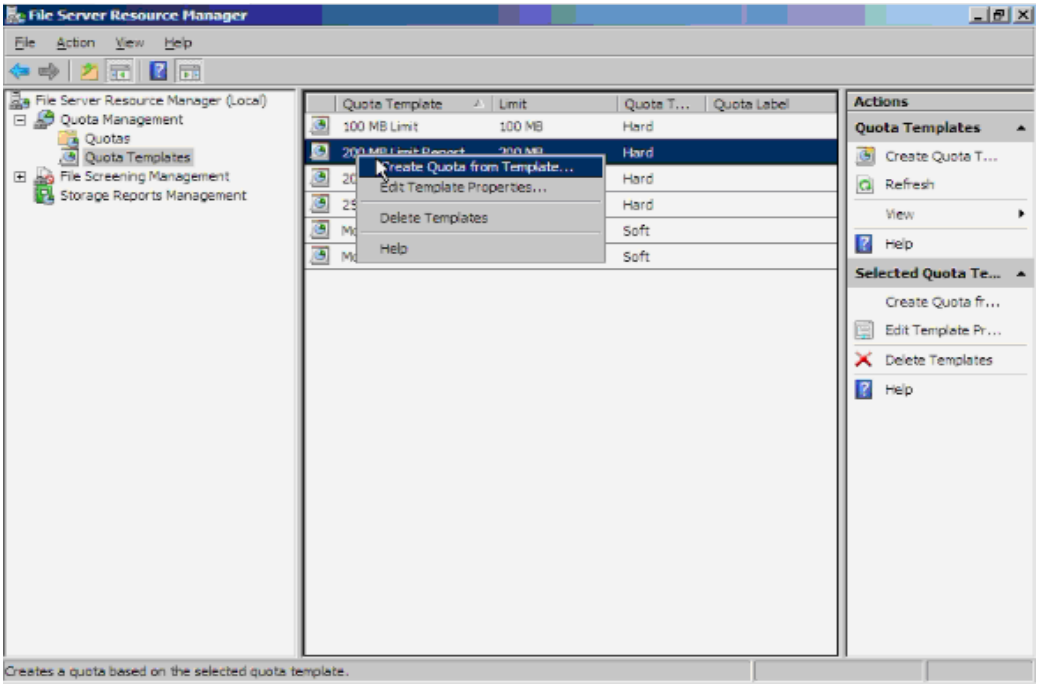
- Tại bảng **Create File Screen Exception**,ở mục **Exception path** ,chọn đường dẫn đến thư mục sẽ áp dụng **file screen exception**. Trong mục **File groups** chọn các file group tương ứng để đưa vào file screen exception



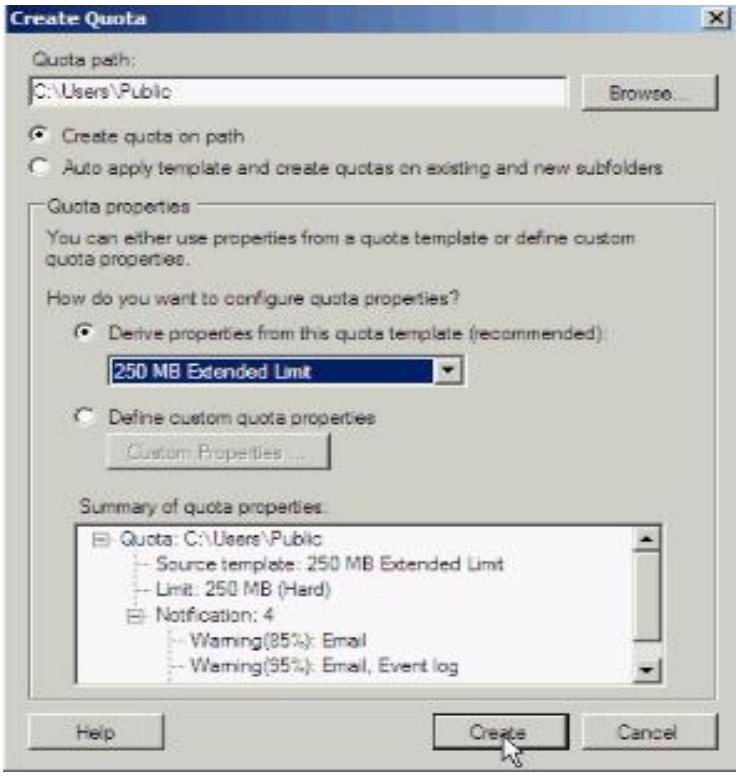
- Chọn **OK** để hoàn tất.

3. Quản lý Quota

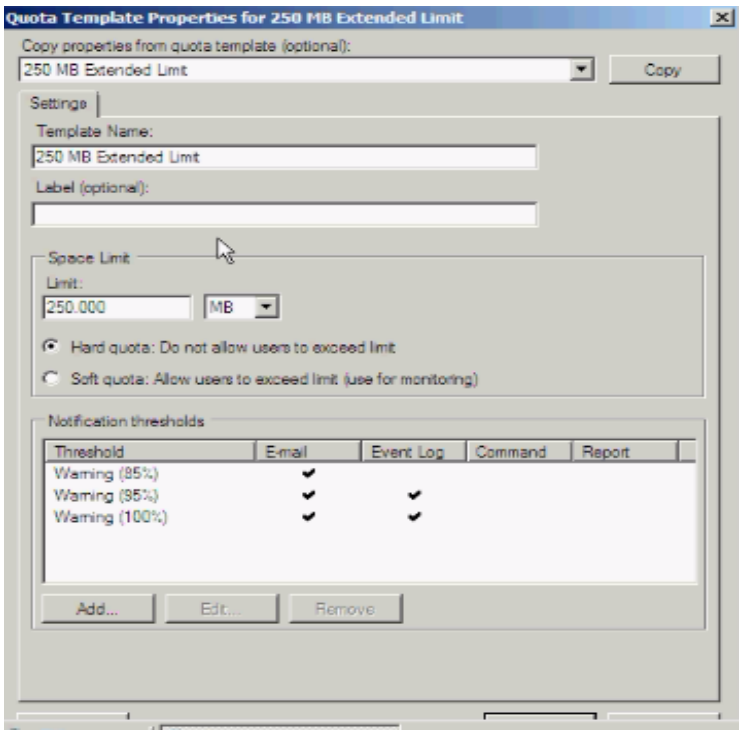
- Để tạo một Quota vào **Start➔Administrative Tools➔File Server Resource Manager**.
- Click vào **Quota Management➔Quota Templates**
- Ở khung giữa,nhấp chuột phải vào một template và chọn **Create Quota from Template**



- Tại bảng **Create Quota**,ở mục **Quota path** chọn đường dẫn đến ổ đĩa hoặc thư mục cần thiết bằng cách click vào **Browse.**
- Đánh dấu chọn vào **Create quota on path**
- Ở mục **Derive properties from this quota template**,chọn một template phù hợp
- Ở mục **Summary of quota properties**,xem lại những thuộc tính của template vừa chọn.

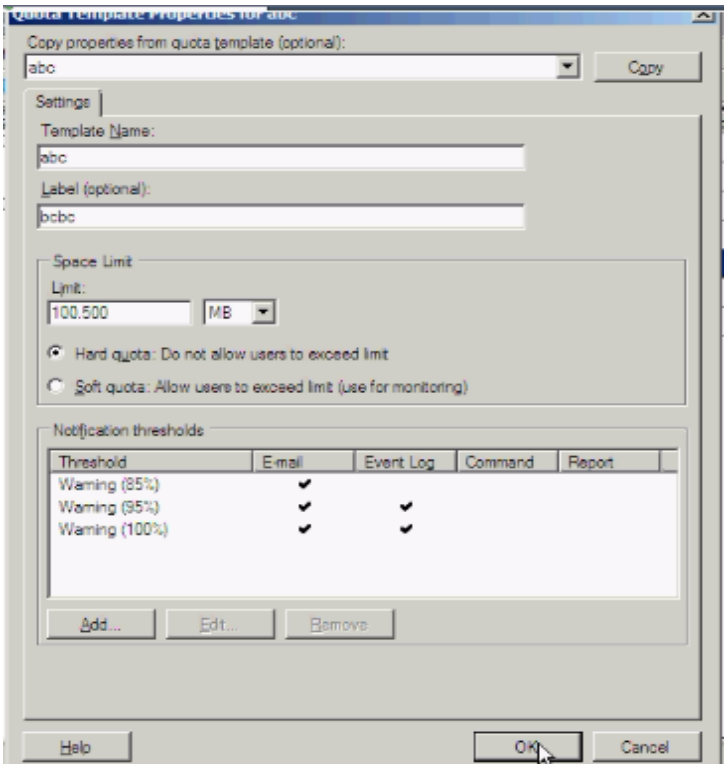


- Chọn Create để tạo một quota mới.Để thay đổi template ,nhấp chuột phải vào một template và chọn Edit Template Properties...Tại đây có thể thay đổi các tùy chọn cho phù hợp với yêu cầu của mình như dung lượng đĩa sẽ cấp quota,hình thức quota là hard quota hay soft quota



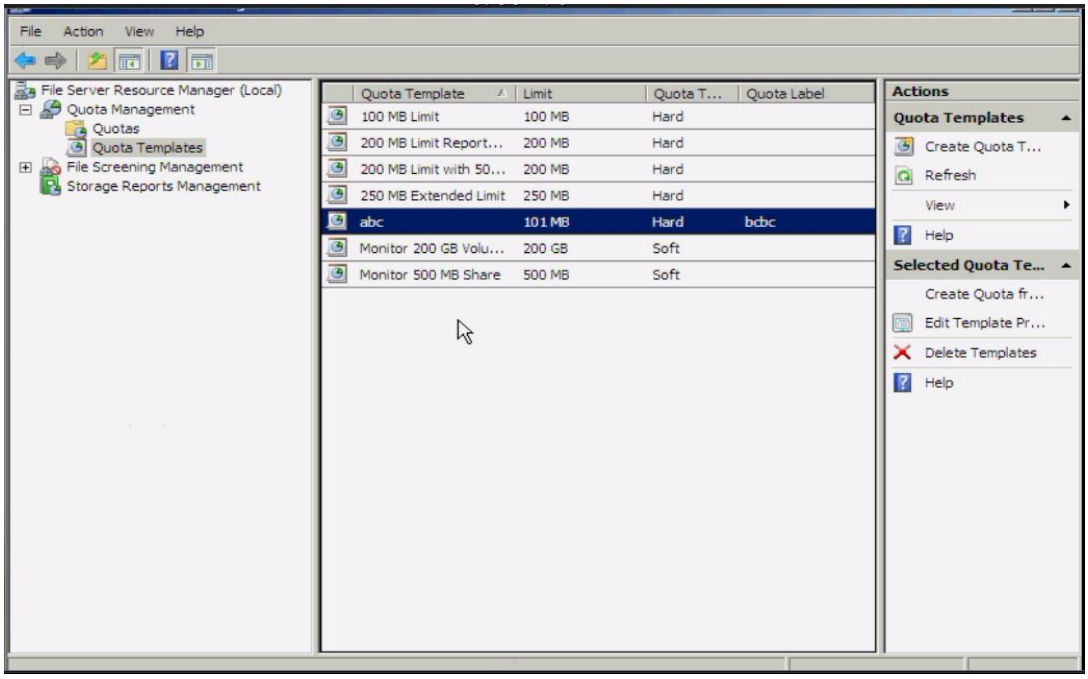
❖ **Tạo một Quota Template**

.- Để tạo một quota template,nhấp chuột phải vào **Quota Templates** và chọn **Create Quota Template**



- Trên bảng Create Quota Template,nếu muốn áp dụng thuộc tính của template đã có vào template của mình chọn một template trong danh sách ở mục **Copy properties from quota template** (optional) và click chọn **Copy**.Nhập tên template vào mục Template Name.Nhập thông tin miêu tả vào mục Label(optional).Ở mục Space Limit,bạn nhập dung lượng cần cấp quota và chọn kiểu hard quota hoặc soft quota.Có thể bổ sung các ngưỡng cảnh báo mới cho template của mình bằng cách

sử dụng chức năng Add ở mục Notification thresholds.Nếu muốn tùy chỉnh,chọn Edit.Sau đó chọn OK để hoàn tất tạo template.



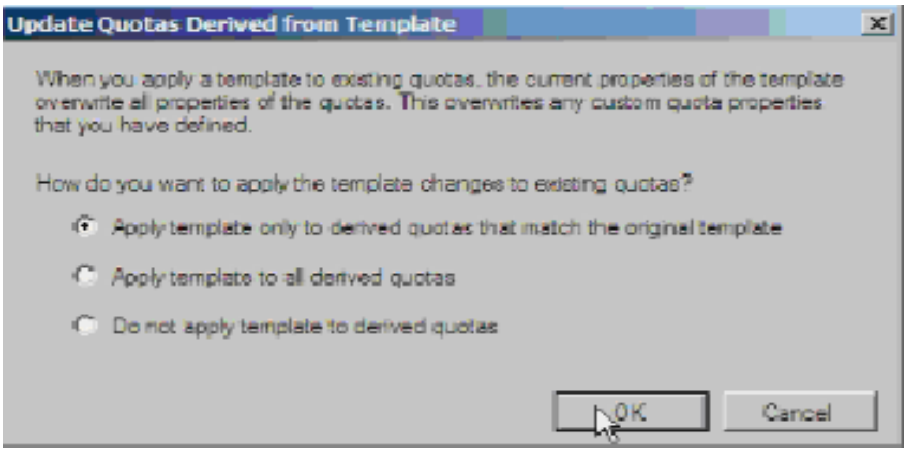
Để tùy chỉnh cho quota template vừa tạo, nhấp chuột phải vào quota template và chọn **Edit Template Properties**..Sau đó thực hiện các thay đổi cần thiết và chọn **OK.**

Tại bảng Update Quotas Derived from Template có 3 sự lựa chọn :

Apply template only to derived quotas that match the original template : cập nhật cho các quota chưa từng được hiệu chỉnh kể từ khi được tạo ra.

Apply template to all derived quotas : cập nhật cho tất cả các quota sử dụng template này

Do not apply template to derived quotas : không muốn thực hiện tao tác cập nhật quota

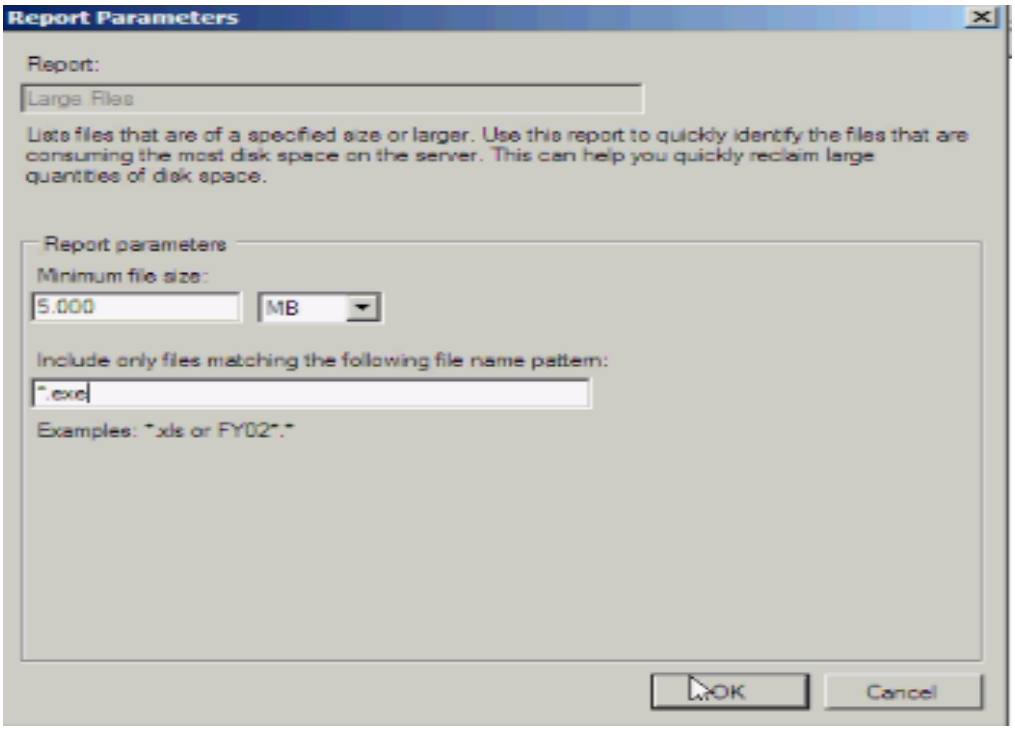


Nhấn **OK** để hoàn tất.

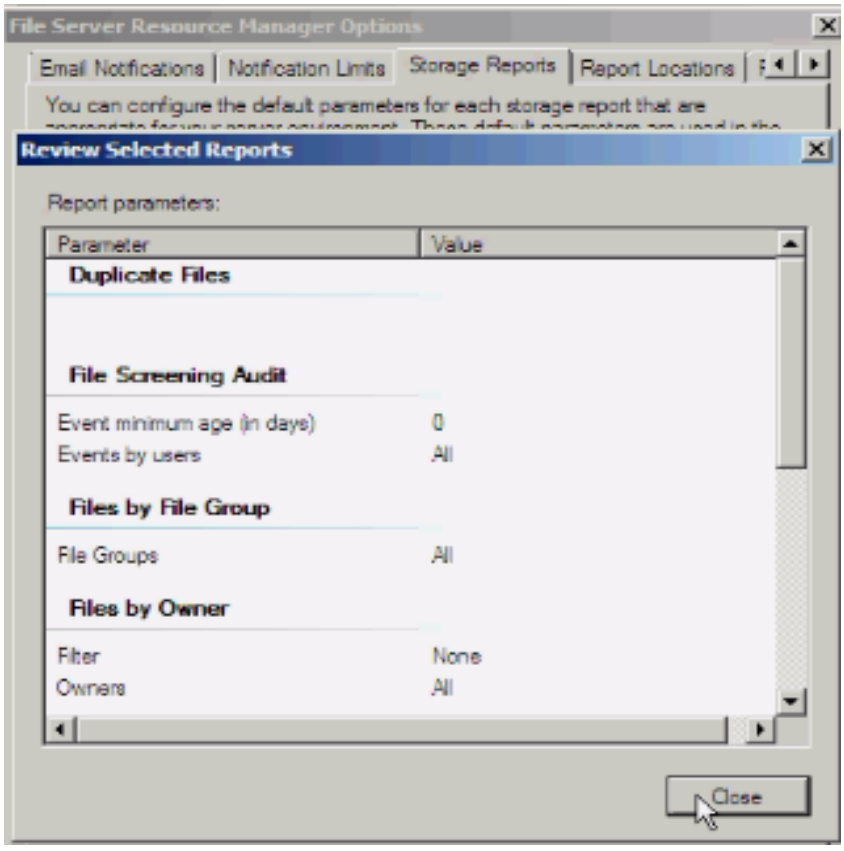
4. Quản lý các báo cáo

- Vào **Start → Administrative Tools → File Server Resoucre Manager**..Righ-click vào **File Server Resource Manager** và chọn **Configure Options**.Ở tab

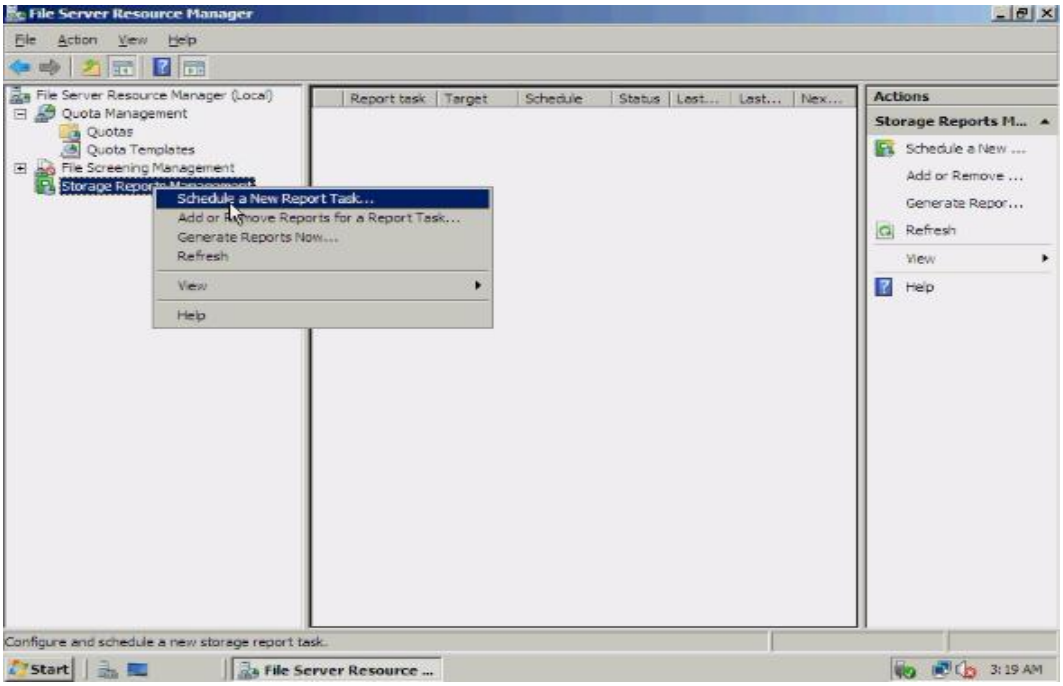
Storage Reports, mục **Configure default parameters**, click chọn loại báo cáo muốn tùy chỉnh và click vào **Edit Parameters**.Sau đó tiến hành thay đổi và chọn **OK.**



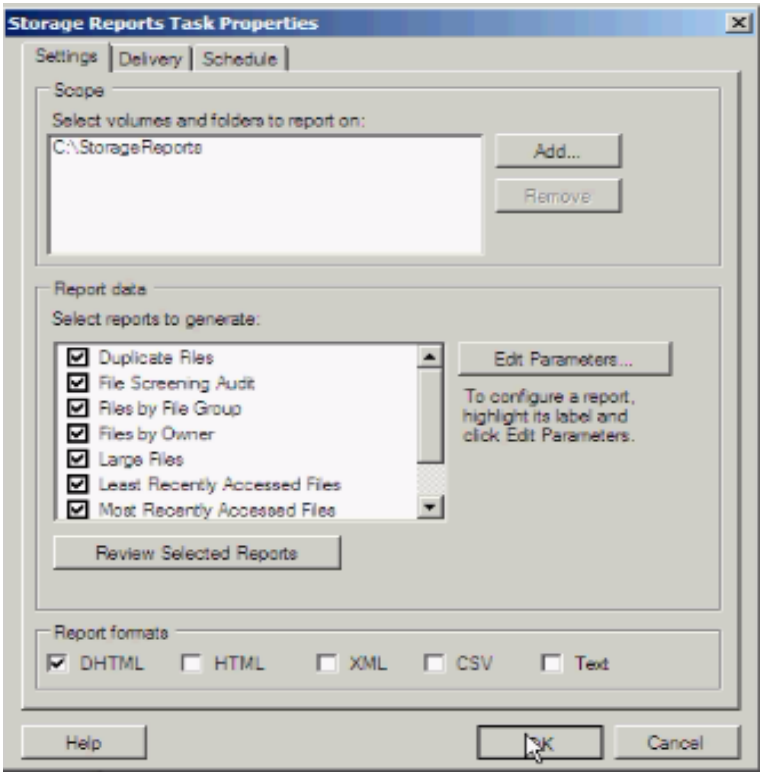
- Để xem lại các thiết lập vừa rồi,click vào **Review Reports**



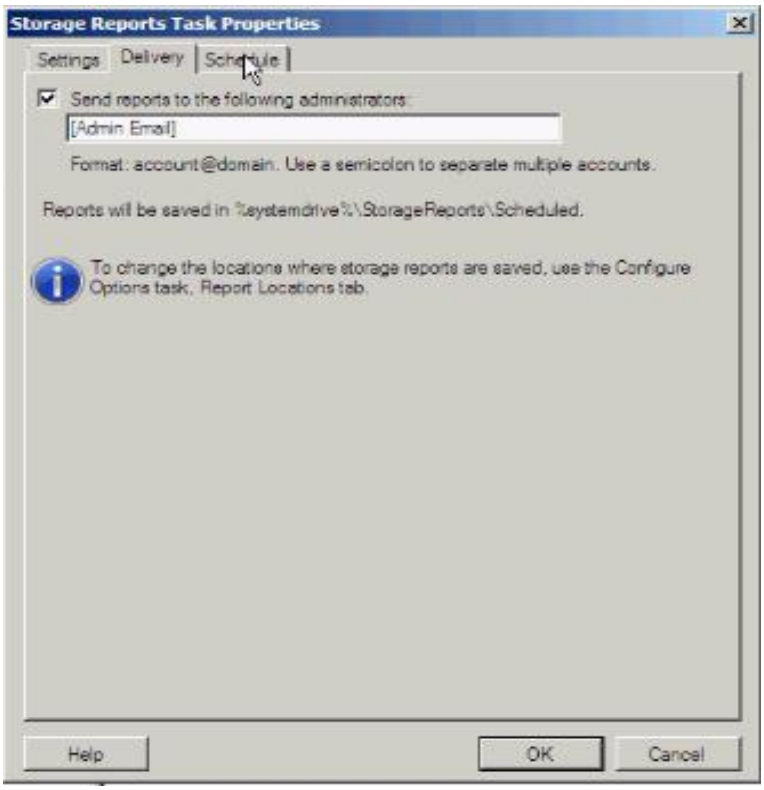
- Sau đó chọn Close và chọn OK để hoàn tất thiết lập.Để lập lịch xuất ra các báo cáo,trong File Server Resource Manager,right-click vào Storage Reports Management và chọn Schedule a New Report Task.



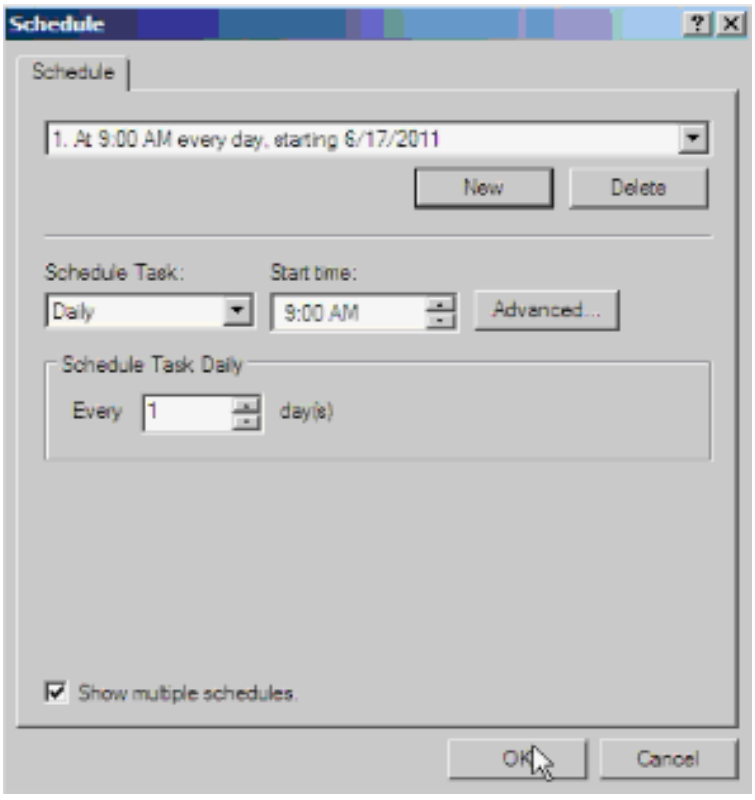
- Tại tab Settings,ở mục Scope,click vào Add để chọn các ổ đĩa hay thư mục cần xuất thông tin báo cáo.Ở mục Report data,chọn các loại báo cáo tương ứng.Với mỗi loại ,bạn có thể sử dụng chức năng Edit Parameters để tùy chỉnh các tham số khi cần.Ở mục Report formats,chọn các định dạng lưu trữ báo cáo,mặc định là Dynamic HTML (DHTML).



- Để gửi báo cáo qua email,mở tab Delivery,đánh dấu chọn vào Send reports to the following administrators và nhập địa chỉ email của người nhận.



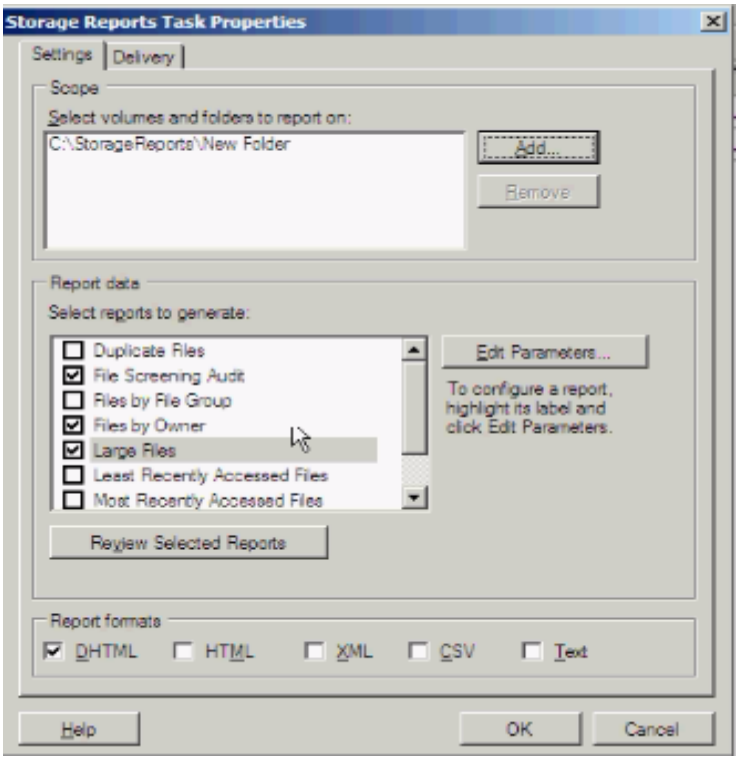
- Ở tab **Schedule**,click vào Create Schedule để lập lịch.Tại bảng Schedule ,click vào New.Sau đó chọn thời gian,nếu muốn thiết lập mở rộng thì click chọn Advance.



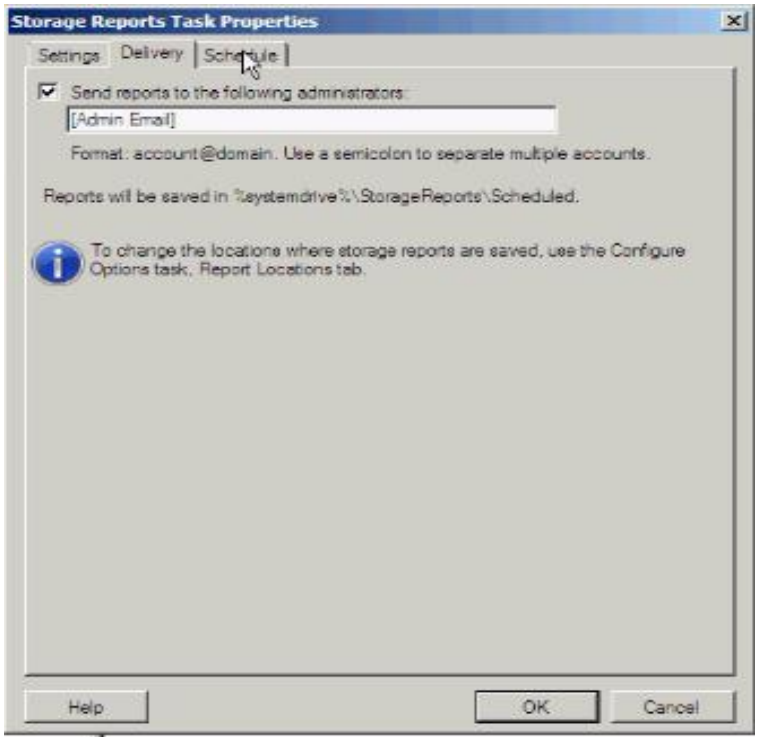
- Chọn **OK** để hoàn tất .

- Sau khi đã thiết lập báo cáo,giờ chúng ta sẽ xuất ra các báo cáo theo nhu cầu.Chuột phải vào Storage Reports Management và chọn Generate Reports Now .Ở tab Settings,tại mục Scope,click vào Add và chọn các ổ đĩa hay thư mục cần xuất thông tin báo cáo.Ở mục Report data,chọn loại báo cáo tương ứng.Với mỗi loại, có

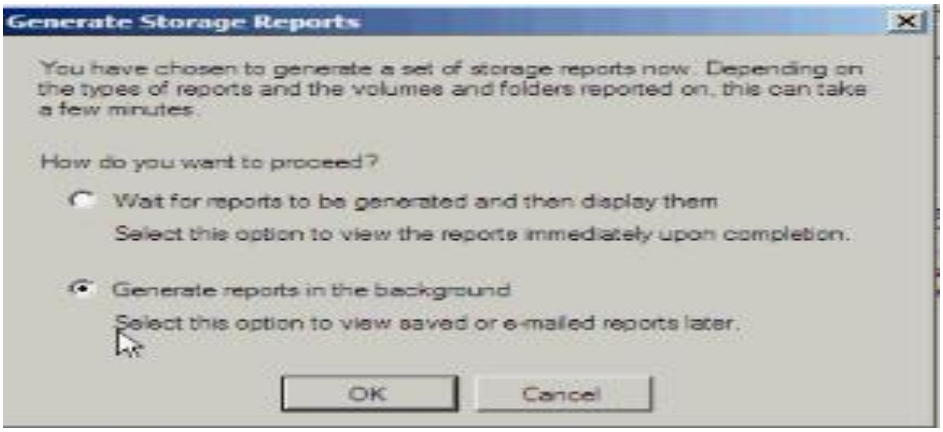
thể sử dụng chức năng Edit Parameters để tùy chỉnh các tham số khi cần.Ở mục Report formats,chọn các định dạng lưu trữ báo cáo.



- Tại tab Delivery,đánh dấu chọn mục **Send reports to the following administrator** và nhập địa chỉ email của người nhận



Sau đó chọn OK.Tại bảng Generate Storage Reports,chọn Generate reports in the background để lưu các báo cáo và xem tại thư mục lưu trữ chúng.



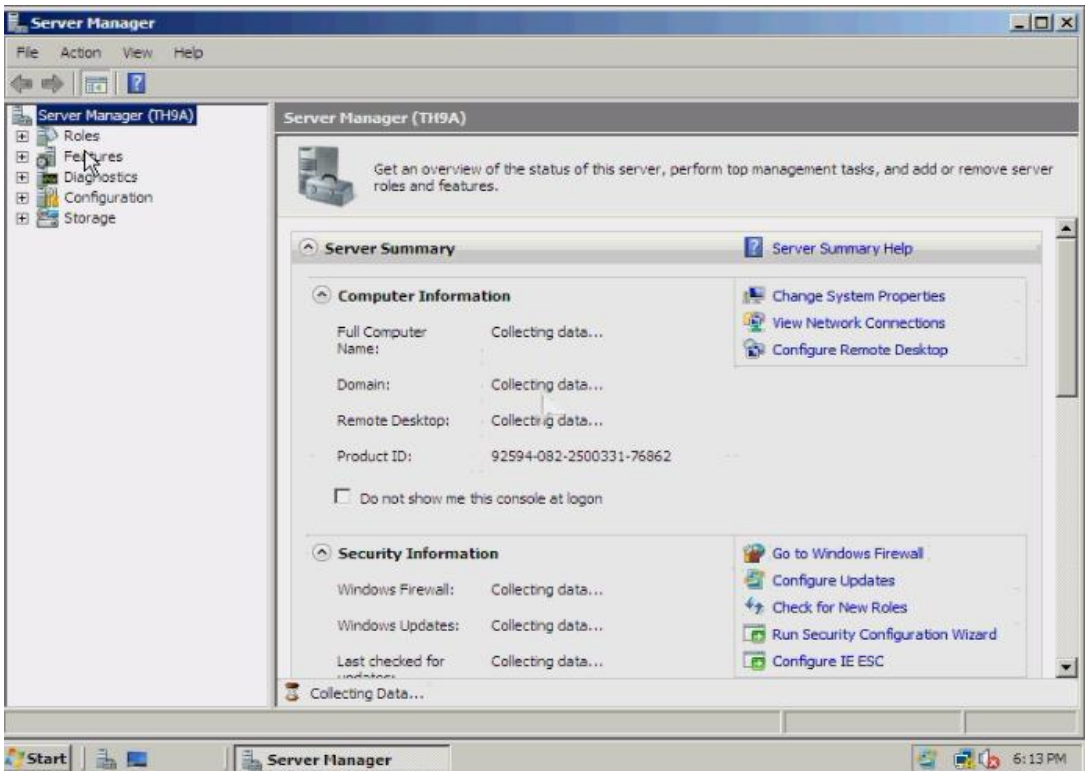
Chọn **OK** để hoàn tất

V. DỊCH VỤ IN ẤN (Print Services)

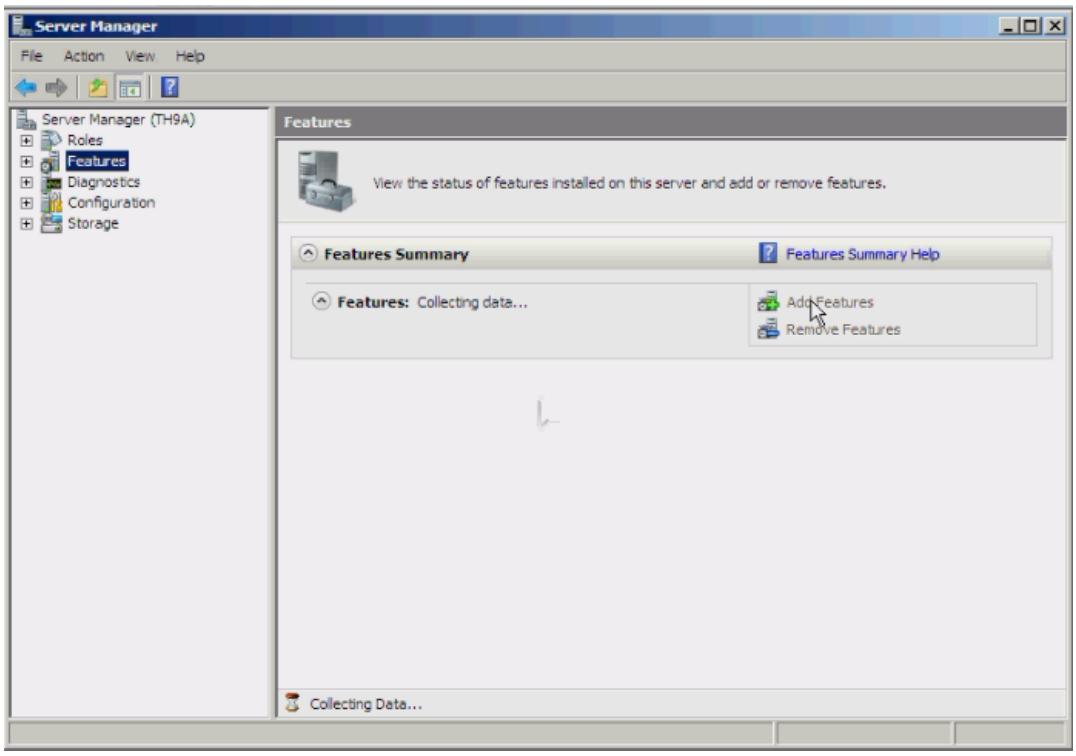
1. Cài đặt

Print Services Tools không được cài đặt mặc định, vì vậy để sử dụng nó cần phải cài đặt thành phần này trước.

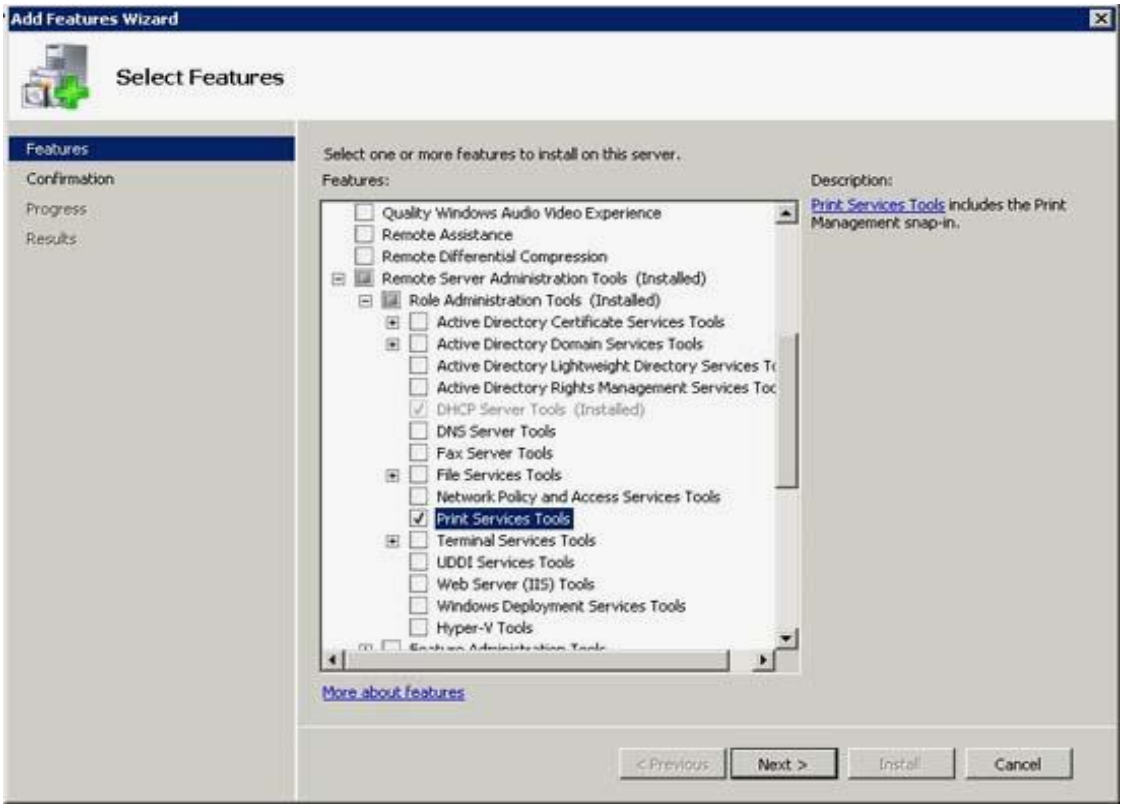
- Chuột phải **My Computer** ➔**Server Manager** ➔Chọn **Features**



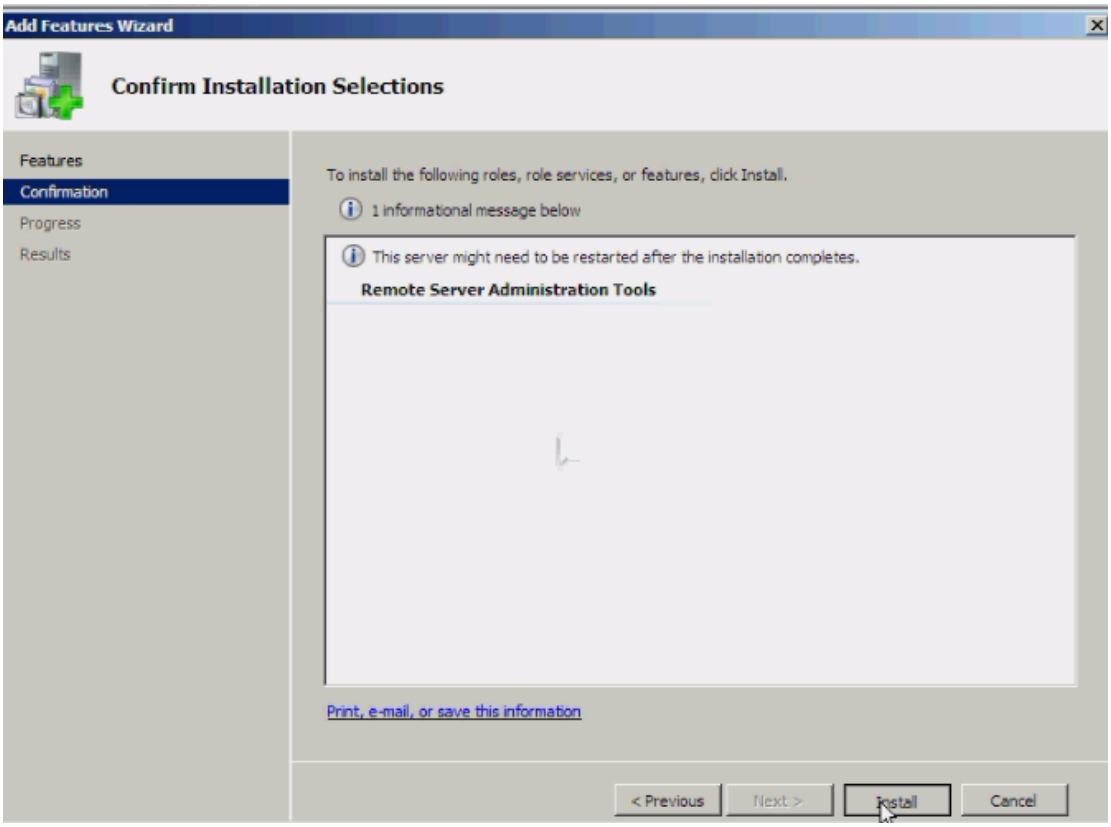
- Chọn **Add Features**.



- Trong mục **Add Features Wizard** ➔ Chọn **Print Services Tools**➔Click **Next.**

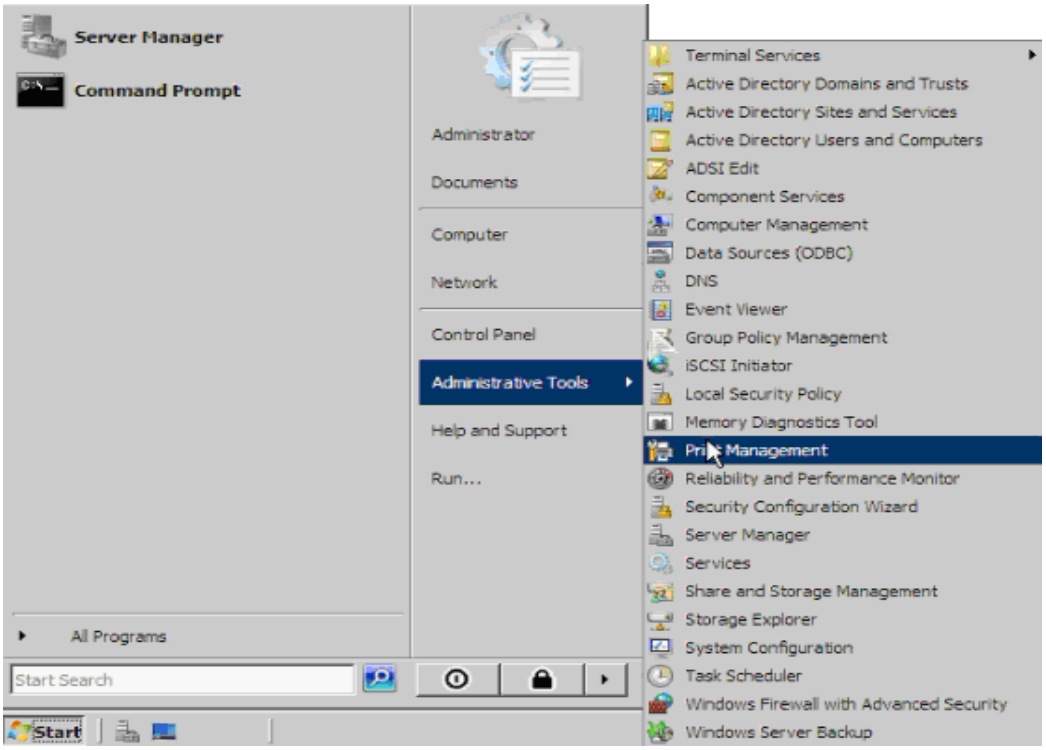


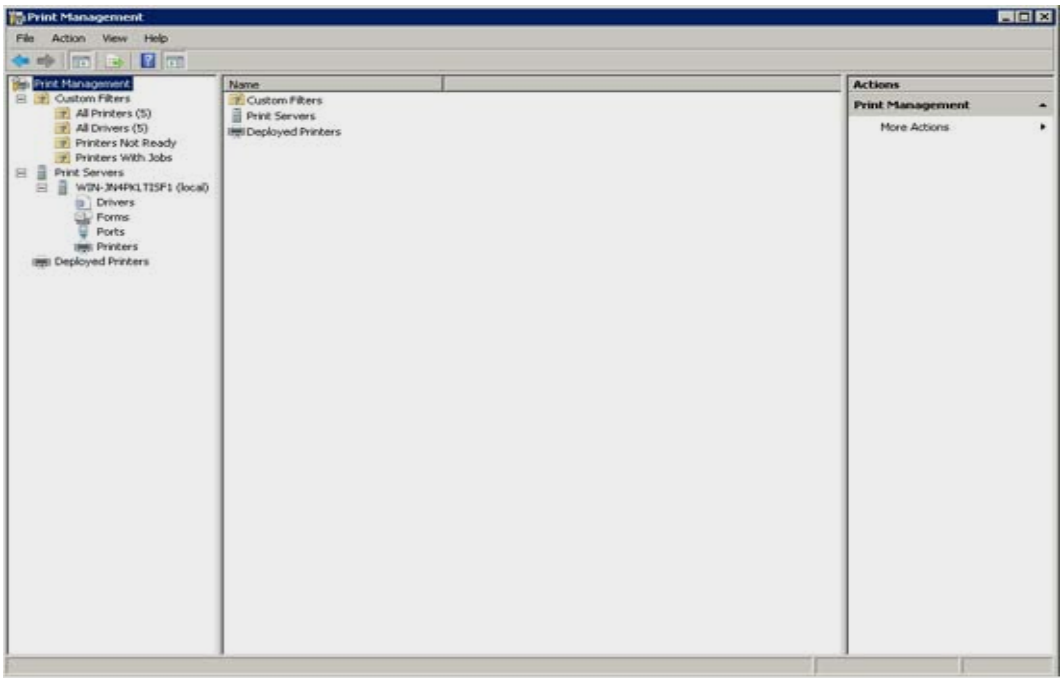
- Tiếp tục nhấn **Install** để cài đặt.Và sau có nhấn **Close** để hoàn tất việc cài đặt.



2. Truy cập Print Sevices Tools

Chọn **Start ➔Administrative Tools ➔Print Management**





3. Quản lý các máy in trong mạng

Đầu tiên Windows đã đặt các mục All Printers và All Drivers một cách tự động trong trường hợp này. Bên cạnh đó máy chủ mà chúng ta đã cài đặt giao diện Print Management là thành viên của miền Active Directory. Một điểm nữa là tên máy chủ tương ứng với mỗi máy in. Mặc dù các máy in mạng nằm ở một điểm nào đó trong mạng nhưng Windows sẽ tự động tạo một hàng đợi cho mỗi máy in trên máy chủ. Một trong các chức năng chính của giao diện quản lý Print Management là cho phép quản lý in ấn mạng tập trung.

VI. DỊCH VỤ WEB

1. Giới thiệu về IIS 7.0

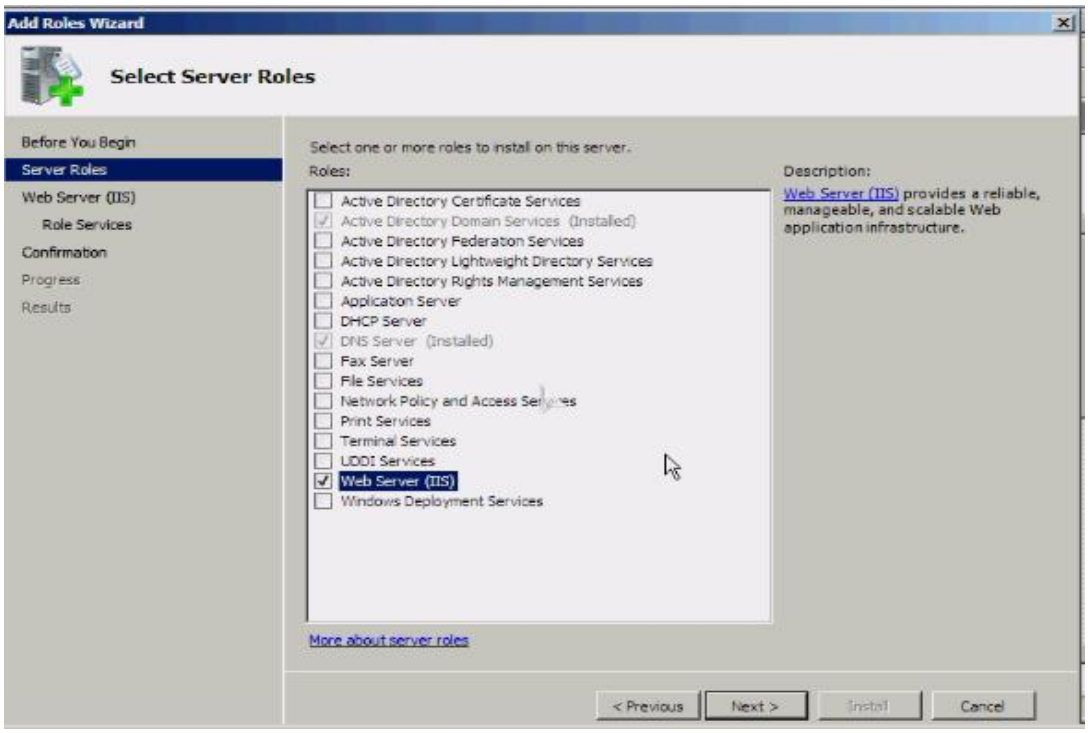
IIS7 được thiết kế để trở thành một nền tảng Web và ứng dụng linh động và an toàn nhất cho Microsoft. Microsoft đã thiết kế lại IIS từ những nền tảng đã có trước đó. IIS có các tính năng

- Bảo mật
- Khả năng mở rộng
- Cấu hình và triển khai
- Quản trị và chuẩn đoán
- Hiệu suất

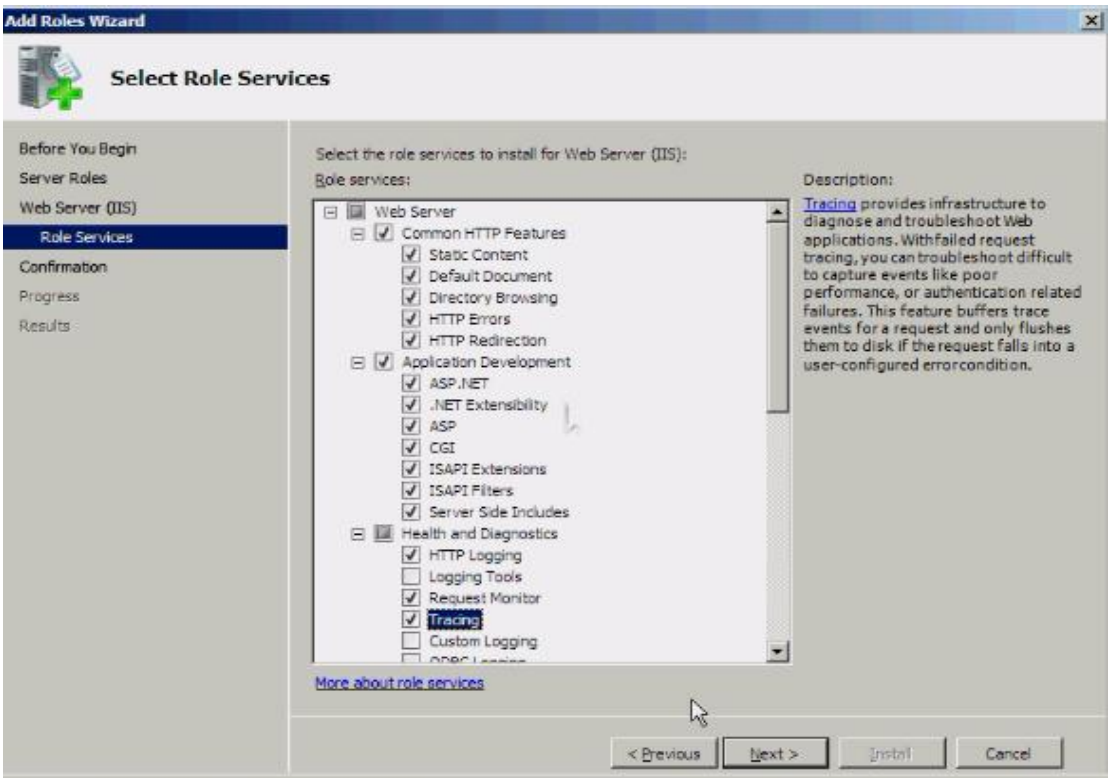
2. Cài đặt IIS 7.0

- Để cài đặt IIS7.0 nhập phải chuột **Computer** chọn **Manage.**Chọn **Roles** trong **Server Manager** sau đó click chọn **Add roles**.

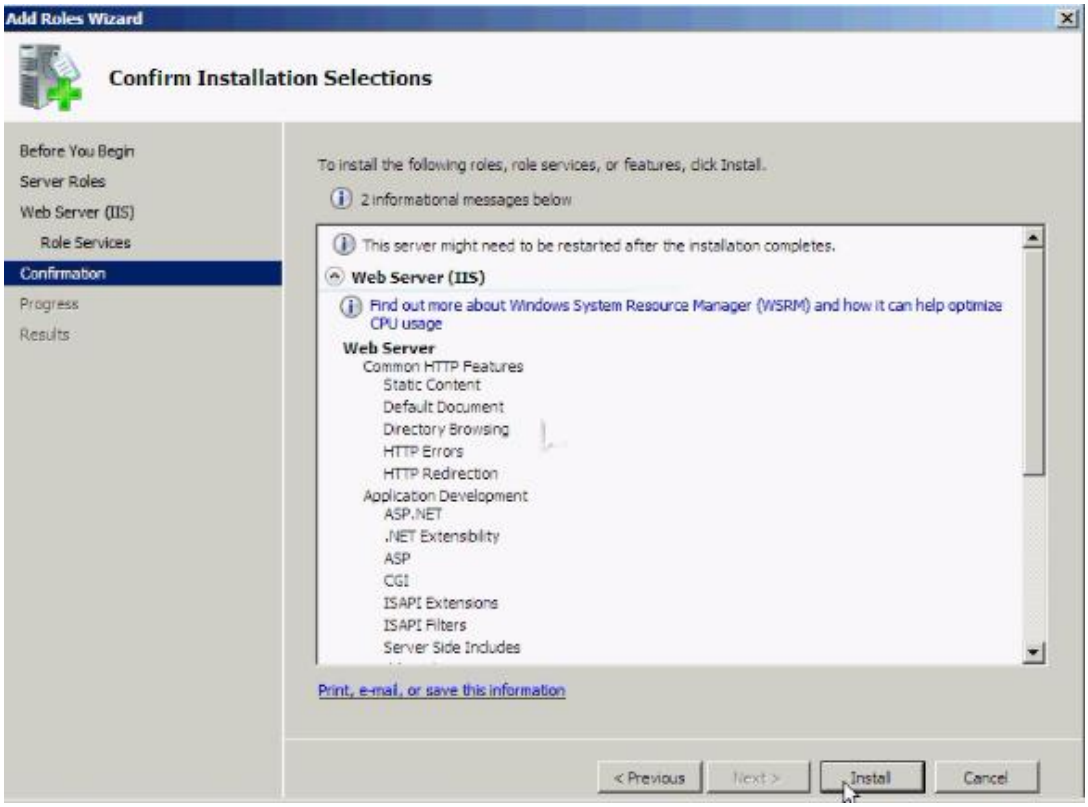
- Chọn **Web Server (IIS)** trong màn hình **Select Server Roles.**



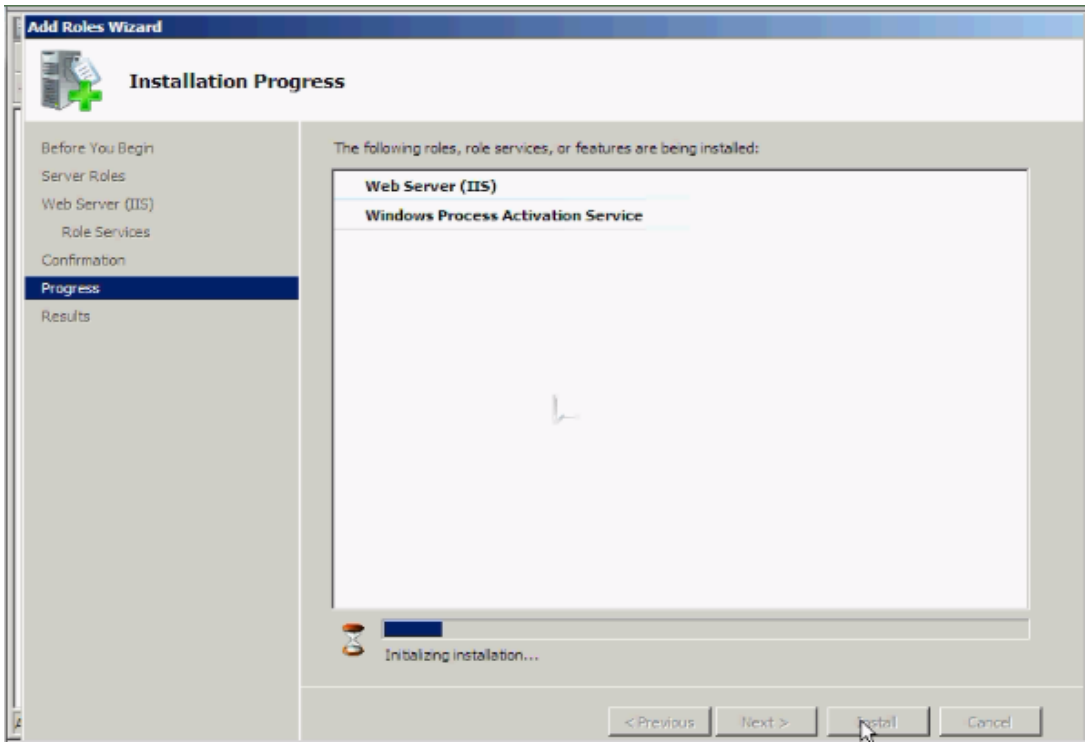
- Windows sẽ bật màn hình **Add Roles Wizard** nhấp chọn **Add Required Features.**Chọn các dịch vụ cần thiết cho **Server** .



- Nhấn **Install** để bắt đầu cài đặt.



Quá trình cài đặt bắt đầu.



- Sau khi cài đặt hoàn tất sẽ thấy trong **Administrative Tools** xuất hiện đến 2 dịch vụ IIS đó là **IIS6** và **IIS7**.

VII. DỊCH VỤ FTP.

1. Giới thiệu về FTP.

- FTP là chữ viết tắc của File Transfer Protocol - Giao thức truyền file. FTP là một giao thức truyền file trên mạng dựa trên chuẩn TCP nên đáng tin cậy.Giao thức truyền tải file - FTP là công cụ quản lý files giữa các máy. FTP cho phép truyền và tải files, quản lý thư mục, và lấy mail. FTP không được thiết kế để truy nhập và thi hành files, nhưng nó là công cụ tuyệt vời để truyền tải files.Windows Server 2008 hỗ trợ 2 version FTP servers là FTP 6.0 và FTP 7.5 . Ở version FTP 7.5 được hỗ tăng cường tính bảo mật và công cụ cho nhà quản trị dễ quản lý.

Những điểm mới :

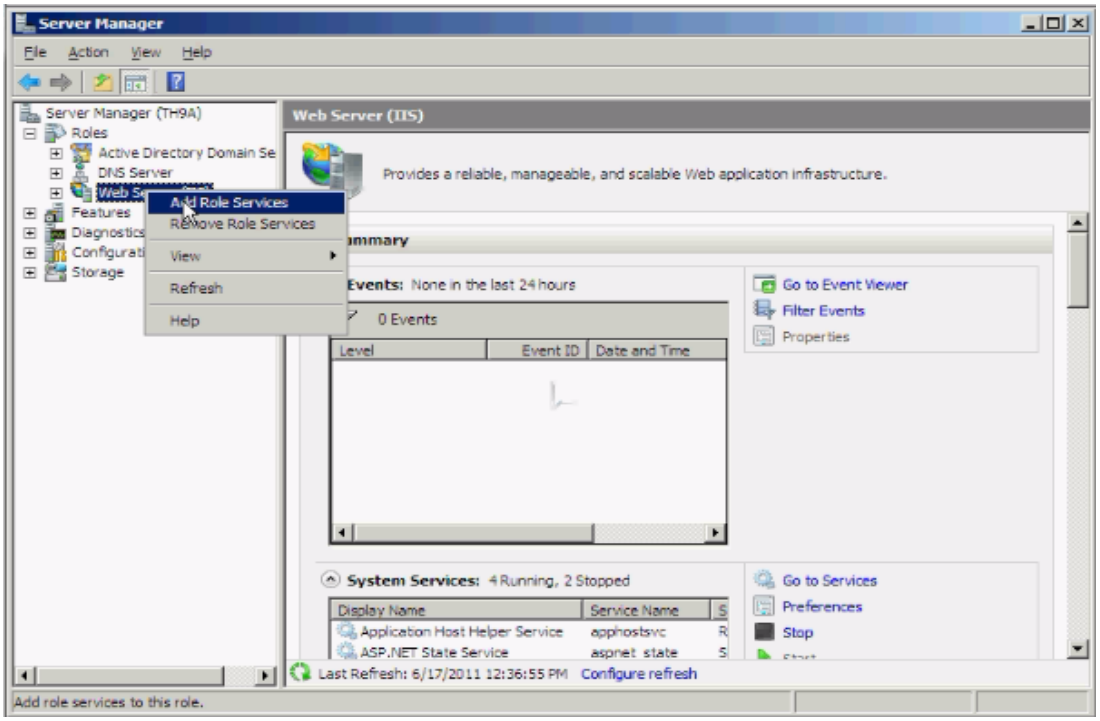
FTP Publishing Server mới gồm có rất nhiều tính năng và các cải thiện.

- Sự tích hợp với IIS 7.0
    - Hỗ trợ cho các chuẩn Internet mới
    - Chia sẻ hosting
    - Khả năng mở rộng
    - Logging
    - Các tính năng khắc phục sự cố

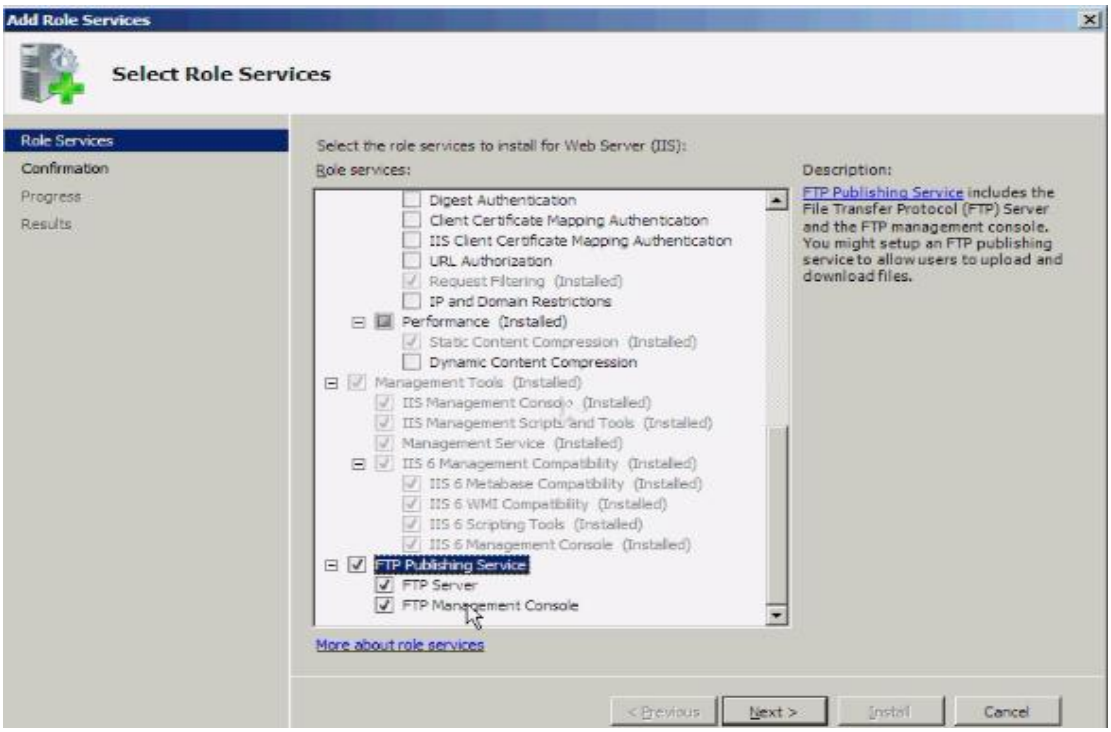
2. Cài đặt và cấu hình.

2.1. Cài đặt.

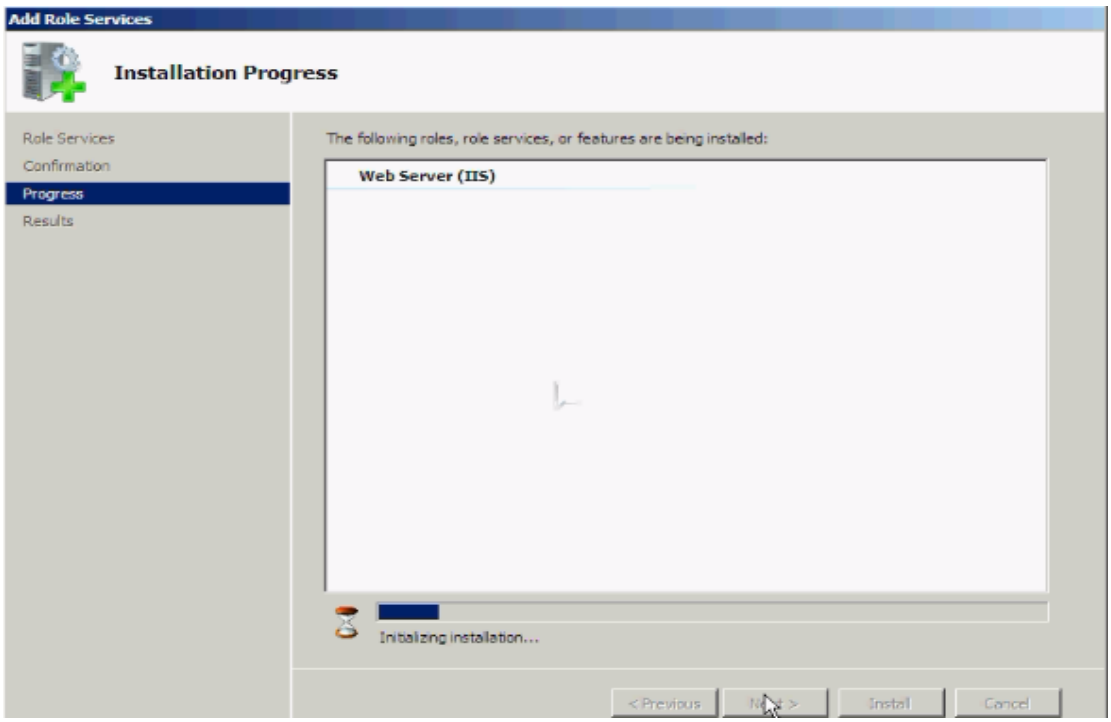
- Vào Server Manager ➔ Roles ➔ Web Server(IIS)➔phải chuột chọn Add Role Services.



- Click chọn **FTP Publishing Service**.



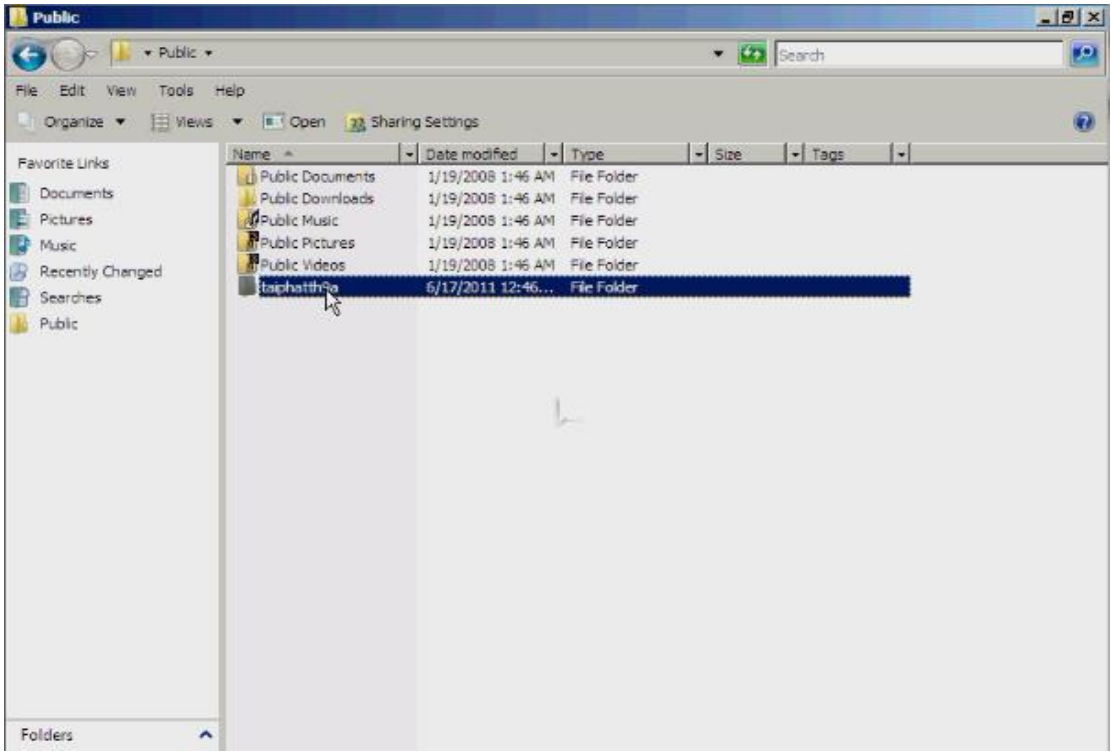
- Click **Install** để cài đặt.



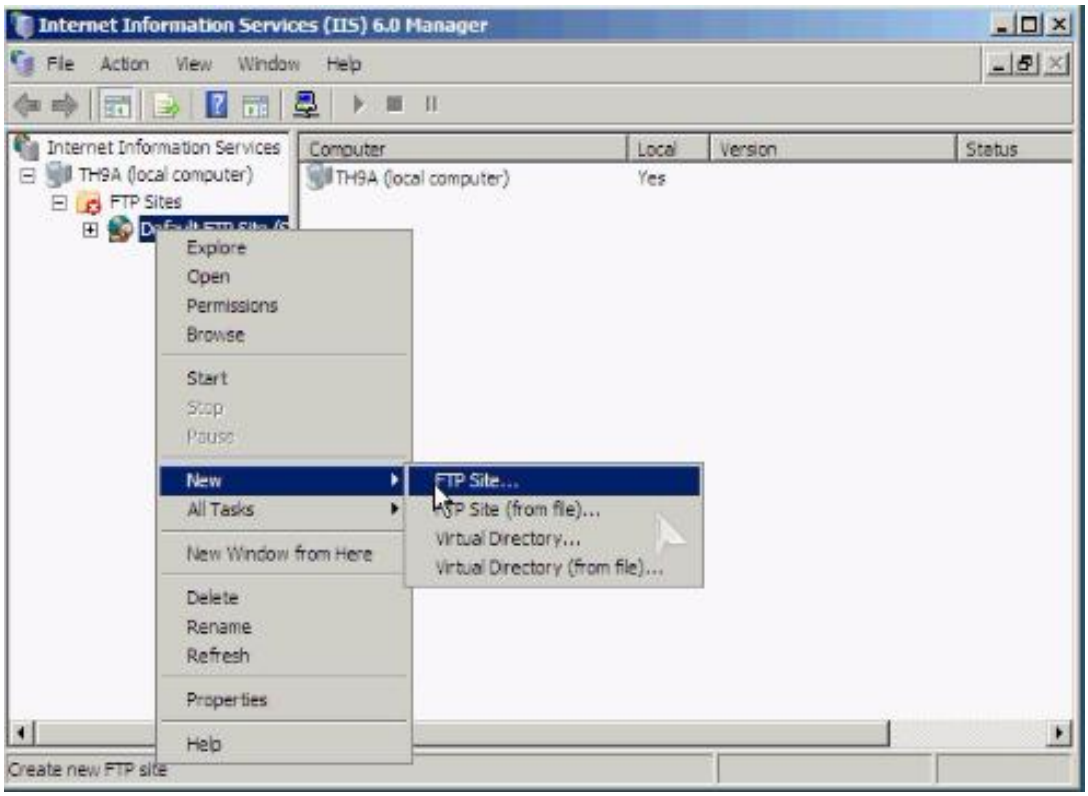
- Quá trình cài đặt hoàn tất. Sau đó nhấn **Close.**

2.2. Cấu hình : tạo một FTP site

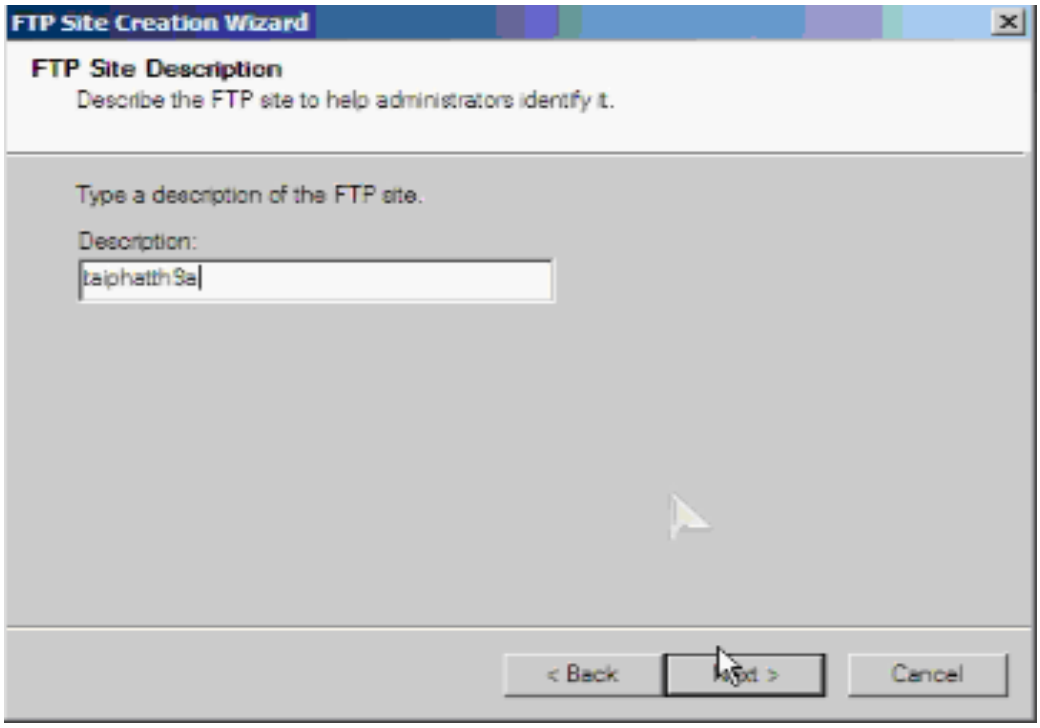
- Trước tiên, ta tạo thư mục cần public :



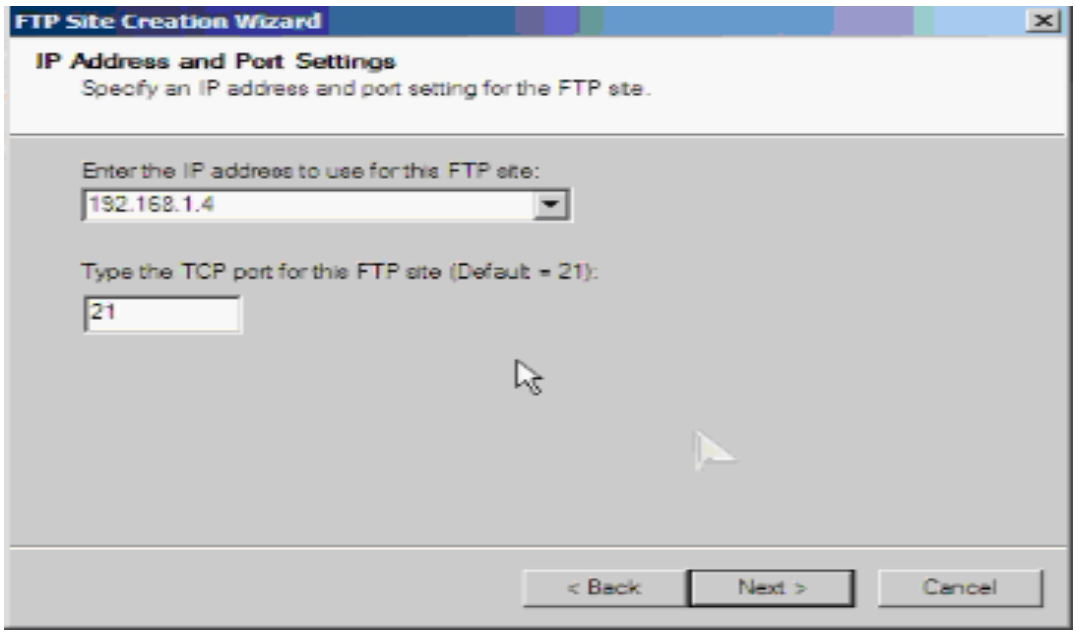
- Vào **Start➔Administrator Tools➔Internet Information Services (IIS) 6.0 Manager**. Bấm phải chuột vào **FTP Sites** hoặc **Default FTP Site➔**chọn **New➔FTP Site..**



- Điền tên gợi nhớ.



- Nhập IP máy server và dùng port mặc định FTP là **21**



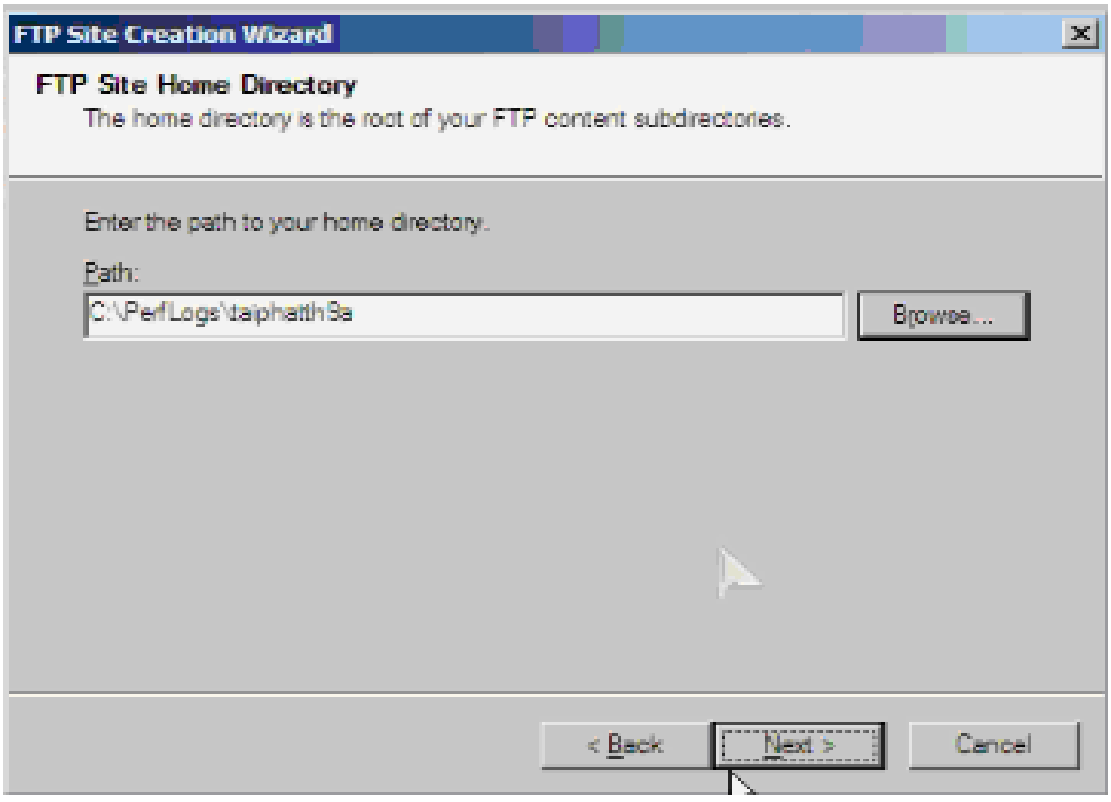
- Chọn các mức bảo vệ file và ngăn chặn truy cập:

Do not isolate users : cho phép tất cả user đăng nhập vào FTP site.

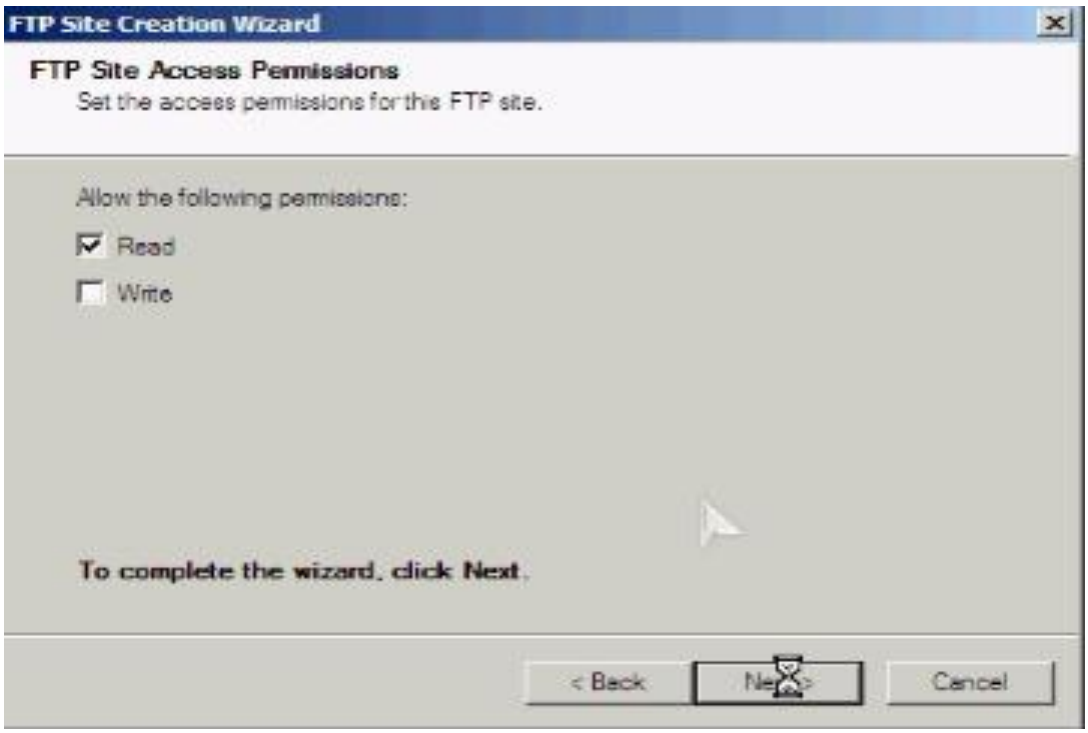
Isolate users : mỗi user sẽ tự được đưa vào thư mục chỉ định

Isolate users using Active Directory : Cho phép user đăng nhập vào FTP site nhưng phải có account ở Active Directory.

- Nhập đường dẫn thư mục cần publish



- Thiết lập quyền hạn cho người truy cập đối với file.



- Sau đó nhấn **Finish** để hoàn tất.

CHƯƠNG 4: USER - GROUP

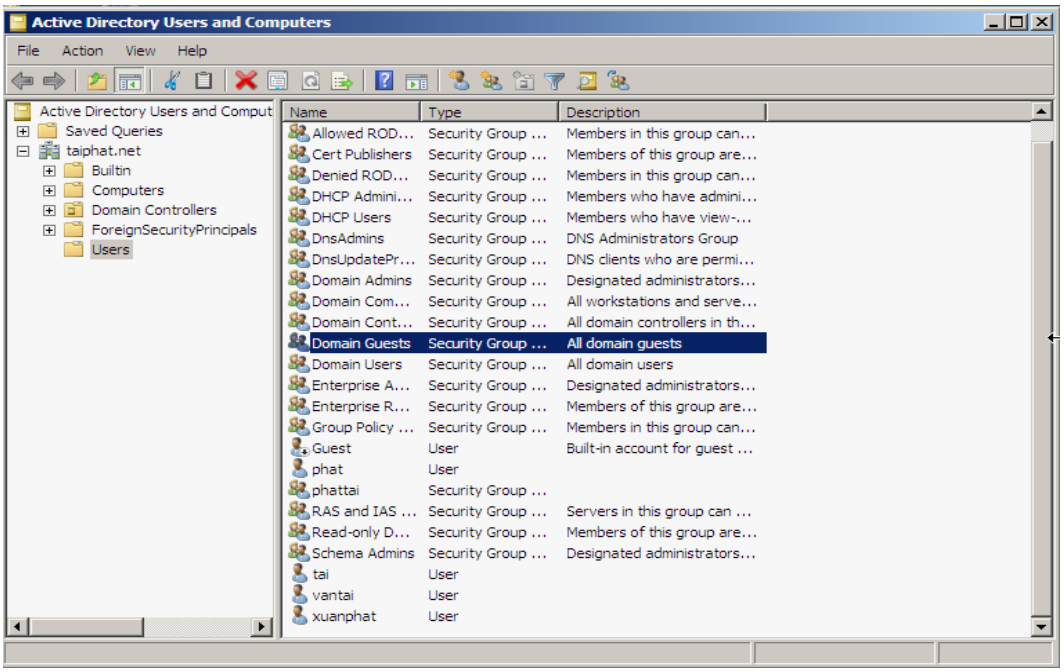
I. GIỚI THIỆU VỀ LOCAL USER VÀ LOCAL GROUP

Thông thường một máy tính không phải chỉ có một người nào đó sử dụng duy nhất mà trên thực tế ngay cả máy nhà đôi vẫn có ít nhất từ 2-3 người sử dụng. Tuy nhiên nếu tất cả mọi người đều sử dụng chung một tài khoản thì những dữ liệu riêng tư của mình không cho người khác thấy. Nhưng nếu máy tính là máy chung của công ty và vấn đề đặt ra là ta không muốn tài liệu của người mình, người khác có thể xem tùy tiện được. Cách tốt nhất là cấp cho mỗi nhân viên một máy nhất định và yêu cầu họ đặt password lên máy của mình, nhưng như thế thì rất tốn kém và không được ưa chuộng. Chính vì thế người quản trị mạng sẽ sử dụng công cụ Local Users and Groups để tạo các tài khoản người dùng trên cùng một máy, khi đó dữ liệu của người này người kia không thể truy cập được.

II. TẠO CÁC LOCAL USER

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

-Vào **Start➔Programs➔Administrative Tools ➔Active Directory Users and Computers**.



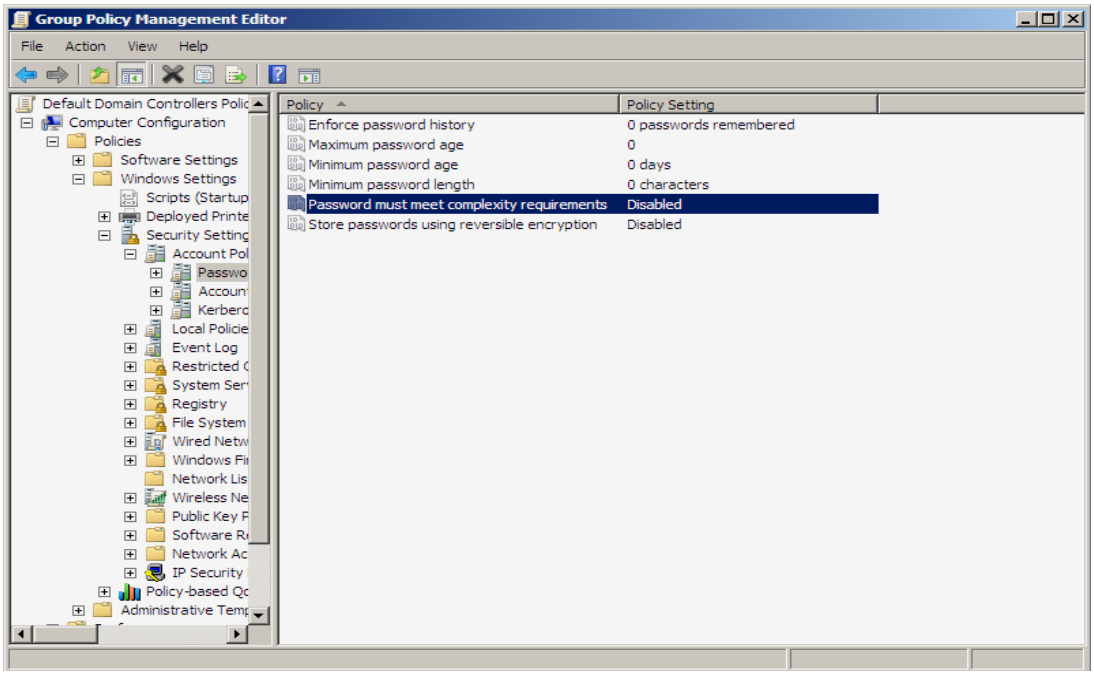
- Chuột phải **User ➔ New User ➔** tại bảng **New Object – User** điền đầy đủ các thông tin vào First Name, Last Name, Full Name.

- Chọn **Next** để tiếp tục.Xuất hiện bảng thiết lập password.Đây là mật khẩu của bạn ứng với tên tài khoản đã tạo ở trên,dùng để đăng nhập vào domain.

- Pasword phải thỏa mãn các chính sách mặc định của Windows Server 2008.Password ít nhất là 7 kí tự và phải có các thành phần sau :

- Các kí tự thường : a,b,c,d,e…..
- Các kí tự in hoa : A,B,C,D,E….
- Các chữ số : 1,2,3,4,5….
- Các kí tự đặc biệt : @,!,$,&,#....

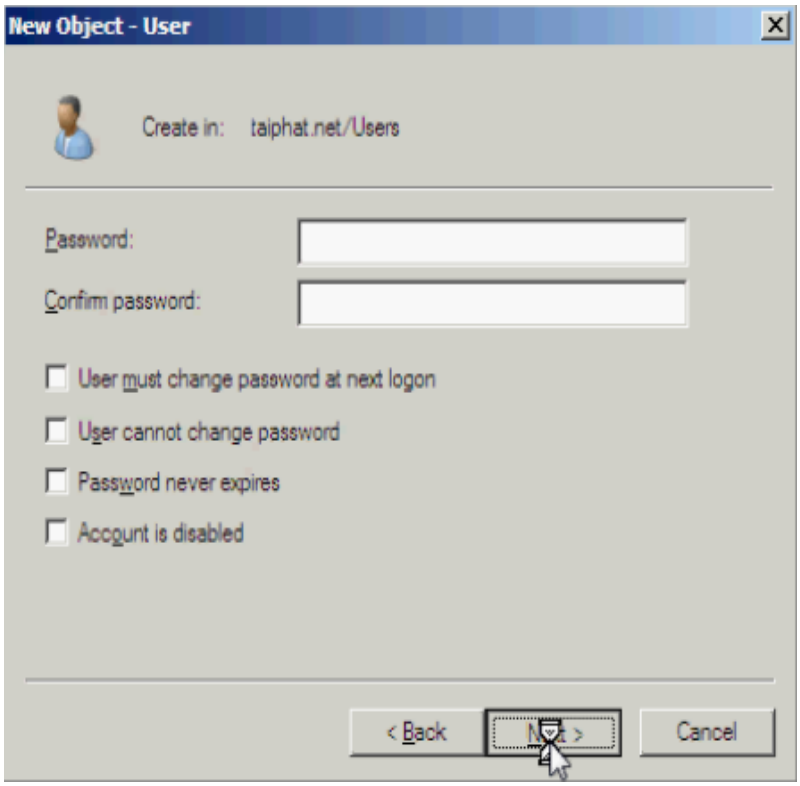
- Ở đây không thiết lập password vì trong **Group Policy Management Editor** đã vô hiệu hóa password.



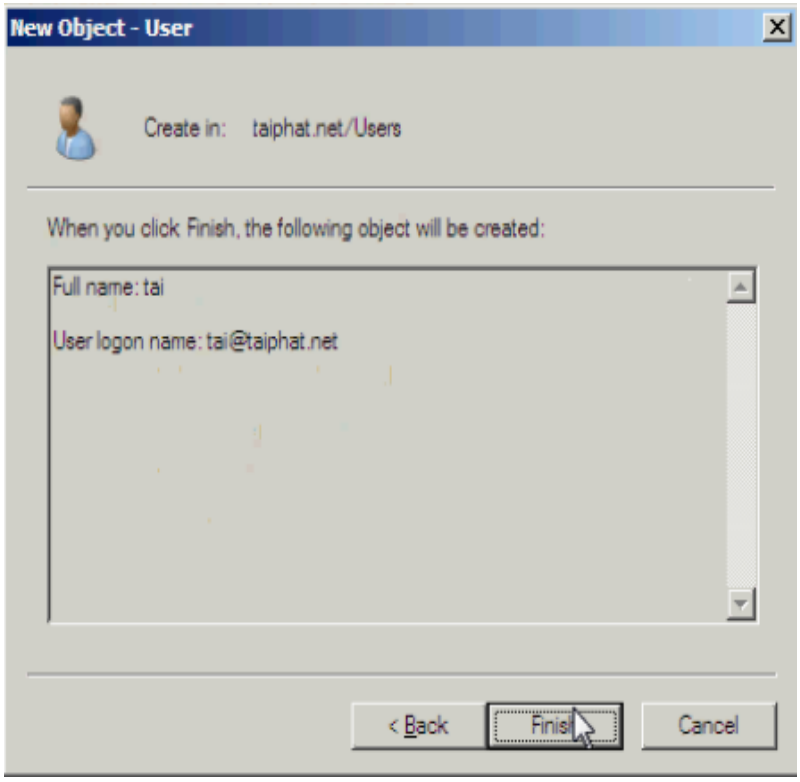
- Lưu ý 4 dòng :

- **User must change password at next logon** : bắt buộc user phải thay đổi password ở lần đăng nhập kế tiếp
- **User cannot change password** : user không có quyền thay đổi password
- **Password never expires** : password không có thời hạn qui định
- **Account is disabled** : vô hiệu hóa tài khoản.

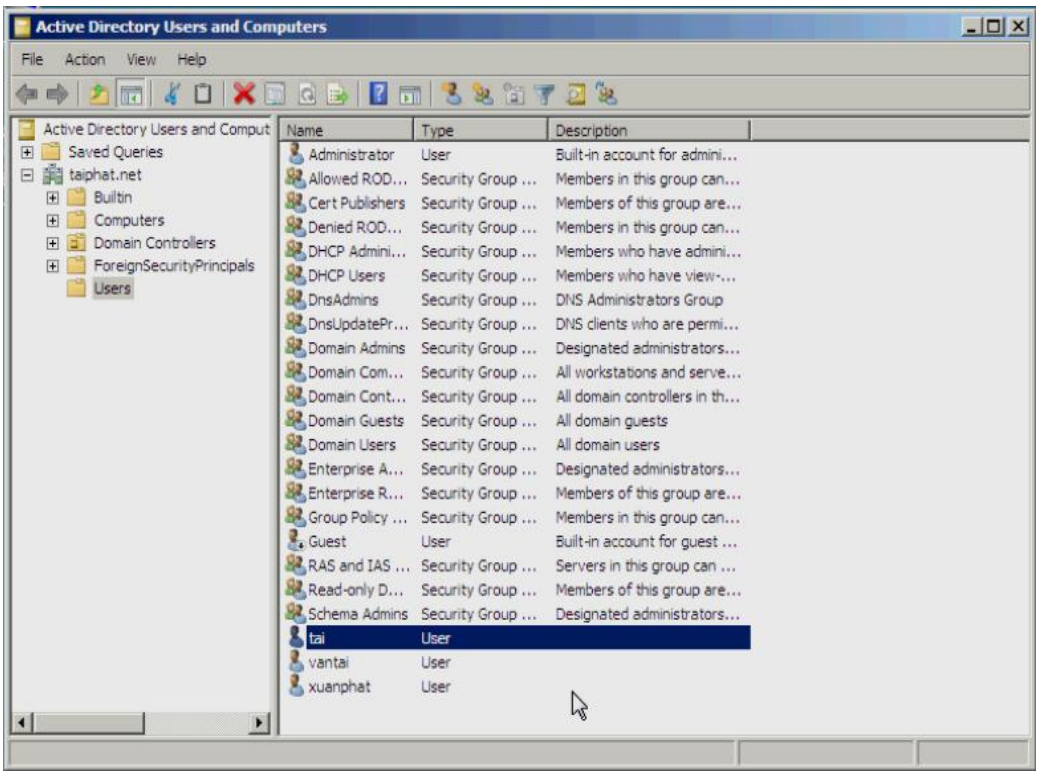
- Ở đây sẽ không chọn mục nào hết. Nhấn **Next.**



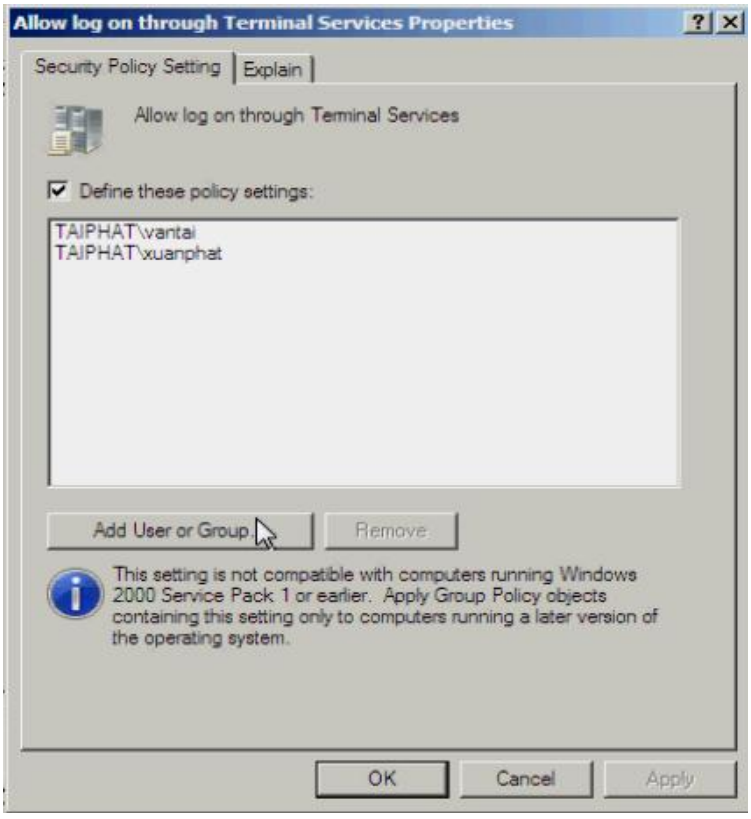
- Chọn **Next** để tiếp tục.Ở bảng tiếp theo là thông tin về user chuẩn bị được tạo.



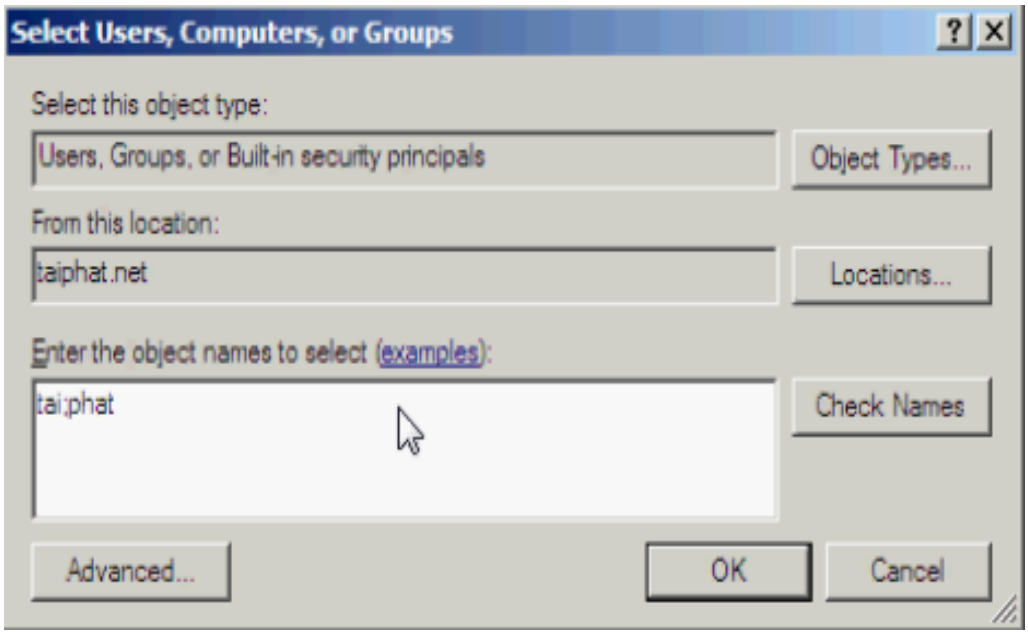
- Chọn **Finish** để kết thúc.
- Tiếp theo,kiểm tra thử user đã được tạo .Click đúp vào User và kiểm tra.



Để gán cho User có thể đăng nhập vào domain. Vào **Group Policy Management Editor.** Chọn **Allow log on through Terminal Services**.

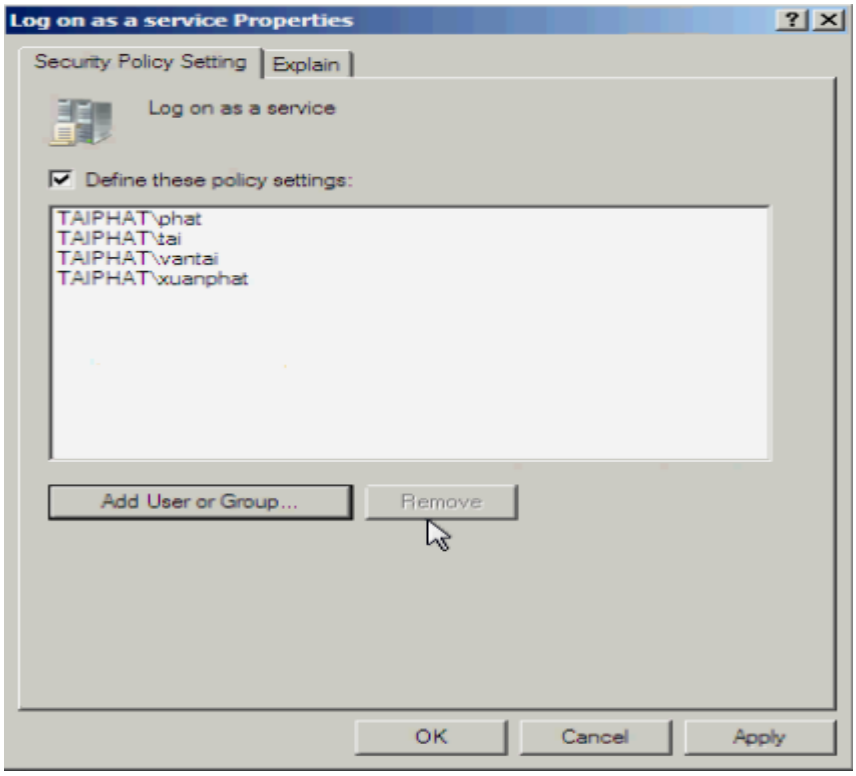


Add User or Group ➔ Browse ➔ đánh tên user rồi **Check Names ➔ OK**.



User tai , phat đã được chọn để logon. Và nhấn **OK**

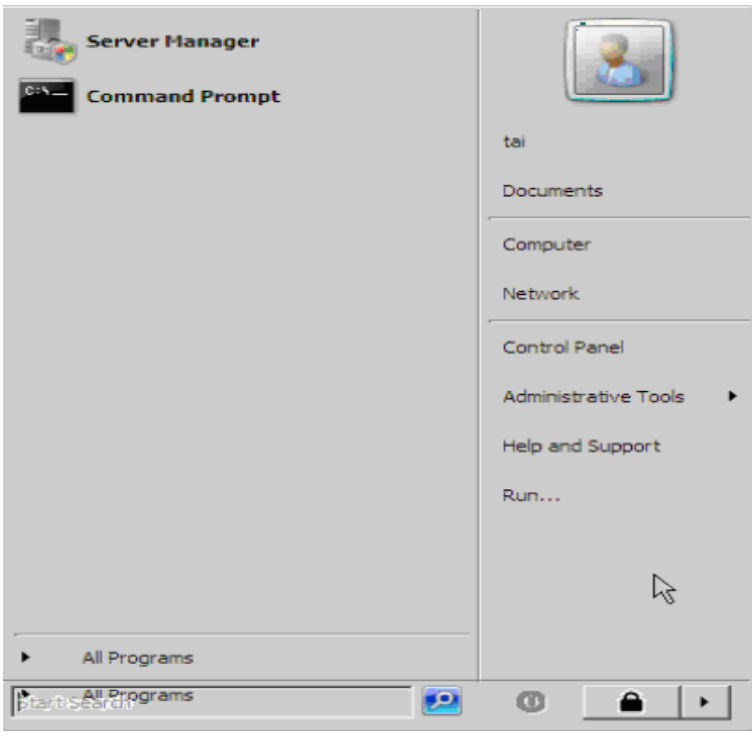
Vào **Logon as a Service.** Cũng gán quyền cho user như trên. User tai , phat đã được gán quyền được logon.



Xong sau đó vào **Start ➔ Run ➔** gõ lệnh **gpupdate /force** để cập nhật user.

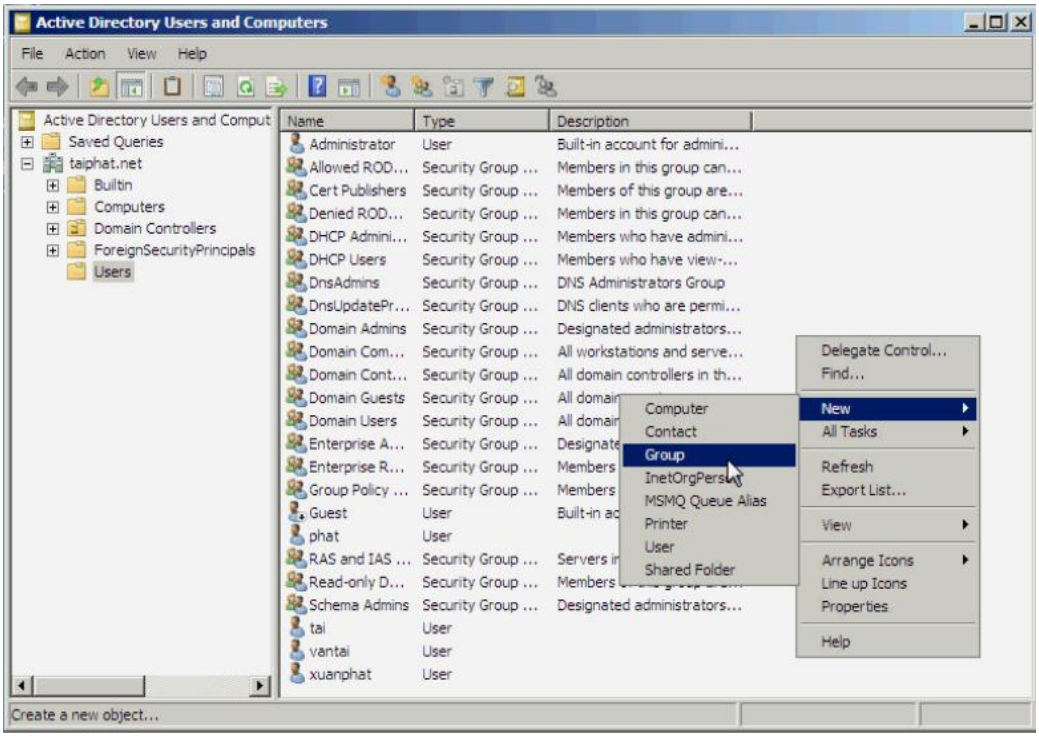
Sau đó **Log off** để đăng nhập **user** vào **Administrator.**Nhập tên user đã được gán quyền và nhấn OK.(không cần password) vì khi nảy ta đã không nhập password.

Vào **Start** để xem user đã đăng nhập vào.

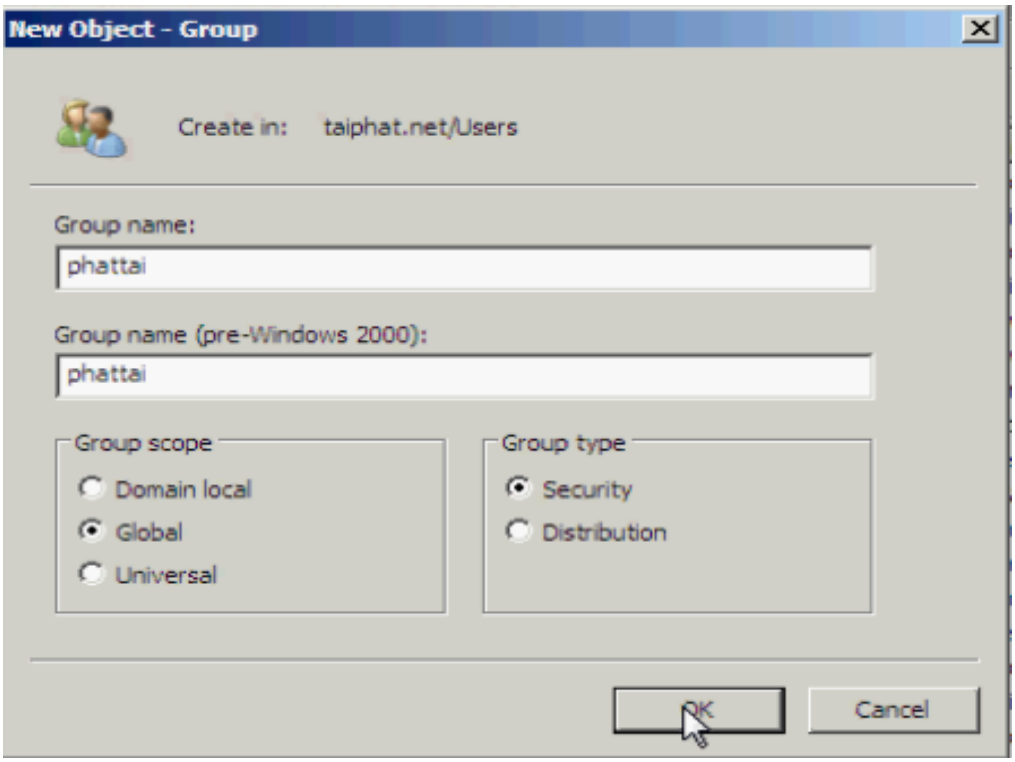


III. TẠO LOCAL GROUP

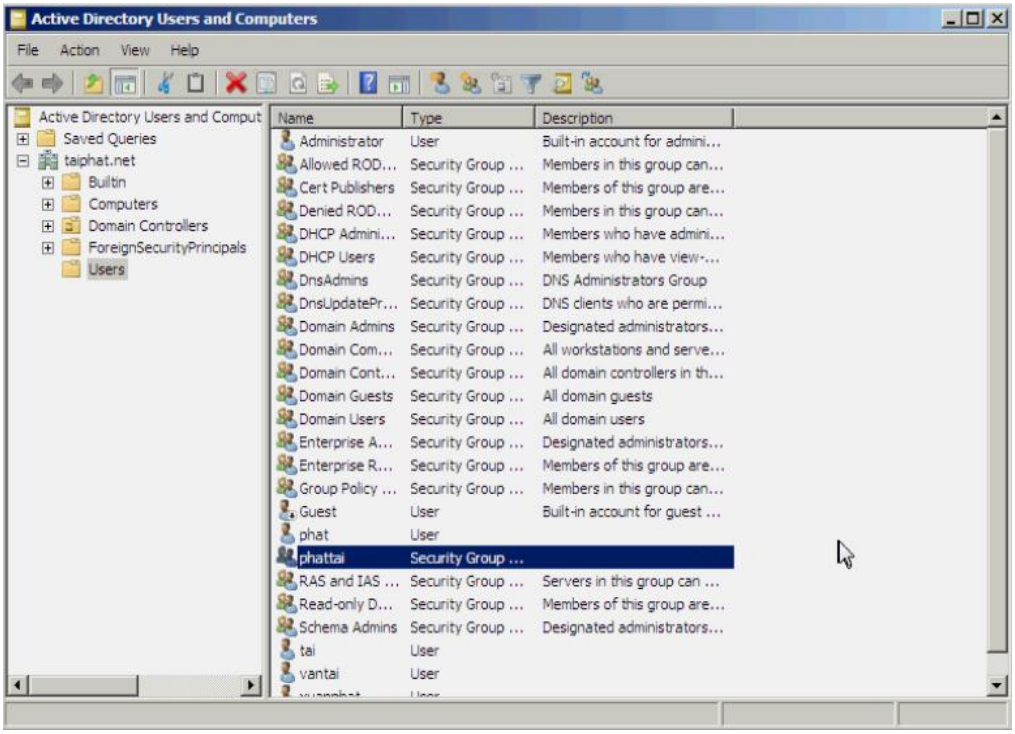
Để tạo một group mới.Nhấp chuột phải vào User và chọn **New ➔ Group**.



Tại ô **Group name** gõ tên group.Sau đó chọn **OK**



Kiểm tra lại group đã được tạo bằng cách click vào User

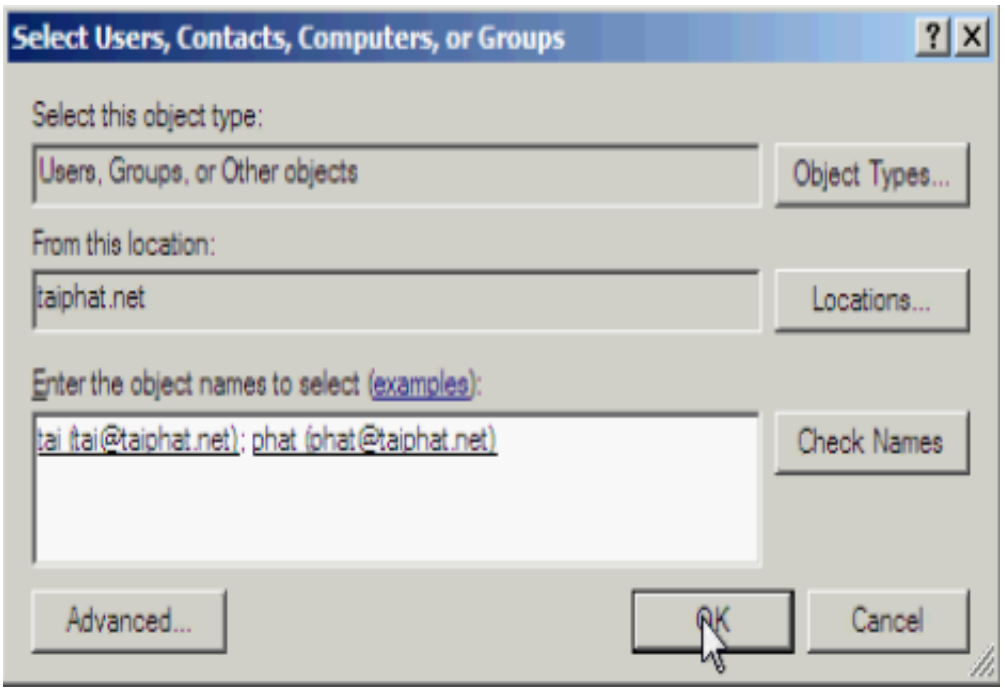


Để đưa user vào group phattai ,nhấp chuột phải vào group và chọn **Properties**. Tại **tab Member**.Chọn **Add..**

Tại ô **Enter the object name to select** bạn gõ tên user muốn đưa vào group.

Sau khi gõ tên user,chọn **Check Names** để kiểm tra.

Và kết quả là tồn tại user này trên domain.



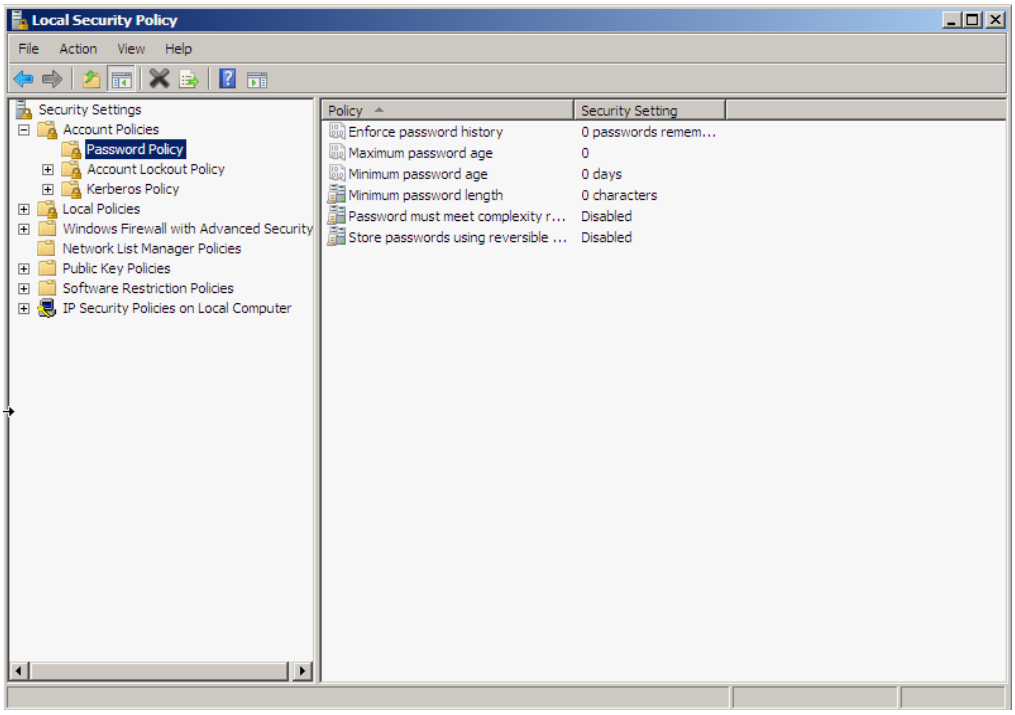
Sau khi thêm user vào group.Chọn **OK** để xác nhận

CHƯƠNG 5: CHÍNH SÁCH BẢO MẬT (GROUP POLICY)

I. ACCOUNT POLICY

1. Password policy

Vào **Aministrator ➔ Local Sercurity Policy ➔ Account policies**.

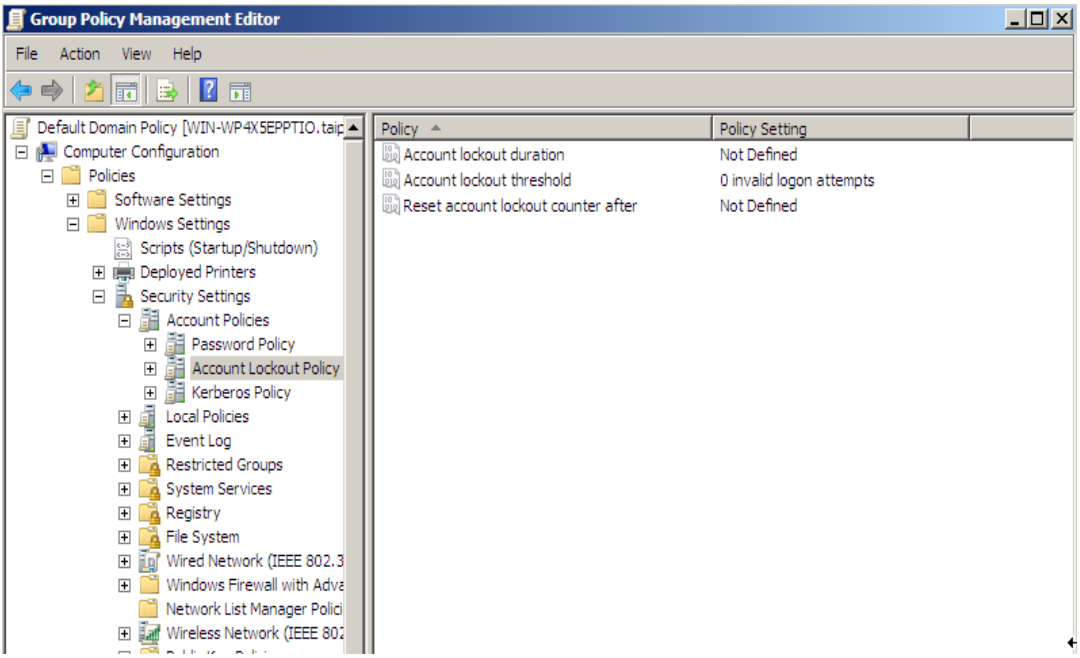


Trong này bao gồm các mục:

- **Password must meet complexity** … : khi đặt password cho wins phải có đủ độ phức tạp.(hoa, thường, số, ký tự đặc biệt). Mặc định tính năng này sẽ bị disable, để gia tăng chế độ bảo mật nên chọn Enable
- **Minimum password age**: mặc định giá trị này là 0 nếu ta thay nó bằng con số khác 0 VD là 3 chẳng hạn thì user chỉ có quyền thay đổi password 3 ngày một lần mà thôi.
- **Minimum password length**: Độ dài tối thiểu của password
- **Enforce password history**: nhớ bao nhiêu password không cho đặt trùng.
- **Store password using reversible** … : mã hoá password.

2. Account lockout policy

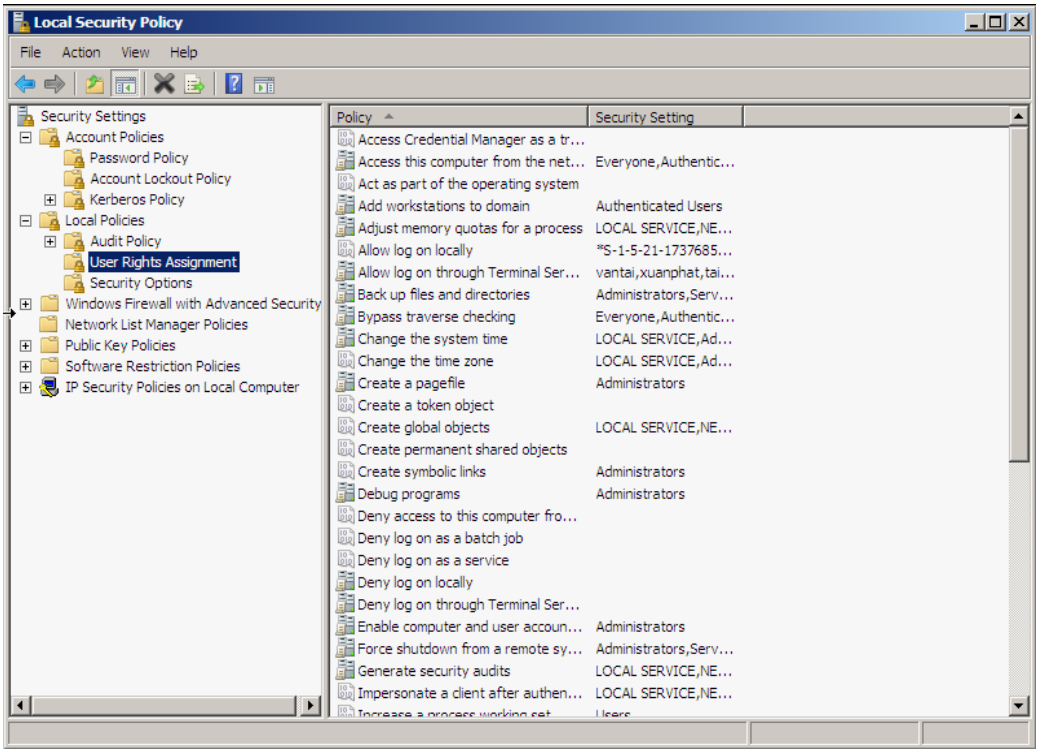
- **Account lockout threshold**: để khoá account khi đăng nhập sai.
- **Account lockout duration**: khoá account trong 30 phút khi đang nhập sai.
- **Reset account lockout counter after**: xoá bộ nhớ đánh pass.



II. LOCAL POLICY

1. User rights assignment:

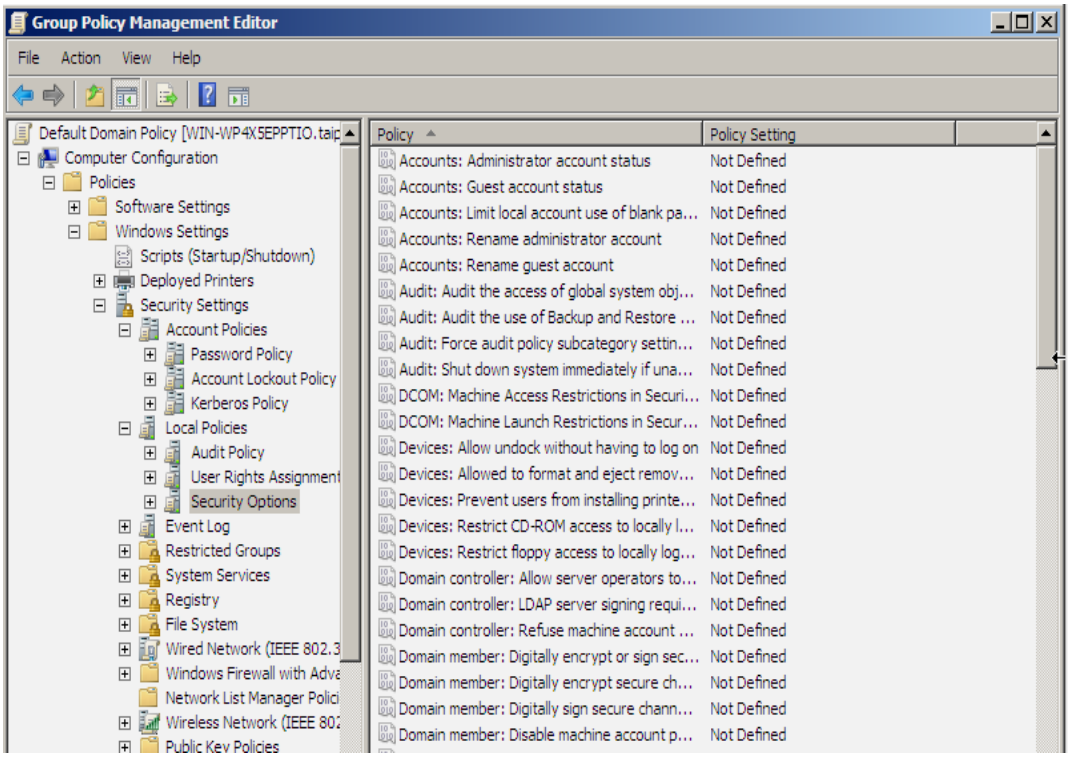
Vào **Administrator ➔ Local Sercurity➔Local policies.**



- **Deny logon locally**: chọn user không cho đăng nhập vào máy tính.
- **Change the system time**: những người được thay đổi giờ hệ thống.
- **Shutdown the system**: những người có quyền tắt máy.
- **Allow log on through Terminal Services**: cho phép đăng nhập.
- **Log on as a Service**: đăng nhập như một dịch vụ.

Và còn rất nhiều tính năng khác

2. Sercurity options



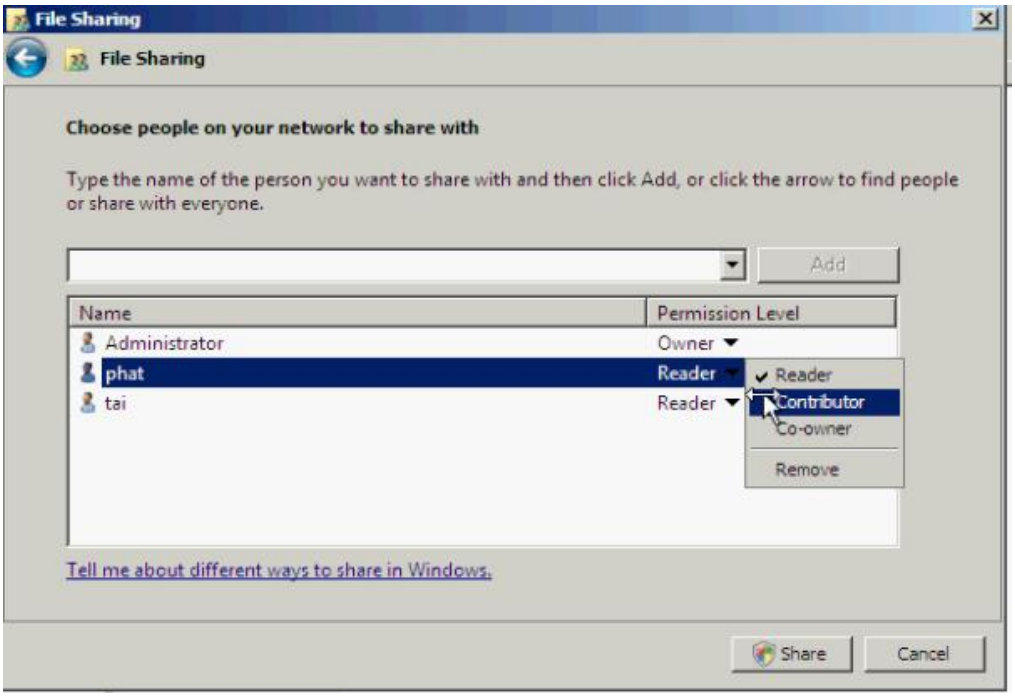
- **Interactive logon**: **Do not display last user name**: Khi user logout máy cửa sổ đăng nhập sẽ không ghi lại account user vừa logon.
- **Interactive logon**: **Message text for users attempting to log on**: Bạn có thể nhắn gởi một nội dung nào đó tới các user trước khi họ logon vào máy với nội dung nhắn gởi ở đây.
- **Interactive logon**: **Message title for users attempting to log on**: Bạn nhập tiêu đề của hộp nội dung nhắn gởi vào đây.

I. KIỂM SOÁT QUYỀN TRUY CẬP HỆ THỐNG TỆP NTFS

1. Phân quyền đơn giản

- Windows có một cơ chế kiểm soát truy nhập rất đơn giản là share đồng thời phân quyền. Muốn share, chọn lệnh Share..., lần lượt Add một folder, hãy click nút phụ của con chuột vào folder ấy, sẽ hiện context menu từng nhóm người dùng (hay từng người dùng), cứ mỗi nhóm chọn Permission Level để phân quyền cho nhóm ấy. Xong ấn nút Share.
- Theo cách này, mỗi nhóm có thể có một trong ba quyền truy nhập.

- **Reader** (người xem). Xem toàn bộ nội dung folder.
- **Contributor** (người đóng góp). Xem toàn bộ nội dung folder, có thể tạo thêm file và folder và sửa file / folder mà bản thân đã thêm.
- **Co-owner** (đồng chủ sở hữu). Xem và sửa toàn bộ nội dung của folder, kể cả các file/folder mà người khác tạo ra.



- Ba quyền này không độc lập với nhau. Co-owner bao hàm Contributor, và Contributor lại bao hàm Viewer.
- Cơ chế này rất dễ dùng và tiện dùng, nhưng không dùng được trong nhiều trường hợp. Hơn nữa, cơ chế này không có trên Windows Server 2003 mà chỉ có ở Windows Server 2008.

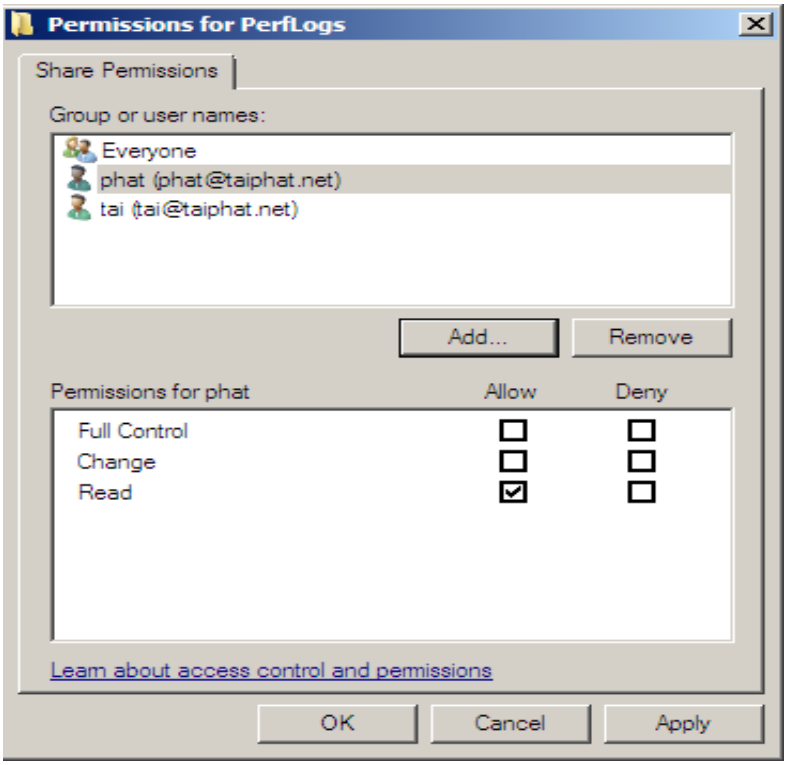
2. Phân quyền cơ bản

2.1. Giới thiệu cơ chế phân quyềnNTFS

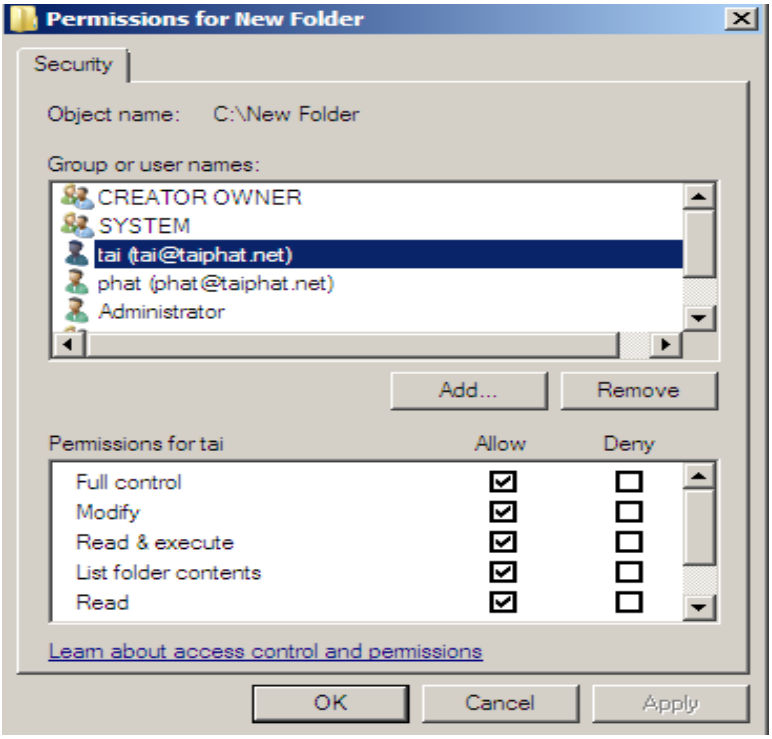
- Cơ chế kiểm soát truy nhập cơ bản trên Windows Server là kết hợp giữa hai cơ chế phân quyền: phân quyền trên hệ thống tệp NTFS và phân quyền trên giao thức chia xẻ tệp CIFS (hay còn gọi là phân quyền share).

Phân quyền CIFS có ba quyền:

- Read (đọc)
- Change (sửa)
- Full Control (toàn quyền).



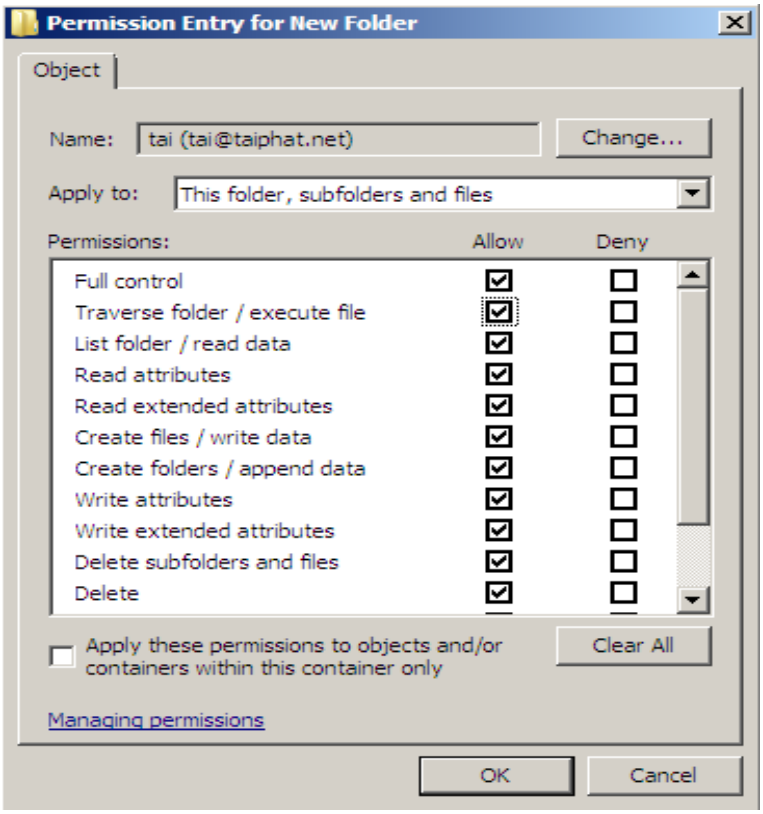
- Ba quyền này không độc lập với nhau. Full Control bao hàm Change, và Change bao hàm Read.
- Phân quyền NTFS có 6 quyền: Full Control (toàn quyền), Modify (sửa), Read & Execute (đọc tệp và chạy chương trình),List folder contents (hiện nội dung thư mục), Read (đọc), và Write (viết).



- Khi truy nhập server từ máy trạm, quyền truy nhập là giao giữa hai quyền CIFS và NTFS. Do đó, trong thực tiễn làm việc, để giảm bớt sự phức tạp, khi tạo nhiều share trên một server, có thể và nên tạo các share ấy theo cùng một quyền (CIFS) thống nhất cho mọi share và mọi người dùng, cụ thể:
  - Trên mọi share tự quản, Everyone có quyền Full Control.
  - Trên mọi share quản chế, Everyone có quyền Change.
- Sự phân biệt quyền truy nhập giữa các nhóm khác nhau và trên các share khác nhau khi đó sẽ chỉ thể hiện ở phân quyền NTFS.

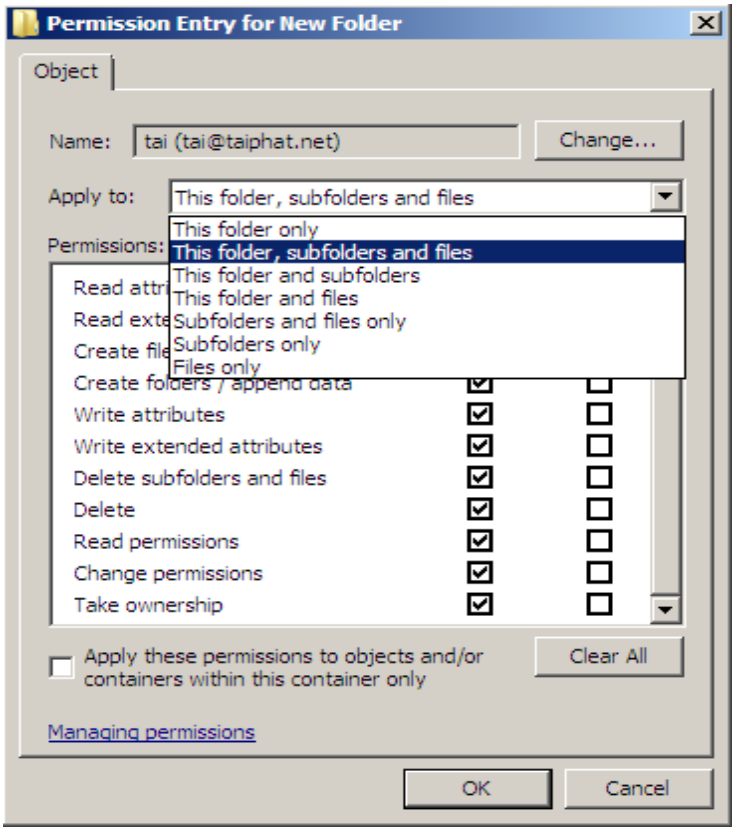
2.2. Các công cụ phân quyền NTFS

- Tất cả quyền truy nhập cơ sở của NTFS là :
  - **Traverse folder/execute file** (đi xuyên qua folder / thi hành file).
  - **List folder/read data** (hiện thư mục, đọc dữ liệu).
  - **Read attributes** (đọc thuộc tính).
  - **Read extended attributes** (đọc thuộc tính mở rộng).
  - **Create files/write data** (tạo file, viết dữ liệu).
  - **Create folders/append data** (tạo folder, nối dữ liệu).
  - **Write attributes** (viết thuộc tính). Cho phép thay đổi các thuộc tính của file và folder.
  - **Write extended attributes** (viết thuộc tính mở rộng).
  - **Delete subfolders and files** (xóa folder con và file).
  - **Delete** (xóa).
  - **Read permissions** (đọc quyền).
  - **Change permissions** (đổi quyền).
  - **Take ownership** (đoạt chủ quyền).



- Khi phân quyền cho một folder, quyền đã phân sẽ có thể sẽ áp dụng lên cả các folder con và file bên trong, việc này gọi là thừa kế. Việc thừa kế thực hiện theo một trong sáu kiểu sau đây.

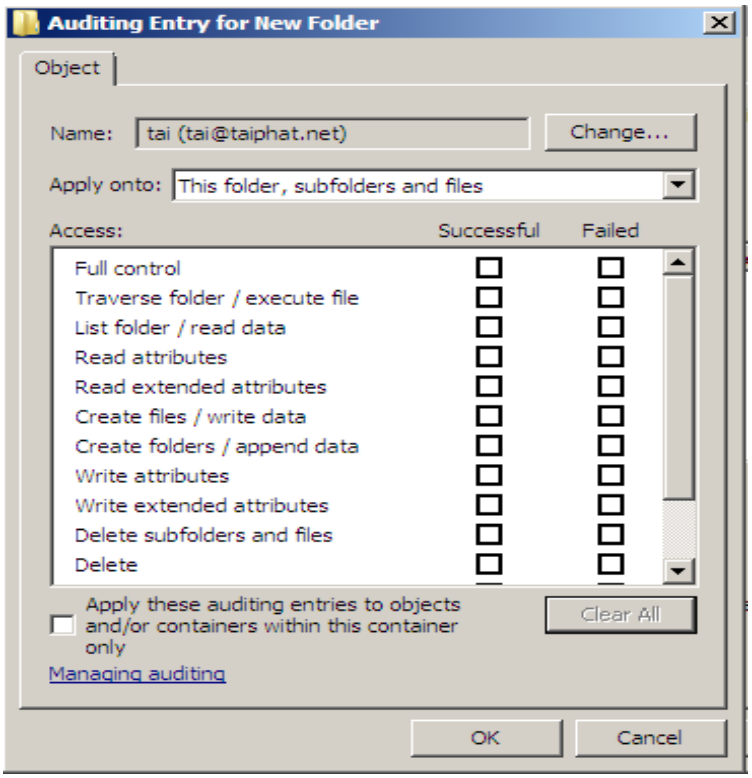
- **This folder only** (chỉ folder này thôi). Quyền chỉ áp dụng cho folder này, không thừa kế.
- **This folder, subfolders and files** (folder này, các folder con và các file). Quyền áp dụng cho folder này, các folder con và các file. Thừa kế toàn phần.
- **This folder and subfolders** (folder này và các folder con). Quyền áp dụng cho folder này và các folder con. Các folder con thừa kế.
- **This folder and files** (folder này và các file). Quyền áp dụng cho folder này và các file. Các file thừa kế.
- **Subfolders and files only** (các folder con và các file thôi). Quyền áp dụng chỉ cho các folder con và các file. Thừa kế toàn phần ngoại trừ bản thân.
- **Subfolders only** (chỉ các folder con thôi). Quyền áp dụng chỉ cho các folder con. Các folder thừa kế ngoại trừ bản thân.



2.3. Thực hiện các quyền cơ bản của dữ liệu doanh nghiệp trên NTFS

- Trong hệ thống tệp NTFS, năm quyền cơ bản trên folder dữ liệu doanh nghiệp được thực hiện theo những công thức sau đây:

- Quyền sử dụng = Read & Execute, List Folder Contents và Read this folder, subfolders and files.
- Quyền đóng góp = quyền sử dụng + Create files / Write data và Create folders/Append data this folder and subfolders.
- Quyền biên tập = quyền sử dụng + Modify và Write this folder, subfolders and files.
- Quyền xem thư mục = List folder / Read data this folder and subfolders.
- Quyền xem quyền = Read Permissions this folder and subfolders.
- Quyền xem quyền = Read Permissions this folder, subfolders and files.



II. NGUYÊN TẮC KHI ÁP DỤNG QUYỀN TRUY CẬP

1. Nguyên tắc hoạch định thư mục chương trình

Dưới đây là 1 số nguyên tắc chung cần áp dụng khi chỉ định các cấp độ truy cập NTFS cho thư mục:

- Bỏ quyền truy cập NTFS mặc định ở cấp độ Full Control từ nhóm Everyone và đem cấp cho nhóm Administrators.
- Chỉ định cấp độ truy cập Full Control hoặc Change đối với thư mục thích hợp cho những nhóm chịu trách nhiệm nâng cấp và xử lí lỗi phần mềm.
- Nếu các chương trình mạng thường trú dung chung, cấp quyền truy cập ở cấp độ Read cho nhóm Users.

2 Nguyên tắc hoạch đinh thư mục dữ liệu

- Bỏ quyền truy cập NTFS ở cấp độ mặc định Full Control từ nhóm Everyone và đem cấp cho nhóm Administrators.
- Chỉ định cấp độ Add&Read cho nhóm Users và cấp độ PC cho nhóm CreatorOwner. Việc này sẽ cung cấp cho người dùng đăng nhập cục bộ khả năng hủy bỏ và sữa chữa chỉ những thư mục và tập tin họ đã sao chép hoặc tạo ra trên máy tính mà họ đăng nhập.

2. Nguyên tắc hoạch định thư mục cá nhân

- Tập trung mọi thư mục cá nhân trên 1 Volume NTFS riêng biệt với Volume chứa hệ điều hành và các chương trình, nhằm hợp lí hóa công tác quản trị và sao lưu dữ liệu

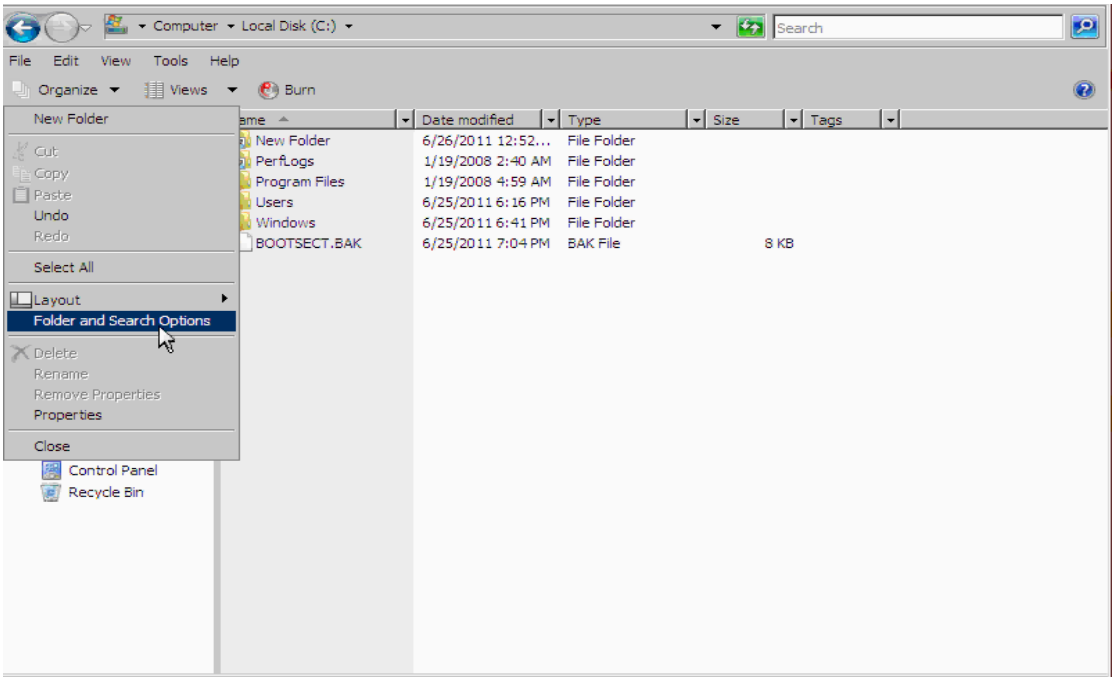
• Dùng biến %UserName% để tự động gán tên tài khoản của người dung cho thư mục và tự động chỉ định quyền truy cập NTFS ở cấp độ PC cho người tương ứng.

4. Tạo thư mục cá nhân (Home Folder) trên Volume NTFS

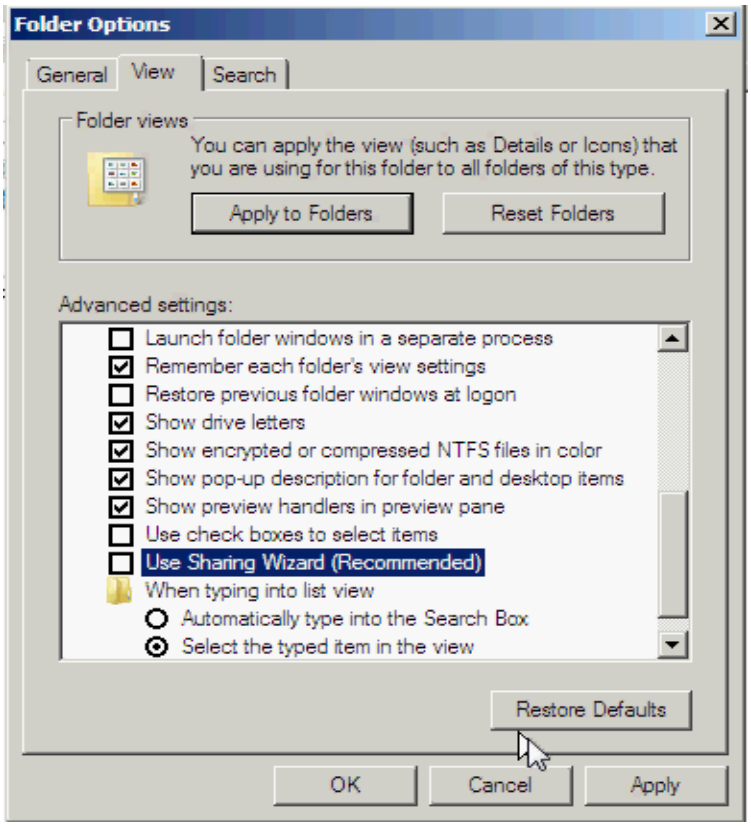
- Lưu trữ thư mục cá nhân trên một Volume NTFS có thuận lợi rất lớn, có thể tổ chức chúng thành hệ thống phân tầng và giới hạn khả năng truy cập ở những người dùng tương ứng mà không cần chia sẽ từng thư mục.

III. SHARE PERMISSION

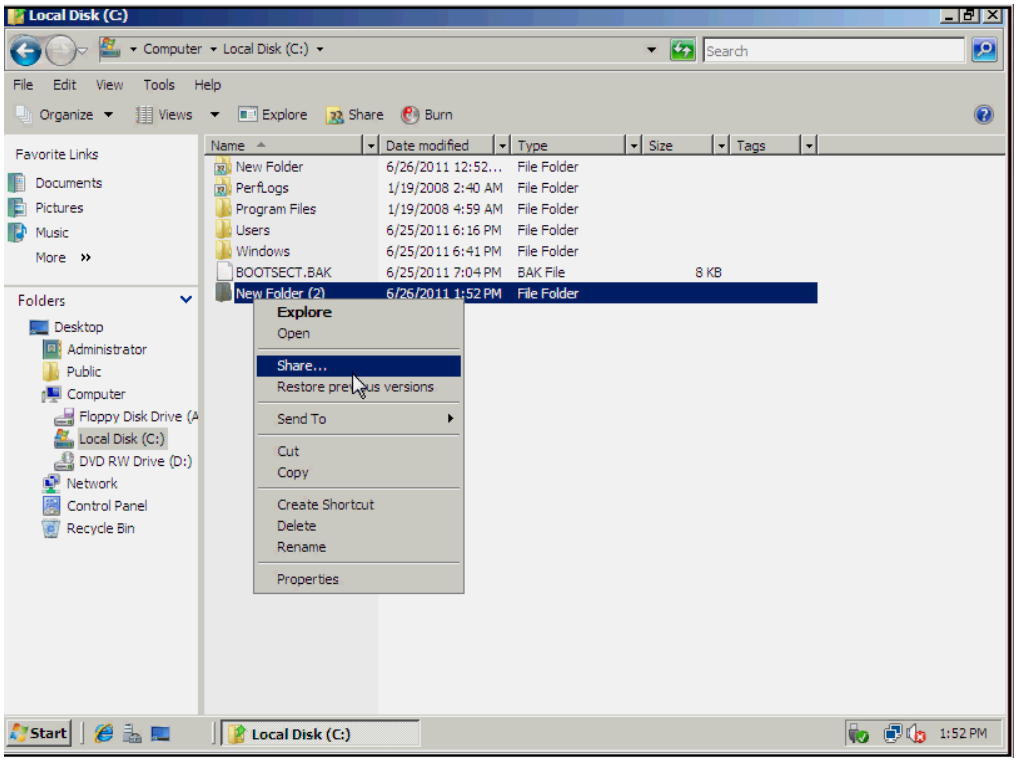
- Đầu tiên mở trình Windows Explorer ra chọn Organize ➔ Folder and Search Options.



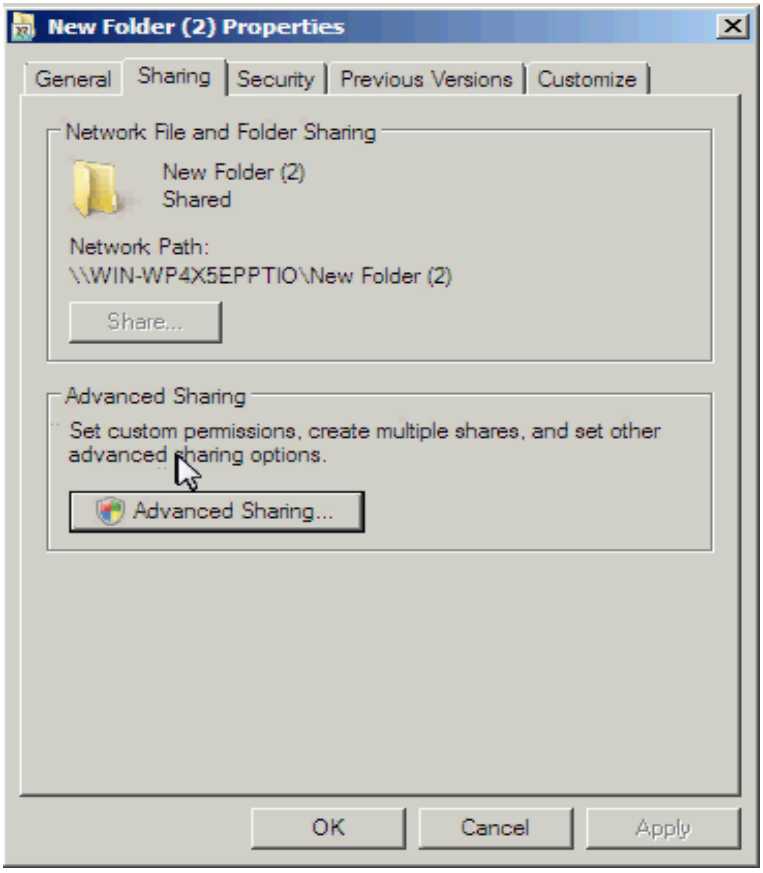
- Chọn Tab View sau đó click bỏ chọn mục Use Sharing Wizard (Recommended).



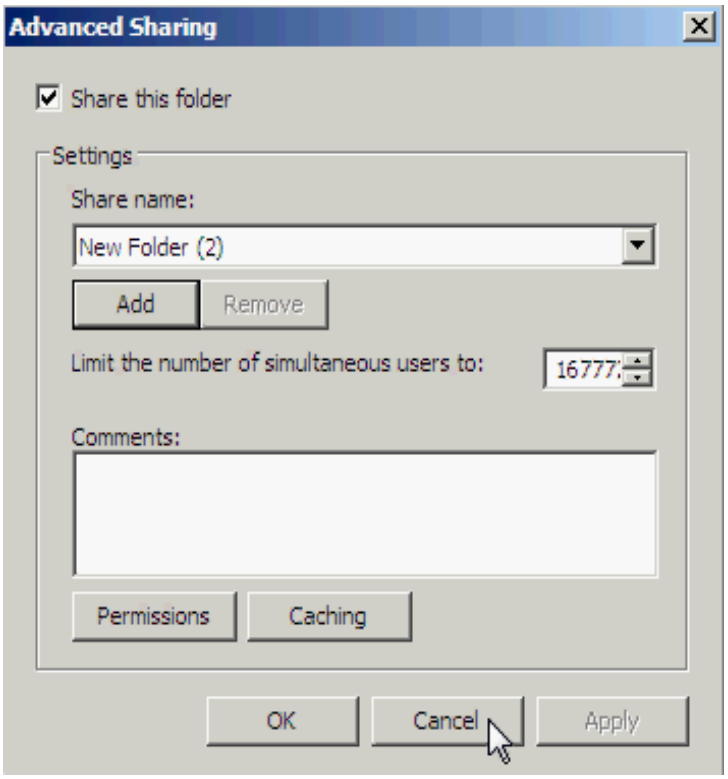
Trong Windows server 2008 để chia sẻ một thư mục nào đó nhấp chuột phải vào thư mục cần share chọn Share…



- Nhấp chọn Advanced Sharing...

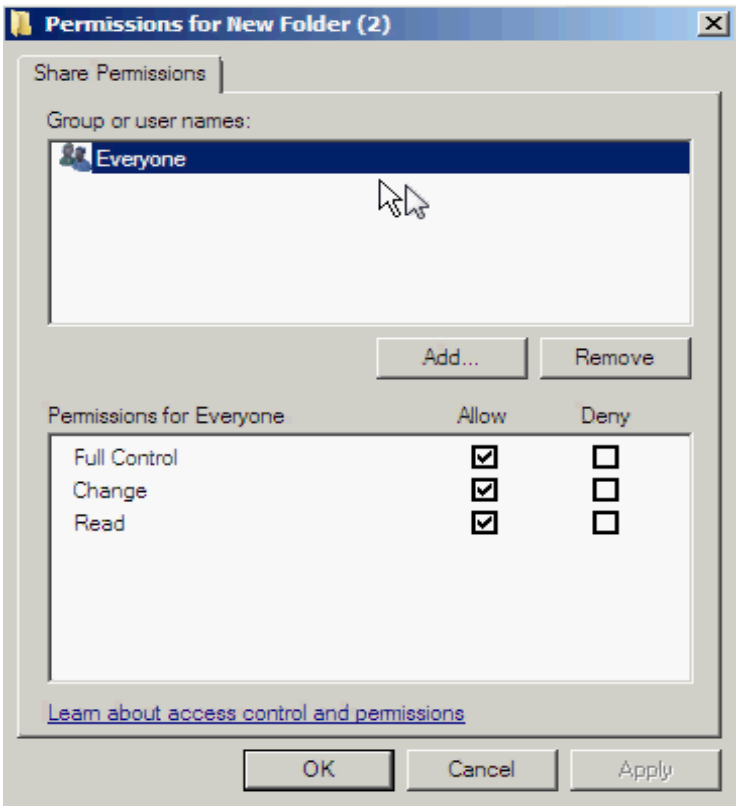


- Ở ô Share Name máy sẽ tự lấy tên default là tên thư mục hiện hành bạn có thể chỉnh sửa tên này tùy ý.

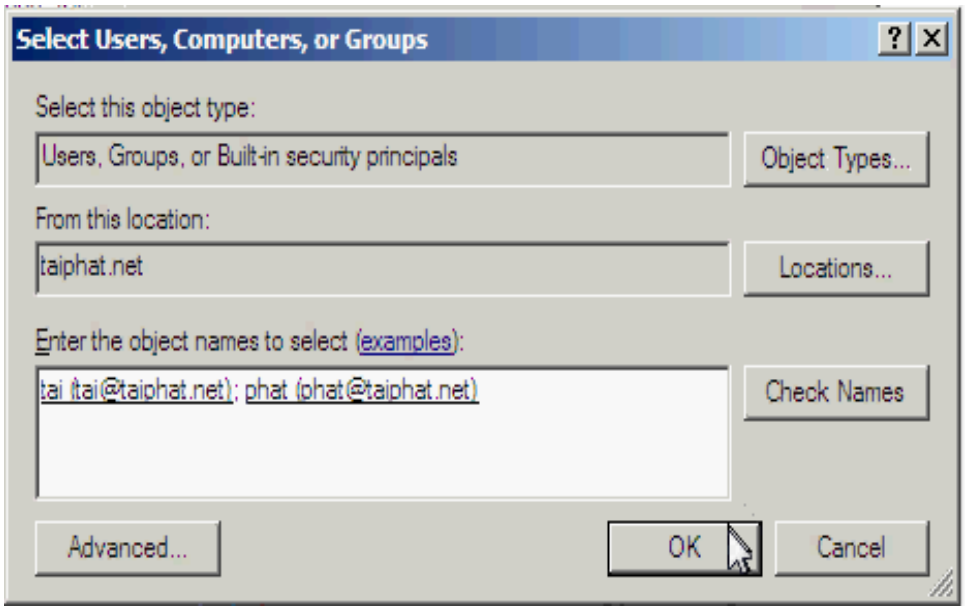


Với các tùy chọn là Allow: User có quyền truy cập tài nguyên với quyền hạn tương ứng.

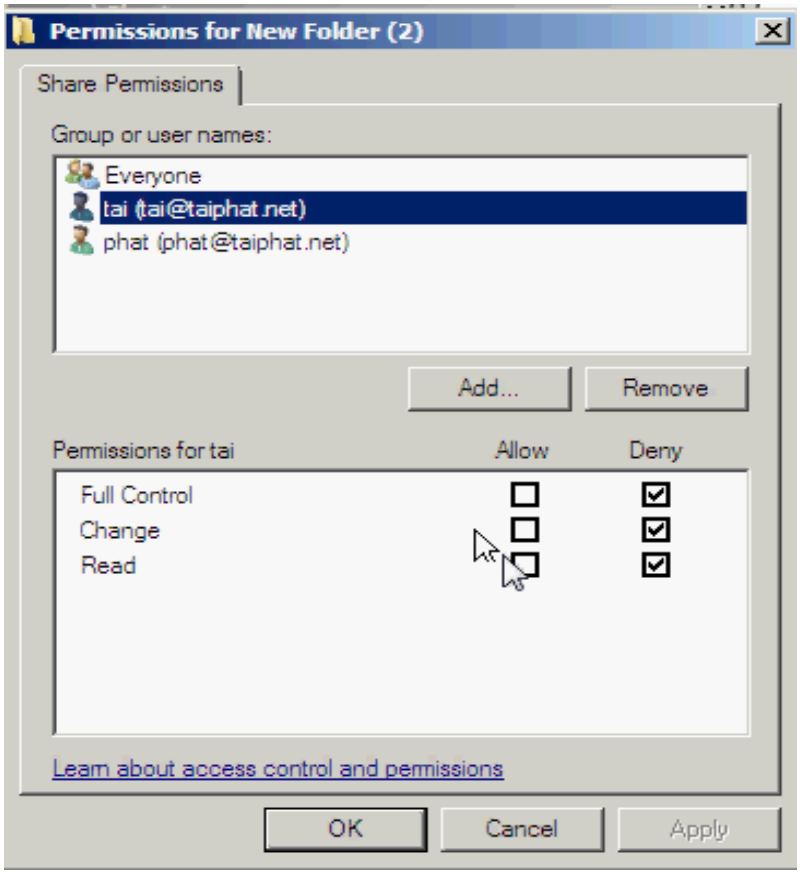
Với các tùy chọn là Deny: User không có quyền truy cập tài nguyên với quyền hạn tương ứng.



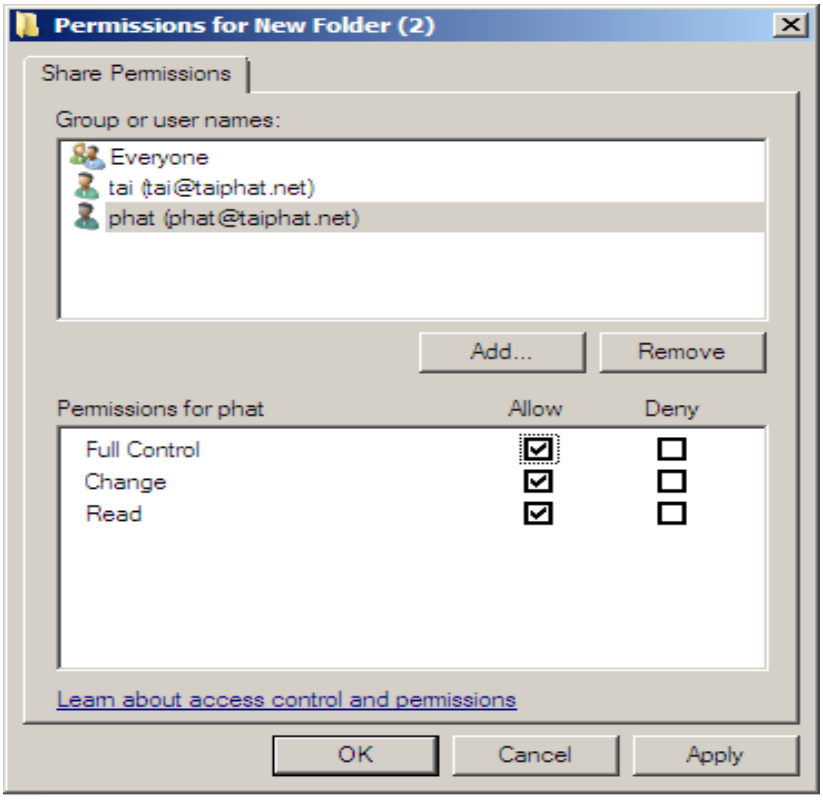
Để thực hiện phân quyền cho các Group thì ta cần Deny tất cả các quyền của Group User này.
Sau khi Deny tất cả các quyền của Group User nhấp nút Add thể thêm Group hoặc User vào.



Trong này giả sử Add thêm User tai và cũng Set quyền cho User này là Deny tất cả mọi quyền.

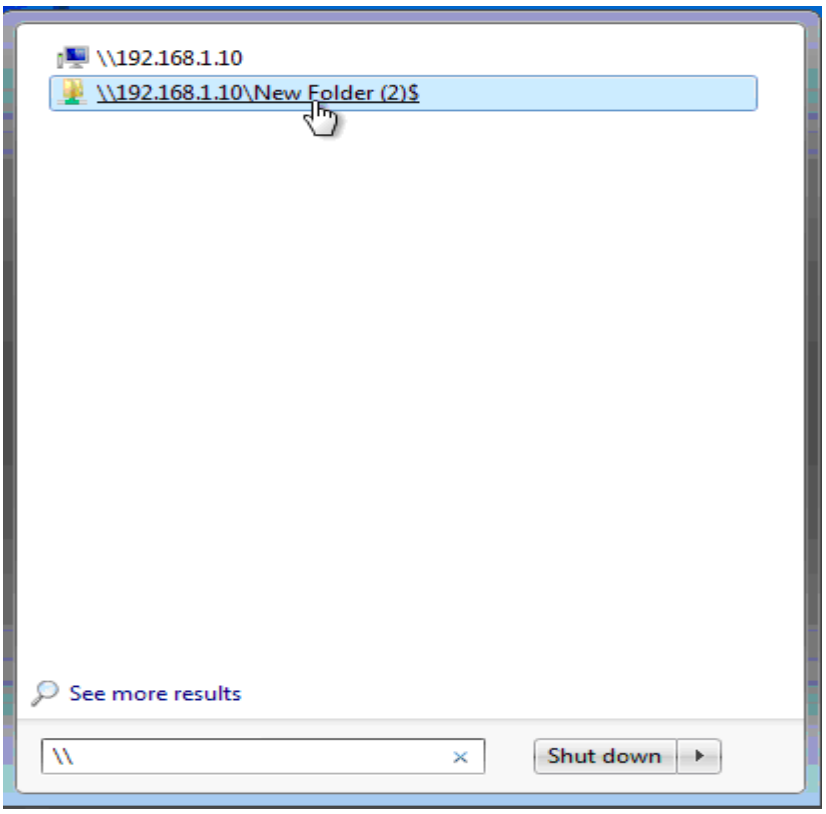


Tương tự Add thêm User phat và Set quyền cho User này là Allow tất cả mọi quyền.

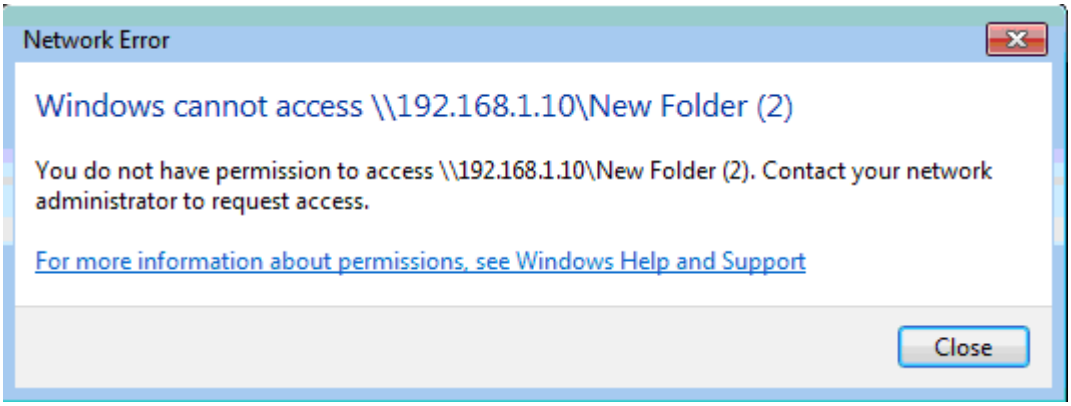


Để tạo một thư mục mà không muốn cho ai thấy (chỉ có gõ lệnh mới vào được) thì thêm dấu $ vào ngay sau Share Name của mình.

VD: Máy có IP là 192.168.1.10 và thư mục Share có tên là New Folder (2)$. Trong này giả sử ta Add thêm User tai và Set quyền cho User này là Allow tất cả mọi quyền. Khi đó truy cập từ máy khác vào phải nhập là \\172.16.1.10\New Folder (2)$ thì mới vào được.

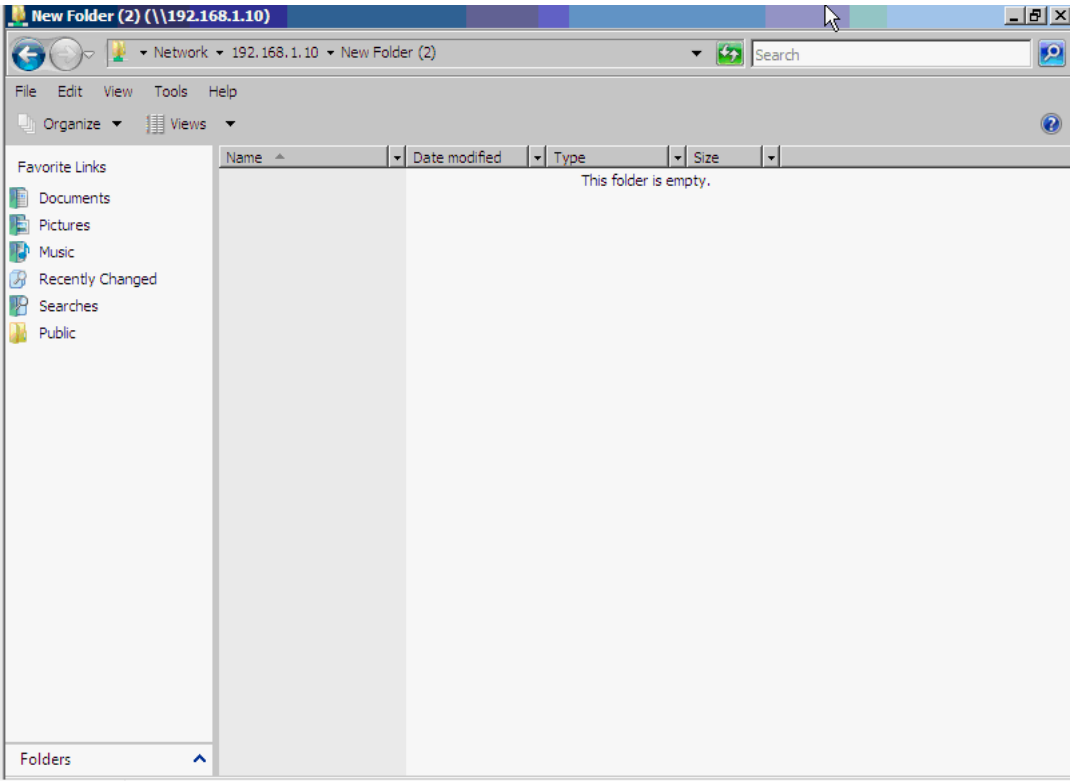


Bây giờ từ một máy Client khác, truy cập thư mục New Folder (2) với User là tai

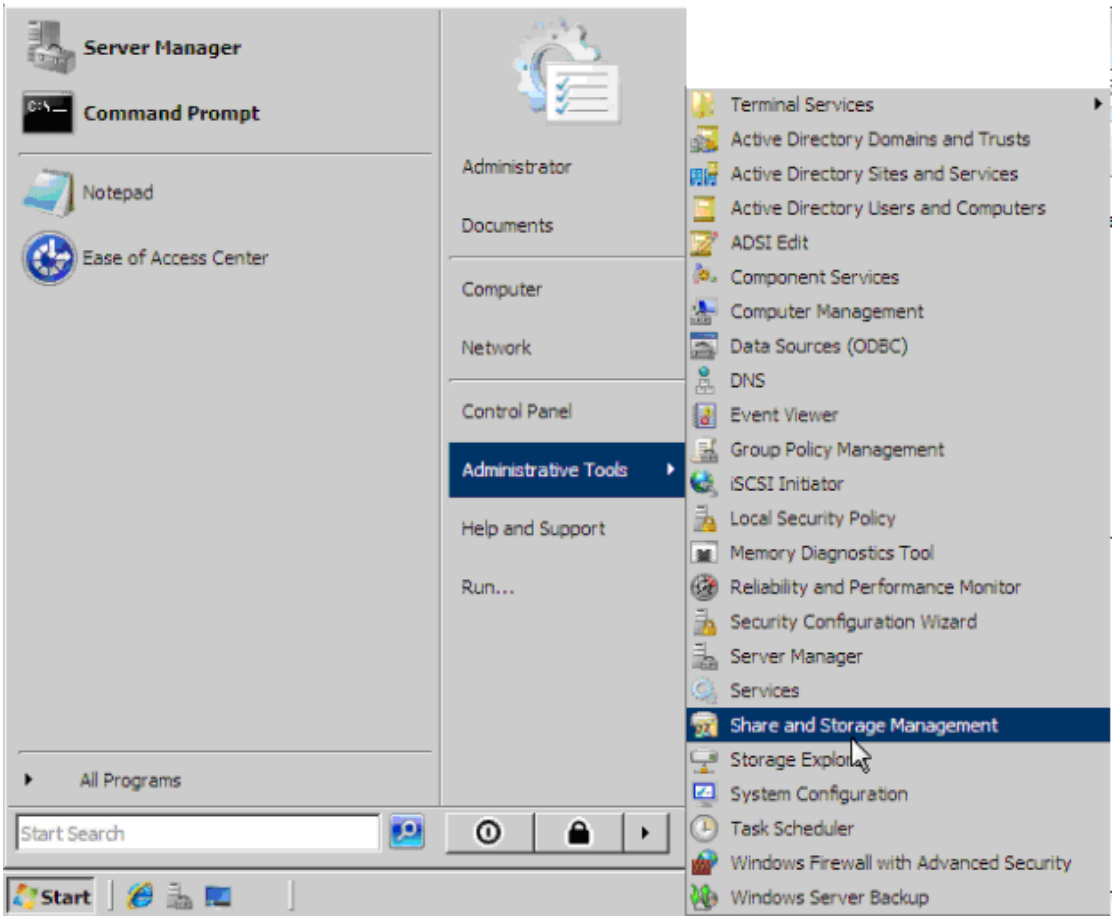


Máy sẽ báo là không có lối vào lý do là đã Set cho User tai bị Deny tất cả.

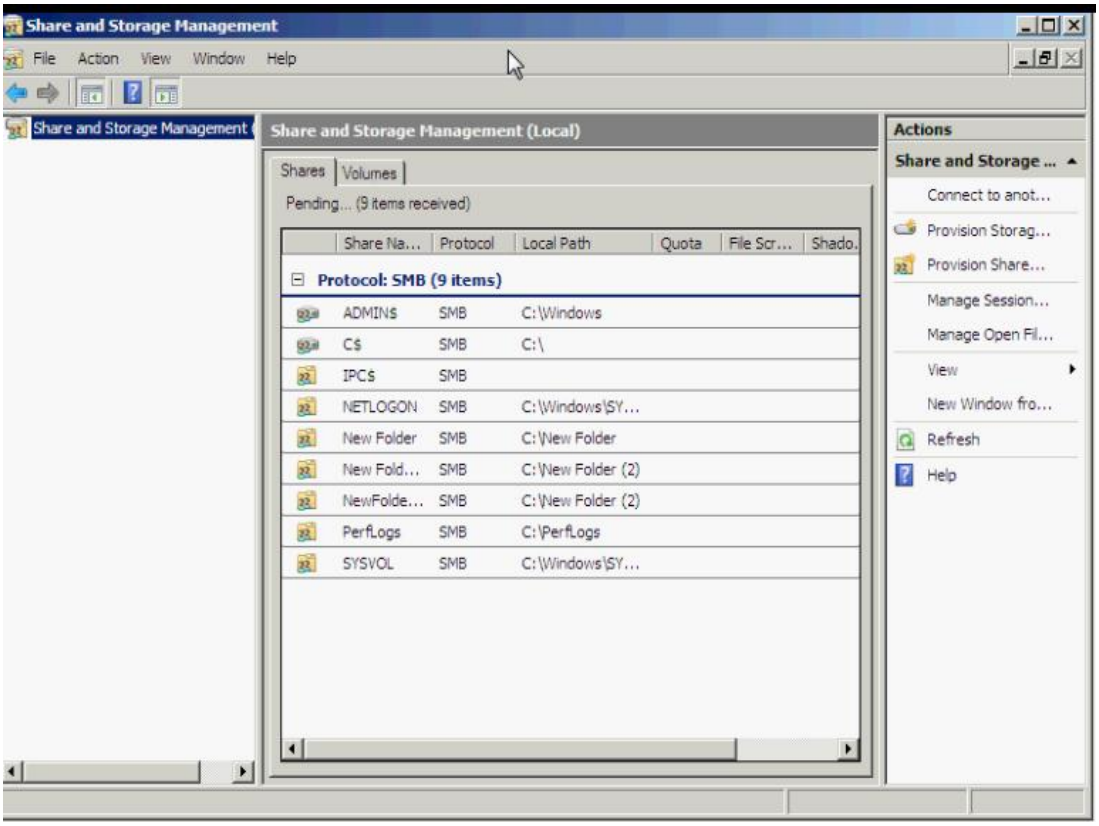
User tai bị từ chối truy cập New Folder (2) . Tuy nhiên với User phat thì có thể xem được các tài nguyên trong này.



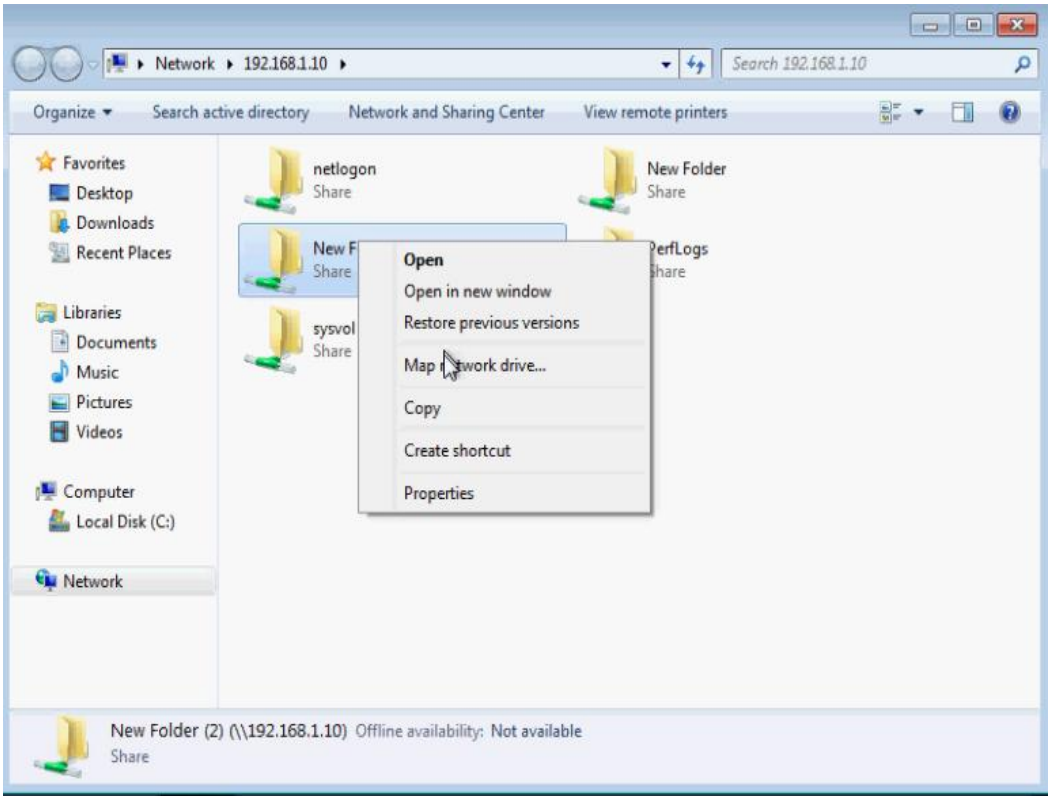
Để xem các thư mục Share ẩn trong Windows, vào **Administrative Tools➔Share and Storage Management.**



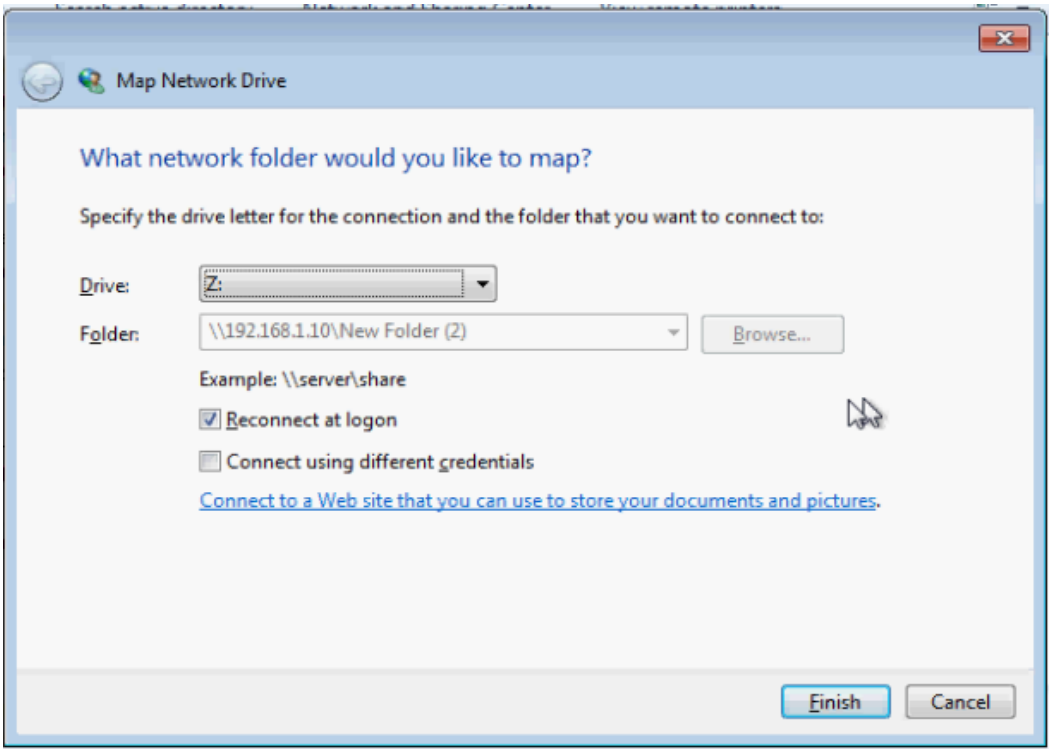
Trong này sẽ liệt kê toàn bộ các thư mục đã Share trước đó.



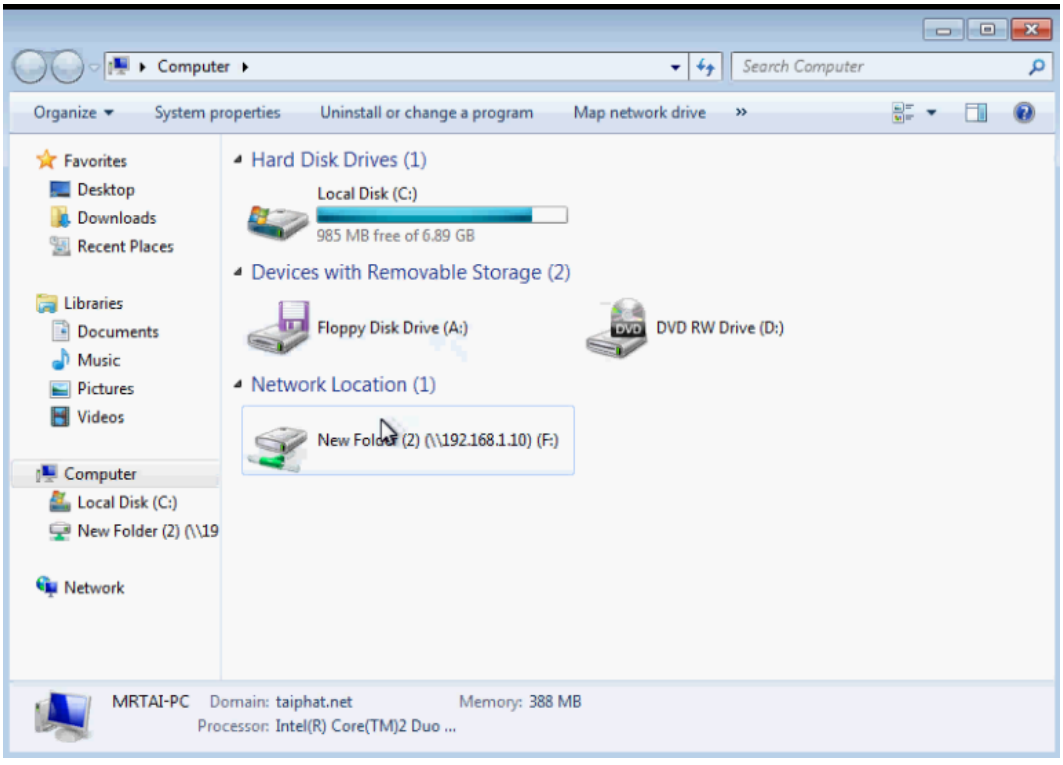
Để tránh phải mất công nhập dòng lệnh \\[IP máy tới]\[thư mục share] chúng ta có thể ánh xạ ổ đĩa đối với các thư mục Share thường xuyên truy cập bằng cách nhấp phải vào thư mục đã Share cần ánh xạ và chọn Map Network Drive…



Trong cửa sổ Map Nerwork Drive hiện ra bạn chọn tên ổ đĩa ánh xạ và click Finish.



Vào Computer sẽ thấy xuất hiện thêm ổ đĩa mới (Ổ đĩa ánh xạ). Nhấp vào đấy sẽ đi đến ngay thư mục mà bạn vừa ánh xạ.



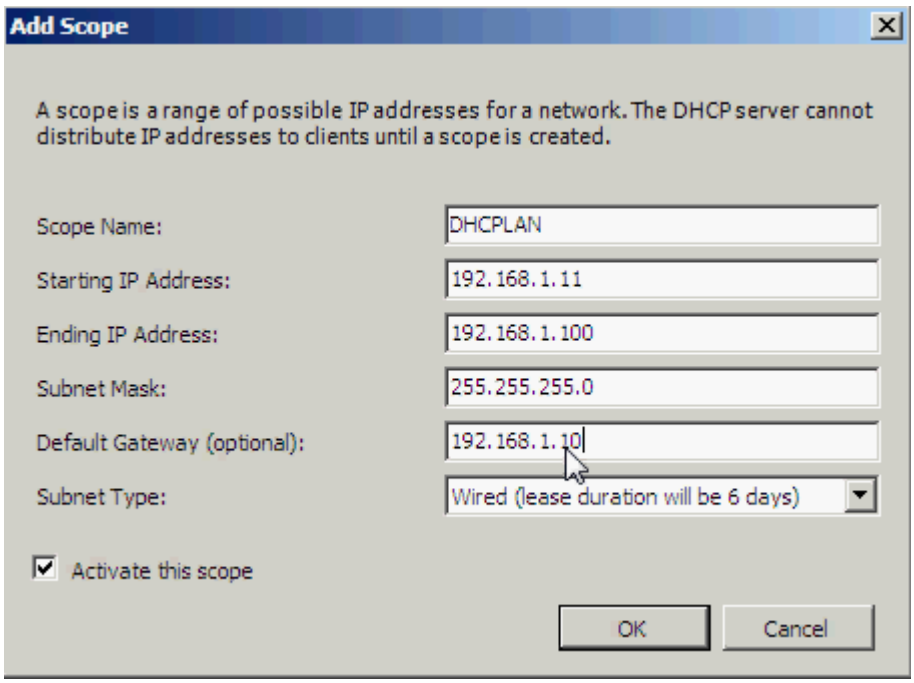
CHƯƠNG 7: XÂY DỰNG MÔ HÌNH MẠNG MỘT CÔNG TY

I. CẤU HÌNH DỊA CHỈ IP, DHCP,DNS

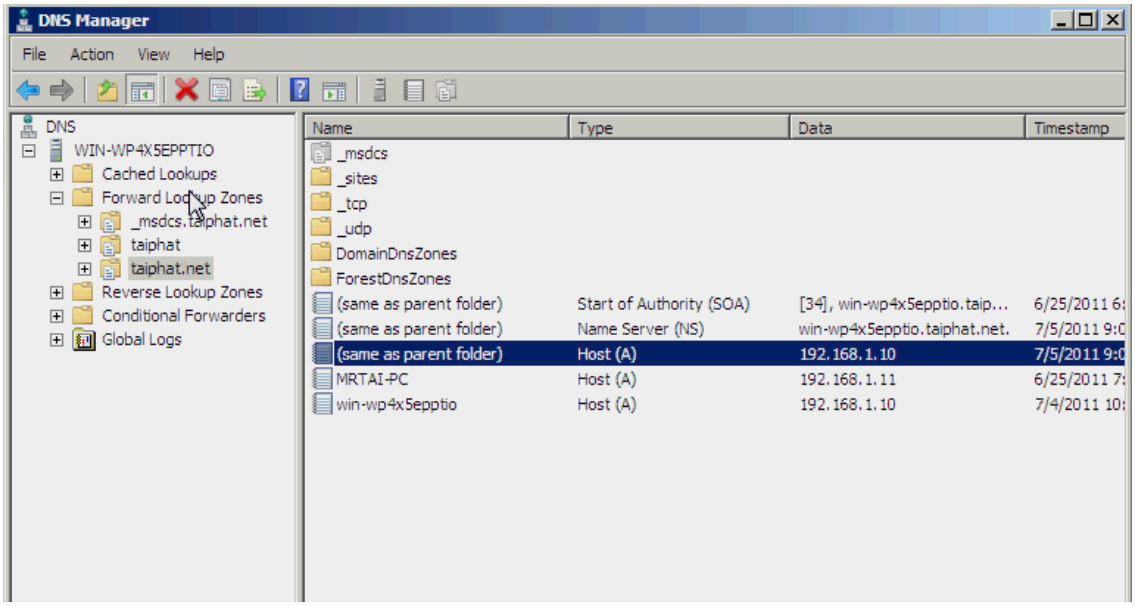
1. Cấu hình địa chỉ IP

	Server	Client
IP address	**192.168.1.10**	**192.168.1.11 ➔30**
Subnet mask	**255.255.255.0**	**255.255.255.0**
Default gateway	**192.168.1.10**	**192.168.1.10**
Preferred DNS	**192.168.1.10**	**192.168.1.10**

2. Cấu hình DHCP

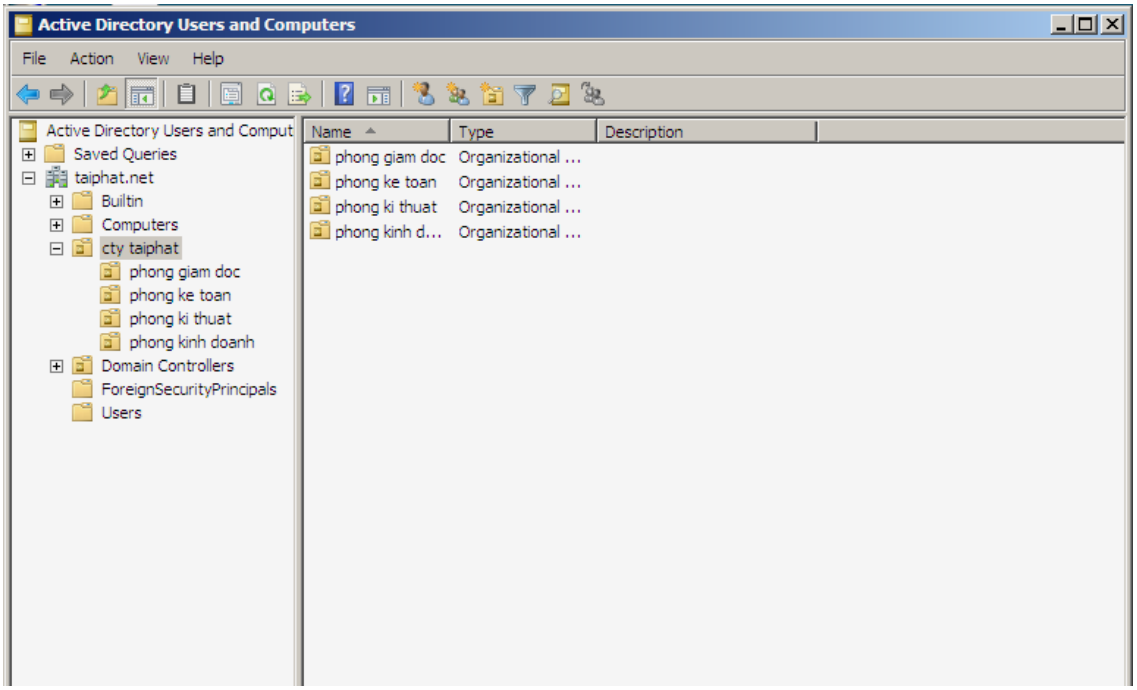


3.Cấu hình DNS

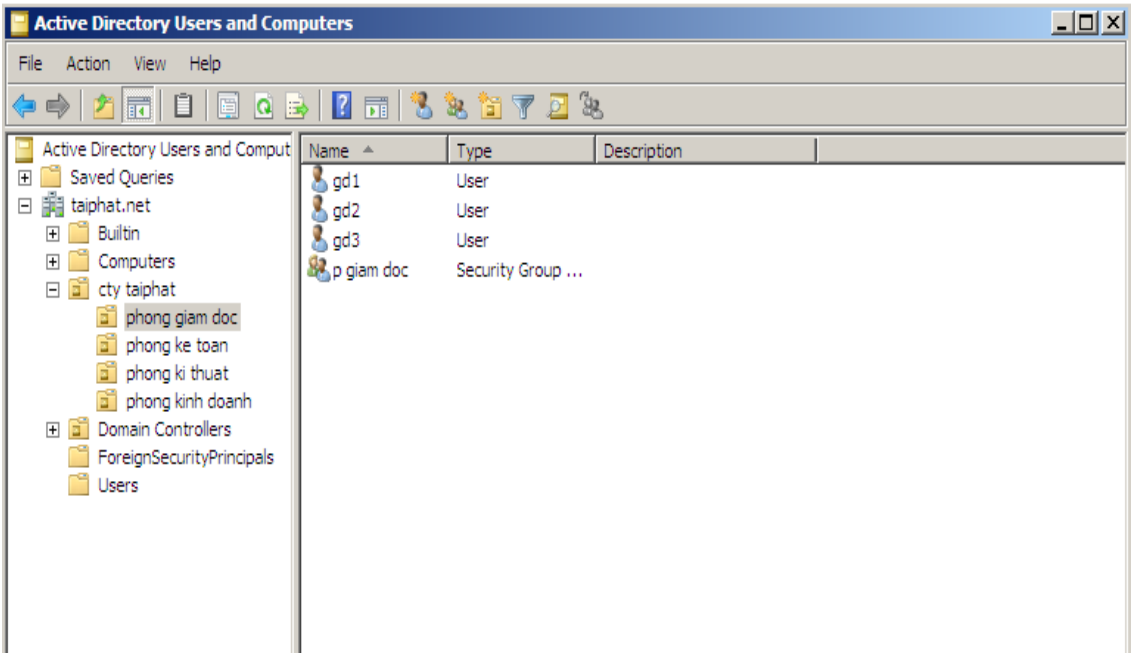


II. TẠO OU,USER VÀ GROUP

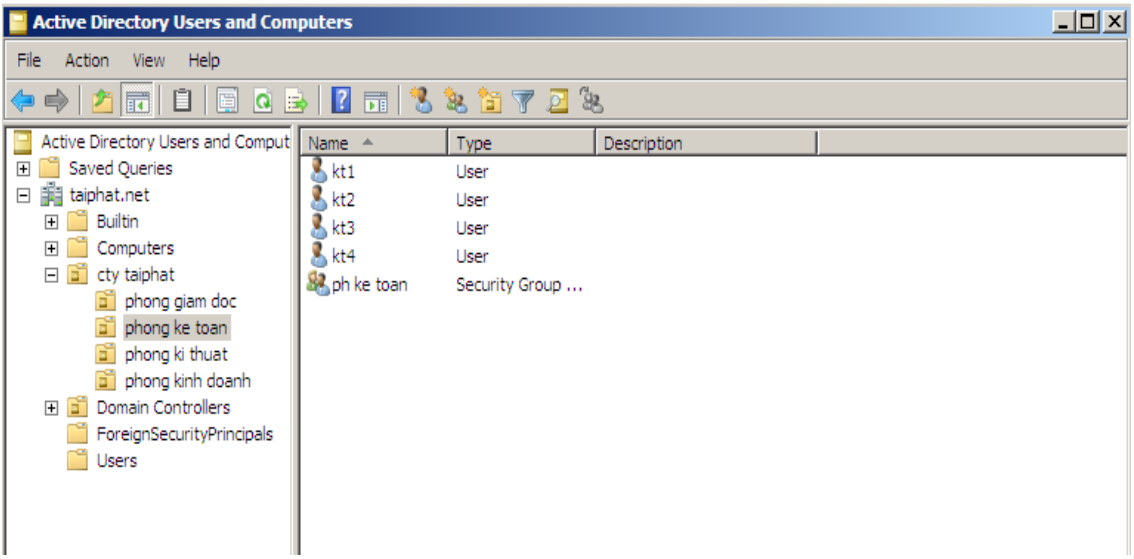
Công ty taiphat gồm 4 phòng : Phòng Giám Đốc , Phòng Kế Toán , Phòng Kỹ Thuật , Phòng Kinh Doanh.



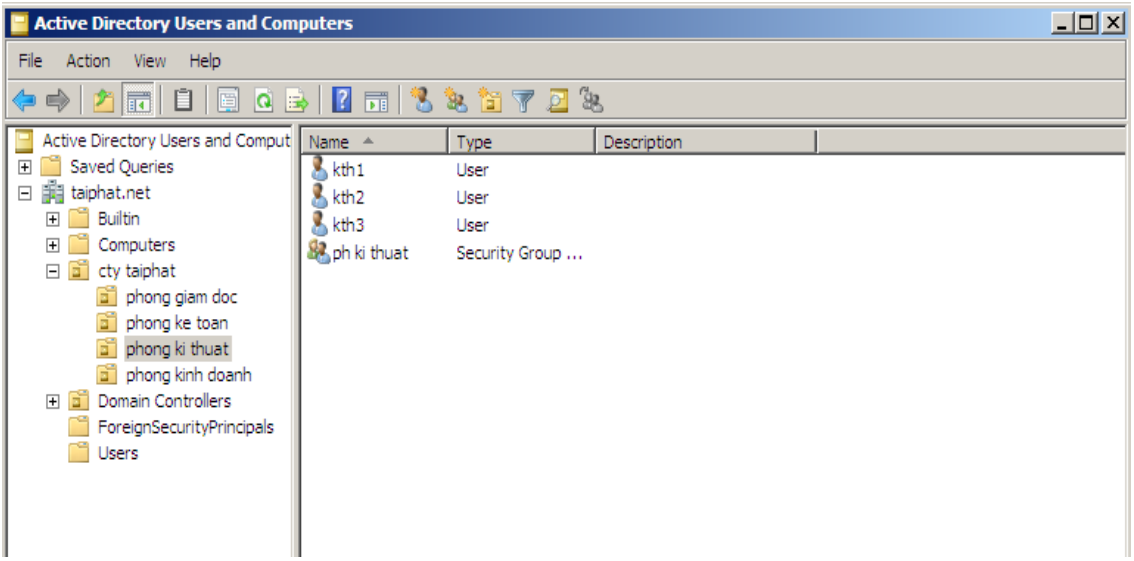
Phòng Giám Đốc gồm 3 user : gd1, gd2, gd3.



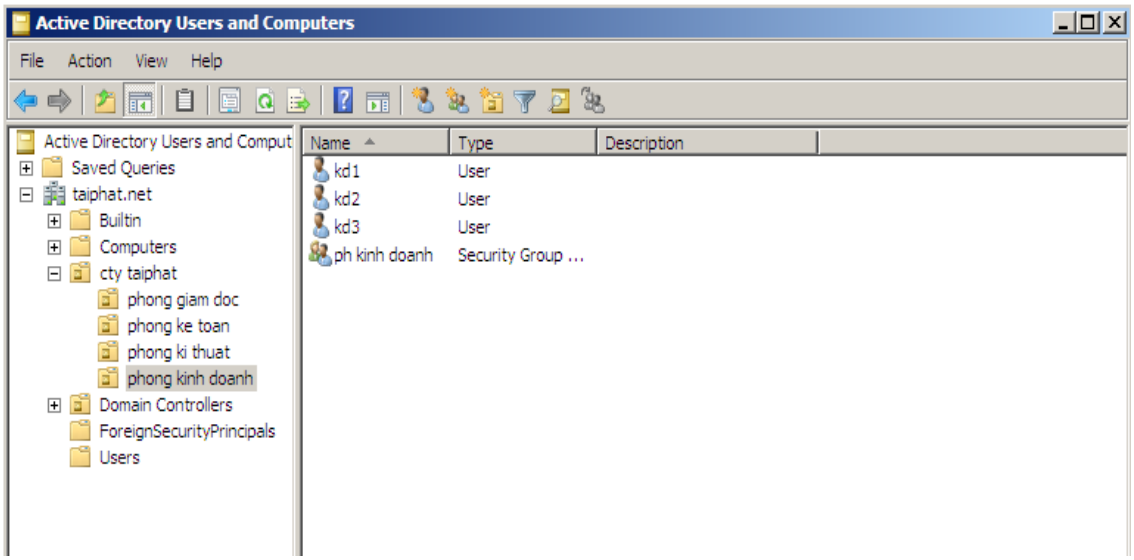
Phòng Kế toán gồm 4 user : kt1, kt2, kt3, kt4.



Phòng Kỹ thuật gồm 3 user : kth1, kth2, kth3.

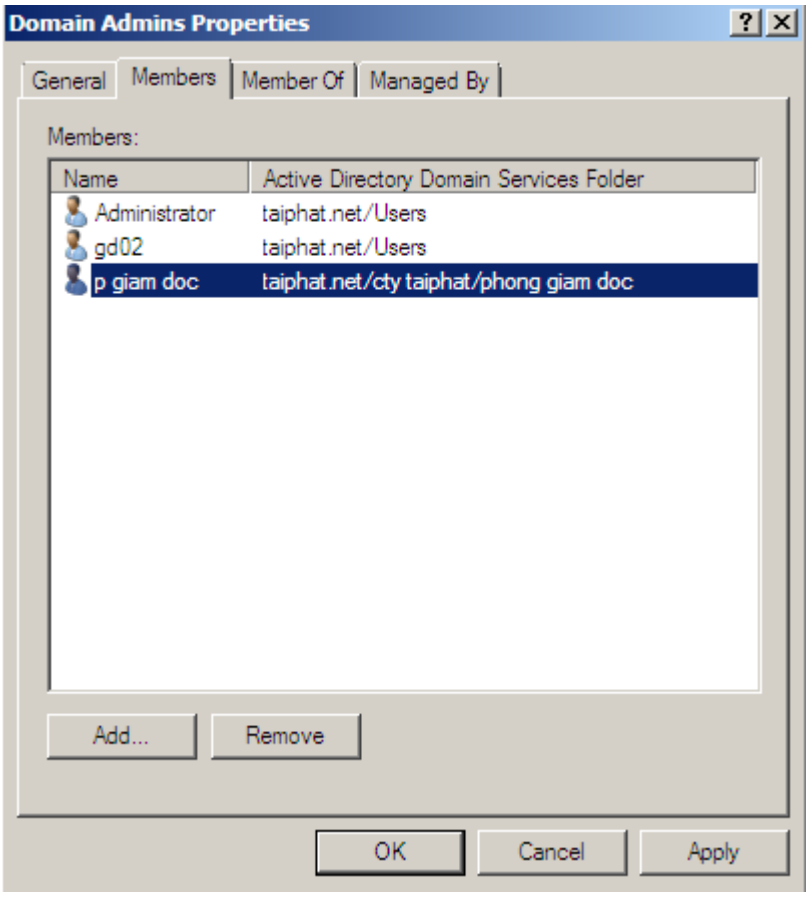


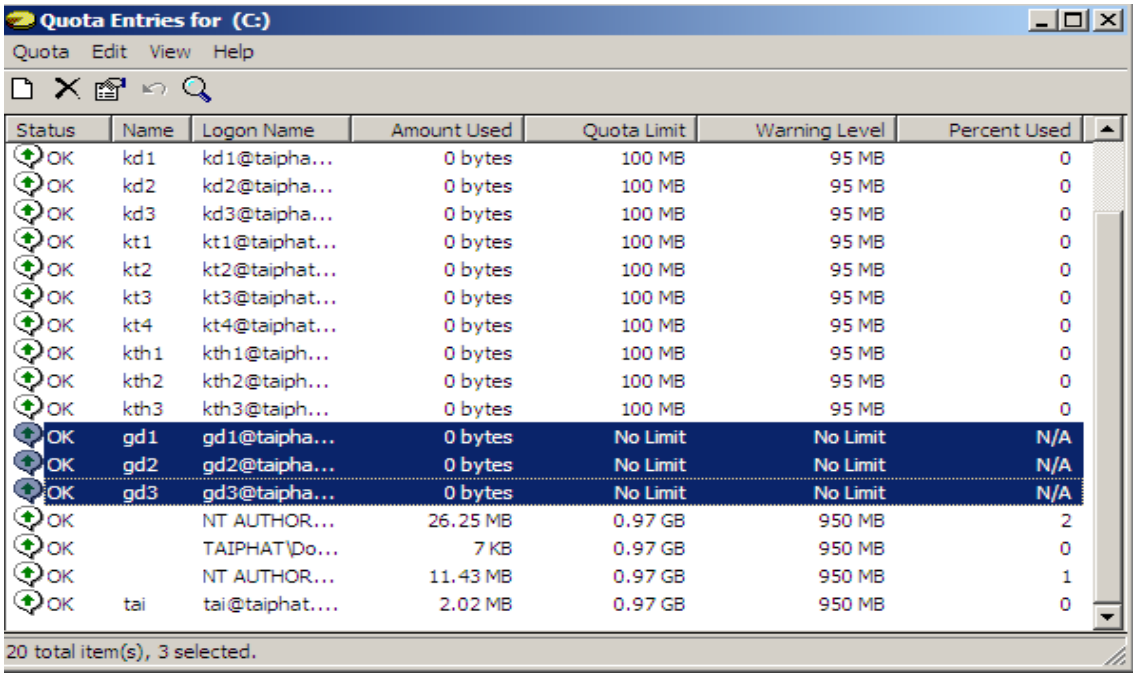
Kinh Doanh gồm 3 user : kd1, kd2 , kd3.

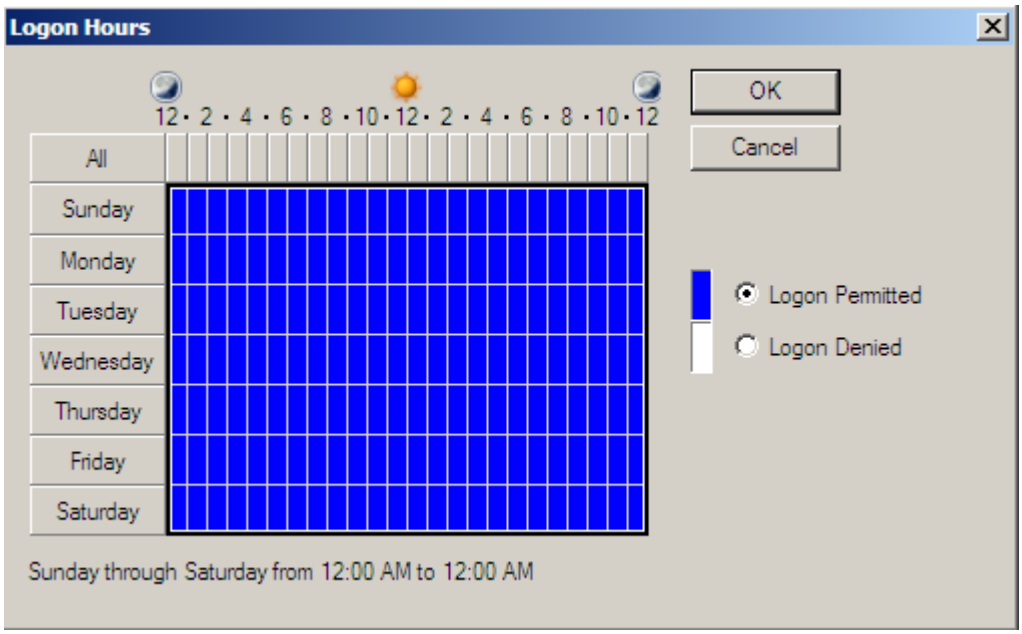


III. GROUP POLICY,DICK QUOTA

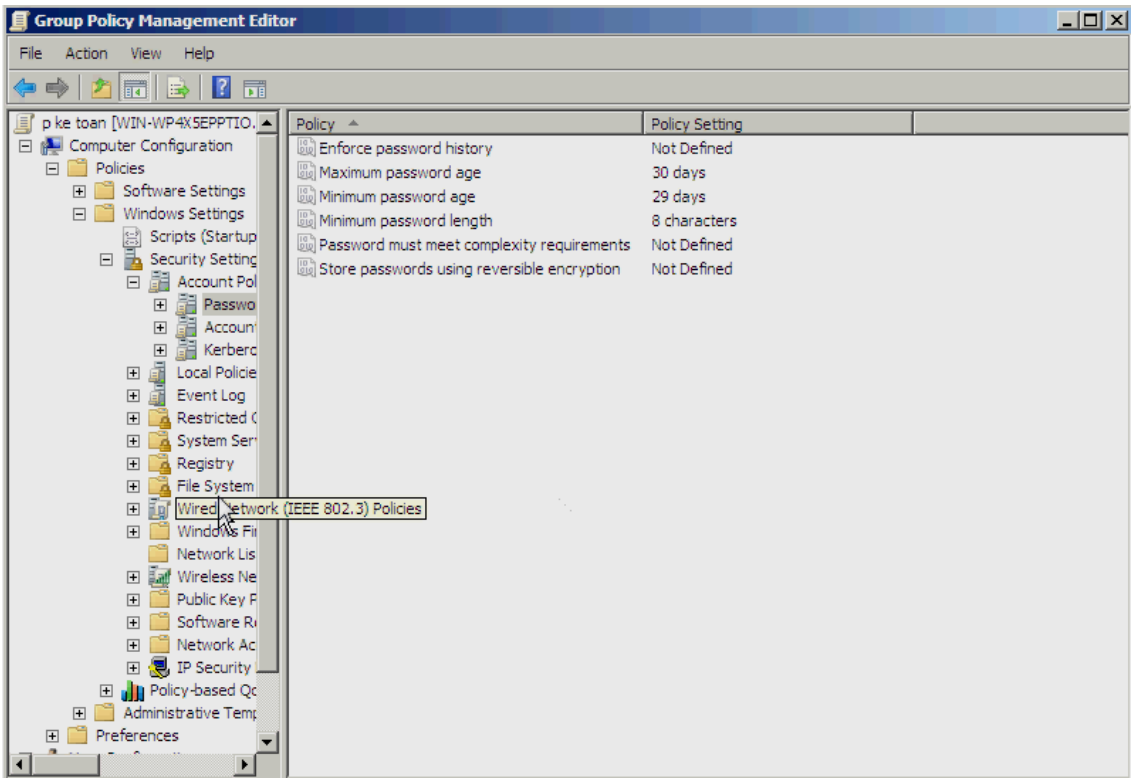
1. Phòng Giám Đốc : các user của phòng giám đốc có toàn quyền trên domain và dung lượng ỗ đĩa không giới hạn, không qui định thời gian vào mạng.



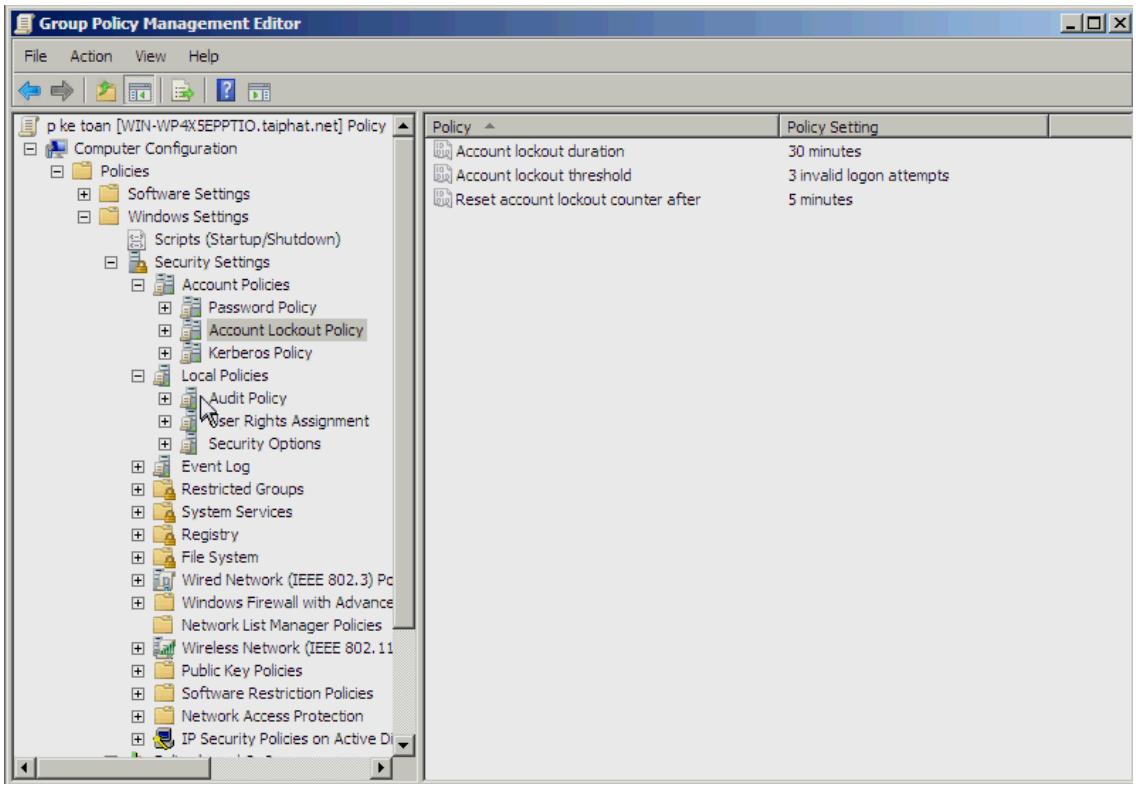




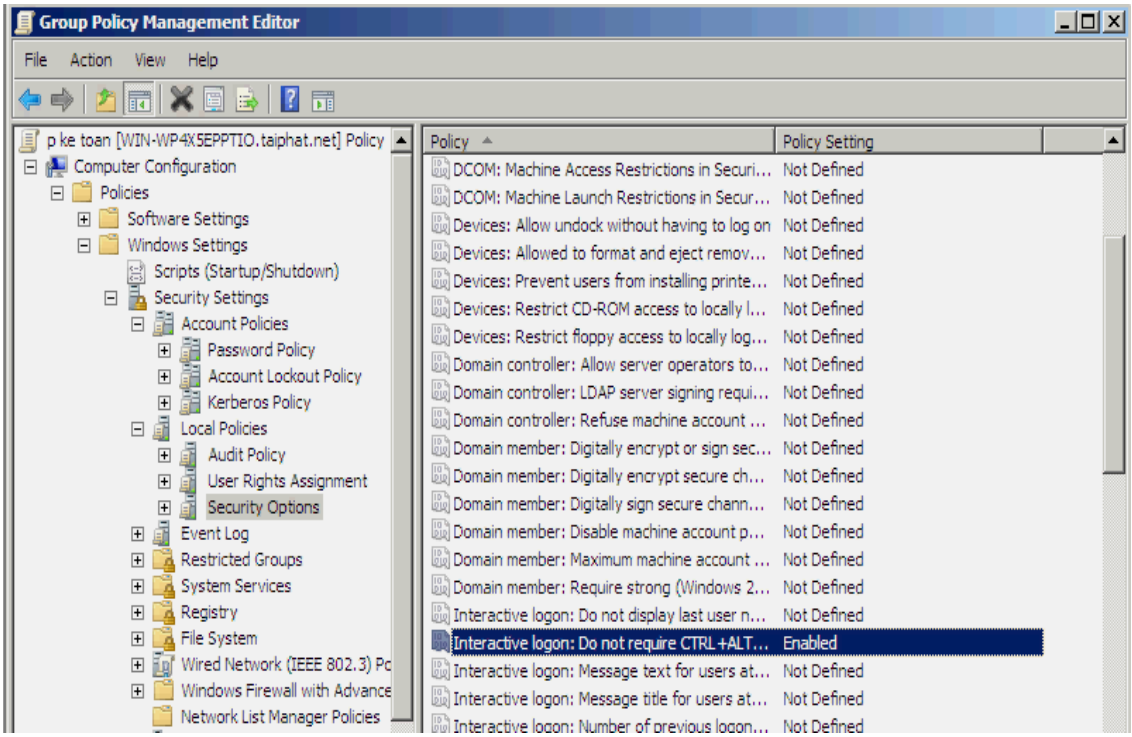
2. Phòng Kế Toán : các user thuộc phòng kế toán có các yêu cầu là mật khẩu ít nhất phải 8 kí tự, thời gian thay đổi mật khẩu là 30 ngày, người dùng đăng nhập sai 3 lần sẽ bị khóa account, thời gian khóa sẽ là 5 phút, user không phải ấn tổ hợp phím Ctrl+Alt+Del khi đăng nhập, dung lượng ổ đĩa tối đa là 100 MB, thời gian vào mạng từ 8h sang -> 14h các ngày thứ hai, tư , sáu.



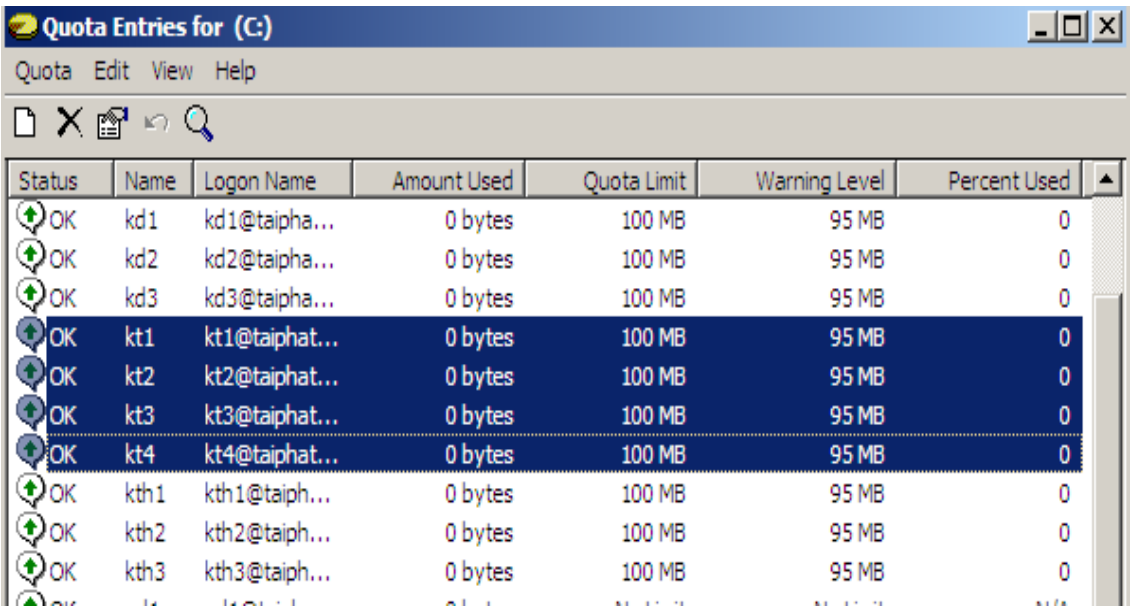
Mật khẩu ít nhất 8 kí tự, thời gian thay đổi mật khẩu là 30 ngày



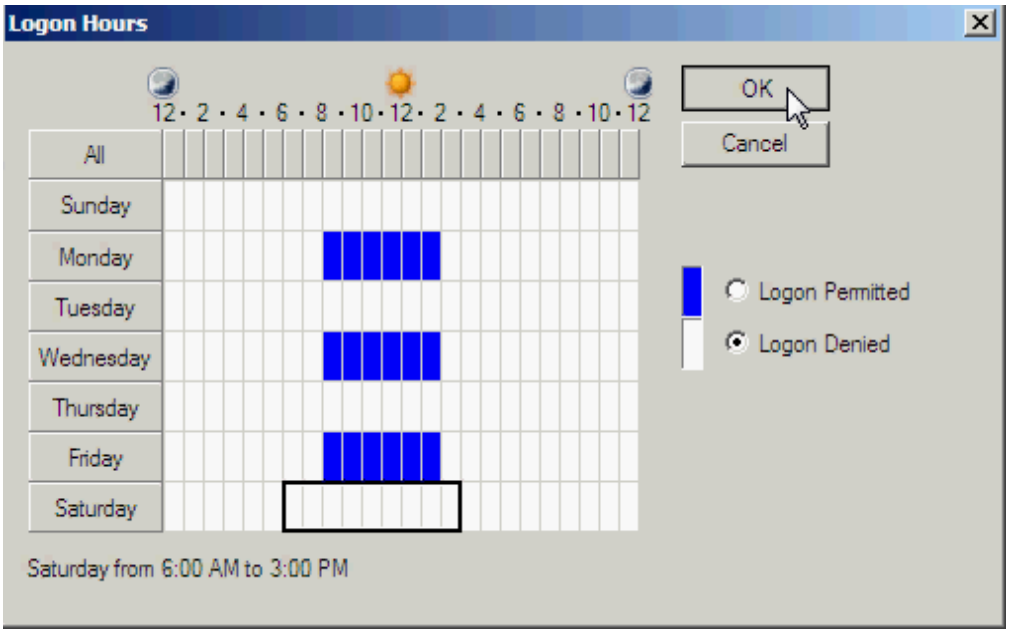
người dùng đăng nhập sai 3 lần sẽ bị khóa account, thời gian khóa sẽ là 5 phút



user không phải ấn tổ hợp phím Ctrl+Alt+Del khi đăng nhập

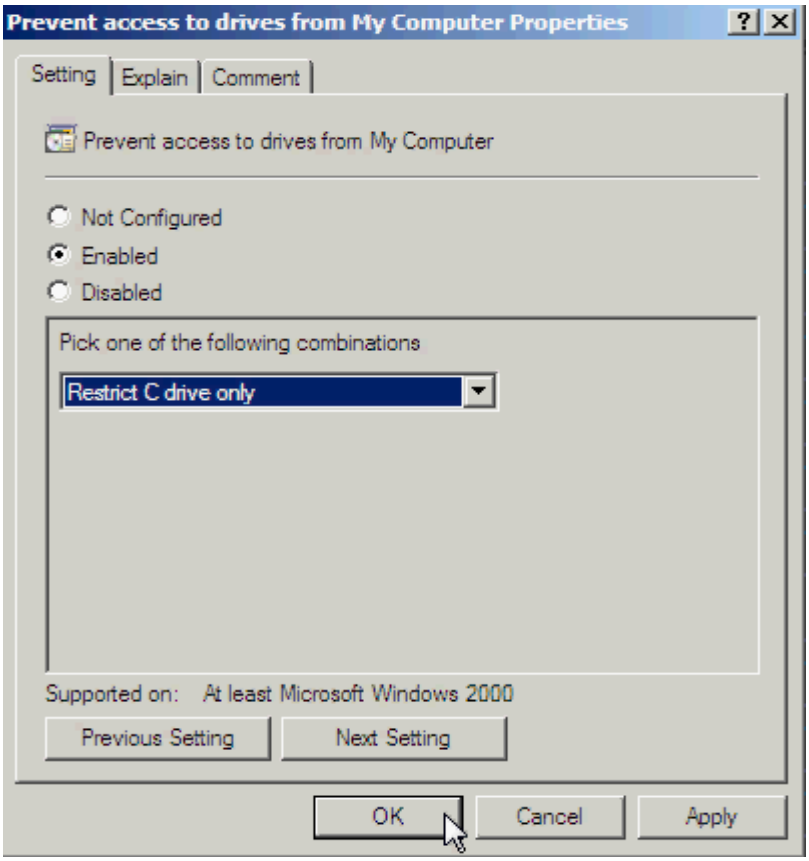


dung lượng ỗ đĩa tối đa là 100 MB

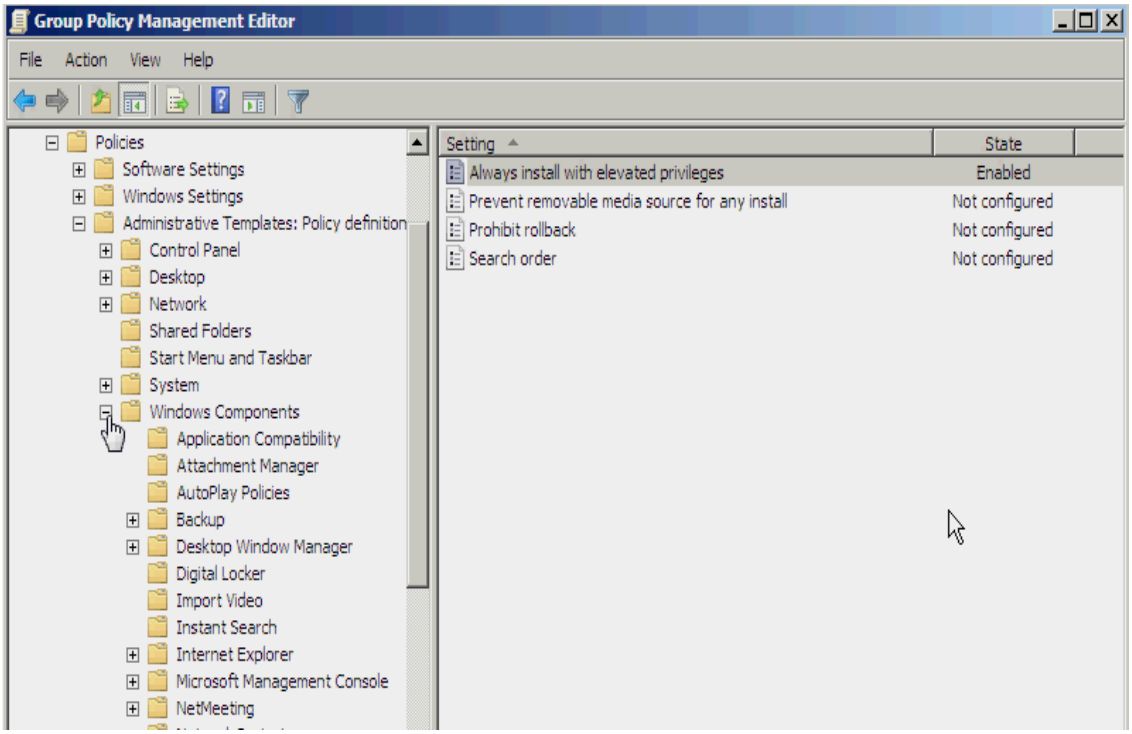


thời gian vào mạng từ 8h sang -> 14h các ngày thứ hai, tư , sáu

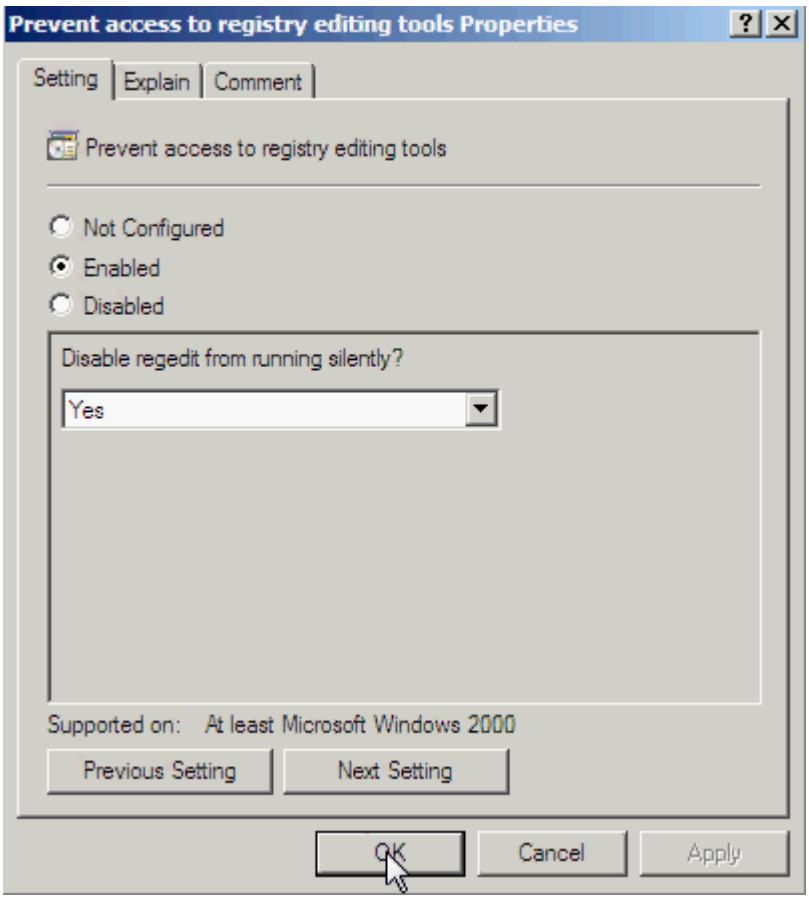
3. Phòng Kinh Doanh : Không cho phép user trên Client truy cập vào ỗ chứa hệ điều hành (ỗ C), không được cài đặt chương trình, không được truy cập vào registry, không được truy cập Control Panel trên máy Client, dung lượng ỗ đĩa tối đa là 100 MB, thời gian đăng nhập từ 8h -> 15h thứ ba, năm , bảy



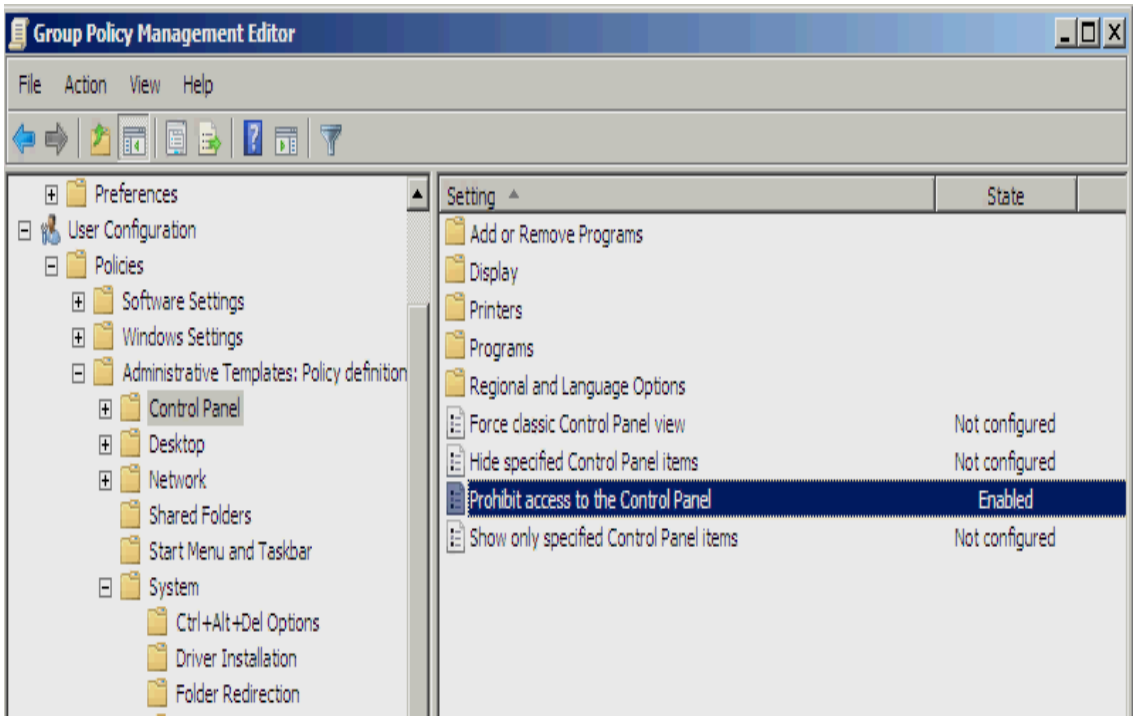
Không cho phép user trên Client truy cập vào ổ chứa hệ điều hành (ổ C)



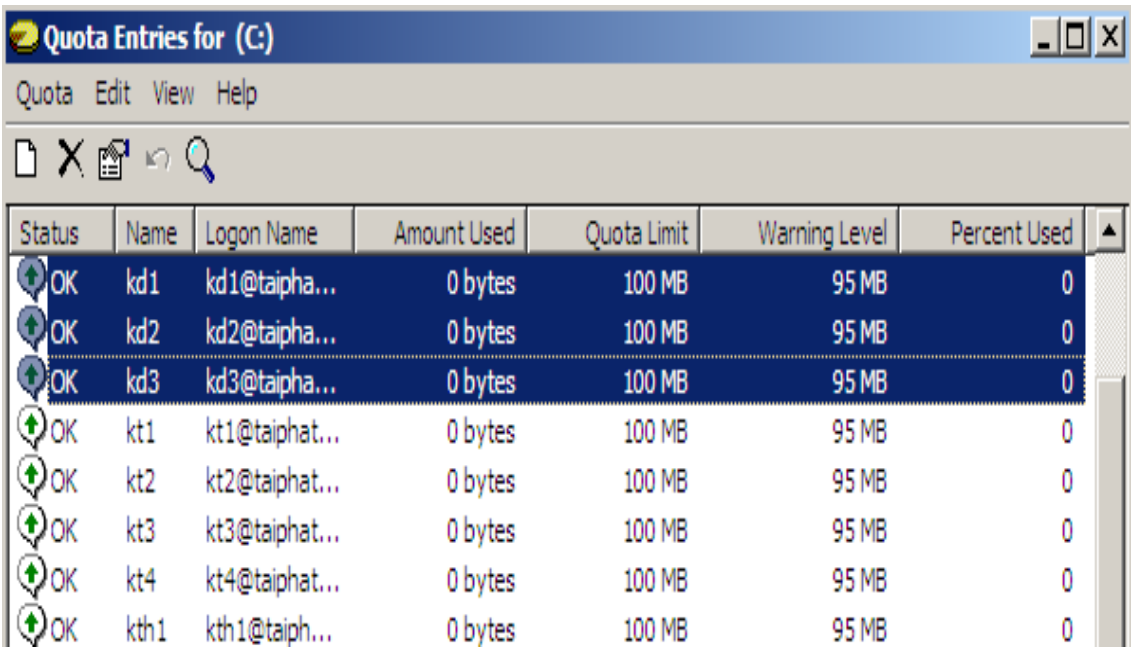
không được cài đặt chương trình



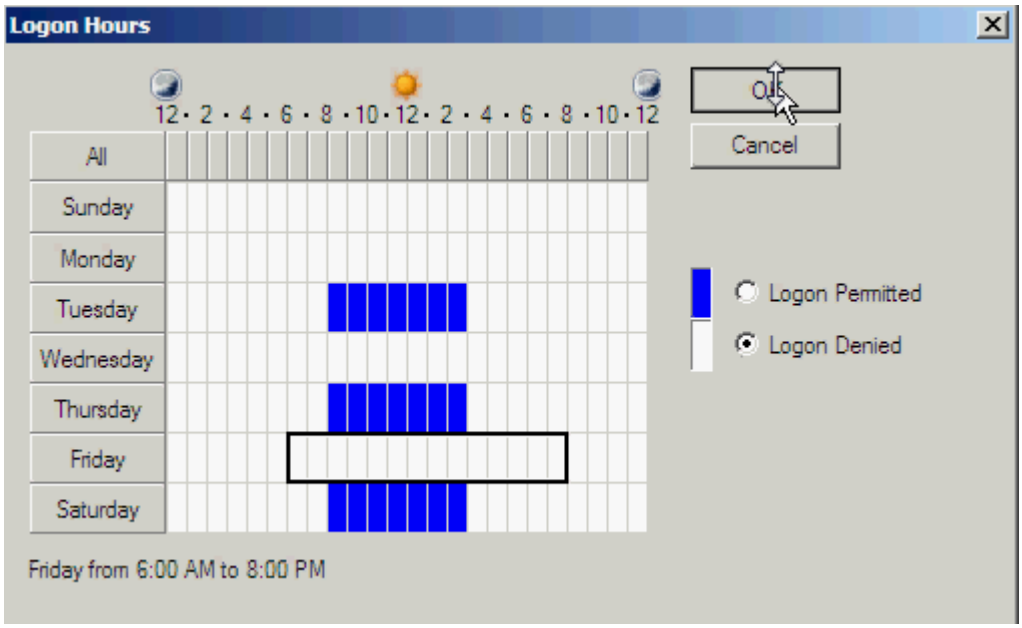
không được truy cập vào registry



không được truy cập Control Panel trên máy Client

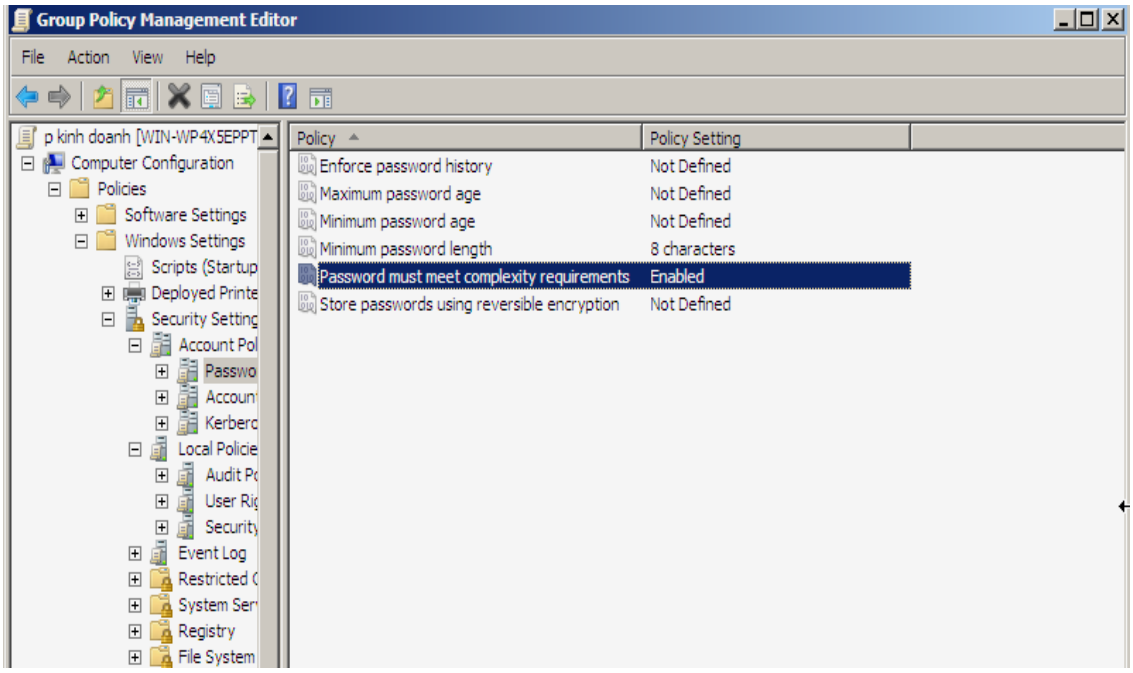


dung lượng ỗ đĩa tối đa là 100 MB

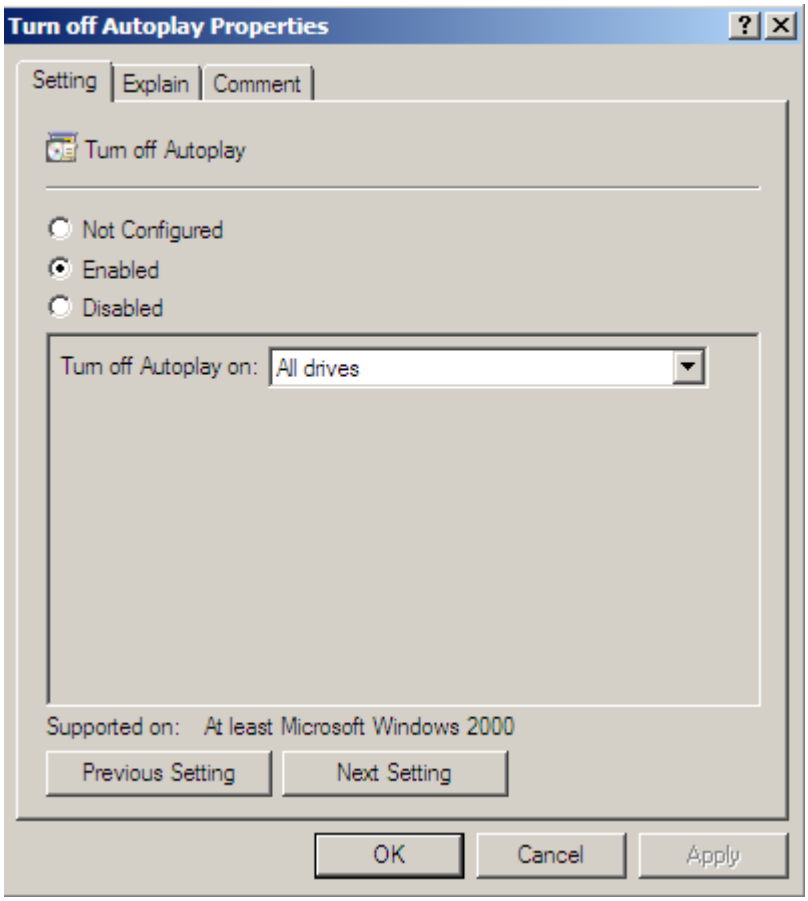


thời gian đăng nhập từ 8h -> 15h thứ ba, năm , bảy

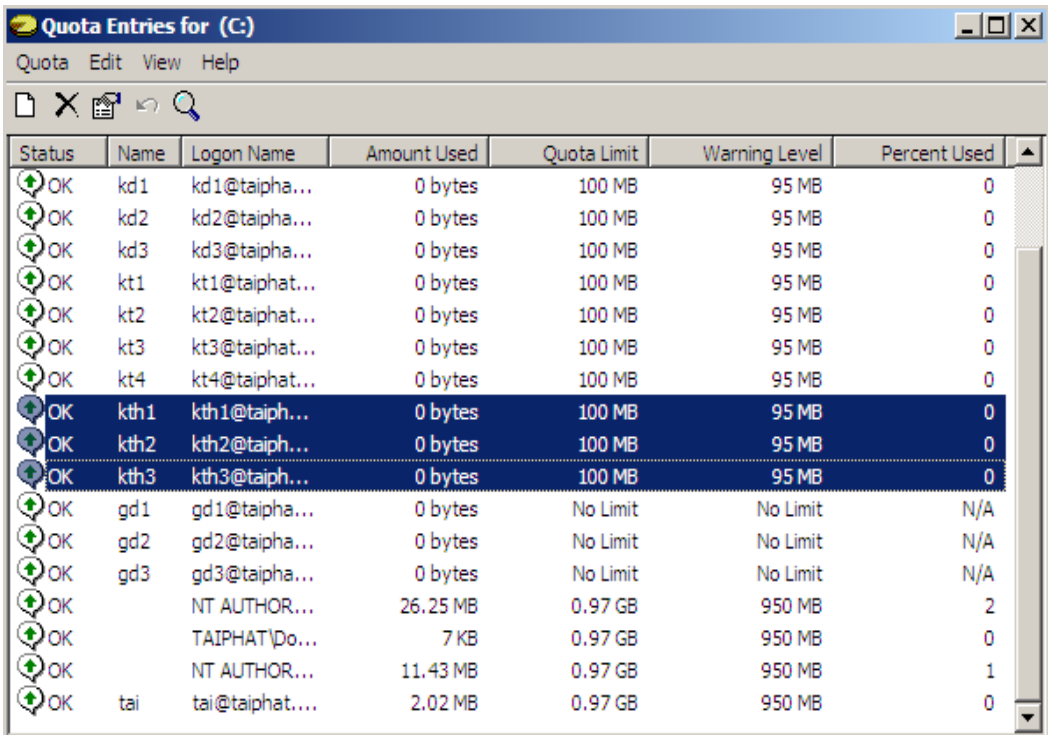
4. Phòng Kỹ Thuật : mật khẩu ngoài viêc có 8 ký tự trở lên thì còn phải có mật khẩu khó, tức là phải có thêm các ký tự (- _ ? / …). Không cho phép Auto play tất cả các loại ỗ đĩa kể cả USB. Dung lượng ỗ đĩa tối đa là 100MB . Thời gian vào mạng từ 5h -> 10h và từ 13h -> 18h các ngày thứ hai, năm , bảy , chủ nhật



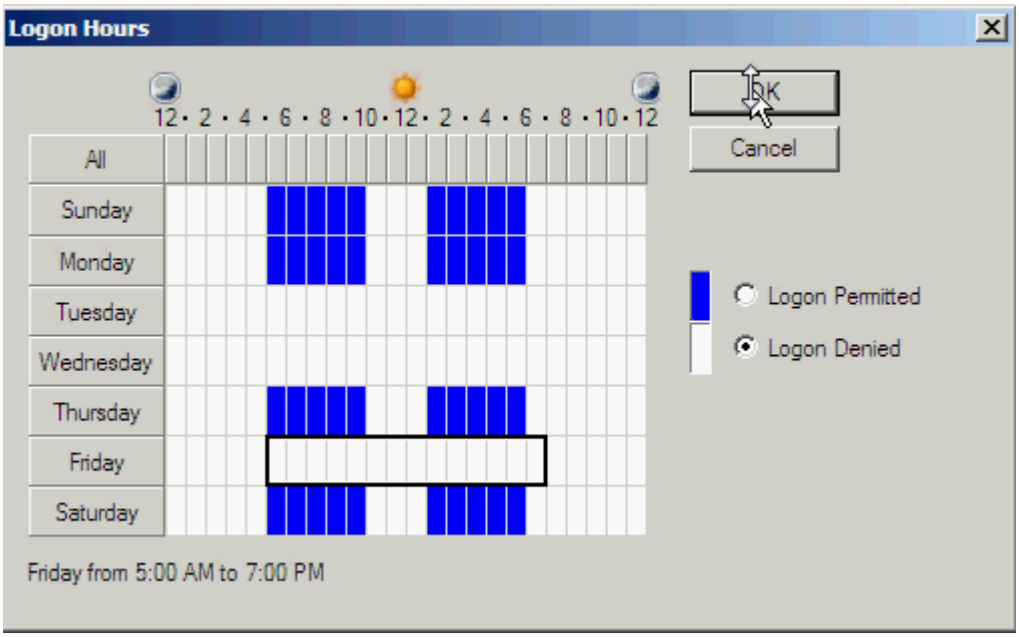
mật khẩu có 8 ký tự trở lên, phải có mật khẩu khó



Không cho phép Auto play tất cả các loại ỗ đĩa kể cả USB



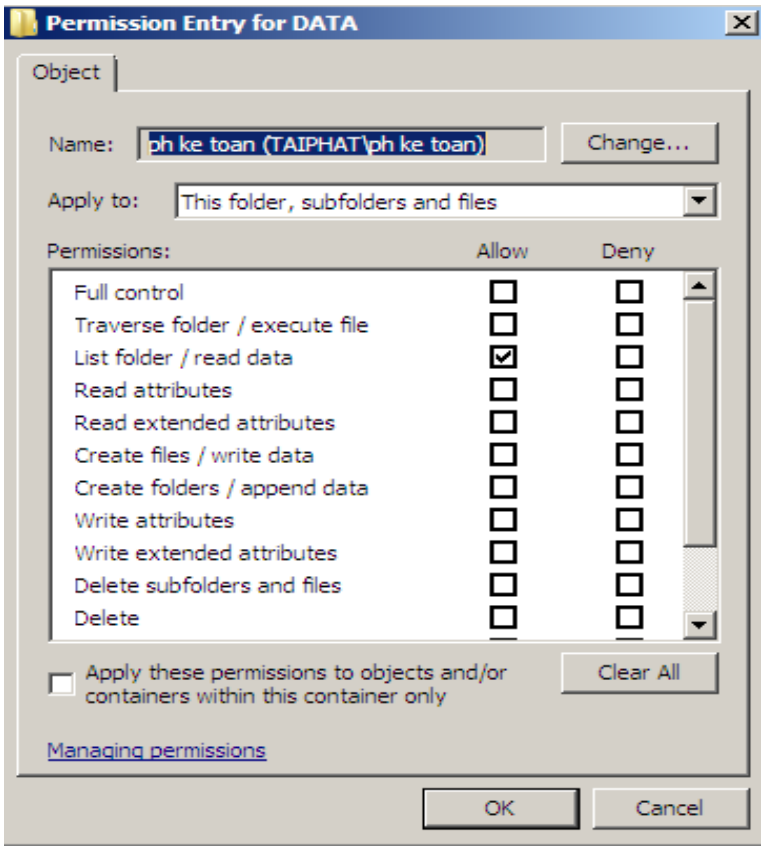
Dung lượng ổ đĩa tối đa là 100MB

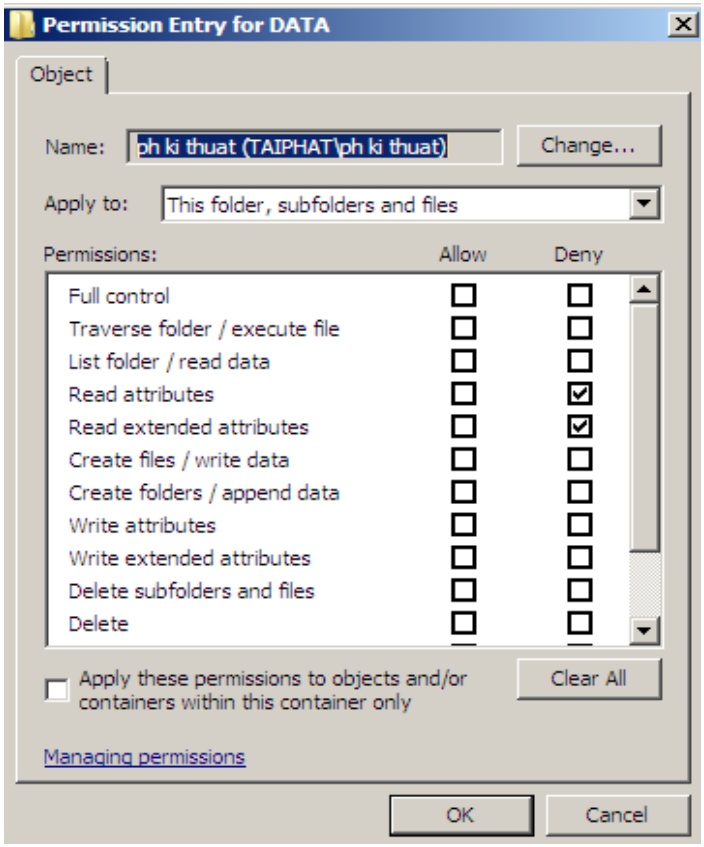


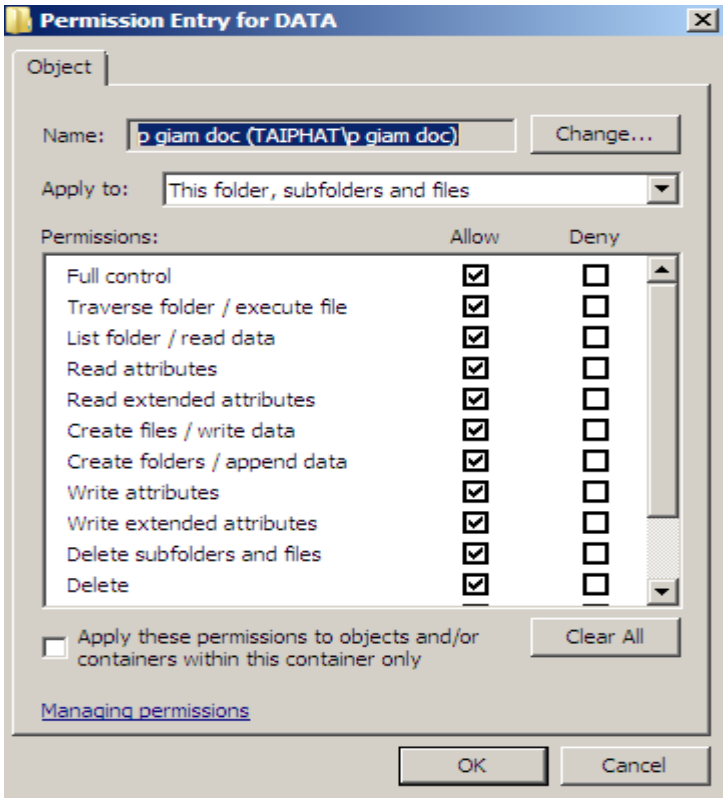
Thời gian vào mạng từ 5h -> 10h và từ 13h -> 18h các ngày thứ hai, năm , bảy , chủ nhật

IV. CHIA SẺ DỮ LIỆU

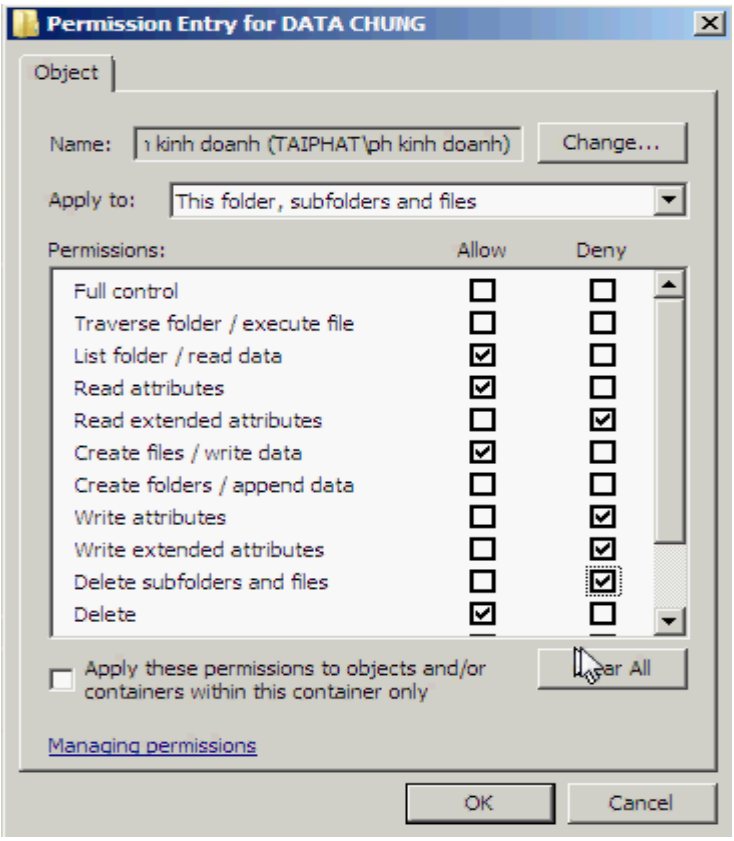
- **Thiết lặp permission trên thư mục DATA :** cho phép các user ở phòng Kế Toán, phòng Kinh Doanh, phòng Kỹ Thuật, chỉ được phép đọc dữ liệu, nhưng không được đọc các thuộc tính, và các thuộc tính mở rộng, các user ở phòng Giám Đốc thì toàn quyền.


Permission Entry for DATA
Object
Name:
ph ke toan (TAIPHAT\ph ke toan)
Change...
Apply to:
This folder, subfolders and files
Permissions:
Allow
Deny
Full control
Traverse folder / execute file
List folder / read data
Read attributes
Read extended attributes
Create files / write data
Create folders / append data
Write attributes
Write extended attributes
Delete subfolders and files
Delete
Apply these permissions to objects and/or containers within this container only
Clear All
Managing permissions
OK
Cancel

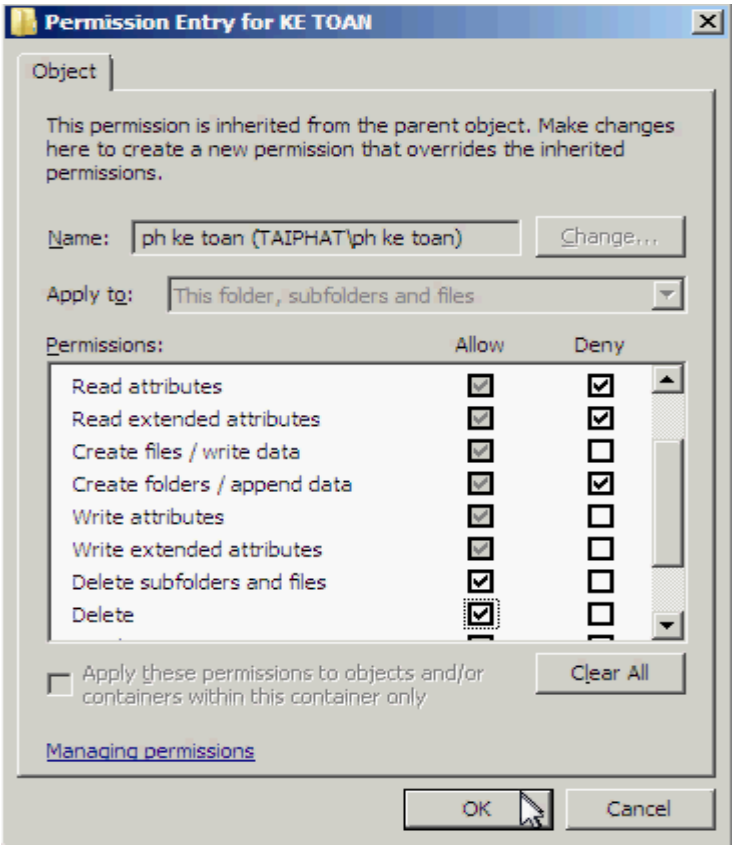

Permission Entry for DATA
Object
Name:
ph ki thuat (TAIPHAT\ph ki thuat)
Change...
Apply to:
This folder, subfolders and files
Permissions:
Allow
Deny
Full control
Traverse folder / execute file
List folder / read data
Read attributes
Read extended attributes
Create files / write data
Create folders / append data
Write attributes
Write extended attributes
Delete subfolders and files
Delete
Apply these permissions to objects and/or containers within this container only
Clear All
Managing permissions
OK
Cancel



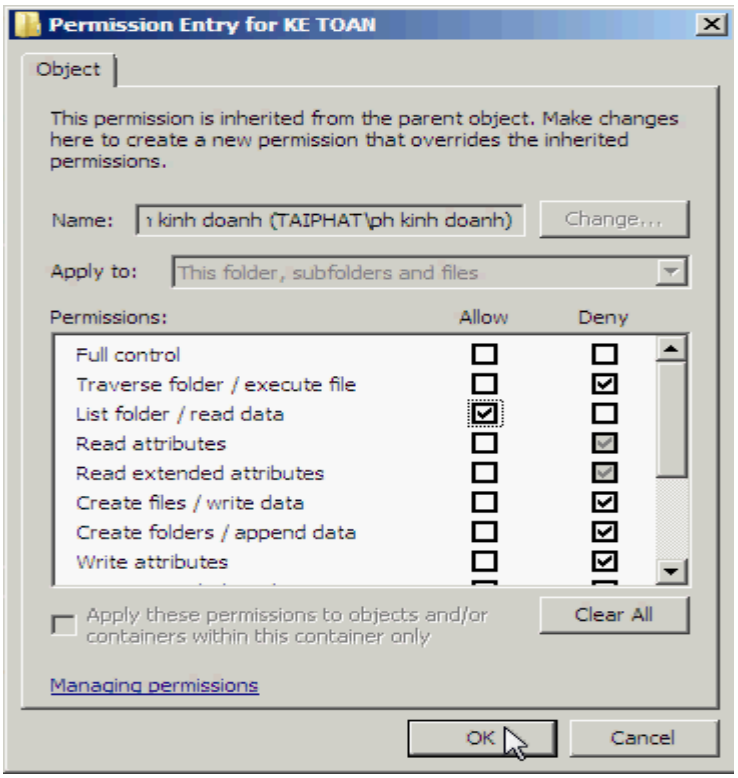
- **Thiết lặp permission trên thư mục DATA chung :** cho phép các user ở phòng Kế Toán, phòng Kinh Doanh, phòng Kỹ Thuật, được phép đọc dữ liệu và đọc các thuộc tính, Được phép tạo file và viết dữ liệu, nhưng không được phép thay đổi các thuộc tính của file và viết các thuộc tính mở rộng, được phép xóa nhưng không được xóa file.



- **Thiết lặp permission trên thư mục Kế Toán :** cho phép các user ở phòng Kế Toán được quyền đọc, nhưng chỉ được đọc dữ liệu không được đọc các thuộc tính của file. Được phép tạo file và viết dữ liệu, và được quyền xóa sửa. Còn các user ở phòng Kinh Doanh và Kỹ Thuật chỉ được phép đọc dữ liệu.

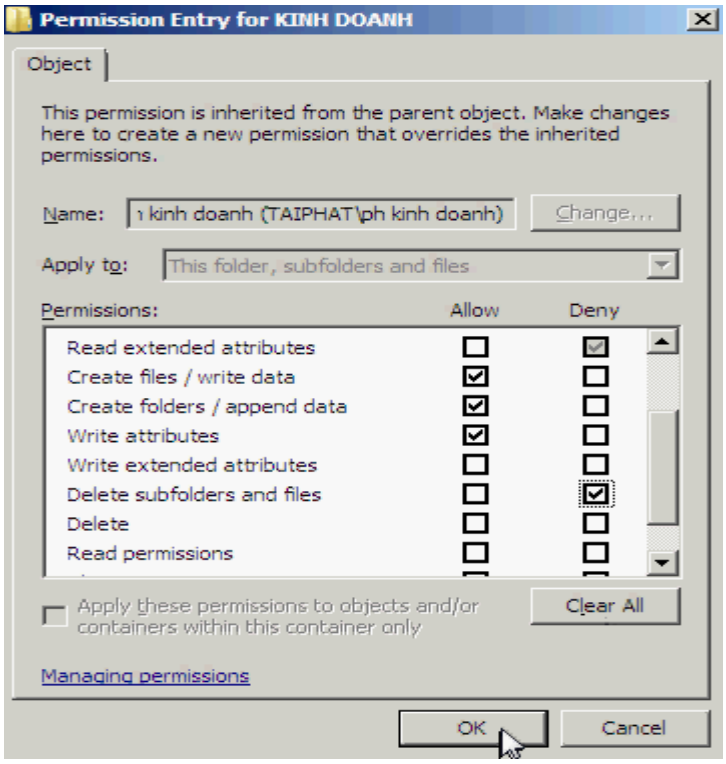


cho phép các user ở phòng Kế Toán được quyền đọc, chỉ được đọc dữ liệu không được đọc các thuộc tính của file. Được phép tạo file và viết dữ liệu, và được quyền xóa sửa

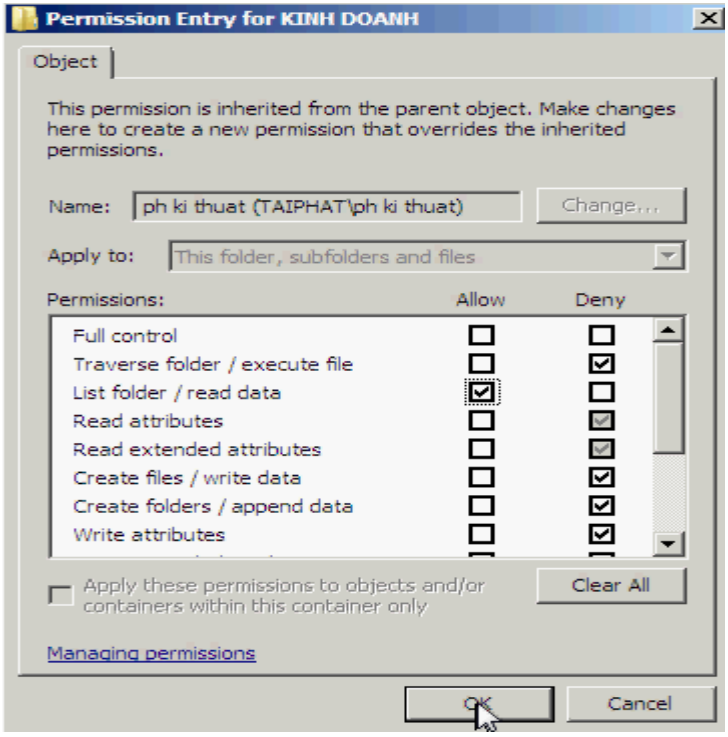


các user ở phòng Kinh Doanh và Kỹ Thuật chỉ được phép đọc dữ liệu.

- **Thiết lặp permission trên thư mục Kinh Doanh :** cho phép các user ở phòng Kinh Doanh được phép đọc dữ liệu và các thuộc tính. Được phép viết dữ liệu,tạo file, folder. Được phép thay đổi các thuộc tính của file và folder nhưng không được phép xóa file và folder. Còn các user ở phòng Kế Toán và phòng Kỹ Thuật chỉ được quyền đọc dữ liệu.

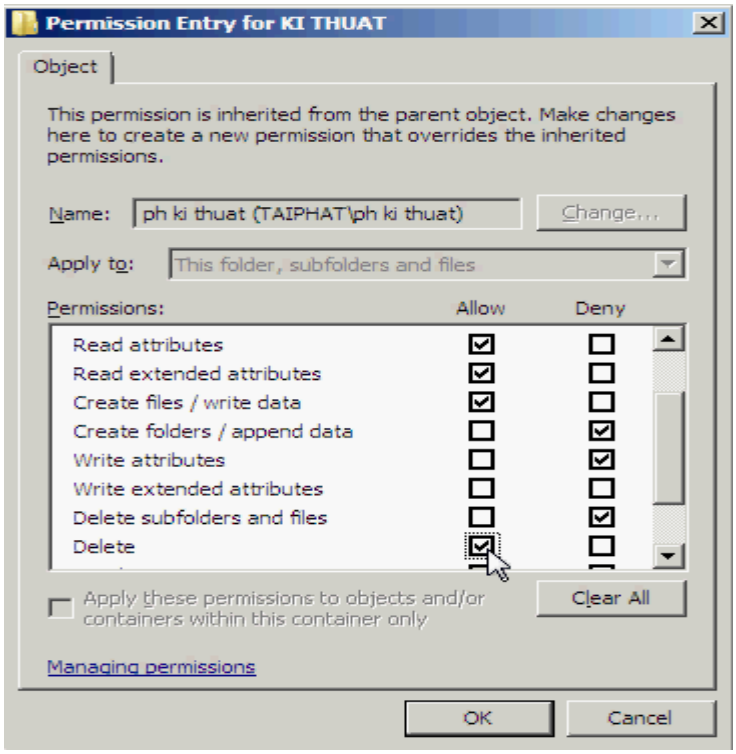


các user ở phòng Kinh Doanh được phép đọc dữ liệu và các thuộc tính. Được phép viết dữ liệu,tạo file, folder. Được phép thay đổi các thuộc tính của file và folder nhưng không được phép xóa file và folder

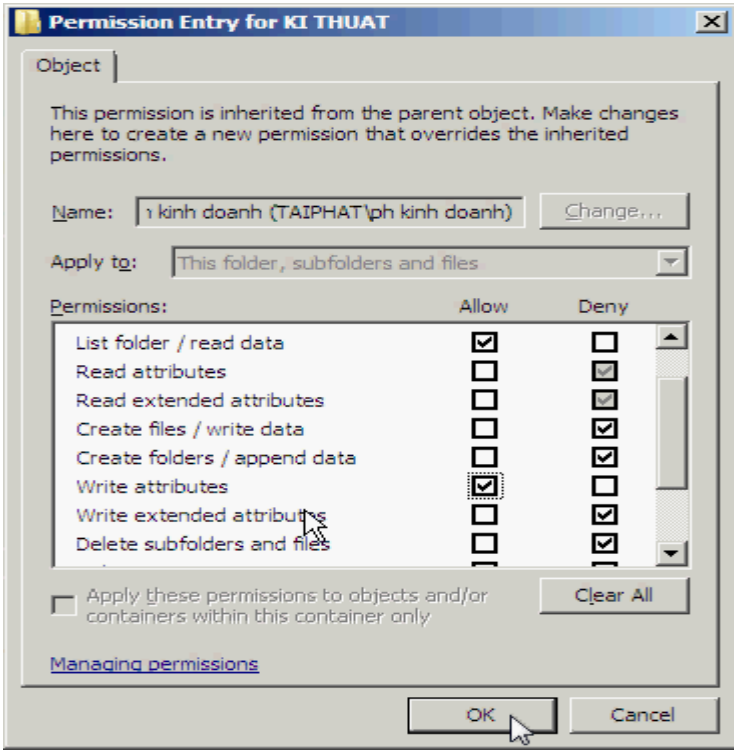


các user ở phòng Kế Toán và phòng Kỹ Thuật chỉ được quyền đọc dữ liệu.

- **Thiết lặp permission trên thư mục Kỹ Thuật :** cho phép các user ở phòng Kỹ Thuật được phép tạo file, đọc dữ liệu và đọc các thuộc tính mở rộng, nhưng không cho phép tạo folder, viết các thuộc tính mở rộng và không được xóa file. Các user o phòng Kinh Doanh và phòng Kế Toán chỉ được phép đọc và ghi dữ liệu



các user ở phòng Kỹ Thuật được phép tạo file, đọc dữ liệu và đọc các thuộc tính mở rộng, nhưng không cho phép tạo folder, viết các thuộc tính mở rộng và không được xóa file

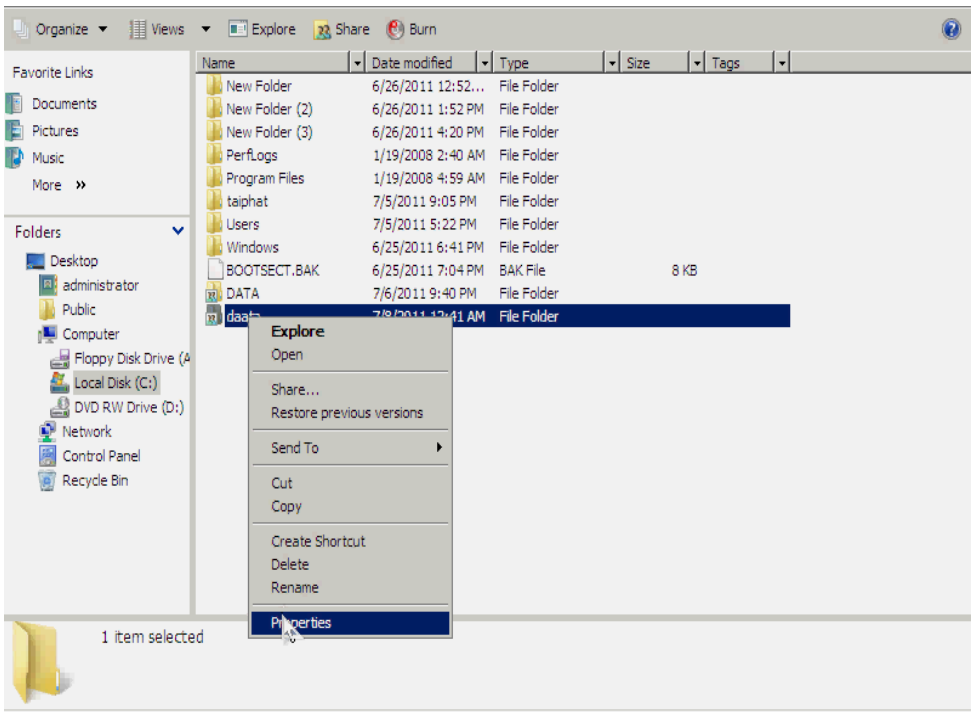


Các user o phòng Kinh Doanh và phòng Kế Toán chỉ được phép đọc và ghi dữ liệu

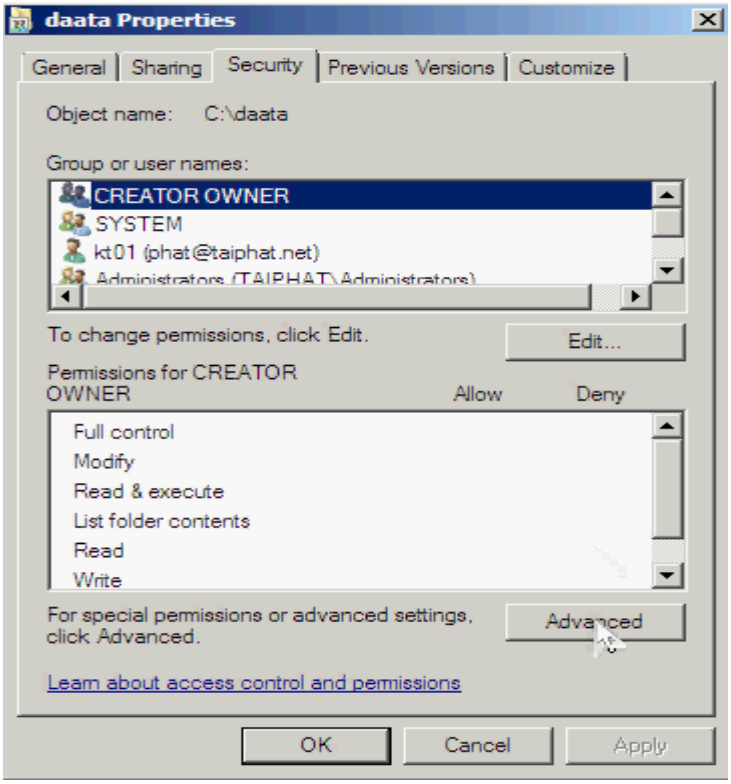
V. KIỂM TOÁN

Thiết lập kiểm toán nhằm để ghi nhận lại những trường hợp truy cập trái phép.

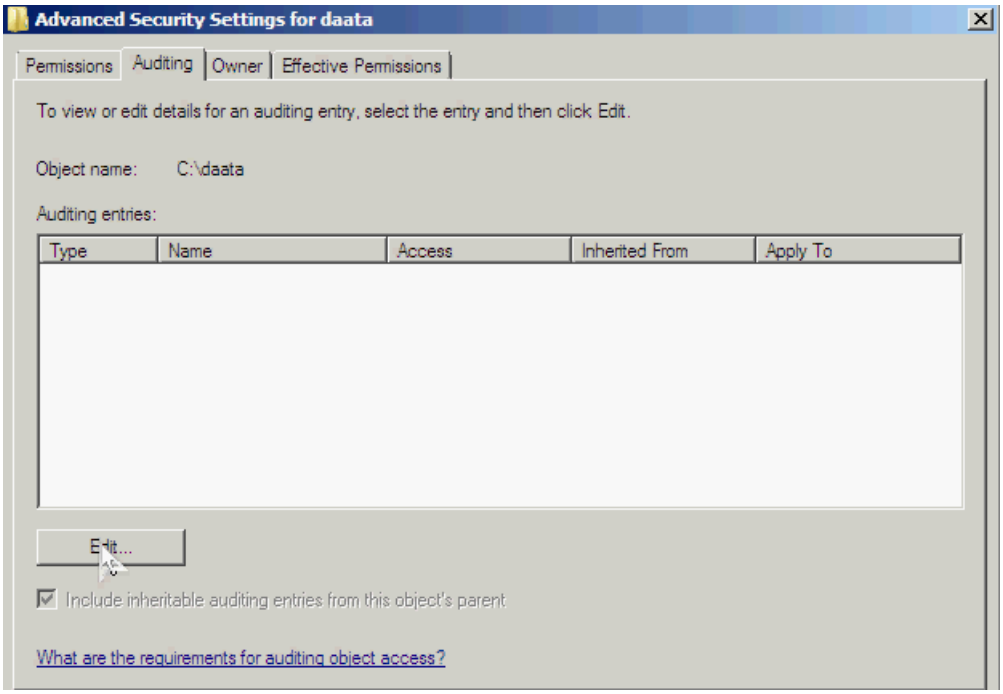
Click phải thư mục **daata ➔ Properties**.



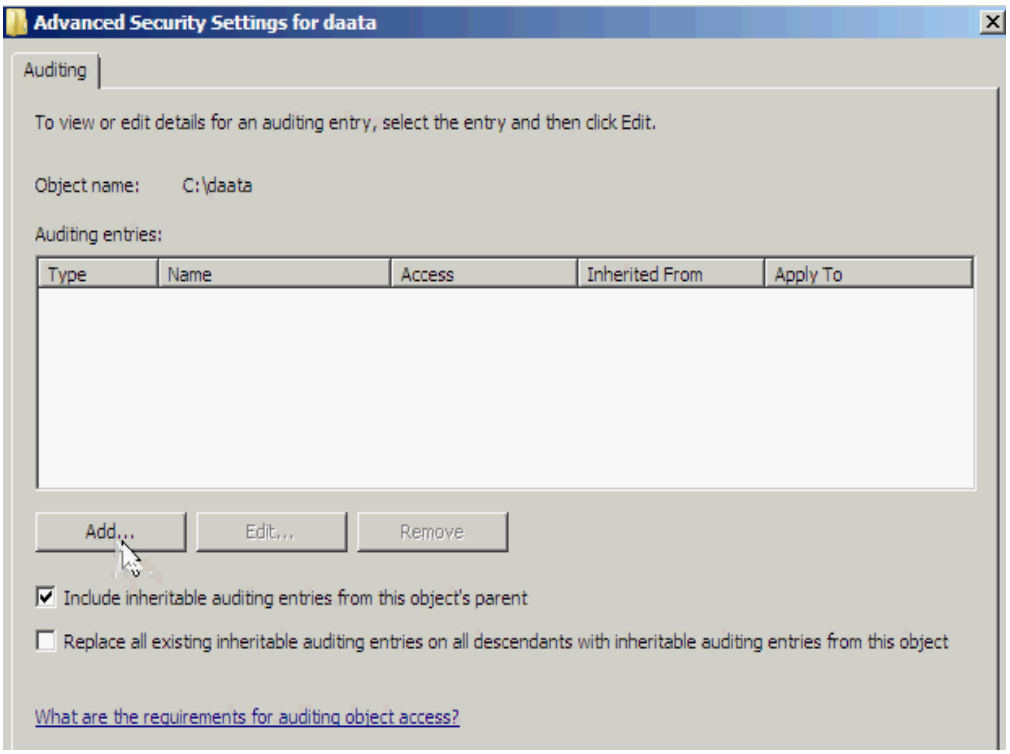
Tab Security ➔ Chọn **Advanced.**



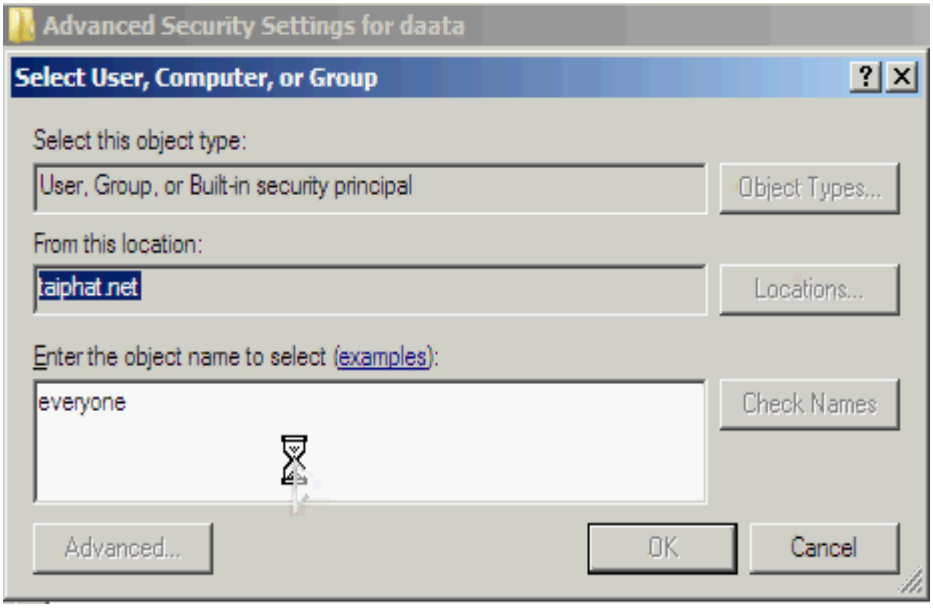
Tab Auditing ➔ Chọn **Edit.**



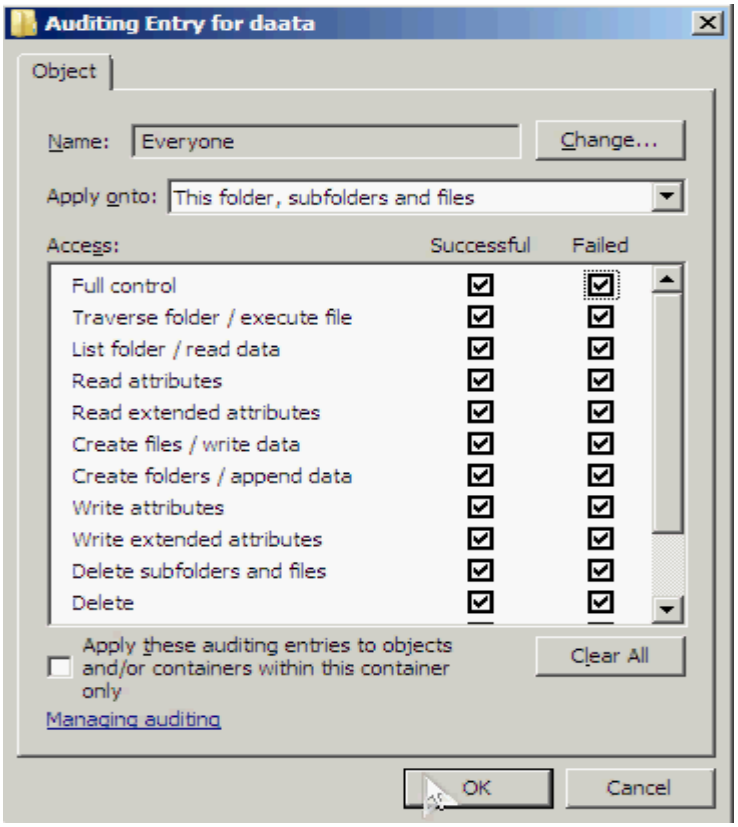
Chọn **Add.**



Nhập **Everyone ➔ Check Names ➔ OK.**



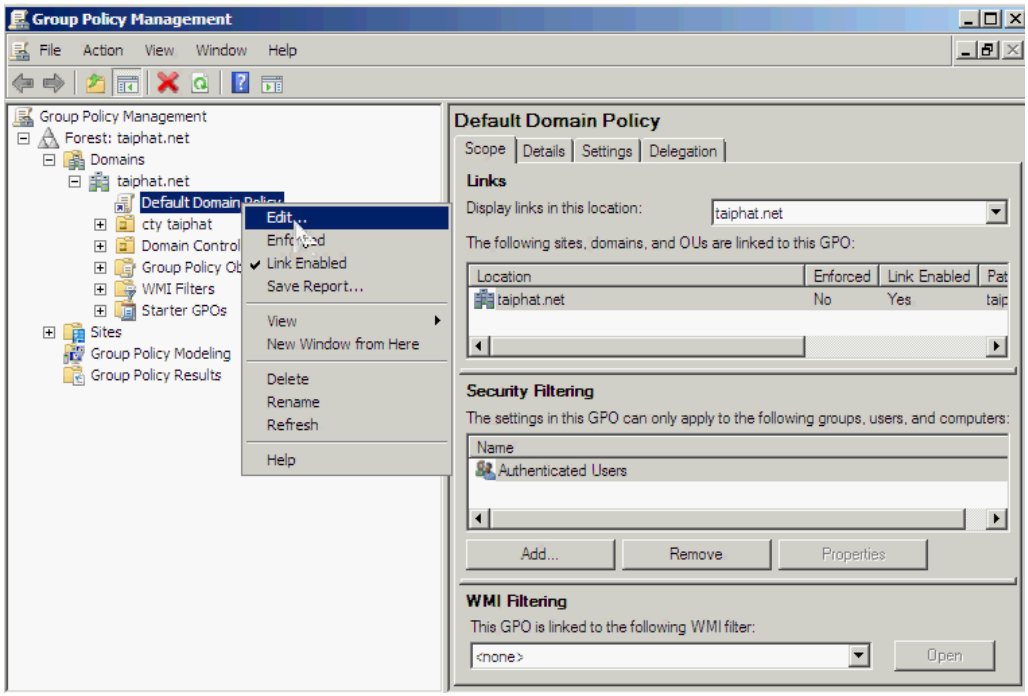
Chọn tất cả các chọn lựa ➔ **OK.**



Và nhấn **OK** để hoàn tất.

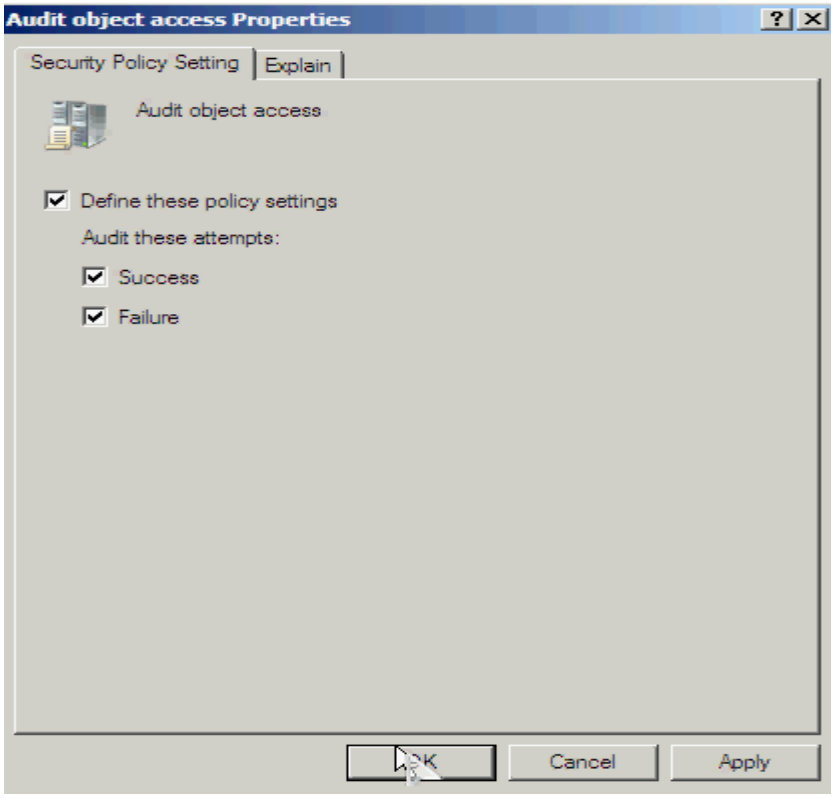
Mở Group Policy Management.

Click phải lên **Default Domain Policy ➔ Edit.**



Click phải **Audit object access ➔ Properties.**

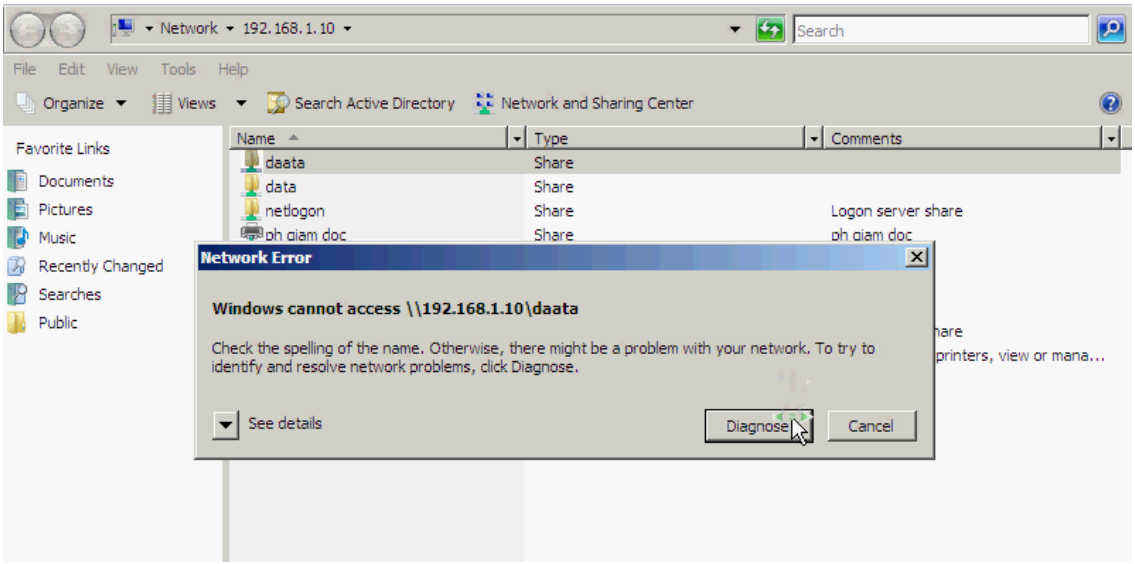
Chọn **Define these policy settings ➔** Chọn **Success , Failure.**



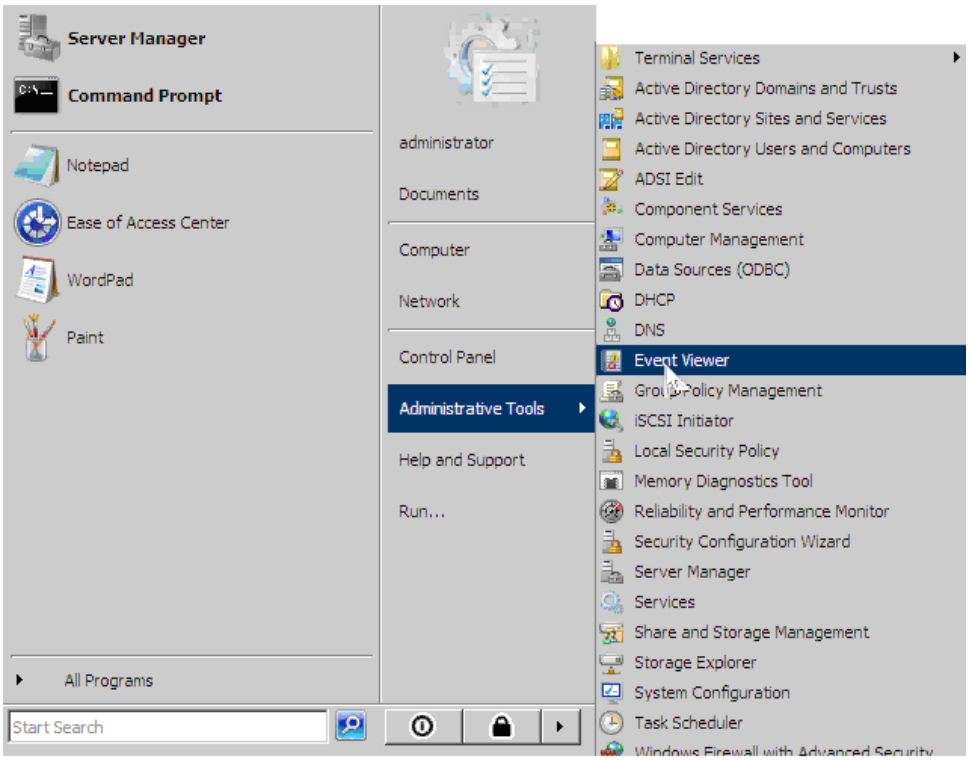
Mở **Run** nhập lệnh **GPUpdate /Force.**

- **Kiểm tra :**

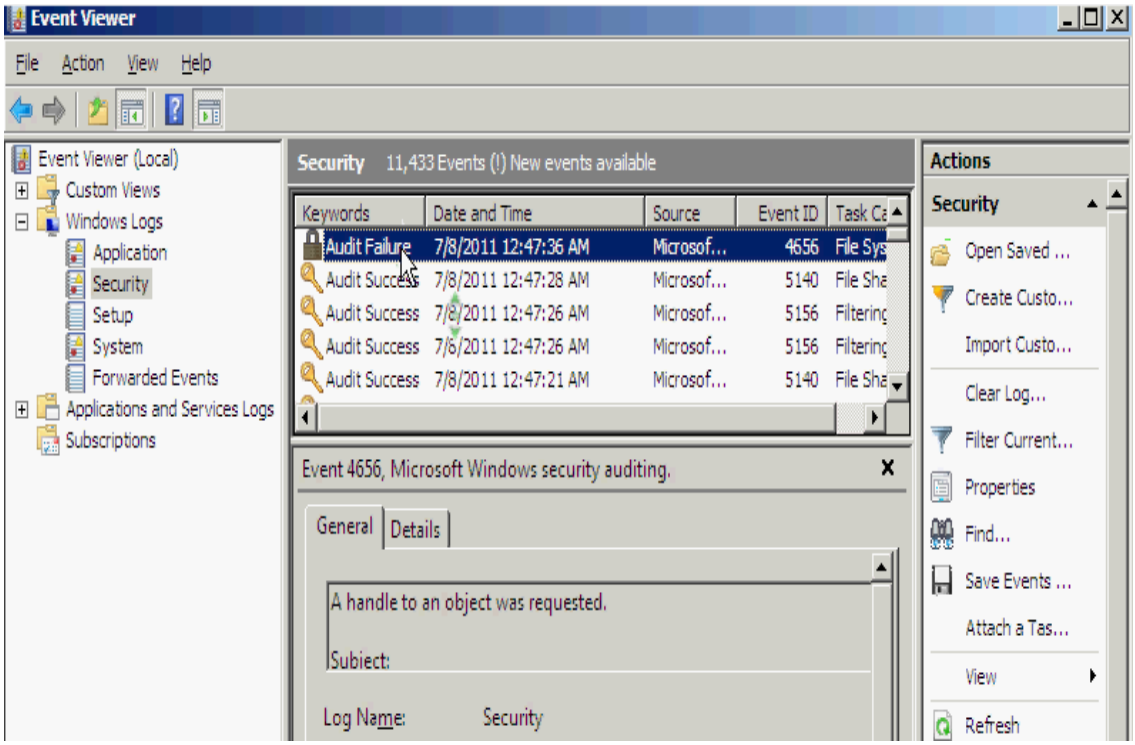
Trên máy **client ➔ log on KT1 ➔** truy cập vào thư mục **daata ➔** báo lỗi không có quyền truy cập.



Trên máy **Server ➔** Mở **Event Viewer.**



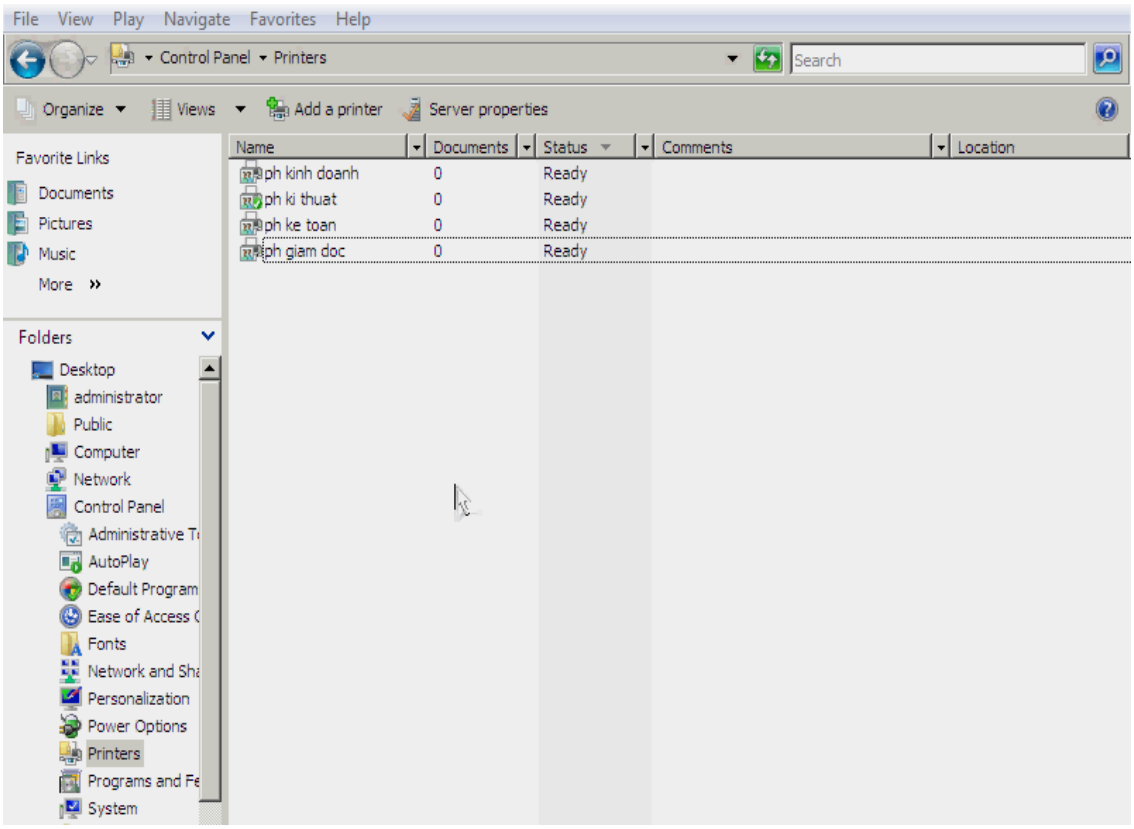
Mở **Windows Logs ➔ Security ➔** Mở các **event Audit Failure (& event id 5140).**



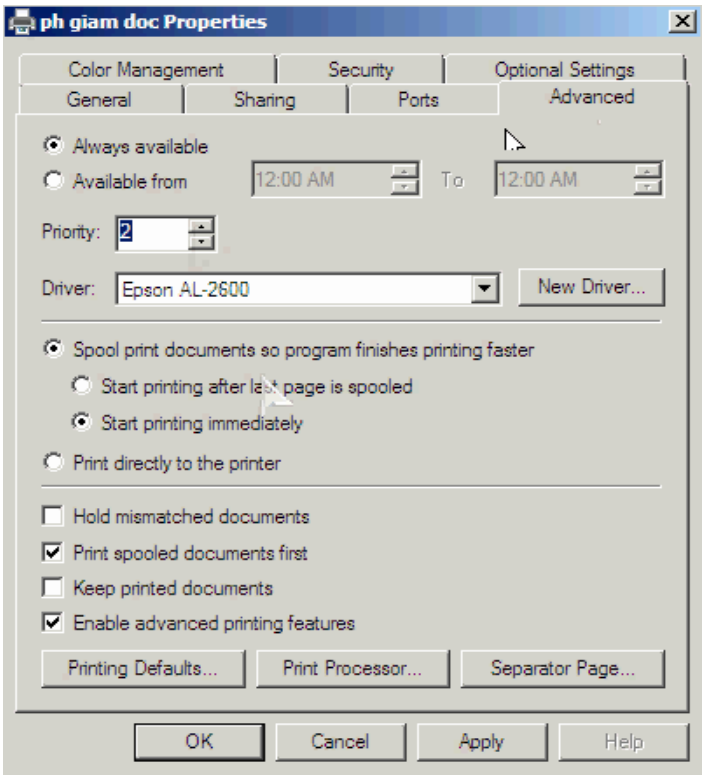
Quan sát thấy trường hợp truy cập trái phép của **KT1** vào thư mục **daata** đã được ghi nhận lại.

VI. QUẢN LÝ MÁY IN

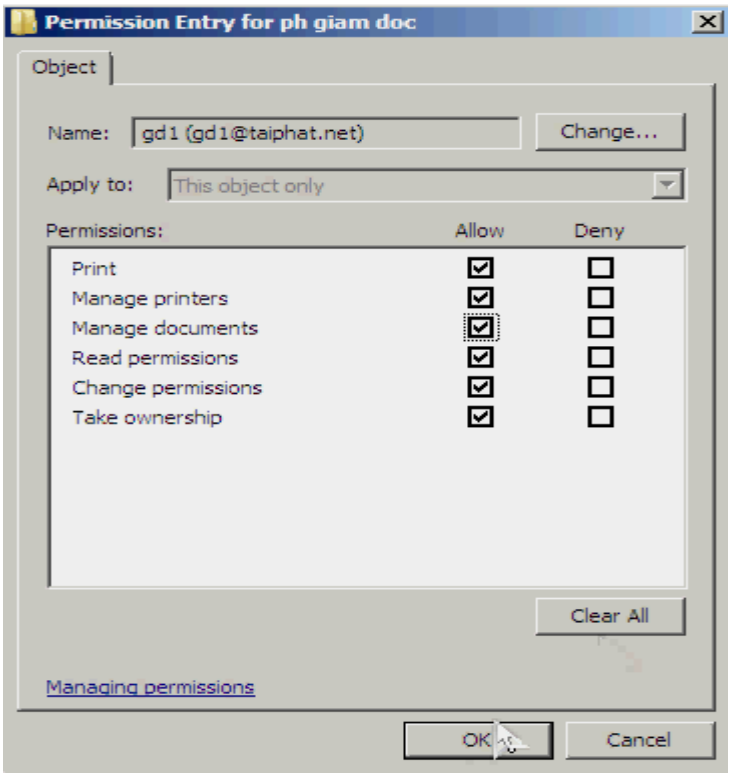
Tạo 4 máy in có tên là **ph giam doc, ph ke toan ,ph kinh doanh, ph ki thuat** tương ứng cho mỗi phòng .



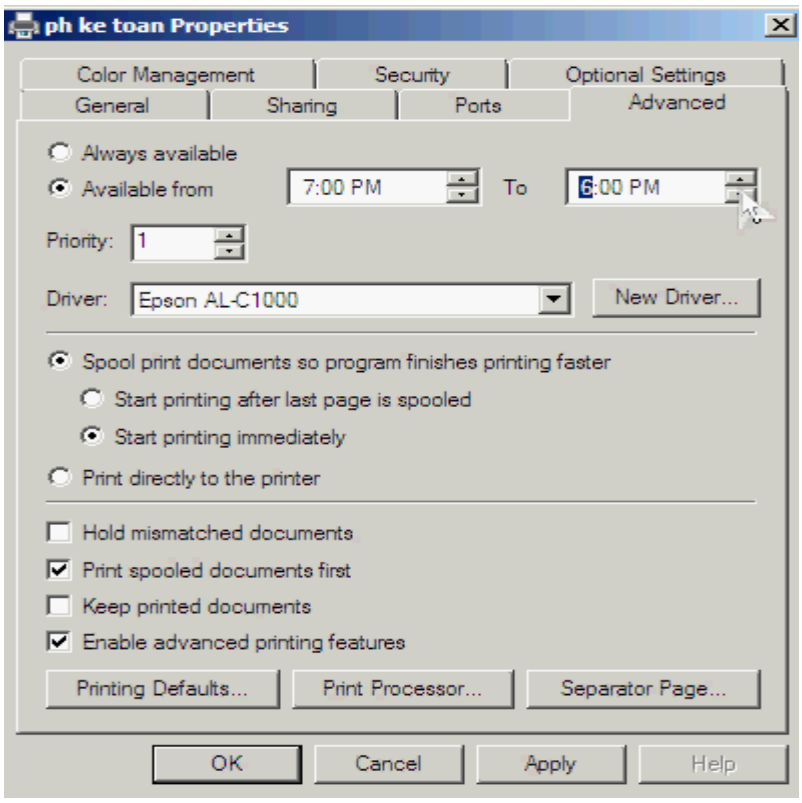
Gán quyền cho các user ở phòng Giám Đốc được quyền in trên máy in tên " ph Giám Đốc". Và cho máy in này luôn ở trạng thái sẵn sàng, gán độ ưu tiên cho máy in này là 2.

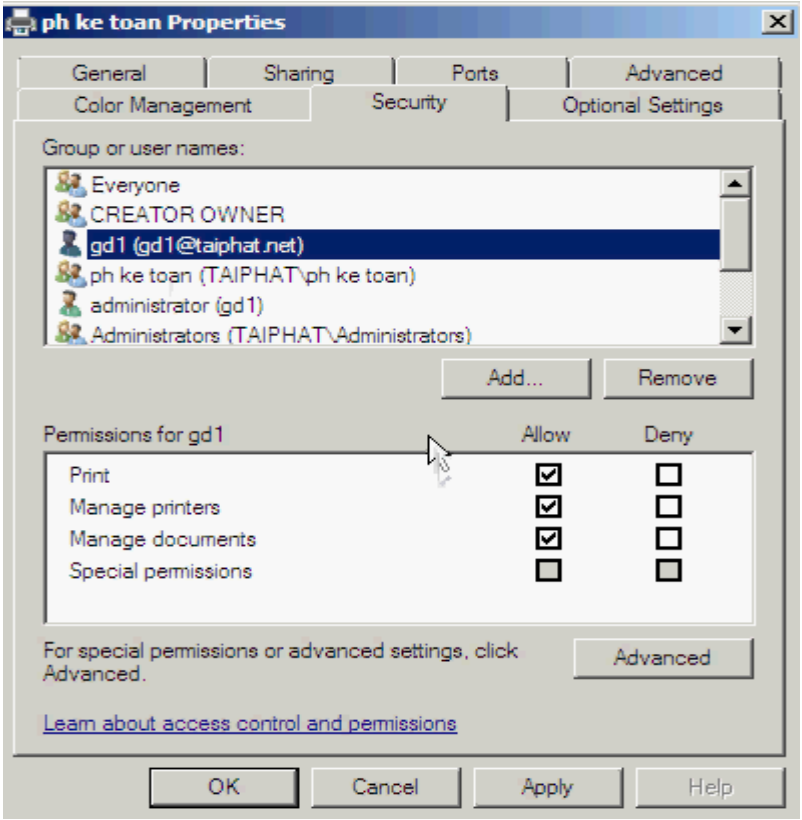


Riêng user gd1 được quyền thay đổi các cấu hình và được quyền xóa tài liệu đã được sử dụng trên máy in "ph Giám Đốc".

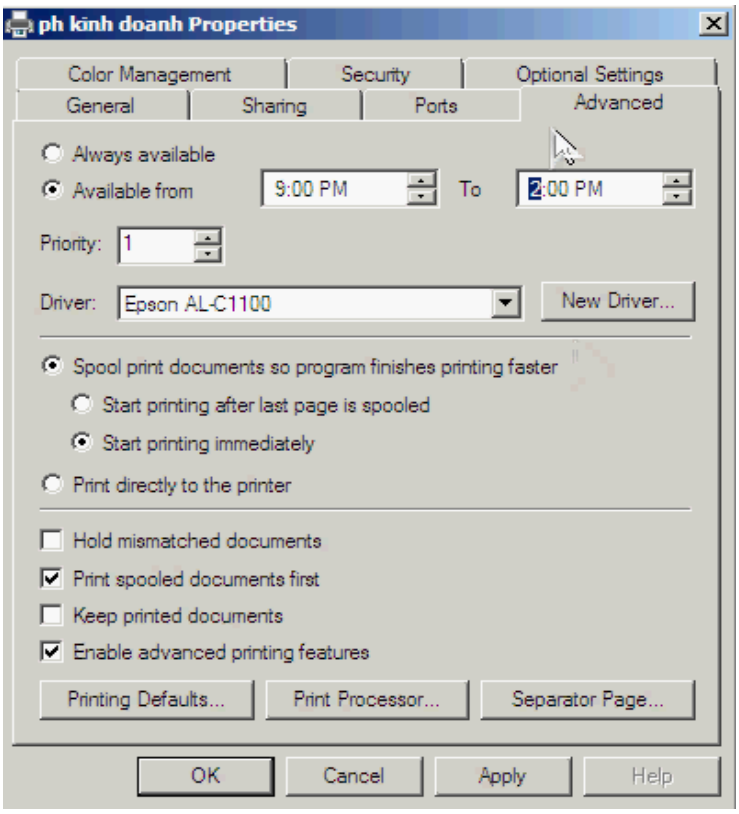


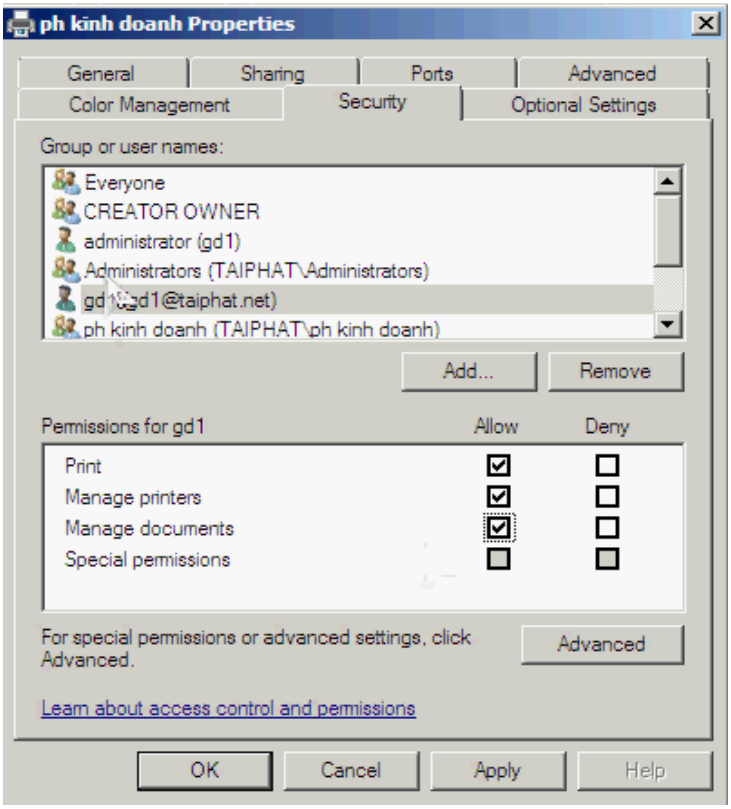
Trên máy in " ph Kế Toán" các user ở phòng Kế Toán được quyền in trên máy in này, thời gian được in từ 7h sáng đến 18h chiều . Mức độ ưu tiên 1, các user ở phòng Giám Đốc được phép in trên máy in này, riêng user gd1 được phép toàn quyền.



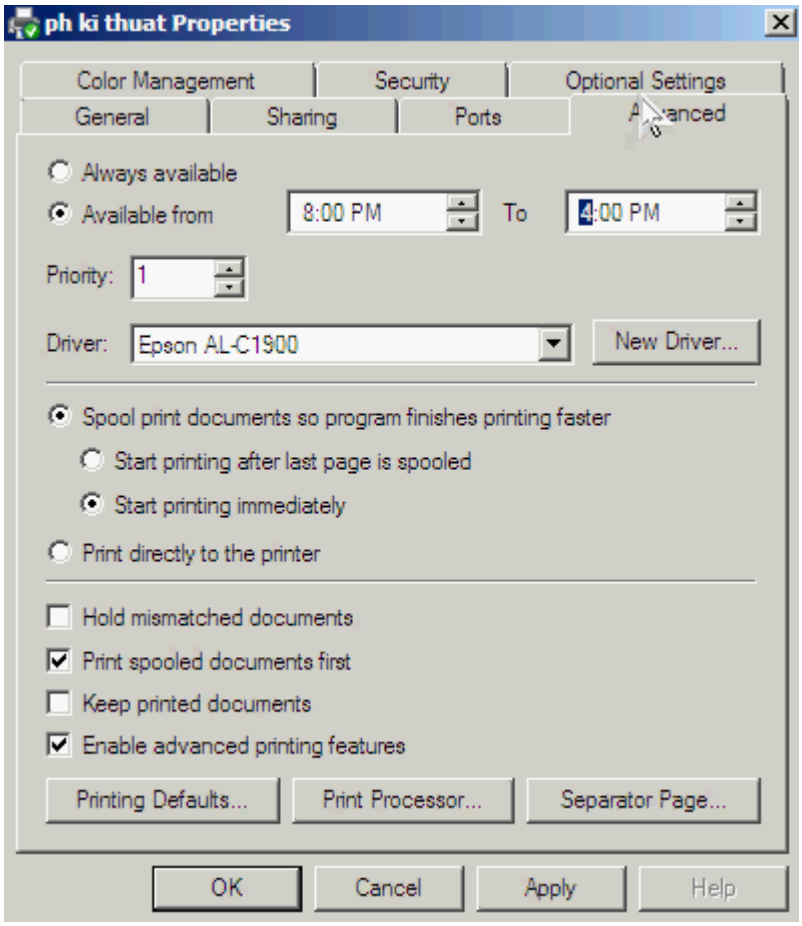


Trên máy in “ph Kinh Doanh” các user ở phòng Kinh Doanh được quyền in trên máy in này, mức độ ưu tiên cho máy in này là 1, thời gian được in từ 9h sáng đến 14h chiều. User gd1 được toàn quyền.





Trên máy in “ph Kỹ Thuật” các user ở phòng Kỹ Thuật được quyền in trên máy in này, thời gian được in từ 8h sáng đến 16h chiều, mức độ ưu tiên là 1.


ph ki thuat Properties
Color Management
Security
Optional Settings
General
Sharing
Ports
Always available
Available from
8:00 PM
To
4:00 PM
Priority:
1
Driver:
Epson AL-C1900
New Driver...
Spool print documents so program finishes printing faster
Start printing after last page is spooled
Start printing immediately
Print directly to the printer
Hold mismatched documents
Print spooled documents first
Keep printed documents
Enable advanced printing features
Printing Defaults...
Print Processor...
Separator Page...
OK
Cancel
Apply
Help