LỜI GIỚI THIỆU

Hoạt động biên soạn giáo trình là một hoạt động nghiên cứu khoa học . Mỗi giáo viên, giảng viên trên cơ sở các phương pháp và nguyên tắc chung sẽ có sự vận dụng sáng tạo vào điều kiện cụ thể của mình để sáng tạo ra các nội dung giảng dạy hấp dẫn, thu hút người học.

Nhằm giúp đội ngũ giáo viên có tài liệu cơ sở để tiến hành các buổi lên lớp được hiệu quả cũng như việc cung cấp tài liệu giúp cho sinh viên nói chung, đặc biệt là sinh viên chuyên ngành Quản trị mạng. Để đáp ứng nhu cầu thực tiễn này khoa Công nghệ thông tin đã tổ chức biên soạn cuốn giáo trình "Cài đặt quản trị Windows" do nhóm giáo viên thuộc chuyên ngành Quản trị mạng đang công tác tại trường TCN KTCN Hùng Vương biên soạn.

Đây là công trình được viết bởi đội ngũ giáo viên đã và đang công tác tại nhà trường cùng với sự góp ý và phản biện của các doanh nghiệp trong lĩnh vực liên quan, tuy vậy, cuốn sách chắc chắn vẫn không tránh khỏi những khiếm khuyết. Chúng tôi mong nhận được ý kiến đóng góp của bạn đọc để cuốn sách được hoàn thiện hơn trong lần tái bản.

Xin trân trọng giới thiệu cùng bạn đọc!

Quận 5, ngày tháng năm 2019

Tham gia biên soạn

1. Chủ biên Nguyễn Quốc Cường

2. Nguyễn Hữu Phước

3. Đỗ Như Hảo

MỤC LỤC

ĐỀ MỤC **TRANG**

GIỚI THIỆU MÔN HỌC CÀI ĐẶT VÀ QUẢN TRỊ WINDOWS

I. VỊ TRÍ, TÍNH CHẤT CỦA MÔ ĐUN:

- Vị trí của mô đun: Mô đun được bố trí sau khi sinh viên học xong các môn học chung, trước các môn học, mô đun đào tạo cơ sở nghề.
- Tính chất của mô đun: Là mô đun nghề đào tạo bắt buộc.

II. MỤC TIÊU MÔ ĐUN:

- Phân biệt sự khác nhau trong việc quản trị máy chủ (Server) và máy trạm (workstation).
- Tạo được tài khoản người dùng, tài khoản nhóm.
- Các kiến thức về việc duy trì tài khoản nhóm và sắp xếp hệ thống hoá các tác vụ quản trị tài khoản người dùng và tài khoản nhóm.
- Các kiến thức chia sẻ và cấp quyền truy cập tài nguyên dùng chung.
- Nguyên tắc thiết lập cấu hình và quản trị in ấn của một máy phục vụ in mạng.
- Các công cụ thu nhập thông tin về tài nguyên mạng và tài nguyên máy tính.
- Công dụng và chức năng của các thiết bị mạng

III. NỘI DUNG MÔ ĐUN:

Chương 1: Introduction to Administering Accounts and Resources

Bài 1: TỔNG QUAN VỀ WINDOWS SERVER

Mục tiêu:

- Phân biệt được về họ hệ điều hành Windows Server;
- Cài đặt được hệ điều hành Windows Server.
- Thực hiện các thao tác an toàn với máy tính.

1. Tổng quan về họ hệ điều hành Windows Server 2003:

Như chúng ta đã biết họ hệ điều hành **Windows 2000 Server** có 3 phiên bản chính là: **Windows 2000 Server**, **Windows 2000 Advanced Server**, **Windows 2000 Datacenter Server**. Với mỗi phiên bản **Microsoft** bổ sung các tính năng mở rộng cho từng loại dịch vụ. Đến khi họ **Server 2003** ra đời thì **Mircosoft** cũng dựa trên tính năng của từng phiên bản để phân loại do đó có rất nhiều phiên bản của họ **Server 2003** được tung ra thị trường. Nhưng 4 phiên bản được sử dụng rộng rãi nhất là: **Windows Server 2003 Standard Edition**, **Enterprise Edition**, **Datacenter Edition**, **Web Edition**.

So với các phiên bản 2000 thì họ hệ điều hành **Server** phiên bản 2003 có những đặc tính mới sau:

- Khả năng kết chùm các **Server** để san sẻ tải (**Network Load Balancing Clusters**) và cài đặt nóng RAM (**hot swap**).
- **Windows Server 2003** hỗ trợ hệ điều hành **WinXP** tốt hơn như: hiểu được chính sách nhóm (**group policy**) được thiết lập trong **WinXP**, có bộ công cụ quản trị mạng đầy đủ các tính năng chạy trên **WinXP.**
- Tính năng cơ bản của **Mail Server** được tính hợp sẵn: đối với các công ty nhỏ không đủ chi phí để mua **Exchange** để xây dựng **Mail Server** thì có thể sử dụng dịch vụ **POP3** và **SMTP** đã tích hợp sẵn vào **Windows Server 2003** để làm một hệ thống mail đơn giản phục vụ cho công ty.
- Cung cấp miễn phí hệ cơ sở dữ liệu thu gọn **MSDE (Mircosoft Database Engine)** được cắt xén từ **SQL Server 2000**.Tuy **MSDE** không có công cụ quản trị nhưng nó cũng giúp ích cho các công ty nhỏ triển khai được các ứng dụng liên quan đến cơ sở dữ liệu mà không phải tốn chi phí nhiều để mua bản **SQL Server**.
- **NAT Traversal** hỗ trợ **IPSec** đó là một cải tiến mới trên môi trường 2003 này, nó cho phép các máy bên trong mạng nội bộ thực hiện các kết nối **peer-to-peer** đến các máy bên ngoài **Internet**, đặt biệt là các thông tin được truyền giữa các máy này có thể được mã hóa hoàn toàn.
- Bổ sung thêm tính năng **NetBIOS over TCP/IP** cho dịch vụ **RRAS (Routing and Remote Access)**. Tính năng này cho phép bạn duyệt các máy tính trong mạng ở xa thông qua công cụ **Network Neighborhood**.
- Phiên bản **Active Directory 1.1** ra đời cho phép chúng ta ủy quyền giữa các gốc rừng với nhau đồng thời việc backup dữ liệu của **Active Directory** cũng dễ dàng hơn.
- Hỗ trợ tốt hơn công tác quản trị từ xa do **Windows 2003** cải tiến **RDP (Remote Desktop Protocol)** có thể truyền trên đường truyền 40Kbps. **Web Admin** cũng ra

đời giúp người dùng quản trị Server từ xa thông qua một dịch vụ Web một cách trực quan và dễ dàng.
- Hỗ trợ môi trường quản trị **Server** thông qua dòng lệnh phong phú hơn.
- Các **Cluster NTFS** có kích thước bất kỳ khác **với Windows 2000 Server** chỉ hỗ trợ 4KB.
- Cho phép tạo nhiều gốc **DFS (Distributed File System)** trên cùng một Server.

2. Chuẩn bị cài đặt windows server

Hoạch định và chuẩn bị đầy đủ là yếu tố quan trọng quyết định quá trình cài đặt có trơn tru hay không. Trước khi cài đặt, bạn phải biết được những gì cần có để có thể cài đặt thành công và bạn đã có được tất cả những thông tin cần thiết để cung cấp cho quá trình cài đặt. Để lên kế hoạch cho việc nâng cấp hoặc cài mới các **Server** bạn nên tham khảo các hướng dẫn từ **Microsoft Windows Server 2003 Deployment Kit** . Các thông tin cần biết trước khi nâng cấp hoặc cài mới hệ điều hành:
- Phần cứng đáp ứng được yêu cầu của **Windows Server 2003.**
- Làm sao để biết được phần cứng của hệ thống có được **Windows Server 2003** hỗ trợ hay không.
- Điểm khác biệt giữa cách cài đặt mới và cách nâng cấp (**upgrade**).
- Những lựa chọn cài đặt nào thích hợp với hệ thống của bạn, chẳng hạn như chiến lược chia **partition** đĩa, và bạn sẽ sử dụng hệ thống tập tin nào…

2.1. Yêu Cầu phần cứng:

- Đối với windows Server 2003 yêu cầu về phần cứng như sau:

Thành phần	Yêu cầu
Bộ xử lý	Tối thiểu: 133 MHz. Khuyến nghị: Tốc độ xử lý 550 MHz hoặc nhanh hơn. Chú ý: hỗ trợ lên đến 8 bộ vi xử lý trên 1 server.
Bộ nhớ	Tối thiểu: 128 MB Khuyến nghị: 256 MB trở lên Tối đa: 64 GB
Không gian ổ đĩa còn trống	1.25 GB đến 2 GB
Ổ đĩa	Ổ CD hoặc DVD-ROM
Màn hình	Super VGA (800 × 600) hoặc màn hình có độ phân giải cao hơn

2.2. Tương thích phần cứng:

Một bước quan trọng trước khi nâng cấp hoặc cài đặt mới Server của bạn là kiểm tra xem phần cứng của máy tính hiện tại có tương thích với sản phẩm hệ điều hành trong họ **Windows Server 2003**. Bạn có thể làm việc này bằng cách chạy chương trình kiểm tra tương thích có sẵn trong đĩa CD hoặc từ trang Web **Catalog**. Nếu chạy chương trình kiểm tra từ đĩa CD, tại dấu nhắc lệnh bạn nhập: ***\i386\winnt32 /checkupgradeonly***.

2.3. Cài đặt mới hoặc nâng cấp:

Trong một số trường hợp hệ thống **Server** chúng ta đang hoạt động tốt, các ứng dụng và dữ liệu quan trọng đều lưu trữ trên **Server** này, nhưng theo yêu cầu chúng ta phải nâng cấp hệ điều hành **Server** hiện tại thành **Windows Server 2003**. Chúng ta cần xem xét nên nâng cấp hệ điều hành đồng thời giữ lại các ứng dùng và dữ liệu hay cài đặt mới hệ điều hành rồi sau cấu hình và cài đặt ứng dụng lại. Đây là vấn đề cần xem xét và lựa chọn cho hợp lý.

Các điểm cần xem xét khi nâng cấp:

- Với nâng cấp (**upgrade**) thì việc cấu hình **Server** đơn giản, các thông tin của bạn được giữ lại như: người dùng (**users**), cấu hình (**settings**), nhóm (**groups**), quyền hệ thống (**rights**), và quyền truy cập (**permissions**)…
- Với nâng cấp bạn không cần cài lại các ứng dụng, nhưng nếu có sự thay đổi lớn về đĩa cứng thì bạn cần backup dữ liệu trước khi nâng cấp.
- Trước khi nâng cấp bạn cần xem hệ điều hành hiện tại có nằm trong danh sách các hệ điều hành hỗ trợ nâng cấp thành **Windows Server 2003** không ?
- Trong một số trường hợp đặc biệt như bạn cần nâng cấp một máy tính đang làm chức năng **Domain Controller** hoặc nâng cấp một máy tính đang có các phần mềm quan trọng thì bạn nên tham khảo thêm thông tin hướng dẫn của **Microsoft** chứa trong thư mục **\Docs** trên đĩa CD **Windows Server 2003 Enterprise**.

Các hệ điều hành cho phép nâng cấp thành **Windows Server 2003 Enterprise Edition**:

- **Windows NT Server 4.0** với **Service Pack 5** hoặc lớn hơn.
- **Windows NT Server 4.0**, **Terminal Server Edition**, với **Service Pack 5** hoặc lớn hơn.
- **Windows NT Server 4.0**, **Enterprise Edition**, với **Service Pack 5** hoặc lớn hơn.
- **Windows 2000 Server.**
- **Windows 2000 Advanced Server.**
- **Windows Server 2003, Standard Edition.**

2.4. Phân chia ổ đĩa:

Đây là việc phân chia ổ đĩa vật lý thành các **partition logic**. Khi chia **partition**, bạn phải quan tâm các yếu tố sau:

- **Lượng không gian cần cấp phát:** bạn phải biết được không gian chiếm dụng bởi hệ điều hành, các chương trình ứng dụng, các dữ liệu đã có và sắp phát sinh.
- **Partition system và boot:** khi cài đặt **Windows 2003 Server** sẽ được lưu ở hai vị trí là **partition system** và **partition boot**. **Partition system** là nơi chứa các tập tin

giúp cho việc khởi động **Windows 2003 Server**. Các tập tin này không chiếm nhiều không gian đĩa. Theo mặc định, **partition active** của máy tính sẽ được chọn làm **partition system**, vốn thường là ổ đĩa C:. **Partition boot** là nơi chứa các tập tin của hệ điều hành. Theo mặc định các tập tin này lưu trong thư mục **WINDOWS**. Tuy nhiên bạn có thể chỉ định thư mục khác trong quá trình cài đặt. **Microsoft** đề nghị **partition** này nhỏ nhất là 1,5 GB.

- Cấu hình đĩa đặc biệt: **Windows 2003 Server** hỗ trợ nhiều cấu hình đĩa khác nhau. Các lựa chọn có thể là **volume simple**, **spanned**, **striped**, **mirrored** hoặc là **RAID-5**.

- **Tiện ích phân chia partition:** nếu bạn định chia **partition** trước khi cài đặt, bạn có thể sử dụng

nhiều chương trình tiện ích khác nhau, chẳng hạn như **FDISK** hoặc **PowerQuest Partition Magic**. Có thể ban đầu bạn chỉ cần tạo một **partition** để cài đặt **Windows 2003 Server**, sau đó sử dụng công cụ **Disk Management** để tạo thêm các **partition** khác.

2.5. Chọn hệ thống tập tin:

Bạn có thể chọn sử dụng một trong ba loại hệ thống tập tin sau:

- ***FAT16*** (**file allocation table**)***:*** là hệ thống được sử dụng phổ biến trên các hệ điều hành **DOS** và **Windows 3.x**. Có nhược điểm là **partition** bị giới hạn ở kích thước 2GB và không có các tính năng bảo mật như **NTFS.**

- ***FAT32:*** được đưa ra năm 1996 theo bản **Windows 95 OEM Service Release 2 (OSR2)**. Có nhiều ưu điểm hơn **FAT16** như: hỗ trợ **partition** lớn đến 2TB; có các tính năng dung lỗi và sử dụng không gian đĩa cứng hiệu quả hơn do giảm kích thước **cluster**. Tuy nhiên **FAT32** lại có nhược điểm là không cung cấp các tính năng bảo mật như **NTFS**.

- ***NTFS:*** là hệ thống tập tin được sử dụng trên các hệ điều hành **Windows NT, Windows 2000**, **Windows 2003**. **Windows 2000, Windows 2003** sử dụng **NTFS** phiên bản 5. Có các đặc điểm sau: chỉ định khả năng an toàn cho từng tập tin, thư mục; nén dữ liệu, tăng không gian lưu trữ; có thể chỉ định hạn ngạch sử dụng đĩa cho từng người dùng; có thể mã hoá các tập tin, nâng cao khả năng bảo mật.

2.6. Chọn chế độ sử dụng giấy phép:

Bạn chọn một trong hai chế độ giấy phép sau đây:

- **Per server licensing**: là lựa chọn tốt nhất trong trường hợp mạng chỉ có một Server và phục cho một số lượng Client nhất định. Khi chọn chế độ giấy phép này, chúng ta phải xác định số lượng giấy phép tại thời điểm cài đặt hệ điều hành. Số lượng giấy phép tùy thuộc vào số kết nối đồng thời của các Client đến Server. Tuy nhiên, trong quá trình sử dụng chúng ta có thể thay đổi số lượng kết nối đồng thời cho phù hợp với tình hình hiện tại của mạng.

- **Per Seat licensing**: là lựa chọn tốt nhất trong trường hợp mạng có nhiều Server. Trong chế độ giấy phép này thì mỗi Client chỉ cần một giấy phép duy nhất để truy xuất đến tất cả các Server và không giới hạn số lượng kết nối đồng thời đến Server.

2.7. Chọn phương án kết nối mạng:

2.7.1. Các giao thức kết nối mạng:

Windows 2003 mặc định chỉ cài một giao thức **TCP/IP**, còn những giao thức còn lại như **IPX**, **AppleTalk** là những tùy chọn có thể cài đặt sau nếu cần thiết. Riêng giao thức **NetBEUI**, **Windows 2003** không đưa vào trong các tùy chọn cài đặt mà chỉ cung cấp kèm theo đĩa **CD-ROM** cài đặt **Windows 2003** và được lưu trong thư mục **\VALUEADD\MSFT\NET\NETBEUI**.

2.7.2. Thành viên trong Workgroup hoặc Domain:

Nếu máy tính của bạn nằm trong một mạng nhỏ, phân tán hoặc các máy tính không được nối mạng với nhau, bạn có thể chọn cho máy tính làm thành viên của **workgroup**, đơn giản bạn chỉ cần cho biết tên **workgroup** là xong.

Nếu hệ thống mạng của bạn làm việc theo cơ chế quản lý tập trung, trên mạng đã có một vài máy **Windows 2000 Server** hoặc **Windows 2003 Server** sử dụng **Active Directory** thì bạn có thể chọn cho máy tính tham gia **domain** này. Trong trường hợp này, bạn phải cho biết tên chính xác của **domain** cùng với tài khoản (gồm có **username** và **password**) của một người dùng có quyền bổ sung thêm máy tính vào **domain**. Ví dụ như tài khoản của người quản trị mạng (**Administrator**).

3. Cài đặt Windows Server 2003:

3.1. Giai đoạn Preinstallation:

Sau khi kiểm tra và chắc chắn rằng máy của mình đã hội đủ các điều kiện để cài đặt **Windows Server 2003**, bạn phải chọn một trong các cách sau đây để bắt đầu quá trình cài đặt.

3.1.1. Cài đặt từ hệ điều hành khác:

Nếu máy tính của bạn đã có một hệ điều hành và bạn muốn nâng cấp lên **Windows 2003 Server** hoặc là bạn muốn khởi động kép, đầu tiên bạn cho máy tính khởi động bằng hệ điều hành có sẵn này, sau đó tiến hành quá trình cài đặt **Windows Server 2003.**

Tùy theo hệ điều hành đang sử dụng là gì, bạn có thể sử dụng hai lệnh sau trong thư mục **I386**:

- **WINNT32.EXE** nếu là Windows 9x hoặc Windows NT.
- **WINNT.EXE** nếu là hệ điều hành khác.

3.1.2. Cài đặt trực tiếp từ đĩa DVD Windows Server 2003:

Nếu máy tính của bạn hỗ trợ tính năng khởi động từ đĩa CD, bạn chỉ cần đặt đĩa CD vào ổ đĩa và khởi động lại máy tính. Lưu ý là bạn phải cấu hình **CMOS Setup**, chỉ định thiết bị khởi động đầu tiên là ổ đĩa **CDROM**. Khi máy tính khởi động lên thì quá trình cài đặt tự động thi hành, sau đó làm theo những hướng dẫn trên màn hình để cài đặt **Windows 2003**.

Bài tập 1: Cài đặt hệ điều hành Windows Server 2003

Trong quá trình cài đặt nên chú ý đến các thông tin hướng dẫn ở thanh trạng thái. Giai đoạn **Text-based setup** diễn ra một số bước như sau:
(1) Cấu hình **BIOS** của máy tính để có thể khởi động từ ổ đĩa **CD-ROM.**
(2) Đưa đĩa cài đặt **Windows 2003 Server** vào ổ đĩa **CD-ROM** và khởi động lại máy.
(3) Khi máy khởi động từ đĩa **CD-ROM** sẽ xuất hiện một thông báo "**Press any key to continue…**" yêu cầu nhấn một phím bất kỳ để bắt đầu quá trình cài đặt.
(4) Nếu máy có ổ đĩa **SCSI** thì phải nhấn phím F6 để chỉ Driver của ổ đĩa đó.

(5) Trình cài đặt tiến hành chép các tập tin và **driver** cần thiết cho quá trình cài đặt.
(6) Nhấn **Enter** để bắt đầu cài đặt.

(7) Nhấn phím **F8** để chấp nhận thỏa thuận bản quyền và tiếp tục quá trình cài đặt. Nếu nhấn **ESC**, thì chương trình cài đặt kết thúc.

(8) Chọn một vùng trống trên ổ đĩa và nhấn phím **C** để tạo một **Partition** mới chứa hệ điều hành.

(9) Nhập vào kích thước của **Partition** mi và nhấn **Enter.**
(10) Chọn **Partition** vừa tạo và nhấn **Enter** để tiếp tục.

(11) Chọn kiểu hệ thống tập tin (**FAT** hay **NTFS**) để định dạng cho **partition**. Nhấn **Enter** để tiếp tục.

(12) Trình cài đặt sẽ chép các tập tin của hệ điều hành vào **partition** đã chọn.

(13) Khởi động lại hệ thống để bắt đầu giai đoạn **Graphical Based**. Trong khi khởi động, không nhấn bất kỳ phím nào khi hệ thống yêu cầu "**Press any key to continue…**"

3.3. Giai đoạn Graphical-Based Setup:

(1) Bắt đầu giai đoạn **Graphical**, trình cài đặt sẽ cài **driver** cho các thiết bị mà nó tìm thấy trong hệ thống.

(2) Tại hộp thoại **Regional and Language Options**, cho phép chọn các tùy chọn liên quan đến ngôn ngữ, số đếm, đơn vị tiền tệ, định dạng ngày tháng năm,….Sau khi đã thay đổi các tùy chọn phù hợp, nhấn **Next** để tiếp tục.

(3) Tại hộp thoại **Personalize Your Software**, điền tên người sử dụng và tên tổ chức. Nhấn **Next.**

(4) Tại hộp thoại **Your Product Key**, điền vào 25 số **CD-Key** vào 5 ô trống bên dưới. Nhấn **Next.**

(5) Tại hộp thoại **Licensing Mode**, chọn chế độ bản quyền là **Per Server** hoặc **Per Seat** tùy thuộc vào tình hình thực tế của mỗi hệ thống mạng.

(6) Tại hộp thoại **Computer Name and Administrator Password**, điền vào tên của **Server** và **Password** của người quản trị (**Administrator**).

(7) Tại hộp thoại **Date and Time Settings**, thay đổi ngày, tháng, và múi giờ (**Time zone**) cho thích hợp.

(8) Tại hộp thoại **Networking Settings**, chọn **Custom settings** để thay đổi các thông số giao thức **TCP/IP**. Các thông số này có thể thay đổi lại sau khi quá trình cài đặt hoàn tất.

(9) Tại hộp thoại **Workgroup or Computer Domain**, tùy chọn gia nhập **Server** vào một W**orkgroup** hay một **Domain** có sẵn. Nếu muốn gia nhập vào **Domain** thì đánh vào tên **Domain** vào ô bên dưới.

(10) Sau khi chép đầy đủ các tập tin, quá trình cài đặt kết thúc. Bạn nhấn tổ hợp phím Ctrl-Alt-Del để đăng nhập và sử dụng Windows Server 2003.

4. Tự động hóa quá trình cài đặt:

Nếu bạn dự định cài đặt hệ điều hành **Windows 2003 Server** trên nhiều máy tính, bạn có thể đến từng máy và tự tay thực hiện quá trình cài đặt như đã hướng dẫn trong chương trước. Tuy nhiên, chắc chắn công việc này sẽ vô cùng nhàm chán và không hiệu quả. Lúc này việc tự động hoá quá trình cài đặt sẽ giúp công việc của bạn trở nên đơn giản, hiệu quả và ít tốn kém hơn.

Có nhiều phương pháp hỗ trợ việc cài đặt tự động. Chẳng hạn, bạn có thể sử dụng phương pháp dùng ảnh đĩa (**disk image**) hoặc phương pháp cài đặt không cần theo dõi (**unattended installation**) thông qua một kịch bản (**script**) hay tập tin trả lời.

4.1. Giới thiệu kịch bản cài đặt:

Kịch bản cài đặt là một tập tin văn bản có nội dung trả lời trước tất cả các câu hỏi mà trình cài đặt hỏi như: tên máy, **DVD-Key**,….Để trình cài đặt có thể đọc hiểu các nội dung trong kịch bản thì nó phải được tạo ra theo một cấu trúc được quy định trước. Để tạo ra được các kịch bản cài đặt, có thể dùng bất kỳ chương trình soạn thảo văn bản nào, chẳng hạn như **Notepad**. Tuy nhiên, kịch bản là một tập tin có cấu trúc nên trong quá trình soạn thảo có thể xảy ra các

sai sót dẫn đến quá trình tự động hóa cài đặt không diễn ra theo ý muốn. Do đó, **Microsoft** đã tạo ra một tiện ích có tên là **Setup Manager** (**setupmgr.exe**) để giúp cho việc tạo ra kịch bản cài đặt được dễ dàng hơn. Sau khi có được kịch bản, có thể sử dụng **Notepad** để thêm, sửa lại một số thông tin để sử dụng kịch bản vào quá trình cài đặt tự động hiệu quả hơn.

4.2. Tự động hóa dùng tham biến dòng lệnh:

Khi tiến hành cài đặt **Windows 2003 Server**, ngoài cách khởi động và cài trực tiếp từ đĩa **DVD-ROM**, còn có thể dùng một trong hai lệnh sau: **winnt.exe** dùng với các máy đang chạy hệ điều hành DOS, **windows 3.x** hoặc **Windows for workgroup**; **winnt32.exe** khi máy đang chạy hệ điều hành **Windows 9x**, **Windows NT** hoặc mới hơn. Hai lệnh trên được đặt trong thư mục **I386** của đĩa cài đặt. Sau đây là cú pháp cài đặt từ 2 lệnh trên:

winnt [/s:[sourcepath]] [/t:[tempdrive]] [/u:[answer_file]]
[/udf:id [,UDB_file]]

Ý nghĩa các tham số:

/s

Chỉ rỏ vị trí đặt của bộ nguồn cài đặt (thư mục I386). Đường dẫn phải là dạng đầy đủ, ví dụ: e:\i386 hoặc **\\server\i386**. Giá trị mặc định là thư mục hiện hành.

/t

Hướng chương trình cài đặt đặt thư mục tạm vào một ổ đĩa và cài **Windows** vào ổ đĩa đó. Nếu không chỉ định, trình cài đặt sẽ tự xác định.

/u

Cài đặt không cần theo dõi với một tập tin trả lời tự động (kịch bản). Nếu sử dụng **/u** thì phải sử dụng **/s.**

/udf

Chỉ định tên của **Server** và tập tin cơ sở dữ liệu chứa tên, các thông tin đặc trưng cho mỗi máy
(unattend.udf).

winnt32 [**/checkupgradeonly**] [**/s:***sourcepath*] [**/tempdrive:***drive_letter***:**]
[**/unattend**[*num*]**:**[*answer_file*]] [**/udf:***id* [,*UDB_file*]]

Ý nghĩa của các tham số:

/checkupgradeonly

Kiểm tra xem máy có tương thích để nâng cấp và cài đặt **Windows 2003 Server** hay không?

/tempdrive

Tương tự như tham số /t

/unattend

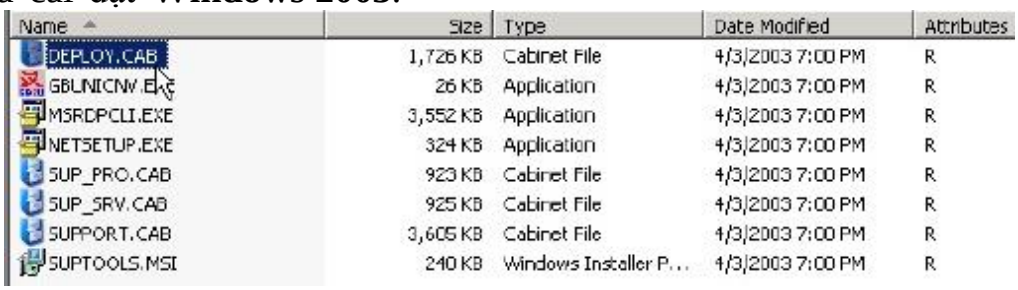
Tương tư như tham số /u

4.3. Sử dụng Setup Manager để tạo ra tập tin trả lời

Setup Manager là một tiện ích giúp cho việc tạo các tập tin trả lời sử dụng trong cài đặt không cần theo dõi. Theo mặc định, **Setup Manager** không được cài đặt, mà được đặt trong tập tin **Deploy.Cab**. Chỉ có thể chạy tiện ích **Setup Manager** trên các hệ điều hành **Windows 2000, Windows XP, Windows 2003**.

Tạo tập tin trả lời tự động bằng **Setup Manager**:

(1). Giải nén tập tin **Deploy.cab** được lưu trong thư mục **Support\Tools** trên đĩa cài đặt **Windows 2003**.



Name	Size	Type	Date Modified	Attributes
DEPLOY.CAB	1,726 KB	Cabinet File	4/3/2003 7:00 PM	R
GBUNICNV.EXE	26 KB	Application	4/3/2003 7:00 PM	R
MSRDPCLI.EXE	3,552 KB	Application	4/3/2003 7:00 PM	R
NETSETUP.EXE	324 KB	Application	4/3/2003 7:00 PM	R
SUP_PRO.CAB	923 KB	Cabinet File	4/3/2003 7:00 PM	R
SUP_SRV.CAB	925 KB	Cabinet File	4/3/2003 7:00 PM	R
SUPPORT.CAB	3,605 KB	Cabinet File	4/3/2003 7:00 PM	R
SUPTOOLS.MSI	240 KB	Windows Installer P...	4/3/2003 7:00 PM	R

(2). Thi hành tập tin **Setupmgr.exe**

(3). Hộp thoại **Setup Manager** xuất hiện, nhấn **Next** để tiếp tục.

(4). Xuất hiện hộp thoại **New or Existing Answer File**. Hộp thoại này cho phép bạn chỉ định tạo ra một tập tin trả lời mới, một tập tin trả lời phản ánh cấu hình của máy tính hiện hành hoặc là chỉnh sửa một tập tin sẵn có. Bạn chọn **Create new** và nhấn **Next**.

(5) . Tiếp theo là hộp thoại **Type of Setup**. Chọn **Unattended Setup** và chọn **Next**.

(6). Trong hộp thoại **Product**, chọn hệ điều hành cài đặt sử dụng tập tin trả lời tự động. Chọn **Windows Server 2003, Enterprise Edition**, nhấn **Next**.

(7). Tại hộp thoại **User Interaction**, chọn mức độ tương tác với trình cài đặt

của người sử dụng. Chọn **Fully Automated**, nhấn **Next**.
(8). Xuất hiện hộp thoại **Distribution Share**, chọn **Setup from a CD**, nhấn **Next**.

(9). Tại hộp thoại **License Agreement**, đánh dấu vào **I accept the terms of …**, nhấn **Next**.

(10). Tại cửa sổ **Setup Manager**, chọn mục **Name and Organization**. Điền tên và tổ chức sử dụng hệ điều hành. Nhấn **Next**.

(11). Chọn mục **Time Zone** \ chọn múi giờ (**GMT+7:00) Bangkok, Hanoi, Jarkata**. Nhấn **Next**.

(12). Tại mục **Product Key**, điền **DVD-Key** vào trong 5 ô trống. Nhấn **Next**.

(13). Tại mục **Licensing Mode**, chọn loại bản quyền thích hợp. Nhấn **Next**.

(14). Tại mục **Computer Names**, điền tên của các máy dự định cài đặt. Nhấn **Next**.

(15). Tại mục **Administrator Password**, nhập vào **password** của người quản trị. Nếu muốn mã hóa **password** thì đánh dấu chọn vào mục "**Encrypt the Administrator password…**". Nhấn **Next**

(16). Tại mục **Network Component**, cấu hình các thông số cho giao thức **TCP/IP** và cài thêm các giao thức. Nhấn **Next**.

(17). Tại mục **Workgroup or Domain**, gia nhập máy vào **Workgroup** hoặc **Domain** có sẵn. Nhấn **Next**.

(18). Cuối cùng, trong thư mục đã chỉ định, **Setup Manager** sẽ tạo ra ba tập tin. Nếu bạn không thay đổi tên thì các tập tin là:
Unattend.txt: đây là tập tin trả lời, chứa tất cả các câu trả lời mà **Setup Manager** thu thập được.
Unattend.udb: đây là tập tin cơ sở dữ liệu chứa tên các máy tính sẽ được cài đặt. Tập tin này chỉ được tạo ra khi bạn chỉ định danh sách các tập tin và được sử dụng khi bạn thực hiện cài đặt không cần theo dõi.
Unattend.bat: chứa dòng lệnh với các tham số được thiết lập sẵn. Tập tin này cũng thiết lập các biến môi trường chỉ định vị trí các tập tin liên quan.

4.4. Sử dụng tập tin trả lời:

Có nhiều cách để sử dụng các tập tin được tạo ra trong bước trên. Bạn có thể thực hiện theo một trong hai cách dưới đây:

4.4.1. Sử dụng đĩa CD Windows 2003 Server có thể khởi động được:

Sửa tập tin Unattend.txt thành WINNT.SIF và lưu lên đĩa mềm.
Đưa đĩa CD Windows 2003 Server và đĩa mềm trên vào ổ đĩa, khởi động lại máy tính, đảm bảo ổ đĩa CD là thiết bị khởi động đầu tiên. Chương trình cài đặt trên đĩa CD sẽ tự động tìm đọc tập tin WINNT.SIF trên đĩa mềm và tiến hành cài đặt không cần theo dõi.

4.4.2. Sử dụng một bộ nguồn cài đặt Windows 2003 Server

Chép các tập tin đã tạo trong bước trên vào thư mục **I386** của nguồn cài đặt **Windows 2003 Server**. Chuyển vào thư mục **I386**.
Tuỳ theo hệ điều hành đang sử dụng mà sử dụng lệnh **WINNT.EXE** hoặc **WINNT32.EXE** theo cú pháp sau:

WINNT /s:e:\i386 /u:unattend.txt

Hoặc

WINNT32 /s:e:\i386 /unattend:unattend.txt

Nếu chương trình **Setup Manager** tạo ra tập tin **Unatend.UDB** do bạn đã nhập vào danh sách tên các máy tính, và giả định bạn định đặt tên máy tính này là **server01** thì cú pháp lệnh sẽ như sau:
WINNT /s:e:\i386 /u:unattend.txt /udf:server01,unattend.udf

Chương 2: Managing User and Computer Accounts

Bài 2: DỊCH VỤ TÊN MIỀN (DNS)

Mục tiêu:

- Trình bày được cấu trúc cơ sở dữ liệu của hệ thống tên miền;
- Mô tả được sự hoạt động và phân cấp của hệ thống tên miền;
- Cài đặt và cấu hình hệ thống tên miền DNS.
- Thực hiện các thao tác an toàn với máy tính.

1. Tổng quan về DNS:

1.1. Giới thiệu DNS:

Mỗi máy tính trong mạng muốn liên lạc hay trao đổi thông tin, dữ liệu cho nhau cần phải biết rõ địa chỉ IP của nhau. Nếu số lượng máy tính nhiều thì việc nhớ những địa chỉ IP này rất là khó khăn. Vì vậy, **DNS (Domain Name System)** là giải pháp dùng tên thay cho địa chỉ IP khó nhớ khi sử dụng các dịch vụ trên mạng. Vì thế, người ta nghĩ ra cách làm sao ánh xạ địa chỉ IP thành tên máy tính.

Ban đầu do quy mô mạng ARPanet (tiền thân của mạng Internet) còn nhỏ chỉ vài trăm máy, nên chỉ có một tập tin đơn HOSTS.TXT lưu thông tin về ánh xạ tên máy thành địa chỉ IP. Trong đó tên máy chỉ là 1 chuỗi văn bản không phân cấp (flat name). Tập tin này được duy trì tại 1 máy chủ và các máy chủ khác lưu giữ bản sao của nó. Tuy nhiên khi quy mô mạng lớn hơn, việc sử dụng tập tin HOSTS.TXT có các nhược điểm như sau:

- Lưu lượng mạng và máy chủ duy trì tập tin HOSTS.TXT bị quá tải do hiệu ứng "cổ chai".
- Xung đột tên: Không thể có 2 máy tính có cùng tên trong tập tin HOSTS.TXT. Tuy nhiên do tên máy không phân cấp và không có gì đảm bảo để ngăn chặn việc tạo 2 tên trùng nhau vì không có cơ chế uỷ quyền quản lý tập tin nên có nguy cơ bị xung đột tên.
- Không đảm bảo sự toàn vẹn: việc duy trì 1 tập tin trên mạng lớn rất khó khăn. Ví dụ như khi tập tin HOSTS.TXT vừa cập nhật chưa kịp chuyển đến máy chủ ở xa thì đã có sự thay đổi địa chỉ trên mạng rồi.

Tóm lại việc dùng tập tin HOSTS.TXT không phù hợp cho mạng lớn vì thiếu cơ chế phân tán và mở rộng. Do đó, dịch vụ DNS ra đời nhằm khắc phục các nhược điểm này. Người thiết kế cấu trúc của dịch vụ DNS là Paul Mockapetris - USC's Information Sciences Institute, và các khuyến nghị RFC của DNS là RFC 882 và 883, sau đó là RFC 1034 và 1035 cùng với 1 số RFC bổ sung như bảo mật trên hệ thống DNS, cập nhật động các bản ghi DNS …

Lưu ý: Hiện tại trên các máy chủ vẫn sử dụng được tập tin hosts.txt để phân giải tên máy tính thành địa chỉ IP (trong Windows tập tin này nằm trong thư mục WINDOWS\system32\drivers\etc)

Dịch vụ DNS hoạt động theo mô hình Client-Server: phần Server gọi là máy chủ phục vụ tên hay còn gọi là Name Server, còn phần Client là trình phân giải tên - Resolver. Name Server chứa các thông tin CSDL của DNS, còn Resolver đơn giản chỉ là các hàm thư viện dùng để tạo các truy vấn (query) và gửi chúng qua đến Name Server. DNS được thi hành như một giao thức tầng Application

trong mạng TCP/IP.

DNS là 1 CSDL phân tán. Điều này cho phép người quản trị cục bộ quản lý phần dữ liệu nội bộ thuộc phạm vi của họ, đồng thời dữ liệu này cũng dễ dàng truy cập được trên toàn bộ hệ thống mạng theo mô hình **Client-Server**. Hiệu suất sử dụng dịch vụ được tăng cường thông qua cơ chế nhân bản (**replication**) và lưu tạm (**caching**). Một **hostname** trong domain là sự kết hợp giữa những từ phân cách nhau bởi dấu chấm(.).

Sơ đồ tổ chức DNS

Cấu trúc của một tên miền

− Domain sẽ có dạng : lable.lable.label...lable
− Độ dài tối đa của một tên miền là 255 ký tự
− Mỗi một Lable tối đa là 63 ký tự
− Lable phải bắt đầu bằng chữ hoặc số và chỉ được phép chứa chữ, số, dấu trừ(-), dấu chấm (.) mà không được chứa các ký tự khác.

Loại tên	**Miêu tả**	**Ví dụ**
Gốc (domain root)	Nó là đỉnh của nhánh cây của tên miền. Nó xác định kết thúc của domain (fully qualified domain names FQDNs).	Đơn giản nó chỉ là dấu chấm (**.**) sử dụng tại cuối của tên ví như "www.microsoft.com."
Tên miền cấp 1 (Top-level domain)	Là hai hoặc ba ký tự xác định nước/khu vực hoặc các tổ chức	".com", xác định tên sử dụng trong xác định là tổ chức thương mại .
Tên miền cấp 2 (Second-level domain)	Nó rất đa dạng trên internet, nó có thể là tên của một công ty, một tổ chức hay một cá nhân .v.v. đăng ký trên internet.	"microsoft.com.", là tên miền cấp hai đăng ký là công ty Microsoft.
Tên miền cấp nhỏ hơn	Chia nhỏ thêm ra của tên miên cấp hai xuống thường được sử dụng như chi "example.microsoft.com." là phần quản lý tài liệu ví dụ của microsof (Subdomain) nhánh, phòng ban của một cơ quan hay một chủ đề nào đó.	

Cơ sở dữ liệu(CSDL) của **DNS** là một cây đảo ngược. Mỗi nút trên cây cũng lại là gốc của 1 cây con. Mỗi cây con là 1 phân vùng con trong toàn bộ CSDL **DNS** gọi là 1 miền (**domain**). Mỗi domain có thể phân chia thành các phân vùng con nhỏ hơn gọi là các miền con (**subdomain**).

Mỗi **domain** có 1 tên (**domain name**). Tên **domain** chỉ ra vị trí của nó trong CSDL **DNS**. Trong **DNS** tên miền là chuỗi tuần tự các tên nhãn tại nút đó đi ngược lên nút gốc của cây và phân cách nhau bởi dấu chấm.

Tên nhãn bên phải trong mỗi **domain name** được gọi là **top-level**

domain. Trong ví dụ trước srv1.csc.hcmuns.edu.vn, vậy miền ".vn" là **top-level domain**. Bảng sau đây liệt kê **top-level domain**.

Tên miền	Mô tả
.com	Các tổ chức, công ty thương mại
.org	Các tổ chức phi lợi nhuận
.net	Các trung tâm hỗ trợ về mạng
.edu	Các tổ chức giáo dục
.gov	Các tổ chức thuộc chính phủ
.mil	Các tổ chức quân sự
.int	Các tổ chức được thành lập bởi các hiệp ước quốc tế

Bên cạnh đó, mỗi nước cũng có một **top-level domain**. Ví dụ **top-leveldomain** của Việt Nam là .vn, Mỹ là .us, ta cóthể tham khảo thêm thông tin địa chỉ tên miền tại địa chỉ: **http://www.thrall.org/domains.htm**

Tên miền quốc gia	Tên quốc gia
.vn	Việt Nam
.us	Mỹ
.uk	Anh
.jp	Nhật Bản
.ru	Nga
.cn	Trung Quốc

1.2. Đặc điểm của DNS trong Windows Server:

- **Conditional forwarder**: Cho phép **Name Server** chuyển các yêu cầu phân giải dựa theo tên domain trong yêu cầu truy vấn.
- **Stub zone**: hỗ trợ cơ chế phân giải hiệu quả hơn.
- Đồng bộ các **DNS zone** trong **Active Directory** (**DNS zone replication in Active Directory**).
- Cung cấp một số cơ chế bảo mật tốt hơn trong các hệ thống **Windows** trước đây.
- Luân chuyển (**Round robin**) tất cả các loại **RR**.
- Cung cấp nhiều cơ chế ghi nhận và theo dõi sự cố lỗi trên **DNS**.
- Hỗ trợ giao thức **DNS Security Extensions** (**DNSSEC**) để cung cấp các tính năng bảo mật cho việc lưu trữ và nhân bản (**replicate**) **zone**.
- Cung cấp tính năng **EDNS0** (**Extension Mechanisms for DNS**) để cho phép **DNS Requestor** quản bá những **zone transfer packet** có kích thước lớn hơn 512 byte.

2. Cách phân bố dữ liệu quản lý trên tên miền:

Những **root name server** (.) quản lý những **top-level domain** trên **Internet.** Tên máy và địa chỉ **IP** của những **name server** này được công bố cho mọi người biết và chúng được liệt kê trong bảng sau. Những **name server** này cũng có thể đặt khắp nơi trên thế giới.

Tên máy tính	Địa chỉ IP
H.ROOT-SERVERS.NET	128.63.2.53
B.ROOT-SERVERS.NET	128.9.0.107
C.ROOT-SERVERS.NET	192.33.4.12
D.ROOT-SERVERS.NET	128.8.10.90
E.ROOT-SERVERS.NET	192.203.230.10
I.ROOT-SERVERS.NET	192.36.148.17
F.ROOT-SERVERS.NET	192.5.5.241
F.ROOT-SERVERS.NET	39.13.229.241
G.ROOT-SERVERS.NET	192.112.88.4
A.ROOT-SERVERS.NET	198.41.0.4

Thông thường một tổ chức được đăng ký một hay nhiều domain name. Sau đó, mỗi tổ chức sẽ cài đặt một hay nhiều name server và duy trì cơ sở dữ liệu cho tất cả những máy tính trong domain. Những name server của tổ chức được đăng ký trên Internet. Một trong những name server này được biết như là Primary Name Server. Nhiều Secondary Name Server được dùng để làm backup cho Primary Name Server. Trong trường hợp Primary bị lỗi, Secondary được sử dụng để phân giải tên.

Primary Name Server có thể tạo ra những subdomain và ủy quyền những subdomain này cho những Name Server khác.

3. Hoạt động của hệ thống DNS:

Truy vấn DNS và trả lời của hệ thống DNS cho client sử dụng thủ tục UDP cổng 53, UPD hoạt động ở mức thứ 3 (network) của mô hình OSI, UDP là thủ tục phi kết nối (connectionless), tương tự như dịch vụ gửi thư bình thường bạn cho thư vào thùng thư và hy vọng có thể chuyển đến nơi bạn cần gửi tới.

Mỗi một message truy vấn được gửi đi từ client bao gồm ba phần thông tin :

- Tên của miền cần truy vấn (tên đầy đủ FQDN)
- Xác định loại bản ghi là mail, web ...
- Lớp tên miền (phần này thường được xác định là IN internet, ở đây không đi sâu vào phần này)

Ví dụ : tên miền truy vấn đầy đủ như "hostname.example.microsoft.com.", và loại truy vấn là địa chỉ A. Client truy vấn DNS hỏi "Có bản ghi địa chỉ A cho máy

tính có tên là "hostname.example.microsoft.com" khi client nhận được câu trả lời của DNS server nó sẽ xác định địa chỉ IP của bản ghi A.

Có một số giải pháp để trả lời các truy vấn DNS. Client có thể tự trả lời bằng cách sử dụng các thông tin đã được lưu trữ trong bộ nhớ cache của nó từ những truy vấn trước đó. DNS server có thể sử dụng các thông tin được lưu trữ trong cache của nó để trả lời hoặc dns server có thể hỏi một dns server khác lấy thông tin đó để trả lời lại client.

Nói chung các bước của một truy vấn gồm có hai phần như sau:

• Truy vấn sẽ bắt đầu ngay tại client computer để xác định câu trả lời

• Khi ngay tại client không có câu trả lời, câu hỏi sẽ được chuyển đến DNS server để tìm câu trả lời.

3.1. Tự tìm câu trả lời truy vấn:

Bước đầu tiên của quá trình sử lý một truy vấn. Tên miền sử dụng một chương trình trên ngay máy tính truy vấn để tìm câu trả lời cho truy vấn. Nếu truy vấn có câu trả lời thì quá trình truy vấn kết thúc

Ngay tại máy tính truy vấn thông tin được lấy từ hai nguồn sau:

• Trong file HOSTS được cấu hình ngay tại máy tính. Các thông tin ánh xạ từ tên miền sang địa chỉ được thiết lập ở file này được sử dụng đầu tiên. Nó được tải ngay lên bộ nhớ cache của máy khi bắt đầu chạy dns client.

• Thông tin được lấy từ các câu trả lời của truy vấn trước đó. Theo thời gian các câu trả lời truy vấn được lưu giữ trong bộ nhớ cache của máy tính và nó được sử dụng khi có một truy vấn lặp lại một tên miền trước đó.

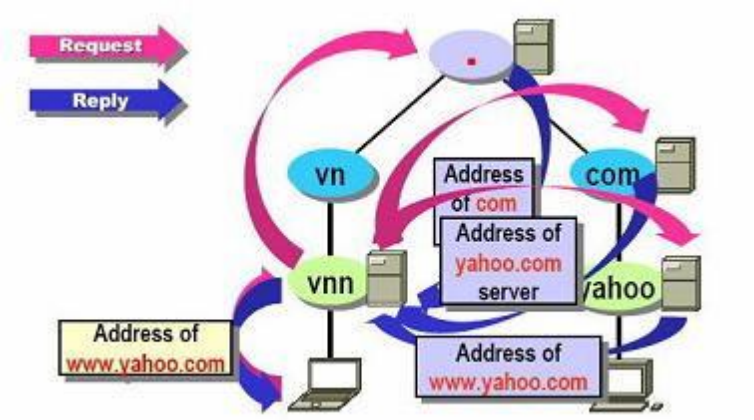
3.2. Truy vấn DNS server:

Khi DNS server nhận được một truy vấn. Đầu tiên nó sẽ kiểm tra câu trả lời liệu có phải là thông tin của bản ghi mà nó quản lý trong các zone của server. Nếu truy vấn phù hợp với bản ghi mà nó quản lý thì nó sẽ sử dụng thông tin đó để trả lời trả lời (authoritatively answer) và kết thúc truy vấn.

Nếu không có thông tin về zone của nó phù hợp với truy vấn. Nó sẽ kiểm tra các thông tin được lưu trong cache liệu có các truy vấn tương tư nào trước đó phù hợp không nếu có thông tin phù hợp nó sẽ sử dụng thông tin đó để trả lời và kết thúc truy vấn.

Nếu truy vấn không tìm thấy thông tin phù hợp để trả lời từ cả cache và zone mà DNS server quản lý thì truy vấn sẽ tiếp tục. Nó sẽ nhờ DNS server khác để trả lời truy vấn đến khi tìm được câu trả lời.

Ví dụ hoạt động của DNS:



Giả sử PC A muốn truy cập đến trang web www.yahoo.com và server vnn chưa lưu thông tin về trang web này, các bước truy vấn sẽ diễn ra như sau:

- Đầu tiên PC A gửi một request hỏi server quản lý tên miền vnn hỏi thông tin về www.yahoo.com. Server quản lý tên miền vnn gửi một truy vấn đến server top level domain.
- Top level domain lưu trữ thông tin về mọi tên miền trên mạng. Do đó nó sẽ gửi lại cho server quản lý tên miền vnn địa chỉ IP của server quản lý miền com (gọi tắt server com).
- Khi có địa chỉ IP của server quản lý tên miền com thì lập tức server vnn hỏi server com thông tin về yahoo.com. Server com quản lý toàn bộ những trang web có domain là com, chúng gửi thông tin về địa chỉ IP của server yahoo.com cho server vnn.
- Lúc này server vnn đã có địa chỉ IP của yahoo.com rồi. Nhưng PC A yêu cầu dịch vụ www chứ không phải là dịch vụ ftp hay một dịch vụ nào khác. Do đó server vnn tiếp tục truy vấn tới server yahoo.com để yêu cầu thông tin về server quản lý dịch vụ www của yahoo.com.
- Lẽ đương nhiên khi nhận được truy vấn thì server yahoo.com gửi lại cho server vnn địa chỉ IP của server quản lý www.yahoo.com.
- Cuối cùng là server vnn gửi lại địa chỉ IP của server quản lý www.yahoo.com. cho PC A và PC A kết nối trực tiếp đến nó. Và bây giờ thì server vnn đã có thông tin về www.yahoo.com cho những lần truy vấn đến sau của các client khác.

4. Một số khái niệm cơ bản:

4.1. Domain name và zone:

Một miền gồm nhiều thực thể nhỏ hơn gọi là miền con (**subdomain**). Ví dụ, miền **ca** bao gồm nhiều miền con như **ab.ca, on.ca, qc.ca,..** . Bạn có thể ủy quyền một số miền con cho những **DNS Server** khác quản lý. Những miền và miền con mà **DNS Server** được quyền quản lý gọi là **zone**. Như vậy, một **Zone** có thể gồm một miền, một hay nhiều miền con.

Các loại **zone**:

- **Primary zone**: Cho phép đọc và ghi cơ sở dữ liệu.
- **Secondary zone**: Cho phép đọc bản sao cơ sở dữ liệu.

- **Stub zone**: chứa bản sao cơ sở dữ liệu của **zone** nào đó, nó chỉ chứa chỉ một vài **RR(Resource Record)**.

4.2. Fully Qualified Domain Name (FQDN):

Mỗi nút trên cây có một tên gọi(không chứa dấu chấm) dài tối đa 63 ký tự. Tên rỗng dành riêng cho gốc (**root**) cao nhất và biểu diễn bởi dấu chấm. Một tên miền đầy đủ của một nút chính là chuỗi tuần tự các tên gọi của nút hiện tại đi ngược lên nút gốc, mỗi tên gọi cách nhau bởi dấu chấm. Tên miền có xuất hiện dấu chấm sau cùng được gọi là tên tuyệt đối (**absolute**) khác với tên tương đối là tên không kết thúc bằng dấu chấm. Tên tuyệt đối cũng được xem là tên miền đầy đủ đã được chứng nhận (**Fully Qualified Domain Name – FQDN**).

4.3. Sự ủy quyền (Delegation):

Một trong các mục tiêu khi thiết kế hệ thống DNS là khả năng quản lý phân tán thông qua cơ chế uỷ quyền (delegation). Trong một miền có thể tổ chức thành nhiều miền con, mỗi miền con có thể được uỷ quyền cho một tổ chức khác và tổ chức đó chịu trách nhiệm duy trì thông tin trong miền con này. Khi đó, miền cha chỉ cần một con trỏ trỏ đến miền con này để tham chiếu khi có các truy vấn.

Không phải một miền luôn luôn tổ chức miền con và uỷ quyền toàn bộ cho các miền con này, có thể chỉ có vài miền con được ủy quyền.

4.4. Forwarders:

Là kỹ thuật cho phép Name Server nội bộ chuyển yêu cầu truy vấn cho các Name Server khác để phân giải các miền bên ngoài.

4.5. Stub zone:

Là zone chứa bảng sao cơ sở dữ liệu DNS từ master name server, Stub zone chỉ chứa các resource record cần thiết như : A, SOA, NS, một hoặc vài địa chỉ của master name server hỗ trợ cơ chế cập nhật Stub zone, chế chứng thực name server trong zone và cung cấp cơ chế phân giải tên miền được hiệu quả hơn, đơn giản hóa công tác quản trị.

4.6. Dynamic DNS:

Dynamic DNS là phương thức ánh xạ tên miền tới địa chỉ IP có tần xuất thay đổi cao. Dịch vụ DNS động (Dynamic DNS) cung cấp một chương trình đặc biệt chạy trên máy tính của người sử dụng dịch vụ dynamic DNS gọi là Dynamic Dns Client. Chương trình này giám sát sự thay đổi địa chỉ IP tại host và liên hệ với hệ thống DNS mỗi khi địa chỉ IP của host thay đổi và sau đó update thông tin vào cơ sở dữ liệu DNS về sự thay đổi địa chỉ đó.

4.7. Active Directory-integrated zone:

Sử dụng Active Directory-integrated zone có một số thuận lợi sau:

- DNS zone lưu trữ trong trong Active Directory, nhờ cơ chế này mà dữ liệu được bảo mật hơn.
- Sử dụng cơ chế nhân bản của Active Directory để cập nhận và sao chép cơ sở dữ liệu DNS.
- Sử dụng secure dynamic update.
- Sử dụng nhiều master name server để quản lý tên miền thay vì sử dụng một master name server.

5. Phân loại Domain Name Server:

5.1. Primary Name Server:

Mỗi miền phải có một Primary Name Server. Server này được đăng kí trên Internet để quản lý miền. Mọi người trên Internet đều biết tên máy tình và địa chỉ IP của Server này. Người quản trị DNS sẽ tổ chức những tập tin CSDL trên Primary Name Server. Server này có nhiệm vụ phân giải tất cả các máy trong miền hay zone.

5.2. Secondary Name Server:

Mỗi miền có một Primary Name Server để quản lý CSDL của miền. Nếu như Server này tạm ngưng hoạt động vì một lý do nào đó thì việc phân giải tên máy tính thành địa chỉ IP và ngược lại xem như bị gián đoạn. Việc gián đoạn này làm ảnh hưởng rất lớn đến những tổ chức có nhu cầu trao đổi thông tin ra ngoài Internet cao. Nhằm khắc phục nhược điểm này, những nhà thiết kế đã đưa ra một Server dự phòng gọi là Secondary(hay Slave) Name Server. Server này có nhiệm vụ sao lưu tất cả những dữ liệu trên Primary Name Server và khi Primary Name Server bị gián đoạn thì nó sẽ đảm nhận việc phân giải tên máy tính thành địa chỉ IP và ngược lại. Trong một miền có thể có một hay nhiều Secondary Name Server. Theo một chu kỳ, Secondary sẽ sao chép và cập nhật CSDL từ Primary Name Server. Tên và địa chỉ IP của Secondary Name Server cũng được mọi người trên Internet biết đến.

5.3. Caching Name Server:

Caching Name Server không có bất kỳ tập tin CSDL nào. Nó có chức năng phân giải tên máy trên những mạng ở xa thông qua những Name Server khác. Nó lưu giữ lại những tên máy đã được phân giải trước đó và được sử dụng lại những thông tin này nhằm mục đích:

- Làm tăng tốc độ phân giải bằng cách sử dụng cache.
- Giảm bớt gánh nặng phân giải tên máy cho các Name Server.
- Giảm việc lưu thông trên những mạng lớn.

6. Resource Record (RR):

RR là mẫu thông tin dùng để mô tả các thông tin về cơ sở dữ liệu DNS, các mẫu tin này được lưu trong các file cơ sở dữ liệu DNS (\systemroot\system32\dns).

6.1. SOA(Start of Authority):

Trong mỗi tập tin CSDL phải có một và chỉ một record SOA (start of authority). Record SOA chỉ ra rằng máy chủ Name Server là nơi cung cấp thông tin tin cậy từ dữ liệu có trong zone.

Cú pháp của record SOA.

[tên-miền] IN SOA [tên-server-dns] [địa-chỉ-email] (
serial number;
refresh number;
retry number;
experi number;
Time-to-live number)

- Serial : Áp dụng cho mọi dữ liệu trong zone và là 1 số nguyên. Trong ví dụ, giá trị này bắt đầu từ 1 nhưng thông thường người ta sử dụng theo định dạng thời gian như 2012032501. Định dạng này theo kiểu YYYYMMDDNN, trong đó YYYY là năm, MM là tháng, DD là ngày và NN số lần sửa đổi dữ liệu zone trong ngày. Bất kể là theo định dạng nào, luôn luôn phải tăng số này lên mỗi lần sửa đổi dữ liệu zone. Khi máy máy chủ Secondary liên lạc với máy chủ Primary, trước tiên nó sẽ hỏi số serial. Nếu số serial của máy Secondary nhỏ hơn số serial của máy Primary tức là dữ liệu zone trên Secondary đã cũ và sau đó máy Secondary sẽ sao chép dữ liệu mới từ máy Primary thay cho dữ liệu đang có hiện hành.
- Refresh: Chỉ ra khoảng thời gian máy chủ Secondary kiểm tra dữ liệu zone trên máy Primary để cập nhật nếu cần. Trong ví dụ trên thì cứ mỗi 3 giờ máy chủ Secondary sẽ liên lạc với máy chủ Primary để cập nhật dữ liệu nếu có. Giá trị này thay đổi tuỳ theo tần suất thay đổi dữ liệu trong zone.
- Retry: nếu máy chủ Secondary không kết nối được với máy chủ Primary theo thời hạn mô tả trong refresh (ví dụ máy chủ Primary bị shutdown vào lúc đó thì máy chủ Secondary phải tìm cách kết nối lại với máy chủ Primary theo một chu kỳ thời gian mô tả trong retry. Thông thường giá trị này nhỏ hơn giá trị refresh.
- Expire: Nếu sau khoảng thời gian này mà máy chủ Secondary không kết nối được với máy chủ Primary thì dữ liệu zone trên máy Secondary sẽ bị quá hạn. Một khi dữ liệu trên Secondary bị quá hạn thì máy chủ này sẽ không trả lời mọi truy vấn về zone này nữa. Giá trị expire này phải lớn hơn giá trị refresh và giá trị retry.
- TTL: Viết tắt của time to live. Giá trị này áp dụng cho mọi record trong zone và được đính kèm trong thông tin trả lời một truy vấn. Mục đích của nó là chỉ ra thời gian mà các máy chủ Name Server khác cache lại thông tin trả lời. Việc cache thông tin trả lời giúp giảm lưu lượng truy vấn DNS trên mạng.

6.2. NS (Name Server)

Record tiếp theo cần có trong zone là NS (name server) record. Mỗi Name Server cho zone sẽ có một NS record.

Cú pháp:

[domain_name] IN NS [DNS-Server_name]

Ví dụ: Record NS sau:

qtm.com. IN NS dnsserver.qtm.com.

qtm.com. IN NS server.qtm.com.

chỉ ra 2 name servers cho miền qtm.com

6.3. A (Address) và CNAME (Canonical Name)

Record A (Address) ánh xạ tên máy (hostname) vào địa chỉ IP. Record CNAME (canonical name) tạo tên bí danh alias trỏ vào một tên canonical. Tên canonical là tên host trong record A hoặc lại trỏ vào 1 tên canonical khác.

Cú pháp record A:

[tên-máy-tính] IN A [địa-chỉ-IP]

Ví dụ: record A trong tập tin db.qtm

server.qtm.com. IN A 172.29.14.1

diehard.qtm.com. IN A 172.29.14.4

// Multi-homed hosts

server.qtm.com. IN A172.29.14.1

server.qtm.com. IN A192.253.253.1

6.4. AAAA

Ánh xạ tên máy (hostname) vào địa chỉ IP version 6

Cú pháp:

[tên-máy-tính] IN AAAA [địa-chỉ-IPv6]

Ví dụ

Server IN AAAA 1243:123:456:789:1:2:3:456ab

6.5. SRV:

Cung cấp cơ chế định vị dịch vụ, Active Directory sử dụng Resource Record này để xác định domain controllers, global catalog servers, Lightweight Directory Access Protocol (LDAP) servers.

Các field trong SVR:

- Tên dịch vụ service.
- Giao thức sử dụng.
- Tên miền (domain name).
- TTL và class.
- Priority.
- Weight (hỗ trợ load balancing).
- Port của dịch vụ.
- Target chỉ định FQDN cho host hỗ trợ dịch vụ.

6.6. MX (Mail Exchange):

DNS dùng record MX trong việc chuyển mail trên mạng Internet. Ban đầu chức năng chuyển mail dựa trên 2 record: record MD (mail destination) và record

MF (mail forwarder) records. MD chỉ ra đích cuối cùng của một thông điệp mail có tên miền cụ thể. MF chỉ ra máy chủ trung gian sẽ chuyển tiếp mail đến được máy chủ đích cuối cùng. Tuy nhiên, việc tổ chức này hoạt động không tốt. Do đó, chúng được tích hợp lại thành một record là MX. Khi nhận được mail, trình chuyển mail (mailer) sẽ dựa vào record MX để quyết định đường đi của mail. Record MX chỉ ra một mail exchanger cho một miền - mail exchanger là một máy chủ xử lý (chuyển mail đến mailbox cục bộ hay làm gateway chuyển sang một giao thức chuyển mail khác như UUCP) hoặc chuyển tiếp mail đến một mail exchanger khác (trung gian) gần với mình nhất để đến tới máy chủ đích cuối cùng hơn dùng giao thức SMTP (Simple Mail Transfer Protocol).

Để tránh việc gửi mail bị lặp lại, record MX có thêm 1 giá trị bổ sung ngoài tên miền của mail exchanger là 1 số thứ tự tham chiếu. Đây là giá trị nguyên không dấu 16-bit (0-65535) chỉ ra thứ tự ưu tiên của các mail exchanger.

Cú pháp record MX:

[domain_name] IN MX [priority] [mail-host]

Ví dụ record MX sau :

qtm.com. IN MX 10 mailserver.qtm.com.

Chỉ ra máy chủ mailserver.qtm.com là một mail exchanger cho miền qtm.com với số thứ tự tham chiếu 10.

Chú ý: các giá trị này chỉ có ý nghĩa so sánh với nhau. Ví dụ khai báo 2 record MX:

qtm.com. IN MX 1 listo.qtm.com. qtm.com. IN MX 2 hep.qtm.com.

Trình chuyển thư mailer sẽ thử phân phát thư đến mail exchanger có số thứ tự tham chiếu nhỏ nhất trước. Nếu không chuyển thư được thì mail exchanger với giá trị kế sau sẽ được chọn. Trong trường hợp có nhiều mail exchanger có cùng số tham chiếu thì mailer sẽ chọn ngẫu nhiên giữa chúng.

6.7. PTR (Pointer):

Record PTR (pointer) dùng để ánh xạ địa chỉ IP thành Hostname.

Cú pháp:

[Host-ID.{Reverse_Lookup_Zone}] IN PTR [tên-máy-tính]

Ví dụ:

Các record PTR cho các host trong mạng 192.249.249:

1.14.29.172.in-addr.arpa. IN PTR server.qtm.com.

7. Cài đặt và cấu hình DNS:

Có nhiều cách cài đặt dịch vụ **DNS** trên môi trường **Windows** như: Ta có thể cài đặt **DNS** khi ta nâng cấp máy chủ lên **domain controllers** hoặc cài đặt

DNS trên máy **stand-alone Windows 2003 Server.**

7.1. Các bước cài đặt dịch vụ DNS:

Khi cài đặt dịch vụ DNS trên Windows 2003 Server đòi hỏi máy này phải được cung cấp địa chỉ IP tĩnh, sau đây là một số bước cơ bản nhất để cài đặt dịch vụ DNS trên Windows 2003 stand-alone Server.

- Chọn **Start | Control Panel | Add/Remove Programs.**
- Chọn **Add or Remove Windows Components** trong hộp thoại **Windows components.**
- Từ hộp thoại ở bước 2 ta chọn **Network Services** sau đó chọn nút **Details**
- Chọn tùy chọn Domain Name System(DNS), sau đó chọn nút OK
- Chọn Next sau đó hệ thống sẽ chép các tập tin cần thiết để cài đặt dịch vụ (bạn phải đảm bảo có đĩa DVDROM Windows 2003 trên máy cục bộ hoặc có thể truy xuất tài nguyên này từ mạng). Chọn nút Finish để hoàn tất quá trình cài đặt.

7.2. Cấu hình dịch vụ DNS:

Sau khi ta cài đặt thành công dịch vụ DNS, ta có thể tham khảo trình quản lý dịch vụ này như sau:

- Ta chọn Start | Programs | Administrative Tools | DNS. Nếu ta không cài DNS cùng với quá trình cài đặt Active Directory thì không có zone nào được cấu hình mặc định.
- Event Viewer: Đây trình theo dõi sự kiện nhật ký dịch vụ DNS, nó sẽ lưu trữ các thông tin về: cảnh giác (alert), cảnh báo (warnings), lỗi (errors).
- Forward Lookup Zones: Chứa tất cả các zone thuận của dịch vụ DNS, zone này được lưu tại máy DNS Server.
- Reverse Lookup Zones: Chứa tất cả các zone nghịch của dịch vụ DNS, zone này được lưu tại máy DNS Server.

7.2.1. Tạo Forward Lookup Zones:

Forward Lookup Zone để phân giải địa chỉ Tên máy (hostname) thành địa chỉ IP. Để tạo zone này ta thực hiện các bước sau:

- Chọn nút Start | Administrative Tools | DNS.
- Chọn tên DNS server, sau đó Click chuột phải chọn New Zone. Chọn Next trên hộp thoại Welcome to New Zone Wizard.
- Chọn Zone Type là Primary Zone | Next.
- Chọn Forward Lookup Zone | Next
- Chỉ định Zone Name để khai báo tên Zone (Ví dụ: csc.com), chọn Next.

- Từ hộp thoại Zone File, ta có thể tạo file lưu trữ cơ sở dữ liệu cho Zone(zonename.dns) hay ta có thể chỉ định Zone File đã tồn tại sẵn (tất cả các file này được lưu trữ tại %systemroot%\system32\dns), tiếp tục chọn Next.
- Hộp thoại Dynamic Update để chỉ định zone chấp nhận Secure Update, nonsecure Update hay chọn không sử dụng Dynamic Update, chọn Next.

- Chọn Finish để hoàn tất.

7.2.2. Tạo Reverse Lookup Zone:

Sau khi ta hoàn tất quá trình tạo Zone thuận ta sẽ tạo Zone nghịch (Reverse Lookup Zone) để hỗ trợ cơ chế phân giải địa chỉ IP thành tên máy(hostname).

- Để tạo Reverse Lookup Zone ta thực hiện trình tự các bước sau: Chọn Start | Programs | Administrative Tools | DNS. Chọn tên của DNS server, Click chuột phải chọn New Zone
- Chọn Next trên hộp thoại Welcome to New Zone Wizard. Chọn Zone Type là Primary Zone | Next. Chọn Reverse Lookup Zone | Next.
- Gõ phần địa chỉ mạng(NetID) của địa chỉ IP trên Name Server | Next.

- Tạo mới hay sử dụng tập tin lưu trữ cơ sở dữ liệu cho zone ngược, sau đó chọn Next.

- Hộp thoại Dynamic Update để chỉ định zone chấp nhận Secure Update, nonsecure Update hãy chọn sử dụng Dynamic Update, chọn Next. Chọn Finish để hoàn tất.

7.2.3. Tạo Resource Record (RR):

Sau khi ta tạo **zone** thuận và **zone** nghịch, mặc định hệ thống sẽ tạo ra hai **resource record NS** và **SOA**.

- Tạo **RR A**:

Để tạo **RR A** để ánh xạ **hostname** thành tên máy, để làm việc này ta Click chuột **Forward Lookup Zone**, sau đó Click chuột phải vào tên **Zone | New Host,** sau đó ta cung cấp một số thông tin về **Name**, **Ip address,** sau đó chọn **Add Host.**
Chọn **Create associated pointer (PTR) record** để tạo **RR PTR** trong **zone** nghịch (trong hình ví dụ ta tạo **hostname** là **server** có địa chỉ **IP** là 172.29.14.149).

- Tạo **RR CNAME**:

Trong trường hợp ta muốn máy chủ **DNS Server** vừa có tên **server.csc.com** vừa có tên **ftp.csc.com** để phản ánh đúng chức năng là một **DNS Server**, **FTP server**,…Để tạo **RR Alias** ta thực hiện như sau:
- Click chuột **Forward Lookup Zone**, sau đó Click chuột phải vào tên **Zone | New Alias (CNAME),** sau đó ta cung cấp một số thông tin về:

- **Alias Name**: Chỉ định tên **Alias** (ví dụ ftp).
- **Full qualified domain name(FQDN) for target host:** chỉ định tên **host** muốn tạo **Alias** (ta có thể gõ tên **host** vào mục này hoặc ta chọn nút **Browse** sau đó chọn tên host).

- Tạo **RR MX** (**Mail Exchanger**):

Trong trường hợp ta tổ chức máy chủ **Mail** hỗ trợ việc cung cấp hệ thống thư điện tử cho miền cục bộ, ta phải chỉ định rõ địa chỉ của **Mail Server** cho tất cả các miền bên ngoài biết được địa chỉ này thông qua việc khai báo **RR MX**. Mục đích chính của **RR** này là giúp cho hệ thống bên ngoài có thể chuyển thư vào bên trong miền nội bộ. Để tạo **RR** này ta thực hiện như sau:
- Click chuột **Forward Lookup Zone**, sau đó Click chuột phải vào tên **Zone | New Mail Exchanger (MX) …** , sau đó ta cung cấp một số thông tin về:
- **Host or child domain:** Chỉ định tên máy hoặc địa chỉ miền con mà **Mail Server** quản lý, thông
thường nếu ta tạo **MX** cho miền hiện tại thì ta không sử dụng thông số này.
- **Full qualified domain name(FQDN) of mail server:** Chỉ định tên của máy chủ **Mail Server** quản lý mail cho miền nội bộ hoặc miền con.
- **Mail server priority:** Chỉ định độ ưu tiên của **Mail Server** (Chỉ định máy nào ưu tiên xử lý **mail** trước máy nào).
- Trong Hình bên dưới ta tạo một **RR MX** để khai báo máy chủ **mailsvr.csc.com** là máy chủ quản lý **mail** cho miền **csc.com**.

7.3. Kiểm tra hoạt động của dịch vụ DNS:

Muốn kiểm tra quá trình hoạt động của dịch vụ **DNS** ta thực hiện các bước sau:

**** Khai báo Resolver:***

Để chỉ định rõ cho **DNS Client** biết địa chỉ máy chủ **DNS Server** hỗ trợ việc phân giải tên miền.

- Để thực hiện khai báo **Resolver** ta chọn **Start | Settings | Network Connections** | Chọn **Properties** của **Local Area Connection** | Chọn **Properties** của **Internet Control (TCP/IP)**, sau đó chỉ định hai thông số .

- **Referenced DNS server**: Địa chỉ của máy chủ **Primary DNS Server**.
- **Alternate DNS server**: Địa chỉ của máy chủ **DNS** dự phòng hoặc máy chủ **DNS** thứ hai.

**** Kiểm tra hoạt động:***

Ta có thể dùng công cụ **nslookup** để kiểm tra quá trình hoạt động của dịch vụ **DNS**, phân giải **resource record** hoặc phân giải tên miền. để sử dụng được công cụ **nslookup** ta vào **Start | Run | nslookup**.

Cần tìm hiểu một vài tập lệnh của công cụ **nslookup**.
>set type=<RR_Type>

Trong đó <**RR_Type**> là loại **RR** mà ta muốn kiểm tra, sau đó gõ tên của **RR** hoặc tên miền cần kiểm tra
>set type=any: Để xem mọi thông tin về **RR** trong miền, sau đó ta gõ <**domain name**> để xem thông tin về các **RR** như **A**, **NS**, **SOA**, **MX** của miền này.

Bài tập 2: Tạo Zone tích hợp với Active Directory:

Trong quá trình nâng cấp máy **Stand-Alone Server** thành **Domain Controller** bằng cách cài **Active Directory** ta có thể chọn cơ chế cho phép hệ thống tự động cài đặt và cấu hình dịch vụ **DNS** tích hợp chung với **Active Directory**, nếu ta chọn theo cách này thì sau khi quá trình nâng cấp hoàn tất, ta có thể tham khảo cơ sở dữ liệu của **DNS** tích hợp chung với **Active Directory** thông qua trình quản lý dịch vụ **DNS**.

Trong hình này ta tham khảo cơ sở dữ liệu của **DNS** quản lý tên miền **csc.com** được tích hợp chung với **Active Directory**.
Tuy nhiên khi ta cho hệ thống tự động cấu hình cơ sở dữ liệu cho **zone** thì nó chỉ tạo một số cơ sở dữ liệu cần thiết ban đầu để nó thực hiện một số thao tác truy vấn và quản lý cơ sở dữ liệu cho **Active Directory**. Để cho **DNS** hoạt động tốt hơn thì ta mô tả thêm thông tin **resource record** cần thiết vào, điều cần thiết nhất là ta tạo **Reverse Lookup Zone** cho **Active Integrated Zone** vì ban đầu hệ thống không tạo ra **zone** này, mô tả thêm thông tin **record PTR** cho từng **resource record A** trong **Forward Lookup Zone.**
Ta có thể tạo một **zone** mới tích hợp với **Active Directory** theo các bước sau:
Bấm chuột phải vào tên **DNS Server** trong **DNS management console**, chọn **New Zone**…| chọn **Next**.
Trong hộp thoại **zone type** ta chọn **Primary Zone** với cơ chế lưu trữ zo**n**e trong **AD**, tiếp tục chọn **Next**.

Chọn tạo **zone** thuận (**Forward Lookup Zone**) | **Next**.
Chỉ định tên **zone** (**Zone Name**) | **Next**.
Chỉ định **Dynamic Update** trong trường hợp ta muốn tạo **DDNS** cho **zone** này, trong trường hợp này ta chọn **Allow both nonsecure and secure dynamic updates | Next**.

Chọn **Finish** để hoàn tất quá trình, sau khi hoàn thành ta có thể mô tả **resource record** cho **zone** này, tạo thêm **Reverse Lookup Zone** trong trường hợp ta muốn hỗ trợ phân giải nghịch.

7.5. Thay đổi một số tùy chọn trên Name Server:

Trong phần này ta khảo sát một vài tùy chọn cần thiết để tạo hiệu chỉnh thông tin cấu hình cho **DNS**. Thông thường có ba phần chính trong việc thay đổi tùy chọn.
- Tùy chọn cho **Name Server**.
- Tùy chọn cho từng **zone name**.
- Tùy chọn cho từng **RR** trong **zone name**.

* Tùy chọn cho **Name Server**.
Cho phép thay đổi một số tùy chọn chính của **Name Server** bao gồm: Cấu hình **Forwarder**, Cấu hình **Root hints**, đặt một số tùy chọn cho phép theo dõi **log** (**Event Logging**), quản lý các truy vấn (**Monitoring query**), **debug logging**,... và một số hiệu chỉnh khác.
Để sử dụng tùy chọn này ta chọn **Properties** của tên **server** trong **DNS management console.**

- **Cấu hình Forwader**: Chọn **Tab Forwarders** từ màn hình **properties** của **Name Server**

- **Cấu hình Root hints:** Ta có thể tham khảo danh sách các **Root name server** quản lý các **Top- Level domain**, thông qua hộp thoại này ta có thể thêm, xóa, hiệu chỉnh địa chỉ của **Root hints**, thông thường các địa chỉ này hệ thống có thể tự nhận biết.

Chương 3: Managing Groups

Bài 3: DỊCH VỤ THƯ MỤC ACTIVE DIRECTORY

Mục tiêu của bài học:

- Trình bày được cấu trúc của Active Directory trên windows server;
- Cài đặt và cấu hình được máy điều khiển vùng.
- Thực hiện các thao tác an toàn với máy tính.

1. Active Directory:

1.1. Giới thiệu:

AD (Active Directory) là dịch vụ thư mục chứa các thông tin về các tài nguyên trên mạng, có thể mở rộng và có khả năng tự điều chỉnh cho phép bạn quản lý tài nguyên mạng hiệu quả. Để có thể làm việc tốt với Active Directory, chúng ta sẽ tìm hiểu khái quát về Active Directory, sau đó khảo sát các thành phần của dịch vụ này.

Các đối tượng AD bao gồm dữ liệu của người dùng (user data), máy in(printers), máy chủ (servers), cơ sở dữ liệu (databases), các nhóm người dùng (groups), các máy tính (computers), và các chính sách bảo mật (security policies).

Ngoài ra một khái niệm mới được sử dụng là *container* (tạm dịch là tập đối tượng). Ví dụ Domain là một tập đối tượng chứa thông tin người dùng, thông tin các máy trên mạng, và chứa các đối tượng khác.

1.2. Chức năng của Active Directory:

- Lưu giữ một danh sách tập trung các tên tài khoản người dùng, mật khẩu tương ứng và các tài khoản máy tính.
- Cung cấp một Server đóng vai trò chứng thực (authentication server) hoặc Server quản lý đăng nhập (logon Server), Server này còn gọi là domain controller (máy điều khiển vùng).
- Duy trì một bảng hướng dẫn hoặc một bảng chỉ mục (index) giúp các máy tính trong mạng có thể dò tìm nhanh một tài nguyên nào đó trên các máy tính khác trong vùng
- Cho phép chúng ta tạo ra những tài khoản người dùng với những mức độ quyền (rights) khác nhau như: toàn quyền trên hệ thống mạng, chỉ có quyền backup dữ liệu hay shutdown Server từ xa…
- Cho phép chúng ta chia nhỏ miền của mình ra thành các miền con (subdomain) hay các đơn vị tổ chức OU (Organizational Unit). Sau đó chúng ta có thể ủy quyền cho các quản trị viên bộ phận quản lý từng bộ phận nhỏ.

1.3. Directory Services:

1.3.1. Giới thiệu Directory Services:

Directory Services (dịch vụ danh bạ) là hệ thống thông tin chứa trong **NTDS.DIT** và các chương trình quản lý, khai thác tập tin này. Dịch vụ danh bạ là một dịch vụ cơ sở làm nền tảng để hình thành một hệ thống **Active Directory**.

Một hệ thống với những tính năng vượt trội của **Microsoft**.

1.3.2. Các thành phần trong Directory Services:

Đầu tiên, bạn phải biết được những thành phần cấu tạo nên dịch vụ danh bạ là gì? Bạn có thể so sánh dịch vụ danh bạ với một quyển sổ lưu số điện thoại. Cả hai đều chứa danh sách của nhiều đối tượng khác nhau cũng như các thông tin và thuộc tính liên quan đến các đối tượng đó.

a. **Object** (đối tượng).

Trong hệ thống cơ sở dữ liệu, đối tượng bao gồm các máy in, người dùng mạng, các server, các máy trạm, các thư mục dùng chung, dịch vụ mạng, … Đối tượng chính là thành tố căn bản nhất của dịch vụ danh bạ.

b. **Attribute** (thuộc tính).

Một thuộc tính mô tả một đối tượng. Ví dụ, mật khẩu và tên là thuộc tính của đối tượng người dùng mạng. Các đối tượng khác nhau có danh sách thuộc tính khác nhau, tuy nhiên, các đối tượng khác nhau cũng có thể có một số thuộc tính giống nhau. Lấy ví dụ như một máy in và một máy trạm cả hai đều có một thuộc tính là địa chỉ **IP**.

c. **Schema** (cấu trúc tổ chức).

Một **schema** định nghĩa danh sách các thuộc tính dùng để mô tả một loại đối tượng nào đó. Ví dụ, cho rằng tất cả các đối tượng máy in đều được định nghĩa bằng các thuộc tính tên, loại **PDL** và tốc độ. Danh sách các đối tượng này hình thành nên **schema** cho lớp đối tượng "máy in". **Schema** có đặc tính
là tuỳ biến được, nghĩa là các thuộc tính dùng để định nghĩa một lớp đối tượng có thể sửa đổi được. Nói tóm lại **Schema** có thể xem là một danh bạ của cái danh bạ **Active Directory**.

d. **Container** (vật chứa).

Vật chứa tương tự với khái niệm thư mục trong **Windows**. Một thư mục có thể chứa các tập tin và các thư mục khác. Trong **Active Directory**, một vật chứa có thể chứa các đối tượng và các vật chứa khác. Vật chứa cũng có các thuộc tính như đối tượng mặc dù vật chứa không thể hiện một thực thể thật sự nào đó như đối tượng. Có ba loại vật chứa là:

- **Domain**: khái niệm này được trình bày chi tiết ở phần sau.
- **Site**: một **site** là một vị trí. **Site** được dùng để phân biệt giữa các vị trí cục bộ và các vị trí xa xôi. Ví dụ, công ty XYZ có tổng hành dinh đặt ở **San**

Fransisco, một chi nhánh đặt ở **Denver** và một văn phòng đại diện đặt ở **Portland** kết nối về tổng hành dinh bằng **Dialup Networking**. Như vậy hệ

thống mạng này có ba **site**.

- **OU (Organizational Unit):** là một loại vật chứa mà bạn có thể đưa vào đó người dùng, nhóm, máy tính và những **OU** khác. Một **OU** không thể chứa các đối tượng nằm trong domain khác. Nhờ việc một **OU** có thể chứa các **OU** khác, bạn có thể xây dựng một mô hình thứ bậc của các vật chứa để mô hình hoá cấu trúc của một tổ chức bên trong một domain. Bạn nên sử dụng **OU** để giảm thiểu số lượng domain cần phải thiết lập trên hệ thống.

e. Global Catalog.

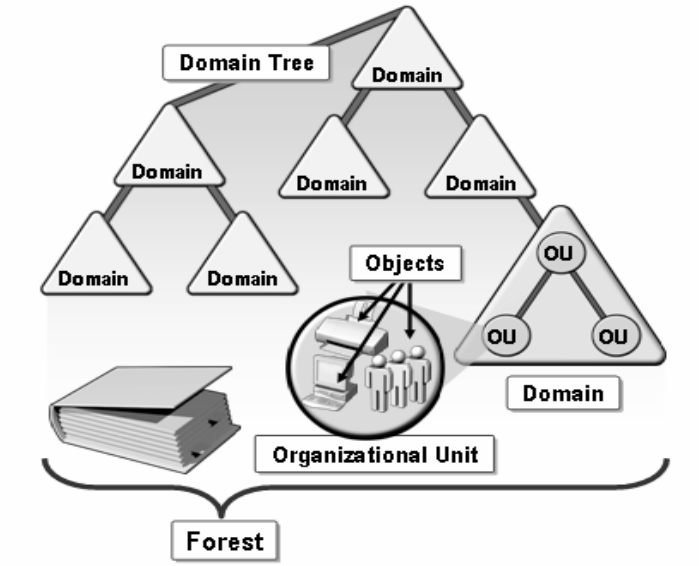
- Dịch vụ **Global Catalog** dùng để xác định vị trí của một đối tượng mà người dùng được cấp quyền truy cập. Việc tìm kiếm được thực hiện xa hơn những gì đã có trong **Windows NT** và không chỉ có thể định vị được đối tượng bằng tên mà có thể bằng cả những thuộc tính của đối tượng.
- Giả sử bạn phải in một tài liệu dày 50 trang thành 1000 bản, chắc chắn bạn sẽ không dùng một máy in **HP Laserjet 4L**. Bạn sẽ phải tìm một máy in chuyên dụng, in với tốc độ 100ppm và có khả năng đóng tài liệu thành quyển. Nhờ **Global Catalog**, bạn tìm kiếm trên mạng một máy in với các thuộc tính như vậy và tìm thấy được một máy **Xerox Docutech 6135**. Bạn có thể cài đặt **driver** cho máy in đó và gửi **print job** đến máy in. Nhưng nếu bạn ở **Portland** và máy in thì ở **Seattle** thì sao? **Global Catalog** sẽ cung cấp thông tin này và bạn có thể gửi **email** cho chủ nhân của máy in, nhờ họ in giùm.
- Một ví dụ khác, giả sử bạn nhận được một thư thoại từ một người tên **Betty Doe** ở bộ phận kế toán. Đoạn thư thoại của cô ta bị cắt xén và bạn không thể biết được số điện thoại của cô ta. Bạn có thể dùng **Global Catalog** để tìm thông tin về cô ta nhờ tên, và nhờ đó bạn có được số điện thoại của cô ta.
- Khi một đối tượng được tạo mới trong **Active Directory**, đối tượng được gán một con số phân biệt gọi là **GUID** (**Global Unique Identifier**). **GUID** của một đối tượng luôn luôn cố định cho dù bạn có di chuyển đối tượng đi đến khu vực khác.

Chương 7: Managing Access to Objects in Organizational Units

2. Các thành phần của AD:

2.1. Cấu trúc AD logic:

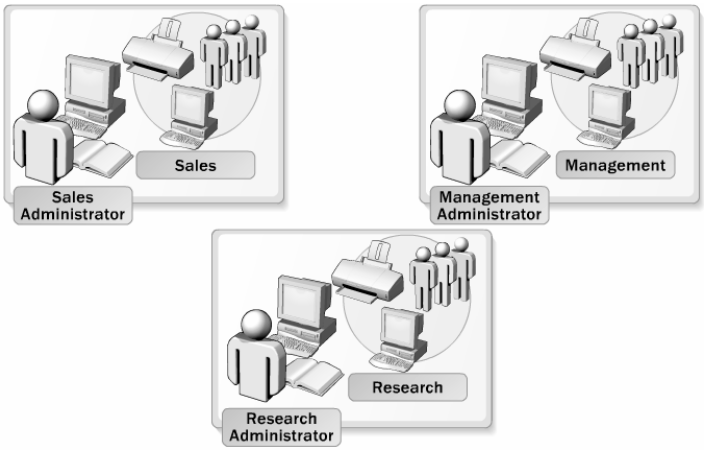
Gồm các thành phần: domains (vùng), organization units (đơn vị tổ chức), trees (hệ vùng phân cấp) và forests (tập hợp hệ vùng phân cấp) .



2.1.1. Organizational Units:

Organizational Unit hay **OU** là đơn vị nhỏ nhất trong hệ thống **AD**, 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. **OU** cũng được thiết lập dựa trên **subnet IP** và được định nghĩa là "một hoặc nhiều **subnet** kết nối tốt với nhau". Việc sử dụng **OU** có hai công dụng chính sau:

- 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 phụ tá quản trị viên 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 (**GPO**), các chính sách nhóm này chúng ta sẽ tìm hiểu ở các chương sau.



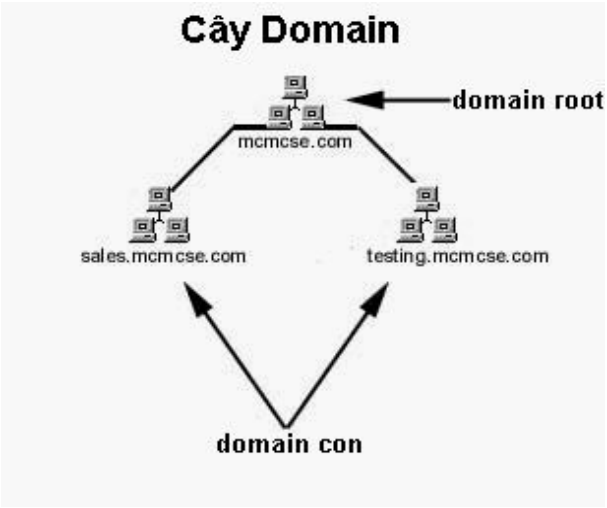
2.1.2. Domain:

Domain là đơn vị chức năng nòng cốt của cấu trúc **logic Active Directory**. Nó là phương tiện để qui định một tập hợp những người dùng, máy tính, tài nguyên chia sẻ có những qui tắc bảo mật giống nhau từ đó giúp cho việc quản lý các truy cập vào các **Server** dễ dàng hơn. **Domain** đáp ứng ba chức năng chính sau:

- Đóng vai trò như một khu vực quản trị (**administrative boundary**) các đối tượng, là một tập hợp các định nghĩa quản trị cho các đối tượng chia sẻ như: có chung một cơ sở dữ liệu thư mục, các chính sách bảo mật, các quan hệ ủy quyền với các **domain** khác.
- Giúp chúng ta quản lý bảo mật các các tài nguyên chia sẻ.
- Cung cấp các **Server** dự phòng làm chức năng điều khiển vùng (**domain controller**), đồng thời ảm bảo các thông tin trên các **Server** này được được đồng bộ với nhau.

2.1.3 Domain Tree

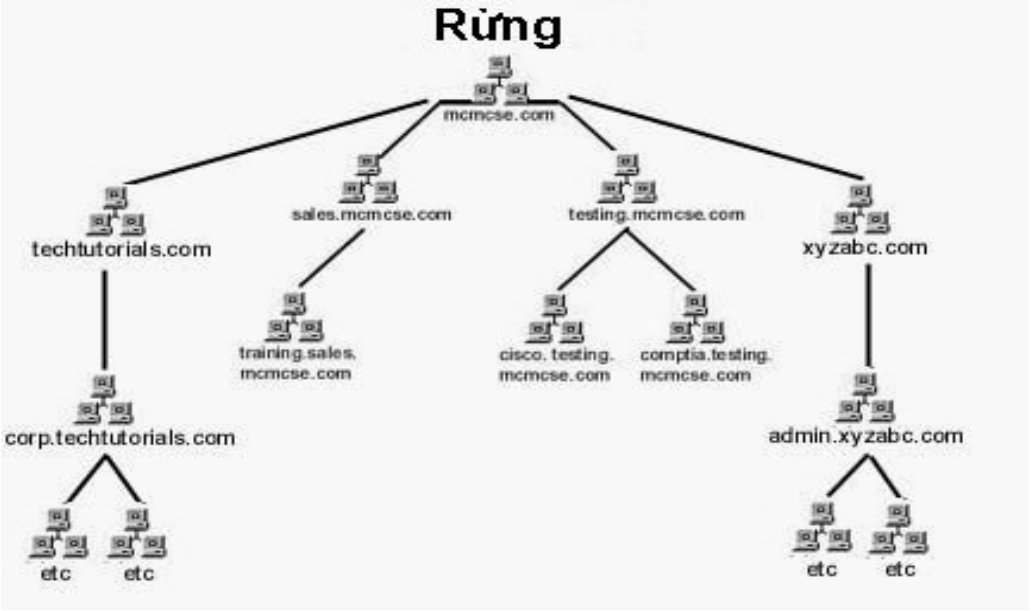
Domain Tree là cấu trúc bao gồm nhiều **domain** được sắp xếp có cấp bậc theo cấu trúc hình cây. **Domain** tạo ra đầu tiên được gọi là **domain root** và nằm ở gốc của cây thư mục. Tất cả các **domain** tạo ra sau sẽ nằm bên dưới **domain root** và được gọi là **domain** con (**child domain**). Tên của các **domain** con phải khác biệt nhau. Khi một **domain root** và ít nhất một **domain** con được tạo ra thì hình thành một cây **domain**. Khái niệm này bạn sẽ thường nghe thấy khi làm việc với một dịch vụ thư mục. Bạn có thể thấy cấu trúc sẽ có hình dáng của một cây khi có nhiều nhánh xuất hiện.



2.1.4. Forest:

Forest (rừng) được xây dựng trên một hoặc nhiều **Domain Tree**, nói cách khác **Forest** là tập hợp các **Domain Tree** có thiết lập quan hệ và ủy quyền cho nhau. Ví dụ giả sử một công ty nào đó, chẳng hạn như **Microsoft**, thu mua một công ty khác. Thông thường, mỗi công ty đều có một hệ thống **Domain Tree** riêng

và để tiện quản lý, các cây này sẽ được hợp nhất với nhau bằng một khái niệm là rừng



Trong ví dụ trên, công ty mcmcse.com thu mua được techtutorials.com và xyzabc.com và hình thành rừng từ gốc mcmcse.com

2.2. Cấu trúc AD vật lý:

Gồm: sites và domain controllers.

- Địa bàn (site): là tập hợp của một hay nhiều mạng con kết nối với nhau, tạo điều kiện truyền thông qua mạng dễ dàng, ấn định ranh giới vật lý xung quanh các tài nguyên mạng.
- Điều khiển vùng (domain controllers): là máy tính chạy Windows Server chứa bản sao dữ liệu vùng. Một vùng có thể có một hay nhiều điều khiển vùng. Mỗi sự thay đổi dữ liệu trên một điều khiển vùng sẽ được tự động cập nhật lên các điều khiển khác của vùng.

3. Cài đặt và cấu hình Active Directory (AD):

3.1. Nâng cấp Server thành Domain Controller(DC):

3.1.1. Giới thiệu:

Theo mặc định, tất cả các máy **Windows Server 2003** khi mới cài đặt đều là **Server** độc lập (**standalone server**). Chương trình **DCPROMO** chính là **Active Directory Installation Wizard** và được dùng để nâng cấp một máy không phải là **DC** (**Server Stand-alone**) thành một máy **DC** và ngược lại giáng cấp một máy **DC** thành một **Server** bình thường. Chú ý đối với **Windows Server 2003** thì bạn có thể đổi tên máy tính khi đã nâng cấp thành **DC**.

Trước khi nâng cấp **Server** thành **Domain Controller**, bạn cần khai báo đầy đủ các thông số **TCP/IP**, đặc biệt là phải khai báo **DNS Server** có địa chỉ chính là địa chỉ IP của **Server** cần nâng cấp. Nếu bạn có khả năng cấu hình dịch vụ **DNS** thì bạn nên cài đặt dịch vụ này trước khi nâng cấp **Server**, còn ngược lại thì bạn chọn cài đặt **DNS** tự động trong quá trình nâng cấp. Có hai cách để bạn chạy chương trình **Active Directory Installation Wizard**: bạn dùng tiện ích **Manage Your Server** trong **Administrative Tools** hoặc nhấp chuột vào **Start** \ **Run**, gõ lệnh **DCPROMO**.

3.1.2. Các bước cài đặt.

Chọn menu **Start** - **Run**, nhập **DCPROMO** trong hộp thoại **Run**, và nhấn nút **OK**. Khi đó hộp thoại **Active Directory Installation Wizard** xuất hiện. Bạn nhấn **Next** để tiếp tục.

Chương trình xuất hiện hộp thoại cảnh báo: **DOS, Windows 95** và **WinNT SP3** trở về trước sẽ bị loại ra khỏi miền **Active Directory** dựa trên **Windows Server 2003**. Bạn chọn **Next** để tiếp tục.

Trong hộp thoại **Domain Controller Type**, chọn mục **Domain Controller for a New Domain** và nhấn chọn **Next**. (Nếu bạn muốn bổ sung máy điều khiển vùng vào một **domain** có sẵn, bạn sẽ chọn **Additional domain cotroller for an existing domain**.)

Đến đây chương trình cho phép bạn chọn một trong ba lựa chọn sau: chọn **Domain in new forest** nếu bạn muốn tạo **domain** đầu tiên trong một rừng mới, chọn **Child domain in an existing domain tree** nếu bạn muốn tạo ra một **domain** con dựa trên một cây **domain** có sẵn, chọn **Domain tree in an existing forest** nếu bạn muốn tạo ra một cây **domain** mới trong một rừng đã có sẵn.

Hộp thoại **New Domain Name** yêu cầu bạn tên **DNS** đầy đủ của **domain** mà bạn cần xây dựng.

Hộp thoại **NetBIOS Domain Name**, yêu cầu bạn cho biết tên **domain** theo chuẩn **NetBIOS** để tương thích với các máy **Windows NT**. Theo mặc định, tên **Domain NetBIOS** giống phần đầu của tên **Full DNS**, bạn có thể đổi sang tên khác hoặc chấp nhận giá trị mặc định. Chọn **Next** để tiếp tục.

Hộp thoại **Database and Log Locations** cho phép bạn chỉ định vị trí lưu trữ **database Active Directory** và các tập tin **log**. Bạn có thể chỉ định vị trí khác hoặc chấp nhận giá trị mặc định. Tuy nhiên theo khuyến cáo của các nhà quản trị mạng thì chúng ta nên đặt tập tin chứa thông tin giao dịch (**transaction log**) ở một đĩa cứng vật lý khác với đĩa cứng chứa cơ sở dữ liệu của **Active Directory** nhằm tăng hiệu năng của hệ thống. Bạn chọn **Next** để tiếp tục.

Hộp thoại **Shared System Volume** cho phép bạn chỉ định ví trí của thư mục **SYSVOL**. Thư mục này phải nằm trên một **NTFS5 Volume**. Tất cả dữ liệu đặt trong thư mục **Sysvol** này sẽ được tự động sao chép sang các **Domain Controller** khác trong miền. Bạn có thể chấp nhận giá trị mặc định hoặc chỉ định ví trí khác, sau đó chọn **Next** tiếp tục. (Nếu **partition** không sử dụng định dạng **NTFS5**, bạn sẽ thấy một thông báo lỗi yêu cầu phải đổi hệ thống tập tin).

DNS là dịch vụ phân giải tên kết hợp với **Active Directory** để phân giải tên các máy tính trong miền. Do đó để hệ thống **Active Directory** hoạt động được thì trong miền phải có ít nhất một **DNS Server** phân giải miền mà chúng ta cần thiết lập. Theo đúng lý thuyết thì chúng ta phải cài đặt và cấu hình dịch vụ **DNS** hoàn chỉnh trước khi nâng cấp **Server**, nhưng do hiện tại các bạn chưa học về dịch vụ này nên chúng ta chấp nhận cho hệ thống tự động cài đặt dịch vụ này. Chúng ta sẽ tìm hiểu chi tiết dịch vụ **DNS** ở giáo trình "Dịch Vụ Mạng". Trong hộp thoại xuất hiện bạn chọn lựa chọn thứ hai để hệ thống tự động cài đặt và cấu hình dịch vụ **DNS.**

Trong hộp thoại **Permissions**, bạn chọn giá trị **Permission Compatible with pre-Windows 2000 servers** khi hệ thống có các **Server** phiên bản trước **Windows 2000**, hoặc chọn **Permissions compatible only with Windows 2000 servers** or **Windows Server 2003** khi hệ thống của bạn chỉ toàn các **Server Windows 2000** và **Windows Server 2003.**

Trong hộp thoại **Directory Services Restore Mode Administrator Password**, bạn sẽ chỉ định mật khẩu dùng trong trường hợp **Server** phải khởi động vào chế độ **Directory Services Restore Mode**. Nhấn chọn **Next** để tiếp tục.

Hộp thoại **Summary** xuất hiện, trình bày tất cả các thông tin bạn đã chọn. Nếu tất cả đều chính xác, bạn nhấn **Next** để bắt đầu thực hiện quá trình cài đặt, nếu có thông tin không chính xác thì bạn chọn **Back** để quay lại các bước trước đó.

Hộp thoại **Configuring Active Directory** cho bạn biết quá trình cài đặt đang thực hiện những gì. Quá trình này sẽ chiếm nhiều thời gian. Chương trình cài đặt cũng yêu cầu bạn cung cấp nguồn cài đặt **Windows Server 2003** để tiến hành sao chép các tập tin nếu tìm không thấy.

Sau khi quá trình cài đặt kết thúc, hộp thoại **Completing the Active Directory Installation Wizard** xuất hiện. Bạn nhấn chọn **Finish** để kết thúc.

Cuối cùng, bạn được yêu cầu phải khởi động lại máy thì các thông tin cài đặt mới bắt đầu có hiệu lực. Bạn nhấn chọn nút **Restart Now** để khởi động lại. Quá trình thăng cấp kết thúc.

3.2. Gia nhập máy trạm vào Domain:

3.2.1. Giới thiệu:

Một máy trạm gia nhập vào một **domain** thực sự là việc tạo ra một mối quan hệ tin cậy (**trust relationship**) giữa máy trạm đó với các máy **Domain Controller** trong vùng. Sau khi đã thiết lập quan hệ tin cậy thì việc chứng thực người dùng **logon** vào mạng trên máy trạm này sẽ do các máy điều khiển vùng đảm nhiệm. Nhưng chú ý việc gia nhập một máy trạm vào miền phải có sự đồng ý của người quản trị mạng cấp miền và quản trị viên cục bộ trên máy trạm đó. Nói cách khác khi bạn muốn gia nhập một máy trạm vào miền, bạn phải đăng nhập cục bộ vào máy trạm với vai trò là **administrator,** sau đó gia nhập vào miền, hệ thống sẽ yêu cầu bạn xác thực bằng một tài khoản người dùng cấp miền có quyền **Add Workstation to Domain** (bạn có thể dùng trực tiếp tài khoản **administrator** cấp miền)

3.2.2. Các bước cài đặt:

Đăng nhập cục bộ vào máy trạm với vai trò người quản trị (có thể dùng trực tiếp tài khoản **administrator**).
Nhấp phải chuột trên biểu tượng My Computer, chọn **Properties**, hộp thoại **System Properties** xuất hiện, trong **Tab Computer Name**, bạn nhấp chuột vào nút **Change**. Hộp thoại nhập liệu xuất hiện bạn nhập tên miền của mạng cần gia nhập vào mục **Member of Domain**.

Máy trạm dựa trên tên miền mà bạn đã khai báo để tìm đến **Domain Controller** gần nhất và xin gia nhập vào mạng, **Server** sẽ yêu cầu bạn xác thực với một tài khoản người dùng cấp miền có quyền quản trị.

Sau khi xác thực chính xác và hệ thống chấp nhận máy trạm này gia nhập vào miền thì hệ thống xuất hiện thông báo thành công và yêu cầu bạn **reboot** máy lại để đăng nhập vào mạng.
Đến đây, bạn thấy hộp thoại **Log on to Windows** mà bạn dùng mỗi ngày có vài điều khác, đó là xuất hiện thêm mục **Log on to**, và cho phép bạn chọn một trong hai phần là: **NETCLASS**, **This Computer**. Bạn chọn mục **NETCLASS** khi bạn muốn đăng nhập vào miền, nhớ rằng lúc này bạn phải dùng tài khoản người dùng cấp miền. Bạn chọn mục **This Computer** khi bạn muốn **logon** cục bộ vào máy trạm nào và nhớ dùng tài khoản cục bộ của máy.

3.3. Công cụ quản trị các đối tượng trong Active Directory:

Một trong bốn công cụ quản trị hệ thống **Active Directory** thì công cụ **Active Directory User and Computer** là công cụ quan trọng nhất và chúng ta sẽ gặp lại nhiều trong trong giáo trình này, từng bước ta sẽ khảo sát hết các tính năng trong công cụ này. Công cụ này có chức năng tạo và quản lý các đối tượng cơ bản của hệ thống **Active Directory**.

Theo hình trên chúng ta thấy trong miền netclass.edu.vn có các mục sau:
- **Builtin**: chứa các nhóm người dùng đã được tạo và định nghĩa quyền sẵn.
- **Computers**: chứa các máy trạm mặc định đang là thành viên của miền. Bạn cũng có thể dùng tính năng này để kiểm tra một máy trạm gia nhập vào miền có thành công không.
- **Domain Controllers**: chứa các điều khiển vùng (**Domain Controller**) hiện đang hoạt động trong miền. Bạn cũng có thể dùng tính năng này để kiểm tra việc tạo thêm **Domain Controller** đồng hành có thành công không.
- **ForeignSecurityPrincipals**: là một vật chứa mặc định dành cho các đối tượng bên ngoài miền đang xem xét, từ các miền đã thiết lập quan hệ tin cậy (**trusted domain**).
- **Users**: chứa các tài khoản người dùng mặc định trên miền.

Chương 4: Managing Access to Resources

Bài 4: QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM

Mục tiêu:

- Mô tả được tài khoản người dùng, tài khoản nhóm, các thuộc tính của người dùng;
- Tạo và quản trị được tài khoản người dùng, tài khoản nhóm.
- Thực hiện các thao tác an toàn với máy tính.

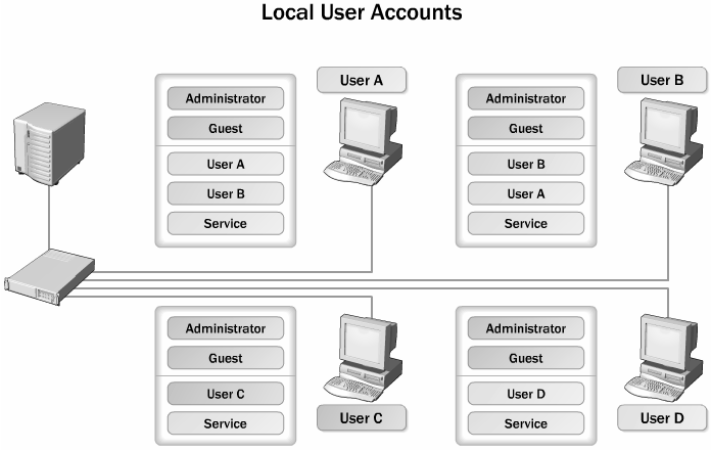
1. Định nghĩa tài khoản người dùng và tài khoản nhóm:

1.1. Tài khoản người dùng:

Tài khoản người dùng (**user account**) là một đối tượng quan trọng đại diện cho người dùng trên mạng, chúng được phân biệt với nhau thông qua chuỗi nhận dạng **username**. Chuỗi nhận dạng này giúp hệ thống mạng phân biệt giữa người này và người khác trên mạng từ đó người dùng có thể đăng nhập vào mạng và truy cập các tài nguyên mạng mà mình được phép.

1.1.1. Tài khoản người dùng cục bộ:

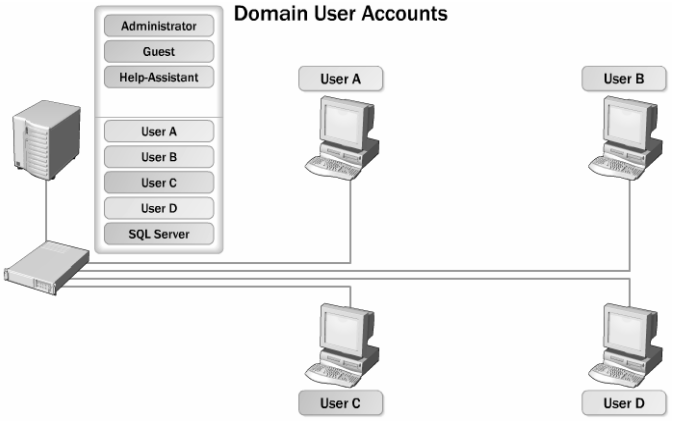
Tài khoản người dùng cục bộ (local user account) là tài khoản người dùng được định nghĩa trên máy cục bộ và chỉ được phép logon, truy cập các tài nguyên trên máy tính cục bộ. Nếu muốn truy cập các tài nguyên trên mạng thì người dùng này phải chứng thực lại với máy domain controller hoặc máy tính chứa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



1.1.2. 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**.



1.1.3. Yêu cầu về tài khoản người dùng:

- Mỗi **username** phải từ 1 đến 20 ký tự (trên **Windows Server 2003** thì tên đăng nhập có thể dài đến 104 ký tự, tuy nhiên khi đăng nhập từ các máy cài hệ điều hành **Windows NT 4.0** về trước thì mặc định chỉ hiểu 20 ký tự).
- Mỗi **username** là chuỗi duy nhất của mỗi người dùng có nghĩa là tất cả tên của người dùng và nhóm không được trùng nhau.
- **Username** không chứa các ký tự sau: " / \ [ ] : ; | = , + * ? < >
- Trong một **username** có thể chứa các ký tự đặc biệt bao gồm: dấu chấm câu, khoảng trắng, dấu gạch ngang, dấu gạch dưới. Tuy nhiên, nên tránh các khoảng trắng vì những tên như thế phải đặt trong dấu ngoặc khi dùng các kịch bản hay dòng lệnh.

1.2. Tài khoản nhóm:

Tài khoản nhóm (**group account**) là một đối tượng đại diện cho một nhóm người nào đó, dùng cho việc quản lý chung các đối tượng người dùng. Việc phân bổ các người dùng vào nhóm giúp chúng ta dễ dàng cấp quyền trên các tài nguyên mạng như thư mục chia sẻ, máy in. Chú ý là tài khoản người dùng có thể đăng nhập vào mạng nhưng tài khoản nhóm không được phép đăng nhập mà chỉ dùng để quản lý. Tài khoản nhóm được chia làm hai loại: nhóm bảo mật (**security group**) và nhóm phân phối (**distribution group**)

1.2.1. Nhóm bảo mật:

Nhóm bảo mật là loại nhóm được dùng để cấp phát các quyền hệ thống (rights) và quyền truy cập (permission). Giống như các tài khoản người dùng,

các nhóm bảo mật đều được chỉ định các SID. Có ba loại nhóm bảo mật chính là: local, global và universal. Tuy nhiên nếu chúng ta khảo sát kỹ thì có thể phân thành bốn loại như sau: local, domain local, global và universal.

Local group (nhóm cục bộ) là loại nhóm có trên các máy stand-alone Server, member server, Win2K Pro hay WinXP. Các nhóm cục bộ này chỉ có ý nghĩa và phạm vi hoạt động ngay tại trên máy chứa nó thôi.

Domain local group (nhóm cục bộ miền) là loại nhóm cục bộ đặc biệt vì chúng là local group nhưng nằm trên máy Domain Controller. Các máy Domain Controller có một cơ sở dữ liệu Active Directory chung và được sao chép đồng bộ với nhau do đó một local group trên một Domain Controller này thì cũng sẽ có mặt trên các Domain Controller anh em của nó, như vậy local group này có mặt trên miền nên được gọi với cái tên nhóm cục bộ miền. Các nhóm trong mục Built-in của Active Directory là các domain local.

Global group (nhóm toàn cục hay nhóm toàn mạng) là loại nhóm nằm trong Active Directory và được tạo trên các Domain Controller. Chúng dùng để cấp phát những quyền hệ thống và quyền truy cập vượt qua những ranh giới của một miền. Một nhóm global có thể đặt vào trong một nhóm local của các server thành viên trong miền. Chú ý khi tạo nhiều nhóm global thì có thể làm tăng tải trọng công việc của Global Catalog.

Universal group (nhóm phổ quát) là loại nhóm có chức năng giống như global group nhưng nó dùng để cấp quyền cho các đối tượng trên khắp các miền trong một rừng và giữa các miền có thiết lập quan hệ tin cậy với nhau. Loại nhóm này tiện lợi hơn hai nhóm global group và local group vì chúng dễ dàng lồng các nhóm vào nhau. Nhưng chú ý là loại nhóm này chỉ có thể dùng được khi hệ thống của bạn phải hoạt động ở chế độ Windows 2000 native functional level hoặc Windows Server 2003 functional level có nghĩa là tất cả các máy Domain Controller trong mạng đều phải là Windows Server 2003 hoặc Windows 2000 Server.

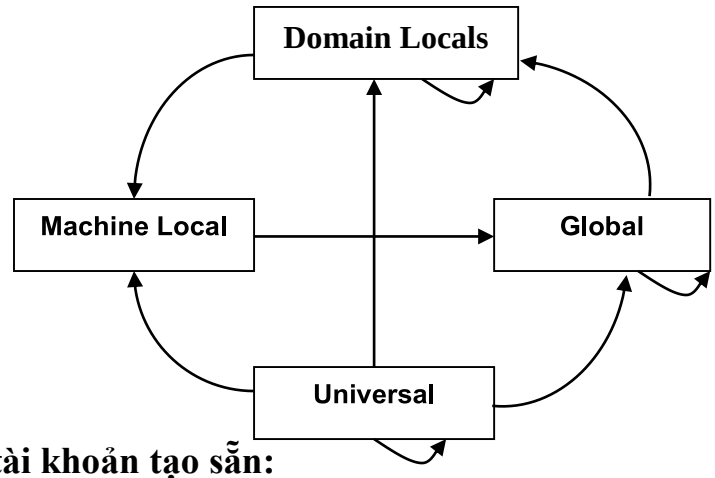
1.2.2. Nhóm phân phối:

Nhóm phân phối là một loại nhóm phi bảo mật, không có SID và không xuất hiện trong các ACL (Access Control List). Loại nhóm này không được dùng bởi các nhà quản trị mà được dùng bởi các phần mềm và dịch vụ. Chúng được dùng để phân phối thư (e-mail) hoặc các tin nhắn (message). Bạn sẽ gặp lại loại nhóm này khi làm việc với phần mềm MS Exchange.

1.2.3. Qui tắc gia nhập nhóm:

- Tất cả các nhóm Domain local, Global, Universal đều có thể đặt vào trong nhóm Machine Local.
- Tất cả các nhóm Domain local, Global, Universal đều có thể đặt vào trong chính loại nhóm của mình.

- Nhóm Global và Universal có thể đặt vào trong nhóm Domain local. Nhóm Global có thể đặt vào trong nhóm Universal.



2. Các tài khoản tạo sẵn:

2.1. 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 2003** 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 nằng 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:

Tên tài khoản	**Mô tả**
Administrator	**Administrator** 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 **Windows Server 2003**. 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 **Guest** 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
ILS_Anonymous_User	Là tài khoản đặc biệt được dùng cho dịch vụ **ILS**. **ILS** hỗ trợ cho các ứng dụng điện thoại có các đặc tính như: **caller ID**, **video conferencing**, **conference calling**, và **faxing**. Muốn sử dụng **ILS** thì dịch vụ **IIS** phải được cài đặt.
IUSR_computer- name	Là tài khoản đặc biệt được dùng trong các truy cập giấu tên trong dịch vụ **IIS** trên máy tính có cài **IIS**.

IWAM_computer- name	Là tài khoản đặc biệt được dùng cho **IIS** khởi động các tiến trình của các ứng dụng trên máy có cài **IIS**.
Krbtgt	Là tài khoản đặc biệt được dùng cho dịch vụ trung tâm phân phối khóa (**Key Distribution Center**)
TSInternetUser	Là tài khoản đặc biệt được dùng cho **Terminal Services**.

2.2. Tài khoản nhóm Domain Local tạo sẵn:

Như 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.

Tên nhóm	Mô tả
Administrators	Nhóm 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 **Domain Admins** và **Enterprise Admins** là thành viên mặc định của nhóm **Administrators**.
Account Operators	Thành 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 **container Built-in** và **OU**.
Domain Controllers	Nhóm này chỉ có trên các **Domain Controller** và mặc định không có thành viên nào, thành viên của nhóm có thể đăng nhập cục bộ vào các **Domain Controller** nhưng không có quyền quản trị các chính sách bảo mật.
Backup Operators	Thành viên của nhóm này có quyền lưu trữ dự phòng (**Backup**) và phục hồi (**Retore**) hệ thống tập tin. Trong trường hợp hệ thống tập tin là **NTFS** 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 **Backup**. Nếu muốn truy cập trực tiếp thì họ phải được gán quyền.
Guests	Là nhóm bị hạn chế quyền truy cập các tài nguyên trên mạng. Các thành viên nhóm này là người dùng vãng lai không phải là thành viên của mạng. Mặc định các tài khoản **Guest** bị khóa
Print Operator	Thành viên của nhóm này có quyền tạo ra, quản lý và xóa bỏ các đối tượng máy in dùng chung trong Active Directory.
Server Operators	Thành viên của nhóm này có thể quản trị các máy server trong miền như:
Users	Mặc định 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.

Replicator	Nhóm này được dùng để hỗ trợ việc sao chép danh bạ trong **Directory Services**, nhóm này không có thành viên mặc định.
Incoming Forest Trust Builders	Thành 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.
Network Configuration Operators	Thành viên nhóm này có quyền sửa đổi các thông số **TCP/IP** trê các máy
Pre-Windows 2000 Compatible	Nhóm 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 **WinNT** cũ.
Remote Desktop User	Thành viên nhóm này có thể đăng nhập từ xa vào các **Domain Controller** trong miền, nhóm này không có thành viên mặc định.
Performace Log Users	Thành viên nhóm này có quyền truy cập từ xa để ghi nhận lại những giá trị về hiệu năng của các máy **Domain Controller**, nhóm này cũng không có thành viên mặc định.
Performace Monitor Users	Thành viên nhóm này có khả năng giám sát từ xa các máy **Domain Controller**.

Ngoài ra còn một số nhóm khác như DHCP Users, DHCP Administrators, DNS Administrators… các nhóm này phục vụ chủ yếu cho các dịch vụ, chúng ta sẽ tìm hiểu cụ thể trong từng dịch vụ ở giáo trình "Dịch Vụ Mạng". Chú ý theo mặc định hai nhóm Domain Computers và Domain Controllers được dành riêng cho tài khoản máy tính, nhưng bạn vẫn có thể đưa tài khoản người dùng vào hai nhóm này.

2.3. 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 **member server** và các máy trạm (**Win2K Pro, WinXP**) đã đưa nhóm **Domain Admins** là thành viên của nhóm cục bộ **Administrators** 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 **Users** trên các máy **server** 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 **administrator** miền là thành viên của nhóm này.
Enterprise Admins	Đây là một nhóm **universal**, 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 **administrators** trên các **Domain Controller** trong rừng.
Schema Admins	Nhóm **universal** này cũng chỉ xuất hiện trong miền gốc của rừng, thành viên của nhóm này có thể chỉnh sửa cấu trúc tổ chức (**schema**) của **Active Directory**.

2.4. Các nhóm tạo sẵn đặc biệt:

Ngoài các nhóm tạo sẵn đã trình bày ở trên, hệ thống **Windows Server 2003** còn có một số nhóm tạo sẵn đặt 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.
- **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 hữa 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. Quản lý tài khoản người dùng và nhóm cục bộ:

3.1. Công cụ quản lý tài khoản người dùng cục bộ

Muốn tổ chức và quản lý người dùng cục bộ, ta dùng công cụ **Local Users and Groups**. Với công cụ này bạn có thể tạo, xóa, sửa các tài khoản người dùng, cũng như thay đổi mật mã. Có hai phương thức truy cập đến công cụ **Local Users and Groups**:

- Dùng như một **MMC** (**Microsoft Management Console**) snap-in.
- Dùng thông qua công cụ **Computer Management.**

Các bước dùng để chèn **Local Users and Groups snap-in** vào trong **MMC**:

- Chọn **Start \ Run**, nhập vào hộp thoại **MMC** và ấn phím **Enter** để mở cửa sổ **MMC**.

- Chọn Console \ Add/Remove Snap-in để mở hộp thoại Add/Remove Snap-in
- Nhấp chuột vào nút Add để mở hộp thoại Add Standalone Snap-in. Chọn Local Users and Groups và nhấp chuột vào nút Add. Hộp thoại Choose Target Machine xuất hiện, ta chọn Local Computer và nhấp chuột vào nút Finish để trở lại hộp thoại Add Standalone Snap-in.
- Nhấp chuột vào nút Close để trở lại hộp thoại Add/Remove Snap-in.
- Nhấp chuột vào nút OK, ta sẽ nhìn thấy Local Users and Groups snap-in đã chèn vào MMC như hình sau.
- Lưu Console bằng cách chọn Console \ Save, sau đó ta nhập đường dẫn và tên file cần lưu trữ. Để tiện lợi cho việc quản trị sau này ta có thể lưu console ngay trên Desktop.
- Nếu máy tính của bạn không có cấu hình MMC thì cách nhanh nhất để truy cập công cụ Local Users and Groups thông qua công cụ Computer Management. Nhấp phải chuột vào My Computer và chọn Manage từ pop-up menu và mở cửa sổ Computer Management. Trong mục System Tools, ta sẽ nhìn thấy mục Local Users and Groups
- Cách khác để truy cập đến công cụ Local Users and Groups là vào Start \ Programs\Administrative Tools \ Computer Management
-

3.2. Các thao tác cơ bản trên tài khoản người dùng cục bộ:

3.2.1. Tạo tài khoản mới:

Trong công cụ **Local Users and Groups**, ta nhấp phải chuột vào **Users** và chọn **New User**, hộp thoại **New User** hiển thị bạn nhập các thông tin cần thiết vào, nhưng quan trọng nhất và bắt buộc phải có là mục **Username**.

3.2.2. Xóa tài khoản:

Bạn nên xóa tài khoản người dùng, nếu bạn chắc rằng tài khoản này không bao giờ cần dùng lại nữa. Muốn xóa tài khoản người dùng bạn mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần xóa, nhấp phải chuột và chọn **Delete** hoặc vào thực đơn **Action** \ **Delete**.

***Chú ý*:** khi chọn **Delete** thì hệ thống xuất hiện hộp thoại hỏi bạn muốn xóa thật sự không vì tránh trường hợp bạn xóa nhầm. Bởi vì khi đã xóa thì tài khoản người dùng này không thể phục hồi được.

3.2.3 Khóa tài khoản:

Khi một tài khoản không sử dụng trong thời gian dài bạn nên khóa lại vì lý do bảo mật và an toàn hệ thống. Nếu bạn xóa tài khoản này đi thì không thể phục hồi lại được do đó ta chỉ tạm khóa. Trong công cụ **Local Users and Groups**, nhấp đôi chuột vào người dùng cần khóa, hộp thoại **Properties** của tài khoản xuất hiện.

Trong **Tab General**, đánh dấu vào mục **Account is disabled.**

3.2.4 Đổi tên tài khoản:

Bạn có thể đổi tên bất kỳ một tài khoản người dùng nào, đồng thời bạn cũng có thể điều chỉnh các thông tin của tài khoản người dùng thông qua chức năng này. Chức năng này có ưu điểm là khi bạn thay đổi tên người dùng nhưng **SID** của tài khoản vẫn không thay đổi. Muốn thay đổi tên tài khoản người dùng bạn mở công cụ **Local Users and Groups**, chọn tài khoản người dùng cần thay đổi tên, nhấp phải chuột và chọn **Rename**.

3.2.5 Thay đổi mật khẩu:

Muốn đổi mật mã của người dùng bạn mở công cụ Local Users and Groups, chọn tài khoản người dùng cần thay đổi mật mã, nhấp phải chuột và chọn Reset password.

4. Quản lý tài khoản người dùng và nhóm trên Active Directory:

4.1. Tạo mới tài khoản người dùng:

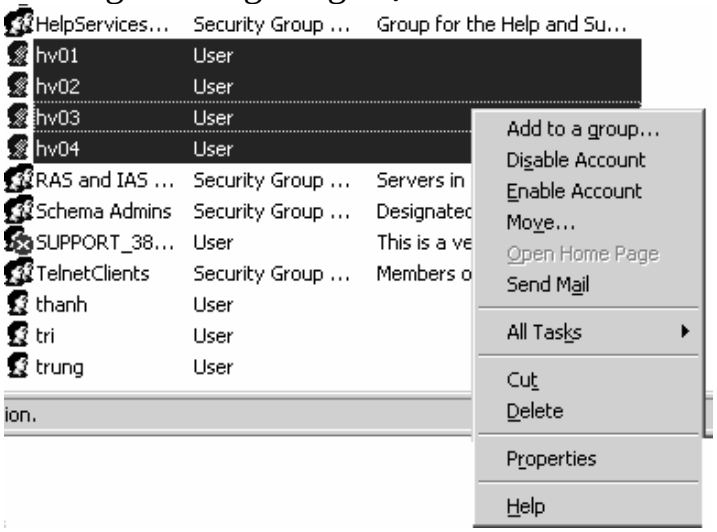
Bạn có thể dùng công cụ Active Directory User and Computers trong Administrative Tools ngay trên máy Domain Controller để tạo các tài khoản người dùng miền. Công cụ này cho phép bạn quản lý tài khoản người dùng từ xa thậm chí trên các máy trạm không phải dùng hệ điều hành Server như WinXP, Win2K Pro. Muốn thế trên các máy trạm này phải cài thêm bộ công cụ Admin Pack. Bộ công cụ này nằm trên Server trong thư mục \Windows\system32\ADMINPAK.MSI. Tạo một tài khoản người dùng trên Active Directory, ta làm các bước sau:

Chọn Start\ Programs\ Administrative Tools\ Active Directory Users and Computers.

4.2. Các thuộc tính của tài khoản người dùng:

Muốn quản lý các thuộc tính của các tài khoản người ta dùng công cụ Active Directory Users and Computers (bằng cách chọn Start\ Programs\ Administrative Tools\ Active Directory Users and Computers), sau đó chọn thư mục Users và nhấp đôi chuột vào tài khoản người dùng cần khảo sát. Hộp thoại Properties xuất hiện, trong hộp thoại này chứa 12 Tab chính, ta sẽ lần lượt khảo sát các Tab này.

Ngoài ra bạn có thể gom nhóm (dùng hai phím Shift, Ctrl) và hiệu chỉnh thông tin của nhiều tài khoản người dùng cùng một lúc.



4.2.1 Các thông tin mở rộng của người dùng:

Tab **General** chứa các thông tin chung của người dùng trên mạng mà bạn đã nhập trong lúc tạo người dùng mới. Đồng thời bạn có thể nhập thêm một số thông tin như: số điện thoại, địa chỉ mail và trang địa chỉ trang Web cá nhân…

Tab **Address** cho phép bạn có thể khai báo chi tiết các thông tin liên quan đến địa chỉ của tài khoản người dùng như: địa chỉ đường, thành phố, mã vùng, quốc gia…

Tab **Telephones** cho phép bạn khai báo chi tiết các số điện thoại của tài khoản người dùng

Tab **Organization** cho phép bạn khai báo các thông tin người dùng về: chức năng của công ty, tên phòng ban trực thuộc, tên công ty …

Bảng mô tả chi tiết các tùy chọn liên quan đến tài khoản người dùng:

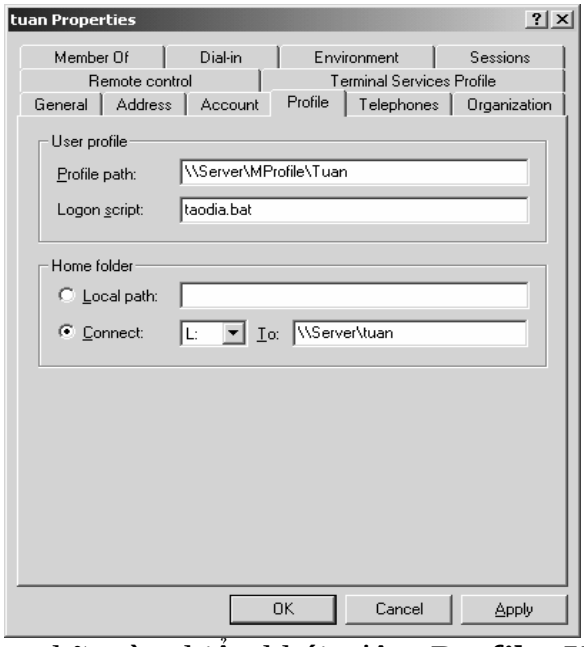
Tùy chọn	Ý nghĩa
User must change password at next logon	Người dùng phải thay đổi mật khẩu lần đăng nhập kế tiếp, sau đó mục này sẽ tự động bỏ chọn.
User cannot change password	Nếu được chọn thì ngăn không cho người dùng tùy ý thay đổi mật khẩu.
Password never expires	Nếu được chọn thì mật khẩu của tài khoản này không bao giờ hết hạn.
Store password using reversible encryption	Chỉ áp dụng tùy chọn này đối với người dùng đăng nhập từ các máy

Account is disabled	Nếu được chọn thì tài khoản này tạm thời bị khóa, không sử dụng được.
Smart card is required for interactive login	Tùy chọn này được dùng khi người dùng đăng nhập vào mạng thông qua một thẻ thông minh (**smart card**), lúc đó người dùng không nhập username và password mà chỉ cần nhập vào một số **PIN**.
Account is trustedfor elegation	Chỉ áp dụng cho các tài khoản dịch vụ nào cần giành được quyền truy cập vào tài nguyên với vai trò những tài khoản người dùng khác
Account is sensitive and cannot be delegated	Dùng tùy chọn này trên một tài khoản khách vãng lai hoặc tạm để đảm bảo rằng tài khoản đó sẽ không được đại diện bởi một tài khoản khác.
Use DES encryption types for this account	Nếu được chọn thì hệ thống sẽ hỗ trợ **Data Encryption Standard** (**DES**) với nhiều mức độ khác nhau.
Do not require Kerberos preauthentication	Nếu được chọn hệ thống sẽ cho phép tài khoản này dùng một kiểu thực hiện giao thức **Kerberos** khác với kiểu của **Windows Server 2003**.

Mục cuối cùng trong Tab này là quy định thời gian hết hạn của một tài khoản người dùng. Trong mục Account Expires, nếu ta chọn Never thì tài khoản này không bị hết hạn, nếu chọn End of: ngày tháng hết hạn thì đến ngày này tài khoản này bị tạm khóa.

4.2.3 Tab Profile:

Tab 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** 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 2003** cho từng người dùng mạng. **Profile** chứa các qui định về màn hình **Desktop**, nội dung của menu **Start,** kiểu cách phối màu sắc, vị trí sắp xếp các **icon**, biểu tượng chuột…

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 **ntuser.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 2003** có ba loại **Profile**:

Local Profile: là **profile** của người dùng được lưu trên máy cục bộ và họ tự cấu hình trên **profile** đó.

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.

Mandatory Profile: người quản trị mạng thêm thông tin đường dẫn **user profile** vào trong thông tin tài khoản người dùng, sau đó chép một profile đã cấu hình sẵn vào đường dẫn đó. Lúc đó các người dùng dùng chung **profile** này và không được quyền thay đổi profile đó.

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 xa 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 2003** 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 **\Windows\SYSVOL\sysvol**, nếu các tập tin script này phục vụ cho các máy tiền **Win2K** thì phải đặt trong thư mục
\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.

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 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). Trong ví dụ này bạn chỉ thư mục cá nhân cho tài khoản Tuan là "\\server\tuan", nhưng bạn có thể thay thế tên tài khoản bằng biến môi trường người dùng như: "\\server\%username%".

4.2.4 Tab Member Of:

Tab Member Of cho phép bạn xem và cấu hình tài khoản người dùng hiện tại là thành viên của những nhóm nào. Một tài khoản người dùng có thể là thành viên của nhiều nhóm khác nhau và nó được thừa hưởng quyền của tất cả các nhóm này. Muốn gia nhập vào nhóm nào bạn nhấp chuột vào nút **Add**, hộp thoại chọn nhóm sẽ hiện ra.

Trong hộp thoại chọn nhóm, nếu bạn nhớ tên nhóm thì có thể nhập trực tiếp tên nhóm vào và sau đó nhấp chuột vào nút **Check Names** để kiểm tra có chính xác không, bạn có thể nhập gần đúng để hệ thống tìm các tên nhóm có liên quan. Đây là tính năng mới của **Windows Server 2003** tránh tình trạng tìm kiếm và hiển thị hết tất cả các nhóm hiện có trong hệ thống. Nếu bạn không nhớ tên nhóm thì chấp nhận nhấp chuột vào nút **Advanced** và **Find Now** để tìm hết tất cả các nhóm
Nếu bạn muốn tài khoản người dùng hiện tại thoát ra khỏi một nhóm nào đó thì bạn chọn nhóm sau đó nhấp chuột vào nút **Remove**.

4.2.5 Tab Dial-in:

Tab **Dial-in** cho phép bạn cấu hình quyền truy cập từ xa của người dùng cho kết nối **dial-in** hoặc **VPN**, chúng ta sẽ khảo sát chi tiết ở chương **Routing and Remote Access**

4.3. Tạo mới tài khoản nhóm:

Bạn tạo và quản lý tài khoản nhóm trên Active Directory thông qua công cụ Active Directory Users and Computers. Trước khi tạo nhóm bạn phải xác

định loại nhóm cần tạo, phạm vi hoạt động của nhóm như thế nào. Sau khi chuẩn bị đầy đủ các thông tin bạn thực hiện các bước sau:

Chọn Start \ Programs \ Administrative Tools \ Active Directory Users and Computers để mở công cụ Active Directory Users and Computers lên. Nhấp phải chuột vào mục Users, chọn New trên pop-up menu và chọn Group.

Hộp thoại New Object – Group xuất hiện, bạn nhập tên nhóm vào mục Group name, trường tên nhóm cho các hệ điều hành trước Windows 2000 (pre-Windows 2000) tự động phát sinh, bạn có thể hiệu chỉnh lại cho phù hợp.

4.4. Các tiện ích dòng lệnh quản lý tài khoản người dùng và tài khoản nhóm:

Windows Server 2003 cung cấp nhiều công cụ dòng lệnh mạnh mẽ, có thể được dùng trong các tập tin xử lý theo lô (**batch**) hoặc các tập tin kịch bản (**script**) để quản lý tài khoản người dùng như thêm, xóa, sửa. **Windows 2003** còn hỗ trợ việc nhập và xuất các đối tượng từ **Active Directory**. Hai tiện ích **dsadd.exe** và **admod.exe** với đối số **user** cho phép chúng ta thêm và chỉnh sửa tài khoản người dùng trong **Active Directory**. Tiện ích **csvde.exe** được dùng để nhập hoặc xuất dữ liệu đối tượng thông qua các tập tin kiểu **CSV** (**comma-separated values**). Đồng thời hệ thống mới này vẫn còn sử dụng hai lệnh **net user** và **net group** của **Windows 2000**.

4.4.1 Lệnh net user:

Chức năng: tạo thêm, hiệu chỉnh và hiển thị thông tin của các tài khoản người dùng . Cú pháp:

net user [username [password | *] [options]] [/domain]
net user username {password | *} /add [options] [/domain]
net user username [/delete] [/domain]

Ý nghĩa các tham số:

- Không tham số: dùng để hiển thị danh sách của tất cả các tài khoản người dùng trên máy tính
- [**Username**]: chỉ ra tên tài khoản người dùng cần thêm, xóa, hiệu chỉnh hoặc hiển thị. Tên của tài khoản người dùng có thể dài đến 20 ký tự.
- [**Password**]: ấn định hoặc thay đổi mật mã của tài khoàn người dùng. Một mật mã phải có chiều dài tối thiểu bằng với chiều dài quy định trong chính sách tài khoản người dùng. Trong **Windows 2000** thì chiều dài của mật mã có thể dài đến 127 ký tự, nhưng trên hệ thống **Win9X** thì chỉ hiểu được 14 ký tự, do đó nếu bạn đặt mật mã dài hơn 14 ký tự thì có thể tài khoản này không thể **logon** vào mạng từ máy trạm dùng **Win9X**.
- [**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.

- [**/add**]: thêm một tài khoản người dùng vào trong cơ sở dữ liệu tài khoản người dùng.
- [**/delete**]: xóa một tài khoản người dùng khỏi cơ sở dữ liệu tài khoản người dùng.
- [**/active:{no | yes}**]: cho phép hoặc tạm khóa tài khoản người dùng. Nếu tài khoản bị khóa thì người dùng không thể truy cập các tài nguyên trên máy tính. Mặc định là cho phép (**active**).
- [**/comment:"text"**]: cung cấp mô tả về tài khoản người dùng, mô tả này có thể dài đến 48 ký tự.
- [**/countrycode:nnn**]: chỉ định mã quốc gia và mã vùng.
- [**/expires:{date | never}**]: quy định ngày hết hiệu lực của tài khoản người dùng.
- [**/fullname:"name"**]: khai báo tên đầy đủ của người dùng.
- [**/homedir:path**]: khai báo đường dẫn thư mục cá nhân của tài khoản, chú ý đường dẫn này đã tồn tại.
- [**/passwordchg:{yes | no}**]: chỉ định người dùng có thể thay đổi mật mã của mình không, mặc định là có thể.
- [**/passwordreq:{yes | no}**]: chỉ định một tài khoản người dùng phải có một mật mã, mặc định là có mật mã.
- [**/profilepath:[path]**]: khai báo đường dẫn **Profile** của người dùng, nếu không hệ thống sẽ tự tạo một profile chuẩn cho người dùng lần **logon** đầu tiên.
- [**/scriptpath:path**]: khai báo đường dẫn và tập tin **logon script**. Đường dẫn này có thể là đường dẫn tuyệt đối hoặc đường dẫn tương đối (ví dụ: %systemroot%\System32\Repl\Import\Scripts).
- [**/times:{times | all}**]: quy định giờ cho phép người dùng logon vào mạng hay máy tính cục bộ. Các thứ trong tuần được đại diện bởi ký tự : M, T, W, Th, F, Sa, Su. Giờ ta dùng AM, PM để phân biệt buổi sáng hoặc chiều. Ví dụ sau chỉ cho phép người dùng làm việc trong giờ hành chính từ thứ 2 đến thứ 6: "M,7AM-5PM; T,7AM-5PM; W,7AM-5PM; Th,7AM-5PM; F,7AM-5PM;"
- [**/workstations:{computername[,...] | *}**]: chỉ định các máy tính mà người dùng này có thể sử dụng để logon vào mạng. Nếu **/workstations** không có danh sách hoặc danh sách là ký tự '*' thì người dùng có thể sử dụng bất kỳ máy nào để vào mạng.

4.4.2 Lệnh net group:

Chức năng: tạo mới thêm, hiển thị hoặc hiệu chỉnh nhóm toàn cục trên **Windows 2003 Server**

Cú pháp:

```
net group [groupname [/comment:"text"]] [/domain]
net group groupname {/add [/comment:"text"] | /delete} [/domain]
net group groupname username[ ...] {/add | /delete} [/domain]
```

Ý nghĩa các tham số:

- Không tham số: dùng để hiển thị tên của Server và tên của các nhóm trên Server đó.
- [**Groupname**]: chỉ định tên nhón cần thêm, mở rộng hoặc xóa.
- [**/comment:"text"**]: thêm thông tin mô tả cho một nhóm mới hoặc có sẵn, nội dung này có thể dài đến 48 ký tự.
- [**/domain**]: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2003 Server** là **primary domain controller** hoặc **Windows 2003 Professional** là thành viên của máy **Windows 2003 Server domain**.
- [**username[...]**]: danh sách một hoặc nhiều người dùng cần thêm hoặc xóa ra khỏi nhóm, các tên này cách nhau bởi khoảng trắng.
- [**/add**]: thêm một nhóm hoặc thêm một người dùng vào nhóm.
- [**/delete**]: xóa một nhóm hoặc xóa một người dùng khỏi nhóm.
-

4.4.3 Các lệnh hỗ trợ dịch vụ Active Driectory trong môi trường Windows Server 2003:

Trên hệ thống **Windows Server 2003**, **Microsoft** phát triển thêm một số lệnh nhằm hỗ trợ tốt hơn cho dịch vụ **Directory** như: **dsadd**, **dsrm**, **dsmove**, **dsget**, **dsmod**, **dsquery**. Các lệnh này thao tác chủ yếu trên các đối tượng **computer, contact, group, ou, user, quota.**

- **Dsadd**: cho phép bạn thêm một **computer**, **contact**, **group**, **ou** hoặc **user** vào trong dịch vụ **Directory**.
- **Dsrm**: xóa một đối tượng trong dịch vụ **Directory**.
- **Dsmove**: di chuyển một đối tượng từ vị trí này đến vị trí khác trong dịch vụ **Directory**.
- **Dsget**: hiển thị các thông tin lựa chọn của một đối tượng **computer**, **contact**, **group**, **ou**, **server** hoặc **user** trong một dịch vụ **Directory**.
- **Dsmod**: chỉnh sửa các thông tin của **computer**, **contact**, **group**, **ou** hoặc **user** trong một dịch vụ **Directory**.
- **Dsquery**: truy vấn các thành phần trong dịch vụ **Directory**.

Ví dụ:

- Tạo một **user** mới: dsadd user "CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn" –samid hv10 –pwd 123
- Xóa một **user**: dsrm "CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn"
- Xem các **user** trong hệ thống: ***dsquery user***
- Gia nhập **user** mới vào nhóm: dsmod group "CN=hs, CN=Users, DC=netclass, DC=edu, DC=vn" –addmbr "CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn"

Chương 5: Implementing Printing

Bài 5: QUẢN TRỊ MÁY IN

Mục tiêu:

- Mô tả về mô hình và thuật ngữ được sử dụng cho tác vụ in ấn trong Windows;
- Cài đặt một máy in logic trên một máy chủ in ấn;
- Chuẩn bị một máy chủ in ấn cho các máy trạm;
- Kết nối một máy trạm in ấn đến một máy in logic trên máy chủ in ấn;
- Quản trị hàng đợi in ấn và các đặc tính máy in;
- Xử lý sự cố các lỗi về máy in.
- Thực hiện các thao tác an toàn với máy tính.

1. 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 2003** 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 2003**. 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 **DVD** 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 2003** 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:

Bài tập 5: Cài đặt máy in (Printer)

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 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.

Chương 6: Managing Printing

2. Quản lý thuộc tính máy in:

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.

2.2. Giấy và chất lượng in

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**

2.3. 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.

3. Cấu hình chia sẻ máy in:

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

Ngoài ra, trong **Tab Sharing**, ta có thể cấu hình **driver** hỗ trợ cho các máy trạm sử dụng máy in trong trường hợp máy trạm không phải là **Windows Server 2003**. Đây là một tính năng cần thiết vì nó cho phép chỉ định các **driver** hỗ trợ in để các máy trạm có thể tải về một cách tự động. Mặc định, **driver** duy nhất được nạp vào là **driver** của hãng **Intel** cho các máy trạm là **Windows 2000, Windows Server 2003**, và **Windows XP**. Để cung cấp thêm các **driver** cho máy trạm khác, bạn nhấp chuột vào nút **Additional Drivers** nằm phía

dưới **Tab Sharing**. Hộp thoại **Additional Drivers** xuất hiện. **Windows Server 2003** hỗ trợ các **driver** thêm vào cho các **Client** là một trong những hệ điều hành sau:

- Itanium Windows XP hay Windows Server 2003.
- x86 Windows 2000, Windows XP, hay Windows Server 2003 (mặc định).
- x86 Windows 95, Windows 98, hay Windows Millennium Edition.
- x86 Windows NT 4.

4. Cấu hình thông số port:

4.1. Cấu hình các thông số trong Tab Port:

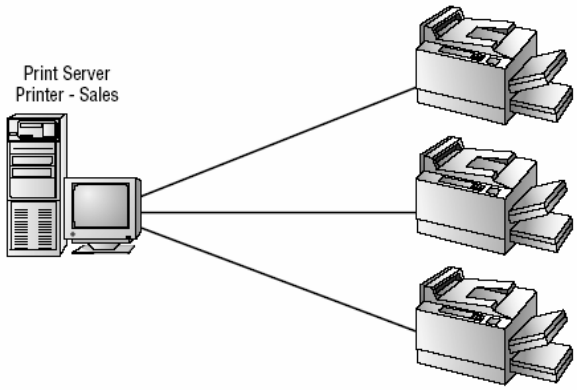
Trong hộp thoại **Properties**, bạn chọn **Tab Port** để cấu hình tất cả các **port** đã được định nghĩa cho máy in sử dụng. Một **port** được định nghĩa như một **interface** sẽ cho phép máy tính giao tiếp với thiết bị máy in. **Windows Server 2003** hỗ trợ các port vật lý (**local port**) và các **port 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 2003** 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 kì 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 xoá 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.

4.2. Printer Pooling:

Printer pool được sử dụng nhằm phối hợp nhiều máy in vật lý với một máy in **logic**, được minh họa như hình bên dưới. Lợi ích của việc sử dụng **printer pool** là máy in rảnh đầu tiên sẽ thực hiện thao tác in ấn cho bạn. Tính năng này rất hữu dụng trong trường hợp ta có một nhóm các máy in vật lý được chia sẻ cho một nhóm người dùng, ví dụ như là nhóm các thư ký



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 Pooling** 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.

4.3. Điều hướng tác vụ in đến một máy in khác

Nếu một máy in vật lý của bạn bị hư, bạn có thể chuyển tất cả các tác vụ in ấn của máy in bị hư sang một máy in khác. Để làm được điều này, trước hết bạn phải đảm bảo máy in mới phải có **driver** giống với máy in cũ. Sau đó, trong **Tab Port**, bạn nhấp chuột vào nút **Add Port**, chọn **Local port** rồi chọn tiếp **New Port**. Hộp thoại **Port Name** xuất hiện, gõ vào tên **UNC** của máy in mới theo định dạng: **\\computername\printer_sharename.**

5. Cấu hình Tab Advanced:

5.1. Các thông số của Tab Advanced

Trong hộp thoại **Properties**, bạn nhấp chuột vào **Tab Advanced** để điều khiển các đặc tính của máy in. Bạn có thể cấu hình các thuộc tính sau:

- Khả năng của máy in
- Độ ưu tiên của máy in
- Driver mà máy in sẽ sử dụng
- Các thuộc tính đồng tác (**spooling**) của máy in

- Cách thức in tài liệu
- Chế độ in mặc định
- Sử dụng bộ xử lý in ấn nào
- Các trang độc lập

5.2. 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 in 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 kì người dùng nào.

5.3. 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. 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.

Ví dụ: giả sử có một máy in được phòng kế toán sử dụng. Những người quản lý trong phòng kế toán luôn luôn muốn tài liệu của họ sẽ được ưu tiên in ra trước các nhân viên khác. Để cấu hình cho việc sắp xếp thứ tự này, ta tạo ra một máy in tên là **MANAGERS** gắn vào **port LPT1** với độ ưu tiên là 99. Sau đó, cũng trên port **LPT1**, ta tạo thêm một máy in nữa tên là **WORKERS** với độ ưu tiên là 1. Sau đó, ta sẽ sử dụng **Tab Security** trong hộp thoại **Properties** để giới hạn quyền sử dụng máy in **MANAGERS** cho những người quản lý. Đối với các nhân viên còn lại trong phòng kế toán, ta cho phép họ sử dụng máy in **WORKERS** (chúng ta sẽ tìm hiểu rõ hơn về **Security** trong phần sau). Khi các tác vụ in xuất phát từ máy in **MANAGERS**, nó sẽ đi vào hàng đợi của của máy in vật lý với độ ưu tiên cao hơn là các tác vụ xuất phát từ máy in **WORKERS**. Do đó, tài liệu của những người quản lý sẽ được ưu tiên in trước.

5.4. Print Driver

Mục **Drive**r trong **Tab Advanced** cho phép bạn chỉ định driver sẽ dùng

cho máy in. Nếu bạn đã cấu hình nhiều máy in trên một máy tính thì bạn có thể chọn bất kì **driver** nào trong các **driver** đã cài đặt. Thao tác thực hiện như sau: Nhấp chuột vào nút **New Driver** để khởi động **Add Printer Driver Wizard**. **Add Printer Driver Wizard** cho phép bạn thực hiện cập nhật cũng như thêm driver mới.

5.5. Spooling

Khi bạn cấu hình tùy chọn **spooling**, bạn cần chỉ định rõ các tác vụ in ấn sẽ được đẩy ra đường ống máy in hay được gửi trực tiếp đến thiết bị máy in. **Spooling** có nghĩa là các thao tác in ấn sẽ được lưu trữ xuống đĩa thành một hàng đợi trước khi các thao tác in này được gửi đến máy in. Có thể xem **spooling** giống như là bộ điều phối in ấn nếu như tại một thời điểm có nhiều người dùng cùng lúc gởi yêu cầu đến máy in. Theo chế độ mặc định, tùy chọn **spooling** sẽ được bật lên sẵn.

5.6. Print Options

Phía dưới **Tab Advance** có chứa bốn tùy chọn in ấn. Đó là các tùy chọn:

- **Hold Mismatched Documents**: tùy chọn này hữu dụng trong trường hợp bạn sử dụng chế độ nhiều biểu mẫu trong một máy in. Mặc định thì tùy chọn này sẽ không được bật lên. Các tác vụ sẽ được in theo chế độ **first-in-first-out (FIFO).** Nếu bạn bật tùy chọn này lên, hệ thống sẽ chọn ưu tiên in trước những tác vụ có chung một biểu mẫu.
- **Print Spooled Documents First**: tùy chọn này qui định rằng các tác vụ in ấn được điều hướng xong trước các loại tác vụ lớn khác. Điều này có nghĩa là các tác vụ in ấn sẽ có độ ưu tiên lớn hơn các loại tác vụ khác trong quá trình điều hướng. Mặc định thì tùy chọn này luôn được bật lên giúp gia tăng hiệu quả làm việc của máy in.
- **Keep Printed Documents**: tùy chọn này qui định rằng các tác vụ in ấn phải được xóa khỏi hàng đợi điều hướng in ấn khi các tác vụ này đã hòan tất quá trình in. Thông thường, bạn muốn xóa các tác vụ in ấn ngay khi nó bắt đầu in bởi vì nếu chúng ta tiếp tục lưu trữ các tác vụ này trong hàng đợi điều hướng và đợi cho đến khi chúng được in xong mới xóa thì sẽ phải tốn dung lượng ổ đĩa cho việc lưu trữ. Mặc định thì tùy chọn này sẽ không được bật lên.
- **Enable Advanced Printing Features**: tùy chọn này qui định rằng bất kì các tính năng mở rộng nào mà máy in của bạn có hỗ trợ ví dụ như **Page**

Order và **Pages Per Sheet** nên được bật lên. Mặc định thì tùy chọn này luôn được bật lên. Chỉ trong trường hợp xảy ra các vấn đề về tương thích thì bạn có thể tắt tùy chọn này. Ví dụ như bạn đang sử dụng **driver** cho một thiết bị máy in tương tự nhưng nó không hỗ trợ tất cả các tính năng của máy in. Trong trường hợp đó, bạn nên tắt tùy chọn này đi.

5.7. Printing Defaults

Nút **Printing Defaults** nằm ở góc trái phía dưới của **Tab Advance**. Nếu bạn nhấp chuột vào nút **Printing Defaults**, hộp thoại **The Printing Preferences** sẽ xuất hiện. Đây cũng chính là hộp thoại sẽ xuất hiện khi bạn nhấp chuột vào nút **Printing Preferences** trong **Tab General**

5.8. Print Processor

Bộ xử lý in ấn được sử dụng để qui định **Windows Server 2003** có cần phải thực hiện các xử lý bổ sung trong công việc in ấn hay không. Bộ xử lý in ấn **WinPrint** mặc định được cài đặt và được **Windows Server 2003** sử dụng. Bộ xử lý in ấn **WinPrint** có thể hỗ trợ một vài kiểu dữ liệu.

Theo mặc định thì hầu hết các ứng dụng trên nền **Window** sử dụng chuẩn **EMF (enhanced metafile)** để gởi các tác vụ đến máy in. Chuẩn **EMF** dùng kiểu dữ liệu **RAW**. Kiểu dữ liệu này sẽ báo với bộ xử lý in ấn là tác vụ này không cần phải sửa đổi độ ưu tiên khi in. Điều này là do nhà sản xuất phần mềm qui định.

Bảng danh sách các kiểu dữ liệu được bộ xử lý in ấn trong **Windows Server 2003** hỗ trợ:

Kiểu dữ liệu	Mô tả
RAW	Không làm thay đổi tài liệu in ấn
RAW (FF appended)	Không làm thay đổi tài liệu in ấn ngoại trừ việc thêm vào một kí tự **form- feed**
RAW (FF Auto)	Không làm thay đổi tài liệu in ấn ngoại trừ việc kiểm tra xem có cần thêm vào một kí tự **form-feed** hay
NT EMF 1.00x	Thường điều hướng các tài liệu được gửi từ các máy
TEXT	Phiên dịch tất cả các kiểu dữ liệu văn bản đơn giản và máy in sẽ thực hiện in bằng cách sử dụng các lệnh

5.9. Separator Pages

Separator pages được sử dụng tại thời điểm bắt đầu của mỗi tài liệu

nhằm mục đích định dạng rõ người dùng nào đã thực hiện việc in tài liệu này. Nếu như máy in không được chia sẻ thì chế độ **Separator pages** vô hình chung sẽ gây ra lãng phí giấy in. Nếu trong trường hợp máy in được chia sẻ cho nhiều người dùng thì chế độ **Separator pages** sẽ hữu dụng trong việc phân phối các tác vụ in ấn đã hoàn tất.

Để thêm một **Separator page**, bạn thực hiện như sau: nhấp chuột vào nút **Separator page** nằm ở góc phải phía **dưới Tab Advance**. Hộp thoại **Separator page** hiện ra, bạn nhấp chuột vào nút **Browse** để chọn tập tin **Separator page** nào bạn muốn sử dụng.

6. Cấu hình Tab Security:

6.1. Giới thiệu Tab Security

Chúng ta có thể kiểm soát quyền truy cập vào máy in **Windows Server 2003** của người dùng cũng như các nhóm người dùng bằng cách cấu hình quyền in ấn. Chúng ta có thể cho phép hoặc không cho phép người dùng truy xuất máy in. Chúng ta cấp quyền in ấn cho người dùng và nhóm người dùng thông qua **Tab Security** trong hộp thoại **Properties** của máy in.

Bảng phân quyền in ấn cho người dùng

Quyền hạn	Mô tả
Print	Cho phép người dùng hoặc một nhóm người dùng có thể kết nối và gửi tác vụ
Manage Printers	Cho phép thực hiện thao tác điều khiển, quản lý máy in. Với quyền này, người dùng hoặc nhóm người dùng có thể dừng hoặc khởi động lại máy in, thay đổi cấu hình của bộ điều tác, chia sẻ hoặc không chia sẻ máy in, thay đổi quyền in ấn, và quản trị các thuộc tính của máy in.
Manage Documents	Cho phép người dùng quản lý các tài liệu in qua các thao tác dừng việc in, khởi động lại, phục hồi lại, hoặc là xoá tài liệu ra khỏi hàng đợi máy in. Người dùng không thể điều khiển trạng thái của máy in.
Special Permissions	Bằng cách chọn **Tab Advanced** trong hộp thoại **Print Permissions**, bạn có thể quản lý các quyền đặc biệt

Theo mặc định, bất kì khi nào một máy in được tạo ra, các quyền in ấn mặc định sẽ được thiết lập. Bảng các quyền in ấn mặc định:

Nhóm quyền	Được phép in	Quản lý in	Quản lý tài liệu in
Administrators	X	X	X
Creator Owner			X
Everyone	X		
Print Operators	X	X	X
Server Operators	X	X	X

6.2. Cấp quyền in cho người dùng/nhóm người dùng

Thông thường, bạn có thể chấp nhận quyền in ấn mặc định đã được thiết lập sẵn. Tuy nhiên, trong một số trường hợp đặc biệt, bạn cần phải hiệu chỉnh lại các quyền in cho thích hợp. Ví dụ: Công ty của bạn vừa trang bị cho phòng **Marketing** một máy in **laser** màu đắt tiền, bạn không muốn ai cũng được phép sử dụng máy in này. Trong trường hợp này, trước tiên bạn phải bỏ tùy chọn **Allow checkbox for the Everyone group**. Sau đó, thêm nhóm **Marketing** vào trong danh sách của **Tab Security**. Cuối cùng bạn cấp cho nhóm **Marketing** quyền **Print**. Muốn thêm các quyền in ấn, bạn thực hiện các bước sau:

1. Ở **Tab Security** trong hộp thoại **Properties** của máy in, nhấp chuột vào nút **Add.**
2. Hộp thoại **Select Users**, **Computers**, **Or Groups** xuất hiện, bạn nhập vào tên của người dùng hoặc nhóm người dùng mà bạn định cấp quyền in ấn rồi nhấp chuột vào nút **Add**. Sau đó, bạn chọn tất cả các người dùng mà bạn muốn cấp quyền và nhấp chuột vào nút **OK.**
3. Chọn người dùng hoặc nhóm người dùng từ danh sách các phân quyền, sau đó chọn **Allow** để cấp quyền hoặc chọn **Deny** để không cấp quyền in ấn, các quyền quản lý máy in hay các quyền quản lý tài liệu in.

Để loại bỏ một nhóm có sẵn trong danh sách phân quyền, ta sẽ chọn nhóm đó và nhấp chuột vào nút **Remove.** Nhóm vừa chọn sẽ không còn được liệt kê trong **Tab Security** nữa và không thể được cấp bất kì quyền hạn in ấn nào.

7. Quản lý print server:

7.1. Hộp thoại quản lý Print Server

Print Server là một một máy tính trên đó có định nghĩa sẵn các máy in.

Khi người dùng gửi một yêu cầu in ấn đến một máy in mạng, thì trước tiên, yêu cầu đó phải được gửi đến **Print Server**. Nói cách khác **Print Server** sẽ có nhiệm vụ quản lý tất cả các máy in **logic** đã được tạo ra trên máy tính. Với tư cách là một **Print Server**, máy tính này phải đủ mạnh để hỗ trợ cho việc đón nhận các tác vụ in ấn và nó cũng phải đủ không gian đĩa trống để chứa các tác vụ in trong hàng đợi.

Bạn có thể quản lý **Print Server** bằng cách cấu hình các thuộc tính trong hộp thoại **Print Server Properties**. Chúng ta mở hộp thoại **Print Server Properties** bằng cách: mở hộp thoại **Printers And Faxes**, chọn **File** rồi chọn tiếp **Server Properties**. Hộp thoại **Print Server Properties** bao gồm các **Tab: Forms, Ports, Drivers** và **Advanced.**

7.2. Cấu hình các thuộc tính Port của Print Server

Trong hộp thoại **Printer Server Properties**, bạn mở **Tab Port**. **Tab** này cũng tương tự như **Tab Port** trong hộp thoại **Properties** của máy in. Sự khác nhau giữa hai **Tab Port** là: **Tab Port** trong hộp thoại **Print Server Properties** được sử dụng để quản lý tất cả các port trên **Print Server**. Còn **Tab port** trong hộp thoại **Properties** của máy in quản lý các **port** của thiết bị máy in vật lý.

7.3. Cấu hình Tab Driver

Trong hộp thoại **Printer Server Properties**, bạn mở **tab Driver**. **Tab Driver** cho phép bạn quản lý các **driver** máy in đã được cài đặt trên **Print Server**. Đối với mỗi **driver** máy in, **Tab** này sẽ hiển thị tên, môi trường và hệ điều hành mà **driver** hỗ trợ.

Sử dụng các tùy chọn trong **Tab Driver**, bạn có thể thêm vào hay loại bỏ hay cập nhật **driver** máy in. Để nhìn thấy các thuộc tính của một **driver** máy in, ta chọn **driver** cần hiển thị và nhấp chuột vào nút **Properties**. Các thuộc tính của một **driver** máy in gồm có:

- Tên **driver**.
- Phiên bản.
- Bộ xử lý.
- Ngôn ngữ.
- Loại dữ liệu mặc định.
- Đường dẫn của **driver**.

8. Giám sát trạng thái hàng đợi máy in:

Chúng ta có thể dùng tiện ích **System Monitor** để quản lý hàng

đợi máy in. **System Monitor** được dùng để theo dõi các **counter** liên quan đến thao tác thực hiện cho nhiều đối tượng máy tính. Muốn quản lý hàng đợi máy in bằng **System Monitor**, ta thực hiện theo các bước sau:

1. Chọn **Start** \ **Administrative Tools** \ **Performance**.
2. Hộp thoại **Performance** sẽ xuất hiện. Mặc định thì tiện ích **System Monitor** sẽ được chọn như hình sau:

3. Nhấp chuột vào nút **Add** (có biểu tượng dấu +) để truy xuất vào hộp thoại **Add Counters**. Sau đó, nhấp chọn **Print Queue Performance Object.**

4. Trong hộp thoại **Add Counters**, bạn có thể chỉ định ra máy tính mà bạn muốn giám sát (cả máy tính cục bộ và máy tính ở xa). **Performance Object** mà bạn cần theo dõi (trong trường hợp này là hàng đợi - **Print Queue**), các **counter** mà bạn muốn theo dõi, và bạn cũng chỉ ra là bạn có muốn theo dõi tất cả các thể hiện hay là bạn chỉ muốn theo dõi một số thể hiện của **counter** được bạn lựa chọn. Nếu bạn chọn tất cả các thể hiện được lựa chọn sẽ cho phép tất cả dữ liệu của tất cả các hàng đợi in ấn đã được định nghĩa trong máy in. Còn nếu bạn chọn chỉ theo dõi một số thể hiện của **counter** thì bạn chỉ theo dõi được dữ liệu từ một số hàng đợi in ấn cá nhân.

Bảng danh sách các hàng đợi in ấn đã được định nghĩa:

Print Queue Counter	**Mô tả**
Add Network Printer Calls	Counter này sẽ chỉ ra bao nhiêu **Print Server** đã được thêm vào các máy in được chia sẻ trong mạng. Con số này được tích lũy từ lần khởi động cuối cùng của **server**
Bytes Printed/Sec	Số **byte** trong thực tế đã được in trên một hàng đợi trong mỗi giây
Enumerate Network Printer Calls	Chỉ ra có bao nhiêu yêu cầu đã được gửi đến **Print Server** từ các danh sách duyệt mạng. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.
Job Errors	Tổng số các lỗi thao tác đã được tường trình bởi hàng đợi in ấn. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.
Jobs	Chỉ ra con số hiện tại các thao tác in ấn vẫn còn trong hàng đợi chưa
Job Spooling	Chỉ ra con số hiện tại các thao tác in ấn đã được điều hướng đến hàng đợi in ấn..

Max Jobs Spooling	Chỉ ra con số tối đa các thao tác in ấn đã được lưu trữ trong hàng đợi in ấn kể từ lần khởi động cuối cùng của **Server**.
Max References	Chỉ ra con số tối đa các tác vụ mở (tham chiếu) đã được gửi đến máy in kể từ lần khởi động cuối cùng của **Server**.
Not Ready Errors	Chỉ ra số lượng các lỗi máy in "chưa sẵn sàng phục vụ" đã được phát sinh trong hàng đợi in ấn. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.
Out of Paper Errors	Chỉ ra số lượng các lỗi máy in không có giấy đã được phát sinh trong hàng đợi in ấn. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.
Total Jobs Printed	Được sử dụng để hiển thị bao nhiêu tác vụ in ấn đã được thực hiện thành công. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.
Total Pages Printed	Được sử dụng để hiển thị bao nhiêu trang đã được in thành công. Con số này được tích luỹ từ lần khởi động cuối cùng của **Server**.

Chương 8: Implementing Group Policy

Bài 6: TẠO VÀ QUẢN LÝ THƯ MỤC DÙNG CHUNG

Mục tiêu:

- Trình bày các loại quyền truy cập dữ liệu;
- Tạo và quản lý các thư mục dùng chung trên mạng.
- Thực hiện các thao tác an toàn với máy tính.

1. Tạo thư mục dùng chung:

1.1. Chia sẻ thư mục dùng chung

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**.

Ý nghĩa của các mục trong **Tab Sharing**:

Mục	Ý nghĩa
Do not share this folder	Chỉ định thư mục này chỉ được phép truy cập cục bộ
Share this folder	Chỉ định 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
Comment	Cho phép người dùng mô tả thêm thông tin về thư mục dùng chung này
User Limit	Cho phép bạn khai báo số kết nối tối đa truy xuất vào thư mục tại một thời điểm
Permissions	Cho phép bạn thiết lập danh sách quyền truy cập thông qua mạng của người dùng
Offline Settings	Cho phép thư mục được lưu trữ tạm tài liệu khi làm việc dưới chế độ **Offline**.

1.2. Cấu hình Share Permissions

Bạn 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. Bạn muốn cấp quyền cho người dùng thì nhấp chuột vào nút **Add**.

Hộp thoại chọn người dùng và nhóm xuất hiện, bạn nhấp đôi chuột vào các tài khoản người dùng và nhóm cần chọn, sau đó chọn **OK**.

Trong hộp thoại xuất hiện, muốn cấp quyền cho người dùng bạn đánh dấu vào mục **Allow**, ngược lại khóa quyền thì đánh dấu vào mục **Deny**.

1.3. Chia sẻ thư mục dùng lệnh netshare:

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

net share sharename

net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]

net share sharename [/users: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.
- **/delete**: xóa thuộc tính chia sẻ của thư mục hiện tại.

Chương 9: Managing the User Environment bằng cách sử dụng Group Policy

2. Quản lý các thư mục dùng chung:

2.1. Xem các thư mục dùng chung:

Mục **Shared Folders** trong công cụ **Computer Management** cho phép bạn tạo và quản lý các thư mục dùng chung trên máy tính. Muốn xem các thư mục dùng chung trên máy tính bạn chọn mục **Shares**. Nếu thư mục dùng chung nào có phần cuối của tên chia sẻ (**share name**) là dấu **$** thì tên thư mục dùng chung này được ẩn đi và không tìm thấy khi bạn tìm kiếm thông qua **My Network Places** hoặc duyệt các tài nguyên mạng.

2.2. Xem các phiên làm việc trên thư mục dùng chung

Muốn xem tất cả các người dùng đang truy cập đến các thư mục dùng chung trên máy tính bạn chọn mục **Session**. Mục **Session** cung cấp các thông tin sau:

- Tên tài khoản người dùng đang kết nối vào tài nguyên chia sẻ.
- Tên máy tính có người dùng kết nối từ đó.
- Hệ điều hành mà máy trạm đang sử dụng để kết nối.
- Số tập tin mà người dùng đang mở.
- Thời gian kết nối của người dùng.
- Thời gian chờ xử lý của kết nối.
- Phải là truy cập của người dùng **Guest** không?

2.3. Xem các tập tin đang mở trong các thư mục dùng chung

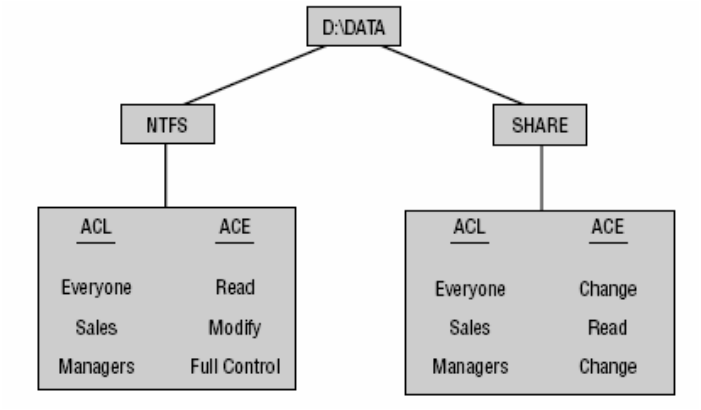
Muốn xem các tập đang mở trong các thư mục dùng chung bạn nhấp chuột vào mục **Open Files**. Mục **Open Files** cung cấp các thông tin sau:

- Đường dẫn và tập tin hiện đang được mở.
- Tên tài khoản người dùng đang truy cập tập tin đó.
- Hệ điều hành mà người dùng sử dụng để truy cập tập tin.
- Trạng thái tập tin có đang bị khoá hay không.
- Trạng thái mở sử dụng tập tin (**Read** hoặc **Write**).

3. 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 2003** 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 điện cho một người dùng hay một nhóm người.



3.1. Các quyền truy cập của NTFS

Tên quyền	Chức năng
Traverse Folder/Execute File	Duyệt các thư mục và thi hành các tập tin chương trình trong thư mục
List Folder/Read Data	Liệt kê nội dung của thư mục và đọc dữ liệu của các tập tin trong thư mục
Read Attributes	Đọc các thuộc tính của các tập tin và thư mục
Read Extended Attributes	Đọc các thuộc tính mở rộng của các tập tin và thư mục
Create File/Write Data	Tạo các 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
Write Attributes	Thay đổi thuộc tính của các tập tin và thư mục
Write Extendd Attributes	Thay đổi thuộc tính mở rộng của các tập tin và thư mục
Delete Subfolders and Files	Xóa thư mục con và các tập tin
Delete	Xóa các tập tin
Read Permissions	Đọc các quyền trên các tập tin và thư mục
Change Permissions	Thay đổi quyền trên các tập tin và thư mục
Take Ownership	Tước quyền sở hữu của các tập tin và thư mục

3.2. Các mức quyền truy cập được dùng trong NTFS

Tên quyền	Full	Modify	Read&	List	Read	Write

	Control		**Execute**	**Folder Contents**		
Traverse Folder /Execute File	X	X	X	X		
List Folder /Read Data	X	X	X	X	X	
Read Attributes	X	X	X	X	X	
Read Extended Attributes	X	X	X	X	X	
Create File /Write Data	X	X				
Create Folder /Append Data	X	X				X
Write Attributes	X	X				X
Write Extended Attributes	X	X				X
Delete Subfolders and Files	X					
Delete	X	X				
Read Permissions	X	X	X	X	X	X
Change Permissions	X					
Take Ownership	X					

3.3. 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 dùng lên các tập tin và thư mục. Bạn nhấp chuột vào **Tab Security** để cấp quyền cho các người dùng.

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**.

3.4. 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 cấp giống như các quyền đang hiển thị trong hộp thoại.

Trong hộp thoại này, **Windows Server 2003** 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.**

3.5. 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.

3.6. 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**.

3.7. Thay đổi người sở hữu thư mục

Bạn muốn xem tài khoản người và nhóm người dùng sở hữa 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**.

Chương 10: Preparing to Monitor Server Performance

Bài 5: QUẢN LÝ ĐĨA

Mục tiêu:

- Phân biệt được các loại định dạng đĩa cứng;
- Công nghệ lưu trữ mới Dynamic storage;
- Mô tả được kỹ thuật nén và mã hoá dữ liệu.
- Thực hiện các thao tác an toàn với máy tính.

1. Cấu hình hệ thống tập tin:

Hệ thống tập tin quản lý việc lưu trữ và định vị các tập tin trên đĩa cứng. **Windows Server 2003** hỗ trợ ba hệ thống tập tin khác nhau: **FAT16**, **FAT32** và **NTFS**. Nếu bạn định sử dụng các tính năng như bảo mật cục bộ, nén và mã hoá các tập tin thì bạn nên dùng **NTFS**. Bảng sau trình bày khả năng của từng hệ thống tập tin trên **Windows Server 2003**:

Khả năng	FAT16	FAT32	NTFS
Hệ điều hành hỗ trợ	Hầu hết các hệ điều hành	Windows 95/98/2000/XP/2003 / Vista/ 7/ 2008	Windows 2000,2000/XP / 2003/ Vista/7/2008
Hỗ trợ tên tập tin dài	256kýtự trên Windows	256 ký tự	256 ký tự
Sử dụng hiệu quả đĩa	Không	Có	Có
Hỗ trợ nén đĩa	Không	Không	Có
Hỗ trợ hạn ngạch	Không	Không	Có
Hỗ trợ mã hoá	Không	Không	Có
Hỗ trợ bảo mật cục bộ	Không	Không	Có
Hỗ trợ bảo mật trên mạng	Có	Có	Có
Kích thước Volume tối đa được hỗ trợ	4GB	32GB	1024GB

Trên **Windows Server 2003/Windows 2000/NT**, bạn có thể sử dụng lệnh **CONVERT** để chuyển đổi hệ thống tập tin từ **FAT16, FAT32** thành **NTFS**. Cú pháp của lệnh như sau:

CONVERT [ổ đĩa:] /fs:ntfs

Chương 11: Monitoring Server Performance

1. Cấu hình đĩa lưu trữ:

Windows Server 2003 hỗ trợ hai loại đĩa lưu trữ: basic và dynamic.

2.1. Basic storage:

Bao gồm các partition primary và extended. Partition tạo ra đầu tiên trên đĩa được gọi là partition primary và toàn bộ không gian cấp cho partition được sử dụng trọn vẹn. Mỗi ổ đĩa vật lý có tối đa bốn partition. Bạn có thể tạo ba partition primary và một partition extended. Với partition extended, bạn có thể tạo ra nhiều partition logical.

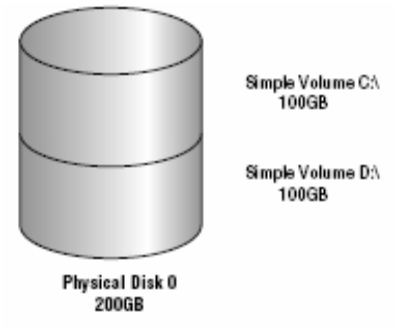
2.2. Dynamic storage:

Đây là một tính năng mới của Windows Server 2003. Đĩa lưu trữ dynamic chia thành các volume dynamic. Volume dynamic không chứa partition hoặc ổ đĩa logic, và chỉ có thể truy cập bằng Windows Server 2003 và Windows 2000. Windows Server 2003/ Windows 2000 hỗ trợ năm loại volume dynamic: simple, spanned, striped, mirrored và RAID-5. Ưu điểm của công nghệ Dynamic storage so với công nghệ Basic storage:

- Cho phép ghép nhiều ổ đĩa vật lý để tạo thành các ổ đĩa logic (Volume).
- Cho phép ghép nhiều vùng trống không liên tục trên nhiều đĩa cứng vật lý để tạo ổ đĩa logic.
- Có thể tạo ra các ổ đĩa logic có khả năng dung lỗi cao và tăng tốc độ truy xuất…

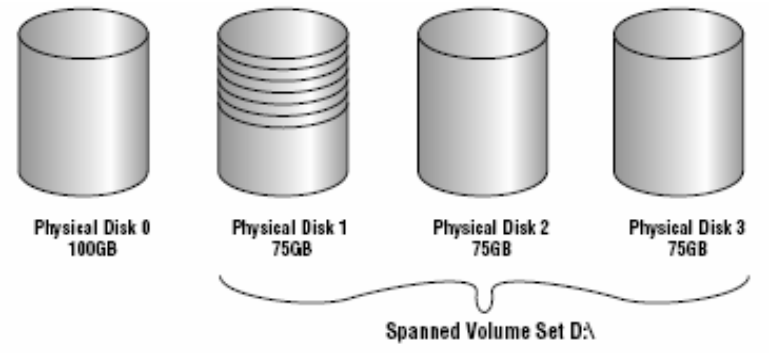
2.2.1 Volume simple:

Chứa không gian lấy từ một đĩa **dynamic** duy nhất. Không gian đĩa này có thể liên tục hoặc không liên tục. Hình sau minh hoạ một đĩa vật lý được chia thành hai **volume** đơn giản.



2.2.2 Volume spanned:

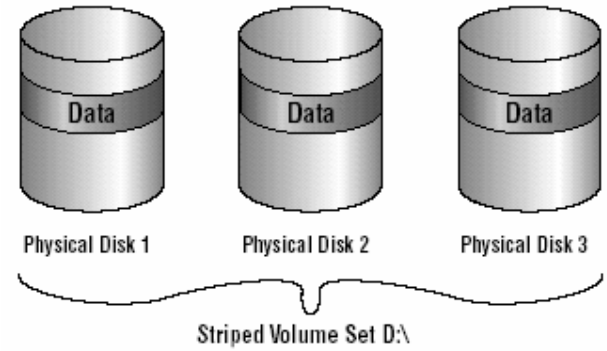
Bao gồm một hoặc nhiều đĩa **dynamic** (tối đa là 32 đĩa). Sử dụng khi bạn muốn tăng kích cỡ của **volume**. Dữ liệu ghi lên **volume** theo thứ tự, hết đĩa này đến đĩa khác. Thông thường người quản trị sử dụng **volume spanned** khi ổ đĩa đang sử dụng trong **volume** sắp bị đầy và muốn tăng kích thước của **volume** bằng cách bổ sung thêm một đĩa khác.



Do dữ liệu được ghi tuần tự nên **volume** loại này không tăng hiệu năng sử dụng. Nhược điểm chính của **volume spanned** là nếu một đĩa bị hỏng thì toàn bộ dữ liệu trên **volume** không thể truy xuất được.

2.2.3 Volume striped:

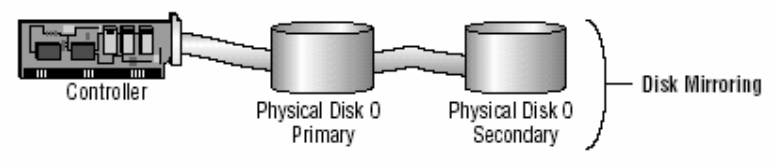
Lưu trữ dữ liệu lên các dãy (**strip**) bằng nhau trên một hoặc nhiều đĩa vật lý (tối đa là 32). Do dữ liệu được ghi tuần tự lên từng dãy, nên bạn có thể thi hành nhiều tác vụ **I/O** đồng thời, làm tăng tốc độ truy xuất dữ liệu. Thông thường, người quản trị mạng sử dụng **volume striped** để kết hợp dung lượng của nhiều ổ đĩa vật lý thành một đĩa **logic** đồng thời tăng tốc độ truy xuất.



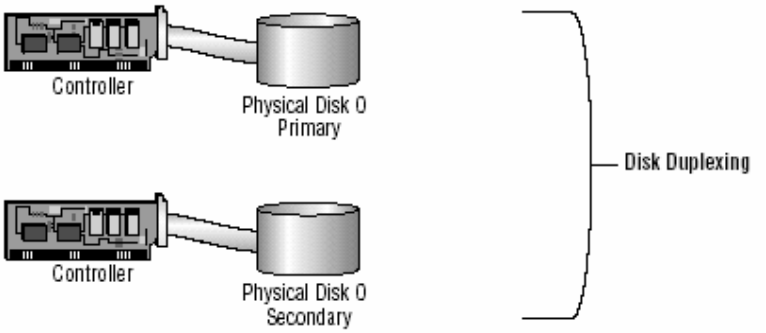
Nhược điểm chính của **volume striped** là nếu một ổ đĩa bị hỏng thì dữ liệu trên toàn bộ **volume** mất giá trị.

Chương 12: Maintaining Device Drivers

Là hai bản sao của một **volume** đơn giản. Bạn dùng một ổ đĩa chính và một ổ đĩa phụ. Dữ liệu khi ghi lên đĩa chính đồng thời cũng sẽ được ghi lên đĩa phụ. **Volume** dạng này cung cấp khả năng dung lỗi tốt. Nếu một đĩa bị hỏng thì ổ đĩa kia vẫn làm việc và không làm gián đoạn quá trình truy xuất dữ liệu. Nhược điểm của phương pháp này là bộ điều khiển đĩa phải ghi lần lượt lên hai đĩa, làm giảm hiệu năng.



Để tăng tốc độ ghi đồng thời cũng tăng khả năng dung lỗi, bạn có thể sử dụng một biến thể của **volume mirrored** là **duplexing**. Theo cách này bạn phải sử dụng một bộ điều khiển đĩa khác cho ổ đĩa thứ hai.



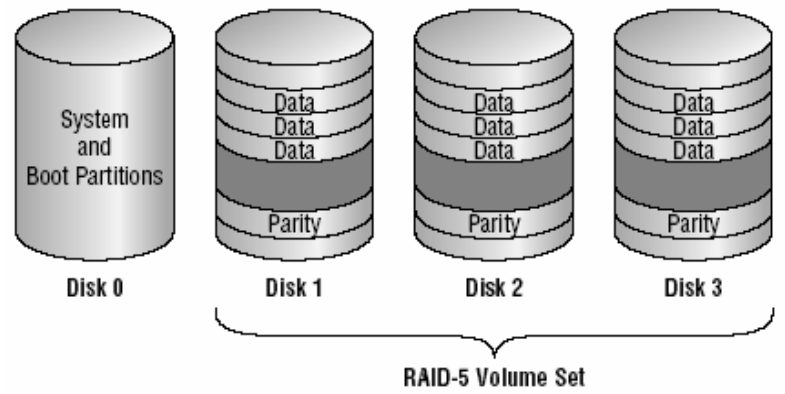
Nhược điểm chính của phương pháp này là chi phí cao. Để có một **volume 4GB** bạn phải tốn đến **8GB** cho hai ổ đĩa.

2.2.5

Chương 13: Managing Disaster Recovery

Volume RAID-5:

Tương tự như **volume striped** nhưng **RAID-5** lại dùng thêm một dãy (**strip**) ghi thông tin kiểm lỗi **parity**. Nếu một đĩa của **volume** bị hỏng thì thông tin **parity** ghi trên đĩa khác sẽ giúp phục hồi lại dữ liệu trên đĩa hỏng. **Volume RAID-5** sử dụng ít nhất ba ổ đĩa (tối đa là 32).



Ưu điểm chính của kỹ thuật này là khả năng dung lỗi cao và tốc độ truy xuất cao bởi sử dụng nhiều kênh I/O.

1. Sử dụng chương trình Disk Manager :

Disk Manager là một tiện ích giao diện đồ hoạ phục vụ việc quản lý đĩa và volume trên môi trường Windows 2000 và Windows Server 2003. Để có thể sử dụng được hết các chức năng của chương trình, bạn phải đăng nhập vào máy bằng tài khoản Administrator. Vào menu Start \ Programs \ Administrative Tools \ Computer Management. Sau đó mở rộng mục Storage và chọn Disk Management. Cửa sổ Disk Management xuất hiện như sau:

3.1. Xem thuộc tính của đĩa:

Nhấp phải chuột lên ổ đĩa vật lý muốn biết thông tin và chọn Properties. Hộp thoại Disk Properties xuất hiện như sau:

Hộp thoại cung cấp các thông tin:

- Số thứ tự của ổ đĩa vật lý
- Loại đĩa (basic, dynamic, DVD-ROM, DVD, đĩa chuyển dời được, hoặc unknown)
- Trạng thái của đĩa (online hoặc offline)
- Dung lượng đĩa
- Lượng không gian chưa cấp phát
- Loại thiết bị phần cứng
- Nhà sản xuất thiết bị
- Tên của adapter
- Danh sách các volume đã tạo trên đĩa

3.2. Xem thuộc tính của volume hoặc đĩa cục bộ:

Trên một ổ đĩa **dynamic**, bạn sử dụng các **volume**. Ngược lại trên một ổ đĩa **basic**, bạn sử dụng các đĩa cục bộ (**local disk**). **Volume** và đĩa cục bộ đều có chức năng như nhau, do vậy các phần sau dựa vào đĩa cục bộ để minh hoạ. Để xem thuộc tính của một đĩa cục bộ, bạn nhấp phải chuột lên đĩa cục bộ đó và chọn **Properties** và hộp thoại **Local Disk Properties** xuất hiện.

3.2.1 Tab General.

Cung cấp các thông tin như nhãn đĩa, loại, hệ thống tập tin, dung lượng đã sử dụng, còn trống và tổng dung lượng. Nút **Disk Cleanup** dùng để mở chương trình **Disk Cleanup** dùng để xoá các tập tin không cần thiết, giải phóng không gian đĩa.

3.2.2 Tab Tools.

Bấm nút **Check Now** để kích hoạt chương trình **Check Disk** dùng để kiểm tra lỗi như khi không thể truy xuất đĩa hoặc khởi động lại máy không đúng cách. Nút **Backup Now** sẽ mở chương trình **Backup Wizard**, hướng dẫn bạn các bước thực hiện việc sao lưu các tập tin và thư mục trên đĩa. Nút **Defragment Now** mở chương trình **Disk Defragment**, dùng để dồn các tập tin trên đĩa thành một khối liên tục, giúp ích cho việc truy xuất đĩa.

3.2.3 Tab Hardware

Liệt kê các ổ đĩa vật lý **Windows Server 2003** nhận diện được. Bên dưới danh sách liệt kê các thuộc tính của ổ đĩa được chọn.

3.2.4 Tab Sharing

Cho phép chia sẻ hoặc không chia sẻ ổ đĩa cục bộ này. Theo mặc định, tất cả các ổ đĩa cục bộ đều được chia sẻ dưới dạng ẩn (có dấu **$** sau tên chia sẻ).

3.2.5 Tab Security

Chỉ xuất hiện khi đĩa cục bộ này sử dụng hệ thống tập tin **NTFS**. Dùng để thiết lập quyền truy cập lên đĩa. Theo mặc định, nhóm **Everyone** được toàn quyền trên thư mục gốc của đĩa.

3.2.6 Tab Quota

Chỉ xuất hiện khi sử dụng **NTFS**. Dùng để quy định lượng không gian đĩa cấp phát cho người dùng.

3.2.7 Shadow Copies

Shadow Copies là dịch vụ cho phép người dùng truy cập hoặc khôi phục những phiên bản trước đây của những tập tin đã lưu, bằng cách dùng một tính năng ở máy trạm gọi là **Previous Versions**.

3.3. Bổ sung thêm một ổ đĩa mới:

3.3.1 Máy tính không hỗ trợ tính năng "hot swap"

Bạn phải tắt máy tính rồi mới lắp ổ đĩa mới vào. Sau đó khởi động máy tính lại. Chương trình **Disk Management** sẽ tự động phát hiện và yêu cầu bạn

ghi một chữ ký đặc biệt lên ổ đĩa, giúp cho **Windows Server 2003** nhận diện được ổ đĩa này. Theo mặc định, ổ đĩa mới được cấu hình là một đĩa **dynamic**.

3.3.2 Máy tính hỗ trợ "hot swap":

Bạn chỉ cần lắp thêm ổ đĩa mới vào theo hướng dẫn của nhà sản xuất mà không cần tắt máy. Rồi sau đó dùng chức năng **Action** **Rescan Disk** của **Disk Manager** để phát hiện ổ đĩa mới này.

3.4. Tạo partition volume mới:

Nếu bạn còn không gian chưa cấp phát trên một đĩa **basic** thì bạn có thể tạo thêm **partition** mới, còn trên đĩa **dynamic** thì bạn có thể tạo thêm **volume** mới. Phần sau hướng dẫn bạn sử dụng **Create Partition Wizard** để tạo một **partition** mới:

Nhấp phải chuột lên vùng trống chưa cấp phát của đĩa **basic** và chọn **Create Logical Drive**.

Xuất hiện hộp thoại **Create Partition Wizard**. Nhấn nút **Next** trong hộp thoại này.

Trong hộp thoại **Select Partition Type**, chọn loại **partition** mà bạn định tạo. Chỉ có những loại còn khả năng tạo mới được phép chọn (tuỳ thuộc vào ổ đĩa vật lý của bạn). Sau khi chọn loại **partition** xong nhấn **Next** để tiếp tục.

Tiếp theo, hộp thoại **Specify Partition Size** yêu cầu bạn cho biết dung lượng định cấp phát. Sau khi chỉ định xong, nhấn **Next**.

Trong hộp thoại **Assign Drive Letter or Path**, bạn có thể đặt cho **partition** này một ký tự ổ đĩa, hoặc gắn (**mount**) vào một thư mục rỗng, hoặc không làm đặt gì hết. Khi bạn chọn kiểu gắn vào một thư mục rỗng thì bạn có thể tạo ra vô số **partition** mới. Sau khi đã quyết định xong, nhấn **Next** để tiếp tục.

Hộp thoại **Format Partition** yêu cầu bạn quyết định có định dạng **partition** này không. Nếu có thì dùng hệ thống tập tin là gì? đơn vị cấp phát là bao nhiêu? nhãn của **partition** (**volume label**) là gì? có định dạng nhanh không? Có nén tập tin và thư mục không? Sau khi đã chọn xong, nhấn **Next** để tiếp tục.

Hộp thoại **Completing** the **Create Partition Wizard** tóm tắt lại các thao tác sẽ thực hiện, bạn phải kiểm tra lại xem đã chính xác chưa, sau đó nhấn **Finish** để bắt đầu thực hiện.

3.5. Thay đổi ký tự ổ đĩa hoặc đường dẫn.

Muốn thay đổi ký tự ổ đĩa cho **partition/volume** nào, bạn nhấp phải chuột lên **volume** đó và chọn **Change Drive Letter and Path**. Hộp thoại **Change Drive Letter and Path** xuất hiện.

Trong hộp thoại này, nhấn nút **Edit** để mở tiếp hộp thoại **Edit Drive Letter and Path**, mở danh sách **Assign a drive letter** và chọn một ký tự ổ đĩa mới định đặt cho **partition/volume** này. Cuối cùng đồng ý xác nhận các thay đổi đã thực hiện.

3.6. Xoá partition/volume

Để tổ chức lại một ổ đĩa hoặc huỷ các dữ liệu có trên một **partition/volume**, bạn có thể xoá nó đi. Để thực hiện, trong cửa sổ **Disk Manager**, bạn nhấp phải chuột lên **partition/volume** muốn xoá và chọn **Delete Partition** (hoặc **Delete Volume**). Một hộp thoại cảnh báo xuất hiện, thông báo dữ liệu trên **partition** hoặc **volume** sẽ bị xoá và yêu cầu bạn xác nhận lại lần nữa thao tác này.

3.7. Cấu hình Dynamic Storage

3.7.1 Chuyển chế độ lưu trữ.

Để sử dụng được cơ chế lưu trữ **Dynamic**, bạn phải chuyển đổi các đĩa cứng vật lý trong hệ thống thành **Dynamic Disk**. Trong công cụ **Computer Management \ Disk Management**, bạn nhấp phải chuột trên các ổ đĩa bên của sổ bên phải và chọn **Convert to Dynamic Disk….** Sau đó đánh dấu vào tất cả các đĩa cứng vật lý cần chuyển đổi chế độ lưu trữ và chọn **OK** để hệ thống chuyển đổi. Sau khi chuyển đổi xong hệ thống sẽ yêu cầu bạn **restart** máy để áp dụng chế độ lưu trữ mới.

3.7.2 Tạo Volume Spanned.

Trong công cụ **Disk Management**, bạn nhấp phải chuột lên vùng trống của đĩa cứng cần tạo **Volume**, sau đó chọn **New Volume.**

Tiếp theo, bạn chọn loại **Volume** cần tạo. Trong trường hợp này chúng ta chọn **Spanned**.

Bạn chọn những đĩa cứng dùng để tạo **Volume** này, đồng thời bạn cũng nhập kích thước mà mỗi đĩa giành ra để tạo **Volume**. Chú ý đối với loại **Volume** này thì kích thước của các đĩa giành cho **Volume** có thể khác nhau.

Bạn gán ký tự ổ đĩa cho **Volume**.

Bạn định dạng **Volume** mà bạn vừa tạo để có thể chứa dữ liệu.

Đến đây đã hoàn thành việc tạo **Volume**, bạn có thể lưu trữ dữ liệu trên **Volume** này theo cơ chế đã trình bày ở phần lý thuyết.

3.7.3 Tạo Volume Striped

Các bước tạo **Volume Striped** cũng tương tự như việc tạo các **Volume** khác nhưng chú ý là kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng tổng các kích thước của các phần trên.

3.7.4 Tạo Volume Mirror.

Các bước tạo **Volume Mirror** cũng tương tự như trên, chú ý kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng chính kích thước của mỗi phần trên.

3.7.5 Tạo Volume Raid-5.

Các bước tạo **Volume Raid-5** cũng tương tự như trên nhưng chú ý là loại **Volume** yêu cầu tối thiểu đến 3 đĩa cứng. Kích thước của các đĩa cứng giành cho loại **Volume** này phải bằng nhau và kích thước của **Volume** bằng 2/3 kích thước của mỗi phần cộng lại.

4. Quản lý việc nén dữ liệu:

Nén dữ liệu là quá trình lưu trữ dữ liệu dưới một dạng thức chiếm ít không gian hơn dữ liệu ban đầu. **Windows Server 2003** hỗ trợ tính năng nén các tập tin và thư mục một cách tự động và trong suốt. Các chương trình ứng dụng truy xuất các tập tin nén một cách bình thường do hệ điều hành tự động giải nén khi mở tập tin và nén lại khi lưu tập tin lên đĩa. Khả năng này chỉ có trên các **partition NTFS**. Nếu bạn chép một tập tin/thư mục trên một **partition** có tính năng nén sang một partition **FAT** bình thường thì hệ điều hành sẽ giải nén tập tin/ thư mục đó trước khi chép đi.

Để thi hành việc nén một tập tin/thư mục, bạn sử dụng chương trình **Windows Explorer** và thực hiện theo các bước sau:

- Trong cửa sổ **Windows Explorer**, duyệt đến tập tin/thư mục định nén và chọn tập tin/thư mục đó.
- Nhấp phải chuột lên đối tượng đó và chọn **Properties**.
- Trong hộp thoại **Properties**, nhấn nút **Advanced** trong **tab General**.
- Trong hộp thoại **Advanced Properties**, chọn mục "**Compress contents to save disk space**" và nhấn chọn **OK**.

Nhấn chọn **OK** trong hộp thoại **Properties** để xác nhận thao tác. Nếu bạn định nén một thư mục, hộp thoại **Confirm Attribute Changes** xuất hiện, yêu cầu bạn lựa chọn hoặc là chỉ nén thư mục này thôi (**Apply changes to this folder only**) hoặc nén cả các thư mục con và tập tin có trong thư mục (**Apply changes to this folder, subfolders and files**). Thực hiện lựa chọn của bạn và nhấn **OK**.

Để thực hiện việc giải nén một thư mục/tập tin, bạn thực hiện tương tự theo các bước ở trên và bỏ chọn mục **Compress contents to save disk space** trong hộp thoại **Advanced Properties**.

5. Thiết lập hạn ngạch đĩa (disk quota).

Hạn ngạch đĩa được dùng để chỉ định lượng không gian đĩa tối đa mà một người dùng có thể sử dụng trên một **volume NTFS**. Bạn có thể áp dụng hạn ngạch đĩa cho tất cả người dùng hoặc chỉ đối với từng người dùng riêng biệt.

Một số vấn đề bạn phải lưu ý khi thiết lập hạn ngạch đĩa:

- Chỉ có thể áp dụng trên các volume **NTFS**.
- Lượng không gian chiếm dụng được tính theo các tập tin và thư mục do người dùng sở hữu.
- Khi người dùng cài đặt một chương trình, lượng không gian đĩa còn trống mà chương trình thấy được tính toán dựa vào hạn ngạch đĩa của người dùng, không phải là lượng không gian còn trống trên **volume**.
- Được tính toán trên kích thước thật sự của tập tin trong trường hợp tập tin/thư mục được nén.

5.1. Cấu hình hạn ngạch đĩa.

Bạn cấu hình hạn ngạch đĩa bằng hộp thoại **Volume Propertise** đã giới thiệu trong phần trên. Bạn cũng có thể mở hộp thoại này bằng cách nhấp phải chuột lên ký tự ổ đĩa trong **Windows Explorer** và chọn **Propertise**. Trong hộp thoại này nhấp chọn **tab Quota**. Theo mặc định tính năng hạn ngạch đĩa không được kích hoạt.

Các mục trong hộp thoại có ý nghĩa như sau:

- **Enable quota management**: thực hiện hoặc không thực hiện quản lý hạn ngạch đĩa.
- **Deny disk space to users exceeding quota limit**: người dùng sẽ không thể tiếp tục sử dụng đĩa khi vượt quá hạn ngạch và nhận được thông báo **out of disk space.**
- **Select the default quota limit for new users on this volume**: định nghĩa các giới hạn sử dụng. Các lựa chọn bao gồm "không định nghĩa giới hạn" (**Do not limit disk space**), "giới hạn cho phép" (**Limit disk space to**) và "giới hạn cảnh báo" (**Set warning level to**).
- **Select the quota logging options for this volume**: có ghi nhận lại các sự kiện liên quan đến sử dụng hạn ngạch đĩa. Có thể ghi nhận khi người dùng vượt quá giới hạn cho phép hoặc vượt quá giới hạn cảnh báo.

Biểu tượng đèn giao thông trong hộp thoại có các trạng thái sau:

- Đèn đỏ cho biết tính năng quản lý hạn ngạch không được kích hoạt.
- Đèn vàng cho biết **Windows Server 2003** đang xây dựng lại thông tin hạn ngạch.
- Đèn xanh cho biết tính năng quản lý đang có tác dụng.

5.2. Thiết lập hạn ngạch mặc định.

Khi bạn thiết lập hạn ngạch mặc định áp dụng cho các người dùng mới trên volume, chỉ những người dùng chưa bao giờ tạo tập tin trên volume đó mới chịu ảnh hưởng. Có nghĩa là những người dùng đã sở hữu các tập tin/thư mục trên volume này đều không bị chính sách hạn ngạch quy định. Như vậy, nếu bạn dự định áp đặt hạn ngạch cho tất cả các người dùng, bạn phải chỉ định hạn ngạch ngay từ khi tạo lập **volume**.

Để thực hiện, bạn mở hộp thoại **Volume Properties** và chọn tab **Quota**. Đánh dấu chọn mục **Enable quota management** và điền vào các giá trị giới hạn sử dụng và giới hạn cảnh báo.

5.3. Chỉ định hạn ngạch cho từng cá nhân.

Trong một vài trường hợp, bạn cần phải chỉ định hạn ngạch cho riêng một người nào đó, chẳng hạn có thể là các lý do sau:

- Người dùng này sẽ giữ nhiệm vụ cài đặt các phần mềm mới, và như vậy họ phải có được lượng không gian đĩa trống lớn.

- Hoặc là người dùng đã tạo nhiều tập tin trên **volume** trước khi thiết lập hạn ngạch, do vậy họ sẽ không chịu tác dụng. Bạn phải tạo riêng một giới hạn mới áp dụng cho người đó.

Để thiết lập, nhấn nút **Quota Entries** trong tab **Quota** của hộp thoại **Volume Properties**. Cửa sổ **Quota Entries** xuất hiện.

Chỉnh sửa thông tin hạn ngạch của một người dùng: nhấn đúp vào mục của người dùng tương ứng, hộp thoại **Quota Setting** xuất hiện cho phép bạn thay đổi các giá trị hạn ngạch.

Bổ sung thêm một mục quy định hạn ngạch: trong cửa sổ **Quota Entries**, vào menu **Quota** chọn mục **New Quota Entry** / xuất hiện hộp thoại **Select Users**, bạn chọn người dùng rồi nhấn **OK** / xuất hiện hộp thoại **Add New Quota Entry**, bạn nhập các giá trị hạn ngạch thích hợp và nhấn **OK**.

6. Mã hoá dữ liệu bằng EFS:

EFS (Encrypting File System) là một kỹ thuật dùng trong **Windows Server 2003** dùng để mã hoá các tập tin lưu trên các **partition NTFS**. Việc mã hoá sẽ bổ sung thêm một lớp bảo vệ an toàn cho hệ thống tập tin. Chỉ người dùng có đúng khoá mới có thể truy xuất được các tập tin này còn những người khác thì bị từ chối truy cập. Ngoài ra, người quản trị mạng còn có thể dùng tác nhân phục hồi (**recovery agent**) để truy xuất đến bất kỳ tập tin nào bị mã hoá.
Để mã hoá các tập tin, tiến hành theo các bước sau:
Mở cửa sổ **Windows Explorer**.
Trong cửa sổ **Windows Explorer**, chọn các tập tin và thưc mục cần mã hoá. Nhấp phải chuột lên các tập tin và thư mục, chọn **Properties**.
Trong hộp thoại **Properties**, nhấn nút **Advanced**.
Hộp thoại **Advanced Properties** xuất hiện, đánh dấu mục **Encrypt contents to secure data** và nhấn OK.
Trở lại hộp thoại **Properties**, nhấn **OK**, xuất hiện hộp thoại **Confirm Attribute Changes** yêu cầu bạn cho biết sẽ mã hoá chỉ riêng thư mục được chọn (**Apply changes to this folder only**) hoặc mã hoá toàn bộ thư mục kể các các thư mục con (**Apply changes to this folder, subfolders and files**). Sau đó nhấn **OK**.
Để thôi không mã hoá các tập tin, bạn thực hiện tương tự theo các bước trên nhưng bỏ chọn mục **Encrypt contents to secure data**.

Chương 14: Maintaining Software by Using Software Update Services

Bài 10: DỊCH VỤ TRUY CẬP TỪ XA

Mục tiêu:

- Trình bày được khái niệm về dịch vụ truy cập từ xa;
- Cấu hình và sử dụng được tính năng Remote Desktop và Remote Assistant.
- Thực hiện các thao tác an toàn với máy tính.

1. Giới thiệu:

Terminal Service là một dịch vụ cho phép người dùng có thể truy cập vào server từ máy client đặt ở 1 vị trí khác bằng cách sử dụng giao thức Remote Desktop Protocol (RDP). RDP chuyển giao diện người dùng của Server về cho máy Client và chuyển các thông tin của hành động phím gõ và di chuyển chuột về lại cho Server.

Terminal Services là một dịch vụ trên Windows 2000, 2003 hỗ trợ người quản trị thực hiện các công việc trên Hệ điều hành Windows 2000, 2003 thông qua mạng mà không cần thiết phải ngồi trực tiếp tại máy đó. Đây là một công cụ rất cần thiết đối với người quản trị Windows.

Terminal Service sử dụng RDP (Remote Desktop Protocol) dựa trên nền TCP/IP. Trên Windows XP cũng có dịch vụ Remote Desktop được coi là bản rút gọn của Terminal Services trên Windows 2003. Remote Desktop trên Windows XP chỉ hỗ trợ 1 session duy nhất. Còn trên Windows 2003 hỗ trợ nhiều session, mỗi session được nối vào một desktop riêng biệt.

Terminal Services client sử dụng port 3389 TCP cho việc truyền thông với máy tính từ xa.

Remote Desktop bao gồm các phần sau :

- Giao thức Remote Desktop
- Phần mềm Client : Remote Desktop Connection

Các chế độ kết nối Remote Desktop:

- Remote Session: trong chế độ này, server sẽ dành tài nguyên của nó là bộ nhớ để cho mỗi user kết nối tới, do đó kết nối Remote desktop giữa các user là độc lập với nhau, và Remote Desktop Server không bị khoá lại.
- Console Session: trong chế độ này, server share bộ nhớ chung với user đang log on locally trên server, do đó, tại 1 thời điểm chỉ logon trên 1 máy, nếu máy này logon vào ngay lập tức máy kia sẽ bị logoff ra ngay và ngược lại.

* Mặc định trên các máy có HĐH Server, nó cho cả 2 chế độ kết nối, còn các máy có HĐH thường làm Remote Desktop Server thì chỉ hỗ trợ mỗi kiểu kết nối là Console.

Vd: trong Windows XP, chỉ cho kết nối theo kiểu Console.

2. Cấu hình dịch vụ Remote Desktop:

Bước 1: Kích hoạt tính năng "Remote Desktop" trên Windows Server 2003

- Trên Windows Server 2003: **Start -> Control Panel -> System**

Trong Tag "**Remote**", đánh dấu chọn vào "**Enable Remote Desktop on this computer**" như hình dưới

Bước 2: Xác định tài khoản được phép Remote Desktop

Start -> Administrative Tools -> Computer Management

Chúng ta quan sát thấy một Group người dùng có tên là "**Remote Desktop Users**", những user nào nằm trong nhóm người dùng này sẽ được phép thực hiện Remote Desktop

Nhấp đôi vào "**Remote Desktop Users**", Mặc định Group này chỉ có một user là "**Administrator**", nếu muốn chúng ta có thể thêm user khác vào Group này để cho phép user này thực hiện Remote Desktop. Ví dụ bên dưới chúng ta thêm một user mới là "**WebAdmin**".

Bước 3: Thực hiện Remote Desktop từ máy client.

Trong Window 7: **Start -> All Programs -> Accessories -> Remote Desktop Connection**

Nhập vào địa chỉ IP hoặc tên máy chủ. Ví dụ bên dưới địa chỉ IP: 192.168.10.117. Chọn "**Connect**"

Nhập vào **User** (bất kỳ user nào nằm trong Group nói đến ở trên) và mật khẩu đăng nhập.

3. Cấu hình dịch vụ Remote Assistant:

Remote Assistance là một tính năng trên Windows XP. Có thể thấy nó gần giống như Remote Desktop, khá giống với Net Meeting.

Với chức năng Remote Assistance, một người sử dụng XP, khi gặp khó khăn sẽ gửi yêu cầu được giúp đỡ - gọi là novice – đến người hỗ trợ - được gọi là expert. Hai bên có thể giao tiếp thông qua cửa sổ chat, talking qua micro, hoặc điều khiển trực tiếp trên desktop của novice. Tất cả với mục đích để người hỗ trợ có thể hướng dẫn một cách chi tiết với người sử dụng XP.

Hướng dẫn dưới đây thực hiện trên Windows XP, tuy nhiên nó cũng có thể áp dụng Windows 2003.

Bước 1: Kiểm tra thiết lập Remote Assistance (trên Novice)

- Trong **Control Panel**, nhấp đúp vào biểu tượng **System** (hoặc trên Desktop, chuột phải vào biểu tượng My Computer, trên menu chuột phải, nhấp Properties.

Trong hộp thoại **System Properties**, chọn tab **Remote**. Chắc chắn đã đánh dấu lựa chọn ở A**llow Remote Assistance invitations to be sent from this computer**. Sau đó nhấp nút **Advanced…**

Trong hình bên dưới, chắc chắn đã đánh dấu lựa chọn **Allow this computer to be controlled remotely**. Ô I**nvitations** cho phép xác lập thời gian có hiệu lực tối đa của một **invitation**. Ngầm định là 30 ngày.

Bước 2: Tạo một invitation của Remote Assistance (trên Novice)

Sau khi kiểm tra thiết lập Remote Assistance, người sử dụng Novice cần tạo một **invitation.**

Click **Start->Programs->Remote Assistance.**

click vào **Invite someone to help you.**

Trong hình trên, có thể lựa chọn phương thức gửi invitation: gửi qua Windows Messenger, qua e-mai, hoặc lưu invitation dưới dạng một file. Ở đây, ta chọn **Save invitation as a file (Advanced).**

Ở hình trên, nhập tên mà bạn muốn xuất hiện trong invitation (với mục đích để Expert biết được Novice nào) và thời hạn có hiệu lực của invitation đó. Ngầm định thời hạn có hiệu lực là 1 giờ. Sau đó nhắp nút **Continue** để tiếp tục.

Trong hình trên, ta nên đánh dấu lựa chọn **Require the recipient to use a password**, sau đó nhập mật khẩu vào hai ô tương ứng Type password và Confirm password. Nhắp nút **Save Invitation** để lưu lại các thông tin trên.

Lưu lại tên file invitation (file có đuôi .msrcincident). Sau khi tạo file invitation, gửi đến **Expert**. Kết thúc việc tạo **invitation** trên **Novice.**

Bước 3: Kết nối từ Expert System đến Novice System

Khi Expert nhận được file invitation (đuôi .msrcincident), Exper dùng Explorer để

Sau khi nhắp đúp vào file, xuất hiện hộp thoại Remote Assistance như hình trên với các thông tin: từ Novice nào, thời gian hết hiệu lực của invitation và yêu cầu nhập mật khẩu. Mật khẩu này do Novice tạo ra ở Bước 2. Sau đó nhắp nút **Yes** để xác nhận.

Sau khi xác nhận, trên máy tính của Expert sẽ chạy chương trình Remote Assistance kết nối đến máy của Novice cần được trợ giúp. Khi đó trên desktop của Novice xuất hiện hộp thoại yêu cầu việc xác nhận kết nối.

Khi đó Novice nhắp **Yes** để cho phép kết nối đến máy của mình. Trên máy của Novice sẽ xuất hiện hộp thoại chứa cửa sổ chat và các điều khiển của Remote Assistance.

Giao diện trên máy của Expert cũng có cửa sổ chat, các điều khiển và Desktop của máy Novice (ở chế độ View-Only)

Khi kết nối, Expert không điều khiển được Desktop của Novice mà chỉ theo dõi được các thao tác của Novice trên Desktop. Khi Expert muốn điều khiển Desktop của Novice, trong hình trên, **Expert** nhắp chuột vào biểu tượng **Take Control**. Khi đó trên desktop của Novice xuất hiện hộp thoại sau.

Trên máy Novice, nhắp **Yes** để cho phép điều khiển Desktop. Khi Novice muốn chấm dứt việc Expert điều khiển Desktop của mình, Novice có thể ấn phím **Esc.**

TÀI LIỆU THAM KHẢO

[1] Tài liệu *Quản trị Windows Server 2003* của trung tâm tin học Đại học Khoa học Tự nhiên.

[2] Giáo trình *Mạng doanh nghiệp* của Đại học sư phạm kỹ thuật Hưng Yên.

[3] Các bài *Lab MCSA* của trung tâm Đào tạo mạng máy tính Nhất Nghệ.

[4] Giáo trình *Quản trị mạng và Các thiết bị mạng* của Trung tâm Điện toán Truyền số liệu KV1.

[5] Các tài liệu và bài giảng khác tham khảo từ Internet.