

**TRƯỜNG ĐẠI HỌC KỸ THUẬT CÔNG NGHIỆP**  
**KHOA ĐIỆN TỬ**  
**BỘ MÔN TIN HỌC CÔNG NGHIỆP**



**BÀI GIẢNG QUẢN TRỊ MẠNG**

*Thái Nguyên – 2020*

**TRƯỜNG ĐẠI HỌC KỸ THUẬT CÔNG NGHIỆP**  
**KHOA ĐIỆN TỬ**  
**BỘ MÔN TIN HỌC CÔNG NGHIỆP**



**BÀI GIẢNG QUẢN TRỊ MẠNG**

**BIÊN SOẠN: TS. NGHIÊM VĂN TÍNH**

## LỜI NÓI ĐẦU

Như chúng ta đã biết khoa học máy tính ngày nay vô cùng phát triển, do yêu cầu công việc muốn trao đổi thông tin với nhau thì người ta cần đến mạng máy tính. Mạng máy tính giúp rút ngắn khoảng cách về địa lí dù bạn ở nơi đâu. Điều đó đã kéo theo sự phát triển không ngừng của các mạng máy tính như: mạng lan, mạng wan, mạng internet. Để đáp ứng yêu cầu trên trong giáo trình quản trị mạng Window server 2008 này sẽ giúp các bạn hiểu rõ hơn về cơ chế vận hành, quản trị mạng máy tính cũng như các phương thức thiết lập chính sách với nhu cầu trao đổi thông tin nhằm bảo mật thông tin đó ngày càng tốt hơn. Window server 2008 là một sự lựa chọn đúng đắn nhất.

Windows Server 2008 (tên mã là “Longhorn”) được xây dựng trên những thành công và sức mạnh của Windows Server 2003 – là hệ điều hành vốn được trao tặng nhiều giải thưởng và những cách tân có trong bản Service Pack 1 và Windows Server 2003 R2. Bổ sung thêm chức năng mới, Windows Server 2008 mang đến những cải tiến mạnh mẽ cho hệ điều hành cơ sở này.

Với những cải tiến đa dạng đã giúp người quản trị tiết kiệm thời gian, chi phí và tận dụng triệt để cấu trúc hạ tầng. Với những tính năng tiên tiến như Network Access Protection và Read-Only Domain Controller đã tăng cường tính bảo mật và an toàn dữ liệu. Ngoài ra, Windows Server 2008 cũng cung cấp các công cụ mới mạnh mẽ như IIS7, Windows Server Manager và Windows PowerShell giúp đơn giản hóa công tác quản trị và cấu hình hệ thống. Ngoài ra, Windows Server 2008 còn tích hợp thêm công cụ Web gán trong và công nghệ ảo hóa nâng cao tính tin cậy và linh động cho hệ thống.

Nói tóm lại, Windows Server 2008 là một cuộc cách mạng mới về dòng sản phẩm Server của Microsoft, giúp cho những người quản trị dễ dàng và chủ động hơn trong việc quản lý, cấu hình các dịch vụ cũng như là quản trị môi trường mạng.

# MỤC LỤC

<b>Chương 1: TỔNG QUAN VỀ QUẢN TRỊ MẠNG</b>	<b>9</b>
1.1	Khái niệm quản trị mạng ..... 9
1.2	Chức năng về quản trị mạng ..... 9
1.3	Tầm quan trọng của quản trị mạng ..... 9
1.4	Các thành phần cơ bản của quản trị mạng ..... 10
1.5	Các mô hình và giai đoạn quản trị mạng ..... 10
<b>1.5.1</b>	<b>1.5.1. Các mô hình quản trị mạng</b> ..... 10
<b>1.5.2</b>	<b>1.5.2. Các giai đoạn quản trị mạng</b> ..... 11
<b>Chương 2.</b>	<b>TỔNG QUAN VỀ HỆ ĐIỀU HÀNH WINDOWS SERVER 2008</b> ..... 14
2.1	Giới thiệu và cài đặt windows server 2008..... 15
<b>2.1.1</b>	<b>Tổng quan về hệ điều hành Windows Server 2008</b> ..... 15
<b>2.1.2</b>	<b>Các công cụ quản trị trên Windows server 2008</b> ..... 15
<b>2.1.3</b>	<b>Chuẩn bị cài đặt Windows server 2008</b> ..... 19
<b>2.1.4</b>	<b>Nâng cấp lên Windows server 2008</b> ..... 21
	<b>Câu hỏi và bài tập</b> ..... 22
2.2	Cài đặt windows server 2008..... 22
<b>2.2.1</b>	<b>Cài đặt thủ công</b> ..... 22
<b>2.2.2</b>	<b>Khởi tạo cấu hình</b> ..... 26
<b>2.2.3</b>	<b>Cài đặt thêm tính năng</b> ..... 28
<b>2.2.4</b>	<b>Cài đặt Server Manager</b> ..... 29
<b>2.2.5</b>	<b>Cài đặt tự động</b> ..... 29
	<b>Câu hỏi và bài tập</b> ..... 31
<b>Chương 3. THIẾT LẬP VÀ QUẢN TRỊ HỆ THỐNG MẠNG</b>	<b>27</b>
3.1	Các mô hình mạng trong môi trường microsoft ..... 28
3.1.1	Mô hình mạng Workgroup ..... 28
<b>3.1.2</b>	<b>Giới thiệu Active Directory</b> ..... 31
<b>3.1.3</b>	<b>Các thành phần cơ bản và chức năng của Active Directory</b> ..... 32
<b>3.1.4</b>	<b>Cài đặt và cấu hình Active Directory</b> ..... 36
<b>3.1.5</b>	<b>Gia nhập máy trạm vào Domain</b> ..... 41
<b>3.1.6</b>	<b>Xây dựng Organizational Unit</b> ..... 43
<b>3.1.7</b>	<b>Tài khoản người dùng User account</b> ..... 44
<b>3.1.8</b>	<b>Tài khoản người dùng nhóm (Groups)</b> ..... 45

## MỤC LỤC

<i>Câu hỏi và bài tập</i> .....	47
3.2 Quản lý tài khoản người dùng và nhóm.....	47
3.2.1 Tài khoản người dùng cục bộ.....	47
3.2.2 Tài khoản người dùng miền.....	48
3.2.3 Chứng thực và kiểm soát truy cập.....	49
3.2.4 Các tài khoản tạo sẵn.....	51
3.2.5 Tài khoản nhóm Domain Local tạo sẵn.....	52
3.2.6 Tài khoản nhóm Global tạo sẵn.....	55
3.2.7 Các nhóm tạo sẵn đặc biệt.....	55
3.2.8 Chính sách tài khoản người dùng.....	56
3.2.9 Chính sách khóa tài khoản (Account Lockout Policy).....	58
3.2.10 Chính sách cục bộ (Local Policies).....	59
3.2.11 Chính sách kiểm toán.....	59
3.2.12 Quyền hệ thống của người dùng.....	61
3.2.13 Các lựa chọn bảo mật.....	68
3.2.14 Chính sách tài khoản người dùng nhóm (Group Policy).....	70
3.2.15 Triển khai một chính sách nhóm trên miền.....	72
3.2.16 Xem chính sách cục bộ của một máy tính ở xa.....	73
3.2.17 Tạo các chính sách miền.....	73
3.2.18 Khai báo một logon script dùng chính sách nhóm.....	74
3.2.19 Hạn chế chức năng của Internet Explorer.....	77
3.2.20 Chỉ cho phép một số ứng dụng được thi hành.....	77
3.2.21 Cài đặt phần mềm ứng dụng (Deploy software).....	78
3.3 Quản lý các thư mục dung chung.....	82
3.3.2 Cấu hình Share Permissions.....	83
3.3.3 Chia sẻ thư mục dùng lệnh net share.....	84
3.3.4 Quyền truy cập NTFS.....	85
3.3.5 Các quyền truy cập của NTFS.....	85
3.3.6 Các mức quyền truy cập được dùng trong NTFS.....	86
3.3.7 Gán quyền truy cập NTFS trên thư mục dùng chung.....	87
3.3.8 Kế thừa và thay thế quyền của đối tượng con.....	89

## MỤC LỤC

3.3.9	<i>Thay đổi quyền khi di chuyển thư mục và tập tin</i> .....	90
3.3.10	<i>Giám sát người dùng truy cập thư mục</i> .....	90
3.3.11	<i>Thay đổi người sở hữu thư mục</i> .....	90
	<i>Câu hỏi và bài tập</i> .....	91
3.4	Home directory, roaming profile & quota .....	92
3.4.1	<i>Khái niệm Profile</i> .....	92
3.4.2	<i>Giới thiệu về Home Directory</i> .....	94
3.4.3	<i>Mục đích sử dụng Home Directory</i> .....	94
3.4.4	<i>Giới thiệu Roaming profile</i> .....	94
3.4.5	<i>Mục đích sử dụng của Roaming Profile</i> .....	94
3.4.6	<i>Dịch vụ tập tin (File Services)</i> .....	94
3.4.7	<i>Quản lý Quota</i> .....	96
3.4.8	<i>Quản lý các báo cáo</i> .....	98
	<i>Câu hỏi và bài tập</i> .....	98
3.5	Quản lý in ấn.....	99
3.5.1	<i>Cài đặt máy in</i> .....	99
3.5.2	<i>Quản lý thuộc tính máy in</i> .....	100
3.5.3	<i>Giấy và chất lượng in</i> .....	100
3.5.4	<i>Các thông số mở rộng</i> .....	101
3.5.5	<i>Cấu hình chia sẻ máy in</i> .....	101
3.5.6	<i>Cấu hình thông số port cho máy in</i> .....	102
3.5.7	<i>Cấu hình các thông số trong Tab Port</i> .....	102
3.5.8	<i>Khả năng sẵn sàng phục vụ của máy in</i> .....	104
3.5.9	<i>Độ ưu tiên (Printer Priority)</i> .....	104
	<i>Câu hỏi và bài tập</i> .....	105

## DANH MỤC HÌNH ẢNH

Hình 1-1. Thiết lập ngôn ngữ .....	18
Hình 1-2. Nhập khóa kích hoạt sản phẩm hợp lệ .....	18
Hình 1-3. Lựa chọn bản Windows Server 2008 để cài đặt .....	19
Hình 1-4. Tùy chọn Upgrade đã bị vô hiệu khi khởi động máy từ đĩa cài đặt Hệ điều hành .....	19
Hình 1-5. Chọn thiết bị lưu trữ và phân chia ổ đĩa Logic .....	20
Hình 1-6. Initial Configuration Tasks Wizard .....	21
Hình 1-7. Lựa chọn tính năng bạn muốn cài đặt .....	23
Hình 1-8. Cài đặt Server Manager .....	24
Hình 1-9. Một đoạn trong file unattend.xml .....	26
Hình 2-1. Mô hình mạng Workgroup.....	28
Hình 2-2. Mô hình mạng Client/Server.....	30
Hình 2-3. Active Directory trên Windows Server 2008.....	32
Hình 2-4. Mô tả Organization Unit - đơn vị tổ chức dữ liệu.....	32
Hình 2-5. Mô tả việc quản lý các đối tượng trong Domain .....	33
Hình 2-6. Cấu trúc cơ sở dữ liệu của Domain.....	34
Hình 2-7. Thành phần cốt lõi kiến trúc Active Directory .....	34
Hình 2-8. Sysvol trong kiến trúc Active Directory .....	35
Hình 2-9. Add Roles khi nâng cấp Domain .....	36
Hình 2-10. Trang hộp thoại Before You Begin.....	36
Hình 2-11. Hộp thoại cài đặt Server Roles.....	37
Hình 2-12. Create a new domain in a new forest.....	37
Hình 2-13. Hộp thoại điền tên miền khi nâng cấp Domain .....	38
Hình 2-14. Hộp thoại chọn Forest Function Level .....	38
Hình 2-15. Hộp thoại Add thêm dịch vụ DNS.....	39
Hình 2-16. Hộp thoại xác thực Add thêm dịch vụ DNS .....	39
Hình 2-17. Hộp thoại đường dẫn lưu trữ Database Active Directory .....	40

Hình 2-18. Hộp thoại thiết lập mật khẩu phục hồi sơ sở dữ liệu của Active Directory .....	40
Hình 2-19. Hộp thoại diễn ra quá trình nâng cấp Domain .....	41
Hình 2-20. Đặt IP cho máy trạm .....	41
Hình 2-21. Hộp thoại gia nhập máy trạm vào Domain .....	42
Hình 2-22. Hộp thông báo gia nhập máy trạm vào Domain thành công .....	42
Hình 2-23. Cấu trúc cây OU.....	43
Hình 2-24. Hộp thoại tạo User Account .....	44
Hình 2-25. Hộp thoại tạo nhóm.....	45
Hình 2-26. Hộp thoại thêm tài khoản người dùng vào trong nhóm .....	45
Hình 2-27. Tổ chức tài khoản người dùng cục bộ.....	47
Hình 2-28. Tổ chức tài khoản người dùng miền .....	48
Hình 2-29. Giao diện chính sách tài khoản người dùng.....	56
Hình 2-30. Giao diện chính sách mật khẩu .....	56
Hình 2-31. Giao diện chính sách kiểm toán .....	59
Hình 2-32. Giao diện truy cập quyền hệ thống của người dùng .....	61
Hình 2-33. Cấp quyền cho User thay đổi giờ hệ thống.....	61
Hình 2-34. Giao diện chính sách bảo mật .....	66
Hình 2-35. Giao diện tạo chính sách miền.....	70
Hình 2-36. Giao diện khai báo logon script dùng chính sách nhóm .....	72
Hình 2-37. Hộp thoại tạo kịch bản logon script .....	72
Hình 2-38. Hộp thoại hạn chế chức năng Explorer.....	73
Hình 2-39. Giao diện cho phép một số ứng dụng được thi hành .....	74
Hình 2-40. Hộp thoại Share Permissions .....	78
Hình 2-41. Các quyền Share Permissions .....	80
Hình 2-42. Tab Security để add người dùng và nhóm .....	84
Hình 2-43. Tab Security để cấp quyền cho các người dùng .....	84
Hình 2-44. Hộp thoại kiểm tra và phân quyền chi tiết .....	85



Hình 2-45. Hộp thoại phân quyền chi tiết cho người dùng.....	86
Hình 2-46. Hộp thoại chọn người dùng làm giám sát.....	87
Hình 2-47. Hộp thoại thay đổi quyền sở hữu người dùng.....	87
Hình 2-48. Hộp thoại cấu hình Profile path và xây dựng kịch bản.....	90
Hình 2-49. Hộp thoại cài đặt dịch vụ thư mục.....	92
Hình 2-50. Cài đặt Quota.....	92
Hình 2-51. Tạo một Quota Template.....	93
Hình 2-52. Hộp thoại lựa chọn cập nhật Quota.....	94
Hình 2-53. Điều chỉnh trang in.....	98
Hình 2-54. Chọn độ sắc nét và màu (nếu có) của máy in.....	98
Hình 2-55. Hộp thoại điều chỉnh thông số mở rộng của máy in.....	99
Hình 2-56. Hộp thoại chia sẻ máy in.....	100
Hình 2-57. Hộp thoại cấu hình Port của máy in.....	101
Hình 2-58. Hộp thoại bật chức năng Printer pool.....	101
Hình 2-59. Set độ ưu tiên của máy in.....	102

## DANH MỤC BẢNG

Bảng 1-1. Yêu cầu phần cứng .....	15
Bảng 1-2. Loại hệ điều hành nâng cấp lên Windows server 2008.....	16
Bảng 2-1. Bảng mô tả các tài khoản người dùng được tạo sẵn.....	50
Bảng 2-2. Bảng mô tả tài khoản nhóm Domain Local tạo sẵn .....	51
Bảng 2-3. Bảng lựa chọn trong chính sách mật khẩu.....	57
Bảng 2-4. Bảng lựa chọn trong chính sách khoá mật khẩu.....	58
Bảng 2-5. Bảng lựa chọn trong chính sách kiểm toán.....	59
Bảng 2-6. Danh sách các quyền hệ thống cấp cho người dùng và nhóm. 62	Bảng
2-7. Bảng lựa chọn bảo mật thông dụng.....	67
Bảng 2-8. Ý nghĩa của các mục trong Tab Sharing .....	79
Bảng 2-9. Quyền truy cập của NTFS .....	81
Bảng 2-10. Bảng phân quyền truy cập được dùng trong NTFS.....	82

# **Chương 1: TỔNG QUAN VỀ QUẢN TRỊ MẠNG**

## **1.1 Khái niệm quản trị mạng**

Quản trị mạng là tổng hợp các hoạt động, phương pháp, thủ tục, và các công cụ liên quan đến điều hành, quản trị, bảo trì, và dự phòng hệ thống mạng.

## **1.2 Chức năng về quản trị mạng**

Hệ thống quản trị mạng bao gồm 4 chức năng cơ bản sau:

- ✓ Điều hành là hoạt động liên quan đến việc giữ cho hệ thống mạng (và các dịch vụ mạng cung cấp) chạy trơn tru. Nó bao gồm việc giám sát mạng để phát hiện các vấn đề sớm nhất có thể trước khi người dùng bị ảnh hưởng.
- ✓ Quản trị liên quan đến việc theo dõi các tài nguyên trên mạng và chúng được phân bổ như thế nào. Nó liên quan đến tất cả các việc cần làm để giữ cho mọi thứ được kiểm soát.
- ✓ Bảo trì liên quan đến việc sửa chữa và nâng cấp. Bảo trì cũng bao gồm các biện pháp chủ động khắc phục và phòng ngừa như điều chỉnh các thông số thiết bị khi cần và thường can thiệp khi cần thiết để làm cho hệ thống chạy tốt hơn.
- ✓ Dự phòng là việc cấu hình tài nguyên trong mạng để đáp ứng như cầu phát sinh, thay thế hoặc phục hồi khi cần thiết.

## **1.3 Tầm quan trọng của quản trị mạng**

Một hệ thống mạng máy tính là một mạng lưới có cấu trúc phức tạp, đòi hỏi yêu cầu quản lý cao và thường xuyên. Nó phải được lên kế hoạch cẩn thận. Cấu hình các thiết bị mạng phải được sửa đổi mà không ảnh hưởng xấu đến phần còn lại của mạng. Lỗi ở một thành phần nào đó cần phải được phát hiện, xác định nguyên nhân và sửa chữa. Mức độ dịch vụ được đảm bảo cho khách hàng và người dùng cuối, ví dụ, một số tiền nhất định của băng thông cần phải được theo dõi và đảm bảo, hay một ứng dụng mạng cần đảm bảo về hiệu năng và mức độ an toàn.

Về phía các nhà cung cấp dịch vụ, vấn đề cạnh tranh và phát triển đòi hỏi họ phải có một kế hoạch và thực thi quản trị mạng tốt để đảm bảo:

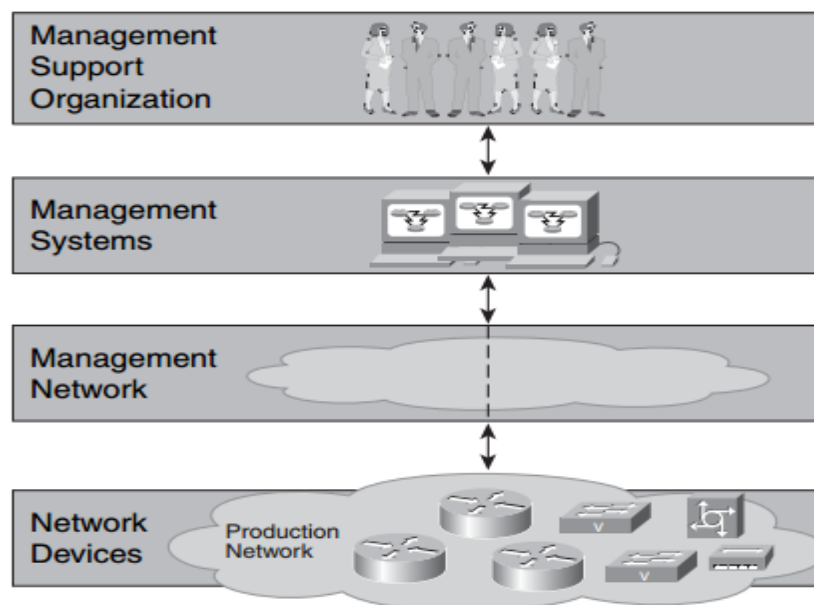
Ai có thể hoạt động mạng với chi phí thấp nhất và vượt qua những tiết kiệm chi phí trên cho khách hàng?

- ✓ Ai cung cấp trải nghiệm khách hàng tốt hơn bằng cách làm cho nó dễ dàng sử dụng nhưng vẫn đảm bảo an toàn.

- ✓ Ai có thể duy trì và đảm bảo chất lượng dịch vụ cao nhất?
- ✓ Ai có thể đưa ra các dịch vụ nhanh chóng và hiệu quả?

#### 1.4 Các thành phần cơ bản của quản trị mạng

- ✓ The Network device: Các thiết bị mạng như Switch, Router...
- ✓ The Management system: Cung cấp hệ thống mạng và các công cụ quản lý.
- ✓ The Management Network: Cung cấp hệ thống liên kết mạng.
- ✓ The Management Support Organization: Tổ chức hỗ trợ quản lý mạng. Thể hiện sự hiện diện yếu tố con người trong thành phần của quản trị mạng. Với chức năng: Lập kế hoạch, theo dõi và điều khiển hoạt động quản trị.



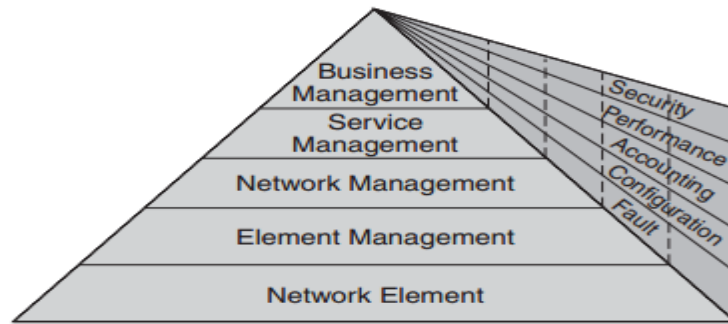
Hình 1: Các thành phần cơ bản trong QTM

#### 1.5 Các mô hình và giai đoạn quản trị mạng

##### 1.5.1 1.5.1. Các mô hình quản trị mạng

###### a) FCAPS

FCAPS (Fault, Configuration, Accounting, Performance, Security) là một mô hình quản lý cơ bản. Ý tưởng là nhóm thành các nhóm chức năng để có thể xử lý hàng loạt các chức năng quản trị được yêu cầu.



Hình 2: Mô hình quản trị FCAPS

### b) OAM&P

Là một mô hình thay thế cho FCAPS là OAM&P (Operations, Administration, Maintenance, and Provisioning). Mô hình OAM & P rất phổ biến ở đặc biệt với các nhà cung cấp dịch vụ viễn thông lớn.

- Operations (Điều hành)
- Administration (Quản trị)
- Maintenance (Bảo trì)
- Provisioning (Cung cấp)

### c) FAB và eTOM

Một mô hình quản trị theo chức năng khác được thiết lập bởi Telemanagement Forum (TMF) là FAB (Fulfillment—Assurance—Billing). Nền tảng dựa trên mô hình của TOM (Telecoms Operations Map) với việc lấy khái niệm quản trị vòng đời làm trung tâm. TOM chia vòng đời thành ba giai đoạn riêng biệt: Fulfillment—Assurance—Billing (FAB) và được áp dụng riêng biệt trong các tầng khác nhau:

- Quản trị hệ thống và mạng
- Điều hành và phát triển dịch vụ
- Chăm sóc khách hàng.

#### 1.5.2 1.5.2. Các giai đoạn quản trị mạng

##### ➤ Lập kế hoạch và thực hiện

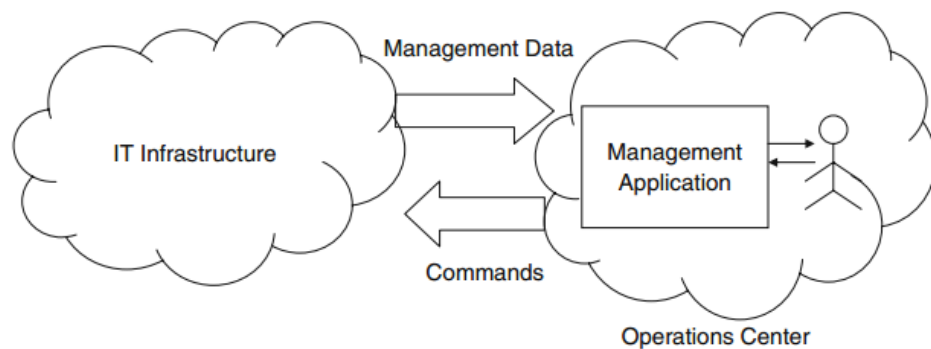
Lập kế hoạch và thực hiện là những giai đoạn quan trọng bảo đảm cho hệ thống mạng máy tính hoạt động trơn tru và hiệu quả. Xây dựng kế hoạch là một yêu cầu điều kiện tiên quyết khi cài đặt một hệ thống máy tính mới hay nâng cấp hệ thống hiện có để giải quyết các yêu cầu mới. Lập kế hoạch đánh dấu giai đoạn đầu tiên của vòng đời của hệ thống máy tính.

- Phân tích yêu cầu
- Bộ môn Tin học Công nghiệp

- Đánh giá hệ thống hiện có
- Lập kế hoạch thỏa mãn các yêu cầu
- Thực thi

➤ Quản trị hoạt động của hệ thống

Công việc của quản trị hoạt động của hệ thống là để giữ cho hệ thống chạy trơn tru không gặp vấn đề gì trong suốt giai đoạn hoạt động. Quản trị các hoạt động thường được thực hiện bởi một nhóm nhỏ các nhà quản trị hệ thống, thường được chia thành các lĩnh vực chuyên môn. Đối với bất kỳ một mạng dù nhỏ hoặc cơ sở hạ tầng CNTT của một công ty nhỏ, người ta sẽ tìm thấy một trung tâm hoạt động chịu trách nhiệm đảm bảo hoạt động thông suốt của toàn bộ cơ sở hạ tầng CNTT của tổ chức đó.



Hình 3: Trung tâm điều hành về CNTT

*Trung tâm điều hành - Dữ liệu quản lý - Giao thức cho tác nhân quản trị - Cấu trúc thông tin quản lý - Cấu trúc tác nhân thiết bị - Cấu trúc quản lý ứng dụng - Chức năng của trung tâm điều khiển*

➤ Theo dõi hệ thống

Giám sát hay theo dõi một hệ thống máy tính được định nghĩa là quá trình thu thập các thông tin trạng thái và cấu hình của các phần tử khác nhau của một hệ thống máy tính và củng cố thông tin đó. Củng cố thông tin có liên quan đến nhiệm vụ làm các báo cáo về hệ thống mạng, làm sạch các thông tin được theo dõi và đưa ra các thông tin quan trọng.

Việc quản lý một hệ thống máy tính đòi hỏi sự giám sát một loạt dữ liệu. Trong phần đầu của chương này, chúng ta nhìn vào một số các loại khác nhau của thông tin tình trạng cần phải được theo dõi để quản trị. Các phần tiếp theo sẽ thảo luận về một mô hình chung cho cấu trúc giám sát trong một mạng lưới hoạt động hệ thống và mở rộng trên các khía cạnh khác nhau của mô hình chung.

*Thông tin cần được theo dõi - Mô hình theo dõi - Thu thập dữ liệu -Tiền xử lý dữ liệu - Quản trị dữ liệu*

## ➤ Quản trị lỗi

Lỗi trong hệ thống máy tính là sự thất bại của một thành phần đảm bảo thống máy tính hoạt động bình thường. Hoạt động của một hệ thống máy tính có thể gặp phải lỗi bởi rất nhiều nguyên nhân. Mỗi lỗi phát sinh cần phải được cảnh báo hoặc có thông báo để thông tin cho bộ phận theo dõi. Những cảnh báo lỗi được giám sát cần được lưu trữ và quản lý bởi bộ phận quản lý lỗi.

*Kiến trúc quản lý lỗi - Các thuật toán chẩn đoán lỗi - Hệ thống tự chữa bệnh - Tránh thất bại*

## ➤ Kiểm toán và thực thi

*Quản lý thời gian hoạt động - Phương pháp tiếp cận để quản lý hiệu quả - thực hiện giám sát và báo cáo - Sự cố trong thực thi - Kế hoạch về khả năng - Quản lý kiểm toán*

## ➤ Quản trị an ninh

Mục tiêu của hệ thống quản lý là cố gắng để giữ cho hệ thống máy tính và mạng chạy đúng và hoàn hảo. Để làm như vậy, hệ thống máy tính phải được tiếp cận với những người được ủy quyền để sử dụng chúng, và không thể truy cập bởi bất cứ ai không được phép sử dụng chúng. Một sự truy cập trái phép có thể gây ra một số vấn đề trong hoạt động của hệ thống, bao gồm cả từ chối truy cập đến người sử dụng hợp pháp, gây ảnh hưởng đến hoạt động của hệ thống, hoặc làm cho hệ thống cư xử theo cách mà có thể gây hại cho người sử dụng. Như vậy, quản lý an ninh là một khía cạnh quan trọng của bất kỳ loại hình quản lý hệ thống máy tính.

Quản trị an ninh thông tin có thể được chia thành năm khía cạnh: xác thực, bảo mật, tính toàn vẹn, không thoái thác, và sẵn sàng. Xác thực là công việc để đảm bảo rằng bất kỳ người dùng hoặc chương trình truy cập thông tin được xác định một cách chính xác. Bảo mật có nghĩa là thông tin chỉ được hiển thị cho người dùng có thẩm quyền. Tính toàn vẹn đề cập đến việc đảm bảo rằng thông tin hoặc các hệ thống có chứa các thông tin không bị hỏng. Không thoái thác có nghĩa là nguồn gốc của thông tin sẽ được bảo vệ và đối tượng tạo cũng không thể từ chối trách nhiệm cho việc tạo ra các thông tin đó. Sẵn sàng là nhiệm vụ để đảm bảo truy cập thông tin và dịch vụ kịp thời và đáng tin cậy cho những người có thẩm quyền để sử dụng chúng.

Các kỹ thuật bảo đảm an ninh

- Kỹ thuật chung
- Quản trị bảo mật cho máy tính cá nhân
- Quản trị an ninh cho máy chủ máy tính
- Quản trị an ninh cho mạng máy tính
- Các vấn đề phát sinh khi hoạt động

## **Chương 2. TỔNG QUAN VỀ HỆ ĐIỀU HÀNH WINDOWS SERVER 2008**

### ➤ Giới thiệu chương:

- Trong chương này nhằm giúp cho sinh viên hiểu rõ hơn về 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 thiện 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.

### ➤ Mục tiêu chương:



- 2008
- Trình bày chính xác các tính năng của hệ điều hành Windows Server
  - Phát biểu chính xác phương pháp tự động hóa quá trình cài đặt
  - Cài đặt được điều hành Windows Server 2008 R2
  - Thiết lập cài đặt tự động hệ điều hành Windows XP/Server 2003 và Windows 7/Server 2008 R2.
  - Tự tin thiết kế, sửa chữa, khắc phục lỗi trong hệ thống mạng.
  - Có tính cẩn trọng khi triển khai hệ thống mạng và an toàn điện.

## **2.1 Giới thiệu và cài đặt windows server 2008**

### ***2.1.1 Tổng quan về hệ điều hành 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 công việc của doanh nghiệp.

Windows Server 2008 xây dựng trên sự thành công và sức mạnh của hệ điều hành đã có trước đó là Windows Server 2003 và những cách tân có trong bản Service Pack 1 và Windows Server 2003 R2. Mặc dù vậy Windows Server 2008 hoàn toàn hơn hẳn các hệ điều hành tiền nhiệm. 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.

### ***2.1.2 Các công cụ quản trị trên Windows server 2008***

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 được 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.

#### 2.1.2.1 *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.

#### 2.1.2.2 *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

### 2.1.2.3 *Windows Deployment 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 Service 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.

### 2.1.2.4 *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 người dùng cuối: cho phép người dùng cuối có thể chạy các chương trình từ Terminal Services server.

### 2.1.2.5 *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.

#### 2.1.2.6 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 viện API (Application Programming Interface), cho phép các nhà quản trị lập trình nhằm tăng tính bảo mật cho mình

### 2.1.2.7 *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.

### 2.1.2.8 *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 chuyển giao gọi là failover.

Những phiên bản sau hỗ trợ:

Windows Server 2008 Enterprise

Windows Server 2008 Datacenter

Windows Server 2008 Itanium

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.

### **2.1.3 Chuẩn bị cài đặt Windows server 2008**

#### **1.1.3.1 Yêu cầu phần cứng**

**Bảng 1-1. Yêu cầu phần cứng**

<b>Phần cứng</b>	<b>cầu tối thiểu</b>	<b>Đề nghị</b>
xử lý	(x86), 1,4 Ghz (x64)	hoặc lớn hơn
	B RAM	
lượng trống		

Windows Server 2008 hỗ trợ cả 2 cấu trúc vi xử lý 32-bit và 64-bit. Tuy nhiên, phiên bản mới nhất là Windows Server 2008 R2, Windows Midmarket Server và Windows Small Business với những tính năng đa dịch vụ, các phiên bản này chỉ hỗ trợ cấu trúc vi xử lý 64-bit.

RAM hỗ trợ tối đa cho hệ thống 32-bit là 4GB khi chạy phiên bản Standard Edition và 64GB khi chạy phiên bản Enterprise và Datacenter. Nếu

chạy hệ thống 64-bit, bộ nhớ RAM có thể hỗ trợ lên đến 32GB và 2 Tb RAM

cho phiên bản Enterprise và Datacenter. Thêm vào đó, Windows Server 2008 hỗ trợ hệ thống Itanium, tuy nhiên chip xử lý Intel Itanium 2 nhân là cần thiết.

#### 2.1.4 Nâng cấp lên Windows server 2008

**Bảng 1-2. Loại hệ điều hành nâng cấp lên Windows server 2008.**

Những phiên bản trước	Nâng cấp lên Windows Server 2008
Windows Server 2003 R2 Standard, Enterprise hoặc Datacenter Edition	đầy đủ
Windows Server 2003 Service Pack 1 (SP1) Standard, Enterprise hoặc Datacenter Edition	đầy đủ
Windows Server 2003 Service Pack 2 (SP2) Standard, Enterprise hoặc Datacenter Edition	đầy đủ
Windows NT 4.0	không hỗ trợ
Windows 2000 Server	không hỗ trợ
Windows XP	không hỗ trợ
Windows Vista	không hỗ trợ
Windows 7	không hỗ trợ

Để nâng cấp lên phiên bản Windows Server 2008, cần phải chạy các hệ điều hành ở cấp độ server. Không thể nâng cấp các phiên bản Windows dành cho người dùng như Windows XP hoặc Windows Vista lên Windows Server 2008. Để nâng cấp lên Windows Server 2008, hệ thống của bạn phải chạy Windows Server 2003. Việc nâng cấp từ Windows NT 4.0 và Windows 2000 Server không được hỗ trợ. Việc nâng cấp từ những phiên bản Windows Server 2003 lên phiên bản Windows Server 2008 Server Core không được hỗ trợ. Việc nâng cấp chỉ thực hiện được ở những phiên bản giống nhau. Khi nâng cấp lên phiên bản Windows Server 2008, mọi cấu hình thiết lập, file và các chương

trình đều được giữ lại.

### ***Câu hỏi và bài tập***

✍ Trình bày các yêu cầu phần cứng khi cài đặt Windows Server 2008?

✍ Phân loại hệ điều hành ở các phiên bản cũ có thể nâng cấp Windows Server 2008?

## **2.2 Cài đặt windows server 2008**

### ***2.2.1 Cài đặt thủ công***

Tiến trình cài đặt Windows Server 2008 được tổ chức rất hợp lý. Nếu đã từng cài đặt Windows Server 2003 hẳn bạn vẫn còn nhớ rằng trong quá trình cài đặt, bạn được yêu cầu trả lời những câu hỏi về cấu hình. Với Windows Server 2008, những yêu cầu này đã được chuyển tới phần Initial Configuration Tasks Wizard xuất hiện khi hoàn tất cài đặt. Sau đây là danh sách những thông tin bạn cần cung cấp trong quá trình cài đặt:

Ngôn ngữ, đơn vị tiền tệ và thông tin bàn phím (ngôn ngữ nhập liệu)

Khóa kích hoạt sản phẩm hợp lệ

Vị trí cài đặt

Ấn bản hệ điều hành sắp cài đặt (nếu không nhập khóa sản phẩm)

Cài đặt nâng cấp hay cài đặt mới

Toàn bộ việc cài đặt Windows Server 2008 chỉ qua ba phần:

Cài đặt hệ điều hành, bao gồm cả xác nhận mã khóa hợp lệ

Khởi tạo cấu hình Initial Configuration Tasks

Cài đặt Server Manager

Cho đĩa cài đặt Windows Server 2008 vào ổ và khởi động máy chủ từ đĩa cài.

Khi được yêu cầu chọn ngôn ngữ, thời gian, đơn vị tiền tệ và thông tin bàn phím, bạn hãy đưa ra lựa chọn thích hợp rồi click Next.

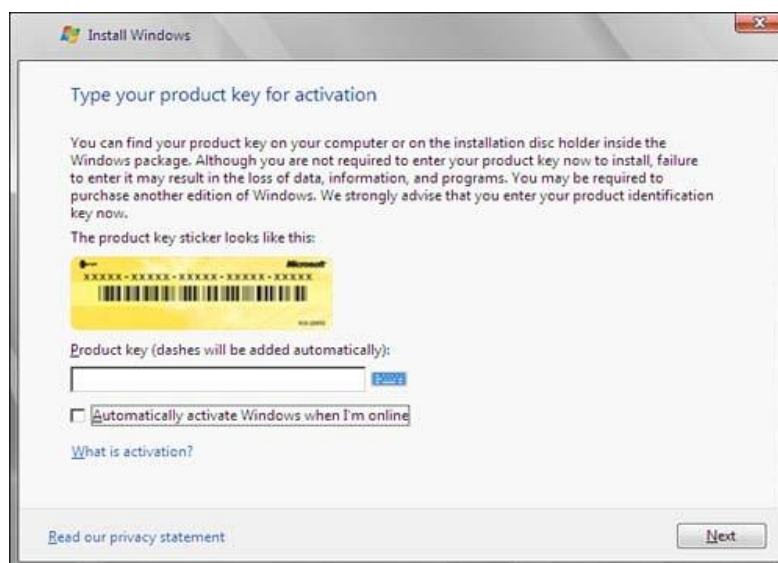




Hình 1-1. Thiết lập ngôn ngữ

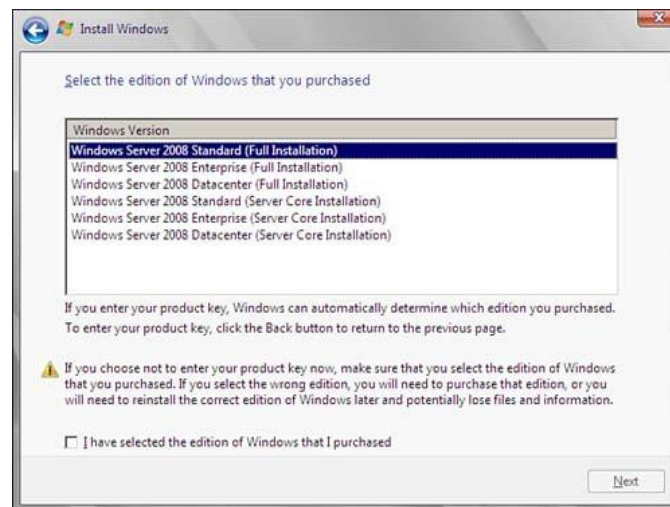
Tùy chọn Install Now xuất hiện. Nếu chưa chắc chắn về yêu cầu phần cứng, bạn có thể click vào liên kết What to Know Before Installing Windows để biết thêm chi tiết.

Nhập khóa kích hoạt sản phẩm (product key) và đánh dấu kiểm vào ô Automatically Activate Windows When I'm Online. Click Next.



Hình 1-2. Nhập khóa kích hoạt sản phẩm hợp lệ

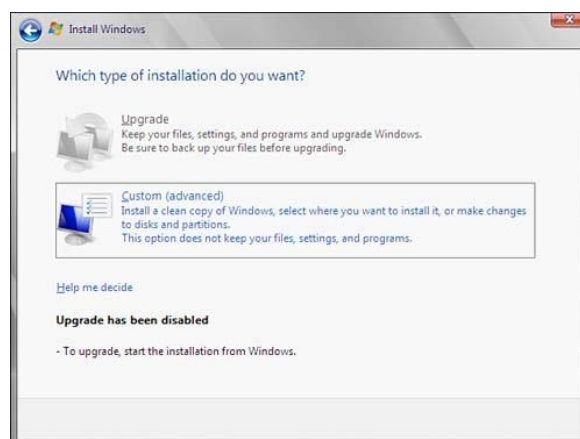
Nếu chưa nhập khóa sản phẩm ở mục trước, bây giờ bạn sẽ phải lựa chọn ấn bản Windows Server 2008 sắp cài đặt và đánh dấu kiểm vào ô I Have Selected an Edition of Windows That I Purchased. Nếu bạn đã nhập khóa sản phẩm hợp lệ, trình cài đặt sẽ tự động nhận diện được ấn bản Windows Server 2008 bạn sắp cài đặt. Click **Next**.



**Hình 1-3. Lựa chọn bản Windows Server 2008 để cài đặt**

Đọc các điều khoản quy định và chấp nhận bằng cách đánh dấu ô kiểm. Click **Next**.

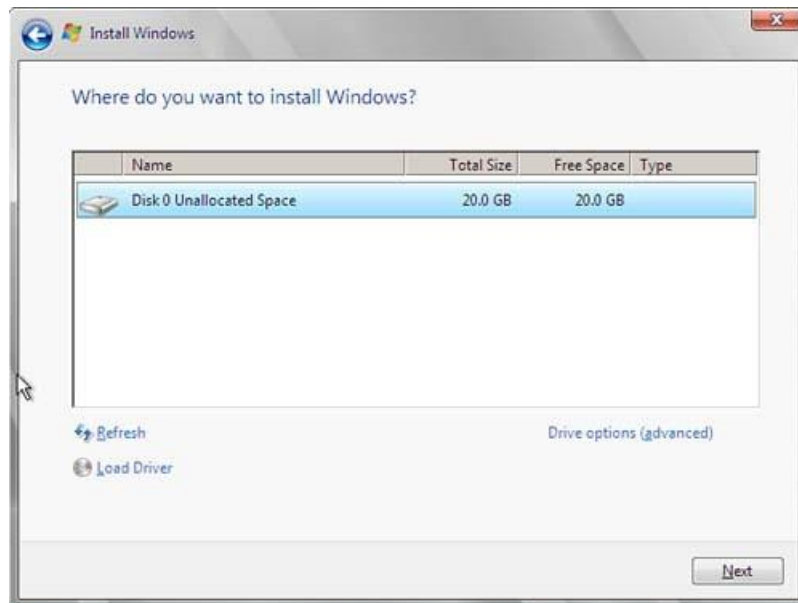
Ở cửa sổ mới xuất hiện, do bạn khởi động máy từ đĩa cài nên tùy chọn Upgrade (nâng cấp) đã bị vô hiệu. Click **Custom (Advanced)**.



**Hình 1-4. Tùy chọn Upgrade đã bị vô hiệu khi khởi động máy từ đĩa cài đặt Hệ điều hành**

**Lưu ý:** Nếu bạn muốn tiến hành cài đặt nâng cấp, bạn cần chạy trình cài đặt trong môi trường Windows.

2.2.1.1 Trên cửa sổ tiếp theo, bạn cần lựa chọn vị trí cài đặt Windows. Nếu có driver của các thiết bị lưu trữ bên thứ ba, cần cài đặt ngay bằng cách click liên kết *Load Driver*.



**Hình 1-5. Chọn thiết bị lưu trữ và phân chia ổ đĩa Logic**

Lúc này, Windows sẽ bắt đầu được cài đặt vào hệ thống. Bạn có thể thấy từng bước tiến trình hoàn tất thể hiện bằng phần trăm. Trong quá trình cài đặt, máy chủ sẽ phải khởi động lại nhiều lần. Trình cài đặt sẽ hoàn thành những tác vụ sau đây:

Sao chép tệp tin

Mở rộng tệp tin

Cài đặt chức năng

Cài đặt cập nhật

Hoàn thành

Khi quá trình cài đặt hoàn tất, hãy thay đổi mật khẩu tài khoản quản trị administrator trước khi đăng nhập. Sau khi mật khẩu được thay đổi và bạn đã đăng nhập vào hệ điều hành, như vậy là bạn đã xong phần 1 của việc cài đặt.



**Lưu ý:** Trên thực tế, bạn sẽ thường gán địa chỉ IP tĩnh cho máy chủ cơ sở hạ tầng. Trong trường hợp này, bạn sẽ cần thu thập thông tin đó cùng với địa chỉ IP hợp lệ cho default gateway và cho máy chủ DNS/WINS trước khi cài đặt.

Cung cấp tên máy tính cho máy chủ, cùng với thông tin domain hoặc workgroup.

Bạn cần khởi động lại máy chủ để các thay đổi có tác dụng.

Trong mục Update This Server, bạn có thể thực hiện những việc sau:

Cho phép tự động cập nhật và phản hồi

Cấu hình việc tải về và cài đặt những cập nhật của hệ điều hành

Trong mục Customize This Server, bạn có thể thực hiện những việc sau:

Thêm vai trò (role) máy chủ.

Khi bạn chọn một vai trò, trình hướng dẫn sẽ giúp bạn hoàn thành việc cài đặt vai trò. Bạn có thể lựa chọn các vai trò sau:

Active Directory Certificate Services

Active Directory Domain Services

Active Directory Federation Services

Active Directory Lightweight Directory Services

Active Directory Rights Management Services

Application Server

DHCP Server

DNS Server

Fax Server

File Services

Network Policy and Access Services

Print Services

Terminal Services

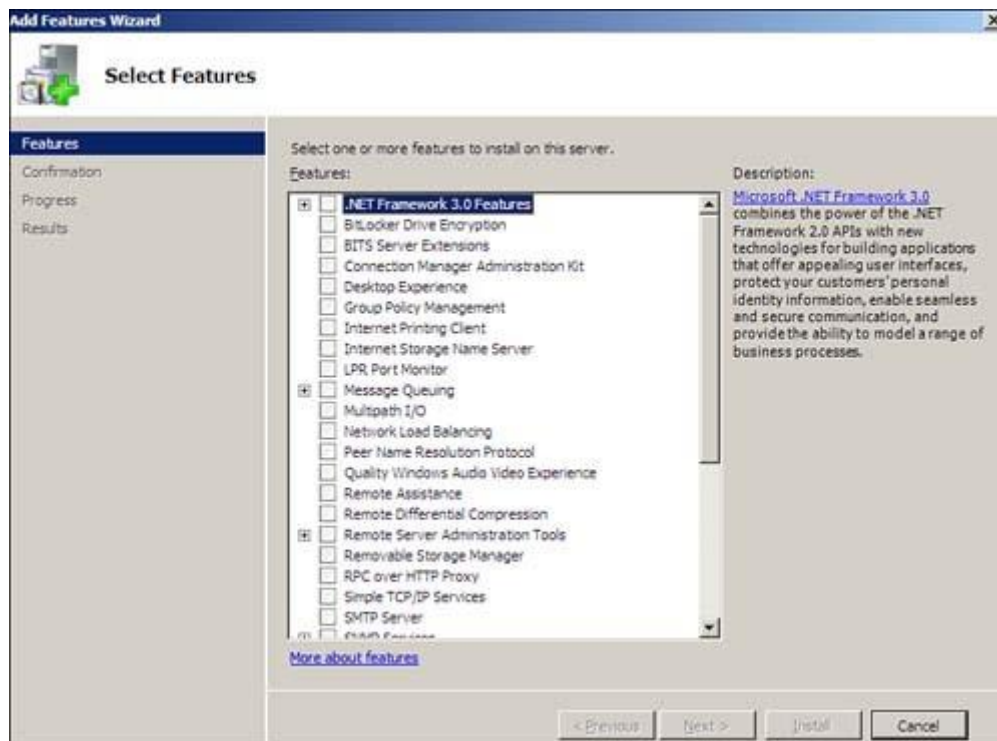
UDDI Services

Web Server (IIS)

Windows Deployment Services

### 2.2.3 Cài đặt thêm tính năng.

Cũng như thêm vai trò, khi bạn lựa chọn tính năng, trình hướng dẫn sẽ giúp bạn hoàn thành việc cài đặt tính năng đó. Có rất nhiều tính năng cho bạn lựa chọn.



**Hình 1-7. Lựa chọn tính năng bạn muốn cài đặt**

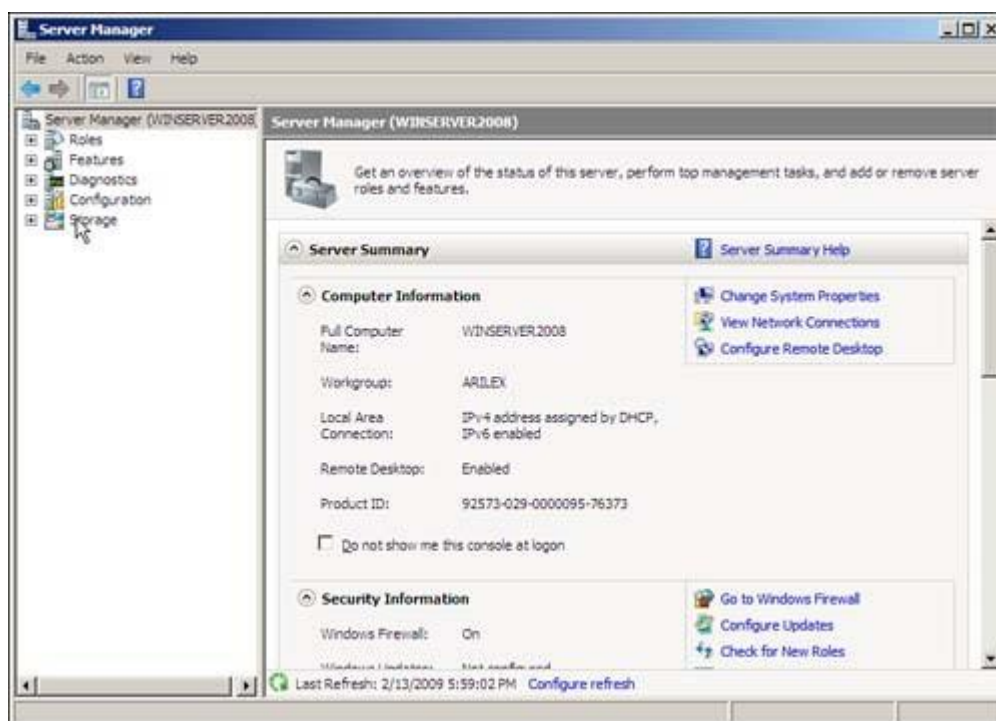
**Lưu ý:** Đối với cả hai danh sách vai trò và tính năng, khi bạn điểu sáng một vai trò hoặc tính năng nào đó, bạn sẽ thấy phần mô tả ở bên phải danh sách. Khi bạn lựa chọn các vai trò và tính năng, cần nhớ rằng nên cài đặt càng ít càng tốt, tốt nhất là chỉ nên lựa chọn những thứ bạn dự định sử dụng. Nếu bạn cài đặt các vai trò hoặc tính năng không cần thiết, bạn sẽ cài đặt luôn cả những dịch vụ vô ích và có khả năng mở toang những công không có giá trị trong sản xuất khiến máy chủ không còn an toàn.

Cho phép Remote Desktop kết nối tới máy chủ

Cấu hình thiết lập tường lửa hệ điều hành. Theo mặc định, tường lửa được kích hoạt sẵn.

Tiếp theo sẽ là phần ba của quá trình cài đặt.

## 2.2.4 Cài đặt Server Manager



Hình 1-8. Cài đặt Server Manager

Server Manager cho bạn một cái nhìn toàn cục về máy chủ. Khi nhìn vào phần chi tiết mặc định, bạn có thể thấy thông tin máy tính, thông tin bảo mật và bản tóm tắt các vai trò và tính năng đã cài đặt. Nhìn xuống phía dưới, bạn sẽ thấy tài nguyên và phần hỗ trợ. Phía bên trái cửa sổ là các công cụ giúp bạn thêm/bớt và cấu hình các vai trò cũng như các tính năng. Bạn cũng sẽ thấy các tùy chọn để chẩn đoán, cấu hình và quản lý ổ đĩa. Sau khi xác lập các thay đổi trong Server Manager, công việc cài đặt thủ công của bạn đã thực sự hoàn tất.

## 2.2.5 Cài đặt tự động

Vậy là bạn đã hoàn tất công việc cài đặt thủ công, phần tiếp theo của bài viết sẽ giới thiệu cho bạn quá trình cài đặt tự động. Với Windows Server 2008, bạn sử dụng file *unattend.xml* thay vì *unattend.txt*. Thực ra, file *unattend.xml* cũng thay thế cả các file *Sysprep.inf*, *Winbom.ini*, và *Cmdlines.txt*. Định dạng XML đã được thông qua vì nó giúp các công việc mô tả các giá trị lồng nhau,

thêm phần tử mới và xác thực file trả lời trở nên dễ dàng hơn. Bạn có thể mở file unattend.xml trong Internet Explorer phiên bản 5.5 trở lên để phân tích cú pháp file .xml và xem liệu nó có được xây dựng hoàn chỉnh. Nếu tập tin không được xây dựng chính xác, Internet Explorer sẽ báo cho bạn biết chỗ nào bị lỗi.

Để cài đặt tự động, bạn chạy file setup.exe với từ khóa *unattend*

```
C:>setup.exe /unattend:<path>\unattend.xml
```

File unattend.xml chứa những câu trả lời cần thiết khi chạy setup.exe, cụ thể là các thông tin như tên máy tính, việc chấp nhận thỏa thuận cấp phép người dùng cuối (EULA), thông tin đĩa cài đặt v.v... Bạn cũng có thể cho hiển thị hoặc ẩn đi giao diện người dùng (UI) đối với mỗi giá trị được thiết lập bằng cách sử dụng **ShowUI flag = Yes/No**. Sau đây là cách trình cài đặt phản ứng khi bạn sử dụng ShowUI flag:

ShowUI flag = Yes và thiết lập được chỉ rõ trong file unattend.xml: Trình cài đặt sử dụng thiết lập được chỉ rõ trong file unattend.xml và hiển thị giao diện người dùng theo thiết lập đó.

ShowUI flag = No và thiết lập được chỉ rõ trong file unattend.xml: Trình cài đặt sử dụng thiết lập được chỉ rõ trong file unattend.xml và không hiển thị giao diện người dùng.

ShowUI flag = Yes và thiết lập không được chỉ rõ trong file unattend.xml: Trình cài đặt hiển thị giao diện người dùng với giá trị mặc định và người dùng có thể thay đổi thiết lập này nếu cần.

ShowUI flag = No và thiết lập không được chỉ rõ trong file unattend.xml: Trình cài đặt sử dụng giá trị mặc định và không hiển thị giao diện người dùng.

Khi tiến hành cài đặt tự động qua mạng, trình cài đặt hệ thống phải có quyền truy cập vào file unattend.xml. Khi trình cài đặt khởi chạy từ ổ CD/DVD, nó sẽ tìm kiếm file unattend.xml trong các vị trí sau:

Thư mục hiện hành

Vị trí khởi chạy file setup.exe

Ổ đĩa mềm, USB hoặc ổ CD/DVD khác



Cú pháp cho file unattend.xml được chia nhỏ thành các phần tử, và mỗi phần tử cần mở và đóng theo thứ tự chính xác (khi lồng nhau). Một khi đảm bảo điều này, nó sẽ là một file .xml được xây dựng hoàn chỉnh. Chỉ có một phần tử gốc duy nhất: <unattend>.



```
<userdata>
  <AcceptEula>value</AcceptEula> (Yes/No)
  <FullName showUI="">value</FullName> (126 char max)optional
  <Organization showUI="">value</Organization> (126 char max)optional
  <ComputerName""showUI="">value</ComputerName> (15 char max)
  <ProductKey>****_****_****_****</ProductKey> (Valid Product Key)
</Userdata>
<DiskConfig>
  <Disk ID="" wipeDisk=""/> (ID is a 0-based number, wipeDisk=Yes/No)
  <Partition Action="" Label="" Size="" Letter="" Format="" Type=""/>
</DiskConfig>
```

**Hình 1-9. Một đoạn trong file unattend.xml**

Quá trình vận hành file unattend.xml sẽ ngừng lại với một thông báo lỗi nếu bất cứ điều nào sau đây là đúng:

Thỏa thuận cấp phép người dùng cuối không được chấp nhận

Khóa kích hoạt sản phẩm không hợp lệ

Không thể ghi vào đĩa cài đặt

Việc tạo file unattend.xml có thể hơi rắc rối một chút, tuy nhiên khi bạn đã tạo thành công, nó sẽ giúp công việc dễ dàng hơn rất nhiều. Có một số công cụ sẵn có trên web có thể giúp bạn tạo tập tin này. Bạn cũng có thể thỏa sức sáng tạo bằng cách thêm vào vài đoạn script để tự động đặt tên cho các máy tính tuân theo quy ước về cách đặt tên của bạn cũng như nhiều tùy chọn cấu hình khác.

### ***Câu hỏi và bài tập***

 Thực hành cài đặt Windows Server 2008 trên phần mềm Vmware.

### Chương 3. THIẾT LẬP VÀ QUẢN TRỊ HỆ THỐNG MẠNG

#### ➤ Giới thiệu chương:

Trong chương này nhằm cung cấp cho sinh viên các kỹ năng cơ bản về quản trị hệ thống mạng máy tính. Qua đó sinh viên có thể tự lắp đặt, cài đặt và vận hành một hệ thống mạng cục bộ và sử dụng các kỹ thuật quản trị cần thiết để bảo vệ an toàn dữ liệu cá nhân. Ngoài ra môn học còn cung cấp cho sinh viên khái niệm mô hình quản trị mạng Client – Server, các dịch vụ mạng phổ biến ngày nay. Áp dụng công nghệ của Microsoft, sinh viên sẽ triển khai nghiên cứu các ứng dụng của các dịch vụ mạng trong các mô hình quản trị mạng dạng Client-Server để từ đó có đủ kỹ năng để vận hành cho hệ thống mạng Client-Server cho các doanh nghiệp.

#### ➤ Mục tiêu chương:

Cung cấp cho sinh viên các kiến thức cơ bản về mô hình mạng và nguyên tắc hoạt động của các mô hình mạng. Cung cấp cho sinh viên kiến thức về nguyên tắc vận hành của các thiết bị mạng và nguyên lý triển khai hệ thống mạng cục bộ; trang bị cho sinh viên kiến thức và nguyên tắc hoạt động của mô hình Client – Server và các dịch vụ mạng căn bản.

Qua môn học này sinh viên được trang bị các kỹ năng để có thể cài đặt hệ thống mạng cục bộ và thực hiện các yêu cầu quản trị trên hệ thống mạng cục bộ. Bên cạnh đó sinh viên cũng được trang bị kỹ năng khai thác và vận hành các dịch vụ mạng theo mô hình Client – Server để có thể quản trị một hệ thống mạng lớn, tập trung và đáp ứng được các yêu cầu quản trị của doanh nghiệp.

Môn học này giúp sinh viên có khả năng phân tích, phán đoán và khoanh vùng các sự cố xảy ra trong hệ thống mạng cục bộ và mô hình Client – Server. Với môn học, sinh viên sẽ có khả năng tư duy, phân tích các yêu cầu nghiệp vụ để từ đó đưa ra các giải pháp kỹ thuật phù hợp, triển khai hệ thống để đáp ứng nhu cầu của khách hàng, doanh nghiệp.

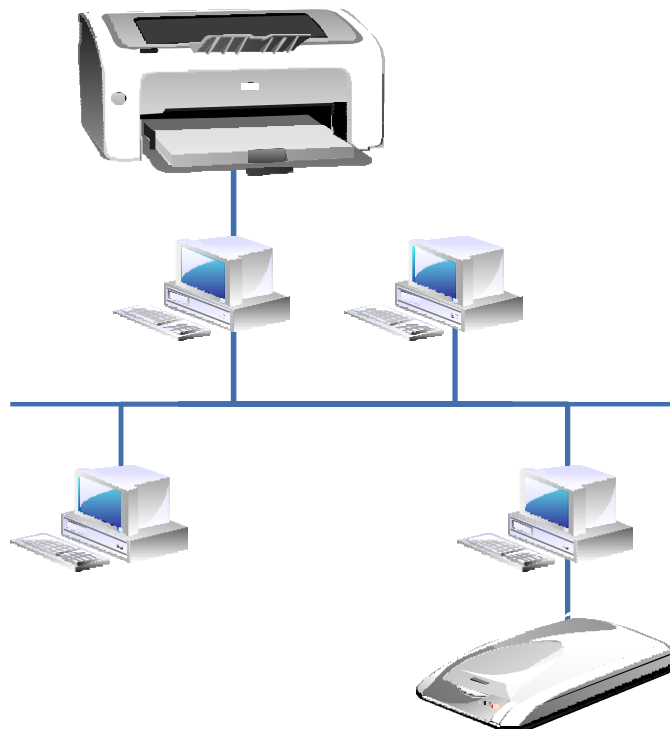
## Chương 3: Thiết lập và quản trị hệ thống mạng

### 3.1 Các mô hình mạng trong môi trường microsoft

#### 3.1.1 Mô hình mạng Workgroup

Mô hình mạng Workgroup là một nhóm máy tính mạng cùng chia sẻ tài nguyên như file dữ liệu, máy in. Nó là một nhóm logic của các máy tính mà tất cả chúng có cùng tên nhóm. Có thể có nhiều nhóm làm việc (workgroups) khác nhau cùng kết nối trên một mạng cục bộ (LAN).

Trong mô hình này, các máy tính có quyền hạn ngang nhau và không có các máy tính chuyên dụng làm nhiệm vụ cung cấp dịch vụ hay quản lý. Các máy tính tự bảo mật và quản lý các tài nguyên của riêng mình. Đồng thời, các máy tính cục bộ này cũng tự chứng thực cho người dùng cục bộ.



**Hình 2-1. Mô hình mạng Workgroup**

Mô hình mạng Workgroup cũng được coi là mạng peer-to-peer bởi vì tất cả các máy trong workgroup có quyền chia sẻ tài nguyên như nhau mà không cần sự chỉ định của Server. Mỗi máy tính trong nhóm tự bảo trì, bảo mật cơ sở dữ liệu cục bộ của nó. Điều này có nghĩa là, tất cả sự quản trị về tài khoản người

## Chương 3: Thiết lập và quản trị hệ thống mạng

dùng, bảo mật cho nguồn tài nguyên chia sẻ không được tập trung hóa. Bạn có thể kết nối tới một nhóm đã tồn tại hoặc khởi tạo một nhóm mới.

### 3.1.1.1 Ưu điểm mô hình Workgroup

Ưu điểm là Workgroups không yêu cầu máy tính chạy trên hệ điều hành Windows Server để tập trung hóa thông tin bảo mật; workgroups thiết kế và hiện thực đơn giản và không yêu cầu lập kế hoạch có phạm vi rộng và quản trị như domain yêu cầu; workgroups thuận tiện đối với nhóm có số máy tính ít và gần nhau ( $\leq 20$  máy).

### 3.1.1.2 Nhược điểm Workgroup

Nhược điểm là mỗi người dùng phải có một tài khoản người dùng trên mỗi máy tính mà họ muốn đăng nhập; bất kỳ sự thay đổi tài khoản người dùng, như là thay đổi mật khẩu hoặc thêm tài khoản người dùng mới, phải được làm trên tất cả các máy tính trong Workgroup, nếu bạn quên bổ sung tài khoản người dùng mới tới một máy tính trong nhóm thì người dùng mới sẽ không thể đăng nhập vào máy tính đó và không thể truy xuất tới tài nguyên của máy tính đó; việc chia sẻ thiết bị và file được xử lý bởi các máy tính riêng, và chỉ cho người dùng có tài khoản trên máy tính đó được sử dụng.

### 3.1.1.3 Mô hình mạng Domain (Client – Server)

Mô hình mạng Domain (hay mô hình Server) là một nhóm máy tính mạng cùng chia sẻ cơ sở dữ liệu thư mục tập trung (central directory database). Thư mục dữ liệu chứa tài khoản người dùng và thông tin bảo mật cho toàn bộ Domain. Thư mục dữ liệu này được biết như là thư mục hiện hành (Active Directory).

Ngược lại với mô hình Workgroup, trong mô hình Domain thì việc quản lý và chứng thực người dùng mạng tập trung tại máy tính Primary Domain Controller. Các tài nguyên mạng cũng được quản lý tập trung và cấp quyền hạn cho từng người dùng. Lúc đó trong hệ thống có các máy tính chuyên dụng làm nhiệm vụ cung cấp các dịch vụ và quản lý các máy trạm.

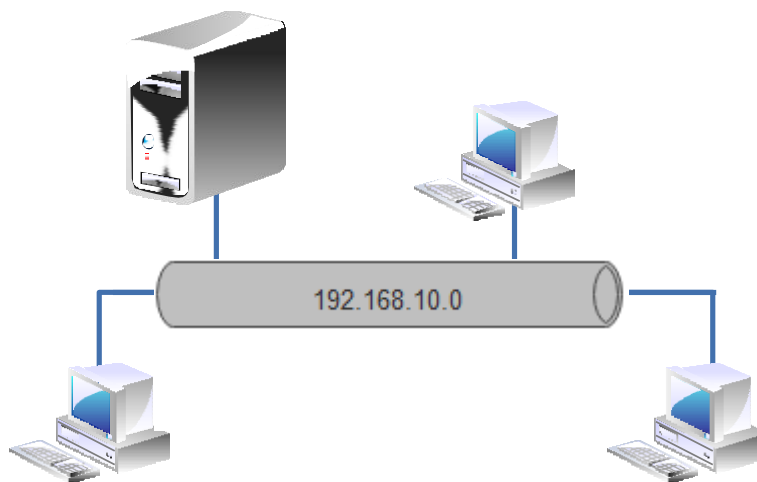
Trong một Domain, thư mục chỉ tồn tại trên các máy tính được cấu hình như máy điều khiển miền (domain controller). Một domain controller là một Server quản lý tất cả các khía cạnh bảo mật của Domain. Không giống như

### Chương 3: Thiết lập và quản trị hệ thống mạng

mạng Workgroup, bảo mật và quản trị trong domain được tập trung hóa. Để có Domain controller, những máy chủ (server) phải chạy dịch vụ làm Domain controller (dịch vụ được tích hợp sẵn trên các phiên bản Windows Server

Một domain không được xem như một vị trí đơn hoặc cấu hình mạng riêng biệt. Các máy tính trong cùng domain có thể ở trên một mạng LAN hoặc WAN. Chúng có thể giao tiếp với nhau qua bất kỳ kết nối vật lý nào, như: Dial-up, Integrated Services Digital Network (ISDN), Ethernet, Token Ring, Frame Relay, Satellite, Fibre Channel.

Ưu điểm là cho phép quản trị tập trung. Nếu người dùng thay đổi mật khẩu của họ, thì sự thay sẽ được cập nhật tự động trên toàn Domain; Domain cung cấp quy trình đăng nhập đơn giản để người dùng truy xuất các tài nguyên mạng mà họ được phép truy cập; Domain cung cấp linh động để người quản trị có thể khởi tạo mạng rất rộng lớn.



**Hình 2-2. Mô hình mạng Client/Server**

Các thành phần cơ bản trong Windows Server có thể chứa các kiểu máy tính sau:

- Máy điều khiển miền (Domain controllers) lưu trữ và bảo trì bản sao thư mục. Trong domain, tài khoản người dùng được tạo một lần, Windows Server ghi nó trong thư mục này. Khi người dùng đăng nhập tới máy tính trong domain, domain controller kiểm tra thư mục nhờ tên người sử dụng, mật khẩu và giới hạn đăng nhập. Khi có nhiều domain controllers, chúng định kỳ tái tạo thông tin thư mục của chúng.

## Chương 3: Thiết lập và quản trị hệ thống mạng

- Các máy chủ thành viên (Member servers): Một máy member server là một máy chủ mà không được cấu hình như là domain controller. Máy chủ không lưu trữ thông tin thư mục và không thể xác nhận domain người dùng. Các máy chủ có thể cung cấp các tài nguyên chia sẻ như các thư mục dùng chung hay các máy in.
- Các máy tính trạm (Client computers): Các máy tính trạm chạy một hệ điều hành dùng cho máy trạm của người dùng và cho phép người dùng truy cập tới nguồn tài nguyên trong domain.

Không giống như Workgroup, Domain phải tồn tại trước khi người dùng tham gia vào nó. Việc tham gia vào Domain luôn yêu cầu người quản trị Domain cung cấp tài khoản cho máy tính của người dùng tới domain đó. Tuy nhiên, nếu người quản trị cho người dùng đúng đặc quyền, người dùng có thể khởi tạo tài khoản máy tính của mình trong quá trình cài đặt.

### 3.1.2 Giới thiệu Active Directory

Active Directory là một kiến trúc độc quyền của Microsoft. Đây là một kiến trúc không thể thiếu được trên Windows Server, được hiểu nôm na là một dịch vụ thư mục. Active Directory là một hệ thống được chuẩn hóa với khả năng quản trị tập trung hoàn hảo về người dùng cũng như các nguồn tài nguyên trong một hệ thống mạng.

Active Directory là một kiến trúc độc quyền của Microsoft. Đây là một kiến trúc không thể thiếu được trên Windows Server, được hiểu nôm na là một dịch vụ thư mục. Active Directory là một hệ thống được chuẩn hóa với khả năng quản trị tập trung hoàn hảo về người dùng cũng như các nguồn tài nguyên trong một hệ thống mạng. Cũng cần phải chú ý, Active Directory được sử dụng trong mô hình mạng “*Server – Client*”.

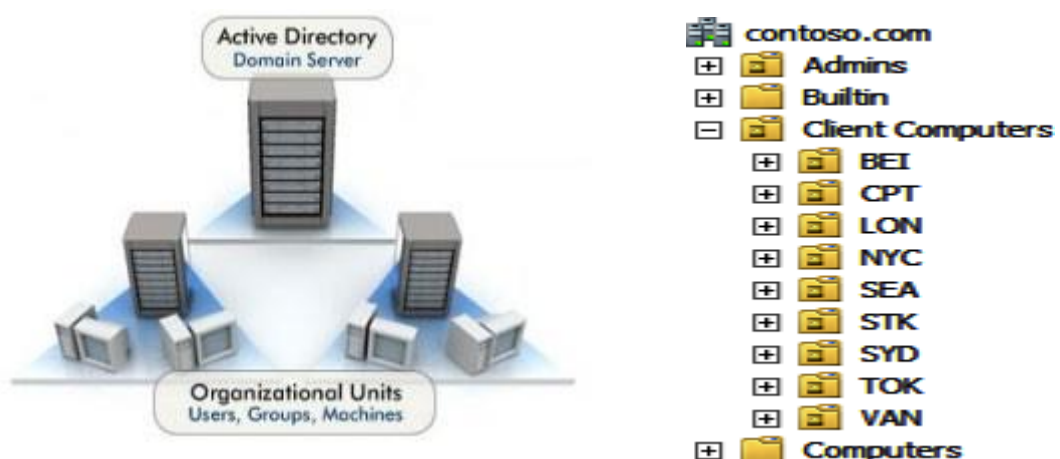


Hình 2-3. Active Directory trên Windows Server 2008

### 3.1.3 Các thành phần cơ bản và chức năng của Active Directory

#### 3.1.3.1 OU (Organization Unit)

Đây được coi là một trong những khái niệm căn bản nhất trong Active Directory. Vậy OU là gì? Cần nhớ là điểm ưu việt của Active Directory là nó có thể chứa tới hàng triệu đối tượng khác nhau. Vậy làm sao để quản lý các đối tượng này một cách hiệu quả. Bạn sẽ không phải ngồi lần mò hoặc tìm kiếm trong cả đống đối tượng như vậy mà đơn giản hơn các đối tượng đó có thể được nhóm lại với nhau theo một tiêu chí hay nguyên tắc nào đó – và đó chính là OU (hay còn được gọi là đơn vị tổ chức dữ liệu).



Hình 2-4. Mô tả Organization Unit - đơn vị tổ chức dữ liệu

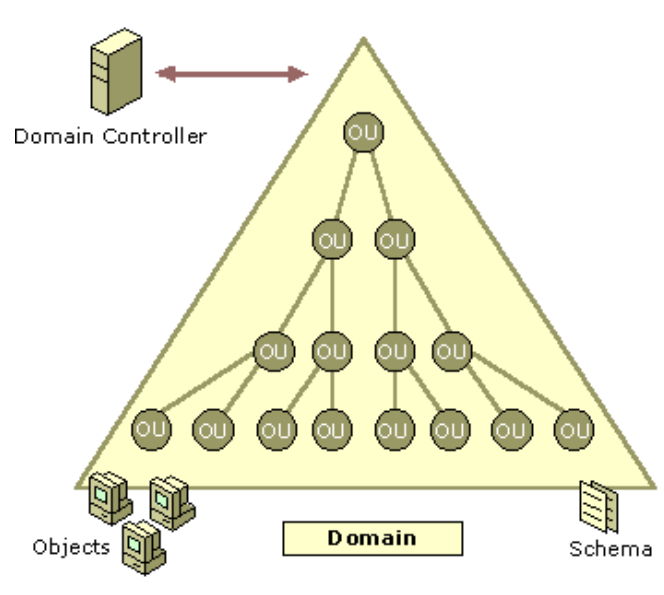
Trong thực tế, các bạn có thể sử dụng OU để lưu các tài khoản người dùng trong một phòng ban, hay các máy tính trong phòng ban đó, hoặc cũng có thể

### Chương 3: Thiết lập và quản trị hệ thống mạng

tổ chức cả công ty thành một cây thư mục các OU chứa các máy tính, các group, hay các tài khoản người dùng như hình trên.

#### 3.1.3.2 Domain (tên miền)

Domain ở đây được hiểu là một miền, có nghĩa là khi hệ thống của bạn sử dụng Active Directory, đồng nghĩa là tất cả các máy tính trong này đều thuộc về ít nhất là cùng một miền nào đó. Trong một miền thì phải có ít nhất là một máy chủ quản lý miền (Domain Controller) trở lên. Các máy chủ trong cùng một miền thì sẽ đồng bộ với nhau về các đối tượng trong miền đó (Domain Name Context). Các máy chủ này sẽ đảm trách các vai trò về quản lý chung trên toàn miền đó.



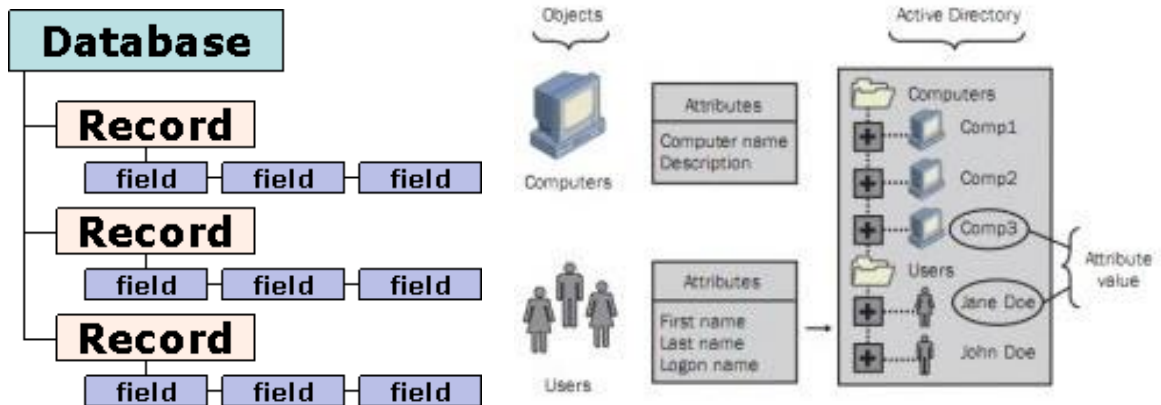
**Hình 2-5. Mô tả việc quản lý các đối tượng trong Domain**

#### 3.1.3.3 Kiến trúc của Active Directory

Active Directory như một cơ sở dữ liệu (Database)? Với các bạn học lập trình, hẳn cũng rõ có 2 khái niệm rất thân quen, đó là các bản ghi (record) và các trường (field). Nói Active Directory như là một database chính là ở điểm này.



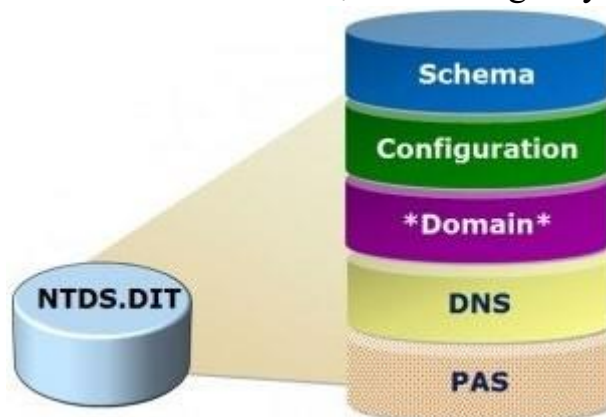
## Chương 3: Thiết lập và quản trị hệ thống mạng



Hình 2-6. Cấu trúc cơ sở dữ liệu của Domain

Có thể thấy rất đơn giản ở đây, kiến trúc Active Directory bao gồm nhiều đối tượng (objects) và trên mỗi một đối tượng lại có nhiều thuộc tính (attribute) khác nhau. Ở hình trên, trong AD có 2 kiểu đối tượng là máy tính và người dùng. Với mỗi máy tính lại bao gồm thuộc tính như tên máy tính, mô tả về máy tính đó. Với người dùng thì thuộc tính lại là họ, tên và tên đăng nhập hệ thống.

Đó là lý do tại sao chúng ta có thể so sánh Active Directory như một database, thứ hai, cũng có thể coi Active Directory như một Datastore, vậy Datastore là gì? Hiểu rộng thì cứ xem nó là một cái khung, một cái thùng chứa, hay hiểu đơn giản đi thì cứ coi nó như một cái ổ cứng máy tính cũng được.



Hình 2-7. Thành phần cốt lõi kiến trúc Active Directory

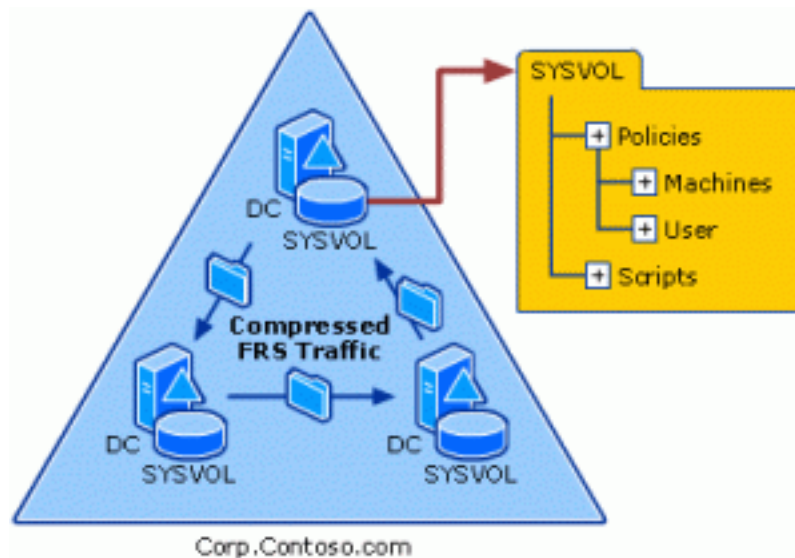
### 3.1.3.3.1 Datastore này sẽ bao gồm 2 thành phần:

- Thứ nhất: NTDS.DIT

### Chương 3: Thiết lập và quản trị hệ thống mạng

- Domain: tại đây chứa các đối tượng mà các bạn sẽ phải tương tác hàng ngày, ví dụ như user, computer, OU....
- Schema: là nơi lưu trữ các định nghĩa về từng thuộc tính trên mỗi đối tượng
- Configuration: chứa toàn bộ các cấu hình của Active Directory
- DNS: một hệ thống Active Directory thường là luôn tích hợp kèm với dịch vụ DNS, mọi cấu hình thuộc về DNS được lưu tại đây.
- Global Catalog: đảm nhiệm chức năng chứng thực (authentication) cho các đối tượng trong một hệ thống Active Directory. Máy chủ quản trị miền nào (Domain controller) lưu trữ Global Catalog thì được gọi là Global Catalog Server.
- Thứ hai: SYSVOL

Đây là một thư mục chứa các chính sách dành cho các đối tượng người dùng hoặc máy tính và các đoạn script quan trọng khác. Cần chú ý là các chính sách này không giống như việc hệ thống gán quyền truy cập các tài nguyên (authorization)



**Hình 2-8. Sysvol trong kiến trúc Active Directory**

## Chương 3: Thiết lập và quản trị hệ thống mạng

### 3.1.4 Cài đặt và cấu hình Active Directory

Tương tự như Windows Server 2003 khi nâng cấp Domain Controller 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



Hình 2-9. Add Roles khi nâng cấp Domain

Khi đó, xuất hiện trang Before You Begin, nhấn Next để tiếp tục



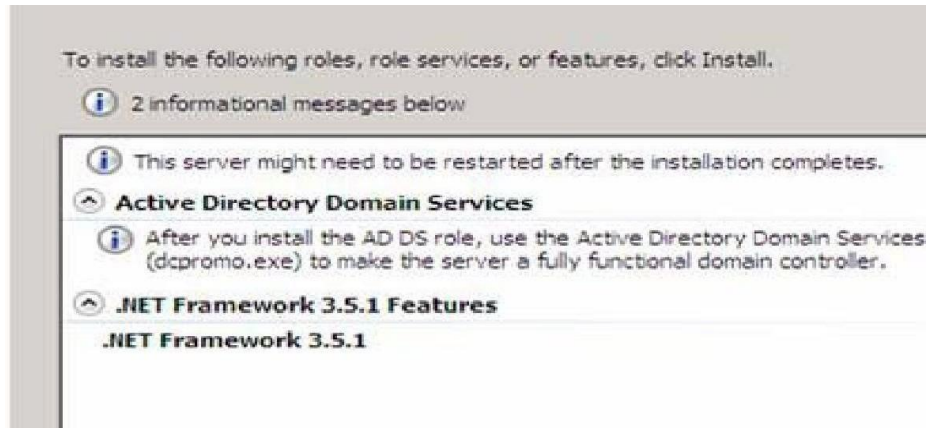
Hình 2-10. Trang hộp thoại Before You Begin

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.

## Chương 3: Thiết lập và quản trị hệ thống mạng

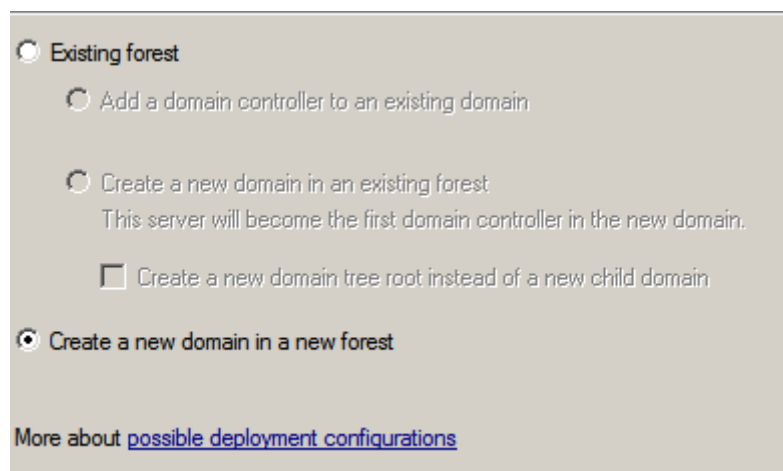
Kích Install để cài đặt các file yêu cầu



**Hình 2-11. Hộp thoại cài đặt Server Roles**

Sau khi cài đặt thành công dịch vụ Server Roles Vào Start → Run → DCPROMO thì hộp thoại Welcome to the Active Directory Domain Service Installation Wizard → Kích Next → Kích Next

Trong trang Choose a Deployment Configuration → Create a new domain in a new forest



**Hình 2-12. Create a new domain in a new forest**

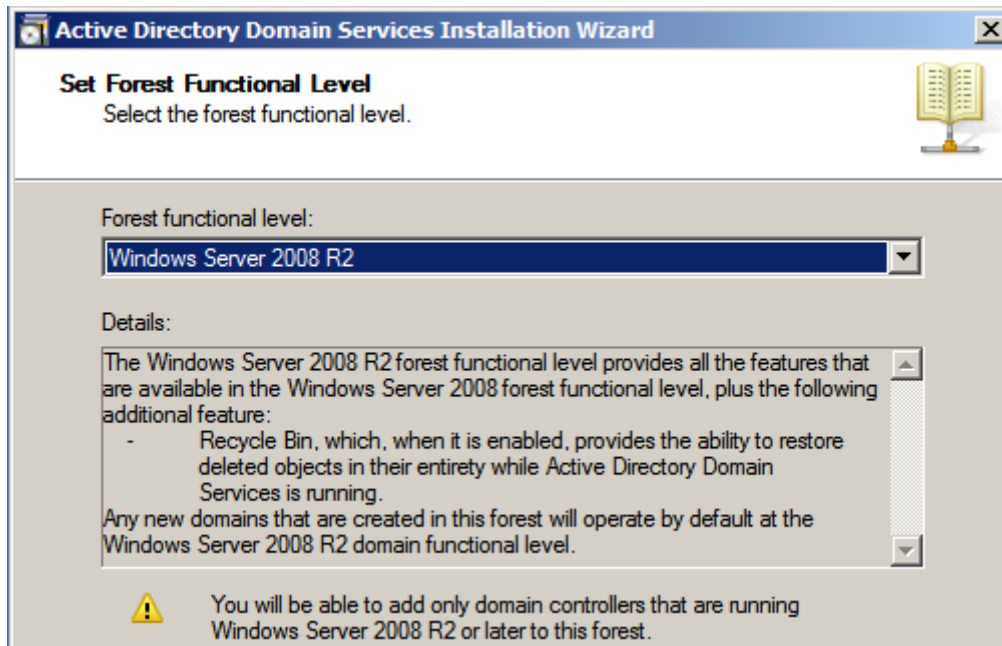
Trong trang Name the Forest Root Domain, nhập vào tên của miền trong hộp nhập liệu FQDN of the forest root domain. Nhấn Next để tiếp tục

## Chương 3: Thiết lập và quản trị hệ thống mạng



Hình 2-13. Hộp thoại điền tên miền khi nâng cấp Domain

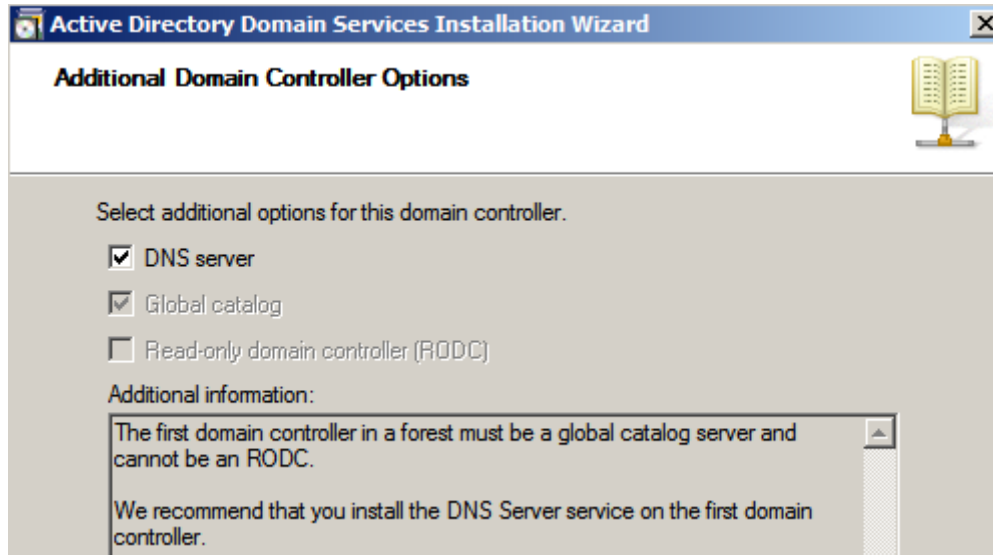
Trong trang Set Forest Functional Level, chọn Windows Server 2008. Nhấn Next để tiếp tục.



Hình 2-14. Hộp thoại chọn Forest Function Level

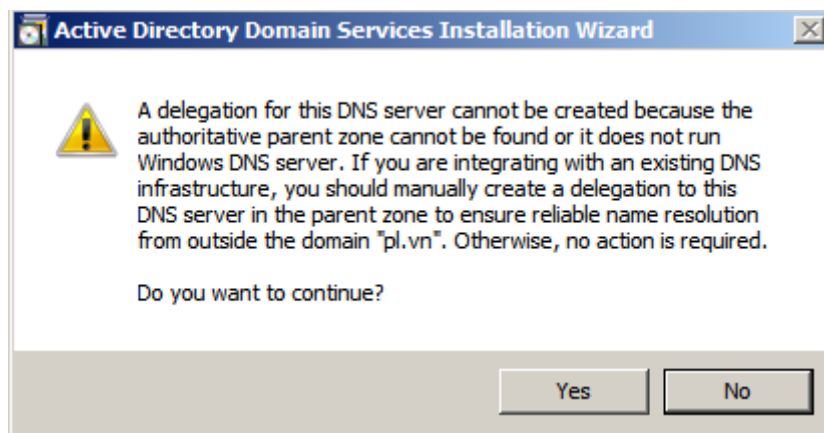
Trong trang Additional Domain Controller Options, Chọn DNS server và kích Next

### Chương 3: Thiết lập và quản trị hệ thống mạng



**Hình 2-15. Hộp thoại Add thêm dịch vụ DNS**

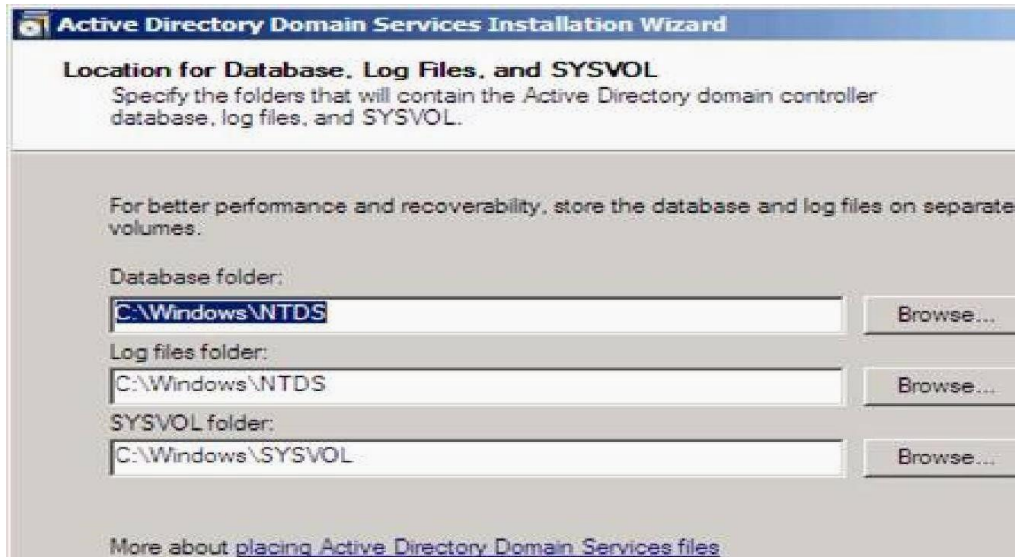
Một hộp thoại sẽ xuất hiện nói rằng không thể tạo đại diện cho máy chủ DNS này vì không thể tìm thấy vùng xác thực hoặc nó không chạy Windows DNS server. Lý do cho điều này là vì đây là DC đầu tiên trên mạng. Nhấn Next để tiếp tục.



**Hình 2-16. Hộp thoại xác thực Add thêm dịch vụ DNS**

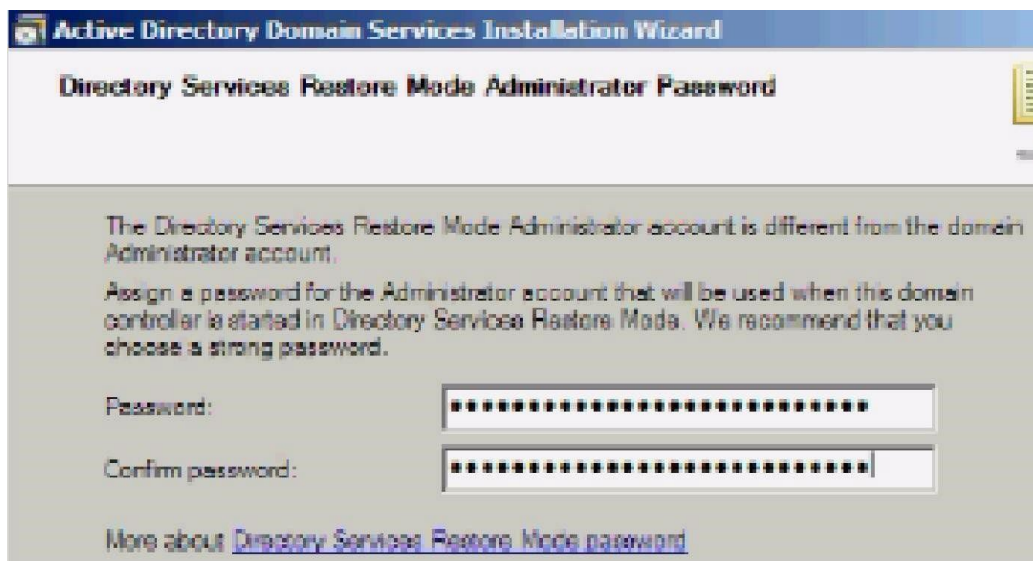
Đường dẫn lưu trữ Database, Log Files và SYSVOL, ta có thể thay đổi đường dẫn tại vị trí khác. Tuy nhiên, nơi lưu trữ các thành phần này phải là phân vùng được định dạng NTFS, kích Next

### Chương 3: Thiết lập và quản trị hệ thống mạng



**Hình 2-17. Hộp thoại đường dẫn lưu trữ Database Active Directory**

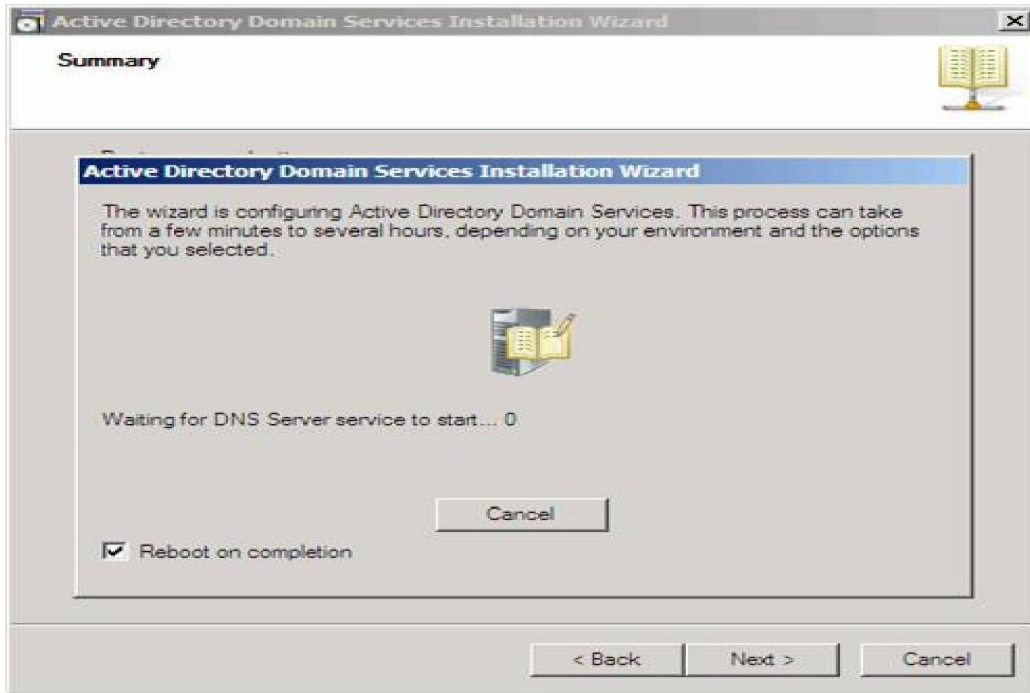
Trong Directory Service Restore Mode Administrator Password, nhập một mật khẩu mạnh vào các hộp nhập liệu Password và Confirm password.



**Hình 2-18. Hộp thoại thiết lập mật khẩu phục hồi sơ sở dữ liệu của Active Directory**

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 Domain được hoàn tất.

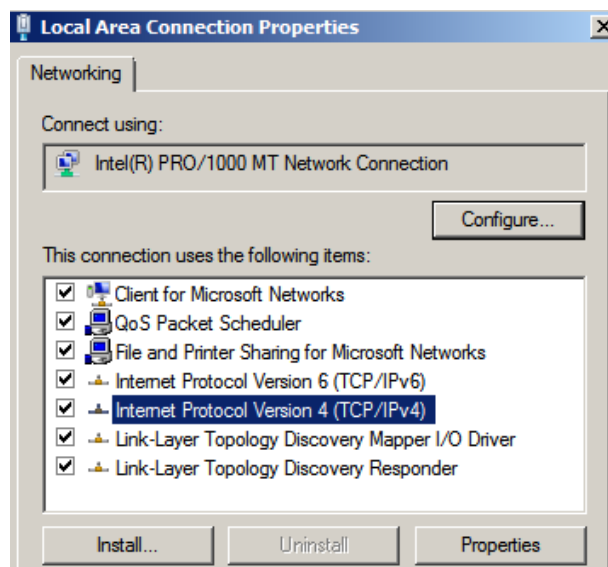
## Chương 3: Thiết lập và quản trị hệ thống mạng



Hình 2-19. Hộp thoại diễn ra quá trình nâng cấp Domain

### 3.1.5 Gia nhập máy trạm 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



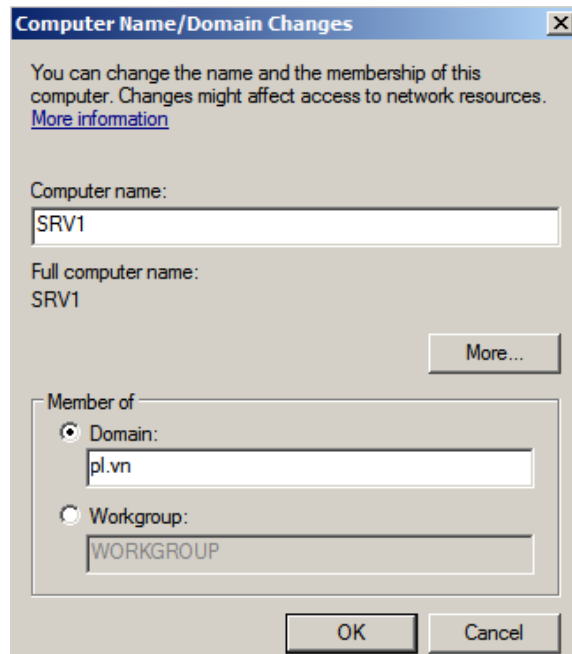
Hình 2-20. Đặt IP cho máy trạm

Tại máy trạm click phải My Computer → Properties → Change Settings.



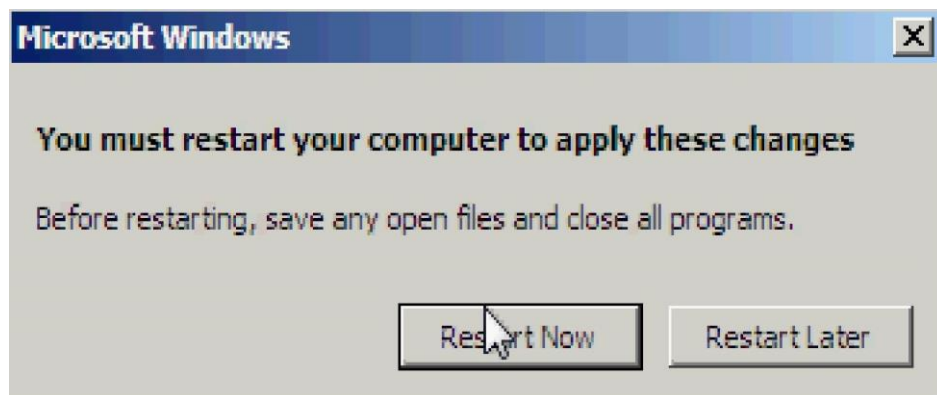
**Chương 3: Thiết lập và quản trị hệ thống mạng**  
Nhấn nút Change. Chọn Domain → Nhập tên domain

## Chương 3: Thiết lập và quản trị hệ thống mạng



**Hình 2-21. Hộp thoại gia nhập máy trạm vào Domain**

Nhấn OK → Nhấn Close → Restart Now. Công việc gia nhập máy trạm vào Domain thành công.



**Hình 2-22. Hộp thông báo gia nhập máy trạm vào Domain thành công**

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

### **3.1.6 Xây dựng Organizational Unit**

Organizational Units hay OU là đơn vị nhỏ nhất trong hệ thống Active Directory, nó được xem là một vật chứa các đối tượng (Object) được dùng để sắp xếp các đối tượng khác nhau phục vụ cho mục đích quản trị của bạn. Việc sử dụng OU có hai công dụng chính như sau:

## Chương 3: Thiết lập và quản trị hệ thống mạng

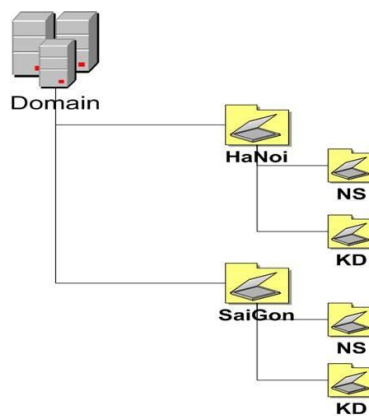
Trao quyền kiểm soát một tập hợp các tài khoản người dùng, máy tính hay các thiết bị mạng cho một nhóm người hay một quản trị viên phụ nào đó (sub-administrator), từ đó giảm bớt công tác quản trị cho người quản trị toàn bộ hệ thống.

Kiểm soát và khóa bớt một số chức năng trên các máy trạm của người dùng trong OU thông qua việc sử dụng các đối tượng chính sách nhóm (Group Policy)

- Vào Administrative Tools → Active Directory User and Computer hoặc vào Start → Run gõ: dsa.msc.

- Right click tại Server → New → Organizational Unit → Gõ tên OU →

Ok.



Hình 2-23. Cấu trúc cây OU

### 3.1.7 Tài khoản người dùng User account

Trong hệ thống mạng Windows Server 2008, người dùng muốn truy cập vào tài nguyên mạng cần phải có một user account. Với user account này, người dùng sẽ được chứng thực và cấp phát quyền truy cập.

Một user account là một đối tượng chứa tất cả các thông tin định nghĩa một người dùng trong Windows Server 2008.

Windows Server 2008 có các kiểu user account:

- User account domain: được tạo trên máy chủ DC. User này có thể logon vào bất kỳ các máy Client nào trên mạng. User được tạo trên DC thì mặc định tài khoản này sẽ là Domain user, tuy nhiên có thể gán quyền cho user vào nhóm [Member of] để có các quyền khác.

## Chương 3: Thiết lập và quản trị hệ thống mạng

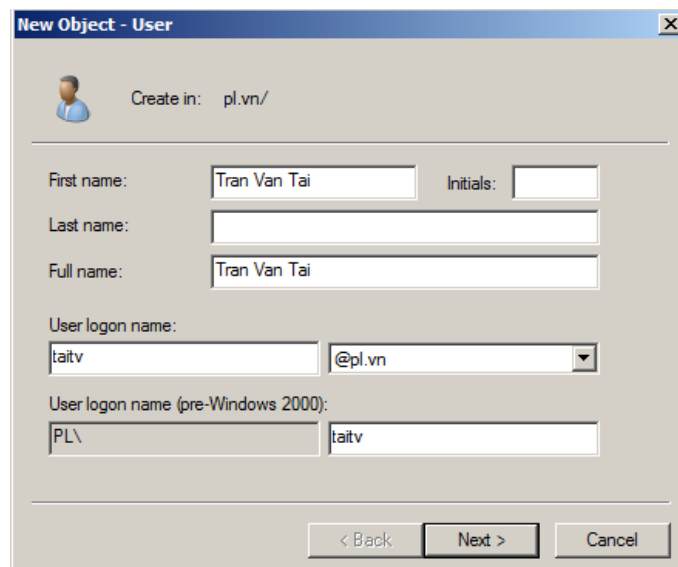
- Built in account: là các tài khoản được tạo sẵn khi cài hệ điều hành và thăng cấp thành DC. Mục đích là để trao quyền đặc biệt cho người dùng trên hệ điều hành. Ví dụ một số Built in account:

- Administrator
- Account operator
- Backup operator
- Print operator
- Guest

- Local user account: là tài khoản người dùng được định nghĩa trên máy cục bộ và chỉ được phép logon, truy cập các tài nguyên trên máy tính cục bộ. Nếu muốn truy cập các tài nguyên trên mạng thì người dùng này phải chứng thực lại với máy domain controller hoặc máy tính chứa tài nguyên chia sẻ.

- Tạo tài khoản người dùng: Right click tại OU cần chứa các User → New → User → Điền đầy đủ thông tin của User → Next → Điền Password.

- Chú ý: Password mặc định khi khởi tạo Domain phải đặt  $\geq 7$  ký tự và Password phải phức tạp. Vd: P@ssword.



The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: pl.vn/'. Below this, there are several input fields: 'First name' with 'Tran Van Tai', 'Last name' (empty), 'Full name' with 'Tran Van Tai', 'User logon name' with 'taitv', and 'User logon name (pre-Windows 2000)' with 'PL\'. There are also 'Initials' and '@pl.vn' dropdown menus. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

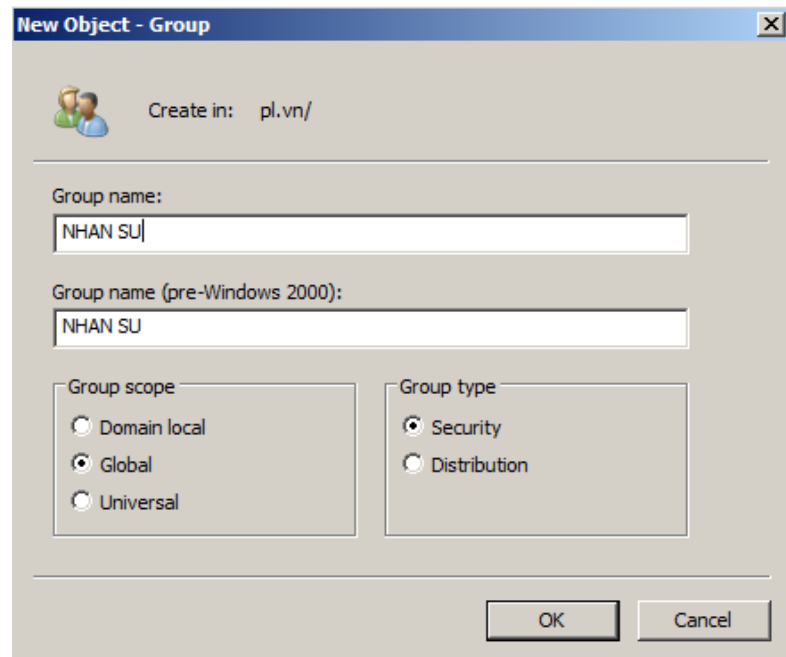
Hình 2-24. Hộp thoại tạo User Account

### 3.1.8 Tài khoản người dùng nhóm (Groups)

- Tạo nhóm

### Chương 3: Thiết lập và quản trị hệ thống mạng

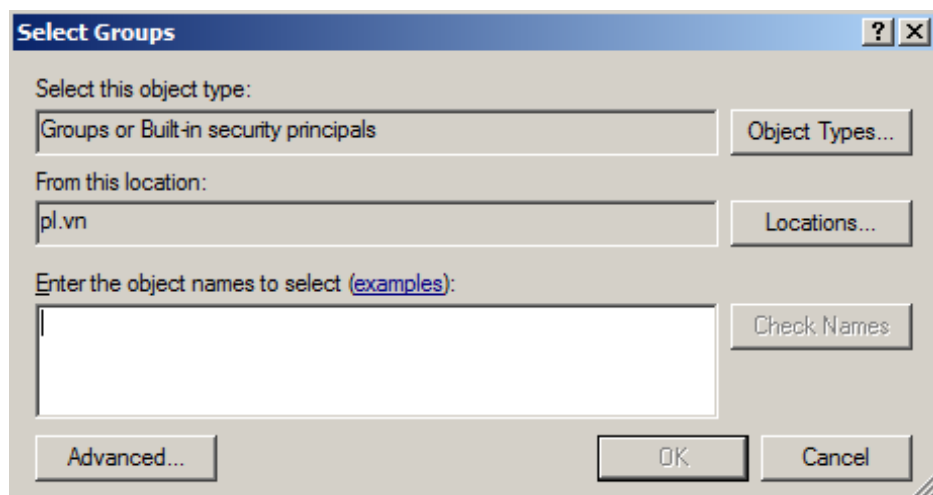
Right click tại OU cần chứa các Group → New → Group → Gõ tên Group → Ok.



Hình 2-25. Hộp thoại tạo nhóm

- Add User vào trong nhóm

Chọn một hoặc nhiều User cần Add vào Group. Right click vào đối tượng User đã chọn → Add to Group → Gõ tên Group cần Add → Ok.

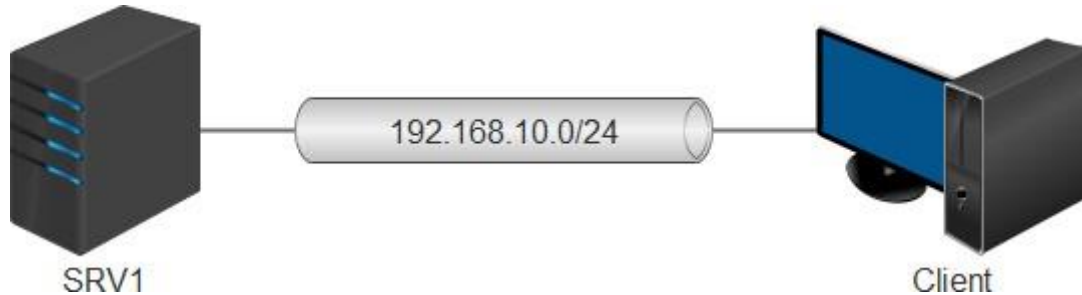


Hình 2-26. Hộp thoại thêm tài khoản người dùng vào trong nhóm

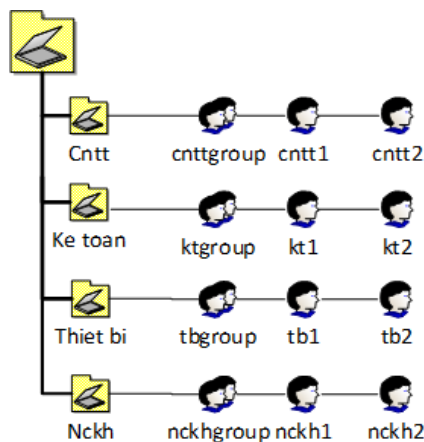
## Chương 3: Thiết lập và quản trị hệ thống mạng

### Câu hỏi và bài tập

Cho mô hình mạng sau:



- ✍ Thiết lập Ip cho hệ thống theo mô hình trên.
- ✍ Xây dựng Domain với tên miền: Hotec.edu.vn



- ✍ Tạo User, OU, Group, Add User vào trong Group
- ✍ Cho máy Client tham gia vào Doamain
- ✍ Máy Client đăng nhập vào các User vừa tạo

### 3.2 Quản lý tài khoản người dùng và nhóm

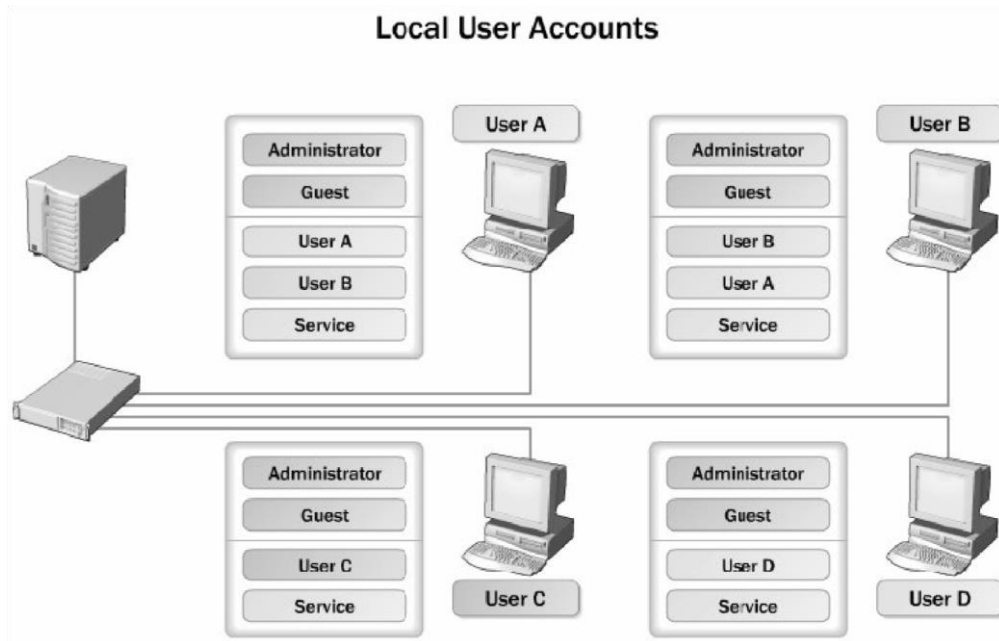
#### 3.2.1 Tài khoản người dùng cục bộ

Tài khoản người dùng cục bộ (local user account) là tài khoản người dùng được định nghĩa trên máy cục bộ và chỉ được phép logon, truy cập các tài nguyên trên máy tính cục bộ. Nếu muốn truy cập các tài nguyên trên mạng thì người dùng này phải chứng thực lại với máy domain controller hoặc máy tính chứa tài nguyên chia sẻ. Bạn tạo tài khoản người dùng cục bộ với công cụ Local Users and Group trong Computer Management (COMPMGMT.MSC). Các tài

## Chương 3: Thiết lập và quản trị hệ thống mạng

khoản cục bộ tạo ra trên máy stand-alone server, member server hoặc các máy trạm đều được lưu trữ trong tập tin cơ sở dữ liệu

SAM (Security Accounts Manager). Tập tin SAM này được đặt trong thư mục `\Windows\system32\config`.



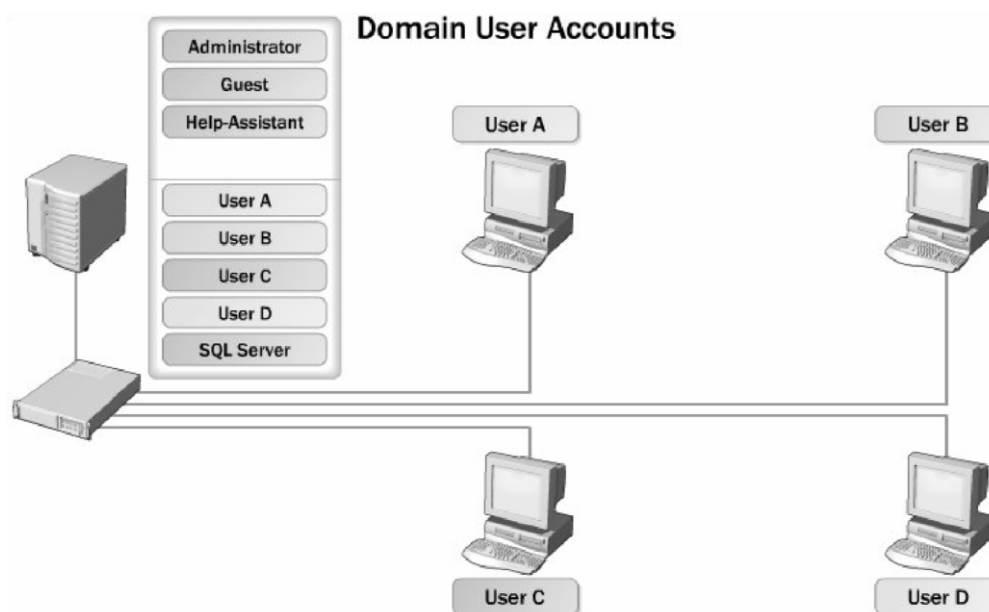
Hình 2-27. Tổ chức tài khoản người dùng cục bộ

### 3.2.2 Tài khoản người dùng miền

Tài khoản người dùng miền (domain user account) là tài khoản người dùng được định nghĩa trên Active Directory và được phép đăng nhập (logon) vào mạng trên bất kỳ máy trạm nào thuộc vùng. Đồng thời với tài khoản này người dùng có thể truy cập đến các tài nguyên trên mạng. Bạn tạo tài khoản người dùng miền với công cụ Active Directory Users and Computer (Dsa.msc).

Khác với tài khoản người dùng cục bộ, tài khoản người dùng miền không chứa trong các tập tin cơ sở dữ liệu SAM mà chứa trong tập tin NTDS.DIT, theo mặc định thì tập tin này chứa trong thư mục `\Windows\NTDS`.

## Chương 3: Thiết lập và quản trị hệ thống mạng



Hình 2-28. Tổ chức tài khoản người dùng miền

### 3.2.3 Chứng thực và kiểm soát truy cập

#### 3.2.3.1 Các giao thức chứng thực

Chứng thực trong Windows Server 2008 là quy trình gồm hai giai đoạn: đăng nhập tương tác và chứng thực mạng. Khi người dùng đăng nhập vùng bằng tên và mật mã, quy trình đăng nhập tương tác sẽ phê chuẩn yêu cầu truy cập của người dùng. Với tài khoản cục bộ, thông tin đăng nhập được chứng thực cục bộ và người dùng được cấp quyền truy cập máy tính cục bộ. Với tài khoản miền, thông tin đăng nhập được chứng thực trên Active Directory và người dùng có quyền truy cập các tài nguyên trên mạng. Như vậy với tài khoản người dùng miền ta có thể chứng thực trên bất kỳ máy tính nào trong miền. Windows 2008 hỗ trợ nhiều giao thức chứng thực mạng, nổi bật nhất là:

- Kerberos V5: là giao thức chuẩn Internet dùng để chứng thực người dùng và hệ thống.
- NT LAN Manager (NTLM): là giao thức chứng thực chính của Windows NT.
- Secure Socket Layer/Transport Layer Security (SSL/TLS): là cơ chế chứng thực chính được dùng khi truy cập vào máy phục vụ Web an toàn.



## Chương 3: Thiết lập và quản trị hệ thống mạng

### 3.2.3.2 Số nhận diện bảo mật SID

Tuy hệ thống Windows Server 2008 dựa vào tài khoản người dùng (user account) để mô tả các quyền hệ thống (rights) và quyền truy cập (permission) nhưng thực sự bên trong hệ thống mỗi tài khoản được đặc trưng bởi một con số nhận dạng bảo mật SID (Security Identifier). SID là thành phần nhận dạng không trùng lặp, được hệ thống tạo ra đồng thời với tài khoản và dùng riêng cho hệ thống xử lý, người dùng không quan tâm đến các giá trị này. SID bao gồm phần SID vùng cộng thêm với một RID của người dùng không trùng lặp. SID có dạng chuẩn “S-1-5-21-D1-D2-D3-RID”, khi đó tất cả các SID trong miền đều có cùng giá trị D1, D2, D3, nhưng giá trị RID là khác nhau. Hai mục đích chính của việc hệ thống sử dụng SID là:

- Dễ dàng thay đổi tên tài khoản người dùng mà các quyền hệ thống và quyền truy cập không thay đổi.
- Khi xóa một tài khoản thì SID của tài khoản đó không còn giá trị nữa, nếu chúng ta có tạo một tài khoản mới cùng tên với tài khoản vừa xóa thì các quyền cũ cũng không sử dụng được bởi vì khi tạo tài khoản mới thì giá trị SID của tài khoản này là một giá trị mới

### 3.2.3.3 Kiểm soát hoạt động truy cập của đối tượng

Active Directory là dịch vụ hoạt động dựa trên các đối tượng, có nghĩa là người dùng, nhóm, máy tính, các tài nguyên mạng đều được định nghĩa dưới dạng đối tượng và được kiểm soát hoạt động truy cập dựa vào bộ mô tả bảo mật ACE. Chức năng của bộ mô tả bảo mật bao gồm:

- Liệt kê người dùng và nhóm nào được cấp quyền truy cập đối tượng.
- Định rõ quyền truy cập cho người dùng và nhóm.
- Theo dõi các sự kiện xảy ra trên đối tượng.
- Định rõ quyền sở hữu của đối tượng.

Các thông tin của một đối tượng Active Directory trong bộ mô tả bảo mật được xem là mục kiểm soát hoạt động truy cập ACE (Access Control Entry). Một ACL (Access Control List) chứa nhiều ACE, nó là danh sách tất cả người dùng và nhóm có quyền truy cập đến đối tượng. ACL có đặc tính kế

## Chương 3: Thiết lập và quản trị hệ thống mạng

thừa, có nghĩa là thành viên của một nhóm thì được thừa hưởng các quyền truy cập đã cấp cho nhóm này.

### 3.2.4 Các tài khoản tạo sẵn

#### 3.2.4.1 Tài khoản người dùng tạo sẵn

Tài khoản người dùng tạo sẵn (Built-in) là những tài khoản người dùng mà khi ta cài đặt Windows Server 2008 thì mặc định được tạo ra. Tài khoản này là hệ thống nên chúng ta không có quyền xóa đi nhưng vẫn có quyền đổi tên (chú ý thao tác đổi tên trên những tài khoản hệ thống phức tạp một chút so với việc đổi tên một tài khoản bình thường do nhà quản trị tạo ra). Tất cả các tài khoản người dùng tạo sẵn này đều nằm trong Container Users của công cụ Active Directory User and Computer. Sau đây là bảng mô tả các tài khoản người dùng được tạo sẵn:

**Bảng 2-1. Bảng mô tả các tài khoản người dùng được tạo sẵn**

Tên tài khoản	Mô tả
Administrator	<b>Administrator</b> là một tài khoản đặc biệt, có toàn quyền trên máy tính hiện tại. Bạn có thể đặt mật khẩu cho tài khoản này trong lúc cài đặt <b>Windows Server 2008</b> . Tài khoản này có thể thi hành tất cả các tác vụ như tạo tài khoản người dùng, nhóm, quản lý các tập tin hệ thống và cấu hình máy in...
Guest	Tài khoản <b>Guest</b> cho phép người dùng truy cập vào các máy tính nếu họ không có một tài khoản và mật mã riêng. Mặc định là tài khoản này không được sử dụng, nếu được sử dụng thì thông thường nó bị giới hạn về quyền, ví dụ như là chỉ được truy cập <b>Internet</b> hoặc in ấn.
Anonymous_User	Tài khoản đặc biệt được dùng cho dịch vụ <b>IIS</b> . <b>IIS</b> hỗ trợ cho các ứng dụng điện thoại có các đặc tính như: <b>caller ID</b> , <b>video conferencing</b> , <b>conference calling</b> , và <b>faxing</b> . Muốn sử dụng <b>IIS</b> thì dịch vụ <b>IIS</b> phải được cài đặt.

### Chương 3: Thiết lập và quản trị hệ thống mạng

Tên tài khoản	Mô tả
_computername	khoản đặc biệt được dùng trong các truy cập giấu tên trong dịch vụ <b>IIS</b> trên máy tính có cài <b>IIS</b> .
!_computername	khoản đặc biệt được dùng cho <b>IIS</b> khởi động các tiến trình của các ứng dụng trên máy có cài <b>IIS</b> .
	khoản đặc biệt được dùng cho dịch vụ trung tâm phân phối khóa ( <b>Distribution Center</b> )
ernetUser	khoản đặc biệt được dùng cho <b>Terminal Services</b> .

#### 3.2.5 Tài khoản nhóm Domain Local tạo sẵn

Nhưng chúng ta đã thấy trong công cụ Active Directory User and Computers, container Users chứa nhóm universal, nhóm domain local và nhóm global là do hệ thống đã mặc định quy định trước. Nhưng một số nhóm domain local đặc biệt được đặt trong container Built-in, các nhóm này không được di chuyển sang các OU khác, đồng thời nó cũng được gán một số quyền cố định trước nhằm phục vụ cho công tác quản trị. Bạn cũng chú ý rằng là không có quyền xóa các nhóm đặc biệt này.

**Bảng 2-2. Bảng mô tả tài khoản nhóm Domain Local tạo sẵn**

Tên nhóm	Mô tả
administrators	này mặc định được ấn định sẵn tất cả các quyền hạn cho nên thành viên của nhóm này có toàn quyền trên hệ thống mạng. Nhóm <b>Domain Admins</b> và <b>Enterprise Admins</b> là thành viên mặc định của nhóm <b>Administrators</b> .

### Chương 3: Thiết lập và quản trị hệ thống mạng

nhóm	Mô tả
nt Operators	viên của nhóm này có thể thêm, xóa, sửa được các tài khoản người dùng, tài khoản máy và tài khoản nhóm. Tuy nhiên họ không có quyền xóa, sửa các nhóm trong <b>container Built-in</b> và <b>OU</b> .
in ollers	này chỉ có trên các <b>Domain Controller</b> và mặc định không có thành viên nào, thành viên của nhóm có thể đăng nhập cục bộ vào các <b>Domain Controller</b> nhưng không có quyền quản trị các chính sách bảo mật.
p ORS	viên của nhóm này có quyền lưu trữ dự phòng ( <b>Backup</b> ) và phục hồi ( <b>Retore</b> ) hệ thống tập tin. Trong trường hợp hệ thống tập tin là <b>NTFS</b> và họ không được gán quyền trên hệ thống tập tin thì thành viên của nhóm này chỉ có thể truy cập hệ thống tập tin thông qua công cụ <b>Backup</b> . Nếu muốn truy cập trực tiếp thì họ phải được gán quyền.
	om bị hạn chế quyền truy cập các tài nguyên trên mạng. Các thành viên nhóm này là người dùng vắng lai không phải là thành viên của mạng.  ình các tài khoản <b>Guest</b> bị khóa
Operator	viên của nhóm này có quyền tạo ra, quản lý và xóa bỏ các đối tượng máy in dùng chung trong Active Directory.
Operators	viên của nhóm này có thể quản trị các máy server trong miền như: cài đặt, quản lý máy in, tạo và quản lý thư mục dùng chung, backup dữ liệu, định dạng đĩa, thay đổi giờ...
	ình mọi người dùng được tạo đều thuộc nhóm này, nhóm này có quyền tối thiểu của một người dùng nên việc truy cập rất hạn chế.

### Chương 3: Thiết lập và quản trị hệ thống mạng

nhóm	Mô tả
ator	này được dùng để hỗ trợ việc sao chép danh bạ trong <b>Directory Services</b> , nhóm này không có thành viên mặc định.
ing Forest Trust Builders	viên nhóm này có thể tạo ra các quan hệ tin cậy hướng đến, một chiều vào các rừng. Nhóm này không có thành viên mặc định.
rk guration ors	viên nhóm này có quyền sửa đổi các thông số <b>P</b> trên các máy <b>Domain Controller</b> trong miền.
indows 2000 atable Access	này có quyền truy cập đến tất cả các tài khoản người dùng và tài khoản nhóm trong miền, nhằm hỗ trợ cho các hệ thống <b>WinNT</b> cũ.
e Desktop User	viên nhóm này có thể đăng nhập từ xa vào các <b>Domain Controller</b> trong miền, nhóm này không có thành viên mặc định.
mace Log Users	viên nhóm này có quyền truy cập từ xa để ghi nhận lại những giá trị về hiệu năng của các máy <b>Domain Controller</b> , nhóm này cũng không có thành viên mặc định.
mace Monitor Users	viên nhóm này có khả năng giám sát từ xa các máy <b>in Controller</b> .

## Chương 3: Thiết lập và quản trị hệ thống mạng

### 3.2.6 Tài khoản nhóm Global tạo sẵn

Tên nhóm	Mô tả
Domain Admins	Thành viên của nhóm này có thể toàn quyền quản trị các máy tính trong miền vì mặc định khi gia nhập vào miền các <b>member server</b> và các máy trạm ( <b>Win2K Pro, WinXP</b> ) đã đưa nhóm <b>Domain Admins</b> là thành viên của nhóm cục bộ <b>Administrators</b> trên các máy này.
Domain Users	Theo mặc định mọi tài khoản người dùng trên miền đều là thành viên của nhóm này. Mặc định nhóm này là thành viên của nhóm cục bộ <b>Users</b> trên các máy <b>server</b> thành viên và máy trạm.
Group Policy Creator Owners	Thành viên nhóm này có quyền sửa đổi chính sách nhóm của miền, theo mặc định tài khoản <b>administrator</b> miền là thành viên của nhóm này.
Enterprise Admins	Đây là một nhóm <b>universal</b> , thành viên của nhóm này có toàn quyền trên tất cả các miền trong rừng đang xét. Nhóm này chỉ xuất hiện trong miền gốc của rừng thôi. Mặc định nhóm này là thành viên của nhóm <b>administrators</b> trên các <b>Domain Controller</b> trong rừng.
Schema Admins	Nhóm <b>universal</b> này cũng chỉ xuất hiện trong miền gốc của rừng, thành viên của nhóm này có thể chỉnh sửa cấu trúc tổ chức ( <b>schema</b> ) của <b>Active Directory</b> .

### 3.2.7 Các nhóm tạo sẵn đặc biệt

Ngoài các nhóm tạo sẵn đã trình bày ở trên, hệ thống Windows Server 2008 còn có một số nhóm tạo sẵn đặc biệt, chúng không xuất hiện trên cửa sổ của công cụ Active Directory User and Computer, mà chúng chỉ xuất hiện trên các ACL của các tài nguyên và đối tượng. Ý nghĩa của nhóm đặc biệt này là:

- Interactive: đại diện cho những người dùng đang sử dụng máy tại chỗ.

## Chương 3: Thiết lập và quản trị hệ thống mạng

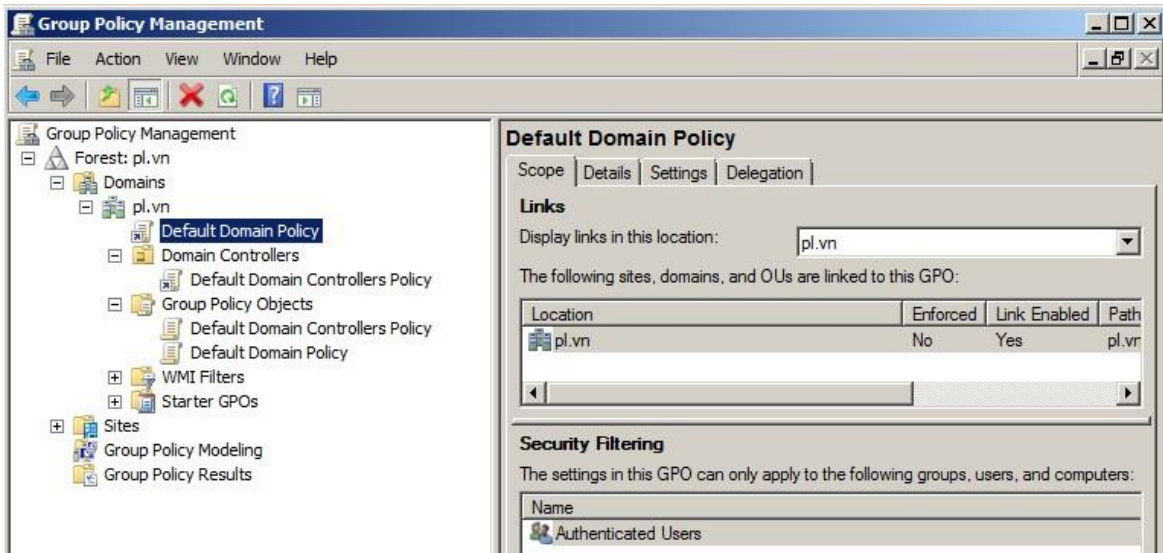
- Network: đại diện cho tất cả những người dùng đang nối kết mạng đến một máy tính khác.
- Everyone: đại diện cho tất cả mọi người dùng.
- System: đại diện cho hệ điều hành.
- Creator owner: đại diện cho những người tạo ra, những người sở hữu một tài nguyên nào đó như: thư mục, tập tin, tác vụ in ấn (print job)...
- Authenticated users: đại diện cho những người dùng đã được hệ thống xác thực, nhóm này được dùng như một giải pháp thay thế an toàn hơn cho nhóm everyone.
- Anonymous logon: đại diện cho một người dùng đã đăng nhập vào hệ thống một cách nặc danh, chẳng hạn một người sử dụng dịch vụ FTP.
- Service: đại diện cho một tài khoản mà đã đăng nhập với tư cách như một dịch vụ.
- Dialup: đại diện cho những người đang truy cập hệ thống thông qua Dial-up Networking.

### 3.2.8 Chính sách tài khoản người dùng

#### 3.2.8.1 Chính sách tài khoản người dùng (System Policy)

Chính sách tài khoản người dùng (Account Policy) được dùng để chỉ định các thông số về tài khoản người dùng mà nó được sử dụng khi tiến trình logon xảy ra. Nó cho phép bạn cấu hình các thông số bảo mật máy tính cho mật khẩu, khóa tài khoản và chứng thực Kerberos trong vùng. Nếu trên Server thành viên thì bạn sẽ thấy hai mục Password Policy và Account Lockout Policy, trên máy Windows Server 2008 làm domain controller thì bạn sẽ thấy ba thư mục Password Policy, Account Lockout Policy và Kerberos Policy. Trong Windows Server 2008 cho phép bạn quản lý chính sách tài khoản tại hai cấp độ là: cục bộ và miền. Muốn cấu hình các chính sách tài khoản người dùng ta vào Start \ Programs \ Administrative Tools \ Group policy Management.

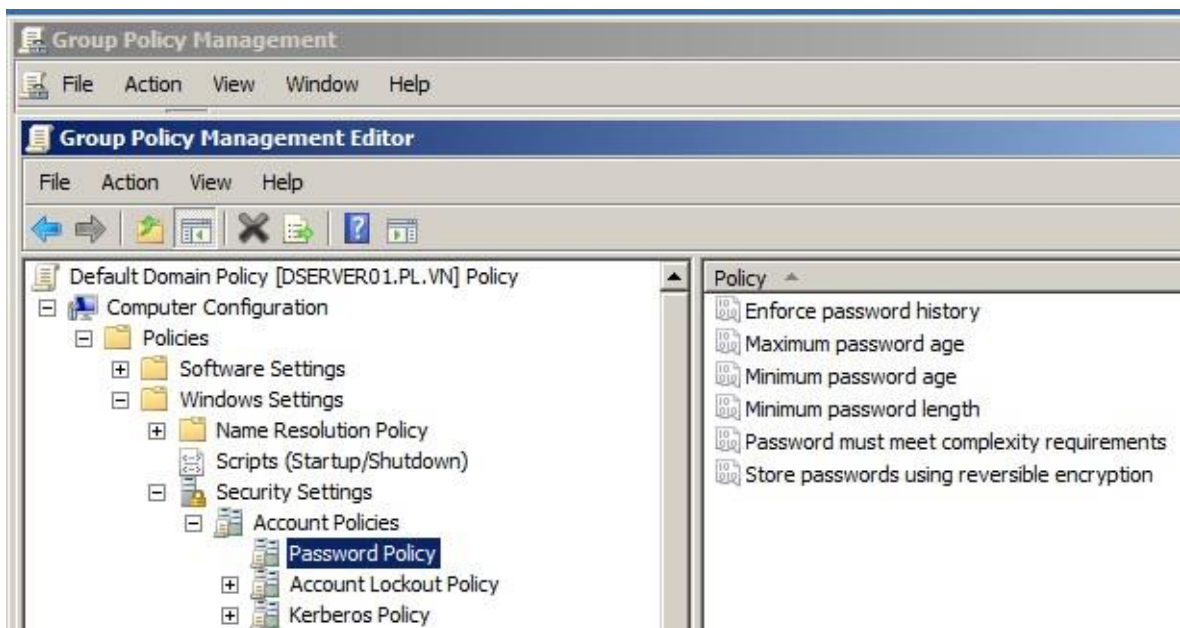
## Chương 3: Thiết lập và quản trị hệ thống mạng



Hình 2-29. Giao diện chính sách tài khoản người dùng

### 3.2.8.2 Chính sách mật khẩu

Chính sách mật khẩu (Password Policies) nhằm đảm bảo an toàn cho mật khẩu của người dùng để tránh các trường hợp đăng nhập bất hợp pháp vào hệ thống. Chính sách này cho phép bạn qui định chiều dài ngắn nhất của mật khẩu, độ phức tạp của mật khẩu...



Hình 2-30. Giao diện chính sách mật khẩu

- Các lựa chọn trong chính sách mật khẩu:



### Chương 3: Thiết lập và quản trị hệ thống mạng

**Bảng 2-3. Bảng lựa chọn trong chính sách mật khẩu**

<b>Chính sách</b>	<b>Mô tả</b>	<b>Mặc định</b>
Force Password Complexity	đặt mật mã không được giống nhau	24
Maximum Password Age	Giới hạn số ngày nhiều nhất mà mật mã người dùng có hiệu lực	42
Minimum Password Age	Số ngày tối thiểu trước khi người dùng có thể thay đổi mật mã.	1
Minimum Password Length	đài ngắn nhất của mật mã	7
Passwords Must Meet Complexity Requirements	Mật khẩu phải có độ phức tạp như: có ký tự hoa, thường, có ký số.	Cho phép
Require Password Using Possible Encryption for All Users in the Domain	Mật mã người dùng được lưu dưới dạng mã hóa	Không cho phép

#### **3.2.9 Chính sách khóa tài khoản (Account Lockout Policy)**

Chính sách khóa tài khoản (Account Lockout Policy) quy định cách thức và thời điểm khóa tài khoản trong vùng hay trong hệ thống cục bộ. Chính sách này giúp hạn chế tấn công thông qua hình thức logon từ xa.

- Các thông số cấu hình chính sách khóa tài khoản:

## Chương 3: Thiết lập và quản trị hệ thống mạng

Bảng 2-4. Bảng lựa chọn trong chính sách khoá mật khẩu

Chính sách	Mô tả	Mặc định
Account Lockout Threshold	Định số lần cố gắng đăng nhập trước khi tài khoản bị khóa	Tài khoản sẽ không bị khóa)
Account Lockout Duration	Định thời gian tài khoản	Nếu <b>Account Lockout Threshold</b> được thiết lập thì giá trị này là 30 phút.
Account Lockout Reset After	Định thời gian đếm lại số lần đăng nhập không thành công	Nếu <b>Account Lockout Threshold</b> được thiết lập thì giá trị này là 30

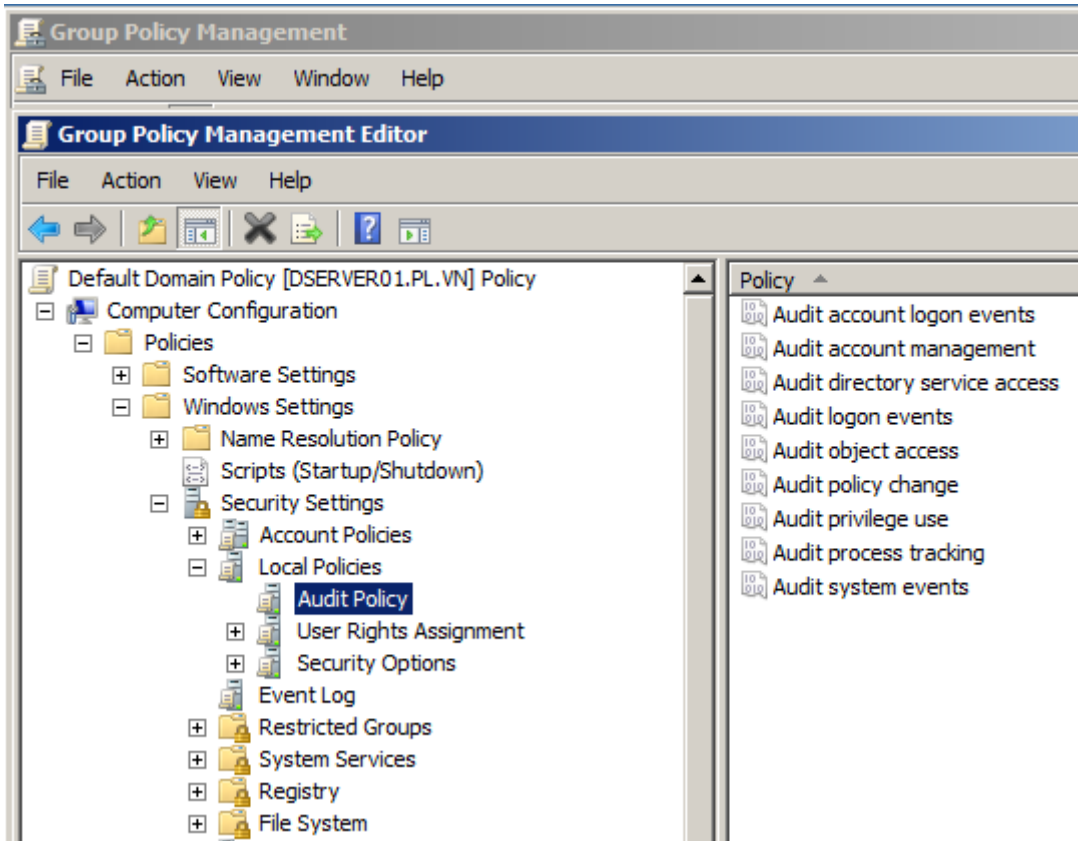
### 3.2.10 Chính sách cục bộ (Local Policies)

Chính sách cục bộ (Local Policies) cho phép bạn thiết lập các chính sách giám sát các đối tượng trên mạng như người dùng và tài nguyên dùng chung. Đồng thời dựa vào công cụ này bạn có thể cấp quyền hệ thống cho các người dùng và thiết lập các lựa chọn bảo mật.

### 3.2.11 Chính sách kiểm toán

Chính sách kiểm toán (Audit Policies) giúp bạn có thể giám sát và ghi nhận các sự kiện xảy ra trong hệ thống, trên các đối tượng cũng như đối với các người dùng. Bạn có thể xem các ghi nhận này thông qua công cụ Event Viewer, trong mục Security.

### Chương 3: Thiết lập và quản trị hệ thống mạng



**Hình 2-31. Giao diện chính sách kiểm toán**

- Các lựa chọn trong chính sách kiểm toán:

**Bảng 2-5. Bảng lựa chọn trong chính sách kiểm toán**

Chính sách	Mô tả
Account Logon Events	toán những sự kiện khi tài khoản đăng nhập, hệ thống sẽ ghi nhận khi người dùng <b>logon</b> , <b>logoff</b> hoặc tạo một kết nối mạng
Account Management	ống sẽ ghi nhận khi tài khoản người dùng hoặc nhóm có sự thay đổi thông tin hay các thao tác quản trị liên quan đến tài khoản người dùng.
Directory Service Access	hân việc truy cập các dịch vụ thư mục

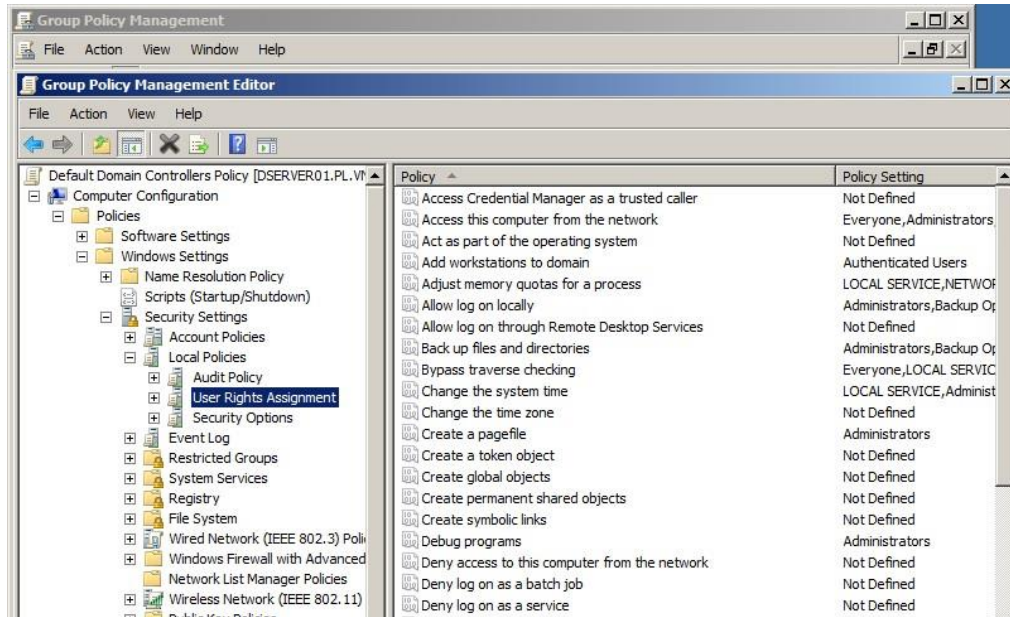
### Chương 3: Thiết lập và quản trị hệ thống mạng

Chính sách	Mô tả
Logon Events	ghi nhận các sự kiện liên quan đến quá trình logon như thi hành một <b>logon script</b> hoặc truy cập đến một <b>roaming profile</b> .
Object Access	ghi nhận việc truy cập các tập tin, thư mục, và máy in.
Policy Change	ghi nhận các thay đổi trong chính sách kiểm toán.
privilege use	Windows sẽ ghi nhận lại khi bạn thao tác quản trị trên các quyền hệ thống như cấp hoặc xóa quyền của một ai đó.
process tracking	Chính sách kiểm toán này theo dõi hoạt động của chương trình chạy hệ điều hành.
system event	Windows sẽ ghi nhận mỗi khi bạn khởi động lại máy hoặc tắt máy.

#### 3.2.12 Quyền hệ thống của người dùng

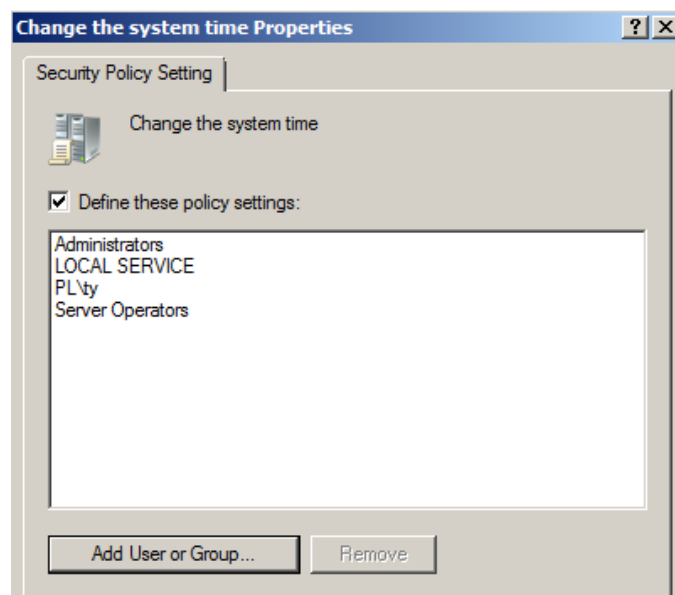
Đối với hệ thống Windows Server 2008, bạn có hai cách cấp quyền hệ thống cho người dùng là: gia nhập tài khoản người dùng vào các nhóm tạo sẵn (built-in) để kế thừa quyền hoặc bạn dùng công cụ User Rights Assignment để gán từng quyền rời rạc cho người dùng. Cách thứ nhất bạn đã biết sử dụng ở chương trước, chỉ cần nhớ các quyền hạn của từng nhóm tạo sẵn thì bạn có thể gán quyền cho người dùng theo yêu cầu. Để cấp quyền hệ thống cho người dùng theo cách thứ hai thì bạn phải dùng công cụ Local Security Policy (nếu máy bạn không phải Domain Controller) hoặc Domain Controller Security Policy (nếu máy bạn là Domain Controller). Trong hai công cụ đó bạn mở mục Local Policy \ User Rights Assignment.

### Chương 3: Thiết lập và quản trị hệ thống mạng



Hình 2-32. Giao diện truy cập quyền hệ thống của người dùng

Để thêm, bớt một quyền hạn cho người dùng hoặc nhóm, bạn nhấp đôi chuột vào quyền hạn được chọn, nó sẽ xuất hiện một hộp thoại chứa danh sách người dùng và nhóm hiện tại đang có quyền này. Bạn có thể nhấp chuột vào nút Add để thêm người dùng, nhóm vào danh sách hoặc nhấp chuột vào nút Remove để xóa người dùng khỏi danh sách. Ví dụ minh họa sau là bạn cấp quyền thay đổi giờ hệ thống (change the system time) cho người dùng “ty”



Hình 2-33. Cấp quyền cho User thay đổi giờ hệ thống

### **Chương 3: Thiết lập và quản trị hệ thống mạng**

- Danh sách các quyền hệ thống cấp cho người dùng và nhóm:

### Chương 3: Thiết lập và quản trị hệ thống mạng

**Bảng 2-6. Danh sách các quyền hệ thống cấp cho người dùng và nhóm**

Quyền	Mô tả
Is This Computer from the Network	phép người dùng truy cập máy tính thông qua mạng. Mặc định mọi người đều có quyền này.
Part of the Operating System	phép các dịch vụ chứng thực ở mức thấp chứng thực với bất kỳ người dùng nào.
Workstations to the in	phép người dùng thêm một tài khoản nh vào vùng.
Up Files and Directories	phép người dùng sao lưu dự phòng (backup) các tập tin và thư mục bất chấp các tập tin và thư mục này người đó có quyền không.
Is Traverse Checking	phép người dùng duyệt qua cấu trúc thư mục nếu người dùng không có quyền xem (list) nội dung thư mục này.
Change the System Time	phép người dùng thay đổi giờ hệ thống của máy tính.
Change a Pagefile	phép người dùng thay đổi kích thước của Page File.
Change a Token Object	phép một tiến trình tạo một thẻ bài nếu tiến trình này dùng NTCreatToken API.

### Chương 3: Thiết lập và quản trị hệ thống mạng

Quyền	Mô tả
Permanent Shared Objects	hép một tiến trình tạo một đối tượng thư mục thông qua Windows 2000 Object Manager.
Programs	hép người dùng gắn một chương trình debug vào bất kỳ tiến trình nào.
Access to This Computer from the Network	hép bạn khóa người dùng hoặc nhóm không được truy cập đến các máy tính trên mạng.
Logon as a Batch File	hép bạn ngăn cản những người dùng và nhóm được phép logon như một batch file.
Logon as a Service	hép bạn ngăn cản những người dùng và nhóm được phép logon như một services.
Logon Locally	hép bạn ngăn cản những người dùng và nhóm truy cập đến máy tính cục bộ.
Computer and User Accounts to be Trusted by Delegation	hép người dùng hoặc nhóm được ủy quyền cho người dùng hoặc một đối tượng máy tính.
Shutdown from a Remote System	hép người dùng shut down hệ thống từ xa thông qua mạng



### Chương 3: Thiết lập và quản trị hệ thống mạng

Quyền	Mô tả
Rate Security Audits	hép người dùng, nhóm hoặc một tiến trình tạo một entry vào Security log.
File Quotas	hép người dùng điều khiển các hạn ngạch của các tiến trình.
Process Scheduling Priority	hép người dùng định một tiến trình có thể tăng hoặc giảm độ ưu tiên đã được gán cho tiến trình khác.
Load and Unload Device Drivers	hép người dùng có thể cài đặt hoặc gỡ bỏ các driver của các thiết bị.
Pages in Memory	hép người dùng trang trong vùng nhớ.
Run as a Batch Job	hép một tiến trình logon vào hệ thống và thi hành một tập tin chứa các lệnh hệ thống.
Run as a Service	hép một dịch vụ logon và thi hành một dịch vụ riêng.
Run Locally	hép người dùng logon tại máy tính Server.
System Audit and Security Log	hép người dùng quản lý Security log.

### Chương 3: Thiết lập và quản trị hệ thống mạng

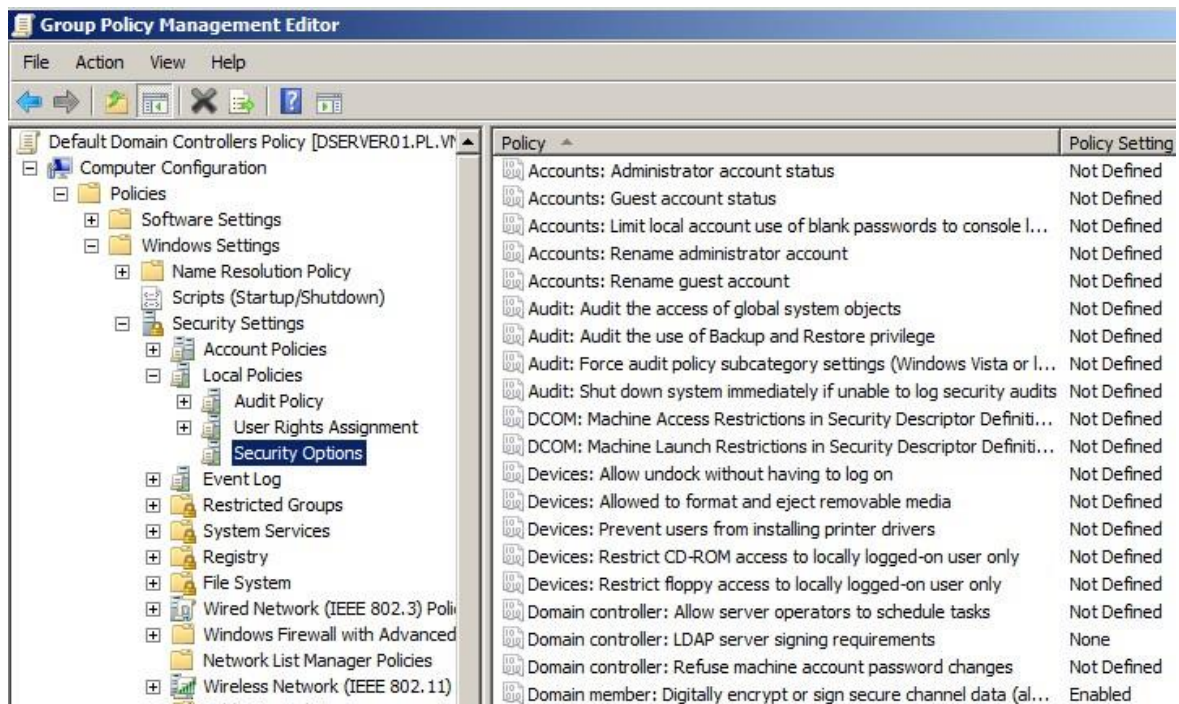
Quyền	Mô tả
<p>Control Firmware Environment</p>	<p>Cho phép người dùng hoặc một tiến trình hiệu chỉnh các biến môi trường hệ thống.</p>
<p>Control Single Process</p>	<p>Cho phép người dùng giám sát các tiến trình bình thường thông qua công cụ Performance Logs and Alerts.</p>
<p>Control System Performance</p>	<p>Cho phép người dùng giám sát các tiến trình hệ thống thông qua công cụ Performance Logs and Alerts.</p>
<p>Control Computer from Remote</p>	<p>Cho phép người dùng gỡ bỏ một Laptop thông qua giao diện người dùng của Windows 2000.</p>
<p>Control a Process Level Token</p>	<p>Cho phép một tiến trình thay thế một token mặc định mà được tạo bởi một tiến trình con.</p>
<p>Control Files and Directories</p>	<p>Cho phép người dùng phục hồi tập tin và thư mục, bất chấp người dùng này có quyền trên tập tin và thư mục này hay không.</p>
<p>Control Shutdown the System</p>	<p>Cho phép người dùng shut down cục bộ Windows 2000.</p>

### Chương 3: Thiết lập và quản trị hệ thống mạng

Quyền	Mô tả
ronize Directory Service Data	hép người dùng đồng bộ dữ liệu với một dịch vụ thư mục.
Ownership of Files or Other ts	gười dùng tước quyền sở hữu của một đối tượng hệ thống.

#### 3.2.13 Các lựa chọn bảo mật

Các lựa chọn bảo mật (Security Options) cho phép người quản trị Server khai báo thêm các thông số nhằm tăng tính bảo mật cho hệ thống như: không cho phép hiển thị người dùng đã logon trước đó hay đổi tên tài khoản người dùng tạo sẵn (Administrator, Guest). Trong hệ thống Windows Server 2008 hỗ trợ cho chúng ta rất nhiều lựa chọn bảo mật, nhưng trong giáo trình này chúng ta chỉ khảo sát các lựa chọn thông dụng.



**Chương 3: Thiết lập và quản trị hệ thống mạng**  
**Hình 2-34. Giao diện chính sách bảo mật**

### Chương 3: Thiết lập và quản trị hệ thống mạng

- Một số lựa chọn bảo mật thông dụng:

**Bảng 2-7. Bảng lựa chọn bảo mật thông dụng**

Tên lựa chọn	Mô tả
Shutdown: allow system to be shutdown without having to logon	Cho phép người dùng <b>shutdown</b> hệ thống mà không cần logon.
System: audit the access of global system objects	Giám sát việc truy cập các đối tượng hệ thống toàn cục.
Work security: force logoff when logon hours expires.	Thực hiện <b>logoff</b> khỏi hệ thống khi người dùng hết thời gian sử dụng hoặc tài khoản hết hạn.
Interactive logon: do not require CTRL+ALT+DEL	Không yêu cầu ấn ba phím <b>CTRL+ALT+DEL</b> để logon.
Interactive logon: do not display last user name	Không hiển thị tên người dùng đã logon trên màn hình loại <b>Logon</b> .
Administrators: rename administrator account	Cho phép đổi tên tài khoản <b>Administrator</b> thành tên mới.
Administrators: rename guest account	Cho phép đổi tên tài khoản <b>Guest</b> thành tên mới.

#### 3.2.14 Chính sách tài khoản người dùng nhóm (Group Policy)

##### 3.2.14.1 Giới thiệu chức năng của Group Policy

Triển khai phần mềm ứng dụng: bạn có thể gom tất cả các tập tin cần thiết để cài đặt một phần mềm nào đó vào trong một gói (package), đặt nó lên

### Chương 3: Thiết lập và quản trị hệ thống mạng

Server, rồi dùng chính sách nhóm hướng một hoặc nhiều máy trạm đến gói phần mềm đó. Hệ thống sẽ tự động cài đặt phần mềm này đến tất cả các máy trạm mà không cần sự can thiệp nào của người dùng.

Gán các quyền hệ thống cho người dùng: chức năng này tương tự với chức năng của chính sách hệ thống. Nó có thể cấp cho một hoặc một nhóm người nào đó có quyền tắt máy server, đổi giờ hệ thống hay backup dữ liệu...

Giới hạn những ứng dụng mà người dùng được phép thi hành: chúng ta có thể kiểm soát máy trạm của một người dùng nào đó và cho phép người dùng này chỉ chạy được một vài ứng dụng nào đó thôi như: Outlook Express, Word hay Internet Explorer.

Kiểm soát các thiết lập hệ thống: bạn có thể dùng chính sách nhóm để qui định hạn ngạch đĩa cho một người dùng nào đó. Người dùng này chỉ được phép lưu trữ tối đa bao nhiêu MB trên đĩa cứng theo qui định.

Thiết lập các kịch bản đăng nhập, đăng xuất, khởi động và tắt máy: trong hệ thống NT4 thì chỉ hỗ trợ kịch bản đăng nhập (logon script), nhưng Windows 2000 và Windows Server 2008 thì hỗ trợ cả bốn sự kiện này được kích hoạt (trigger) một kịch bản (script). Bạn có thể dùng các GPO để kiểm soát những kịch bản nào đang chạy.

Đơn giản hóa và hạn chế các chương trình: bạn có thể dùng GPO để gỡ bỏ nhiều tính năng khỏi Internet Explorer, Windows Explorer và những chương trình khác.

Hạn chế tổng quát màn hình Desktop của người dùng: bạn có thể gỡ bỏ hầu hết các đề mục trên menu Start của một người dùng nào đó, ngăn chặn không cho người dùng cài thêm máy in, sửa đổi thông số cấu hình của máy trạm...

#### *3.2.14.2 So sánh giữa System Policy và Group Policy*

Vừa rồi ở chương trước, chúng ta đã tìm hiểu về chính sách hệ thống (System Policy), tiếp theo chúng ta sẽ tìm hiểu về chính sách nhóm (Group Policy). Vậy hai chính sách này khác nhau như thế nào.

Chính sách nhóm chỉ xuất hiện trên miền Active Directory, nó không tồn tại trên miền NT4.

### Chương 3: Thiết lập và quản trị hệ thống mạng

Chính sách nhóm làm được nhiều điều hơn chính sách hệ thống. Tất nhiên chính sách nhóm chứa tất cả các chức năng của chính sách hệ thống và hơn thế nữa, bạn có thể dùng chính sách nhóm để triển khai một phần mềm cho một hoặc nhiều máy một cách tự động.

Chính sách nhóm tự động hủy bỏ tác dụng khi được gỡ bỏ, không giống như các chính sách hệ thống.

Chính sách nhóm được áp dụng thường xuyên hơn chính sách hệ thống. Các chính sách hệ thống chỉ được áp dụng khi máy tính đăng nhập vào mạng thôi. Các chính sách nhóm thì được áp dụng khi bạn bật máy lên, khi đăng nhập vào một cách tự động vào những thời điểm ngẫu nhiên trong suốt ngày làm việc.

Bạn có nhiều mức độ để gán chính sách nhóm này cho người từng nhóm người hoặc từng nhóm đối tượng.

Chính sách nhóm tuy có nhiều ưu điểm nhưng chỉ áp dụng được trên máy Win2K, WinXP và Windows Server 2003, Windows server 2008

#### ***3.2.15 Triển khai một chính sách nhóm trên miền***

Chúng ta cấu hình và triển khai Group Policy bằng cách xây dựng các đối tượng chính sách (GPO). Các GPO là một vật chứa (container) có thể chứa nhiều chính sách áp dụng cho nhiều người, nhiều máy tính hay toàn bộ hệ thống mạng. Bạn dùng chương trình Group Policy Object Editor để tạo ra các đối tượng chính sách. Trong cửa sổ chính của Group Policy Object Editor có hai mục chính: cấu hình máy tính (computer configuration) và cấu hình người dùng (user configuration).

Điều kế tiếp bạn cũng chú ý khi triển khai Group Policy là các cấu hình chính sách của Group Policy được tích lũy và kế thừa từ các vật chứa (container) bên trên của Active Directory. Ví dụ các người dùng và máy tính vừa ở trong miền vừa ở trong OU nên sẽ nhận được các cấu hình từ cả hai chính sách cấp miền lẫn chính sách cấp OU. Các chính sách nhóm sau 90 phút sẽ được làm tươi và áp dụng một lần, nhưng các chính nhóm trên các Domain Controller được làm tươi 5 phút một lần. Các GPO hoạt động được không chỉ nhờ chỉnh sửa các thông tin trong Registry mà còn nhờ các thư viện liên kết động (DLL) làm phần mở rộng đặt tại các máy trạm. Chú ý nếu bạn dùng chính sách nhóm thì chính

## Chương 3: Thiết lập và quản trị hệ thống mạng

sách nhóm tại chỗ trên máy cục bộ sẽ xử lý trước các chính sách dành cho site, miền hoặc OU.

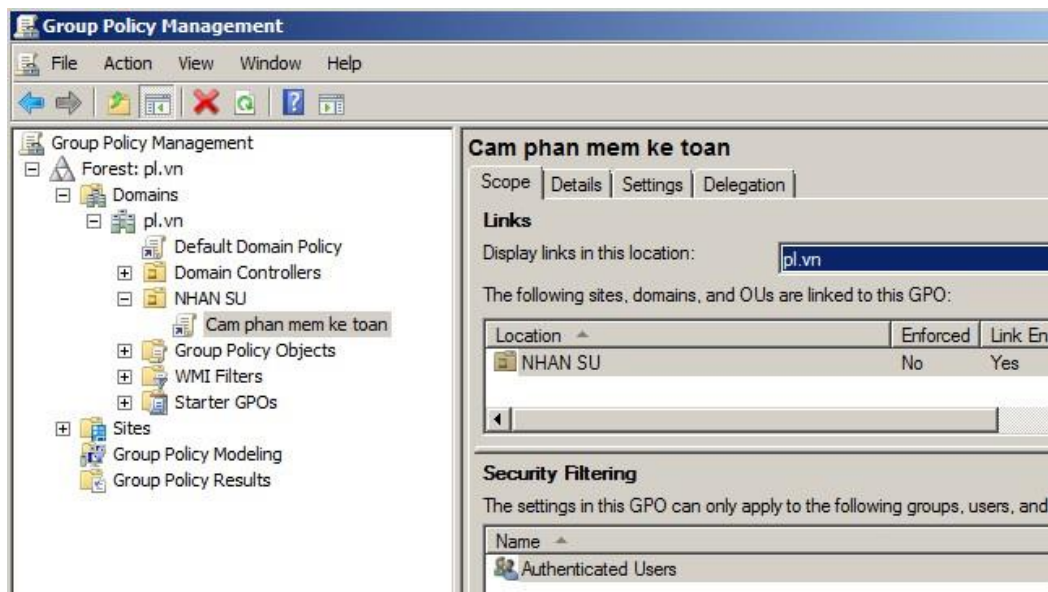
### 3.2.16 Xem chính sách cục bộ của một máy tính ở xa

Để xem một chính sách cục bộ trên các máy tính khác trong miền, bạn phải có quyền quản trị trên máy đó hoặc quản trị miền. Lúc đó bạn có thể dùng lệnh GPEDIT.MSC /gpcomputer: machinename, ví dụ bạn muốn xem chính sách trên máy PC01 bạn gõ lệnh GPEDIT.MSC /gpcomputer: PC01.

Chú ý: không thể dùng cách này để thiết lập các chính sách nhóm ở máy tính ở xa, do tính chất bảo mật Microsoft không cho phép bạn ở xa thiết lập các chính sách nhóm.

### 3.2.17 Tạo các chính sách miền

Chúng ta dùng snap-in Group Policy trong Active Directory User and Computer hoặc gọi trực tiếp tiện ích Group Policy Object Editor từ dòng lệnh trên máy Domain Controller để tạo ra các chính sách nhóm cho miền. Nếu bạn mở Group Policy từ Active Directory User and Computer thì trong khung cửa sổ chính của chương trình bạn nhấp chuột phải vào biểu tượng tên miền (trong ví dụ này là netclass.edu.vn), chọn Properties. Trong hộp thoại xuất hiện bạn chọn Tab Group Policy



Hình 2-35. Giao diện tạo chính sách miền



### Chương 3: Thiết lập và quản trị hệ thống mạng

Nếu chưa tạo ra một chính sách nào thì bạn chỉ nhìn thấy một chính sách tên Default Domain Policy. Cuối hộp thoại có một checkbox tên Block Policy inheritance, chức năng của mục này là ngăn chặn các thiết định của mọi chính sách bất kỳ ở cấp cao hơn lan truyền xuống đến cấp đang xét.

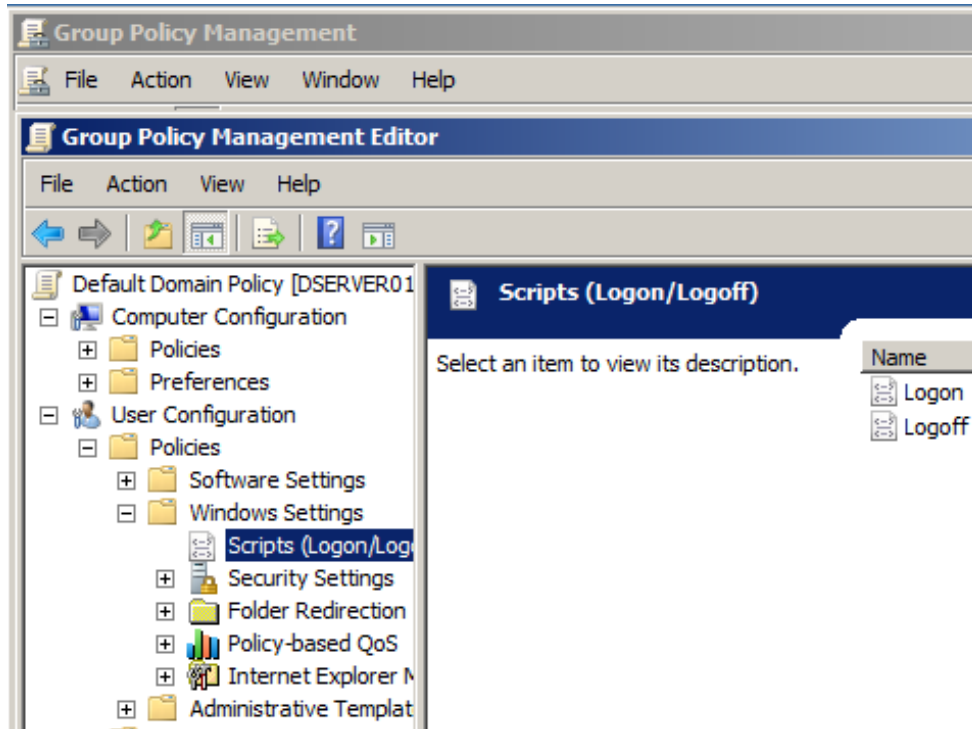
Chú ý rằng chính sách được áp dụng đầu tiên ở cấp site, sau đó đến cấp miền và cuối cùng là cấp OU. Chọn chính sách Default Domain Policy và nhấp chuột vào nút Option để cấu hình các lựa chọn việc áp dụng chính sách. Trong hộp thoại Options, nếu đánh dấu vào mục No Override thì các chính sách khác được áp dụng ở dòng dưới sẽ không phủ quyết được những thiết định của chính sách này, cho dù chính sách đó không đánh dấu vào mục Block Policy inheritance. Tiếp theo nếu đánh dấu vào mục Disabled, thì chính sách này sẽ không hoạt động ở cấp này, Việc disable chính sách ở một cấp không làm disable bản thân đối tượng chính sách.

#### ***3.2.18 Khai báo một logon script dùng chính sách nhóm***

Trong Windows Server 2008 hỗ trợ cho chúng ta bốn sự kiện để có thể kích hoạt các kịch bản (script) hoạt động là: startup, shutdown, logon, logoff. Trong công cụ Group Policy Object Editor, bạn có thể vào Computer Configuration \ Windows Settings \ Scripts để khai báo các kịch bản sẽ hoạt động khi startup, shutdown. Đồng thời để khai báo các kịch bản sẽ hoạt động khi logon, logoff thì bạn vào User Configuration \ Windows Settings \ Scripts. Trong ví dụ này chúng ta tạo một logon script, quá trình gồm các bước sau:

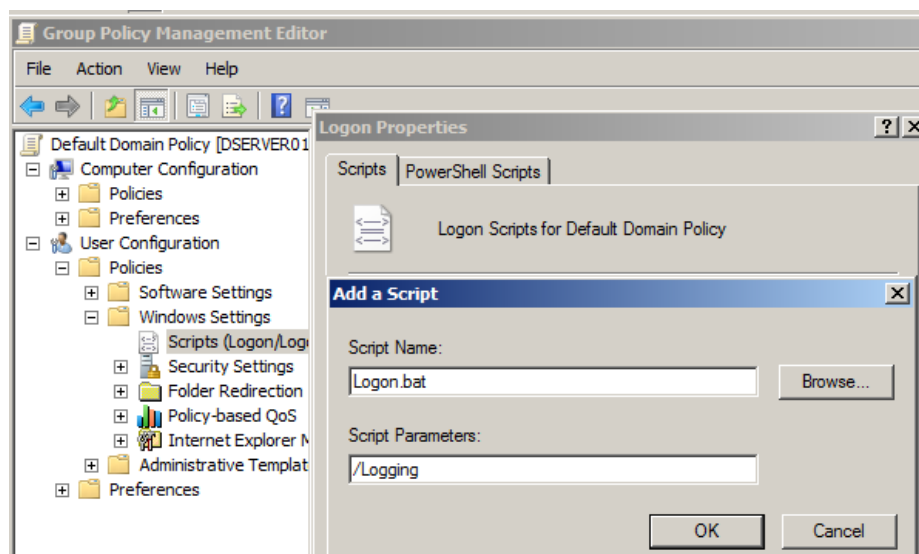
Mở công cụ Group Policy Object Editor, vào mục User Configuration \ Windows Settings \ Scripts.

### Chương 3: Thiết lập và quản trị hệ thống mạng



**Hình 2-36. Giao diện khai báo logon script dùng chính sách nhóm**

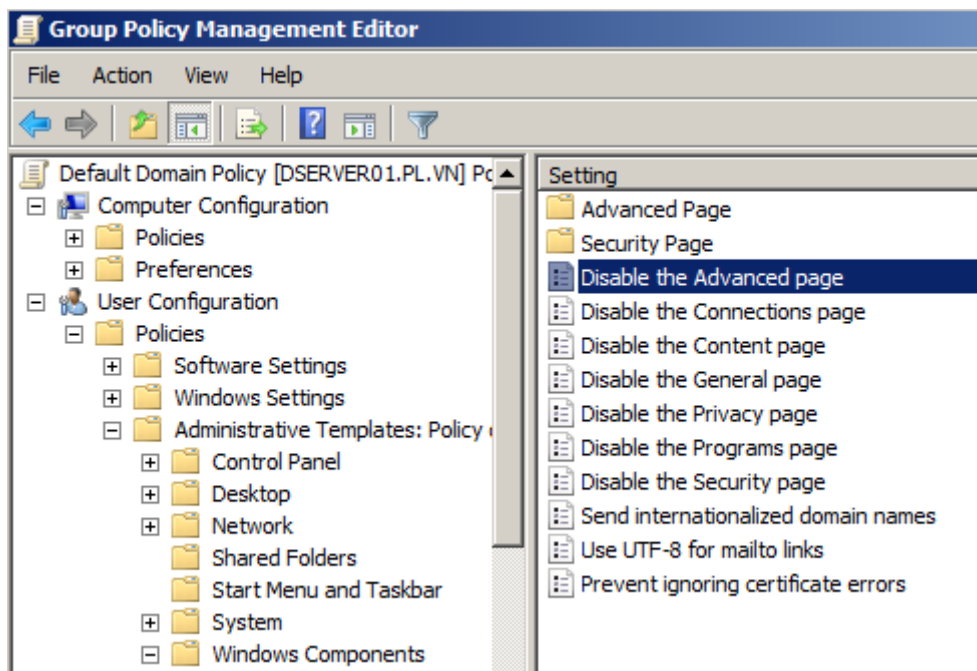
Nhấp đúp chuột vào mục Logon bên cửa sổ bên phải, hộp thoại xuất hiện, bạn nhấp chuột tiếp vào nút Add để khai báo tên tập tin kịch bản cần thi hành khi đăng nhập. Chú ý tập tin kịch bản này phải được chứa trong thư mục `c:\Windows\system32\grouppolicy\user\script\logon`. Thư mục này có thể thay đổi, tốt nhất bạn nên nhấp chuột vào nút Show Files phía dưới hộp thoại để xem thư mục cụ thể chứa các tập tin kịch bản này.



**Chương 3: Thiết lập và quản trị hệ thống mạng**  
**Hình 2-37. Hộp thoại tạo kịch bản logon script**

### 3.2.19 Hạn chế chức năng của Internet Explorer

Trong ví dụ này chúng ta muốn các người dùng dưới máy trạm không được phép thay đổi bất kỳ thông số nào trong Tab Security, Connection và Advanced trong hộp thoại Internet Options của công cụ Internet Explorer. Để làm việc này, trong công cụ Group Policy Object Editor, bạn vào User Configuration\Administrative Templates Windows Components\Internet Explorer\Internet Control Panel, chương trình sẽ hiện ra các mục chức năng của IE có thể giới hạn.

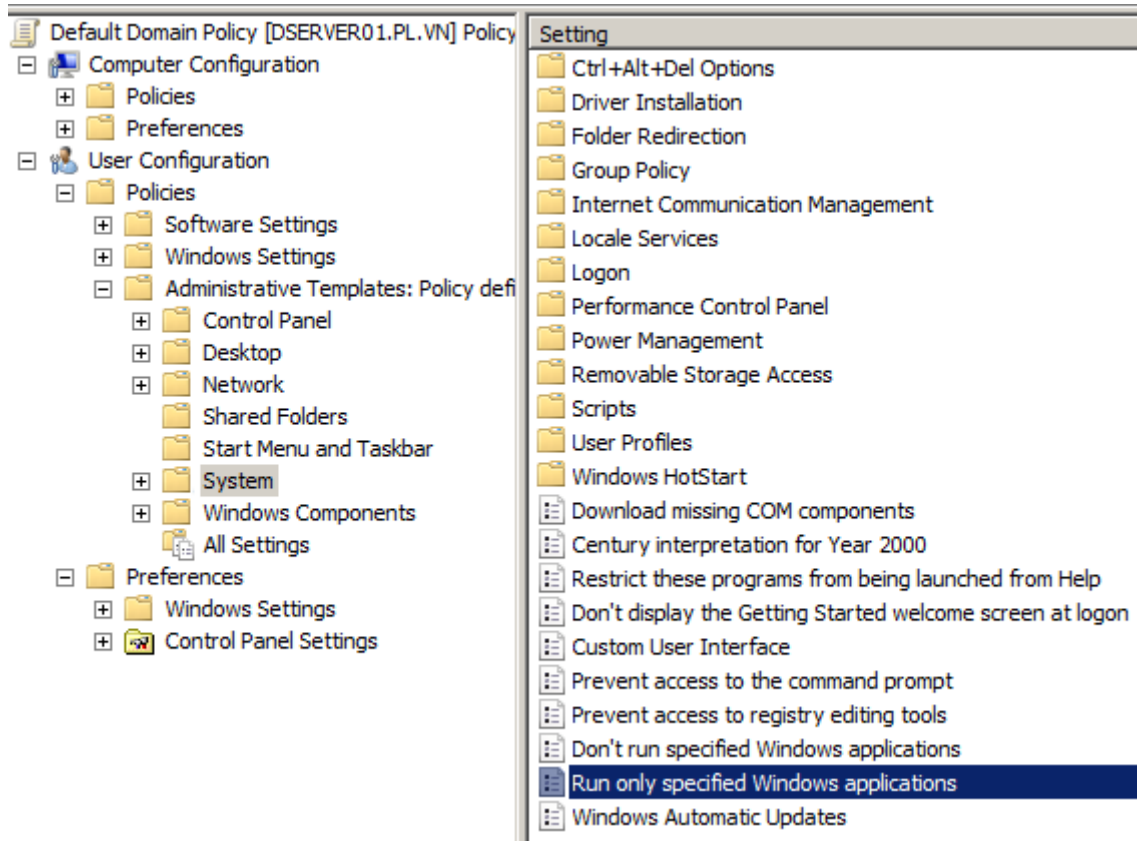


Hình 2-38. Hộp thoại hạn chế chức năng Explorer

### 3.2.20 Chỉ cho phép một số ứng dụng được thi hành

Để cấu hình Group Policy chỉ cho phép các người dùng dưới máy trạm chỉ sử dụng được một vài ứng dụng nào đó, trong công cụ Group Policy Object Editor, bạn vào User Configuration \ Administrative Templates. Sau đó nhấp đúp chuột vào mục Run only allowed Windows applications để chỉ định các phần mềm được phép thi hành.

## Chương 3: Thiết lập và quản trị hệ thống mạng



Hình 2-39. Giao diện cho phép một số ứng dụng được thi hành

### 3.2.21 Cài đặt phần mềm ứng dụng (Deploy software)

Dùng Software Installation extension, bạn có thể quản lý tập trung việc cài đặt phần mềm trên một máy tính client bằng cách ‘assigning application’ (chỉ định ứng dụng) đến user hoặc máy tính; hoặc bằng cách ‘publishing application’ (phổ biến ứng dụng) cho user. Bạn chỉ định phần mềm có tính chất bắt buộc hoặc cần thiết đến user và computer. Và bạn phổ biến phần mềm mà có thể có ích cho công việc của user. Phần mềm đã chỉ định và phổ biến được lưu trong một software distribution point (SDP), một nơi trên mạng mà user có thể lấy được phần mềm mà họ cần.

#### - Assigning Applications

Khi bạn chỉ định một ứng dụng đến một user, ứng dụng được thông báo đến user trên menu Start vào lần tới khi anh ta hoặc cô ta đăng nhập trên một trạm làm việc, và những thiết lập registry cục bộ, bao gồm cả filename extension đã được cập nhật. Việc thông báo ứng dụng đi theo user bất chấp anh ta hoặc cô ta đăng nhập trên máy tính nào. Ứng dụng này được cài đặt lần đầu

### Chương 3: Thiết lập và quản trị hệ thống mạng

tiên khi user kích hoạt ứng dụng trên máy tính, bằng một trong những cách: chọn ứng dụng trên menu Start, mở một tài liệu đã được liên kết với ứng dụng.

- Publishing Applications

Khi bạn phổ biến một ứng dụng đến user, ứng dụng không hiện ra như là đã được cài đặt trên máy tính của user. Không có shortcut trên desktop hoặc menu Start, và không có những sự cập nhật được tạo ra trong registry cục bộ trên máy tính của user. Thay vào đó, những ứng dụng đã được phổ biến lưu những thuộc tính về sự thông báo của chúng trong Active Directory. Những thông tin như tên của ứng dụng và những file liên quan được phô ra cho user trong Active Directory container. Ứng dụng sẵn sàng cho user cài đặt bằng cách dùng Add Or Remove Programs trong Control Panel hoặc bằng cách click một file đã được liên kết với ứng dụng (như file .xls được liên kết với Microsoft Excel).

- Dịch vụ Windows Installer

Software Installation extension dùng dịch vụ Windows Installer để bảo trì phần mềm một cách có hệ thống. Dịch vụ Windows Installer chạy nền (background) và cho phép hệ điều hành quản lý tiến trình cài đặt phù hợp với thông tin trong gói (package) Windows Installer. Gói Windows Installer là một file chứa thông tin mô tả tình trạng cài đặt của ứng dụng.

Bởi vì dịch vụ Windows Installer quản lý tình trạng cài đặt, nên nó luôn biết tình trạng của phần mềm. Nếu có vấn đề trong lúc cài đặt, Windows Installer có thể trả máy tính về được biết là tốt nhất trước đó. Nếu bạn cần chỉnh sửa các chức năng sao khi cài đặt, Windows Installer cho phép bạn làm điều đó. Bởi vì Software Installation extension dùng Windows Installer, user được lợi trong việc ứng dụng tự sửa chữa chính nó. Windows Installer lưu ý khi một file chương trình thiếu sót và ngay lập tức cài đặt lại những file thiếu hoặc bị hư hại, bằng cách sửa chữa ứng dụng. Cuối cùng, Windows Installer cho phép bạn gỡ bỏ phần mềm khi bạn không cần nữa.

Dịch vụ Windows Installer, chính nó cũng bị ảnh hưởng bởi những thiết lập trong Group Policy. Bạn có thể tìm thấy những thiết lập này trong nút Windows Installer, nút này bên trong nút Windows Components >

### Chương 3: Thiết lập và quản trị hệ thống mạng

Administrative Templates, cả trong Computer Configuration và User Configuration. Gói Windows Installer

Một Windows Installer package (gói) là một file chứa những chỉ dẫn rõ ràng quá trình cài đặt và gỡ bỏ những ứng dụng riêng biệt. Bạn có thể triển khai phần mềm dùng Software Installation extension bằng cách dùng một Windows Installer package. Có 2 loại Windows Installer package:

Native Windows Installer package (.msi): Những file này đã được phát triển như một phần của ứng dụng và tận hưởng đầy đủ sự thuận tiện của dịch vụ Windows Installer. Tác giả hoặc nhà phân phối của phần mềm có khả năng cung cấp một Windows Installer package dạng “bẩm sinh”.

Repackaged application (.msi): Những file này thường là những ứng dụng được đóng gói lại, vì chúng không có một Windows Installer package dạng “bẩm sinh”. Tuy đã được đóng gói lại thành Native Windows Installer package và làm việc như một Native Windows Installer package, nhưng một repackaged Windows Installer package chứa một sản phẩm đơn với tất cả thành phần và ứng dụng liên quan tới sản phẩm được cài đặt như một chức năng duy nhất. Còn một Native Windows Installer package chứa một sản phẩm đơn với nhiều chức năng có thể được cài đặt riêng lẻ từng chức năng một như những chức năng riêng biệt.

#### - Application (.zap) File

Bạn cũng có thể triển khai phần mềm dùng Software Installation extension bằng cách sử dụng một application file. Application file là một file text chứa các chỉ dẫn về cách phổ biến một ứng dụng, lấy từ một chương trình cài đặt đã tồn tại (Setup.exe hoặc Install.exe). Application file dùng mở rộng

.zap. Hãy dùng file .zap khi bạn không thể phát triển một Windows Installation package “bẩm sinh” hoặc repackaged ứng dụng để tạo ra một repackaged Windows Installation package. Một file .zap không hỗ trợ các chức năng của Windows Installer. Khi bạn triển khai một ứng dụng bằng cách dùng file .zap, ứng dụng được cài đặt bằng chính chương trình Setup.exe hoặc Install.exe nguyên bản của nó. Phần mềm này chỉ có thể được phổ biến và user chỉ có thể chọn nó bằng cách dùng Add Or Remove Programs trong Control Panel. Vì thế

### Chương 3: Thiết lập và quản trị hệ thống mạng

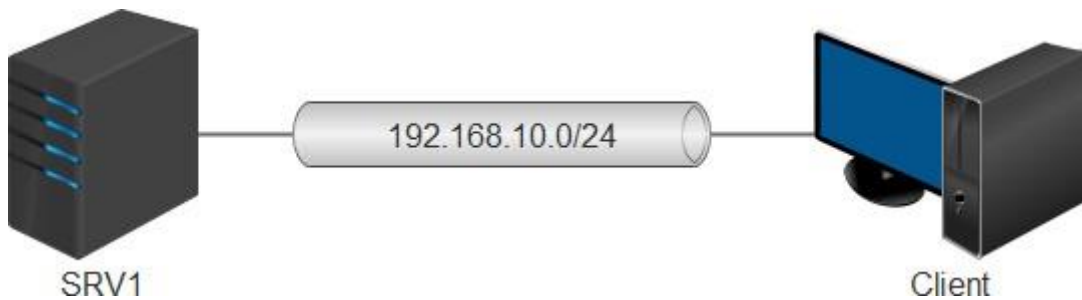
bạn hãy dùng file .msi để triển khai phần mềm với Group Policy bất cứ khi nào có thể.

- Add Or Remove Programs trong Control Panel

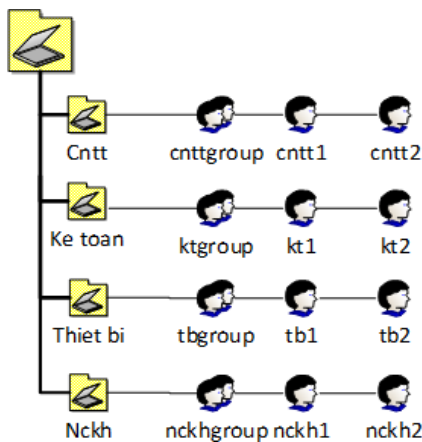
Add Or Remove Programs trong Control Panel cho phép user cài đặt, chỉnh sửa hoặc gỡ bỏ một ứng dụng đã được phổ biến hoặc sửa chữa một ứng dụng bị hư hại. Bạn có thể kiểm soát phần mềm nào user dùng được bên trong Add Or Remove Programs bằng cách dùng các thiết lập của Group Policy. User không cần phải tìm một network share, dùng CD-ROM, hoặc là cài đặt, sửa chữa và nâng cấp phần mềm của chính họ.

#### Câu hỏi và bài tập

Cho mô hình mạng sau:



- ✍ Thiết lập Ip cho hệ thống theo mô hình trên.
- ✍ Xây dựng Domain với tên miền: tnut.edu.vn



- ✍ Tạo User, OU, Group, Add User vào trong Group



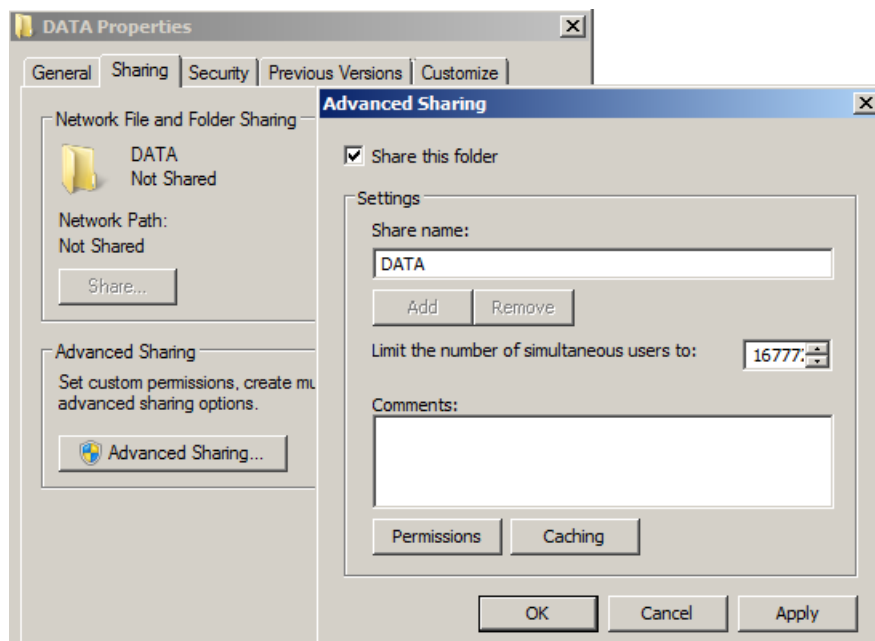
## Chương 3: Thiết lập và quản trị hệ thống mạng

- ✍ Cho máy Client tham gia vào Doomain
- ✍ Máy Client đăng nhập vào các User vừa tạo
- ✍ Cấm nhân viên phòng Ketoansử dụng Keyboard trong Control Panel.
- ✍ Cấu hình chính sách Password Policy, Account lockout policy
  - ✍ Cấm nhân viên phòng Thiet bị sử dụng Mouse, Keyboard trong Control Panel.
  - ✍ Cấu hình cho user phòng Thiet bị được phép đổi password, thử password tb2 trên máy client

### 3.3 Quản lý các thư mục dung chung

#### 3.3.1 Chia sẻ dữ liệu (Share Permission)

Các tài nguyên chia sẻ là các tài nguyên trên mạng mà các người dùng có thể truy xuất và sử dụng thông qua mạng. Muốn chia sẻ một thư mục dùng chung trên mạng, bạn phải logon vào hệ thống với vai trò người quản trị (Administrators) hoặc là thành viên của nhóm Server Operators, tiếp theo trong Explorer bạn nhấp phải chuột trên thư mục đó và chọn Properties, hộp thoại Properties xuất hiện, chọn Tab Sharing.



Hình 2-40. Hộp thoại Share Permissions

### Chương 3: Thiết lập và quản trị hệ thống mạng

**Bảng 2-8. Ý nghĩa của các mục trong Tab Sharing**

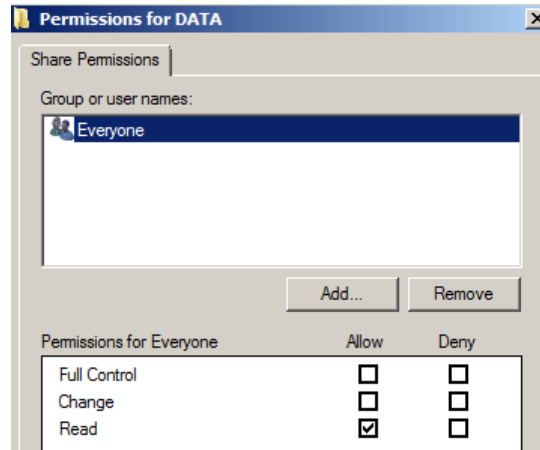
Mục	Mô tả
Not share this folder	Thư mục này chỉ được phép truy cập cục bộ
Share this folder	Thư mục này được phép truy cập cục bộ và truy cập qua mạng
Share name	Tên thư mục mà người dùng mạng nhìn thấy và truy cập
Share description	Cho phép người dùng mô tả thêm thông tin về thư mục dùng chung này
Share limit	Cho phép bạn khai báo số kết nối tối đa truy xuất vào thư mục tại một thời điểm
Share permissions	Cho phép bạn thiết lập danh sách quyền truy cập thông qua mạng của người dùng

#### 3.3.2 Cấu hình Share Permissions

Muốn cấp quyền cho các người dùng truy cập qua mạng thì dùng Share Permissions. Share Permissions chỉ có hiệu lực khi người dùng truy cập qua mạng chứ không có hiệu lực khi người dùng truy cập cục bộ. Khác với NTFS Permissions là quản lý người dùng truy cập dưới cấp độ truy xuất đĩa. Trong hộp thoại Share Permissions, chứa danh sách các quyền sau:

- Full Control: cho phép người dùng có toàn quyền trên thư mục chia sẻ.
- Change: cho phép người dùng thay đổi dữ liệu trên tập tin và xóa tập tin trong thư mục chia sẻ.
- Read: cho phép người dùng xem và thi hành các tập tin trong thư mục chia sẻ.

## Chương 3: Thiết lập và quản trị hệ thống mạng



Hình 2-41. Các quyền Share Permissions

### 3.3.3 Chia sẻ thư mục dùng lệnh *net share*

Chức năng: tạo, xóa và hiển thị các tài nguyên chia sẻ.

Cú pháp:

`net share sharename`

```
netshare sharename=drive:path s:number /unlimited]
```

```
[/remark:"text"]net share sharename rs:number unlimited]
```

`[/remark:"text"] net share {sharename | drive:path} /delete` Ý nghĩa các tham số:

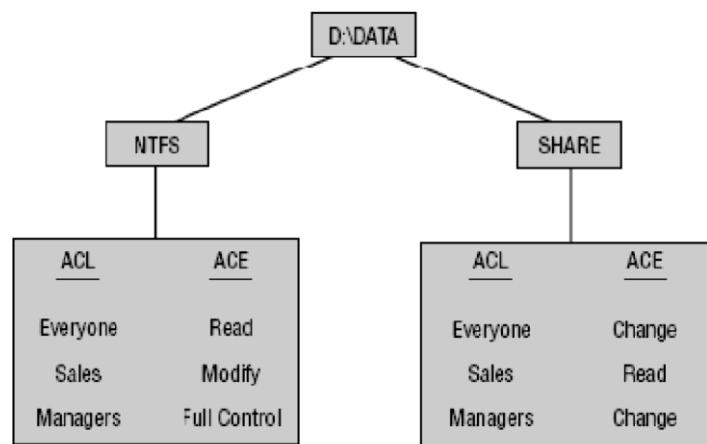
- [Không tham số]: hiển thị thông tin về tất cả các tài nguyên chia sẻ trên máy tính cục bộ
- [Sharename]: tên trên mạng của tài nguyên chia sẻ, nếu dùng lệnh `net share` với một tham số `sharename` thì hệ thống sẽ hiển thị thông tin về tài nguyên dùng chung này.
- [drive:path]: chỉ định đường dẫn tuyệt đối của thư mục cần chia sẻ.
- [/users:number]: đặt số lượng người dùng lớn nhất có thể truy cập vào tài nguyên dùng chung này.
- [/unlimited]: không giới hạn số lượng người dùng có thể truy cập vào tài nguyên dùng chung này.
- [/remark:"text"]: thêm thông tin mô tả về tài nguyên này.

### Chương 3: Thiết lập và quản trị hệ thống mạng

- /delete: xóa thuộc tính chia sẻ của thư mục hiện tại.

#### 3.3.4 Quyền truy cập NTFS

Có hai loại hệ thống tập được dùng cho partition và volume cục bộ là FAT (bao gồm FAT16 và FAT32). FAT partition không hỗ trợ bảo mật nội bộ, còn NTFS partition thì ngược lại có hỗ trợ bảo mật; có nghĩa là nếu đĩa cứng của bạn định dạng là FAT thì mọi người đều có thể thao tác trên các file chứa trên đĩa cứng này, còn ngược lại là định dạng NTFS thì tùy theo người dùng có quyền truy cập không, nếu người dùng không có quyền thì không thể nào truy cập được dữ liệu trên đĩa. Hệ thống Windows Server 2008 dùng các ACL (Access Control List) để quản lý các quyền truy cập của đối tượng cục bộ và các đối tượng trên Active Directory. Một ACL có thể chứa nhiều ACE (Access Control Entry) đại diện cho một người dùng hay một nhóm người.



#### 3.3.5 Các quyền truy cập của NTFS

Bảng 2-9. Quyền truy cập của NTFS

Mục	Mô tả
Traverse Folder/Execute File	Duyệt các thư mục và thi hành các tập tin chương trình trong thư mục
Folder/Read	Liệt kê nội dung của thư mục và đọc dữ liệu của các tập tin trong thư mục
Attributes	Thuộc tính của các tập tin và thư mục

### Chương 3: Thiết lập và quản trị hệ thống mạng

Mục	Mô tả
Read Extended Attributes	Đọc thuộc tính mở rộng của các tập tin và thư mục
File/Write	Đọc tập tin mới và ghi dữ liệu lên các tập tin này
Create Folder/Append Data	Tạo thư mục mới và chèn thêm dữ liệu vào các tập tin
Attributes	Đổi thuộc tính của các tập tin và thư mục
Write Extended Attributes	Đổi thuộc tính mở rộng của các tập tin và thư mục
Delete Subfolders and Files	Xóa thư mục con và các tập tin
Execute	Thực thi các tập tin
Permissions	Quyền truy cập trên các tập tin và thư mục
Change Permissions	Đổi quyền trên các tập tin và thư mục
Ownership	Quyền sở hữu của các tập tin và thư mục

#### 3.3.6 Các mức quyền truy cập được dùng trong NTFS

Bảng 2-10. Bảng phân quyền truy cập được dùng trong NTFS

Full Control	Modify	Read & Execute	List Folder Contents (folders only)		
X	X	X	X		

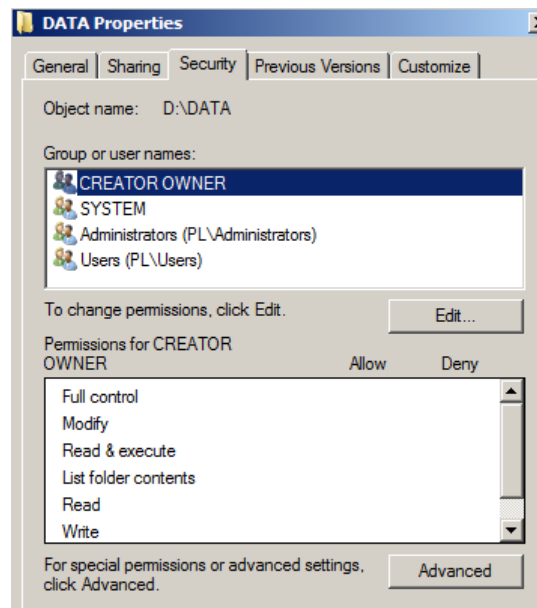
### Chương 3: Thiết lập và quản trị hệ thống mạng

Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Folder/Read	X	X	X	X	
Attributes	X	X	X	X	
Extended Attributes	X	X	X	X	
Files/Write	X				X
Files/Append Data	X				X
Attributes	X				X
Extended Attributes	X				X
Subfolders and Files					
Permissions	X	X	X	X	X
Ownership					
Serialize	X	X	X	X	X

#### 3.3.7 Gán quyền truy cập NTFS trên thư mục dùng chung

Bạn muốn gán quyền NTFS, thông qua Windows Explorer bạn nhấp phải chuột vào tập tin hay thư mục cần cấu hình quyền truy cập rồi chọn Properties. Hộp thoại Properties xuất hiện. Nếu ổ đĩa của bạn định dạng là FAT thì hộp thoại chỉ có hai Tab là General và Sharing. Nhưng nếu đĩa có định dạng là NTFS thì trong hộp thoại sẽ có thêm một Tab là Security. Tab này cho phép ta có thể quy định quyền truy cập cho từng người dùng hoặc một nhóm người

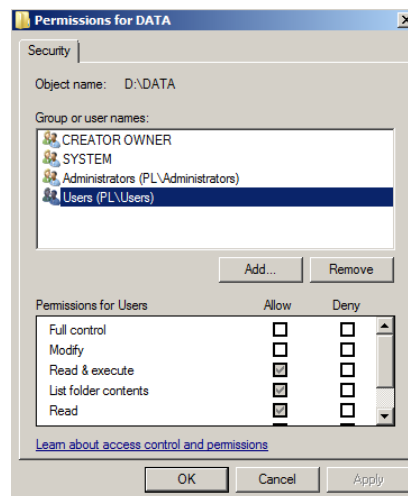
**Chương 3: Thiết lập và quản trị hệ thống mạng**  
dùng lên các tập tin và thư mục. Bạn nhấp chuột vào Tab Security để cấp quyền cho các người dùng.



**Hình 2-42. Tab Security để add người dùng và nhóm**

Muốn cấp quyền truy cập cho một người dùng, bạn nhấp chuột vào nút Add, hộp thoại chọn lựa người dùng và nhóm xuất hiện, bạn chọn người dùng và nhóm cần cấp quyền, nhấp chuột vào nút Add để thêm vào danh sách, sau đó nhấp chuột vào nút OK để trở lại hộp thoại chính.

Hộp thoại chính sẽ xuất hiện các người dùng và nhóm mà bạn mới thêm vào, sau đó chọn người dùng và nhóm để cấp quyền. Trong hộp thoại đã hiện sẵn danh sách quyền, bạn muốn cho người dùng đó có quyền gì thì bạn đánh dấu vào phần Allow, còn ngược lại muốn cấm quyền đó thì đánh dấu vào mục Deny.

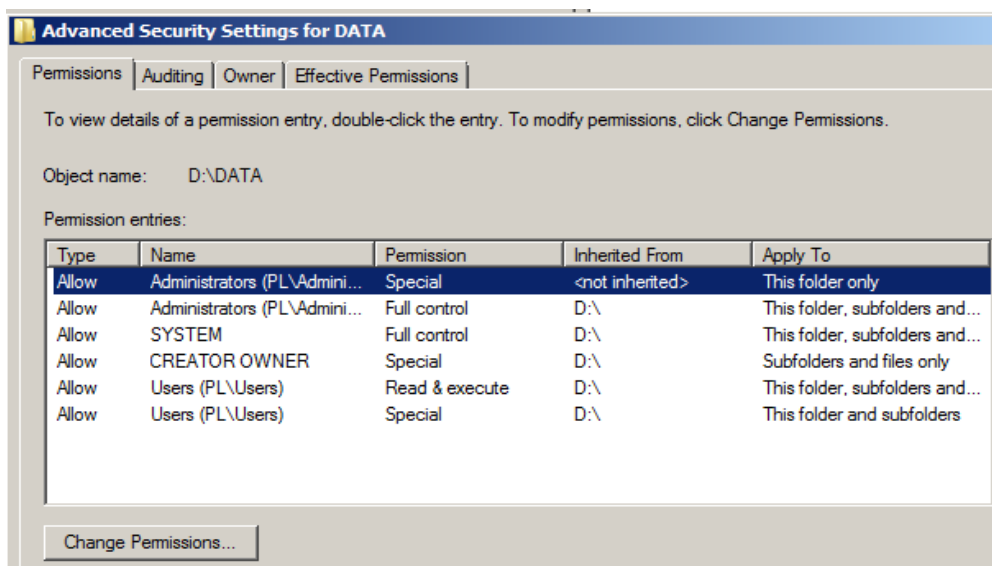


**Hình 2-43. Tab Security để cấp quyền cho các người dùng**

## Chương 3: Thiết lập và quản trị hệ thống mạng

### 3.3.8 Kế thừa và thay thế quyền của đối tượng con

Trong hộp thoại chính trên, chúng ta có thể nhấp chuột vào nút Advanced để cấu hình chi tiết hơn cho các quyền truy cập của người dùng. Khi nhấp chuột vào nút Advanced, hộp thoại Advanced Security Settings xuất hiện, trong hộp thoại, nếu bạn đánh dấu vào mục Allow inheritable permissions from parent to propagate to this object and child objects thì thư mục hiện tại được thừa hưởng danh sách quyền truy cập từ thư mục cha, bạn muốn xóa những quyền thừa hưởng từ thư mục cha bạn phải bỏ đánh dấu này. Nếu danh sách quyền truy cập của thư mục cha thay đổi thì danh sách quyền truy cập của thư mục hiện tại cũng thay đổi theo. Ngoài ra nếu bạn đánh dấu vào mục Replace permission entries on all child objects with entries shown here that apply to child objects thì danh sách quyền truy cập của thư mục hiện tại sẽ được áp dụng xuống các tập tin và thư mục con có nghĩa là các tập tin và thư mục con sẽ được thay thế quyền truy cập giống như các quyền đang hiển thị trong hộp thoại.

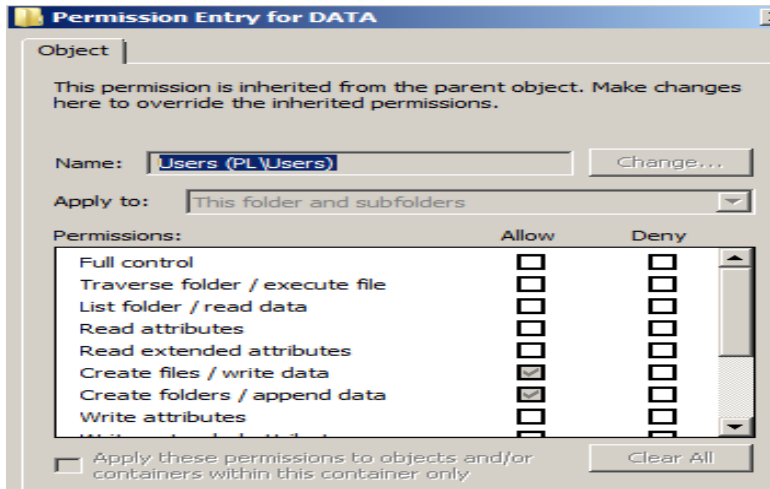


**Hình 2-44. Hộp thoại kiểm tra và phân quyền chi tiết**

Trong hộp thoại này, Windows Server 2008 cũng cho phép chúng ta kiểm tra và cấu hình lại chi tiết các quyền của người dùng và nhóm, để thực hiện, bạn chọn nhóm hay người dùng cần thao tác, sau đó nhấp chuột vào nút Edit.



## Chương 3: Thiết lập và quản trị hệ thống mạng



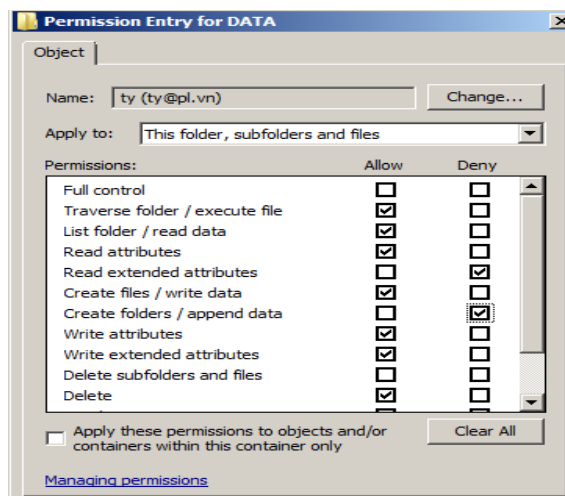
Hình 2-45. Hộp thoại phân quyền chi tiết cho người dùng

### 3.3.9 Thay đổi quyền khi di chuyển thư mục và tập tin

Khi chúng ta sao chép (copy) một tập tin hay thư mục sang một vị trí mới thì quyền truy cập trên tập tin hay thư mục này sẽ thay đổi theo quyền trên thư mục cha chứa chúng, nhưng ngược lại nếu chúng ta di chuyển (move) một tập tin hay thư mục sang bất kì vị trí nào thì các quyền trên chúng vẫn được giữ nguyên.

#### 3.3.10 Giám sát người dùng truy cập thư mục

Bạn muốn giám sát và ghi nhận lại các người dùng thao tác trên thư mục hiện tại, trong hộp thoại Advanced Security Settings, chọn Tab Auditing, nhấp chuột vào nút Add để chọn người dùng cần giám sát, sau đó bạn muốn giám sát việc truy xuất thành công thì đánh dấu vào mục Successful, ngược lại giám sát việc truy xuất không thành công thì đánh dấu vào mục Failed.

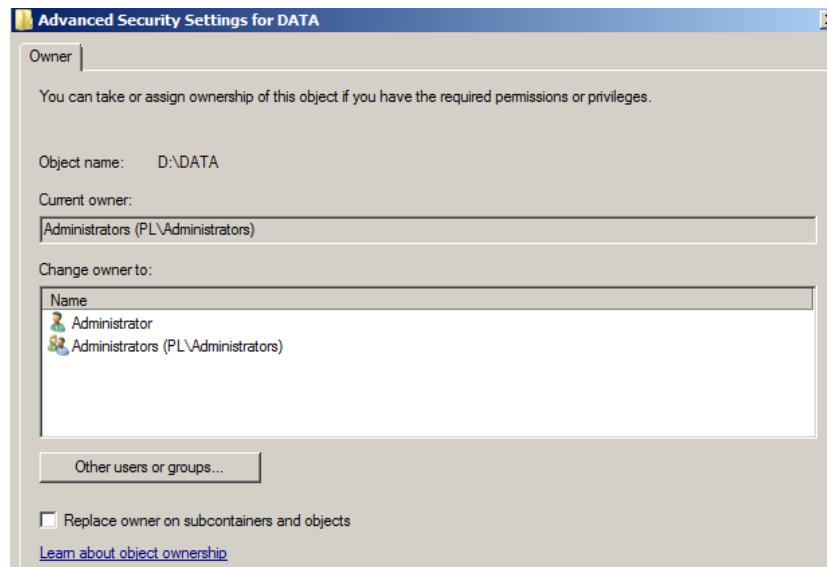


Hình 2-46. Hộp thoại chọn người dùng làm giám sát

### 3.3.11 Thay đổi người sở hữu thư mục

### Chương 3: Thiết lập và quản trị hệ thống mạng

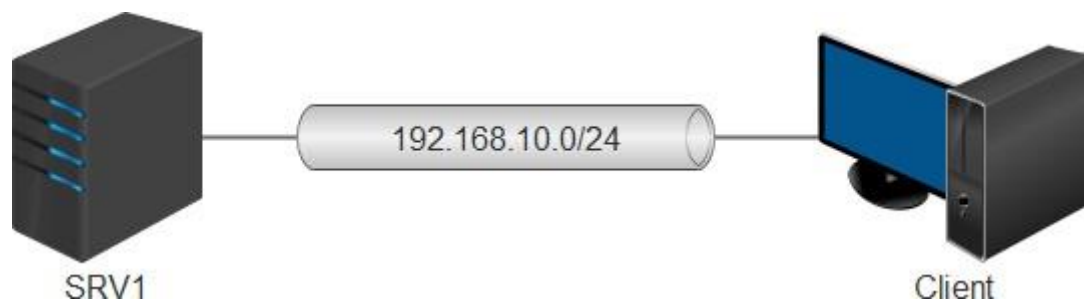
Bạn muốn xem tài khoản người và nhóm người dùng sở hữu thư mục hiện tại, trong hộp thoại Advanced Security Settings, chọn Tab Owner. Đồng thời bạn cũng có thể thay đổi người và nhóm người sở hữu thư mục này bằng cách nhấp chuột vào nút Other Users or Groups.



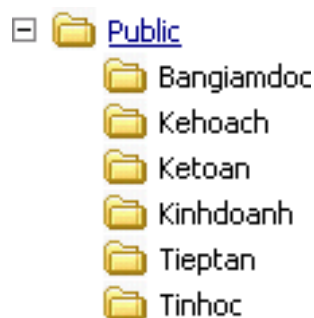
Hình 2-47. Hộp thoại thay đổi quyền sở hữu người dùng

#### Câu hỏi và bài tập

Cho mô hình mạng sau:



- ✍ Thiết lập Ip cho hệ thống theo mô hình trên.
- ✍ Xây dựng Domain với tên miền: tnut.edu.vn



✍ Tạo User, OU, Group, Add User vào trong Group

✍ Cho máy Client tham gia vào Doamain

### Chương 3: Thiết lập và quản trị hệ thống mạng

✍ Máy Client đăng nhập vào các User vừa tạo

✍ Yêu cầu 1: Share Permission

Chia sẻ thư mục Public sao cho quyền của user vẫn áp dụng đúng khi user truy cập qua mạng.

✍ Yêu cầu 2: Creator Owner

Phân quyền sao cho user các phòng ban nào có quyền tạo tài liệu thì user đó có toàn quyền trên tài liệu do mình tạo ra.

✍ Yêu cầu 3: Special permission

- Create Files / Write Data và Create Folder / Append Data

Phân quyền trên thư mục Kinhdoanh và Bangiamdoc sao cho user thuộc phòng Kinh doanh và giám đốc được quyền truy cập và tạo tài liệu (file, folder) nhưng không được xoá, sửa tài liệu của nhau.

- List Folder / Read Data

Phân quyền trên thư mục Ketoan sao cho các user thuộc phòng Kế toán chỉ được quyền tạo file và truy cập file do chính user đó tạo ra nhưng không truy cập được file của user khác.

- Traverse Folder / Execute File

Yêu cầu học viên chỉnh policy không cho phép group Everyone và Users được quyền tự động traverse folder.

Phân quyền trên thư mục Public và Tinhoc sao cho các user thuộc phòng tin học không được phép truy cập, tạo, xoá, sửa trên thư mục Public nhưng lại có quyền truy cập và tạo tài liệu ( file, folder ) trên thư mục Tinhoc.

## 3.4 Home directory, roaming profile & quota

### 3.4.1 Khái niệm Profile

Profile cho phép bạn khai báo đường dẫn đến Profile của tài khoản người dùng hiện tại, khai báo tập tin logon script được tự động thi hành khi người dùng đăng nhập hay khai báo home folder. Chú ý các tùy chọn trong Tab Profile này chủ yếu phục vụ cho các máy trạm trước Windows 2000, còn đối với các máy trạm từ Win2K trở về sau như: Win2K Pro, WinXP, Windows Server 2003, Windows Server 2008 thì chúng ta có thể cấu hình các lựa chọn này trong Group Policy

Trước tiên chúng ta hãy tìm hiểu khái niệm Profile. User Profiles là một thư mục chứa các thông tin về môi trường của Windows Server 2008 cho từng người dùng mạng. Profile chứa các qui định về màn hình Desktop, nội dung Bộ môn Tin học Công nghiệp

### Chương 3: Thiết lập và quản trị hệ thống mạng

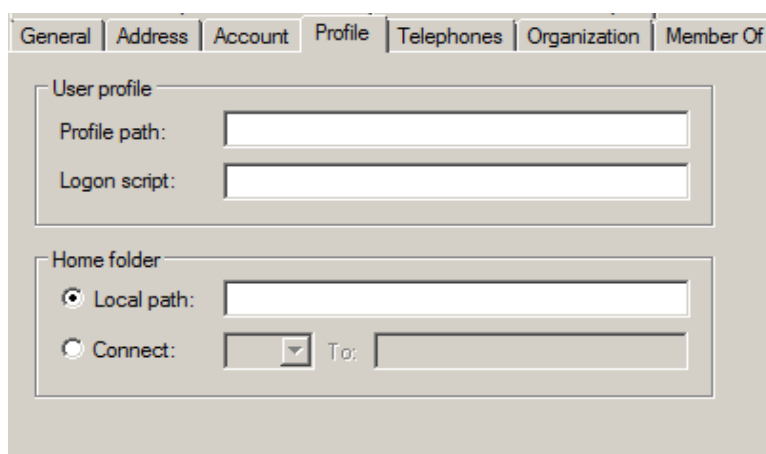
của menu Start, kiểu cách phối màu sắc, vị trí sắp xếp các icon, biểu tượng chuột...

3.4.1.1 Mặc định khi người dùng đăng nhập vào mạng, một profile sẽ được mở cho người dùng đó. Nếu là lần đăng nhập lần đầu tiên thì họ sẽ nhận được một profile chuẩn. Một thư mục có tên giống như tên của người dùng đăng nhập sẽ được tạo trong thư mục Documents and Settings. Thư mục profile người dùng được tạo chứa một tập tin nuser.dat, tập tin này được xem như là một thư mục con chứa các liên kết thư mục đến các biểu tượng nền của người dùng. Trong Windows Server 2008 có ba loại Profile: Local Profile, Roaming Profile, Mandatory profile.

Kịch bản đăng nhập (logon script hay login script) là những tập tin chương trình được thi hành mỗi khi người dùng đăng nhập vào hệ thống, với chức năng là cấu hình môi trường làm việc của người dùng và phân phát cho họ những tài nguyên mạng như ổ đĩa, máy in (được ánh xạ từ Server). Bạn có thể dùng nhiều ngôn ngữ kịch bản để tạo ra logon script như: lệnh shell của DOS/NT/Windows, Windows Scripting Host (WSH), VBScript, Jscript...

Đối với Windows Server 2008 thì có hai cách để khai báo logon script là: khai báo trong thuộc tính của tài khoản người dùng thông qua công cụ Active Directory User and Computers, khai báo thông qua Group Policy. Nhưng chú ý trong cả hai cách, các tập tin script và mọi tập tin cần thiết khác phải được đặt trong thư mục chia sẻ SYSVOL, nằm trong C:\Windows\SYSVOL\sysvol, nếu các tập tin script này phục vụ cho các máy tiền Win2K thì phải đặt trong thư mục

C:\Windows\Sysvol\sysvol\domainname\scripts. Để các tập tin script thi hành được bạn nhớ cấp quyền cho các người dùng mạng có quyền Read và Excute trên các tập tin này. Sau đây là một ví dụ về một tập tin logon script.



Hình 2-48. Hộp thoại cấu hình Profile path và xây dựng kịch bản

### 3.4.2 Giới thiệu về Home Directory

Thư mục cá nhân (Home folder hay Home directory) là thư mục dành riêng cho mỗi tài khoản người dùng, giúp người dùng có thể lưu trữ các tài liệu và tập tin riêng, đồng thời đây cũng là thư mục mặc định tại dấu nhắc lệnh. Muốn tạo một thư mục cá nhân cho người dùng thì trong mục Connect bạn chọn ổ đĩa hiển thị trên máy trạm và đường dẫn mà đĩa này cần ánh xạ đến (chú ý là các thư mục dùng chung đảm bảo đã chia sẻ).

### 3.4.3 Mục đích sử dụng Home Directory

Home Directory là 1 thuộc tính của domain user, cho phép tạo ra nơi lưu trữ dữ liệu của user trên File Server. Sau khi cấu hình Home Directory xong, hệ thống tự động thực hiện:

- Tạo Folder tương ứng với tên mỗi user.
- Phân quyền NTFS Full Control cho mỗi user tương ứng.
- Map Network Drive.

### 3.4.4 Giới thiệu Roaming profile

Roaming Profile: là loại Profile được chứa trên mạng và người quản trị mạng thêm thông tin đường dẫn user profile vào trong thông tin tài khoản người dùng, để tự động duy trì một bản sao của tài khoản người dùng trên mạng.

### 3.4.5 Mục đích sử dụng của Roaming Profile

User lần đầu tiên đăng nhập vào 1 máy trạm nào đó thì nó sẽ tạo ra một Profile. Việc sử dụng Roaming profile khắc phục tình trạng tạo ra một local profile cho người dùng

### 3.4.6 Dịch vụ tập tin (File Services)

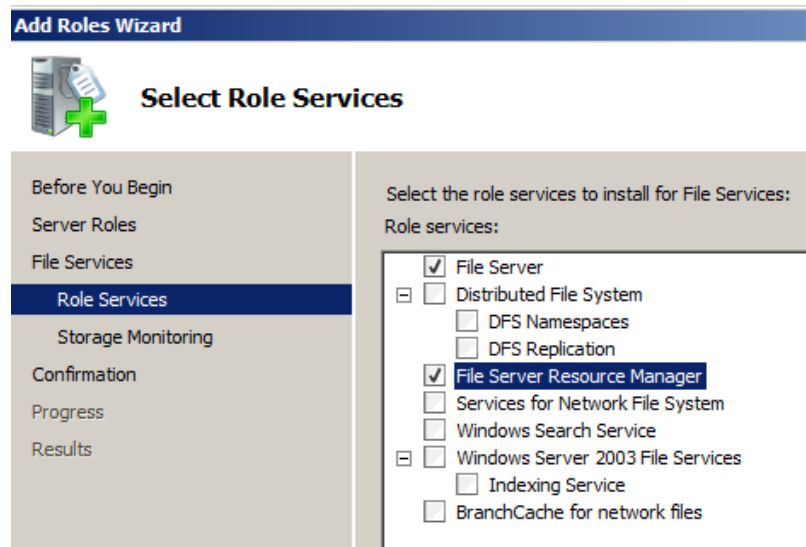
File Server Resource Manager là một tập hợp các công cụ cho phép người quản trị có thể điều khiển và quản lý dữ liệu trên các server chạy hệ điều hành Windows Server 2008 một cách hiệu quả. Với công cụ này, có thể cấu hình quota trên cả ổ đĩa và thư mục, ngăn cấm sao chép những định dạng mà bạn chỉ định,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

## Chương 3: Thiết lập và quản trị hệ thống mạng

3.4.6.1 Để cài đặt dịch vụ File Services vào Server Manager → Roles → Add Roles.



Hình 2-49. Hộp thoại cài đặt dịch vụ thư mục



Hình 2-50. Cài đặt Quota

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

## Chương 3: Thiết lập và quản trị hệ thống mạng

### 3.4.7 Quản lý Quota

Để tạo một Quota vào Start → Administrative Tools → File Server Resource Manager → Click vào Quota Management → Quota Templates

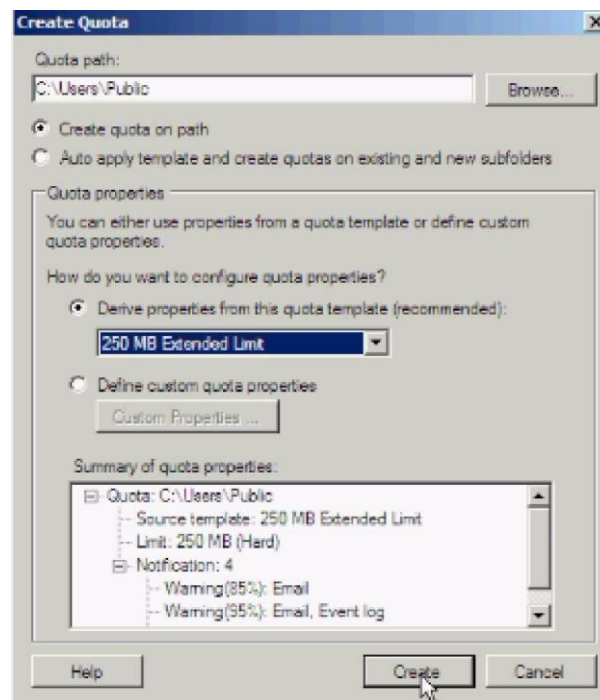
Ở khung giữa, nhấp chuột phải vào một template và chọn Create Quota from Template

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



Hình 2-51. Tạo một Quota Template

### Chương 3: Thiết lập và quản trị hệ thống mạng

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.

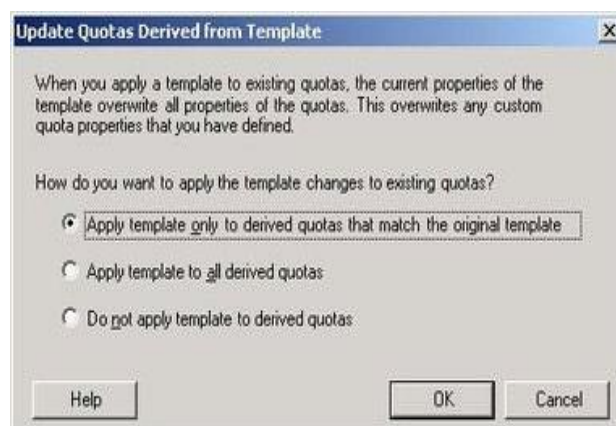
Để tùy chỉnh cho quota template vừa tạo, nhấp chuột phải vào quota template và chọn Edit Template Properties...Sau đó thực hiện các thay đổi cần thiết và chọn OK.

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 quota: cập nhật cho tất cả các quota sử dụng template này  
Do not apply template to derived quota: không muốn thực hiện tạo tác cập nhật quota.

Nhấn OK để hoàn tất.



Hình 2-52. Hộp thoại lựa chọn cập nhật Quota



## Chương 3: Thiết lập và quản trị hệ thống mạng

### 3.4.8 Quản lý các báo cáo

Vào Start → Administrative Tools → File Server Resource Manager...Right-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

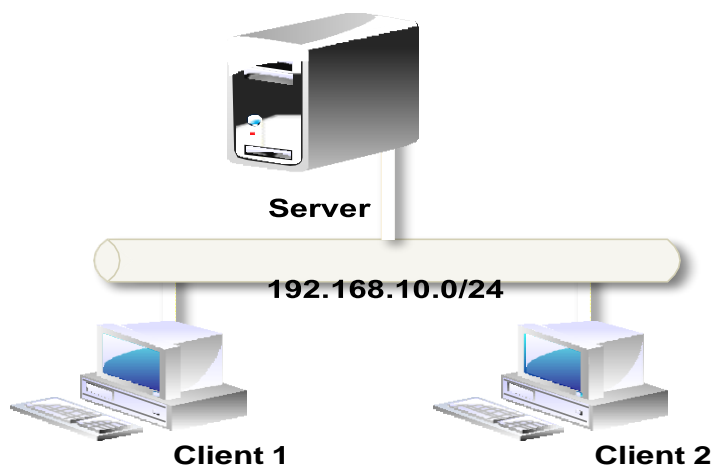
Sau đó chọn Close và chọn OK để hoàn tất thiết lập. Để lập lịch xuất ra các báo cáo, trong File Server Resource Manager, right-click vào Storage Reports Management và chọn Schedule a New Report Task.

Tại tab Settings, ở mục Scope, lick 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.

### ***Câu hỏi và bài tập***

Cho mô hình mạng sau:



nhau.

✍ Thiết lập IP theo mô hình đảm bảo các máy tính liên lạc được với

✓ Thiết lập Local Profile.

## Chương 3: Thiết lập và quản trị hệ thống mạng

- ✓ Thiết lập Roaming Profile.
- ✓ Thiết lập Mandatory Profile.
- ✓ Thiết lập Home Dir.

- **Quản lý in ấn**

### 3.4.9 Cài đặt máy in

Trước khi bạn có thể truy xuất vào thiết bị máy in vật lý thông qua hệ điều hành Windows Server 2008 thì bạn phải tạo ra một máy in logic. Nếu máy in của bạn có tính năng Plug and Play thì máy in đó sẽ được nhận diện ra ngay khi nó được gắn vào máy tính dùng hệ điều hành Windows Server 2008.

Tiện ích Found New Hardware Wizard sẽ tự động bật lên. Tiện ích này sẽ hướng dẫn cho bạn từng bước để cài đặt máy in. Nếu hệ điều hành nhận diện không chính xác thì bạn dùng đĩa CD được hãng sản xuất cung cấp kèm theo máy để cài đặt.

Ngoài ra, bạn cũng có thể tự mình thực hiện tạo ra một máy in logic bằng cách sử dụng tiện ích Add Printer Wizard. Để có thể tạo ra một máy in logic trong Windows Server 2008 thì trước hết bạn phải đăng nhập vào hệ thống với vai trò là một thành viên của nhóm Administrators hay nhóm Power Users (trong trường hợp đây là một Server thành viên) hay nhóm Server Operators (trong trường hợp đây là một domain controller).

Bạn có thể tạo ra một máy in logic cục bộ tương ứng với một máy in vật lý được gắn trực tiếp vào máy tính cục bộ của mình hoặc tương ứng với một máy in mạng (máy in mạng được gắn vào một máy tính khác trong mạng hay một thiết bị Print Server). Muốn thao tác bằng tay để tạo ra một máy in cục bộ hay một máy in mạng, chúng ta lần lượt thực hiện các thao tác sau đây:

Nhấp chuột chọn Start, rồi chọn Printers And Faxes.

Nhấp chuột vào biểu tượng Add Printer, tiện ích Add Printer Wizard sẽ được khởi động. Nhấp chuột vào nút Next để tiếp tục.

Hộp thoại Local Or Network Printer xuất hiện. Bạn nhấp vào tùy chọn Local Printer Attached To This Computer trong trường hợp bạn có một máy in vật lý gắn trực tiếp vào máy tính của mình. Nếu trường hợp ta đang tạo ra một máy in logic ứng với một máy in mạng thì ta nhấp vào tùy chọn A Printer Attached To Another Computer. Nếu máy in được gắn trực tiếp vào máy tính, bạn có thể chọn thêm tính năng Automatically Detect And Install My Plug And Play Printer. Tùy chọn này cho phép hệ thống tự động quét máy tính của bạn

### Chương 3: Thiết lập và quản trị hệ thống mạng

để phát hiện ra các máy in Plug and Play, và tự động cài đặt các máy in đó cho bạn. Khi đã hoàn tất việc chọn lựa, nhấp chuột vào nút Next để sang bước kế tiếp.

Nếu máy in vật lý đã được tự động nhận diện bằng tiện ích Found New Hardware Wizard. Tiện ích này sẽ hướng dẫn bạn tiếp tục cài đặt driver máy in qua từng bước.

Hộp thoại Print Test Page xuất hiện. Nếu thiết bị máy in được gắn trực tiếp vào máy tính của bạn, bạn nên in thử một trang kiểm tra để xác nhận rằng mọi thứ đều được cấu hình chính xác. Ngược lại, nếu máy in là máy in mạng thì bạn nên bỏ qua bước này. Nhấp chuột vào nút Next để sang bước kế tiếp.

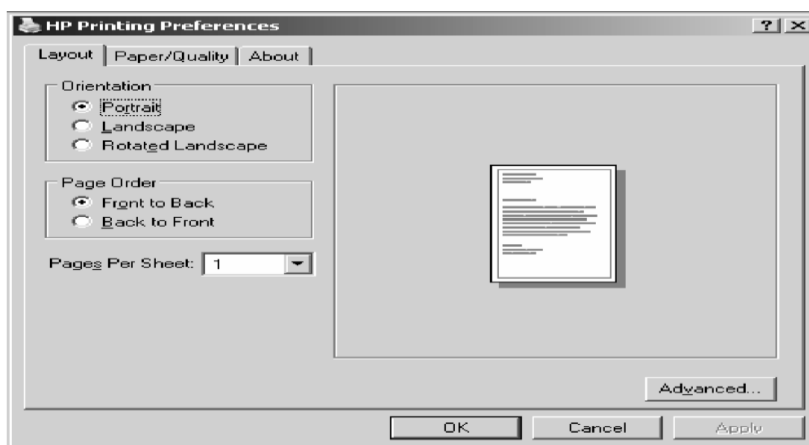
Hộp thoại Completing The Add Printer Wizard hiện ra. Hộp thoại này đem đến cho chúng ta một cơ hội để xác nhận rằng tất cả các thuộc tính máy in đã được xác lập chính xác. Nếu bạn phát hiện có thông tin nào không chính xác, hãy nhấp chuột vào nút Back để quay lại sửa chữa thông tin cho đúng. Còn nếu nhận thấy mọi thứ đều ổn cả thì bạn nhấp chuột vào nút Finish.

Một biểu tượng máy in mới sẽ hiện ra trong cửa sổ Printer And Faxes. Theo mặc định, máy in sẽ được chia sẻ.

#### 3.4.10 Quản lý thuộc tính máy in

##### 2.5.2.1 Cấu hình Layout

Trong hộp thoại Printing Preferences, chọn Tab Layout. Sau đó trong mục Orientation, bạn chọn cách thức in trang theo chiều ngang hay chiều dọc. Trong mục Page Order, bạn chọn in từ trang đầu đến trang cuối của tài liệu hoặc in theo thứ tự ngược lại. Trong mục Pages Per Sheet, bạn chọn số trang tài liệu sẽ được in trên một trang giấy.

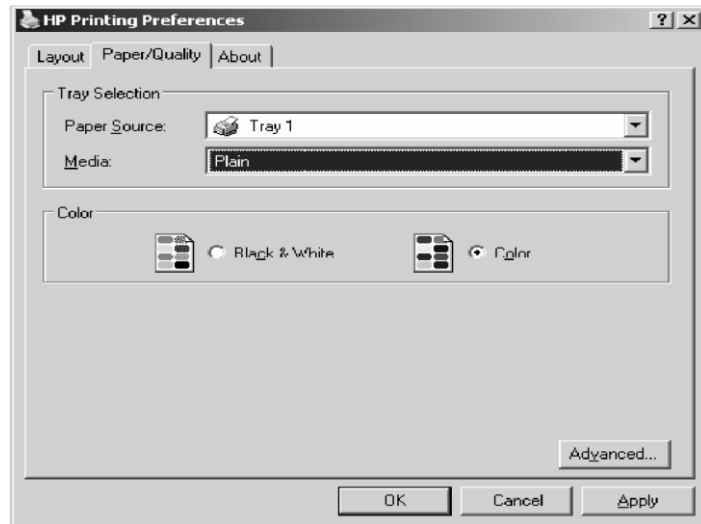


Hình 2-53. Điều chỉnh trang in

#### 3.4.11 Giấy và chất lượng in

### Chương 3: Thiết lập và quản trị hệ thống mạng

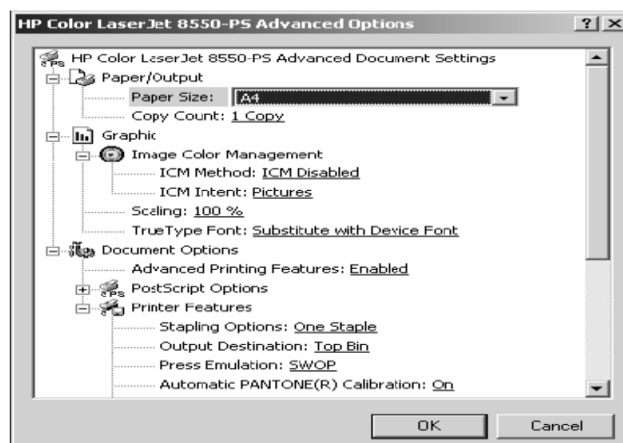
Cũng trong hộp thoại Printing Preferences, để qui định giấy và chất lượng in, chúng ta chọn Tab Paper/Quality. Các tùy chọn trong Tab Paper/Quality phụ thuộc vào đặc tính của máy in. Ví dụ, máy in chỉ có thể cung cấp một tùy chọn là Paper Source. Còn đối với máy in HP OfficeJet Pro Cxi, chúng ta có các tùy chọn là: Paper Source, Media, Quality Settings và Color.



Hình 2-54. Chọn độ sắc nét và màu (nếu có) của máy in

#### 3.4.12 Các thông số mở rộng

Nhấp chuột vào nút Advanced ở góc dưới bên phải của hộp thoại Printing Preferences. Hộp thoại Advanced Options xuất hiện cho phép bạn điều chỉnh các thông số mở rộng. Chúng ta có thể có các tùy chọn của máy in như: Paper/Output, Graphic, Document Options, và Printer Features. Các thông số mở rộng có trong hộp thoại Advanced Options phụ thuộc vào driver máy in mà bạn đang sử dụng.



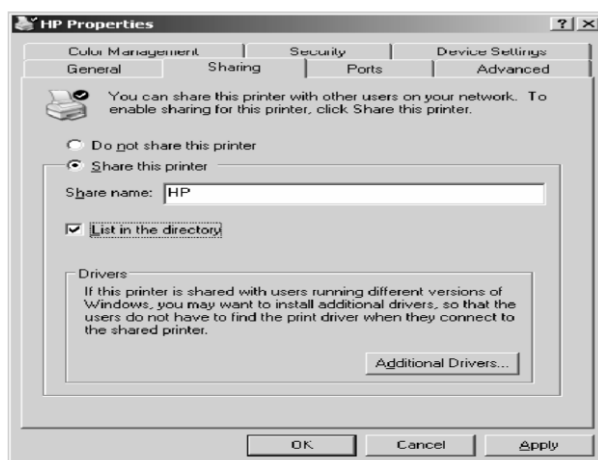
Hình 2-55. Hộp thoại điều chỉnh thông số mở rộng của máy in

#### 3.4.13 Cấu hình chia sẻ máy in

Nhấp phải chuột lên máy in, chọn Properties. Hộp thoại Properties xuất

**Chương 3: Thiết lập và quản trị hệ thống mạng**  
hiện, bạn chọn Tab Sharing.

Để chia sẻ máy in này cho nhiều người dùng, bạn nhấp chuột chọn Share this printer. Trong mục Share name, bạn nhập vào tên chia sẻ của máy in, tên này sẽ được nhìn thấy trên mạng. Bạn cũng có thể nhấp chọn mục List In The Directory để cho phép người dùng có thể tìm kiếm máy in thông qua Active Directory theo một vài thuộc tính đặc trưng nào đó.



**Hình 2-56. Hộp thoại chia sẻ máy in**

#### **3.4.14 Cấu hình thông số port cho máy in**

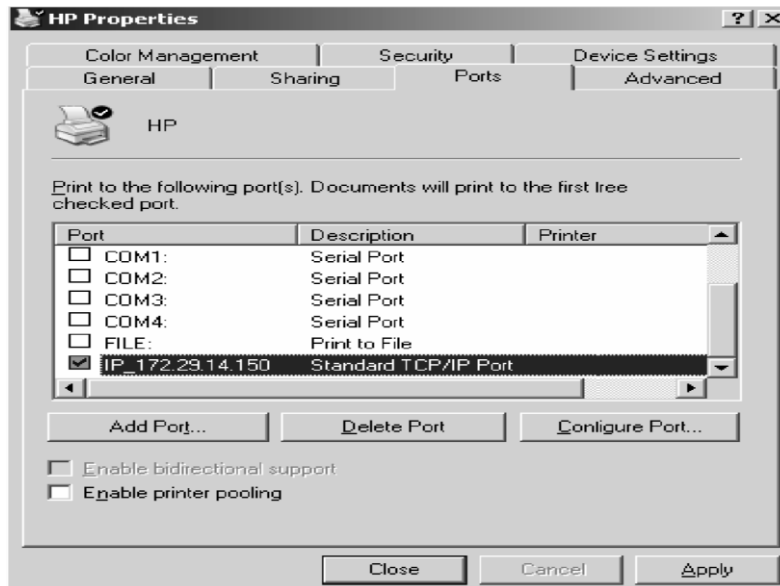
#### **3.4.15 Cấu hình các thông số trong Tab Port**

Trong hộp thoại Properties, bạn chọn Tab Port để cấu hình tất cả các port đã được định nghĩa cho máy in sử dụng. Một port được định nghĩa như một interface sẽ cho phép máy tính giao tiếp với thiết bị máy in. Windows Server 2008 hỗ trợ các port vật lý (local port) và các port TCP/IP chuẩn (port logic).

Port vật lý chỉ được sử dụng khi ta gắn trực tiếp máy in vào máy tính. Trong trường hợp Windows Server 2008 đang được triển khai trong một nhóm làm việc nhỏ, hầu như bạn phải gắn máy in vào port LPT1.

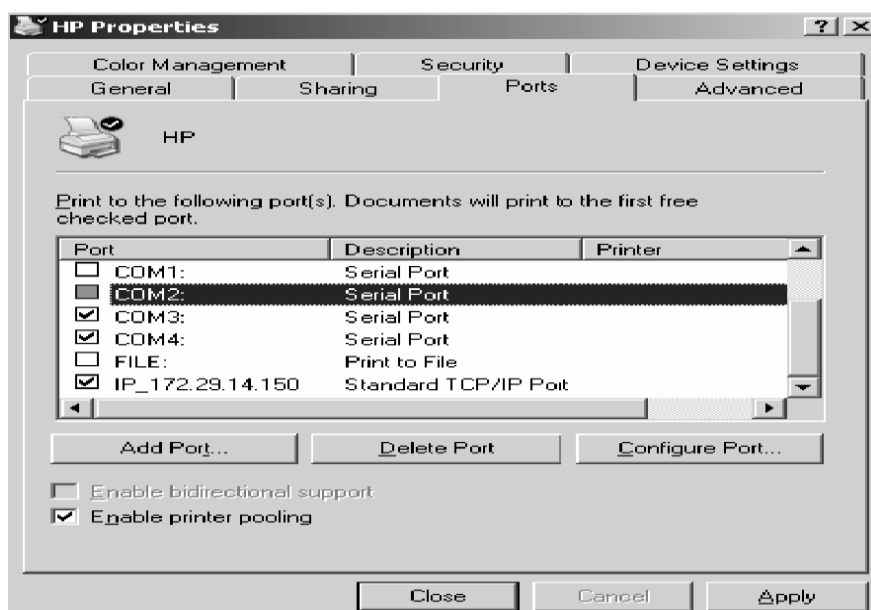
Port TCP/IP chuẩn được sử dụng khi máy in có thể kết nối trực tiếp vào mạng (trên máy in có hỗ trợ port RJ45) và máy in này có một địa chỉ IP để nhận dạng. Ưu điểm của máy in mạng là tốc độ in nhanh hơn máy in cục bộ và máy in có thể đặt bất kỳ nơi nào trong hệ thống mạng. Khi đó bạn cần chỉ định một port TCP/IP và khai báo địa chỉ IP của máy in mạng. Cùng với việc xóa và cấu hình lại một port đã tồn tại, bạn cũng có thể thiết lập printer pooling và điều hướng các công việc in ấn đến một máy in khác.

### Chương 3: Thiết lập và quản trị hệ thống mạng



**Hình 2-57. Hộp thoại cấu hình Port của máy in**

Để cấu hình một printer pool, bạn nhấp chuột vào tùy chọn Enable Printer Pooling nằm ở phía dưới Tab Port trong hộp thoại Properties. Sau đó, kiểm tra lại tất cả các port mà ta dự định gắn các máy in vật lý trong printer pool vào. Nếu ta không chọn tùy chọn Enable Printer Pool thì ta chỉ có một port duy nhất cho mỗi máy in. Chú ý tất cả các máy in vật lý trong một printer pool phải sử dụng cùng một driver máy in.



**Hình 2-58. Hộp thoại bật chức năng Printer pool**

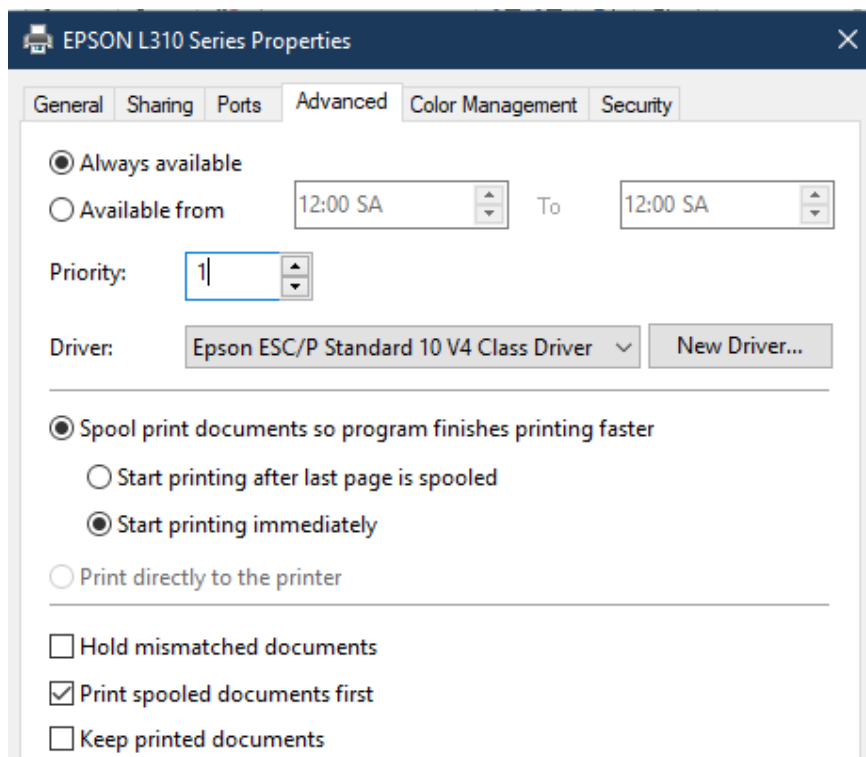
## Chương 3: Thiết lập và quản trị hệ thống mạng

### 3.4.16 Khả năng sẵn sàng phục vụ của máy in

Thông thường, chúng ta cần kiểm tra khả năng sẵn sàng phục vụ của máy in trong trường hợp chúng ta có nhiều máy tính cùng sử dụng một thiết bị in. Mặc định thì tùy chọn Always Available luôn được bật lên. Do đó, người dùng có thể sử dụng máy in 24 tiếng một ngày. Để giới hạn khả năng phục vụ của máy in, bạn chọn Available From và chỉ định khoảng thời gian mà máy in sẽ phục vụ. Ngoài khoảng thời gian này, máy in sẽ không phục vụ cho bất kỳ người dùng nào.

### 3.4.17 Độ ưu tiên (Printer Priority)

Khi bạn đặt độ ưu tiên, bạn sẽ định ra bao nhiêu công việc sẽ được gửi trực tiếp vào thiết bị in. Ví dụ, bạn có thể sử dụng tùy chọn này khi 2 nhóm người dùng cùng chia sẻ một máy in và bạn cần điều khiển độ ưu tiên đối với các thao tác in ấn trên thiết bị in này.



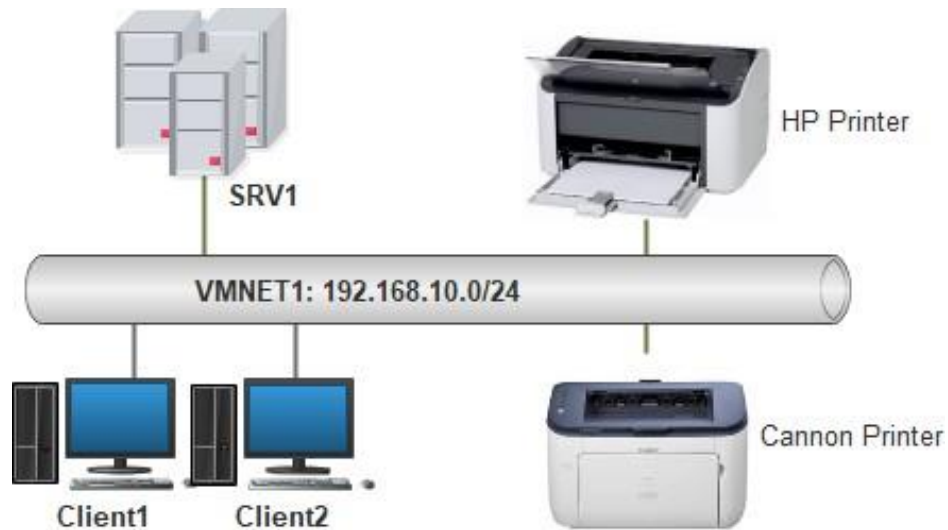
Hình 2-59. Set độ ưu tiên của máy in

Trong Tab Advanced của hộp thoại Properties, bạn sẽ đặt độ ưu tiên bằng các giá trị từ 1 đến 99, với 1 là có độ ưu tiên thấp nhất và 99 là có độ ưu tiên cao nhất.

## Chương 3: Thiết lập và quản trị hệ thống mạng

### *Câu hỏi và bài tập*

Cho mô hình mạng sau:



Sử dụng dịch vụ Print Management với Group Policy để tự động cài đặt máy in và driver cho các User hoặc Computer trong doanh nghiệp.

Hướng dẫn:

- Cài đặt Print Management
- Cài đặt Printer
- Deploy Printer cho Users
- Deploy Printer cho Computer
- Cấu hình Group Policy
- Client kiểm tra



## Chương 3: Thiết lập và quản trị hệ thống mạng

### TÀI LIỆU THAM KHẢO

- I Trung tâm Đào tạo Mạng máy tính Nhất Nghệ, ***LAB MCSA 2003 70-270 & 70-290***, 2006.
- II Trung tâm Đào tạo Công nghệ mạng & Lập trình Việt Chuyên, ***LAB 70-290***, 2007.
- III Dan Holme, Orin Thomas, ***MCSA/MCSE Self-Paced Training Kit Managing and Maintaining a Microsoft Windows Server 2003 Environment Microsoft***, 2004.